

# SD-Branch Deployment Guide

FortiOS 7.0



**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>

**NSE 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](mailto:techdoc@fortinet.com)



September 19, 2022

FortiOS 7.0 SD-Branch Deployment Guide

01-704-761366-20220919

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Executive summary	5
Audience	6
About this guide	6
<b>Solution overview</b>	<b>8</b>
<b>Design overview</b>	<b>9</b>
Use cases and topologies	9
Design concept and considerations	9
WAN edge	10
LAN edge	12
<b>Deployment procedures</b>	<b>14</b>
WAN edge	14
Underlay	15
Overlay	17
Routing	20
WAN edge intelligence	25
LAN edge	37
FortiSwitch	38
FortiAP	44
Security	46
<b>Appendix A - Products used</b>	<b>52</b>
<b>Appendix B - Documentation references</b>	<b>53</b>

# Change Log

Date	Change Description
2022-06-17	Initial release.
2022-07-14	Updated some images.
2022-08-02	Updated <a href="#">FortiAP on page 44</a> and <a href="#">Creating AP profiles on page 46</a> .
2022-08-18	Updated <a href="#">Security on page 46</a> .
2022-09-19	Updated <a href="#">Defining performance SLA on page 25</a> .

# Introduction

This guide describes how to deploy Secure SD-Branch. It begins with an executive summary followed by a description of the target audience and how this guide fits into the 4D documentation series for SD-WAN technology.

## Executive summary

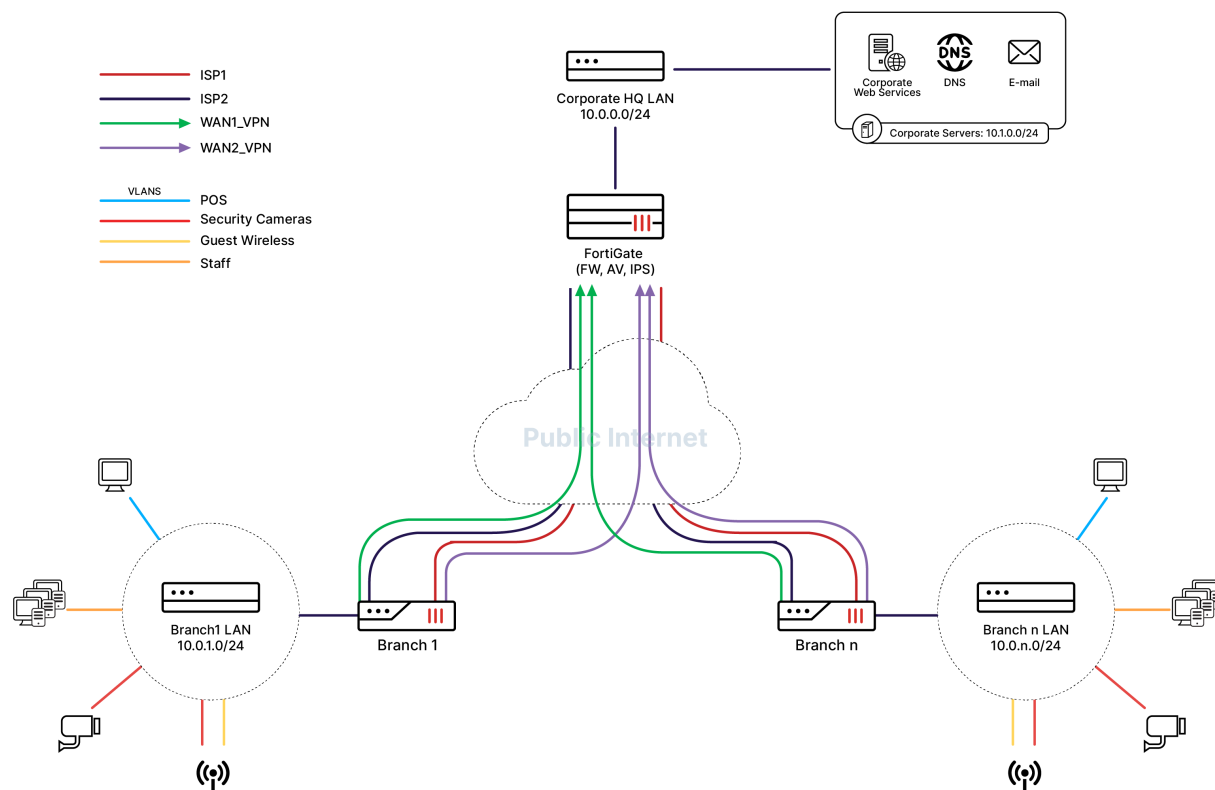
Secure SD-Branch is an extension of SD-WAN to secure the LAN edge in addition to the WAN edge by extending the Next Generation firewall security through the access layer. This convergence of LAN, SD-WAN, and routing into a unified platform with single pane of glass management uses software to simplify the management of the branch. SD-Branch takes the benefits of SD-WAN's ease-of-use and automation and applies them to the LAN.

One paradigm suggests that complexity follows security increases, and attempts to reduce complexity often result in compromised functionality and/or performance. SD-Branch addresses these problems by extending the proven WAN security of the FortiGate to the LAN, then applies dynamic rules to the unified WAN and LAN in a human-friendly format, resulting in an easy to understand and manage, highly secure branch network that enhances user experience by increasing application performance and connectivity.

In a standard SD-Branch setup, FortiGate contains all the intelligence of SD-WAN that will apply to the WAN Edge. It also extends its security to the access layer through the FortiSwitch and FortiAP, which form the LAN edge.

Furthermore, in larger deployments SD-Branch can be scaled out to many branches, and each branch connects back to the headquarter (HQ) hub device for centralized management, logging, and monitoring. While this guide does not cover the central management aspects of SD-Branch, we will demonstrate a topology with scalability in mind.

Example hub and spoke SD-Branch setup:



## Audience

This guide is intended for network and security engineers, who want hands-on experience configuring SD-WAN. The guide will help you develop the steps necessary to implement the final SD-Branch solution specific to your business. The contained configurations are examples for retail and office branches, and should be used as a reference when the topology and use case match your needs, and revised where necessary. For scalable deployment, FortiManager offers a systematic approach to deployment and continued management of many branch sites. See the [SD-WAN 6.4 Deployment for MSSPs](#).

It is beneficial to have read the associated design guide for a deeper understanding of the contained configuration, and to be familiar with the devices covered in this guide, such as FortiGate, FortiSwitch, and FortiAP.

## About this guide

This guide is the third step in the four-step process of Define, Design, Deploy, and Demo:

1. The define step describes the business need of extending WAN intelligence, security, and scalable management has been defined.
2. The design step describes a design that meets these needs by integrating multiple solutions into one unified

platform.

**3.** The deploy step provides a step by step guide of the configurations necessary to implement the complete solution.

This guide is intended to introduce SD-WAN configuration. The guide provides steps to implement the framework of SD-WAN directly on a FortiGate, but may omit specific steps where readers must make design decisions to further configure their devices. This guide does not detail all of the available features that SD-WAN may provide once implemented, nor does it provide instructions on scaling the deployment to many sites and managing the configuration accordingly. It is beneficial to read the associated design guide for a deeper understanding of the contained configuration. Please refer to the following supporting documentation for further details:

- [FortiOS 7.2 Administration Guide > SD-WAN chapter](#)
- [SD-WAN / SD-Branch 6.4 Architecture for MSSPs](#)
- [SD-WAN 6.4 Deployment for MSSPs](#)

# Solution overview

Maintaining a site's digital security and performance is an involved task that can be complex and time consuming. When applying SD-WAN at a branch location, you can expect a reduction in complexity and overhead while enhancing performance through the use of:

- Enhanced link health monitoring and self-healing
  - By evaluating meaningful connectivity from each WAN connection, individual application connectivity failure can be detected when the link looks otherwise healthy
  - Intelligent failover and steering resolves issues without any need for administrative intervention
- Segmentation
  - Built-in principle of least privilege and network or resource isolation ensures important data is only available as necessary
- Wireless and switch integration
  - Extending the single pane of glass management not only to include each site, but the access layer within that site as well
  - Complexity reduction with seamless extension of Fortinet WAN security to the LAN
- Analytical data for each site
  - Meaningful representation of important statistics to drive business decisions and evaluate branch performance

In this solution, we'll look closely at a single branch location and explore how to implement SD-WAN with a few of the possible SD-WAN capabilities with regards to two common branch types: retail and office. This guide focuses on the branch configuration.

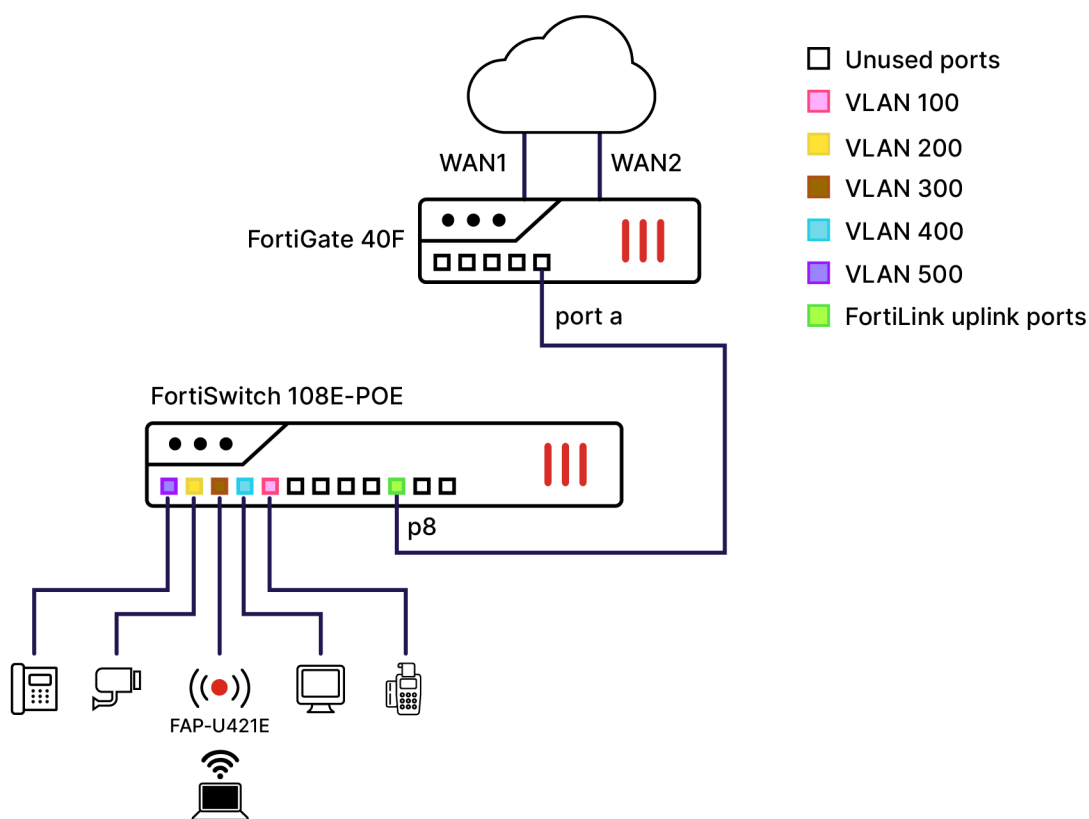


# Design overview

This section includes the following topics:

- [Use cases and topologies on page 9](#)
- [Design concept and considerations on page 9](#)

## Use cases and topologies



You can replace one of the WAN links from FortiGate to the internet with an LTE connection and use it for failover, if an outage occurs on the primary link. See [FortiExtender](#) documentation for further information.

## Design concept and considerations

Each SD-Branch design includes the following major sections:

- [WAN edge on page 10](#)
- [LAN edge on page 12](#)

## WAN edge

SD-WAN utilizes five (5) design principles:

- [Underlay on page 10](#)
- [Overlay on page 10](#)
- [Routing on page 11](#)
- [WAN edge intelligence on page 11](#)
- Security

This section describes all principles, except security, which is covered in the LAN section. See [Security on page 13](#).



At least two WAN connections are required to implement SD-WAN.

---

## Underlay

An underlay network describes the physical connections, such as ISP circuit, MPLS private line or cellular data. For SD-WAN, the underlay type does not matter. Following are examples of different connection options and justification for the selection.

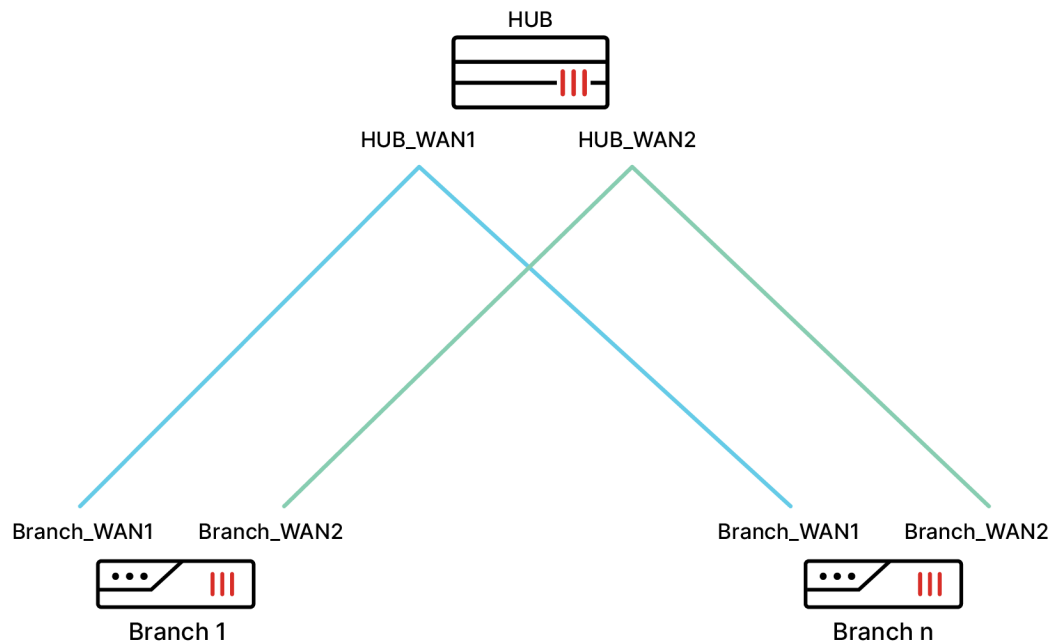
- Retail branch  
As retail companies often have a large number of branch locations with small data throughput to cloud services (for example, payment) and headquarters (for example, inventory management, sales statistics), it is cost effective to use a single WAN connection and have a backup link in place for use only as necessary. FortiExtender is ideal to establish a backup link through 3G/4G/5G wireless connection, ensuring business continuity through health monitoring and self-healing where failover only occurs in the event of a WAN outage.
- Office branch  
Conversely a company with branch offices has comparatively fewer locations, larger application traffic throughput, and sensitive application traffic, such as VoIP.  
Since these branch offices utilize their internet connection significantly more, it makes sense to have multiple dedicated lines to leverage the same resiliency of WAN redundancy described earlier and to enable further SD-WAN features, such as application steering for sensitive traffic, traffic load-balancing, and bandwidth optimization.

## Overlay

An overlay network is the virtual network, such as an IPsec connection, that rides on top of the underlay.

In the following example, IPsec VPN connects each underlay interface to the hub:

- Branch\_WAN1 connects to HUB\_WAN1
- Branch\_WAN2 connects to HUB\_WAN2



These will be referred to as WAN1\_VPN and WAN2\_VPN respectively.

## Routing

Setup of appropriate routing relationships and policies is key to ensuring that a secure SD-WAN solution scales without increasing complexity.

- **Retail branch**  
Static routes can be leveraged for routing across the overlay network to simplify configuration. Static routes are possible because connecting a retail branch back to the hub is not complex and rarely changes.
- **Office branch**  
Branch offices can also use static routes; however, branch offices may need to communicate with each other, which requires significantly more initial configuration and continued configuration as branch offices are added. Therefore it is recommended to use a dynamic routing protocol, such as BGP.  
BGP also has the added benefit of enabling ADVPN to allow branch offices to build on-demand overlay tunnels to other branch offices for direct communication, improving performance and reducing overhead on the hub.

## WAN edge intelligence

WAN edge intelligence is responsible for controlling the flow of traffic using rules, logic, and real-time metrics of important resources.

**Health-check servers**, as defined by an IP address or FQDN, are important business resources, such as a server in headquarters or cloud applications.

**Performance metrics** are defined for the health-check servers, such as specifying that latency thresholds must be under 200ms and packet loss less than 2%.

Define an **SD-WAN service rule** to ensure that all traffic should use WAN1\_VPN, unless the metrics are not met, then fail over to the next most viable tunnel.

## LAN edge

FortiSwitch and FortiAP consolidate branch services through the convergence of security and network access with FortiLink. FortiSwitch and FortiAP integrate with FortiGate to extend SD-WAN benefits into the network access layer. This enables network and security administrators to create and enforce the same network security policies across the enterprise, including out to the network branch.

This section contains the following topics:

- [FortiSwitch on page 12](#)
- [FortiAP on page 12](#)
- [Security on page 13](#)

## FortiSwitch

While many users will connect to your network over WiFi, some devices still require wired connections, such as VoIP phones, POS terminals, security cameras, printers, TVs, and desktops. With the variety of devices and security needs, it is necessary to segment these devices in different subnets and VLANs. The built-in NAC features on the FortiGate switch controller enable you to segment the devices and define rules for segmenting your devices at a very granular level.

- Retail branch
  - PoE for FortiAP, security cameras, and possibly wired phones
  - Integrated segmentation for transactions (for example, for PCIDSS compliance), guest traffic (for example, public WiFi), operations (for example, manager PC, security cameras, phone)
- Office branch
  - Wired connections for desktop endpoints
  - PoE for security cameras, phones, FortiAP
  - Integrated segmentation for transactions (for example, for PCIDSS compliance), guest traffic (for example, public WiFi), operations (for example, manager PC, security cameras, phone)
  - Network Access Control for BYoD and IoT devices that leverage device detection

## FortiAP

On the SD-Branch, the FortiGate acts as the wireless controller to manage the FortiAP(s) on that site. Depending on the size of the store, two or more FortiAP can be deployed.

- Retail branch
  - Guest network for customers
  - Private network for employees
- Office branch
  - Guest network for office guests
  - Private network for employees
  - Rogue AP detection

## Security

Security policies constitute an essential part of the SD-WAN configuration, ensuring that all outgoing and incoming traffic is adequately inspected at Layer 7 of the OSI model and compliant with corporate security policy prior to egress of the branch edge.

Permit only specific traffic across SD-WAN. Non-corporate destined traffic leverages Direct Internet Access (DIA).

Isolate business traffic from any guest wireless.

Apply next generation threat detection and prevention to inbound and outbound traffic, regardless of which SD-WAN interface is selected.

# Deployment procedures

This section describes how to configure the following elements of the branch location:

- [WAN edge on page 14](#)
- [LAN edge on page 37](#)

Additional configuration, such as security policies, is not provided.

## WAN edge

The WAN chapter explains how to create and use the following key components:



For the underlay interfaces, this document uses port1 and port2 in the examples, but you can use any port you wish.

Underlay	Interfaces:	Use:
	• port1	• ISP1 connectivity
	• port2	• ISP2 connectivity
	Zones:	Use:
	• WAN1 (port1)	• SD-WAN rules and firewall policies
Overlay	• WAN2 (port2)	• SD-WAN rules and firewall policies
	Interfaces:	Use:
	• WAN1-VPN	• Establishing hub device connectivity
	• WAN2-VPN	• Establishing hub device connectivity
	Zones:	Use:
	• WAN1_VPN (WAN1-VPN)	• SD-WAN rules and firewall policies
	• WAN2_VPN (WAN2-VPN)	• SD-WAN rules and firewall policies

Routing	BGP neighbors	Use:
	<ul style="list-style-type: none"> <li>• WAN1_VPN to and from HUB_VPN1</li> </ul>	<ul style="list-style-type: none"> <li>• Routing information</li> </ul>
	<ul style="list-style-type: none"> <li>• WAN2_VPN to and from HUB_VPN2</li> </ul>	<ul style="list-style-type: none"> <li>• Routing information</li> </ul>
	Static Routes:	Use:
	<ul style="list-style-type: none"> <li>• ISP1 gateway</li> </ul>	<ul style="list-style-type: none"> <li>• DHCP assumed</li> </ul>
	<ul style="list-style-type: none"> <li>• ISP2 gateway</li> <li>• Blackhole for LAN supernet</li> </ul>	<ul style="list-style-type: none"> <li>• DHCP assumed</li> <li>• Will be selected for corporate traffic in the event VPNs are down</li> </ul>
WAN edge intelligence	Performance SLAs:	Use:
	<ul style="list-style-type: none"> <li>• Headquarters (HQ)</li> </ul>	<ul style="list-style-type: none"> <li>• Checks the quality of both VPN links to a resource behind the hub device</li> </ul>
	<ul style="list-style-type: none"> <li>• Internet</li> </ul>	<ul style="list-style-type: none"> <li>• Checks the quality of both ISP links to an internet resource</li> </ul>
	SD-WAN rules:	Use:
	<ul style="list-style-type: none"> <li>• HQ</li> </ul>	<ul style="list-style-type: none"> <li>• Uses HQ SLA to ensure traffic to HQ only uses healthy VPN links</li> </ul>
	<ul style="list-style-type: none"> <li>• Business_Internet</li> <li>• Non_Business_Internet</li> </ul>	<ul style="list-style-type: none"> <li>• Uses Internet SLA to measure WAN link quality and routes specific application traffic over the best link</li> <li>• Route non-business traffic out of the lowest cost WAN link</li> </ul>

Following is an overview of how to configure the WAN edge:

1. Configure the underlay. See [Underlay on page 15](#).
2. Configure the overlay. See [Overlay on page 17](#).
3. Configure routing. See [Routing on page 20](#).
4. Configure WAN edge intelligence. See [WAN edge intelligence on page 25](#).

## Underlay

The branch underlay uses two (2) WAN connections with different Internet Service Providers (ISPs). Create two SD-WAN zones named *WAN1* and *WAN2* respectively, and then add a WAN connection to each zone. By using two SD-WAN zones, you can create granular policies for SD-WAN zone, and use different policies for the other SD-WAN zone.

Following is an overview of the procedure:

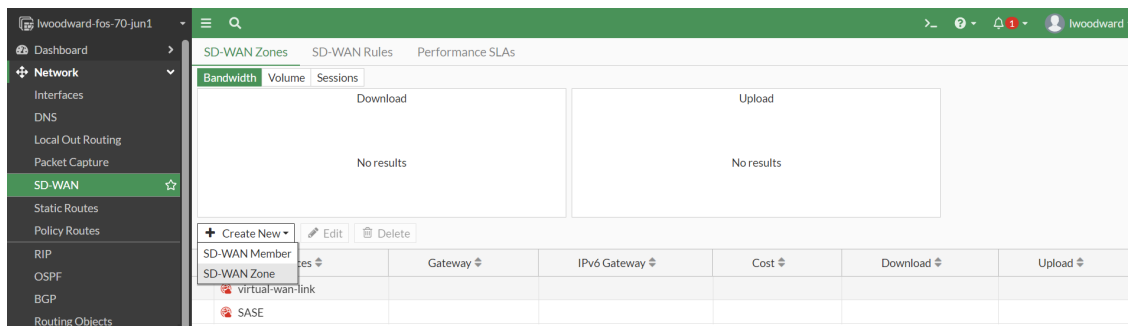
1. Create two SD-WAN zones for the underlay. See [Creating SD-WAN zones for the underlay on page 16](#).
2. Add SD-WAN members to each zone. See [Adding SD-WAN members to underlay zones on page 16](#).

## Creating SD-WAN zones for the underlay

Create two SD-WAN zones named *WAN1* and *WAN2* respectively for the underlay.

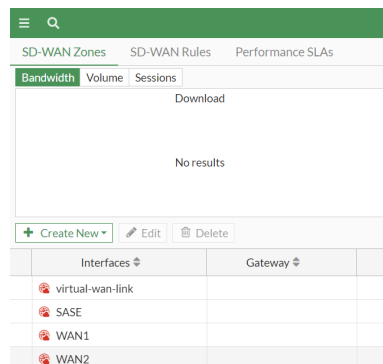
**To create SD-WAN zones:**

1. Go to *Network > SD-WAN > SD-WAN Zones*.
2. Create an SD-WAN zone named *WAN1*:
  - a. Click *Create New > SD-WAN Zone*.



- b. Set *Name* to *WAN1*, and click *OK*.
3. Create an SD-WAN zone named *WAN2*:
  - a. Click *Create New > SD-WAN Zone*.
  - b. Set *Name* to *WAN2*, and click *OK*.

The *WAN1* and *WAN2* zones are created.



## Adding SD-WAN members to underlay zones

After creating the SD-WAN zones for the underlay, create an SD-WAN member to add one WAN interface to one zone, and then repeat the procedure to add the second WAN interface to the second zone.

**To add SD-WAN members to underlay zones:**

1. On the *Network > SD-WAN > SD-WAN Zones* page, click *Create New > SD-WAN Member*. The *New SD-WAN Member* page is displayed.
2. Set the following options, and click *OK*:
  - a. Set *Interface* to your WAN interface.
  - b. Set *SD-WAN Zone* to one of the zones you created.

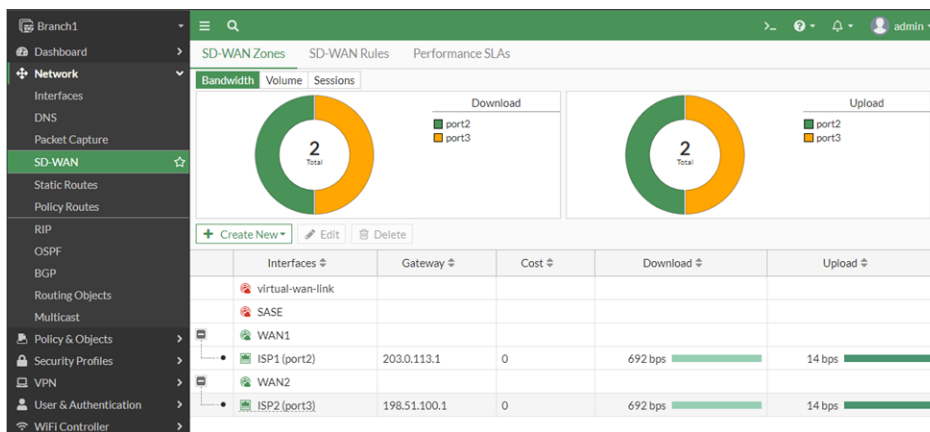


- c. Set *Gateway* to the IP address provided by the ISP.  
If your WAN interface uses DHCP to receive an IP address, leave the *Gateway* set to *0.0.0.0*.

**New SD-WAN Member**

Interface	ISP1 (port2)
SD-WAN Zone	WAN1
Gateway	0.0.0.0
Cost	0
Priority	0
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled

3. Repeat this procedure for the second WAN interface.  
The WAN interfaces are added to the SD-WAN zones.



## Overlay

The underlay for both retail and office branch locations rely on each WAN interface establishing a VPN tunnel to a hub interface. VPN tunnels are put into zones for reference in policies.

Following is an overview of the procedure:

1. Create two (2) IPsec tunnels for the overlay. See [Creating IPsec tunnels for the overlay on page 17](#).
2. Create SD-WAN zones for the IPsec tunnels. See [Defining SD-WAN zones for the overlay on page 19](#).
3. Create SD-WAN members for the zones. See [Defining SD-WAN members on page 20](#).

### Creating IPsec tunnels for the overlay

Create two IPsec tunnels named *WAN1\_VPN* and *WAN2\_VPN*.

This example describes how to create an IPsec tunnel named *WAN1\_VPN*. Use the same procedure to create a second IPsec tunnel named *WAN2\_VPN*, adjusting the IP address and interface as necessary.

Many settings can be used to configure IPsec tunnels. Adjust the tunnel settings to fit your requirements.

**To create a VPN tunnel:**

1. Go to **VPN > IPsec Tunnels**, and click **+Create New > IPsec Tunnel**. The *VPN Creation Wizard* is displayed.
2. Set the following options, and click **Next**:
  - a. Set *Name* to **WAN1-VPN**.
  - b. Set *Template* type to **Custom**.  
The *Network* options are displayed.
3. Set the *Network* options:
  - a. Set *IP Address* to the remote IP address of your hub's WAN1 interface.
  - b. Set *Interface* to the WAN1 interface.
  - c. Select **Mode Config**.
  - d. Expand **Advanced**, and set the following options:
    - Set *Add route* to **Disabled**.
    - Set *Auto discovery sender* to **Disabled**.
    - Set *Auto discovery receiver* to **Enabled**.
    - Set *Exchange interface IP* to **Disabled**.
    - Set *Device creation* to **Enabled**.

**Network** ✓ ↺

IP Version IPv4

Remote Gateway  
Static IP Address

IP Address  
203.0.113.1

Interface  
ISP1 (port2)

Local Gateway ⏻

Mode Config ✓

NAT Traversal Enable Disable Forced

Keepalive Frequency 10

Dead Peer Detection Disable On Idle On Demand

DPD retry count 3

DPD retry interval 20 s

Forward Error Correction Egress Ingress

**Advanced...**

Add route ✓ Enabled ✗ Disabled

Auto discovery sender ✓ Enabled ✗ Disabled

Auto discovery receiver ✓ Enabled ✗ Disabled

Exchange interface IP ✓ Enabled ✗ Disabled

Device creation ✓ Enabled ✗ Disabled

4. Set the *Authentication* options:
  - a. Set *Method* to **Pre-shared Key**.
  - b. Set *IKE Version* to **2**.

Authentication

Method: Pre-shared Key

Pre-shared Key: [masked]

IKE Version: 1

5. Set the *Phase 1 Proposal* options:
  - a. Remove any unneeded *Encryption* and *Authentication* combinations.
  - b. Select your desired *Diffie-Hellman Groups*, *Key Lifetime*, and enter a *Local ID*.

Phase 1 Proposal

Encryption: AES128 Authentication: SHA256

Diffie-Hellman Groups: ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☒ 14 ☒ 5 ☐ 2 ☐ 1

Key Lifetime (seconds): 86400

Local ID: Branch1

6. Click OK. The IPsec tunnel is created for WAN1.
7. Repeat this procedure for WAN2. The IPsec tunnel is created for WAN2.

Tunnel	Interface Binding	Status	Ref.
WAN1-VPN	ISP1 (port2)	Inactive	1
WAN2-VPN	ISP2 (port3)	Inactive	1

## Defining SD-WAN zones for the overlay

Create two SD-WAN zones named *WAN1\_VPN* and *WAN2\_VPN*.

### To define SD-WAN zones for the overlay:

1. Go to *Network > SD-WAN > SD-WAN Zones*.
2. Create an SD-WAN zone named *WAN1\_VPN*:
  - a. Click *Create New > SD-WAN Zone*.
  - b. Set name to *WAN1\_VPN*, and click OK.

Name: WAN1\_VPN

Interface members: +

3. Create an SD-WAN zone named *WAN2\_VPN*:
    - a. Click *Create New > SD-WAN Zone*.
    - b. Set name to *WAN2\_VPN*, and click OK.
- The *WAN1\_VPN* and *WAN2\_VPN* zones are created.

## Defining SD-WAN members

Define the SD-WAN members for each overlay VPN, and add them to their respective zone. Set the *WAN2\_VPN* member to be a cost of 10.

### To define SD-WAN members:

1. On the *Network > SD-WAN > SD-WAN Zones* page, click *Create New > SD-WAN Member*. The *New SD-WAN Member* page is displayed.
2. Set the following options, and click *OK*:
  - a. Set *Interface* to *WAN1\_VPN*.
  - b. Set *SD-WAN Zone* to *WAN1\_VPN*.
3. Repeat this procedure to create the *WAN2\_VPN* interface, and add it to the *WAN2\_VPN* zone. The overlay VPN interfaces are added to the SD-WAN zones.

Note: The VPN tunnels come up shortly after adding the VPN interfaces to their SD-WAN zones.

	Interfaces ↕	Gateway ↕	Cost ↕	Download ↕	Upload ↕
WAN1	Internet_A (port1)	10.100.67.1	0	840 bps	871 bps
WAN2	Internet_B (port2)	10.100.67.9	0	32 bps	76 bps
WAN1_VPN	WAN1_VPN	0.0.0.0	0	0 bps	0 bps
WAN2_VPN	WAN2_VPN	0.0.0.0	10	0 bps	0 bps

## Routing

Each underlay interface requires a route to reach its default gateway. You can use a static route or a dynamic routing protocol, if your Internet Service Provider (ISP) supports the protocol. For the purpose of this chapter, static route connectivity to your ISP is assumed.

Furthermore, BGP is used to propagate the headquarter LAN and server subnets to the branch devices. BGP is also used by branch devices to advertise their LAN to headquarters (HQ). In addition to the headquarter LAN being reachable through the hub interfaces, office branch devices may require inter-branch communication at times. By default, this traffic is relayed through the FortiGate at HQ; however, you may consider establishing tunnels between branch devices on demand to reduce the HQ load and even increase performance. You can accomplish this by using Auto Discovery VPN (ADVPN), which offers scalable configuration and resources. ADVPN enables the hub device to instruct branch devices how to establish direct paths to other branch devices only when needed. For more information, see [FortiOS 7.0 Administration Guide](#).

Following is an overview of the procedure:

1. Create a blackhole route. See [Creating a blackhole route on page 21](#).
2. Configure BGP. See [Configuring BGP on page 21](#).
3. View the populated FortiGate routing table. See [Viewing the FortiGate routing table on page 24](#).

## Creating a blackhole route

A static route is used to blackhole any headquarter traffic from egressing an underlay interface if both VPN tunnels are down.

Starting with the static route, create the blackhole route to prevent corporate traffic leaks.

### To create a blackhole route:

1. Go to *Network > Static routes*, and click *Create New > IPv4 Static Route*.
2. Set *Destination* to *Subnet*, and enter summary of your corporate LAN, which should include the branch LANs. The following example uses *10.0.0.0/8*.

The screenshot shows the FortiGate web interface for configuring a new static route. The left sidebar is expanded, showing the 'Network' menu with 'Static Routes' selected. The main panel is titled 'New Static Route' and has three tabs: 'Subnet', 'Named Address', and 'Internet Service'. The 'Subnet' tab is selected, and the following fields are visible:

- Destination:** Subnet (selected), 10.0.0.0/8
- Interface:** Blackhole (selected)
- Administrative Distance:** 10
- VRF ID:** 0
- Comments:** Write a comment... (0/255 characters)
- Status:** Enabled (selected), Disabled (unselected)

At the bottom right of the panel are 'OK' and 'Cancel' buttons.

3. Set *Interface* to *Blackhole*.
4. Click *OK*.

## Configuring BGP

Add two BGP neighbors: one for each VPN interface on the hub device that we want to peer with.



If you cannot view the *Network > BGP* tree menu, go to *System > Feature visibility*, and enable *Advanced Routing* in the *Core Features* column.

**To configure BGP:**

1. Go to *Network > BGP*.
2. Set the following options:
  - a. Set *Local AS* to *65001*.
  - b. Set *Router ID* to *10.0.1.1/24*, which is the first IP address of the branch LAN.
3. In the *Neighbors* section, create a new neighbor:
  - a. Click *Create New*. The *Add Neighbor* pane is displayed.
  - b. Set *IP* to *10.10.10.1*, which is the hub device's IPsec tunnel interface IP address for WAN1.
  - c. Set *Remote AS* to *65001*.
  - d. Select *Soft reconfiguration*.
  - e. Select *Capability: route refresh*.
  - f. Click *OK*. The neighbor is added.
4. In the *Neighbors* section, create another new neighbor:
  - a. Click *Create New*. The *Add Neighbor* pane is displayed.
  - b. Set *IP* to *10.10.11.1*, which is the hub device's IPsec tunnel interface IP address for WAN2.
  - c. Set *Remote AS* to *65001*.
  - d. Select *Soft reconfiguration*.
  - e. Select *Capability: route refresh*.
  - f. Click *OK*. The neighbor is added.
5. In the *Networks* section, set *IP/Netmask* to *10.0.1.0/24*.
6. Expand the *Advanced* section, and set the following options:
  - a. Set *Keepalive* to *5*.
  - b. Set *Holdtime* to *15*.
7. Expand the *Best Path Selection* section, and set the following options:
  - a. Enable *IBGP multi path*.
  - b. Enable *Additional path*.

8. Click *Apply*.

The screenshot displays the FortiOS SD-Branch configuration interface. On the left is a dark sidebar with a menu. The 'Network' section is expanded, and 'BGP' is selected and highlighted in green. The main content area on the right is titled 'Local BGP Options' and contains several sections:

- Local BGP Options:** Includes input fields for 'Local AS' (65001) and 'Router ID' (10.0.1.1).
- Neighbors:** A table with columns 'IP' and 'Remote AS'. It contains two entries: 10.10.10.1 and 10.10.11.1, both pointing to Remote AS 65001. There are '+ Create New', 'Edit', and 'Delete' buttons at the top. A count of 2 is shown at the bottom right.
- Neighbor Groups:** A table with columns 'Name' and 'Remote AS'. It is currently empty with the text 'No results'. There are '+ Create New', 'Edit', and 'Delete' buttons at the top. A count of 0 is shown at the bottom right.
- Neighbor Ranges:** A table with columns 'Prefix', 'Neighbor Group', and 'Maximum Neighbor Number'. It is currently empty with the text 'No results'. There are '+ Create New', 'Edit', and 'Delete' buttons at the top. A count of 0 is shown at the bottom right.
- Networks:** Includes an input field for 'IP/Netmask' with the value 10.0.1.0 255.255.255.0. There is a dropdown arrow and a '+' button below the input field.

The sidebar menu includes the following items: Branch1, Dashboard, Network (expanded), Interfaces, DNS, Packet Capture, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP (selected), Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System (marked with a red '1'), Security Fabric, and Log & Report.

### Advanced Options

Cluster ID	<input type="text" value="0.0.0.0"/>
Default Local Preference	<input type="text" value="100"/>
Distance external	<input type="text" value="20"/>
Distance internal	<input type="text" value="200"/>
Distance local	<input type="text" value="200"/>
Keepalive	<input type="text" value="5"/>
Holdtime	<input checked="" type="checkbox"/> <input type="text" value="15"/>
Background scan	<input checked="" type="checkbox"/> <input type="text" value="60"/>

### Best Path Selection

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

## Viewing the FortiGate routing table

After some time, routes are propagated between the branch device and the headquarter device, and then installed to the FortiGate routing table.



**To view the FortiGate routing table:**

```

get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
B      10.0.0.0/24 [200/0] via 10.10.10.1 (recursive via WAN1-VPN tunnel 203.0.113.1),
00:00:08
[200/0] via 10.10.11.1 (recursive via WAN2-VPN tunnel 198.51.100.1), 00:00:08
C      10.0.1.0/24 is directly connected, port4
B      10.1.0.0/24 [200/0] via 10.10.10.1 (recursive via WAN1-VPN tunnel 203.0.113.1),
00:00:08
[200/0] via 10.10.11.1 (recursive via WAN2-VPN tunnel 198.51.100.1), 00:00:08
C      10.10.10.0/24 is directly connected, WAN1-VPN
S      10.10.10.1/32 [15/0] via WAN1-VPN tunnel 203.0.113.1, [1/0]
C      10.10.10.2/32 is directly connected, WAN1-VPN
C      10.10.11.0/24 is directly connected, WAN2-VPN
S      10.10.11.1/32 [15/0] via WAN2-VPN tunnel 198.51.100.1, [1/0]
C      10.10.11.2/32 is directly connected, WAN2-VPN
C      198.51.100.0/24 is directly connected, port3
C      203.0.113.0/24 is directly connected, port2

```

## WAN edge intelligence

By measuring the performance of both the WAN links, as well as specific applications over the links, SD-WAN can steer traffic to ensure the best performance and quality possible. Branch locations often have dissimilar WAN links, where one is a high quality link, and the other is a less expensive, lower quality link. As such we prefer business traffic to utilize WAN1 provided that it meets pre-defined SLA targets. This applies to business traffic destined for the internet (through the underlay) as well as traffic destined for HQ using the VPN (through the overlay).

Following is an overview of the procedure:

1. Define performance SLA to measure the health of VPN tunnels and WAN links. See [Defining performance SLA on page 25](#).
2. Create SD-WAN rules for traffic. See [Creating SD-WAN rules on page 28](#).

With the completion of Underlay, Overlay, Routing, and WAN edge intelligence, the WAN half of SD-Branch configuration is finished. The next section discusses the LAN side configurations of SD-Branch. See [LAN edge on page 37](#).

## Defining performance SLA

Create performance SLA to measure the health of VPN tunnels and WAN links.

Following is an overview of the procedure:

1. Create performance SLA for VPN tunnels to monitor underlay links. See [Defining VPN performance SLA on page 26](#).
2. Create performance SLA for WAN links to monitor the overlay. See [Defining WAN performance SLA on page 27](#).

## Defining VPN performance SLA

Create performance SLA to measure the health of VPN tunnels to monitor overlay links.

### To configure VPN performance SLA:

1. Go to *Network > SD-WAN > Performance SLAs*, and click *Create New*.
2. Set the following options:
  - a. Set *Name* to *HQ\_VPN*.
  - b. Set *Server* to *10.1.0.1*.
  - c. Set *Participants* to *Specify*, and select *WAN1-VPN*, *WAN2-VPN*.
3. Enable *SLA Target*, and set the following options:
  - a. Set *Latency threshold* to *100 ms*.
  - b. Set *Jitter threshold* to *25 ms*.
  - c. Set *Packet Loss threshold* to *1 %*.
4. In the *Link Status* section, set the following options:
  - a. Set *Failures before inactive* to *3*.
  - b. Set *Restore link after* to *3*.
5. Click *OK*.

The screenshot shows the FortiOS configuration interface for a new performance SLA. The left sidebar contains a navigation menu with the following items: Branch1, Dashboard, Network (expanded), Interfaces, DNS, Packet Capture, SD-WAN (selected), Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, and Log & Report. The main content area is titled 'New Performance SLA' and contains the following configuration fields:

- Name:** HQ\_VPN
- Probe mode:** Active (selected), Passive, Prefer Passive
- Protocol:** Ping (selected), HTTP, DNS
- Server:** 10.1.0.1
- Participants:** All SD-WAN Members (selected), Specify (button). Below this, a list shows WAN1-VPN and WAN2-VPN, each with a remove button (X).
- SLA Target:** (toggle switch is on)
- Latency threshold:** 100 ms
- Jitter threshold:** 25 ms
- Packet Loss threshold:** 1 %
- Link Status:**
  - Check interval:** 500 ms
  - Failures before inactive:** 3
  - Restore link after:** 3 check(s)
- Actions when Inactive:**
  - Update static route:** (toggle switch is on)

## Defining WAN performance SLA

Create performance SLA to measure the health of WAN links to monitor underlay links.

### To configure WAN performance SLA:

1. Go to *Network > SD-WAN > Performance SLAs*, and click *Create New*.
2. Set the following options:
  - a. Set *Name* to *Internet*.
  - b. Set *Server* to *1.1.1.1*.
  - c. Set *Participants* to *Specify*, and select *ISP1*, *ISP2*.
3. Enable *SLA Target*, and set the following options:
  - a. Set *Latency threshold* to 250 ms.
  - b. Set *Jitter threshold* to 55 ms.
  - c. Set *Packet Loss threshold* to 1 %.

4. In the *Link Status* section, set the following options:
  - a. Set *Failures before inactive* to 3.
  - b. Set *Restore link after* to 3.
5. Click *OK*.

The screenshot shows the FortiOS configuration interface for a new performance SLA. The left sidebar contains a navigation menu with options like Branch1, Dashboard, Network, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, and Log & Report. The main panel is titled 'New Performance SLA' and contains the following configuration fields:

- Name:** Internet
- Probe mode:** Active (selected), Passive, Prefer Passive
- Protocol:** Ping (selected), HTTP, DNS
- Server:** 1.1.1.1
- Participants:** All SD-WAN Members (selected), Specify
- SLA Target:** (toggle off)
- Latency threshold:** 250 ms
- Jitter threshold:** 55 ms
- Packet Loss threshold:** 1 %
- Link Status:**
  - Check interval:** 500 ms
  - Failures before inactive:** 3
  - Restore link after:** 3 check(s)
- Actions when Inactive:**
  - Update static route:** (toggle on)

## Creating SD-WAN rules

We will create two rules: one for traffic destined for HQ, and one for business traffic not destined for HQ. The first rule will specify traffic destined for HQ to take a VPN through WAN1 to HUB1 or HUB2, provided the measured SLA is met. Otherwise the traffic will use either VPN through WAN2 to HUB1 or HUB2. The second rule uses application identification to ensure business related traffic prefers the highest quality link at any given time. A final catch-all rule is created for the remaining traffic.

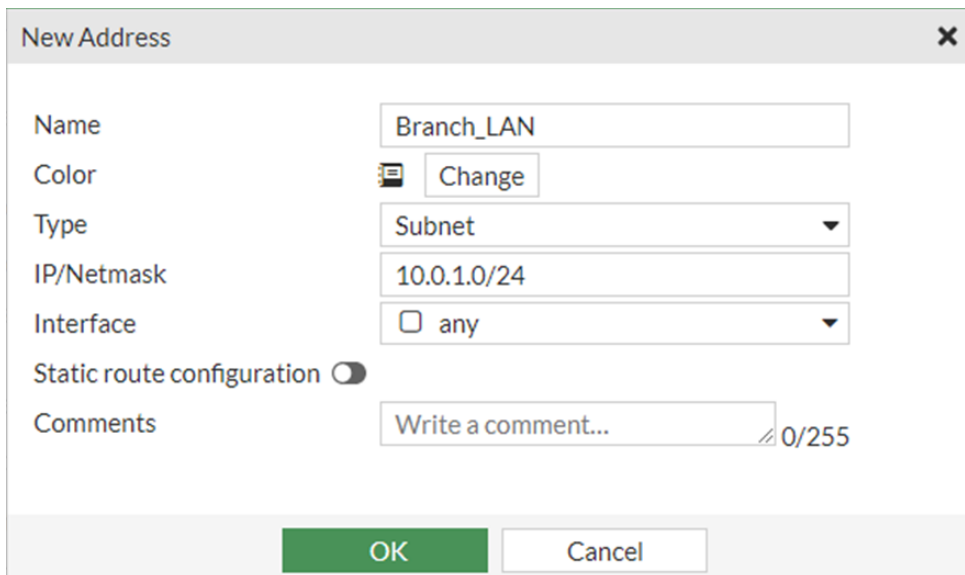
Following is an overview of the procedure:

1. Define SD-WAN rules for traffic from the branch to HQ. See [Defining rules for branch to HQ traffic on page 29](#).
2. Define SD-WAN rules for business traffic to the internet. See [Defining rules for business internet on page 32](#).
3. Define SD-WAN rules for non-business traffic to the internet. See [Defining rules for non-business traffic on page 33](#).
4. Edit the Non-Business\_Internet rule to specify it is for any traffic that is NOT part of the RFC-1918 subnets. See [Editing the Non-Business\\_Internet rule on page 36](#).

## Defining rules for branch to HQ traffic

### To create SD-WAN rules for branch to HQ traffic:

1. Go to *Network > SD-WAN > SD-WAN Rules*, and click *Create New*.
2. Set *Name* to *Branch\_to\_HQ*.
3. In the *Source* section, set the following options:
  - a. Click *Source Address*. The *Select Entries* pane is displayed.
  - b. Click *+Create > Address* to define an object for your LAN network named *Branch\_LAN*. The *New Address* pane is displayed.
  - c. Set *Name* to *Branch\_LAN*.
  - d. Set *IP/Netmask* to *10.0.1.0/24*.



The screenshot shows the 'New Address' configuration window. The fields are as follows:

Field	Value
Name	Branch_LAN
Color	Change
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	<input type="checkbox"/> any
Static route configuration	<input type="checkbox"/>
Comments	Write a comment... 0/255

- e. Click *OK*. The *Branch\_LAN* object displays in the list.
  - f. Select *Branch\_LAN*, and click *Close*.
4. In the *Destination* section, set the following options:
  - a. Click *Address*. The *Select Entries* pane is displayed.
  - b. Click *+Create > Address* to define an object for your HQ network named *HQ\_LAN*. The *New Address* pane is displayed.
  - c. Set *Name* to *HQ\_LAN*.

- d. Set *IP/Netmask* to *10.0.0.0/8*.

New Address

Name

Color

Type

IP/Netmask

Interface ☐ any

Static route configuration ☐

Comments  0/255

- e. Click *OK*. The *HQ\_LAN* object displays in the list.
- f. Select *HQ\_LAN*, and click *Close*.
5. In the *Outgoing Interfaces* section, set the following options:
- Select *Lowest Cost (SLA)*.
  - Set *Interface Preference* to *WAN1\_VPN*, *WAN2\_VPN*.
  - Set *Required SLA target* to *HQ\_VPN*.
6. Click *OK*.

Priority Rule

Name

Branch\_to\_HQ

Source

Source address

Branch\_LAN

×

+

User group

+

Destination

Address

HQ\_LAN

×

+

Protocol number

TCP UDP **ANY** Specify

0

Internet Service

+

Application

+

Outgoing Interfaces

Select a strategy for how outgoing interfaces will be chosen.

☐ Manual

Manually assign outgoing interfaces.

☐ Best Quality

The interface with the best measured performance is selected.

☒ **Lowest Cost (SLA)**

The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

☐ Maximize Bandwidth (SLA)

Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

WAN1-VPN

×

WAN2-VPN

×

+

Zone preference

+

Required SLA target

HQ\_VPN

×

+

Forward DSCP

☐

Reverse DSCP

☐

Status

Enable

Disable

OK

Cancel

## Defining rules for business internet

To create SD-WAN rules for business internet traffic:

1. Go to *Network > SD-WAN > SD-WAN Rules*, and click *Create New*.
2. Set *Name* to *Business\_Internet*.
3. In the *Source* section, click *Source Address*, and select *Branch\_LAN*.
4. In the *Destination* section, set the following options:
  - a. Click *Application*. The *Select Entries* pane is displayed.
  - b. Click *+Create > Application Group*. The *New Application Group* pane is displayed.
  - c. Set *Name* to *Critical\_Apps*.
  - d. Click *Members* and select one or more applications that are critical to your business. Click *Close* when done.

The screenshot shows the 'New Application Group' dialog box. The 'Group Name' field is filled with 'Critical\_Apps'. The 'Type' dropdown is set to 'Application'. The 'Members' list contains three items: 'Microsoft.Outlook.com', 'Salesforce', and 'Zoom', each with a small 'x' icon to its right. Below the list is a '+' icon. The 'Comments' field has a placeholder text 'Write a comment...' and a character count '0/255'. At the bottom, there are 'OK' and 'Cancel' buttons.

- e. Click *OK*. The *Critical\_Apps* object displays in the list.
  - f. Select *Critical\_Apps*, and click *Close*.
5. In the *Outgoing Interfaces* section, set the following options:
  - a. Select *Best Quality*.
  - b. Set *Interface Preference* to *ISP1, ISP2*.
  - c. Set *Measured SLA* to *Internet*.
6. Click *OK*.



Priority Rule

Name

Business\_Internet

Source

Source address

Branch\_LAN

+

×

User group

+

Destination

Address

+

Internet Service

+

Application

Critical\_Apps

+

×

Outgoing Interfaces

Select a strategy for how outgoing interfaces will be chosen.

☐ Manual

Manually assign outgoing interfaces.

☒ Best Quality

The interface with the best measured performance is selected.

☐ Lowest Cost (SLA)

The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

☐ Maximize Bandwidth (SLA)

Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

ISP1 (port2)

×

ISP2 (port3)

×

+

Zone preference

+

Measured SLA

Internet

Quality criteria

Latency

Forward DSCP

☐

Reverse DSCP

☐

Status

Enable

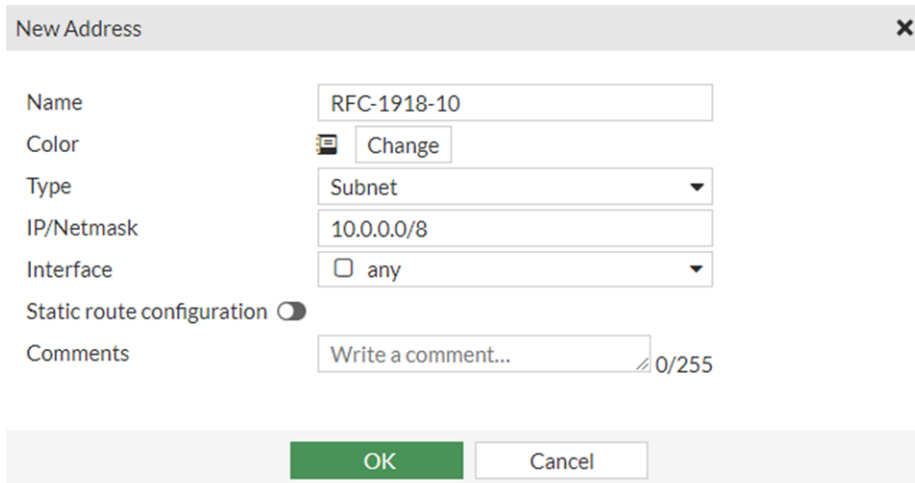
Disable

## Defining rules for non-business traffic

This rule catches all remaining traffic. Matching traffic is defined as traffic destined for any non-private (RFC-1918) IP addresses.

**To create SD-WAN rules for non-business internet traffic:**

1. Go to *Network > SD-WAN > SD-WAN Rules*, and click *Create New*.
2. Set *Name* to *Non-Business\_Internet*.
3. In the *Source* section, click *Source Address*, and select *Branch\_LAN*.
4. In the *Destination* section, create and select an address object named *RFC-1918-10*:
  - a. Click *Address*. The *Select Entries* pane is displayed.
  - b. Click *+Create > Address*. The *New Address* pane is displayed.
  - c. Set *Name* to *RFC-1918-10*.
  - d. Set *IP/Netmask* to *10.0.0.0/8*.

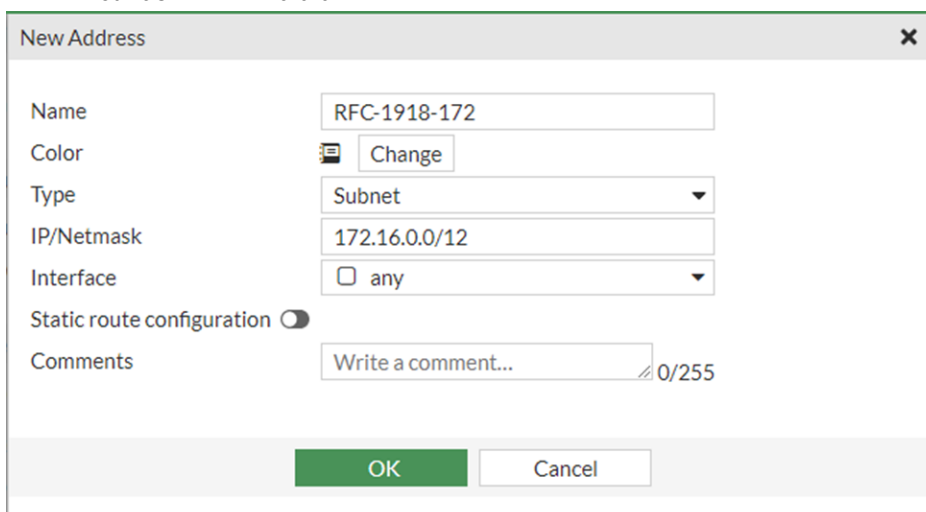


The screenshot shows the 'New Address' configuration window. The title bar is 'New Address' with a close button. The form contains the following fields and controls:

- Name:** RFC-1918-10
- Color:** A color selection icon followed by a 'Change' button.
- Type:** Subnet (dropdown menu)
- IP/Netmask:** 10.0.0.0/8
- Interface:** any (dropdown menu with a checkbox icon)
- Static route configuration:** A toggle switch that is currently turned off.
- Comments:** Write a comment... (text area) 0/255

At the bottom, there are two buttons: 'OK' (green) and 'Cancel' (white).

- e. Click *OK*. The *RFC-1918-10* object displays in the list.
  - f. Select *RFC-1918-10*. The *Select Entries* pane remains displayed.
5. Create and select an address object named *RFC-1918-172*:
    - a. In the *Select Entries* pane, click *+Create > Address*. The *New Address* pane is displayed.
    - b. Set *Name* to *RFC-1918-172*.
    - c. Set *IP/Netmask* to *172.16.0.0/12*.



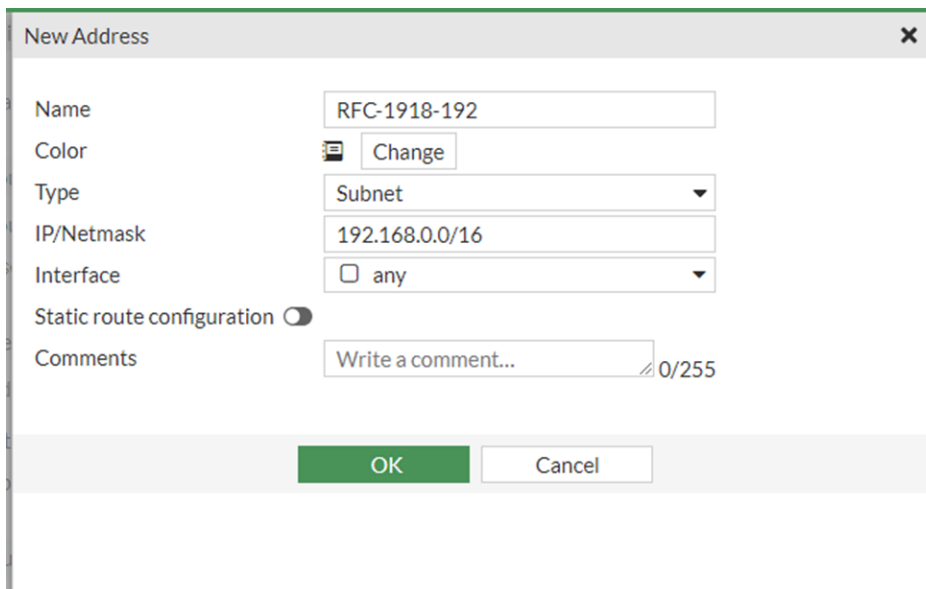
The screenshot shows the 'New Address' configuration window for the second object. The title bar is 'New Address' with a close button. The form contains the following fields and controls:

- Name:** RFC-1918-172
- Color:** A color selection icon followed by a 'Change' button.
- Type:** Subnet (dropdown menu)
- IP/Netmask:** 172.16.0.0/12
- Interface:** any (dropdown menu with a checkbox icon)
- Static route configuration:** A toggle switch that is currently turned off.
- Comments:** Write a comment... (text area) 0/255

At the bottom, there are two buttons: 'OK' (green) and 'Cancel' (white).

- d. Click *OK*. The *RFC-1918-172* object displays in the list.
- e. Select *RFC-1918-172*. The *Select Entries* pane remains open.

6. Create and select an address object named *RFC-1918-192*:
  - a. In the *Select Entries* pane, click *+Create > Address*. The *New Address* pane is displayed.
  - b. Set *Name* to *RFC-1918-192*.
  - c. Set *IP/Netmask* to *192.168.0.0/16*.

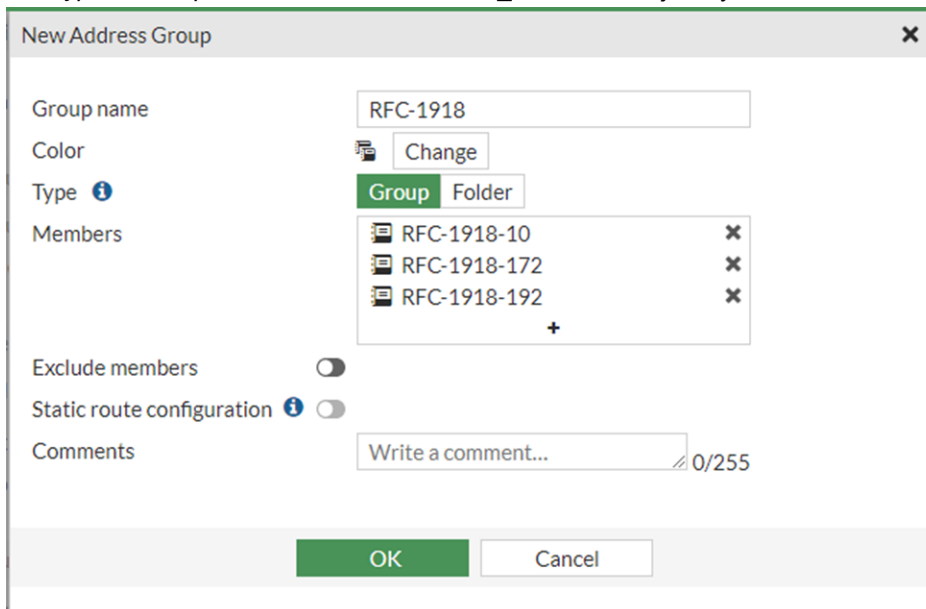


The *New Address* dialog box is shown with the following fields and values:

- Name:** RFC-1918-192
- Color:** [Color icon] Change
- Type:** Subnet
- IP/Netmask:** 192.168.0.0/16
- Interface:** any
- Static route configuration:** [Off]
- Comments:** Write a comment... 0/255

Buttons: OK, Cancel

- d. Click *OK*. The *RFC-1918-192* object displays in the list.
  - e. Select *RFC-1918-192*.
7. Create and select an address group named *RFC-1918*:
  - a. In the *Select Entries* pane, click *+Create > Address Group*. The *New Address Group* pane is displayed.
  - b. Set *Name* to *RFC-1918*.
  - c. Set *Type* to *Group*, and select the *RFC-1918\_<number>* objects you created.



The *New Address Group* dialog box is shown with the following fields and values:

- Group name:** RFC-1918
- Color:** [Color icon] Change
- Type:** Group (selected), Folder
- Members:**
  - RFC-1918-10
  - RFC-1918-172
  - RFC-1918-192
- Exclude members:** [Off]
- Static route configuration:** [Off]
- Comments:** Write a comment... 0/255

Buttons: OK, Cancel

- d. Click *OK*. The *RFC-1918* object displays in the list.
  - e. Select *RFC-1918*. Click *Close*.

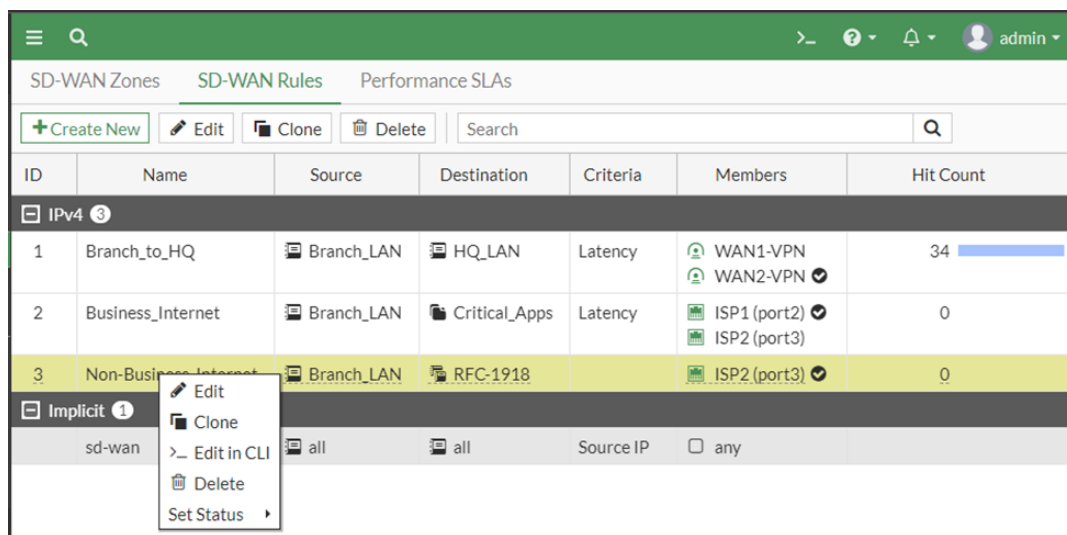
8. In the *Outgoing Interfaces* section, set the following options:
  - a. Select *Manual*.
  - b. Set *Interface Preference* to *ISP2*. This assumes that ISP2 is a lower quality or cheaper link and is preferred for non-critical traffic.
9. Click *OK*. The *Non-Business\_Internet* rule is displayed.

## Editing the Non-Business\_Internet rule

Edit the *Non-Business\_Internet* rule to specify it is for any traffic that is NOT part of the RFC-1918 subnets.

### To edit the Non-Business\_Internet rule in the CLI:

1. On the *Network > SD-WAN > SD-WAN Rules* page, right-click the *Non-Business\_Internet* rule, and select *Edit in CLI*.



2. Configure the service:

```
Branch1# config system sdwan
Branch1 (sdwan) # config service
Branch1 (service) # edit 3
Branch1 (3) # show
config service
  edit 3
    set name "Non-Business_Internet"
    set dst "RFC-1918"
    set src "Branch_LAN"
    set priority-members 2
  next
end
```

The `priority-members 2` option is the index of your ISP2 interface object.

3. Enable `dst-negate`:

```
set dst-negate enable
end
end
```

4. Close the CLI menu, and reload the *SD-WAN Rules* page. The *Destination address* displays a red *!* in front of the

name to indicate it is for any destination that is NOT part of the RFC-1918 subnets.

SD-WAN Zones		SD-WAN Rules		Performance SLAs		
+ Create New		Edit	Clone	Delete	Search	
ID	Name	Source	Destination	Criteria	Members	Hit Count
IPv4 3						
1	Branch_to_HQ	Branch_LAN	HQ_LAN	SLA	WAN1-VPN WAN2-VPN	266
2	Business_Internet	Branch_LAN	Critical_Apps	Latency	ISP1 (port2) ISP2 (port3)	0
3	Non-Business_Internet	Branch_LAN	RFC-1918		ISP2 (port3)	0
Implicit 1						
	sd-wan	all	all	Source IP	any	

## LAN edge

The LAN chapter explains how to create and use the following key components:

FortiGate	Interfaces:	Use:
	<ul style="list-style-type: none"> <li>porta</li> </ul>	<ul style="list-style-type: none"> <li>FortiLink</li> </ul>
	Firewall policies:	Use:
	<ul style="list-style-type: none"> <li>Branch LAN to HQ</li> <li>HQ to Branch LAN</li> <li>Branch business to internet</li> <li>Branch guest to internet</li> </ul>	<ul style="list-style-type: none"> <li>From the Branch subnet to HQ subnets</li> <li>Inverse of the above rule</li> <li>Branch business destined for Internet resources</li> <li>Branch guest internet access</li> </ul>

FortiSwitch	Interfaces:	Use:
	• port1	• Voice
	• port2	• Security_Camera
	• port3	• Guest (wireless)
	• port4	• Staff (wireless)
	• port5	• Point of sale
	• port8	• FortiLink
	VLANs:	Use:
	• VLAN 10	• AP VLAN
	• VLAN 100	• Point of sale
	• VLAN 200	• Security_Camera
	• VLAN 300	• Guest (wireless)
FortiAP	• VLAN 400	• Staff (wireless)
	• VLAN 500	• Voice
	SSID:	Use:
	• ACME Staff	• Corporate wireless
	• ACME Guest	• Internet-only wireless

Following is an overview of how to configure the WAN edge:

1. Configure FortiSwitch. See [FortiSwitch on page 38](#).
2. Configure FortiAP. See [FortiAP on page 44](#).
3. Configure firewall policies for security. See [Security on page 46](#).

## FortiSwitch

FortiGate uses FortiLink to manage FortiSwitch. FortiLink allows the FortiGate to fully manage a FortiSwitch as if it was simply part of the FortiGate. VLAN tags are provisioned automatically, and trunks don't need to be configured—the FortiGate and FortiSwitch act as a unified device.

Following is an overview of the procedure:

1. Remove FortiLink ports from the LAN hardware switch. See [Removing ports from the LAN hardware switch interface on page 39](#).
2. Configure the FortiLink interface. See [Configuring the FortiLink interface on page 39](#).
3. Enable the switch controller feature. See [Enabling switch controller on page 40](#).
4. Connect the FortiLink ports to the FortiSwitch. See [Connecting FortiLink ports to switch ports on page 40](#).
5. Verify FortiGate is managing the FortiSwitch. See [Verifying managed FortiSwitches on page 40](#).
6. Create VLANs in the switch controller. See [Configuring VLANs in the switch controller on page 41](#).
7. Assign VLANs to switch ports. See [Assigning VLANs to switch ports on page 43](#).
8. Enable FortiSwitch features. See [Enabling FortiSwitch features on page 43](#).

## Removing ports from the LAN hardware switch interface

By default, LAN ports are grouped together into the LAN hardware switch interface. An internal hardware switch controller connects the ports, and the ports are part of the same broadcast domain.

On FortiGate models without dedicated FortiLink ports, such as port A and port B, you can remove two of the LAN ports from the LAN interface to be used in the FortiLink interface.

### To remove ports:

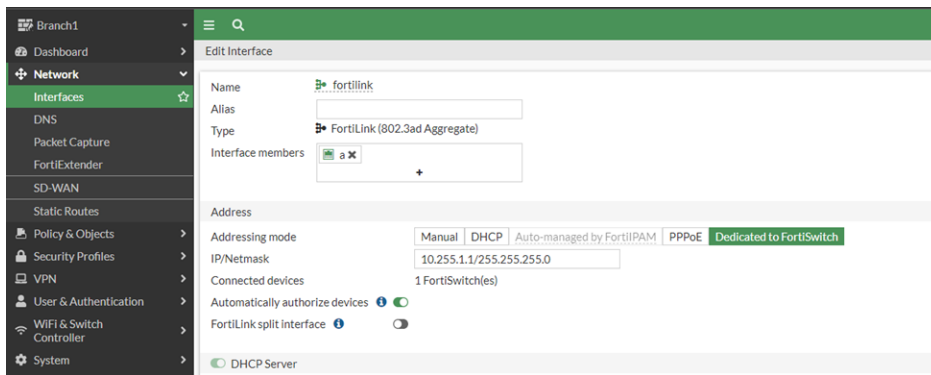
1. Go to *Network > Interfaces*, and double-click LAN interface to open it for editing.
2. In the *Interface Members* box, remove two physical ports by clicking the X for each one.  
The two ports with the highest numbers are often used, but any port can be used.
3. Click *OK* at the bottom.  
On the *Interface* page, the two ports are removed from the LAN interface, and the interfaces are displayed under the *Physical Interface* grouping.

## Configuring the FortiLink interface

FortiLink connects switches (and APs) directly to FortiGate so that the network acts as a single device.

### To configure the FortiLink interface:

1. Go to *Network > Interfaces*, and double-click *fortilink* to open the interface for editing.
2. Review the *Interface members* option. Do you see two members or no members?  
Take one of the following actions:
  - If you see two members, FortiLink is ready to connect to a switch. Note the port labels for the two members. The ports are likely labeled *A* and *B*, if they exist on your physical FortiGate.
  - If you see no interface members, select the two physical LAN ports that were removed in the previous section. See [Removing ports from the LAN hardware switch interface on page 39](#).
3. Set the following settings in the *Address* section:
  - a. Set *Address mode* to *Dedicated to FortiSwitch*.
  - b. Enable *Automatically authorize devices*.  
Devices can be manually admitted one at a time later if you wish.
  - c. Disable *FortiLink split interface*. The split interface is used in scenarios where two or more switches are connected directly to a FortiGate.
4. Enable *DCHP server*. The connected FortiSwitch will receive an IP address in this range.
5. Click *OK* to save the FortiLink settings.



## Enabling switch controller

Ensure the *WiFi & Switch Controller* tree menu is visible in the GUI by checking feature visibility.

### To enable switch controller in the GUI:

1. Go to *System > Feature Visibility*, enable *Switch Controller* and *WiFi Controller*.
2. Reload the FortiOS GUI. The tree menu displays the *WiFi & Switch Controller*.

### To enable switch controller in the CLI:

1. Go to the CLI and enter the following command:

```
config system global
    set switch-controller enable
end
```

2. Reload the FortiOS GUI. The tree menu displays the *WiFi & Switch Controller*.

## Connecting FortiLink ports to switch ports

### To connect FortiLink ports:

1. Remove the FortiSwitch from the box, and deploy it, whether mounting it in a rack or otherwise.
2. Power on the FortiSwitch device.
3. Connect the FortiSwitch to the FortiGate by using two Ethernet connections.  
Use the two designated FortiLink ports of the FortiGate to connect to the last two ports on the FortiSwitch.
4. Wait a few minutes for the switch to display in FortiOS.

## Verifying managed FortiSwitches

### To verify managed FortiSwitches:

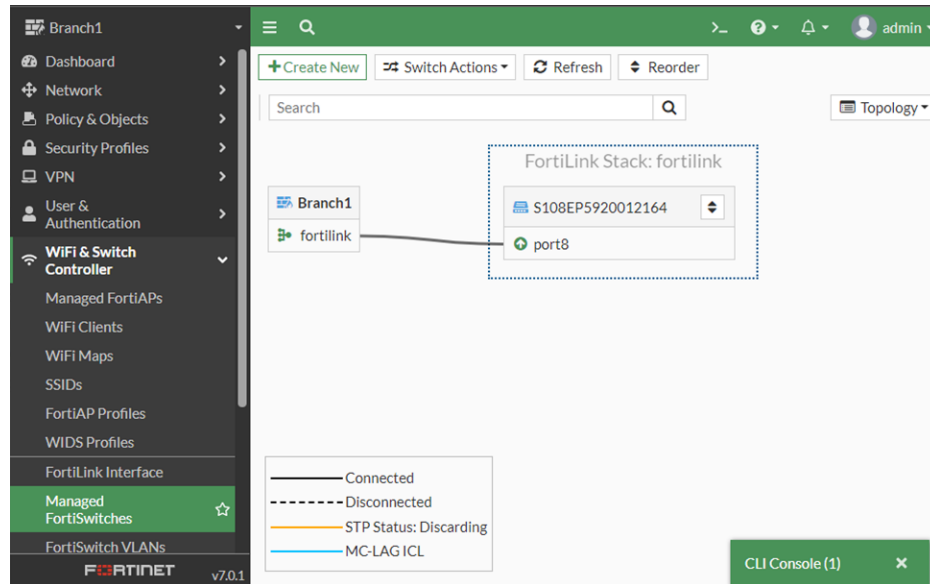
1. Go to *WiFi & switch controller > Managed FortiSwitches*.
2. Select *Topology View* from the upper-right corner dropdown menu.  
The FortiSwitch should be visible, connected to the FortiGate, and authorized.  
If FortiSwitch is not authorized, click the icon, and authorize it.



The *Topology View* displays the logical connection between the FortiGate and the connected FortiSwitch.

3. Hover the mouse over the switch icon to view a context menu with several options.

The FortiSwitch is now connected, authorized, and ready for configuration.



## Configuring VLANs in the switch controller

VLANs will be created for the following items:

- Point of Sales (POS) systems
- Employee WiFi
- Guest WiFi
- Security Cameras
- Phones

Following is a summary of the procedure:

1. Create a VLAN. See [Creating VLANs on page 42](#).
2. Configure FortiSwitch ports. See [Configure FortiSwitch ports on page 42](#).

Repeat these steps for each VLAN you will use. For example:

Branch subnet	10.0.1.0/24
Staff	10.0.1.129/26 (10.0.1.128 - 10.0.1.191)
Security Cameras	10.0.1.193/27 (10.0.1.192 – 10.0.1.223)
POS subnet	10.0.1.225/28 (10.0.1.224 – 10.0.1.239)
Voice subnet	10.0.1.241/28 (10.0.1.240 – 10.0.1.255)
Reserved for Staff wireless	10.0.1.0/25 (10.0.1.0 - 10.0.1.127)

Name	VLAN ID	IP
_default.fortilink (_default)	1	0.0.0.0 0.0.0.0
voice.fortilink (voice)	4091	0.0.0.0 0.0.0.0
video.fortilink (video)	4090	0.0.0.0 0.0.0.0
onboarding.fortilink (onboarding)	4089	0.0.0.0 0.0.0.0
Staff	400	10.0.1.1 255.255.255.128
Guest	300	10.0.1.129 255.255.255.192
Security_Camera	200	10.0.1.193 255.255.255.224
POS	100	10.0.1.225 255.255.255.240
Voice	500	10.0.1.241 255.255.255.240
quarantine.fortilink (quarantine)	4093	10.255.11.1 255.255.255.0
rspan.fortilink (rspan)	4092	10.255.12.1 255.255.255.0
nac_segment.fortilink (nac_segment)	4088	10.255.13.1 255.255.255.0

## Creating VLANs

### To create VLANs in the switch controller:

- Go to *WiFi & Switch Controller > FortiSwitch VLANs*, and click *Create New*. The *New Interface* pane is displayed.
- Set the following options to create a VLAN for POS:
  - Set *Interface Name* to *POS*.
  - Set *VLAN ID* to *100*.
  - Set *Color* to *Red*.
  - Set *Role* to *LAN*.
  - In the *IP/Netmask* box, enter a subnet for your POS. In this example *10.0.1.225/28* is used.
  - Enable *DHCP Server* for IPv4 or IPv6, if required.
  - Enable *Device detection*.
  - Enable *Block intra-VLAN traffic*.
- Click *OK*. The VLAN is created.

## Configure FortiSwitch ports

### To configure FortiSwitch ports:

- Go to *WiFi & Switch Controller > FortiSwitch Ports*.
- Click a port row.
- Click the *Native VLAN* column in one of the selected entries to change the native VLAN.
- Select the appropriate VLAN from the displayed list. The new value is assigned to the selected port.
- Click the + icon in the *Allowed VLANs* column to change the allowed VLANs.
- Select one or more of the VLANs (or the value all) from the displayed list. The new value is assigned to the selected port.

## Assigning VLANs to switch ports

Now that VLANs and ports are configured, it is time assign VLANs to the switch ports. This method assigns VLANs statically to a port.

### To assign VLANs to switch ports:

- Go to *WiFi & Switch Controller > FortiSwitch Ports*.  
Notice that the FortiLink ports show the FortiGate itself in the native VLAN column. No need to configure a trunk port.
- Change the VLAN:
  - Hover the mouse over the current native VLAN of that port. A pencil icon is displayed.
  - Click the pencil icon to open the port for editing. The *Select Entries* dialog box is displayed.
  - Choose the VLAN to assign to this port.  
If a VLAN hasn't been defined yet, click the *Create* to create a new VLAN.
  - Click *Apply* to save the change.

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping	Transceiver
port1		Static		Edge Port Spanning Tree Protocol	Staff	quarantine.fortilink (quarantine)	Powered		Untrusted	
port2		Static		Edge Port Spanning Tree Protocol	Security_Camera	quarantine.fortilink (quarantine)	Powered		Untrusted	
port3		Static		Edge Port Spanning Tree Protocol	Staff	quarantine.fortilink (quarantine)	Powered		Untrusted	
port4		Static		Edge Port Spanning Tree Protocol	AP_MGMT	quarantine.fortilink (quarantine)	Powered 8.30W	PU321E5E19004817 PU321E5E19004817	Untrusted	
port5		Static		Edge Port Spanning Tree Protocol	POS	quarantine.fortilink (quarantine)			Untrusted	
port6		Static		Edge Port Spanning Tree Protocol	Staff	quarantine.fortilink (quarantine)			Untrusted	
port7					FGT40FTK20031510					
port8					FGT40FTK20031510					
port9		Static		Edge Port Spanning Tree Protocol	Staff	quarantine.fortilink (quarantine)			Untrusted	
port10		Static		Edge Port Spanning Tree Protocol	Staff	quarantine.fortilink (quarantine)			Untrusted	

## Enabling FortiSwitch features

Enable the following FortiSwitch features:

- Network assisted device detection, which allows the FortiGate unit to use the information about connected devices detected by the managed FortiSwitch unit.
- IoT scanning, which leverages the FortiGuard service to identify Internet of things (IoT) devices. This feature requires an IoT Detection Service license.

### To enable FortiSwitch features:

- Enable network-assisted device detection:
 

```
config switch-controller network-monitor-settings
    set network-monitoring enable
end
```
- Enable IoT scanning:
  - Go to *WiFi & Switch Controller > FortiLink Interface*.
  - Enable *IoT scanning*.
  - Click *Apply*.

## FortiAP

The FortiAP will be connected to the FortiSwitch for PoE and managed by the FortiGate.

This deployment guide does not cover the details of installing access points (APs). For details, see the [FortiAP QuickStart Guides](#).

Following is an overview of the procedure:

1. Add an AP VLAN. See [Adding an AP VLAN on page 44](#).
2. Assign the AP VLAN to AP ports on the FortiSwitch. See [Assigning AP VLAN to AP ports on FortiSwitch on page 44](#).
3. Create SSIDs. See [Creating SSIDs on page 45](#).
4. Define an AP profile. See [Creating AP profiles on page 46](#).

### Adding an AP VLAN

Prepare an AP VLAN by going to FortiSwitch VLANs and creating a VLAN for AP management on the control plane. The VLAN is used to create security isolation between the AP management on the control channel and user traffic on the data channel. You can use many different methods to configure administrative access. For alternative methods, see the [Campus WLAN Architecture Guide](#).

#### To add an AP VLAN:

1. Go to *WiFi & Switch Controller > FortiSwitch VLANs*, and click *Create New*.
2. Enter a name for the interface.
3. In the Address section, set the following options:
  - a. Set *Addressing Mode* to *Manual*.
  - b. Set *IP/Netmask* to a VLAN or gateway IP address.
4. Under *Administrative Access*, select *Security Fabric Connection* under administrative access. Add others as needed.
5. Under *Network*, set the following option:
  - a. Enable *Device detection*.
  - b. Enable *Automatically authorize devices*.  
Even in a high-security environment, it is recommended to enable this option, until initial deployment is done.  
Then disable the option to lock down the network.
6. Enable *DHCP Server*, and configure the IP range.
7. Click *OK*.

### Assigning AP VLAN to AP ports on FortiSwitch

When you connect a FortiAP to a FortiSwitch port that is assigned an AP VLAN, the FortiAP automatically connects to the FortiGate, receives an IP address, and becomes authorized. To simplify the deployment, a FortiAP connects to a FortiSwitch PoE port for power source.

Following is an overview of the procedure:

1. Assign an AP VLAN to AP ports. See [Assigning an AP VLAN to AP ports on page 45](#).
2. Use an Ethernet cable to connect the APs to FortiSwitch. See [Connect the APs to FortiSwitch on page 45](#).
3. Verify managed APs. See [Verifying managed APs on page 45](#).

## Assigning an AP VLAN to AP ports

### To assign an AP VLAN to AP ports:

1. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
2. Identify a port that supports PoE.
3. Change the native VLAN to the AP VLAN:
  - a. Hover the mouse over the native VLAN of the port. A pencil icon is displayed.
  - b. Click the pencil icon to open the port for editing. The *Select Entries* dialog box is displayed.
  - c. Choose the VLAN to assign to this port.  
If a VLAN hasn't been defined yet, click the *Create* to create a new VLAN.
  - d. Click *Apply* to save the change.

## Connect the APs to FortiSwitch

### To use connect the APs to FortiSwitch:

1. Use Ethernet cables to connect the APs to the correct ports on the PoE-capable FortiSwitch.
2. Wait a few minutes for the AP devices to boot up and become authorized.  
In FortiOS, you can check the progress by going to *Security Fabric > Physical Topology* or by going to *WiFi & Switch Controller > Managed FortiAPs*.

## Verifying managed APs

### To verify APs:

1. Go to *WiFi & Switch Controller > Managed FortiAPs*.
2. If necessary, use the dropdown menu on the right-hand side to change from *Group* to *AP*.
3. If necessary, authorize APs that have not been automatically authorized by using the right-click menu or the *Edit* button.
4. It is recommended to rename the APs to indicate location, such as *MainLobby* or *Breakroom* by editing the AP.

## Creating SSIDs

Create SSIDs for guest wireless access and staff wireless access.

This example uses a passphrase for authentication. You may consider alternative forms of authentication. For example, you could use a captive portal for guest wireless so that they must consent to a terms of use agreement before gaining internet access. Or for Employee access, you can use WPA2-Enterprise with RADIUS to authenticate against users in an existing RADIUS server or Active Directory. Refer to the [FortiAP documentation](#) for further details on configuring security and user authentication. See also the [Secure Wireless Concept Guide > WLAN Configurations > Security](#) for different options.

### To create SSIDs:

1. Go to *WiFi & Switch Controller > SSIDs*, and click *Create New > SSID*.
2. Set the following options:
  - a. Enter a name for the SSID, such as *Guest*.  
The SSID name is internal and is not required to match the over-the-air SSID.
  - b. Set *Traffic mode* to *Tunnel*. In tunnel mode, WLANs are treated as interfaces in FortiGate and behave as a VLAN interface.
  - c. Set *IP/Netmask* to an IP address (VLAN GW). Choose a subnet outside of 10.0.0.0/8.
  - d. Enable *DHCP Server*, and set up the DHCP server.
  - e. Set *SSID* to a name, such as *ACME Guest*.
  - f. Set *Security Mode*, for example, *WPA2*.
  - g. Set *Passphrase* to an entry that you can give to guests.
3. Click *OK*.
4. Repeat this procedure for staff wireless, changing the name and address ranges to be 10.1.0.1/25 and 10.0.1.2 – 10.0.1.127.

## Creating AP profiles

### To create AP profiles:

1. Go to *WiFi & Switch Controller > FortiAP Profiles*, and click *Create New*.  
You may also edit the default profile for your AP model.
2. Set *Name* to *Branch\_AP*.
3. Set the following options in the *Radio 1* section:
  - a. Set *Mode* to *Access Point*.
  - b. Select *Channels*.
  - c. Adjust *Transmit power* as necessary.
  - d. Set *SSIDs* to *Manual*, and select *ACME Guest* and *ACME Staff*.
4. Set the following options in the *Radio 2* section:
  - a. Set *Mode* to *Access Point*.
  - b. Select *Channels*.
  - c. Adjust *Transmit power* as necessary.
  - d. Set *SSIDs* to *Manual*, and select *ACME Guest* and *ACME Staff*.
5. Click *OK*.
6. Select *Managed FortiAPs*, and right-click the connected AP to select *Assign Profile > Branch\_AP*.

## Security

Security is handled by firewall policies. Only traffic identification and permission is considered. Security profiles should be configured to meet your company's security posture and requirements and applied to policies.



If you are unable to specify multiple interfaces in the policy, go to *System > Feature Visibility*, and enable *Multiple Interface Policies*.

---

Following is an overview of the procedure:

1. Create zones to use in firewall policies. See [Creating zones to simplify policies on page 47](#).
2. Create a firewall policy for traffic from branch devices to HQ. See [Allowing traffic from branch LAN to HQ on page 47](#).
3. Create a firewall policy for traffic from HQ to branch devices. See [Allowing traffic from HQ to branch LAN on page 48](#).
4. Create a firewall policy for traffic from branch devices to the internet. See [Allowing traffic from branch to internet on page 49](#).
5. Create a firewall policy for wireless guest traffic to the internet. See [Allowing guest wireless traffic to internet on page 50](#).

See also [Other applications on page 50](#).

## Creating zones to simplify policies

Using zones can make the purpose of a policy more transparent to the administrator. We will create a zone called *Staff\_Zone* that will contain all the source interfaces for staff traffic.

### To create zones:

1. Go to *Network > Interfaces*, and select *+Create New > Zone*.
2. Name the zone *Staff\_Zone*, and add the following interfaces:
  - Staff
  - Voice
  - ACME\_Staff (Staff\_WiFi)
3. Click *OK* to save.

## Allowing traffic from branch LAN to HQ

This policy will allow traffic sourced from the branch subnet destined for HQ subnets. Change the incoming interface to reflect the interfaces and VLANs that require HQ connectivity.

### To allow traffic from branch to HQ:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*. The *New Policy* pane is displayed.
2. Set *Name* to *Branch\_to\_HQ*.
3. Set the following options:
  - a. Set *Incoming interface* to *Staff\_Zone*.
  - b. Set *Outgoing interface* to *WAN1\_VPN* and *WAN2\_VPN* zones.
  - c. Set *Source* to *Branch\_LAN*.
  - d. Set *Destination* to *HQ\_LAN*.
  - e. Set *Schedule* to *always*.
  - f. Set *Service* to *ALL*.
  - g. Set *Action* to *Accept*.

New Policy

Name ⓘ	Branch_to_HQ	
Incoming Interface	<input type="checkbox"/> Staff_zone	×
	+	
Outgoing Interface	<input checked="" type="checkbox"/> WAN1_VPN	×
	<input checked="" type="checkbox"/> WAN2_VPN	×
	+	
Source	<input checked="" type="checkbox"/> Branch_LAN	×
	+	
Destination	<input checked="" type="checkbox"/> HQ_LAN	×
	+	
Schedule	<input checked="" type="checkbox"/> always	▼
Service	<input checked="" type="checkbox"/> ALL	×
	+	
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY	
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based	

4. Click OK.

## Allowing traffic from HQ to branch LAN

Copy the *Branch\_to\_HQ* firewall policy, and then use it to create a firewall policy for traffic from HQ to branch offices.

**To allow traffic from HQ to branch:**

1. Go to *Policy & Objects > Firewall Policy*. The firewall policies are displayed.
2. Right-click *Branch\_to\_HQ*, and select *Copy*.

+ Create New Edit Delete

Policy Lookup Search

Interface Pair View By Sequence IPv4 + IPv6

Name	From	To	Source	Destination
Branch_to_HQ	<input checked="" type="checkbox"/> B01_LAN (port3)	<input checked="" type="checkbox"/> WAN1_VPN <input checked="" type="checkbox"/> WAN2_VPN	<input checked="" type="checkbox"/> Branch_LAN	<input checked="" type="checkbox"/> HQ_LAN
Implicit Deny	<input type="checkbox"/> any		<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all

Policy

- Set Status
- Filter by From
- Copy
- Paste



3. Right click *Branch\_to\_HQ*, and select *Paste > Below*.

Name	From	To	Source	Destination
Branch_to_HQ	B01_LAN (port3)	WAN1_VPN WAN2_VPN	Branch_LAN	HQ_LAN
Implicit_Deny	any		all	all

Policy

- Set Status
- Filter by From
- Copy
- Paste
  - ^ Above
  - ~ Below
- + Insert Empty Policy
- + Insert Sequence Grouping

4. Double-click the pasted rule to open it for editing, and set the following options:

- Set *Name* to *HQ\_to\_Branch*.
- Reverse the settings for *Incoming Interfaces* and *Outgoing Interfaces*.
- Reverse the settings for *Source* and *Destination*.
- Enable *Enable this policy*.

5. Click *OK* to save the changes.

Name	From	To	Source	Destination	Schedule	Service	Action
Branch_to_HQ	B01_LAN (port3)	WAN1_VPN WAN2_VPN	Branch_LAN	HQ_LAN	always	ALL	✓ ACCEPT
HQ_to_Branch	WAN1_VPN WAN2_VPN	B01_LAN (port3)	HQ_LAN	Branch_LAN	always	ALL	✓ ACCEPT

## Allowing traffic from branch to internet

This policy allows local subnets to access the internet directly. This may be necessary for business cloud applications, as well as local staff internet access. Adjust the incoming interfaces as necessary.

### To allow traffic from branch to internet:

- Go to *Policy & Objects > Firewall Policy*, and click *Create New*. The *New Policy* pane is displayed.
- Set *Name* to *Branch\_to\_Internet*.
- Set the following options:
  - Set *Incoming interface* to *LAN, Staff, Security Cameras, POS subnet, Voice subnet, ACME staff*.
  - Set *Outgoing interface* to *WAN1\_VPN* and *WAN2\_VPN* zones.
  - Set *Source* to *Branch\_LAN*.
  - Set *Destination* to *All*.
  - Set *Schedule* to *always*.
  - Set *Service* to *ALL*.
  - Set *Action* to *Accept*.

New Policy	
Name ⓘ	Branch_to_Internet
Incoming Interface	<div> <input type="checkbox"/> Staff_zone           <div>+</div> <div>×</div> </div>
Outgoing Interface	<div> <input checked="" type="checkbox"/> WAN1           <div>+</div> <div>×</div> </div> <div> <input checked="" type="checkbox"/> WAN2           <div>+</div> <div>×</div> </div>
Source	<div> <input checked="" type="checkbox"/> Branch_LAN           <div>+</div> <div>×</div> </div>
Destination	<div> <input checked="" type="checkbox"/> all           <div>+</div> <div>×</div> </div>
Schedule	always
Service	<div> <input checked="" type="checkbox"/> ALL           <div>+</div> <div>×</div> </div>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

4. Click OK.

## Allowing guest wireless traffic to internet

This policy allows guest access to the internet. This access is limited to the second lower quality WAN link named *LAN2*.

### To allow guest wireless traffic to the internet:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*.
2. Set the following options:
  - a. Enter a name.
  - b. Set *Incoming Interface* to *ACME Guest*.
  - c. Set *Source* to *Guest\_WLAN\**.  
\*The *Guest\_WLAN* address object is created automatically based on the Guest SSID name.
  - d. Set *Outgoing Interface* to *WAN2*.
  - e. Set *Destination* to *All*.
  - f. Set *Service* to *All*.
  - g. Set *Action* to *Accept*.
  - h. Enable *NAT*.
3. Click *OK* to save the policy.

## Other applications

You may have noticed we created three VLANs that are not referenced in any policy. To create policies for these VLANs (*Voice*, *POS*, *Security\_Camera*), you must know where each service connects to. For example, if your security cameras stream and record to storage hosted at your HQ, you can create a policy identical to *Branch\_to\_HQ*, replacing *Staff\_*

*Zone* with the *Security\_Camera* VLAN. You may also add it directly to the *Branch\_to\_HQ* policy, if the security policies are sufficient for all traffic.

## Appendix A - Products used

The following product models and firmware were used in this guide:

Product	Model	Firmware
FortiOS	Any	7.0 and later
FortiSwitch	Any	7.0 and later
FortiAP	Any	7.0 and later

# Appendix B - Documentation references

## Feature Documentation

- [FortiOS 7.0.2 Administration Guide > SD-WAN overview](#)
- [FortiOS 6.4.0 SD-Branch Retail Playbook](#)

## Solution Hub

- <https://docs.fortinet.com/sdwan/7.0>

## 4-D Resources

- [SD-WAN / SD-Branch Concept Guide](#)
- [SD-WAN / SD-Branch Architecture for MSSP](#)
- [SD-WAN Architecture for Enterprises](#)
- [SD-Branch ZTP Framework with FortiManager](#)
- [LAN Edge Deployment Guide](#)



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.