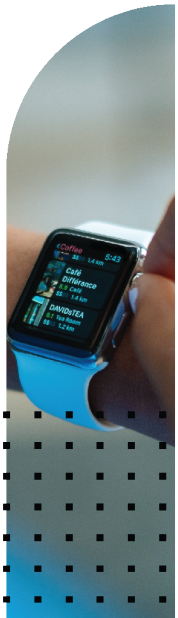
Admin Guide

FortiExtender (Managed) 7.2.0



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

October 18, 2023
FortiExtender (Managed) 7.2.0 Admin Guide

TABLE OF CONTENTS

Change Log 5
Introduction 6
FortiOS and FortiExtender OS compatibility 7
Supported hardware models 8
Before you begin 9
FortiExtender and FortiGate integration 10
FortiGate-FortiExtender zero-touch provisioning (ZTP) 11
Connect to FortiGate 11
Wireless WAN extension to WAN interfaces of FortiGate 11
Wireless extension to internal LAN interface of FortiGate 12
Authorize FortiExtender on FortiOS 12
VLAN mode and performance 13
Enable FortiExtender Controller on FortiOS 13
Support for device password and allowed protocols for FortiExtender in FortiGate. 14
FortiExtender as FortiGate LAN extension 15
Introduce LAN extension mode for FortiExtender 15
Using the backhaul IP when the FortiGate access controller is behind NAT 23
Bandwidth limits on the FortiExtender Thin Edge 30
IPAM in FortiExtender LAN extension mode 31
FortiExtender LAN extension in public cloud FGT-VM 36
Allow FortiExtender to be managed and used in a non-root VDOM 43
Discover a FortiExtender unit 48
De-authorize a discovered FortiExtender 49
The default FortiExtender profile 49
Allowaccess for FortiExtender management 52
Set bandwidth limit for LAN extension 53
Configure FortiExtender admin password 54
Discovery response lockdown 55
Wildcard 55
Data transportation over the LAN extension interface 56
LAN extension configuration in a profile 58
Backhaul IP in LAN extension 60
Manage dual FortiExtender devices 61
Active/Passive mode 61
Active/Active mode 61
Cellular as backup of Ethernet WAN 61
SD-WAN 61
Configure cellular settings 63
Create a data plan 63
Set the default SIM 65
Enable SIM-switch 66
Report to FortiGate 67
Capwap mode 67

VLAN mode 68
CAPWAP on multiple ports for broadcast discovery 69
Check current manage mode 70
Get modem status 71
Stopping data traffic on overaged LTE interface 72
Use cases 73
Redundant with FGT in IP Pass-through mode 73
Enable DHCP server on FortiExtender and the VRRP primary router 75
Enable DHCP relay on both FortiExtender and the VRRP primary router 76
FortiExtender for FortiGate HA configuration 78
Network topology 79
Prerequisites 79
Configuration procedures 79

Change Log

Date	Change Description
October 18, 2023	Updated FortiExtender for FortiGate HA configuration on page 78.
April 18, 2022	Added Allow FortiExtender to be managed and used in a non-root VDOM on page 43.
April 11, 2022	Initial release.

Introduction

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

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

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

FortiOS and FortiExtender OS compatibility

FortiExtender (Managed) 7.2.0 supports FortiOS 6.2.x, 6.4.x, and 7.0.x. For more information about compatibility between versions of FortiOS and FortiExtender OS, see FortiOS & FortiExtender OS Compatibility Matrix.

Supported hardware models

FortiExtender OS 7.2.0 supports the following FortiExtender hardware models:

Model	Market
FortiExtender 511F	Global
FortiExtender 311F	Global
FortiExtender 212F	Global
FortiExtender 200F	Global
FortiExtender 101F-EA	EMEA, Brazil, and parts of APAC
FortiExtender 101F-AM	North America
FortiExtender 211E	Global
FortiExtender 201E	North and South Americas, EMEA, and parts of APAC

For more information about FortiExtender OS and hardware compatibility, see FortiExtender OS & Hardware Platform Compatibility Matrix.

All FortiExtender units come with a Bluetooth button, which is off by default. Bluetooth discovery will be active for 90 seconds after you press and hold the Bluetooth button for more than three seconds. Once connected, as an example, from the FortiExplorer app, you can access the devices via Bluetooth. As a good security practice, we strongly recommend setting your own password before deploying FortiExtender in your environment.

Before you begin

Before you start to configure your FortiGate-managed FortiExtender unit, we assume:

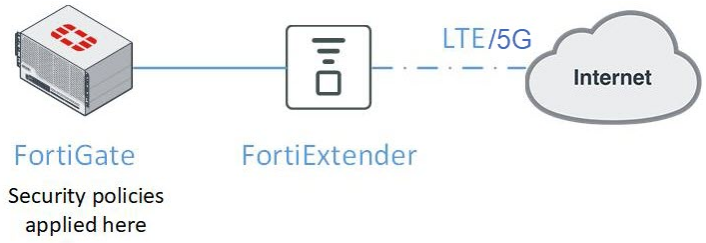
- You have completed the installation of the FortiExtender unit, as outlined in the QuickStart Guide. (**Note:** You can power the FortiExtender unit using an external power adapter or by POE when connected to the POE/PSE port of the FortiGate.)
- You have administrative access to the FortiExtender GUI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

FortiExtender and FortiGate integration

FortiExtender works as an extended WAN interface in IP pass-through mode.

The following paragraphs highlight the network topology for integrating FortiExtender with FortiGate.

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



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

The FortiExtender and the FortiGate share the same LTE IP in WAN-extension mode. In pre-4.2.2 releases, FortiExtender does not allow access to SSH/HTTPS/HTTP/Telnet service via the LTE interface, so all the traffic to those default services goes to FortiGate. FortiExtender 4.2.2 adds local SSH/HTTPS/HTTP/Telnet service support via the LTE interface. To distinguish local services from FortiGate services, you must configure the FortiExtender to use different ports. Otherwise, all traffic to these default services will be sent to the

FortiExtender locally instead of FortiGate.

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

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

FortiGate-FortiExtender zero-touch provisioning (ZTP)

FortiExtender 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:

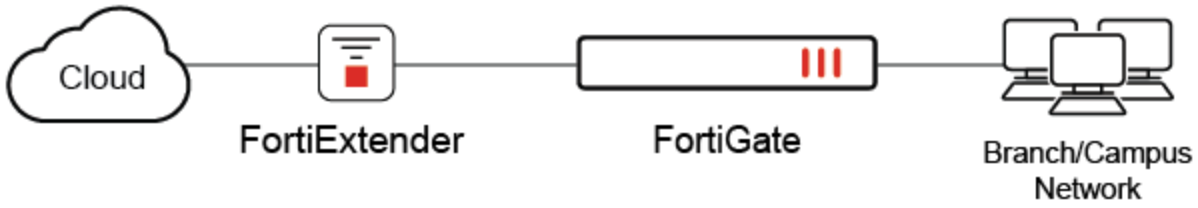
1. A SIM card without a PIN code is expected to be used for ZTP, and the default APN should be retrieved automatically at first connection.
2. Acting as a DHCP client, the FortiGate connects to the FortiExtender LAN port (1, 2, or 3) interface to obtain a private IP to reach FortiManager.
3. The FortiGate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

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:

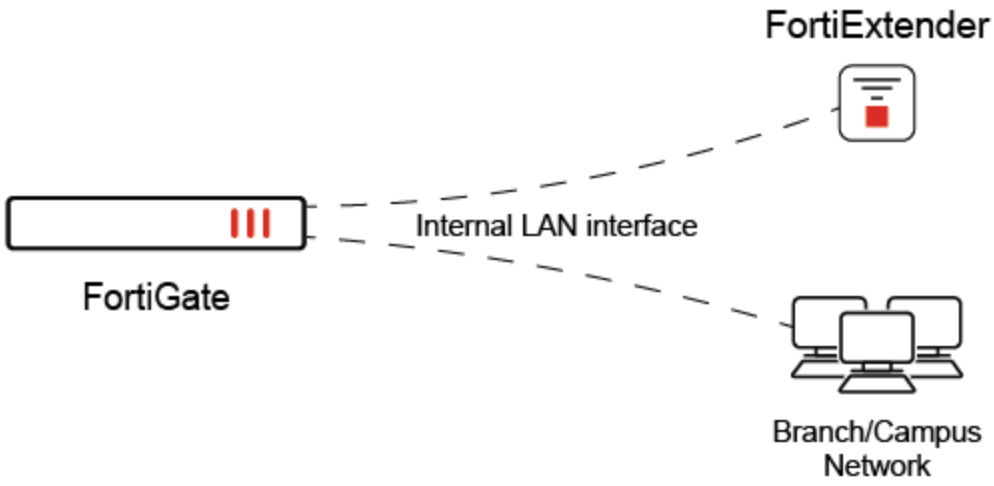
- Connect the FortiGate port (such as WAN1/WAN2) in DHCP client mode to a FortiExtender LAN port (1—3). In this option, the FortiGate interface acquires DHCP lease from the FortiExtender LAN DHCP server, and has a default gateway as the FortiExtender LAN interface IP address.
- If the FortiGate internal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



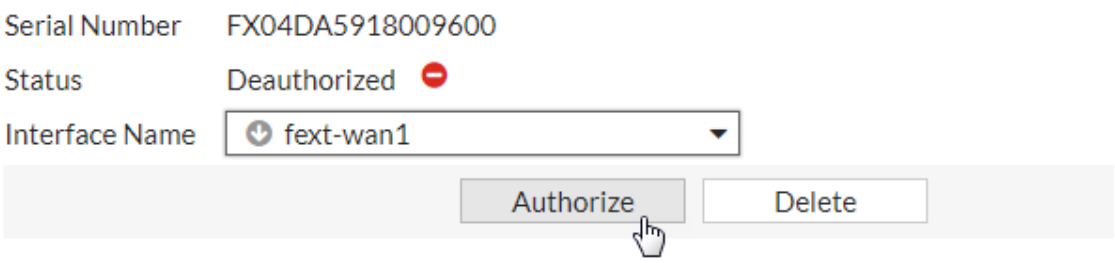
In some scenarios, you may want to connect the FortiExtender to an internal LAN interface of the FortiGate (to use POE power or some other means). In this case, if the FortiGate internal LAN is running a DHCP server, connect the FortiGate to port4 of the FortiExtender (FEX-201E/211E) which acquires DHCP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

VLAN mode and performance

For FortiGate to FortiExtender connectivity, alternate VLAN mode is supported. It is an alternative for the default CAPWAP mode. While using 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 with a switch. In case of a switch in between, the switch should be configured to allow the configured VLANs.

VLAN mode must be explicitly enabled, as it is disabled by default on FortiGate, and that all the FEX-WAN interfaces must be deleted before VLAN mode is enabled.

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

Ensure that the VLAN interface is created based on the physical interface of your connected FortiExtender.

Enable FortiExtender Controller on FortiOS

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

1. Enable the FortiExtender Controller on the FortiGate.

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

2. Make sure that your FortiGate enables FortiExtender Controller.
   The FortiExtender-related GUI is enabled by default.
3. Enable the CAPWAP access to use the FortiGate interface to which the FortiExtender is connected.

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

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

Support for device password and allowed protocols for FortiExtender in FortiGate.

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

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

```
FX201E5919000027 # config system management fortigate
    FX201E5919000027 (fortigate) # show
    config system management fortigate
        set ac-discovery-type broadcast
        set ac-ctl-port 5246
        set ac-data-port 25246
        set discovery-intf lan
        set ingress-intf lan <=== The value cannot be edited and unset
    end
```

For a FortiExtender configured as LAN extension of a FortiGate, the ingress interface is "`le-switch`", whose allowaccess will be changed as the configuration from the FortiGate. In the following example, the "`le-switch`" is a predefined switch interface which will be automatically generated by the system when the FortiExtender is

managed by the FortiGate. The entry "`le-switch`" under "`config system switch-interface`" is read-only and cannot be edited or deleted.

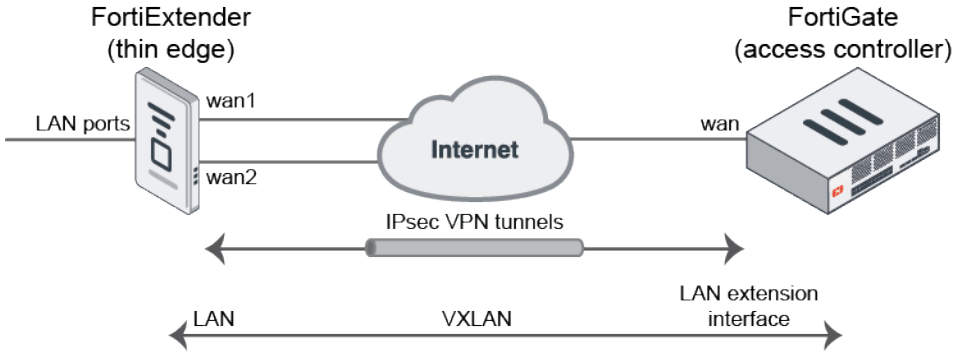
```
config system switch-interface
      edit le-switch <=== The entry cannot be edited or deleted
            set members le-agg-link lan
            set stp disable
      next
end
```

FortiExtender as FortiGate LAN extension

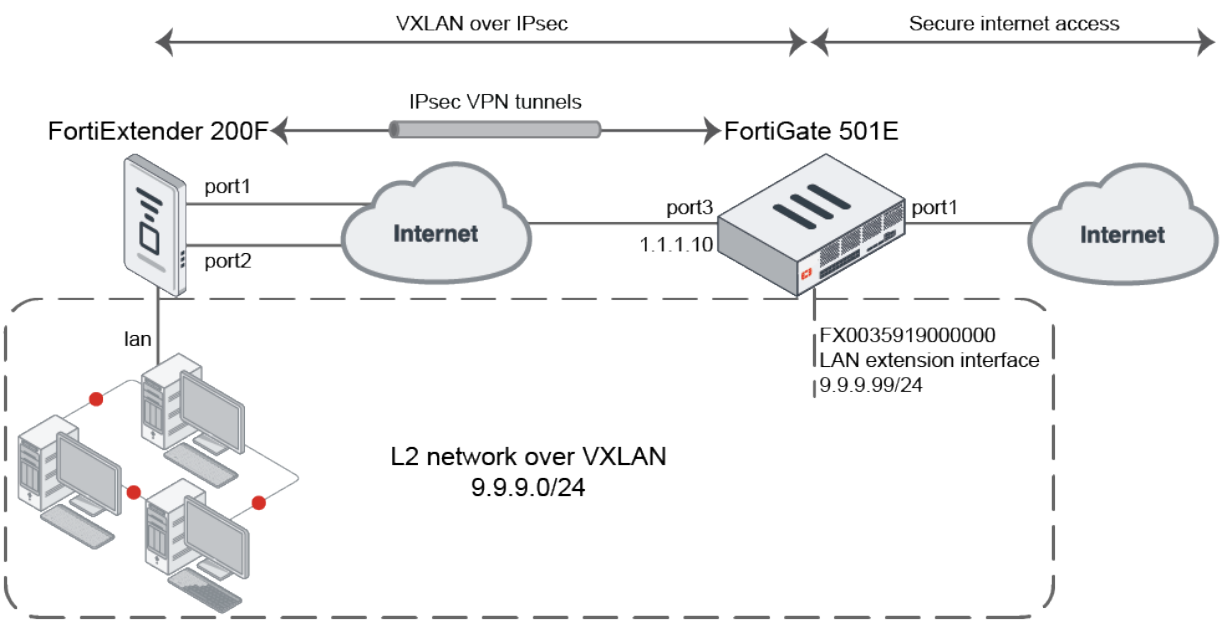
This section discusses how to configure FortiExtender as the LAN extension interface of FortiGate.

Introduce LAN extension mode for FortiExtender

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



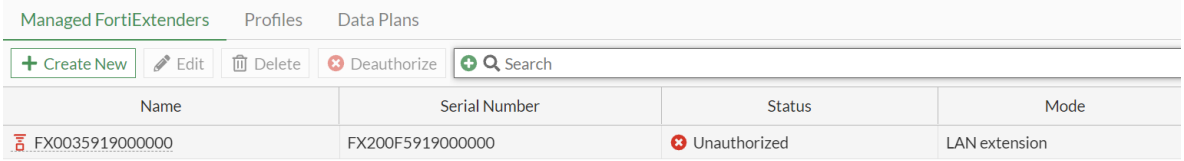
Authorizing the devices

To discover and authorize the FortiExtender in the GUI:

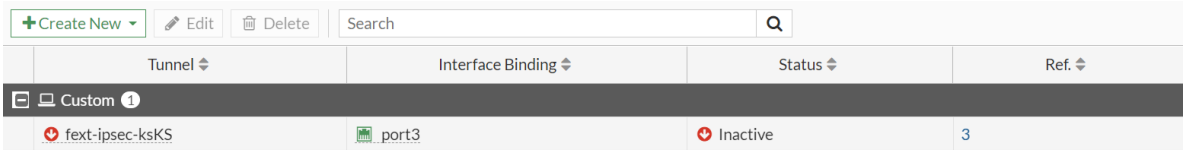
1. On the FortiGate, enable the Security Fabric connection on port3 to allow the FortiExtender to connect over CAPWAP:
   a. Go to *Network* > *Interfaces* and edit port3.
   b. In the *Administrative Access* section, select *PING* and *Security Fabric Connection*.
   c. Click *OK*.
2. On the FortiExtender,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

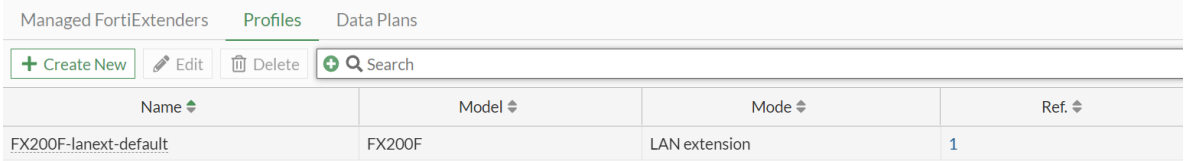
   Once the FortiExtender's discovery packet reaches port3 on the FortiGate, the FortiExtender will appear under *Network* > *FortiExtenders* as unauthorized.



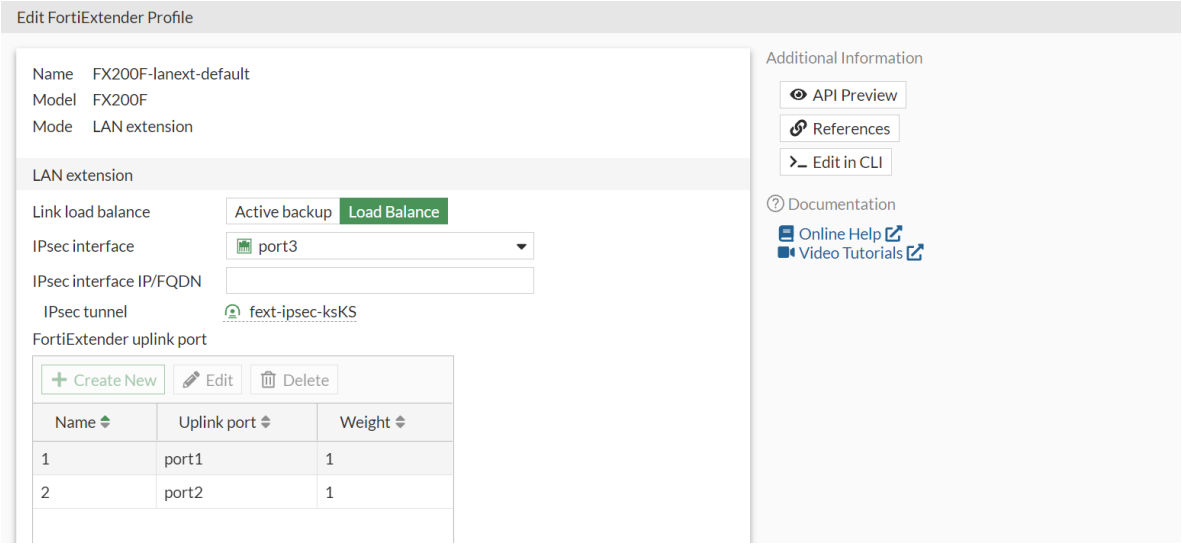
The FortiGate automatically creates a VPN profile for this FortiExtender, which appears on the *VPN* > *IPsec Tunnels* page.



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

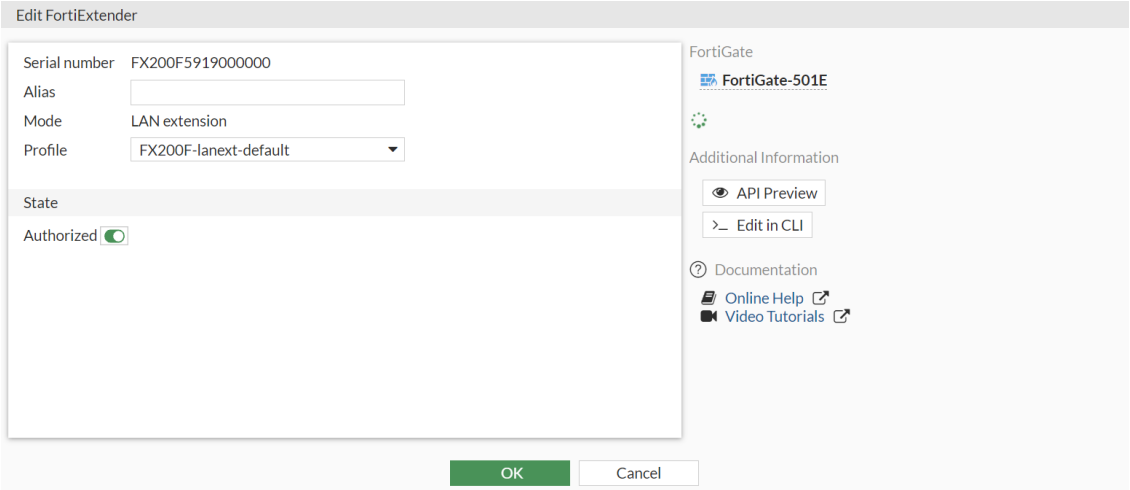


The FortiExtender profile is configured based on the FortiExtender model. It automatically selects *Load Balance* (as the *Link load balance* setting), the IPsec interface, and the pre-configured tunnel.

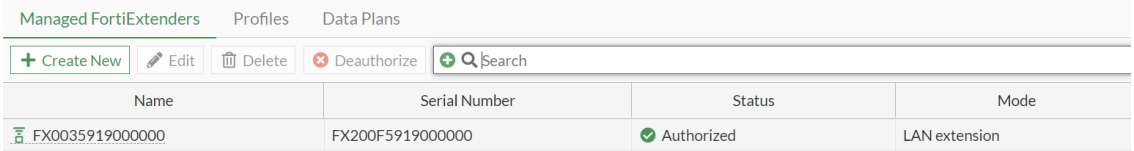


3. Authorize the FortiExtender:
   a. Go to *Network* > *FortiExtenders*, select the *Managed FortiExtenders* tab, and edit the discovered FortiExtender.

b. In the *Status* section, enable *Authorized*.



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



To discover and authorize the FortiExtender in the 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 extender-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 extender-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
```

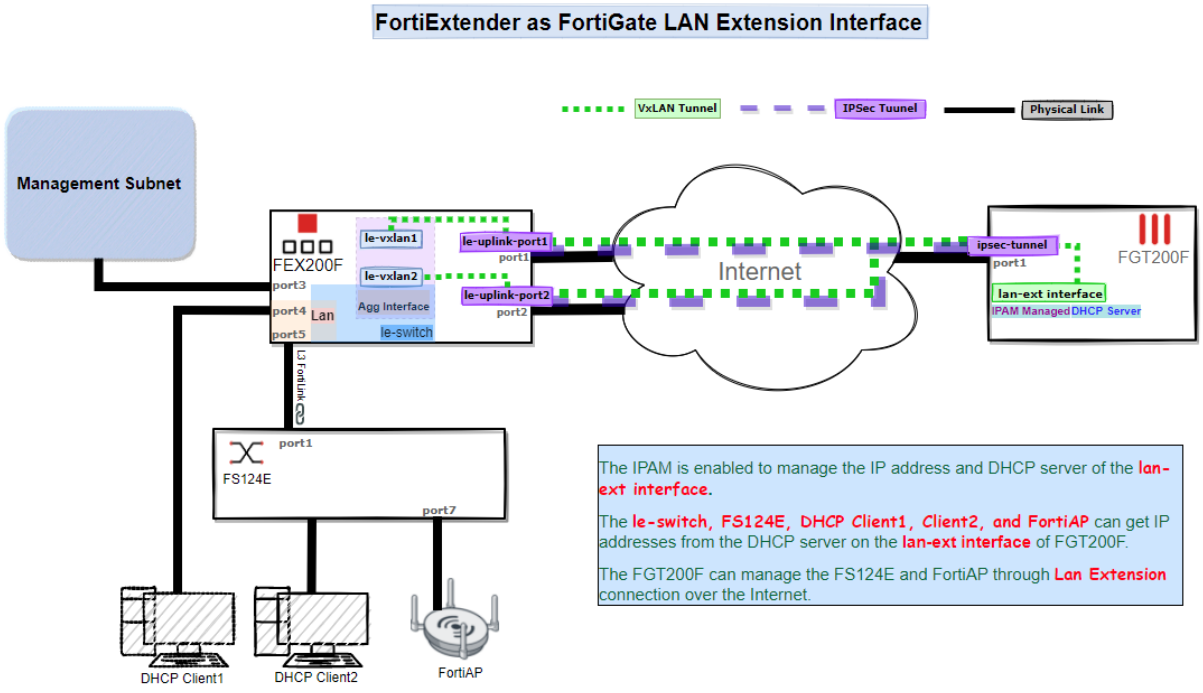
6. Authorize the FortiExtender:

```
config extender-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:

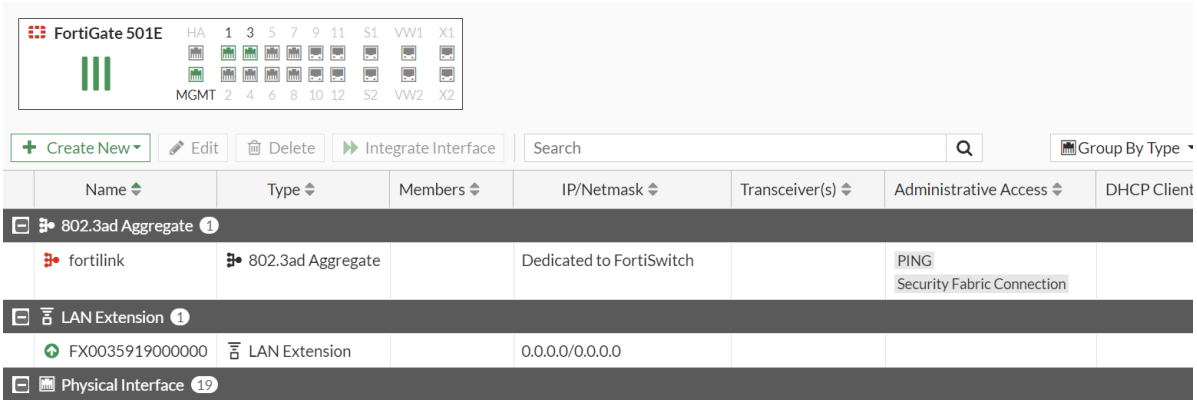
```
config system aggregate-interface
    edit le-agg-link
        set mode loadbalance
        set mapping-timeout 60
        config members
            edit le-vxlan-port1
                set interface le-vxlan-port1
                set weight 1
                set health-check-event le-agg-port1
                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.

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.

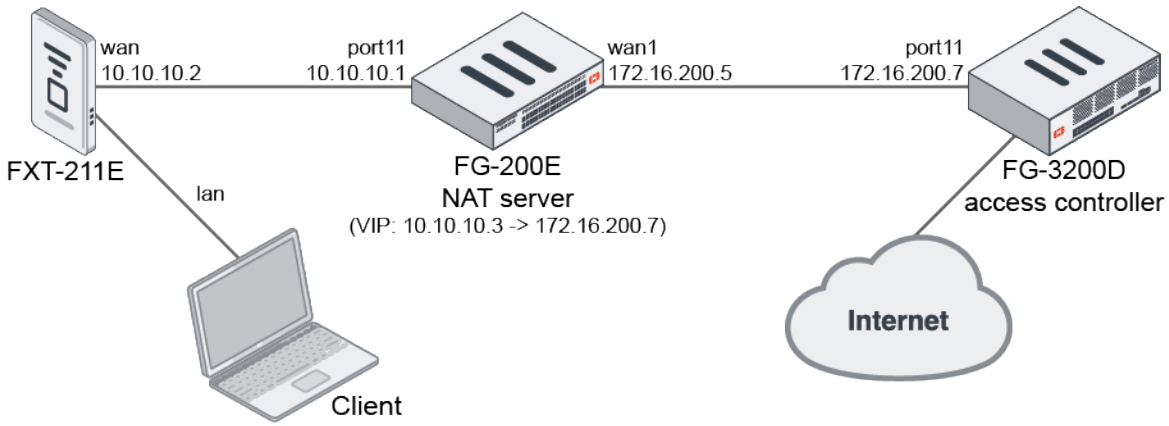
When the default IKE port 500 is inaccessible, you can configure a custom IKE port on the FortiExtender and the FortiGate.

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

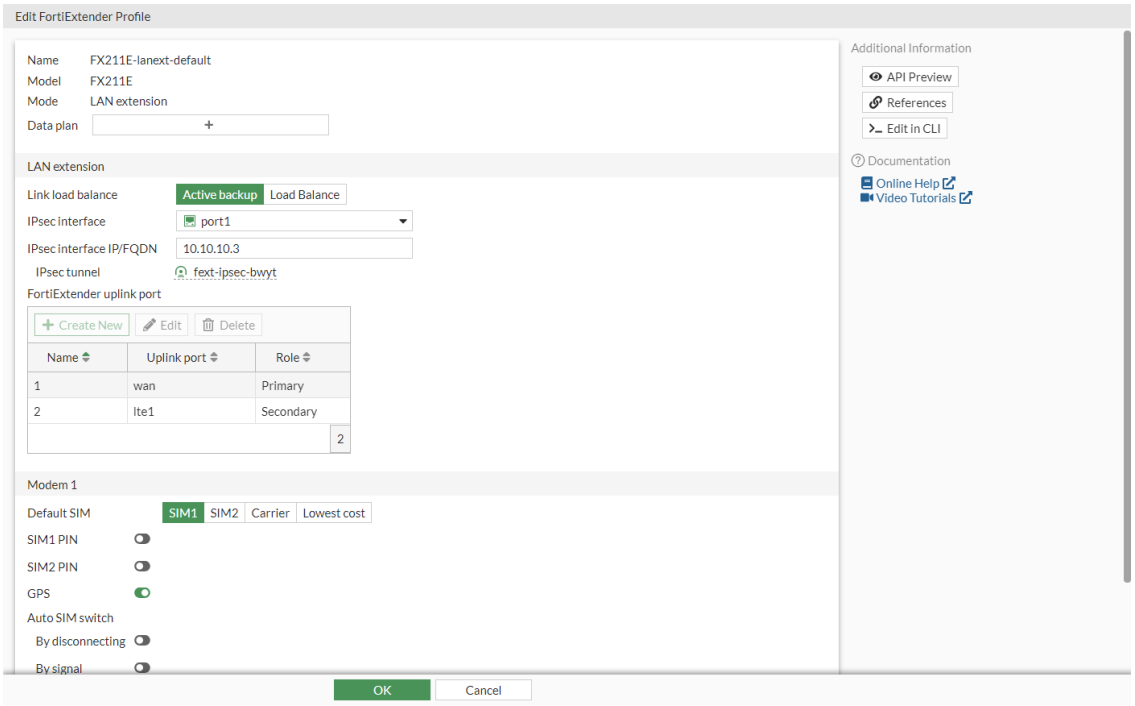
The following topology is used for the first three examples and assumes that the FortiExtender has already been discovered (see Introduce LAN extension mode for FortiExtender on page 15 for more information).



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

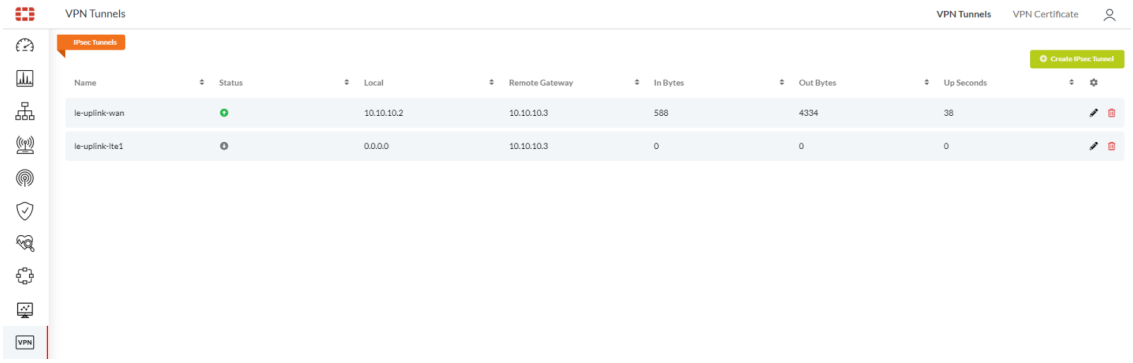
To configure an IP as a backhaul address in the GUI:

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 extender-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
```

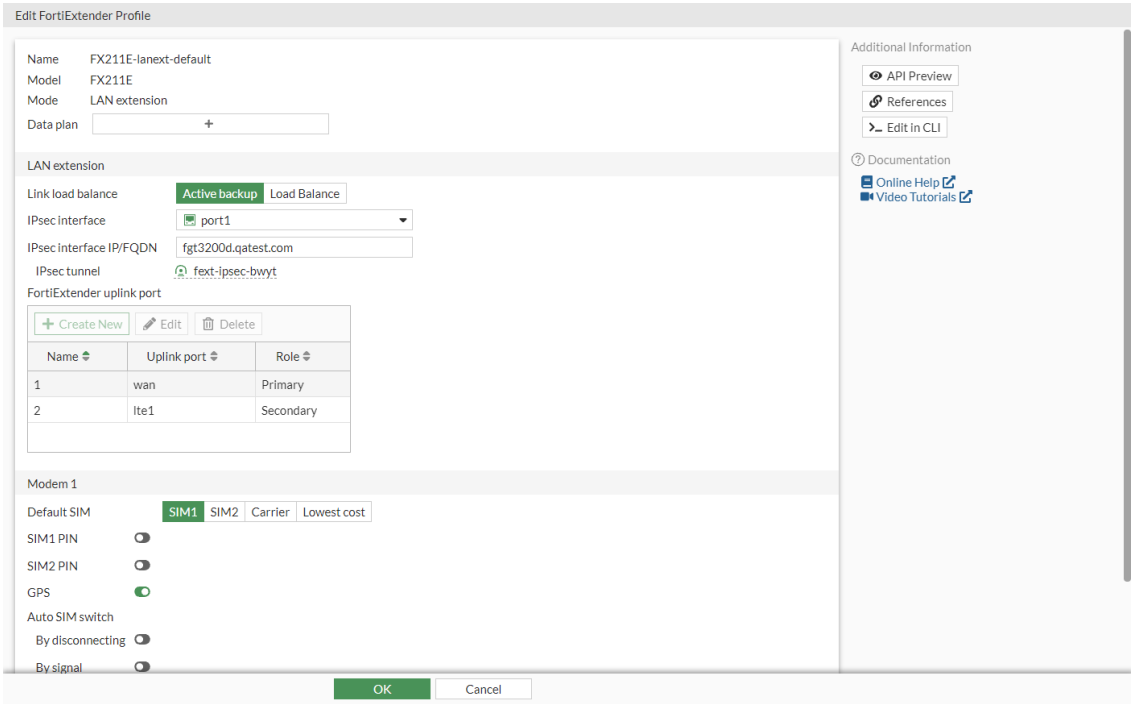
2. Verify the configuration in FortiExtender:

```
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

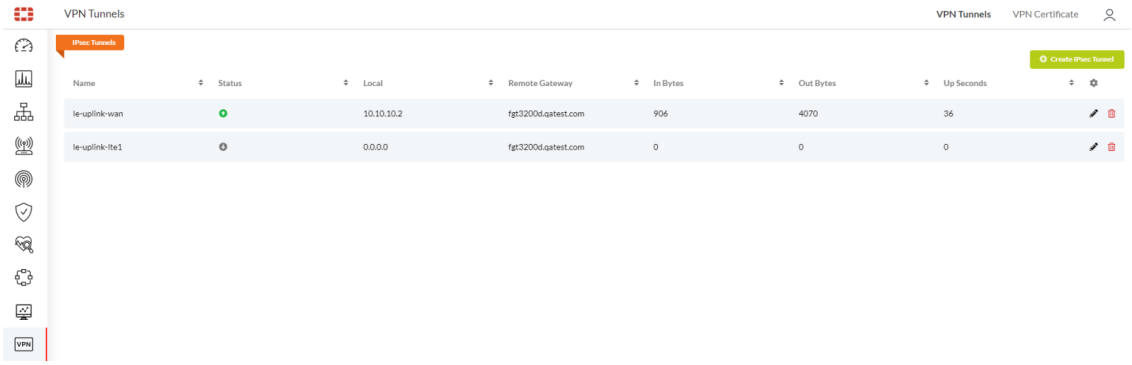
To configure an FQDN as a backhaul address in the GUI:

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 extender-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
```

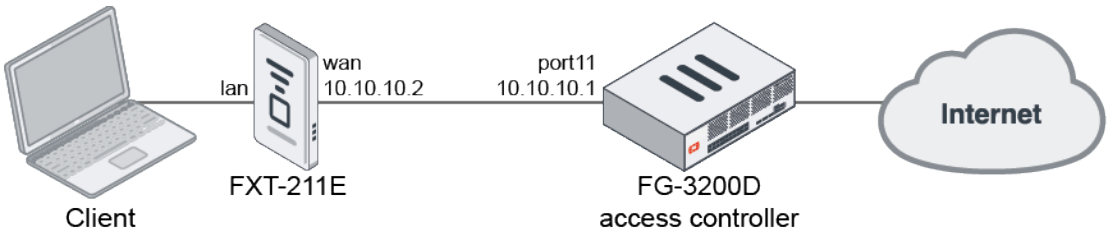
6. Verify the IPsec tunnel status on the FortiExtender to confirm that Port 4500 is used:

```
~ # 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 extender-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 extender-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
```

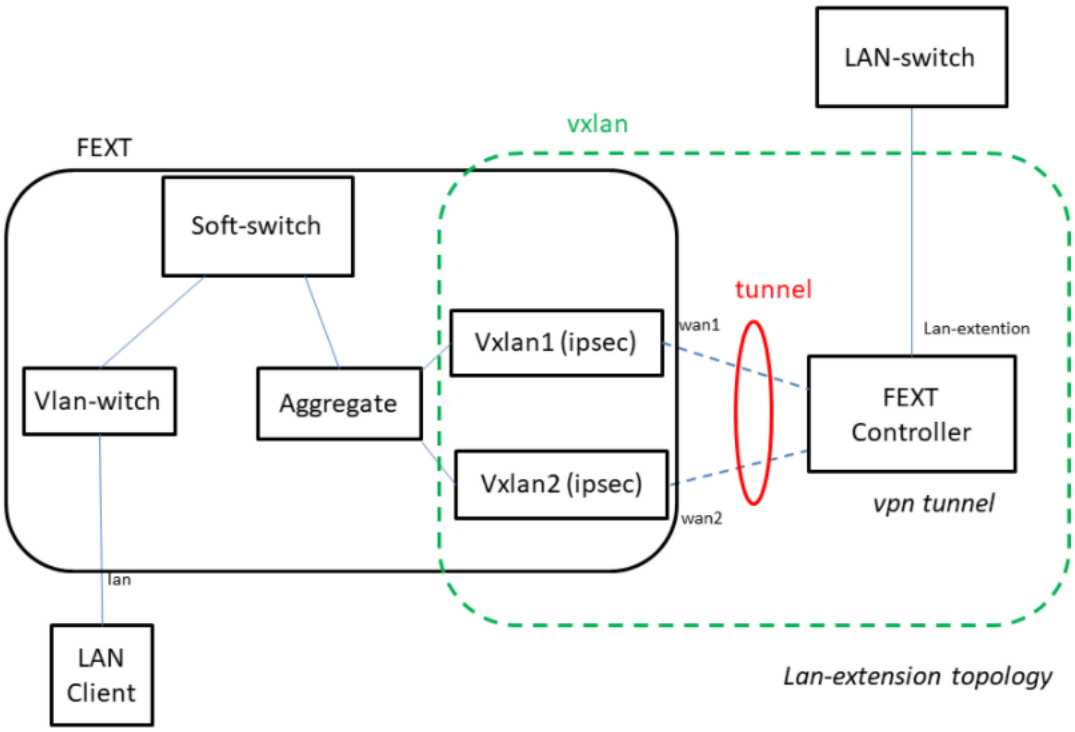
If bandwidth enforcement is disabled on the FortiGate, the configuration that was pushed to the FortiExtender will be removed.

IPAM in FortiExtender LAN extension mode

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

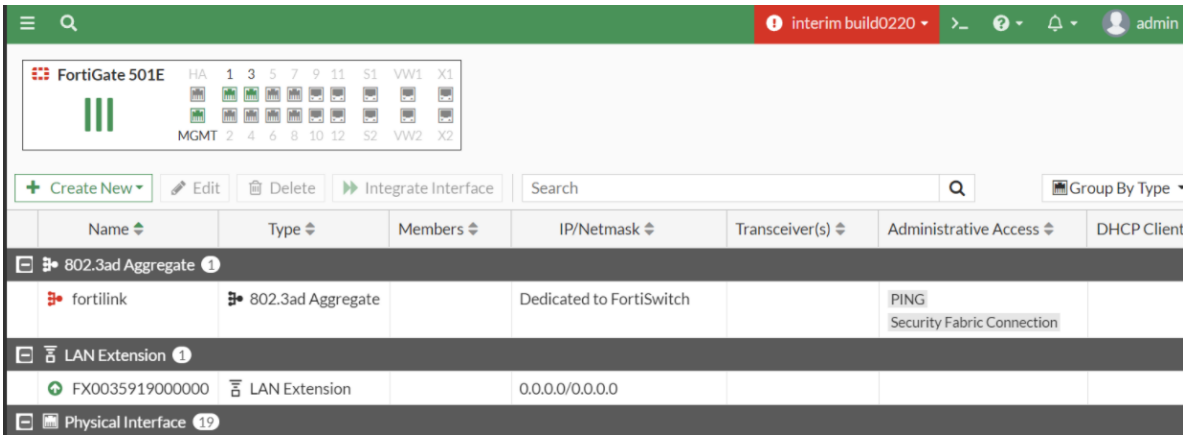
The LAN client connecting to the FortiExtender LAN interface will get DHCP allocation from the lan-extension interface. It can then reach the Internet via the firewall policy in the FortiExtender controller.

Topology

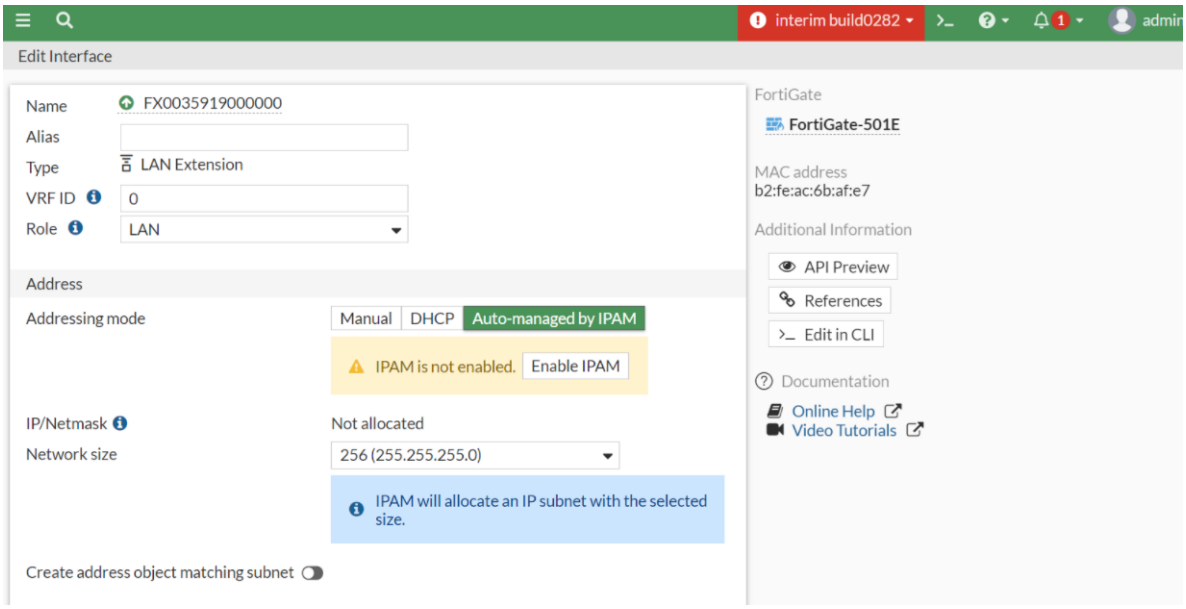


To configure IPAM in the FortiExtender lan-extension interface in the GUI:

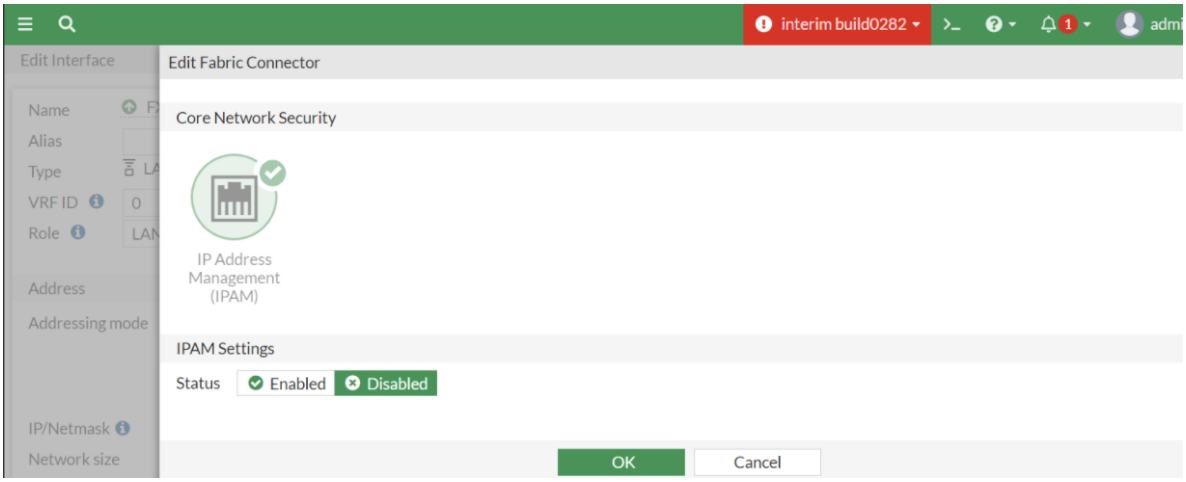
1. On the FortiGate device, go to *Interfaces.* You will see that the LAN extension interface has already been created in the FortiExtender controller.



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.*

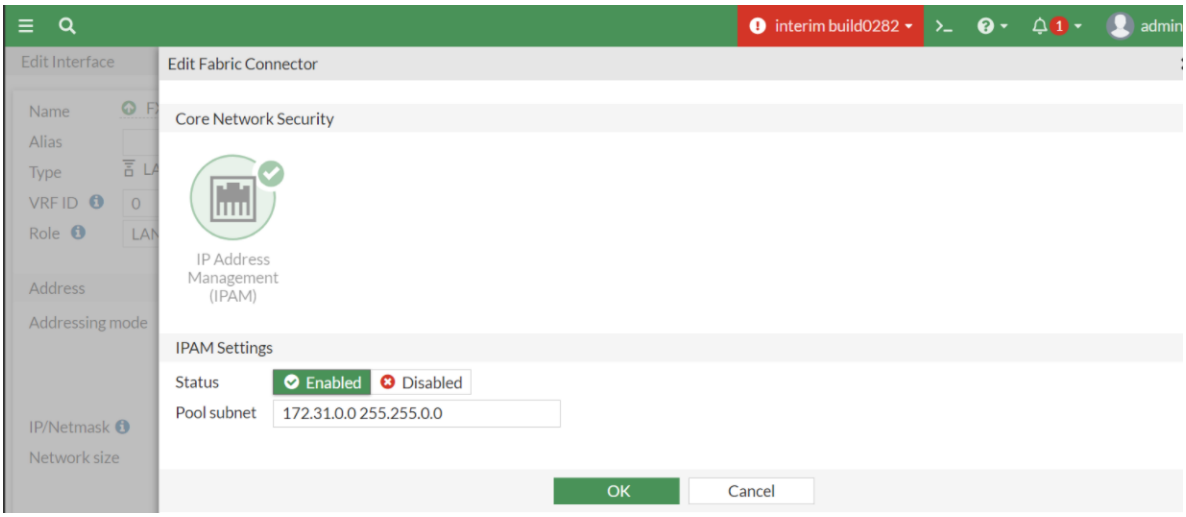


4. For *IPAM Settings* > *Status*, select *Enable* and then *OK*. The IP pool now is selected for FX0035919000000.

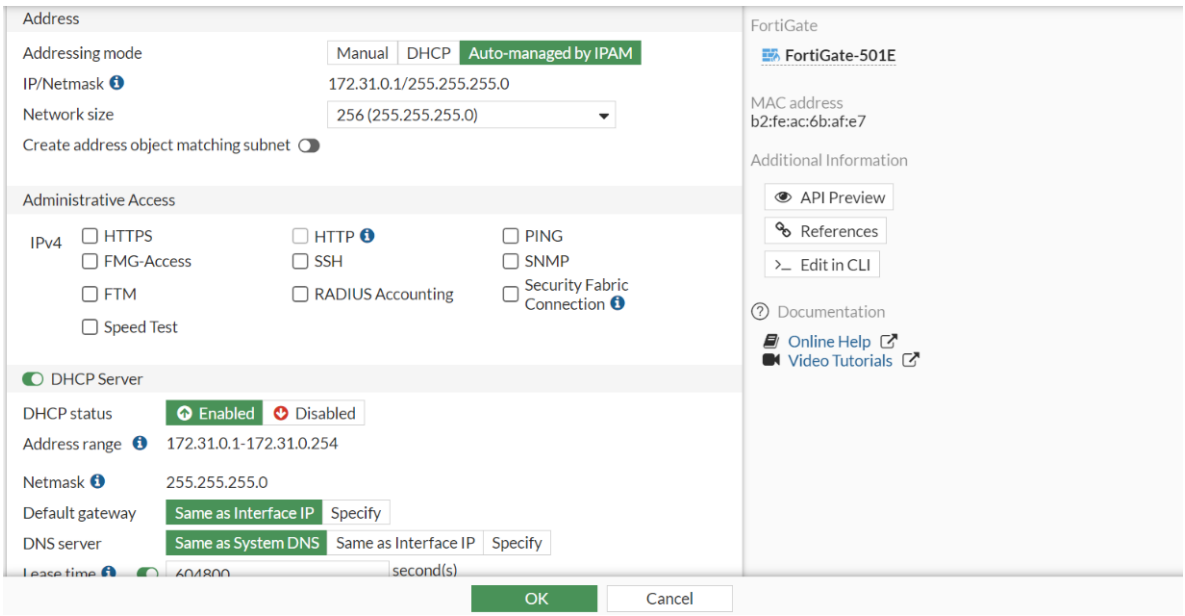


The subnet configured above is for a standalone device.

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

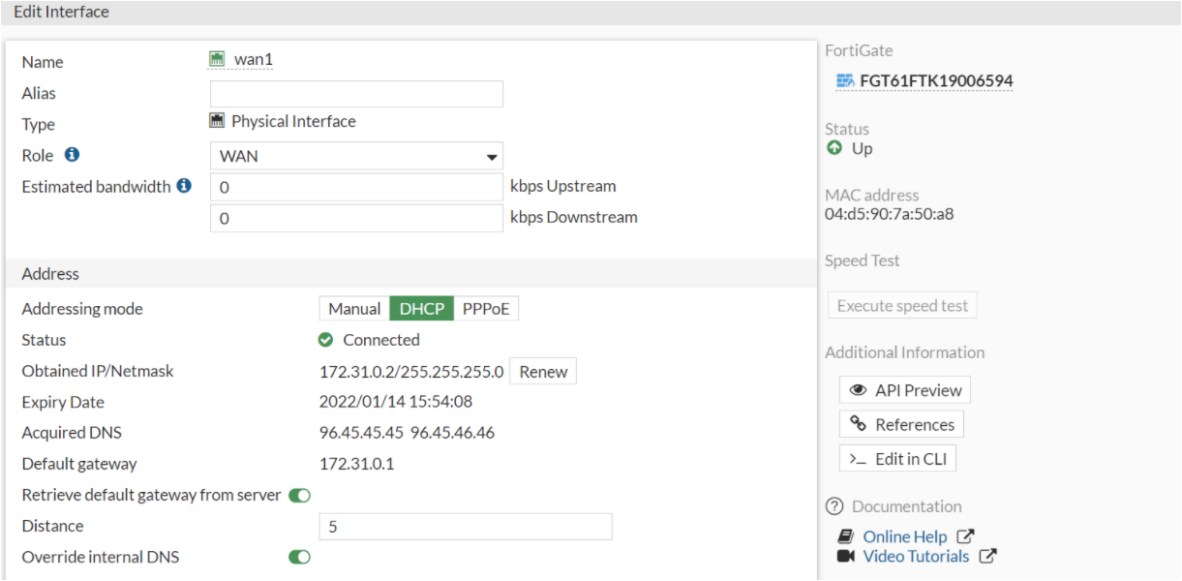


The IP and DHCP server on FX0035919000000 will be set accordingly.



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
```

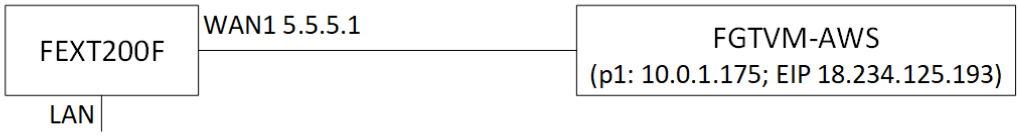
```
        end
        set interface "fext-ipsec-wiUx"
    next
end

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 FGT-VM

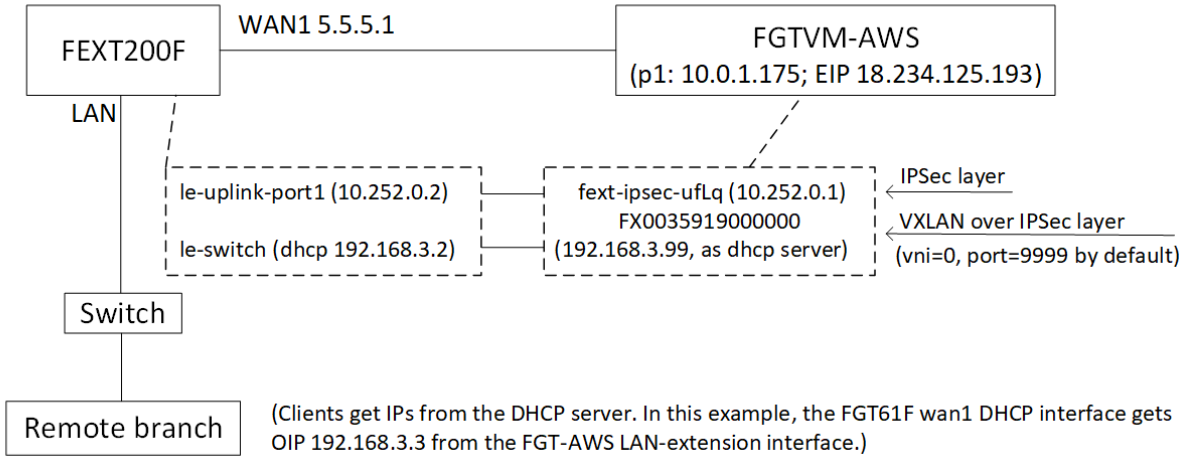
The FortiExtender LAN extension feature allows a FortiGate to extend its LAN functionality to a remote FortiExtender. In this enhancement, the FortiExtender LAN extension is added to the FGT-VM running on Public Clouds.

Topology in demo configuration:

Before LAN extension



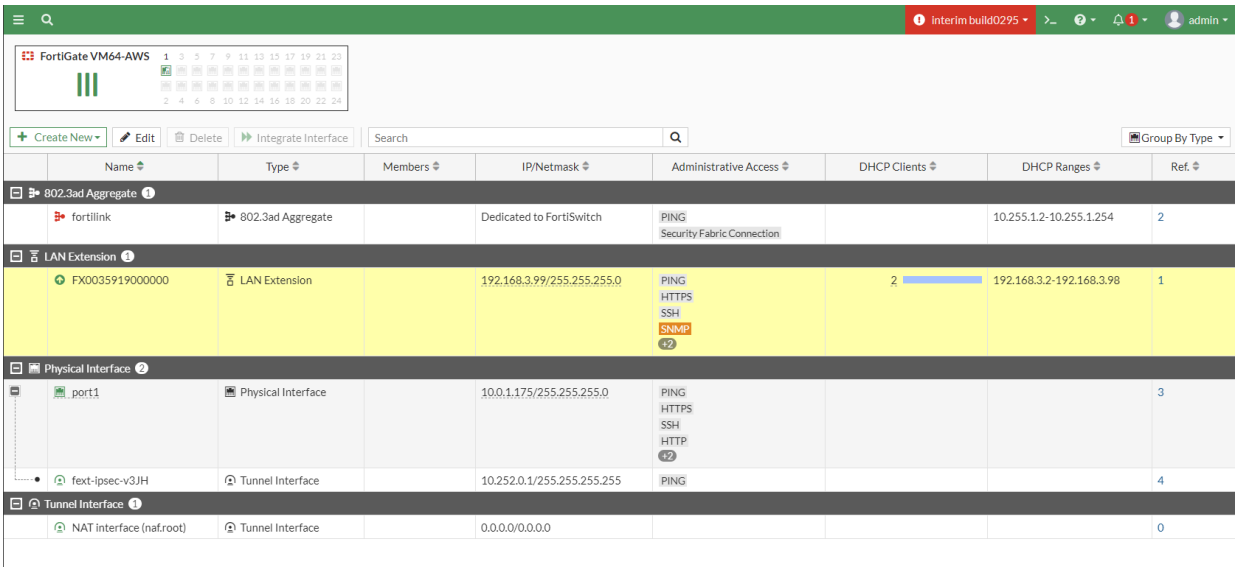
After LAN extension



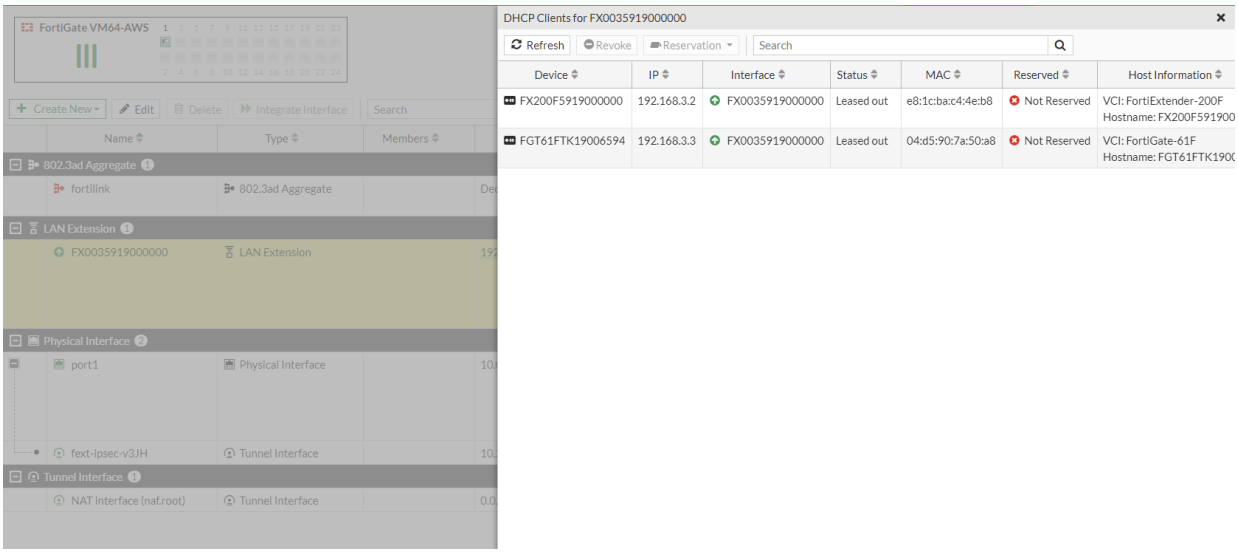
Note:
In this demo, the FEXT200F LAN interface includes port4 and port5, which are members of the le-switch. After the FEXT and the FGTVM connect successfully, the FGTVM is able to extend LAN to the remote branch on the FEXT LAN interface via VXLAN.

GUI

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



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



CLI

Step 1: Configure the FortiExtender:

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

   FX200F5919000000 # execute ping 18.234.125.193
   PING 18.234.125.193 (18.234.125.193): 56 data bytes
```

```
    64 bytes from 18.234.125.193: seq=0 ttl=233 time=68.132 ms

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

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

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

Step 2: Configure the FGT-AWS:

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

```
        edit "port1"
            set allowaccess ping https ssh http fgfm fabric
        next
    end
    config extender-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 extender-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 extender-controller extender
        edit "FX0035919000000"
            set authorized enable
        next
    end
```

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

```
FGT-AWS-EXT # sh vpn ipsec phase1-interface
            config vpn ipsec phase1-interface
                edit "fext-ipsec-v3JH"
                    set type dynamic
                    set interface "port1"
                    set ike-version 2
                    set peertype one
                    set net-device disable
                    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
                    set localid "localid-
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/TBq6dXlzeXymkw8cyoizM2a8SeyWao2sGnLCkqqkHItruVfy7
jy10dMp6AzaFlnxP6f9k8hTEBKxqUOS3+ccvSLFWvM7ouuaWgA6Hdu4StWsBVMc85tBFe+H6PTnVpRFaRCYQE
0yatuM9tcWQXCilsuv66HlAYvGlw==
                    set dpd-retryinterval 60
                next
            end

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

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

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

            total fdb num: 3
```

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

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

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

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



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

***** Remote branch PC behind FEXT lan interface is able to get the ip from FGT-AWS
vxlan interface dhcp server.
In this demo, a FGT61F acts as a PC behind FEXT, this FGT61 wan1 interface is the
same switch as FEXT lan interface port4.
Set FGT61 wan1 interface as dhcp client, it can get ip address (in this demo it's
192.168.3.3) from FGT-AWS lan-extension interface.

FGT61FTK19006594 # show system interface wan1
config system interface
    edit "wan1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh snmp
        set type physical
        set role wan
        set snmp-index 1
```

```
    next
end


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

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

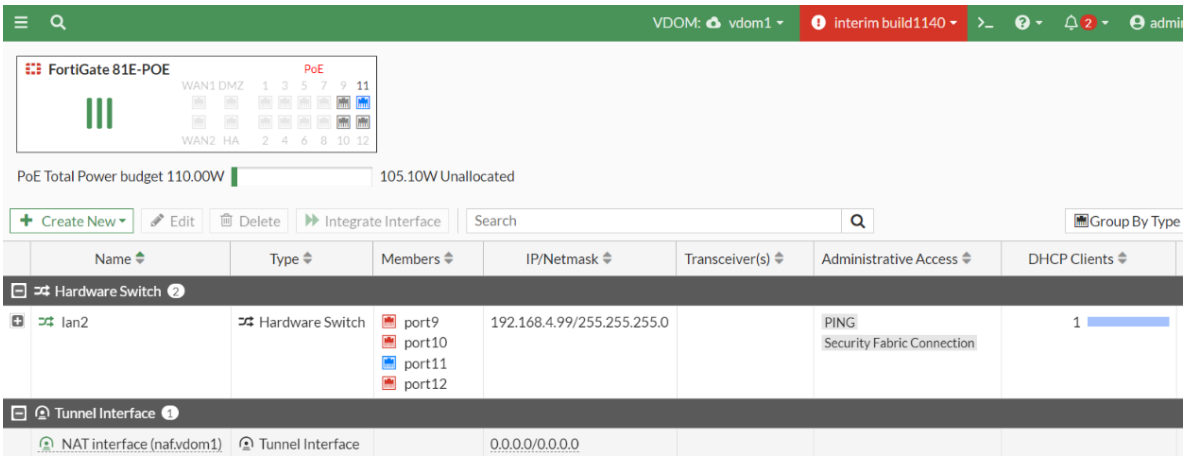
```
FGT-AWS-EXT # exec ping 192.168.3.3
PING 192.168.3.3 (192.168.3.3): 56 data bytes
64 bytes from 192.168.3.3: icmp_seq=0 ttl=255 time=68.9 ms
64 bytes from 192.168.3.3: icmp_seq=1 ttl=255 time=68.6 ms

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

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

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

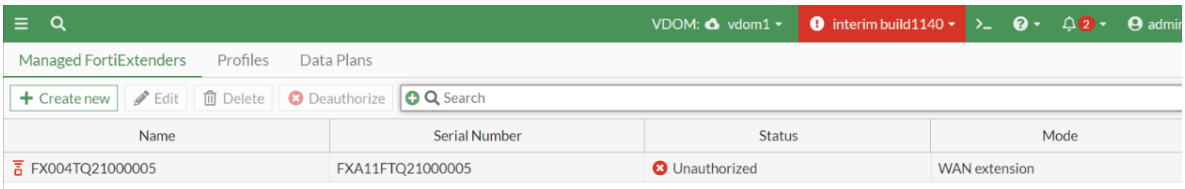
GUI operating procedures

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



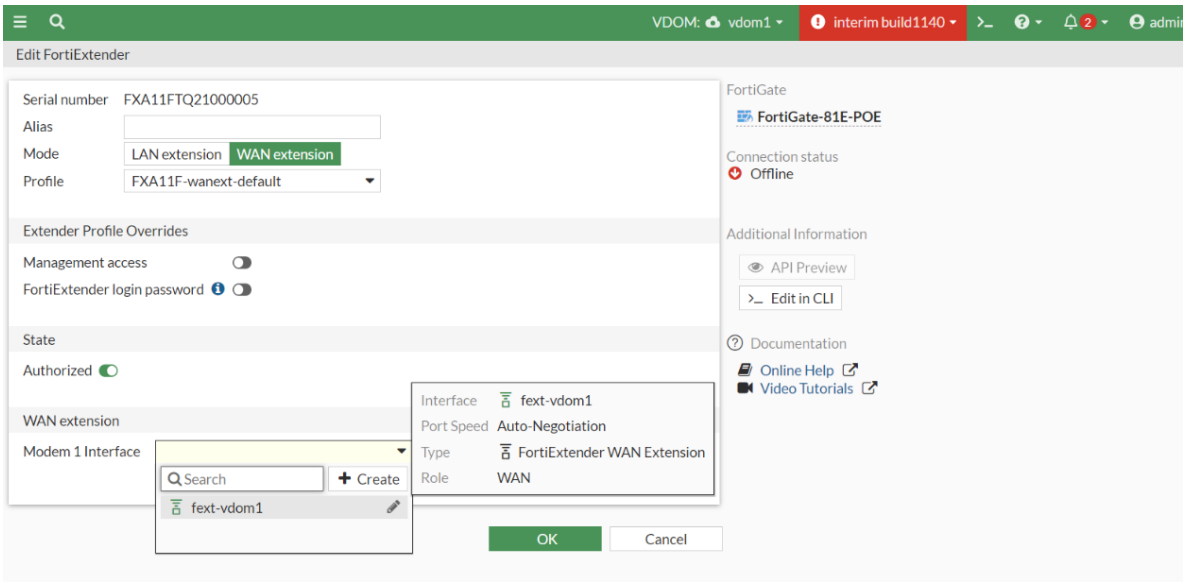
2. The FortiExtender can be discovered in the VDOM.

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

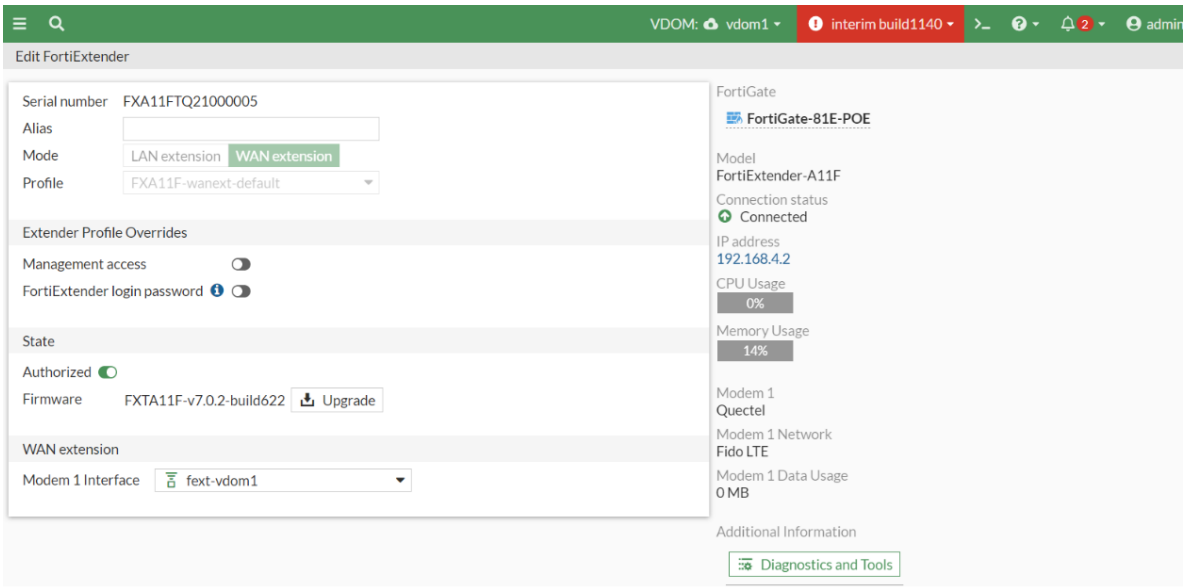


3. After it is authorized, the FortiExtender can provide an interface to the VDOM.

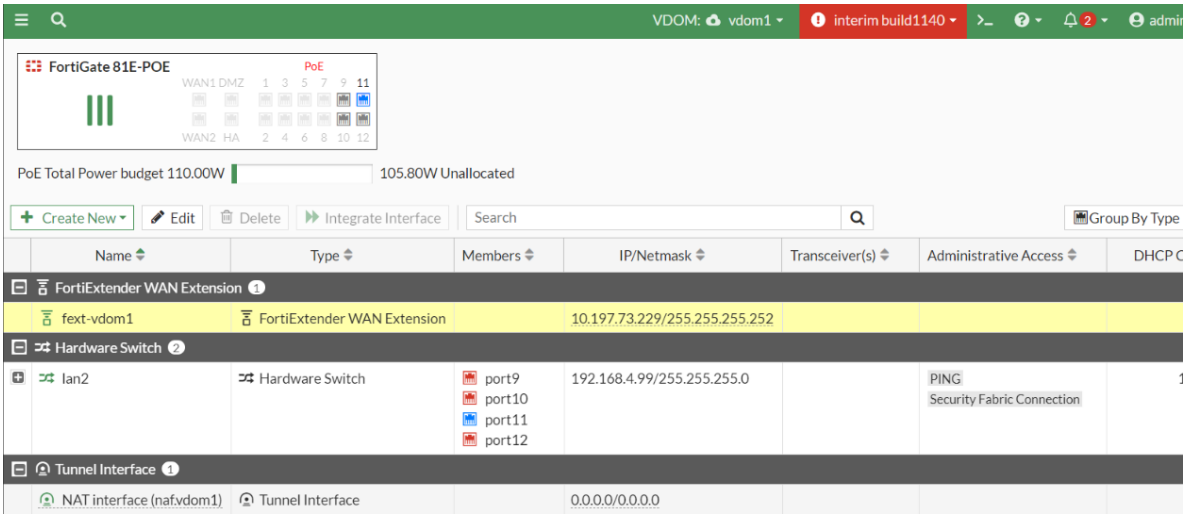
The FortiExtender can be authorized to bond a FortiExtender type interface to the LTE modem.



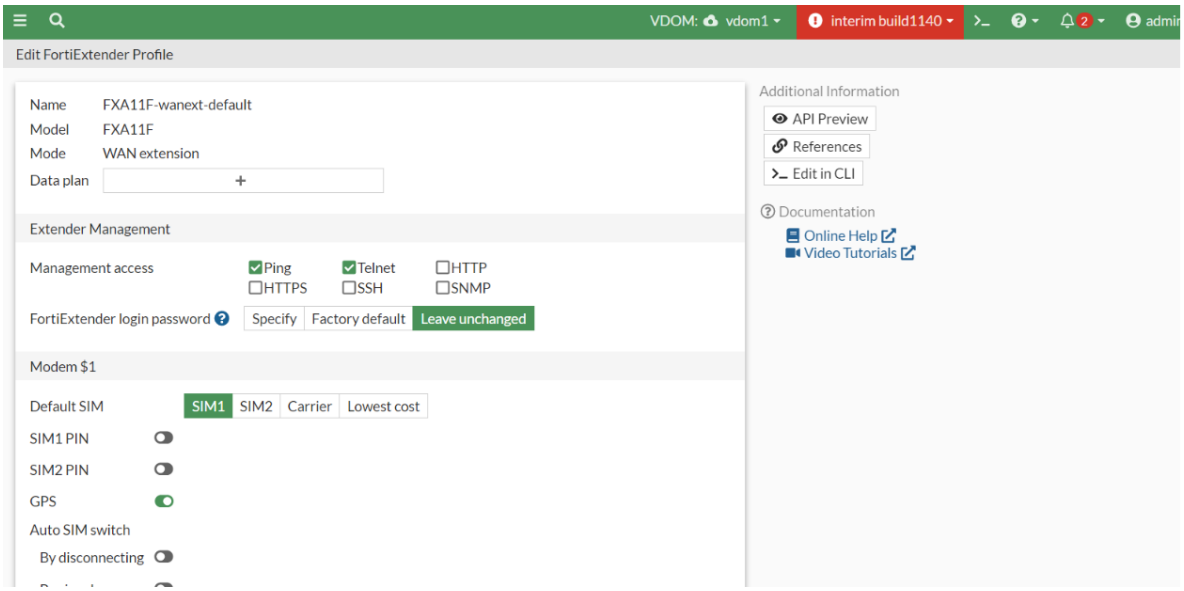
The FortiExtender is connected to the FortiGate after authorization.

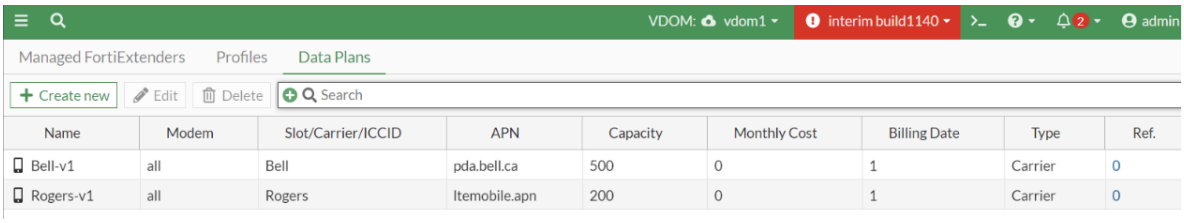


The FortiGate gets the IP and gateway for the FortiExtender type interface in the VDOM.



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





CLI operating procedures

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

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

2. Create a FortiExtender type interface in the VDOM.

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

```
    next
end
```

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

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

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

```
FortiGate-81E-POE (vdom1) # get system interface | grep fext-vdom1
== [ fext-vdom1 ]
name: fext-vdom1   mode: dhcp    ip: 10.197.73.229 255.255.255.252   status: up
 netbios-forward: disable    type: fext-wan   netflow-sampler: disable    sflow-
sampler: disable    src-check: enable    explicit-web-proxy: disable    explicit-
ftp-proxy: disable    proxy-captive-portal: disable    mtu-override: disable
 drop-overlapped-fragment: disable    drop-fragment: disable

FortiGate-81E-POE (vdom1) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

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

5. Modify the FortiExtender profile.

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

Discover a FortiExtender unit

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

- Broadcast
- Static IP

Broadcast

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

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

Static

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

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

For the FortiGate, you must ensure that the interface used for discovery should have allowaccess with `"fabric"`, as shown in the example below:

```
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 << fabric should be one option
           in allowaccess
      set type hard-switch
      set stp enable
      set role lan
      set snmp-index 21
   next
end
```

De-authorize a discovered FortiExtender

You can de-authorize a discovered FortiExtender via the FortiGate console using the following command:

```
config extender-controller extender
   edit "FX0035919000027"
      set authorized disable
   next
end
```

The default FortiExtender profile

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

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

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

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

These two ports will be linked as an aggregated interface in the FortiExtender and you can specify load-balance mode on it. More detailed LAN extension configuration is covered in LAN extension configuration in a profile on page 58.

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

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

The following example is for illustration only.

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

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

For the LAN extension, the default profile for the FortiExtender 201E generated on the FortiGate would look as follows. For details of LAN extension configuration, go to LAN extension configuration in a profile on page 58.

```
config extender-controller extender-profile
    edit "FX201E-lanext-default"
        set id 3
        set extension lan-extension
        config cellular
            config sms-notification
            end
            config modem1
            end
        end
        config lan-extension
            set ipsec-tunnel "fext-ipsec-ut4Z"
            set backhaul-interface "lan"
            config backhaul
                edit "1"
                    set port wan
                    set role primary
                next
                edit "2"
                    set port lte1
                    set role secondary
                next
            end
        end
    next
end
```

```
  # get FX201E-wanext-default (default value will be shown below)
  name : FX201E-lanext-default
  id : 3
  model : FX201E
  extension : lan-extension
  allowaccess :
  login-password-change: no
  enforce-bandwidth : disable
  cellular:
    dataplan :
    controller-report:
        status : disable
    sms-notification:
        status : disable
    modem1:
        redundant-mode : disable
        conn-status : 0
        default-sim : sim1
        gps : enable
        sim1-pin : disable
        sim2-pin : disable
        auto-switch:
            disconnect : disable
            signal : disable
            dataplan : disable
            switch-back :
```

```
          switch-back-time : 00:01
          switch-back-timer : 86400
lan-extension:
  link-loadbalance : activebackup
  ipsec-tunnel : fext-ipsec-ut4Z
  backhaul-interface : lan
  backhaul-ip :
  backhaul:
      == [ 1 ]
      name: 1
      == [ 2 ]
      name: 2
```

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

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

Allowaccess for FortiExtender management

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

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

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

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

```
config extender-controller extender
    edit "FX0015919000027"
        set id "FX201E5919000027"
        set authorized enable
        set extension-type lan-extension
        set override-allowaccess enable
```

```
            set allowaccess ping telnet
            set profile "FX201E-lanext-default"
        next
    end
```

Set bandwidth limit for LAN extension

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

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

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

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

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

```
        set traffic-shaper le-traffic-shaper
    next
  end
```

Configure FortiExtender admin password

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

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

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

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

Discovery response lockdown

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

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

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

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

Wildcard

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

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

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

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

Take FX200F for example. You can configure as follows:

```
config extender-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 extender-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 extender-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 extender-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.

LAN extension configuration in a profile

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

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

Parameter	Description
name	The profile name
id	The profile ID (for system internal record)
model	The FortiExtender model for the profile
extension [lan-extension | wan-extension]	The extension type for the profile
alloweaccess [telent|http|https|snmp|ping|ssh]	The multi-option setting for the lan-extension switch interface of the FortiExtender. For more details, see Allowaccess for FortiExtender management on page 52.
login-password-change [yes|no|default]	The setting of the admin password of the FortiExtender. For more details, see Configure FortiExtender admin password on page 54
enforce-bandwidth [enable|disable]	Enable or disable enforcement of bandwidth limit. **Note:** "enforce-bandwidth", which is disabled by default, is used to limit the egress bandwidth used to send traffic from the FortiExtender. For more details, see Set bandwidth limit for LAN extension on page 53.
bandwidth-limit	Specify the bandwidth limit.

Parameter	Description
`link-loadbalance [activebackup | loadbalance]`	Two ports are configured for the FortiExtender for load-balancing. For `activebackup` mode, you can configure `"role"` (primary or 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 60.

The following is an example of a backhaul configuration:

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

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

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

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

Backhaul IP in LAN extension

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

On the FortiExtender

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

On the FortiGate:

```
config extender-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.

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

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

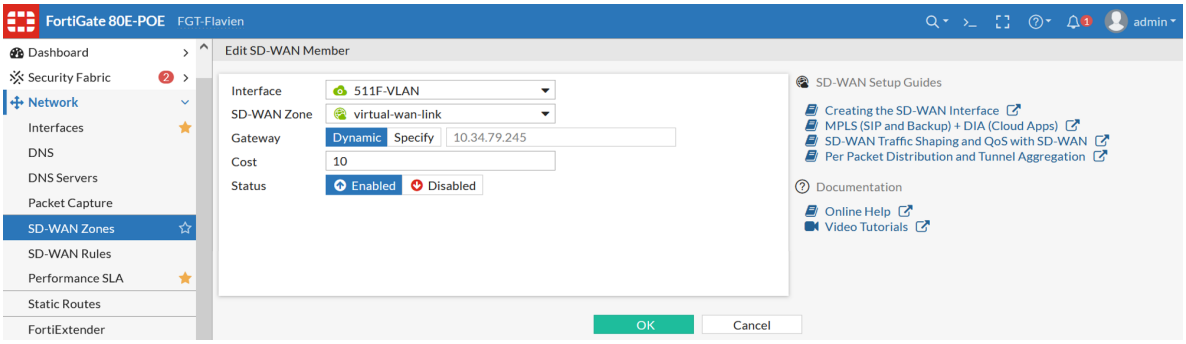
SD-WAN

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

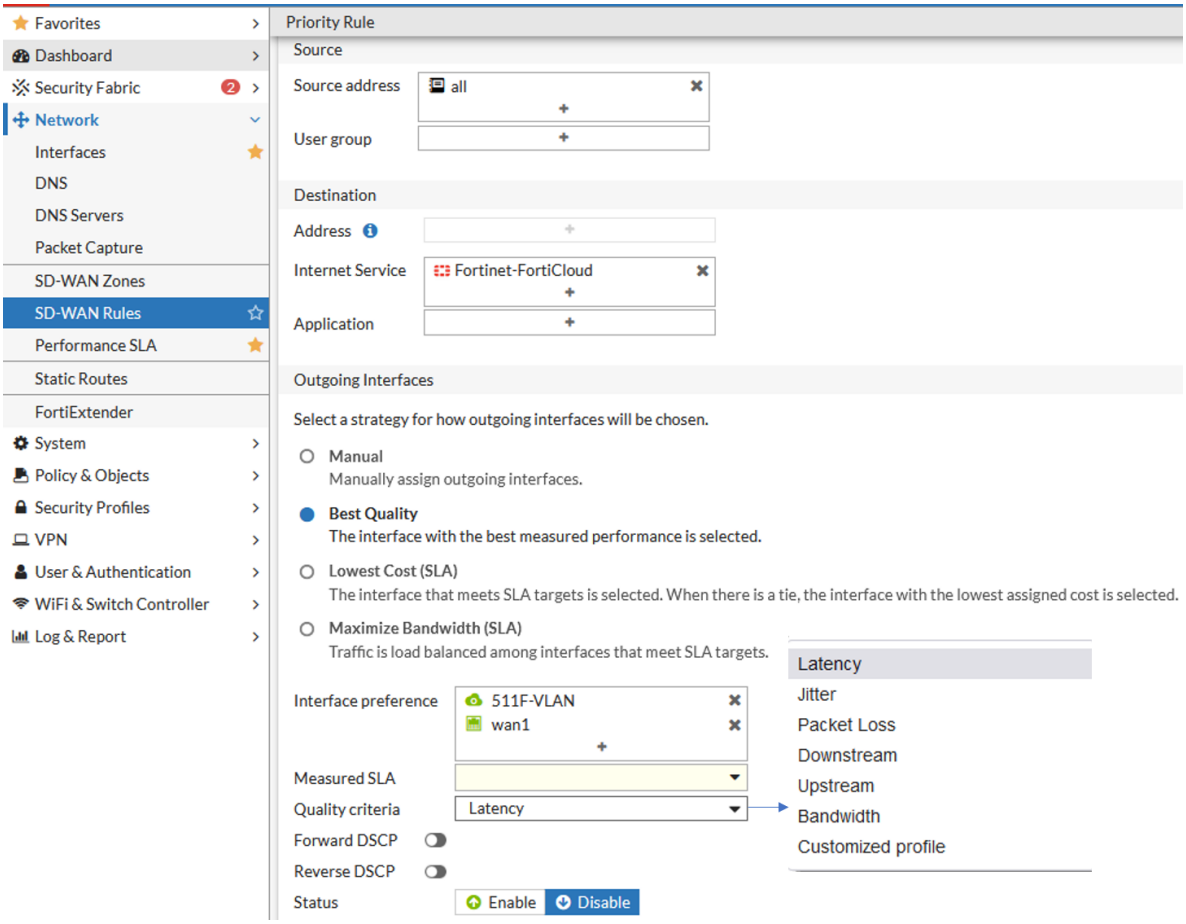
and backup service through associations with a FortiExtender link. This enables aggregation of multiple interfaces into a single SD-WAN interface using a single policy.

To accomplish this:

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



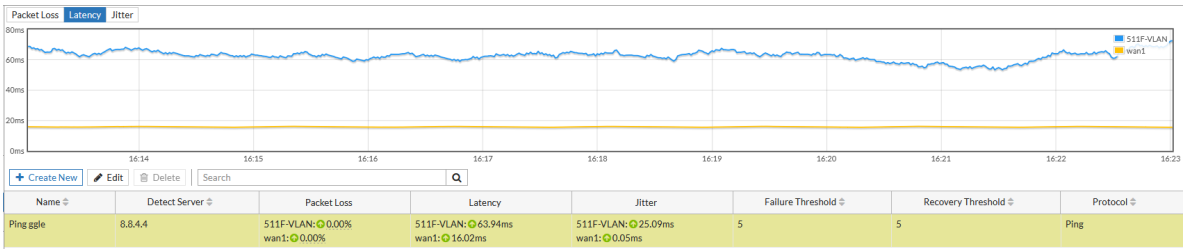
2. Define the priority rule, for instance, with the Best Quality strategy based on the Latency or Jitter criterion as shown in the following example.



3. Order or combine your policies as illustrated below.

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used
IPv4 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		

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



Configure cellular settings

Configuration of the cellular settings involves the following tasks:

- Create a data plan on page 63
- Set the default SIM on page 65
- Enable SIM-switch on page 66
- Report to FortiGate on page 67
- Capwap mode on page 67
- VLAN mode on page 68

Create a data plan

You can configure a data plan on the FortiGate with the following parameters:

```
config extender-controller dataplan
    edit Verizon
        set modem modem1
        set type by-carrier
        set carrier Verizon
        set apn WE01.VZWSTATIC
        set auth NONE
```

```
        set user
        set pwd
        set pdn ipv4-only
        set signal-threshold 0
        set signal-period 0
        set capacity 0
        set monthly-fee 0
        set billing-date 0
        set overage disable
        set preferred-subnet 32
        set private-network disable
    next
end
```

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

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

Parameter	Description
preferred-subnet	DHCP subnet.
private-network	(Enable/disable) blocking all non-NATed traffic.

Set the default SIM

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

You can set the default SIM by

- Set the default SIM by preferred carrier on page 65
- Set the default SIM by low cost on page 65
- Set the default SIM by SIM slot on page 66

Set the default SIM by preferred carrier

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

```
config extender-controller extender
    edit <FEX_SN>
        set authorized enable
        config modem1
            set ifname <fext-wan>
            set default-sim carrier
            set preferred-carrier <carrier name>
        end
    next
end
```

Set the default SIM by low cost

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

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

```
config extender-controller extender
    edit <FEX SN>
        set authorized enable
        config modem1
            set ifname <fext-wan>
            set default-sim cost
        end
    next
end
```

Set the default SIM by SIM slot

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

```
config extender-controller extender
    edit <FEX SN>
        set authorized enable
        config modem1
            set ifname <fext-wan>
            set default-sim sim1|2
        end
    next
end
```

Enable SIM-switch

```
config extender-controller extender
    edit <FEX SN>
        set authorized enable
        config modem1
            set ifname <fext-wan>
            config auto-switch
                set by-disconnect enable
                set by-signal disable
                set by-data-plan disable
                set disconnect-threshold 1
                set disconnect-period 600
                set switch-back by time by-timer set switch-back-by-time 00:01
                set switch-back-by-timer 3600
            end
        end
    next
end
```

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

Parameter	Description
by-disconnect	The SIM card switches when the active card gets disconnected according to the `'disconnect-threshold'` and `'disconnect-period'`.
by-signal	The SIM card switches when the signal strength gets weaker than the signal-threshold.
by-data-plan	The SIM card switches when `'capacity'` is overrun and `'overage'` is enabled.
disconnect-threshold	The number (1 —100) of disconnects for SIM switch to take place.

Parameter	Description
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.

Report to FortiGate

```
config extender-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 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
```

VLAN mode

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

Configurations on FortiExtender

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

```
config system interface
      edit vlan1
            set type vlan
            set vid 100
            set ingress-intf lan
      next
end
```

Virtual Wire Pair

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

```
config system virtual-wire-pair
   set lte1-mapping vlan1
end
```

CAPWAP on multiple ports for broadcast discovery

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

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

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

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

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

Check current manage mode

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

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

Get modem status

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

```
FX201E5919002499 # get modem status
Modem status:
    modem             : Modem1
    usb path          : 2-1.2 (sdk 0)
    vender            : Sierra Wireless, Incorporated
    product           : Sierra Wireless, Incorporated
    model             : EM7455
    SIM slot          : SIM1
    revision          : SWI9X30C_02.32.11.00 r8042 CARMD-EV-FRMWR2 2019/05/15
21:52:20
    imei              : 359073065340568
    iccid             : 8933270100000296108
    imsi              : 208270100029610
    pin status        : enable
    pin code          : 0000
    carrier           : 436627|coriolis|EU
    APN               : N/A
    service           : LTE
    sim pin (sim1)    : 3 attempts left
    sim puk (sim1)    : 10 attempts left
    rssi (dBm)        : -68
    signal_strength   : 64
    ca state          : ACTIVE
    cell ID           : 00A25703
    band              : B7
    band width        : 20
    sinr (dB )        : 7.4
    rsrp (dBm)        : -99
    rsrq (dB )        : -13.1
    plan_name         : coriolis100G
    connect_status    : CONN_STATE_CONNECTED
    reconnect count   : 0
    smart sim switch  : disabled
    up time (sec)     : 26670
    clock (UTC)       : 20/05/27,20:08:33+08
    temperature       : 60
    activation_status : N/A
    roaming_status    : N/A
    Latitude          : 37.376281
    Longitude         : -122.010817
```

Stopping data traffic on overaged LTE interface

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

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

Use cases

This section discuses some typical use cases to deploy FortiExtender.

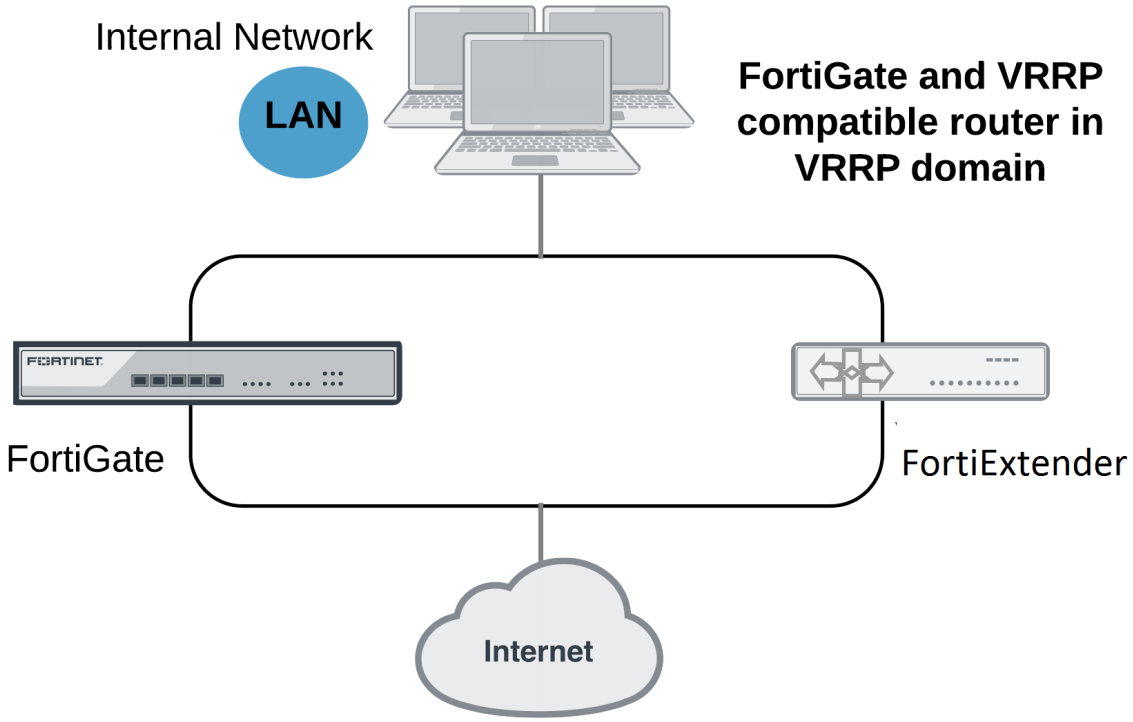
- Redundant with FGT in IP Pass-through mode on page 73
- FortiExtender for FortiGate HA configuration on page 78

Redundant with FGT in IP Pass-through mode

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

For more information about VRRP, see RFC 3768.

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



General configuration procedures

1. The FortiExtender LAN interface consists of multiple ports by default. Be sure to separate out an individual port from the LAN-switch for VRRP purposes. (Refer to "Step 3: Verify the port settings on FortiExtender" in FortiExtender for FortiGate HA configuration on page 78.)
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:

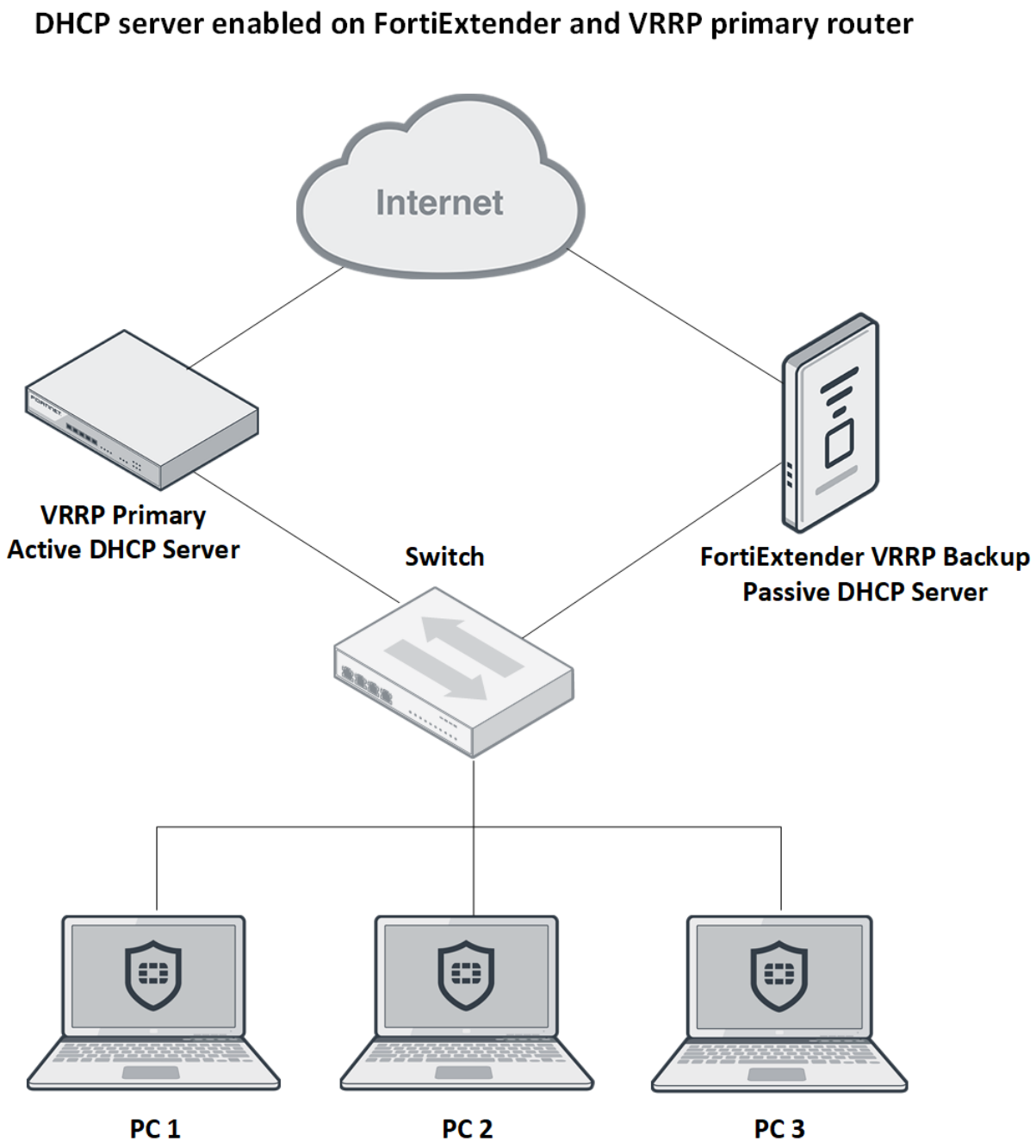
```
get router info vrrp
```

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, seeConfigure 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.

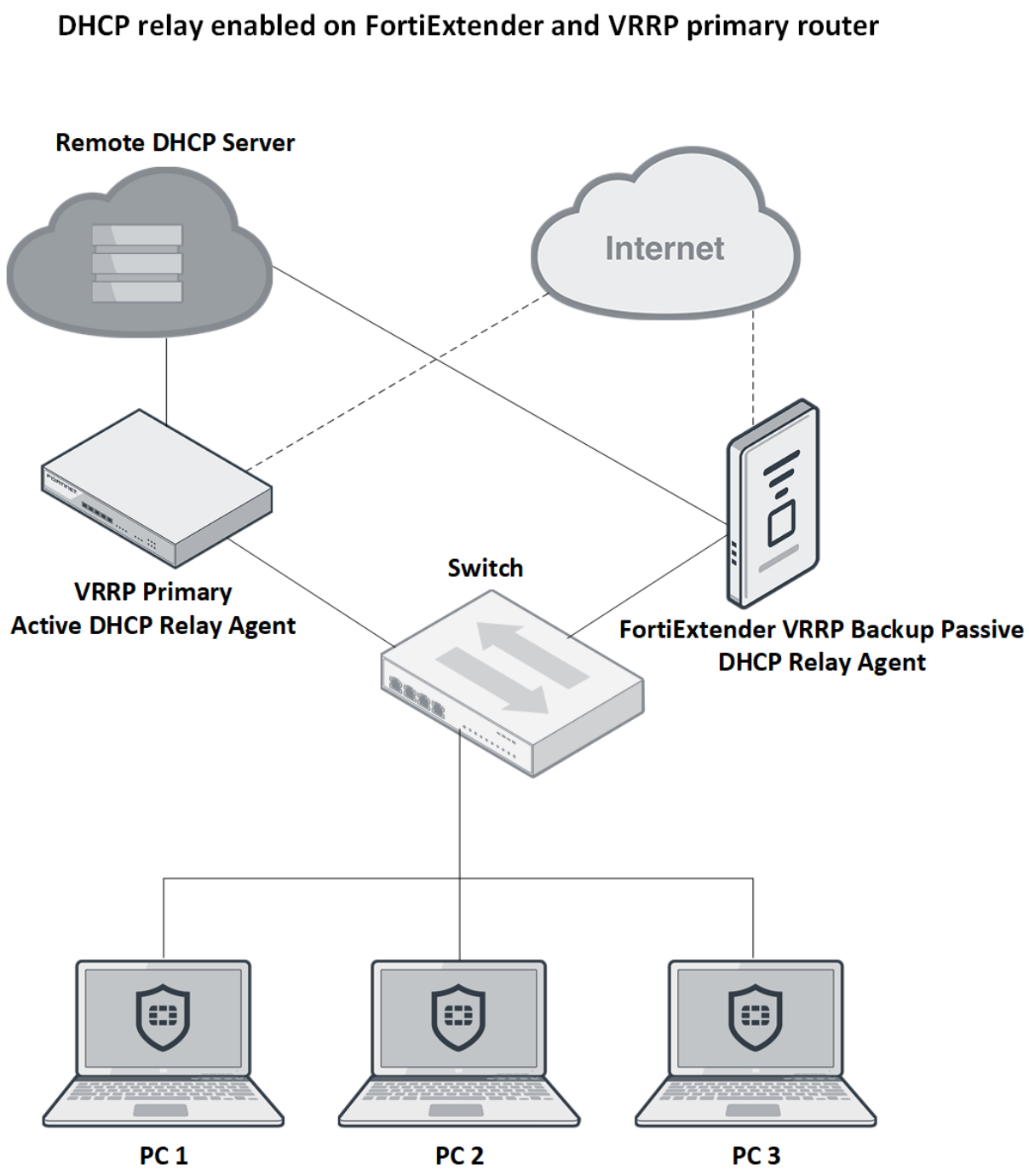
For information on DHCP relay configuration, see Configure DHCP relay.

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.

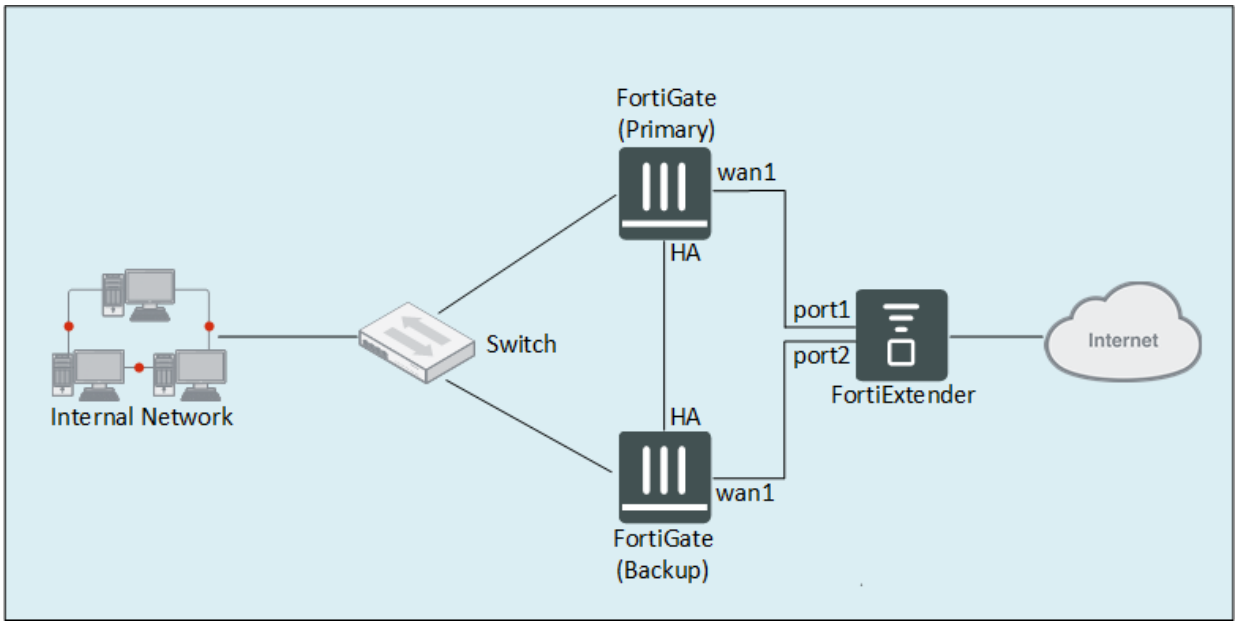


FortiExtender for FortiGate HA configuration

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.

Network topology



Prerequisites

- The FortiExtender 201E device must be physically networked with the two FortiGate devices, with its port1 connected to wan1 on the primary FortiGate and port2 connected to wan1 on the backup FortiGate, as illustrated in the Network topology.
- The two FortiGate devices must be physically connected via the HA port on both of them, as illustrated in the Network topology.
- The two FortiGate devices must be running the same version of FOS.

The FortiGate devices used in this sample configuration are both running FOS 6.2.1.

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. Then, select *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 two *Heartbeat interfaces* (one at a time) by doing the following:
      i. Click **+** (plus sign), and (from the pop-up list of interfaces) select *ha.*
      ii. Set *Heartbeat Interface Priority* to *50.*
      iii. Click *OK.*
      iv. Click **+** (plus sign) again, and (from the pop-up list of interfaces) select **wan1.**
      v. Set **Heartbeat Interface Priority** to 50.
      vi. 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. Then, select **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 two **Heartbeat interfaces** (one at a time) by doing the following:
      i. Click **+** (plus sign), and (from the pop-up list of interfaces) select **ha.**
      ii. Set **Heartbeat Interface Priority** to 50.
      iii. Click **OK.**
      iv. Click **+** (plus sign) again, and (from the pop-up list of interfaces) select **wan1.**
      v. Set **Heartbeat Interface Priority** to 50.
      vi. Click **OK.**

- Ensure that the Device Priority value on the primary FortiGate is higher than the one for the backup FortiGate.
- Ensure that two heartbeat interfaces are selected and the Heartbeat Interface Priority are both set to 50 on both.

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
        edit port4
        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.

Copyright© 2025 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.