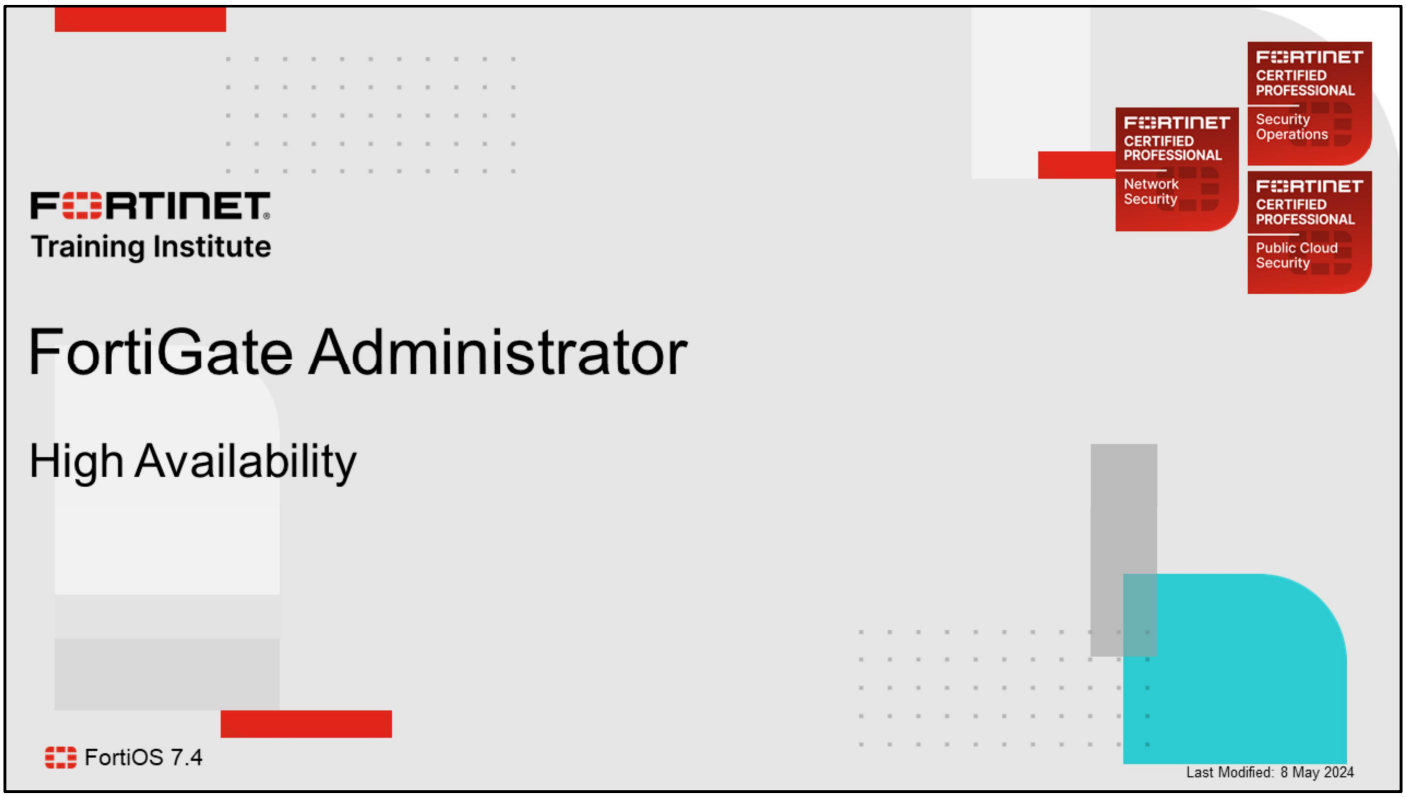


In this lesson, you will learn about the fundamentals of FortiGate high availability (HA) and how to configure it. FortiGate HA provides a solution for enhanced reliability and increased performance.

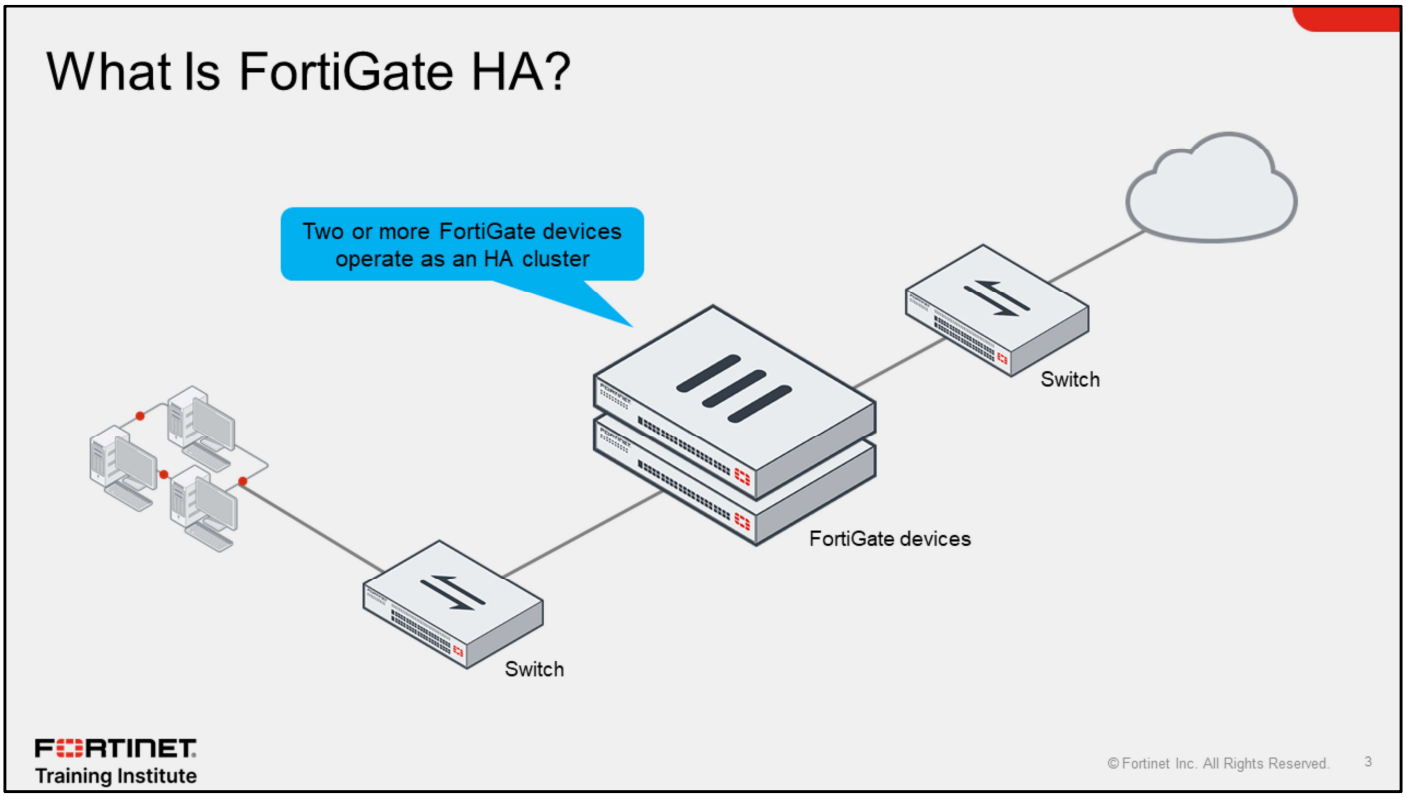
Objectives

- Configure HA (FGCP)
- Configure HA failover
- Configure HA session synchronization
- Configure the HA management interface
- Verify the normal operation of an HA cluster
- Upgrade an HA cluster

FORTINET Training Institute

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

By demonstrating competence in FortiGate HA, you will be able to configure a redundant firewall cluster in your network, verify its operational status, and make changes to suit your business and security requirements.

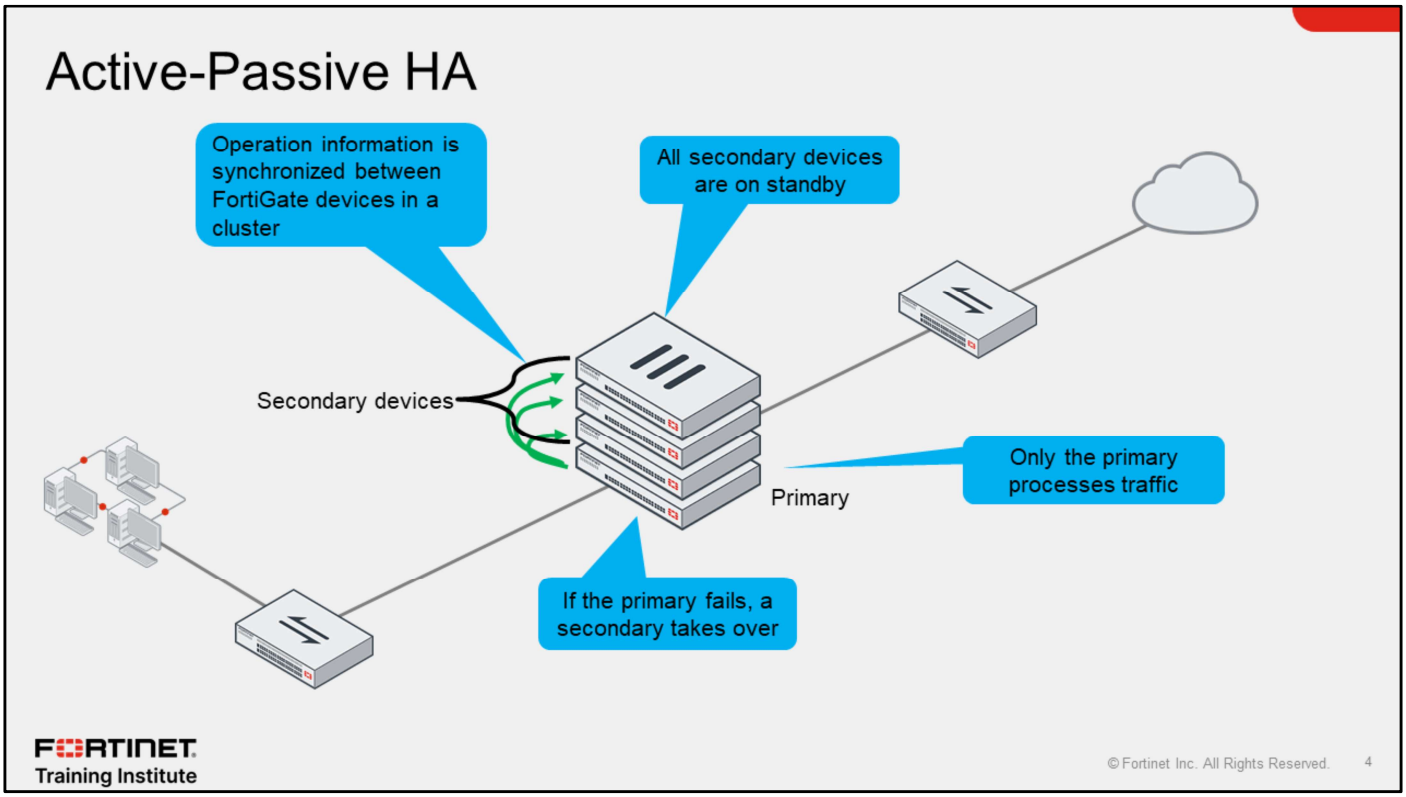


FortiGate HA uses the FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health of members. FortiGate HA links and synchronizes two or more FortiGate devices to form a cluster for redundancy and performance purposes.

A cluster includes one device that acts as the primary FortiGate (also called the active FortiGate). The primary sends its complete configuration to other members that join the cluster, overwriting their configuration (except for a few settings). It also synchronizes session information, FIB entries, FortiGuard definitions, and other operation-related information to the secondary devices, which are also known as standby devices.

The cluster shares one or more heartbeat interfaces among all devices—also known as members—for synchronizing data and monitoring the health of each member.

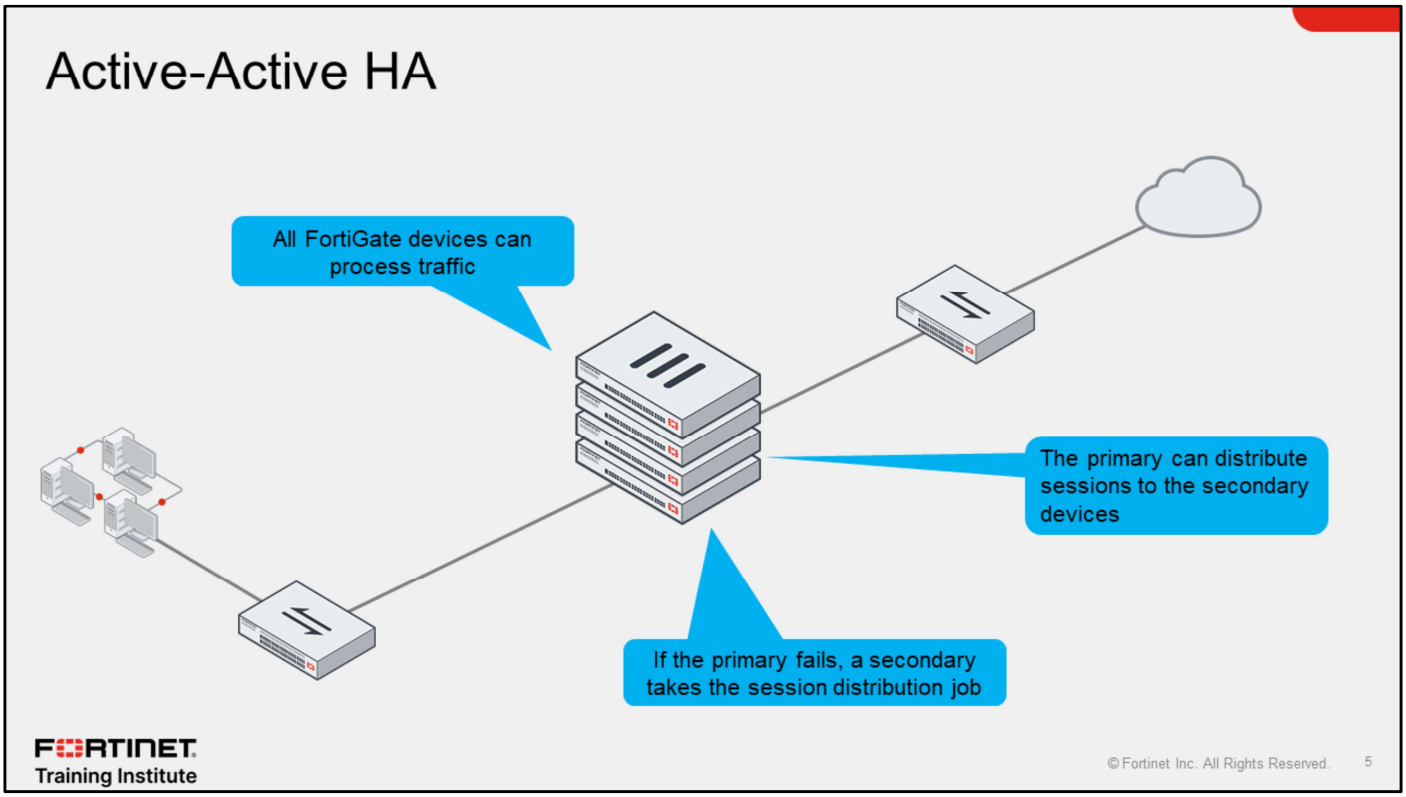
There are two HA operation modes available: active-active and active-passive. Now, you will learn about the differences.



In active-passive mode, the primary FortiGate is the only FortiGate that actively processes traffic. Secondary FortiGate devices remain in passive mode, monitoring the status of the primary device.

In either of the two HA operation modes, the operation information (sessions, FIB entries, and so on) of the primary FortiGate is synchronized with secondary devices. If a problem is detected on the primary FortiGate, one of the secondary devices takes over the primary role. This event is called an *HA failover*.

If a secondary FortiGate device fails, the primary updates its list of available secondary FortiGate devices. It also starts monitoring for the failed secondary, waiting for it to come online again.



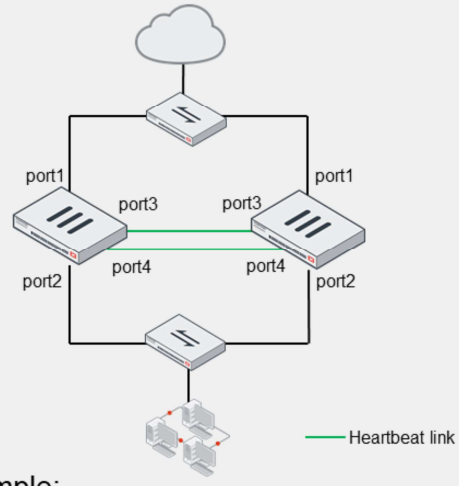
The other HA mode is active-active.

Like active-passive HA, in active-active HA, the operation-related data is synchronized between devices in the cluster. Also, if a problem is detected on the primary device, one of the secondary devices takes over the role of the primary to process the traffic.

However, one of the main differences from active-passive mode is that in active-active mode, all cluster members can process traffic. That is, based on the HA settings and traffic type, the primary FortiGate can distribute supported sessions to the secondary devices. If one of the secondary devices fails, the primary also reassigns sessions to a different secondary FortiGate.

HA Requirements

- All members must have the same:
  - Model
  - Firmware version
  - Licensing
    - If different, the cluster uses the lowest-level license
  - Hard drive configuration
  - Operating mode (management VDOM)
- Setup:
  - Same HA group ID, group name, password, and heartbeat interface settings
- Best practice:
  - Use at least two heartbeat interfaces
  - Initially, switch DHCP and PPPoE interfaces to static configuration



Example:

```
config system ha
     set mode a-p
     set group-id 10
     set group-name "Training"
     set password <password>
     set hbdev "port3" 10 "port4" 20
end
```

FORTINET Training Institute

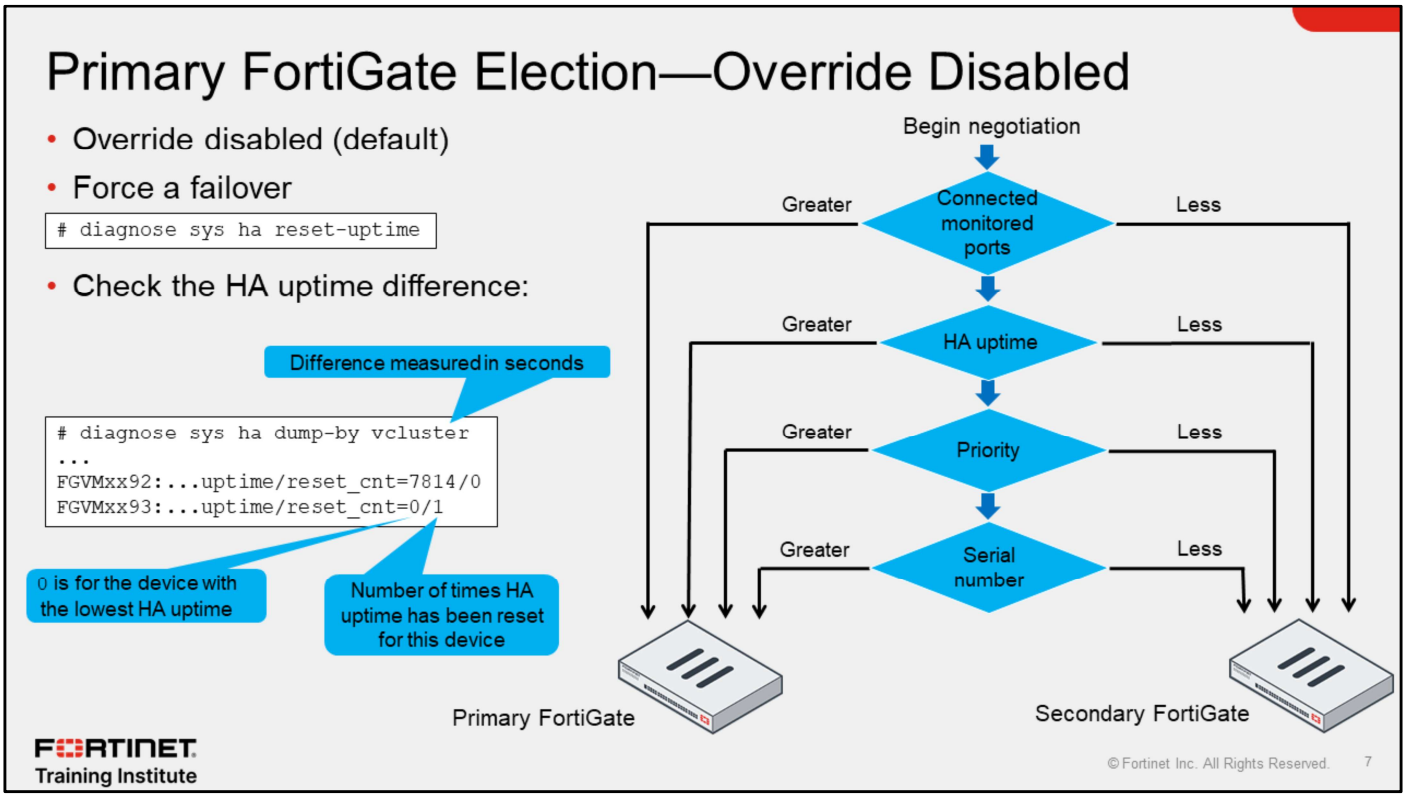
To successfully form an HA cluster, you must ensure that the members have the same:

- Model: the same hardware model or VM model
- Firmware version
- Licensing: includes the FortiGuard license, virtual domain (VDOM) license, FortiClient license, and so on
- Hard drive configuration: the same number and size of drives and partitions
- Operating mode: the operating mode—NAT mode or transparent mode—of the management VDOM. VDOMs divide a FortiGate device into two or more virtual units, essentially dividing one physical firewall into additional logical devices.

If the licensing level among members isn't the same, the cluster resolves to use the lowest licensing level among all members. For example, if you purchase FortiGuard Web Filtering for only one of the members in a cluster, none of the members will support FortiGuard Web Filtering when they form the cluster.

From a configuration and setup point of view, you must ensure that the HA settings on each member have the same group ID, group name, password, and heartbeat interface settings. Try to place all heartbeat interfaces in the same broadcast domain, or for two-member clusters, connect them directly. It's also a best practice to configure at least two heartbeat interfaces for redundancy purposes. This way, if one heartbeat link fails, the cluster uses the next one, as indicated by the priority and position in the heartbeat interface list. The priority is defined as seen on this slide, and a higher value means higher priority.

If you are using DHCP or Point-to-Point Protocol over Ethernet (PPPoE) interfaces, use static configuration during the cluster initial setup to prevent incorrect address assignment. After the cluster is formed, you can revert to the original interface settings.



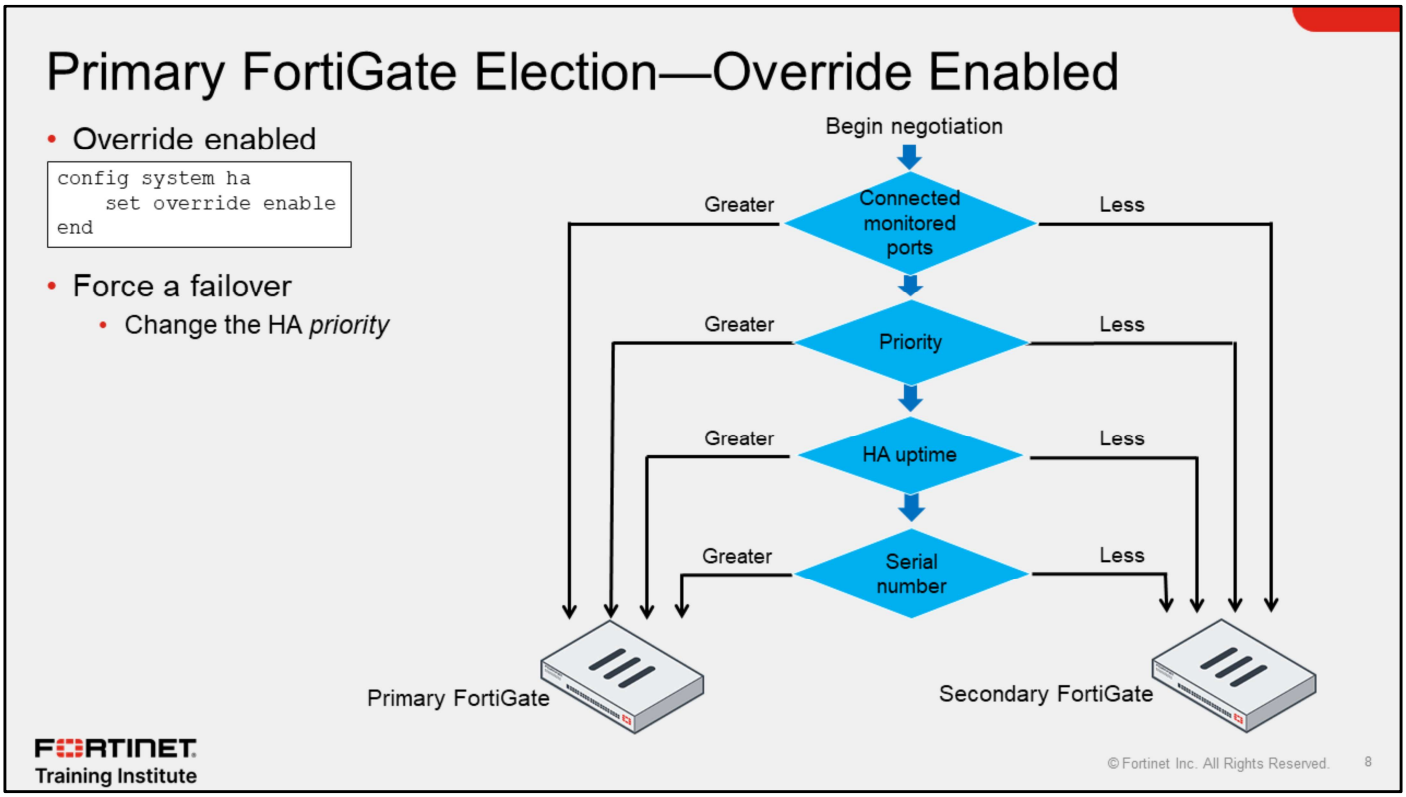
This slide shows the different criteria that a cluster considers during the primary FortiGate election process. The criteria order evaluation depends on the HA override setting. This slide shows the order when the HA override setting is disabled, which is the default behavior. Note that the election process stops at the first matching criteria that successfully selects a primary FortiGate in a cluster.

1. The cluster compares the number of monitored interfaces that have a status of up. The member with the most available monitored interfaces becomes the primary.
2. The cluster compares the HA uptime of each member. The member with the highest HA uptime, by at least five minutes, becomes the primary.
3. The member with the highest priority becomes the primary.
4. The member with the highest serial number becomes the primary.

When HA override is disabled, the HA uptime has precedence over the priority setting. This means that if you must manually fail over to a secondary device, you can do so by reducing the HA uptime of the primary FortiGate. You can do this by running the `diagnose sys ha reset-uptime` command on the primary FortiGate, which resets its HA uptime to 0.

Note that the `diagnose sys ha reset-uptime` command resets the HA uptime and not the system uptime. Also, note that if a monitoring interface fails, or a member reboots, the HA uptime for that member is reset to 0.

This slide also shows how to identify the HA uptime difference between members. The member with `0` in the `uptime` column indicates the device with the lowest uptime. The example shows that the device with the serial number ending in `92` has an HA uptime that is `7814` seconds higher than the other device in the HA cluster. The `reset_cnt` column indicates the number of times the HA uptime has been reset for that device.

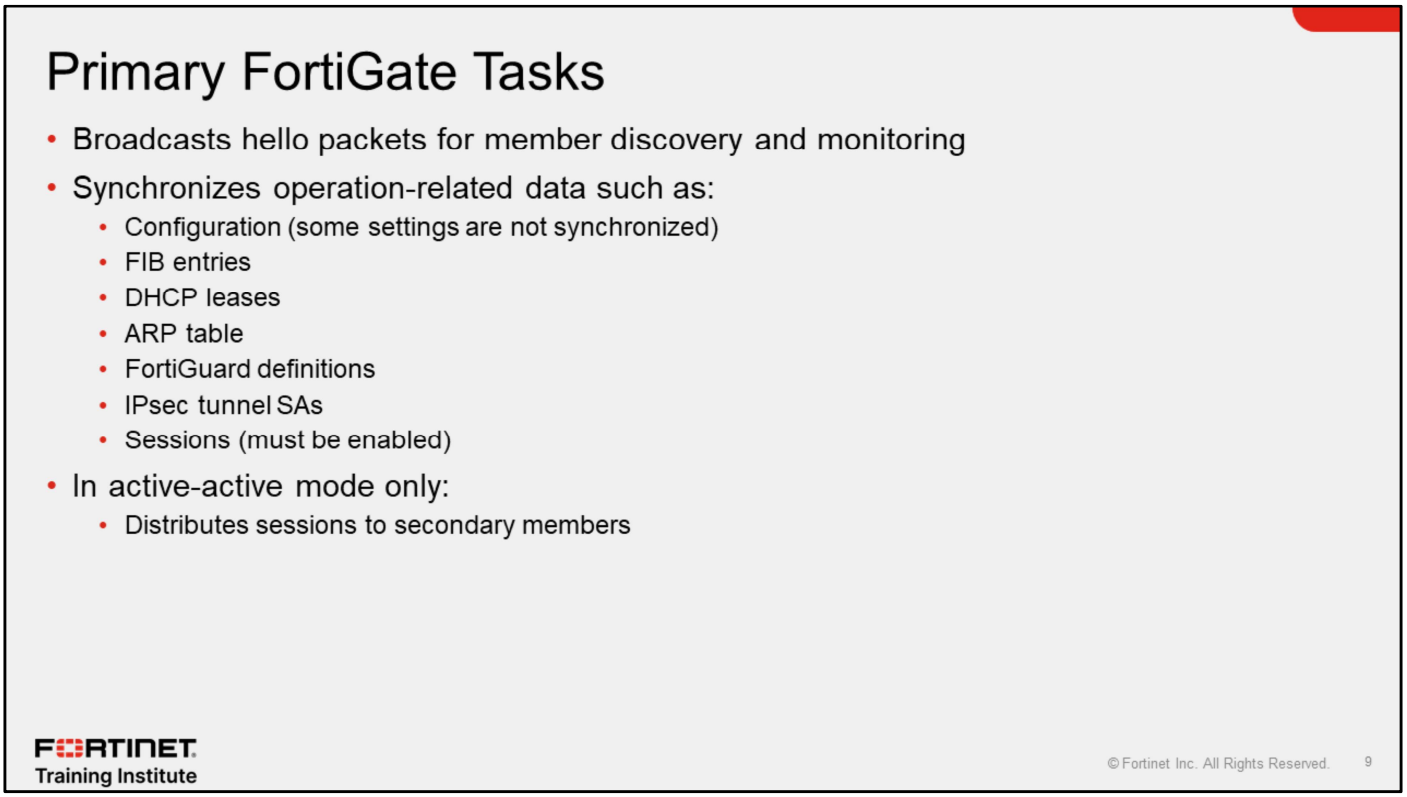


If the HA override setting is enabled, the priority is considered before the HA uptime.

The advantage of this method is that you can specify which device is the preferred primary every time (as long as it is up and running) by configuring it with the highest HA priority value. The disadvantage is that a failover event is triggered not only when the primary fails, but also when the primary is available again. That is, when the primary becomes available again, it takes its primary role back from the secondary FortiGate that temporarily replaced it.

When override is enabled, the easiest way of triggering a failover is to change the HA priorities. For example, you can either increase the priority of one of the secondary devices, or decrease the priority of the primary.

The override setting and device priority values are not synchronized to cluster members. You must manually enable override and adjust the priority on each member.



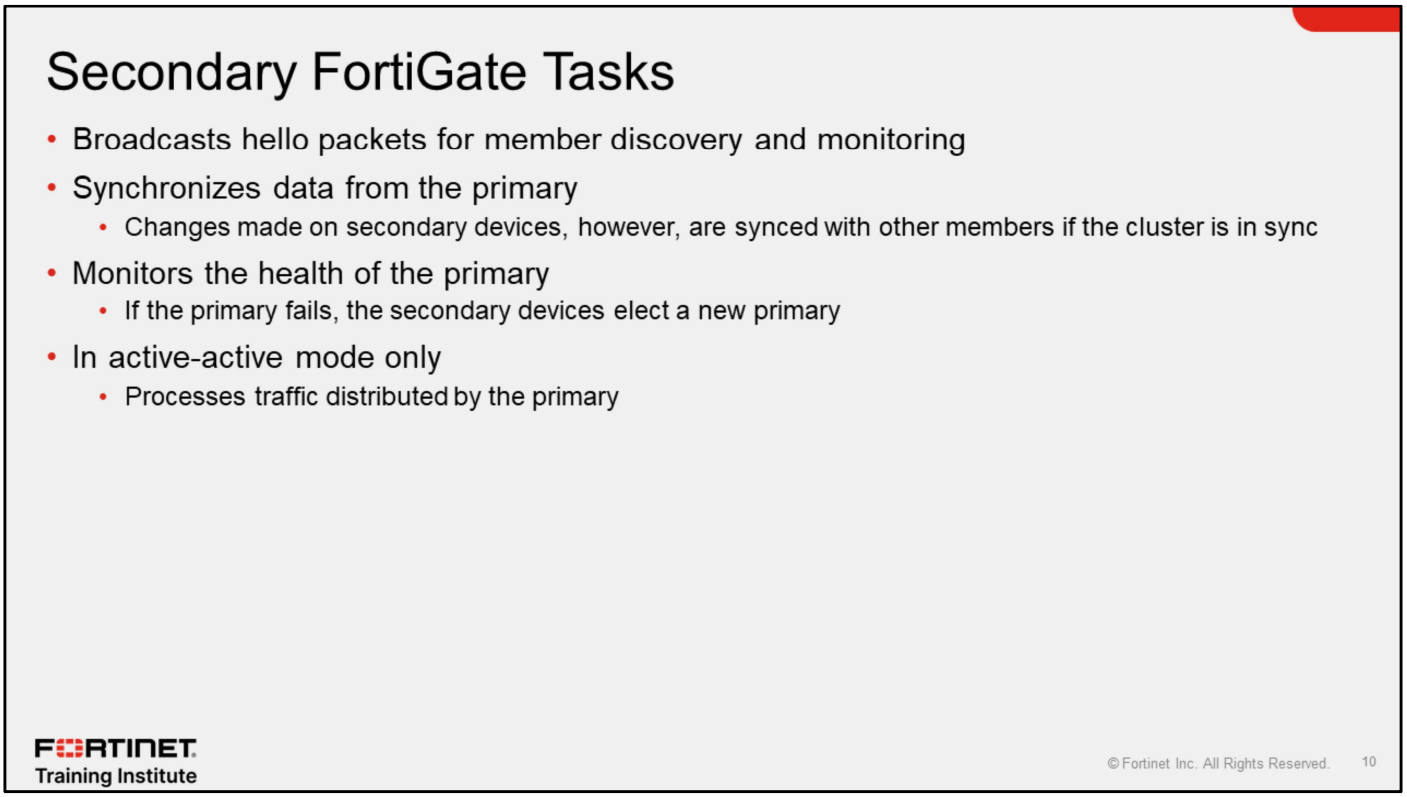
So, what are the tasks of a primary FortiGate?

It monitors the cluster by broadcasting hello packets and listening for hello packets from other members in the cluster. The members use the hello packets to identify if other FortiGate devices are alive and available.

The primary FortiGate also synchronizes its operation-related data to the secondary members. Some of the data synchronized includes its configuration, FIB entries, DHCP leases, ARP table, FortiGuard definitions, and IPsec tunnel security associations (SAs). Note that some parts of the configuration are not synchronized because they are device-specific. For example, the host name, HA priority, and HA override settings are not synchronized.

Optionally, you can configure the primary FortiGate to synchronize qualifying sessions to all the secondary devices. When you enable session synchronization, the new primary can resume communication for sessions after a failover event. The goal is for existing sessions to continue flowing through the new primary FortiGate with minimal or no interruption. You will learn which types of sessions you can enable synchronization for later in the lesson.

In active-active mode only, a primary FortiGate is also responsible for distributing sessions to secondary members.

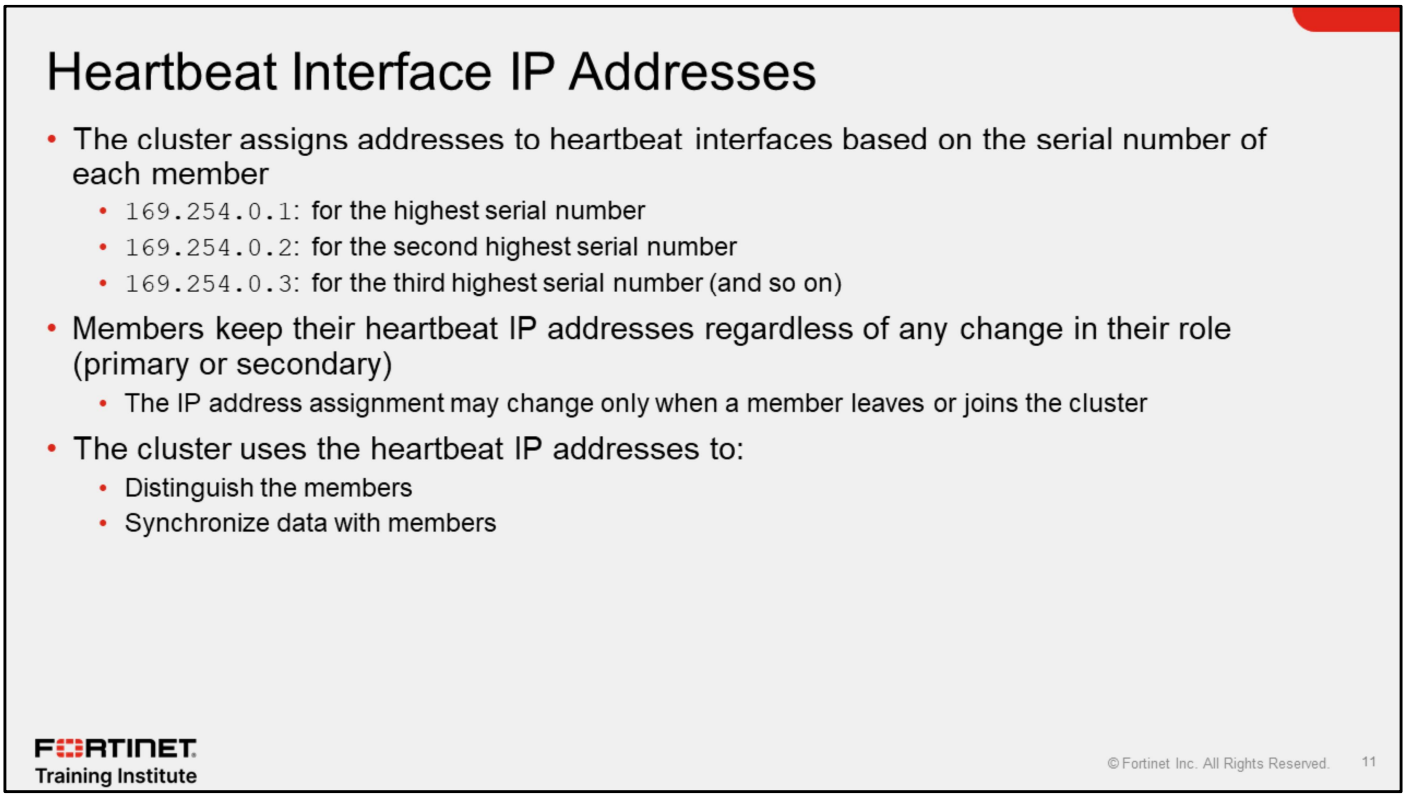


Now, take a look at the tasks of secondary FortiGate devices.

Like the primary, secondary members also broadcast hello packets for discovery and monitoring purposes.

In addition, in active-passive mode, the secondary devices act as a standby device, receiving synchronization data but not actually processing any traffic. If the primary FortiGate fails, the secondary devices elect a new primary. Once a cluster is in sync, configuration changes made on a secondary device are propagated to other members. In other words, with a cluster that is in sync, you can make changes on any of its members—not just the primary device only—and all changes are synchronized among the cluster members. However, it is recommended that you make configuration changes on the primary device because this prevents the loss of configuration changes if there are synchronization issues between cluster members.

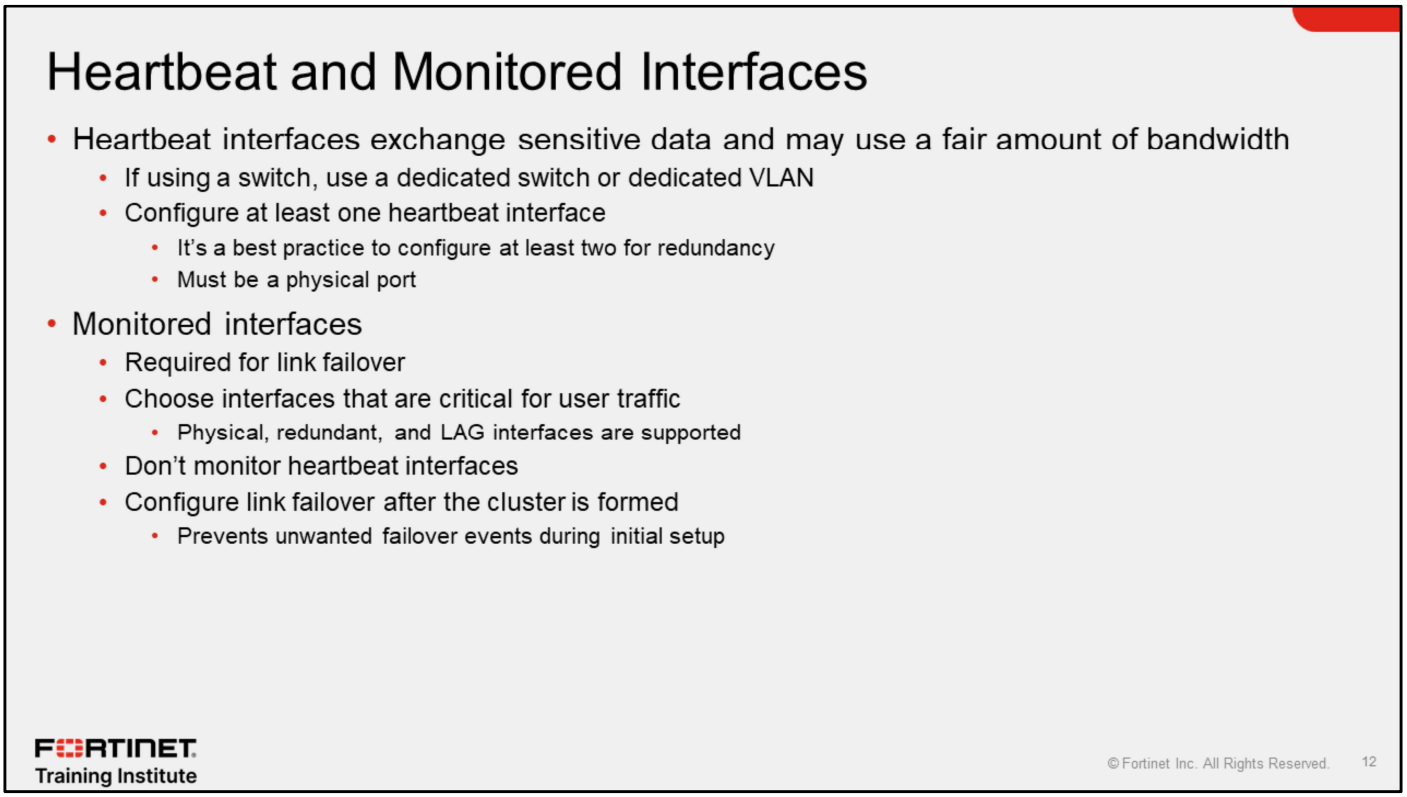
In active-active mode, the secondary devices don't wait passively. They process all traffic assigned to them by the primary device.



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. These IPs are non-routable and are used for FGCP operations only.

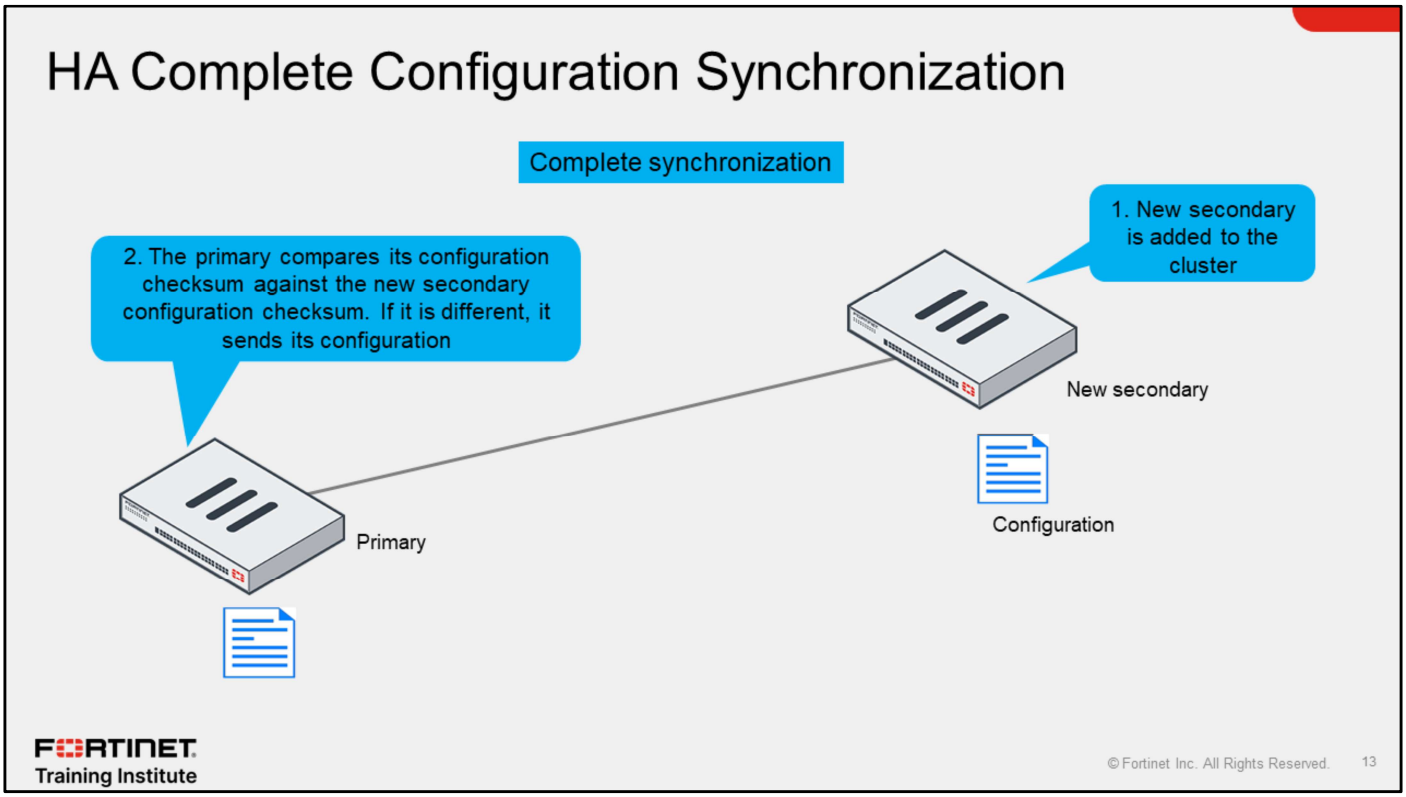


Heartbeat interfaces exchange sensitive information about the cluster operation and may require a fair amount of bandwidth for data synchronization. For this reason, if you use a switch to connect the heartbeat interfaces, it's recommended that you use a dedicated switch or, at least, that you place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

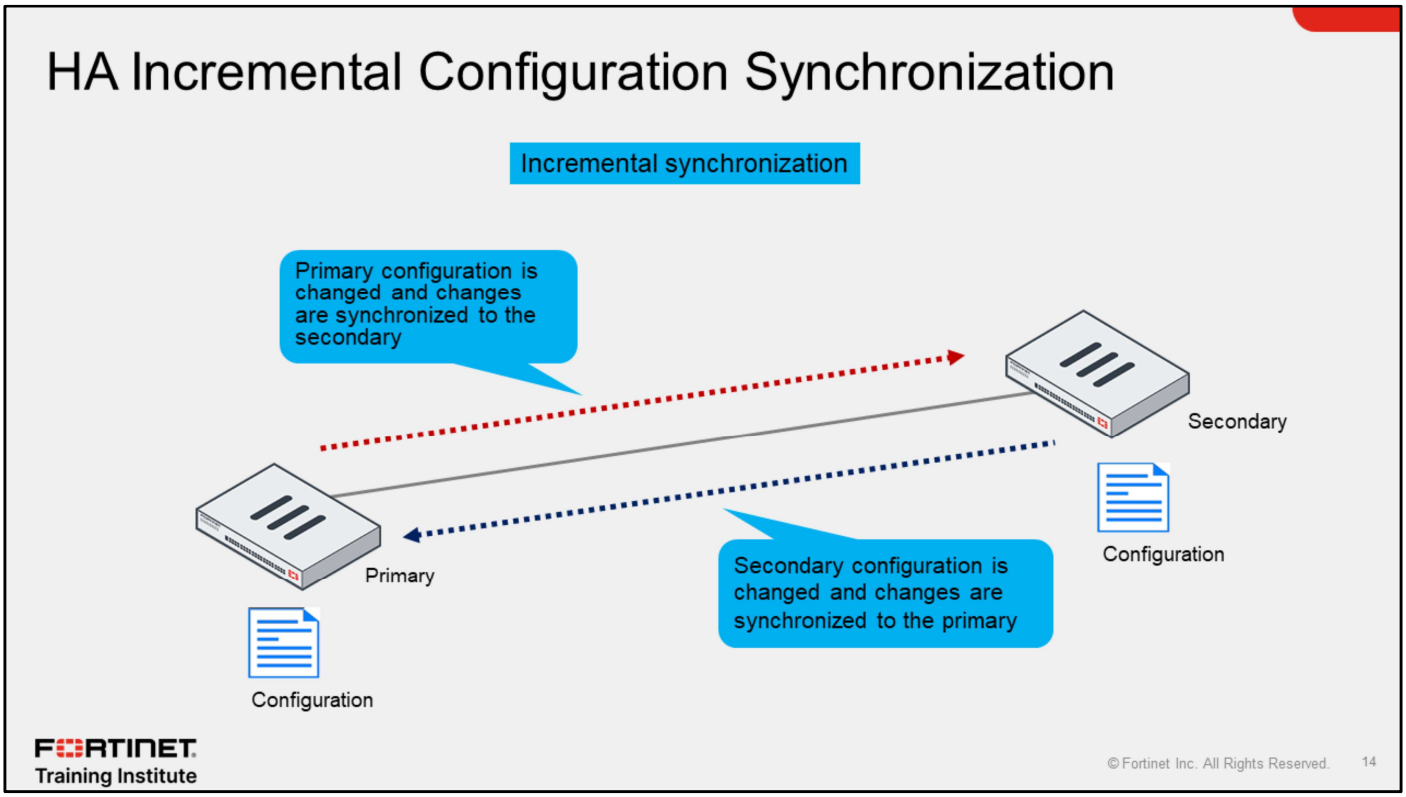
As a best practice, wait until a cluster is up and running and all interfaces are connected before configuring link failover. This is because a monitored interface can be disconnected during the initial setup and, as a result, trigger a failover before the cluster is fully configured and tested.



To prepare for a failover, an HA cluster keeps its configurations in sync.

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 the configuration of an HA cluster device (primary or secondary), 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.

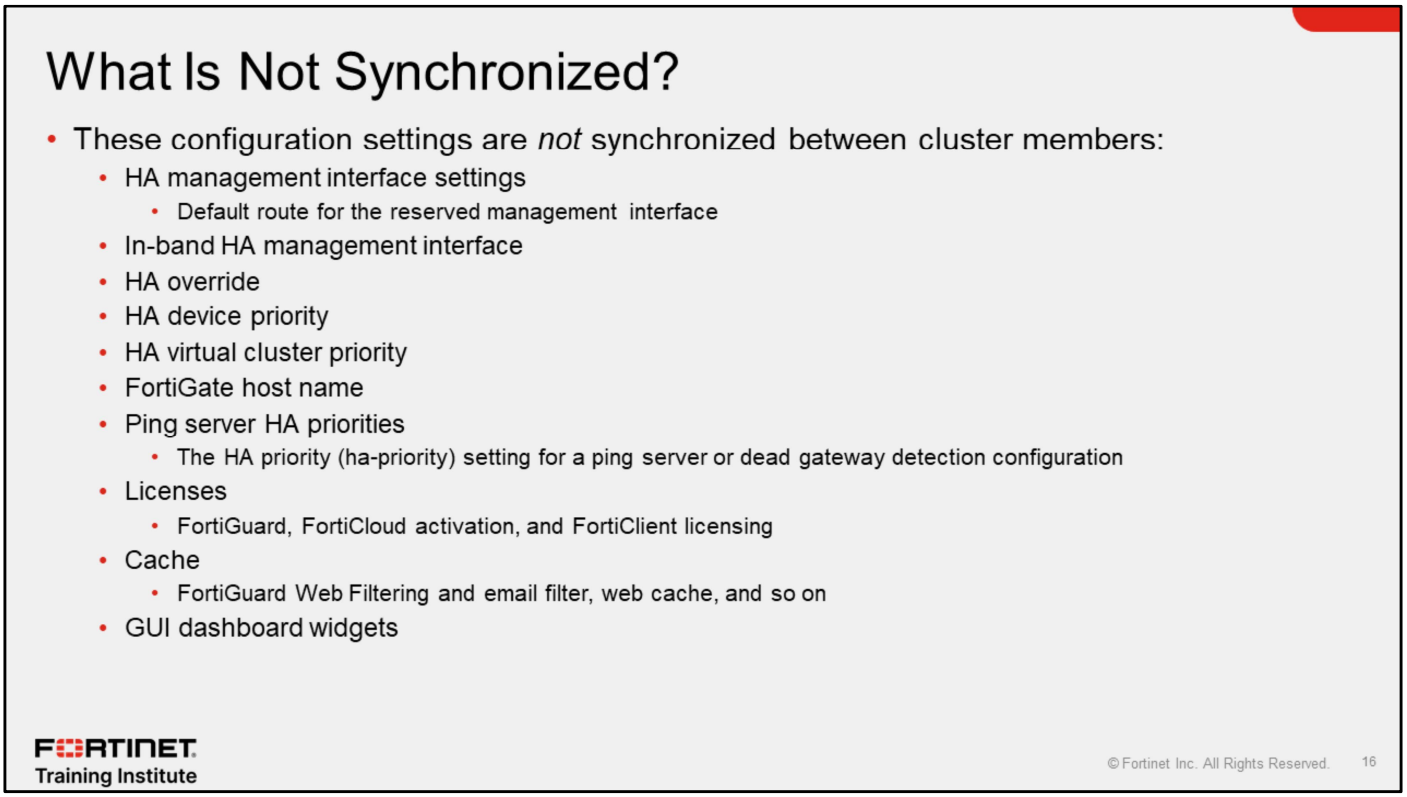
HA Configuration Synchronization

- 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 Training Institute

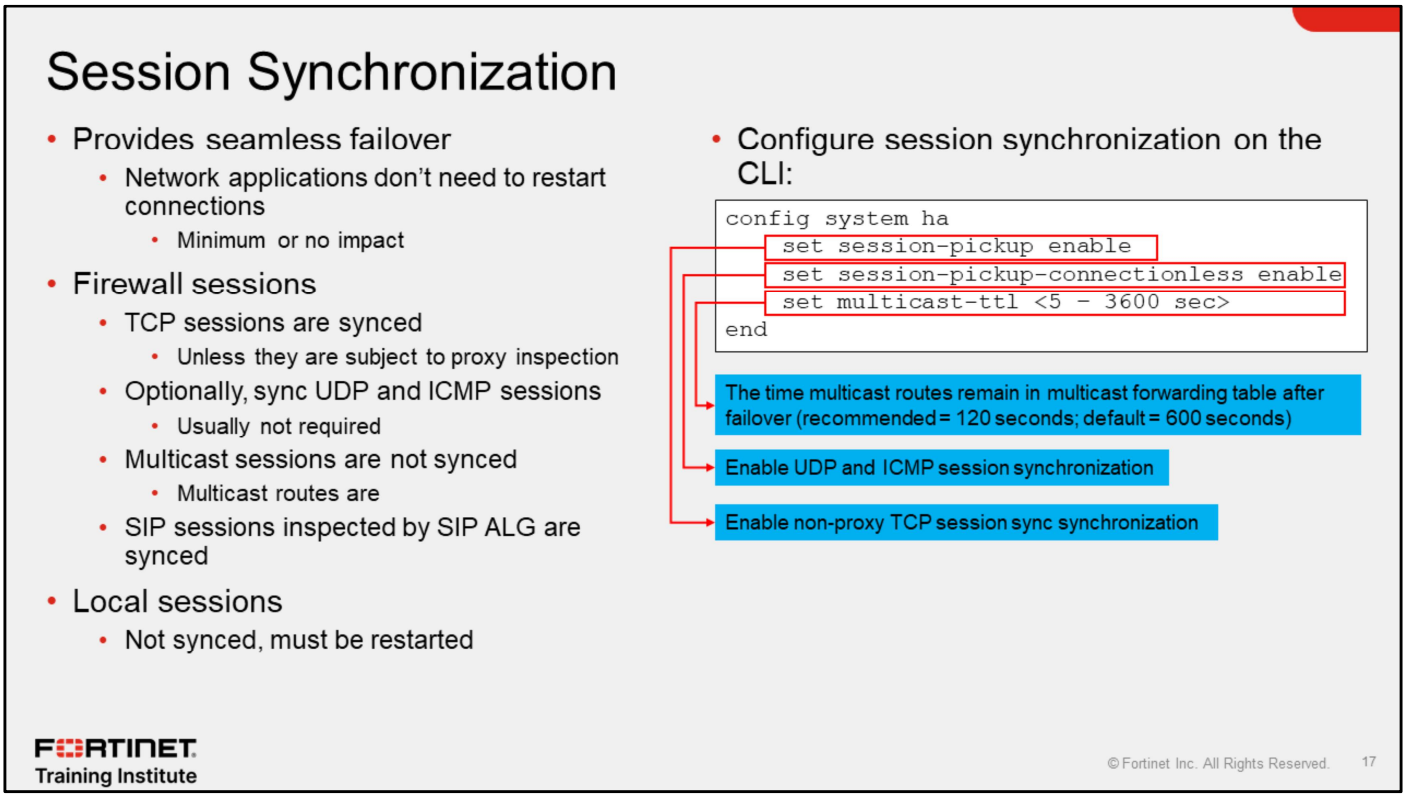
HA propagates more than just configuration details. Some runtime data, such as DHCP leases and FIB entries, are also synchronized.

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 in HA. 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
- GUI dashboard widgets



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.

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
- FortiGate doesn't synchronize data for SSL VPN users
  - Users must restart the SSL VPN tunnel after a failover by reconnecting to the VPN

FORTINET Training Institute

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, users have to restart the SSL VPN tunnel after a failover by reconnecting to the VPN.

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
- 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 Training Institute

The most common types of failovers are device failovers and link failovers. A device failover occurs when the secondary devices stop receiving 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, an issue on one of the interfaces on the primary, or an administrator-triggered failover. 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 x 100 ms x 6 = 1200 ms

- Link failover
  - Configure one or more monitored interfaces:

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

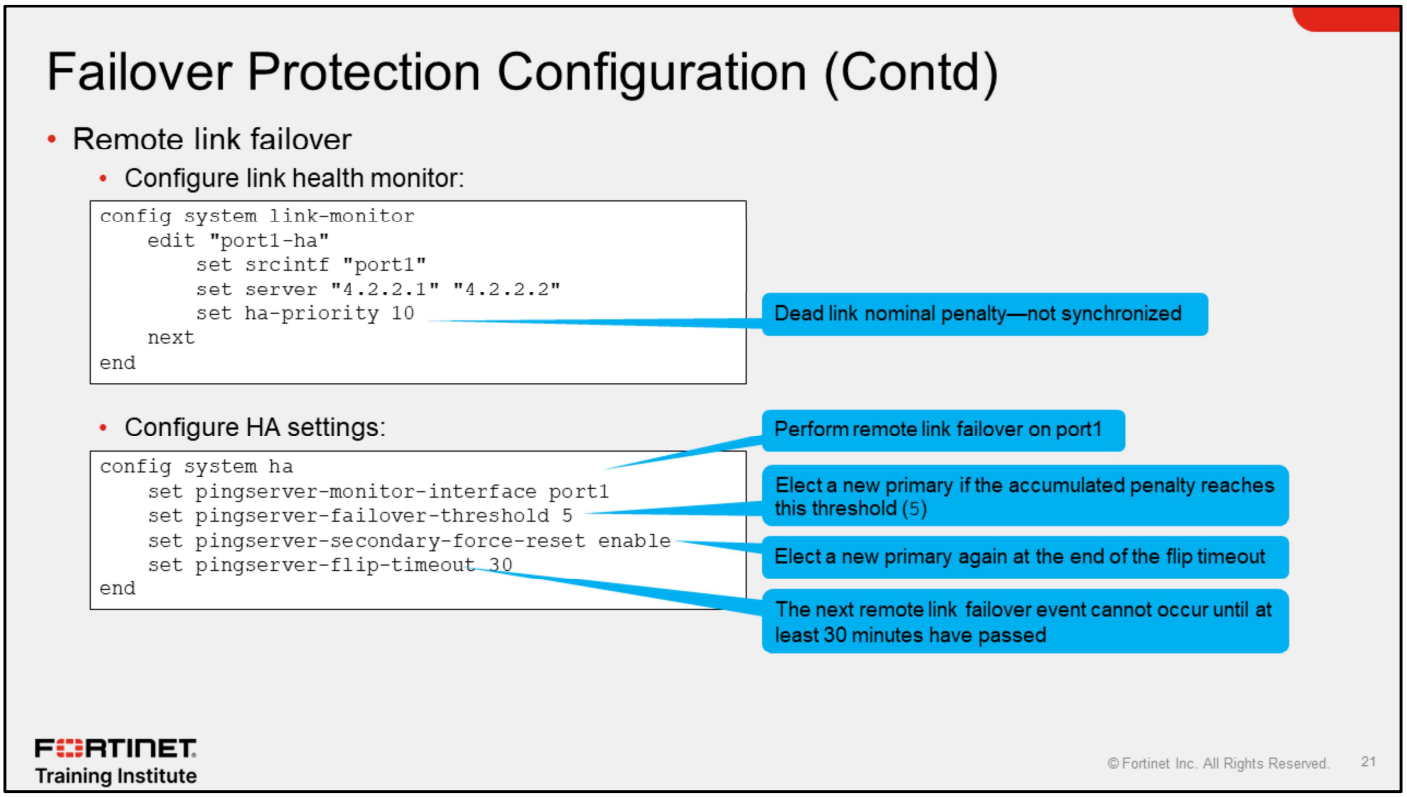
  - Supported interfaces:
    - Physical
    - Redundant
    - LAG

FORTINET Training Institute

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).

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.



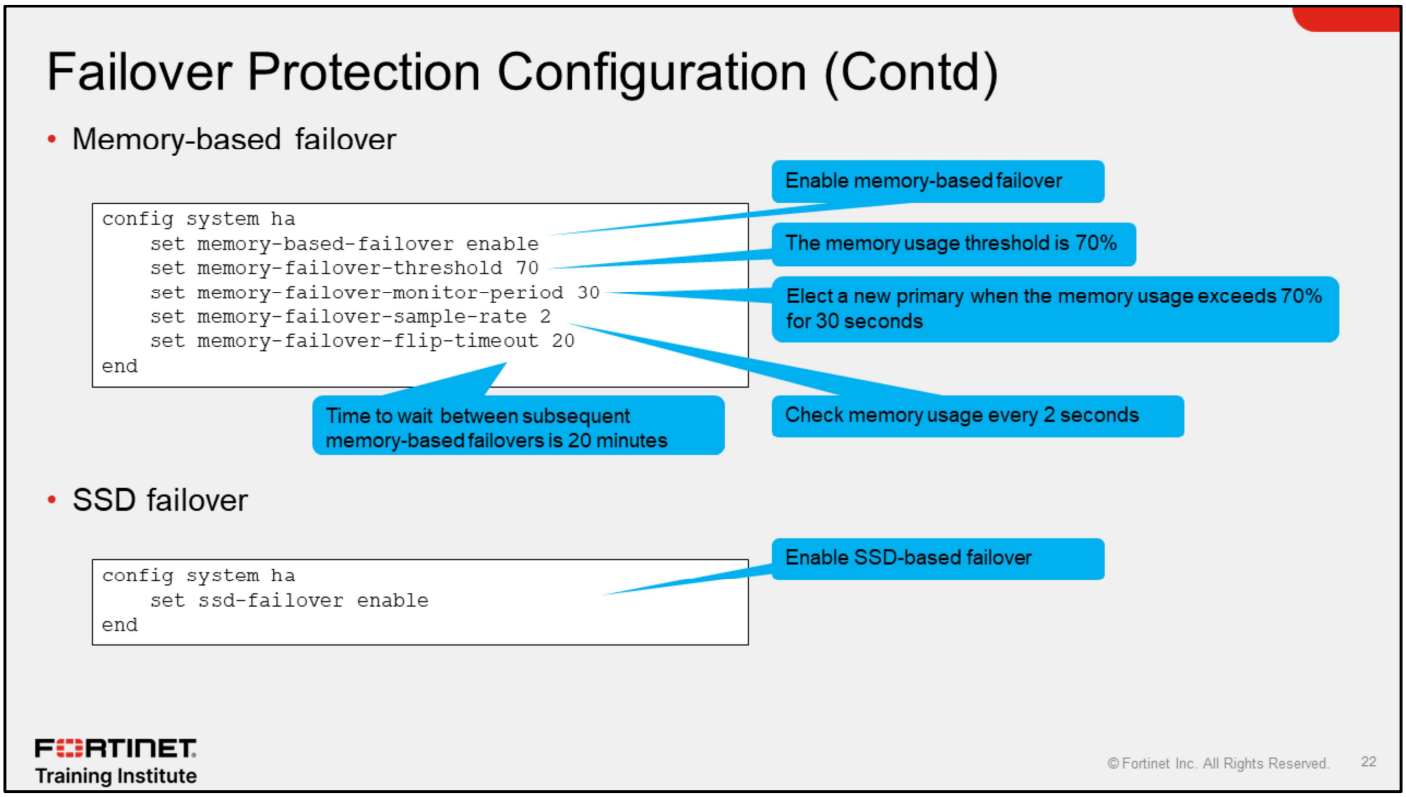
This slide shows a configuration example for remote link failover.

First, you configure the link health monitor. 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 with 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 pingserver flip timeout has passed. In other words, in this case the cluster can only encounter one remote link failover event per every 30 minutes or more. This prevents a flapping connection from continuously triggering HA failover.

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.



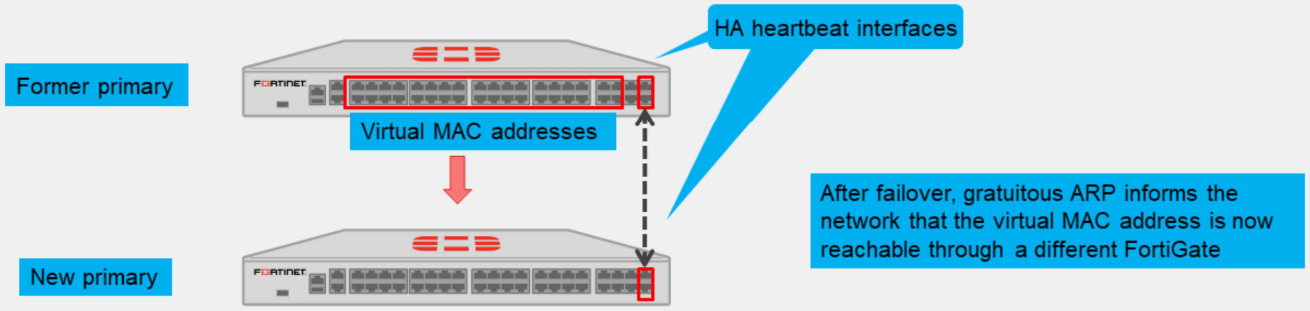
The HA configuration shown on this slide instructs FortiGate to perform memory-based failover as follows:

- 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.
- After a memory-based failover, the same FortiGate member waits at least 20 minutes before another memory-based failover can occur. Other cluster members can still initiate a memory-based failover if they meet their criteria.
- Each member in the cluster checks its memory usage every 2 seconds.

If during the primary election, the memory usage of all members is 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.

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

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, virtual cluster ID (if enabled), and interface index number are 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.

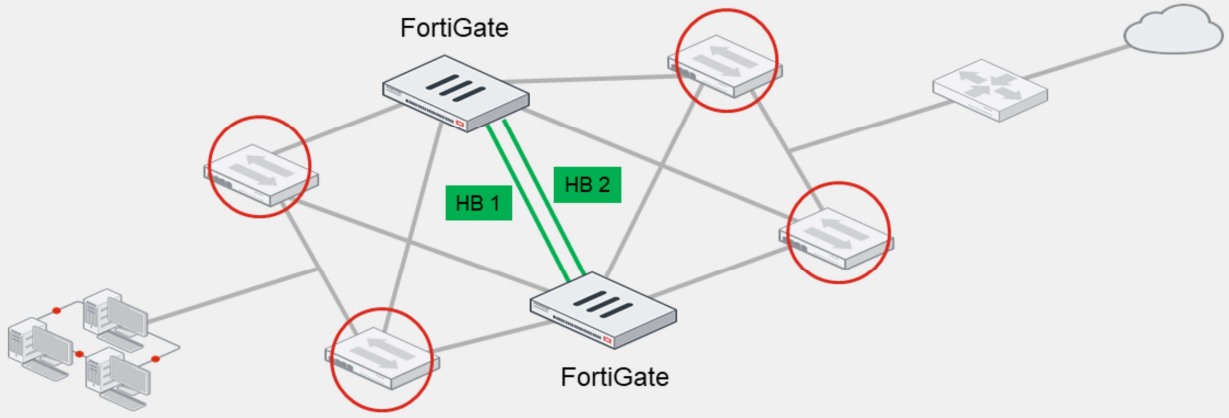
Through the heartbeats, the primary informs all secondary devices about the assigned virtual MAC address. Upon failover, a secondary adopts the same virtual MAC addresses for the equivalent interfaces.

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.

Full Mesh HA

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

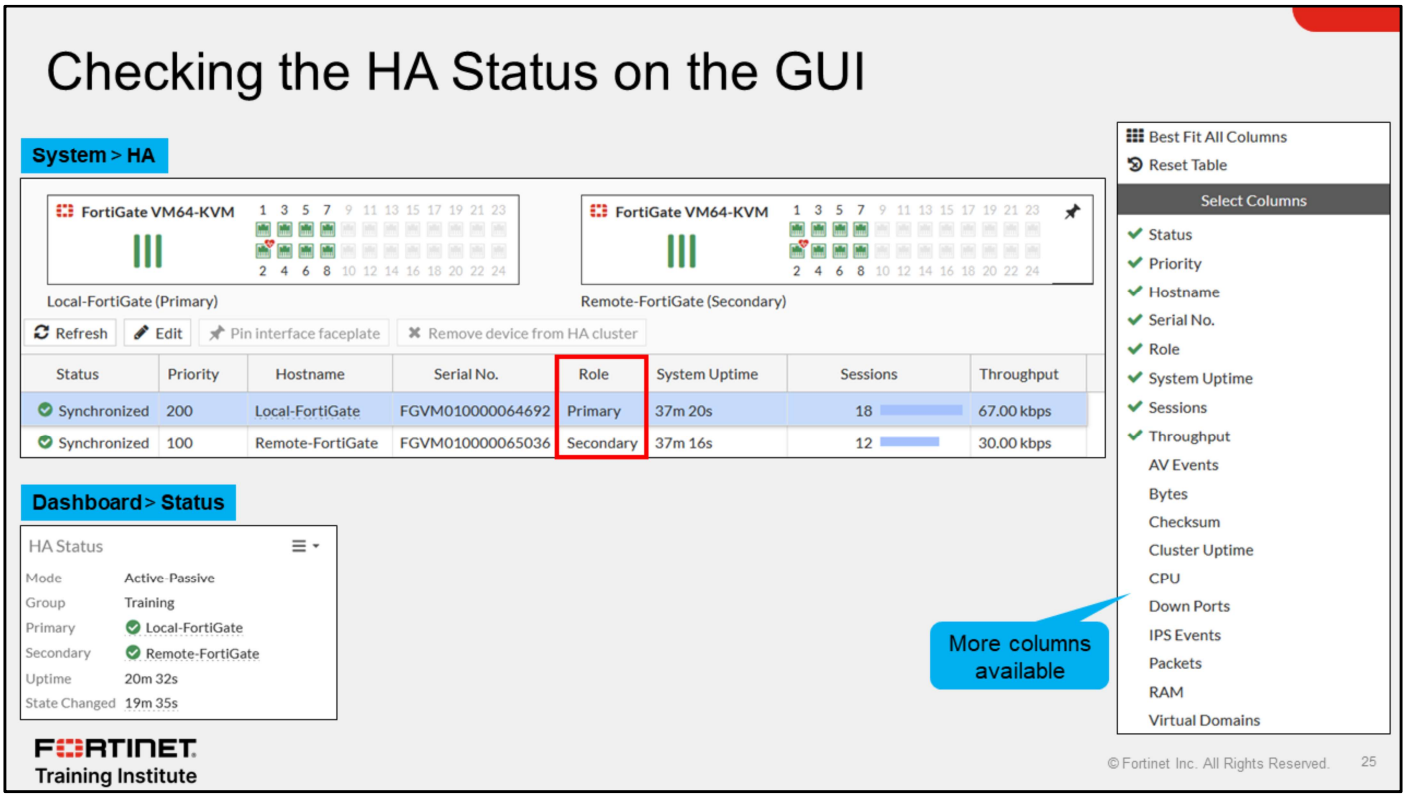


FORTINET Training Institute

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.

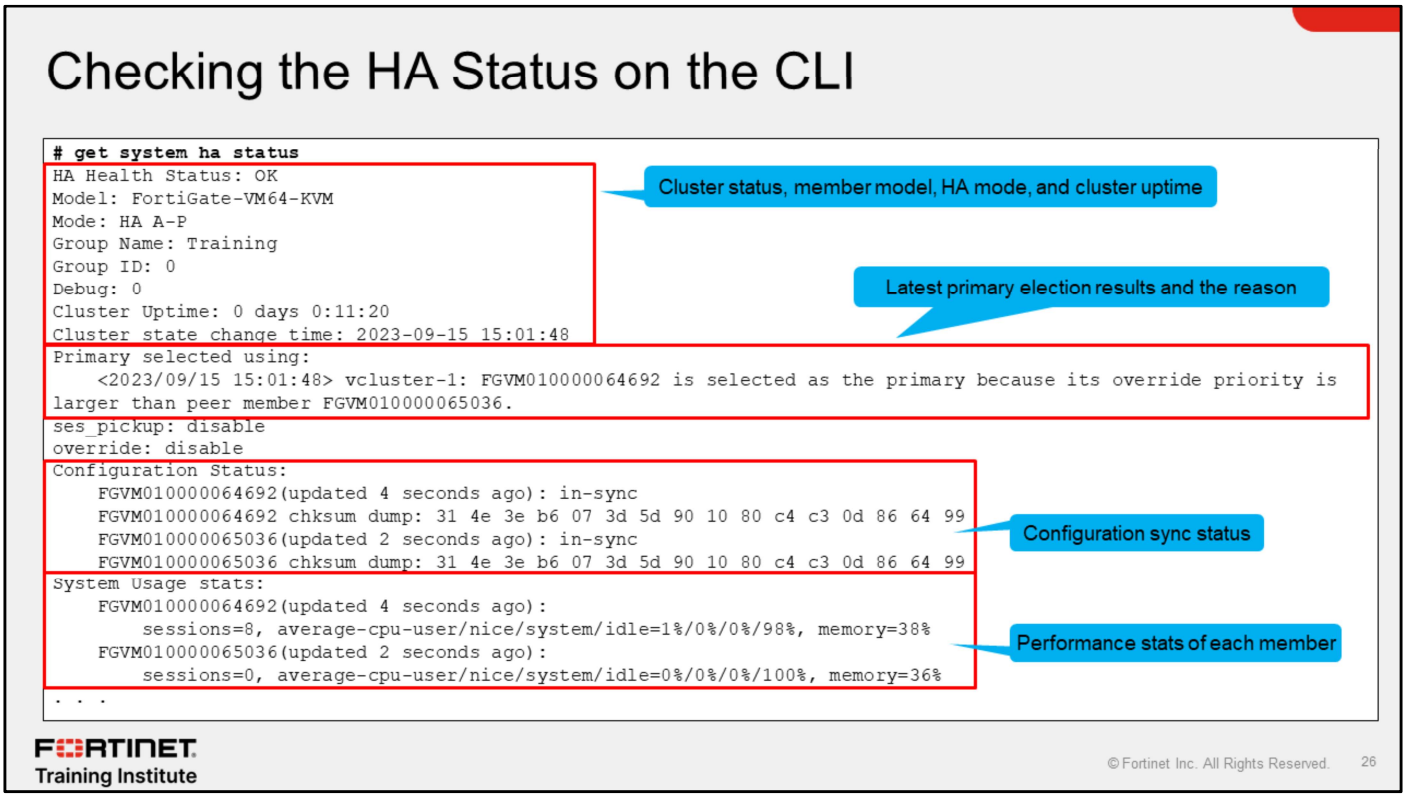
To achieve redundancy with adjacent switches, you must deploy redundant or LAG interfaces. If you use redundant interfaces, only one interface remains active. This prevents a Layer 2 loop and a standard switch should suffice. However, if you want to use LAG interfaces, then you must ensure that the switch 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.



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, active sessions, and more.

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.

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.

Next, you can see the latest primary election events, the result, and the reason.

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.

Checking the HA Status on the CLI (Contd)

```
. . .
HBDEV stats:
    FGVM010000064692(updated 3 seconds ago):
        port2: physical/10000full, up, rx-bytes/packets/dropped/errors=4029545/11074/0/0, tx=5360086/11576/0/0
    FGVM010000065036(updated 1 seconds ago):
        port2: physical/10000full, up, rx-bytes/packets/dropped/errors=5377151/11684/0/0, tx=4023101/10991/0/0
MONDEV stats:
    FGVM010000064692(updated 3 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=42166263/29629/0/0, tx=570354/5486/0/0
    FGVM010000065036(updated 1 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=14470/141/0/0, tx=0/0/0/0
PINGSVR stats:
    FGVM010000064692(updated 3 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=42166263/29629/0/0, tx=570354/5486/0/0
        pingsvr: state=up(since 2023/09/15 15:29:58), server=8.8.8.8, ha_prio=5
    FGVM010000065036(updated 1 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=14470/141/0/0, tx=0/0/0/0
        pingsvr: state=N/A(since 2023/09/15 15:30:00), server=8.8.8.8, ha_prio=5
Primary     : Local-FortiGate , FGVM010000064692, HA cluster index = 1
Secondary   : Remote-FortiGate, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

Heartbeat, monitored, and remote link interfaces status

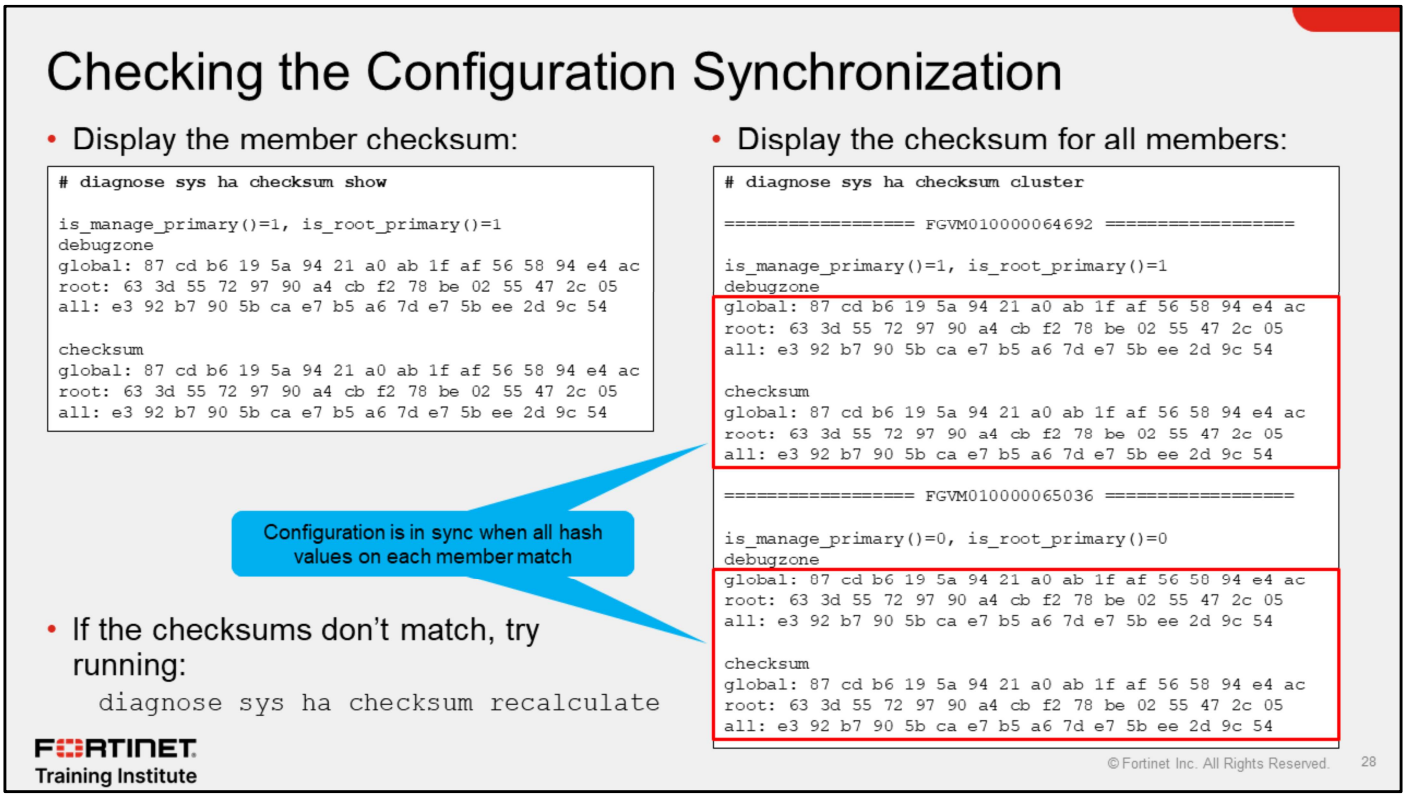
Member role, host name, serial number, and ID

FORTINET Training Institute

This slide shows the second part of the example output that the `get 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, 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.

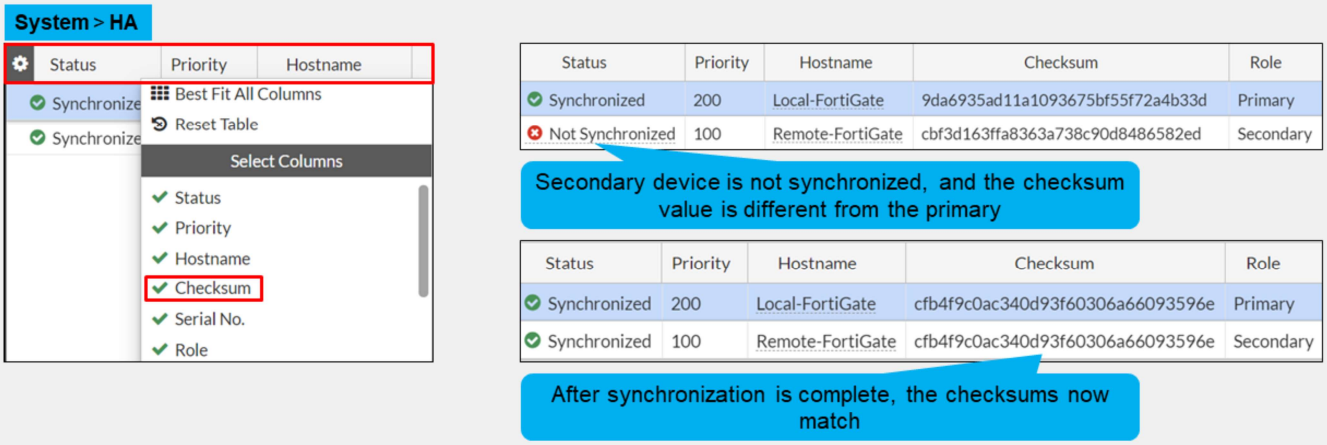
To calculate checksums, FortiGate computes a hash value for each of the following configuration scopes:

- `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.

Checking the Configuration Synchronization (GUI)

- Right-click the table header row and select the **Checksum** column
- After enabling it, you can compare checksums for members in the HA cluster



FORTINET Training Institute

You can also view FortiGate device checksums in the **System** > **HA** interface. To enable the column, right-click on the top header row, and then select the **Checksum** column to display.

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.
<0>     Subsidiary unit FGVM010000065036
```

FORTINET Training Institute

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.

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

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.

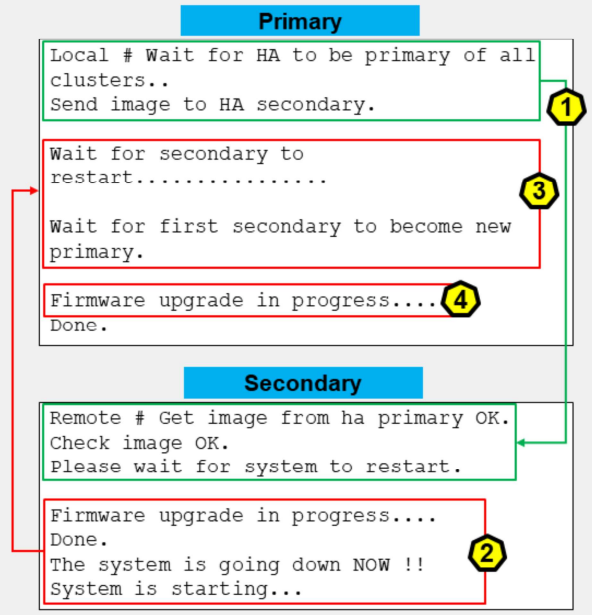
Firmware Upgrade

- Use the GUI or CLI
- Uninterruptible upgrade is enabled by default:

```
config system ha
    set upgrade-mode simultaneous | uninterruptible |
     local-only | secondary-only
end
```

- Upgrade process (uninterruptible upgrade):
  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



FORTINET Training Institute

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, uninterruptible upgrade is enabled by default, so that secondary members in a cluster are upgraded first. 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 expedite the process, you can enable simultaneous upgrade. However, this option will have a service impact. The local-only option allows you to upgrade only the local device. The secondary-only option allows you to upgrade the secondary members, but the primary FortiGate will not be upgraded. The local-only and secondary-only options are only meant to temporarily put the cluster on different firmware versions—to provide more control on which member to upgrade, and when. Configurations will not synchronize while the cluster has different firmware versions.

Knowledge Check

1. What is the default order criteria (override disabled) for selecting the primary device in an HA cluster?

✓ A. Connected monitored ports > HA uptime > priority > serial number
B. Priority > HA uptime > connected monitored ports > serial number

2. Which session type can you synchronize in an HA cluster?

A. BGP peerings
✓ B. Non-proxy TCP sessions

3. Which statement about the firmware upgrade process in an HA cluster is true?

✓ A. You upload the new firmware to the primary FortiGate only.
B. The members do not reboot.

Review

- ✓ Configure HA (FGCP)
- ✓ Configure HA failover
- ✓ Configure HA session synchronization
- ✓ Configure the HA management interface
- ✓ Verify the normal operation of an HA cluster
- ✓ Upgrade the HA cluster

FORTINET Training Institute

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.