

WatchGuard[®] High Availability Guide

High Availability for WatchGuard System Manager



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2007 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*.

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Software Version: WFS 7.5

Document Version: HighAvailability-7.5-1

WatchGuard® High Availability Guide

The WatchGuard® High Availability upgrade enables the installation of two Fireboxes on one network in a failover configuration with one Firebox® in active mode and the other in standby mode. The standby Firebox activates when the active Firebox goes off line. After a Firebox becomes active, it stays active until it goes off line and the standby Firebox starts as the active unit. The two Fireboxes in a High Availability pair must have the same configuration file. High Availability is easy to set up and makes sure that your network firewall stays in operation.

NOTE

In this User Guide, the word Firebox refers to a Firebox® III or a Firebox® X hardware device unless we tell you differently. Illustrations of Fireboxes are interchangeable unless we tell you differently.

The High Availability Failover Process

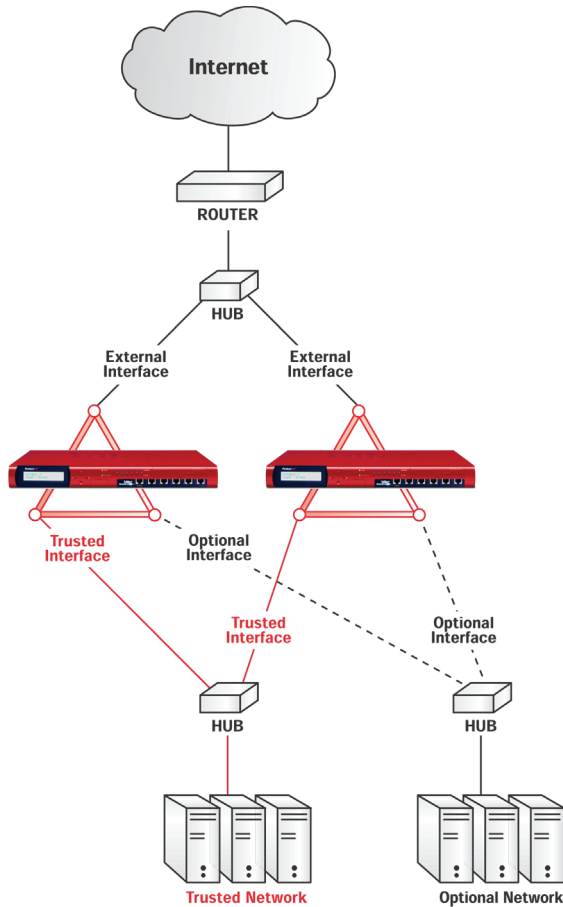
To create a High Availability pair, you must have two Firebox® devices that are the same model. One is the active Firebox and the other is the standby Firebox. The relationship between the active Firebox and the standby Firebox is dynamic. When the

Firebox starts, it becomes the active Firebox. If two Firebox devices start at the same time, they negotiate active and standby status.

If both of the Firebox devices are active and connected to the network, one Firebox restarts in standby mode. This is referred to as High Availability stand down.

Each Firebox must use the same method to connect to the network. For example, if the external interface of the first Firebox connects to a hub or switch, then you must connect the external interface of the second Firebox to the same hub or switch. Repeat for each Firebox interface.

This figure shows a network with a High Availability pair:



You can use any Firebox interface for the High Availability connection between the two Firebox devices. The default configuration uses the trusted interfaces. The standby Firebox must use a reserved IP address on the same subnet as the High Availability interface on the active Firebox. This allows the active Firebox and the standby Firebox to send and receive connection information:

- ARP packets which are known as High Availability heartbeats

-
- TCP connection state information

The standby Firebox sends out ARP packets on the network at a five second interval. These packets request the MAC address of the active Firebox. Then the active Firebox replies with its MAC address. If the standby Firebox does not receive two consecutive responses, it thinks the active Firebox is off line. The standby Firebox then goes to active mode. It starts with the last known TCP connection information sent by the off line Firebox.

NOTE

Because the heartbeat is a Layer 2 broadcast, a switch or other device that operates between the two Firebox heartbeat interfaces must send and receive Layer 2 broadcasts. WatchGuard recommends that the heartbeat interfaces are connected with a hub, and not a switch, for this reason. See your switch documentation to see if it allows Layer 2 broadcasts.

The TCP connection state information is the most current information about the TCP connections on the active Firebox. The standby Firebox requests the TCP connection state information from the active Firebox. The active Firebox sends this data on TCP port 4105.

The two Firebox devices in a High Availability pair must have the same configuration. To put a new configuration file on to the pair:

The management station must have a connection to each Firebox. The management station must also be on the same subnet as the interfaces that the Firebox devices use for High Availability.

First, save the configuration file to the management station before you save the file to the Firebox devices. If you try to upload a configuration file directly from a public folder on a network, the file only goes on the active Firebox.

Installing High Availability

When you buy the High Availability upgrade, you receive a certificate. Use the instructions on the certificate to go to the LiveSecurity® Service Web site and activate your upgrade. After you activate the upgrade, you get a High Availability license key. You must add a unique High Availability license key to each Firebox in the High Availability pair.

Also, each Firebox® in the pair must have the same version of WatchGuard System Manager software and firmware. You must install the same upgrades on the active Firebox and the standby Firebox.

NOTE

The Firebox X models use a different High Availability license for each Firebox. The same High Availability license is used for two Firebox III models. This is because Firebox X license keys are associated with the unit serial number.

You must register each Firebox at the LiveSecurity Web site. When you go to the WatchGuard Web site to register a High Availability license for the Firebox X model, you select one Firebox as the active unit and you select the other Firebox as the standby unit. Then a new Feature Key is generated at the LiveSecurity Web site.

Most of the options you purchase for a Firebox X are copied to the standby unit when LiveSecurity makes the new Feature Key. This Feature Key turns on most of the same features for the standby Firebox X unit as you have on the active Firebox. Here are the exceptions:

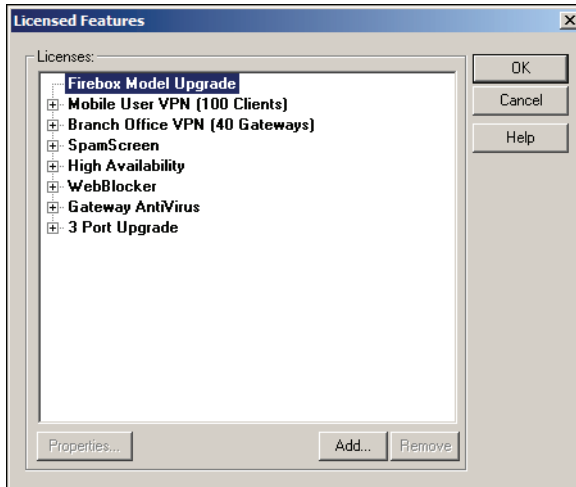
- You must purchase and activate a High Availability license for each Firebox X unit.
- If you apply a model upgrade to one Firebox, then a Firebox model upgrade must be purchased and applied for the standby box, too. For example, if the active Firebox is a Firebox X500 that you upgraded to a Firebox X700, and the partner High Availability Firebox you select is a Firebox X500, you must first upgrade the standby unit to a Firebox X700.

Any other license that is on the active Firebox, such as WebBlocker or SpamScreen or Gateway AntiVirus, is sent to the standby Firebox Feature Key when you activate the High Availability license for the active box.

After you register the High Availability License, get the new Feature Key. You use the same Feature Key for each unit in a High Availability pair. For information about importing a Firebox Feature Key, see the FAQ:

https://www.watchguard.com/support/advancedfaqs/fbx_featurekey.asp

- 1 From Policy Manager, click **Setup > Licensed Features**.
The Licensed Features dialog box appears.



- 2 Click **Add**.
The Add/Import License Keys dialog box appears.
- 3 In the **Add/Import License Keys** dialog box, type or paste the Feature Key you get from the LiveSecurity Web site.
You can also click Browse to find a text file with the license keys.
- 4 Click **OK**.
The High Availability license appears on the Licensed Features dialog box.

Connecting Fireboxes in a High Availability Pair

You must install one of the Fireboxes first. Then you add the Feature Key that turns on High Availability. Then you can configure the second Firebox using the High Availability Wizard or you can configure it manually.

If you do not have a Firebox installed

If you have two new Fireboxes and each Firebox is not installed, you first install one of the two Fireboxes. Use the QuickSetup Wizard to make an initial configuration file and save it to one Firebox. Then import the Feature Key as described above and save the configuration to the Firebox. This turns on the High Availability feature. Continue to the section “Configuring High Availability,” on page 7.

If you have one Firebox installed now.

If you have one Firebox installed but did not start on High Availability for this Firebox, import the Feature Key as described above and save the configuration to the installed Firebox.

Configuring High Availability

There are two methods to configure High Availability. Both methods require that your management station is connected to the standby Firebox with the blue serial cable. Connect one end of the serial cable to the Firebox’s Console port. Connect the other end of the serial cable to the management station’s COM1 port.

If you do not have the blue serial cable that comes with the Firebox, use a null-modem serial cable.

Your management station computer must also be connected to the same Ethernet network as the Firebox.

- 1 You can use the Quick Setup Wizard to install High Availability. When you use this method, both Fireboxes must be connected to the network. The High Availability interface must be the trusted interface.
- 2 You can use the manual method to install High Availability. To use this method it is not necessary that the standby

Firebox is connected to the network. Any Firebox interface can be the High Availability interface.

If you use the manual method and the standby Firebox is not connected to the network, connect a crossover Ethernet cable between the management station and the standby Firebox trusted interface.

NOTE

Each Firebox in a High Availability pair has a different IP address. You must not let a device on the same subnet as the High Availability pair use the Firebox IP addresses. This can cause the traffic between the two devices to stop, and the active Firebox to start a failover to the standby Firebox.

Configuring High Availability with the wizard

Preparation

Before you configure your network for High Availability, make sure that:

- You have the High Availability Feature Keys from the LiveSecurity Web site
- The two Firebox devices are the same model
- The active Firebox is turned on
- The standby Firebox is turned off
- The management station computer is connected to the standby box using the blue serial cable
- The two Firebox devices are connected with Ethernet cables to the network

Each Firebox must use the same method to connect to the network. For example, if the external interface of the first Firebox connects to a hub or switch, then you must connect the external interface of the second Firebox to the same hub or switch. Repeat for each Firebox interface.

The High Availability interface will be the trusted interface.

Configuring using the Wizard

- 1 Click **Start > Programs > WatchGuard > QuickSetup Wizard**.

The QuickSetup Wizard appears.

- 2 From the drop-down list, select Click **Establish a High-Availability Firebox Cluster**. Click **Next**.

The High Availability Configuration screen appears.
- 3 Type the IP address of the active Firebox in the **Active Firebox IP Address** field.

This must be the trusted interface IP address of the active Firebox.
- 4 In the **Stand-By IP Address** field, type an unused IP address from the same subnet as the High Availability interface on the active Firebox.

The default is the trusted interface.
- 5 Click **Next**.

The Enter Active Firebox Passwords screen appears.
- 6 Type the Firebox status passphrase twice.

The status passphrase is the read-only passphrase for the active Firebox.
- 7 Type the Firebox configuration passphrase twice.

The configuration passphrase is the read-write passphrase for the active Firebox.
- 8 Click **Next**.

The Copy Active Firebox Setup for Fail-safe Operation screen appears.
- 9 From the drop-down list, select the Serial Cable method to connect the two Firebox devices. You must also select the computer's serial port from the drop-down list.
- 10 Type the temporary IP address for the standby Firebox.

You must use an IP address that is different from the management station IP address but is on the same subnet. This IP address can not be the same IP address as the standby Firebox.
- 11 Click **Next**.
- 12 When the Wizard tells you, turn on the standby Firebox.
- 13 The Wizard identifies the Fireboxes and shows you the High Availability Feature Keys. If you have not entered the High Availability Feature Keys, you must do that now.
- 14 Click **OK**.
- 15 The Wizard configures both boxes and both boxes start again. The standby box will start in standby mode and the active box will start in active mode.

The configuration is complete.

Configuring High Availability manually

You usually use this method to configure the standby box when the standby box is not connected to the network.

Preparation

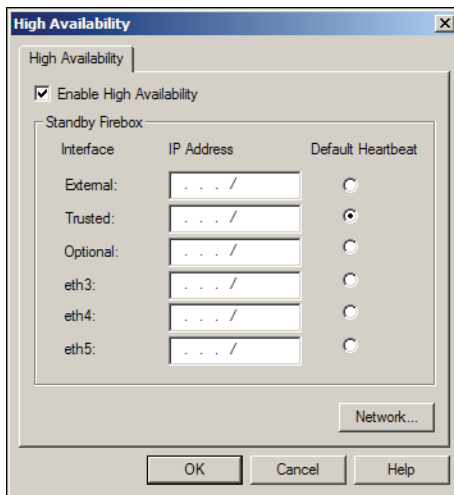
Before you manually configure your standby Firebox for High Availability, make sure that:

- The active Firebox has been configured with the High Availability Feature Key. See “Installing High Availability,” on page 5
- Your management station computer has the current configuration file for the active Firebox.
- The two Firebox devices are the same model.
- You have the Feature Key that turns on High Availability.
- The standby Firebox is turned off.
- The management station computer is connected to the standby Firebox using the blue serial cable.
- The management station computer is connected to the standby Firebox with an Ethernet cable.
- Configuring manually

After you add the High Availability license keys to the configuration file of the active Firebox, you can configure the standby Firebox.

- 1 Open Policy Manager on the management station. Open the configuration that is currently on the active Firebox.
From the Policy Manager, click File > Open Configuration File.
Browse to the location of the current configuration of the active Firebox.
- 2 From Policy Manager, click **Network > High Availability**.

The High Availability dialog box appears. You do not see eth3, eth4 and eth5 if you have a Firebox III.



- 3 Select the **Enable High Availability** checkbox.
The Standby Firebox fields activate.
- 4 Select the **Default Heartbeat** option for your High Availability interface.
The default is the trusted interface. You can choose a different interface, but you can only use one interface for High Availability.
- 5 In the **IP Address** field next to the interface you selected, type an IP address from the same subnet as the High Availability interface on the active Firebox. This is the permanent IP address of the standby Firebox.
No other device can use the IP address of the standby Firebox.
- 6 Click **OK**.
- 7 Connect the blue serial cable that came with one of the Fireboxes to COM1 of the management station computer and to the Console port of the standby Firebox.
- 8 From Firebox System Manager, click **Main Menu > Tools > Advanced > Flash Disk Management**.
- 9 Click the **Boot from the System Area (Factory Default)** option. Click **Continue**.
- 10 Type an IP address that is in the same subnet as the management station PC but is not the heartbeat IP address.

This is the temporary IP address for the Firebox when it is in the factory default mode.

- 11 Click **OK**.
- 12 From the drop-down list, select the COM port which connects your management station to the Firebox. Use the blue serial cable.
- 13 Click **OK**.
- 14 Turn on the standby Firebox.
The Flash Disk Management tool starts the Firebox and gives it the temporary IP address.
- 15 Open the Policy Manager with the current configuration for the active Firebox.
- 16 Click **File > Save > To Firebox**.
- 17 Type the temporary IP address that you used in step 10.
- 18 Type the configuration passphrase. The default passphrase for a new Firebox is `wg`. Click **OK**.
- 19 Save the new configuration file to the Firebox. Give the standby Firebox the same configuration passphrase and status passphrase as the active Firebox.
The Policy Manager sends a new flash image to the standby Firebox. The standby Firebox starts again.

If the standby Firebox is connected to the network and the active Firebox is operating, the standby box goes to standby mode. The configuration is complete.

If the standby Firebox is connected only to the management station PC, it goes to active mode. Turn off the standby Firebox. Connect both the standby Firebox and the active Firebox to the network as described at the start of the High Availability Guide. Turn on the active unit if it is not on. Turn on the standby box. The configuration is complete.

Testing the failover process

To make a test of the High Availability configuration, turn off the active Firebox. In less than 15 seconds, the standby Firebox becomes the active Firebox. It gets all packet filter connections that were active before the first Firebox went off line and starts

to route traffic for them. Then, turn on the first Firebox. It starts and goes to standby mode.

Identifying the active and standby Fireboxes.

You can identify which Firebox is the standby Firebox and which Firebox is the active Firebox.

For the Firebox III models:

- The front panel display shows the Armed and SysA lights on the active Firebox.
- The SysA and the SysB lights go on and off on the standby Firebox.

For the Firebox X models:

- The front panel display shows “SysA-Armed” when you push the up button on the active box.
- The front panel display shows “HA-Standby” when you push the up button on the standby box.

