FortiWeb

On OCB-FE

Troubleshooting Guide

8th April 2019

Version 1.0

document control

date	version no.	author	change/addition
8-April-2019	1.0	Ahmad Samak	Creation

table of contents

1 References

Reference	Description	Link to document
[1]	Fortinet Knowledge Base	http://cookbook.fortinet.com/fortiweb/
[2]	Technical Documentation	http://docs.fortinet.com
[3]	Video Tutorials	http://video.fortinet.com

2 Introduction

This document provides troubleshooting techniques for some frequently encountered problems of the FortiWeb-VM. It includes general troubleshooting methods and specific troubleshooting tips using both the command line interface (CLI) and the Web-based Manager.

Some CLI commands provide troubleshooting information not available through the Web-based Manager. The Web-based Manager is better suited for viewing large amounts of information on screen, reading logs and archives, and viewing status through the dashboard.

3 FortiOS Ports

In the TCP and UDP stacks, there are 65 535 ports available for applications to use when communicating with each other. Many of these ports are commonly known to be associated with specific applications or protocols. These known ports can be useful when troubleshooting your network.

Use the following ports while troubleshooting the FortiGate device:

Port(s)	Functionality
UDP 53	DNS lookup, RBL lookup
UDP 53 or UDP 8888	FortiGuard Antispam or Web Filtering rating lookup
UDP 53 (default) or UDP 8888 and UDP 1027 or UDP 1031	FDN Server List - source and destination port numbers vary by originating or reply traffic. See the article “How do I troubleshoot performance issues when FortiGuard Web Filtering is enabled?” in the Knowledge Base.
UDP 123	NTP Synchronization
UDP 162	SNMP Traps
UDP 514	SYSLOG - All FortiOS versions can use syslog to send log messages to remote syslog servers. FortiOS v2.80 and v3.0 can also view logs stored remotely on a FortiAnalyzer unit.
TCP 22	Configuration backup to FortiManager unit or FortiGuard Analysis and Management Service.
TCP 25	SMTP alert email, encrypted virus sample auto-submit
TCP 389 or TCP 636	LDAP or PKI authentication
TCP 443	FortiGuard Antivirus or IPS update - When requesting updates from a FortiManager unit instead of directly from the FDN, this port must be reconfigured as TCP 8890.
TCP 443	FortiGuard Analysis and Management Service
TCP 514	FortiGuard Analysis and Management Service log transmission (OFTP)
TCP 541	SSL Management Tunnel to FortiGuard Analysis and Management Service (FortiOS v3.0 MR6 or later)
TCP 514	Quarantine, remote access to logs and reports on a FortiAnalyzer unit, device registration with FortiAnalyzer units (OFTP)
TCP 1812	RADIUS authentication
TCP 8000 and TCP 8002	FSSO
TCP 10151	FortiGuard Analysis and Management Service contract validation

4 FortiAnalyzer/FortiManager Ports

If you have a FortiAnalyzer unit or FortiManager unit on your network you may need to use the following ports for troubleshooting network traffic.

Functionality	Port(s)
DNS lookup	UDP 53
NTP synchronization	UDP 123
Windows share	UDP 137-138
SNMP traps	UDP 162
Syslog, log forwarding	UDP 514
Log and report upload	TCP 21 or TCP 22
SMTP alert email	TCP 25
User name LDAP queries for reports	TCP 389 or TCP 636
RVS update	TCP 443
RADIUS authentication	TCP 1812
Log aggregation client	TCP 3000

5 Troubleshooting Methodologies

Before you begin troubleshooting anything but the most minor issues, you need to prepare. Doing so will shorten the time to solve your issue. This section helps to explain how you prepare before troubleshooting, as well as creating a troubleshooting plan and contacting support.

5.1 Establish a baseline

FortiWeb units operate at all layers of the OSI model. For this reason troubleshooting problems can become complex. If you establish a normal operation parameters, or baseline, for your system before the problem occurs it will help reduce the complexity when you are troubleshooting.

Many of the guiding questions in the following sections are some form of comparing the current problem situation to normal operation on your FortiWeb unit. For this reason it is a best practice that you know what your normal operating status is, and have a record of it you can refer to. This can easily be accomplished by monitoring the system performance with logs, SNMP tools, or regularly running information gathering commands and saving the output. This regular operation data will show trends, and enable you to see when changes happen and there may be a problem.

Note Back up your FortiOS configuration on a regular basis. This is a good practice for everyday as well as when troubleshooting. You can restore the backed up configuration when needed and save the time and effort of re-creating it from the factory default settings.

Some fundamental CLI commands you can use to obtain normal operating data for your system:

get system status	Displays versions of firmware and FortiGuard engines, and other system information.
get system performance status	Displays CPU and memory states, average network usage, average sessions and session setup rate, virus caught, IPS attacks blocked, and uptime.
get hardware memory	Displays informations about memory
get system session status	Displays total number of sessions
get router info routing-table all	Displays all the routes in the routing table including their type, source, and other useful data.
get ips session	Displays memory used and max available to IPS as well and counts.
get webfilter ftgd-statistics	Displays list of FortiGuard related counts of status, errors, and other data.
diagnose firewall statistic show	Displays the amount of network traffic broken down into categories such as email, VoIP, TCP, UDP, IM, Gaming, P2P, and

	Streaming.
diag system session list	Displays current detailed sessions list
show system dns	Displays configured DNS servers
diag sys ntp status	Displays informations about ntp servers

These commands are just a sample. Feel free to include any extra information gathering commands that apply to your system.

For an extensive snapshot of your system, run the CLI command used by TAC to gather extensive information about a system — exec tac report. It runs many diagnostic commands that are for specific configurations. This means no matter what features you are using, this command will record their current state. Then if you need to perform troubleshooting at a later date, you can run the same command again and compare the differences to quickly locate suspicious output you can investigate.

5.2 Define the Problem

The following questions can help determine the scope of the problem and isolate it:

- What is the problem?
  Do not assume that the problem is being experienced is the actual problem. First determine that the problem does not lie elsewhere before starting to troubleshoot the FortiGate device.

- Has it ever worked before?
  If the device never worked from the first day, you may not want to spend time troubleshooting something that could well be defective. See “Troubleshooting bootup”

- Can the problem be reproduced at will or is it intermittent?
  If the problem is intermittent, it may be dependent on system load. Also an intermittent problem can be very difficult to troubleshoot due to the difficulty reproducing the issue.

- What has changed?
  Do not assume that nothing has changed in the network. Use the FortiGate event log to see if any configuration changes were made. The change could be in the operating environment, for example, a gradual increase in load as more sites are forwarded through the firewall.

  If something has changed, see what the affect is if the change is rolled back.

- Determine the scope of the problem - after you have isolated the problem what applications, users, devices, and operating systems does it effect?

Before you can solve a problem, you need to understand it. Often this step can be the longest in this process.

Ask questions such as:

- What is not working? Be specific.
- Is there more than one thing not working?
- Is it partly working? If so, what parts are working?
- Is it a connectivity issue for the whole device, or is there an application that isn't reaching the Internet?

Be as specific as possible with your answers, even if it takes a while to find the answers.

These questions will help you define the problem. Once the problem is defined, you can search for a solution and then create a plan on how to solve it.

5.3 Gathering Facts

Fact gathering is an important part of defining the problem. Record the following information as it applies to the problem:

- Where did the problem occur?
- When did the problem occur and to whom?
- What components are involved?
- What is the affected application?
- Can the problem be traced using a packet sniffer?
- Can the problem be traced in the session table or using system debugging?
- Can log files be obtained that indicate a failure has occurred?

Answers to these questions will help you narrow down the problem, and what you have to check during your troubleshooting. The more things you can eliminate, the fewer things you need to check during troubleshooting. For this reason, be as specific and accurate as you can while gathering facts.

5.4 Create a Troubleshooting Plan

Once you have defined the problem, and searched for a solution you can create a plan to solve that problem. Even if your search didn't find a solution to your problem you may have found some additional things to check to further define your problem.

The plan should list all the possible causes of the problem that you can think of, and how to test for each possible cause.

Your troubleshooting plan will act as a checklist so that you know what you have tried and what is left to check. This is important to have if more than one person will be doing the troubleshooting. Without a written plan, people will become easily confused and steps will be skipped. Also if you have to hand over the problem to someone else, providing them with a detailed list of what data has been gathered and what solutions have been already tried demonstrates a good level of professionalism.

Be ready to add to your plan as needed. After you are part way through, you may discover that you forgot some tests or a test you performed discovered new information. This is normal.

Also if you contact support, they will require information about your problem as well as what you have already tried to fix the problem. This should all be part of your plan.

5.4.1 providing Supporting Elements

If the Fortinet Technology Assistance Center (TAC) needs to be contacted to help you with your issue, be prepared to provide the following information:

- The firmware build version (use the get system status command)
- A network topology diagram
- A recent configuration file
- Optionally, a recent debug log
- Tell the support team what troubleshooting steps have already been performed and the results.

Note

Do not provide the output from exec tac report unless Support requests it. The output from that command is very large and is not required in many cases.

5.5 Obtain any required additional equipment

You may require additional networking equipment, computers, or other equipment to test your solution.

Normally network administrators have additional networking equipment available either to loan you, or a lab where you can bring the FortiGate unit to test.

If you do not have access to equipment, check for shareware applications that can perform the same task. Often there are software solutions when hardware is too expensive.

5.6 Ensure you have administrator level access to required equipment

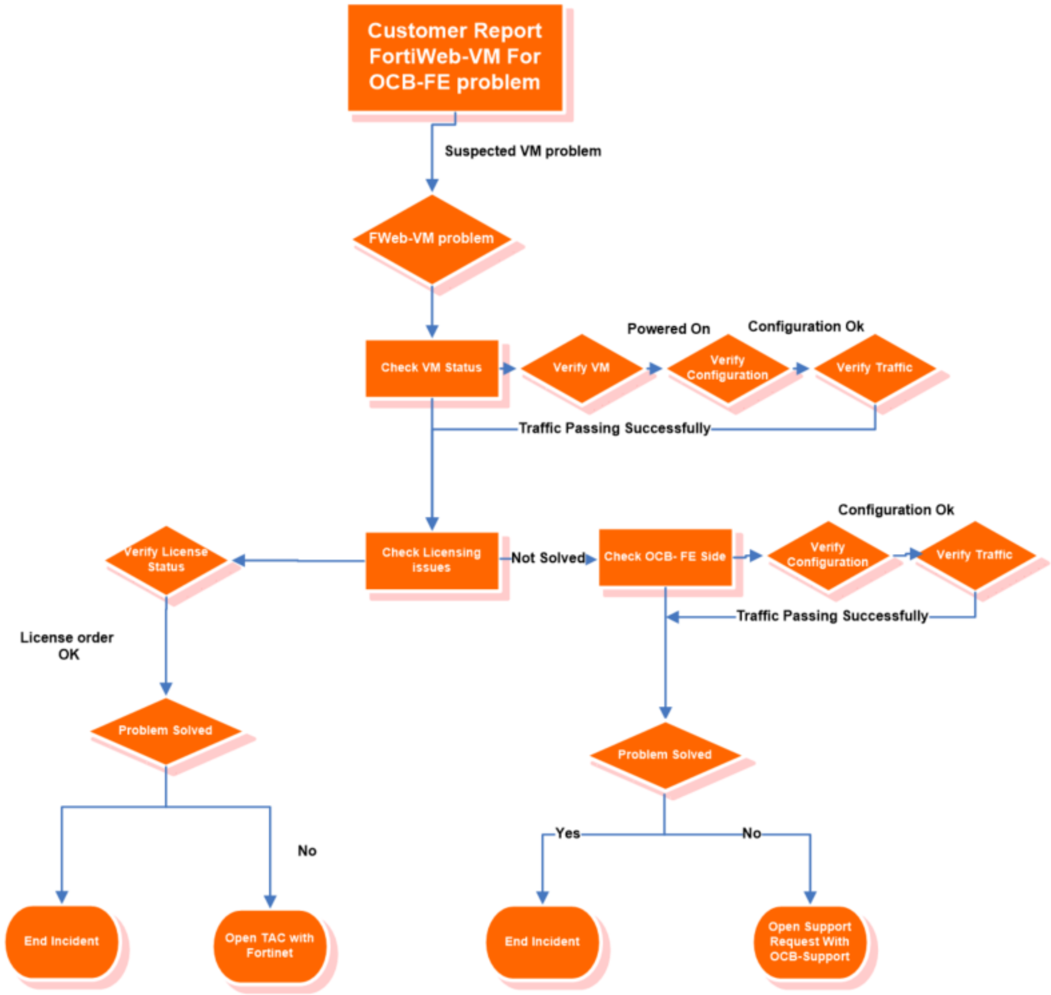
Before troubleshooting your FortiGate unit, you will need administrator access to the equipment. If you are a client on a FortiGate unit with virtual domains enabled, often you can troubleshoot within your own VDOM. However, you should inform your FortiGate unit's super admin that you will be doing troubleshooting.

Also, you may need access to other networking equipment such as switches, routers, and servers to help you test. If you do not normally have access to this equipment, contact your network administrator for assistance.

5.7 Contact Fortinet customer support for assistance

You have defined your problem, researched a solution, put together a plan to find the solution, and executed that plan. At this point if the problem has not been solved, it’s time to contact Fortinet Customer Support for assistance.

6 FortiWeb-VM troubleshooting Decision Tree



FortiWeb-VM For OCB-FE

Troubleshooting Decision Diagram

7 Troubleshooting

This topic provides guidelines to help you resolve issues if your FortiWeb appliance is not behaving as you expect. Keep in mind that if you cannot resolve the issue on your own, you can contact Fortinet Technical Support.

7.1 Tools

To locate network errors and other issues that may prevent connections from passing to or through the FortiWeb appliance, FortiWeb appliances feature several troubleshooting tools.

Troubleshooting methods and tips may use:

- the command line interface (CLI)
- the web UI
- external third-party tools

Some CLI commands provide troubleshooting information not available through the web UI; third-party tools on external hosts can test connections from perspectives that cannot be achieved locally.

7.1.1 Ping & Traceroute

If your FortiWeb appliance cannot connect to other hosts, try using ICMP (ping and traceroute) to determine if the host is reachable or to locate the node of your network at which connectivity fails, such as when static routes are incorrectly configured. You can do this from the FortiWeb appliance using CLI commands.

For example, you might use ping to determine that 172.16.1.10 is reachable:

```
execute ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=64 time=2.4 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.8 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=1.4 ms

--- 172.20.120.167 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.4/2.4 ms
```

or that 192.168.1.10 is **not** reachable:

```
execute ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...

--- 192.168.1.10 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

If the host is not reachable, you can use traceroute to determine the router hop or host at which the connection fails:

```
execute traceroute 192.168.1.10
traceroute to 192.168.1.10 (192.168.1.10), 32 hops max, 72 byte
    packets
1  192.168.1.2 2 ms 0 ms 1 ms
2  * * *
```

7.1.2 Log messages

Log messages often contain clues that can aid you in determining the cause of a problem. FortiWeb appliances can record log messages when errors occur that cause failures, upon significant changes, and upon processing events.

Depending on the type, log messages may appear in either the event, attack, or traffic logs. The FortiWeb appliance must be enabled to record event, attack, and traffic log messages; otherwise, you cannot analyze the log messages for events of that type. To enable logging of different types of events, select Log&Report > Log Config > Other Log Settings.

During troubleshooting, you may find it useful to reduce the logging severity threshold for more verbose logs, to include more information on less severe events. To configure the severity threshold, go to Log&Report > Log Config > Global Log Settings.

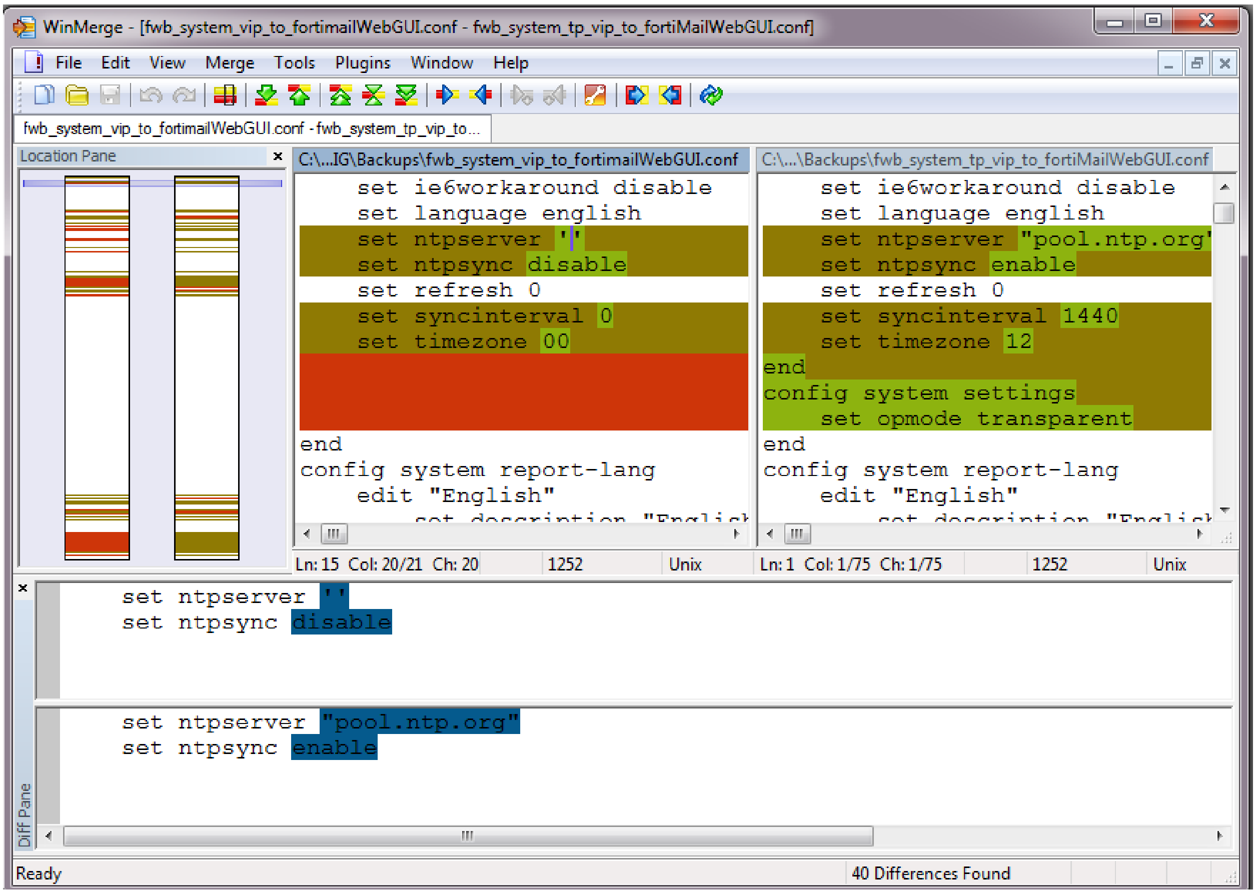
7.1.3 Diff

You can compare backups of the core configuration file with your current configuration. This can be useful if, for example:

- A previously configured feature is no longer functioning, and you are not sure what in the configuration has changed.
- You want to recreate something configured previously, but do not remember what the settings were.

Difference programs can help you to quickly find all changes.

Configuration differences highlighted in WinMerge


WinMerge - [fwb_system_vip_to_fortimailWebGUI.conf - fwb_system_tp_vip_to_fortiMailWebGUI.conf]
File Edit View Merge Tools Plugins Window Help
fwb_system_vip_to_fortimailWebGUI.conf - fwb_system_tp_vip_to...
Location Pane
C:\...IG\Backups\fwb_system_vip_to_fortimailWebGUI.conf
C:\...\Backups\fwb_system_tp_vip_to_fortiMailWebGUI.conf
Ln: 15 Col: 20/21 Ch: 20 1252 Unix
Ln: 1 Col: 1/75 Ch: 1/75 1252 Unix
Diff Pane
Ready
40 Differences Found

```
    set ie6workaround disable
    set language english
    set ntpserver ''
    set ntpsync disable
    set refresh 0
    set syncinterval 0
    set timezone 00



end
config system report-lang
    edit "English"
        set description "English
```

```
    set ie6workaround disable
    set language english
    set ntpserver "pool.ntp.org"
    set ntpsync enable
    set refresh 0
    set syncinterval 1440
    set timezone 12
end
config system settings
    set opmode transparent
end
config system report-lang
    edit "English"
        set description "English
```

```
    set ntpserver ''
    set ntpsync disable
```

```
    set ntpserver "pool.ntp.org"
    set ntpsync enable
```

There are many such difference-finding programs, such as WinMerge and the original diff. They can compare your configurations, line by line, and highlight parts that are new, modified, or deleted.

7.1.4 Packet Capture

Packet capture, also known as sniffing or packet analysis, records some or all of the packets seen by a network interface (that is, the network interface is used in promiscuous mode). By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiWeb appliances have a built-in sniffer. Packet capture on FortiWeb appliances is similar to that of FortiGate appliances. To use the built-in sniffer, connect to the CLI and enter the following command:

```
diagnose    network    sniffer    packet    [{any    |    <interface_name>}
[{none | '<filter_str>'} [{1 | 2 | 3} [<packets_int>]]]]
```

where:

- <interface_name> is either the name of a network interface, such as port1, or enter any for all interfaces.
- '<filter_str>' is the sniffer filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 80', or enter none for no filters. Filters use tcpdump syntax.

- {1 | 2 | 3} is an integer indicating whether to display the network interface names, packet headers, and/or payloads for each packet that the network interface sends, receives, or sees:
- 1 — Display the packet capture timestamp, plus basic fields of the IP header: the source IP address, the destination IP address, protocol name, and destination port number.
- Does not display all fields of the IP header; it omits:

IP version number bits

Internet header length (ihl)

type of service/differentiated services code point (tos)

explicit congestion notification

total packet or fragment length

packet ID

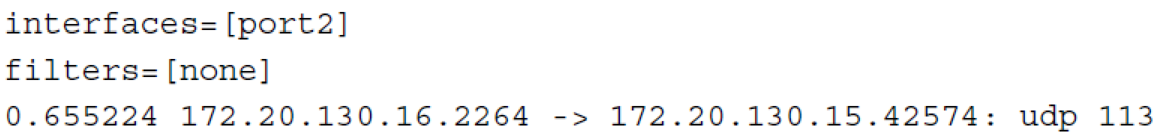
IP header checksum

time to live (TTL)

IP flag

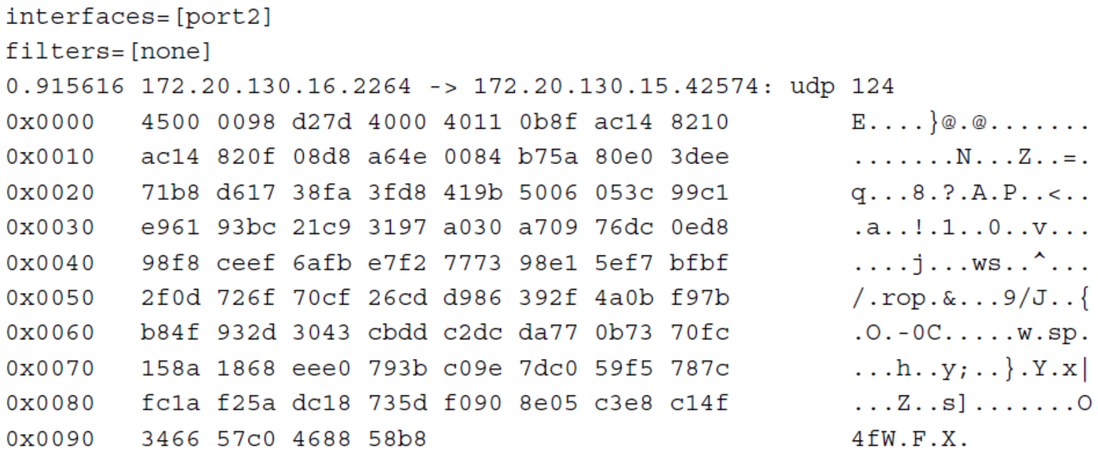
fragment offset

options bits



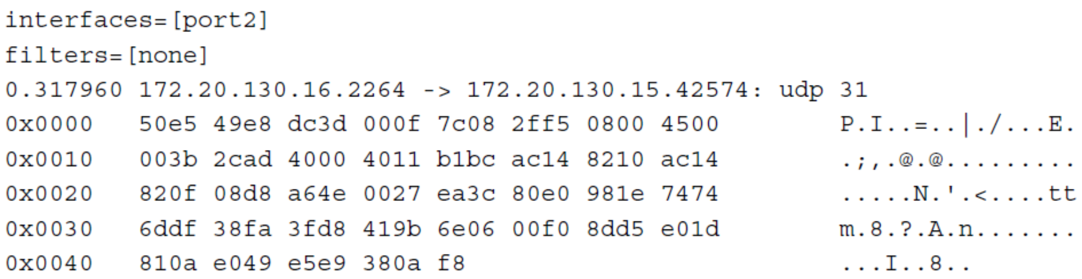
```
interfaces=[port2]
filters=[none]
0.655224 172.20.130.16.2264 -> 172.20.130.15.42574: udp 113
```

- 2 — All of the output from 1, plus the packet payload in both hexadecimal and ASCII. e.g.:



```
interfaces=[port2]
filters=[none]
0.915616 172.20.130.16.2264 -> 172.20.130.15.42574: udp 124
0x0000   4500 0098 d27d 4000 4011 0b8f ac14 8210       E....}@.@.......
0x0010   ac14 820f 08d8 a64e 0084 b75a 80e0 3dee       .......N...Z..=.
0x0020   71b8 d617 38fa 3fd8 419b 5006 053c 99c1       q...8.?.A.P..<..
0x0030   e961 93bc 21c9 3197 a030 a709 76dc 0ed8       .a..!.1..0..v...
0x0040   98f8 ceef 6afb e7f2 7773 98e1 5ef7 bfbf       ....j...ws..^...
0x0050   2f0d 726f 70cf 26cd d986 392f 4a0b f97b       /.rop.&...9/J..{
0x0060   b84f 932d 3043 cbdd c2dc da77 0b73 70fc       .O.-0C.....w.sp.
0x0070   158a 1868 eee0 793b c09e 7dc0 59f5 787c       ...h..y;..}.Y.x|
0x0080   fc1a f25a dc18 735d f090 8e05 c3e8 c14f       ...Z..s].......O
0x0090   3466 57c0 4688 58b8                           4fW.F.X.
```

- 3 — All of the output from 2, plus the link layer (Ethernet) header. e.g.:



```
interfaces=[port2]
filters=[none]
0.317960 172.20.130.16.2264 -> 172.20.130.15.42574: udp 31
0x0000   50e5 49e8 dc3d 000f 7c08 2ff5 0800 4500       P.I..=..|./...E.
0x0010   003b 2cad 4000 4011 b1bc ac14 8210 ac14       .;,.@.@.........
0x0020   820f 08d8 a64e 0027 ea3c 80e0 981e 7474       .....N.'.<....tt
0x0030   6ddf 38fa 3fd8 419b 6e06 00f0 8dd5 e01d       m.8.?.A.n.......
0x0040   810a e049 e5e9 380a f8                        ...I..8..
```

- <packets_int> is the number of packets the sniffer reads before stopping. Packet capture output is printed to your CLI display until you stop it by pressing Ctrl+C, or until it reaches the number of packets that you have specified to capture.

For example, you might capture all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by 3).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl+C. The sniffer then confirms that five packets were seen by that network interface.

(Verbose output can be very long. As a result, output shown below is truncated after only one packet.)

```
FortiWeb# diagnose network sniffer packet port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 ..........)...E.
0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@.;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f........
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or............
0x0040 86bb 0000 0000 0103 0303 ..........
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is often, but not always, preferable to analyze the output by loading it into in a network protocol analyzer application such as Wireshark (http://www.wireshark.org/).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output to a file. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as PuTTY

- a plain text editor such as Notepad

- a Perl interpreter
- network protocol analyzer software such as Wireshark

To view packet capture output using PuTTY and Wireshark

1. On your management computer, start PuTTY.

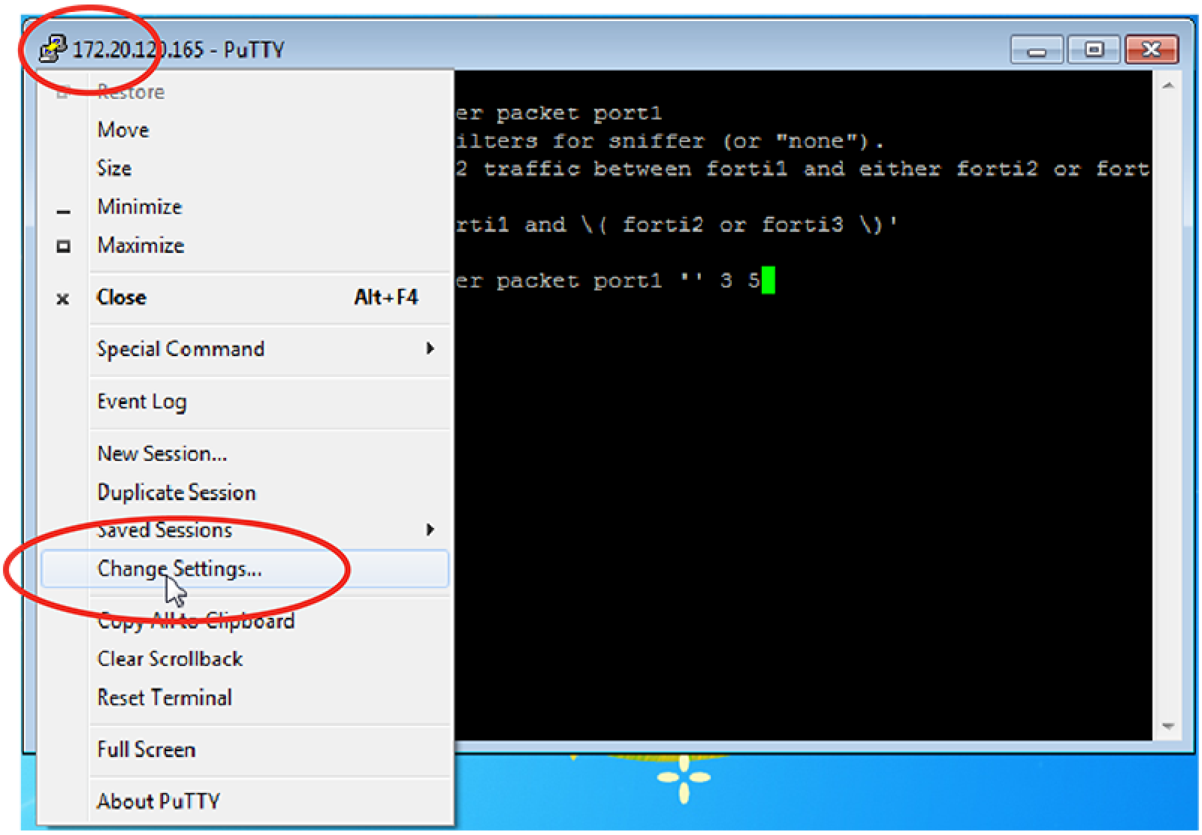
2. Use PuTTY to connect to the FortiWeb appliance using either a local console, SSH, or Telnet connection. For details, see the FortiWeb CLI Reference.

3. Type the packet capture command, such as:

diagnose network sniffer packet port1 'tcp port 443' 3

but do **not** press Enter yet.

4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select **Change Settings**.



```
er packet port1
ilters for sniffer (or "none").
2 traffic between forti1 and either forti2 or fort

rti1 and \( forti2 or forti3 \)'

er packet port1 '' 3 5
```

A dialog appears where you can configure PuTTY to save output to a plain text file.

5. In the **Category** tree on the left, go to **Session** > **Logging.**

6. In **Session logging**, select **Printable output**.

7. In **Log file name**, click the **Browse** button, then choose a directory path and file name such as C:\Users\MyAccount\packet_capture.txt to save the packet capture to a plain text file. (You do not need to save it with the .log file extension.)

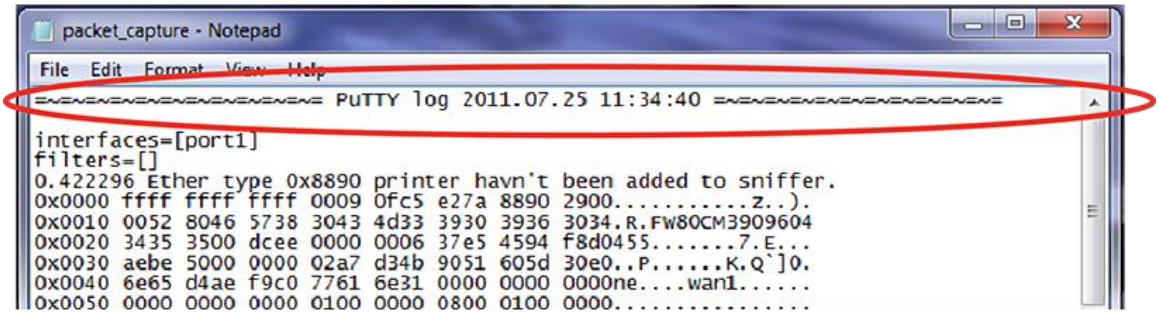
8. Click **Apply**.

9. Press Enter to send the CLI command to the FortiWeb appliance, beginning packet capture.

10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press Ctrl + C to stop the capture.

11. Close the PuTTY window.

12. Open the packet capture file using a plain text editor such as Notepad.



```
=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2011.07.25 11:34:40 =~=~=~=~=~=~=~=~=~=~=~=

interfaces=[port1]
filters=[]
0.422296 Ether type 0x8890 printer havn't been added to sniffer.
0x0000 ffff ffff ffff 0009 0fc5 e27a 8890 2900...........z..).
0x0010 0052 8046 5738 3043 4d33 3930 3936 3034.R.FW80CM3909604
0x0020 3435 3500 dcee 0000 0006 37e5 4594 f8d0455.......7.E...
0x0030 aebe 5000 0000 02a7 d34b 9051 605d 30e0..P......K.Q`]0.
0x0040 6e65 d4ae f9c0 7761 6e31 0000 0000 0000ne....wan1......
0x0050 0000 0000 0000 0100 0000 0800 0100 0000................
```

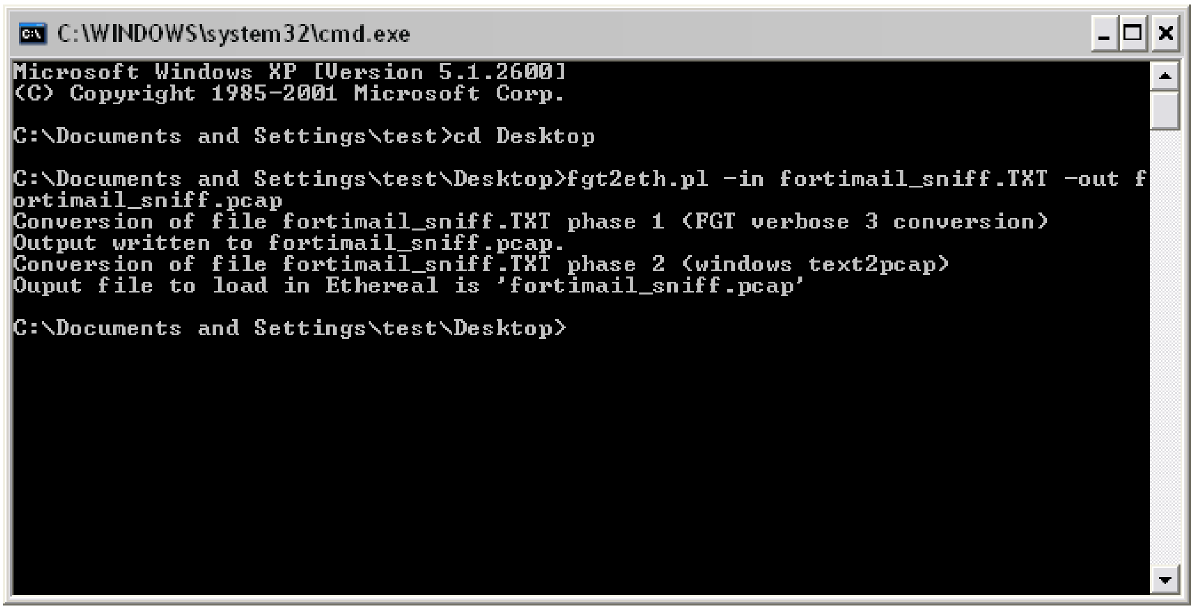
13. Delete the first and last lines, which look like this:

```
=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2/17/2016.07.25 11:34:40
    =~=~=~=~=~=~=~=~=~=~=~=
FortiWeb-2000 #
```

14. Convert the plain text file to a format recognizable by your network protocol analyzer application.

You can convert the plain text file to a format (.pcap) recognizable by Wireshark (formerly called Ethereal) using the fgt2eth.pl Perl script.

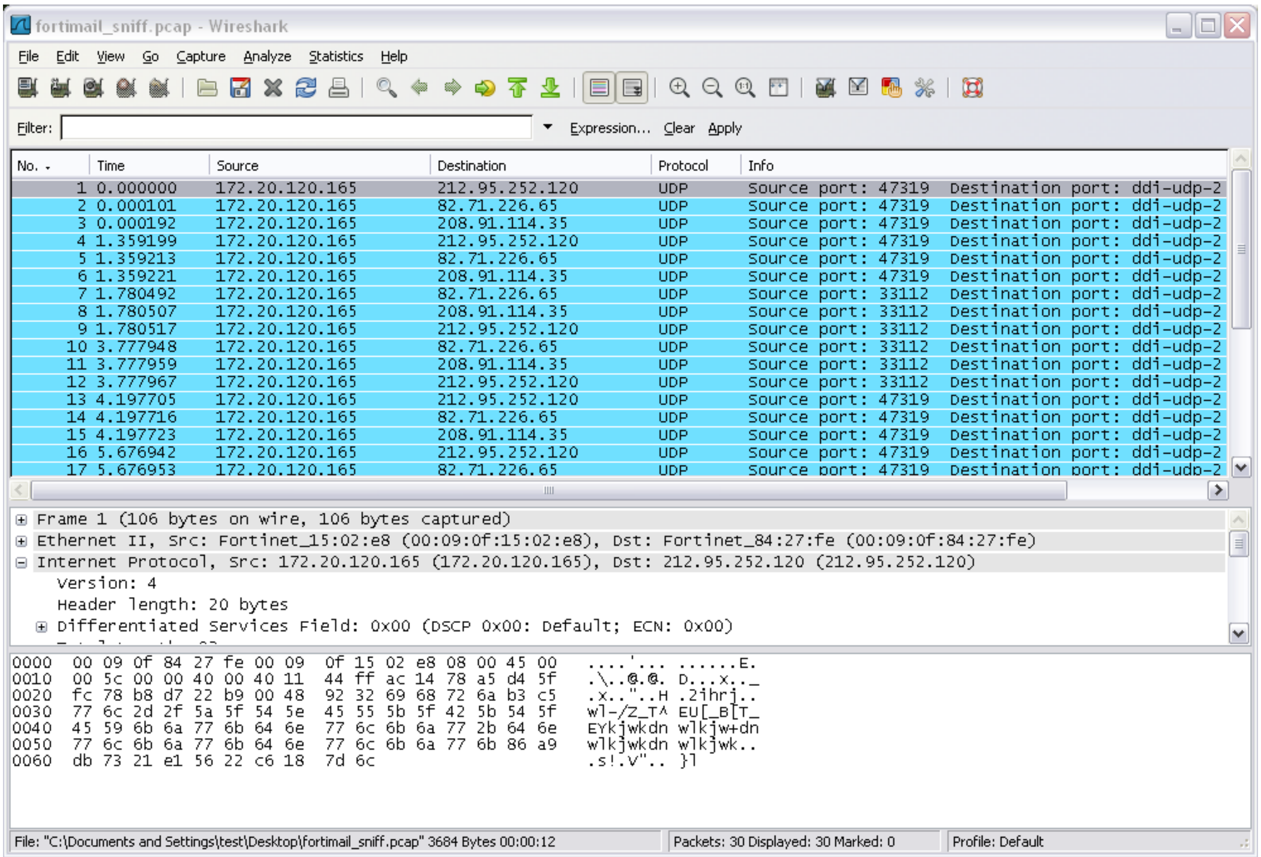
Converting sniffer output to .pcap format



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\test>cd Desktop

C:\Documents and Settings\test\Desktop>fgt2eth.pl -in fortimail_sniff.TXT -out f
ortimail_sniff.pcap
Conversion of file fortimail_sniff.TXT phase 1 (FGT verbose 3 conversion)
Output written to fortimail_sniff.pcap.
Conversion of file fortimail_sniff.TXT phase 2 (windows text2pcap)
Ouput file to load in Ethereal is 'fortimail_sniff.pcap'

C:\Documents and Settings\test\Desktop>
```

15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

Viewing sniffer output in Wireshark



fortimail_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time      Source          Destination     Protocol Info
     1 0.000000  172.20.120.165  212.95.252.120  UDP      Source port: 47319  Destination port: ddi-udp-2
     2 0.000101  172.20.120.165  82.71.226.65    UDP      Source port: 47319  Destination port: ddi-udp-2
     3 0.000192  172.20.120.165  208.91.114.35   UDP      Source port: 47319  Destination port: ddi-udp-2
     4 1.359199  172.20.120.165  212.95.252.120  UDP      Source port: 47319  Destination port: ddi-udp-2
     5 1.359213  172.20.120.165  82.71.226.65    UDP      Source port: 47319  Destination port: ddi-udp-2
     6 1.359221  172.20.120.165  208.91.114.35   UDP      Source port: 47319  Destination port: ddi-udp-2
     7 1.780492  172.20.120.165  82.71.226.65    UDP      Source port: 33112  Destination port: ddi-udp-2
     8 1.780507  172.20.120.165  208.91.114.35   UDP      Source port: 33112  Destination port: ddi-udp-2
     9 1.780517  172.20.120.165  212.95.252.120  UDP      Source port: 33112  Destination port: ddi-udp-2
    10 3.777948  172.20.120.165  82.71.226.65    UDP      Source port: 33112  Destination port: ddi-udp-2
    11 3.777959  172.20.120.165  208.91.114.35   UDP      Source port: 33112  Destination port: ddi-udp-2
    12 3.777967  172.20.120.165  212.95.252.120  UDP      Source port: 33112  Destination port: ddi-udp-2
    13 4.197705  172.20.120.165  212.95.252.120  UDP      Source port: 47319  Destination port: ddi-udp-2
    14 4.197716  172.20.120.165  82.71.226.65    UDP      Source port: 47319  Destination port: ddi-udp-2
    15 4.197723  172.20.120.165  208.91.114.35   UDP      Source port: 47319  Destination port: ddi-udp-2
    16 5.676942  172.20.120.165  212.95.252.120  UDP      Source port: 47319  Destination port: ddi-udp-2
    17 5.676953  172.20.120.165  82.71.226.65    UDP      Source port: 47319  Destination port: ddi-udp-2
```

```
⊞ Frame 1 (106 bytes on wire, 106 bytes captured)
⊞ Ethernet II, Src: Fortinet_15:02:e8 (00:09:0f:15:02:e8), Dst: Fortinet_84:27:fe (00:09:0f:84:27:fe)
⊟ Internet Protocol, Src: 172.20.120.165 (172.20.120.165), Dst: 212.95.252.120 (212.95.252.120)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
0000  00 09 0f 84 27 fe 00 09  0f 15 02 e8 08 00 45 00   ....'... ......E.
0010  00 5c 00 00 40 00 40 11  44 ff ac 14 78 a5 d4 5f   .\..@.@. D...x.._
0020  fc 78 b8 d7 22 b9 00 48  92 32 69 68 72 6a b3 c5   .x.."..H .2ihrj..
0030  77 6c 2d 2f 5a 5f 54 5e  45 55 5b 5f 42 5b 54 5f   wl-/Z_T^ EU[_B[T_
0040  45 59 6b 6a 77 6b 64 6e  77 6c 6b 6a 77 2b 64 6e   EYkjwkdn wlkjw+dn
0050  77 6c 6b 6a 77 6b 64 6e  77 6c 6b 6a 77 6b 86 a9   wlkjwkdn wlkjwk..
0060  db 73 21 e1 56 22 c6 18  7d 6c                     .s!.V".. }l
```

File: "C:\Documents and Settings\test\Desktop\fortimail_sniff.pcap" 3684 Bytes 00:00:12 | Packets: 30 Displayed: 30 Marked: 0 | Profile: Default

7.2 Solutions by issue type

7.2.1 Connectivity issues

One of your first tests when configuring a new policy should be to determine whether allowed traffic is flowing to your web servers.

- Is there a server policy applied to the web server or servers FortiWeb was installed to protect? If it is operating in reverse proxy mode, FortiWeb will not allow any traffic to reach a protected web server unless there is a matching server policy that permits it.

- If your network utilizes secure connections (HTTPS) and there is no traffic flow, is there a problem with your certificate?

- If you run a test attack from a browser aimed at your web site, does it show up in the attack log?

To verify, configure FortiWeb to detect the attack, then craft a proof-of-concept that will trigger the attack sensor. For example, to see whether directory traversal attacks are being logged and/or blocked, you could use your web browser to go to:

http://www.example.com/login?user=../../../../

Under normal circumstances, you should see a new attack log entry in the Attack Log widget of the system dashboard.

Examining the ARP table

When you have poor connectivity, another good place to look for information is the address resolution protocol (ARP) table. A functioning ARP is especially important in high-availability configurations.

To check the ARP table in the CLI, enter:

```
diagnose network arp list
```

Checking routing

ping and traceroute are useful tools in network connectivity and route troubleshooting.

Since you typically use these tools to troubleshoot, you can allow ICMP, the protocol used by these tools, in firewall policies and on interfaces only when you need them. Otherwise, disable ICMP for improved security and performance.

By default, the FortiWeb appliance will forward only HTTP/HTTPS traffic to your protected web servers. (That is, routing/IP-based forwarding is disabled.) For information on enabling forwarding of FTP or other protocols, see the config router setting command in the FortiWeb CLI Reference.

By default, FortiWeb appliances will respond to ping and traceroute. However, if the appliance does not respond, and there are no firewall policies that block it, ICMP type 0 (ECHO_REPSPONSE) might be effectively disabled.

To enable ping and traceroute responses from FortiWeb

1. Go to **System > Network > Interface.**

   To access this part of the web UI, you must have **Read** and **Write** permission in your administrator's account access profile to items in the **Router Configuration** category.

2. In the row for the network interface which you want to respond to ICMP type 8 (ECHO_REQUEST) for ping and UDP for traceroute, click **Edit**.

   A dialog appears.

3. Enable PING.

4. If Trusted Host #1, Trusted Host #2, and Trusted Host #3 have been restricted, verify that they include your computer or device's IP address. Otherwise FortiWeb will not respond.

5. Click **OK.**

   The appliance should now respond when another device such as your management computer sends a ping or traceroute to that network interface.

To verify routes between clients and your web servers

1. Attempt to connect **through** the FortiWeb appliance, from a client to a protected web server, via HTTP and/or HTTPS.

   If the connectivity test fails, continue to the next step.

2. Use the ping command on both the client and the server to verify that a route exists between the two. Test traffic movement in both directions: from the client to the server, and the server to the client. Web servers do not need to be able to initiate a connection, but must be able to send reply traffic along a return path.

   If the routing test **succeeds**, continue with step 4.

   If the routing test **fails**, continue to the next step.

3. Use the tracert or traceroute command on both the client and the server (depending on their operating systems) to locate the point of failure along the route.

   If the route is broken when it reaches the FortiWeb appliance, first examine its network interfaces and routes. To display network interface addresses and subnets, enter the CLI command:

   ```
   show system interface
   ```

   To display all recently-used routes with their priorities, enter the CLI command:

   ```
   diagnose network route list
   ```

   You may need to verify that the physical cabling is reliable and not loose or broken, that there are no IP address or MAC address conflicts or blacklisting, misconfigured DNS records, and otherwise rule out problems at the physical, network, and transport layer.

   If these tests **succeed**, a route exists, but you cannot connect using HTTP or HTTPS, an application-layer problem is preventing connectivity.

4. For application-layer problems, on the FortiWeb, examine the:

- matching server policy and all components it references
- certificates (if connecting via HTTPS)
- web server service/daemon (it should be running, and configured to listen on the port specified in the server policy for HTTP and/or HTTPS, for virtual hosts, they should be configured with a correct Host:name)

On routers and firewalls between the host and the FortiWeb appliance, verify that they permit HTTP and/or HTTPS connectivity between them.

Testing for connectivity with ping

The ping command sends a small data packet to the destination and waits for a response. The response has a timer that may expire, indicating that the destination is unreachable via ICMP.

Connectivity via ICMP only proves that a route exists. It does **not** prove that connectivity also exists via other protocols at other layers such as HTTP.

ICMP is part of Layer 3 on the OSI Networking Model. ping sends Internet Control Message Protocol (ICMP) ECHO_REQUEST (“ping”) packets to the destination, and listens for ECHO_RESPONSE (“pong”) packets in reply.

Some networks block ICMP packets because they can be used in a ping flood or denial of service (DoS) attack if the network does not have anti-DoS capabilities, or because ping can be used by an attacker to find potential targets on the network.

Beyond basic existence of a possible route between the source and destination, ping tells you the amount of packet loss (if any), how long it takes the packet to make the round trip (latency), and the variation in that time from packet to packet (jitter).

If ping shows **some** packet loss, investigate:

- cabling to eliminate loose connections
- ECMP, split horizon, or network loops
- all equipment between the ICMP source and destination to minimize hops

If ping shows **total** packet loss, investigate:

- cabling to eliminate incorrect connections
- all firewalls, routers, and other devices between the two locations to verify correct IP addresses, routes, MAC lists, trusted hosts, and policy configurations

If ping finds an outage between two points, use traceroute to locate exactly where the problem is.

To ping a device from the FortiWeb CLI

1. Log in to the CLI via either SSH, Telnet, or You can ping from the FortiWeb appliance in the **CLI Console** widget of the web UI.

2. If you want to adjust the behavior of execute ping, first use the execute ping options command.

3. Enter the command:

execute ping <destination_ipv4>

where <destination_ipv4> is the IP address of the device that you want to verify that the appliance can connect to, such as 192.168.1.1.

To verify that routing is bidirectionally symmetric, you should also ping the appliance.

If the appliance can reach the host via ICMP, output similar to the following appears:

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=253 time=6.5 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=253 time=7.4 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=253 time=6.0 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=253 time=5.5 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=253 time=7.3 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.5/6.5/7.4 ms
```

If the appliance **cannot** reach the host via ICMP, output similar to the following appears:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...

--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

“100% packet loss” and “Timeout” indicates that the host is not reachable.

Testing routes & latency with traceroute

traceroute sends ICMP packets to test each hop along the route. It sends three packets to the destination, and then increases the time to live (TTL) setting by one, and sends another three packets to the destination. As the TTL increases, packets go one hop farther along the route until they reach the destination.

Most traceroute commands display their maximum hop count — that is, the maximum number of steps it will take before declaring the destination unreachable — before they start tracing the route. The TTL setting may result in routers or firewalls along the route timing out due to high latency.

Where ping only tells you if the signal reached its destination and returned successfully, traceroute shows each step of its journey to its destination and how long each step takes. If you specify the destination using a domain name, the traceroute output can also indicate DNS problems, such as an inability to connect to a DNS server.

By default, traceroute uses UDP with destination ports numbered from 33434 to 33534. The traceroute utility usually has an option to specify use of ICMP ECHO_REQUEST (type 8) instead, as used by the Windows tracert utility. If you have a firewall and you want traceroute to work from both machines (Unix-like systems and Windows) you will need to allow **both** protocols inbound through your firewall (UDP ports 33434 - 33534 and ICMP type 8).

To trace the route to a device from the FortiWeb CLI

1. Log in to the CLI via either SSH, Telnet, or You can ping from the FortiWeb appliance in the **CLI Console** widget of the web UI.

2. Enter the command:

```
execute traceroute {<destination_ipv4> | <destination_fqdn>}
```

where {<destination_ipv4> | <destination_fqdn>} is a choice of either the device’s IP address or its fully qualified domain name (FQDN).

For example, you might enter:

```
execute traceroute www.example.com
```

If the appliance **has** a complete route to the destination, output similar to the following appears:

```
traceroute to www.fortinet.com (66.171.121.34), 32 hops max, 84 byte packets

1 172.16.1.2 0 ms 0 ms 0 ms

2 209.87.254.221 <static-209-87-254-221.storm.ca> 2 ms 2 ms 2 ms

3 209.87.239.129 <core-2-g0-1-1104.storm.ca> 2 ms 1 ms 2 ms

4 67.69.228.161 2 ms 2 ms 3 ms

5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 3 ms 2 ms

6 64.230.132.234 <core2-ottawatc_POS5-0-0.net.bell.ca> 20 ms 20 ms 20 ms

7 64.230.132.58 <core4-toronto21_POS0-12-4-0.net.bell.ca> 24 ms 21 ms 24 ms

8 64.230.138.154 <bx4-toronto63_so-2-0-0-0.net.bell.ca> 8 ms 9 ms 8 ms
```

```
9 64.230.185.145 <bx2-ashburn_so2-0-0.net.bell.ca> 23 ms 23 ms 23 ms

10 12.89.71.9 23 ms 22 ms 22 ms

11 12.122.134.238 <cr2.wswdc.ip.att.net> 100 ms 12.123.10.130 <cr2.wswdc.ip.att.net> 101 ms 102 ms

12 12.122.18.21 <cr1.cgcil.ip.att.net> 101 ms 100 ms 99 ms

13 12.122.4.121 <cr1.sffca.ip.att.net> 100 ms 98 ms 100 ms

14 12.122.1.118 <cr81.sj2ca.ip.att.net> 98 ms 98 ms 100 ms

15 12.122.110.105 <gar2.sj2ca.ip.att.net> 96 ms 96 ms 96 ms

16 12.116.52.42 94 ms 94 ms 94 ms

17 203.78.181.10 88 ms 87 ms 87 ms

18 203.78.181.130 90 ms 89 ms 90 ms

19 66.171.121.34 <fortinet.com> 91 ms 89 ms 91 ms

20 66.171.121.34 <fortinet.com> 91 ms 91 ms 89 ms
```

Each line lists the routing hop number, the IP address and FQDN (if any) of that hop, and the 3 response times from that hop. Typically a value of <1ms indicates a local router.

If the appliance **does not** have a complete route to the destination, output similar to the following appears:

```
traceroute to 10.0.0.1 (10.0.0.1), 32 hops max, 84 byte packets

1 172.16.1.2 0 ms 0 ms 0 ms

2 172.16.1.10 0 ms 0 ms 0 ms

3 * * *

4 * * *
```

Examining the routing table

When a route does not exist, or when hops have high latency, examine the routing table. The routing table is where the FortiWeb appliance caches recently used routes.

If a route is cached in the routing table, it saves time and resources that would otherwise be required for a route lookup. If the routing table is full and a new route must be added, the oldest, least-used route is deleted to make room.

To check the routing table in the CLI, enter:

```
diagnose network route list
```

Checking port assignments

If you are attempting to connect to FortiWeb on a given network port, and the connection is expected to occur on a different port number, the attempt will fail. For a list of ports used by FortiWeb, see Appendix A: Port numbers. For ports used by your own HTTP network services, see Defining your network services.

Performing a packet trace

When troubleshooting malformed packet or protocol errors, it helps to look inside the protocol headers of packets to determine if they are traveling along the route you expect, and with the flags and other options you expect.

If you configure virtual servers on your FortiWeb appliance, packets' destination IP addresses will be those IP addresses, not the physical IP addresses (i.e., the IP address of port1, etc.). An ARP update is sent out when a virtual IP address is configured.

If the packet trace shows that packets are arriving at your FortiWeb appliance's interfaces but no HTTP/HTTPS packets egress, check that:

- Physical links are firmly connected, with no loose wires
- Network interfaces/bridges are brought up (see Configuring the network interfaces)
- Link aggregation peers, if any, are up (see Link aggregation)
- VLAN IDs, if any, match (see Adding VLAN subinterfaces)
- Virtual servers or V-zones exist, and are enabled (see Configuring a bridge (V-zone) and Configuring virtual servers on your FortiWeb)
- Matching policies exist, and are enabled (see Configuring basic policies)
- If using HTTPS, valid server/CA certificates exist (see How to offload or inspect HTTPS)
- IP-layer, and HTTP-layer routes, if necessary, match (see Adding a gateway and Routing based on HTTP content)
- Web servers are responsive, if server health checks are configured and enabled (see Configuring server up/down checks)
- Load balancers, if any, are defined (see Defining your proxies, clients, & X-headers)
- Clients are not blacklisted (see Monitoring currently blocked IPs)

Debugging the packet processing flow

If you have determined that network traffic is not entering and leaving the FortiWeb appliance as expected, or not flowing through policies and scans as expected, you can debug the packet flow using the CLI.

For example, the following commands enable debug logs and the logs timestamp, and set other parameters for debug logging:

```
diagnose debug enable
diagnose debug console timestamp enable
diagnose debug application proxy 7
diagnose debug flow show module-process-detail
diagnose debug flow trace start
diagnose debug flow filter server-ip 172.16.1.20
```

Checking the SSL/TLS handshake & encryption

If the client is attempting to make an HTTPS connection, but the attempt fails after the connection has been initiated, during negotiation, the problem may be with SSL/TLS. Symptoms may include error messages such as:

- ssl_error_no_cypher_overlap
  (Mozilla Firefox 9.0.1)

- Error 113 (net::ERROR_SSL_VERSION_OR_CIPHER_MISMATCH): Unknown error.
  (Google Chrome 16.0.912.75 m)

Expected SSL/TLS behavior varies by SSL inspection vs. SSL offloading (see Offloading vs. inspection):

SSL offloading — Reverse proxy mode only (see Supported features in each operation mode). The handshake is between the client and FortiWeb. If the connection cannot be established, verify that the browser supports one of the key exchanges, encryption algorithms, and authentication (hashes) offered by FortiWeb. See Supported cipher suites & protocol versions.

SSL inspection — True transparent proxy, offline protection mode and transparent inspection mode only.
The handshake is between the client and the **web server**. If the connection cannot be established, verify that the browser supports one of the key exchanges, encryption algorithms, and authentication (hashes) suggested by the web server. Server-side, you must also verify that your web server supports enough cipher suites that all required clients can connect.

Google Chrome will prefer an anonymous Diffie-Hellman key exchange. This has the property of perfect forward secrecy, which makes SSL inspection theoretically impossible. To guarantee that this is not used to hide attacks from FortiWeb, you must disable it on your web server. On Apache, you would add !ADH to the SSLCipherSuite configuration line. For example:

SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW

If you are not sure which cipher suites are currently supported, you can use SSL tools such as OpenSSL to discover support. For example, you could use this client-side command to know whether the web server or FortiWeb supports strong (HIGH) encryption:

openssl s_client -connect example.com:443 -cipher HIGH

or supports deprecated or old versions such as SSL 2.0:

openssl s_client -ssl2 -connect example.com:443

If your web servers are required to comply with PCI DSS, you should make sure that your web servers do not allow weak encryption. For example, if your web servers accept SSL 2.0 or MD5 hashes, you may fail your PCI DSS audit.

7.2.2 Resources issues

This section includes troubleshooting questions related to sluggish or stalled performance.

- Is a process consuming too much system resources?
- Is a server under attack?
- Has there been a sustained spike in HTTP traffic related to a specific policy?

Killing system-intensive processes

Use the CLI to view the per-CPU/core process load level and a list of the most system-intensive processes. This may show processes that are consuming resources unusually. For example:

```
diagnose system top 10
```

The above command generates a report of processes every 10 seconds. The report provides the process names, their process ID (pid), status, CPU usage, and memory usage.

The report continues to refresh and display in the CLI until you press q (quit).

Once you locate an offending PID, you can terminate it:

```
diagnose system kill 9 <pid_int>
```

To determine if high load is frequently a problem, you can display the average load level by using these CLI commands:

```
get system performance

diagnose system load
```

If the issue recurs, and corresponds with a signature or configuration change, you may need to optimize regular expressions to prevent the issue from recurring. See Debugging the packet processing flowand Regular expression performance tips.

Monitoring traffic load

Heavy traffic loads can cause sustained high CPU or RAM usage. If this is unusual, no action may be required, unless you are being subject to a DoS attack. Sustained heavy traffic load may indicate that you need a more powerful model of FortiWeb.

In the FortiWeb appliance's web UI, you can view traffic load two ways:

- Monitor current HTTP traffic on the dashboard. Go to **System** > **Status** > **Status** and examine the graphs in the **Policy Summary** widget.
- Examine traffic history in the traffic log. Go to **Logs&Report** > **Log Access** > **Traffic**.

Preparing for attacks

A prolonged denial of service (DoS) or brute-force login attack (to name just a few) can bring your web servers to a standstill, if your FortiWeb appliance is not configured for it.

To fight DoS attacks, see DoS prevention.

In the FortiWeb appliance's web UI, you can watch for attacks in two ways:

- Monitor current HTTP traffic on the dashboard. Go to **System** > **Status** > **Status** and examine the attack event history graph in the **Policy Summary** widget.
- Examine attack history in the traffic log. Go to **Logs&Report** > **Log Access** > **Attack**.

Before attacks occur, use the FortiWeb appliance's rich feature set to configure attack defenses.

7.2.3 Login Issues

If the person cannot access the login page at all, it is usually actually a connectivity issue (see Ping & traceroute and Configuring the network settings) unless all accounts are configured to accept logins only from specific IP addresses.

If an administrator can connect, but cannot log in, even though providing the correct account name and password, and is receiving this error message:

```
Too many bad login attemptsor reached max number of logins. Please try
again in a few minutes. Login aborted.
```

single administrator mode may have been enabled.

If the person has lost or forgotten his or her password, the admin account can reset other accounts' passwords.

Checking user authentication policies

In FortiWeb, users and organized into groups. Groups are part of authentication policies. If several users have authentication problems, it is possible someone changed authentication policy or user group memberships. If a user is legitimately having an authentication policy, you need to find out where the problem lies.

To troubleshoot user access

1. In the web UI, go to **User > User Group > User Group** and examine each group to locate the name of the problem user.

2. Note the user group to which the affected users belong, especially if multiple affected users are part of one group. If the user is not a group member, there is no access.

3. Go to **Application Delivery > Authentication Policy > Authentication Rule** and determine which rule contains the problem user group. If the user group is not part of a rule, there is no access.

4. Go to **Application Delivery > Authentication Policy > Authentication Policy** and locate the policy that contains the rule governing the problem user group. If the rule is not part of a policy, there is no access.

5. Go to **Policy > Web Protection Profile > Inline Protection Profile** and determine which profile contains the related authentication policy. If the policy is not part of a profile, there is no access.

6. Make sure that inline protection profile is included in the server policy that applies to the server the user is trying to access. If the profile is not part of the server policy, there is no access.

Authentication involves user groups, authentication rules and policy, inline protection policy, and finally, server policy. If a user is not in a user group used in the policy for a specific server, the user will have no access.

When an administrator account cannot log in from a specific IP

If an administrator is entering his or her correct account name and password, but cannot log in from some or all computers, examine that account's trusted host definitions (see Trusted Host #1). It should include all locations where that person is allowed to log in, such as your office, but should **not** be too broad.

Remote authentication query failures

If your network administrators' or other accounts reside on an external server (e.g. Active Directory or RADIUS), first switch the account to be locally defined on the FortiWeb appliance. If the local account **fails**, correct connectivity between the client and appliance (see Connectivity issues). If the local account **succeeds**, troubleshoot connectivity between the appliance and your authentication server. If routing exists but authentication still fails, you can verify correct vendor-specific attributes and other protocol-specific fields by running a packet trace (see Packet capture).

Resetting passwords

If someone has forgotten or lost his or her password, or if you need to change an account's password, the admin administrator can reset the password.

If you forget the password of the admin administrator, however, you will **not** be able to reset its password through the web UI. You can either:

- reset the FortiWeb appliance to its default state (including the default administrator account and password) by restoring the firmware. For instructions, see Restoring firmware ("clean install").
- connect to the local console, reboot the FortiWeb appliance, and set the password (see To reset the admin account's password)

To reset an account's password

1. Log in as the admin administrator account.
2. Go to **System** > **User** > **User**.
3. Click the row to select the account whose password you want to change.
4. Click **Edit**.
5. In the **New Password** and **Confirm Password** fields, type the new password.
6. Click **OK**.

The new password takes effect the next time that account logs in.

7. Power off the FortiWeb appliance.
8. Find the serial number of the FortiWeb.

This is usually on the bottom of physical appliances. If you have previously registered the appliance to associate it with your Fortinet Technical Support account, you can also retrieve it from the web site.

9. On your computer, copy the serial number.

This is so that you are ready to quickly paste it into the terminal emulator. (Typing it slowly may cause the login to time out.) The serial number is **case sensitive**.

10. While the appliance is shut down, connect the local console port of your appliance to your computer.

11. On your management computer, start a terminal emulator such as PuTTY. For details, see To connect to the CLI using a local console connection.

12. Power on the FortiWeb appliance.

Power on self-test (POST) and other messages should begin to appear in the console.

13. Between 15 - 30 seconds after the login prompt appears, immediately enter:

```
maintainer
```

then enter:

```
bcpb<serial-number_str>
```

where <serial-number_str> is the serial number. (If you have copied it, in PuTTY, you can right-click to quickly paste it, instead of typing it in. This will prevent the login from timing out.)

If you are successful, the CLI will welcome you, and you can then enter the following commands to reset the admin account’s password:

```
config system admin

edit admin

set password <new-password_str>

end

exit
```

where <new-password_str> is the password for the administrator account named admin.

If you do **not** enter both the correct user name and the password within the correct time frame, the console will display an error message:

```
The hashed password length is invalid
```

To attempt the login again, power cycle the appliance.

7.2.4 Data Storage Issues

If FortiWeb cannot locally store any data such as logs, reports, and web site backups for anti-defacement, it might have a damaged or corrupted hard disk. For fixes, see Hard disk corruption or failure.

If FortiWeb has been storing data but has suddenly stopped, first verify that FortiWeb has not used all of its local storage capacity by entering this CLI command:

```
diagnose system mount list
```

to display disk usage for all mounted file systems, such as:

```
Filesystem 1k-blocks Used Available Use% Mounted on

/dev/ram0 61973 31207 30766 50% /

none 262144 736 261408 0% /tmp

none 262144 0 262144 0% /dev/shm

/dev/sdb2 38733 25119 11614 68% /data

/dev/sda1 153785572 187068 145783964 0% /var/log

/dev/sdb3 836612 16584 777528 2% /home
```

If a full disk is not the problem, examine the configuration to determine if an administrator has disabled those features that store data.

If neither of those indicate the cause of the problem, verify that the disk's file system has not been mounted in read-only mode, which can occur if the hard disk is experiencing problems with its write capabilities (see Hard disk corruption or failure).

7.2.5 Bootup Issues

FortiWeb appliances usually have multiple disks. FortiWeb stores its firmware (operating system) and configuration files in a flash disk, but most models of FortiWeb also have an internal hard disk or RAID that is used to store non-configuration/firmware data such as logs, reports, auto-learning data, and web site backups for anti-defacement. During startup, after FortiWeb loads its boot loader, FortiWeb will attempt to mount its data disk. If this fails due to errors, you will have the opportunity to attempt to recover the disk.

To determine if one of FortiWeb's internal disks may either:

- have become corrupted

- have experienced mechanical failure

view the event log. If the data disk failed to mount, you should see this log message:

```
date=2012-09-27 time=07:49:07 log_id=00020006 msg_id=000000000002 type=event
subtype="system" pri=alert device_id=FV-1KC3R11700136 timezone="(GMT-5:00)Eastern Time(US &
Canada)" msg="log disk is not mounted"
```

Connect to FortiWeb’s CLI via local console, then supply power. After the boot loader starts, you should see this prompt:

```
Press [enter] key for disk integrity verification.
```

Pressing the Enter key will cause FortiWeb to check the hard disk’s file system to attempt to resolve any problems discovered with that disk’s file system, and to determine if the disk can be mounted (mounted disks should appear in the internal list of mounted file systems, /etc/mtab). During the check, FortiWeb will describe any problems that it finds, and the results of disk recovery attempts, such as:

```
ext2fs_check_if_mount: Can’t detect if filesystem is mounted due to missing mtab file while determining
where /dev/sda1 is mounted.

/dev/sda1: recovering journal

/dev/sda1: clean, 56/61054976 files, 3885759/244190638 blocks
```

If the problem occurs while FortiWeb is still running (or after an initial reboot and attempt to repair the file system), in the CLI, enter:

```
diagnose hardware harddisk list
```

to display the number and names of mounted file systems.

For example, on a FortiWeb 1000C with a single properly functioning internal hard disk plus its internal flash disk, this command should show two file systems:

```
name size(M)

sda 1000204.89

sdb 1971.32
```

where sda, the larger file system, is from the hard disk used to store non-configuration/firmware data.

If that command does **not** list the data disk’s file system, FortiWeb did not successfully mount it. Try to reboot and run the file system check.

If the data disk’s file system **is** listed and appears to be the correct size, FortiWeb could mount it. However, there still could be other problems preventing the file system from functioning, such as being mounted in read-only mode, which would prevent new logs and other data from being recorded. To determine this, enter:

diagnose hardware logdisk info

to display the count, capacity, RAID status/level, partition numbers, and read-write/read-only mount status.

For example, on a FortiWeb-1000C with a single properly functioning data disk, this command should show:

disk number: 1

disk[0] size: 976.76GB

raid level: raid1

partition number: 1

mount status: read-write

You can also display the status of each individual disk in the RAID array:

FortiWeb # diag hardware raid list

disk-number size(M) level

0(OK),1(OK), 1877274 raid1

If the file system could **not** be fixed by the file system check, it may be physically damaged or components may have worn out prematurely. Most commonly, this is caused by either:

- failing to shut down FortiWeb's operating system before disconnecting the power (e.g. someone pulled the power plug while FortiWeb was running)
- logging misconfiguration (e.g. logging very frequent logs like traffic logs or debug logs for an extended period of time to the local hard drive)

7.2.6 Issues forwarding non-HTTP/HTTPS traffic

If FortiWeb is operating in reverse proxy mode, by default, it does not forward non HTTP/HTTPS protocols to protected servers.

However, you can use the following command to enable IP-based forwarding (routing):

```
config router setting
 set ip-forward {enable | disable}
end
```