# FortiOS™ Handbook

## Troubleshooting for FortiOS 5.0

FortiOS™ Handbook - Troubleshooting for FortiOS 5.0

March 10, 2014

01-504-129304-20130814



| | |
|---|---|
| Technical Documentation | docs.fortinet.com |
| Knowledge Base | kb.fortinet.com |
| Customer Service & Support | support.fortinet.com |
| Training Services | training.fortinet.com |
| FortiGuard | fortiguard.com |
| Document Feedback | techdocs@fortinet.com |

# Contents

# Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

This guide is intended for administrators who need guidance on different network needs and information on basic and advanced troubleshooting.

This chapter contains the following topics:



## Before you begin

Before you begin using this guide, take a moment to verify the following:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.

While using the instructions in this guide, note that:

- Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

## How this guide is organized

This handbook chapter describes concepts of troubleshooting and solving issues that may occur with FortiGate units.

This guide contains the following chapters:

Life of a Packet explains the different layers and modules a packet goes through in FortiOS, including the order of operations.

Verifying FortiGate admin access security explains how to verify and configure administrative access.

Troubleshooting resources walks you through Fortinet's resources for troubleshooting.

Troubleshooting tools describes some of the basic commands and parts of FortiOS that can help you with troubleshooting.

Troubleshooting methodologies walks you through best practice concepts of FortiOS troubleshooting.

Technical Support Organization Overview describes how Fortinet Support operates, what they will need from you if you contact them, and what you can expect in general.

Common questions answers most of the common questions.

# 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.

This section contains the following topics:



## 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 packed 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.

## 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 recieved.

## 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.

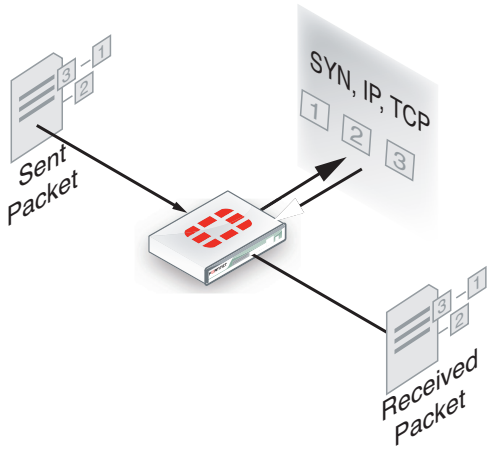
## Differences between connections and sessions

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.

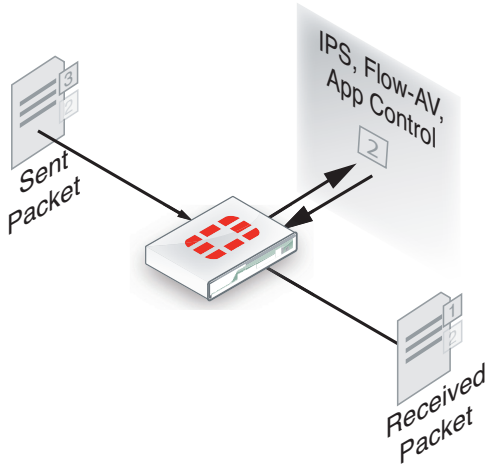
**Figure 1:** Stateful inspection of packets through the FortiGate unit




## 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.

**Figure 2:** Flow inspection of packets through the FortiGate unit

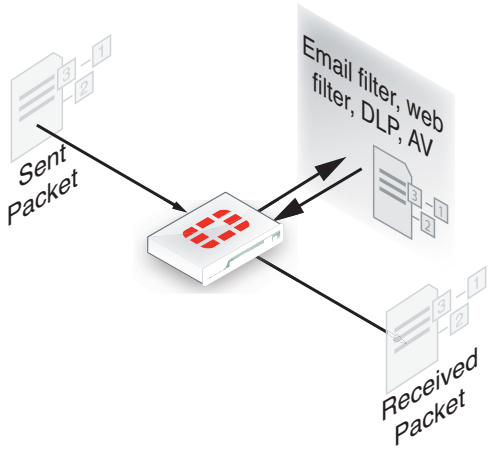



Flow inspection typically requires less processing than proxy inspection, and therefore flow antivirus, web filtering, and DLP inspection performance can be better than proxy inspection performance. However, some threats can only be detected when a complete copy of the payload (for example a complete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

## 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.

**Figure 3:** Proxy inspection of packets through the FortiGate unit




## 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.

**Table 1:** Inspection methods comparison

| 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 |

**Table 1:** Inspection methods comparison

| Feature | Stateful | Flow | Proxy |
|---|---|---|---|
| Application control | | yes | |
| IPS | | yes | |
| Delay in traffic | | no | small |
| Reconstruct entire content | | no | yes |

## 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.

**Table 2: FortiOS security functions and security layers**

| 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 |

## 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 4 on page 13 is a high level view of the packet's journey.

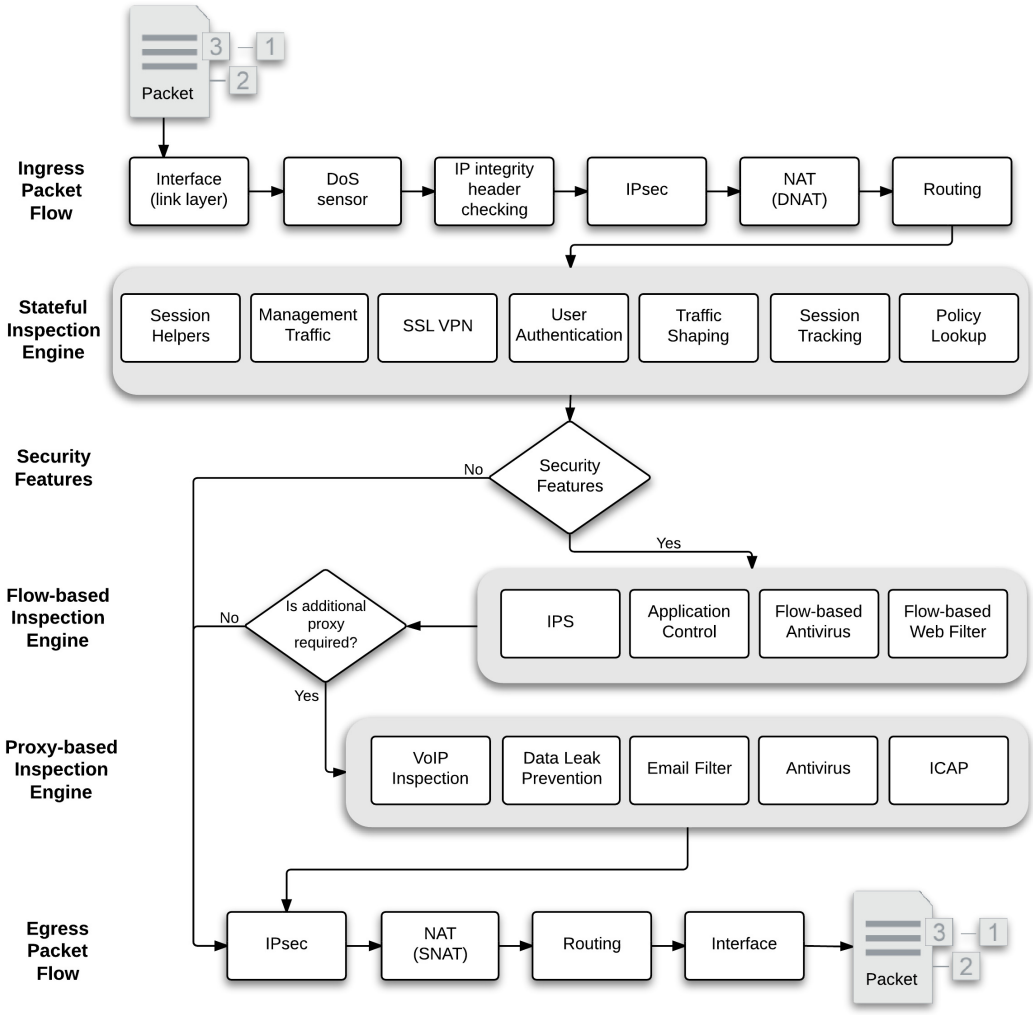
The description following is a high-level description of these steps as a packet enters the FortiGate unit towards its destination on the internal network. Similar steps occur for outbound traffic.

## Packet inspection (Ingress)

In Figure 4 on page 13, 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

**Figure 4:** Packet flow process



## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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 FortiAnalyzer 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.

## 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.

## 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.

## 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.

### 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.

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

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

### 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.

### 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.

### 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.

### Routing

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

### Egress

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

## 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

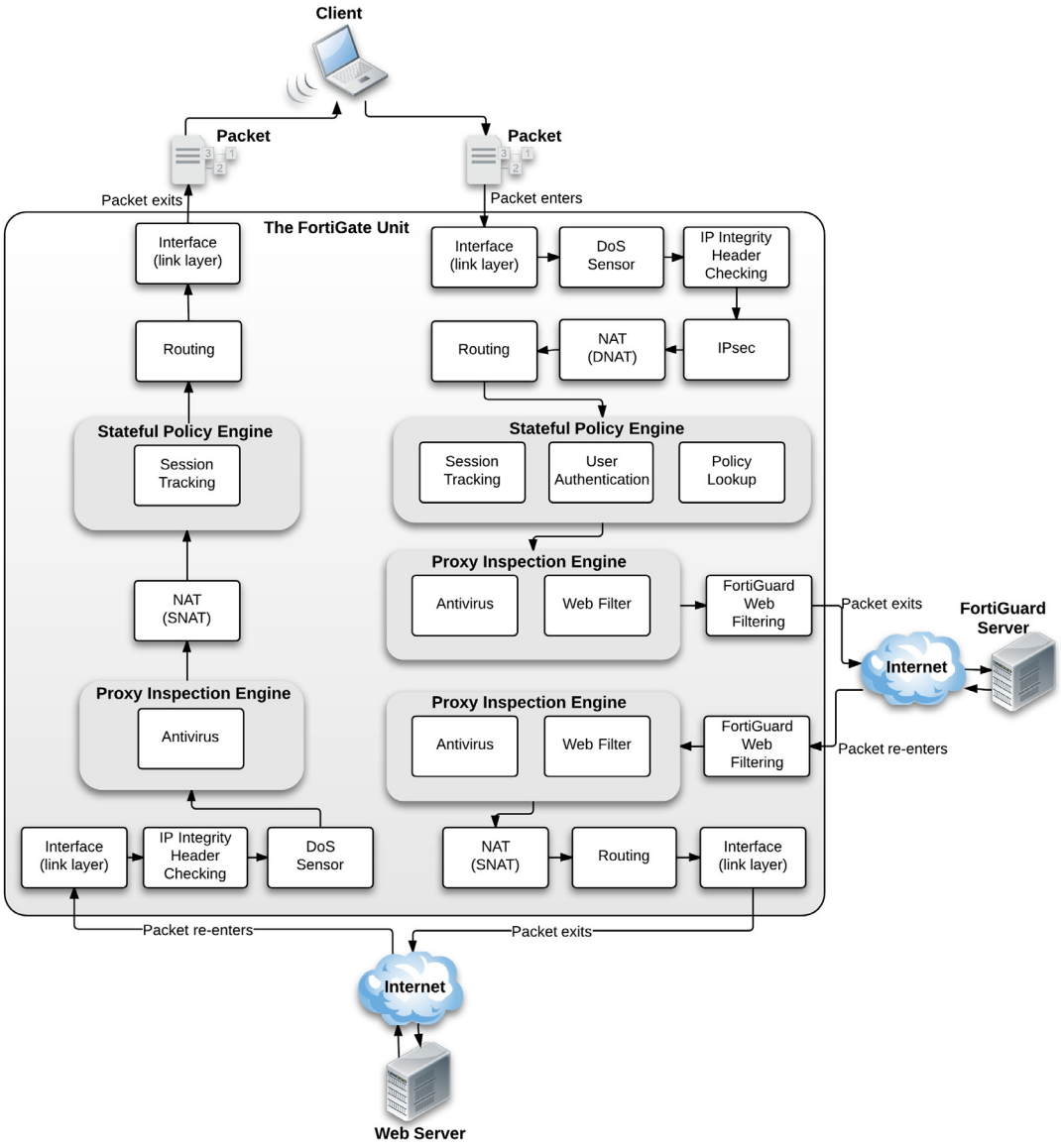
   **2.1** Link level CRC and packet size checking.
3. IP integrity header checking.
4. DoS sensor.
5. Proxy inspection

   **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

This process is illustrated in Figure 5.

**Figure 5:** Client/server connection




## 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

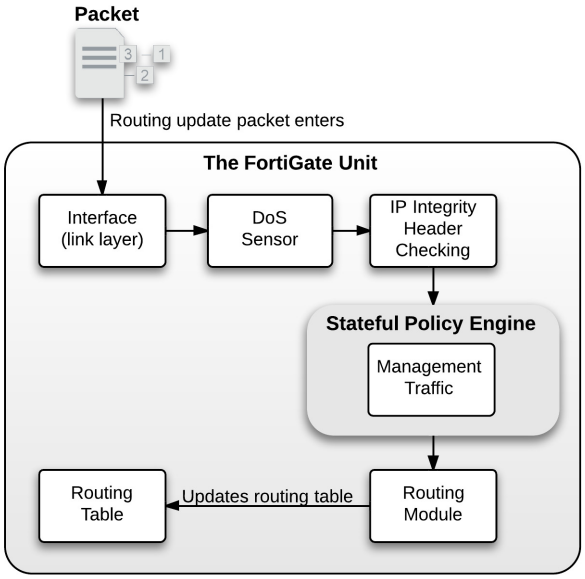
   **2.1** Link level CRC and packet size checking. If the size is correct, the packet continues, otherwise it is dropped.
3. DoS sensor - checks are done to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking, verifying the IP header length, version and checksums.
5. Stateful policy engine

   **5.1** Management traffic (local traffic)

6. Routing module
   **6.1** Update routing table

Figure 6 illustrates the process steps.

**Figure 6:** Routing table update




## 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

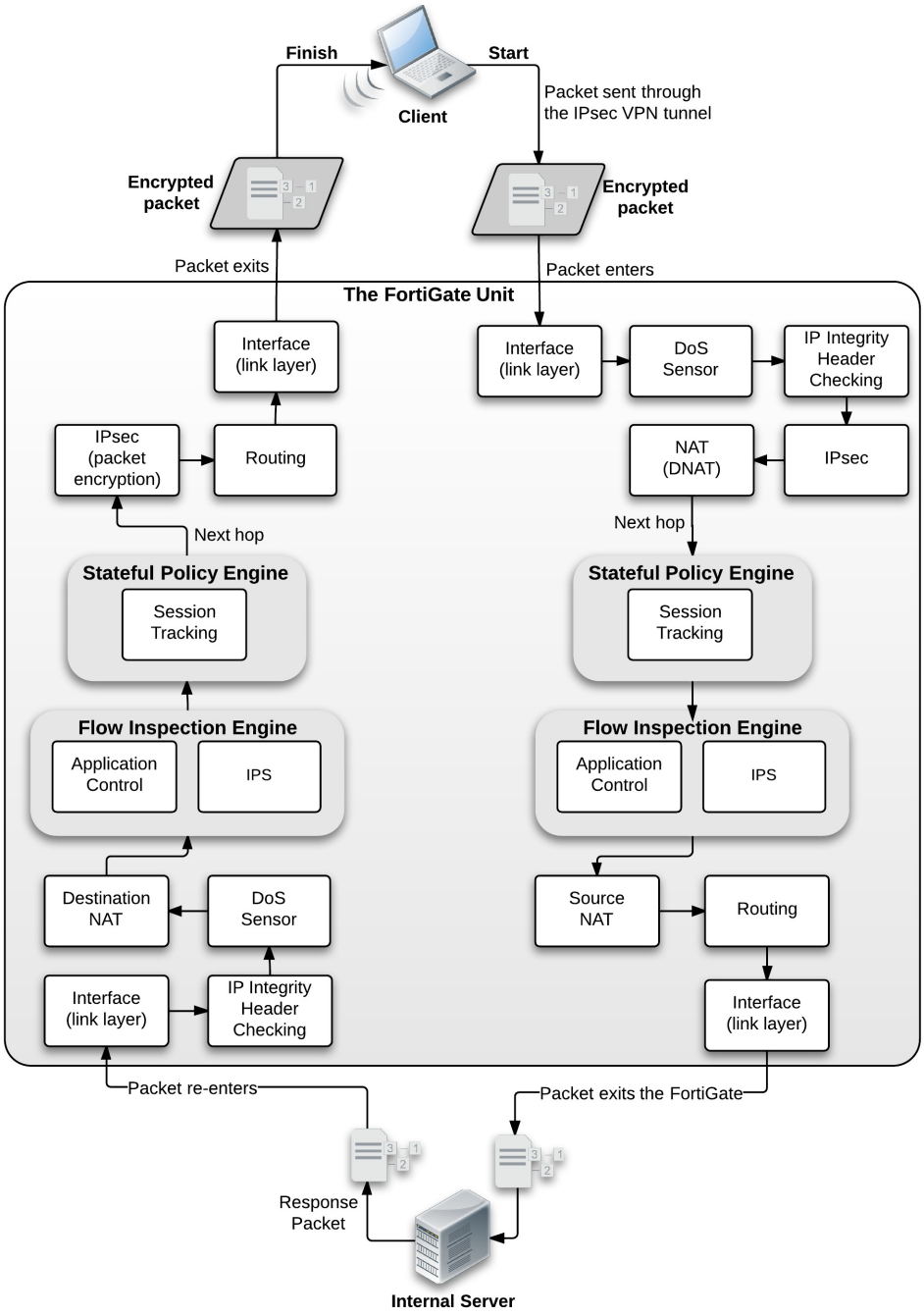
11. Interface transmission to network
12. Packet forwarded to internal server

**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

Figure 7 illustrates the process.

**Figure 7:** Dialup IPsec with application control



# 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.

- Install the FortiGate unit in a physically secure location
- Add new administrator accounts
- Change the admin account name and limit access to this account
- Only allow administrative access to the external interface when needed
- When enabling remote access, configure Trusted Hosts and Two-factor Authentication
- Change the default administrative port to a non-standard port
- Enable Password Policy
- Maintain short login timeouts
- Modify administrator account Lockout Duration and Threshold values
- Disable auto installation via USB
- Auditing and Logging

## 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.

## 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*.

## 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.

## 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
```

# 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.

## 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.

## 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*.

## 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.

## 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.

## 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
```

## 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:

### 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
```

### 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.

## 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
```

## 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.

# 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

## 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

# 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.

This section contains the following topics:



## 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:



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.

### 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
```

## 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
```

## 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. |
| `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. |

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 |
| 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 |

## 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.

**Table 3:** Possible hardware errors and 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 packed 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. |

**Table 3:** Possible hardware errors and meanings

| Field | Definition |
|---|---|
| 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. |

## 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
```

## 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 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 | 3,584 | 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.

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
```

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:

**Table 4:**

| 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. |

## 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.

## 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*.

## 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
```

`diag debug flow` output is recorded as event log messages and are sent to a FortiAnalyzer 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."
```

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."
```

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"
```

## 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.

| 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:

```
'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.<br>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.<br>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<br>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.<br>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).<br>Separate multiple vlans with commas. |
| **Protocol** | Enter one or more protocol. Separate multiple protocol with commas. Enter a 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.

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

Run the following commands:

```
diag npu np2 fastpafth 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.

## 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>
```

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 FortiAnalyzer 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
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 |

## 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.

## 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>`).

## 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:

**Table 5:**

| 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 |

## 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.

**Table 6:**

| 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 |

## 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

- Troubleshooting process for FortiGuard updates
- FortiGuard server settings
- FortiGuard URL rating

### 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.

## 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. This includes

- Displaying the server list
- Sorting the server list
- Calculating weight

### 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

# 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.

This section contains the following topics:



## 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.

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

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

| | |
|---|---|
| `get system status` | Displays versions of firmware and FortiGuard engines, and other system information. |
| `get system performance status` | Displays CPU and memory states, average network usage, average sessions and session setup rate, virus caught, IPS attacks blocked, and uptime. |
| `get hardware memory` | Displays informations about memory |

| | |
|---|---|
| `get system session status` | Displays total number of sessions |
| `get router info routing-table all` | Displays all the routes in the routing table including their type, source, and other useful data. |
| `get ips session` | Displays memory used and max available to IPS as well and counts. |
| `get webfilter ftgd-statistics` | Displays list of FortiGuard related counts of status, errors, and other data. |
| `diagnose firewall statistic show` | Displays the amount of network traffic broken down into categories such as email, VoIP, TCP, UDP, IM, Gaming, P2P, and Streaming. |
| `diag system session list` | Displays current detailed sessions list |
| `show system dns` | Displays configured DNS servers |
| `diag sys ntp status` | Displays informations about ntp servers |

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

## 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 awhile 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.

## 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.

## 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.

### 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.

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.

For additional information about contacting Fortinet Customer Support, see “Technical Support Organization Overview” on page 62.

All of this is your troubleshooting plan.

## 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.

## 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.

## 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, its time to contact Fortinet Customer Support for assistance.

For more information, see “Technical Support Organization Overview” on page 62.

# 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.

This section contains the following topics:



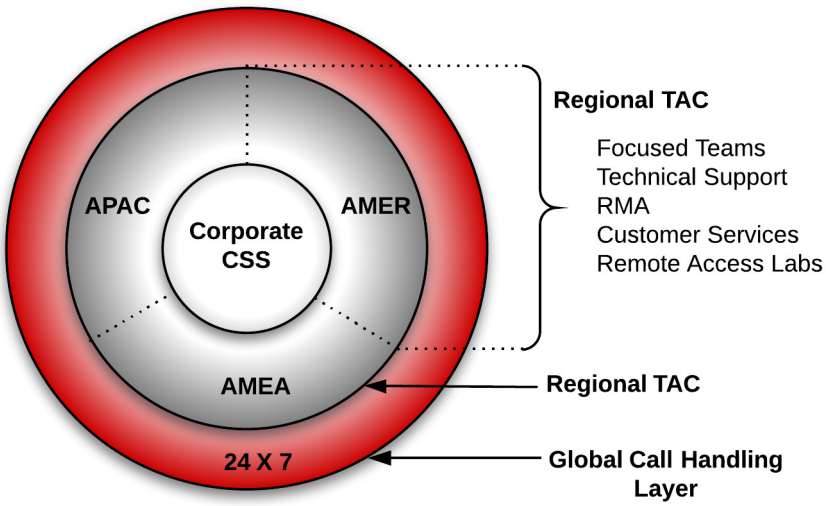
## Fortinet Global Customer Services Organization

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.

**Figure 8:** Fortinet regions and TAC



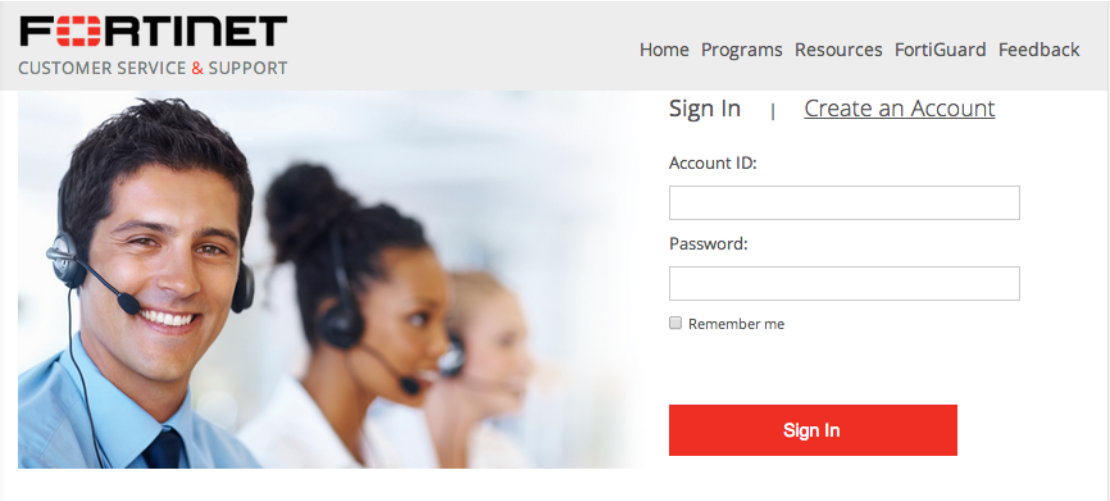
## Creating an account

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/

**Figure 9:** Customer service and support home page



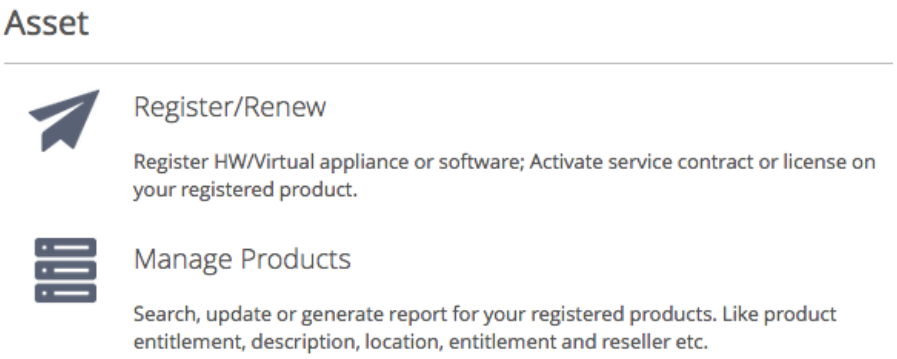

Once the support account has been created, product details can be provided by going to the *Product Register/Renew* and *Manage Product* buttons displayed on the home page. Alternately, the product registration can be completed at a later time.

## 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.

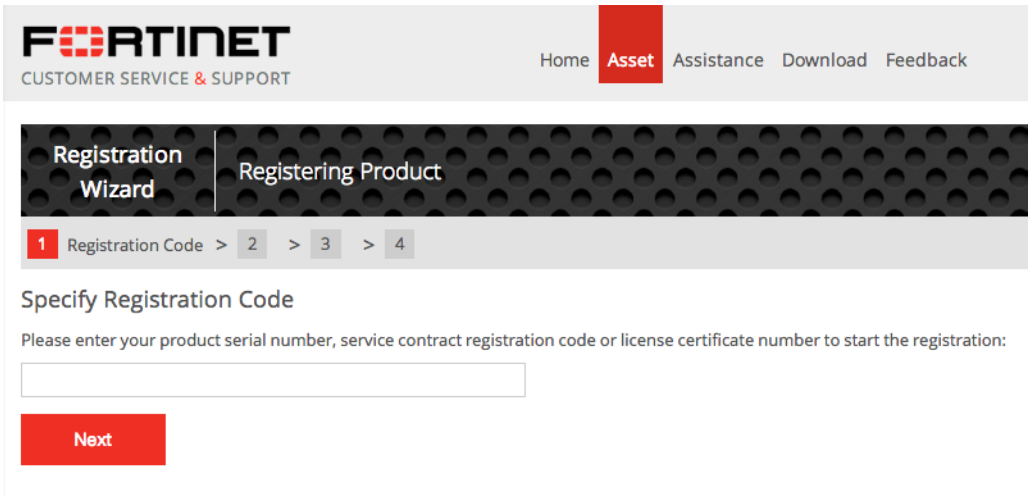
   **Figure 10:**Register/Renew and Manage Products menu




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.

**Figure 11:**Adding a product to a support account




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.

**Figure 12:**Registration wizard


# 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

## 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.

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

### 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.

## 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.

## Support priority levels

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

### 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.

### 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.

### 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.

### 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.

## 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.

# Common questions

The general troubleshooting tips include, and can help answer the following questions.

### How to check hardware connections

Are all the cables and interfaces connected properly?

Is the LED for the interface green?

### How to check FortiOS network settings

If you are having problems connecting to the management interface, is your protocol enabled on the interface for administrative access?

Is there an IP address on the interface?

### How to check CPU and memory resources

Is your CPU running at almost 100 percent usage?

Are you running low on memory?

### How to check modem status

Is the modem connected?

Are there PPP issues?

### How to run ping and traceroute

Are you experiencing complete packet loss?

### How to check the logs

Do you need to identify a problem?

### How to verify the contents of the routing table (in NAT mode)

Are there routes in the routing table for default and static routes?

Do all connected subnets have a route in the routing table?

Does a route wrongly have a higher priority than it should?

### How to verify the correct route is being used

Has the traffic been routed correctly?

### How to verify the correct firewall policy is being used

Is the correct firewall policy applied to the expected traffic?

### How to check the bridging information in Transparent mode

Are you having problems in Transparent mode?

### How to check number of sessions used by UTM proxy

Have you reached the maximum number of sessions for a protocol?

Are new sessions failing to start for a certain protocol?

### How to examine the firewall session list

Are there active firewall sessions?

### How to check wireless information

Is the wireless network functioning properly?

### How to verify FortiGuard connectivity

Is the FortiGate unit communicating properly with FortiGuard?

### How to perform a sniffer trace (CLI and Packet Capture)

Is traffic entering the FortiGate unit and does it arrive on the expected interface?

Is the ARP resolution correct for the next-hop destination?

Is the traffic exiting the FortiGate unit to the destination as expected?

Is the traffic being sent back to the originator?

### How to debug the packet flow

Is the traffic entering or leaving the FortiGate unit as expected?

## How to check hardware connections

If there is no traffic flowing from the FortiGate unit, it may be a hardware problem.

To check hardware connections:

- Ensure the network cables are properly plugged into the interfaces.
- Ensure there are connection lights for the network cables on the unit.
- Change the cable if the cable or its connector are damaged or you are unsure about the cable's type or quality—such as straight through or crossover, or possibly exposed wires at the connector.
- Connect the FortiGate unit to different hardware.
- Ensure the link status is set to *Up* for the interface, (see *Network* > *Interface* > *Status)*. The link status is based on the physical connection and cannot be set in FortiOS.

If any of these solve the problem, it was a hardware connection problem. You should still perform some basic software connectivity tests to ensure complete connectivity. It might also be that the interface is disabled, or has its *Administrative Status* set to *Down*.

**To enable an interface - web-based manager**

1. Using the web-based management interface, go to *System* > *Network* > *Interface*.
2. Select and edit the interface to enable, such as *port1*.
3. Find *Administrative Status* at the bottom of the screen, and select *Up*.
4. Select *Apply*.

**To enable an interface - CLI**

```
config system interface
  edit port1
    set status enable
  next
end
```

## How to check FortiOS network settings

FortiOS network settings are present in both the web-based manager interface and the CLI. The following information includes troubleshooting and best practice information. The network settings include:

- Interface settings
- DNS settings
- DHCP Server settings

### Interface settings

If you can access the FortiGate unit with the management cable only, the first step is to display the interface settings. To display the settings for the internal interface, use the following CLI command:

```
FGT# show system interface <Interface_mane>
```

For a complete listing of all the possible interface settings, use the following CLI command:

```
config system interface
  edit <Interface_name>
  get
end
```

Check the interface settings to ensure they are not preventing traffic. Specific things to check include (only the web-based manager names are shown, CLI names may vary slightly):

- **Link Status —** *Down* until a valid cable is plugged into this interface, after which it will be *Up*. The Link Status is shown physically by the connection LED for the interface. If it lights up green, it is a good connection. If Link Status is *Down*, the interface does not work. Link Status is also displayed on the *System* > *Network* > *Interface* screen by default.
- **Addressing mode —** Do not use *DHCP* if you don't have a DHCP server —you will not be able to logon to an interface in DHCP mode as it will not have an IP address.
- **IP/Netmask —** An interface needs an IP address to be able to connect to other devices. Ensure there is a valid IP address in this field. The one exception is if *DHCP* is enabled for this interface to get its IP address from an external DHCP server.
- **IPv6 address —** The same protocol must be used by both ends to complete the connection. Ensure both this interface and the remote connection are both using IPv4 or both using IPv6 addressing.
- **Administrative access —** If no protocols are selected, you will have to use the local management cable to connect to the unit. If you are using IPv6, configure the IPv6 administrative access protocols.
- **Administrative status —** Set to *Up* or the interface will not work.

## DNS settings

While this section is not complicated, many networking problems can be traced back to DNS problems. Things to check in this area include:

- Are there values for both primary and secondary entries?
- Is the local domain name correct?
- Are you using IPv6 addressing? If so, are the IPv6 DNS settings correct?
- Are you using Dynamic DNS (DDNS)? If so, is it using the correct server, credentials, and interface?
- Can you contact both DNS servers to verify the servers are operational?
- If an interface addressing mode is set to DHCP and is set to override the internal DNS, is that interface receiving a valid DNS entry from the DHCP server? Is it a reasonable address and can it be contacted to verify it's operational?
- Are there any DENY security policies that need to allow DNS?
- Can any internal device perform a successful traceroute to a location using the FQDN? See Traceroute.

### DHCP Server settings

DHCP Servers are common on internal and wireless networks. If the DHCP server is not configured properly it can cause problems. Things to check in this area include:

- Is the DHCP server entry set to *Relay*? If so, verify there is another DHCP server to which requests can be relayed. Otherwise, it should be set to *Server*.
- Is the DHCP server enabled?
- Does this DHCP server use a valid range of IP addresses? Are those addresses in use by other devices? If one or more devices are using IP addresses in this range, you can use the IP reservation feature to ensure the DHCP server does not use these addresses.
- Is there a gateway entry? Include a gateway entry to ensure clients of this server have a default route.
- Is the system DNS setting being used? The best practice is to avoid confusion by using the system DNS whenever possible. However, the option to specify up to three custom DNS servers is available, and all three entries should be used for redundancy.

There are some situations, such as a new wireless interface, or during the initial FortiGate unit configuration, where interfaces override the system DNS entries. When this happens, it often shows up as intermittent Internet connectivity. To fix the problem, go to *System* > *Network* > *DNS* and ensure to enable *Use FortiGuard Servers*.

## How to check CPU and memory resources

System resources are shared and a number of processes run simultaneously on the FortiGate unit. If one of these processes consumes nearly all the resources.

A quick way to monitor CPU and memory usage is on the System Dashboard using the *System Resources* widgets. They have both a visual gauge displayed to show you the usage.

To check the system resources on your FortiGate unit, run the following CLI command:

```
FGT# get system performance status
```

This command provides a quick and easy snapshot of the FortiGate.

The first line of output shows the CPU usage by category. A FortiGate that is doing nothing will look like:

```
CPU states: 0% user 0% system 0% nice 100% idle
```

However, if your network is running slow you might see something like:

```
CPU states: 1% user 98% system 0% nice 1% idle
```

This line shows that all the CPU is used up by system processes. Normally this should not happen as it shows the FortiGate is overloaded for some reason. If you see this overloading, you should investigate farther as it's possible a process, such as scanunitid, is using all the resources to scan traffic, in which case you need to reduce the amount of traffic being scanned by blocking unwanted protocols, configuring more security policies to limit scanning to certain protocols, or similar actions. It is also possible that a hacker has gained access to your network and is overloading it with malicious activity such as running a spam server or using zombie PCs to attack other networks on the Internet. You can get additional CPU related information with the CLI command `get system performance top`. This command shows you all the top processes running on the FortiGate unit (names on the left) and their CPU usage. If a process is using most of the CPU cycles, investigate it to determine if it's normal activity.

The second line of output from `get system performance status` shows the memory usage. Memory usage should not exceed 90 percent. If memory is too full, some processes will not be able to function properly. For example, if the system is running low on memory, antivirus

scanning will go into failopen mode where it will start dropping connections or bypass the antivirus system.

The other lines of output, such as average network usage, average session setup rate, viruses caught, and IPS attacks blocked can also help you determine why system resource usage it high. For example, if network usage is high it will result in high traffic processing on the FortiGate, or if the session setup rate is very low or zero the proxy may be overloaded and not able to do its job.

### How to troubleshoot high memory usage

As with any system, FortiOS has a finite set of hardware resources such as memory and all the running processes share that memory. Depending on their workload, each process will use more or less as needed, usually more in high traffic situations. If some processes use all the available memory, other processes will have no memory available and not be able to function.

When high memory usage happens, you may experience services that appear to freeze up and connections are lost or new connections are refused.

If you are seeing high memory usage in the *System Resources* widget, it could mean that the unit is dealing with high traffic volume, which may be causing the problem, or it could be when the unit is dealing with connection pool limits affecting a single proxy. If the unit is receiving large volumes of traffic on a specific proxy, it is possible that the unit will exceed the connection pool limit. If the number of free connections within a proxy connection pool reaches zero, problems may occur.

Use the following CLI command, which uses the antivirus failopen feature. Setting it to idledrop will drop connections based on the clients that have the most connections open. This helps to determine the behavior of the FortiGate antivirus system if it becomes overloaded in high traffic.

```
config system global
  set av-failopen idledrop
end
```

Use the following CLI command, which gives you information about current memory usage:

```
diagnose hardware sysinfo memory
```

**Sample output:**

```
        total:    used: free:  shared: buffers:  cached: shm:
Mem:  2074185728 756936704 1317249024 0 20701184 194555904
   161046528
Swap:        0        0        0
MemTotal:      2025572 kB
MemFree:       1286376 kB
MemShared:           0 kB
Buffers:         20216 kB
Cached:         189996 kB
SwapCached:          0 kB
Active:          56644 kB
Inactive:       153648 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:      2025572 kB
LowFree:       1286376 kB
SwapTotal:           0 kB
SwapFree:            0 kB
```

## How to troubleshoot high CPU usage

FortiOS has many features. If many of them are used at the same time, it can quickly use up all the CPU resources. When this happens, you will experience connection related problems stemming from the FortiOS unit trying to manage its workload by refusing new connections, or even more aggressive methods.

Some examples of features that are CPU intensive are VPN high level encryption, having all traffic undergo all possible scanning, logging all traffic, and packets, and dashboard widgets that frequently update their data.

1. **Determine how high the CPU usage is currently.**

   There are two main ways to do this. The easiest is to go to *System* > *Dashboard* > *Status* and look at the resource monitor. This is a dial gauge that displays a percentage use for the CPU. If its at the red-line, you should take action. The other method is to use the Dashboard CLI widget to enter `diag sys top`.

   Sample output:

```
Run Time:  11 days, 23 hours and 36 minutes
0U, 0S, 98I; 1977T, 758F, 180KF
          newcli      286      R       0.1     0.8
       ipsengine       78      S <     0.0     3.1
       ipsengine       64      S <     0.0     3.0
       ipsengine       77      S <     0.0     3.0
       ipsengine       68      S <     0.0     2.9
       ipsengine       66      S <     0.0     2.9
       ipsengine       79      S <     0.0     2.9
       scanunitd      133      S <     0.0     1.8
         pyfcgid      267      S       0.0     1.8
         pyfcgid      269      S       0.0     1.7
         pyfcgid      268      S       0.0     1.6
          httpsd      139      S       0.0     1.6
         pyfcgid      266      S       0.0     1.5
       scanunitd      131      S <     0.0     1.4
       scanunitd      132      S <     0.0     1.4
     proxyworker       90      S       0.0     1.3
         cmdbsvr       43      S       0.0     1.1
     proxyworker       91      S       0.0     1.1
         miglogd       55      S       0.0     1.1
          httpsd      135      S       0.0     1.0
```

Where the codes displayed on the second output line mean the following:

- `U` is % of user space applications using CPU. In the example, `0U` means 0% of the user space applications are using CPU.
- `S` is % of system processes (or kernel processes) using CPU. In the example, `0S` means 0% of the system processes are using the CPU.
- `I` is % of idle CPU. In the example, `98I` means the CPU is 98% idle.
- `T` is the total FortiOS system memory in Mb. In the example, `1977T` means there are 1977 Mb of system memory.
- `F` is free memory in Mb. In the example, `758F` means there is 758 Mb of free memory.
- `KF` is the total shared memory pages used. In the example, `180KF` means the system is using 180 shared memory pages.

Each additional line of the command output displays information for each of the processes running on the FortiGate unit. For example, the third line of the output is:

```
newcli      286      R       0.1     0.8
```

Where:

- `newcli` is the process name. Other process names can include `ipsengine`, `sshd`, `cmdbsrv`, `httpsd`, `scanunitd`, and `miglogd`.
- `286` is the process ID. The process ID can be any number.
- `R` is the current state of the process. The process state can be:
  - `R` running
  - `S` sleep
  - `Z` zombie
  - `D` disk sleep.
- `0.1` is the amount of CPU that the process is using. CPU usage can range from 0.0 for a process that is sleeping to higher values for a process that is taking a lot of CPU time.
- `0.8` is the amount of memory that the process is using. Memory usage can range from 0.1 to 5.5 and higher.

Enter the following single-key commands when `diagnose sys top` is running:

- Press `q` to quit and return to the normal CLI prompt.
- Press `p` to sort the processes by the amount of CPU that the processes are using.
- Press `m` to sort the processes by the amount of memory that the processes are using.

2. **Determine what features are using most of the CPU resources.**

   There is a command in the CLI to let you see the top few processes currently running that use the most CPU resources. The CLI command `get system performance top` outputs a table of information. You are interested in the second most right column, CPU usage by percentage. If the top few entries are using most of the CPU, note which processes they are and investigate those features to try and reduce their CPU load. Some examples of processes you will see include:

   - `ipsengine` — the IPS engine that scans traffic for intrusions
   - `scanunitd` — antivirus scanner
   - `httpsd` — secure HTTP
   - `iked` — internet key exchange (IKE) in use with IPsec VPN tunnels
   - `newcli` — active whenever you are accessing the CLI
   - `sshd` — there are active secure socket connections
   - `cmdbsrv` — the command database server application

   Go to the features that are at the top of the list and look for evidence of them overusing the CPU. Generally the monitor for a feature is a good place to start.

3. **Check for unnecessary CPU "wasters".**

   These are some best practises that will reduce your CPU usage, even if you are not experiencing high CPU usage. Note that if you require a feature this section tells you to turn off, ignore it.

   - Use hardware acceleration wherever possible to offload tasks from the CPU. Offloading tasks such as encryption frees up the CPU for other tasks.
   - Avoid the use of GUI widgets that require computing cycles, such as the Top Sessions widget. These widgets are constantly polling the system for their information, which uses CPU and other resources.
   - Schedule antivirus, IPS, and firmware updates during off peak hours. Usually these don't consume CPU resources but they can disrupt normal operation.
   - Check the log levels and which events are being logged. This is the severity of the messages that are recorded. Consider going up one level to reduce the amount of logging. Also if there are events you do not need to monitor, remove them from the list.
   - Log to FortiCloud instead of memory or Disk. Logging to memory quickly uses up resources. Logging to local disk will impact overall performance and reduce the lifetime of the unit. Fortinet recommends logging to FortiCloud which doesn't use much CPU.
   - If the disk is almost full, transfer the logs or data off the disk to free up space. When a disk is almost full it consumes a lot of resources to find the free space and organize the files.
   - If you have packet logging enabled, consider disabling it. When it's enabled it records every packet that comes through that policy.
   - Halt all sniffers and traces.
   - Ensure you are not scanning traffic twice. If traffic enters the FortiGate unit on one interface, goes out another, and then comes back in again that traffic does not need to be rescanned. Doing so is a waste of resources. However, ensure that traffic truly is being scanned once.
   - Reduce the session timers to close unused sessions faster. To do this in the CLI enter the following commands and values. These values reduce the values from defaults. Note that `tcp-timewait` has 10 seconds added by the system by default.

     ```
     config system global
       set tcp-halfclose-timer 30
       set tcp-halfopen-timer 30
       set tcp-timewait-timer 0
     ```

```
    set udp-idle-timer 60
  end
```

- Enable only features that you need under *System* > *Config* > *Features*.

4. **When CPU usage is under control, use SNMP to monitor CPU usage. Alternately, use logging to record CPU and memory usage every 5 minutes.**

   Once things are back to normal, you should set up a warning system to alert you of future CPU overusage. A common method to do this is with SNMP. SNMP monitors many values on the FortiOS and allows you to set high water marks that will generate events. You run an application on your computer to watch for and record these events. Go to *System* > *Config* > *SNMP* to enable and configure an SNMP community. If this method is too complicated, you can use the *System Resources* widget to record CPU usage. However, this method will not alert you to problems - it will just record them as they happen.

## How to check modem status

Sometimes the modem may not work properly, or the unit may not be detecting the modem. Use the following diagnostic commands to help you troubleshoot issues with the modem.

```
diagnose sys modem {cmd | com | detect | history | wireless-id}
```

You should always run the following diagnose command after inserting the USB modem into the unit:

```
diagnose sys modem detect
```

You can view the modem configuration by using the `get system modem` command. You can also view the modem's vendor identification as well as the custom product identification number from the information output from the `get system modem` command.

When the modem is not being detected by the unit, use the following command:

```
diagnose sys modem wireles-id
```

When there are connectivity issues, use the following to help you resolve them:

- `diag debug enable` – activates the debug on the console
- `diag debug application modemd` – dumps communication between the modem and the unit.
- `diag debug application pppd` – dumps the PPP negotiating messages.
- `execute modem dial` – displays modem debug output.

The modem diagnose output should not contain any error on the way to initializing. You should also verify the number that is used to dial with your ISP.

## How to run ping and traceroute

Ping and traceroute are useful tools in network troubleshooting. Alone, either one can determine network connectivity between two points. However, ping can be used to generate simple network traffic to view with diagnose commands on the FortiGate unit. This combination can be very powerful when locating network problems.

In addition to their normal uses, ping and traceroute can tell you if your computer or network device has access to a domain name server (DNS). While both tools can use IP addresses alone, they can also use domain names for devices. This is an added troubleshooting feature

that can be useful in determining why particular services, such as email or web browsing, may not be working properly.

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

Both ping and traceroute require particular ports to be open on firewalls, or else they cannot function. Since you typically use these tools to troubleshoot, you can allow them in the security policies and on interfaces only when you need them, and otherwise keep the ports disabled for added security.

## Ping

The ping command sends a very small packet to the destination, and waits for a response. The response has a timer that may expire, indicating the destination is unreachable. The behavior of ping is very much like a sonar ping from a submarine, where the command gets its name.

Ping is part of Layer-3 on the 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 (such as Ping of Death or a smurf attack), or by an attacker to find active locations on the network. By default, FortiGate units have ping enabled while broadcast-forward is disabled on the external interface.

### What ping can tell you

Beyond the basic connectivity information, ping can tell 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 there is some packet loss detected, you should investigate the following:

- Possible ECMP, split horizon, or network loops.
- Cabling to ensure no loose connections.
- Verify which security policy was used (use the packet count column on the *Policy & Objects* > *Policy* page).

If there is total packet loss, you should investigate the following:

- **Hardware —** ensure cabling is correct, and all equipment between the two locations is accounted for.
- **Addresses and routes —** ensure all IP addresses and routing information along the route is configured as expected.
- **Firewalls —** ensure all firewalls, including FortiGate unit security policies allow PING to pass through.

### How to use ping

Ping syntax is the same for nearly every type of system on a network.

### To ping from a FortiGate unit

1. Connect to the CLI either through telnet or through the CLI widget on the web-based manager dashboard.
2. Enter `exec ping 10.11.101.101` to send 5 ping packets to the destination IP address. There are no options for this command.

   **Sample output:**

   ```
   Head_Office_620b # exec ping 10.11.101.101
   ```

```
PING 10.11.101.101 (10.11.101.101): 56 data bytes
64 bytes from 10.11.101.101: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 10.11.101.101: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=4 ttl=255 time=0.2 ms

--- 10.11.101.101 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.3 ms
```

**To ping from an MS 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 `ping 10.11.101.100` to ping the default internal interface of the FortiGate unit with four packets.

   Other options include:
   - `-t` to send packets until you press “Control-C”
   - `-a` to resolve addresses to domain names where possible
   - `-n X` to send X ping packets and stop

   **Sample output:**

```
C:\>ping 10.11.101.101

Pinging 10.11.101.101 with 32 bytes of data:
Reply from 10.11.101.101: bytes=32 time=10ms TTL=255
Reply from 10.11.101.101: bytes=32 time<1ms TTL=255
Reply from 10.11.101.101: bytes=32 time=1ms TTL=255
Reply from 10.11.101.101: bytes=32 time=1ms TTL=255

Ping statistics for 10.11.101.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

**To ping from a Linux PC**

1. Go to a shell prompt.
2. Enter “`ping 10.11.101.101`”.

## Traceroute

Where ping will only tell you if it reached its destination and came back successfully, traceroute will show each step of its journey to its destination and how long each step takes. If ping finds an outage between two points, traceroute can be used to locate exactly where the problem is.

### What is traceroute

Traceroute works by sending ICMP packets to test each hop along the route. It will send out three packets, and then increase the time to live (TTL) setting by one each time. This effectively allows the packets to go one hop farther along the route. This is the reason 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. Also, 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.

By default, traceroute uses UDP datagrams 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 if you want traceroute to work from both machines (Unix-like systems and Windows) you will need to allow both protocols inbound through your FortiGate security policies (UDP with ports from 33434 to 33534 and ICMP type 8).

You can also use the packet count column of the *Policy & Objects* > *Policy* page to track traceroute packets. This allows you to verify the connection, but also confirm which security policy the traceroute packets are using.

**What traceroute can tell you**

Ping and traceroute have similar functions—to verify connectivity between two points. The big difference is that traceroute shows you each step of the way, where ping does not. Also, ping and traceroute use different protocols and ports, so one may succeed where the other fails.

You can verify your DNS connection using traceroute. If you enter an FQDN instead of an IP address for the traceroute, DNS will try to resolve that domain name. If the name does not get resolved, you know you have DNS issues.

**How to use traceroute**

The traceroute command varies slightly between operating systems. Note that in MS Windows the command name is shortened to "`tracert`". Also, your output will list different domain names and IP addresses along your route.

**To use traceroute on an MS 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 "`tracert fortinet.com`" to trace the route from the PC to the Fortinet web site.

**Sample output:**

```
C:\>tracert fortinet.com

Tracing route to fortinet.com [208.70.202.225]
over a maximum of 30 hops:
1    <1 ms    <1 ms    <1 ms  172.20.120.2
2    66 ms    24 ms    31 ms 209-87-254-xxx.storm.ca [209.87.254.221]
3    52 ms    22 ms    18 ms  core-2-g0-0-1104.storm.ca [209.87.239.129]
4    43 ms    36 ms    27 ms  core-3-g0-0-1185.storm.ca [209.87.239.222]
5    46 ms    21 ms    16 ms  te3-x.1156.mpd01.cogentco.com
[38.104.158.69]
6    25 ms    45 ms    53 ms  te8-7.mpd01.cogentco.com [154.54.27.249]
7    89 ms    70 ms    36 ms  te3-x.mpd01.cogentco.com [154.54.6.206]
8    55 ms    77 ms    58 ms  sl-st30-chi-.sprintlink.net [144.232.9.69]
9    53 ms    58 ms    46 ms  sl-0-3-3-x.sprintlink.net [144.232.19.181]
10    82 ms    90 ms    75 ms  sl-x-12-0-1.sprintlink.net
[144.232.20.61]
11   122 ms   123 ms   132 ms  sl-0-x-0-3.sprintlink.net
[144.232.18.150]
12   129 ms   119 ms   139 ms  144.232.20.7
```

```
13   172 ms   164 ms   243 ms  sl-321313-0.sprintlink.net
[144.223.243.58]
14    99 ms    94 ms    93 ms  203.78.181.18
15   108 ms   102 ms    89 ms  203.78.176.2
16    98 ms    95 ms    97 ms  208.70.202.225

Trace complete.
```

The first, or the left column, is the hop count, which cannot go over 30 hops. When that number is reached, the traceroute ends.

The second, third, and fourth columns display how much time 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 the column farthest to the right, is the domain name of that device and its IP address or possibly just the IP address.

**To perform a traceroute on a Linux PC**

1. Go to a command line prompt.
2. Enter "`traceroute fortinet.com`".

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

**To perform a traceroute from the FortiGate**

1. Connect to the CLI either through telnet or through the CLI widget on the web-based manager dashboard.
2. Enter `exec traceroute www.fortinet.com` to trace the route to the destination IP address. There are no options for this command.

   Output appears as follows:

```
# execute traceroute www.fortinet.com
traceroute to www.fortinet.com (66.171.121.34), 32 hops max, 84 byte
packets
1  172.20.120.2  0.637 ms  0.653 ms  0.279 ms
2  209.87.254.221 <static-209-87-254-221.storm.ca>  2.448 ms  2.519 ms
2.458 ms
3  209.87.239.129 <core-2-g0-2.storm.ca>  2.917 ms  2.828 ms  9.324 ms
4  209.87.239.199 <core-3-bdi1739.storm.ca>  13.248 ms  12.401 ms
13.009 ms
5  216.66.41.113 <v502.core1.tor1.he.net>  17.181 ms  12.422 ms  12.268
ms
6  184.105.80.9 <100ge1-2.core1.nyc4.he.net>  21.355 ms  21.518 ms
21.597 ms
7  198.32.118.41 <ny-paix-gni.twgate.net>  83.297 ms  84.416 ms  83.782
ms
8  203.160.228.217 <217-228-160-203.TWGATE-IP.twgate.net>  82.579 ms
82.187 ms  82.066 ms
9  203.160.228.229 <229-228-160-203.TWGATE-IP.twgate.net>  82.055 ms
82.455 ms  81.808 ms
10  203.78.181.2  82.262 ms  81.572 ms  82.015 ms
11  203.78.186.70  83.283 ms  83.243 ms  83.293 ms
12  66.171.127.177  84.030 ms  84.229 ms  83.550 ms
13  66.171.121.34 <www.fortinet.com>  84.023 ms  83.903 ms  84.032 ms
14  66.171.121.34 <www.fortinet.com>  83.874 ms  84.084 ms  83.810 ms
```

## How to check the logs

This step in troubleshooting can be forgotten, but its an important one. Logging records the traffic passing through the FortiGate unit to your network and what action the FortiGate unit took during its scanning process of the traffic. This recorded information is called a log message.

When you configure FortiOS initially, log as much information as you can. If needed, logging of unused features can be turned off or scaled back if the logs generated are too large.

As with most troubleshooting steps, before you can determine if the logs indicate a problem, you need to know what logs result from normal operation. Without a baseline it is difficult to properly troubleshoot.

When troubleshooting with log files:

- Compare current logs to a recorded baseline of normal operation.
- If needed increase the level of logging (such as from Warning to Information) to obtain more information.

When increasing logging levels, ensure that alert email is configured and both disk usage and log quota are selected. This ensures you will be notified if the increased logging causes problems. You can also use Logging Monitor (located in *Log&Report* > *Monitor* > *Logging Monitor*) to determine the activities that generate the most log entries.

- check all logs to ensure important information is not overlooked
- filter or order log entries based on different fields (such as level, service, or IP address) to look for patterns that may indicate a specific problem (such as frequent blocked connections on a specific port for all IP addresses)

Logs will help identify and locate any problems, but they will not solve the problems. The job of logs is to speed up your problem solving and save you time and effort.

For more information on Logging and Log Reports, see the Logging and Reporting guide.

## How to verify the contents of the routing table (in NAT mode)

When you have some connectivity, or possibly none at all a good place to look for information is the routing table.

The routing table is where all the currently used routes are stored for both static and dynamic protocols. If a route is in the routing table, it saves the time and resources of a lookup. If a route is 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. If your FortiGate unit is in Transparent mode, you are unable to perform this step.

If the FortiGate is running in NAT mode, verify that all desired routes are in the routing table: local subnets, default routes, specific static routes, and dynamic routing protocols.

To check the routing table in the web-based manager, use the Routing Monitor by going to *Router* > *Monitor* > *Routing Monitor*.

In the CLI, use the command `get router info routing-table all`. Sample output:

```
FGT# get router info routing-table all

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
```

```
       * - candidate default

S*      0.0.0.0/0 [10/0] via 172.20.120.2, wan1
C       10.31.101.0/24 is directly connected, internal
C       172.20.120.0/24 is directly connected, wan1
```

## How to verify the correct route is being used

If you have more than one default route and wants to make sure that traffic is flowing as expected via the right route, you can run a trace route from a machine in the local area network, this will indicate you the first hop that the traffic goes through.

**Sample output:**

```
C:\>tracert www.fortinet.com

Tracing route to www.fortinet.com [66.171.121.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.10.1.99
  2     1 ms    <1 ms    <1 ms  172.20.120.2
  3     3 ms     3 ms     3 ms  static-209-87-254-221.storm.ca
[209.87.254.221]
  4     3 ms     3 ms     3 ms  core-2-g0-2.storm.ca [209.87.239.129]
  5    13 ms    13 ms    13 ms  core-3-bdi1739.storm.ca [209.87.239.199]
  6    12 ms    19 ms    11 ms  v502.core1.tor1.he.net [216.66.41.113]
  7    22 ms    22 ms    21 ms  100ge1-2.core1.nyc4.he.net
[184.105.80.9]
  8    84 ms    84 ms    84 ms  ny-paix-gni.twgate.net [198.32.118.41]
  9    82 ms    84 ms    82 ms  217-228-160-203.TWGATE-IP.twgate.net
[203.160.22
8.217]
 10    82 ms    81 ms    82 ms  229-228-160-203.TWGATE-IP.twgate.net
[203.160.22
8.229]
 11    82 ms    82 ms    82 ms  203.78.181.2
 12    84 ms    83 ms    83 ms  203.78.186.70
 13    84 ms     *       85 ms  66.171.127.177
 14    84 ms    84 ms    84 ms  fortinet.com [66.171.121.34]
 15    84 ms    84 ms    83 ms  fortinet.com [66.171.121.34]

Trace complete.
```

In this scenario, the first hop contains the IP address `10.10.1.99`, which is the internal interface of the FortiGate. The second hop contains the IP address `172.20.120.2`, to which the wan1 interface of the FortiGate is connected, so we can conclude that the route via wan1 interface is being used for this traffic.

Also debug the packet flow in the CLI shows the route taken for each session.

Sample output:

```
id=20085 trace_id=319 func=vf_ip4_route_input line=1597 msg="find a
route: gw-172.20.120.2 via wan1"
```

For more information on debuging the packet flow, see How to debug the packet flow.

## How to verify the correct firewall policy is being used

If you have more than one firewall policy, use the count column to check which policy is being used, the count must show traffic increasing. To do so, go to *Policy & Objects* > *Policy* page.

Also debuging the packet flow in the CLI shows the policy id allowing the traffic.

Sample output:

```
id=13 trace_id=1 func=fw_forward_handler line=650 msg="Allowed by
Policy-14: SNAT"
```

For more information on debuging the packet flow, see How to debug the packet flow.

## How to check the bridging information in Transparent mode

When FortiOS is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit.

Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues, and there are no bridges listed, that is a likely cause. Check for the MAC address of the interface or device in question.

### How to check the bridging information

To list the existing bridge instances on the FortiGate unit, use the following command:

```
diagnose netlink brctl list
```

**Sample output:**

```
#diagnose netlink brctl list
list bridge information
1. root.b fdb: size=256  used=6    num=7    depth=2    simple=no
Total 1 bridges
```

### How to display forwarding domain information

Forwarding domains, or collision domains, are used in routing to limit where packets are forwarded on the network. Layer-2 broadcasts are limited to the same group. By default, all interfaces are in group 0. For example, if the FortiGate unit has 12 interfaces, only two may be in the same forwarding domain, which will limit packets that are broadcast to only those two interfaces. This reduces traffic on the rest of the network.

Collision domains prevent the forwarding of ARP packets to all VLANs on an interface. Without collision domains, duplicate MAC addresses on VLANs may cause ARP packets to be duplicated. Duplicate ARP packets can cause some switches to reset.

It is important to know what interfaces are part of which forwarding domains as this determines which interfaces can communicate with each other.

To manually configure forwarding domains in Transparent mode, use the following FortiOS CLI command:

```
config system interface
  edit <interface_name>
  set forward-domain <integer>
end
```

**To display the information for forward domains**

Use the following command:

```
diagnose netlink brctl domain <name> <id>
```

where <name> is the name of the forwarding domain to display and <id> is the domain id.

**Sample output**

```
diagnose netlink brctl domain ione 101
show bridge root.b ione forward domain.
id=101 dev=trunk_1 6
```

**To list the existing bridge MAC table, use the following command:**

```
diagnose netlink brctl name host <name>
```

**Sample output**

```
show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table
```

| port no | device | devname | mac addr | ttl | attributes |
|---|---|---|---|---|---|
| 2 | 7 | wan2 | 02:09:0f:78:69:00 | 0 | Local Static |
| 5 | 6 | vlan_1 | 02:09:0f:78:69:01 | 0 | Local Static |
| 3 | 8 | dmz | 02:09:0f:78:69:01 | 0 | Local Static |
| 4 | 9 | internal | 02:09:0f:78:69:02 | 0 | Local Static |
| 3 | 8 | dmz | 00:80:c8:39:87:5a | 194 | |
| 4 | 9 | internal | 02:09:0f:78:67:68 | 8 | |
| 1 | 3 | wan1 | 00:09:0f:78:69:fe | 0 | Local Static |

**To list the existing bridge port list, use this command:**

```
diagnose netlink brctl name port <name>
```

**Sample Output:**

```
show bridge root.b data port.
trunk_1  peer_dev=0
internal  peer_dev=0
dmz  peer_dev=0
wan2  peer_dev=0
wan1  peer_dev=0
```

## How to check number of sessions used by UTM proxy

Each FortiGate model has a set limit of the maximum number of sessions the UTM proxy supports. The UTM proxy handles all the traffic for the following protocols: HTTP, SMTP, POP3, IMAP, FTP, and NNTP. If the proxy for a protocol fills up its session table, the FortiGate unit will enter conserve mode, where it behaves differently, until entries and memory free up again.

### Conserve or failopen mode

Once you reach the limit, depending on your FortiGate unit's conserve mode configuration, no new sessions are created until an old ones end. You can configure your FortiGate unit's

behavior when memory is running low or the proxy connection limit has been reached. There are two related commands for this in the CLI:

```
config system global
  set av-failopen-session {enable | disable}
  set av-failopen { idledrop | off | one-shot | pass}
end
```

`av-failopen-session` must be enabled to set the behavior for these conditions. When it is enabled, and a proxy for a protocol runs out of room in its session table that protocol goes into failopen mode and behaves as defined in the `av-failopen` command.

`av-failopen` determines the behavior of the proxy until entries are free in the session table again for that proxy.

- **idledrop —** This option removes idle sessions from the session table, starting with the clients that have the most sessions currently open. This method assumes that idle sessions are not being used and it will not cause problems to close these sessions. This is usually true, but some applications may have problems with this and start complaining about either not having or being able to open a session. If this occurs, try another method to check if this is really the problem. This is a secure option as no unscanned traffic is allowed to pass.
- **off —** This option turns off accepting any new AV sessions, but will continue to process any existing AV sessions that are currently active. All the protocols listed (HTTP, SMTP, POP3, IMAP, FTP, and NNTP) are scanned by FortiGate Antivirus. If AV scanning is enabled, av-failopen off is selected, and the proxy session table fills up, then no new sessions of that type will be accepted. For example, if POP3 session table is filled and email AV scanning is enabled, no more POP3 connections will be allowed until the session table gets some free space. This is a secure option because no unscanned traffic is allowed to pass.
- **one-shot —** When memory is low, bypass the antivirus system. The name one-shot comes from the fact that once you are in one-shot av-failopen mode, you must set av-failopen to either *pass* or *off* to restart AV scanning. This is a very unsecure option because it allows all traffic without AV scanning, and it never reverts to normal without manual assistance.
- **pass —** When memory is low, bypass the antivirus system much as one-shot. The difference is that when memory is freed up, the system will start AV scanning automatically again. This is an unsecure option because it allows traffic to pass without AV scanning. However, it is better than one-shot because it automatically restarts AV scanning when possible.

If the proxy session table is full for one or more protocols and your FortiGate unit enters into conserve or failopen mode, it will appear as if you have lost connections, network services are intermittent or non-existent, and yet other services work normally for a while until their sessions end and they join the queue of session-starved applications.

### Checking sessions in use

To make troubleshooting this type of problem easier, sessions are broken down by which protocol they use. This provides you with statistics and errors specific to one of the protocols.

Due to the amount of output from this command, you should connect to the CLI with a terminal program, such as puTTY, that logs output. Otherwise, you will likely not be able to access all the output information from the command.

In the following output, only the HTTP entries are displayed. The other protocols have been removed in an attempt to shorten the output. There will be separate entries for each supported protocol (HTTP, SMTP, POP3, IMAP, FTP, and NNTP) in each section of the output.

**To check sessions in use and related errors - CLI**

```
FGT# # get test proxyworker 4
```

```
Worker[0]
HTTP Common
Current Connections                                  8/8032
Max Concurrent Connections                           76


Worker Stat
Running time (HH:MM:SS:usec)           29:06:27:369365
Time in loop scanning                      2:08:000198
Error Count (accept)                                 0
Error Count (read)                                   0
Error Count (write)                                  0
Error Count (poll)                                   0
Error Count (alloc)                                  0
Last Error                                           0
Acceptor Read                                     6386
Acceptor Write                                   19621
Acceptor Close                                       0

HTTP Stat
Bytes sent                                      667012 (kb)
Bytes received                                  680347 (kb)
Error Count (alloc)                                  0
Error Count (accept)                                 0
Error Count (bind)                                   0
Error Count (connect)                                0
Error Count (socket)                                 0
Error Count (read)                                 134
Error Count (write)                                  0
Error Count (retry)                                 40
Error Count (poll)                                   0
Error Count (scan reset)                             2
Error Count (urlfilter wait)                         3
Last Error                                         104
Web responses clean                              17950
Web responses scan errors                           23
Web responses detected                              16
Web responses infected with worms                    0
Web responses infected with viruses                  0
Web responses infected with susp                     0
Web responses file blocked                           0
Web responses file exempt                            0
Web responses bannedword detected                    0
Web requests oversize pass                          16
Web requests oversize block                          0
Last Server Scan errors                            102
URL  requests exempt                                 0
URL  requests blocked                                0
URL  requests passed                                 0
URL  requests submit error                           0
URL  requests rating error                           0
URL  requests rating block                           0
URL  requests rating allow                       10025
URL  requests infected with worms                    0
Web  requests detected                               0
Web  requests file blocked                           0
```

```
Web  requests file exempt                              0
POST requests clean                                  512
POST requests scan errors                              0
POST requests infected with viruses                    0
POST requests infected with susp                       0
POST requests file blocked                             0
POST requests bannedword detected                      0
POST requests oversize pass                            0
POST requests oversize block                           0
Web request  backlog drop                              0
Web response backlog drop                              0


Worker Accounting
poll=721392/649809/42 pollfail=0 cmdb=85 scan=19266 acceptor=25975

HTTP Accounting
setup_ok=8316 setup_fail=0 conn_ok=0 conn_inp=8316
urlfilter=16553/21491/20 uf_lookupf=0
scan=23786 clt=278876 srv=368557

SMTP Accounting
setup_ok=12 setup_fail=0 conn_ok=0 conn_inp=12
scan=12 suspend=0 resume=0 reject=0 spamadd=0 spamdel=0 clt=275
   srv=279

POP3 Accounting
setup_ok=30 setup_fail=0 conn_ok=0 conn_inp=30
scan=3 clt=5690 srv=5836

IMAP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
scan=0 clt=0 srv=0

FTP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
scan=0 clt=0 srv=0 datalisten=0 dataclt=0 datasrv=0

NNTP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
scan=0 clt=0 srv=0
```

The output from this command falls into the following sections:

- **HTTP Common current connections —** There is an entry for each protocol that displays the connections currently used, and the maximum connections allowed. This maximum is for the UTM proxy, which means all the protocols connections combined cannot be larger than this number. To support this, note that the maximum session count for each protocol is the same. You may also see a line titled `Max Concurrent Connections` for each protocol. This number is the maximum connections of this type allowed at one time. If VDOMs are enabled, this value is defined either on the global or per-VDOM level at *VDOM > Global Resources* or in the CLI at `config system resource-limits`.
- **Worker Stat —** This is statistics about the UTM proxy including how long it has been running, and how many errors it has found.
- **HTTP Stat —** This section includes statistics about the HTTP protocol proxy. This is a very extensive list covering errors, web responses, and any UTM positive matches. There are

similar sections for each protocol, but the specific entries in each vary based on what UTM scanning is looking for in each — spam control for email, file transfer blocking for FTP, and so on.

- **Worker Accounting —** Lists accounting information about the UTM proxy such as polling statistics, how many sessions were scanned, and how many were just accepted. This information can tell you if expect AV scanning is taking place or not. Under normal operation there should be no errors or fails.
- **HTTP Accounting —** The accounting sections for each protocol provide information about successful session creation, failures, how many sessions are being scanned or filtered, and how many are client or server originated. If setup_fail is larger than zero, run the command again to see if it is increasing quickly. If it is, your FortiGate unit may be in conserve mode.

### Related commands

To dump memory usage:

```
# get test proxyworker 1
```

To display statistics per VDOM:

```
# get test proxyworker 4444
```

To restart the proxy:

```
# get test proxyworker 99
```

## How to examine the firewall session list

One further step is to examine the firewall session. The firewall session list displays all the sessions the FortiGate unit has open. You will be able to see if there are strange patterns such as no sessions apart from the internal network, or all sessions are only to one IP address.

When examining the firewall session list in the CLI, filters may be used to reduce the output. In the web-based manager, the filters are part of the interface.

**To examine the firewall session list - web-based manager** go to *System* > *Dashboard* > *Top Sources*

**To examine the firewall session list - CLI**

When examining the firewall session list, there may be too many sessions to display. In this case it will be necessary to limit or filter the sessions displayed by source or destination address, or NATed address or port. If you want to filter by more than one of these, you need to enter a separate line for each value.

The following example shows filtering the session list based on a source address of 10.11.101.112.

```
FGT# diag sys session filter src 10.11.101.112
FGT# diag sys session list
```

The following example shows filtering the session list based on a destination address of 172.20.120.222.

```
FGT# diag sys session filter dst 172.20.120.222
FGT# diag sys session list
```

**To clear all sessions corresponding to a filter - CLI**

```
FGT# diag sys session filter dst 172.20.120.222
FGT# diag sys session clear
```

### Check source NAT information

Remember NAT when troubleshooting connections. NAT is especially important if you are troubleshooting from the remote end of the connection outside the FortiGate unit firewall. On the dashboard session list, pay attention to *Src address after NAT*, and *Src port after NAT*. These columns display the IP and port values after NAT has been applied.

The NAT values can be helpful to ensure they are the values you expect, and to ensure the remote end of the sessions can see the expected IP address and port number.

When displaying the session list in the CLI, you can match the NATed source address (`nsrc`) and port (`nport`). This can be useful if multiple internal IP addresses are NATed to a common external facing source IP address.

```
FGT# diag sys session filter nsrc 172.20.120.122
FGT# diag sys session filter nport 8888
FGT# diag sys session list
```

## How to check wireless information

Wireless connections, stations, and interfaces have different issues than other physical interfaces.

### Troubleshooting station connection issue

To check whether station entry is created on Access Control:

```
FG600B3909600253 # diagnose wireless-controller wlac -d sta
* vf=0 wtp=70 rId=2 wlan=open ip=0.0.0.0 mac=00:09:0f:db:c4:03 rssi=0
idle=148 bw=0 use=2
 vf=0 wtp=70 rId=2 wlan=open ip=172.30.32.122 mac=00:25:9c:e0:47:88
rssi=-40 idle=0 bw=9 use=2
```

### Enable diagnostic for particular station

This example uses the station MAC address to find where it is failing:

```
FG600B3909600253 # diagnose wireless-controller wlac sta_filter
00:25:9c:e0:47:88 1
Set filter sta 00:25:9c:e0:47:88 level 1
FG600B3909600253 # 71419.245 <ih> IEEE 802.11 mgmt::disassoc <==
00:25:9c:e0:47:88 vap open rId 1 wId 0 00:09:0f:db:c4:03
71419.246 <dc> STA del 00:25:9c:e0:47:88 vap open rId 1 wId 0
71419.246 <cc> STA_CFG_REQ(34) sta 00:25:9c:e0:47:88 del ==> ws
(0-192.168.35.1:5246) rId 1 wId 0
71419.246 <cc> STA del 00:25:9c:e0:47:88 vap open ws
(0-192.168.35.1:5246) rId 1 wId 0 00:09:0f:db:c4:03 sec open reason
I2C_STA_DEL
71419.247 <cc> STA_CFG_RESP(34) 00:25:9c:e0:47:88 <== ws
(0-192.168.35.1:5246) rc 0 (Success).
```

## How to verify FortiGuard connectivity

You can verify the FortiGuard connectivity in the *License Information* widget under *System* > *Dashboard* > *Status.* When FortiGate is connected to FortiGuard, a green check mark appears for available FortiGuard services.

From CLI, execute ping “service.fortiguard.net” and “update.fortiguard.net”.

**Sample output:**

```
FG100D# execute ping service.fortiguard.net
PING guard.fortinet.net (208.91.112.196): 56 data bytes
64 bytes from 208.91.112.196: icmp_seq=0 ttl=51 time=61.0 ms
64 bytes from 208.91.112.196: icmp_seq=1 ttl=51 time=60.0 ms
64 bytes from 208.91.112.196: icmp_seq=2 ttl=51 time=59.6 ms
64 bytes from 208.91.112.196: icmp_seq=3 ttl=51 time=58.9 ms
64 bytes from 208.91.112.196: icmp_seq=4 ttl=51 time=59.2 ms

--- guard.fortinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 58.9/59.7/61.0 ms

FG100D# execute ping update.fortiguard.net
PING fds1.fortinet.com (208.91.112.68): 56 data bytes
64 bytes from 208.91.112.68: icmp_seq=0 ttl=53 time=62.0 ms
64 bytes from 208.91.112.68: icmp_seq=1 ttl=53 time=61.8 ms
64 bytes from 208.91.112.68: icmp_seq=2 ttl=53 time=61.3 ms
64 bytes from 208.91.112.68: icmp_seq=3 ttl=53 time=61.9 ms
64 bytes from 208.91.112.68: icmp_seq=4 ttl=53 time=61.8 ms
```

## How to perform a sniffer trace (CLI and Packet Capture)

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

If your FortiGate unit has NP2/NP4 interfaces that are offloading traffic, this will change the sniffer trace. Before performing a trace on any NP2/NP4 interfaces, you should disable offloading on those interfaces.

### What can sniffing packets tell you

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the 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.

Sniffing packets can also tell you if the FortiGate unit is silently dropping packets for reasons such as Reverse Path Forwarding (RPF), also called Anti Spoofing, which prevents an IP packet from being forwarded if its Source IP does not either belong to a locally attached subnet (local interface), or be part of the routing between the FortiGate unit and another source (static route, RIP, OSPF, BGP). Note that RPF can be disabled by turning on asymmetric routing in the CLI (`config system setting, set asymetric enable`), however this will disable stateful inspection on the FortiGate unit and cause many features to be turned off.

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 the traffic will be using the virtual IP addresses. This is due to the ARP update that is sent out when the VIP address is configured.

### How do you sniff packets

The general form of the internal FortiOS packet sniffer command is:

```
diag sniffer packet <interface_name> <'filter'> <verbose> <count>
```

To stop the sniffer, type `CTRL+C`.

| | |
|---|---|
| **<interface_name>** | The name of the interface to sniff, such as “port1” or “internal”. This can also be “any” to sniff all interfaces. |
| **<‘filter’>** | What to look for in the information the sniffer reads. “none” indicates no filtering, and all packets will be displayed as the other arguments indicate.<br>The filter must be inside single quotes (‘). |
| **<verbose>** | The level of verbosity as one of:<br>**1 -** print header of packets<br>**2 -** print header and data from IP of packets<br>**3 -** print header and data from Ethernet of packets<br>**4-** print header of packets with interface name |
| **<count>** | The number of packets the sniffer reads before stopping. If you do not put a number here, the sniffer will run forever unit you stop it with <CTRL C>. |

For a simple sniffing example, enter the CLI command `diag sniffer packet port1 none 1 3`. This will display the next three packets on the port1 interface using no filtering, and using verbose level 1. At this verbosity level you can see the source IP and port, the destination IP and port, action (such as ack), and sequence numbers.

In the output below, port 443 indicates these are HTTPS packets, and 172.20.120.17 is both sending and receiving traffic.

```
Head_Office_620b # diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.545306 172.20.120.17.52989 -> 172.20.120.141.443: psh 3177924955
   ack 1854307757

0.545963 172.20.120.141.443 -> 172.20.120.17.52989: psh 1854307757
   ack 3177925808

0.562409 172.20.120.17.52988 -> 172.20.120.141.443: psh 4225311614
   ack 3314279933
```

For a more advanced example of packet sniffing, the following commands will report packets on any interface travelling between a computer with the host name of “PC1” and the computer with the host name of “PC2”. With verbosity 4 and above, the sniffer trace will display the interface names where traffic enters or leaves the FortiGate unit. Remember to stop the sniffer, type `CTRL+C`.

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2>" 4
```

or

```
FGT# diagnose sniffer packet any "(host <PC1> or host <PC2>) and
   icmp" 4
```

The following sniffer CLI command includes the ARP protocol in the filter which may be useful to troubleshoot a failure in the ARP resolution (for instance PC2 may be down and not responding to the FortiGate ARP requests).

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2> or arp" 4
```

## Packet Capture

When troubleshooting networks, it helps to look inside the header of the packets. This helps to determine if the packets, route, and destination are all what you expect. Packet capture can also be called a network tap, packet sniffing, or logic analyzing.

**To use the packet capture:**

1. Go to *System* > *Network* > *Packet Capture*.
2. Select the interface to monitor and select the number of packets to keep.
3. Select `Enable Filters`.
4. Enter the information you want to gather from the packet capture.
5. Select `OK`.

To run the capture, select the `play` button in the progress column in the packet capture list. If not active, *Not Running* will also appear in the column cell. The progress bar will indicate the status of the capture. You can stop and restart it at any time.

When the capture is complete, click the `Download` icon to save the packet capture file to your hard disk for further analysis.

Packet capture tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- Finding missing traffic.
- Seeing if sessions are setting up properly.
- Locating ARP problems such as broadcast storm sources and causes.
- Confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks.
- Confirming routing is working as you expect.
- Wireless client connection problems.
- Intermittent missing PING packets.
- A particular type of packet is having problems, such as UDP, which is commonly used for streaming video.

If you are running a constant traffic application such as ping, packet capture can tell you if the traffic is reaching the destination, how the port enters and exits the FortiGate unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start capturing packets, you need to have a good idea of what you are looking for. Capture is used to confirm or deny your ideas about what is happening on the network. If you try capture without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to capture enough packets to really understand all of the patterns and behavior that you are looking for.

## How to debug the packet flow

Traffic should come in and leave the FortiGate unit. If you have determined that network traffic is not entering and leaving the FortiGate unit as expected, debug the packet flow.

Debugging can only be performed using CLI commands. Debugging the packet flow requires a number of debug commands to be entered as each one configures part of the debug action, with the final command starting the debug.

If your FortiGate unit has FortiASIC NP4 interface pairs that are offloading traffic, this will change the packet flow. Before performing the debug on any NP4 interfaces, you should disable offloading on those interfaces.

The following configuration assumes that PC1 is connected to the internal interface of the FortiGate unit and has an IP address of 10.11.101.200. PC1 is the host name of the computer.

To debug the packet flow in the CLI, enter the following commands:

```
FGT# diag debug disable
FGT# diag debug flow filter add <PC1>
FGT# diag debug flow show console enable
FGT# diag debug flow show function-name enable
FGT# diag debug flow trace start 100
FGT# diag debug enable
```

The `start 100` argument in the above list of commands will limit the output to 100 packets from the flow. This is useful for looking at the flow without flooding your log or displaying too much information.

To stop all other debug activities, enter the command:

```
FGT# diag debug flow trace stop
```

The following is an example of debug flow output for traffic that has no matching security policy, and is in turn blocked by the FortiGate unit. The denied message indicates that the traffic was blocked.

```
id=20085 trace_id=319 func=resolve_ip_tuple_fast line=2825
   msg="vd-root received a packet(proto=6,
   192.168.129.136:2854->192.168.96.153:1863) from port3."

id=20085 trace_id=319 func=resolve_ip_tuple line=2924 msg="allocate
   a new session-013004ac"

id=20085 trace_id=319 func=vf_ip4_route_input line=1597 msg="find a
   route: gw-192.168.150.129 via port1"

id=20085 trace_id=319 func=fw_forward_handler line=248 msg=" Denied
   by forward policy check"
```

# Index

## R



## S



## T



## U



## V