Business Services

FortiGate

on OCB-FE
Troubleshooting Guide

6th December 2018
version 1.0

Document control

date	version no.	author	change/addition
6th December 2018	1.0	Ahmad Samak	Document Creation

Business Services orange

Table of contents

Business
Services   orange

Business
Services orange™

1 Introduction

This document provides troubleshooting techniques for some frequently encountered problems of the FortiGate 5.x. 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.

Business Services   orange

2 Ports

2.1 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

Business Services   orange™

2.2 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

Business
Services   orange

3 Troubleshooting resources

Before you begin troubleshooting, you need to know Fortinet's troubleshooting resources. Doing so will shorten the time to solve your issue. Indeed, an administrator can save time and effort during the troubleshooting process by first checking if the issue has been experienced before. Several self-help resources are available to provide valuable information about FortiOS technical issues, including:

Technical Documentation

Installation Guides, Administration Guides, Quick Start Guides, and other technical documents are available online at the following URL:

http://docs.fortinet.com

Fortinet Video Library

The Fortinet Video Library hosts a collection of video which provide valuable information about Fortinet products.

http://video.fortinet.com

Release Notes

Issues that are uncovered after the technical documentation has been published will often be listed in the Release Notes that accompany the device.

Knowledge Base

The Fortinet Knowledge Base provides access to a variety of articles, white papers, and other documentation providing technical insight into a range of Fortinet products. The Knowledge Base is available online at the following URL:

http://kb.fortinet.com

Fortinet Technical Discussion Forums

An online technical forums allow administrators to contribute to discussions about issues related to their Fortinet products. Searching the forum can help the administrator identify if an issue has been experienced by another user. The support forums can be accessed at the following URL:

http://support.fortinet.com/forum

Fortinet Training Services Online Campus

The Fortinet Training Services Online Campus hosts a collection of tutorials and training materials which can be used to increase knowledge of the Fortinet products.

http://campus.training.fortinet.com

Business
Services   orange

Fortinet Customer Support

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, its time to contact Fortinet Customer Support for assistance.

http://support.fortinet.com

4 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.

4.1 Establish a baseline

FortiGate 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 FortiGate 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

Business Services orange™

These commands are just a sample. Feel free to include any extra information gathering commands that apply to your system. For example if you have active VPN connections, record information about them using the get vpn * series of commands.

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.

4.2   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.

4.3   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.

4.4   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.

4.4.1   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.

Business
Services   orange

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.

4.5   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.

4.6   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.

4.7   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.

Business
Services   orange

5 Troubleshooting Decision Tree

5.1 (FG-VM + OCB-FE) troubleshooting diagram

FortiGate - VM
Troubleshooting Decision Diagram (FG-VM + Orange Flex Engine)

Business
Services orange™
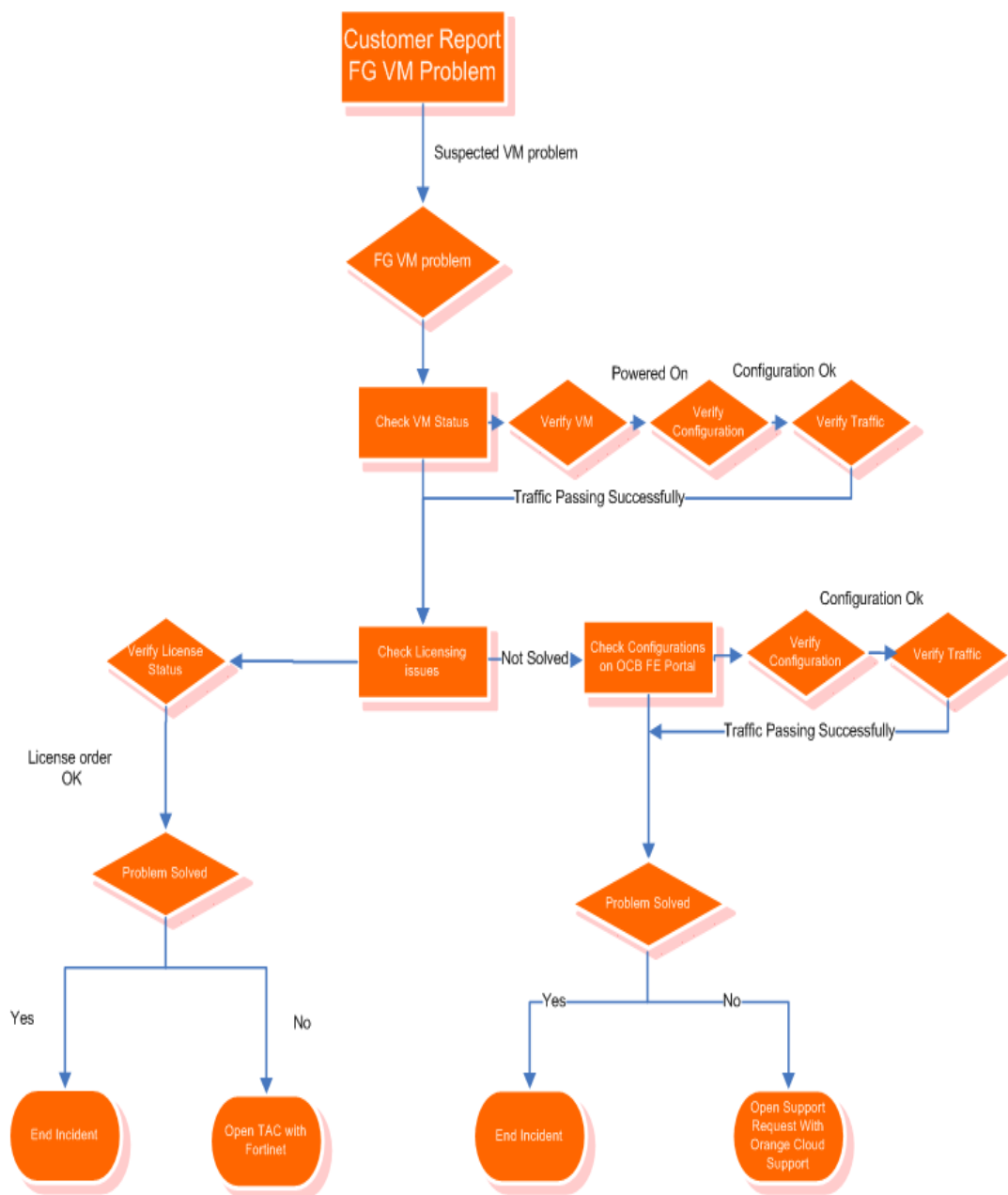
5.2 FortiGate VM + IPSec troubleshooting diagram

FortiGate - VM
Troubleshooting Decision Diagram (PAN-VM + IPSec VPNs)
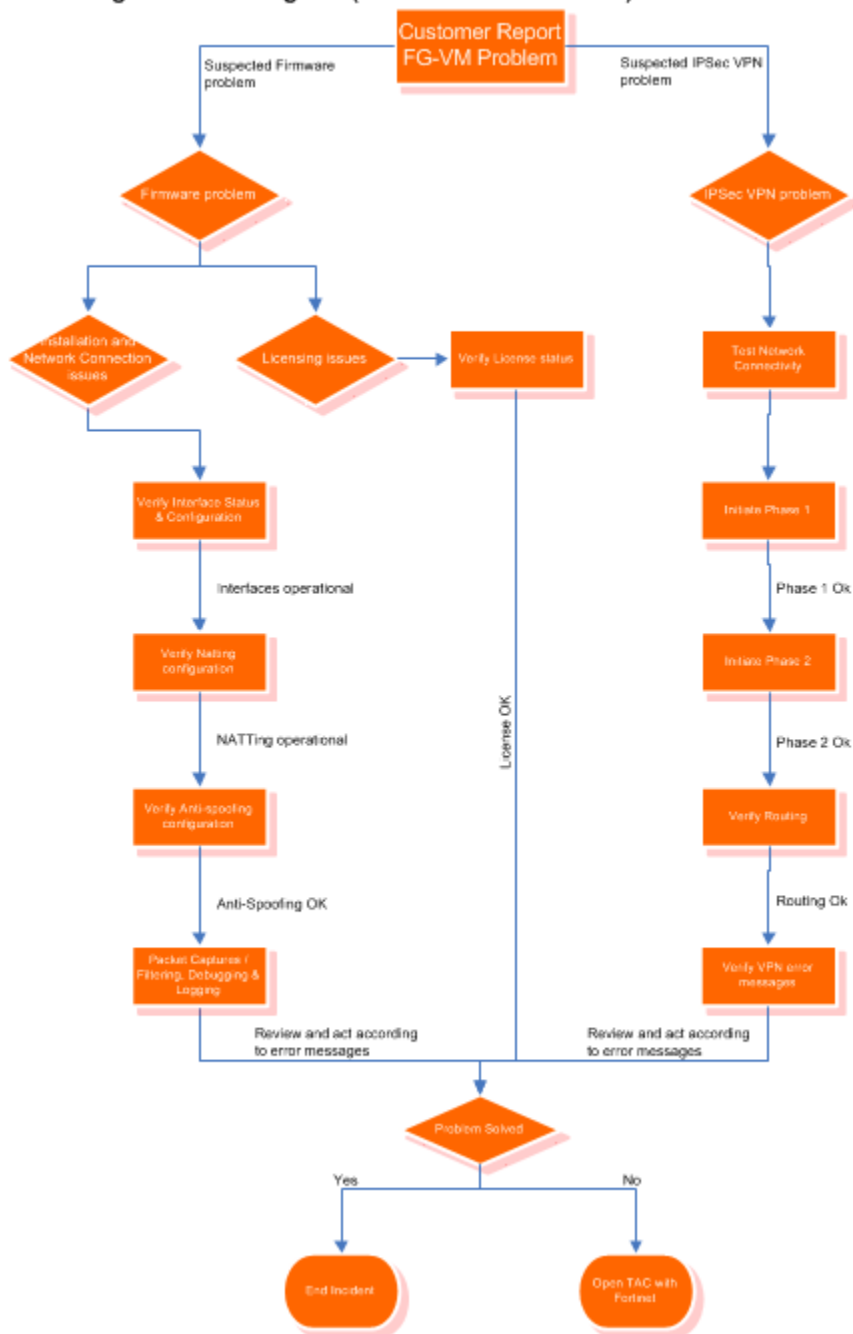
5.3   Licensing

	FORTIGATE-VM00	FORTIGATE-VM01/01V	FORTIGATE-VM02/02V	FORTIGATE-VM04/04V
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 1	1 / 1	1 / 2	1 / 4
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10
Memory Support (Minimum / Maximum)	1 GB / 2 GB	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	32 / 32	32 / 64	256 / 512	256 / 512
Virtual Domains (Default / Maximum)	1 / 1	1 / 10	10 / 25	10 / 50
Firewall Policies (VDOM / System)	5,000	20,000 / 40,000	50,000 / 100,000	50,000 / 100,000
Maximum Number of FortiTokens	1,000	1,000	1,000	5,000
Maximum Number of Registered Endpoints	N/A	2,000	2,000	8,000
Unlimited User License	Yes	Yes	Yes	Yes
System Performance				
Firewall Throughput (UDP Packets, SR-IOV Enabled)		9.0 Gbps	11.5 Gbps	15.0 Gbps
Concurrent Sessions (TCP)		1.0 Million	2.6 Million	4.3 Million
New Sessions / Second (TCP)		85,000	100,000	125,000
IPsec VPN Throughput (AES256+SHA1, 512 Byte)		850 Mbps	1.15 Gbps	2.65 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		2,000	2,000	2,000
Client-to-Gateway IPsec VPN Tunnels		6,000	12,000	20,000
SSL-VPN Throughput		500 Mbps	750 Mbps	1.5 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)		1,000	2,000	4,500
IPS Throughput (HTTP / Enterprise Mix) [1]		3.0 Gbps / 950 Mbps	4.4 Gbps / 1.7 Gbps	7.5 Gbps / 3.0 Gbps
Application Control Throughput [2]		1.5 Gbps	2.6 Gbps	4.0 Gbps
NGFW Throughput [3]		550 Mbps	1.3 Gbps	2.2 Gbps
Threat Protection Throughput [4]		450 Mbps	1.0 Gbps	1.7 Gbps
CAPWAP Throughput [5]		1.0 Gbps	1.6 Gbps	2.4 Gbps

	FORTIGATE-VM08/08V	FORTIGATE-VM16/16V	FORTIGATE-VM32/32V	FORTIGATE-VMUL/ULV
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 8	1 / 16	1 / 16	1 / 16
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10
Memory Support (Minimum / Maximum)	1 GB / 12 GB	1 GB / 24 GB	1 GB / 48 GB	1 GB / Unlimited GB
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096
Virtual Domains (Default / Maximum)	10 / 250	10 / 500	10 / 500	10 / 500
Firewall Policies (VDOM / System)	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000
Maximum Number of FortiTokens	5,000	5,000	5,000	5,000
Maximum Number of Registered Endpoints	20,000	20,000	20,000	20,000
Unlimited User License	Yes	Yes	Yes	Yes
System Performance				
Firewall Throughput (UDP Packets, SR-IOV Enabled)	20.0 Gbps	25.0 Gbps		
Concurrent Sessions (TCP)	8.5 Million	18.0 Million	38.0 Million	
New Sessions / Second (TCP)	150,000	175,000	200,000	
IPsec VPN Throughput (AES256+SHA1, 512 Byte)	5.2 Gbps	6.25 Gbps	6.85 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40,000	40,000	40,000	
Client-to-Gateway IPsec VPN Tunnels	40,000	50,000	64,000	
SSL-VPN Throughput	3.5 Gbps	6.0 Gbps	7.3 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum)	10,000	25,000	40,000	
IPS Throughput (HTTP / Enterprise Mix) [1]	13.5 Gbps / 5.5 Gbps	16.5 Gbps / 9.5 Gbps	18.3 Gbps / 15.5 Gbps	
Application Control Throughput [2]	8.0 Gbps	11.0 Gbps	14.0 Gbps	
NGFW Throughput [3]	4.0 Gbps	5.5 Gbps	11.0 Gbps	
Threat Protection Throughput [4]	3.2 Gbps	4.5 Gbps	8.8 Gbps	

Product	SKU	Description
FortiGate-VM00	FG-VM00	FortiGate-VM 'virtual appliance'. 1x vCPU core, (up to) 2 GB RAM. No VDOM or Extreme DB support.
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core and (up to) 2 GB RAM. No VDOM support for FG-VM01V model.
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM 'virtual appliance'. 2x vCPU cores and (up to) 4 GB RAM. No VDOM support for FG-VM02V model.
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM 'virtual appliance'. 4x vCPU cores and (up to) 6 GB RAM. No VDOM support for FG-VM04V model.
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM 'virtual appliance'. 8x vCPU cores and (up to) 12 GB RAM. No VDOM support for FG-VM08V model.
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM 'virtual appliance'. 16x vCPU cores and (up to) 24 GB RAM. No VDOM support for FG-VM016V model.
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM 'virtual appliance'. 32x vCPU cores and (up to) 48 GB RAM. No VDOM support for FG-VM032V model.
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores and RAM. No VDOM support FG-VMULV model.
Optional Accessories		
Virtual Domain License 11-25	FG-VDOM-25	Single Blade VDOM License Key 11-25 Virtual Domain Upgrade.
Virtual Domain License 26-50	FG-VDOM-50	Single Blade VDOM License Key 26-50 Virtual Domain Upgrade.
Virtual Domain License 51-100	FG-VDOM-100	Single Blade VDOM License Key 51-100 Virtual Domain Upgrade.
Virtual Domain License 101-250	FG-VDOM-250	Single Blade VDOM License Key 101-250 Virtual Domain Upgrade.
Virtual Domain License 251-500	FG-VDOM-500	Single Blade VDOM License Key 251-500 Virtual Domain Upgrade.
Virtual Domain License 11-250	FG-VDOM	Single Blade VDOM License Key 11-250 Virtual Domain Upgrade.

5.4   Connectivity Issues

5.4.1 Interfaces

Most connectivity issues for the VM-Series are resolved the same as they are for a physical firewall. As with a physical firewall, be sure to check the interfaces, the interface type (tap, vwire, layer 2, layer 3.) Link speed and duplex are not relevant for a virtual interface and do not need to be checked. Also, be sure to check for interface errors using the show interfaces command.

5.4.2 No Traffic

One of the most common problems that is specific to the VM-Series is an interface not receiving any traffic from the network. For example, a virtual machine is attached to the same port group as a VM-Series firewall and the virtual machine is sending traffic but not getting any response.

In this specific scenario, the traffic log has no recent entries and the counters are empty:
So we can see this isn't an issue of dropped packets – they aren't even showing up on the interface. At this point, we suspect the underlying infrastructure. The interface is up but it is behaving similarly to a physical firewall port with no cable.

Business
Services   orange

6 Run ping and Traceroute

Ping and traceroute are useful tools in network troubleshooting. Both tools accept either IP addresses or fully-qualified domain names as parameters. This can help you determine why particular services, such as email or web browsing, are not working properly.

Note If ping does not work, you likely have it disabled on at least one of the interface settings, and firewall policies for that interface.

Both ping and traceroute require particular ports to be open on firewalls to function. Since you typically use these tools to troubleshoot, you can allow them in the firewall policies and on interfaces only when you need them, and otherwise keep the ports disabled for added security.

6.1 Check connections 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 the destination is unreachable.

Ping is part of Layer-3 on the Open Systems Interconnection (OSI) Networking Model. Ping sends Internet Control Message Protocol (ICMP) "echo request" packets to the destination, and listens for "echo response" packets in reply. However, many public networks block ICMP packets because ping can be used in a denial of service (DoS) attack, or by an attacker to find active locations on the network. By default, FortiGate units have ping enabled.

If ping does not work from your FortiGate unit, make sure it was not disabled. Go to System > Network > Interface. Examine the list of allowed protocols in the Access column for the port used by the Web-based Manager (usually port1). If ping is not in the list, enable it.

To enable ping:

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

2. Select the *Edit* icon in the applicable row. A dialog window appears.

3. Select *PING* on the *Edit Interface* dialog window.

4. Select OK.
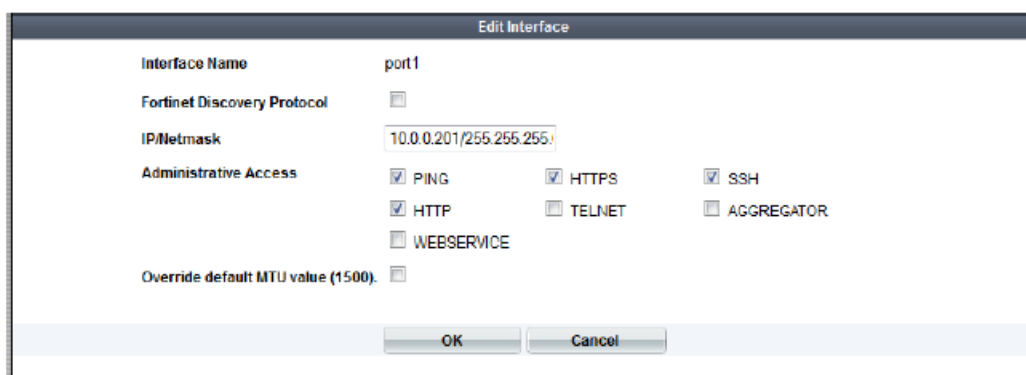
What ping can tell you

Beyond the basic connectivity information, ping tells you the amount of packet loss (if any), how long it takes the packet to make the round trip, and the variation in that time from packet to packet.

If ping shows any packet loss, you should investigate:

- possible ECMP, split horizon, or network loops;
- cabling to ensure no loose connections.

If ping shows total packet loss, you should investigate:

- hardware to ensure cabling is correct;
- all equipment between the two locations to determine they are properly connected;
- addresses and routes to ensure all IP addresses and routing information along the route is configured as expected;
- firewalls to ensure they are set to allow ping to pass through.

How to use ping

You can ping from the FortiGate unit in the CLI Console widget of the Web-based Manager or through CLI. For example:

> *execute ping 172.20.120.169*

If the FortiGate Web-based Manager and CLI are not available, you can run ping on a Windows or Linux PC.

To ping a device from a Windows PC:

1. Open a command window.
   - In Windows XP, select Start > Run, enter cmd, and select OK.
   - In Windows 7, select the Start icon, enter cmd in the search box, and select cmd.exe from the list.

2. In the command window, enter the ping command and an IP address, for example:
   ping 172.20.120.169

Ping options include:

   - -t, to send packets until you press Control-C
   - -a, to resolve addresses to domain names where possible
   - -n x, where x is an integer stating the number of packets to send

To ping a device from a Linux PC:

1. Go to a command line prompt.
2. Enter:
   /bin/etc/ping 172.20.120.169

6.2   Check routes with traceroute

Traceroute sends ICMP packets to test each hop along the route. It sends three packets, and then increases the time to live (TTL) setting by one each time. This effectively allows the packets to go one hop farther along the route. This explains why most traceroute commands display their maximum hop count before they start tracing the route; that is the maximum number of steps it will take before declaring the destination unreachable. The TTL setting may result in steps along the route timing out due to slow responses. There are many possible reasons for this to occur.

Traceroute by default 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

Business
Services   orange

(Unix-like systems and Windows) you will need to allow both protocols inbound through your firewall (UDP with ports from 33434 to 33534 and ICMP type 8).

What traceroute can tell you

Where ping only tells you if the signal reached its destination and came back successfully, traceroute shows each step of its journey to its destination and how long each step takes. If ping finds an outage between two points, use traceroute to locate exactly where the problem is. The traceroute output can identify other problems, such as an inability to connect to a DNS server.

How to use traceroute

You can run a route trace from the FortiGate unit in the CLI Console widget of the Web-based Manager or through CLI, for example:

> *execute traceroute docs.fortinet.com*

If the FortiGate Web-based Manager and CLI are not available, you can trace a route on a Windows or Linux PC.

To use traceroute on a Windows PC:

1. Open a command window.
   - In Windows XP, select Start > Run, enter cmd, and select OK.
   - In Windows 7, select the Start icon, enter cmd in the search box, and select cmd.exe from the list.

2. Enter the tracert command to trace the route from the host PC to the destination web site, for example:

> *tracert fortinet.com*

In the tracert output, the first, or left column, is the hop count, which cannot go over 30 hops. The second, third, and fourth columns are how long each of the three packets takes to reach this stage of the route. These values are in milliseconds and normally vary quite a bit. Typically a value of <1ms indicates a local connection.

The fifth, or far right column, is the domain name of that device and its IP address or possibly just the IP address.

To use traceroute on a Linux PC:

1. Go to a command line prompt.
2. Enter:

> */bin/etc/traceroute fortinet.com*

The Linux traceroute output is very similar to the MS Windows tracert output.

Verify the contents of the routing table

When you have little connectivity, a good place to look for information is the routing table. The routing table is where the FortiGate unit stores currently used static routes. If a route is in the routing table, it saves the time and resources of a lookup. If a route was not used for a while and a new route needs to be added, the oldest, least-used route is bumped if the routing table is full. This ensures the most recently used routes stay in the table.

To check the routing table in the CLI, enter:

> *diagnose system route list*

Business Services | orange™

7 What can sniffing packets tell you

Packet sniffing can tell you if the traffic is reaching its destination, what the port of entry is on the FortiGate unit, if the ARP resolution is correct, and if the traffic is being sent back to the source as expected. Packet sniffing can also tell you if the FortiGate unit is silently dropping packets.

If you configure virtual IP addresses on your FortiGate unit, it will use those addresses in preference to the physical IP addresses. You will notice this when you are sniffing packets because all traffic will use the virtual IP addresses. This is due to the ARP update that is sent out when the virtual IP address is configured.

7.1 Perform a sniffer trace

When troubleshooting networks and routing in particular, it helps to look inside the headers of packets to determine if they are traveling along the route you expect. Packet sniffing is also called a network tap, packet capture, or logic analyzing.

To sniff packets

The CLI syntax of the internal FortiGate packet sniffer command is:

diagnose sniffer packet <interface_name> <filter_str> <verbose-level> <count_int>

This example checks network traffic on port1, with no filter, and captures 10 packets:

diagnose network sniffer packet port1 none 1 10

7.2 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.

7.3 Ensure you have administrator access to required equipment

Before troubleshooting your FortiGate unit, you will need administrator access to the equipment.

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.

8 Troubleshooting tools

FortiOS provides a number of tools that help with troubleshooting both hardware and software issues. These tools include diagnostics and ports; ports are used when you need to understand the traffic coming in or going out on a specific port, for example, UDP 53, which is used by the FortiGate unit for DNS lookup and RBL lookup.

This section also contains information about troubleshooting FortiGuard issues.

8.1 FortiOS diagnostics

A collection of diagnostic commands are available in FortiOS for troubleshooting and performance monitoring. Within the CLI commands, the two main groups of diagnostic commands are get and diagnose commands. Both commands display information about system resources, connections, and settings that enable you to locate and fix problems, or to monitor system performance.

This topic includes diagnostics commands to help with:

- Check date and time
- Resource usage
- Proxy operation
- Hardware NIC
- Traffic trace
- Session table
- Firewall session setup rate
- Finding object dependencies
- Flow trace
- Packet sniffing and packet capture
- FA2 and NP2 based interfaces
- Debug command
- The execute tac report command
- Other commands

Additional diagnostic commands related to specific features are covered in the chapter for that specific feature. For example in-depth diagnostics for dynamic routing are covered in the dynamic routing chapter.

8.1.1   Check date and time

The system date and time are important for FortiGuard services, when logging events, and when sending alerts. The wrong time will make the log entries confusing and difficult to use.

Use Network Time Protocol (NTP) to set the date and time if possible. This is an automatic method that does not require manual intervention. However, you must ensure the port is allowed through the firewalls on your network. FortiToken synchronization requires NTP in many situations.

How to check the date and time - web-based manager

1. Go to **System Information > System Time** on the dashboard.

Alternately, you can check the date and time using the CLI commands execute date and execute time.

2. If required, select Change to adjust the date and time settings.

You can set the time zone, date and time, and select NTP usage. In the CLI, use the following commands to change the date and time:

config system global
* set timezone (use ? to get a list of IDs and descriptions of their timezone)*
* set*
config system ntp
config ntpserver
* edit 1*
*   set server "ntp1.fortinet.net"*
*   next*
* edit 2*
*   set server "ntp2.fortinet.net"*
* next*
* end*
*   set ntpsync enable*
*   set syncinterval 60*
* end*

8.1.2   Resource usage

Each program running on a computer has one or more processes associated with it. For example if you open a Telnet program, it will have an associated telnet process. The same is true in FortiOS. All the processes have to share the system resources in FortiOS including memory and CPU.

Use get system performance status command to show the FortiOS performance status.

Sample output:

FGT#get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
CPU0 states: 0% user 0% system 0% nice 100% idle
CPU1 states: 0% user 0% system 0% nice 100% idle
CPU2 states: 0% user 0% system 0% nice 100% idle
CPU3 states: 0% user 0% system 0% nice 100% idle
Memory states: 25% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30 minutes
Average sessions: 5 sessions in 1 minute, 5 sessions in 10 minutes, 4 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days, 12 hours, 7 minutes

Monitor the CPU/memory usage of internal processes using the following command:

get system performance top <delay> <max_lines>

The data listed by the command includes the name of the daemon, the process ID, whether the process is sleeping or running, the CPU percentage being used, and the memory percentage being used.

Sample output:

> *FGT#get system performance top 10 100*
> *Run Time: 0 days, 11 hours and 30 minutes*
> *0U, 0S, 100I; 1977T, 1470F, 121KF*
> *pyfcgid 120 S 0.0 1.3*
> *pyfcgid 121 S 0.0 1.3*
> *pyfcgid 122 S 0.0 1.3*
> *pyfcgid 53 S 0.0 1.3*
> *ipsengine 75 S < 0.0 1.3*
> *ipsengine 66 S < 0.0 1.3*
> *ipsengine 73 S < 0.0 1.3*
> *ipsengine 74 S < 0.0 1.3*
> *ipsengine 79 S < 0.0 1.3*
> *ipsengine 80 S < 0.0 1.3*
> *cmdbsvr 43 S 0.0 1.0*
> *proxyworker 110 S 0.0 1.0*
> *proxyworker 111 S 0.0 1.0*
> *httpsd 125 S 0.0 0.8*
> *httpsd 52 S 0.0 0.8*
> *httpsd 124 S 0.0 0.8*
> *newcli 141 R 0.0 0.7*
> *newcli 128 S 0.0 0.7*
> *fgfmd 102 S 0.0 0.7*
> *iked 86 S 0.0 0.7*

8.1.3   Proxy operation

Monitor proxy operations using the following command:

> *diag test application <application> <option>*

The <application> value can include the following:

acd	Aggregate Controller.
ddnscd	DDNS client daemon.
dhcp6c	DHCP6 client daemon.
dhcprelay	DHCP relay daemon.
dlpfingerprint	DLP fingerprint daemon.
dlpfpcache	DLP fingerprint cache daemon.
dnsproxy	DNS proxy.
dsd	DLP Statistics daemon.
forticldd	FortiCloud daemon.
forticron	FortiCron daemon.
fsd	FortiExplorer daemon.
ftpd	FTP proxy.
harelay	HA relay daemon.
http	HTTP proxy.
imap	IMAP proxy.

Business
Services
orange

info-sslvpnd	SSL-VPN info daemon.
ipldbd	IP load balancing daemon.
ipsengine	ips sensor
ipsmonitor	ips monitor
ipsufd	IPS urlfilter daemon.
l2tpcd	L2TP client daemon.
lted	USB LTE daemon.
miglogd	Miglog logging daemon.
nat64d	NAT 64 daemon.
nntp	NNTP proxy.
pop3	POP3 proxy.
pptpcd	PPTP client.
proxyacceptor	Proxy acceptor.
proxyworker	Proxy worker.
quarantined	Quarantine daemon.
radiusd	RADIUS daemon.
reportd	Report daemon.
reputation	Client reputation daemon.
scanunit	Scanning unit.
sflowd	sFlow daemon.
smtp	SMTP proxy.
snmpd	SNMP daemon.
sqldb	SQL database daemon.
ssh	SSH proxy.
sslacceptor	SSL proxy.
sslworker	SSL proxy.
swctrl_authd	Switch controller authentication daemon.
uploadd	Upload daemon.
urlfilter	URL filter daemon.
wa_cs	WAN optimization cs server.
wa_dbd	WAN optimization storage server.
wad	WAN optimization proxy.
wad_diskd	WAN optimization disk access daemon.
wccpd	WCCP daemon.
wpad	WPA daemon.

Business
Services   orange

The <option> value depends from the application value used in the command. Here are some examples:

▪ If the application is http, the CLI command will be

diag test application http <option>

The <option> value can be one from the following:

2	Drop all connections
22	Drop max idle connections
222	Drop all idle connections
4	Display connection stat
44	Display info per connection
444	Display connections per state
4444	Display per-VDOM statistics
44444	Display information about idle connections
55	Display tcp info per connection
6	Display ICAP information
70	Disable ICAP 'Allow: 204' (default)
71	Enable ICAP 'Allow: 204'
72	Drop all ICAP server connections
11	Display the SSL session ID cache statistics
12	Clear the SSL session ID cache statistics
13	Display the SSL session ID cache
14	Clear the SSL session ID cache
80	Show Fortinet bar SSL-VPN bookmark info
81	Show Fortinet bar SSL-VPN bookmark cache
82	Show Fortinet bar SSL-VPN bookmark LRU list

▪ If the application is ipsmonitor, the CLI command will be

diag test application ipsmonitor <option>

The <option> value can be one from the following:

1	Display IPS engine information
2	Toggle IPS engine enable/disable status
3	Display restart log
4	Clear restart log
5	Toggle bypass status
6	Submit attack characteristics now

Business
Services   orange

10	IPS queue length
11	Clear IPS queue length
12	IPS L7 socket statistics
13	IPS session list
14	IPS NTurbo statistics
15	IPSA statistics
97	Start all IPS engines
98	Stop all IPS engines
99	Restart all IPS engines and monitor

8.1.4   Hardware NIC

Monitor hardware network operations using the following command:

diag hardware deviceinfo nic <interface>

The information displayed by this command is important as errors at the interface are indicative of data link or physical layer issues which may impact the performance of the FortiGate unit.

The following is sample output when <interface> = internal:

System_Device_Name port5
Current_HWaddr 00:09:0f:68:35:60
Permanent_HWaddr 00:09:0f:68:35:60
Link up
Speed 100
Duplex full
[……]
Rx_Packets=5685708
Tx_Packets=4107073
Rx_Bytes=617908014
Tx_Bytes=1269751248
Rx_Errors=0
Tx_Errors=0
Rx_Dropped=0
Tx_Dropped=0
[…..]

The *diag hardware deviceinfo nic* command displays a list of hardware related error names and values. The following table explains the items in the list and their meanings.

Field	Definition
Rx_Errors = rx error count	Bad frame was marked as error by PHY.
Rx_CRC_Errors + Rx_Length_Errors - Rx_Align_Errors	This error is only valid in 10/100M mode.
Rx_Dropped or Rx_No_Buffer_Count	Running out of buffer space.
Rx_Missed_Errors	Equals Rx_FIFO_Errors + CEXTERR (Carrier Extension Error

	Count). Only valid in 1000M mode, whichis marked by PHY.
Tx_Errors = Tx_Aborted_Errors	ECOL (Excessive Collisions Count). Only valid in half-duplex mode.
Tx_Window_Errors	LATECOL (Late Collisions Count). Late collisions are collisions that occur after 64-byte time into the transmission of the packet while working in 10 to100Mb/s data rate and 512-byte timeinto the transmission of the packet while working in the 1000Mb/s data rate. This register only increments if transmits are enabled and the device is in half-duplex mode.
Rx_Dropped	See Rx_Errors.
Tx_Dropped	Not defined.
Collisions	Total number of collisions experienced by the transmitter. Valid in half-duplex mode.
Rx_Length_Errors	Transmission length error.
Rx_Over_Errors	Not defined.
Rx_CRC_Errors	Frame CRC error.
Rx_Frame_Errors	Same as Rx_Align_Errors. This error is only valid in 10/100M mode.
Rx_FIFO_Errors	Same as Rx_Missed_Errors - a missed packet count.
Tx_Aborted_Errors	See Tx_Errors.
Tx_Carrier_Errors	The PHY should assert the internal carrier sense signal during every transmission. Failure to do so may indicate that the link has failed or the PHY has an incorrect link configuration. This register only increments if transmits are enabled. This register is not valid in internal SerDes 1 mode (TBI mode for the 82544GC/EI) and is only valid when the Ethernet controller is operating at full duplex.
Tx_FIFO_Errors	Not defined.
Tx_Heartbeat_Errors	Not defined.
Tx_Window_Errors	See LATECOL.
Tx_Single_Collision_Frames	Counts the number of times that a successfully transmitted packet encountered a single collision. The value only increments if transmits are enabled and the Ethernet controller is in half-duplex mode.
Tx_Multiple_Collision_Frames	A Multiple Collision Count which counts the number of times that a transmit encountered more than one collision but less than 16. The value only increments if transmits are enabled and the Ethernet controller is in half-duplex mode.
Tx_Deferred	Counts defer events. A defer event occurs when the transmitter cannot immediately send a packet due to the medium being busy because another device is transmitting, the IPG timer has not expired, half-duplex deferral events are occurring, XOFF frames are being received, or the link is not up. This register only increments if transmits are enabled. This counter does not increment for streaming transmits that are deferred due to TX IPG.
Rx_Frame_Too_Longs	The Rx frame is over size.

Rx_Frame_Too_Shorts	The Rx frame is too short.
Rx_Align_Errors	This error is only valid in 10/100M mode.
Symbol Error Count	Counts the number of symbol errors between reads - SYMERRS. The count increases for every bad symbol received, whether or not a packet is currently being received and whether or not the link is up. This register only increments in internal SerDes mode.

8.1.5   Traffic trace

Traffic tracing allows a specific packet stream to be followed. This is useful to confirm packets are taking the route you expected on your network.

View the characteristics of a traffic session though specific security policies using:
> *diag sys session*

Trace per-packet operations for flow tracing using:
> *diag debug flow*

Trace per-Ethernet frame using:
> *diag sniffer packet*

8.1.6   Session table

A session is a communication channel between two devices or applications across the network. Sessions enable FortiOS to inspect and act on a sequential group of packets in a session all together instead of inspecting each packet individually. Each of these sessions has an entry in the session table that includes important information about the session.

Use as a tool

Session tables are useful troubleshooting tools because they allow you to verify connections that you expect to see open. For example, if you have a web browser open to browse the Fortinet website, you would expect a session entry from your computer, on port 80, to the IP for the Fortinet website. Another troubleshooting method is if there are too many sessions for FortiOS to process, you can examine the session table for evidence why this is happening.

The FortiGate session table can be viewed from either the CLI or the web-based manager. The most useful troubleshooting data comes from the CLI. The session table in web-based manager also provides some useful summary information, particularly the current policy number that the session is using.

Web-based manager session information

In the web-based manager there are actually two places to view session information — the policy session monitor, and the dashboard Top Sources, Top Destinations and Top Applications

Top Sessions Dashboard

Top Sources Dashboard shows Top Sessions by source Address, Top Destinations shows Top sessions by Destination address, and Top Applications shows Top Sessions by applications. If there are not enough entries in the session table, try browsing to a different web site and re-examine the

Business
Services   orange™

table. The Policy ID shows which security policy matches the session. The sessions that do not have a Policy ID entry originate from the FortiGate device

Session monitor

The session monitor is the session table. It lists the protocol used, source and destination addresses, source and destination ports, what policy ID was matched (if any), how long until the session expires, and how long it has been established.

If there is no policy ID listed in the session entry, the traffic originated from the FortiGate unit. Otherwise all sessions must match a security policy to pass through the FortiGate unit. You can specify a filter to show Forward Traffic only. To do this, click on the Edit icon (it looks like a pencil)

As there are potentially many sessions active at one time, there are different methods you can use to filter unimportant sessions out of your search. The easiest filter is to display only IPv4 or IPv6 sessions. By default both are displayed.

#	Src	Src Port	Dst	Dst Port	Policy ID	Expiry (sec)	Duration (sec)	
1	192.168.1.200:53659	53659	157.55.56.147	40004	1	26	153	✕
2	192.168.1.200:53659	53659	157.55.56.151	40020	1	124	55	✕
3	192.168.1.200:53659	53659	157.56.52.38	40045	1	88	91	✕
4	192.168.1.200:53659	53659	75.158.90.51	56715	1	83	150	✕
5	192.168.1.200:61730	61730	70.78.76.207	49149	1	3,594	28	✕
6	192.168.1.200:53659	53659	157.55.130.150	40020	1	11	168	✕
7	192.168.1.200:61638	61638	111.253.246.196	45660	1	3,594	398	✕
8	192.168.1.200:53659	53659	157.55.235.148	40004	1	66	113	✕
9	192.168.1.200:53659	53659	157.55.235.160	40044	1	128	52	✕
10	192.168.1.200:53875	53875	216.2.48.143	8888	1	56	123	✕
11	192.168.1.200:53659	53659	65.55.223.27	40012	1	105	74	✕
12	192.168.1.200:53659	53659	213.199.179.141	40021	1	127	52	✕
13	192.168.1.200:53659	53659	213.199.179.145	40037	1	10	169	✕
14	192.168.1.200:53659	53659	64.4.23.156	40032	1	54	125	✕
15	192.168.1.200:53659	53659	157.55.235.161	40013	1	88	91	✕
16	192.168.1.200:53659	53659	65.55.223.13	40021	1	124	55	✕
17	192.168.1.200:53659	53659	65.55.223.38	40029	1	103	76	✕
18	192.168.1.200:53876	53876	208.91.112.195	8888	1	56	123	✕
19	192.168.1.200:53876	53876	208.91.112.197	8888	1	56	123	✕

How to find which security policy a specific connection is using

Every program and device on your network must have a communication channel, or session, open to pass information. The FortiGate unit manages these sessions with its many features from traffic shaping, to antivirus scanning, and even blocking known bad web sites. Each session has an entry in the session table. In the web, you can use the Session Monitor or Top Session Dashboard to view session information.

You may want to find information for a specific session, say a secure web browser session, for troubleshooting. For example if that web browser session is not working properly, you can check the session table to ensure the session is still active, and that it is going to the proper address. It can also tell you the security policy number it matches, so you can check what is happening in that policy.

Business
Services   orange

1. **Know your connection information.**

You need to be able to identify the session you want. For this you need the source IP address (usually your computer), the destination IP address if you have it, and the port number which is determined by the program being used. Some commons ports are:

- port 80 (HTTP for web browsing),
- port 22 (SSH used for secure login and file transfers)
- port 23 (telnet for a text connection)
- port 443 (HTTPS for secure web browsing

2. **Find your session and policy ID.**

Follow **System > Dashboard> Top Sources** to the session table monitor. Find your session by finding your source IP address, destination IP address if you have it, and port number. The policy ID is listed after the destination information. If the list of sessions is very long, you can filter the list to make it easier to find your session.

3. **When there are many sessions, use a filter to help you find your session.**

If there are multiple pages of sessions it is difficult to find a single session. To help you in your search you can use a filter to block out sessions that you don't want. Select the filter icon next to Src Address. In the window that pops up, enter your source IP address and select Apply. Now only sessions that originate from your IP address will be displayed in the session table. If the list is still too long, you can do the same for the Src port. That will make it easy to find your session and the security policy ID. When you are finished remember to clear the filters.

CLI session information

The session table output from the CLI (diag sys session list) is very verbose. Even on a system with a small amount of traffic, displaying the session table will generate a large amount of output. For this reason, filters are used to display only the session data of interest.

You can filter a column in the web-based manager by clicking the funnel icon on the column heading or from the CLI by creating a filter.

An entry is placed in the session table for each traffic session passing through a security policy. The following command will list the information for a session in the table:

```
diag sys session list
Sample Output:
FGT# diag sys session list
session info: proto=6 proto_state=05 expire=89 timeout=3600 flags=00000000 av_idx=0
use=3
bandwidth=204800/sec      guaranteed_bandwidth=102400/sec      traffic=332/sec      prio=0
logtype=session ha_id=0 hakey=4450
tunnel=/
state=log shape may_dirty
statistic(bytes/packets/err): org=3408/38/0 reply=3888/31/0 tuples=2
orgin->sink: org pre->post, reply pre->post oif=3/5 gwy=192.168.11.254/10.0.5.100
hook=post dir=org act=snat 10.0.5.100:1251->192.168.11.254:22(192.168.11.105:1251)
hook=pre dir=reply act=dnat 192.168.11.254:22->192.168.11.105:1251(10.0.5.100:1251)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 domain_info=0 auth_info=0 ftgd_info=0 ids=0x0 vd=0 serial=00007c33 tos=ff/ff
```

**Business
Services** orange

Since output can be verbose, the filter option allows specific information to be displayed, for example:

diag sys session filter <option>

The <option> values available include the following:

clear	Clear session filter.
dintf	Destination interface.
dport	Destination port.
dst	Destination IP address.
duration	duration
expire	expire
negate	Inverse filter.
nport	NAT'd source port
nsrc	NAT'd source ip address
policy	Policy ID.
proto	Protocol number.
proto-state	Protocol state.
sintf	Source interface.
sport	Source port.
src	Source IP address.
vd	Index of virtual domain. -1 matches all.

Even though UDP is a sessionless protocol, the FortiGate unit still keeps track of the following two different states:

- UDP reply not seen with a value of 0
- UDP reply seen with a value of 1

The following illustrates FW session states from the session table:

State	Meaning
log	Session is being logged.
local	Session is originated from or destined for local stack.
ext	Session is created by a firewall session helper.
may_dirty	Session is created by a policy. For example, the session for ftp control channel will have this state but ftp data channel will not. This is also seen when NAT is enabled.
ndr	Session will be checked by IPS signature.
nds	Session will be checked by IPS anomaly.
br	Session is being bridged (TP) mode.

8.1.7   Firewall session setup rate

The number of sessions that can be established in a set period of time is useful information. A session is an end-to-end TCP/IP connection for communication with a limited lifespan. If you record the setup rate during normal operation, when you experience problems you have that setup rate with the current number to see if its very different. While this will not solve your problems, it can be a useful step to help you define your problem.

A reduced firewall session setup rate could be the result of a number of things from a lack of system resources on the FortiGate unit, to reaching the limit of your session count for your VDOM.

To view your session setup rate - web-based manager

1.   Got to System > Dashboard.

2.   Maximize Top Sources

3.   Read the New Sessions per Second value displayed at the bottom.

If the Top Sessions widget is not visible on your dashboard, go to the + Widget button at the top of the window. When a window pops up, select Top Sessions for it to be added to the dashboard.

To view your session setup rate method 1- CLI

> *FGT# get sys performance status*
> *CPU states: 0% user 0% system 0% nice 100% idle*
> *Memory states: 10% used*
> *Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes,*
> *13 kbps in 30 minutes*
> *Average sessions: 31 sessions in 1 minute, 30 sessions in 10*
> *minutes, 31 sessions in 30 minutes*
> *Average session setup rate: 0.5 sessions per second in last 1*
> *minute, 0 sessions per second in last 10 minutes, 0 sessions per*
> *second in last 30 minutes*
> *Virus caught: 0 total in 1 minute*
> *IPS attacks blocked: 0 total in 1 minute*
> *Uptime: 44 days, 18 hours, 42 minutes*

The information you are looking for is the Average sessions section, highlighted in the above output. In this example you can see there were 31 sessions in 1 minute, or an average of 0.5 sessions per second. The values for 10 minutes and 30 minutes allow you to take a longer average for a more reliable value if your FortiGate unit is working at maximum capacity. The smallest FortiGate unit can have 1 000 sessions established per second across the unit.

Remember that session setup rate is a global command. If you have multiple VDOMs configured with many sessions in each one, the session setup rate per VDOM will be slower than if there were no VDOMs configured.

8.1.8   Finding object dependencies

An administrator may not be permitted to delete a configuration object if there are other configuration objects that depend on it. This command identifies other objects which depend on or make reference to the configuration object in question. If an error is displayed that an object is in use and cannot be deleted, this command can help identify the source of the problem.

Another use is if you have a virtual interface with objects that depend on it, you need to find and remove those dependencies before you delete that interface.

CLI method

When running multiple VDOMs, this command is run in the Global configuration only and it searches for the named object both in the Global and VDOM configuration most recently used:

diag sys checkused <path.object.mkey>

For example, to verify which objects are referred to in a security policy with an ID of 1, enter the command as follows:

diag sys checkused firewall.policy.policyid 1

To check what is referred to by interface port1, enter the following command:

diag sys checkused system.interface.name port1

To show all the dependencies for an interface, enter the command as follows:

diag sys checkused system.interface.name <interface name>

Sample Output:

entry used by table firewall.address:name '10.98.23.23_host'
entry used by table firewall.address:name 'NAS'
entry used by table firewall.address:name 'all'
entry used by table firewall.address:name 'fortinet.com'
entry used by table firewall.vip:name 'TORRENT_10.0.0.70:6883'
entry used by table firewall.policy:policyid '21'
entry used by table firewall.policy:policyid '14'
entry used by table firewall.policy:policyid '19'

In this example, the interface has dependent objects, including four address objects, one VIP, and three security policies.

Web-based manager method

In the web-based manager, the object dependencies for an interface can be easily checked and removed.

To remove interface object dependencies - web-based manager

1. Go to System > Interfaces.
   The number in the Ref. column is the number of objects that refer to this interface.

2. Select the number in the Ref. column for the desired interface.
   A Window listing the dependencies will appear.

3. Use these detailed entries to locate and remove object references to this interface.
   The trash can icon will change from gray when all object dependencies have been removed.

4. Remove the interface by selecting the check box for the interface, and select Delete.

Business
Services   orange

8.1.9   Flow trace

To trace the flow of packets through the FortiGate unit, use the following command:

diag debug flow trace start

Follow packet flow by setting a flow filter using this command:

diag debug flow filter <option>

Filtering options include the following:

addr IP address
clear clear filter
daddr destination IP address
dport destination port
negate inverse filter
port port
proto protocol number
saddr source IP address
sport source port
vd index of virtual domain, -1 matches all

Enable the output to be displayed to the CLI console using the following command:

diag debug flow show console

Note	diag debug flow output is recorded as event log messages and are sent to a FortiGate unit if connected. Do not let this command run longer than necessary since it generates significant amounts of data.

Start flow monitoring with a specific number of packets using this command:

diag debug flow trace start <N>

Stop flow tracing at any time using:

diag debug flow trace stop

The following is an example of the flow trace for the device at the following IP address: 203.160.224.97

diag debug enable
diag debug flow filter addr 203.160.224.97
diag debug flow show console enable
diag debug flow show function-name enable
diag debug flow trace start 100

Flow trace output example - HTTP

Connect to the web site at the following address to observe the debug flow trace. The display may vary slightly:

http://www.fortinet.com

Comment: SYN packet received:

id=20085 trace_id=209 func=resolve_ip_tuple_fast
line=2700 msg="vd-root received a packet(proto=6,
192.168.3.221:1487->203.160.224.97:80) from port5."

Business
Services   orange™

SYN sent and a new session is allocated:

> *id=20085 trace_id=209 func=resolve_ip_tuple line=2799*
> *msg="allocate a new session-00000e90"*

Lookup for next-hop gateway address:

> *id=20085 trace_id=209 func=vf_ip4_route_input line=1543*
> *msg="find a route: gw-192.168.11.254 via port6"*

Source NAT, lookup next available port:

> *id=20085 trace_id=209 func=get_new_addr line=1219*
> *msg="find SNAT: IP-192.168.11.59, port-31925"*
> *direction"*

Matched security policy. Check to see which policy this session matches:

> *id=20085 trace_id=209 func=fw_forward_handler line=317*
> *msg="Allowed by Policy-3: SNAT"*

Apply source NAT:

> *id=20085 trace_id=209 func=__ip_session_run_tuple*
> *line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"*
> *SYN ACK received:*
> *id=20085 trace_id=210 func=resolve_ip_tuple_fast line=2700*
> *msg="vd-root received a packet(proto=6, 203.160.224.97:80-*
> *>192.168.11.59:31925) from port6."*

Found existing session ID. Identified as the reply direction:

> *id=20085 trace_id=210 func=resolve_ip_tuple_fast line=2727*
> *msg="Find an existing session, id-00000e90, reply*
> *direction"*

Apply destination NAT to inverse source NAT action:

> *id=20085 trace_id=210 func=__ip_session_run_tuple*
> *line=1516 msg="DNAT 192.168.11.59:31925-*
> *>192.168.3.221:1487"*

Lookup for next-hop gateway address for reply traffic:

> *id=20085 trace_id=210 func=vf_ip4_route_input line=1543*
> *msg="find a route: gw-192.168.3.221 via port5"*

ACK received:

> *id=20085 trace_id=211 func=resolve_ip_tuple_fast line=2700*
> *msg="vd-root received a packet(proto=6,*
> *192.168.3.221:1487->203.160.224.97:80) from port5."*

Match existing session in the original direction:

> *id=20085 trace_id=211 func=resolve_ip_tuple_fast line=2727*
> *msg="Find an existing session, id-00000e90, original*
> *direction"*

Apply source NAT:

> *id=20085 trace_id=211 func=__ip_session_run_tuple*
> *line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"*

Receive data from client:

> *id=20085 trace_id=212 func=resolve_ip_tuple_fast*
> *line=2700 msg="vd-root received a packet(proto=6,*
> *192.168.3.221:1487->203.160.224.97:80) from port5."*

Business
Services   orange

Match existing session in the original direction:

> *id=20085 trace_id=212 func=resolve_ip_tuple_fast*
> *line=2727 msg="Find an existing session, id-00000e90,*
> *original direction"*

Apply source NAT:

> *id=20085 trace_id=212 func=__ip_session_run_tuple*
> *line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"*

Receive data from server:

> *id=20085 trace_id=213 func=resolve_ip_tuple_fast*
> *line=2700 msg="vd-root received a packet(proto=6,*
> *203.160.224.97:80->192.168.11.59:31925) from port6."*

Match existing session in reply direction:

> *id=20085 trace_id=213 func=resolve_ip_tuple_fast*
> *line=2727 msg="Find an existing session, id-00000e90,*
> *reply direction"*

Apply destination NAT to inverse source NAT action:

> *id=20085 trace_id=213 func=__ip_session_run_tuple*
> *line=1516 msg="DNAT 192.168.11.59:31925-*
> *>192.168.3.221:1487"*

Flow trace output example - IPsec (policy-based)

> *id=20085 trace_id=1 msg="vd-root received a packet(proto=1, 10.72.55.240:1->10.71.55.10:8)*
> *from internal."*
> *id=20085 trace_id=1 msg="allocate a new session-00001cd3"*
> *id=20085 trace_id=1 msg="find a route: gw-66.236.56.230 via wan1"*
> *id=20085 trace_id=1 msg="Allowed by Policy-2: encrypt"*
> *id=20085 trace_id=1 msg="enter IPsec tunnel-RemotePhase1"*
> *id=20085 trace_id=1 msg="encrypted, and send to 15.215.225.22 with source 66.236.56.226"*
> *id=20085 trace_id=1 msg="send to 66.236.56.230 via intf-wan1"*
> *id=20085 trace_id=2 msg="vd-root received a packet (proto=1, 10.72.55.240:1-1071.55.10:8)*
> *from internal."*
> *id=20085 trace_id=2 msg="Find an existing session, id-00001cd3, original direction"*
> *id=20085 trace_id=2 msg="enter IPsec ="encrypted, and send to 15.215.225.22 with source*
> *66.236.56.226" tunnel-RemotePhase1"*
> *id=20085 trace_id=2 msgid=20085 trace_id=2 msg="send to 66.236.56.230 via intf-wan1"*

8.1.10   Packet sniffing and packet capture

FortiOS devices can sniff packets using commands in the CLI or capture packets using the web-based manager. The differences between the two methods are not large.

Packet sniffing in the CLI is well suited for spot checking traffic from the CLI, but if you have complex filters to enter it can be a lot of work to enter them each time. You can also save the sniffing output; however, you must log to a file and then analyze the file later by hand.

Packet capture in the web-based manager makes it easy to set up multiple filters at once and just run one or two as you need them. You also have controls to start and stop capturing as you wish. Packet capture output is downloaded to your local computer as a *.pcap file which requires a third party application to read the file, such as Wireshark. This method is useful to send Fortinet support information to help resolve an issue.

Business
Services   orange

Features	Packet sniffing	Packet capture
Command location	CLI	web-based manager
Third party software required	puTTY to log plaintext output	Wireshark to read *.pcap files
Read output in plain text file	yes	no
Read output as *.pcap file using Wireshark	no	yes
Easily configure single quick and simple filter	yes	no
Record packet interface	yes	no
Configure complex sniffer filters on multiple interface	no	yes
sniff IPv6	hard	easy
sniff non-IP packets	no	yes
Filter packets by protocol and/or port	easy	easy
Filter packets by source and/or destination address	easy	easy

Packet sniffing

Before you start sniffing packets on the CLI, you should be prepared to capture the output to a file — there can be huge amounts of data that you will not be able to see without saving it to a file. One method is to use a terminal program like puTTY to connect to the FortiGate unit's CLI. Then once the packet sniffing count is reached you can end the session and analyze the output in the file.

Details within packets passing through particular interfaces can be displayed using the packet sniffer with the following command:

diag sniffer packet <interface> <filter> <verbose> <count> <tsformat>

The <interface> value is required, with the rest being optional. If not included the default values will be "none".

For example the simplest valid sniffer command would be:

diag sniffer packet any

The <interface> value can be any physical or virtual interface name. Use any to sniff packets on all interfaces.

The <filter> value limits the display of packets using filters, including Berkeley Packet Filtering (BPF) syntax. The <filter> value must be enclosed in quotes.

'[[src|dst] host <host_name_or_IP1>] [[src|dst] host <host_name_or_IP2>]
[[arp|ip|ip6|gre|esp|udp|tcp] [port_no]] [[arp|ip|ip6|gre|esp|udp|tcp] [port_no]]'

If a second host is specified in the filter, only the traffic between the two hosts will be displayed. Optionally, you can use logical OR to match only one of the hosts, or match one of multiple protocols or ports. When defining a port, there are up to two parts — protocol and port number.

For example, to display UDP 1812 traffic or TCP 8080 traffic, use the following:

Business Services orange

'udp port 1812 or tcp port 8080'

To display all IP traffic that has a source of 192.168.1.2 and a destination of 192.168.2.3:
   'ip src host 192.168.1.2 and dst host 192.168.2.3'

The <verbose> option allows different levels of information to be displayed. The verbose levels include:

1 Print header of packets

2 Print header and data from the IP header of the packets

3 Print header and data from the Ethernet header of the packets

4 Print header of packets with interface name

5 Print header and data from IP of packets with interface name

6 Print header and data from Ethernet of packets with interface name

The <count> value indicates the number of packets to sniff before stopping. If this variable is not included, or is set to zero, the sniffer will run until you manually halt it with Ctrl-C.

The <tsformat> value define the format of timestamp. It can be:

a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms

l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms

otherwise: relative to the start of sniffing, ss.ms

Packet capture

FortiOS 5 includes packet capture to the web-based manager. To configure packet capture filters, go to **System > Network > Packet Capture**.

When you add a packet capture filter, enter the following information and select **OK**.

Interface	Select the interface to sniff from the dropdown menu. You must select one interface. You cannot change the interface without deleting the filter and creating a new one, unlike the other fields.
Max Packets to Capture	Enter the number of packets to capture before the filter stops. This number cannot be zero. You can halt the capturing before this number is reached.
Enable Filters	Select this option to specify your filter fields
Host(s)	Enter one or more hosts IP address Separate multiple hosts with commas. Enter a range using a dash without spaces, for example 172.16.1.5-172.16.1.15 or enter a subnet.
Port(s)	Enter one or more ports to capture on the selected interface. Separate multiple ports with commas. Enter a range using a dash without spaces, for example 88-90
VLAN(s)	Enter one or more vlans (if there is any). Separate multiple vlans with commas.
Protocol	Enter one or more protocol. Separate multiple protocol with commas. Enter a

Business
Services   orange

	range using a dash without spaces, for example 1-6, 17, 21-25
Include IPv6 packets	Select this option if you are troubleshooting IPv6 networking, or if your network uses IPv6. Otherwise, leave it disabled.
Capture Non-IP packets	The protocols available in the list are all IP based except for ICMP (ping). To capture non-IP based packets select this feature. Some examples of non-IP packets include IPsec, IGMP, ARP, and as mentioned ICMP.

If you select a filter and go back to edit it, you have the added option of starting and stopping packet capture in the edit window, or downloading the captured packets. You can also see the filter status and the number of packets captured.

You can also select the filter and select Start to start capturing packets. While the filter is running, you will see the number of captured packets increasing until it reaches the max packet count or you select Stop. While the filter is running you cannot download the output file.

When the packet capture is complete, you can select Download to send the packet capture filter captured packets to your local computer as a *.pcap file. To read this file format, you will need to use Wireshark or a similar third party application. Using this tool you will have extensive analytics available to you and the full contents of the packets that were captured.

8.1.11   FA2 and NP2 based interfaces

Many Fortinet products contain network processors. Some of these products contain FortiAccel (FA2) network processors while others contain NP2 network processors. Network processor features, and therefore offloading requirements, vary by network processor model.

When using the FA2- and NP2-based interfaces, only the initial session setup will be seen through the diag debug flow command. If the session is correctly programmed into the ASIC (fastpath), the debug flow command will no longer see the packets arriving at the CPU. If the NP2 functionality is disabled, the CPU will see all the packets, however, this should only be used for troubleshooting purposes.

First, obtain the NP2 and port numbers with the following command:

diag npu np2 list

Sample output:

ID PORTS
-- -----
0 port1
0 port2
0 port3
0 port4
ID PORTS
-- -----
1 port5
1 port6
1 port7
1 port8
ID PORTS
-- -----
2 port9
2 port10

Business
Services

orange™

2 port11
2 port12
ID PORTS
-- -----
3 port13
3 port14
3 port15
3 port16

Run the following commands:

> *diag npu np2 fastpaf th disable <dev_id>*

(where dev_id is the NP2 number)

Then, run this command:

> *diag npu np2 fastpath-sniffer enable port1*

Sample output:

> *NP2 Fast Path Sniffer on port1 enabled*

This will cause all traffic on port1 of NP2 to be sent to the CPU meaning a standard sniffer trace can be taken and other diag commands should work if it was a standard CPU driven port.

These commands are only for the newer NP2 interfaces. FA2 interfaces are more limited as the sniffer will only capture the initial packets before the session is offloaded into HW (FA2). The same holds true for the diag debug flow command as only the session setup will be shown, however, this is usually enough for this command to be useful.

8.1.12   Debug command

Debug output provides continuous, real-time event information. Debugging output continues until it is explicitly stopped or until the unit is rebooted. Debugging output can affect system performance and will be continually generated even though output might not be displayed in the CLI console.

Debug information displayed in the console will scroll in the console display and may prevent CLI commands from being entered, for example, the command to disable the debug display. To turn off debugging output as the display is scrolling by, press the ↑ key to recall the recent diag debug command, press backspace, and type "0", followed by Enter.

Debug output display is enabled using the following command:
> *diag debug enable*

When finished examining the debug output, disable it using:
> *diag debug disable*

Once enabled, indicate the debug information that is required using this command:
> *diag debug <option> <level>*

Business
Services   orange™

Debug command options include the following:

application	application
authd	Authentication daemon.
cli	Debug CLI.
cmdb-trace	Trace CLI.
config-error-log	Configure error log info.
console	console
crashlog	Crash log info.
disable	Disable debug output.
enable	Enable debug output.
flow	Trace packet flow in kernel.
fsso-polling	FSSO active directory poll module.
info	Show active debug level settings.
kernel	kernel
rating	Display rating info.
report	Report for tech support.
reset	Reset all debug level to default.
rtmon	rtmon daemon
sql-log-error	SQL log database error info
urlfilter	urlfilter

The debug level can be set at the end of the command. Typical values are 2 and 3, for example:

> *diag debug application DHCPS 2*
> *diag debug application spamfilter 2*

Fortinet support will advise which debugging level to use.

Timestamps can be enabled to the debug output using the following command:

> *diag debug console timestamp enable*

Debug output example

This example shows the IKE negotiation for a secure logging connection from a FortiGate unit to a FortiGate system.

> *diag debug reset*
> *diag vpn ike log-filter src-addr4 192.168.11.2*
> *diag debug enable*

Sample Output:

> *FGh_FtiLog1: IPsec SA connect 0 192.168.11.2->192.168.10.201:500, natt_mode=0 rekey=0*
> *phase2=FGh_FtiLog1*
> *FGh_FtiLog1: using existing connection, dpd_fail=0*

Business Services   orange

FGh_FtiLog1: found phase2 FGh_FtiLog1
FGh_FtiLog1: IPsec SA connect 0 192.168.11.2 -> 192.168.10.201:500 negotiating
FGh_FtiLog1: overriding selector 225.30.5.8 with 192.168.11.2
FGh_FtiLog1: initiator quick-mode set pfs=1536...
FGh_FtiLog1: try to negotiate with 1800 life seconds.
FGh_FtiLog1: initiate an SA with selectors: 192.168.11.2/0.0.0.0->192.168.10.201, ports=0/0,
protocol=0/0
Send IKE Packet(quick_outI1):192.168.11.2:500(if0) -> 192.168.10.201:500, len=348
Initiator: sent 192.168.10.201 quick mode message #1 (OK)
FGh_FtiLog1: set retransmit: st=168, timeout=6.

In this example:

192.168.11.2->192.168.10.201:500	Source and Destination gateway IP address
dpd_fail=0	Found existing Phase 1
pfs=1536...	Create new Phase 2 tunnel

8.1.13   The execute tac report command

exec tac report is an execute command that runs an exhaustive series of diagnostic commands. It runs commands that are only needed if you are using certain features like HA, VPN tunnels, or a modem. The report takes a few minutes to complete due to the amount of output generated. If you have your CLI output logged to a file, you can run this command to familiarize yourself with the CLI commands involved.

When you call Fortinet Customer Support, you will be asked to provide information about your unit and its current state using the output from this CLI command.

8.1.14   Other commands

ARP table

To view the ARP cache, use the following command:
  get sys arp

 To view the ARP cache in the system, use this command:
  diag ip arp list

Sample output:

index=14   ifname=internal   224.0.0.5   01:00:5e:00:00:05   state=00000040   use=72203
confirm=78203 update=72203 ref=1
index=13   ifname=dmz   192.168.3.100   state=00000020   use=1843   confirm=650179
update=644179 ref=2 ? VIP
index=13   ifname=dmz   192.168.3.109   02:09:0f:78:69:ff   state=00000004   use=71743
confirm=75743 update=75743 ref=1
index=14   ifname=internal   192.168.11.56   00:1c:23:10:f8:20   state=00000004   use=10532
confirm=10532 update=12658 ref=4

To remove the ARP cache, use this command:
execute clear system arp table

To remove a single ARP entry, use:
diag ip arp delete <interface name> <IP address>

To remove all entries associated with a particular interface, use this command:
diag ip arp flush <interface name>

To add static ARP entries, use the following command:
config system arp-table

Time and date settings

Check time and date settings for log message timestamp synchronization (the Fortinet support group may request this) and for certificates that have a time requirement to check for validity. Use the following commands:

execute time
current time is: 12:40:48
last ntp sync:Thu Mar 16 12:00:21 2006
execute date
current date is: 2006-03-16

To force synchronization with an NTP server, toggle the following command:
set ntpsync enable/disable

If all devices have the same time, it helps to correlate log entries from different devices.

IP address

There may be times when you want to verify the IP addresses assigned to the FortiGate unit interfaces are what you expect them to be. This is easily accomplished from the CLI using the following command.

diag ip address list

The output from this command lists the IP address and mask if available, the index of the interface (a sort of ID number) and the devname is the name of the interface. While physical interface names are set, virtual interface names can vary. Listing all the virtual interface names is a good use of this command. For vsys_ha and vsys_fgfm, the IP addresses are the local host — these are internally used virtual interfaces.

```
# diag ip address list
IP=10.31.101.100->10.31.101.100/255.255.255.0 index=3 devname=internal
IP=172.20.120.122->172.20.120.122/255.255.255.0 index=5 devname=wan1
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=8 devname=root
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=11 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=13 devname=vsys_fgfm
```

Other related commands include flushing the IP addresses (diag ip address flush), which will force a reload of the IP addresses. This can be useful if you think an IP address is wrong and don't want to reboot the unit. You can add or delete a single IP address (diag ip address add <ipv4_addr> or diag ip address delete <ipv4_addr>).

Business
Services   orange™

8.2   FortiGuard troubleshooting

The FortiGuard service provides updates to Antivirus, IPsec, Webfiltering, and more. The FortiGuard Distribution System (FDS) involves a number of servers across the world that provide updates to your FortiGate unit. Problems can occur both with connection to FDS, and its configuration on your local FortiGate unit. Some of the more common troubleshooting methods are listed here including

8.2.1   Troubleshooting process for FortiGuard updates

The following process are the logical steps to take when troubleshooting FortiGuard update problems. This includes antivirus (AV), intrusion protection services (IPS), antispam (AS), and web filtering (WB).

1. Does the device have a valid licence that includes these services?

    Each device requires a valid FortiGuard license to access updates for some or all of these services. You can verify the support contract status for your devices at the Fortinet Support website — https://support.fortinet.com/.

2. If the device is part of an HA cluster, do all members of the cluster have the same level of support?

    As with the previous step, you can verify the support contract status for all the devices in your HA cluster at the Fortinet Support website.

3. Have services been enabled on the device?

    To see the FortiGuard information and status for a device, in the web-based manager go to System > Config > FortiGuard. On that page you can verify the status of each component, and if required enable each service. If there are problems, see the FortiGuard section of the FortiOS Handbook.

4. Is the device able to communicate with FortiGuard servers?

    At System > Config > FortiGuard you can also attempt to update AV and IPS, or test the availability of WF and AS default and alternate ports. If there are problems, see the FortiGuard section of the FortiOS Handbook.

5. Is there proper routing to reach the FortiGuard servers?

    Ensure there is a static or dynamic route that enables your ForitGate unit to reach the FortiGuard servers. Usually a generic default route to the internet is enough, but you may need to verify this if your network is complex.

6. Are there issues with DNS?

    An easy way to test this is to attempt a traceroute from behind the FortiGate unit to an external network using the FQDN for a location. If the traceroute FQDN name does not resolve, you have general DNS problems.

7. Is there anything upstream that might be blocking FortiGuard traffic, either on the network or ISP side?

    Many firewalls block all ports by default, and often ISPs block ports that are low. There may be a firewall between the FortiGate unit and the FortiGuard servers that is blocking the traffic. FortiGuard uses port 53 by default, so if it is being blocked you need to either open a hole for it, or change the port it is using.

8. Is there an issue with source ports?

   It is possible that ports used to contact FortiGuard are being changed before reaching FortiGuard or on the return trip before reaching your FortiGate unit. A possible solution for this is to use a fixed-port at NATd firewalls to ensure the port remains the same. Packet sniffing can be used to find more information on what is happening with ports.

9. Are there security policies that include antivirus?

   If no security policies include antivirus, the antivirus databse will not be updated. If antivirus is included, only the database type used will be updated.

8.2.2   FortiGuard server settings

Your local FortiGate unit connects to remote FortiGuard servers get updates to FortiGuard information such as new viruses that may have been found or other new threats. This section demonstrates ways to display information about FortiGuard server information on your FortiGate unit, and how to use that information and update it to fix potential problems.

Displaying the server list

The get webfilter status command shows the list of FDS servers the FortiGate unit is using to send web filtering requests. Rating requests are only sent to the server on the top of the list in normal operation. Each server is probed for Round Trip Time (RTT) every two minutes.

You can optionally add a refresh rate to the end of this command and that will determine how often the server list will be refreshed.

Rating may not be enabled on your FortiGate unit.

> *get webfilter status*

Sample Output:
> *Locale : english*
> *License : Contract*
> *Expiration : Thu Oct 9 02:00:00 2011*
> *Hostname : fortiguard.example.com*
> *-=- Server List (Mon Feb 18 12:55:48 2008) -=-*

IP	Weight	RTT	Flags	TZ	Packets	CurrLost	TotalLost
a.b.c.d	0	1	DI	2	1926879	0	11176
10.1.101.1	10	329		1	10263	0	633
10.2.102.2	20	169		0	16105	0	80
10.3.103.3	20	182		0	6741	0	776
10.4.104.4	20	184		0	5249	0	987
10.5.105.5	25	181		0	12072	0	178

Output Details

Hostname is the name of the FortiGuard server the FortiGate unit will attempt to contact. The Server List includes the IP addresses of alternate servers if the first entry cannot be reached. In this example the IP addresses are not public addresses

The following flags in get webfilter status indicate the server status:

- D - the server was found through the DNS lookup of the hostname. If the hostname returns more than one IP address, all of them will be flagged with D and will be used first for INIT requests before falling back to the other servers.

- I - the server to which the last INIT request was sent.

- F - the server has not responded to requests and is considered to have failed.

- T - the server is currently being timed.

Sorting the server list
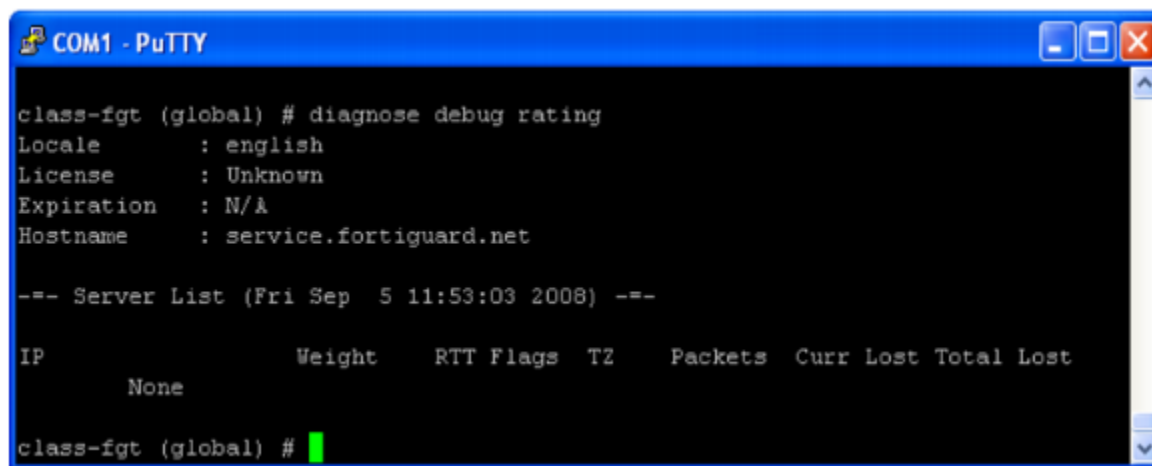
The server list is sorted first by weight. The server with the smallest RTT is put at the top of the list, regardless of weight. When a packet is lost (there has been no response in 2 seconds), it will be resent to the next server in the list. Therefore, the top position in the list is selected based on RTT while the other list positions are based on weight.

Calculating weight

The weight for each server increases with failed packets and decreases with successful packets. To lower the possibility of using a remote server, the weight is not allowed to dip below a base weight, calculated as the difference in hours between the FortiGate unit and the server times 10. The further away the server is, the higher its base weight and the lower in the list it will appear.

Note	The output for the *diag debug rating* command will vary based on the state of the FortiGate device.

The following output is from a FortiGate device that has no DNS resolution for service.fortiguard.net.

If only three IP addresses appear with the D flag, it means that DNS is good but probably the FortiGuard ports 53 and 8888 are blocked.

When the license is expired, an INIT request will be sent every 10 minutes for up to six attempts. If a license is not found after this limit is reached, the INIT requests will be sent every day.

A low source port number may appear which means that ports 1024 and 1025 could be blocked on the path to the FDS. Increase the source port on the FortiGate device with the following commands:

> *config sys global*
> *set ip-src-port-range <start-end> (Default 1024-25000)*

Be careful moving ports like this as it may cause some services to stop working if they can't access their original ports. If you make this change, ensure all services that use ports are checked and updated to new port numbers if needed.

8.2.3   FortiGuard URL rating

The following commands can be used to troubleshoot issues with FortiGuard URL ratings:

> *diag debug enable*
> *diag debug application urlfilter -1*

Sample output:

> *id=93000   msg="pid=57   urlfilter_main-723   in   main.c   received   pkt:count=91, a=/tmp/.thttp.socket/21" id=22009 msg="received a request /tmp/.thttp.socket, addr_len=21: d= ="www.goodorg.org:80, id=12853, vfid=0, type=0, client=192.168.3.90, url=/" id=99501 user="N/A" src=192.168.3.90 sport=1321 dst=<dest_ip> dport=80 service="http" cat=43 cat_desc="Organisation" hostname="www.goodorg.org" url="/" status=blocked msg="URL belongs to a denied category in policy"*

Sample output:

> *id=22009   msg="received   a   request   /tmp/.thttp.socket,   addr_len=21: d=pt.dnstest.google.com:80, id=300, vfid=0, type=0, client=192.168.3.12, url=/gen_204"*
>
> *id=93003 user="N/A" src=192.168.3.12 sport=21715 dst=<dest_ip> dport=80 service="http" cat=41 cat_desc="Search Engines" hostname="pt.dnstest.google.com" url="/gen_204"* status=passthrough msg="URL belongs to an allowed category in the policy"

id=93000		The process ID (PID) is listed along with the function in the file running (main.c). Then it lists the number of packets received and the associated socket where the packets came from.
	msg="pid=57 urlfilter_main-723 in main.c received pkt:count=91, a=/tmp/.thttp.socket/21"	
id=22009		Received a request on a particular socket (/tmp/.thttp.socket). The website to be rated is "www.goodorg.org:80" and the client browser that wants the verification is 192.169.3.90.
	msg="received a request /tmp/.thttp.socket, addr_len=21: d= ="www.goodorg.org:80, id=12853, vfid=0, type=0, client=192.168.3.90, url=/"	
id=99501		No user associated with this source address (192.168.3.90) and port (1321). The destination IP is unknown and the port is the
	user="N/A" src=192.168.3.90	

| | sport=1321 dst=<dest_ip> dport=80 service="http" cat=43 cat_desc="Organisation" hostname="www.goodorg.org" url="/" status=blocked msg="URL belongs to a denied category in policy" | standard HTTP port 80, which is confirmed by service=http. The cat keyword gives the category of the URL being checked, which turns out to be an organization. This is confirmed by the hostname of "goodorg.org". The status is stated as blocked with the reason stated as "URL belongs to a denied category in policy". |

Business Services orange

9 Verifying FortiGate admin access security

FortiOS provides a number of methods that help to enhance FortiGate administrative access security. This section describes FortiGate administrative access security best practices.

9.1 Install the FortiGate unit in a physically secure location

A good place to start with is physical security. Install the FortiGate unit in a secure location, such as a locked room or a room with restricted access. This way unauthorized users can't get physical access to the device.

If unauthorized users have physical access they can disrupt your entire network by disconnecting your FortiGate unit (either by accident or on purpose). They could also connect a console cable and attempt to log into the CLI. Also, when a FortiGate unit reboots, a person with physical access can interrupt the boot process and install different firmware.

9.2 Add new administrator accounts

Rather than allowing all administrators to access the FortiGate unit with the admin administrator account you should create administrator accounts for each person that requires administrative access. That way you can track who has made configuration changes and performed other administrative activities. Keep the number of administrative accounts to a minimum to keep better control on who can access the device.

To add administrators go to **System > Admin > Administrators** and select **Create New**.

If you want administrators to have access to all FortiGate configuration options, their accounts should have the prof_admin admin profile. Administrators with this profile can do anything except add new administrator accounts.

At least one account should always have the super_admin profile as this profile is required to add and remove administrators. To improve security only a very few administrators (usually one) should be able to add new administrators.

If you want some administrator accounts to have limited access to the FortiGate configuration you can create custom admin profiles that only allow access to selected parts of the configuration. To add custom admin profiles, go to **System > Admin > Admin Profiles** and select **Create New**.

For example, if you want to add an admin profile that does not allow changing firewall policies, when you configure the admin profile set Firewall Configuration to None or Read Only.

9.3 Change the admin account name and limit access to this account

The default super_admin administrator account, admin, is a well-known administrator name so if this account is available it could be easier for attackers to access the FortiGate unit because they know they can log in with this name, only having to determine the password. You can improve security by changing this name to one more difficult for an attacker to guess. To do this, create a new administrator account with the super_admin admin profile and log in as that administrator. Then go to **System > Admin > Administrators** and edit the admin administrator and change the Administrator name.

Once the account has been renamed you could delete the super_admin account that you just added. Consider also only using the super-admin account for adding or changing administrators. The less this account is used to less likely that it could be compromised. You could also store the account name and password for this account in a secure location in case for some reason the account name or password is forgotten.

9.4 Only allow administrative access to the external interface when needed

When possible, don't allow administration access on the external interface and use internal access methods such as IPsec VPN or SSL VPN.

To disable administrative access on the external interface, go to System > Network > Interfaces, edit the external interface and disable HTTPS, PING, HTTP, SSH, and TELNET under Administrative Access.

This can also be done with CLI using following commands:

```
config system interface
  edit <external_interface_name>
    unset allowaccess
end
```

Please note that this will disable all services on the external interface including CAPWAP, FMG-Access, SNMP, and FCT-Access.

If you need some of these services enabled on your external interface, for example CAPWAP and FMG-Access to ensure connectivity between FortiGate unit and respectively FortiAP and FortiManager, then you need to use following CLI command:

```
config system interface
  edit <external_interface_name>
    set allowaccess capwap fgfm
end
```

9.5 When enabling remote access, configure Trusted Hosts and Two-factor Authentication

If you have to have remote access and can't use IPsec or SSL VPN then you should only allow HTTPS and SSH and use secure access methods such as trusted hosts and Two-facor authentication.

9.5.1 Configuring Trusted Hosts

Setting trusted hosts for administrators limits what computers an administrator can log in the FortiGate unit from. When you identify a trusted host, the FortiGate unit will only accept the administrator's login from the configured IP address or subnet. Any attempt to log in with the same credentials from any other IP address or any other subnet will be dropped. To ensure the administrator has access from different locations, you can enter up to ten IP addresses or subnets. Ideally, this should be kept to a minimum. For higher security, use an IP address with a net mask of 255.255.255.255, and enter an IP address (non-zero) in each of the three default trusted host fields.

Trusted hosts are configured when adding a new administrator by going to System > Admin > Administrators in the web-based manager and selecting Restrict this Admin Login from Trusted Hosts Only, or config system admin in the CLI.

The trusted hosts apply to the web-based manager, ping, snmp and the CLI when accessed through SSH. CLI access through the console port is not affected.

Also ensure all entries contain actual IP addresses, not the default 0.0.0.0.

9.5.2   Configuring Two-factor Authentication

FortiOS 5.0 provides support for FortiToken and FortiToken Mobile. FortiToken Mobile is a Fortinet application that enables you to generate One Time Passwords (OTPs) on a mobile device for FortiGate two-factor authentication. The user's mobile device and the FortiGate unit must be connected to the Internet to activate FortiToken mobile. Once activated, users can generate OTPs on their mobile device without having network access. FortiToken Mobile is available for iOS and Android devices from their respective Application stores. No cellular network is required for activation.

The latest FortiToken Mobile documentation is available from the FortiToken page of the

Fortinet Technical Documentation website.

Two free trial tokens are included with every registered FortiGate unit. Additional tokens can be purchased from your reseller or from Fortinet.

To assign a token to an administrator go to System > Admin > Administrators and either add a new or select an existing administrator to assign the token to. Configure the administrator as required, you need to enter your email address and phone number in order to receive the activation code for the FortiToken mobile. Select Enable Two-factor Authentication. Select the token to associate with the administrator. Select OK to assign the token to the administrator.

To configure your FortiGate unit to send email or SMS messages go to System > Config > Messaging Servers.

9.6   Change the default administrative port to a non-standard port

Administration Settings under System > Admin > Settings or config system global in the CLI, enable you to change the default port configurations for administrative connections to the FortiGate unit for added security. When connecting to the FortiGate unit when the port has changed, the port must be included. For example, if you are connecting to the FortiGate unit using HTTPS over port 8081, the url would be https://192.168.1.99:8081

If you make a change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is not used for other services.

9.7   Enable Password Policy

Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. For example, if "p4ssw0rd" is used as a password, it can be cracked.

Password policies, available by going to System > Admin > Settings > Enable Password Policy, enable you to create a password policy that any administrator who updates their passwords, must follow. Using the available options you can define the required length of the password, what it must contain (numbers, upper and lower case, and so on) and an expiry time frame. The FortiGate unit will warn of any password that is added and does not meet the criteria.

9.8   Maintain short login timeouts

To avoid the possibility of an administrator walking away from the management computer and leaving it exposed to unauthorized personnel, you can add an idle time-out. That is, if the web-based manager is not used for a specified amount of time, the FortiGate unit will automatically log the administrator out. To continue their work, they must log in again.

The time-out can be set as high as 480 minutes, or eight hours, although this is not recommend.

To set the idle time out, go to System > Admin > Settings and enter the amount of time for the Idle Timeout. A best practice is to keep the default of 5 min.

When logging into the console using SSH, the default time of inactivity to successfully log into the FortiGate unit is 120 seconds (2 minutes). You can configure the time to be shorter by using the CLI to change the length of time the command prompt remains idle before the FortiGate unit will log the administrator out. The range can be between 10 and 3600 seconds. To set the logout time enter the following CLI commands:

> *config system global*
>   *set admin-ssh-grace-time <number_of_seconds>*
> *end*

9.9   Modify administrator account Lockout Duration and Threshold values

Account lockout policies control how and when accounts are locked out of the FortiGate unit. These policies are described and implemented as follows:

9.9.1   Administrator account Lockout Duration

If someone violates the lockout controls by entering an incorrect user name and/or password, account lockout duration sets the length of time the account is locked. the lockout duration can be set to a specific length of time using a value between 1 and 4294967295 seconds. The default value is 60 seconds.

When it's required use the CLI to modify the lockout duration as follow:

> *config system global*
>   *set admin-lockout-duration <integer>*
> *end*

9.9.2   Administrator account Lockout Threshold

The lockout threshold sets the number of invalid logon attempts that are allowed before an account is locked out. You may set a value that balances the need to prevent account cracking against the needs of an administrator who may have difficulty accessing their account.

Its normal for an administrator to sometimes take a few attempts to logon with the right password.

The lockout threshold can be set to any value from 1 to 10. The Default value is 3, which is normally a good setting. However, to improve security you could reduce it to 1 or 2 as long as administrators know to take extra care when entering their passwords.

Use the following CLI command to modify the lockout threshold:

> *config system global*
>   *set admin-lockout-threshold <integer>*

end

Keep in mind that the higher the lockout value, the higher the risk that someone may be able to break into the FortiGate unit.

9.10 Disable auto installation via USB

An attacker with a physical access to the device could load a new configuration or firmware on the FortiGate using the USB port, reinitializing the device through a power cut. To avoid this, execute the following CLI commands:

config system auto-install
  set auto-install-config disable
  set auto-install-image disable
end

9.11 Auditing and Logging

Audit web facing administration interfaces. By default, FortiGate logs all deny action, you can check these actions by going **to Log & Report > Event Log > System**. This default behavior should not be changed. Also secure log files in a central location such as FortiCloud and configure alert email which provides an efficient and direct method of notifying an administrator of events. You can configure log settings by going to **Log & Report > Log Config**.

An auditing schedule should be established to routinely inspect logs for signs of intrusion and probing.

10 Life of a Packet

Directed by security policies, a FortiGate unit screens network traffic from the IP layer up through the application layer of the TCP/IP stack. This chapter provides a general, high-level description of what happens to a packet as it travels through a FortiGate security system.

The FortiGate unit performs three types of security inspection:

- stateful inspection, that provides individual packet-based security within a basic session state

- flow-based inspection, that buffers packets and uses pattern matching to identify security threats

- proxy-based inspection, that reconstructs content passing through the FortiGate unit and inspects the content for security threats.

Each inspection component plays a role in the processing of a packet as it traverses the FortiGate unit in route to its destination. To understand these inspections is the first step to understanding the flow of the packet.

10.1 Stateful inspection

With stateful inspection, the FortiGate unit looks at the first packet of a session to make a security decision. Common fields inspected include TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid communication and that the data is not corrupted or poorly formed.

What makes it stateful is that one or both ends must save information about the session history in order to communicate. In stateless communication, only independent requests and responses are used, that do not depend on previous data. For example, UDP is stateless by nature because it has no provision for reliability, ordering, or data integrity.

The FortiGate unit makes the decision to drop, pass or log a session based on what is found in the first packet of the session. If the FortiGate unit decides to drop or block the first packet of a session, then all subsequent packets in the same session are also dropped or blocked without being inspected. If the FortiGate unit accepts the first packet of a session, then all subsequent packets in the same session are also accepted without being inspected.

10.1.1 Connections over connectionless

A connection is established when two end points use a protocol to establish connection through use of various methods such as segment numbering to ensure data delivery, and handshaking to establish the initial connection. Connections can be stateful because they record information about the state of the connection. Persistent connections reduce request latency because the end points do not need to re-negotiate the connection multiple times, but instead just send the information without the extra overhead. By contrast, connectionless communication does not keep any information about the data being sent or the state. It is based on an autonomous response/reply that is independent of other responses/replies that may have gone before. One example of connectionless communication is IP.

Benefits of connections over connectionless include being able to split data up over multiple packets, the data allows for a best-effort approach, and once the connection is established subsequent packets

are not required to contain the full addressing information which saves on bandwidth. Connections are often reliable network services since acknowledgements can be sent when data is received.

10.1.2 What is a session?

A session is established on an existing connection, for a defined period of time, using a determined type of communication or protocol. Sessions can have specific bandwidth , and time to live (TTL) parameters.

You can compare a session to a conversation. A session is established when one end point initiates a request by establishing a TCP connection on a particular port, the receiving end is listening on that port, and replies. You could telnet to port 80 even though telnet normally uses port 23, because at this level, the application being used cannot be determined.

However, the strong points of sessions and stateful protocols can also be their weak points. Denial of service (DoS) attacks involve creating so many sessions that the connection state information tables are full and the unit will not accept additional sessions.

10.1.3 Differences between connections and sessions

In almost all cases, established sessions are stateful and all involve connections. However, some types of connections, such as UDP, are stateless, and are not sessions.

This means that not all traffic can be inspected by stateful inspection, because some of it is stateless. For example IP packets are stateless. Communications using HTTP are stateless, but HTTP often uses cookies to store persistent data in a way that approaches stateful.

Stateful inspection of sessions has the benefit of being able to apply the initial connection information to the packets that follow — the end points of the session will remain the same as will the protocol for example. That information can be examined for the first packet of the session and if it is malicious or not appropriate, the whole session can be dropped without committing significant resources.
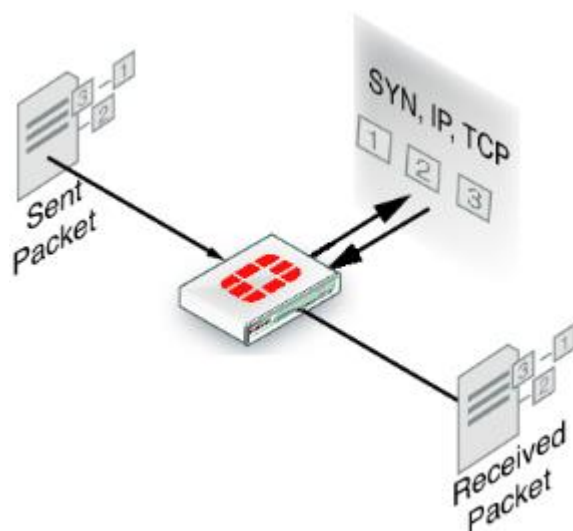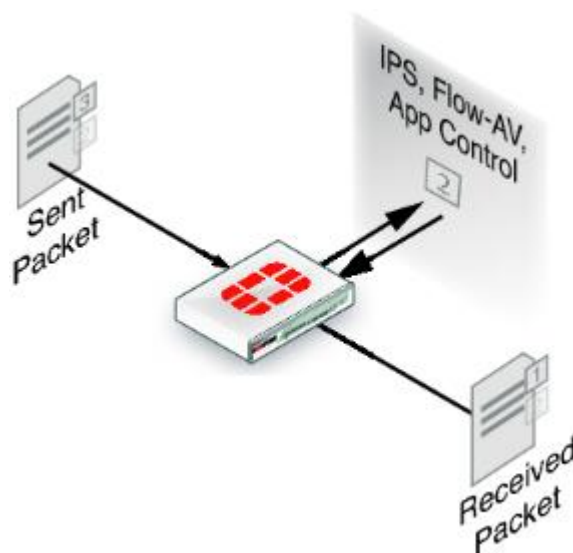

10.2 Flow inspection

With flow inspection (also called flow-based inspection), the FortiGate unit samples multiple packets in a session and multiple sessions, and uses a pattern matching engine to determine the kind of activity

that the session is performing and to identify possible attacks or viruses. For example, if application control is operating, flow inspection can sample network traffic and identify the application that is generating the activity. Flow inspection using IPS samples network traffic and determines if the traffic constitutes an attack. Flow inspection can also be used for antivirus protection, web filtering, and data leak protection (DLP). Flow inspection occurs as the data is passing from its source to its destination. Flow inspection identifies and blocks security threats in real time as they are identified.

Flow inspection typically requires less processing than proxy inspection, and therefore flow antivirus, web filtering, and DLP inspection performance can be better than proxy inspection performance. However, some threats can only be detected when a complete copy of the payload (for example a complete email attachment) is obtained so, proxy inspection tends to be more accurate and complete than flow inspection.

10.3 Proxy inspection

Proxy inspection examines the content contained in content protocol sessions for security threats. Content protocols include HTTP, FTP, and email protocols. Security threats can be found in files and other content downloaded using these protocols. With proxy inspection, the FortiGate unit downloads the entire payload of a content protocol session and re-constructs it. For example, proxy inspection can reconstruct an email message and its attachments. After a satisfactory inspection the FortiGate unit passes the content on to the client. If the proxy inspection detects a security threat in the content, the content is removed from the communication stream before it reaches its destination. For example, if proxy inspection detects a virus in an email attachment, the attachment is removed from the email message before its sent to the client. Proxy inspection is the most thorough inspection of all, although it requires more processing power, and this may result in lower performance.
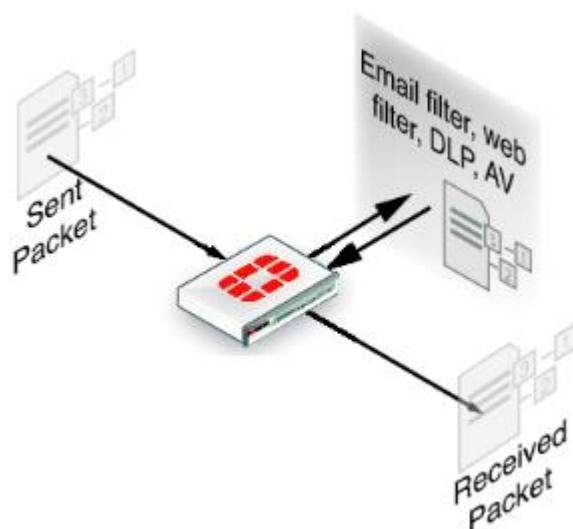
10.4 Comparison of inspection layers

The three inspection methods each have their own strengths and weaknesses. The following table looks at all three methods side-by-side.

Feature	Stateful	Flow	Proxy
Inspection unit per session	first packet	selected packets	complete content
Memory, CPU required	low	medium	high
Level of threat protection	good	better	best
Authentication	yes		
IPsec and SSL VPN	yes		
Antivirus protection		yes	yes
Web Filtering		yes	yes
Data Leak Protection (DLP)		yes	yes
Application control		yes	
IPS		yes	
Delay in traffic		no	small
Reconstruct entire content		no	yes

10.5 FortiOS functions and security layers

Within these security inspection types, FortiOS functions map to different inspections. The table below outlines when actions are taken as a packet progresses through its life within a FortiGate unit.

Security Function	Stateful	Flow	Proxy
Firewall	yes		
IPsec VPN	yes		
Traffic Shaping	yes		
User Authentication	yes		
Management Traffic	yes		
SSL VPN	yes		
Intrusion Prevention		yes	
Antivirus		yes	yes
Application Control		yes	
Web filtering		yes	yes
DLP			yes
Email Filtering		yes	yes
VoIP inspection			yes

10.6 Packet flow

After the FortiGate unit's external interface receives a packet, the packet proceeds through a number of steps on its way to the internal interface, traversing each of the inspection types, depending on the security policy and security profile configuration. The diagram in Figure 166 is a high level view of the packet's journey.

The description following is a high-level description of these steps as a packet enters the FortiGate unit towards its destination on the internal network. Similar steps occur for outbound traffic.

10.6.1   Packet inspection (Ingress)

In Figure below, in the first set of steps (ingress), a number of header checks take place to ensure the packet is valid and contains the necessary information to reach its destination. This includes:

- Packet verification - during the IP integrity stage, verification is performed to ensure that the layer 4 protocol header is the correct length. If not, the packet is dropped.

- Session creation - the FortiGate unit attempts to create a session for the incoming data

- IP stack validation for routing - the firewall performs IP header length, version and checksum verifications in preparation for routing the packet.

- Verifications of IP options - the FortiGate unit validates the rouging information

Business
Services   orange™
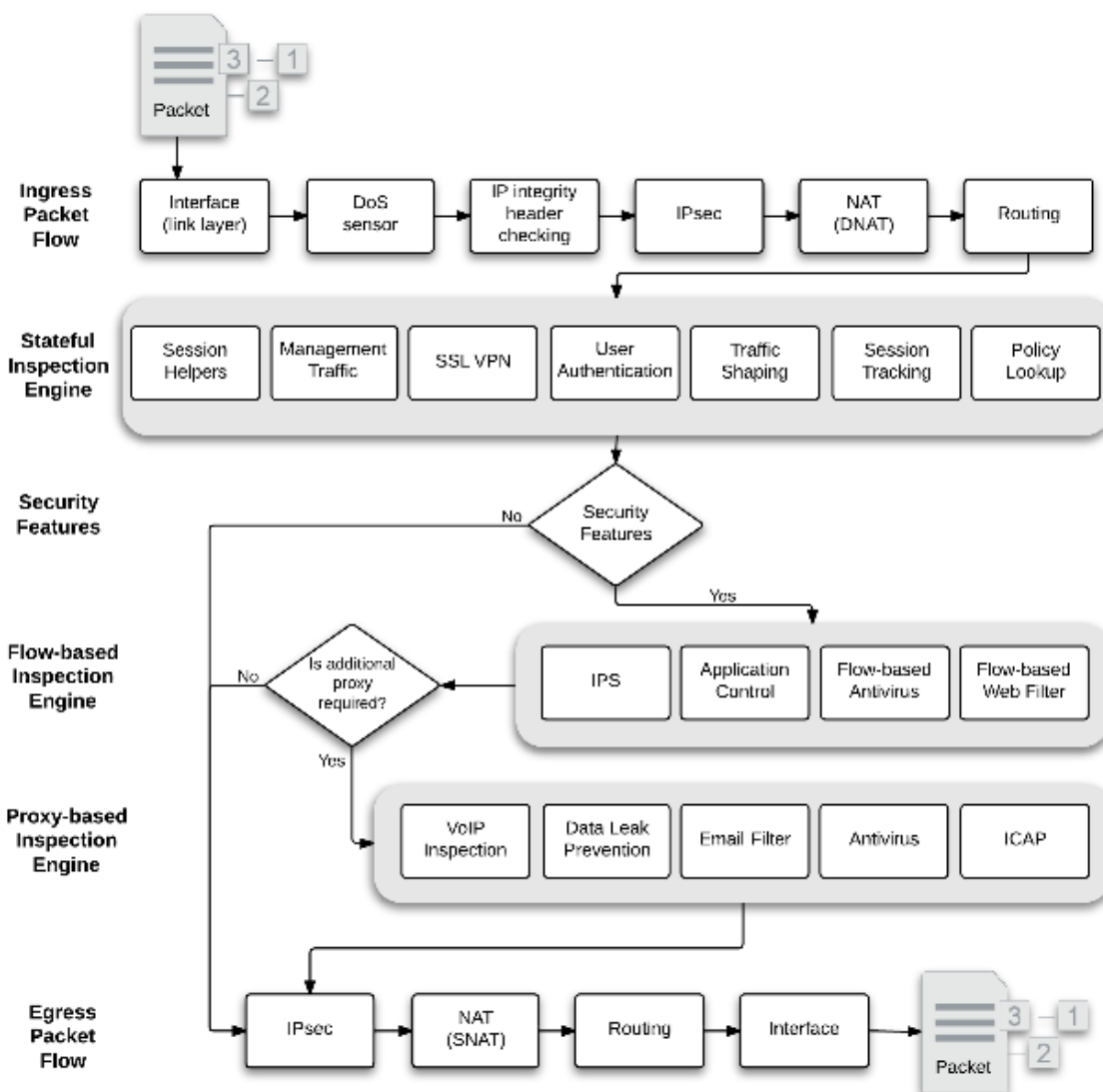
10.6.2   Interface

Ingress packets are received by a FortiGate interface. The packet enters the system, and the interface network device driver passes the packet to the Denial of Service (DoS) sensors, if enabled, to determine whether this is a valid information request or not.

10.6.3   DoS sensor

DoS scans are handled very early in the life of the packet to determine whether the traffic is valid or is part of a DoS attack. Unlike signature-based IPS which inspects all the packets within a certain traffic flow, the DoS module inspects all traffic flows but only tracks packets that can be used for DoS attacks (for example TCP SYN packets), to ensure they are within the permitted parameters. Suspected DoS attacks are blocked, other packets are allowed.

Business
Services   orange

10.6.4   IP integrity header checking

The FortiGate unit reads the packet headers to verify if the packet is a valid TCP, UDP, ICMP, SCTP or GRE packet. The only verification that is done at this step to ensure that the protocol header is the correct length. If it is, the packet is allowed to carry on to the next step. If not, the packet is dropped.

10.6.5   IPsec

If the packet is an IPsec packet, the IPsec engine attempts to decrypt it. The IPsec engine applies the correct encryption keys to the IPsec packet and sends the unencrypted packet to the next step. IPsec is bypassed when for non-IPsec traffic and for IPsec traffic that cannot be decrypted by the FortiGate unit.

10.6.6   Destination NAT (DNAT)

The FortiGate unit checks the NAT table and determines the destination IP address for the traffic. This step determines whether a route to the destination address actually exists.

For example, if a user's browser on the internal network at IP address 192.168.1.1 visited the web site www.example.com using NAT, after passing through the FortiGate unit the source IP address becomes NATed to the FortiGate unit external interface IP address. The destination address of the reply back from www.example.com is the IP address of the FortiGate unit internal interface. For this reply packet to be returned to the user, the destination IP address must be destination NATed to 192.168.1.1.

DNAT must take place before routing so that the FortiGate unit can route packets to the correct destination.

10.6.7   Routing

The routing step determines the outgoing interface to be used by the packet as it leaves the FortiGate unit. In the previous step, the FortiGate unit determined the real destination address, so it can now refer to its routing table and decide where the packet must go next.

Routing also distinguishes between local traffic and forwarded traffic and selects the source and destination interfaces used by the security policy engine to accept or deny the packet.

10.6.8   Policy lookup

The policy look up is where the FortiGate unit reviews the list of security policies which govern the flow of network traffic, from the first entry to the last, to find a match for the source and destination IP addresses and port numbers. The decision to accept or deny a packet, after being verified as a valid request within the stateful inspection, occurs here. A denied packet is discarded. An accepted packet will have further actions taken. If IPS is enabled, the packet will go to Flow-based inspection engine, otherwise it will go to the Proxy-based inspection engine.

If no other security options are enabled, then the session was only subject to stateful inspection. If the action is accept, the packet will go to Source NAT to be ready to leave the FortiGate unit.

10.6.9   Session tracking

Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions.

10.6.10   User authentication

User authentication added to security policies is handled by the stateful inspection engine, which is why Firewall authentication is based on IP address. Authentication takes place after policy lookup selects a security policy that includes authentication. This is also known as identify-based policies. Authentication also takes place before security features are applied to the packet.

10.6.11   Management traffic

This local traffic is delivered to the FortiGate unit TCP/IP stack and includes communication with the web-based manager, the CLI, the FortiGuard network, log messages sent to FortiGate or a remote syslog server, and so on. Management traffic is processed by applications such as the web server which displays the FortiOS web-based manager, the SSH server for the CLI or the FortiGuard server to handle local FortiGuard database updates or FortiGuard Web Filtering URL lookups.

10.6.12   SSL VPN traffic

For local SSL VPN traffic, the internal packets are decrypted and are routed to a special interface. This interface is typically called ssl.root for decryption. Once decrypted, the packets go to policy lookup.

10.6.13   ICAP traffic

If you enable ICAP in a security policy, HTTP (and optionally HTTPS) traffic intercepted by the policy is transferred to ICAP servers in the ICAP profile added to the policy. The FortiGate unit is the surrogate, or "middle-man", and carries the ICAP responses from the ICAP server to the ICAP client; the ICAP client then responds back, and the FortiGate unit determines the action that should be taken with these ICAP responses and requests.

10.6.14   Session helpers

Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. For example, the SIP VoIP protocol uses TCP control packets with a standard destination port to set up SIP calls. To successfully process SIP VoIP calls, FortiOS must be able to extract information from the body of the SIP packet and use this information to allow the voice-carrying packets through the firewall.

FortiOS uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow those protocols to send packets through the firewall.

10.6.15   Flow-based inspection engine

Flow-based inspection is responsible for IPS, application control, flow-based antivirus scanning and VoIP inspection. Packets are sent to flow-based inspection if the security policy that accepts the packets includes one or more of these security features.

   Note   Flow-based antivirus scanning is only available on some FortiGate models.

Business
Services

Once the packet has passed the flow-based engine, it can be sent to the proxy inspection engine or egress.

10.6.16 Proxy-based inspection engine

The proxy inspection engine is responsible for carrying out antivirus protection, email filtering (antispam), web filtering and data leak prevention. The proxy engine will process multiple packets to generate content before it is able to make a decision for a specific packet.

10.6.17 IPsec

If the packet is transmitted through an IPsec tunnel, it is at this stage the encryption and required encapsulation is performed. For non-IPsec traffic (TCP/UDP) this step is bypassed.

10.6.18 Source NAT (SNAT)

When preparing the packet to leave the FortiGate unit, it needs to NAT the source address of the packet to the external interface IP address of the FortiGate unit. For example, a packet from a user at 192.168.1.1 accessing www.example.com is now using a valid external IP address as its source address.

10.6.19 Routing

The final routing step determines the outgoing interface to be used by the packet as it leaves the FortiGate unit.

10.6.20 Egress

Upon completion of the scanning at the IP level, the packet exits the FortiGate unit.

10.7 Example 1: client / server connection

The following example illustrates the flow of a packet of a client/web server connection with authentication and FortiGuard URL and antivirus filtering.

This example includes the following steps:

Initiating connection from client to web server

1. Client sends packet to web server.
2. Packet intercepted by FortiGate unit interface.
2.1 Link level CRC and packet size checking. If the size is correct, the packet continues, otherwise it is dropped.
3. DoS sensor - checks are done to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking, verifying the IP header length, version and checksums.
5. Next hop route
6. Policy lookup
7. User authentication
8. Proxy inspection
8.1 Web Filtering

8.2 FortiGuard Web Filtering URL lookup

8.3 Antivirus scanning

9. Source NAT

10. Routing

11. Interface transmission to network

12. Packet forwarded to web server

Response from web server

1. Web Server sends response packet to client.

2. Packet intercepted by FortiGate unit interface

2.1 Link level CRC and packet size checking.

3. IP integrity header checking.

4. DoS sensor.

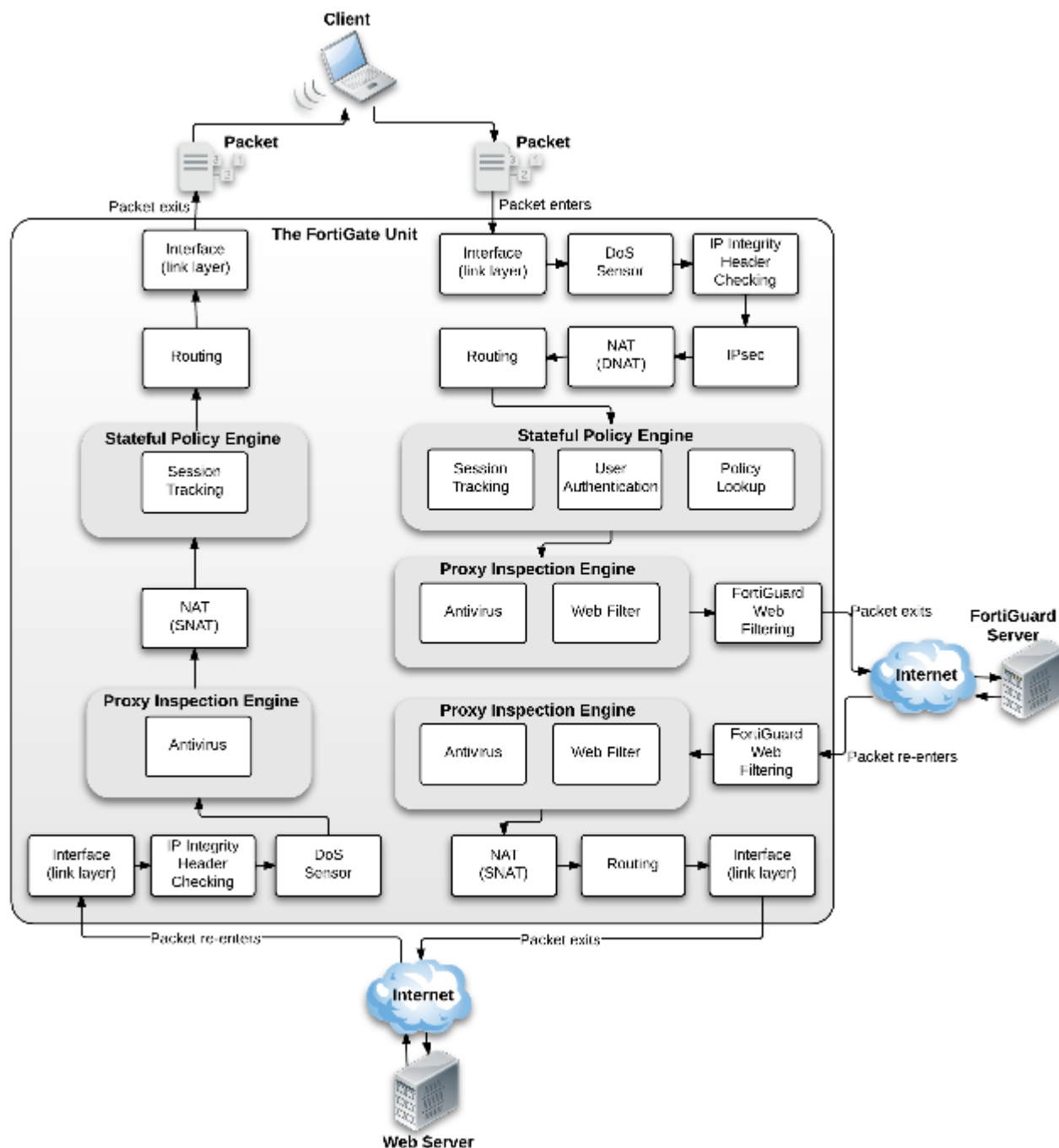5. Proxy inspection

5.1 Antivirus scanning.

6. Source NAT.

7. Stateful Policy Engine

7.1 Session Tracking

8. Next hop route

9. Interface transmission to network

10. Packet returns to client

Business
Services   orange

10.8 Example 2: Routing table update

The following example illustrates the flow of a packet when there is a routing table update. As this is low level, there is no security involved. This example includes the following steps:

1. FortiGate unit receives routing update packet

2. Packet intercepted by FortiGate unit interface

2.1 Link level CRC and packet size checking. If the size is correct, the packet continues, otherwise it is dropped.

3. DoS sensor - checks are done to ensure the sender is valid and not attempting a denial of service attack.

4. IP integrity header checking, verifying the IP header length, version and checksums.

5. Stateful policy engine

5.1 Management traffic (local traffic)

6. Routing module

6.1 Update routing table
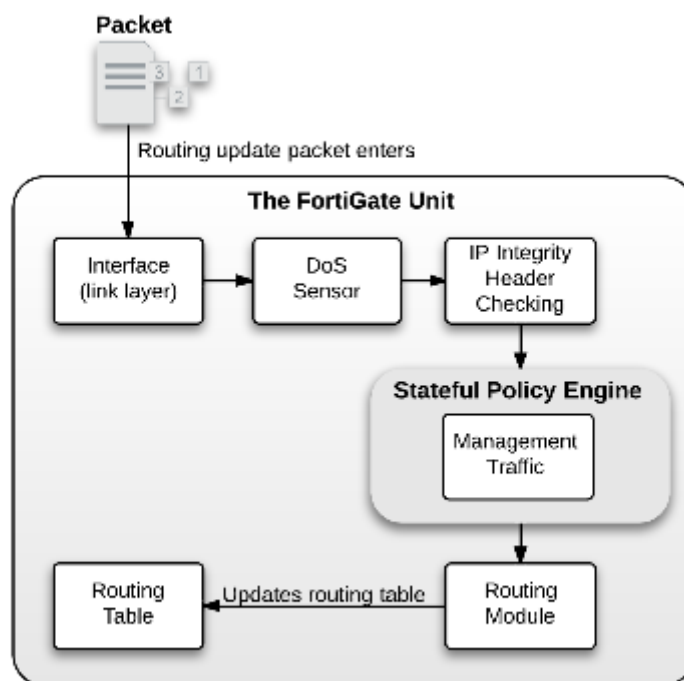
10.9 Example 3: Dialup IPsec VPN with application control

This example includes the following steps:

1. FortiGate unit receives IPsec packet from Internet

2. Packet intercepted by FortiGate unit interface

2.1 Link level CRC and packet size checking. If the size is correct, the packet continues, otherwise it is dropped.

3. DoS sensor - checks are done to ensure the sender is valid and not attempting a denial of service attack.

4. IP integrity header checking, verifying the IP header length, version and checksums.

5. IPsec

5.1 Determines that packet matched IPsec phase 1 configuration

5.2 Unencrypted packet

6. Next hop route

7. Stateful policy engine

7.1 Session tracking

8. Flow inspection engine

8.1 IPS

8.2 Application control

9. Source NAT

10. Routing

11. Interface transmission to network

12. Packet forwarded to internal server

Response from server

1. Server sends response packet

2. Packet intercepted by FortiGate unit interface

2.1 Link level CRC and packet size checking

3. IP integrity header checking.

4. DoS sensor

5. Flow inspection engine

5.1 IPS

5.2 Application control

6. Stateful policy engine

6.1 Session tracking

7. Next hop route

8. IPsec

8.1 Encrypts packet

9. Routing

10. Interface transmission to network

11. Encrypted Packet returns to internet

Business
Services orange

Business
Services   orange
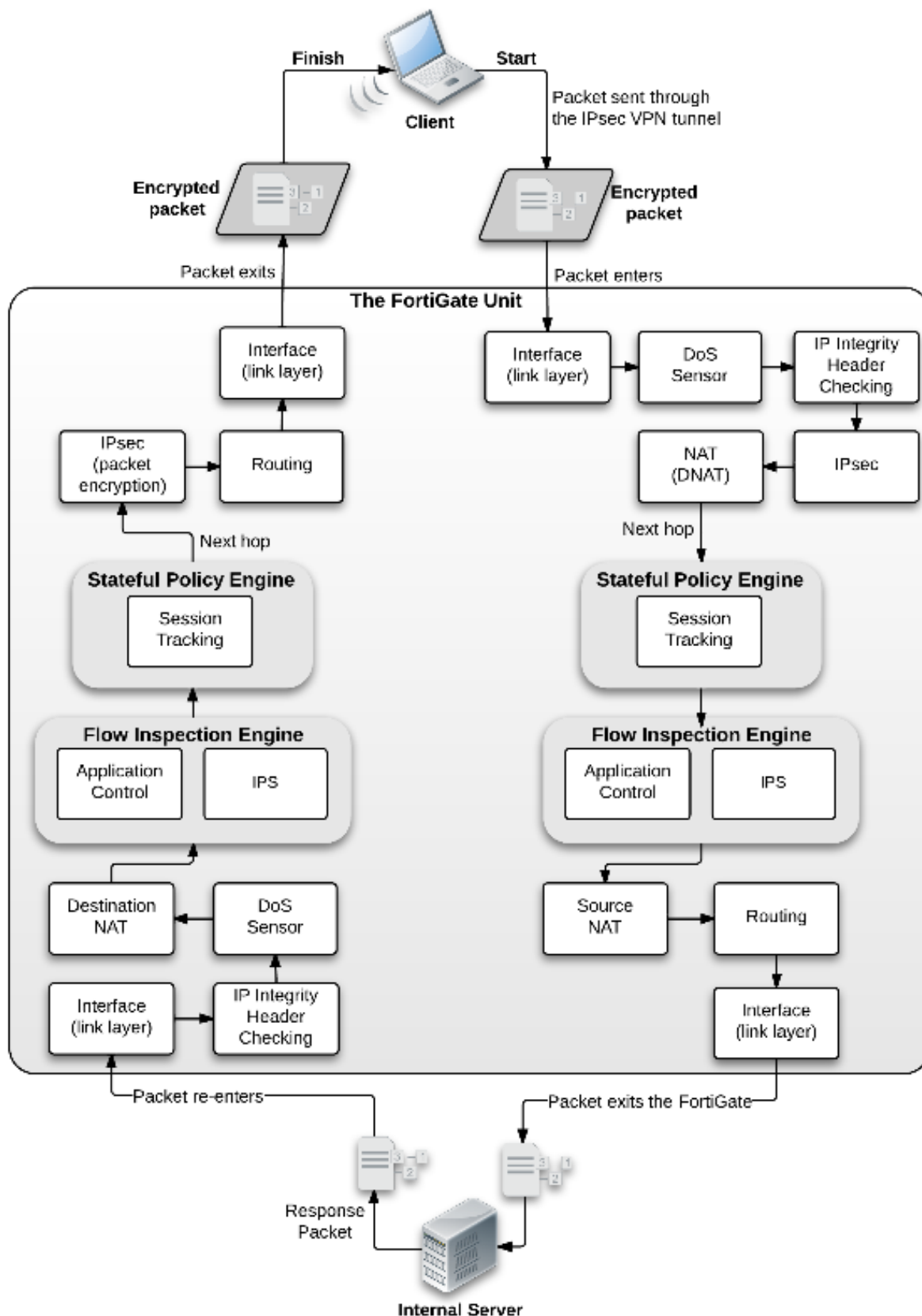
11 Technical Support Organization Overview

This section explains how Fortinet's technical support works, as well as how you can easily create an account to get technical support for when issues arise that you cannot solve yourself.

11.1 Fortinet Global Customer Services Organization

The Fortinet Global Customer Services Organization is composed of three regional Technical Assistance Centers (TAC):

- The Americas (AMER)
- Europe, Middle East, and Africa (EMEA)
- Asia Pacific (APAC)

The regional TACs are contacted through a global call center. Incoming service requests are then routed to the appropriate TAC. Each regional TAC delivers technical support to the customers in its regions during its hours of operation. These TACs also combine to provide seamless, around-the-clock support for all customers.
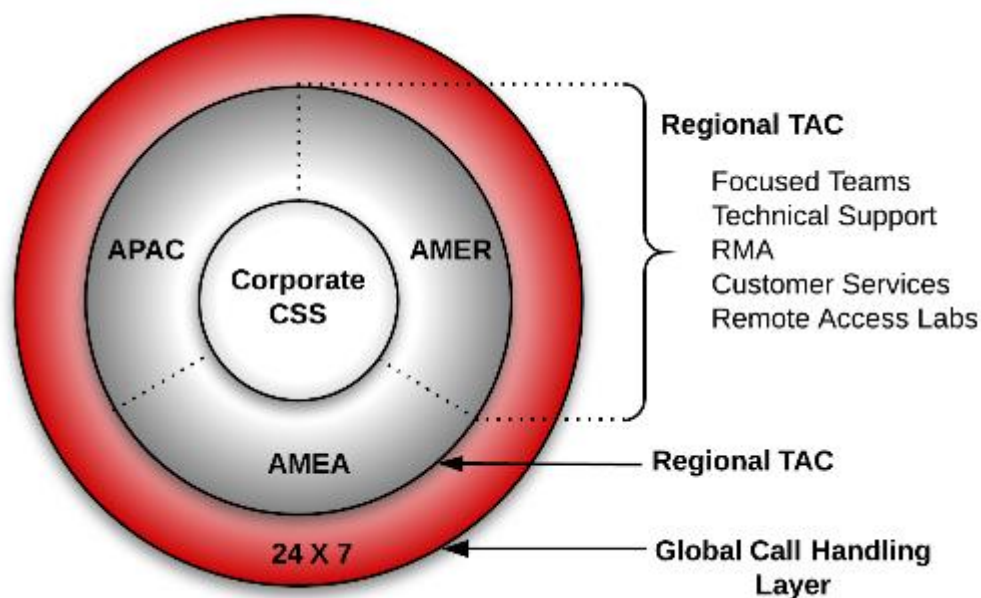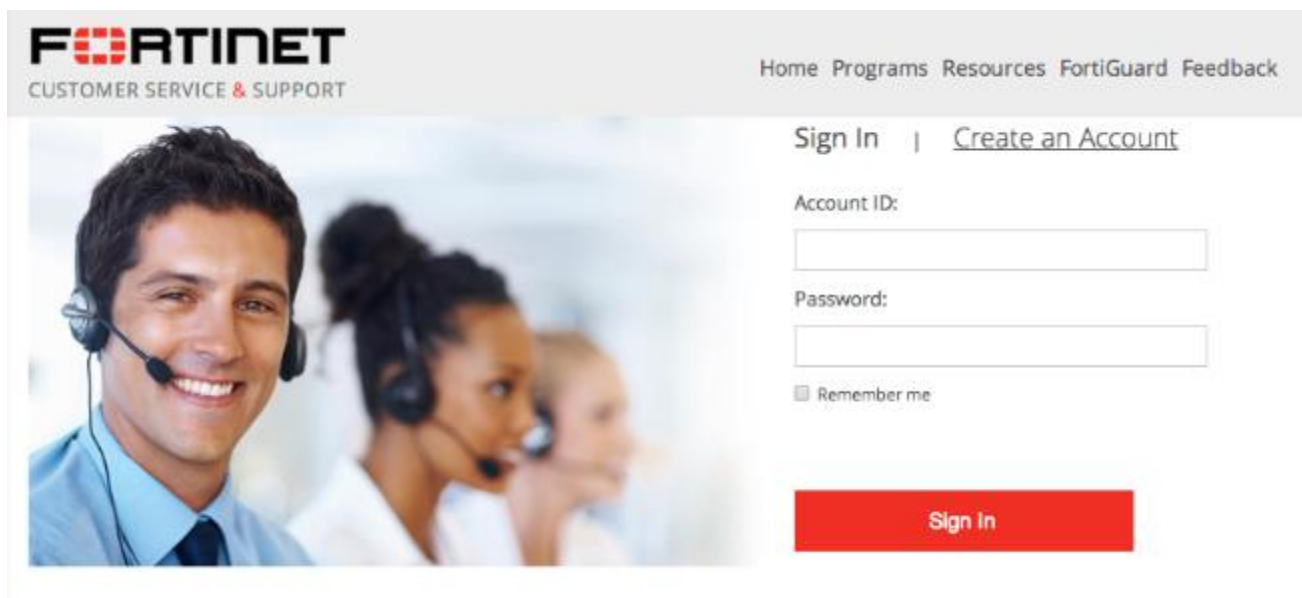
11.2 Creating an account

To receive technical support and service updates, Fortinet products in the organization must be registered. The Product Registration Form on the support website will allow the registration to be completed online. Creating an account on the support website is the first step in registering products.

Go to the Fortinet support site shown below:

https://support.fortinet.com/

Business Services
orange™

Once the support account has been created, product details can be provided by going to the *Product Register/Renew* and Manage Product buttons displayed on the home page. Alternately, the product registration can be completed at a later time.

11.3 Registering a device

Complete the following steps when registering a device for support purposes:

1. Log in using the Username and Password defined when the account was created

2. Under the Asset section, select Register/Renew to go to the Registration Wizard. Alternatively, use the Asset menu at the top of the page.

3. Get a serial number from the back of the FortiGate unit or from the exterior of the FortiGate shipping box.

4. Enter the serial number, service contract registration code or license certificate number to start the product registration.

5. Enter your registration information.

6. Read and accept the license agreement.

7. Complete the verification process.

8. Select Finish to complete the registration process.

11.4 Contact customer service & support

After you define your problem, researched a solution, created a plan, and executed that plan, and if you have not solved the problem, it is time to contact Customer Service & Support for assistance.

To receive technical support and service updates, your Fortinet product must be registered and reflect a valid support contract. Registration, support programs, assistance, and regional phone contacts are available at the following URL:

> https://support.fortinet.com

When you are registered and ready to contact support:

1. Prepare the following information first:

   • your contact information;

   • the firmware version;

   • a recent server policy configuration;

   • access to recent event, traffic and attack logs;

   • a network topology diagram and IP addresses;

   • a list of troubleshooting steps performed so far and the results.

For bootup problems:

   • provide all console messages and output;

   • if you suspect a hard disk issue, provide your evidence.

2. Document the problem and the steps you took to define the problem.

3. Open a support ticket.

11.5 Reporting problems

Problems can be reported to a Fortinet Technical Assistance Center in the following ways:

- By logging an online ticket
- By phoning a technical support center

11.5.1   Logging online tickets

Problem reporting methods differ depending on the type of customer.

Fortinet partners

Fortinet Partners are entitled to priority web-based technical support. This service is designed for partners who provide initial support to their customers and who need to open a support ticket with Fortinet on their behalf. We strongly encourage submission and follow up of support tickets using this service.

The support ticket can be submitted after logging into the partner website using one of the following links using FortiPartner account details:
http://partners.fortinet.com

This link will redirect to the general Fortinet Partner Portal extranet website. Click Support > Online Support Ticket.
https://forticare.fortinet.com/customersupport/Login/CommonLogin.aspx

Fortinet customers

There are two methods to report a technical issue on the Fortinet Support website: creating a technical support ticket by product or creating any type of ticket with the Ticket Wizard for more options.

 Fortinet customers should complete the following steps to create a support ticket by product:

1. Log in to the support website at the following address with the account credentials used when the account was created:
   https://support.fortinet.com

2. Navigate to the top menu, click Asset and select Manage/View Products.

3. In the product list, select the product that is causing the problem.

4. On the left side bar, go to the Assistance category, and select Technical Request to create a TA Ticket.

5. Complete the Create TA Ticket fields.

6. Click View Products.

7. In the Products List, select the product that is causing the problem.

8. Complete the Create Support Ticket fields.

9. Select Finish to complete the support ticket.

Fortinet customers who would like to submit a customer service ticket, DOA ticket, RMA ticket, or FortiGuard service ticket should use the Ticket Wizard and complete the following steps:

1. Log in to the support website at the following address with the account credentials used when the account was created:
   https://support.fortinet.com

2. Navigate to the top menu, click Assistance and select Create a Ticket from the drop down menu.

3. Select a ticket type and complete the remaining steps in the Ticket Wizard.

4. Select Finish to complete the ticket.

Following up on online tickets

Perform the following steps to follow up on an existing issue.

Partners should log into the following web site:
http://partners.fortinet.com

Customers should log into the following site:
http://support.fortinet.com.

1. Log in with the account credentials used when the account was created.

2. Navigate to the top menu, click Assistance, and select Manage Tickets.

3. Use the search field on the View Tickets page to locate the tickets assigned to the account.

4. Select the appropriate ticket number. Closed tickets cannot be updated. A new ticket must be submitted if it concerns the same problem.

5. Add a New Comment or Attachment.

6. Click Submit when complete.

Note	Every web ticket update triggers a notification to the ticket owner, or ticket queue supervisor.

11.5.2 Telephoning a technical support center

The Fortinet Technical Assistance Centers can also be contacted by phone.

Call Fortinet Support Center at 1-408-486-7899 (international) or go to http://www.fortinet.com/support/contact_support.html and select your country from the drop-down list for local contact number.

11.6 Assisting technical support

The more information that can be provided to Fortinet technical support, the better they can assist in resolving the issue. Every new support request should contain the following information:

▪ A valid contact name, phone number, and email address.

▪ A clear and accurate problem description.

▪ A detailed network diagram with complete IP address schema.

- The configuration file, software version, and build number of the Fortinet device.

- Additional log files such as Antivirus log, Attack log, Event log, Debug log or similar information to include in the ticket as an attachment. If a third-party product is involved, for example, email server, FTP server, router, or switch, please provide the information on its software revision version, configuration, and brand name.

11.7 Support priority levels

Fortinet technical support assigns the following priority levels to support cases:

11.7.1 Priority 1

This Critical priority is assigned to support cases in which:

- The network or system is down causing customers to experience a total loss of service.

- There are continuous or frequent instabilities affecting traffic-handling capability on a significant portion of the network.

- There is a loss of connectivity or isolation to a significant portion of the network.

- This issue has created a hazard or an emergency.

11.7.2 Priority 2

This Major priority is assigned to support cases in which:

- The network or system event is causing intermittent impact to end customers.

- There is a loss of redundancy.

- There is a loss of routine administrative or diagnostic capability.

- There is an inability to deploy a key feature or function.

- There is a partial loss of service due to a failed hardware component.

11.7.3 Priority 3

This Medium priority is assigned to support cases in which:

- The network event is causing only limited impact to end customers.

- Issues seen in a test or pre-production environment exist that would normally cause adverse impact to a production network.

- The customer is making time sensitive information requests.

- There is a successful workaround in place for a higher priority issue.

11.7.4 Priority 4

This Minor priority is assigned to support cases in which:

- The customer is making information requests and asking standard questions about the configuration or functionality of equipment.

Customers must report Priority 1 and 2 issues by phone directly to the Fortinet EMEA Support Center.

For lower priority issues, you may submit an assistance request (ticket) via the web system.

The web ticket system also provides a global overview of all ongoing support requests.

11.8 Return material authorization process

In some cases hardware issues are experienced and a replacement unit must be sent. This is referred to as a Return Material Authorization (RMA). In these cases or RMAs, the support contract must be moved to the new device. Customers can move the support contract from the failing production unit to the new device through the support web site.

To move the support contract to a new device

1. Log in to the support web site with the credentials indicated when the account was created.

2. From Manage Products, locate the serial number of the defective unit from the list of devices displayed for the account. The Product Info for the selected device will be displayed.

3. In the left side bar under the Assistance section, select RMA Transfer.

4. Enter the Original Serial Number of the original device, enter the New Serial Number, and click Replace to complete the transfer.

This will transfer the support contract from the defective unit to the new unit with the serial number provided.

Business
Services   orange

References

[1] FortiGate 5.0.6 Online Help, February 2014.
   http://docs.fortinet.com/d/fortigate-506-online-help