

**DO NOT REPRINT****© FORTINET**

## Heartbeat Interface IP Addresses

- The cluster assigns addresses to heartbeat interfaces based on the serial number of each member
  - 169.254.0.1: for the highest serial number
  - 169.254.0.2: for the second highest serial number
  - 169.254.0.3: for the third highest serial number (and so on)
- Members keep their heartbeat IP addresses regardless of any change in their role (primary or secondary)
  - The IP address assignment may change only when a member leaves or joins the cluster
- The cluster uses the heartbeat IP addresses to:
  - Distinguish the members
  - Synchronize data with members



© Fortinet Inc. All Rights Reserved.

16

FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number. The IP address 169.254.0.2 is assigned to the device with the second highest serial number, and so on. The IP address assignment does not change when a failover happens. Regardless of the device role at any time (primary or secondary), its heartbeat IP address remains the same.

A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster. In those cases, the cluster renegotiates the heartbeat IP address assignment, this time taking into account the serial number of any new device, or removing the serial number of any device that left the cluster.

The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data.

**DO NOT REPRINT****© FORTINET**

## Heartbeat and Monitored Interfaces

- Heartbeat interfaces exchange sensitive data and may use a fair amount of bandwidth
  - If using a switch, use a dedicated switch or dedicated VLAN
  - Configure at least one heartbeat interface
    - It's a best practice to configure at least two for redundancy
    - Must be a physical port
- Monitored interfaces
  - Required for link failover
  - Choose interfaces that are critical for user traffic
    - Physical, redundant, and LAG interfaces are supported
  - Don't monitor heartbeat interfaces
  - Configure link failover after the cluster is formed
    - Prevents unwanted failover events during initial setup



© Fortinet Inc. All Rights Reserved.

17

Heartbeat interfaces exchange sensitive information about the cluster operation and may require a fair amount of bandwidth for data synchronization. For this reason, if you use a switch to connect the heartbeat interfaces, it's recommended that you use a dedicated switch or, at least, that you place the heartbeat traffic on a dedicated VLAN.

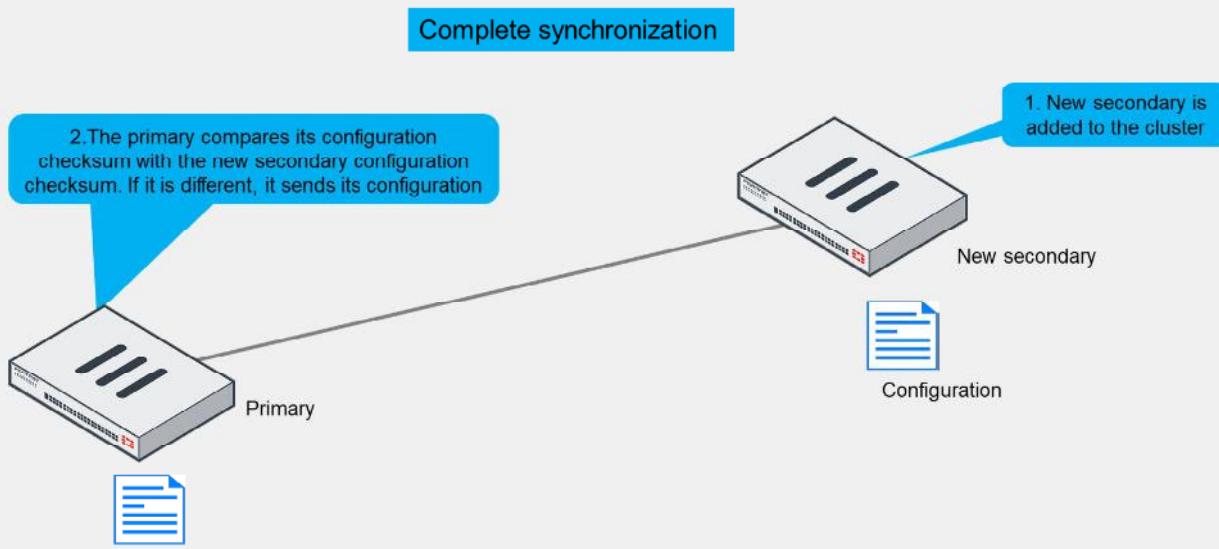
In addition, you must configure at least one port as a heartbeat interface, but preferably two for redundancy. For heartbeat interfaces, you can use physical interfaces only. That is, you can't use VLAN, IPsec VPN, redundant, or 802.3ad aggregate interfaces. You cannot use FortiGate switch ports either.

For link failover to work, you must configure one or more monitored interfaces. A monitored interface should be an interface whose failure has a critical impact in the network, and therefore, should trigger a device failover. For example, your LAN or WAN interfaces are usually good choices for monitored interfaces. Heartbeat interfaces, however, should not be configured as monitored interfaces because they are not meant to handle user traffic. Note that you can monitor physical ports, redundant interfaces, and link aggregation group (LAG) interfaces.

As a best practice, wait until a cluster is up and running and all interfaces are connected before configuring link failover. This is because a monitored interface can be disconnected during the initial setup and, as a result, trigger a failover before the cluster is fully configured and tested.

DO NOT REPRINT  
© FORTINET

## HA Complete Configuration Synchronization



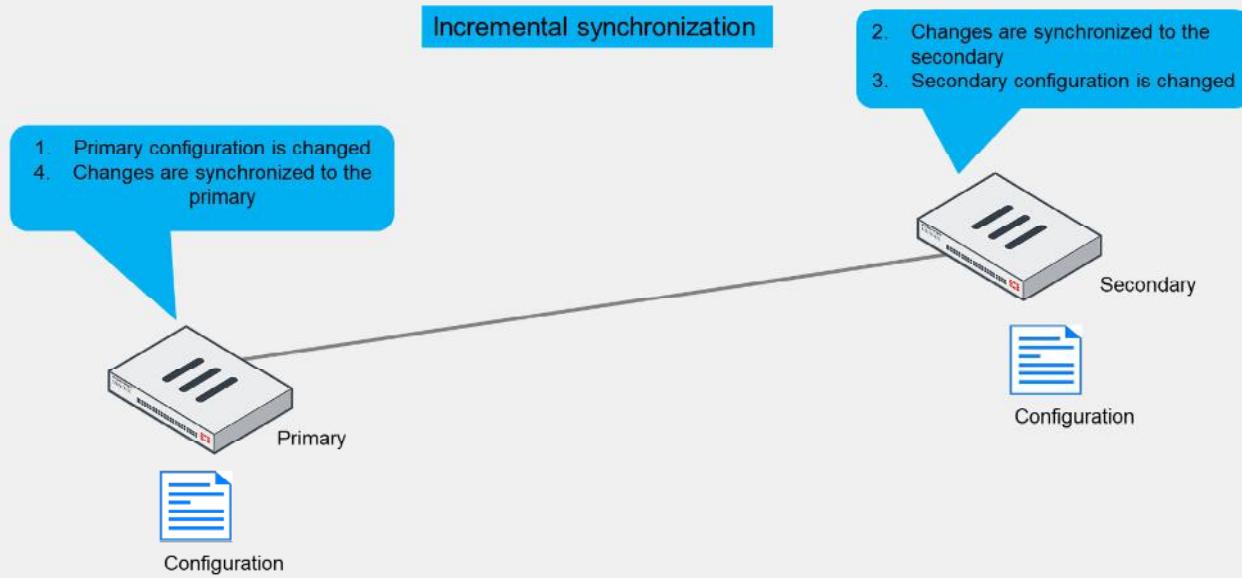
To prepare for a failover, an HA cluster keeps its configurations in sync. You will explore that now.

FortiGate HA uses a combination of both incremental and complete synchronizations.

When you add a new FortiGate to the cluster, the primary FortiGate compares its configuration checksum with the new secondary FortiGate configuration checksum. If the checksums don't match, the primary FortiGate uploads its complete configuration to the secondary FortiGate.

**DO NOT REPRINT**  
© FORTINET

## HA Incremental Configuration Synchronization



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

19

After the initial synchronization is complete, whenever a change is made to an HA cluster device's (primary or secondary) configuration, incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link. An HA synchronization process running on each cluster device receives the configuration change and applies it to the cluster device. For example, if you create a firewall address object, the primary doesn't resend its complete configuration—it sends only the new object.

Another example is in an HA setup with multiple VDOMs and virtual clustering, where the secondary device is acting as the primary FortiGate for VDOM2. Any changes made on VDOM2 is synchronized with the primary FortiGate.

**DO NOT REPRINT****© FORTINET**

## HA Configuration Synchronization

- Incremental synchronization also includes:
  - Dynamic data such as DHCP leases, FIB entries, IPsec SAs, session information, and so on
- Periodically, HA checks for synchronization
  - If the checksums match, the cluster is in sync
  - If the checksums don't match after five attempts, the secondary downloads the whole configuration from the primary



© Fortinet Inc. All Rights Reserved.

20

HA propagates more than just configuration details. Some runtime data, such as DHCP leases and FIB entries, are also synchronized.

By default, the cluster checks every 60 seconds to ensure that all devices are synchronized. If a secondary device is out of sync, its checksum is checked every 15 seconds. If the checksum of the out-of-sync secondary device doesn't match for five consecutive checks, a complete resynchronization to that secondary device is done.

**DO NOT REPRINT****© FORTINET**

## What Is Not Synchronized?

- These configuration settings are *not* synchronized between cluster members:
  - HA management interface settings
    - HA default route for the reserved management interface
  - In-band HA management interface
  - HA override
  - HA device priority
  - HA virtual cluster priority
  - FortiGate host name
  - Ping server HA priorities
    - The HA priority (ha-priority) setting for a ping server or dead gateway detection configuration
  - Licenses\*
    - FortiGuard, FortiCloud activation, and FortiClient licensing
  - Cache
    - FortiGuard Web Filtering and email filter, web cache, and so on
- The primary FortiGate synchronizes all other configuration settings

**Note:**

\* FortiToken licenses (serial numbers) are synchronized



© Fortinet Inc. All Rights Reserved.

21

Not all the configuration settings are synchronized. There are a few that are not, such as:

- System interface settings of the HA reserved management interface and the HA default route for the reserved management interface
- In-band HA management interface
- HA override
- HA device priority
- Virtual cluster priority
- FortiGate host name
- HA priority setting for a ping server (or dead gateway detection) configuration
- All licenses except FortiToken licenses (serial numbers)
- Cache

The primary FortiGate synchronizes all other configuration settings, including all other HA settings.

**DO NOT REPRINT****© FORTINET**

## Session Synchronization

- Provides seamless failover
  - Network applications don't need to restart connections
    - Minimum or no impact
- Firewall sessions
  - TCP sessions are synced by default
    - Unless they are subject to proxy inspection
  - Optionally, sync UDP and ICMP sessions
    - Usually not required
  - Multicast sessions are not synced
    - Multicast routes are
  - SIP sessions inspected by SIP ALG
- Local sessions
  - Not synced, must be restarted

- Configure session synchronization on the CLI:

```
config system ha
  set session-pickup enable
  set session-pickup-connectionless enable
  set multicast-ttl <5 - 3600 sec>
end
```

The time multicast routes remain in multicast forwarding table after failover (recommended = 120 seconds; default = 600 seconds)

Enable UDP and ICMP session synchronization

Enable non-proxy TCP session sync synchronization

Session synchronization provides seamless session failover. When the primary fails, the new primary can resume traffic for synchronized sessions without network applications having to restart the connections.

By default, the feature synchronizes TCP firewall sessions that are not subject to proxy-based inspection. An exception to this rule is TCP SIP sessions inspected by SIP ALG. Even though SIP ALG performs proxy-based inspection on SIP sessions, FortiGate can still synchronize such SIP sessions. Firewall sessions, also known as pass-through sessions, are user traffic sessions that travel across FortiGate. TCP firewall sessions that are subject to flow-based inspection or no inspection at all, are synchronized to secondary members.

You can also enable the synchronization of UDP and ICMP sessions. Although both protocols are connectionless protocols, FortiGate still allocates sessions for UDP and ICMP connections in its session table. Usually, the synchronization of UDP and ICMP sessions is not required because most UDP and ICMP connections can resume communication if their session information is lost.

For multicast traffic, FortiGate synchronizes multicast routes only. That is, FortiGate doesn't synchronize multicast sessions, which should be fine because multicast sessions are mostly UDP-based and, as mentioned before, UDP sessions can usually resume communication if their session information is lost. To ensure the multicast routing information across members is accurate, you can adjust the multicast time to live (TTL) timer. The timer controls how long the new primary keeps the synced multicast routes in the multicast forwarding table. The smaller the timer value, the more often the routes are refreshed, and so the more accurate the multicast forwarding table is. The recommended timer value is 120 seconds.

Local-in and local-out sessions, which are sessions that are terminated at or initiated by FortiGate, respectively, are not synchronized either. For example, BGP peerings, OSPF adjacencies, as well as SSH and HTTPS management connections must be restarted after a failover.

**DO NOT REPRINT****© FORTINET**

## IPsec and SSL VPN Synchronization

- FortiGate automatically synchronizes data for:
  - IPsec
    - IKE and IPsec SAs
      - Tunnels continue to be up after failover
    - Sessions over IPsec require you to enable session synchronization for session failover
  - SSL VPN web mode
    - Authentication information
    - Web mode users don't have to reauthenticate after failover
      - They must still restart connections over SSL VPN
- FortiGate doesn't synchronize data for SSL VPN tunnel mode users
  - Tunnel mode users must restart the SSL VPN tunnel after failover



© Fortinet Inc. All Rights Reserved.

23

The primary FortiGate automatically synchronizes all IKE and IPsec security associations (SAs) to secondary members. This enables the new primary to resume existing IPsec tunnels after a failover. Note that you must also enable session synchronization if you want the new primary to also resume existing IPsec sessions. Otherwise, after a failover, you must still restart existing TCP connections made over IPsec tunnels, even though the IPsec tunnels continue to be up on the new primary.

For SSL VPN, the primary FortiGate synchronizes the authentication information for SSL VPN web mode users only. That is, they are using SSL VPN web mode, the SSL VPN users don't have to authenticate again after a failover. However, the users must still restart the connections made using SSL VPN web mode to regain access to protected resources. Note that FortiGate doesn't synchronize any information for SSL VPN tunnel mode. That is, after a failover, SSL VPN tunnel mode users must restart their SSL VPN tunnel connection, as well as any connection made through the tunnel.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which information is synchronized in an HA cluster?  
 A. Firewall policies and objects  
 B. FortiGate host name
  
2. Which one of the following session types can be synchronized in an HA cluster?  
 A. BGP peerings  
 B. Non-proxy TCP sessions

**DO NOT REPRINT****© FORTINET**

## Lesson Progress

**HA Operation Modes****HA Cluster Synchronization****HA Failover and Workload****Monitoring and Troubleshooting**

Good job! You now understand HA cluster synchronization.

Now, you will learn about HA cluster failover protection types and workload for primary and secondary FortiGate devices in an HA cluster.

**DO NOT REPRINT****© FORTINET**

## HA Failover and Workload

### Objectives

- 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

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

By demonstrating competence in failover types and workload, you will be able to identify how enhanced reliability is achieved through HA failover protection. You will also learn about the distribution of traffic in an active-active cluster and distributing traffic using virtual clustering.

# DO NOT REPRINT

© FORTINET

## Failover Protection

- Types:
  - Device failover
    - The secondary devices stop receiving hello packets from the primary
  - Link failover
    - The link of one or more monitored interfaces goes down
  - Remote link failover
    - One or more interfaces are monitored using the link health monitor
    - The primary fails if the accumulated penalty of all failed interfaces reaches the configured threshold
  - Memory-based failover
    - Memory utilization on the primary exceeds the configured threshold and monitoring period
  - SSD failover
    - FortiOS detects extended filesystem (Ext-fs) errors in an SSD
    - Only available for devices with SSDs
- Identify failover protection type by looking at:
  - Event logs, SNMP traps, and alert email record failover events
- Enable session synchronization for seamless session failover



© Fortinet Inc. All Rights Reserved.

27

The most common types of failovers are device failovers and link failovers. However, you can also configure remote link failover and memory-based failover. When a failover event is triggered, the secondary devices elect a new primary.

A device failover is triggered when the secondary devices stop receiving the heartbeat hello packets from the primary.

A link failover occurs when the link status of a monitored interface on the primary FortiGate goes down. You can configure an HA cluster to monitor one or more interfaces. If a monitored interface on the primary FortiGate is unplugged, or its link status goes down, a new primary FortiGate is elected.

When you configure remote link failover, FortiGate uses the link health monitor feature to monitor the health of one or more interfaces against one or more servers that act as beacons. The primary FortiGate fails if the accumulated penalty of all failed interfaces reaches the configured threshold.

If you enable memory-based failover, an HA failover is triggered when the memory utilization on the primary FortiGate reaches the configured threshold for the configured monitoring period. You can also enable SSD failover, which triggers a failover if FortiOS detects Ext-fs errors on an SSD on the primary FortiGate.

There are multiple events that might trigger an HA failover, such as a hardware or software failure on the primary FortiGate or an issue on one of the interfaces on the primary. When a failover occurs, an event log is generated. Optionally, you can configure the device to also generate SNMP traps and alert emails.

Make sure that you enable session pickup for sessions you want to protect from a failover event. This way, the new primary can resume traffic for these sessions.

## Failover Protection Configuration

- Device failover

- Always enabled
- Adjust the failover time:

```
config system ha
  set hb-interval <1 - 20>
  set hb-interval-in-milliseconds 100ms | 10ms
  set hb-lost-threshold <1 - 60>
end

Number of failed heartbeats before device is dead
Heartbeat interval
Number of heartbeat interval units
```

- Default values vary by model

- FortiGate 2000E:
  - hb-interval: 2
  - hb-interval-in-milliseconds: 100ms
  - hb-lost-threshold: 6
  - Total failover time =  $2 \times 100\text{ ms} \times 6 = 1200\text{ ms}$

- Link failover

- Configure one or more monitored interfaces:

```
config system ha
  set monitor <interface1> <interface2> ...
end
```

- Supported interfaces:

- Physical
- Redundant
- LAG

When you configure HA, device failover is always enabled. However, you can adjust the settings that dictate the failover time. To speed up failover, you can reduce the values for all three settings shown on this slide. To reduce false positives, increase their values.

The default values for the three settings vary by model. For example, using the default values on a FortiGate 2000E model results in a device failover time of 1200 milliseconds (1.2 seconds). Note that the 10-millisecond heartbeat interval is supported on NP6 platforms only.

To configure link failover, you must configure one or more monitored interfaces, as shown on this slide. Note that you can configure only physical, redundant, and LAG interfaces as monitored interfaces.

**DO NOT REPRINT**  
**© FORTINET**

## Failover Protection Configuration (Contd)

- Remote link failover

- Configure link health monitor:

```
config system link-monitor
    edit "port1-ha"
        set srcintf "port1"
        set server "4.2.2.1" "4.2.2.2"
        set ha-priority 10
    next
end
```

Dead link nominal penalty—not synchronized

- Configure HA settings:

```
config system ha
    set pingserver-monitor-interface port1
    set pingserver-failover-threshold 5
    set pingserver-secondary-force-reset enable
    set pingserver-flip-timeout 30
end
```

Perform remote link failover on port1

Elect a new primary if the accumulated penalty reaches this threshold (5)

Elect a new primary again at the end of the flip timeout

The next primary election is in 30 minutes

This slide shows a configuration example for remote link failover.

First, you configure link health monitor, as shown in the *Routing* lesson. The `ha-priority` setting in the link health monitor configuration defines the penalty applied to the member after the link is detected as dead. Note that the `ha-priority` setting has local significance only, and therefore, is not synchronized to other members.

The next step is to configure the HA settings related to remote link failover. The configuration on this slide instructs FortiGate to perform remote link failover on port1 as follows:

- When port1 is detected as dead, the nominal penalty (10) is added to the global penalty, which is initially set to 0.
- If the accumulated penalty reaches the penalty threshold (5), then the cluster elects a new primary. A failover occurs when a secondary member has a lower accumulated penalty than the primary. If so, the secondary member with the lowest accumulated penalty becomes the new primary.
- The cluster doesn't elect a new primary again until the flip timeout (30 minutes) has passed.

If during the primary election, the accumulated penalty of all members is the same, then other criteria, such as monitored interfaces, priority, uptime, and so on, are used as tiebreakers to elect the new primary.

**DO NOT REPRINT**  
**© FORTINET**

## Failover Protection Configuration (Contd)

- Memory-based failover
  - Configure HA settings:

```
config system ha
  set memory-based-failover enable
  set memory-failover-threshold 70
  set memory-failover-monitor-period 30
  set memory-failover-sample-rate 2
  set memory-failover-flip-timeout 20
end
```

Enable memory-based failover

The memory usage threshold is 70%

Elect a new primary when the memory usage exceeds 70% for 30 seconds

Check memory usage every 2 seconds

The next primary election is in 20 minutes

The HA configuration shown on this slide instructs FortiGate to perform memory-based failover as follows:

- When the memory on the primary reaches the threshold (70%) and stays like that for 30 seconds, then the cluster elects a new primary.
- During primary election, a failover occurs when the memory usage on a secondary member is lower than the configured memory threshold (70%). If so, the secondary member becomes the new primary.
- The cluster doesn't elect a new primary again until the flip timeout (20 minutes) has passed.
- Each member in the cluster checks its memory usage every 2 seconds.

If during the primary election, the memory usage of all members are below or above the threshold, then other criteria, such as monitored interfaces, priority, uptime, and so on, are used as tiebreakers to elect the new primary.

**DO NOT REPRINT****© FORTINET**

## Failover Protection Configuration (Contd)

- SSD failover

- Configure HA settings:

```
config system ha  
    set ssd-failover enable  
end
```

Enable memory-based failover



© Fortinet Inc. All Rights Reserved.

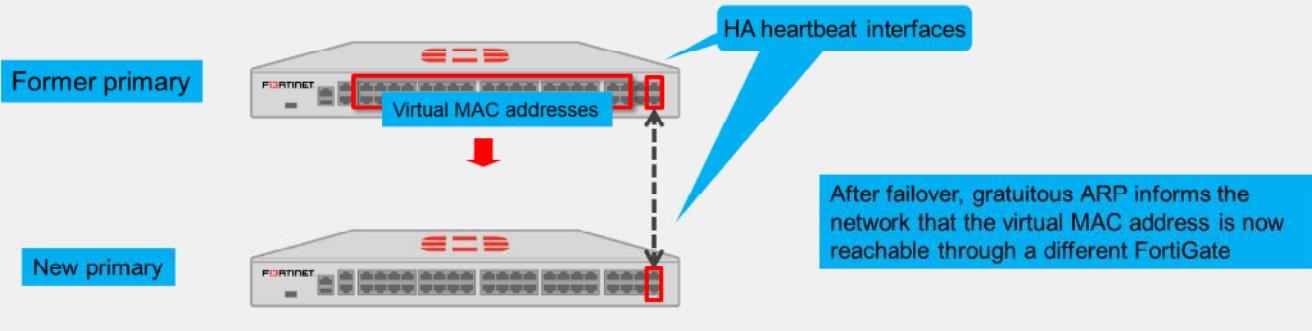
31

The HA configuration shown on this slide instructs FortiGate to perform a failover when any of the SSD disks on the primary FortiGate report Ext-fs errors. Note that this feature is supported only on FortiGate models with SSD disks.

**DO NOT REPRINT**  
**© FORTINET**

## Virtual MAC Addresses and Failover

- On the primary, each interface is assigned a virtual MAC address
  - HA heartbeat interfaces are not assigned a virtual MAC address
- Upon failover, the newly elected primary adopts the same virtual MAC addresses as the former primary



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

32

To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses. When a primary joins an HA cluster, each interface is assigned a virtual MAC address. The HA group ID is used in the creation of virtual MAC addresses assigned to each interface. So, if you have two or more HA clusters in the same broadcast domain, and using the same HA group ID, you might get MAC address conflicts. For those cases, it is strongly recommended that you assign different HA group IDs to each cluster.

Through the heartbeats, the primary informs all secondary devices about the assigned virtual MAC address. Upon failover, a secondary adopts the same virtual MAC addresses for the equivalent interfaces.

The new primary broadcasts gratuitous ARP packets, notifying the network that each virtual MAC address is now reachable through a different switch port.

Note that the MAC address of a reserved HA management interface is not changed to a virtual MAC address. Instead, the reserved management interface keeps its original MAC address.

**DO NOT REPRINT****© FORTINET**

## Failure of a Secondary FortiGate

- Active-passive HA cluster
  - The primary updates the list of available secondary FortiGate devices
- Active-active HA cluster
  - The primary updates the list of available secondary FortiGate devices and redistributes sessions to prevent failed secondary devices



© Fortinet Inc. All Rights Reserved.

33

As you learned earlier in this lesson, if a primary fails, a new primary is elected. But what happens if a secondary FortiGate device fails? It depends on the HA mode.

In an active-passive cluster, the primary only updates its list of available secondary FortiGate devices. It also starts monitoring for the failed secondary, waiting for it to come online again.

However, in an active-active cluster, the secondary devices can handle traffic. So, the primary (which tracks and assigns sessions to each secondary) must not only update its list of available secondary FortiGate devices, but also reassign sessions from the failed FortiGate to a different secondary FortiGate.

**DO NOT REPRINT****© FORTINET**

## Workload

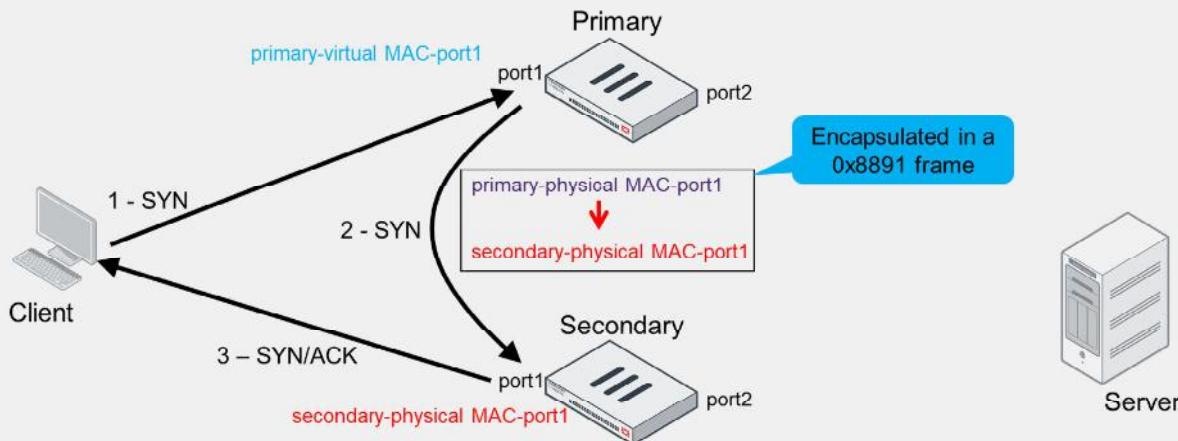
- Active-passive HA cluster
  - The primary receives and processes all traffic
  - The secondary waits passively
- Active-active HA cluster
  - The primary receives all traffic and redirects some proxy-based sessions to secondary devices
    - Enable `load-balance-all` to force distribution of all sessions

This is how the workload is distributed between roles, depending on the HA mode.

Notice that traffic workload is distributed in active-active mode only. However, keep in mind that by default, only sessions that are subject to proxy inspection are distributed to secondary devices. If you want to force the distribution of sessions that are subject to flow inspection or no inspection at all, then you must enable the `load-balance-all` setting under HA configuration—this setting is disabled by default.

**DO NOT REPRINT**  
**© FORTINET**

## Active-Active Traffic Flow (Proxy Inspection)



1. srcMAC client, dstMAC **primary-virtual MAC-port1**, TCP SYN dport 80
2. srcMAC primary-physical MAC-port1, dstMAC **secondary-physical MAC-port1**, TCP SYN dport 80 (Ethernet frame 0x8891)
3. srcMAC **secondary-physical MAC-port1**, dstMAC client, TCP SYN/ACK sport 80

In active-active mode, the following occurs:

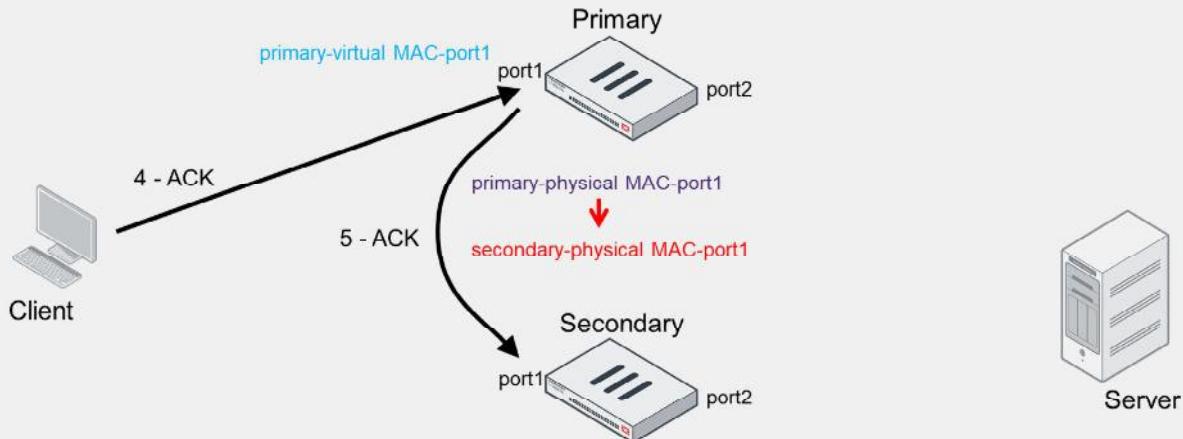
- The traffic destined to the cluster is sent to the primary. Because all network ports on the primary—except the heartbeat ports—are assigned a virtual MAC address, the traffic is destined to the virtual MAC address of the receiving port on the primary FortiGate.
- For traffic that is distributed to the secondary, the traffic destined to the endpoints is sent by the secondary. The traffic is sourced from the physical MAC address of the egressing port on the secondary.

This slide shows the flow for distributed traffic that is subject to proxy inspection:

- The client sends a SYN packet, which is forwarded to port1 on the primary. The packet destination MAC address is the virtual MAC address on port1.
- The primary forwards the SYN packet to the selected secondary. In this example, the source MAC address of the packet is changed to the physical MAC address of port1 on the primary and the destination MAC address to the physical MAC address of port1 on the secondary. This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic.
- The secondary responds to the client with a SYN/ACK packet that contains the physical MAC address of port1 on the secondary as the source and the MAC address of the client as the destination.

**DO NOT REPRINT**  
**© FORTINET**

## Active-Active Traffic Flow (Proxy Inspection) (Contd)

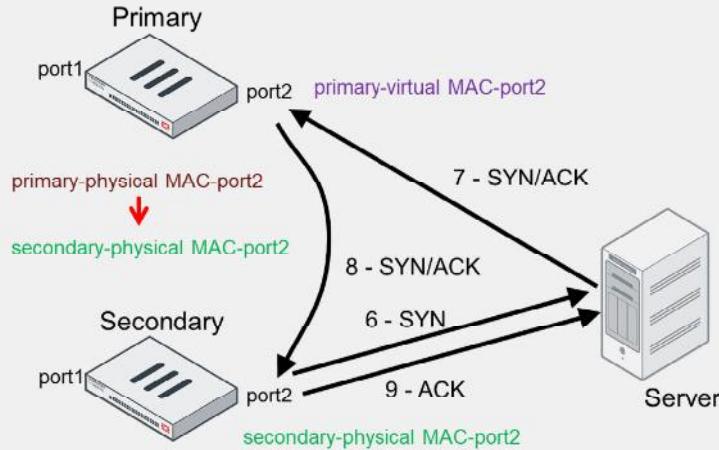


- 4. srcMAC client, dstMAC **primary-virtual MAC-port1**, TCP ACK dport 80
- 5. srcMAC **primary-physical MAC-port1**, dstMAC **secondary-physical MAC-port1**, TCP ACK dport 80

4. The client acknowledges the SYN/ACK by sending an ACK to the cluster. The ACK packet is destined to port1 on the primary.
5. The primary receives the packet and knows that it matches a session that was previously distributed to the secondary. As a result, the primary forwards the ACK packet to the corresponding secondary FortiGate. The packet is sourced from the physical MAC address of port1 on the primary and destined to the physical MAC address of port1 on the secondary. The three-way handshake on the client side is complete.

**DO NOT REPRINT**  
**© FORTINET**

## Active-Active Traffic Flow (Proxy Inspection) (Contd)



- 6. srcMAC **secondary physical MAC-port2**, dstMAC server, TCP SYN dport 80
- 7. srcMAC server, dstMAC **primary-virtual MAC-port2**, TCP SYN/ACK sport 80
- 8. srcMAC **primary-physical MAC-port2**, dstMAC **secondary-physical MAC-port2**, TCP SYN/ACK sport 80
- 9. srcMAC **secondary-physical MAC-port2**, dstMAC server, TCP ACK dport 80

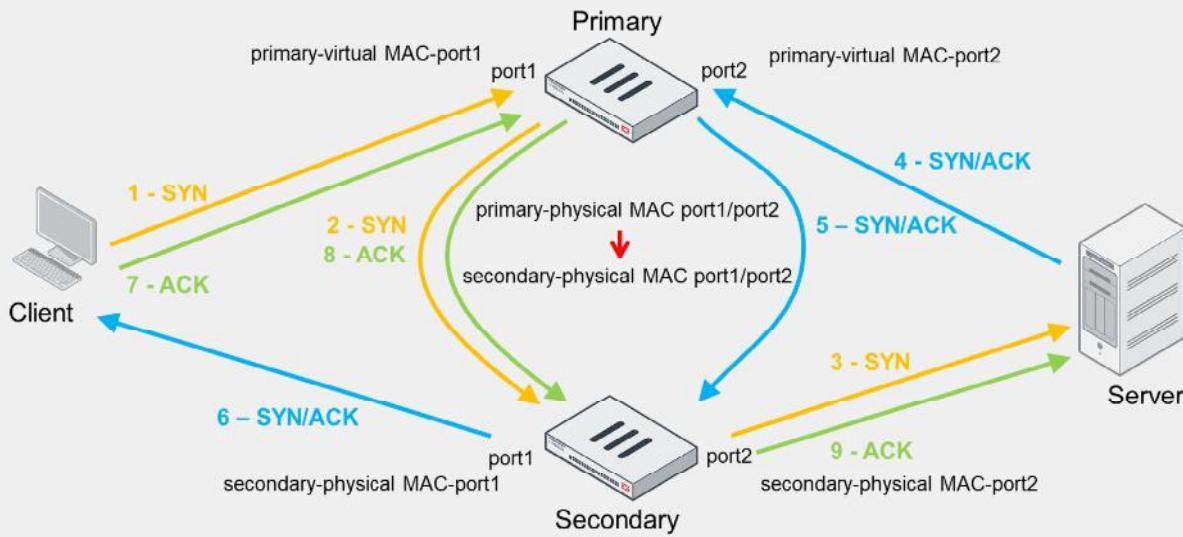
6. The secondary starts the connection with the server by sending a SYN packet using the physical MAC address of port2 as the source. Note that FortiGate contacts the server after it finishes the three-way handshake to the client, not before. The same behavior is seen when FortiGate operates in standalone mode and performs proxy-based inspection.
7. The SYN/ACK packet from the server is sent to port2 on the primary. The destination MAC address is the virtual MAC address of port2.
8. The primary receives the packet and knows that it matches a session that was previously distributed to the secondary. The primary forwards the SYN/ACK packet to the corresponding secondary FortiGate. The packet is sourced from the physical MAC address of port2 on the primary and destined to the physical MAC address of port2 on the secondary.
9. The secondary responds to the server with an ACK packet that contains the physical MAC address of port2 on the secondary as the source and the MAC address of the server as the destination.

The three-way handshake on the server side is also complete. From now on, packets that the client sends follow the same flow. For example, an HTTP GET request packet from the client is first received by the primary, which then forwards it to the secondary for proxy-based inspection. If the packet is allowed, the secondary forwards the packet to the server. Any server response packets to the client HTTP GET request are sent to the primary, which then forwards the packets to the secondary for inspection, and so on.

Note that the goal of active-active mode is to leverage unused CPU and memory resources on secondary devices. The intention is not really to load balance traffic. In fact, because the traffic from endpoints is always sent to the primary, you usually see more traffic on the primary than any secondary devices.

**DO NOT REPRINT**  
**© FORTINET**

## Active-Active Traffic Flow (No Proxy Inspection)



When there is no proxy inspection, that is, when traffic is either subject to flow inspection or no inspection at all, sessions are distributed to the secondary FortiGate only if you enable the `load-balance-all` setting (which is disabled by default) under HA configuration. In addition, as in proxy inspection, you will also see the following behavior:

- Traffic sourced from the client or server and destined to the FortiGate cluster is sent to the primary FortiGate. The source and destination MAC addresses are the endpoint (client or server) and the primary FortiGate virtual MAC address, respectively.
- The primary FortiGate may, in turn, forward the traffic to the secondary if the session is to be load balanced.
- When distributing the traffic to the secondary, FortiGate uses the physical MAC addresses of the primary and secondary devices interfaces as the source and destination MAC addresses, respectively.
- If traffic is load balanced to the secondary FortiGate, any traffic sourced from the cluster and destined to the endpoint is sourced from the secondary FortiGate. This means that the source MAC address is the physical address of the secondary egress interface.

When compared to proxy inspection, the difference is that FortiGate does not reply to packets on behalf of the client or server. For example, instead of replying to the SYN packet that the client sends, FortiGate forwards the packet to the server through the secondary. Similarly, FortiGate forwards packets that the server sends to the client through the secondary.

# DO NOT REPRINT

## © FORTINET

### Unsupported Sessions for Active-Active Load Balancing

- Sessions that can't be load balanced
  - ICMP, multicast, broadcast, SIP ALG, IM, P2P, and IPsec VPN
  - SSL VPN, HTTP multiplexing, SSL offloading, WAN optimization, explicit web proxy, and WCCP
- HTTPS sessions are not load balanced if they are subject to proxy-based inspection
- HTTPS sessions are load balanced only when `load-balance-all` is enabled and:
  - The inspection mode is set to flow mode, or
  - The inspection mode is set to proxy mode and the HTTPS traffic is not inspected
- Session failover and session load balancing
  - Some sessions can be synced, but not necessarily load balanced
  - For example, ICMP sessions can be synced (`session-pickup-connection` must be enabled) but can't be load balanced



© Fortinet Inc. All Rights Reserved.

39

In active-active mode, not all sessions qualify for active-active load balancing. This slide shows a list of sessions that can't be load balanced.

Most of the internet traffic nowadays is HTTPS. For this reason, it is important to understand the limitations for HTTPS traffic load balancing. You must know that HTTPS sessions are not load balanced if they are subject to proxy-based inspection. In fact, the only two scenarios in which HTTPS sessions are load balanced is when the `load-balance-all` setting is enabled and:

- The inspection mode is set to flow mode, or
- The inspection mode is set to proxy mode and the HTTPS traffic is not inspected.

Do not confuse session failover with session load balancing. While some sessions can be synchronized to secondary members for session failover protection, those same sessions aren't necessarily supported for active-active load balancing. For example, ICMP sessions can be synchronized to secondary members if you enable the `session-pickup-connectionless` setting, but they cannot be load balanced.

**DO NOT REPRINT**  
**© FORTINET**

## Active-Active Load Balancing Methods

| Method             | Description  |
|--------------------|--|
| none               | The primary handles all sessions   |
| leastconnection    | Sessions are sent to the member with the least number of sessions  |
| round-robin        | Default method. Sessions are distributed equally across members  |
| weight-round-robin | The more weight a member is assigned, the more sessions it handles                                       |
| random             | Sessions are distributed randomly across members   |
| ip hub             | Sessions with the same source and destination IP pair are handled by the same member                     |
| ipport             | Distribution based on source address, source port, destination address, and destination port information |

In active-active mode, when the primary device distributes sessions, it uses one of the following load balancing methods:

- **none:** Load balancing is turned off. The primary handles all sessions.
- **leastconnection:** The primary distributes sessions to the member with the least number of sessions.
- **round-robin:** This is the default method. The primary distributes sessions equally across members.
- **weight-round-robin:** The primary distributes sessions across members based on the member weight. The higher the member weight, the more sessions are distributed to that member.
- **random:** The primary distributes sessions randomly across members.
- **ip and hub:** The primary distributes sessions with the same source and destination IP pair to the same member. Both methods, **ip** and **hub**, work the same way. Both names in the configuration were kept for legacy compatibility purposes. The **hub** schedule will be removed in a future FortiOS version.
- **ipport:** The primary distributes sessions based on the source address, source port, destination address, and destination port information. The more diverse the traffic is, the more evenly the traffic is distributed across members.

**DO NOT REPRINT**  
**© FORTINET**

## Active-Active Load Balancing Methods (Contd)

- Configure link health monitor:

```
config system ha
  set schedule none | hub | leastconnection | round-robin | weight-round-robin | random | ip | ipport
end
```

- If using weight-round-robin, configure the member weight on the primary FortiGate:

```
config system ha
  set weight <id> <weight>
end
```

- Example—33% of sessions to primary and 67% to secondary

```
# get system ha status
...
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1

# config system ha
# set weight 0 1
# set weight 1 2
# end
```



© Fortinet Inc. All Rights Reserved.

41

You set the load balancing method by configuring the `schedule` setting, as shown on this slide.

When you select the weight-round-robin method, you must also configure the weight for each member, as shown on this slide. You indicate the member ID followed by its weight. The higher the member weight, the more sessions are distributed to that member. You can obtain the member ID from the output of the `get system ha status` command.

This slide also shows a configuration example for a weight-based distribution of 67% of sessions to the secondary FortiGate and 33% of sessions to the primary device. That is, for every three connections that qualify for load balancing, two of them are distributed to the secondary, and one of them to the primary.

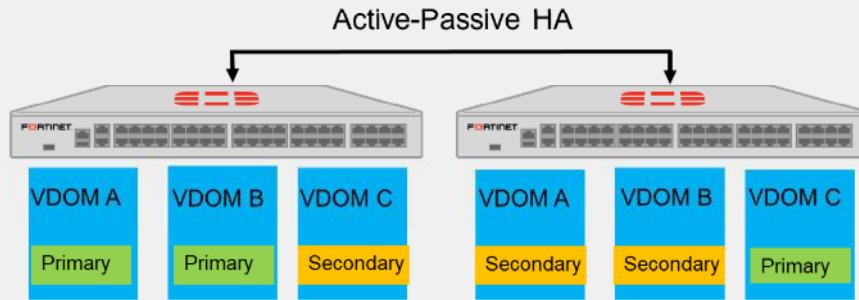
Note that you apply the member weight configuration for all members on the primary device. That is, you don't have to apply the weight on each member individually. The cluster will synchronize the configuration to each member for you.

# DO NOT REPRINT

## © FORTINET

### Virtual Clustering

- Virtual clusters are an extension of FGCP for FortiGate with multiple VDOMs
  - The HA cluster *must* consist of *only two* FortiGate devices
- Allows FortiGate to be the primary for some VDOMs and the secondary for the other VDOMs



So far, you've learned about HA clustering where each FortiGate device acts as a whole security domain.

But, if you have an HA cluster with multiple VDOMs, you can configure *virtual clusters*.

Virtual clusters allow you to have one device acting as the primary for one VDOM, and as the secondary for a different VDOM. Each VDOM has a primary and a secondary FortiGate. Any device can act as the primary for some VDOMs, and the secondary for the other VDOMs, at the same time. Because traffic from different VDOMs can go to different primary FortiGate devices, you can use virtual clustering to manually distribute your traffic between the two cluster devices and allow the failover mechanism for each VDOM between two FortiGate devices.

Note that if you deploy virtual clustering with more than two FortiGate devices, only two FortiGate devices will process the traffic.

When you add additional (third or fourth) FortiGate devices to a virtual cluster, the primary FortiGate and first secondary FortiGate handle all traffic, and the remaining FortiGate(s) will be operating in standby mode. In the event of a failure of the primary or first secondary FortiGate, one of the remaining FortiGate devices takes over as the new primary or secondary FortiGate and starts handling the traffic.

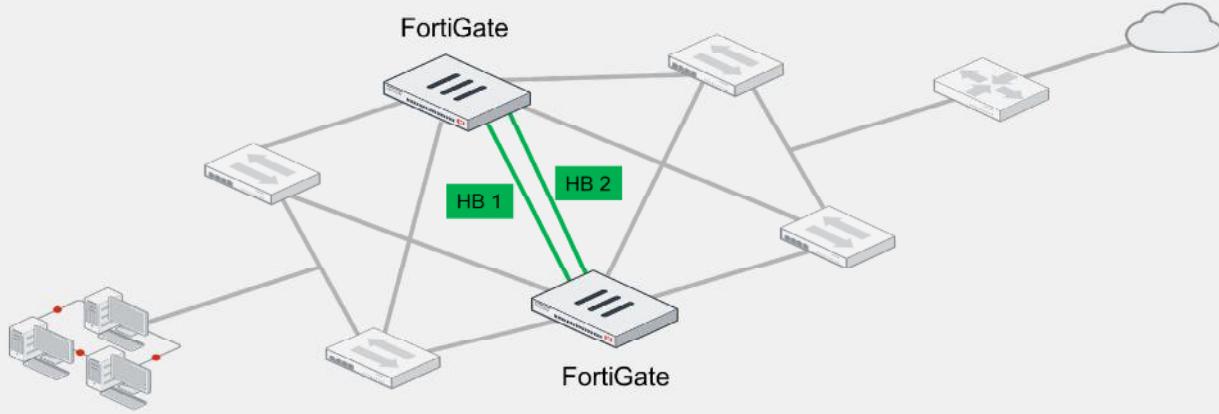
FGCP in Active-Active mode cannot load balance any sessions that traverse NPU VDOM links or regular VDOM links. If Active-Active session load balancing between VDOMs is required, use an external router to handle the inter-VDOM routing.

# DO NOT REPRINT

## © FORTINET

### Full Mesh HA

- Eliminates a single point of failure
- Requires redundant or LAG interfaces
  - If using LAG interfaces, the switch must support MCLAG or something similar
  - FortiSwitch supports MCLAG



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

43

At the beginning of this lesson, you reviewed a simple HA topology. Now, take a look at a more robust topology. It is called *full mesh HA*.

The goal of a full mesh HA topology is to eliminate a single point of failure, not only by having multiple FortiGate devices forming a cluster, but also by having redundant links to the adjacent switches. The goal is to have two switches for both upstream and downstream links, and then connect the redundant links to different switches. For example, the topology on this slide shows two FortiGate devices forming a cluster, and each FortiGate is connected to two redundant switches, using two different interfaces.

To achieve redundancy with adjacent switches, you must deploy redundant or LAG interfaces. If you use redundant interfaces, only one interface remains active. This avoids a Layer 2 loop and a standard switch should suffice. However, if you want to use LAG interfaces, then you must ensure that the switch supports multichassis link aggregation group (MCLAG) or a similar virtual LAG technology that enables you to form a LAG whose interface members connect to different switches. FortiSwitch, which is a Fortinet Ethernet switch, supports MCLAG. You can use FortiSwitch as the adjacent switch to deploy a full mesh HA topology with FortiGate.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. An HA failover occurs when the link status of a monitored interface on the \_\_\_\_\_ goes down.  
 A. Primary FortiGate  
 B. Secondary FortiGate
  
2. In an active-passive HA cluster, you can configure virtual clustering between only \_\_\_\_\_ FortiGate devices with multiple VDOMs.  
 A. Two  
 B. Four

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



HA Operation Modes



HA Cluster Synchronization



HA Failover and Workload



Monitoring and Troubleshooting

Good job! You now understand HA failover and workload.

Now, you will learn about monitoring and troubleshooting an HA cluster.

**DO NOT REPRINT****© FORTINET**

## Monitoring and Troubleshooting

### Objectives

- Verify the normal operation of an HA cluster
- Configure an HA management interface
- Upgrade the HA cluster firmware

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

By demonstrating competence in monitoring and troubleshooting, you will be able to make sure the cluster is synchronized properly. You will also learn how to configure and access secondary devices in an HA cluster and how to upgrade the firmware on the HA cluster.

# DO NOT REPRINT

## © FORTINET

### Checking the HA Status on the GUI

The screenshot shows the FortiGate GUI with two main sections: 'System > HA' and 'Dashboard > Status'.

**System > HA**

- HA Status:** Shows two cluster members: 'Local-FortiGate (Primary)' and 'Remote-FortiGate (Secondary)'. Both are synchronized with priority 200 and 100 respectively.
- Table Headers:** Status, Priority, Hostname, Serial No., Role, Uptime, Sessions, Throughput.
- Data:**

| Status       | Priority | Hostname         | Serial No.      | Role      | Uptime | Sessions | Throughput |
|--------------|----------|------------------|-----------------|-----------|--------|----------|------------|
| Synchronized | 200      | Local-FortiGate  | FGVM01000064692 | Primary   | 3d 23h | 11       | 22.00 kbps |
| Synchronized | 100      | Remote-FortiGate | FOVM01000065036 | Secondary | 0s     | 5        | 17.00 kbps |
- Actions:** Refresh, Edit, Remove device from HA cluster.

**Dashboard > Status**

- HA Status Widget:** Displays mode (Active-Active), group (Training), and member status (Primary, Secondary).
- Actions:** Refresh, Edit, Remove device from HA cluster.
- More columns available:** A callout box points to a dropdown menu listing various system metrics like AV Events, Bytes, Checksum, Cluster Uptime, CPU, Down Ports, etc.

**Fortinet Training Institute** © Fortinet Inc. All Rights Reserved. 47

The **HA** page on the FortiGate GUI shows important information about the health of your HA cluster. For each cluster member, the page shows whether the member is synchronized or not, and its status, host name, serial number, role, priority, uptime, and active sessions.

On the **HA** page, you can remove a device from a cluster. When you remove a device from HA, the device operation mode is set to standalone. You can also enable more columns that display other important information about each member such as the checksum, CPU, and memory.

You can also add the **HA Status** widget on the **Dashboard** page. The widget provides a summary of the HA status on the device.

# DO NOT REPRINT

## © FORTINET

### Checking the HA Status on the CLI

```
# get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 210
Debug: 0
Cluster Uptime: 2 days 21:28:23
Cluster state change time: 2022-04-20 18:28:23
Primary selected using:
<2022/04/20 18:28:23> vcluster-1: SN1 is selected as the primary because its uptime is larger than peer member SN2.
<2022/04/20 16:13:49> vcluster-1: SN2 is selected as the primary because its uptime is larger than peer member SN1.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
Configuration Status:
SN1(updated 4 seconds ago): in-sync
SN2(updated 4 seconds ago): in-sync
System Usage stats:
SN1(updated 4 seconds ago):
sessions=17, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=57%
SN2(updated 4 seconds ago):
sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=56%
...
...
```

Cluster status, member model, HA mode, and cluster uptime

Latest primary election results and the reason

Configuration sync status

Performance stats of each member

**Note:** Displayed serial numbers are not real



© Fortinet Inc. All Rights Reserved.

48

You can get more information about the HA status on the FortiGate CLI by using the `get system ha status` command.

The command displays comprehensive HA status information in a user-friendly output and is usually executed as the first step when troubleshooting HA. This slide shows the first part of an example output that the command provides. Note that the serial numbers of members have been replaced by fake ones (SN1 and SN2), so the output fits on this slide.

At the beginning of the output, you can see the cluster status, the member model, the HA mode in use, and the cluster uptime. The example output shows that the cluster status is good, the member model is FortiGate-VM64-KVM, and the HA mode is active-passive. The cluster has also been up for almost three days.

Next, you can see the latest primary election events, the result, and the reason. The output indicates that a different member was elected as the primary during the last two election events. In both cases, the member was elected because it had a higher HA uptime.

The configuration status information is displayed next. It indicates the configuration sync status for each member. For both members, the configuration is in sync.

Following the configuration status information, you can see the system usage statistics, which report on performance statistics for each member. They indicate the number of sessions that each member handles, as well as the average CPU and memory usage. Note that the `sessions` field accounts for any sessions that the member handles, and not only the sessions that are distributed when the HA mode is active-active.

**DO NOT REPRINT**  
**© FORTINET**

## Checking the HA Status on the CLI (Contd)

```
...
HBDEV stats:
SNI(updated 4 seconds ago):
    port9: physical/10000full, up, rx-bytes/packets/dropped/errors=154604218/304596/0/0, tx=352015560/498020/0/0
SN2(updated 4 seconds ago):
    port9: physical/10000full, up, rx-bytes/packets/dropped/errors=386075683/578563/0/0, tx=269160874/516602/0/0
MONDEV stats:
SNI(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0, tx=13209070/157763/0/0
SN2(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0, tx=6345393/37126/0/0
PINGSVR stats:
SNI(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0, tx=13209070/157763/0/0
    pingsvr: state=up(since 2022/04/20 16:13:50), server=10.9.15.40, ha_prio=5
SN2(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0, tx=6345393/37126/0/0
    pingsvr: state=N/A(since 2022/04/20 16:13:54), server=10.9.15.40, ha prio=5
Primary      : Local-FortiGate , SNI, HA cluster index = 0
Secondary    : Remote-FortiGate, SN2, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: SNI, HA operating index = 0
Secondary: SN2, HA operating index = 1
```

Heartbeat, monitored, and remote link interfaces status

Member role, host name, serial number, and ID

**Note:** Displayed serial numbers are not real

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

49

This slide shows the second part of the example output that the `diagnose system ha status` command provides.

The output begins with the status information for the configured heartbeat, monitored, and remote link interfaces. These interfaces enable the cluster to perform device failover, link failover, and remote link failover protection, respectively.

Next, the output shows the role, host name, serial number, and ID information for each member of the cluster. The output indicates that the Local-FortiGate and Remote-FortiGate devices are primary and secondary members, respectively.

**DO NOT REPRINT**  
**© FORTINET**

## Checking the Configuration Synchronization

- Display the member checksum:

```
# diagnose sys ha checksum show

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11
```

Configuration is in sync when all hash values on each member match

- If the checksums don't match, try running:

```
diagnose sys ha checksum recalculate
```

- Display the checksum for all members:

```
# diagnose sys ha checksum cluster

===== FGVM010000112065 =====

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

===== FGVM010000065036 =====

is_manage_primary()=0, is_root_primary()=0
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root: cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all: 98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11
```

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

50

The `diagnose sys ha checksum` command tree enables you to check the cluster configuration sync status. In most cases, you want to use the `diagnose sys ha checksum cluster` command to view the cluster checksum. The output includes the checksum of each member in the cluster.

When you run the `diagnose sys ha checksum cluster` command, the checksum is polled from each member using the heartbeat interface. If HA is not working properly, or if there are heartbeat communication issues, then the command may not show the checksum for members other than the one you run the command on. An alternative is to connect to each member individually and run the `diagnose sys ha checksum show` command instead. This command displays only the checksum of the member you are connected to.

After you obtain the checksums of each member, you can identify the configuration sync status by comparing the checksums. If all members show the exact hash values for each configuration scope, then the configuration of all members is in sync.

To calculate checksums, FortiGate computes a hash value for each of the following configuration scopes:

- global: global configuration, such as global settings, FortiGuard settings, and so on
- root: settings and objects specific to the root VDOM—if you configure multiple VDOMs, FortiGate computes hash values for each VDOM
- all: global configuration plus the configuration of all VDOMs

In some cases, the configuration of members is in sync even though the checksums are different. For these cases, try running the `diagnose sys ha checksum recalculate` command to recalculate the HA checksums.

**DO NOT REPRINT**  
© FORTINET

## Switching to the CLI of Another Member

- Using the FortiGate CLI, you can connect to the CLI of any member:

```
# execute ha manage <member_id> <admin_username>
```

- To list the ID of each member, use a question mark:

```
# execute ha manage ?  
<id>    please input peer box index.  
<1>    Subsidiary unit FGVM0100000xxxxx
```

- The CLI connection is made over SSH and Ethernet frames type 0x8893



© Fortinet Inc. All Rights Reserved.

51

When troubleshooting HA, you may need to connect to the CLI of another member from the CLI of the member you are currently connected to. You do this by using the `execute ha manage` command to connect to the other member.

For example, when you connect to the cluster over SSH using any of the cluster virtual IP addresses, you connect to the primary member. If you then want to connect to another member, you can use the `execute ha manage` command to access its CLI.

This command requires you to indicate the ID of the member you want to connect to and the username you will use to log in. To get the list of member IDs, you can add a question mark to the end of the `execute ha manage` command, as shown on this slide.

Note that when you switch to the CLI of another member, FortiGate establishes an SSH session to that member over the heartbeat interface. The SSH session is then encapsulated in Ethernet frames type 0x8893.

**DO NOT REPRINT**  
© FORTINET

## Force a Permanent Secondary Role on the Primary

- Set the primary to have a permanent secondary:

```
Local-FortiGate # execute ha failover set  
Caution: This command will trigger an HA failover.  
It is intended for testing purposes.  
Do you want to continue? (y/n)
```

- A failover occurs, and the device remains as secondary device
  - *Use the command for testing, demo, or troubleshooting purposes only*
  - Not recommended in production networks

- To view the permanent secondary role status:

```
Local-FortiGate # execute ha failover status  
failover status: set
```

- Revert the permanent secondary role state:

```
Local-FortiGate # execute ha failover unset
```



© Fortinet Inc. All Rights Reserved.

52

You can set the primary FortiGate to have a permanent secondary role using the `execute ha failover set` command. When you do this, a failover occurs, and the former primary member remains as a secondary member permanently, regardless of the status of other members in the cluster. That is, the impacted member never takes over the cluster even if it's the best candidate for the primary role.

You can revert the permanent secondary role state by running the `execute ha failover unset` command. Note that you should set the primary member to a permanent secondary role for testing, troubleshooting, and demonstration purposes only. Do not use this feature in production networks.

**DO NOT REPRINT****© FORTINET**

## Connect to Any Member Directly

- Reserved HA management interface
  - Out-of-band
  - Up to four dedicated interfaces
  - For local-in traffic and *some* local-out traffic
  - Separate routing table
  - Configuration example (not synchronized):

```
config system ha
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port10"
      set gateway 192.168.100.254
    next
  end
config system interface
  edit "port10"
    set ip 192.168.100.1 255.255.255.0
    set allowaccess ping https ssh snmp
  next
end
```

- In-band HA management interface
  - In-band
  - Use any user-traffic interface
  - For local-in and local-out traffic
  - Shared routing table
  - Configuration example (not synchronized):

```
config system interface
  edit "port1"
    set management-ip 10.0.10.1 255.0.0.0
    set allowaccess ping https ssh snmp
  next
end
```



© Fortinet Inc. All Rights Reserved.

53

When you connect to a cluster using any of its virtual IP addresses, you always connect to the primary. You can then switch to the CLI of any member in the cluster by using the `execute ha manage` command. But what if you want to access the GUI of a secondary member or maybe poll data from it using SNMP? For this, you need a way to access each member directly regardless of its role in the cluster.

FortiGate provides two ways for the administrator to connect to a member directly no matter what the member role is. The reserved HA management interface is the out-of-band option. You configure up to four dedicated management interfaces, and you assign them a unique address on each member. You can then use the unique address assigned to each member to connect to them directly. You can also instruct FortiGate to use the dedicated management interface for some outbound management services such as SNMP traps, logs, and authentication requests.

Alternatively, you can configure in-band HA management, which enables you to assign a unique management address to a member without having to set aside an interface for that purpose. You assign the management address to any user-traffic that the member uses, and then connect to the member using that unique management address.

If you have unused interfaces, then it's generally more convenient to use a reserved HA management interface because the user and management traffic don't have to compete. Many FortiGate models come with a management interface that you can use for this purpose. Also, the routing information for a reserved HA management interface is placed in a separate routing table, which means that you don't see the interface routes in the FortiGate routing table. This allows for segmentation between data and management traffic.

This slide also shows configuration examples for both management options. For both options, the configuration you apply on a member is not synchronized to other members in the cluster.

# DO NOT REPRINT

© FORTINET

## Firmware Upgrade

- Apply the new firmware using the GUI or CLI
- Uninterruptible upgrade is enabled by default:

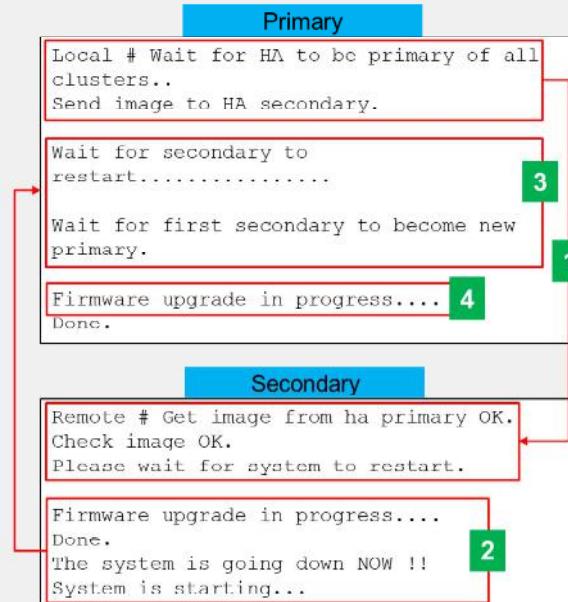
```
config system ha
    set uninterruptible-upgrade enable | disable
end
```

- Firmware upgrade process (uninterruptible upgrade enabled):
  1. The primary sends the firmware image to the secondary devices
  2. The secondary devices upgrade their firmware
  3. The first secondary to finish becomes the primary\*
  4. The former primary becomes a secondary device and upgrades its firmware\*\*

**Note:**

\* If HA mode is active-active, the primary temporarily takes over all the traffic.

\*\* Enable the `override` setting on the primary to ensure it takes over the cluster after the firmware upgrade completes.



You upgrade an HA cluster in the same way you do for standalone FortiGate devices. That is, you can apply the new firmware using the GUI firmware upgrade tool. In HA, this usually means connecting to the primary FortiGate GUI to apply the new firmware. You can also use the CLI if you prefer.

Also, like on standalone FortiGate devices, the device must reboot to apply the new firmware. However, by default, members in a cluster are upgraded one at a time to minimize service disruption. This feature is called uninterrupted upgrade and is enabled by default. After the administrator applies the new firmware on the primary, uninterrupted upgrade works as follows:

1. The primary sends the firmware to all secondary members using the heartbeat interface.
2. The secondary devices upgrade their firmware first. If the cluster is operating in active-active mode, the primary temporarily takes over all traffic.
3. The first secondary that finishes upgrading its firmware takes over the cluster.
4. The former primary becomes a secondary device and upgrades its firmware next.

Note that depending on the HA settings and uptime, the original primary may remain as a secondary after the upgrade. Later, if required, you can issue a manual failover. Alternatively, you can enable the `override` setting on the primary FortiGate to ensure it takes over the cluster again after it upgrades its firmware, as long as the device is assigned the higher priority.

If you want the cluster to upgrade all members at the same time to speed up the firmware upgrade process, you can disable uninterrupted upgrade, as shown on this slide. Just keep in mind this will result in a service impact during the firmware upgrade.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which member is the heartbeat interface IP address 169.254.0.1 assigned to?  
 A. The member with the highest serial number  
 B. The member with the highest priority
  
2. Which statement about the firmware upgrade process on an HA cluster is true?  
 A. You upload the new firmware to the primary FortiGate only.  
 B. The members do not reboot.

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



HA Operation Modes



HA Cluster Synchronization



HA Failover and Workload



Monitoring and Troubleshooting

Congratulations! You have completed this lesson.

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

**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



## FortiGate Infrastructure

Diagnostics



Last Modified: 13 June 2022

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

**DO NOT REPRINT**

© FORTINET

## Lesson Overview



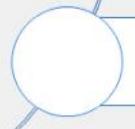
**General Diagnosis**



**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.

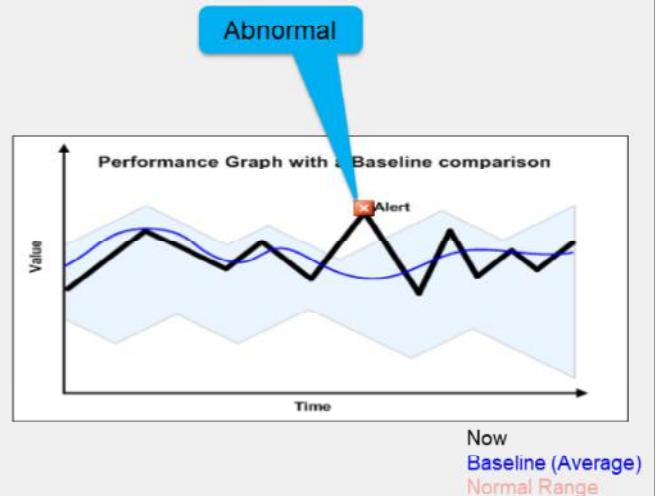
By demonstrating competence in general diagnosis, you will be able to discover general information about the status of FortiGate.

# 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.

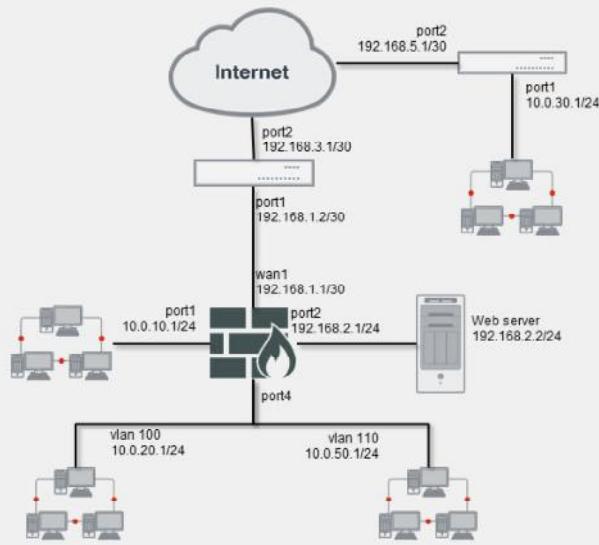
Normal is measured and defined in many ways. It can be performance: the expected CPU and memory utilization, bandwidth, and traffic volumes. But, it can also be your network topology: which devices are normally connected at each node. It is also behavior: traffic flow directions, which protocols are 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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

5

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
Version: FortiGate-40F-364G v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Virus-DB: 90.01760(2022-04-26 16:26)
Extended DB: 90.01760(2022-04-26 16:26)
AV AI/ML Model: 2.05403(2022-04-26)
IPS-DB: 20.00304(2022-04-26 00:08) FortiGate physical
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 20.00304(2022-04-26 00:08)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 3.00331(2022-04-25 16:10)
IoT-Detect: 0.00000(2001-01-01 00:00)
Serial-Number: FG40FITKXXXXXX
BIOS version: 05000004
System Part-Number: P24695-03
Log hard disk: Not available
Hostname: FortiGate
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1157
Release Version Information: GA
System time: Wed Apr 27 12:43:57 2022
Last reboot reason: power cycle
```

```
FortiGate # get system status
Version: FortiGate-VM64-KVM v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Virus-DB: 81.00091(2020-10-14 16:20)
Extended DB: 81.00091(2020-10-14 16:20)
Extreme DB: 1.00000(2018-04-09 16:20)
AV AI/ML Model: 0.00000(2001-01)
IPS-DB: 6.00741(2015-12-01 02:30) FortiGate VM
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 2.00797(2020-10-14 05:06)
IoT-Detect: 0.00000(2001-01-01 00:00)
Serial-Number: FGVM010000064692
License Status: Valid
VM Resources: 1 CPU/1 allowed, 2007 MB RAM
Log hard disk: Available
Hostname: FortiGate
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1157
Release Version Information: GA
FortiOS x86-64: Yes
System time: Wed Apr 27 04:16:15 2022
Last reboot reason: shutdown
```



© 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             :0lif
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         |



© Fortinet Inc. All Rights Reserved.

8

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 FortiGate VM interface
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



© Fortinet Inc. All Rights Reserved.

15

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"
```

The diagram illustrates the flow of a SYN packet through FortiGate. It highlights specific log entries and connects them to their respective processing steps:

- IP addresses, port numbers, and incoming interface**: Points to the first log entry: "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".
- Create a new session**: Points to the second log entry: "allocate a new session-00007fc0".
- Found a matching route. Shows next-hop IP address and outgoing interface**: Points to the third log entry: "find a route: flag=04000000 gw-10.200.1.254 via port1".
- Matching firewall policy**: Points to the fourth log entry: "Allowed by Policy-1: SNAT".
- Source NAT**: Points to the fifth log entry: "SNAT 10.0.1.10->10.200.1.1:49886".

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: 8.8.8.8

Protocol: **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: 8.8.8.8

Destination IP: 8.8.8.8

Destination port: 10.0.1.10

Protocol: ICMP

Start debug flow

FORTINET  
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 gnum=100004, use addr/rnfh hash, len=2
07:08:02 165 checked gnum=100004 policy=1, ret-no-match, act-accept
07:08:02 165 checked gnum=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 gnum=100004, use addr/rnfh hash, len=2
07:08:01 checked gnum=100004 policy=1, ret-no-match, act-accept
07:08:01 checked gnum=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
```



© Fortinet Inc. All Rights Reserved.

25

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



© Fortinet Inc. All Rights Reserved.

27

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:

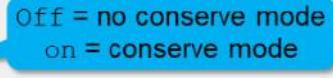
- `off`: All new sessions with content scanning enabled are not passed but FortiGate processes the current active sessions.
- `pass` (default): All new sessions pass without inspection until FortiGate switches back to non-conserve mode.
- `one-shot`: Similar to `pass` in that traffic passes without inspection.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



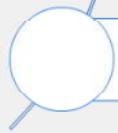
General Diagnosis



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.

**DO NOT REPRINT**  
© FORTINET

## 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

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically  
 Use the following IP address:

IP address: 192.168.1.1  
 Subnet mask: 255.255.255.0  
 Default gateway: 192.168.1.99

Obtain DNS server address automatically  
 Use the following DNS server addresses:

Preferred DNS server: . . .  
 Alternate DNS server: . . .

Validate settings upon exit

OK Cancel Advanced...

TFTP server IP address configuration

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.