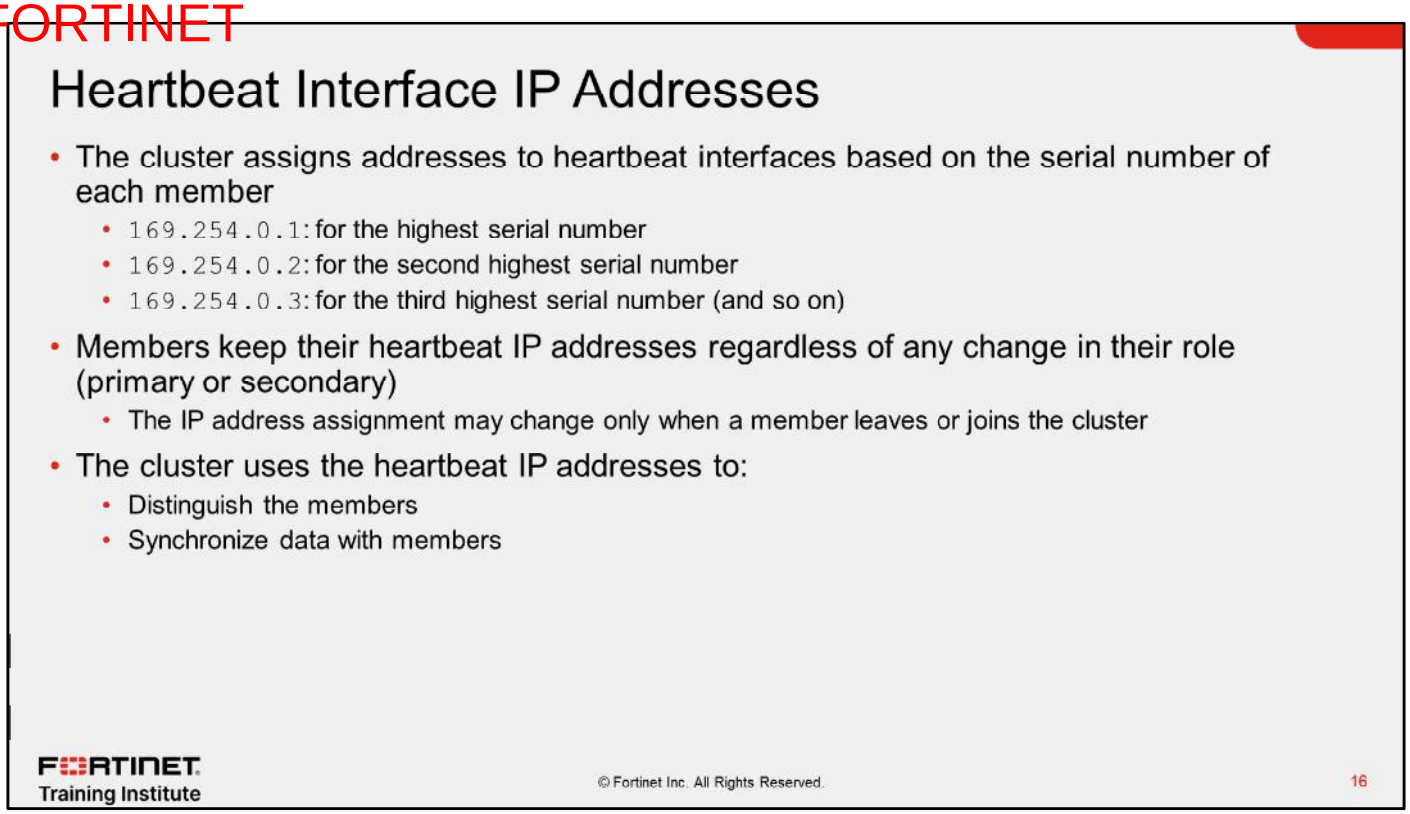
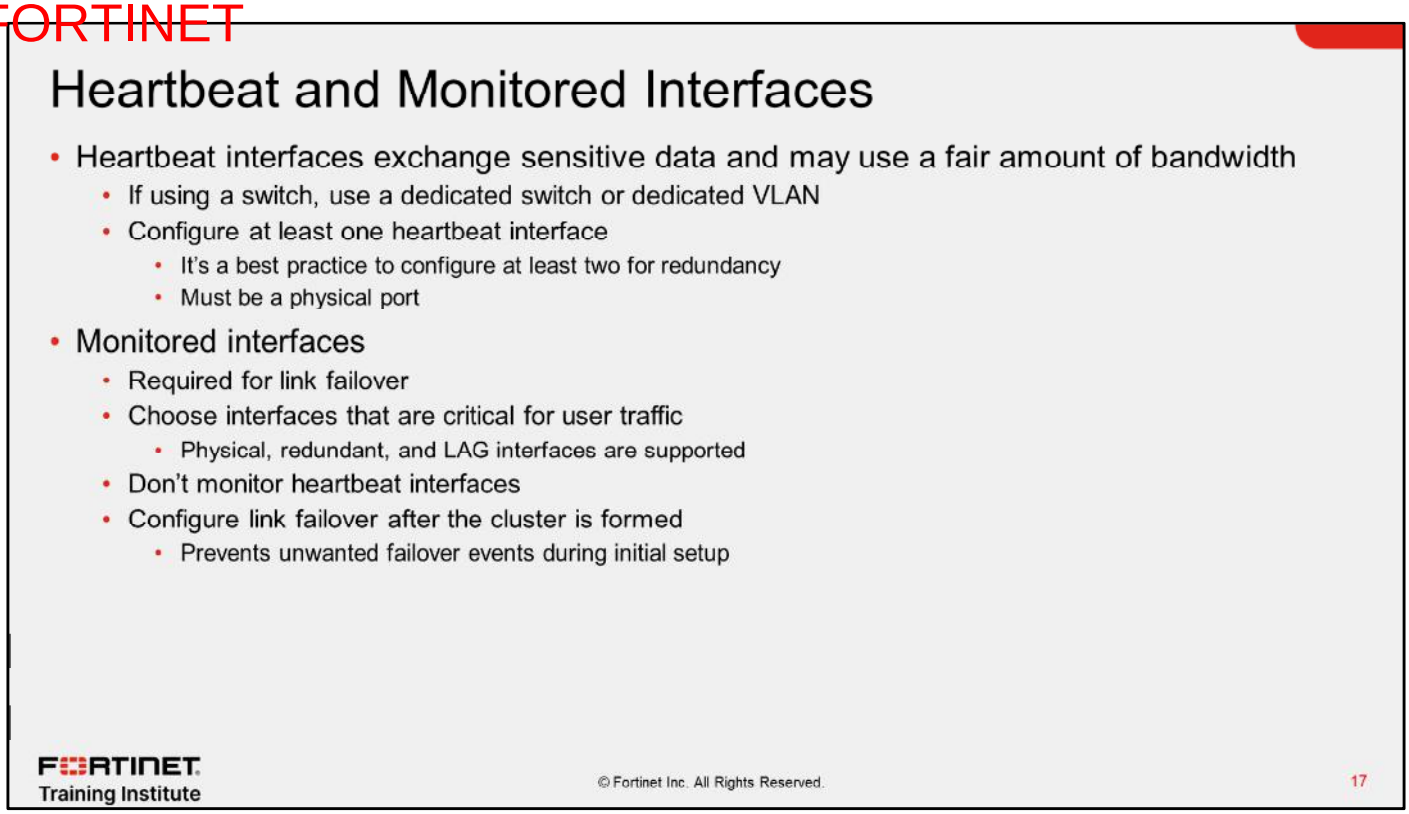


FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number. The IP address 169.254.0.2 is assigned to the device with the second highest serial number, and so on. The IP address assignment 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.

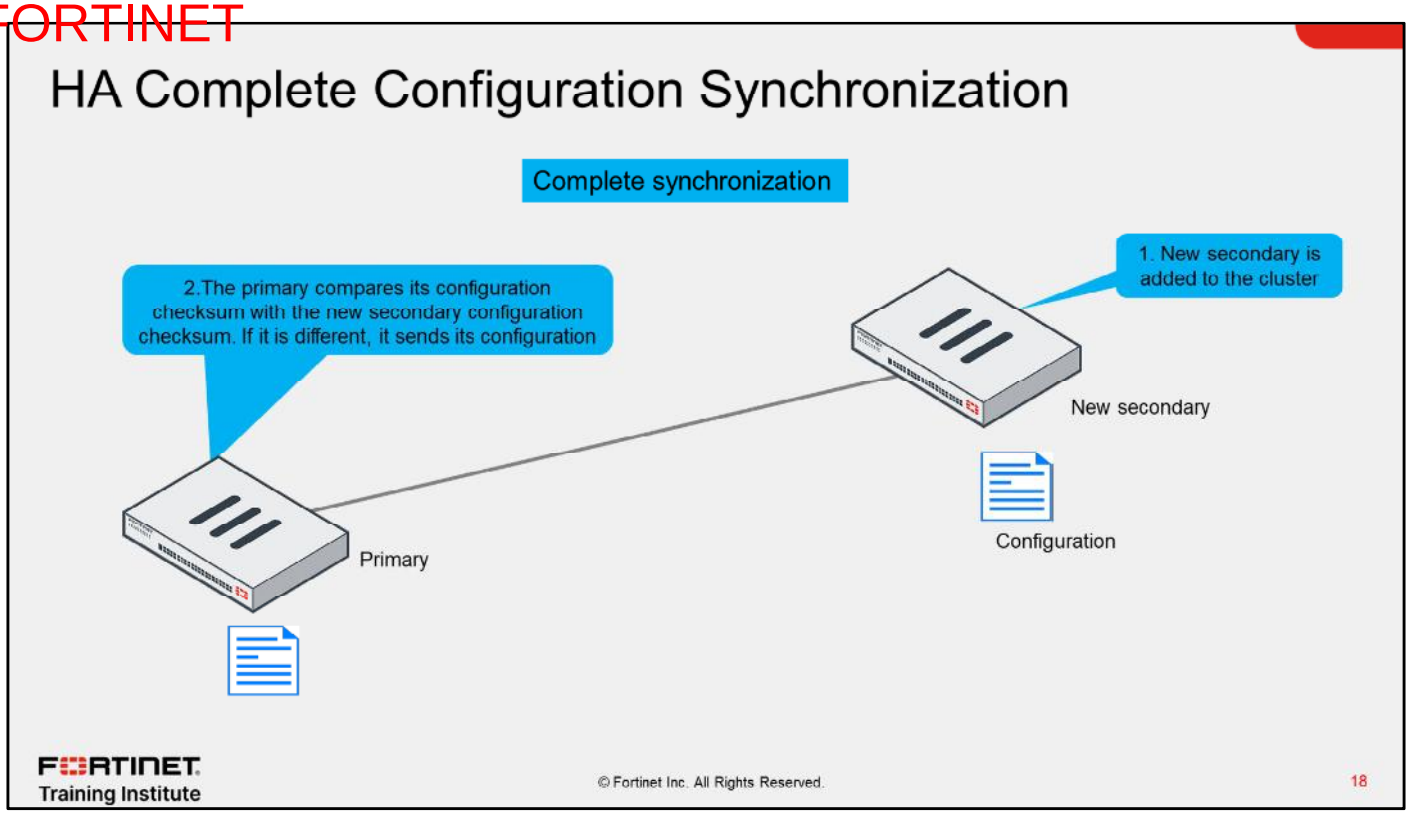


Heartbeat interfaces exchange sensitive information about the cluster operation and may require a fair amount of bandwidth for data synchronization. For this reason, if you use a switch to connect the heartbeat interfaces, it's recommended that you use a dedicated switch or, at least, that you place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

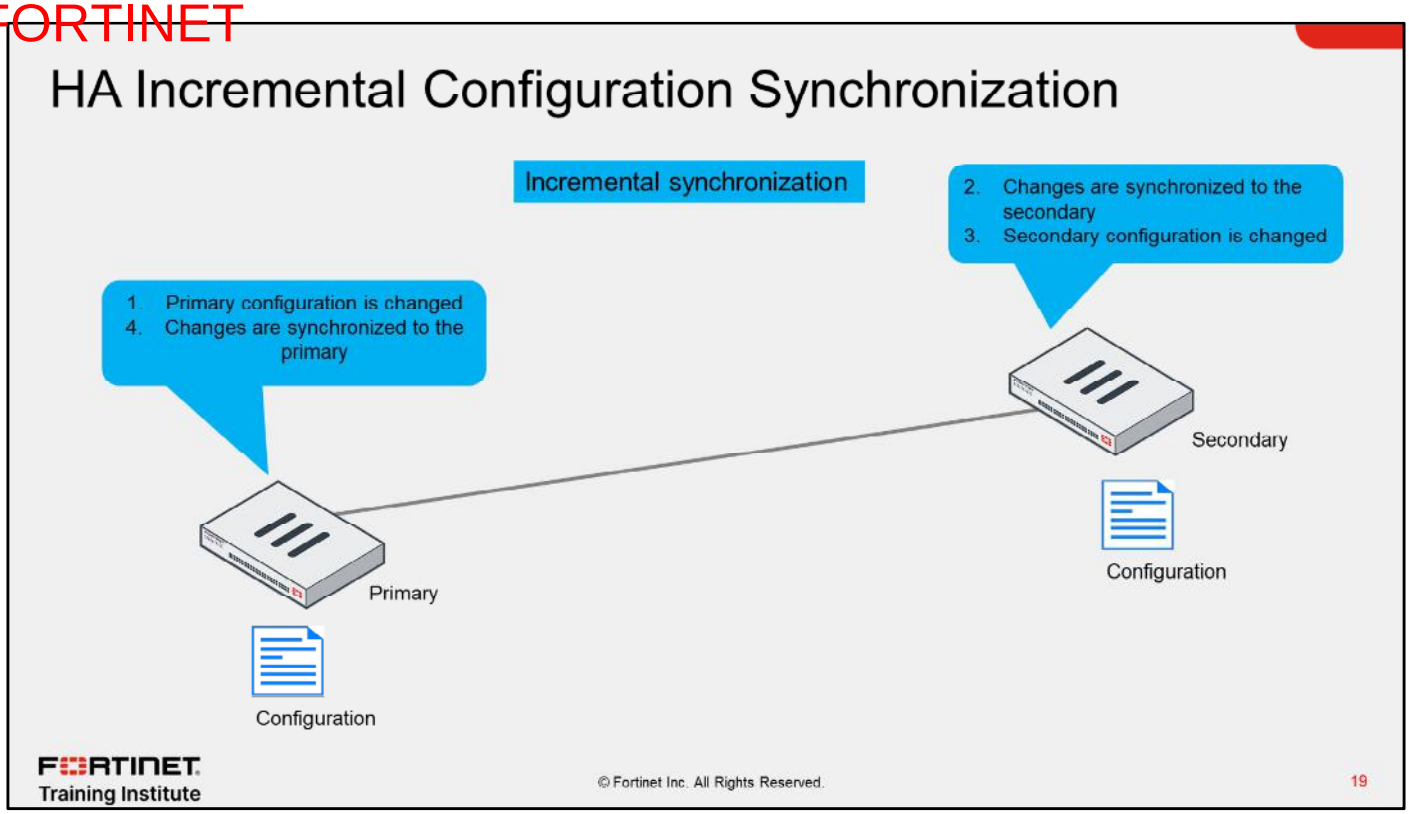
As a best practice, wait until a cluster is up and running and all interfaces are connected before configuring link failover. This is because a monitored interface can be disconnected during the initial setup and, as a result, trigger a failover before the cluster is fully configured and tested.



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

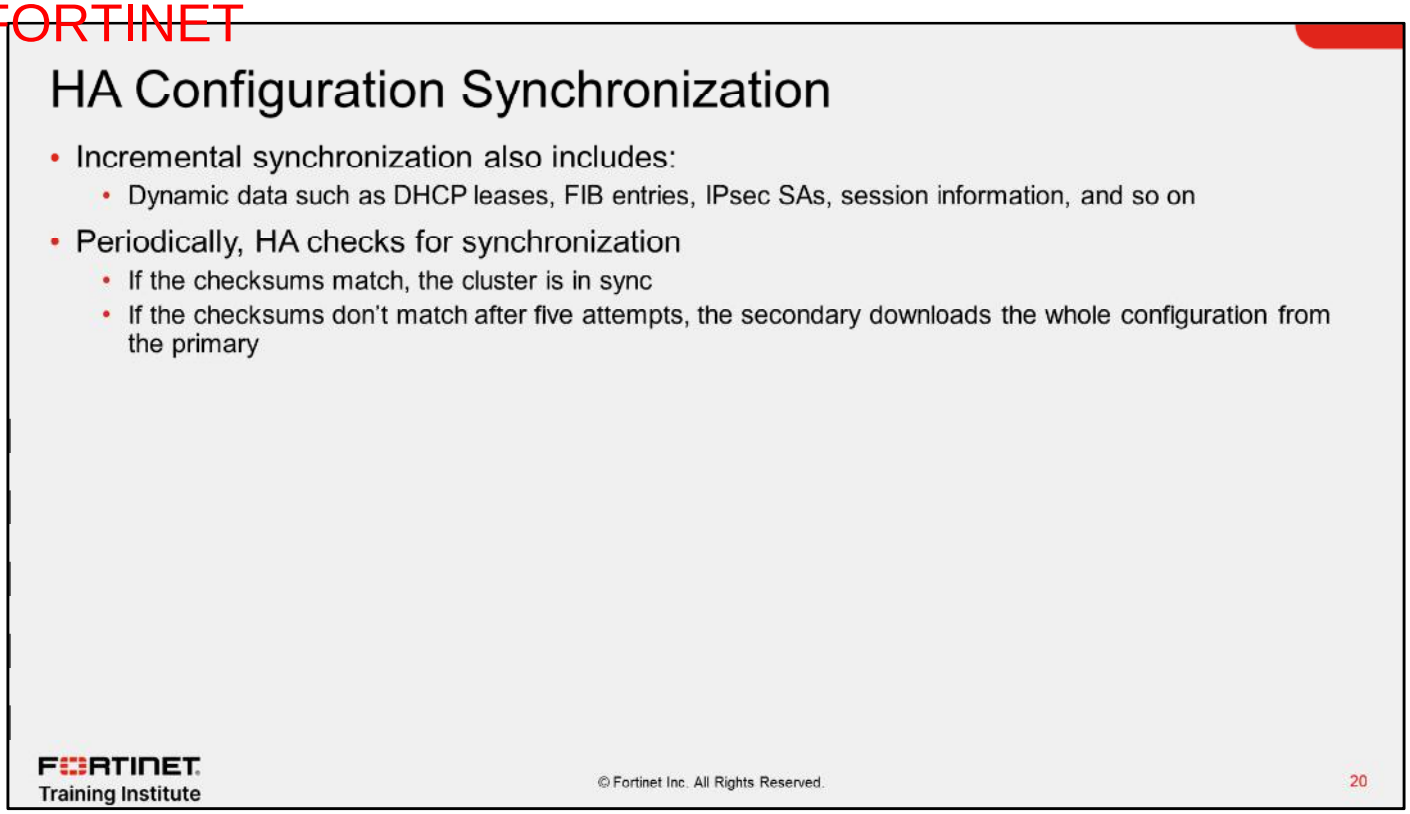
FortiGate HA uses a combination of both incremental and complete synchronizations.

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.



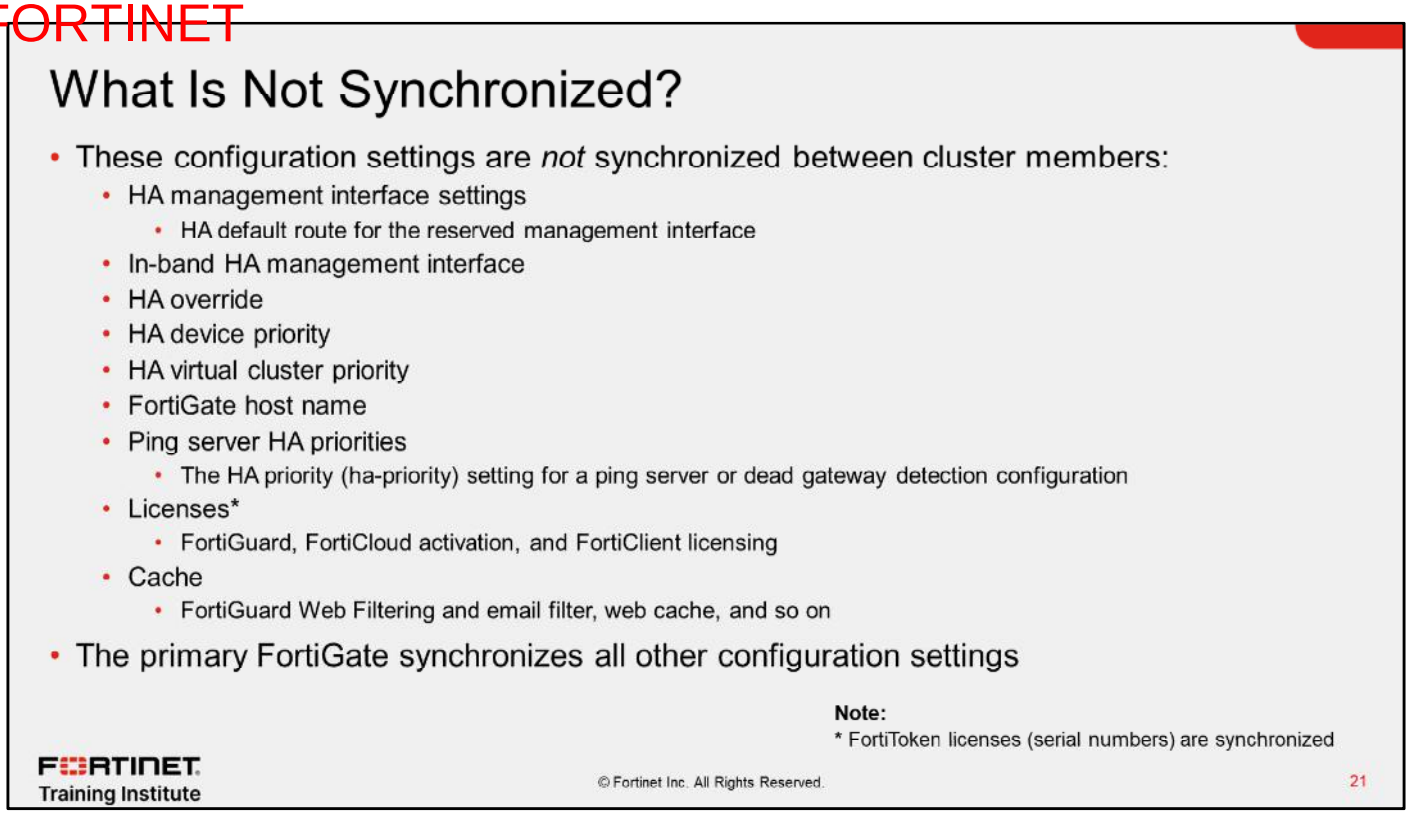
After the initial synchronization is complete, whenever a change is made to an HA cluster device's (primary or secondary) configuration, incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link. An HA synchronization process running on each 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.



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

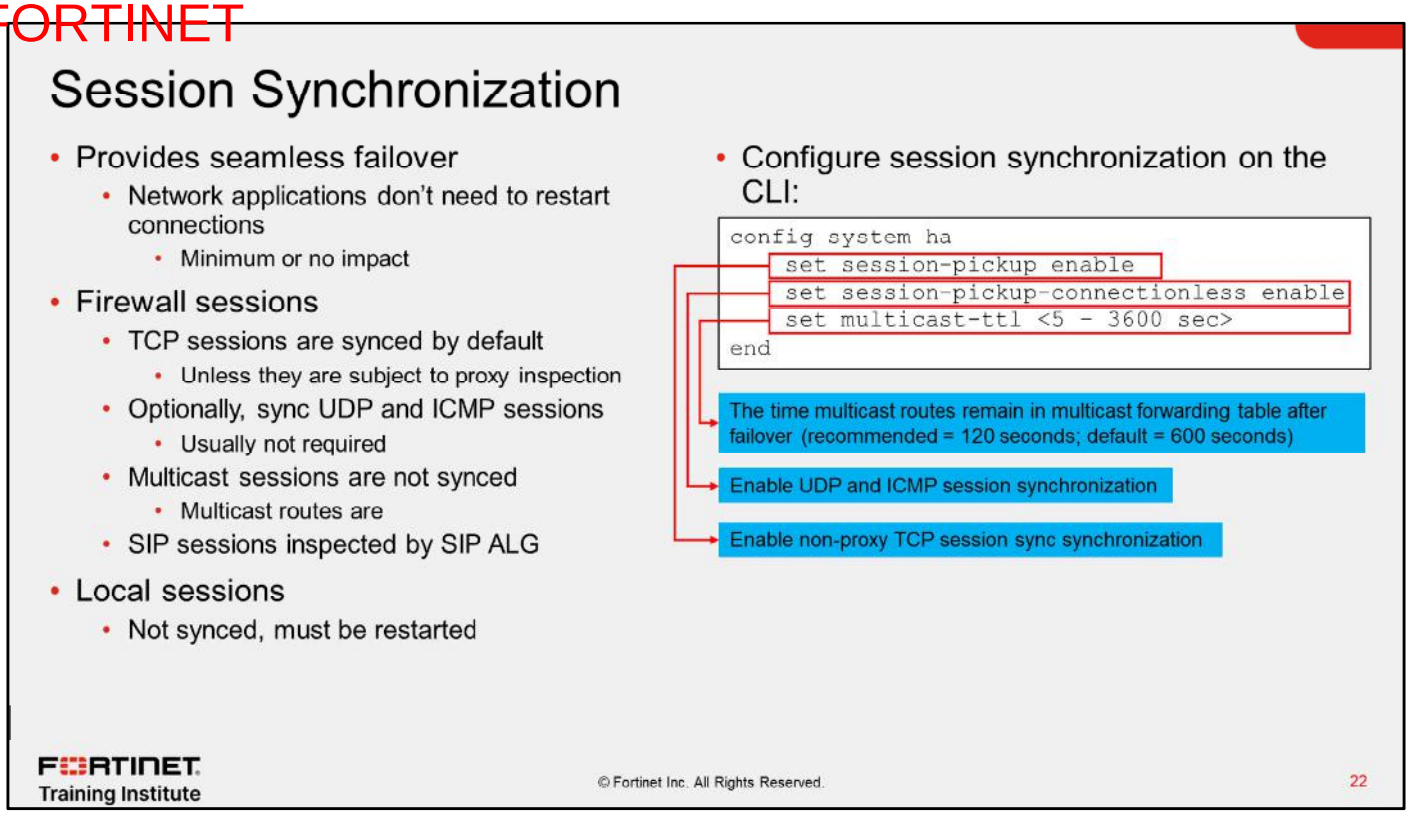
By default, the cluster checks every 60 seconds to ensure that all devices are synchronized. If a secondary device is out of sync, its checksum is checked every 15 seconds. If the checksum of the out-of-sync secondary device doesn't match for five consecutive checks, a complete resynchronization to that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



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.



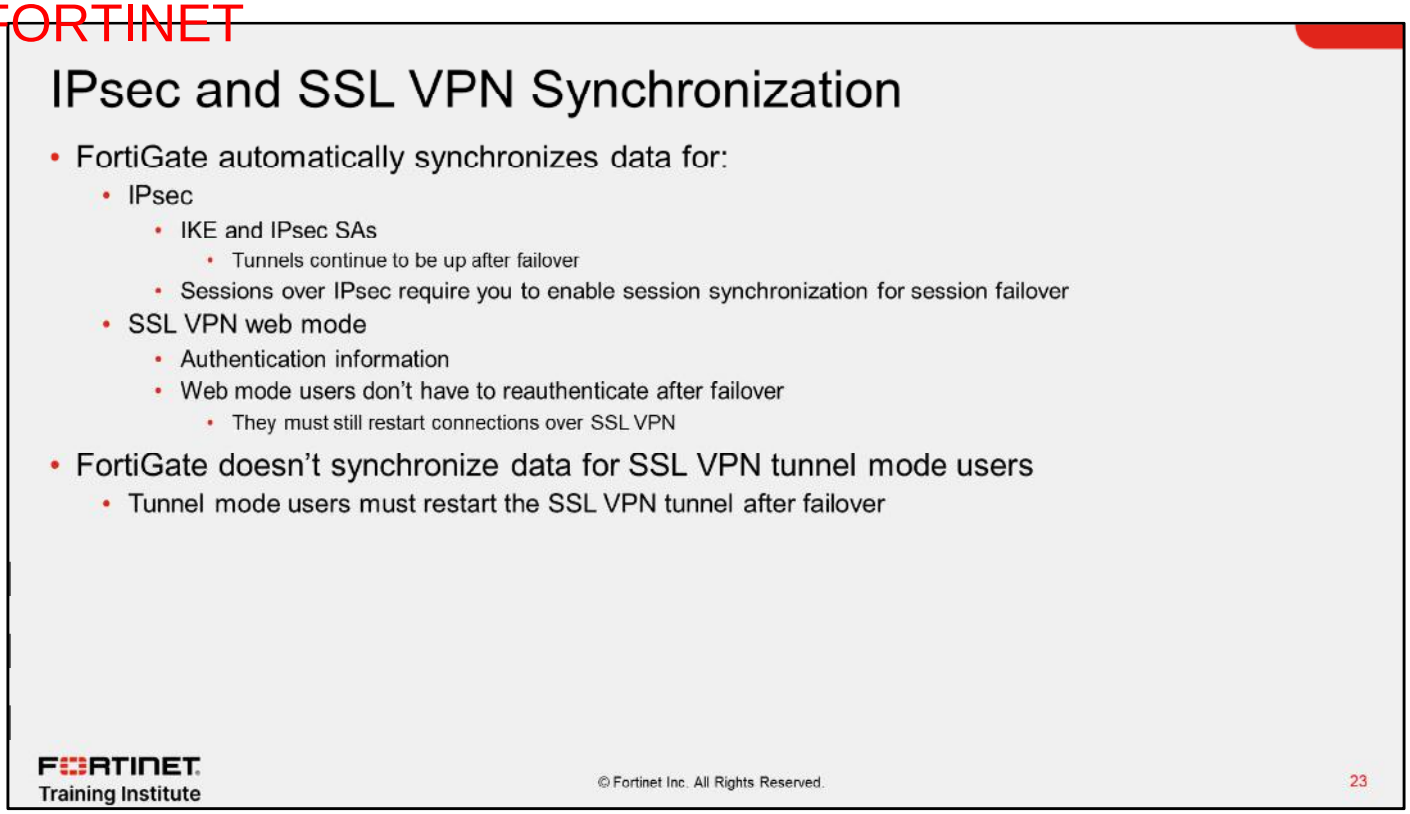
Session synchronization provides seamless session failover. When the primary fails, the new primary can resume traffic for synchronized sessions without network applications having to restart the connections.

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.



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.

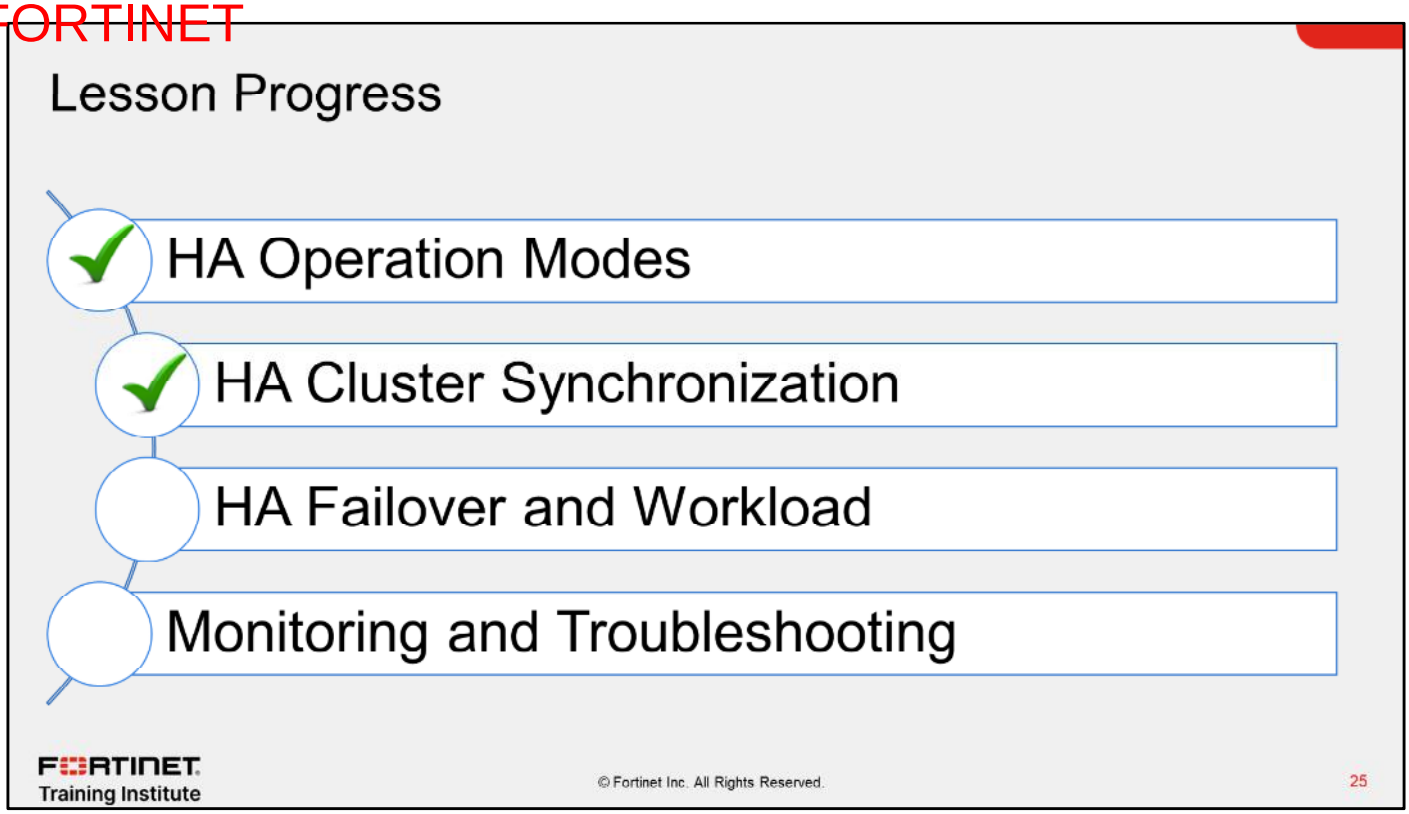
Knowledge Check

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

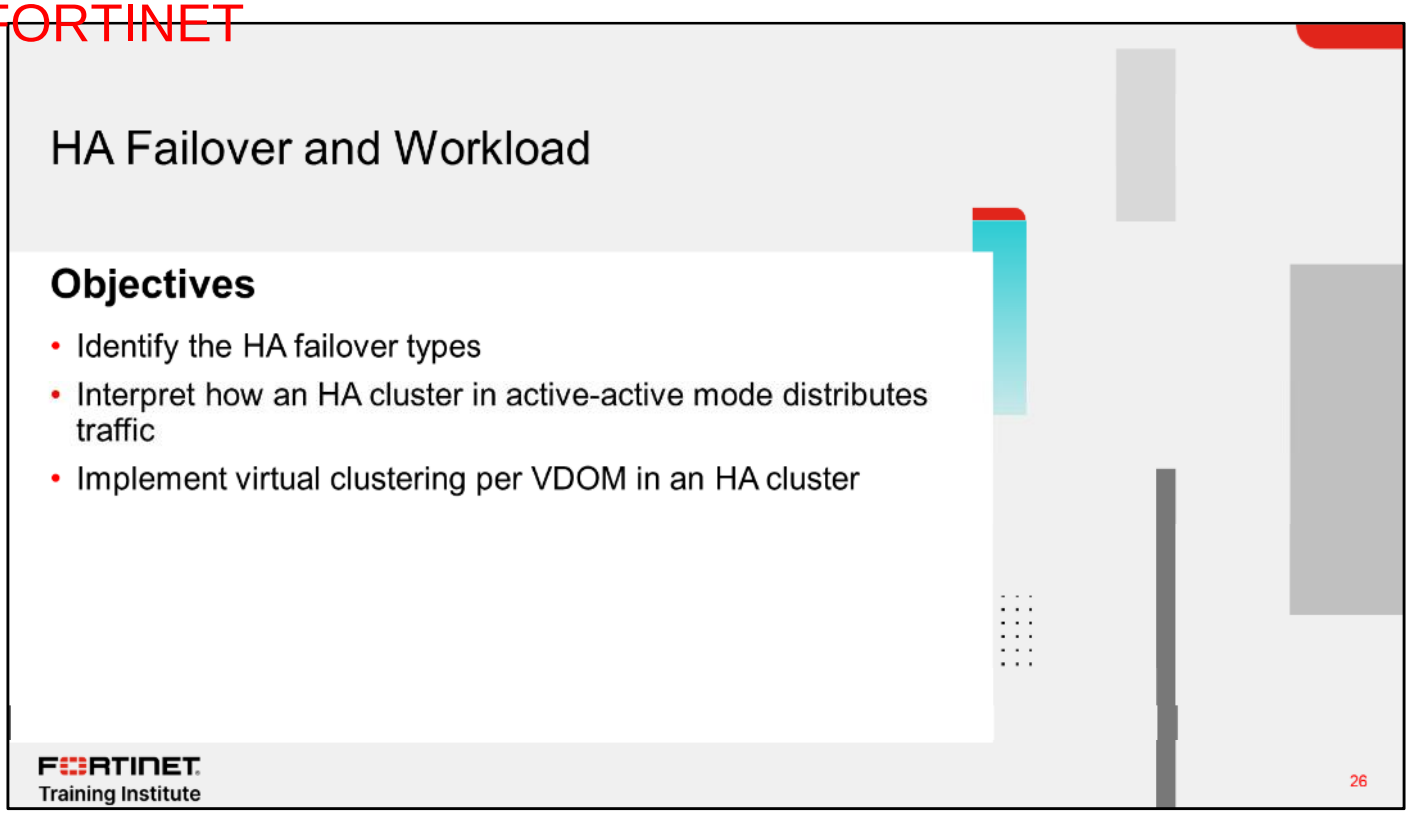
FORTINET Training Institute

24



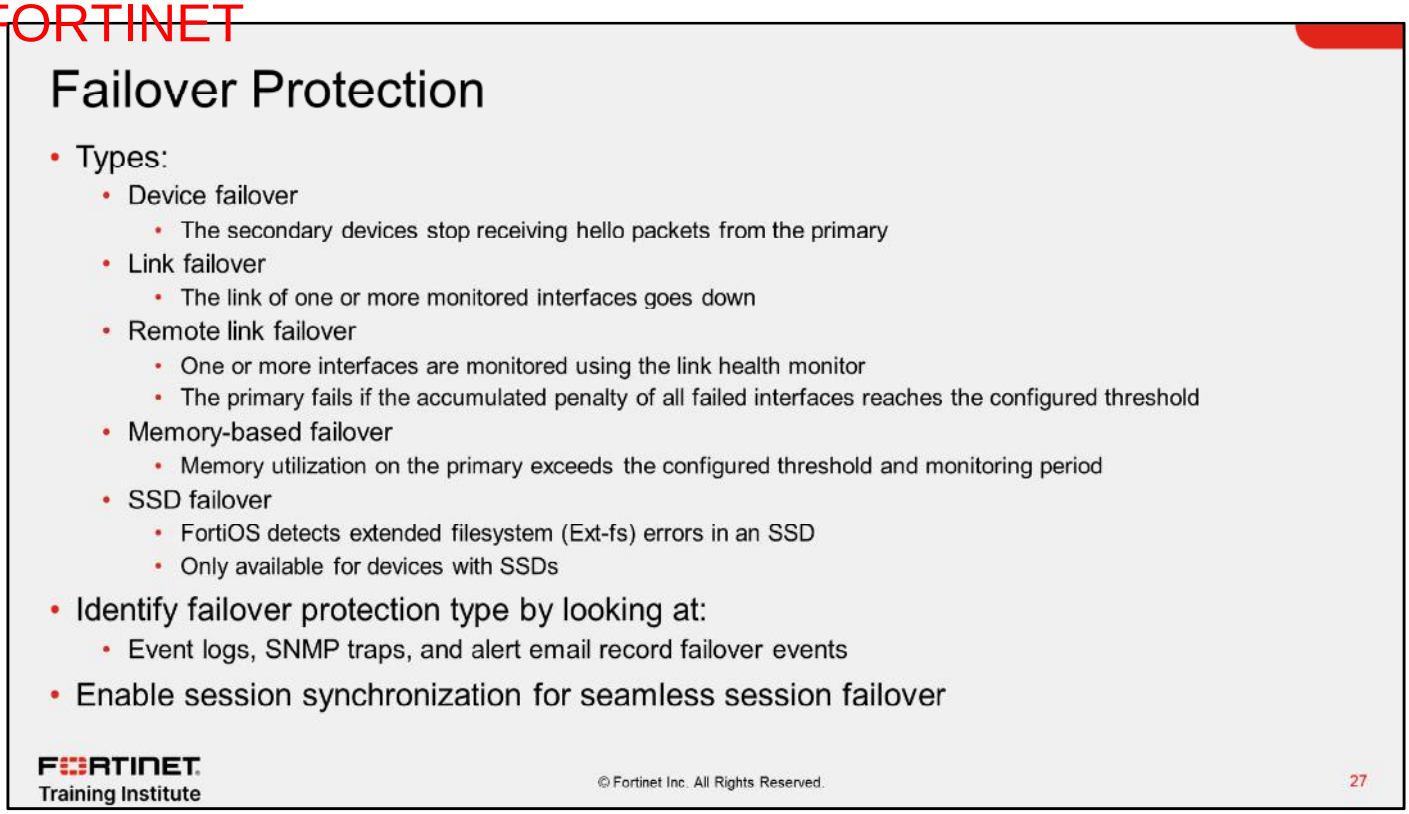
Good job! You now understand HA cluster synchronization.

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



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.



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.

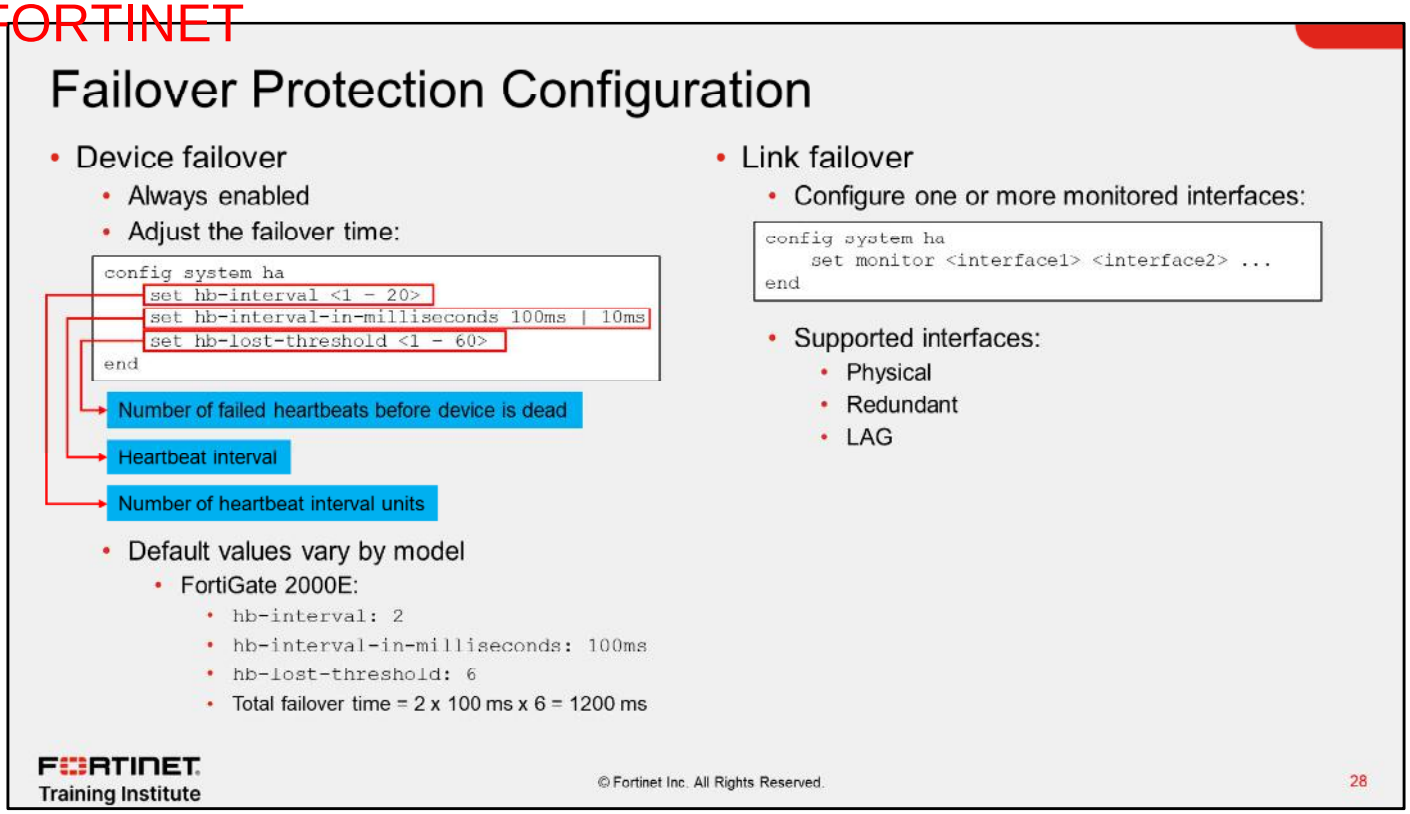
A link failover occurs when the link status of a monitored interface on the primary FortiGate goes down. You can configure an HA cluster to monitor one or more interfaces. If a monitored interface on the primary FortiGate is unplugged, or its link status goes down, a new primary FortiGate is elected.

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.

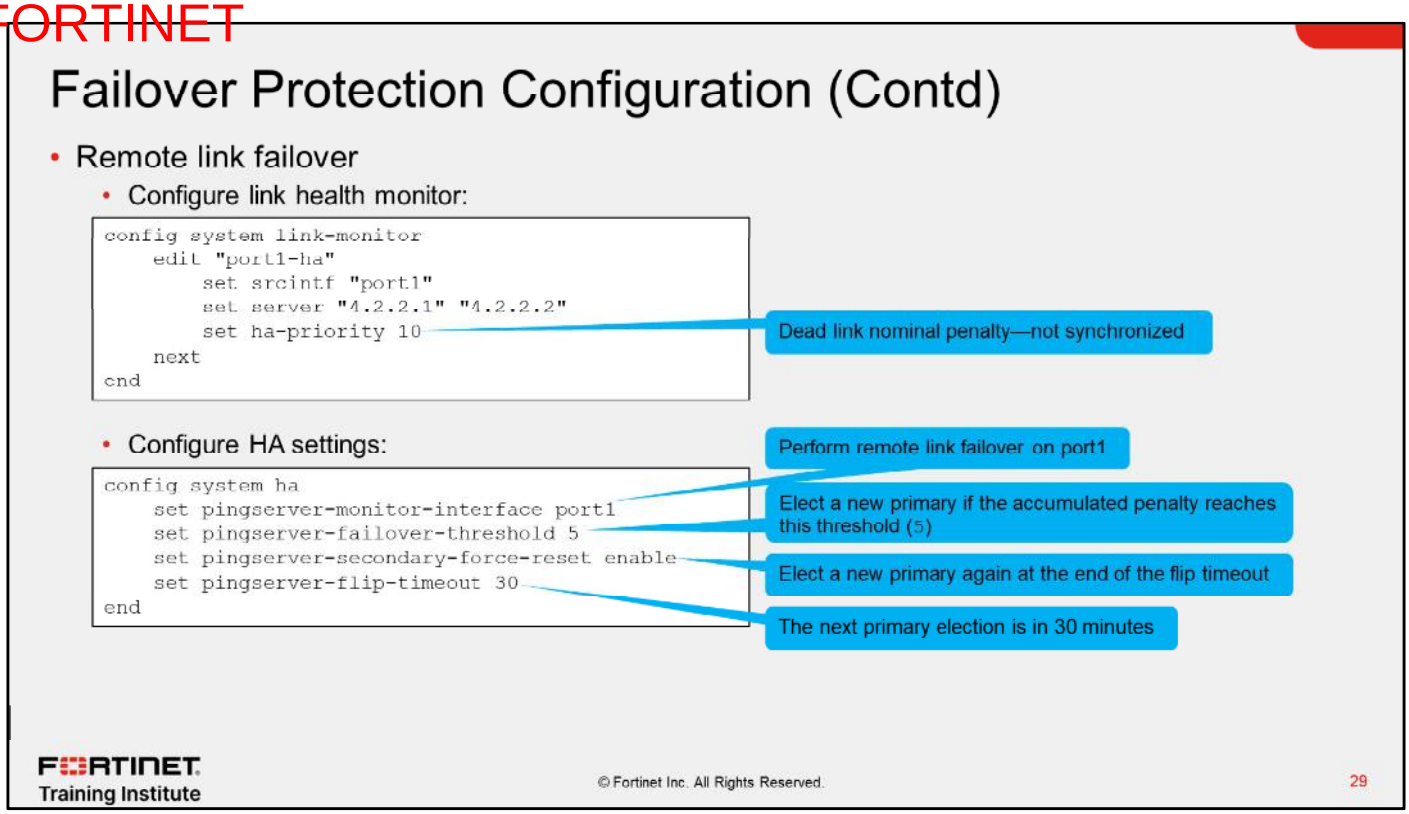
Make sure that you enable session pickup for sessions you want to protect from a failover event. This way, the new primary can resume traffic for these sessions.



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.



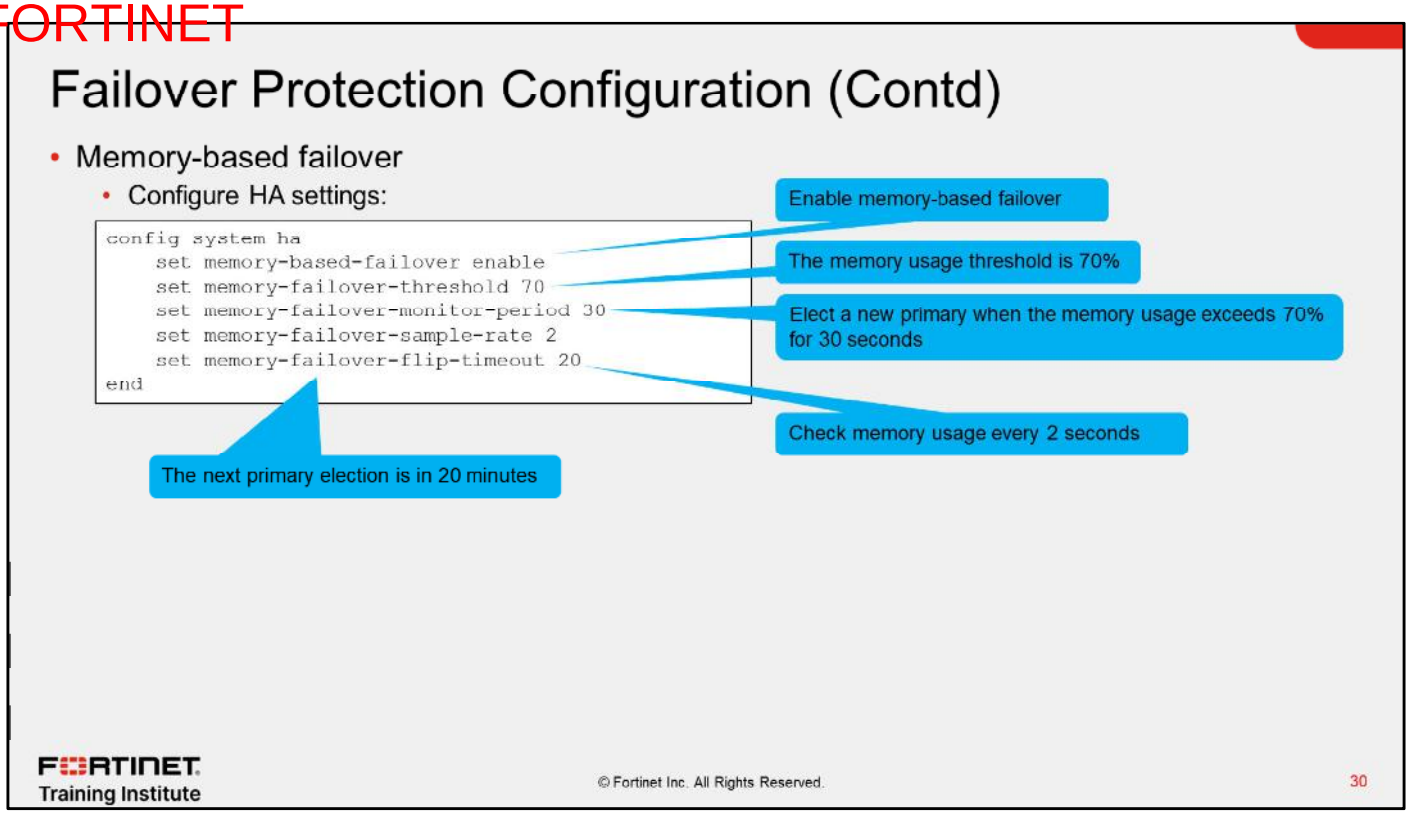
This slide shows a configuration example for remote link failover.

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.

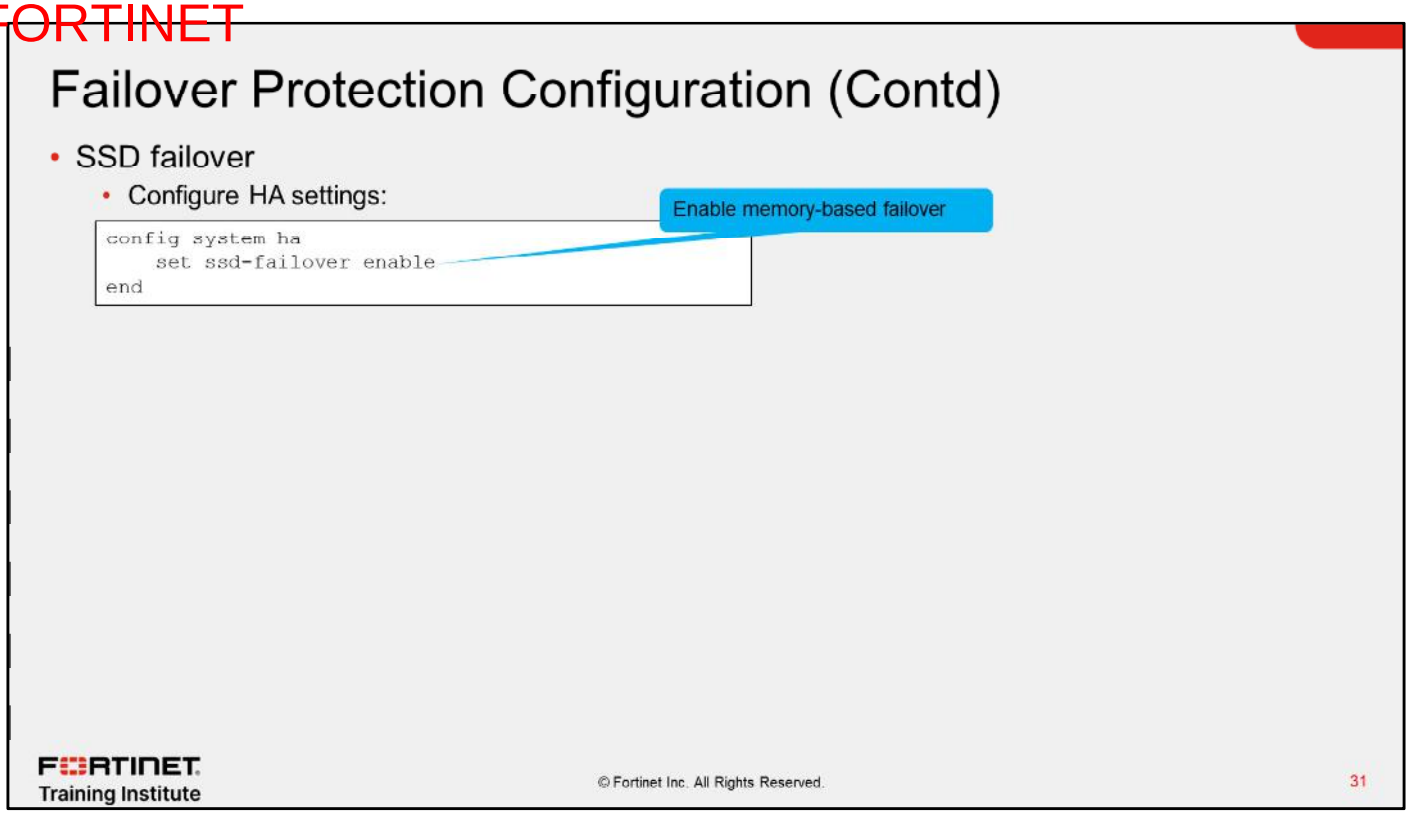
If during the primary election, the accumulated penalty of all members is the same, then other criteria, such as monitored interfaces, priority, uptime, and so on, are used as tiebreakers to elect the new primary.



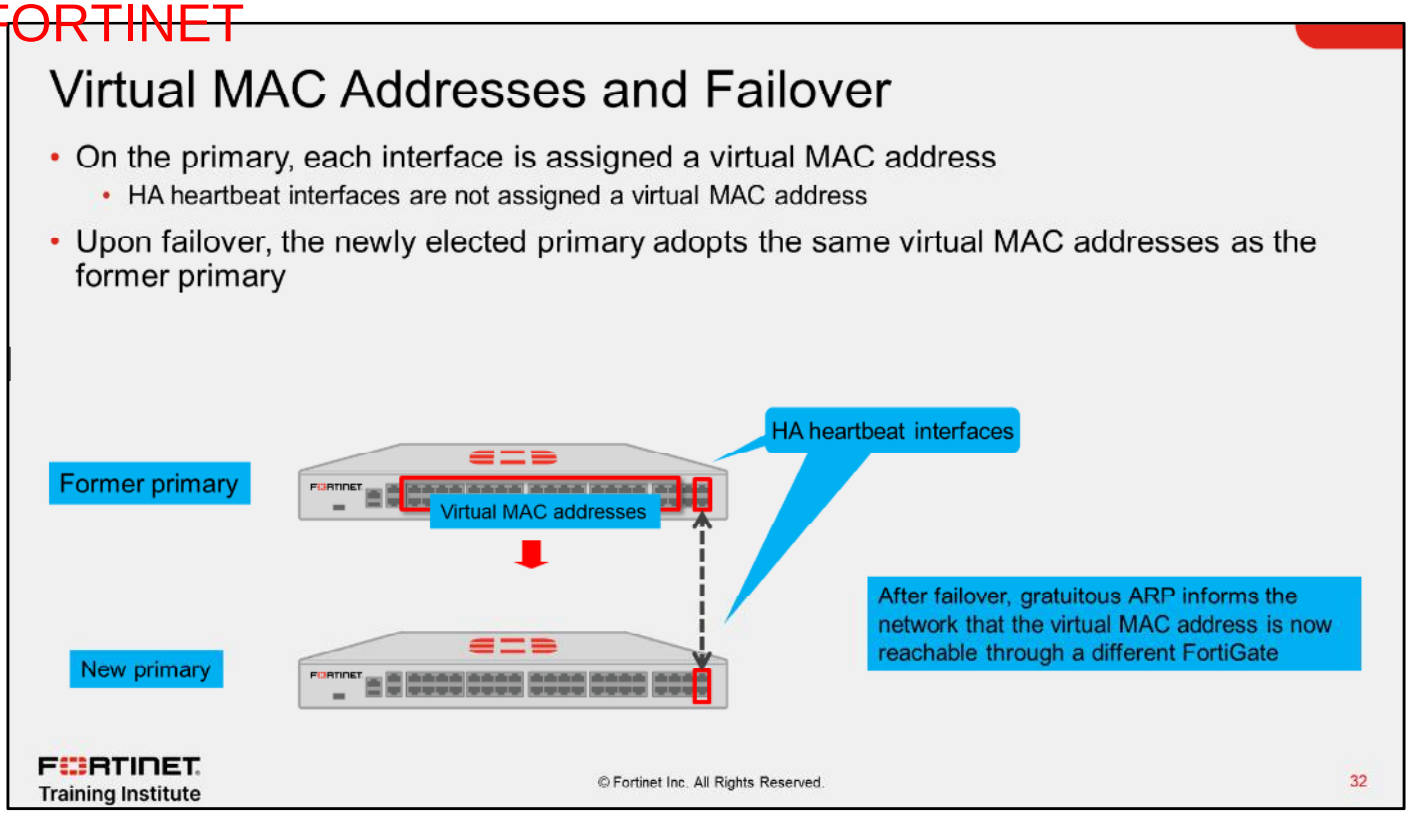
The HA configuration shown on this slide instructs FortiGate to perform memory-based failover as follows:

- 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.



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.

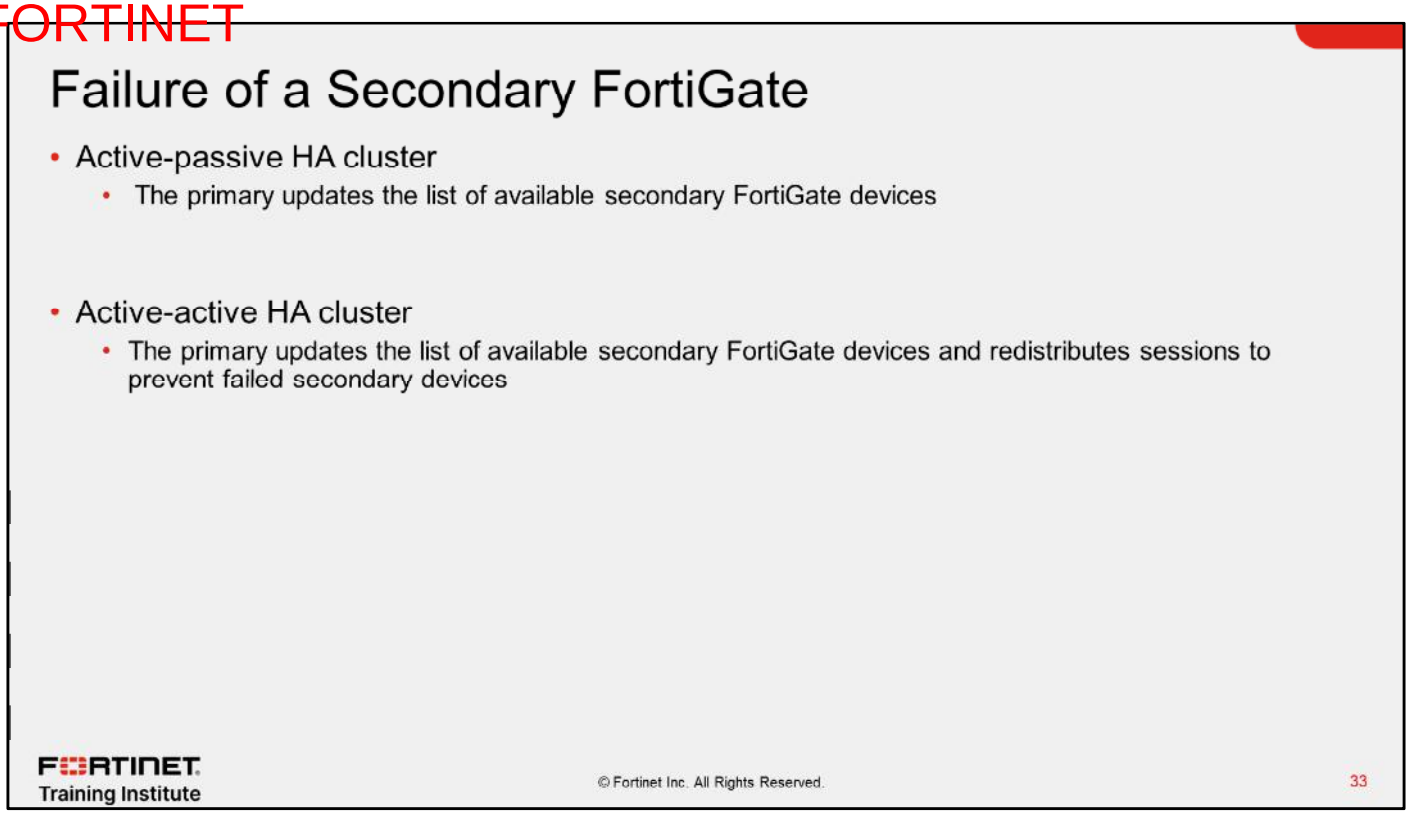


To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses. When a primary joins an HA cluster, each interface is assigned a virtual MAC address. The HA group ID is used in the creation of virtual MAC addresses assigned to each interface. So, if you have two or more HA clusters 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.

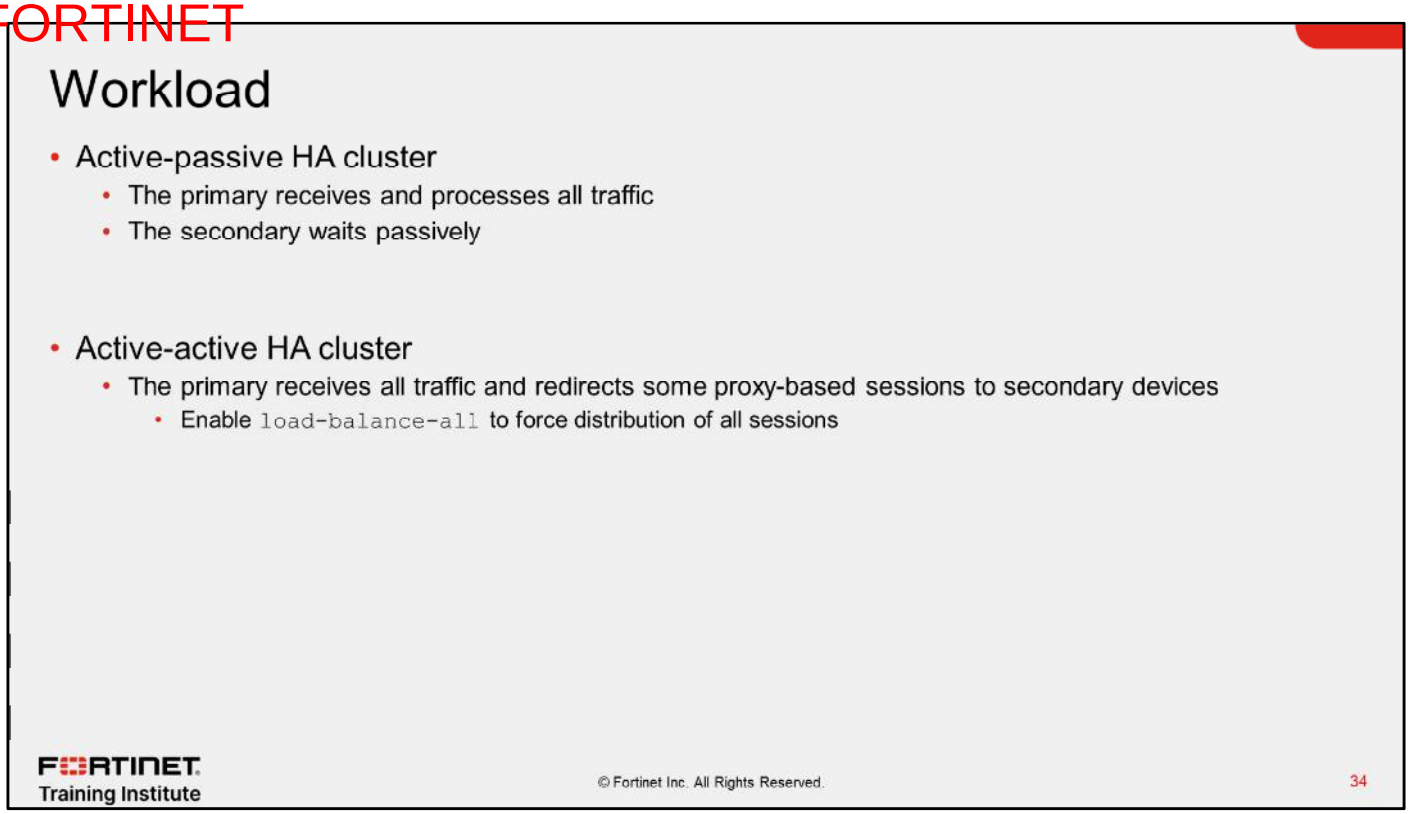
Note that the MAC address of a reserved HA management interface is not changed to a virtual MAC address. Instead, the reserved management interface keeps its original MAC address.



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.

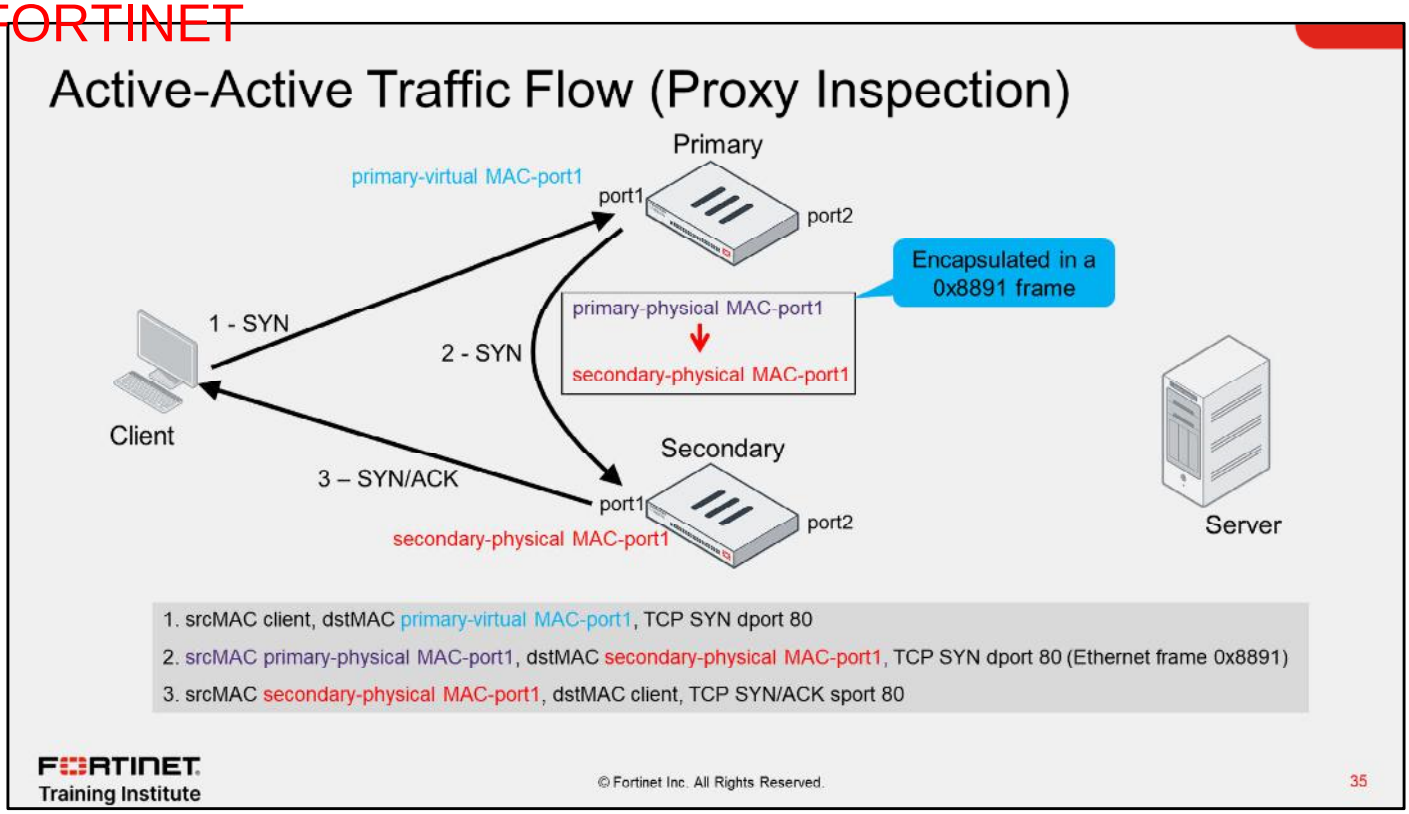
In an active-passive cluster, the primary only updates its list of available secondary FortiGate devices. It also starts monitoring for the failed secondary, waiting for it to come online again.

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.



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.

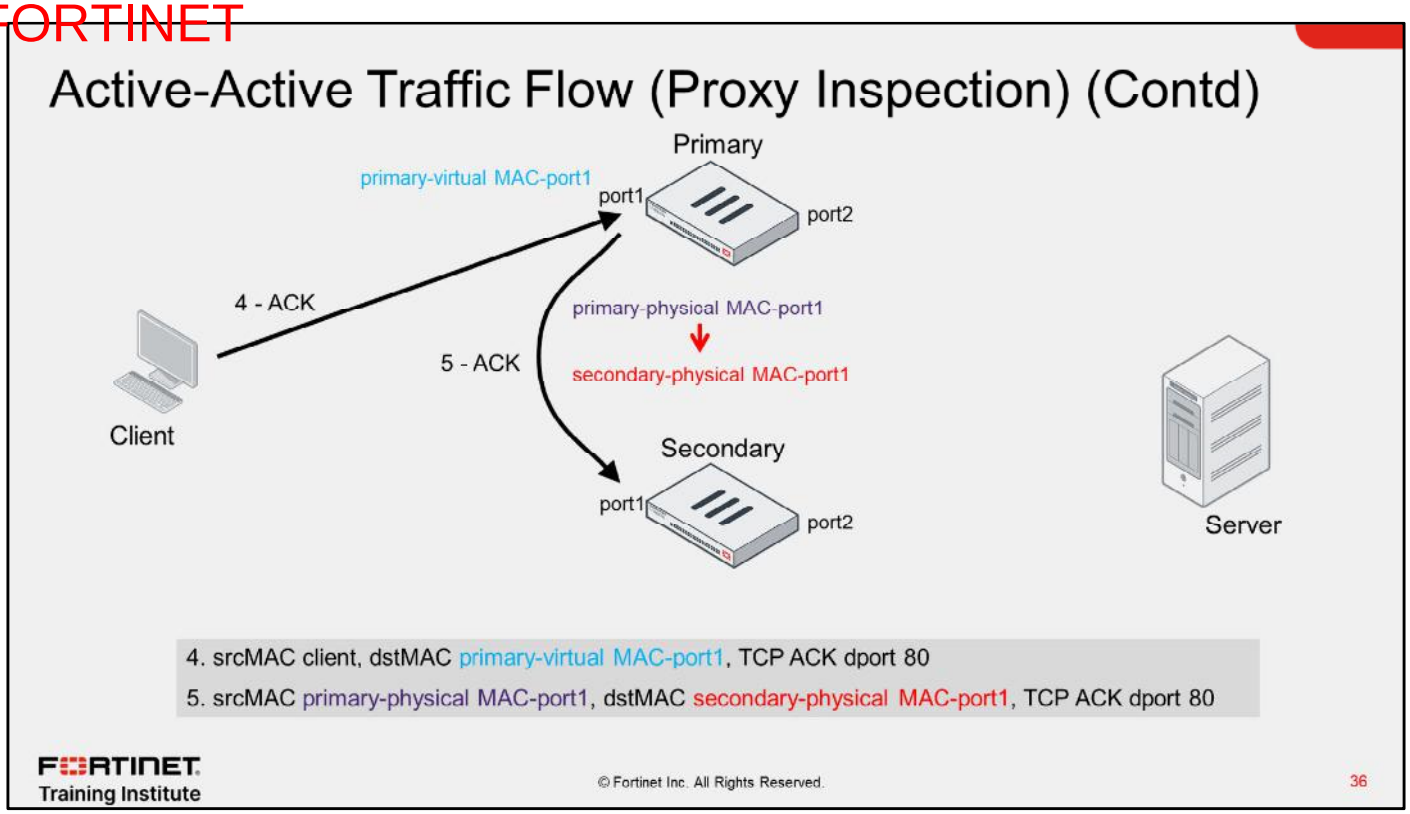


In active-active mode, the following occurs:

- 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.

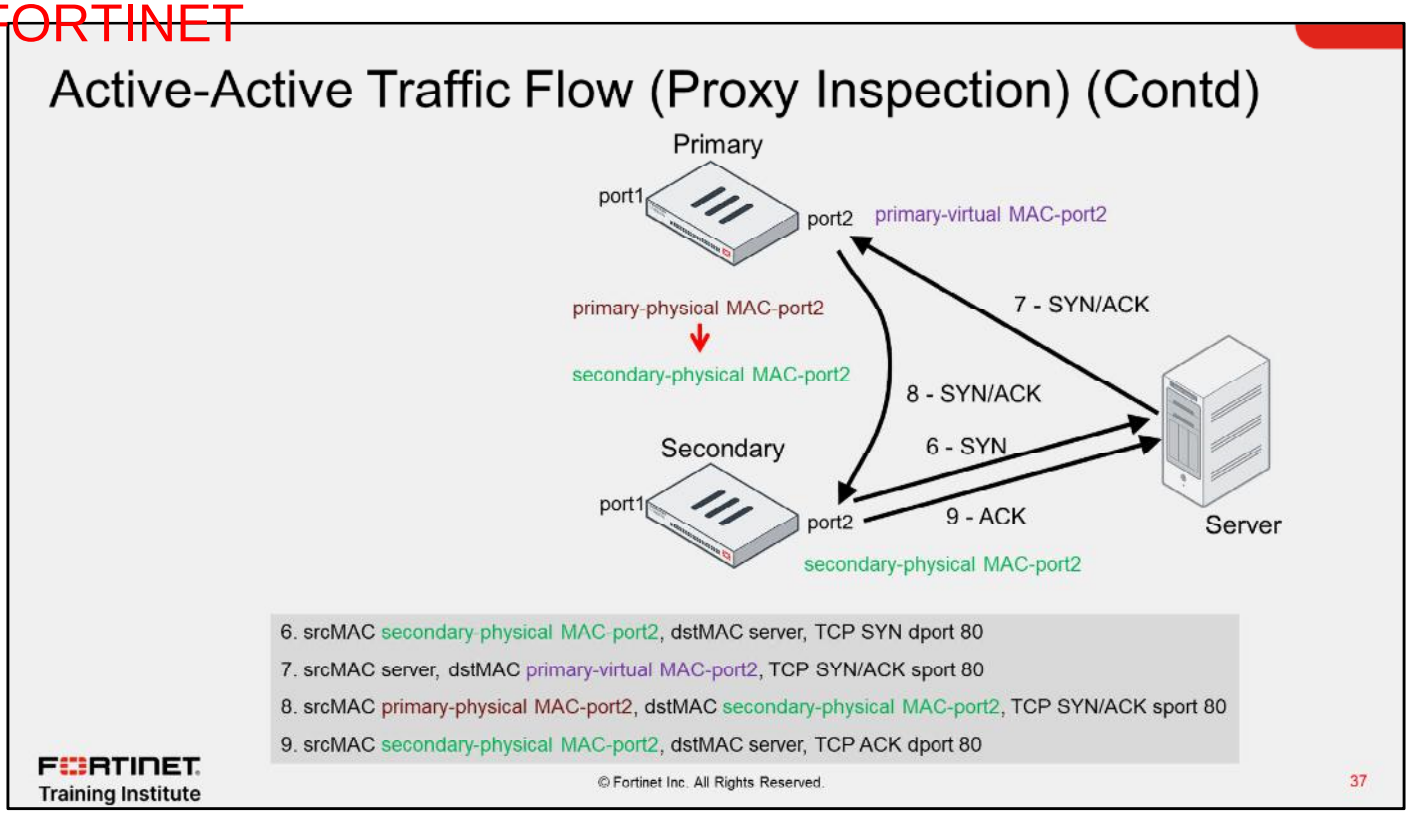
This slide shows the flow for distributed traffic that is subject to proxy inspection:

1. 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.
2. 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.
3. 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.



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.



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.

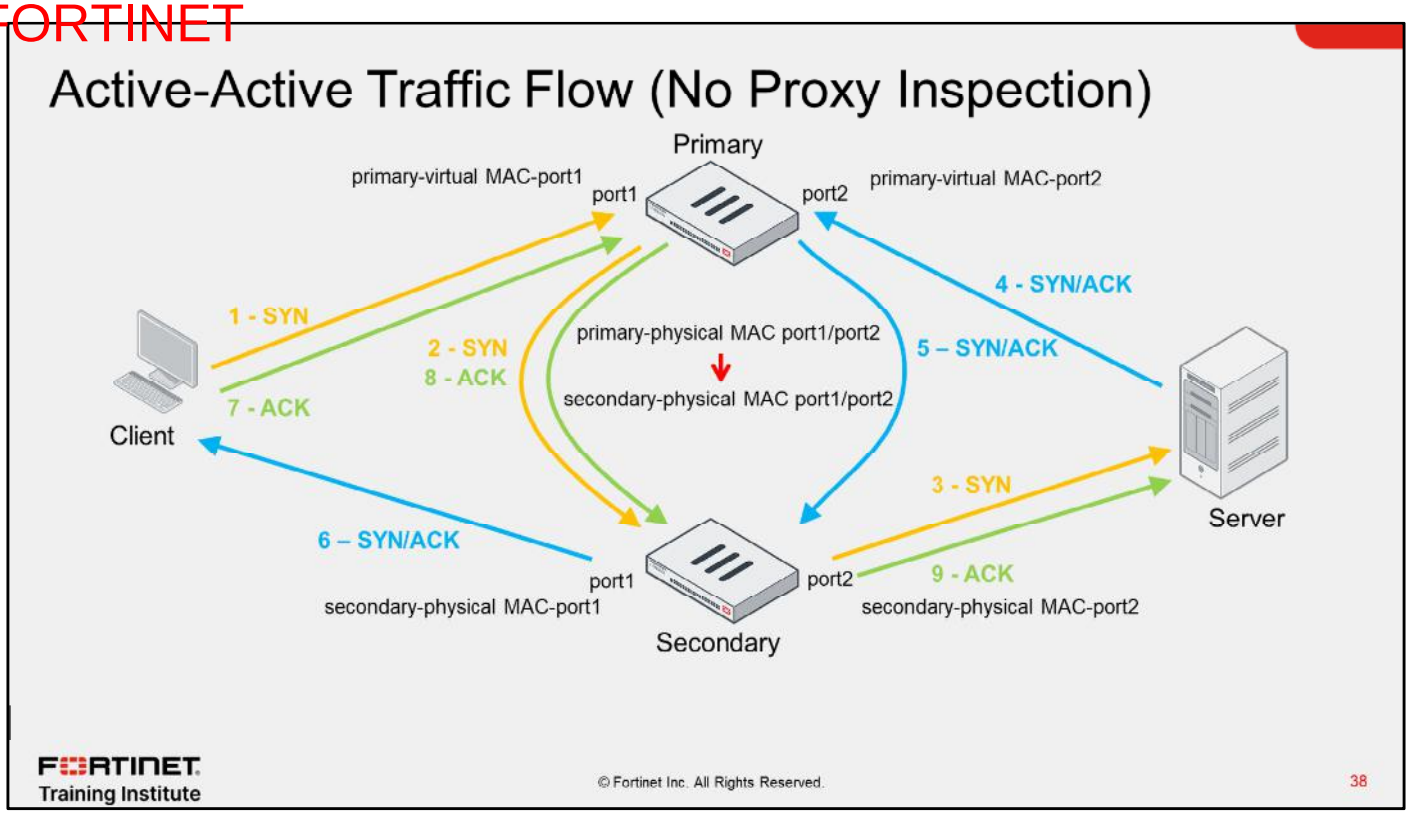
7. The SYN/ACK packet from the server is sent to port2 on the primary. The destination MAC address is the virtual MAC address of port2.

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.

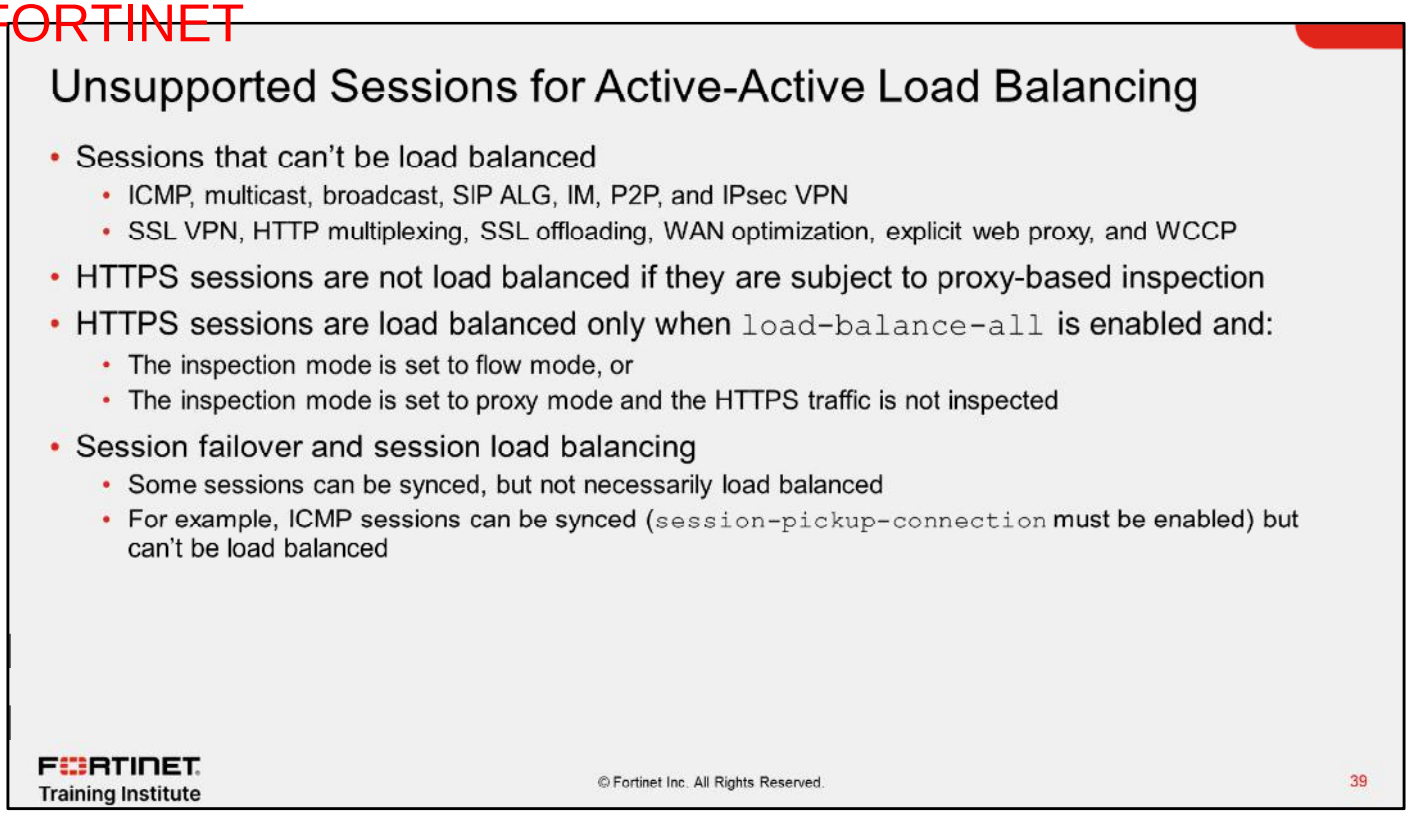
Note that the goal of active-active mode is to leverage unused CPU and memory resources on secondary devices. The intention is not really to load balance traffic. In fact, because the traffic from endpoints is always sent to the primary, you usually see more traffic on the primary than any secondary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



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.



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.

Active-Active Load Balancing Methods

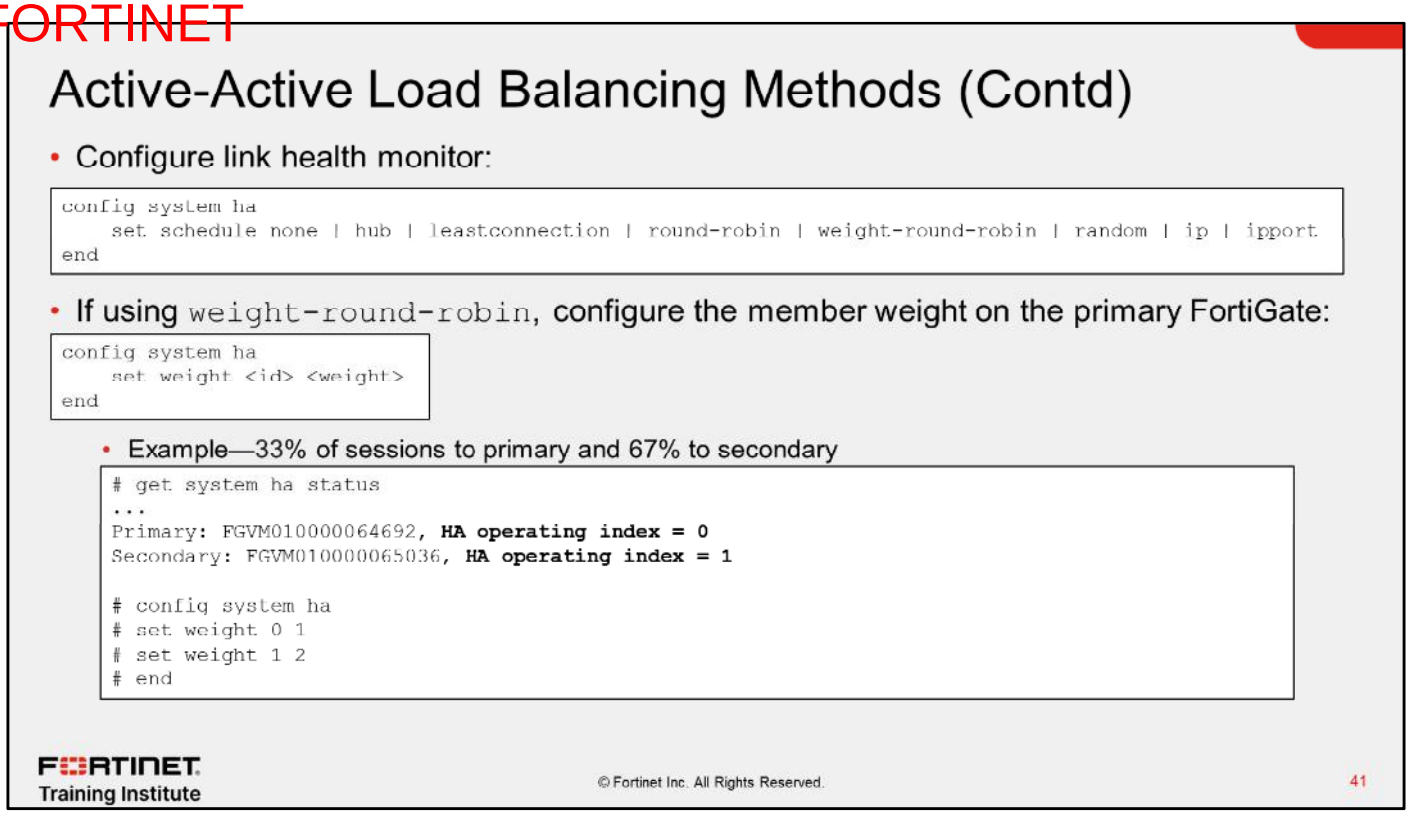
Method	Description
none	The primary handles all sessions
leastconnection	Sessions are sent to the member with the least number of sessions
round-robin	Default method. Sessions are distributed equally across members
weight-round-robin	The more weight a member is assigned, the more sessions it handles
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

FORTINET Training Institute

40

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.



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

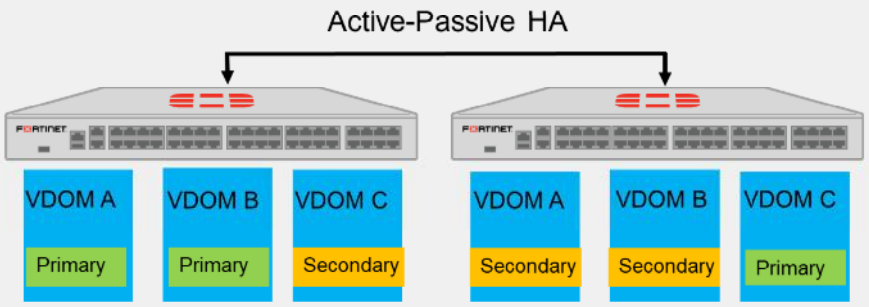
When you select the `weight-round-robin` method, you must also configure the weight for each member, as shown on this slide. You indicate the member ID followed by its weight. The higher the member weight, the more sessions are distributed to that member. You can obtain the member ID from the output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

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



FORTINET Training Institute

42

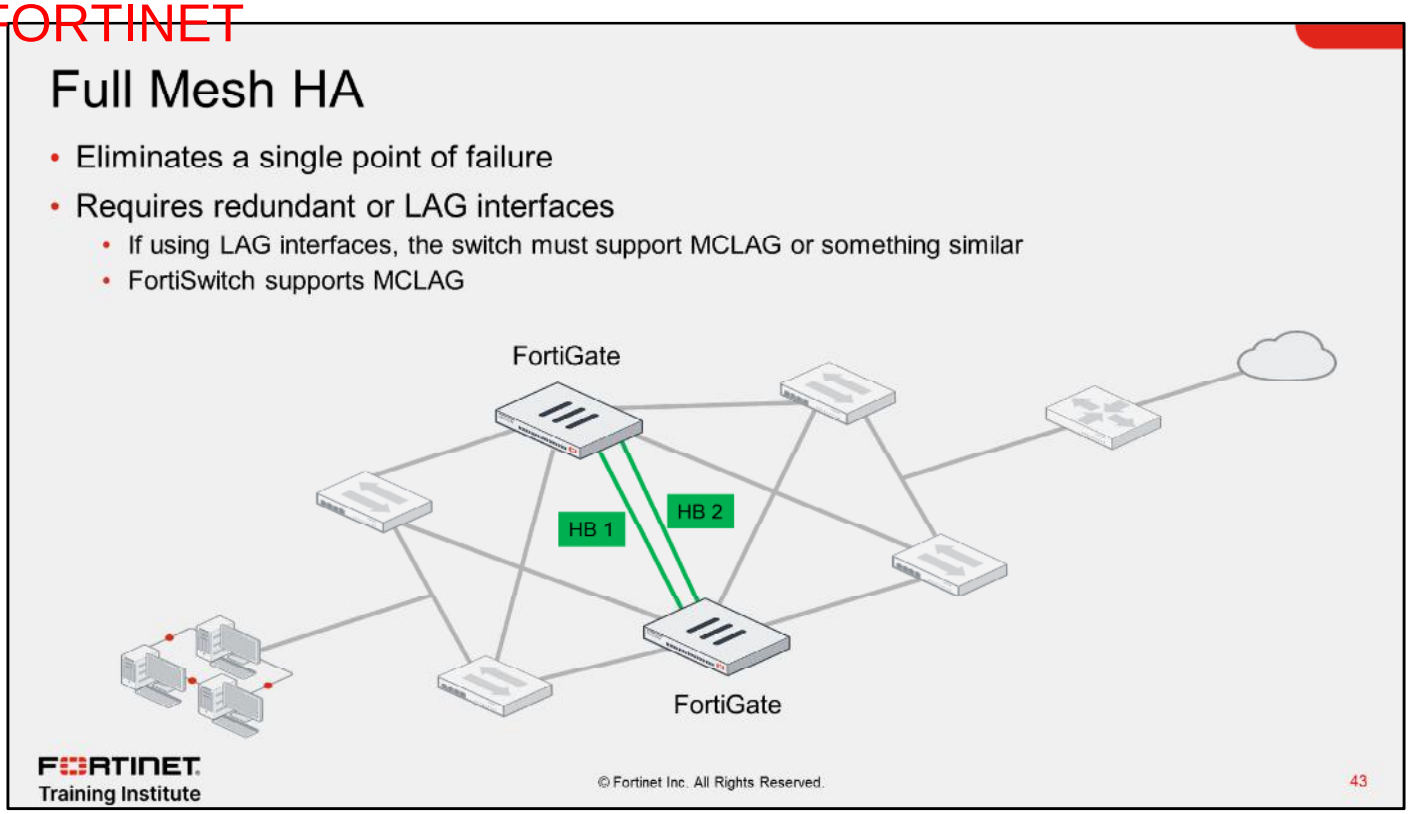
So far, you've learned about HA clustering where each FortiGate device acts as a whole security domain.

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.



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.

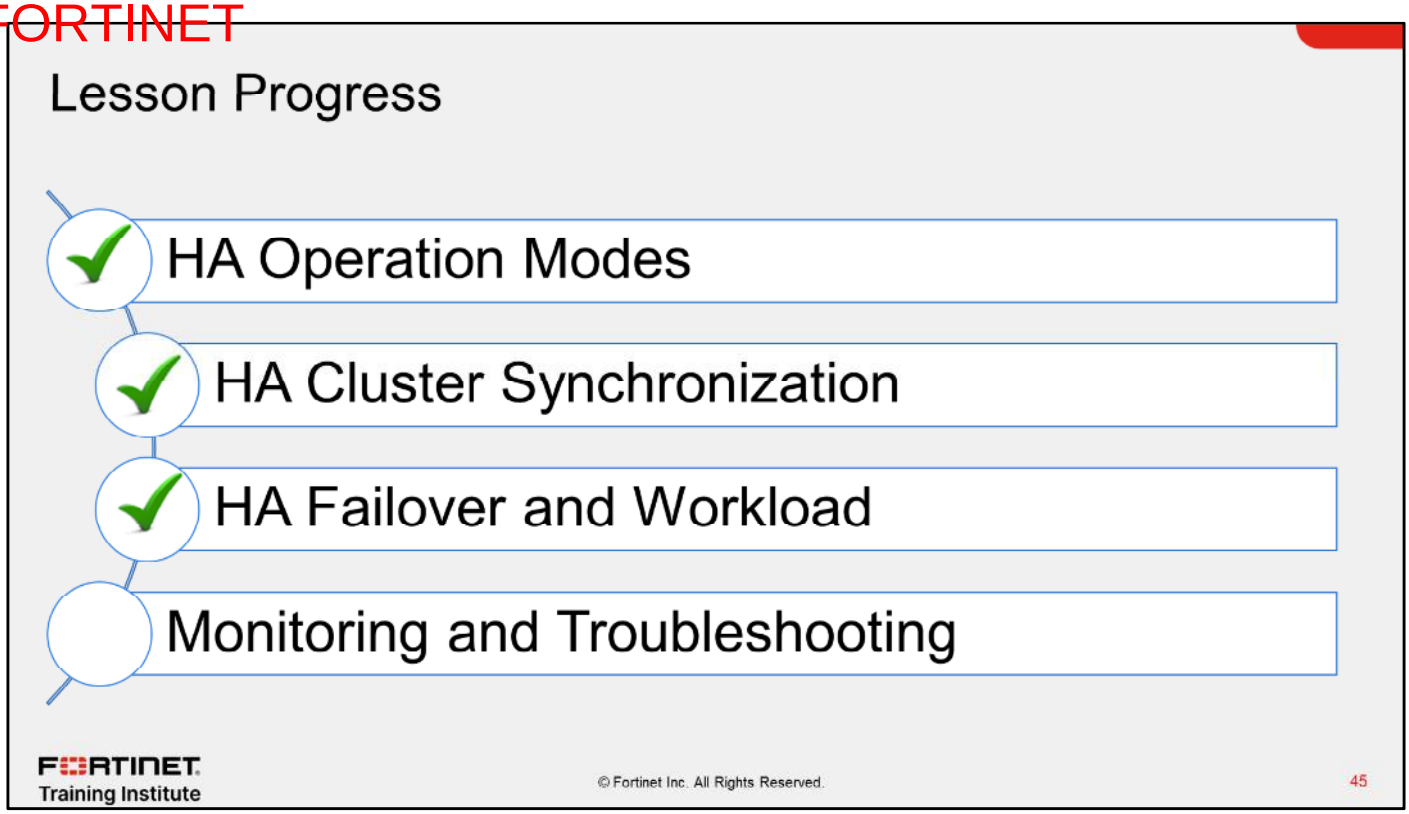
Knowledge Check

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

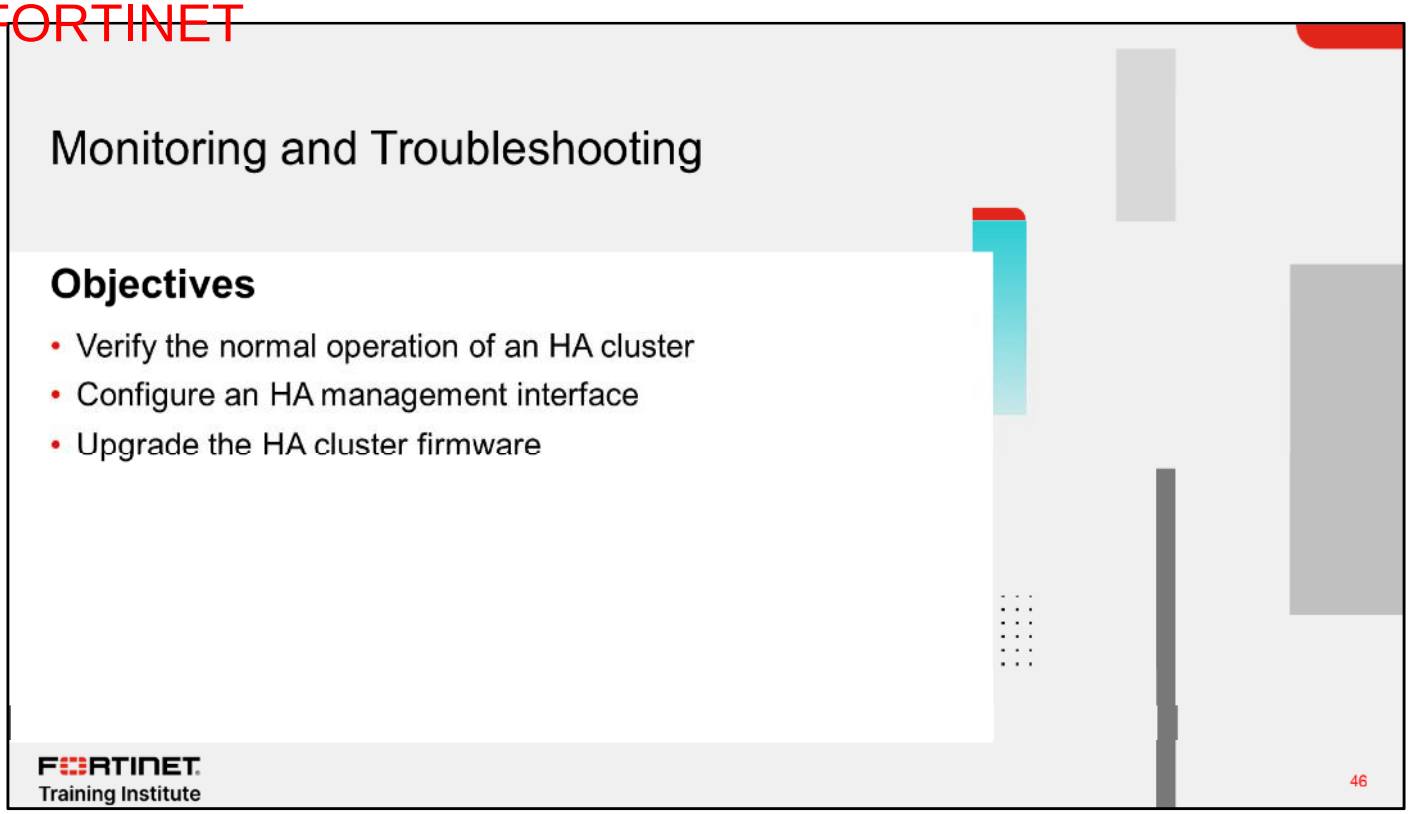
FORTINET Training Institute

44



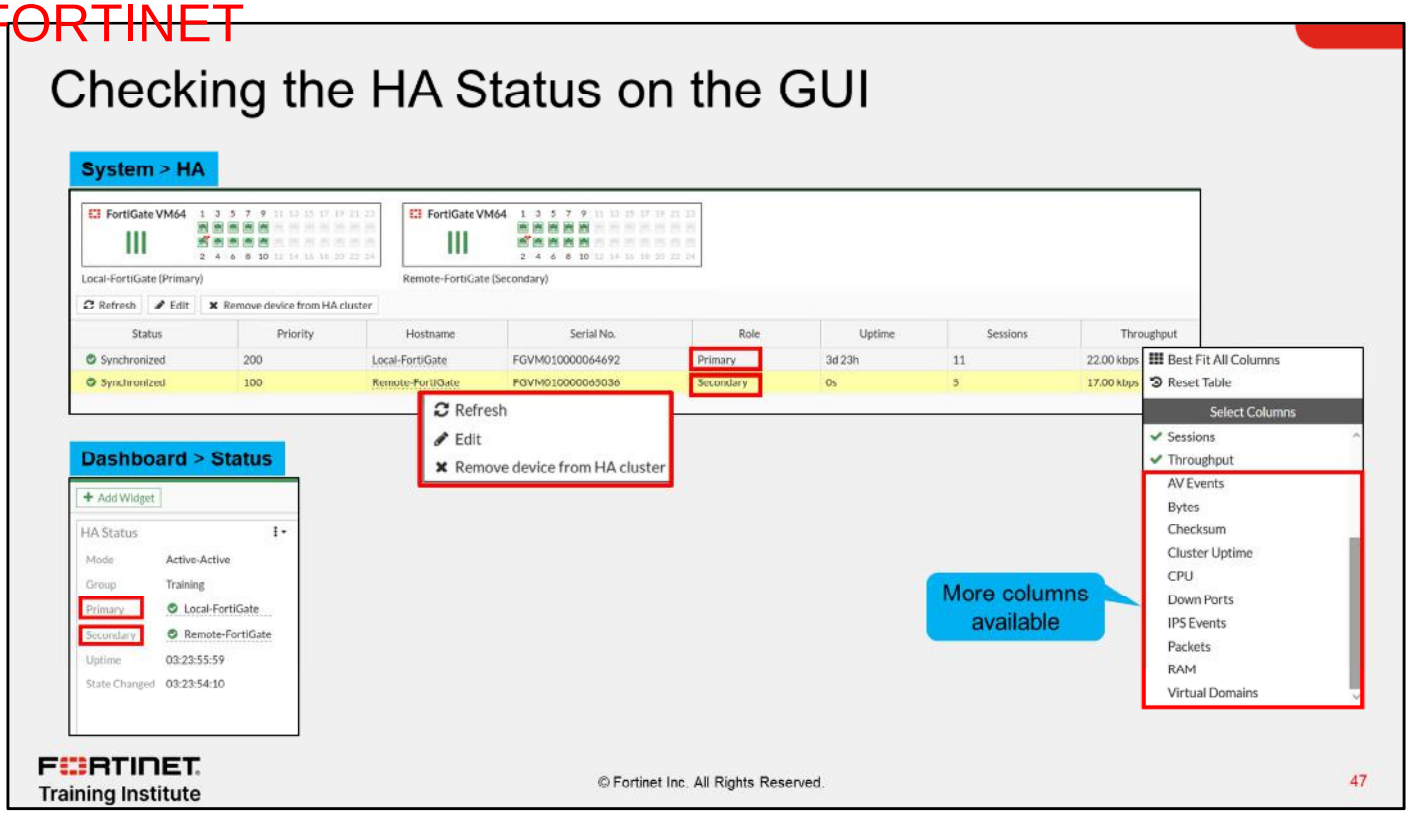
Good job! You now understand HA failover and workload.

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



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

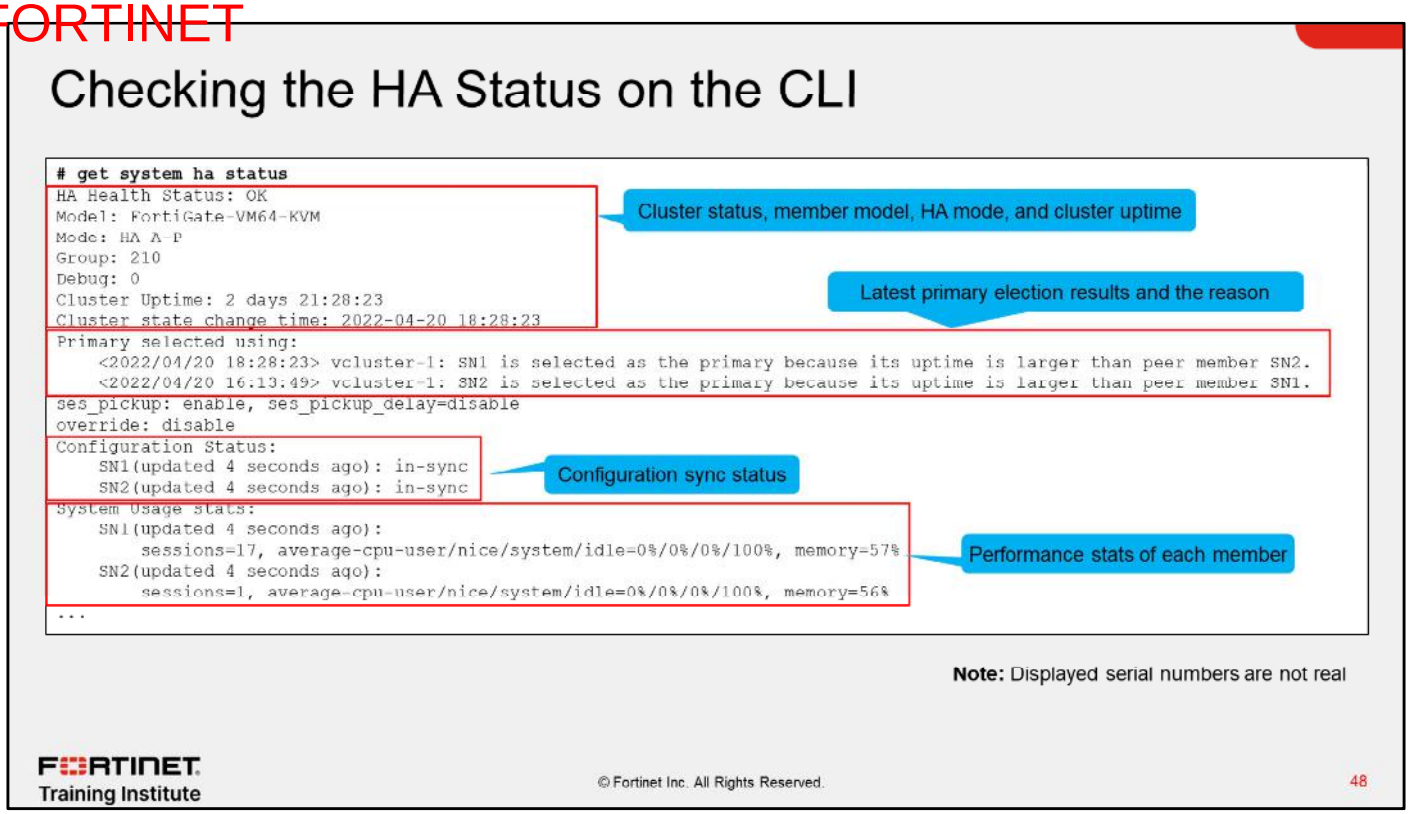
By demonstrating competence in monitoring and troubleshooting, you will be able to make sure the cluster is synchronized properly. You will also learn how to configure and access secondary devices in an HA cluster and how to upgrade the firmware on the HA cluster.



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.



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

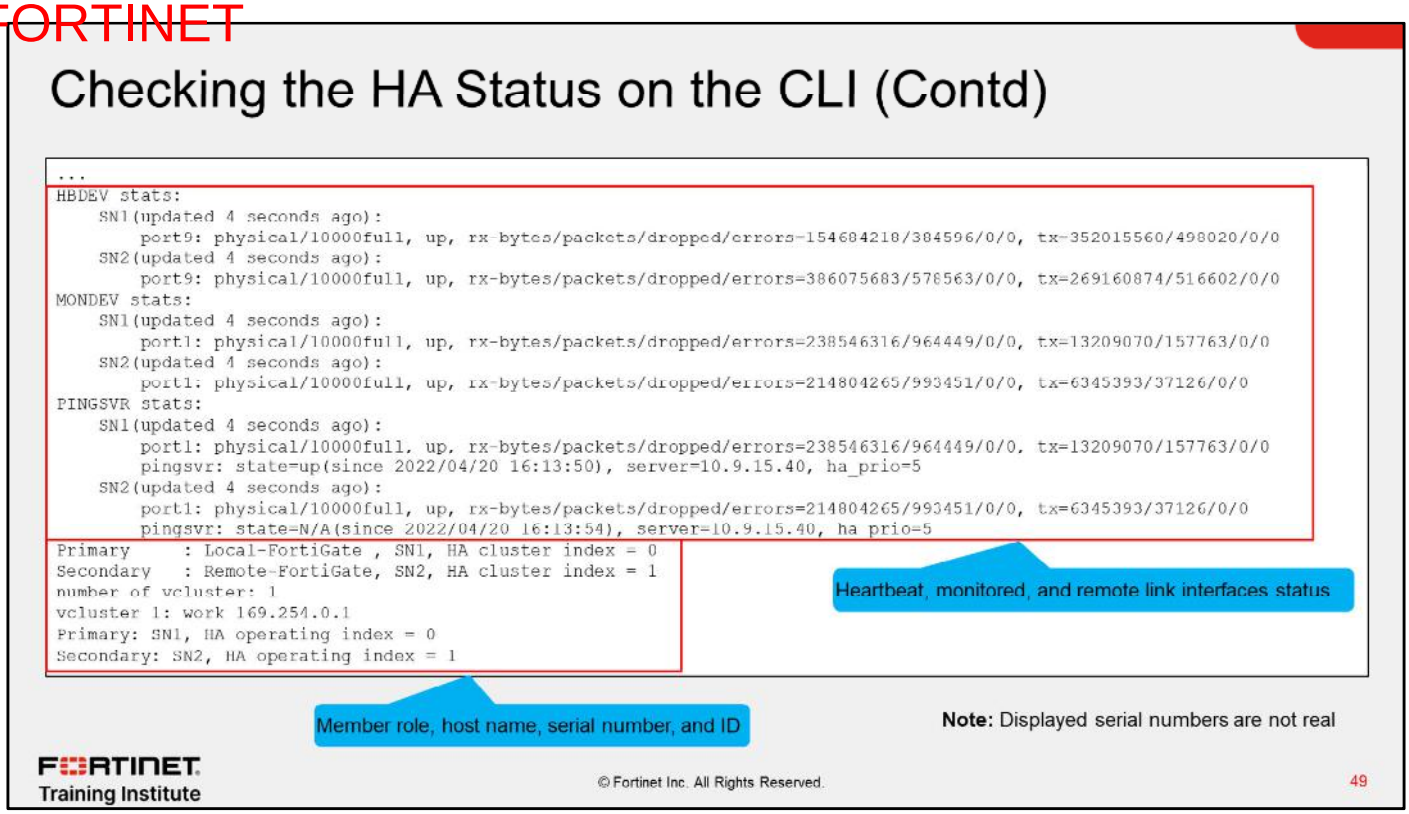
The command displays comprehensive HA status information in a user-friendly output and is usually executed as the first step when troubleshooting HA. This slide shows the first part of an example output that the command provides. Note that the serial numbers of members have been replaced by fake ones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

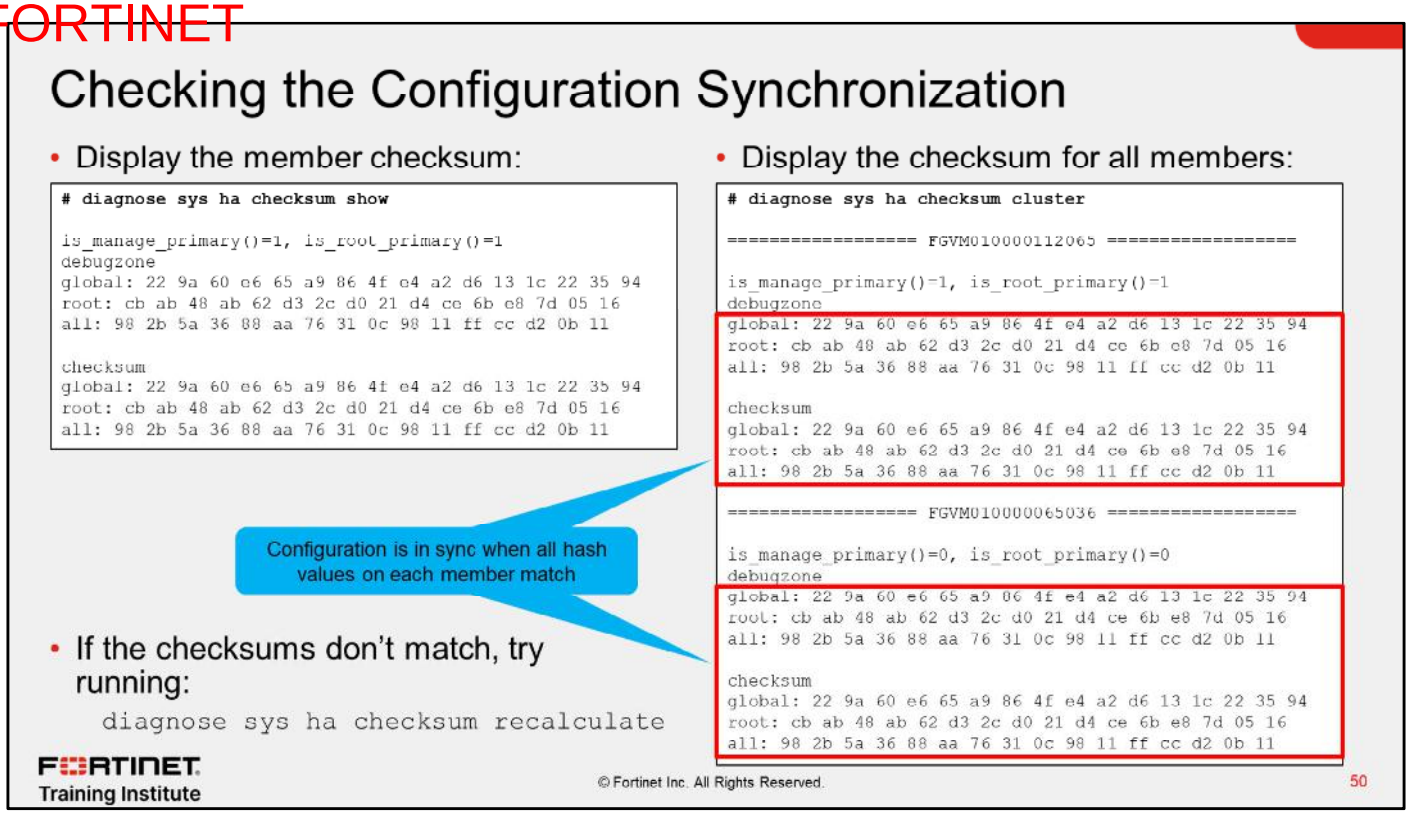
Following the configuration status information, you can see the system usage statistics, which report on performance statistics for each member. They indicate the number of sessions that each member handles, as well as the average CPU and memory usage. Note that the `sessions` field accounts for any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



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.



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.

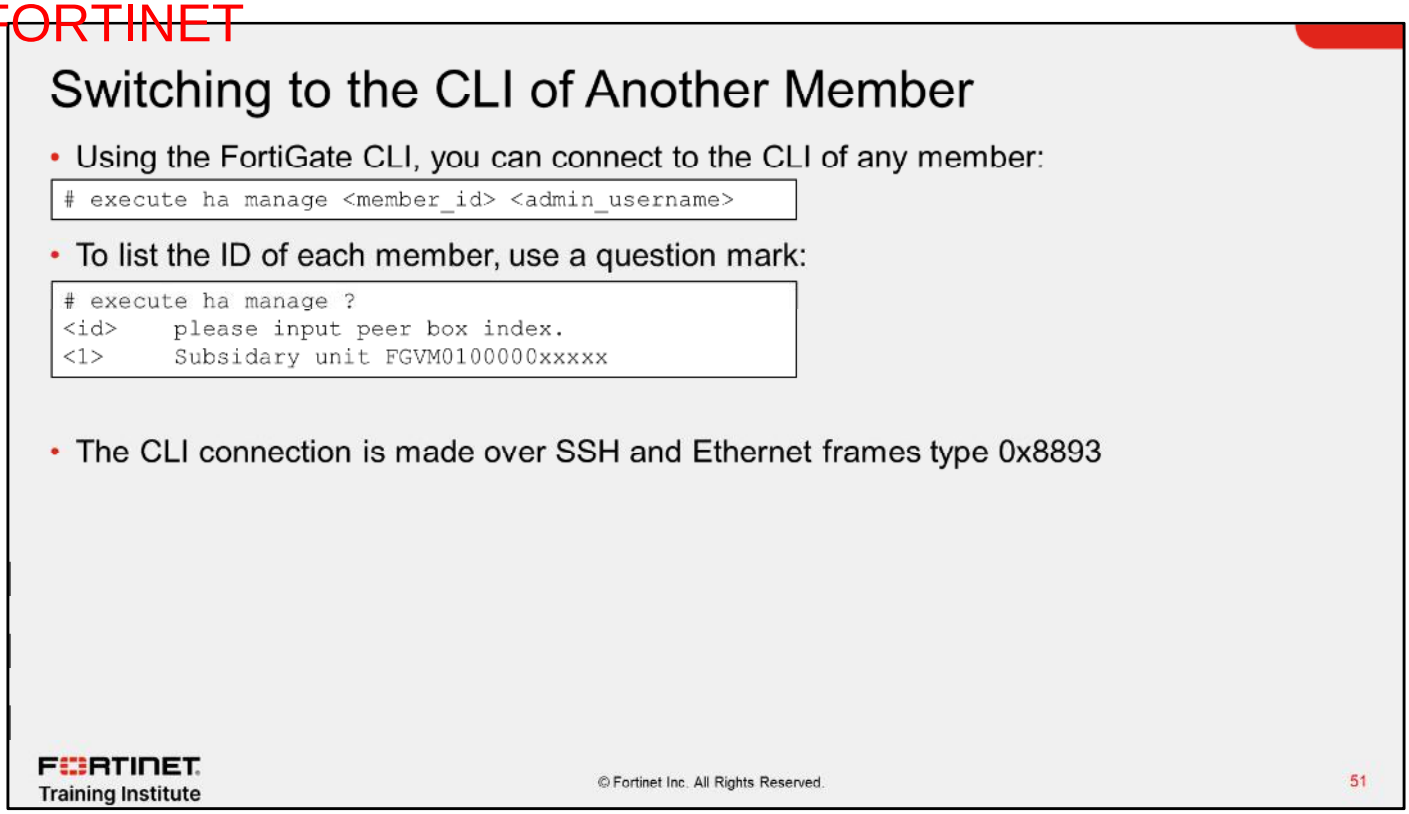
When you run the `diagnose sys ha checksum cluster` command, the checksum is polled from each member using the heartbeat interface. If HA is not working properly, of if there are heartbeat communication issues, then the command may not show the checksum for members other than the one you run the command 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.

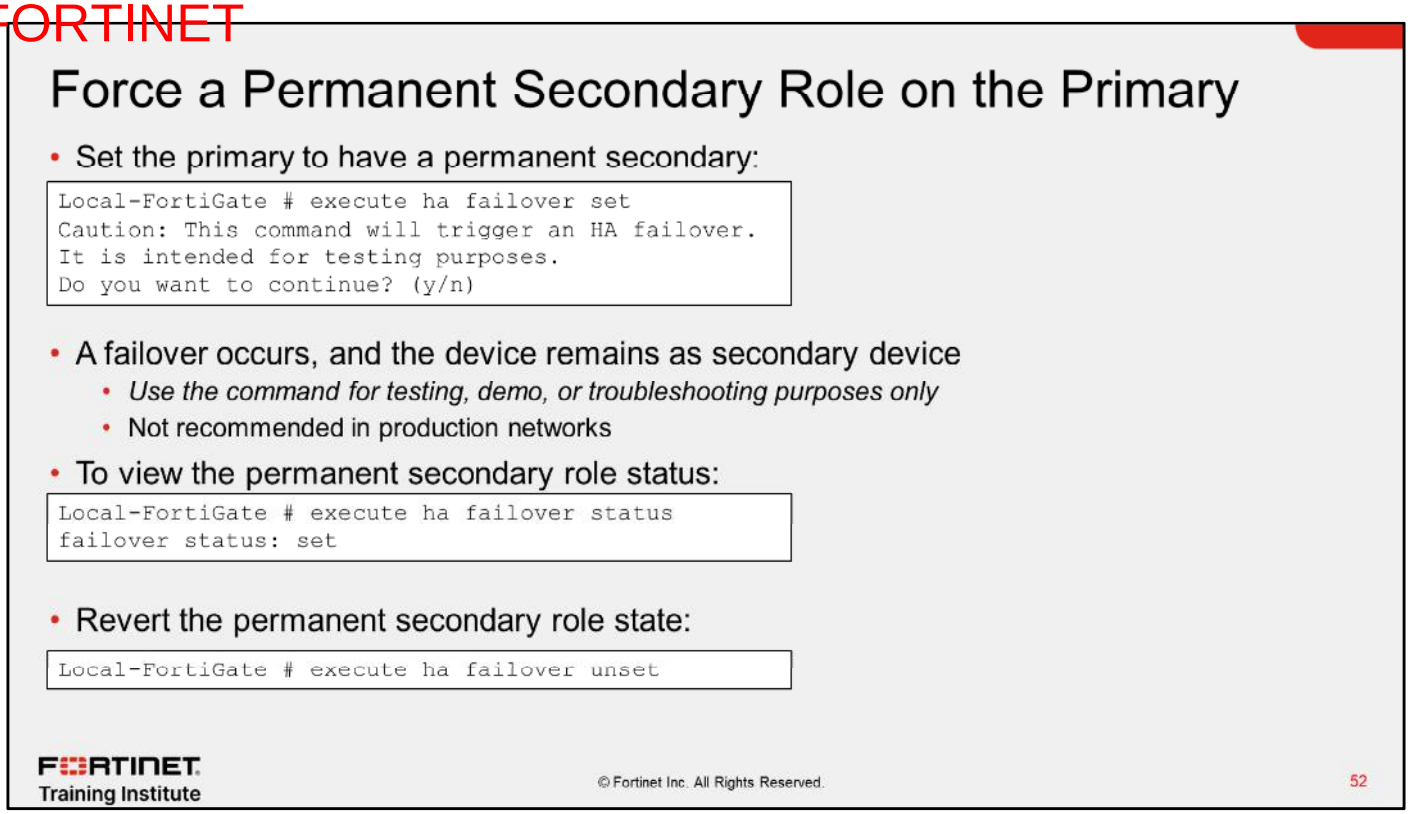


When troubleshooting HA, you may need to connect to the CLI of another member from the CLI of the member you are currently connected to. You do this by using the `execute ha manage` command to connect to the other member.

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.



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.

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
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 Training Institute

53

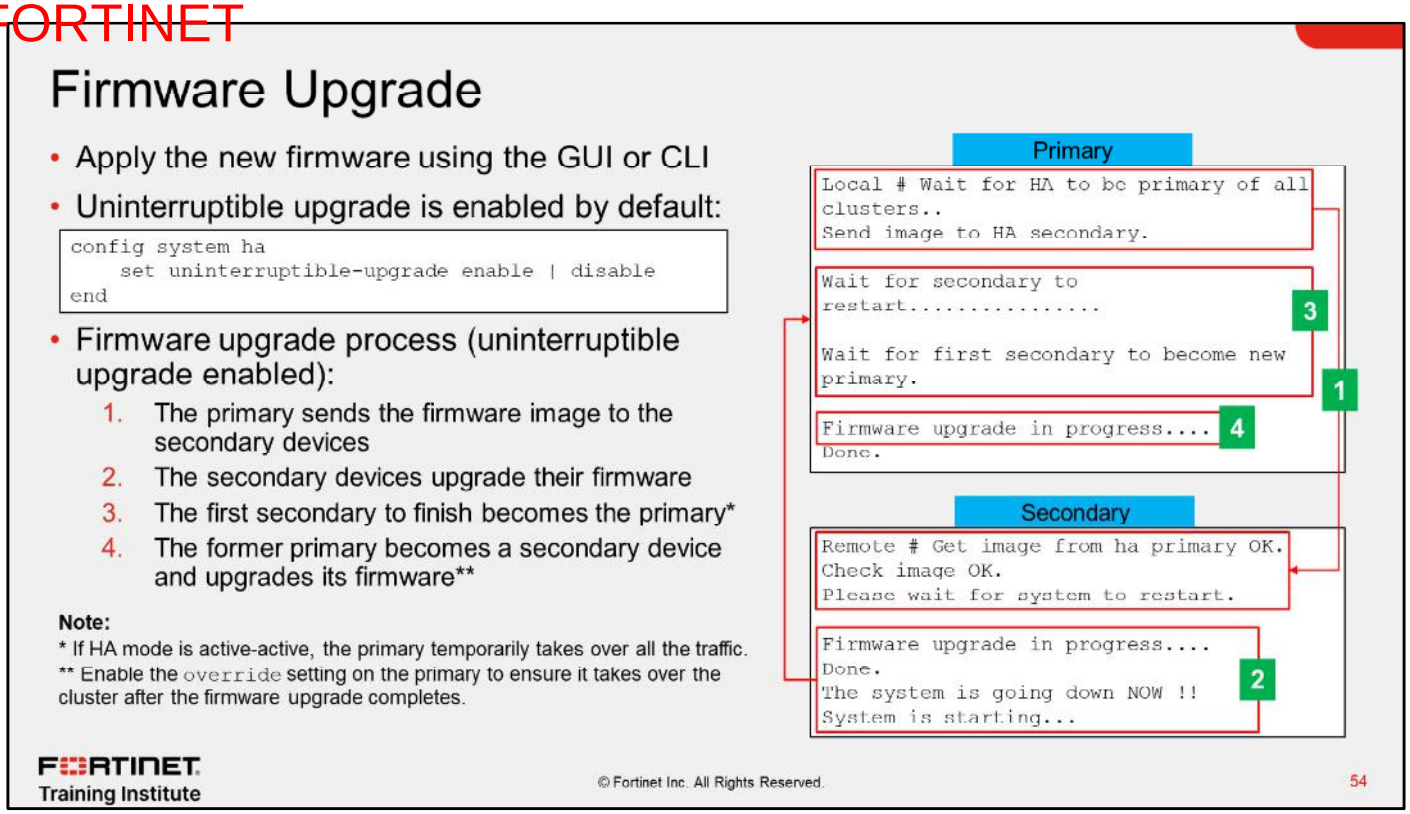
When you connect to a cluster using any of its virtual IP addresses, you always connect to the primary. You can then switch to the CLI of any member in the cluster by using the `execute ha manage` command. But what if you want to access the GUI of a secondary member or maybe poll data from it using SNMP?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



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 uninterruptible upgrade and is enabled by default. After the administrator applies the new firmware on the primary, uninterruptible 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 uninterruptable upgrade, as shown on this slide. Just keep in mind this will result in a service impact during the firmware upgrade.

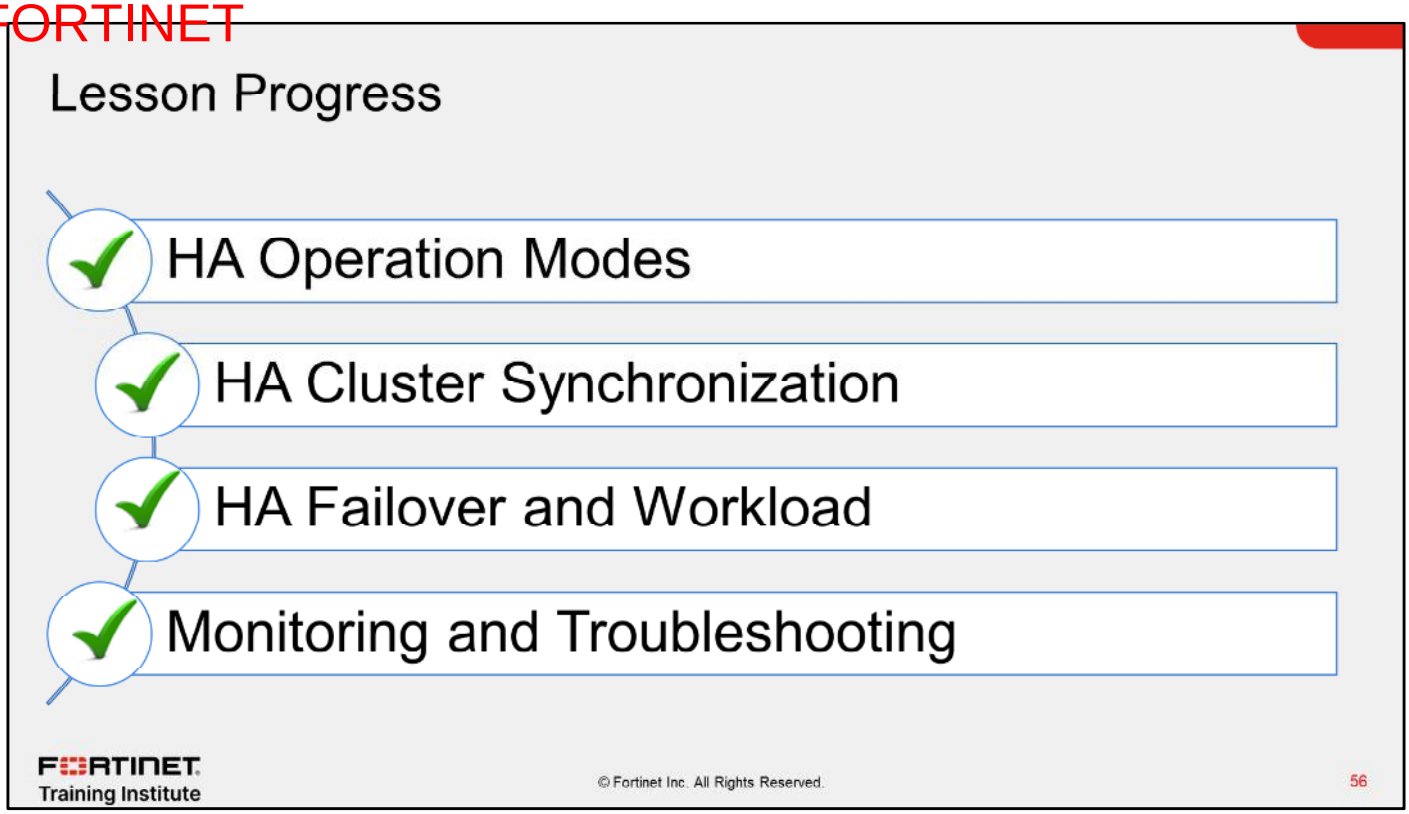
Knowledge Check

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.

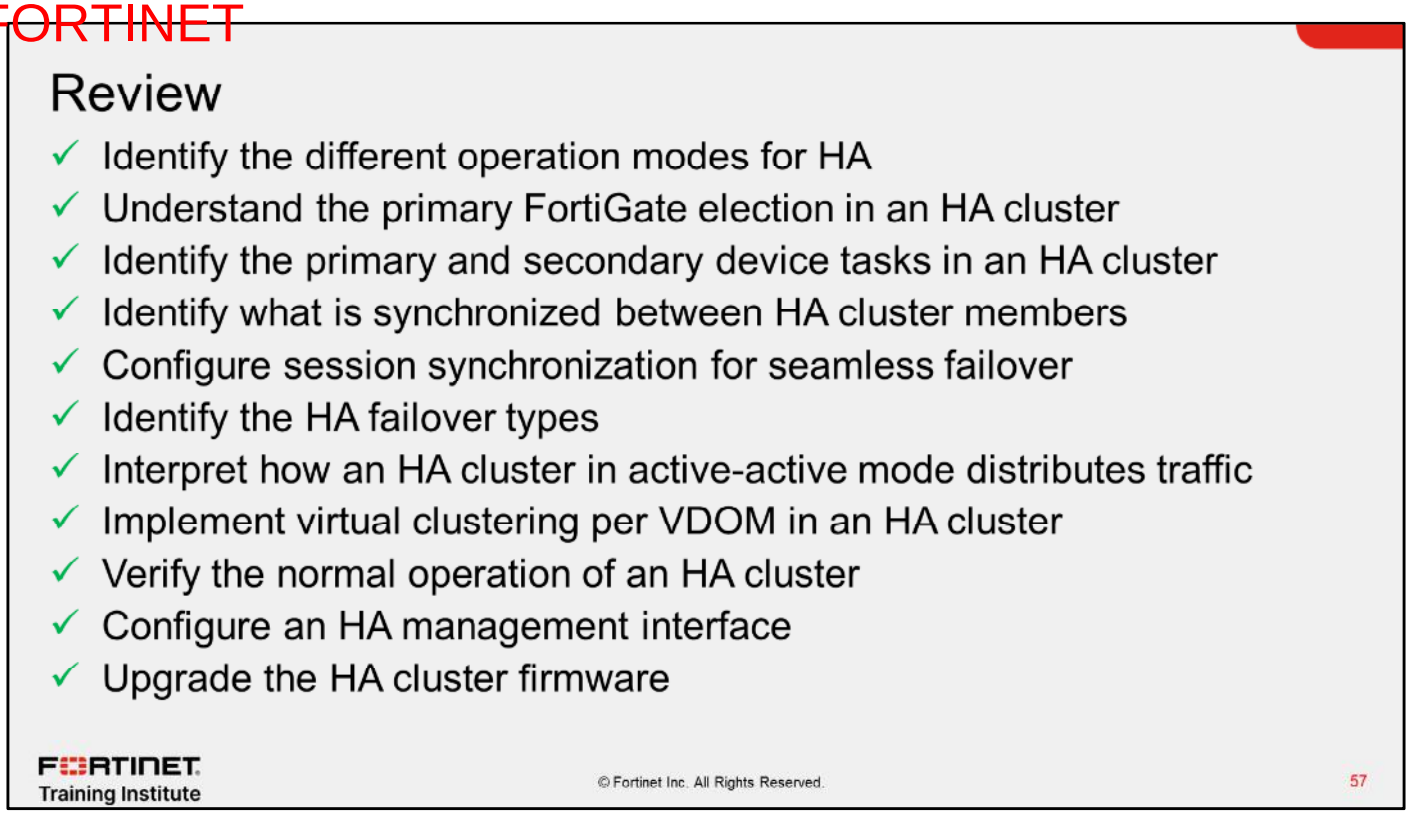
FORTINET Training Institute

55



Congratulations! You have completed this lesson.

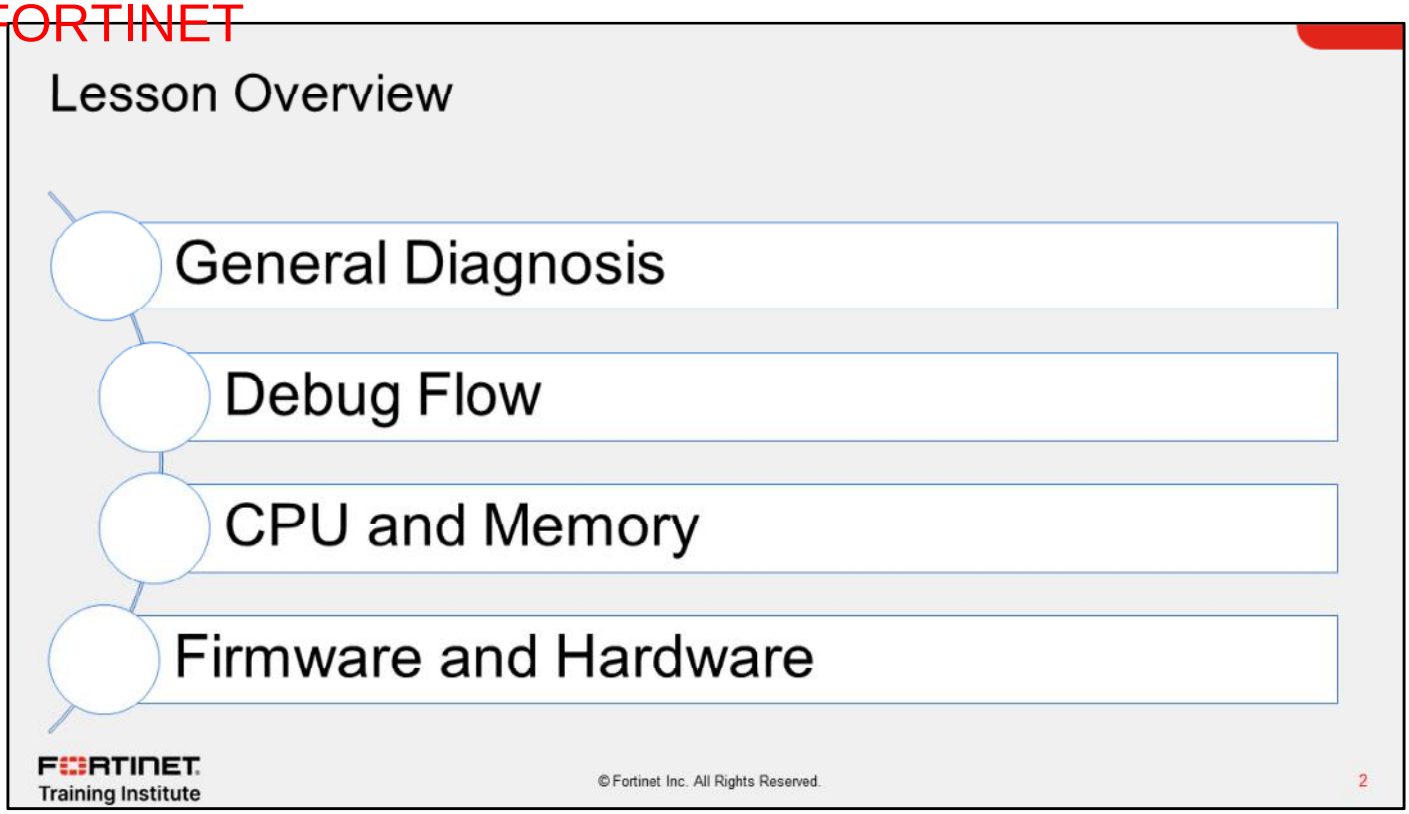
Now, you will review the objectives that you covered in this lesson.



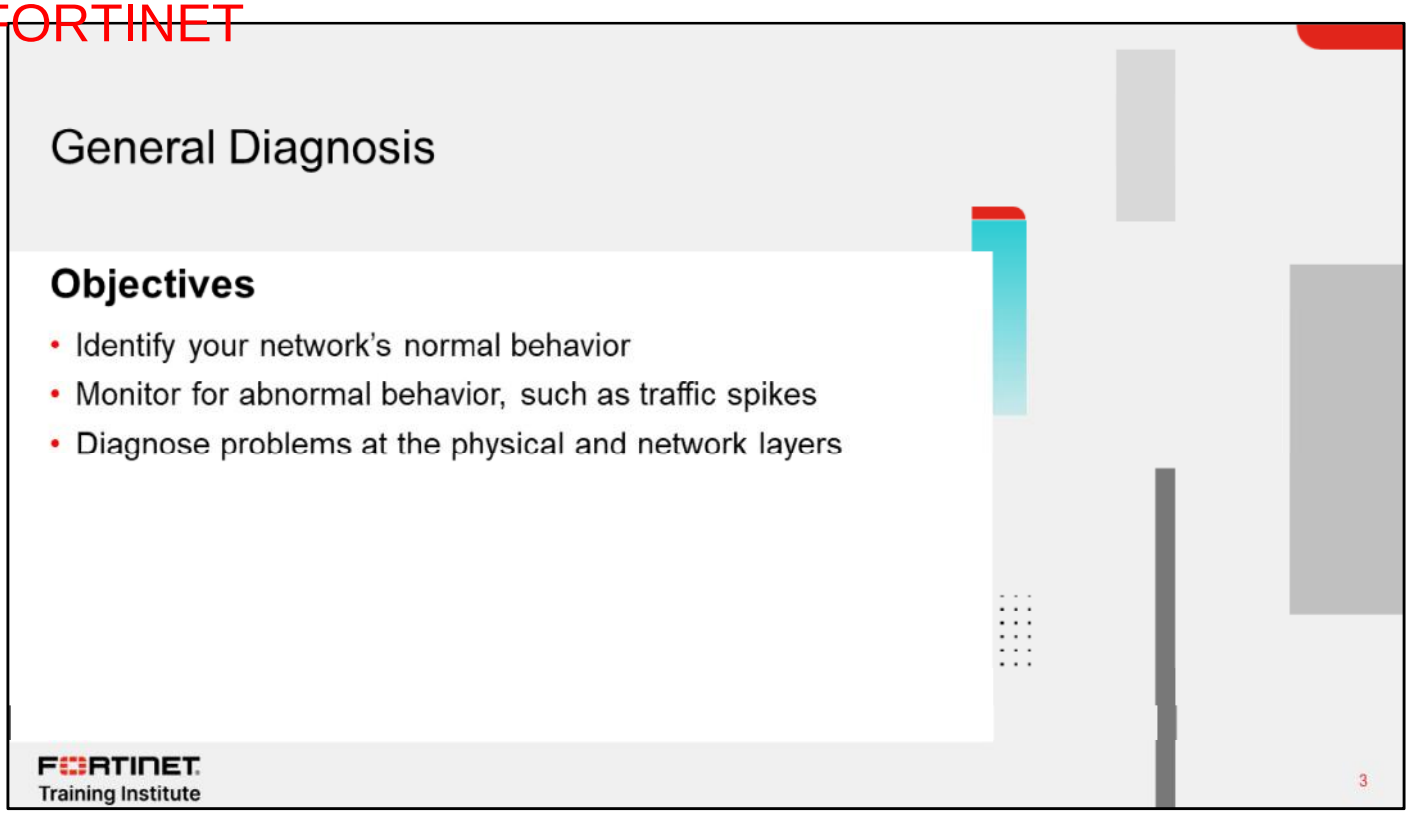
This slide shows the objectives that you covered in this lesson.

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

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

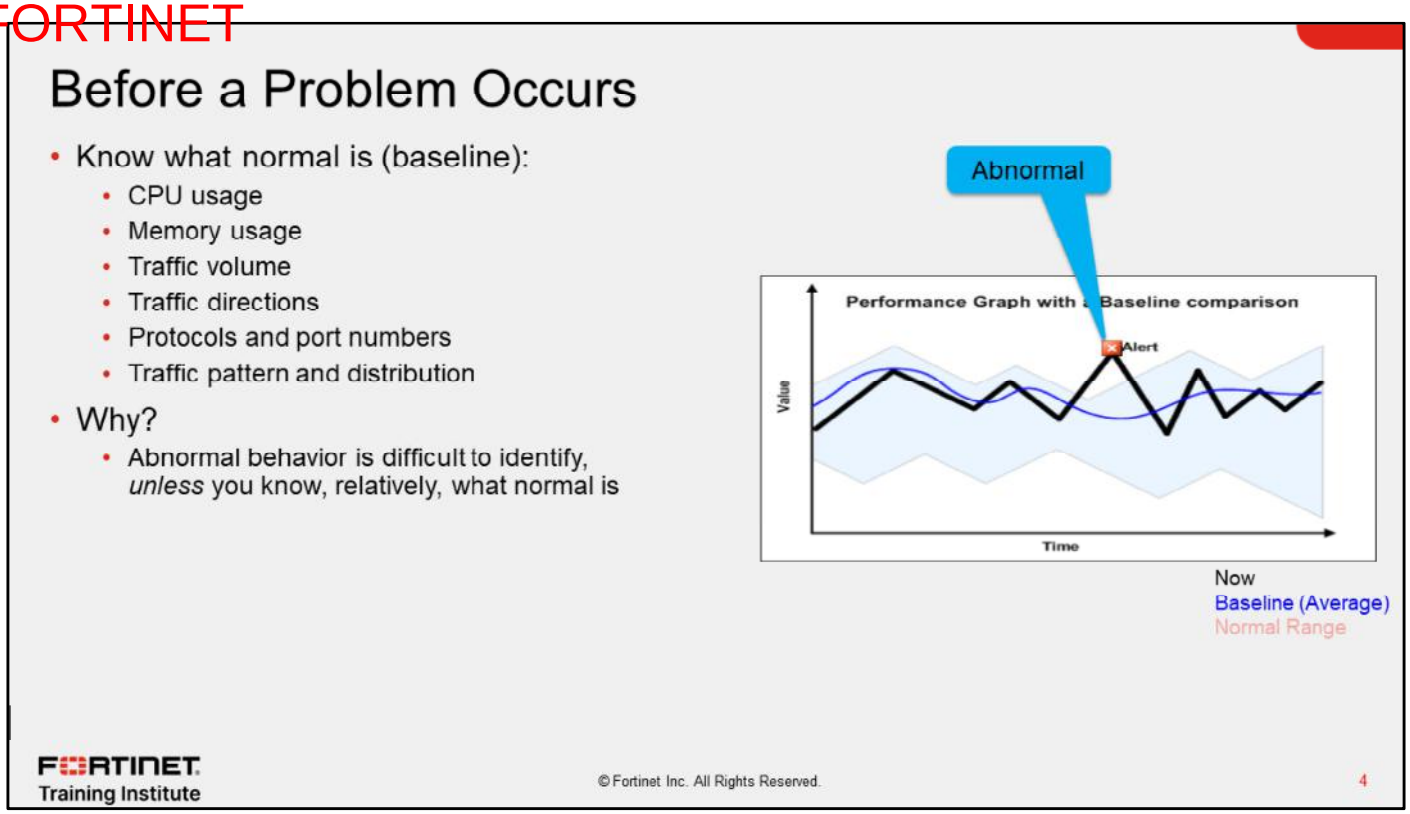


In this lesson, you will learn about the topics shown on this slide.



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.



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

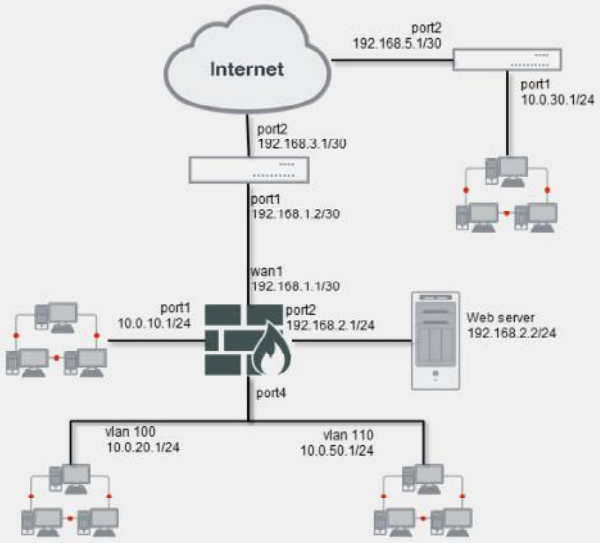
In order to define any problem, first you must know what your network's *normal* behavior is.

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

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

Network Diagrams

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



FORTINET Training Institute

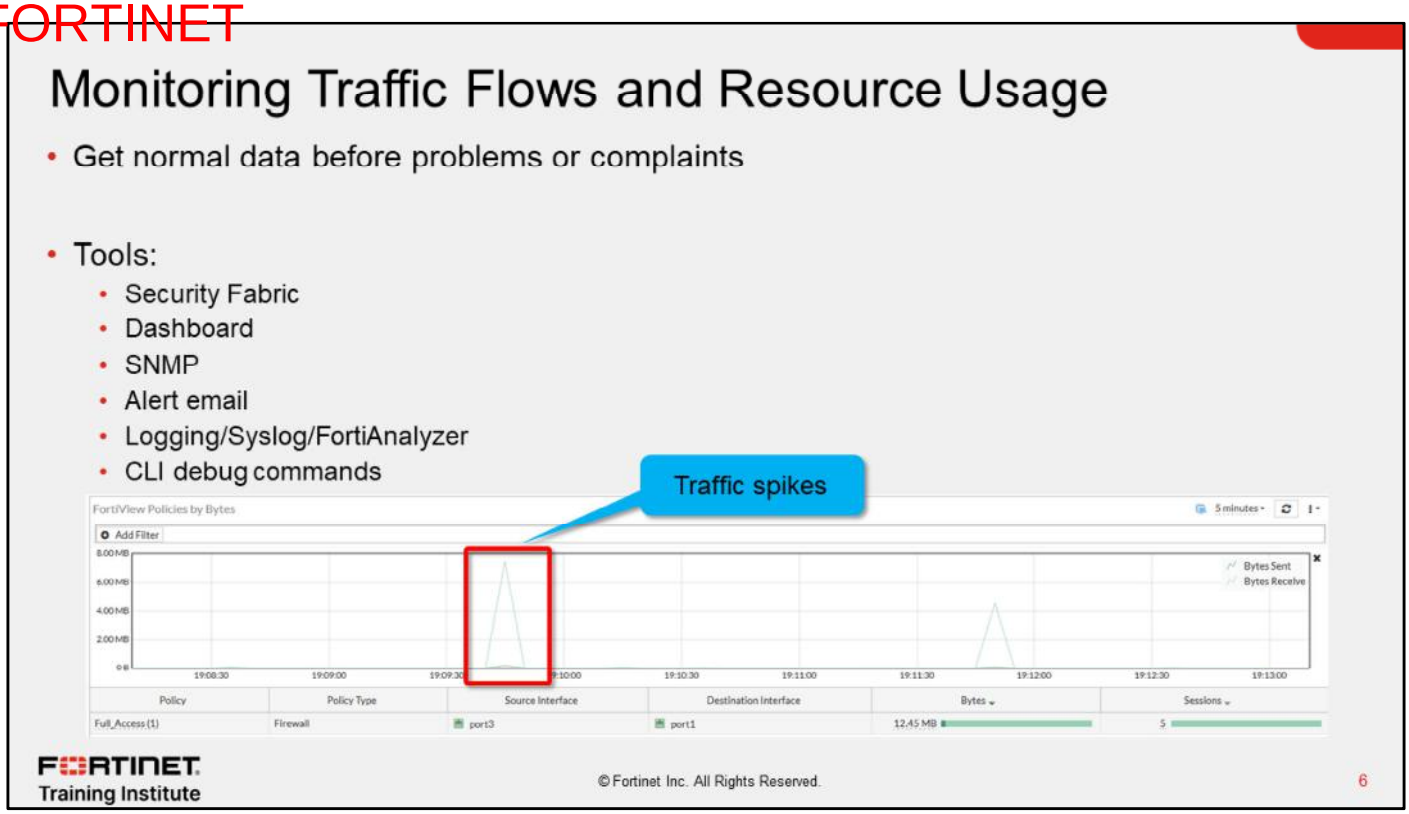
5

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

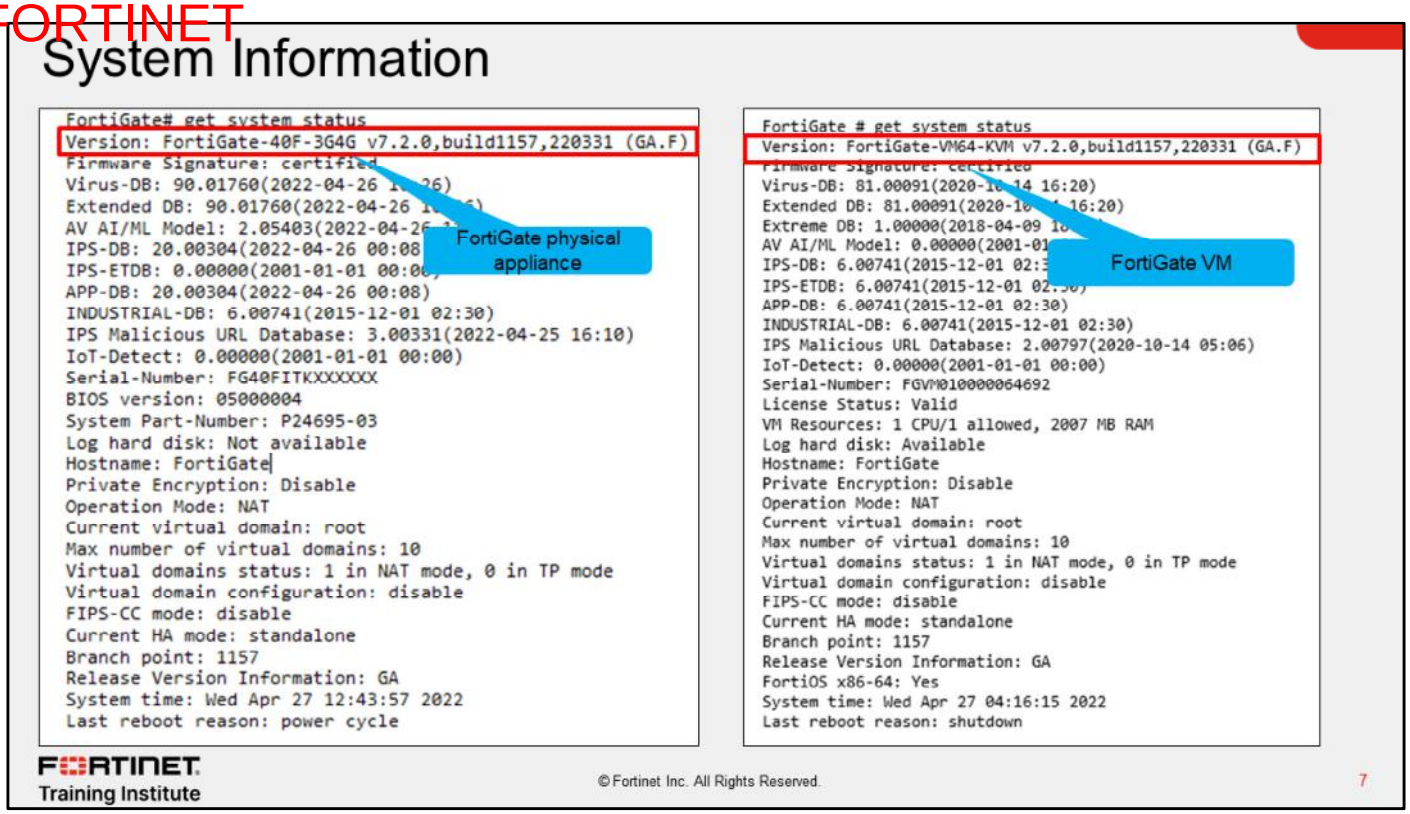
A physical diagram shows how cables, ports, and devices are connected between buildings and cabinets.
A logical diagram shows relationships (usually at OSI Layer 3) between virtual LANs, IP subnets, and routers. It can also show application protocols such as HTTP or DHCP.



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

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

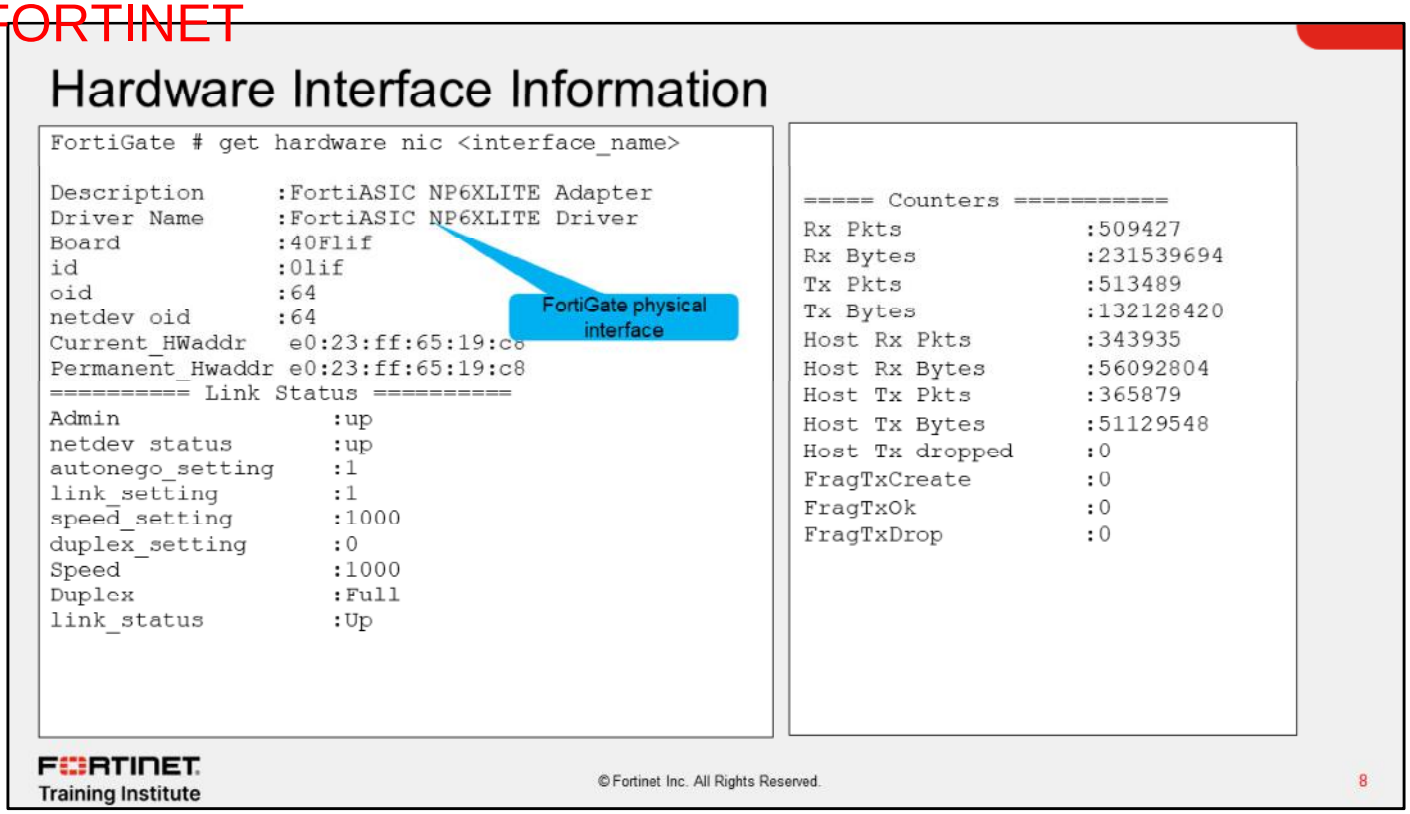
Get data on both the typical maximum and minimum for the time and date. That is, on a workday or holiday, how many bits per second should ingress or egress each interface in your network diagrams?



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

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

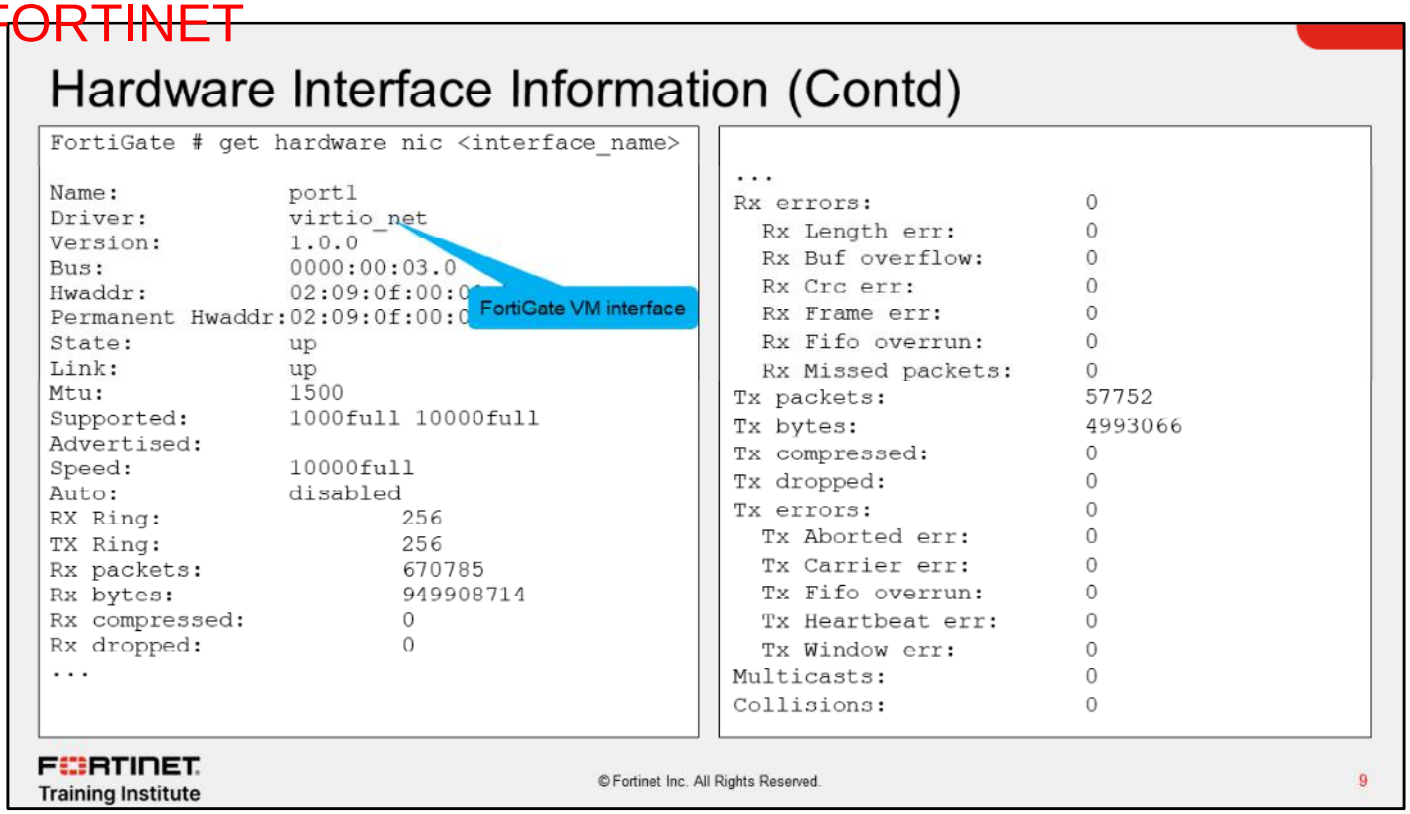
- Model
- Serial number
- Firmware version
- Host name
- FortiGuard license status
- System time
- Version of the FortiGuard antivirus, IPS, and IP reputation databases, and others



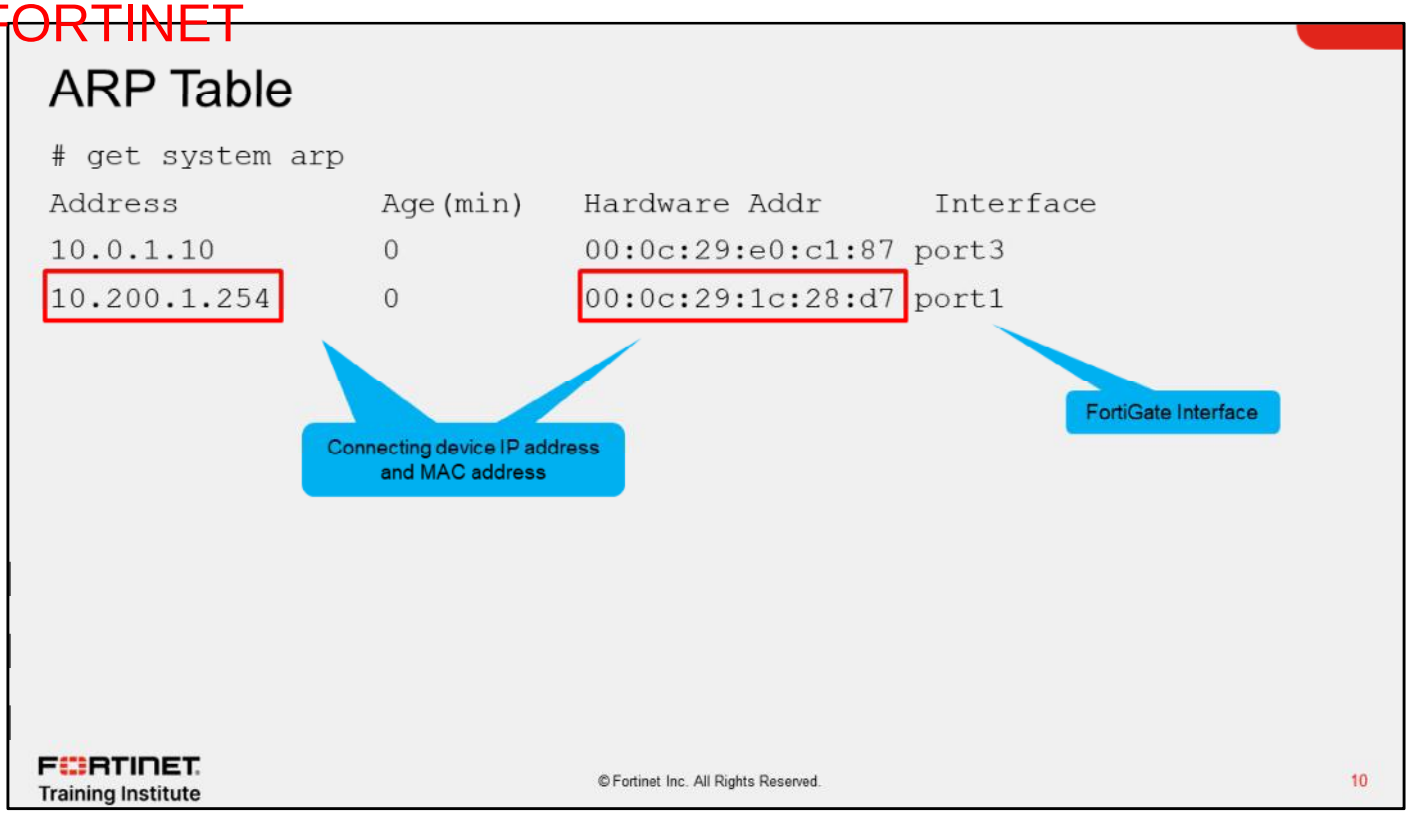
At the physical layer, troubleshooting analyzes which ports are plugged in, media capacity, and negotiated speed and duplex mode.

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.



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



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.

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 Training Institute

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.

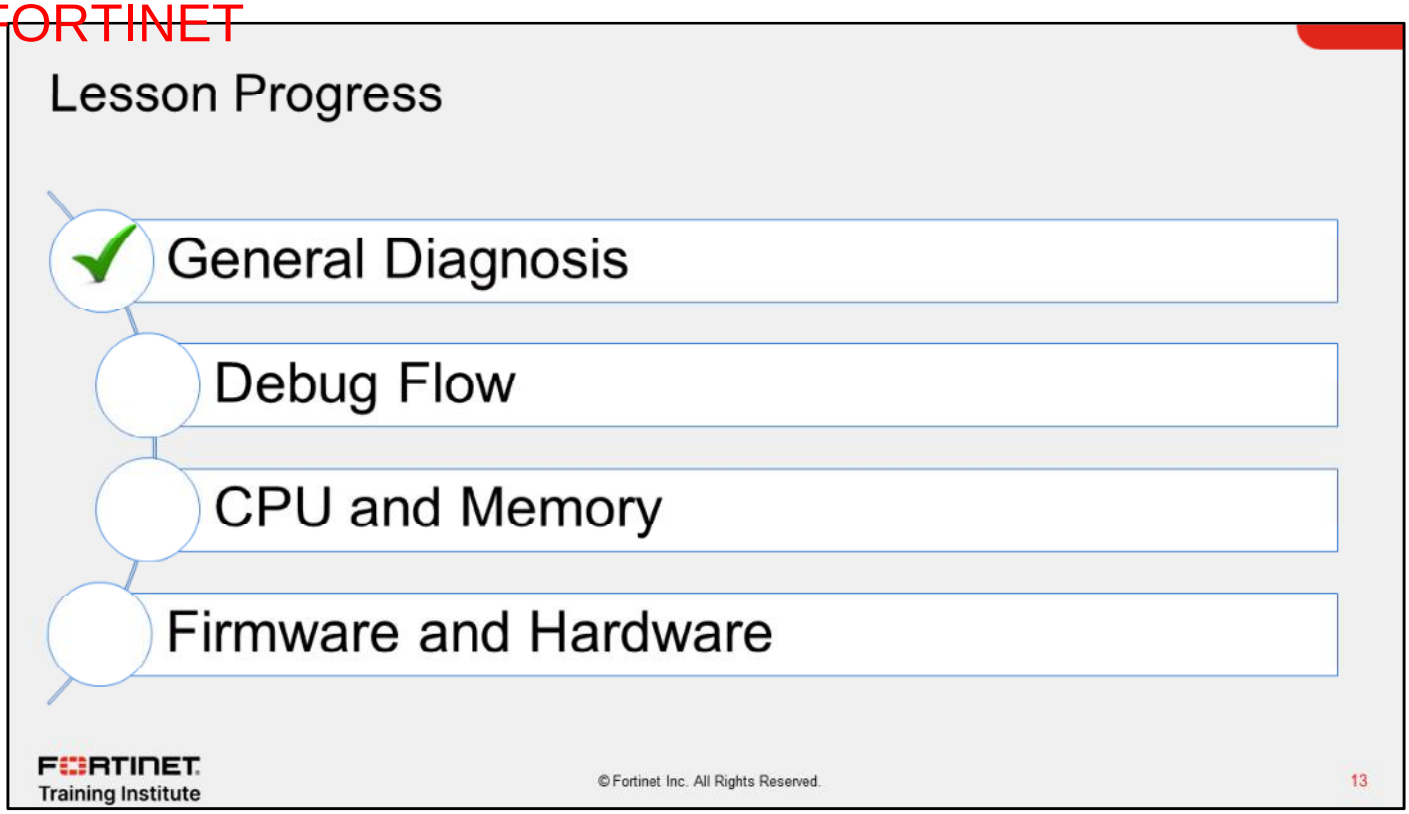
Knowledge Check

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`

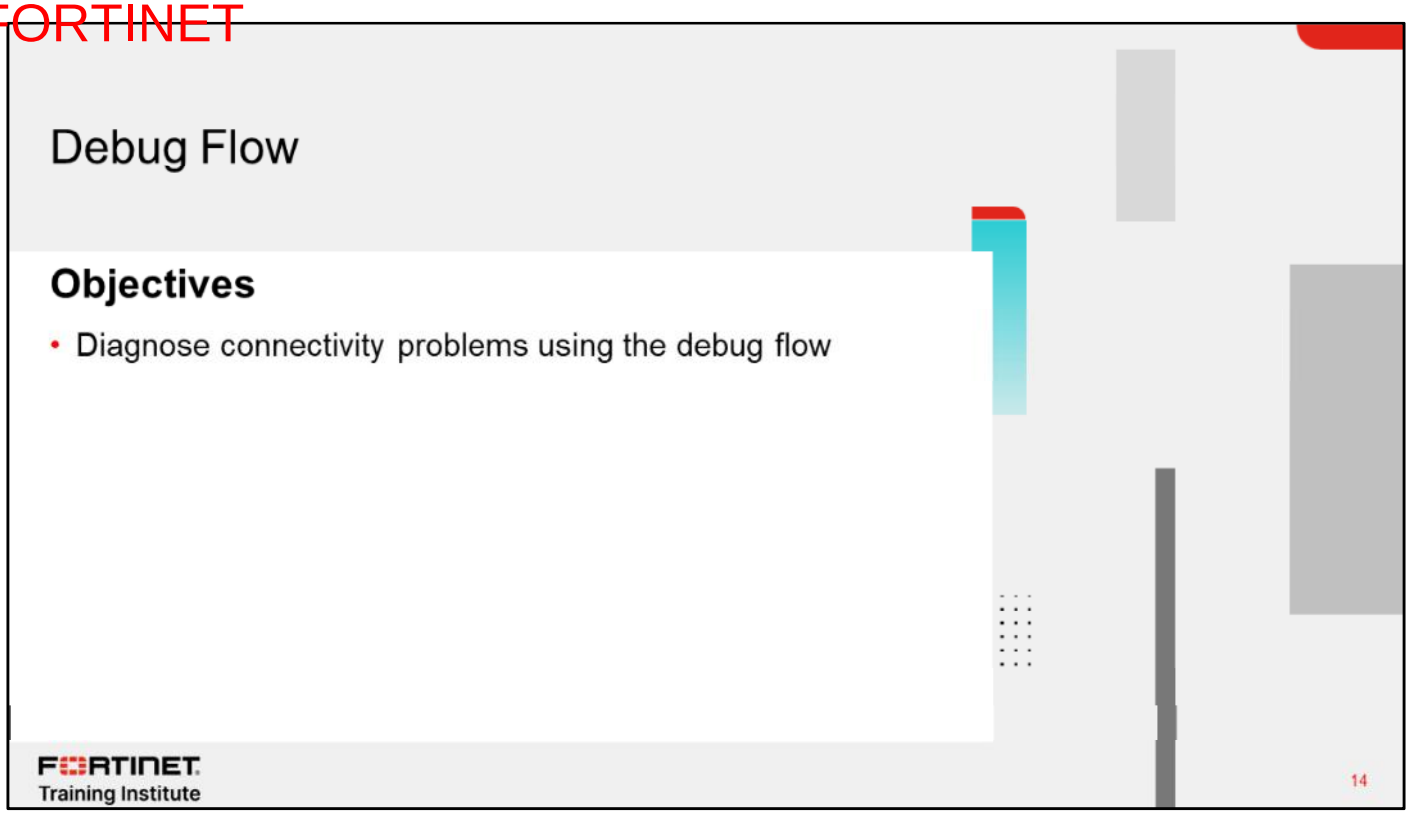
FORTINET Training Institute

12



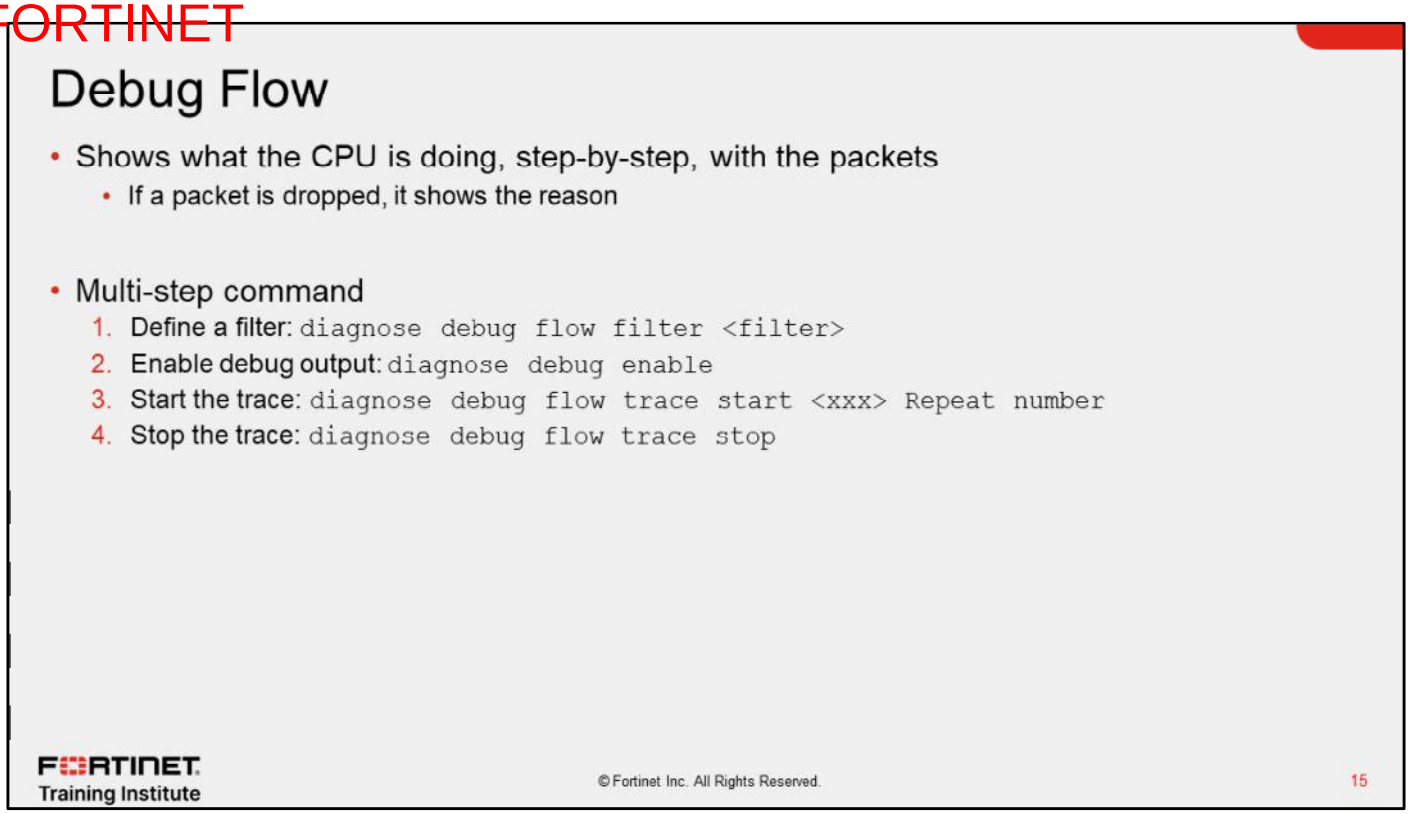
Good job! You now understand general diagnostics.

Now, you will learn about debug flow.



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

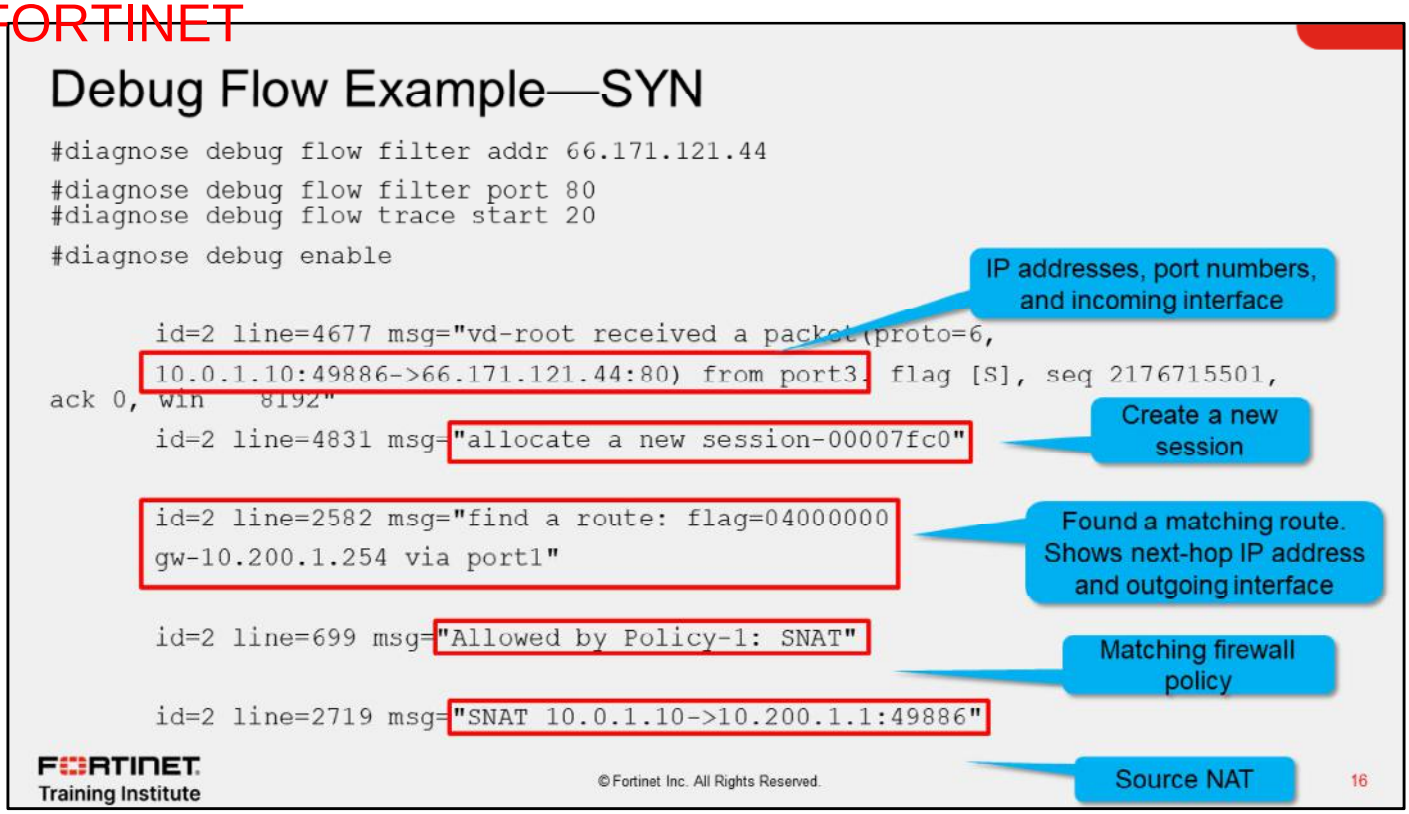
By demonstrating competence in the debug flow, you will be able to diagnose connectivity problems.



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

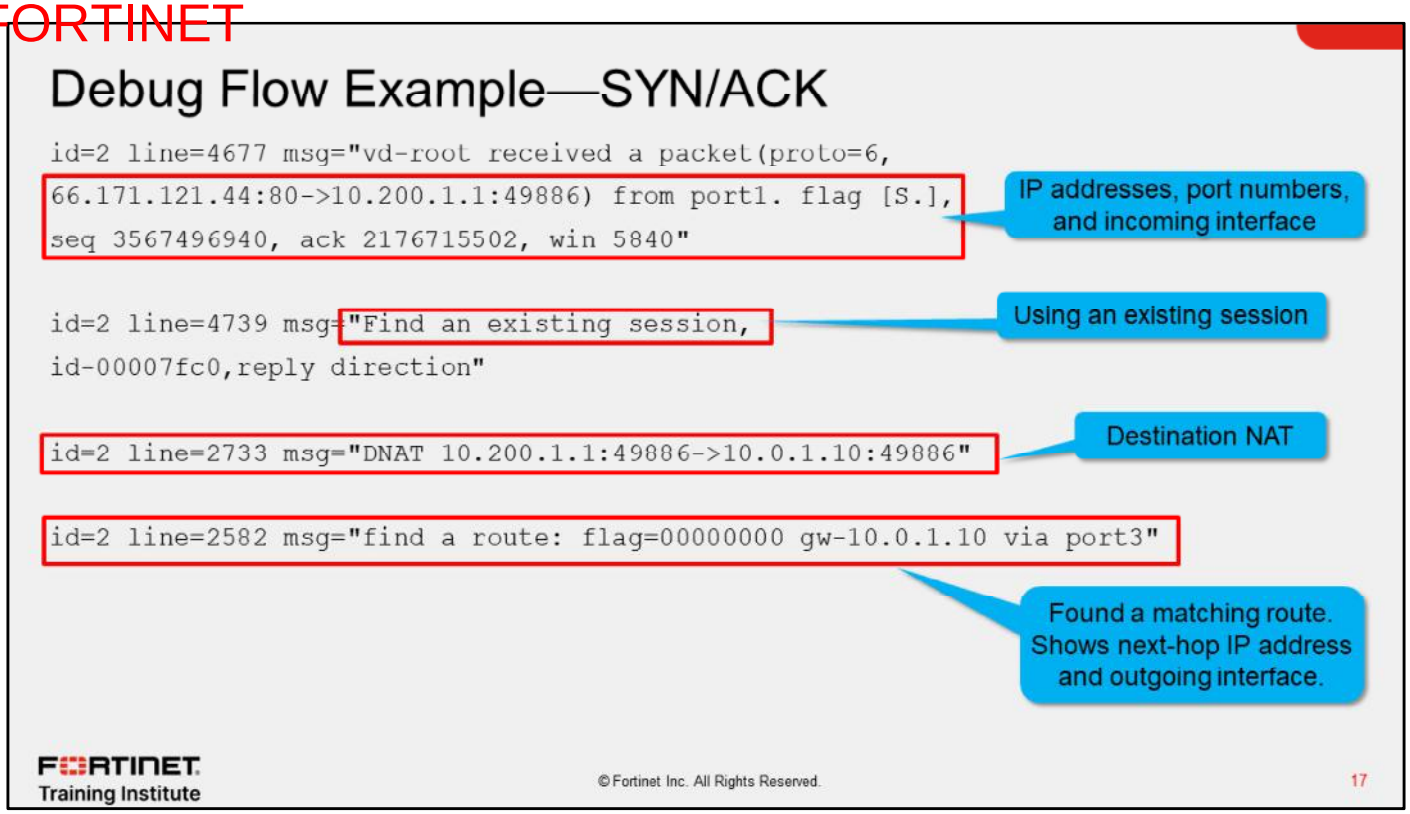
The debug flow shows, step-by-step, how the CPU is handling each packet.

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



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

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

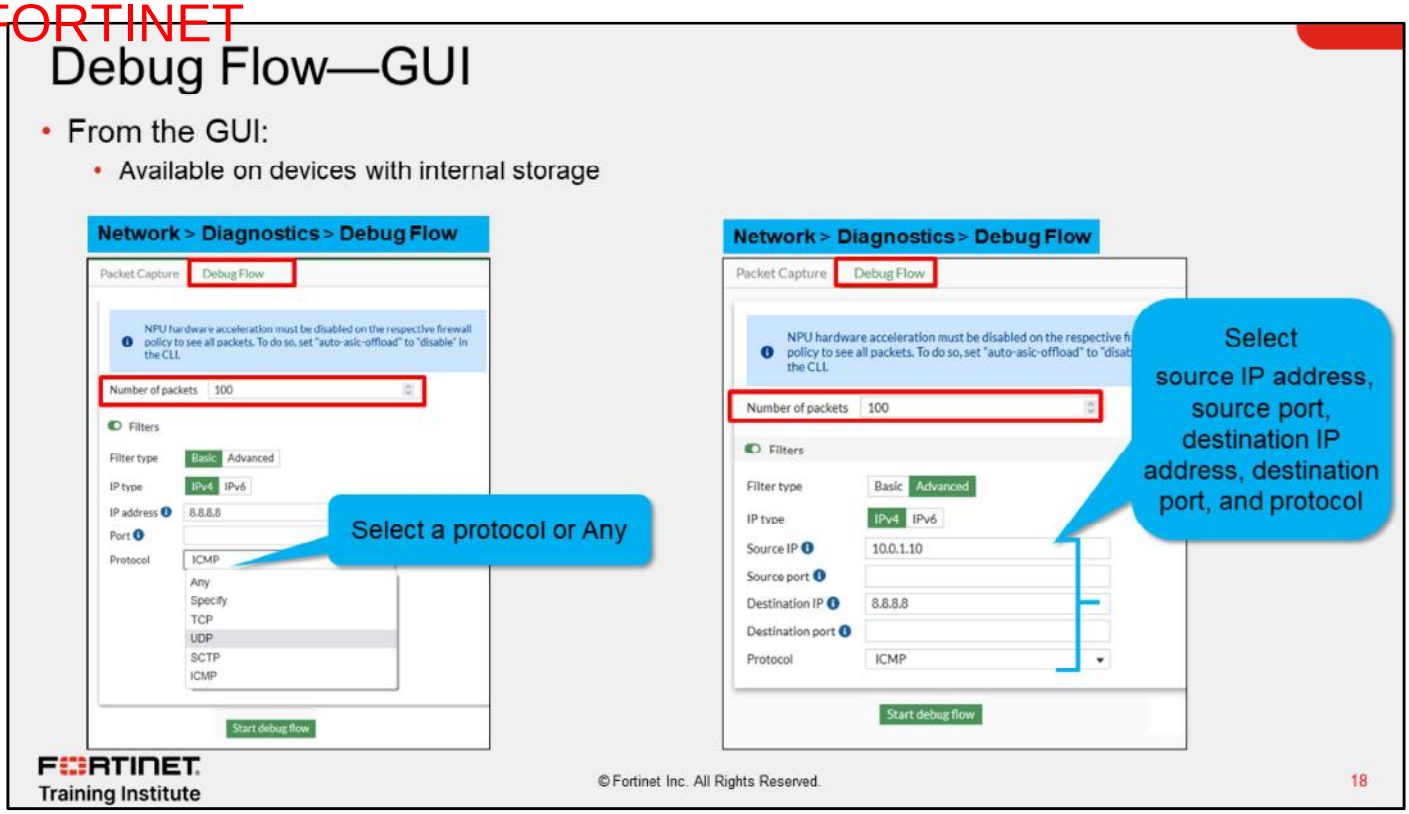


This slide shows the output for the SYN/ACK packet, which is from the same `diagnose debug` command shown on the previous slide. It shows:

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

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

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

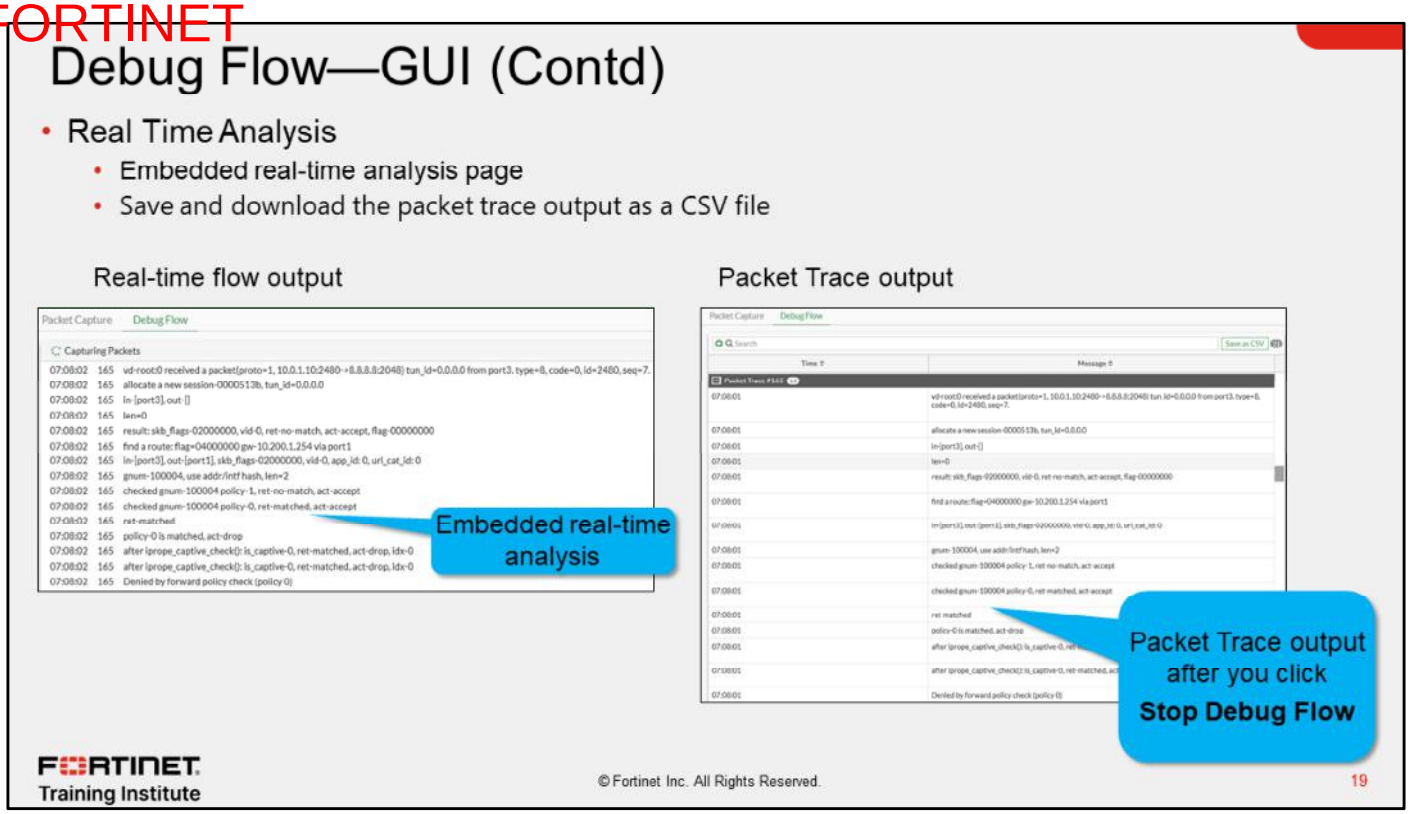


The Debug Flow tool allows you to view debug flow output on the GUI in real time until you stop the debug process.

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

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

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



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.

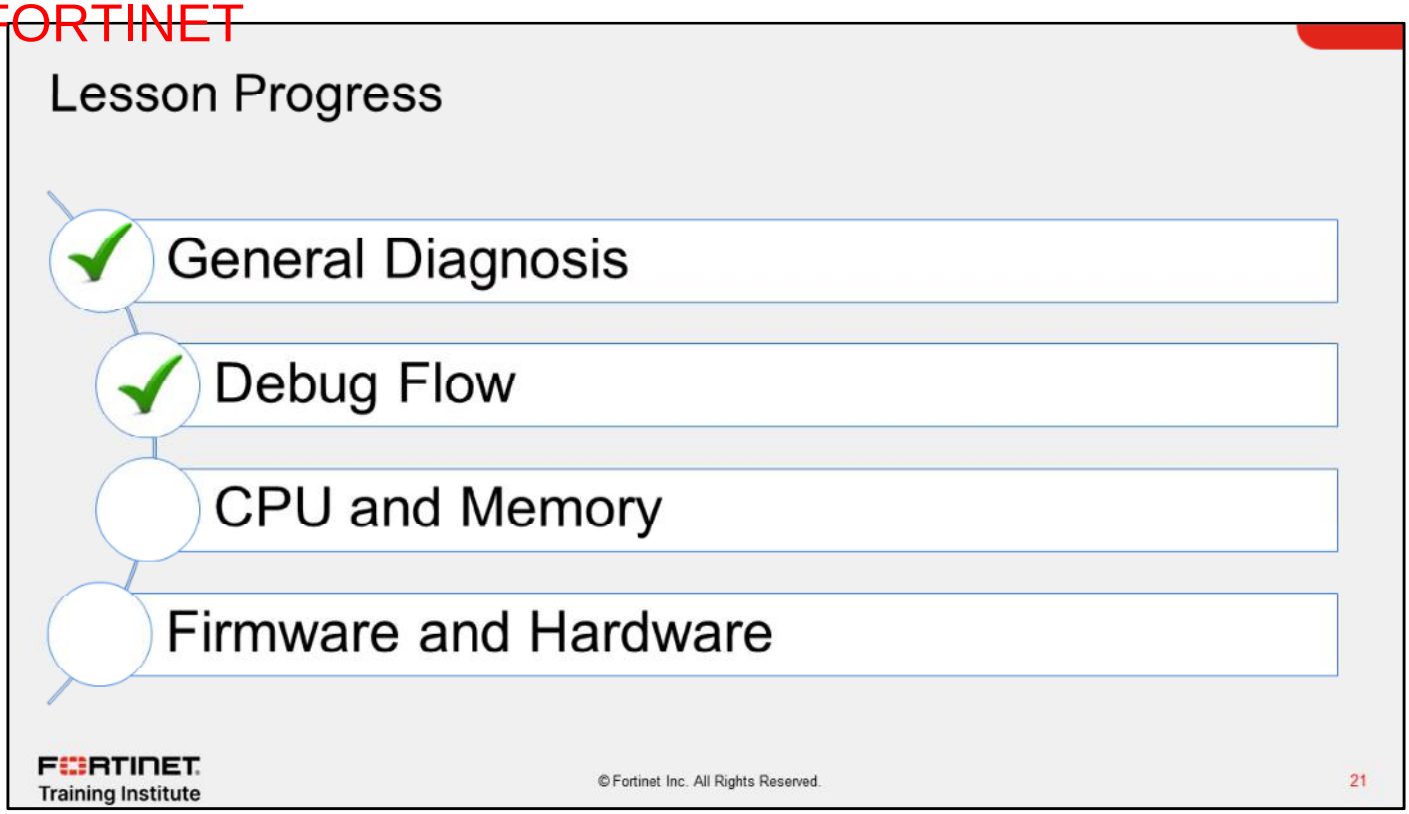
Knowledge Check

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

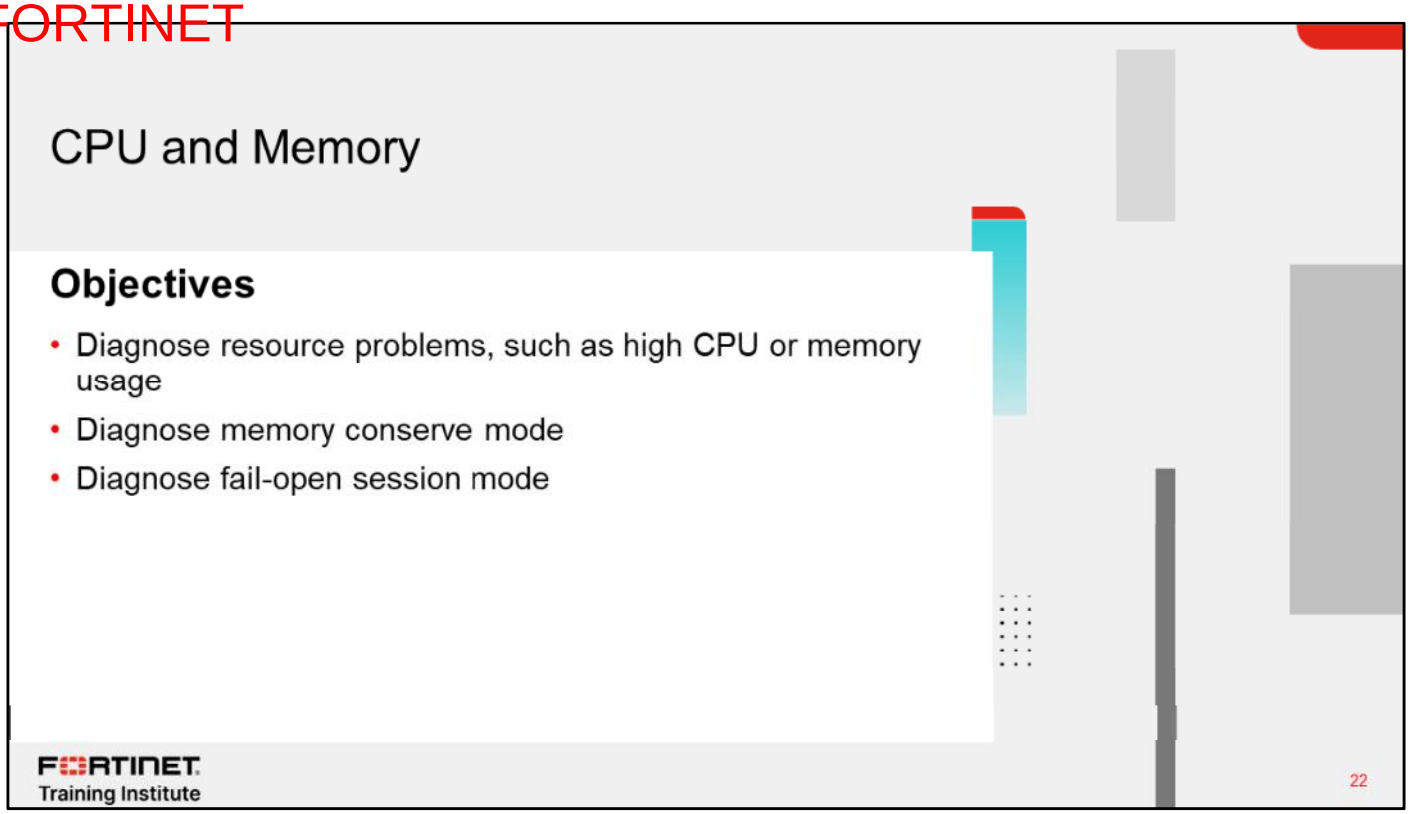
FORTINET Training Institute

20



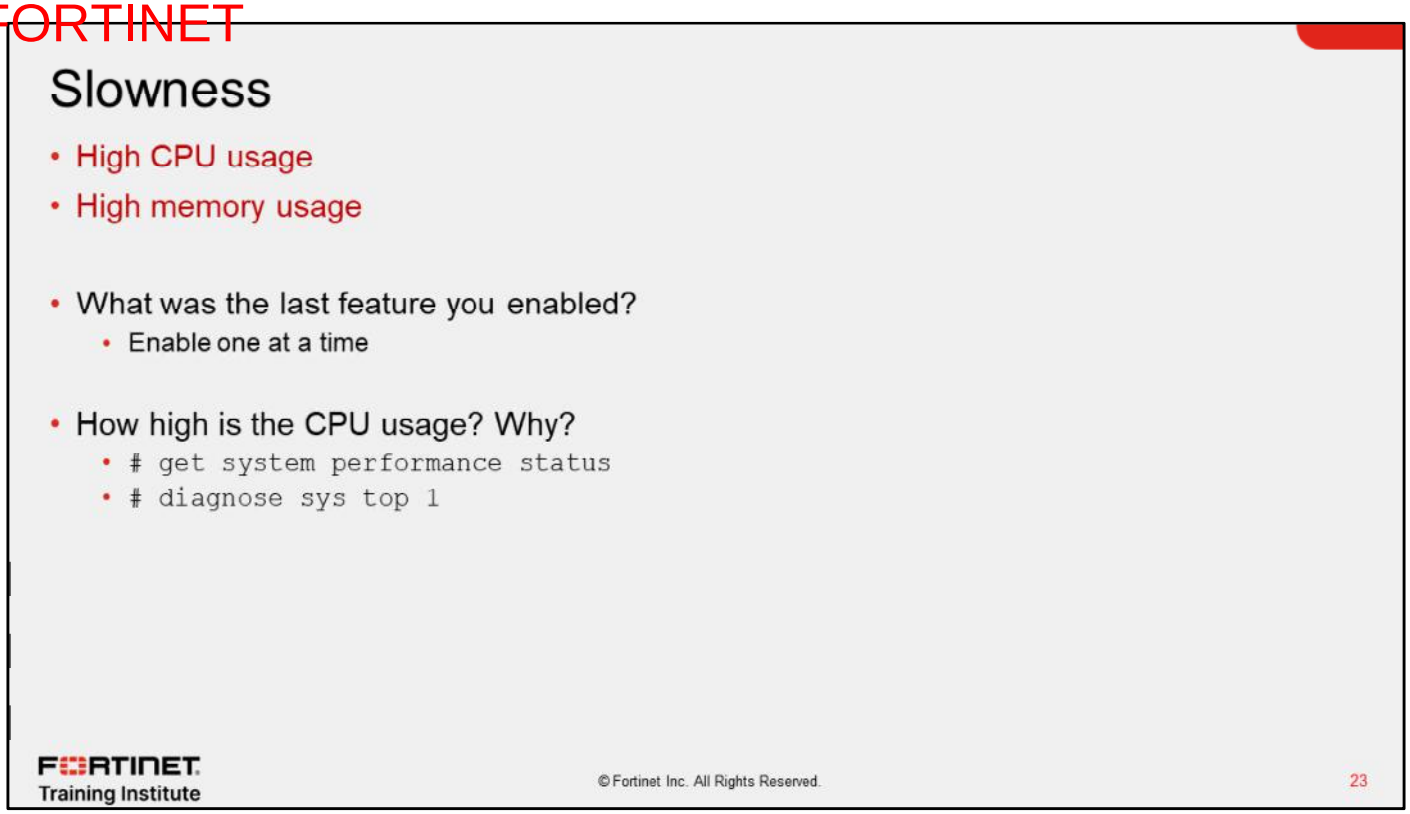
Good job! You now understand debug flow.

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



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

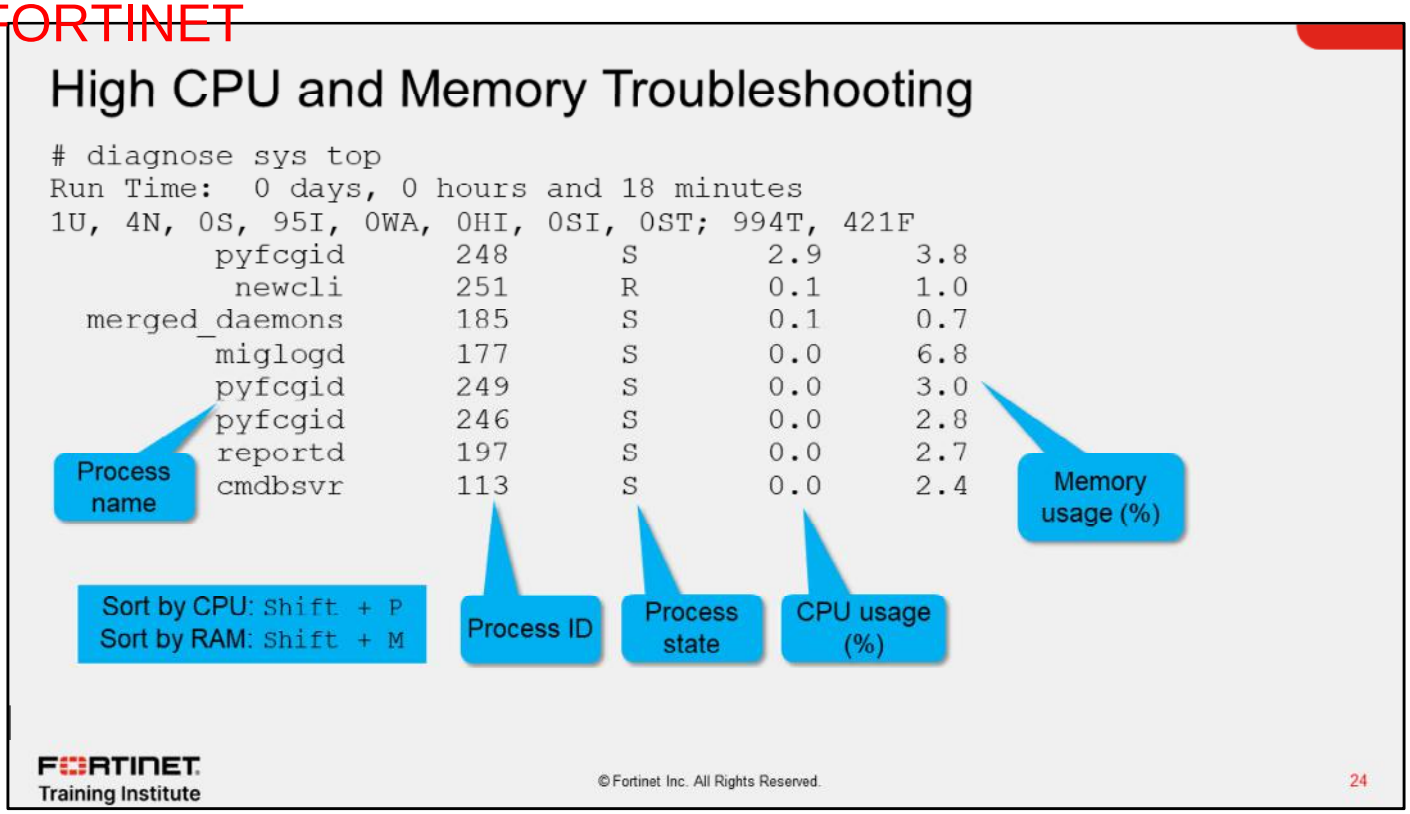
By demonstrating competence in CPU and memory, you will be able to diagnose the most common CPU and memory problems.



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.



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`.

Memory Conserve Mode

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

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

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

FORTINET Training Institute

25

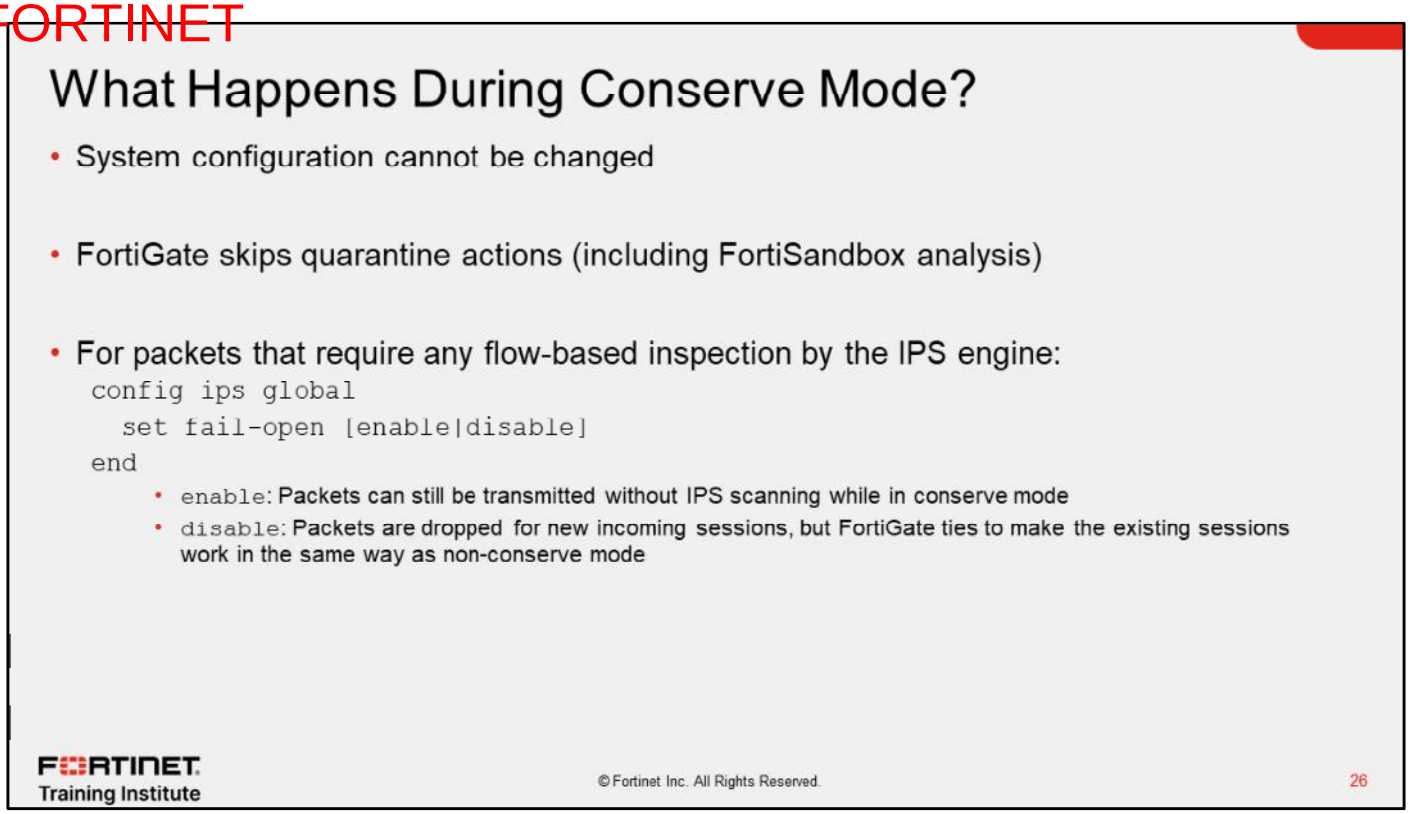
If memory usage becomes too high, FortiGate may enter into memory conserve mode. While FortiGate is in memory conserve mode, it must take action to prevent memory usage from increasing, which could cause the system to become unstable and inaccessible.

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.



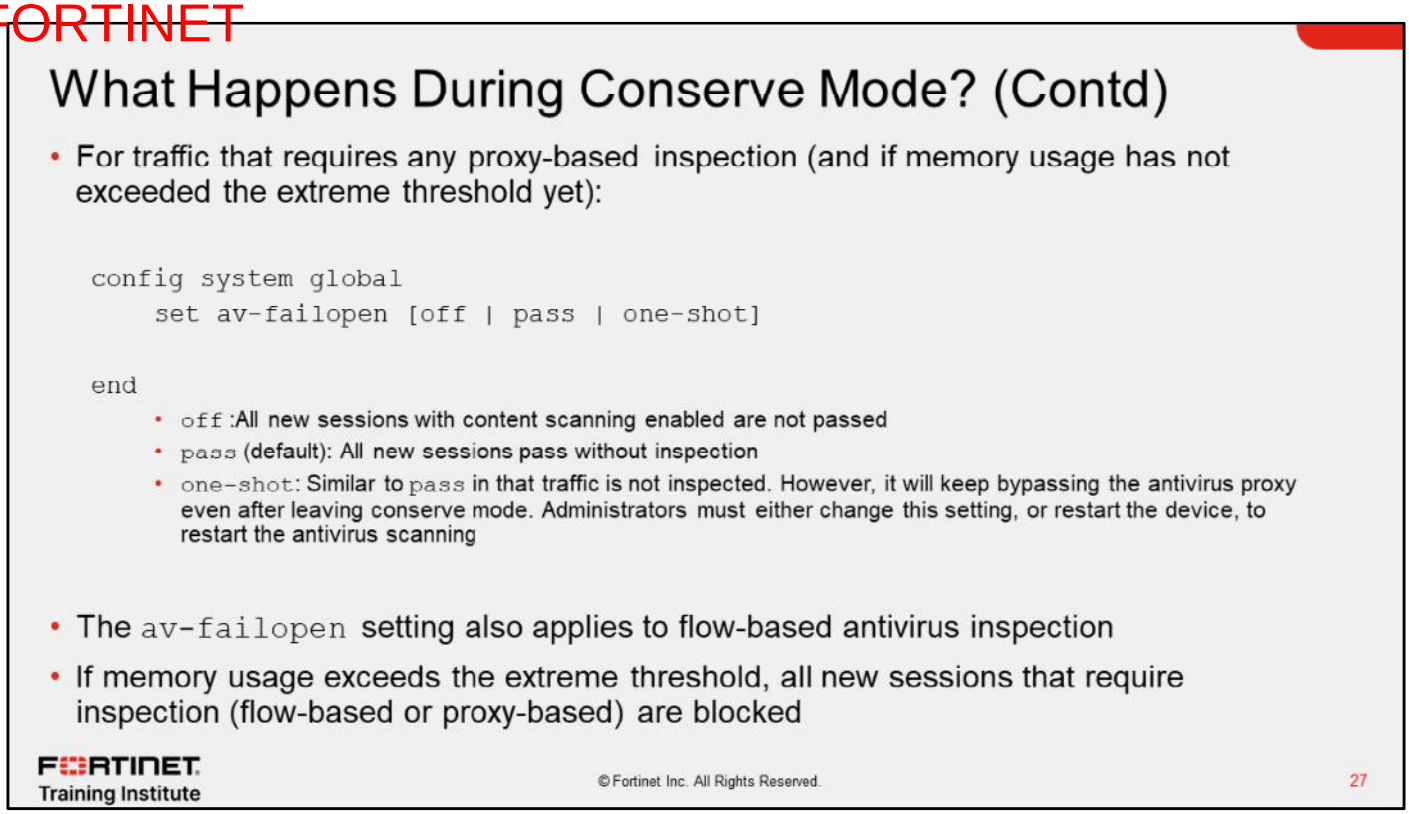
What actions does FortiGate take to preserve memory while in conserve mode?

- 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.



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

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

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

System Memory Conserve Mode Diagnostics

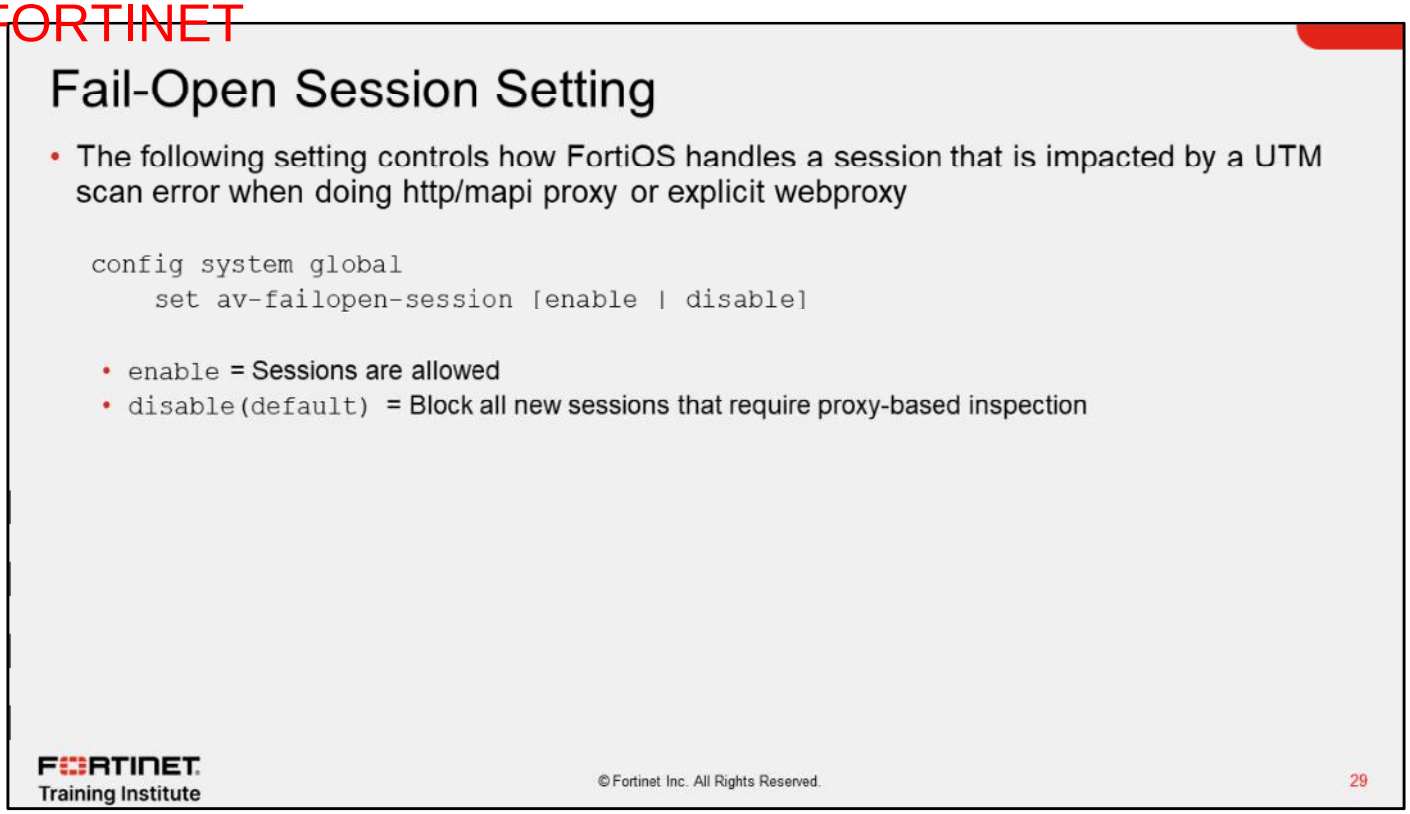
```
# diagnose hardware sysinfo conserve
memory conserve mode:                          on
total RAM:                                   3040 MB
memory used:                                 2706 MB   89% of total RAM
memory freeable:                              334 MB   11% of total RAM
memory used +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

Off = no conserve mode
on = conserve mode

FORTINET Training Institute

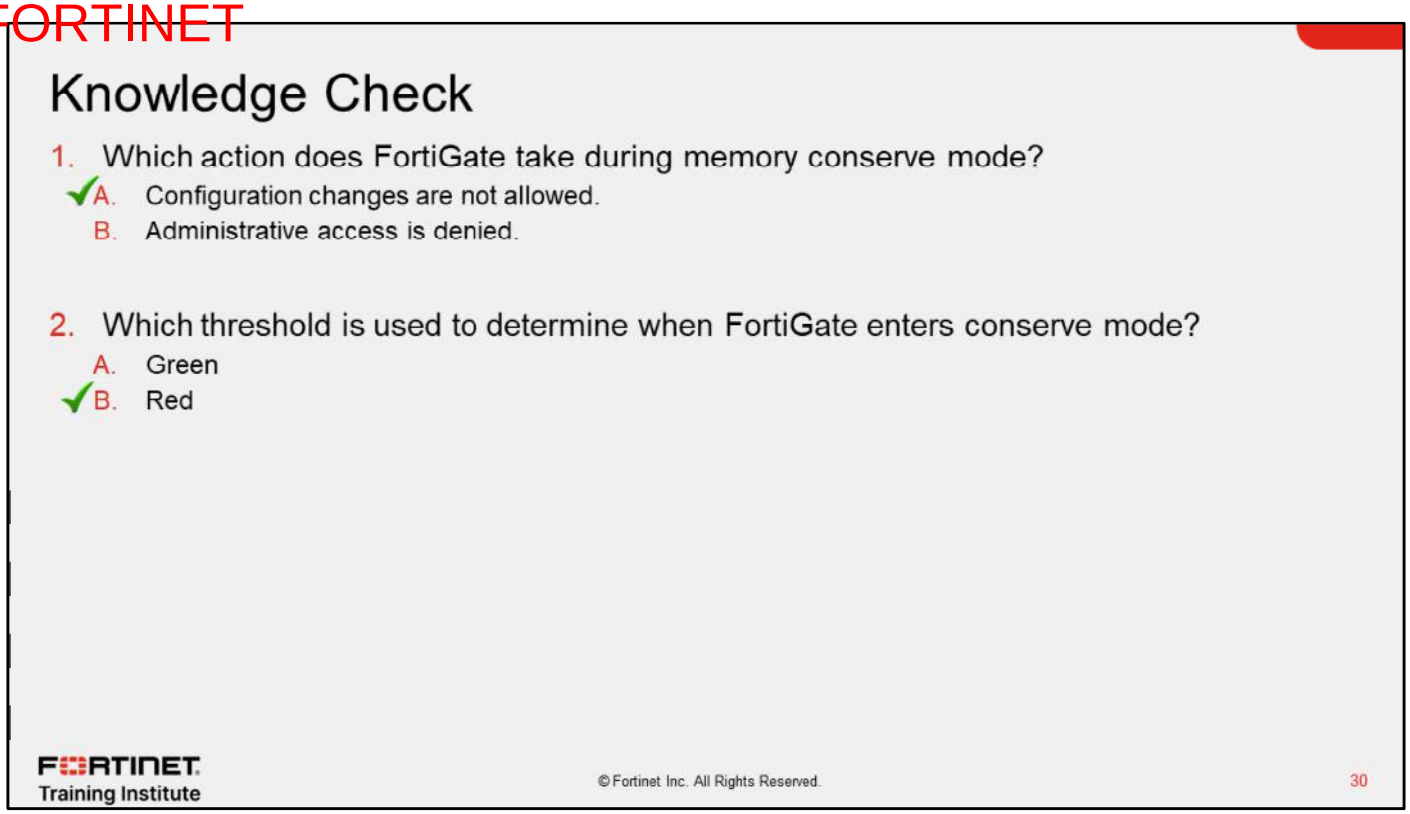
28

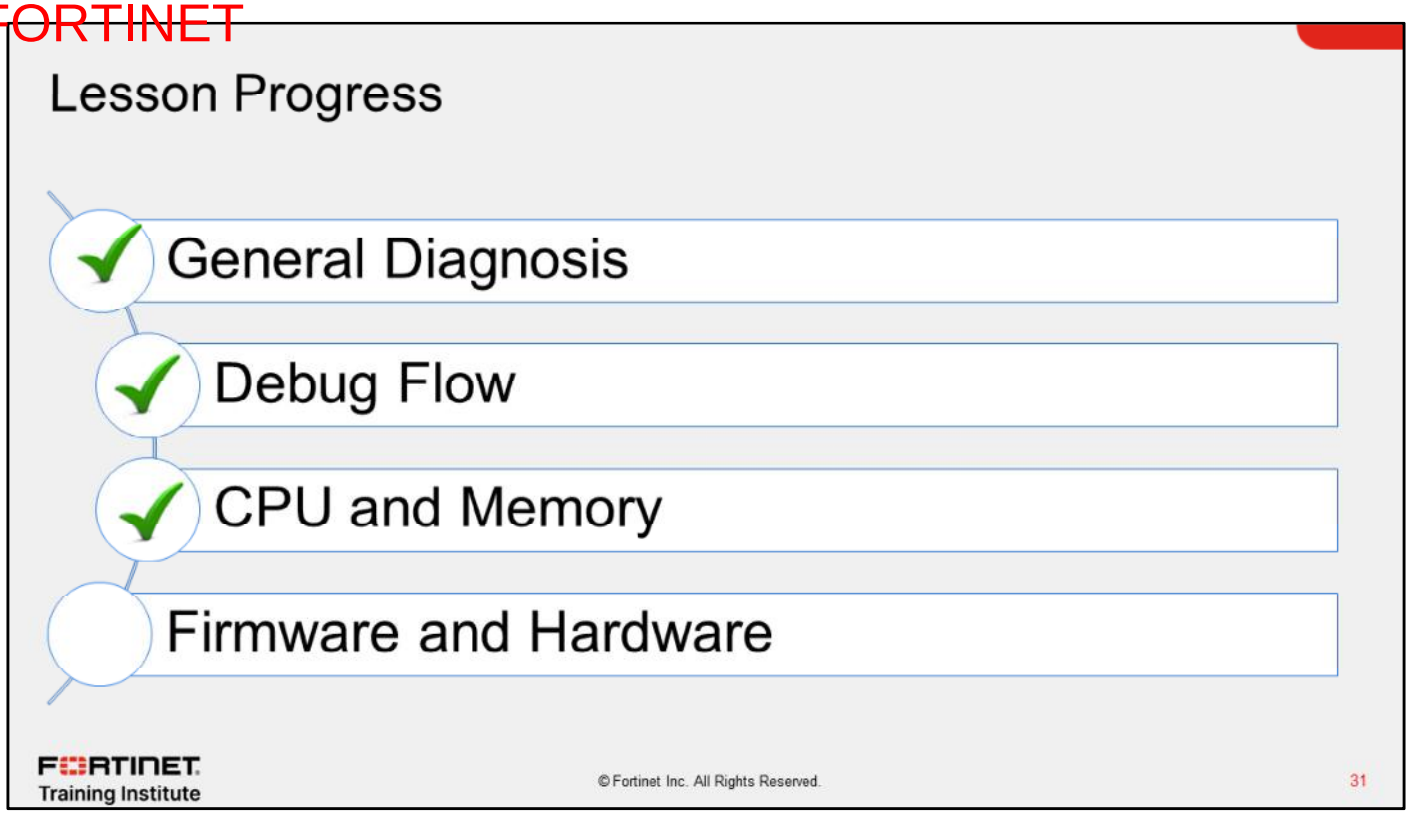
The `diagnose hardware sysinfo conserve` command is used to identify if a FortiGate device is currently in memory conserve mode.



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.

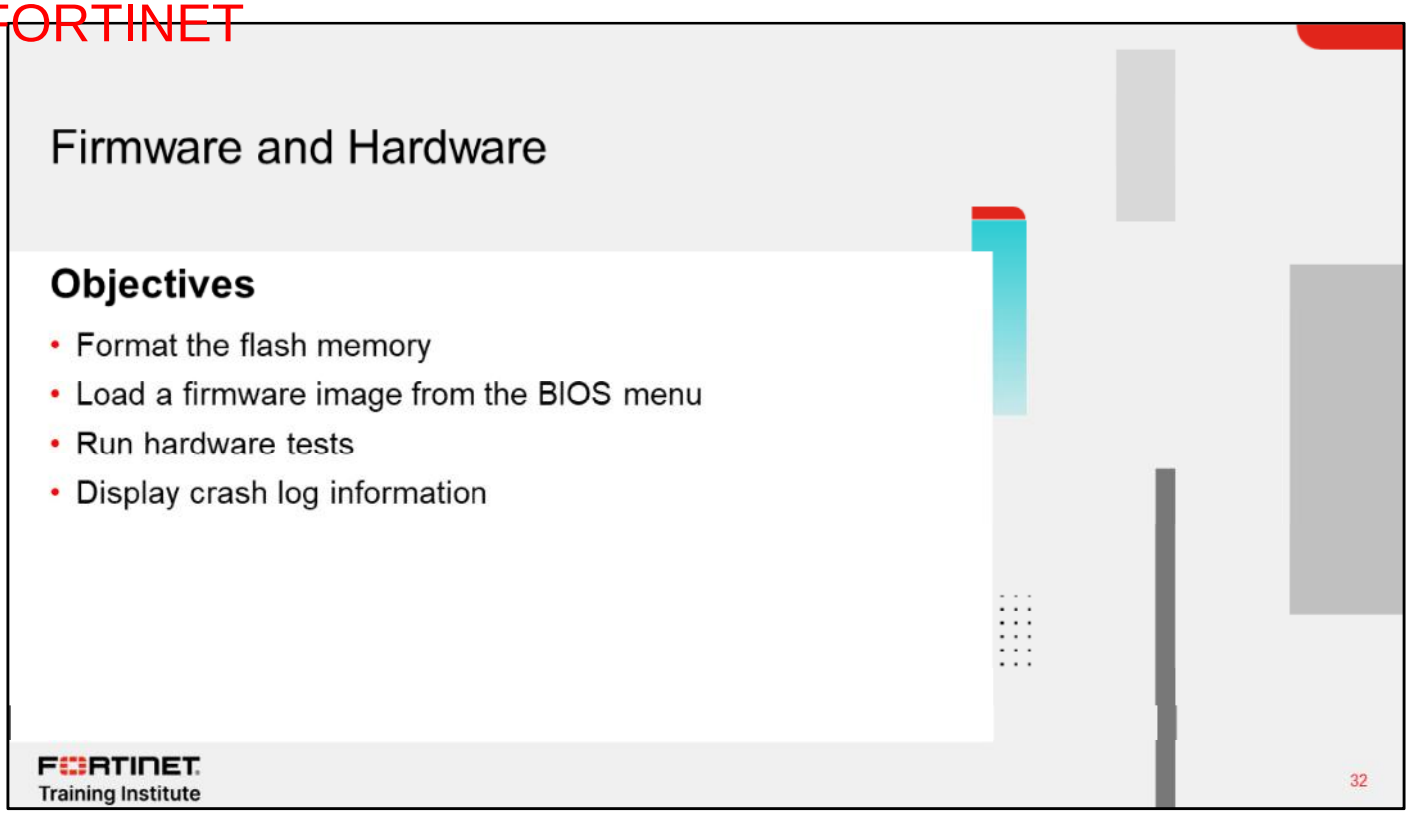
If `av-failopen-session` is enabled, FortiGate allows all the sessions. Otherwise, by default, it blocks new sessions that require proxy-based inspection until new sockets become available.





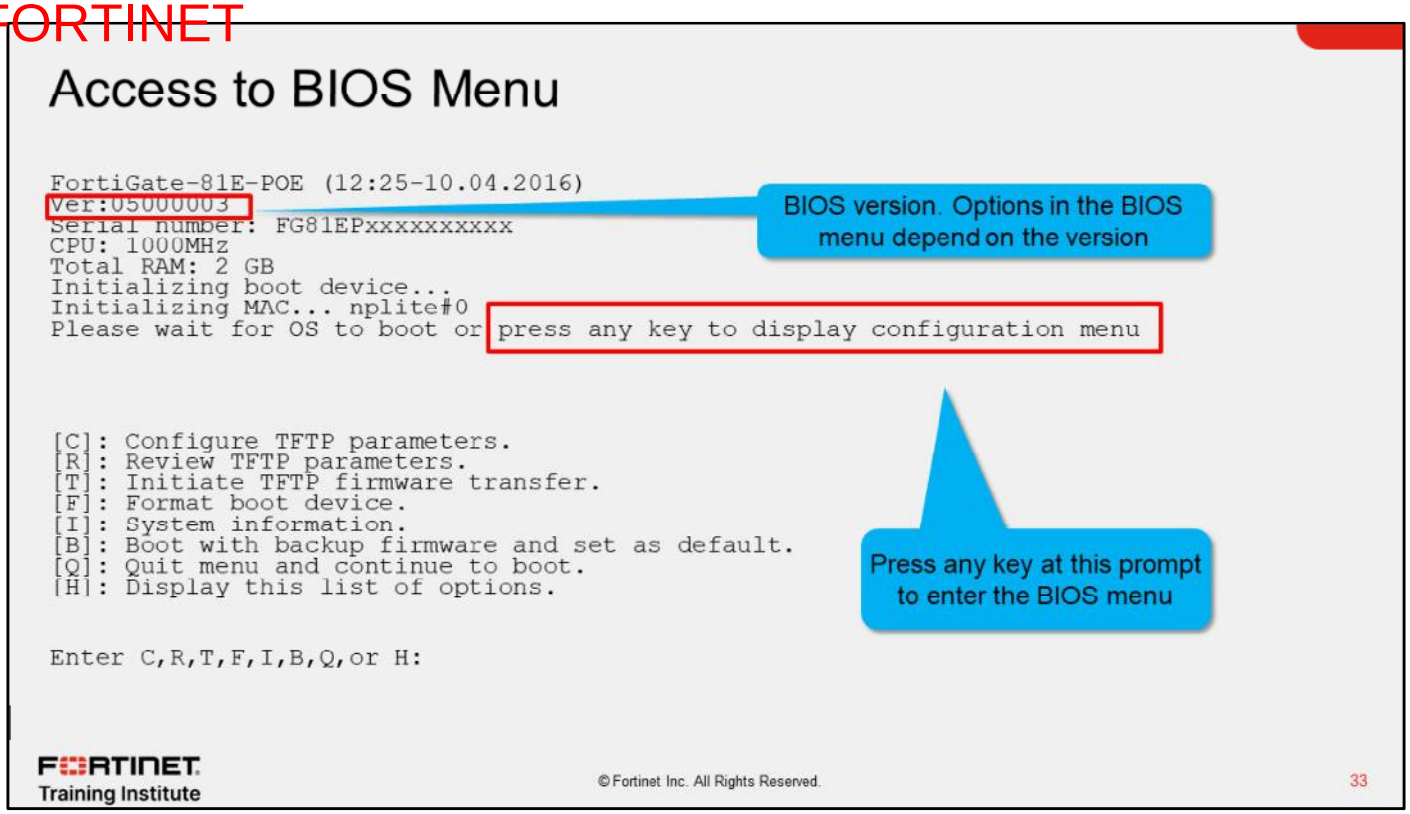
Good job! You now understand FortiGate CPU and memory diagnosis.

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



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

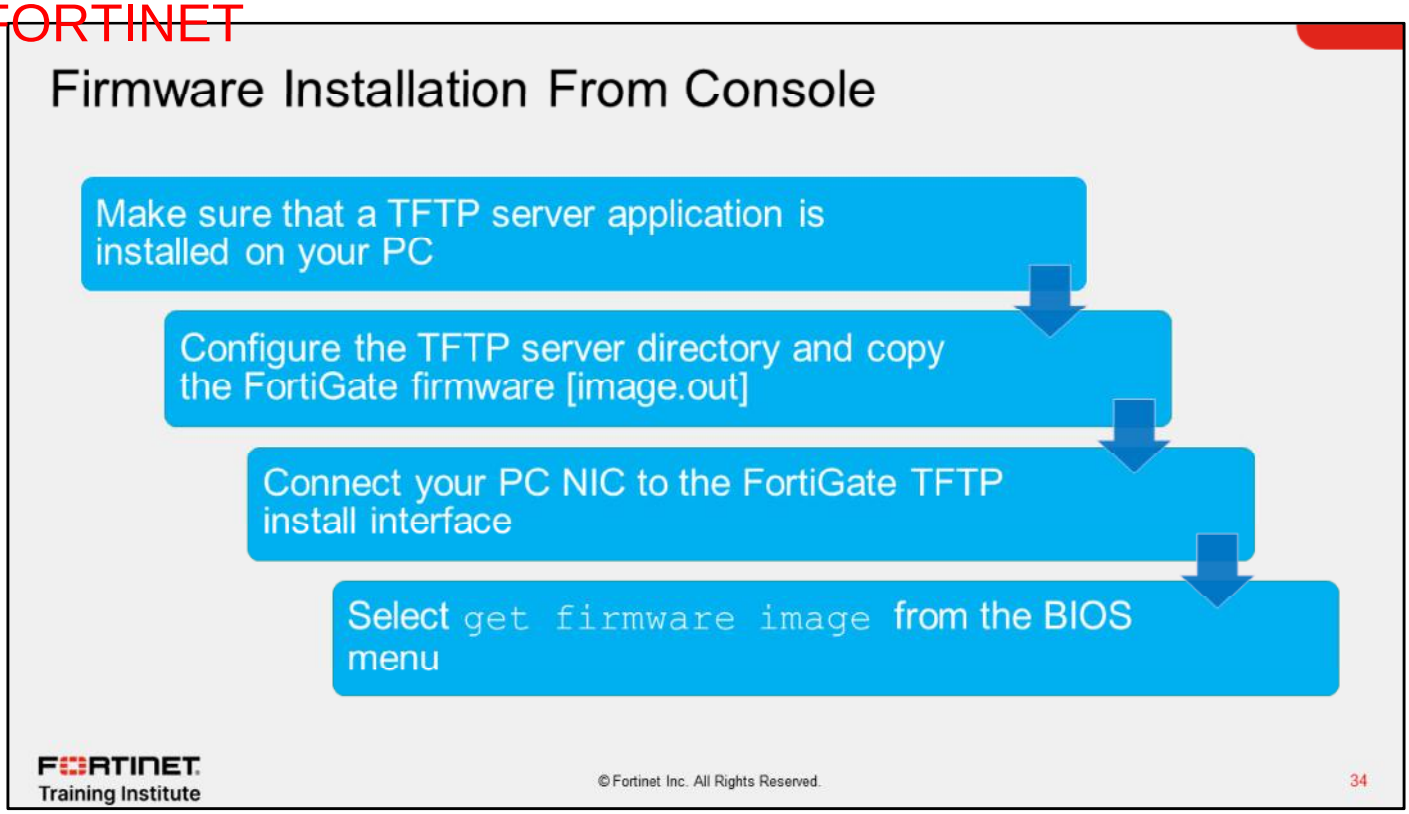
By demonstrating competence in firmware and hardware, you will be able to diagnose the most common firmware and hardware problems.



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
```

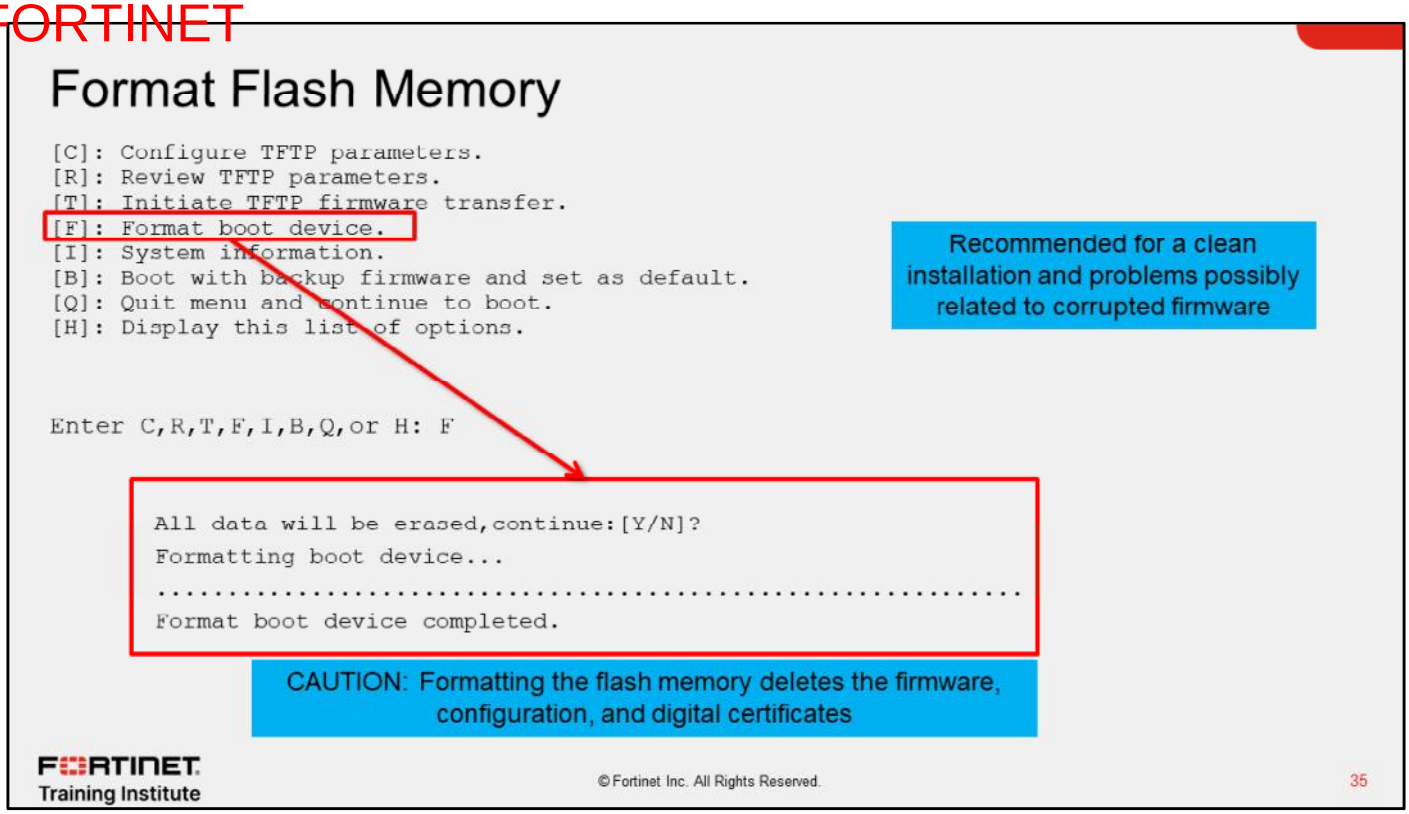
While this prompt is displayed, press any key to interrupt the booting process and display the BIOS menu. In the BIOS menu, you can see the options shown on this slide.



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

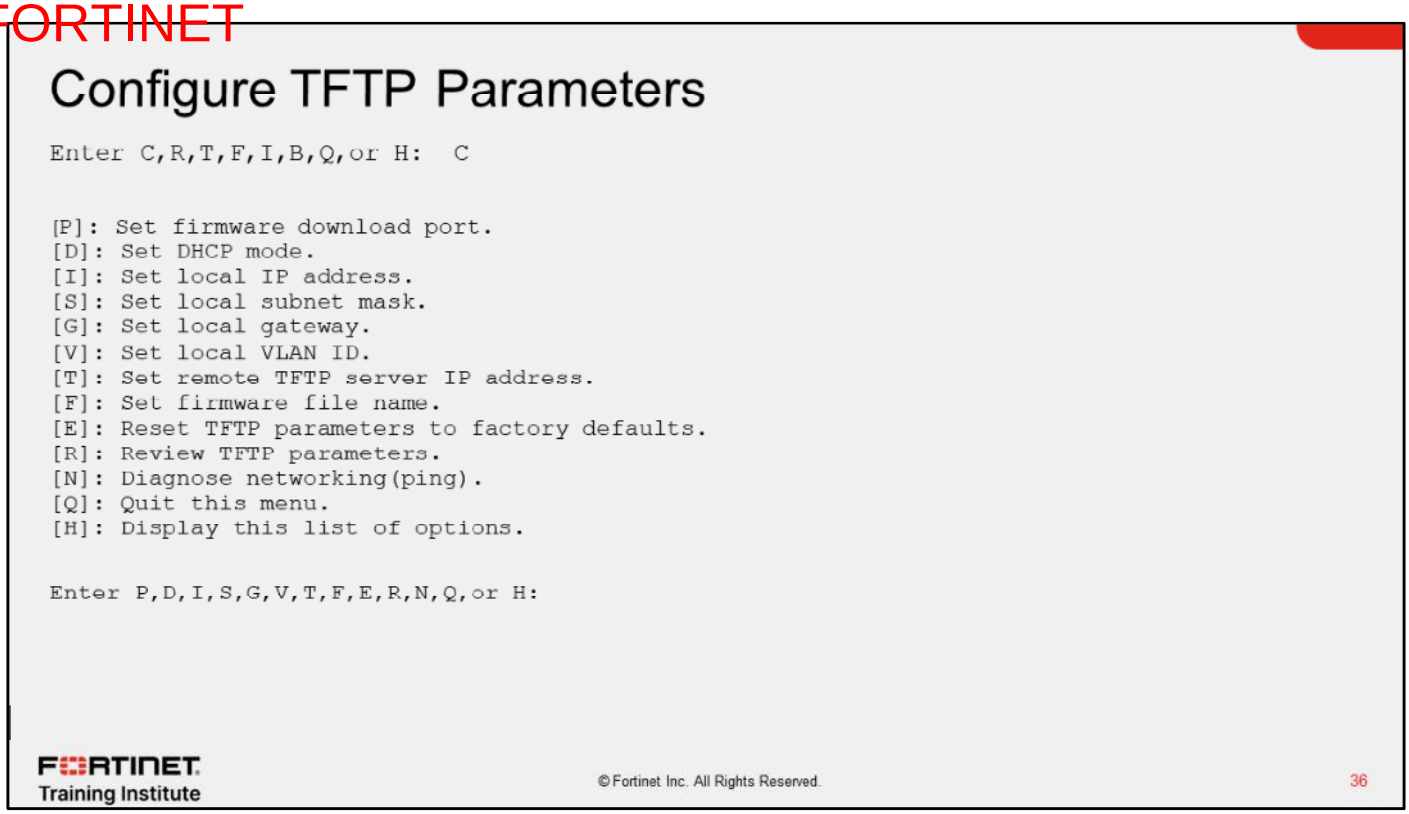
1. Run a TFTP server.
2. Configure the TFTP server with the folder where the firmware image file is stored.
3. Connect the PC Ethernet port to the FortiGate TFTP installation interface.
4. Select `get firmware image` from the BIOS menu.

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.

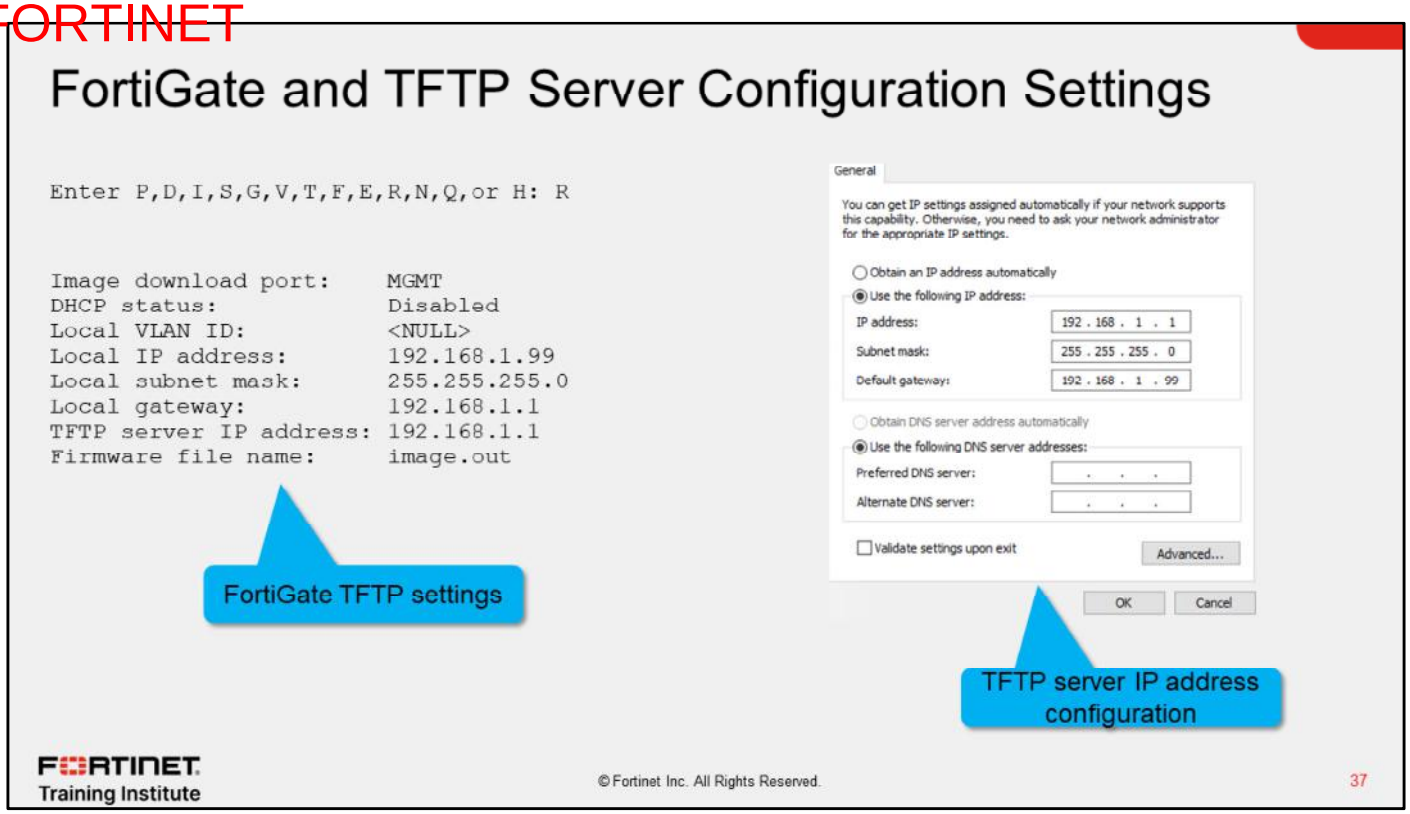


From the BIOS menu, select `F` to format the flash memory.

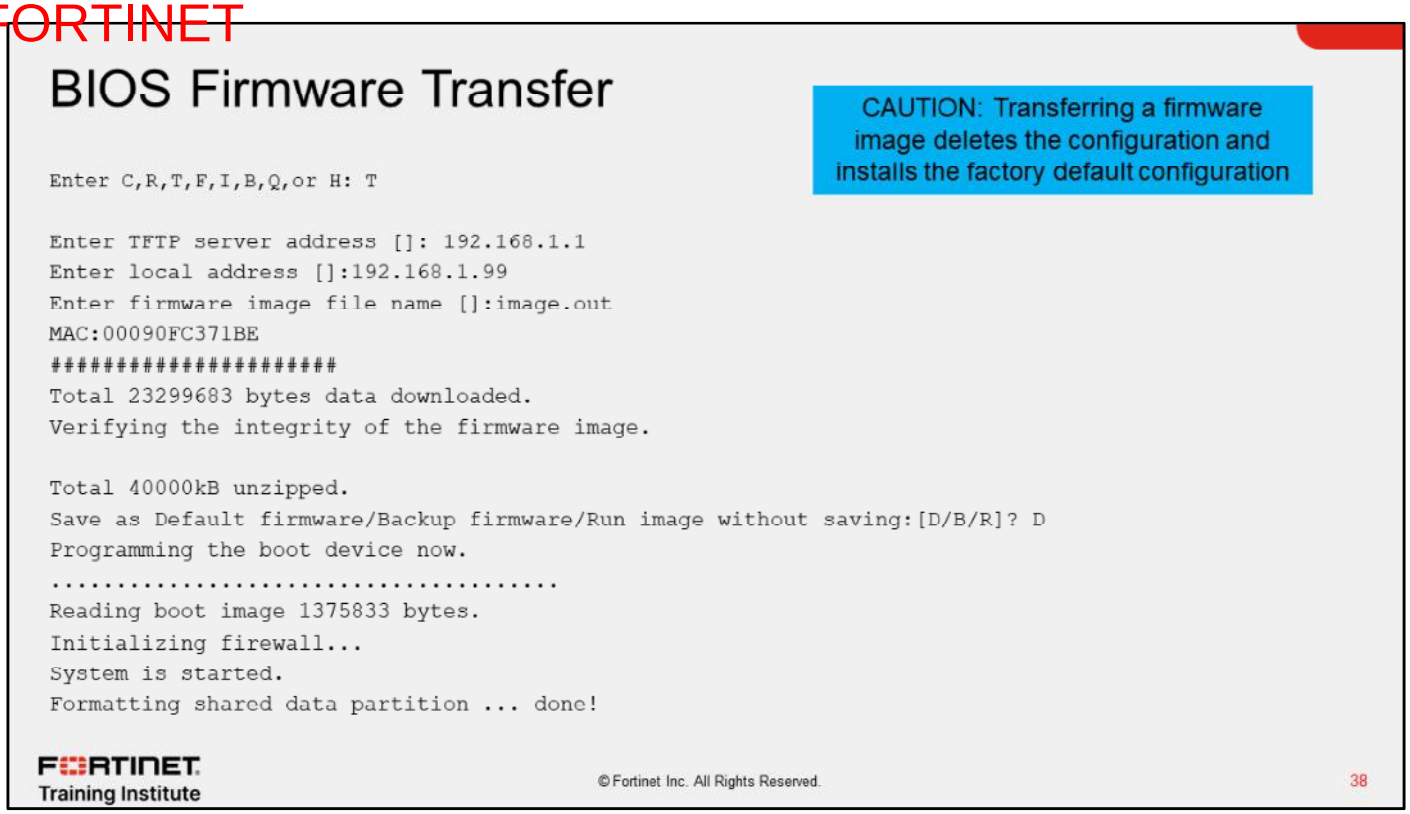
Doing this might be required if the firmware gets corrupted, or if the administrator wants to do a clean installation of new firmware. Keep in mind, though, that formatting the flash memory deletes any information stored on it, such as firmware images, configuration, and digital certificates.



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.



Press `R` to review the TFTP configuration settings.
After you have configured the TFTP parameters, press `Q` to return to the main configuration menu.



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

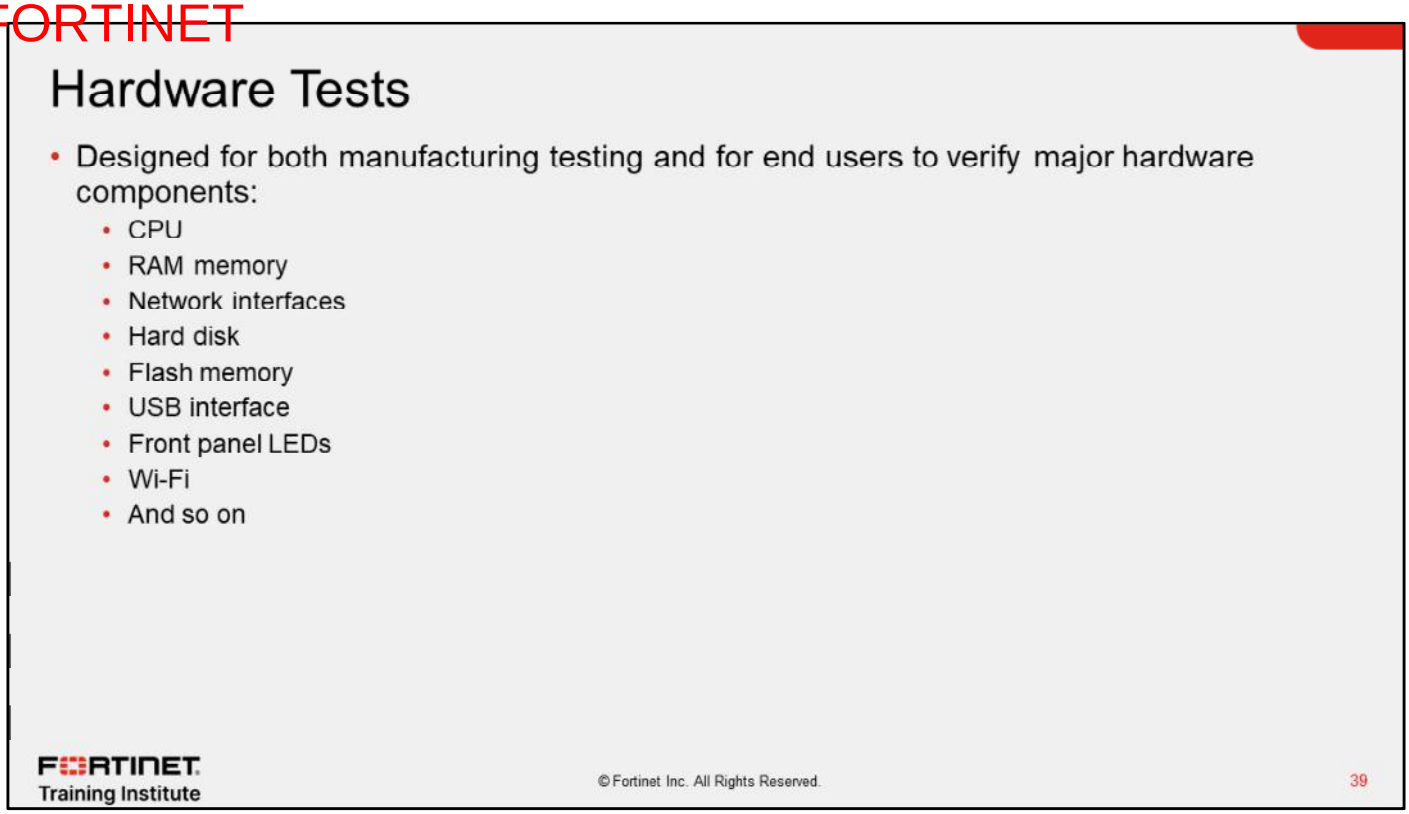
The BIOS requires you to enter:
- The IP address of the TFTP server
- The FortiGate IP address (it must be in the same class-C subnet as the TFTP server)
- The name of the firmware image

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`.

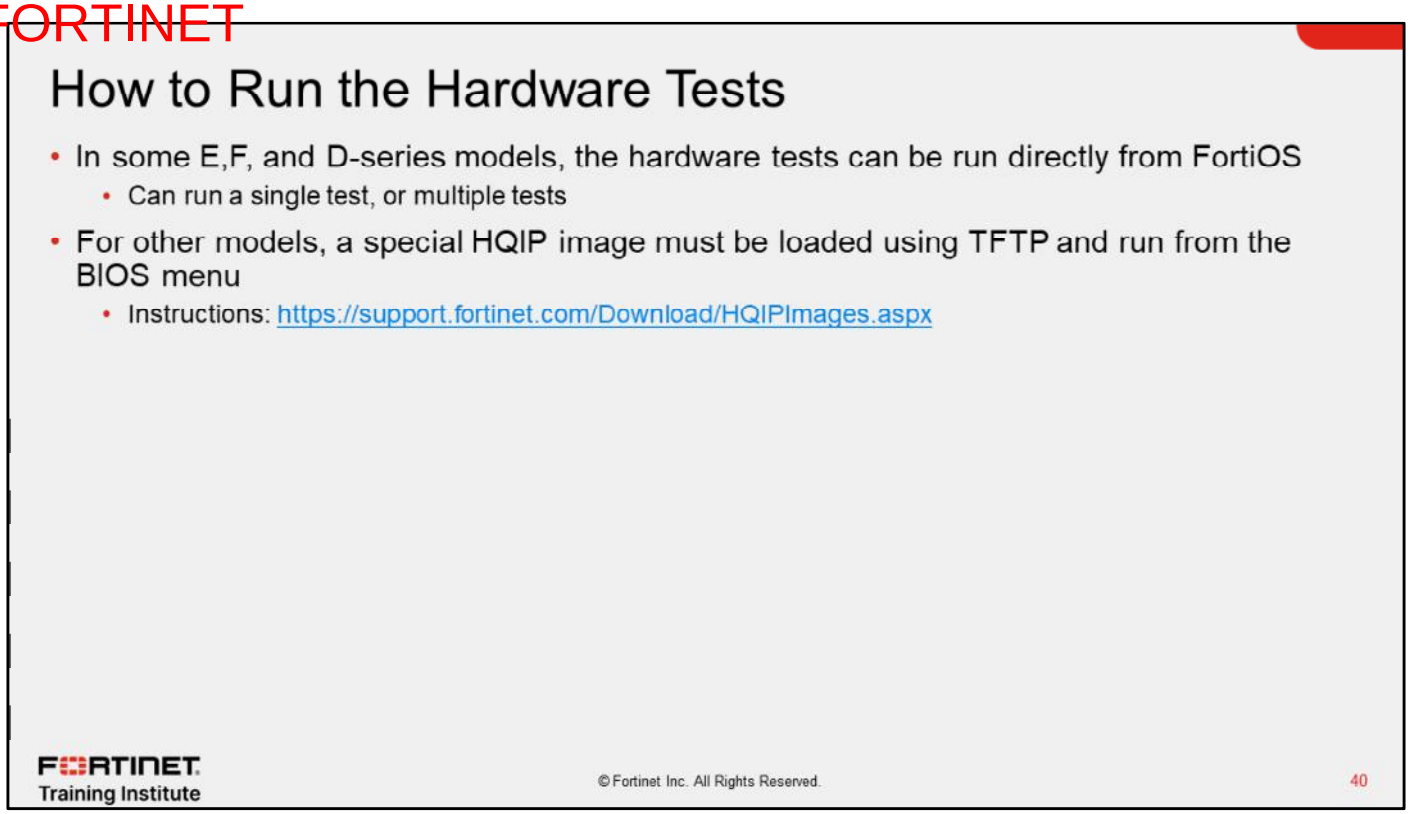
The last option (`Run the image without saving it`) allows you to run and test firmware without overwriting any existing firmware in the memory. After you have finished the tests and are ready to roll back the change, you must reboot the device, and the previously existing firmware will be used.



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

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

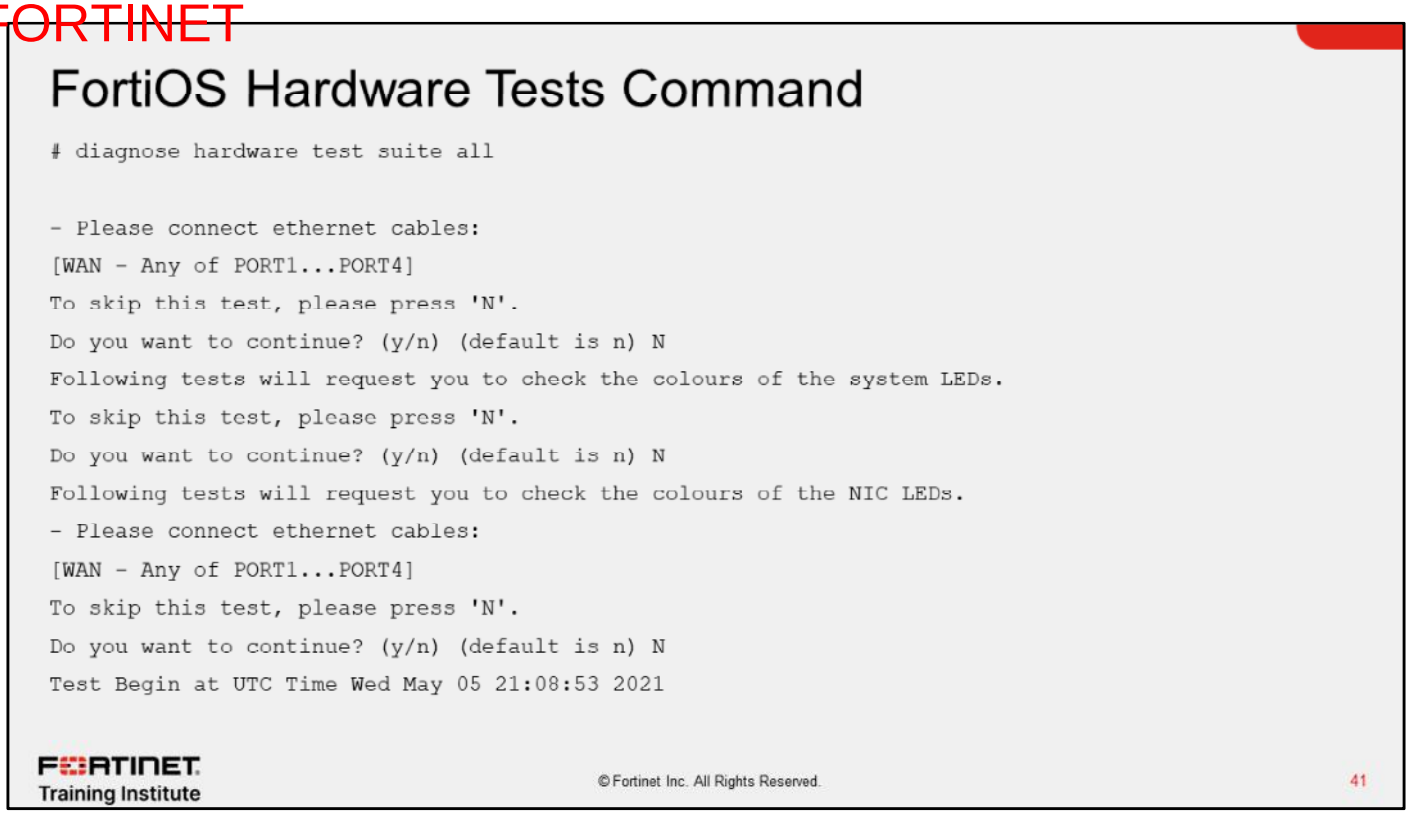
How do you run the hardware tests? It depends on the FortiGate model.



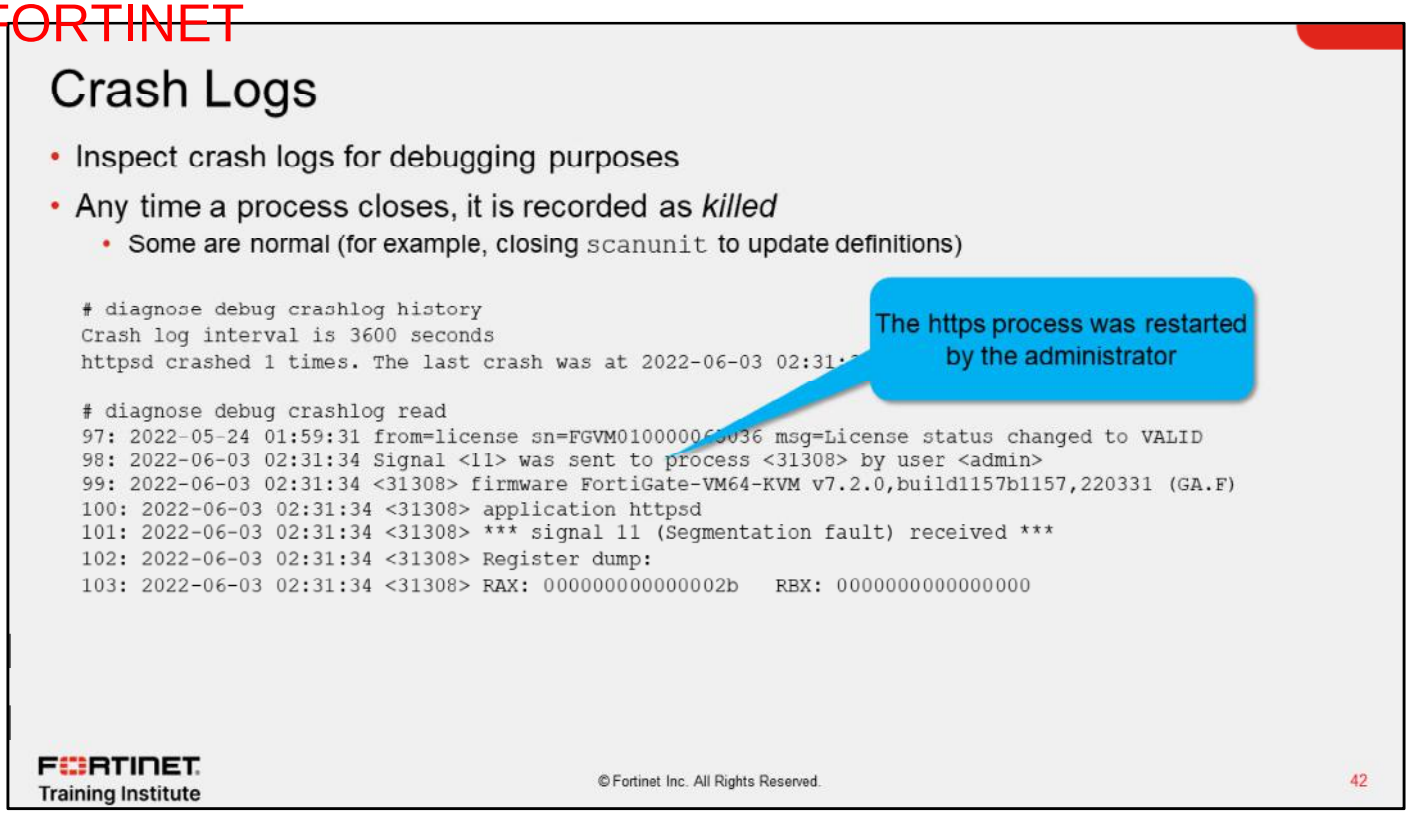
For some FortiGate E, F, and D-series models, you can run the hardware tests directly from the FortiOS CLI.

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.



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.



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.

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"
```

FORTINET Training Institute

43

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

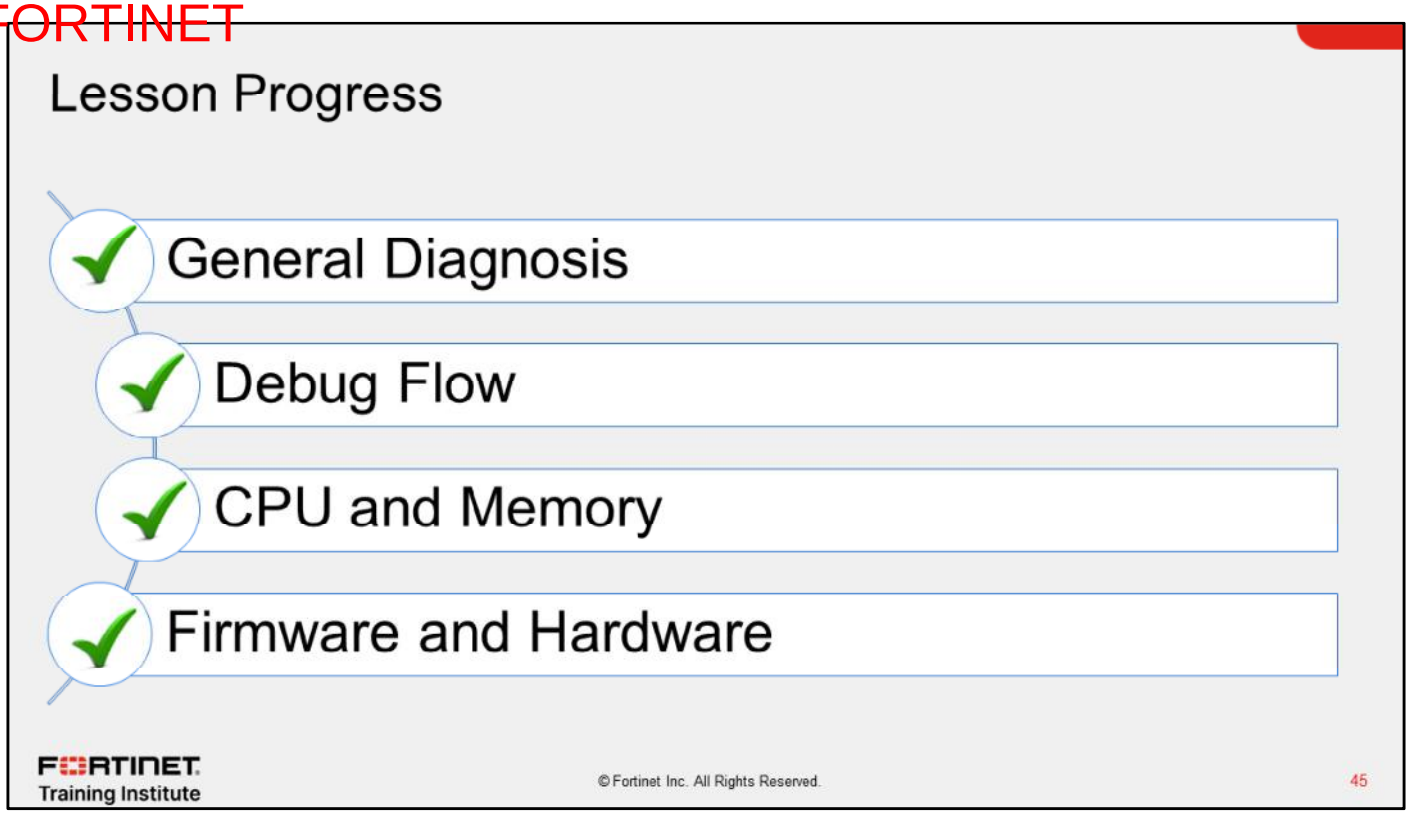
Knowledge Check

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

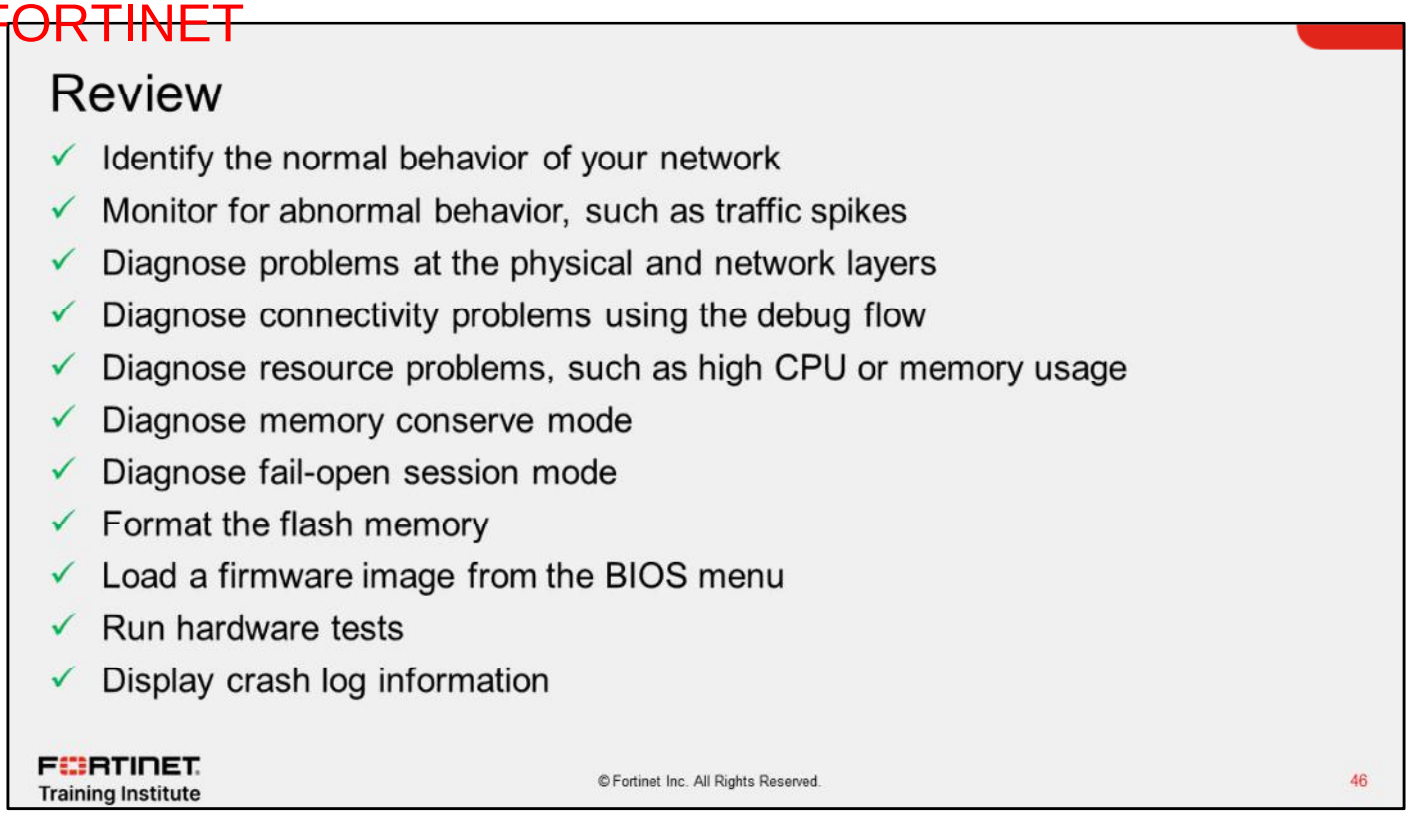
FORTINET Training Institute

44



Congratulations! You have completed the lesson.

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



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.