

Admin Guide

FortiExtender (Managed) 7.6.1



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



Dec 3, 2024

FortiExtender (Managed) 7.6.1 Admin Guide

TABLE OF CONTENTS

Change Log	5
Introduction	6
FortiOS and FortiExtender OS compatibility	7
Before you begin	8
Register with FortiCare	9
FortiExtender and FortiGate integration	11
FortiExtender monitoring overview	11
Provision FortiExtender firmware upon authorization	16
Connect to FortiGate	17
Wireless WAN extension to WAN interfaces of FortiGate	18
Wireless extension to internal LAN interface of FortiGate	18
Authorize FortiExtender on FortiOS	19
Enable FortiExtender Controller on FortiOS	20
Support for device password and allowed protocols for FortiExtender in FortiGate	20
FortiExtender as FortiGate LAN extension	22
Authorizing the devices	23
Backhaul tunnel and VXLAN auto-deployment	26
Configuring the LAN extension and firewall policy	29
Using the backhaul IP when the FortiGate access controller is behind NAT	31
Examples	31
Bandwidth limits on the FortiExtender Thin Edge	39
IPAM in FortiExtender LAN extension mode	40
FortiExtender LAN extension in public cloud FGT-VM	47
Allow FortiExtender to be managed and used in a non-root VDOM	54
GUI operating procedures	54
CLI operating procedures	58
Discover a FortiExtender unit	60
Broadcast	60
Static	60
De-authorize FortiExtender devices	62
The default FortiExtender profile	64
Allow access for FortiExtender management	67
Set bandwidth limit for LAN extension	68
Configure FortiExtender admin password	69
Discovery response lockdown	70
Wildcard	71
Data transportation over the LAN extension interface	73
LAN extension configuration in a profile	75
Backhaul IP in LAN extension	77
Fast failover of CAPWAP control channel between two uplinks	78
Topology	78

CLI	79
VLAN support for LAN-extension mode	82
Enable wireless configuration on FortiExtender	92
Dynamic Frequency Selection channels	93
Configure WiFi VAPs as members of switch interface	95
Configure split tunneling in LAN extension mode	97
FortiExtender as FortiGate WAN extension	100
FortiGate-FortiExtender zero-touch provisioning (ZTP)	100
VLAN mode	101
Set up FortiExtender as the WAN-extension of FortiGate using VLAN mode	101
Hitless failover in WAN-extension mode in HA configuration	105
Multiple APNs in WAN-Extension mode	107
Manage dual FortiExtender devices	109
Active/Passive mode	109
Active/Active mode	109
Cellular as backup of Ethernet WAN	109
SD-WAN	109
Configure cellular settings	111
Create a data plan	111
Set the default SIM	113
Enable SIM-switch	114
Configure SIM-switch based on link health	114
Report to FortiGate	116
VLAN mode	116
CAPWAP on multiple ports for broadcast discovery	118
CAPWAP mode	118
Check current manage mode	120
Get modem status	121
Stopping data traffic on overaged LTE interface	122
Access other devices via SSH	123
Use cases	124
Redundant with FGT in IP Pass-through mode	124
Enable DHCP server on FortiExtender and the VRRP primary router	126
Enable DHCP relay on both FortiExtender and the VRRP primary router	127
FortiExtender for FortiGate HA configuration	130
Example network topology	130
Prerequisites	130
Configuration procedures	131

Change Log

Date	Change Description
2024-12-03	Updated VLAN support for LAN-extension mode on page 82.
2024-11-25	Initial release.

Introduction

FortiExtender is a plug-and-play customer premises equipment (CPE) device. As a 3G/4G LTE and 5G wireless WAN extender, FortiExtender can provide a primary WAN link for retail POS, ATM, and kiosk systems, or a failover WAN link to your primary Internet connection to ensure business continuity. You can deploy it both indoors and outdoors by choosing the right model and appropriate enclosures.

FortiExtender can be deployed in standalone mode as a wireless router, managed individually or centrally from FortiEdge Cloud, or managed by FortiGate as part of the integrated Fortinet Fabric Solutions.

This *Guide* is for FortiExtender managed by FortiGate only. For information about standalone FortiExtender or FortiExtender managed by FortiEdge Cloud, refer to their respective Admin Guides.

FortiOS and FortiExtender OS compatibility

For more information about compatibility between versions of FortiOS and FortiExtender OS, see [FortiOS & FortiExtender OS Compatibility Matrix](#).

Before you begin

Before you start to configure your FortiGate-managed FortiExtender unit, ensure that you have completed the following:

- You have completed the installation of the FortiExtender unit, as outlined in the QuickStart Guide. (**Note:** You can power the FortiExtender unit using an external power adapter or by POE when connected to the POE/PSE port of the FortiGate.)
- You have administrative access to the FortiExtender GUI or CLI.
- You have installed the FortiGate unit on your network and have administrative access to the FortiGate GUI and CLI.

Register with FortiCare

After installing and authorizing your FortiExtender on FortiGate, you can register your FortiExtender to FortiCare. FortiCare enables you to manage security fabric devices such as FortiAP, FortiSwitch, and FortiExtender from a root FortiGate device. Once your FortiExtender is registered with FortiCare, you gain access to more streamlined ticket reporting and tracking services. You can also download historic and recent modem firmware and device images from FortiCare.

There are two ways to add FortiExtenders to FortiCare:

- Through the FortiGate CLI: The FortiExtender must have an active connection to the FortiGate
- Through the [FortiCloud portal](#): For more information about registering through FortiCloud, refer to the [FortiCloud Services documentation](#).

To register a FortiExtender to FortiCare via FortiGate - CLI

1. Ensure that you meet the following requirements:

- Your FortiGate is registered with FortiCare and able to access FortiCare
- The FortiGate is up-to-date with the latest FortiOS release.
- The FortiExtender is connected to and managed by FortiGate, either as LAN extension or WAN extension.
- The FortiExtender is not already registered with FortiCare on any account.

2. From the FortiGate CLI, enter the following command:

```
# diag forticare direct-registration product-registration
```

To view available CLI options, enter `-help`.

Example:



```
# diag forticare direct-registration product-registration -help
Options: a:A:y:C:c:T:eF:f:hI:i:l:O:o:p:P:z:R:r:S:s:t:v:N:G
        --<long>                                -<short>
        account_id                             a:
        address                                A:
        city                                   y:
        company                                C:
        ...
```

3. Example registration:

```
# diag forticare direct-registration product-registration -a user@example.com -p
fortinet123!A -N FXA21FTQ22000012 -T "CA" -R "other" -e 1
```

Account info:

```
contract_number=[] account_id=[user@example.com] password=[***]
reseller_id=0 reseller=[other]
isGovernment=0
first_name=[] last_name=[] company=[]
title=[] address=[] city=[]
state=[] state_code=[] country_code=0
post_code=[] phone=[] fax=[]
```

```
industry=[] industry_id=0 orgsize=[] orgsize_id=0
version=0 SN=[FXA21FTQ22000012] existing=1
Prepare to register product into this account.
Do you want to continue? (y/n)y

Registration successful
```

FortiExtender and FortiGate integration

FortiExtender and FortiGate integration is used for following purposes:

- [FortiExtender as FortiGate LAN extension on page 22](#)
- [FortiExtender as FortiGate WAN extension on page 100](#)

The number of FortiExtender devices that can be used in FortiExtender as FortiGate LAN/WAN extension varies, depending on the FortiGate platform you chose. The following table highlights the maximum numbers of FortiExtenders that FortiGate platforms can support in such configurations.

Maximum number of FortiExtenders supported by FortiGate (FortiOS 7.4.0 and later)

FortiGate models	Maximum number of FortiExtender Devices Supported	
	WAN extension	LAN extension
FortiGate 40F, 60E & their variants; FortiGate VM01	2	0
FortiGate 60F, 70F, 80E, 80F, 90E and their variants, and FortiGate VM02	2	4
FortiGate 100E to 900G and their variants, and FortiGate VM04	2	8
FortiGate 1000D to 2600F and their variants, and FortiGate VM08	2	16
FortiGate 3000D and above, and FortiGate VM16 and above	2	32

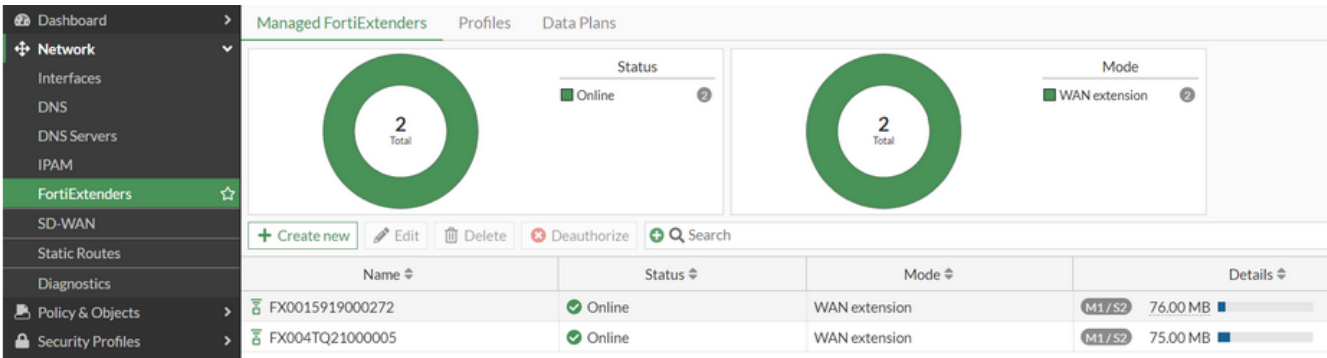
FortiExtender monitoring overview

The *Managed FortiExtenders* tab on the *Network > FortiExtenders* page contains the following monitoring features:

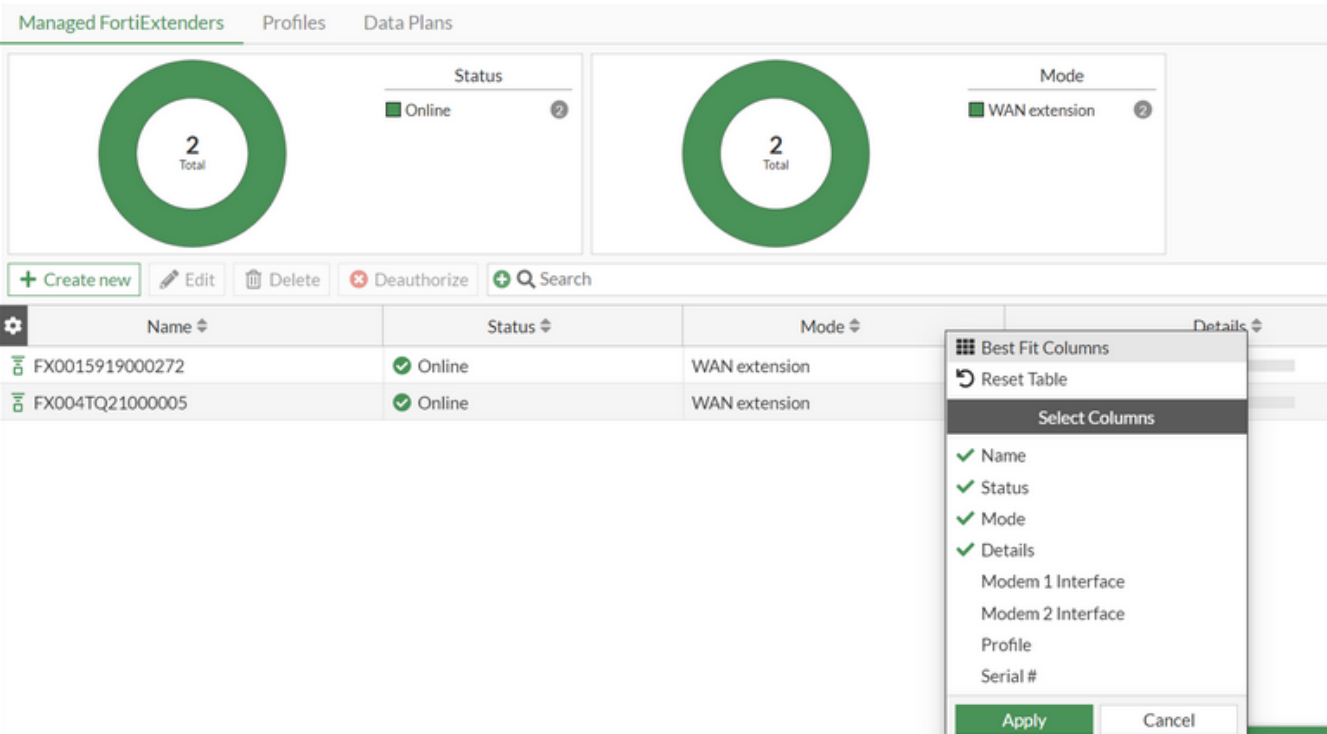
- Profile tab on the *Network > FortiExtenders* page has two charts: Status and Mode.
- Status column with Online, Offline, Waiting For Authorization states.
- A default Details column filled with the data used by the modem/SIM card when FortiExtender is in WAN-extension mode, or filled with the connected IPsec tunnel used with the FortiGate when FortiExtender is in LAN-extension mode.
- When FortiExtender is in WAN-extension mode, you can view modem information by left-clicking or hovering the mouse over the FortiExtender name to show a tooltip, and then clicking "Diagnostics and Tools".
- An optional "Serial #" column.

FortiExtender default page and option selection

By default, the page shows the name of each FortiExtender, but Serial number is not in default display.



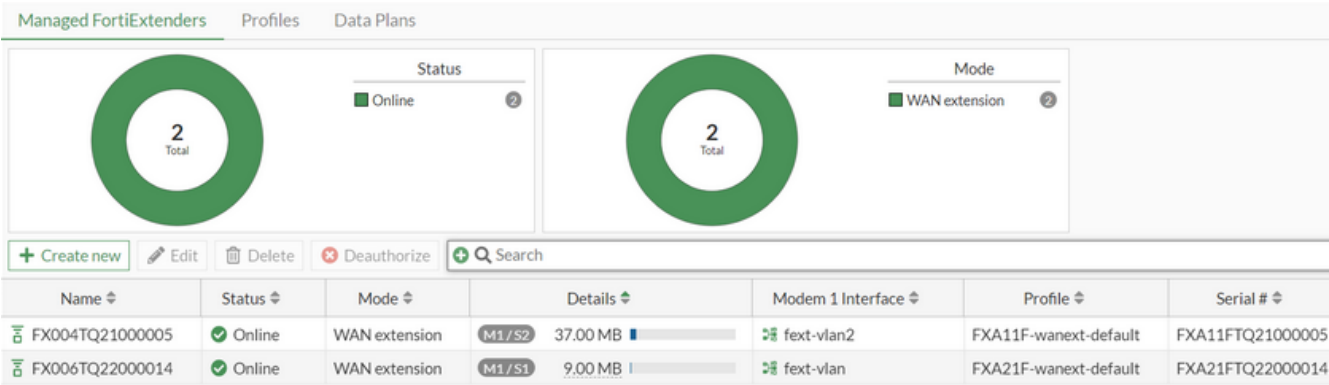
You can click in the default column to view more options and add more columns, such as "Serial #".



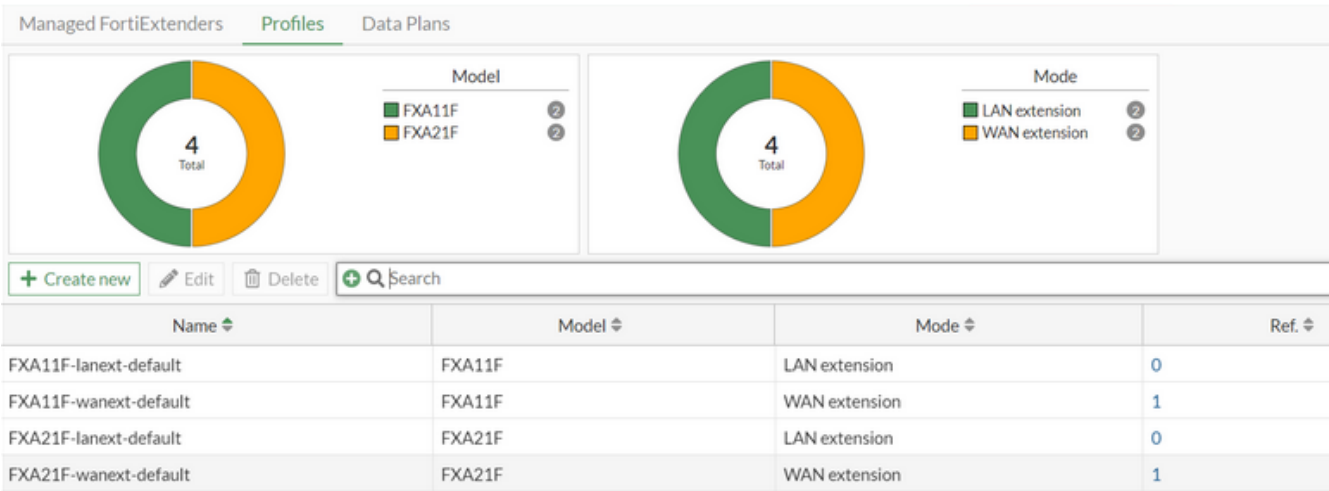
FortiGate GUI monitoring page when FortiExtender is authorized in wan-extension mode



- The "Modem 1 Interface #" column shows the FortiGate virtual interface which is built on the FortiExtender. This is the FortiGate WAN interface which extends to the FortiExtender LTE-modem.
- The "Details" column shows the data used on Modem1 / SIM1 in FXA21FTQ22000014.



FortiGate GUI provides the profiles used for each FortiExtender



FortiGate GUI provides profile settings for wan-extension



- "Default SIM" defines which SIM card starts to work first.
- SIM switch can be enabled by data plan. Assuming SIM1 uses Bell card. When its usage has reached the data limit in the plan, SIM2 (using Telus card) will be engaged to for service.

FortiGate GUI provides detailed FortiExtender diagnostics pages



You can left-click the name of an FortiExtender or hover the mouse over the name to get the tooltip, as shown in the following image.

1. Click the name of a FortiExtender to get the following page.

Name	Status	Mode	Details	Modem 1 Interface	Profile	Serial #
FX0015919000272	Online	WAN extension	76.00 MB	fext-201	FX201E-wanext-default	FX201E5919000272
FX004TQ21000005	Online	WAN extension	75.00 MB	fext-101	FXA11F-wanext-default	FXA11FTQ21000005

- Click "Diagnostics and Tools" to open the Diagnostics and Tools page.

The screenshot shows the 'Diagnostics and Tools' page for a specific FortiExtender (FX004TQ21000005). The page is divided into several sections:

- General Information:**
 - Serial Number: FXA11FTQ21000005
 - Status: Authorized
 - Base MAC Address: e8:ed:d6:36:2f:30
 - IPv4 Address: 192.168.1.111
- Modem Health:**
 - General: Authorized
 - CPU Usage: 0%
 - Memory Usage: 18%
 - Temperature: 60.50 °C
 - Modem 1 Health: Connected
 - Signal Strength: -85 dBm
 - Signal Quality: -12 dBm
- Modem Status Table:**

SIM Slot	Status	Carrier	Phone Number	Switch Status	Data Usage	imsi	icc
SIM 1	Not inserted			Backup	0 MB	N/A	
SIM 2	Inserted	Bell	My Number	Active	37 MB of 600 MB	302610030602455	89302610

FortiGate GUI monitoring page when FortiExtender is authorized in lan-extension mode



The "Details" column shows the IPsec tunnel between FortiGate and FortiExtender.

The screenshot shows the 'Managed FortiExtenders' page. It features a summary section with two donut charts: 'Status' (2 Online) and 'Mode' (2 LAN extension). Below this is a table of managed FortiExtenders:

Name	Status	Mode	Details	Modem 1 Interface	Profile	Serial #
FX006TQ22000014	Online	LAN extension	fext-ipsec-j9hh		FXA21F-lanext-default	FXA21FTQ22000014
FX004TQ21000005	Online	LAN extension	fext-ipsec-xdxy		FXA11F-lanext-default	FXA11FTQ21000005

FortiGate GUI provides Profile settings for lan-extension



- You can set the IPsec tunnel connection between FortiExtender and FortiGate on this page.
- After multiple connections from FortiExtender (as uplink) are established, you can select load balance mode on this page.

Edit FortiExtender Profile

LAN extension

Link load balance: **Active backup** Load Balance

Ipssec interface: **lan**

Ipssec interface IP/FQDN:

Ipssec tunnel: **fext-ipsec-xdxy**

FortiExtender uplink port

[+ Create New](#) [Edit](#) [Delete](#)

Name	Uplink port	Role
1	wan	Primary
2	lte1	Secondary

Modem \$1

Default SIM: **SIM1** SIM2 Carrier Lowest cost

SIM1 PIN: ☐

SIM2 PIN: ☐

Additional Information

[API Preview](#)

[References](#)

[Edit in CLI](#)

Online Guides

[Relevant Documentation](#)

[Video Tutorials](#)

FortiAnswers

[Join the Discussion](#)

FortiGate GUI provides the settings for data plan



- Each data plan is associated with a carrier name. After the SIM card is active, the modem will detect the carrier and use the corresponding plan.
- Each data plan has a data limit (capacity) that can be used by the SIM card. The data limit is reset after the billing date.

Dashboard	Managed FortiExtenders	Profiles	Data Plans
Network	+ Create new	Edit	Delete
Interfaces	Search		
DNS	Name	Modem	Slot/Carrier/ICCID
DNS Servers	Bell-plan	all	Bell
IPAM	Fido-plan	all	Fido
FortiExtenders	Telus-plan	all	Telus
SD-WAN			

Name	Modem	Slot/Carrier/ICCID	APN	Capacity	Monthly Cost	Billing Date	Type	Ref.
Bell-plan	all	Bell	pda.bell.ca	600	0	1	Carrier	1
Fido-plan	all	Fido	ltemobile.apn	1,000	0	1	Carrier	3
Telus-plan	all	Telus	sp.telus.com	800	0	1	Carrier	3

Provision FortiExtender firmware upon authorization

FortiExtender is now able to automatically perform firmware provisioning using CLI commands. This makes it possible to allow federated upgrade of an FortiExtender unit upon discovery and authorization by the FortiGate. The FortiExtender will be upgraded to the latest firmware from FortiGuard, based on the matching FortiExtender firmware version that matches each FortiOS firmware version.

1. FortiGuard has a matrix which contains following table for each FortiExtender. The matrix code is FEXV.

```
FGTVersion=7.2.1|FGTBuildNum=01247|FEXPlatform=FX201E|FEXVersion=7.2.0|FEXBuildNum=00113
|ImageIdentifier=07002000FIMG1000102000
```

2. Test condition: The FortiGate has v7.2.1 b1247 and the FortiExtender has v7.0.3 b056.

```
config system global
    set fortiextender-provision-on-authorization enable
end
```

3. Once the FortiGate has authorized the FortiExtender, automatical update is enabled for one time.

```
config extension-controller extender
    edit "FX0015919000272"
        set id "FX201E5919000272"
        set authorized enable <<----- Upon user auth,
        set device-id 1
        set extension-type wan-extension
        set profile "FX201E-wanext-default"
        set override-allowaccess enable
        set allowaccess ping telnet
        set override-login-password-change enable
        config wan-extension
            set modem1-extension "fext-201"
        end
        set firmware-provision-latest once <<----- Config is automatically set to
            "once"
    next
end
```

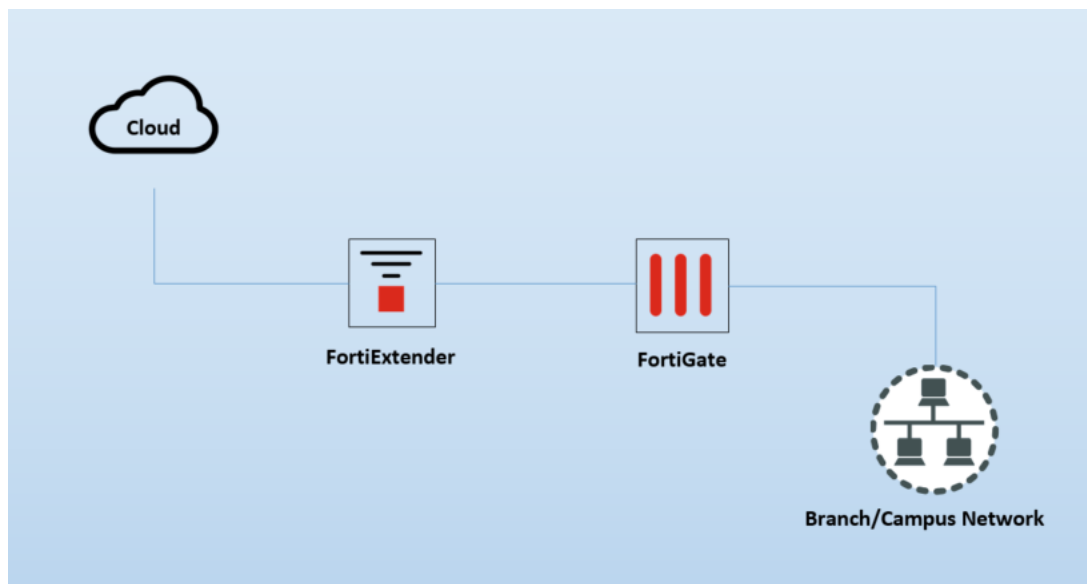
4. Once the FortiGate starts to manage the FortiExtender and detects that the FortiExtender's build is lower than that in the matrix (v7.2.0 b0113), the FortiGate will push the image (b0113) to FortiExtender.

Connect to FortiGate

When setting up a FortiExtender out of box with FortiExtender OS version 7.0.0 or later, you can connect the FortiExtender to a FortiGate in either of the following ways:

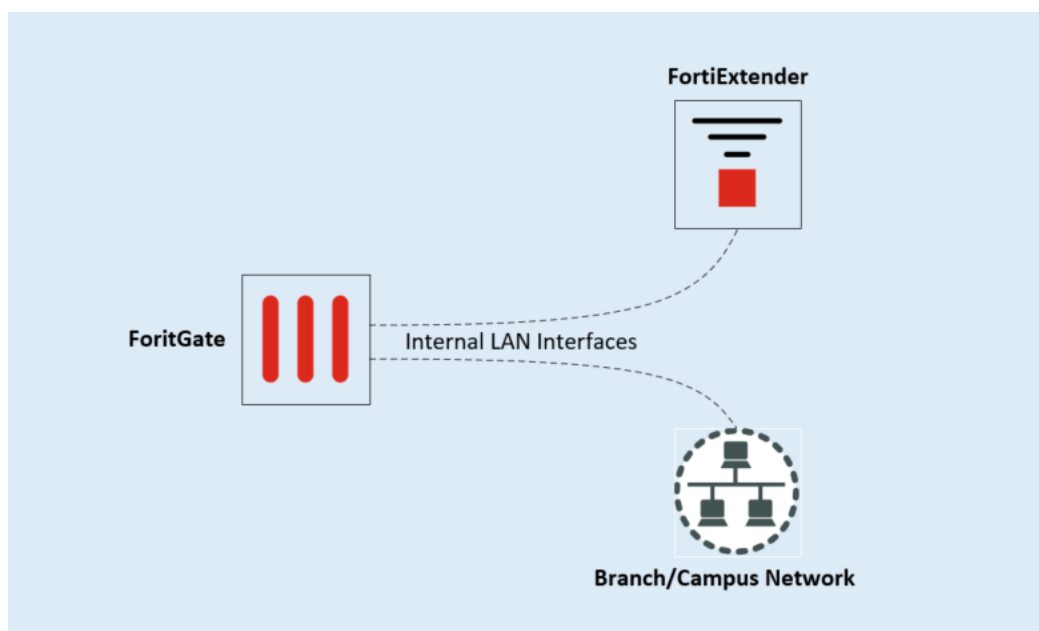
- Connect the FortiGate port (such as WAN1/WAN2) in DHCP client mode to a FortiExtender LAN port (1—3). In this option, the FortiGate interface acquires DHCP lease from the FortiExtender LAN DHCP server, and has a default gateway as the FortiExtender LAN interface IP address.
- If the FortiGate internal /LAN is running a DHCP server, connect the FortiGate to port4 of the FortiExtender, which acquires DHCP lease from the FortiGate DHCP server.

Wireless WAN extension to WAN interfaces of FortiGate



Connect the FortiGate WAN port (e.g., WAN1 or WAN2) which is in DHCP client mode to a FortiExtender LAN port (LAN 1—3 in FortiExtender 201E/211E). In this option, the FortiGate WAN interface acquires DHCP lease from the FortiExtender LAN DHCP server, and has a default gateway as the FortiExtender LAN interface IP address, as illustrated above.

Wireless extension to internal LAN interface of FortiGate



In some scenarios, you may want to connect the FortiExtender to an internal LAN interface of the FortiGate (to use POE power or some other means). In this case, if the FortiGate internal LAN is running a DHCP server, connect the FortiGate to port4 of the FortiExtender (FEX-201E/211E) which acquires DHCP lease from the FortiGate DHCP server, as illustrated above.

Authorize FortiExtender on FortiOS

Once the FortiExtender is discovered, you must authorize it by associating it either with a virtual WAN interface or a VLAN interface.

To authorize the FortiExtender device in FortiOS:

1. Go to *Network > FortiExtender*, and wait for the FortiExtender device to be discovered by the FortiGate.
2. Bind the device to an interface and authorize it.
In FortiGate 5.4 and later releases, you must manually create either a virtual WAN interface of type FEX-WAN or a VLAN sub-interface, and link it to the FortiExtender as part of the authorization process, as illustrated below.

Serial Number	FX04DA5918009600
Status	Deauthorized 
Interface Name	 fext-wan1 
Authorize Delete	

Make sure that the FortiExtender and the FortiGate are connected on Layer 2 by default. If they are not connected via Layer 2 but can reach each other via Layer-3 networking, configure the FortiExtender with static discovery using the following FortiExtender CLI commands:



```
config system management fortigate
    set ac-discovery-type static
    config static-ac-addr
        edit 1
            set server 192.168.1.99
        next
        edit 2
            set server fortinet.com
        next
    end
    set discovery-intf lan port4
end
```

Enable FortiExtender Controller on FortiOS

After connecting your FortiExtender LAN port to the FortiGate, do the following:

1. Enable the FortiExtender Controller on the FortiGate.

```
config system global
    set fortiextender enable
end
```

2. Make sure that your FortiGate enables FortiExtender Controller.

The FortiExtender-related GUI is enabled by default.

3. Enable the CAPWAP access to use the FortiGate interface to which the FortiExtender is connected.

```
config system interface
    edit lan
        append allowaccess fabric
    next
end
```



The "append allowaccess fabric" command is introduced in FOS 6.2.3, and applies to FortiGate devices running FOS 6.2.3 and later. If you are connecting your FortiExtender to a pre-FortiOS 6.2.3 FortiGate device, you MUST use "append allowaccess capwap" instead.



Be sure to keep the following in mind:

- If FortiLink is enabled, the FortiExtender must be connected to the FortiGate through FortiLink.
- If FortiLink is enabled and the FortiExtender is not part of FortiLink, the discovery type on the FortiExtender must be static.

Support for device password and allowed protocols for FortiExtender in FortiGate

This feature enables you to configure FortiExtender admin password from FortiGate. You can also configure allowaccess of the ingress interface from the FortiGate so that the FortiGate can manage the FortiExtender based on the protocol specified in allowaccess.

For FortiExtenders configured as WAN extension in FortiGate, the ingress interface is the one specified in "ingress-intf" under "config system management fortigate". In the following example, the allowaccess of the "lan" interface will be changed as the configuration from the FortiGate. The value of "ingress-intf" will be automatically filled by the system when the FortiExtender is managed by the FortiGate. It cannot be edited or unset.

```
FX201E5919000027 # config system management fortigate
FX201E5919000027 (fortigate) # show
config system management fortigate
    set ac-discovery-type broadcast
    set ac-ctl-port 5246
    set ac-data-port 25246
    set discovery-intf lan
```

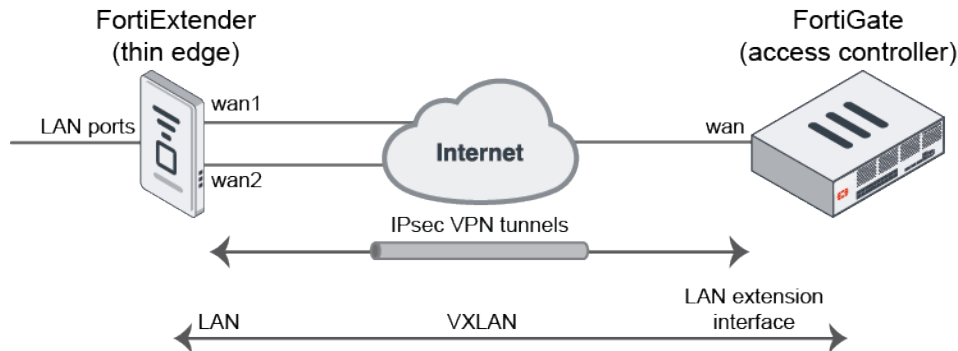
```
    set ingress-intf lan <=== The value cannot be edited and unset
end
```

For a FortiExtender configured as LAN extension of a FortiGate, the ingress interface is "le-switch", whose allowaccess will be changed as the configuration from the FortiGate. In the following example, the "le-switch" is a predefined switch interface which will be automatically generated by the system when the FortiExtender is managed by the FortiGate. The entry "le-switch" under "config system switch-interface" is read-only and cannot be edited or deleted.

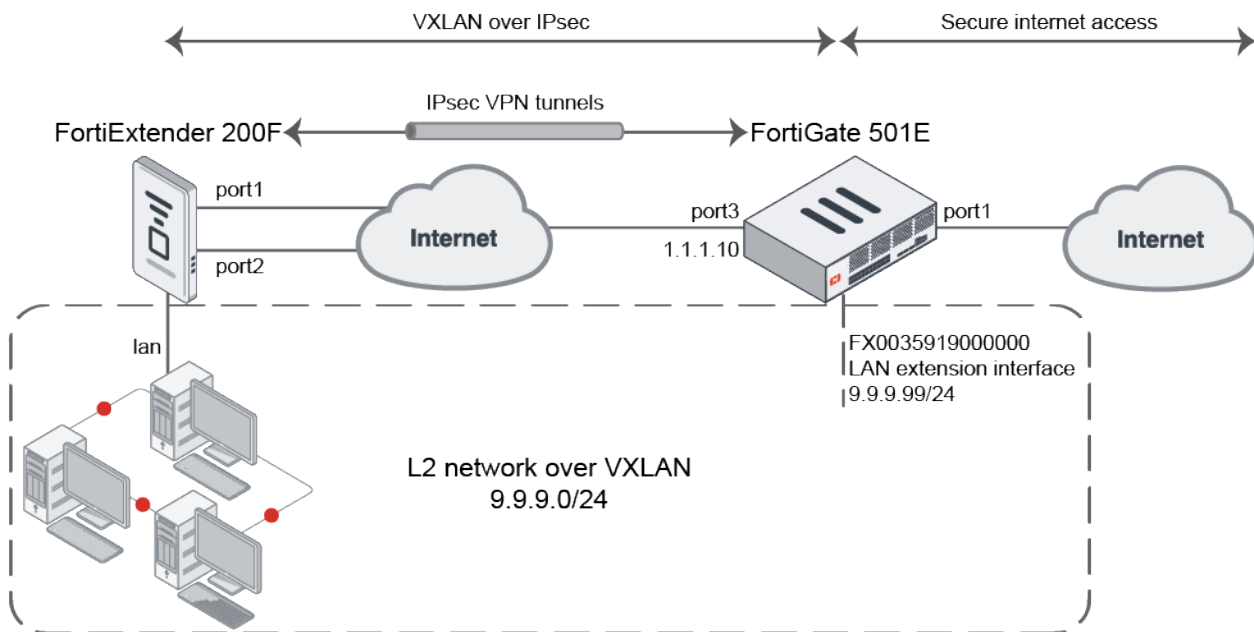
```
config system switch-interface
    edit le-switch <=== The entry cannot be edited or deleted
        set members le-agg-link lan
        set stp disable
    next
end
```

FortiExtender as FortiGate LAN extension

LAN extension is a configuration mode on the FortiGate that allows the FortiExtender to provide remote thin edge connectivity back to the FortiGate over a backhaul connection. A FortiExtender deployed at a remote location will discover the FortiGate access controller (AC) and form an IPsec tunnel (or multiple tunnels when multiple links exist on the FortiExtender) back to the FortiGate. A VXLAN is established over the IPsec tunnels to create an L2 network between the FortiGate and the network behind the remote FortiExtender.



In the following example, a FortiGate 501E is the FortiExtender AC that provides secure internet access to the remote network behind the FortiExtender 200F thin edge. The FortiGate 501E has two WAN connections: one is used as an inbound backhaul connection and the other for outbound internet access. The FortiExtender 200F has two wired WAN/uplink ports connected to the internet. Once the FortiExtender discovers the FortiGate AC and is authorized by the FortiGate, the FortiGate pushes an extender profile to the FortiExtender. From the profile, the extender uses the configurations to form two IPsec tunnels back to the FortiGate. Additional VXLAN aggregate interfaces are automatically configured to create an L2 network between the FortiExtender LAN port and a virtual LAN extension interface on the FortiGate. Clients behind the FortiExtender can now connect to the internet through the FortiGate that secures the internet connection.



Authorizing the devices

To discover and authorize the FortiExtender in the GUI:

- On the FortiGate, enable the Security Fabric connection on port3 to allow the FortiExtender to connect over CAPWAP:
 - Go to *Network > Interfaces* and edit port3.
 - In the *Administrative Access* section, select *PING* and *Security Fabric Connection*.
 - Click *OK*.
- On the FortiExtender, connect to the CLI via SSH and set the AC server address to the FortiGate:

```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
        set server 1.1.1.10
      next
    end
  set ac-ctl-port 5246
  set ac-data-port 25246
  set discovery-intf port1 port2
  set ingress-intf
end
end
```

Once the FortiExtender's discovery packet reaches port3 on the FortiGate, the FortiExtender will appear under *Network > FortiExtenders* as unauthorized.

Managed FortiExtenders			
+ Create New Edit Delete Deauthorize Search			
Name	Serial Number	Status	Mode
FX003591900000	FX200F591900000	Unauthorized	LAN extension

The FortiGate automatically creates a VPN profile for this FortiExtender, which appears on the *VPN > IPsec Tunnels* page.

+ Create New Edit Delete Search			
Tunnel	Interface Binding	Status	Ref.
Custom 1			
fext-ipsec-ksKS	port3	Inactive	3

The FortiGate also creates an extender profile for that model of FortiExtender, which appears on the *Network > FortiExtenders > Profiles* tab.

Managed FortiExtenders			
+ Create New Edit Delete Search			
Name	Model	Mode	Ref.
FX200F-lanext-default	FX200F	LAN extension	1

The FortiExtender profile is configured based on the FortiExtender model. It automatically selects *Load Balance* (as the *Link load balance* setting), the IPsec interface, and the pre-configured tunnel.

Edit FortiExtender Profile

Name: FX200F-lanext-default
Model: FX200F
Mode: LAN extension

LAN extension

Link load balance: Active backup **Load Balance**

IPsec interface: port3

IPsec interface IP/FQDN:

IPsec tunnel: fext-ipsec-ksKS

FortiExtender uplink port

+ Create New Edit Delete

Name	Uplink port	Weight
1	port1	1
2	port2	1

Additional Information

API Preview
References
Edit in CLI

Documentation
Online Help
Video Tutorials

3. Authorize the FortiExtender:

- Go to **Network > FortiExtenders**, select the **Managed FortiExtenders** tab, and edit the discovered FortiExtender.
- In the **Status** section, enable **Authorized**.

Edit FortiExtender

Serial number: FX200F5919000000
Alias:
Mode: LAN extension
Profile: FX200F-lanext-default

State

Authorized: ☒

FortiGate

FortiGate-501E

Additional Information

API Preview
Edit in CLI

Documentation
Online Help
Video Tutorials

OK Cancel

- Click **OK**. The device now displays as authorized.

Managed FortiExtenders			
Profiles Data Plans			
+ Create New Edit Delete Deauthorize Search			
Name	Serial Number	Status	Mode
FX0035919000000	FX200F5919000000	Authorized	LAN extension

To discover and authorize the FortiExtender in the CLI:

- On the FortiGate, enable the Security Fabric connection on port3 to allow the FortiExtender to connect over CAPWAP:

```
config system interface
  edit "port3"
    set vdom "root"
    set ip 1.1.1.10 255.255.255.0
    set allowaccess ping fabric
  next
end
```

2. On the FortiExtender, connect to the CLI via SSH and set the AC server address to the FortiGate:

```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
        set server 1.1.1.10
      next
    end
  set ac-ctl-port 5246
  set ac-data-port 25246
  set discovery-intf port1 port2
  set ingress-intf
end
end
```

3. The FortiGate discovers the FortiExtender and some basic configurations are automatically initialized in FortiOS:

```
config extension-controller extender
  edit "FX0035919000000"
    set id "FX200F5919000000"
    set device-id 0
    set extension-type lan-extension
    set profile "FX200F-lanext-default"
  next
end
```

4. An IPsec tunnel is automatically created for the detected FortiExtender:

```
config vpn ipsec phase1-interface
  edit "fext-ipsec-ksKS"
    set type dynamic
    set interface "port3"
    set ike-version 2
    set peertype one
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set localid "localid-5bzuqs54dGni2TT0x2NePg0HexHW2piQ44aZ4NiGe8SVxxBnFuiqZqo"
    set dpd on-idle
    set comments "[FX200F-lanext-default] Do NOT edit. Automatically generated by
extender controller."
    set peerid "peerid-svxVy5bZbPxZdfoIQBNA7YrkSKBA9UilvZsvYcVrgp1Uy0aFMCVZzGzh"
    set psksecret ENC <secret>
    set dpd-retryinterval 60
  next
end
config vpn ipsec phase2-interface
  edit "fext-ipsec-ksKS"
    set phase1name "fext-ipsec-ksKS"
```

```

        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set comments "[FX200F-lanext-default] Do NOT edit. Automatically generated by
extender controller."
    next
end

```

5. A FortiExtender profile is created for the model of the detected FortiExtender:

```

config extension-controller extender-profile
    edit "FX200F-lanext-default"
        set id 0
        set model FX200F
        set extension lan-extension
        config lan-extension
            set link-loadbalance loadbalance
            set ipsec-tunnel "fext-ipsec-ksKS"
            set backhaul-interface "port3"
            config backhaul
                edit "1"
                    set port port1
                next
                edit "2"
                    set port port2
                next
            end
        end
    end
end

```

6. Authorize the FortiExtender:

```

config extension-controller extender
    edit "FX0035919000000"
        set authorized enable
    next
end

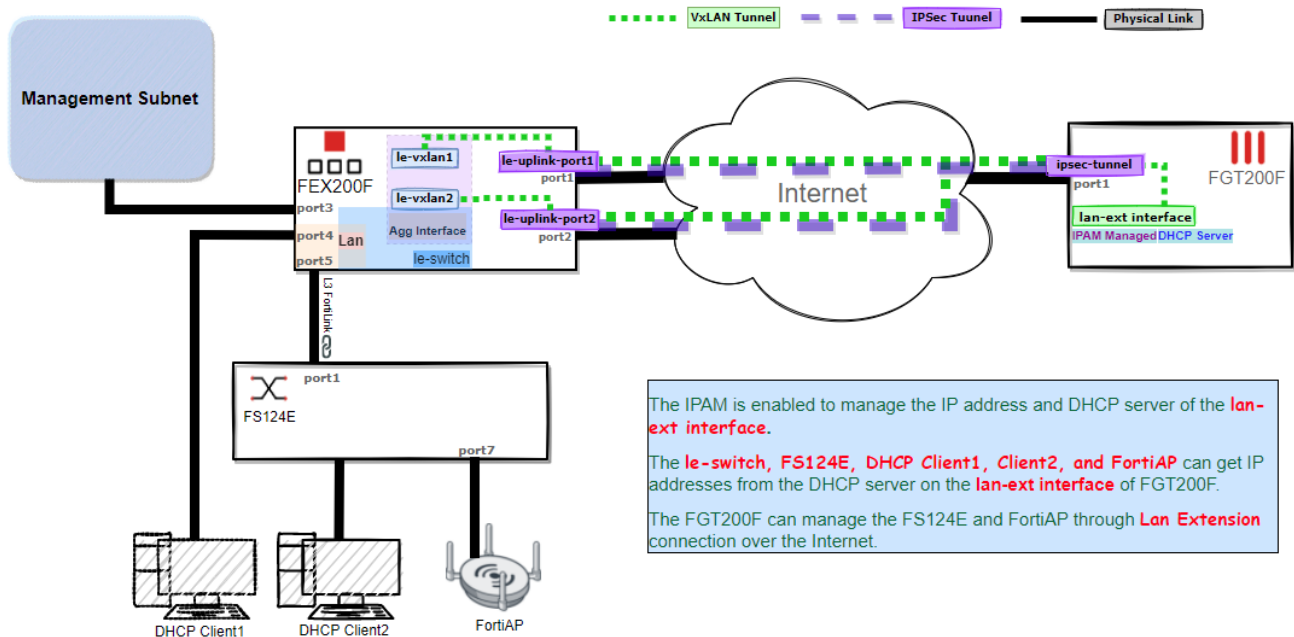
```

Backhaul tunnel and VXLAN auto-deployment

Once the FortiExtender is authorized, the FortiGate immediately pushes the IPsec tunnel configuration to the extender. This forces the FortiExtender to establish the tunnel and form the VXLAN mechanism.

In the following diagram, the VXLANs are built on the IPsec tunnels between the FortiExtender and the FortiGate. The two VXLAN interfaces are aggregated to provide load balancing and redundancy. A softswitch is also used to combine the aggregate interface with the local LAN ports, which allows the LAN ports to be part of the VXLAN. This ultimately combines the local LAN ports with the virtual LAN extension interface on the FortiGate AC.

FortiExtender as FortiGate LAN Extension Interface



Underlying configurations that are automatically configured:

1. The FortiExtender receives the IPsec configurations from the FortiGate and creates the corresponding tunnels for each uplink:

```
config vpn ipsec phase1-interface
    edit le-uplink-port1
        set ike-version 2
        set keylife 86400
        set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
        set dhgrp 14 5
        set interface port1
        set type static
        set remote-gw 1.1.1.10
        set authmethod psk
        set psksecret *****
        set localid peerid-svxVy5bZbPxZdfoIQBNA7YrkSKBA9UilvZsvYcVrgp1Uy0aFMCVZzGzh
        set peerid localid-5bzuqs54dGni2TT0x2NePg0HexHW2piQ44aZ4NiGe8SVxxBnFuiqZqo
        set add-gw-route enable
        set dev-id-notification disable
    next
    edit le-uplink-port2
        set ike-version 2
        set keylife 86400
        set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
        set dhgrp 14 5
        set interface port2
```

```

        set type static
        set remote-gw 1.1.1.10
        set authmethod psk
        set psksecret *****
        set localid peerid-svxVy5bZbPxZdfoIQBNA7YrkSKBA9Ui1vZsvYcVrgp1Uy0aFMCVZzGzh
        set peerid localid-5bzuqs54dGni2TT0x2NePg0HexHW2piQ44aZ4NiGe8SVxxBnFuiqZqo
        set add-gw-route enable
        set dev-id-notification disable
    next
end

```

2. VXLAN interfaces are formed over each tunnel:

```

config system vxlan
    edit le-vxlan-port1
        set vni 0
        set remote-ip 10.252.0.1
        set local-ip 10.252.0.2
        set dstport 9999
    next
    edit le-vxlan-port2
        set vni 0
        set remote-ip 10.252.0.1
        set local-ip 10.252.0.3
        set dstport 9999
    next
end

```

3. An aggregate interface is configured to load balance between the two VXLAN interfaces:

```

config system aggregate-interface
    edit le-agg-link
        set mode loadbalance
        set mapping-timeout 60
        config members
            edit le-vxlan-port1
                set interface le-vxlan-port1
                set weight 1
                set health-check-event le-agg-port1
                set health-check-fail-cnt 5
                set health-check-recovery-cnt 5
            next
            edit le-vxlan-port2
                set interface le-vxlan-port2
                set weight 1
                set health-check-event le-agg-port2
                set health-check-fail-cnt 5
                set health-check-recovery-cnt 5
            next
        end
    next
end

```

4. The softswitch bridges the aggregate interface and the local LAN to connect the LAN to the VXLAN bridged L2 network, which spans across to the FortiGate LAN extension interface:

```

config system switch-interface
    edit le-switch
        set members le-agg-link lan
    end
end

```

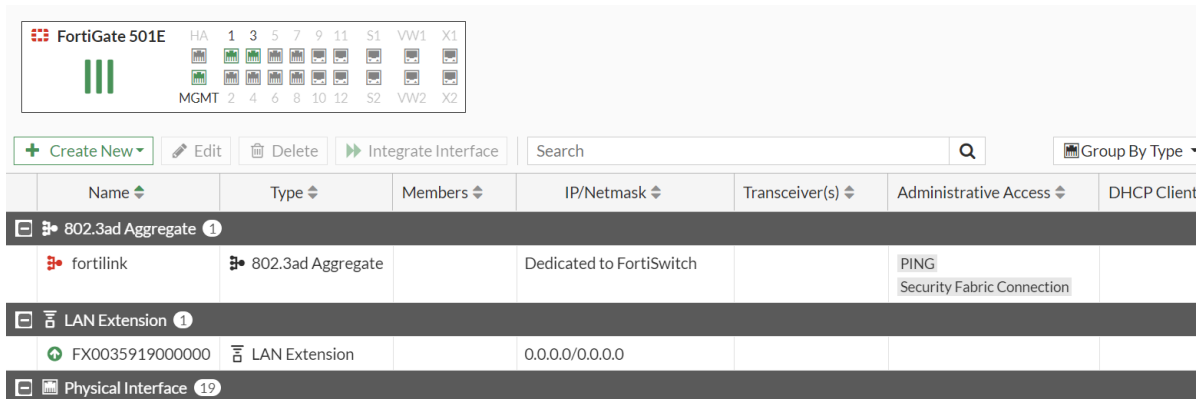
```

        set stp disable
    next
end

```

Configuring the LAN extension and firewall policy

Once the IPsec tunnel is set up and the VXLAN is created over the IPsec tunnel, the new LAN extension interface appears on the FortiGate.



To configure the LAN extension interface and firewall policy:

- Edit the LAN extension interface:
 - Go to Network > Interfaces and edit the LAN extension interface.
 - Configure the *IP/Netmask* (9.9.9.99/255.255.255.0). Other devices on the remote LAN network will configure this as their gateway.
 - Optionally, enable *DHCP Server* to assign IPs to the remote devices using DHCP.
 - Click OK.
- Configure the firewall policy to allow traffic from the LAN extension interface to the WAN (port1):
 - Go to *Policy & Objects > Firewall Policy* and click *Create New*.
 - Enter the following:

Incoming Interface	FX0035919000000
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable (NAT)

- Configure the other settings as needed, such as security profiles.

d. Click *OK*.

This policy allows the remote LAN clients to access the internet through the backhaul channel. Clients in the remote LAN behind the FortiExtender will now be able to receive an IP over DHCP and reach the internet securely through the FortiGate.

Using the backhaul IP when the FortiGate access controller is behind NAT

When the FortiGate LAN extension controller is behind a NAT device, remote thin edge FortiExtenders must connect to the FortiGate through a backhaul address. This is an address on the upstream NAT device that forwards traffic to the FortiGate. It can be configured as an IP or FQDN in the FortiGate extender profile.

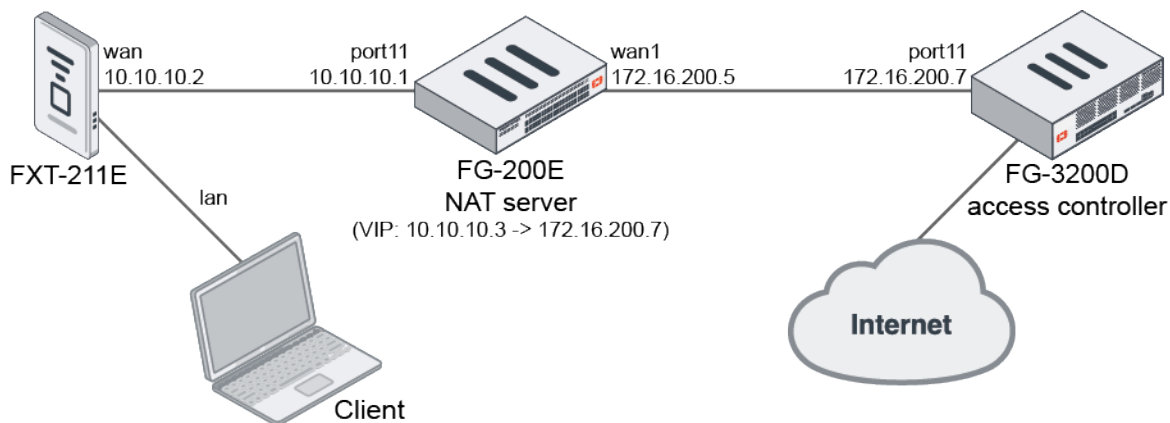
When the default IKE port 500 is inaccessible, you can configure a custom IKE port on the FortiExtender and the FortiGate.

This topic contains four configuration examples:

- [Configuring an IP as a backhaul address in the FortiGate extender profile](#)
- [Configuring an FQDN as a backhaul address in the FortiGate extender profile](#)
- [Configuring the IKE port on FortiExtender when NAT traversal is enabled in the FortiGate IPsec tunnel settings](#)
- [Configuring the IKE port on FortiExtender when NAT traversal is disabled in the FortiGate IPsec tunnel settings](#)

Examples

The following topology is used for the first three examples and assumes that the FortiExtender has already been discovered (see [FortiExtender as FortiGate LAN extension](#) on page 22 for more information).



Configuring an IP as a backhaul address in the FortiGate extender profile

To configure an IP as a backhaul address in the GUI:

1. Edit the LAN extension profile:
 - a. Go to *Network > FortiExtenders*, select the *Profiles* tab, and edit the default LAN extension profile (FX211E-lanext-default).

- b. In the *LAN extension* section, set the *IPsec interface IP/FQDN* to *10.10.10.3*.

Edit FortiExtender Profile

Name: FX211E-lanext-default
 Model: FX211E
 Mode: LAN extension
 Data plan: +

LAN extension

Link load balance: **Active backup** Load Balance

IPsec interface: port1

IPsec interface IP/FQDN: 10.10.10.3

IPsec tunnel: .fext-ipsec-bwyt

FortiExtender uplink port

Name	Uplink port	Role
1	wan	Primary
2	lte1	Secondary

Modem 1

Default SIM: **SIM1** SIM2 Carrier Lowest cost

SIM1 PIN: ☐

SIM2 PIN: ☐

GPS: ☒

Auto SIM switch

By disconnecting: ☐

By signal: ☐

OK Cancel

- c. Click OK.

2. Authorize the FortiExtender:

- a. Go to *Network > FortiExtenders*, select the *Managed FortiExtenders* tab, and edit the discovered FortiExtender.
- b. In the *Status* section, enable *Authorized*.
- c. Click OK.

In FortiExtender, the *VPN Tunnels* page displays the IPsec tunnel *le-uplink-wan* as up. The *Remote Gateway* is set to *10.10.10.3*.

VPN Tunnels

VPN Tunnels VPN Certificate

Name	Status	Local	Remote Gateway	In Bytes	Out Bytes	Up Seconds
le-uplink-wan	●	10.10.10.2	10.10.10.3	588	4334	38
le-uplink-lte1	●	0.0.0.0	10.10.10.3	0	0	0

To configure an IP as a backhaul address in the CLI:**1. Configure the backhaul IP address:**

```

config extension-controller extender-profile
  edit "FX211E-lanext-default"
    set id 1
    set model FX211E
    set extension lan-extension
    config cellular
      config sms-notification
      end
      config modem1
      end
    end
    config lan-extension
      set ipsec-tunnel "fext-ipsec-bwyt"
      set backhaul-interface "port1"
      set backhaul-ip "10.10.10.3"
      config backhaul
        edit "1"
          set port wan
          set role primary
        next
        edit "2"
          set port ltel
          set role secondary
        next
      end
    end
  next
end

```

2. Verify the configuration in FortiExtender:

```

config vpn ipsec phase1-interface
  edit le-uplink-wan
    set ike-version 2
    set keylife 86400
    set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
  3des-sha1
    set dhgrp 14 5
    set interface wan
    set type static
    set remote-gw 10.10.10.3
    set authmethod psk
    set psksecret *****
    set localid peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRTeXnb4mUi6MmXX
    set peerid localid-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZk09t
    set add-gw-route enable
    set dev-id-notification disable
  next
end

```

Configuring an FQDN as a backhaul address in the FortiGate extender profile

To configure an FQDN as a backhaul address in the GUI:

1. Edit the LAN extension profile:
 - a. Go to *Network > FortiExtenders*, select the *Profiles* tab, and edit the default LAN extension profile (*FX211E-lanext-default*).
 - b. In the *LAN extension* section, set the *IPsec interface IP/FQDN* to *fgt3200d.qatest.com*.

Edit FortiExtender Profile

Name: FX211E-lanext-default
 Model: FX211E
 Mode: LAN extension
 Data plan: +

LAN extension

Link load balance: **Active backup** Load Balance

IPsec interface: port1

IPsec interface IP/FQDN: fgt3200d.qatest.com

IPsec tunnel: fext-ipsec-bwyt

FortiExtender uplink port

+ Create New Edit Delete

Name	Uplink port	Role
1	wan	Primary
2	lte1	Secondary

Modem 1

Default SIM: **SIM1** SIM2 Carrier Lowest cost

SIM1 PIN: ☐

SIM2 PIN: ☐

GPS: ☒

Auto SIM switch

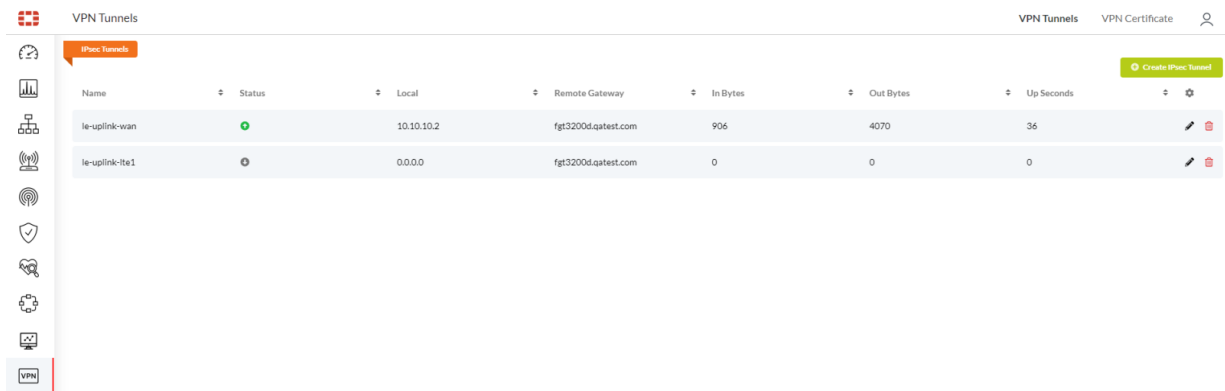
By disconnecting: ☐

By signal: ☐

OK Cancel

- c. Click **OK**.
2. Authorize the FortiExtender:
 - a. Go to *Network > FortiExtenders*, select the *Managed FortiExtenders* tab, and edit the discovered FortiExtender.
 - b. In the *Status* section, enable *Authorized*.
 - c. Click **OK**.

In FortiExtender, the *VPN Tunnels* page displays the IPsec tunnel *le-uplink-wan* as up. The *Remote Gateway* is set to *fgt3200d.qatest.com*.



Name	Status	Local	Remote Gateway	In Bytes	Out Bytes	Up Seconds	
le-uplink-wan	●	10.10.10.2	fgt3200d.qatest.com	906	4070	36	 
le-uplink-lte1	●	0.0.0.0	fgt3200d.qatest.com	0	0	0	 

To configure an FQDN as a backhaul address in the CLI:

1. Configure the backhaul IP address:

```
config extension-controller extender-profile
  edit "FX211E-lanext-default"
    set id 1
    set model FX211E
    set extension lan-extension
    config cellular
      config sms-notification
      end
      config modem1
      end
    end
    config lan-extension
      set ipsec-tunnel "fext-ipsec-bwyt"
      set backhaul-interface "port1"
      set backhaul-ip "fgt3200d.qatest.com"
      config backhaul
        edit "1"
          set port wan
          set role primary
        next
        edit "2"
          set port lte1
          set role secondary
        next
      end
    end
  next
end
```

2. Verify the configuration in FortiExtender:

```
config vpn ipsec phase1-interface
  edit le-uplink-wan
    set ike-version 2
    set keylife 86400
    set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
    set dhgrp 14 5
```

```

        set interface wan
        set type ddns
        set remotegw-ddns fgt3200d.qatest.com
        set authmethod psk
        set psksecret *****
        set localid peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRTeXnb4mUi6MmXX
        set peerid localid-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZkO9t
        set add-gw-route enable
        set dev-id-notification disable
    next
end

```

Configuring the IKE port on the FortiExtender when NAT traversal is enabled in the FortiGate IPsec tunnel settings

To configure the IKE port on FortiExtender when NAT traversal is enabled:

1. Set the IKE port on the FortiGate:

```

config system settings
    set ike-port 6000
end

```

2. Set the IKE port on the FortiExtender:

```

config system settings
    set ike-port 6000
end

```

3. Start a packet capture on the FG-200E's port11 with the filter set to UDP protocol and port 4500 or 6000.
4. Terminate the IPsec VPN tunnel in FortiExtender:

```

~ # swanctl -t -i le-uplink-wan
[IKE] deleting IKE_SA le-uplink-wan[5] between 10.10.10.2[peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRTeXnb4mUi6MmXX]...10.10.10.3[localid-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZkO9t]
[IKE] sending DELETE for IKE_SA le-uplink-wan[5]
[ENC] generating INFORMATIONAL request 2 [ D ]
[NET] sending packet: from 10.10.10.2[4500] to 10.10.10.3[6000] (80 bytes)
[NET] received packet: from 10.10.10.3[6000] to 10.10.10.2[4500] (80 bytes)
[ENC] parsed INFORMATIONAL response 2 [ ]
[IKE] IKE_SA deleted
terminate completed successfully

```

5. Verify the packet capture on the FG-200E. During the tunnel setup, the first packet from the FortiExtender has the source port set to 6000, but it changes to 4500. This is because FortiExtender only supports Port 4500 when NAT traversal is enabled:

```

# diagnose sniffer packet port11 'udp and port 4500 or port 6000' 4
interfaces=[port11]
filters=[udp and port 4500 or port 6000]
...
24.064847 port11 -- 10.10.10.2.6000 -> 10.10.10.3.6000: udp 936
24.065929 port11 -- 10.10.10.3.6000 -> 10.10.10.2.6000: udp 428

```

```
24.119178 port11 -- 10.10.10.2.4500 -> 10.10.10.3.6000: udp 612
24.120272 port11 -- 10.10.10.3.6000 -> 10.10.10.2.4500: udp 276
```

6. Verify the IPsec tunnel status on the FortiExtender to confirm that Port 4500 is used:

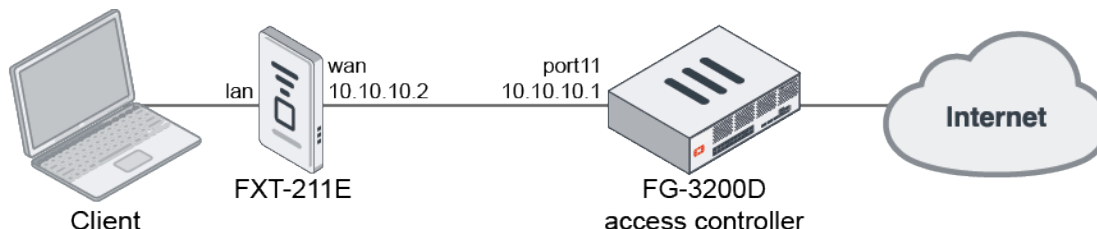
```
~ # swanctl -l
le-uplink-wan: #3, ESTABLISHED, IKEv2, 1fbb2997d6a5afc7_i* 5d500758882339f4_r
  local 'peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRTeXnb4mUi6MmXX' @ 10.10.10.2
[4500]
  remote 'localid-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZkO9t' @ 10.10.10.3
[6000]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  established 90s ago, rekeying in 85289s
  le-uplink-wan: #3, reqid 3, INSTALLED, TUNNEL-in-UDP, ESP:AES_CBC-128/HMAC_SHA1_96
    installed 90s ago, rekeying in 38952s, expires in 47430s
    in c3406a5a (0x000000005), 1512 bytes, 18 packets, 2s ago
    out 7d17257c (0x000000005), 8000 bytes, 52 packets, 2s ago
    local 10.252.8.2/32
    remote 10.252.8.1/32
```



NAT traversal has the default value enabled in the FortiGate IPsec tunnel settings, and it is not recommended to change any IPsec tunnel configurations even if there is a NAT server between the FortiExtender and the FortiGate access controller. The IPsec tunnel always uses Port 4500 for NAT traversal.

Configuring the IKE port on FortiExtender when NAT traversal is disabled in the FortiGate IPsec tunnel settings

NAT traversal is enabled by default in the FortiGate IPsec tunnel setting and it cannot be changed in the GUI. If NAT traversal is disabled, the IPsec tunnel can use a custom IKE port (port 6300 in this example).



To configure the IKE port on FortiExtender when NAT traversal is disabled:

1. Set the IKE port on the FortiGate:

```
config system settings
  set ike-port 6300
end
```

2. Set the IKE port on the FortiExtender:

```
config system settings
  set ike-port 6300
end
```

3. Verify the IPsec tunnel status on the FortiExtender to confirm that port 6300 is used:

```
~ # swanctl -l
le-uplink-wan: #2, ESTABLISHED, IKEv2, 14a9fe5800b9d0b9_i* 9dd465f634ed9abd_r
  local 'peerid-aRuaScJBVVJlDWKrrKcY8VcHF8Vg6cgLQkpEtdzDRpRTVvapxdeeJoiO' @ 10.10.10.2
[6300]
  remote 'localid-dCcVF2kc5PWVuKbNvWEoBlm332ik5dz1jtRqxfaxxiH4G7y5wLDAPcN' @ 10.10.10.1
[6300]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  established 3606s ago, rekeying in 82066s
le-uplink-wan: #1, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-128/HMAC_SHA1_96
  installed 3606s ago, rekeying in 37205s, expires in 43914s
  in c3ae8beb (0x00000003), 60564 bytes, 721 packets, 1s ago
  out d0d92a63 (0x00000003), 343410 bytes, 2365 packets, 1s ago
  local 10.252.8.2/32
  remote 10.252.8.1/32
```

Bandwidth limits on the FortiExtender Thin Edge

The FortiGate LAN extension controller can push a bandwidth limit to the FortiExtender Thin Edge. The limit is enforced on the FortiExtender using traffic shaping.

To configure a bandwidth limit:

1. On the FortiGate, create a LAN extension profile with bandwidth control enabled and a bandwidth limit configured (in Mbps):

```
config extension-controller extender-profile
  edit "FX200F-lanext-default"
    set model FX200F
    set extension lan-extension
    set enforce-bandwidth enable
    set bandwidth-limit 20
  next
end
```

2. Add a FortiExtender in LAN extension mode and apply the profile to it:

```
config extension-controller extender
  edit "FX0035919000000"
    set id "FX200F5919000000"
    set authorized enable
    set extension-type lan-extension
    set profile "FX200F-lanext-default"
  next
end
```

3. On the FortiExtender, confirm that the bandwidth configuration has been pushed to it:

```
config firewall shaper
  config traffic-shaper
    edit le-traffic-shaper
      set max-bandwidth 20
      set bandwidth-unit mbps
    next
  end
end
config firewall shaping-policy
  edit le-shaping-policy
    set status enable
    set dstintf le-agg-link
    set traffic-shaper le-traffic-shaper
  next
end
```

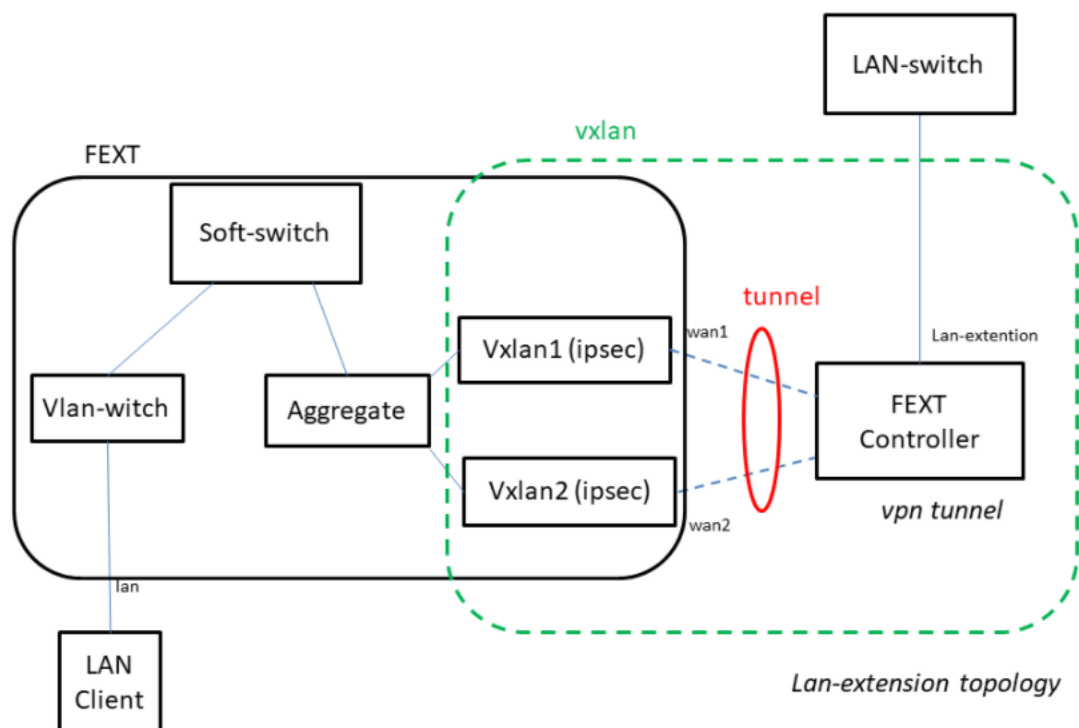
If bandwidth enforcement is disabled on the FortiGate, the configuration that was pushed to the FortiExtender will be removed.

IPAM in FortiExtender LAN extension mode

After authorizing the FortiExtender in LAN-extension mode, the FortiExtender controller generates a new lan-extension interface.

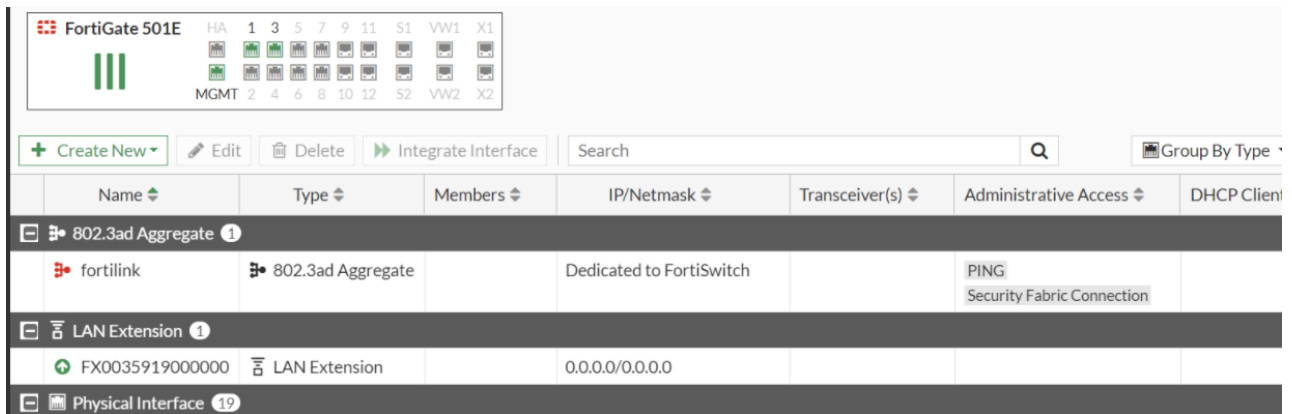
The LAN client connecting to the FortiExtender LAN interface will get DHCP allocation from the lan-extension interface. It can then reach the Internet via the firewall policy in the FortiExtender controller.

Topology



To configure IPAM in the FortiExtender lan-extension interface in the GUI:

1. On the FortiGate device, go to *Interfaces*. You will see that the LAN extension interface has already been created in the FortiExtender controller.



2. In the *LAN Extension* section, highlight the lan-extension interface (FX0035919000000), and select *Edit*.
3. For *Addressing mode*, select *Auto-managed by IPAM > Enable IPAM*.

Edit Interface

Name: ↑ FX0035919000000

Alias:

Type: LAN Extension

VRF ID ⓘ:

Role ⓘ: LAN

Address

Addressing mode: Manual DHCP Auto-managed by IPAM

⚠ IPAM is not enabled. Enable IPAM

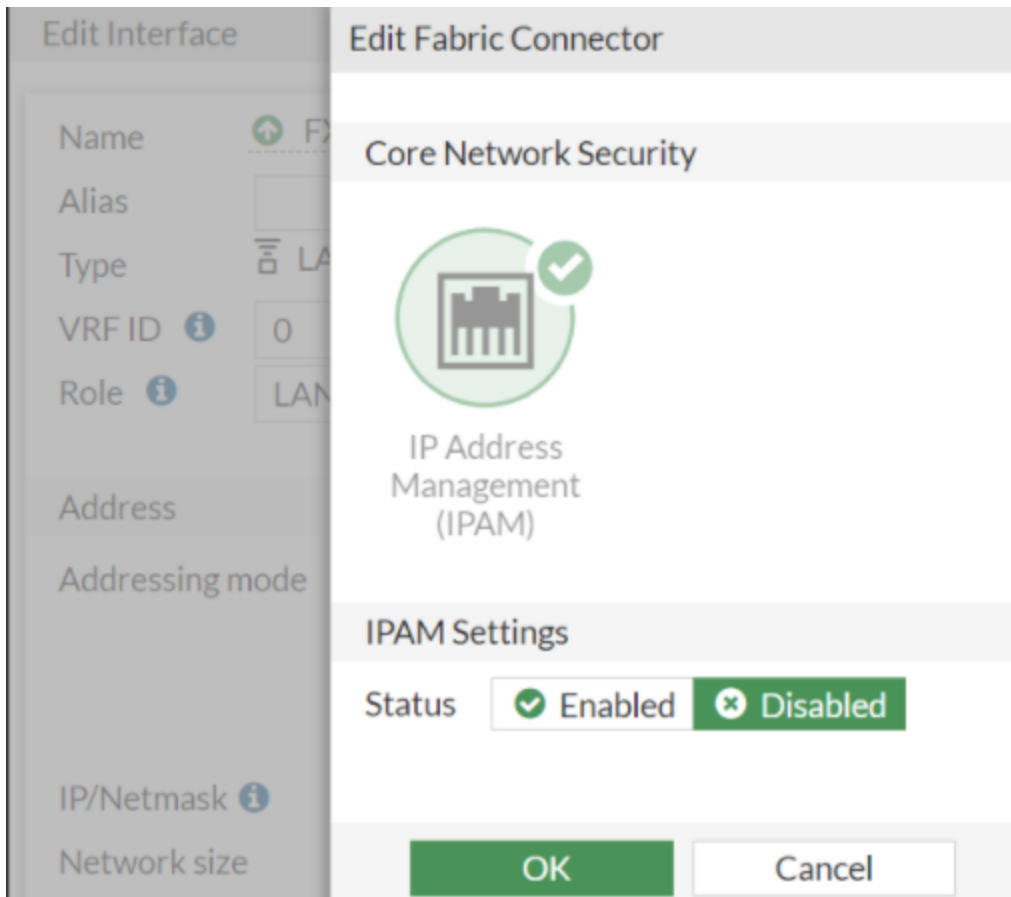
IP/Netmask ⓘ: Not allocated

Network size: 256 (255.255.255.0)

ⓘ IPAM will allocate an IP subnet with the selected size.

Create address object matching subnet ☐

4. For *IPAM Settings > Status*, select *Enable* and then *OK*. The IP pool now is selected for FX0035919000000.



The screenshot shows the 'Edit Fabric Connector' dialog in the FortiGate GUI. The 'Core Network Security' section is expanded, displaying 'IP Address Management (IPAM)' with a green checkmark icon. Below this, the 'IPAM Settings' section shows the 'Status' as 'Enabled' (with a green checkmark icon) and 'Disabled' (with a red X icon). The 'OK' button is highlighted in green.



The subnet configured above is for a standalone device.

If the FortiGate is a Security Fabric Downstream device, the subnet in the pool will be sent from the Security Fabric Root device.

The screenshot displays the FortiGate configuration interface. On the left, the 'Edit Interface' panel is partially visible, showing fields for Name, Alias, Type, VRF ID (0), Role (LAN), Address, Addressing mode, IP/Netmask, and Network size. The main panel is titled 'Edit Fabric Connector' and shows the configuration for 'Core Network Security'. A green checkmark icon indicates that the configuration is successful. Below the icon, the text 'IP Address Management (IPAM)' is displayed. The 'IPAM Settings' section shows the 'Status' as 'Enabled' (with a green checkmark) and 'Disabled' (with a red X). The 'Pool subnet' is set to '172.31.0.0 255.255.0.0'. At the bottom, there are 'OK' and 'Cancel' buttons.

The IP and DHCP server on FX0035919000000 will be set accordingly.

Address

Addressing mode

ManualDHCPAuto-managed by IPAM

IP/Netmask ⓘ

172.31.0.1/255.255.255.0

Network size

256 (255.255.255.0) ▼

Create address object matching subnet

○

Administrative Access

IPv4

☐ HTTPS

☐ FMG-Access

☐ FTM

☐ Speed Test

☐ HTTP ⓘ

☐ SSH

☐ RADIUS Accounting

☐ PING

☐ SNMP

☐ Security Fabric Connection ⓘ

☒ DHCP Server

DHCP status

EnabledDisabled

Address range ⓘ

172.31.0.1-172.31.0.254

Netmask ⓘ

255.255.255.0

Default gateway

Same as Interface IPSpecify

DNS server

Same as System DNSSame as Interface IPSpecify

Lease time ⓘ

604800second(s)

OK

Cancel

The client will get DHCP allocation from FX0035919000000.



The client is a FortiGate-61F whose wan1 connects the lan-interface on the FortiExtender.

Edit Interface

Name

wan1

Alias

Type

Physical Interface

Role ⓘ

WAN ▾

Estimated bandwidth ⓘ

0

0

kbps Upstream

kbps Downstream

Address

Addressing mode

Manual DHCP PPPoE

Status

✓ Connected

Obtained IP/Netmask

172.31.0.2/255.255.255.0 Renew

Expiry Date

2022/01/14 15:54:08

Acquired DNS

96.45.45.45 96.45.46.46

Default gateway

172.31.0.1

Retrieve default gateway from server

☑

Distance

5

Override internal DNS

☑

To configure IPAM in the FortiExtender lan-extension interface in the CLI:

Originally, the lan-extension interface has the following options after the FortiExtender is authorized:

```
config system interface
  edit "FX0035919000000"
    set vdom "root"
    set type lan-extension
    set role lan
    set snmp-index 27
    config ipv6
      set ip6-send-adv enable
      set ip6-other-flag enable
    end
    set interface "fext-ipsec-wiUx"
  next
end
```

After IPAM is set as the addressing mode for FX0035919000000 in the GUI, the following steps are created in the CLI:

```
config system ipam
    set status enable
end

config system interface
    edit "FX0035919000000"
        set vdom "root"
        set ip 172.31.0.1 255.255.255.0
        set type lan-extension
        set role lan
        set snmp-index 27
        set ip-managed-by-fortiipam enable
        config ipv6
            set ip6-send-adv enable
            set ip6-other-flag enable
        end
        set interface "fext-ipsec-wiUx"
    next
end

config system dhcp server
    edit 3
        set dns-service default
        set default-gateway 172.31.0.1
        set netmask 255.255.255.0
        set interface "FX0035919000000"
        config ip-range
            edit 1
                set start-ip 172.31.0.1
                set end-ip 172.31.0.254
            next
        end
        set dhcp-settings-from-fortiipam enable
        config exclude-range
            edit 1
                set start-ip 172.31.0.1
                set end-ip 172.31.0.1
            next
        end
    next
end
```

FortiExtender LAN extension in public cloud FGT-VM

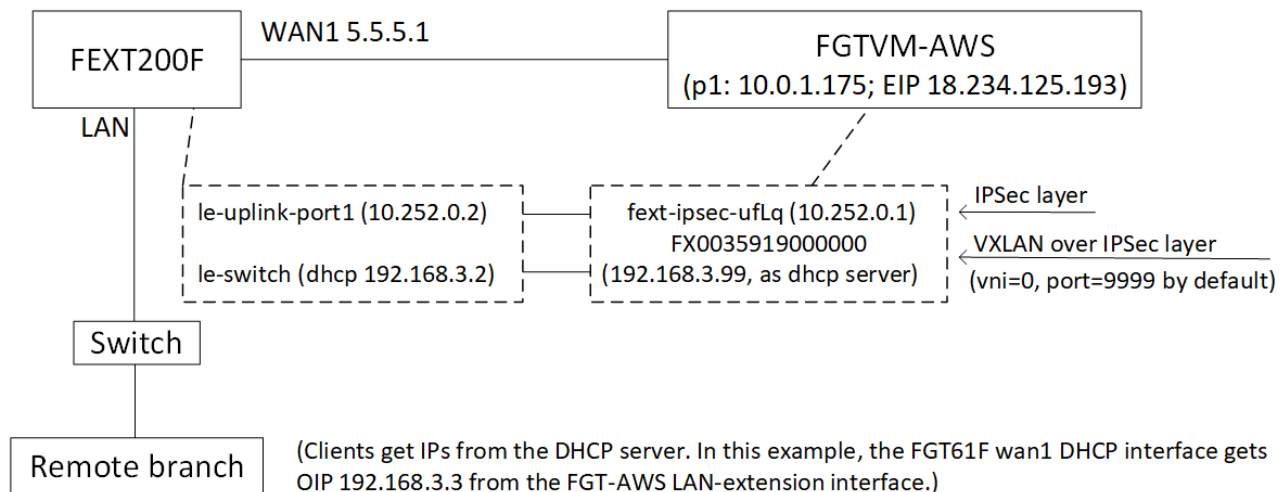
The FortiExtender LAN extension feature allows a FortiGate to extend its LAN functionality to a remote FortiExtender. In this enhancement, the FortiExtender LAN extension is added to the FGT-VM running on Public Clouds.

Topology in demo configuration:

Before LAN extension



After LAN extension



Note:

In this demo, the FEXT200F LAN interface includes port4 and port5, which are members of the le-switch. After the FEXT and the FGTVM connect successfully, the FGTVM is able to extend LAN to the remote branch on the FEXT LAN interface via VXLAN.

GUI

The LAN-extension interface is up on the FGT-AWS.

FortiGate VM64-AWS 1 3 5 7 9 11 13 15 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24 Create New Edit Delete Integrate Interface Search Group By Type								
Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.	
802.3ad Aggregate								
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2	
LAN Extension								
FX0035919000000	LAN Extension		192.168.3.99/255.255.255.0	PING HTTPS SSH SNMP +2	2	192.168.3.2-192.168.3.98	1	
Physical Interface								
port1	Physical Interface		10.0.1.175/255.255.255.0	PING HTTPS SSH HTTP +2				3
fext-ipsec-v3JH	Tunnel Interface		10.252.0.1/255.255.255.255	PING				4
Tunnel Interface								
NAT interface (nafroot)	Tunnel Interface		0.0.0.0/0.0.0.0					0

The FGT-AWS LAN-extension interface is able to act as a DHCP server over VXLAN, and remote branch computers (In this demo, it's an FGT61F) behind the FortiExtender are able to get IP addresses from the DHCP server on the FGT-AWS LAN-extension interface.

FortiGate VM64-AWS 1 3 5 7 9 11 13 15 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24 Create New Edit Delete Integrate Interface Search						
802.3ad Aggregate fortilink 802.3ad Aggregate						
LAN Extension FX0035919000000 LAN Extension						
Physical Interface port1 Physical Interface						
Tunnel Interface fext-ipsec-v3JH Tunnel Interface						
Tunnel Interface NAT interface (nafroot) Tunnel Interface						

DHCP Clients for FX0035919000000						
Refresh Revoke Reservation Search						
Device	IP	Interface	Status	MAC	Reserved	Host Information
FX200F5919000000	192.168.3.2	FX0035919000000	Leased out	e8:1c:bac:4:4e:b8	Not Reserved	VCI: FortiExtender-200F Hostname: FX200F591900
FGT61FTK19006594	192.168.3.3	FX0035919000000	Leased out	04:d5:90:7a:50:a8	Not Reserved	VCI: FortiGate-61F Hostname: FGT61FTK1900

CLI

Step 1: Configure the FortiExtender:

```

FX200F5919000000 # config system interface
FX200F5919000000 (interface) # edit port1
FX200F5919000000 (port1) # set mode static
FX200F5919000000 (port1) <M> # set ip 5.5.5.1/24
FX200F5919000000 (port1) <M> # set gateway 5.5.5.99
FX200F5919000000 (port1) <M> # end

```

```

FX200F5919000000 # execute ping 18.234.125.193
PING 18.234.125.193 (18.234.125.193): 56 data bytes
64 bytes from 18.234.125.193: seq=0 ttl=233 time=68.132 ms

FX200F5919000000 # config system management
FX200F5919000000 (management) # set discovery-type fortigate
Changing "discovery-type" may affect networking mode and virtual-wire-pair
configuration, resulting in system reboot!
Do you want to continue? (y/n)y

FX200F5919000000 (management) <M> # config fortigate
FX200F5919000000 (fortigate) # set ac-discovery-type static
FX200F5919000000 (fortigate) <M> # config static-ac-addr
FX200F5919000000 (static-ac-addr) # edit 1
FX200F5919000000 (1) <M> # set server 18.234.125.193
FX200F5919000000 (1) <M> # next
FX200F5919000000 (static-ac-addr) # end
FX200F5919000000 (fortigate) <M> # set discovery-intf port1
FX200F5919000000 (fortigate) <M> # end
FX200F5919000000 (management) <M> # end

config system switch-interface
    edit le-switch
        set members le-agg-link lan
        set stp disable
    next
end
edit lan
    set type lan-switch
    set status up
    set mode static
    set ip
    set gateway
    set mtu-override enable
    set mtu 1500
    set distance 50
    set vrrp-virtual-mac enable
    config vrrp
        set status disable
    end
    set allowaccess http https ssh ping telnet
next
config system lan-switch
    config ports
        edit port4
        next
        edit port5
        next
    end
end
end

```

Step 2: Configure the FGT-AWS:

```

FGT-AWS-EXT # show system global
config system global
    set fortiextender enable
    set hostname "FGT-AWS-EXT"

```

```

end
config system interface
    edit "port1"
        set allowaccess ping https ssh http fgfm fabric
    next
end
config extension-controller extender <=====This table is automatically added after
FGT detects the FEXT over "fabric" protocol on the port1
    edit "FX0035919000000"
        set id "FX200F5919000000"
        set device-id 0
        set extension-type lan-extension
        set profile "FX200F-lanext-default"
    next
end
config extension-controller extender-profile
    edit "FX200F-lanext-default"
        set id 0
        set model FX200F
        set extension lan-extension
        config lan-extension
            set ipsec-tunnel "fext-ipsec-ufLq"
            set backhaul-interface "port1"
            set backhaul-ip "18.234.125.193"
            config backhaul
                edit "1"
                    set port port1
                    set role primary
                next
            end
        end
    next
end
config extension-controller extender
    edit "FX0035919000000"
        set authorized enable
    next
end

```

Step 3: The FGT-AWS and the FEXT connect automatically over IPSec. There is no need to configure it manually, but you must ensure that IPSec works:

```

FGT-AWS-EXT # sh vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "fext-ipsec-v3JH"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype one
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set localid "localid-
760sv1bSXj2wrUASE1uwcryLKilXEUlmhlv1FehZ2u97lqHDPukCjFh"
        set dpd on-idle
        set comments "[FX200F-lanext-default] Do NOT edit. Automatically
generated by extender controller."

```

```

        set peerid "peerid-
4GyQg3yg01w5ye7oaPQNQLQs9fM8qyXReabC3lBsOPeZGSdiqfJp8tjl"
        set psksecret ENC
IyjGZpuZykJBmtOL4cfEoQQ/yNM4N1kDXvB/TBq6dXlzeXymkw8cyoizM2a8SeyWao2sGnLCkqqkHIttruVfy7jy10dMp
6AzaFlnxP6f9k8hTEBKxqUOS3+ccvSLFWvM7ouuaWgA6Hdu4StWsBVMc85tBFfe+H6PTnVpRFaRCYQE0yatuM9tcWQXCi
lsuv66HlAYvGlw==
        set dpd-retryinterval 60
    next
end

FGT-AWS-EXT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=fext-ipsec-v3JH_0 ver=2 serial=3 10.0.1.175:4500->204.101.161.19:64916 tun_
id=204.101.161.19 tun_id6=::10.0.0.3 dst_mtu=9001 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/9088 options
[2380]=rgwy-chg rport-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0
parent=fext-ipsec-v3JH index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=0 olast=0 ad=/0
stat: rxp=6334 txp=710 rxb=1190272 txb=62655
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=0 interval=10 remote_port=64916
proxyid=fext-ipsec-v3JH proto=0 sa=1 ref=4 serial=1 add-route
src: 0:10.252.0.1-10.252.0.1:0
dst: 0:10.252.0.2-10.252.0.2:0
SA: ref=3 options=682 type=00 soft=0 mtu=8926 expire=40316/0B replaywin=2048
seqno=2c7 esn=0 replaywin_lastseq=000018be itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=43189/43200
dec: spi=07c1e02b esp=aes key=16 b0e867d4cb6b4ebc6778ea7dff3819db
ah=sha1 key=20 70e681e26a5bdcaa60e16f32d714b4ee74073306
enc: spi=c6e96e0d esp=aes key=16 139e01770682b809d24702bb9c446e8f
ah=sha1 key=20 89ffb4be3b6b9db9145be6f0d37ee49d01940a2f
dec:pkts/bytes=6334/764822, enc:pkts/bytes=710/115536
-----
name=fext-ipsec-v3JH ver=2 serial=1 10.0.1.175:0->0.0.0.0:0 tun_id=10.0.0.1 tun_
id6=::10.0.0.1 dst_mtu=0 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/512 options
[0200]=frag-rfc accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=2907 olast=2907 ad=/0
stat: rxp=6336 txp=712 rxb=1190592 txb=62823
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0

```

Step 4: Ensure that VXLAN over IPSec is set up automatically between the FGT cloud VM and the FortiExtender. (There is no need to configure it manually.)

```

FGT-AWS-EXT # diagnose sys vxlan fdb list FX0035919000000
mac=00:00:00:00:00:00 state=0x0082 remote_ip=10.252.0.2 port=9999 vni=0
ifindex=9
mac=e8:1c:ba:c4:4e:b8 state=0x0002 remote_ip=10.252.0.2 port=9999 vni=0
ifindex=9
mac=04:d5:90:7a:50:a8 state=0x0002 remote_ip=10.252.0.2 port=9999 vni=0
ifindex=9

total fdb num: 3

```

Step 5: Set the IP address for the FGT-AWS LAN-extension interface, and ensure that the FGT-AWS LAN-extension interface is able to act as DHCP server over VXLAN:

```
FGT-AWS-EXT # show system dhcp server 100
```

```
config system dhcp server
  edit 100
    set default-gateway 192.168.3.99
    set netmask 255.255.255.0
    set interface "FX0035919000000"
    config ip-range
      edit 1
        set start-ip 192.168.3.2
        set end-ip 192.168.3.98
      next
    end
  next
end

config system interface
  edit "FX0035919000000"
    set vdom "root"
    set ip 192.168.3.99 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
    set type lan-extension
    set role lan
    set snmp-index 7
    set interface "fext-ipsec-v3JH"
  next
end
```

```
***** FEXT le-switch interface is able to get the ip (192.168.3.2) from FGT-AWS vxlan
interface dhcp server
FX200F5919000000 # get system interface
== [ le-switch ]
name: le-switch      status: online/up/link up      type: switch      mac:
e8:1c:ba:c4:4e:b8   mode: dhcp      ip: 192.168.3.2/24      mtu: 1500
gateway: 192.168.3.99
```

***** Remote branch PC behind FEXT lan interface is able to get the ip from FGT-AWS vxlan interface dhcp server.

In this demo, a FGT61F acts as a PC behind FEXT, this FGT61 wan1 interface is the same switch as FEXT lan interface port4.

Set FGT61 wan1 interface as dhcp client, it can get ip address (in this demo it's 192.168.3.3) from FGT-AWS lan-extension interface.

```
FGT61FTK19006594 # show system interface wan1
config system interface
  edit "wan1"
    set vdom "root"
    set mode dhcp
    set allowaccess ping https ssh snmp
    set type physical
    set role wan
```

```
        set snmp-index 1
    next
end
```

```
FGT61FTK19006594 # diag hardware deviceinfo nic wan1
Current_HWaddr      04:d5:90:7a:50:a8
Permanent_HWaddr    04:d5:90:7a:50:a8
```

Step 6: Ensure that the FGT-AWS is able to access the remote branch behind the FortiExtender via VXLAN:

```
FGT-AWS-EXT # exec ping 192.168.3.3
PING 192.168.3.3 (192.168.3.3): 56 data bytes
64 bytes from 192.168.3.3: icmp_seq=0 ttl=255 time=68.9 ms
64 bytes from 192.168.3.3: icmp_seq=1 ttl=255 time=68.6 ms

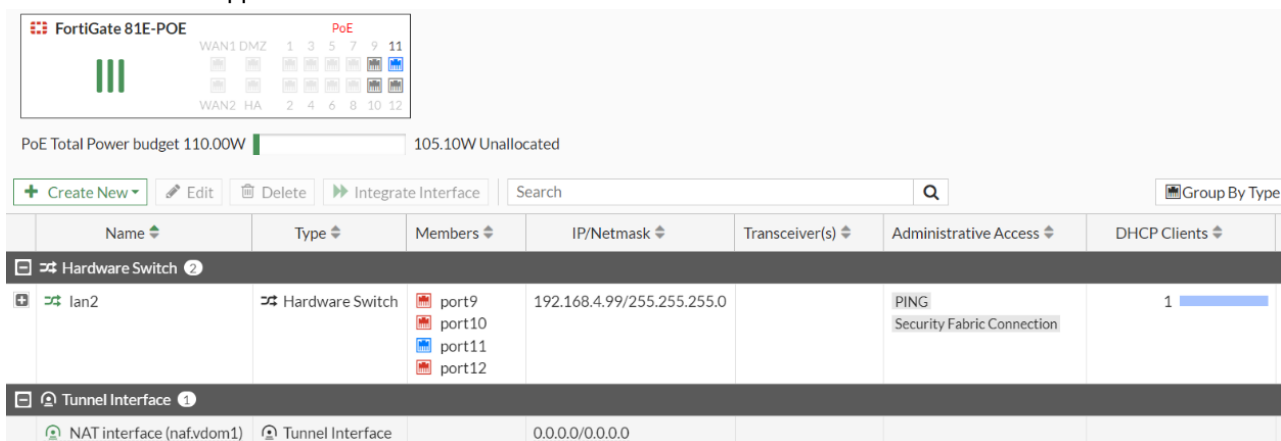
FGT-AWS-EXT # diag ip arp list
index=13 ifname=FX0035919000000 192.168.3.3 04:d5:90:7a:50:a8 state=00000008 use=362
confirm=362 update=429 ref=3
```

Allow FortiExtender to be managed and used in a non-root VDOM

This feature allows FortiExtender to be managed and used in a non-root VDOM.

GUI operating procedures

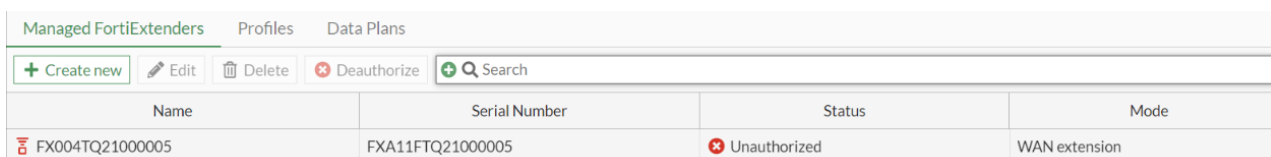
1. The FortiExtender appears in the Network section in each VDOM.



2. The FortiExtender can be discovered in the VDOM.



The VDOM must get an interface (lan2) with Security Fabric Connection and a DHCP server. Then the FortiExtender can be discovered when connecting to lan2 port11.



3. After it is authorized, the FortiExtender can provide an interface to the VDOM.



The FortiExtender can be authorized to bond a FortiExtender type interface to the LTE modem.

Edit FortiExtender

Serial number

FXA11FTQ21000005

Alias

Mode

LAN extension

WAN extension

Profile

FXA11F-wanext-default

Extender Profile Overrides

Management access

FortiExtender login password

State

Authorized

WAN extension

Modem 1 Interface

Search

+ Create

fext-vdom1

Interface

fext-vdom1

Port Speed

Auto-Negotiation

Type

FortiExtender WAN Extension

Role

WAN

OK

Cancel



The FortiExtender is connected to the FortiGate after authorization.

Edit FortiExtender

Serial number

FXA11FTQ21000005

Alias

Mode

LAN extension

WAN extension

Profile

FXA11F-wanext-default

Extender Profile Overrides

Management access

FortiExtender login password

State

Authorized

Firmware

FXTA11F-v7.0.2-build622

Upgrade

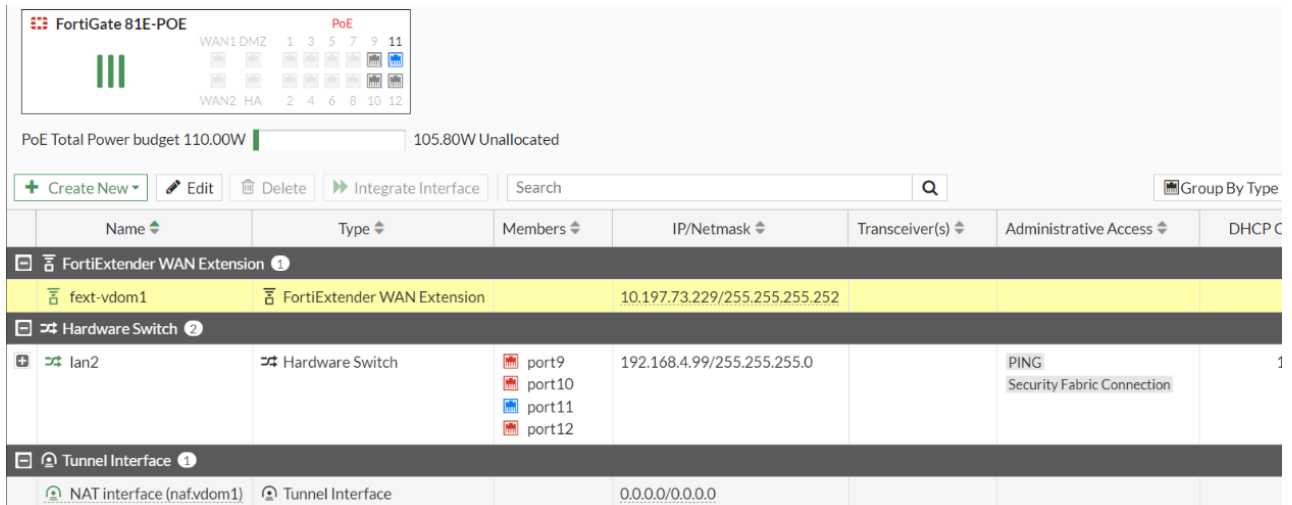
WAN extension

Modem 1 Interface

fext-vdom1



The FortiGate gets the IP and gateway for the FortiExtender type interface in the VDOM.



PoE Total Power budget 110.00W 105.80W Unallocated

[+ Create New](#)
[Edit](#)
[Delete](#)
[Integrate Interface](#)

[Group By Type](#)

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP C
FortiExtender WAN Extension 1						
fext-vdom1	FortiExtender WAN Extension		10.197.73.229/255.255.255.252			
Hardware Switch 2						
Ian2	Hardware Switch	port9 port10 port11 port12	192.168.4.99/255.255.255.0		PING Security Fabric Connection	1
Tunnel Interface 1						
NAT interface (nafvdom1)	Tunnel Interface		0.0.0.0/0.0.0.0			

4. A FortiExtender profile and data plan can be set up per VDOM.

Edit FortiExtender Profile

Name: FXA11F-wanext-default
 Model: FXA11F
 Mode: WAN extension
 Data plan:

Extender Management

Management access:
 ☒ Ping
 ☒ Telnet
 ☐ HTTP
 ☐ HTTPS
 ☐ SSH
 ☐ SNMP

FortiExtender login password ?

Modem \$1

Default SIM:

SIM1 PIN: ☐

SIM2 PIN: ☐

GPS: ☒

Auto SIM switch:

By disconnecting: ☐

Managed FortiExtenders Profiles Data Plans								
+ Create new Edit Delete + Search								
Name	Modem	Slot/Carrier/ICCID	APN	Capacity	Monthly Cost	Billing Date	Type	Ref.
 Bell-v1	all	Bell	pda.bell.ca	500	0	1	Carrier	0
 Rogers-v1	all	Rogers	Itemobile.apn	200	0	1	Carrier	0

CLI operating procedures

1. Set up the interface to discover FortiExtender in the VDOM.

```
config system interface
  edit "lan2"
    set vdom "vdom1"
    set ip 192.168.4.99 255.255.255.0
    set allowaccess ping fabric
    set type hard-switch
    set snmp-index 32
  next
end
```

2. Create a FortiExtender type interface in the VDOM.

```
config system interface
  edit "fext-vdom1"
    set vdom "vdom1"
    set mode dhcp
    set type fext-wan
    set role wan
    set snmp-index 34
  next
end
```

3. Authorize the discovered FortiExtender and bond the FortiExtender type interface.

```
config extension-controller extender
  edit "FX004TQ21000005"
    set id "FXA11FTQ21000005"
    set authorized enable
    set device-id 1
    set extension-type wan-extension
    set profile "FXA11F-wanext-default"
    config wan-extension
      set modem1-extension "fext-vdom1"
    end
  next
end
```

4. Check the IP and gateway from the FortiExtender interface.

```
FortiGate-81E-POE (vdom1) # get system interface | grep fext-vdom1
== [ fext-vdom1 ]
name: fext-vdom1   mode: dhcp   ip: 10.197.73.229 255.255.255.252   status: up
```

```

netbios-forward: disable    type: fext-wan    netflow-sampler: disable    sflow-sampler:
disable    src-check: enable    explicit-web-proxy: disable    explicit-ftp-proxy:
disable    proxy-captive-portal: disable    mtu-override: disable    drop-overlapped-
fragment: disable    drop-fragment: disable

```

```

FortiGate-81E-POE (vdom1) # 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
       V - BGP VPNv4
       * - candidate default

```

```

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 10.197.73.230, fext-vdom1, [1/0]
C       10.197.73.228/30 is directly connected, fext-vdom1
C       192.168.4.0/24 is directly connected, lan2

```

5. Modify the FortiExtender profile.

```

config extension-controller extender-profile
  edit "FXA11F-wanext-default"
    set id 4
    set model FXA11F
    set allowaccess ping telnet
    config cellular
      config sms-notification
      end
      config modem1
      end
    end
  next
end

```

6. Create a FortiExtender data plan.

```

config extension-controller dataplan
  edit "Rogers-v1"
    set type carrier
    set carrier "Rogers"
    set apn "ltemobile.apn"
    set capacity 200
  next
end

```

Discover a FortiExtender unit

For a FortiGate acting as the access controller (AC) to discover a FortiExtender unit, the FortiGate must be able to reach the FortiExtender. There are two ways in which a FortiExtender with the factory default configuration can be discovered by a FortiGate:

- Broadcast
- Static IP

Broadcast

The FortiExtender can be discovered when sending broadcast traffic in its local subnet. In this case, the FortiGate and the FortiExtender must be in the same subnet. The interfaces specified in "discovery-intf" configured on the FortiExtender should include the interface that can reach out to the FortiGate, as shown in the example below:

```
config system management fortigate
    set ac-discovery-type broadcast
    set discovery-intf lan port4
end
```

Static

The FortiExtender sends discover requests to a preconfigured IP address on the FortiGate. You can specify multiple FortiGates in IPv4-address or FQDN format. The FortiExtender will choose one that it can reach and connect. You can specify up to 16 FortiGate entries in the configuration. See the following example:

```
config system management fortigate
    set ac-discovery-type static
    config static-ac-addr
        edit 1
            set server 192.168.1.99
        next
        edit 2
            set server fortinet.com
        next
    end
    set discovery-intf lan port4
end
```

From the FortiGate, configure the interface used for discovery and set `allowaccess` to `fabric` and `ping`:

```
config system interface
    edit "lan"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
        set allowaccess ping https ssh fgfm fabric
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 21
    end
```

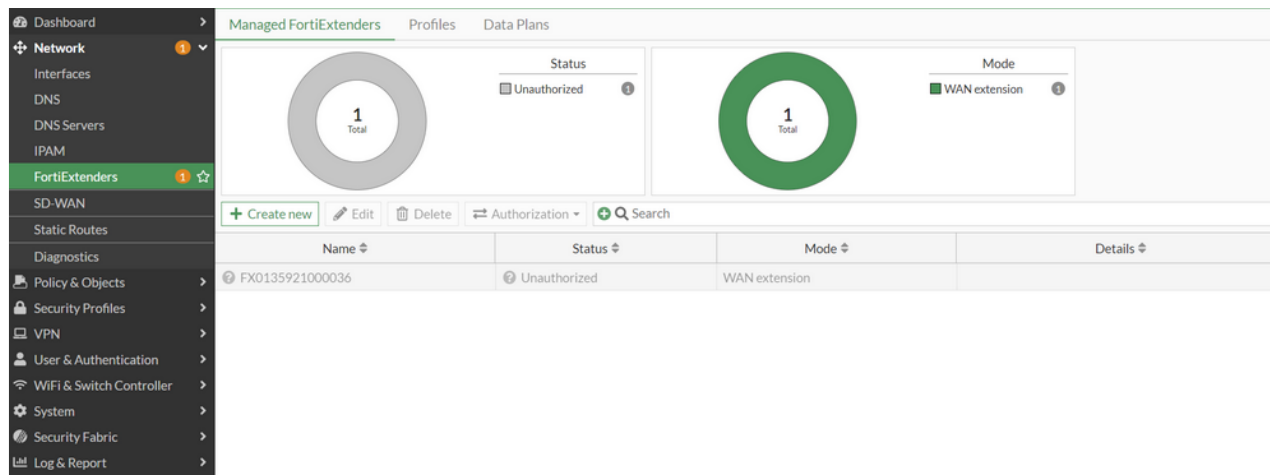
```
    next
end
```

De-authorize FortiExtender devices

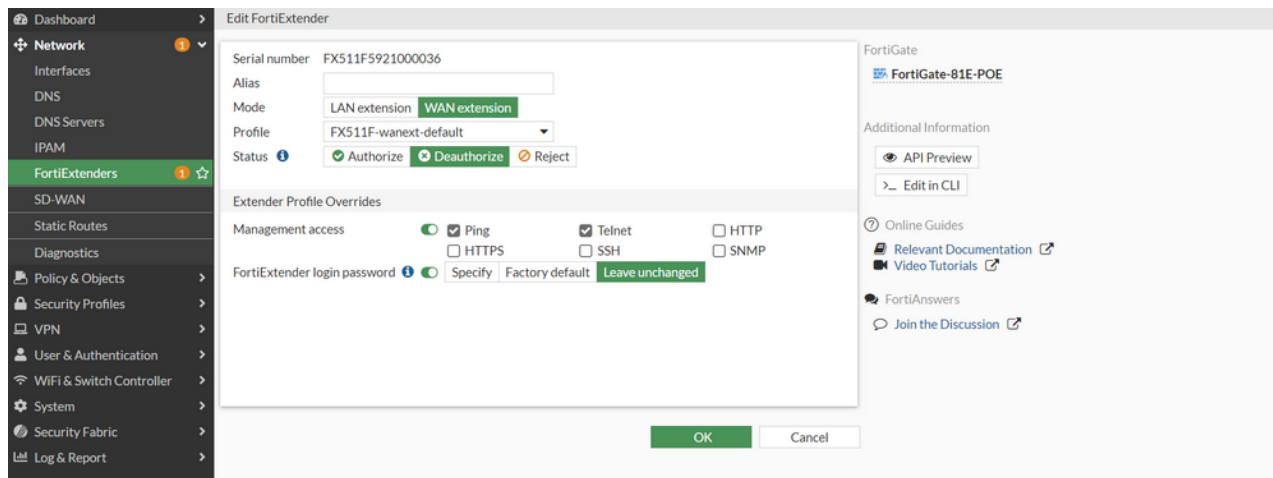
FortiExtenders discovered by the FortiGate configured as a controller used to show up on the FortiGate GUI as pending authorization, causing confusion in certain situations. This enhancement enables you to disable a discovered FortiExtender device on a FortiGate configured as a FortiExtender controller from the GUI or the CLI.

GUI

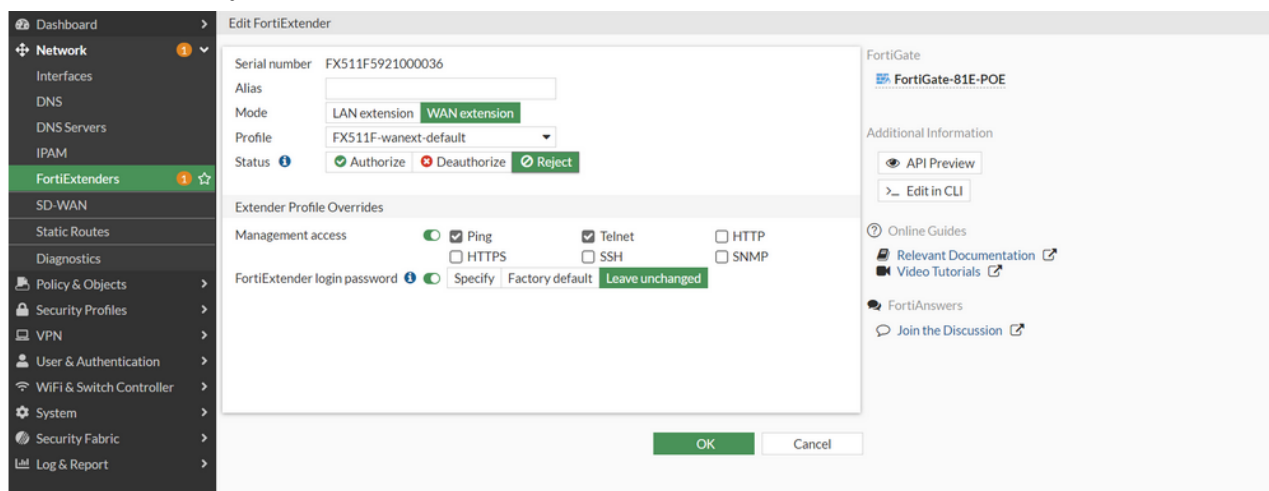
1. Locate the FortiExtender in "Unauthorized" status.



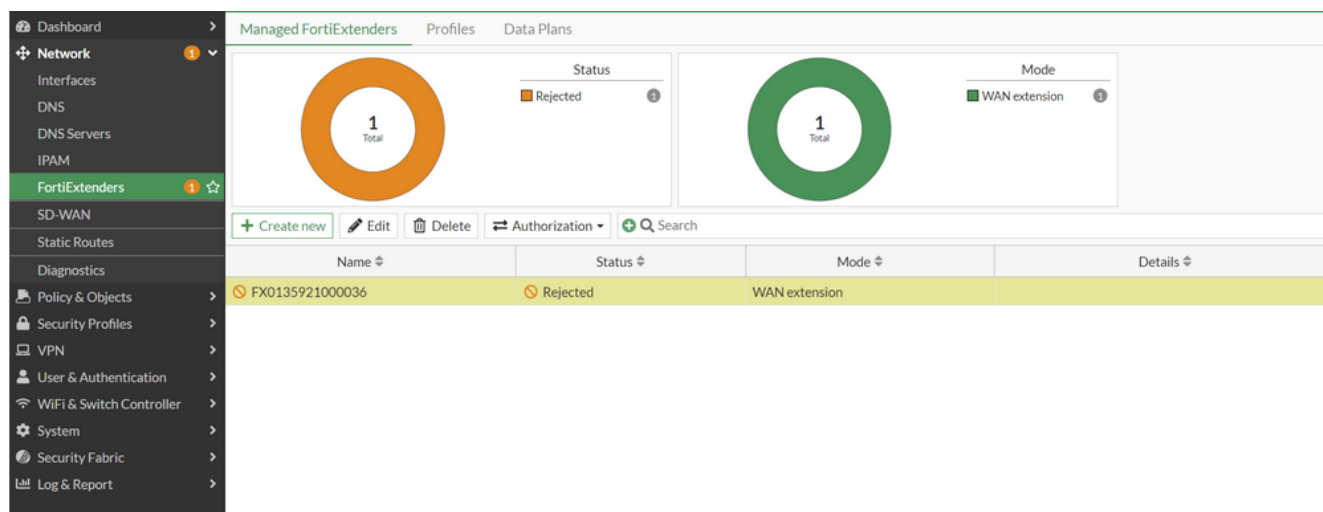
2. Select the FortiExtender and click "Edit". Note: The original status is "Deauthorized"



3. Set the status to "Reject", and click OK.



The following image shows the status of the FortiExtender after it is being rejected.



CLI

When the FortiExtender is in "discovered" state.

```
config extension-controller extender
edit "FX0135921000036"
set id "FX511F5921000036"
set authorized discovered
```

You can change it to "disable" state. It will be shown as "Reject" in the GUI.

```
config extension-controller extender
edit "FX0135921000036"
set id "FX511F5921000036"
set authorized disable
```

The default FortiExtender profile

In some circumstances, a default profile (or 2 default profiles) will be automatically generated.

The profile or profiles are generated based on the FortiExtender model. For FortiExtender models without LTE/5G modems, such as FortiExtender 200F, FortiGate will generate a LAN extension profile as follows:

```
config extension-controller extender-profile
  edit "FX200F-lanext-default"
    set id 0
    set model FX200F
    set extension lan-extension
    config lan-extension
      set link-loadbalance loadbalance
      set ipsec-tunnel "fext-ipsec-WrXw"
      set backhaul-interface "port2"
      config backhaul
        edit "1"
          set port port1
        next
        edit "2"
          set port port2
        next
      end
    end
  next
end
```

In this default FortiExtender 200F profile, there are two default backhaul ports: port1 and port2. It indicates that the FortiExtender 200F will use its port1 and port2 for the uplinks connected to the FortiGate. The underlying data transportation will be VLAN over IPsec, which is transparent to users.

These two ports will be linked as an aggregated interface in the FortiExtender and you can specify load-balance mode on it. More detailed LAN extension configuration is covered in [LAN extension configuration in a profile on page 75](#).

For FortiExtender models with LTE/5G modems, two default profiles will be generated: one for WAN extension and the other for LAN extension.

For WAN extension, the default profile with default values for FortiExtender 201E is as follows:



The following example is for illustration only.

```
config extension-controller extender-profile
  edit "FX201E-wanext-default"
    set id 2
    config cellular
      config sms-notification
      end
      config modem1
      end
    end
  end
end
```

```
        end
    next
end

# get FX201E-wanext-default (default value will be shown below)
name : FX201E-wanext-default
id : 2
model : FX201E
extension : wan-extension
allowaccess :
login-password-change: no
cellular:
    dataplan :
    controller-report:
        status : disable
    sms-notification:
        status : disable
    modem1:
        redundant-mode : disable
        conn-status : 0
        default-sim : sim1
        gps : enable
        sim1-pin : disable
        sim2-pin : disable
        auto-switch:
            disconnect : disable
            signal : disable
            dataplan : disable
            switch-back :
                switch-back-time : 00:01
                switch-back-timer : 86400
```

For the LAN extension, the default profile for the FortiExtender 201E generated on the FortiGate would look as follows.
For details of LAN extension configuration, go to [LAN extension configuration in a profile on page 75](#).

```
config extension-controller extender-profile
    edit "FX201E-lanext-default"
        set id 3
        set extension lan-extension
        config cellular
            config sms-notification
            end
            config modem1
            end
        end
    config lan-extension
        set ipsec-tunnel "fext-ipsec-ut4Z"
        set backhaul-interface "lan"
        config backhaul
            edit "1"
                set port wan
                set role primary
            next
            edit "2"
                set port ltel
                set role secondary
            next
        end
    end
end
```

```
        end
    end
next
end

# get FX201E-wanext-default (default value will be shown below)
name : FX201E-lanext-default
id : 3
model : FX201E
extension : lan-extension
allowaccess :
login-password-change: no
enforce-bandwidth : disable
cellular:
    dataplan :
    controller-report:
        status : disable
    sms-notification:
        status : disable
    modem1:
        redundant-mode : disable
        conn-status : 0
        default-sim : sim1
        gps : enable
        sim1-pin : disable
        sim2-pin : disable
        auto-switch:
            disconnect : disable
            signal : disable
            dataplan : disable
            switch-back :
            switch-back-time : 00:01
            switch-back-timer : 86400
lan-extension:
    link-loadbalance : activebackup
    ipsec-tunnel : fext-ipsec-ut4Z
    backhaul-interface : lan
    backhaul-ip :
    backhaul:
        == [ 1 ]
        name: 1
        == [ 2 ]
        name: 2
```



After upgrading to 7.0.2 or later from 3.2, the default behavior is "unset allowaccess" to prevent direct management of the FortiExtender by anything other than the FortiGate. If you want to exert some direct control over the device, you can change the default behavior using the following CLI commands:

```
config extension-controller extender-profile
    edit "FX211E-wanext-default"
        set allowaccess ping https
        set login-password-change no
    end
```

Allowaccess for FortiExtender management

The allowaccess configuration controls the types of traffic that the FortiExtender uplink interface is allowed to send to the FortiGate. There are six options that you can configure as needed:

- Ping
- Telnet
- HTTP
- HTTPS
- SSH
- SNMP

```
config extension-controller extender-profile
    edit "FX201E-lanext-default"
        set allowaccess ping telnet http https ssh snmp
    next
end
```

Each FortiExtender associated with this profile has the same allowaccess settings specified in the profile. However, it can also be overridden per device. For example, the following FortiExtender will use the allowaccess specified in the extender entry instead of the one specified in the profile, "FX201E-lanext-default".

```
config extension-controller extender
    edit "FX0015919000027"
        set id "FX201E5919000027"
        set authorized enable
        set extension-type lan-extension
        set override-allowaccess enable
        set allowaccess ping telnet
        set profile "FX201E-lanext-default"
    next
end
```

Set bandwidth limit for LAN extension

Just like `allowaccess` and `login password`, the bandwidth limit for the LAN extension can be configured in a profile, and can also be overridden in an extender entry.

```
config extension-controller extender-profile
  edit "FX200F-lanext-default"
    set model FX200F
    set extension lan-extension
    set enforce-bandwidth [enable|disable]
    set bandwidth-limit 1000 // only shown when enforce-bandwidth is enable
    config lan-extension
      ...
    end
  end
config extension-controller extender
  edit "FX0015919000027"
    set id "FX201E5919000027"
    set authorized enable
    set extension-type lan-extension
    set override-enforce-bandwidth [enable|disable] // override the profile setting
    set enforce-bandwidth [enable|disable]
    set bandwidth-limit 1003 // only shown when enforce-bandwidth is enable
    set profile "FX201E-lanext-default"
  next
end
```

Parameter	Description
<code>enforce-bandwidth</code> <code>[enable disable]</code>	Enable/Disable the enforcement of bandwidth limit on the LAN extension interface.
<code>bandwidth-limit</code> <code><integer></code>	Set the FortiExtender LAN extension interface bandwidth limit in Mbps. The range is from 1 to 16776000.

Once it is configured, the FortiExtender will have the "shaper" configuration as shown in the example below, and it can have bandwidth limit with the configuration. The terms "le-traffic-shaper" and "le-shaping-policy" are predefined, and will be created in the FortiExtender.

```
config firewall shaper traffic-shaper
  edit le-traffic-shaper
    set max-bandwidth 1024 // set bandwidth-unit mbps
  next
end
config firewall shaping-policy
  edit le-shaping-policy
    set status enable
    set dstintf le-agg-link
    set traffic-shaper le-traffic-shaper
  next
end
```

Configure FortiExtender admin password

You can configure the admin login password of a FortiExtender via the FortiGate console. Similar to allowaccess, it can be configured in a profile and also can be overridden in an extender entry.

```
config extension-controller extender
edit "FX201E0123456789"
    set override-login-password-change [enable|disable]
    set login-password-change [yes|default|no]
    set login-password <string>
next
end
config extension-controller extender-profile
edit "FX201E-default"
    set login-password-change [yes|default|no]
    set login-password <string>
next
end
```

Parameter	Description
set login-password-change [yes default no]	Use one of the following options: • yes — Change the administrator login password of the FortiExtender. • default — Keep the managed administrator login password set to the factory default. • no — Do not change the administrator login password.
set override-login-password-change [enable disable]	Enter either of the following: • enable — Override the administrator login password setting in the profile. • disable — Use the administrator login password setting in the profile.
set login-password <string>	Set the administrator login password of the managed FortiExtender.



In earlier releases of FortiOS, there is a "set login-password" command in the extender entry, but there are no "login-password-change" and "override-login-password-change" attributes. If you have configured your administrator login password in an earlier version of FortiOS, the "login-password-change" attribute will be set to "yes" and your login-password will remain the same as before after upgrade.

Discovery response lockdown

By default, FortiGate automatically generate a FortiExtender entry if a newly added FortiExtender discovers it, that is to say when the FortiExtender is sending a discovery request.

In order to prevent rogue devices from detecting or scanning the FortiGate, you can enable "`fortiextender-discovery-lockdown`" to ensure that the discovery response is sent to a pre-authorized device only.

Once enabled, the FortiGate will not automatically generate an extender entry when a newly discovered FortiExtender joins the network. Instead, it will only accept discovery request from a pre-authorized extender entry. By default, "`fortiextender-discovery-lockdown`" is disabled. You can enable it using the following command:

```
config system global
    set fortiextender-discovery-lockdown enable
end
```

Wildcard

In some cases, you may not know the ID (i.e., serial number) of a FortiExtender, but still intend to pre-create an extender entry in the FortiGate for easy deployment. You can use the wildcard * (asterisk) in the "id" attribute when manually creating an extender entry.

The rule for using wildcard is to have a 6-digit model name followed by 10 * (asterisks).

Below are the 6-digit model names of FortiExtender devices:

- FX201E
- FX211E
- FX200F
- FXA11F
- FXE11F
- FXA21F
- FXE21F
- FXA22F
- FXE22F
- FX212F
- FX311F
- FX312F
- FX511F
- FVG21F
- FVA21F
- FVG22F
- FVA22F
- FX04DA

Take FX200F for example. You can configure as follows:

```
config extension-controller extender
  edit <entry> << any entry name you like (less than 15 characters)>
    set id FX200F*****
    set extension lan-extension
    set profile "FX200F-lanext-default"
  next
end
```

You can also pre-authorize the entry as well, as shown below:

```
config extension-controller extender
  edit <entry>
    set authorized enable
    set id FX200F*****
    set extension lan-extension
    set profile "FX200F-lanext-default"
  next
end
```

Whenever a new FX200F joins (assuming its serial number is FX200F5919000001), the FortiGate will select the extender entry and replace the "id" with its serial number. If there are more than two wildcard entries with the same model, it will choose the one that has "set authorized" enabled because of its higher priority.

```
config extension-controller extender
  edit entry1
    set id FX201E*****
    set extension lan-extension
    set profile "FX201E-lanext-default"
  next
  edit entry2
    set authorized enable
    set id FX200F5919000001
    set extension lan-extension
    set profile "FX201E-lanext-default"
  next
end
```

Data transportation over the LAN extension interface

FortiGate automatically generates a "lan-extension" interface for each FortiExtender that it has authorized. The name of the interface is the same as the FortiExtender entry name.

```
config extension-controller extender
    edit "FX0015919000027"
        set id "FX201E5919000027"
        set authorized enable
        set device-id 1
        set extension-type lan-extension
        set override-allowaccess enable
        set profile "FX201E-lanext-default"
    next
end
config system interface
    edit "FX0015919000027"
        set vdom "root"
        set type lan-extension
        set role lan
        set snmp-index 26
        set interface "fext-ipsec-ut4Z"
    next
end
```

This interface is the virtual interface that abstracts all the details of the underlying transportation tunneling protocol. You can view the interface as a LAN interface in the FortiGate. Unlike a real LAN interface, this "lan-extension" interface will connect the FortiExtender across the internet.

It is transparent to users to provide a reliable, secure interface. For example, you can configure the "ip" of this interface and enable DHCP server on it.

```
config system interface
    edit "FX0015919000027"
        set vdom "root"
        set ip 192.168.3.99 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
        set type lan-extension
        set role lan
        set snmp-index 26
        set interface "fext-ipsec-ut4Z"
    next
end
config system dhcp server
    edit 3
        set default-gateway 192.168.3.99
        set netmask 255.255.255.0
        set interface "FX0015919000027"
        config ip-range
            edit 1
                set start-ip 192.168.3.2
                set end-ip 192.168.3.98
            next
        next
    next
end
```

```
        end
    next
end
```

An appropriate firewall policy can be used to forward traffic out of the FortiGate's WAN interface. Suppose that "wan1" is the WAN interface of the FortiGate, you can configure it as follows. You can also apply a more strict firewall policy based on your need.

```
config firewall policy
    edit 1
        set name "LAN-EXT"
        set uuid 8b7c21e4-221e-51ec-0a0d-34e7b478557b
        set srcintf "FX0015919000027"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

On the FortiExtender side, the "lan" interface will be mapped to the "lan-extension" interface on the FortiGate. You can have computers directly connected to any of the LAN ports on the FortiExtender, or have a switch between the LAN and the computers. The computers will get IPs from the DHCP server configured in "lan-extension" interface and can forward traffic out through the FortiGate based on the firewall policy.

LAN extension configuration in a profile

The following example shows the "lan-extension" configuration in a default LAN extension profile.

```
FortiGate (extender-profile) # get FX200F-lanext-default
name : FX200F-lanext-default
id : 4
model : FX200F
extension : lan-extension
allowaccess :
login-password-change: no
enforce-bandwidth : enable
bandwidth-limit : 200
lan-extension:
link-loadbalance : loadbalance
ipsec-tunnel : fext-ipsec-rthk
backhaul-interface : lan
backhaul-ip :
backhaul:
== [ 1 ]
name: 1
== [ 2 ]
name: 2
```

Parameter	Description
name	The profile name
id	The profile ID (for system internal record)
model	The FortiExtender model for the profile
extension [lan-extension wan-extension]	The extension type for the profile
alloweaccess [telent http https snmp ping ssh]	The multi-option setting for the lan-extension switch interface of the FortiExtender. For more details, see Allowaccess for FortiExtender management on page 67 .
login-password-change [yes no default]	The setting of the admin password of the FortiExtender. For more details, see Configure FortiExtender admin password on page 69
enforce-bandwidth [enable disable]	Enable or disable enforcement of bandwidth limit. Note: "enforce-bandwidth", which is disabled by default, is used to limit the egress bandwidth used to send traffic from the FortiExtender. For more details, see Set bandwidth limit for LAN extension on page 68 .
bandwidth-limit	Specify the bandwidth limit.

Parameter	Description
link-loadbalance [activebackup loadbalance]	Two ports are configured for the FortiExtender for load-balancing. For <code>activebackup</code> mode, you can configure <code>"role"</code> (primary or secondary) on the two backhaul ports. For <code>loadbalance</code> mode, you can configure <code>"weight"</code> on each backhaul port.
ipsec-tunnel	This is the IPsec tunnel interface that will be used in underlying data transportation. It provide secure connection between the FortiExtender and the FortiGate. This entry will be auto-generated.
backhaul-interface	This is the egress interface for data transportation between the FortiGate and the other FortiExtenders using this profile. The default will be automatically filled with the interface that is used to manage the FortiExtender. You can configure it based on your network topology.
backhaul-ip	This is used for the FortiGate behind a NAT device (or DNAT, LoadBalancer, etc.). The <code>"backhaul-ip"</code> is the external IP of the NAT device. For details, see Backhaul IP in LAN extension on page 77 .

The following is an example of a backhaul configuration:

```
FortiGate (backhaul) # edit 1
FortiGate (1) # get
name : 1
port : port1
weight : 1
```

If link-loadbalance is configured as `"activebackup"`, the following will be shown:

```
name : 1
port : port1
role : primary
```

Parameter	Description
name	The name of the backhaul entry.
port	The port on the FortiExtender that sends traffic to the FortiGate in LAN extension.
weight	Enter the weight if the link-loadbalance is configured as <code>"loadbalance"</code> .
role [primary secondary]	Specify whether the port is primary or secondary.

Backhaul IP in LAN extension

There is one optional `backhaul-ip` configuration in FortiGate to be used in the case that FortiGate is behind a NAT. The `backhaul-ip` is the external IP used in this NAT device. Both the FortiExtender and the FortiGate need to be aware of this `backhaul-ip`. On the FortiExtender, it needs to specify in its discovery static IP.

On the FortiExtender

```
config system management fortigate
  set ac-discovery-type static
  config static-ac-addr
    edit 1
      set server <backhaul-ip>
    next
  end
end
```

On the FortiGate:

```
config extension-controller extender-profile
  edit "FX200F-lanext-default"
    config lan-extension
      set backhaul-ip <backhaul-ip>
    end
  next
end
```



The NAT device needs to have port mapping/forwarding configuration, which is beyond the scope of this document.

Fast failover of CAPWAP control channel between two uplinks

When a FortiExtender is configured as a FortiGate LAN extension and has two uplinks to the FortiGate access controller (AC), the system is able to perform a fast failover of the CAPWAP LAN extension control channel. Two CAPWAP sessions are established between the FortiGate and the FortiExtender: one is active and the other is standby. When the active uplink goes down, the CAPWAP LAN extension control channel changes to use the other standby uplink quickly. When the previously active uplink comes back up, the CAPWAP LAN extension control channel continues to use the previously standby uplink used for the failover event as the control channel.

To display the active and standby sessions for the CAPWAP LAN extension control channel on the FortiGate:

1. Execute the CLI command `get extender session-info`.

In the CLI output, the active session is marked as `lan-extension` and the standby session is marked as `secondary`.

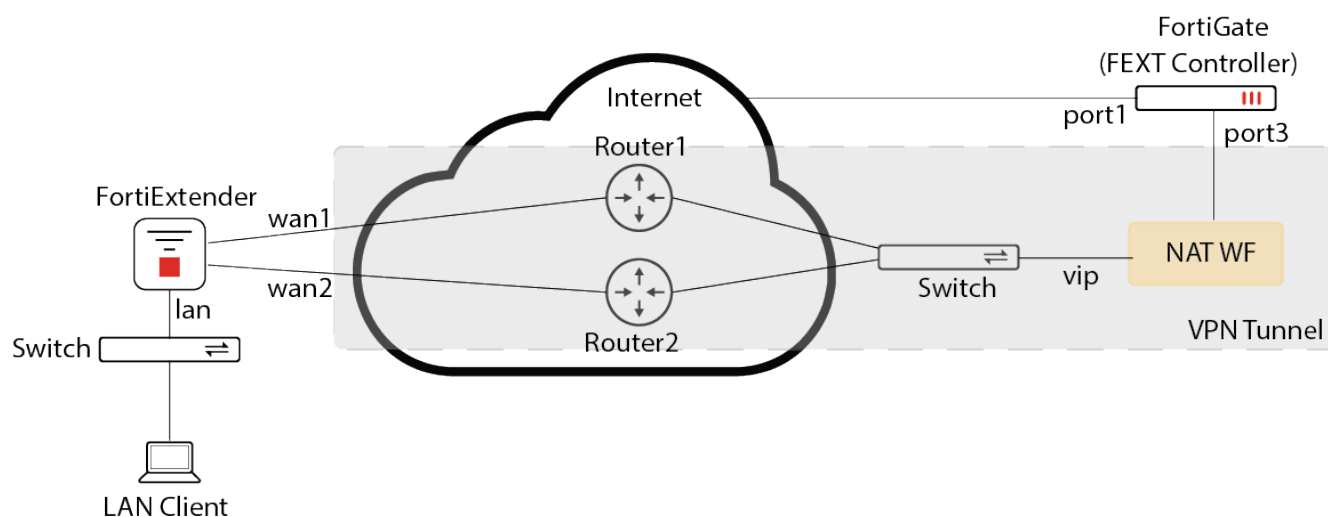
To display the active and standby sessions for the CAPWAP LAN extension control channel on the FortiExtender:

1. Execute the CLI command `get extender status`.

In the CLI output, the active and standby sessions and the uplink ports are displayed when both uplinks are up; only the active session and the uplink port are displayed when a single uplink is up.

Topology

In the following diagram, the FortiGate (FEXT controller) port3 has the CAPWAP control channel to the FortiExtender (uplinks wan1 and wan2). The FortiExtender-200F port1 and port2 stand for wan1 and wan2.



CLI

The following CLI outputs show the configuration of the uplink failover event and how this new feature works.

1. Once the FortiExtender has two uplinks (port1, port2) that can reach the FortiGate, two CAPWAP sessions are established. One of them is the CAPWAP control channel (5246).

*** FGT console displays two extender sessions, one of which works as lan-extension control channel.

```
FortiGate-501E # get extender session-info
Total 2 WS sessions, 0 AS sessions:
fg connectors:
extender sessions:
FX00300000000000 : 3.3.3.1:60440 (dport 65535) seconadry, running, install,
data-enable, refcnt 5, miss_echos -1, up-time 363 secs, change 1
FX00300000000000 : 3.3.3.1:5246 (dport 47997) lan-extension, running, install,
data-enable, refcnt 7, miss_echos -1, up-time 2216 secs, change 0
```

*** FEXT console displays CAPWAP channel with active session (port1) and standby session (port2):

```
FX200F00000000000 # get extender status
Extender Status
  name           : FX200F00000000000
  mode           : CAPWAP
  session        : active
    fext-addr     : 5.5.5.1
    ingress-intf  : port1
    controller-addr : 1.1.1.10:5246
    controller-name : FG5H1E5818904105
    uptime       : 0 days, 0 hours, 36 minutes, 31 seconds
    management-state : CWWS_RUN
  session        : standby
    fext-addr     : 6.6.6.1
    ingress-intf  : port2
    controller-addr : 1.1.1.10:5246
    controller-name : FG5H1E5818904105
    uptime       : 0 days, 0 hours, 5 minutes, 38 seconds
    management-state : CWWS_RUN
  base-mac       : E8:1C:BA:C4:4E:B1
  network-mode   : lan-extension
  fgt-backup-mode : backup
  discovery-type  : static
  discovery-interval : 5
  echo-interval   : 30
  report-interval : 30
```

```

statistics-interval : 120
mdm-fw-server       : fortiextender-firmware.forticloud.com
os-fw-server        : fortiextender-firmware.forticloud.com
FX200F0000000000 #

```

2. Once the active uplink (port1) is down, the secondary session becomes the CAPWAP control channel (60440).

*** FGT console displays remaining extender session as lan-extension control channel.

```
FortiGate-501E # get extender session-info
```

```

Total 1 WS sessions, 0 AS sessions:
fg connectors:
extender sessions:
FX00300000000000 : 3.3.3.1:60440 (dport 36583) lan-extension, running, install,
data-enable, refcnt 7, miss_echos -1, up-time 481 secs, change 0

```

*** FEXT console displays CAPWAP channel with active session (port2):

```

FX200F0000000000 # get extender status
Extender Status
name           : FX200F0000000000
mode           : CAPWAP
session        : standby
  fext-addr     : 0.0.0.0
  ingress-intf  :
  controller-addr : 1.1.1.10:5246
  controller-name : FG5H1E5818904105
  management-state : CWWS_DISCOVERY
session        : active
  fext-addr     : 6.6.6.1
  ingress-intf  : port2
  controller-addr : 1.1.1.10:5246
  controller-name : FG5H1E5818904105
  uptime        : 0 days, 0 hours, 7 minutes, 56 seconds
  management-state : CWWS_RUN
base-mac       : E8:1C:BA:C4:4E:B1
network-mode   : lan-extension
fgt-backup-mode : backup
discovery-type : static
discovery-interval : 5
echo-interval  : 30
report-interval : 30
statistics-interval : 120
mdm-fw-server  : fortiextender-firmware.forticloud.com
os-fw-server   : fortiextender-firmware.forticloud.com
FX200F0000000000 #

```

3. Once the uplink (port1) is recovered, the FortiGate console displays two extender sessions. The lan-extension control channel has no change (still via port2 on FEXT).

*** FGT console displays two extender sessions, one of which works as lan-extension control channel.

```
FortiGate-501E # get extender session-info
```

```
Total 2 WS sessions, 0 AS sessions:
```

```
fg connectors:
```

```
extender sessions:
```

```
FX00300000000000 : 3.3.3.1:5246 (dport 65535) seconadry, running, install,
data-enable, refcnt 5, miss_echos -1, up-time 201 secs, change 1
FX00300000000000 : 3.3.3.1:60440 (dport 36583) lan-extension, running, install,
data-enable, refcnt 7, miss_echos -1, up-time 1904 secs, change 0
```

*** FEXT console displays CAPWAP channel with active session (port2) and standby session (port1):

```
FX200F00000000000 # get extender status
```

```
Extender Status
```

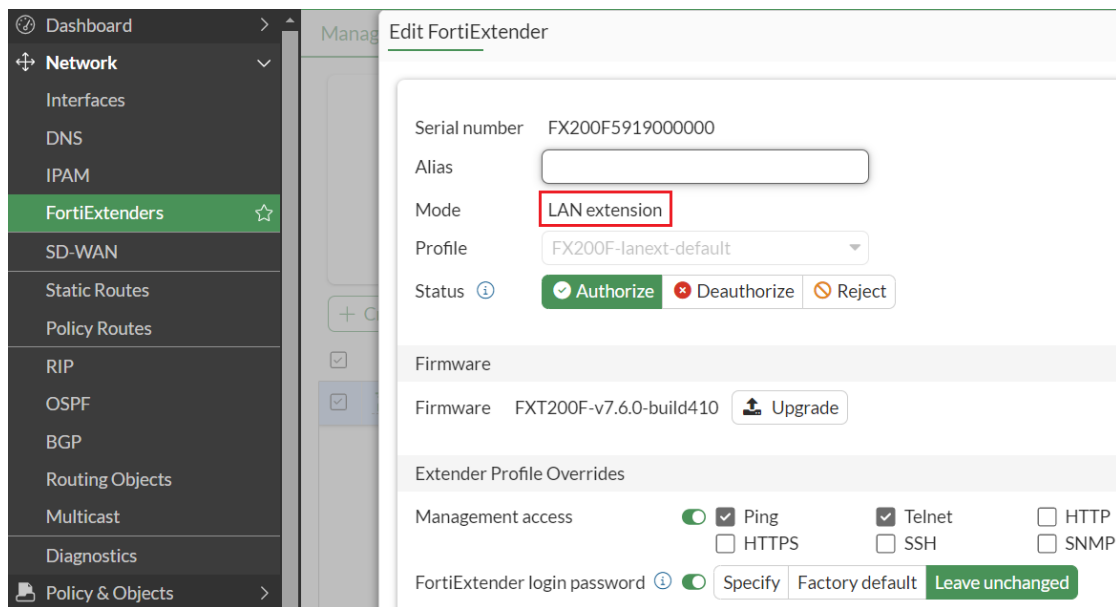
```
name           : FX200F00000000000
mode            : CAPWAP
session        : standby
  fext-addr     : 5.5.5.1
  ingress-intf  : port1
  controller-addr : 1.1.1.10:5246
  controller-name : FG5H1E5818904105
  uptime       : 0 days, 0 hours, 1 minutes, 55 seconds
  management-state : CWWS_RUN
session        : active
  fext-addr     : 6.6.6.1
  ingress-intf  : port2
  controller-addr : 1.1.1.10:5246
  controller-name : FG5H1E5818904105
  uptime       : 0 days, 0 hours, 30 minutes, 18 seconds
  management-state : CWWS_RUN
base-mac       : E8:1C:BA:C4:4E:B1
network-mode   : lan-extension
fgt-backup-mode : backup
discovery-type : static
discovery-interval : 5
echo-interval  : 30
report-interval : 30
statistics-interval : 120
mdm-fw-server  : fortiextender-firmware.forticloud.com
os-fw-server   : fortiextender-firmware.forticloud.com
FX200F00000000000 #
```

VLAN support for LAN-extension mode

You can configure VLAN (Virtual Local Area Network) support on FortiExtender in LAN extension mode through the FortiGate LAN extension profile. Once you add the VLAN configurations to the LAN extension profile, FortiGate then synchronizes the VLAN configurations to the FortiExtender and the FortiExtender applies the VLAN configuration to the soft switch. Clients from a different port in the LAN switch can set a dedicated VLAN ID and the FortiGate Access Controller can apply a dedicated firewall policy for each VLAN interface.

To configure VLAN support - GUI:

1. From the FortiGate, go to *Network > FortiExtenders* and configure the FortiExtender to run in LAN extension mode.



2. Go to *Network > Interfaces* and add VLAN interfaces to the LAN extension interface.
 - a. Click *Create new* and configure the following:
 - In *Interface*, select the FortiExtender LAN extension interface you created.
 - In *VLAN ID (pvid)* enter the corresponding value.
 - Enter the *IP/Netmask*.
 - If needed, configure the DHCP server. DHCP servers are enabled in these VLAN interfaces and will

provide IP and gateway addresses to clients behind the FortiExtender.

New Interface

Type: VLAN

VLAN protocol: 802.1Q 802.1AD

Interface: FV018TF23000011

VLAN ID: 200

Role: LAN

Address

Addressing mode: Manual IPAM DHCP PPPoE One-Arm Sniffer

IP/Netmask: 192.168.200.1/255.255.255.0

Create address object matching subnet: ☒

Name: vlan200 address

Destination: 192.168.200.0/24

Secondary IP address: ☐

Administrative Access

IPv4:

- ☐ SCIM
- ☐ PING
- ☐ SNMP
- ☐ Security Fabric Connection
- ☐ HTTPS
- ☐ FMG-Access
- ☐ FTM
- ☐ Speed Test
- ☐ HTTP
- ☐ SSH
- ☐ RADIUS Accounting

☒ **DHCP Server**

DHCP status: Enabled Disabled

Address range: 192.168.200.2-192.168.200.254

OK Cancel

- When you are finished, click **OK** to save.

Interfaces	+ Create new + Search			
	Name	Type	Members	IP/Netmask
802.3ad Aggregate 1				
	fortilink	802.3ad Aggregate		Dedicated to FortiSwitch
LAN Extension 3				
	FX0035919000000	LAN Extension		172.31.0.254/255.255.255.0 (IPAM)
	v201	VLAN		21.21.21.99/255.255.255.0
	v401	VLAN		41.41.41.99/255.255.255.0
Physical Interface 19				
	ha	Physical Interface		0.0.0.0/0.0.0.0
	mgmt	Physical Interface		10.6.30.103/255.255.255.0

- Go to **Network > FortiExtenders** and edit the FortiExtender *Profile*.
- Under **LAN extension > FortiExtender downlink**, click **Create new** to create a new downlink.

Manage Edit FortiExtender Profile

LAN extension

IPsec interface IP/FQDN 1.1.1.10

IPsec tunnel fext-ipsec-QdzC

FortiExtender uplink port

+ Create New Edit Delete

☐	Name	Uplink port	Weight
☐	1	port1	1
☐	2	port2	1

FortiExtender downlink

+ Create new Edit Delete

☐	Name	Interface	VLAN ID
☐	downlink-v201	port4	201
☐	downlink-v401	port5	401

6. Select the *Interface* and enter the *VLAN ID* you want to bind to the FortiExtender LAN switch port.

Manage Edit FortiExtender downlink

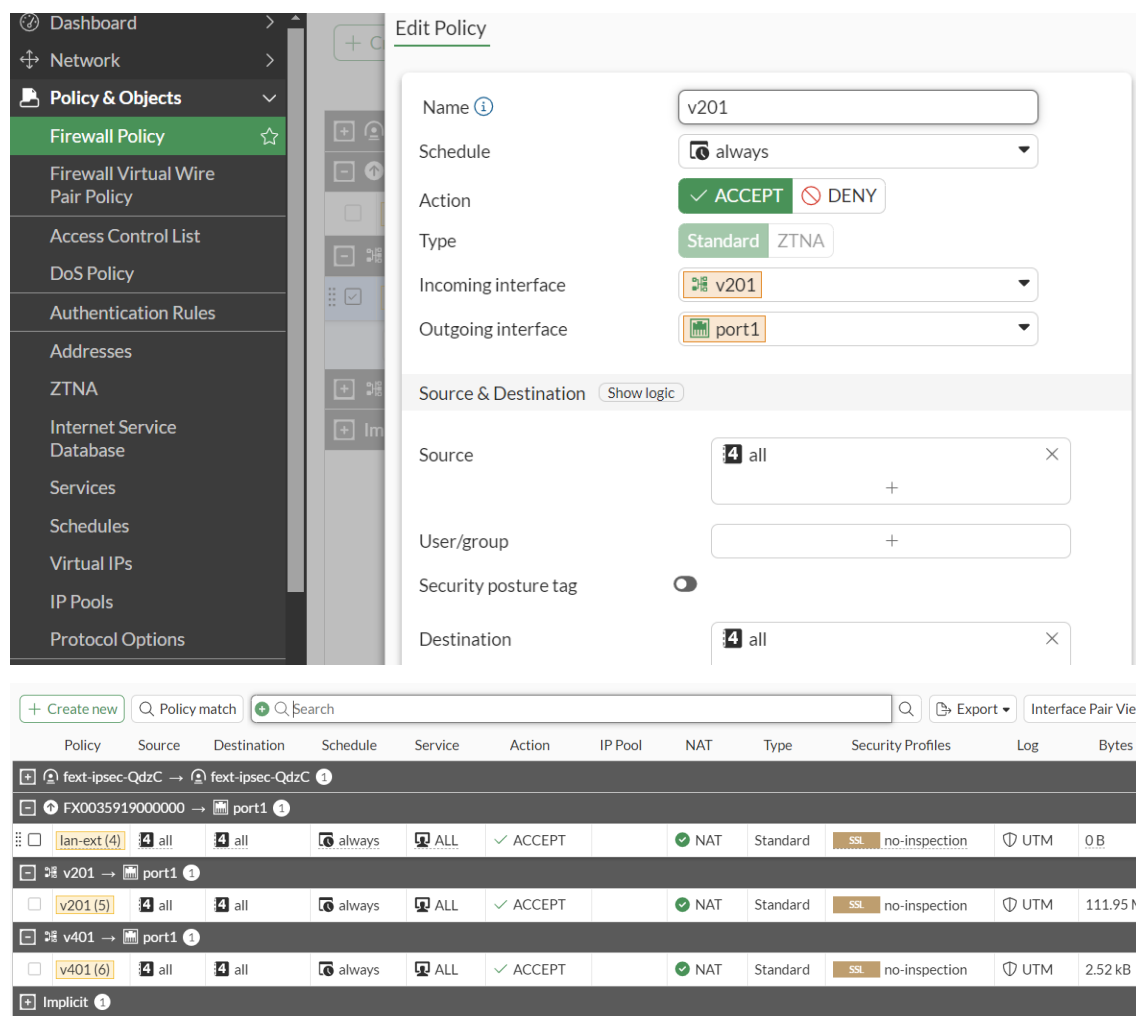
Name downlink-v201

Type Physical port

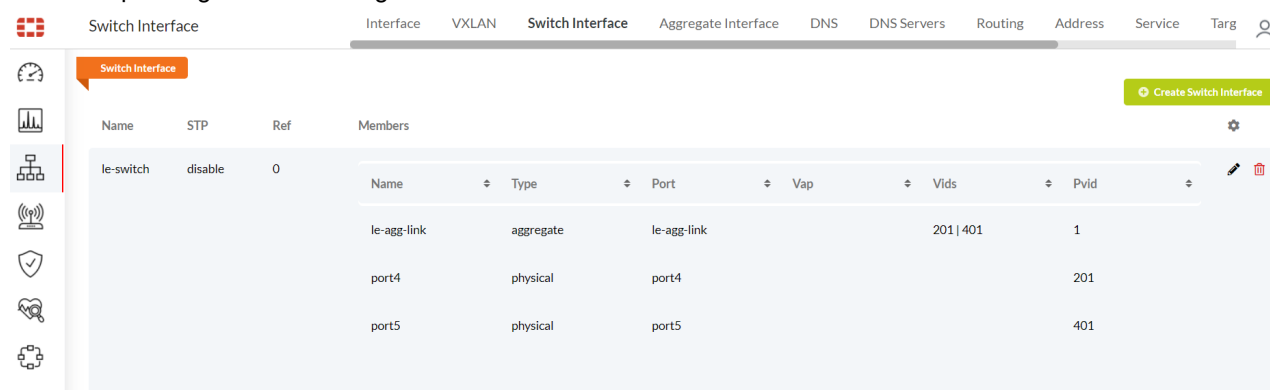
Interface port4

VLAN ID 201

7. When you are finished, click **OK**.
8. In the FortiGate Access Controller, go to *Policy & Objects > Firewall Policy* and create a firewall policy for each VLAN interface designated as a downlink.



9. When you are done configuring on the FortiGate Access Controller, you can check the FortiExtender device to see the corresponding downlink configurations.



To configure VLAN support - CLI:

1. From the FortiGate CLI, configure the FortiExtender downlink interface in the LAN extension profile. In this example, multiple VLAN configurations are added to set the pvid of port 2 to 200.

```

config extension-controller extender-profile
edit "FVA22F-lanext-default"
set extension lan-extension
config lan-extension
set ipsec-tunnel "fext-ipsec-5S2s"
set backhaul-interface "internal1"
config backhaul
edit "1"
set port wan
set role primary
next
edit "2"
set port ltel
set role secondary
next
end
end
config downlinks
edit "1"
set type port
set port port2
set pvid 200
next
end
end
next
end

```

Parameters	Description
config downlinks	
type	Interface type for physical ports. Set this option to <code>port</code> or <code>set to vap</code> for lan-ext-vap WiFi.
port	Set the port name. This field is not needed if <code>type</code> is set to <code>vap</code> .
vap	Virtual Access Point name. This field is not needed if <code>type</code> is set to <code>port</code> .
pvid	Port VLAN ID, ranging from 1 to 4089. Note: <code>pvid 1</code> is reserved for untagged traffic.

2. After you configure the downlink interface, manually create the VLAN interface under the FortiExtender LAN extension interface.

- a. Configure the system interface.

```

config system interface
edit "FV018TF23000011"
set vdom "root"
set ip 212.21.2.1 255.255.255.0
set allowaccess ping ssh
set type lan-extension
set role lan
set snmp-index 32
set interface "fext-ipsec-5S2s"
next

```

```

edit "vlan200"
    set vdom "root"
    set ip 192.168.200.1 255.255.255.0
    set device-identification enable
    set role lan
    set snmp-index 33
    set ip-managed-by-fortiipam disable
    set interface "FV018TF23000011"
    set vlanid 200
next
end

```

b. If needed, configure the DHCP server.

```

config system dhcp server
    edit 9
        set dns-service default
        set default-gateway 192.168.200.1
        set netmask 255.255.255.0
        set interface "vlan200"
        config ip-range
            edit 1
                set start-ip 192.168.200.2
                set end-ip 192.168.200.254
            next
        end
    next
end

```

- 3.** After configuring the extension profile in the FortiGate, the settings are automatically synced to the FortiExtender. No manual configuration is needed on the FortiExtender side.

To verify that configurations have been successful synced:

You can use the following CLI commands to check the status and VLAN ID of the switch interfaces on FortiExtender.

```

# get system switch-interface status
le-switch:
    span      : disable
    vlan support : enable
    members:
        le-agg-link
        port2
    wlan members:

# get system switch-interface vlan
port      vlan ids
le-agg-link      1 PVID Egress Untagged
                200

le-switch      1 PVID Egress Untagged

1      None
bap0   None
port2  1 Egress Untagged
        200 PVID Egress Untagged

```

Example VLAN configurations

Example 1: FortiExtender VLAN configuration syntax

The following CLI example shows a FortiExtender where the VLAN ID (`pvid`) 101 has been set to port1 and VLAN ID 102 to port 4. The aggregate port switch (`le-agg-link`) has been configured to accept all the VLAN IDs.



The FortiGate LAN extension profile must have these settings configured and synced to the FortiExtender. You cannot enable these settings directly on the FortiExtender; you must make them through the FortiGate LAN extension profile first.

```
config system switch-interface
  edit le-switch
    set vlan-support enable
    config member
      edit port1 # access port
        set type physical
        set port port1
        set vids
        set pvid 101
      next
      edit port4 # access port
        set type physical
        set port port4
        set vids
        set pvid 102
      next
      edit le-agg-link # trunk port
        set type aggregate
        set port le-agg-link
        set vids 101 102
        set pvid 0
      next
    end
    set stp disable
  next
end
```

Parameter	Description
<code>config system switch-interface</code>	
<code>vlan-support</code>	Enable/disable VLAN support.
<code>config member</code>	
<code>type</code>	Interface type.
<code>port</code>	Interface within the virtual switch.
<code>vap</code>	Virtual Access Point, which must NOT be configured as a WLAN bridge, will be added as a member of the switch-interface.

Parameter	Description
vids	VLAN ID list, ranging from 1 to 4089.
pvid	Port VLAN ID, ranging from 1 to 4089.

Example 2: FortiOS LAN extension profile with no PVID downlink interface settings

If the PVIDs are not configured in the FortiGate downlink interface, FortiExtender adds LAN extension members in the switch interface by default. The default LAN extension members for most platforms are the LAN interface, the lan-ext-vap WiFi (for models that support Wi-Fi), and port1 for FBS10F-WiFi. The `vlan-support` value is disabled because the configuration does not have multiple VLAN settings.

FortiOS configuration	Synched FortiExtender configurations
<pre> config extension-controller extender-profile edit "FVA22F-lanext-default" set id 3 set model FVA22F set extension lan-extension set allowaccess ping http https config cellular set dataplan "test" config sms-notification end config modem1 end config modem2 end end config wifi set country US config radio-1 set mode AP set band 2.4GHz set status enable set operating-standard auto set channel CH1 set lan-ext-vap "2" set local-vaps "1" end config radio-2 set mode AP set band 5GHz set status disable set operating-standard auto end end end </pre>	<pre> config system switch-interface edit le-switch set vlan-support disable config member edit le-agg-link set type aggregate set port le-agg-link set vids next edit lan set type physical set port lan set vids set pvid 1 next edit 2 set type vap set vap 2 set pvid 0 next end set stp disable set ts-mode disable next end </pre>

FortiOS configuration	Synched FortiExtender configurations
<pre> config lan-extension set ipsec-tunnel "fext-ipsec- 5S2s" set backhaul-interface "internal1" config backhaul edit "1" set port wan set role primary next edit "2" set port ltel set role secondary next end end next end </pre>	

Example 3: FortiOS LAN extension profile with PVID downlink interface settings

In this example, the FortiOS LAN extension profile is configured with PVID downlink interface settings so the PVID of port2 is set to 200.

Because there are downlink PVID settings, only the configured interfaces are in the switch interface. All other default interfaces are removed. The `vlan-support` value is also enabled.

FortiOS configuration	Synched FortiExtender configurations
<pre> config extension-controller extender- profile edit "FVA22F-lanext-default" set id 3 set model FVA22F set extension lan-extension set allowaccess ping http https config cellular set dataplan "test" config sms-notification end config modem1 end config modem2 end end end end </pre>	<pre> config system switch-interface edit le-switch set vlan-support enable config member edit le-agg-link set type aggregate set port le-agg-link set vids 200 next edit port2 set type physical set port port2 set vids set pvid 200 next end set stp disable set ts-mode disable next </pre>

FortiOS configuration	Synched FortiExtender configurations
<pre> config wifi set country US config radio-1 set mode AP set band 2.4GHz set status enable set operating-standard auto set channel CH1 set lan-ext-vap "2" set local-vaps "1" end config radio-2 set mode AP set band 5GHz set status disable set operating-standard auto end end config lan-extension set ipsec-tunnel "fext-ipsec- 5S2s" set backhaul-interface "internal1" config backhaul edit "1" set port wan set role primary next edit "2" set port ltel set role secondary next end config downlinks edit "1" set type port set port port2 set pvid 200 next end end next end </pre>	<pre> end </pre>

Enable wireless configuration on FortiExtender

Starting from FEXT OS 7.4.4, wireless configurations are supported on select FortiExtender models used as FortiGate LAN extension.

To enable wireless configuration:

1. From the FortiGate, configure a wireless virtual Access Point (VAP):

```
config extension-controller extender-vap
    edit "local-vap-1"
        set type local-vap
        set ssid "local-vap1"
        set max-clients 100
        set broadcast-ssid enable
        set security OPEN
        set ip-address 192.168.7.7 255.255.255.0
        set start-ip 192.168.7.100
        set end-ip 192.168.7.200
    next
    edit "local-vap-2"
        set type local-vap
        set ssid "local-vap2"
        set max-clients 0
        set broadcast-ssid enable
        set security WPA2-Personal
        set passphrase xxxxx
        set ip-address 192.168.8.9 255.255.255.0
        set start-ip 192.168.8.100
        set end-ip 192.168.8.200
        set allowaccess http https ping
    next
    edit "lanext-vap1"
        set type lan-ext-vap
        set ssid "lan-ext-ssid"
        set max-clients 0
        set broadcast-ssid enable
        set security WPA2-Personal
        set passphrase xxxxx
        set allowaccess ping telnet http https ssh snmp
    next
end
```

2. In the extender-profile for lan-extension mode, configure wireless settings:

```
config wifi
    set country US
    config radio-1
        set mode AP
        set band 2.4GHz
        set status enable
        set operating-standard auto
        set guard-interval auto
```

```
        set channel CH1 CH6 CH10
        set bandwidth auto
        set power-level 100
        set beacon-interval 100
        set 80211d enable
        set max-clients 0
        set extension-channel auto
        set bss-color-mode auto
        set bss-color 0
        set lan-ext-vap "lanext-vap1"
        set local-vaps "local-vap1"
    end
config radio-2
    set mode AP
    set band 5GHz
    set status enable
    set operating-standard auto
    set guard-interval auto
    set channel CH36 CH149
    set bandwidth auto
    set power-level 100
    set beacon-interval 100
    set 80211d enable
    set max-clients 0
    set extension-channel auto
    set bss-color-mode auto
    set bss-color 0
    set lan-ext-vap "lanext-vap1"
    set local-vaps "local-vap1" "local-vap2"
end
end
```

3. Authorize the FortiExtender on the FortiGate. After LAN-Extension is created on the FortiGate, the wireless configuration profile will be synced to the FortiExtender, and the device is ready for WiFi networking.

Dynamic Frequency Selection channels

In many countries, regulatory requirements may limit the number of 5 GHz channels available or restrict their usage because the spectrum is shared with other technologies and services. For example, in the US, sixteen of the twenty-five 5 GHz channels are used by military, weather radar, and satellite communications. Wi-Fi networks operating in those bands are required to employ a radar detection and avoidance capability known as Dynamic Frequency Selection (DFS).

Using DFS, supported FortiExtenders automatically scan for and adjust the frequency of a radio if a radar event is detected. This greatly expands the number of channels available for use, improving performance.



DFS channels are enabled on FEV21xF and FBS10F models, but access is dependent on regional regulations. For example, in the CE region, regulations forbid FEV models from using DFS models when operating in AP mode. They can only use DFS 100-140 channels when operating in client mode.

Note the following behavior when selecting channels:

- You cannot select a fixed DFS channel and must select at least one non-DFS channel. This is to prevent FortiExtender from spending 60-600 seconds running a Channel Availability Check (CAC) to check for signals on that channel.
- To ensure that Wi-Fi on FEV21xF devices is available as quickly as possible, DFS channels are skipped during the automatic initial channel selection on the 5GHz Wi-Fi radio.

The following table summarizes the conditions under which DFS channel selections are available for each FortiExtender model:

Scenario	DFS channel selection permission	
	FEV21xF	FBS10F
Fixed channel	Deny	Deny
Initial channel selection once the radio is up	Deny	Allow
Running time channel selection	Allow	Allow



In FEV-21xF models:

- Channels 132/136 can only work in 20/40MHz.
- Channels 140/165 can only work in 20MHz.
- Channel 144 is not available.

In FEV-21xF-AM:

- Channels 132/136/140/144 can work in 20/40/80Mhz.
- Channel 165 can only work in 20MHz.

To configure DFS channels on a FortiGate managed FortiExtender - GUI:

1. From the FortiGate GUI, go to *Network > FortiExtenders > Profiles*.
2. Click *Create new* or edit an existing FortiExtender profile.
3. Select a supported *Model*.
4. :Set *Mode* to *LAN extension*.
5. Under *WiFi*, select the channels you want.

Edit FortiExtender Profile

WiFi

Country/Region: Aruba

2.4 GHz WiFi Radio: 5 GHz WiFi Radio

Status: ☒ Enable ☐ Disable

Operating standard: Auto

Extension channel: Auto Higher Lower

Bandwidth: Auto 20MHz 40MHz 80MHz

Guard interval: Auto 400ns 800ns

Transmit power: 100%

Channels: ☐ 36 ☐ 40 ☐ 44 ☐ 48
☐ 149 ☐ 153 ☐ 157 ☐ 161
☐ 165

LAN extension SSID:

Local SSID:

6. When you are finished, click OK.

To configure DFS channels on a FortiGate managed FortiExtender - CLI:

```
config extension-controller extender-profile
edit <profile>
config wifi
config radio
set channel <choose from DFS channel list>
end
end
next
end
```

Configure WiFi VAPs as members of switch interface

Starting from its 7.4.4 release, FortiExtender has enhanced the configuration schema for the system switch-interface to support WiFi Virtual Access Points (VAPs) as members of a switch-interface. A VAP can now be added as members of a switch-interface as long as it is not specified as a WLAN bridge. In so doing, the VAP shares DHCP servers and firewall policies with the switch-interface.

This feature allows for greater flexibility in configuring switch-interfaces and VAPs, enabling you to manage your network resources and configurations more efficiently.

To add a WiFi VAP as member of a switch interface:

1. Create a virtual access point (VAP), with wlan-bridge set to no.

```
FXW30FTF23000020 # config wifi vap
FXW30FTF23000020 (vap) # show
config wifi vap
    edit vap1
        set ssid FXW30F-WiFi
        set broadcast-ssid enable
        set dtim 1
        set rts-threshold 2347
        set max-clients 0
        set target-wake-time enable
        set bss-color-partial enable
        set mu-mimo enable
        set wlan-bridge no
        config ap-security
            set security-mode WPA2-Personal
            set pmf
            set passphrase *****
        end
    next
end
```

2. Add the VAP to the radio profile.

```
FXW30FTF23000020 # config wifi radio-profile
FXW30FTF23000020 (radio-profile) # show
config wifi radio-profile
    edit r2
        set band 5GHz
        set status enable
        set role lan
        set operating-standards auto
        set beacon-interval 100
        set 80211d enable
        set max-clients 0
        set power-mode auto
        set channel
        set bandwidth auto
        set extension-channel auto
        set guard-interval auto
        set bss-color-mode auto
        set vap vap1
    next
end
```

3. Add the VAP as a member of a switch interface.

```
FXW30FTF23000020 (switch-interface) # show
config system switch-interface
    edit lan
        set vlan-support disable
```

```

        config member
            edit m1
                set type vap
                set vap vap1
                set pvid 0
            next
        end
        set stp disable
    next
end

```

4. Verify the current VAP and bridge interface maps.

```

FXW30FTF23000020 # get wifi vap-maps all
vap id            bridg name      ap interface
vap1              lan             aap0
vap2              vap2
vap3              vap3            aap1

FXW30FTF23000020 #

```

Configure split tunneling in LAN extension mode

When FortiExtender is configured in LAN extension mode, you can configure split tunneling to control which traffic gets routed for further inspection and which traffic can be sent directly to their destination. This avoids overloading your secured network with unnecessary traffic.

Split tunnel configurations can only be made from the FortiGate. The settings will then be pushed to the FortiExtender where they can be viewed in the in read-only mode.



For example, FortiExtender can be managed by FortiSASE and used for microbranch deployments—a branch office deployment with a LAN behind a FortiExtender and secure internet access (SIA) over a backhaul connection to FortiSASE.

When FortiExtender is connected to FortiSASE for SIA, all traffic is sent to the SASE POP for inspection. However, you can configure split tunneling to control which traffic gets forwarded to the SASE overlay for inspection and which traffic bypasses the SASE and travels directly to their destination. Sensitive traffic can be forwarded to FortiSASE while traffic for video or audio streaming services can bypass FortiSASE and go directly to their destination.

For more information about FortiExtender and FortiSASE integration, refer to the [FortiSASE Administration Guide](#).

To configure split tunneling in LAN extension mode

In this example, specified services like `iperf3` and traffic with the destination network address of `vsdb` will go through the `le-switch` and then the NAT route to local WAN. Meanwhile default traffic from the LAN side will continue to be sent to the default gateway (the IP address configured in `lan-ext` on the remote FortiOS).

1. From the FortiGate, configure a custom network service for iperf3.

```
config firewall service custom
  edit iperf3
    set protocol TCP
    set tcp-portrange 5201-5204
  next
end
```

2. Configure split tunneling in the FortiGate LAN extension extender profile. Under `traffic-split-services`, you can select your configured firewall addresses and services.

```
config extension-controller extender-profile
  edit "FX200F-lanext-default"
    set id 1
    set model FX200F
    set extension lan-extension
    config lan-extension
      set link-loadbalance loadbalance
      set ipsec-tunnel "fext-ipsec-K3Vx"
      set backhaul-interface "wan2"
      config backhaul
        edit "2"
          set port port1
        next
        edit "3"
          set port port2
        next
      end
    end
    config traffic-split-services
      edit "ts1"
        set vsdb enable
        set address "all"
        set service "iperf3"
      next
    end
  end
next
end
```

When you apply the configurations, they are automatically synced to the FortiExtender devices.

3. Verify the synced configurations from the FortiExtender CLI.

```
config system switch-interface edit le-switch
  set vlan-support disable
  config member
    edit le-agg-link
      set type aggregate
      set port le-agg-link
      set vids
    next
    edit lan
      set type physical
      set port lan
      set vids
      set pvid 1
    next
  end
```

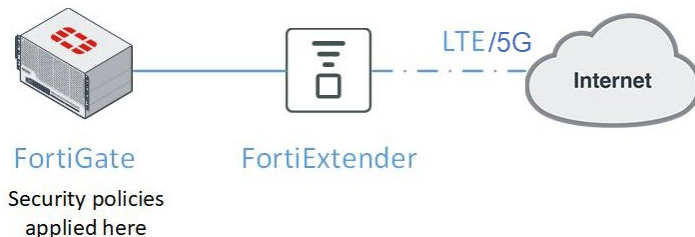
```
set stp disable
set ts-mode include
config traffic-split
  edit 1
    set dst-mac ba:a2:a6:39:c5:3d
    set dst-addr le-ts-all
    set services le-ts-iperf3
  next
next
end
```

Note that these configurations are auto-generated and cannot be edited while in LAN extension mode.

FortiExtender as FortiGate WAN extension

FortiExtender can work as FortiGate's extended WAN interface in IP pass-through mode. The following paragraphs highlight the network topology for integrating FortiExtender with FortiGate in such an application.

In this scenario, FortiGate manages FortiExtender over the Control and Provisioning of Wireless Access Points (CAPWAP) protocol in IP pass-through mode. Unlike a standalone 3G/4G/5G wireless WAN extender, the FortiExtender managed by FortiGate integrates directly into the FortiGate Connected UTM (Unified Threat Management) and is managed from the familiar FortiOS interface. This not only enables security policies to be seamlessly applied to the FortiExtender, but also provides visibility to the performance and data usage of the connection.



In this situation, you can connect one FortiExtender device to two FortiGate devices for a high availability (HA) configuration in active-passive deployment, or two FortiExtender devices to two FortiGate devices in active-active deployment to provide dual active redundancy for wireless WAN access as well.

The FortiExtender and the FortiGate share the same LTE IP in WAN-extension mode. To distinguish local services from FortiGate services, you must configure the FortiExtender to use different ports. Otherwise, all traffic to these default services will be sent to the FortiExtender locally instead of FortiGate.

To configure FortiExtender local SSH/HTTPS/HTTP/Telnet service support via the LTE interface:

```
config system management
    config local-access
        set https 22443
        set ssh 2222
    end
end
```

FortiGate-FortiExtender zero-touch provisioning (ZTP)

FortiExtender in WAN extension mode supports FortiGate-FortiExtender zero-touch provisioning (ZTP). The FortiExtender default discovery mode is set to auto with DHCP server enabled over the LAN interface. The process is outlined stepwise as follows:

1. A SIM card without a PIN code is expected to be used for ZTP, and the default APN should be retrieved automatically at first connection.
2. Acting as a DHCP client, the FortiGate connects to the FortiExtender LAN port (1, 2, or 3) interface to obtain a private IP to reach FortiManager.
3. The FortiGate reports the discovered FortiExtender to FortiManager to authorize it (FortiExtender).

4. Once authorized, the FortiExtender switches to IP-passthrough mode and then reboots itself.
5. Upon booting up in IP-passthrough mode, the FortiExtender serves as the FortiExtender WAN interface of the FortiGate.

VLAN mode

VLAN mode is an alternative to the default CAPWAP mode for FortiGate to FortiExtender connectivity. In the default FEX-WAN type interface, all traffic to and from the FortiGate is encapsulated in the CAPWAP data channel. In VLAN mode, traffic is sent and received on the VLAN interface. Because there is no encapsulation overhead and data traffic is processed in userspace currently, VLAN mode delivers better performance with the requirement that the VLAN interface be directly created on the port on which the FortiExtender is connected to the FortiGate.

It is important to note that in VLAN mode, the FortiExtender and the FortiGate can be connected directly to each other or through a switch. In case of a switch in between, the switch must be configured to support the configured VLANs.

Set up FortiExtender as the WAN-extension of FortiGate using VLAN mode

Before you start, keep the following in mind:

- Ensure that the VLAN interface is created according to the actual physical interface of the connected FortiExtender.
- For some models such as FBS and FEX-G/R models, each physical port has an Ethernet interface in the kernel; there is no physical LAN-switch interface. Since FortiExtender does not support VLAN over a softswitch interface, it can't use the LAN as the discovery interface for VLAN WAN-extension mode.

To resolve this, you can do one of the following:

- Separate one port (port1, port2, or port3) from the LAN switch.
- Use the default port4 as the discovery interface.



In this sample configuration, Port 4 of the FortiExtender is directly connected to the WAN2 interface on the FortiGate.

Configure the FortiGate

1. Create a WAN2 interface, setting the IP address to 192.168.2.99 with a DHCP server running on it and allowing Security Fabric connection traffic.
2. Enable `fortiextender-vlan-mode`:



- By default, VLAN mode is disabled on FortiGate, and must be explicitly enabled on the FortiGate:

```
config system global
(global)set fortiextender-vlan-mode enablevlan
(global)end
```

- Before enabling VLAN mode, you must delete all the FortiExtender-WAN interfaces created on the device.
-

3. Create a VLAN interface (any VLAN ID, e.g., 123) on top of the WAN2 interface, name it FEXVLAN, and make this interface type DHCP client.

The screenshot shows the 'New Interface' configuration page in the FortiGate GUI. The left sidebar contains the navigation menu with 'Network' > 'Interfaces' selected. The main panel is titled 'New Interface' and contains the following configuration fields:

- Name:** FEXVLAN
- Alias:** (empty)
- Type:** VLAN
- VLAN protocol:** 802.1Q (selected), 802.1AD
- Interface:** wan2
- VLAN ID:** 123
- VRF ID:** 0
- Role:** LAN

Below the interface configuration, the **Address** section is visible:

- Addressing mode:** Manual, **DHCP** (selected), Auto-managed by IPAM, PPPoE
- Retrieve default gateway from server:** ☒
- Distance:** 5
- Override internal DNS:** ☒
- Create address object matching subnet:** ☒
- Name:** FEXVLAN address
- Destination:** 0.0.0.0/0.0.0.0

The **Administrative Access** section shows various protocols that can be enabled:

- IPv4:**
 - ☐ HTTPS
 - ☐ FMG-Access
 - ☐ FTM
 - ☐ Speed Test
 - ☐ HTTP
 - ☐ SSH
 - ☐ RADIUS Accounting
- Other:**
 - ☐ PING
 - ☐ SNMP
 - ☐ Security Fabric Connection

The **Network** section at the bottom shows **Device detection** is enabled.

Configure the FortiExtender

1. Ensure that the port4 interface is connected to WAN2 to get the IP address (192.168.2.98) from the FortiGate.
2. On the FortiExtender GUI, select *Setting>Management*, and set the following:
 - Controller — FortiGate
 - Discovery Type — Static
 - Discovery Interface — port4
 - Static Access Control Address > Server —192.168.2.99

Management Setup [Cancel] [Save]

Controller

auto **fortigate** cloud local

Fortigate

Discovery Type

broadcast **static**

Discovery Interface

port4 x

Controller CTL Port

5246

Ingress Interface

port4

Static Access Control Address

[+ Create]

Server	ID
192.168.2.99	1

- On the FortiGate GUI, select *Network>FortiExtenders*, wait for the FortiExtender to be discovered by the FortiGate, and then authorize the FortiExtender by setting the following:
 - Mode — WAN extension
 - Modem 1 Interface — FEXVLAN

Edit FortiExtender

Serial number FX511FTQ XXXXXXXX

Alias

Mode LAN extension **WAN extension**

Profile FX511F-wanext-default

Extender Profile Overrides

Management access ☒ Ping ☒ Telnet ☒ HTTP ☒ HTTPS ☒ SSH ☒ SNMP

FortiExtender login password

State

Authorized ☒

WAN extension

Modem 1 Interface FEXVLAN

- Wait for a few moments, for the FortiExtender may need to reboot when the mode is changed from NAT to IP-passthrough (VLAN).

5. After the WAN extension tunnel is set up, check its status from the FortiExtender Dashboard for the following Controller Information:
 - FortiGate, with Status — Connected
 - Mode — FortiGate (ip-passthrough (VLAN))
6. Check the status of the WAN extension with the following FortiExtender CLI command:

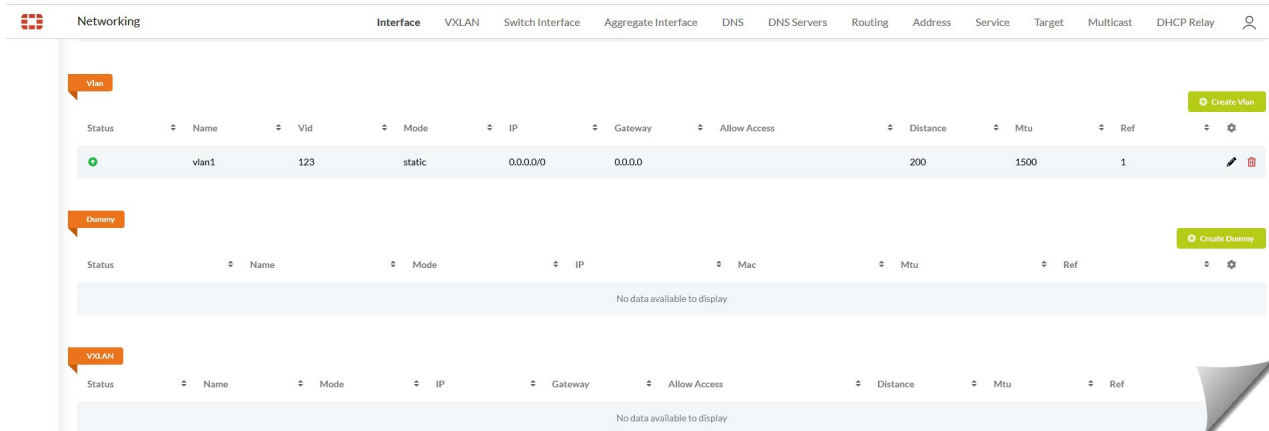
```
# get extender status
```

```

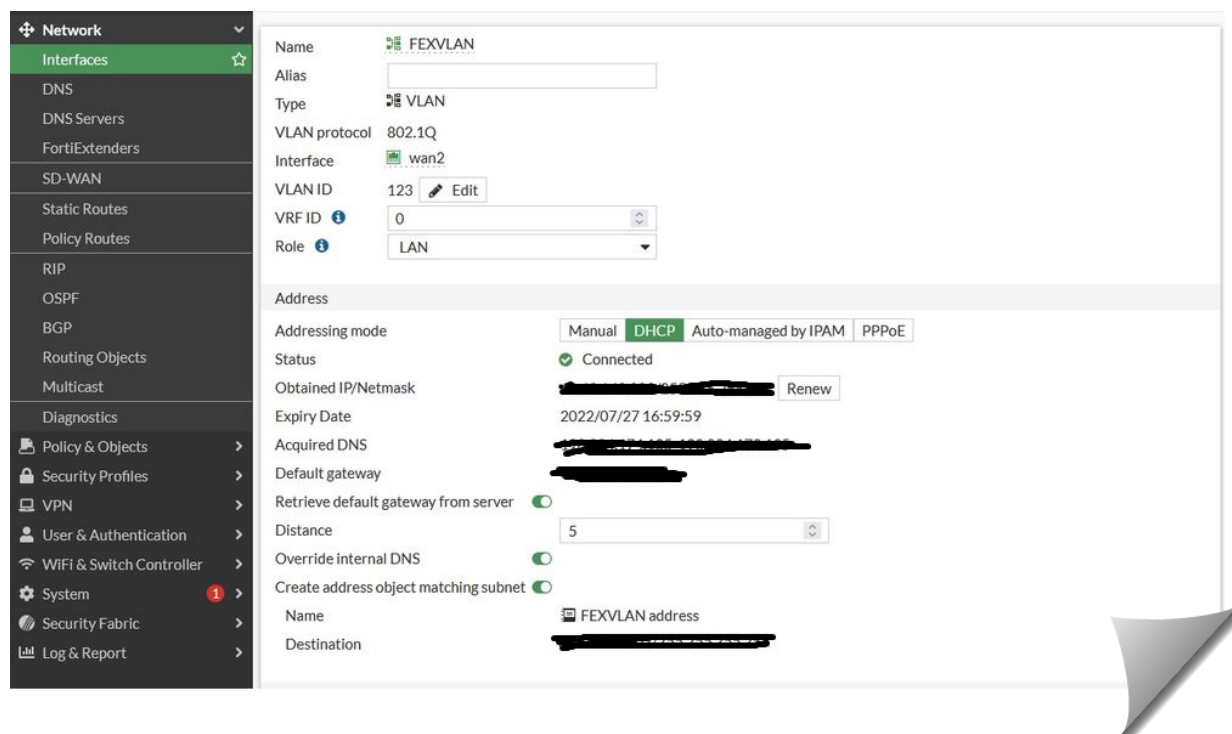
Fortinet

FX511FTQ login: Modem 1: Cellular Data Session started successfully
FX511FTQ login: admin
Password:
FX511FTQ # get extender status
Extender Status
name           : FX511FTQ
mode           : CAPWAP
fext-addr      : 192.168.2.98
ingress-intf   : port4
fext-wan-addr  : 
controller-addr : 192.168.2.99:5246,25246
controller-name : FGT81B
uptime         : 0 days, 0 hours, 50 minutes, 28 seconds
management-state : CWS RUN
base-mac       : 94:FF:3C:0D:1A:C0
network-mode   : ip-passthrough (vlan)
fgt-backup-mode : backup
discovery-type : static
discovery-interval : 5
echo-interval  : 30
report-interval : 30
statistics-interval : 120
mdm-fw-server  : fortiextender-firmware.forticloud.com
ps-fw-server   : fortiextender-firmware.forticloud.com
  
```

The FortiGate will send the VLAN ID to the FortiExtender over CAPWAP, and the FortiExtender will then create a VLAN interface automatically with the name VLAN1 and vid 123, for example. No special configuration is needed.



Now when the FortiExtender modem is connected to the internet, the FortiGate VLAN interface, i.e., FEXVLAN, will get the same IP address as the one of the FortiExtender LTE interface.



On the FortiGate, after configuring the correct firewall policy, the client behind the FortiGate can go to the internet via the FEXVLAN interface. This will ensure that the VLANs are separated for data traffic from control traffic.

Hitless failover in WAN-extension mode in HA configuration

In the following HA configuration, the FortiGates are connected to the FortiExtender LAN interface which has port2 and port3.

```
config system interface
  edit lan
    set type lan-switch
    set status up
    set mode static
    set ip 192.168.140.40/24
    set gateway 192.168.140.61
    set mtu-override enable
    set mtu 1500
    set distance 50
    set vrrp-virtual-mac enable
    config vrrp
      set status disable
    end
    set allowaccess ping telnet http https ssh snmp
  next

config system lan-switch
  config ports
    edit port2
```

```
        next
        edit port3
        next
    end
end

config system management
    set discovery-type fortigate
    config fortigate
        set ac-discovery-type static
        config static-ac-addr
            edit 1
                set server 192.168.140.61
            next
        end
        set ac-ctl-port 5246
        set ac-data-port 25246
        set discovery-intf lan
        set ingress-intf lan
    end
    config cloud
        set dispatcher fortiextender-dispatch.forticloud.com
        set dispatcher-port 443
        set mode nat
        set proxy disable
    end
    config local
        set mode ip-passthrough
    end
    config local-access
        set http 80
        set https 443
        set ssh 22
        set telnet 23
        set idle-timeout 480
    end
    config fortigate-backup
        set vrrp-interface
        set status disable
    end
end
```

Upon successful connection, the status of the FortiExtender show the connected FortiGates' names in the controller-name field, as shown in the following code example.

```
FX201E5919000165 # get extender status
Extender Status
  name : FX201E5919000165
  mode : CAPWAP
  session : active
    fext-addr : 192.168.140.40
    ingress-intf : lan
    fext-wan-addr : 100.100.143.89
    controller-addr : 192.168.140.61:5246,25246
    controller-name : FG200E4Q17913693
    uptime : 1 days, 0 hours, 28 minutes, 57 seconds
    management-state : CWWS_RUN
```

```
session : standby
fext-addr : 192.168.140.40
ingress-intf : lan
fext-wan-addr : 100.100.143.89
controller-addr : 192.168.140.61:5248,25248
controller-name : FG200ETK19908988
uptime : 1 days, 0 hours, 28 minutes, 55 seconds
management-state : CWWS_RUN
base-mac : 04:D5:90:47:D9:69
network-mode : ip-passthrough (vlan)
fgt-backup-mode : backup
discovery-type : static
discovery-interval : 5
echo-interval : 30
report-interval : 30
statistics-interval : 120
mdm-fw-server : fortiextender-firmware.forticloud.com
os-fw-server : fortiextender-firmware.forticloud.com
```

Multiple APNs in WAN-Extension mode

When operating in WAN-Extension mode, multi-path cellular channel extensions can support multiple simultaneous Packet Data Networks (PDN). The following FortiExtender models support multiple Access Point Names (APNs):

- FEX-511G
- FEX-511G-WiFi

Having multiple APNs enables you to configure multiple data sessions on a single modem with a single SIM. This provides you with more flexibility to customize data traffic steering. You can configure multiple PDNs to segment your traffic to suit your organization's needs. For example, you can configure one PDN as a public network and one as a private network, extending the cellular connectivity from the FortiExtender to the FortiGate.



Support for configuring multiple PDNs can only be done with one SIM card inserted; it will not work if there is more than one SIM card inserted.

To configure multiple APNs:

1. From the FortiGate CLI, configure the FortiExtender extender profile and set your APNs under `dataplan`. Then enable `multiple-PDN` and configure your PDNs.

```
config extension-controller extender-profile
edit <FEX-profile1>
set extension-type wan-extension
...
config cellular 1
...
set dataplan <plan1> <plan2> <plan3>
config modem1
```

```

...
    set multiple-PDN enable/disable
    set pdn1-dataplan <pdn-plan1>
    set pdn2-dataplan <pdn-plan2>
    set pdn3-dataplan <pdn-plan3>
    set pdn4-dataplan <pdn-plan4>
end
next
end

```

- When setting APNs under `dataplan`, you must enter them in the order provided by the ISP. Use a comma to separate the data plan names. For example, `Plan1, Plan2, Plan3, Plan4`.
- If the ISP only provides three APNs, you cannot create a fourth APN and set a `pdn4-dataplan plan4`.

2. From the FortiGate CLI, configure the Extender controller and set your WAN-Extension PDN interfaces.

```

config extension-controller extender
edit FEX1
    set id <FEX-SN>
    set extension-type wan-extension
    set authorized enable
    set profile "FEX1-wanext-profile"
    config wan-extension
        set modem1-pdn1-interface <fex-wan1>
        set modem1-pdn2-interface <fex-wan2>
        set modem1-pdn3-interface <fex-wan3>
        set modem1-pdn4-interface <fex-wan4>
    end
end
next
end

```

- The wan-extension interfaces should already be created before you assign them to this configuration.
- The interface selection should be unique and not duplicated.

3. From the FortiExtender CLI, configure the LTE plan for each PDN.

```

config lte setting modem1
    set multi-pdn <enable|disable>
    set ltel1-plan <dataplan name for apn1>
    set ltel1_1-plan <dataplan name for apn2>
    set ltel1_2-plan <dataplan name for apn3>
    set ltel1_3-plan <dataplan name for apn4>
end

```

When configuring the LTE plan, be aware of the following design behaviors:

- By default, the `ltel1-plan`, `ltel1_1-plan`, `ltel1_2-plan`, and `ltel1_3-plan` are directly mapped to the `ltel1`, `ltel1_1`, `ltel1_2`, and `ltel1_3` interfaces on the FortiExtender, respectively.
- `ltel1_1`, `ltel1_2`, `ltel1_3` will all show their state as `up` regardless of if `multiple-pdn` is enabled or disabled.
- The virtual-wire-pair shows four `capwap1`, `capwap1_1`, `capwap1_2`, and `capwap1_3` mapped with `ltel1`, `ltel1_1`, `ltel1_2`, and `ltel1_3`, even if only three APNs were provided
- Avoid manually changing the down/up state of `ltel1`, `ltel1_1`, `ltel1_2`, and `ltel1_3`.
- The `ltel1`, `ltel1_1`, and `ltel1_2` interfaces all work as a family. Either all interfaces will have IP addresses and show as an `up` state, or all interfaces will be down.



Manage dual FortiExtender devices

Active/Passive mode

By default, each FortiGate device can support up to two FortiExtender devices at a time. The first FortiExtender linked interface can be configured to have a lower distance than the second FortiExtender linked interface.

Active/Active mode

To have access to active internet sessions on both FortiExtender devices simultaneously, authorize both FortiExtender devices and configure the distance, priority, and firewall policies accordingly.

Cellular as backup of Ethernet WAN

In this redundant mode of operation, the FortiExtender daemon running on the FortiGate monitors a given WAN link on the FortiGate, and brings up the FortiExtender's cellular internet access when the WAN link is down and brings down the FortiExtender cellular internet when the WAN link comes up. For example:

```
config extension-controller extender
  edit <FEX SN>
    set authorized enable
    config modem1
      set ifname <fext-wan interface>
      set redundant-mode enable
      set redundant-intf <wan interface, ie wan1>
    end
  next
end
```

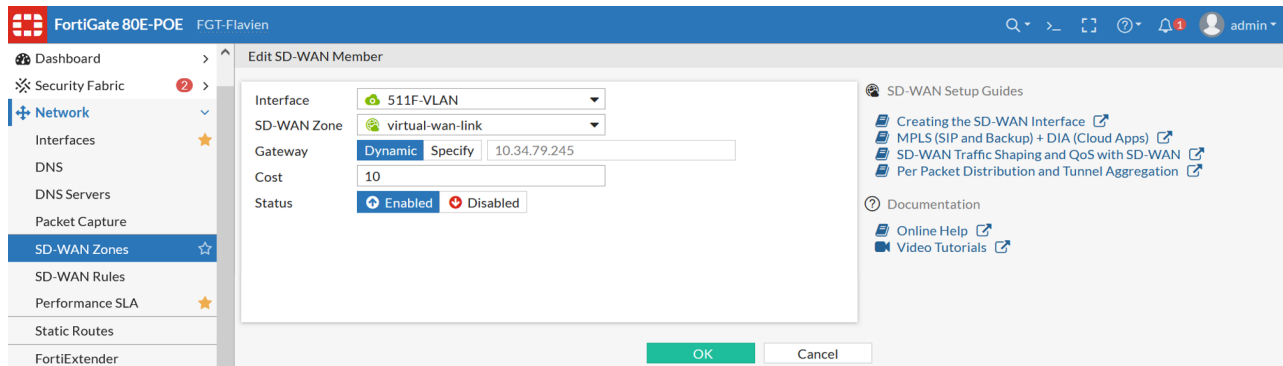
In this mode of operation, the FortiExtender interface comes up if the WAN interface goes down and goes down if the WAN interface comes up.

SD-WAN

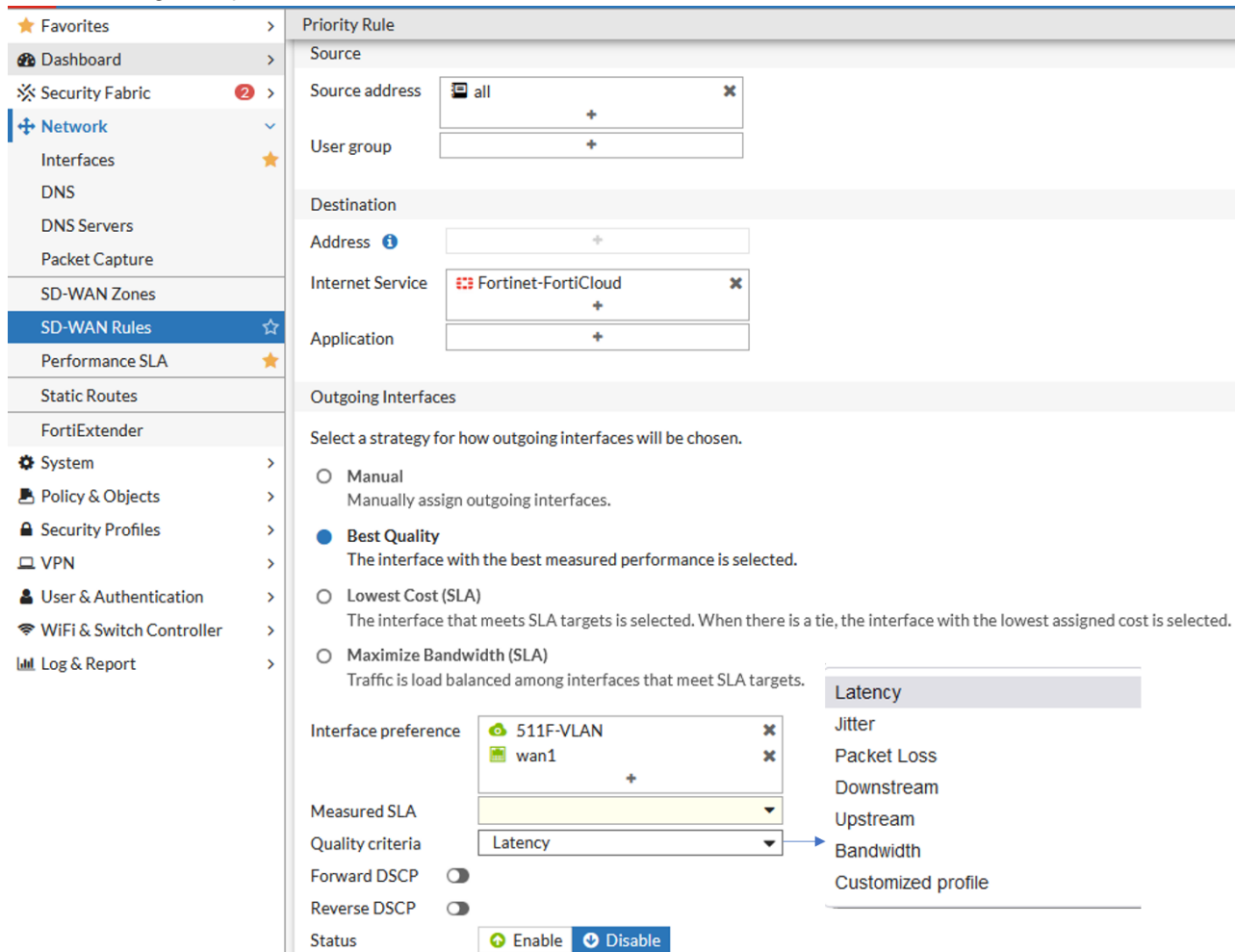
FortiOS recognizes and uses FortiExtender as a valid interface within an SD-WAN interface zone. Using SD-WAN, FortiGate becomes a WAN path controller and supports diverse connectivity methods. With FortiExtender, 3G/4G/5G can be used as the primary connection, a backup interface, or a load-balanced WAN access method with Application-Aware WAN path control selection. It provides high availability and QoS for business-critical applications by using the best effort access for low-priority applications through low-cost links and backup service through associations with a FortiExtender link. This enables aggregation of multiple interfaces into a single SD-WAN interface using a single policy.

To accomplish this:

1. Add the FortiExtender interface as a member of the SD-WAN interface, as illustrated below.



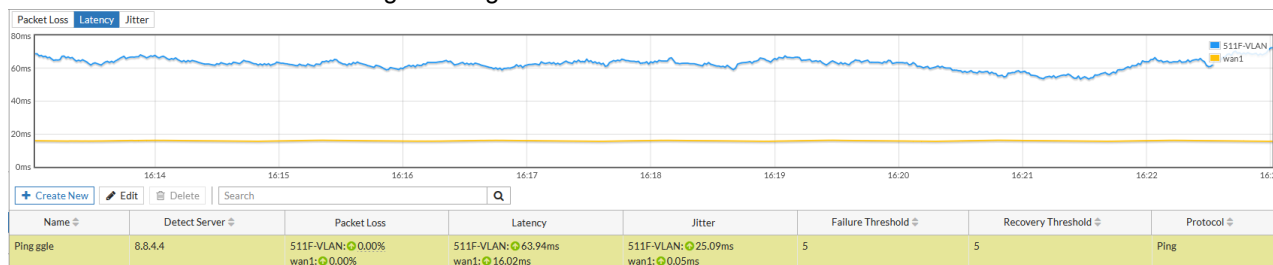
2. Define the priority rule, for instance, with the Best Quality strategy based on the Latency or Jitter criterion as shown in the following example.



3. Order or combine your policies as illustrated below.

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used
IPv4							
6	nPerfFree5G	all	FreeParisNPerf		511F-VLAN	387	Wednesday
7	Citrix-Fiber	all	Citrix.CDN Citrix.Services Citrix.Services_Podio GoToMeeting GoToWebinar		wan1	1,014	10 minutes ago
5	Test5G		Deezer Salesforce Schwab		511F-VLAN wan1	2,039	26 minutes ago
3	FortiCloudVia5G	all	Fortinet-FortiCloud		511F-VLAN wan1		
2	AlarmVia5G	Alarme	all		511F-VLAN		
4	fcld_eu_ping_5G_only		FortiCloud_EU		511F-VLAN		
1	LowestCost		all	SLA	511F-VLAN wan1	1,754,895	2021/08/04 16:18:40
Implicit							
	sd-wan	all	all	Source IP	any		

4. Monitor the 4G/5G link health using the integrated Performance SLA tool in FortiGate.



Configure cellular settings

Configuration of the cellular settings involves the following tasks:

- Create a data plan on page 111
- Set the default SIM on page 113
- Enable SIM-switch on page 114
- Report to FortiGate on page 116
- CAPWAP mode on page 118
- VLAN mode on page 116

Create a data plan

You can configure a data plan with the following parameters:

```
config lte plan
edit Verizon
set modem modem1
set type by-carrier
set carrier Verizon
set apn WE01.VZWSTATIC
```

```

set auth NONE
set user
set pwd
set pdn ipv4-only
set signal-threshold 0
set signal-period 0
set capacity 0
set monthly-fee 0
set billing-date 0
set overage disable
set preferred-subnet 32
set private-network disable
next
end

```



When "private network" is enabled, FortiExtender allows the flow of non-NATed IP traffic on to an LTE interface. Otherwise, it does not.

Parameter	Description
modem	Choose "modem1", "modem2", or "all".
type	Choose the way for the modem to select the SIM card: - carrier— Assign by SIM carrier. - slot— Assign to SIM slot 1 or 2. - iccid— Assign to a specific SIM by its serial number (18 to 22 digits). - generic— Compatible with any SIM. Assigned if no other data plan matches the chosen SIM.
iccid	The serial number of the SIM, mandatory for "set type by-iccid".
carrier	The SIM card carrier, mandatory for "set type by-carrier".
slot	The SIM card slot, mandatory for "set type by-slot"
apn	The APN of the SIM card.
auth-type	The Authorization mode.
username	The username.
password	The password.
pdn	The Packet Data Network (PDN) IP address family.
signal-threshold	The signal-strength threshold beyond which SIM switch will occur. Note: Enter an integer value from <50> to <100> (default = <100>).
signal-period	The length of time (from 600 to 18000 seconds) for SIM switch to occur when signal strength remains below the set signal threshold for more than half of the set period.
capacity	The data capacity per month (from 0 to 102400000 MB).
monthly-fee	The monthly fee for the data plan (from 0 to 1000000).

Parameter	Description
billing-date	The billing date of the month.
preferred-subnet	DHCP subnet.
private-network	(Enable/disable) blocking all non-NATed traffic.

Set the default SIM

When installing two SIM cards in one modem, you can set the default SIM to use.

You can set the default SIM by

- [Set the default SIM by preferred carrier on page 113](#)
- [Set the default SIM by low cost on page 113](#)
- [Set the default SIM by SIM slot on page 113](#)

Set the default SIM by preferred carrier

Use this option to set the default SIM if you have SIM cards from different carriers.

```
config lte setting
  config modem1
    set default-sim by-carrier
    set preferred-carrier <carrier name>
  end
next
end
```

Set the default SIM by low cost

This option applies when you need to choose the low-cost SIM over a more expensive one.

You must configure two entries under “config lte plan” for the two SIM cards separately. The system will calculate the cost based on the “set capacity” and “monthly-fee”.

```
config lte setting
  config modem1
    set default-sim by-cost
  end
next
end
```

Set the default SIM by SIM slot

The default SIM is sim1. You can change it to sim2 using the following commands:

```
config lte setting
  config modem1
    set default-sim sim1|sim2
```

```

    end
  next
end

```

Enable SIM-switch

```

config lte setting
  config modem1
    config auto-switch
      set by-disconnect enable
      set by-signal disable
      set by-data-plan disable
      set disconnect-threshold 1
      set disconnect-period 600
      set switch-back by time by-timer set switch-back-by-time 00:01
      set switch-back-by-timer 3600
    end
  end
next
end

```



SIM-switching can be configured by data plan, disconnect settings, signal strength, coupled with switch back by time or by timer. All these options are under the “Auto switch” setting.

Parameter	Description
by-disconnect	The SIM card switches when the active card gets disconnected according to the 'disconnect-threshold' and 'disconnect-period'.
by-signal	The SIM card switches when the signal strength gets weaker than the signal-threshold.
by-data-plan	The SIM card switches when 'capacity' is overrun and 'overage' is enabled.
disconnect-threshold	The number (1 —100) of disconnects for SIM switch to take place.
disconnect-period	The evaluation period (600 — 18000) in seconds for SIM switch.
switch-back	Enables switching back to the preferred SIM card.
switch-back-by-time	Switches over to the preferred SIM /carrier at a specified (UTC) time (HH:MM).
switch-back-by-timer	Switches over to the preferred SIM/carrier after a given time (3600- 2147483647) in seconds.

Configure SIM-switch based on link health

FortiExtender enables you to configure automatic SIM switch based on the link health.



For more information, refer to the CLI Reference Guide.

To use this feature:

1. Configure an hmon hchk instance:

```
config hmon hchk
  edit sim-health
    set protocol ping
    set interval 10
    set probe-cnt 1
    set probe-tm 2
    set probe-target 166.253.42.211
    set interface ltel
    set src-type none
    set filter loss
  next
end
```

2. Link the auto-switch instance to the config hmon hchk instance:

```
FX511FTQ21001152 # config lte setting modem1 auto-switch
FX511FTQ21001152 (auto-switch) # show
  config lte setting modem1 auto-switch
    set by-disconnect disable
    set by-signal disable
    set by-data-plan disable
    set by-health-monitor enable
    config health-monitor
      set event sim-health
      set fail-cnt 3
      set recovery-cnt 2
      set by-latency enable
      set latency-threshold 150
      set by-jitter enable
      set jitter-threshold 150
      set recover-by-reboot enable
      set max-switches-allowed 4
      set max-switches-interval 1800
    end
```

Parameter	Description
event sim-health	"sim-health" refers to the config hmon hchk instance above.
fail-cnt 3	The link is deemed unusable if three pings have failed.
recovery-cnt 2	The link is considered usable if two pings have succeeded.
by-latency	Enable/Disable latency monitoring on the active SIM card.
latency-threshold	Latency in milliseconds for SLA to make decisions.
by-jitter	Enable/Disable jitter monitoring on the active SIM card.

Parameter	Description
jitter-threshold	Jitter in milliseconds for SLA to make decisions.
recover-by-reboot [disable enable]	Enable/Disable. If enabled, the system will reboot if the following two conditions are met: - max-switches-allowed - max-switches-interval See below.
max-switches-allowed 5	5 switches
max-switches-interval 1800	Within 1,800 seconds

Report to FortiGate

```

config extension-controller extender
    edit <FEX SN>
        set authorized enable
        config controller-report
            set status [enable|disable]
            set interval 300
            set signal-threshold 10
        end
    end
next
end

```

Parameter	Description
status	Enable or disable periodic controller report.
interval	The interval at which to notify the FortiGate (once every 30 to 86,400 seconds; the default is 300).
signal-threshold	The signal strength threshold (10 — 50 dBm). The FortiExtender notifies the FortiGate once the RSSI change has exceeded the set threshold.

VLAN mode

CAPWAP mode does not perform as well as expected on low-end FortiGate devices, so VLAN mode has been introduced to improve performance. A FortiExtender in VLAN mode is also managed by a FortiGate in the same way as it is in CAPWAP mode, but it uses VLAN to forward traffic between the FortiGate and itself.

Configurations on FortiExtender

The VLAN interface is created automatically on the FortiExtender, and cannot be edited or removed.

```

config system interface
    edit vlan1
        set type vlan
        set vid 100
    end
end

```

```
        set ingress-intf lan
    next
end
```

Virtual Wire Pair

Just like CAPWAP mode, Virtual Wire Pair Configurations of the virtual wire pair are created automatically, and cannot be edited or removed. These configurations specify the mapping of the LTE interfaces and the VLAN interfaces.

```
config system virtual-wire-pair
    set ltel-mapping vlan1
end
```

CAPWAP on multiple ports for broadcast discovery

Starting from Version 4.2.1, FortiExtender is able to discover FortiGate on multiple interfaces. It achieves this by sending discovery messages on multiple ports (port1, port2, port3, and port4), one at a time, until it has successfully connected with a FortiGate.

```
config system management fortigate
    set ac-discovery-type broadcast
    set ac-ctl-port 5246
    set ac-data-port 25246
    set discovery-intf lan port4
    set ingress-intf
end
```

By default, FortiExtender starts the discovery process with the LAN ports (port1 through port3) first. If it fails to establish a connection after several attempts, it will move on to port4. If it fails on port4, it will go back to the LAN ports and start the process all over again.

A LAN interface has a static IP of 192.168.200.99 and a DHCP server IP of 192.168.200.110 — 192.168.200.210. We recommend connecting to the WAN port on FortiGate for ZTP.

The port4 interface is set for DHCP mode, and must be connected to the internal port on the FortiGate to obtain an IP address for the CAPWAP tunnel, which is the same as in previous versions.

CAPWAP mode

In CAPWAP IP pass-through mode, the FortiExtender is managed by a FortiGate, and traffic is forwarded via the CAPWAP tunnel between the FortiGate and the FortiExtender. Refer to FortiGate documentation on how to manage a FortiExtender on a FortiGate. Once a FortiExtender is managed by a FortiGate, the following configurations will be synced from the FortiGate and generated automatically.

Configurations on FortiExtender

The `ingress-intf` in system management setting is set automatically, and cannot be edited.

```
config system management fortigate
    set ingress-intf lan
end
```

CAPWAP interface

The `capwap` interface is created automatically, and cannot be edited or removed.

```
config system interface
    edit capwap1
        set type capwap
        set rid 1
    next
end
```

Virtual wire pair

Configurations of the virtual wire pair are created automatically. They cannot be edited or removed. These configurations specify the mapping of the LTE interfaces and the `capwap` interfaces. For example, 'set ltel-mapping capwap1' means the traffic from the `capwap1` interface will be sent out by the `lte1` interface.

```
config system virtual-wire-pair
    set ltel-mapping capwap1
end
```

Check current manage mode

You can configure and manage your FortiExtender from FortiGate or FortiEdge Cloud. If you are not sure "who" is your FortiExtender's controller, use the following command to find out:

```
FX511F5921000053 # get extender status
Extender Status
  name           : FX511F5921000053
  mode           : CLOUD
  fext-addr      : 192.168.237.1
  fext-wan-addr  : 25.75.193.57
  controller-addr : fortiextender-dispatch.forticloud.com:443
  deployed       : true
  account-id     : 343849
  uptime         : 5 days, 17 hours, 2 minutes, 45 seconds
  management-state : CWWS_RUN
  base-mac       : E8:ED:D6:03:D2:58
  network-mode   : ip-passthrough
  fgt-backup-mode : backup
  discovery-type  : cloud
  discovery-interval : 5
  echo-interval   : 30
  report-interval : 30
  statistics-interval : 120
  mdm-fw-server   : fortiextender-firmware.forticloud.com
  os-fw-server    : fortiextender-firmware.forticloud.com
```

Get modem status

You can use the following command to get your modem status:

```
FX201E5919002499 # get modem status
```

Modem status:

```
modem                : Modem1
usb path              : 2-1.2 (sdk 0)
vender               : Sierra Wireless, Incorporated
product              : Sierra Wireless, Incorporated
model                : EM7455
SIM slot              : SIM1
revision              : SWI9X30C_02.32.11.00 r8042 CARMD-EV-FRMWR2 2019/05/15 21:52:20
imei                 : 359073065340568
iccid                 : 8933270100000296108
imsi                  : 208270100029610
pin status            : enable
pin code              : 0000
carrier               : 436627|coriolis|EU
APN                   : N/A
service               : LTE
sim pin (sim1)        : 3 attempts left
sim puk (sim1)        : 10 attempts left
rssi (dBm)            : -68
signal_strength       : 64
ca state              : ACTIVE
cell ID               : 00A25703
band                  : B7
band width            : 20
sinr (dB )            : 7.4
rsrp (dBm)            : -99
rsrq (dB )            : -13.1
plan_name             : coriolis100G
connect_status        : CONN_STATE_CONNECTED
reconnect count       : 0
smart sim switch      : disabled
up time (sec)         : 26670
clock (UTC)           : 20/05/27,20:08:33+08
temperature           : 60
activation_status     : N/A
roaming_status        : N/A
Latitude              : 37.376281
Longitude              : -122.010817
```

Stopping data traffic on overaged LTE interface

When an LTE interface has breached its data usage limit, FortiExtender will stop forwarding outgoing traffic (except for management traffic) to that interface. The following types of traffic are affected:

- NATed traffic
- VPN data traffic on IPsec Tunnel based on the overaged LTE interface
- IP-passthrough traffic

Access other devices via SSH

You can log into other devices from FortiExtender via SSH using the following command:

```
#execute ssh username serverip
```

For example, "execute ssh admin 192.168.1.115" lets the user "admin" to log into the device with the IP address "192.168.1.115" via SSH.

Use cases

This section discusses some typical use cases to deploy FortiExtender.

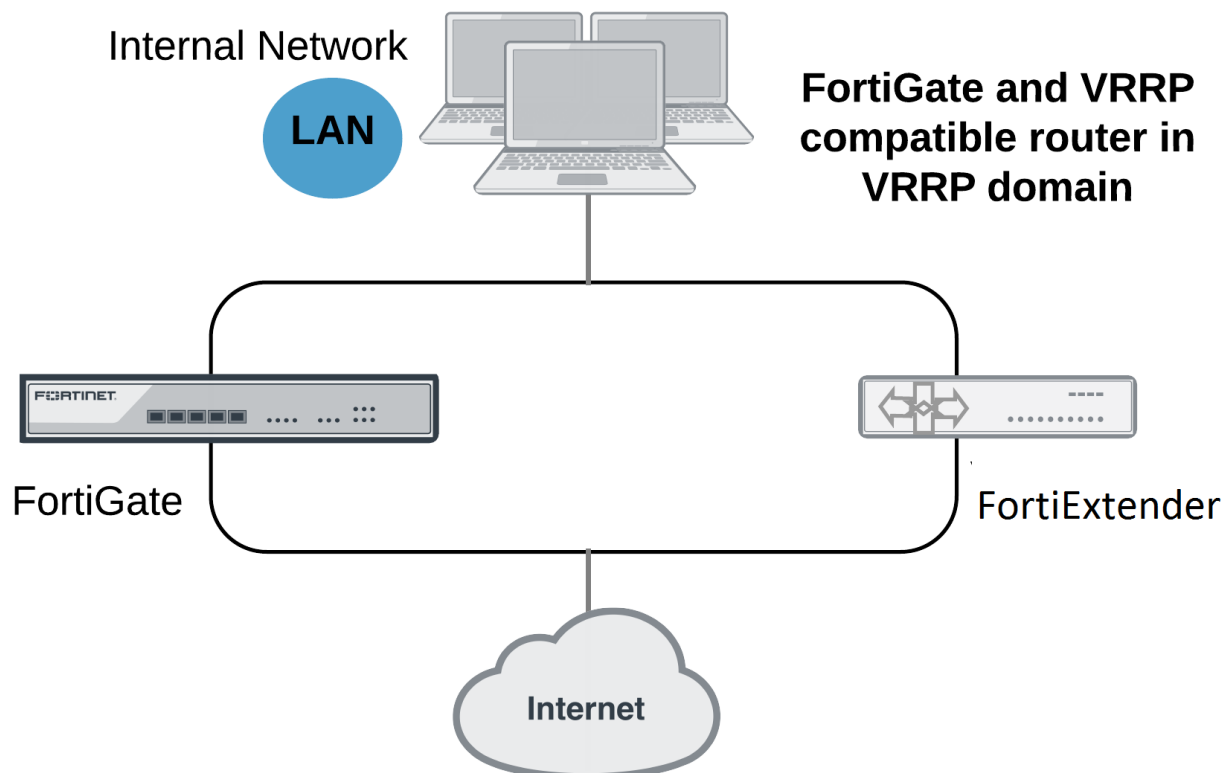
- [Redundant with FGT in IP Pass-through mode on page 124](#)
- [FortiExtender for FortiGate HA configuration on page 130](#)

Redundant with FGT in IP Pass-through mode

A Virtual Router Redundancy Protocol (VRRP) configuration can be used as a high-availability (HA) solution to ensure network connectivity in the event of a failing FortiGate router. With VRRP enabled on FortiExtender, all traffic will transparently fail over to FortiExtender when the FortiGate on your network fails. When the failed FortiGate is restored, it will take over the processing of traffic for the network.

For more information about VRRP, see [RFC 3768](#).

Use Case 1: FortiExtender in VRRP mode while being managed from FortiGate.



General configuration procedures

1. The FortiExtender LAN interface consists of multiple ports by default. Be sure to separate out an individual port from the LAN-switch for VRRP purposes. (Refer to "Step 3: Verify the port settings on FortiExtender" in [FortiExtender for FortiGate HA configuration on page 130.](#))
2. Continue managing FortiExtender from FortiGate over the LAN interface (NOT the VRRP interface).
3. Configure the VRRP gateway IP on the newly separated individual port on the FortiExtender and the corresponding VRRP port on the FortiGate.
4. Set the VRRP priority of the FortiExtender VRRP interface to a value lower than that of the FortiGate VRRP interface.
5. Create a firewall policy on the FortiExtender to forward traffic from the newly created VRRP interface to the LTE internet. See [Configure firewall policies.](#)
6. Ensure the VRRP ports on the FortiExtender and the FortiGate are connected by verifying that the FortiExtender is in backup mode and the FortiGate is in primary mode by running command 'get router info vrrp'.

In normal operations, all traffic to the internet passes through the primary VRRP interface of the FortiGate. The primary VRRP router, which is the FortiGate, sends VRRP advertisement messages to the backup router, i.e., the FortiExtender. The backup FortiExtender will not attempt to become a primary router while receiving these messages. If the primary router fails, the backup FortiExtender becomes the new primary router after a brief delay, during which the new primary router, i.e., FortiExtender sends gratuitous ARP packets to the network to map the default route GW IP address of the network to the MAC address of the new primary router. All packets sent to the default router are now being sent to the new primary router, i.e., FortiExtender. Upon switchover, the network will not continue to benefit from FortiOS security features until the FortiGate is back online.

To enable VRRP on the interface attached to the LAN port on the FortiGate:

```
config system interface
    edit <port num>
        set vdom "root"
        set ip <ip> <subnet mask>
        set allowaccess ping
        set vrrp-virtual-mac enable
        config vrrp
            edit <vrrp id>
                set vrip <vrrp IP>
                set priority <priority>
            next
        end
    next
end
```

To enable VRRP on the FortiExtender:

```
config system management
    set discovery-type fortigate
    config fortigate-backup
        set vrrp-interface <vrrp interface i.e por1>
        set status enable
    end
end
config system interface wan vrrp
    set status enable
```

```
set version 2 <only 2 is supported currently>
set ip <IP of virtual router>
set id <vrrp id>
set priority <priority>
set adv-interval <advertisement interval in seconds>
set start-time <initialization timer for backup router, typically 1>
set preempt <enable | disable> (preempting primary typically disable)
end
```



The VRRP interfaces on the FortiGate and the FortiExtender must be individual ports, and must not be part of a LAN switch with static IP address configurations. Devices reliant on the internet from the FortiGate or the FortiExtender must also have a static IP configured.

To display the status of virtual router on FortiExtender:

```
get router info vrrp
```

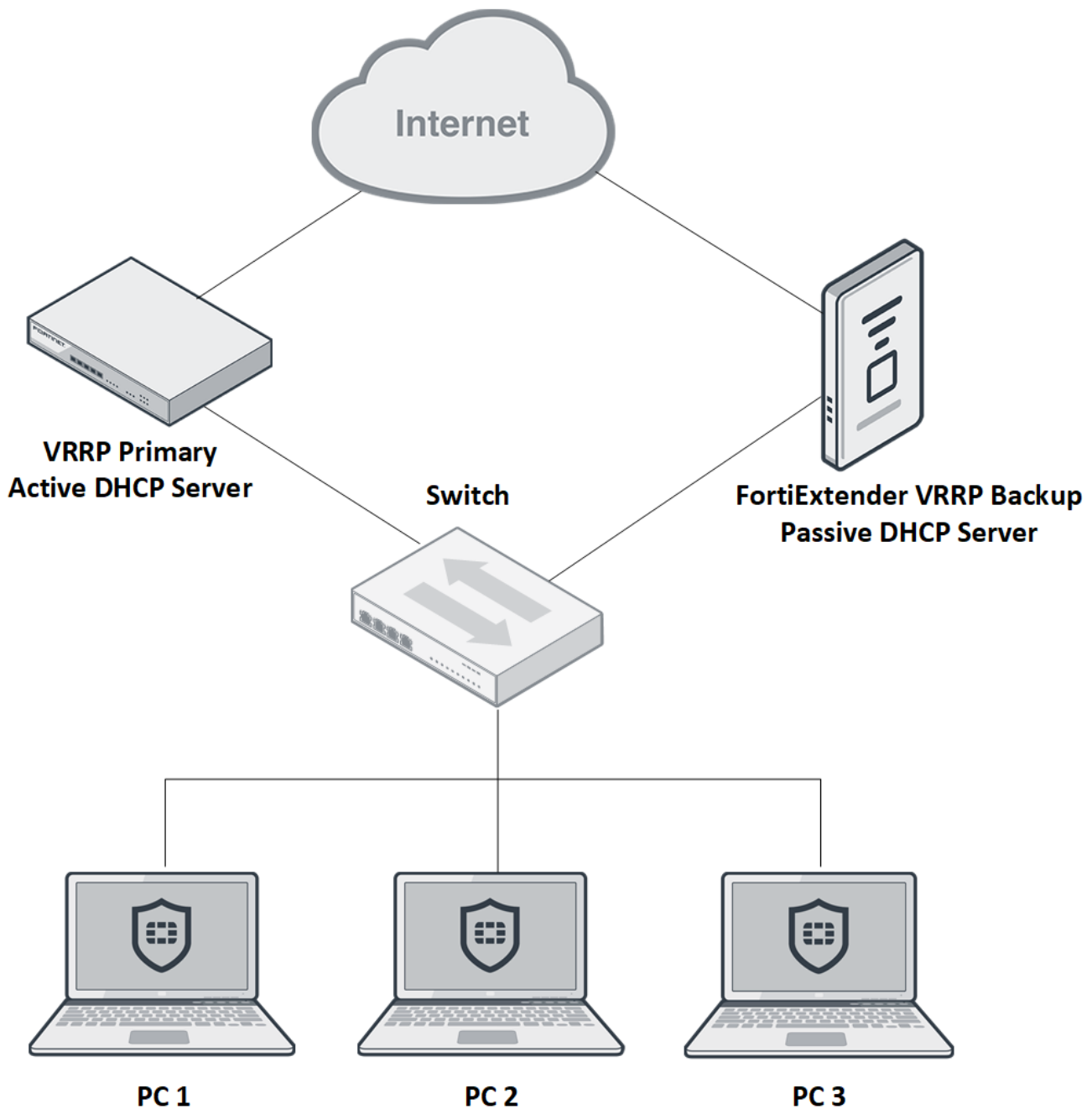
Enable DHCP server on FortiExtender and the VRRP primary router

To ensure uninterrupted presence of a DHCP server when one of the VRRP-capable routers is down, you must ensure IP address availability all the time. Typically, both the VRRP primary and the backup routers are configured with DHCP servers with reserved IP addresses to their corresponding MAC addresses.

The FortiExtender configured in VRRP backup mode will not launch the replicated copy of the DHCP server until and unless the VRRP primary router goes down; The FortiExtender will also terminate the DHCP server when the VRRP primary router comes back up. This ability ensures that the hosts in the VRRP domain always get the same IP address, irrespective of which VRRP router is in operation, without causing any IP address conflict.

For information on DHCP server configuration, see [Configure DHCP server](#).

DHCP server enabled on FortiExtender and VRRP primary router



Enable DHCP relay on both FortiExtender and the VRRP primary router

You must guarantee IP address availability to ensure access to the DHCP server at any time. The hosts must be able to access a DHCP server locally or remotely on an uninterrupted basis. In the event that the DHCP server is not present

locally, a DHCP relay agent service is needed to receive DHCP requests from DHCP hosts and forwards the requests to the remote DHCP server, receive responses from the server, and cater to the needs of DHCP clients. In this configuration, the FortiExtender which acts in VRRP backup mode will be running a DHCP relay agent on a VRRP interface; the VRRP primary router is also running a DHCP relay agent on the respective VRRP interface. This ability ensures that the hosts in the VRRP domain always get the same IP address, irrespective of which VRRP router is in operation, without causing any IP address conflict because the requests are catered to by the same remote DHCP server.

For information on DHCP relay configuration, see [Configure DHCP relay](#).

DHCP relay

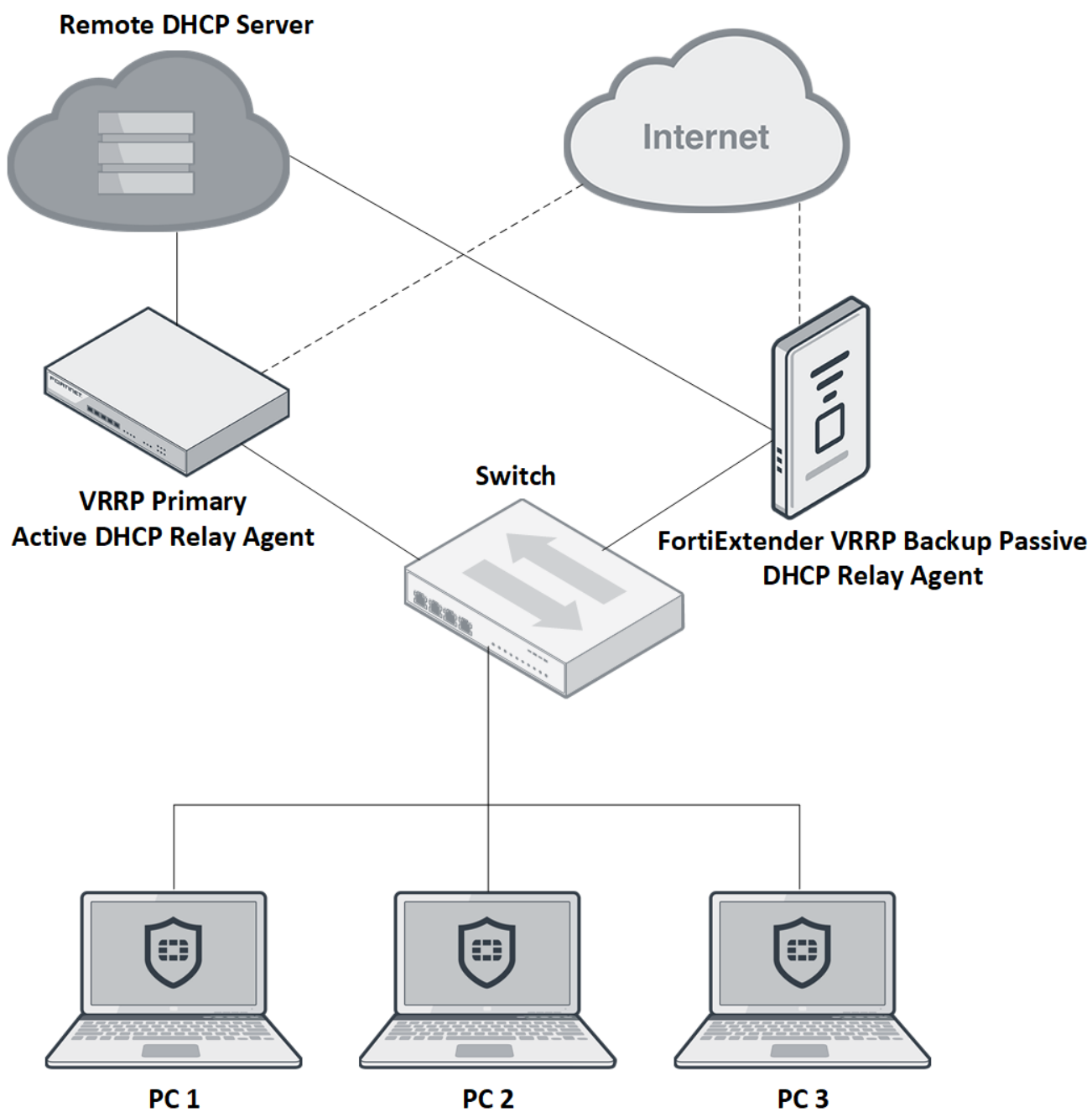
FortiExtender supports DHCP relay agent which enables it to fetch DHCP leases from a remote server. It has to be configured per interface. See the following example:

```
config system dhcprelay
  edit 1
    set status enable
    set client-interfaces <vrrp interface name on which relay agent services are offered>
    set server-interface <interface name through which DHCP server can be reachable>
    set server-ip <remote dhcp server IP>
  end
```



The DHCP relay and DHCP server services can be run on any VRRP interface, which could be either a separate port or a VLAN interface.

DHCP relay enabled on FortiExtender and VRRP primary router



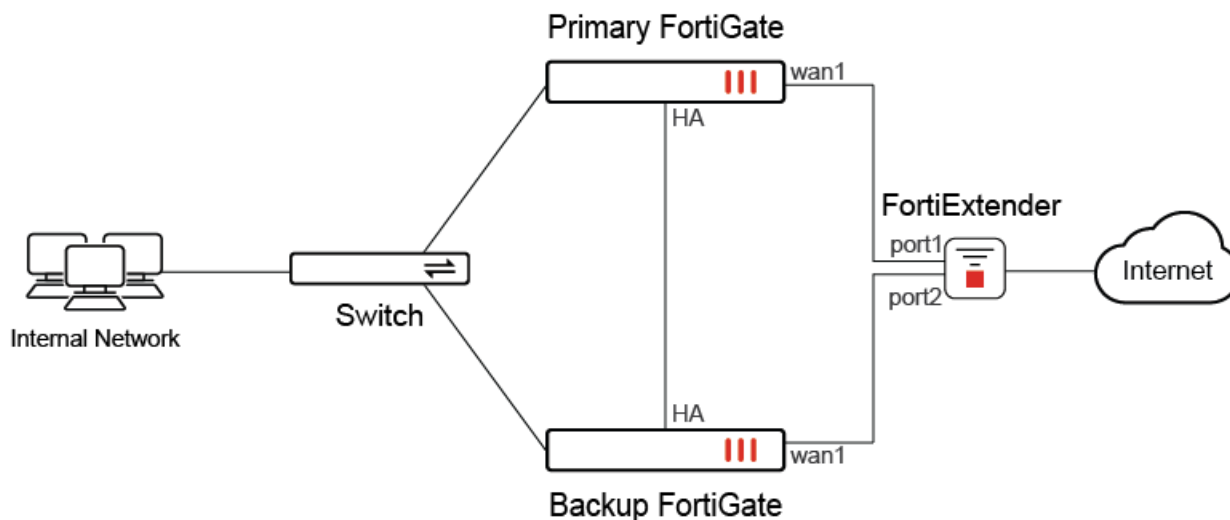
FortiExtender for FortiGate HA configuration



All models of FortiExtender devices support connecting to a FortiGate HA pair, except the legacy 40D models. FortiExtender 201E is used in the following discussion for illustration purposes.

This use case discusses how to use a FortiExtender 201E to support two FortiGate devices in HA configuration to ensure uninterrupted network connectivity and business continuity. It provides step-by-step instructions on how to configure the FortiGate HA cluster from the FortiGate GUI. It also provides the FortiExtender CLI commands to verify the port configuration of FortiExtender 201E as a WAN switch to support the FortiGate HA configuration.

Example network topology



Prerequisites

- The FortiExtender 201E device must be physically networked with the two FortiGate devices, with its port1 connected to a physical port (for example, wan1) on the primary FortiGate and port2 connected to the same physical port number on the backup FortiGate, as illustrated in the example network topology.
- The two FortiGate devices must be physically connected via the HA port on both of them, as illustrated in the example network topology. On FortiGate models that do not have a HA port, you can connect another pair of physical ports as dedicated heartbeat interfaces.
- The two FortiGate devices must be running the same version of FortiOS.



The FortiGate devices used in this sample configuration are both running FOS 7.6.0.

Configuration procedures

This configuration involves the following major steps:

Step 1: Configure the primary FortiGate

1. Log in to the GUI of the primary FortiGate device.
2. From the menu, go to *Dashboard > Status*.
The *Status* page opens.
3. Locate the *System Information* widget, click the *Hostname*, and (from the drop-down menu) select the *Configure settings in System > Settings* link.
The *System Settings* page opens.
4. Change the *Hostname* to something that identifies the FortiGate as the primary device, and click *Apply*.
5. Go to *System > HA*, click the top part of the page to highlight it, and click *Edit*.
The *High Availability* page opens.



The *Edit* button will not be available until the top part of the Status page is highlighted.

6. Make the following required entries and/or selections:
 - a. Change *Mode* to *Active-Passive*.
 - b. Set *Device Priority* to a value greater than the one set on the backup FortiGate.
 - c. Specify the *Group name*.
 - d. Set the *Password*.
 - e. Select *Heartbeat interfaces* by doing the following:
 - i. Click + (plus sign), and (from the pop-up list of interfaces) select either *ha* or the heartbeat interfaces you connected in the Prerequisites section.
 - ii. Click *OK*.
 - f. Optionally, configure link failover by monitoring the FortiGate port that is connected to the FortiExtender by doing the following:
 - i. Select *Monitoring interfaces*.
 - ii. Click + (plus sign) again, and (from the pop-up list of interfaces) select *wan1*.
 - iii. Click *OK*.

Step 2: Configure the backup FortiGate

1. Log in to the GUI of the backup FortiGate device.
2. From the menu, go to *Dashboard > Status*.
The *Status* page opens.
3. Locate the *System Information* widget, click the *Hostname*, and (from the drop-down menu) select the *Configure settings in System > Settings* link.
The *System Settings* page opens.
4. Change the *Host name* to something that identifies the FortiGate as the backup device, and click *Apply*.
5. Go to *System > HA*, click the top part of the page to highlight it, and click *Edit*.
The *High Availability* page opens.



The *Edit* button will not be available until the top part of the Status page is highlighted.

6. Make the following required entries and/or selections:
 - a. Change *Mode* to *Active-Passive*.
 - b. Set the *Device Priority* value smaller than the one set for the primary FortiGate.
 - c. Set the *Group name* to be the same as the one set on the primary FortiGate.
 - d. Set the *Password* to be the same as the one set on the primary FortiGate.
 - e. Select *Heartbeat interfaces* by doing the following:
 - i. Click + (plus sign), and (from the pop-up list of interfaces) select either *ha* or the heartbeat interfaces you connected to in the Prerequisites section.
 - ii. Click *OK*.
 - f. Optionally, configure link failover by monitoring the FortiGate port that is connected to the FortiExtender by doing the following:
 - i. Select *Monitoring interfaces*.
 - ii. Click + (plus sign) again, and (from the pop-up list of interfaces) select *wan1*.
 - iii. Click *OK*.

Step 3: Verify the port settings on FortiExtender

1. Ensure that Port 1 on the back of the FortiExtender is connected to the WAN1 port on the primary FortiGate. Refer to the Network topology.
2. Ensure that Port 2 on the back of the FortiExtender is connected to the WAN1 port on the backup FortiGate. Refer to the Network topology.
3. Run the following commands to verify and ensure that the physical Ports 1 and 2 are aggregated in the LAN switch port.

```
FX211E5919000011 # config system interface
FX211E5919000011 (interface) # edit lan
FX211E5919000011 (lan) # show
edit lan
    set type lan-switch
    set status up
    set mode dhcp
    set mtu 1500
    set vrrp-virtual-mac enable
    config vrrp
        set status disable
    end
    set allowaccess http https ssh ping telnet
next

FX211E5919000011 # config system lan-switch
FX211E5919000011 (lan-switch) # show
config system lan-switch
    config ports
        edit port1
        next
        edit port2
```

```
next
edit port3
next
end
end
```



- VLAN mode is best suited for high availability purposes because it delivers better throughput.
 - The "show" commands above yield the default settings of FortiExtender 201E as a LAN switch, which can be used out of the box to support FortiGate HA configurations. We recommend using these settings without change unless you are confident in your ability to configure custom settings of your own. If you prefer to configure your own LAN switch, be sure to use the aforementioned commands to double-check its configuration before putting FortiExtender to work.
-



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.