FortiExtender (Managed) - Admin Guide

Version 7.0.1

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

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 11, 2021
FortiExtender (Managed) 7.0.1 Admin Guide

TABLE OF CONTENTS

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 wireless router, managed individually or centrally from FortiExtender-Cloud or in FortiGate managed-mode as part of the integrated Fortinet Fabric Solutions.

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

Before you begin

For information about FortiExtender hardware compatibility, refer to the table below.

Hardware & operating system compatibility

Hardware platform	FortiExtender OS		
	4.2.3	7.0.0	7.0.1
201E	Yes	Yes	Yes
211E	Yes	Yes	Yes
200F	Yes	Yes	Yes
511F	No	No	Yes

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

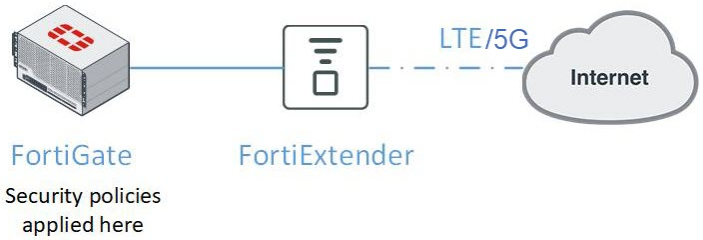
- You have completed the installation of the FortiExtender unit, as outlined in the QuickStart Guide. (**Note:** You can power FortiExtender unit using an external power adapter or by POE when connected to the POE/PSE port of FortiGate.)
- You have administrative access to the FortiExtender GUI or CLI for any troubleshooting needed.
- You have installed a 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 FortiExtender, but also provides visibility to the performance and data usage of the connection.



In this scenario, you can connect a FortiExtender to two FortiGate devices for a high availability (HA) configuration in Active-Passive, and two FortiExtenders to two FortiGate devices in Active-Active deployments, providing dual active redundancy for wireless WAN access as well.

FortiExtender and 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 service goes to FortiGate. FortiExtender 4.2.2 adds local ssh/https/telnet/http service support via the LTE interface. To distinguish local services from FortiGate services, you must configure FortiExtender to use different ports. Otherwise, all traffic to these default services will be sent to 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 provision (ZTP). 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, FortiGate connects to a FortiExtender LAN port (1, 2, or 3) interface to obtain a private IP to reach FortiManager.
3. FortiGate reports the discovered FortiExtender to FortiManager to authorize it (FortiExtender).
4. Once authorized, FortiExtender switches to IP-passthrough mode and then reboots itself.
5. Upon booting up in IP-passthrough mode, FortiExtender serves as the FortiExtender WAN interface of FortiGate.

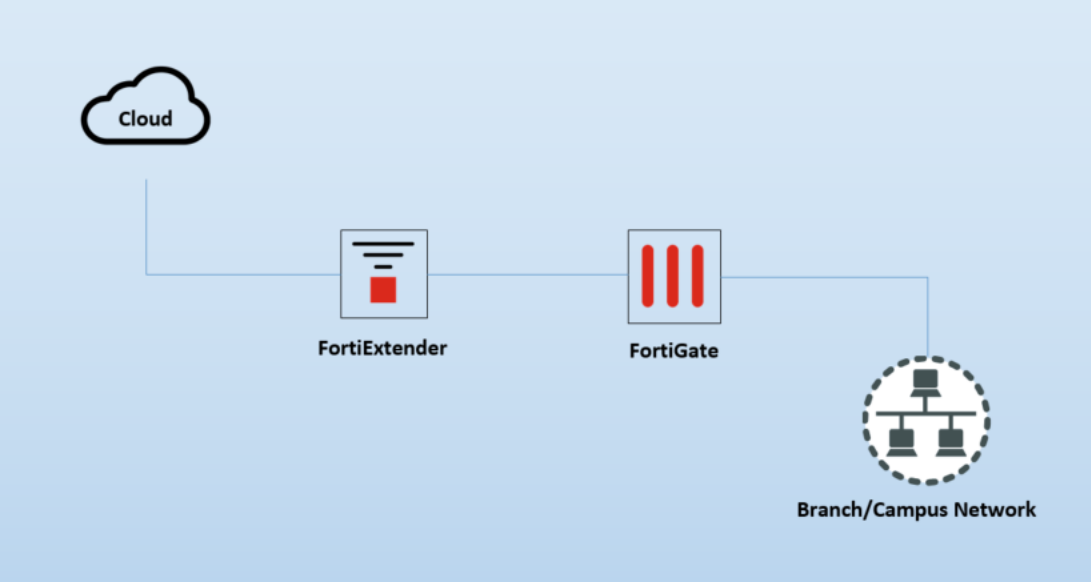
Connect to FortiGate

When setting up a FortiExtender out of box with FortiExtender OS version 7.0.1, you can connect FortiExtender to FortiGate in either of the following ways:

- Connect the FortiGate port in DHCP client mode (such as WAN1/WAN2) 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 FortiExtender, which acquires DHCP lease from the FortiGate DHCP server.

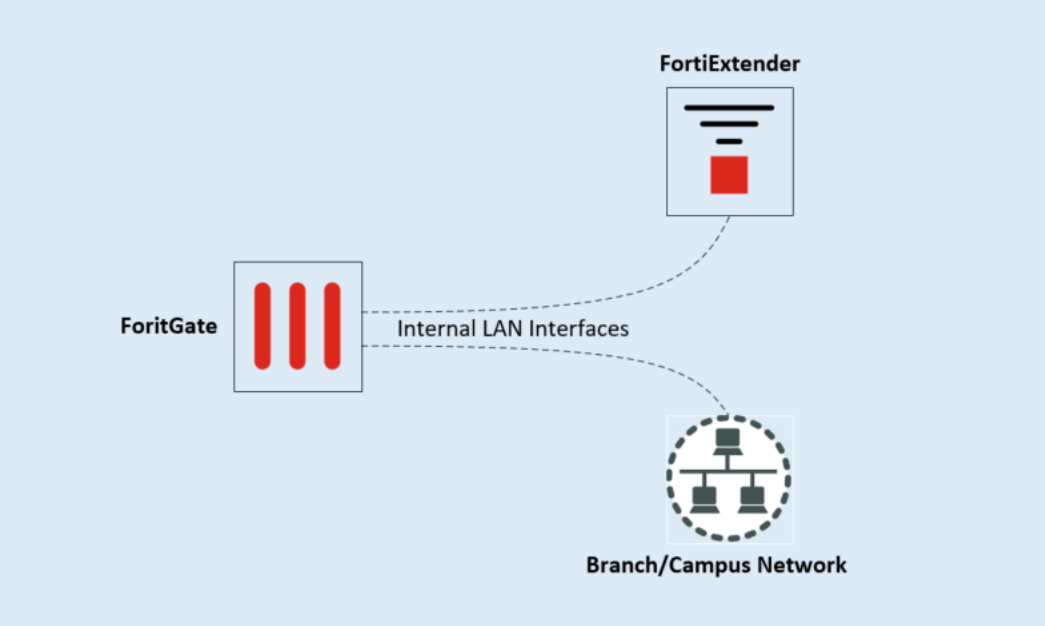
When setting up a FortiExtender out of box with FortiExtender OS version 7.0.0 or later, you can connect FortiExtender to FortiGate in either of the following ways:

Wireless WAN extension to WAN interfaces of FortiGate



Connect the FortiGate WAN port(e.g., WAN1, 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 LAN/internal interfaces of FortiGate



In some scenarios, you may want to connect FortiExtender to an internal/LAN interface of 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 (FEX-201E/211E) of FortiExtender which acquires DHCP lease from the FortiGate DHCP server, as illustrated above.

Enable FortiExtender Controller on FortiOS

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

a. Enable the FortiExtender Controller on FortiGate.

```
# config system global
(global) # set fortiextender enable
(global) # end
```

b. Make sure that your FortiGate enables FortiExtender Controller.
The FortiExtender-related GUI is enabled by default.

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

```
config system interface
edit lan
     append allowaccess fabric
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, FortiExtender must be connected to FortiGate through FortiLink.
- If FortiLink is enabled and FortiExtender is not part of FortiLink , the discovery type on FortiExtender must be static.

LAN 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 the traffic to and from FortiGate is encapsulated in the CAPWAP data channel. In VLAN mode, the 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 FortiExtender is connected to FortiGate. It is important to note that in VLAN mode, Fortiextender and Fortigate can be connected directly to each other or via a switch. In case of a switch in between, the switch should be configured to allow the configured ALANs.

Note that 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
(global) # set fortiextender-vlan-mode enable
(global) # end
```

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

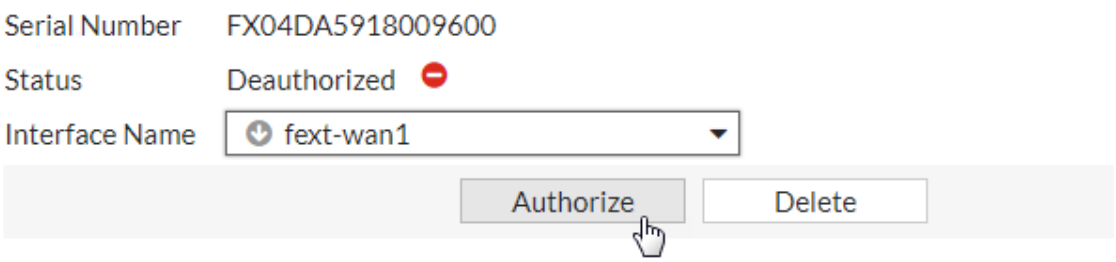
Authorize FortiExtender on FortiOS

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 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 FortiExtender as part of the authorization process, as illustrated

below.



Make sure that FortiExtender and 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 your FortiExtender with static discovery using the following FortiExtender CLI commands:

```
config system management fortigate
     set ac-discovery-type static
     set static-ac-ip-addr 192.168.1.99
     set ac-ctl-port 5246
     set ac-data-port 25246
end
```

Configure cellular settings

Configuration of the cellular settings involves the following tasks:

Create a data plan

You can configure a data plan on the FortiGate with the below 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
```

When "`private network`" is enabled, FortiExtender allows the flow of non-NAT'ed 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.

Parameter	Description
	• 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	Set the APN of the SIM card.
auth-type	Choose the Authorization mode.
username	Set the username.
password	Set the password.
pdn	Choose the Packet Data Network (PDN) IP address family.
signal-threshold	Set the signal-strength threshold beyond which SIM switch will occur. **Note:** Enter an integer value from <50> to <100> (default = <100>).
signal-period	Set 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	Set data capacity per month (from 0 to 102400000 MB).
monthly-fee	Set the monthly fee for the data plan (from 0 to 1000000).
billing-date	Set the billing date of the month.
preferred-subnet	DHCP subnet.
private-network	Enable/disable blocking all non-NAT'ed traffic.

Set the default SIM

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

You can set the default SIM by

- Set the default SIM by preferred carrier on page 12
- Set the default SIM by low cost on page 13
- Set the default SIM by SIM slot on page 13

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
   end
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
   end
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
   end
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
```

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

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

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
end
```

Parameter	Description
status	Enable or disable periodic controller report.
interval	The interval at which to notify the FortiGate (once every 30 to 86400 seconds; the default is 300).
signal-threshold	The signal strength threshold (10 - 50 dBm). FortiExtender notifies the FortiGate once the RSSI change has exceeded the set threshold.

Capwap mode

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

Configurations On FortiExtender

You can manually configure the attached physical interface of CAPWAP Interface field. Otherwise, the system will default it to 'lan'.

```
FX212E5919000009 # config system management fortigate
FX212E5919000009 (fortigate) # set ingress-intf lan
FX212E5919000009 (fortigate) <M> # show
config system management fortigate
set ingress-intf lan
end
FX212E5919000009 (fortigate) <M> #
```

Capwap Interface

The capwap interface is created automatically. You can not edit or remove it.

```
FX212E5919000009 # config system interface
FX212E5919000009 (interface) # edit capwap1
FX212E5919000009 (capwap1) # show
edit capwap1
set type capwap
set rid 1
next
FX212E5919000009 (capwap1) # end
FX212E5919000009 #
```

For FEX-212E, you must also configure the following because it has dual modems.

```
FX212E5919000009 # config system interface
FX212E5919000009 (interface) # edit capwap2
FX212E5919000009 (capwap2) # show
edit capwap2
set type capwap
set rid 2
next
FX212E5919000009 (capwap2) #
```

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 capwap1 interface will be sent out by the lte1 interface.

```
FX212E5919000009 # config system virtual-wire-pair
FX212E5919000009 (virtual-wire-pair) # show config system virtual-wire-pair set lte1-
```

```
mapping capwap1 set lte2-mapping capwap2 end
FX212E5919000009 (virtual-wire-pair) #
```

VLAN mode

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

Configurations on FortiExtender

The VLAN interface is created automatically on FortiExtender. You cannot edit it or remove it.

```
FX212E5919000009 # config system interface
FX212E5919000009 (interface) # edit vlan1
FX212E5919000009 (vlan1) # show
edit vlan1
set type vlan
set vid 100
set ingress-intf lan
next
FX212E5919000009 (vlan1) # next
FX212E5919000009 (interface) # edit vlan2
FX212E5919000009 (vlan2) # show
edit vlan2
set type vlan
set vid 200
set ingress-intf lan
next
FX212E5919000009 (vlan2)
```

Virtual Wire Pair

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

```
FX212E5919000009 (virtual-wire-pair) # show
config system virtual-wire-pair
   set lte1-mapping vlan1
   set lte2-mapping vlan2
end
FX212E5919000009 (virtual-wire-pair) #
```

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 FortiGate monitors a given WAN link on the FortiGate, and brings up 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
```

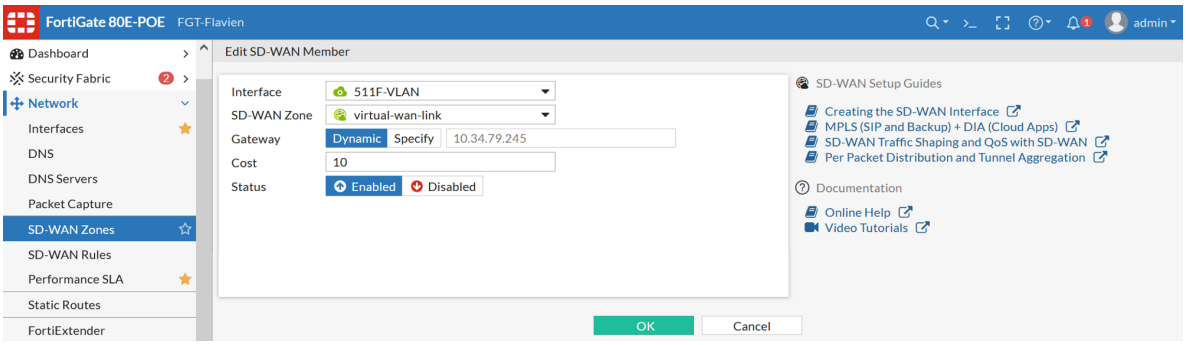
In this mode of operation, the FortiExtender interface comes up if the WAN interface goes down and goes down if the WAN interface comes up.

SD-WAN

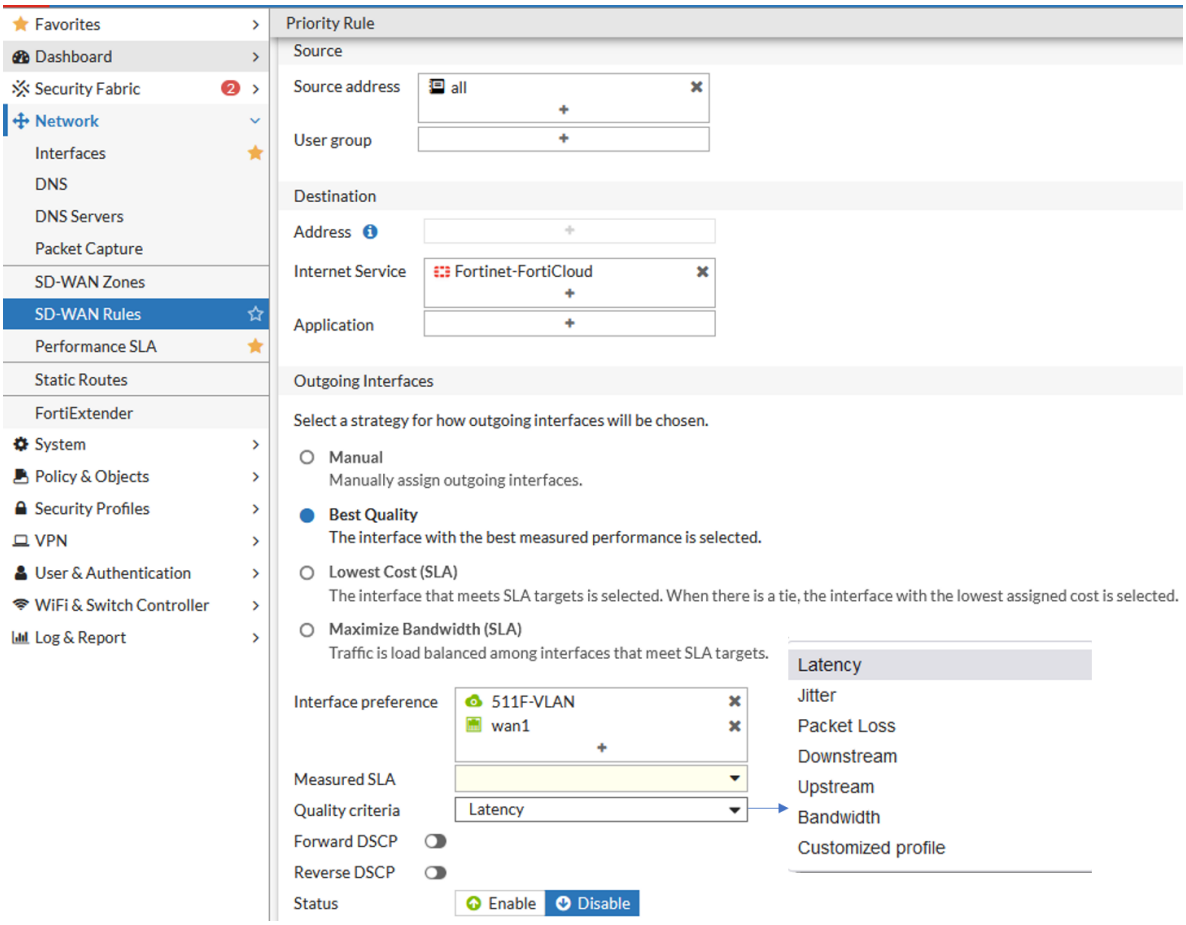
FortiOS recognizes and uses FEX as a valid interface within an SD-WAN interface zone. Using SD-WAN, FortiGate becomes a WAN path controller and supports diverse connectivity methods. With FEX, 3G/4G/5G can be used as a primary connection, a backup interface, or a load-balanced WAN access method with 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 backs up service through associations with an 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.



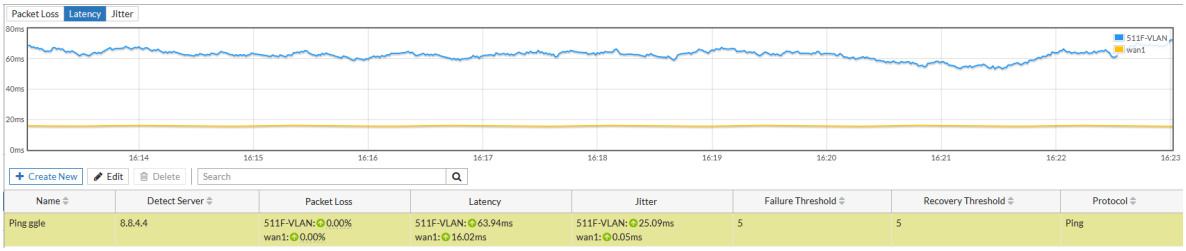
2. Define the priority rule, as shown in the following example, for instance, with the Best Quality strategy based on the Latency or Jitter criterion.



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.



CAPWAP on multiple ports for broadcast discovery

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

```
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, it starts the discovery process with the LAN ports (from 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 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 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:

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

Use cases

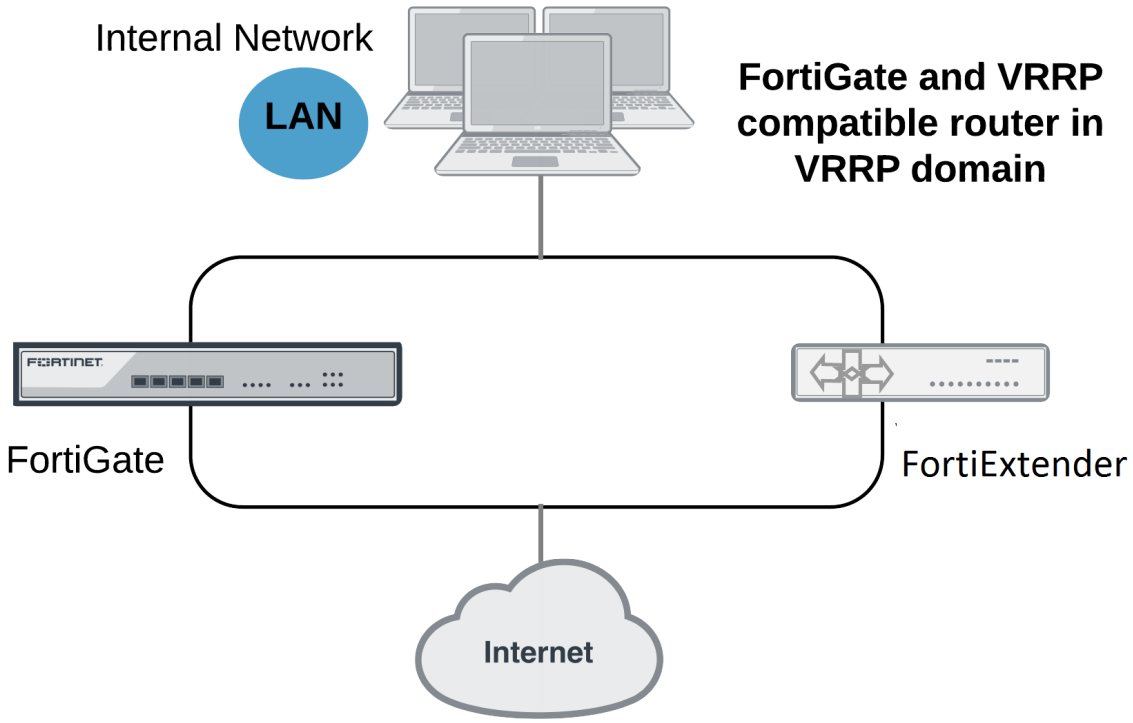
This section discuses some typical use cases to deploy FortiExtender.

Redundant with FGT in IP Pass-through mode

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 FEX-201E for FortiGate HA configuration on page 29.)

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 the FortiGate VRRP interface's priority.
5. Create a firewall policy on the FortiExtender to forward traffic from newly created VRRP interface to the LTE internet (Refer to 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 master mode by running command "get router info vrrp".

In normal operations, all traffic to the internet passes through the primary VRRP interface of 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 FortiGate:

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

To enable VRRP on FortiExtender:

```
config system management
set discovery-type fortigate
       config fortigate-backup
               vrrp-interface <vrrp interface i.e por1>
               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 master typically disable)
end
```

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

To display the status of virtual router on FortiExtender:

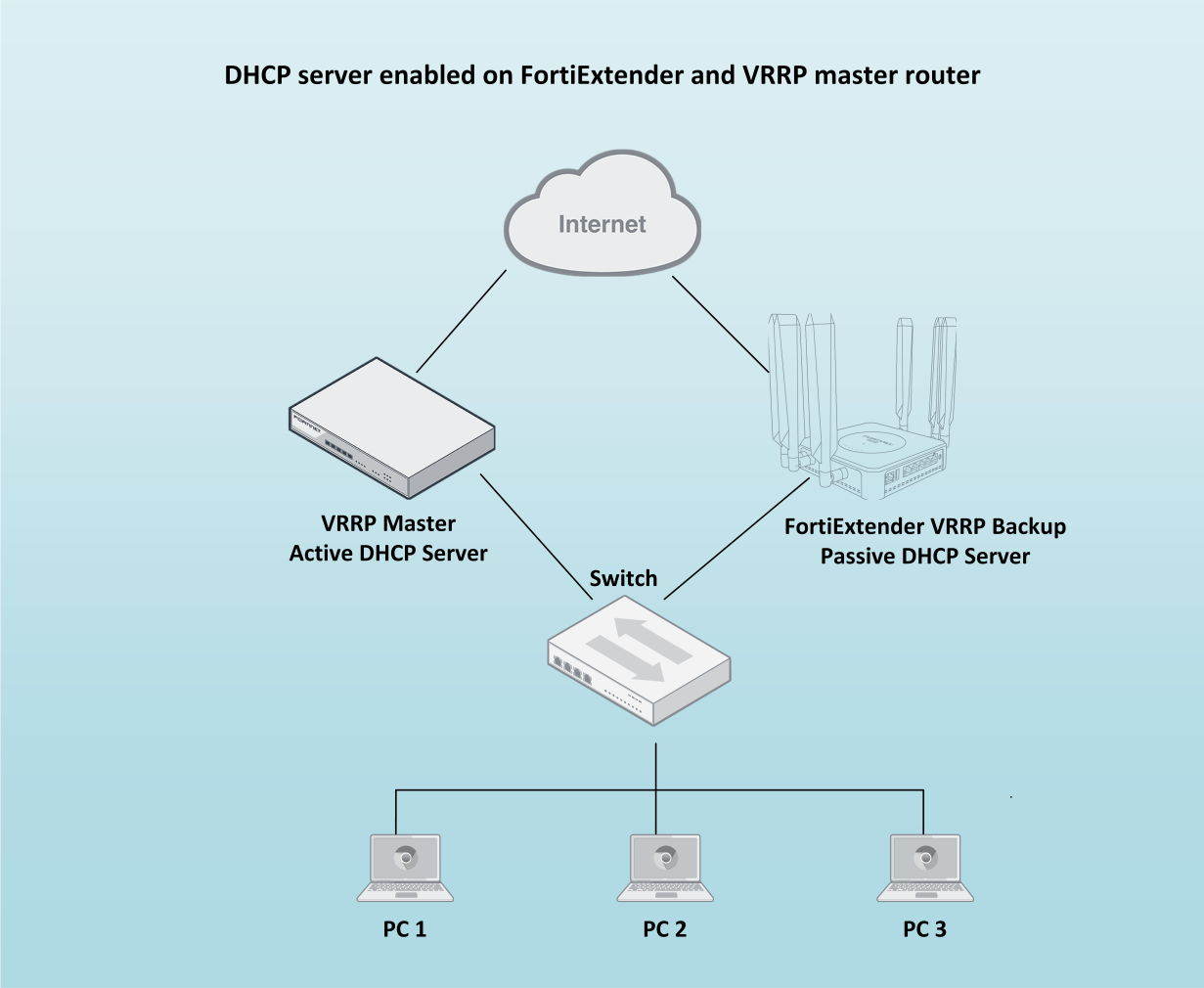
```
get router info vrrp
```

Enable DHCP server on FortiExtender and the VRRP master 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 master and the backup routers are configured with DHCP servers with reserved IP addresses to their corresponding MAC addresses.

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

For information on DHCP server configuration, refer to Configure DHCP server.



Enable DHCP relay on both FortiExtender and the VRRP master 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 master router is also running a DHCP relay agent on the respective VRRP interface. This ability ensures that the hosts in the VRRP domain always gets the same IP address, irrespective of which VRRP router is in operation, without causing any IP address conflicts because the requests are catered to by the same remote DHCP server.

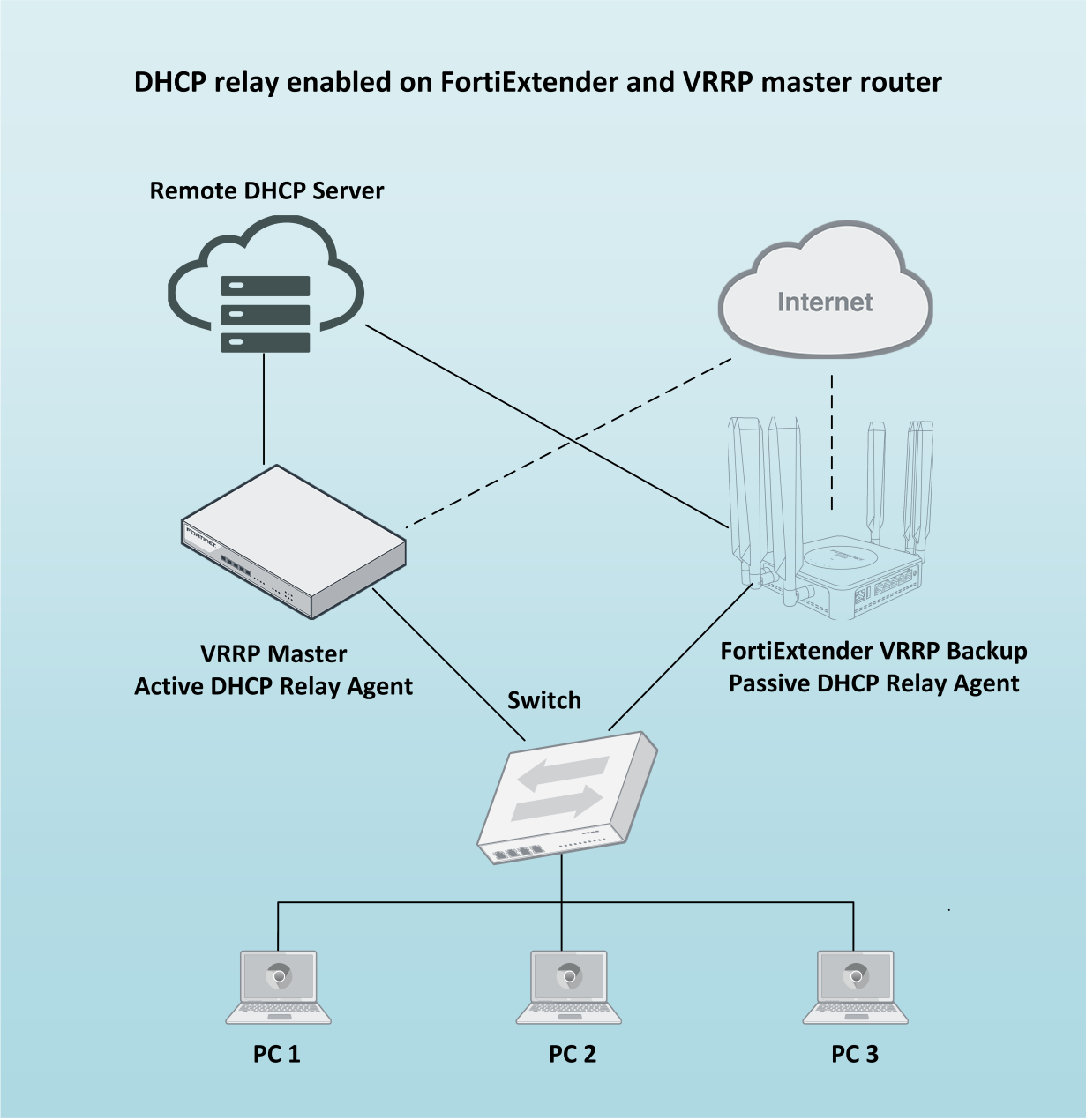
For information on DHCP relay configuration, refer to Configure DHCP relay.

DHCP relay

FortiExtender now supports DHCP relay agent which enables it to fetch DHCP leases from a remote server. It has to be configured per interface. Example below:

```
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
```

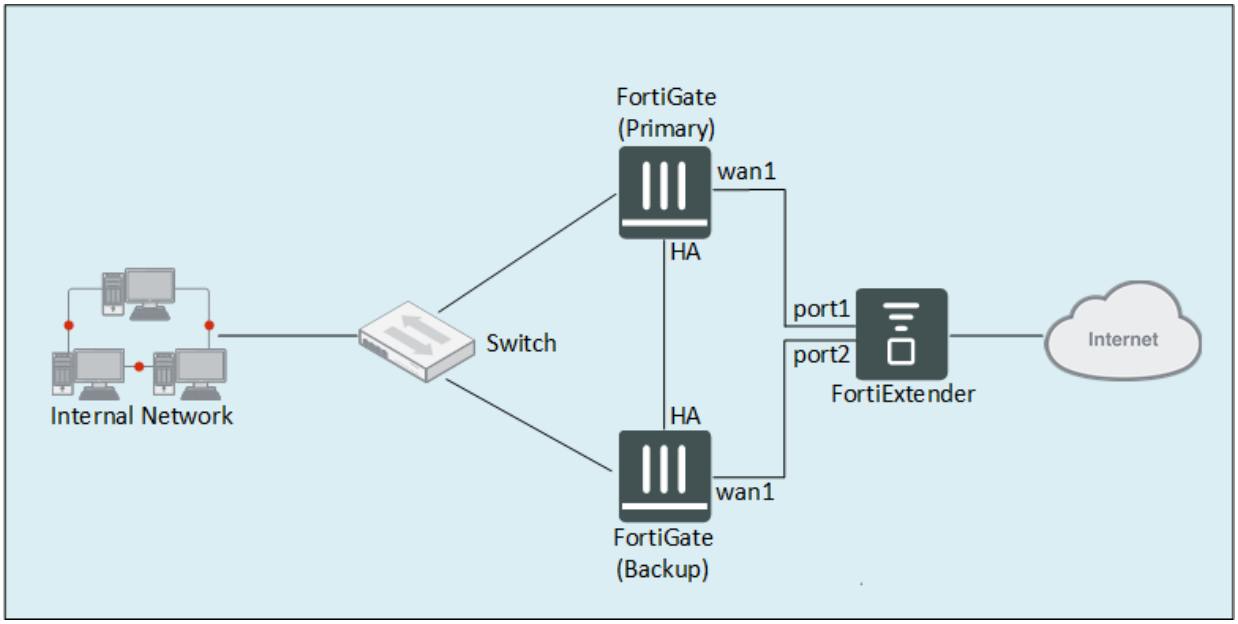
The DHCP relay and DHCP server services can be run on any VRRP interface, which could be either a separate port or a VLAN interface.



FEX-201E for FortiGate HA configuration

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 Port 1 connected to wan1 on the primary FortiGate and Port 2 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 **Host name** 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 a **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.

Change Log

Date	Change Description
August 11, 2021	FortiExtender (Managed) 7.0.1 Admin Guide 2nd draft.