Contents

Introduction ........................................................................................................... 9
Revision history ....................................................................................................... 10
This document ........................................................................................................ 10
New FortiOS v3.0 HA features ............................................................................... 11
  Mixing newer and older FortiGate-100A and 200A modules cannot form HA clusters ................................................................. 11
  New HA heartbeat failure SNMP trap ................................................................ 12
  FortiGate-5000 series base backplane interfaces used for data traffic .......... 12
  HA non-interrupting firmware upgrade ............................................................ 12
  New HA categories for alert email ..................................................................... 12
  HA status information displayed on cluster dashboard .................................... 12
  Virtual clustering .............................................................................................. 13
  Full mesh HA .................................................................................................. 13
  Changes to the FGCP ....................................................................................... 13
  HA configuration changes ................................................................................ 14
  Override not enabled by default ....................................................................... 16
  New cluster members list .................................................................................. 16
  Disconnecting FortiGate units from a cluster .................................................. 17
  Downloading a debug log .................................................................................. 17
FortiGate HA terminology ................................................................................... 17
Fortinet documentation ....................................................................................... 21
  Fortinet Tools and Documentation CD .............................................................. 21
  Fortinet Knowledge Center ............................................................................... 21
  Comments on Fortinet technical documentation ........................................... 21
Customer service and technical support ............................................................ 21
FortiGate Clustering Protocol (FGCP) ............................................................... 23
  FGCP heartbeat ................................................................................................ 23
  HA Telnet sessions ........................................................................................... 24
Heartbeat interfaces ............................................................................................ 24
Primary unit selection .......................................................................................... 25
  Connected monitored interfaces ..................................................................... 27
  Age ................................................................................................................... 27
  Device priority ................................................................................................ 28
  FortiGate unit serial number .......................................................................... 28
  Controlling primary unit selection by changing the device priority ............... 28
  Using override to make sure the primary unit always has the highest device priority ............................................................... 29
  Configuration changes made to an HA cluster can be lost if override is enabled ........................................................................... 29
  Override and disconnecting a unit from a cluster ......................................... 30
## Contents

- **Cluster virtual MAC addresses** .............................................................. 31
  - Changing the HA group ID .............................................................. 31
  - How the virtual MAC address is determined .................................. 32
  - Example virtual MAC addresses .................................................. 32
  - Virtual MAC address conflicts .................................................... 33
- **Device and link failover** ........................................................................ 34
  - Device failover .............................................................................. 35
  - Link failover .................................................................................. 35
  - Multiple link failures ..................................................................... 36
  - Failover and attached network equipment ...................................... 36
- **HA configuration synchronization** .......................................................... 36
  - Incremental synchronization .......................................................... 36
  - Periodic synchronization ................................................................ 38
- **HA operating modes** ............................................................................ 39
  - Active-passive HA (failover protection) .......................................... 39
  - Active-active HA (load balancing and failover protection) ............... 40
- **FortiGate HA compatibility with PPP protocols** .................................. 40
- **Upgrading HA cluster firmware** ............................................................ 40
  - Changing how a cluster processes firmware upgrades .................. 41
- **Viewing and managing log messages for individual cluster units** ......... 41
  - About HA event log messages ...................................................... 42
- **Disconnecting a unit from a cluster** ...................................................... 43
- **HA and redundant interfaces** ............................................................... 44
  - HA interface monitoring, link failover, and redundant interfaces ...... 45
  - HA MAC addresses and redundant interfaces ................................ 45
  - Connecting multiple redundant interfaces to one switch while operating in active-passive HA mode ...................................................... 46
  - Connecting multiple redundant interfaces to one switch while operating in active-active HA mode ...................................................... 46
- **HA and 802.3 aggregate interfaces** .......................................................... 46
  - HA interface monitoring, link failover, and 802.3ad aggregation ...... 47
  - HA MAC addresses and 802.3ad aggregation ................................ 47
  - HA active-passive mode and LACP ................................................ 47
- **HA and dynamic routing failover** ............................................................ 48
  - The problem with dynamic routing and HA .................................... 48
  - The FortiOS HA resolution ............................................................... 48
- **Configuration reference** .......................................................................... 49
  - Configuring HA web-based manager options (virtual clustering not enabled) .............................................................. 49
  - Configuring HA web-based manager options for virtual clustering..... 50
HA web-based manager options ................................................................. 51
  Mode ........................................................................................................... 52
  Device Priority .......................................................................................... 52
  Group Name ............................................................................................... 53
  Password .................................................................................................... 53
  Enable Session pickup ............................................................................. 53
  Port Monitor ............................................................................................... 54
  Heartbeat Interface .................................................................................... 54
  VDOM partitioning ................................................................................... 57

Changing subordinate unit host name and device priority ....................... 57

config system ha (CLI command) ............................................................... 58
  Command syntax pattern ........................................................................... 58
  Examples .................................................................................................... 67

get system ha status (CLI command) ......................................................... 69
  Command syntax pattern ........................................................................... 69
  Examples .................................................................................................... 71

execute ha disconnect (CLI command) ...................................................... 74
  Command syntax ....................................................................................... 74
  Example ...................................................................................................... 74

execute ha manage (CLI command) ......................................................... 75
  Command syntax ....................................................................................... 75
  Examples .................................................................................................... 75

execute ha synchronize (CLI command) .................................................... 76
  Command syntax ....................................................................................... 76

Configuring and connecting HA clusters ................................................. 77
  About the procedures in this chapter ....................................................... 77

Configuring and connecting an HA cluster .............................................. 77
  Configuring a FortiGate unit for HA operation ....................................... 78
  Connecting a FortiGate HA cluster ......................................................... 79

Basic NAT/Route mode installation ........................................................... 80
  Example NAT/Route mode HA network topology .................................... 80
  Configuring a NAT/Route mode active-active HA cluster ..................... 81

Basic Transparent mode installation ......................................................... 88
  Example Transparent mode HA network topology .................................. 88
  Configuring a Transparent mode active-active HA cluster .................... 89

Converting a standalone FortiGate unit to a cluster .................................. 97

Adding a new unit to an operating cluster ................................................. 98

HA between two FortiGate-5020 chassis .................................................. 99
  Network configuration .............................................................................. 100
  Changing the HA heartbeat interface configuration ................................ 100
Operating a cluster .......................................................... 137

Operating a cluster .......................................................... 137
  About HA configuration synchronization .......................... 138
  Cluster members list overview ....................................... 139
  Viewing HA statistics ..................................................... 140
  Changing the HA configuration of an operating cluster ....... 141
  Changing subordinate unit host name and device priority .... 142
  Upgrading HA cluster firmware ..................................... 143
  Changing how the cluster processes firmware upgrades ..... 143
  Adding a new unit to a functioning cluster ....................... 144
  Viewing and managing log messages for individual cluster units 144
  Monitoring cluster units for failover ............................... 145
  Managing individual cluster units ................................. 146
  Disconnecting a cluster unit from a cluster ..................... 146
  Adding a disconnected FortiGate unit back to its cluster .... 147
  Cluster communication with RADIUS and LDAP servers ...... 148

HA clusters and FortiGuard services .................................... 148
  The FDN and active-passive clusters ............................. 149
  The FDN and active-active clusters .............................. 149
  The FDN and virtual clustering ..................................... 149

Clusters and logging .......................................................... 150
  Viewing and managing logs for an HA cluster ................. 150
  HA log messages ......................................................... 151
  Admin log messages .................................................... 153
  Example log message scenarios .................................... 154

Clusters and SNMP .............................................................. 155

Clusters and quarantine .......................................................... 156
  Viewing and managing quarantined files for an HA cluster .......................... 156

Advanced HA configuration options ........................................ 157
  Controlling how HA synchronizes routing table updates ....... 157
  Modifying heartbeat timing .......................................... 158
  Enabling or disabling HA heartbeat encryption and authentication .. 159
  Setting the number of gratuitous arps sent by a primary unit .. 160

Managing a FortiGate virtual clustering configuration ............... 160
  Virtual cluster members list overview ........................... 161
  Changing the HA configuration of an operating virtual cluster 164

Index .................................................................................. 167
Introduction

FortiGate high availability (HA) provides a solution for two key requirements of critical enterprise networking components: enhanced reliability and increased performance.

FortiGate HA is implemented by configuring two or more FortiGate units to operate as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewalling, VPN, IPS, virus scanning, web filtering, and spam filtering services.

**Figure 1: HA cluster consisting of two FortiGate-3600 units**

Inside the cluster the individual FortiGate units are called cluster units. These cluster units share state and configuration information. If one cluster unit fails, the other units in the cluster automatically replace that unit, taking over the work that the failed unit was doing. After the failure, the cluster continues to process network traffic and provide normal FortiGate services with virtually no interruption.

Every FortiGate cluster contains one primary unit (also called the master unit) and one or more subordinate units (also called slave or backup units). The primary unit controls how the cluster operates. The roles that the primary and subordinate units play in the cluster depend on the mode in which the cluster operates. See “Active-passive HA (failover protection)” on page 39 and “Active-active HA (load balancing and failover protection)” on page 40.
The ability of an HA cluster to continue providing firewall services after a failure is called failover. FortiGate HA failover means that your network does not have to rely on one FortiGate unit to continue functioning. You can install additional units and form an HA cluster. Other units in the cluster will take over if one of the units fails.

A second HA feature, called load balancing, can be used to increase performance. A cluster of FortiGate units can increase overall network performance by sharing the load of processing network traffic and providing security services. The cluster appears to your network to be a single device, adding increased performance without changing your network configuration.

Virtual clustering extends HA features to provide failover protection and load balancing for a FortiGate operating with virtual domains. A virtual cluster consists of a cluster of two FortiGate units operating with virtual domains. Traffic on different virtual domains can be load balanced between the cluster units.

FortiGate models 800 and above can use redundant interfaces to create a cluster configuration called full mesh HA. Full mesh HA is a method of reducing the number of single points of failure on a network that includes an HA cluster.

This chapter contains the following sections:

- Revision history
- This document
- New FortiOS v3.0 HA features
- FortiGate HA terminology
- Fortinet documentation
- Customer service and technical support

**Revision history**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-30003-0112-20061020</td>
<td>First Release for MR3.</td>
</tr>
</tbody>
</table>

**This document**

This document contains detailed information about how FortiGate HA and the FortiGate Clustering Protocol (FGCP) works. This document all describes all FortiGate HA configuration options, contains detailed configuration examples, and describes how to operate FortiGate clusters. Future versions of this document will include more and more configuration examples and more information about HA functionality.

This document contains the following chapters:

- **Introduction** (this chapter) briefly introduces HA, describes new v2.80 HA features, and defines the HA-related terminology used in this document. This chapter also lists new FortiOS v3.0 HA features.
Introduction

Mixing newer and older FortiGate-100A and 200A modules cannot form HA clusters

- FortiGate Clustering Protocol (FGCP) describes the FGCP clustering protocol and its features, including the HA heartbeat, primary unit selection, device and link failover, and introduces the active-passive and active-active HA modes. This chapter also provides overviews of FortiGate HA features such as virtual clustering, full mesh HA, and HA and 802.3 aggregate interfaces, and HA and routing.
- Configuration reference describes all HA-related web-based manager and command line interface (CLI) configuration settings.
- Configuring and connecting HA clusters describes configuring HA clusters and contains HA clustering configuration examples.
- Configuring and connecting virtual clusters describes configuring HA virtual clusters and contains virtual clustering configuration examples.
- Configuring and operating FortiGate full mesh HA describes configuring FortiGate Full mesh HA and contains a full mesh HA configuration example.
- Operating a cluster describes how to operate a cluster and includes detailed information about how various FortiGate systems operate differently in a cluster.

New FortiOS v3.0 HA features

This section lists and describes new FortiOS v3.0 HA features as well as HA features that have changed between FortiOS v2.80 and FortiOS v3.0.

- Mixing newer and older FortiGate-100A and 200A modules cannot form HA clusters
- New HA heartbeat failure SNMP trap
- FortiGate-5000 series base backplane interfaces used for data traffic
- HA non-interrupting firmware upgrade
- New HA categories for alert email
- HA status information displayed on cluster dashboard
- Virtual clustering
- Full mesh HA
- Changes to the FGCP
- HA configuration changes
- Override not enabled by default
- New cluster members list
- Disconnecting FortiGate units from a cluster
- Downloading a debug log

Mixing newer and older FortiGate-100A and 200A modules cannot form HA clusters

Newer models of the FortiGate-100A and the FortiGate-200A contain more advanced switch hardware. Because of this hardware change, you cannot create a FortiGate HA cluster that includes both the old and new hardware versions of these FortiGate units. You can tell whether you have an older or newer version of the FortiGate-100A or 200A by the serial number of the unit:
New HA heartbeat failure SNMP trap

FortiOS v3.0 MR3 adds a new FortiGate SNMP HA heartbeat failure trap. The SNMP agent now sends a trap when HA heartbeat packets are not received on the active HA heartbeat interface and the cluster fails over to using the next HA heartbeat interface.

New HA heartbeat failure SNMP trap

FortiGate-5000 series base backplane interfaces used for data traffic

For FortiOS v3.0 MR2 and previous releases the FortiGate-5000 series module backplane interfaces could only be used for HA heartbeat traffic. These interfaces were named port9 and port10 and were only visible from the HA web-based manager page and the `config system ha` CLI command.

In FortiOS v3.0 MR3, the backplane interfaces are still the default HA heartbeat interfaces. However, you can now also configure the backplane interfaces as regular firewall interfaces and use them to route traffic through the FortiGate-5000 series chassis backplane between FortiGate-5000 series modules. You can also use HA port monitoring to monitor backplane interfaces just as you would any other FortiGate interface.

As with any other interface you can mix HA heartbeat traffic and data traffic on the same backplane interface. However, this configuration is not recommended because HA heartbeat traffic can use a significant amount of bandwidth.

HA non-interrupting firmware upgrade

FortiOS v3.0 MR2 supports upgrading the FortiOS firmware running on an HA cluster without interrupting communication through the cluster. The non-interrupting upgrade process uses the steps described in “Upgrading HA cluster firmware” on page 40 to upgrade the cluster firmware.

New HA categories for alert email

You can go to Log & Report > Log Config > Alert E-mail to configure the cluster to send alert email for HA status changes. HA status changes occur when a cluster unit switches between operating as a primary and operating as a subordinate unit. Configuring alert e-mail HA status change messages means that the cluster will send alert email if status change, which may indicate a failover occurs.

HA status information displayed on cluster dashboard

The cluster web-based manager dashboard displays the HA status, the cluster name and the host name and serial number for the primary unit (Master) and all subordinate units (Slave) in the cluster. You can select Configure beside the HA status to go to System > Config > HA and change HA options. The dashboard also displays a cluster unit front panel illustration.

- FortiGate-100A units starting with serial number FG100A2905500001 have the advanced switch hardware. To create a cluster of FortiGate-100A units they must all have a serial number higher or lower than FG100A2905500001.
- FortiGate-200A units starting with serial number FG200A2905500001 have the advanced switch hardware. To create a cluster of FortiGate-200A units they must all have a serial number higher or lower than FG200A2905500001.
If virtual domains are enabled, the cluster web-based manager dashboard displays the HA status, and the host name and serial number of both of the units in the virtual cluster. You can select Configure beside the HA status to go to System > Config > HA and change HA options. The display also includes the cluster name and the role of each cluster unit in virtual cluster 1 and virtual cluster 2.

Virtual clustering

If virtual domains are enabled for a FortiOS v3.0 cluster, you can use FortiOS v3.0 virtual clustering to provide failover protection and load sharing. Virtual clustering is supported for a cluster of two FortiGate units.

Full mesh HA

FortiGate models 800 and above can use redundant interfaces to create a cluster configuration called full mesh HA. Full mesh HA is a method of reducing the number of single points of failure on a network that includes an HA cluster.

Changes to the FGCP

The following changes have been made to the FortiOS v3.0 version of the FortiGate Clustering Protocol (FGCP).

How heartbeat interfaces operate

In FortiOS v3.0 you must select one or more FortiGate interfaces to be heartbeat interfaces. Unlike FortiOS v2.80, you do not set the priority of the heartbeat interfaces.
HA heartbeat hello packets are constantly sent by all of the configured heartbeat interfaces. Using these hello packets, each cluster unit confirms that the other cluster units are still operating. The FGCP selects one of the heartbeat interfaces to be used for communication between the cluster units. The FCGP selects the heartbeat interface to be used based on the linkfail states of the heartbeat interfaces and on the interface index.

The web-based manager lists the FortiGate unit interfaces in alphabetical order. This order corresponds to the interface index order. The selected heartbeat interface that is highest in the interface list (or first in alphabetical order) is used for heartbeat communication between cluster units. If this interface fails or becomes disconnected, the interface that is next highest in the list (or next in alphabetical order) handles all HA heartbeat communication. The heartbeat interface that is higher in the interface list resumes processing all HA heartbeat communication if it becomes connected again.

How link failover works

Configuring the cluster for link failover has been simplified for FortiOS v3.0. In FortiOS v3.0 you select FortiGate interfaces to monitor for link failure. Unlike FortiOS v2.80, you do not set priorities for monitored interfaces.

In FortiOS v3.0, if a monitored interface fails or becomes disconnected, the cluster renegotiates and may select a new primary unit. The new primary unit will be the unit with the fewest failed monitored interfaces. In this way the cluster maintains as many network connections as possible to the primary unit.

Link failover takes precedence over device priority. The cluster unit with the fewest failed monitored interfaces becomes the primary unit, even if other units in the cluster have higher device priorities.

Changes to cluster virtual MAC addresses

The FortiOS v3.0 FGCP assigns a different virtual MAC address to each primary unit interface. You can change the virtual MAC addresses by changing the cluster group id from the FortiGate CLI. For more information, see “Cluster virtual MAC addresses” on page 31.

HA configuration changes

A number of changes have been made to the FortiOS v3.0 web-based manager and CLI HA configuration options. Configuring HA from the web-based manager has been simplified for FortiOS v3.0. For example, the active-active load balancing schedule has been removed and is now a CLI-only option. Also the FortiOS v2.80 requirement to set heartbeat device priorities and monitor priorities have been replaced with check boxes for selecting heartbeat interfaces and interfaces to monitor.

Table 2 lists the FortiOS v3.0 web-based manager configuration changes.
Table 2: FortiOS v3.0 HA web-based manager configuration changes

<table>
<thead>
<tr>
<th>Configuration option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>In FortiOS v3.0 you select Active-Passive or Active-Active mode to operate in HA mode. In FortiOS v2.80 you selected High Availability and then selected the HA mode in two steps.</td>
</tr>
<tr>
<td>Device Priority</td>
<td>The FortiOS v2.80 Unit Priority option has been renamed Device Priority for FortiOS v3.0.</td>
</tr>
<tr>
<td>Group ID</td>
<td>The FortiOS v2.80 Group ID option can only be configured from the CLI for FortiOS v3.0.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Group Name is a new FortiOS v3.0 option. The Group Name identifies the cluster.</td>
</tr>
<tr>
<td>Override Master</td>
<td>The FortiOS v2.80 Override Master option can only be configured from the CLI for FortiOS v3.0. See &quot;Override not enabled by default&quot; on page 16.</td>
</tr>
<tr>
<td>Enable Session Pickup</td>
<td>You can enable session pickup for FortiOS v3.0. In FortiOS v2.80 you could not configure session pickup. Session pickup was always on. Enable session pickup so that if the primary unit fails, all sessions are picked up by the new primary unit. In most cases you would want to enable session pickup. However, if session pickup is not a requirement of your HA installation, you can disable this option to save processing resources and reduce the network bandwidth used by HA session synchronization.</td>
</tr>
<tr>
<td>Schedule</td>
<td>The FortiOS v2.80 schedule option for Active-active clusters has been removed from the FortiOS v3.0 web-based manager. In FortiOS v3.0 you can change the active-active schedule from the CLI. The default schedule is round-robin.</td>
</tr>
<tr>
<td>Port Monitor</td>
<td>The FortiOS v2.80 monitor priorities feature has been renamed Port Monitor and simplified for FortiOS v3.0. You configure Port Monitor by selecting FortiGate interfaces to monitor. The concept of priorities for monitored interfaces has been removed from FortiOS v3.0. See &quot;How link failover works&quot; on page 14 for more information. In addition you can create separate port monitor configurations for each virtual cluster.</td>
</tr>
<tr>
<td>Heartbeat Interface</td>
<td>The FortiOS v2.80 priorities of heartbeat device features has been renamed Heartbeat Interface and simplified for FortiOS v3.0. You configure Heartbeat Interface by selecting the FortiGate interfaces to be used for heartbeat communications. The concept of priorities for heartbeat interfaces has been removed from FortiOS v3.0. See &quot;How heartbeat interfaces operate&quot; on page 13 for more information.</td>
</tr>
<tr>
<td>Virtual Cluster 1</td>
<td>New FortiOS v3.0 virtual clustering configuration options.</td>
</tr>
<tr>
<td>Virtual Cluster 2</td>
<td></td>
</tr>
<tr>
<td>VDOM Partitioning</td>
<td></td>
</tr>
</tbody>
</table>

Table 3 lists the FortiOS v3.0 web-based manager configuration changes.
Override not enabled by default

Early maintenance releases of FortiOS v3.0 enabled the override keyword by default. As of MR2 override is disabled by default.

New cluster members list

From the web-based manager of an operating cluster, you can go to System > Config > HA to view the cluster members list. The FortiOS v3.0 cluster members list includes status information for each of the cluster units. From the cluster members list you can also:

- View HA statistics (similar to the FortiOS v2.80 cluster members list).
- View and optionally change the HA configuration of the cluster.
- View and optionally change the device priority of individual cluster units.
- Disconnect a cluster unit from a cluster.
- Download the debug log for any cluster unit.

Because override master is enabled by default, when you change the Device Priority of the primary unit or any subordinate unit, the cluster renegotiates and the unit with the highest device priority becomes the primary unit.

Figure 4: Example FortiGate-5001SX cluster members list

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>synch-config</td>
<td>New FortiOS v3.0 keyword for enabling or disabling automatic synchronization of primary unit configuration changes to all cluster units.</td>
</tr>
<tr>
<td>uninterruptable-upgrade</td>
<td>New FortiOS v3.0 keyword for enabling or disabling non-interrupting firmware upgrading. See “Upgrading HA cluster firmware” on page 40.</td>
</tr>
<tr>
<td>vcluster-id</td>
<td>New FortiOS v3.0 virtual clustering configuration options.</td>
</tr>
<tr>
<td>vdom</td>
<td></td>
</tr>
<tr>
<td>vcluster2</td>
<td></td>
</tr>
</tbody>
</table>
Disconnecting FortiGate units from a cluster

From the cluster members list, or by using the new `execute ha disconnect` CLI command you can disconnect a FortiGate unit from a functioning cluster. You can disconnect any unit from the cluster even the primary unit.

You might want to disconnect a unit from a functioning cluster if you need this FortiGate unit for another purpose (for example, as a firewall for another network).

Disconnecting a cluster unit in this way does not affect the operation of the cluster. After the unit is disconnected the cluster responds as if the disconnected unit has failed.

For more information, see “Disconnecting a unit from a cluster” on page 43.

Downloading a debug log

From the FortiOS v3.0 cluster members list, you can download an encrypted debug log to a file for any cluster unit. You can send this debug log file to Fortinet Technical Support to help diagnose problems with the cluster or with individual cluster units.

FortiGate HA terminology

The following HA-specific terms are used in this document.

Cluster

A group of FortiGate units that act as a single virtual FortiGate unit to maintain connectivity even if one of the FortiGate units in the cluster fails.

Cluster unit

A FortiGate unit operating in a FortiGate HA cluster.

Device failover

A hardware or software problem that causes a FortiGate unit to stop processing network traffic. If one of the FortiGate units in a cluster fails, all functions, all established firewall connections, and all IPSec VPN sessions¹ are maintained by the other FortiGate units in the HA cluster.

Failover

A FortiGate unit taking over processing network traffic in place of another unit in the cluster that suffered a device failure or a link failure.

Failure

A hardware or software problem that causes a FortiGate unit or a monitored interface to stop processing network traffic.

¹HA does not provide session failover for PPPoE, DHCP, PPTP, and L2TP services.
FGCP
The FortiGate clustering protocol (FGCP) that specifies how the FortiGate units in a cluster communicate to keep the cluster operating.

Full mesh HA
FortiGate models 800 and above can use redundant interfaces to create a cluster configuration called full mesh HA. Full mesh HA is a method of removing single points of failure on a network that includes an HA cluster. Full mesh HA includes redundant connections between all network components. If any single component or any single connection fails, traffic switches to the redundant component or connection.

HA virtual MAC address
When operating in HA mode, all of the interfaces of the primary unit acquire the same HA virtual MAC address. All communications with the cluster must use this MAC address. The HA virtual MAC address is set according to the group ID.

Heartbeat
Also called FGCP heartbeat or HA heartbeat. The heartbeat constantly communicates HA status and synchronization information to make sure that the cluster is operating properly.

Heartbeat device
An ethernet network interface in a cluster that is used by the FGCP for heartbeat communications among cluster units.

Heartbeat failover
If an interface functioning as the heartbeat device fails, the heartbeat is transferred to another interface also configured as an HA heartbeat device.

Hello state
In the hello state a cluster unit has powered on in HA mode, is using HA heartbeat interfaces to send hello packets, and is listening on its heartbeat interfaces for hello packets from other FortiGate units. Hello state may appear in HA log messages.

High availability
The ability that a cluster has to maintain a connection when there is a device or link failure by having another unit in the cluster take over the connection, without any loss of connectivity. To achieve high availability, all FortiGate units in the cluster share session and configuration information.

Link failover
If a link failure causes an interface on the primary unit to stop processing network traffic, a cluster unit that has not experienced the same link failure becomes the new primary unit. All functions, all established firewall connections, and all IPSec VPN sessions fail over to the new primary unit.
Load balancing

Also known as active-active HA. All units in the cluster process network traffic. The FGCP employs a technique called unicast load balancing. The primary unit is associated with the cluster HA virtual MAC address and cluster IP address. The primary unit is the only cluster unit to receive packets sent to the cluster. The primary unit can process packets itself, or propagate them to subordinate units according to a load balancing schedule.

Monitored interface

An interface that is monitored by a cluster to make sure that it is connected and operating correctly. The cluster monitors the connectivity of this interface for all cluster units. If a monitored interface fails or becomes disconnected from its network, the cluster will compensate.

Primary unit

Also called the primary cluster unit, this cluster unit controls how the cluster operates. The primary unit sends hello packets to all cluster units to synchronize session information, synchronize the cluster configuration, and to synchronize the cluster routing table. The hello packets also confirm for the subordinate units that the primary unit is still functioning.

The primary unit also tracks the status of all subordinate units. When you start a management connection to a cluster, you connect to the primary unit.

In an active-passive cluster, the primary unit processes all network traffic. If a subordinate unit fails, the primary unit updates the cluster configuration database.

In an active-active cluster, the primary unit receives all network traffic and redirects this traffic to subordinate units. If a subordinate unit fails, the primary unit updates the cluster status and redistributes load balanced traffic to other subordinate units in the cluster.

The FortiGate firmware uses the term master to refer to the primary unit.

Session pickup

If you enable session pickup for a cluster, if the primary unit fails or a subordinate unit in an active-active cluster fails, all communication sessions with the cluster are maintained or picked up by the cluster after the cluster negotiates to select a new primary unit.

In most cases you would want to enable session pickup. However, if session pickup is not a requirement of your HA installation, you can disable this option to save processing resources and reduce the network bandwidth used by HA session synchronization.

Standby state

A subordinate unit in an active-passive HA cluster operates in the standby state. In a virtual cluster, a subordinate virtual domain also operates in the standby state. The standby state is actually a hot-standby state because the subordinate unit or subordinate virtual domain is not processing traffic but is monitoring the primary unit session table to take the place of the primary unit or primary virtual domain if a failure occurs.

In an active-active cluster all cluster units operate in a work state.
When standby state appears in HA log messages this usually means that a cluster unit has become a subordinate unit in an active-passive cluster or that a virtual domain has become a subordinate virtual domain.

**State synchronization**
The part of the FGCP that maintains connections after failover.

**Subordinate unit**
Also called the subordinate cluster unit, each cluster contains one or more cluster units that are not functioning as the primary unit. Subordinate units are always waiting to become the primary unit. If a subordinate unit does not receive hello packets from the primary unit, it attempts to become the primary unit.

In an active-active cluster, subordinate units keep track of cluster connections, keep their configurations and routing tables synchronized with the primary unit, and process network traffic assigned to them by the primary unit. In an active-passive cluster, subordinate units do not process network traffic. However, active-passive subordinate units do keep track of cluster connections and do keep their configurations and routing tables synchronized with the primary unit.

The FortiGate firmware uses the terms slave and subsidiary unit to refer to a subordinate unit.

**Virtual clustering**
Virtual clustering is an extension of the FGCP for FortiGate units operating with virtual domains. Virtual clustering operates in active-passive mode to provide failover protection between two instances of a virtual domain operating on two different cluster units. By distributing virtual domain processing between the two cluster units you can also configure virtual clustering to provide load balancing between the cluster units.

Virtual clustering operates on two (and only two) FortiGate units with virtual domains enabled. Each virtual domain creates its own cluster. All traffic to and from the virtual domain stays within the virtual domain and is processed by the virtual domain. One cluster unit is the primary unit for each virtual domain and the other cluster unit is the subordinate unit for each virtual domain. The primary unit processes all traffic for the virtual domain. The subordinate unit does not process traffic for the virtual domain.

**Work state**
The primary unit in an active-passive HA cluster, a primary virtual domain in a virtual cluster, and all cluster units in an active-active cluster operate in the work state. A cluster unit operating in the work state processes traffic, monitors the status of the other cluster units, and tracks the session table of the cluster.

When work state appears in HA log messages this usually means that a cluster unit has become the primary unit or that a virtual domain has become a primary virtual domain.
Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com.

Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at http://docs.forticare.com.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.
FortiGate Clustering Protocol (FGCP)

A FortiGate cluster consists of two or more FortiGate units configured for HA operation. Each FortiGate unit in a cluster is called a cluster unit. All cluster units must be the same FortiGate model with the same FortiOS v3.0 firmware build installed. All cluster units must also have the same hard disk configuration and be running in the same operating mode (NAT/Route mode or Transparent mode).

On startup, the cluster units use the FortiGate Clustering Protocol (FGCP) to find other FortiGate units configured for HA operation and create a cluster. During cluster operation, the FGCP shares communication and synchronization information among the cluster units. This communication and synchronization is called the FGCP heartbeat or the HA heartbeat. Often, this is shortened to just heartbeat.

The cluster uses the FGCP to select the primary unit, and to provide device and link failover. The FGCP also manages the two HA modes; active-passive or failover HA and active-active or load balancing HA.

This chapter contains basic descriptions of the following FortiGate HA clustering features:

- FGCP heartbeat
- Heartbeat interfaces
- Primary unit selection
- Cluster virtual MAC addresses
- Device and link failover
- HA configuration synchronization
- HA operating modes
- FortiGate HA compatibility with PPP protocols
- Upgrading HA cluster firmware
- Viewing and managing log messages for individual cluster units
- Disconnecting a unit from a cluster
- HA and redundant interfaces
- HA and 802.3 aggregate interfaces
- HA and dynamic routing failover

FGCP heartbeat

The FGCP heartbeat keeps cluster units communicating with each other. The heartbeat consists of hello packets that are sent at regular intervals by all heartbeat interfaces of each cluster unit. These hello packets describe the state of the cluster unit and are used by other cluster units to keep all cluster units synchronized.
The FGCP heartbeat operates on TCP port 702. The default time interval between HA heartbeats is 200 ms. The IP address used for the HA heartbeat (10.0.0.1, 10.0.0.2 etc) is an independent IP address not assigned to any FortiGate interface.

On startup, a FortiGate unit configured for HA operation broadcasts FGCP heartbeat hello packets from all ha heartbeat interfaces to find other FortiGate units configured to operate in HA mode. If two or more FortiGate units operating in HA mode connect with each other, they compare HA configurations (HA mode, HA password, and HA group ID). If the HA configurations match, the units negotiate to create a cluster.

While the cluster is operating, the FGCP heartbeat confirms that all cluster units are functioning normally. The heartbeat also reports the state of all cluster units, including the communication sessions that they are processing. A fully meshed link state database is shared by all cluster units. This link database tracks the cluster unit interfaces that are connected to networks and the cluster unit interfaces that are not.

The FGCP heartbeat also uses TCP port 23, the telnet port, to communicate statistics among cluster units, to synchronize the configuration, and to allow management connections to individual cluster units.

**HA Telnet sessions**

The FGCP heartbeat also uses telnet administrative sessions (on port 23) between cluster units, to communicate statistics, to synchronize the configuration, and to allow management connections to individual cluster units. These Telnet sessions are also visible from the System > Status > Session web-based manager page.

The administrator name for the HA administrative Telnet sessions is FGT_ha_admin. This administrator name appears in log messages generated by cluster units. For example: the following log message (with time stamp removed) shows that the primary unit has logged out of an administrative Telnet session with a subordinate unit.

```
device_id=FGT-602803030702 log_id=0104032007 type=event subtype=admin pri=information vd=root user=FGT_ha_admin ui=telnet(10.0.0.1) action=logout status=success reason=exit msg="User FGT_ha_admin Logs out from telnet(10.0.0.1)"
```

**Heartbeat interfaces**

A heartbeat interface is an Ethernet network interface in a cluster that is used by the FGCP for HA heartbeat communications between cluster units. You can configure multiple network interfaces to be heartbeat interfaces. The HA configuration in Figure 5 shows port4 and port5/ha configured as heartbeat devices.
By default, for all FortiGate models two interfaces are configured to be heartbeat interfaces. You can change the heartbeat interface configuration as required. For example you can select additional or different heartbeat interfaces. You can also select only one heartbeat interface. In all cases, the heartbeat interface that is highest in the heartbeat interface list is used for all HA heartbeat communication. If this interface fails or becomes disconnected, the selected heartbeat interface that is next highest in the list handles all heartbeat communication.

For the HA cluster to function correctly, you must select at least one heartbeat interface and this interface of all of the cluster units must be connected together. If heartbeat communication is interrupted and cannot failover to a second heartbeat interface, the cluster stops processing traffic.

For more details about configuring heartbeat interfaces including a table of default heartbeat interfaces for each FortiGate model, see “Heartbeat Interface” on page 54.

Primary unit selection

Once FortiGate units recognize that they can form a cluster, the cluster units negotiate to select a primary unit. Primary unit selection is done automatically by the cluster based on the factors shown in Figure 6 and described below.

Negotiation and primary unit selection also takes place if a primary unit fails (device failover) or if a primary unit interface fails (link failover). During a device or link failover, the cluster renegotiates to select a new primary unit using the same criteria as the initial negotiation. After the cluster selects the primary unit, all of the remaining units become subordinate units.
This section describes the factors that affect primary unit selection and how these factors are changed by the setting of the HA override keyword. The override keyword is disabled by default. When override is disabled the cluster may not renegotiate when events occur that may affect the primary unit selection. For example, changing a cluster unit device priority or adding a new cluster unit to a cluster will not cause the cluster to renegotiate when override is disabled.

Usually you would enable override only if you want one of the cluster units to always become the primary unit. If you enable override on a cluster unit you should also set the device priority for this unit higher than the device priority of the other units in the cluster. The override and device priority settings are not synchronized to all cluster units.

When override is enabled and device priority is set highest on the same unit, the cluster is more likely to renegotiate whenever an event occurs that may affect primary unit selection. For example:

- Adding a new unit to a cluster. If the new cluster unit has override enabled and has the highest device priority, the cluster renegotiates and the new cluster unit becomes the primary unit.
- Adding a new unit to a cluster. If primary unit has override enabled and has the highest device priority, and if override is not enabled on the new cluster unit the cluster does not renegotiate and the primary unit does not change.
- Changing the device priority of a cluster unit. If you set the device priority the highest on a cluster unit for which override is enabled the cluster renegotiates and the cluster unit with override enabled and the highest device priority becomes the primary unit.
- Changing the device priority of a cluster unit. If you set the device priority the highest on a cluster unit for which override is not enabled the does not renegotiate and the primary unit does not change.

A cluster always renegotiates if a device or link failure occurs, even if override is disabled.

In most cases you should keep override disabled to reduce how often the cluster negotiates. Frequent negotiations may cause frequent traffic interruptions.

However, you can enable override for one or more cluster units (the override setting is not synchronized to all cluster units) if you want more control over which cluster unit operates as the primary unit. Usually you would select a unit to always become the primary unit, enable override for this unit and set the device priority for this unit higher than for the other units.
**Connected monitored interfaces**

The cluster unit with the highest number of monitored interfaces that are connected to networks becomes the primary unit. Normally, when the cluster starts up, all cluster units have the same monitor priority, so monitored interfaces do not usually affect primary unit selection when the cluster first starts. However, during cluster operation, if a monitored interface fails, the cluster unit with the failed monitored interface cannot become the primary unit. If a monitored interface of the primary unit fails, the cluster renegotiates to select a new primary unit.

**Age**

The amount of time the unit has been in the cluster. Cluster units that have been operating in a cluster longer are more likely to become the primary unit. Units that are added to an already operating cluster are less likely to become the primary unit. Age has the effect of keeping the primary unit from changing when a new unit joins the cluster.

If *override* is enabled for one or more cluster units age is less important in primary unit selection because enabling *override* causes the cluster to negotiate more often. When the cluster renegotiates the age is reset to zero for all cluster units, so all units have the same age.
The **override** setting has the following affect when you add a new unit to a cluster:

- If **override** is enabled for one cluster unit and all other cluster units have the same device priority, the cluster renegotiates and the cluster unit with override enabled becomes the primary unit.
- If **override** is disabled for all cluster units and all of the cluster units have the same device priority, the new unit just joins the cluster as a subordinate unit and the primary unit does not change.
- If **override** is enabled for the new unit and the new unit has the highest device priority, the cluster renegotiates and the new unit becomes the primary unit.
- If **override** is disabled and the new unit has the highest device priority, the new unit just joins the cluster as a subordinate unit and the primary unit does not change.
- If **override** is enabled for all cluster units and all units have the same device priority, the cluster renegotiates and any cluster unit can become the primary unit.

### Device priority

Cluster units with a higher device priority are more likely to become the primary unit. By default, the device priority for all cluster units is 128. You can change the primary unit selection outcome by changing the device priority of the cluster units. The unit with the highest device priority always becomes the primary unit when the cluster starts up or negotiates.

If you increase the device priority of a subordinate unit in an operating cluster to be higher than all other unit device priorities, that subordinate unit becomes the primary unit if **override** is also enabled for that unit. If **override** is disabled, the subordinate unit with the higher priority will not become the primary unit until the cluster renegotiates.

### FortiGate unit serial number

The cluster unit with the highest serial number is more likely to become the primary unit. When first configuring the FortiGate units to be added to a cluster, if you do not change the device priority of any cluster unit, then the cluster unit with the highest serial number always becomes the primary unit.

Age does take precedence over serial number, so if a cluster unit takes longer to join a cluster for some reason (for example if one cluster unit is powered on after the others), that cluster unit will not become the primary unit because the other units have been in the cluster longer.

### Controlling primary unit selection by changing the device priority

You can change the device priority to control which FortiGate unit becomes the primary unit during cluster negotiation. All other factors that influence primary unit selection either cannot be configured (age and serial number) or are synchronized among all cluster units (interface or port monitoring). You can set a different device priority for each cluster unit. During negotiation, if all monitored interfaces are connected, and all cluster units are entering the cluster at the same time, the cluster with the highest device priority becomes the primary unit.
You can set a different device priority for each cluster unit to control the order in which cluster units become the primary unit when the primary unit fails. For example, if you have three units in a cluster you can set the device priorities as shown in Table 4. When the cluster starts up, cluster unit A becomes the primary unit because it has the highest device priority. If unit A fails, unit B becomes the primary unit because unit B has a higher device priority than unit C.

### Table 4: Example device priorities for a cluster of three FortiGate units

<table>
<thead>
<tr>
<th>Cluster unit</th>
<th>Unit priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>200</td>
</tr>
<tr>
<td>B</td>
<td>100</td>
</tr>
<tr>
<td>C</td>
<td>50</td>
</tr>
</tbody>
</table>

### Using override to make sure the primary unit always has the highest device priority

To configure one cluster unit to always become the primary unit you should set its device priority to be higher than the device priorities of the other cluster units and you should enable override for this cluster unit.

Using this configuration, when the cluster is operating normally the primary unit is always the unit with the highest device priority and with override enabled. If the primary unit fails the cluster renegotiates to select another cluster unit to be the primary unit. If the failed primary unit recovers, starts up again and rejoins the cluster, because override is enabled, the cluster renegotiates. Because the failed primary unit has the highest device priority it once again becomes the primary unit.

In the same situation with override disabled, because the age of the failed primary unit is lower than the age of the other cluster units, when the failed primary unit rejoins the cluster it does not become the primary unit. Instead, even though the failed primary unit may have the highest device priority it becomes a subordinate unit because its age is lower than the age of all the other cluster units.

### Configuration changes made to an HA cluster can be lost if override is enabled

Override is enabled by default for early FortiOS v3.0 maintenance releases. In FortiOS v2.80 FortiOS v3.0 MR2 and later override is disabled by default.

Configuration changes made to an HA cluster can be lost if HA override is enabled.

When override is enabled the cluster may renegotiate and potentially select a new primary unit (master) every time a cluster unit leaves or joins a cluster, every time a cluster unit changes status within a cluster, and every time the HA configuration of a cluster unit changes. Override is enabled so that cluster operation is more dynamic. The cluster is more likely to react immediately to an HA configuration change or other factor that could potentially lead to the cluster selecting a new primary unit.
The problem

If override is enabled and you make configuration changes to a cluster these changes can be lost. For example, consider the following sequence:

1. A cluster of two FortiGate units is operating with override enabled.
   - FGT-A: Primary unit with device priority 200 and with override enabled
   - FGT-B: Subordinate unit with device priority 100 and with override disabled
   - If both units are operating, FGT-A always becomes the primary unit because FGT-A has the highest device priority.

2. FGT-A fails and FGT-B becomes the new primary unit.

3. The administrator makes configuration changes to the cluster.
   The configuration changes are made to FGT-B because FGT-B is operating as the primary unit. These configuration changes are not synchronized to FGT-A because FGT-A is not operating.

4. FGT-A is restored and starts up again.

5. The cluster renegotiates and FGT-A becomes the new primary unit.

6. The cluster recognizes that the configurations of FGT-A and FGT-B are not the same.

7. The configuration of FGT-A is synchronized to FGT-B.
   The cluster is now operating with the same configuration as FGT-A. The configuration changes made to FGT-B have been lost.

The solution

When override is enabled, you can prevent configuration changes from being lost by doing the following:

- Verify that all cluster units are operating before making configuration changes (from the web-based manager go to System > Config > HA to view the cluster members list or from the FortiOS v3.0 CLI enter get system ha status).
- Make sure the device priority of the primary unit is set higher than the device priorities of all other cluster units before making configuration changes. For example, you might want to keep all device priorities at the default setting and just raise the device priority of the current primary unit before making configuration changes.
- Disable override either permanently or until all configuration changes have been made and synchronized to all cluster units

Override and disconnecting a unit from a cluster

A similar scenario to the above may occur when you use the Disconnect from Cluster option from the web-based manager or the execute ha disconnect command from the CLI to disconnect a cluster unit from a cluster.
Configuration changes can be lost if and when you reconnect the disconnected unit to the cluster. You should make sure that the device priority of the disconnected unit is lower than the device priority of the current primary unit. Otherwise, when the disconnected unit joins the cluster, the cluster will renegotiate and the disconnected unit may become the primary unit. If this happens, the configuration of the disconnected unit is synchronized to all other cluster units and any configuration changes made since the unit was disconnected are lost.

Cluster virtual MAC addresses

When a cluster is operating, the FGCP assigns virtual MAC addresses to each primary unit interface. The FGCP uses virtual MAC addresses so that if a failover occurs, the new primary unit interfaces will have the same MAC addresses as the failed primary unit interfaces. If the MAC addresses change after a failover, the network would take longer to recover because all attached network devices would have to learn the new MAC addresses before they could communicate with the cluster.

If a cluster is operating in NAT/Route mode, the FGCP assigns a different virtual MAC address to each primary unit interface. VLAN subinterfaces are assigned the same virtual MAC address as the physical interface that the VLAN subinterface is added to. Redundant interfaces or 802.3ad aggregate interfaces are assigned the virtual MAC address of the first interface in the redundant or aggregate list.

If a cluster is operating in Transparent mode, the FGCP assigns a virtual MAC address for the primary unit management IP address. Since you can connect to the management IP address from any interface, all of the FortiGate interfaces appear to have the same virtual MAC address.

When a cluster starts up, after a failover, the primary unit sends gratuitous ARP packets to update the switches connected to the cluster interfaces with the virtual MAC address. The switches update their MAC forwarding tables with this MAC address. As a result, the switches direct all network traffic to the primary unit. Depending on the cluster configuration, the primary unit either processes this network traffic itself or load balances the network traffic among all of the cluster units.

Changing the HA group ID

The cluster virtual MAC addresses depend on the cluster group ID. In most cases you can operate the cluster with the default group ID of zero. However, if you have more than one FortiGate cluster on the same network, each cluster should have a different group ID. If two clusters on the same network have the same group ID, duplicate MAC addresses could cause addressing conflicts on the network. You can change the group ID from the FortiGate CLI using the following command:
How the virtual MAC address is determined

The virtual MAC address is determined based on following formula:

00-09-0f-06-<group-id_hex>-<vcluster_integer><idx>

where

<group-id_hex> is the HA Group ID for the cluster converted to hexadecimal. 

Table 5 lists the virtual MAC address set for each group ID.

Table 5: HA group ID in integer and hexadecimal format

<table>
<thead>
<tr>
<th>Integer Group ID</th>
<th>Hexadecimal Group ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
</tr>
<tr>
<td>1</td>
<td>01</td>
</tr>
<tr>
<td>2</td>
<td>02</td>
</tr>
<tr>
<td>3</td>
<td>03</td>
</tr>
<tr>
<td>4</td>
<td>04</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>10</td>
<td>0a</td>
</tr>
<tr>
<td>11</td>
<td>0b</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>63</td>
<td>3f</td>
</tr>
</tbody>
</table>

<vcluster_integer> is 0 for virtual cluster 1 and 2 for virtual cluster 2. If virtual domains are not enabled, HA sets the virtual cluster to 1 and by default all interfaces are in the root virtual domain. Including virtual cluster and virtual domain factors in the virtual MAC address formula means that the same formula can be used whether or not virtual domains and virtual clustering is enabled.

<idx> is the index number of the interface. In NAT/Route mode, interfaces are numbered from 0 to x (where x is the number of interfaces). The interfaces are listed in alphabetical order on the web-based manager and CLI. The interface at the top of the interface list is first in alphabetical order by name and has an index of 0. The second interface in the list has an index of 1 and so on. In Transparent mode, the index number for the management IP address is 0.

The second last part of the virtual MAC address depends on the HA group ID and is the same for each cluster interface. The last part of the virtual MAC address is different for each cluster interface.

Example virtual MAC addresses

A FortiGate-500 HA cluster operating in NAT/Route mode where the HA group ID has not been changed (default=0) and virtual domains have not been enabled would have the following virtual MAC addresses:

- dmz interface virtual MAC: 00-09-0f-09-00-00
- external interface virtual MAC: 00-09-0f-09-00-01
- ha interface virtual MAC: 00-09-0f-09-00-02
• Internal interface virtual MAC: 00-09-0f-09-00-03
• port1 interface virtual MAC: 00-09-0f-09-00-04
• port2 interface virtual MAC: 00-09-0f-09-00-05
• port3 interface virtual MAC: 00-09-0f-09-00-06
• port4 interface virtual MAC: 00-09-0f-09-00-07
• port5 interface virtual MAC: 00-09-0f-09-00-08
• port6 interface virtual MAC: 00-09-0f-09-00-09
• port7 interface virtual MAC: 00-09-0f-09-00-a0
• port8 interface virtual MAC: 00-09-0f-09-00-0b

If the group ID is changed to 34 these virtual MAC addresses change to:
• dmz interface virtual MAC: 00-09-0f-09-22-00
• external interface virtual MAC: 00-09-0f-09-22-01
• ha interface virtual MAC: 00-09-0f-09-22-02
• Internal interface virtual MAC: 00-09-0f-09-22-03
• port1 interface virtual MAC: 00-09-0f-09-22-04
• port2 interface virtual MAC: 00-09-0f-09-22-05
• port3 interface virtual MAC: 00-09-0f-09-22-06
• port4 interface virtual MAC: 00-09-0f-09-22-07
• port5 interface virtual MAC: 00-09-0f-09-22-08
• port6 interface virtual MAC: 00-09-0f-09-22-09
• port7 interface virtual MAC: 00-09-0f-09-22-0a
• port8 interface virtual MAC: 00-09-0f-09-22-0b

All of the interfaces of a FortiGate-800 HA cluster operating in Transparent mode with group ID set to 10 have the virtual MAC 00-09-0f-09-0a-00.

A FortiGate-5001SX HA cluster operating in NAT/Route mode with virtual domains enabled where the HA group ID has been changed to 23, port5 and port 6 are in the root virtual domain (which is in virtual cluster1), and port7 and port8 are in the vdom_1 virtual domain (which is in virtual cluster 2) would have the following virtual MAC addresses:

port5 interface virtual MAC: 00-09-0f-09-23-05
port6 interface virtual MAC: 00-09-0f-09-23-06
port7 interface virtual MAC: 00-09-0f-09-23-27
port8 interface virtual MAC: 00-09-0f-09-23-28

**Virtual MAC address conflicts**

If two or more clusters are operating on the same network, there is a possibility that a MAC address conflict can occur. Because all clusters use the same formula to calculate cluster virtual MAC addresses, a MAC address conflict can occur in the following configurations:
Virtual MAC address conflicts

- Two clusters are operating on the same network in NAT/Route mode and both clusters have the cluster interface with the same index number connected to the network. For example, both clusters could be using the same FortiGate model and the same interface of each cluster could be connected to the network. This can also happen if each cluster is using a different FortiGate model but the interfaces connected to the network have the same network index.

- Two clusters are operating on the same network in Transparent mode. In this case, all interfaces of both clusters have the same MAC address.

- Two clusters are operating on the same network, one in NAT/Route mode and one in Transparent mode. In this case a conflict can occur of NAT/Route mode cluster interface with interface index 0 is connected to the same network as the cluster operating in Transparent mode.

The solution to all of these conflicts is to use the `config system ha group-id` CLI command to change the HA group ID of one or both of the clusters. In general it is recommended that you change the `group-id` if you are connecting two clusters to the same network.

Device and link failover

The FGCP provides transparent device and link failover. This section describes what device and link failover are and how the cluster responds to each type of failure to maintain network traffic flow. The section also includes information about how network components influence failover times.

If session pickup is enabled, the cluster maintains active network sessions even if a cluster component fails. The cluster recognizes a component failure and takes steps to respond so that the network can continue to operate without interruption. The internal operation of the cluster changes, but network components outside of the cluster notice little or no change.

To support maintaining active network sessions, the FGCP maintains a session table for all communication sessions being processed by the cluster. If a cluster unit fails, this session table information is available to the remaining cluster units, and these cluster units resume the communication sessions that were being processed by the failed cluster unit without interruption.

**Note:** Not all communication sessions can be recovered when a failover occurs. What is maintained and what is not depends on the HA mode that the cluster is operating in. See “Active-passive HA (failover protection)” on page 39 and “Active-active HA (load balancing and failover protection)” on page 40.

If session pickup is disabled, the cluster does not maintain active network sessions after a failover. The FGCP does not maintain an active session table and all communications sessions are temporarily interrupted until the cluster renegotiates. However, negotiation takes place very quickly so the cluster can quickly resume processing network traffic. If a single FortiGate unit or other network component fails network traffic is interrupted until the component can be replaced or traffic routed around it.
A failover can be caused by a hardware failure, software issues, or something as simple as a network cable being disconnected. If a failover occurs, the cluster also records log messages about the event and can be configured to send log messages to a syslog server and to a FortiAnalyzer unit. The cluster can also send SNMP traps and alert email messages. This information can be used by network administrators to find and fix the problem that caused the failure.

**Device failover**

Device failover means that if a cluster unit fails (called a device failure), the cluster reorganizes itself to continue operating with minimal or no effect on network traffic.

**Link failover**

Link failover means that if a monitored interface fails, the cluster reorganizes to re-establish a link to the network that the monitored interface was connected to and to continue operating with minimal or no disruption of network traffic. You configure interface monitoring by selecting the interfaces to monitor as part of the HA configuration. The cluster monitors each cluster unit to determine if the monitored interface is operating and connected.

The cluster can detect a failure of the network interface hardware. The cluster can also determine if individual network interfaces are disconnected from the switch they should be connected to. The cluster cannot determine if the switch that cluster interfaces are connected to is still connected to the network.

Because the primary unit receives all traffic processed by the cluster, a cluster can only process traffic from a network if the primary unit can connect to it. So, if the link that the primary unit has to a network fails, to maintain traffic flow to and from this network, the cluster must select a different primary unit. Unless another link failure has occurred, the new primary unit has an active link to this network.

To support link failover, each cluster unit stores link state information for all monitored cluster units in a link state database. All cluster units keep this link state database up to date by sharing link state information with the other cluster units. If one of the monitored interfaces on one of the cluster units becomes disconnected or fails, this information is immediately transmitted to all cluster units.

If monitored interface on the primary unit fails, the cluster renegotiates to select a new primary unit using the process described in “Primary unit selection” on page 25. Because the cluster unit with the failed monitored interface has the lowest monitor priority, a different cluster unit becomes the primary unit. The cluster maintains all communication sessions in the same manner as for a device failure.

If a monitored interface on a subordinate unit fails, this information is shared with all cluster units. The cluster does not renegotiate. The cluster unit with the failed monitored interface continues to function in the cluster. In an active-active cluster, the subordinate unit can continue processing connections between functioning interfaces. After the failure, if session pickup is enabled, all sessions being processed by the subordinate unit are transferred to other cluster units. All virus scanning sessions being processed by the subordinate unit are lost.
Multiple link failures

Every time a monitored interface fails, the cluster repeats the processes described above. If multiple monitored interfaces fail on more than one cluster unit, the cluster continues to negotiate to select a primary unit that can provide the most network connections.

Figure 7: Example FortiGate-3600 HA interface monitor configuration

Failover and attached network equipment

It normally takes a cluster approximately 6 seconds to complete a failover. However, the actual failover time may depend on how quickly the switches connected to the cluster interfaces accept the cluster MAC address update from the primary unit. If the switches do not recognize and accept the special ARP packets and update their MAC forwarding table, the failover time will increase.

Also, individual session failover depends on whether the cluster is operating in active-active or active-passive mode, and whether the content of the traffic is to be virus scanned. Depending on application behavior, it may take a TCP session a longer period of time (up to 30 seconds) to recover completely.

HA configuration synchronization

The FGCP uses a combination of incremental and periodic synchronization to make sure that the configurations of all cluster units is synchronized.

Incremental synchronization

When you log into the cluster web-based manager or CLI to make configuration changes, you are actually logging into the primary unit. All of your configuration changes are first made to the primary unit. Incremental synchronization then immediately synchronizes these changes to all of the subordinate units.
When you log into a subordinate unit CLI (for example using `execute ha manage`) all of the configuration changes that you make to the subordinate unit are also immediately synchronized to all cluster units, including the primary unit, using the same process.

Whenever a change is made to a cluster unit configuration, incremental synchronization sends the same configuration change to all other cluster units over the HA heartbeat link. An HA synchronization process running on the each cluster unit receives the configuration change and applies it to the cluster unit. The HA synchronization process makes the configuration change by entering a CLI command that appears to be entered by the administrator who made the configuration change in the first place.

Synchronization takes place silently, and no log messages are recorded about the synchronization activity. You can see evidence of incremental synchronization if you enable event logging and set the minimum severity level to Information and then check the event log messages written by the cluster units when you make a configuration change.

**Example: configuration change synchronized from primary unit to subordinate unit**

The following event log message is written by the primary unit when the admin administrator adds firewall policy 3 by connecting to the web-based manager from a management PC with IP address 172.20.120.14 using HTTPS or HTTP:

```
2006-10-20 09:52:20 log_id=0104032126 type=event
subtype=admin pri=notice vd=root user="admin"
ui=GUI(172.20.120.14) seq=3 msg="User admin added new firewall policy 3 from GUI(172.20.120.14)"
```

When incremental synchronization makes the same change to a subordinate unit the subordinate unit writes the following log message:

```
2006-10-20 09:52:20 log_id=0104032126 type=event
subtype=admin pri=notice vd=root user="admin" ui=ha_daemon seq=3 msg="User admin added new firewall policy 3 from ha_daemon"
```

Notice that the two messages are identical except that on the subordinate unit the `ui` (user interface) is `ha_daemon`. `ha_daemon` is the name of the user interface used by the HA synchronization process to make incremental synchronization configuration changes.

**Example: configuration change synchronized from subordinate unit to primary unit**

The following event log message is written by a subordinate unit after the admin administrator logs into the subordinate unit CLI using the `execute ha manage` command and adds firewall policy 6.

```
2006-10-20 11:29:46 log_id=0104032126 type=event
subtype=admin pri=notice vd=root user="admin"
ui=telnet(10.0.0.1) seq=6 msg="User admin added new firewall policy 6 from telnet(10.0.0.1)"
```
Notice the user interface is `telnet(10.0.0.1)`. 10.0.0.1 is the IP address of the HA heartbeat interface of the primary unit. The log message shows that the `execute ha manage` command sets up a telnet session from the primary unit to the subordinate unit over the HA heartbeat link.

When incremental synchronization makes the same change to the primary unit, the primary unit writes the following log message:

```
2006-10-20 11:29:47 log_id=0104032126 type=event
subtype=admin pri=notice vd=root user="admin" ui=ha_daemon
seq=6 msg="User admin added new firewall policy 6 from ha_daemon"
```

Notice again that the messages are identical except for the user interface.

**Periodic synchronization**

Incremental synchronization makes sure that as an administrator makes configuration changes, the configurations of all cluster units remain the same. However, a number of factors could cause one or more cluster units to go out of sync with the primary unit. For example, if you add a new unit to a functioning cluster, the configuration of this new unit will not match the configuration of the other cluster units. It’s not practical to use incremental synchronization to change the configuration of the new unit.

Periodic synchronization is a mechanism that looks for synchronization problems and fixes them. Every minute the cluster compares the configuration file checksum of the primary unit with the configuration file checksums of each of the subordinate units. If all subordinate unit checksums are the same as the primary unit checksum, all cluster units are considered synchronized.

If one or more of the subordinate unit checksums is not the same as the primary unit checksum, the subordinate unit configuration is considered out of sync with the primary unit. The checksum of the out of sync subordinate unit is checked again every 15 seconds. This re-checking occurs in case the configurations are out of sync because an incremental configuration sequence has not completed. If the checksums do not match after 5 checks the primary unit configuration file is loaded into the subordinate unit and the subordinate unit restarts. When the subordinate unit restarts it will now have the same configuration as the primary unit.

The configuration of the subordinate unit is reset in this way because when a subordinate unit configuration gets out of sync with the primary unit configuration there is no efficient way to determine what the configuration differences are and to correct them. Resetting the subordinate unit configuration becomes the most efficient way to resynchronize the subordinate unit.

Synchronization requires that all cluster units run the same FortiOS firmware build. If some cluster units are running different firmware builds, then unstable cluster operation may occur and the cluster units may not be able to synchronize correctly.

**Note:** Re-installing the firmware build running on the primary unit forces the primary unit to upgrade all cluster units to the same firmware build.
Console messages when configuration synchronization fails

If you connect to the console of a subordinate unit that is out of synchronization with the primary unit, messages similar to the following are displayed.

slave is not in sync with master, sequence:0. (type 0x3)
slave is not in sync with master, sequence:1. (type 0x3)
slave is not in sync with master, sequence:2. (type 0x3)
slave is not in sync with master, sequence:3. (type 0x3)
slave is not in sync with master, sequence:4. (type 0x3)
global compared not matched
Wait for system rebooting...

If synchronization problems occur the console message sequence may be repeated over and over again. The messages all include a type value (in the example type 0x3). The type value can help Fortinet Support diagnose the synchronization problem.

HA operating modes

FortiGate clusters can operate in active-passive or active-active mode. Active-passive HA provides failover protection. Active-active HA provides load balancing as well as failover protection.

Active-passive HA (failover protection)

An active-passive (A-P) HA cluster provides hot standby failover protection. An active-passive cluster consists of a primary unit that processes traffic, and one or more subordinate units. The subordinate units are connected to the network and to the primary unit but do not process traffic. Instead, the subordinate units run in a standby state. In this standby state, the subordinate units receive cluster state information from the primary unit. Cluster state information includes a list of all communication sessions being processed by the primary unit. The subordinate units use this information to resume processing network traffic if the primary unit fails.

Active-passive HA provides transparent device failover among cluster units. If a cluster unit fails, another immediately takes its place.

Active-passive HA also provides transparent link failover among cluster units. Each cluster unit stores link state information for all of the cluster units in a link state database. All cluster units keep the database up to date by sharing link state information with the other cluster units.

If an interface on a cluster unit fails or is disconnected, this cluster unit updates the link state database and removes itself from the cluster.

Use active-passive HA for a more resilient session failover environment than active-active HA. In active-passive HA, session failover occurs for all traffic except for virus scanned sessions that are in progress. Active-active HA (described below) does not provide session failover for UDP, ICMP, multicast, and broadcast sessions.
Active-active HA (load balancing and failover protection)

Active-active (A-A) HA load balances network traffic among all cluster units. An active-active HA cluster consists of a primary unit that processes traffic and one or more subordinate units that also process traffic.

The primary unit receives all network traffic. All UDP, ICMP, multicast, and broadcast traffic is processed by the primary unit. The primary unit load balances virus scanning traffic, or optionally all TCP traffic and virus scanning traffic, among all cluster units. By distributing TCP and virus scanning among multiple cluster units, an active-active cluster may have higher throughput than a standalone FortiGate unit or than an active-passive cluster.

In addition to load balancing, active-active HA also provides device and link failover protection similar to an active-passive cluster. If the primary unit fails, a subordinate unit becomes the primary unit and redistributes TCP communications sessions among all remaining cluster units. UDP, ICMP, multicast, and broadcast sessions and virus scanned sessions that are in progress are not failed over and must be restarted. Because UDP, ICMP, multicast, and broadcast traffic are not failed over, active-active HA is a less robust failover solution than active-passive HA.

If a subordinate unit fails, the primary unit redistributes all TCP communications sessions among the remaining cluster units. Virus scanned sessions that are in progress on the subordinate unit are not failed over and must be restarted. UDP, ICMP, multicast, and broadcast sessions being processed by the primary unit are not affected.

FortiGate HA compatibility with PPP protocols

FortiGate HA is not compatible with PPP protocols such as DHCP or PPPoE. If one or more FortiGate unit interfaces is dynamically configured using DHCP or PPPoE you cannot switch to operating in HA mode. Also, if you are operating a FortiGate HA cluster, you cannot change a FortiGate interface in the cluster to be configured dynamically using DHCP or PPPoE.

Configuring a FortiGate interface to be a DHCP server or a DHCP relay agent is not affect by HA operation.

PPTP and L2TP VPNs are supported in HA mode. For a cluster you can configure PPTP and L2TP settings and you can also add firewall policies to allow PPTP and L2TP pass through. However, during a failover, any active PPTP and L2TP sessions are lost and must be restarted after the failover.

Upgrading HA cluster firmware

You can upgrade the FortiOS firmware running on an HA cluster in the same manner as upgrading the firmware running on a standalone FortiGate unit. During a normal firmware upgrade, the cluster upgrades the primary unit and all subordinate units to run the new firmware image. The firmware upgrade takes place without interrupting communication through the cluster.
To upgrade the firmware without interrupting communication through the cluster, the cluster goes through a series of steps that involve first upgrading the firmware running on the subordinate units, then making one of the subordinate units the primary unit, and finally upgrading the firmware on the former primary unit. These steps are transparent to the user and the network, but depending upon your HA configuration may result in the cluster selecting a new primary unit.

The following sequence describes in detail the steps the cluster goes through during a firmware upgrade and how different HA configuration settings may affect the outcome.

1. The administrator uploads a new firmware image from the web-based manager or CLI.
2. If the cluster is operating in active-active mode load balancing is turned off.
3. The cluster upgrades the firmware running on all of the subordinate units.
4. Once the subordinate units have been upgraded, a new primary unit is selected. This primary unit will be running the new upgraded firmware.
5. The cluster now upgrades the firmware of the former primary unit.
6. Depending on the device priority and override configuration of the cluster, one of the following happens
   - If override is enabled and the former primary unit has the highest device priority, the cluster renegotiates and the former primary unit (or the unit with the highest device priority) once again becomes the primary unit.
   - If override is not enabled or if all cluster units have the same device priority, the new primary unit continues to operate as the primary unit and the former primary unit continues to operate as a subordinate unit.
7. If the cluster is operating in active-active mode, load balancing is turned back on.

Changing how a cluster processes firmware upgrades

By default cluster firmware upgrades proceed as described in "Upgrading HA cluster firmware" on page 40. If required, you can use the following CLI command to change how the cluster handles firmware upgrades.

```
config system ha
  set uninterruptable-upgrade {disable | enable}
end
```

The `uninterruptable-upgrade` is enabled by default. If you disable it, the cluster still upgrades the firmware on all cluster units, but all cluster units are upgraded at once; which interrupts communication through the cluster.

Viewing and managing log messages for individual cluster units

1. Connect to the cluster and log into the web-based manager.
   For each log display, the HA Cluster list displays the serial number of the FortiGate unit for which log messages are displayed.
About HA event log messages

HA event log messages always include the host name and serial number of the cluster unit that recorded the message. Most HA log event log messages indicate when a cluster unit switches (or moves) from one HA state to another.

Cluster units can operate in the HA states listed in Table 6:

```
Table 6: HA states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>A FortiGate unit configured for HA operation has started up and is looking for other FortiGate units with which to form a cluster.</td>
</tr>
<tr>
<td>Work</td>
<td>In an active-passive cluster a cluster unit is operating as the primary unit. In an active-active cluster unit is operating as the primary unit or a subordinate unit.</td>
</tr>
<tr>
<td>Standby</td>
<td>In an active-passive cluster the cluster unit is operating as a subordinate unit.</td>
</tr>
</tbody>
</table>
```

HA log Event log messages also indicate the virtual cluster that the cluster unit is operating in as well as the member number of the unit in the cluster. If virtual domains are not enabled, all clusters unit are always operating in virtual cluster 1.

If virtual domains are enabled, a cluster unit may be operating in virtual cluster 1 or virtual cluster 2. The member number indicates the position of the cluster unit in the cluster members list. Member 0 is the primary unit. Member 1 is the first subordinate unit, member 2 is the second subordinate unit, and so on.

The following log message indicates that the cluster unit with host name 5001_Slot_4 and serial number FG50012204400045 has become the primary unit because it is operating in the work state as member 0.

```
2006-06-05 09:18:21 device_id=FG50012204400045 log_id=0105035001 type=event subtype=ha pri=notice msg="HA member 5001_Slot_4[FG50012204400045] move to work state in virtual cluster 1 as member 0"
```

The following log message indicates that the cluster unit with host name 5001_Slot_3 and serial number FG50012205400050 has become the first subordinate unit in an active-passive cluster because it is operating in the standby state as member 1.

```
2006-06-05 09:18:21 device_id=FG50012205400050 log_id=0105035001 type=event subtype=ha pri=notice msg="HA member 5001_Slot_3[FG50012205400050] move to standby state in virtual cluster 1 as member 1"
```

The following log message indicates that the cluster unit with host name 5001_Slot_3 and serial number FG50012205400050 has become the first subordinate unit in an active-active cluster because it is operating in the work state as member 1.

```
2006-06-05 09:18:21 device_id=FG50012205400050 log_id=0105035001 type=event subtype=ha pri=notice msg="HA member 5001_Slot_3[FG50012205400050] move to work state in virtual cluster 1 as member 1"
```
2006-06-05 10:11:12 device_id=FG50012205400050
log_id=0105035001 type=event subtype=ha pri=notice msg="HA
member 5001_Slot_3[FG50012205400050] move to work state in
virtual cluster 1 as member 1"

Disconnecting a unit from a cluster

Use the following procedures to disconnect a cluster unit from a functioning
cluster without disrupting the operation of the cluster. You can disconnect a cluster
unit if you need to use the disconnected FortiGate unit for another purpose, such
as to act as a standalone firewall.

You can use the following procedures for a standard cluster and for a virtual
cluster. To use the follow procedures from a virtual cluster you must be logged in
as the admin administrator and you must have selected Global Configuration.

When you disconnect a cluster unit you must assign an IP address and netmask
to one of the interfaces of the disconnected unit. You can disconnect any unit from
the cluster even the primary unit. After the unit is disconnected the cluster
responds as if the disconnected unit has failed. The cluster may renegotiate and
may select a new primary unit.

When the cluster unit is disconnected the HA mode is changed to standalone. In
addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0
except for the interface that you configure.

Otherwise the configuration of the disconnected unit is not changed. The HA
configuration of the disconnected unit is not changed either.

To disconnect a cluster unit from a cluster

1. Go to System > Config > HA to view the cluster members list.
2. Select the Disconnect from cluster icon for the cluster unit to disconnect from the
cluster.

Figure 8: Disconnect a cluster member

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Interface</th>
<th>IP/Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGT5002001201077</td>
<td>Internal</td>
<td>10.168.20.1/24</td>
</tr>
</tbody>
</table>

- **Serial Number**: Displays the serial number of the cluster unit to be disconnected
  from the cluster.
- **Interface**: Select the interface that you want to configure. You also specify
  the IP address and netmask for this interface. When the FortiGate
  unit is disconnected, all management access options are enabled
  for this interface.
- **IP/Netmask**: Specify an IP address and netmask for the interface. You can use
  this IP address to connect to this interface to configure the
  disconnected FortiGate unit.
3 Select OK.

The FortiGate unit is disconnected from the cluster and the cluster may renegotiate and select a new primary unit. The selected interface of the disconnected unit is configured with the specified IP address and netmask.

**To add a disconnected FortiGate unit back to its cluster**

If you have disconnected a FortiGate unit from a cluster, you can re-connect the disconnected FortiGate unit to the cluster by setting the HA mode of the disconnected unit to match the HA mode of the cluster. Usually the disconnected unit rejoins the cluster as a subordinate unit and the cluster automatically synchronizes its configuration.

**Note:** You do not have to change the HA password on the disconnected unit unless the HA has been changed after the unit was disconnected. Disconnecting a unit from a cluster does not change the HA password.

**Caution:** You should make sure that the device priority of the disconnected unit is lower than the device priority of the current primary unit. You should also make sure that the HA override CLI option is not enabled on the disconnected unit. Otherwise, when the disconnected joins the cluster, the cluster will renegotiate and the disconnected unit may become the primary unit. If this happens, the configuration of the disconnected unit is synchronized to all other cluster units. This configuration change might disrupt the operation of the cluster.

The following procedure assumes that the disconnected FortiGate unit is correctly physically connected to your network and to the cluster hardware but is not running in HA mode and not part of the cluster.

Before you start this procedure you should note the device priority of the primary unit.

1 Log into the disconnected FortiGate unit.

If virtual domains are enabled, log in as the admin administrator and select Global Configuration.

2 Go to **System > Config > HA**.

3 Change Mode to match the mode of the cluster.

4 If required set the HA password to match the password of the cluster.

5 Set the Device Priority lower than the device priority of the primary unit.

6 Select OK.

The disconnected FortiGate unit joins the cluster.

**HA and redundant interfaces**

On FortiGate models 800 and above you can use redundant interfaces to combine two or more interfaces into a single redundant interface.
A redundant interface acquires the MAC address of the first interface in the list of interfaces added to the redundant interface configuration. The interfaces are listed in the redundant configuration in the order in which you add them. From the GUI this means that the first interface that you select is at the top of the list and the second interface that you select is added below the first one. So, for example, if a redundant interface contains port1 and port2, if you select port2 first, port2 will be the first interface added to the redundant interface. From the CLI the order in which you add the interface names to the set member interface command controls the order that the interfaces are added to the redundant interface. The redundant interface appears on the network as a single interface with the MAC address of first interface added to it (in this case port2).

An HA cluster with a redundant interface could consist of two FortiGate-800 units operating in HA mode installed between a server network and the Internet.

The connection between the cluster and the server network consists of a redundant interface connection to port1 and port2 of the FortiGate-800 units in the cluster. The redundant interface is configured as an HA monitored interface. The switch is also connected to the server network.

The cluster is connected to the internet using a gigabyte connection to a switch. The switch connects to port4 of both FortiGate-800 units in the cluster.

**Figure 9: Example cluster with a redundant interface**

**HA interface monitoring, link failover, and redundant interfaces**

HA interface monitoring monitors the redundant interface as a single interface and does not monitor the individual physical interfaces in the redundant interface. HA interface monitoring registers the redundant interface to have failed only if all the physical interfaces in the redundant interface have failed. If only some of the physical interfaces in the redundant interface fail or become disconnected, HA considers the redundant interface to be operating normally.

**HA MAC addresses and redundant interfaces**

For a standalone FortiGate unit a redundant interface has the MAC address of the first physical interface in the redundant interface configuration. A redundant interface consisting of port1 and port2 would have the MAC address of port1.
In an HA cluster, HA changes the MAC addresses of the cluster interfaces to virtual MAC addresses. A redundant interface in a cluster acquires the virtual MAC address that would have been acquired by the first physical interface in the redundant interface configuration.

Connecting multiple redundant interfaces to one switch while operating in active-passive HA mode

HA assigns the same virtual MAC addresses to the subordinate unit interfaces as are assigned to the corresponding primary unit interfaces. Consider a cluster of two FortiGate units operating in active-passive mode with a redundant interface consisting of port1 and port2. You can connect multiple redundant interfaces to the same switch if you configure the switch so that it defines multiple separate redundant interfaces and puts the redundant interfaces of each cluster unit into separate redundant interfaces. In this configuration, each cluster unit forms a separate redundant interface with the switch.

However, if the switch is configured with a single four-port redundant interface configuration, because the same MAC addresses are being used by both cluster units, the switch adds all four interfaces (port1 and port2 from the primary unit and port1 and port2 from the subordinate unit) to the same redundant interface.

To avoid unpredictable results, when you connect a switch to multiple redundant interfaces in an active-passive cluster you should configure separate redundant interfaces on the switch; one for each cluster unit.

Connecting multiple redundant interfaces to one switch while operating in active-active HA mode

In an active-active cluster, all cluster units send and receive packets. To operate a cluster with redundant interfaces in active-active mode, with multiple redundant interfaces connected to the same switch, you must separate the redundant interfaces of each cluster unit into different redundant interfaces on the connecting switch.

HA and 802.3 aggregate interfaces

On FortiGate models 800 and above you can use 802.3ad aggregation to combine two or more interfaces into a single aggregate interface.

An aggregate interface acquires the MAC address of the first interface in the list of interfaces added to the aggregate. The interfaces are listed in the aggregate configuration in alphabetical order. So, for example, if an aggregate contains port1 and port2, the aggregate interface appears on the network as a single interface with the MAC address of port1.

A HA cluster with an aggregate interface could consist of two FortiGate-800 units operating in HA mode. Both FortiGate-800 units are connected to the internet using a gigabyte connection to a switch. The switch connects to port4 of both FortiGate-800 units in the cluster. Virtual domains are not configured.

A server network is connected to a switch using two 100Mb connections. The switch in turn uses link aggregation (2x100Mb) connections to connect to port1 and port2 of the FortiGate-800 units in the cluster. The aggregate interface is configured as an HA monitored interface.
HA interface monitoring, link failover, and 802.3ad aggregation

HA interface monitoring monitors the aggregate interface as a single interface and does not monitor the individual physical interfaces in the aggregate. HA interface monitoring registers the aggregate to have failed only if all the physical interfaces in the aggregate have failed. If only some of the physical interfaces in the aggregate fail or become disconnected, HA considers the aggregate to be operating normally.

HA MAC addresses and 802.3ad aggregation

If a link aggregate configuration uses the Link Aggregate Control Protocol (LACP) (either passive or active) LACP is negotiated over all of the interfaces in any aggregate. For a standalone FortiGate unit, the FortiGate LACP implementation uses the MAC address of the first interface in the aggregate to uniquely identify the aggregate. An aggregate interface consisting of port1 and port2 would have the MAC address of port1.

In an HA cluster, HA changes the MAC addresses of the cluster interfaces to virtual MAC addresses. An aggregate interface in a cluster acquires the virtual MAC address that would have been acquired by the first interface in the aggregate.

HA active-passive mode and LACP

HA assigns the same virtual MAC addresses to the subordinate unit interfaces as are assigned to the corresponding primary unit interfaces. Consider a cluster of two FortiGate units operating in active-passive mode with an aggregate interface consisting of port1 and port2. You can connect multiple aggregate interfaces to the same switch if you configure the switch connecting the aggregate interfaces so that it defines multiple separate aggregates and puts the interfaces of each cluster unit into separate aggregates. In this configuration, each cluster unit forms a separate aggregate with the switch.

However, if the switch is configured with a single four-port aggregate, because the same MAC addresses are being used by both cluster units, the switch adds all four interfaces (port1 and port2 from the primary unit and port1 and port2 from the subordinate unit) to the same aggregate.
This causes problems because the switch distributes traffic over all four interfaces in the aggregate. So traffic could be received on an interface from the primary unit and sent back on an interface connected to the subordinate unit.

To prevent this problem, when you connect a switch to aggregate interfaces in an active-passive cluster you should configure separate aggregates on the switch; one for each cluster unit.

If you must add both FortiGate units to the same aggregate then you can set the `config system interface lACP-ha-slave CLI keyword to disable so that the subordinate unit will not send or accept LACP packets. As a result, the subordinate unit does not participate in the aggregate. When a failover occurs and the subordinate unit becomes the primary unit, the new primary unit starts sending and receiving LACP packets and joins the aggregate. `lACP-ha-slave` is enabled by default. See the FortiGate CLI Reference for more information about the `lACP-ha-slave` keyword.

### HA and dynamic routing failover

This section describes extensions to FortiOS routing protocols to transparently failover an HA cluster without impact to routing decisions in the network.

During an HA state transition, the neighbor routers detect that the primary router has failed. This causes them to stop sending packets to the cluster while the routing topology stabilizes, which in turn causes sessions to be timed out and/or dropped. Extensions have been added to the FortiOS routing protocols, enabling them to notify neighbor routers of the state transition, thereby minimizing the impact to the routing topology.

### The problem with dynamic routing and HA

When dynamic routing is used in the network (and a FortiGate unit must act as a routing node) limitations are introduced during failover. Under this scenario, only 1 FortiGate (the Primary unit) can run dynamic routing protocols to communicate with neighbors. The subordinate units do not run the protocols, and therefore do not build up their internal network maps/databases/etc. As a result, when a failure occurs, the new primary unit must spawn the routing daemons, which will have no dynamic data. This will cause neighbor routers to immediately withdraw the cluster from its routing topology (at least while the network is stabilizing) and packets will not be directed to the cluster. With no packets flowing to the cluster sessions will be timed out and connections will be dropped while the network is stabilizing.

### The FortiOS HA resolution

FortiOS v3.0 applies the principle of graceful restart of routing to solve the problem of dynamic routing failover. Graceful restart or routing involves using built-in protocol extensions to handle the failover gracefully. Neighbor routers will be informed that the cluster has experienced (or will experience) a restart event and will continue sending packets to the cluster, while its routing data stabilizes.
Configuration reference

Use the information in this chapter as a reference to all HA configuration parameters. This chapter describes all web-based manager HA configuration settings and the `config system ha`, `get system ha status`, and `execute ha` commands.

- Configuring HA web-based manager options (virtual clustering not enabled)
- Configuring HA web-based manager options for virtual clustering
- HA web-based manager options
- Changing subordinate unit host name and device priority
- `config system ha` (CLI command)
- `get system ha status` (CLI command)
- `execute ha disconnect` (CLI command)
- `execute ha manage` (CLI command)
- `execute ha synchronize` (CLI command)

**Configuring HA web-based manager options (virtual clustering not enabled)**

To configure HA options so that a FortiGate unit can join an HA cluster, go to **System > Config > HA**.

To change the configuration settings of the primary unit in a functioning cluster, go to **System > Config > HA** to display the cluster members list. Select Edit for the master (or primary) unit in the cluster members list.

**Figure 11** shows an example HA configuration for a FortiGate-5001SX unit operating with virtual domains not enabled. This active-passive HA configuration uses the default device priority, group name, password, and the default setting for enable session pickup. Port monitor has been enabled for port1, port5, and port6. port9 and port10 are the heartbeat interfaces.
To change the host name and device priority of subordinate units in a functioning cluster, go to System > Config > HA to display the cluster members list. Select Edit for the subordinate (or backup) unit to configure. See “Changing subordinate unit host name and device priority” on page 57 for information about configuring subordinate units.

Configuring HA web-based manager options for virtual clustering

**Note:** If your FortiGate cluster uses virtual domains, you are configuring HA virtual clusters. Most virtual cluster HA options are the same as normal HA options. However, virtual clusters include VDOM partitioning options. Other differences between configuration options for regular HA and for virtual clustering HA are described below.

To configure HA options for a FortiGate unit with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to System > Config > HA.

To change the configuration settings of the primary unit in a functioning cluster with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to System > Config > HA to display the cluster members list. Select Edit for the master (or primary) unit in the cluster members list.

Figure 12 shows an example HA configuration for a FortiGate-5001SX unit operating in a virtual clustering configuration. Four virtual domains have been distributed between virtual cluster 1 and virtual cluster 2. The virtual cluster 1 device priority for this FortiGate unit is set higher than the default value so this FortiGate unit is the primary unit for virtual cluster 1; which means this FortiGate unit processes all traffic for Vdom_2 and for the root virtual domain.
To change the host name and device priority of subordinate units in a functioning cluster with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to System > Config > HA to display the cluster members list. Select Edit for the subordinate (or backup) unit to configure. See “Changing subordinate unit host name and device priority” on page 57 for information about configuring subordinate units.

**HA web-based manager options**

Configure HA options so that a FortiGate unit can join a cluster or to change the configuration of an operating cluster or cluster member.

You can configure the following HA options:

- Mode
- Device Priority
- Group Name
- Password
- Enable Session pickup
Mode

Select an HA mode for the cluster or return the FortiGate units in the cluster to standalone mode. When configuring a cluster, you must set all members of the HA cluster to the same HA mode.

**Standalone mode**

The default operation mode. If Standalone mode is selected the FortiGate unit is not operating in HA mode. Select Standalone Mode if you want to stop a cluster unit from operating in HA mode.

**Active-Passive**

Select to configure a cluster for failover HA. In active-passive mode the primary unit processes all connections. All other cluster units passively monitor the cluster status and remain synchronized with the primary unit. Virtual clusters must operate in active-passive mode.

**Active-Active**

Select to configure a cluster for load balancing and failover HA. In active-active mode, each cluster unit actively processes traffic and monitors the status of the other cluster units. The primary unit controls load balancing among all of the cluster units. You cannot select active-active if you are configuring a virtual cluster.

Changing the HA mode of a functioning cluster causes the cluster to renegotiate to operate in the new mode and possibly select a new primary unit.

Device Priority

Optionally set the device priority of the cluster unit. Each cluster unit can have a different device priority. During HA negotiation, the unit with the highest device priority usually becomes the primary unit.

The device priority is not synchronized among cluster units. In a functioning cluster you change device priority to change the priority of any unit in the cluster. Whenever you change the device priority of a cluster unit, when the cluster negotiates, the unit with the highest device priority becomes the primary unit.

Normally, when configuring HA you do not have to change the device priority of any of the cluster units. If all cluster units have the same device priority, when the cluster first starts up the FGCP negotiates to select the cluster unit with the highest serial number to be the primary unit.

Clusters also function normally if all units have the same device priority. However, you can use the device priority if you want to control the roles that individual units play in the cluster. For example, if you want the same unit to always become the primary unit, set this unit device priority higher than the device priority of other cluster units. Also, if you want a cluster unit to always become a subordinate unit, set this cluster unit device priority lower than the device priority of other cluster units.

**Note:** The cluster renegotiates when you change the device priority if override is enabled on the cluster unit for which you changed the device priority. By default, override is not enabled. So changing the device priority of a unit in a functioning cluster may not have any affect until you force the cluster to renegotiate or until the cluster renegotiates because of a failure. You can configure override from the FortiGate CLI. See the FortiGate CLI Reference for information about configuring override. You can also see the FortiGate HA Overview or the FortiGate HA Guide for more information about configuring override and about cluster primary unit selection.
The device priority range is 0 to 255. The default device priority is 128.

If you are configuring a virtual cluster, if you have added virtual domains to both virtual clusters, you can set the device priority that the cluster unit has in virtual cluster 1 and virtual cluster 2. If a FortiGate unit has different device priorities in virtual cluster 1 and virtual cluster 2, the FortiGate unit may be the primary unit in one virtual cluster and the subordinate unit in the other. For more information, see “Virtual clustering load balancing configuration” on page 123 and “Managing a FortiGate virtual clustering configuration” on page 160.

**Group Name**

Add a name to identify the cluster. The maximum group name length is 7 characters. The group name must be the same for all cluster units before the cluster units can form a cluster. After a cluster is operating you can change the group name. The group name change is synchronized to all cluster units.

You do not have to change the default group name, but you can change the group name after the cluster is operating. If you have two clusters on the same network, you should give them different group names.

The group name appears on the FortiGate web-based manager dashboard of a functioning cluster as the Cluster Name.

**Password**

Add a password to identify the cluster. The maximum password length is 15 characters. The password must be the same for all cluster units before the cluster units can form a cluster.

You do not have to add a password to configure a cluster. After a cluster is operating you can change the password. The password change is synchronized to all cluster units. If you have two clusters on the same network, you should give them different passwords.

**Enable Session pickup**

Enable session pickup so that if the primary unit fails, all sessions are picked up by the cluster unit that becomes the new primary unit.

If you enable session pickup, subordinate units maintain session tables that match the primary unit session table. If the primary unit fails, the new primary unit can use its session table to maintain all active communication sessions.

If you do not enable session pickup the subordinate units do not maintain session tables. If the primary unit fails, all sessions are interrupted and must be restarted when the new primary unit is operating.

You must enable session pickup for effective failover protection. If you do not require effective failover protection, leaving session pickup disabled may reduce HA CPU usage and reduce HA heartbeat network bandwidth usage.
Port Monitor

Enable or disable monitoring FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks. If a monitored interface fails or is disconnected from its network the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster unit that still has a connection to the network. This other cluster unit becomes the new primary unit.

If a number of monitored interfaces fail, the cluster unit with most functioning monitored interfaces becomes the primary unit. If more than one cluster unit has the same number and the most monitored interfaces connected, the FGCP compares the device priorities of these more connected cluster units and selects the one with the highest device priority to become the primary unit. If all of these connected cluster units have the same device priority, the connected cluster unit with the highest serial number becomes the primary unit.

If you can re-establish traffic flow through the interface (for example, if you re-connect a disconnected network cable) the interface rejoins the cluster.

You should only monitor interfaces that are connected to networks, because a failover may occur if you monitor an unconnected interface.

The interfaces that you can monitor appear on the port monitor list. You can monitor all FortiGate interfaces including redundant interfaces and 802.3ad aggregate interfaces.

You cannot monitor the following types of interfaces (you cannot select the interfaces on the Port Monitor list):

- FortiGate interfaces that contain an internal switch. This includes the internal interface of all FortiGate-60 and FortiWiFi-60 models as well as the FortiGate-100A, 200A internal interface. This also includes the LAN interface of the FortiGate-500A.
- VLAN subinterfaces.
- IPSec VPN interfaces.
- Individual physical interfaces that have been added to a redundant or 802.3ad aggregate interface.
- FortiGate-5000 series backplane interfaces that have not been configured as network interfaces and can only be configured as heartbeat interfaces.

If you are configuring a virtual cluster you can create a different port monitor configuration for each virtual cluster. Usually for each virtual cluster you would monitor the interfaces that have been added to the virtual domains in each virtual cluster.

Heartbeat Interface

Enable or disable HA heartbeat communication for each interface in the cluster. You must select at least one heartbeat interface. If heartbeat communication is interrupted the cluster stops processing traffic. By default, HA heartbeat communication is set for two interfaces (see Table 7).
You can disable the HA heartbeat for either of these interfaces or enable HA heartbeat for other interfaces. In most cases you can maintain the default heartbeat interface configuration as long as you can connect the heartbeat interfaces together. Configuring HA heartbeat interfaces is the same for virtual clustering and for standard HA clustering.

HA heartbeat hello packets are constantly sent by all of the configured heartbeat interfaces. Using these hello packets, each cluster unit confirms that the other cluster units are still operating. The FGCP selects one of the heartbeat interfaces to be used for communication between the cluster units. The FCGP selects the heartbeat interface to be used based on the linkfail states of the heartbeat interfaces and on the interface index.

The web-based manager lists the FortiGate unit interfaces in alphabetical order. This order corresponds to the interface index order. The selected heartbeat interface that is highest in the interface list (or first in alphabetical order) is used for heartbeat communication between cluster units. If this interface fails or becomes disconnected, the interface that is next highest in the list (or next in alphabetical order) handles all HA heartbeat communication. The heartbeat interface that is higher in the interface list resumes processing all HA heartbeat communication if it becomes connected again.

The HA heartbeat communicates cluster session information, synchronizes the cluster configuration, synchronizes the cluster routing table, and reports individual cluster member status. The HA heartbeat constantly communicates HA status information to make sure that the cluster is operating properly.

You can enable heartbeat communications for physical interfaces, but not for VLAN subinterfaces, IPSec VPN interfaces, redundant interfaces, or for 802.3ad aggregate interfaces. You cannot select these types of interfaces in the heartbeat interface list.

Selecting more heartbeat interfaces increases reliability. If a heartbeat interface fails or is disconnected, the HA heartbeat fails over to the next heartbeat interface.

HA heartbeat traffic can use a considerable amount of network bandwidth. If possible, enable HA heartbeat traffic on interfaces used only for HA heartbeat traffic or on interfaces connected to less busy networks.

You can configure a FortiGate interface that contains an internal switch as an HA heartbeat interface. However this configuration is not recommended for two reasons:

- For security reasons and to save network bandwidth you should keep HA heartbeat traffic off of your internal network, and internal switch interfaces are usually intended to be connected to your internal network.
- Heartbeat packets may be lost if the switch interface is processing high volumes of traffic. Loosing heartbeat packets may lead to unnecessary and repeated failovers.

FortiGate models with switch interfaces include:

- All FortiGate-60 and FortiWiFi-60 internal interfaces.
- FortiGate-100A and 200A internal interfaces.
- FortiGate-500A LAN interface.

Table 7 Lists the default HA heartbeat interfaces for all FortiGate models.
Heartbeat Interface

Table 7: Default HA heartbeat interface configuration for all FortiGate models

<table>
<thead>
<tr>
<th>FortiGate model</th>
<th>Default heartbeat interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate-60 models and FortiWiFi-60 models</td>
<td>dmz*, wan1</td>
</tr>
<tr>
<td>FortiGate-100</td>
<td>dmz*, external</td>
</tr>
<tr>
<td>FortiGate-100A</td>
<td>dmz2*, external</td>
</tr>
<tr>
<td>FortiGate-200</td>
<td>dmz*, external</td>
</tr>
<tr>
<td>FortiGate-200A</td>
<td>dmz2*, external</td>
</tr>
<tr>
<td>FortiGate-300</td>
<td>dmz/ha*, external</td>
</tr>
<tr>
<td>FortiGate-300A</td>
<td>port3*, port4</td>
</tr>
<tr>
<td>FortiGate-400</td>
<td>port3*, port4/ha</td>
</tr>
<tr>
<td>FortiGate-400A</td>
<td>port3*, port4</td>
</tr>
<tr>
<td>FortiGate-500</td>
<td>ha*, port1</td>
</tr>
<tr>
<td>FortiGate-500A</td>
<td>port3*, port4</td>
</tr>
<tr>
<td>FortiGate-800 and 800F</td>
<td>ha*, port1</td>
</tr>
<tr>
<td>FortiGate-1000A and FortiGate-1000AFA2</td>
<td>port3*, port4</td>
</tr>
<tr>
<td>FortiGate-1000A-LENC</td>
<td>port3*, port4</td>
</tr>
<tr>
<td>FortiGate-3000</td>
<td>port3*, port4/ha</td>
</tr>
<tr>
<td>FortiGate-3600</td>
<td>port4*, port5/ha</td>
</tr>
<tr>
<td>FortiGate-4000</td>
<td>external*, oobm</td>
</tr>
<tr>
<td>FortiGate-5001SX and FortiGate-5001FA2</td>
<td>port9*, port10</td>
</tr>
<tr>
<td>FortiGate-5002FB2</td>
<td>port7*, port8</td>
</tr>
<tr>
<td>FortiGate-5005FA2</td>
<td>base1*, base2</td>
</tr>
</tbody>
</table>

* If both HA heartbeat interfaces are connected. The interface highest in the heartbeat interface list (marked in this table with an *) is the interface used for HA heartbeat communication.

The default heartbeat interfaces for FortiGate-5000 series modules connect FortiGate-5000 series modules through the FortiGate-5000 series chassis backplane.

In a FortiGate-5020 chassis, communication between both backplane interfaces is always supported. In a FortiGate-5050 or FortiGate-5140 chassis you must install a FortiSwitch-5003 module in slot1 for communication between the first backplane interfaces (port9 for the 5001SX, 5001FA2 and 5005FA2, port7 for the 5002FB2). In a FortiGate-5050 or FortiGate-5140 chassis you must install a FortiSwitch-5003 module in slot2 for communication between the second backplane interfaces (port10 for the 5001SX, 5001FA2 and 5005FA2, port8 for the 5002FB2).

Heartbeat interface IP addresses

You do not need to assign IP addresses to heartbeat interfaces for these interfaces to be able to process heartbeat packets. The cluster assigns virtual IP addresses to the heartbeat interfaces that are processing traffic. The primary unit heartbeat interface is assigned the IP address 10.0.0.1. The subordinate unit heartbeat interfaces are assigned the IP addresses 10.0.0.2, 10.0.0.3, and so on.
More about HA heartbeat interfaces

For best results, isolate each heartbeat interface on its own network. Heartbeat packets contain sensitive information about the cluster configuration. Also, heartbeat packets may use a considerable amount of network bandwidth and it is preferable to isolate this traffic from your user networks. The extra bandwidth used by heartbeat packets could also reduce the capacity of a FortiGate unit interface to process network traffic.

For most FortiGate models if you do not change the heartbeat interface configuration, you can isolate the default heartbeat interfaces of all of the cluster units by connecting them all to the same switch. Use one switch per heartbeat interface. If the cluster consists of two units you can connect the heartbeat interfaces together using crossover cables. For an example of how to connect heartbeat interfaces, see “Connecting a FortiGate HA cluster” on page 79. For an example of how to connect HA heartbeat interfaces for a “Connecting a FortiGate virtual cluster” on page 119.

HA heartbeat and data traffic are supported on the same cluster interface. In NAT/Route mode, if you decide to use heartbeat interfaces for processing network traffic or for a management connection, you can assign the interface any IP address. This IP address does not affect HA heartbeat traffic.

In Transparent mode, you can connect the heartbeat interface to your network and enable management access. You would then establish a management connection to the interface using the Transparent mode management IP address. This configuration does not affect HA heartbeat traffic.

VDOM partitioning

If you are configuring virtual clustering you can select the virtual domains to be in virtual cluster 1 and the virtual domains to be in virtual cluster 2. The root virtual domain must always be in virtual cluster 1.

Usually you would distribute virtual domains evenly between the two virtual clusters and configure device priorities so that traffic is distributed evenly between the cluster units. For more information, see “Virtual clustering load balancing configuration” on page 123 and “Managing a FortiGate virtual clustering configuration” on page 160.

Changing subordinate unit host name and device priority

To change the host name and device priority of a subordinate unit in an operating cluster, go to System > Config > HA to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

To change the host name and device priority of a subordinate unit in an operating cluster with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to System > Config > HA to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

You can change the host name (Peer) and device priority (Priority) of this subordinate unit. These changes only affect the configuration of the subordinate unit.
Figure 13: Changing the subordinate unit host name and device priority

<table>
<thead>
<tr>
<th>HA Peer Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
</tr>
<tr>
<td>FortiGate-A</td>
</tr>
<tr>
<td>Priority</td>
</tr>
<tr>
<td>128</td>
</tr>
</tbody>
</table>

Peer
View and optionally change the subordinate unit host name.

Priority
View and optionally change the subordinate unit device priority.
The device priority is not synchronized among cluster members. In a functioning cluster you can change device priority to change the priority of any unit in the cluster. The next time the cluster negotiates, the cluster unit with the highest device priority becomes the primary unit.
The device priority range is 0 to 255. The default device priority is 128.

config system ha (CLI command)

Use this command to enable and configure FortiGate high availability (HA) and virtual clustering. HA is supported on FortiGate and FortiWiFi models numbered 60 and higher. Using the config system ha command you must configure all cluster members with the same group name, mode, and password before the FortiGate units can form a cluster.

HA override and priority are not synchronized between cluster units. As well the FortiGate unit host name is not synchronized between cluster units. The primary unit synchronizes all other configuration settings, including the other HA configuration settings.

When virtual domains are enabled for the FortiGate units to be operating in HA mode you are configuring virtual clustering. Using virtual clustering you create two virtual clusters and add virtual domains to each cluster. Configuring virtual clustering is very similar to configuring normal HA except that in a virtual cluster, the HA mode can only be set to active-passive. As well additional options are available for adding virtual domains to each virtual cluster and for setting the device priority for each device in each virtual cluster.

Note: You cannot enable HA mode if one of the FortiGate unit interfaces uses DHCP or PPPoE to acquire an IP address. If DHCP or PPPoE is configured, the config ha mode keyword is not available.

Command syntax pattern

```
config system ha
  set arps <arp_integer>
  set authentication {disable | enable}
  set encryption {disable | enable}
  set group-id <id_integer>
  set group-name <name_str>
  set hb-interval <interval_integer>
  set hb-lost-threshold <threshold_integer>
  set hbdev <interface_names>
  set helo-holddown <holddown_integer>
```
set link-failed-signal {disable | enable}
set load-balance-all {disable | enable}
set mode {a-a | a-p | standalone}
set monitor <interface_names>
set override {disable | enable}
set password <password_str>
set priority <priority_integer>
set route-hold <hold_integer>
set route-ttl <ttl_integer>
set route-wait <wait_integer>
set schedule {hub | ip | ipport | leastconnection | none | random | round-robin | weight-round-robin}
set session-pickup {disable | enable}
set sync-config {disable | enable}
set uninterruptable-upgrade {disable | enable}
set weight <priority-id_integer> <weight_integer>
set vdom <vdom_names>
set vcluster2 {disable | enable}
end
config secondary-vcluster
  set monitor <interface_names>
  set override {disable | enable}
  set priority <priority_integer>
  set vdom <vdom_names>
end

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>arps &lt;arp_integer&gt;</td>
<td>Set the number of gratuitous ARP packets sent by the primary unit. Gratuitous ARP packets are sent when a cluster unit becomes a primary unit. The gratuitous ARP packets configure connected networks to associate the cluster virtual MAC address with the cluster IP address. The range is 1 to 16 gratuitous ARP packets. Normally you would not need to change the number of gratuitous ARP packets.</td>
<td>5</td>
</tr>
<tr>
<td>authentication {disable</td>
<td>enable}</td>
<td>Enable/disable HA heartbeat message authentication. Enabling HA heartbeat message authentication prevents an attacker from creating false HA heartbeat messages. False HA heartbeat messages could affect the stability of the cluster.</td>
</tr>
<tr>
<td>encryption {disable</td>
<td>enable}</td>
<td>Enable/disable HA heartbeat message encryption. Enabling HA heartbeat message encryption prevents an attacker from sniffing HA packets to get HA cluster information.</td>
</tr>
<tr>
<td>group-id &lt;id_integer&gt;</td>
<td>The HA group ID. The group ID range is from 0 to 63. All members of the HA cluster must have the same group ID. Changing the Group ID changes the cluster virtual MAC address. See “Cluster virtual MAC addresses” on page 31.</td>
<td>0</td>
</tr>
<tr>
<td>group-name &lt;name_str&gt;</td>
<td>The HA group name. All cluster members must have the same group name.</td>
<td>FGT-HA</td>
</tr>
</tbody>
</table>
hb-lost-threshold
<threshold_integer>
The lost heartbeat threshold, which is the number of seconds to wait to receive a heartbeat packet from another cluster unit before assuming that the cluster unit has failed. The lost heartbeat threshold range is 1 to 60 seconds.

If the primary cluster unit does not receive a heartbeat packet from a subordinate unit before the heartbeat threshold expires, the primary unit assumes that the subordinate unit has failed.

If a subordinate unit does not receive a heartbeat packet from the primary unit before the heartbeat threshold expires, the subordinate unit assumes that the primary unit has failed. The subordinate unit then begins negotiating to become the new primary unit.

The lower the lost heartbeat interval the faster the cluster responds to a failure. However, you can increase the heartbeat lost threshold if repeated failovers occur because cluster units cannot send heartbeat packets quickly enough.

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hb-lost-threshold</td>
<td>The lost heartbeat threshold, which is the number of seconds to wait to receive a heartbeat packet from another cluster unit before assuming that the cluster unit has failed. The lost heartbeat threshold range is 1 to 60 seconds. If the primary cluster unit does not receive a heartbeat packet from a subordinate unit before the heartbeat threshold expires, the primary unit assumes that the subordinate unit has failed. If a subordinate unit does not receive a heartbeat packet from the primary unit before the heartbeat threshold expires, the subordinate unit assumes that the primary unit has failed. The subordinate unit then begins negotiating to become the new primary unit. The lower the lost heartbeat interval the faster the cluster responds to a failure. However, you can increase the heartbeat lost threshold if repeated failovers occur because cluster units cannot send heartbeat packets quickly enough.</td>
<td>20</td>
</tr>
</tbody>
</table>

hb-interval
<interval_integer>
The heartbeat interval, which is the time between sending heartbeat packets. The heartbeat interval range is 1 to 20 (100*ms).

A heartbeat interval of 2 means the time between heartbeat packets is 200 ms. Changing the heartbeat interval to 5 changes the time between heartbeat packets to 500 ms.

The HA heartbeat packets consume more bandwidth if the hb-interval is short. But if the hb-interval is very long, the cluster is not as sensitive to topology and other network changes.

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hb-interval</td>
<td>The heartbeat interval, which is the time between sending heartbeat packets. The heartbeat interval range is 1 to 20 (100*ms). A heartbeat interval of 2 means the time between heartbeat packets is 200 ms. Changing the heartbeat interval to 5 changes the time between heartbeat packets to 500 ms. The HA heartbeat packets consume more bandwidth if the hb-interval is short. But if the hb-interval is very long, the cluster is not as sensitive to topology and other network changes.</td>
<td>2</td>
</tr>
<tr>
<td>Keywords and variables</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>hbdev &lt;interface_names&gt;</td>
<td>Select the FortiGate interfaces to be heartbeat interfaces. By default HA heartbeat is set for two interfaces. Use the <code>get</code> command to display the heartbeat interface configuration for your FortiGate unit (or see Table 7 on page 56). In most cases you can maintain the default <code>hbdev</code> configuration as long as you can connect the <code>hbdev</code> interfaces together. HA heartbeat hello packets are constantly sent by all of the configured heartbeat interfaces. Using these hello packets, each cluster unit confirms that the other cluster units are still operating. The FGCP selects one of the heartbeat interfaces to be used for communication between the cluster units. The FCGP selects the heartbeat interface to be used based on the linkfail states of the heartbeat interfaces and on the interface index. When you enter <code>set hbdev ?</code> the FortiGate CLI lists the heartbeat interfaces in alphabetical order. This order corresponds to the interface index order. The selected heartbeat interface that is highest in the interface list (or first in alphabetical order) is used for heartbeat communication between cluster units. If this interface fails or becomes disconnected, the interface that is next highest in the list (or next in alphabetical order) handles all HA heartbeat communication. The heartbeat interface that is higher in the interface list resumes processing all HA heartbeat communication if it becomes connected again. To change the heartbeat interface configuration, enter the names of the interfaces to be used as heartbeat interfaces. Use a space to separate each interface name. If you want to remove an interface from the list or add an interface to the list, you must retype the entire updated list. You can enable heartbeat communications for physical interfaces. You cannot enable heartbeat communications for VLAN subinterfaces, for IPSec VPN interfaces, for redundant interfaces, or for 802.3ad aggregated interfaces. Enabling the HA heartbeat for more interfaces increases reliability. If an interface fails, the HA heartbeat can be diverted to another interface. HA heartbeat traffic can use a considerable amount of network bandwidth. If possible, enable HA heartbeat traffic on interfaces only used for HA heartbeat traffic or on interfaces connected to less busy networks. Heartbeat communication must be enabled on at least one interface. If heartbeat communication is interrupted the cluster stops processing traffic.</td>
<td>Depends on the FortiGate model. See Table 7 on page 56.</td>
</tr>
<tr>
<td>helo-holddown &lt;holddown_integer&gt;</td>
<td>The hello state hold-down time, which is the number of seconds that a cluster unit waits before changing from hello state to work state. A cluster unit changes from hello state to work state when it starts up. The hello state hold-down time range is 5 to 300 seconds.</td>
<td>20</td>
</tr>
</tbody>
</table>
### Keywords and variables

<table>
<thead>
<tr>
<th>Command syntax pattern</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-failed-signal</td>
<td>Enable or disable shutting down all primary unit interfaces (except for heartbeat device interfaces) for one second when a link failover occurs. If all interfaces are not shut down in this way, some switches may not detect that the primary unit has become a subordinate unit and may keep sending packets to the former primary unit. If the primary unit interfaces are shut down for one second, connected switches should be able to detect this failure and clear their MAC forwarding tables (also called arp tables). Then, when the new primary unit is operating, the switches can detect the gratuitous arp packets sent by the new primary unit and update their MAC forwarding tables correctly.</td>
<td>disable</td>
</tr>
<tr>
<td>load-balance-all</td>
<td>If mode is set to a-a, configure active-active HA to load balance TCP and virus scanning sessions or to load balance virus scanning sessions only. Enter enable to load balance TCP and virus scanning sessions. Enter disable to load balance only virus scanning sessions. UDP, ICMP, multicast, and broadcast traffic is never load balanced and is always processed by the primary unit.</td>
<td>disable</td>
</tr>
<tr>
<td>mode</td>
<td>Set the HA mode. Enter a-p to create an Active-Passive HA cluster, in which the primary cluster unit is actively processing all connections and the others are passively monitoring the status and remaining synchronized with the primary cluster unit. Enter a-a to create an Active-Active HA cluster, in which each cluster unit is actively processing connections and monitoring the status of the other FortiGate units. All members of an HA cluster must be set to the same HA mode. Enter standalone to remove the FortiGate unit from an HA cluster. Not available if a FortiGate interface mode is set to dhcp or pppoe. a-a mode is not available for virtual clusters.</td>
<td>standalone</td>
</tr>
<tr>
<td>monitor</td>
<td>Enable or disable port monitoring for link failure. Port monitoring monitors FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks. Enter the names of the interfaces to monitor. Use a space to separate each interface name. If you want to remove an interface from the list or add an interface to the list you must retype the list with the names changed as required. You can monitor physical interfaces, redundant interfaces, and 802.3ad aggregated interfaces but not VLAN subinterfaces or IPSec VPN interfaces. You cannot monitor interfaces that are 4-port switches. This includes the internal interface of FortiGate models 60, 60M, 100A, 200A, and FortiWiFi-60. This also includes the LAN interface of the FortiGate-500A.</td>
<td>No default</td>
</tr>
</tbody>
</table>
Override {disable | enable}

Enable or disable forcing the cluster to renegotiate and select a new primary unit every time a cluster unit leaves or joins a cluster, changes status within a cluster, or every time the HA configuration of a cluster unit changes.

If you are configuring virtual clustering you can configure override to enable or disable forcing virtual cluster 1 or virtual cluster 2 to renegotiate every time a unit leaves or joins the virtual cluster, changes status within the virtual cluster, or every time the configuration of the virtual cluster changes.

For example, in a functioning cluster you can edit the configuration of a subordinate unit and make its device priority higher than that priority of the current primary unit. You might want to do this so that the subordinate unit becomes the new primary unit. However, the subordinate unit will not become the primary unit until the cluster renegotiates.

If override is enabled the cluster renegotiates as soon as you change the subordinate unit device priority. The subordinate unit immediately becomes the new primary unit. If override is not enabled, the subordinate unit does not become the new primary unit until the cluster renegotiates, which may not happen until a failover or reboot occurs.

```
password <password_str>
```

Enter a password for the HA cluster. The password must be the same for all FortiGate units in the cluster. The maximum password length is 15 characters.

If you have more than one FortiGate HA cluster on the same network, each cluster must have a different password.

```
priority <priority_integer>
```

Change the device priority of the cluster unit. Each cluster unit can have a different device priority (the device priority is not synchronized among cluster members). During HA negotiation, the unit with the highest device priority becomes the primary cluster unit. The device priority range is 0 to 255.

You can use the device priority to control the order in which cluster units become the primary cluster unit when a cluster unit fails. If you are configuring a virtual cluster, if you have added virtual domains to both virtual clusters, you can set the priority that the cluster unit has in virtual cluster 1 and virtual cluster 2. If a cluster unit has different device priorities in virtual cluster 1 and virtual cluster 2, the cluster unit may be the primary unit in one virtual cluster and the subordinate unit in the other.

```
route-hold <hold_integer>
```

The time that the primary unit waits between sending routing table updates to subordinate units in a cluster.

The route hold range is 0 to 3600 seconds. To avoid flooding routing table updates to subordinate units, set route-hold to a relatively long time to prevent subsequent updates from occurring too quickly.

The route-hold time should be coordinated with the route-wait time. See the route-wait description for more information.
**Command syntax pattern**

**Configuration reference**

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-ttl &lt;ttl_integer&gt;</td>
<td>The time to live for routes in a cluster unit routing table. The time to live range is 0 to 3600 seconds. The time to live controls how long routes remain active in a cluster unit routing table after the cluster unit becomes a primary unit. To maintain communication sessions after a cluster unit becomes a primary unit, routes remain active in the routing table for the route time to live while the new primary unit acquires new routes. Normally, the route-ttl is 0 and the primary unit must acquire new routes before it can continue processing traffic. Normally acquiring new routes occurs very quickly so only a minor delay is caused by acquiring new routes. If the primary unit needs to acquire a very large number of routes, or if for other reasons, there is a delay in acquiring all routes, the primary unit may not be able to maintain all communication sessions. You can increase the route time to live if communication sessions are lost after a failover so that the primary unit can use routes that are already in the routing table, instead of waiting to acquire new routes.</td>
<td>0</td>
</tr>
<tr>
<td>route-wait &lt;wait_integer&gt;</td>
<td>The time the primary unit waits after receiving a routing table update before sending the update to the subordinate units in the cluster. For quick routing table updates to occur, set route-wait to a relatively short time so that the primary unit does not hold routing table changes for too long before updating the subordinate units. The route-wait range is 0 to 3600 seconds. Normally, because the route-wait time is 0 seconds the primary unit sends routing table updates to the subordinate units every time the primary unit routing table changes. Once a routing table update is sent, the primary unit waits the route-hold time before sending the next update. Usually routing table updates are periodic and sporadic. Subordinate units should receive these changes as soon as possible so route-wait is set to 0 seconds. route-hold can be set to a relatively long time because normally the next route update would not occur for a while. In some cases, routing table updates can occur in bursts. A large burst of routing table updates can occur if a router or a link on a network fails or changes. When a burst of routing table updates occurs, there is a potential that the primary unit could flood the subordinate units with routing table updates. Setting route-wait to a longer time reduces the frequency with which additional routing updates are sent, which prevents flooding of routing table updates from occurring.</td>
<td>0</td>
</tr>
</tbody>
</table>
### Keywords and variables

<table>
<thead>
<tr>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>schedule</strong> {<strong>hub</strong></td>
<td><strong>ip</strong></td>
</tr>
<tr>
<td>Active-active load balancing schedule. If the cluster interfaces are connected to switches, use <strong>ip</strong> to distribute traffic to units in a cluster based on the Source IP and Destination IP of the packet. If the cluster units are connected using switches, use <strong>ipport</strong> to distribute traffic to units in a cluster based on the Source IP, source port, destination IP, and destination port of the packet. If the cluster units are connected using switches, use <strong>leastconnection</strong> to distribute traffic to the cluster unit currently processing the fewest connections. If the cluster units are connected using switches, use <strong>none</strong> to distribute traffic to units in a cluster based on their capacity and on how many connections they are currently processing. Weighted round robin distributes traffic more evenly because units that are not processing traffic are more likely to receive new connections than units that are very busy. You can optionally use the <strong>weight</strong> keyword to set a weighting for each cluster unit.</td>
<td><strong>round-robin</strong></td>
</tr>
<tr>
<td><strong>session-pickup</strong> {<strong>disable</strong></td>
<td><strong>enable</strong>}</td>
</tr>
</tbody>
</table>
### Command syntax pattern

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sync-config {disable</td>
<td>enable}</td>
<td>Enable or disable automatic synchronization of primary unit configuration changes to all cluster units.</td>
</tr>
<tr>
<td>uninterruptable-</td>
<td>Uninterruptable upgrade {disable</td>
<td>enable} (disable</td>
</tr>
<tr>
<td>weight &lt;priority-id_integer&gt; &lt;weight_integer&gt;</td>
<td>The weighted round robin load balancing weight to assign to each cluster unit. When you set schedule to weight-round-robin, you can use the weight keyword to set the weight of each cluster unit. The weight is set according to the priority of the unit in the cluster. A FortiGate HA cluster can contain up to 32 FortiGate units so you can set up to 32 weights. The default weight of 1 1 1 1 means that the first four units in the cluster all have the same weight of 1. priority-id_integer is a number from 0 to 31 that identifies the priority of the cluster unit. weight_integer is a number between 0 and 31 that is the weight assigned to the cluster units according to their priority in the cluster. Increase the weight to increase the number of connections processed by the cluster unit with that priority. weight is available when mode is set to a-a and schedule is set to weight-round-robin.</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>vdom &lt;vdom_names&gt;</td>
<td>Add virtual domains to virtual cluster 1 or virtual cluster 2. Virtual cluster 2 is also called the secondary virtual cluster. In the config system ha shell, use set vdom to add virtual domains to virtual cluster 1. Adding a virtual domain to virtual cluster 1 removes it from virtual cluster 2. In the config secondary-vcluster shell, use set vdom to add virtual domains to virtual cluster 2. Adding a virtual domain to virtual cluster 2 removes it from virtual cluster 1. You can use vdom to add virtual domains to a virtual cluster in any combination. You can add virtual domains one at a time or you can add multiple virtual domains at a time. For example, entering set vdom domain_1 followed by set vdom domain_2 has the same result as entering set vdom domain_1 domain_2.</td>
<td>All virtual domains are added to virtual cluster 1.</td>
</tr>
</tbody>
</table>
Examples

This example shows how to configure a FortiGate unit for active-active HA operation. The example shows how to set up a basic HA configuration by setting the HA mode, changing the group-name, and entering a password. You would enter the exact same commands on every FortiGate unit in the cluster. In the example virtual domains are not enabled.

```plaintext
config system ha
  set mode a-a
  set group-name myname
  set password HApass
end
```

The following example shows how to configure a FortiGate unit with virtual domains enabled for active-passive HA operation. In the example, the FortiGate unit is configured with three virtual domains (domain_1, domain_2, and domain_3) in addition to the root virtual domain. The example shows how to set up a basic HA configuration similar to the previous example; except that the HA mode can only be set to a-p. In addition, the example shows how to enable vcluster2 and how to add the virtual domains domain_2 and domain_3 to vcluster2.

```plaintext
config global
  config system ha
    set mode a-p
    set group-name myname
    set password HApass
    set set vcluster2 enable
  config secondary-vcluster
    set vdom domain_2 domain_3
  end
end
```

The following example shows how to change the device priority of the primary unit to 200 so that this cluster unit always becomes the primary unit. When you log into the cluster you are actually connecting to the primary unit. When you change the device priority of the primary unit this change only affects the primary unit because the device priority is not synchronized to all cluster units. After you enter the following commands the cluster renegotiates and may select a new primary unit.

```plaintext
vcluster2 {disable | enable}
```

Enable or disable virtual cluster 2. In the global virtual domain configuration, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use config secondary-cluster to configure virtual cluster 2.

Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcluster2 {disable</td>
<td>Enable or disable virtual cluster 2. In the global virtual domain configuration, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use config secondary-cluster to configure virtual cluster 2. Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.</td>
<td>disable</td>
</tr>
<tr>
<td>config secondary-</td>
<td>Configure virtual cluster 2. You must enable vcluster2. Then you can use config secondary-vcluster to set monitor, override, priority, and vdom for virtual cluster 2.</td>
<td>Same defaults as virtual cluster 1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcluster2 {disable</td>
<td>Enable or disable virtual cluster 2. In the global virtual domain configuration, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use config secondary-cluster to configure virtual cluster 2. Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.</td>
<td>disable</td>
</tr>
<tr>
<td>config secondary-</td>
<td>Configure virtual cluster 2. You must enable vcluster2. Then you can use config secondary-vcluster to set monitor, override, priority, and vdom for virtual cluster 2.</td>
<td>Same defaults as virtual cluster 1.</td>
</tr>
</tbody>
</table>

Examples

This example shows how to configure a FortiGate unit for active-active HA operation. The example shows how to set up a basic HA configuration by setting the HA mode, changing the group-name, and entering a password. You would enter the exact same commands on every FortiGate unit in the cluster. In the example virtual domains are not enabled.

```plaintext
config system ha
  set mode a-a
  set group-name myname
  set password HApass
end
```

The following example shows how to configure a FortiGate unit with virtual domains enabled for active-passive HA operation. In the example, the FortiGate unit is configured with three virtual domains (domain_1, domain_2, and domain_3) in addition to the root virtual domain. The example shows how to set up a basic HA configuration similar to the previous example; except that the HA mode can only be set to a-p. In addition, the example shows how to enable vcluster2 and how to add the virtual domains domain_2 and domain_3 to vcluster2.

```plaintext
config global
  config system ha
    set mode a-p
    set group-name myname
    set password HApass
    set set vcluster2 enable
  config secondary-vcluster
    set vdom domain_2 domain_3
  end
end
```

The following example shows how to change the device priority of the primary unit to 200 so that this cluster unit always becomes the primary unit. When you log into the cluster you are actually connecting to the primary unit. When you change the device priority of the primary unit this change only affects the primary unit because the device priority is not synchronized to all cluster units. After you enter the following commands the cluster renegotiates and may select a new primary unit.

```plaintext
vcluster2 {disable | enable}
```

Enable or disable virtual cluster 2. In the global virtual domain configuration, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use config secondary-cluster to configure virtual cluster 2.

Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcluster2 {disable</td>
<td>Enable or disable virtual cluster 2. In the global virtual domain configuration, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use config secondary-cluster to configure virtual cluster 2. Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.</td>
<td>disable</td>
</tr>
<tr>
<td>config secondary-</td>
<td>Configure virtual cluster 2. You must enable vcluster2. Then you can use config secondary-vcluster to set monitor, override, priority, and vdom for virtual cluster 2.</td>
<td>Same defaults as virtual cluster 1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcluster2 {disable</td>
<td>Enable or disable virtual cluster 2. In the global virtual domain configuration, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use config secondary-cluster to configure virtual cluster 2. Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.</td>
<td>disable</td>
</tr>
<tr>
<td>config secondary-</td>
<td>Configure virtual cluster 2. You must enable vcluster2. Then you can use config secondary-vcluster to set monitor, override, priority, and vdom for virtual cluster 2.</td>
<td>Same defaults as virtual cluster 1.</td>
</tr>
</tbody>
</table>
config system ha
    set priority 200
end

The following example shows how to change the device priority of a subordinate unit to 255 so that this subordinate unit becomes the primary unit. This example involves connecting to the cluster CLI and using the `execute ha manage 0` command to connect to the highest priority subordinate unit. After you enter the following commands the cluster renegotiates and selects a new primary unit.

`execute ha manage 0`
`config system ha
    set priority 255
end`

The following example shows how to change the device priority of the primary unit in virtual cluster 2. The example involves connecting to the virtual cluster CLI and changing the global configuration. In the example virtual cluster 2 has already been enabled so all you have to do is use the `config secondary-vcluster` command to configure virtual cluster 2.

`config global`
`config system ha`
    `config secondary-vcluster
    set priority 50
end`
end

The following example shows how to change the default HA heartbeat device configuration so that port4 and port1 are used for HA heartbeat communication.

`config system ha
    set hbdev port4 port1
end`

The following example shows how to enable monitoring for the external, internal, and DMZ interfaces.

`config system ha
    set monitor external internal dmz
end`

The following example shows how to configure weighted round robin weights for a cluster of three FortiGate units. You can enter the following commands to configure the weight values for each unit:

```
<table>
<thead>
<tr>
<th>Cluster unit priority</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
```

Table 8: Example weights for three cluster units
These commands have the following results:

- The first connection is processed by the primary unit (priority 0, weight 1)
- The next three connections are processed by the first subordinate unit (priority 1, weight 3)
- The next three connections are processed by the second subordinate unit (priority 2, weight 3)

The subordinate units process more connections than the primary unit, and both subordinate units, on average, process the same number of connections.

This example shows how to display the settings for the `system ha` command.

```
get system ha
```

This example shows how to display the configuration for the `system ha` command.

```
show system ha
```

get system ha status (CLI command)

Use this command to display information about an HA cluster. The command displays general HA configuration settings. The command also displays information about how the cluster unit that you have logged into is operating in the cluster.

Usually you would log into the primary unit CLI using SSH or telnet. In this case the `get system ha status` command displays information about the primary unit first, and also displays the HA state of the primary unit (the primary unit operates in the work state). However, if you log into the primary unit and then use the `execute ha manage` command to log into a subordinate unit, (or if you use a console connection to log into a subordinate unit) the `get system status` command displays information about this subordinate unit first, and also displays the HA state of this subordinate unit. The state of a subordinate unit is work for an active-active cluster and standby for an active-passive cluster.

For a virtual cluster configuration, the `get system ha status` command displays information about how the cluster unit that you have logged into is operating in virtual cluster 1 and virtual cluster 2. For example, if you connect to the cluster unit that is the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2, the output of the `get system ha status` command shows virtual cluster 1 in the work state and virtual cluster 2 in the standby state. The `get system ha status` command also displays additional information about virtual cluster 1 and virtual cluster 2.

Command syntax pattern

```
get system ha status
```
The command display includes the following fields. For more information see the examples that follow.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>The FortiGate model number.</td>
</tr>
<tr>
<td>Mode</td>
<td>The HA mode of the cluster: a-a or a-p.</td>
</tr>
<tr>
<td>Group</td>
<td>The group ID of the cluster.</td>
</tr>
<tr>
<td>Debug</td>
<td>The debug status of the cluster.</td>
</tr>
<tr>
<td>ses_pickup</td>
<td>The status of session pickup: enable or disable.</td>
</tr>
<tr>
<td>load balance</td>
<td>The status of the load-balance-all keyword: enable or disable. Relevant to active-active clusters only.</td>
</tr>
<tr>
<td>schedule</td>
<td>The active-active load balancing schedule. Relevant to active-active clusters only.</td>
</tr>
<tr>
<td>Master</td>
<td>Master displays the device priority, host name, serial number, and cluster index of the primary (or master) unit.</td>
</tr>
<tr>
<td>Slave</td>
<td>Slave displays the device priority, host name, serial number, and cluster index of the subordinate (or slave, or backup) unit or units.</td>
</tr>
<tr>
<td>number of vcluster</td>
<td>The number of virtual clusters. If virtual domains are not enabled, the cluster has one virtual cluster. If virtual domains are enabled the cluster has two virtual clusters.</td>
</tr>
<tr>
<td>vcluster 1</td>
<td>The HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 1. If virtual domains are not enabled, vcluster 1 displays information for the cluster. If virtual domains are enabled, vcluster 1 displays information for virtual cluster 1. The HA heartbeat IP address is 10.0.0.2 if you are logged into a the primary unit of virtual cluster 1 and 10.0.0.1 if you are logged into a subordinate unit of virtual cluster 1. vcluster 1 also lists the primary unit (master) and subordinate units (slave) in virtual cluster 1. The list includes the cluster index and serial number of each cluster unit in virtual cluster 1. The cluster unit that you have logged into is at the top of the list. If virtual domains are not enabled and you connect to the primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the primary unit. If virtual domains are not enabled and you connect to a subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you have logged into. If virtual domains are enabled and you connect to the virtual cluster 1 primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the virtual cluster 1 primary unit. If virtual domains are enabled and you connect to the virtual cluster 1 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you are logged into.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the `get system ha status` output for a cluster of two FortiGate-5001 units operating in active-active mode. The cluster group ID, session pickup, load balance all, and the load balancing schedule are all set to the default values. The device priority of the primary unit is also set to the default value. The device priority of the subordinate unit has been reduced to 100. The host name of the primary unit is 5001_Slot_4. The host name of the subordinate unit is 5001_Slot_3.

The command output was produced by connecting to the primary unit CLI (host name 5001_Slot_4).

```
Model: 5000
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
load_balance: disable
schedule: round robin
Master:128 5001_Slot_4      FG50012204400045 1
Slave :100 5001_Slot_3      FG50012205400050 0
number of vcluster: 1
vcluster 1: work 10.0.0.2
Master:0 FG50012204400045
Slave :1 FG50012205400050
```

The following command output was produced by using `execute HA manage 0` to log into the subordinate unit CLI of the cluster shown in the previous example. The host name of the subordinate unit is 5001_Slot_3.

```
Model: 5000
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
load_balance: disable
schedule: round robin
```

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcluster 2</td>
<td>only appears if virtual domains are enabled.</td>
</tr>
<tr>
<td>vcluster 2</td>
<td>displays the HA state (hello, work, or standby)</td>
</tr>
<tr>
<td></td>
<td>and HA heartbeat IP address of the cluster unit that you have logged into in</td>
</tr>
<tr>
<td></td>
<td>virtual cluster 2. The HA heartbeat IP address is 10.0.0.2 if you are</td>
</tr>
<tr>
<td></td>
<td>logged into the primary unit of virtual cluster 2 and 10.0.0.1 if you are</td>
</tr>
<tr>
<td></td>
<td>logged into a subordinate unit of virtual cluster 2.</td>
</tr>
<tr>
<td></td>
<td>vcluster 2 also lists the primary unit (master) and</td>
</tr>
<tr>
<td></td>
<td>subordinate units (slave) in virtual cluster 2. The list includes the</td>
</tr>
<tr>
<td></td>
<td>cluster index and serial number of each cluster unit in virtual cluster 2.</td>
</tr>
<tr>
<td></td>
<td>The cluster unit that you have logged into is at the top of the list.</td>
</tr>
</tbody>
</table>

If you connect to the virtual cluster 2 primary unit CLI, the HA state of the cluster unit in virtual cluster 2 is `work`. The display lists the cluster units starting with the virtual cluster 2 primary unit.

If you connect to the virtual cluster 2 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 2 is `standby`. The display lists the cluster units starting with the subordinate unit that you are logged into.
The following example shows `get system ha status` output for a cluster of three FortiGate-5001 units operating in active-passive mode. The cluster group ID is set to 20 and session pickup is enabled. Load balance all and the load balancing schedule are set to the default value. The device priority of the primary unit is set to 200. The device priorities of the subordinate units are set to 128 and 100. The host name of the primary unit is `5001_Slot_5`. The host names of the subordinate units are `5001_Slot_3` and `5001_Slot_4`.

Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Master:200 5001_Slot_5 FG50012206400112 0
Slave :100 5001_Slot_3 FG50012205400050 1
Slave :128 5001_Slot_4 FG50012204400045 2
number of vcluster: 1
vcluster 1: work 10.0.0.2

The following example shows `get system ha status` output for a cluster of two FortiGate-5001 units with virtual clustering enabled. This command output was produced by logging into the primary unit for virtual cluster 1 (hostname: `5001_Slot_4`, serial number FG50012204400045).

The virtual clustering output shows that the cluster unit with host name `5001_Slot_4` and serial number FG50012204400045 is operating as the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2.

For virtual cluster 1 the cluster unit that you have logged into is operating in the work state and the serial number of the primary unit for virtual cluster 1 is FG50012204400045. For virtual cluster 2 the cluster unit that you have logged into is operating in the standby state and the serial number of the primary unit for virtual cluster 2 is FG50012205400050.

Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Master:128 5001_Slot_4 FG50012204400045 1
Slave :100 5001_Slot_3 FG50012205400050 0
number of vcluster: 2
vcluster 1: work 10.0.0.2
The following example shows `get system ha status` output for the same cluster as shown in the previous example after using `execute ha manage 0` to log into the primary unit for virtual cluster 2 (hostname: 5001_Slot_3, serial number FG50012205400050).

```
Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Slave :100 5001_Slot_3      FG50012205400050 0
Master:128 5001_Slot_4      FG50012204400045 1
number of vcluster: 2
  vcluster 1: standby 10.0.0.2
  Slave :1 FG50012205400050
  Master:0 FG50012204400045
  vcluster 2: work 10.0.0.1
  Slave :1 FG50012204400045
  Master:0 FG50012205400050
Slave :1 FG50012204400045
```

The following example shows `get system ha status` output for a virtual cluster configuration where the cluster unit with hostname: 5001_Slot_4 and serial number FG50012204400045 is the primary unit for both virtual clusters. This command output is produced by logging into cluster unit with host name 5001_Slot_4 and serial number FG50012204400045.

```
Model: 5000
Mode: a-p
Group: 20
Debug: 0
ses_pickup: enable
load_balance: disable
schedule: round robin
Master:128 5001_Slot_4      FG50012204400045 1
Slave :100 5001_Slot_3      FG50012205400050 0
number of vcluster: 2
  vcluster 1: work 10.0.0.2
  Master:0 FG50012204400045
  Slave :1 FG50012205400050
  vcluster 2: work 10.0.0.2
  Master:0 FG50012204400045
  Slave :1 FG50012205400050
```
execute ha disconnect (CLI command)

Use this command to disconnect a FortiGate unit from a functioning cluster. You must specify the serial number of the unit to be disconnected. You must also specify an interface name and assign an IP address and netmask to this interface of the disconnected unit. You can disconnect any unit from the cluster even the primary unit. After the unit is disconnected the cluster responds as if the disconnected unit has failed. The cluster may renegotiate and may select a new primary unit.

To disconnect the unit from the cluster, the execute ha disconnect command sets the HA mode of the disconnected unit to standalone. In addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0. The interface specified in the command is set to the IP address and netmask that you specify in the command. In addition all management access to this interface is enabled. Once the FortiGate unit is disconnected you can use SSH, telnet, HTTPS, or HTTP to connect to and manage the FortiGate unit.

Otherwise the configuration of the disconnected unit is not changed. The HA configuration of the disconnected unit is not changed either. You can reconnect the disconnected unit to the cluster by using the config system ha command to set the mode of the disconnected unit to match the HA mode of the cluster. Usually the disconnected unit rejoins the cluster as a subordinate unit and the disconnected unit’s configuration is synchronized with the primary unit.

**Caution:** You should make sure that the device priority of the disconnected unit is lower than the device priority of the current primary unit and that override is not enabled. Otherwise, when the disconnected joins the cluster, the cluster will renegotiate and the disconnected unit may become the primary unit. If this happens, the configuration of the disconnected unit is synchronized to all other cluster units. This configuration change might disrupt the operation of the cluster.

**Command syntax**

```
execute ha disconnect <cluster-member-serial_str>
    <interface_str> <address_ipv4> <address_ipv4mask>
```

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-member-serial_str</td>
<td>The serial number of the cluster unit to be disconnected.</td>
</tr>
<tr>
<td>interface_str</td>
<td>The name of the interface to configure. The command configures the IP address and netmask for this interface and enables all management access for this interface.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to disconnect a cluster unit with serial number FGT5002803033050. The internal interface of the disconnected unit is set to IP address 1.1.1.1 and netmask 255.255.255.0.

```
estimate ha disconnect FGT5002803033050 internal 1.1.1.1 255.255.255.0
```
execute ha manage (CLI command)

Use this command from the CLI of a FortiGate unit in an HA cluster to log into the CLI of another unit in the cluster. Usually you would use this command from the CLI of the primary unit to log into the CLI of a subordinate unit. However, if you have logged into a subordinate unit CLI, you can use this command to log into the primary unit CLI, or the CLI of another subordinate unit.

You can use CLI commands to manage the cluster unit that you have logged into. If you make changes to the configuration of any cluster unit (primary or subordinate unit) these changes are synchronized to all cluster units.

Command syntax

```
execute ha manage <cluster-index>
```

<table>
<thead>
<tr>
<th>Keywords and variables</th>
<th>Description</th>
</tr>
</thead>
</table>
| cluster-index          | The cluster index number of the cluster unit to log into. The first subordinate unit has a cluster index of zero. If there are more subordinate units their index numbers are 1, 2, and so on. The primary unit has the highest index number. So in a cluster of three FortiGate units:
  • The first subordinate unit has a cluster index of 0
  • The second subordinate unit has a cluster index of 1
  • The primary unit has a cluster index of 2
Enter ? to list the cluster units that you can log into. The list does not show the unit that you are already logged into.

Examples

This example shows how to log into a subordinate unit in a cluster of three FortiGate units. In this example you have already logged into the primary unit. The primary unit has serial number FGT3082103000056. The subordinate units have serial numbers FGT3012803021709 and FGT3082103021989.

```
execute ha manage ?
<id> please input slave cluster index.
<0> Subsidary unit FGT3012803021709
<1> Subsidary unit FGT3082103021989
```

Type 0 and press enter to connect to the subordinate unit with serial number FGT3012803021709. The CLI prompt changes to the host name of this unit. To return to the primary unit, type `exit`.

From the subordinate unit you can also use the `execute ha manage` command to log into the primary unit or into another subordinate unit. Enter the following command:

```
execute ha manage ?
<id> please input slave cluster index.
<0> Subsidary unit FGT3012803021709
<1> Subsidary unit FGT3082103021989
<2> Subsidary unit FGT3082103000056
```

Type 2 and press enter to log into the primary unit or type 1 and press enter to log into the other subordinate unit. The CLI prompt changes to the host name of this unit.
execute ha synchronize (CLI command)

Use this command from a subordinate unit in an HA cluster to manually synchronize its configuration with the primary unit. Using this command you can synchronize the following:

- Configuration changes made to the primary unit (normal system configuration, firewall configuration, VPN configuration and so on stored in the FortiGate configuration file),
- Antivirus engine and antivirus definition updates received by the primary unit from the FortiGuard Distribution Network (FDN),
- IPS attack definition updates received by the primary unit from the FDN,
- Web filter lists added to or changed on the primary unit,
- Email filter lists added to or changed on the primary unit,
- Certification Authority (CA) certificates added to the primary unit,
- Local certificates added to the primary unit.

You can also use the `start` and `stop` keywords to force the cluster to synchronize its configuration or to stop a synchronization process that is in progress.

**Command syntax**

```
execute ha synchronize {config| avupd| attackdef| weblists| emaillists| ca| localcert| all | start | stop}
```

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Synchronize the FortiGate configuration.</td>
</tr>
<tr>
<td>avupd</td>
<td>Synchronize the antivirus engine and antivirus definitions.</td>
</tr>
<tr>
<td>attackdef</td>
<td>Synchronize attack definitions.</td>
</tr>
<tr>
<td>weblists</td>
<td>Synchronize web filter lists.</td>
</tr>
<tr>
<td>emaillists</td>
<td>Synchronize email filter lists.</td>
</tr>
<tr>
<td>ca</td>
<td>Synchronize CA certificates.</td>
</tr>
<tr>
<td>localcert</td>
<td>Synchronize local certificates.</td>
</tr>
<tr>
<td>all</td>
<td>Synchronize all of the above.</td>
</tr>
<tr>
<td>start</td>
<td>Start synchronizing the cluster configuration.</td>
</tr>
<tr>
<td>stop</td>
<td>Stop the cluster from completing synchronizing its configuration.</td>
</tr>
</tbody>
</table>

**Example**

From the CLI of a subordinate unit, use the following commands to synchronize the antivirus and attack definitions on the subordinate FortiGate unit with the primary unit after the FDN has pushed new definitions to the primary unit.

```
execute ha synchronize avupd
execute ha synchronize attackdef
```
Configuring and connecting HA clusters

This chapter contains general procedures and descriptions as well as detailed configuration examples that describe how to configure FortiGate HA clusters. The examples in this chapter include example values only. In most cases you will substitute your own values. The examples in this chapter also do not contain detailed descriptions of configuration parameters. For information about FortiGate HA configuration parameters, see your FortiGate unit online help or “Configuration reference” on page 49.

This chapter contains the following sections:

• About the procedures in this chapter
• Configuring and connecting an HA cluster
• Basic NAT/Route mode installation
• Basic Transparent mode installation
• Converting a standalone FortiGate unit to a cluster
• Adding a new unit to an operating cluster
• HA between two FortiGate-5020 chassis
• FortiGate HA clustering between two FortiGate-5050 chassis
• FortiGate HA clustering between two FortiGate-5140 chassis

About the procedures in this chapter

The procedures in this chapter describe some of many possible sequences of steps for configuring HA clustering. As you become more experienced with FortiOS HA you may choose to use a different sequence of configuration steps.

For simplicity many of these procedures assume that you are starting with new FortiGate units set to the factory default configuration. However, starting from the default configuration is not a requirement for a successful HA deployment. FortiGate HA is flexible enough to support a successful configuration from many different starting points.

Configuring and connecting an HA cluster

Use the following procedures to configure an HA cluster consisting of two or more FortiGate units. These procedures describe how to configure each of the FortiGate units for HA operation and then how to connect the FortiGate units to form a cluster. Once the cluster is connected you can configure it in the same way as you would configure a standalone FortiGate unit.
Confusing a FortiGate unit for HA operation

Each FortiGate unit in the cluster must have the same HA configuration. Use the following procedure to configure each FortiGate unit for HA operation. See “HA web-based manager options” on page 51 for information about the HA options referenced in this procedure.

To configure a FortiGate unit for HA operation

1. Power on the FortiGate unit to be configured.
2. Connect to the web-based manager.
   The FortiGate dashboard is displayed.
3. Under System Information, beside Host Name select Change.
4. Enter a new Host Name for this FortiGate unit.
5. Go to System > Config > HA.
6. Set Mode to Active-Passive or Active-Active.
7. Enter a password for the cluster.
   The password must be the same for all FortiGate units in the HA cluster.
8. Select OK.

Note: You can accept the default configuration for the remaining HA options and change them later, once the cluster is operating.
The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces (see “Cluster virtual MAC addresses” on page 31). To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

9. Power off the FortiGate unit.
10. Repeat this procedure for all of the FortiGate units in the cluster.

Once all of the units are configured, continue with “Connecting a FortiGate HA cluster” on page 79.

**Connecting a FortiGate HA cluster**

Use the following procedure to connect a cluster operating in NAT/Route mode or Transparent mode. Connect the cluster units to each other and to your network. You must connect all matching interfaces in the cluster to the same hub or switch. Then you must connect these interfaces to their networks using the same hub or switch.

Fortinet recommends using switches for all cluster connections for the best performance.

Inserting an HA cluster into your network temporarily interrupts communications on the network because new physical connections are being made to route traffic through the cluster. Also, starting the cluster interrupts network traffic until the individual cluster units are functioning and the cluster completes negotiation. Cluster negotiation is automatic and normally takes just a few seconds. During system startup and negotiation all network traffic is dropped.

**To connect a FortiGate HA cluster**

1. Connect the internal interfaces of each cluster unit to a switch or hub connected to your internal network.
2. Connect the external interfaces of each cluster unit to a switch or hub connected to your external network.
3. Connect one of the default heartbeat interfaces of the cluster units together using another switch or hub.
4. Optionally connect the other default heartbeat interfaces of the cluster units together using another switch or hub.

**Note:** FortiGate-5000 series cluster heartbeat communication uses the FortiGate-5000 chassis backplane. No additional HA heartbeat connections are required.

Refer to Table 7 on page 56 for the default heartbeat interfaces of your FortiGate unit. At least one heartbeat interface should be connected together for the cluster to operate. You can also connect the heartbeat interfaces to a network. If the cluster consists of just two FortiGate units, you can connect the heartbeat interfaces directly using a crossover cable. For more information about heartbeat interfaces, see “Heartbeat Interface” on page 54 and the FortiGate HA Guide.
5  Optionally connect the other interfaces of each cluster unit to a switch or hub connected their networks.

Figure 14 shows a sample network configuration for an HA cluster consisting of two FortiGate-800 units. In this example, only the internal and external interfaces are connected to networks. The HA interfaces are connected for HA heartbeat communication.

Figure 14: HA network configuration

6  Power on all of the cluster units.
As the cluster units start, they negotiate to choose the primary unit and the subordinate units. This negotiation occurs with no user intervention and normally just takes a few seconds.
You can now configure the cluster as if it is a single FortiGate unit.

Basic NAT/Route mode installation

This section describes a simple HA network topology that includes an HA cluster of two FortiGate-3600 units installed between an internal network and the Internet running in NAT/Route mode.

- Example NAT/Route mode HA network topology
- Configuring a NAT/Route mode active-active HA cluster

Example NAT/Route mode HA network topology

Figure 15 shows a typical FortiGate-3600 HA cluster consisting of two FortiGate-3600 units (3600_ha_1 and 3600_ha_2) connected to the same internal and external networks.
The default FortiGate-3600 heartbeat interface configuration sets port4 and port5/ha as the heartbeat interfaces. As a result, in addition to connecting the FortiGate-3600 units to the network, this example describes connecting together the FortiGate-3600 port4 interfaces and port5/ha interfaces (as shown in Figure 15). Because the cluster consists of two FortiGate units, you can make the connections between the port4 interfaces and between the port5/ha interfaces using crossover cables. You could also use switches and regular ethernet cables as shown for the internal and external interfaces.

Figure 15: NAT/Route mode HA network topology

The default FortiGate-3600 heartbeat interface configuration sets port4 and port5/ha as the heartbeat interfaces. As a result, in addition to connecting the FortiGate-3600 units to the network, this example describes connecting together the FortiGate-3600 port4 interfaces and port5/ha interfaces (as shown in Figure 15). Because the cluster consists of two FortiGate units, you can make the connections between the port4 interfaces and between the port5/ha interfaces using crossover cables. You could also use switches and regular ethernet cables as shown for the internal and external interfaces.

Configuring a NAT/Route mode active-active HA cluster

This section describes how to configure an active-active HA cluster to run in NAT/Route mode using the topology shown in Figure 15. The section includes web-based manager and CLI procedures. These procedures assume that the FortiGate-3600 units are running the same FortiOS v3.0 MR2 or greater firmware build and are set to the factory default configuration.

- General configuration steps
- Web-based manager configuration steps
- CLI configuration steps

General configuration steps

1. Configure the FortiGate units for HA operation.
   - Optionally change the FortiGate unit host name.
   - Configure HA.
2. Connect the cluster to the network.
3. Confirm that the cluster units are operating as a cluster and add basic configuration settings to the cluster.
   - View cluster status from the web-based manager or CLI.
   - Add a password for the admin administrative account.
   - Change the IP addresses and netmasks of the internal and external interfaces.
   - Add a default route.
Web-based manager configuration steps

Use the following procedures to configure the FortiGate-3600 units for NAT/Route HA operation.

Note: Give each cluster unit a unique host name to make the individual units easier to identify when they are part of a functioning cluster. The default FortiGate unit host name is the FortiGate serial number. You may want to change this host name to something more meaningful for your network.

To change the FortiGate unit host name

1. Power on the FortiGate unit.
2. Set the IP address of a management computer with an Ethernet connection to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.
3. On a management computer, start Internet Explorer and browse to the address https://192.168.1.99 (remember to include the “s” in https://).
   The FortiGate login is displayed.
4. Type admin in the Name field and select Login.
   The FortiGate dashboard is displayed.
5. Under System Information, beside Host Name select Change.
6. Enter a new Host Name for this FortiGate unit.
7. Select OK.

To configure HA settings

1. Go to System > Config > HA.
2. Select Active-Active.
   Note: This is the minimum required for an active-active HA configuration. You can also configure other HA options, but if you wait until after the cluster is operating you will only have to configure these options once for the cluster instead of separately for each cluster unit.
3. Select OK.
   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces (see “Cluster virtual MAC addresses” on page 31). The MAC addresses of the FortiGate-3600 interfaces change to the following:
   • external interface virtual MAC: 00-09-0f-09-00-00
   • internal interface virtual MAC: 00-09-0f-09-00-01
   • port1 interface virtual MAC: 00-09-0f-09-00-02
   • port2 interface virtual MAC: 00-09-0f-09-00-03
   • port3 interface virtual MAC: 00-09-0f-09-00-04
   • port4 interface virtual MAC: 00-09-0f-09-00-05
   • port5/ha interface virtual MAC: 00-09-0f-09-00-06

   To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`. 
4 Power off the FortiGate unit.
5 Repeat these steps for all of the FortiGate units to be added to the cluster.

To connect the cluster to the network

1 Connect the cluster units.
   • Connect the internal interfaces of each FortiGate unit to a switch or hub connected to the internal network.
   • Connect the external interfaces of each FortiGate unit to a switch or hub connected to the external network.
   • Connect the port4 interfaces of the FortiGate units to each other using a crossover cable. You could also use a switch and two Ethernet cables.
   • Connect the port5/ha interfaces of the FortiGate units to each other using a crossover cable. You could also use a switch and two Ethernet cables.

2 Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention.
   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status and add basic configuration settings to the cluster

Use the following steps to view the cluster dashboard and cluster members list to confirm that the cluster units are operating as a cluster. Then you can configure the cluster to connect to its network. The following are example configuration steps only and do not represent all of the steps required to configure the cluster for a given network.

Note: Once the cluster is operating, because configuration changes are synchronized to all cluster units, configuring the cluster is the same as configuring an individual FortiGate unit. In fact you could have performed the following configuration steps separately on each FortiGate unit before you connected them to form a cluster.
1. Connect a management computer to the internal network, and change the IP address of the management computer to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.

2. Start Internet Explorer and browse to the address https://192.168.1.99 (remember to include the "s" in https://).

   The FortiGate Login is displayed.

3. Type admin in the Name field and select Login.

   The FortiGate dashboard is displayed. The dashboard shows the cluster name (which is the same as the HA Group Name), the host names and serial numbers of the cluster units, and the FortiGate icon changes to show multiple cluster units.

   **Figure 17: Sample FortiGate-3600 cluster dashboard**

4. Go to System > Config > HA to view the cluster members list.

   **Figure 18: Sample FortiGate-3600 cluster members list**

5. Go to System > Admin > Administrators.
   - For admin, select Change password.
   - Enter and confirm a new password.

6. Select OK.
Go to **System > Network > Interface**.
- For internal, select Edit.
- Change the IP/Netmask to 192.168.20.93/24.

Select OK.
- For external, select Edit.
- Change the IP/Netmask to 64.29.46.67/24.

Select OK.

Go to **Router > Static**.
- Edit the default route.

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>0.0.0.0/0.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gateway</strong></td>
<td>64.29.46.1</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>external</td>
</tr>
<tr>
<td><strong>Distance</strong></td>
<td>10</td>
</tr>
</tbody>
</table>

Select OK.

**CLI configuration steps**

**To configure each FortiGate unit for NAT/Route mode HA operation**

1. Power on the FortiGate unit.
2. Connect a null modem cable to the communications port of the management computer and to the FortiGate Console port.
3. Start HyperTerminal, enter a name for the connection, and select OK.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select OK.
5. Select the following port settings and select OK.

<table>
<thead>
<tr>
<th>Bits per second</th>
<th>9600</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
</tbody>
</table>

6. Press Enter to connect to the FortiGate CLI.

The FortiGate unit CLI login prompt appears.

7. Type `admin` and press Enter twice.
8. Change the host name for this FortiGate unit. For example:

```bash
config system global
    set hostname <name_str>
end
```

**Note:** Give each cluster unit a unique host name to make the individual units easier to identify when they are part of a functioning cluster. The default FortiGate unit host name is the FortiGate serial number. You may want to change this host name to something more meaningful for your network.
9 Configure HA settings.

```
config system ha
  set mode a-a
end
```

**Note:** This is the minimum required for an active-active HA configuration. You can also configure other HA options, but if you wait until after the cluster is operating you will only have to configure these options once for the cluster instead of separately for each cluster unit.

The FortiGate unit negotiates to establish an HA cluster.

10 Display the HA configuration (optional).

```
config system ha
  show full-configuration
config system ha
  set group-id 0
  set group-name "FGT-HA"
  set mode a-a
  set password ENC
  set hbdev "port4" "port5/ha"
  set route-ttl 0
  set route-wait 0
  set route-hold 10
  set sync-config enable
  set encryption disable
  set authentication disable
  set hb-interval 2
  set hb-lost-threshold 6
  set helo-holddown 20
  set arps 3
  set session-pickup disable
  set link-failed-signal disable
  set uninterruptable-upgrade enable
  set override disable
  set priority 128
  set schedule round-robin
  unset monitor
  unset vdom
  set vcluster2 disable
  set load-balance-all disable
end
```

11 Power off the FortiGate unit.

12 Repeat these steps for all of the units in the cluster.

**To connect the cluster to the network**

1 Connect the cluster units using the procedure "To connect the cluster to the network" on page 83.
2 Power on the cluster units.
   The units start and negotiate to choose the primary unit and the subordinate unit.
   This negotiation occurs with no user intervention.
   When negotiation is complete the cluster is ready to be configured for your network.

To view cluster status and add basic configuration settings to the cluster

Use the following steps to view cluster status from the CLI and to add some basic settings to the cluster so that it can connect to your network. The following are example configuration steps only and do not represent all of the steps required to configure the cluster for a given network.

1 Determine which cluster unit is the primary unit.
   • Use the null-modem cable and serial connection to re-connect to the CLI of one of the cluster units.
   • Enter the command `get system status`.
     
     If the command output includes `Current HA mode: a-a, master`, the cluster units are operating as a cluster and you have connected to the primary unit. Continue with Step 2.
     
     If the command output includes `Current HA mode: a-a, backup`, you have connected to a subordinate unit. Connect to the other cluster unit, which should be the primary unit and continue with Step 2.

   Note: If the command output includes `Current HA mode: standalone`, the cluster unit is not operating in HA mode and you should review your HA configuration.

2 Enter the following command to confirm the HA configuration of the cluster:
   `get system ha status`
   `Model: 3600`
   `Mode: a-a`
   `Group: 0`
   `Debug: 0`
   `ses_pickup: disable`
   `load_balance: disable`
   `schedule: round robin`
   `Master:128 3600_ha_1 FG36002804060610 1`
   `Slave :128 3600_ha_2 FG36002804033100 0`
   `number of vcluster: 1`
   `vcluster 1: work 10.0.0.2`
   `Master:0 FG36002804060610`
   `Slave :1 FG36002804033100`

   See "get system ha status (CLI command)" on page 69.

3 Add a password for the admin administrative account.
   `config system admin`
   `edit admin`
   `set password <psswrd>`
   `end`

4 Configure the internal interface.
Basic Transparent mode installation

This section describes a simple HA network topology that includes an HA cluster of two FortiGate-800 units installed between an internal network and the Internet and running in Transparent mode.

- Example Transparent mode HA network topology
- Configuring a Transparent mode active-active HA cluster

Example Transparent mode HA network topology

Figure 19 shows a typical FortiGate-500 HA cluster consisting of two FortiGate-500 units (800_ha_1 and 800_ha_2) connected to the same internal and external networks.

Figure 19: Transparent mode HA network topology
The default FortiGate-800 heartbeat interface configuration sets ha and port1 as the heartbeat interfaces. As a result, in addition to connecting the FortiGate-800 units to the network, this example describes connecting together the FortiGate-800 ha interfaces and port1 interfaces (as shown in Figure 19). Because the cluster consists of two FortiGate units, you can make the connections between the ha interfaces and between the port1 interfaces using crossover cables. You could also use switches and regular ethernet cables as shown for the internal and external interfaces.

**Configuring a Transparent mode active-active HA cluster**

This section describes how to configure an active-active HA cluster to run in Transparent mode using the topology shown in Figure 19. The section includes web-based manager and CLI procedures. These procedures assume that the FortiGate-800 units are running the same FortiOS v3.0 MR2 or greater firmware build and are set to the factory default configuration.

- **General configuration steps**
- **Web-based manager configuration steps**
- **CLI configuration steps**

**General configuration steps**

In this configuration example, the configuration steps are identical to the NAT/Route mode configuration steps until the cluster is operating. When the cluster is operating, you can switch to Transparent mode and add basic configuration settings to cluster.

1. Configure the FortiGate units for HA operation.
   - Optionally change the FortiGate unit host name.
   - Configure HA.

2. Connect the cluster to the network.

3. Switch the cluster to Transparent mode and add basic configuration settings to the cluster. Confirm that the cluster units are operating as a cluster.
   - Switch to Transparent mode, add the management IP address and default route.
   - Add a password for the admin administrative account.
   - View cluster status from the web-based manager or CLI.

**Web-based manager configuration steps**

Use the following procedures to configure the FortiGate-800 units for Transparent mode HA operation using the FortiGate web-based manager.

**Note:** Give each cluster unit a unique host name to make the individual units easier to identify when they are part of a functioning cluster. The default FortiGate unit host name is the FortiGate serial number. You may want to change this host name to something more meaningful for your network.

**To change the FortiGate unit host name**

1. Power on the FortiGate unit.

2. Set the IP address of a management computer with an Ethernet connection to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.
3 On a management computer, start Internet Explorer and browse to the address https://192.168.1.99 (remember to include the “s” in https://).
   The FortiGate login is displayed.
4 Type admin in the Name field and select Login.
   The FortiGate dashboard is displayed.
5 Under System Information, beside Host Name select Change.
6 Enter a new Host Name for this FortiGate unit.
7 Select OK.

**To configure HA settings**

1 Go to **System > Config > HA**.
2 Select Active-Active.

**Note:** This is the minimum required for an active-active HA configuration. You can also configure other HA options, but if you wait until after the cluster is operating you will only have to configure these options once for the cluster instead of separately for each cluster unit.

3 Select OK.
   The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces (see “Cluster virtual MAC addresses” on page 31). The MAC addresses of the FortiGate-800 interfaces change to the following:
   - dmz interface virtual MAC: 00-09-0f-09-00-00
   - external interface virtual MAC: 00-09-0f-09-00-01
   - ha interface virtual MAC: 00-09-0f-09-00-02
   - internal interface virtual MAC: 00-09-0f-09-00-03
   - port1 interface virtual MAC: 00-09-0f-09-00-04
   - port2 interface virtual MAC: 00-09-0f-09-00-05
   - port3 interface virtual MAC: 00-09-0f-09-00-06
   - port4 interface virtual MAC: 00-09-0f-09-00-07

To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`. 
4. Power off the FortiGate unit.
5. Repeat these steps for all of the FortiGate units to be added to the cluster.

To connect the cluster to the network

1. Connect the cluster units.
   - Connect the internal interfaces of each FortiGate unit to a switch or hub connected to the internal network.
   - Connect the external interfaces of each FortiGate unit to a switch or hub connected to the external network.
   - Connect the ha interfaces of the FortiGate units to each other using a cross-over cable. You could also use a switch and two ethernet cables.
   - Connect the port1 interfaces of the FortiGate units to each other using a cross-over cable. You could also use a switch and two ethernet cables.

2. Power on all of the cluster units.
The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention.

When negotiation is complete the cluster is ready to be configured for your network.

To switch the cluster to operate in Transparent mode

Switching from NAT/Route to Transparent mode also involves adding the Transparent mode management IP address and default route.

1. Connect a management computer to the internal network, and change the IP address of the management computer to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.

2. Start Internet Explorer and browse to the address https://192.168.1.99 (remember to include the “s” in https://).
The FortiGate Login is displayed.
3 Type admin in the Name field and select Login.
   The FortiGate dashboard is displayed. The dashboard shows the cluster name
   (which is the same as the HA Group Name), the host names and serial numbers
   of the cluster units, and the FortiGate icon changes to show multiple cluster units.
4 Under System Information, beside Operation Mode select Change.
5 Set Operation Mode to Transparent.
6 Configure basic Transparent mode settings.

   | Operation Mode | Transparent  
   | Management IP/Mask | 192.168.20.3/24  
   | Default Gateway | 192.168.20.1  

7 Select Apply.
   The cluster switches to operating in Transparent mode. When you select Apply
   you may temporarily lose connectivity with the cluster because the FGCP
   changes the MAC address of the FortiGate unit interfaces to the management IP
   virtual MAC address. See “Cluster virtual MAC addresses” on page 31. When
   operating in Transparent mode the MAC address of all FortiGate-800 interfaces
   changes to 00-09-0f-09-00-00

To add a password for the admin administrative account
1 Go to System > Admin > Administrators.
   • For admin, select Change password.
   • Enter and confirm a new password.
2 Select OK.

To view cluster status from the web-based manager
1 Go to System > Status.
   The FortiGate dashboard is displayed. The dashboard shows the cluster name
   (which is the same as the HA Group Name), the host names and serial numbers
   of the cluster units, and the FortiGate icon changes to show multiple cluster units.
Go to System > Config > HA to view the cluster members list.

**CLI configuration steps**

Use the following procedures to configure the FortiGate-800 units for Transparent mode HA operation using the FortiGate CLI.

**To configure each FortiGate unit for HA operation**

1. Power on the FortiGate unit.
2. Connect a null modem cable to the communications port of the management computer and to the FortiGate Console port.
3. Start HyperTerminal, enter a name for the connection, and select OK.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select OK.
5. Select the following port settings and select OK.
Configuring a Transparent mode active-active HA cluster

6 Press Enter to connect to the FortiGate CLI. The FortiGate unit CLI login prompt appears.
7 Type `admin` and press Enter twice.
8 Change the host name for this FortiGate unit. For example:

   ```
   config system global
   set hostname <name_str>
   end
   ```

   **Note:** Give each cluster unit a unique host name to make the individual units easier to identify when they are part of a functioning cluster. The default FortiGate unit host name is the FortiGate serial number. You may want to change this host name to something more meaningful for your network.

9 Configure HA settings.

   ```
   config system ha
   set mode a-a
   end
   ```

   **Note:** This is the minimum required for an active-active HA configuration. You can also configure other HA options, but if you wait until after the cluster is operating you will only have to configure these options once for the cluster instead of separately for each cluster unit.

   The FortiGate unit negotiates to establish an HA cluster.

10 Power off the FortiGate unit.

11 Repeat these steps for all of the units in the cluster.

**To connect the cluster to the network**

1 Connect the cluster units using the procedure “To connect the cluster to the network” on page 91.

2 Power on all of the cluster units. The units start and negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention. When negotiation is complete the cluster is ready to be configured for your network.
To connect to the cluster CLI and switch the cluster to Transparent mode

1. Determine which cluster unit is the primary unit.
   - Use the null-modem cable and serial connection to re-connect to the CLI of one of the cluster units.
   - Enter the command `get system status`.
     - If the command output includes `Current HA mode: a-a, master, the cluster units are operating as a cluster and you have connected to the primary unit. Continue with Step 2.`
     - If the command output includes `Current HA mode: a-a, backup, you have connected to a subordinate unit. Connect to the other cluster unit, which should be the primary unit and continue with Step 2.`

   Note: If the command output includes `Current HA mode: standalone, the cluster unit is not operating in HA mode and you should review your HA configuration.`

2. Change to transparent mode.

   ```
   config system settings
   set opmode transparent
   set manageip 192.168.20.3/24
   set gateway 192.168.20.1
   end
   ```

   The cluster switches to Transparent Mode.

   You can now connect to the cluster CLI using SSH to connect to the cluster internal interface using the management IP address (192.168.20.3).

To add a password for the admin administrative account

1. Add a password for the admin administrative account.

   ```
   config system admin
   edit admin
   set password <psswrd>
   end
   ```

To view cluster status from the CLI

1. Enter the following command to display the HA configuration of the cluster.

   ```
   config system ha
   config system ha
   set group-id 34
   set group-name "FGT-HA"
   set mode a-a
   set password ENC
   BEAD279dMG9Tv7PCoQLErl2vDAAn8DZjmlKaB6Oua60iHRbPgejcVdV0
   pwFy
   set hbdev "ha" "port1"
   set route-ttl 0
   set route-wait 0
   set route-hold 10
   set sync-config enable
   set encryption disable
   set authentication disable
   set hb-interval 2
   ```
set hb-lost-threshold 6
set helo-holddown 20
set arps 5
set session-pickup disable
set link-failed-signal disable
set uninterruptable-upgrade enable
set override enable
set priority 128
set schedule round-robin
unset monitor
unset vdom
set vcluster2 disable
set load-balance-all disable
end

2 You can also enter the following command to confirm the HA configuration of the cluster:

get system ha status
Model: 800
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
load_balance: disable
schedule: round robin
Master:128 800_ha_2 FG80028204400045 1
Slave :128 800_ha_1 FG80028205400050 0
number of vcluster: 1
vcluster 1: work 10.0.0.2
Master:0 FG80028204400045
Slave :1 FG80028205400050

See “get system ha status (CLI command)” on page 69.
Converting a standalone FortiGate unit to a cluster

You can convert an already configured and installed FortiGate unit into a cluster by configuring this FortiGate unit to be a primary unit and adding subordinate units.

General configuration steps:
• Configure the original FortiGate unit for HA operation.
• Set the HA Unit Priority of the original FortiGate unit to 255 to make sure that this FortiGate unit becomes the primary unit.

After negotiation the configuration of the original FortiGate unit is synchronized to all cluster units.
• Back up the configuration of the original FortiGate unit.
• Configure one or more new FortiGate units with the same HA configuration as the original FortiGate unit with one exception. Keep the Unit Priority at the default setting, which is 128.
• Connect the FortiGate units into a cluster and connecting the cluster to your network.

When you power on all of the FortiGate units in the cluster the original FortiGate unit becomes the primary unit. Its configuration is synchronized to all of the subordinate units. The entire cluster now operates with the original FortiGate unit configuration. No further configuration changes are required.

The new FortiGate units must:
• Be the same FortiGate model as the original FortiGate unit.
• Have the same hard drive configuration as the original FortiGate unit.
• Be running the same firmware version and build as the original FortiGate unit.

In addition to one or more new FortiGate units, you need sufficient switches or hubs to connect all of the FortiGate interfaces in the cluster.

Converting a FortiGate unit to a primary unit and adding in the subordinate unit or units results in a brief service interruption as you disconnect and reconnect FortiGate interfaces and as the cluster negotiates. Therefore, conversion should only be done during off peak hours.

To configure the original FortiGate unit for HA operation

1. Connect to the FortiGate unit web-based manager.
2. Go to System > Config > HA.
3. Configure the FortiGate unit for HA operation.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Active-Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Priority</td>
<td>255 (Set a high priority so that this unit becomes the primary unit.)</td>
</tr>
</tbody>
</table>

As a minimum you need to change the Mode and Device Priority. You can make other HA configuration changes after the cluster is operating.

4. Select OK.

When the FortiGate unit changes its MAC addresses and attempts to negotiate a cluster, a short service interruption occurs.
5 Set the HA configuration of the new FortiGate units to the same HA mode as the original FortiGate unit.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Active-Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Priority</td>
<td>128 (Keep the default setting.)</td>
</tr>
</tbody>
</table>

There is no need to make any other configuration changes (including network configuration changes, operation mode changes, or virtual domain changes) to the other FortiGate units. Do not change the HA Device Priority of the other FortiGate units.

6 Power off all FortiGate units including the original FortiGate unit.

7 Connect the cluster to your network.

For example, for a configuration similar to the FortiGate-800 cluster configuration described in this chapter, see “To connect the cluster to the network” on page 91.

8 Power on all of the cluster units.

As the units start they change their MAC addresses and then negotiate to choose the primary unit and the subordinate units. This negotiation occurs with no user intervention.

The original the FortiGate unit becomes the primary unit because the device priority of the original FortiGate unit is higher than the device priority of the other FortiGate units. The configuration of the original FortiGate unit is synchronized to all the cluster units, as a result the cluster is quickly up and running and configured for your network. No further configuration changes are required; however, you can modify the cluster HA configuration.

### Adding a new unit to an operating cluster

You can add a new cluster unit to a functioning cluster at any time. The new cluster unit must:

- Be the same FortiGate model as the other cluster units.
- Have the same hard drive configuration as the other cluster units.
- Be running the same or an older firmware version and build as the cluster.

**Note:** If the new cluster unit is running an older firmware build you can use the web-based manager to re-install the cluster firmware build on the cluster. This forces the primary unit to upgrade the firmware running on the new cluster unit.

**Note:** The new cluster unit does not have to be operating in the same mode (NAT/Route or Transparent) as the cluster. When you add the new unit, the cluster will change the operating mode of the new cluster unit as required.

**To add the new unit to a cluster**

1 Configure the new cluster unit with the same HA configuration as the other units in the cluster.
2 Connect the new cluster unit to the cluster.
   For example, for a configuration similar to the FortiGate-800 cluster configuration described in this chapter, see “To connect the cluster to the network” on page 91.
   If you are adding a third unit to the cluster you may have to replace crossover cables used to connect heartbeat devices with a hubs or switches.

3 Turn on the new FortiGate unit.
   When the new cluster unit powers on it negotiates to join the cluster. After it joins the cluster, the cluster synchronizes the new unit configuration with the configuration of the primary unit. The cluster also synchronizes the operating mode of the new cluster unit.

   **To synchronize the firmware build running on the new cluster unit**
   If the firmware build running on the new cluster unit is older than the firmware build running on the other cluster units, use the following steps to synchronize the firmware running on the new cluster unit:

   1 Connect to the cluster using the web-based manager.
   2 Go to **System > Status**.
   3 Select Update beside Firmware Version.
   4 Select the firmware image file name that will install the same firmware build already running on the cluster.
      You can also install a newer firmware build.
   5 Select OK.
   After the firmware image is uploaded to the cluster, the primary unit upgrades all cluster units to this firmware build.

   **Adding a large number of units to a cluster**
   You can use the procedure above to add as many units as required to the cluster.
   When creating a cluster consisting of a large number of units, keep in mind the following.
   • For optimum performance, when connecting interfaces that handle network traffic (for example, the internal and external interfaces) connect the interfaces of each set to a single hub or switch.
      For example, if you are planning on using 10 FortiGate units in the same active-active cluster, make sure you have a 10-port hub for each interface.
   • An HA cluster consisting of 10 FortiGate-300 units requires three 10-port hubs or switches: one for the internal interfaces, one for the external interfaces, and one for the DMZ/HA interfaces.

**HA between two FortiGate-5020 chassis**

The FortiGate-5020 chassis does not support direct ethernet connections between two or more FortiGate-5020 chassis. To configure HA for FortiGate modules installed in two different FortiGate-5020 chassis you must use one or two of the front panel interfaces of the FortiGate modules as HA heartbeat interfaces. Using two (or more) heartbeat interfaces is recommended for redundancy.
Network configuration

The following diagram shows an example of how to connect four FortiGate-5001SX units installed in two FortiGate-5020 chassis to make a cluster of 4 FortiGate-5001SX units.

This example cluster has a relatively basic network configuration. In the configuration, port1 connects to an internal network and port2 connects to the Internet. Port3 to port8 are available to be connected as HA heartbeat interfaces. This example uses port7 and port8 as the HA heartbeat interfaces.

**Figure 23: Network and HA heartbeat connections**

Changing the HA heartbeat interface configuration

To configure FortiGate-5001SX cluster units for HA heartbeat interface connections between modules installed in two FortiGate-5020 chassis, you must change the default FortiGate-5001SX HA heartbeat interface configuration.

By default the FortiGate-5001SX HA heartbeat configuration uses backplane1 and backplane2 as HA heartbeat interfaces. To configure HA heartbeat interfaces for this example configuration, select port7 and port8 to be HA heartbeat interfaces and unselect port9 and port10.
FortiGate HA clustering between two FortiGate-5050 chassis

This article describes how the FortiSwitch-5003 module supports HA clustering for FortiGate-5000 series modules installed in a single chassis and how FortiSwitch-5003 modules can also be used for HA clustering for FortiGate-5000 series modules installed in two FortiGate-5050 chassis.

The FortiSwitch-5003 module provides backplane HA heartbeat communication between FortiGate-5000 series modules installed in a FortiGate-5050 chassis. If you have two FortiGate-5050 chassis that each contain the same FortiGate-5000 series modules and that also each contain one or two FortiSwitch-5003 modules, you can make ethernet connections between the two FortiGate-5050 chassis using the FortiSwitch-5003 modules. These ethernet connections result in backplane HA heartbeat communication between two FortiGate-5050 chassis.

Figure 25: FortiSwitch-5003 front panel

- Mounting Knot
- Extraction Lever
- ZRE0, ZRE1, ZRE2 backplane interfaces
- 10/100/1000Base-T Ethernet
- Out of Band Management
- 100Base-TX Ethernet
- RJ-45 Serial
- Network Activity LEDs
- LED Mode
- Mounting Knot
- Extraction Lever
If you then apply the same HA configuration to the FortiGate-5000 series modules in both chassis, these FortiGate-5000 series modules form a single HA cluster. The cluster is formed because an HA heartbeat link is established between the FortiGate-5000 series modules in both chassis.

**Note:** The FortiSwitch-5003 module supports HA clustering for all FortiGate-5000 series modules. Most of the examples described in this article use FortiGate-5001SX modules.

### FortiGate-5050 backplane interfaces

The FortiGate-5050 chassis has two backplane ethernet interfaces (also called base backplane interfaces). To connect to the backplane interfaces you must install FortiGate-5000 series modules in chassis slots 3, 4, and 5. FortiGate-5001SX and 5001FA2 modules connect to the backplane interfaces as port9 and port10. The FortiGate-5002FB2 module connects to the backplane interfaces as port7 and port8.

A FortiSwitch-5003 module installed in FortiGate-5050 chassis slot 1 supplies backplane switching for the first backplane interface (port9 for the 5001SX and 5001FA2 and port 7 for the FortiGate-5002FB2). A FortiSwitch-5003 module installed in slot 2 provides switching for the second backplane interface (port10 for the 5001SX and 5001FA2 and port8 for the FortiGate-5002FB2).

You can install FortiGate-5000 series modules in slots 1 and 2. However, in these slots the FortiGate-5000 series modules cannot connect to the backplane interfaces. FortiSwitch-5003 modules can only be installed in slots 1 or 2 to provide backplane interface switching.

### HA cluster with 1 FortiSwitch-5003 module

Installing a single FortiSwitch-5003 module in a FortiGate-5050 chassis provides a single backplane HA heartbeat link for up to 3 FortiGate-5001SX modules installed in chassis slots 3, 4, and 5. Usually you would install a single FortiSwitch-5003 module in slot 2 of the FortiGate-5050 chassis although you could also install the FortiSwitch module in slot 1.

Port9 and port10 are the default FortiGate-5001SX HA heartbeat interfaces. One FortiSwitch-5003 module installed in slot 2 means an HA cluster of FortiGate-5001SX modules use port10 for HA heartbeat communication. No change to the FortiGate-5001SX default HA heartbeat configuration is required. You can set one or more of port2 to port8 to be HA heartbeat interfaces so that HA heartbeat communication fails over to one of these interfaces if backplane communication fails or is interrupted.
A single FortiSwitch-5003 module for HA heartbeat communication introduces a single point of failure. If this FortiSwitch-5003 module fails or is removed, HA heartbeat communication will be interrupted. For enhanced reliability you can add a second FortiSwitch-5003 module to slot 1. You can also improve reliability by connecting and configuring one or more other FortiGate-5001SX interfaces as HA heartbeat interfaces.

**Why install a single FortiSwitch-5003 module in slot 2?**

It is recommended that you install a single FortiSwitch-5003 module in slot 2 so that you can select one or more of the other FortiGate-5001SX interfaces to be backup HA heartbeat interfaces. If two or more interfaces are configured to be HA heartbeat interfaces, HA selects the connected HA heartbeat interface with the lowest index to use for HA heartbeat communication. Slot 2 connects to port10; which has the second lowest index (port1 the lowest and port9 the highest). So if the FortiSwitch-5003 module is in slot 2 you can select from port2 to port8 to be backup HA heartbeat interfaces. All HA heartbeat communications will use port10 and failover to an interface with a higher index if port10 becomes disconnected.

If you install a single FortiSwitch-5003 module in slot 1, the cluster uses port9 for HA heartbeat communication. If you select any other HA heartbeat interfaces, one of these other interfaces, if it is connected, will always be used for HA heartbeat communication instead of port9. This is because port9 has the highest interface index so is the last interface selected to be the HA heartbeat interface. So installing a single FortiSwitch-5003 module in slot 1 limits your options for selecting other interfaces for HA heartbeat communication.

**Note:** The FortiGate web-based manager and CLI always lists interfaces in index order.

**HA cluster with 2 FortiSwitch-5003 modules**

Installing a second FortiSwitch-5003 module in slot 1 provides redundant HA heartbeat communication for FortiGate-5001SX modules installed in slots 3, 4, and 5. Port9 and port10 can both be used for HA heartbeat communication. As long as it is connected, port10 is used for HA heartbeat communication. If port10 fails or becomes disconnected, HA heartbeat communication switches to port9.
HA between two FortiGate-5050 chassis

The Ethernet interfaces on the front panel of the FortiSwitch-5003 labelled ZRE0, ZRE1, and ZRE2 provide three connections to the chassis backplane interface that the FortiSwitch-5003 is connected to. You can set up ethernet communications between the backplanes of two FortiGate-5050 chassis by connecting an ethernet cable from any ZRE interface on a FortiSwitch-5003 module in one chassis to a ZRE interface on a FortiSwitch-5003 module in the other chassis. You can use a regular or crossover ethernet cable for this connection. Using this inter-chassis connection, you can set up a cluster of FortiGate-5000 series modules even if the modules are installed in more than one FortiGate-5050 chassis.

For the purposes of inter-chassis connections it makes no difference whether you use the ZRE0, ZRE1, or ZRE2 interface. You can connect an ethernet cable from any of these interfaces on one FortiSwitch-5003 module to any of these interfaces on another FortiSwitch-5003 module installed in the other chassis. You can also use the ZRE interfaces to connect more that two FortiGate-5050 chassis together.

For the inter-chassis communication to work, the FortiGate-5000 series modules must be installed in slots 3, 4, or 5. As well, the inter-chassis connections must be between FortiSwitch-5003 units installed in the same slot in each chassis.

To connect two chassis together, if each chassis has one FortiSwitch-5003 module, the module should be installed in slot 2 of both chassis. If each chassis has two FortiSwitch-5003 modules, the modules in slot 2 must be connected together and the modules in slot 1 must also be connected together.

Note: Installing the FortiSwitch-5003 modules in different slots would result in a mixture of HA heartbeat communications on port9 and port10. FortiGate HA does not support HA heartbeat communication between different interfaces in this way. The result would be the formation of multiple clusters, some using port9 for HA heartbeat communication and some using port10.

Example FortiGate HA cluster between two FortiGate-5050 chassis

The following example shows how to create a cluster of four FortiGate-5001SX modules installed in two FortiGate-5050 chassis. Both of these chassis have two FortiSwitch-5003 modules installed in slots 1 and 2. An ethernet cable connects the ZRE0 interfaces of the FortiSwitch-5003 modules in slot 1. Another ethernet cable connects together the ZRE2 interfaces of the FortiSwitch-5003 modules in slot 2.
**Note:** The ZRE interfaces do not have to be connected as described in this example. The connections could be between ZRE0 of the FortiSwitch-5003 module in one chassis and the ZRE1 interface on the other. The connections between the FortiGate-5003 modules in slot 1 can be the same or different than the connections between the FortiGate-5003 modules in slot 2.

Both FortiGate-5050 chassis include two FortiGate-5001SX modules. The first FortiGate-5050 chassis has FortiGate-5001SX modules installed in slots 3 and 5. The second FortiGate-5050 chassis has FortiGate-5001SX modules installed in slots 3 and 4.

Other than HA, no special configuration of the FortiGate-5001SX modules is required to form this cluster. Once the FortiSwitch-5003 modules are connected you can connect the FortiGate-5001SX modules together and to your network just as you would any cluster of four FortiGate units. Figure 28 shows an example network configuration with port1 of each FortiGate-5001SX module connected to a switch connected to an internal network. Port2 of each FortiGate-5001SX module is connected to a switch connected to the Internet.

**Figure 28:** HA cluster consisting of four FortiGate-5001SX modules installed in two FortiGate-5050 chassis connected by two FortiSwitch-5003 modules

Configure HA on each FortiGate-5001SX module according to your requirements. If you accept the default HA heartbeat configuration, the FortiGate-5001SX units will successfully form a cluster because the FortiGate-5001SX modules use port10 for HA heartbeat communication with port9 as a backup.

**Figure 29** shows an example HA configuration for this cluster of FortiGate-5001SX modules.
Example FortiGate HA cluster between two FortiGate-5050 chassis

Figure 29: Example FortiGate-5001SX HA configuration

Figure 30 shows the FortiGate-5001SX HA cluster dashboard. The host names of the FortiGate-5001SX units have been changed to show the locations of each module.

Figure 30: Dashboard

Figure 31 shows the FortiGate-5001SX HA cluster members list (System > Config > HA). Note that the host names of the FortiGate-5001SX units have been changed to show the locations of each module.
Other configurations

Finally, a few brief notes about other possible configurations:

- Because you can use the FortiSwitch-5003 to connect more than two chassis it is possible to create a cluster of FortiGate modules installed in more than two chassis.
- FortiGate HA and FortiGate-5050/FortiSwitch-5003 chassis backplane communication can support more than one cluster using the same backplane interface for HA heartbeat communication. To separate the clusters, each one should have a unique Group Name and password.
- Because the backplane communication architectures of the FortiGate-5050 and 5140 chassis are the same, you can also connect FortiGate-5050 and FortiGate-5140 chassis together and form clusters between chassis in the same way as described in this article.

FortiGate HA clustering between two FortiGate-5140 chassis

This article describes how the FortiSwitch-5003 module supports HA clustering for FortiGate-5000 series modules installed in a single chassis and how FortiSwitch-5003 modules can also be used for HA clustering for FortiGate-5000 series modules installed in two FortiGate-5140 chassis.

The FortiSwitch-5003 module provides backplane HA heartbeat communication between FortiGate-5000 series modules installed in a FortiGate-5140 chassis. If you have two FortiGate-5140 chassis that each contain the same FortiGate-5000 series modules and that also each contain one or two FortiSwitch-5003 modules, you can make ethernet connections between the two FortiGate-5140 chassis using the FortiSwitch-5003 modules. These ethernet connections result in backplane HA heartbeat communication between two FortiGate-5140 chassis.
If you then apply the same HA configuration to the FortiGate-5000 series modules in both chassis, these FortiGate-5000 series modules form a single HA cluster. The cluster is formed because an HA heartbeat link is established between the FortiGate-5000 series modules in both chassis.

Note: The FortiSwitch-5003 module supports HA clustering for all FortiGate-5000 series modules. Most of the examples described in this article use FortiGate-5001FA2 modules.

**FortiGate-5140 backplane interfaces**

The FortiGate-5140 chassis has two backplane ethernet interfaces (also called base backplane interfaces). To connect to the backplane interfaces you must install FortiGate-5000 series modules in chassis slots 3, 4, and 5. FortiGate-5001SX and 5001FA2 modules connect to the backplane interfaces as port9 and port10. The FortiGate-5002FB2 module connects to the backplane interfaces as port7 and port8.

A FortiSwitch-5003 module installed in FortiGate-5140 chassis slot 1 supplies backplane switching for the first backplane interface (port9 for the 5001SX and 5001FA2 and port 7 for the FortiGate-5002FB2). A FortiSwitch-5003 module installed in slot 2 provides switching for the second backplane interface (port10 for the 5001SX and 5001FA2 and port8 for the FortiGate-5002FB2).

You can install FortiGate-5000 series modules in slots 1 and 2. However, in these slots the FortiGate-5000 series modules cannot connect to the backplane interfaces. FortiSwitch-5003 modules can only be installed in slots 1 or 2 to provide backplane interface switching.

**HA cluster with 1 FortiSwitch-5003 module**

Installing a single FortiSwitch-5003 module in a FortiGate-5140 chassis provides a single backplane HA heartbeat link for up to 12 FortiGate-5001FA2 series modules installed in chassis slots 3 to 14. Usually you would install a single FortiSwitch-5003 module in slot 2 of the FortiGate-5140 chassis although you could also install the FortiSwitch module in slot 1.

Port9 and port10 are the default FortiGate-5001FA2 HA heartbeat interfaces. One FortiSwitch-5003 module installed in slot 2 means an HA cluster of FortiGate-5001FA2 modules use port10 for HA heartbeat communication. No change to the FortiGate-5001FA2 default HA heartbeat configuration is required. You can set one or more of port2 to port8 to be HA heartbeat interfaces so that HA heartbeat communication fails over to one of these interfaces if backplane communication fails or is interrupted.
Figure 33: One FortiSwitch-5003 module installed in slot 2 provides HA heartbeat communication on backplane port10 for FortiGate-5001FA2 modules

A single FortiSwitch-5003 module for HA heartbeat communication introduces a single point of failure. If this FortiSwitch-5003 module fails or is removed, HA heartbeat communication will be interrupted. For enhanced reliability you can add a second FortiSwitch-5003 module to slot 1. You can also improve reliability by connecting and configuring one or more other FortiGate-5001FA2 interfaces as HA heartbeat interfaces.

Why install a single FortiSwitch-5003 module in slot 2?

It is recommended that you install a single FortiSwitch-5003 module in slot 2 so that you can select one or more of the other FortiGate-5001FA2 interfaces to be backup HA heartbeat interfaces. If two or more interfaces are configured to be HA heartbeat interfaces, HA selects the connected HA heartbeat interface with the lowest index to use for HA heartbeat communication. Slot 2 connects to port10; which has the second lowest index (port1 the lowest and port9 the highest). So if the FortiSwitch-5003 module is in slot 2 you can select from port2 to port8 to be backup HA heartbeat interfaces. All HA heartbeat communications will use port10 and failover to an interface with a higher index if port10 becomes disconnected.

If you install a single FortiSwitch-5003 module in slot 1, the cluster uses port9 for HA heartbeat communication. If you select any other HA heartbeat interfaces, one of these other interfaces, if it is connected, will always be used for HA heartbeat communication instead of port9. This is because port9 has the highest interface index so is the last interface selected to be the HA heartbeat interface. So installing a single FortiSwitch-5003 module in slot 1 limits your options for selecting other interfaces for HA heartbeat communication.
HA cluster with 2 FortiSwitch-5003 modules

Installing a second FortiSwitch-5003 module in slot 1 provides redundant HA heartbeat communication for FortiGate-5001FA2 modules installed in slots 3 to 14. Port9 and port10 can both be used for HA heartbeat communication. As long as it is connected, port10 is used for HA heartbeat communication. If port10 fails or becomes disconnected, HA heartbeat communication switches to port9.

Figure 34: FortiSwitch-5003 modules installed in slots 1 and 2 provide HA heartbeat communication on port9 and port10

HA between two FortiGate-5140 chassis

The Ethernet interfaces on the front panel of the FortiSwitch-5003 labelled ZRE0, ZRE1, and ZRE2 provide three connections to the chassis backplane interface that the FortiSwitch-5003 is connected to. You can set up ethernet communications between the backplanes of two FortiGate-5140 chassis by connecting an ethernet cable from any ZRE interface on a FortiSwitch-5003 module in one chassis to a ZRE interface on a FortiSwitch-5003 module in the other chassis. You can use a regular or crossover ethernet cable for this connection. Using this inter-chassis connection, you can set up a cluster of FortiGate-5000 series modules even if the modules are installed in more than one FortiGate-5140 chassis.
For the purposes of inter-chassis connections it makes no difference whether you use the ZRE0, ZRE1, or ZRE2 interface. You can connect an ethernet cable from any of these interfaces on one FortiSwitch-5003 module to any of these interfaces on another FortiSwitch-5003 module installed in the other chassis. You can also use the ZRE interfaces to connect more that two FortiGate-5140 chassis together.

For the inter-chassis communication to work, the FortiGate-5000 series modules must be installed in slots 3 to 14. As well, the inter-chassis connections must be between FortiSwitch-5003 units installed in the same slot in each chassis.

To connect two chassis together, if each chassis has one FortiSwitch-5003 module, the module should be installed in slot 2 of both chassis. If each chassis has two FortiSwitch-5003 modules, the modules in slot 2 must be connected together and the modules in slot 1 must also be connected together.

**Note:** Installing the FortiSwitch-5003 modules in different slots would result in a mixture of HA heartbeat communications on port9 and port10. FortiGate HA does not support HA heartbeat communication between different interfaces in this way. The result would be the formation of multiple clusters, some using port9 for HA heartbeat communication and some using port10.

**Example FortiGate HA cluster between two FortiGate-5140 chassis**

The following example shows how to create a cluster of six FortiGate-5001FA2 modules installed in two FortiGate-5140 chassis. Both of these chassis have two FortiSwitch-5003 modules installed in slots 1 and 2. An ethernet cable connects the ZRE0 interfaces of the FortiSwitch-5003 modules in slot 1. Another ethernet cable connects together the ZRE1 interfaces of the FortiSwitch-5003 modules in slot 2.

**Note:** The ZRE interfaces do not have to be connected as described in this example. The connections could be between ZRE0 of the FortiSwitch-5003 module in one chassis and the ZRE1 interface on the other. The connections between the FortiGate-5003 modules in slot 1 can be the same or different than the connections between the FortiGate-5003 modules in slot 2.

Both FortiGate-5140 chassis include three FortiGate-5001FA2 modules. The first FortiGate-5140 chassis has FortiGate-5001FA2 modules installed in slots 6, 8, and 10. The second FortiGate-5140 chassis has FortiGate-5001FA2 modules installed in slots 7, 9, and 11.

Other than configuring HA, no special configuration of the FortiGate-5001FA2 modules is required to form this cluster. Once the FortiSwitch-5003 modules are connected you can connect the FortiGate-5001FA2 modules together and to your network just as you would any cluster of six FortiGate units. Figure 35 shows an example network configuration with port1 of each FortiGate-5001FA2 module connected to a switch connected to an internal network. Port2 of each FortiGate-5001FA2 module is connected to a switch connected to the Internet.
Configure HA on each FortiGate-5001FA2 module according to your requirements. If you accept the default HA heartbeat configuration, the FortiGate-5001FA2 units will successfully form a cluster because the FortiGate-5001FA2 modules use port10 for HA heartbeat communication with port9 as a backup.

Figure 29 shows an example HA configuration for this cluster of FortiGate-5001FA2 modules.
Figure 36: Example FortiGate-5001FA2 HA configuration

Figure 31 shows the FortiGate-5001FA2 HA cluster members list (System > Config > HA). The host names of the FortiGate-5001FA2 units have been changed to show the locations of each module.

Figure 37: Cluster members list

Other configurations

Finally, a few brief notes about other possible configurations:
• Because you can use the FortiSwitch-5003 to connect more than two chassis it is possible to create a cluster of FortiGate modules installed in more than two chassis

• FortiGate HA and FortiGate-5140/FortiSwitch-5003 chassis backplane communication can support more than one cluster using the same backplane interface for HA heartbeat communication. To separate the clusters, each one should have a unique Group Name and password.

• Because the backplane communication architectures of the FortiGate-5050 and 5140 chassis are the same, you can also connect FortiGate-5140 and FortiGate-5050 chassis together and form clusters between chassis in the same way as described in this article.
Configuring and connecting virtual clusters

This chapter provides an introduction to virtual clustering and also contains general procedures and configuration examples that describe how to configure FortiGate HA virtual clustering.

The examples in this chapter include example values only. In most cases you will substitute your own values. The examples in this chapter also do not contain detailed descriptions of configuration parameters. For information about FortiGate HA configuration parameters, see your FortiGate unit online help or “Configuration reference” on page 49.

This chapter contains the following sections:

• Virtual clustering overview
• Virtual clustering configuration steps
• Virtual clustering load balancing configuration

Virtual clustering overview

If virtual domains are enabled for a cluster, FortiOS HA operates using virtual clustering. Virtual clustering is an extension of the FGCP for FortiGate units operating with virtual domains. Virtual clustering operates in active-passive mode to provide failover protection between two instances of a virtual domain operating on two different cluster units. By distributing virtual domain processing between the two cluster units you can also configure virtual clustering to provide load balancing between the cluster units similar to active-active HA load balancing.

Virtual clustering and failover protection

Virtual clustering operates on a cluster of two (and only two) FortiGate units with virtual domains enabled. Each virtual domain creates a cluster between instances of the virtual domain on the two FortiGate units in the virtual cluster. All traffic to and from the virtual domain stays within the virtual domain and is processed by the virtual domain. One cluster unit is the primary unit for each virtual domain and one cluster unit is the subordinate unit for each virtual domain. The primary unit processes all traffic for the virtual domain. The subordinate unit does not process traffic for the virtual domain. If a cluster unit fails all traffic fails over to the cluster unit that is still operating.

Virtual clustering and heartbeat interfaces

The HA heartbeat provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides these HA heartbeat services for all of the virtual domains in the cluster. You do not have to add a heartbeat interface to a virtual domain.
Virtual clustering and load balancing

Even though virtual clustering operates in active-passive mode you can configure a form of load balancing by configuring virtual clustering to distribute traffic between both cluster units. To configure load balancing for virtual clustering you set one cluster unit to be the primary unit for some virtual domains and you set the other cluster unit to be the primary unit for the remaining virtual domains. Distributing the virtual domains evenly between the two cluster units results in the processing load for your network being balanced between the two cluster units.

In this configuration, failover protection does not change. If one of the units in the cluster fails, all processing is resumed by the remaining cluster unit. No traffic interruption occurs for virtual domains for which the remaining cluster unit was the primary unit. Traffic may be interrupted temporarily for virtual domains for which the failed unit was the primary unit while processing fails over to the remaining cluster unit.

Configuring HA options for virtual clustering

Note: If your FortiGate cluster uses virtual domains, you are configuring HA virtual clusters. Most virtual cluster HA options are the same as normal HA options. However, virtual clusters include VDOM partitioning options. Other differences between configuration options for regular HA and for virtual clustering HA are described below.

To configure HA options for a FortiGate unit with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to System > Config > HA.
See "HA web-based manager options" on page 51 for detailed information about HA options.

To change the host name and device priority of subordinate units in a functioning cluster, go to **System > Config > HA** to display the cluster members list. Select **Edit** for the subordinate (or backup) unit to configure. See "Changing subordinate unit host name and device priority" on page 57 for information about configuring subordinate units.
Virtual clustering configuration steps

Use the following procedures to configure virtual clustering for two FortiGate units. These procedures describe how to configure two new FortiGate units for virtual clustering, including configuring the two cluster units for HA operation, how to connect the cluster units, and then how to enable virtual domain configuration and add virtual domains to the cluster. These procedures also describe how to configure virtual clustering. Once the virtual cluster is operating you can configure the cluster in the same way as you would configure a standalone FortiGate unit with multiple virtual domains.

The procedures in this section describe one of many possible sequences of steps for configuring virtual clustering. As you become more experienced with FortiOS HA, virtual clustering and virtual domains you may choose to use a different sequence of configuration steps.

For simplicity these procedures assume that you are starting with new FortiGate units set to the factory default configuration. However, starting from the default configuration is not a requirement for a successful HA deployment. FortiGate HA is flexible enough to support a successful configuration from many different starting points.

Configuring two new FortiGate units for virtual clustering

This procedure describes how to configure virtual clustering starting with two FortiGate units set to default values and not connected to any networks.

Both FortiGate units in the cluster must have the same HA configuration. Use the following procedure to configure each FortiGate unit for HA operation. See “HA web-based manager options” on page 51 for information about the HA options referenced in this procedure.

To configure two new FortiGate units for virtual clustering

1. Power on the FortiGate unit to be configured.
2. Connect to the web-based manager.
3. Optionally give the FortiGate unit a unique host name.
   • Under System Information, beside Host Name select Change.
   • Enter a new Host Name for this FortiGate unit.
   Use host names to identify individual cluster units.
4. Go to System > Config > HA.
5. Set Mode to Active-Passive.
   Active-Active HA is not supported for virtual clustering.
6. Enter a password for the virtual cluster.
   The password must be the same for both FortiGate units in the virtual cluster.
7. Select OK.

Note: You can accept the default configuration for the remaining HA options and change them later, once the cluster is operating.
The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces (see “Cluster virtual MAC addresses” on page 31). To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.

8 Repeat this procedure for the other FortiGate unit in the virtual cluster.

Use the information in “Connecting a FortiGate virtual cluster” on page 119 to connect the virtual cluster.

**Connecting a FortiGate virtual cluster**

Use the following procedure to connect two FortiGate units to operate using virtual clustering. Connect the cluster units to each other and to your network. You must connect all matching interfaces in the cluster to the same hub or switch. Then you must connect these interfaces to their networks using the same hub or switch.

Fortinet recommends using switches for all cluster connections for the best performance.

Inserting an HA cluster into your network temporarily interrupts communications on the network because new physical connections are being made to route traffic through the cluster. Also, starting the cluster interrupts network traffic until the individual cluster units are functioning and the cluster completes negotiation. Cluster negotiation is automatic and normally takes just a few seconds. During system startup and negotiation all network traffic is dropped.

**To connect a FortiGate virtual cluster**

1 Connect the internal interfaces of each cluster unit to a switch or hub connected to your internal network.

2 Connect the external interfaces of each cluster unit to a switch or hub connected to your external network.

3 Connect one of the default heartbeat interfaces of the cluster units together using another switch or hub.

4 Optionally connect the other default heartbeat interfaces of the cluster units together using another switch or hub.

**Note:** FortiGate-5000 series cluster heartbeat communication uses the FortiGate-5000 chassis backplane. No additional HA heartbeat connections are required.

Refer to Table 7, “Default HA heartbeat interface configuration for all FortiGate models,” on page 56 for the default heartbeat interfaces of your FortiGate unit. At least one heartbeat interface should be connected together for the cluster to operate. You can also connect the heartbeat interfaces to a network. You can connect the heartbeat interfaces directly using a crossover cable. For more information about heartbeat interfaces, see “Heartbeat Interface” on page 54.
Optionally connect the other interfaces of each cluster unit to a switch or hub connected their networks.

Figure 39 shows a sample network configuration for virtual cluster consisting of two FortiGate-5001SX units. In this example, the virtual cluster has two virtual domains. The port5 and port6 interface are in the root virtual domain and the port7 and port8 interfaces are in a virtual domain named vdom_1. Site 1 connects to the root virtual domain and Site 2 connects to the vdom_1 virtual domain. The example includes the following network connections:

- The port5 interfaces are connected together and to the Site 1 network.
- The port6 interfaces are connected together and to the external router.
- The port7 interfaces are connected together and to the Site 2 network.
- The port8 interfaces are connected together and to the external router.

HA heartbeat communication through the FortiGate-5000 chassis back plane is not shown.

Figure 39: HA network configuration

Power on all of the cluster units.

As the cluster units start, they negotiate to choose the primary unit and the subordinate units. This negotiation occurs with no user intervention and normally just takes a few seconds.

You can now configure the virtual cluster in the same way as a single FortiGate unit.

Enabling virtual domains for a cluster

The following procedure describes how to enable virtual domain configuration for a FortiGate HA cluster. This procedure is the same as enabling virtual domain configuration for a standalone FortiGate unit.

To enable virtual domains for a cluster

1. Connect to the cluster web-based manager as the admin administrator.
2. Select Global Configuration.
3. Go to System > Admin > Settings.
4. Enable Virtual Domain Configuration.
5. Select Apply.
The cluster logs you off. You can now log in again as admin, add virtual domains, and configure virtual clustering.

See the FortiGate VLAN and VDOM Guide for more information about enabling virtual domains and how the web-based manager changes after virtual domains are enabled.

Adding virtual domains to a cluster

Adding virtual domains to an HA cluster is the same as adding virtual domains to a standalone FortiGate unit.

To add virtual domains to a cluster

1. Connect to the cluster web-based manager as the admin administrator.
   If virtual domain configuration is enabled, the Virtual Domain Configuration web-based manager page is displayed.
2. Select Create New to add a virtual domain.
3. Enter a name for the new virtual domain and select OK.
   Add more virtual domains as required.

Enabling virtual clustering

After configuring the cluster, enabling virtual domain configuration, and adding virtual domains you are ready to enable virtual clustering. Before enabling virtual clustering, a cluster of FortiGate units with virtual domains enabled operates in the same way as a standard HA cluster. One FortiGate unit in the cluster operates as the primary unit for all of the virtual domains. The cluster operates in active-passive mode, so only the primary unit processes traffic.

Enable virtual clustering by modifying the HA configuration to distribute the virtual domains between two virtual clusters. Then by adjusting device priorities for each cluster unit in each virtual cluster, one of the cluster units can operate as the primary unit for some of the virtual domains and the other cluster unit can operate as the primary unit for the other virtual domains. The result is traffic processing distributed between both cluster units, achieving a result similar to an active-active HA.

To enable virtual clustering

1. Connect to the cluster web-based manager as the admin administrator.
   The Virtual Domain Configuration web-based manager page is displayed.
2. Select Global Configuration.
3. Go to System > Config > HA.
   The Cluster Members List is displayed showing only Virtual Cluster 1. All virtual domains and both cluster units are shown in Virtual Cluster 1.

Note: The following steps are not required if you are only using virtual clustering for failover protection. Completing these steps only results in distributing traffic between both cluster units in the virtual cluster.
Enabling virtual clustering

Configuring and connecting virtual clusters

4 Select the Edit icon for the primary (master) unit for Virtual Cluster 1.

5 Under VDOM portioning distribute the virtual domains between virtual cluster 1 and virtual cluster 2.

Initially all virtual domains are added to virtual cluster 1. In most cases you would want to distribute the virtual domains between both virtual clusters so that each virtual cluster processes the same amount of network traffic. This makes sure that traffic is evenly distributed between the cluster units. You can distribute the virtual domains however you want. This distribution can also be changed at any time.

6 Select OK.

The cluster renegotiates. After a few seconds the cluster members list displays both virtual clusters. If you have not changed any device priority settings, the same cluster unit is the primary unit (master) for both virtual domains.

7 Select the edit icon for the primary unit for virtual cluster 1 or virtual cluster 2.

Virtual clustering HA options are displayed. You can change the device priority for the primary unit in both of the virtual clusters.

---

**Figure 40: Example Cluster Members list with two virtual domains in Virtual Cluster 1**

<table>
<thead>
<tr>
<th>Virtual Cluster 1</th>
<th>View HA Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cluster Member</td>
</tr>
<tr>
<td><img src="image1" alt="Cluster Members" /></td>
<td>Fgt-5003_slot3</td>
</tr>
<tr>
<td><img src="image2" alt="Cluster Members" /></td>
<td>Fgt-5003_slot4</td>
</tr>
</tbody>
</table>

**Figure 41: Example Cluster Members list with virtual domains distributed between both virtual clusters**

<table>
<thead>
<tr>
<th>Virtual Cluster 1</th>
<th>View HA Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cluster Member</td>
</tr>
<tr>
<td><img src="image3" alt="Cluster Members" /></td>
<td>Fgt-5003_slot3</td>
</tr>
<tr>
<td><img src="image4" alt="Cluster Members" /></td>
<td>Fgt-5003_slot4</td>
</tr>
</tbody>
</table>

**Virtual Cluster 2**

Virtual Domains: vdom_1

<table>
<thead>
<tr>
<th>Cluster Member</th>
<th>Hostname</th>
<th>Role</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image5" alt="Cluster Members" /></td>
<td>Fgt-5003_slot3</td>
<td>MASTER</td>
<td>120</td>
</tr>
<tr>
<td><img src="image6" alt="Cluster Members" /></td>
<td>Fgt-5003_slot4</td>
<td>SLAVE</td>
<td>120</td>
</tr>
</tbody>
</table>
8. Set the Device priority for this cluster unit to 200 in virtual cluster 1 and to 50 in virtual cluster 2 and select OK.

You can select different device priority values. If no other device priority values have been changed the selected cluster unit becomes the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2.

Figure 42: Example Cluster Members list with virtual domains distributed between both virtual clusters and device priorities changed

You can also configure other HA settings for the virtual cluster. See “Virtual clustering load balancing configuration” on page 123

Virtual clustering load balancing configuration

To simplify configuration of virtual clustering, you do not have to configure HA separately for each virtual domain. Instead you create a global HA configuration similar to the standard HA configuration without virtual domains.

The HA configuration for virtual clustering includes configuring VDOM partitioning of virtual domains between two virtual clusters (called Virtual Cluster 1 and Virtual Cluster 2). You configure VDOM partitioning by distributing virtual domains between the two virtual clusters. You can also set the device priority that each cluster unit has in each virtual cluster. By default both cluster units have the same device priority in each virtual cluster and the FGCP automatically selects the primary unit for each virtual cluster.

Once the cluster is operating, you can divide the virtual domains between virtual cluster 1 and virtual cluster 2 to distribute traffic between these virtual clusters. Then you can adjust device priorities so that one cluster unit is the primary unit for virtual cluster 1 and the other cluster unit is the primary unit for virtual cluster 2. Since the primary unit processes all traffic for a virtual domain the end result is that both FortiGate units in the cluster are processing traffic. The primary unit for virtual cluster 1 is processing all of the traffic for the virtual domains in virtual cluster 1 and the primary unit for virtual cluster 2 is processing all of the traffic for the virtual domains in virtual cluster 2.
At any time you can move virtual domains between virtual cluster 1 and virtual cluster 2 to adjust load balancing between the cluster units.

This section describes a simple virtual domain configuration and how to implement it on a virtual cluster so that traffic received by the cluster is processed by both cluster units. The virtual domain configuration is described in Table 9.

Table 9: Example virtual domain configuration

<table>
<thead>
<tr>
<th>Virtual Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>Contains the port5 and port6 interfaces. port5 is connected to an internal network called Site 1. port6 is connected to an external router and the Internet. All traffic from Site 1 is received by port5 and all allowed traffic is forwarded out port6 to the Internet.</td>
</tr>
<tr>
<td>vdom_1</td>
<td>Contains the port7 and port8 interfaces. port7 is connected to an internal network called Site 2. port8 is connected to an external router and the Internet. All traffic from Site 2 is received by port7 and all allowed traffic is forwarded out port8 to the Internet.</td>
</tr>
</tbody>
</table>

This virtual cluster consists of two FortiGate-5001SX units with host names FortiGate_A and FortiGate_B. Virtual clustering is configured so that all traffic received by the root virtual domain is processed by FortiGate_A and all traffic received by the vdom_1 virtual domain is processed by FortiGate_B. The virtual clustering configuration is shown in Table 10 and Table 11. The virtual cluster and how traffic flows through the cluster is shown in Figure 43.

Table 10: Virtual Cluster 1 configuration

<table>
<thead>
<tr>
<th>Virtual Domains</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FortiGate_A</td>
</tr>
<tr>
<td>root</td>
<td>Priority</td>
</tr>
<tr>
<td></td>
<td>200</td>
</tr>
<tr>
<td>Role</td>
<td>Primary</td>
</tr>
</tbody>
</table>

Table 11: Virtual Cluster 2 configuration

<table>
<thead>
<tr>
<th>Virtual Domains</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FortiGate_A</td>
</tr>
<tr>
<td>vdom_1</td>
<td>Priority</td>
</tr>
<tr>
<td></td>
<td>100</td>
</tr>
<tr>
<td>Role</td>
<td>Subordinate</td>
</tr>
</tbody>
</table>
To connect the root virtual domain, the port5 interfaces of both cluster units are connected to a switch that is also connected to the Site 1 network. The port6 interfaces of both cluster units are connected to a switch that is also connected to the external router and to the Internet.

To connect the vdom_1 virtual domain, the port7 interfaces of both cluster units are connected to a switch that is also connected to the Site 2 network. The port8 interfaces of both cluster units are connected to a switch that is also connected to the external router and to the Internet.

The virtual clusters have been configured so that FortiGate_A is the primary unit for the root virtual domain. This means that all traffic destined for the root virtual domain is received and processed by FortiGate_A.

FortiGate-B is the primary unit for vdom_1. This means that all traffic destined for vdom_1 is received and processed by FortiGate_B.

A benefit of this virtual cluster configuration is load balancing between the cluster units. FortiGate_A is processing root traffic and FortiGate_B is processing vdom_1 traffic. So the load for all traffic is shared between the cluster units.

If FortiGate_A fails, FortiGate_B becomes the primary unit for both virtual clusters.
Configuring and operating FortiGate full mesh HA

This chapter provides an introduction to full mesh HA and also contains general procedures and configuration examples that describe how to configure FortiGate full mesh HA.

The examples in this chapter include example values only. In most cases you will substitute your own values. The examples in this chapter also do not contain detailed descriptions of configuration parameters. For information about FortiGate HA configuration parameters, see your FortiGate unit online help or “Configuration reference” on page 49.

This chapter contains the following sections:

- Full mesh HA overview
- Full mesh HA configuration example

Full mesh HA overview

FortiGate models 800 and above can use redundant interfaces to create a cluster configuration called full mesh HA. Full mesh HA is a method of reducing the number of single points of failure on a network that includes an HA cluster.

When two or more FortiGate units are connected to a network in an HA cluster the reliability of the network is improved because the HA cluster replaces a single FortiGate unit as a single point of failure. With a cluster, a single FortiGate unit is replaced by a cluster of two or more FortiGate units.

However, even with a cluster, potential single points of failure remain. The interfaces of each cluster unit connect to a single switch and that switch provides a single connection to the network. If the switch fails or if the connection between the switch and the network fails service is interrupted to that network.
The HA cluster does improve the reliability of the network because switches are not as complex components as FortiGate units, so are less likely to fail. However, for even greater reliability, a configuration is required that includes redundant connections between the cluster the networks that it is connected to.

This redundant configuration can be achieved using FortiGate redundant interfaces and a full mesh HA configuration. In a full mesh HA configuration, you connect an HA cluster consisting of two or more FortiGate units to the network using redundant interfaces and redundant switches. Each redundant interface is connected to two switches and both of these switches are connected to the network.

The resulting full mesh configuration, an example is shown in Figure 45, includes redundant connections between all network components. If any single component or any single connection fails, traffic switches to the redundant component and connection.
Full mesh HA and redundant heartbeat interfaces

A full mesh HA configuration also includes redundant HA heartbeat interfaces. At least two heartbeat interfaces should be selected in the HA configuration and both sets of HA heartbeat interfaces should be connected. The HA heartbeat interfaces do not have to be configured as redundant interfaces because the FGCP handles failover between heartbeat interfaces.

Full mesh HA, redundant interfaces and 802.3ad aggregate interfaces

Full mesh HA is supported for both redundant interfaces and 802.3ad aggregate interfaces. In most cases you would simply use redundant interfaces. However, if your switches support 802.3ad aggregate interfaces and split multi-trunking you can use aggregate interfaces in place of redundant interfaces for full mesh HA. One advantage of using aggregate interfaces is that all of the physical interfaces in the aggregate interface can send and receive packets. As a result, using aggregate interfaces may increase the bandwidth capacity of the cluster.

Usually redundant and aggregate interfaces consist of two physical interfaces. However, you can add more than two physical interfaces to a redundant or aggregate interface. Adding more interfaces can increase redundancy protection. Adding more interfaces can also increase bandwidth capacity if you are using 802.3ad aggregate interfaces.
Full mesh HA configuration example

Figure 46 shows a full mesh HA configuration with a cluster of two FortiGate-5001SX units. This section describes the FortiGate configuration settings and network components required for a full mesh HA configuration. This section also contains example steps for setting up this full mesh HA configuration. The procedures in this section describe one of many possible sequences of steps for configuring full mesh HA. As you become more experienced with FortiOS, HA, and full mesh HA you may choose to use a different sequence of configuration steps.

For simplicity these procedures assume that you are starting with two new FortiGate units set to the factory default configuration. However, starting from the default configuration is not a requirement for a successful HA deployment. FortiGate HA is flexible enough to support a successful configuration from many different starting points.

These procedures describe how to configure a cluster operating in NAT/Route mode because NAT/Route is the default FortiGate operating mode. However, the steps are the same if the cluster operates in Transparent mode. You can either switch the cluster units to operate in Transparent mode before beginning these procedures, or you can switch the cluster to operate in Transparent mode after HA is configured and the cluster is connected and operating.

Figure 46: Example full mesh HA configuration
FortiGate-5001SX full mesh HA configuration

The two FortiGate-5001SX units (1 and 2) can be operating in NAT/Route or Transparent mode. Aside from the standard HA settings, the FortiGate-5001SX configuration includes the following:

- The port9 and port10 interfaces configured as heartbeat interfaces (default configuration)
- The port1 and port2 interfaces added to a redundant interface. Port1 is the active physical interface in this redundant interface
- The port3 and port4 interfaces added to a redundant interface. Port3 is the active physical interface in this redundant interface

A full mesh HA configuration also includes redundant HA heartbeat interfaces. If the FortiGate-5001SX units are installed in a FortiGate-5020 chassis, the redundant port9 and port10 HA heartbeat interfaces are connected through the chassis backplane. If the FortiGate-5001SX units are installed in a FortiGate-5050 or FortiGate-5140 chassis you must install redundant FortiSwitch modules (for example two FortiSwitch-5003 units).

Full mesh switch configuration

Two switches (or equivalent optical hubs) labeled switch 1 and switch 2 and connected to the internal network. Establish an interswitch-link (ISL) between switch 1 and switch 2.

Two switches (or equivalent optical hubs) labelled switch 3 and switch 4 and connected to the external router and the Internet. Establish an interswitch-link (ISL) between switch 1 and switch 2.

Full mesh network connections

Make the following physical network connections for FortiGate 1:

- Port1 to switch 1 (active)
- Port2 to switch 2 (inactive)
- Port3 to switch 3 (active)
- Port4 to switch 4 (inactive)

Make the following physical network connections for FortiGate 2:

- Port1 to switch 2 (active)
- Port2 to switch 1 (inactive)
- Port3 to switch 4 (active)
- Port4 to switch 3 (inactive)

How packets travel from the internal network through the full mesh cluster and to the Internet

If the cluster is operating in active-passive mode and FortiGate 2 is the primary unit, all packets take the following path from the internal network to the internet:

1. From the internal network to switch 2. (Switch 2 is the active connection to FortiGate 2; which is the primary unit. The primary unit receives all packets.)
2. From switch 2 to the FortiGate 2 port1 interface. (Active connection between switch 2 and FortiGate 2. Port1 is the active member of the redundant interface)
3 From FortiGate 2 port1 to FortiGate 2 port3. (Active connection between FortiGate 2 and switch 4. Port1 is the active member of the redundant interface)
4 From switch 4 to the external router and the Internet.

Configuring FortiGate-5001SX units for HA operation

Each FortiGate-5001SX unit in the cluster must have the same HA configuration. Use the following procedure to configure the FortiGate-5001SX units for HA operation. See “HA web-based manager options” on page 51 for information about the HA options referenced in this procedure.

To configure the FortiGate-5001SX units for HA operation

1 Install the FortiGate-5001SX units in the chassis. Install FortiSwitch units in the chassis and turn on chassis power.
2 Connect to the web-based manager of one of the FortiGate-5001SX units.
3 Optionally give the FortiGate unit a unique host name.
   Use host names to identify individual cluster units.
4 Go to System > Config > HA.
5 Set Mode to Active-Passive or Active-Active.
6 Enter a password for the cluster.
   The password must be the same for all FortiGate units in the HA cluster.
7 Select OK.

Note: You can accept the default configuration for the remaining HA options and change them later, once the cluster is operating.

The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate unit interfaces (see “Cluster virtual MAC addresses” on page 31). To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to `arp -d`.
8 Repeat this procedure for the other FortiGate-5001SX unit in the cluster.

The FortiGate-5001SX units negotiate to form a cluster.

Adding redundant interfaces to the cluster

Now that the cluster is operating you can add redundant interfaces to the cluster before making additional configuration changes. You cannot add physical interfaces to a redundant interface if the physical interfaces have been configured with an IP address or other interface configuration options. An interface can only be added to a redundant interface if the interface IP/Netmask is set to
0.0.0.0/0.0.0.0. Depending on your FortiGate unit configuration, the interfaces that you want to add to a redundant interface may be set to this IP/Netmask. If the interface IP/Netmask is not 0.0.0.0/0.0.0.0, you must set the IP/Netmask to 0.0.0.0/0.0.0.0 from the CLI. The following command shows how to do this for the port5:

```plaintext
config system interface
  edit port5
    unset ip
end
```

You cannot add a physical interface to a redundant interface if the physical interface is included in other configuration settings. For example, the interface cannot be added to firewall policies, cannot be included in any static routes, you can’t have added any secondary IPs to the interface, and so on.

The following procedure describes how to add port1 and port2 to one redundant interface and port3 and port4 to another redundant interface. Starting at the FortiGate default configuration you must remove default IP addresses from port1 and port2 and you must also remove port2 from the default route. The following procedure does not go into details about how to do this or how to maintain a connection to the web-based manager during these steps. There are a number of ways to complete these steps depending on your configuration. For example you could use a console connection to the CLI to configure a different interface (for example port5) with an IP address and administrative access.

**To add redundant interfaces to the cluster**

1. Connect to the cluster CLI.
2. Edit port1, port2, port3, and port4 to set the IP/Netmask of these interfaces to 0.0.0.0/0.0.0.0.

Use the following CLI commands:

```plaintext
config system interface
  edit port1
    unset ip
next
  edit port2
    unset ip
next
  edit port3
    unset ip
next
  edit port4
    unset ip
end
```

3. Connect to the cluster web-based manager.
4. Go to **Router > Static > Static Route**.
5. Delete the default route.

   You should also delete any other routes added for port1, port2, port3, or port4. You can also edit static routes to set the Device to a different interface name.
6. Go to **System > Network > Interface**.
7. Select Create New and add the first redundant interface.
Connecting the full mesh cluster to your network

Use the following procedure to connect the cluster of two FortiGate-5001SX units in a full mesh HA configuration. The procedure describes how to connect the interfaces of FortiGate 1 and FortiGate 2 as shown in Figure 46 on page 130.

To connect the cluster to your network

1. Make the following physical network connections for FortiGate 1:
   - Connect FortiGate-5001SX port1 to switch 1.
   - Connect FortiGate-5001SX port2 to switch 2.
   - Connect FortiGate-5001SX port3 to switch 3.
   - Connect FortiGate-5001SX port4 to switch 4.

2. Make the following physical network connections for FortiGate 2:
   - Connect FortiGate-5001SX port1 to switch 2.
   - Connect FortiGate-5001SX port2 to switch 1.
   - Connect FortiGate-5001SX port3 to switch 4.
   - Connect FortiGate-5001SX port4 to switch 3.

3. Connect switch 1 and switch 2 to the internal network.
4. Connect switch 3 and switch 4 to the external router.

5. Enable ESL communication between switch 1 and switch 2 and between switch 3 and switch 4.

The basic full mesh HA configuration is now complete. You can configure the cluster in the same way as configuring a standalone FortiGate unit. You can operate the cluster and change HA settings in the same way as a standard HA cluster.

Full mesh HA for virtual clustering

FortiGate models 800 and above support full mesh HA configuration for a FortiGate cluster operating as a virtual cluster. Configuring full mesh HA for virtual clustering is just an extension of full mesh HA to each virtual domain in the cluster.
For example, a cluster of two FortiGate-5001SX units can operate as an HA cluster with virtual domains and virtual clustering enabled. The cluster can be configured with two virtual domains: the root virtual domain and you can add a virtual domain and name it vdom_1.

The root virtual domain can contain the following interfaces:

- Redundant interface R_Int_1_2 containing physical interfaces port1 and port2. R_Int_1_2 can be connected to redundant switches connected to an internal network.
- Redundant interface R_Int_3_4 containing physical interfaces port3 and port4. R_Int_3_4 can be connected to redundant switches connected to the Internet.

The vdom_1 virtual domain can contain the following interfaces:

- Redundant interface R_Int_5_6 containing physical interfaces port5 and port6. R_Int_5_6 can be connected to redundant switches connected to an internal network.
- Redundant interface R_Int_7_8 containing physical interfaces port7 and port8. R_Int_7_8 can be connected to redundant switches connected to the Internet.

You could mix full mesh and regular HA configurations between virtual domains. For example, you can configure full mesh HA for the root virtual domain and regular HA for the vdom_1 virtual domain.

**Note:** The physical interfaces that you add to a redundant interface must be added to the same virtual domain as the redundant interface before you can add them to the redundant interface.
Operating a cluster

With some exceptions, you can operate a cluster in much the same way as you operate a standalone FortiGate unit. This chapter describes those exceptions and also the similarities involved in operating a cluster instead of a standalone FortiGate unit. This chapter also describes how to configure some advanced HA configuration options.

This chapter contains the following sections:

- Operating a cluster
- HA clusters and FortiGuard services
- Clusters and logging
- Clusters and SNMP
- Clusters and quarantine
- Advanced HA configuration options
- Managing a FortiGate virtual clustering configuration

The configurations of all of the FortiGate units in a cluster are synchronized so that the FortiGate units can simulate a single FortiGate unit. Because of this synchronization, you manage the HA cluster instead of managing the individual cluster units. You manage the cluster by connecting to the web-based manager using any cluster interface configured for HTTPS or HTTP administrative access. You can also manage the cluster by connecting to the CLI using any cluster interface configured for SSH or telnet administrative access.

The cluster web-based manager dashboard displays the cluster name, the host name and serial number of each cluster member, and also shows the role of each unit in the cluster. The roles can be master (primary unit) and slave (subordinate units). The dashboard also displays a cluster unit front panel illustration.

Figure 47: Example cluster web-based manager dashboard
You can also go to **System > Config > HA** to view the cluster members list. This includes status information for each cluster unit. You can also use the cluster members list for a number of HA cluster management functions including changing the HA configuration of an operating cluster, changing the host name and device priority of a subordinate unit, and disconnecting a cluster unit from a cluster. See “Cluster members list overview” on page 139.

You can use FortiGate log messages to view information about the status of the cluster. See “Viewing and managing log messages for individual cluster units” on page 144. You can use SNMP to manage the cluster by configuring a cluster interface for SNMP administrative access. Using an SNMP manager you can get cluster configuration information and receive traps. For a list of HA MIB fields, see “HA-related FortiGate traps” on page 155 and “HA MIB fields” on page 156.

If your FortiGate model has a front panel LCD you can identify the role of a cluster unit. On the primary unit the LCD displays **primary**. One the subordinate units, the LCD displays **slave <priority_id>**. The **priority_id** is the priority that the subordinate unit has in the cluster. If there are three units in an active-active Cluster the LCD displays are:

- primary (a-a)
- slave 1 (a-a)
- slave 2 (a-a)

You can manage individual cluster units by using SSH, telnet, or the CLI console on the web-based manager dashboard to connect to the CLI of the cluster. From the CLI you can use the `execute ha manage` command to connect to the CLI of any unit in the cluster.

You can also manage individual cluster units by using a null-modem cable to connect to any cluster unit CLI. From there you can use the `execute ha manage` command to connect to the CLI of each unit in the cluster. See “Managing individual cluster units” on page 146 for more information.

- About HA configuration synchronization
- Cluster members list overview
- Changing the HA configuration of an operating cluster
- Changing subordinate unit host name and device priority
- Upgrading HA cluster firmware
- Changing how the cluster processes firmware upgrades
- Adding a new unit to a functioning cluster
- Viewing and managing log messages for individual cluster units
- About HA event log messages
- Monitoring cluster units for failover
- Managing individual cluster units
- Disconnecting a cluster unit from a cluster
- Adding a disconnected FortiGate unit back to its cluster

**About HA configuration synchronization**

You can change the cluster configuration by connecting to the cluster and changing the configuration of the primary unit. The cluster automatically synchronizes all configuration changes to the subordinate units in the cluster as the changes are made.
From the CLI if you make changes to a subordinate unit configuration, these changes are also synchronized to all cluster units.

The only configuration changes that are not synchronized are the FortiGate host name, the HA device priority, and the HA override CLI setting. You can give each cluster unit a unique host name to help to identify cluster members. Individual cluster units are also identified by their serial number. For more information about cluster synchronization, see the FortiGate HA Overview and the FortiGate HA Guide.

Cluster members list overview

Display the cluster members list to view the status of the FortiGate units in an operating cluster. To display the cluster members list, go to System > Config > HA.

From the cluster members list you can also:
- View HA statistics (see “Viewing HA statistics” on page 140).
- View and optionally change the HA configuration of the operating cluster (see “Changing the HA configuration of an operating cluster” on page 141).
- View and optionally change the host name and device priority of a subordinate unit (see “Changing subordinate unit host name and device priority” on page 142).
- Disconnect a cluster unit from a cluster (see “Disconnecting a cluster unit from a cluster” on page 146).
- Download the Debug log for any cluster unit. You can send this debug log file to Fortinet Technical Support to help diagnose problems with the cluster or with individual cluster units.

Figure 48: Example FortiGate-5001SX cluster members list

View HA Statistics
Display the serial number, status, and monitor information for each cluster unit. See “Viewing HA statistics” on page 140.

Up and down arrows
Change the order in which cluster members are listed. The operation of the cluster or of the units in the cluster are not affected. All that changes is the order in which cluster units are displayed on the cluster members list.

Cluster member
Illustrations of the front panels of the cluster units. If the network jack for an interface is shaded green, the interface is connected. Pause the mouse pointer over each illustration to view the cluster unit host name, serial number, and how long the unit has been operating (up time). The list of monitored interfaces is also displayed.
Viewing HA statistics

From the cluster members list you can select View HA statistics to display the serial number, status, and monitor information for each cluster unit. To view HA statistics, go to System > Config > HA and select View HA Statistics.

**Figure 49: Example HA statistics (active-passive cluster)**

<table>
<thead>
<tr>
<th>Serial No.</th>
<th>Status</th>
<th>Up Time</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGS0012664400960</td>
<td>0 days 0 hours 49 minutes 44 seconds</td>
<td>Memory Usage</td>
<td>Network Utilization 15 Kbps</td>
</tr>
<tr>
<td>FGS0012664400980</td>
<td>0 days 0 hours 44 minutes 34 seconds</td>
<td>Memory Usage</td>
<td>Network Utilization 4 Kbps</td>
</tr>
</tbody>
</table>
### Changing the HA configuration of an operating cluster

To change the configuration settings of an operating cluster, go to **System > Config > HA** to display the cluster members list. Select Edit for the master (or primary) unit in the cluster members list to display the HA configuration page for the cluster.

You can use the HA configuration page to check and fine tune the configuration of the cluster after the cluster is up and running. For example, if you connect or disconnect cluster interfaces you may want to change the Port Monitor configuration.

Any changes you make on this page, with the exception of changes to the device priority, are first made to the primary unit configuration and then synchronized to the subordinate units. Changing the device priority only affects the primary unit.

<table>
<thead>
<tr>
<th>Refresh every</th>
<th>Select to control how often the web-based manager updates the HA statistics display.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back to HA monitor</td>
<td>Close the HA statistics list and return to the cluster members list.</td>
</tr>
<tr>
<td>Serial No.</td>
<td>Use the serial number ID to identify each FortiGate unit in the cluster. The cluster ID matches the FortiGate unit serial number.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of each cluster unit. A green check mark indicates that the cluster unit is operating normally. A red X indicates that the cluster unit cannot communicate with the primary unit.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time in days, hours, minutes, and seconds since the cluster unit was last started.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Displays system status information for each cluster unit.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>The current CPU status of each cluster unit. The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>The current memory status of each cluster unit. The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>The number of communications sessions being processed by the cluster unit.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>The number of packets that have been processed by the cluster unit since it last started up.</td>
</tr>
<tr>
<td>Virus Detected</td>
<td>The number of viruses detected by the cluster unit.</td>
</tr>
<tr>
<td>Network Utilization</td>
<td>The total network bandwidth being used by all of the cluster unit interfaces.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>The number of bytes that have been processed by the cluster unit since it last started up.</td>
</tr>
<tr>
<td>Intrusion Detected</td>
<td>The number of intrusions or attacks detected by Intrusion Protection running on the cluster unit.</td>
</tr>
</tbody>
</table>
Changing subordinate unit host name and device priority

To change the host name and device priority of a subordinate unit in an operating cluster, go to **System > Config > HA** to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

To change the host name and device priority of a subordinate unit in an operating cluster with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to **System > Config > HA** to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

You can change the host name (Peer) and device priority (Priority) of this subordinate unit. These changes only affect the configuration of the subordinate unit.

**Figure 50: High Availability configuration**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Active-Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Priority</td>
<td>128</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cluster Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peer Monitor</th>
<th>Heartbeat Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td></td>
</tr>
<tr>
<td>port2</td>
<td></td>
</tr>
<tr>
<td>port3</td>
<td></td>
</tr>
<tr>
<td>port4</td>
<td></td>
</tr>
<tr>
<td>port5</td>
<td></td>
</tr>
<tr>
<td>port6</td>
<td></td>
</tr>
<tr>
<td>port7</td>
<td></td>
</tr>
<tr>
<td>port8</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 51: Changing the subordinate unit host name and device priority**

**Peer**

View and optionally change the subordinate unit host name.

**Priority**

View and optionally change the subordinate unit device priority.

The device priority is not synchronized among cluster members. In a functioning cluster you can change device priority to change the priority of any unit in the cluster. The next time the cluster negotiates, the cluster unit with the highest device priority becomes the primary unit.

The device priority range is 0 to 255. The default device priority is 128.
Upgrading HA cluster firmware

You can upgrade the FortiOS firmware running on an HA cluster in the same manner as upgrading the firmware running on a standalone FortiGate unit. During a normal firmware upgrade, the cluster upgrades the primary unit and all subordinate units to run the new firmware image. The firmware upgrade takes place without interrupting communication through the cluster.

To upgrade the firmware without interrupting communication through the cluster, the cluster goes through a series of steps that involve first upgrading the firmware running on the subordinate units, then making one of the subordinate units the primary unit, and finally upgrading the firmware on the former primary unit. These steps are transparent to the user and the network, but depending upon your HA configuration may result in the cluster selecting a new primary unit.

The following sequence describes in detail the steps the cluster goes through during a firmware upgrade and how different HA configuration settings may affect the outcome.

1. The administrator uploads a new firmware image from the web-based manager or CLI.
2. If the cluster is operating in active-active mode load balancing is turned off.
3. The cluster upgrades the firmware running on all of the subordinate units.
4. Once the subordinate units have been upgraded, a new primary unit is selected. This primary unit will be running the new upgraded firmware.
5. The cluster now upgrades the firmware of the former primary unit.
6. Depending on the device priority and override configuration of the cluster, one of the following happens:
   - If override is enabled and the former primary unit has the highest device priority, the cluster renegotiates and the former primary unit (or the unit with the highest device priority) once again becomes the primary unit.
   - If override is not enabled or if all cluster units have the same device priority, the new primary unit continues to operate as the primary unit and the former primary unit continues to operate as a subordinate unit.
7. If the cluster is operating in active-active mode, load balancing is turned back on.

Changing how the cluster processes firmware upgrades

By default cluster firmware upgrades proceed as described in "Upgrading HA cluster firmware" on page 143. If required, you can use the following CLI command to change how the cluster handles firmware upgrades.

```plaintext
config system ha
   set uninterruptable-upgrade {disable | enable}
end
```

`uninterruptable-upgrade` is enabled by default. If you disable `uninterruptable-upgrade` the cluster still upgrades the firmware on all cluster units, but all cluster units are upgraded at once; which interrupts communication through the cluster.
Adding a new unit to a functioning cluster

This procedure describes how to add a new FortiGate unit to a functioning cluster. Adding a new unit to a cluster does not interrupt the operation of the cluster.

To add a new unit to a functioning cluster

1. Configure the new cluster unit for HA operation with the same HA configuration as the other units in the cluster.
2. If the cluster is running in Transparent mode, change the operating mode of the new cluster unit to Transparent mode.
3. Connect the new cluster unit to the cluster.
4. Power on the new cluster unit.
   When the unit starts it negotiates to join the cluster. After it joins the cluster, the cluster synchronizes the new unit configuration with the configuration of the primary unit.

Viewing and managing log messages for individual cluster units

1. Connect to the cluster and log into the web-based manager.
   For each log display, the HA Cluster list displays the serial number of the FortiGate unit for which log messages are displayed.
3. Set HA Cluster to the serial number of one of the cluster units to display log messages for that cluster unit.
   You can view, search and manage logs saved to memory or logs saved to the hard disk, depending on the Log & Report configuration of the cluster.

About HA event log messages

HA event log messages always include the host name and serial number of the cluster unit that recorded the message. Most HA log event log messages indicate when a cluster unit switches (or moves) from one HA state to another.

Cluster units can operate in the HA states listed in Table 12:

<table>
<thead>
<tr>
<th>Table 12: HA states</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hello</strong></td>
</tr>
<tr>
<td>A FortiGate unit configured for HA operation has started up and is looking for other FortiGate units with which to form a cluster.</td>
</tr>
<tr>
<td><strong>Work</strong></td>
</tr>
<tr>
<td>In an active-passive cluster a cluster unit is operating as the primary unit. In an active-active cluster unit is operating as the primary unit or a subordinate unit.</td>
</tr>
<tr>
<td><strong>Standby</strong></td>
</tr>
<tr>
<td>In an active-passive cluster the cluster unit is operating as a subordinate unit.</td>
</tr>
</tbody>
</table>

HA log Event log messages also indicate the virtual cluster that the cluster unit is operating in as well as the member number of the unit in the cluster. If virtual domains are not enabled, all clusters unit are always operating in virtual cluster 1. If virtual domains are enabled, a cluster unit may be operating in virtual cluster 1 or virtual cluster 2. The member number indicates the position of the cluster unit in the cluster members list. Member 0 is the primary unit. Member 1 is the first subordinate unit, member 2 is the second subordinate unit, and so on.
The following log message indicates that the cluster unit with host name 5001_Slot_4 and serial number FG50012204400045 has become the primary unit because it is operating in the work state as member 0.

2006-06-05 09:18:21 device_id=FG50012204400045
log_id=0105035001 type=event subtype=ha pri=notice msg="HA member 5001_Slot_4[FG50012204400045] move to work state in virtual cluster 1 as member 0"

The following log message indicates that the cluster unit with host name 5001_Slot_3 and serial number FG50012205400050 has become the first subordinate unit in an active-passive cluster because it is operating in the standby state as member 1.

2006-06-05 09:18:21 device_id=FG50012205400050
log_id=0105035001 type=event subtype=ha pri=notice msg="HA member 5001_Slot_3[FG50012205400050] move to standby state in virtual cluster 1 as member 1"

The following log message indicates that the cluster unit with host name 5001_Slot_3 and serial number FG50012205400050 has become the first subordinate unit in an active-active cluster because it is operating in the work state as member 1.

2006-06-05 10:11:12 device_id=FG50012205400050
log_id=0105035001 type=event subtype=ha pri=notice msg="HA member 5001_Slot_3[FG50012205400050] move to work state in virtual cluster 1 as member 1"

Monitoring cluster units for failover

If the primary unit in the cluster fails, the units in the cluster renegotiate to select a new primary unit. Failure of the primary unit results in the following:

- If SNMP is enabled, the new primary unit sends the trap message "HA switch". This trap indicates that the primary unit in an HA cluster has failed and has been replaced with a new primary unit.
- If event logging is enabled and HA activity event is selected, the new primary unit records a log message similar to the following that shows that the unit has become the primary unit for the cluster:
  
  2006-06-05 08:44:15 device_id=FG50012204400045
  log_id=0105035001 type=event subtype=ha pri=notice msg="HA member 5001_Slot_4[FG50012204400045] move to work state in virtual cluster 1 as member 0"

- If alert email is configured to send email for HA status changes, the new primary unit sends an alert email containing the log message recorded by the event log.
  
  - The cluster contains fewer FortiGate units. The failed primary unit no longer appears on the Cluster Members list.
  - The host name and serial number of the primary unit changes.

If a subordinate unit fails, the cluster continues to function normally. Failure of a subordinate unit results in the following:

- The cluster contains fewer FortiGate units. The failed unit no longer appears on the Cluster Members list.
Managing individual cluster units

The following procedure describes how to use SSH to log into the primary unit CLI and from there to use the `execute ha manage` command to connect to the CLI of any other unit in the cluster. The procedure is very similar if you use telnet, or the web-based manager dashboard CLI console.

You can use the `execute ha manage` command from the CLI of any cluster unit to log into the CLI of another cluster unit. Usually you would use this command from the CLI of the primary unit to log into the CLI of a subordinate unit. However, if you have logged into a subordinate unit CLI, you can use this command to log into the primary unit CLI, or the CLI of another subordinate unit.

Using SSH or telnet or the web-based manager dashboard CLI console you can only log into the primary unit CLI. Using a direct console connection you can log into any cluster unit. In both cases you can use `execute ha manage` to connect to the CLI of other cluster units.

**Note:** You log into the subordinate unit using the FGT_ha_admin administrator account. This built-in administrator account gives you read and write permission on the subordinate unit. Normally this built-in administrative account is not visible, however FGT_ha_admin does appear in event log messages.

1. Use SSH to connect to the cluster and log into the primary unit CLI. Connect to any cluster interface configured for SSH administrative access to log into the cluster.

2. Enter the following command followed by a space and type a question mark (?):
   ```
   execute ha manage
   ```
   The CLI displays a list of all the subordinate units in the cluster. Each cluster unit is numbered, starting at 1. The information displayed for each cluster unit includes the unit serial number and the host name of the unit.

3. Complete the command with the number of the subordinate unit to log into. For example, to log into subordinate unit 1, enter the following command:
   ```
   execute ha manage 1
   ```
   Press Enter to connect to and log into the CLI of the selected subordinate unit. If this subordinate unit has a different host name, the CLI prompt changes to this host name.
   You can use CLI commands to manage this subordinate unit. If you make changes to the configuration of any cluster unit (primary or subordinate unit) these changes are synchronized to all cluster units.

4. You can now use the `execute ha manage` command to connect to any other cluster unit (including the primary unit). You can also use the `exit` command to return to the primary unit CLI.

Disconnecting a cluster unit from a cluster

Use the following procedures to disconnect a cluster unit from a functioning cluster without disrupting the operation of the cluster. You can disconnect a cluster unit if you need to use the disconnected FortiGate unit for another purpose, such as to act as a standalone firewall.
You can use the following procedures for a standard cluster and for a virtual clustering configuration. To use the following procedures from a virtual cluster you must be logged in as the admin administrator and you must have selected Global Configuration.

When you disconnect a cluster unit you must assign an IP address and netmask to one of the interfaces of the disconnected unit. You can disconnect any unit from the cluster even the primary unit. After the unit is disconnected, the cluster responds as if the disconnected unit has failed. The cluster may renegotiate and may select a new primary unit.

When the cluster unit is disconnected the HA mode is changed to standalone. In addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0 except for the interface that you configure.

Otherwise the configuration of the disconnected unit is not changed. The HA configuration of the disconnected unit is not changed either.

**To disconnect a cluster unit from a cluster**

1. Go to System > Config > HA to view the cluster members list.
2. Select the Disconnect from cluster icon for the cluster unit to disconnect from the cluster.

**Figure 52: Disconnect a cluster member**

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Interface</th>
<th>IP/Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGT50026B1021077</td>
<td>Internal</td>
<td>10.1.1.12/24</td>
</tr>
</tbody>
</table>

Serial Number
Displays the serial number of the cluster unit to be disconnected from the cluster.

Interface
Select the interface that you want to configure. You also specify the IP address and netmask for this interface. When the FortiGate unit is disconnected, all management access options are enabled for this interface.

IP/Netmask
Specify an IP address and netmask for the interface. You can use this IP address to connect to this interface to configure the disconnected FortiGate unit.

3. Select OK.

The FortiGate unit is disconnected from the cluster and the cluster may renegotiation and select a new primary unit. The selected interface of the disconnected unit is configured with the specified IP address and netmask.

**Adding a disconnected FortiGate unit back to its cluster**

If you have disconnected a FortiGate unit from a cluster, you can re-connect the disconnected FortiGate unit to the cluster by setting the HA mode of the disconnected unit to match the HA mode of the cluster. Usually the disconnected unit rejoins the cluster as a subordinate unit and the cluster automatically synchronizes its configuration.
Cluster communication with RADIUS and LDAP servers

Operating a cluster

**Note:** You do not have to change the HA password on the disconnected unit unless the HA password has been changed after the unit was disconnected. Disconnecting a unit from a cluster does not change the HA password.

**Caution:** You should make sure that the device priority of the disconnected unit is lower than the device priority of the current primary unit. You should also make sure that the HA override CLI option is not enabled on the disconnected unit. Otherwise, when the disconnected joins the cluster, the cluster will renegotiate and the disconnected unit may become the primary unit. If this happens, the configuration of the disconnected unit is synchronized to all other cluster units. This configuration change might disrupt the operation of the cluster.

The following procedure assumes that the disconnected FortiGate unit is correctly physically connected to your network and to the cluster but is not running in HA mode and not part of the cluster.

Before you start this procedure you should note the device priority of the primary unit.

**To add a disconnected FortiGate unit back to its cluster**

1. Log into the disconnected FortiGate unit.
   If virtual domains are enabled, log in as the admin administrator and select Global Configuration.

2. Go to **System > Config > HA**.

3. Change Mode to match the mode of the cluster.

4. If required, change the group name and password to match the cluster.

5. Set the Device Priority lower than the device priority of the primary unit.

6. Select OK.

   The disconnected FortiGate unit joins the cluster.

**Cluster communication with RADIUS and LDAP servers**

In an operating cluster, only the primary unit communicates with RADIUS and LDAP servers. In a cluster that is operating in active-passive mode, only the primary unit processes traffic, so the primary unit communicates with RADIUS or LDAP servers. In a cluster that is operating in active-active mode, subordinate units send RADIUS and LDAP requests to the primary unit. The primary unit relays the requests to the RADIUS or LDAP server and relays the responses back to the subordinate unit.

**HA clusters and FortiGuard services**

This section describes how various FortiGate HA clustering configurations communicate with the FDN.

In an operating FortiGate HA cluster, only the primary unit communicates with the FortiGuard Distribution Network (FDN). The primary unit communicates with the FDN to download FortiGuard Antivirus updates and FortiGuard Intrusion Protection updates, to request FortiGuard Web Filtering ratings, and to lookup FortiGuard Antispam information.
You must register and licence all of the units in a cluster for all of required FortiGuard services, because any cluster unit could potentially become the primary unit.

**The FDN and active-passive clusters**

For an active-passive cluster, only the primary unit processes traffic and only the primary unit communicates with the FDN. The primary unit receives FortiGuard Antivirus and FortiGuard Intrusion Protection updates from the FDN and copies these updates to the subordinate units. The primary unit also requests FortiGuard Web Filtering ratings and FortiGuard Antispam information. In an active-passive cluster the FortiGuard Web Filter URL cache operates on a primary unit in the same way as for a standalone FortiGate unit.

**The FDN and active-active clusters**

For an active-active cluster, both the primary unit and the subordinate units process traffic. The primary unit receives FortiGuard Antivirus and FortiGuard Intrusion Protection updates from the FDN and copies these updates to the subordinate units. The primary unit requests FortiGuard Web Filtering ratings and FortiGuard Antispam information for the traffic processed by the primary unit.

In an active-active cluster, the primary unit handles FortiGuard Web Filtering and FortiGuard Antispam requests for the subordinate units. Because the subordinate units also process traffic, they send FortiGuard requests to the primary unit and the primary unit relays the requests to the FDN. The primary unit also relays the FDN responses back to the subordinate units. In an active-active cluster, the primary unit FortiGuard Web Filtering URL cache operates on the primary unit and is used for primary unit and subordinate unit URL requests.

**The FDN and virtual clustering**

For a virtual clustering configuration the management virtual domain on the cluster unit that is the primary unit for the management virtual domain communicates with the FDN. This management virtual domain receives FortiGuard Antivirus and Intrusion Protection updates. The updates are copied to both cluster units where they can be used by all of the operating virtual domains.

In a virtual clustering configuration, the virtual domains operate in active-passive HA mode. For each virtual domain, only the primary unit for the virtual domain is processing traffic for that virtual domain. The primary units for each virtual domain send FortiGuard Antispam and FortiGuard Web Filtering requests to the management virtual domain. The primary unit for the management virtual domain sends the requests to the FDN. The primary unit for the management virtual domain receives responses from the FDN and returns the responses to the virtual domains that made the original requests.

The FortiGuard Web Filtering cache operates on the primary unit for the management virtual domain. This cache is used for all FortiGuard Web Filtering requests.
Clustering and logging

This section describes the log messages that provide information about how HA is functioning, how to view and manage logs for each unit in a cluster, and provides some example log messages that are recorded during specific cluster events.

You configure logging for a cluster in the same way as configuring logging for a standalone FortiGate unit. Log configuration changes made to the cluster are shared by all cluster units.

All cluster units record log messages separately to the cluster unit’s log disk or to the cluster unit’s system memory. You can view and manage log messages for each cluster unit from the cluster web-based manager Log Access page.

All cluster units also send log messages to a remote syslog server, FortiLog unit and WebTrends server. Subordinate units first send log messages to the primary unit using the HA heartbeat device link. The primary unit forwards the log messages to the remote syslog server, FortiLog unit, and WebTrends server.

When you configure a FortiLog unit to receive log messages from a FortiGate cluster, you should add each cluster unit to the FortiLog device configuration so that the FortiLog unit can receive log messages from all cluster units.

• Viewing and managing logs for an HA cluster
• HA log messages
• Admin log messages
• Example log message scenarios

Viewing and managing logs for an HA cluster

You can view individual cluster unit logs from the cluster web-based manager.

To view and manage logs for individual cluster units

1 Log into the cluster web-based manager.

2 Go to Log&Report > Log Access.

The Traffic, Event, Attack, Antivirus, Web Filter, and Spam Filter logs for the primary unit are displayed.

The HA Cluster list displays the device ID (the FortiGate serial number) of the cluster unit for which logs are displayed.

3 Select the device ID of a cluster unit to display log messages for that unit.

You can filter, sort, search, and delete log messages for each cluster unit.
HA log messages

The following log messages are generated by HA activity.

**Message ID:** 35001

**Log Type:** Event Log - HA Activity

**Severity:** Notification

**Message:**

- HA group id changed to<value_ha_id>
- HA slave became master
- HA move to standalone mode
- HA move to work status
- HA master became slave
- HA move to standby state
- Detected HA member dead
- Detected new joined HA member

**Meaning:** The messages describe changes in cluster unit status. These changes in status occur if a cluster unit fails or starts up or if a link fails or is restored. These events may cause the cluster to renegotiate and the status of the units in the cluster to change. The events that cause changes in cluster unit status are recorded by the log messages listed below. Each message includes the serial number of the cluster unit reporting the message. You can use the serial number to determine which cluster unit's status has changed.

- **HA group id changed to<value_ha_id>**
  - The group ID has been changed for this cluster unit.

- **HA slave became master**
  - This cluster unit was operating as a subordinate unit and is now the primary unit.

- **HA move to standalone mode**
  - The operation mode of this cluster unit has changed from HA to standalone.
HA log messages

Operating a cluster

---

**HA move to work status**
This cluster unit is now operating in HA mode. In an active-passive cluster, this cluster unit is the primary unit. In an active-active cluster all cluster units operate in work status.

**HA master became slave**
This cluster unit was operating as a primary unit and is now operating as a subordinate unit.

**HA move to standby state**
This cluster unit is now operating in active-passive HA mode as a subordinate unit.

**Detected HA member dead**
This cluster unit has detected that another cluster unit has failed. The message does not specify which cluster unit has failed.

**Detected new joined HA member**
This cluster unit has detected that a new FortiGate unit has joined the cluster.

---

**Message ID:** 35001  
**Log Type:** Event Log - HA Activity  
**Severity:** Warning  
**Message:** HA monitored interface `<interface_name>` link failed  
**Meaning:** The specified monitored interface on this cluster unit failed or was disconnected. This message is only displayed if an interface configured with a HA monitor priority fails or is disconnected.

---

**Message ID:** 35010  
**Log Type:** Event Log - HA Activity  
**Severity:** Critical  
**Message:** HA mode changed to standalone  
**Meaning:** This cluster unit was removed from a cluster because the cluster unit HA mode was changed to standalone.

---

**Message ID:** 35011  
**Log Type:** Event Log - HA Activity  
**Severity:** Critical  
**Message:** HA mode changed to A-A  
**Meaning:** This cluster unit was changed to operate in active-active mode. The cluster unit may have initially be operating in standalone mode or active-passive mode.
### Admin log messages

The following messages are not specifically HA messages, but appear during HA status changes.

**Message ID:** 32007  
**Log Type:** Event Log - Admin Event  
**Severity:** Information  
**Message:** User FGT_ha_admin Logs out from telnet(10.0.0.1).  
**Meaning:** The FGT_ha_admin administrator has logged out of a telnet session. The telnet session is an HA heartbeat telnet session from the primary unit (IP address 10.0.0.1) to the cluster unit that wrote the log message. See "HA Telnet sessions" on page 24 for information about HA heartbeat telnet sessions.

---

**Message ID:** 32138  
**Log Type:** Event Log - Admin Event  
**Severity:** Critical  
**Message:** user=ha_slave ui=ha_daemon action=reboot msg="User ha_slave rebooted the device from ha_daemon"  
**Meaning:** The HA process restarted a subordinate unit. This may occur if the cluster needs to renegotiate or if the configuration or firmware version of the subordinate unit is not synchronized with the primary unit.
Example log message scenarios

This section displays some log message sequences when specific cluster events occur. The date and time stamp is removed from the beginning of each message.

Example: Primary unit removed from cluster
In the following sequence occurs for a cluster of three FortiGate-60 units. In the following sequence, the primary unit fails and the remaining units, negotiate until the cluster unit with serial number 602104400531 becomes the primary unit.

1. device_id=FGT-602803030702 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA slave became master"
2. device_id=FGT-602803030702 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected HA member dead"
3. device_id=FGT-602104400531 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA slave became master"
4. device_id=FGT-602104400531 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected HA member dead"
5. device_id=FGT-602104400531 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA slave became master"
6. device_id=FGT-602104400531 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected HA member dead"
7. device_id=FGT-602803030702 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA master became slave"
8. device_id=FGT-602803030702 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected new joined HA member"
9. device_id=FGT-602104400531 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected new joined HA member"

Example: Primary unit added back to cluster
In the following message sequence a FortiGate unit with serial number 602104400533 is configured with override master enabled and with a higher unit priority than the FortiGate unit with serial number 602803030702 and the FortiGate unit with serial number 602104400531. The FortiGate unit with serial number 602104400533 joins the cluster consisting of the other two FortiGate units.

1. device_id=FGT-602803030702 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA master became slave"
2. device_id=FGT-602803030702 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected new joined HA member"
3. device_id=FGT-602803030702 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA slave became master"
4. device_id=FGT-602104400531 log_id=0105035001 type=event subtype=ha pri=notice vd=root msg="HA slave became master"
Clusters and SNMP

You can use SNMP to manage a cluster by configuring a cluster interface for SNMP administrative access. Using an SNMP manager you can get cluster configuration and status information and receive traps. For a list of HA MIB fields, see “HA-related FortiGate traps” on page 155 and “HA MIB fields” on page 156.

You configure SNMP for a cluster in the same way as configuring SNMP for a standalone FortiGate unit. SNMP configuration changes made to the cluster are shared by all cluster units.

An SNMP manager connects to the primary unit to view configuration and status information for the primary unit. You cannot use SNMP to view configuration and status information for subordinate units.

Both the primary and subordinate units send traps to SNMP managers. Subordinate units first send traps to the primary unit using the HA heartbeat device link. The primary then unit forwards the traps to SNMP managers. HA traps indicate when a cluster unit has started and when interfaces have been connected to disconnected.

Table 13: HA-related FortiGate traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ColdStart</td>
<td>Standard traps as described in RFC 1215.</td>
</tr>
<tr>
<td>WarmStart</td>
<td></td>
</tr>
<tr>
<td>LinkUp</td>
<td></td>
</tr>
<tr>
<td>LinkDown</td>
<td></td>
</tr>
<tr>
<td>HA switch (fnTrapHaSwitch)</td>
<td>The primary unit in an HA cluster fails and is replaced with a new primary unit.</td>
</tr>
<tr>
<td>HA Heartbeat Failure (fnTrapHaHBFail)</td>
<td>HA monitored interface fails heartbeat.</td>
</tr>
</tbody>
</table>
Clustering and quarantine

You can configure quarantine for a cluster in the same way as configuring quarantine for a standalone FortiGate unit. Quarantine configuration changes made to the cluster are shared by all cluster units.

In an active-active cluster, both the primary unit and the subordinate units accept antivirus sessions and may quarantine files. In an active-passive cluster, only the primary unit quarantines files. Multiple cluster units in an active-passive cluster may have quarantined files if different cluster units have been the primary unit.

All cluster units quarantine files separately to their own log disk. You can view and manage log messages for each cluster unit from the cluster web-based manager Log Access page.

Viewing and managing quarantined files for an HA cluster

You can view individual cluster unit quarantined files from the cluster web-based manager.

To view and manage quarantine files for individual cluster units

1. Log into the cluster web-based manager.
2. Go to Anti-Virus > Quarantine > Quarantined Files.
   The quarantined files list is displayed.
   The HA Cluster list displays the device ID (the FortiGate serial number) of the cluster unit for which the quarantined files list is displayed.
3. Select the device ID of a cluster unit to display the quarantine file list for that unit.
   You can sort and filter the quarantined file list for each cluster unit. You can also delete, download, and submit quarantined files for each cluster unit.

### Table 14: HA MIB fields

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnHaSchedule</td>
<td>Load balancing schedule for A-A mode.</td>
</tr>
<tr>
<td>fnHaStatsTable</td>
<td>Statistics for the individual FortiGate unit in the HA cluster.</td>
</tr>
<tr>
<td>fnHaStatsIndex</td>
<td>The index number of the unit in the cluster.</td>
</tr>
<tr>
<td>fnHaStatsSerial</td>
<td>The FortiGate unit serial number.</td>
</tr>
<tr>
<td>fnHaStatsCpuUsage</td>
<td>The current FortiGate unit CPU usage (%).</td>
</tr>
<tr>
<td>fnHaStatsMemUsage</td>
<td>The current unit memory usage (MB).</td>
</tr>
<tr>
<td>fnHaStatsNetUsage</td>
<td>The current unit network utilization (Kbps).</td>
</tr>
<tr>
<td>fnHaStatsSesCount</td>
<td>The number of active sessions.</td>
</tr>
<tr>
<td>fnHaStatsPktCount</td>
<td>The number of packets processed.</td>
</tr>
<tr>
<td>fnHaStatsByteCount</td>
<td>The number of bytes processed by the FortiGate unit</td>
</tr>
<tr>
<td>fnHaStatsIdsCount</td>
<td>The number of attacks that the IPS detected in the last 20 hours.</td>
</tr>
<tr>
<td>fnHaStatsAvCount</td>
<td>The number of viruses that the antivirus system detected in the last 20 hours.</td>
</tr>
</tbody>
</table>
Advanced HA configuration options

A number of advanced HA configuration options are available from the FortiGate CLI. You can use these options to control a number of features such as how routing table updates are synchronized among cluster units, the timing of HA heartbeat packets, and so on. This section describes:

- Controlling how HA synchronizes routing table updates
- Modifying heartbeat timing
- Enabling or disabling HA heartbeat encryption and authentication
- Setting the number of gratuitous arps sent by a primary unit

Controlling how HA synchronizes routing table updates

In a functioning cluster, the primary unit must keep all subordinate unit routing tables up to date and synchronized with the primary unit. You can use the following CLI commands to control the timing of routing table updates.

Command syntax

```
config system ha
  set route-hold <hold_integer>
  set route-ttl <ttl_integer>
  set route-wait <wait_integer>
end
```

**route-hold <hold_integer>**

The time that the primary unit waits between sending routing table updates to subordinate units in a cluster.

The route hold range is 0 to 3600 seconds. The default route hold time is 10 seconds.

To avoid flooding routing table updates to subordinate units, set `route-hold` to a relatively long time to prevent subsequent updates from occurring too quickly.

The `route-hold` time should be coordinated with the `route-wait` time. See the `route-wait` description for more information.

**route-ttl <ttl_integer>**

The time to live for routes in a cluster unit routing table.

The time to live range is 0 to 3600 seconds. The default time to live is 0 seconds.
The time to live controls how long routes remain active in a cluster unit routing table after the cluster unit becomes a primary unit. To maintain communication sessions after a cluster unit becomes a primary unit, routes remain active in the routing table for the route time to live while the new primary unit acquires new routes.

Normally, the route-ttl is 0 and the primary unit must acquire new routes before it can continue processing traffic. Normally acquiring new routes occurs very quickly so only a minor delay is caused by acquiring new routes.

If the primary unit needs to acquire a very large number of routes, or if for other reasons, there is a delay in acquiring all routes, the primary unit may not be able to maintain all communication sessions. You can increase the route time to live if communication sessions are lost after a failover so that the primary unit can use routes that are already in the routing table, instead of waiting to acquire new routes.

\[ \text{route-wait <wait_integer>} \]

The time the primary unit waits after receiving routing table update before sending the update to the subordinate units in the cluster.

For quick routing table updates to occur, set route-wait to a relatively short time so that the primary unit does not hold routing table changes for too long before updating the subordinate units.

The route-wait range is 0 to 3600 seconds. The default route-wait is 0 seconds.

Normally, because the route-wait time is 0 seconds the primary unit sends routing table updates to the subordinate units every time the primary unit routing table changes.

Once a routing table update is sent, the primary unit waits the route-hold time before sending the next update.

Usually routing table updates are periodic and sporadic. Subordinate units should receive these changes as soon as possible so route-wait is set to 0 seconds. route-hold can be set to a relatively long time because normally the next route update would not occur for a while.

In some cases, routing table updates can occur in bursts. A large burst of routing table updates can occur if a router or a link on a network fails or changes. When a burst of routing table updates occurs, there is a potential that the primary unit could flood the subordinate units with routing table updates. Setting route-wait to a longer time reduces the frequency with which additional routing updates are sent, which prevents flooding of routing table updates from occurring.

**Modifying heartbeat timing**

In an HA cluster, if a cluster unit CPU becomes very busy, the cluster unit may not be able to send heartbeat packets on time. If heartbeat packets are not sent on time other units in the cluster may think that the cluster unit has failed and the cluster will experience a failover.

A cluster unit CPU may become very busy if the cluster is subject to a syn flood attack, if network traffic is very heavy, or for other similar reasons.

You can use the following CLI commands to configure how the cluster times HA heartbeat packets:
Command syntax

```plaintext
config system ha
  set hb-lost-threshold <threshold_integer>
  set helo-holddown <holddown_integer>
  set hb-interval <interval_integer>
end
```

**hb-lost-threshold <threshold_integer>**

The lost heartbeat threshold is the number of seconds to wait to receive a heartbeat packet from another cluster unit before assuming that the cluster unit has failed. The lost heartbeat threshold range is 1 to 60 seconds. The default lost heartbeat threshold range is 6 seconds.

If the primary unit does not receive a heartbeat packet from a subordinate unit before the heartbeat threshold expires, the primary unit assumes that the subordinate unit has failed.

If a subordinate unit does not receive a heartbeat packet from the primary unit before the heartbeat threshold expires, the subordinate unit assumes that the primary unit has failed. The subordinate unit then begins negotiating to become the new primary unit.

The lower the lost heartbeat interval the faster the cluster responds to a failure. However, you can increase the heartbeat lost threshold if repeated failovers occur because cluster units cannot sent heartbeat packets quickly enough.

**helo-holddown <holddown_integer>**

The hello state hold-down time is the number of seconds that a cluster unit waits before changing from hello state to work state. A cluster unit changes from hello state to work state when it starts up.

The hello state hold-down time range is 5 to 300 seconds. The hello state hold-down time default is 20 seconds.

**hb-interval <interval_integer>**

The heartbeat interval is the time between sending heartbeat packets. The heartbeat interval range is 1 to 20 (100*ms). The heartbeat interval default is 2 (200 ms).

A heartbeat interval of 2 means the time between heartbeat packets is 200 ms. Changing the heartbeat interval to 5 changes the time between heartbeat packets to 500 ms.

The HA heartbeat packets consume more bandwidth if the `hb-interval` is short. But if the `hb-interval` is very long, the cluster is not as sensitive to topology and other network changes.

**Enabling or disabling HA heartbeat encryption and authentication**

You can enable or disable HA heartbeat encryption and authentication to encrypt and authenticate HA heartbeat packets. HA heartbeat packets should be encrypted and authenticated if the cluster interfaces that send HA heartbeat packets are also connected to your networks. If ha heartbeat packets are not encrypted the cluster password will be exposed. If ha heartbeat packets are not authenticated an attacker may be able to sniff HA pages to get cluster information.
Enabling HA encryption and authentication could reduce cluster performance.

**Command syntax**

```plaintext
config system ha
  set authentication {disable | enable}
  set encryption {disable | enable}
end
```

**authentication {disable | enable}**

Enable/disable HA heartbeat message authentication. Enabling HA heartbeat message authentication prevents an attacker from creating false HA heartbeat messages. False HA heartbeat messages could affect the stability of the cluster.

Authentication is disabled by default.

**encryption {disable | enable}**

Enable/disable HA heartbeat message encryption. Enabling HA heartbeat message encryption prevents an attacker from sniffing HA packets to get HA cluster information.

Encryption is disabled by default.

### Setting the number of gratuitous arps sent by a primary unit

You can use the following command to set the number of gratuitous arp packets that are sent by a primary unit. Gratuitous arp packets are sent when a cluster unit becomes a primary unit to notify attached network devices to send packets to the primary unit.

**Command syntax**

```plaintext
config system ha
  set arps <arp_integer>
end
```

**arps <arp_integer>**

Set the number of gratuitous ARP packets sent by the primary unit. Gratuitous ARP packets are sent when a cluster unit becomes a primary unit. The gratuitous ARP packets configure connected networks to associate the cluster virtual MAC address with the cluster IP address. The range is 1 to 16 gratuitous ARP packets.

### Managing a FortiGate virtual clustering configuration

Managing a FortiGate virtual clustering configuration is very similar to managing a cluster that does not contain virtual domains. Most of the information in this chapter also applies to managing a virtual clustering configuration. This managing a virtual clustering configuration describes what is different when managing a virtual cluster.
If virtual domains are enabled, the cluster web-based manager dashboard displays the cluster name and the role of each cluster unit in virtual cluster 1 and virtual cluster 2.

Figure 55: Example virtual clustering web-based manager dashboard

The configuration and maintenance options that you have when you connect to a virtual cluster web-based manager or CLI depend on the virtual domain that you connect to and the administrator account that you use to connect.

If you connect to a cluster as the administrator of a virtual domain, you connect directly to the virtual domain. Since HA virtual clustering is a global configuration, virtual domain administrators cannot see HA configuration options. However, virtual domain administrators see the host name of the cluster unit that they are connecting to on the web browser title bar or CLI prompt. This host name is the host name of the primary unit for the virtual domain. Also, when viewing log messages by going to Log & Report > Log Access virtual domain administrator can select to view log messages for either of the cluster units.

Figure 56: Viewing log messages from a virtual domain in a virtual cluster

If you connect to a cluster as the administrator to the Virtual Domain Configuration web-based manager page or to the global CLI. Even so you are connecting to an interface and to the virtual domain that the interface has been added to. The virtual domain that you connect to does not make a difference for most configuration and maintenance operations. However, there are a few exceptions. You connect to the FortiGate unit that functions as the primary unit for the virtual domain. So the host name displayed on the web browser title bar and on the CLI is the host name of this primary unit.

- Virtual cluster members list overview
- Changing the HA configuration of an operating virtual cluster

Virtual cluster members list overview

If virtual domains are enabled, you can display the cluster members list to view the status of the operating virtual clusters. The virtual cluster members list shows the status of both virtual clusters including the virtual domains added to each virtual cluster.

To display the virtual cluster members list for an operating cluster log in as the admin administrator, select Global Configuration and go to System > Config > HA.
The fields and functions of the virtual cluster members list are the same as the fields and functions described in “Cluster members list overview” on page 139 with the following exceptions.

- When you select the edit icon for a primary unit in a virtual cluster, you can change the virtual cluster 1 and virtual cluster 2 device priority of this cluster unit and you can edit the VDOM partitioning configuration of the cluster.
- When you select the edit icon for a subordinate unit in a virtual cluster, you can change the device priority for the subordinate unit for the selected virtual cluster.

Also, the HA cluster members list changes depending on the cluster unit. For the virtual cluster described in the “Virtual clustering load balancing configuration” on page 123 if you connect to port 5 you are connecting to FortiGate_A (FortiGate_A is displayed on the web browser title bar). Select Global Configuration and go to System > Config > HA. From either cluster members list you can select edit for FortiGate_A to change the HA configuration for the virtual cluster and to set device priorities for FortiGate_A in virtual cluster 1 and virtual cluster 2. If you select edit for FortiGate_B in virtual cluster 1 you can change the host name of FortiGate_B and change the device priority of FortiGate_B in virtual cluster 1. If you select edit for FortiGate_B in virtual cluster 2 you can change the host name of FortiGate_B and change the device priority of FortiGate_B in virtual cluster 2.
If you connect to port 7 you are connecting to FortiGate_B (FortiGate_B is displayed on the web browser title bar). Select Global Configuration and go to System > Config > HA. From either cluster members list you can select edit for FortiGate_B to change the HA configuration for the virtual cluster and to set device priorities for FortiGate_B in virtual cluster 1 and virtual cluster 2. If you select edit for FortiGate_A in virtual cluster 1 you can change the host name of FortiGate_A and change the device priority of FortiGate_A in virtual cluster 1. If you select edit for FortiGate_A in virtual cluster 2 you can change the host name of FortiGate_A and change the device priority of FortiGate_A in virtual cluster 2.
Changing the HA configuration of an operating virtual cluster

To change the configuration settings of the primary unit in a functioning cluster with virtual domains enabled, log in as the admin administrator, select Global Configuration and go to System > Config > HA to display the cluster members list. Select Edit for the master (or primary) unit in virtual cluster 1 or virtual cluster 2 to display the HA configuration page for the virtual cluster.

You can use the virtual cluster HA configuration page to check and fine tune the configuration of both virtual clusters after the cluster is up and running. For example, you may want to change the Port Monitor configuration for virtual cluster 1 and virtual cluster 2 so that each virtual cluster monitors its own interfaces.

You can also use this configuration page to move virtual domains between virtual cluster 1 and virtual cluster 2. Usually you would distribute virtual domains between the two virtual clusters to balance the amount of traffic being processed by each virtual cluster.

Any changes you make on this page, with the exception of changes to the device priorities, are first made to the primary unit configuration and then synchronized to the subordinate unit.

You can also adjust device priorities to configure the role of this cluster unit in the virtual cluster. For example, to distribute traffic to both cluster units in the virtual cluster configuration, you would want one cluster unit to be the primary unit for virtual cluster 1 and the other cluster unit to be the primary unit for virtual cluster 2. You can create this configuration by setting the device priorities. The cluster unit with the highest device priority in virtual cluster 1 becomes the primary unit for virtual cluster 1. The cluster unit with the highest device priority in virtual cluster 2 becomes the primary unit in virtual cluster 2.
Figure 60: FortiGate-5001SX HA virtual cluster configuration
Index

Numerics
802.3ad aggregate interface
  full mesh HA 129
  HA MAC addresses 47
  HA port monitoring 47

A
active sessions
  HA statistics 141
Active-Active
  HA mode 52
Active-Passive
  HA mode 52
admin log messages 153
age
  primary unit selection 27
alert email
  HA 145
all
  execute ha synchronize 76
arp table 62
arp 160
  gratuitous 160
  system ha 59
attached network equipment
  failover 36
attackdef
  execute ha synchronize 76
authentication
  heartbeat 159
  system ha 59
authentication (disable | enable) 160
avupd
  execute ha synchronize 76

B
back to HA monitor
  HA statistics 141
backup unit
  HA 9

C
csa
  execute ha synchronize 76
cluster 58
  configuring in NAT/Route mode 81
  configuring in transparent mode 89
  definition 17
  large number of units 99
  operating 137
  virtual 58
  virtual cluster 115
cluster member 139
  cluster members list 139
  priority 140
  role 140
cluster name 53
cluster unit
  connect to a cluster 146
  definition 17
  disconnect from a cluster 146
comments, documentation 21
config
  system ha synchronize 76
configuration
  synchronization 36
connected monitored interfaces
  primary unit selection 27
connecting a FortiGate HA cluster 79
connecting a virtual cluster 119
console messages
  synchronization fails 39
CPU usage
  HA statistics 141
customer service 21

D
default heartbeat device configuration
  HA 56
device
  failover 34, 35
  device failover
    definition 17
device priority
  changing 16
  HA 52
  primary unit selection 28
  subordinate unit 57, 142
DHCP
  HA 40
disconnecting a unit from a cluster
  override 30
documentation
  commenting on 21
  Fortinet 21

E
eemailists
  execute ha synchronize 76
enable session pickup
  HA 53
enabling virtual domain configuration 120
encryption
  heartbeat 159
  system ha 59
Index

encryption {disable | enable} 160

F
failover 52
  and attached network equipment 36
definition 17
device 34, 35
HA 10
heartbeat 18
link 18, 34, 35
monitoring cluster units 145
failover protection 115
  virtual clustering 115
failure
  definition 17
  multiple link failures 36
FDN 146
FGCP
definition 18
FGT\_ha\_admin
  HA administrator account 24, 146
firmware upgrade
  HA 40, 143
FortiGate documentation
  commenting on 21
FortiGate unit serial number
  primary unit selection 28
FortiGate-5020
  chassis 99
FortiGuard 148
FortiGuard Antispam 148
FortiGuard Antivirus 148
FortiGuard Distribution Network 148
FortiGuard Intrusion Protection 148
FortiGuard Web Filtering 148
FortiLog 150
Fortinet customer service 21
Fortinet documentation 21
Fortinet Knowledge Center 21
forwarding
  MAC forwarding table 62
full mesh
  HA 10, 13, 127
  redundant HA heartbeat interfaces 129
full mesh HA 128
  and virtual clustering 134
  configuration example 130
definition 18

G
gratuitous arps 160
group ID
  virtual MAC address 31
group name
  HA 53
  HA cluster name 53
group-id
  system ha 59
group-name
  system ha 59

H
HA 58, 119, 120, 139
  Active-Active mode 52
  active-active mode and redundant interfaces 46
  Active-Passive mode 52
  active-passive mode and LACP 47
  active-passive mode and redundant interfaces 46
  add a new unit to a functioning cluster 144
  adding redundant interfaces to a cluster 132
  adding virtual domains 121
  alert email 145
  and LACP 47
  backup unit 9
  changing firmware upgrade 41, 143
  changing the device priority 16
  cluster member 139
  cluster members list 139
  cluster units 9
  configuration 51
  configuration synchronization 138
  configure a FortiGate unit for HA operation 78
  configuring virtual clustering 118
  connect a cluster unit 146
  connect a FortiGate HA cluster 79
default heartbeat device configuration 56
device priority 52
DHCP 40
disconnect a cluster unit 146
enable session pickup 53
enable virtual clustering 121
enabling virtual domain configuration 120
event log message 42, 144
failover 10, 52
FGT\_ha\_admin administrator account 24, 146
firmware upgrade 40, 143
full mesh 10, 13, 127, 128
full mesh and 802.3ad aggregate interfaces 129
full mesh and redundant heartbeat interfaces 129
full mesh HA and virtual clustering 134
full mesh HA configuration example 130
group name 53
heartbeat interface 54
heartbeat interface IP addresses 56
host name 42, 144
host name 140
interface monitoring and aggregate interfaces 47
interface monitoring and redundant interfaces 45
L2TP 40
link failover and aggregate interfaces 47
link failover and redundant interfaces 45
load balancing 10, 52
log message 42, 144
MAC addresses and aggregate interfaces 47
MAC addresses and redundant interfaces 45
manage individual cluster units 146
manage logs for individual cluster units 41, 144
master unit 9
mode 52
monitor cluster units for a failover 145
password 53
port monitor 54
port monitoring and aggregate interfaces 47
port monitoring and redundant interfaces 45
PPP 40
INDEX

PPPoE 40
PPTP 40
primary unit 9
redundant interface 10, 13, 127
session pickup 53
slave unit 9
Standalone mode 52
standby state 42, 144
states 42, 144
subordinate unit 9
subordinate unit device priority 57, 142
subordinate unit host name 57, 142
synchronization 138
VDOM partitioning 57
viewing HA statistics 140
virtual cluster 115
virtual clustering 10
virtual domains 115
work state 42, 144

ha
arps 59
authentication 59
encryption 59
group-id 59
group-name 59
hbdev 61
hb-interval 60
hb-lost-threshold 60
helolholdown 61
link-failed-signal 62
load-balance-all 62
mode 62
monitor 62
override 63
password 63
priority 63
route-hold 63
route-ttl 64
route-wait 64
schedule 65
secondary-vcluster 67
session-pickup 65
sync-config 66
uninterruptable-upgrade 66
vcluster2 67
vdom 66
weight 66
HA group name 53
HA heartbeat
definition 18
HA statistics
active sessions 141
back to HA monitor 141
CPU usage 141
intrusion detected 141
memory usage 141
monitor 141
network utilization 141
refresh every 141
serial no 141
status 141
total bytes 141
total packets 141
up time 141
virus detected 141
HA virtual MAC address
definition 18
ha_daemon
HA user interface 37
hbdev
system ha 61
hb-interval 159
system ha 60
hb-lost-threshold 159
system ha 60
heartbeat
authentication 159
definition 18
encryption 159
hello state hold-down time 159
interval 159
lost heartbeat threshold 159
modifying heartbeat timing 158
heartbeat device
definition 18
heartbeat failover
definition 18
heartbeat interface 24
virtual clustering 115
heartbeat interfaces 115
heartbeat, HA
interface 54
interface IP addresses 56
hello state
definition 18
hello state hold-down time 159
helolholdown 159
system ha 61
high availability 58
definition 18
hostname
cluster members list 140

I
incremental
synchronization 36
interface
heartbeat 24
introduction
Fortinet documentation 21
intrusion detected
HA statistics 141
IP address
heartbeat interface 56

K
keyword 26

L
L2TP
HA 40
LACP
and HA 47
lacp-ha-slave
<table>
<thead>
<tr>
<th>CLI keyword</th>
<th>large number of units to a cluster 99</th>
</tr>
</thead>
<tbody>
<tr>
<td>link</td>
<td>large number of units to a cluster 99</td>
</tr>
<tr>
<td>link failover</td>
<td>34, 35</td>
</tr>
<tr>
<td>link-failed-signal</td>
<td>system ha 62</td>
</tr>
<tr>
<td>load balancing</td>
<td>definition 19</td>
</tr>
<tr>
<td>load-balance-all</td>
<td>system ha 62</td>
</tr>
<tr>
<td>log messages</td>
<td>admin 153</td>
</tr>
<tr>
<td>log messages</td>
<td>example log message scenarios 154</td>
</tr>
<tr>
<td>log messages</td>
<td>HA 151</td>
</tr>
<tr>
<td>log messages</td>
<td>primary unit added back to cluster 154</td>
</tr>
<tr>
<td>log messages</td>
<td>primary unit removed from cluster 154</td>
</tr>
<tr>
<td>logs</td>
<td>admin log messages 153</td>
</tr>
<tr>
<td>logs</td>
<td>example log message scenarios 154</td>
</tr>
<tr>
<td>logs</td>
<td>HA log messages 151</td>
</tr>
<tr>
<td>net</td>
<td>HA 63</td>
</tr>
<tr>
<td>lost heartbeat threshold</td>
<td>159</td>
</tr>
</tbody>
</table>

| MAC          | MAC forwarding table 62                |
| MAC address  | virtual 31                              |
| manage cluster units | primary cluster unit 19 |
| master unit  | HA 9                                    |
| memory usage | HA statistics 141                       |
| MIB           | HA 155                                  |
| Mode          | HA 52                                   |
| mode          | config system ha 62                     |
| monitor       | HA statistics 141                       |
| monitored interface | HA statistics 141 |
| quarantine    | 156                                     |
| primary unit selection | 27                                     |
| PPP           | HA 40                                   |
| PPPoE         | HA 40                                   |
| PPTP          | HA 40                                   |
| PPTP          | HA 40                                   |
| primary cluster unit | definition 19 |
| PPP           | HA 40                                   |
| PPPoE         | HA 40                                   |
| PPTP          | HA 40                                   |
| primary unit selection | 27                                     |
| PPP           | HA 40                                   |
| PPPoE         | HA 40                                   |
| PPTP          | HA 40                                   |
| primary unit selection | 27                                     |
| PPP           | HA 40                                   |
| PPPoE         | HA 40                                   |
| PPTP          | HA 40                                   |
| quarantine    | 156                                     |
| viewing and managing quarantined files for an HA cluster 156 |
R

RADIUS 148
redundant interface
  adding to a cluster 132
  HA active-active mode 46
  HA active-passive mode 46
  HA MAC addresses 45
  HA port monitoring 45
refresh every
  HA statistics 141
role
  cluster members 140
route hold 157
route-hold 157
  system ha 63
route-ttl 157
  system ha 64
route-wait 158
  system ha 64
routing table updates
  synchronizing 157

S

schedule
  system ha 65
secondary-vcluster
  system ha 67
selecting the primary unit 25
serial no
  HA statistics 141
serial number
  primary unit selection 28
session pick-up
  definition 19
session pickup
  HA 53
session-pickup
  system ha 65
slave unit
  HA 9
SNMP 155
  MIB 155
  trap 155
Standalone mode
  HA 52
standby state
  definition 19
  HA 42, 144
start
  execute ha synchronize 76
state
  hello 18
  standby 19
  work 20
state synchronization
  definition 20
statistics
  viewing HA statistics 140
status
  HA statistics 141

T

table
  arp 62
  MAC forwarding table 62
technical support 21
  time to live for routes 157
timing
  modifying heartbeat timing 158
total bytes
  HA statistics 141
total packets
  HA statistics 141
Transparent mode 89
  CLI configuration steps 85, 93
  configuring an active-active HA cluster 89
  general configuration steps 89
  web-based manager configuration steps 89
trap
  SNMP 155

U

uninterruptable-upgrade
  system ha 66
up time
  HA statistics 141

V

vcluster2
  system ha 67
vdom
  system ha 66
VDOM partitioning
  HA 57
virtual cluster 115
  and virtual domains 115
  configuring 118
  connecting to a network 119
  enable 121
  enabling virtual domain configuration 120
  HA 10
virtual clustering 58
  adding virtual domains 121
definition 20
enabling virtual domain configuration 120
full mesh HA 134
virtual domain
  adding to a cluster 121
  enabling for HA 120
  enabling virtual domain configuration for HA 120
virtual MAC address 31
  conflict 33
  definition 18
  group ID 31
  how its determined 32
virus detected
  HA statistics 141

W
  web-based manager configuration steps 89
  NAT/Route mode 82
  weblists
    execute ha synchronize 76
  WebTrends server 150
  weight
    system ha 66
  work state
    definition 20
    HA 42, 144