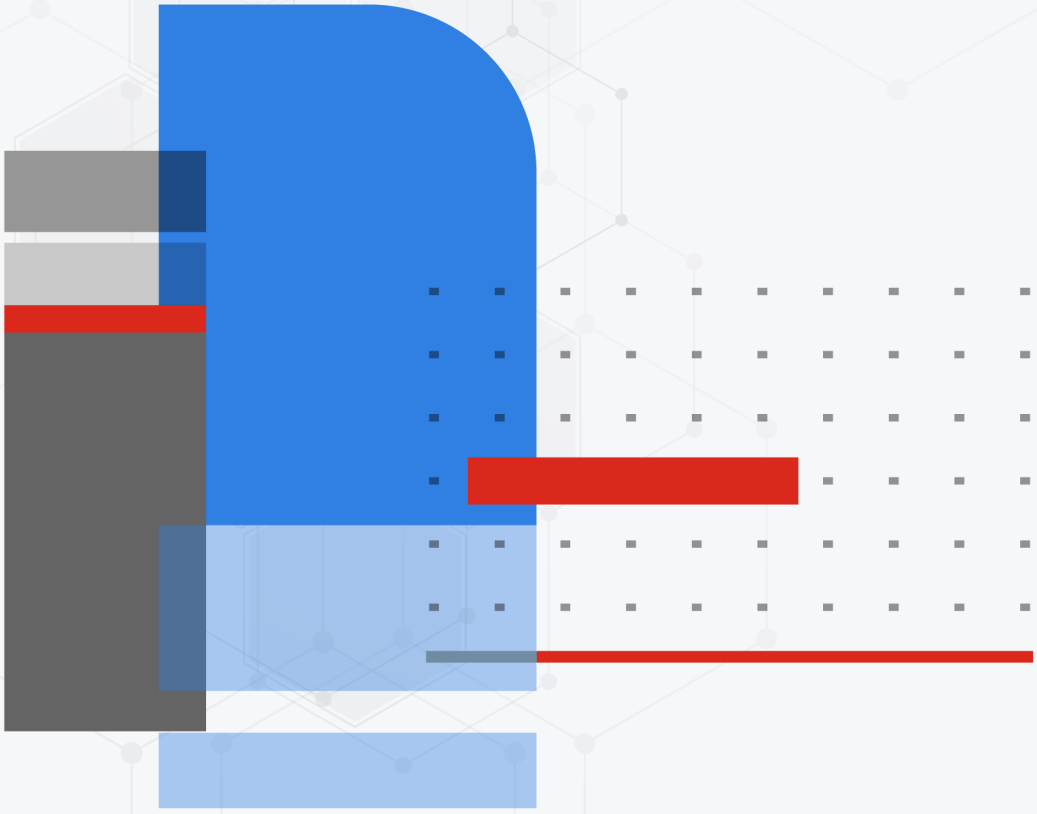
SD-WAN Overlay Migration from OCVPN to OaaS Deployment Guide

Overlay-as-a-Service 23.3



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 7, 2023
Overlay-as-a-Service 23.3 SD-WAN Overlay Migration from OCVPN to OaaS Deployment Guide
85-233-810439-20230907

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-09-07	Initial release.

Deployment overview

In FortiOS 7.2.4 and earlier, FortiOS supports Overlay Controller VPN (OCVPN), which is a cloud based solution to simplify IPsec VPN setup. When OCVPN is enabled, IPsec phase1-interfaces, phase2-interfaces, static routes, and firewall policies are generated automatically on all FortiGates that belong to the same community network. A community network is defined as all FortiGates registered to FortiCare using the same FortiCare account.

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 7.4.1 and later.

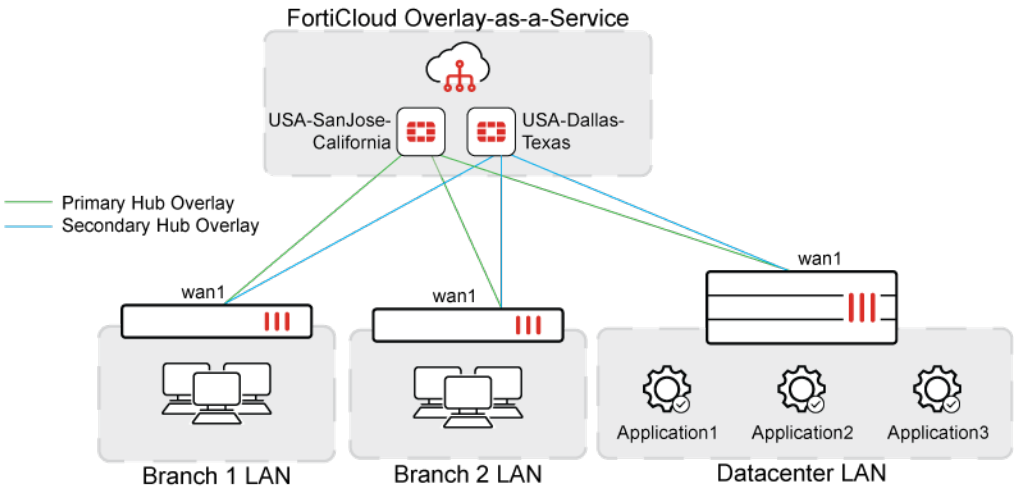
Currently, OaaS supports a geo-redundant, dual hub architecture where the SD-WAN overlay hub is powered by FortiOS and managed by FortiCloud, and your branch FortiGates and datacenter FortiGates are configured as spokes within this overlay.

- 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 just 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.

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 7.4.1 and later.



This document provides a deployment example of Fortinet Inc.'s Secure SD-WAN solution covering the migration of an existing hub-spoke SD-WAN with ADVPN shortcut solution orchestrated using OCVPN to the geo-redundant, dual hub architecture for a single SD-WAN region orchestrated using OaaS.

Using a similar scenario and topology example from the Single datacenter (active-passive gateway) section of the SD-WAN Architecture for Enterprise guide, we will walk through deploying the core components by providing configuration examples to help you migrate from OCVPN to OaaS for a hub-spoke ADVPN shortcut SD-WAN overlay solution.

The goal is to pivot from reliance on the OCVPN cloud portal and OCVPN-generated configuration on the FortiGate devices to using the FortiCloud OaaS cloud portal and an OaaS topology to generate SD-WAN overlay configuration on these devices. We will focus on the services located within on-premise datacenters and on providing users working in regional branches or offices with access to those services.

Audience

This guide is primarily created for a technical audience, including system architects and design engineers, who want to deploy Fortinet Inc. Secure SD-WAN in brownfield, or existing scenarios where the existing solution has been orchestrated using OCVPN.

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

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.

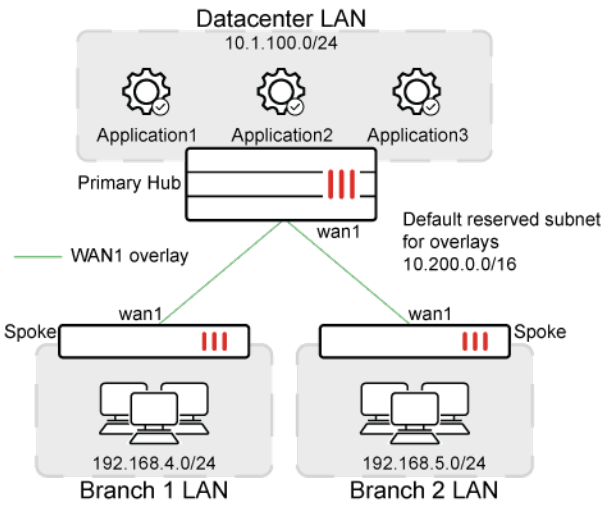
Design considerations

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

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

OCVPN hub-spoke with ADVPN shortcut architecture

OCVPN supports a hub-and-spoke with ADVPN shortcut network topology. See Hub-spoke OCVPN with ADVPN shortcut.



Traditionally referred to as hub and spoke, this design is the fundamental building block of our solution. In this design, the SD-WAN Gateway (sometimes referred to as the hub or *Primary Hub* in the diagram) acts as a headend into the business application or private workload. SD-WAN gateways can be located in a single datacenter or central office, and typically provide connectivity for remote locations.

This architecture uses the BGP per overlay method for its routing design. See BGP per overlay.

This example topology will be used to demonstrate deployment procedures to migrate this SD-WAN deployment from OCVPN to OaaS. In the topology, 10.254.0.0/16 is the default reserved subnet used for IP addressing of overlays.

Migrating from OCVPN to OaaS

To migrate from OCVPN to OaaS, it is important to convert the OCVPN hub-spoke with ADVPN shortcut network topology into an OaaS network topology that works in a similar way.

OaaS supports a different hub-spoke architecture than the OCVPN hub-spoke architecture:

- Datacenter LAN is implemented behind a spoke instead of behind a hub (*Primary Hub*).
- LAN interfaces on the hub do not contain any customer resources or services.
- The hub is maintained by Fortinet Inc. within the FortiCloud infrastructure.

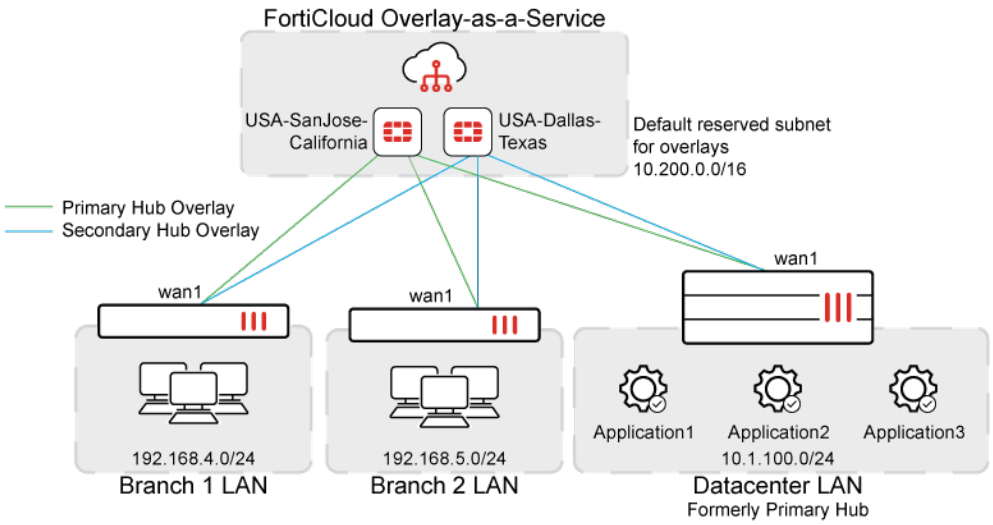
Nevertheless, the OaaS hub-spoke architecture achieves the same functionality as the OCVPN hub-spoke architecture, namely, that spokes (branches) can access resources on the hub (datacenter) and that spokes can access other spokes directly. With the OaaS hub-spoke architecture, spoke-to-datacenter and spoke-to-spoke access are both achieved by using ADVPN shortcut tunnels.

OaaS SD-WAN geo-redundant, dual hub architecture

OaaS supports a geo-redundant, dual hub architecture for a single SD-WAN region 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.

This architecture uses the BGP on loopback method for its routing design. See BGP on loopback.

OaaS can configure an overlay for the hub-and-spoke topology using ADVPN and two geo-located hubs which work the same way as the OCVPN network topology presented above:



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 above hub-and-spoke topology, the SD-WAN overlay hub is powered by FortiOS and deployed in FortiCloud where a primary hub and a secondary hub 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 for retrieving interface information and for installing configuration settings orchestrated from OaaS.

By default, OaaS has reserved 10.200.0.0/16 by default for overlay IP addressing of all spokes and this network should not be used in either the LAN subnets or WAN network. If there is conflict, this reserved subnet can be modified 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.

Deployment assumptions

The following is assumed:

- Brownfield deployment of existing Fortinet Inc. Secure SD-WAN FortiGate devices, which have been previously and successfully configured using the OCVPN cloud portal on a supported FortiOS version (FortiOS 7.2.4 and below).
- Each remote site or spoke includes a FortiGate VM or hardware device with a valid OaaS license.
- Upon upgrading to FortiOS 7.4.1 and later, all IPsec Phase 1 and Phase 2 configuration, firewall policies, and routing configuration previously generated by the OCVPN service will remain although the OCVPN-specific configuration in `config vpn ocvpn` will be removed.

- The spokes' ISPs must allow traffic over UDP port 500 and UDP port 4500 for NAT traversal (NAT-T) for ADVPN tunnels to be set up successfully.
- 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.
- Each remote site or spoke has a single WAN connection.
- WAN connections can reach all other devices in the region.
- All WAN interfaces have already been configured and have default gateways and 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 7.4.1 and later.

Product prerequisites

The following are product prerequisites:

- FortiOS 7.4.1 or later on the FortiGates acting as spokes.
- FortiCloud Overlay-as-a-Service licenses for all spokes.

Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 10 for detailed configuration steps:

1. Review the existing OCVPN configuration settings on the FortiGate devices and plan OaaS configuration settings, accordingly; ensuring no conflicts occur between these two sets of configuration settings.
2. Prepare the FortiGate devices for OaaS by upgrading the FortiGate device to FortiOS 7.4.1 or above, and running FortiGate CLI commands to remove conflicting configuration settings.
3. Using the OaaS portal, orchestrate and install OaaS configuration settings that will exist alongside the existing OCVPN configuration on the FortiGate devices.
4. Perform testing and verification of the OaaS configuration.
5. (Optional) Delete the OCVPN configuration.

Deployment procedures

The 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:

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

OaaS only supports FortiGate devices running FortiOS 7.4.1 and later.

Prerequisites

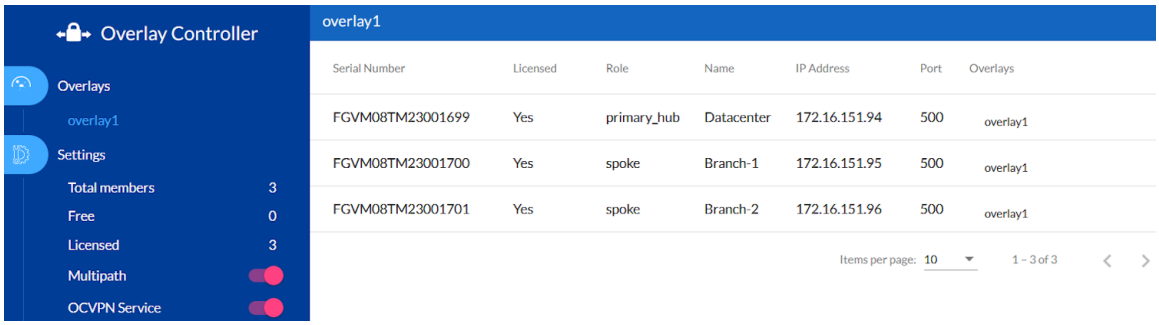
This guide presumes the following prerequisites have been met:

- All FortiGate spokes sites (branches and datacenters) have an OaaS license.
- All FortiGates in the SD-WAN region are running FortiOS 7.4.1. or 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 in any existing network zone.
- The WAN port is not bound to any SD-WAN zone.

Review existing OCVPN configuration and plan OaaS configuration

The existing configuration in this deployment guide is based on the hub-and-spoke with ADVPN shortcut network topology that has been orchestrated using OCVPN.

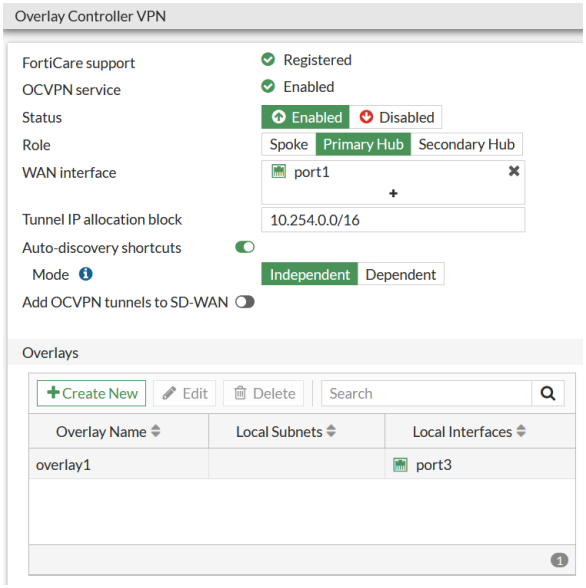
The OCVPN portal is accessible at https://ocvpnportal.fortinet.com.



Review the existing configuration generated by OCVPN. Take note of the WAN interfaces and the LAN interfaces and subnets behind the FortiGate hub device and behind the FortiGate spoke devices.

OCVPN Datacenter primary hub configuration:

- In the GUI:

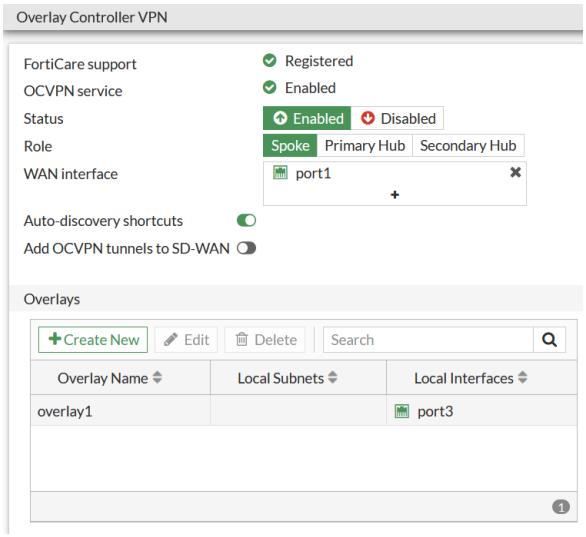


- In the CLI:

```
config vpn ocvpn
    set status enable
    set role primary-hub
    set wan-interface “port1”
    set nat disable
    set ip-allocation-block 10.254.0.0 255.255.0.0
    config overlays
        edit “overlay1”
            config subnets
                edit 1
                    set type interface
                    set interface “port3”
                next
            end
        next
    end
end
```

OCVPN Branch-1 spoke configuration:

- In the GUI:



- In the CLI:

```
config vpn ocvpn
    set status enable
    set wan-interface "port1"
    config overlays
        edit "overlay1"
            config subnets
                edit 1
                    set type interface
                    set interface "port3"
                next
            end
        next
    end
end
```

WAN interfaces:

- WAN is connected to port1 on the Datacenter FortiGate.
- WAN is connected to port1 on the Branch 1 FortiGate.
- WAN is connected to port1 on the Branch FortiGate.

These WAN links will be configured as ISPs in the OaaS topology.

LAN interfaces:

- LAN is connected to port3 on the Datacenter FortiGate.
- LAN is connected to port3 on the Branch 1 FortiGate.
- LAN is connected to port3 on the Branch 2 FortiGate.
- Datacenter LAN is 10.1.100.0/24.
- Branch 1 LAN is 192.168.4.0/24.
- Branch 2 LAN is 192.168.5.0/24.

These LAN subnets will be configured as subnets in the OaaS topology.

Based on the prerequisites for OaaS, the following OCVPN-generated configuration settings are not compatible with the OaaS-generated configuration settings and will need to be removed:

- Firewall policies
- BGP network table
- SD-WAN members, if previously configured

Planning the new configuration

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

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

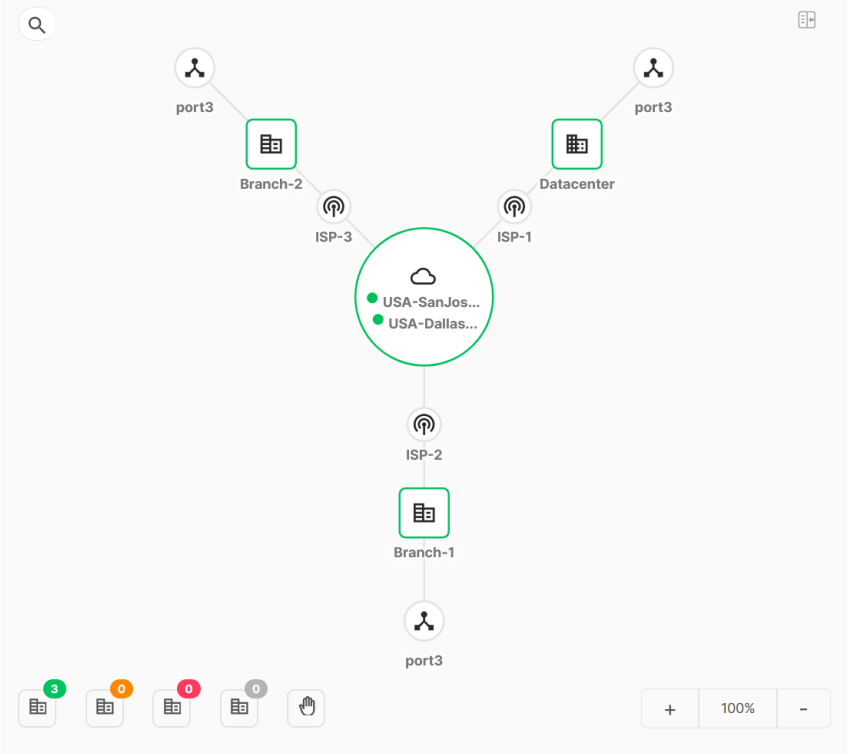
Firewall policies

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

OaaS creates wildcard allow policies for the tunnel overlays on the spoke FortiGates. For some cases, these policies do not provide the necessary granularity to restrict overlay traffic to specific subnets or hosts.

Network Topology

The deployment example in this guide uses the below network topology in the OaaS portal:



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

OaaS topology component	SD-WAN topology component
USA-SanJose-California FortiCloud Hub	Primary Hub
USA-Dallas-Texas FortiCloud Hub	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 spoke
ISP-2	Underlay used by Branch-1 spoke
port3	Branch-1 LAN
Branch-2 (Branch site type)	Spoke at Branch-2 location
ISP-3	Underlay used by Branch-2 spoke
port3	Branch-1 LAN

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

Prepare FortiGate devices for OaaS

Prepare the FortiGate devices for OaaS by upgrading the FortiGate device to FortiOS 7.4.1 or above, and running FortiGate CLI commands to remove conflicting configuration settings:

- Upgrade FortiOS firmware on page 15
- Remove incompatible configuration settings on page 15

Upgrade FortiOS firmware

OaaS supports FortiGate devices running FortiOS 7.4.1 or above. Therefore, each FortiGate device in the topology needs to be upgraded to FortiOS 7.4.1 or above prior to being included in an OaaS topology.

See Firmware & Registration in the FortiOS Admin Guide for different methods of upgrading FortiOS firmware on the FortiGate devices.

Remove incompatible configuration settings

Based on the prerequisites for OaaS, the following OCVPN-generated configuration settings are not compatible with the OaaS-generated configuration settings and will need to be removed using the CLI commands below:

Deleting firewall policies for WAN and LAN ports will disrupt all user traffic including outgoing Internet access and incoming server access on your network and should not be performed on FortiGate devices in production environments.

Ensure you have scheduled a maintenance window and have performed a FortiGate configuration backup before removing any firewall policies. See Configuration Backups in the FortiOS Administration Guide.

After installing the configuration settings orchestrated by OaaS, you must selectively restore the firewall policies for WAN ports and must recreate firewall policies for LAN ports using the `oaas_lan_zone` instead of LAN ports to restore all user traffic on your network.

- Firewall policies:

```
config firewall policy
    purge
        This operation will clear all table!
        Do you want to continue? (y/n)y
end
```

- BGP network table:

```
config router bgp
    config network
        purge
            This operation will clear all table!
            Do you want to continue? (y/n)y
    end
end
```

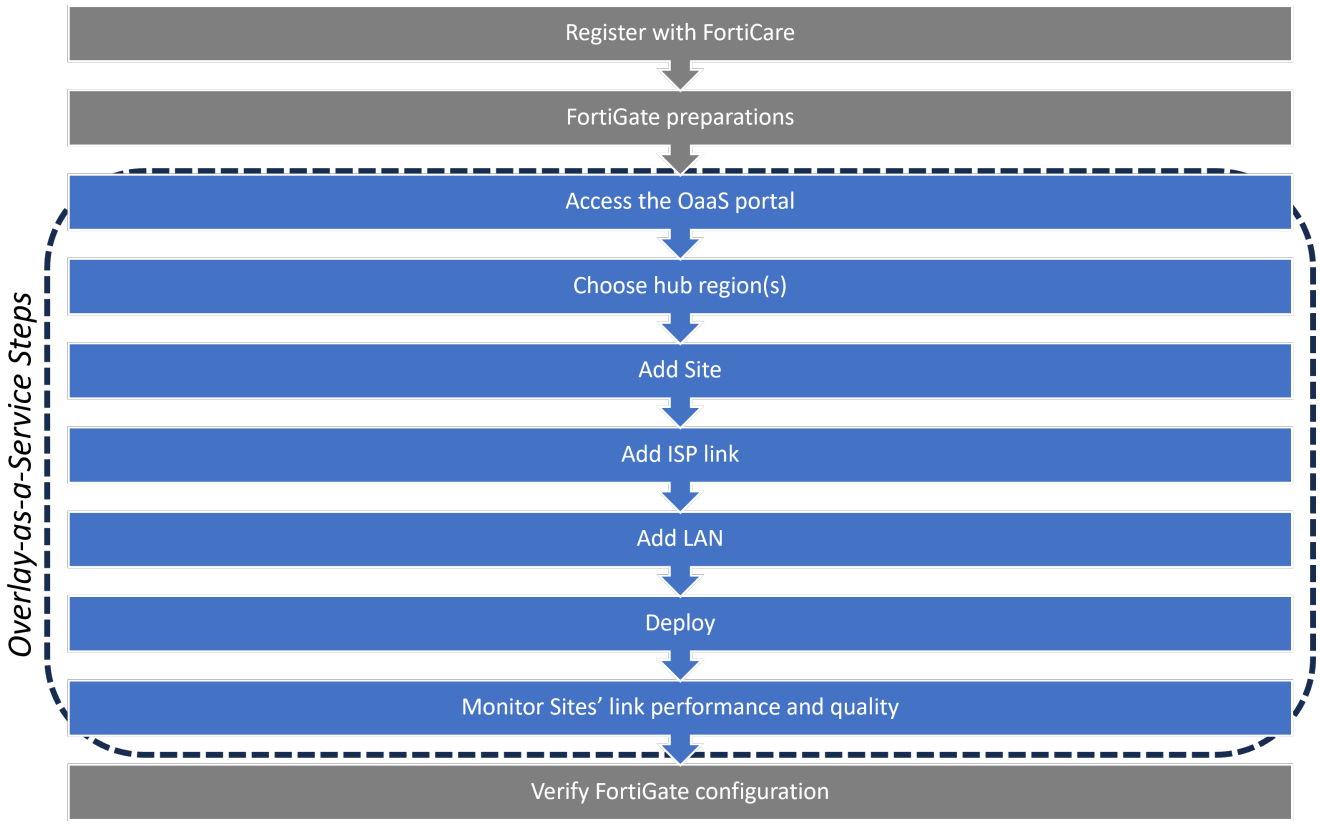
- SD-WAN members, if Add OCVPN tunnels to SD-WAN was enabled in OCVPN settings (`set sdwan enable` under `config vpn ocvpn`):

```
config system sdwan
    config members
        purge
            This operation will clear all table!
            Do you want to continue? (y/n)y
    end
end
```

Configuration steps in OaaS

Following is a summary of the steps required to configure an SD-WAN overlay using FortiCloud OaaS for orchestration:

1. Register FortiCloud OaaS licenses in FortiCloud. See Registering FortiCloud Overlay-as-a-Service licenses in FortiCloud on page 17.
2. Prepare the FortiGate SD-WAN devices for integration with OaaS. See Preparing the FortiGate SD-WAN devices on page 17.
3. Deploy a new SD-WAN region by configuring the topology of the FortiGate in OaaS. See Deploying the new SD-WAN region using OaaS on page 19.
   a. Choose hub regions.
   b. Add site.
   c. Add ISP link.
   d. Add LAN.
   e. Deploy.
4. Monitor link performance and quality across SD-WAN devices in OaaS. See Monitoring link performance and quality across SD-WAN devices in OaaS on page 24.
5. Test and verify connectivity between sites deployed using OaaS. See Testing and verifying connectivity between sites deployed using OaaS on page 27.



Registering FortiCloud Overlay-as-a-Service licenses in FortiCloud

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. Please refer to the OaaS ordering guide for details.

Currently, the OaaS requires each spoke FortiGate to have an OaaS SKU applied to it. You must register FortiGate devices used with OaaS to the same FortiCloud account used to log into OaaS. You must also obtain a FortiCloud OaaS license and apply it to each FortiGate device in the overlay.

For details on registering products, see Registering assets.

Preparing the FortiGate SD-WAN devices

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 FortiCloud, and activate the FortiGate devices with FortiGate Cloud. See Registering with FortiCloud and activating with FortiGate Cloud on page 17.
2. Configure each FortiGate with a WAN IP address and a default gateway IP address for accessing the Internet. See Configuring the FortiGate on page 18.

Registering with FortiCloud and activating with FortiGate Cloud

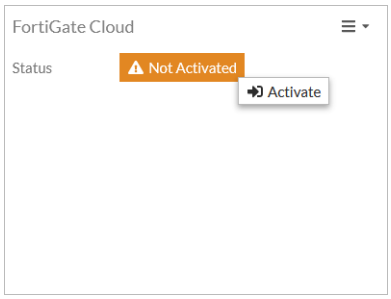
The FortiGate devices must be registered with FortiCloud and activated with FortiGate Cloud.

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

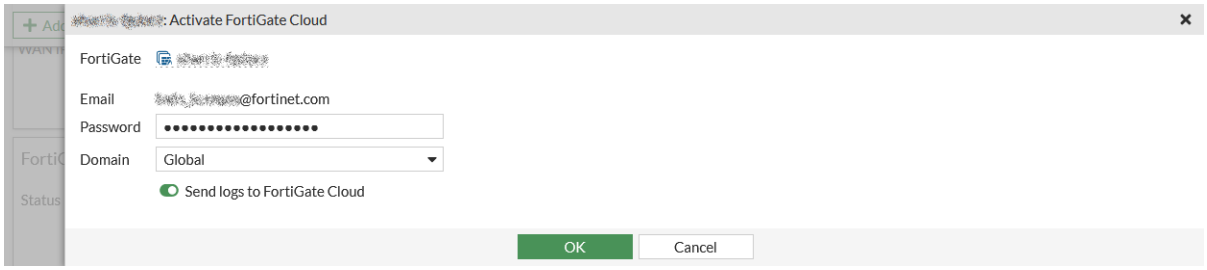
Typically, for FortiGate devices already registered with FortiCloud, you can activate them on the FortiGate GUI.

To configure an additional incoming interface on a spoke:

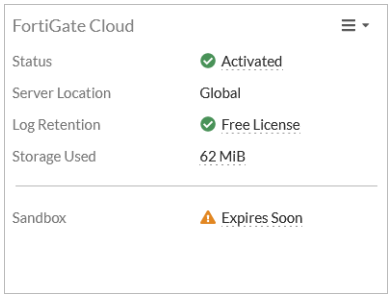
1. Go to *Dashboard* > *Status*.
2. In the *FortiGate Cloud* widget, click *Not Activated* > *Activate*.



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 in the FortiCloud Asset Management Guide.

For details on activating the FortiGate with FortiGate Cloud, see FortiCare and FortiGate Cloud login in the FortiOS Administration Guide.

Configuring the FortiGate

The FortiGate must be configured with a WAN IP address and default gateway for accessing the Internet. See Basic configuration in the FortiOS Administration Guide.

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

OaaS has specific requirements for the FortiGate configuration prior to orchestration:

- WAN and LAN ports must not be in any predefined zone and must not be a member of any other SD-WAN zone. See Zone in the FortiOS Administration Guide.
- WAN and LAN ports must not be bound to any existing firewall policies. See Firewall Policy in the FortiOS Administration Guide.
- 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 in the FortiOS Administration Guide.

These steps are required because OaaS will be obtaining the interface configuration and displaying it for overlay configuration in the OaaS portal.

Deleting firewall policies for WAN and LAN ports will disrupt all user traffic including outgoing Internet access and incoming server access on your network and should not be performed on FortiGate devices in production environments.

Ensure you have scheduled a maintenance window and have performed a FortiGate configuration backup before removing any firewall policies. See Configuration Backups in the FortiOS Administration Guide.

After installing the configuration settings orchestrated by OaaS, you must selectively restore the firewall policies for WAN ports and must recreate firewall policies for LAN ports using the `oaas_lan_zone` instead of LAN ports to restore all user traffic on your network.

Deploying the new SD-WAN region using OaaS

The general process of deploying a new SD-WAN region using OaaS is as follows:

1. Access the Overlay-as-a-Service portal. See Accessing the OaaS portal on page 19.
2. Choose the hub locations. See Choosing the hub locations on page 19.
3. Add a new site. See Adding a new site on page 20.
4. Add an ISP for your site. See Adding an ISP for your site on page 21.
5. Add a subnet for your site. See Adding a subnet for your site on page 22.
6. Apply the changes. See Applying changes and viewing Task Status on page 23.

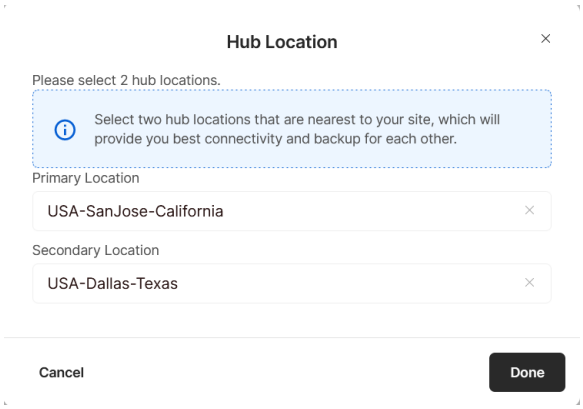
Accessing the OaaS portal

To access the Overlay-as-a-Service portal, go to https://overlay-as-a-service.forticloud.com/ and log in using your FortiCloud account. Upon log in, you will enter the *Home* view.

Choosing the hub locations

To choose the hub locations:

1. Go to *Topoology*. The Setup Topology view is displayed.
   Right-click the *Hub*.
2. Click *Choose two locations*. The *Hub Location* dialog opens.
3. Use the *Primary Location* and *Secondary Location* dropdown lists to select your locations.



4. Click *Done*.

Adding a new site

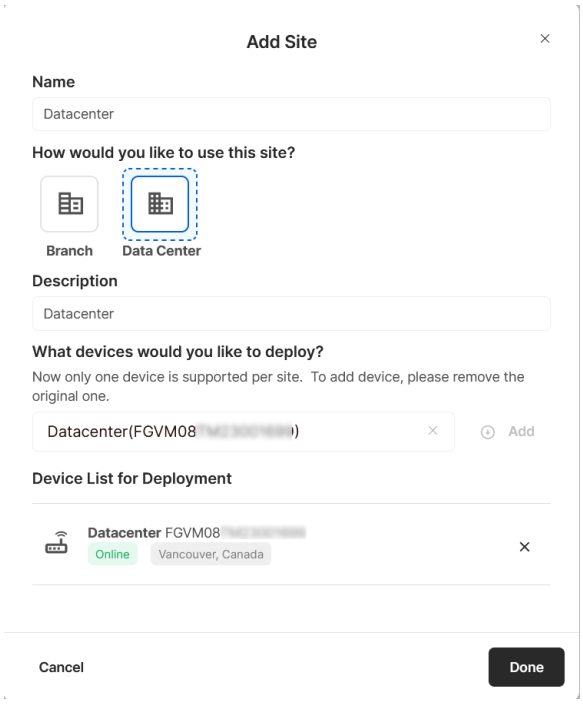
Sites are authorized FortiGate SD-WAN devices. Add FortiGate devices to the region.

To add a site:

1. Click the *Hub*.
2. Select *Add Site*. The *Add Site* dialog opens.
3. Enter a *Name* for the site.
4. Set the site as either a *Branch* or *Data Center*.

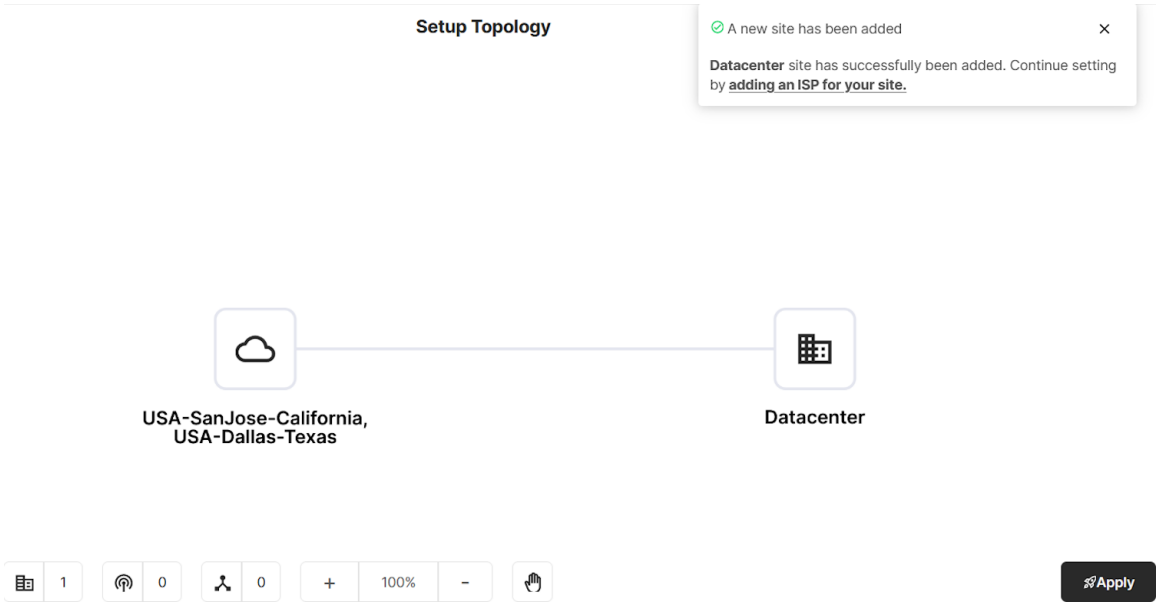
Branch and *Data Center* sites affect how the site is displayed on the *Home* and *Topology* pages. OaaS configuration and management is not affected.

5. (Optional) Enter a *Description*.
6. Select the FortiGate device to deploy from the *Device* dropdown menu.
7. Click *Add*.



It is critical that the FortiGate device added for deployment appears with the status of *Online*. If not, you must perform some troubleshooting to check if the device has been powered on, has been activated or logged in to FortiGate Cloud, and is configured and connected to its ISP's WAN link properly.

8. Click *Done*. A new site is connected to the hub.

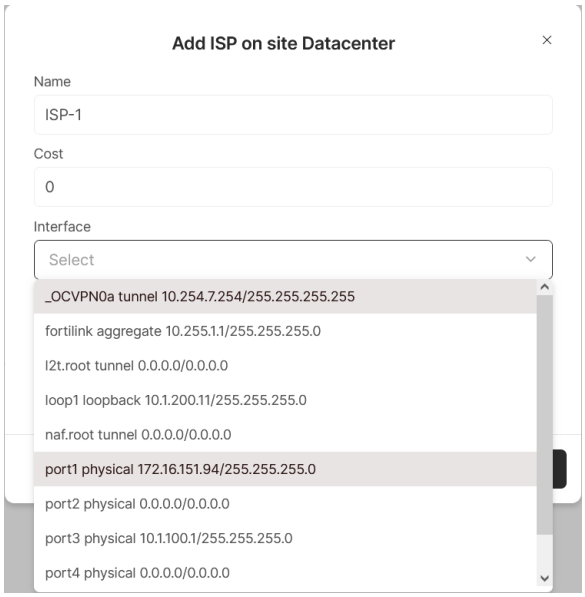


Adding an ISP for your site

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

To add an ISP:

1. Click the site.
2. Select *Add ISP*. The *Add ISP on site <Site>* dialog opens.
3. Enter a *Name* for the ISP.
4. Enter the cost assigned to the ISP in the *Cost* field.
5. Select the interface from the *Interface* dropdown list.



6. (Optional) Enter a *Description*.
7. Click *Done*.

Adding a subnet for your site

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

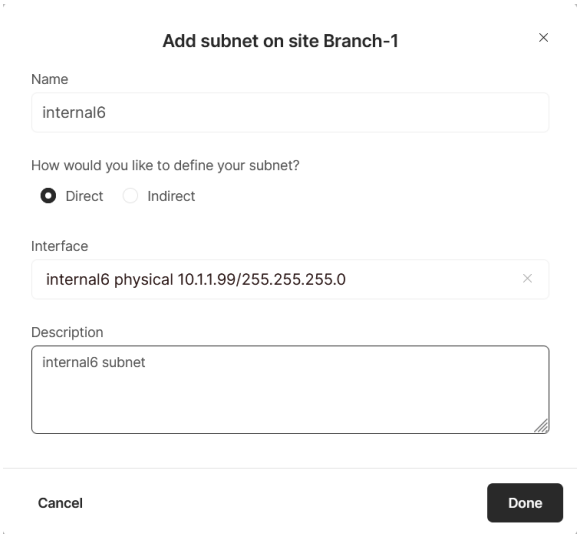
To add a subnet:

1. Click the site.
2. Select *Add Subnet*. The *Add subnet on site <Site>* dialog opens.
   a. Enter a *Name*.
   b. Select *Direct* or *Indirect* for the subnet definition.

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, 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 from the *Interface* dropdown list.



d. (Optional) Enter a *Description*.

e. Click *Done*.

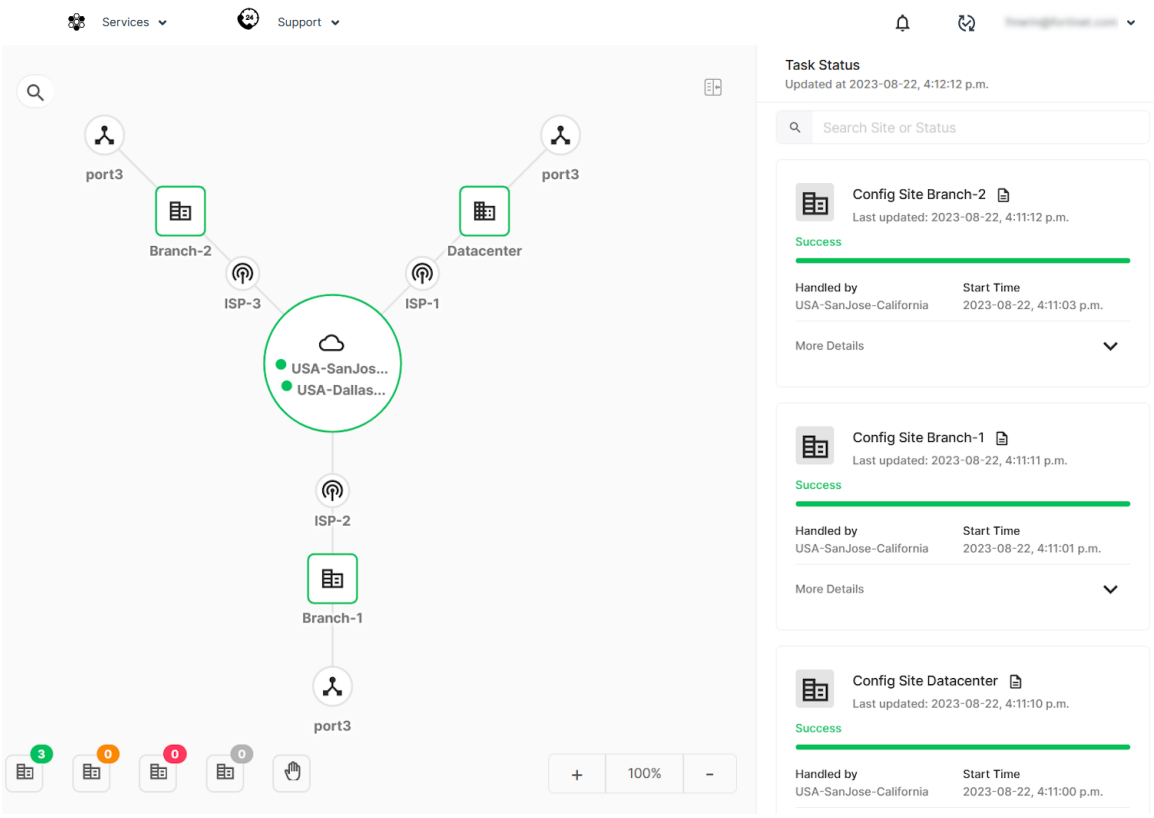
Applying changes and viewing Task Status

You may wish to add several sites with their corresponding ISP and subnets in the *Topology* view. For this deployment example, you will need to add Branch-1 and Branch-2 sites to the topology.

When have completed adding sites and their corresponding configuration, apply the change.

To apply changes:

1. Click *Apply*. After clicking *Apply*, the sync process runs in the background.
2. Click the *X* at top-right to close the *Setup Topology* page 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.



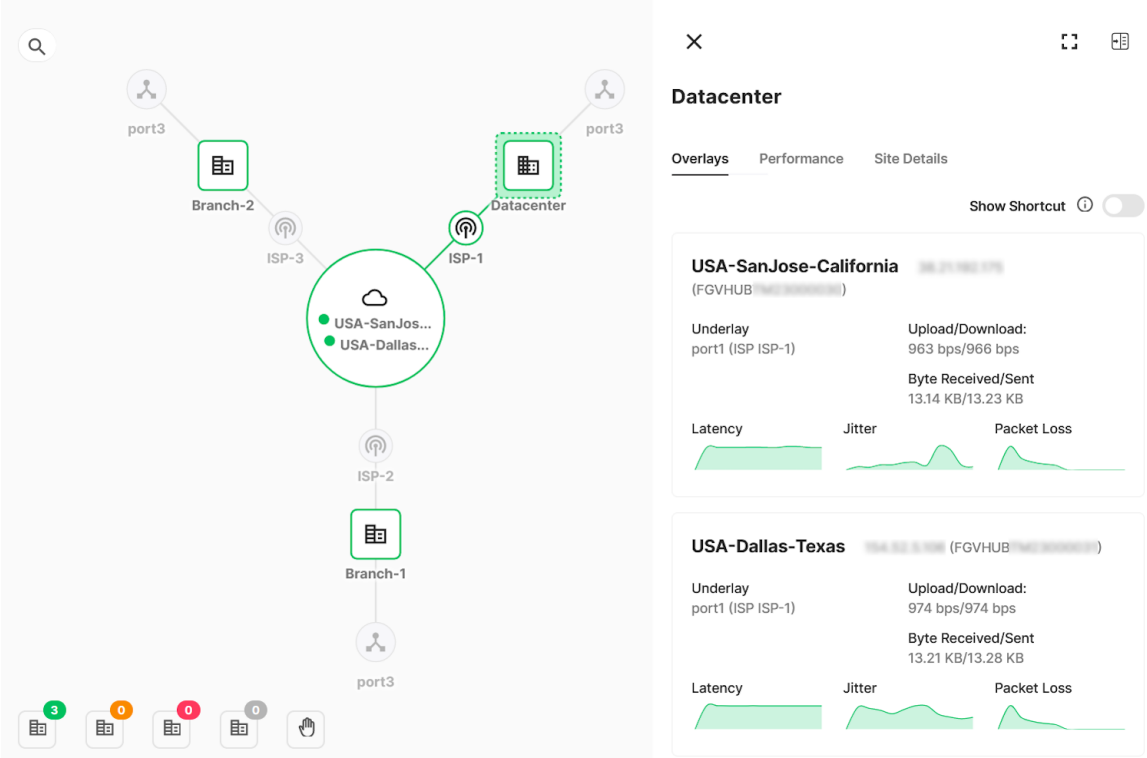
You can view the FortiGate configuration that was installed by the task by clicking on the *View Config* icon to the right of the task name. A pane with the configuration that was installed by the task will display.

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

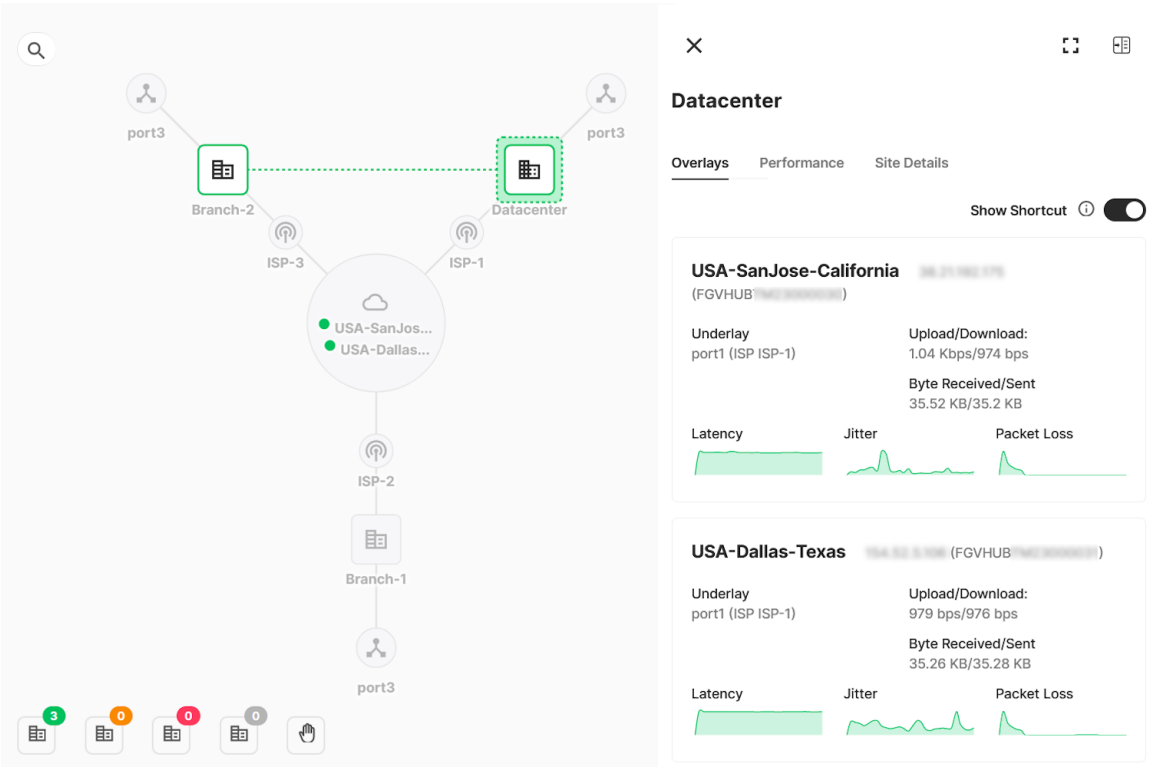
Monitoring link performance and quality across SD-WAN devices in OaaS

In the *Home* page, you can monitor link performace:

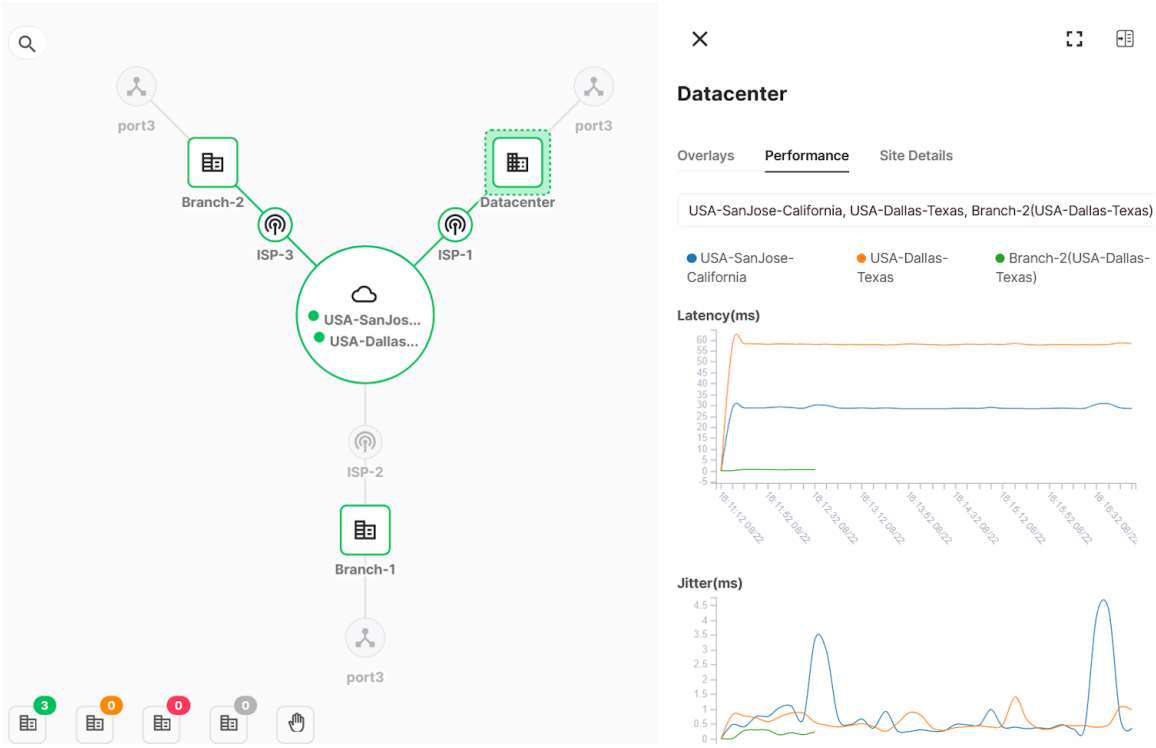
- Select any of the sites in the diagram to monitor the health of their *Overlays*, monitor the *Performance*, and view *Site Details*.



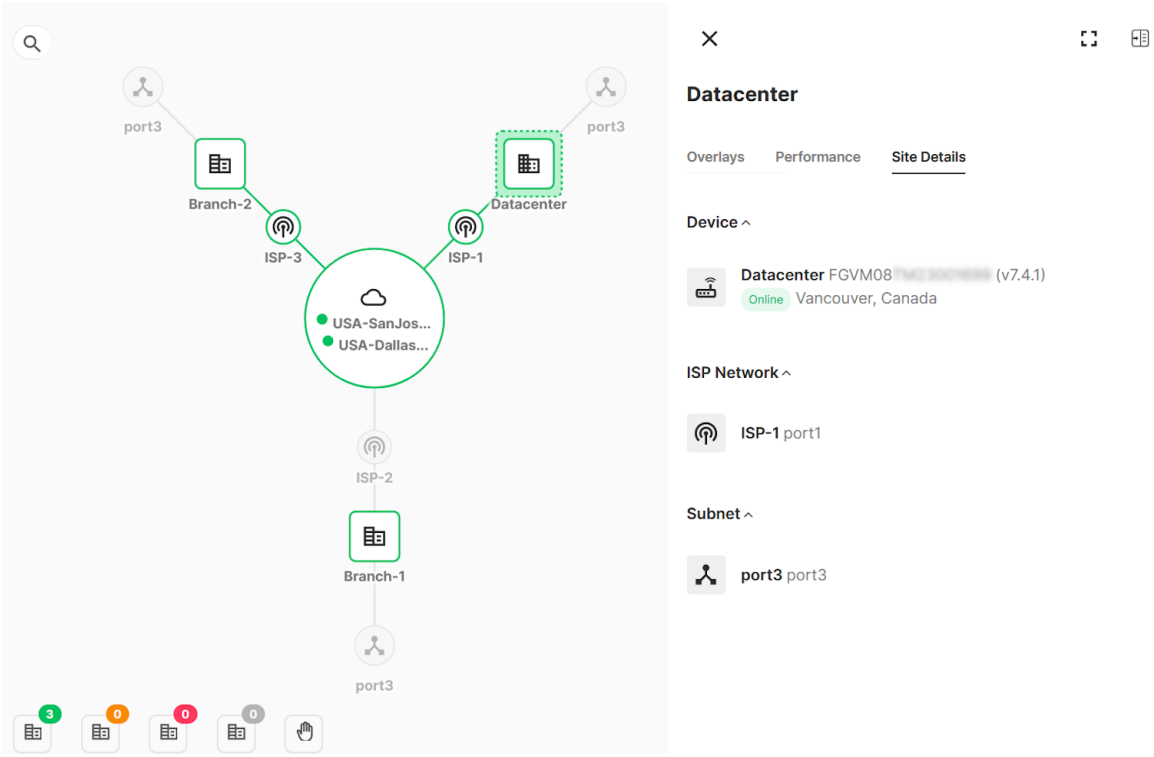
- Select *Overlays* and enable *Show Shortcut* to monitor the health of the shortcut tunnels between sites.



- Select *Performance* and then monitor the latency, jitter, and packet loss in graphs. Select a time stamp to view the values for the hub locations and remote sites on the graphs.



- Select *Site Details* to review a site's details.



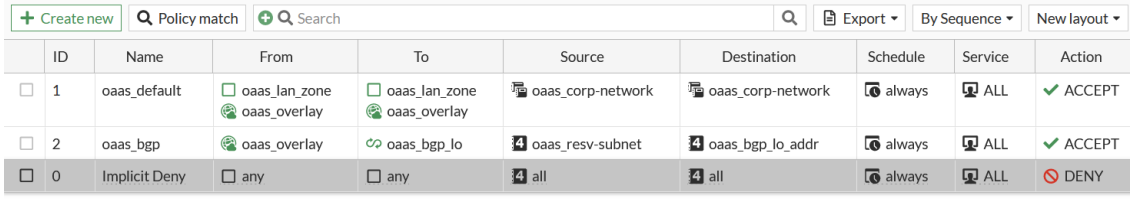
Testing and verifying connectivity between sites deployed using OaaS

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

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 wildcard allow policies for the tunnel overlays on the spoke FortiGates. 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 reference these specific configuration settings created by OaaS:

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

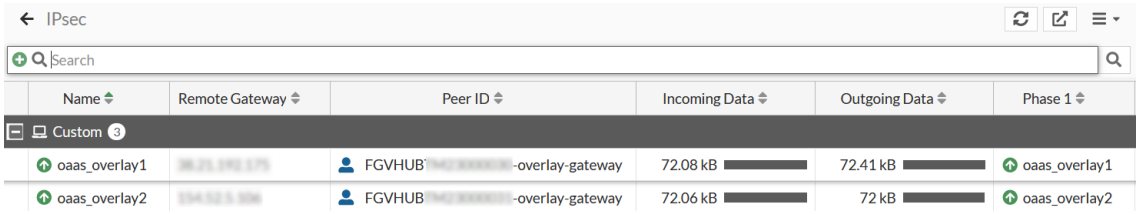
However, to ensure proper operation of OaaS with regards to topology changes and updates, ensure that you do not reference any other OaaS configuration settings in firewall policies and other configuration settings that you have added after installing settings orchestrated from OaaS.

Verifying IPsec VPN tunnels on a spoke

To verify IPsec VPN tunnels on a spoke:

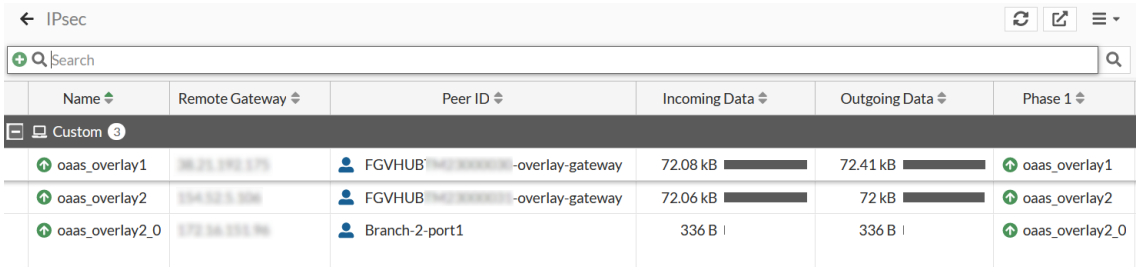
1. Go to *Dashboard* > *Network* and click the *IPsec* widget to expand it.
2. Verify the IPsec tunnels that go back to the hub.

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



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

   For example, *oaas_overlay2_0* is identified as the spoke's tunnel that was created for Datacenter to Branch-2 traffic.



Verifying BGP routing on a spoke

To verify BGP routing on a spoke:

1. In the CLI, check the BGP peering status:

```
# get router info bgp summary

VRF 0 BGP router identifier 10.200.0.50, local AS number 65001
BGP table version is 9
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      60      58        8    0    0 00:12:05        3
10.200.0.3  4      65001      60      57        8    0    0 00:12:05        3

Total number of neighbors 2
```

2. Check the BGP advertised routes:

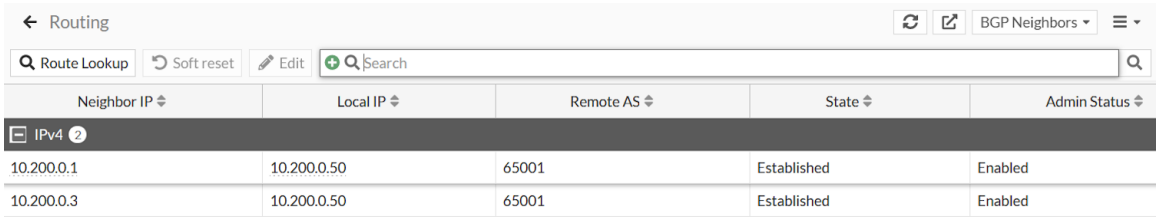
```
# get router info bgp neighbors 10.200.0.1 advertised-routes
VRF 0 BGP table version is 9, local router ID is 10.200.0.50
```

```
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
*>i10.1.100.0/24    10.200.0.50                       100  32768        0 I <-/->

Total number of prefixes 1
```

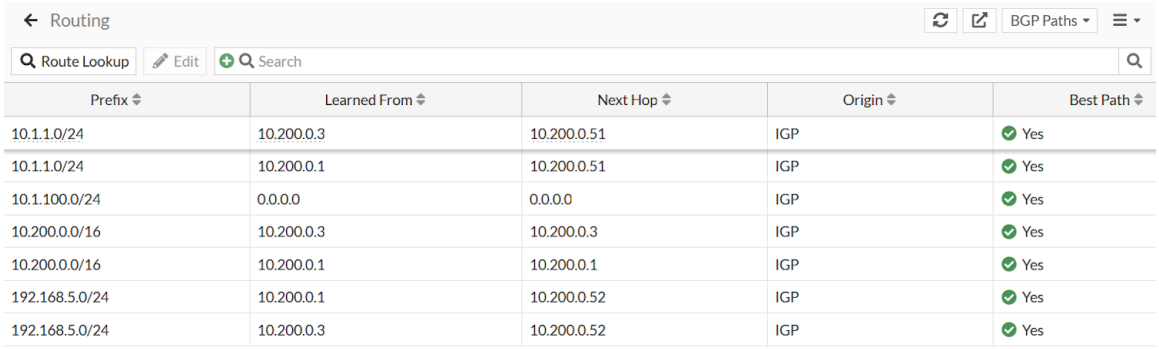
3. Check the BGP learned routes:

```
# get router info bgp neighbors 10.200.0.1 received-routes
VRF 0 BGP table version is 9, local router ID is 10.200.0.50
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      10.200.0.51                       100      0        0 I <-/->
*>i10.200.0.0/16    10.200.0.1                        100      0        0 I <-/->
*>i192.168.5.0      10.200.0.52                       100      0        0 I <-/->

Total number of prefixes 3
```

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



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

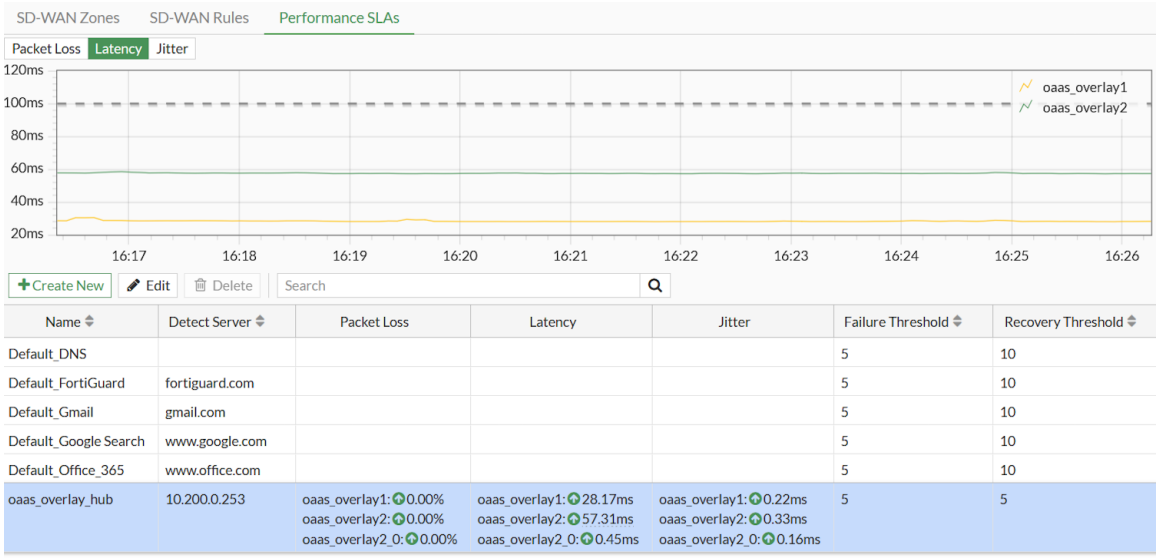


Verifying the performance SLAs on a spoke

To verify the performance SLAs on a spoke:

1. 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_overlay2_0*.



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_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: 28.17ms oaas_overlay2: 57.31ms oaas_overlay2_0: 0.45ms	oaas_overlay1: 0.22ms oaas_overlay2: 0.33ms oaas_overlay2_0: 0.16ms	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`:

```
# 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.

Verifying spoke-to-spoke ADVPN communication

To verify spoke-to-spoke ADVPN communication:

1. From Datacenter LAN IP address (10.1.100.1), ping the LAN IP address behind Branch-2 (192.168.5.4):

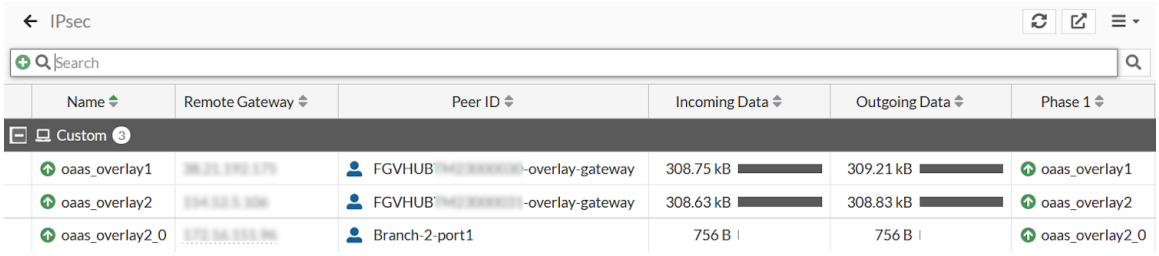
```
# execute ping-options source 10.1.100.1
# execute ping 192.168.5.4
PING 192.168.5.4 (192.168.5.4): 56 data bytes
64 bytes from 192.168.5.4: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.5.4: icmp_seq=1 ttl=255 time=0.7 ms
```

```
64 bytes from 192.168.5.4: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 192.168.5.4: icmp_seq=3 ttl=255 time=0.3 ms
64 bytes from 192.168.5.4: icmp_seq=4 ttl=255 time=0.2 ms

--- 192.168.5.4 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.7 ms
```

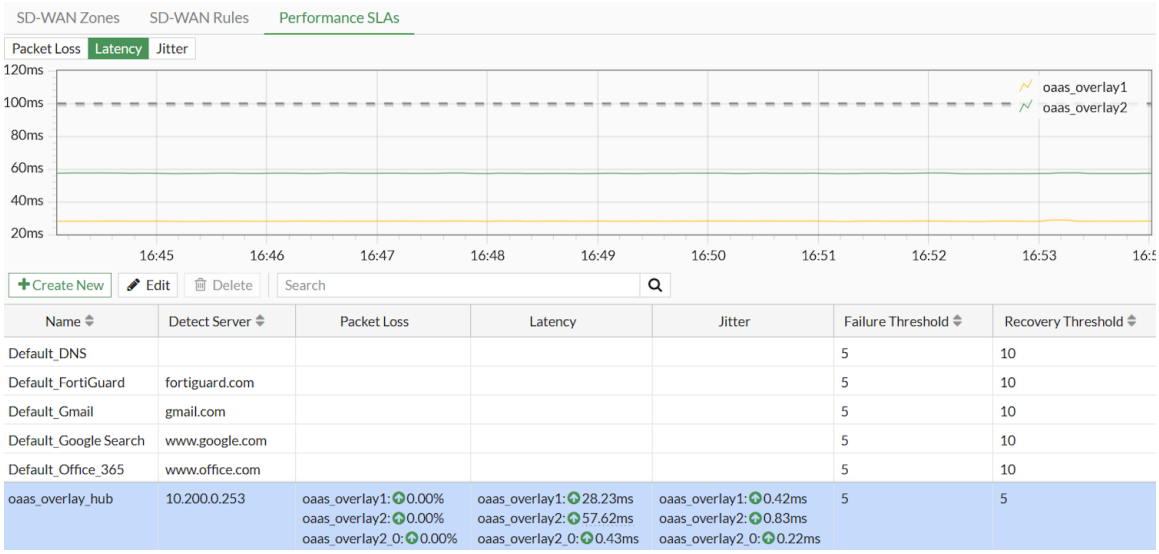
2. Verify the IPsec tunnel summary:
   a. In the CLI, enter the following:

```
# get vpn ipsec tunnel summary
'oaas_overlay2_0' 172.16.151.96:0  selectors(total,up): 2/2  rx(pkt,err): 9/0  tx
(pkt,err): 9/3
'oaas_overlay1' 38.21.192.175:4500  selectors(total,up): 1/1  rx(pkt,err): 5445/0  tx
(pkt,err): 5454/12
'oaas_overlay2' 154.52.5.106:4500  selectors(total,up): 1/1  rx(pkt,err): 5442/0  tx
(pkt,err): 5449/12
oaas_overlay2_0 is identified as the spoke's tunnel that was created for Datacenter
to Branch-2 traffic.
```

   b. In the GUI, go to *Dashboard* > *Network* and click the *IPsec* widget to expand it.



3. Go to *Network* > *SD-WAN* and select the *Performance SLAs* tab to verify that the performance SLA was updated.



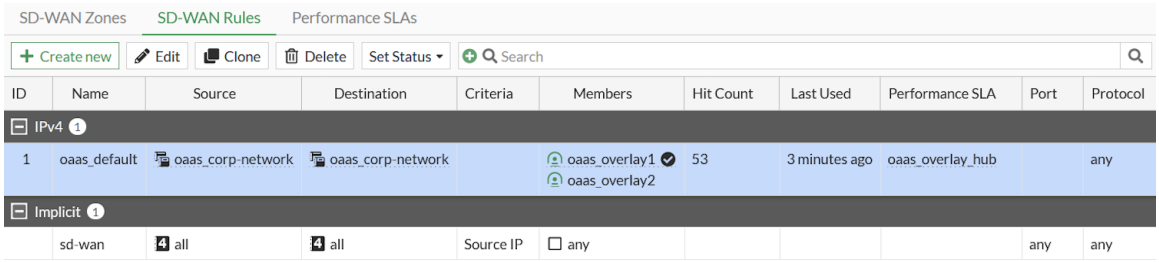
The first performance SLA, *oaas_overlay_hub*, that corresponds to the spoke-to-hub VPN tunnel is shown as up.

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. Go to *Network* > *SD-WAN*.
2. Select the *SD-WAN Rules* tab.
3. View the SD-WAN rule created by OaaS called *oaas_default* corresponding to the performance SLA *oaas_overlay_hub*.



If you need to create other SD-WAN rules, the new rules should be configured and placed below the *oaas_default* rule.

(Optional) Deleting OCVPN configuration

After installing configuration settings orchestrated from OaaS and verifying connectivity between sites, you can consider deleting the configuration settings orchestrated from OaaS.

On the FortiGate, use the CLI command `show | grep OCVPN -f` to find all instances of OCVPN-related configuration settings. The below settings were found using this exact command:

- BGP neighbor range table
- BGP neighbor group table
- Router Policy
- IPsec Phase 2 and Phase 1
- PKI user group and PKI users
- Address groups and address objects

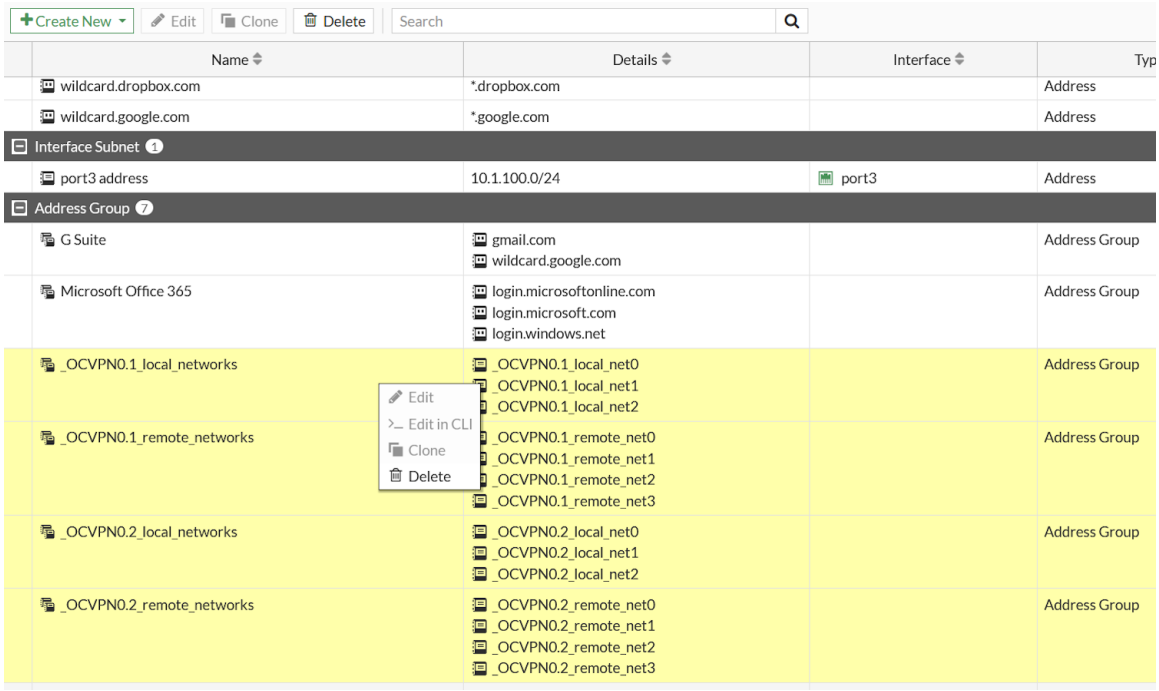
Repeat the above CLI commands to delete each address group and address object with the comment “Generated by OCVPN Cloud Service.”

Alternatively, it is more convenient to use the FortiGate GUI. On the *Policy & Objects* > *Addresses* page, use CTRL + left click to select multiple address groups and address objects and delete them at once.

To delete multiple address groups in the GUI:

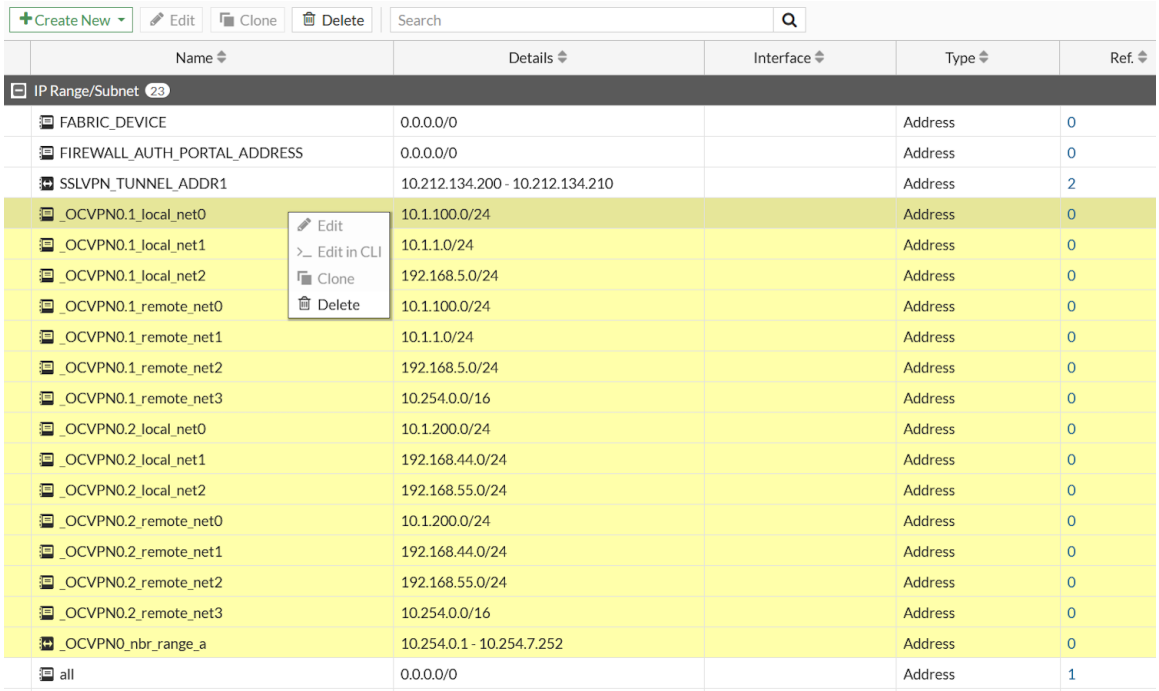
1. Select multiple addresses using CTRL + left click.
2. Right-click on the selection and select *Delete*.

3. Click *OK* to confirm.



To delete multiple address objects in the GUI:

1. Select multiple objects using CTRL + left click.
2. Right-click on the selection and select *Delete*.
3. Click *OK* to confirm.



Appendix A: FortiGate configuration settings installed by OaaS

This appendix primarily serves as a reference for administrators migrating from OCVPN and OaaS who are troubleshooting why their OaaS configuration is not installing as expected on their FortiGate devices deployed in OaaS.

Also, this appendix provides details for expert administrators interested in the actual FortiGate configuration settings installed by OaaS.

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

The OaaS configures SD-WAN rules on each of the spokes and therefore provides a complete SD-WAN deployment.

OCVPN uses BGP per overlay for its routing design whereas OaaS uses BGP on loopback. For the differences between these routing designs, see Routing design methods.

The following is sample configuration from the Datacenter site used in this deployment example. The configuration of other sites should be similar except for various device-specific settings with differing IP addresses and serial numbers.

```
config system sdwan
    set status enable
end
config system sdwan
    config health-check
        edit "Default_DNS"
        next
    end
end
config system sdwan
    config health-check
        edit "Default_Office_365"
        next
    end
end
```

```
config system sdwan
    config health-check
        edit "Default_Gmail"
        next
    end
end
config system sdwan
    config health-check
        edit "Default_Google Search"
        next
    end
end
config system sdwan
    config health-check
        edit "Default_FortiGuard"
        next
    end
end
config system settings
    set location-id 10.200.0.49
end
config system interface
    edit "oaas_bgp_lo"
        set vdom "root"
        set ip 10.200.0.49 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
config system interface
    edit "oaas_bgp_lo"
        config ipv6
        end
    next
end
config system zone
    edit "oaas_lan_zone"
        set interface "port3"
    next
end
config vpn ipsec phase1-interface
    edit "oaas_overlay1"
        set interface "port1"
        set ike-version 2
        set keylife 2800
        set peertype any
        set net-device enable
        set exchange-ip-addr4 10.200.0.49
        set proposal aes256-sha256
        set add-route disable
        set localid "Datacenter-port1"
        set dpd on-idle
        set idle-timeout enable
        set auto-discovery-receiver enable
        set dev-id-notification enable
        set dev-id "<FortiGate serial number>"
```

```
        set remote-gw OaaS-Datacenter-1-IP
        set psksecret <Pre-shared key>
        unset dpd-retryinterval
        set dpd-retryinterval 5
    next
end
config vpn ipsec phase1-interface
    edit "oaas_overlay2"
        set interface "port1"
        set ike-version 2
        set keylife 2800
        set peertype any
        set net-device enable
        set exchange-ip-addr4 10.200.0.49
        set proposal aes256-sha256
        set add-route disable
        set localid "Datacenter-port1"
        set dpd on-idle
        set idle-timeout enable
        set auto-discovery-receiver enable
        set dev-id-notification enable
        set dev-id "<FortiGate serial number>"
        set remote-gw OaaS-Datacenter-2-IP
        set psksecret <Pre-shared key>
        unset dpd-retryinterval
        set dpd-retryinterval 5
    next
end
config vpn ipsec phase2-interface
    edit "oaas_overlay1"
        set phase1name "oaas_overlay1"
        set proposal aes256-sha256
        set keepalive enable
        set keylifeseconds 3600
    next
end
config vpn ipsec phase2-interface
    edit "oaas_overlay2"
        set phase1name "oaas_overlay2"
        set proposal aes256-sha256
        set keepalive enable
        set keylifeseconds 3600
    next
end
config router route-map
    edit "oaas_tag-<Primary OaaS Hub Serial Number>"
    next
end
config router route-map
    edit "oaas_tag-<Primary OaaS Hub Serial Number>"
        config rule
            edit 1
                unset match-metric
                unset match-tag
                unset match-vrf
                unset set-ip-nexthop
```

```
                unset set-ip-prefsrc
                unset set-vpnv4-nexthop
                unset set-ip6-nexthop
                unset set-ip6-nexthop-local
                unset set-local-preference
                unset set-metric
                unset set-originator-id
                set set-tag <Unique Tag ID>
                unset set-weight
                set set-flags 8
                unset set-route-tag
                unset set-priority
            next
        end
    next
end
config router route-map
    edit "oaas_tag-<Secondary OaaS Hub Serial Number>"
    next
end
config router route-map
    edit "oaas_tag-<Secondary OaaS Hub Serial Number>"
        config rule
            edit 1
                unset match-metric
                unset match-tag
                unset match-vrf
                unset set-ip-nexthop
                unset set-ip-prefsrc
                unset set-vpnv4-nexthop
                unset set-ip6-nexthop
                unset set-ip6-nexthop-local
                unset set-local-preference
                unset set-metric
                unset set-originator-id
                set set-tag <Unique Tag ID>
                unset set-weight
                set set-flags 8
                unset set-route-tag
                unset set-priority
            next
        end
    next
end
config router bgp
    set router-id 10.200.0.49
end
config router bgp
    config neighbor
        edit "10.200.0.1"
            set advertisement-interval 1
            set soft-reconfiguration enable
            set interface "oaas_bgp_lo"
            unset remote-as
            set remote-as 65001
            set route-map-in "oaas_tag-<Primary OaaS Hub Serial Number>"
```

```
            set connect-timer 1
            set update-source "oaas_bgp_lo"
        next
    end
end
config router bgp
    config neighbor
        edit "10.200.0.3"
            set advertisement-interval 1
            set soft-reconfiguration enable
            set interface "oaas_bgp_lo"
            unset remote-as
            set remote-as 65001
            set route-map-in "oaas_tag-<Secondary OaaS Hub Serial Number>"
            set connect-timer 1
            set update-source "oaas_bgp_lo"
        next
    end
end
config router bgp
    config network
        edit 1
            set prefix 10.1.100.0 255.255.255.0
        next
    end
end
config firewall address
    edit "oaas_port3"
        set subnet 10.1.100.0 255.255.255.0
    next
end
config firewall address
    edit "oaas_resv-subnet"
        set subnet 10.200.0.0 255.255.0.0
    next
end
config firewall address
    edit "oaas_bgp_lo_addr"
        set subnet 10.200.0.49 255.255.255.255
    next
end
config firewall addrgrp
    edit "oaas_corp-network"
        set member "oaas_port3" "all"
    next
end
config system sdwan
end
config system sdwan
    config health-check
        edit "Default_DNS"
        next
    end
end
config system sdwan
    config health-check
```

```
        edit "Default_Office_365"
        next
    end
end
config system sdwan
    config health-check
        edit "Default_Gmail"
        next
    end
end
config system sdwan
    config health-check
        edit "Default_Google Search"
        next
    end
end
config system sdwan
    config health-check
        edit "Default_FortiGuard"
        next
    end
end
config system sdwan
    config members
        edit 1
            set interface "oaas_overlay1"
            set zone "oaas_overlay"
            set source 10.200.0.49
            set priority 10
        next
    end
end
config system sdwan
    config members
        edit 2
            set interface "oaas_overlay2"
            set zone "oaas_overlay"
            set source 10.200.0.49
            set priority 10
        next
    end
end
config system sdwan
    config health-check
        edit "oaas_overlay_hub"
            set server "10.200.0.253"
            set embed-measured-health enable
            set sla-fail-log-period 10
            set sla-pass-log-period 10
            set members "1" "2"
        next
    end
end
config system sdwan
    config health-check
        edit "oaas_overlay_hub"
```

```
            config sla
                edit 1
                    set link-cost-factor latency
                    set latency-threshold 100
                next
            end
        next
    end
end
config system sdwan
    config neighbor
        edit "10.200.0.1"
            set member "1"
            set health-check "oaas_overlay_hub"
            set sla-id 1
        next
    end
end
config system sdwan
    config neighbor
        edit "10.200.0.3"
            set member "2"
            set health-check "oaas_overlay_hub"
            set sla-id 1
        next
    end
end
config system sdwan
    config service
        edit 1
            set name "oaas_default"
            set mode sla
            set dst "oaas_corp-network"
            set src "oaas_corp-network"
            set hold-down-time 20
            set priority-members "1" "2"
            set tie-break fib-best-match
        next
    end
end
config system sdwan
    config service
        edit 1
            config sla
                edit "oaas_overlay_hub"
                    set id 1
                next
            end
        next
    end
end
config firewall policy
    edit 1
        set name "oaas_default"
        set srcintf "oaas_lan_zone" "oaas_overlay"
        set dstintf "oaas_lan_zone" "oaas_overlay"
```

```
        set action accept
        set srcaddr "oaas_corp-network"
        set dstaddr "oaas_corp-network"
        set schedule "always"
        set service "ALL"
    next
end
config firewall policy
    edit 2
        set name "oaas_bgp"
        set srcintf "oaas_overlay"
        set dstintf "oaas_bgp_lo"
        set action accept
        set srcaddr "oaas_resv-subnet"
        set dstaddr "oaas_bgp_lo_addr"
        set schedule "always"
        set service "ALL"
    next
end
```

www.fortinet.com