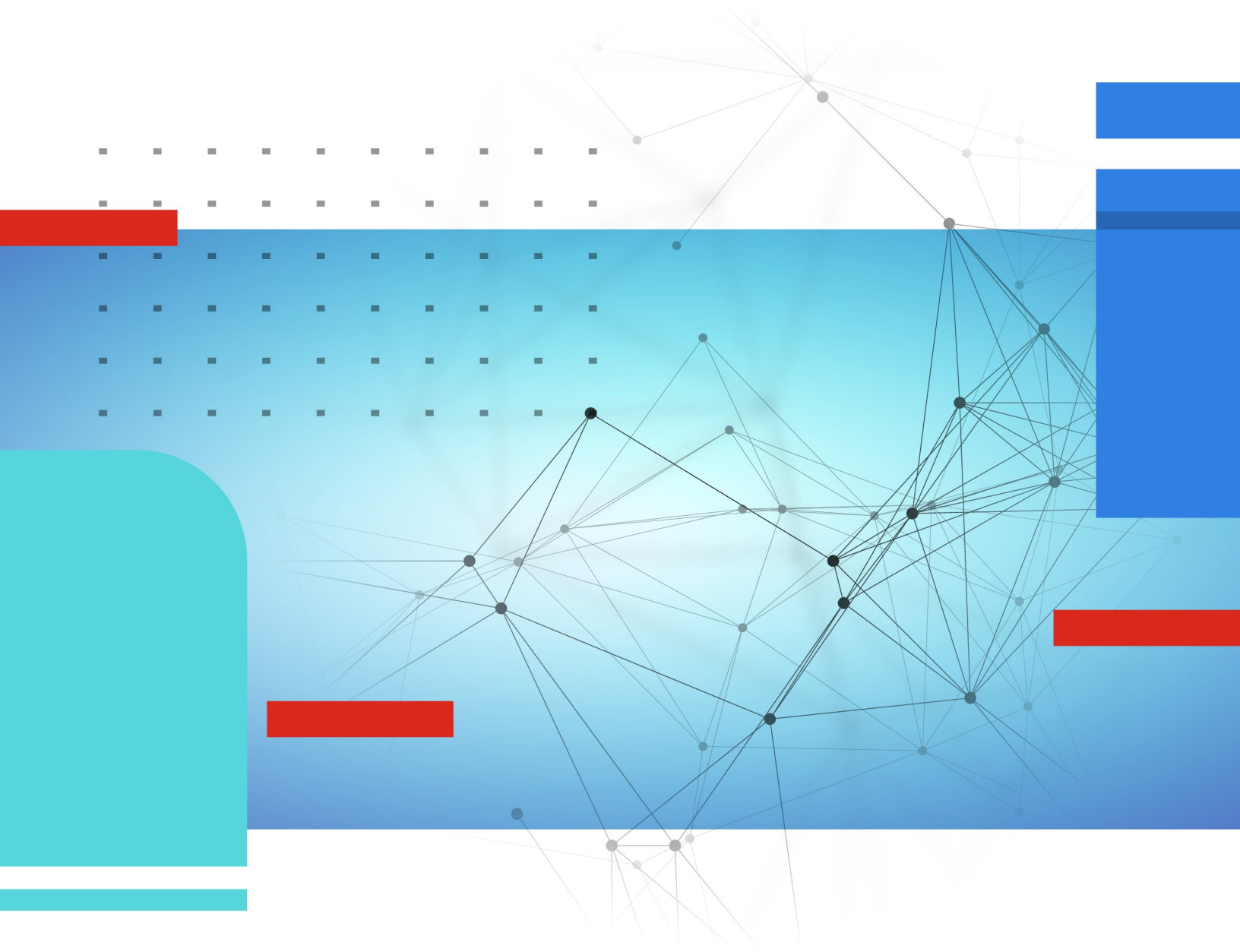
Troubleshooting Guide

FortiExtender 7.6.0



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

Sep 16, 2024
FortiExtender 7.6.0 Troubleshooting Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-08-12	Initial release.
2024-09-16	Renamed FortiExtender Cloud to FortiEdge Cloud.

Introduction

The FortiExtender Troubleshooting Guide covers several important command line interface (CLI) commands that can be used for log gathering, analysis, and troubleshooting, as well as common troubleshooting scenarios you may encounter.

FortiExtender debug and diagnose commands cheat sheet

This cheat sheet lists several important CLI commands that can be used for log gathering, analysis, and troubleshooting.

General Health, CPU, and Memory

Command	Description
`get system version`	Show the system version output.
`get system status`	Show the system status output including SN, BIOS version, model, system time, and etc.
`get system performance status`	Show the system performance status output including CPU status, usage rate, memory states, up time, and SOC temperature.
`execute debuginfo export tftp <remote_file> <tftp_server>`	Export the debuginfo zip file via TFTP server.

Daemon status

Command	Description
`get system app-status`	Show the application running state and PID.
`execute restartapp`	Restart a specified application.

Admin sessions

Command	Description
`get system admin status`	Show the administrator status and their account profile info.
`execute disconnect-admin-session`	Disconnect an administrator session.
`execute ssh <username> <ssh_server>`	SSH into a host using the host server IP.

Command	Description
`execute api-user generate-key <user_name>`	Generate keys for API users.
`execute api-user show-key <user_name>`	Show key for API users.

Routing Debug

Command	Description
`get router info routing-table all`	Show all routing table entries.
`get router info policy`	Show policy based routing rule.
`get router info target`	Show route target entries.
`get router info multicast pim-sm vifs`	Show multicast pim-sm virtual interfaces.
`get router info multicast pim-sm table`	Show multicast pim-sm routing table.
`get router info multicast pim-sm rp`	Show multicast pim-sm RP information.
`get router info ospf status`	Show OSPF status.
`get router info ospf database`	Show OSPF database summary.
`get router info ospf interface`	Show OSPF interface information.
`get router info ospf neighbor`	Show OSPF neighbor list.
`get router info ospf route`	Show OSPF routing table.
`get router info vrrp`	Show VRRP information.
`execute ip`	Execute IP rule.
`execute iptables`	Execute iptables rule.
`execute iptables-save`	Show contents of IP tables information.
`execute route`	Show route information.
`execute netstat`	Show network connections.
`execute ping`	Start ping to a certain host.

Interfaces

Command	Description
`get system interface`	Show all system interface information.
`get system lan-switch status`	Show LAN-switch status and information.
`get system vxlan status`	Show VXLAN interface status.
`get system switch-interface status`	Show switch interface status.
`get system aggregate-interface status`	Show aggregate interface status.
`get system pppoe status`	Show system PPPoE interface status.
`execute ifconfig`	Show all network interface configuration information.
`execute interface dhcpclient-renew <interface_name>`	Renew interface's DHCP lease.

DHCP server/client

Command	Description
`get system dhcp-client lease-info`	Show system DHCP client lease information.
`get system dhcp-server config`	Show system DHCP server configuration.
`get system dhcp-server clients <dhcp-server-name>`	Show system DHCP server's connected clients information.
`execute interface dhcpclient-renew <interface_name>`	Renew interface's DHCP lease.

NTP debug

Command	Description
`get timezone list`	Show supported timezone list.
`execute date`	Show system date and time.

SNMP daemon debug

Command	Description
`execute snmpmibs export tftp <mib_file> <tftp_ server>`	Export SNMP MIBs file via TFTP server.

Virtual-WAN verification and debug

Command	Description
`get vwan status`	Show system virtual-wan interface status.
`get vwan member`	Show virtual-wan member information.

DNS server and proxy debug

Command	Description
`get system dns`	Show system DNS information.
`get dnsproxy stats`	Show dnsproxy statistics.
`execute nslookup`	Run DNS query to a certain host.
`execute dnsproxy cache clear`	Clear DNS cache.
`execute dnsproxy cache dump`	Dump DNS cache.
`execute dnsproxy database dump`	Dump DNS database.

CPM/cloud connection status

Command	Description
`get cpm status`	Show connection status to FortiEdge Cloud.
`get extender status`	Show FortiExtender system status.

Health monitor debug

Command	Description
`get hmon interface-monitoring`	Show health monitor interface monitor instance.
`get hmon hchk`	Show health monitor health check instance.
`execute hmon interface-monitoring <interface>`	Run interface monitor health check on certain interfaces.
`execute hmon hchk protocol ping <-I interface> target`	Run health check on certain interfaces with ping protocol.
`execute hmon hchk protocol http [<port <portnum>] [http-get <url>] [<-I interface>] target`	Run health check on certain interfaces with http protocol.
`execute hmon hchk protocol dns <-I interface> target`	Run health check on certain interfaces with DNS protocol.

VPN

Command	Description
`get vpn ipsec configurations`	Show IPSec VPN configurations.
`get vpn ipsec tunnel details`	Show IPSec VPN tunnel information.
`get vpn ipsec tunnel name <Tunnel_name>`	Show IPSec VPN tunnel names.

Command	Description
`get vpn ipsec negotiation error`	Show IPSec VPN negotiation errors.
`get vpn certificate ca details`	Show VPN CA certificate details.
`get vpn certificate local details`	Show VPN local certificate details.
`execute vpn certificate ca import tftp <remote_file> <local_name> <ip>`	Import CA certificate from TFTP server.
`execute vpn certificate local import tftp <remote_file> <local_name> <ip> <passwd>`	Import local certificate from TFTP server.

LTE/modem state debug

Command	Description
`get modem status`	Show the modem connection status.
`get modem firmware-version`	Show the modem firmware version.
`get modem data-usage`	Show the current data usage on each modem and SIM.
`get lte carrier <mcc_num> <mnc_num>`	Show the carrier information with query to MCC and MNC combination.
`get lte plan`	Show the LTE plan entries.
`get lte service`	Show the LTE service.
`get lte sim-imsi-record`	Show the SIM IMSI records.
`execute dmlog filter show`	Show dmlog filter files.
`execute dmlog filter add`	Add dmlog filter files.
`execute dmlog filter delete`	Delete dmlog filter files.
`execute dmlog start modem1`	Run dmlog debug info collection on modem 1.
`execute dmlog export tftp`	Export dmlog debug information to TFTP server.

Command	Description
`execute modemfw get tftp`	Get modem firmware via TFTP.
`execute modemfw delete`	Delete modem firmware.
`execute modemfw upgrade`	Upgrade modem firmware.
`execute modemfw show`	Show modem firmware version check.
`execute modemfw getIMEI`	Get modem IMEI number.
`execute modemfw AtTest`	Run modem AT command test.
`execute modemfw checkSIM`	Perform detection of SIM slot.
`execute modemfw playCW`	Play continuous waveform radio.
`execute modemfw create`	Load modem firmware from TFTP to flash.
`execute modemfw show-profiles`	Display profiles in modem.
`execute modem data-usage clear`	Clear data usage for specific modem or SIM card.
`execute modem data-usage set sim <imsi> <usage in megabyte>`	Manually set SIM's data usage in megabytes.
`execute modem show-log latest modem1| modem2| all`	Print modem's latest log.
`execute modem delete-sim-record modem1|modem2 all| imsi [xxxx]`	Delete SIM IMSI record from database.
`execute modem modem1|modem2 sim1|sim2 puk unlock <puk_code> <new_sim_pin>`	Unlock SIM with new SIM pin code.
`execute minicom /dev/ttyUSBX [at-cmd]`	Run modem's AT command.
`execute sim-switch modem1|modem2`	Run manual SIM switch on modem 1 or modem 2.

RADIUS authentication debug

Command	Description
`execute debug FNBAMD <command>`	Fortinet non-blocking Authentication Daemon (FNBAMD) is used to communicate with a remote authentication server. This shows RADIUS authentication related messages such as what packets the FortiExtender sends to which RADIUS server and what response the FortiExtender received. • `error`: error • `info`: information • `todo`: need to be implement • `dbg`: debug level 1 • `fatal`: fatal error • `warning`: warning • `trace`: trace • `config`: fnbamd config • `auth_state`: fnbamd auth state info • `radius`: fnbamd RADIUS related info • `admin_info`: fnbamd admin related info

Packet sniffer (tcpdump)

Command	Description
`execute tcpdump -i <interface>`	Start packet capture on certain interface.
`execute tcpdump host <ip>`	Start packet capture to certain host.

Troubleshooting Scenarios

This section covers common troubleshooting scenarios you may encounter.

Cloud mode

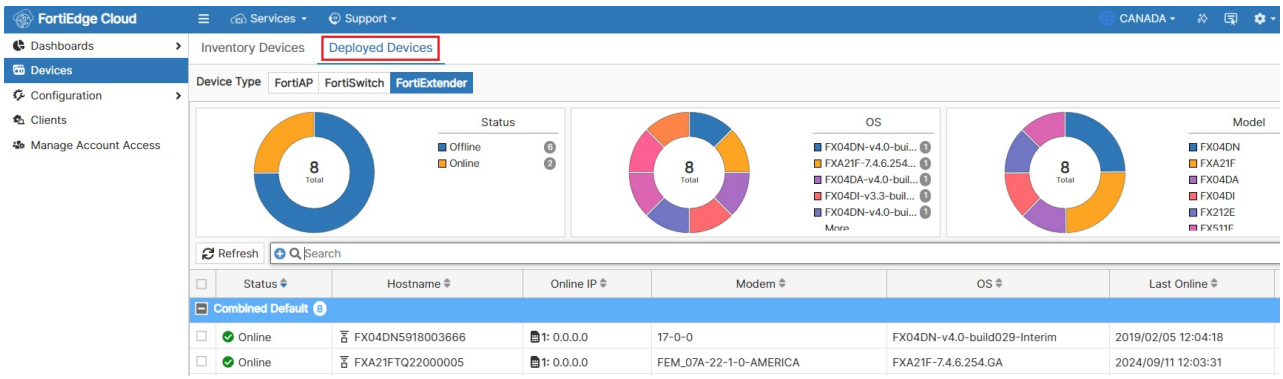
This section covers troubleshooting scenarios when using FortiEdge Cloud to manage your FortiExtenders.

Failure to deploy on FortiEdge Cloud

1. Ensure that the FortiExtender has the correct configurations for cloud mode:
   a. Set `discovery-type` to `cloud` or `auto`.
   b. Verify the dispatcher address is correct: `fortiextender-dispatch.forticloud.com`.
   c. Verify the `dispatcher-port` is correct: default value `443`.

```
config system management
  set discovery-type cloud
  config cloud
    set dispatcher fortiextender-dispatch.forticloud.com
    set dispatcher-port 443
  end
end
```

2. Make sure the device in FortiEdge Cloud is deployed with a profile. The device in FortiEdge Cloud should be in the *Deployed Devices* tab, not in the *Inventory Devices* tab.



3. Verify the FortiExtender can connect to the internet:

a. Using the FortiExtender CLI, check that the device can successful ping 8.8.8.8.
If not, check the FortiExtender LTE/WAN connection.

b. Using the FortiExtender CLI, ping the cloud domain name.
It should return a correct IP address like 66.35.19.33. If not, it could be a FortiExtender DNS issue.

```
FXA21FTQ22000005 # execute ping fortiextender-dispatch.forticloud.com
PING fortiextender-dispatch.forticloud.com (66.35.19.33): 56 data bytes
^C
^C
--- fortiextender-dispatch.forticloud.com ping statistics ---
10 packets transmitted, 0 packets received, 100% packet loss
FXA21FTQ22000005 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=58 time=9.792 ms
64 bytes from 8.8.8.8: seq=1 ttl=58 time=9.711 ms
64 bytes from 8.8.8.8: seq=2 ttl=58 time=9.641 ms
64 bytes from 8.8.8.8: seq=3 ttl=58 time=9.675 ms
64 bytes from 8.8.8.8: seq=4 ttl=58 time=9.620 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 9.620/9.687/9.792 ms
```

4. Verify that the FortiExtender EXTD process is running and working well:

a. From the FortiExtender CLI, enter `get system app-status`.
The `EXTD` state should be `RUNNING`.

```
FX511FTQ21001152 # get system app-status s
          name                 type          command      pid    state
       SYSLOGD        APP_T_MONIPID          syslogd     1115  RUNNING
        CONFIG          APP_T_INFRA      json_config     1119  RUNNING
         ZEBRA        APP_T_MONIPID            zebra     1120  RUNNING
         OSPFD        APP_T_MONIPID            ospfd     1122  RUNNING
          NETD          APP_T_INFRA            netd     1125  RUNNING
          EXTD        APP_T_MONIHB       extenderd     1356  RUNNING
           GUI          APP_T_MONIHB            kore     1366  RUNNING
          HMON        APP_T_MONIPID            hmon     1365  RUNNING
     IPSEC_START        APP_T_MONIPID         starter     1375  RUNNING
        IPSECD         APP_T_MONIHB          ipsecd     1379  RUNNING
    FIREWALLD         APP_T_MONIHB       firewalld     1387  RUNNING
         PIMD         APP_T_MONIHB            pimd     1389  RUNNING
        SNMPD         APP_T_MONIHB           snmpd     1399  RUNNING
        TEAMD         APP_T_MONIHB           teamd     1404  RUNNING
       ROUTED         APP_T_MONIHB          routed     1408  RUNNING
         SSHD        APP_T_MONIPID            sshd     1423  RUNNING
      TELNETD        APP_T_MONIPID         telnetd     1352  RUNNING
      CONNMGR     APP_T_MONIHB_EXG         connmgr     1428  RUNNING
         QOSD         APP_T_MONIHB            qosd     1434  RUNNING
    DNSPROXY         APP_T_MONIHB        dnsproxy     1437  RUNNING
        XDSLD     APP_T_MONIPID_EXG           xdsld     1446  RUNNING
       DHCPC          APP_T_MONIHB           dhcpc     1452  RUNNING
FX511FTQ21001152 # execute restartapp EXTD
FX511FTQ21001152 #
```

5. Try restarting the EXTD process to initialize the cloud connection.

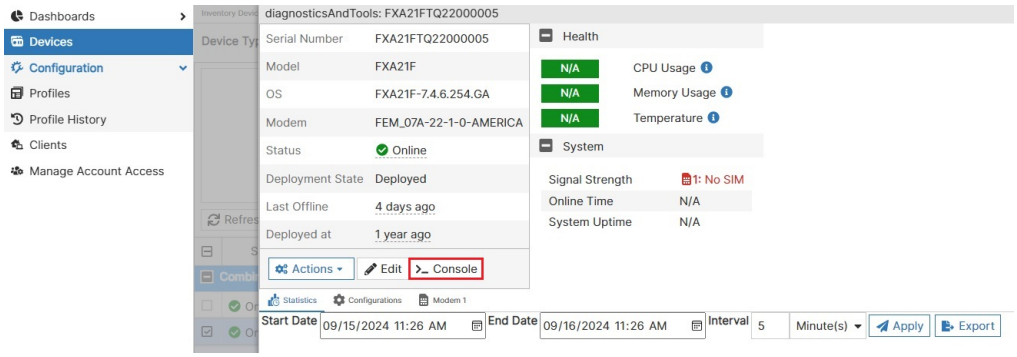
a. From the FortiExtender CLI, enter `execute restartapp EXTD`.

6. From the FortiExtender CLI, run `get extender status` to check the cloud connection status.
The `management-state` should change from `CWWS_CLD_CONN/CWWS_SULKING` to `CWWS_RUN`.

```
FX511FTQ21001152 # get extender status
Extender Status
    name                : FX511FTQ21001152
    mode                : CLOUD
    fext-addr           : 0.0.0.0
    ingress-intf        :
    fext-wan-addr       : 166.253.42.215
    controller-addr     : fortiextender-dispatch.forticloud.com:443
    deployed            : true
    account-id          : 0
    management-state    : CWWS_CLD_CONN
    base-mac            : 94:FF:3C:0D:1A:C0
    network-mode        : nat
    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
FX511FTQ21001152 # get extender status
Extender Status
    name                : FX511FTQ21001152
    mode                : CLOUD
    fext-addr           : 166.253.42.215
    ingress-intf        : lte1
    fext-wan-addr       : 166.253.42.215
    controller-addr     : fortiextender-dispatch.forticloud.com:443
    deployed            : true
    account-id          : 1282046
    uptime              : 0 days, 0 hours, 0 minutes, 0 seconds
    management-state    : CWWS_RUN
    base-mac            : 94:FF:3C:0D:1A:C0
    network-mode        : nat
    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
```

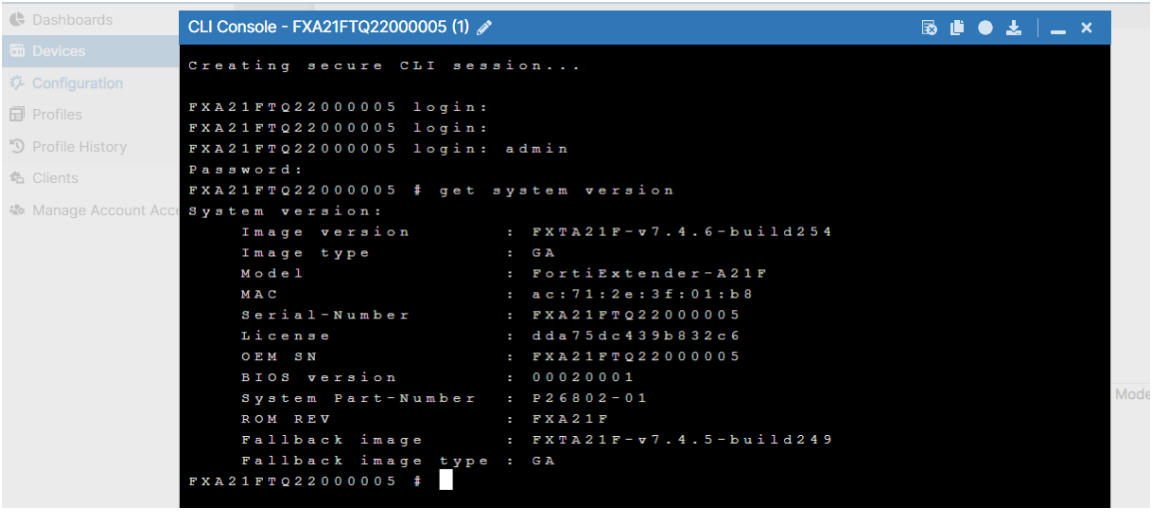
Device stuck in sulking/syncing state

1. Use the FortiEdge Cloud's browser console to connect to the FortiExtender.
   a. Go to *Device* > *Deployed Devices* and double-click the FortiExtender you want to connect to.
   b. In the *Diagnostic And Tools* view, click >_*Console* to open the browser console window.

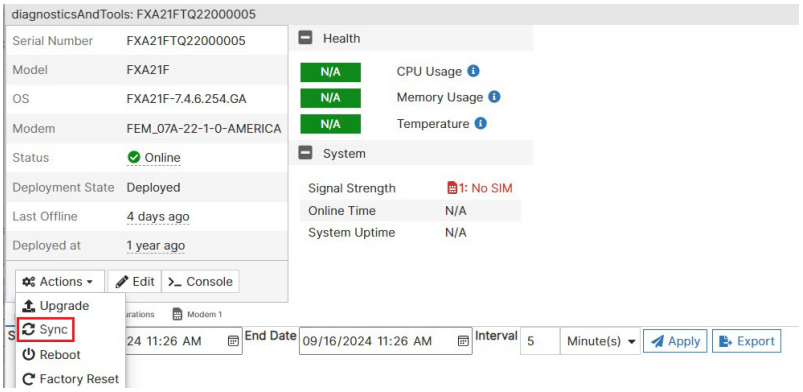


   c. Try running some commands from the console window, if it is not successful, check the FortiExtender's internet

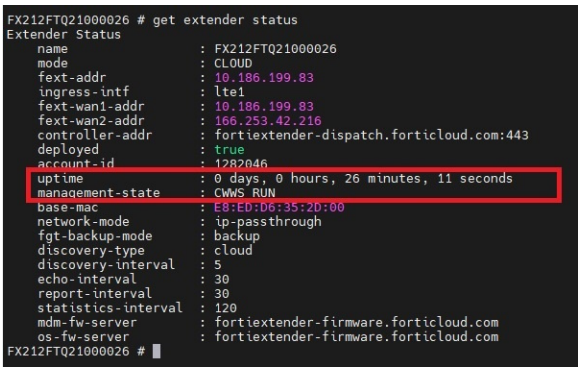
connection and status.



2. Try to sync the device from FortiEdge Cloud.
   a. Go to *Device* > *Deployed Devices* and double-click the FortiExtender you want to connect to.
   b. Select *Actions* > *Sync* and then click *OK* to confirm.



3. Verify that the FortiExtender has a stable connection with FortiEdge Cloud.
   a. From the FortiExtender device, access the CLI and run `get extender status` to check the `management-state` and `uptime`.
   b. The `management-state` should be in `CWWS_RUN` status while the uptime should be greater than two minutes.



4. Check the FortiExtender network latency. If the network has high latency, the FortiExtender will have problems synchronizing with the cloud.

```
FX212FTQ21000026 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=113 time=165.522 ms
64 bytes from 8.8.8.8: seq=1 ttl=113 time=31.413 ms
64 bytes from 8.8.8.8: seq=2 ttl=113 time=54.153 ms
64 bytes from 8.8.8.8: seq=3 ttl=113 time=29.971 ms
64 bytes from 8.8.8.8: seq=4 ttl=113 time=37.727 ms
64 bytes from 8.8.8.8: seq=5 ttl=113 time=45.525 ms
64 bytes from 8.8.8.8: seq=6 ttl=113 time=29.247 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 29.247/56.222/165.522 ms
FX212FTQ21000026 #
```

5. Try resetting the cloud connection from FortiExtender.
   a. From the FortiExtender CLI, enter `execute restartapp EXTD`.

FortiGate managed mode: WAN-Extension and LAN-Extension

This section covers troubleshooting scenarios when using FortiGate managed FortiExtenders in WAN-Extension and LAN-Extension modes.

FortiExtender entries not generated automatically on FortiGate

1. Check the FortiExtender `discovery-type` is set to `FortiGate` or `auto` mode.
2. Check the FortiExtender `discovery-intf` can ping FortiGate's control port, which connects to FortiExtender. The FortiGate should also be able to ping back to FortiExtender.
3. If ping fails, check whether the interface on FortiExtender and FortiGate are up and connected properly with the correct IP address and netmask.
4. Check if CAPWAP traffic is allowed and that Fabric is set in the allowaccess list on the FortiGate control port.

WAN-Extension can't reach the CWWS_RUN state after FortiGate authorizes FortiExtender

1. Turn on `execute debug EXTD ac_disc on` to check if the `discovery-intf` setting is correct.
2. Check that `DISCOVERY_REQ` and `DISCOVERY_RESP` respond properly. For more details, refer to execute debug EXTD ac_disc on on page 38 in Appendix A.

WAN-Extension is established and stays in CWWS_RUN state after set authorized enable on FortiGate, but the FortiGate fext-wan interface does not get IP address

1. Check the FortiExtender to see if it has a working SIM inserted.
2. Check the FortiExtender `get modem status` output to see if the modem is in the `connected` state.
3. If the preceding steps both work, check the following:
   a. When operating in CAPWAP IP-passthrough mode, check if the CAPWAP interface is automatically created in the system interface.
   b. When operating in VLAN IP-passthrough mode, check if the VLAN interface is automatically created in system interface.

4. Check FortiExtender to see if vitual-wire-pair configuration is automatically created and if the mapping is correct.
5. If the issue still persists, on FortiGate, capture packets on the FortiGate fext-wan interface or vlan interface by running `execute system interface dhcp-renew`. Check if DHCP packets can be captured on both the FortiGate side and FortiExtender side.
6. Turn on debug and collect the debug log output to file a ticket for technical support:

```
execute debug EXTD info on =>  this will show the capwap control channel work flow
execute debug NETD info on
execute debug CONNMGR connection on
execute iptables-save
get extender status
```

Failure to ssh/https/telnet to the virtual interface

1. Check that the virtual interface has allowaccess enabled for ssh/https/telnet.
2. Check the proper routing table by running `execute iptables-save`.

LAN-Extension is established and stays in CWWS_RUN state, but the VPN tunnel is not up

1. Check VPN IPSec phase1-interface configuration.
2. Check VPN IPSec phase2-interface configuration.
3. Get VPN IPSec negotiation error.
4. Execute debug IPSECD error/info.

LAN-Extension is established and stay in CWWS_RUN state, but the le-switch can't get IP address

1. Check that DHCP is enabled and configured properly on FortiGate.
2. Check the firewall policy configuration on FortiGate.
3. Check if FortiExtender related configurations are pushed from the FortiGate controller and if the IPSec VPN tunnel is established.
4. FortiExtender should display vxlan, aggregate, switch-interface after steps 1 and 2. If not, turn on the following debug output to collect more information:

```
execute debug EXTD fgvsp on => this output will show vxlan, aggregate, switch-intf,
firewall policy
get system aggregate-interface status
get vpn ipsec configurations
get vpn ipsec negotiation error
get vpn ipsec tunnel details
```

The client failed to send data correctly

Executing a packet capture show what packet is received from related interfaces.

1. On FortiGate, run `diagnose sniffer packet $intf 'port 5246`
2. On FortiExtender, run `execute tcpdump -I $intf port 5246`, where `$intf` is the discovery interface in FortiExtender's config system management > config fortigate > set discovery-intf.

CAPWAP Control Channel state machine

This section lists the definitions for the various statuses within the `get extender status output (CWWS_RUN).`

`CWWS_IDLE`	The IDLE state indicates that the initialization is complete and the start of the CAPWAP state machine.
`CWWS_DISCOVERY`	FortiExtender sends out the discovery request and waits for the FortiGate's responses.
`CWWS_AC_SELECT`	FortiExtender selects a FortiGate to connect to based on the response time.
`CWWS_DTLS_SETUP`	FortiExtender invokes the DTLSStart command which starts the DTLS session establishment with the chosen FortiGate and waits for the result.
`CWWS_DTLS_AUTHORIZE`	FortiExtender performs an authorization check against the FortiGate's credentials.
`CWWS_DTLS_CONN`	FortiExtender has successfully authorized the FortiGate's credentials indicating that the DTLS session was successfully established.
`CWWS_JOIN`	FortiExtender enters the join state by transmitting the join request to the FortiGate.
`CWWS_IMAGE`	FortiExtender enters the image state when it receives a successful join response message and determines that the software version in the image identifier message element is not the same as its currently running image.
`CWWS_CONFIG`	FortiExtender enters the configure state when it receives a successful join response message and determines that the included image identifier message element is the same as its currently running image. FortiExtender then transmits the configuration status request message to FortiGate.
`CWWS_DATA_CHECK`	FortiExtender enters this state when it receives a successful configuration status response message from the FortiGate. FortiExtender then transmits the change state event request message to FortiGate.
`CWWS_RUN`	FortiExtender enters this state when it receives a successful change state event response message from the FortiGate, indicating that the CAPWAP session was successfully established.
`CWWS_DTLS_TD`	This state transition occurs when the retransmit counter has reached the MaxRetransmit count, or when an error has occurred in the DTLS stack, causing the DTLS session to be torn down.
`CWWS_SULKING`	The SULKING state provides the silent period, minimizing the possibility for Denial-of-Service (DoS) attacks.

FortiExtenders in standalone mode

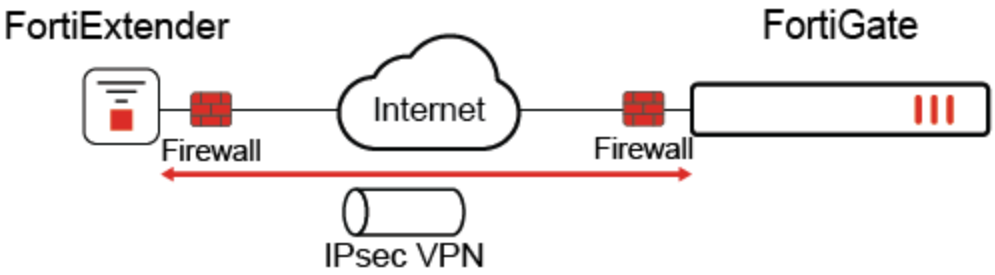
This section covers common troubleshooting scenarios when using FortiExtenders deployed in standalone mode.

Using IPsec VPN to connect branch offices (FortiGate)

The VPN configuration process consist of the following steps:

1. Configure phase-1 parameters.
2. Configure phase-2 parameters.
3. Configure firewall policies.
4. Configure route.

Failure to establish a VPN tunnel with a peer party

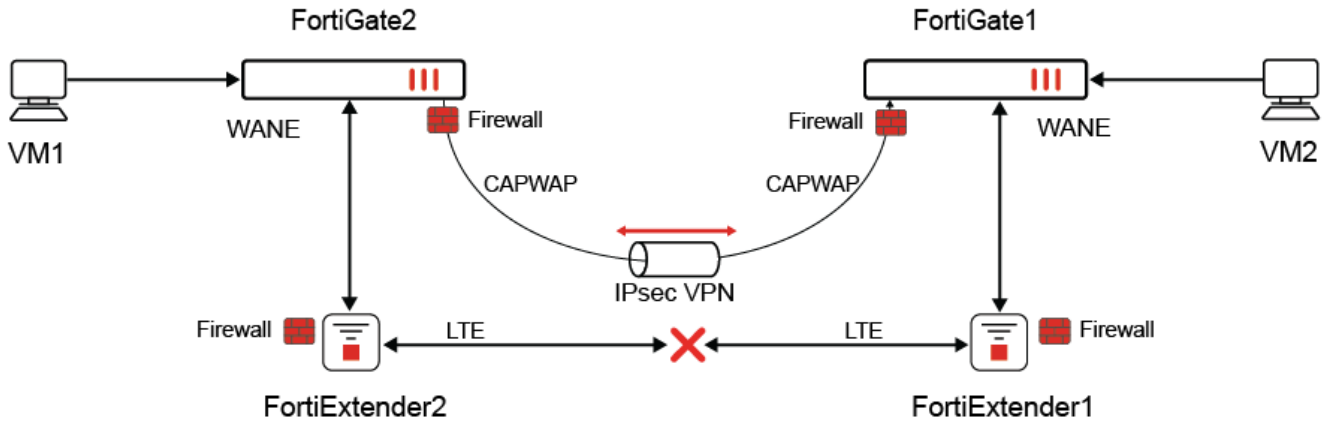


Failure to establish a VPN connection is usually related to mismatching VPN tunnel configurations or a disconnected underlay network. To troubleshoot:

1. From the FortiExtender, check if the remote peer gateway is reachable by issuing commands:
   - `execute tcpdump`
   - `execute ping`
2. Check if there is a configuration mismatch between local and remote parties.
   a. Run `get vpn ipsec negotiation error`. The error message might provide additional information.
   b. From the FortiExtender GUI, navigate to *Logs* > *VPN* and read the relevant message.
   Look for the error details to determine if the error occurred during phase1 or phase2.
   - If the error occurred during phase1, check the VPN phase1-interface configuration.
     The mismatched configuration is most likely in the IKE version, pre-shared secret/certification, or proposals.
   - If the error occurred during phase2, check the VPN phase2-interface configuration, firewall policies, and traffic selector pairs.

It is important to check the relevant firewall policies. If firewall rules are missing on the remote FortiGate peer side, the VPN might not come up.

Unstable VPN link over LTE with peer FortiGate



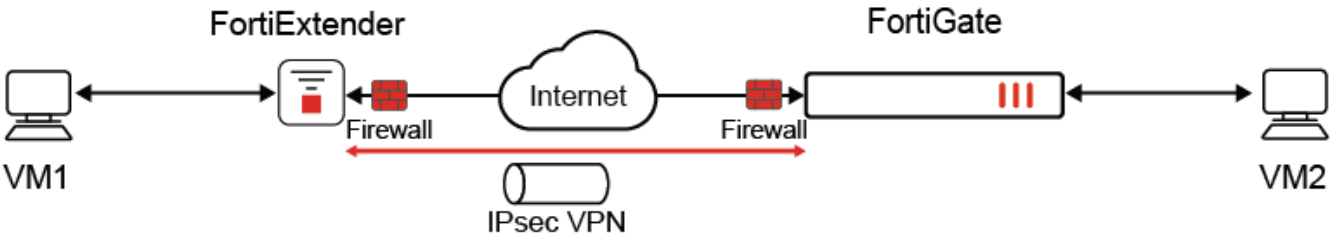
An unstable VPN link usually indicates that the underlay network connection is of reduced quality, such as having a link go down or an interface IP change. When the IPsec VPN tunnel is over LTE, you can run ping command towards an Internet address such as 8.8.8.8 to test LTE link stability:

```
# execute ping <Internet_IP_address>
```

Depending on the carrier setting, the LTE connection IP might be occasionally renewed, which could trigger an IPSECD process to renegotiate.

If the FortiExtender is acting as a FortiGate WAN Extension and an IPsec tunnel went through FortiExtender/LTE but terminated at FortiGate, you can check the FortiGate *VPN Events* log to see if the tunnel up/down events are related to a LTE link state change. Meanwhile, you can also examine the IPSec configurations such as the phase1 DPD setting and phase2 auto-negotiate enabling.

No outgoing or incoming packets via the tunnel



To allow traffic to pass through an IPSec VPN, the phase2 traffic selector/route and relevant firewall policy needs to be properly configured. Traffic selectors are used for routing desired traffic through the VPN tunnel. Data traffic is then checked by the firewall. If the VPN link is up but expected data is not passing through, you should examine the relevant traffic selectors and firewall policy configuration on both sides. Look for conflicting routes or firewall rules. You can sniff traffic using *tcpdump* to see where the traffic goes.

To further investigate IPSec issues, you can turn on the process "IPSECD" for debugging. This prints more details to the console or file.

To enable IPSECD debugging:

```
# execute debug IPSECD              # check which IPSEC sub-modes are on
# execute debug IPSECD ike on       # turn on IKE debugging
# execute debug log-to-console on   # print IPSECD logs to console
# execute debug log-to-console off  # turn-off console logs
# execute debug clear               # clear all debug info
```

Virtual WAN link, load balance, and failover/failback

The `get VWAN status` returns an empty output

1. Virtual VWAN only functions when FortiExtender operates in NAT mode. Check the network mode in `get extender status` to confirm that NAT mode is configured.
2. Check configurations under `system virtual-wan interface` to see if the type, members, and status are correctly configured
3. Check configurations under `system vwan-member` to see if the target and health check event is correctly linked.

No link load balance is seen in the virtual WAN interface

1. While running traffic, use the command `get vwan status` to check the link data usage. Issue the command several times to see the increments of incoming and outgoing data. An active member is expected to be seen with an increasing amount of incoming and outgoing packets.
2. Check the member's health status with the command `get hmon hchk <instance>` to see if all members are alive.
3. Check that related firewall and routing policies allow the virtual wan interface to pass and steer traffic.

   Example firewall and routing policy configuration:

```
config firewall policy
    edit vwan_permit_out
        set srcintf any
        set dstintf vwan1
        set srcaddr lan
        set dstaddr all
        set action accept
        set status enable
        set service ALL
        set nat disable
    next
    edit vw_mb1_nat
        set srcintf any
        set dstintf wan
        set srcaddr lan
        set dstaddr all
        set action accept
        set status enable
        set service ALL
        set nat enable
    next
    edit vw_mb2_nat
```

```
            set srcintf any
            set dstintf lte1
            set srcaddr lan
            set dstaddr all
            set action accept
            set status enable
            set service ALL
            set nat enable
        next
    end
    config router policy
        edit to_vwan
            set input-device
            set srcaddr lan
            set dstaddr all
            set service ALL
            set target target.vwan1
            set status enable
            set comment
        next
    end
```

Modem/LTE sessions

General steps to take when noticing LTE connection errors

1. Verify the APN configuration is correct and consistent with what the carrier provided.
   Run `AT+CGDCONT?` to show the list of profiles and APNs.
2. Verify that the allotted data from the SIM's plan is still available.
3. Verify that the SIM card has established a successful connection before (not necessarily in a FortiExtender).
   a. If you have a new SIM card, try enabling the `pause-modem-manager` for at least 300 seconds.
   b. Try inserting the SIM card into a different SIM slot to see if it's a hardware issue with that particular SIM slot.
4. Verify that the antennas have been properly attached to the FortiExtender device.
5. Check the error message in the `get modem status` output.
6. Upgrade or downgrade to the most recent GA OS image and modem firmware image, and then try to establish an LTE connection.
7. If possible, try and see if a connection can be established with a SIM card from a different carrier.
8. Check if the problem persists after a device reboot or manual power cycle.
9. There are two common `get modem status` errors:
   - 209 - ERR PDN IPV4 CALL THROTTLED: V4 PDN is in a throttled state due to previous VSNCP bring up failure(s). The time for which the IPv4 PDN is throttled is determined by the IPv4 throttling timers maintained in the profile.
     i. Usually you would need to check the APN or the provisioning with the carrier first.
   - 1204 error PS not attached state.
     i. Usually due to an incorrectly configured APN.

Modem is in not insert state

1. If the modem is showing up as not inserted, check the `lsusb` output.
   The expected values should include 2c7c/800 or 2c7c/900.
2. Check `dmesg` output.
   a. Check the OS image version and upgrade to 7.2.3 GA if necessary.
3. To restore the modem to a normal status, power off the FortiExtender device completely and wait 2+ minutes before powering on.
4. If possible, manually remove the modem and then replace it. Check the status again.
5. The modem is usually expected to recover after running these steps. If the issue persists, contact Fortinet Support and provide the device mode, SN, and debug logs.

Modem is in start session state

1. Confirm if the SIM card is working and correctly provisioned your ISP carrier.
   You can cross-check by inserting the SIM into a mobile device and see if it dials up correctly.
2. Confirm in config LTE plan that there is a corresponding data plan configured for the SIM card.
   Verify the APN field matches the one provided by your ISP carrier.
3. Check if the plan is correctly applied by running `get modem status`.
   Verify the name in the data plan field matches your configured plan.
4. Check the modem firmware package version to ensure that it is the package downloaded from Fortinet support site.
   To check the modem version, use `get modem firmware-version`.
5. Check the signal strength to ensure FortiExtender is placed at location with strong reception.
6. Remove and reinsert the SIM to start a modem state machine re-initialization.
   Wait for the modem status to change from *init*, to *select sim*, to *start session*, and then to *connected*.
7. Collect the debug logs and connection manager logs for further investigation.

Modem failure code

When using general or customized SIMs across various locations, different modem failure codes will occur. Raise a ticket with the Fortinet support team and attach the failure code along with debug logs and dmlogs for further analysis.

SIM switch failure/timeout

1. If the modem is switching between two SIM cards while unable to maintain connection to one, try and see if the LTE connection is stable with just one SIM card
2. Manually trigger the SIM switch using CLI command `execute sim-switch modem[1|2]`.
3. Check that the modem firmware being used is the latest.

Modem firmware upgrade failure

1. After rebooting the FortiExtender device, you can try a different modem firmware upgrade method (via Cloud portal, tftp, FortiExtender GUI, etc.) if those options are available.

2. If the platform uses a Sierra modem, the individual modem firmware files may be uploaded and configured in the LTE section, Carrier subsection.
3. The *execute modemfw show all* command shows all the modem firmware files currently on the FortiExtender device.
   a. `AT!IMPREF?` can show the current firmware version and modem status

If the errors persist, the following steps may be taken to collect more information:

4. Run `execute debug CONNMGR state on` or the more verbose `execute debug CONNMGR info on` to collect debug logs for the modem
   a. Use `execute debug clear` to end log collection.
   b. Use `execute debug log-to-console` if the connection is not a serial one.
5. From the FortiExtender GUI, the LTE section has a dmLog subsection.
   a. From there, a log of the modem info can be manually collected and then exported for customer support team analysis.

FortiExtender LTE Error Codes

This section explores some of the more commonly seen error messages from FortiExtenders using LTE connection. Although the exact cause of the error messages may require further analysis, here are some common causes and available solutions.

The verbose error message in `get modem status` helps provide insight about the potential causes behind connectivity issues.

Error Messages

If the `get modem status` output is stuck in one of the following:

`CONN_STATE_MDM_INIT`	1. Try to physically re-insert the SIM card into the FortiExtender. 2. Verify the SIM can be detected and connects successfully in a different device (e.g. phone)
`CONN_STATE_MDM_INIT [AGENT_MDM_RESETTING]`	1. If the FortiExtender cannot recover on its own after a reasonable period of time, manually reboot the device.
`CONN_STATE_FAILURE_SAFE [AGENT_MDM_RESET_ POWEROFFING]`	This occurs after the modem exhausts a set number of tries to connect to the network. 1. You may need to manually reboot the device if access to AT commands is restricted.
`CONN_STATE_DISCONNECTED`	This is a known issues that specifically affects T-Mobile plans using band 41 1. Disable using AT commands.

If the `event lte sim read` failed before the start session, `result=AGENT_ERR_AT_COMMAND(30)`

1. Ensure the FortiExtender has been upgraded to latest GA OS firmware.

If the `get modem status` output is stuck in `CONN_STATE_START_SESSION`:

```
failure code: CallFailed
failure reason: 1 - Reason unspecified, check the verbose call end reason
failure type: 2 - Internal
verbose reason: 209 - ERR PDN IPV4 CALL THROTTLED: V4 PDN is in throttled state due to
previous VSNCP bring up failure(s). The time for which the IPv4 PDN is throttled is
determined by the IPv4 throttling timers maintained in the profile
```

1. Ensure the APN is configured correctly.
2. Ensure the SIM is provisioned correctly.
3. Verify there are no recent changes in the billing plan.
4. Ensure the SIM works in a different device (e.g. phone).
5. If the carrier requires profile 1 specifically, enable `default-profile` in the configuration of the relevant lte carrier.
6. Try enforcing IPv4 only in lte setting configurations by enabling force-ipv4.

```
verbose reason: 1204 - ERR PS not attached state
```

1. Ensure the APN is configured correctly.

```
failure code: 1014 - Call Failed
failure type: 3 - Call Manager defined
verbose reason: 1078 - UNKNOW CER
PS state : PS_Detached [profile 1]
```

1. Could be related to the modem having issues registering with the network.
2. Ensure `default-profile` is enabled in lte carrier configuration.
3. Ensure the APN is correctly configured.

```
verbose reason: 2001 - NO SRV: data call is brought down because traffic channel request
got rejected by CM(Call
Manager) since device has no service
```

1. Could be caused by incorrect carrier identification. You can configure specific mcc mnc in lte simmap configuration.

```
failure code: 0
failure reason: 0 - confirm the connection failed
failure type: 0 -
verbose reason: 0 -
```

1. Try enforcing `LTE-only` mode, no 5G.

Constant `Find a new SIM IMSI:[imsi], try to activate it, please wait 300 seconds. . . . . . . . . . .`

1. May need to configure a longer activation period in lte setting configuration, particularly if this SIM has not been used before.
2. If activation issues persist, try physically re-inserting it into the same SIM slot, or a different SIM slot on the FortiExtender device.

For FortiExtender devices with Quectel modems, the output of AT command AT+CEER can be cross-referenced with the Quectel LTE Standard Error Code for error codes not listed here.

Primary DNS Service and Interface as DNS Service

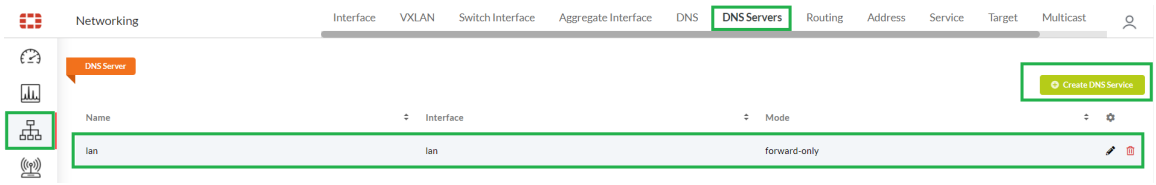
This section covers common troubleshooting scenarios relating to Primary DNS Service and Interface as DNS Service.

Client fails to get DNS service

1. Check the DNS service configuration.
   - From the CLI:

     ```
     config system dns-server
       edit lan
         set interface lan
         set mode forward-only
       next
     end
     ```

   - From the GUI:
     i. From the FortiExtender GUI, go to *Networking* > *DNS Servers* and click *Create DNS Service* to edit.

2. Check the DNS server pool through the CLI command `get system dns`.
   There must be a primary DNS server, a secondary DNS server, or Acquired DNS servers as depicted in the following example:

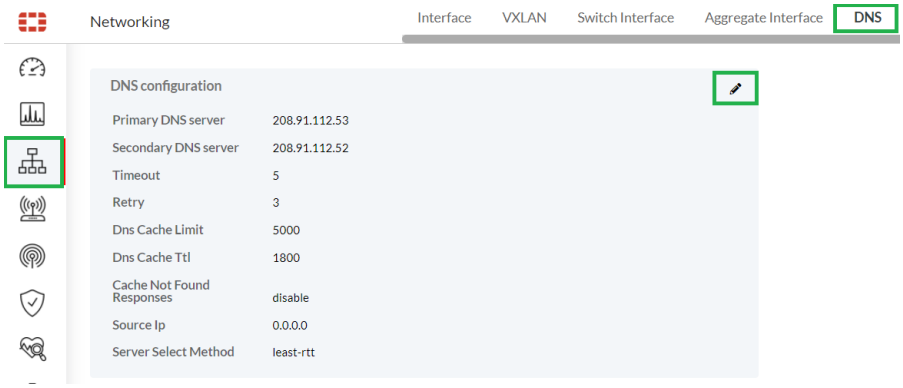
   ```
   FX211E5920002402 # get system dns
   primary                : 208.91.112.53
   secondary              : 208.91.112.52
   timeout                : 5
   retry                  : 3
   dns-cache-limit        : 5000
   dns-cache-ttl          : 1800
   cache-notfound-responses: disable
   source-ip              : 0.0.0.0
   server-select-method   : least-rtt
   acquired servers       :
       lte1:   10.177.0.34, 10.177.0.210
   ```

3. If there are no primary or secondary DNS server configured, you must configure them.
   - To configure a primary or secondary DNS server via the CLI:

     ```
     config system dns
       set primary 208.91.112.53
       set secondary 208.91.112.52
     end
     ```

   - To configure a primary or secondary DNS server via the GUI:
     From the FortiExtender GUI, go to *Networking* > *DNS* and click *Edit* to configure the primary/secondary DNS

server.



DNS resolution fails to use designated DNS servers

When designating a DNS servers for domain naming address resolution, you can configure a designated DNS server, as shown in the following examples:

```
FX211E5920002402 # config system dns
FX211E5920002402 (dns) # show
config system dns
    set primary 208.91.112.53
    set secondary 208.91.112.52
    set timeout 5
    set retry 3
    set dns-cache-limit 5000
    set dns-cache-ttl 1800
    set cache-notfound-responses disable
    set source-ip 0.0.0.0
    set server-select-method least-rtt
end
```

1. Set the primary and secondary servers:

   ```
   FX211E5920002402 (dns) # set primary 1.1.1.1
   FX211E5920002402 (dns) <M> # set secondary 8.8.8.8
   ```

2. After updating the DNS servers, check the DNS pool.

   Designated DNS servers must be presented in system DNS pool, as shown in the following:

   ```
   FX211E5920002402 (dns) # set primary 1.1.1.1
   FX211E5920002402 (dns) <M> # set secondary 8.8.8.8
   FX211E5920002402 (dns) <M> # end
   FX211E5920002402 # get system dns
   primary                 : 1.1.1.1
   secondary               : 8.8.8.8
   timeout                 : 5
   retry                   : 3
   dns-cache-limit         : 5000
   dns-cache-ttl           : 1800
   cache-notfound-responses: disable
   source-ip               : 0.0.0.0
   server-select-method    : least-rtt
   ```

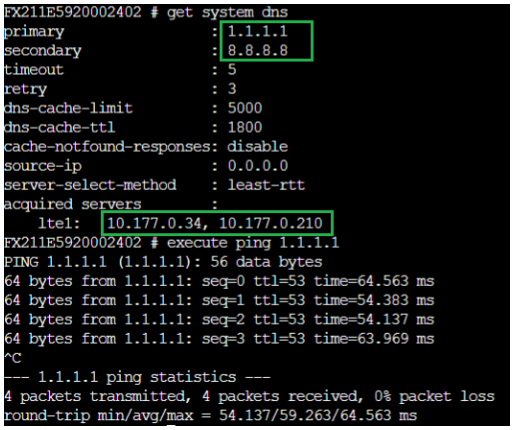
```
acquired servers        :
    lte1:   10.177.0.34, 10.177.0.210
```

Slow DNS Service

1. Check the DNS cache setting:

```
config system dns
  set dns-cache-limit 5000
  set dns-cache-ttl 1800
end
```

2. Check the performance of DNS servers in the DNS server pool through the CLI command `get system dns`:
   Use ping or route trip to check the performance of DNS servers. If the DNS server is slow, change it to a faster server.



Failure to get domain resolution from local DNS entries

1. Check the DNS service mode.

```
config system dns-server
  edit lan
    set interface lan
    set mode recursive
  next
end
```

   The `recursive` and `non-cursive` service modes can access the DNS database.

   In `forward-only` mode, the interface does not access the DNS database and instead redirects the DNS request to an external DNS server.

2. Check the DNS database view type.

```
config system dns-server
  edit banana.com
    set view shadow
  next
end
```

In `recursive` mode, the first priority is to access the shadow DNS database, and if there is no domain naming solution, it then forwards to the system DNS servers.

In `non-recursive mode`, it first accesses the public DNS database, if there is no naming solution, then the DNS service returns no solution.

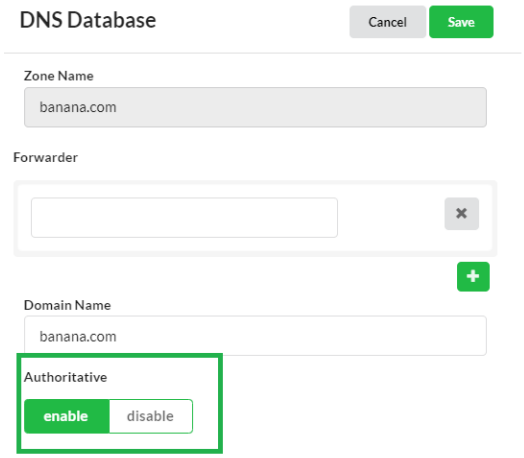
Failure to provide local domain naming service as the Authoritative Server

Check that `authoritative` is enabled.

- Using the CLI:

```
config system dns-server
  edit banana.com
    set authoritative enable
  next
end
```

- Using the GUI:
  a. From the FortiExtender GUI, go to *Networking* > *DNS Servers* and click *Edit* in *DNS Database*.
  b. Check if *Authoritative* is set to *enable*.



Virtual Router Redundancy Protocol for redundant internet service

This section covers common troubleshooting scenarios relating to Virtual Router Redundancy Protocol (VRRP).

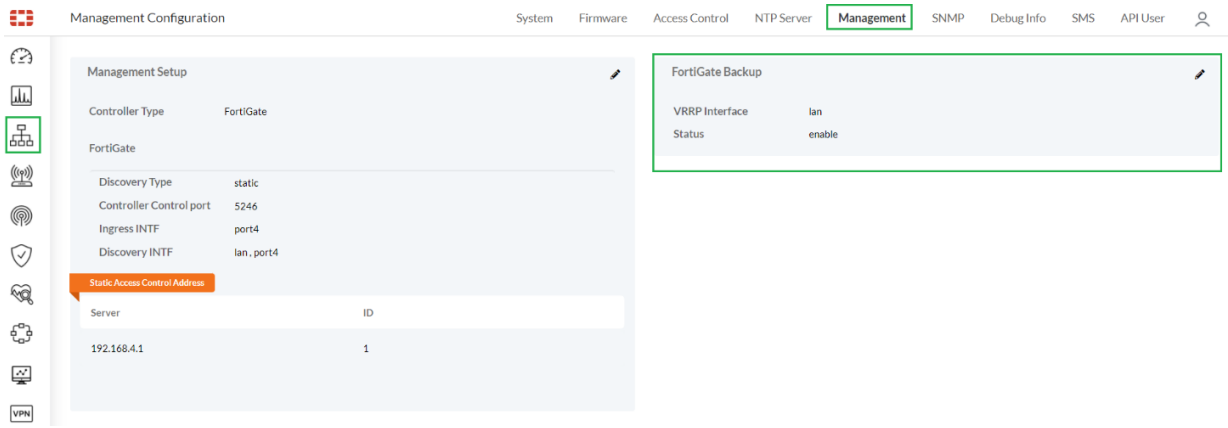
Failure to switch to FortiExtender service after the FortiGate WAN service goes down

1. From the FortiExtender device, enable and check the VRRP status.
   - To enable the VRRP service - CLI:

```
config system management
  config fortigate-backup
```

```
    set status enable
    set vrrp-interface <interface>
  end
end
```

- To enable the VRRP service - GUI:
  i. From the FortiExtender GUI, go to *Setting* > *Management* and locate the *FortiGate Backup* section.
  ii. Click *Edit* and set *VRRP Status* to *enable*.

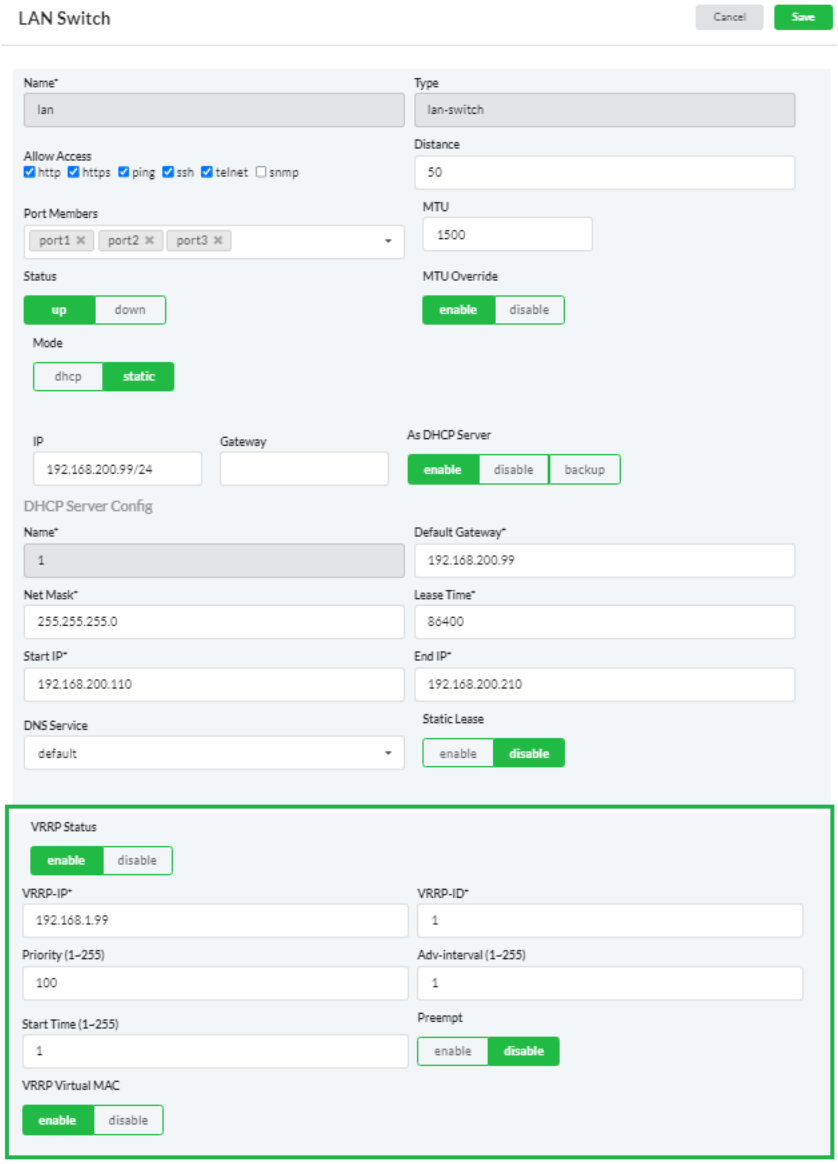


2. Check the VRRP configuration for the specific interface from the FortiExtender device.
   - To check the VRRP configuration - CLI:

```
config system interface
  edit lan
    config vrrp
      set id 1
      set ip 192.168.1.99
      set priority 100
    end
  end
end
```

   - To check the VRRP configuration - GUI:
     From the FortiExtender GUI, go to *Networking* > *LAN Switch*.

Edit *lan* and set *VRRP Status* to *enable*.



3. From the FortiGate, verify that the VRRP configurations for id, ip, and VRRP IP address are correct.

```
config system interface
  edit wan1
    config vrrp
      edit 1
        set vrgrp 1
        set vrip 192.168.1.99
        set priority 1
      next
    end
  next
end
```

Failure to switch service from FortiExtender to FortiGate after the FortiGate service recovers

From the FortiExtender, check the preempt settings. In order for FortiGate to restore service, you need to disable the `preempt` setting under the FortiExtender's `vrrp`. Meanwhile, you need to enable the `preempt` setting on the FortiGate side.

To disable preempt on FortiExtender:

```
config system interface
  edit lan
    config vrrp
      set preempt disable
    end
  end
end
```

To enable preempt on FortiGate:

```
config system interface
  edit wan1
    config vrrp
      edit 1
        set preempt enable
      next
    end
  end
end
```

Note: The preempt setting is enabled by default.

Failure to use FortiGate service when FortiGate and FortiExtender services are both up

Check the VRRP service's priority setting on FortiExtender and FortiGate. If the priority setting with the lower value, has higher priority to provide VRRP services.

To check the priority setting on FortiExtender:

```
config system interface
  edit lan
    config vrrp
      set priority 100
    end
  end
end
```

To check the priority setting on FortiGate:

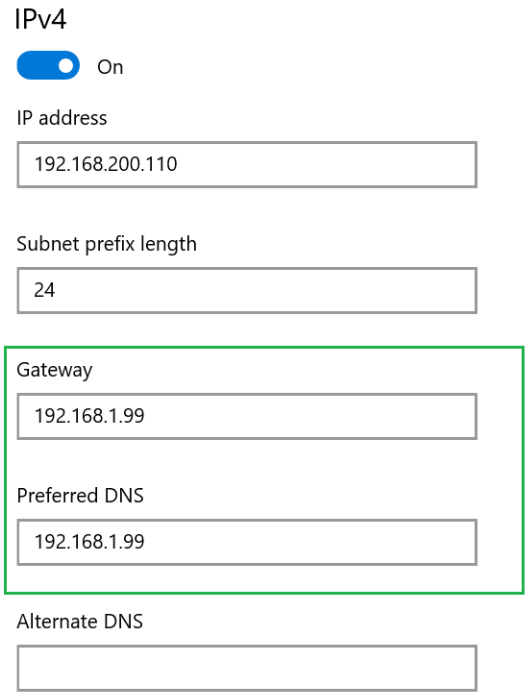
```
config system interface
  edit wan1
    config vrrp
```

```
      edit 1
        set priority 1
      next
    end
  end
end
```

Set `priority` to a lower value to let FortiGate have higher service priority.

Client fails to get DNS service when the FortiGate service is down while FortiExtender is still up through VRRP

1. Check the DNS service setting on the client using the VRRP IP address.
   The VRRP IP address should be identical for both the FortiExtender and FortiGate configurations. In this example, the VRRP IP address 192.168.1.99.
2. Configure the server, switch, or client using the VRRP IP address for both the Gateway service and DNS server.



Appendix A

This section contains examples of working debug outputs.

WAN-Extension Virtual wire pair configuration

```
FX511F # config system virtual-wire-pair
FX511F (virtual-wire-pair) # show
config system virtual-wire-pair
    set lte1-mapping capwap1
end
```

get system aggregate-interface status

```
le-agg-link:
        le-vxlan-port2(le-vxlan-port2): linkup ALIVE aggregated active
        le-vxlan-port1(le-vxlan-port1): linkup ALIVE aggregated active
```

get vpn ipsec configurations

```
le-uplink-port1: IKEv2, no reauthentication, rekeying every 86400s, dpd delay 20s
  local:  192.168.141.39
  remote: 192.168.144.75
  local pre-shared key authentication:
    id: peerid-2PELOCMnoqSif87gMr7Hs6xogn2BGV2poSgCbsE98vSyieAMqhdey8tj
  remote pre-shared key authentication:
    id: localid-j5C939amRtVtX1ku0D42ywbOcWymSPulpNC6nEypc4i8sM9MHNkwAIW
  le-uplink-port1: TUNNEL, rekeying every 43200s, dpd action is clear
    local:  10.252.0.6/32
    remote: 10.252.0.1/32
le-uplink-port2: IKEv2, no reauthentication, rekeying every 86400s, dpd delay 20s
  local:  192.168.142.39
  remote: 192.168.144.75
  local pre-shared key authentication:
    id: peerid-2PELOCMnoqSif87gMr7Hs6xogn2BGV2poSgCbsE98vSyieAMqhdey8tj
  remote pre-shared key authentication:
    id: localid-j5C939amRtVtX1ku0D42ywbOcWymSPulpNC6nEypc4i8sM9MHNkwAIW
  le-uplink-port2: TUNNEL, rekeying every 43200s, dpd action is clear
    local:  10.252.0.7/32
    remote: 10.252.0.1/32
```

get vpn ipsec tunnel details

```
le-uplink-port1: #18, ESTABLISHED, IKEv2, fcffed7d3f8b90de_i* cd80580175b10582_r
  local  'peerid-2PELOCMnoqSif87gMr7Hs6xogn2BGV2poSgCbsE98vSyieAMqhdey8tj' @ 192.168.141.39
[4500]
  remote 'localid-j5C939amRtVtX1ku0D42ywbOcWymSPulpNC6nEypc4i8sM9MHNkwAIW' @ 192.168.144.75
[4500]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  established 72365s ago, rekeying in 10196s
  le-uplink-port1: #15, reqid 2, INSTALLED, TUNNEL, ESP:AES_CBC-128/HMAC_SHA1_96/MODP_2048
    installed 37462s ago, rekeying in 2519s, expires in 10058s
    in  c52b3080 (0x00000003), 628908 bytes,  7487 packets,     1s ago
    out 260e69a4 (0x00000003), 3366528 bytes, 25156 packets,     1s ago
    local  10.252.0.6/32
    remote 10.252.0.1/32
le-uplink-port2: #17, ESTABLISHED, IKEv2, 1f1fc64731ca8e2c_i* ee989d437a71c196_r
  local  'peerid-2PELOCMnoqSif87gMr7Hs6xogn2BGV2poSgCbsE98vSyieAMqhdey8tj' @ 192.168.142.39
[4500]
  remote 'localid-j5C939amRtVtX1ku0D42ywbOcWymSPulpNC6nEypc4i8sM9MHNkwAIW' @ 192.168.144.75
[4500]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  established 76675s ago, rekeying in 7329s
  le-uplink-port2: #14, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-128/HMAC_SHA1_96/MODP_2048
    installed 38355s ago, rekeying in 1118s, expires in 9165s
    in  c7d2bbdd (0x00000004), 643860 bytes,  7665 packets,     2s ago
    out 260e69a3 (0x00000004), 646232 bytes,  7687 packets,     2s ago
    local  10.252.0.7/32
    remote 10.252.0.1/32
```

execute debug EXTD ac_disc on

```
[1682097761]EXTD    :ac_disc :get_indev_ifname_by_ip:88      : | (tid 0x7f867dfd60)
ingress-intf for 192.168.140.61 is lan
[1682097761]EXTD    :ac_disc :is_ingress_intf_in_discovery_intfs:531     : | (tid
0x7f867dfd60) sessin_id 1, ingress_intf lan
[1682097761]EXTD    :ac_disc :cwWtpDiscoveryIgnore:743     : | (tid 0x7f867dfd60) The
discovery request will be sent as the intf lan to reach 192.168.140.61 is included in
discovery-intf
[1682097761]EXTD    :ac_disc :cwWtpSendDiscoverReq:836     : | (tid 0x7f867dfd60)
sending DISCOVERY REQ msg to 192.168.140.61 (hostname: 192.168.140.61).
[1682097761]EXTD    :ac_disc :cwWtpProcDiscoverResp:143     : | (tid 0x7f867dfd60)
received DISCOVERY_RESP from 192.168.140.61/5246
[1682097761]EXTD    :ac_disc :cwWtpDiscoveryConnectAc:864     : | (tid 0x7f867dfd60)
Found AC 192.168.140.61 using discovery type 1
[1682097761]EXTD    :ac_disc :cwWtpDiscoveryConnectAc:878     : | (tid 0x7f867dfd60) AC
hostname 192.168.140.61 to be resolved under current discovery type 1
[1682097762]EXTD    :ac_disc :cwWtpDiscoveryReqSendtoAc:764     : | (tid 0x7f867dfd60)
Try to sending DISCOVERY REQ msg. discovery_type 1
[1682097762]EXTD    :ac_disc :cwWtpSelectBestAC:1019    : | (tid 0x7f867dfd60) AC 0
candidate 192.168.140.61 score 10240.00 dtlsPolicy clear  skip 0 until 0 curr 99
[1682097762]EXTD    :ac_disc :CWWS_AC_SELECT_enter:1128    : | (tid 0x7f867dfd60)
select AC 192.168.140.61 (192.168.140.61 10240.00) to join ....
```

```
[1682097762]EXTD    :ac_disc :get_indev_ifname_by_ip:74      : | (tid 0x7f867dfd60)
Command: "ip route get 192.168.140.61 2> /dev/null"
[1682097762]EXTD    :ac_disc :get_indev_ifname_by_ip:88      : | (tid 0x7f867dfd60)
ingress-intf for 192.168.140.61 is lan
[1682097762]EXTD    :ac_disc :get_indev_ifname_by_ip:74      : | (tid 0x7f867dfd60)
Command: "ip route get 192.168.140.61 2> /dev/null"
[1682097762]EXTD    :ac_disc :get_indev_ifname_by_ip:88      : | (tid 0x7f867dfd60)
ingress-intf for 192.168.140.61 is lan
[1682097763]EXTD    :ac_disc :update_capwap_vlan_interface:2285    : | (tid
0x7f867dfd60) Config ingress-intf to lan while entering FGT CAPWAP RUN state
```

execute debug EXTD fgvsp on

```
[1684786308]EXTD    :ac_disc :cwWtpFsm_advance:726     : | (tid 0x7fb23aed00) Config
ingress-intf to empty while leaving FGT RUN state
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryGetAcInfo:677     : | (tid 0x7fb23aed00)
Discover FGT with type 1
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryGetAcInfo:689     : | (tid 0x7fb23aed00)
cwConf static_ac_addr count 1
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryGetAcInfo:694     : | (tid 0x7fb23aed00)
cwConf static_ac_addr server[0]: 192.168.144.75
[1684786312]EXTD    :ac_disc :cwWtpGetAcAddr:639     : | (tid 0x0) AC host for DNS
lookup: 192.168.144.75
[1684786312]EXTD    :ac_disc :cwWtpGetAcAddr:651     : | (tid 0x0) DNS lookup for
192.168.144.75 successfully, entry->addr is 192.168.144.75
[1684786312]EXTD    :ac_disc :cwWtpGetAcAddr:657     : | (tid 0x0) send CWWE_FGT_
NSLOOKUP_BACK back to main thread
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryUpdAcInfo:729     : | (tid 0x7fb23aed00)
as.acInfoListCnt 1
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryUpdAcInfo:746     : | (tid 0x7fb23aed00)
as.acInfoList[0].hostname 192.168.144.75 1
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryReqSendtoAc:813     : | (tid 0x7fb23aed00)
Try to sending DISCOVERY REQ msg. discovery_type 1
[1684786312]EXTD    :ac_disc :_get_indev_ifname_by_ip_fgt:113     : | (tid
0x7fb23aed00) Command: "ping -w 1 -q -c 1 192.168.144.75 -I port2 2> /dev/null"
[1684786312]EXTD    :ac_disc :_get_indev_ifname_by_ip_fgt:130     : | (tid
0x7fb23aed00) ingress-intf for 192.168.144.75 is port2
[1684786312]EXTD    :ac_disc :is_ingress_intf_in_discovery_intfs:532     : | (tid
0x7fb23aed00) sessin_id 2, ingress_intf port2
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryIgnore:792     : | (tid 0x7fb23aed00) The
discovery request will be sent as the intf port2 to reach 192.168.144.75 is included in
discovery-intf
[1684786312]EXTD    :ac_disc :cwWtpSendDiscoverReq:838     : | (tid 0x7fb23aed00)
sending DISCOVERY REQ msg to 192.168.144.75 (hostname: 192.168.144.75).
[1684786312]EXTD    :ac_disc :cwWtpProcDiscoverResp:143     : | (tid 0x7fb23aed00)
received DISCOVERY_RESP from 192.168.144.75/5246
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryConnectAc:913     : | (tid 0x7fb23aed00)
Found AC 192.168.144.75 using discovery type 1
[1684786312]EXTD    :ac_disc :cwWtpDiscoveryConnectAc:927     : | (tid 0x7fb23aed00) AC
hostname 192.168.144.75 to be resolved under current discovery type 1
[1684786313]EXTD    :ac_disc :cwWtpDiscoveryReqSendtoAc:813     : | (tid 0x7fb23aed00)
Try to sending DISCOVERY REQ msg. discovery_type 1
[1684786313]EXTD    :ac_disc :cwWtpSelectBestAC:1068    : | (tid 0x7fb23aed00) AC 0
```

```
candidate 192.168.144.75 score 5363.81 dtlsPolicy clear  skip 0 until 0 curr 2927518
[1684786313]EXTD    :ac_disc :CWWS_AC_SELECT_enter:1180    : | (tid 0x7fb23aed00)
select AC 192.168.144.75 (192.168.144.75 5363.81) to join ....
[1684786313]EXTD    :ac_disc :_get_indev_ifname_by_ip_fgt:113     : | (tid
0x7fb23aed00) Command: "ping -w 1 -q -c 1 192.168.144.75 -I port2 2> /dev/null"
[1684786313]EXTD    :ac_disc :_get_indev_ifname_by_ip_fgt:130     : | (tid
0x7fb23aed00) ingress-intf for 192.168.144.75 is port2
[1684786313]EXTD    :fgvsp   :update_extender_status:381     : | (tid 0x7fb23aed00) set
extension to 1 with active FSM setting
[1684786313]EXTD    :ac_disc :_get_indev_ifname_by_ip_fgt:113     : | (tid
0x7fb23aed00) Command: "ping -w 1 -q -c 1 192.168.144.75 -I port2 2> /dev/null"
[1684786313]EXTD    :ac_disc :_get_indev_ifname_by_ip_fgt:130     : | (tid
0x7fb23aed00) ingress-intf for 192.168.144.75 is port2
[1684786313]EXTD    :fgvsp   :config_lan_extension_clear_handler:1473    : | (tid
0x7fb23aed00) receive CW_ME_TYPE_EXT_LAN_EXTENSION_CLEAR
[1684786313]EXTD    :fgvsp   :config_lan_extension_upd_handler:1220    : | (tid
0x7fb23aed00) receive CW_ME_TYPE_EXT_LAN_EXTENSION
[1684786313]EXTD    :fgvsp   :config_lan_extension_upd_handler:1220    : | (tid
0x7fb23aed00) receive CW_ME_TYPE_EXT_LAN_EXTENSION
[1684786313]EXTD    :fgvsp   :config_v2_extender_handler:329     : | (tid 0x7fb23aed00)
receive CW_ME_TYPE_EXT_EXTENDER
[1684786313]EXTD    :fgvsp   :str_2_extender_conf:39      : | (tid 0x7fb23aed00) magic:
12345, header num: 1, total len: 24
[1684786313]EXTD    :fgvsp   :update_generic_extender:231     : | (tid 0x7fb23aed00)
allowaccess sent from FGT is 80000000
[1684786313]EXTD    :fgvsp   :update_generic_extender:299     : | (tid 0x7fb23aed00)
interface le-switch allowaccess is configured as 0
[1684786313]EXTD    :fgvsp   :update_generic_extender:307     : | (tid 0x7fb23aed00)
bandwidth-limit sent from FGT is 0
```

execute debug EXTD info on

```
[1684786673]EXTD    :(null)  :cwWtpProcTimerMsg:810     : | (tid 0x7fb23aed00) got a
timer message type CWTMR_ECHO_INTERVAL id 521688
[1684786673]EXTD    :event   :cwWtpProcTimerMsg:906     : | (tid 0x7fb23aed00) gen type
CWWE_ECHO_INTV_TMR_EXPIRE
[1684786673]EXTD    :event   :cwWtpProcTimerMsg:907     : | (tid 0x7fb23aed00) WTP_EV_
GEN - CWWE_ECHO_INTV_TMR_EXPIRE meInfo (nil) msgPtr (nil) len 0
[1684786673]EXTD    :(null)  :cwWtpProcTimerMsg:810     : | (tid 0x7fb23aed00) got a
timer message type CWTMR_DATA_CHANNEL_KEEP_ALIVE id 521690
[1684786673]EXTD    :event   :cwWtpProcTimerMsg:906     : | (tid 0x7fb23aed00) gen type
CWWE_DC_KEEP_ALIVE_TMR_EXPIRE
[1684786673]EXTD    :event   :cwWtpProcTimerMsg:907     : | (tid 0x7fb23aed00) WTP_EV_
GEN - CWWE_DC_KEEP_ALIVE_TMR_EXPIRE meInfo (nil) msgPtr (nil) len 0
[1684786673]EXTD    :state   :cwWtpFsmThread:297     : | (tid 0x7fb23aed00) =====
Received event from socket 7, 40-bytes event (37) =====
[1684786673]EXTD    :state   :cwWtpFsm_advance:802     : | (tid 0x7fb23aed00) FSM: old
CWWS_RUN(15) ev CWWE_ECHO_INTV_TMR_EXPIRE(37) new CWWS_RUN(15)
[1684786673]EXTD    :state   :cwws_to_run:2118    : | (tid 0x7fb23aed00) CWWS_RUN,
CWWE_ECHO_INTV_TMR_EXPIRE
[1684786673]EXTD    :state   :update_extender_status:355     : | (tid 0x7fb23aed00)
controller 2, data 3 (network_mode 4), masters 3, active 0x4ca620, standby 0x54d4e8
[1684786673]EXTD    :state   :update_extender_status:444     : | (tid 0x7fb23aed00) to_
```

```
update 0 - return
[1684786673]EXTD    :state   :ext_check_network_mode:139     : | (tid 0x7fb23aed00)
discovery_type 8, fortigate data 3, cloud network_mode 4, local network_mode 4 - mode 4
[1684786673]EXTD    :state   :capwap_echo_request_handling:1440    : | (tid
0x7fb23aed00) tx ECHO_REQ to 192.168.144.75:5246.
[1684786673]EXTD    :protocol:cwWtpSendEchoReq:1011    : | (tid 0x7fb23aed00) sending
ECHO REQ msg.
[1684786673]EXTD    :message :cwWtpSendRawMsgQueue:351     : | (tid 0x7fb23aed00)
SENDING OUT type 13 seqNum 97
[1684786673]EXTD    :dtls    :cwDtlsMsgCbFn:648     : | (tid 0x7fb23aed00) [outgoing]
ver 0 [length 13 (0x000d)]
[1684786673]EXTD    :dtls    :wtpDtlsWrite:224     : | (tid 0x7fb23aed00) SSL_write()
was successful(len= 16, rc = 16)
[1684786673]EXTD    :(null)  :cu_swtp_send_ctl_msg:337     : | (tid 0x7fb23aed00)
wtpDtlsWrite(16) succeeded.
[1684786673]EXTD    :timer   :cwWtpSendRawMsgQueue:354     : | (tid 0x7fb23aed00)
cwAddTimer ReXmit success.
[1684786673]EXTD    :message :cwWtpPendingMsgAdd:335     : | (tid 0x7fb23aed00) type 13
seqNum 97 AT head 15 Cnt 1
[1684786673]EXTD    :timer   :capwap_echo_request_handling:1443    : | (tid
0x7fb23aed00) cwAddTimer EchoInterval success.
[1684786673]EXTD    :state   :cwWtpFsmThread:307     : | (tid 0x7fb23aed00) ===== event
from sock 7   handling end =====
[1684786673]EXTD    :state   :cwWtpFsmThread:297     : | (tid 0x7fb23aed00) =====
Received event from socket 7, 40-bytes event (90) =====
[1684786673]EXTD    :state   :cwWtpFsm_advance:802     : | (tid 0x7fb23aed00) FSM: old
CWWS_RUN(15) ev CWWE_DC_KEEP_ALIVE_TMR_EXPIRE(90) new CWWS_RUN(15)
[1684786673]EXTD    :state   :cwws_to_run:2118    : | (tid 0x7fb23aed00) CWWS_RUN,
CWWE_DC_KEEP_ALIVE_TMR_EXPIRE
[1684786673]EXTD    :state   :update_extender_status:355     : | (tid 0x7fb23aed00)
controller 2, data 3 (network_mode 4), masters 3, active 0x4ca620, standby 0x54d4e8
[1684786673]EXTD    :state   :update_extender_status:444     : | (tid 0x7fb23aed00) to_
update 0 - return
[1684786673]EXTD    :state   :ext_check_network_mode:139     : | (tid 0x7fb23aed00)
discovery_type 8, fortigate data 3, cloud network_mode 4, local network_mode 4 - mode 4
[1684786673]EXTD    :state   :capwap_dc_dead_detact_handling:1357    : | (tid
0x7fb23aed00) tx DATA_CHAN_ALIVE to 192.168.144.75:25246.
[1684786673]EXTD    :protocol:cwWtpSend_dc_keep_alive_msg:763     : | (tid
0x7fb23aed00) sending DATA CHANNEL KEEP ALIVE msg.
[1684786673]EXTD    :timer   :capwap_dc_dead_detact_handling:1363    : | (tid
0x7fb23aed00) cwAddTimer DcKeepAlive_ReXmit success.
[1684786673]EXTD    :timer   :capwap_dc_dead_detact_handling:1367    : | (tid
0x7fb23aed00) cwAddTimer DcKeepAlive success.
[1684786673]EXTD    :state   :cwWtpFsmThread:307     : | (tid 0x7fb23aed00) ===== event
from sock 7   handling end =====
[1684786673]EXTD    :dtls    :cwWtpProcOutCipherCtlMsg:60      : | (tid 0x7fb23aed00)
calling recv()
[1684786673]EXTD    :message :cwWtpSendRawMsg:29      : | (tid 0x7fb23aed00) 57B ==>
192.168.144.75/5246 - cipher message
[1684786673]EXTD    :dtls    :cwWtpProcOutCipherCtlMsg:72      : | (tid 0x7fb23aed00)
successfully sent data(57)...
[1684786673]EXTD    :dtls    :cwWtpProcOutCipherCtlMsg:60      : | (tid 0x7fb23aed00)
calling recv()
[1684786673]EXTD    :datachan:cwWtpProcInputDataMsg:1567    : | (tid 0x7fb23aed00)
====== socket 11 ======
[1684786673]EXTD    :datachan:cwWtpProcInputDataMsg:1579    : | (tid 0x7fb23aed00) 30
```

```
bytes read
[1684786673]EXTD    :datachan:cwWtpProcInputDataMsg:1593    : | (tid 0x7fb23aed00) rx
DATA_CHAN_ALIVE from 192.168.144.75:25246.
[1684786673]EXTD    :event   :cwWtpProcInputDataMsg:1594    : | (tid 0x7fb23aed00) WTP_
EV_GEN - CWWE_DC_KEEP_ALIVE_RECV meInfo (nil) msgPtr (nil) len 0
[1684786673]EXTD    :datachan:cwWtpProcInputDataMsg:1602    : | (tid 0x7fb23aed00)
pingsvr healthy
[1684786673]EXTD    :datachan:cwWtpProcInputDataMsg:1636    : | (tid 0x7fb23aed00)
====== Done ======
[1684786673]EXTD    :state   :cwWtpFsmThread:297     : | (tid 0x7fb23aed00) =====
Received event from socket 7, 40-bytes event (89) =====
[1684786673]EXTD    :state   :cwWtpFsm_advance:802     : | (tid 0x7fb23aed00) FSM: old
CWWS_RUN(15) ev CWWE_DC_KEEP_ALIVE_RECV(89) new CWWS_RUN(15)
[1684786673]EXTD    :state   :cwws_to_run:2118    : | (tid 0x7fb23aed00) CWWS_RUN,
CWWE_DC_KEEP_ALIVE_RECV
[1684786673]EXTD    :state   :update_extender_status:355     : | (tid 0x7fb23aed00)
controller 2, data 3 (network_mode 4), masters 3, active 0x4ca620, standby 0x54d4e8
[1684786673]EXTD    :state   :update_extender_status:444     : | (tid 0x7fb23aed00) to_
update 0 - return
[1684786673]EXTD    :state   :ext_check_network_mode:139     : | (tid 0x7fb23aed00)
discovery_type 8, fortigate data 3, cloud network_mode 4, local network_mode 4 - mode 4
[1684786673]EXTD    :state   :capwap_dc_keepalive_handling:1347    : | (tid
0x7fb23aed00) DATA CHAN (WTP - AC 192.168.144.75:25246) is alive.
[1684786673]EXTD    :timer   :capwap_dc_keepalive_handling:1348    : | (tid
0x7fb23aed00) cwDelTimer DcKeepAlive_ReXmit success.
[1684786673]EXTD    :timer   :capwap_dc_keepalive_handling:1350    : | (tid
0x7fb23aed00) cwDelTimer DcDeadInterval success.
[1684786673]EXTD    :timer   :capwap_dc_keepalive_handling:1351    : | (tid
0x7fb23aed00) cwAddTimer DcDeadInterval success.
```

www.fortinet.com