



# FortiGate High Availability Overview

## Technical Note

|  |   |
|--|---|
| <i>FortiGate High Availability Overview Technical Note</i> |   |
| <b>Document Version:</b>                                   | 1   |
| <b>Publication Date:</b>                                   | February 22, 2005   |
| <b>Description:</b>  | This document provides an overview for FortiGate FortiOS v2.80 High Availability. |
| <b>Product:</b>  | FortiOS v2.80 MR8   |
| <b>Document Number:</b>                                    | 01-28008-0177-20050222  |

**Fortinet Inc.**

*FortiGate High Availability Overview Technical Note*

FortiOS v2.80

22 February 2005

01-28008-0177-20050222

© 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.

**Trademarks**

ABACAS, APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Table of Contents

|  |           |
|--|-----------|
| <b>Introduction .....</b>                                    | <b>5</b>  |
| This document .....  | 6         |
| FortiGate HA terminology .....                               | 6         |
| FortiGate documentation .....                                | 9         |
| Related documentation .....                                  | 9         |
| FortiManager documentation .....                             | 10        |
| FortiClient documentation .....                              | 10        |
| FortiMail documentation.....                                 | 10        |
| FortiLog documentation .....                                 | 10        |
| Fortinet Knowledge Center .....                              | 11        |
| Comments on Fortinet technical documentation.....            | 11        |
| Customer service and technical support.....                  | 11        |
| <b>FortiGate HA features .....</b>                           | <b>13</b> |
| FGCP heartbeat.....  | 13        |
| Heartbeat devices .....                                      | 14        |
| Heartbeat device IP addresses.....                           | 15        |
| Primary unit selection.....                                  | 16        |
| Active-passive HA (failover protection) .....                | 17        |
| Active-active HA (load balancing and failover) .....         | 18        |
| HA device and link failover.....                             | 18        |
| Device failover .....  | 18        |
| Link failover .....  | 19        |
| Failover and attached network equipment .....                | 21        |
| FortiGate HA compatibility with PPP protocols.....           | 21        |
| <b>Installation and configuration examples .....</b>         | <b>23</b> |
| Basic NAT/Route mode installation .....                      | 23        |
| Example NAT/Route mode HA network topology .....             | 23        |
| Configuring a NAT/Route mode active-active HA cluster .....  | 24        |
| Basic Transparent mode installation.....                     | 31        |
| Example Transparent mode HA network topology .....           | 31        |
| Configuring a Transparent mode active-active HA cluster..... | 32        |
| Converting a standalone FortiGate unit to a cluster.....     | 37        |
| Adding a new unit to an operating cluster.....               | 39        |

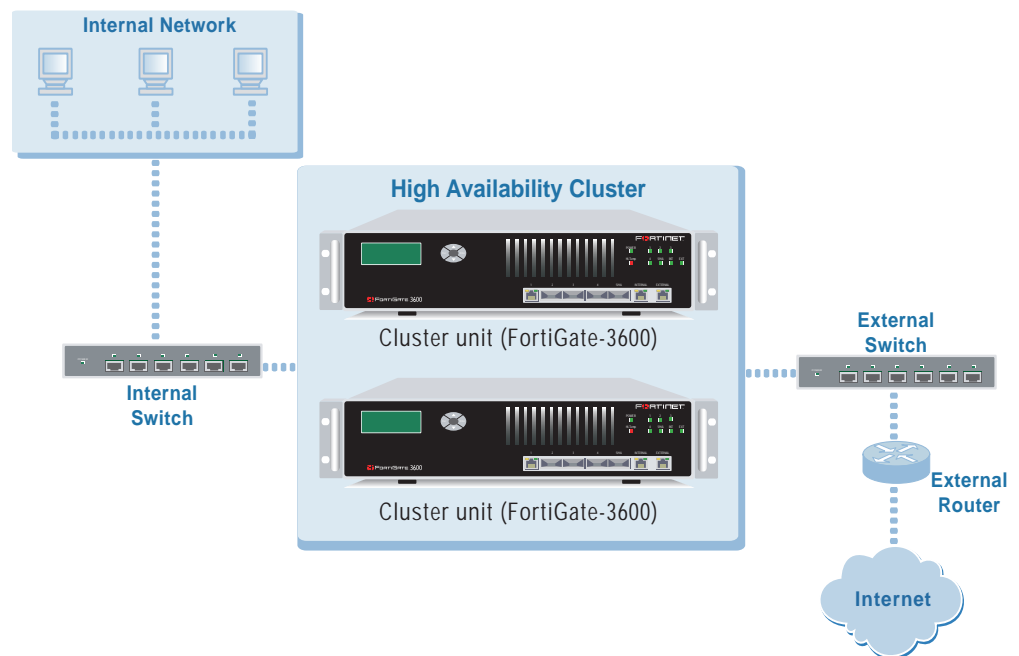


# Introduction

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 protection, 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 Overview Technical Note* contains basic descriptions of how FortiGate HA operates. This document also contains some useful configuration examples. However, this document does not describe HA configuration settings or how to manage a FortiGate cluster in HA mode. For detailed information about HA configuration settings, see your FortiGate unit online help or your [FortiGate Administration Guide](#). For a complete description of FortiGate HA, see the [FortiOS v2.80 HA Guide](#).

This document contains the following chapters:

- [Introduction](#) (this chapter) briefly introduces HA, describes new v2.80 HA features, and defines the HA-related terminology used in this document.
- [FortiGate HA features](#) describes the FGCP clustering protocol and its features, including the HA heartbeat, primary unit selection, device and link failover, and introduces the active-passive and active-active HA modes.
- [Installation and configuration examples](#) contains a NAT/Route mode and a Transparent mode HA installation and configuration example.

## 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.

---

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

## **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.

## **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.

## **High availability**

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

## **Link failover**

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

## Load balancing

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

## Monitored interface

An interface that is 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.

## 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

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*  
Provide 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.
- *FortiGate High Availability Guide*  
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS Guide*  
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate VPN Guide*  
Explains how to configure VPNs using the web-based manager.
- *FortiGate VLANs and VDOMs User Guide*  
Explains how to configure FortiGate virtual lans (VLANs) and Vdoms (Virtual domains). Includes detailed configuration examples.

## Related documentation

Additional information about Fortinet products is available from the following related documentation.

## FortiManager documentation

- *FortiManager QuickStart Guide*  
Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.
- *FortiManager System Administration Guide*  
Describes how to use the FortiManager System to manage FortiGate devices.
- *FortiManager System online help*  
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the FortiManager Console as you work.

## FortiClient documentation

- *FortiClient Host Security User Guide*  
Describes how to use FortiClient Host Security software to set up a VPN connection from your computer to remote networks, scan your computer for viruses, and restrict access to your computer and applications by setting up firewall policies.
- *FortiClient Host Security online help*  
Provides information and procedures for using and configuring the FortiClient software.

## FortiMail documentation

- *FortiMail Administration Guide*  
Describes how to install, configure, and manage a FortiMail unit in gateway mode and server mode, including how to configure the unit; create profiles and policies; configure antispam and antivirus filters; create user accounts; and set up logging and reporting.
- *FortiMail online help*  
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Web Mail Online Help*  
Describes how to use the FortiMail web-based email client, including how to send and receive email; how to add, import, and export addresses; and how to configure message display preferences.

## FortiLog documentation

- *FortiLog Administration Guide*  
Describes how to install and configure a FortiLog unit to collect FortiGate and FortiMail log files. It also describes how to view FortiGate and FortiMail log files, generate and view log reports, and use the FortiLog unit as a NAS server.
- *FortiLog online help*  
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

## Fortinet Knowledge Center

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

## Comments on Fortinet technical documentation

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

**[amer\\_support@fortinet.com](mailto:amer_support@fortinet.com)** For customers in the United States, Canada, Mexico, Latin America and South America.

**[apac\\_support@fortinet.com](mailto:apac_support@fortinet.com)** For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia.

**[eu\\_support@fortinet.com](mailto:eu_support@fortinet.com)** 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 HA features

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 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. During cluster operation, the FGCP shares communication and synchronization information among the cluster units. This communication and synchronization is called the FGCP heartbeat or the HA heartbeat. Often, this is shortened to just heartbeat.

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

This chapter contains basic descriptions of the following FortiGate HA clustering features. For more information these features and about FortiGate HA clustering, see the [FortiOS v2.80 HA Guide](#).

- [FGCP heartbeat](#)
- [Heartbeat devices](#)
- [Primary unit selection](#)
- [Active-passive HA \(failover protection\)](#)
- [Active-active HA \(load balancing and failover\)](#)
- [HA device and link failover](#)
- [FortiGate HA compatibility with PPP protocols](#)

## FGCP heartbeat

The FGCP heartbeat keeps the 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.

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.

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.

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

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

## 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**

The screenshot shows the FortiGate configuration interface for High Availability. The 'High Availability' mode is selected, with 'Active-Active' as the HA mode. The Group ID is 34 and the Unit Priority is 128. The 'Override master' checkbox is unchecked. The Password and Retype Password fields are masked with asterisks. The Schedule is set to Round-Robin. Below these settings is a table for configuring heartbeat device priorities for various interfaces.

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

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

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.

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 have a heartbeat device priority. And this interface of all of the 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. In HA mode 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 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.

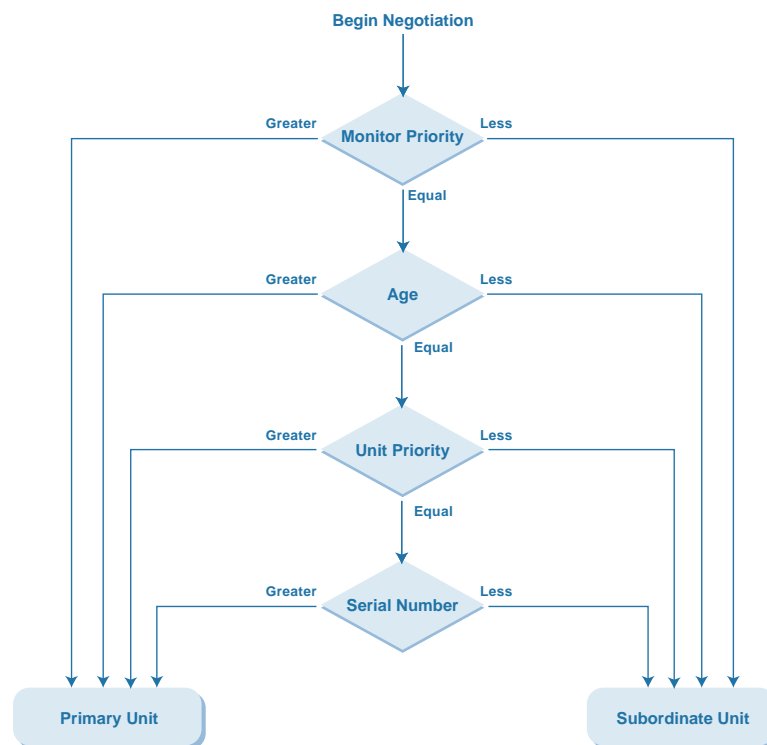
For most FortiGate models if you do not change the heartbeat device configuration, you would isolate the HA interfaces of all of the cluster units by connecting them all to the same switch. If the cluster consists of two FortiGate units you can connect the heartbeat device interfaces directly using a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

## 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 the factors 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. Cluster units that have been operating in a cluster longer are more likely to become the primary unit.

- Unit Priority** The unit priority set by the administrator. Cluster units with a higher 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 one of the cluster units. The unit with the highest unit priority always becomes the primary unit when the cluster starts up.
- Serial Number** The FortiGate unit serial number. Cluster units with higher serial numbers are more likely to become the primary unit. When first configuring the FortiGate units to be added to a cluster, if you do not change the monitor priority or unit priority, then the FortiGate unit with the highest serial number always becomes the primary unit.

Primary unit selection also takes place if a primary unit fails (device failover) or if a primary unit interface fails (link failover). During a device or link failover, the cluster renegotiates to select a new primary unit using the same criteria as the initial negotiation. After the cluster selects the primary unit, all of the remaining units become subordinate units.

The FGCP assigns a virtual MAC address to all of the primary unit interfaces. 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 MAC address change. As a result, the switches send 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.

## Active-passive HA (failover protection)

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

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

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

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

Use active-passive HA for a more resilient session failover environment than active-active HA. In active-passive HA, session failover occurs for all traffic. Active-active HA (described below) 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 this limitation, active-active HA is a less robust failover solution than active-passive HA.

## HA device and link failover

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

FortiOS HA failover maintain 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, the cluster also records log messages about the event and can be configured to send log messages to a syslog server and to a FortiLog unit. The cluster can also send SNMP traps. This information can be used by network administrators to find and fix the problem that caused the failure.

## Device failover

Device failover means that if a 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. If a cluster unit fails, this session table information is available to the remaining cluster units, and these cluster units and resume communication sessions without interruption.

As we have seen, a cluster consists of a primary unit and one or more subordinate units. The 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 16](#). 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 16](#). 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 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. 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 failure of the network interface hardware. The cluster can also determine if individual network interfaces are disconnected from the switch they should be connected to. Note, the cluster cannot determine if the switch that cluster interfaces are connected to is still connected to the network.

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

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

If monitored interface on the primary unit fails, the cluster renegotiates to select a new primary unit using the process described in “Primary unit selection” on page 16. Because the cluster unit with the failed monitored interface has the lowest monitor priority, a different cluster unit becomes the primary unit. The cluster maintains all communication sessions in the same manner as for a device failure.

If a monitored interface on a subordinate unit fails, this information is shared with all cluster units. The cluster does not renegotiate. The cluster unit with the failed monitored link 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.

### Multiple link failures

Every time a monitored interface fails, the cluster repeats the processes described above. If multiple monitored interfaces fail on more the one cluster unit, the cluster continues to negotiate to select a primary unit that can provide the best service to the highest priority networks.

Figure 4: Example FortiGate-500 HA configuration with monitor priorities set

The screenshot shows the FortiGate configuration page for High Availability. The 'High Availability' mode is selected. The 'Cluster Members' section is expanded, showing 'Active-Active' mode, Group ID 34, and Unit Priority 128. Below this is a table for configuring heartbeat device and monitor priorities for various interfaces.

| 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     |  |                            |

## 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.

## FortiGate HA compatibility with PPP protocols

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

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

PPTP and L2TP 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. However, during a failover, any active PPTP and L2TP sessions are lost and must be restarted after the failover.



# 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 your [FortiGate Administration Guide](#).

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](#)

## Basic NAT/Route mode installation

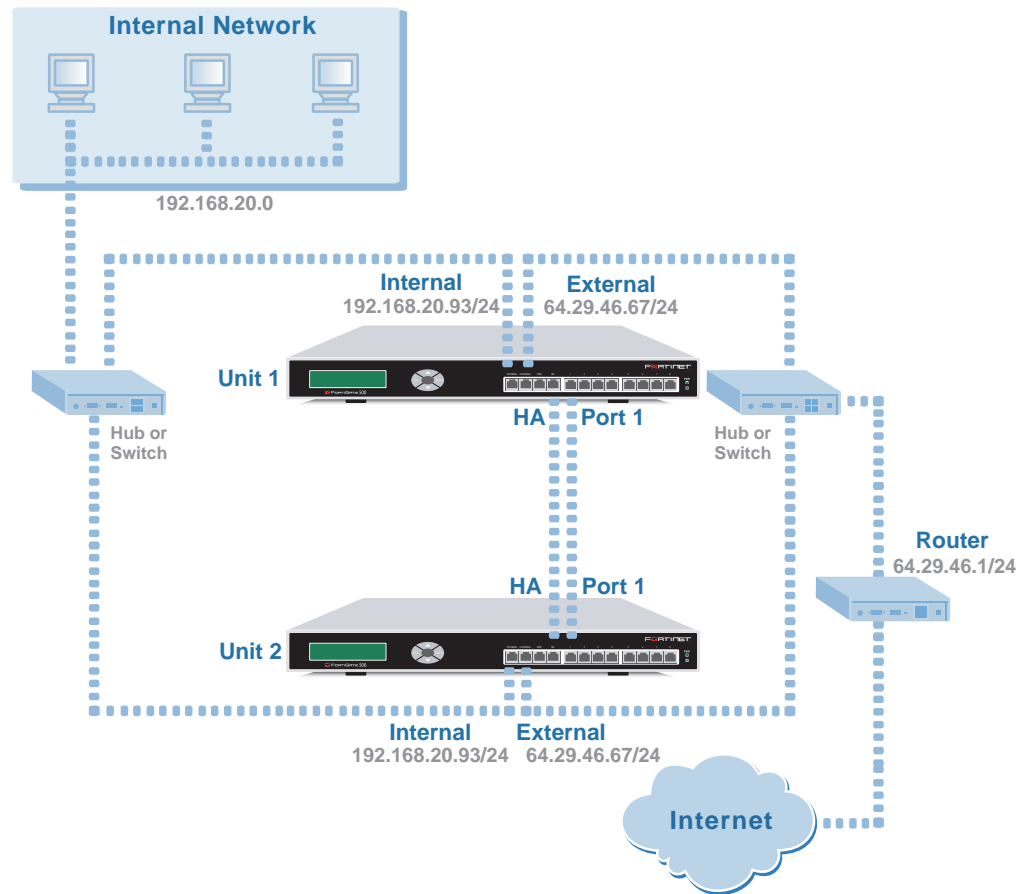
This section describes a simple HA network topology that includes an HA cluster of two FortiGate-500 units installed between an internal network and the Internet.

- [Example NAT/Route mode HA network topology](#)
- [Configuring a NAT/Route mode active-active HA cluster](#)

### Example NAT/Route mode HA network topology

[Figure 5](#) 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 5: 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 5). 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.

## Configuring a NAT/Route mode active-active HA cluster

This section describes how to configure an active-active HA cluster to run in NAT/Route mode using the topology shown in Figure 5. The section includes web-based manager and CLI procedures. These procedures assume that the FortiGate-500s are running the same v2.80 firmware build and are set to the factory default configuration.

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

## General configuration steps

- 1 Configure the FortiGate units for HA operation.
  - 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.



**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.

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 6: Example active-active HA configuration**

| 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     |  |                            |

- 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. You could also use a switch and two ethernet cables.
  - Connect the Port 1 interfaces of the FortiGate units to each other using a cross-over cable. You could also use a switch and two ethernet cables.
- 2 Power on 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 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

### 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 27](#).

**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

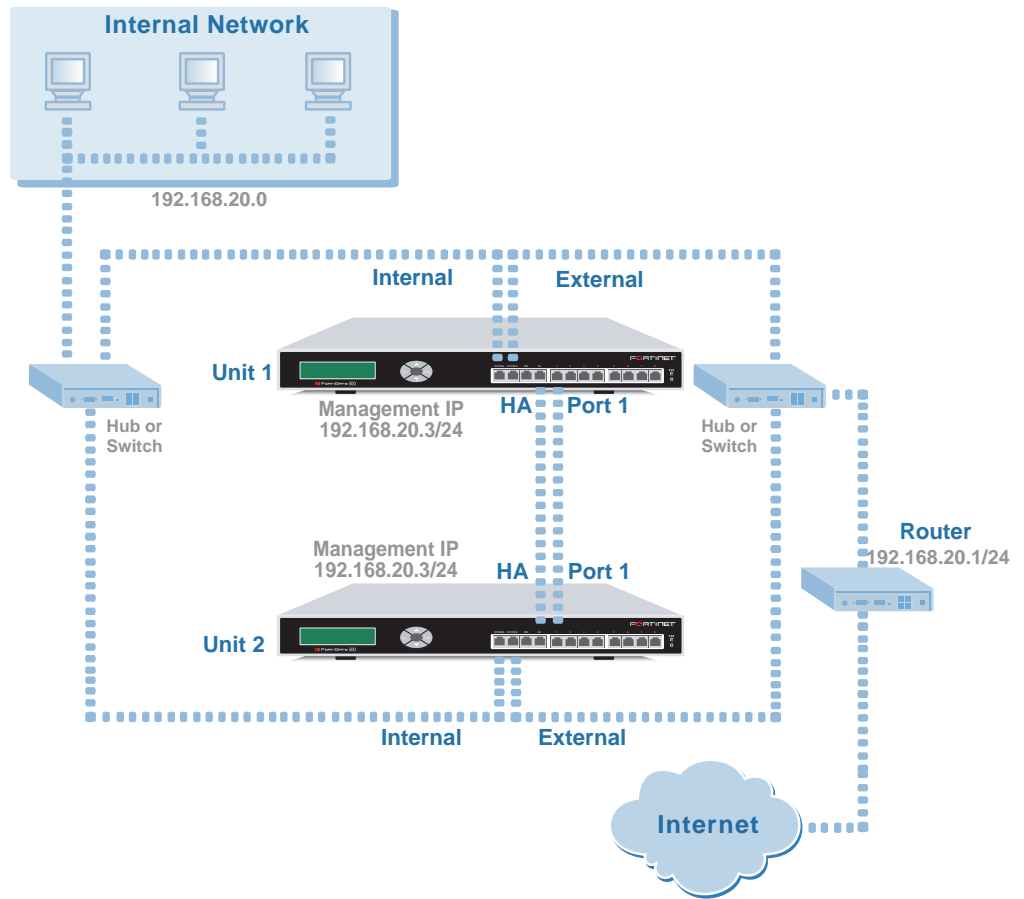
This section describes a simple HA network topology that includes an HA cluster of two FortiGate-500 units installed between an internal network and the Internet and running in Transparent mode.

- [Example Transparent mode HA network topology](#)
- [Configuring a Transparent mode active-active HA cluster](#)

### Example Transparent mode HA network topology

Figure 7 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 7: 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 7](#)). 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.

## Configuring a Transparent mode active-active HA cluster

This section describes how to configure an active-active HA cluster to run in Transparent mode using the topology shown in [Figure 7](#). The section includes web-based manager and CLI procedures. These procedures assume the FortiGate-500s are running FortiOS v2.80 MR3 firmware and set to the factory default configuration.

### General configuration steps

- 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 HA operation.

#### 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.

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. You could also use a switch and two ethernet cables.
  - Connect the Port 1 interfaces of the FortiGate units to each other using a cross-over cable. You could also use a switch and two ethernet cables.

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

#### To 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

#### 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 33](#).
- 2 Power on all of the HA units in the cluster.  
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 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

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

General configuration steps:

- Configure the original FortiGate unit for HA operation.
- Set the HA Unit Priority of the original FortiGate unit to 255 to make sure that this FortiGate unit becomes the primary unit.  
After negotiation the configuration of the original FortiGate unit is synchronized to all cluster units.
- Back up the configuration of the original FortiGate unit.
- Configure one or more new FortiGate units with the same HA configuration as the original FortiGate unit with one exception. Keep the Unit Priority at the default setting, which is 128.
- Connect the FortiGate units into a cluster and connecting the cluster to your network.

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

The new FortiGate units must:

- Be the same FortiGate model as the original FortiGate unit.
- Have the same hard drive configuration as the original FortiGate unit.
- Be running the same firmware version and build as the original FortiGate unit.

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

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

### To configure the original FortiGate unit for HA operation

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

|                        |   |
|------------------------|---|
| <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

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

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



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



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

### To add the new unit to a cluster

- 1 Configure the new cluster unit with the same HA configuration as the other units in the cluster.

- 2 Connect the new cluster unit to the cluster.

For example, to add a new unit to the FortiGate-500 cluster shown in [Figure 5](#) or [Figure 6](#):

- 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.