In this lesson, you will learn about using diagnostic commands and tools.

Objectives

- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers
- Diagnose connectivity problems using sniffer and debug flow
- Diagnose resource problems, such as high CPU or memory usage
- Diagnose memory conserve mode

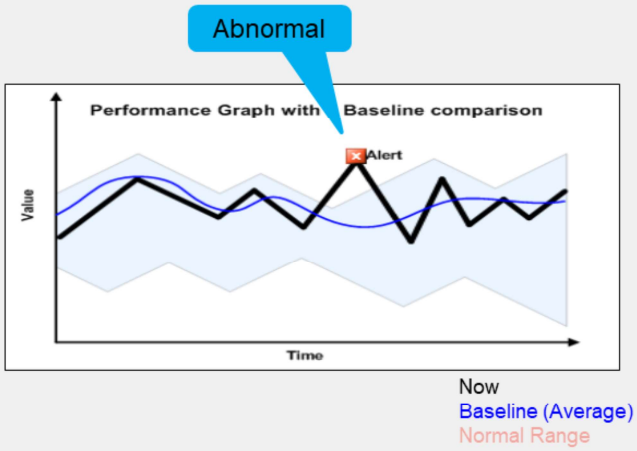
FORTINET Training Institute

After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in general diagnosis, you will be able to discover general information about the status of FortiGate.

Before a Problem Occurs

- Know what normal is (baseline):
  - CPU usage
  - Memory usage
  - Traffic volume
  - Traffic directions
  - Protocols and port numbers
  - Traffic pattern and distribution
- Why?
  - Abnormal behavior is difficult to identify, *unless* you know, relatively, what normal is



FORTINET Training Institute

Diagnosis is the process of finding the underlying cause of a problem.

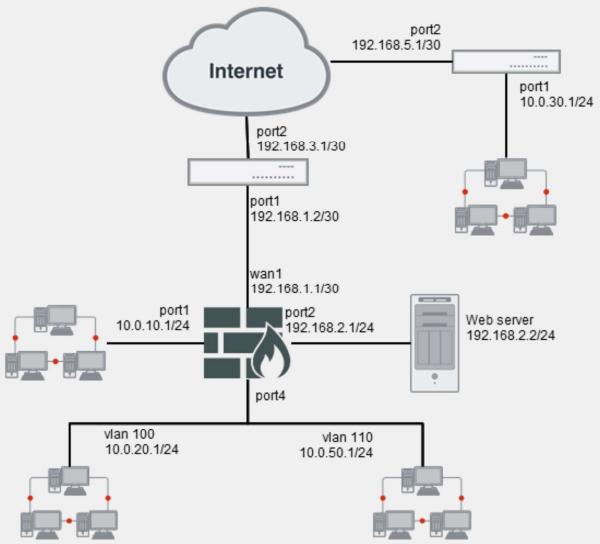
In order to define any problem, first you must know what your network's *normal* behavior is.

In the graph shown on this slide, the range that indicates *normal* is shown in blue. What exactly is this blue line? It indicates the averages—our baseline. What is the thick black line? It's the current behavior. When the current behavior (black line) leaves the normal range, an abnormal event is happening.

Normal is measured and defined in many ways. It can be performance: the expected CPU and memory utilization, bandwidth, and traffic volumes. But, it can also be your network topology: which devices are normally connected at each node. It is also behavior: traffic flow directions, which protocols are blocked or proxied, and the distribution of protocols and applications used during specific times of the day, week, or year.

Network Diagrams

- Why?
  - Explaining or analyzing complex networks is difficult and time-consuming without them
- Physical diagrams:
  - Include cables, ports, and physical network devices
  - Show relationships at layer 1 and layer 2
- Logical diagrams:
  - Include subnets, routers, logical devices
  - Show relationships at layer 3



FORTINET Training Institute

What is the first way to define what is *normal* for your network?

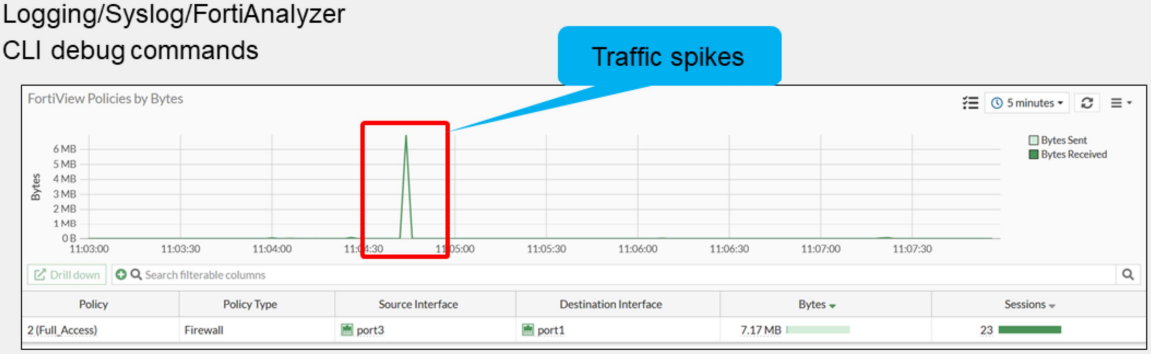
Flows and other specifications of *normal* behaviour are derived from topology. So, during troubleshooting, a network diagram is essential. If you create a ticket with Fortinet Technical Support, a network diagram should be the first thing you attach.

Network diagrams sometimes combine the two types of diagrams:
- Physical
- Logical

A physical diagram shows how cables, ports, and devices are connected between buildings and cabinets.
A logical diagram shows relationships (usually at OSI layer 3) between virtual LANs, IP subnets, and routers. It can also show application protocols such as HTTP or DHCP.

Monitoring Traffic Flows and Resource Usage

- Get normal data before problems or complaints
- Tools:
  - Security Fabric
  - Dashboard
  - SNMP
  - Alert email
  - Logging/Syslog/FortiAnalyzer
  - CLI debug commands

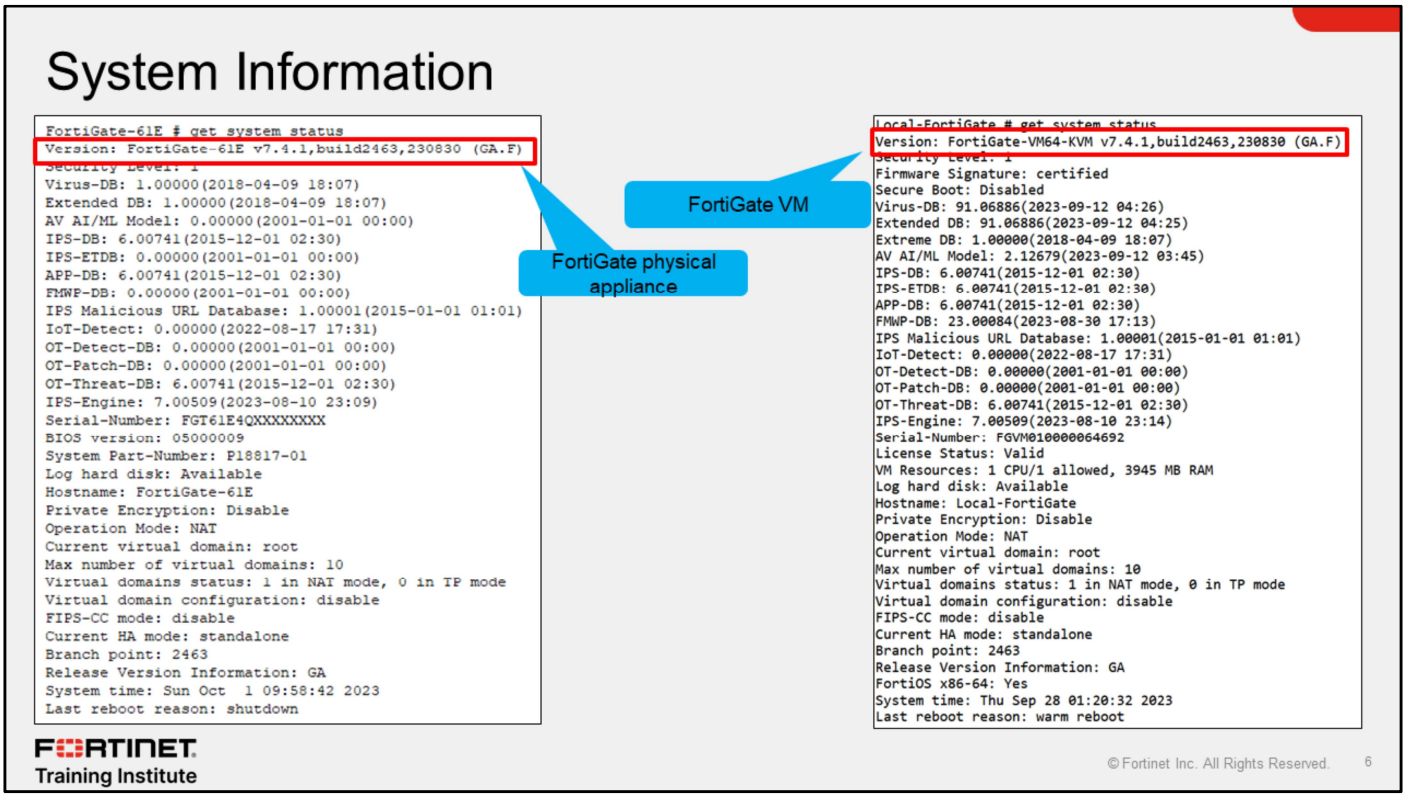


FORTINET Training Institute

Another way to define normal is to know the average performance range. On an ongoing basis, collect data that shows normal usage.

For example, if traffic processing is suddenly slow, and the FortiGate CPU use is 75%, what does that indicate? If CPU use is usually 60–69%, then 75% is probably still normal. But if normal is 12–15%, there may be a problem.

Get data on both the typical maximum and minimum for the time and date. That is, on a workday or holiday, how many bits per second should ingress or egress each interface in your network diagrams?



How can we get information about the current status? First, look at CLI commands; you can use them through a local console, even if network issues make GUI access slow or impossible.

A few commands provide system statuses. The `get system status` command provides mostly general-purpose information. The output shows:

- Model
- Serial number
- Firmware version
- Host name
- FortiGuard license status
- System time
- Version of the FortiGuard antivirus, IPS, and IP reputation databases, and others

Network Layer Troubleshooting

```
# execute ping-options
adaptive-ping     Adaptive ping <enable|disable>.
data-size         Integer value to specify datagram size in bytes.
df-bit            Set DF bit in IP header <yes | no>.
interface         Auto | <outgoing interface>.
interval          Integer value to specify seconds between two pings.
pattern           Hex format of pattern, e.g. 00ffaabb.
repeat-count      Integer value to specify how many times to repeat PING.
...

# execute ping <x.x.x.x> "IP address or domain name"

# execute traceroute <x.x.x.x> "Destination IP address or hostname"
```

FORTINET Training Institute

Say that FortiGate can contact some hosts through port1, but not others. Is the problem in the physical layer or the link layer? Neither. Connectivity has been proven with at least part of the network. Instead, you should check the network layer. To test this, as usual, start with ping and traceroute.

The same commands exist for IPv6: `execute ping` becomes `execute ping6`, for example.

Remember: Location matters. Tests are accurate only if you use the same path as the traffic that you are troubleshooting. To test from FortiGate (to FortiAnalyzer or FortiGuard, for example), use the FortiGate `execute ping` and `execute traceroute` CLI commands. But, to test the path through FortiGate, also use `ping` and `tracert` or `traceroute` from the endpoint—from the Windows, Linux, or Mac OS X computer—not only from the FortiGate CLI.

Because of NAT and routing, you might need to specify a different ping source IP address—the default address is the IP of the outgoing interface. If there is no response, verify that the target is configured to reply to ICMP echo requests.

Packet Capture

- Packet sniffer command:
  - `#diagnose sniffer packet <interface> <filter> <verbose> <count> <tsformat>`
  - `<count>` stops packet capture after this many packets
  - `<tsformat>` changes the time stamp format
  - `a` – Absolute UTC time
  - `l` – Local time

Level	IP headers	IP payload	Ethernet headers	Port names
1	✓			
2	✓	✓		
3	✓	✓	✓	
4	✓			✓
5	✓	✓		✓
6	✓	✓	✓	✓

FORTINET Training Institute

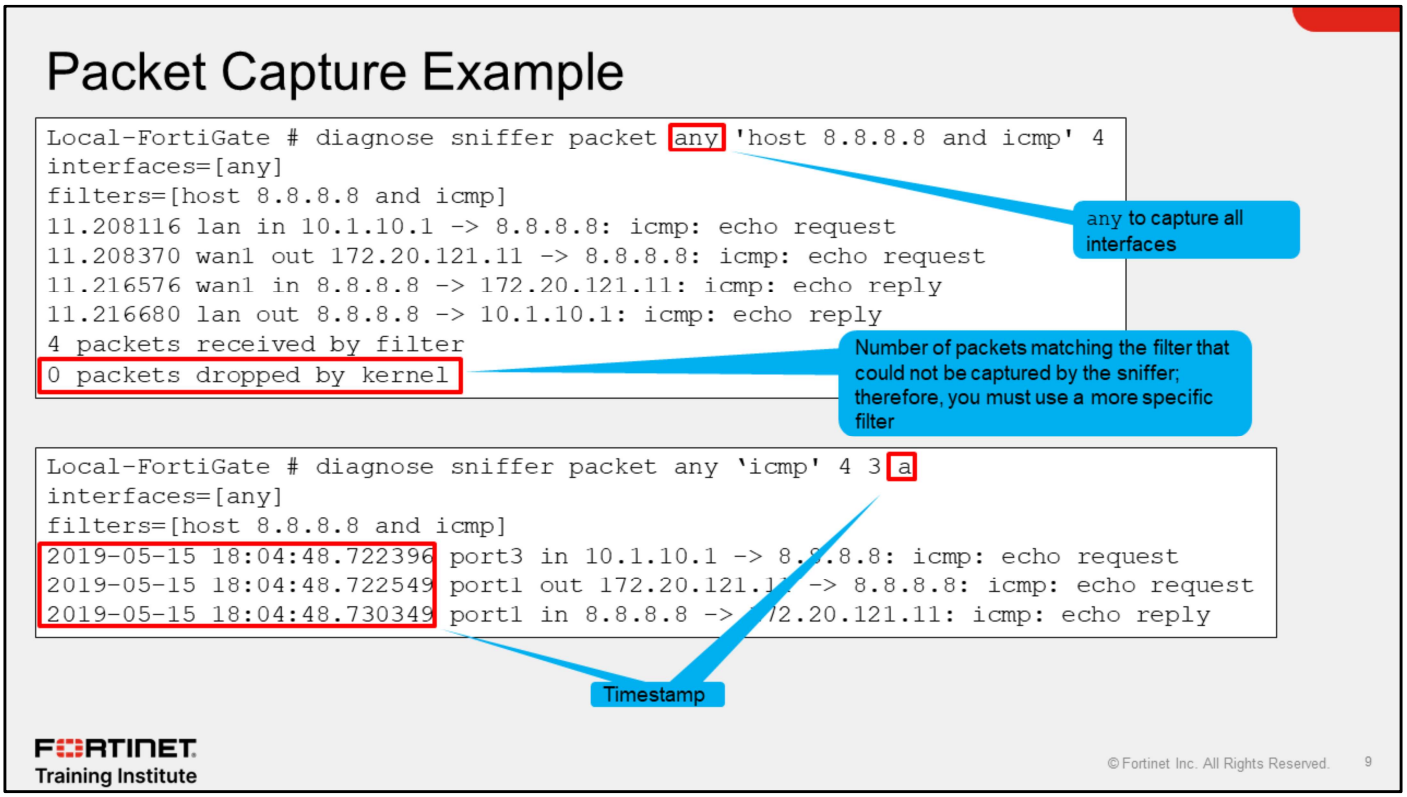
FortiGate includes the sniffer command, which is a useful tool when troubleshooting requires you to dig further to diagnose the source of the issue.

The sniffer command can sniff packets on physical or virtual interfaces. If the sniffer command is set to `any`, it can sniff all available interfaces simultaneously.

You can use a filter to customize and narrow down the packets that you want to capture. The sniffer filter uses Berkeley Packet Filter (BPF) syntax.

The `verbose` setting has six verbosity levels:

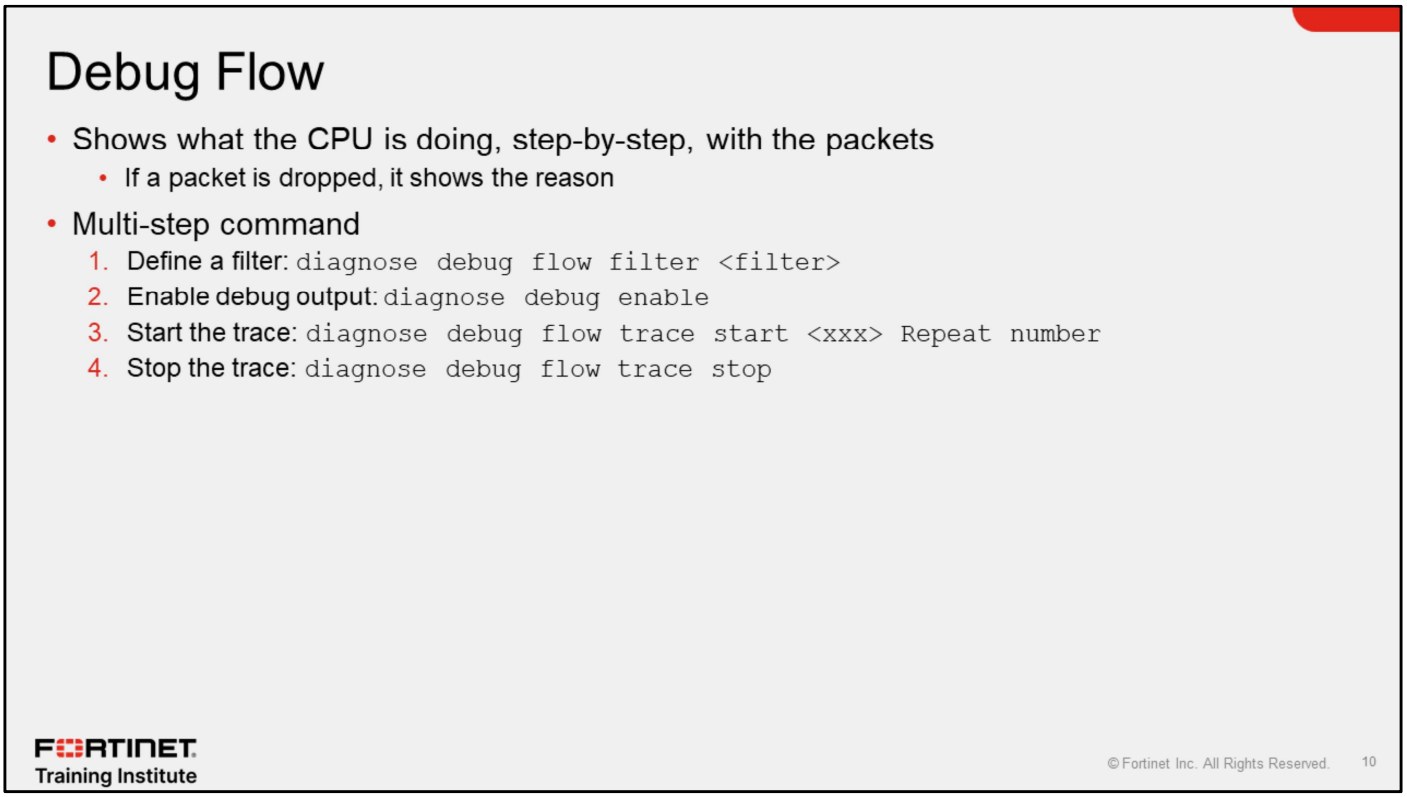
- `1`: print header of packets
- `2`: print header and data from the IP header of the packets
- `3`: print header and data from the Ethernet header of the packets
- `4`: print header of packets with interface name
- `5`: print header and data from IP of packets with interface name
- `6`: print header and data from Ethernet of packets with interface name



To sniffer traffic in all interfaces, use the keyword `any` as the interface name.

Stop the sniffer by pressing `Ctrl+C`, and check for dropped packets. If there were dropped packets during the sniffer, it means that not all the traffic that matched the sniffer filter could be captured. So, you might need to capture the traffic again using a stricter filter.

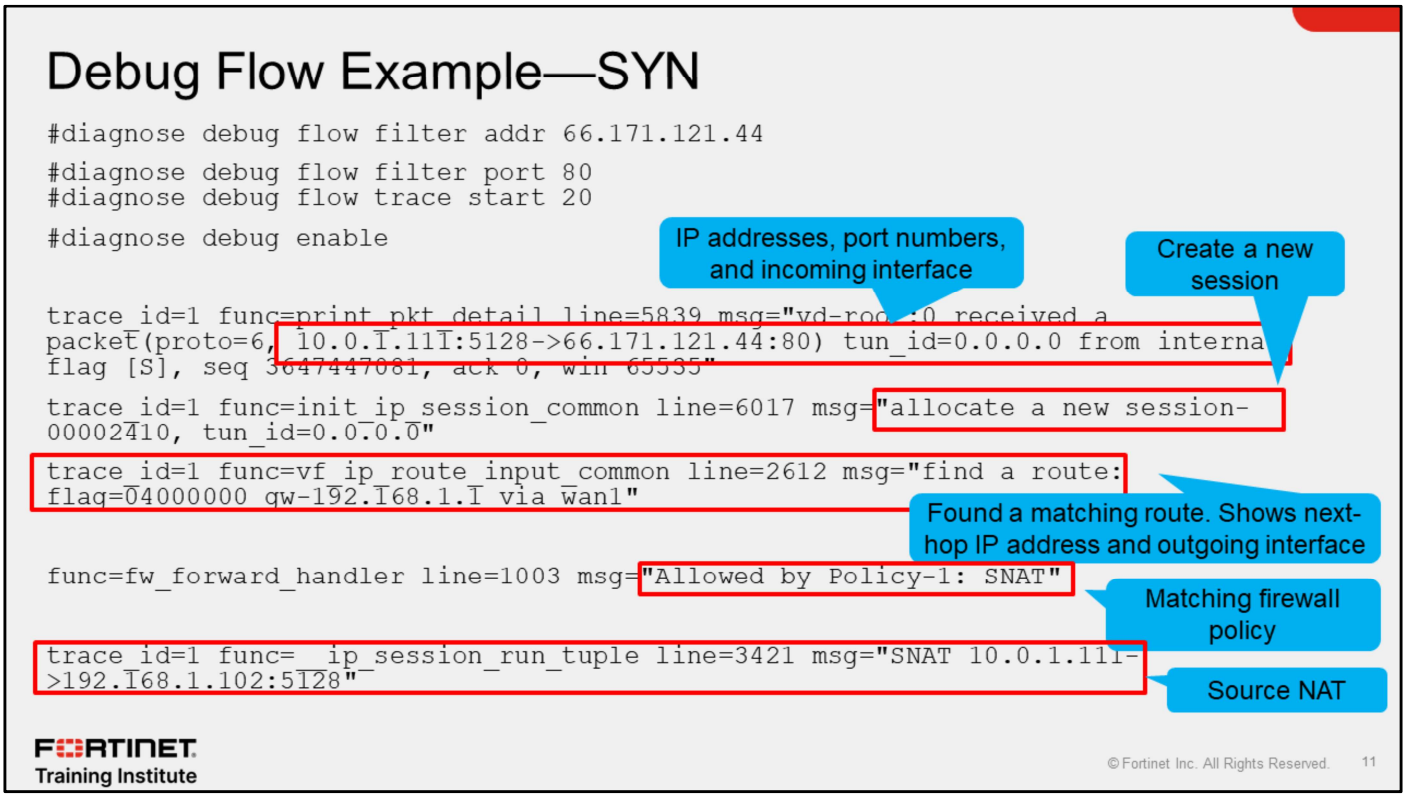
If you do not specify an option for the timestamp, the debug shows the time, in seconds, since it started running. You can prepend the local system time to easily correlate a packet with another recorded event.



If FortiGate is dropping packets, can a packet capture (sniffer) be used to identify the reason? To find the cause, you should use the debug (packet) flow.

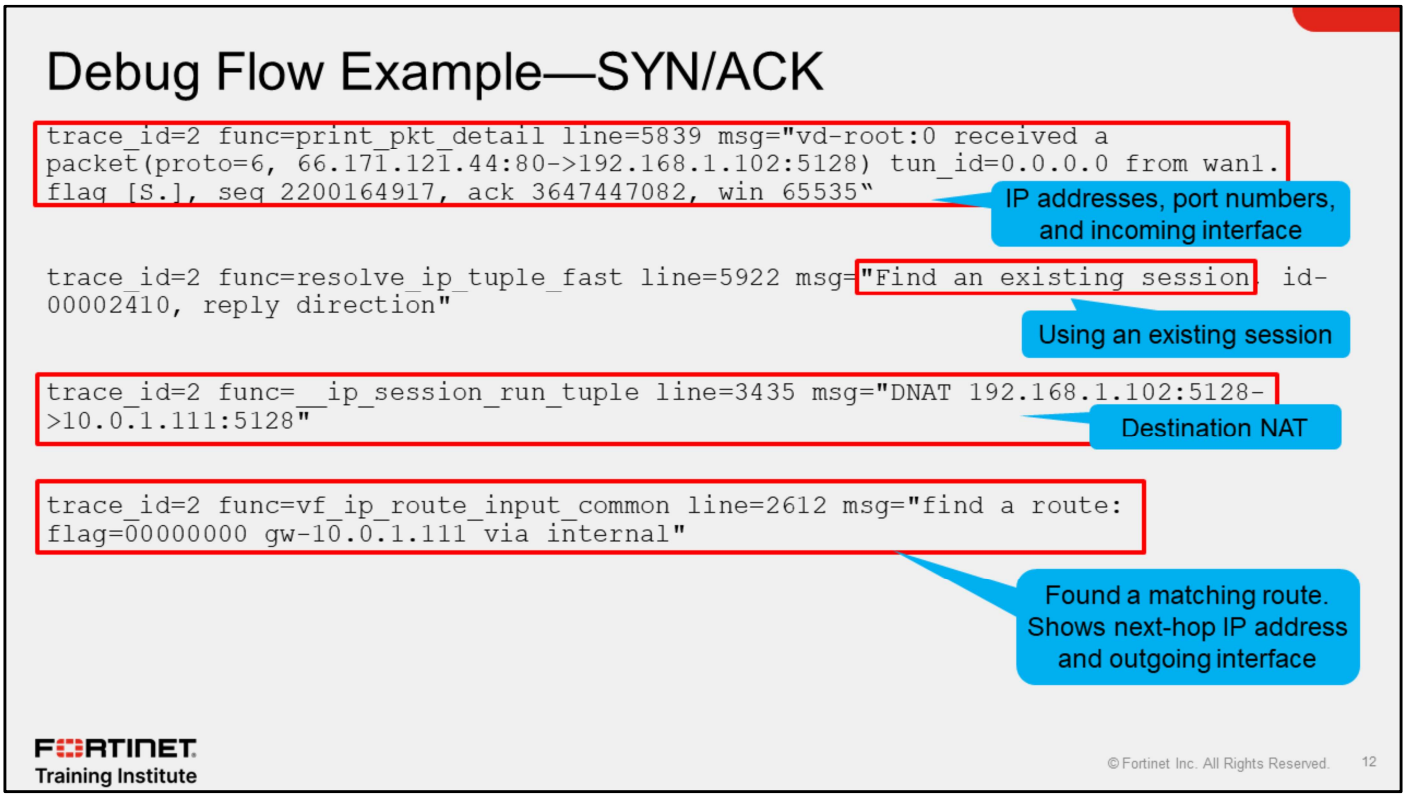
The debug flow shows, step-by-step, how the CPU is handling each packet.

To use the debug flow, follow these steps:
1. Define a filter.
2. Enable debug output.
3. Start the trace.
4. Stop the trace when it`s finished.



This slide shows an example of a debug flow output of the above `diagnose debug flow` commands,which captures the first packet of a TCP three-way handshake, the SYN packet. It shows:

- The packet arriving at FortiGate, indicating the source and destination IP addresses, port numbers, and incoming interface
- FortiGate creating a session, indicating the session ID
- The route to the destination, indicating the next-hop IP address and outgoing interface
- The ID of the policy that matches and allows this traffic
- How the source NAT is applied

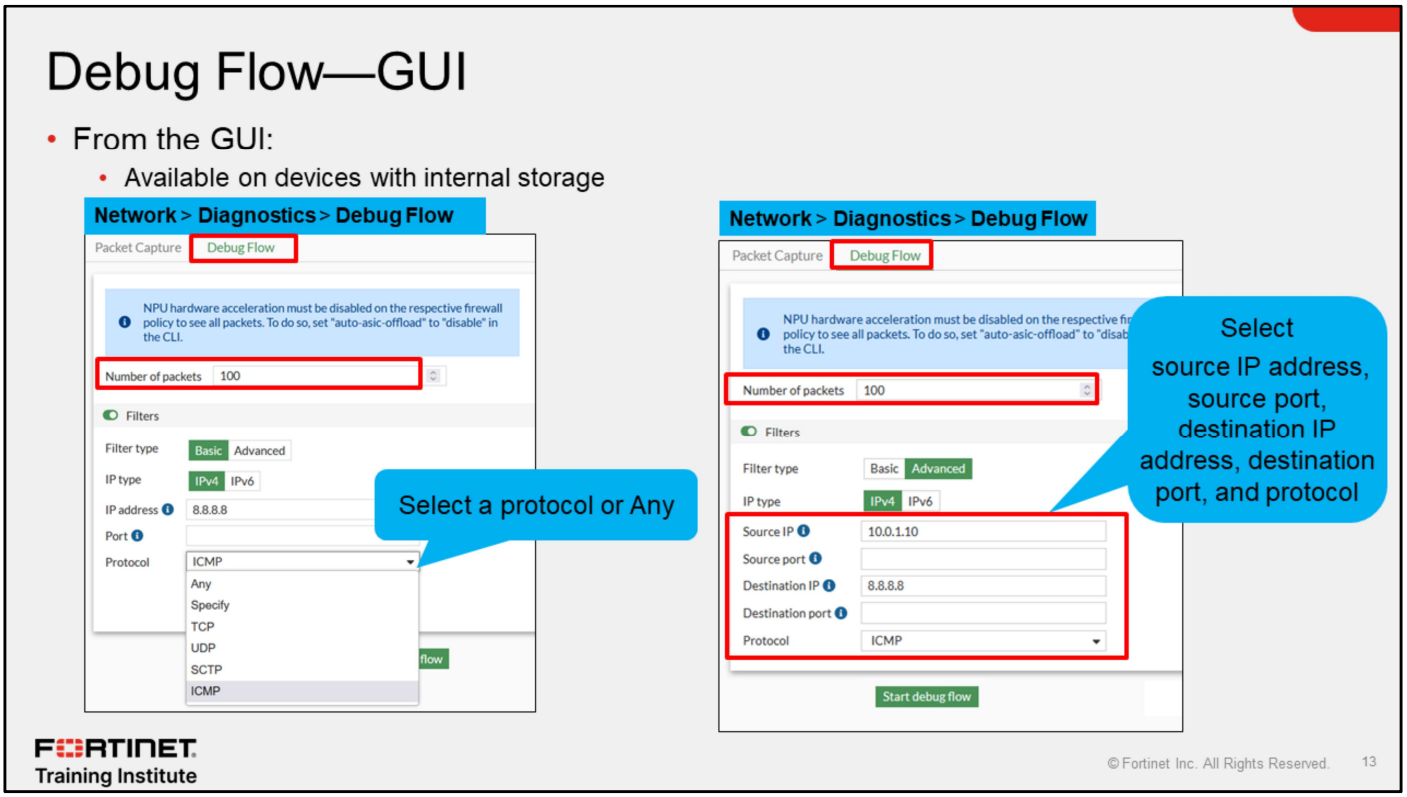


This slide shows the output for the SYN/ACK packet, which is from the same `diagnose debug` command shown on the previous slide. It shows:

- The packet arrival, indicating again the source and destination IP addresses, port numbers, and incoming interface
- The ID of the existing session for this traffic. This number matches the ID of the session created during the SYN packet. The ID is unique for each session, and useful to trace the request/reply packets of the session.
- How the destination NAT is applied
- The route to the destination, indicating again the next-hop IP address and outgoing interface.

If the packet is dropped by FortiGate, this debug shows the reason for that action.

This tool is useful for many other troubleshooting cases, including when you need to understand why a packet is taking a specific route, or why a specific NAT IP address is being applied.



The Debug Flow tool allows you to view debug flow output on the GUI in real time until you stop the debug process.

This tool helps you to examine the packet flow details directly on the GUI.

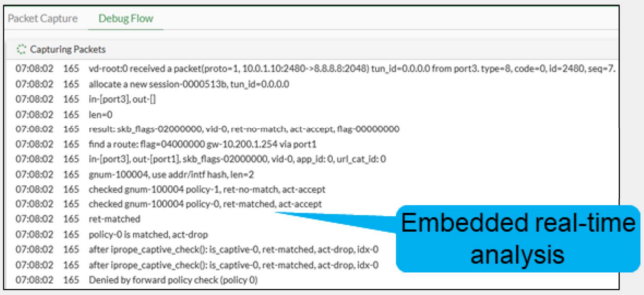
After you stop the debug flow, you can view the completed output, and filter it by time, message, or function. You can also export the output as a CSV file.

You can set up the Debug Flow tool to use either Basic or Advanced filter options. **Basic** allows you to filter using basic criteria such as host address, port number, and protocol name. **Advanced** allows you to filter by source IP address, source port, destination IP address, destination port, and protocol.

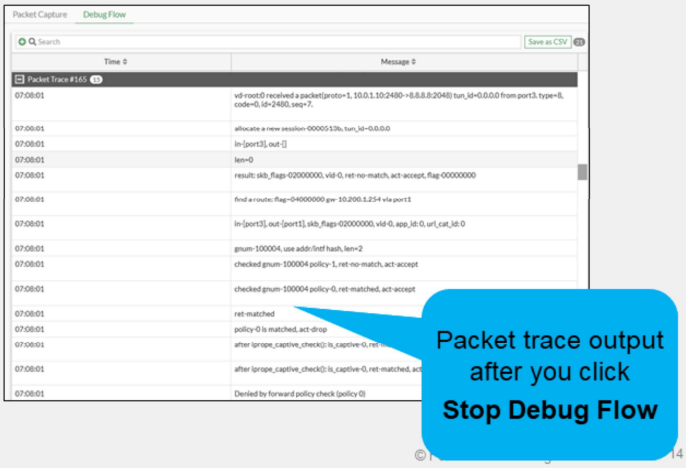
Debug Flow—GUI (Contd)

- Real–time analysis
  - Embedded real-time analysis page
  - Save and download the packet trace output as a CSV file

Real-time flow output



Packet Trace output

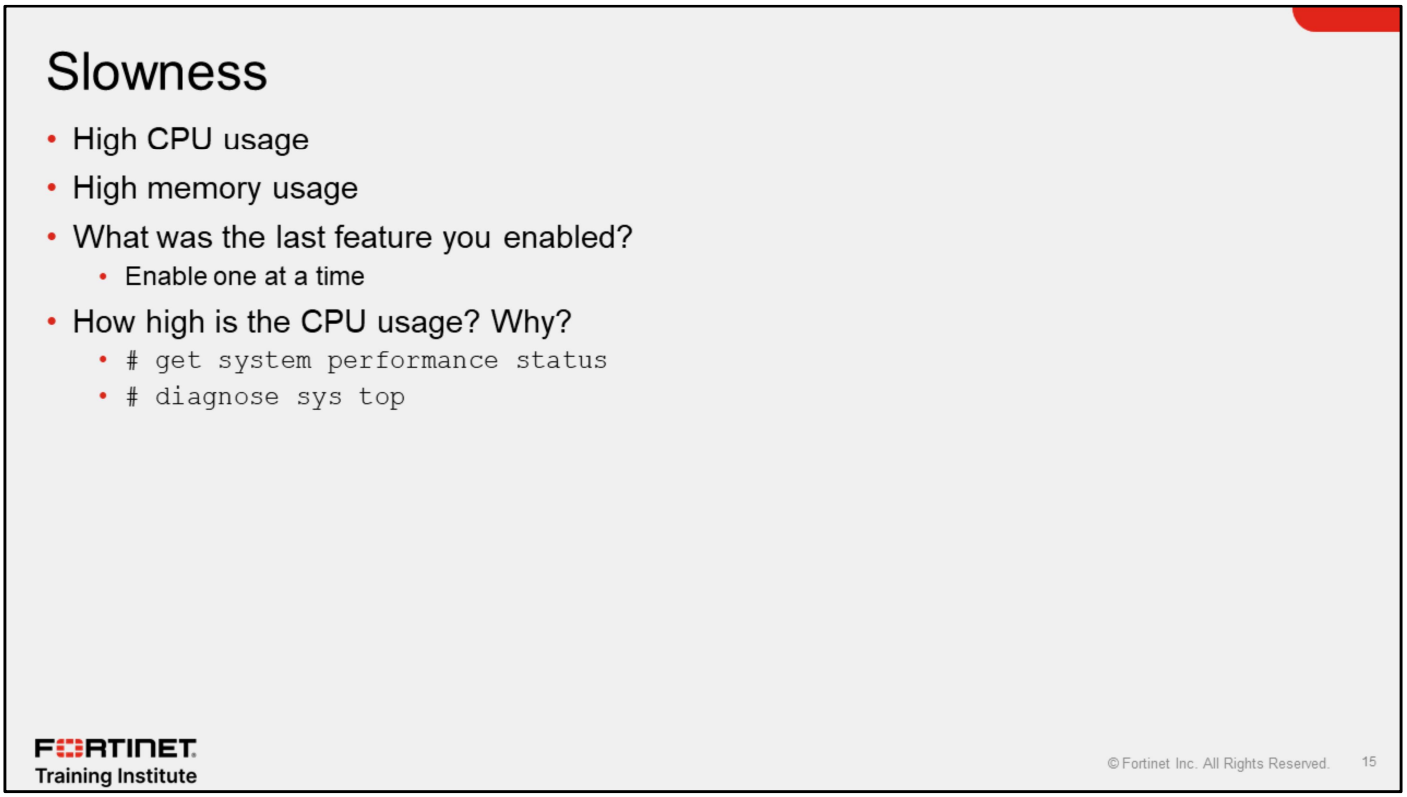


FORTINET Training Institute

After you start the debug flow, the GUI starts displaying the captured packets based on the filter.

When you stop the debug flow, FortiGate displays a packet trace output that you can download and save as a CSV file.

The main difference between these two outputs is that real-time messages are displayed for real-time analysis, but you can save the packet trace outputs and download them for future reference.



Not all problems are network connectivity failures. Sometimes, there are resource problems in the devices.

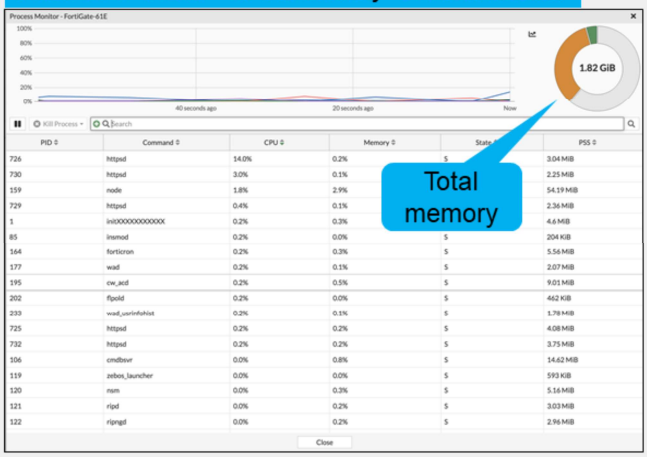
What else could cause latency? After you have eliminated problems with the physical media and bandwidth usage, you should check the FortiGate resources usage: CPU and memory.

If usage is high, there are tools that can identify which feature is consuming the most CPU. Additionally, you can troubleshoot faster if you know precisely which change (if any) corresponds with the time the problem began.

High CPU and Memory Troubleshooting—Process Monitor

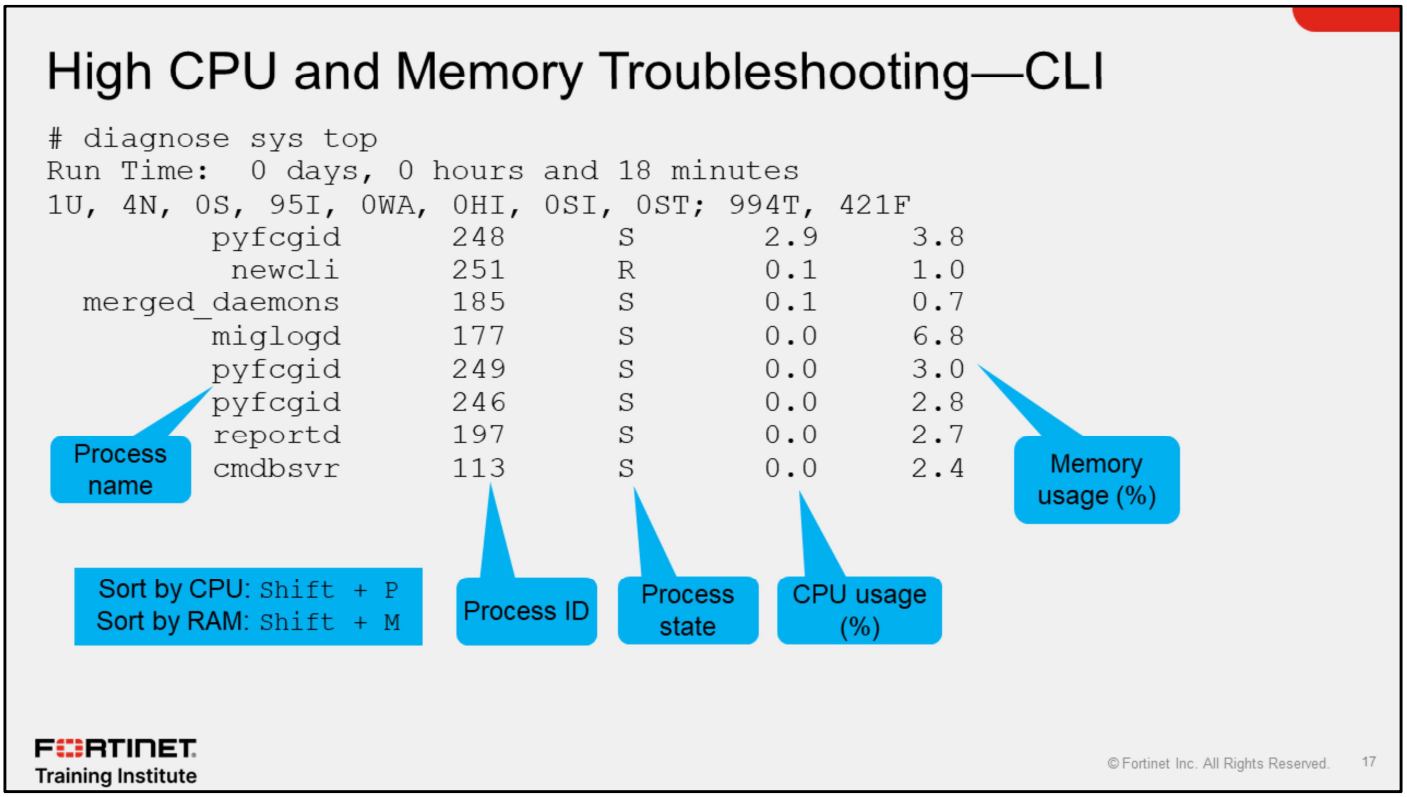
- Processing monitor displays running processes
- Each process shows CPU and memory usage
- Can apply filters and sorting to fine–tune results
- Allow terminating processes

Dashboard > Status > CPU or Memory > Process monitor



FORTINET Training Institute

You can use the process to view the running processes and their CPU and memory usage levels. You can apply filters, sort, and terminate processes in the process monitor.



Next, examine the output for `diagnose sys top`. It lists processes that use the most CPU or memory. Some common processes include:

- `ipsengine`, `scanunitd`, and other inspection processes
- `reportdk`
- `fgfmd` for FortiGuard and FortiManager connections
- `forticron` for scheduling
- Management processes (`newcli`, `miglogd`, `cmdb`, `sshd`, and `httpsd`)

To sort the list by highest CPU usage, press `Shift+P`. To sort by highest RAM usage, press `Shift+M`.

Memory Conserve Mode

- FortiOS protects itself when memory usage is high
  - It prevents using so much memory that FortiGate becomes unresponsive
- Three configurable thresholds:

Threshold	Definition	Default (% of total RAM)
Green	Threshold at which FortiGate exits conserve mode	82%
Red	Threshold at which FortiGate enters conserve mode	88%
Extreme	Threshold at which new sessions are dropped	95%

```
config system global
    set memory-use-threshold-red <percentage>
    set memory-use-threshold-extreme <percentage>
    set memory-use-threshold-green <percentage>
end
```

FORTINET Training Institute

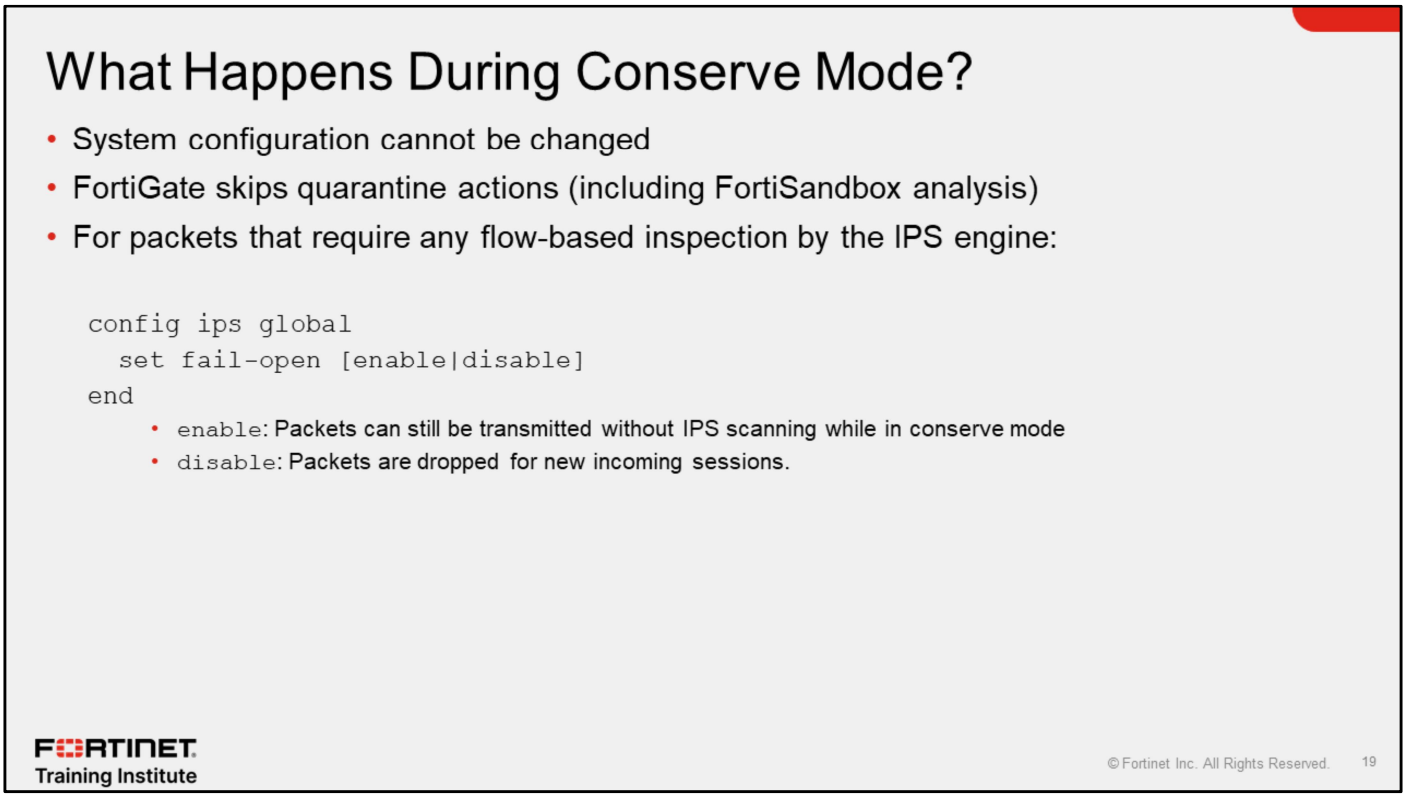
If memory usage becomes too high, FortiGate may enter into memory conserve mode. While FortiGate is in memory conserve mode, it must take action to prevent memory usage from increasing, which could cause the system to become unstable and inaccessible.

Memory conserve mode is never a desirable state because it impacts the user traffic.

Three different configurable thresholds define when FortiGate enters and exits conserve mode. If memory usage goes above the percentage of total RAM defined as the red threshold, FortiGate enters conserve mode. The actions that the device takes depend on the device configuration.

If memory usage keeps increasing, it might exceed the extreme threshold. While memory usage is above this highest threshold, all new sessions are dropped.

The third configuration setting is the green threshold. If memory usage goes below this threshold, FortiGate exits conserve mode.



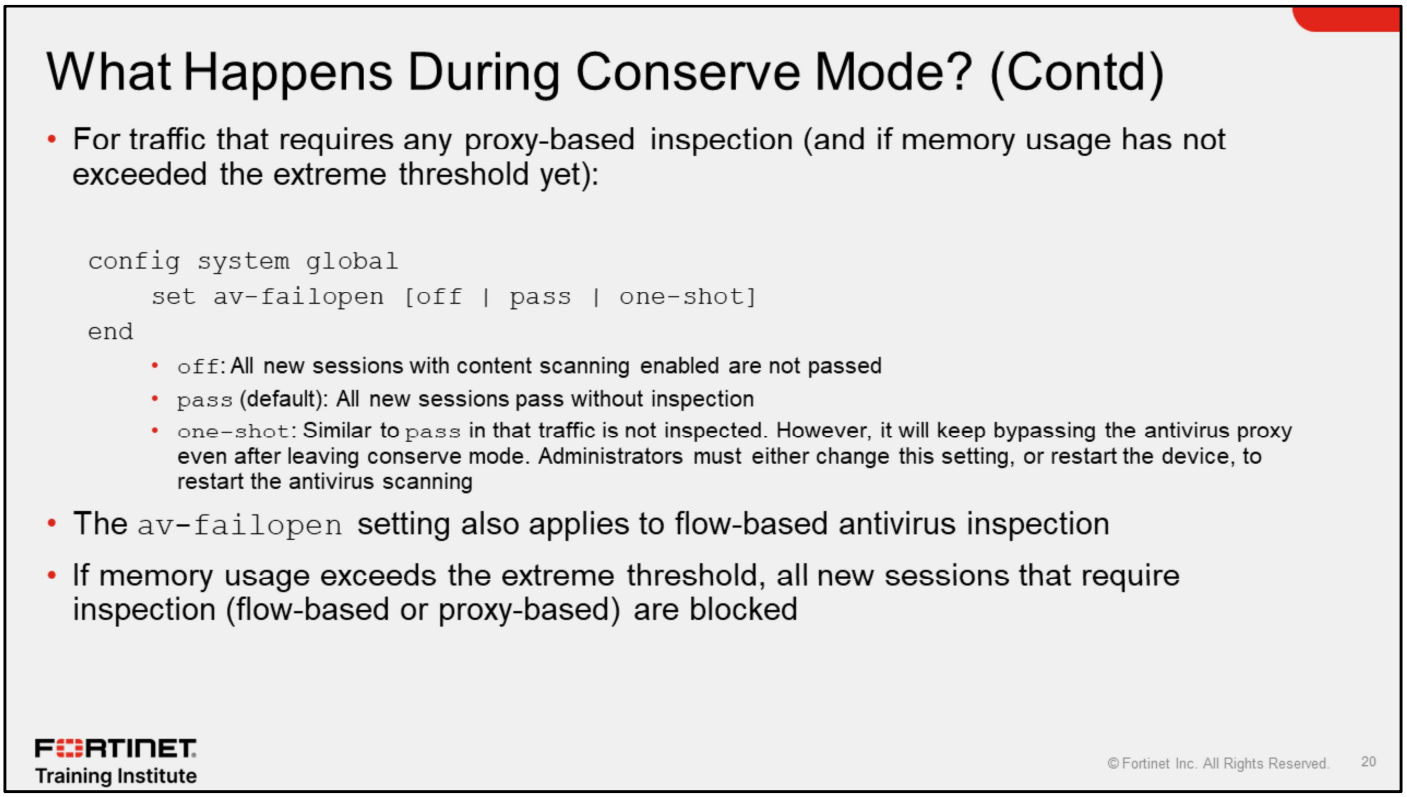
What actions does FortiGate take to preserve memory while in conserve mode?

- FortiGate does not accept configuration changes, because they might increase memory usage.
- FortiGate does not run any quarantine action, including forwarding suspicious files to FortiSandbox.
- You can configure the `fail-open` setting under `config ips global` to control how the IPS engine behaves when the IPS socket buffer is full.

If the IPS engine does not have enough memory to build more sessions, the `fail-open` setting determines whether the FortiGate should drop the sessions or bypass the sessions without inspection.

It is important to understand that the IPS `fail-open` setting is not just for conserve mode—it kicks in whenever IPS fails. Most failures are due to a high CPU issue or a high memory (conserve mode) issue. Enable the setting so that packets can still be transmitted while in conserve mode (or during any other IPS failure) but are not inspected by IPS. Disable the setting so that packets are dropped for new, incoming sessions.

Remember that the IPS engine is used for all types of flow-based inspections. The IPS engine is also used when FortiGate must identify the network application, regardless of the destination TCP/UDP port (for example, for application control). Note that NTurbo doesn't support the `fail-open` setting. If fail open is triggered, new sessions that would typically be accelerated with NTurbo are dropped, even if the `fail-open` setting is enabled.



The `av-failopen` setting defines the action that is applied to any proxy-based inspected traffic, while the unit is in conserve mode (and as long as the memory usage does not exceed the extreme threshold). This setting also applies to flow-based antivirus inspection. Three different actions can be configured:

- `off`: All new sessions with content scanning enabled are not passed but FortiGate processes the current active sessions.
- `pass` (default): All new sessions pass without inspection until FortiGate switches back to non-conserve mode.
- `one-shot`: Similar to `pass` in that traffic passes without inspection. However, it will keep bypassing the antivirus proxy even after it leaves conserve mode. Administrators must either change this setting, or restart the unit to restart the antivirus scanning

However, if the memory usage exceeds the extreme threshold, new sessions are always dropped, regardless of the FortiGate configuration.

System Memory Conserve Mode Diagnostics

```
# diagnose hardware sysinfo conserve
memory conserve mode:                          on
total RAM:                                     3040 MB
memory used:                                   2706 MB   89% of total RAM
memory freeable:                                334 MB   11% of total RAM
memory used + freeable threshold extreme:      2887 MB   95% of total RAM
memory used threshold red:                     2675 MB   88% of total RAM
memory used threshold green:                   2492 MB   82% of total RAM
```

Off = no conserve mode
on = conserve mode

FORTINET Training Institute

The `diagnose hardware sysinfo conserve` command is used to identify if a FortiGate device is currently in memory conserve mode.

Fail-Open Session Setting

- The following setting controls how FortiOS handles a session that is impacted by a unified threat management (UTM) scan error when doing http/mapi proxy or explicit webproxy

```
config system global
    set av-failopen-session [enable | disable]
```

- `enable` = Sessions are allowed
- `disable(default)` = Block all new sessions that require proxy-based inspection

FORTINET Training Institute

Another undesirable state for FortiGate is the fail-open session mode. This mode kicks in, not during a high-memory situation, but when a proxy on FortiGate runs out of available sockets to process more proxy-based inspected traffic.

If `av-failopen-session` is enabled, FortiGate allows all the sessions. Otherwise, by default, it blocks new sessions that require proxy-based inspection until new sockets become available.

Knowledge Check

1. Which information is displayed in the output of a debug flow?
   - ✓A. Incoming interface and matching firewall policy
   - B. Matching security profile and traffic log

2. When is a new TCP session allocated?
   - ✓A. When a SYN packet is received
   - B. When a SYN/ACK packet is received

3. Which action does FortiGate take during memory conserve mode?
   - ✓A. Configuration changes are not allowed.
   - B. Administrative access is denied.

Review

- ✓ Monitor for abnormal behavior, such as traffic spikes
- ✓ Diagnose problems at the physical and network layers
- ✓ Diagnose connectivity problems using sniffer and debug flow
- ✓ Diagnose resource problems, such as high CPU or memory usage
- ✓ Diagnose memory conserve mode

FORTINET Training Institute

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use diagnostic commands and tools, and learned more about FortiGate status and operation.