

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify the different operation modes for HA
- ✓ Understand the primary FortiGate election in an HA cluster
- ✓ Identify the primary and secondary device tasks in an HA cluster
- ✓ Identify what is synchronized between HA cluster members
- ✓ Configure session synchronization for seamless failover
- ✓ Identify the HA failover types
- ✓ Interpret how an HA cluster in active-active mode distributes traffic
- ✓ Implement virtual clustering per VDOM in an HA cluster
- ✓ Verify the normal operation of an HA cluster
- ✓ Configure an HA management interface
- ✓ Upgrade the HA cluster firmware



© Fortinet Inc. All Rights Reserved.

57

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

By mastering the objectives covered in this lesson, you learned about the fundamentals of FortiGate HA and how to configure it.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Infrastructure

Diagnostics

FortiOS 7.2

Last Modified: 13 June 2022

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

DO NOT REPRINT

© FORTINET

Lesson Overview



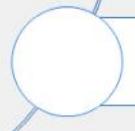
General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT

© FORTINET

General Diagnosis

Objectives

- Identify your network's normal behavior
- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers

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

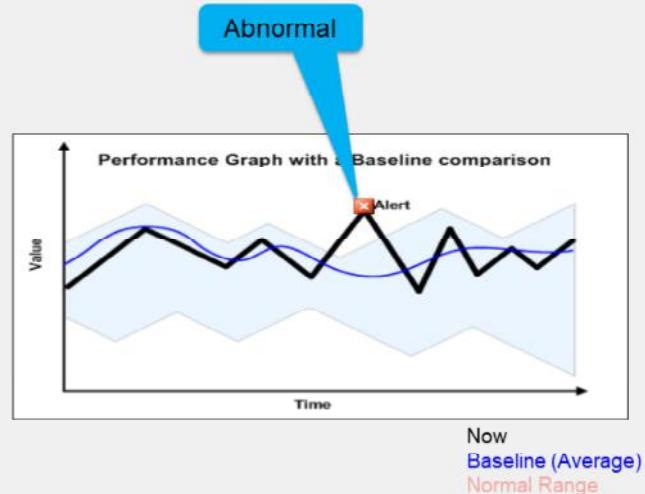
By demonstrating competence in general diagnosis, you will be able to discover general information about the status of FortiGate.

DO NOT REPRINT

© FORTINET

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



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.

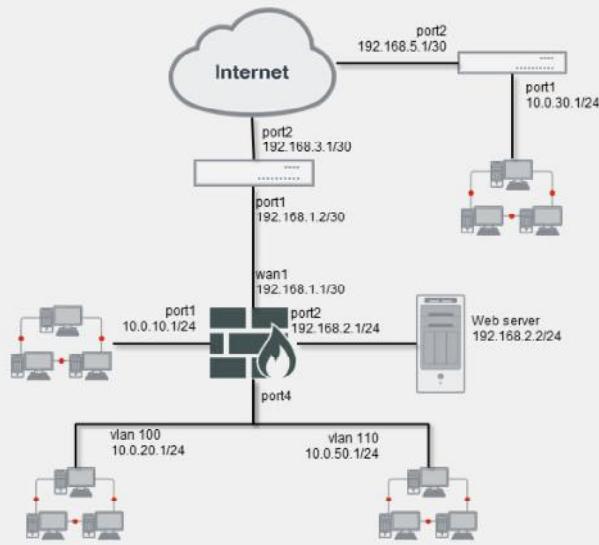
Normal is measured and defined in many ways. It can be performance: the expected CPU and memory utilization, bandwidth, and traffic volumes. But, it can also be your network topology: which devices are normally connected at each node. It is also behavior: traffic flow directions, which protocols are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

DO NOT REPRINT

© FORTINET

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



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:

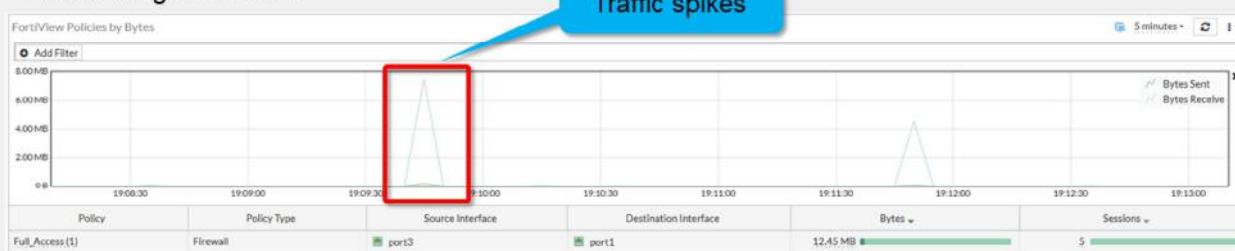
- Physical
- Logical

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.

DO NOT REPRINT
© FORTINET

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

© Fortinet Inc. All Rights Reserved.

6

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?

DO NOT REPRINT

© FORTINET

System Information

| FortiGate# set system status | | FortiGate # get system status | |
|--|--|--|--|
| Version: FortiGate-40F-364G v7.2.0,build1157,220331 (GA.F) | | Version: FortiGate-VM64-KVM v7.2.0,build1157,220331 (GA.F) | |
| Firmware Signature: certified | | Firmware Signature: certified | |
| Virus-DB: 90.01760(2022-04-26 16:26) | | Virus-DB: 81.00091(2020-10-14 16:20) | |
| Extended DB: 90.01760(2022-04-26 16:26) | | Extended DB: 81.00091(2020-10-14 16:20) | |
| AV AI/ML Model: 2.05403(2022-04-26 16:08) | | Extreme DB: 1.00000(2018-04-09 16:20) | |
| IPS-DB: 20.00304(2022-04-26 00:08) | | AV AI/ML Model: 0.00000(2001-01-01 02:30) | |
| IPS-ETDB: 0.00000(2001-01-01 00:00) | | IPS-DB: 6.00741(2015-12-01 02:30) | |
| APP-DB: 20.00304(2022-04-26 00:08) | | IPS-ETDB: 6.00741(2015-12-01 02:30) | |
| INDUSTRIAL-DB: 6.00741(2015-12-01 02:30) | | APP-DB: 6.00741(2015-12-01 02:30) | |
| IPS Malicious URL Database: 3.00331(2022-04-25 16:10) | | INDUSTRIAL-DB: 6.00741(2015-12-01 02:30) | |
| IoT-Detect: 0.00000(2001-01-01 00:00) | | IPS Malicious URL Database: 2.00797(2020-10-14 05:06) | |
| Serial-Number: FG40FITKXXXXXX | | IoT-Detect: 0.00000(2001-01-01 00:00) | |
| BIOS version: 05000004 | | Serial-Number: FGVM010000064692 | |
| System Part-Number: P24695-03 | | License Status: Valid | |
| Log hard disk: Not available | | VM Resources: 1 CPU/1 allowed, 2007 MB RAM | |
| Hostname: FortiGate | | Log hard disk: Available | |
| Private Encryption: Disable | | Hostname: FortiGate | |
| Operation Mode: NAT | | Private Encryption: Disable | |
| Current virtual domain: root | | Operation Mode: NAT | |
| Max number of virtual domains: 10 | | Current virtual domain: root | |
| Virtual domains status: 1 in NAT mode, 0 in TP mode | | Max number of virtual domains: 10 | |
| Virtual domain configuration: disable | | Virtual domains status: 1 in NAT mode, 0 in TP mode | |
| FIPS-CC mode: disable | | Virtual domain configuration: disable | |
| Current HA mode: standalone | | FIPS-CC mode: disable | |
| Branch point: 1157 | | Current HA mode: standalone | |
| Release Version Information: GA | | Branch point: 1157 | |
| System time: Wed Apr 27 12:43:57 2022 | | Release Version Information: GA | |
| Last reboot reason: power cycle | | FortiOS x86-64: Yes | |
| | | System time: Wed Apr 27 04:16:15 2022 | |
| | | Last reboot reason: shutdown | |

FOR**TI****NET**
Training Institute

© Fortinet Inc. All Rights Reserved.

7

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

DO NOT REPRINT
© FORTINET

Hardware Interface Information

```
FortiGate # get hardware nic <interface_name>
Description      :FortiASIC NP6XLITE Adapter
Driver Name     :FortiASIC NP6XLITE Driver
Board          :40Flif
id             :01if
oid            :64
netdev oid     :64
Current_Hwaddr  e0:23:ff:65:19:c8
Permanent_Hwaddr e0:23:ff:65:19:c8
===== Link Status =====
Admin          :up
netdev status   :up
autonego_setting :1
link_setting    :1
speed_setting   :1000
duplex_setting  :0
Speed          :1000
Duplex         :Full
link_status     :Up
```

FortiGate physical interface

```
===== Counters =====
Rx Pkts          :509427
Rx Bytes         :231539694
Tx Pkts          :513489
Tx Bytes         :132128420
Host Rx Pkts    :343935
Host Rx Bytes   :56092804
Host Tx Pkts    :365879
Host Tx Bytes   :51129548
Host Tx dropped  :0
FragTxCreate    :0
FragTxOk        :0
FragTxDrop      :0
```

At the physical layer, troubleshooting analyzes which ports are plugged in, media capacity, and negotiated speed and duplex mode.

At the data link layer, diagnostics often analyze how many frames are being dropped because of CRC errors or collisions.

The get hardware nic command is used to display the FortiGate interface hardware and status information. The output might vary depending on the model and NIC driver version.

DO NOT REPRINT
© FORTINET

Hardware Interface Information (Contd)

```
FortiGate # get hardware nic <interface_name>
```

```
Name: port1
Driver: virtio_net
Version: 1.0.0
Bus: 0000:00:03.0
Hwaddr: 02:09:0f:00:00:00
Permanent Hwaddr: 02:09:0f:00:00:00
State: up
Link: up
Mtu: 1500
Supported: 1000full 10000full
Advertised: 10000full
Speed: 10000full
Auto: disabled
RX Ring: 256
TX Ring: 256
Rx packets: 670785
Rx bytes: 949908714
Rx compressed: 0
Rx dropped: 0
...
```

```
...
Rx errors: 0
Rx Length err: 0
Rx Buf overflow: 0
Rx Crc err: 0
Rx Frame err: 0
Rx Fifo overrun: 0
Rx Missed packets: 0
Tx packets: 57752
Tx bytes: 4993066
Tx compressed: 0
Tx dropped: 0
Tx errors: 0
Tx Aborted err: 0
Tx Carrier err: 0
Tx Fifo overrun: 0
Tx Heartbeat err: 0
Tx Window err: 0
Multicasts: 0
Collisions: 0
```

The output on this slide shows the driver name, hardware address, administrative status, and link status, along with send and receive packets and errors.

DO NOT REPRINT
© FORTINET

ARP Table

```
# get system arp
```

| Address | Age (min) | Hardware Addr | Interface |
|--------------|-----------|-------------------|-----------|
| 10.0.1.10 | 0 | 00:0c:29:e0:c1:87 | port3 |
| 10.200.1.254 | 0 | 00:0c:29:1c:28:d7 | port1 |

Connecting device IP address
and MAC address

FortiGate Interface

If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table. The `get system arp` command is used for that purpose. It shows the FortiGate interface, IP address, and associated MAC address. This command lists the information for all external devices connected to the same LAN segments where FortiGate is connected. The current IP and MAC addresses of FortiGate are not included.

DO NOT REPRINT**© FORTINET**

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 <ip> IP address or domain name
# execute traceroute <dest> IP address or hostname
```



© Fortinet Inc. All Rights Reserved.

11

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.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which CLI command can be used to determine the MAC address of a FortiGate default gateway?
 A. get system arp
 B. get hardware nic

2. Which CLI command can be used to diagnose a physical layer problem?
 A. execute traceroute
 B. get hardware nic

DO NOT REPRINT

© FORTINET

Lesson Progress



General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Good job! You now understand general diagnostics.

Now, you will learn about debug flow.

DO NOT REPRINT

© FORTINET

Debug Flow

Objectives

- Diagnose connectivity problems using the debug flow

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

By demonstrating competence in the debug flow, you will be able to diagnose connectivity problems.

DO NOT REPRINT**© FORTINET**

Debug Flow

- Shows what the CPU is doing, step-by-step, with the packets
 - If a packet is dropped, it shows the reason
- Multi-step command
 1. Define a filter: `diagnose debug flow filter <filter>`
 2. Enable debug output: `diagnose debug enable`
 3. Start the trace: `diagnose debug flow trace start <xxxx> Repeat number`
 4. Stop the trace: `diagnose debug flow trace stop`

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.

DO NOT REPRINT
© FORTINET

Debug Flow Example—SYN

```
#diagnose debug flow filter addr 66.171.121.44
#diagnose debug flow filter port 80
#diagnose debug flow trace start 20
#diagnose debug enable

id=2 line=4677 msg="vd-root received a packet(proto=6,
10.0.1.10:49886->66.171.121.44:80) from port3, flag [S], seq 2176715501,
ack 0, win 8192"
id=2 line=4831 msg="allocate a new session-00007fc0"

id=2 line=2582 msg="find a route: flag=04000000
gw-10.200.1.254 via port1"

id=2 line=699 msg="Allowed by Policy-1: SNAT"
id=2 line=2719 msg="SNAT 10.0.1.10->10.200.1.1:49886"
```

IP addresses, port numbers,
and incoming interface

Create a new
session

Found a matching route.
Shows next-hop IP address
and outgoing interface

Matching firewall
policy

Source NAT

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

DO NOT REPRINT

© FORTINET

Debug Flow Example—SYN/ACK

```
id=2 line=4677 msg="vd-root received a packet(proto=6,  
66.171.121.44:80->10.200.1.1:49886) from port1. flag [S.],  
seq 3567496940, ack 2176715502, win 5840"
```

IP addresses, port numbers,
and incoming interface

```
id=2 line=4739 msg="Find an existing session,  
id-00007fc0,reply direction"
```

Using an existing session

```
id=2 line=2733 msg="DNAT 10.200.1.1:49886->10.0.1.10:49886"
```

Destination NAT

```
id=2 line=2582 msg="find a route: flag=00000000 gw-10.0.1.10 via port3"
```

Found a matching route.
Shows next-hop IP address
and outgoing interface.

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.

DO NOT REPRINT

© FORTINET

Debug Flow—GUI

- From the GUI:
 - Available on devices with internal storage

Network > Diagnostics > Debug Flow

Packet Capture Debug Flow

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

Filters

Filter type: Basic Advanced

IP type: IPv4 IPv6

IP address: 8.8.8.8

Port: 80

Protocol: ICMP

Any
Specify
TCP
UDP
SCTP
ICMP

Start debug flow

Network > Diagnostics > Debug Flow

Packet Capture Debug Flow

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

Filters

Filter type: Basic Advanced

IP type: IPv4 IPv6

Source IP: 10.0.1.10

Source port: 80

Destination IP: 8.8.8.8

Destination port: 80

Protocol: ICMP

Start debug flow

F
ORTINET

 Training Institute

© Fortinet Inc. All Rights Reserved.

18

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.

DO NOT REPRINT

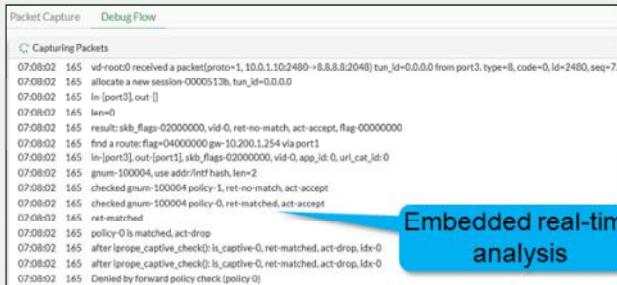
© FORTINET

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

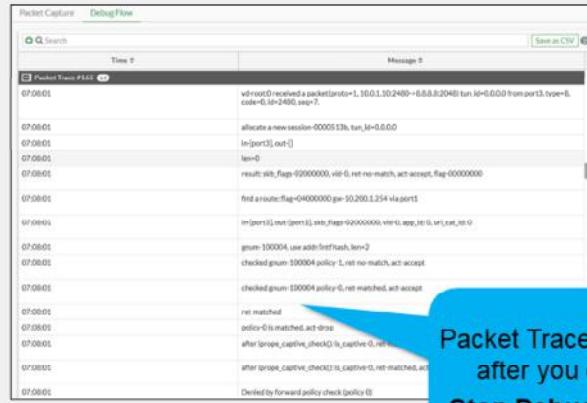


```

Packet Capture Debug Flow
Capturing Packets
07:08:02 165 vd-root0 received a packet(proto>1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.
07:08:02 165 allocate a new session 0000513b, tun_id=0.0.0.0
07:08:02 165 In-[port3],out []
07:08:02 165 len=0
07:08:02 165 result: skb_flags=02000000, vid=0, ret-no-match, act-accept, flag=00000000
07:08:02 165 find a route: flag=04000000 gw=10.200.1.254 via port1
07:08:02 165 In-[port3],out-[port1], skb_flags=02000000, vid=0, app_id=0, url_cat_id=0
07:08:02 165 grnum=100004, use addr/rnt hash, len=2
07:08:02 165 checked grnum=100004 policy=1, ret-no-match, act-accept
07:08:02 165 checked grnum=100004 policy=0, ret-matched, act-accept
07:08:02 165 ret-matched
07:08:02 165 policy=0 is matched, act-drop
07:08:02 165 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:02 165 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:02 165 Denied by forward policy check (policy 0)

```

Packet Trace output



```

Packet Capture Debug Flow
Packet Trace File
Message
07:08:01 vd-root0 received a packet(proto>1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.

07:08:01 allocate a new session 0000513b, tun_id=0.0.0.0
07:08:01 In-[port3],out []
07:08:01 len=0
07:08:01 result: skb_flags=02000000, vid=0, ret-no-match, act-accept, flag=00000000
07:08:01 find a route: flag=04000000 gw=10.200.1.254 via port1
07:08:01 In-[port3],out-[port1], skb_flags=02000000, vid=0, app_id=0, url_cat_id=0
07:08:01 grnum=100004, use addr/rnt hash, len=2
07:08:01 checked grnum=100004 policy=1, ret-no-match, act-accept
07:08:01 checked grnum=100004 policy=0, ret-matched, act-accept
07:08:01 ret-matched
07:08:01 policy=0 is matched, act-drop
07:08:01 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:01 after iprope_captive_check(): is_captive=0, ret-matched, act-drop, idx=0
07:08:01 Denied by forward policy check (policy 0)

```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

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.

DO NOT REPRINT

© FORTINET

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 allowed
 B. When a SYN/ACK packet is allowed

DO NOT REPRINT

© FORTINET

Lesson Progress



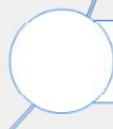
General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Good job! You now understand debug flow.

Now, you will learn about FortiGate CPU and memory diagnosis.

DO NOT REPRINT

© FORTINET

CPU and Memory

Objectives

- Diagnose resource problems, such as high CPU or memory usage
- Diagnose memory conserve mode
- Diagnose fail-open session mode

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

By demonstrating competence in CPU and memory, you will be able to diagnose the most common CPU and memory problems.

DO NOT REPRINT

© FORTINET

Slowness

- High CPU usage
- High memory usage
- What was the last feature you enabled?
 - Enable one at a time
- How high is the CPU usage? Why?
 - # get system performance status
 - # diagnose sys top 1



© Fortinet Inc. All Rights Reserved.

23

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.

DO NOT REPRINT**© FORTINET**

High CPU and Memory Troubleshooting

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
1U, 4N, 0S, 95I, 0WA, 0HI, 0SI, 0ST; 994T, 421F
  pyfcgid      248      S      2.9      3.8
  newcli       251      R      0.1      1.0
  merged_daemons 185      S      0.1      0.7
  miglogd      177      S      0.0      6.8
  pyfcgid      249      S      0.0      3.0
  pyfcgid      246      S      0.0      2.8
  reportd      197      S      0.0      2.7
  cmdbsvr      113      S      0.0      2.4
```

Process name

Memory usage (%)

Sort by CPU: Shift + P
Sort by RAM: Shift + M

Process ID

Process state

CPU usage (%)

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
- `reportd`
- `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.

DO NOT REPRINT

© FORTINET

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
```

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.

DO NOT REPRINT**© FORTINET**

What Happens During Conserve Mode?

- System configuration cannot be changed
- FortiGate skips quarantine actions (including FortiSandbox analysis)
- For packets that require any flow-based inspection by the IPS engine:
config ips global
 set fail-open {enable|disable}
end
 - enable: Packets can still be transmitted without IPS scanning while in conserve mode
 - disable: Packets are dropped for new incoming sessions, but FortiGate tries to make the existing sessions work in the same way as non-conserve mode



© Fortinet Inc. All Rights Reserved.

26

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, but allow FortiOS to try to make the existing sessions work in the same way as non-conserve mode.

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.

DO NOT REPRINT

© FORTINET

What Happens During Conserve Mode? (Contd)

- For traffic that requires any proxy-based inspection (and if memory usage has not exceeded the extreme threshold yet):

```
config system global
    set av-failopen [off | pass | one-shot]

end
    • off :All new sessions with content scanning enabled are not passed
    • pass (default): All new sessions pass without inspection
    • one-shot: Similar to pass in that traffic is not inspected. However, it will keep bypassing the antivirus proxy even after leaving conserve mode. Administrators must either change this setting, or restart the device, to restart the antivirus scanning
```

- The `av-failopen` setting also applies to flow-based antivirus inspection
- If memory usage exceeds the extreme threshold, all new sessions that require inspection (flow-based or proxy-based) are blocked

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:

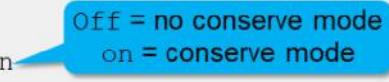
- `off`: All new sessions with content scanning enabled are not passed but FortiGate processes the current active sessions.
- `pass` (default): All new sessions pass without inspection until FortiGate switches back to non-conserve mode.
- `one-shot`: Similar to `pass` in that traffic passes without inspection. 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.

DO NOT REPRINT
© FORTINET

System Memory Conserve Mode Diagnostics

```
# diagnose hardware sysinfo conserve  
memory conserve mode:  
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
```

on  Off = no conserve mode
on = conserve mode



© Fortinet Inc. All Rights Reserved.

28

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

DO NOT REPRINT**© FORTINET**

Fail-Open Session Setting

- The following setting controls how FortiOS handles a session that is impacted by a 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 Inc. All Rights Reserved.

29

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.

DO NOT REPRINT

© FORTINET

Knowledge Check

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

2. Which threshold is used to determine when FortiGate enters conserve mode?
 A. Green
 B. Red

DO NOT REPRINT

© FORTINET

Lesson Progress



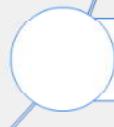
General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Good job! You now understand FortiGate CPU and memory diagnosis.

Now, you will learn about FortiGate firmware and hardware diagnosis.

DO NOT REPRINT

© FORTINET

Firmware and Hardware

Objectives

- Format the flash memory
- Load a firmware image from the BIOS menu
- Run hardware tests
- Display crash log information

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

By demonstrating competence in firmware and hardware, you will be able to diagnose the most common firmware and hardware problems.

DO NOT REPRINT**© FORTINET**

Access to BIOS Menu

FortiGate-81E-POE (12:25-10.04.2016)

Ver:05000003

Serial number: FG81EPxxxxxxxxxx

CPU: 1000MHz

Total RAM: 2 GB

Initializing boot device...

Initializing MAC... nplite#0

Please wait for OS to boot or press any key to display configuration menu

BIOS version. Options in the BIOS menu depend on the version

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,I,B,Q,or H:

Press any key at this prompt to enter the BIOS menu

On the FortiGate BIOS, administrators can run some operations over the flash memory and firmware images. To access the BIOS menu, you must reboot the device while connected to the console port. The booting process, at one point, shows the following message:

Press any key to display configuration menu

While this prompt is displayed, press any key to interrupt the booting process and display the BIOS menu. In the BIOS menu, you can see the options shown on this slide.

Firmware Installation From Console

Make sure that a TFTP server application is installed on your PC

Configure the TFTP server directory and copy the FortiGate firmware [image.out]

Connect your PC NIC to the FortiGate TFTP install interface

Select get firmware image from the BIOS menu

After reformatting the flash memory, you must install the firmware image from the BIOS menu. Follow these steps:

1. Run a TFTP server.
2. Configure the TFTP server with the folder where the firmware image file is stored.
3. Connect the PC Ethernet port to the FortiGate TFTP installation interface.
4. Select get firmware image from the BIOS menu.

The interface assigned as the TFTP installation interface depends on the model. However, and in most cases, it is either the *port1* or *internal* interface.

DO NOT REPRINT**© FORTINET**

Format Flash Memory

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Recommended for a clean
installation and problems possibly
related to corrupted firmware

Enter C,R,T,F,I,B,Q,or H: F

All data will be erased, continue: [Y/N]?

Formatting boot device...

.....

Format boot device completed.

CAUTION: Formatting the flash memory deletes the firmware,
configuration, and digital certificates

From the BIOS menu, select F to format the flash memory.

Doing this might be required if the firmware gets corrupted, or if the administrator wants to do a clean installation of new firmware. Keep in mind, though, that formatting the flash memory deletes any information stored on it, such as firmware images, configuration, and digital certificates.

DO NOT REPRINT**© FORTINET**

Configure TFTP Parameters

Enter C,R,T,F,I,B,Q,or H: C

[P]: Set firmware download port.
[D]: Set DHCP mode.
[I]: Set local IP address.
[S]: Set local subnet mask.
[G]: Set local gateway.
[V]: Set local VLAN ID.
[T]: Set remote TFTP server IP address.
[F]: Set firmware file name.
[E]: Reset TFTP parameters to factory defaults.
[R]: Review TFTP parameters.
[N]: Diagnose networking(ping).
[Q]: Quit this menu.
[H]: Display this list of options.

Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:



© Fortinet Inc. All Rights Reserved.

36

From the BIOS menu, select C to configure TFTP parameters. Use the menu options to configure parameters, such as local IP address, subnet mask, gateway address, and firmware file name.

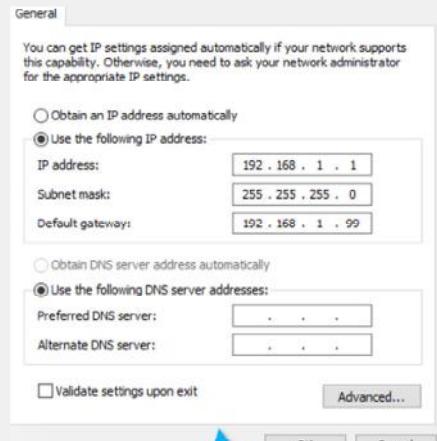
DO NOT REPRINT
© FORTINET

FortiGate and TFTP Server Configuration Settings

Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H: R

Image download port: MGMT
 DHCP status: Disabled
 Local VLAN ID: <NULL>
 Local IP address: 192.168.1.99
 Local subnet mask: 255.255.255.0
 Local gateway: 192.168.1.1
 TFTP server IP address: 192.168.1.1
 Firmware file name: image.out

FortiGate TFTP settings



TFTP server IP address configuration

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

37

Press R to review the TFTP configuration settings.

After you have configured the TFTP parameters, press Q to return to the main configuration menu.

DO NOT REPRINT
© FORTINET

BIOS Firmware Transfer

Enter C,R,T,F,I,B,Q,or H: T

CAUTION: Transferring a firmware image deletes the configuration and installs the factory default configuration

```
Enter TFTP server address []: 192.168.1.1
Enter local address []:192.168.1.99
Enter firmware image file name []:image.out
MAC:00090FC371BE
#####
Total 23299683 bytes data downloaded.
Verifying the integrity of the firmware image.

Total 40000kB unzipped.
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]? D
Programming the boot device now.
.
.
.
Reading boot image 1375833 bytes.
Initializing firewall...
System is started.
Formatting shared data partition ... done!
```



© Fortinet Inc. All Rights Reserved.

38

From the BIOS menu, press **T** to initiate the TFTP firmware transfer.

The BIOS requires you to enter:

- The IP address of the TFTP server
- The FortiGate IP address (it must be in the same class-C subnet as the TFTP server)
- The name of the firmware image

If everything is OK, you should see a series of pound signs, indicating that the device is downloading the image. The BIOS will then verify the integrity of the file and give you the following three options:

- Save it as the default firmware
- Save it as the backup firmware
- Run the image without saving it

If the firmware is going to be used in production, select the first option: Save it as the default firmware.

The last option (Run the image without saving it) allows you to run and test firmware without overwriting any existing firmware in the memory. After you have finished the tests and are ready to roll back the change, you must reboot the device, and the previously existing firmware will be used.

DO NOT REPRINT

© FORTINET

Hardware Tests

- Designed for both manufacturing testing and for end users to verify major hardware components:
 - CPU
 - RAM memory
 - Network interfaces
 - Hard disk
 - Flash memory
 - USB interface
 - Front panel LEDs
 - Wi-Fi
 - And so on



© Fortinet Inc. All Rights Reserved.

39

As with any other electronic device, damage to RAM can cause intermittent crashes.

If you suspect hardware failure, you can run hardware tests.

How do you run the hardware tests? It depends on the FortiGate model.

DO NOT REPRINT
© FORTINET

How to Run the Hardware Tests

- In some E, F, and D-series models, the hardware tests can be run directly from FortiOS
 - Can run a single test, or multiple tests
- For other models, a special HQIP image must be loaded using TFTP and run from the BIOS menu
 - Instructions: <https://support.fortinet.com/Download/HQIPImages.aspx>



© Fortinet Inc. All Rights Reserved.

40

For some FortiGate E, F, and D-series models, you can run the hardware tests directly from the FortiOS CLI.

For other models, you must download special HQIP hardware testing images from the Fortinet Technical Support website.

The steps for uploading the hardware test image are the same as the ones used for uploading a firmware image. You can run the hardware test image without saving it in the flash memory, so any existing firmware image won't be overwritten.

DO NOT REPRINT**© FORTINET**

FortiOS Hardware Tests Command

```
# diagnose hardware test suite all

- Please connect ethernet cables:
[WAN - Any of PORT1...PORT4]
To skip this test, please press 'N'.
Do you want to continue? (y/n) (default is n) N
Following tests will request you to check the colours of the system LEDs.
To skip this test, please press 'N'.
Do you want to continue? (y/n) (default is n) N
Following tests will request you to check the colours of the NIC LEDs.
- Please connect ethernet cables:
[WAN - Any of PORT1...PORT4]
To skip this test, please press 'N'.
Do you want to continue? (y/n) (default is n) N
Test Begin at UTC Time Wed May 05 21:08:53 2021
```



© Fortinet Inc. All Rights Reserved.

41

For some models, the command `diagnose hardware test suite all` runs the hardware tests from FortiOS. The hardware tests require user interaction while running. Users can skip some of the steps. Some tests require connecting external devices (such as USB flash drives) or network cables to FortiGate.

DO NOT REPRINT

© FORTINET

Crash Logs

- Inspect crash logs for debugging purposes
- Any time a process closes, it is recorded as *killed*
 - Some are normal (for example, closing `scanunit` to update definitions)

```
# diagnose debug crashlog history
Crash log interval is 3600 seconds
httpsd crashed 1 times. The last crash was at 2022-06-03 02:31:34

# diagnose debug crashlog read
97: 2022-05-24 01:59:31 from=license sn=FGVM0100000/5036 msg=License status changed to VALID
98: 2022-06-03 02:31:34 Signal <11> was sent to process <31308> by user <admin>
99: 2022-06-03 02:31:34 <31308> firmware FortiGate-VM64-KVM v7.2.0,build1157b1157,220331 (GA.F)
100: 2022-06-03 02:31:34 <31308> application httpsd
101: 2022-06-03 02:31:34 <31308> *** signal 11 (Segmentation fault) received ***
102: 2022-06-03 02:31:34 <31308> Register dump:
103: 2022-06-03 02:31:34 <31308> RAX: 0000000000000002b RBX: 0000000000000000
```

The https process was restarted
by the administrator

Another area you might want to monitor, purely for diagnostics, is the crash logs. Crash logs are available through the CLI.

Any time a process is closed for any reason, the crash log records this as a crash. Most of the logs in the crash log are normal. For example, any time the antivirus definitions package is updated, the `scanunit` process needs to close down in order to apply the new package. This is a normal shutdown. Some logs in the crash log shows they are initiated by a user, which indicates the administrator manually restarted a process.

Some logs in the crash log might indicate problems. For that reason, the crash logs are frequently requested by Fortinet Technical Support for troubleshooting purposes.

This slide shows the commands you have to use to get a crash log. The crashlog output shows the http process is restarted by the administrator.

Two commands can show information from the crash logs:

- `diagnose debug crashlog history` lists a summary of the processes that have crashed, how many crashes have happened, and the time of the last crash.
- `diagnose debug crashlog read` provides details about each crash, in addition to other system events, such as conserve mode entry and exit times.

DO NOT REPRINT**© FORTINET**

Conserve Mode Events in Crash Logs

- The crash log also records conserve mode events

- Entering:

```
12: 2021-04-06 14:10:16 logdesc="Kernel enters conserve mode" service=kernel
conserve-on free="127962
13: 2021-04-06 14:10:16 pages" red="128000 pages" msg="Kernel enters conserve
mode"
```

- Exiting:

```
14: 2021-04-06 14:19:55 logdesc="Kernel leaves conserve mode" service=kernel
conserve=exit
15: 2021-04-06 14:19:55 free="192987 pages" green="192000 pages" msg="Kernel
leaves conserve mode"
```

This slide shows the entries generated in the crash logs when FortiGate enters and exits memory conserve mode.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which types of information are stored in the crash log?
 A. Process crashes and conserve mode events
 B. Traffic logs and security logs

2. Which protocol is used to upload new firmware from the console?
 A. HTTP/HTTPS
 B. TFTP

DO NOT REPRINT

© FORTINET

Lesson Progress



General Diagnosis



Debug Flow



CPU and Memory



Firmware and Hardware

Congratulations! You have completed the lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify the normal behavior of your network
- ✓ Monitor for abnormal behavior, such as traffic spikes
- ✓ Diagnose problems at the physical and network layers
- ✓ Diagnose connectivity problems using the debug flow
- ✓ Diagnose resource problems, such as high CPU or memory usage
- ✓ Diagnose memory conserve mode
- ✓ Diagnose fail-open session mode
- ✓ Format the flash memory
- ✓ Load a firmware image from the BIOS menu
- ✓ Run hardware tests
- ✓ Display crash log information



© Fortinet Inc. All Rights Reserved.

46

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.



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.