

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 - 2004 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 7.3

Document Version: HighAvailability-7.3-1

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 is taken 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

The term "Firebox" refers to a Firebox® III or a Firebox® X unless specifically stated. Illustrations of Fireboxes are interchangeable unless specifically stated.

The High Availability Failover Process

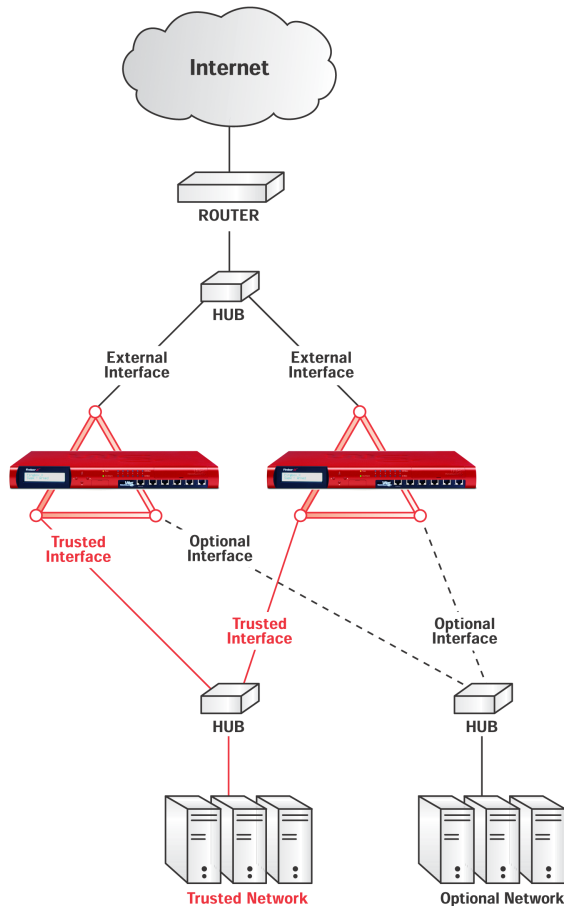
To create a High Availability pair, it is necessary to have two Firebox® devices that are the same model. One is the active Firebox and the other is the standby Firebox. The relationship between the active Firebox and the standby Firebox is dynamic. When the Firebox starts, it becomes the active Firebox. If two

Firebox appliances start at the same time, they negotiate active and standby status.

If both of the Firebox appliances are active and connected to the network, one Firebox restarts in standby mode. This is called *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.

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 appliances. 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 exchange 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 on 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 in a 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. 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 to the 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 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.

It is also necessary that each Firebox® in the pair 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.

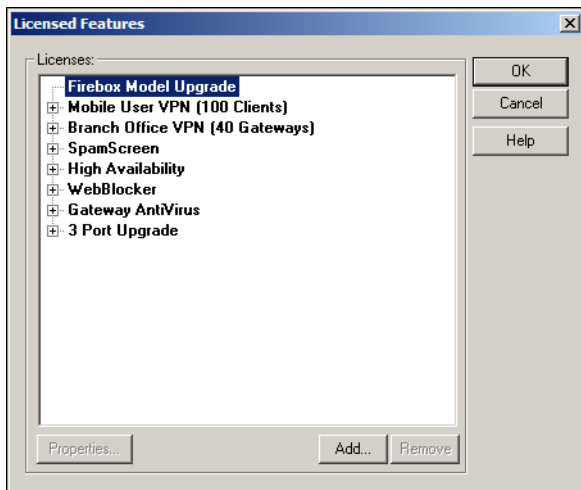
NOTE

The Firebox X models use a different installation procedure than the Firebox III models. This is because Firebox X license keys are associated with the unit serial number.

You must add all the license keys for the active Firebox X and the standby Firebox X to the configuration file. This allows each Firebox in the pair to use all of the options you have when it becomes the active Firebox. Thus, for each upgrade you enable, you enter two license keys into the Firebox X configuration file: one for the active Firebox and one for the standby Firebox.

For more information, browse to the LiveSecurity Web site.

- 1 From Policy Manager, select **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 your license keys.
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

The method you use to connect the Firebox® devices in a High Availability pair is related to your current network configuration.

Adding a standby Firebox to a Firebox installation

If your standby Firebox has the WatchGuard System Manager v7.2 or later installed, use a TCP/IP network connection to configure each Firebox.

If your standby Firebox does not have WatchGuard System Manager v7.2 or later installed, connect it to the management station with a serial cable. Use the QuickSetup Wizard to make an initial configuration file and save it to the Firebox. Then

enable the High Availability interface. The default High Availability interface is the trusted interface.

Connect an Ethernet cable to the High Availability interface. Connect the other end to the same switch or hub as the active Firebox. For more information, see the *Reference Guide* chapter “Firebox Read-Only System Area.”

Creating a new installation

If both Fireboxes are packaged with WatchGuard System Manager v7.2 or later, use a network connection to configure the Fireboxes via TCP/IP.

Configuring High Availability

Before you configure your network for High Availability, make sure that the two Firebox devices are:

- The same model
 - On the same subnet
 - Connected to the network with the same interface
- The default High Availability interface is the trusted interface.

You must also identify which device is the active Firebox and which device is the standby Firebox. We recommend that you put a label on the hardware to identify the units. If you have an operational Firebox in your network, this becomes the active Firebox. The second device you install is the standby Firebox. You can use the QuickSetup Wizard to configure a High Availability pair. The wizard connects the two Firebox devices on the trusted interface.

You can also use the Policy Manager to manually configure your devices for High Availability. With the Policy Manager, you can select any interface for High Availability.

Configuring High Availability with the wizard

- 1 Select **Start > Programs > WatchGuard > QuickSetup Wizard**.
The QuickSetup Wizard appears.
- 2 Click **Establish a High-Availability Firebox Cluster** from the drop-down list. Click **Next**.
The High Availability Configuration screen appears.
- 3 Type the IP address of the active Firebox in the **Active Firebox IP Address** field.
- 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 Use the drop-down list to select a method to connect the two Firebox devices. You can connect to the Firebox devices with a serial cable or an Ethernet cable.
We recommend that you use TCP/IP (Hands-Free). If you use Serial, you must also select the serial port from the drop-down list.
- 10 Type the temporary IP address for the standby Firebox.
You must use the same IP address as the Stand-By IP address you typed in step 4.
- 11 Click **Next**. If you selected Serial in step 9, go to step 14. Otherwise, continue.
- 12 Type or accept the **Current Configuration Pass Phrase**.
This is the read-write passphrase for the standby Firebox. If this is a new Firebox, accept the default password, wg.
- 13 Click **OK**.

-
- 14 When the wizard tells you, turn on the standby Firebox.

The QuickSetup Wizard identifies the Fireboxes and requests the High Availability license keys. After you enter the license keys, the standby Firebox starts in standby mode.

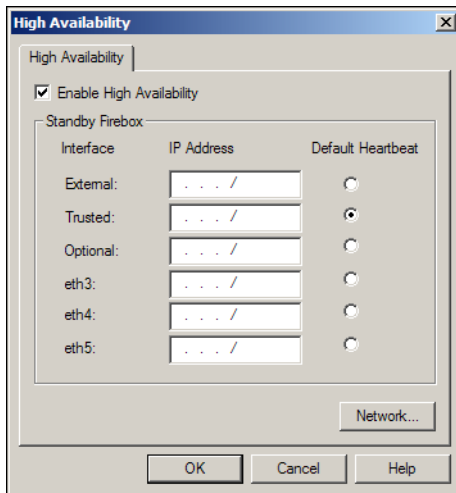
NOTE

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 manually

After you add the High Availability license keys to the configuration files of the two Firebox devices, you can configure the standby Firebox.

- 1 From Policy Manager, select **Network > High Availability**. The High Availability dialog box appears. You do not see eth3, eth4 and eth5 if you have a Firebox III.



- 2 Select the **Enable High Availability** checkbox. The Standby Firebox fields activate.
- 3 Select the **Default Heartbeat** option for your High Availability interface. The default is the trusted interface. You can only use one interface for High Availability. You can not use the interface for any other function.

- 4 In the **IP Address** field next to 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.
- 5 Click **OK**.
- 6 Save the configuration to the active Firebox.
- 7 Close Policy Manager.
- 8 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.
- 9 From Firebox System Manager, click **Main Menu > Tools > Advanced > Flash Disk Management**.
- 10 Select the **Boot from the System Area (Factory Default)** option. Click **Continue**.
A warning appears that you must use a serial cable.
- 11 Click **Yes**.
- 12 Type the IP address you used in step 4 for the High Availability interface.
- 13 Click **OK**.
- 14 Use the drop-down list to select the COM port which connects your management station to the Firebox. Use the blue serial cable.
- 15 Click **OK**.
The Flash Disk Management tool starts the Firebox and gives it the temporary IP address.
- 16 Open the Policy Manager with your current configuration.
- 17 Click **File > Save > To Firebox**.
- 18 Type the temporary IP address.
- 19 Type the configuration passphrase. The default passphrase for a new Firebox is `wg`. Click **OK**.
- 20 Save the new configuration file to the Firebox. Give the standby Firebox with the same configuration passphrase and status passphrase as the active Firebox.
The second Firebox starts again and goes to standby mode.

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.