FortiGate Troubleshooting Guide

Regulatory compliance
FCC Class A Part 15 CSA/CUS

Table of content

1 Ticket creation requirements

If you are a Fortinet Partner, we strongly recommend you to open your tickets using your Partner account. If you don't do so, your tickets are logged by the FortiCare application as end-users tickets and therefore you loose the benefits of being a partner.

In order for Fortinet Technical Support to provide you with the quickest and best quality of support, we would recommend that a ticket be initially opened with:

1. A clear problem description

A ticket must deal with a single issue. Do not hesitate and create several tickets when reporting several issues on the same unit.

When possible, the description should mention the working scenario and the non-working scenario.

When related to a complex configuration, the description should mention the firewall policies and the protection profiles affected by the problem.

2. The problem history

The initial description must indicate:

- If the unit has worked properly before with the same configuration
- If the problem appeared after an upgrade. If so, which firmware was previously running
- If the problem appeared after a configuration change. If so, which settings have been modified
- If other versions have been tested, please indicate the working and non working firmwares

3. A network diagram

A detailed network diagram must indicate:

- Each configured Fortinet device interface (including the interface used for management).
- All IPs and netmasks of each interface and attached host(s).
- The traffic flow and type, which is causing the problem. Indicate the source and destination devices. If the responsible traffic flow is not known, identify all traffic flows of the concerned protocol. For example, detail the outgoing and incoming SMTP traffic flow, to and from the email client.
- Identify any relays/proxies/secondary servers which might be used in your network layout and their usage. For example, whether a web/ftp client is configured to first access a proxy, or if two SMTP email servers are relaying emails to each other.
- Identify whether any load balancers are being used, and for which protocols/ports.
- For a transparent mode issue, a layer 2 diagram is required as well.

4. The configuration file

The one provided must be the latest one.

In case of a working and a non-working scenario, the configuration file provided must be the one of the non-working scenario.

When the problem appeared after an upgrade, it is recommended to also provide the configuration that was running properly before the upgrade.

When the problem is related to units running in HA mode, it is recommended to provide the HA settings of the slave unit. They can be retrieved from the slave's cli with the command **#get sys ha**

When the problem is related to a FortiClient dialup user, please provide us with the FortiClient version and an export of the FortiClient settings (.vpl file).

5. The debug log of the unit

It can be retrieved under System > Maintenance > Backup & Restore > Advanced.

When the problem is related to units running in HA mode, the debug log of the master and the slave units must be submitted. They can be retrieved under System > Config > HA

6. A reproduction scenario

In case the problem can be reproduced, please indicate the steps one has to go through to reproduce and therefore troubleshoot the problem.

7. A description and the results of the troubleshooting steps already achieved

Please mention any troubleshooting action already performed and its result.

The next part will guide you through common debug outputs that can help you troubleshooting an issue.

Please provide the outputs of these debug commands upon ticket creation. You should clearly indicate how each debug was retrieved.
For example:

- The trace sniff_ok.txt was retrieved using the configuration file named config_ok.cfg and accessing web site www.fortinet.com
- The trace sniff_ko.txt was retrieved using the configuration file named config_ko.cfg and accessing web site www.fortinet.com

2 Initial troubleshooting steps

2.1 IPsec VPN issues

2.1.1 The tunnel fails to connect

In such cases, please provide us with the following debug outputs:

- The ike debug output

1. Enable debug with:
#diag debug en
#diag debug console timestamp en
#diag debug app ike –1
When other working VPN tunnels generate ike debug as well, you can filter your debug by specifying the public IP of the remote peer.
#diag debug app ike –1 x.x.x.x
2. Connect the tunnel and capture all outputs
3. Disable debug with
#diag debug dis
#diag debug console timestamp dis
#diag debug app ike 0

- A sniffer trace

1. Start a sniffer with
#diag sniff packet interfaceName 'host x.x.x.x' 3
Where x.x.x.x is the public IP of the remote gateway or dialup client
2. Connect the tunnel and capture all outputs
3. Stop the sniffer with ctrl+c and verify that your trace is clean (see section Using packet sniffer).

2.1.2 The client fails to retrieve its IP through DHCP

In such cases, please provide us with the following debug outputs:

- The dhcp debug output

1. Enable debug with:
#diag debug en
#diag debug console timestamp en
#diag debug app dhcprelay 7 -> if using an IPsec DHCP relay
#diag debug app dhcps 7 -> if using an IPsec DHCP sever
2. Connect the tunnel and capture all outputs
3. Disable debug with
#diag debug dis
#diag debug console timestamp dis
#diag debug app dhcprelay 0
#diag debug app dhcps 0

- A sniffer trace

As the external interface only sees encrypted traffic it is exceptionally indicated to sniff on all interfaces with the keyword 'any'.
1. Start a sniffer with
#diag sniff packet any 'udp port 67 or udp port 68' 6
2. Connect the tunnel and capture all outputs
3. Stop the sniffer with ctrl+c

NB: In a setup with a DHCP relay, you can additionally sniff on the interface where your DHCP server sits.

2.1.3 Problems with traffic going through the tunnel

In such cases, please mention clearly the name of the tunnel that is affected. Also, please provide us with the following debug information:

- Retrieve information about active tunnels with:

#diag vpn tunnel list

Repeat this command 5 times with 5 sec interval time while your are trying to send traffic through the tunnel.

#diag debug en
#diag vpn gw list

- Sniffer traces

Please take 2 sniffer traces simultaneously at both ends of the tunnel.
In case of a site to site, please sniff in verbose 3 at both ends while you try sending traffic into the tunnel.
In case of a dialup, you can sniff in the FortiClient virtual adapter on one side (with Ethereal for example) and use the FortiGate embedded sniffer on the FortiGate side.

2.2 HA issues

2.2.1 Synchronization issues

Please provide us with:

- The synchronization error message

It can be retrieved from the slave console port and should look like:

slave is not in sync with master, sequence:0. (type 0x3)

If you have no access to the console, this message can also be retrieved by enabling the following debug on the slave unit:

#diag debug en
#diag debug app hatalk 255

This debug can then be disabled with:

#diag debug dis
#diag debug app hatalk 0

- The following debug outputs

In case the slave unit continuously reboots, we recommend you to stop synchronization prior to retrieving these outputs. To do so, connect to the slave unit and type '**#exec ha synchro stop**'.
Note that you must then type '**#exec ha synchro start** when you wish to restart synchronization.

Then retrieve the following outputs on **BOTH** the master and the slave units

#get sys sta
#get sys perf status
#get sys ha
#diag sys ha status
#diag sys ha dump 2
#diag sys ha dump 3
#diag sys ha showcs
#diag sys ha showcs 1
#diag sys ha showcs 2
#diag sys ha showcs 3
#diag netl dev list
#diag hard dev nic <HAportName>
#show full-configuration

NB: The slave unit can be reached from the master with the command
#exec ha manage slave_id

NB2: When the command 'show full-configuration' breaks the output with the option 'more', we would recommend you to set the following option:

#config system console
#set output standard
#end

2.2.2 Rebuilding a cluster

In case you wish to build a cluster or try to recover from a synchronization issue.

1. Disconnect the slave unit from the cluster and reset it to factory defaults
2. On the master unit, modify the HA settings to keep only the minimum HA parameters:
    a. group-id

b. group-name
c. password
d. unit priority
e. mode
f. hbdev

In particular make sure that port monitoring settings are all disabled.

3. On the slave unit, configure only these minimum HA parameters
4. Reconnect the slave unit. Note that it may reboot once when synchronizing.

2.3 Transparent mode issues

Please provide us with the following details when troubleshooting a transparent mode issue:

- MAC addresses details

Please add to your Layer2 network diagram the MAC addresses of the hosts involved in the setup. When reading a sniffer trace taken from a transparent mode scenario, Fortinet Support needs to map these MAC addresses to the appropriate devices.

Also, please indicate when VRRP/HSRP or load balancing / fail over mechanisms are used.

- Dump the bridge information with:

#diagnose netlink brctl list

- Dump the vdom bridge forwarding table with:

#diagnose netlink brctl name host <vd_name>.b

where <vd_name> is the virtual domain name

- Sniffer traces

When you experience traffic problems, please take 2 sniffer traces simultaneously on the internal and external interfaces. These traces must be captured in verbose 3.

2.4 Anti-Spam issues

For such issues, please provide a detailed diagram of your mail traffic flow.

2.4.1 Which banned word is being matched?

In such cases, please use the following cli command:
 # diag spamfilter bword matchfilter '<logstring>'
Where <logstring> is the group of numbers read from the end of the log entry.

2.4.2 Other anti-spam issues

Please dump the following outputs:

- Checking and monitoring proxy activity

#diag debug en
#diag debug app smtp 3

#diag test app smtp 4
#diag test app smtp 44
#diag test app smtp 444

NB: the example is given for SMTP but the same applies for POP3 and IMAP.

- Checking FortiGuard

#diag debug en
#diag debug app spamfilter 3

#diag spamfilter fortishield statistics list

2.5 Web filtering issues

For such issues, please provide a detailed diagram of your web traffic flow. Don't forget to mention any proxy or load balancing device.

2.5.1 Which banned word is being matched?

In such cases, please use the following cli command:
#diag webfilter bword matchfilter '<logstring>'
Where <logstring> is the group of numbers read from the end of the log entry.

2.5.2 Other web filtering issues

Please dump the following outputs:

- Checking and monitoring proxy activity:

#diag debug en
#diag debug app http 3

#diag test app http 4
#diag test app http 4
#diag test app http 444

- Checking FortiGuard

#diag debug en
#diag debug app urlfilter 3

#diag webfilter fortiguard statistics list

2.6 FortiGate blocking traffic

In this scenario, please gather the output of:

- The packet sniffer. Sniff simultaneously on both the internal and external interfaces
- The session filter
- The debug flow

Further details regarding the usage of above commands can be found in section 2.10

2.7 FSAE issues

For any FSAE issue, please provide us with the following details:

- Fortigate firmware version: ex. 3.00MR4
- FSAE version: ex. 3.0.018
- AD Server version: ex. Windows2003 server
- Client workstation details:
  OS: WindowsXP sp2
  Hardware: ex. Dell Latitude 620

2.7.1 The FortiGate can't retrieve the list of groups

When using the FSAE feature, the list of AD groups should appear in the GUI under 'User > Windows AD'. If the list is empty:
1. Start a sniffer to capture the traffic exchanged between the AD server and the FortiGate
2. From a command line, type:
#exec fsae refresh

2.8 Unstable unit

In such cases, please dump the following outputs:
#get sys sta
#get sys perf status
#diag sys top 1 100 →let run for 10-15s and escape pressing 'q'
#diag netl dev list
#diag netl int list
#diag hard dev nic interfaceName
 # diag hard sys mem

If your units run in cluster, above commands must be retrieved on both devices. Also, please retrieve as well:
#diag sys ha status
#get sys ha

2.9 Freezing / Crashing unit

In such cases, please go through the following steps and provide us with the results:

- LCD check

When applicable to your FortiGate model, please indicate whether the LCD panel is frozen or responsive.

- Management traffic check

Does the unit reply to echo requests?
Can you manage it through the GUI?
Can you manage it through the cli?

- Console port check

Is the console port responsive?

- Kernel crash debug

1. Enable debug with:
#diag debug en
#diag debug console timestamp en
#diag debug kernel level 5
2. Connect a PC to the console port and log all information being printed to the HyperTerminal.

2.10Other troubleshooting tips

2.10.1 Using packet sniffer

http://kc.forticare.com/default.asp?id=1186&SID=&Lang=1

All traces provided to support must be provided in verbose 3.

Make sure that no packet was dropped by kernel. To do so, verify the last line being displayed when you stop the trace.

10858 packets received by filter
0 packets dropped by kernel

When packets are dropped, try a more specific filter.

Always sniff specifying the interface name, in other words, avoid using 'any'.
When not possible, sniff with 'any' but in verbose 6
#diag sniff packet any 'filter' 6

In order to sniff on a pppoe interface, use ppp0 as the interface name. If you have several pppoe interfaces it will be pppx where x is the appropriate index.

When sniffing on an A-A cluster, to not forget to sniff on **BOTH** the master and the slave unit interfaces.

2.10.2 Tracking sessions with the session filter

From the GUI, you can lookup for a session under:
System > Status > Sessions > Details

From the cli:
1. First set your filters with
#diag sys session filter ...
2. Print the sessions matching your filter with:
#diag sys session list

2.10.3 Tracking sessions with the debug flow

From the cli, you can track your traffic using the following commands:
1. Enable debug with
#diag debug en
2. Set your filters with
#diag debug flow filter ...
3. Then type:
#diag debug flow show console en
#diag debug flow show function-name en
#diag debug flow trace start 100 (to get 100 lines)
4. Generate the traffic and capture the output

2.10.4 Testing authentication

These cli commands can help you test your radius or ldap server:
#diag test auth rad <server_name> <chap | pap | mschap | mschap2> <username> <pwd>
#diag test authserver ldap server <server_name> <username> <pwd>

When experiencing authentication issues with a radius or LDAP server, please take a sniffer trace of the authentication traffic flowing between the FortiGate and the server.

2.10.5 Other useful commands

1. IP addresses

#diag ip address list

Displays all IP addresses assigned to interfaces including VIPs and IP pools.

2. ARP table

#diag ip arp list

Display the FortiGate unit ARP cache.

3. Routing table

#diag ip route list

Display the current routing table in the kernel. All routing decisions depend on this table. The kernel routing table is updated dynamically as the routing configuration or dynamic routing changes.

4. Resources usage

#diag sys top 1 100

From left to right, the columns are:
process name
process id
CPU usage
memory usage

#diag sys kill signal_number process_id

As signal_number you can use for example:
9 as SIGKILL
15 as SIGTERM

5. PPPoE interface

#diag debug en
#diag debug app ppp 3

This debug is useful for the F60DSL models

6. Interface status

#diag hard dev nic portName

2.11 Hardware issues

For hardware issues, please refer to Article 1067 on the Knowledge Center and follow the link to the Hardware Troubleshooting Page

Whenever you perform a maintenance operation through the console port, please log all outputs being printed. These logs are useful information to provide when logging a ticket for a hardware issue.

For any RMA ticket, please make sure that the following information are provided upon ticket creation:

1. The output of the HQIP test
2. A console capture of the boot process if the unit does not boot properly
3. The output of any maintenance operation that you have performed while trying to recover