DEFINE • DESIGN • **DEPLOY** • DEMO

Enterprise Data Center Switching with FortiLink

Deployment Guide

Version 7.4.3

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

FORTINET VIDEO LIBRARY
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 LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 31, 2024
Enterprise Data Center Switching with FortiLink 7.4.3 Deployment Guide
11-743-981334-20240531

TABLE OF CONTENTS

Change log

Date	Change Description
May 31, 2024	Initial release

Introduction

Executive summary

This deployment guide shows how to build a scalable network for the common enterprise data center using FortiSwitch and FortiGate devices. The FortiSwitch units are centrally managed by the FortiGate device over FortiLink. All FortiSwitch units—providing connectivity and enough bandwidth for the servers—form multichassis link aggregation groups (MCLAGs) to achieve high availability. The FortiGate devices protect the servers from the internet and secure server-to-server communications by inspecting inter-VLAN and intra-VLAN traffic. This guide also explains how to deploy inter-VLAN routing offload, which moves basic layer-3 functionality for trusted VLANs from the FortiGate device to the FortiSwitch unit.

Intended audience

This guide is intended for network and security architects and engineers who are interested in deploying Fortinet's FortiSwitch units in a new environment or in replacing their equipment in an existing environment. Readers are expected to have a firm understanding of networking and security concepts.

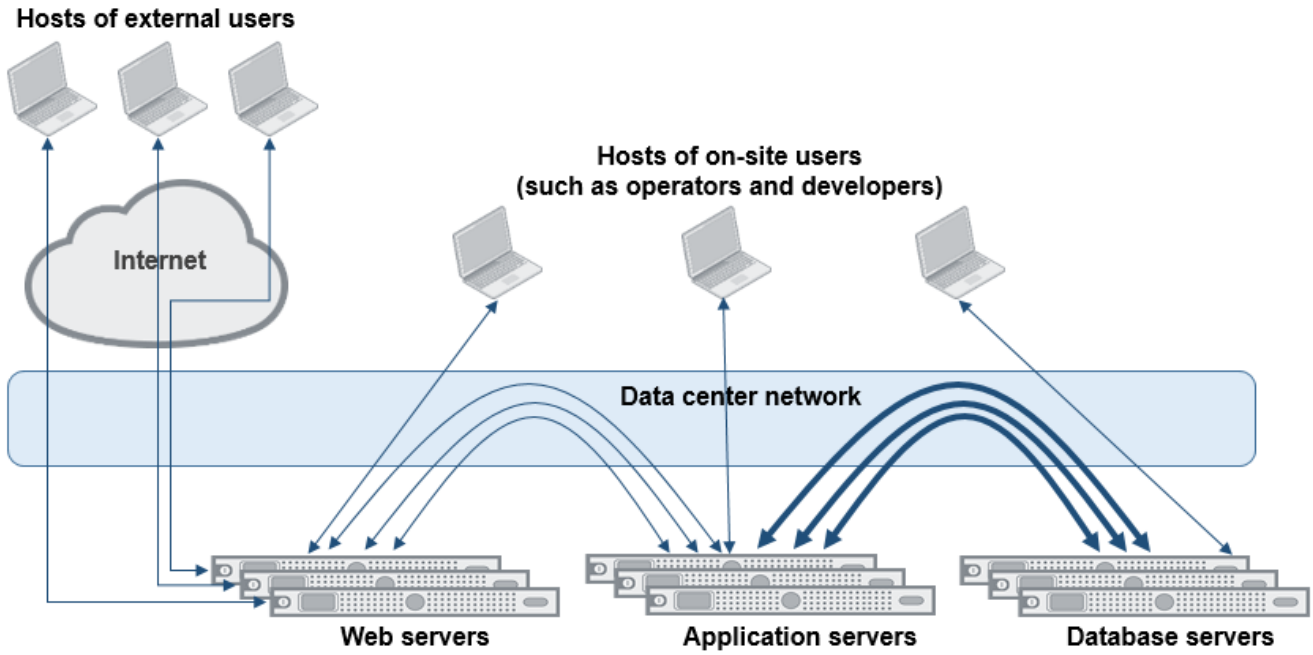
About this guide

The deployment guide provides the design and deployment steps involved in deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture and design outlined in this guide is suitable for them. It is advisable to review the administration guide if readers are still in the process of selecting the right architecture.

This deployment guide presents one of many possible ways to deploy the solution. It might omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product administration guides, Knowledge Base articles, cookbooks, release notes, and other documents where appropriate.

Requirements and design overview

This document describes an enterprise data center network based on a three-layer model with on-site and external users, as shown in the following figure. The servers and hosts of on-site users are connected to multiple FortiSwitch units. The FortiGate devices secure the communications between the servers and hosts and manage the FortiSwitch units.



Based on the requirements in the figure, four VLANs and the corresponding subnets are assigned. Between each pair of these VLANs and subnets, different policies are applied according to the requirements. The following table summarizes the VLANs and subnets required for this design and the policies that need to be configured.

Purpose	VLAN	Subnet	Policy
Database servers	VLAN10	192.168.10.0/24	High traffic between VLAN10 and VLAN20
Application servers	VLAN20	192.168.20.0/24	High traffic between VLAN10 and VLAN20
Web servers	VLAN30	192.168.30.0/24	VLAN30 can be accessed from the internet. The servers in VLAN30 can access the servers in VLAN20.
Hosts of on-site users	VLAN40	192.168.40.0/24	Microsegmentation is required. The hosts in VLAN40 can access the servers in VLAN10, VLAN20, VLAN30, and the internet.

A high volume of traffic between VLAN10 and VLAN20 is expected because application servers send lots of requests to database servers and receive massive responses. To optimize the performance of the FortiGate device keeping the application servers secure from the outside, the FortiSwitch unit can offload the traffic between VLAN10 and VLAN20. Microsegmentation is applied to VLAN40, where the hosts of on-site users are connected.

Deployment overview

This section gives an overview of the three-tier topology used for this deployment, how to select the FortiGate and FortiSwitch models for this deployment, and an example of the physical topology used for this deployment.

Three-tier topology

In today's data center network, the spine-leaf architecture is widely deployed. Spine switches aggregate leaf switches. The servers are connected to the leaf switches. The spine-leaf architecture provides enough bandwidth for north-south traffic (between the internet and servers), as well as for east-west traffic (between the servers). Even when the server workloads increase and the network bandwidth is not enough, the spine-leaf architecture can be expanded by adding more links between the spine and the leaf level. If the number of servers is not enough and there are not enough ports on the leaf switches, another leaf switch can be added to accommodate more servers.

In the example in this document, tier-1 FortiSwitch units serve as the spine switches, and tier-2 FortiSwitch units serve as the leaf switches. In addition, tier-3 FortiSwitch units serve the hosts of on-site users.

All FortiSwitch units are managed by FortiGate devices using FortiLink.

All tier-1 and tier-2 FortiSwitch units are active-active because the tier-1 and tier-2 switches form MCLAG peer groups. In a normal state, all FortiSwitch units and the links between FortiSwitch units are active. Any single failure of a FortiSwitch unit or a link does not affect the end-to-end communication, except for a brief outage.

Two FortiGate devices form a high-availability (HA) cluster, so no single failure of a FortiGate device affects the end-to-end communication as well.

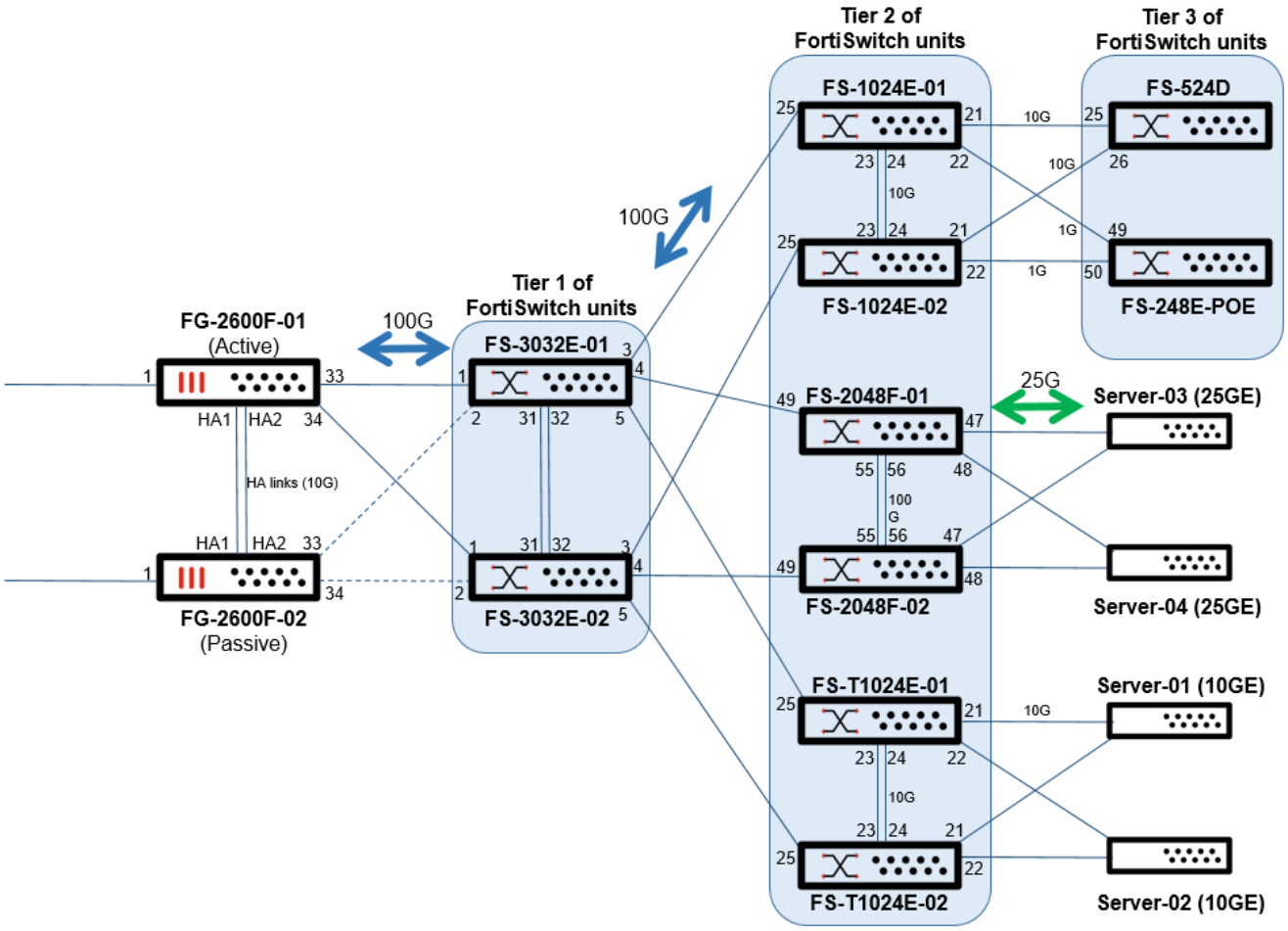
Choosing FortiGate and FortiSwitch models

In this example, based on the estimated workload and port speeds, two FG-2600F models are used.

For Tier-1 FortiSwitch units, the FS-3032E model is selected because this model has 32 x 100GE ports to aggregate the tier-2 FortiSwitch units. All tier-2 FortiSwitch units need 100GE uplinks toward tier 1, so, based on the port speeds of the server downlinks, the FS-2048F (25GE SFP28), FS-1024E (10GE SFP+), and FS-T1024E (10GBASE-T) models are selected.

Physical topology

The following figure is an example of the physical topology for this deployment.



All links between tier-1 and tier-2 FortiSwitch units are 100GE. Tier-1 FortiSwitch units are connected to FortiGate devices by 100GE as well.

Servers with 25GE-capable interfaces are connected to two FS-2048F switches in tier 2. Servers with 10GBASE-T interfaces are connected to two FS-T1024E switches in tier 2. If there are servers with 10GE SFP+ interfaces, they can be connected to the FS-1024E switches in tier-2 (not shown in physical topology example).

The tier-3 FortiSwitch uplinks are 10G and 1G. The tier-3 FortiSwitch units are connected to two FS-1024E switches in tier 2 because the hosts of on-site users do not need high bandwidth compared to servers.

There are four VLANs in this topology. In a common data center powered by virtualization, every VLAN is extended to the ports where servers are connected to support the live migration of virtual machines. So, in the example in this document, all four VLANs are allowed on all ports facing toward the servers. If you want to optimize the links between tier 1 and tier 2, you can move the virtual machines to the appropriate server.

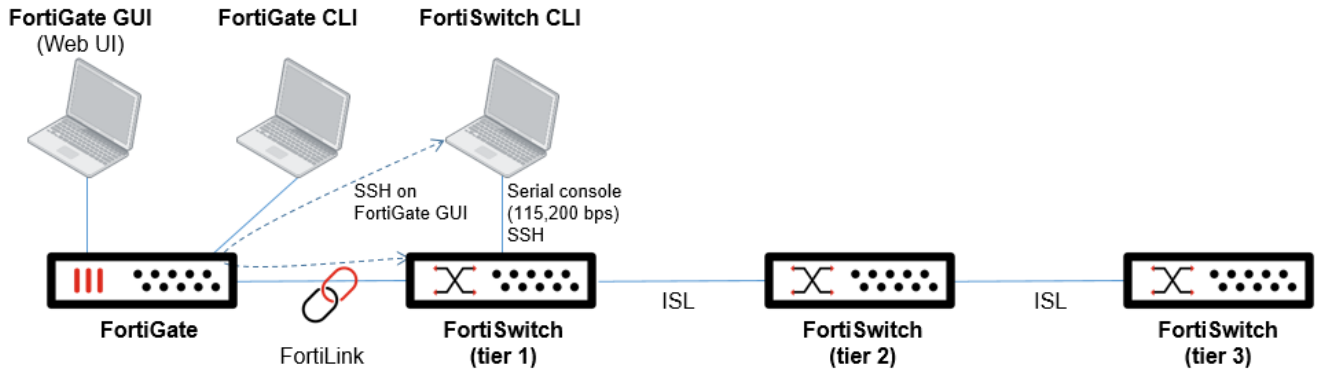
Deployment procedures

To deploy the example physical topology, follow these steps:

Accessing and configuring FortiGate and FortiSwitch devices

Using a FortiLink setup, there are three ways to access and configure FortiGate and FortiSwitch devices:

- Using the FortiGate GUI (FortiOS)
- Using the FortiGate CLI with SSH or the serial console
- Using the FortiSwitch CLI with the serial console or by invoking the FortiSwitch CLI from the FortiGate GUI (with SSH)



You can use the FortiGate GUI for most of the configurations. However, some features (such as routing offload and renaming FortiSwitch units) are only supported on the FortiGate CLI with FortiOS 7.4.3 and FortiSwitchOS 7.4.3.

To use routing offload, you need to install the advanced features license on the tier-1 FortiSwitch units. Refer to Downloading a license file.

When your FortiSwitch units are managed by a FortiGate device, basically you do not have to use the FortiSwitch CLI. In this document, the following three configurations are done in the FortiSwitch CLI. However, 2 and 3 can also be configured by using custom commands in the FortiGate CLI.

1. Connecting the ports of the tier-1 FortiSwitch units to the FortiGate devices
2. Configuring `auto-isl-port-group` on the tier-1 FortiSwitch units to connect multiple MCLAG peer groups in tier 2
3. MCLAG split-brain detection

Prerequisites

This architecture guide assumes that the following tasks have already been done:

- All FortiGate and FortiSwitch devices are connected by cables (optical transceivers, fiber optic cables, and direct-attach cables).
- The two FortiGate devices are already configured as an active-passive pair.
- All FortiSwitch units are using the factory defaults and are powered down.

In some data center deployments, switches are connected to an out-of-band (OOB) network by the management interface. On FortiSwitch units managed by a FortiGate device, an OOB network might be useful for troubleshooting, but it is not mandatory for the initial deployment. In the example topology, the management interfaces of the FortiSwitch units are not used.

Preparation

Before configuring the example, complete the following tasks:

- In the FortiGate CLI, configure the admin password for each FortiSwitch unit managed by the FortiGate devices. Use the following commands to automatically configure the admin password on all FortiSwitch units managed by this FortiGate device:

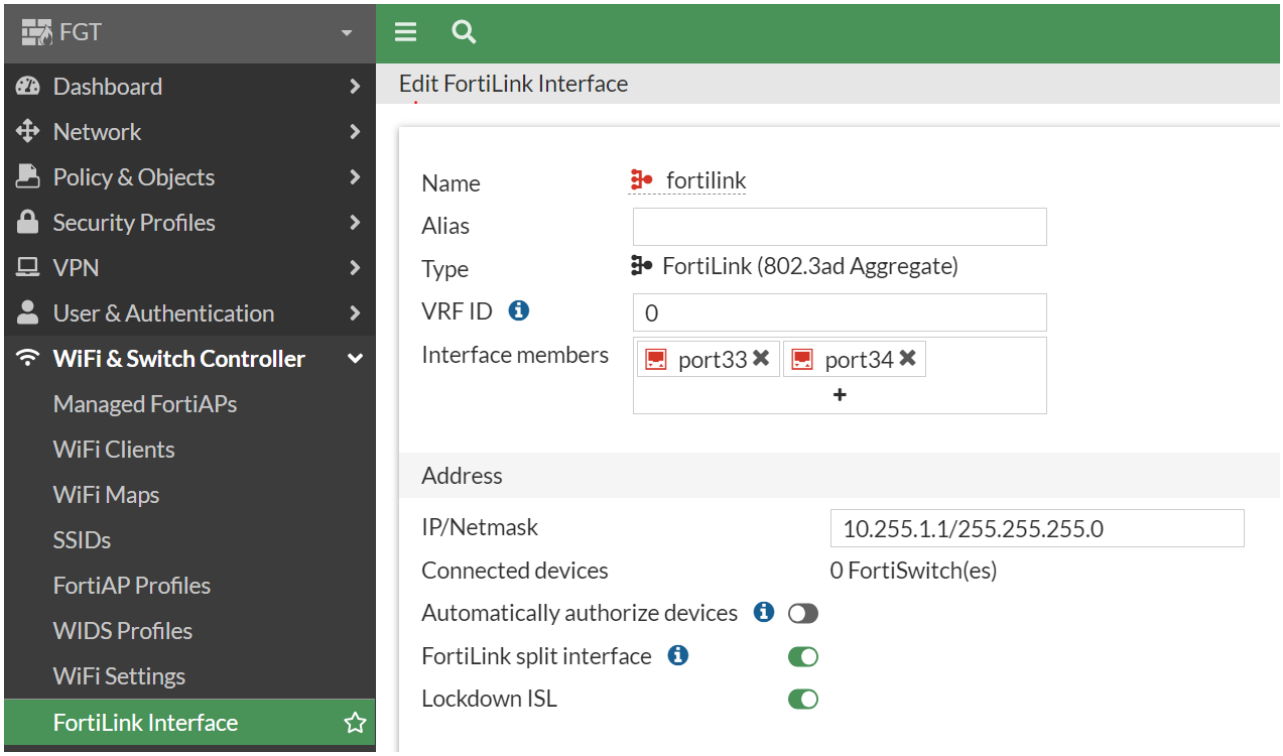
```
FGT # config switch-controller switch-profile
FGT (switch-profile) # edit default
FGT (default) # set login-passwd-override enable
FGT (default) # set login-passwd <admin password of FortiSwitch>
FGT (default) # end
```

- In the example topology, the FortiGate devices and the tier-1 FortiSwitch units are connected by a 100GE direct-attach cable (FN-CABLE-QSFP28-1) on port33 and port34 of the FortiGate device. Configure the following settings in the FortiGate CLI:

```
FGT # config system interface
FGT (interface) # edit port33
FGT (port33) # set mediatype cr4
FGT (port33) # set speed 100Gfull
FGT (port33) # set forward-error-correction disable
FGT (port33) # next
FGT (interface) # edit port34
```

```
FGT (port34) # set mediatype cr4
FGT (port34) # set speed 100Gfull
FGT (port34) # set forward-error-correction disable
FGT (port34) # next
FGT (interface) # end
```

- Using the FortiGate GUI, add two members, port33 and port34, to the *fortilink* interface.



Configuring tier 1: First FS-3032E switch

To configure the first FS-3032E switch:

1. Power on the first FS-3032E switch.
2. Use the FortiSwitch CLI to enter the following commands:

```
FS3E32T421000171 # config switch physical-port
FS3E32T421000171 (physical-port) # edit port1
FS3E32T421000171 (port1) # set speed 100000cr4
FS3E32T421000171 (port1) # set fec-state disabled
FS3E32T421000171 (port1) # next
FS3E32T421000171 (physical-port) # edit port2
FS3E32T421000171 (port2) # set speed 100000cr4
FS3E32T421000171 (port2) # set fec-state disabled
FS3E32T421000171 (port2) # next
FS3E32T421000171 (physical-port) # end
```

3. After the first FS-3032E switch is discovered by the FortiGate device, authorize the switch.
4. After the switch goes online, rename it using the following commands:

```
FGT # config switch-controller managed-switch
```

```
FGT (managed-switch) # rename FS3E32T421000171 to FS-3032E-01
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # end
```

NOTE: You can use the FortiGate GUI to rename the switch before authorizing it.

5. When you can see the first FS-3032E switch from the FortiGate device as “FS-3032E-01,” enter the following commands using the FortiGate CLI. Although these commands are similar to the commands in step 2, the FortiGate device overwrites the FortiSwitch port configuration, so you need to enter these commands in the FortiGate CLI to keep the configuration consistent.

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # edit FS-3032E-01
FGT (FS-3032E-01) # config ports
FGT (ports) # edit port1
FGT (port1) # set speed 100000cr4
FGT (port1) # set fec-state disabled
FGT (port1) # next
FGT (ports) # edit port2
FGT (port2) # set speed 100000cr4
FGT (port2) # set fec-state disabled
FGT (port2) # next
FGT (ports) # end
FGT (FS-3032E-01) # end
```

Configuring tier 1: Second FS-3032E switch

To configure the second FS-3032E switch:

1. Power on the second FS-3032E switch.

   The second FS-3032E switch is discovered by the FortiGate device through the links toward the first FS-3032E switch.
2. Authorize the second FS-3032E switch.
3. Use the following commands to rename the second FS-3032E switch:

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # rename FS3E32T421000082 to FS-3032E-02
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # end
```

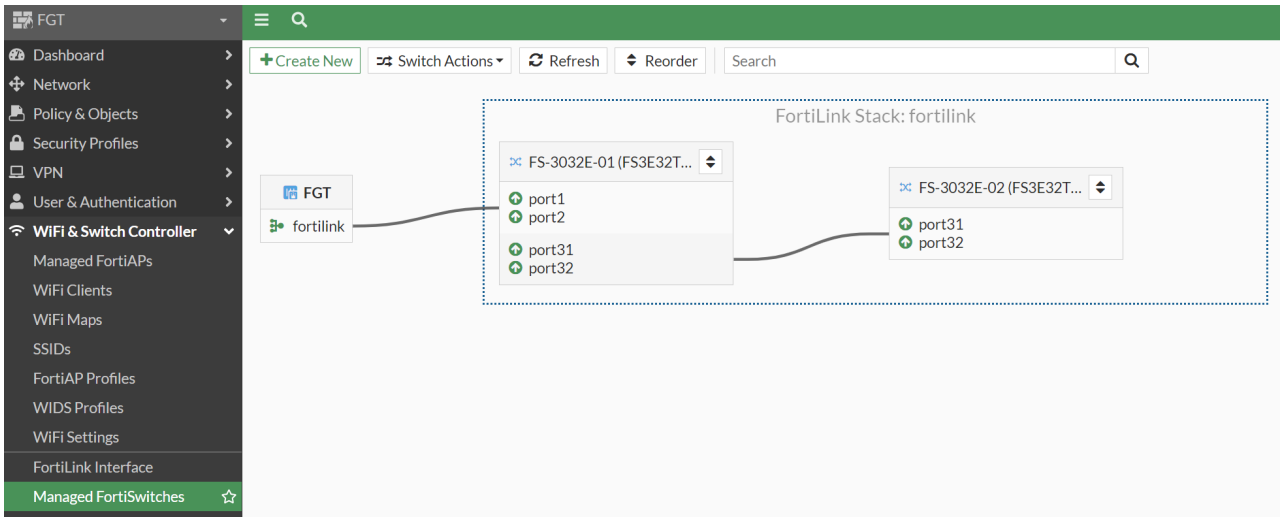
4. After the second FS-3032E switch is online and visible from the FortiGate device as “FS-3032E-02, ” enter the following commands using the FortiGate CLI:

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # edit FS-3032E-02
FGT (FS-3032E-02) # config ports
FGT (ports) # edit port1
FGT (port1) # set speed 100000cr4
FGT (port1) # set fec-state disabled
FGT (port1) # next
FGT (ports) # edit port2
FGT (port2) # set speed 100000cr4
FGT (port2) # set fec-state disabled
FGT (port2) # next
```

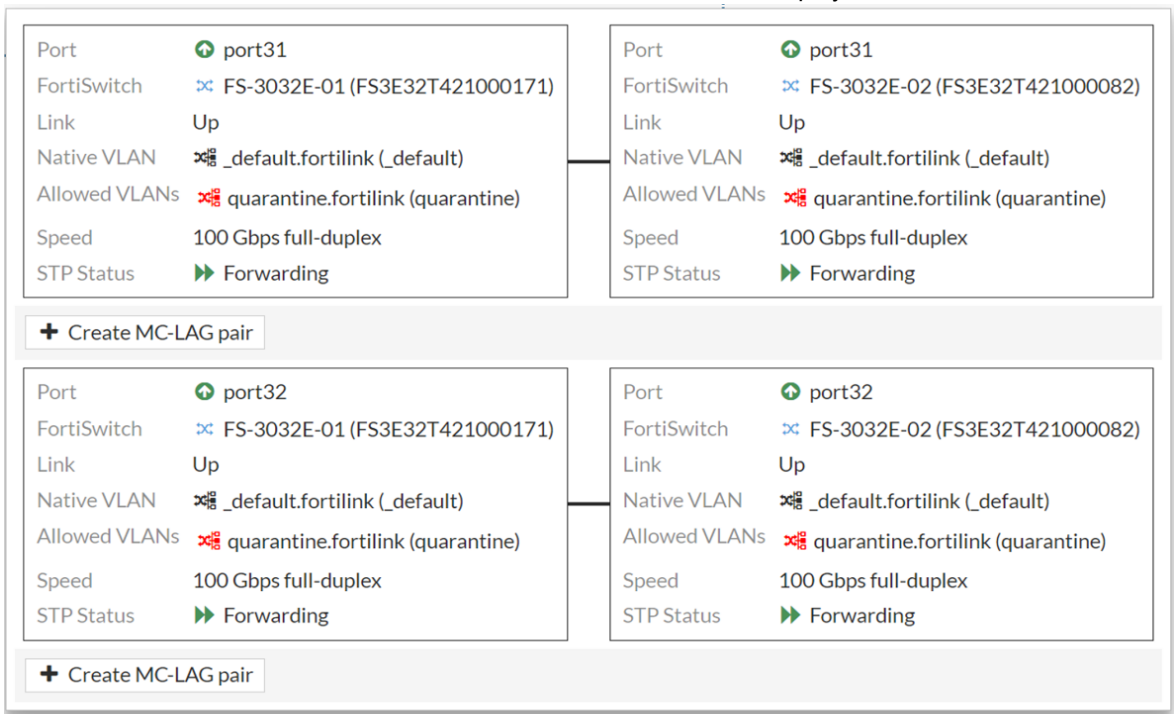
```
FGT (ports) # end
FGT (FS-3032E-02) # end
```

5. In the FortiGate GUI, go to *WiFi & Switch Controller* > *Managed FortiSwitches* and select *Topology* from the dropdown list.

   You can see that the links from FS-3032E-02 to the FortiGate device are up.

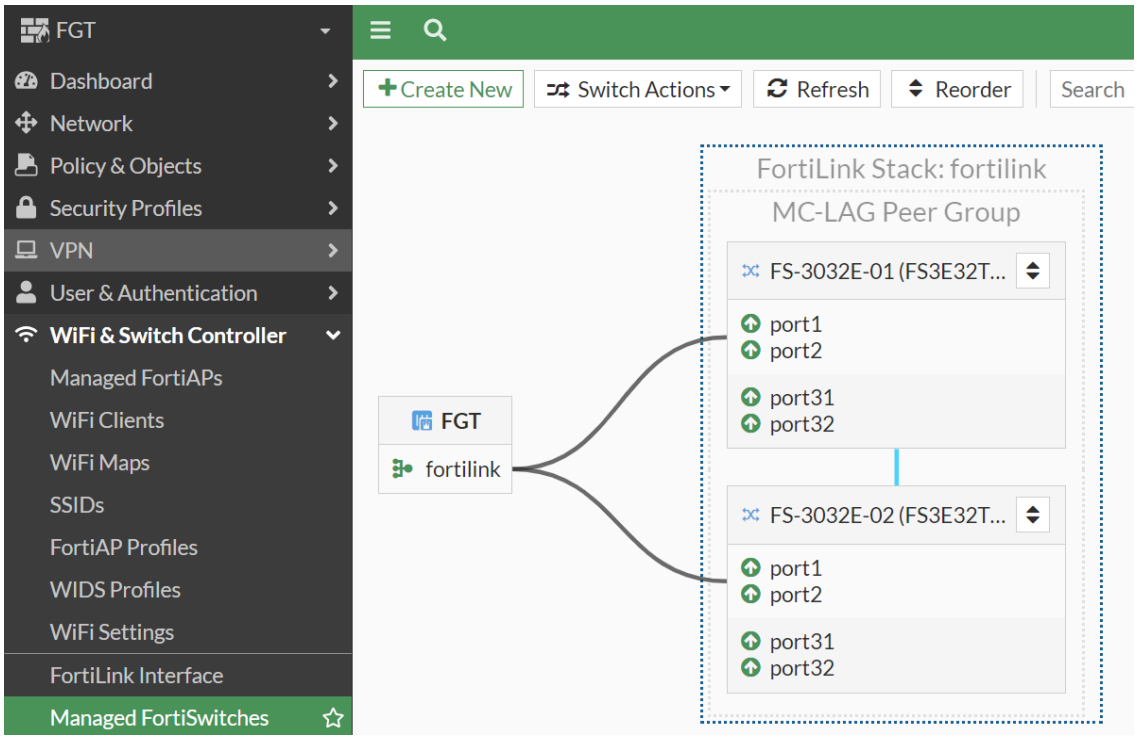


6. You can use the FortiGate GUI or CLI to configure an MCLAG on the Tier-1 FortiSwitch units. In the FortiGate GUI, hover the cursor over the link between the two FS-3032E switches to display the detail window:



7. In the detail window, click *Create MC-LAG pair*.
8. Disable the FortiLink split interface.

   After a short while, the MCLAG peer group is formed, as shown in the following figure.



Configuring tier 2: When there are multiple MCLAG peer groups in tier 2

In FortiOS 7.4.3 with FortiSwitchOS 7.4.3, if there are two or more tier-2 MCLAG peer groups connected to tier-1 FortiSwitch units to form an MCLAG, you need to configure the `auto-isl-port-group` on the tier-1 FortiSwitch units using the FortiSwitch CLI. Without this configuration, the MCLAG between the tier 1 and tier 2 is not formed correctly.

In the example topology, there are three MCLAG peer groups in tier 2. You need to enter the following commands on the tier-1 FortiSwitch units, FS-3032E-01 and FS-3032E-02, using the FortiSwitch CLI. Enter the same commands on both FortiSwitch units.

```
FS-3032E-01 # config switch auto-isl-port-group
FS-3032E-01 (auto-isl-port-g~o) # edit Tier2-1024E
FS-3032E-01 (Tier2-1024E) # set members port3
FS-3032E-01 (Tier2-1024E) # next
FS-3032E-01 (auto-isl-port-g~o) # edit Tier2-2048F
FS-3032E-01 (Tier2-2048F) # set members port4
FS-3032E-01 (Tier2-2048F) # next
FS-3032E-01 (auto-isl-port-g~o) # edit Tier2-T1024E
FS-3032E-01 (Tier2-T1024E) # set members port5
FS-3032E-01 (Tier2-T1024E) # next
FS-3032E-01 (auto-isl-port-g~o) # end
```

Configuring tier 2: Two FS-1024E switches

To configure the two FS-1024E switches:

1. Power on both FS-1024E switches.
2. After each FS-1024E switch is discovered by the FortiGate device, authorize the switch.
3. Rename each FortiSwitch unit:

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # rename FS1E24TF23003805 to FS-1024E-01
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # rename FS1E24TF23003810 to FS-1024E-02
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # end
```

4. Configure an MCLAG peer group.

   In tier 2 and tier 3, you can use the FortiGate CLI to configure the MCLAG peer group. Because port23 and port24 on the FS-1024E-01 and FS-1024E-02 switches are connected back-to-back, configure an LLDP profile on these ports to create an interchassis link (ICL) for the MCLAG.

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # edit FS-1024E-01
FGT (FS-1024E-01) # config ports
FGT (ports) # edit port23
FGT (port23) # set lldp-profile default-auto-mclag-icl
FGT (port23) # next
FGT (ports) # edit port24
FGT (port24) # set lldp-profile default-auto-mclag-icl
FGT (port24) # next
FGT (ports) # end
FGT (FS-1024E-01) # next
FGT (managed-switch) # edit FS-1024E-02
FGT (FS-1024E-02) # config ports
FGT (ports) # edit port23
FGT (port23) # set lldp-profile default-auto-mclag-icl
FGT (port23) # next
FGT (ports) # edit port24
FGT (port24) # set lldp-profile default-auto-mclag-icl
FGT (port24) # next
FGT (ports) # end
FGT (FS-1024E-02) # end
```

Configuring tier 2: Two FS-2048F switches and two FS-T1024E switches

To configure the two FS-2048F switches and two FS-T1024E switches:

1. On the two FS-2048F switches, the steps to configure each FortiSwitch unit are almost the same as the steps to configure the two FS-1024E switches, except that port55 and port56 are members of the ICL.

```
FGT # config switch-controller managed-switch
```

```
FGT (managed-switch) # rename FS2F48TV23000194 to FS-2048F-01
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # rename FS2F48TV23000243 to FS-2048F-02
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # end

FGT # config switch-controller managed-switch
FGT (managed-switch) # edit FS-2048F-01
FGT (FS-2048F-01) # config ports
FGT (ports) # edit port55
FGT (port55) # set lldp-profile default-auto-mclag-icl
FGT (port55) # next
FGT (ports) # edit port56
FGT (port56) # set lldp-profile default-auto-mclag-icl
FGT (port56) # next
FGT (ports) # end
FGT (FS-2048F-01) # next
FGT (managed-switch) # edit FS-2048F-02
FGT (FS-2048F-02) # config ports
FGT (ports) # edit port55
FGT (port55) # set lldp-profile default-auto-mclag-icl
FGT (port55) # next
FGT (ports) # edit port56
FGT (port56) # set lldp-profile default-auto-mclag-icl
FGT (port56) # next
FGT (ports) # end
FGT (FS-2048F-02) # end
```

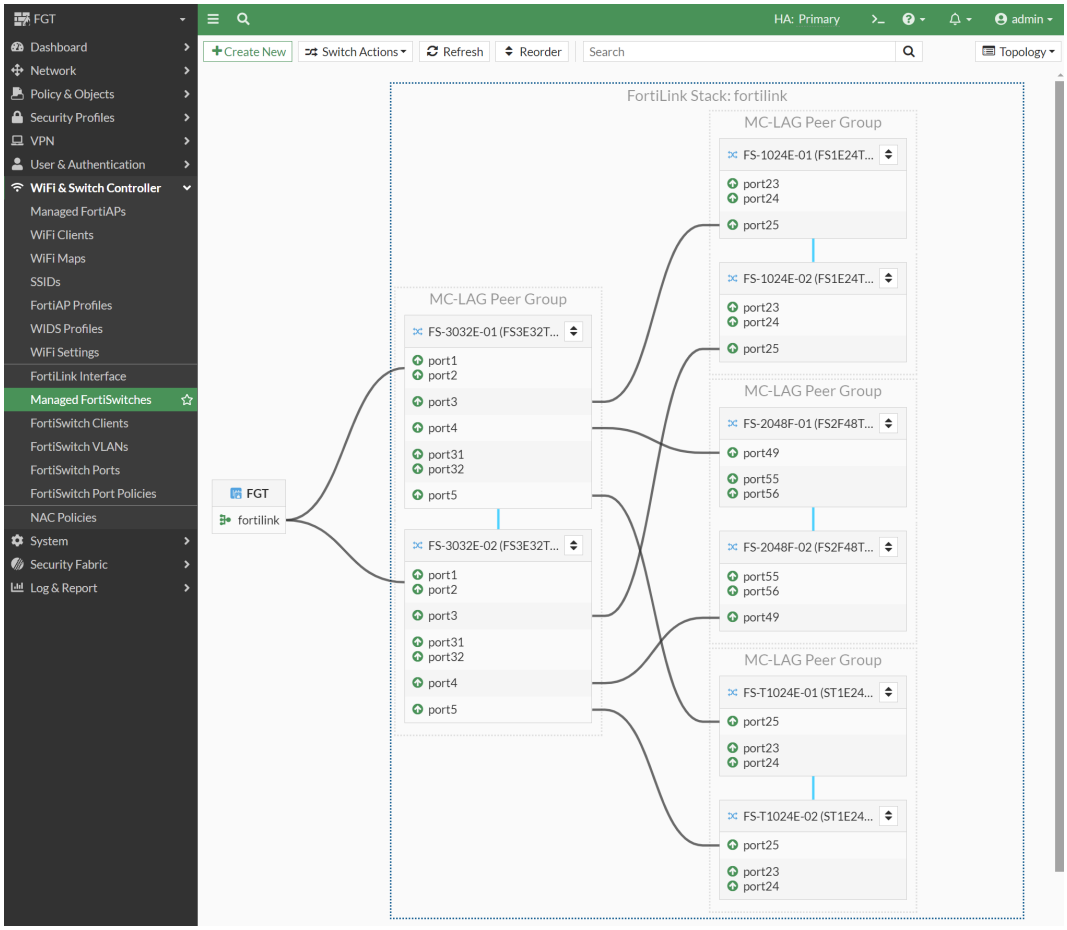
2. On the two FS-T1024E switches, the steps to configure each FortiSwitch unit are exactly same as the steps for the two FS-1024E switches.

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # rename ST1E24TF21000347 to FS-T1024E-01
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # rename ST1E24TF21000408 to FS-T1024E-02
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # end

FGT # config switch-controller managed-switch
FGT (managed-switch) # edit FS-T1024E-01
FGT (FS-T1024E-01) # config ports
FGT (ports) # edit port23
FGT (port23) # set lldp-profile default-auto-mclag-icl
FGT (port23) # next
FGT (ports) # edit port24
FGT (port24) # set lldp-profile default-auto-mclag-icl
FGT (port24) # next
FGT (ports) # end
FGT (FS-T1024E-01) # next
FGT (managed-switch) # edit FS-T1024E-02
FGT (FS-T1024E-02) # config ports
FGT (ports) # edit port23
FGT (port23) # set lldp-profile default-auto-mclag-icl
FGT (port23) # next
```

```
FGT (ports) # edit port24
FGT (port24) # set lldp-profile default-auto-mclag-icl
FGT (port24) # next
FGT (ports) # end
FGT (FS-T1024E-02) # end
```

3. After you have configured the FortiSwitch units and MCLAG peer groups for tier 1 and tier 2, you can see the following Topology view in the FortiGate GUI:



Configuring the tier-3 switches

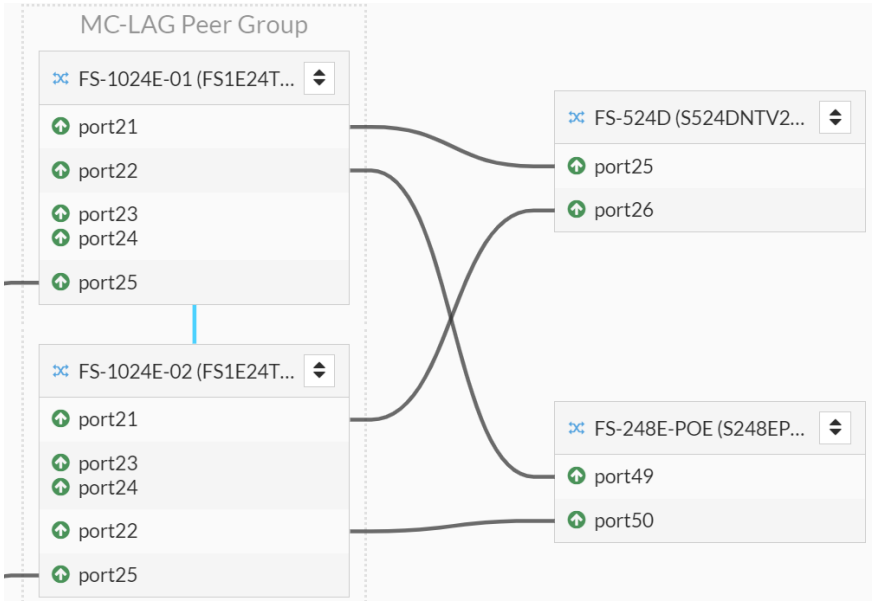
To configure the tier-3 switches:

1. Power on the FS-524D and FS-248E-POE switches for tier 3.
2. Authorize the switches.
3. Rename the switches.

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # rename S524DNTV23000332 to FS-524D
Rename the managed-switch will make the switch offline and online momentarily
Do you want to continue? (y/n)y
FGT (managed-switch) # rename S248EP3X17000126 to FS-248E-POE
Rename the managed-switch will make the switch offline and online momentarily
```

```
Do you want to continue? (y/n)y
FGT (managed-switch) # end
```

The Topology view looks like the following figure:



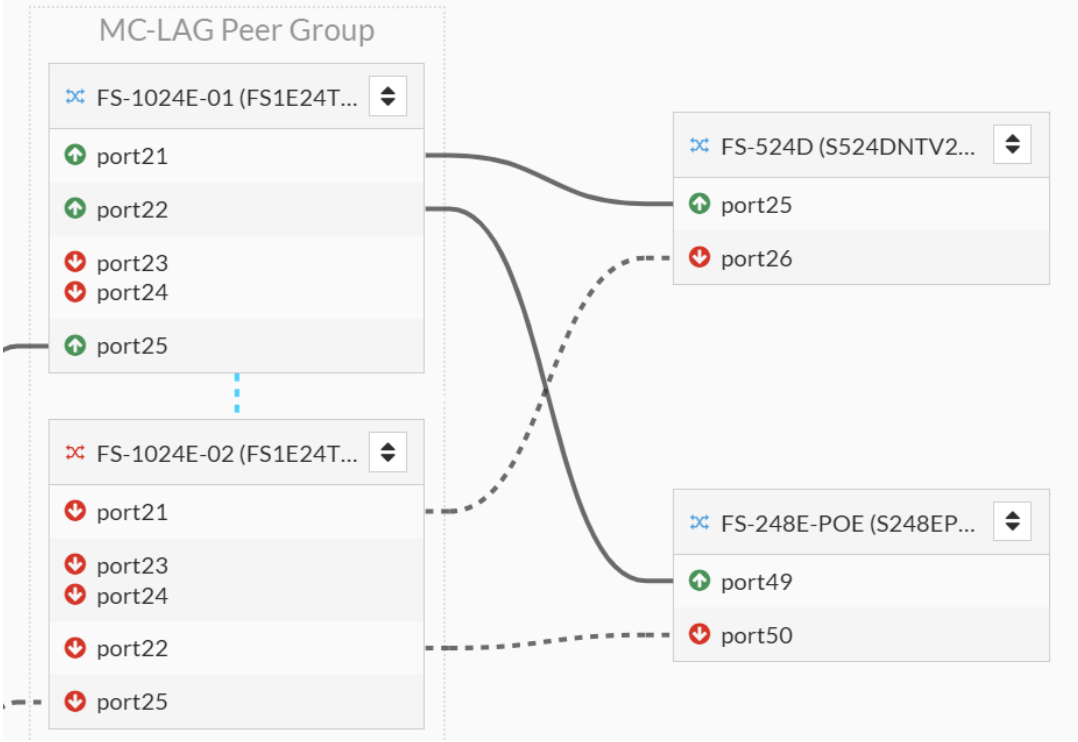
Configuring MCLAG split-brain detection

On the tier-2 MCLAG peer group of FS-1024E switches, configure MCLAG split-brain detection. To select which FortiSwitch unit becomes dormant when the split-brain state (all members of the ICL are down) is detected, at least one FortiSwitch unit is connected to both FortiSwitch units in the MCLAG peer group.

```
FS-1024E-01 # config switch global
FS-1024E-01 (global) # set mclag-split-brain-detect enable
FS-1024E-01 (global) # set mclag-split-brain-all-ports-down enable
FS-1024E-01 (global) # set mclag-split-brain-priority 80
FS-1024E-01 (global) # end
FS-1024E-02 # config switch global
FS-1024E-02 (global) # set mclag-split-brain-detect enable
FS-1024E-02 (global) # set mclag-split-brain-all-ports-down enable
FS-1024E-02 (global) # set mclag-split-brain-priority 20
FS-1024E-02 (global) # end
```

For details, refer to Detecting a split-brain state.

When the all members of the ICL are down (in a split-brain state), the FortiSwitch unit configured with a lower `mclag-split-brain-priority` becomes dormant, and all ports go down, as shown in the following figure.



Enter the `diagnose switch mclag icl` command in the FortiSwitch CLI to see a detailed status of the ICL and split-brain detection.

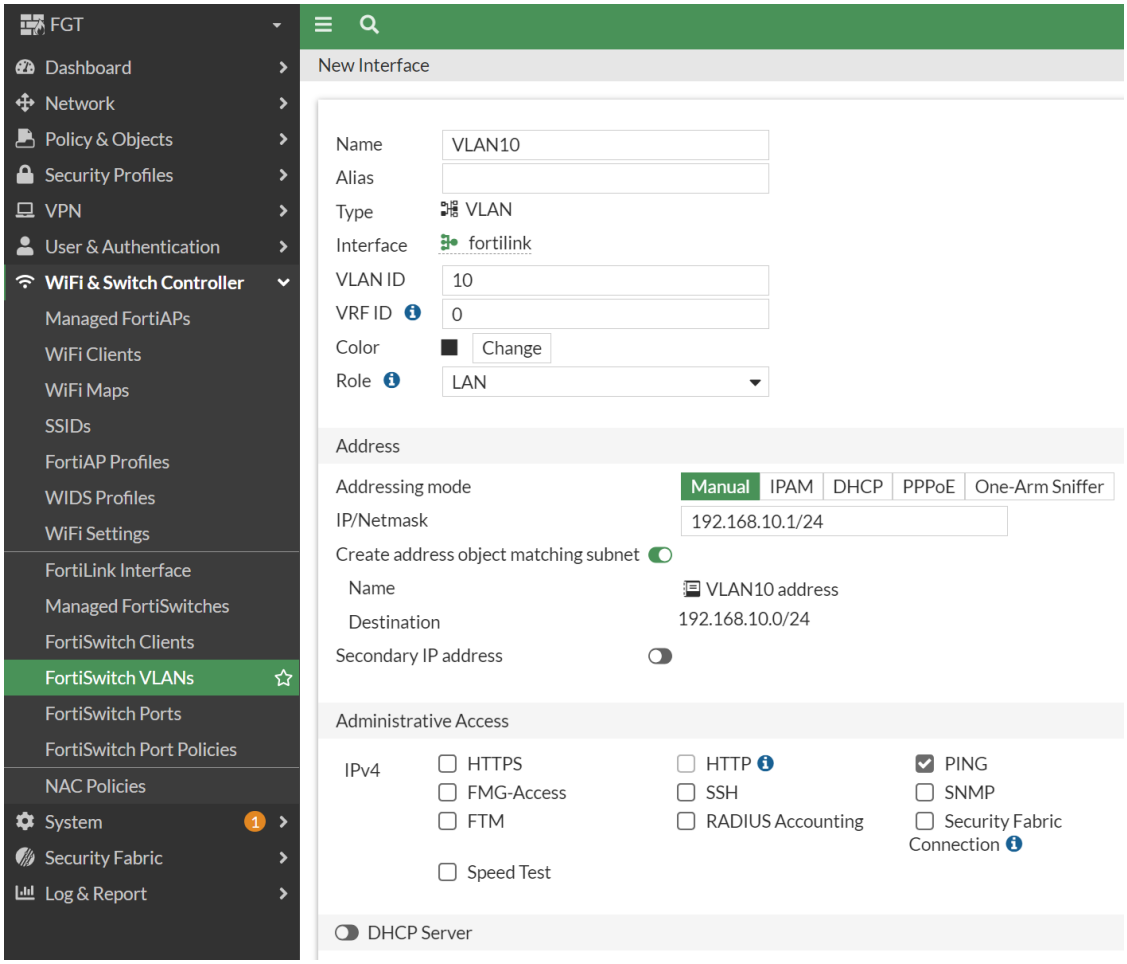
You can also configure MCLAG split-brain detection on the other MCLAG peer groups in this example.

Creating the VLAN interfaces on the FortiGate device

Create four FortiLink VLANs on the IP addresses listed in the table. These are the VLAN interfaces on the FortiGate device. In this example, the DHCP server is not enabled. However, you can use a DHCP server if you specify the appropriate default gateways for each VLAN.

VLAN name	IP address
VLAN10 (database servers)	192.168.10.1
VLAN20 (application servers)	192.168.20.1
VLAN30 (web servers)	192.168.30.1
VLAN40 (hosts of on-site users)	192.168.40.1

For example, to configure VLAN10:

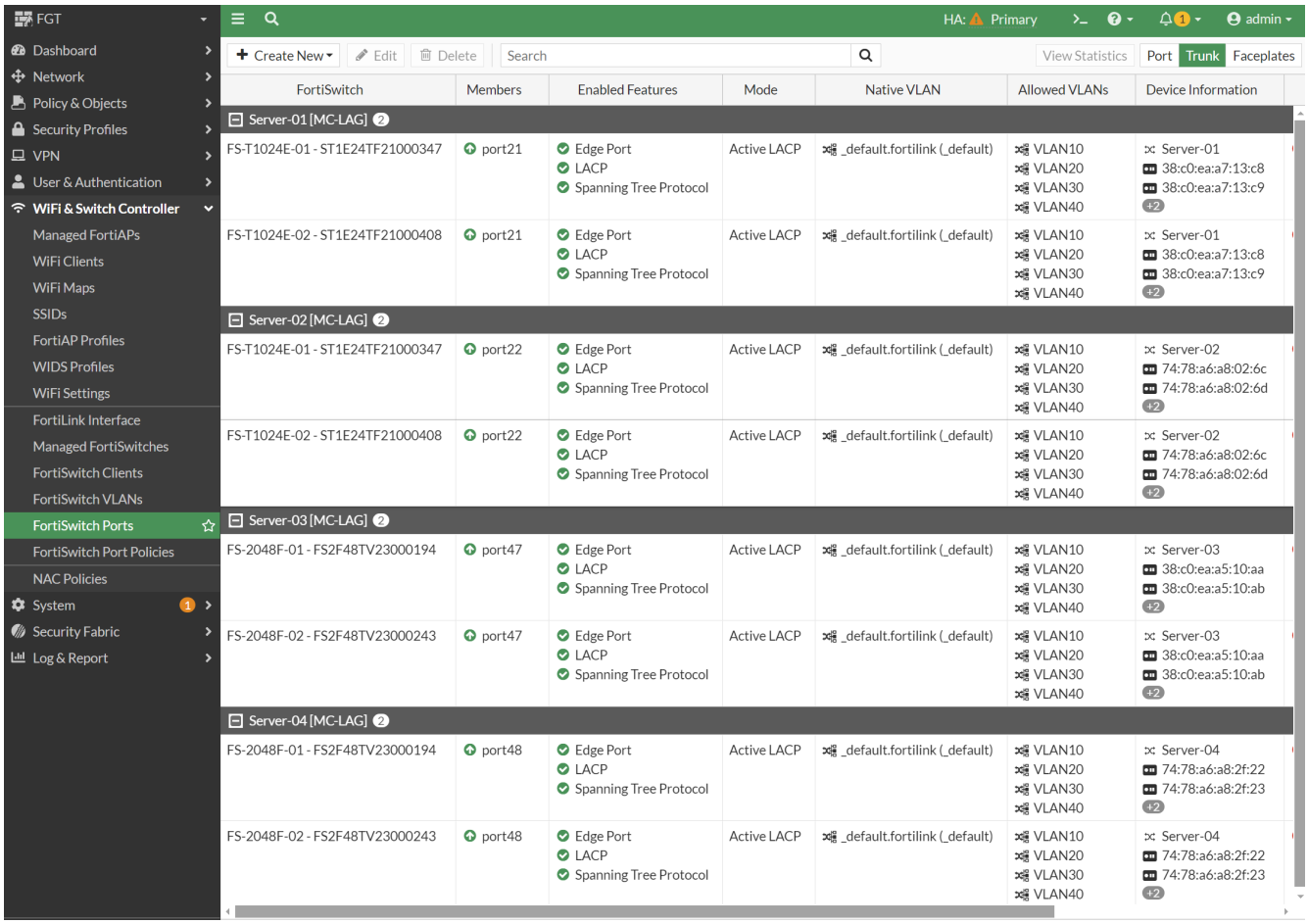


Connecting the servers

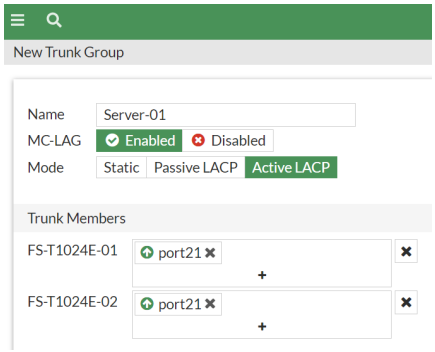
In the example topology, there are four servers:

- Server-01 and Server-02 are dual-homed (dual-connected) to the FS-T1024E-01 and FS-T1024E-02 switches by 10GBASE-T.
- Server-03 and Server-04 are dual-homed to the FS-2048F-01 and FS-2048F-02 switches by 25GBASE-CR (25GE direct-attach cable).

All four servers are configured as trunks (MC-LAG with network interface card teaming or network interface card bonding) with LACP enabled; they are connected to a FortiSwitch trunk with `set mode lacp-active` configured. Without (static) LACP, each server can also be connected to a trunk of FortiSwitch units configured with the `set lacp-mode static` command. See the following figure.



As shown in the following figure, you can use the FortiGate GUI to configure the LACP mode on each FortiSwitch trunk.



You also need to configure which VLANs are “Allowed VLANs” for each server. On the server side, you need to make sure the corresponding VLANs are allowed with 802.1Q tags, too.

Configuring the routing offload

Routing offload is supported on the tier-1 FortiSwitch units and can be configured with the FortiGate CLI in FortiOS 7.4.3 with FortiSwitchOS 7.4.3. For more details about routing offload, refer to Configuring inter-VLAN routing offload. To see

which FortiSwitch models support routing offload, refer to the FortiSwitchOS Feature Matrix.

To configure the routing offload, you must have an advanced features license on the tier-1 switches (the two FS-3032E switches in the example topology). For more information about using the advanced feature license, see Downloading a license file.

You need to use the FortiGate CLI to configure the routing offload for the two FS-3032E switches. After you have used the CLI to configure the FortiGate device, the FortiGate device automatically generates the required configuration, including virtual routing and forwarding (VRF) and the Virtual Router Redundancy Protocol (VRRP). VRRP is enabled when an MCLAG is configured for routing offload. Then the FortiGate device pushes the routing offload configuration to the two FS-3032E units over FortiLink.

In the example topology, both VLAN10 and VLAN20 are trusted VLANs for routing offload. VLAN30 and VLAN40 are regular VLANs. So, the traffic between VLAN10 and VLAN20 are forwarded by the FortiSwitch unit, instead of the FortiGate device. Because the traffic between VLAN10 and VLAN20 does not go through the FortiGate device, the FortiGate device does not enforce any security policies.

The following table summarizes the assigned IP addresses on the FortiGate and FortiSwitch devices for each VLAN.

VLAN name	FortiGate VLAN interface	VRRP virtual IP address	Router IP address (SVI) on FS-3032E-01	Router IP address (SVI) on FS-3032E-02
VLAN10 (database servers)	192.168.10.1 **(do not use as a default gateway)**	192.168.10.2 **(default gateway)**	192.168.10.3	192.168.10.4
VLAN20 (application servers)	192.168.20.1 **(do not use as a default gateway)**	192.168.20.2 **(default gateway)**	192.168.20.3	192.168.20.4
VLAN30 (web servers)	192.168.30.1 **(default gateway)**	Not applicable	Not applicable	Not applicable
VLAN40 (hosts of on-site users)	192.168.40.1 **(default gateway)**	Not applicable	Not applicable	Not applicable

On each trusted VLAN, there are four routers:

- FortiGate VLAN interface
- VRRP virtual IP address (`switch-controller-offload-ip`)
- The router IP (`router-ip`) address for FS-3032E-01
- The router IP (`router-ip`) address for FS-3032E-02

The `switch-controller-offload-ip` value is used as the VRRP virtual IP address shared by FS-3032E-01 and FS-3032E-02. All hosts in the trusted VLANs should use the `switch-controller-offload-ip` address as the default gateway. If the host in the trusted VLAN uses the FortiGate VLAN interface as the default gateway, the host cannot communicate with other VLANs as expected.

To configure the routing offload:

1. Use the FortiGate CLI to specify the trusted VLANs:

```
FGT # config system interface
FGT (interface) # edit VLAN10
FGT (VLAN10) # set switch-controller-offload enable
```

```
FGT (VLAN10) # set switch-controller-offload-ip 192.168.10.2
FGT (VLAN10) # set switch-controller-offload-gw enable
FGT (VLAN10) # next
FGT (interface) # edit VLAN20
FGT (VLAN20) # set switch-controller-offload enable
FGT (VLAN20) # set switch-controller-offload-ip 192.168.20.2
FGT (VLAN20) # end
```

Configure `set switch-controller-offload-gw enable` on **one** trusted VLAN (a VLAN with `set switch-controller-offload enable` configured).

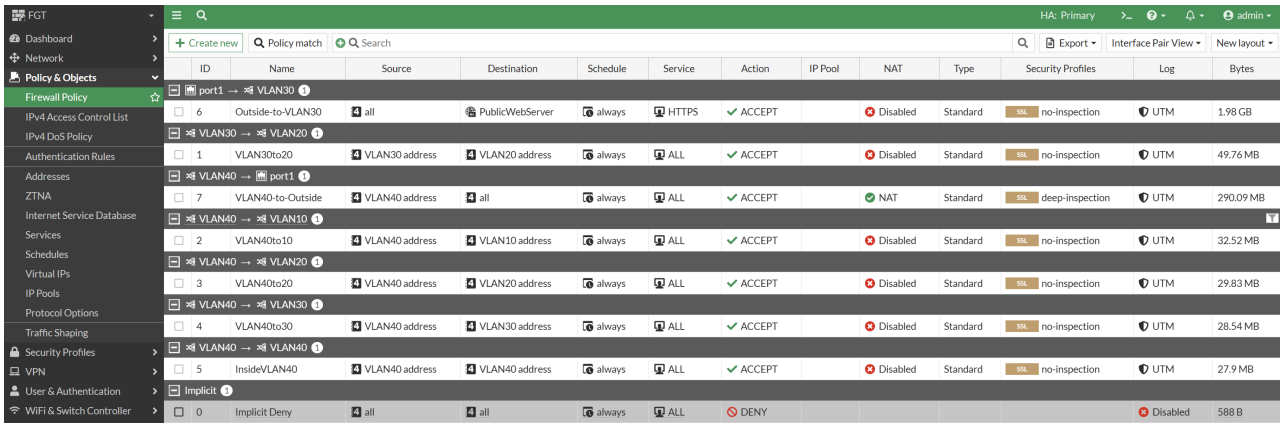
2. Enable and configure routing offload on the tier-1 FortiSwitch units:

```
FGT # config switch-controller managed-switch
FGT (managed-switch) # edit FS-3032E-01
FGT (FS-3032E-01) # set route-offload enable
FGT (FS-3032E-01) # set route-offload-mclag enable
FGT (FS-3032E-01) # config route-offload-router
FGT (route-offload-router) # edit VLAN10
new entry 'VLAN10' added
FGT (VLAN10) # set router-ip 192.168.10.3
FGT (VLAN10) # next
FGT (route-offload-router) # edit VLAN20
new entry 'VLAN20' added
FGT (VLAN20) # set router-ip 192.168.20.3
FGT (VLAN20) # next
FGT (route-offload-router) # end
FGT (FS-3032E-01) # next
FGT (managed-switch) # edit FS-3032E-02
FGT (FS-3032E-02) # set route-offload enable
FGT (FS-3032E-02) # set route-offload-mclag enable
FGT (FS-3032E-02) # config route-offload-router
FGT (route-offload-router) # edit VLAN10
new entry 'VLAN10' added
FGT (VLAN10) # set router-ip 192.168.10.4
FGT (VLAN10) # next
FGT (route-offload-router) # edit VLAN20
new entry 'VLAN20' added
FGT (VLAN20) # set router-ip 192.168.20.4
FGT (VLAN20) # next
FGT (route-offload-router) # end
FGT (FS-3032E-02) # end
```

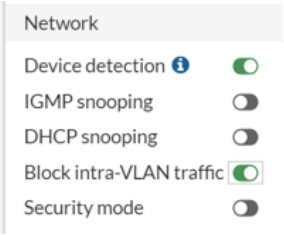
Configuring the firewall policies and blocking intra-VLAN traffic

To configure the firewall policies and block intra-VLAN traffic:

1. Use the table in Requirements and design overview on page 6 to configure the firewall policies.
   Because routing offload is enabled on VLAN10 and VLAN20, no policy is required between these two VLANs.



2. In the FortiGate GUI, enable *Block Intra-VLAN traffic* on VLAN40.



3. After you enable *Block Intra-VLAN traffic* in the example topology, packets sent from the hosts in VLAN40 are received by the VLAN40 interface of the FortiGate device and forwarded back to same interface. You need to use the FortiGate CLI to prevent traffic with the same local ingress and egress interface from being forwarded without a policy check:

```
FGT # config system global
FGT (global) # set allow-traffic-redirect disable
FGT (global) # end
```

4. In the FortiGate CLI, configure the proxy ARP.

```
FGT # config system proxy-arp
FGT (proxy-arp) # edit 1
FGT (1) # set interface VLAN40
FGT (1) # set ip 192.168.40.5
FGT (1) # set end-ip 192.168.40.254
FGT (1) # next
FGT (proxy-arp) # end
```

Verifying the end-to-end communication

In the example topology, end-to-end communication is allowed or denied by firewall policies, routing offload, and blocking Intra-VLAN traffic, as described in the following table.

Source\Destination	To VLAN10	To VLAN20	To VLAN30	To VLAN40	To the internet
From VLAN10 (database servers)	Allowed and forwarded by the FortiSwitch unit	Allowed and forwarded by routing offload	Denied by the FortiGate device	Inspected by the FortiGate device (return traffic only)	Denied by the FortiGate device
From VLAN20 (application servers)	Allowed and forwarded by routing offload	Allowed and forwarded by the FortiSwitch unit	Inspected by the FortiGate device (return traffic only)	Inspected by the FortiGate device (return traffic only)	Denied by the FortiGate device
From VLAN30 (web servers)	Denied by the FortiGate device	Inspected by the FortiGate device	Allowed and forwarded by the FortiSwitch unit	Inspected by the FortiGate device (return traffic only)	Inspected by the FortiGate device (return traffic only)
From VLAN40 (hosts of on-site users)	Inspected by the FortiGate device	Inspected by the FortiGate device	Inspected by the FortiGate device	Inspected by the FortiGate device (*Block Intra-VLAN traffic*)	Inspected by the FortiGate device
From the internet	Denied by the FortiGate device	Denied by the FortiGate device	Inspected by the FortiGate device	Denied by the FortiGate device	Not applicable

By adding more policies, external users, such as developers and operators, can remotely access the application and database servers through the internet securely.

You can use the FortiSwitch CLI to see how many bytes and packets are forwarded by routing offload:

```
FS-3032E-01 # get system interface vlan
== [vlan]
   ==[VLAN10]
      mode: static
      ip: 192.168.10.3 255.255.255.0
      ipv6: ::/0
      status: up
      rx : 8645334 bytes 135060 packets
      tx : 219756 bytes 3619 packets
   ==[VLAN20]
      mode: static
      ip: 192.168.20.3 255.255.255.0
      ipv6: ::/0
      status: up
      rx : 3981018 bytes 82492 packets
      tx : 58398 bytes 788 packets
   ==[rspan]
      mode: dhcp
      ip: 0.0.0.0 0.0.0.0
      ipv6: ::/0
```

```
      status: down
      rx : 0 bytes 0 packets
      tx : 0 bytes 0 packets

FS-3032E-02 # get system interface vlan
== [vlan]
   ==[VLAN10]
      mode: static
      ip: 192.168.10.4 255.255.255.0
      ipv6: ::/0
      status: up
      rx : 7406348 bytes 120410 packets
      tx : 2138298 bytes 42158 packets
   ==[VLAN20]
      mode: static
      ip: 192.168.20.4 255.255.255.0
      ipv6: ::/0
      status: up
      rx : 4269690 bytes 91093 packets
      tx : 1603758 bytes 29592 packets
   ==[rspan]
      mode: dhcp
      ip: 0.0.0.0 0.0.0.0
      ipv6: ::/0
      status: down
      rx : 0 bytes 0 packets
      tx : 0 bytes 0 packets
```

Appendix A: Products used in this guide

This architecture guide also applies to later versions of the products listed in the table.

The following product models and firmware were used in the topology example:

Product	Model	Firmware
FortiGate	FG-2600F	7.4.3
FortiSwitch	FS-3032E	7.4.3
FortiSwitch	FS-2048F	7.4.3
FortiSwitch	FS-1024E	7.4.3
FortiSwitch	FS-T1024E	7.4.3
FortiSwitch	FS-524D	7.4.3
FortiSwitch	FS-248E-POE	7.4.3

Appendix B: Documentation references

For more information, use the following resources:

- Administration guides
  - FortiOS Administration Guide
  - FortiLink Guide
  - FortiSwitchOS Administration Guide
- Solutions hub
  - Secure Access

www.fortinet.com

Copyright© 2024 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 Chief Legal Officer, 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.