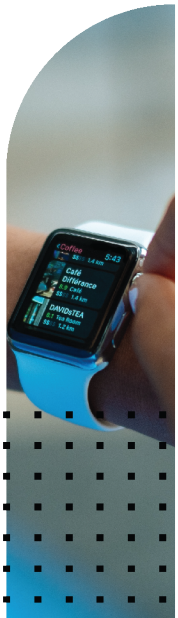
FortiLink over Multi-vendor Networks Using VXLAN Deployment Guide

FortiOS and FortiSwitchOS 7.2.2



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

May 17, 2023
FortiOS and FortiSwitchOS 7.2.2 FortiLink over Multi-vendor Networks Using VXLAN Deployment Guide
11-722-800776-20230517

TABLE OF CONTENTS

Change log

Date	Change Description
October 24, 2022	Initial release
December 2, 2022	Updated the “Configure the FortiSwitch unit for FortiLink over VXLAN” and “Configure the FortiGate device for FortiLink over VXLAN” sections.
May 17, 2023	Updated the note in the “Example 1: Basic FortiLink-over-VXLAN setup” section.

Introduction

Executive summary

Virtual eXtensible LAN (VXLAN) can be used to create a layer-2 overlay network when managing FortiSwitch units over a layer-3 network. The FortiGate device can use the VXLAN to manage multiple FortiSwitch units. If the FortiSwitch unit being managed supports hardware-based VXLAN, the FortiSwitch unit can also forward FortiSwitch VLANs (user traffic) to a FortiGate device over VXLAN. *This document is focused on FortiSwitch models that support hardware-based VXLAN.*

Intended audience

This guide is intended for an audience who is interested in deploying Fortinet's Secure Access Solution in a new environment or replacing their equipment in an existing environment. Readers are expected to have a firm understanding of networking, wireless, and security concepts. Interested audiences might include the following:

- Network, wireless, and security architects
- Network, wireless, and security engineers

About this guide

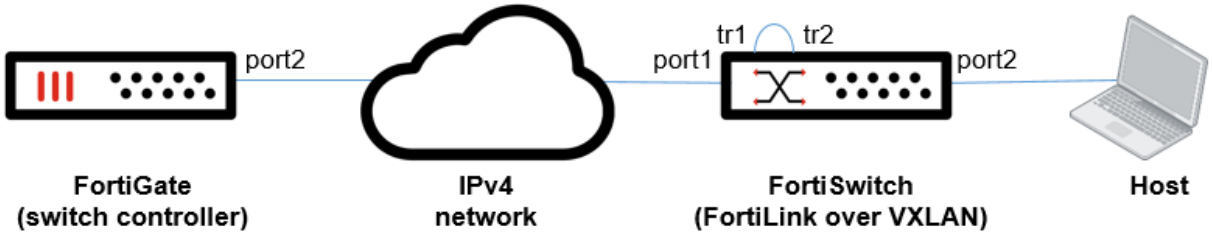
The deployment guide provides the design and deployment steps involved in deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture and design outlined in this guide is suitable for them. It is advisable to review the administration guide 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 the product administration guides, Knowledge Base articles, cookbooks, release notes, and other documents where appropriate.

Design overview

Use case and topology

The following figure shows the minimum topology of FortiLink over VXLAN using an IPv4 network.

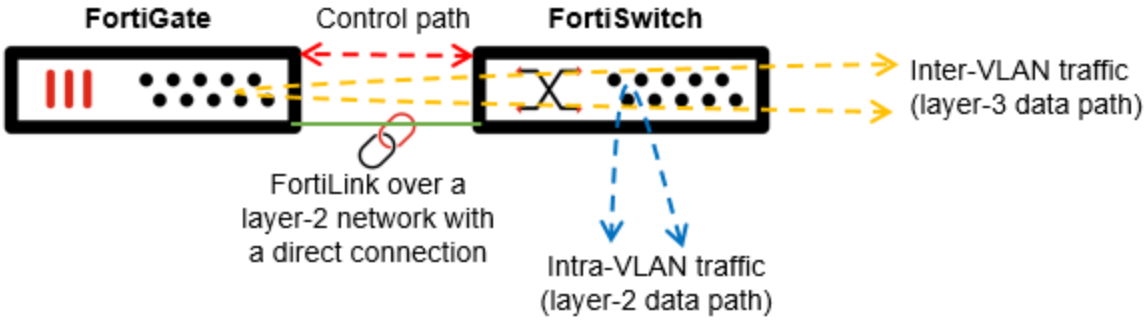


Design concept and considerations

There are three methods to use FortiLink to manage FortiSwitch units:

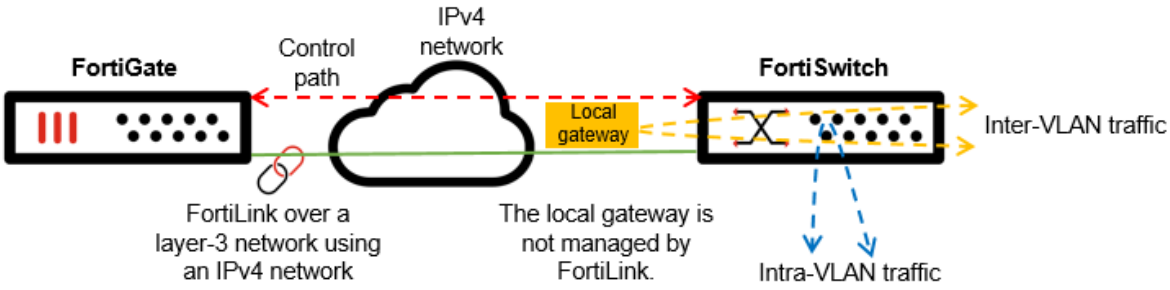
- FortiLink over a layer-2 network

  This method requires a direct connection between the FortiSwitch unit and FortiGate device. In this document, a *control path* is where a FortiGate device sends and receives packets to manage a FortiSwitch unit. A *data path* is where data packets are being forwarded and transmitted between a FortiSwitch unit and a FortiGate device. As the FortiGate device and FortiSwitch unit are directly connected, the control path goes through this direct connection. For the data path, the FortiSwitch unit forwards data packets within a VLAN (layer-2 data path); the FortiGate device forwards data packets between different VLANs (layer-3 data path). All FortiSwitch models support this method.



- FortiLink over a layer-3 network

  This method connects the FortiSwitch unit and FortiGate device through any IPv4 network (and IPv6 networks in a future release). The IPv4 network can be built with third-party devices. In this method, the control path is established over the IPv4 network. Unlike using FortiLink over a layer-2 network, the FortiGate device does not automatically use the FortiSwitch unit to handle the data path. This means that the *local gateway* in the following figure will handle inter-VLAN traffic, but the local gateway is not managed by FortiLink. All FortiSwitch models support this method.

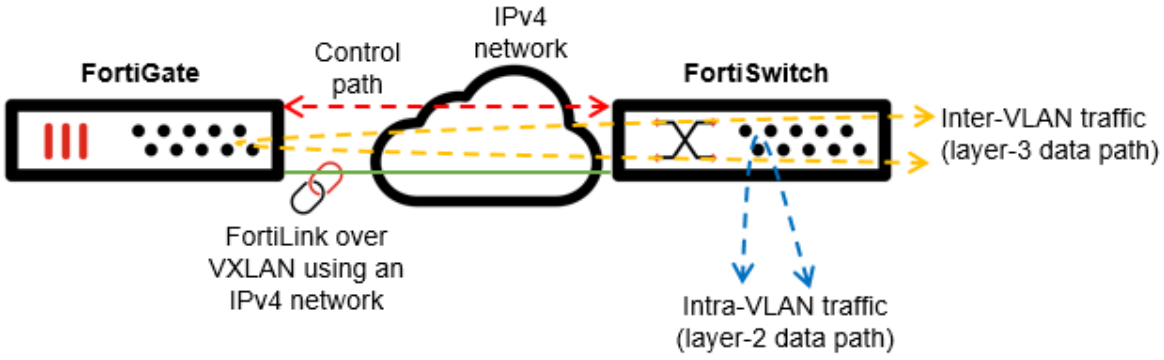


- FortiLink over VXLAN

  This method connects the FortiSwitch unit and FortiGate device through any IPv4 network with an MTU overhead of 50 bytes. The FortiSwitch unit forwards FortiSwitch VLANs (user traffic) using VXLAN to the FortiGate device to route traffic based on firewall policies. Refer to the Feature Matrix for details about which FortiSwitch models support VXLAN.

  Both the control path and data path are VXLAN encapsulated. So FortiLink over VXLAN is logically equivalent to FortiLink over layer 2 when the FortiSwitch unit supports a hardware-based VXLAN.

  The VXLAN tunnel is statically configured and established (that is, no EVPN).



Requirements

The following are required for FortiLink over VXLAN:

- MTU

  At least 1,550 bytes of MTU are required, if the MTU of the overlay network is 1,500 bytes. Because the FortiSwitch unit does not support fragmentation or re-assembly, you need to adjust the MTU to avoid fragmentation.

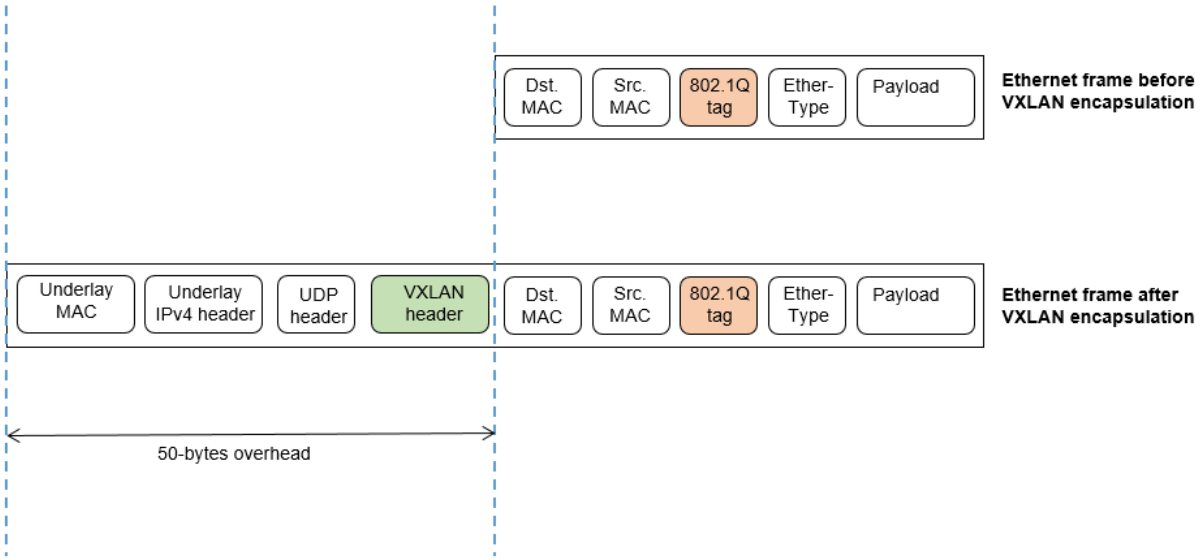
- Multicast

  Hardware-based VXLAN on the FortiSwitch unit supports BUM (Broadcast, Unknown Unicast, and Multicast) replication, so you do not have to run multicast routing on the underlay network.

- Routing
  Static routing was used in the deployment described in this document, but dynamic routing is also supported.
- NAT
  Virtual IP (VIP) network address translation (NAT) can be used along with FortiLink over VXLAN.
- IPsec
  IPsec can be used along with FortiLink over VXLAN.
- To forward FortiSwitch VLANs over VXLAN by hardware, a physical loopback cable and the corresponding configuration are required.

VLAN-to-VNI mapping

The 802.1Q tag (4 bytes) contains the VLAN ID, which is 12 bits long. The VXLAN header (8 bytes) contains the VXLAN network identifier (VNI), which is 24 bits long. When both a FortiSwitch unit and a FortiGate device add a VXLAN header on FortiLink over VXLAN, one VNI value is used in most cases, and the original VLAN ID in the 802.1Q tag is retained.



Deployment procedures

This section covers the following deployment examples:

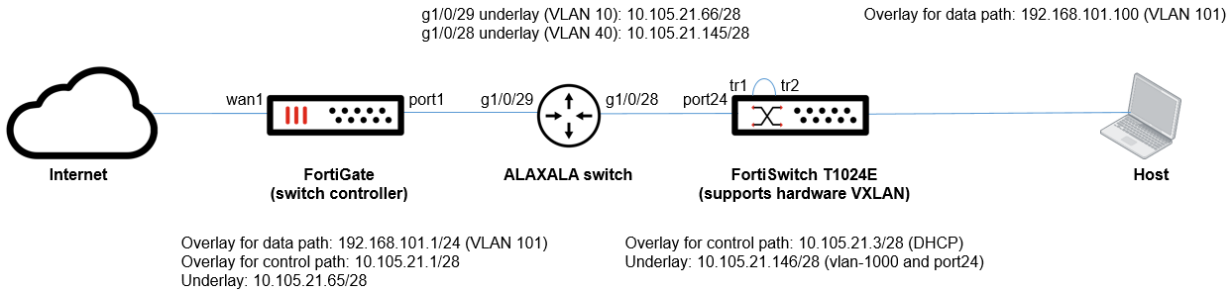
Example 1: Basic FortiLink-over-VXLAN setup

The following example is a FortiLink-over-VXLAN setup. In this example, the ALAXALA switch is used as a router between the FortiGate device and the FortiSwitch unit. All packets of the control path and data path are VXLAN encapsulated and go through the ALAXALA switch.

NOTE: If you do not have an ALAXALA switch (available only in Japan at this point), any layer-3 switch or router can be used if the requirements are met.

At this point, you need to use the CLI for most of the configuration of FortiLink over VXLAN on both the FortiSwitch unit and FortiGate device. In addition, the ALAXALA switch just supports CLI configuration.

After the VXLAN tunnel is established between the FortiGate device and the FortiSwitch unit, the FortiSwitch unit will be discovered by the FortiGate device, just like in a FortiLink-over-layer-2 network. After you have authorized the FortiSwitch unit, you can manage the FortiSwitch unit over VXLAN. For example, you can configure FortiSwitch VLANs using the GUI.



For more information, refer to Managing FortiSwitch units on VXLAN interfaces as well.

Configure the FortiSwitch unit for FortiLink over VXLAN

The following example shows how to configure FortiLink over VXLAN on the FortiSwitch unit:

1. Configure a VLAN to use as the underlay for VXLAN.

```
config system interface
  edit "vlan-1000"
    set ip 10.105.21.146 255.255.255.240
```

```
      set allowaccess ping https ssh
      set vlanid 1000
      set interface "internal"
   next
end
```

2. Configure a static route to the underlay IPv4 address of the FortiGate device.

```
config router static
   edit 1
      set device "vlan-1000"
      set dst 10.105.21.65 255.255.255.255
      set gateway 10.105.21.145
   next
end
```

3. Configure the switch trunk to make it static and disable the automatic VLAN provisioning.

   NOTE: `port24` is connected to the ALAXALA switch as a router.

```
config switch trunk
     edit "vxlan-underlay"
        set auto-isl 1
        set static-isl enable
        set static-isl-auto-vlan disable
        set members "port24"
     next
end
```

4. Configure the underlay interface. The native VLAN matches the VLAN used for the underlay for the VXLAN defined in step 1 (Configure a VLAN to use as the underlay for VXLAN.).

```
config switch interface
   edit "vxlan-underlay"
      set native-vlan 1000
   next
end
```

5. Assign VLAN ID 4094 to the “internal” interface that will be used to establish the FortiLink connection with the FortiGate device over VXLAN.

```
config switch interface
   edit "internal"
      set native-vlan 4094
   next
end
```

6. To use a hardware-based VXLAN, you need to configure two trunks. They are `tr1` and `tr2` in this example. Each trunk is assigned one physical link, `port25` and `port26` in this example. They should be connected to each other by a physical loopback cable.

7. Create and configure trunk `tr1`.

```
config switch trunk
   edit "tr1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port25"
   next
end
```

8. Configure the `tr1` interface with a native VLAN of 4087 and disable STP.

```
config switch interface
   edit "tr1"
      set native-vlan 4087
```

```
      set stp-state disabled
   next
end
```

9. Create and configure trunk `tr2`. Leave the rest of the values at the defaults.

```
config switch trunk
   edit "tr2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port26"
   next
end
```

10. In the configuration for the `tr2` interface, the `set allowed-vlans 1-4094` command means that all VLANs are FortiSwitch VLANs and that they are VXLAN encapsulated and forwarded to the FortiGate device.

```
config switch interface
   edit "tr2"
      set native-vlan 4094
      set allowed-vlans 1-4094
   next
end
```

11. Configure the VXLAN interface with `tr1` as the tunnel-loopback interface.
    - The `vni` is used for VXLAN encapsulation.
    - The `remote-ip` points to the FortiGate device.

```
config system vxlan
   edit "vx-4094"
      set vni 123456
      set interface "vlan-1000"
      set tunnel-loopback "tr1"
      set remote-ip "10.105.21.65"
   next
end
```

Configure the FortiGate device for FortiLink over VXLAN

1. Configure the system interface connected to the ALAXALA switch, which is the router (gateway) toward the FortiSwitch unit.

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.105.21.65 255.255.255.240
      set allowaccess ping https ssh http
   next
end
```

2. Configure the VXLAN interface. The `vni` should be same value as on the FortiSwitch unit. The `remote-ip` points to the underlay IPv4 address of FortiSwitch unit.

```
config system vxlan
   edit "flk-vxlan"
      set interface "port1"
      set vni 123456
      set remote-ip "10.105.21.146"
   next
```

```
end
```

3. Enable FortiLink on the `vxlan` interface created in step 2 and set the IPv4 address. The underlined commands are automatically configured.

```
config system interface
   edit "flk-vxlan"
      set vdom "root"
      set fortilink enable
      set ip 10.105.21.1 255.255.255.240
      set allowaccess ping fabric
      set type vxlan
      set lldp-reception enable
      set lldp-transmission enable
      set interface "port1"
   next
end
```

4. Configure a static route toward the FortiSwitch unit.

```
config router static
   edit 0
      set dst 10.105.21.128 255.255.255.192
      set gateway 10.105.21.66
      set device "port1"
   next
end
```

5. Configure the DHCP server to provide the switch-controller IPv4 address to the FortiSwitch unit. DNS and NTP services are provided by the FortiGate device.

```
config system dhcp server
   edit 0
      set dns-service local
      set ntp-service local
      set default-gateway 10.105.21.1
      set netmask 255.255.255.240
      set interface "flk-vxlan"
      config ip-range
         edit 1
            set start-ip 10.105.21.2
            set end-ip 10.105.21.14
         next
      end
      set vci-match enable
      set vci-string "FortiSwitch"
   next
end
```

Configure the ALAXALA switch as a router

The `gigabitethernet 1/0/29` is connected to the FortiGate device. The `gigabitethernet 1/0/28` is connected to the FortiSwitch unit managed by FortiLink over VXLAN.

```
system mtu 9216

interface gigabitethernet 1/0/28
   mtu 9216
   switchport mode access
   switchport access vlan 40
```

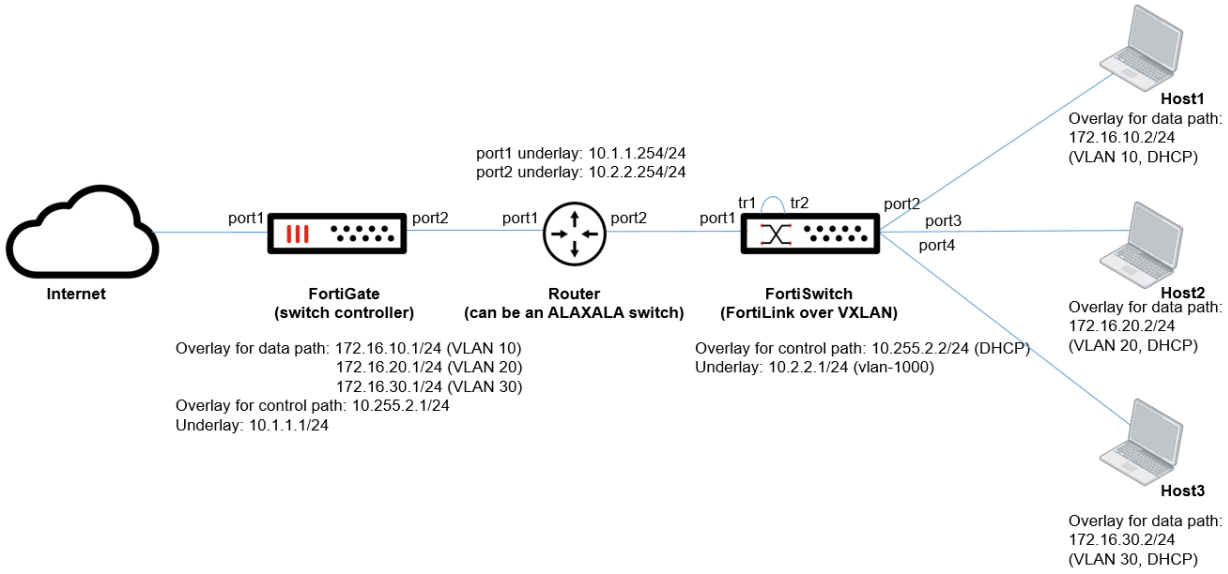
```
interface gigabitethernet 1/0/29
   mtu 9216
   switchport mode access
   switchport access vlan 10

interface vlan 40
   ip address 10.105.21.145 255.255.255.240
   ip mtu 9216

interface vlan 10
   ip address 10.105.21.66 255.255.255.240
   ip mtu 9216
```

Example 2: Add multiple VLANs to the deployment

Example 2 is a variant of Example 1. When you finish configuring the FortiSwitch unit, FortiGate device, and router, the VXLAN tunnel is established between the FortiSwitch unit and FortiGate device through the router., and then FortiLink over VXLAN becomes operational. After this point, you can configure this setup with the GUI just the same as FortiLink over layer 2. For example, after the FortiSwitch unit is managed by FortiLink over VXLAN from the FortiGate device, you can configure FortiSwitch VLANs with the GUI. No CLI configuration is required. After you add multiple FortiSwitch VLANs, the three hosts can communicate with each other through FortiLink over VXLAN and the FortiGate device. You need to configure policies on the FortiGate device to allow this traffic.



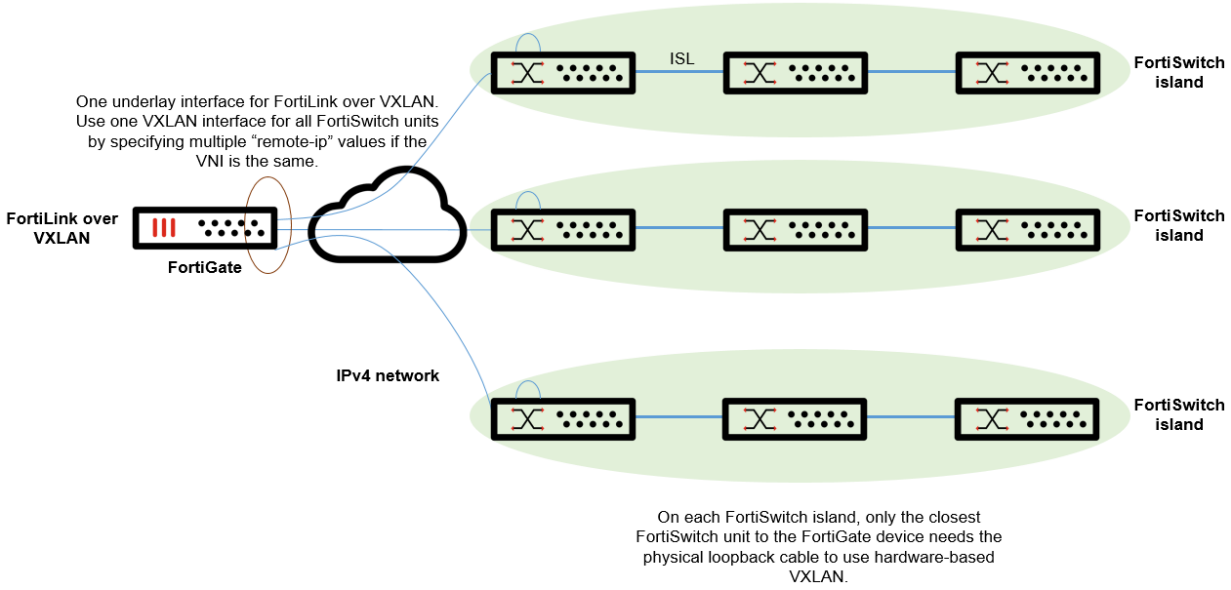
Example 3: Add multiple FortiSwitch units to the deployment

FortiLink over VXLAN supports up to 300 FortiSwitch units, depending on the FortiGate model.

There are two ways to add more FortiSwitch units to the deployment when using FortiLink over VXLAN.

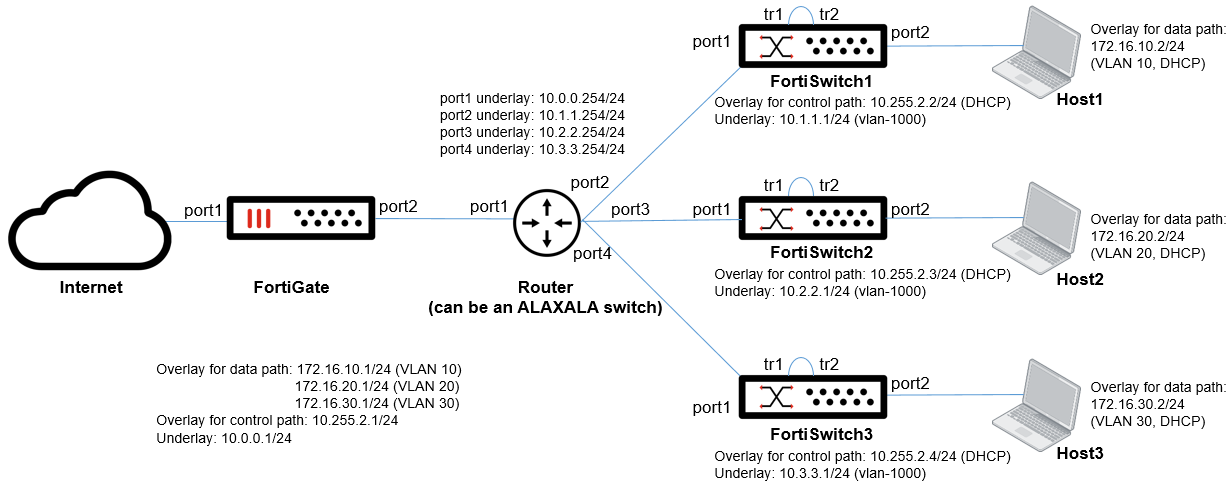
- Add more FortiSwitch islands (vertically). See Vertical scaling (adding FortiSwitch islands) on page 14.
- Add tier-2 members to FortiSwitch islands (horizontally). See Horizontal scaling (adding tier-2 members to a FortiSwitch island) on page 15.

The following figure shows three FortiSwitch islands. Each FortiSwitch island contains three members.



Vertical scaling (adding FortiSwitch islands)

The following figure shows how to deploy three FortiSwitch islands.



The three hosts can communicate with each other through FortiLink over VXLAN and the FortiGate device. The VLAN for a host connected to each island should be different from the other VLANs. In this example, VLAN 10, 20, and 30 are used on the three islands, so inter-VLAN (inter-island) communication can be routed by the FortiGate device. In other words, you cannot extend the same VLAN across islands. You need to configure policies on the FortiGate device to allow inter-VLAN traffic.

To configure the FortiGate device:

You have to configure three values for `remote-ip`, one each for FortiSwitch1, FortiSwitch2, and FortiSwitch3.

```
config system vxlan
   edit "flk-vxlan"
      set interface "port2"
      set vni 123456
      set remote-ip "10.1.1.1" "10.2.2.1" "10.3.3.1"
   next
end
```

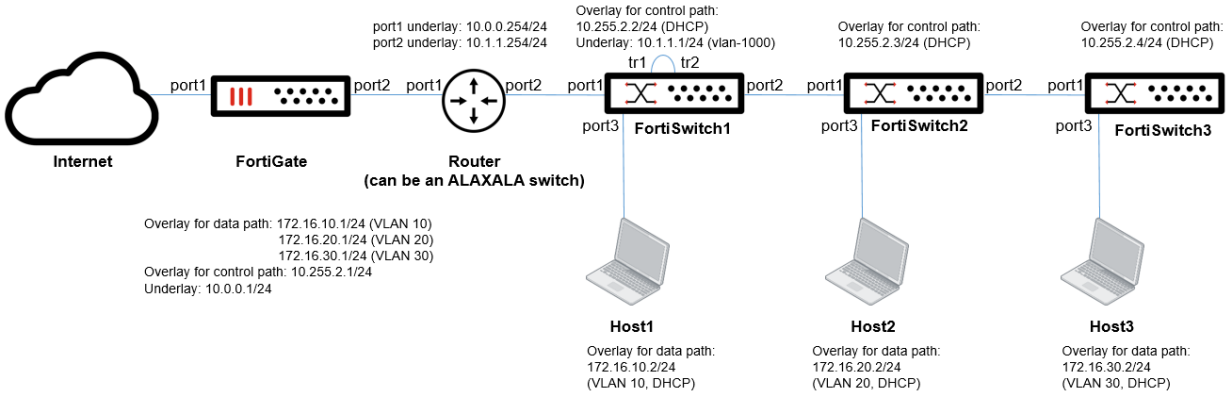
To configure FortiSwitch1, FortiSwitch2, and FortiSwitch3:

On FortiSwitch1, FortiSwitch2 and FortiSwitch3, the VNI value should be the same; however, you need to configure unique IPv4 addresses for the underlay (10.1.1.1, 10.2.2.1, and 10.3.3.1 in this example).

```
config system vxlan
   edit "vx-4094"
      set vni 123456
      set tunnel-loopback "tr1"
      set interface "vlan-1000"
      set remote-ip "10.0.0.1"
   next
end
```

Horizontal scaling (adding tier-2 members to a FortiSwitch island)

The following figure shows how to deploy a single FortiSwitch island with three members.



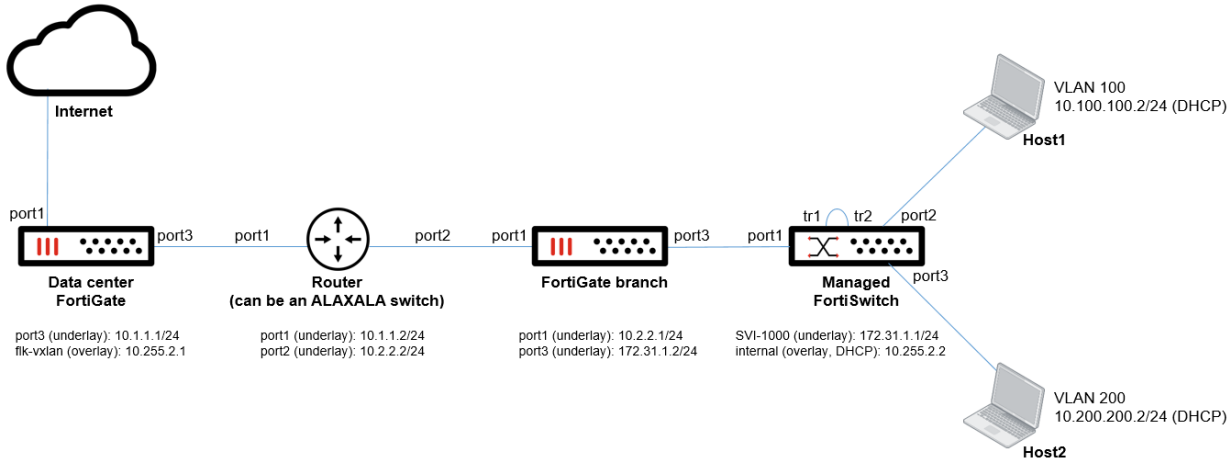
When you add FortiSwitch2 and FortiSwitch3, there is zero-touch configuration, just like a tier-2 FortiSwitch unit connected to a tier-1 FortiSwitch unit with FortiLink over a layer-2 network. Also, physical loopback cables are not required on FortiSwitch2 and FortiSwitch3 because they do not perform VXLAN encapsulation. FortiSwitch1 performs VXLAN encapsulation for packets from FortiSwitch2 and FortiSwitch3.

After you build the Example 1 setup, you only have to connect FortiSwitch2 and FortiSwitch3 and power them up. Then FortiSwitch2 and FortiSwitch3 are managed by FortiLink over VXLAN from the FortiGate device through FortiSwitch1, and you can configure FortiSwitch2 and FortiSwitch3 using the GUI.

In this example, when you configure VLAN 10, 20, and 30 with the GUI, the three hosts can communicate with each other through FortiLink over VXLAN and the FortiGate device. You need to configure policies on the FortiGate device to allow this traffic.

Example 4: Configure NAT with FortiLink over VXLAN

VIP NAT by the FortiGate device is supported along with FortiLink over VXLAN. In the following figure, NAT and port forwarding on the FortiGate branch are used to translate the source address from 172.3.1.1 to 10.2.2.99 when packets are sent out. From the FortiGate device, the VXLAN tunnel is established with 10.2.2.99, which is translated from 172.3.1.1. On the other hand, from the FortiSwitch unit, the VXLAN tunnel is established with 10.1.1.1.



To configure the FortiGate device:

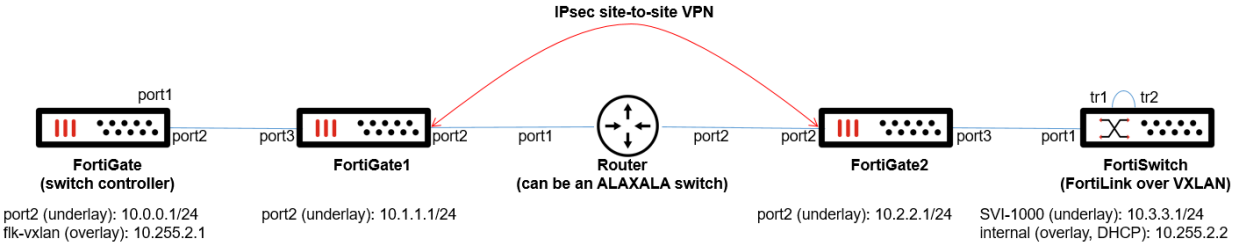
```
config system vxlan
   edit "flk-vxlan"
      set interface "port3"
      set vni 123456
      set remote-ip "10.2.2.99"
   next
end
```

To configure the managed FortiSwitch unit:

```
config system vxlan
   edit "vx-4094"
      set vni 123456
      set tunnel-loopback "tr1"
      set interface "vlan-1000"
      set remote-ip "10.1.1.1"
   next
end
```

Example 5: Configure IPsec with FortiLink over VXLAN

To encrypt both the control path and data path, you can use Internet Protocol Security (IPsec) along with FortiLink over VXLAN. The following figure shows a FortiLink-over-VXLAN deployment with an IPsec site-to-site VPN. For FortiLink over VXLAN, the IPsec site-to-site VPN is transparent. So the VXLAN configurations are the same whether IPsec is used or not.



To configure the FortiGate device:

```
config system vxlan
   edit "flk-vxlan"
      set interface "port2"
      set vni 123456
      set remote-ip "10.3.3.1"
   next
end
```

To configure the managed FortiSwitch unit:

```
config system vxlan
   edit "vx-4094"
      set vni 123456
      set tunnel-loopback "tr1"
      set interface "vlan-1000"
      set remote-ip "10.0.0.1"
   next
end
```

Appendix A: Products used in this guide

The following product models and firmware were used in the guide.

Product	Model	Firmware
FortiGate	FG-101E	7.2.2
FortiSwitch	FS-T1024E	7.2.2
ALAXALA switch	AX3660S-24S8XW	OS-L3M Ver. 12.1.Q.X

Appendix B: Documentation references

For more information, use the following resources:

- Product administration guides
  - FortiOS Administration Guide
  - FortiLink Administration Guide
  - ALAXALA product manuals
- Solution hub
  - Secure Access

www.fortinet.com