



# FortiGate High Availability

## Guide

<i>FortiGate High Availability Guide</i>	
<b>Document Version:</b>	5
<b>Publication Date:</b>	March 10, 2005
<b>Description:</b>	This document describes FortiGate FortiOS v2.80 High Availability. This document continues to be a work in progress. You are encouraged to forward your comments and suggestions for improvements about this document to <a href="mailto:techdoc@fortinet.com">techdoc@fortinet.com</a> .
<b>Product:</b>	FortiOS v2.80 MR8
<b>Document Number:</b>	01-28008-0112-20050310

**Fortinet Inc.**

© Copyright 2005 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

*FortiGate High Availability Guide*

FortiOS v2.80

March 7, 2005

01-28008-0112-20050310

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

For technical support, please visit <http://www.fortinet.com>.

Send information about errors or omissions in this document or any Fortinet technical documentation to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

Version	Date	Description of changes
5th Release	March 7, 2005	First non-draft version. Extensively re-written to include FortiOS v2.80 content.
	March 10, 2005	The first paragraph in the section " <a href="#">HA operating modes</a> " on page 22 confused the features of active-active and active-passive HA modes. The paragraph has been corrected to state the following "Active-passive HA provides failover protection. Active-active HA provides load balancing as well as failover protection."

# Table of Contents

<b>Introduction .....</b>	<b>7</b>
This document .....	8
New v2.80 HA features .....	9
Multiple heartbeat devices .....	9
Primary unit selection.....	9
Link failover.....	9
Synchronizing the cluster configuration .....	10
Preventing configuration changes on subordinate units .....	10
Controlling how HA synchronizes routing table changes.....	10
Modifying HA heartbeat timing.....	10
Enabling and disabling HA heartbeat encryption .....	10
FortiGate HA terminology .....	10
FortiGate documentation .....	13
Comments on Fortinet technical documentation.....	14
Customer service and technical support.....	14
<b>FortiGate Clustering Protocol (FGCP) .....</b>	<b>15</b>
FGCP heartbeat.....	15
HA heartbeat Telnet sessions.....	16
Heartbeat devices.....	16
Heartbeat device IP addresses.....	18
Primary unit selection.....	18
Cluster virtual MAC address .....	20
Subordinate unit priority .....	20
Controlling primary unit selection.....	21
Using override master to control primary unit selection .....	22
HA operating modes .....	22
Active-passive HA (failover).....	22
Active-active HA (load balancing and failover) .....	23
Device failover and link failover .....	23
Device failover .....	23
Link failover.....	24

**Configuration reference ..... 25**

- Web-based manager HA configuration settings ..... 25
  - Standalone Mode ..... 26
  - Cluster Members ..... 26
  - High Availability ..... 26
  - Mode ..... 26
  - Group ID ..... 27
  - Unit Priority ..... 27
  - Override Master ..... 28
  - Password ..... 28
  - Schedule ..... 28
  - Priorities of Heartbeat Device ..... 29
  - Monitor priorities ..... 32
- config system ha ..... 32
- execute ha manage ..... 41
- execute ha synchronize ..... 42

**FortiGate HA installation and configuration examples ..... 43**

- Basic NAT/Route mode installation ..... 43
  - Example NAT/Route mode HA network topology ..... 44
  - General configuration steps ..... 45
  - Web-based manager configuration steps ..... 45
  - CLI configuration steps ..... 48
- Basic Transparent mode installation ..... 51
  - Example Transparent mode HA network topology ..... 51
  - General configuration steps ..... 52
  - Web-based manager configuration steps ..... 53
  - CLI configuration steps ..... 55
- Converting a standalone FortiGate unit to a cluster ..... 57
- Adding a new unit to an operating cluster ..... 59
  - Adding a large number of units to a cluster ..... 61
- Customizing primary unit selection ..... 61
  - Network topology ..... 62
  - General configuration steps ..... 62
  - Web-based manager configuration steps ..... 64
  - CLI configuration steps ..... 69
  - Testing failover ..... 73
- Configuring monitor priorities for link failover protection ..... 76
  - Web-based manager configuration steps ..... 77
  - CLI configuration steps ..... 78
  - Testing failover ..... 79

## Operating a cluster ..... 83

Operating a cluster.....	83
Cluster web-based manager.....	84
Cluster CLI.....	85
Cluster front panel and LCD .....	85
Viewing the status of cluster units.....	85
Upgrading cluster firmware .....	87
Changing the cluster operating mode .....	87
Changing HA configuration options .....	88
Managing subordinate units.....	88
FGCP compatibility with PPP protocols .....	89
Cluster communication with the FortiProtect Distribution Network .....	89
Clusters and FortiGuard/FortiShield .....	89
Cluster communication with RADIUS and LDAP servers .....	90
Synchronizing the cluster configuration .....	90
Clusters and logging .....	92
Viewing and managing logs for an HA cluster .....	92
HA log messages.....	93
Admin log messages.....	95
Example log message scenarios .....	95
Clusters and SNMP .....	97
Clusters and quarantine.....	98
Viewing and managing quarantined files for an HA cluster .....	98
Advanced HA configuration options.....	99
Controlling how HA synchronizes routing table updates.....	99
Modifying heartbeat timing.....	101
Enabling or disabling HA heartbeat encryption and authentication .....	102
Setting the number of gratuitous arps sent by a primary unit .....	103

## Failover protection..... 105

Active-passive failover .....	105
Failover exceptions .....	106
Active-active failover .....	107
Device failover .....	107
Link failover.....	108
How link failover maintains traffic flow .....	109
Multiple link failures.....	111
Example link failover scenarios.....	111
NAT/Route mode active-passive cluster packet flow .....	112
Packet flow from client to web server .....	113
Packet flow from web server to client .....	114
When a device failover occurs .....	114

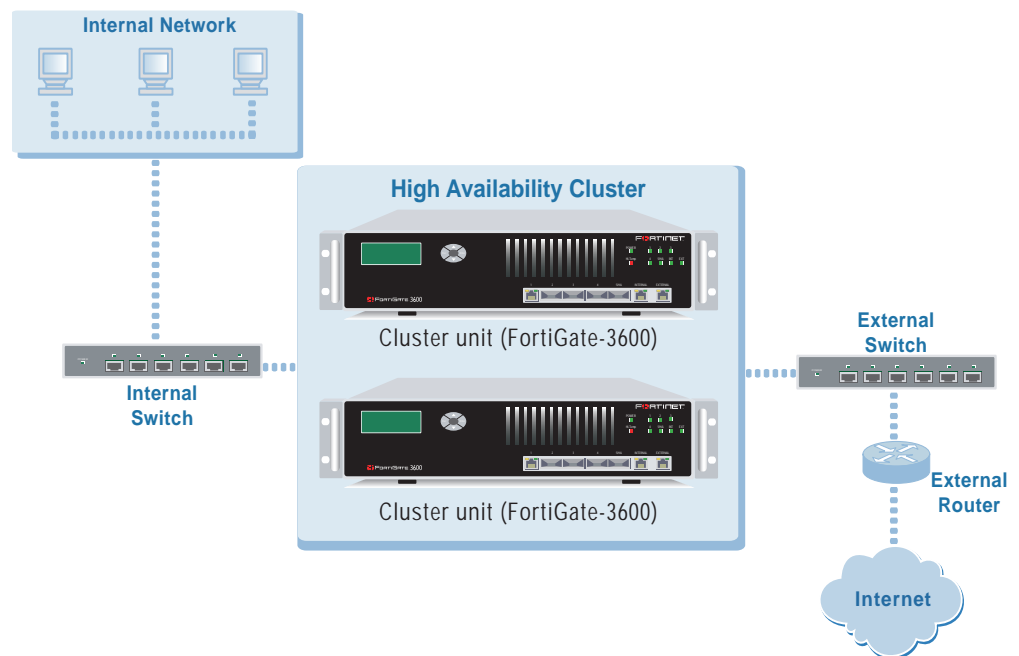
Transparent mode active-passive cluster packet flow .....	114
Packet flow from client to mail server .....	115
Packet flow from mail server to client .....	116
When a device failover occurs .....	116
Monitoring cluster units for failover .....	117
Monitoring for device failure .....	117
Failover performance .....	118
Device failover performance .....	118
Link failover performance.....	118
Failover performance test results.....	118
<b>Active-active load balancing.....</b>	<b>121</b>
Load balancing overview .....	121
Load balancing schedules .....	121
Selecting which packets are load balanced .....	122
More about active-active failover .....	123
Configuring load balancing settings .....	123
Selecting a load balancing schedule.....	123
Load balancing virus scanning sessions and TCP sessions .....	124
Configuring weighted-round-robin weights .....	124
NAT/Route mode active-active cluster packet flow.....	125
Packet flow from client to web server .....	126
Packet flow from web server to client .....	127
When a failover occurs .....	127
Transparent mode active-active cluster packet flow .....	128
Packet flow from client to mail server .....	128
Packet flow from mail server to client .....	129
When a failover occurs .....	130
<b>HA with third-party products .....</b>	<b>131</b>
Troubleshooting layer-2 switches .....	131
Layer-2 switch restrictions .....	132
Configuring layer-2 switch MAC address tables .....	133
Failover issues with layer-3 switches.....	133
Changing spanning tree protocol settings for some switches.....	134
Spanning Tree protocol (STP) .....	134
Bridge Protocol Data Unit (BPDU) .....	134
Failover and attached network equipment.....	135
<b>Index .....</b>	<b>137</b>

# Introduction

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

FortiGate HA consists of two or more FortiGate units operating 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 firewall, VPN, IPS, virus scanning, web filtering, and spam filtering services.

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



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. The cluster continues to process network traffic and provide normal FortiGate services with virtually no interruption.

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 firewall 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.

## This document

This *FortiGate High Availability Guide* contains the following chapters:

- [Introduction](#) briefly introduces HA, describes new v2.80 HA features, and defines the HA-related terminology.
- [FortiGate Clustering Protocol \(FGCP\)](#) describes the FGCP clustering protocol, including the HA heartbeat, primary unit selection, device and link failover, and introduces the active-passive and active-active HA modes.
- [FortiGate HA installation and configuration examples](#) contains detailed HA installation and configuration examples.
- [Operating a cluster](#) contains information you need to know to be able to operate a cluster. This chapter includes information about how to upgrade cluster firmware, how to synchronize the cluster configuration, how to monitoring cluster performance, and how logging, SNMP, and the quarantine function works with a cluster. This chapter also describes some advanced HA settings.
- [Failover protection](#) describes how HA active-passive failover protection works, provides detailed NAT/Route and Transparent mode active-passive packet flow descriptions, includes a summary of active-active failover protection, and provides information about device failover and link failover.
- [Active-active load balancing](#) describes how HA active-active load balancing works and provides active-active packet flow examples for NAT/Route and Transparent mode HA.
- [HA with third-party products](#) provides information about operating FortiGate clusters with third party products such as layer-2 and layer-3 switches.
- [Configuration reference](#) describes all HA-related web-based manager and command line interface (CLI) configuration settings.

## New v2.80 HA features

The following new or changed HA features are available in FortOS v2.80:

- [Multiple heartbeat devices](#)
- [Primary unit selection](#)
- [Link failover](#)
- [Synchronizing the cluster configuration](#)
- [Preventing configuration changes on subordinate units](#)
- [Controlling how HA synchronizes routing table changes](#)
- [Modifying HA heartbeat timing](#)
- [Enabling and disabling HA heartbeat encryption](#)

### Multiple heartbeat devices

By default, two cluster interfaces are configured to be heartbeat devices. The active heartbeat device has a priority of 100. A second, or backup heartbeat device has a priority of 50.

You can configure multiple cluster interfaces to be heartbeat devices. If the active heartbeat device fails or becomes disconnected, HA heartbeat traffic fails over to the heartbeat device with the next highest priority.

### Primary unit selection

More options are available for controlling primary unit selection:

- Monitor Priority
- Age
- Unit priority
- Serial number

For more information about these options and about primary unit selection, see [“Primary unit selection” on page 18](#).

### Link failover

If a link failure causes an interface on the primary unit to stop processing network traffic from a specific network, 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.

If a high priority link on a subordinate unit fails, this cluster unit will be less likely to become the primary unit if the primary unit fails.

Link failover keeps traffic flowing on the most important networks at the sacrifice of the traffic on less important networks.

For more information about link failover, see [“Link failover” on page 108](#).

## Synchronizing the cluster configuration

The process for synchronizing the cluster configuration has been improved for FortOS v2.80. The primary unit sends configuration changes to the subordinate units. Each subordinate unit then compares its configuration with the primary unit configuration. If a difference is found, the subordinate attempts to re-synchronize its configuration.

For information and how synchronizing the cluster configuration functions, see [“Synchronizing the cluster configuration” on page 90](#).

## Preventing configuration changes on subordinate units

If you connect to the cluster command line interface (CLI) you can use the `execute ha manage` command to connect to the CLI of any subordinate unit. From the subordinate unit you can change the FortiGate unit host name, the HA unit priority, and the override master setting. The CLI prevents you from making any other configuration changes. The connection between the primary unit and the subordinate unit uses the telnet port (TCP port 23).

## Controlling how HA synchronizes routing table changes

You can control how HA routing table updates are propagated to all cluster units. In some configurations, routing table updates may take a while to complete or may cause performance issues. By changing HA routing table update timers you can minimize these issues. For information, see [“Controlling how HA synchronizes routing table updates” on page 99](#).

## Modifying HA heartbeat timing

HA heartbeat timing can be fine tuned to deal with timing and other issues that can result in failovers occurring without a failure having occurred. For information, see [“Modifying heartbeat timing” on page 101](#).

## Enabling and disabling HA heartbeat encryption

You can enable or disable HA heartbeat encryption to encrypt the cluster password that is sent in HA heartbeat packets. HA heartbeat packets should be encrypted if the cluster interfaces that send HA heartbeat packets are also connected to your networks. If these packets are not encrypted the cluster password will be exposed. For more information, see [“Enabling or disabling HA heartbeat encryption and authentication” on page 102](#).

## 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 sessions<sup>1</sup> 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.

## FGCP

The FortiGate clustering protocol (FGCP) that specifies how the FortiGate units in a cluster communicate to keep the cluster operating.

## 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. See [“Group ID” on page 27](#) for more information about the HA virtual MAC address and its relationship with 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.

---

1. HA does not provide session failover for PPPoE, DHCP, PPTP, and L2TP services.

## 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. For more details, see [“Active-active load balancing” on page 121](#).

## Monitored interface

An interface that is configured with a monitor priority. 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. For more information see [“Link failover” on page 108](#).

## 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 re-directs 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.

## 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.

## State synchronization

The part of the FGCP that maintains connections after failover.

## FortiGate documentation

For information about FortiGate HA configuration parameters, see your FortiGate unit online help or the latest [FortiGate Administration Guide](#) and [FortiGate CLI Reference](#), both available from the [Fortinet Knowledge Center](#).

Up to date articles about FortiGate HA are also available from the Fortinet Knowledge Center [FortiOS v2.80 High Availability \(HA\)](#) page.

The most current version of this FortiGate High Availability Guide is also available from the Fortinet Knowledge Center [FortiOS v2.80 HA Guide](#) page.

Information about FortiGate products is available from the following guides:

- [FortiGate QuickStart Guides](#)  
Provide basic information about connecting and installing a FortiGate unit.
- [FortiGate Installation Guides](#)  
Describe how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- [FortiGate Administration Guides](#)  
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- [FortiGate online help](#)  
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

- [FortiGate CLI Reference Guide](#)  
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- [FortiGate Log Message Reference Guide](#)  
Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.

## 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](mailto:techdoc@fortinet.com).

## Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet Technical Support web site at <http://support.fortinet.com>.

You can also register Fortinet products and service contracts from <http://support.fortinet.com> and change your registration information at any time.

Technical support is available through email from any of the following addresses. Choose the email address for your region:

- |                                  |   |
|----------------------------------|---|
| <b>amer_support@fortinet.com</b> | For customers in the United States, Canada, Mexico, Latin America and South America.                            |
| <b>apac_support@fortinet.com</b> | For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia. |
| <b>eu_support@fortinet.com</b>   | For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.                 |

For information about our priority support hotline (live support), see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- your name
- your company's name and location
- your email address
- your telephone number
- your support contract number (if applicable)
- the product name and model number
- the product serial number (if applicable)
- the software or firmware version number
- a detailed description of the problem

# 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 v2.80 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. To form a cluster, the FGCP protocol selects one FortiGate unit to be the primary unit. The remaining cluster units become subordinate units. The primary unit controls cluster operation and represents the cluster presence on the network.

During cluster operation, the FGCP shares communication session, link status, and configuration information among cluster units. The cluster uses the FGCP 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 describes the basics of the role that the FGCP plays in FortiGate cluster operations. This chapter contains the following sections:

- [FGCP heartbeat](#)
- [Heartbeat devices](#)
- [Primary unit selection](#)
- [HA operating modes](#)
- [Device failover and link failover](#)

## FGCP heartbeat

Central to the FGCP is communication between FortiGate units to identify cluster units and to share information between cluster units. The FGCP communication protocol is called the FGCP heartbeat or the HA heartbeat. Often, this is shortened to just heartbeat.

The FGCP heartbeat keeps cluster units communicating with each other. The heartbeat consists of hello packets that are sent at regular intervals by 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.

On startup, a FortiGate unit configured for HA operation broadcasts FGCP heartbeat hello packets 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 group ID, and HA password). If the HA configurations match, the units negotiate to create a cluster.

The FGCP heartbeat operates on TCP port 702. The 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. You can view HA heartbeat sessions from the web-based manager System > Status > Session page. HA heartbeat sessions appear as TCP sessions between the HA heartbeat interface IP addresses that use port 702 as the destination port.

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.

## HA heartbeat 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 devices

A heartbeat device 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 devices. An interface becomes a heartbeat device when it is assigned a heartbeat device priority. The HA configuration in [Figure 2](#) shows port3 and port4/ha configured as heartbeat devices.

**Figure 2: Example FortiGate-3000 heartbeat device configuration**

Standalone Mode  
 High Availability

Mode: Active-Active  
 Group ID: 34 (0-63)  
 Unit Priority: 128 (0-255)  
 (The unit with the highest priority will be HA master.)

Override master:  Enable

Password: \*\*\*\*\*  
 Retype Password: \*\*\*\*\*

Schedule: Round-Robin

Interface	Priorities of Heartbeat Device (0-512)	Monitor Priorities (0-512)
internal		
external		
port1		
port2		
port3	50	
port4/ha	100	

Apply

The heartbeat device with the highest priority is the active heartbeat device. In Figure 2, port4/ha is the active heartbeat device. The active heartbeat device sends and receives all heartbeat communications. If the active heartbeat device fails or is disconnected on one or more of the cluster units, the heartbeat device with the next highest priority becomes the active heartbeat device. This is called heartbeat device failover. Heartbeat device failover occurs transparently, without interrupting the communication sessions being processed by the cluster and without affecting cluster synchronization.

By default, for all FortiGate units, two interfaces are configured to be heartbeat devices. The active heartbeat device has a priority of 100. A second, or backup heartbeat device has a priority of 50.

- The FortiGate-300, 400, 500, 800, 1000, 3000, and 3600 HA interface has the highest heartbeat device priority.
- The FortiGate-60, 100, 200, and the FortiWiFi-60 DMZ interface has the highest heartbeat device priority.
- The FortiGate-100A and 200A DMZ2 interface has the highest heartbeat device priority.
- The FortiGate-300A, 400A, and 500A port4 interface has the highest heartbeat device priority.
- The FortiGate-4000 out of band management interface has the highest heartbeat device priority.
- The FortiGate-5000 has two dedicated HA heartbeat devices (Port 9 and Port 10). Port 10 has the highest heartbeat device priority.

You can change the heartbeat device configuration as required. All interfaces can be assigned different heartbeat priorities. You can also configure only one interface to be a heartbeat device. You can set the heartbeat device priority for each interface to any number between 1 and 512. In all cases, the heartbeat device with the highest priority is used for all HA heartbeat communication. If this interface fails or becomes disconnected, the interface with the next highest priority handles all of the heartbeat traffic.

For the HA cluster to function correctly, at least one interface must be a heartbeat device. Also the heartbeat devices of all cluster units must be connected together. If heartbeat communication is interrupted and cannot fail over to a second heartbeat device, the cluster stops processing traffic.

## Heartbeat device IP addresses

You do not need to assign IP addresses to the heartbeat device interfaces for them to be able to process heartbeat packets. The FGCP assigns virtual IP addresses to the heartbeat device interfaces. The primary unit heartbeat device IP address is 10.0.0.1. Subordinate units are assigned heartbeat device IP addresses 10.0.0.2, 10.0.0.3, and so on.

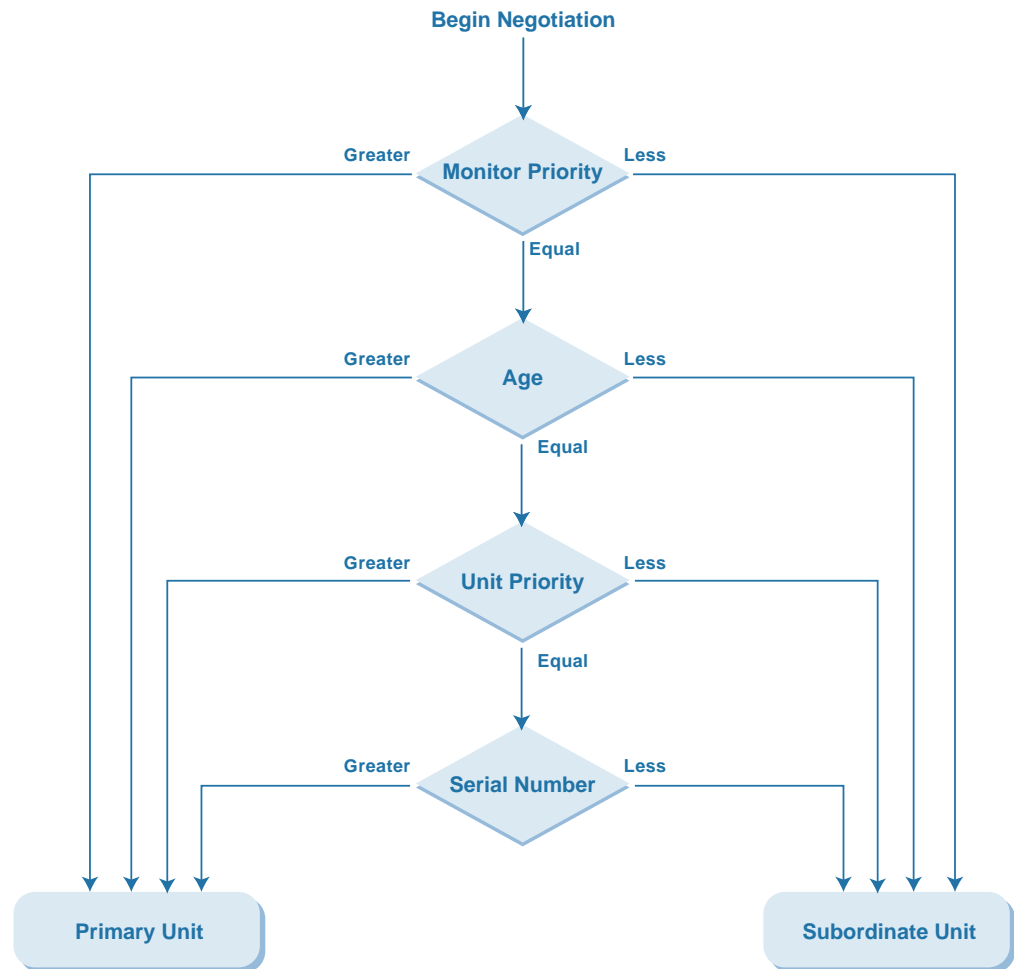
For best results, isolate the heartbeat devices from your user networks by connecting the heartbeat devices to a separate switch that is not connected to any network. If the cluster consists of two FortiGate units you can connect the heartbeat device interfaces directly using a crossover cable. Heartbeat packets contain sensitive information about the cluster configuration. Heartbeat packets may also use a considerable amount of network bandwidth. For these reasons, it is preferable to isolate heartbeat packets from your user networks.

Both HA heartbeat and data traffic are supported on the same FortiGate interface. In NAT/Route mode, if you decide to use the heartbeat device interfaces for processing network traffic or for a management connection, you can assign the interface any IP address. In Transparent mode, you can connect the interface to your network and configure management access to it. These configurations do not affect heartbeat traffic or the heartbeat device IP addresses.

## Primary unit selection

Once FortiGate units recognize that they can form a cluster, the cluster selects a primary unit. Primary unit selection is done automatically by the cluster based on monitor priority, age, unit priority, and FortiGate unit serial number as shown in [Figure 3](#).

Figure 3: Selecting the primary unit



**Monitor Priority** The cluster unit with the highest monitor priority becomes the primary unit. Normally, when the cluster starts up, all cluster units have the same monitor priority, so monitor priority does not affect primary unit selection when the cluster first starts. However, during operation if a monitored interface fails, the cluster unit with the failed interface has a lower monitor priority and so cannot become the primary unit.

**Age** The amount of time the unit has been in the cluster. The longer that a cluster unit has been operating in a cluster, the more likely it is that this unit will become the primary unit. When a negotiation starts, age is reset to zero for all negotiating cluster units. If a cluster is operating and a new unit attempts to join the cluster, the age of the units already in the cluster is not reset, so the unit added to the functioning cluster becomes a subordinate unit.

**Unit Priority** The unit priority set by the administrator. Cluster units with a higher unit priority are more likely to become the primary unit. By default, the unit priority for all cluster units is 128. You can change the primary unit selection outcome by changing the unit priority of the cluster units.

**Serial Number** The FortiGate unit serial number. Cluster units with higher serial numbers are more likely to become the primary unit. If you do not change the unit priority, the FortiGate unit with the highest serial number always becomes the primary unit.

Primary unit selection also occurs 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.

## Cluster virtual MAC address

To complete primary unit selection, the FGCP assigns a virtual MAC address to all primary unit interfaces. This virtual MAC address is created based on the cluster group ID. See ["Group ID" on page 27](#) for information about the Group ID and how the group ID affects the virtual MAC address.

The primary unit sends special ARP packets to update the switches connected to the cluster interfaces with this MAC address change. The switches update their MAC forwarding tables with this MAC address change. 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.

## Subordinate unit priority

Normally, after the primary unit is selected, the cluster organizes the subordinate units into a priority order using the same method as was used to select the primary unit. This means that if you do not change the monitor priority or unit priority, the subordinate units are arranged in priority order that matches their serial numbers. This priority order does not affect which cluster unit becomes the primary unit if the current primary unit fails. It's just a way of organizing the cluster units. When viewing cluster information or managing individual cluster units from the CLI, the cluster units are listed in priority order ([Figure 4](#)).

**Figure 4: Cluster members list showing cluster units listed in priority order**

Cluster ID	Status	Up Time	Monitor			
FGT-602104400533	✔	0 days 0 hours 8 minutes 59 seconds	CPU Usage 0%	Active Sessions 16	Total Packets 1337	Virus Detected 0
			Memory Usage 60%	Network Utilization 11 Kbps	Total Bytes 565170	Intrusion Detected 0
FGT-602803030702	✔	0 days 0 hours 9 minutes 19 seconds	CPU Usage 3%	Active Sessions 7	Total Packets 55	Virus Detected 0
			Memory Usage 55%	Network Utilization 15 Kbps	Total Bytes 8058	Intrusion Detected 0
FGT-602104400531	✔	0 days 0 hours 8 minutes 23 seconds	CPU Usage 0%	Active Sessions 6	Total Packets 23	Virus Detected 0
			Memory Usage 55%	Network Utilization 10 Kbps	Total Bytes 4956	Intrusion Detected 0

## Controlling primary unit selection

You can change the unit 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 (monitor priority). Unit priority can be individually set 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 unit priority becomes the primary unit.

You can configure a different unit priority for each cluster unit to control the order in which cluster units become the primary unit when a cluster unit fails. For example, if you have three units in a cluster you can set the unit priorities as shown in Table 1. When the cluster starts up, cluster unit A becomes the primary unit because it has the highest unit priority. If cluster unit A fails, cluster unit B becomes the primary unit because cluster unit B has a higher unit priority than cluster unit C.

**Table 1: Example unit priorities for a cluster of three cluster units**

Cluster unit	Unit priority
A	200
B	100
C	50

## Using override master to control primary unit selection

Another HA setting, called override master, forces the cluster to renegotiate to select the primary unit. Usually you would enable override master for the cluster unit with the highest unit priority. If override master is not enabled, the cluster unit with the highest unit priority may not always maintain its position as the primary unit.

In a functioning cluster that has just started up, the primary unit will always be the cluster unit with the highest unit priority. Of course, if this primary unit fails, another unit becomes the primary unit. If the failed primary unit recovers, starts up again and rejoins the cluster it cannot become the primary unit because its age is lower than the age of the other cluster units. You have lost control of selecting the primary unit.

If you enable override master on the unit with the highest unit priority, when this unit joins an already functioning cluster, override master causes the cluster to renegotiate. When negotiation starts, the age of all the units in the negotiation is reset to zero. Age is not a factor in the negotiation, and the unit with the highest unit priority becomes the primary unit.

You can also enable override master for all cluster units to make sure that whenever a failure occurs the cluster always negotiates to select the primary unit. If you do not enable override master for all cluster units, when the primary unit fails, the cluster may not select the expected unit to be the new primary unit. Normally this is not an issue. But if you want full control over which unit becomes the primary unit after a failover, you can enable override master.

## 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)

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. Subordinate units use this information to resume processing network traffic if the primary unit fails. Cluster state information also includes a link state database that stores link state information for all of the cluster units. Link state information is used for link failover. All cluster units keep these databases up to date by sharing state information with the other cluster units.

Use active-passive HA for a more resilient session failover environment than active-active HA (described below). In active-passive HA, session failover occurs for all traffic. Active-active HA does not provide session failover for virus scanning traffic.

## Active-active HA (load balancing and failover)

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 and ICMP 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. If a subordinate unit fails, the primary unit redistributes TCP communications sessions among the remaining cluster units. UDP, ICMP, and virus scanning sessions are not failed over. Because of these limitations, active-active HA is a less robust failover solution than active-passive HA.

## Device failover and link failover

The FGCP provides transparent device and link failover. Failover 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.

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, cluster units record log messages about the event and send SNMP traps. This information can be used by network administrators to find and fix the problem that caused the failure.

The sections below provide brief introductions to device and link failover. See [“Failover protection” on page 105](#) for a more complete discussion of device and link failover.

### Device failover

Device failover means that if a device in the cluster (a cluster unit) fails, the cluster reorganizes itself to continue operating with minimal or no effect on network traffic. To support device failover, the cluster maintains a session table for all communication sessions being processed by the cluster. The session table information is available to the remaining cluster units after a failure. Using this information, the remaining cluster units can resume communication sessions without interruption.

## Link failover

Link failover means that if a monitored link fails, the cluster reorganizes to re-establish the link and to continue operating with minimal or no disruption of network traffic. A monitored link is a cluster interface configured with a monitor priority. If you configure monitor priorities for interfaces connected to high priority networks, link failover maintains traffic flow to and from these high priority networks.

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 high priority network fails, to maintain traffic flow to and from this network, the cluster must select a different primary unit. The new primary unit will have an active link to this network and traffic flow is maintained.

# Configuration reference

Use the information in this chapter as a reference to all HA configuration parameters. This chapter describes all **System > Config > HA** web-based manager settings and all `config system ha` and `execute ha` keywords. This chapter also describes the syntax and output for some `diagnose sys ha` commands.

- [Web-based manager HA configuration settings](#)
- [config system ha](#)
- [execute ha manage](#)
- [execute ha synchronize](#)



**Note:** If you change the HA settings of a running cluster, the cluster negotiates and may select a new primary unit. See [“Changing HA configuration options” on page 88](#).

## Web-based manager HA configuration settings

From the web-based manager go to **System > Config > HA** and use the options described below to configure HA.

- [Standalone Mode](#)
- [Cluster Members](#)
- [High Availability](#)
- [Mode](#)
- [Group ID](#)
- [Unit Priority](#)
- [Override Master](#)
- [Password](#)
- [Schedule](#)
- [Priorities of Heartbeat Device](#)
- [Monitor priorities](#)

Figure 5: HA configuration (FortiGate-3600)

Interface	Priorities of Heartbeat Device (0-512)	Monitor Priorities (0-512)
internal		
external		
port1		
port2		
port3		
port4	50	
port5/ha	100	

## Standalone Mode

Standalone mode is 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.

## Cluster Members

When the cluster is operating, you can select Cluster Members to view the status of all FortiGate units in the cluster. Status information includes the cluster ID, status, up time, weight, and monitor information. For more information, see [“Viewing the status of cluster units” on page 85](#).

## High Availability

Select High Availability to operate the FortiGate unit in HA mode. After selecting High Availability, complete the remainder of the HA configuration.

## Mode

All members of the HA cluster must be set to the same HA mode.

**Active-Active** Load balancing and failover HA. Each cluster unit actively processes connections and monitors the status of the other cluster units. The primary unit controls load balancing among all of the cluster units.

**Active-Passive** Failover HA. The primary unit processes all connections. All other cluster units passively monitor the cluster status and remain synchronized with the primary unit.

## Group ID

The group ID range is from 0 to 63. All cluster units must have the same group ID. When the FortiGate units are switched to HA mode, all of the interfaces of all of the cluster units acquire the same virtual MAC address. This virtual MAC address is set according to the group ID. [Table 2](#) lists the virtual MAC address set for each group ID.

**Table 2: HA group ID and virtual MAC address**

Group ID	Virtual MAC Address
0	00-09-0f-06-ff-00
1	00-09-0f-06-ff-01
2	00-09-0f-06-ff-02
3	00-09-0f-06-ff-03
...	...
63	00-09-0f-06-ff-3f

If you have more than one HA 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, the duplicate MAC addresses cause addressing conflicts on the network.

## Unit Priority

Optionally set the unit priority of the cluster unit. Each cluster unit can have a different unit priority. The unit priority is not synchronized among cluster members. Each cluster unit can have a different unit priority. During HA negotiation, the unit with the highest unit priority becomes the primary unit. The unit priority range is 0 to 255. The default unit priority is 128.

You can use the unit priority to control the order in which cluster units become the primary unit when a cluster unit fails. For example, if you have three FortiGate units in a cluster you can set the unit priorities as shown in [Table 3](#). Cluster unit A will always be the primary unit because it has the highest priority. If cluster unit A fails, cluster unit B becomes the primary unit because cluster unit B has a higher unit priority than cluster unit C.

**Table 3: Example unit priorities for a cluster of three cluster units**

Cluster unit	Unit priority
A	200
B	100
C	50

In a functioning cluster, if you change the unit priority of the current primary unit to a lower priority, when the cluster renegotiates a different cluster unit becomes the primary unit.

## Override Master

Configure a cluster unit to always override the current primary unit and become the primary unit. Enable override master for the cluster unit that you have given the highest unit priority. Enabling override master means that this cluster unit always becomes the primary unit.

In a typical FortiGate cluster configuration, the primary unit is selected automatically. In some situations, you might want to control which unit becomes the primary unit. You can configure a FortiGate unit as the permanent primary unit by setting a high unit priority and by selecting override master. With this configuration, the same cluster unit always becomes the primary unit.

If override master is enabled and the primary unit fails, another cluster unit becomes the primary unit. When the cluster unit with override master enabled rejoins the cluster it overrides the current primary unit and becomes the new primary unit. When this override occurs, all communication sessions through the cluster are lost and must be re-established.

Override master is not synchronized to all cluster units.

In a functioning cluster, if you select override master for a cluster unit the cluster re-negotiates and may select a new primary unit.

## Password

Enter a password for the HA cluster. The password must be the same for all cluster units. 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.

## Schedule

If you are configuring an active-active cluster, select a load balancing schedule.

<b>None</b>	No load balancing. Select None when the cluster interfaces are connected to load balancing switches. If you select None, the Primary unit does not load balance traffic and the subordinate units process incoming traffic that does not come from the Primary unit. For all other load balancing schedules, all traffic is received first by the Primary unit, and then forwarded to the subordinate units. The subordinate units only receive and process packets sent from the primary unit.
<b>Hub</b>	Load balancing if the cluster interfaces are connected to a hub. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet.
<b>Least-Connection</b>	Least connection load balancing. If the cluster units are connected using switches, select Least Connection to distribute network traffic to the cluster unit currently processing the fewest connections.
<b>Round-Robin</b>	Round robin load balancing. If the cluster units are connected using switches, select Round-Robin to distribute network traffic to the next available cluster unit.

<b>Weighted Round-Robin</b>	Weighted round robin load balancing. Similar to round robin, but weighted values are assigned to each of the units in a cluster based on their capacity and on how many connections they are currently processing. For example, the primary unit should have a lower weighted value because it handles scheduling and forwards traffic. Weighted round robin distributes traffic more evenly because units that are not processing traffic will be more likely to receive new connections than units that are very busy. To configure weighted round robin weights, see <a href="#">“Configuring weighted-round-robin weights” on page 124</a> .
<b>Random</b>	Random load balancing. If the cluster units are connected using switches, select Random to randomly distribute traffic to cluster units.
<b>IP</b>	Load balancing according to IP address. If the cluster units are connected using switches, select IP to distribute traffic to units in a cluster based on the Source IP and Destination IP of the packet.
<b>IP Port</b>	Load balancing according to IP address and port. If the cluster units are connected using switches, select IP Port to distribute traffic to units in a cluster based on the source IP, source port, destination IP, and destination port of the packet.

By default a FortiGate HA active-active cluster load balances virus scanning sessions among all cluster units. All other traffic is processed by the primary unit. Using the CLI, you can configure the cluster to load balance TCP network traffic among all cluster units. See [“Load balancing virus scanning sessions and TCP sessions” on page 124](#).

## Priorities of Heartbeat Device

Enable or disable HA heartbeat communication and set the heartbeat priority for each interface in the cluster.

By default, HA heartbeat communication is set for two interfaces. 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 device configuration as long as you can connect the heartbeat device interfaces together.

The heartbeat priority must be set for at least one cluster interface. If heartbeat communication is interrupted the cluster stops processing traffic.

To enable HA heartbeat communication for an interface, enter a priority for the interface. To disable HA heartbeat communication for an interface, delete the priority for the interface.

The HA heartbeat priority range is 0 to 512. The interface with the highest priority handles all HA heartbeat traffic. If this interface fails or becomes disconnected, the interface with the next highest priority handles all HA heartbeat traffic.

The cluster units use the ethernet interfaces configured with HA heartbeat priorities for HA heartbeat communication. 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.

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.

**Table 4: Default heartbeat device configuration**

FortiGate model	Default heartbeat device	Default priority
FortiGate-60	WAN1	50
	DMZ	100
FortiGate-100	External	50
	DMZ	100
FortiGate-100A	External	50
	DMZ 2	100
FortiGate-200	External	50
	DMZ	100
FortiGate-200A	External	50
	DMZ 2	100
FortiGate-300	External	50
	DMZ/HA	100
FortiGate-300A	Port 3	50
	Port 4	100
FortiGate-400	Port 3	50
	Port 4/HA	100
FortiGate-400A	Port 3	50
	Port 4	100
FortiGate-500	Port 1	50
	HA	100
FortiGate-500A	Port 3	50
	Port 4	100
FortiGate-800	Port 1	50
	HA	100
FortiGate-1000	Port 3	50
	Port 4/HA	100
FortiGate-3000	Port 3	50
	Port 4/HA	100
FortiGate-3600	Port 4	50
	Port 5/HA	100
FortiGate-4000	External	50
	oobm	100
FortiGate-5000	Port 9	50
	Port 10	100

By default a FortiGate-5000 HA cluster uses Port 9 and Port 10 for heartbeat communication. Port 9 and Port 10 are not visible on the FortiGate-5000 faceplate or on the web-based manager, but they are visible on the CLI. You can use the CLI to view and change the heartbeat priority configuration for Port 9 and Port 10. You can use the web-based manager or the CLI to set the heartbeat priority for other interfaces.

Change the heartbeat device priorities as required to control the interface that is used for heartbeat traffic and the interface to which heartbeat traffic reverts if the interface with the highest heartbeat priority fails or is disconnected.

Setting the heartbeat priority for more interfaces increases the reliability of the cluster. To optimize bandwidth use, you can route most heartbeat traffic to interfaces that handle less network traffic. You can also create a failover path by setting heartbeat priorities so that you can control the order in which interfaces are used for heartbeat traffic.

The heartbeat priority must be set for at least one cluster interface. If heartbeat communication is interrupted the cluster stops processing traffic.

### Heartbeat device IP addresses

You do not need to assign IP addresses to heartbeat device interfaces for them to be able to process heartbeat packets. The cluster assigns virtual IP addresses to the heartbeat device interfaces. The primary unit heartbeat device interface is assigned the IP address 10.0.0.1 and the subordinate unit heartbeat device interface is assigned the IP address 10.0.0.2. A third cluster unit would be assigned the IP address 10.0.0.3 and so on.

For best results, isolate each heartbeat device 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 the interface to process network traffic.

For most FortiGate models if you do not change the heartbeat device configuration, you would isolate the HA interfaces of all of the cluster units by connecting them all to the same switch. If the cluster consists of two FortiGate units you can connect the heartbeat device interfaces directly using a crossover cable.

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

In Transparent mode, you can connect the 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.

## Monitor priorities

Enable or disable monitoring a FortiGate interface to verify that the interface is functioning properly and connected to its network. If a monitored interface fails or is disconnected from its network the interface leaves the cluster. The cluster reroutes 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 you can re-establish traffic flow through the interface (for example, if you re-connect a disconnected network cable) the interface rejoins the cluster. If Override Master is enabled for this FortiGate unit (see [“Override Master” on page 28](#)), this FortiGate unit becomes the primary unit in the cluster again.

Increase the priority of interfaces connected to higher priority networks or networks with more traffic. The monitor priority range is 0 to 512. Changes to monitor priorities are synchronized to all cluster units.

If a high priority interface on the primary unit fails, one of the other units in the cluster becomes the new primary unit to provide better service to the high priority network.

If a low priority interface fails on one cluster unit and a high priority interface fails on another cluster unit, a unit in the cluster with a working connection to the high priority interface would, if it becomes necessary to negotiate a new primary unit, be selected instead of a unit with a working connection to the low priority interface.

## config system ha

Use this command to enable and configure FortiGate high availability (HA). HA is supported on FortiGate models numbered 60 and higher and on the FortiWiFi-60. Using the `config system ha` command you must configure all cluster members with the same group ID, mode, and password before putting the cluster into HA mode.

Group ID, mode, and password are not synchronized between cluster units. The primary unit synchronizes all other configuration settings, including the other HA configuration settings.



**Note:** You cannot enable HA mode if one of the FortiGate unit interfaces is configured using DHCP or PPPoE. If DHCP or PPPoE is configured, the `config ha mode` keyword is not available.

### Command syntax pattern

```
config system ha
  set <keyword> <variable>

config system ha
  unset <keyword>

get system ha

show system ha
```

## system ha command keywords and variables

Keywords and variables	Description	Default
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.	3
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.	disable
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.	disable
groupid <id_integer>	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.	0
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. 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 send heartbeat packets quickly enough.	6
hb-interval <interval_integer>	The heartbeat interval 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.	2

**system ha command keywords and variables (Continued)**

Keywords and variables	Description	Default
hbdev <interface-name_str> <priority_integer>	<p>Enable or disable HA heartbeat communication and set the heartbeat priority for each interface in the cluster.</p> <p>By default HA heartbeat is set for two interfaces. 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 <code>hbdev</code> configuration as long as you can connect the <code>hbdev</code> interfaces together.</p> <p>Enter all of the names and heartbeat priorities for the interfaces to be configured. If you want to remove an interface from the list or add an interface to the list, you must retype the list with the interface and its priority removed or added.</p> <p>The cluster units use the ethernet interfaces configured with HA heartbeat priorities for HA heartbeat communication. 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.</p> <p>The heartbeat priority range is 0 to 512. The interface with the highest priority handles all of the heartbeat traffic. If this interface fails or becomes disconnected, the interface with the next highest priority handles all of the heartbeat traffic.</p> <p>You can enable heartbeat communications for physical interfaces, but not for VLAN subinterfaces.</p> <p>Enabling the HA heartbeat for more interfaces increases reliability. If an interface fails, the HA heartbeat can be diverted to another interface.</p> <p>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.</p> <p>Heartbeat communication must be enabled on at least one interface. If heartbeat communication is interrupted the cluster stops processing traffic.</p>	See <a href="#">Table 4 on page 30</a> .
hello-holddown <holddown_integer>	<p>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.</p> <p>The hello state hold-down time range is 5 to 300 seconds.</p>	20
load-balance-all {disable   enable}	<p>Configure active-active HA to load balance TCP and virus scanning sessions or to load balance virus scanning sessions only. Enter <code>enable</code> to load balance TCP and virus scanning sessions. Enter <code>disable</code> to load balance only virus scanning sessions.</p>	disable

**system ha command keywords and variables (Continued)**

Keywords and variables	Description	Default
mode {a-a   a-p   standalone}	<p>Set the HA mode.</p> <p>Enter <code>a-p</code> to create an Active-Passive HA cluster, in which the primary unit is actively processing all connections and the others are passively monitoring the status and remaining synchronized with the primary unit.</p> <p>Enter <code>a-a</code> 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.</p> <p>All members of an HA cluster must be set to the same HA mode.</p> <p>Enter <code>standalone</code> to remove the FortiGate unit from an HA cluster.</p>	standalone
monitor {<interface-1_str> <priority-1_integer> <interface_2_str> <priority-2_integer>}	<p>Enable or disable monitoring FortiGate interfaces and setting monitor priorities. You can enter one or more interface names followed by a space and a monitor priority. Use a space to separate each interface name and priority pair. If you want to remove an interface from the list, add an interface to the list, or change the monitor priority of an interface you must retype the list with the options changed as required.</p> <p>You can monitor physical interfaces but not VLAN subinterfaces.</p> <p>FortiGate models that contain an internal switch do not support interface monitoring and device failover for this interface. 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.</p> <p>Increase the priority of interfaces connected to higher priority networks or networks with more traffic. The monitor priority range is 0 to 255.</p> <p>If a high priority interface on the primary unit fails, one of the other units in the cluster becomes the new primary unit to provide better service to the high priority network.</p> <p>If a low priority interface fails on one cluster unit and a high priority interface fails on another cluster unit, a unit in the cluster with a working connection to the high priority interface would, if it becomes necessary to negotiate a new primary unit, be selected instead of a unit with a working connection to the low priority interface.</p>	No default
override {disable   enable}	<p>Configure the FortiGate unit to always override the current primary unit and become the primary unit in its place. Enable Override Master for the cluster unit that you have given the highest unit priority. Enabling Override Master means that this cluster unit always becomes the primary unit.</p>	disable
password <password_str>	<p>Enter a password for the HA cluster. The password must be the same for all FortiGate units in the HA cluster. The maximum password length is 15 characters.</p>	No default

**system ha command keywords and variables (Continued)**

Keywords and variables	Description	Default
priority <priority_integer>	<p>Optionally set the unit priority of the cluster unit. Each cluster unit can have a different unit priority (the unit priority is not synchronized among cluster members). During HA negotiation, the unit with the highest unit priority becomes the primary unit. The unit priority range is 0 to 255.</p> <p>You can use the unit priority to control the order in which cluster units become the primary unit when a cluster unit fails. For example, if you have three FortiGate-3600s in a cluster you can set the unit priorities as shown in <a href="#">Table 3</a>. Cluster unit A will always be the primary unit because it has the highest priority. If cluster unit A fails, cluster unit B becomes the primary unit because cluster unit B has a higher unit priority than cluster unit C.</p>	128
route-hold <hold_integer>	<p>The time that the primary unit waits between sending routing table updates to subordinate units in a cluster.</p> <p>The route hold range is 0 to 3600 seconds.</p> <p>To avoid the flooding routing table updates to subordinate units, set <code>route-hold</code> to a relatively long time to prevent subsequent updates from occurring too quickly.</p> <p>The <code>route-hold</code> time should be coordinated with the <code>route-wait</code> time. See the <code>route-wait</code> description for more information.</p>	10
route-ttl <tll_integer>	<p>The time to live for routes in a cluster unit routing table.</p> <p>The time to live range is 0 to 3600 seconds.</p> <p>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.</p> <p>Normally, the <code>route-ttl</code> 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.</p> <p>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.</p>	0

**system ha command keywords and variables (Continued)**

Keywords and variables	Description	Default
<code>route-wait</code> <code>&lt;wait_integer&gt;</code>	<p>The time the primary unit waits after receiving a routing table update before sending the update to the subordinate units in the cluster.</p> <p>For quick routing table updates to occur, set <code>route-wait</code> to a relatively short time so that the primary unit does not hold routing table changes for too long before updating the subordinate units.</p> <p>The <code>route-wait</code> range is 0 to 3600 seconds.</p> <p>Normally, because the <code>route-wait</code> time is 0 seconds the primary unit sends routing table updates to the subordinate units every time the primary unit routing table changes.</p> <p>Once a routing table update is sent, the primary unit waits the <code>route-hold</code> time before sending the next update.</p> <p>Usually routing table updates are periodic and sporadic. Subordinate units should receive these changes as soon as possible so <code>route-wait</code> is set to 0 seconds. <code>route-hold</code> can be set to a relatively long time because normally the next route update would not occur for a while.</p> <p>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 <code>route-wait</code> to a longer time reduces the frequency with which additional routing updates are sent, which prevents flooding of routing table updates from occurring.</p>	0

### system ha command keywords and variables (Continued)

Keywords and variables	Description	Default
<pre> schedule {hub   ip   ipport   leastconnection   none   random   round-robin   weight-round-robin} </pre>	<p>A-A load balancing schedule.</p> <p><code>none</code>: no load balancing. Use <code>none</code> when the cluster interfaces are connected to load balancing switches.</p> <p><code>hub</code>: load balancing if the cluster interfaces are connected to a hub. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet.</p> <p><code>leastconnection</code>: least connection load balancing. If the cluster units are connected using switches, use <code>leastconnection</code> to distribute traffic to the cluster unit currently processing the fewest connections.</p> <p><code>round-robin</code>: round robin load balancing. If the cluster units are connected using switches, use <code>round-robin</code> to distribute traffic to the next available cluster unit.</p> <p><code>weight-round-robin</code>: weighted round robin load balancing. Similar to round robin, but weighted values are assigned to each of the units in a cluster based on their capacity and on how many connections they are currently processing. For example, the primary unit should have a lower weighted value because it handles scheduling and forwards traffic. Weighted round robin distributes traffic more evenly because units that are not processing traffic will be more likely to receive new connections than units that are very busy. You can optionally use the <code>weight</code> keyword to set a weighting for each cluster unit.</p> <p><code>random</code>: random load balancing. If the cluster units are connected using switches, use <code>random</code> to randomly distribute traffic to cluster units.</p> <p><code>ip</code>: load balancing according to IP address. If the cluster units are connected using switches, use <code>ip</code> to distribute traffic to units in a cluster based on the Source IP and Destination IP of the packet.</p> <p><code>ipport</code>: load balancing according to IP address and port. If the cluster units are connected using switches, use <code>ipport</code> to distribute traffic to units in a cluster based on the source IP, source port, destination IP, and destination port of the packet.</p>	round-robin

**system ha command keywords and variables (Continued)**

Keywords and variables	Description	Default
weight <priority-id_integer> <weight_integer>	The weighted round robin load balancing weight to assign to each cluster unit. When you set <code>schedule</code> to <code>weight-round-robin</code> you can use the <code>weight</code> 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.  <code>priority-id_integer</code> is a number from 0 to 31 that identifies the priority of the cluster unit. <code>weight_integer</code> is a number between 0 and 32 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.	1 for all 32 units

**Examples**

This example shows how to configure a FortiGate unit for active-active HA operation. The example shows how to enter the basic HA configuration (`mode`, `group_id`, and `password`). You would enter the exact same command on every FortiGate unit in the cluster.

```
config system ha
  set mode a-a
  set groupid 15
  set password HA1passw0rd
end
```

The following example shows how to enable heartbeat for the internal interface and how to set the priority to 100.

```
config system ha
  set hbdev internal enable
  set hbdev_priority internal 100
end
```

The following example shows how to enable connection monitoring for the external, internal and DMZ interfaces and how to set the monitor priority of the internal interface to 200, the monitor priority of the external interface to 100, and the monitor priority of the DMZ interface to 50.

```
config system ha
  set monitor internal 200 external 100 dmz 50
end
```

This example shows how to display the settings for the `system ha` command. This command displays a table of HA configuration options and their current settings. The information displayed is the HA configuration of the cluster unit to which you are connected.

```
get system ha
  groupid           : 63
  mode              : a-a
  override          : enable
  password          : *
  priority          : 100
  schedule          : round-robin
  monitor           : internal 100
  hbdev             : ha 100 port1 50
  route-ttl         : 0
  route-wait        : 0
  route-hold        : 10
  encryption        : disable
  authentication    : disable
  hb-interval       : 4
  hb-lost-threshold : 6
  helo-holddown    : 20
  arps              : 3
  load-balance-all : disable
```

This example shows how to display the configuration for the `system ha` command. This command displays the HA configuration stored in the FortiGate configuration database.

```
show system ha
  config system ha
    set groupid 63
    set mode a-a
    set monitor internal 100
    set override enable
    set password ENC
    8IGXTTYa9Im07O6yQRt7rezaZEprLj5OFfwAhuzbDTon8pV5lH+DnXWkK
    USLlBL+DxxgR5bxDcAolerOe+NwTJNXXPx+/7KLaetSqtn9nx+EAqu
    set priority 100
    set load-balance-all disable
  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 5: Example weights for three cluster units**

Cluster unit priority	Weight
0	1
1	3
2	3

```

config system ha
  set schedule weight-round-robin
  set weight 0 1
  set weight 1 3
  set weight 2 3
end

```

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.

## execute ha manage

Use this command from the CLI of the primary unit in an HA cluster to connect to the CLI of another unit in the cluster.

### Command syntax

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

### Example

This example shows how to connect to a subordinate unit in a cluster of three FortiGate units.

```

execute ha manage ?
<1>    Subsidiary unit FPS3012803021709
<2>    Subsidiary unit FPS3082103021989

```

Type 2 and press enter to connect to the second unit in the list. The CLI prompt changes to the host name of this unit. To return to the primary unit, type `exit`.

## execute ha synchronize

Use this command from a subordinate unit 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 FortiProtect 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}
```

### execute ha synchronize command keywords and variables

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

### Example

From the CLI on 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
```

# FortiGate HA installation and configuration examples

This chapter contains detailed examples that describe a variety of FortiGate cluster installations and configurations. The examples also illustrate how to change the HA configuration to achieve specific results.

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 the latest [FortiGate Administration Guide](#) and [FortiGate CLI Reference](#), both available from the [Fortinet Knowledge Center](#).

This chapter contains the following configuration examples:

- [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](#)
- [Customizing primary unit selection](#)
- [Configuring monitor priorities for link failover protection](#)

For configuration examples involving third party products, see [“Troubleshooting layer-2 switches”](#) on page 131.

## Basic NAT/Route mode installation

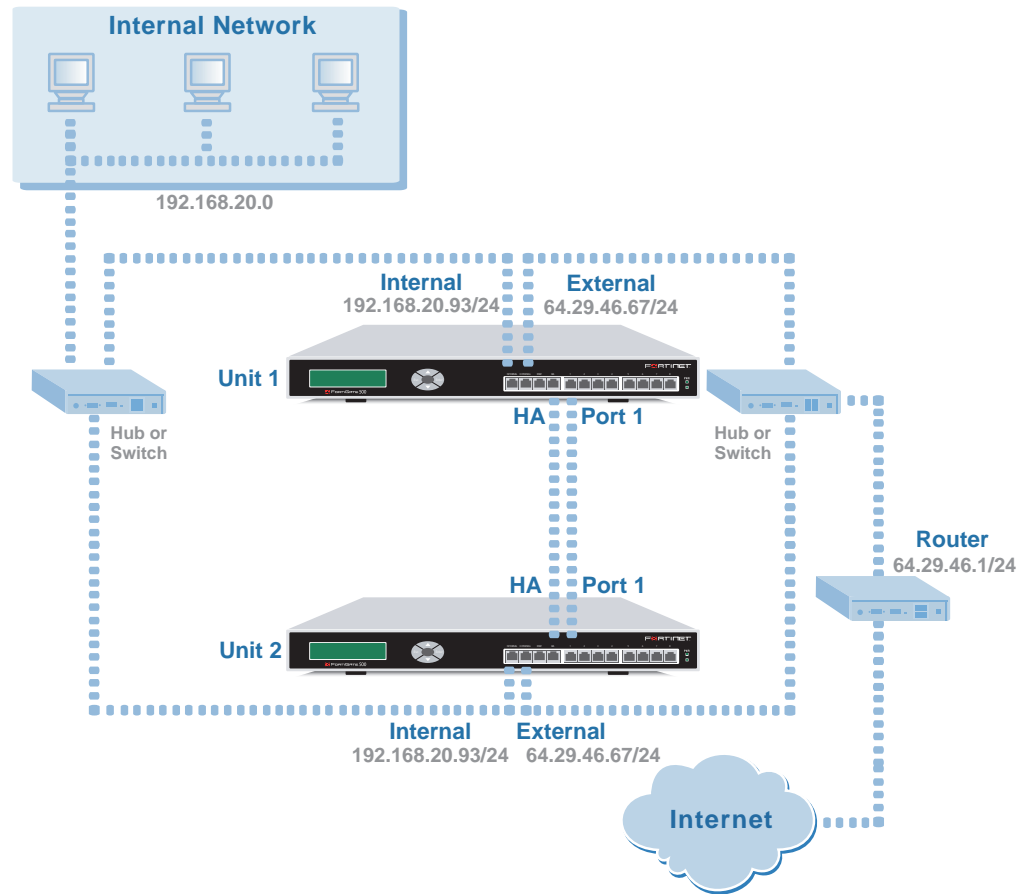
This example describes a simple HA network topology that includes an HA cluster of two FortiGate-500 units installed between an internal network and the Internet. The example includes web-based manager and CLI procedures.

- [Example NAT/Route mode HA network topology](#)
- [General configuration steps](#)
- [Web-based manager configuration steps](#)
- [CLI configuration steps](#)

## Example NAT/Route mode HA network topology

Figure 6 shows a typical FortiGate-500 HA cluster consisting of two FortiGate-500 units (Unit 1 and Unit 2) connected to the same internal and external networks.

Figure 6: NAT/Route mode HA network topology



The default FortiGate-500 Priorities of Heartbeat Device configuration sets the heartbeat device priority of the HA interface to 100 and Port 1 to 50. As a result, in addition to connecting the FortiGate-500 units to their networks, this example describes connecting together the FortiGate-500 HA interfaces and Port 1 interfaces (as shown in Figure 6). Because the cluster consists of two FortiGate units, you can make the connections between the HA interfaces and between the Port 1 interfaces using crossover cables. You could also use switches as shown for the internal and external interfaces.

## General configuration steps

This section describes how to configure an active-active HA cluster to run in NAT/Route mode using the topology shown in [Figure 6](#). These procedures assume that the FortiGate-500 units are running the same v2.80 firmware build and are set to the factory default configuration.

- 1 Configure the FortiGate units for HA operation.
  - Change the FortiGate unit host name.
  - Configure HA.
- 2 Connect the cluster to the network.
- 3 Add basic configuration settings to the cluster.
  - 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-500 units for NAT/Route HA operation from the FortiGate unit 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.

### 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.
- 5 Go to **System > Status**.
- 6 Beside Host Name select Change.
- 7 Enter a new Host Name for this FortiGate unit.
- 8 Select OK.

### To configure HA settings

- 1 Go to **System > Config > HA**.
- 2 Select High Availability.
- 3 Configure HA settings.

<b>Mode</b>	Active-Active
<b>Group ID</b>	63

<b>Unit Priority</b>	128 (Keep the default setting).
<b>Override master</b>	Keep the default setting.
<b>Password</b>	ha500pswd
<b>Retype Password</b>	ha500pswd
<b>Schedule</b>	Round-Robin
<b>Priorities of Heartbeat Device</b>	Keep the default setting.
<b>Monitor Priorities</b>	Keep the default setting.



**Note:** You can change the Priorities or Heartbeat Device and Monitor priorities when the cluster is operating.

#### 4 Select Apply.

The FortiGate unit negotiates to establish an HA cluster. When you select apply you temporarily lose connectivity with the FortiGate unit because the HA cluster negotiates to select the primary unit. Also, the MAC address of all of the FortiGate unit interfaces change. See [“Group ID” on page 27](#).

In this example, the MAC address of all of the FortiGate-500 interfaces changes to 00-09-0f-06-ff-3f. You need to wait for the management computer’s ARP table to be updated with this new MAC address before you can re-connect to the FortiGate unit. You can manually delete the address of the FortiGate-500 interface from the management computer’s ARP table to be able to re-connect more quickly. From a command or terminal window you can use the `arp -d` command to delete ARP table entries.

**Figure 7: Example active-active HA configuration**

Standalone Mode  
 High Availability

Cluster Members  
 Mode: Active-Active (dropdown)  
 Group ID: 63 (0-63)  
 Unit Priority: 128 (0-255)  
 (The unit with the highest priority will be HA master.)  
 Override master:  Enable  
 Password: \*\*\*\*\*  
 Retype Password: \*\*\*\*\*  
 Schedule: Round-Robin (dropdown)

Interface	Priorities of Heartbeat Device (0-512)	Monitor Priorities (0-512)
internal		
external		
dmz		
ha	100	
port1	50	
port2		
port3		
port4		
port5		
port6		
port7		
port8		

Apply

- 5 Power off the FortiGate unit.
- 6 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.
  - Connect the Port 1 interfaces of the FortiGate units to each other using a cross-over cable.
- 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.

#### To add basic configuration settings to the cluster

Use the following steps to 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.
- 4 Go to **System > Admin > Administrators**.
  - For admin, select Change password.
  - Enter and confirm a new password.
- 5 Select OK.
- 6 Go to **System > Network > Interface**.
  - For internal, select Edit.
  - Change the IP/Netmask to 192.168.20.93/24.
- 7 Select OK.
  - For external, select Edit.
  - Change the IP/Netmask to 64.29.46.67/24.
- 8 Select OK.
- 9 Go to **Router > Static**.
  - Edit the default route.

<b>Destination IP/Mask</b>	0.0.0.0/0.0.0.0
<b>Gateway</b>	64.29.46.1
<b>Device</b>	external
<b>Distance</b>	10

- 10 Select OK.

## CLI configuration steps

Use the following procedures to configure the FortiGate-500 units for NAT/Route HA operation from the FortiGate unit CLI.

### 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.

```
Bits per second 9600
Data bits       8
Parity          None
Stop bits       1
Flow control    None
```

- 6 Press Enter to connect to the FortiGate CLI.  
The following prompt appears:  
FortiGate-500 login:
- 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 FortiGate unit in the cluster a unique host name to make the individual units easier to identify when they are part of a functioning cluster.

- 9 Configure HA settings.

```
config system ha
    set mode a-a
    set groupid 63
    set password ha500pswd
    set schedule round-robin
end
```



**Note:** You can accept default values for unit priority, override master, priorities of heartbeat devices, monitor priorities and other HA settings.

The FortiGate unit negotiates to establish an HA cluster.

- 10 Display the HA configuration (optional).

```
get system ha
groupid           : 63
mode              : a-a
override          : disable
password          : *
priority          : 128
schedule          : round-robin
monitor           :
hbdev             : ha 100 port1 50
route-ttl         : 0
```

```

route-wait          : 0
route-hold          : 10
encryption          : disable
authentication      : disable
hb-interval         : 4
hb-lost-threshold   : 6
helo-holddown       : 20
arps                : 3
load-balance-all   : disable

```

- 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 47](#).
- 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 add basic configuration settings to the cluster

Use the following steps 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 FortiGate 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 last line of the command output is the following, you have connected to the primary unit:  
Current HA status: mode=a-a, idx=0
  - If the value of `idx` is a number greater than 0, you have logged into a subordinate unit.
  - Connect to another FortiGate unit in the cluster and repeat until you have connected to the primary unit.
- 2 Add a password for the admin administrative account.

```

config system admin
  edit admin
    set password <psswr>
  end

```

- 3 Configure the internal interface.

```

config system interface
  edit internal
    set ip 192.168.20.93/24
  end

```

**4** Configure the external interface.

```
config system interface
  edit external
    set ip 64.29.46.67/24
  end
```

**5** Add a default route.

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 64.29.46.1
    set device external
  end
```

## Basic Transparent mode installation

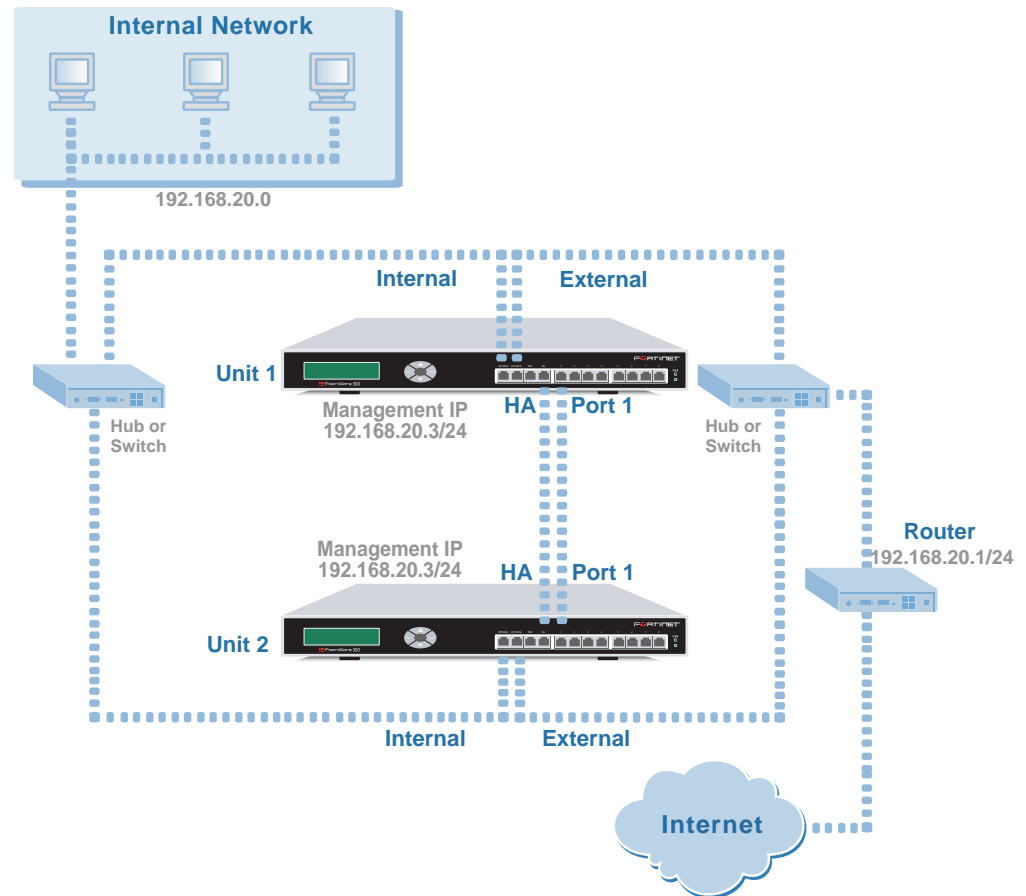
This example describes a simple HA network topology that includes an HA cluster of two FortiGate-500 units installed between an internal network and the Internet and running in Transparent mode. The example includes web-based manager and CLI procedures.

- [Example Transparent mode HA network topology](#)
- [General configuration steps](#)
- [Web-based manager configuration steps](#)
- [CLI configuration steps](#)

## Example Transparent mode HA network topology

[Figure 8](#) shows a typical FortiGate-500 HA cluster consisting of two FortiGate-500 units (Unit 1 and Unit 2) connected to the same internal and external networks.

Figure 8: Transparent mode HA network topology



The default FortiGate-500 Priorities of Heartbeat Device configuration sets the heartbeat device priority of the HA interface to 100 and Port 1 to 50. As a result, in addition to connecting the FortiGate-500 units to their networks, this example describes connecting together the FortiGate-500 HA interfaces and Port 1 interfaces (as shown in [Figure 8](#)). Because the cluster consists of two FortiGate units, you can make the connections between the HA interfaces and between the Port 1 interfaces using crossover cables. You could also use switches as shown for the internal and external interfaces.

## General configuration steps

This section describes how to configure an active-active HA cluster to run in Transparent mode using the topology shown in [Figure 8](#). These procedures assume the FortiGate-500 units are running FortiOS v2.80 MR3 firmware and set to the factory default configuration.

- 1 Configure the FortiGate unit for HA operation.
- 2 Change to Transparent mode.



**Note:** The host name is reset to the default host name after a FortiGate unit switches to Transparent mode. You can change the host name of the FortiGate units after the cluster is running.

- 3 Connect the cluster to the network.
- 4 Add basic configuration settings to the cluster.
  - Add a password for the admin administrative account
  - Change management IP address
  - Add a default route

## Web-based manager configuration steps

Use the following procedures to configure the FortiGate-300 units for Transparent mode HA operation from the FortiGate web-based manager.

### To configure HA settings

- 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.
- 5 Go to **System > Config > HA**.
- 6 Select High Availability.
- 7 Configure HA settings.

<b>Mode</b>	Active-Active
<b>GroupID</b>	63
<b>Unit Priority</b>	128 (Keep the default setting).
<b>Override master</b>	Keep the default setting.
<b>Password</b>	ha500pswd
<b>Retype Password</b>	ha500pswd
<b>Schedule</b>	Round-Robin
<b>Priorities of Heartbeat Device</b>	Keep the default setting.
<b>Monitor Priorities</b>	Keep the default setting.



**Note:** You can change the Priorities or Heartbeat Device and Monitor priorities when the cluster is operating.

**8** Select Apply.

The FortiGate unit negotiates to establish an HA cluster. When you select apply you temporarily lose connectivity with the FortiGate unit because the HA cluster negotiates to select the primary unit. Also, the MAC address of all of the FortiGate unit interfaces change. See [“Group ID” on page 27](#).

In this example, the MAC address of all of the FortiGate-500 interfaces changes to 00-09-0f-06-ff-3f. You need to wait for the management computer’s ARP table to be updated with this new MAC address before you can re-connect to the FortiGate unit. You can manually delete the address of the FortiGate-500 interface from the management computer’s ARP table to be able to re-connect more quickly. From a command or terminal window you can use the `arp -d` command to delete ARP table entries.

**To change to Transparent mode**

- 1 Reconnect to the web-based manager.
- 2 Go to **System > Status**.
- 3 Beside Operation Mode select Change.
- 4 For Operation Mode, select Transparent and select OK.
- 5 Allow the FortiGate unit to restart in Transparent Mode and then turn off the power.
- 6 Repeat these steps for all of the cluster units.

**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.
  - Connect the Port 1 interfaces of the FortiGate units to each other using a cross-over cable.
- 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 add basic configuration settings to the cluster**

Use the following steps 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 From a management computer connected to your internal network, change the IP address of the management computer to the static IP address 10.10.10.2 and a netmask of 255.255.255.0.
  - 2 Start Internet Explorer and browse to the address `https://10.10.10.1` (remember to include the “s” in `https://`).
- The FortiGate Login is displayed.

- 3 Type `admin` in the Name field and select Login.
- 4 Go to **System > Admin > Administrators**.
  - For admin, select Change password.
  - Enter and confirm a new password.
- 5 Select OK.
- 6 Go to **System > Network > Management**.

<b>Management IP/Netmask</b>	192.168.20.3
<b>Default Gateway</b>	192.168.20.1
<b>Management virtual domain</b>	root (Keep the default setting.)

- 7 Select OK.

## CLI configuration steps

Use the following procedures to configure the FortiGate-300 units for Transparent mode HA operation from the FortiGate CLI.

### To configure each FortiGate unit for Transparent 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.

```
Bits per second 9600
Data bits       8
Parity          None
Stop bits       1
Flow control    None
```

- 6 Press Enter to connect to the FortiGate CLI.  
The following prompt appears:  
FortiGate-500 login:
- 7 Type `admin` and press Enter twice.
- 8 Configure HA settings.

```
config system ha
  set mode a-a
  set groupid 63
  set password ha500pswd
  set schedule round-robin
end
```



**Note:** You can accept default values for unit priority, override master, heartbeat device priority, monitor priority and other HA settings.

The FortiGate unit negotiates to establish an HA cluster.

**9** Display the HA configuration (optional).

```
get system ha
  groupid           : 63
  mode              : a-a
  override          : disable
  password          : *
  priority          : 128
  schedule          : round-robin
  monitor           :
  hbdev             : ha 100 port1 50
  route-ttl         : 0
  route-wait        : 0
  route-hold        : 10
  encryption        : disable
  authentication    : disable
  hb-interval       : 4
  hb-lost-threshold : 6
  helo-holddown     : 20
  arps              : 3
  load-balance-all : disable
```

**10** Change to transparent mode.

```
config system global
  set opmode transparent
end
```

The FortiGate unit restarts. After a few seconds, the login prompt appears.

**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 54](#).

**2** Power on all of the HA units in the cluster.

As the units power on they negotiate to choose the primary unit and the subordinate units. This negotiation occurs with no user intervention.

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

### To add basic configuration settings to the cluster

Use the following steps 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 FortiGate 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 last line of the command output is the following, you have connected to the primary unit:  

```
Current HA status: mode=a-a, idx=0
```
  - If the value of `idx` is a number greater than 0, you have logged into a subordinate unit.
  - Connect to another FortiGate unit in the cluster and repeat until you have connected to the primary unit.

- 2 Add a password for the admin administrative account.

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

- 3 Change the management interface IP address.

```
config system manageip
  set ip 192.168.20.3/24
end
```

- 4 Add a default route.

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.20.1
  end
```

## Converting a standalone FortiGate unit to a cluster

This example describes how to convert an already configured and installed FortiGate unit into a cluster by changing this FortiGate unit into a primary unit and adding subordinate units.

Use the following 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.

<b>Mode</b>	Active-Active
<b>GroupID</b>	34
<b>Unit Priority</b>	255 (Set a high priority so that this unit becomes the primary unit.)
<b>Override master</b>	Keep the default setting.
<b>Password</b>	ha500pswd
<b>Retype Password</b>	ha500pswd
<b>Schedule</b>	Round-Robin
<b>Priorities of Heartbeat Device</b>	Keep the default setting.
<b>Monitor Priorities</b>	Keep the default setting.

- 4 Select Apply  
When the FortiGate unit changes its MAC addresses and attempts to negotiate a cluster, a short service interruption occurs.
- 5 Configure the new cluster units with the same HA configuration as the original FortiGate unit with one exception. Do not change the unit priority.

<b>Mode</b>	Active-Active
<b>GroupID</b>	34
<b>Unit Priority</b>	128 (Keep the default setting.)
<b>Override master</b>	Keep the default setting.
<b>Password</b>	ha500pswd
<b>Retype Password</b>	ha500pswd
<b>Schedule</b>	Round-Robin
<b>Priorities of Heartbeat Device</b>	Keep the default setting.
<b>Monitor Priorities</b>	Keep the default setting.

- 6 If the original FortiGate unit was operating in Transparent mode, switch the new FortiGate units to Transparent mode.
- 7 Power off all FortiGate units including the original FortiGate unit.
- 8 Connect the cluster to your network.  
For example, for the FortiGate-500 cluster configurations described in this chapter:
  - 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 cross-over cables or a switch or hub.
  - Connect the Port 1 interfaces of the FortiGate units to each other using cross-over cables or a switch or hub.
- 9 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 unit. This negotiation occurs with no user intervention.  
When negotiation is complete the cluster is configured for your network and no further configuration changes are required.

## Adding a new unit to an operating cluster

This example describes how to add a new FortiGate unit to an operating HA cluster without interrupting network traffic. The new FortiGate 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 FortiOS v2.80 firmware build as the cluster.



**Note:** If the new cluster unit is running an older firmware build than what is running on the cluster, re-installing the current firmware build on the cluster 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, to add a new unit to the FortiGate-500 cluster shown in [Figure 6](#) or [Figure 7](#):
  - Connect the internal interface to the same switch or hub as the cluster internal interfaces.
  - Connect the external interface to the same switch or hub as the cluster external interfaces.
  - Connect the HA interface to the same switch or hub as the cluster HA interfaces.  
If you are adding a third unit to the cluster you may have to replace a cross-over cable with a hub or switch and connect all of the HA interfaces to this hub or switch.
  - Connect the Port 1 interface to the same switch or hub as the cluster Port 1 interfaces.  
If you are adding a third unit to the cluster you may have to replace another crossover cable with a hub or switch and connect all of the Port 1 interfaces to this hub or switch.
- 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.

## Customizing primary unit selection

This configuration example describes how to configure a cluster of three FortiGate-60 units named FGT-60\_A, FGT-60\_B, and FGT-60\_C. In this cluster, the FortiGate-60 units are operating in NAT/Route mode and the internal, external, and DMZ interfaces are connected to networks. The cluster is configured so that:

- FGT-60\_A always operates as the primary unit
- If FGT-60\_A fails, FGT-60\_B becomes the primary unit
- If the failed FGT-60\_A is restored and added back into the cluster, FGT-60\_A once again becomes the primary unit
- The WAN2 interface is the primary heartbeat device
- The DMZ and WAN1 interfaces are backup heartbeat devices

To configure the cluster so that FGT-60\_A always becomes the primary unit, set the unit priorities so that FGT-60\_A has the highest unit priority, FGT-60\_B has the second highest unit priority and FGT-60\_C has the lowest unit priority. Even with unit priorities set in this manner, FGT-60\_B may not always become the primary unit if FGT\_60\_A fails. To make sure the cluster negotiates as expected you should also enable override master for all cluster units. The combination of setting unit priorities and enabling override master makes sure cluster negotiation occurs as planned.

This example configuration describes:

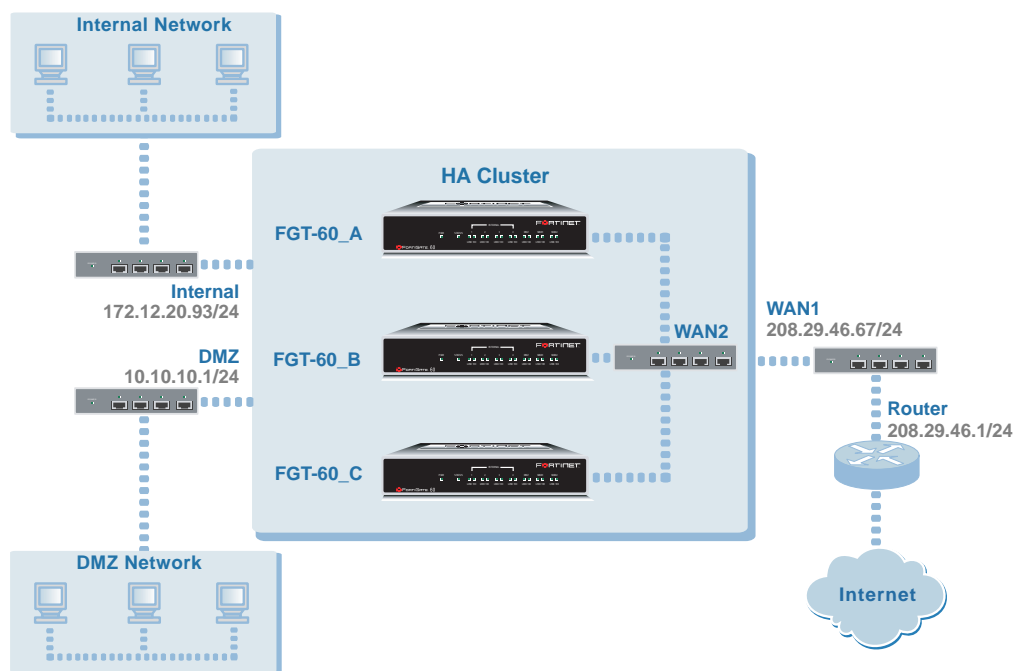
- [Network topology](#)
- [General configuration steps](#)
- [Web-based manager configuration steps](#)
- [CLI configuration steps](#)
- [Testing failover](#)

## Network topology

Figure 6 shows the cluster of three FortiGate-60 units.

- Connect the internal interfaces of all three FortiGate-60 units to a switch and connect the switch to the internal network.
- Connect the WAN1 interfaces of all three FortiGate-60 units to a switch and connect the switch to the external network.
- Connect the DMZ interfaces of all three FortiGate-60 units to a switch and connect the switch to the DMZ network.
- Connect the WAN2 interfaces of all three FortiGate-60 units to a switch for HA heartbeat traffic.

Figure 9: FortiGate-60 cluster network topology



## General configuration steps

This section describes how to configure an active-passive HA cluster to run in NAT/Route mode using the topology shown in Figure 9. These procedures assume that the FortiGate-60 units are running the same v2.80 firmware build and are set to the factory default configuration.

1. Configure FGT-60\_A.
  - Set the host name to FGT-60\_A.
  - Configure HA settings as shown in Table 6.

Table 6: FGT-60\_A configuration

HA Option	Setting		Description
<b>Mode</b>	Active-Passive		All cluster units must operate in the same HA mode.
<b>Group ID</b>	25		All cluster units must have the same group ID.
<b>Unit Priority</b>	200		Set the FGT-60_A unit priority higher than for the other units in the cluster.
<b>Override master</b>	Enable		Enable override master so that FGT-60_A always becomes the primary unit.
<b>Password</b>	ha60pswd		All cluster units must have the same password.
<b>Priorities of Heartbeat Device</b>	internal		The HA heartbeat uses WAN2.
	wan1	25	If WAN2 fails or is disconnected, DMZ becomes the heartbeat device.
	wan2	100	If the DMZ interface fails or is disconnected, WAN1 becomes the heartbeat device.
	dmz	50	
<b>Monitor Priorities</b>	No change.		Configure monitor priorities after the cluster is operating.

- 2 Configure FGT-60\_B.
  - Set the host name to FGT-60\_B.
  - Configure HA settings as shown in [Table 7](#).

Table 7: FGT-60\_B configuration

HA Option	Setting		Description
<b>Mode</b>	Active-Passive		All cluster units must operate in the same HA mode.
<b>Group ID</b>	25		All cluster units must have the same group ID.
<b>Unit Priority</b>	100		Set the FGT-60_B unit priority between the unit priority of the FGT-60_A and the FGT-60_B.
<b>Override master</b>	Enable		Enable override master so that FGT-60_B always becomes the primary unit of FGT-60_A fails.
<b>Password</b>	ha60pswd		All cluster units must have the same password.
<b>Priorities of Heartbeat Device</b>	No change.		Because FGT-60_A becomes the primary unit, the priorities of heartbeat device configuration of FGT-60_A is synchronized to all cluster units after the cluster is operating.
<b>Monitor Priorities</b>	No change.		Configure monitor priorities after the cluster is operating.

- 3 Configure FGT-60\_B.
  - Set the host name to FGT-60\_C.
  - Configure HA settings as shown in [Table 8](#).

Table 8: FGT-60\_B configuration

HA Option	Setting	Description
<b>Mode</b>	Active-Passive	All cluster units must operate in the same HA mode.
<b>Group ID</b>	25	All cluster units must have the same group ID.
<b>Unit Priority</b>	50	Set the FGT-60_C unit priority to be lower than the unit priorities of FGT-60_A and FGT-60_B.
<b>Override master</b>	Enable	Enable override master so that the cluster negotiates as planned.
<b>Password</b>	ha60pswd	All cluster units must have the same password.
<b>Priorities of Heartbeat Device</b>	No change.	Because FGT-60_A becomes the primary unit, the priorities of heartbeat device configuration of FGT-60_A is synchronized to all cluster units after the cluster is operating.
<b>Monitor Priorities</b>	No change.	Configure monitor priorities after the cluster is running.

- 4 Connect the cluster to the network.
- 5 Add basic configuration settings to the cluster.
  - 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-60 units from the FortiGate web-based manager.

- [To configure FGT-60\\_A](#)
- [To configure FGT-60\\_B](#)
- [To configure FGT-60\\_C](#)

### To configure FGT-60\_A

- 1 Power on the FortiGate unit and log into the web-based manager.
- 2 Go to **System > Status**.
- 3 Beside Host Name select Change and set host name to FGT-60\_A.
- 4 Select OK.
- 5 Go to **System > Config > HA**.
- 6 Select High Availability.
- 7 Configure HA settings for FGT-60\_A:

<b>Mode</b>	Active-Passive	
<b>Group ID</b>	25	
<b>Unit Priority</b>	200	
<b>Override master</b>	Enable	
<b>Password</b>	ha60pswd	
<b>Retype Password</b>	ha60pswd	
<b>Priorities of Heartbeat Device</b>	<b>internal</b>	
	<b>wan1</b>	25
	<b>wan2</b>	100
	<b>dmz</b>	50
<b>Monitor Priorities</b>	Keep the default setting.	

**8** Select Apply.

The FortiGate unit negotiates to establish an HA cluster. When you select apply you temporarily lose connectivity with the FortiGate unit because the HA cluster negotiates to select the primary unit. Also, the MAC address of all of the FortiGate unit interfaces changes. See “Group ID” on page 27.

In this example, the MAC address of all of the FortiGate-60 interfaces changes to 00-09-0f-06-ff-19. You need to wait for the management computer’s ARP table to be updated with this new MAC address before you can re-connect to the FortiGate unit. To be able to re-connect more quickly, you can manually delete the FortiGate unit MAC address from the management computer’s ARP table. From a command or terminal window you can use the `arp -d` command to delete ARP table entries.

**Figure 10: FGT-60\_A HA configuration**

**9** Power off FGT-60\_A.

**To configure FGT-60\_B**

- 1** Power on the FortiGate unit and log into the web-based manager.
- 2** Go to **System > Status**.

- 3 Beside Host Name select Change and set host name to FGT-60\_B.
- 4 Select OK.
- 5 Go to **System > Config > HA**.
- 6 Select High Availability.
- 7 Configure HA settings for FGT-60\_B:

<b>Mode</b>	Active-Passive
<b>Group ID</b>	25
<b>Unit Priority</b>	100
<b>Override master</b>	Enable
<b>Password</b>	ha60pswd
<b>Retype Password</b>	ha60pswd
<b>Priorities of Heartbeat Device</b>	Keep the default setting.
<b>Monitor Priorities</b>	Keep the default setting.

- 8 Select Apply.  
 The FortiGate unit negotiates to establish an HA cluster. When you select apply you temporarily lose connectivity with the FortiGate unit because the HA cluster negotiates to select the primary unit. Also, the MAC address of all of the FortiGate unit interfaces change. See [“Group ID” on page 27](#).

In this example, the MAC address of all of the FortiGate-60 interfaces changes to 00-09-0f-06-ff-19. You need to wait for the management computer’s ARP table to be updated with this new MAC address before you can re-connect to the FortiGate unit. To be able to re-connect more quickly, you can manually delete the FortiGate unit MAC address from the management computer’s ARP table. From a command or terminal window you can use the `arp -d` command to delete ARP table entries.

**Figure 11: FGT-60\_B HA configuration**

The screenshot shows the FortiGate HA configuration page. The 'High Availability' radio button is selected. The 'Mode' is set to 'Active-Passive'. The 'Group ID' is 25 and 'Unit Priority' is 100. The 'Override master' checkbox is checked and labeled 'Enable'. Password fields are filled with asterisks. Below is a table for interface priorities:

Interface	Priorities of Heartbeat Device (0-512)	Monitor Priorities (0-512)
internal		
wan1		
wan2		
dmz		

An 'Apply' button is located at the bottom of the configuration area.

- 9 Power off FGT-60\_B.

**To configure FGT-60\_C**

- 1 Power on the FortiGate unit and log into the web-based manager.
- 2 Go to **System > Status**.
- 3 Beside Host Name select Change and set host name to FGT-60\_C.
- 4 Select OK.
- 5 Go to **System > Config > HA**.
- 6 Select High Availability.
- 7 Configure HA settings for FGT-60\_C:

<b>Mode</b>	Active-Passive
<b>Group ID</b>	25
<b>Unit Priority</b>	50
<b>Override master</b>	Enable
<b>Password</b>	ha60pswd
<b>Retype Password</b>	ha60pswd
<b>Priorities of Heartbeat Device</b>	Keep the default setting.
<b>Monitor Priorities</b>	Keep the default setting.

- 8 Select Apply.  
 The FortiGate unit negotiates to establish an HA cluster. When you select apply you temporarily lose connectivity with the FortiGate unit because the HA cluster negotiates to select the primary unit. Also, the MAC address of all of the FortiGate unit interfaces change. See ["Group ID" on page 27](#).  
 In this example, the MAC address of all of the FortiGate-60 interfaces changes to 00-09-0f-06-ff-19. You need to wait for the management computer's ARP table to be updated with this new MAC address before you can re-connect to the FortiGate unit. To be able to re-connect more quickly, you can manually delete the FortiGate unit MAC address from the management computer's ARP table. From a command or terminal window you can use the `arp -d` command to delete ARP table entries.

**Figure 12: FGT-60\_C HA configuration**

Interface	Priorities of Heartbeat Device (0-512)	Monitor Priorities (0-512)
internal		
wan1		
wan2		
dmz		

9 Power off FGT-60\_C.

**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 WAN1 interfaces of each FortiGate unit to a switch or hub connected to the external network.
- Connect the DMZ interfaces of each FortiGate unit to a switch or hub connected to the DMZ network.
- Connect the WAN2 interfaces of each FortiGate unit to a switch or hub.

2 Power on all of the cluster units.

The units start and negotiate to choose FGT-60\_A as the primary unit. This negotiation occurs with no user intervention.

**To add basic configuration settings to the cluster**

Use the following steps to 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.
- 4 Go to **System > Admin > Administrators**.
  - For admin, select Change password.
  - Enter and confirm a new password.
- 5 Select OK.
- 6 Go to **System > Network > Interface**.
  - For internal, select Edit.
  - Change the IP/Netmask to 172.12.20.93/24.
- 7 Select OK.
  - For WAN1, select Edit.
  - Change the IP/Netmask to 208.29.46.67/24.
- 8 Select OK.
  - For DMZ, select Edit.
  - Change the IP/Netmask to 10.10.10.1/24.
- 9 Select OK.
- 10 Go to **Router > Static**.
  - Edit the default route.

<b>Destination IP/Mask</b>	0.0.0.0/0.0.0.0
<b>Gateway</b>	208.29.46.1
<b>Device</b>	wan1
<b>Distance</b>	10

- 11 Select OK.

## CLI configuration steps

Use the following procedures to configure the FortiGate-60 units from the FortiGate CLI.

- [To configure FGT-60\\_A](#)
- [To configure FGT-60\\_B](#)
- [To configure FGT-60\\_C](#)

### To configure FGT-60\_A

- 1 Power on the FortiGate unit and log into the CLI.
- 2 Change the host name. Enter:
 

```
config system global
  set hostname FGT-60_A
end
```
- 3 Configure HA settings.

```
config system ha
  set mode a-p
  set groupid 25
  set priority 200
  set override enable
  set password ha60pswd
  set hbdev wan1 25 wan2 100 dmz 50
end
```



**Note:** You can accept default values for other HA settings.

The FortiGate unit negotiates to establish an HA cluster.

**4** Display the HA configuration (optional).

```
get system ha
  groupid           : 25
  mode              : a-p
  override          : enable
  password          : *
  priority          : 200
  schedule          : round-robin
  monitor           :
  hbdev             : wan1 25 wan2 100 dmz 50
  route-ttl        : 0
  route-wait       : 0
  route-hold       : 10
  encryption       : disable
  authentication   : disable
  hb-interval      : 2
  hb-lost-threshold : 6
  helo-holddown    : 20
  arps             : 3
```

**To configure FGT-60\_B**

**1** Power on the FortiGate unit and log into the CLI.

**2** Change the host name. Enter:

```
config system global
  set hostname FGT-60_B
end
```

**3** Configure HA settings.

```
config system ha
  set mode a-p
  set groupid 25
  set priority 100
  set override enable
end
```



**Note:** You can accept default values for other HA settings.

The FortiGate unit negotiates to establish an HA cluster.

**4** Display the HA configuration (optional).

```
get system ha
  groupid           : 25
  mode              : a-p
  override          : enable
  password          : *
  priority          : 100
  schedule          : round-robin
  monitor           :
  hbdev             : dmz 100 wan1 50
  route-ttl         : 0
  route-wait        : 0
  route-hold        : 10
  encryption        : disable
  authentication    : disable
  hb-interval        : 2
  hb-lost-threshold : 6
  helo-holddown     : 20
  arps              : 3
```

**To configure FGT-60\_C**

**1** Power on the FortiGate unit and log into the CLI.

**2** Change the host name. Enter:

```
config system global
  set hostname FGT-60_A
end
```

**3** Configure HA settings.

```
config system ha
  set mode a-p
  set groupid 25
  set priority 50
  set override enable
end
```



**Note:** You can accept default values for other HA settings.

The FortiGate unit negotiates to establish an HA cluster.

**4** Display the HA configuration (optional).

```
get system ha
  groupid           : 25
```

```
mode                : a-p
override            : enable
password            : *
priority            : 50
schedule            : round-robin
monitor             :
hbdev               : dmz 100 wan1 50
route-ttl           : 0
route-wait          : 0
route-hold          : 10
encryption          : disable
authentication      : disable
hb-interval         : 2
hb-lost-threshold  : 6
helo-holddown      : 20
arps                : 3
```

### To connect the cluster to the network

- 1 Connect the cluster units using the procedure [“To connect the cluster to the network” on page 68](#).
- 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 add basic configuration settings to the cluster

Use the following steps 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 Connect to the primary unit CLI by connecting to the FGT-60\_A console port.
- 2 Add a password for the admin administrative account.

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

- 3 Configure the internal interface.

```
config system interface
  edit internal
    set ip 172.12.20.93/24
  end
```

- 4 Configure the DMZ interface.

```
config system interface
  edit dmz
    set ip 10.10.10.1/24
  end
```

5 Configure the WAN1 interface.

```
config system interface
  edit wan1
    set ip 208.29.46.67/24
  end
```

6 Add a default route.

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 208.29.46.1
    set device external
  end
```

## Testing failover

When the example FortiGate-60 cluster is up and running, FGT-60\_A will always be the primary unit. [Figure 13](#) shows a sample cluster members list for this cluster. Go to **System > Config > HA** and select Cluster Members to view the cluster members list. [Figure 13](#) shows the cluster units listed in order of unit priority.

In [Figure 13](#):

- FGT-60\_A has cluster ID FGT-602104400533 (primary unit, unit priority 200)
- FGT-60\_B has cluster ID FGT-602803030702 (unit priority 100)
- FGT-60\_C has cluster ID FGT-602104400531 (unit priority 50)

**Figure 13: Cluster members list, all cluster units operating**

Cluster ID	Status	Up Time	Monitor			
FGT-602104400533	✔	0 days 0 hours 8 minutes 59 seconds	CPU Usage 6%	Active Sessions 16	Total Packets 1337	Virus Detected 0
			Memory Usage 60%	Network Utilization 11 Kbps	Total Bytes 565170	Intrusion Detected 0
FGT-602803030702	✔	0 days 0 hours 9 minutes 19 seconds	CPU Usage 9%	Active Sessions 7	Total Packets 55	Virus Detected 0
			Memory Usage 55%	Network Utilization 15 Kbps	Total Bytes 8058	Intrusion Detected 0
FGT-602104400531	✔	0 days 0 hours 8 minutes 23 seconds	CPU Usage 0%	Active Sessions 6	Total Packets 23	Virus Detected 0
			Memory Usage 55%	Network Utilization 10 Kbps	Total Bytes 4956	Intrusion Detected 0

## If the primary unit fails

If the primary unit fails, the remaining cluster units renegotiate and FGT-60\_B (ID FGT-602104400531) becomes the primary unit as shown in [Figure 14](#).

In [Figure 14](#):

- FGT-60\_B has cluster ID FGT-602803030702 (primary unit, unit priority 100)
- FGT-60\_C has cluster ID FGT-602104400531 (unit priority 50)

**Figure 14: Cluster members list, primary unit failed**

Cluster ID	Status	Up Time	Monitor			
FGT-602803030702	Up	0 days 0 hours 10 minutes 46 seconds	CPU Usage 0%	Active Sessions 17	Total Packets 733	Virus Detected 0
			Memory Usage 59%	Network Utilization 11 Kbps	Total Bytes 237662	Intrusion Detected 0
FGT-602104400531	Up	0 days 0 hours 9 minutes 53 seconds	CPU Usage 0%	Active Sessions 7	Total Packets 29	Virus Detected 0
			Memory Usage 56%	Network Utilization 13 Kbps	Total Bytes 6354	Intrusion Detected 0

## If the primary unit is restored

If the primary unit is restored to the cluster, the cluster renegotiates and FGT-60\_A once again becomes the primary unit. In [Figure 15](#) the up time for FGT-60\_A is shorter than that for the other FortiGate units, indicating that it has just joined the cluster.

[Figure 15](#) also shows that right after FGT-60\_A rejoins the cluster, FGT-60\_C and FGT-60\_B are not in the expected priority order in the cluster. When FGT-60\_A rejoined the cluster, FGT-60\_B was forced to leave and then rejoin the cluster. As a result the age of FGT-60\_C in the cluster is greater than the age of FGT-60\_B, so FGT-60\_B has a lower priority.

In [Figure 15](#):

- FGT-60\_A has cluster ID FGT-602104400533 (primary unit, unit priority 200)
- FGT-60\_C has cluster ID FGT-602104400531 (unit priority 50)
- FGT-60\_B has cluster ID FGT-602803030702 (unit priority 100)

**Figure 15: Cluster members list, primary unit has rejoined cluster**

Refresh every		10 seconds	Go	<a href="#">Back to HA configuration page &gt;&gt;</a>			
Cluster ID	Status	Up Time	Monitor				
FGT-602104400533	✔	0 days 0 hours 4 minutes 36 seconds	CPU Usage 0%	Active Sessions 16	Total Packets 1711	Virus Detected 0	
			Memory Usage 60%	Network Utilization 11 Kbps	Total Bytes 521002	Intrusion Detected 0	
FGT-602104400531	✔	0 days 0 hours 16 minutes 23 seconds	CPU Usage 0%	Active Sessions 4	Total Packets 65	Virus Detected 0	
			Memory Usage 55%	Network Utilization 10 Kbps	Total Bytes 12617	Intrusion Detected 0	
FGT-602803030702	✔	0 days 0 hours 17 minutes 16 seconds	CPU Usage 0%	Active Sessions 7	Total Packets 1882	Virus Detected 0	
			Memory Usage 57%	Network Utilization 10 Kbps	Total Bytes 610315	Intrusion Detected 0	

### Resetting the priority order

After a few minutes the cluster recognizes that FGT-60\_B should have a higher priority in the cluster than FGT-60\_C. The cluster restarts FGT-60\_B and FGT-60\_C. For a short time, only FGT-60\_A appears in the cluster members list. FGT-60\_B and FGT-60\_C renegotiate and rejoin the cluster in the expected priority order as shown in [Figure 16](#). The required for this process varies depending on the cluster configuration and other factors. During this checking and renegotiation cluster traffic is maintained by the primary unit.

In [Figure 16](#):

- FGT-60\_A has cluster ID FGT-602104400533 (primary unit, unit priority 200)
- FGT-60\_B has cluster ID FGT-602803030702 (unit priority 100)
- FGT-60\_C has cluster ID FGT-602104400531 (unit priority 50)

Figure 16: Cluster members list, primary unit has rejoined cluster

Refresh every		10 seconds	Go	Back to HA configuration page >>			
Cluster ID	Status	Up Time	Monitor				
FGT-602104400533	✔	0 days 0 hours 11 minutes 24 seconds	CPU Usage 2%	Active Sessions 16	Total Packets 4038	Virus Detected 0	
			Memory Usage 60%	Network Utilization 11 Kbps	Total Bytes 1220522	Intrusion Detected 0	
FGT-602803030702	✔	0 days 0 hours 7 minutes 6 seconds	CPU Usage 19%	Active Sessions 4	Total Packets 36	Virus Detected 0	
			Memory Usage 56%	Network Utilization 10 Kbps	Total Bytes 9770	Intrusion Detected 0	
FGT-602104400531	✔	0 days 0 hours 6 minutes 46 seconds	CPU Usage 8%	Active Sessions 7	Total Packets 32	Virus Detected 0	
			Memory Usage 56%	Network Utilization 10 Kbps	Total Bytes 8715	Intrusion Detected 0	

## Configuring monitor priorities for link failover protection

Link failure protection makes sure a cluster can process traffic from a high priority network even if the interface of a cluster unit connected to the high priority network fails or is disconnected. To configure link failure protection, you add monitor priorities to the HA configuration of the cluster. Adding a monitor priority to an interface means that the cluster monitors the interface to make sure that it is connected and operating. If a monitored interface of any cluster unit fails, the monitor priority of that cluster unit changes and the cluster registers this change. If the change in monitor priority reduces the primary unit monitor priority below that of other cluster units, the cluster renegotiates to select a primary unit. The result of the renegotiation could be that the cluster selects a new primary unit based on the changes in the monitor priority of the cluster. See [“Primary unit selection” on page 18](#) for information about how the monitor priority affects primary unit selection.

For a cluster to maintain a connection to a high priority network, the primary unit must have a functioning interface connected to that network. If the primary unit interface to a high priority network fails, the cluster renegotiates to select a primary unit that does have a functioning interface connected to that network.

This configuration example describes how to change the cluster configured in [“Customizing primary unit selection” on page 61](#) to implement link failover protection. This example describes how to configure the cluster so that:

- WAN1 traffic to the external network has the highest priority. Set Monitor priority for WAN1 to a high value so that if the primary unit WAN1 interface fails or is disconnected, the cluster selects a primary unit with an operating and connected WAN1 interface.
- DMZ connections to the DMZ network have a lower priority. Set monitor priority for DMZ to a lower value. Because a monitor priority is set, if the primary unit DMZ interface fails or is disconnected, the cluster selects a primary unit with an operating and connected DMZ interface. However, because the DMZ interface has a lower monitor priority than the WAN1 interface, if a DMZ interface fails on one cluster unit and the WAN1 interface fails on another cluster unit, the cluster unit with the failed DMZ interface becomes the primary unit because it is more important to maintain connections to the WAN1 interface and the external network.
- Do not set monitor priority for the internal interface because the FortiGate-60 internal interface is a switch and you cannot add a monitor priority to a cluster interface that is also a switch.
- Do not set monitor priority for the WAN2 interface because the WAN2 interfaces are not connected to a network. The WAN2 interfaces are heartbeat devices. If the WAN2 interface of one of the cluster units fails or is disconnected, the HA heartbeat is transferred to the next heartbeat device (in this example, the DMZ interface).

This example configuration describes:

- [Web-based manager configuration steps](#)
- [CLI configuration steps](#)
- [Testing failover](#)

## Web-based manager configuration steps

Use the following procedure to add monitor priorities to the cluster configuration from the web-based manager.

### To add monitor priorities to the cluster

- 1 Log into the cluster web-based manager.
- 2 Go to **System > Config > HA**.
- 3 Configure monitor priorities for the cluster.

Monitor Priorities	internal	
	wan1	200
	wan2	
	dmz	100

- 4 Select Apply.  
The cluster synchronizes this configuration change to all cluster units.

**Figure 17: Cluster HA configuration with monitor priorities**

The screenshot shows the FortiGate configuration page for High Availability. The 'High Availability' mode is selected. The 'Cluster Members' section shows 'Active-Passive' mode, Group ID 25, and Unit Priority 200. The 'Override master' checkbox is checked. Below this is a table for 'Monitor Priorities'.

Interface	Priorities of Heartbeat Device (0-512)	Monitor Priorities (0-512)
internal		
wan1	25	200
wan2	100	
dmz	50	100

An 'Apply' button is located at the bottom of the configuration area.

## CLI configuration steps

Use the following procedure to add monitor priorities to the cluster configuration from the CLI.

### To add monitor priorities to the cluster

- 1 Log into the cluster CLI.
- 2 Add monitor priorities to the HA settings.

```
config system ha
    set monitor wan1 200 dmz 100
end
```

The cluster synchronizes this configuration change to all cluster units.

- 3 Display the HA configuration (optional).

```
get system ha
groupid           : 25
mode              : a-p
override          : enable
password          : *
priority          : 200
schedule          : round-robin
monitor           : wan1 200 dmz 100
hbdev             : wan1 25 wan2 100 dmz 50
route-ttl         : 0
route-wait        : 0
route-hold        : 10
encryption        : disable
authentication    : disable
hb-interval       : 2
hb-lost-threshold : 6
helo-holddown     : 20
arps              : 3
```

## Testing failover

When the example FortiGate-60 cluster is up and running, FGT-60\_A will always be the primary unit. [Figure 13 on page 73](#) shows a sample cluster members list for this cluster. Go to **System > Config > HA** and select Cluster Members to view the cluster members list.

Depending on firewall policies, traffic can flow between the internal, external, and DMZ networks.

### FGT-60\_A WAN1 interface disconnected

FGT-60\_A is the primary unit. Disconnecting the primary unit WAN1 interface causes the cluster to re-negotiate. FGT-60\_B becomes the primary unit and FGT-60\_A has the lowest priority in the cluster. The units are ranked in the cluster priority list according to their total monitor priority. The total monitor priority of a cluster unit is the sum of the monitor priorities of all operating and connected interfaces.

In [Figure 18](#):

- FGT-60\_B has cluster ID FGT-602803030702 (primary unit, monitor priority 300, unit priority 100)
- FGT-60\_C has cluster ID FGT-602104400531 (monitor priority 300, unit priority 50)
- FGT-60\_A has cluster ID FGT-602104400533 (monitor priority 100, unit priority 200)

Depending on firewall policies, traffic can still flow between the internal, external, and DMZ networks.

**Figure 18: Cluster members list, primary unit WAN1 interface disconnected**

Refresh every 10 seconds <a href="#">Go</a> <a href="#">Back to HA configuration page &gt;&gt;</a>						
Cluster ID	Status	Up Time	Monitor			
FGT-602803030702	✔	0 days 1 hours 8 minutes 42 seconds	CPU Usage 0%	Active Sessions 17	Total Packets 2514	Virus Detected 0
			Memory Usage 60%	Network Utilization 17 Kbps	Total Bytes 922536	Intrusion Detected 0
FGT-602104400531	✔	0 days 1 hours 0 minutes 21 seconds	CPU Usage 0%	Active Sessions 6	Total Packets 99	Virus Detected 0
			Memory Usage 56%	Network Utilization 15 Kbps	Total Bytes 14412	Intrusion Detected 0
FGT-602104400533	✔	0 days 0 hours 12 minutes 52 seconds	CPU Usage 0%	Active Sessions 5	Total Packets 2442	Virus Detected 0
			Memory Usage 57%	Network Utilization 15 Kbps	Total Bytes 1071019	Intrusion Detected 0

**FGT-60\_A and FGT-60\_B WAN1 interfaces disconnected**

Disconnecting the FGT-60\_A and FGT-60\_B WAN1 interfaces causes the cluster to re-negotiate. FGT-60\_C becomes the primary unit and FGT-60\_B has the lowest priority in the cluster.

In [Figure 19](#):

- FGT-60\_C has cluster ID FGT-602104400531 (primary unit, monitor priority 300, unit priority 50)
- FGT-60\_A has cluster ID FGT-602104400533 (monitor priority 100, unit priority 200)
- FGT-60\_B has cluster ID FGT-602803030702 (monitor priority 100, unit priority 100)

Depending on firewall policies, traffic can still flow between the internal, external, and DMZ networks.

**Figure 19: Cluster members list, FGT-60-A and FGT-60\_B WAN1 interfaces disconnected**

Refresh every 10 seconds		Go		Back to HA configuration page >>			
Cluster ID	Status	Up Time	Monitor				
FGT-602104400531	✔	0 days 1 hours 32 minutes 51 seconds	CPU Usage 8%	Active Sessions 9	Total Packets 7129	Virus Detected 0	
			Memory Usage 59%	Network Utilization 85 Kbps	Total Bytes 2278664	Intrusion Detected 0	
FGT-602104400533	✔	0 days 0 hours 45 minutes 22 seconds	CPU Usage 3%	Active Sessions 3	Total Packets 2497	Virus Detected 0	
			Memory Usage 57%	Network Utilization 24 Kbps	Total Bytes 1087094	Intrusion Detected 0	
FGT-602803030702	✔	0 days 1 hours 41 minutes 13 seconds	CPU Usage 8%	Active Sessions 1	Total Packets 5964	Virus Detected 0	
			Memory Usage 57%	Network Utilization 15 Kbps	Total Bytes 1971992	Intrusion Detected 0	

### FGT-60\_C DMZ interface disconnected

Disconnecting the FGT\_60\_C DMZ interface in addition to the FGT-60\_A and FGT-60\_B WAN1 interfaces does not cause the cluster to re-negotiate. FGT-60\_C remains the primary unit and FGT-60\_B has the lowest priority in the cluster.

- FGT-60\_C has cluster ID FGT-602104400531 (primary unit, monitor priority 200, unit priority 50)
- FGT-60\_A has cluster ID FGT-602104400533 (monitor priority 100, unit priority 200)
- FGT-60\_B has cluster ID FGT-602803030702 (monitor priority 100, unit priority 100)

Depending on firewall policies, traffic can still flow between the internal and external networks. Because the primary unit (FGT-60\_C) no longer has a connection to the DMZ network, traffic cannot flow between the DMZ network and any of the other networks. This occurs because monitor priorities are configured to favour traffic flow to and from the internal network (WAN1 interface) instead of the DMZ network.

Even with so many interfaces disconnected, the cluster continues to process traffic passing between the internal and external networks. In addition, as long as the heartbeat interfaces are connected, the cluster shares session and configuration information. So you can make configuration changes to the cluster. For example, if you decided that you want connections to and from the DMZ interface instead of the WAN1 interface, you could connect to the cluster web-based manager and set the DMZ monitor priority higher than the WAN1 monitor priority. This configuration change would be shared among all cluster members, the cluster would renegotiate, and FGT-60\_B would become the primary unit. Because FGT-60\_B has connections to the DMZ and internal networks, traffic would be able to flow between these networks.

### **FGT-60\_C and FGT-60\_A DMZ interfaces disconnected**

Disconnecting the FGT\_60\_C and FGT-60\_A DMZ interfaces in addition to the FGT-60\_A and FGT-60\_B WAN1 interfaces does not cause the cluster to re-negotiate. FGT-60\_C remains the primary unit and FGT-60\_A has the lowest priority in the cluster.

- FGT-60\_C has cluster ID FGT-602104400531 (primary unit, monitor priority 100, unit priority 50)
- FGT-60\_B has cluster ID FGT-602803030702 (monitor priority 100, unit priority 100)
- FGT-60\_A has cluster ID FGT-602104400533 (monitor priority 0, unit priority 200)

Depending on firewall policies, traffic can still flow between the internal and external networks. Because the primary unit (FGT-60\_C) no longer has a connection to the DMZ network, traffic cannot flow between the DMZ network and any of the other networks.

Even with so many interfaces disconnected, the cluster continues to process traffic passing between the internal and external networks. In addition, as long as the heartbeat interfaces are connected, the cluster shares session and configuration information.

# 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](#)
- [Clusters and logging](#)
- [Clusters and SNMP](#)
- [Clusters and quarantine](#)
- [Advanced HA configuration options](#)

## Operating a cluster

The FGCP automatically synchronizes the configurations of all cluster units. This synchronization means that the cluster functions as a single entity and not as a collection of FortiGate units. So, you configure and manage the cluster instead of configuring and managing individual cluster units.

For the most part, you manage an operating cluster in the same way as you manage a standalone FortiGate unit. You can connect to the cluster web-based manager using any cluster network interface configured for HTTPS or HTTP administrative access. You can also connect to the cluster CLI using any cluster network interface configured for SSH or Telnet administrative access. In both cases, you are actually connecting to the primary unit and when you make configuration changes to the cluster, the changes are made to the primary unit first. The primary unit then synchronizes these configuration changes to the subordinate units.

Almost all configuration settings and even the system date and time are synchronized among all cluster members. Only the FortiGate host name, HA unit priority, and HA master override are not synchronized. You can give each cluster unit an individual host name so that you can identify individual cluster units. You can configure different HA unit priority and master override settings to control how a cluster unit functions in the cluster.

This section describes:

- [Cluster web-based manager](#)
- [Cluster CLI](#)
- [Cluster front panel and LCD](#)
- [Viewing the status of cluster units](#)
- [Upgrading cluster firmware](#)
- [Changing the cluster operating mode](#)
- [Changing HA configuration options](#)
- [Managing subordinate units](#)
- [FGCP compatibility with PPP protocols](#)
- [Cluster communication with the FortiProtect Distribution Network](#)
- [Clusters and FortiGuard/FortiShield](#)
- [Cluster communication with RADIUS and LDAP servers](#)
- [Synchronizing the cluster configuration](#)

## Cluster web-based manager

The cluster web-based manager is very similar to the standalone FortiGate web-based manager. The only differences are:

- You can go to **System > Config > HA** and select Cluster Members for a dashboard view of the status of all cluster units. See [“To view the status of cluster units from the web-based manager” on page 85](#).
- You can go to **Log&Report > Log Access** and view and manage disk and memory logs for each cluster unit. See [“Viewing and managing logs for an HA cluster” on page 92](#).
- If the cluster units contain log disks, you can go to **Anti-Virus > Quarantine** and view and manage the quarantine list for each cluster unit. See [“Clusters and quarantine” on page 98](#).



**Note:** Individual cluster units write their own log messages, send their own SNMP traps, and send their own quarantine files to FortiLog. For more information, see [“Clusters and logging” on page 92](#), [“Clusters and SNMP” on page 97](#), and [“Clusters and quarantine” on page 98](#)

### System status, router monitor and IPSec VPN monitor

The cluster web-based manager system status page displays the following information for the primary unit only:

- Recent virus detections
- Content summary
- Interface status
- System resources
- recent intrusion detections

The system status session page shows sessions being processed by the primary unit only.

The cluster DHCP Dynamic IP list, router monitor, and IPSec VPN monitor all display information about the primary unit only. You cannot display this information for subordinate units.

## Cluster CLI

The cluster CLI is very similar to the standalone FortiGate web-based manager. The only differences are:

- You can use `get system status` to view the current HA status of the cluster unit. See [“To view the status of a cluster unit from the CLI” on page 87](#)
- You can use `execute ha manage` to log into a subordinate unit CLI. A number of options are available from the subordinate unit CLI. As well, a number of restrictions are imposed. See [“Managing subordinate units” on page 88](#) for the details.
- You can use `execute ha synchronize` to force the cluster to synchronize its configuration. See [“To manually synchronize the configuration of a subordinate unit” on page 90](#).

## Cluster front panel and LCD

You can identify the role of a cluster unit from the front panel LCD. On the primary unit the LCD displays `primary`. On 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 the Cluster the LCD displays are:

- `primary (a-a)`
- `slave 1 (a-a)`
- `slave 2 (a-a)`

## Viewing the status of cluster units

You can view the status of cluster units from the web-based manager and from the cluster CLI.

### To view the status of cluster units from the web-based manager

- 1 Log into the cluster web-based manager.
- 2 Go to **System > Config > HA**.
- 3 Select Cluster Members.

The cluster members list appears. Cluster units are shown in order of priority in the cluster with the primary unit at the top of the list.

Figure 20: Example cluster members list

Refresh every		10 seconds		Go		Back to HA configuration page >>	
Cluster ID	Status	Up Time	Monitor				
FGT-602104400533	✔	0 days 0 hours 8 minutes 59 seconds	CPU Usage 	Active Sessions	Total Packets	Virus Detected	
			Memory Usage 	Network Utilization	Total Bytes	Intrusion Detected	
FGT-602803030702	✔	0 days 0 hours 9 minutes 19 seconds	CPU Usage 	Active Sessions	Total Packets	Virus Detected	
			Memory Usage 	Network Utilization	Total Bytes	Intrusion Detected	
FGT-602104400531	✔	0 days 0 hours 8 minutes 23 seconds	CPU Usage 	Active Sessions	Total Packets	Virus Detected	
			Memory Usage 	Network Utilization	Total Bytes	Intrusion Detected	

<b>Refresh every</b>	Set the refresh interval to control how often the web-based manager updates the system status display.
<b>Go</b>	Set the selected refresh interval.
<b>Back to HA configuration page</b>	Close the cluster members list and return to the HA configuration page.
<b>Cluster ID</b>	Use the cluster ID to identify each FortiGate unit in the cluster. The cluster ID matches the FortiGate unit serial number.
<b>Status</b>	Indicates the status of each cluster unit. A green check mark indicates that the cluster unit is operating normally. A grey X indicates that the cluster unit cannot communicate with the cluster unit.
<b>Up Time</b>	The time in days, hours, minutes, and seconds since the cluster unit was last started.
<b>Monitor</b>	Displays system status information for each cluster unit.
<b>CPU Usage</b>	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.
<b>Memory Usage</b>	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.
<b>Active Sessions</b>	The number of communications sessions being processed by each cluster unit.
<b>Total Packets</b>	The number of packets that have been processed by the cluster unit since it last started.
<b>Virus Detected</b>	The number of viruses detected by the cluster unit since it last started.
<b>Network Utilization</b>	The total network bandwidth being used by all of the cluster unit interfaces.

**Total Bytes** The number of bytes that have been processed by the cluster unit since it last started.

**Intrusion Detected** The number of intrusions or attacks detected by the cluster unit.

### To view the status of a cluster unit from the CLI

Use the following procedure to view the HA status of a cluster unit. You can use this procedure by logging into the cluster CLI using SSH or Telnet, or by logging into the CLI of a cluster unit using a console connection.

- 1 Log into the CLI.
- 2 Display system status. Enter:

```
get system status
```

The last line of the system status display includes current HA status for the cluster unit that you have logged into. For example, the following shows that you have connected to the primary unit CLI and that the cluster is operating in active-passive mode.

```
Current HA status: mode=a-p, idx=0
```

## Upgrading cluster firmware

You can upgrade a cluster running FortiOS v2.80 to a new FortiOS v2.80 firmware version from the cluster web-based manager or CLI using a standard firmware upgrade procedure. The new firmware version is first uploaded and installed in the primary unit. The primary unit then updates the firmware of the subordinate units.

Upgrading to a new firmware version may interrupt network traffic as the cluster installs the new firmware version and all of the cluster units restart.



**Note:** Installing firmware from a system reboot using the CLI removes the unit from the cluster because HA settings are lost when the cluster unit reverts to factory default settings.



**Note:** To upgrade a cluster from FortiOS v2.50 to FortiOS v2.80 you must upgrade the individual cluster units and then reform the cluster. See the [Fortinet Knowledge Center High Availability](#) page for more information.



**Note:** You cannot upgrade cluster firmware from the cluster web-based manager or CLI if some cluster units are running different firmware builds. However, re-installing the firmware build running on the primary unit forces the primary unit to upgrade all cluster units to the same firmware build.

## Changing the cluster operating mode

You can change the cluster operating mode from NAT/Route to Transparent mode or from Transparent to NAT/Route mode from the cluster web-based manager or CLI using standard procedures. When you change the operating mode from the cluster web-based manager or CLI, each cluster unit restarts in the new operating mode and then negotiates to rejoin the cluster. All HA settings are kept. All other configuration settings (for example, interface IP addresses, firewall policies and so on) are reset to factory defaults. When the cluster is functioning in the new operating mode, you can configure it in the same way as a standalone FortiGate unit.

## Changing HA configuration options

From the cluster web-based manager or CLI you can change the cluster HA mode, group ID, password, heartbeat device priorities, and monitor priorities without restarting the cluster or interrupting traffic processing. Just like any other configuration change, the cluster synchronizes the changed settings to all cluster units and then begins operating using the new configuration.

The HA unit priority and override master setting is not synchronized to each cluster member. When a cluster is operating, you can change the unit priority and override master setting of the primary unit from the cluster web-based manager or CLI. To change the unit priority and override master setting for a subordinate unit without interrupting cluster operation you must connect to subordinate unit CLI. See [“Managing subordinate units”](#).

## Managing subordinate units

You can connect to a subordinate unit CLI using a direct console connection. You can also connect to the cluster CLI and use the `execute ha manage` command to connect to the CLI of any subordinate unit. The primary unit starts a Telnet (TCP port 23) administrative session to the subordinate unit using the heartbeat devices. This Telnet session appears on the cluster web-based manager session list as a TCP session between 10.0.0.1 and 10.0.0.2 (or 10.0.0.3 etc. depending on the subordinate unit connected to). The Telnet session logs into the subordinate unit using the built-in `ha_admin` administrator account.

From the subordinate unit CLI you can change the FortiGate unit host name and the HA unit priority and override master settings. The CLI prevents you from making any other configuration changes.

You can also use `get` commands to view subordinate unit configuration and status information. Most `execute` commands are also available, although commands such as `execute ping` may not work as expected. But you can use `execute` commands to reboot or shut down the subordinate unit, format the subordinate unit log disk, and reset the subordinate unit to its factory default configuration.

### To connect to a subordinate unit CLI

- 1 Log into the cluster CLI.  
You can use SSH or Telnet to log into the cluster CLI or you can use a console connection to the primary unit CLI. To use a console connection, you must know which unit is the primary unit.
- 2 Enter the following command followed by a space and type a question mark (?):

```
execute ha manage
```

The CLI displays a list of the serial numbers of all if the subordinate units in the cluster. Each entry is numbered, starting at 1.

```
execute ha manage
<id>    please input slave cluster index.
<1>     Subsidiary unit FGT-602104400531
<2>     Subsidiary unit FGT-602104400533
```

- 3 Complete the `execute ha manage` command with the number of the subordinate unit to log into. For example, to log into subordinate unit 1, enter:

```
execute ha manage 1
```

You are logged into the selected subordinate unit CLI. The CLI prompt includes the host name of this subordinate unit followed by a `$`. For example:

```
FGT-60_A $
```

- 4 Enter the following command to return to the cluster CLI:

```
exit
```

## FGCP compatibility with PPP protocols

FortiGate HA is not compatible with PPP protocols such as DHCP or PPPoE. If one or more FortiGate unit interfaces uses DHCP or PPPoE to acquire an IP address, you cannot switch to operating in HA mode. Also, in an operating cluster, you cannot change an interface to use DHCP or PPPoE.

Configuring a FortiGate interface to be a DHCP server or a DHCP relay agent is not affected by HA operation. However, if a failure occurs, DHCP sessions are not failed over to the new primary unit and must be reestablished after a failover. In an active-active cluster, the primary unit handles all DHCP services.

PPTP and L2TP are supported in HA mode. You can configure PPTP and L2TP settings; you can also add firewall policies to allow PPTP and L2TP pass through. PPTP and L2TP sessions are not failed over to a new primary unit and must be reestablished after a failover. In an active-active cluster, all PPTP and L2TP sessions are processed by the primary unit.

## Cluster communication with the FortiProtect Distribution Network

In an operating cluster, the primary unit communicates with the FortiProtect Distribution Network (FDN). All cluster units must be registered and licensed for antivirus and attack definition updates because any cluster unit can potentially become the primary unit.

When the primary unit receives antivirus or attack definition updates from the FDN, the primary unit copies these updates to the subordinate units.

## Clusters and FortiGuard/FortiShield

In an operating cluster, only the primary unit communicates with the FortiGuard/FortiShield networks. All cluster units must have the required FortiGuard/FortiShield licenses because any cluster unit can potentially become the primary unit.

In a cluster that is operating in active-passive mode, only the primary unit processes traffic and only the primary unit communicates with the FortiGuard/FortiShield network. In a cluster that is operating in active-active mode, subordinate units send FortiGuard/FortiShield requests to the primary unit. The primary unit relays the requests to the FortiGuard/FortiShield network and relays the responses back to the subordinate unit.

The web-based manager displays FortiGuard/FortiShield status for the primary unit only. FortiGuard/FortiShield reports are based on primary unit statistics and not on cluster statistics.

## 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.

## Synchronizing the cluster configuration

When you change the cluster configuration the primary unit synchronizes the configuration changes to the subordinate units. To synchronize the subordinate units, the primary unit starts a Telnet (TCP port 23) administrative session to the subordinate units using the heartbeat devices. The Telnet session logs into the subordinate unit using the built-in `ha_admin` administrator account. Otherwise, synchronization takes place silently, and no log messages are recorded.

After synchronization, each subordinate unit compares its new configuration with the primary unit configuration. If a difference is found, the subordinate attempts to re-synchronize its configuration. If synchronization fails after five attempts, the subordinate unit reboots and repeats the synchronization process. Rebooting the subordinate unit resets all processes so that synchronization can proceed normally. See [“Console messages when configuration synchronization fails” on page 91](#) for a listing of the messages that appear on a subordinate unit console if synchronization fails.

Synchronization will only work if all cluster units must be running the same FortiOS v2.80 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.

### To manually synchronize the configuration of a subordinate unit

Use the following procedure to manually synchronize the configuration of a subordinate unit. You may need to do this if the subordinate unit cannot synchronize its configuration with the primary unit.

- 1 Connect to the cluster and log into the CLI.
- 2 Use the `execute ha manage` command to connect to a subordinate unit CLI.

- 3 Use the `execute ha synchronize` command to synchronize the configuration of this subordinate unit.

Using the `execute ha synchronize` command you can select what to synchronize and you can also start and stop the synchronization process. See [“execute ha synchronize” on page 42](#) for information about the `execute ha synchronize` command.

### Console messages when configuration synchronization fails

If a subordinate cannot synchronize its configuration with the primary unit, the subordinate unit makes five attempts to perform the synchronization. If all 5 attempts fail, the subordinate unit restarts and tries to synchronize its configuration again. If you connect to the subordinate unit console connection, messages similar to the following appear:

```
slave and master config difference 25
slave: webfilter.script: 76fc48b1b1fdc37869f1ff8fd99b90c6
master: firewall.profile: 67b0e36c5b8b07acf0bb64f6cb356db3
slave is not sync with master, sequence:0. (type 0x3)
slave and master config difference 25
slave: webfilter.script: 76fc48b1b1fdc37869f1ff8fd99b90c6
master: firewall.profile: 67b0e36c5b8b07acf0bb64f6cb356db3
config subtile difference 85
slave:
master: al      F
slave is not sync with master, sequence:1. (type 0x3)
slave and master config difference 25
slave: webfilter.script: 76fc48b1b1fdc37869f1ff8fd99b90c6
master: firewall.profile: 67b0e36c5b8b07acf0bb64f6cb356db3
config subtile difference 85
slave:
master: al.b
slave is not sync with master, sequence:2. (type 0x3)
slave and master config difference 25
slave: webfilter.script: 76fc48b1b1fdc37869f1ff8fd99b90c6
master: firewall.profile: 67b0e36c5b8b07acf0bb64f6cb356db3
config subtile difference 85
slave:
master: al.b
slave is not sync with master, sequence:3. (type 0x3)
slave and master config difference 25
slave: webfilter.script: 76fc48b1b1fdc37869f1ff8fd99b90c6
master: firewall.profile: 67b0e36c5b8b07acf0bb64f6cb356db3
config subtile difference 85
slave:
master: al.b
slave is not sync with master, sequence:4. (type 0x3)
slave is synchronizing configure file. Wait for reboot!
```

## Clusters 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 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.

Figure 21: Example cluster log access

#	Date	Time	Level	User Interface	Action	Message
5	2005-02-26	11:12:04	notice			Detected new joined HA member
6	2005-02-26	11:12:04	notice			HA move to work state
7	2005-02-26	11:11:40	critical			HA mode changed to A-A
8	2005-02-26	11:11:30	information	GUI(172.20.120.11)	login	User admin login successfully from GUI(172.20.120.11)
9	2005-02-26	10:36:46	notice			Detected new joined HA member
10	2005-02-26	10:33:49	notice			Detected HA member dead
11	2005-02-26	10:30:00	notice			Detected new joined HA member
12	2005-02-26	10:27:02	notice			Detected HA member dead
13	2005-02-26	10:26:31	information	GUI(172.20.120.11)	login	User admin login successfully from GUI(172.20.120.11)
14	2005-02-26	10:25:35	notice			HA slave became master
15	2005-02-26	10:25:35	notice			HA monitored interface wan1 link ready
16	2005-02-26	10:25:31	notice			HA move to standby state
17	2005-02-26	10:25:31	notice			HA monitored interface dmz link ready
18	2005-02-26	10:25:08	notice			HA master became slave
19	2005-02-26	10:25:08	warning			HA monitored interface wan1 link failed
20	2005-02-26	10:24:37	notice			HA slave became master
21	2005-02-26	10:23:26	notice			HA move to standby state
22	2005-02-26	10:23:11	information	telnet(10.0.0.1)	logout	User FGT_ha_admin Logs out from telnet(10.0.0.1)
23	2005-02-26	10:21:53	information	telnet(10.0.0.1)	logout	User FGT_ha_admin Logs out from telnet(10.0.0.1)
24	2005-02-26	10:21:42	information	telnet(10.0.0.1)	logout	User FGT_ha_admin Logs out from telnet(10.0.0.1)
25	2005-02-26	10:20:49	notice			HA master became slave
26	2005-02-26	10:20:49	warning			HA monitored interface dmz link failed
27	2005-02-26	10:18:42	information	GUI(172.20.120.11)	login	User admin login successfully from GUI(172.20.120.11)
28	2005-02-26	10:18:13	notice			HA slave became master

## HA log messages

The following log messages are generated by HA activity.

<b>Message ID:</b>	35001						
<b>Severity:</b>	Notification						
<b>Message:</b>	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						
<b>Meaning:</b>	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.						
	<table border="0"> <tr> <td>HA group id changed to&lt;value_ha_id&gt;</td> <td>The group ID has been changed for this cluster unit.</td> </tr> <tr> <td>HA slave became master</td> <td>This cluster unit was operating as a subordinate unit and is now the primary unit.</td> </tr> <tr> <td>HA move to standalone mode</td> <td>The operation mode of this cluster unit has changed from HA to standalone.</td> </tr> </table>	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 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 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  
**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  
**Severity:** Critical  
**Message:** msg="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  
**Severity:** Critical  
**Message:** msg="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.

---



---

**Message ID:** 35012  
**Severity:** Critical  
**Message:** msg="HA mode changed to A-P"  
**Meaning:** This cluster unit was changed to operate in active-passive mode. The cluster unit may have initially be operating in standalone mode or active-active mode.

---

---

<b>Message ID:</b>	35013
<b>Severity:</b>	Critical
<b>Message:</b>	msg="HA mode changed to unknown"
<b>Meaning:</b>	This cluster unit was changed to operate in an unknown mode.

---

## Admin log messages

The following messages are not specifically HA messages, but appear during HA status changes.

---

<b>Message ID:</b>	32007
<b>Severity:</b>	Information
<b>Message:</b>	User FGT_ha_admin Logs out from telnet(10.0.0.1).
<b>Meaning:</b>	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 <a href="#">"HA heartbeat Telnet sessions"</a> on page 16 for information about HA heartbeat telnet sessions.

---



---

<b>Message ID:</b>	32138
<b>Severity:</b>	Critical
<b>Message:</b>	user=ha_slave ui=ha_daemon action=reboot msg="User ha_slave rebooted the device from ha_daemon"
<b>Meaning:</b>	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. See ["Customizing primary unit selection"](#) on page 61 for the description of the cluster configuration. 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. See [“Customizing primary unit selection” on page 61](#) for the description of the cluster configuration.

- 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"
- 5 device\_id=FGT-602104400533 log\_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected new joined HA member"
- 6 device\_id=FGT-602104400531 log\_id=0105035001 type=event subtype=ha pri=notice vd=root msg="Detected new joined HA member"

## 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 MIB fields” on page 98](#) and [“HA-related FortiGate traps” on page 97](#).

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. HA traps indicate when a cluster unit has started and when interfaces have been connected to disconnected.

**Table 9: HA-related FortiGate traps**

Trap message	Description
ColdStart WarmStart LinkUp LinkDown	Standard traps as described in RFC 1215.
HA state	HA state changes. The trap message includes the previous state, the new state and a flag indicating whether the unit is the primary unit.
HA switch	The primary unit in an HA cluster fails and is replaced with a new primary unit.

**Table 10: HA-related System MIB field**

MIB field	Description
haMode	The current FortiGate High-Availability (HA) mode (standalone, A-A, A-P)

Table 11: HA MIB fields

MIB field	Description
<b>groupid</b>	HA group ID.
<b>priority</b>	The clustering priority of the individual FortiGate unit in a cluster.
<b>override</b>	The master-override setting (enable or disable) for an individual FortiGate unit in a cluster.
<b>autoSync</b>	Auto config synchronization flag.
<b>schedule</b>	Load balancing schedule for A-A mode.
<b>stats</b>	Statistics for all of the units in the HA cluster.
<b>index</b>	The index number of the FortiGate unit.
<b>serial</b>	The FortiGate unit serial number.
<b>cpuUsage</b>	The current FortiGate unit CPU usage as a percent.
<b>memUsage</b>	The current FortiGate unit memory usage (in MB).
<b>netUsage</b>	The current FortiGate unit network utilization (in Mbps).
<b>sesCount</b>	The number of active sessions being processed by the FortiGate unit.
<b>pktCount</b>	The number of packets processed by the FortiGate unit.
<b>byteCount</b>	The number of bytes processed by the FortiGate unit
<b>idsCount</b>	The number of attacks detected by the IPS running on the FortiGate unit in the last 20 hours.
<b>avCount</b>	The number of viruses detected by the antivirus system running on the FortiGate unit in the last 20 hours.

## Clusters 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.

**Figure 22: Example cluster quarantined files access**

File Name	Date	Service	Status	Status Description	DC	TTL	Upload Status
winmx331.exe	03/15/2004 20:53	POP3	Blocked	File was stopped by file block pattern.	0	EXP.	N
AUTOPLAY.EXE	03/15/2004 20:54	POP3	Blocked	File was stopped by file block pattern.	0	EXP.	N
AFWeeklyReport.doc	03/15/2004 20:46	POP3	Blocked	File was stopped by file block pattern.	1	EXP.	N
Internet.doc	03/15/2004 20:53	POP3	Blocked	File was stopped by file block pattern.	0	EXP.	Y

## 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 <tll_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 the 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.

### **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

```
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 packets to get cluster information.

Enabling HA encryption and authentication could reduce cluster performance.

### **Command syntax**

```
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

```
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.



# Failover protection

FortiGate active-passive HA provides failover protection. This means that an active-passive cluster can provide FortiGate Antivirus Firewall services even when one of the cluster units encounters a problem that would result in complete loss of connectivity for a stand-alone FortiGate unit. This failover protection provides a backup mechanism that can be used to reduce the risk of unexpected downtime, especially in a mission-critical environment.

This chapter describes how HA failover protection works and provides detailed NAT/Route and Transparent mode packet flow descriptions. This chapter contains the following sections:

- [Active-passive failover](#)
- [Active-active failover](#)
- [Device failover](#)
- [Link failover](#)
- [NAT/Route mode active-passive cluster packet flow](#)
- [Transparent mode active-passive cluster packet flow](#)
- [Monitoring cluster units for failover](#)
- [Failover performance](#)

## Active-passive failover

To achieve failover protection in an active-passive cluster, one of the cluster units functions as the primary unit, while the rest of the cluster units are subordinate units, operating in a stand-by mode. The cluster IP addresses and HA virtual MAC addresses are associated with the cluster interfaces of the primary unit. All traffic directed at the cluster is actually sent to and processed by the primary unit.

While the cluster is functioning, the primary unit functions as a FortiGate Antivirus Firewall for the networks that it is connected to. In addition, the primary unit and subordinate units use the FGCP heartbeat to keep in constant communication. The primary unit informs the subordinate units of all changes to the cluster connection and state tables, keeping these subordinate units up-to-date with the traffic currently being processed by the cluster. The subordinate units report their status to the cluster unit and receive and store connection and state table updates.

If the primary unit encounters a problem that is severe enough to cause a failover, the remaining cluster units negotiate to select a new primary unit. This occurs because all of the subordinate units are constantly waiting to negotiate to become primary units. Only the heartbeat packets sent by the primary unit keep the subordinate units from becoming primary units. Each received heartbeat packet resets negotiation timers in the subordinate units. If this timer is allowed to run out because the subordinate units do not receive heartbeat packets from the primary unit, the subordinate units assume that the primary unit has failed, and negotiate to become primary units themselves.

Using the same FCGP negotiant process that occurs when the cluster starts up, the subordinate units negotiate to select a new primary unit. Once a subordinate unit wins the negotiation and becomes a primary unit, the new primary unit recognizes all open connections that were being handled by the cluster. The connections continue to be processed and are handled according to their last known state.

If the failed primary unit recovers, it will become a subordinate unit, unless override master is selected (see [“Override Master” on page 28](#)) and its unit priority is set higher than the unit priority of other cluster units (see [“Unit Priority” on page 27](#)).

Even though in an active-passive cluster subordinate units do not actively process connections, they do play an active part in the cluster. Subordinate units continuously receive connection state and link state information from the primary unit. The subordinate units maintain the same table of connection and link states as the primary unit, so that they can resume communication through the cluster if the primary unit fails.

Subordinate units also report their own operation and link status to the cluster. If a subordinate unit fails, it is actively removed from the cluster by the cluster units that are still operating.

## Failover exceptions

During a failover event, active-passive clusters resume all communication sessions with one exception. Virus scanning sessions that are in progress are not failed over. If an HTTP or FTP download is in progress, the interrupted download has to be restarted. As well, if email attachment is being virus scanned, after the failover the email session must be restarted by the email client or server.

Also, FortiGate failover does not support PPP protocols such as PPPoE, DHCP, PPTP and L2TP. See [“FGCP compatibility with PPP protocols” on page 89](#) for more information.

If override master is enabled and the primary unit fails, another cluster unit becomes the primary unit. When the cluster unit with override master enabled rejoins the cluster it overrides the current primary unit and becomes the new primary unit. When this override occurs, all communication sessions through the cluster are lost and must be re-established.

## Active-active failover

HA failover in a cluster running in active-active mode is similar to the active-passive failover mechanism described in this chapter. Active-active subordinate units are constantly waiting to negotiate to become primary units and continuously receive connection state information from the primary unit. If the primary unit fails, the subordinate units use the same mechanism to detect that the primary unit has failed and to negotiate to select a new primary unit. The new primary unit also maintains communication sessions through the cluster using the shared connection state table.

Active-active mode load balances connections among all cluster units. After a failover, the cluster must maintain all of these communication sessions. To manage the sessions the functioning cluster uses a load balancing schedule to distribute connections to all cluster units. The shared connection state table tracks the communication sessions being processed by all cluster units (not just the primary unit). After a failover, the new primary unit uses the load balancing schedule to re-distribute all of the communication sessions recorded in the shared connection state table among all of the remaining cluster units. The connections continue to be processed by the cluster, but possibly by a different cluster unit, and are handled according to their last known state

For more information about active-active HA load balancing and failover, see [“Active-active load balancing” on page 121](#).

## Device failover

Device failover means that if a device in the cluster (a cluster unit) fails, the cluster reorganizes itself to continue operating with minimal or no effect on network traffic. To support device failover, the cluster maintains a session table for all communication sessions being processed by the cluster. The session table information is available to the remaining cluster units after a failure. Using this information, the remaining cluster units can resume communication sessions without interruption.

Primary and subordinate units play different roles in the cluster depending on whether the cluster is operating in active-active or active-passive mode. How the cluster responds to a device failure depends on the cluster operating mode and on the cluster unit that fails.

In active-passive mode, if the primary unit fails, the cluster renegotiates to select a new primary unit using the process described in [“Primary unit selection” on page 18](#). All communication sessions are resumed by the new primary unit without interrupting network traffic. In active-passive mode if a subordinate unit fails, information about the failed unit is removed from the remaining cluster unit session tables. Otherwise no change takes place in how the cluster operates and network traffic is not interrupted.

In active-active mode, if the primary unit fails, the cluster also renegotiates to select a new primary unit using the process described in [“Primary unit selection” on page 18](#). The primary unit redistributes TCP sessions among all remaining cluster units according to the load balancing schedule. The TCP sessions resume with no loss of data. All virus scanning sessions and all UDP and ICMP sessions that were being processed by the cluster are lost and must be restarted. Depending on the cluster configuration, as new virus scanning and TCP sessions are received, they are distributed to cluster units using the cluster load balancing schedule. New UDP and ICMP sessions are processed by the new primary unit.

In active-active mode, if a subordinate unit fails, information about the failed unit is removed from the remaining cluster unit session tables. All virus scanning sessions that were being processed by the cluster are lost and must be restarted. TCP sessions being processed by the cluster are resumed. The primary unit redistributes TCP sessions among all remaining cluster units according to the load balancing schedule. UDP and ICMP sessions are not affected by a subordinate unit failure because they continue to be processed by the primary unit.

## Link failover

Link failover means that if a monitored interface in the primary unit fails, the cluster reorganizes to re-establish a connection to the network connected to the monitored interface and to continue operating with minimal or no disruption of network traffic. A monitored link is a cluster interface configured with a monitor priority. You configure a cluster to monitor links as part of the cluster HA configuration. The cluster monitors each cluster unit to determine if the monitored interface is operating and connected. The cluster can detect a hardware failure of the network interface. The cluster can also determine if a cluster interface becomes disconnected or if the switch that cluster interfaces are connected to loses power. However, the cluster cannot determine if one of these switches becomes disconnected from the network.

Figure 23: Example FortiGate-500 HA configuration with monitor priorities set

Standalone Mode  
 High Availability

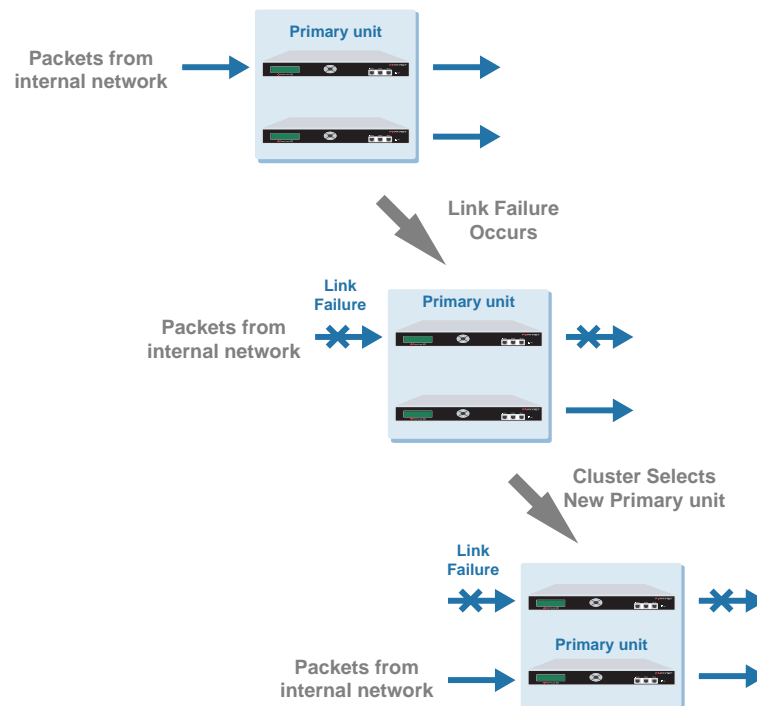
Cluster Members  
 Mode: Active-Active  
 Group ID: 34 (0-63)  
 Unit Priority: 128 (0-255)  
 (The unit with the highest priority will be HA master.)  
 Override master:  Enable  
 Password: \*\*\*\*\*  
 Retype Password: \*\*\*\*\*  
 Schedule: Round-Robin

Interface	Priorities of Heartbeat Device (0-512)	Monitor Priorities (0-512)
internal		300
external		200
dmz		
ha	100	
port1	50	
port2		100
port3		
port4		
port5		
port6		
port7		
port8		

Apply

## How link failover maintains traffic flow

Identifying an interface as a high priority link means that the cluster should make sure communications continue functioning for the network connected to the interface. 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 high priority network fails, to maintain traffic flow to and from this network, the cluster must select a different primary unit. The new primary unit will have an active link to the high priority network.

**Figure 24: An Internal interface link failover causes a cluster to select a new primary unit**

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 a monitored interface on the primary unit fails, the cluster renegotiates to select a new primary unit. The cluster unit with the highest monitor priority becomes the primary unit. Usually this means that another cluster unit becomes the primary unit. If a low-priority interface on the primary unit fails and a high priority interface has failed on other cluster units, the same unit could become the primary unit again. The primary unit selected is the one with the highest total monitor priority as well as the other factors that contribute to primary unit selection. During link failover, the cluster maintains all communication sessions in the same manner as for a device failure.

In an active-passive cluster, after this link failover, the primary unit processes all traffic and all subordinate units, even the former primary unit, share session and link status. In an active-active cluster, the primary unit load balances traffic to all the units in the cluster. The former primary unit can process connections between its functioning interfaces (for, example if the cluster has connections to an internal, external, and DMZ network, the former primary unit can still process connections between the external and DMZ networks). The active-active cluster also shares all session and link status information with all cluster units, including the former primary unit.

If a monitored interface on a subordinate unit fails, the subordinate unit shares this information with all cluster units. The cluster does not renegotiate. The subordinate 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, all TCP 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. Later on if the primary unit fails, this subordinate unit may not be able to become a primary unit because of the link failure.

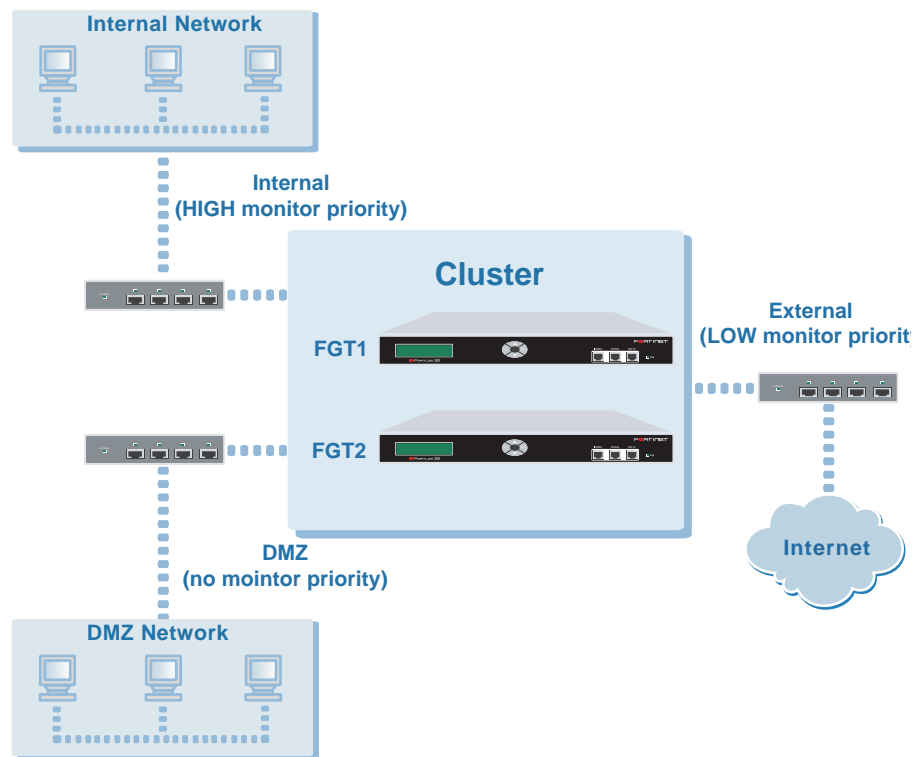
## Multiple link failures

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 best service to the highest priority networks.

## Example link failover scenarios

For the following examples, assume a cluster configuration consisting of two FortiGate units (FGT1 and FGT2) connected to three networks: internal, external, and DMZ. The cluster processes traffic flowing between the internal and external networks, between the internal and DMZ networks, and between the external and DMZ networks. The internal Interface has a higher monitor priority than interface external and FGT1 has a higher unit priority than FGT2. If there are no link failures, FGT1 becomes the primary unit.

Figure 25: Sample link failover scenario topology



**Example 1: the internal link on FGT1 fails**

If the internal link on FGT1 fails, FGT2 becomes primary unit because it has fewer interfaces with a link failure. If the cluster is operating in active-active mode, the cluster load balances traffic between the external and DMZ networks. Traffic between the internal and external and between the internal and DMZ networks is processed by the primary unit only. If the cluster is operating in active-passive mode, all traffic is handled by primary unit only.

**Example 2: internal link on FGT1 and external link on FGT 2 fail**

If the internal link on FGT1 and the external link on FGT2 fail, then FGT2 becomes the primary unit because FGT2 can maintain a connection to the high priority internal network. Only traffic between the internal and DMZ networks can pass through the cluster and the traffic is handled by the primary unit only. No load balancing will occur if the cluster is operating in active-active mode.

**Example 3: internal link on FGT1 and then internal link on FGT2 fails**

If the internal link on FGT1 fails, FGT2 becomes the primary unit. If the internal link on FGT2 fails next, FGT1 reverts back to being the primary unit because it has a higher unit priority than FGT2. If the cluster is operating in active-active mode, the cluster load balances all traffic between the external and DMZ networks. If the cluster is operating in active-passive mode, traffic between the external and DMZ networks is processed by the primary unit only.

**Example 4: internal link on FGT2 and then internal link on FGT1 fails**

If the internal link on FGT2 fails, FGT1 remains the primary unit. If the internal link on FGT1 fails next, FGT1 remains the primary unit because it has a higher unit priority than FGT2.

**Example 5: internal link on FGT1 and internal link on FGT2 fail at the same time**

If the internal link on FGT1 and the internal link on FGT2 fail at the same time, FGT1 remains the primary unit.

## NAT/Route mode active-passive cluster packet flow

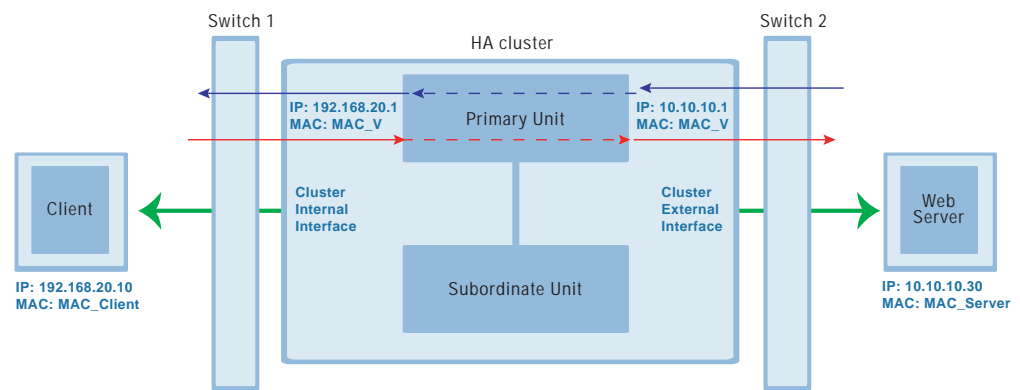
This section describes an example of how packets are processed and how failover occurs in an active-passive HA cluster running in NAT/Route mode. In the example, the NAT/Route mode cluster acts as the internet firewall for a client computer's internal network. The client computer's default route points at the IP address of the cluster internal interface. The client connects to a web server on the Internet. Internet routing routes packets from the cluster external interface to the web server, and from the web server to the cluster external interface.

In NAT/Route mode, three MAC addresses are involved in active-passive communication between the client and the web server when the primary unit processes the connection:

- Virtual MAC address (MAC\_V) assigned to all primary unit interfaces,
- Client MAC address (MAC\_Client),
- Server MAC address (MAC\_Server),

In NAT/Route mode, the HA cluster works as a gateway when it responds to ARP requests. Therefore, the client and the server only know the gateway MAC address, which is the HA virtual MAC address (MAC\_V). The HA virtual MA address is described in “Group ID” on page 27.

**Figure 26: NAT/Route mode active-passive packet flow**



## Packet flow from client to web server

- 1 The client computer requests a connection from 192.168.20.10 to 10.10.10.30.
- 2 The default route on the client computer recognizes 192.168.20.1 (the cluster IP address) as the gateway to the external network where the web server is located.
- 3 The client computer issues an ARP request to 192.168.20.1.
- 4 The primary unit intercepts the ARP request, and responds with the HA virtual MAC address (MAC\_V) which corresponds to its IP address of 192.168.20.1.
- 5 The client's request packet reaches the primary unit internal interface.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_Client
<b>Destination</b>	10.10.10.30	MAC_V

- 6 The primary unit processes the packet.
- 7 The primary unit forwards the packet from its external interface to the web server.

	IP address	MAC address
<b>Source</b>	10.10.10.1	MAC_V
<b>Destination</b>	10.10.10.30	MAC_Server

- 8 The primary unit continues to process packets in this way unless a failover occurs.

### Packet flow from web server to client

- 1 When the web server responds to the client's packet, the cluster external interface IP address (10.10.10.1) is recognized as the gateway to the internal network.
- 2 The web server issues an ARP request to 10.10.10.1.
- 3 The primary unit intercepts the ARP request, and responds with the HA virtual MAC address (MAC\_V) which corresponds its IP address of 10.10.10.1.
- 4 The web server then sends response packets to the primary unit external interface.

	IP address	MAC address
<b>Source</b>	10.10.10.30	MAC_Server
<b>Destination</b>	10.10.10.1	MAC_V

- 5 The primary unit processes the packet.
- 6 The primary unit forwards the packet from its internal interface to the client.

	IP address	MAC address
<b>Source</b>	10.10.10.30	MAC_V
<b>Destination</b>	192.168.20.10	MAC_Client

- 7 The primary unit continues to process packets in this way unless a failover occurs.

### When a device failover occurs

- 1 If the primary unit fails the remaining unit negotiates to become the primary unit.
- 2 The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC address.  
The new primary unit has the same IP address as the failed primary unit.
- 3 The new primary units sends a special ARP request to the 192.168.20.x network to associate its internal IP address with the HA virtual MAC address.
- 4 The new primary units sends a special ARP request to the external network to associate its external IP address with the HA virtual MAC address.
- 5 Traffic sent to the cluster is now received and processed by the new primary unit.  
If there were more than two cluster units in the original cluster, these remaining units would become subordinate units.

## Transparent mode active-passive cluster packet flow

This section describes and example of how packets are processed and how failover occurs in an active-passive HA cluster running in Transparent mode. The cluster is installed on an internal network in front of a mail server and the client connects to the mail server through the Transparent mode cluster.

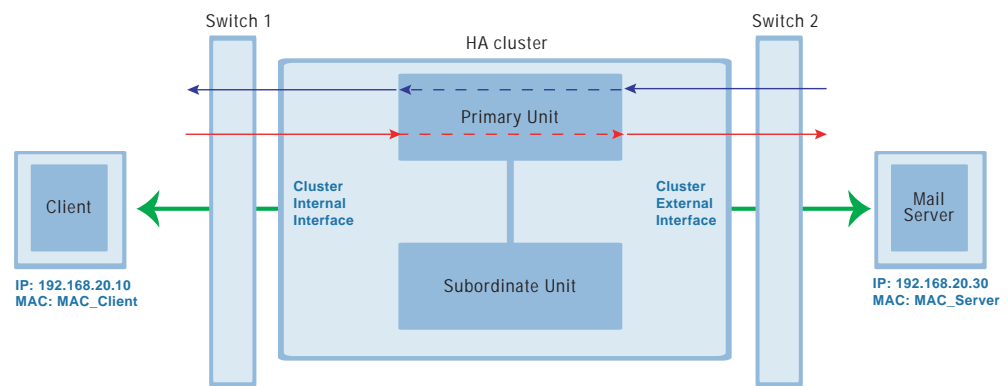
In Transparent mode, two MAC addresses are involved in active-active communication between a client and a server when the primary unit load balances packets to the subordinate unit:

- Client MAC address (MAC\_Client)
- Server MAC address (MAC\_Server)

The HA virtual MAC address is not directly involved in communicate between the client and the server. The client computer sends packets to the mail server and the mail server sends responses. In both cases the packets are intercepted and processed by the cluster.

The cluster's presence on the network is transparent to the client and server computers. The primary unit sends special ARP packets to Switch 1 that associate all MAC addresses on the network segment connected to the cluster external interface with the HA virtual MAC address. The primary unit also sends special ARP packets to Switch 2 that associate all MAC addresses on the network segment connected to the cluster internal interface with the HA virtual MAC address. In both cases, this results in the switches sending packets to the primary unit interfaces.

**Figure 27: Transparent mode active-passive packet flow**



## Packet flow from client to mail server

- 1 The client computer requests a connection from 192.168.20.10 to 192.168.20.30.
- 2 The client computer issues an ARP request to 192.168.20.30.
- 3 The primary unit forwards the ARP request to the mail server.
- 4 The mail server responds with its MAC address (MAC\_Server) which corresponds to its IP address of 192.168.20.30. The primary unit returns the ARP response to the client computer.
- 5 The client's request packet reaches the primary unit internal interface.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_Client
<b>Destination</b>	192.168.20.30	MAC_Server

- 6 The primary unit processes the packet.

- 7 The primary unit forwards the packet from its external interface to the mail server.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_Client
<b>Destination</b>	192.168.20.30	MAC_Server

- 8 The primary unit continues to process packets in this way unless a failover occurs.

## Packet flow from mail server to client

- 1 To respond to the client computer, the mail server issues an ARP request to 192.168.20.10.
- 2 The primary unit forwards the ARP request to the client computer.
- 3 The client computer responds with its MAC address (MAC\_Client) which corresponds to its IP address of 192.168.20.10. The primary unit returns the ARP response to the mail server.
- 4 The mail server's response packet reaches the primary unit external interface.

	IP address	MAC address
<b>Source</b>	192.168.20.30	MAC_Server
<b>Destination</b>	192.168.20.10	MAC_Client

- 5 The primary unit processes the packet.
- 6 The primary unit forwards the packet from its internal interface to the client.

	IP address	MAC address
<b>Source</b>	192.168.20.30	MAC_Server
<b>Destination</b>	192.168.20.10	MAC_Client

- 7 The primary unit continues to process packets in this way unless a failover occurs.

## When a device failover occurs

- 1 If the primary unit fails the remaining unit negotiates to become the primary unit.
- 2 The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC address.
- 3 The new primary unit sends special ARP requests to switch 1 to associate its MAC address with the MAC addresses on the network segment connected to the external interface.
- 4 The new primary unit sends special ARP requests to switch 2 to associate its MAC address with the MAC addresses on the network segment connected to the internal interface.
- 5 Traffic sent to the cluster is now received and processed by the new primary unit. If there were more than two cluster units in the original cluster, these remaining units would become subordinate units.

## Monitoring cluster units for failover

You can use logging and SNMP to monitor cluster units for failover. Both the primary and subordinate units can be configured to write log messages and send SNMP traps if a failover occurs. You can also log into the cluster web-based manager and CLI to determine if a failover has occurred.

### Monitoring for device failure

If the primary unit experiences a device failure, the units in the cluster renegotiate to select a new primary unit. Failure of the primary unit results in the following:

- The new primary unit writes the following messages to the event log:  

```
device_id=FGT-602803030702 log_id=0105035001 type=event
subtype=ha pri=notice vd=root msg="HA slave became master"
device_id=FGT-602803030702 log_id=0105035001 type=event
subtype=ha pri=notice vd=root msg="Detected HA member dead"
```
- The subordinate units in the cluster write the following message to the event log.  

```
device_id=FGT-602104400531 log_id=0105035001 type=event
subtype=ha pri=notice vd=root msg="Detected HA member dead"
```
- 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.
- Log into the cluster web-based manager. If the primary unit has changed, the host name of the new primary unit appears on the system status page. Go to System > Config > HA and select cluster members. A different device ID appears at the top of the cluster members list. The list may also include fewer cluster units because the failed primary unit no longer appears on the Cluster Members list.
- Log into the cluster CLI. If the primary unit has changed, the host name of the new primary unit appears in the CLI prompt. Enter `execute ha manage ?` to display the list of subordinate units. The list includes fewer subordinate units if a unit has failed and not rejoined the cluster

If a subordinate unit experiences a device failure, the cluster continues to function normally. Failure of a subordinate unit results in the following:

- The primary unit and the subordinate units in the cluster write the following message to the event log. The message is written by each unit remaining in the cluster.  

```
device_id=FGT-602104400531 log_id=0105035001 type=event
subtype=ha pri=notice vd=root msg="Detected HA member dead"
```
- Log into the cluster web-based manager. The HA cluster members list contains fewer cluster members, but the same primary unit should be at the top of the list.
- Log into the cluster CLI. Enter `execute ha manage ?` to display the list of subordinate units. The list includes fewer subordinate units if a unit has failed and not rejoined the cluster

## Failover performance

This section describes the designed device and link failover times for a FortiGate cluster and also shows results of a failover performance test.

- [Device failover performance](#)
- [Link failover performance](#)
- [Failover performance test results](#)

### Device failover performance

By design FGCP device failover time is 2 seconds. All cluster units regularly receive HA heartbeat packets from all other cluster units over the HA heartbeat link. If any cluster unit does not receive a heartbeat packet from any other cluster unit for 2 seconds, the cluster unit that has not sent heartbeat packets is considered to have failed.

It may take another few seconds for the cluster to negotiate and re-distribute communication sessions.

You can change the `hb-lost-threshold` to increase or decrease the device failover time. See [“Modifying heartbeat timing” on page 101](#) for information about using `hb-lost-threshold`, and other heartbeat timing settings.

### Link failover performance

Link failover time is controlled by how long it takes for a cluster to synchronize the cluster link database. When a link failure occurs, the cluster unit that experienced the link failure uses HA heartbeat packets to broadcast the updated link database to all cluster units. When all cluster units have received the updated database the failover is complete.

It may take another few seconds for the cluster to negotiate and re-distribute communication sessions.

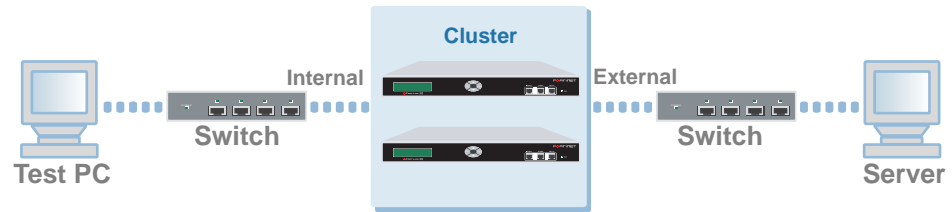
### Failover performance test results

This section describes a simple failover performance test for a FortiGate cluster. In the test a cluster is installed between a PC running Windows 2000 and a server. For each performance test case the PC continuously sends 50 ping packets through the cluster to the server. The response waiting time for the ping packets is 1 second. The ping command is:

```
ping -w 1000 -n 50 <server_IP>
```

A failure is simulated and when the failover occurs, the number of return packets that are lost is the number of seconds required for failover. Device failure is simulated by restarting the primary unit (restart) and by disconnecting the power from the primary unit (power off). Link failure is simulated by adding a monitor priority to the cluster internal interface and then disconnecting the internal interface ethernet cable.

Figure 28: Failover performance test topology



## Test results

Table 12 shows the average failover times in seconds for a network processing minimal traffic. Failover times may be different for different network conditions.

Table 12: FortiOS v2.80 HA failover time (in seconds)

Action	NAT/Route Mode		Transparent Mode	
	Active-Passive	Active-Active	Active-Passive	Active-Active
Link Failure	1	2	1	1
Restart	2	3	3	3
Power Off	2	2	2	2



# Active-active load balancing

FGCP active-active load balancing distributes network traffic among all of the units in a cluster. Load balancing can improve cluster performance because the processing load is shared among multiple FortiGate units.

This chapter describes how active-active load balancing works and provides detailed NAT/Route and Transparent mode packet flow descriptions.

- [Load balancing overview](#)
- [Configuring load balancing settings](#)
- [NAT/Route mode active-active cluster packet flow](#)
- [Transparent mode active-active cluster packet flow](#)

## Load balancing overview

In active-active HA mode, the FGCP uses unicast load balancing in which 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 propagates the packets to subordinate units, using the active-active load balancing schedule.

### Load balancing schedules

The load balancing schedule controls how the primary unit distributes packets to all cluster units. You can select from the following load balancing schedules.

<b>None</b>	No load balancing. Select None when the cluster interfaces are connected to load balancing switches. If you select None, the Primary unit does not load balance traffic and the subordinate units process incoming traffic that does not come from the Primary unit. For all other load balancing schedules, all traffic is received first by the Primary unit, and then forwarded to the subordinate units. The subordinate units only receive and process packets sent from the primary unit.
<b>Hub</b>	Load balancing if the cluster interfaces are connected to a hub. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet.
<b>Least-Connection</b>	Least connection load balancing. If the cluster units are connected using switches, select Least Connection to distribute network traffic to the cluster unit currently processing the fewest connections.
<b>Round-Robin</b>	Round robin load balancing. If the cluster units are connected using switches, select Round-Robin to distribute network traffic to the next available cluster unit.

<b>Weighted Round-Robin</b>	Weighted round robin load balancing. Similar to round robin, but weighted values are assigned to each of the units in a cluster based on their capacity and on how many connections they are currently processing. For example, the primary unit should have a lower weighted value because it handles scheduling and forwards traffic. Weighted round robin distributes traffic more evenly because units that are not processing traffic will be more likely to receive new connections than units that are very busy.
<b>Random</b>	Random load balancing. If the cluster units are connected using switches, select Random to randomly distribute traffic to cluster units.
<b>IP</b>	Load balancing according to IP address. If the cluster units are connected using switches, select IP to distribute traffic to units in a cluster based on the Source IP and Destination IP of the packet.
<b>IP Port</b>	Load balancing according to IP address and port. If the cluster units are connected using switches, select IP Port to distribute traffic to units in a cluster based on the source IP, source port, destination IP, and destination port of the packet.

Once a packet has been propagated to a subordinate unit, all packets that are part of that same communication session are also propagated to that same subordinate unit. Traffic is distributed according to communication session, not just according to individual packet.

Any subordinate unit that receives a forwarded packet processes it, without applying load balancing. Note that subordinate units are still considered to be active, because they perform routing, virus scanning, and other FortiGate unit tasks on their share of the traffic. Active subordinate units also share their session and link status information with all cluster units. The only things that active members do not do is make load balancing decisions.

Even though the primary unit is responsible for the load balancing process, the primary unit still acts like a FortiGate unit in that it processes packets, performing routing, firewall, virus scanning, and other FortiGate unit tasks on its share of the traffic. Depending on the load balancing schedule used, the primary unit may assign itself a smaller share of the total load.

## Selecting which packets are load balanced

The primary unit processes all UDP and ICMP traffic. By default, the primary unit also processes all TCP traffic and load balances virus scanning traffic among all cluster units. You can change the default configuration so that the cluster load balances both TCP traffic and virus scanning traffic among all cluster units.

Load balancing increases network bandwidth usage and also increases the load on the primary unit CPU. Because of this, in some network environments, load balancing TCP traffic may not result in an overall cluster performance increase. However, in other network environments, TCP load balancing may improve cluster performance.

If the cluster is configured to load balance virus scanning sessions, the primary unit uses the load balancing schedule to distribute HTTP, FTP, SMTP, POP3, and IMAP packets to be virus scanned, among the primary unit and the subordinate units. Load balancing virus scanning traffic is much more likely to increase cluster performance. Virus scanning is processor intensive for the cluster unit that is performing the virus scanning. Distributing virus scanning over the cluster units significantly reduces the processing load on the primary unit. As a result overall cluster performance should improve. See [“Load balancing virus scanning sessions and TCP sessions” on page 124.](#)

## More about active-active failover

If a subordinate unit fails, the primary unit re-distributes the connections that the subordinate unit was processing among the remaining active cluster members. If the primary unit fails, the subordinate units negotiate to select a new primary unit. The new primary unit continues to distribute packets among the remaining active cluster units.

Failover works in a similar way if the cluster consists of only two units. If the primary unit fails the subordinate unit negotiates and becomes the new primary unit. If the subordinate unit fails, the primary unit processes all traffic. In both cases, the single remaining unit continues to function as a primary unit, maintaining the HA virtual MAC address for all of its interfaces.

## Configuring load balancing settings

This section describes how to configure the following load balancing settings:

- [Selecting a load balancing schedule](#)
- [Load balancing virus scanning sessions and TCP sessions](#)
- [Configuring weighted-round-robin weights](#)

### Selecting a load balancing schedule

You can select a load balancing schedule from the web-based manager or the CLI. You can select the load balancing schedule when initially configuring the cluster and you can change the load balancing schedule at any time while the cluster is operating without affecting cluster operation.

#### To select a load balancing schedule from the web-based manager

- 1 Log into the cluster web-based manager.
- 2 Go to **System > Config > HA**.
- 3 Select a schedule from the schedule list.
- 4 Select apply.
- 5 The cluster switches to the new load balancing schedule.  
See [“Schedule” on page 28](#) for descriptions of the load balancing schedules.

#### To select a load balancing schedule from the CLI

- 1 Log into the cluster CLI.
- 2 Select a load balancing schedule. Enter:

```
config system ha
  set schedule <schedule_name>
end
```
- 3 The cluster switches to the new load balancing schedule.  
See [“schedule {hub | ip | ipport | leastconnection | none | random | round-robin | weight-round-robin}” on page 38](#) for descriptions of the load balancing schedules.

## Load balancing virus scanning sessions and TCP sessions

By default a FortiGate active-active cluster load balances virus scanning sessions among all of the cluster units. All other traffic is processed by the primary unit. Using the CLI, you can configure the cluster to load balance TCP traffic among all cluster units in addition to virus scanning sessions. UDP and ICMP traffic is always processed by the primary unit. You can only change load balancing in this way from the CLI.

### To load balancing virus scanning sessions and TCP sessions

- 1 Log into the cluster CLI.
- 2 Enable load balancing virus scanning and TCP sessions. Enter:

```
config system ha
  set load-balance-all enable
end
```

For more information, see [“load-balance-all {disable | enable}” on page 34](#).

## Configuring weighted-round-robin weights

By default, in active-active HA mode the weighted round-robin schedule assigns the same weight to each cluster unit. From the CLI you can use the following command to configure a weight value for each cluster unit.

```
config system ha
  set weight <priority-id_integer> <weight_integer>
end
```

The weight value sets the maximum number of connections that are sent to a cluster unit before a connection can be sent to the next cluster unit. You can set weight values to control the number of connections processed by each cluster unit. For example, you might want to reduce the number of connections processed by the primary unit by increasing the weight assigned to the subordinate units.

Weight values are entered as two values; the priority order of the unit in the cluster (in the range 0 to 31) followed by its weight (also in the range 0 to 31). For example, if you have a cluster of three units, you can enter the following commands to configure the weight values for each unit:

**Table 13: Example weights for three cluster units**

Cluster unit priority	Weight
0	1
1	3
2	3

```
config system ha
  set weight 0 1
  set weight 1 3
  set weight 2 3
end
```

This command has 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.

## NAT/Route mode active-active cluster packet flow

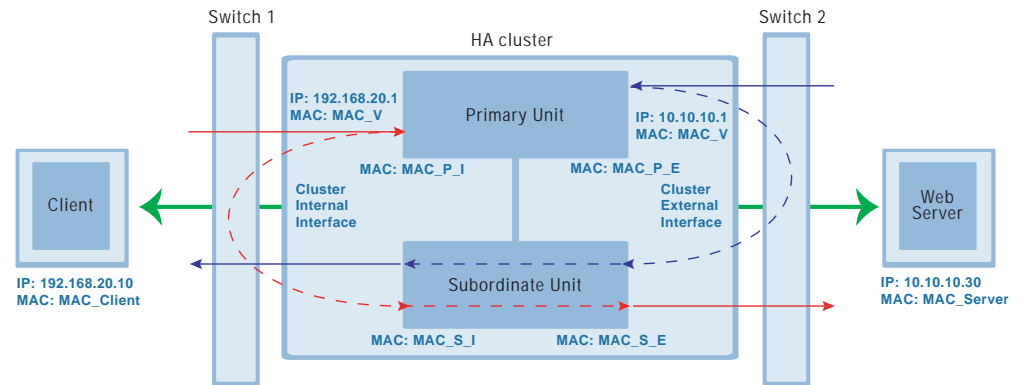
This section describes an example of how packets are load balanced and how failover occurs in an active-active HA cluster running in NAT/Route mode. In the example, the NAT/Route mode cluster acts as the internet firewall for a client computer's internal network. The client computer's default route points at the IP address of the cluster internal interface. The client connects to a web server on the Internet. Internet routing routes packets from the cluster external interface to the web server, and from the web server to the cluster external interface.

In NAT/Route mode, seven MAC addresses are involved in active-active communication between the client and the web server when the primary unit load balances packets to the subordinate unit:

- Virtual MAC address (MAC\_V) assigned to all primary unit interfaces,
- Client MAC address (MAC\_Client),
- Server MAC address (MAC\_Server),
- Primary unit original internal MAC address (MAC\_P\_I),
- Primary unit original external MAC address (MAC\_P\_E),
- Subordinate unit internal MAC address (MAC\_S\_I),
- Subordinate unit external MAC address (MAC\_S\_E).

In NAT/Route mode, the HA cluster works as a gateway when it responds to ARP requests. Therefore, the client and the server only know the gateway MAC address, which is the HA virtual MAC address (MAC\_V). The HA virtual MA address is described in ["Group ID" on page 27](#).

Figure 29: NAT/Route mode active-active packet flow



### Packet flow from client to web server

- 1 The client computer requests a connection from 192.168.20.10 to 10.10.10.30.
- 2 The default route on the client computer recognizes 192.168.20.1 (the cluster IP address) as the gateway to the external network where the web server is located.
- 3 The client computer issues an ARP request to 192.168.20.1.
- 4 The primary unit intercepts the ARP request, and responds with the HA virtual MAC address (MAC\_V) which corresponds to its IP address of 192.168.20.1.
- 5 The client's request packet reaches the primary unit internal interface.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_Client
<b>Destination</b>	10.10.10.30	MAC_V

- 6 The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit internal interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit internal interface.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_P_I
<b>Destination</b>	10.10.10.30	MAC_S_I

- 7 The subordinate unit recognizes that the packet has been forwarded from the primary unit and processes it.
- 8 The subordinate unit forwards the packet from its external interface to the web server.

	IP address	MAC address
<b>Source</b>	10.10.10.1	MAC_S_E
<b>Destination</b>	10.10.10.30	MAC_Server

- 9 The primary unit forwards further packets in the same session to the subordinate unit.
- 10 Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

## Packet flow from web server to client

- 1 When the web server responds to the client's packet, the cluster external interface IP address (10.10.10.1) is recognized as the gateway to the internal network.
- 2 The web server issues an ARP request to 10.10.10.1.
- 3 The primary unit intercepts the ARP request, and responds with the HA virtual MAC address (MAC\_V) which corresponds its IP address of 10.10.10.1.
- 4 The web server then sends response packets to the primary unit external interface.

	IP address	MAC address
<b>Source</b>	10.10.10.30	MAC_Server
<b>Destination</b>	10.10.10.1	MAC_V

- 5 The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit external interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit external interface.

	IP address	MAC address
<b>Source</b>	10.10.10.30	MAC_P_E
<b>Destination</b>	10.10.10.1	MAC_S_E

- 6 The subordinate unit recognizes that packet has been forwarded from the primary unit and processes it.
- 7 The subordinate unit forwards the packet from its internal interface to the client.

	IP address	MAC address
<b>Source</b>	10.10.10.30	MAC_S_I
<b>Destination</b>	192.168.20.10	MAC_Client

- 8 The primary unit forwards further packets in the same session to the subordinate unit.
- 9 Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

## When a failover occurs

- 1 If the primary unit fails, the remaining unit negotiates to become the primary unit.
- 2 The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC address.  
The new primary unit has the same IP address as the failed primary unit.
- 3 The new primary units sends a special ARP request to the 192.168.20.x network to associate its internal IP address with the HA virtual MAC address.
- 4 The new primary units sends a special ARP request to the external network to associate its external IP address with the HA virtual MAC address.
- 5 Traffic sent to the cluster is now received and processed by the new primary unit.  
If there were more than two cluster units in the original cluster, the new primary unit would load balance packets to the remaining cluster members.

## Transparent mode active-active cluster packet flow

This section describes an example of how packets are load balanced and how failover occurs in an active-active HA cluster running in Transparent mode. The cluster is installed on an internal network in front of a mail server and the client connects to the mail server through the Transparent mode cluster.

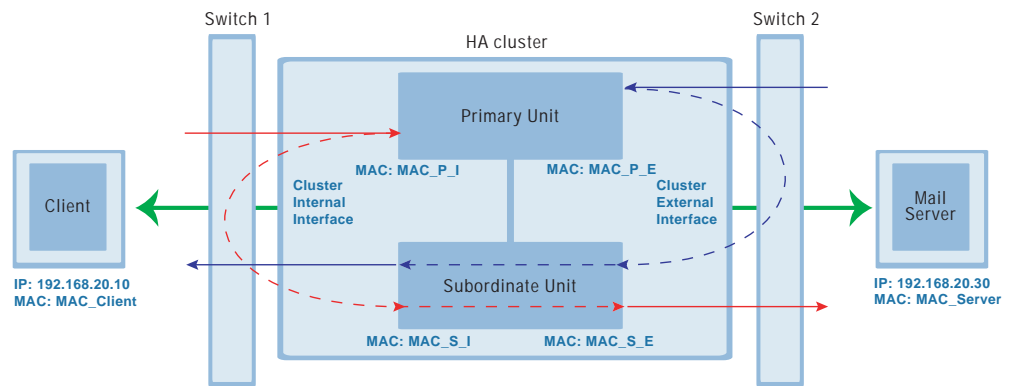
In Transparent mode, six MAC addresses are involved in active-active communication between a client and a server when the primary unit load balances packets to the subordinate unit:

- Client MAC address (MAC\_Client),
- Server MAC address (MAC\_Server),
- Primary unit original internal MAC address (MAC\_P\_I),
- Primary unit original external MAC address (MAC\_P\_E),
- Subordinate unit internal MAC address (MAC\_S\_I),
- Subordinate unit external MAC address (MAC\_S\_E).

The HA virtual MAC address is not directly involved in communication between the client and the server. The client computer sends packets to the mail server and the mail server sends responses. In both cases the packets are intercepted and load balanced among cluster members.

The cluster's presence on the network and its load balancing are transparent to the client and server computers. The primary unit sends special ARP packets to Switch 1 that associate all MAC addresses on the network segment connected to the cluster external interface with the HA virtual MAC address. The primary unit also sends special ARP packets to Switch 2 that associate all MAC addresses on the network segment connected to the cluster internal interface with the HA virtual MAC address. In both cases, this results in the switches sending packets to the primary unit interfaces.

**Figure 30: Transparent mode active-active packet flow**



### Packet flow from client to mail server

- 1 The client computer requests a connection from 192.168.20.10 to 192.168.20.30.
- 2 The client computer issues an ARP request to 192.168.20.30.

- 3 The primary unit forwards the ARP request to the mail server.
- 4 The mail server responds with its MAC address (MAC\_Server) which corresponds to its IP address of 192.168.20.30. The primary unit returns the ARP response to the client computer.
- 5 The client's request packet reaches the primary unit internal interface.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_Client
<b>Destination</b>	192.168.20.30	MAC_Server

- 6 The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit internal interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit internal interface.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_P_I
<b>Destination</b>	192.168.20.30	MAC_S_I

- 7 The subordinate unit recognizes that packet has been forwarded from the primary unit and processes it.
- 8 The subordinate unit forwards the packet from its external interface to the mail server.

	IP address	MAC address
<b>Source</b>	192.168.20.10	MAC_S_E
<b>Destination</b>	192.168.20.30	MAC_Server

- 9 The primary unit forwards further packets in the same session to the subordinate unit.
- 10 Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

## Packet flow from mail server to client

- 1 To respond to the client computer, the mail server issues an ARP request to 192.168.20.10.
- 2 The primary unit forwards the ARP request to the client computer.
- 3 The client computer responds with its MAC address (MAC\_Client) which corresponds to its IP address of 192.168.20.10. The primary unit returns the ARP response to the mail server.
- 4 The mail server's response packet reaches the primary unit external interface.

	IP address	MAC address
<b>Source</b>	192.168.20.30	MAC_Server
<b>Destination</b>	192.168.20.10	MAC_Client

- 5 The primary unit decides that the subordinate unit should handle this packet, and forwards it to the subordinate unit external interface. The source MAC address of the forwarded packet is changed to the actual MAC address of the primary unit external interface.

	IP address	MAC address
<b>Source</b>	192.168.20.30	MAC_P_E
<b>Destination</b>	192.168.20.10	MAC_S_E

- 6 The subordinate unit recognizes that packet has been forwarded from the primary unit and processes it.
- 7 The subordinate unit forwards the packet from its internal interface to the client.

	IP address	MAC address
<b>Source</b>	192.168.20.30	MAC_S_I
<b>Destination</b>	192.168.20.10	MAC_Client

- 8 The primary unit forwards further packets in the same session to the subordinate unit.
- 9 Packets for other sessions are load balanced by the primary unit and either sent to the subordinate unit or processed by the primary unit.

## When a failover occurs

- 1 If the primary unit fails the remaining unit negotiates to become the primary unit.
- 2 The new primary unit changes the MAC addresses of all of its interfaces to the HA virtual MAC address.
- 3 The new primary units sends special ARP requests to switch 1 to associate its MAC address with the MAC addresses on the network segment connected to the external interface.
- 4 The new primary units sends special ARP requests to switch 2 to associate its MAC address with the MAC addresses on the network segment connected to the internal interface.
- 5 Traffic sent to the cluster is now received and processed by the new primary unit. If there were more than two cluster units in the original cluster, the new primary unit would load balance packets to the remaining cluster members.

# HA with third-party products

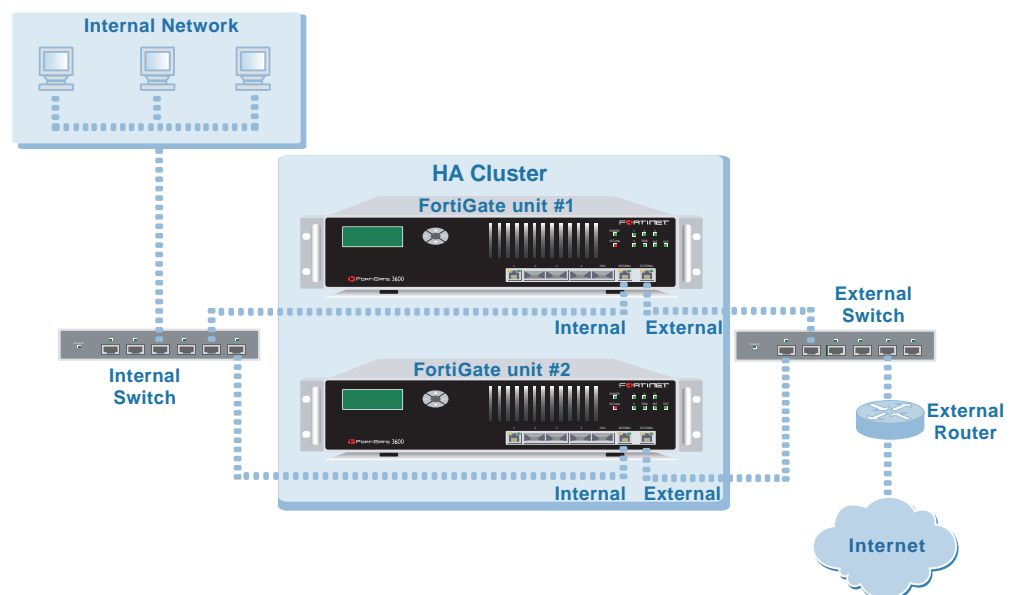
This chapter provides information about operating FortiGate clusters with third party products such as layer-2 and layer-3 switches. This chapter describes:

- [Troubleshooting layer-2 switches](#)
- [Failover issues with layer-3 switches](#)
- [Changing spanning tree protocol settings for some switches](#)
- [Failover and attached network equipment](#)

## Troubleshooting layer-2 switches

Issues may occur because of the way an HA cluster assigns MAC addresses to the primary unit. In a functioning HA cluster, all primary unit interfaces are assigned the same virtual MAC address. This virtual MAC address is in the format 00-09-0f-06-ff-xx. The last byte of the virtual MAC address is the hexadecimal equivalent of the group ID. See “[Group ID](#)” on page 27 for more information about the HA group ID and the virtual MAC address.

**Figure 31: Typical HA configuration, each interface connected to a different switch**



Assigning the virtual MAC addresses in this way results in two restrictions when installing HA clusters:

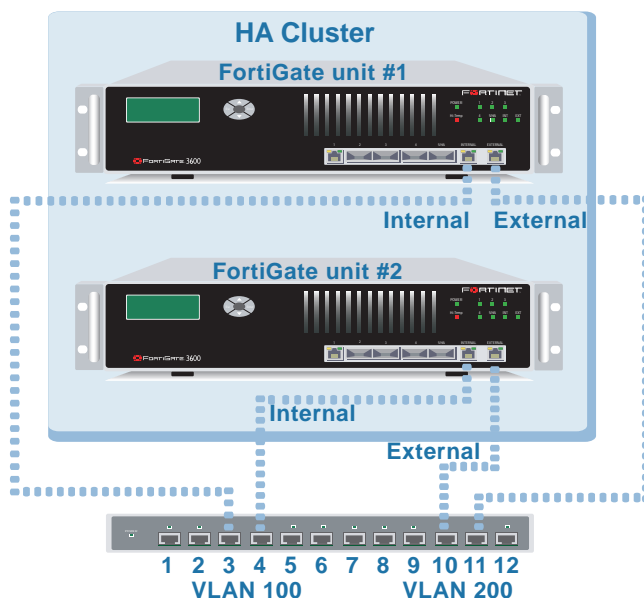
- Two clusters with the same group ID can not connect to the same switch and cannot be installed on the same network unless they are separated by a router.
- Two or more interfaces on the same primary unit cannot be connected to the same switch unless the traffic is separated using VLANs and unless the switch is VLAN-aware.

## Layer-2 switch restrictions

In [Figure 31](#), FortiGate unit #1 and FortiGate unit #2 are running as an HA cluster. The internal interfaces of both FortiGate units are connected to the internal switch. The external interfaces of both FortiGate units connect to the external switch. In this configuration, the HA cluster works with any layer-2 switches from any vendor. There are no issues associated with virtual MAC addresses in this configuration.

In [Figure 32](#), the internal interfaces of both FortiGate units connect to VLAN 100 and the external interfaces of both FortiGate units connect to VLAN 200 of the same switch. This design may have problem depends on the function of the switch.

**Figure 32: Both FortiGate units connected to separate VLANs on the same switch**



If FortiGate unit #1 is the primary unit, then its internal and external interfaces have the same virtual MAC address. The switch detects the same MAC address at interfaces 3 and 11. If the switch's MAC forwarding table recognizes VLANs, separate entries are added to the forwarding table for interface 3 and 11. Interface 3 forwards packets to the virtual MAC address and VLAN 100. Interface 11 forwards packets to the virtual MAC address and VLAN 200.

If the switch supports a global MAC-forwarding table that is not VLAN-aware, the switch detects a MAC address conflict between interface 3 and 11. In this case, only one entry is added to the MAC forwarding table. For some switches, the forwarding interface for the virtual MAC address will be either 3 or 11. For other switches, the forwarding interface for the virtual MAC address alternates between 3 and 11. In either case, the cluster will not function correctly.

If you experience the global MAC-forwarding table problem with the switch that you are using, the current workaround is to use two switches in a configuration similar to [Figure 31](#).

## Configuring layer-2 switch MAC address tables

Some switches support the ability to statically configure MAC addresses to multiple ports. For example many Cisco switches that normally use a global MAC address table will allow use of the command:

```
mac-address-table static hw-addr in-port out-port-list
```

`hw-addr`            The MAC address to add to the address table.

`in-port`            The input port from which packets received with a destination address of `hw-addr` are forwarded to the list of ports in the `out-port-list`. The `in-port` must belong to the same VLAN as all the ports in the `out-port-list`.

`out-port-list`      The list of ports to which packets received on ports in `in-port` are forwarded. All ports in the list must belong to the same VLAN.

## Failover issues with layer-3 switches

After a failover, the new primary unit sends special ARP packets to refresh the MAC forwarding tables of the switches connected to the cluster. If the cluster is connected using layer-2 switches, the MAC forwarding tables are refreshed by the special ARP packets and the switches start directing packets to the new primary unit.

In some configurations that use layer-3 switches, after a failover, the layer-3 switches may not successfully re-direct traffic to the new primary unit. The possible reason for this is that the layer-3 switch might keep a table of IP addresses and interfaces and may not update this table for a relatively long time after the failover (the table is not updated by the special ARP packets). Until the table is updated, the layer-3 switch keeps forwarding packets to the now failed cluster unit. As a result, traffic stops and the cluster does not function.

As of the release date of this document, Fortinet has not developed a workaround for this problem. One possible solution would be to clear the forwarding table on the layer-3 switch.

## Changing spanning tree protocol settings for some switches

Configuration changes may be required when you are running an active-active HA cluster that is connected to a switch that operates using the spanning tree protocol. For example, the following spanning tree parameters may need to be changed:

- Maximum Age** The time that a bridge stores the spanning tree bridge control data unit (BPDU) before discarding it. A maximum age of 20 seconds means it may take 20 seconds before the switch changes a port to the listening state.
- Forward Delay** The time that a connected port stays in listening and learning state. A forward delay of 15 seconds assumes a maximum network size of seven bridge hops, a maximum of three lost BPDUs and a hello-interval of 2 seconds.

For an active-active HA cluster to be compatible with the spanning tree algorithm, the FGCP requires that the sum of maximum age and forward delay should be less than 20 seconds. The maximum age and forward delay settings are designed to prevent layer 2 loops. If there is no possibility of layer 2 loops in the network, you could reduce the forward delay to the minimum value.

For some Dell 3348 switches the default maximum age is 20 seconds and the default forward delay is 15 seconds. In this configuration the switch cannot work with a FortiGate HA cluster. However, the switch and cluster are compatible if the maximum age is reduced to 10 seconds and the forward delay is reduced to 5 seconds.

## Spanning Tree protocol (STP)

Spanning tree protocol is an IEEE 802.1 standard link management protocol that for media access control bridges. STP uses the spanning tree algorithm to provide path redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. Loops can be created if there are more than one route between two hosts. To control path redundancy, STP creates a tree that spans all of the switches in an extended network. Using the information in the tree, the STP can force redundant paths into a standby, or blocked, state. The result is that only one active path is available at a time between any two network devices (preventing looping). Redundant links are used as backups if the initial link should fail. Without spanning tree in place, it is possible that two connections may be simultaneously live, which could result in an endless loop of traffic on the network.

## Bridge Protocol Data Unit (BPDU)

BPDU are spanning tree data messages exchanged across switches within an extended network. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

## 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.



# Index

## A

- active sessions
  - HA cluster members 86
- all 42
- arps 33
- attackdef 42
- authentication 33
- avupd 42

## B

- back to HA configuration page
  - HA cluster members 86

## C

- ca 42
- CLI 85
- cluster
  - definition 10
  - large number of units 61
- cluster configuration
  - synchronizing 10
- cluster ID
  - HA cluster members 86
- cluster members
  - HA 26, 85, 87
- cluster unit
  - definition 11
- config 42
- configuration changes
  - preventing on subordinate units 10
- content summary 84
- CPU usage
  - HA cluster members 86
- customer service 14

## D

- dailover
  - definition 11
- date 83
- device failover
  - definition 11
- DHCP 89

## E

- emaillists 42
- encryption 33

## F

- failover
  - heartbeat 11
  - issues with layer-3 switches 133
  - link 9, 12
- failure
  - definition 11
- FGCP
  - definition 11
- FGT\_ha\_admin 16
- firmware
  - upgrading cluster firmware 87
- FortiGuard 89
- FortiLog 92
- Fortinet customer service 14
- FortiProtect Distribution Network 89
- FortiShield 89

## G

- go
  - HA cluster members 86
- group ID
  - HA 27
- groupid 33

**H**

- HA 26
  - cluster members 26, 85, 87
  - configure weighted-round-robin weights 124
  - group ID 27
  - HA monitor 85, 87
  - heartbeat failover 18
  - link failover scenarios 111
  - manage individual cluster units 88
  - mode 26
  - monitor priorities 32
  - override master 28
  - password 28
  - priorities of heartbeat device 29
  - schedule 28
  - unit priority 27
  - view the status of each cluster member 85, 87
- ha
  - arps 33
  - authentication 33
  - encryption 33
  - groupid 33
  - hb-interval 33
  - hb-lost-threshold 33
  - hello-holddown 34
  - load-balance-all 34
  - mode 35
  - monitor 35
  - override 35
  - password 35
  - priority 36
  - route-hold 36
  - route-ttl 36
  - route-wait 37
  - schedule 38
  - weight 39
- HA cluster members
  - active sessions 86
  - back to HA configuration page 86
  - cluster ID 86
  - CPU usage 86
  - go 86
  - intrusion detected 87
  - memory usage 86
  - monitor 86
  - network utilization 86
  - refresh every 86
  - status 86
  - total bytes 87
  - total packets 86
  - up time 86
  - virus detected 86
- HA heartbeat
  - definition 11
  - encryption 10
  - timing 10
- HA virtual MAC address
  - definition 11

- ha\_admin
  - administrator account 88, 90
- hbdev 34
- hb-interval 33
- hb-lost-threshold 33
- heartbeat
  - definition 11
  - failover 18
- heartbeat device
  - definition 11
- heartbeat failover
  - definition 11
- hello-holddown 34
- High Availability 26
- high availability
  - definition 12
- hub
  - HA schedule 28, 121

**I**

- interface status 84
- intrusion detected
  - HA cluster members 87
- IP 29, 122
- IP port
  - HA schedule 29, 122
- IPSec VPN monitor 84

**L**

- L2TP 89
- large number of units to a cluster 61
- layer-2 switch
  - MAC address tables 133
  - troubleshooting 131
- layer-3 switch
  - failover issues 133
  - troubleshooting 131
- LDAP 90
- Least-Connection
  - HA schedule 28, 121
- link failover 9
  - definition 12
- load balancing
  - definition 12
- load-balance-all 34
- localcert 42

**M**

- MAC address table
  - layer-2 switch 133
- manage cluster units
  - HA 88
- memory usage
  - HA cluster members 86
- mode 35
  - HA 26

- monitor 35
  - HA 85, 87
  - HA cluster members 86
  - router 84
  - VPN 84
- monitor priorities
  - HA 32
- monitored interface
  - definition 12
- multiple heartbeat devices 9

## N

- NAT/Route mode
  - general configuration steps 45, 62
  - HA network topology 44, 62
  - web-based manager configuration steps 45, 64
- network topology
  - NAT/Route mode HA 44, 62
- network utilization
  - HA cluster members 86
- none
  - HA schedule 28, 121

## O

- override 35
- override master
  - HA 28

## P

- password 35
  - HA 28
- PPP 89
- PPPoE 89
- PPTP 89
- primary cluster unit
  - definition 12
- primary unit
  - definition 12
- primary unit selection 9
- priorities of heartbeat device 29
- priority 36

## R

- RADIUS 90
- random
  - HA schedule 29, 122
- recent intrusion detections 84
- recent virus detections 84
- refresh every
  - HA cluster members 86
- Round-Robin
  - HA schedule 28, 121
- route-hold 36
- router monitor 84

- route-ttl 36
- route-wait 37
- routing table
  - synchronizing changes 10

## S

- schedule 38
  - HA 28
- standalone mode 26
- start 42
- state synchronization
  - definition 13
- status
  - HA cluster members 86
  - system 84
- stop 42
- subordinate cluster unit
  - definition 13
- subordinate unit
  - allowed configuration changes 88
  - configuration changes 88
  - definition 13
  - preventing configuration changes 88
- synchronize
  - cluster configuration 10
- system date 83
- system resources 84
- system status 84
- system status session 84
- system time 83

## T

- technical support 14
- time 83
- timing
  - HA heartbeat 10
- total bytes
  - HA cluster members 87
- total packets
  - HA cluster members 86
- Transparent mode 53
  - CLI configuration steps 48, 55, 69
  - general configuration steps 52
  - web-based manager configuration steps 53
- troubleshooting
  - layer-2 switch 131
  - layer-3 switch 131

## U

- unit priority
  - HA 27
- up time
  - HA cluster members 86
- upgrade
  - cluster firmware 87

**V**

virtual MAN address  
    definition 11  
virus detected  
    HA cluster members 86  
VPN monitor 84

**W**

web-based manager 84

web-based manager configuration steps 53  
    NAT/Route mode 45, 64  
weblists 42  
weight 39  
weighted round-robin  
    HA schedule 29, 122  
weighted-round-robin  
    configuring weights 124