Admin Guide

FortiExtender (Managed) 7.6.5

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

Apr 9, 2026
FortiExtender (Managed) 7.6.5 Admin Guide
36-765-1236481-20260326

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 **12**
Managed FortiExtender overview 12
Managed FortiExtenders 13
FortiExtender SSIDs 15
FortiExtender Profiles 17
Data Plans 20
Provision FortiExtender firmware upon authorization 22
Connect to FortiGate 23
Wireless WAN extension to WAN interfaces of FortiGate 23
Wireless extension to internal LAN interface of FortiGate 24
Authorize FortiExtender on FortiOS 24
Enable FortiExtender Controller on FortiOS 25
Check current management mode 27
Support for device password and allowed protocols for FortiExtender in FortiGate 28
Configuring FortiExtender in a non-root VDOM 29
FortiExtender as FortiGate LAN extension **34**
Authorizing the devices 35
Backhaul tunnel and VXLAN auto-deployment 39
Configuring the LAN extension and firewall policy 42
FortiGate-FortiExtender LAN-extension ZTP 43
Using the backhaul IP when the FortiGate access controller is behind NAT 46
Examples 46
Bandwidth limits on the FortiExtender Thin Edge 54
IPAM in FortiExtender LAN extension mode 56
FortiExtender LAN extension in public cloud FortiGate-VM 63
Discover a FortiExtender unit 70
Broadcast 70
Static 70
De-authorize FortiExtender devices 72
LAN extension profile configuration 74
Backhaul configuration 76
Discovery response lockdown 78
Wildcard 79
Data transportation over the LAN extension interface 81
Backhaul IP in LAN extension 83
Fast failover of CAPWAP control channel between two uplinks 84
Topology 84

CLI 85
VLAN support for LAN extension mode 88
Wireless configurations on FortiExtender 97
Create a LAN extension SSID for FortiExtender 97
Configure a FortiExtender profile 98
Apply the profile to FortiExtender and authorize the device 99
Configure the LAN extension interface as a DHCP server 100
Configuring a firewall policy 102
Verify settings 103
Dynamic Frequency Selection channels 104
Configure split tunneling in LAN extension mode 106
FortiExtender as FortiGate WAN extension 112
FortiGate-FortiExtender WAN-extension ZTP 112
VLAN mode on FortiExtender as the WAN-extension of FortiGate 113
Configuring VLAN with Port4 113
Configuring VLAN with the LAN port 120
Hitless failover in WAN-extension mode in HA configuration 129
Multiple APNs in WAN-Extension mode 131
Manage dual FortiExtender devices 135
Active/Passive mode 135
Active/Active mode 135
Cellular as backup of Ethernet WAN 135
SD-WAN 136
Configure cellular settings 139
Configuring a data plan 139
Set the default SIM 141
Configure SIM-switch 142
Configure SIM-switch based on link health 145
Report to FortiGate 146
CAPWAP on multiple ports for broadcast discovery 147
CAPWAP mode 147
Get modem status 149
Access other devices via SSH 150
Use cases 151
Redundant with FortiGate in IP pass-through mode 151
Enable DHCP server on FortiExtender and the VRRP primary router 153
Enable DHCP relay on both FortiExtender and the VRRP primary router 154
IPv6 in IP pass-through mode 155
FortiExtender for FortiGate HA configuration 158
Example network topology 159
Prerequisites 159
Configuration procedures 159

Change Log

Date	Change Description
2026-02-13	Initial release.
2026-03-09	Added FortiGate-FortiExtender LAN-extension ZTP on page 43.
2026-04-09	Updated FortiExtender and FortiGate integration on page 12.

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 7.6.5 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 or through FortiExplorer Go (for applicable BLE capable models).

  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

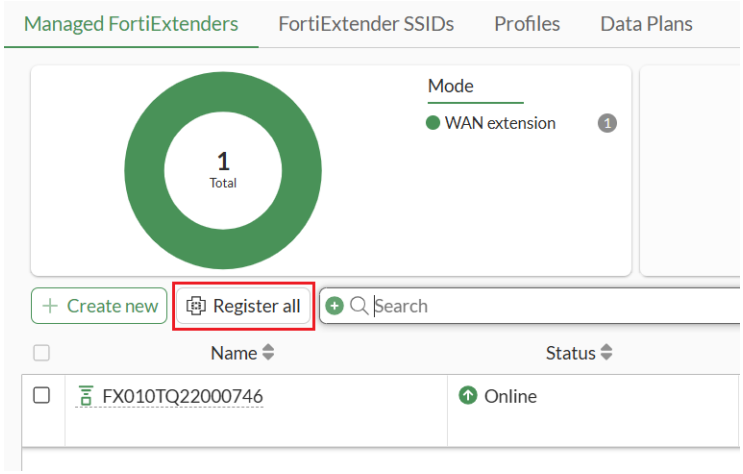
After installing and authorizing your FortiExtender on FortiGate, you can register your FortiExtender to FortiCare. FortiCare enables you to manage security fabric devices such as FortiAP, FortiSwitch, and FortiExtender from a root FortiGate device. Once your FortiExtender is registered with FortiCare, 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.

You can add FortiExtenders to FortiCare through the following methods:

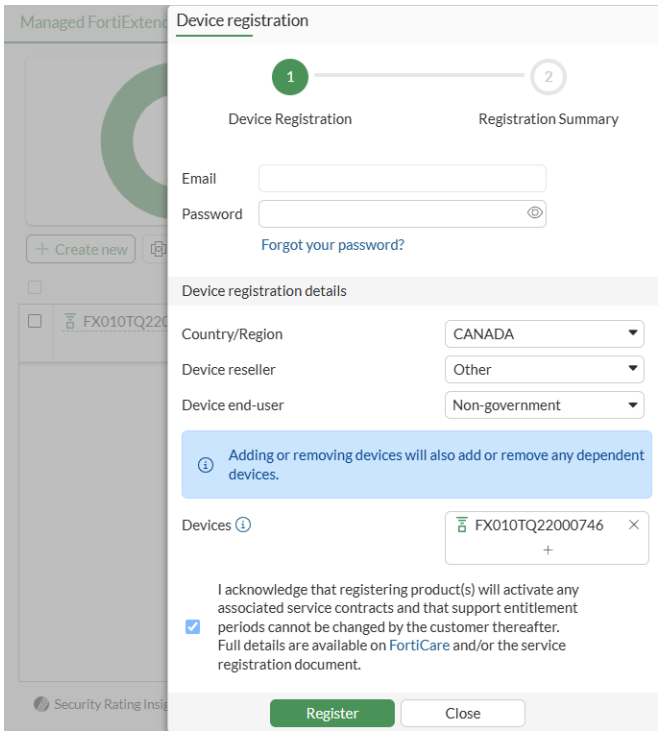
- Through the FortiGate (GUI and CLI): The FortiExtender must have an active connection to the FortiGate
- Through the FortiCloud portal: For more information about registering through FortiCloud, refer to the FortiCloud Services documentation.

To register a FortiExtender to FortiCare via FortiGate - GUI

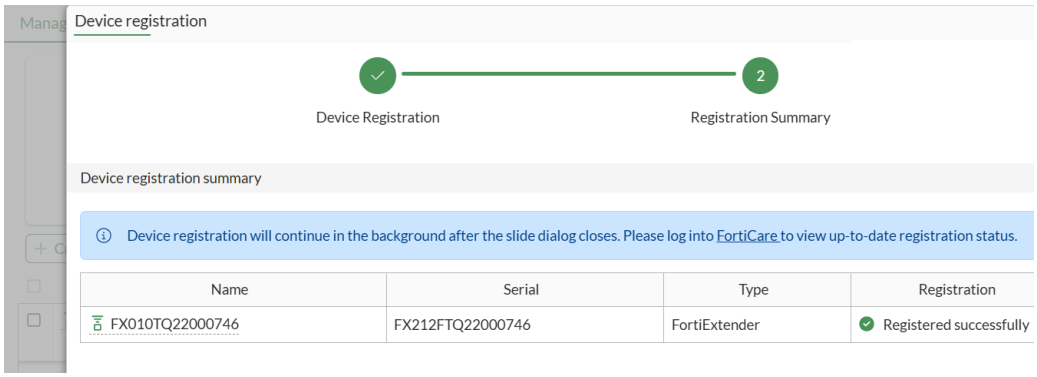
1. From the FortiGate, go to *Network > FortiExtenders > Managed FortiExtenders*.
   If there are any authorized FortiExtenders that have not been registered yet, a *Register all* button is available.



2. Click *Register all* to begin registering your device.
3. Complete the following:
   a. Enter your FortiCloud account credentials.
   b. Enter the device registration details.
   c. Select the device serial numbers of the FortiExtenders you want to register.
   d. When you are finished, click *Register*.



4. FortiGate displays the registration result.



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 can be integrated with FortiGate for following purposes:

- FortiExtender as FortiGate LAN extension on page 34
- FortiExtender as FortiGate WAN extension on page 112

This section contains general topics that apply to FortiExtenders operating in LAN extension and WAN extension mode.

Maximum number of FortiExtenders supported by FortiGate

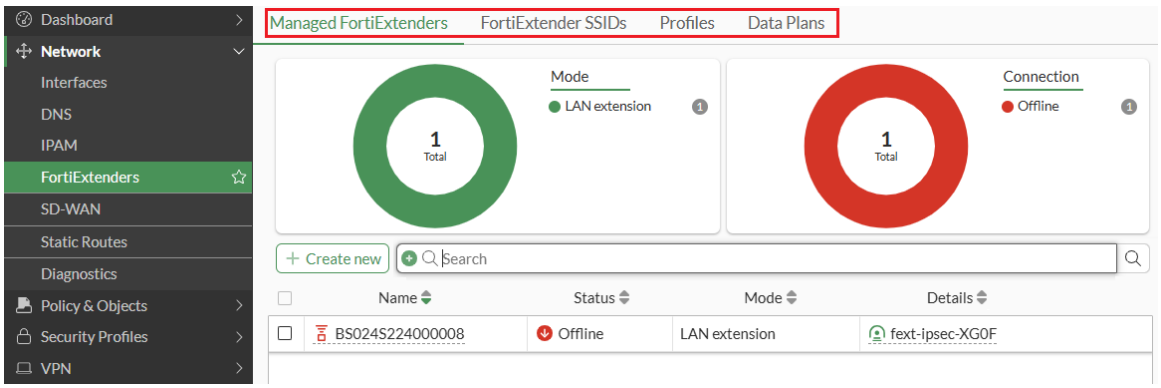
The number of FortiExtender devices that can be used as FortiGate LAN/WAN extension is dependent on the available memory of the FortiGate platform. The following table highlights the maximum numbers of FortiExtenders that FortiGate platforms can support in such configurations.

FortiGate Models/VM	WAN	LAN
FortiGate 40F series and its variants, FortiGate 50G series and their variants, FortiGate VM01	2	0
FortiGate 60F, 70F, 80F series and their variants, FortiGate 70G, 90G series and their variants, FortiGate VM02	2	16
FortiGate 100E to 200F series and their variants, FortiGate 120G series and their variants	2	16
FortiGate 400F to 900G series and their variants, FortiGate VM04	2	32
FortiGate 1000D to 2600F series and their variants, FortiGate VM08	2	256
FortiGate 3000D and higher, FortiGate VM16 and higher	2	1024

Managed FortiExtender overview

When a FortiExtender is managed by FortiGate, you can manage and configure your FortiExtender devices from *Network* > *FortiExtenders*. This section contains four tabs related to managing your FortiExtenders:

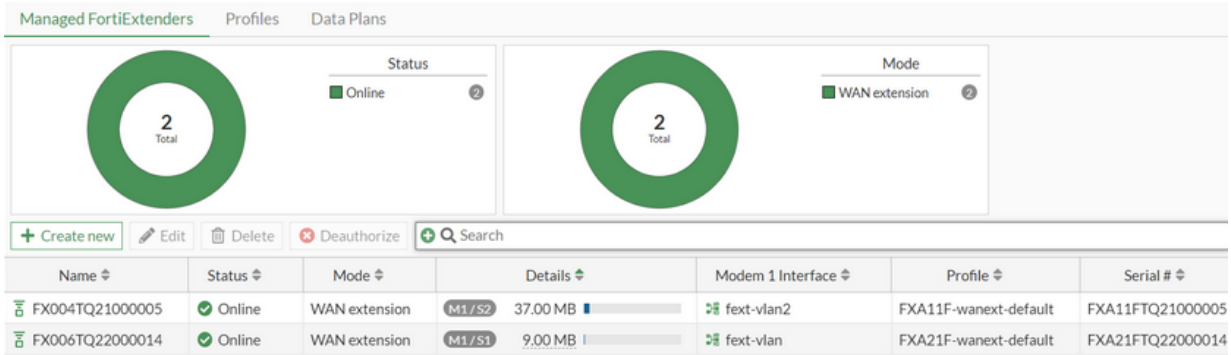
Menu Tabs	Description
Managed FortiExtenders (Default)	Add new FortiExtenders and view a list of your FortiGate managed devices. You can see their connection status, mode, and apply filtering options.
FortiExtender SSIDs	Create and manage your FortiExtender SSIDs.
Profiles	Create and manage your FortiExtender profiles.
Data Plans	Create and manage your FortiExtender data plans.



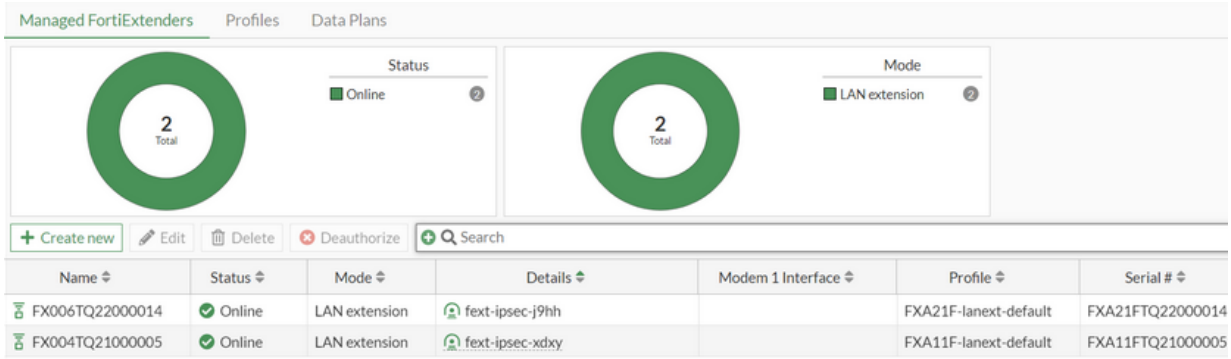
Managed FortiExtenders

The *Managed FortiExtenders* tab in the *Network* > *FortiExtenders* page contains the following:

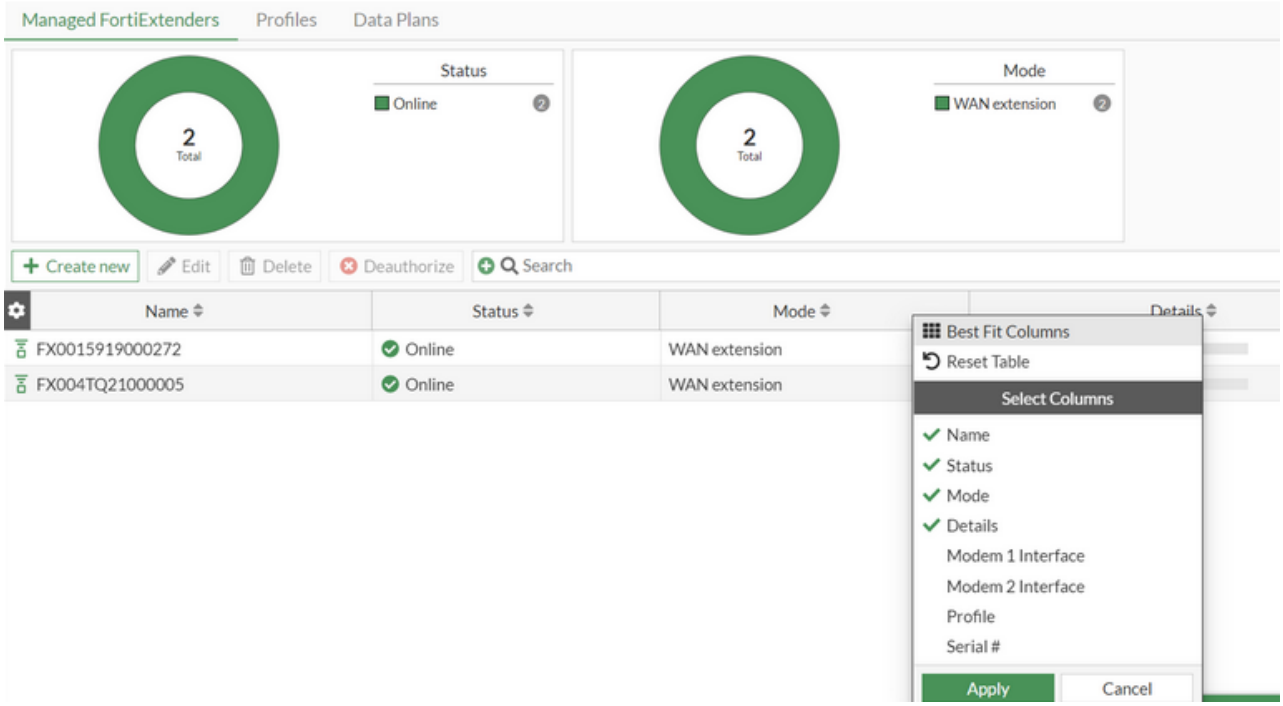
- An overview of FortiExtenders detected on your network as well as their connection status and extension mode.
- Columns that show different information depending on which extension mode the FortiExtender device is operating in.
  - **WAN extension mode:**
    - The *Details* column shows data used on the modem/SIM card.
    - 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.



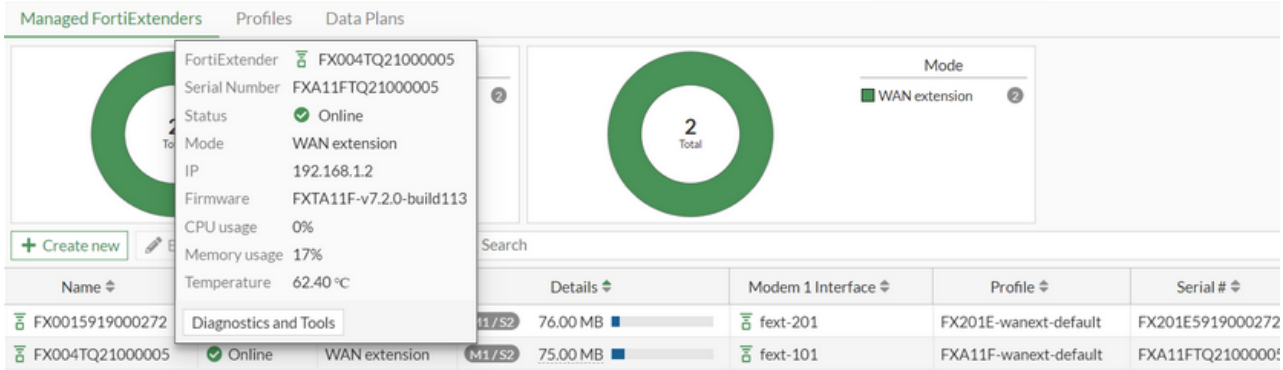
  - **In LAN extension mode:**
    - The *Details* column shows the connected IPsec tunnel used between FortiGate and FortiExtender.

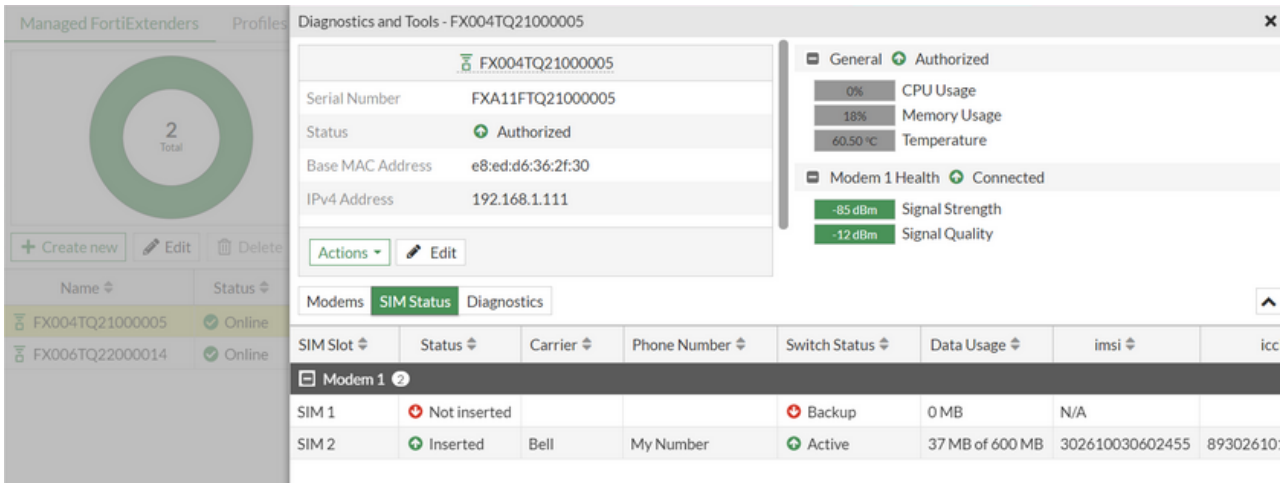


- Options to add additional columns when right-clicking column headers.



- When FortiExtender is in WAN extension mode, you can view modem information by left-clicking the name of the FortiExtender or hover the mouse over the name to get the tooltip to appear. From the tooltip, you can select *Diagnostics and Tools* to see the detailed FortiExtender diagnostic pages.



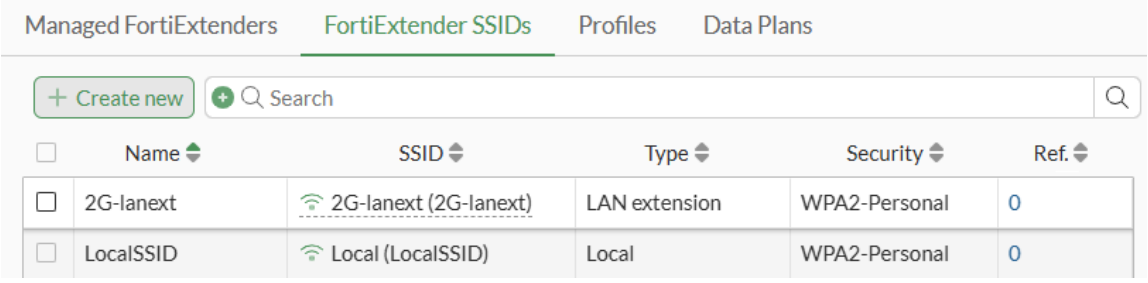


FortiExtender SSIDs

The *FortiExtenders SSIDs* tab in the *Network > FortiExtenders* page enables you to create and manage your FortiExtender SSIDs.

FortiExtender SSIDs are supported on supported FortiExtender models when used as a FortiGate LAN extension. This allows wireless clients behind a managed FortiExtender to access the internet, even when the FortiGate is in LAN extension mode.

FortiExtender SSIDs must be applied to a FortiExtender LAN extension profile to take affect.



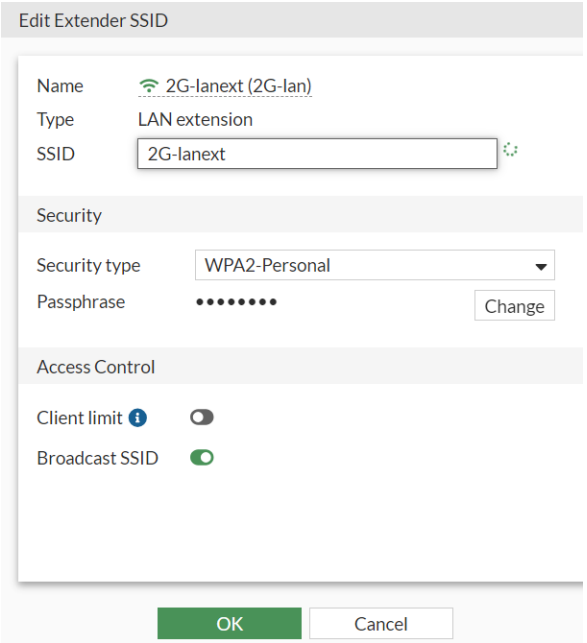
For information on configuring a FortiExtender SSID from the CLI, see Wireless configurations on FortiExtender on page 97.

To configure a FortiExtender SSID - GUI:

1. Go to *Network > FortiExtenders > FortiExtender SSIDs*, and click *Create new*.
2. Configure the following options:

Name	Enter a name for your SSID plan.
Type	Select what type of SSID you want: • *Local SSID*: The SSIDs to be used by FortiExtender's local network.

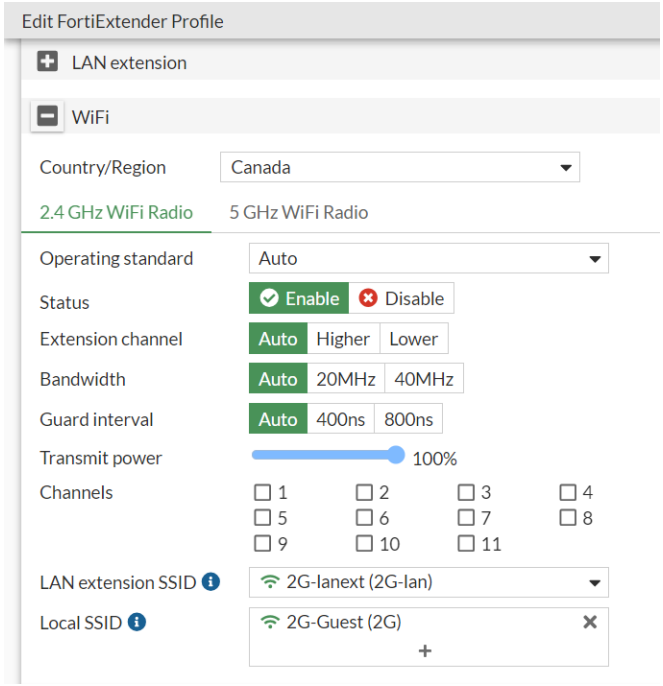
	Connected devices may access the local network or internet, which are directly controlled by FortiExtender's firewall policies. Each radio can manage up to three local SSIDs simultaneously. • *LAN extension SSID*: The SSID to be used by the LAN extension network. All device traffic via this SSID will follow the IPsec tunnel to the FortiExtender's LAN extension controller FortiGate.
SSID	Enter an SSID name to be broadcasted.
Security type	Select a security type.
Passphrase	Enter a password for the SSID.
Client limit	The maximum number of clients allowed to connect to this SSID.
Broadcast SSID	Select if you want to broadcast the SSID.
IP/Netmask	For Local SSIDs only. Enter the FortiExtender IP address.
Address range	For Local SSIDs only. Enter the FortiExtender IP address range.
Administrative access	For Local SSIDs only. Select which types of administrative access you want to allow for the FortiExtender.



3. When you are finished, click *OK*.

To apply the SSID to a FortiExtender profile:

1. Go to *Network* > *FortiExtenders* > *Profiles* and select or create a supported FortiExtender profile.
2. Ensure the profile *Mode* is set to *LAN extension* and expand the *WiFi* section.
3. Select the radio band you want to use, *2.4 GHz WiFi Radio* or *5 GHz WiFi Radio* and set the *Status* to *Enable*.

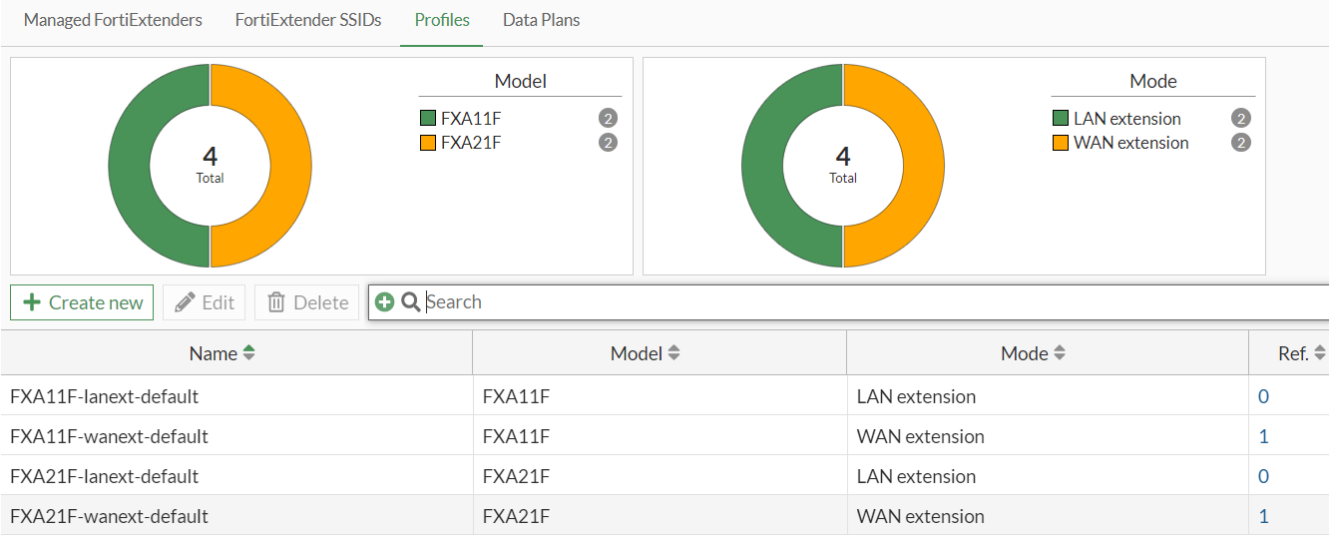


4. In *LAN extension SSID*, select a LAN type SSID.
5. In *Local SSID*, select a Local type SSID.
6. When you are finished, click *OK*.

FortiExtender Profiles

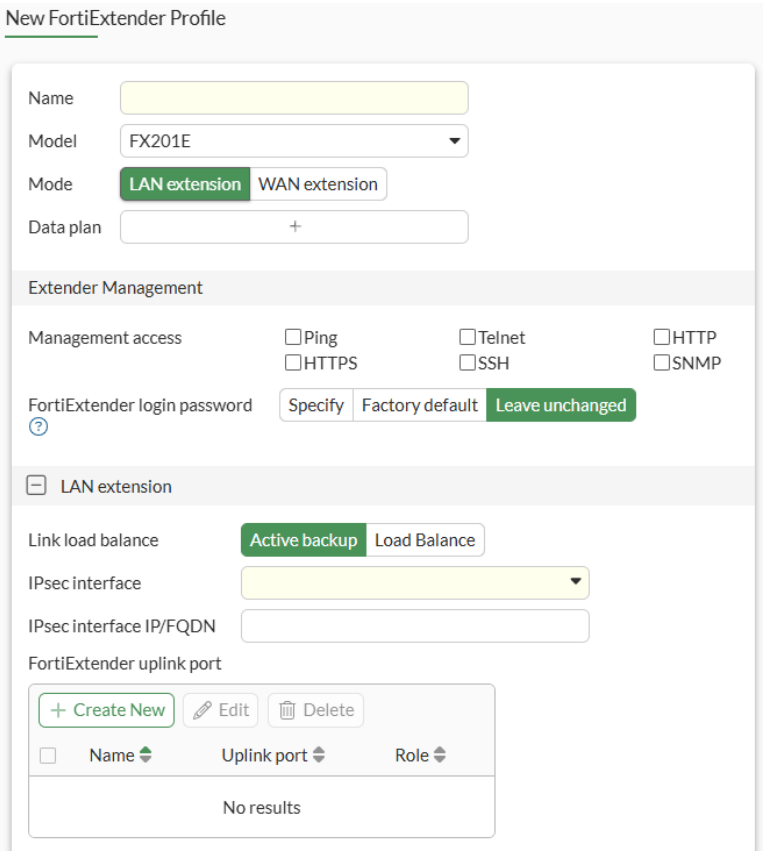
The *Profiles* tab in the *Network* > *FortiExtenders* page enables you to create and manage your FortiExtender profiles. A FortiExtender profile defines the data plan, modem settings, SIM switching behavior for a particular FortiExtender model, and FortiExtender controller reporting options. The profile can also be used to configure the IPsec tunnel connection between FortiExtender and FortiGate if the FortiExtender is in LAN extension mode.

Different profiles configurations are available depending on whether the FortiExtender is operating in WAN extension or LAN extension mode.



To configure a FortiExtender profile - GUI:

1. *Go to Network > FortiExtenders > Profiles* and click *Create new*.
2. Enter a *Name* for the FortiExtender Profile.
3. In *Model*, select the FortiExtender model to which this profile applies.
4. In *Mode*, select which extension setting you want.
   The FortiExtender Profile loads configurations specific to the extension mode you selected.



5. Configure the following general options:

Data plan	Select the data plan you want to apply to this profile.
Management access	Select which types of management access you want to allow to the FortiExtender:
FortiExtender login password	Select if you want set a new FortiExtender login password, set it the default password, or leave the current password unchanged.

6. If you selected LAN extension mode, configure the following LAN extension settings:

Link load balance	Select a link load balance strategy. • *Active backup*: Has only one active connection that automatically switches to a backup connection if the primary fails. • *Load Balance*: Actively distributes traffic across multiple connections to optimize performance.
IPsec interface	Select an IPsec phase1 interface.
IPsec interface IP/FQDN	Enter an IPsec phase1 IPv4/FQDN. This is used to specify the external IP/FQDN when the FortiGate unit is behind a NAT device.
FortiExtender uplink port	Create and add an uplink port.
Name	Enter a FortiExtender LAN extension backhaul name.
Uplink port	Select a FortiExtender uplink port.
Weight	For load balance strategy only. Enter a Weighted round robin weight parameter.
FortiExtender downlink	Create and add a downlink port.
Name	Enter a FortiExtender LAN extension downlink name.
Interface	Select a FortiExtender LAN extension downlink port.
VLAN ID	Enter a FortiExtender LAN extension downlink port VLAN ID (PVID).

7. For each modem, configure the following:

Default SIM	Define which SIM card starts to work first. • *SIM1*: Use SIM #1 by default. • *SIM2*: Use SIM#2 by default. • *Carrier*: Assign a default SIM based on your preferred carrier. • *Lowest cost*: Assign a default SIM based on cost.
SIM 1/2 PIN	Enable/disable the SIM PIN. If enabled, you can change the PIN.
GPS	Enable/disable the FortiExtender GPS.
Auto SIM Switch	Select how you want to determine when the SIM switches: • *By disconnecting*: Switch based on cellular disconnections. You can set a threshold or time period in seconds. • *By signal*: Switch based on cellular signal quality. • *By data plan*: Switch when data usage has reached the data limit in the

	plan.

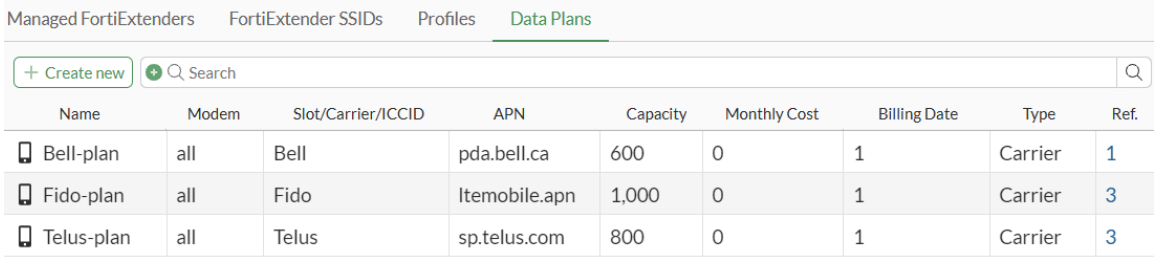
8. Configure the FortiExtender controller report options:

Controller report	Enable/disable controller reporting.
Interval	Set the controller report interval.
Signal threshold	Set the controller report signal threshold.

9. When you are finished, click OK.
   The profile is saved and can be applied to a FortiExtender.

Data Plans

The *Data Plans* tab in the *Network* > *FortiExtenders* page enables you to create and manage your FortiExtender data plans. Data plans allow users to configure connectivity settings based on modem, carrier, slot, SIM ID, or cost. Users can specify billing details related to the data plan, as well as smart switch thresholds to define when to switch over to a different SIM.



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	Itemobile.apn	1,000	0	1	Carrier	3
Telus-plan	all	Telus	sp.telus.com	800	0	1	Carrier	3

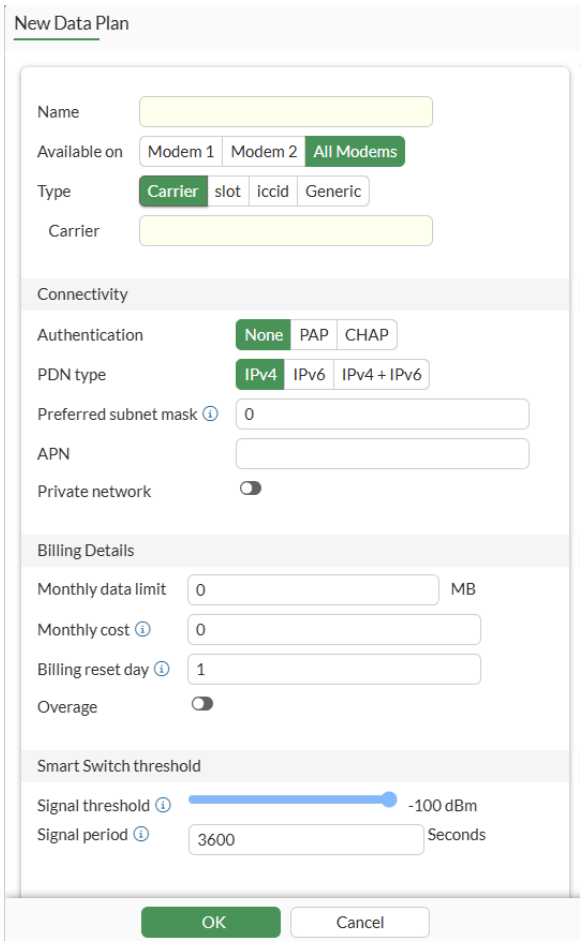
FortiExtender has multiple SIM card slots and modems depending on the model, and each modem can make one connection with one of the SIMs associated with the modem. A data plan allows users to create general configurations that work across multiple SIMs, or specific plans that work on a specific SIM. Each data plan is associated with a carrier name.

When a modem connects to the network through a SIM, it will read the SIM information and try to match a data plan based on the modem ID and type. It then uses the data plan connectivity settings to connect (authentication, PDN type, preferred subnet, APN, private network). The billing details (such as the monthly data limit) and smart switch threshold settings define how the SIMs will be switched. Each data plan has a data limit (capacity) that can be used by the SIM card and that data limit is reset after the billing date.

Data plans must be applied to a FortiExtender profile to take effect. Once the FortiExtender is managed by a FortiExtender profile, the data plan is synced with the FortiExtender.

To configure a data plan - GUI:

1. Go to *Network* > *FortiExtenders* > *Data Plans* and click *Create new*.
   The *New Data Plan* window loads.



2. Enter a *Name* for the data plan.
3. Configure the following options:

Available on	Select which modem you want this plan to be available on.
Type	Select which SIM the modem uses: • *Carrier*: Assign the SIM by carrier name. • *slot*: Assign based on SIM slot. • *iccid*: Assign a specific SIM based on its ICCID number. • *Generic*: Use any SIM if no other data plan matches the chosen SIM.
Authentication	Select an authentication type.
PDN type	Select a PDN IP address family.
Preferred subnet mask	Enter the preferred DHCP subnet.
APN	Enter the APN of the SIM card.
Private network	Enable/disable blocking all non-NATed traffic.
Monthly data limit	Enter the data plan limit per month.
Monthly cost	Enter in the plan's local currency.

Billing reset day	Enter the day of the month the billing cycle resets.
Overage	Enable/disable data plan overage detection.
Signal threshold	Specify a minimum threshold for signal strength to fall below in order to trigger a SIM switch
Signal period	Enter the amount of time in seconds that the signal strength must remain below the threshold to trigger a SIM switch.

4. When you are finished, click *OK*.

To configure a data plan - CLI:

```
config extension-controller dataplan
    edit "Telus-modem1"
        set modem-id modem1
        set type carrier
        set carrier "Telus"
        set capacity 2000
        set billing-date 30
    next
    edit "Fido-modem2"
        set modem-id modem2
        set type carrier
        set carrier "Generic"
        set capacity 3000
    next
    edit "Bell"
        set type carrier
        set carrier "Bell"
        set apn "pda.bell.ca"
        set capacity 6000
    next
end
```

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|Image
Identifier=07002000FIMG1000102000
```

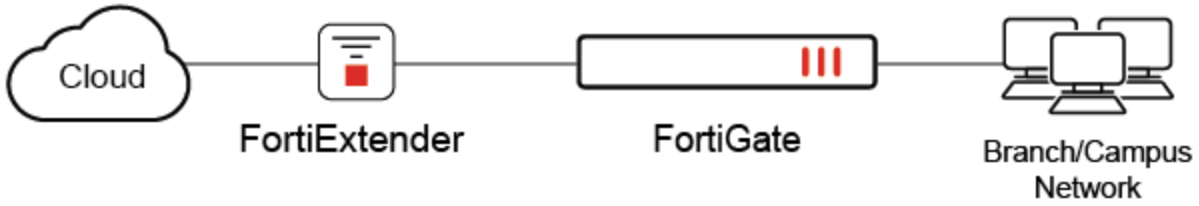
2. Test condition: The FortiGate has v7.2.1 b1247 and the FortiExtender has v7.0.3 b056.
```
config system global
      set fortiextender-provision-on-authorization enable
end
```
3. Once the FortiGate has authorized the FortiExtender, automatical update is enabled for one time.
```
   config extension-controller 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.

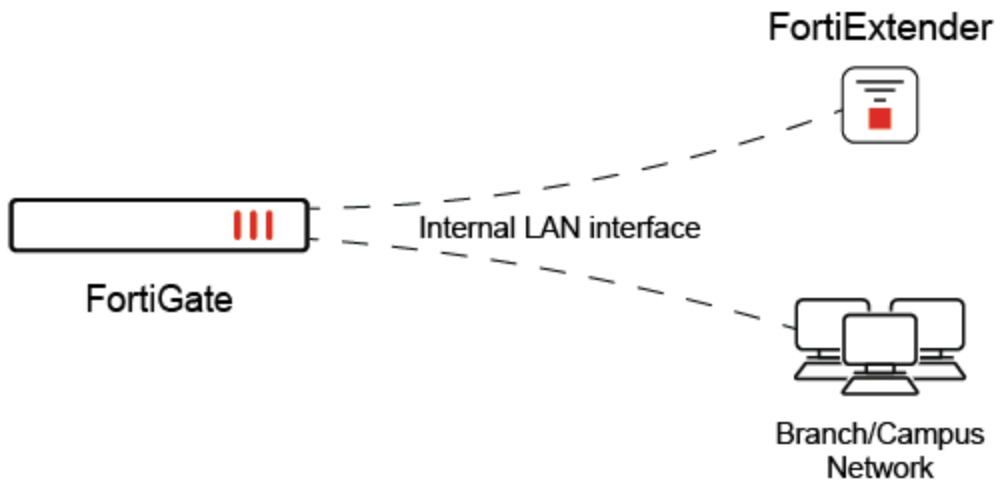
Wireless WAN extension to WAN interfaces of FortiGate



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



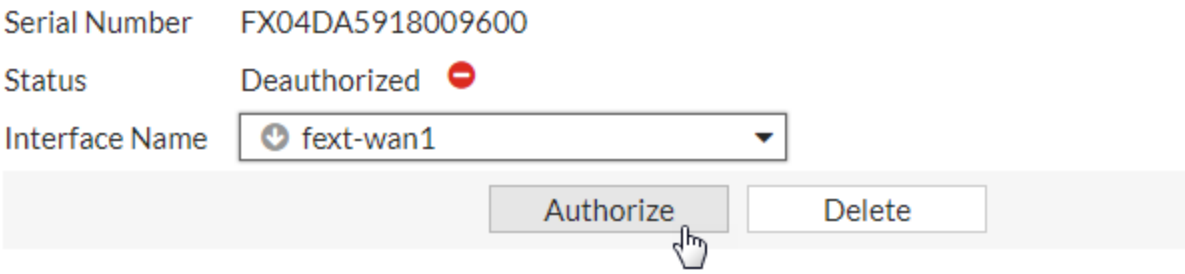
In some scenarios, you may want to connect the FortiExtender to an internal LAN interface of the FortiGate (to use POE power or some other means). In this case, if the FortiGate internal LAN is running a DHCP server, connect the FortiGate to port4 of the FortiExtender (FEX-201E/211E) which acquires DHCP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



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 was 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 allowacess 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.

Check current management mode

You can configure and manage your FortiExtender from FortiGate or FortiEdge Cloud. For FortiEdge Cloud management, the FortiExtender must have a valid support contract as well as a FortiEdge Cloud license.

If you are not sure "who" is your FortiExtender's controller, use the following command to find out:

```
FX511FTQ21001152 # get extender status
Extender Status
    name : FX511FTQ21001152
    mode : CAPWAP
    session : active
      fext-addr : 192.168.101.43
      ingress-intf : lan
      fext-wan-addr : 26.237.146.79
      controller-addr : 192.168.101.63:5246,25246
      controller-name : FG200FT921901199
      uptime : 0 days, 0 hours, 2 minutes, 25 seconds
      management-state : CWWS_RUN
    session : standby
      fext-addr : 0.0.0.0
      ingress-intf :
      fext-wan-addr : 26.237.146.79
      controller-addr : 0.0.0.0:5246,25246
      controller-name :
      management-state : CWWS_SULKING (H)
    session : obm
      fext-addr : 10.107.41.43
      ingress-intf : wan
      controller-addr : fortiextender-alpha-dispatch.forticloud.com:443
      account-id : 1208893
      uptime : 0 days, 0 hours, 3 minutes, 33 seconds
      management-state : CWWS_RUN
    base-mac : 94:FF:3C:0D:1A:C0
    network-mode : ip-passthrough (capwap)
    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
```

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.

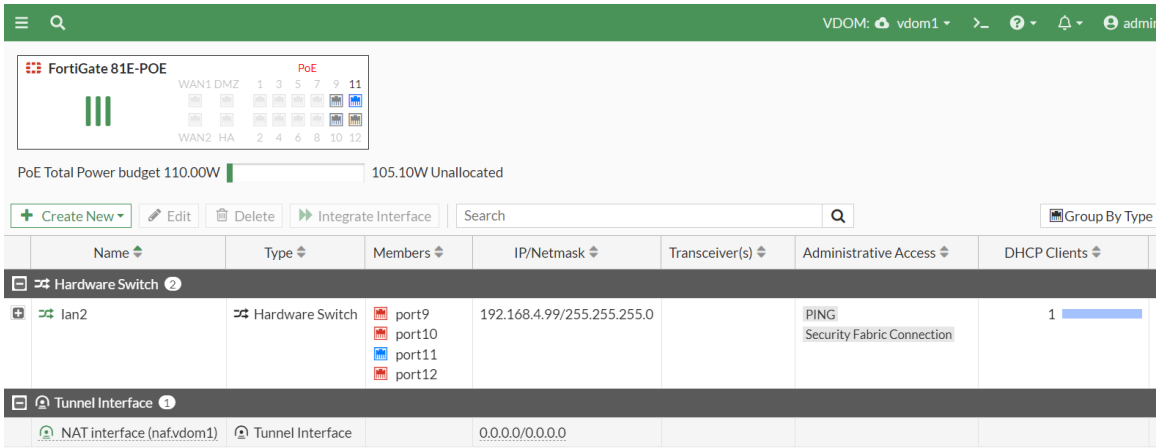
```
config system switch-interface
      edit le-switch <=== The entry cannot be edited or deleted
            set members le-agg-link lan
            set stp disable
      next
end
```

Configuring FortiExtender in a non-root VDOM

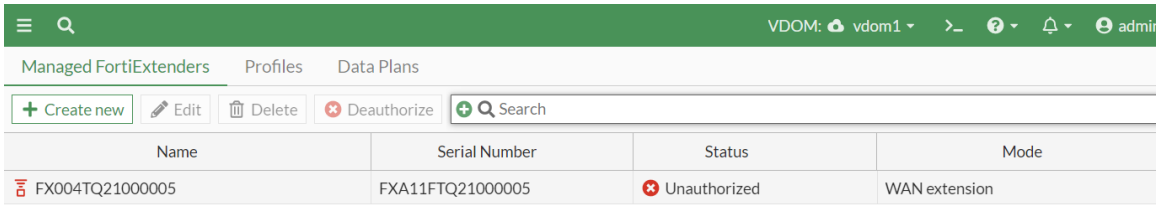
You can configure FortiExtender be managed and used in a non-root VDOM.

To configure FortiExtender in a non-root VDOM - GUI:

1. The FortiExtender can be found in each VDOM under *Network > Interfaces*. Configure the VDOM so that gets an interface (lan2) with Security Fabric Connection and a DHCP server. Then the FortiExtender can be discovered when connecting to lan2 port11.

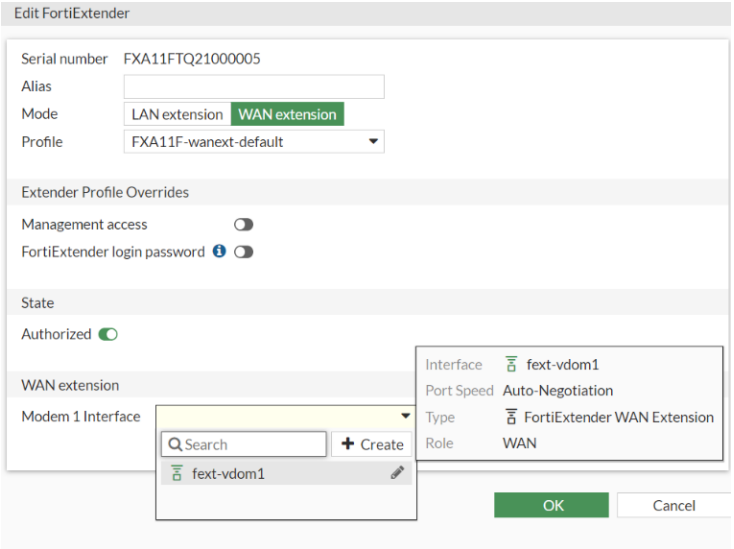


2. *Go to Network > FortiExtenders > Managed FortiExtenders* and right click the FortiExtender. Select *Authorization > Authorize*.



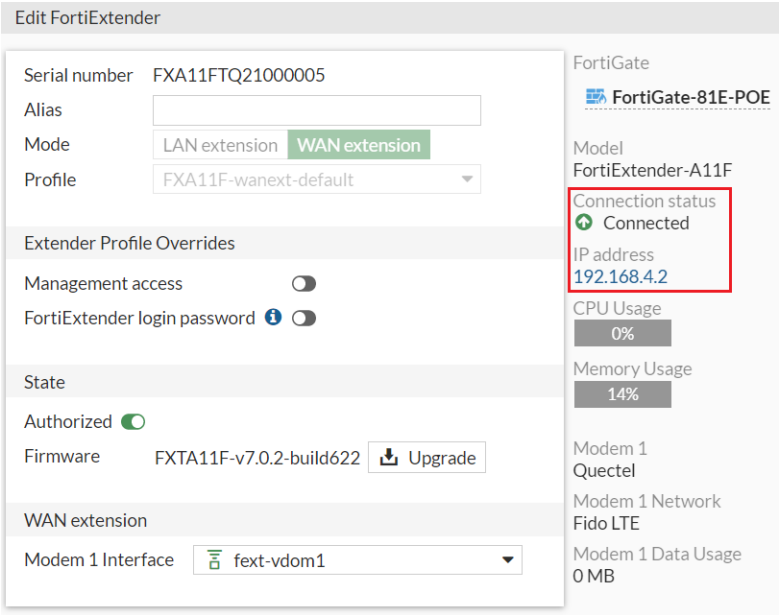
After it is authorized, the FortiExtender can provide an interface to the VDOM.

3. Click to edit the FortiExtender and then assign the FortiExtender interface to the LTE modem.

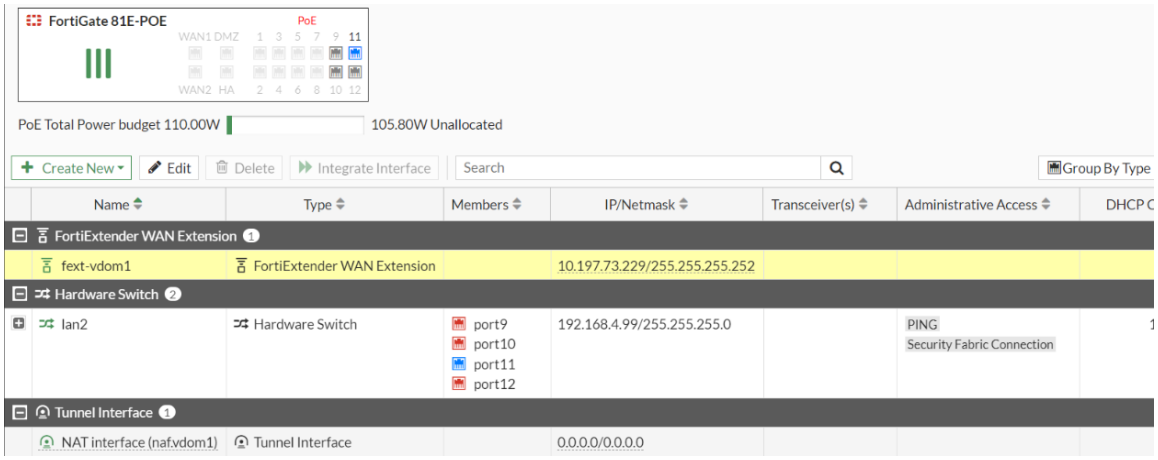


4. When you are finished, click OK.

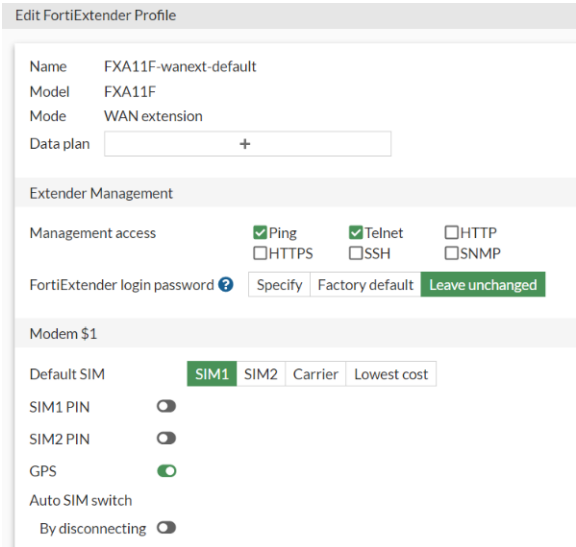
The FortiExtender connects to the FortiGate after authorization.



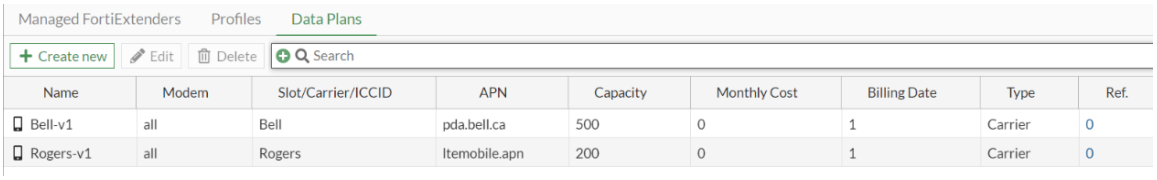
The FortiGate receives an IP and gateway address for the FortiExtender type interface in the VDOM.



5. Configure the FortiExtender profile and data plan per VDOM.
   - To configure a FortiExtender profile, go to *Network > FortiExtenders > Profiles*.



   - To configure a FortiExtender profile, go to *Network > FortiExtenders > Data Plans*.



To configure FortiExtender in a non-root VDOM - CLI:

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 assign the FortiExtender interface you previously created.

```
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. To verify configurations, 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. Configure 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
```

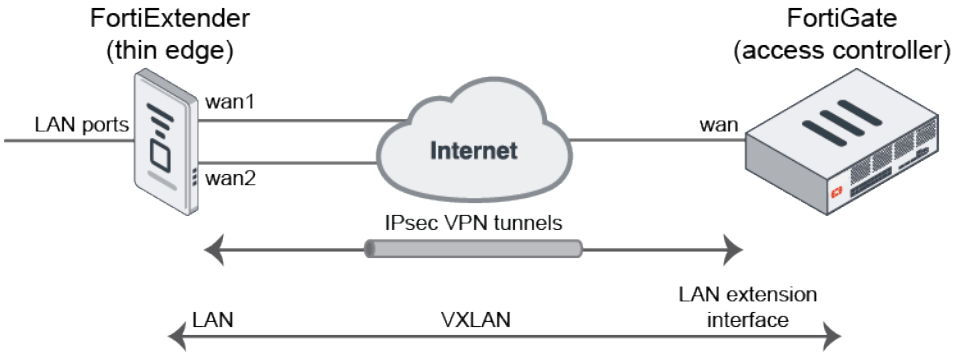
6. Create a FortiExtender data plan.

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

FortiExtender as FortiGate LAN extension

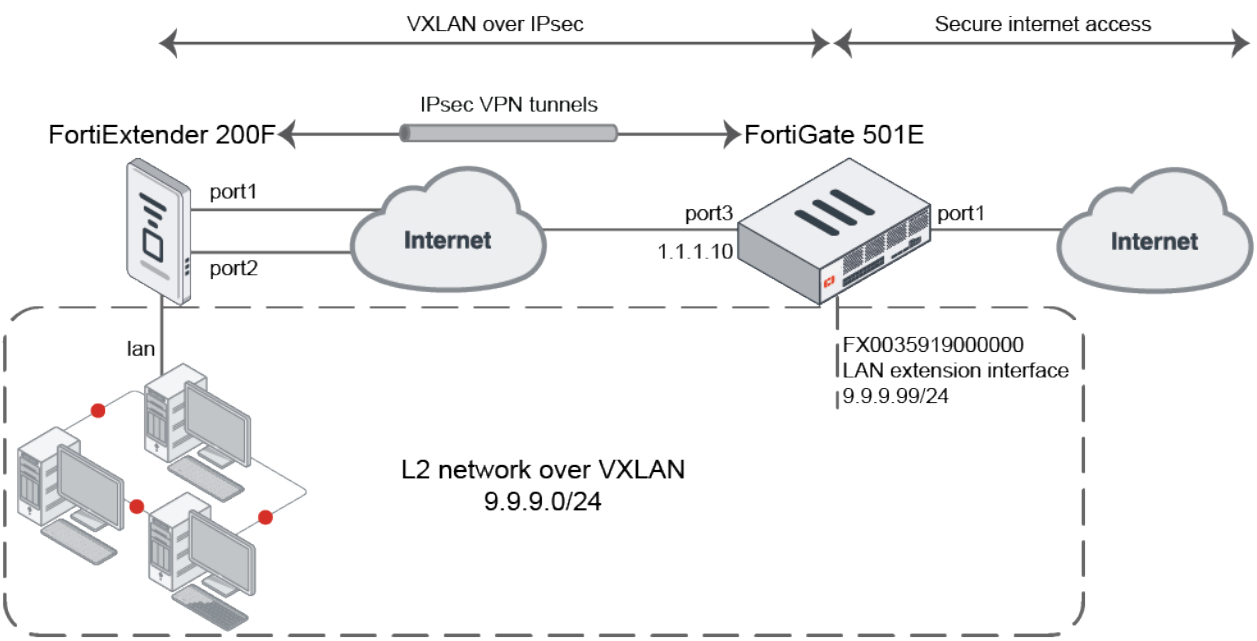
Many enterprises find themselves with locations where a small network exists and needs to be secured, but where it is unnecessary or cost prohibitive to deploy a firewall appliance. In those situations, security can be extended to the site in question from a centralized location, leaving only a "thin edge" of networking equipment at the site, while security actions are performed elsewhere.

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 topology, a FortiGate 501E acting as the FortiExtender AC provides secure internet access to the remote network behind the FortiExtender 200F thin edge.

- The FortiGate has two WAN connections: one is used as an inbound backhaul connection and the other for outbound internet access.
- The FortiExtender has two wired WAN/uplink ports connected to the internet.



Configuring LAN extension mode consists of the following:

1. The FortiExtender must discover the FortiGate AC and be authorized by the FortiGate.

   Once the FortiExtender is authorized, the FortiGate pushes an automatically configured extender profile to the FortiExtender. Using configurations from that profile, the FortiExtender forms two IPsec tunnels back to the FortiGate.
2. VXLAN aggregate interfaces and backhaul tunnels are deployed.

   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.
3. The LAN extension interface and firewall policies must be configured.

   Once the IPsec tunnel is set up, the LAN extension interface and firewall policies must be configured so clients behind the FortiExtender can connect to the internet through the FortiGate that secures the internet connection.

Authorizing the devices

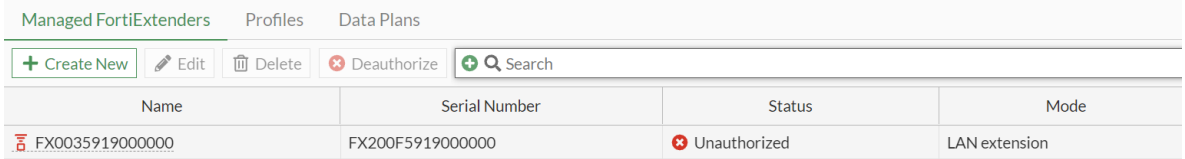
To discover and authorize the FortiExtender - GUI:

1. On the FortiGate, enable the Security Fabric connection on port3 to allow the FortiExtender to connect over CAPWAP:
   a. Go to *Network* > *Interfaces* and edit port3.
   b. In the *Administrative Access* section, select *PING* and *Security Fabric Connection*.
   c. Click *OK*.

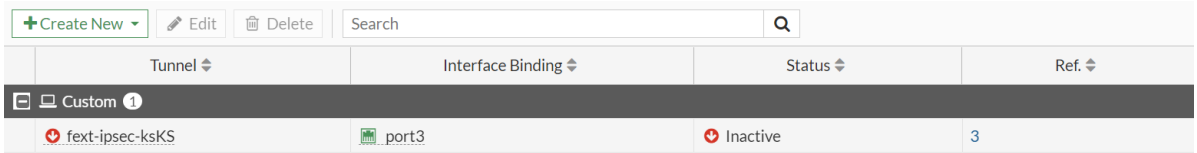
2. On the FortiExtender, connect to the CLI via SSH and set the AC server address to the FortiGate:

```
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
```

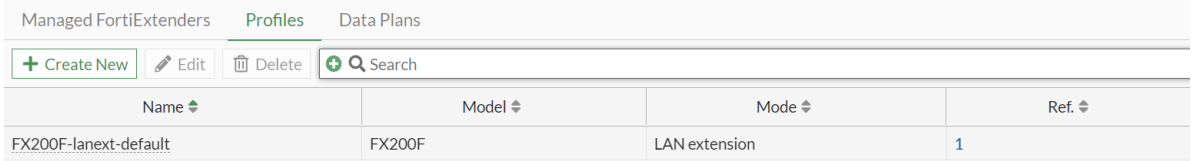
Once the FortiExtender's discovery packet reaches port3 on the FortiGate, the FortiExtender will appear under *Network > FortiExtenders* as unauthorized.



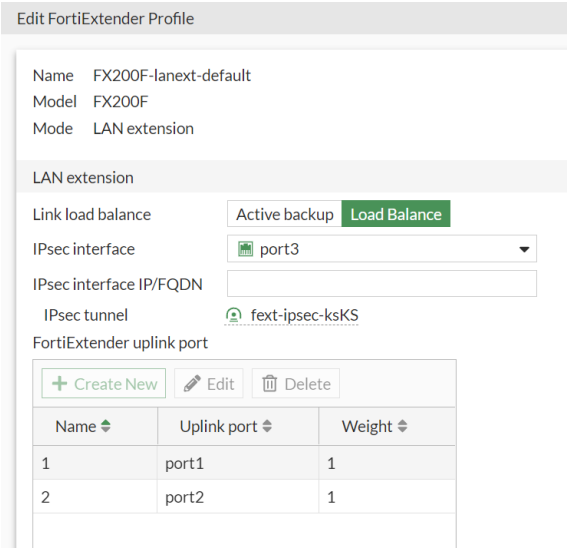
The FortiGate automatically creates a VPN profile for this FortiExtender, which appears on the *VPN > IPsec Tunnels* page.



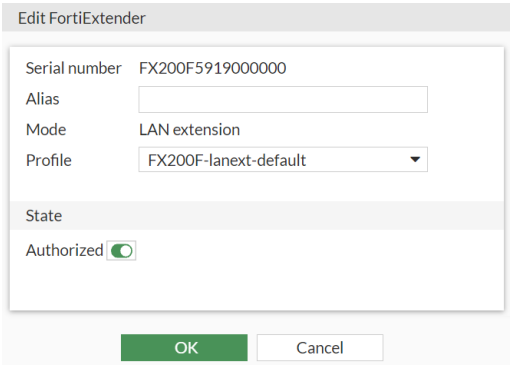
The FortiGate also automatically creates an extender profile for that model of FortiExtender, which appears on the *Network > FortiExtenders > Profiles* tab.



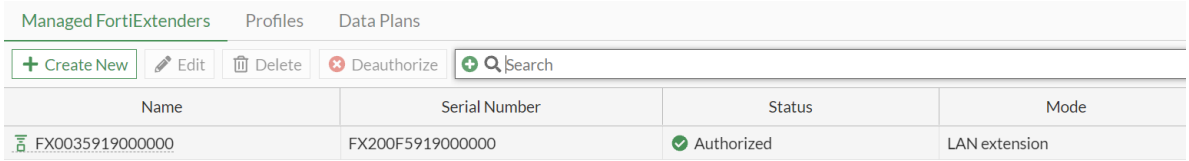
The FortiExtender profile is configured based on the FortiExtender model. It automatically selects *Load Balance* (as the *Link load balance* setting), the IPsec interface, and the pre-configured tunnel.



3. 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*. The device now displays as authorized.



To discover and authorize the FortiExtender - CLI:

1. 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-svxVy5bZbPxZdfoIQBNA7YrkSKBA9Ui1vZsvYcVrgp1Uy0aFMCVZzGzh"
        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
```

6. Authorize the FortiExtender:

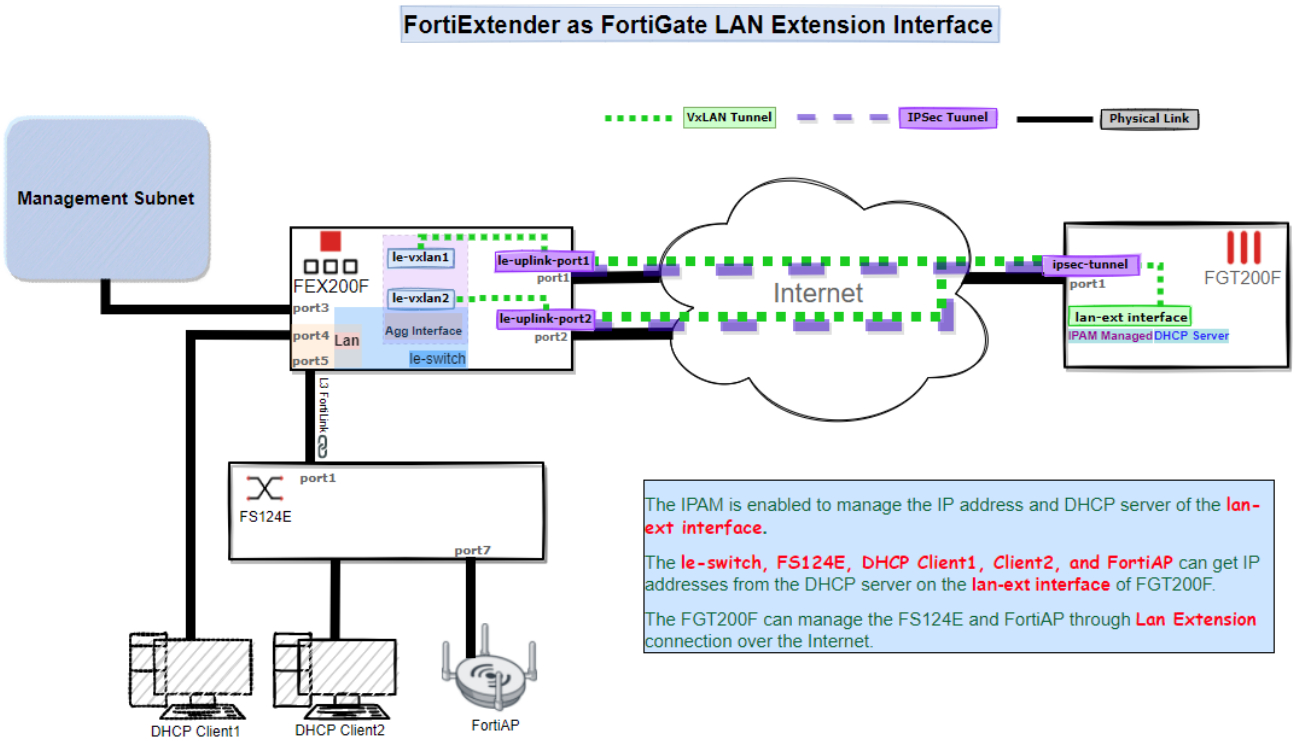
```
config extension-controller extender
    edit "FX0035919000000"
        set authorized enable
    next
end
```

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.



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 3des-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-svxVy5bZbPxZdfoIQBNA7YrkSKBA9Ui1vZsvYcVrgp1Uy0aFMCVZzGzh
        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 3des-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
```

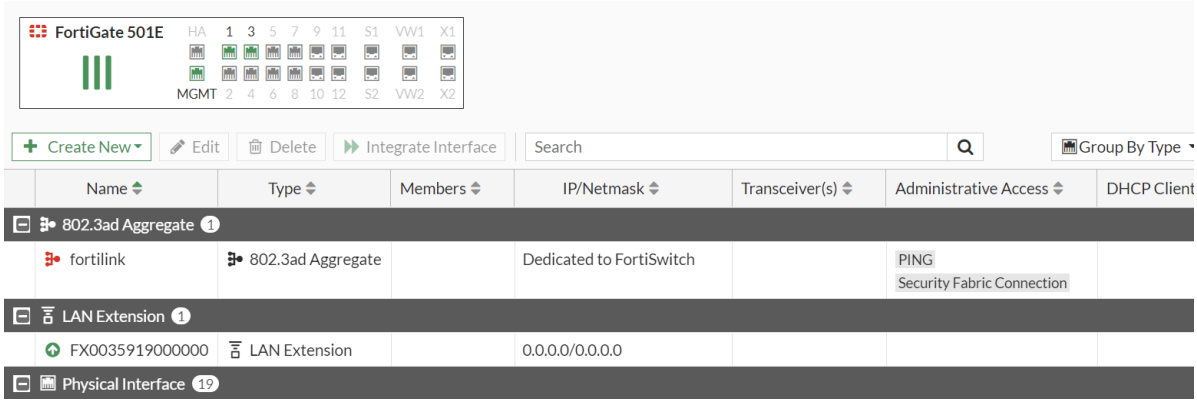
```
    next
end
```

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
        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:

1. Edit the LAN extension interface:
   a. Go to *Network* > *Interfaces* and edit the LAN extension interface.
   b. 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.
   c. Optionally, enable *DHCP Server* to assign IPs to the remote devices using DHCP.
   d. Click *OK*.
2. Configure the firewall policy to allow traffic from the LAN extension interface to the WAN (port1):
   a. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
   b. Enter the following:

Incoming Interface	FX0035919000000
Outgoing Interface	port1

Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable (NAT)

c. 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.

FortiGate-FortiExtender LAN-extension ZTP

For users with a FortiZTP license, you can establish a LAN-Extension (LE) connection between a FortiExtender and a FortiGate using zero-touch provisioning. This process consist of the following steps:

1. Configure the FortiExtender for cloud discovery.
2. Configure the Extender Controller in FortiZTP
3. Provision the FortiExtender in FortiZTP
4. The configuration update is automatically applied to the FortiExtender.
5. The FortiExtender automatically establishes an connection with the FortiGate.

You must meet the following prerequisites in order for FortiZTP to establish a connection:

- The FortiExtender must have internet connectivity (via WAN or LTE).
- The FortiGate must be reachable from the FortiExtender (public IP/address or routable IP).
- The FortiExtender serial number must be registered in FortiZTP.
- The FortiGate must allow FortiExtender authorization.

To configure FortiZTP for a FortiGate-FortiExtender LAN-extension connection:

1. From the FortiExtender CLI, set the `discovery-type` to either `auto` or `cloud`.

```
config system management
  set discovery-type auto
end
```

2. In the FortiZTP portal, configure the FortiExtender External Controller address and add the FortiGate address. For more information, refer to the *FortiZTP Administration Guide*.

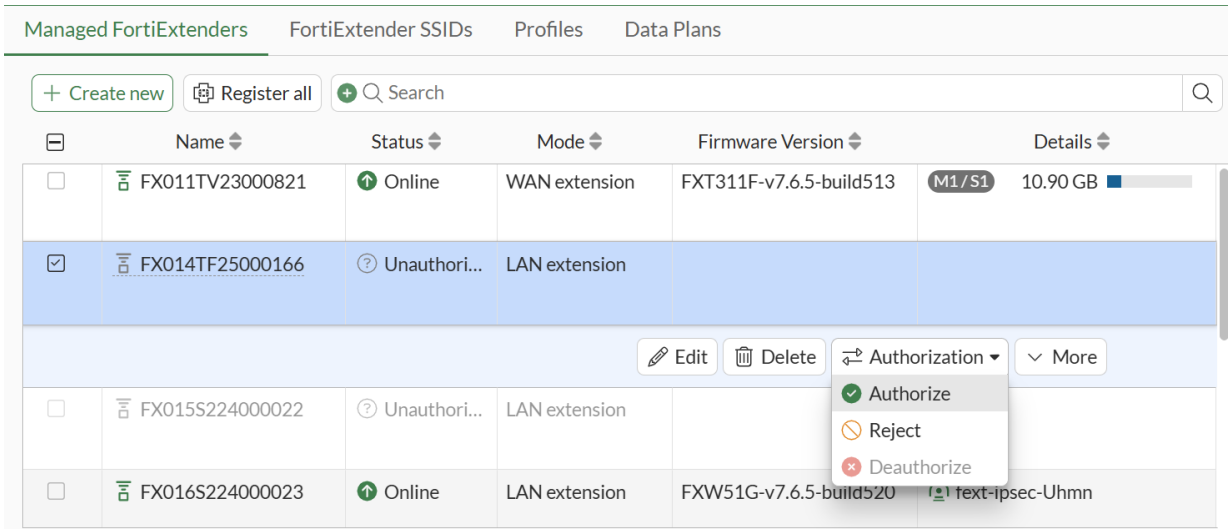
The FortiGate address must match the public or reachable IP address of the target FortiGate as the address will be delivered to the FortiExtender during provisioning.

3. Provision the FortiExtender in the FortiZTP portal.
   a. Go to *Assets* and select the FortiExtender you want to provision and click *Provision*.
   b. In *Target Location*, select the interface used to connect to the FortiGate and then click *Provision*.
   c. FortiZTP begins to provision the target FortiExtender. When provisioning is complete, the *Status* column changes to *Provisioned*.
4. The FortiExtender receives the provisioning configuration from FortiZTP.
   a. During this process, the FortiExtender connects to FortiCloud and downloads the updated configuration. The console displays "`Receive Configuration to connect to FortiGate...`"
   b. Once the configuration is successfully applied, the discovery mode switches to `fortigate`, cloud based discovery is no longer used, and the provisioned IP address and interface settings are assigned.
   c. Example configuration after ZTP:

```
config system management
  set discovery-type fortigate
  config fortigate
      set ac-discovery-type static
      config static-ac-addr
          edit FGT
              set server 166.164.98.51
          next
      end
      set ac-ctl-port 5246
      set ac-data-port 25246
      set discovery-intf lte1
      set ingress-intf
  end
end
```

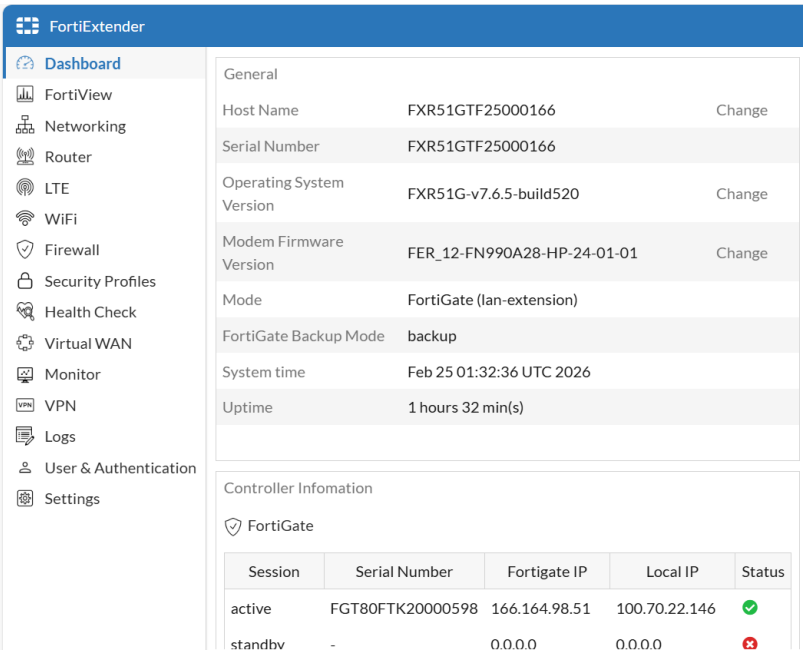
5. After the configuration is successfully applied to the FortiExtender, the FortiExtender begins to connect to the FortiGate and automatically performs the following actions:
   a. The FortiExtender initiates control channel communication with the FortiGate.
   b. The FortiGate detects a new FortiExtender device.

      If required, the FortiGate administrator may need to authorize the device.



c. Once authorized, the state changes to `CWWS_RUN`.

The LAN-Extension tunnel is established and the FortiExtender LE interface receives a valid IP address from the FortiGate (if configured).



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.

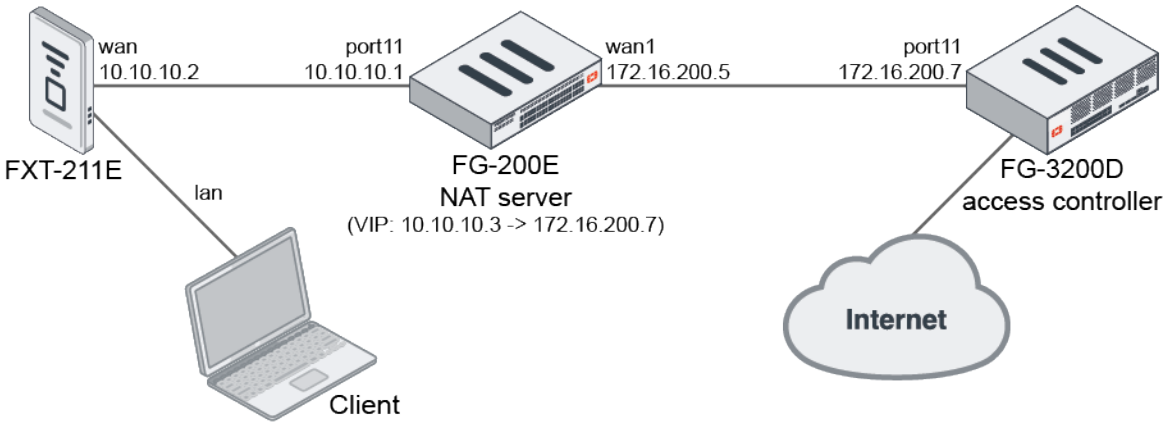
When the default IKE port 500 is inaccessible, you can configure a custom IKE port on the FortiExtender and the FortiGate.

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

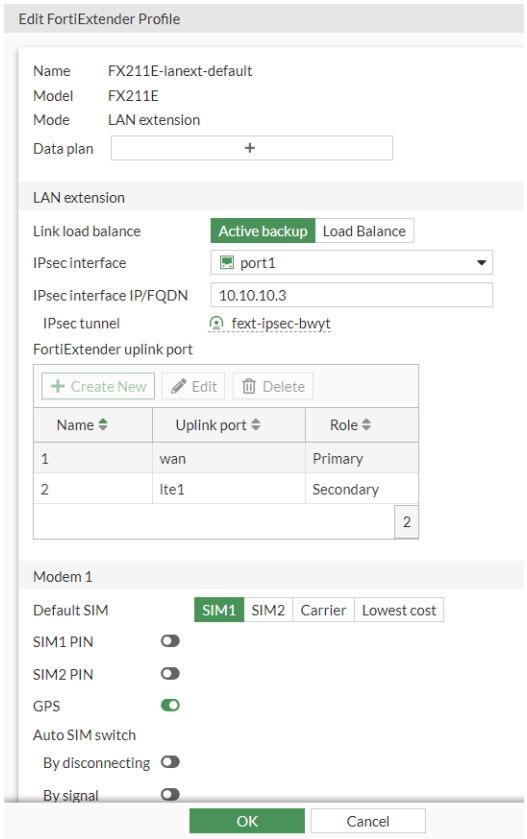
The following topology is used for the first three examples and assumes that the FortiExtender has already been discovered (see FortiExtender as FortiGate LAN extension on page 34 for more information).



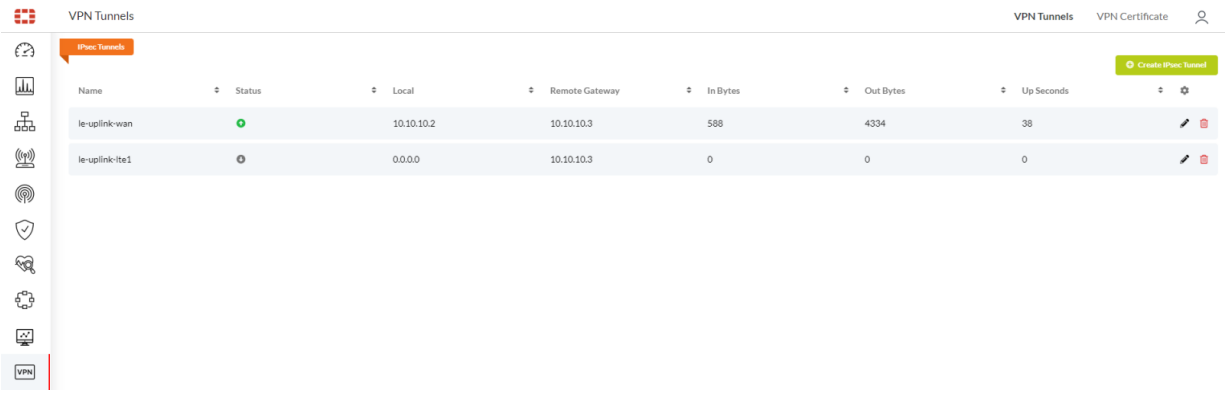
Configuring an IP as a backhaul address in the FortiGate extender profile

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*.



   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*.



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 lte1
                    set role secondary
                next
            end
        end
    next
end
```

2. Verify the configuration in FortiExtender:

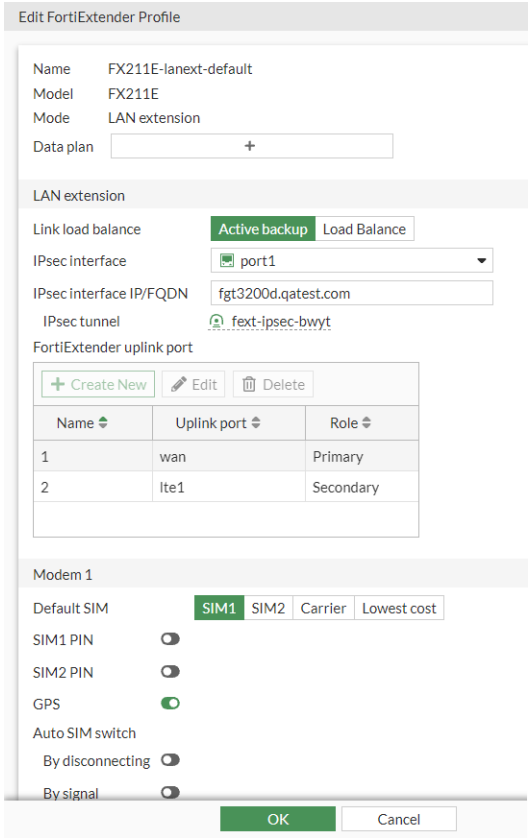
```
config vpn ipsec phase1-interface
    edit le-uplink-wan
        set ike-version 2
        set keylife 86400
```

```
        set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 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-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZkO9t
        set add-gw-route enable
        set dev-id-notification disable
    next
end
```

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

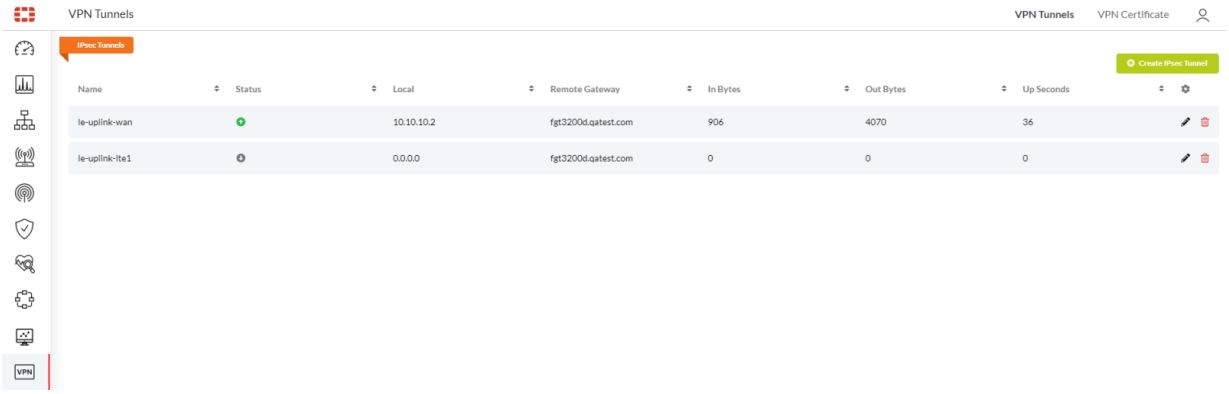
To configure an FQDN as a backhaul address in the GUI:

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*.



   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*.



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 3des-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
```

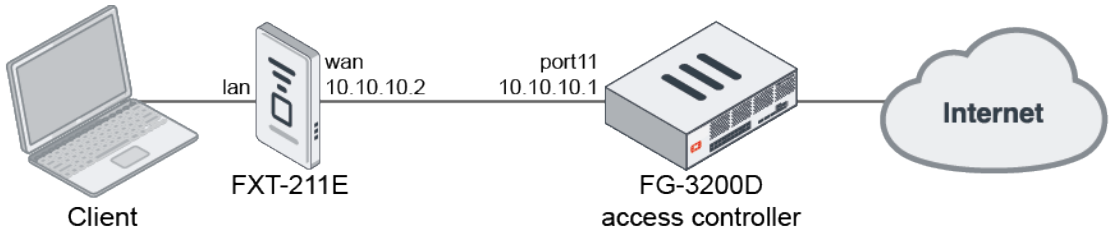
6. Verify the IPsec tunnel status on the FortiExtender to confirm that Port 4500 is used:

```
~ # 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 (0x00000005),   1512 bytes,    18 packets,     2s ago
    out 7d17257c (0x00000005),   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-aRuaScJBVVJ1DWKrrKcY8VcHF8Vg6cgLQkpEtdzDRpRTVvapxdeeJoiO' @ 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
```

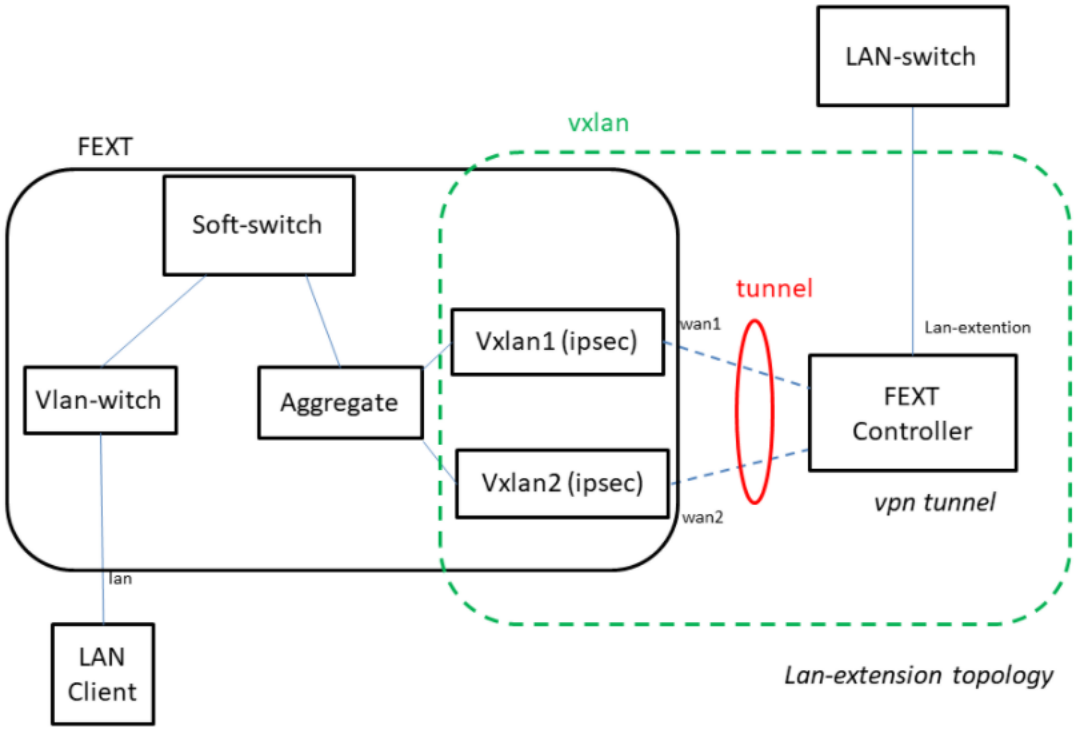
If bandwidth enforcement is disabled on the FortiGate, the configuration that was pushed to the FortiExtender will be removed.

IPAM in FortiExtender LAN extension mode

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

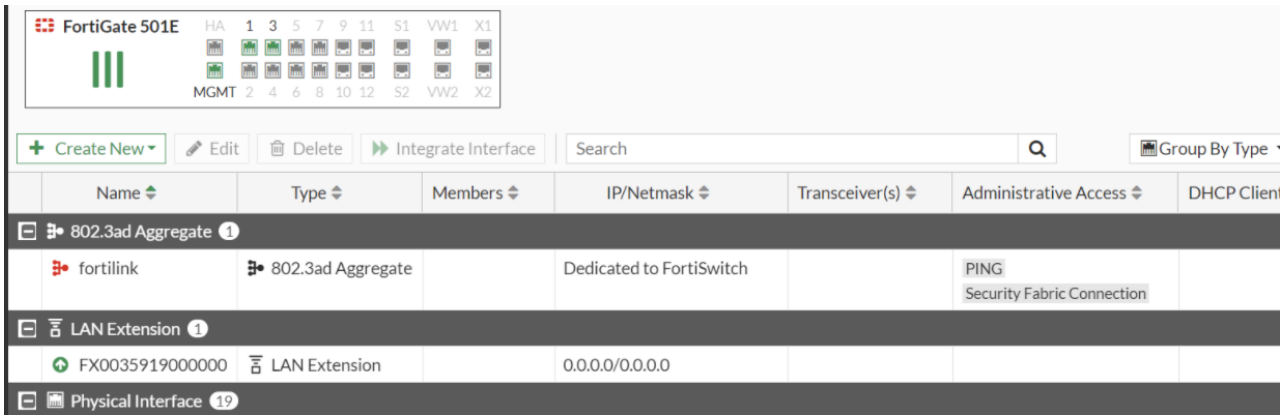
The LAN client connecting to the FortiExtender LAN interface will get DHCP allocation from the LAN extension interface. It can then reach the Internet via the firewall policy in the FortiExtender controller.

Topology

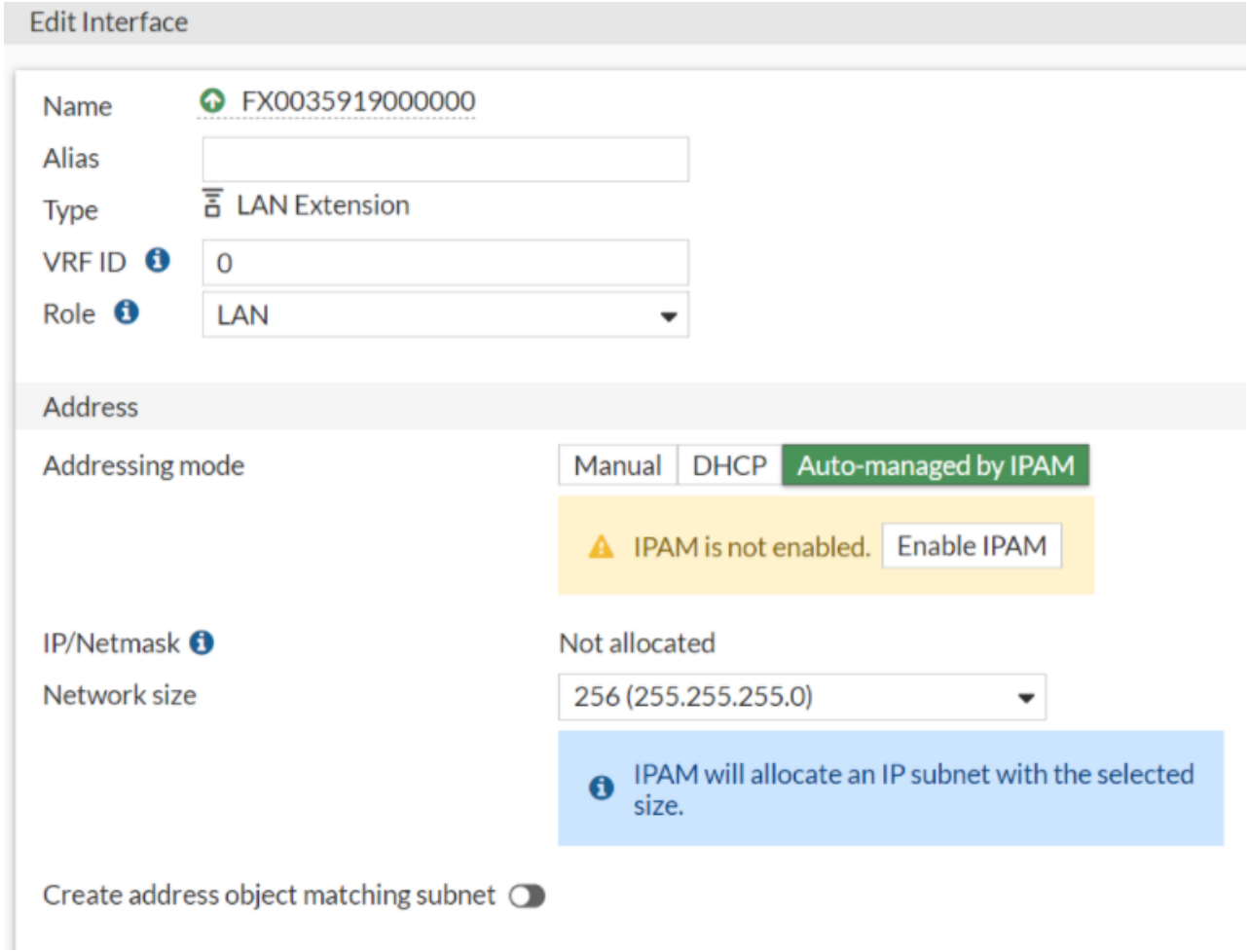


To configure IPAM in the FortiExtender LAN extension interface in the GUI:

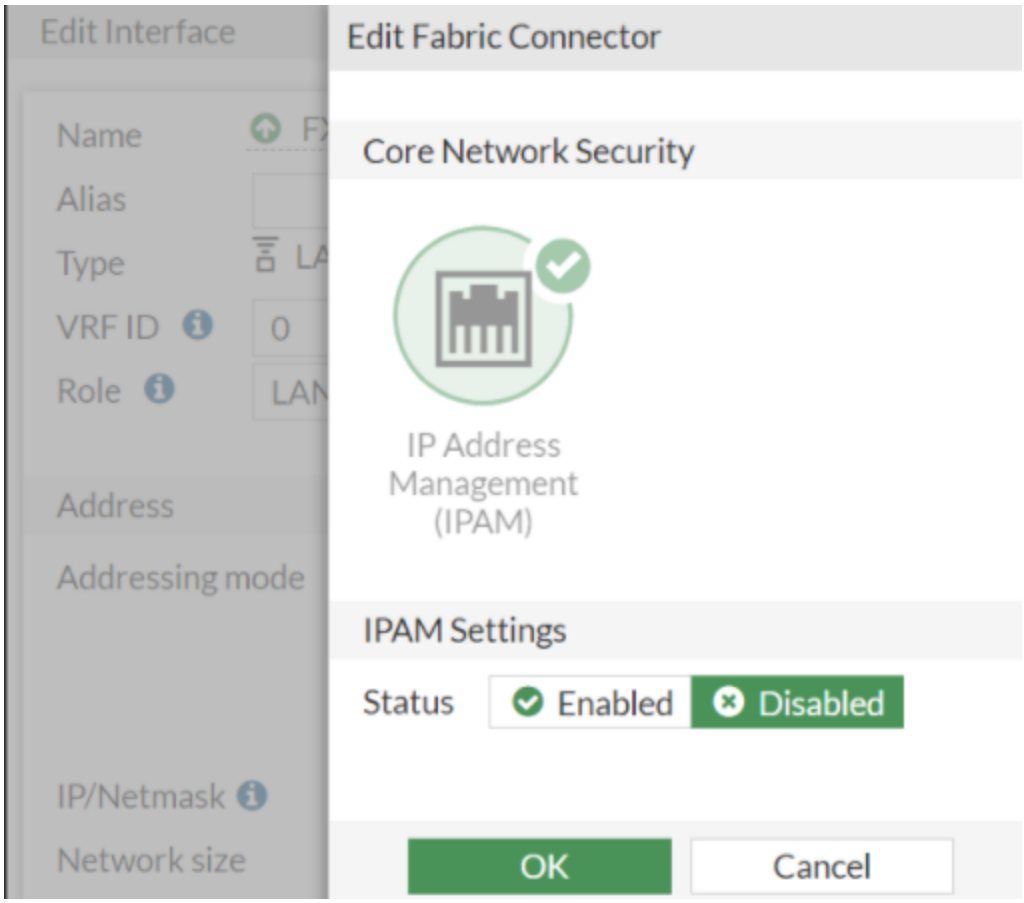
1. On the FortiGate device, go to *Interfaces*. You will see that the LAN extension interface has already been created in the FortiExtender controller.



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*.

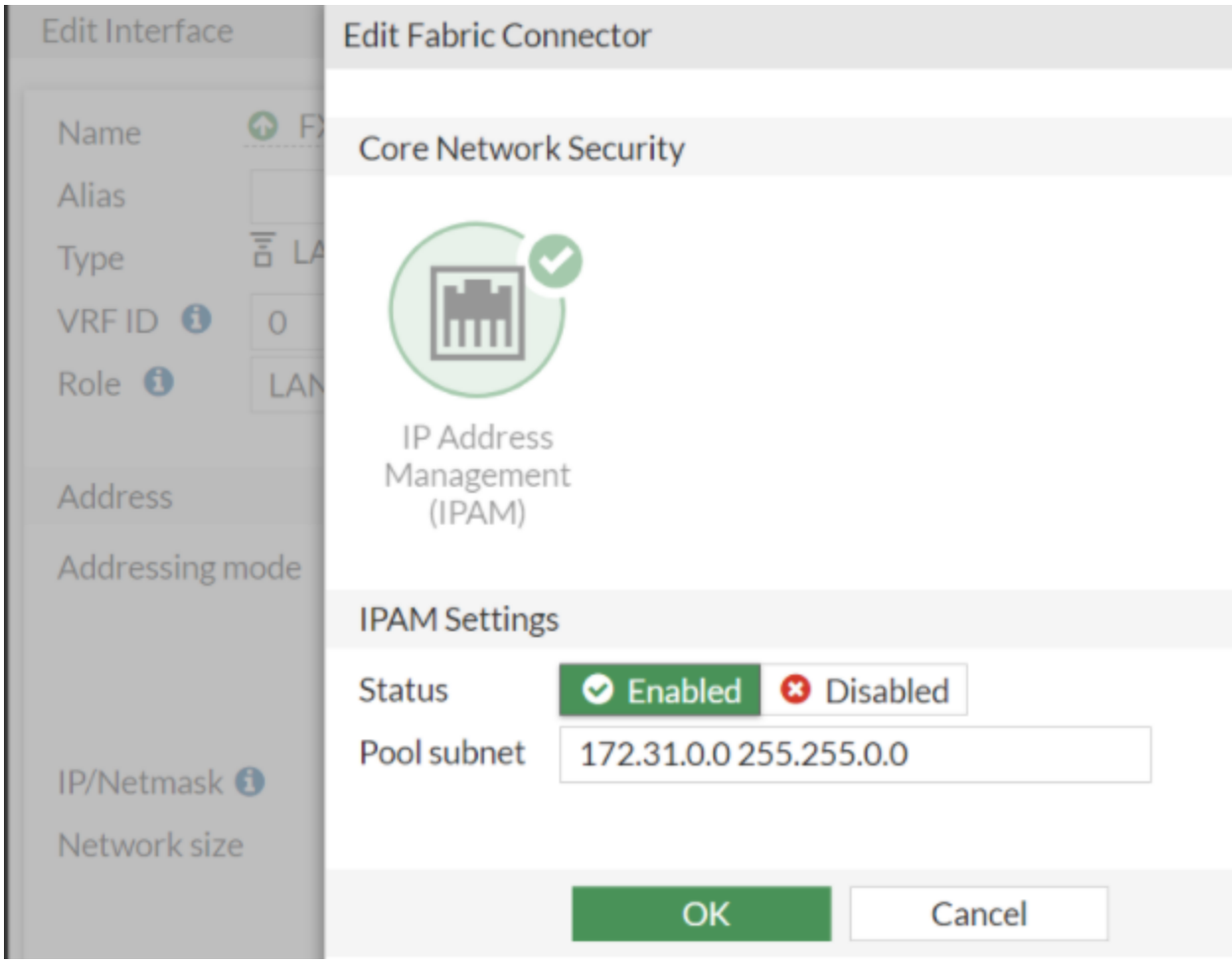


4. For *IPAM Settings* > *Status*, select *Enable* and then *OK*. The IP pool now is selected for FX0035919000000.

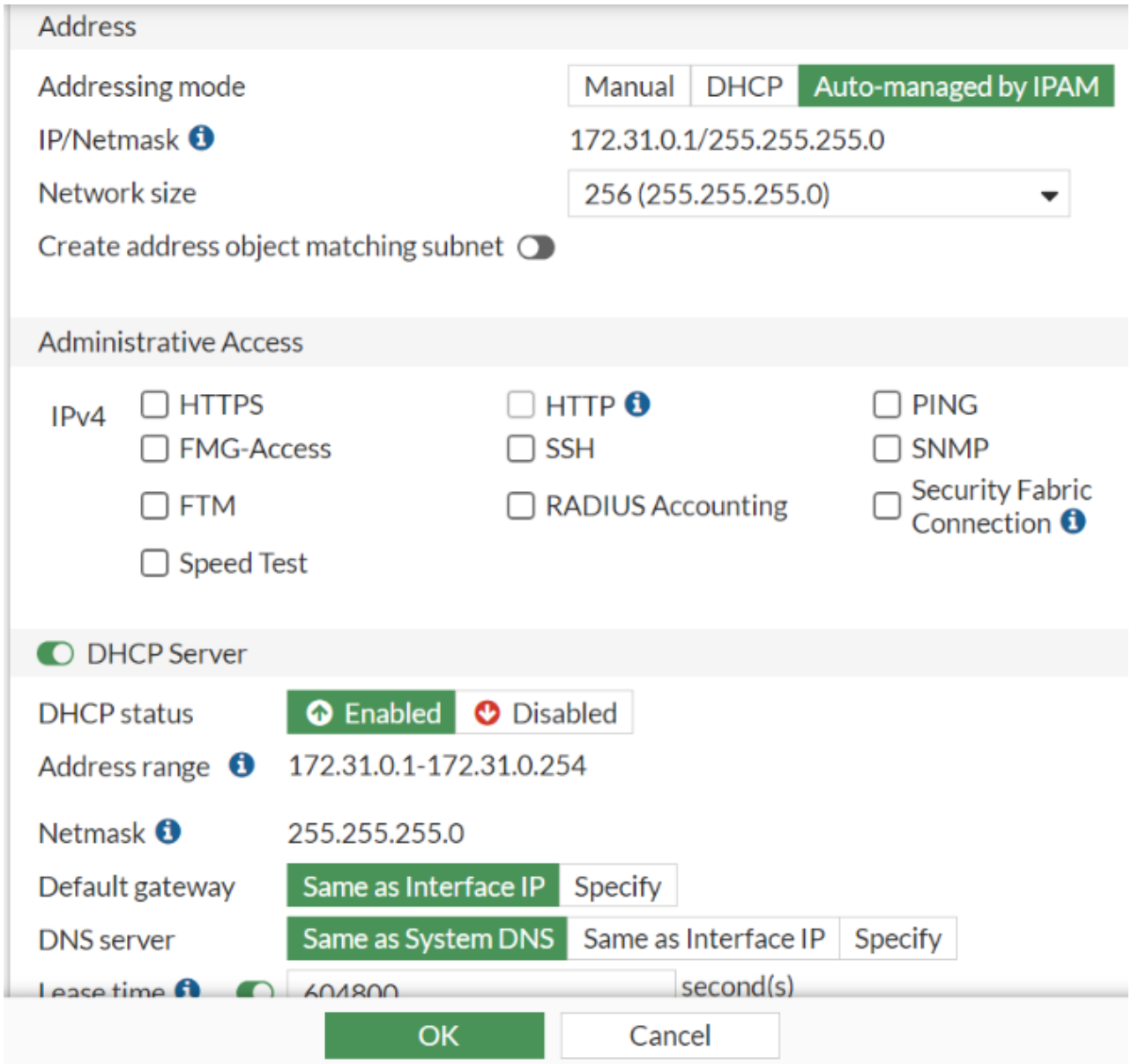


The subnet configured above is for a standalone device.

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

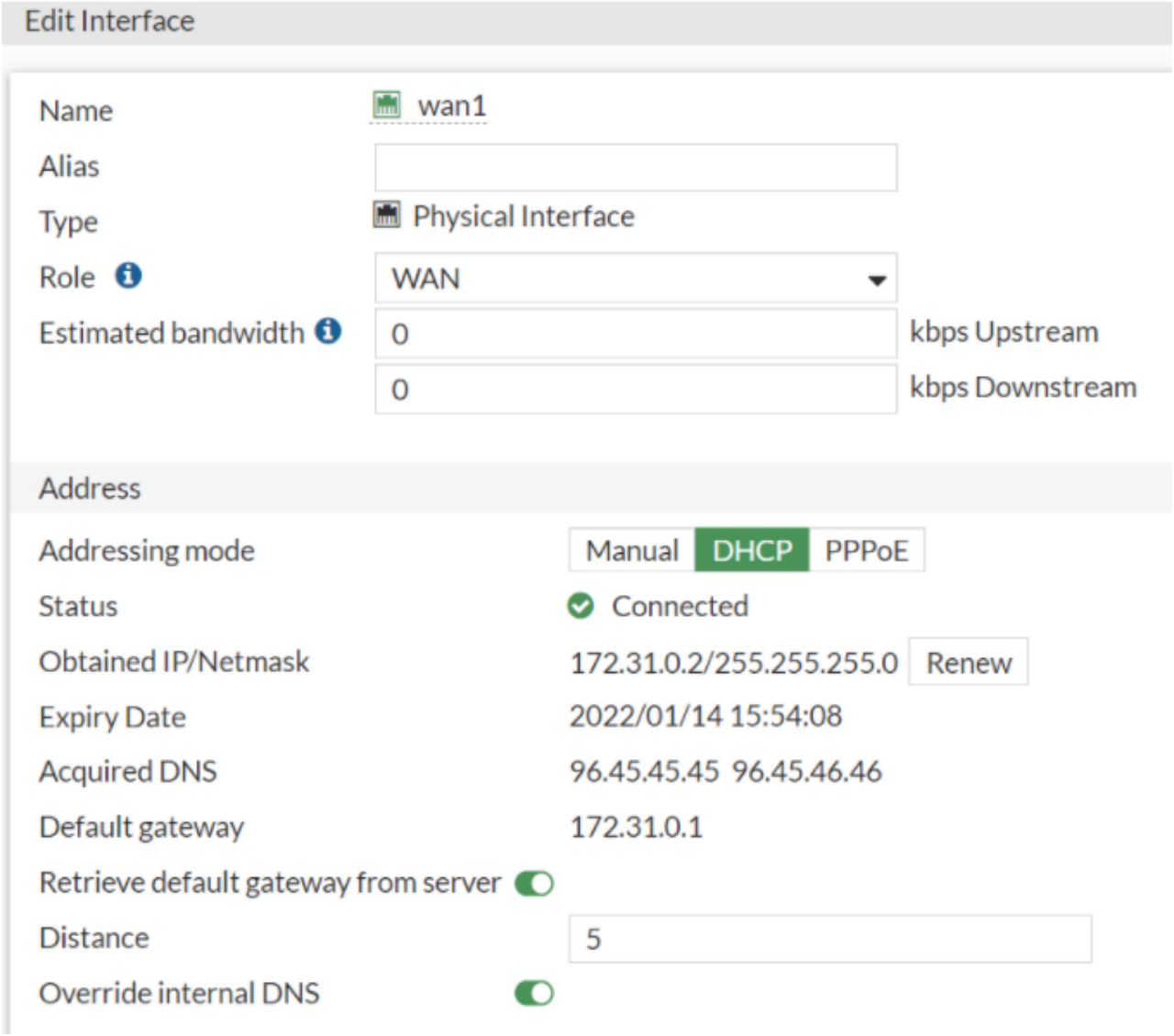


The IP and DHCP server on FX0035919000000 will be set accordingly.



The client will get DHCP allocation from FX0035919000000.

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



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
```

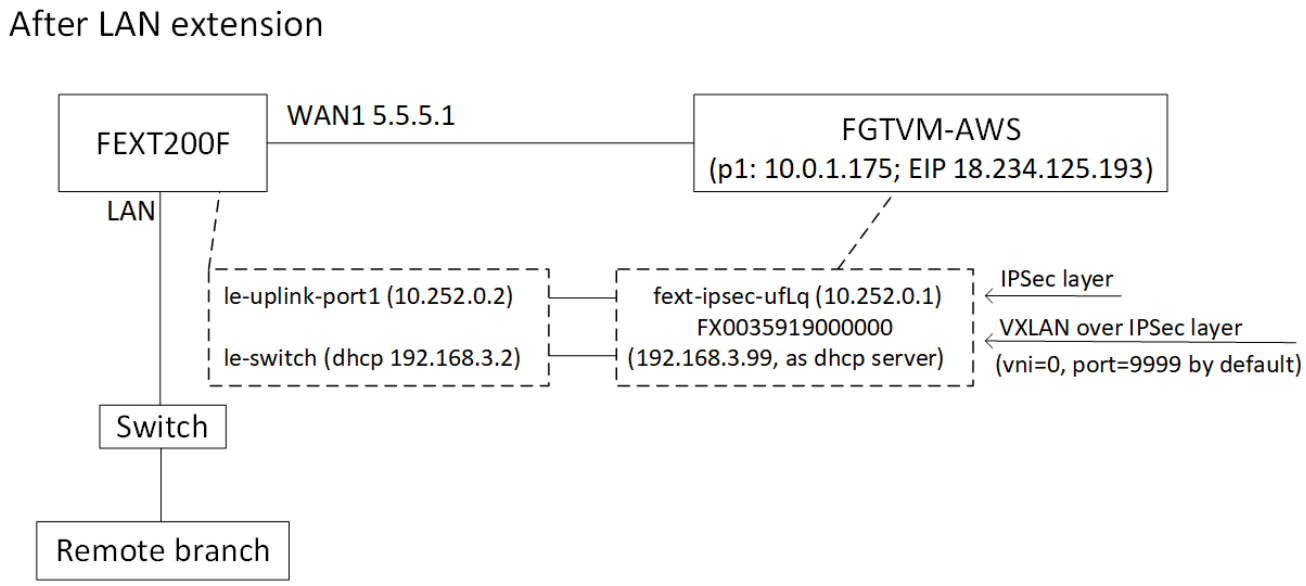
After IPAM is set as the addressing mode for FX0035919000000 in the GUI, the following steps are created in the CLI:

```
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 FortiGate-VM

The FortiExtender LAN extension feature allows a FortiGate to extend its LAN functionality to a remote FortiExtender. This enables FortiExtender LAN extension to be added to the FortiGate-VM running on Public Clouds.

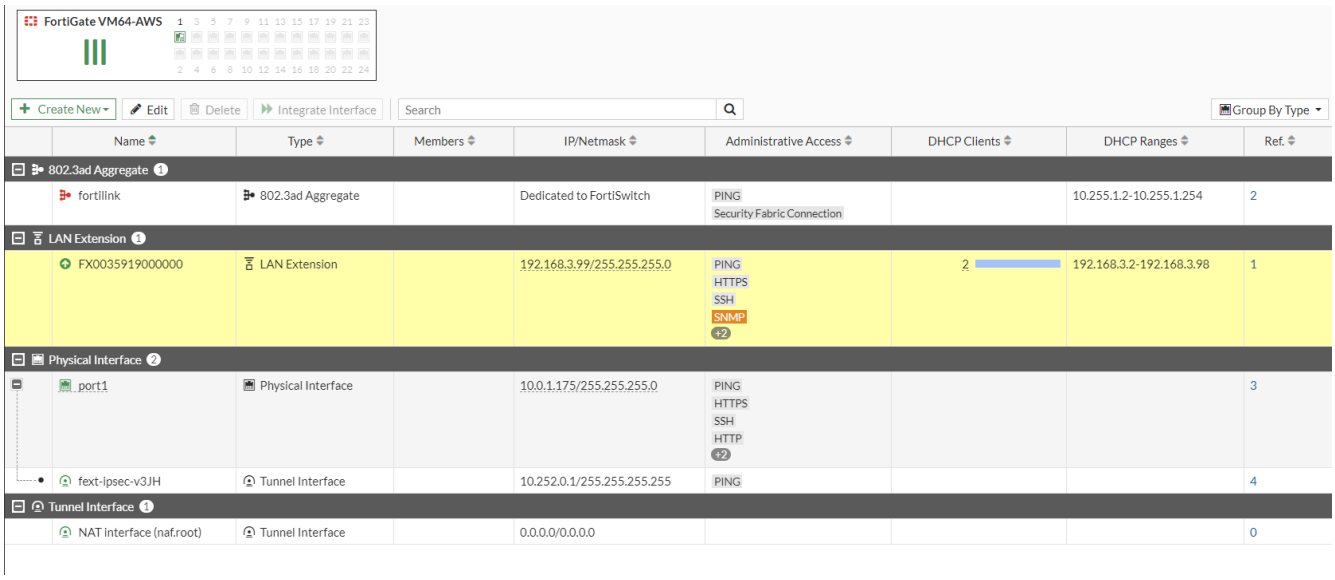
FortiExtender LAN configuration in FortiGate-VM topology:



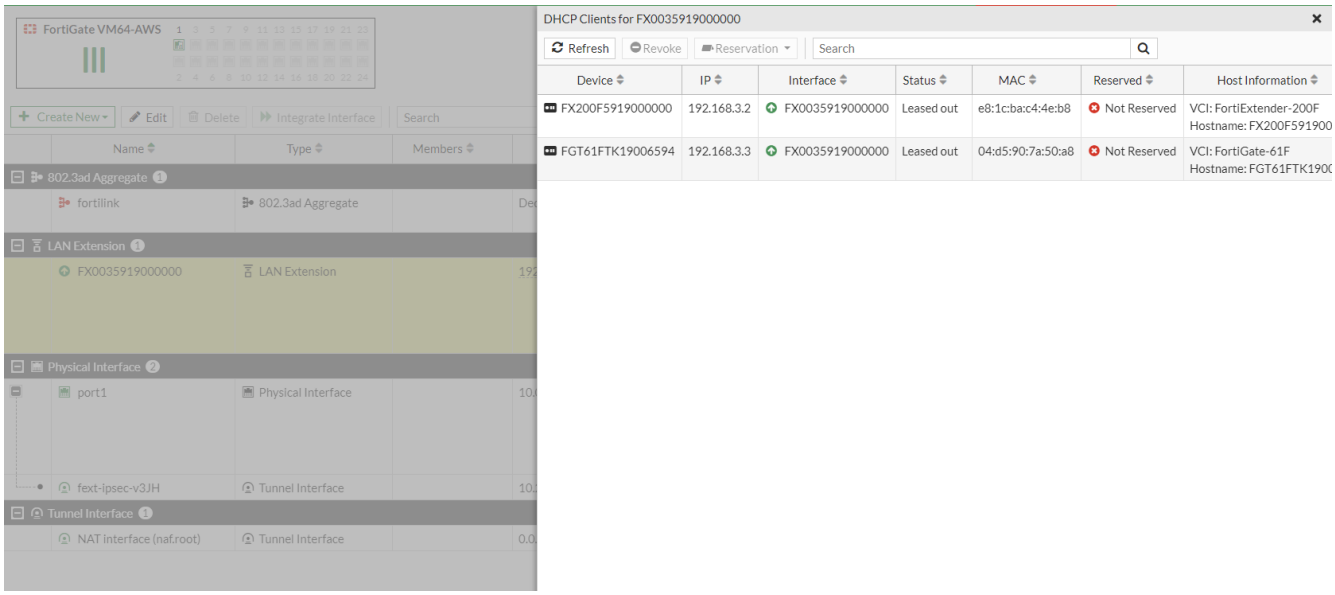
Clients get IPs from the DHCP server. In this example, the FGT-61F WAN1 DHCP interface gets IP 192.168.3.3 from the FortiGate-AWS LAN extension interface.

In this example, the FEXT-200F LAN interface includes port4 and port5, which are members of the le-switch. After the FortiExtender and FortiGate-VM connect successfully, the FortiGate-VM is able to extend LAN to the remote branch on the FortiExtender LAN interface via VXLAN.

From the FortiGate-AWS, you can view the LAN extension interface.



The FortiGate-AWS LAN extension interface is able to act as a DHCP server over VXLAN, and remote branch computers behind the FortiExtender are able to get IP addresses from the DHCP server on the FortiGate-AWS LAN extension interface.



To configure a FortiExtender LAN extension to a FortiGate-VM - CLI:

1. Configure the FortiExtender:

```
FX200F5919000000 # config system interface
  edit port1
    set mode static
    set ip 5.5.5.1/24
    set gateway 5.5.5.99
  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

config system management
  set discovery-type fortigate

config fortigate
  set ac-discovery-type static
  config static-ac-addr
    edit 1
      set server 18.234.125.193
    next
  end
  set discovery-intf port1
  end
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
```

2. Configure the FortiGate-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
```

3. The FortiGate-AWS and the FortiExtender 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-
760sv1bSXj2wrUASE1uwcryLKi1XEUlmh1v1FehZ2u97lqHDPUkCjFh"
                    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/TBq6dXlzeXymkw8cyoizM2a8SeyWao2sGnLCkqqkHItruVfy7jy10dMp6A
zaFlnxP6f9k8hTEBKxqUOS3+ccvSLFWvM7ouuaWgA6Hdu4StWsBVMc85tBFe+H6PTnVpRFaRCYQE0yatuM9tcWQXCilsuv
66HlAYvGlw==
                    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
```

4. Ensure that VXLAN over IPSec is set up automatically between the FortiGate 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
```

5. Set the IP address for the FortiGate-AWS LAN extension interface, and ensure that the FortiGate-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
```

The FortiExtender le-switch interface is able to get an IP (192.168.3.2) from the FortiGate-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
```

The remote branch PC behind the FortiExtender LAN interface is able to get the IP from the FortiGate-AWS VXLAN interface DHCP server.

In this example, a FGT61F acts as a PC behind the FortiExtender. This FGT61 WAN1 interface is the same switch as the FortiExtender LAN interface port4.

Set the FGT61 WAN1 interface as the DHCP client so it can get an IP address (for example, 192.168.3.3) from the FortiGate-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
```

6. Ensure that the FortiGate-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
```

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
```

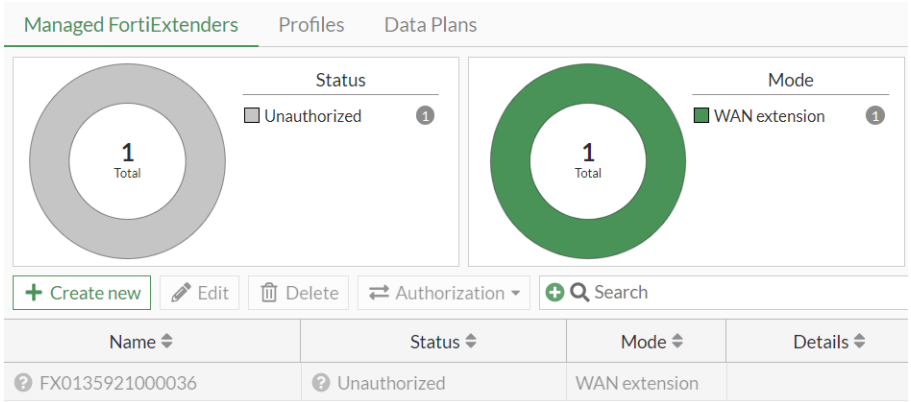
```
            set stp enable
            set role lan
            set snmp-index 21
         next
      end
```

De-authorize FortiExtender devices

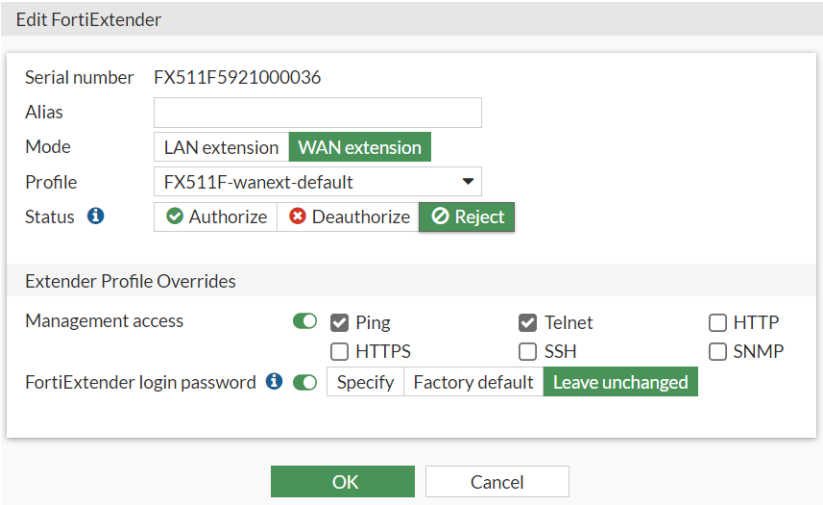
From the FortiOS GUI, you can de-authorize a discovered FortiExtender device on a FortiGate configured as a FortiExtender controller from the GUI or the CLI.

To de-authorize a FortiExtender - GUI:

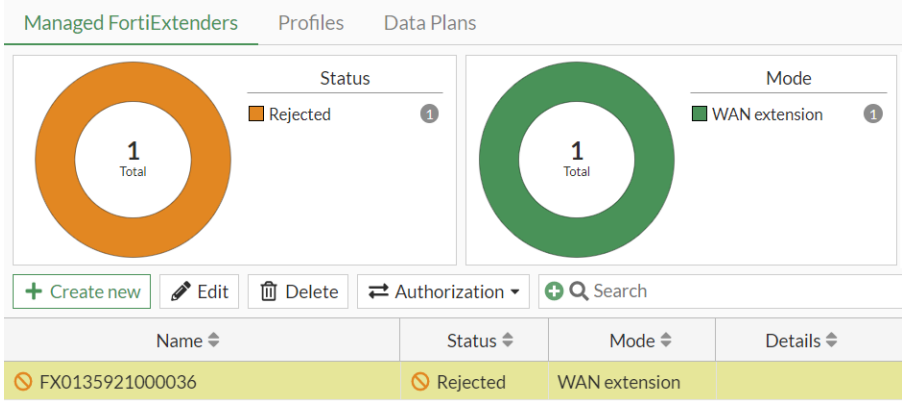
1. Go to *Network* > *FortiExtenders* and locate the FortiExtender you want to de-authorize.



2. Select the FortiExtender and then click *Edit*.
   Set the *Status* to *Reject*, and click *OK*.



The FortiExtender status changes to *Rejected* on the Dashboard.



To de-authorize a FortiExtender - CLI:

Set `authorized` to `disable`.

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

LAN extension profile configuration

FortiGate automatically generates default profile based on the FortiExtender model.

- For FortiExtender models without LTE/5G modems, FortiGate will generate a single LAN extension profile. In that default profile, there are two default backhaul ports: port1 and port2. The FortiExtender uses 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.
- For FortiExtender models with LTE/5G modems, two default profiles will be generated: one for WAN extension and the other for LAN extension.

The following configuration options are available in a LAN extension profile:

```
config extension-controller extender-profile
  edit "FX200F-lanext-default"
    set id 4
    set model FX200F
    set authorized enable
    set extension lan-extension
    set override-enforce-bandwidth
    set enforce-bandwidth enable
    set bandwidth-limit 1000
    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
```

Parameter	Description
`id`	The profile ID (for system internal record)
`model`	The FortiExtender model for the profile
`extension`	The extension type for the profile
`alloweaccess`	Control the types of traffic that the FortiExtender uplink interface is allowed to send to the FortiGate.

Parameter	Description
	• Ping • Telnet • HTTP • HTTPS • SSH • SNMP
`set override-login-password-change`	Enable/Disable overriding the administrator login password setting in the profile.
`login-password-change`	Set the admin password of the FortiExtender. • `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 login-password <string>`	Set the administrator login password of the managed FortiExtender.
`enforce-bandwidth`	Enable/Disable the enforcement of bandwidth limit on the LAN extension interface. **Note:** `"enforce-bandwidth"`, which is disabled by default, is used to limit the egress bandwidth used to send traffic from the FortiExtender.

`bandwidth-limit`	Set the FortiExtender LAN extension interface bandwidth limit in Mbps. The range is from 1 to 16776000.
	Once configured, the FortiExtender will have a firewall `"shaper"` configuration that can also be configured with a bandwidth limit.
	`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`
	`le-traffic-shaper` and `le-shaping-policy` are predefined, and will be created in the FortiExtender.

config lan-extension	
`link-loadbalance`	Two ports are configured for the FortiExtender for load-balancing. • For `activebackup` mode, you can configure `"role"` (primary or

Parameter	Description
	secondary) on the two backhaul ports. • For `loadbalance` mode, you can configure `"weight"` 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 `"backhaul-ip"` is the external IP of the NAT device. For details, see Backhaul IP in LAN extension on page 83.

Backhaul configuration

```
config lan-extension
  set link-loadbalance activebackup
  set ipsec-tunnel "fext-ipsec-VRSq"
  set backhaul-interface "wan1"
  set backhaul-ip ''
  config backhaul
    edit "1"
      set port lte1
      set role secondary
      set health-check-interval 5
      set health-check-probe-cnt 1
      set health-check-probe-tm 2
      set health-check-fail-cnt 5
      set health-check-recovery-cnt 5
    next
  end
end
```

Parameter	Description
`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 `loadbalance`.
`role`	Specify whether the port is primary or secondary.
`health-check-interval`	Health monitoring interval in seconds (1 - 3600, default = 5).

Parameter	Description
`health-check-probe-cnt`	Number of health monitoring probes to send within an interval (1 - 10, default = 1).
`health-check-probe-tm`	Health monitoring probe timeout in seconds (1 - 10, default = 2).
`health-check-fail-cnt`	Number of failures before the link is considered dead (1 - 10, default = 5).
`health-check-recovery-cnt`	Number of successful checks before the link is considered alive (1 - 10, default = 5).

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
            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-extenson" interface and can forward traffic out through the FortiGate based on the firewall policy.

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:

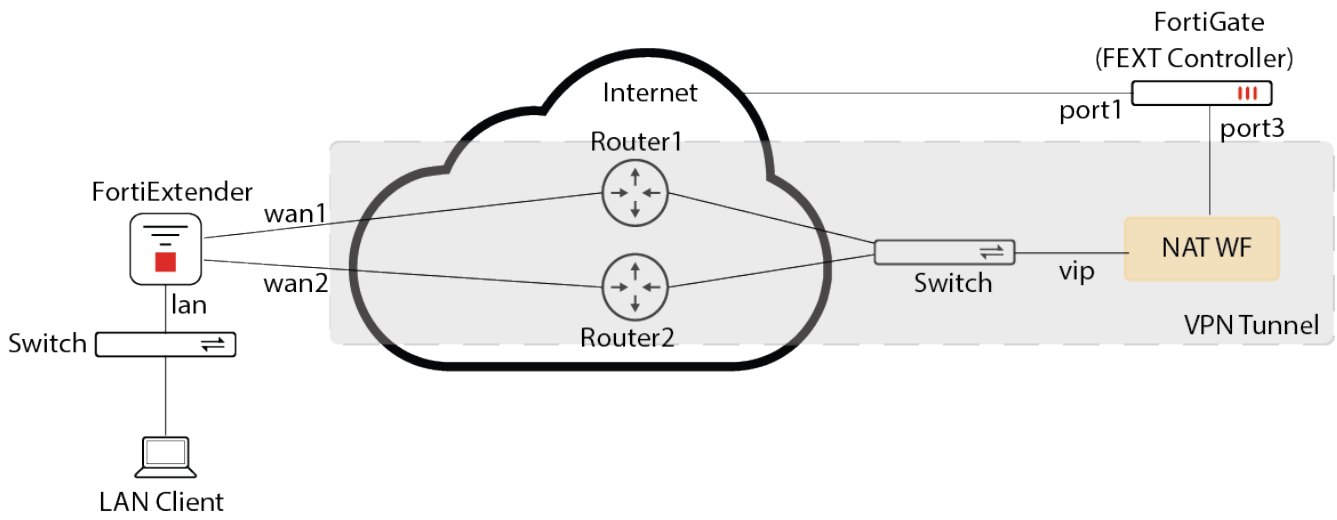
1. Execute the CLI command `get extender session-info`.
   In the CLI output, the active session is marked as `lan-extension` and the standby session is marked as `secondary`.

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:
FX0030000000000 : 3.3.3.1:60440 (dport 65535) seconadry,  running,  install,      data-
enable, refcnt 5, miss_echos -1, up-time 363 secs, change 1
FX0030000000000 : 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):

FX200F0000000000 # get extender status
Extender Status
    name                 : FX200F0000000000
    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:
FX0030000000000 : 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:
FX0030000000000 : 3.3.3.1:5246 (dport 65535) seconadry,  running,  install,      data-
enable, refcnt 5, miss_echos -1, up-time 201 secs, change 1
FX0030000000000 : 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):

FX200F0000000000 # get extender status
Extender Status
    name                 : FX200F0000000000
    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
FX200F0000000000 #
```

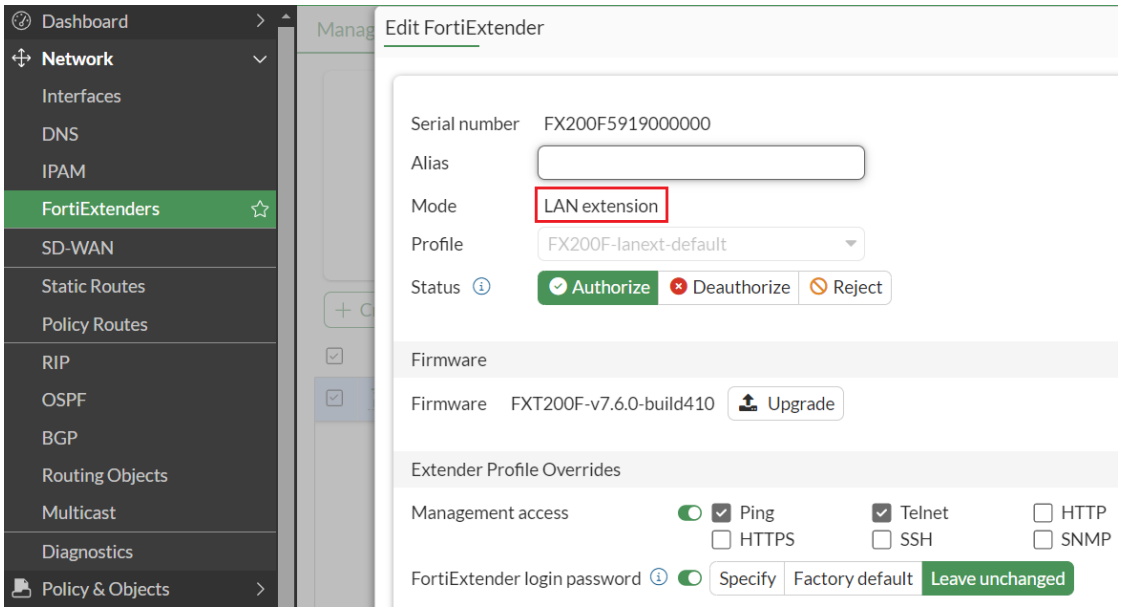
VLAN support for LAN extension mode

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.

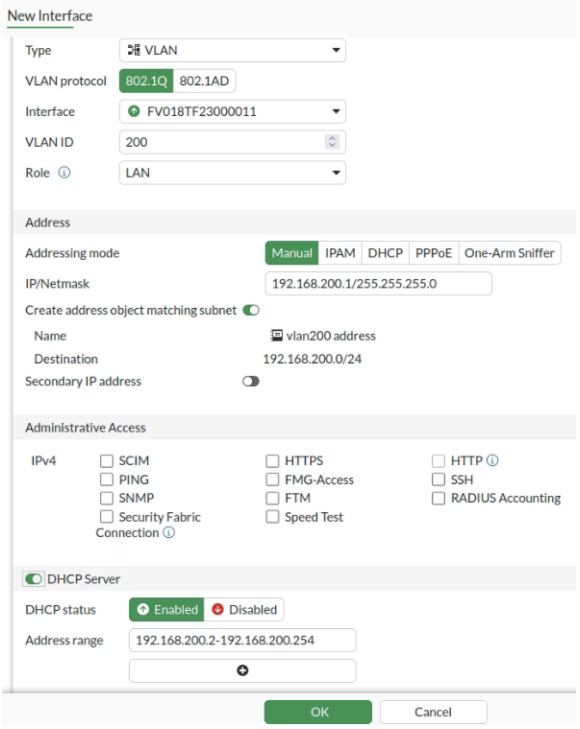
When configuring from the CLI, you can also configure the VLAN ID list (VIDs) to create tagged traffic out of FortiExtender ports.

To configure VLAN support - GUI:

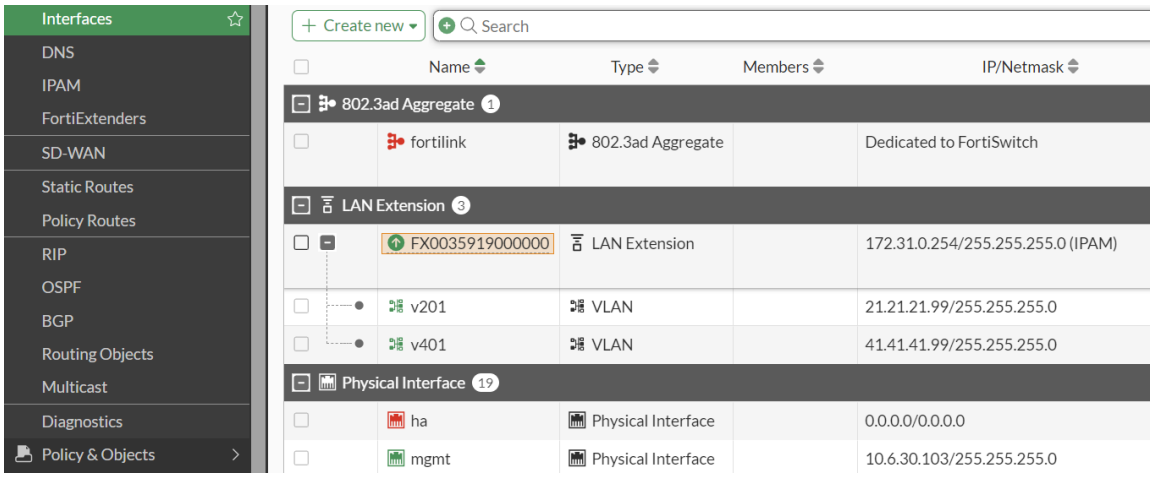
1. From the FortiGate, go to *Network* > *FortiExtenders* and configure the FortiExtender to run in LAN extension mode.



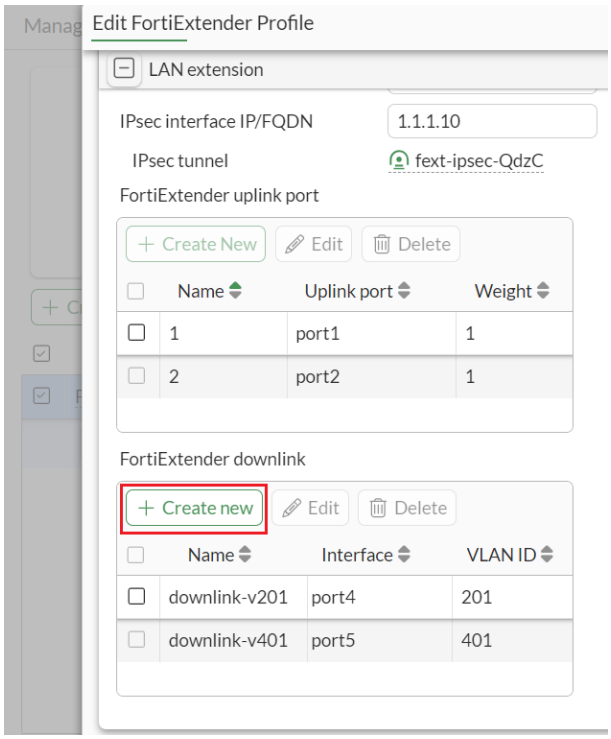
2. Go to *Network* > *Interfaces* and add VLAN interfaces to the LAN extension interface.
   a. Click *Create new* and configure the following:
      - In *Interface*, select the FortiExtender LAN extension interface you created.
      - In *VLAN ID* (pvid) enter the corresponding value.
      - Enter 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.



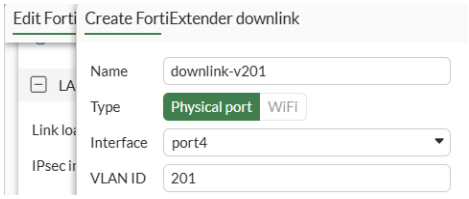
3. When you are finished, click *OK* to save.



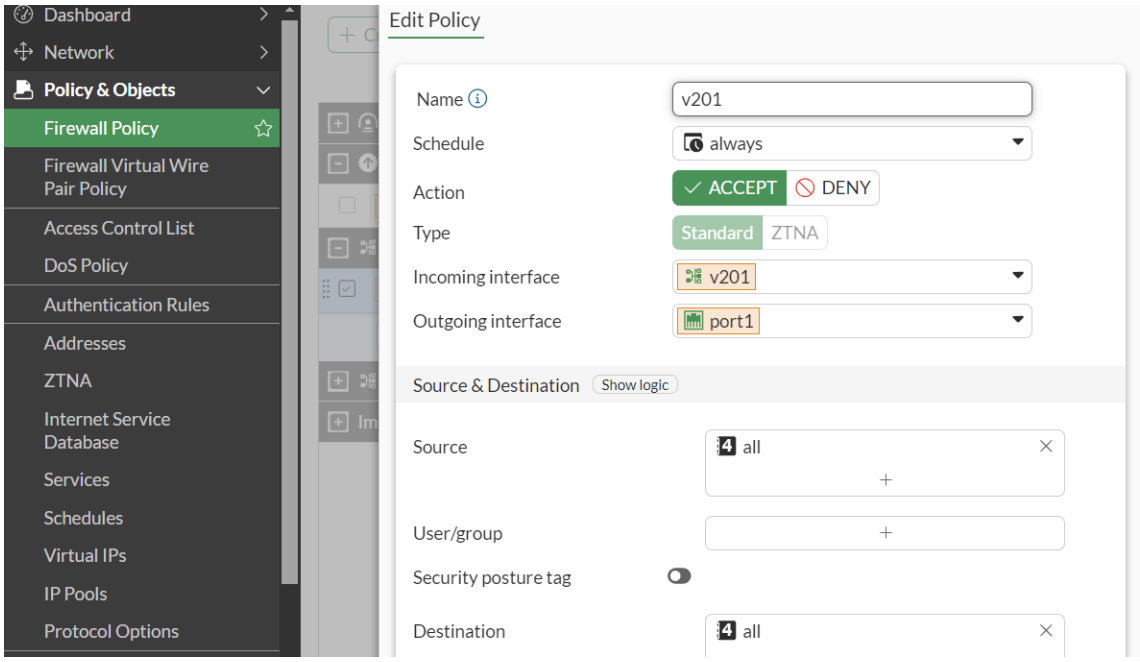
4. Go to *Network* > *FortiExtenders* and edit the FortiExtender *Profile*.
5. Under *LAN extension* > *FortiExtender downlink*, click *Create new* to create a new downlink.

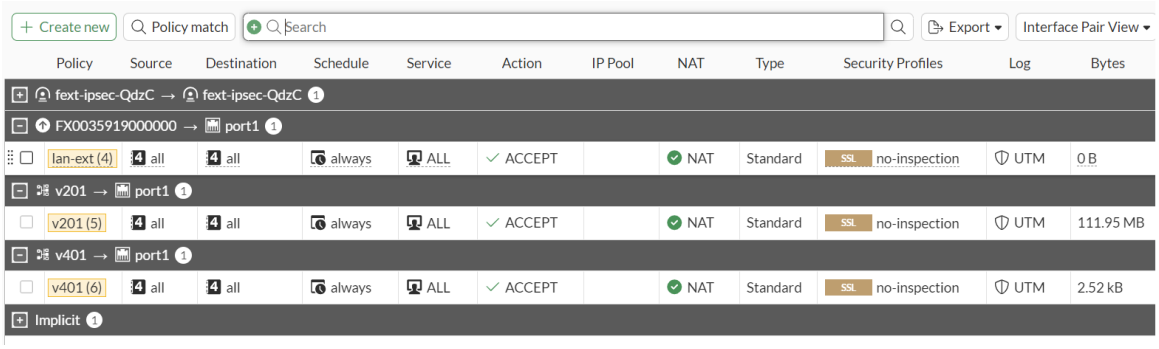


6. Select the *Interface* and enter the *VLAN ID* you want to bind to the FortiExtender LAN switch port.

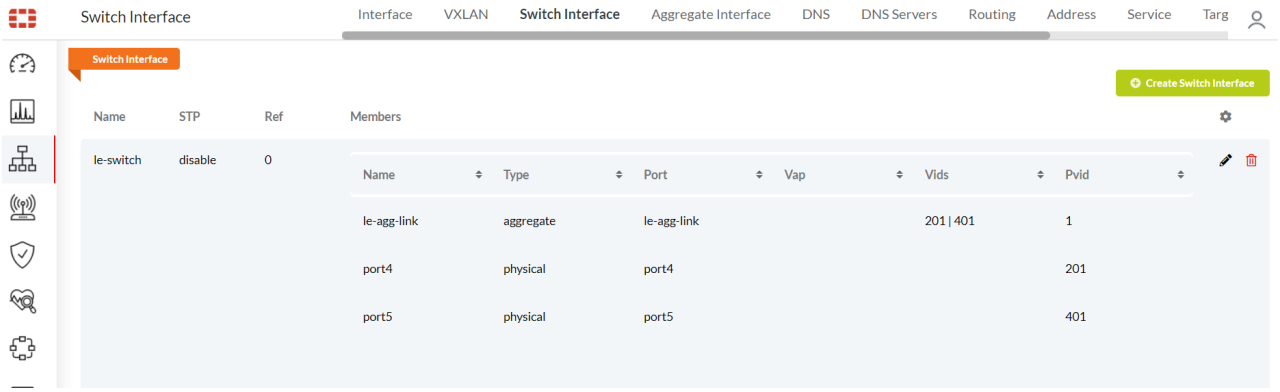


7. When you are finished, click *OK*.
8. In the FortiGate Access Controller, go to *Policy & Objects* > *Firewall Policy* and create a firewall policy for each VLAN interface designated as a downlink.





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.

```
config extension-controller extender-profile
  edit "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 lte1
          set role secondary
        next
      end
    end
      config downlinks
        edit "1"
          set type port
          set port port2
          set pvid 200
          set vids 10 20 30
        next
      end
    next
  next
end
```

Parameters	Description
`config downlinks`	
`type`	Select the FortiExtender LAN extension downlink type • `port`: port • `vap`: Wi-F VAP (requires at least one available LAN extension SSID)
`port`	This option is only available if `type` is set to `port`. Select the FortiExtender LAN extension downlink port (`port` is the VLAN interface added to the FortiExtender interface). The available downlink ports depend on the FortiExtender model.
`vap`	This option is only available if `type` is set to `vap`. Enter the name of the FortiExtender LAN extension downlink VAP.
`pvid`	Port VLAN ID, ranging from 1 to 4089. **Note**: `pvid 1` is reserved for untagged traffic.
`*vids`	Set the FortiExtender LAN extension downlink PVID (`pvid` is the VLAN ID). Enter VID numbers 1 - 4089 using a space for separation. Up to 50 VIDs are accepted. **Note:** Support for configuring vids is dependent your FortiExtender model.

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

`config extension-controller extender-profile`
`  edit "FVA22F-lanext-default"`
`  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 lte1`
`  set role secondary`
	`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`

FortiOS configuration	Synched FortiExtender configurations

`next`
`end`
`end`
`next`
`end`
	`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`

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 port1 is configured with a PVID of 100, and port2 is configured with a PVID of 200 and VIDs of 27 and 77.

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

`config extension-controller extender-profile`
`edit "FVA22F-lanext-default"`
`config lan-extension`
`set ipsec-tunnel "fext-ipsec-yqx8"`
`set backhaul-interface "internal3"`
`config backhaul`
`edit "1"`
`set port lte1`
`set role secondary`
`next`
`edit "2"`
`set port wan`
`set role primary`
`next`
`end`
`config downlinks`
`edit "1"`
`set type port`
`set port port1`
`set pvid 100`
`next`
`edit "2"`
`set type port`
	`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 100 200 27 77`
	`next`
	`edit port1`
	`set type physical`
	`set port port1`
	`set vids`
	`set pvid 100`
	`set security-8021x-member-mode enable`
	`next`
	`edit port2`
	`set type physical`
	`set port port2`
	`set vids 27 77`
	`set pvid 200`
	`set security-8021x-member-mode enable`
	`next`

FortiOS configuration	Synched FortiExtender configurations

`set port port2`
`set pvid 200`
`set vids 27 77`
`next`
`end`
`end`
`next`
`end`
	`end`
	`next`
	`end`

Wireless configurations on FortiExtender

You can enable wireless configurations on supported FortiExtender models used as FortiGate LAN extension. Clients connected to a WiFi access point on a managed FortiExtender can access the internet, even when FortiGate is in LAN extension mode. This example describes how to configure a WiFi access point with internet access for a managed FortiExtender:

1. Create a LAN extension SSID for FortiExtender on page 97.
2. Configure a FortiExtender profile on page 98.
3. Apply the profile to FortiExtender and authorize the device on page 99.
4. Configure the LAN extension interface as a DHCP server on page 100.
5. Configuring a firewall policy on page 102.
6. Verify settings on page 103.

Create a LAN extension SSID for FortiExtender

To create a LAN extension SSID - GUI:

See FortiExtender SSIDs on page 15.

To create a LAN extension SSID - CLI:

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
```

Configure a FortiExtender profile

Use a FortiExtender profile to define the LAN extension settings, such as the radio band for the LAN extension SSID, to create a WiFi SSID.

To add the SSID to a FortiExtender profile - GUI

See FortiExtender SSIDs on page 15.

To add the SSID to a FortiExtender profile - CLI

Add the SSID you configured to a extender profile set to LAN extension mode:

```
config extension-controller extender-profile
  edit "FVA22F-lanext-default"
    set extension lan-extension
    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
```

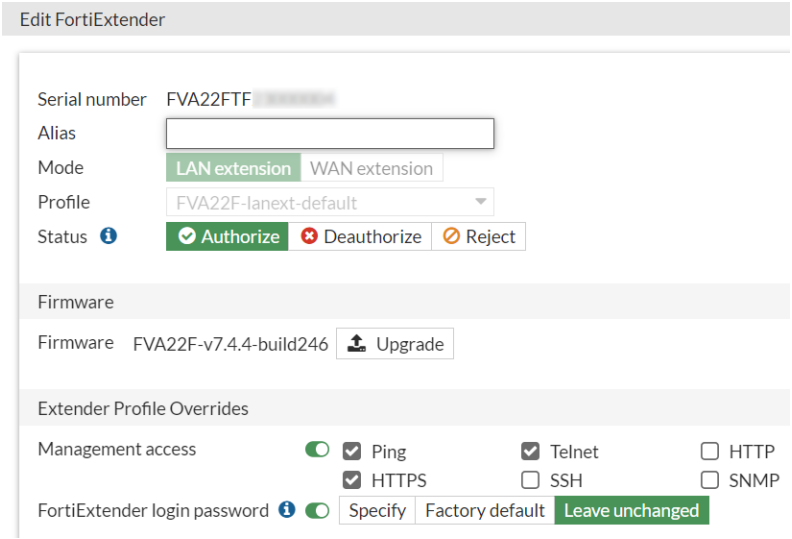
```
        set channel CH1 CH6 CH10
        set bandwidth auto
        set power-level 100
        set beacon-interval 100
        set 80211d enable
        set max-clients 0
        set extension-channel auto
        set bss-color-mode auto
        set bss-color 0
        set lan-ext-vap "lanext-vap1"
        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
  next
end
```

Apply the profile to FortiExtender and authorize the device

Associate the profile with FortiExtender and authorize the device. The profile settings are applied to the device during the authorization process.

To apply the profile to an authorized FortiExtender - GUI:

1. Go to *Network* > *FortiExtenders*, and double-click a FortiExtender device to open its settings.
2. In the *Profile* list, select the profile.
3. Click *Authorize*.



4. Set the remaining options, and then click *OK*.

To apply the profile to an authorized FortiExtender - CLI:

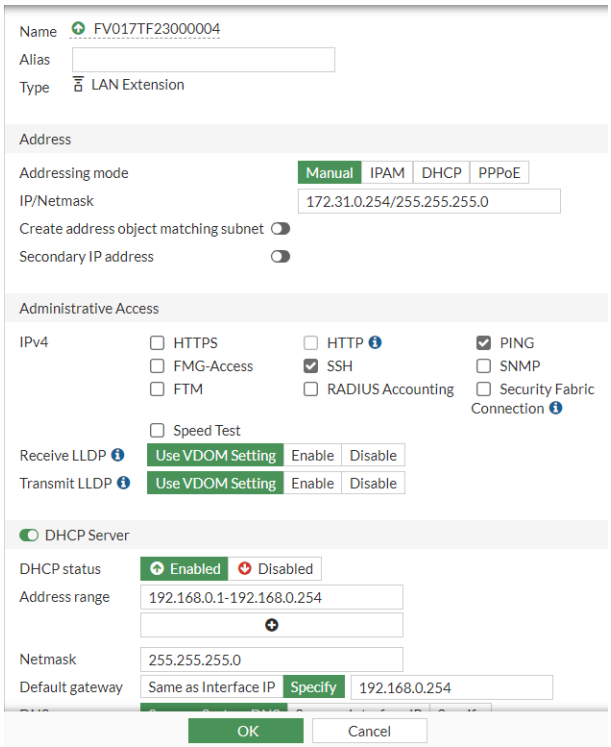
```
config extension-controller extender
  edit "FV017TF23000004"
    set id "FVA22FTF23000004"
    set authorized enable
    set device-id 0
    set extension-type lan-extension
    set profile "FVA22F-lanext-default"
  next
end
```

Configure the LAN extension interface as a DHCP server

Configure the LAN extension interface as an DHCP server to assign IP addresses to WiFi clients.

To configure the LAN extension interface as a DHCP server - GUI:

1. Go to *Network* > *Interfaces*, and double-click the LAN extension interface to open it for editing.
2. Enable *DHCP Server*.
3. Set *Address range*, *Netmask*, and *Default gateway*.



4. Set the remaining options as desired, and click *OK*.

To configure the LAN extension interface as a DHCP server - CLI:

1. Assign an IP address to the LAN extension interface:

```
config system interface
    edit "FV017TF23000004"
        set vdom "root"
        set ip 172.31.0.254 255.255.255.0
        set allowaccess ping ssh
        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
```

2. Configure the DHCP server on the LAN extension interface:

```
config system dhcp server
    edit 3
        set dns-service default
        set default-gateway 172.31.0.254
```

```
        set netmask 255.255.255.0
        set interface "FV017TF23000004"
        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 172.31.0.254
                set end-ip 172.31.0.254
            next
        end
    next
end
```

3. Confirm that the DHCP server can assign IP addresses to clients connecting to the FortiExtender Virtual Access Point (VAP).

   In this example, an iPhone connects to the FortiExtender 2.4GHz radio VAP named 2G-lan and receives an IP address of 172.31.0.3 from the LAN extension interface.

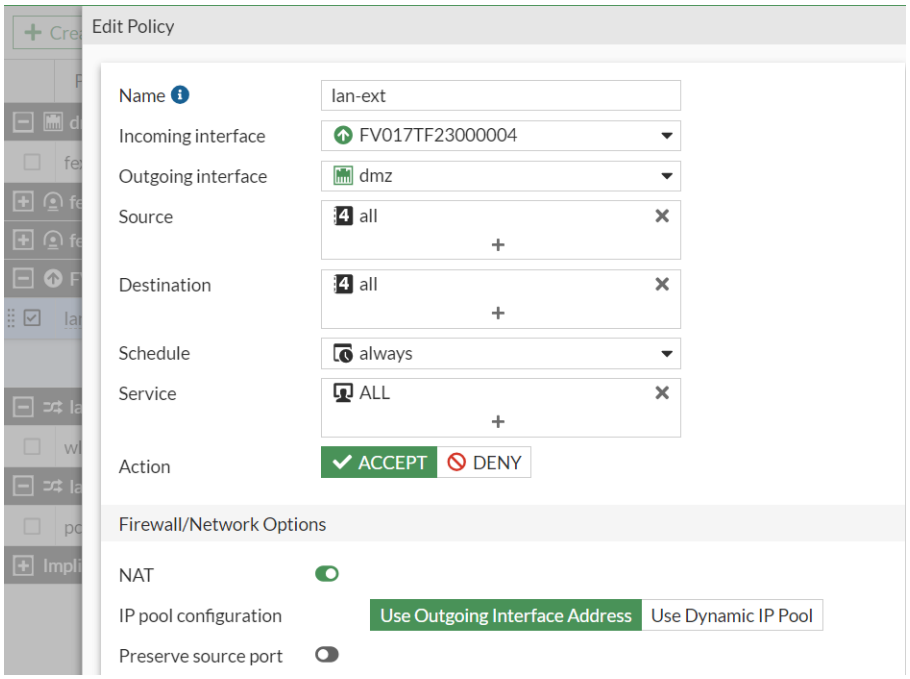
```
execute dhcp lease-list
FV017TF23000004
  IP            MAC-Address             Hostname            VCI                 SSID
     AP                  SERVER-ID           Expiry
  172.31.0.2    74:78:a6:8b:52:ff       FVA22FTF23000004    FortiExtenderVehicl
                        3                   Fri Apr 19 13:30:48 2024
  172.31.0.3    0a:ba:c9:5f:47:4d
```

Configuring a firewall policy

Configure a firewall policy with incoming interface set to the LAN extension interface to allow FortiExtender WiFi clients to reach the internet.

To configure a firewall policy to use the LAN extension interface - GUI:

1. Go to *Policy & Objects > Firewall Policy* and double-click the LAN extension policy to open it for editing.
2. Set *Incoming interface* to the LAN extension interface.
3. Set *Outgoing Interface*.



4. Set the remaining options as desired, and click *OK*.

To configure a firewall policy to use the LAN extension interface - CLI:

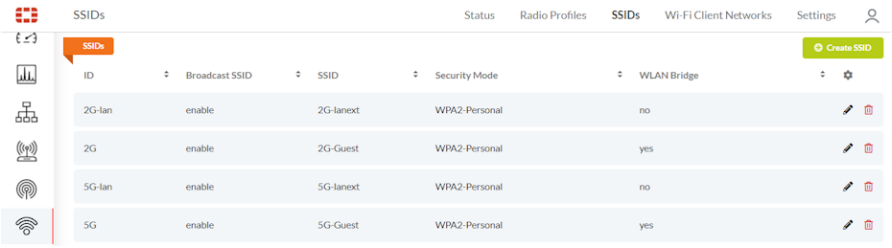
```
config firewall policy
...
    edit 4
        set name "lan-ext"
        set uuid 341c7010-270b-51ec-16b6-309891e3e880
        set srcintf "FV017TF23000004"
        set dstintf "dmz"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

Verify settings

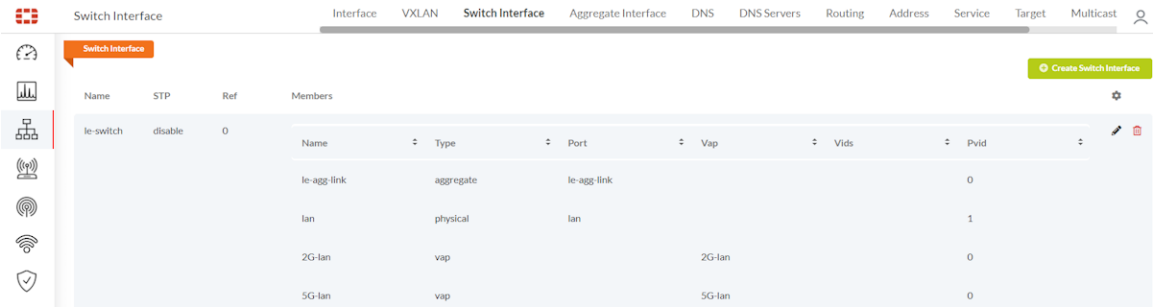
Verify that FortiExtender received the configuration from FortiGate.

To verify FortiExtender received the configuration:

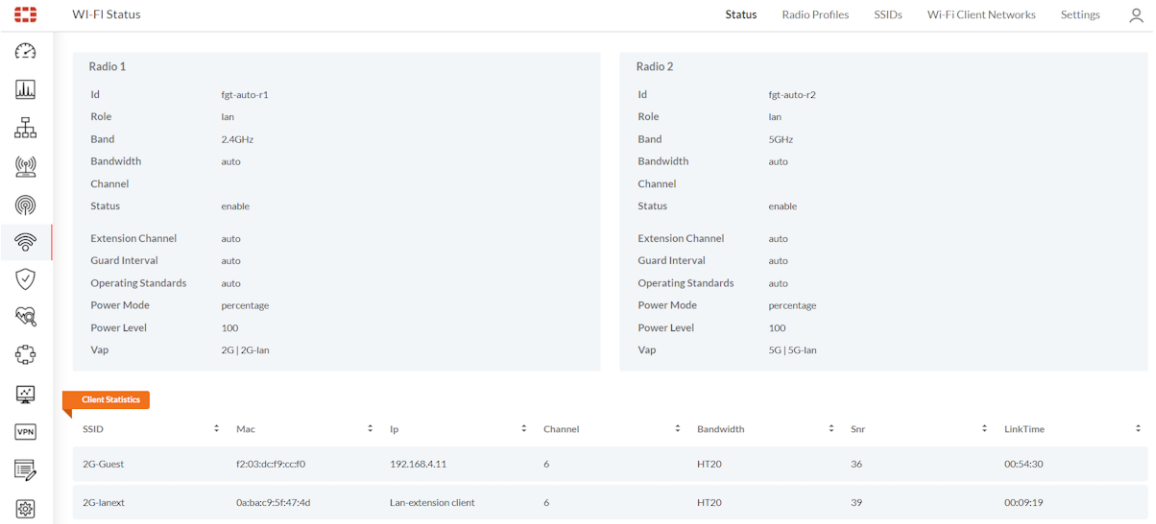
1. On FortiExtender GUI, go to *WiFi* > *SSIDs*, and verify that the device received a LAN extension type of SSID. In this example, the LAN extension type of SSID is named 2G-lanext.



2. Go to *Networking* > *Switch Interface*, and verify that the device received the WiFi interface for the LAN extension. In this example, the WiFi interface is named 2G-lan.



3. Go to *Wi-Fi* > *Status*, and verify that the WiFi client is connected to the LAN extension SSID. In this example, the client is connected to 2G-lanext.



4. Confirm the FortiExtender WiFi client can reach the internet.

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:

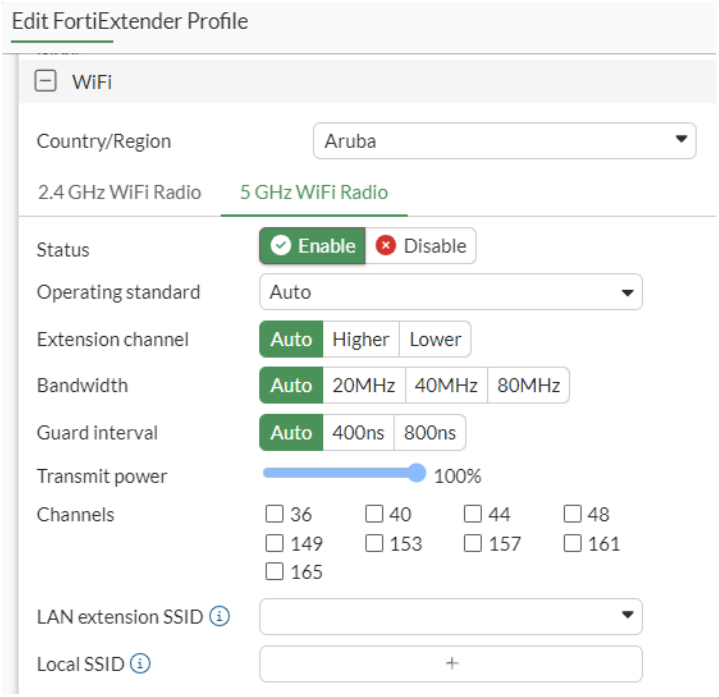
Scenario	DFS channel selection permission	
	FEV21xF	FBS10F
Fixed channel	Deny	Deny
Initial channel selection once the radio is up	Deny	Allow
Running time channel selection	Allow	Allow

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.



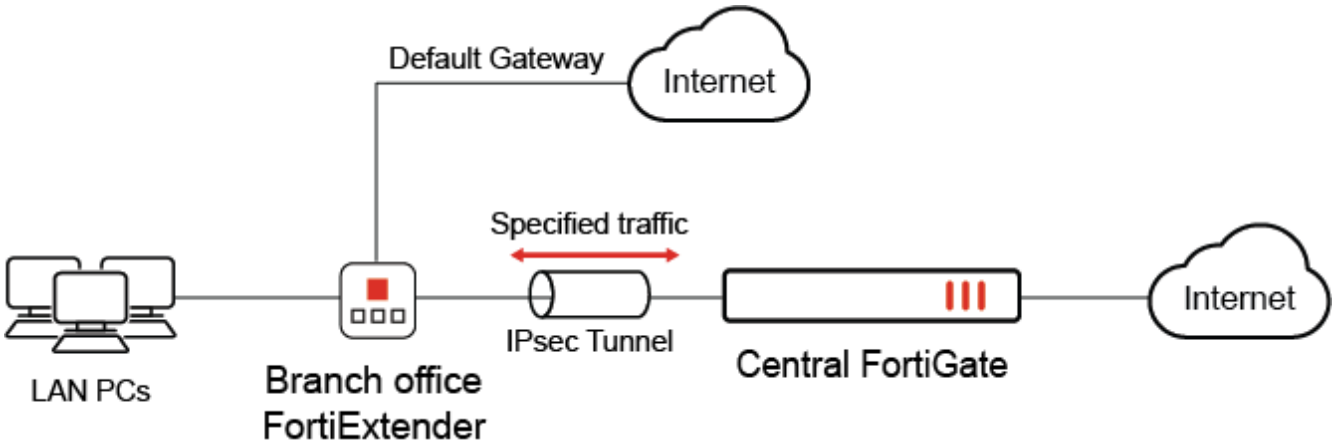
6. When you are finished, click *OK*.

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 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.

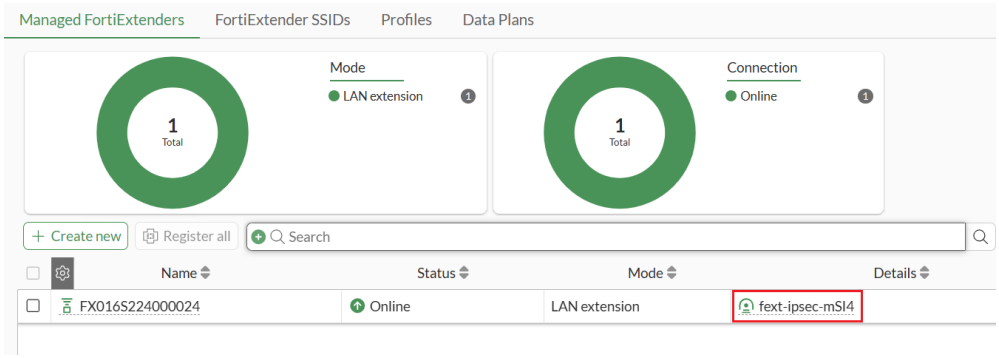
For example, FortiExtender can be managed by FortiSASE and used for microbranch deployments—a branch office deployment with a LAN behind a FortiExtender and secure internet access (SIA) over a backhaul connection to FortiSASE.

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 - GUI:

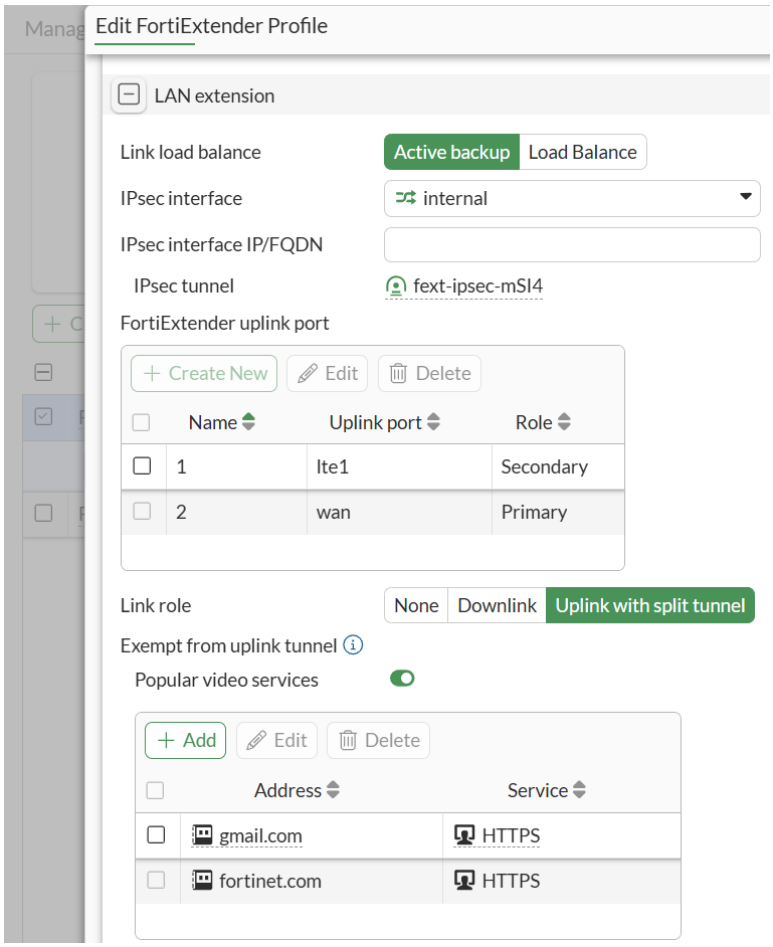
1. From the FortiGate, go to *Network > FortiExtenders > Managed FortiExtenders* and locate the FortiExtender you want to configure split tunneling for.
2. In the details column, you can find the name of the IPsec tunnel between the FortiExtender and FortiGate.



3. Go to *Network > FortiExtenders> Profiles* and click *Create new* or edit an existing FortiExtender profile.
4. Under *LAN extension*, you can configure the IPsec tunnel between the FortiGate and FortiExtender uplink port.

5. In *Link role*, select *Uplink with split tunnel* to select which traffic you want to exempt from being sent to the IPsec tunnel. You can enable *Popular video services* or add specific addresses in services you want to exempt.

   In the following example, popular video services, as well as https links to specific addresses are exempted from being sent to the IPsec tunnel.



6. When you are finished, click *OK*.

   FortiExtender clients will receive DHCP assignments from the FortiGate LAN extension interface.

7. To configure a firewall policy for FortiExtender clients, go to *Policy & Objects* > *Firewall Policy*, and click *Create new* to define a policy.

8. Configure the following:

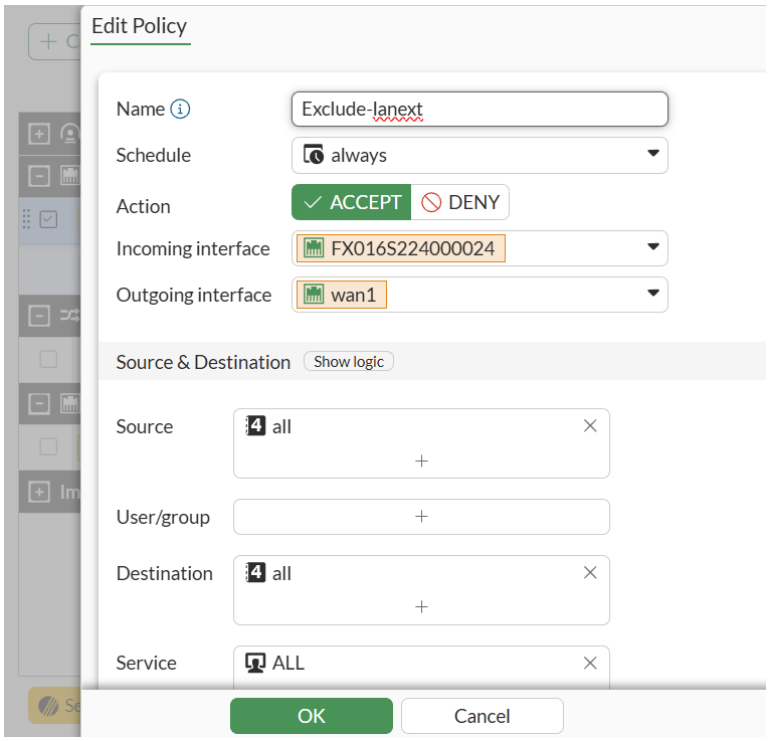
   a. Set the *Action* to *ACCEPT*.

   b. In the *Incoming interface*, set it to the FortiGate LAN extension interface.

      Note: FortiExtender clients receive DHCP assignments from the FortiGate LAN extension interface.

   c. In *Outgoing interface*, set it to *wan1*.

   d. When you are finished, click *OK*.



As defined in split tunneling mode, traffic will use this firewall policy to access the internet for initialization, DNS, and etc.

9. Once the session is established, the split traffic will be sent to the FortiExtender WAN interface via the FortiExtender firewall. This traffic will no longer use the IPsec tunnel.
   - The FortiExtender firewall only accepts the traffic from FortiExtender LAN clients, which is defined as *le-ts-le-switch* (the DHCP range in FortiGate LAN extension interface).
   - FortiExtender will forward the split traffic to a local interface with default gateway.

To configure split tunneling in LAN extension mode - CLI:

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
      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 synched to the FortiExtender devices.

3. Verify the synched 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
  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
```

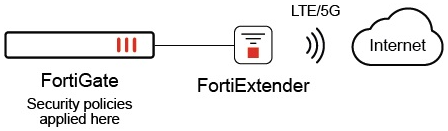
```
  next
end
```

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.

In this scenario, FortiGate manages FortiExtender over the 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 FortiOS. 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 WAN extension mode, you can connect a FortiExtender to two FortiGates in HA active-passive mode, or connect two FortiExtenders to two FortiGates in HA active-active mode to provide dual active redundancy for wireless WAN access.

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 WAN-extension 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 on FortiExtender as the WAN-extension of FortiGate

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.

You can configure VLAN mode with FortiExtender using either Port4 or the LAN port.

- Configuring VLAN with Port4 on page 113: Port4 works in DHCP client mode.
- Configuring VLAN with the LAN port on page 120: The LAN port acts as a DHCP server.

Configuring VLAN with Port4

When you configure VLAN mode on the FortiExtender using Port4, the port4 works in DHCP client 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.

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

Configure the FortiGate

1. Go to *Network* > *Interfaces* and select or create a WAN2 interface.
   a. Set the IP address to 192.168.2.99
   b. Enable *Security Fabric Connection* traffic.
   c. Enable *DHCP Server* and enter an *Address range* of 192.168.2.98-192.168.2.98.

Edit Interface

Name wan2
Alias
Type Physical Interface
VRF ID 0
Role LAN

Address

Addressing mode Manual | IPAM | DHCP | PPPoE | One-Arm Sniffer
IP/Netmask 192.168.2.99/24
Create address object matching subnet
Name wan2 address
Destination 192.168.2.0/24
Secondary IP address

Administrative Access

IPv4
- [ ] HTTPS
- [ ] FMG-Access
- [ ] FTM
- [ ] HTTP
- [ ] SSH
- [ ] RADIUS Accounting
- [x] PING
- [ ] SNMP
- [x] Security Fabric Connection
- [ ] Speed Test
- [ ] SCIM

Receive LLDP Use VDOM Setting | Enable | Disable
Transmit LLDP Use VDOM Setting | Enable | Disable

DHCP Server

DHCP status Enabled | Disabled
Address range 192.168.2.98-192.168.2.98
Netmask 255.255.255.0
Default gateway Same as Interface IP | Specify
DNS server Same as System DNS | Same as Interface IP | Specify
Lease time 604800 second(s)
FortiClient On-Net Status Default | Specify

Alternatively, you can configure from the CLI with the following:

```
config system interface
  edit "wan2"
    set vdom "root"
    set ip 192.168.2.99 255.255.255.0
    set allowaccess ping fabric
    set type physical
    set role wan
    set snmp-index 4
  next
end
```

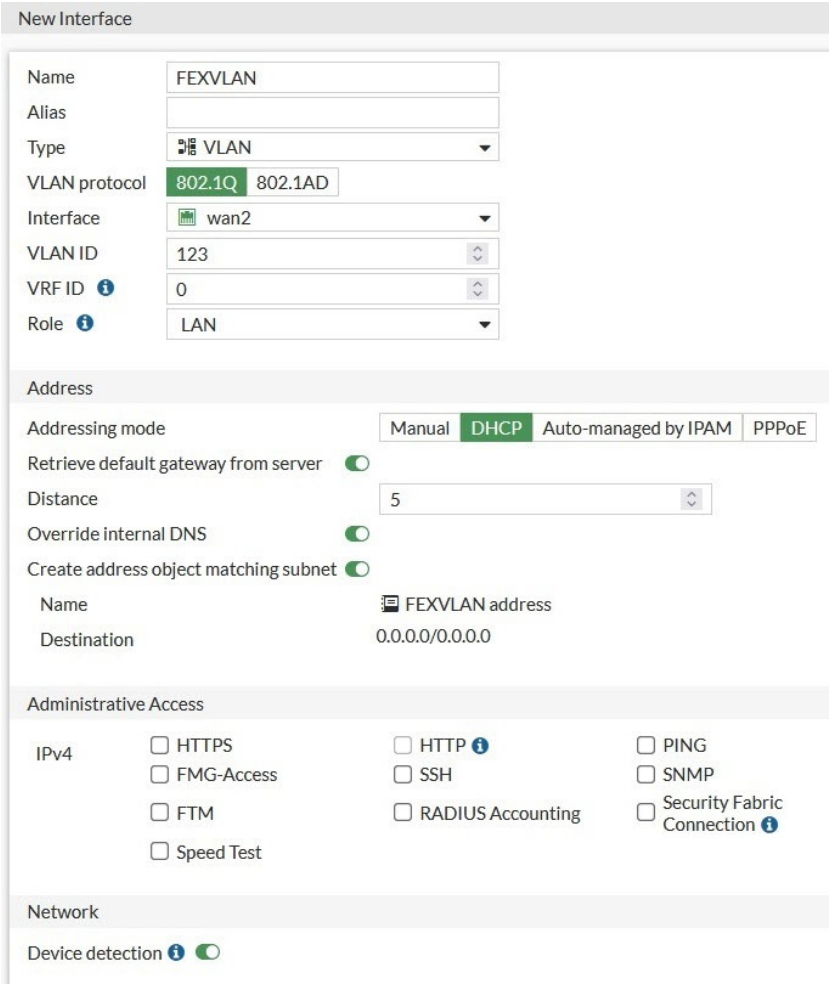
```
config system dhcp server
  edit 6
    set default-gateway 192.168.2.99
    set netmask 255.255.255.0
    set interface "wan2"
    config ip-range
      edit 1
        set start-ip 192.168.2.98
        set end-ip 192.168.2.98
      next
    end
  next
end
```

You must enable the DHCP server and configure an address lease pool of 192.168.2.98-192.168.2.98. This ensures that the FortiExtender obtains the correct address. Without this configuration, the FortiExtender will be unable to switch from CAPWAP to VLAN passthrough and the modem interface on the FortiGate never comes up.

2. Enable `fortiextender-vlan-mode`:

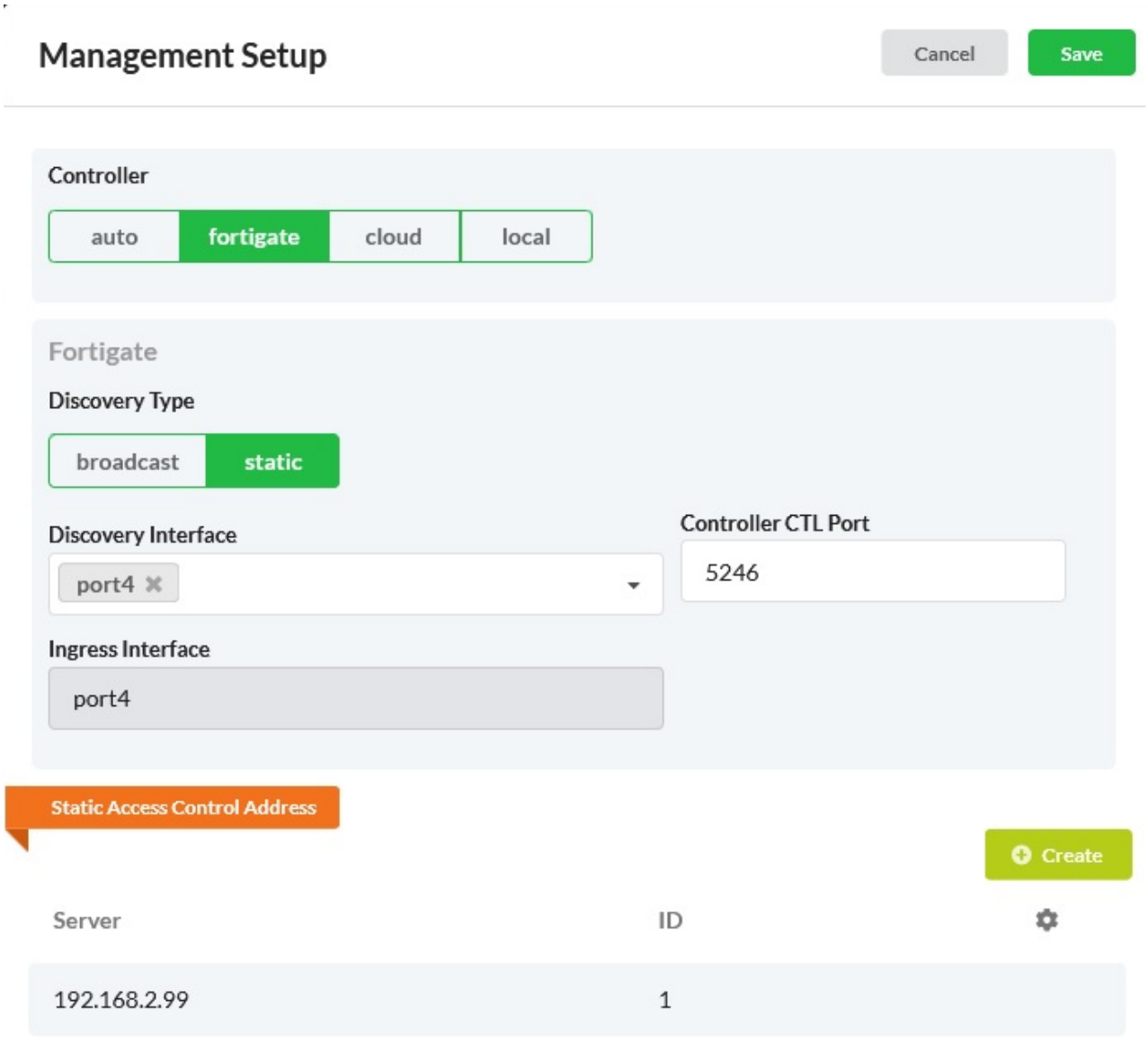
- By default, VLAN mode is disabled on FortiGate, and must be explicitly enabled on the FortiGate:
  ```
  config system global
     (global)set fortiextender-vlan-mode enable
     (global)end
  ```
- Before enabling VLAN mode, you must delete all the FortiExtender-WAN interfaces created on the device.

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.

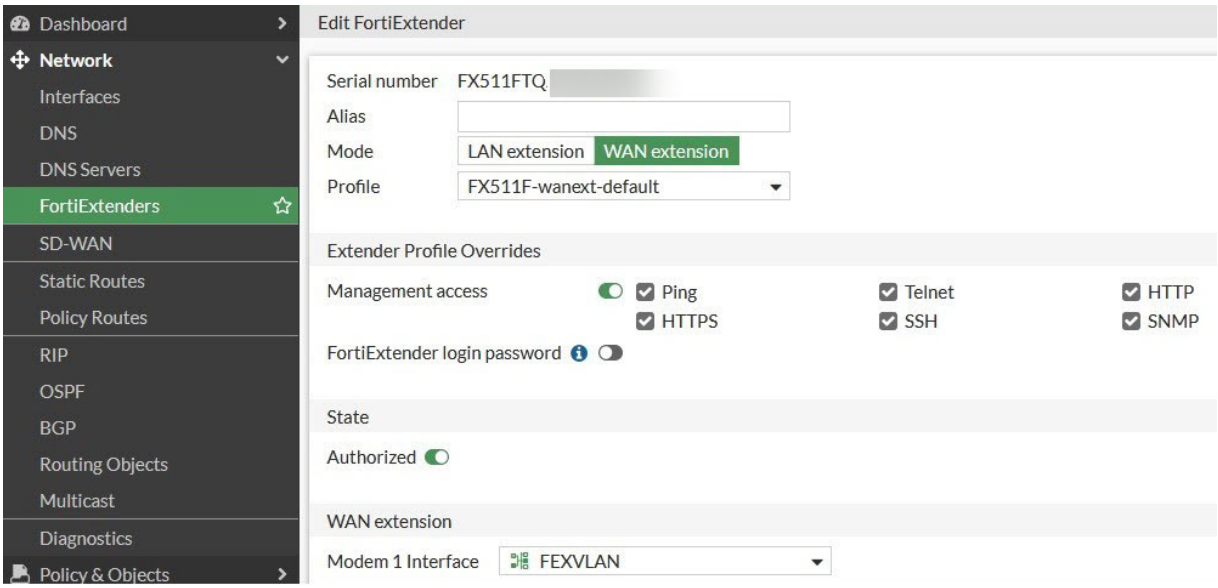


Configure the FortiExtender

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



3. 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

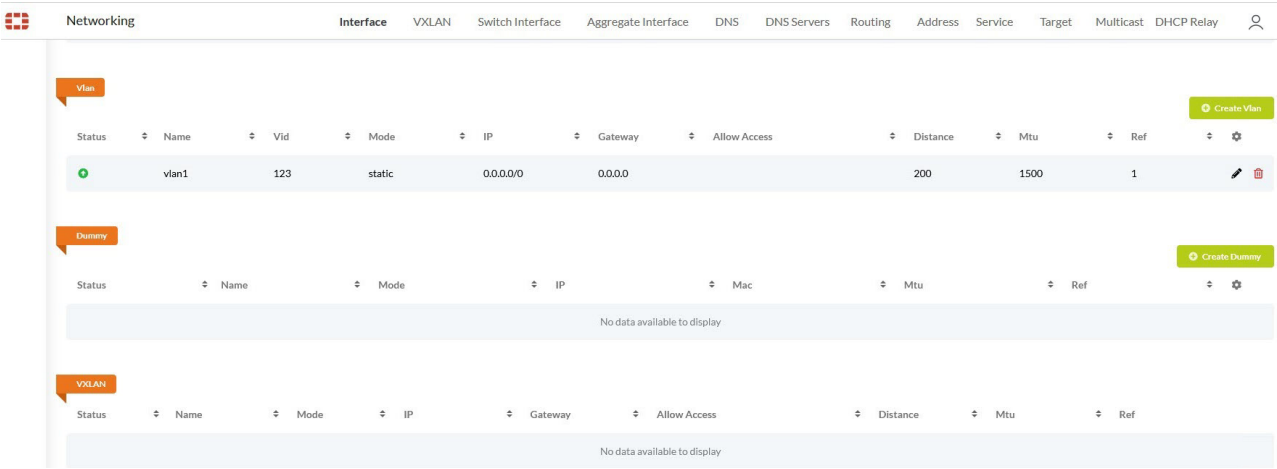


4. Wait for a few moments, for the FortiExtender may need to reboot when the mode is changed from NAT to IP-passthrough (VLAN).
5. After the WAN extension tunnel is set up, check its status from the FortiExtender Dashboard for the following Controller Information:
   - FortiGate, with Status — Connected
   - Mode — FortiGate (ip-passthrough (VLAN))
6. Check the status of the WAN extension with the following FortiExtender CLI command:

```
# get extender status
```

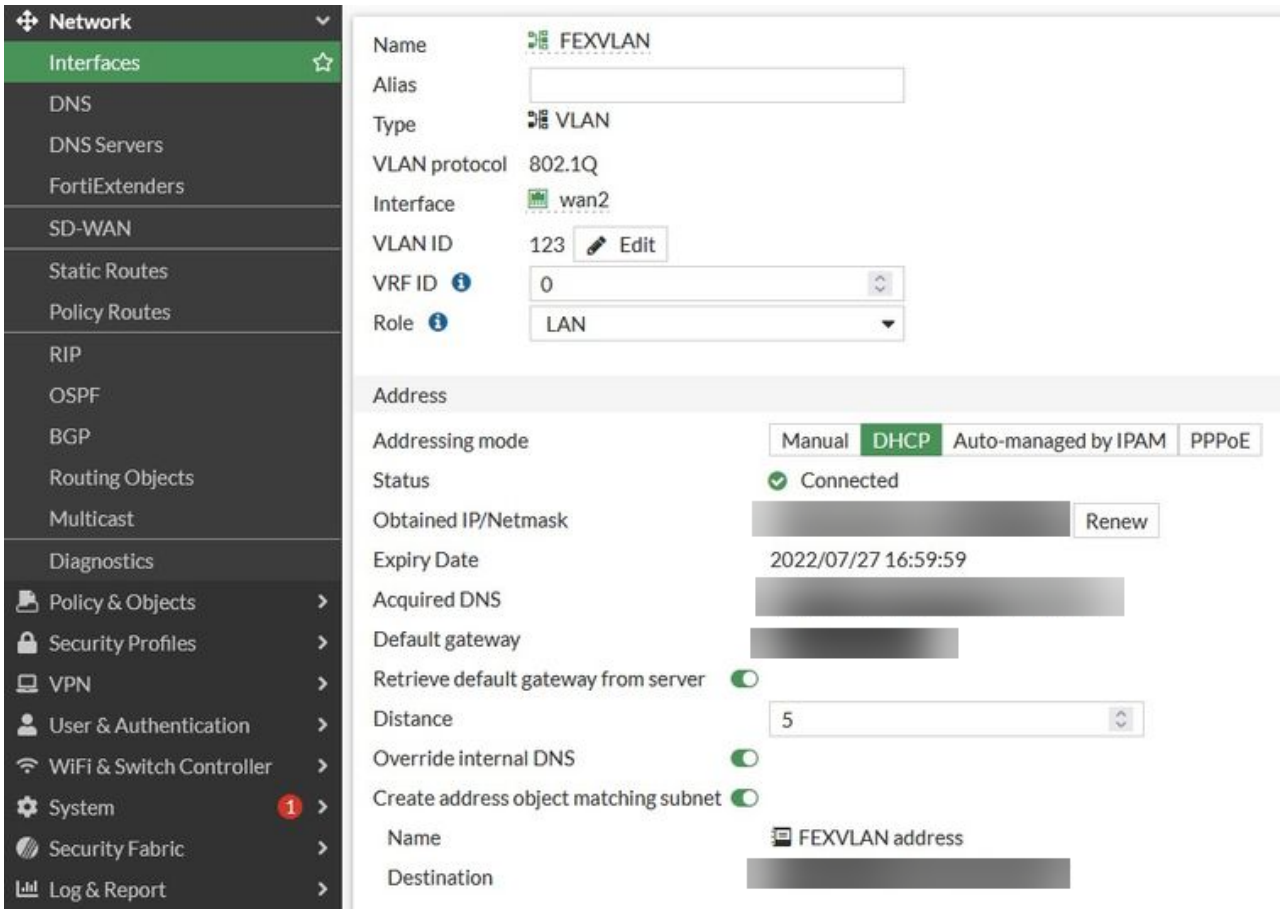
```
FX511FTQ[redacted]# get extender status
Extender Status
    name                : FX511FTQ[redacted]
    mode                : CAPWAP
    fext-addr           : 192.168.2.98
    ingress-intf        : port4
    fext-wan-addr       : [redacted]
    controller-addr     : 192.168.2.99:5246,25246
    controller-name     : FGT81E[redacted]
    uptime              : 0 days, 0 hours, 50 minutes, 28 seconds
    management-state    : CWWS_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
```

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. 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
    set ingress-intf lan
  next
end
```

7. 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.

Configuring VLAN with the LAN port

When you configure VLAN mode on the FortiExtender using the LAN port, the LAN acts as a DHCP server.

Before you start:

- Ensure that the VLAN interface is created according to the actual physical interface of the connected FortiExtender.

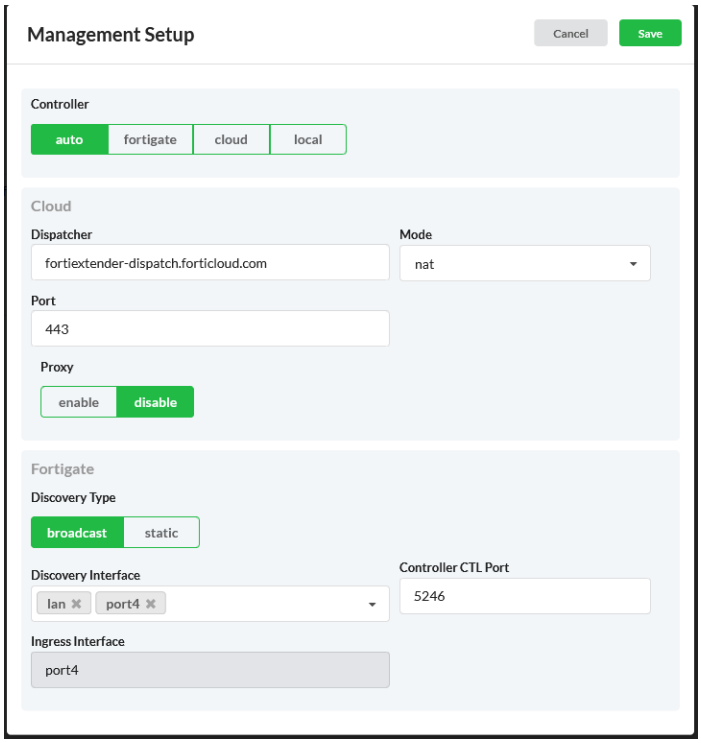
This sample configuration shows how to build a WAN-Extension VLAN connection between a FortiGate WAN2 interface and a FortiExtender LAN interface.

Configure the FortiExtender

1. Ensure that the FortiExtender LAN interface is connected to FortiGate WAN2 to get the IP address from the FortiGate.
2. From the FortiExtender, verify that the DHCP server is set to the `lan` interface.

```
config system dhcpserver
  edit 1
    set status enable
    set lease-time 86400
    set dns-service default
    set ntp-service specify
    set ntp-server1
    set ntp-server2
    set ntp-server3
    set default-gateway 192.168.200.99
    set netmask 255.255.255.0
    set interface lan
    set start-ip 192.168.200.110
    set end-ip 192.168.200.210
    set mtu 1500
    set vci_match disable
    set reserved-address disable
  next
end
```

3. Verify that the FortiExtender can be discovered by the FortiGate.
   - From the FortiExtender GUI:
     i. Go to *Setting* > *Management*, and verify the following configurations:
        - Controller — auto
        - Discovery Type — broadcast
        - Discovery Interface — lan, port4
        - Controller CTL Port — 5246



- CLI:

```
config system management
  set discovery-type auto
  config 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
  config cloud
    set dispatcher fortiextender-dispatch.forticloud.com
    set dispatcher-port 443
    set mode nat
    set proxy disable
  end
  config local
    set mode nat
  end
  config local-access
    set http 80
    set https 443
    set ssh 22
    set telnet 23
    set idle-timeout 5
  end
  config fortigate-backup
    set vrrp-interface
```

```
    set status disable
  end
end
```

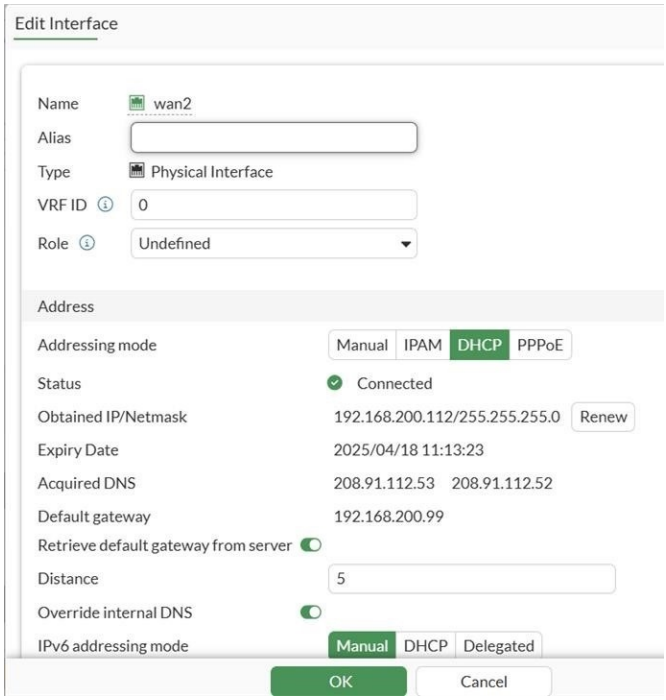
4. When you are finished, you can begin configuring from the FortiGate side.

Configure the FortiGate

1. By default, `fortiextender-vlan-mode` is disabled on FortiGate, and must be explicitly enabled on the FortiGate. Before enabling VLAN mode, you must delete all the FortiExtender-WAN interfaces created on the device.

```
config system global
  set fortiextender-vlan-mode enable
end
```

2. In the WAN2 interface, configure your mode and administrative access.
   - From the FortiGate GUI:
     i. Go to *Network* > *Interfaces* and select or create a WAN2 interface.
     ii. Set the *Addressing mode* to *DHCP*.
     iii. Enable *Ping* and *Security Fabric Connection* traffic.
     iv. When you are finished, click *OK*.

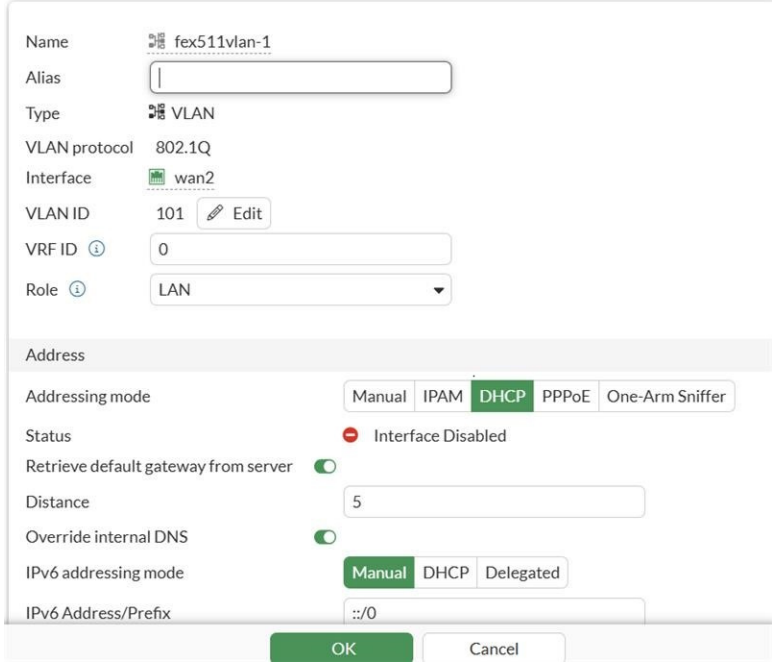


   - From the FortiGate CLI:

```
config system interface
  edit "wan2"
    set vdom "root"
```

```
    set mode dhcp
    set allowaccess ping fabric
    set type physical
    set description "WAN_Ext"
    set snmp-index 2
  next
end
```

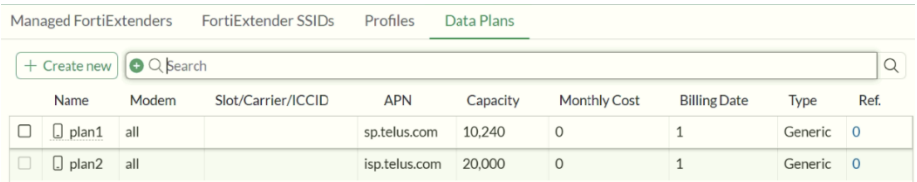
3. Create a VLAN interface on top of the WAN2 interface and configure the mode and interface.
   - From the FortiGate GUI:
     i. Go to *Network* > *Interfaces* and create a VLAN interface.
     ii. Set the *Role* to *LAN*.
     iii. Set the *Addressing mode* to *DHCP*.
     iv. When you are finished, click *OK*.



   - From the FortiGate CLI:

```
config system interface
  edit "fex511vlan-1"
    set vdom "root"
    set mode dhcp
    set status down
    set device-identification enable
    set role lan
    set snmp-index 18
    set interface "wan2"
    set mtu-override enable
    set vlanid 101
  next
end
```

4. Configure the data plans for each carrier.
   - From the FortiGate GUI:
     i. Go to *Network* > *FortiExtenders* > *Data Plans* and click *Create new* to configure data plans as needed.



Name	Modem	Slot/Carrier/ICCID	APN	Capacity	Monthly Cost	Billing Date	Type	Ref.
plan1	all		sp.telus.com	10,240	0	1	Generic	0
plan2	all		isp.telus.com	20,000	0	1	Generic	0

   - From the FortiGate CLI:

```
config extension-controller dataplan
  edit "plan1"
    set apn "sp.telus.com"
    set capacity 10240
  next
  edit "plan2"
    set apn "isp.telus.com"
    set capacity 20000
  next
end
```

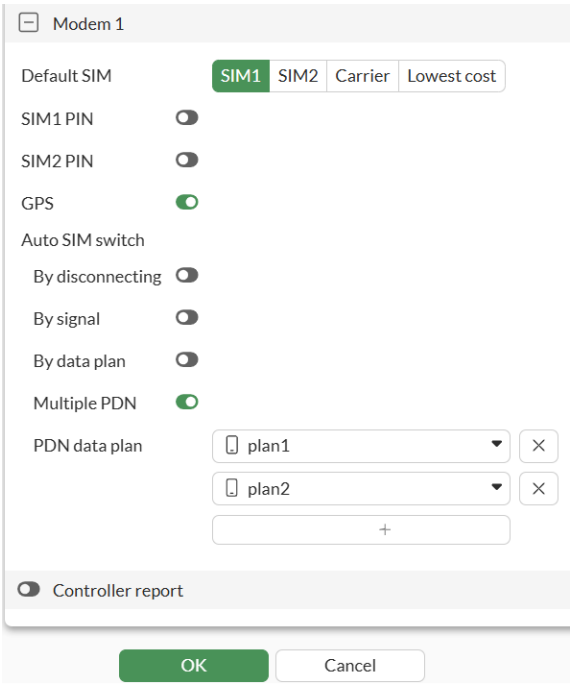
5. After FortiGate discovers the FortiExtender, it automatically creates a WAN-extension profile. You can find them in *Network* > *FortiExtenders* > *Profiles* or in the following CLI locations:
   a. Under the WAN-extension profile:

```
config extension-controller extender-profile
  edit "FXW51G-wanext-default"
    set id 0
    set model FXW51G
    config cellular
      set dataplan "plan1" "plan2"
      config sms-notification
      end
      config modem1
      end
    end
  next
end
```

   b. Under `extension-controller extender`.

```
config extension-controller extender
  edit "FX016S224000027"
    set id "FXW51GS224000027"
    set authorized discover
    set device-id 0
    set extension-type wan-extension
    set profile "FXW51G-wanext-default"
  next
end
```

6. In the Extender profile, enable `multi-pdn` and `sim-pin` as necessary and add your data plans. Note that only this feature is only available on FortiExtender models that support multiple APNs.
   - From the FortiGate GUI:
     i. Go to *Network > FortiExtenders > Profiles* and select the WAN-extension profile.
     ii. Under the modem section, enable *Multiple PDN* and add the data plans.
     iii. When you are finished, click *OK*.

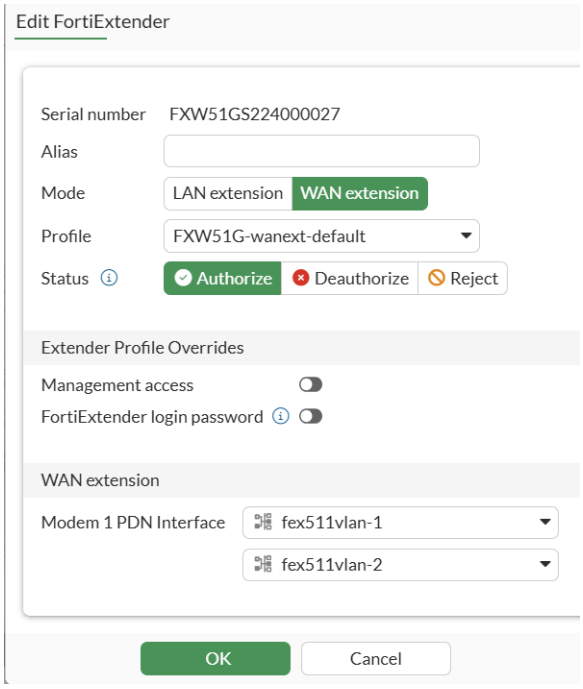


   - From the FortiGate CLI:

```
config extension-controller extender-profile
  edit "FXW51G-wanext-default"
    set id 0
    set model FXW51G
    config cellular
      set dataplan "plan1" "plan2"
      config sms-notification
      end
      config modem1
        set sim1-pin enable
        set sim1-pin-code ENC *
        set multiple-PDN enable
        set pdn1-dataplan "plan1"
        set pdn2-dataplan "plan2"
        set pdn3-dataplan ''
        set pdn4-dataplan ''
      end
    end
  next
end
```

7. Once your FortiExtenders are discovered by the FortiGate, authorize the FortiExtender.

- From the FortiGate GUI:
  i. Go to *Network* > *FortiExtenders* > *Managed FortiExtenders* and select the FortiExtender you want to Authorize.
  ii. In *Status*, select *Authorize*.



- From the FortiGate CLI:

```
config extension-controller extender
  edit "FX016S224000027"
    set id "FXW51GS224000027"
    set authorized enable
    set device-id 0
    set extension-type wan-extension
    set profile "FXW51G-wanext-default"
    config wan-extension
      set modem1-pdn1-interface "fex511vlan-1"
      set modem1-pdn2-interface "fex511vlan-2"
    end
  next
end
```

To verify your FortiExtender and FortiGate VLAN connection:

1. From the FortiGate, enter the following commands to verify that the FortiGate can receive the FortiExtender IP and can ping the internet:

```
FortiGate-80F # get system interface | grep vlan-1
== [ fex511vlan-1 ]
name: fex511vlan-1   mode: dhcp    management-ip: 0.0.0.0 0.0.0.0   ip: 25.24.90.204
255.255.255.248   status: up    netbios-forward: disable    type: vlan   netflow-sampler:
```

```
disable    sflow-sampler: disable    src-check: enable    explicit-web-proxy: disable
explicit-ftp-proxy: disable    proxy-captive-portal: disable    trunk: disable    switch-
controller-feature: none    wccp: disable    drop-overlapped-fragment: disable    drop-
fragment: disable    mtu-override: disable

FortiGate-80F # execute ping-options interface fex511vlan-1

FortiGate-80F # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=51 time=33.6 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=21.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=15.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=16.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=16.0 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 15.0/20.4/33.6 ms
```

2. From the FortiExtender, enter the following commands:

```
get extender status
Extender Status
    name                 : FXW51GS224000027
    mode                 : CAPWAP
    session              : active
      fext-addr          : 192.168.200.99
      ingress-intf       : lan
      fext-wan-addr      : 25.18.245.44
      controller-addr    : 192.168.200.110:5246,25246
      controller-name    : FGT80FTK22071065
      uptime             : 0 days, 0 hours, 29 minutes, 57 seconds
      management-state   : CWWS_RUN
    session              : standby
      fext-addr          : 0.0.0.0
      ingress-intf       :
      fext-wan-addr      : 25.18.245.44
      controller-addr    : 192.168.200.110:5248,25248
      controller-name    :
      management-state   : CWWS_DISCOVERY
    session              : obm
      fext-addr          : 0.0.0.0
      ingress-intf       :
      controller-addr    : fortiextender-dispatch.forticloud.com:443
      account-id         : 0
      management-state   : CWWS_CLD_CONN
    base-mac             : 78:18:EC:DE:33:88
    network-mode         : ip-passthrough (vlan)
    fgt-backup-mode      : backup
    discovery-type       : broadcast
    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
```

The FortiExtender management state should be in `CWWS_RUN`, indicating VLAN mode over the LAN interface has been successfully created between the FortiGate and FortiExtender.

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

Multiple PDNs are not supported in IPv6 or in IPv4-IPv6 dual stack scenarios.

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):

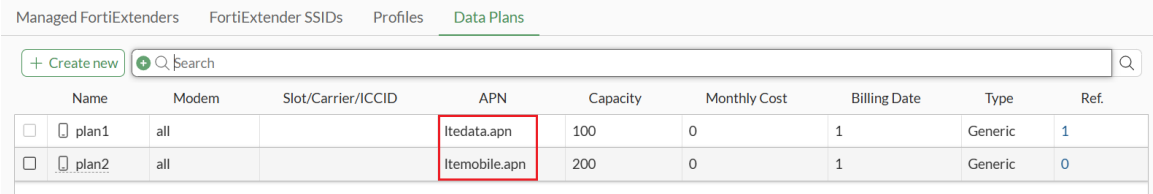
- FEX-511G
- FEX-511G-WiFi

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. By using different APNs to create multiple Packet Data Networks (PDNs), FortiGate can establish up to four FortiExtender virtual interfaces from a single FortiExtender modem. These interfaces provide you with more flexibility to customize data traffic steering, improving FortiGate connectivity and performance through FortiExtender.

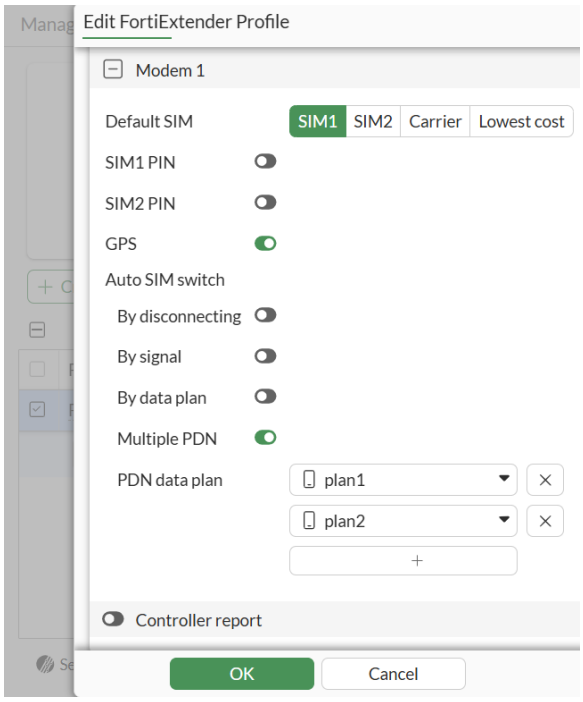
- Support for configuring multiple PDNs can only be done with one SIM card inserted; it will not work if there is more than one SIM card inserted.
- CHAP authentication with any order APN is supported, but this feature is dependent on whether the ISP also supports it. Check with your ISP before making your configurations.

To configure multiple APNs - GUI:

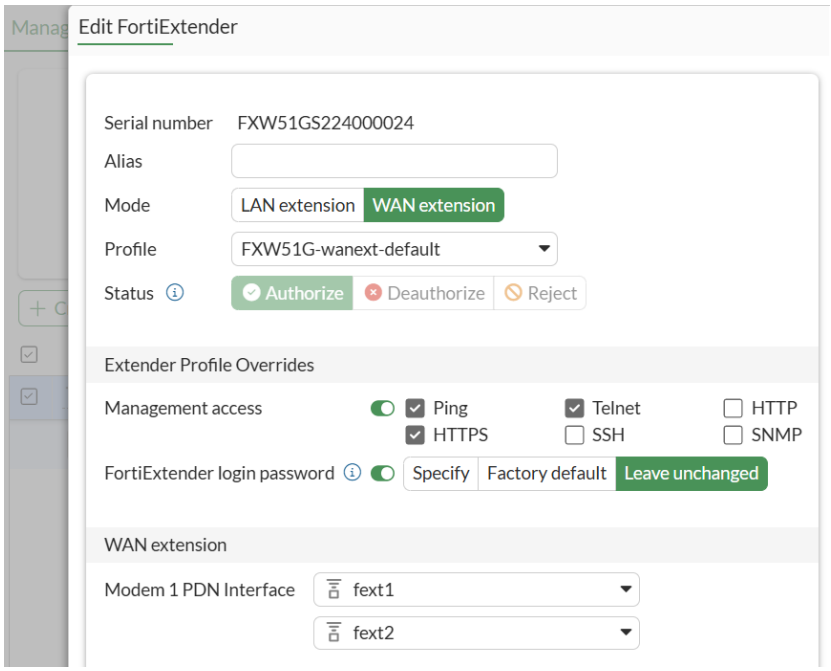
1. From the FortiGate, go to *Network* > *FortiExtenders* > *Data Plans* and click *Create new* to create multiple data plans with unique APNs.



2. Go to *Network* > *FortiExtenders* > *Profiles* and create a FortiExtender profile.
3. Select a model that supports multiple APNs, and then set the *Mode* to *WAN extension*.
4. Under the modem section, enable *Multiple PDN* and add the multiple data plans (with different APN) to the same modem.

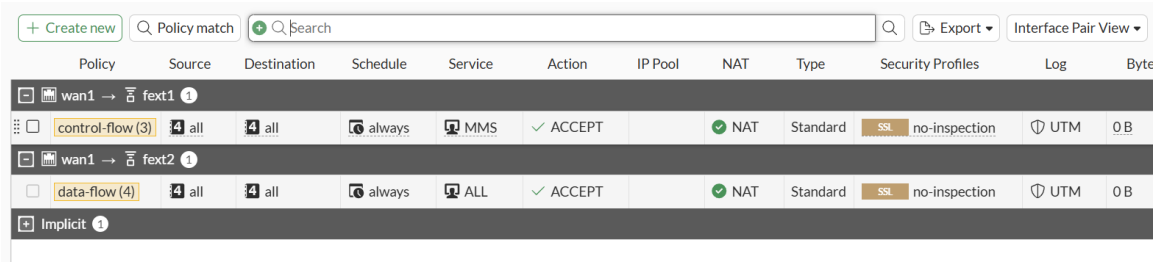


5. When you are finished, click *OK*.
6. Go to *Network* > *FortiExtenders* > *Manged FortiExtenders* and *Authorize* the FortiExtender.
7. Under *WAN extension*, add your FortiExtender interfaces to the *Modem 1 PDN Interface*.



Multiple FortiExtender interfaces can be created to match the different PDN.

8. Go to *Policy & Objects > Firewall Policy* and create firewalls policies to steer different traffic flows to different FortiExtender interfaces based on PDNs.



To configure multiple APNs - CLI:

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`.
- CHAP authentication with any order APN is supported, but this feature is dependent on whether the ISP also supports it. Check with your ISP before making your configurations.
- 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
  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 lte1-plan <dataplan name for apn1>
  set lte1_1-plan <dataplan name for apn2>
  set lte1_2-plan <dataplan name for apn3>
  set lte1_3-plan <dataplan name for apn4>
end
```

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

- By default, the `lte1-plan`, `lte1_1-plan`, `lte1_2-plan`, and `lte1_3-plan` are directly mapped to the `lte1`, `lte1_1`, `lte1_2`, and `lte1_3` interfaces on the FortiExtender, respectively.
- `lte1_1`, `lte1_2`, `lte1_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 `lte1`, `lte1_1`, `lte1_2`, and `lte1_3`, even if only three APNs were provided
- Avoid manually changing the down/up state of `lte1`, `lte1_1`, `lte1_2`, and `lte1_3`.
- The `lte1`, `lte1_1`, and `lte1_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-profile
  edit "FX511F-wanext-default"
    set id 3
    set model FX511F
    config cellular
      set dataplan "1"
      config sms-notification
      end
      config modem1
        set redundant-mode enable
        set redundant-intf "wan1" <wan interface, ie wan1>
      end
    end
  next
end
```

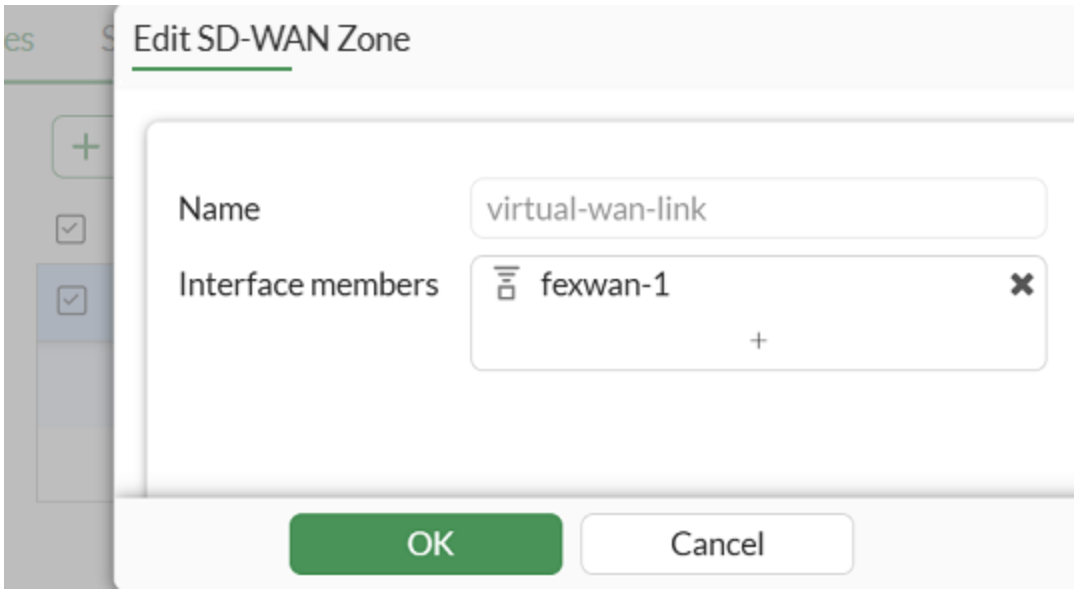
In this mode of operation, the FortiExtender interface comes up if the WAN interface goes down and goes down if the WAN interface comes up.

SD-WAN

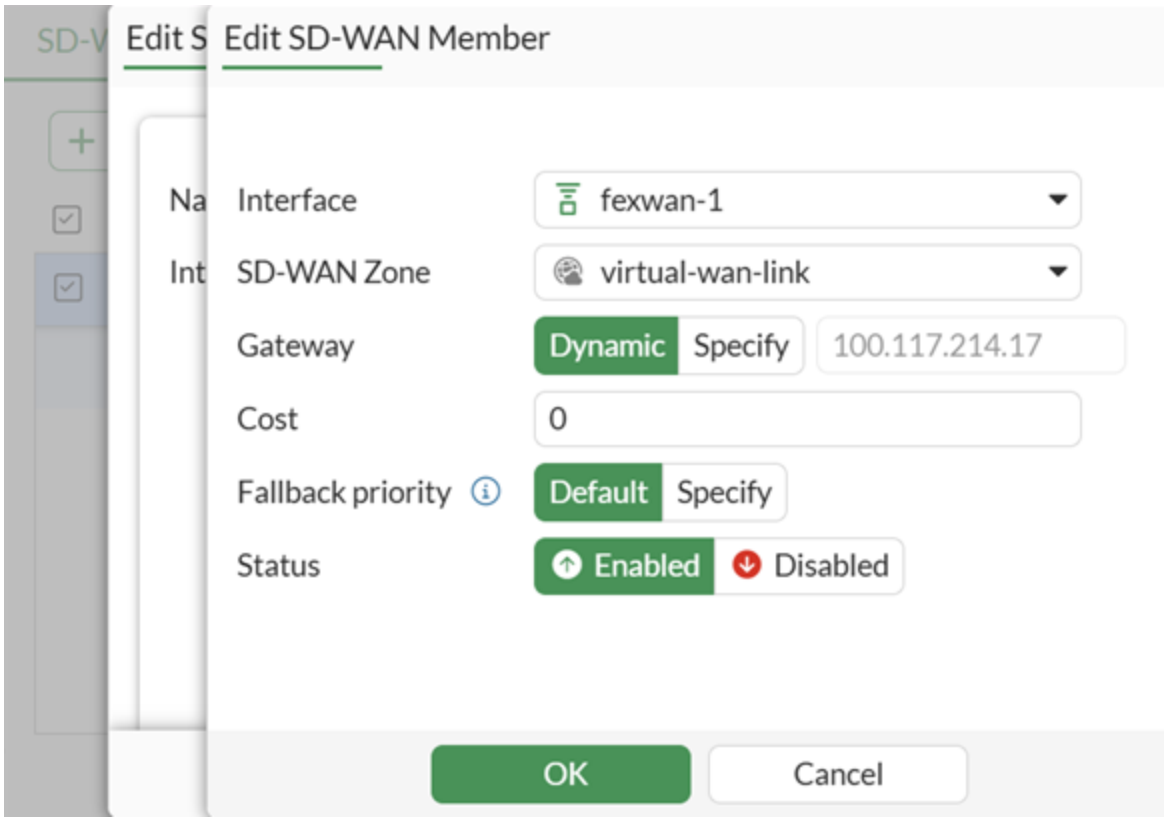
FortiOS recognizes and uses FortiExtender as a valid interface within an SD-WAN interface zone. Using SD-WAN, FortiGate becomes a WAN path controller and supports diverse connectivity methods. With FortiExtender, 3G/4G/5G can be used as the primary connection, a backup interface, or a load-balanced WAN 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 configure FortiExtender as an SD-WAN interface:

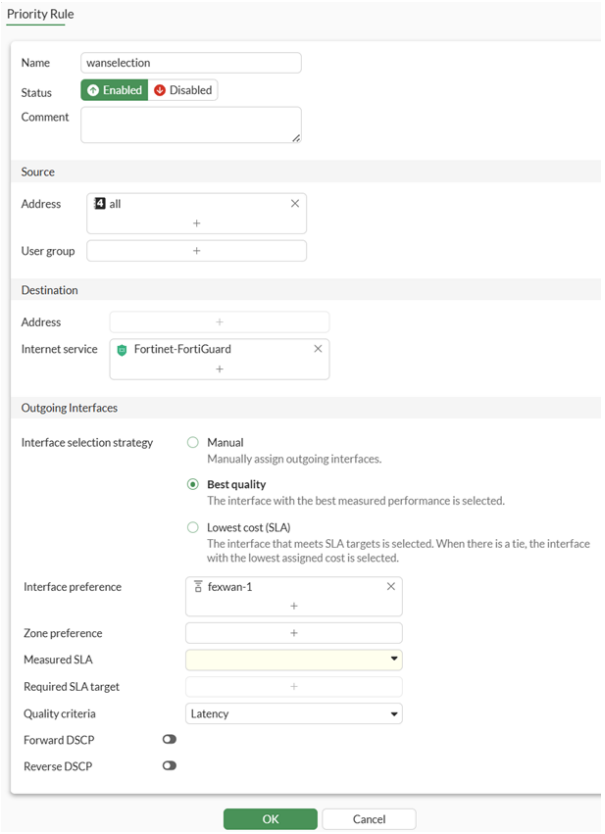
1. Go *Network* > *SD-WAN* > *SD-WAN Zones* and click to edit the *virtual-wan-link* interface.



2. Click the *Interface members* field to add a new SD-WAN member.



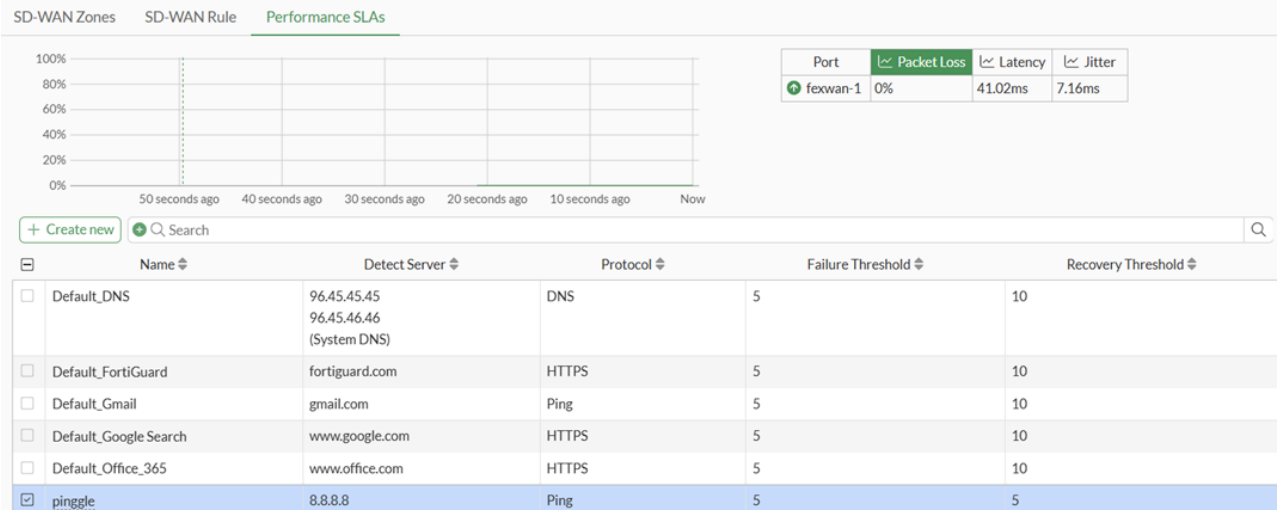
3. Go to *Network > SD-WAN > SD-WAN Rule* and define the priority rule. In this example, the *Outgoing Interfaces* is using the *Best Quality* strategy based on the Latency or Jitter criterion.



4. Order or combine your policies as illustrated below.

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used
IPv4 7							
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 1							
	sd-wan	all	all	Source IP	any		

5. 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:

- Configuring a data plan on page 139
- Set the default SIM on page 141
- Configure SIM-switch on page 142
- Configure SIM-switch based on link health on page 145
- Report to FortiGate on page 146
- VLAN mode on FortiExtender as the WAN-extension of FortiGate on page 113

Configuring a data plan

A Data Plan contains information about the service plan that you have signed up or subscribed from a mobile service provider or carrier as well as configurations to define how each model selects a SIM card. It identifies your mobile service provider, and contains information such as your SIM credentials, allowed data usage, and billing cycle.

To create a data plan - CLI:

You can configure a data plan with the following CLI parameters from the FortiExtender:

```
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 an LTE interface has breached its data usage limit (`overage`), 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

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>).

Parameter	Description
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).
billing-date	The billing date of the month.
overage	When an LTE interface has breached its data usage limit (`overage`), 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
preferred-subnet	DHCP subnet.
private-network	When enabled, FortiExtender allows the flow of non-NATed IP traffic on to an LTE interface.
session-dial-timeout	In some case, it may take time for the modem to establish a session. In these cases, you can configure a longer start session timeout to ensure that the modem has enough time to connect. The default value is `0`, meaning "disabled". You can set it to a larger value ranging from 0-180.

To create a data plan - GUI:

1. From the FortiExtender GUI, go to *LTE > Plan > Create Plan*.
2. Enter your desired plan configurations.
3. When you are finished, click *Save*.

Set the default SIM

When installing two SIM cards in one modem, you can select which default SIM to use. You can use the following criteria to set the default SIM:

- Set the default SIM by preferred carrier on page 141
- Set the default SIM by low cost on page 142
- Set the default SIM by SIM slot on page 142

Set the default SIM by preferred carrier

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

From the FortiExtender CLI, configure the following:

```
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`.

From the FortiExtender CLI, configure the following:

```
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 FortiExtender CLI commands:

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

Configure SIM-switch

You can configure SIM switching between the currently active eSIM profile and the SIM in the physical SIM slot 1. SIM-switch does not switch between eSIM profiles.

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.

FortiExtender comes with two SIM-card slots per modem, with the first one (i.e., sim1) being the default. SIM-switch works only when you have two SIM cards installed on a FortiExtender device with the feature enabled on it. SIM-switch is disabled by default.

When SIM-switch is enabled, FortiExtender can automatically switch to sim2 to maintain the current LTE connection when any of the following situations occurs:

- **By Disconnect:** An Internet session gets disconnected. By default, FortiExtender automatically switches to sim2 if sim1 gets disconnected for three times within 600 seconds.
- **By Data Plan:** Data usage has exceeded the set limit of your data plan and overage is disabled. By default, overage is disabled. SIM-switch does not occur if overage is enabled.
- **By Signal:** The relative signal (RSSI value) stays lower than the specified value for a major part of the time period defined. By default, the RSSI value is -100, and the time period is 600 seconds. This means that SIM-switch occurs if the RSSI value stays below -100 for more than 300 seconds.

  RSSI Values and LED State

RSSI	LED-1	LED-2	LED-3	LED-4
0, or N/A, or 'rssi<=-100'	OFF	OFF	OFF	OFF
-90~-81	ON	OFF	OFF	OFF
-80~-71	ON	ON	OFF	OFF
-70~-61	ON	ON	ON	OFF
rssi>=-60	ON	ON	ON	ON

- **By Health Monitor:** Based on the link health you configure. This requires configuring an hmon hhck instance and linking the auto-switch instance to that configured health check (see Configure SIM-switch based on link health on page 145).

To configure SIM-switch:

1. From the FortiExtender CLI, configure the following:

```
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
```

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.

Parameter	Description
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.

To force an immediate SIM-switch:

You can force the FortiExtender to immediately switch a modem's inactive SIM to the active SIM. From the FortiExtender CLI, enter the following command:

```
#execute sim-switch [modem1 | modem2]
```

The FortiExtender must have two SIMs for the command to work (or if eSIM is enabled, then an eSIM profile needs to be active). Modem2 is only available if the FortiExtender platform has two modems.

SIM switch-back

You can configure a FortiExtender to automatically fail back to the preferred SIM card after a failover.

To enable SIM switch-back:

```
config lte setting
  config modem1
    config auto-switch
      set switch-back [by-time | by-timer]
      set switch-back-time (HH:MM)
      set switch-back-timer (3600 – 2147483647)
    end
  end
end
```

Parameter	Description
`switch-back`	Direct modem to switch back to a preferred SIM when the secondary SIM is active. • `by-time`: Switch back at a specified time using the HH:MM format. • `by-timer`: Switch back after the specified duration is over.
`switch-back-time`	Switch over to the preferred SIM/carrier at the specified UTC time in HH:MM format.
`switch-back-timer`	Switch over to the preferred SIM/carrier after the given duration.

Configure SIM-switch based on link health

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

To configure SIM-switch based on link-health:

1. From the FortiExtender CLI, configure an hmon hchk instance. The instance in this example is named "`sim-health`".

```
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 lte1
        set src-type none
        set filter loss
    next
end
```

2. Configure the SIM switch settings to enable switching `by-health-monitor`, and link the hmon hchk instance you configured.

```
config lte setting
  config modem1
    config 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
    end
  end
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.
`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
    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.

CAPWAP on multiple ports for broadcast discovery

FortiExtender can discover FortiGate on multiple interfaces 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 it or removed. These configurations specify the mapping of the LTE interfaces and the `capwap` interfaces. For example, `'set lte1-mapping capwap1'` means the traffic from the `capwap1` interface will be sent out by the `lte1` interface.

```
config system virtual-wire-pair
      set lte1-mapping capwap1
end
```

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
```

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 covers common FortiExtender use cases.

WAN extension mode use cases

- Redundant with FortiGate in IP pass-through mode on page 151
- IPv6 in IP pass-through mode on page 155

WAN and LAN extension mode use cases

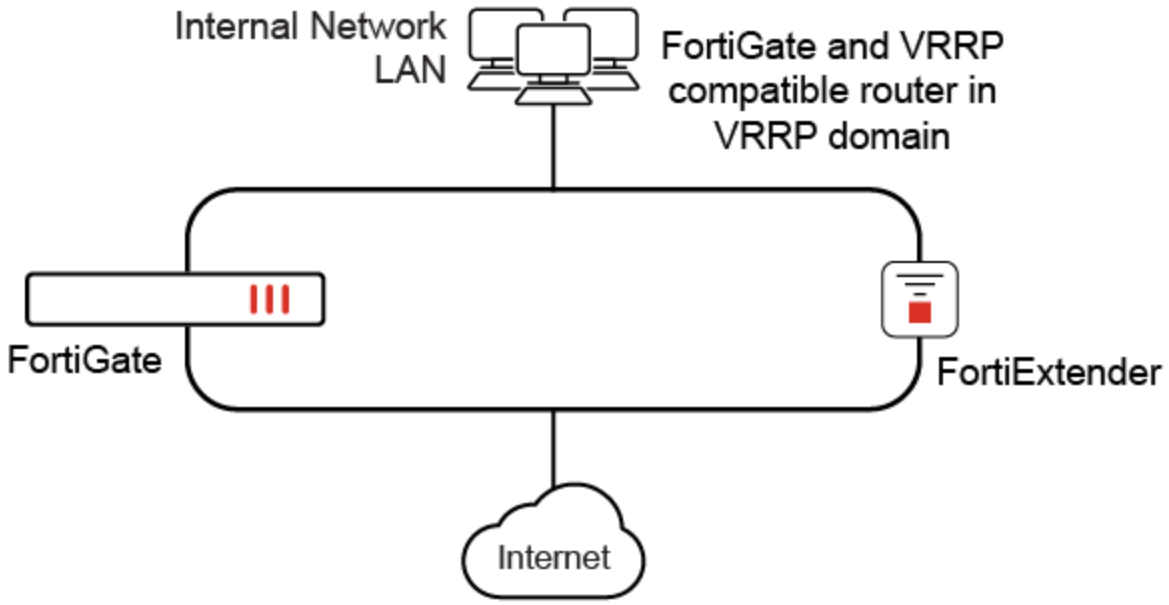
- FortiExtender for FortiGate HA configuration on page 158

Redundant with FortiGate 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 158.)
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:

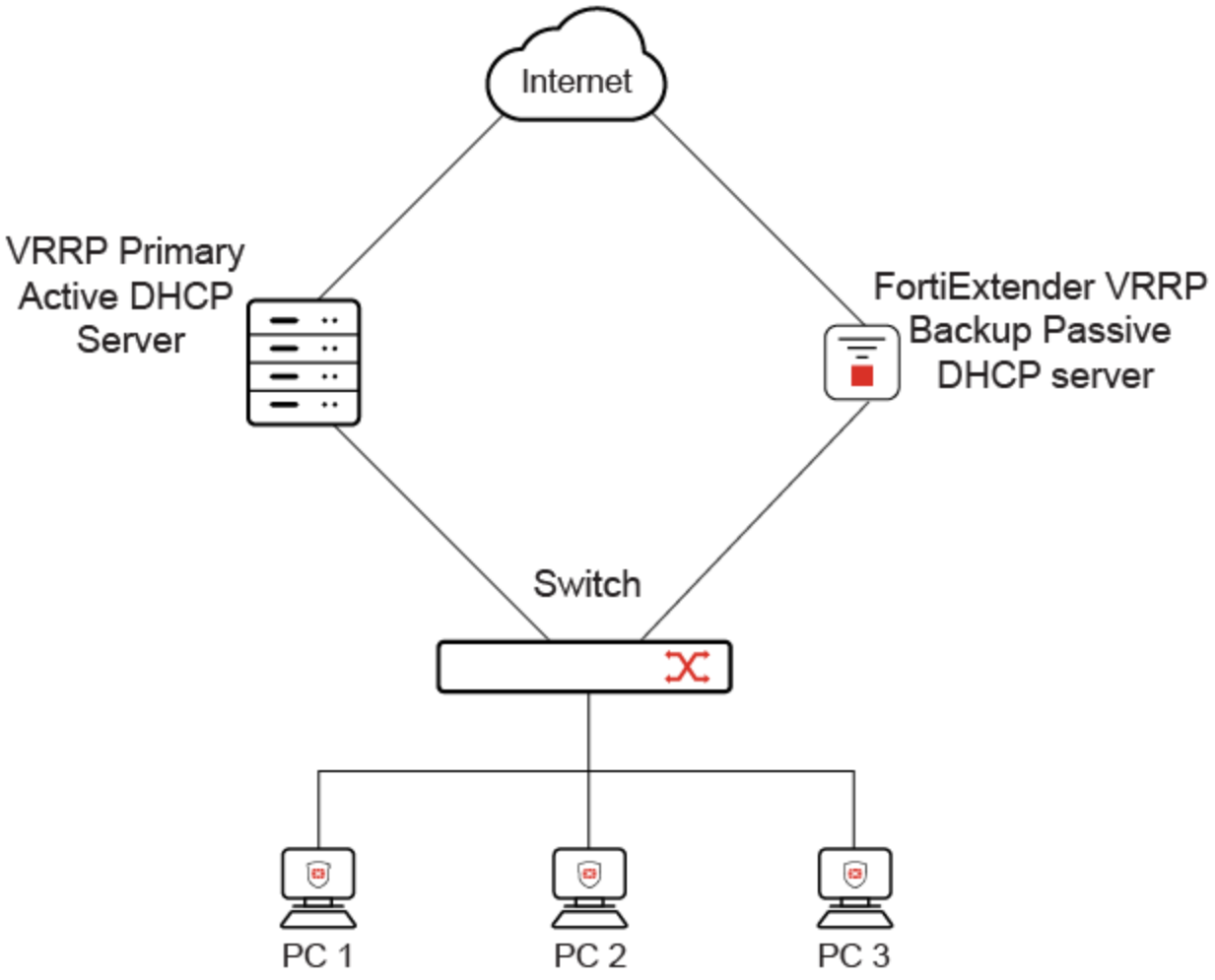
```
get router info vrrp
```

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.



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.

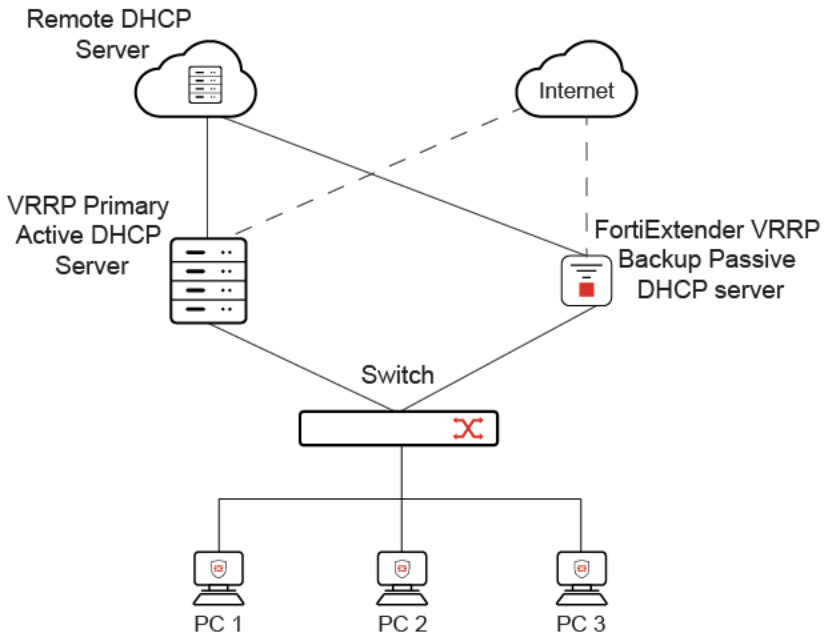
For information on DHCP relay configuration, see Configure DHCP relay.

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.



IPv6 in IP pass-through mode

FortiExtender supports IPv6 in stateless address autoconfiguration (SLAAC). This enables FortiGate to obtain the IPv6 prefix for Internet access.

To configure IPv6 in IP pass-through mode:

1. From the FortiExtender CLI, enable IPv6 in the data plan.

```
config lte plan
  edit 1
    set pdn ipv6
  next
end
```

2. From the FortiOS CLI, enable IPv6 under the FortiGate's FortiExtender interface.

```
config system interface
  edit "fex-vlan"
    set vdom "root"
    set mode dhcp
    set role wan
    config ipv6
      set dhcp6-prefix-delegation enable
      set autoconf enable
    end
    set interface "internal"
    set vlanid 123
  next
end
```

`dhcp6-prefix-delegation`	Enable/disable DHCPv6 prefix delegation. Router advertisement (RA) as upstream interface.

3. Configure the LAN to receive upstream prefixes from the WAN interface, for example, `fex-vlan`.

```
config system interface
  edit "internal"
    set vdom "root"
    set ip 192.168.1.99 255.255.255.0
    set allowaccess ping https ssh fgfm fabric
    config ipv6
      set ip6-mode delegated
      set ip6-allowaccess ping
      set ip6-send-adv enable
      set ip6-manage-flag enable
      set ip6-other-flag enable
      set ip6-upstream-interface "fex-vlan"
      set ip6-subnet ::100:0:10/96
    end
  next
end
```

`ip6-manage-flag`	Enable/disable the managed flag. Enable to force clients to use DHCPv6.
`ip6-other-flag`	Enable/disable the other DHCPv6 configuration flag.

ip6-upstream-interface	Enter the upstream interface name.
ip6-subnet	Enter the subnet to routing prefix. Append to the upstream prefix.

4. Configure the DHCPv6 server that gives unique IPv6 addresses based on upstream prefixes.

```
config system dhcp6 server
  edit 2
    set subnet ::100:0:0/96 =>
    set interface "internal"
    set upstream-interface "fex-vlan"
    set ip-mode delegated
    set dns-server1 2001:4860:4860::8888
  next
end
```

subnet	Unique id, append to upstream prefix.
upstream-interface	Upstream interface name from where delegated information is provided.
ip-mode	Method used to assign client IP. Similar to forming delegated prefixes
dns-server1	Public DNS server configuration.

5. Configure a firewall policy for IPv6 traffic.

```
config firewall policy
  edit 1
    set uuid 0f523b50-06a1-51ec-3bfc-cb547f32d1de
    set srcintf "any"
    set dstintf "any"
    set action accept
    set srcaddr6 "all"
    set dstaddr6 "all"
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

To verify your configurations are successful:

1. From the FortiGate, check the IPv6 address on the WAN interface.

```
FortiGate-60E-POE # diagnose ipv6 address list | grep fex-vlan
dev=24 devname=fex-vlan flag= scope=0 prefix=64 addr=2600:1010:b000:bf11:724c:a5ff:feff:7bff
preferred=4294967295 valid=4294967295 cstamp=144926 tstamp=144993
dev=24 devname=fex-vlan flag= scope=0 prefix=64 addr=2600:1010:b053:bcb4:724c:a5ff:feff:7bff
preferred=4294967295 valid=4294967295 cstamp=106066 tstamp=106066
dev=24 devname=fex-vlan flag=P scope=253 prefix=64 addr=fe80::724c:a5ff:feff:7bff
preferred=4294967295 valid=4294967295 cstamp=10214 tstamp=10214
```

The IPv6 address should use SLAAC with a 64-bit prefix.

2. Check the IPv6 routing table.

```
FortiGate-60E-POE # get router info6 routing-table database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, 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, B - BGP
       > - selected route, * - FIB route, p - stale info
Timers: Uptime

Routing table for VRF=0
K *> ::/0 via fe80::1e05:3dff:fe71:0, fex-vlan, 00:35:00
K * ::/0 via fe80::66be:19ff:fef3:0, fex-vlan, 00:41:28
C *> ::1/128 via ::, root, 00:57:22
C *> 2600:1010:b000:bf11::/64 via ::, fex-vlan, 00:34:58
K * 2600:1010:b000:bf11::/64 via ::, fex-vlan, 00:35:00
C *> 2600:1010:b000:bf11:0:100::/96 via ::, internal, 00:34:58
C *> 2600:1010:b053:bcb4::/64 via ::, fex-vlan, 00:35:00
K * 2600:1010:b053:bcb4::/64 via ::, fex-vlan, 00:41:28
C *> fe80::/64 via ::, fex-vlan, 00:35:00
```

3. Check the IPv6 addresses on the LAN side.

```
diagnose ipv6 address list | grep internal
dev=23 devname=internal flag=P scope=0 prefix=96 addr=2600:1010:b000:bf11:0:100:0:10
preferred=4294967295 valid=4294967295 cstamp=144995 tstamp=144995
dev=23 devname=internal flag=P scope=253 prefix=64 addr=fe80::724c:a5ff:feff:7bff
preferred=4294967295 valid=4294967295 cstamp=106089 tstamp=106089
```

4. Check that you can ping the internet over IPv6.

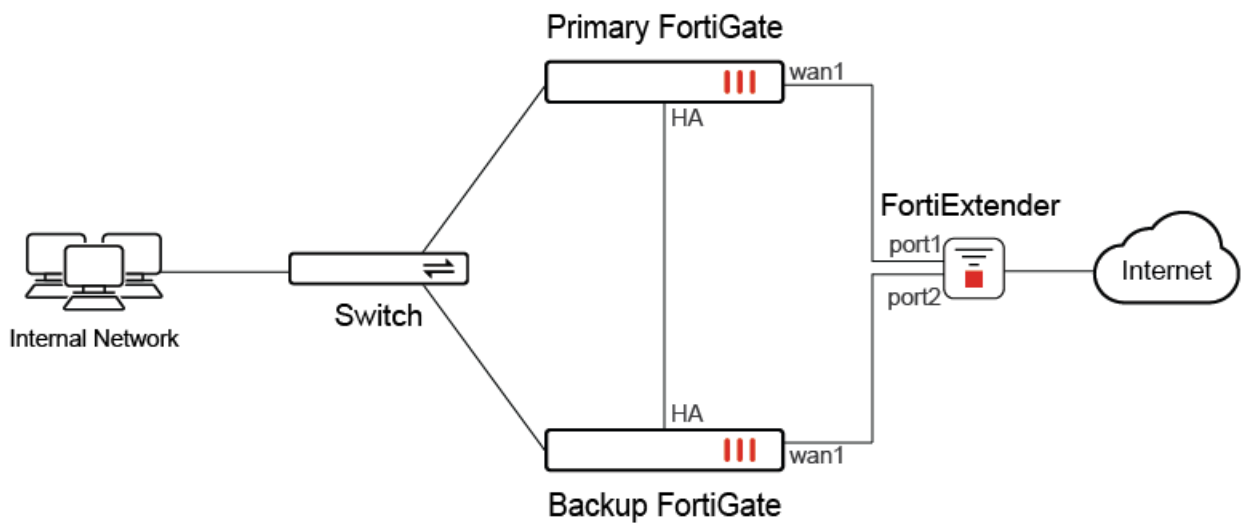
```
FortiGate-60E-POE # execute ping6 google.com
PING google.com(2607:f8b0:4005:80f::200e) 56 data bytes
64 bytes from 2607:f8b0:4005:80f::200e: icmp_seq=1 ttl=114 time=31.5 ms
64 bytes from 2607:f8b0:4005:80f::200e: icmp_seq=2 ttl=114 time=28.8 ms
64 bytes from 2607:f8b0:4005:80f::200e: icmp_seq=3 ttl=114 time=57.8 ms
64 bytes from 2607:f8b0:4005:80f::200e: icmp_seq=4 ttl=114 time=38.3 ms
64 bytes from 2607:f8b0:4005:80f::200e: icmp_seq=5 ttl=114 time=37.6 ms
```

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© 2026 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.