

WatchGuard® Firebox™ System Install Guide

Firebox System 4.6



Disclaimer

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 and Patent Information

Copyright© 1998 - 2001 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, Firebox, LiveSecurity, and SpamScreen are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

Red Hat® is a registered trademark of Red Hat, Inc. This product is not a product of Red Hat, Inc. and is not endorsed by Red Hat, Inc. This is a product of WatchGuard and we have no relationship with Red Hat, Inc.

Adobe, Acrobat, the Acrobat logo, and PostScript are trademarks of Adobe Systems Incorporated.

© 1999 BackWeb Technologies, Inc. All rights reserved. BackWeb is a registered trademark of BackWeb Technologies, Inc.

CyberNOT, CyberNOT List, CyberYES, and CyberYES List are trademarks of Learning Company Properties Inc.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-1999 The OpenSSL Project. All rights reserved.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

VPCOM™ Copyright © 1997-1999 Ashley Laurent, Inc. All rights reserved.

All other trademarks and tradenames are the property of their respective owners.

Printed in the United States of America.

DocVer: WatchGuard Firebox System 4.6 Install Guide - 4.6.1

PartNum: 1200019

Declaration of Conformity

WatchGuard Technologies, Inc.
505 Fifth Avenue South
Suite 500
Seattle WA 98104-3892

Declares the CE-marked product:

Product Models:	Firebox family of appliances	
Complies with:	73/23/EEC Low Voltage Directive 89/336/EEC Electromagnetic Compatibility Directive	
Compliance Standards:	EN60950:1992	Electrical Safety A1:1993, A2:1993, A3:1995, A4:1997, A11:1997
	EN55022, Class A	RF Emissions Information Technology
	EN50082-1	EMC Immunity Standard

FCC Certification

This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1 This device may not cause harmful interference.
- 2 This device must accept any interference received, including interference that may cause undesired operation.

CE Notice

The official CE symbol indicates compliance of this WatchGuard Technologies, Inc. product to the EMC directive of the European Community. The CE symbol found here or elsewhere indicates that this WatchGuard product meets or exceeds the following standards:

EN60950:1992	Electrical Safety A1:1993, A2:1993, A3:1995, A4:1997, A11:1997
EN55022, Class A	RF Emissions Information Technology
EN50082-1	EMC Immunity Standard



CSA Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouleur du Canada.

WatchGuard Firebox System Install Guide

The WatchGuard Firebox System is an interdependent system of software. The hardware elements of the Firebox system are:

- Firebox—a security appliance for implementing security policies and protection.
- Management Station—the computer that administers the Firebox. This computer runs the Control Center software, which provides access to WatchGuard Firebox System applications and displays a real-time monitor of traffic through the firewall, connection status, tunnel status, and recent log activity.
- Event Processor—the computer that receives and stores log messages and issues notifications. (The Management Station can also serve as the Event Processor.)

This guide walks you through the installation process step-by-step to ensure a smooth and easy installation.

Selecting Computers

One of the first tasks before installation is determining which computers to use for different functions in the security system:

- Choose the computer to use for the Management Station.
The Management Station operating system platform must be Windows 98, Windows NT, or Windows 2000. (For more information on system requirements, see the next page.)
- Choose the computer to use for the primary event processor, also known as the log host (can be the same one as the Management Station). You can set up multiple event processors for redundancy.

Meeting System Requirements

Make sure you have the proper software, browser, and hardware for running the WatchGuard Firebox System version 4.6 or 4.6.1.

Software requirements

WatchGuard Firebox System version 4.6 or 4.6.1 can run on Microsoft Windows 98, Windows NT 4.0, or Windows 2000 as specified below:

Windows 98 Requirements

- Microsoft Windows 98

Windows NT Requirements

- Microsoft Windows NT 4.0 Service Pack 4, 5, or 6a

Windows 2000 Requirements

- Microsoft Windows 2000 SR1

Web browser requirements

Make sure you have the proper software for running the installation from the CD and for viewing Online Help. Microsoft Internet Explorer® 5.01 or later is required to run the installation from the CD. The following HTML-based browsers are recommended to view WatchGuard Online Help:

- Netscape Communicator® 4.7 or later
- Microsoft Internet Explorer 5.01 or later

Hardware requirements

Make sure you have the proper hardware. Minimum hardware requirements are the same as for the operating system on which WatchGuard Firebox System 4.6 or 4.6.1 runs. The recommended hardware ranges are listed below:

Hardware Feature	Minimum Requirement (for Management Station)
CPU	Pentium II
Memory	Same as for operating system. Recommended: 64 MB for Windows 98 64 MB for Windows NT 4.0 64 MB for Windows 2000 Professional 256 MB for Windows 2000 Server
Hard disk space	25 MB to install all WatchGuard modules 15 MB minimum for log files Additional space as required for log files Additional space as required for multiple configuration files
CD-ROM drive	One CD-ROM drive to install WatchGuard from its CD-ROM distribution disk

Backing up Files and Removing Previous Versions (Upgrade Only)

If you are upgrading from a previous version of the Firebox System, perform the following steps (otherwise, you can skip this section):

- 1 Back up the current Firebox configuration file. To do this, save the file to a new name and place it in a directory other than the WatchGuard directory.
- 2 Exit and disable the Event Processor.

NOTE

If you are running Windows NT or Windows 2000, disabling the Event Processor does not stop the service. Stop the service first, either from the Event Processor interface or using one of the following procedures:

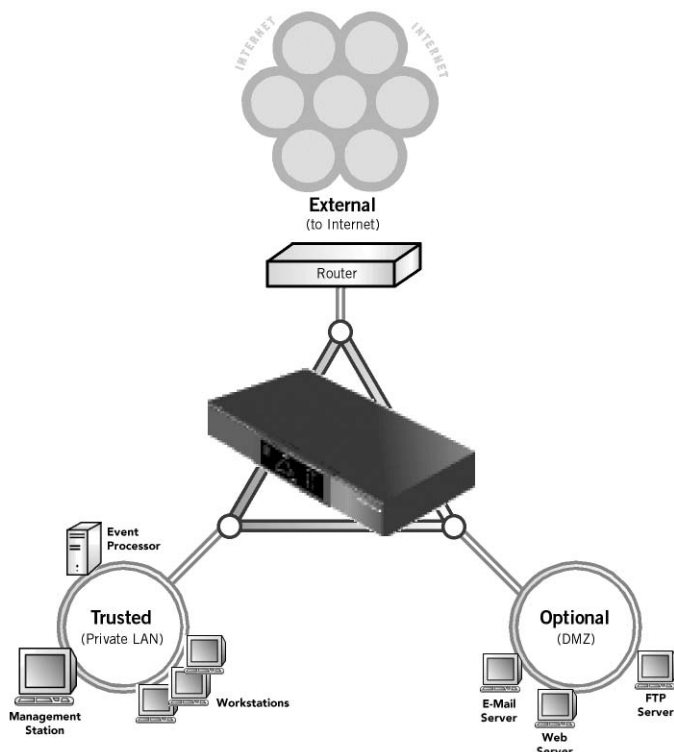
If you are running Windows NT: Click Start=>Settings=>Control Panel=>Services. Then, from the Services menu, click the name of the service. Click Stop.

If you are running Windows 2000, click Start=>Settings=>Control Panel=>Administrative Tools=>Services. Click the name of the service. Click Stop.

- 3 Uninstall any previous versions of WatchGuard software.

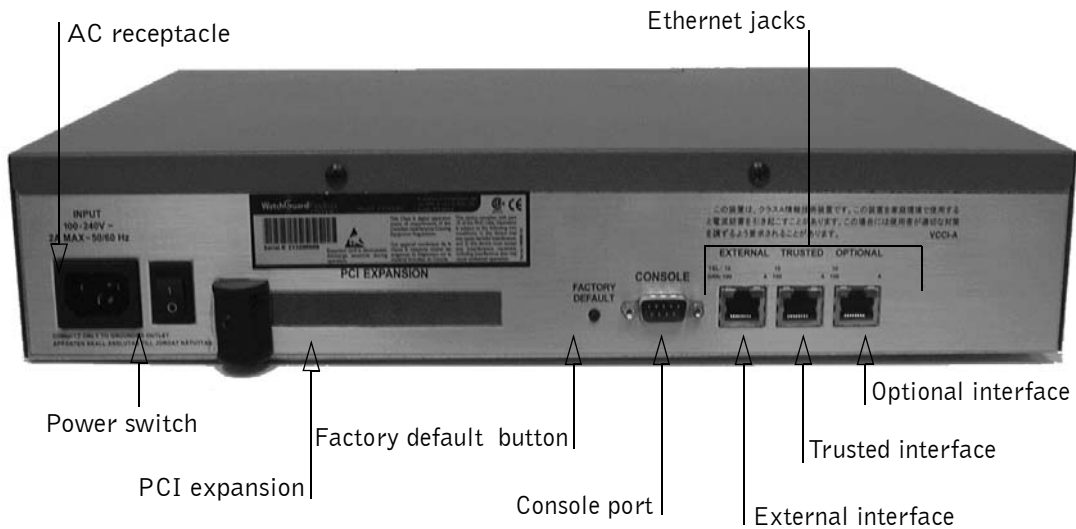
Determining a Network Location for the Firebox

The most common location of the Firebox, and the one that is nearly always used, is directly behind the Internet router, as pictured below.

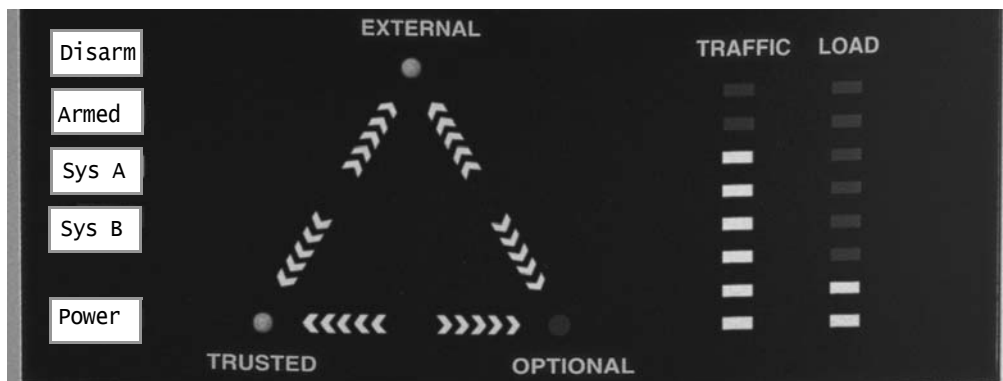


Connecting a Firebox

You can connect to and initialize a new Firebox in two ways: over a network using TCP/IP or via a serial cable. The following figure shows the connections on the back of the Firebox.



The following figure shows a close-up of the panel on the front of the Firebox.



Connecting a Firebox for hands-free installation

This process uses TCP/IP to connect and initialize a new Firebox. The Firebox will automatically obtain its IP address.

- 1 Place the Firebox on a desktop or in a rack in a location convenient to the external router.
- 2 Use the green (Ethernet) cable (provided with the Firebox) to connect the Firebox Trusted interface to the same network as the computer that will act as the Firebox Management Station.

- 3 Install the power cord from the AC receptacle on the Firebox to a power source.
- 4 When prompted to do so during the QuickSetup wizard (see “Working with the QuickSetup Wizard” on page 7), select **Use TCP/IP to Configure** as the configuration access method.

You can tell that hands-free networking is enabled because both the Sys A light and the segment of the security triangle between External and Optional are flashing on and off. (See the illustration on the previous page for locating these portions of the Firebox.)

Connecting a Firebox for serial cable initialization

This process requires that you manually create an IP address.

- 1 Place the Firebox in a location convenient to the Management Station.
- 2 Use the blue serial cable to connect the Firebox console port with the Management Station COM port. Use the red crossover cable to connect the Trusted interface to the Management Station Ethernet port.
- 3 Install the power cord from the Firebox AC receptacle to a power source.
- 4 When prompted to do so during the QuickSetup wizard (see “Working with the QuickSetup Wizard” on page 7), select **Use Serial Cable to Assign IP Address** as the configuration access method.

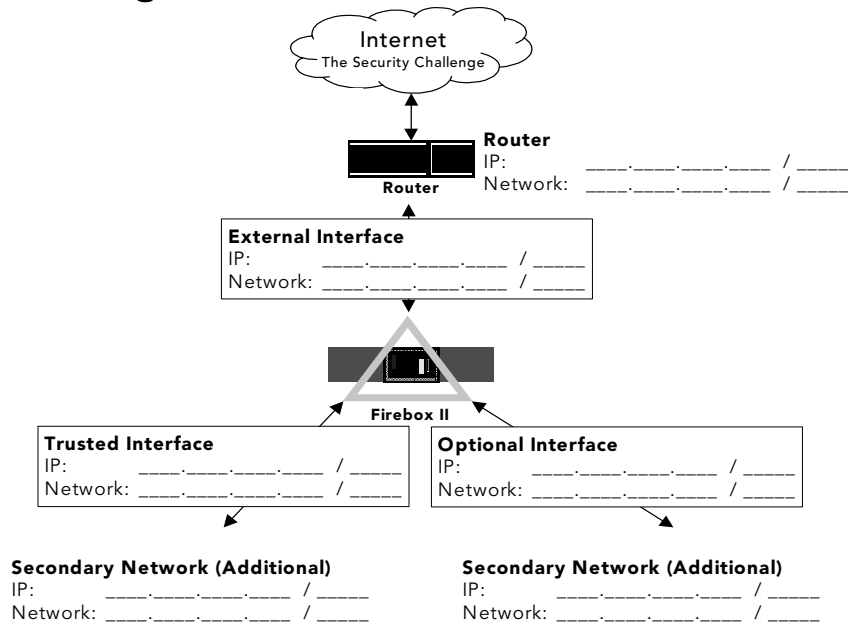
Completing the Network Configuration Worksheet

We encourage you to complete the Network Configuration Worksheet on the following page before running the QuickSetup wizard to install the WatchGuard Firebox System for the first time. By completing the worksheet, you will be prepared to answer prompts for IP addresses. The resulting basic configuration file will more closely match the true network environment.

NOTE

A standard letter-size version of the Network Configuration Worksheet is available in PDF format on the installation CD-ROM in the Documentation folder.

Network Configuration Worksheet



Label	IP Addresses
Event Processor	_____
Default Gateway	_____
Firebox Interface (Drop-in Only)	_____ / _____
External Interface (Routed Only)	_____ / _____
Trusted Interface (Routed Only)	_____ / _____
Optional Interface (Routed Only)	_____ / _____
Secondary Network	_____ / _____
SMTP Server	_____
HTTP Server (Routed Only)	_____
FTP Server (Routed Only)	_____

Starting the Installation

The Firebox System integrated installation wizard activates the LiveSecurity license key, and downloads and installs the Management Station software.

DEPENDENCIES

- Computer with 25 MB space on the local hard disk, to be used as the Management Station.
 - [Optional] Connection to Internet
-

To start the installation, do the following:

- 1 Exit all applications on the computer selected for the Firebox System. Insert the WatchGuard Firebox System disk into the CD-ROM drive.
The installation wizard should start automatically. If it does not, use Windows Explorer to find `install.exe` in the root directory of the WatchGuard Firebox System CD-ROM. Double-click `install.exe` to start the installation process.
- 2 Click **Activate LiveSecurity Service**. The installation program automatically verifies whether or not there is an Internet connection. This is an important step. The LiveSecurity Service updates you whenever there is an alert that is important to you.
- 3 The LiveSecurity Installation wizard begins. Use the **Next** and **Back** buttons to move through the Installation wizard.

Working with the QuickSetup Wizard

The final step of the WatchGuard Firebox System installation is to fill out the required information in the QuickSetup wizard. The QuickSetup wizard creates a basic configuration file and saves it to the primary area of the Firebox flash disk. The Firebox loads this primary configuration file when it boots.

The QuickSetup wizard also writes a basic configuration file called `wizard.cfg` to the Management Station hard disk.

By default, the QuickSetup wizard starts automatically after you finish installing the Firebox System software. To manually start the QuickSetup wizard from the Windows desktop, select **Start** ⇒ **Programs** ⇒ **WatchGuard** ⇒ **QuickSetup Wizard**.

The first step of the QuickSetup wizard prompts you to select a configuration option: either drop-in mode or routed mode. These configurations are described in the next two sections.

Choosing a configuration option

In the first step of the QuickSetup wizard, you are asked to select a configuration option: routed mode or drop-in mode. The characteristics of each are discussed below.

Drop-in mode

A drop-in network configuration is useful for situations where you can distribute the network's logical address space across the Firebox interfaces. In a drop-in configuration, you place the Firebox physically between the router and the LAN, without reconfiguring any of the machines on the Trusted interface.

Characteristics of a drop-in configuration:

- A single IP network not subdivided into smaller IP networks.
- The Firebox performs proxy ARP.
- All trusted computers must have their ARP caches flushed or timed out.
- All three Firebox interfaces are assigned the same IP address.
- The IP addresses of secondary networks are listed in the configuration file.

Routed mode

A routed network configuration is for situations where the Firebox is put in place with separate logical networks on its interfaces. It assigns separate network addresses to at least two of the three Firebox interfaces.

Characteristics of a routed configuration:

- There is more than one network recognized by the Firebox.
- You can relate different networks to different interfaces. Those networks then come under the protection and access rules set up for that interface.
- Each interface must be on a separate logical network.
- If there are more than three networks, additional networks are added as secondary networks.
- If there are only two networks behind the Firebox and you want to use the routed configuration, use only the External and Trusted interfaces (do not use the Optional interface).

Entering the Firebox IP address

On the wizard's next screen, you enter the IP address for each Firebox interface and specify whether you have an additional network on each interface.

Firebox Interface: In a drop-in configuration, because all three interfaces share the same IP address, you need to enter only one address. In a routed configuration, however, each of the three Firebox interfaces has a different IP address. You need to enter the IP address for each interface.

Unused IP: If you have a secondary network on the Trusted interface, enable the checkbox labeled **I have an additional non-routed network behind my Firebox**. Enter an unused IP address on the secondary network.

Entering IP addresses

To type in your IP address, type the digits and periods in sequence. Do not use the TAB key to jump past the periods.

If your address has a network mask, use slash notation to enter it. For information on using slash notation, click the Help button on this screen.

Entering the Firebox default gateway

On the wizard's next screen, enter the IP address of the default gateway to the Firebox. This must be the IP address of your Internet router. Also, this IP address

should be on the same network as the IP address you entered for the Firebox External interface.

Configuring the public servers

For a drop-in configuration, on the wizard's next screen, you enter information for your public servers.

For drop-in configurations:

- 1 Enable the checkboxes that describe your network configuration:
I have an SMTP server behind my Firebox.
I have an HTTP server behind my Firebox.
I have an FTP server behind my Firebox.
- 2 Enter the IP addresses for each server on your network.

For routed configurations:

- 1 Enable the checkbox labeled **I have an SMTP server behind my Firebox.**
- 2 Enter the SMTP server IP address.
- 3 Use the drop list to select whether the server is on the Trusted or Optional network.

Creating passwords for the Firebox

On the wizard's next screen, you create passwords for the Firebox. Passwords must be at least seven characters long. They can be any combination of numbers, letters, and special characters. You must create two passwords:

Status password

The password used for establishing read-only connections to the Firebox.

Configuration password

The password used for establishing read/write connections to the Firebox.

The status and configuration passwords need to be different.

Tips for creating secure passwords

Although an attacker can crack any password eventually, you can tighten your security using the following tips:

- Don't use words in standard dictionaries, even if you use them backward or in a foreign language. Create your own acronyms instead.
- Don't use proper names, especially company names or those of famous people.
- Use a combination of uppercase and lowercase characters, numerals, and special characters (such as Im4e@tiN9).

Uploading the security policy

On the wizard's next screen, you send a security policy to the Firebox.

Choose the Firebox configuration access method: If the Firebox is connected to the same network as the Management Station, select **Use TCP/IP to Configure for Hands-Free Installation**. (You can tell that hands-free networking is enabled because both the Sys A light and the segment of the security triangle between External and Optional are flashing on and off.)

If the Firebox is connected directly to the Management Station with a blue serial cable, select **Use Serial Cable to Assign IP Address for Serial Cable Initialization**.

Serial port: If you selected **Use Serial Cable to Assign IP Address for Serial Cable Initialization**, select the name of the serial port on the Management Station from which the blue serial cable is connected.

To send the security policy to your Firebox, assign it a temporary IP address so this machine can communicate with it. Enter this address in the **Temporary IP Address** field.

Finishing the setup

On the wizard's next screen, you review the information you previously entered:

- 1 Review the settings. Click **OK**.

The information is saved to a file named `wizard_setup.txt` in the WatchGuard installation directory. The QuickSetup wizard creates a basic configuration file and saves it to the local hard disk as `wizard.cfg`. It then attempts to contact the Firebox.
- 2 If using hands-free (TCP/IP) installation, enter the factory-installed configuration password: `wg`.
- 3 If using serial cable installation, turn the Firebox off and then on.

The QuickSetup wizard attempts to connect to the Firebox. If the network has multiple Fireboxes with the read-write pass phrase "wg", the Firebox selector dialog box appears. Use the Blink Lights button to select the address of the Firebox you are currently configuring. When a connection is made, the wizard uploads a basic configuration file to the primary area of the Firebox flash disk and initializes the Firebox with the IP addresses you provided. When complete, the Firebox Sys A and Armed indicators illuminate.
- 4 Reboot your external router. This clears the ARP cache.

After You Install

The Firebox can now communicate with the Management Station over the network. Perform the following post-installation steps:

- If you have not done so already, install the Firebox on the network. Initially, this is done over the Trusted interface.

The most common location is physically between the Internet router and connections to your trusted and optional networks. See "Determining a Network Location for the Firebox" on page 3.
- Connect the Ethernet lines to the Firebox Trusted, External, and Optional interfaces as appropriate.

Specific connections vary according to the drop-in or routed network configuration created. You are not required to connect the Optional interface if it is not part of your network configuration.

- Reboot the Management Station.
If you have designated the Management Station as the primary event processor, the LiveSecurity Event Processor starts.
- Begin configuring your security system. After installation, the next steps are delineating your network and applying protection for services such as SMTP and FTP. For information on how to do this, see the *User Guide*.

