
WatchGuard LiveSecurity System Install Guide

LiveSecurity System 4.0



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, 1999 WatchGuard Technologies, Inc.® All rights reserved.

WatchGuard Technologies, Inc.®, WatchGuard® are registered trademarks, and Firebox™ is a trademark of WatchGuard Technologies, Inc. in the USA and other countries.

VPCOM© 1997-1999 Ashley Laurent Inc. All Rights Reserved

Certain materials herein are Copyright ©1995-1999 Microsystems Software, Inc. Cyber Patrol® is a registered trademark of Microsystems Software, Inc. CyberNOT™ and CyberNOT List™ are trademarks of Microsystems Software, Inc.

Ethernet™ is a trademark of Xerox Corporation. Microsoft®, NetMeeting™, Windows®, Windows 95®, Windows 98®, Windows NT®, and Windows NT Server® are either registered trademarks or trademarks of Microsoft Corporation in the USA and other countries.

Java™ is a trademark of Sun Microsystems®.

PostScript® is a registered trademark of Adobe Systems, Inc.

X Window™ is a trademark of the Massachusetts Institute of Technology.

RealAudio™, RealVideo™, and RealNetwork™ are trademarks of RealNetworks, Inc.

StreamWorks™ and StreamWorks Player™ are trademarks of Xing Technology Corporation.

VDOLive™ and VDOPhone™ are trademarks of VDOnet Corp.

Certain materials herein are Copyright ©1992-99 RSA Data Security, Inc. and Copyright ©Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5015009, 5126739, and 5146221, and other patents pending.

Many of the other designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and WatchGuard Technologies, Inc. was aware of a trademark claim, the designations have been printed with initial capital letters or all capital letters.

Printed in the United States of America.

DocVer: S-40-Install-4

Table of Contents

Documentation	6
<i>Description of Technical Publications</i>	6
<i>Notational Conventions</i>	7
Before You Install	8
<i>Terms You Should Know</i>	8
<i>Selecting Computers</i>	8
<i>Before Upgrading to 4.0 from Previous Versions</i>	8
Installing the LiveSecurity System	9
<i>STEP 1: Install the LiveSecurity Client</i>	9
<i>STEP 2: Register LiveSecurity and Download Software</i>	11
<i>STEP 3: Authenticate the Security System software</i>	13
<i>STEP 4: Install the WatchGuard Security System</i>	15
Designing a Basic Network Configuration	17
<i>Drop-In Network</i>	17
<i>Drop-In Network Using Dynamic NAT</i>	20
<i>Subnetted Network</i>	23
<i>Subnetted Network Using Dynamic NAT</i>	26
<i>Completing the Network Configuration Worksheet</i>	28
<i>Network Configuration Worksheet</i>	29
Running the QuickSetup Wizard	30
<i>Basic (Drop-In) Network Configuration</i>	31
<i>Advanced (Subnetted) Network Configuration</i>	34
After You Install	37



Welcome to WatchGuard

We appreciate your purchase of the WatchGuard LiveSecurity System. The WatchGuard LiveSecurity System consists of a suite of management and security software tools coupled with a plug-and-play network appliance called the WatchGuard Firebox. LiveSecurity is specifically designed to guard critical corporate or organizational assets from a continually changing barrage of threats.

The LiveSecurity System by its nature requires interdependence among distributed software, downloadable software, your Firebox, and the computer you use to administer the Firebox (the Management Station). This document walks you through these interdependent steps so your installation goes smoothly and you understand what is downloaded, expanded, installed, and configured.

Documentation

All WatchGuard LiveSecurity System documentation is copied to your local hard drive during the installation process. They are also located on the LiveSecurity Installation CD-ROM in the Documentation folder. The documents are in the form of PDF files. You must have a copy of the Acrobat Adobe Reader® to read and print these files. Hard copies of the *Release Notes*, *Install Guide* and *User Guide* are included with the purchase of a Firebox.

Description of Technical Publications

Release Notes

Read these first to learn about known issues and new features since our prior release.

Internet Security Handbook

If you are a relative newcomer to the field of network security, read our security concepts primer. Learn more about Internet security and how our product, the LiveSecurity System, addresses the principal threats to your network.

Install Guide

This guide takes you step-by-step through the process of downloading the LiveSecurity Broadcast Service, installing the LiveSecurity Control Center, and using the QuickSetup Wizard to create an initial security policy configuration.

User Guide

The QuickSetup Wizard creates only the most basic configuration file. The *User Guide* steps through the many features of the LiveSecurity Control Center and Security Suite software. It includes sections on how to use our LiveSecurity services, configure and administer a security policy, and implement virtual private networking.

Reference Guide

A supplement to the *User Guide*, the *Reference Guide* provides additional material used to configure services and features such as detailed information about the IP protocol and a glossary of terms.

RUVPN Client Brochures

WatchGuard supports two forms of remote user virtual private networking: PPTP and IPSec. For your convenience, WatchGuard includes an end-user brochure for each RUVPN type. This information is also available within the *User Guide*.

Notational Conventions

WatchGuard manuals use the following notational conventions:

- When you select a menu command from a cascading menu, the command names are separated by an arrow (⇒) but with no special or separate font. For example, if the text says to: Select File ⇒Open, this means you should click the File menu and then click the Open command.
- Web site addresses display in a sans-serif font. For example:
`http://www.watchguard.com`
- Code and directory entries display in a sans-serif font. For example:
`[watchGuard installation directory]\RUVPN\Exp`

Before You Install

Terms You Should Know

There are a few terms that are commonly used by WatchGuard when referring to our product and how it is implemented.

- **Management Station** — The computer on which you install and run the WatchGuard LiveSecurity Control Center.
- **Log host** — The computer which receives and stores log messages. You can configure the Management Station to also serve as the log host.
- **Trusted network** — The network behind the firewall which must be protected from the security challenge.
- **External network** — The network presenting the security challenge, typically the Internet.
- **Optional network** — A network protected by the firewall which communicates with both the Trusted and the External networks. Typically, the Optional network is used for “public” servers such as an FTP or Web server.

Selecting Computers

- Choose the computer you will use for the Management Station. The Management Station operating system platform must be Windows 95, Windows 98 or Windows NT (Service Pack 4.0).
- Choose the computer you will use for the LiveSecurity Broadcast System. Verify that it has access to the Internet via Microsoft Internet Explorer® 4.0 (or later) or Netscape Communicator® 4.5 (or later). WatchGuard recommends that you use your Management Station as the computer for the LiveSecurity Broadcast System. However, if your configuration requires it you can designate an alternate computer.
- Choose the computer you will use for the primary log host. The primary log host can be either the Management Station or another computer.

Before Upgrading to 4.0 from Previous Versions

- Make a copy of your current Firebox configuration file.
- Do *not* uninstall any previous versions of WatchGuard software.

Installing the LiveSecurity System

- Insert the WatchGuard LiveSecurity disk into the CD-ROM drive of the computer you selected for the LiveSecurity Broadcast Service. The LiveSecurity installation wizard should start automatically. If it does not, use Windows Explorer® to find `lsinstall.exe` in the root directory of the WatchGuard LiveSecurity System CD-ROM. Double-click `lsinstall.exe` to start the installation process.
- Read and accept the license agreement.

STEP 1: Install the LiveSecurity Client

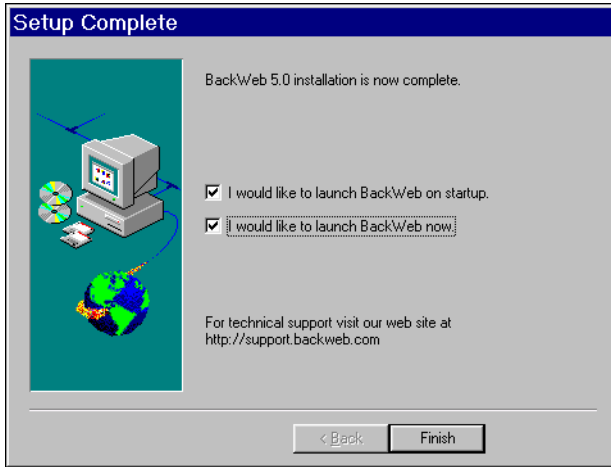
In this step you install the WatchGuard LiveSecurity client developed by BackWeb from the CD-ROM to the hard drive of your computer. The client, also known as the LiveSecurity Inbox, is the controlling software that "listens" to the LiveSecurity Web site, receives and stores software updates, threat responses, and information alerts, and informs you when you receive a broadcast.

WatchGuard pre-configures the customized LiveSecurity Inbox to establish secure connections to our LiveSecurity Broadcast server. Our client will not work with any other BackWeb client installation.



- a. Click STEP 1 Install the WatchGuard LiveSecurity Client. The Choose Destination Location dialog box opens.
- b. Click Next to accept the default installation directory `C:\Program Files\watchGuard\LiveSecurity`.

If desired, use the Browse button to select an alternative destination directory. As the wizard copies the LiveSecurity Inbox to your computer, it displays a progress indicator. When complete, the wizard then displays the Setup Complete dialog box.



- c. Enable or disable these checkboxes as appropriate:

I would like to launch BackWeb on startup.

When enabled, the LiveSecurity Inbox BackWeb client starts automatically whenever you reboot your computer. WatchGuard recommends enabling this checkbox (i.e. do check) so that the LiveSecurity client will always monitor for broadcasts.

I would like to launch BackWeb now.

When enabled, the LiveSecurity Inbox BackWeb client starts. WatchGuard recommends leaving this checkbox enabled (i.e. checked). However, you may need to minimize the LiveSecurity Inbox to view the LiveSecurity installation dialog box when you proceed to STEP 2.

- d. Click Finish.

The LiveSecurity client installation wizard closes and returns you to the main LiveSecurity installation screen.

- e. Reboot your computer if prompted to do so.



NOTE

With some NT installations, clicking Yes fails to restart the computer. If this occurs, click No. The installation wizard closes. Restart your computer manually.

If the computer restarts, the LiveSecurity installation wizard should start automatically. If it does not, use Windows Explorer® to find `lsinstall.exe` in the root directory of the LiveSecurity CD. Double-click `lsinstall.exe` to resume the installation process.

STEP 2: Register LiveSecurity and Download Software

In this step you register your LiveSecurity subscription, download the LiveSecurity Control Center (the software used to manage your Firebox), and enable access to WatchGuard Technical Support.

If your site requires that you be authenticated before you can access the Internet or the World Wide Web, make sure that you have done so before beginning Step 2.



NOTE

Downloading the software simply transfers the compressed files from a WatchGuard server to your local computer. Later, in Step 3 you authenticate the software, and in Step 4 you decompress and install it.

- a. Click STEP 2 Register your LiveSecurity subscription.
Your Web browser opens and displays the LiveSecurity registration screen.



- b. Complete the LiveSecurity Registration form.

Asterisks mark fields required for successful registration. The profile information assists WatchGuard to target information and updates to your needs. The following tips may assist you with completing the form:

- Navigate fields using either the Tab key or mouse.
- The Firebox serial number is displayed in two locations:
 - A small silver sticker on the outside of the shipping box
 - A sticker on the back of the Firebox just below the UPC bar code
- Your login and password will be e-mailed to the address provided on the registration form. Verify that you entered a valid e-mail address.
- The License Key number is located on the WatchGuard LiveSecurity Agreement License Key Certificate. Enter the number in the exact format shown on the key, including hyphens.
- When you complete the registration form, click the Submit button.

After you submit and WatchGuard accepts your registration, a display appears enabling you to select a server from which to download the WatchGuard Security System.



NOTE

If your registration is not accepted, check your registration form. Verify that you entered all required fields, re-check your serial number, and verify that you entered the numbers and hyphens of your License Key exactly as they appear.

The most common reason for registration to fail is incorrectly typing the numbers and hyphens of the License Key.

Alternative to Downloading the Control Center Software

WatchGuard encourages you to download the most recent version of our software from the LiveSecurity Web site. This ensures that your software includes the most recent updates and enhancements to address new security challenges. However, if you have a slow Internet connection, you can install the software from the LiveSecurity CD-ROM. Skip steps "c" and "d" below.

- c.** Choose a server for your download.

WatchGuard recommends selecting the server geographically closest to your location. Upon selecting a server, a scrollable list of WatchGuard software and documentation appears. You should have already installed the first choice, the LiveSecurity client software, during Step 1. Scroll to the next choice.

- d.** Download the Firebox software.

Select FBII and Upgraded FB10/100 Security System software. Select the option to save the download to a disk. WatchGuard recommends saving the download to your Windows Desktop where you can easily find it later.

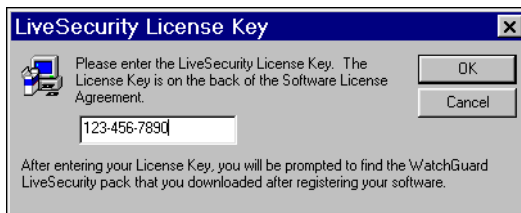
- e.** Minimize your Web browser.

- f. Connect your Firebox for initialization and configuration.
 - Using the serial cable supplied with the installation kit, connect a serial port from the Management Station to the CONSOLE port on the back of the Firebox.
 - Connect a red colored "cross cable" from the Management Station's network connection to the Firebox's Trusted interface.
 - Connect AC power to the Firebox but do not turn it on.

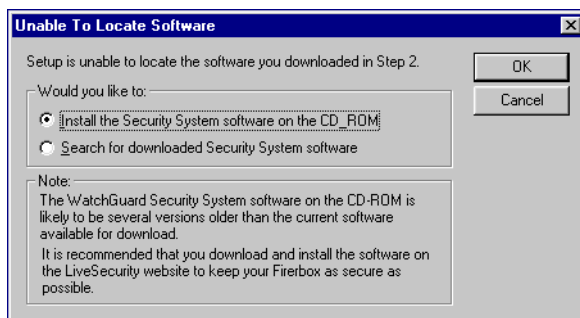
STEP 3: Authenticate the Security System software

In this step, you supply your LiveSecurity license key number to activate the LiveSecurity client for receipt of broadcasts sent specifically to you. You also authenticate the Security System software.

- a. Click STEP 3 Authenticate the Security System software.
The LiveSecurity License Key dialog box appears.



- b. Enter your LiveSecurity License Key from your License Key Certificate.
Enter only the numbers. The field automatically delineates the hyphens.
- c. Click OK.
The installation wizard searches your hard drive for the LiveSecurity Control Center installation package.
- d. At this point, one of three paths can be chosen. If the wizard finds the installation software, proceed to task "g".
For installations with most Windows and Web browser platforms, the wizard automatically finds the installation package copied to the local drive, verifies the digital signature of the installation package, and prepares for installation.
- e. If you downloaded the software from the Web site but the installation wizard is unable to locate the file, the Unable to Locate Software dialog box appears. Select Search for Downloaded Security System Software.



Browse to locate WatchGuard.wls. Click Open. Proceed to task “g”.

The wizard verifies the digital signature of the installation package and prepares for installation.

- f. If you did not download the most recent version of the software from the LiveSecurity Web site, select Install the Security System Software on the CD-ROM. Select a Firebox type. Click OK.

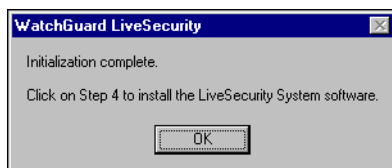


NOTE

Select Firebox II for all versions of the Firebox II and Firebox II *Plus* hardware.

The wizard verifies the digital signature of the installation package and prepares for installation.

When the wizard completes preparing the computer for installing the Security System software, an Initialization Complete dialog box appears.



- g. Click OK.



NOTE

If you installed the LiveSecurity Inbox on a machine other than your Management Station, you must now move or copy **watchguard.exe** to the Management Station. WatchGuard recommends that you store the file in a folder you create named **C:\Program Files\watchGuard**.

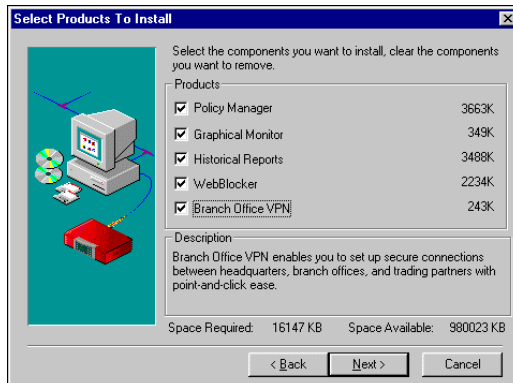
STEP 4: Install the WatchGuard Security System

In this step you run the WatchGuard Security System installation program. The LiveSecurity Control Center (a.k.a. WatchGuard Security System) is the interface for administering and monitoring your security policy.

- a. Click Step 4 Install the WatchGuard Security System.
A WinZip extractor opens.



- b. Click Setup.
After decompressing the files, the installation wizard opens.
- c. Follow the installation wizard instructions to correctly set up the LiveSecurity Control Center software on your computer.
- d. Select the WatchGuard products to install. Click Next.
WatchGuard recommends that you install the entire product list. For a brief description of any WatchGuard product, position your mouse over the name.



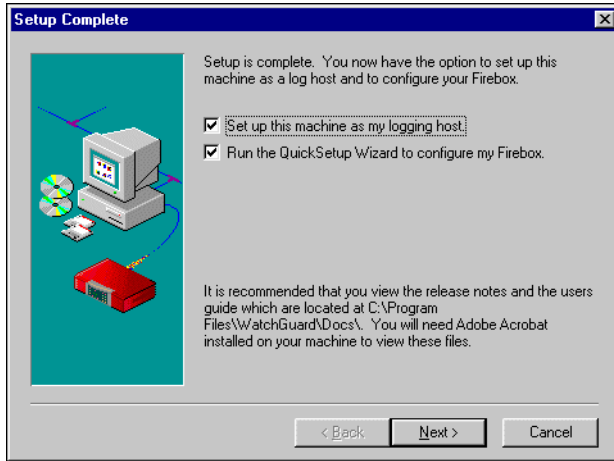
- e. In the Setup Complete dialog box, enable or disable these checkboxes as appropriate:

Set up this machine as my logging host.

When enabled, your Management Station becomes the logging host. If you disable (i.e. do not check) this checkbox, you will have no default logging host. You can set up a logging host later.

Run the wizard to configure my Firebox.

When enabled, the installation wizard automatically initiates the QuickSetup Wizard immediately after completing the LiveSecurity installation.



f. Click Finish.

The installation wizard closes and the WatchGuard Docs folder appears. You can also open documentation from the Windows desktop. Select Start ⇒ Programs ⇒ WatchGuard ⇒ Documentation.

g. If you receive a message indicating that a read-only file was found and asking whether or not you want to copy the file, click No.

You must click No or the setup terminates. This is a known issue and does not affect the installation.

h. Open and view the included documentation.

You must have the Adobe Acrobat Reader® to open the PDF versions of our documentation. Read the *Release Notes* first to acquaint yourself with the functions and dependencies of the software release you just installed. The *Internet Security Handbook* explains many networking and security principles while the *User Guide* provides procedural instructions on many configuration and administrative tasks.

i. Complete the “Network Configuration Worksheet” on page 29, then run the QuickSetup Wizard.

j. Close the LiveSecurity Installation dialog box. Click Yes.

You must close the LiveSecurity installation dialog box before removing the CD-ROM.

Designing a Basic Network Configuration

The purpose of the four sample network configurations included in this section is to clarify configuration issues as well as demonstrate in some detail how to set up a typical security policy configuration. Careful study of these examples should facilitate using the QuickSetup Wizard to create a basic configuration file designed to meet your security policy objectives. For more information about developing a security policy and implementing a firewall, read the *Internet Security Handbook* found on the installation CD-ROM in the Documentation directory.

Each example includes a description, tips on when to use the configuration type, details about the addressing scheme, an addressing diagram, a table of QuickSetup Wizard data, and the additional configuration required after completing basic installation. The *User Guide* provides step-by-step instructions on how to complete each procedure.

Drop-In Network

The first example is a basic class C network typically used by small to medium-sized enterprises. A class C network theoretically has 256 available addresses. A few of these addresses are reserved for system use. To configure this type of network using the QuickSetup Wizard, do not check the Advanced checkbox on the first wizard screen.

When to Use

A drop-in network configuration works well for the system administrator with an existing network connected to a single router that in turn connects to the world. The Firebox “drops in” between the router and the security challenge: the Internet. The addressing scheme behind the Firebox remains unchanged.

Addressing

If all interfaces are on the same network, you can assign the same IP address to all three Firebox interfaces: Trusted, External, and Optional. Let the Firebox perform ARP. For more information about ARP, see the *Internet Security Handbook*.

For our example, we will assign the router an IP address of 111.222.121.1 and the Firebox an IP address of 111.222.121.2. Since we are assigning the same IP to all three interfaces, the default gateway of the machines on both Trusted and Optional networks should be the IP address of the

router or the interface of the Firebox. The log host for this example shares duty with the Management Station running the LiveSecurity Control Center. Our SMTP server is on the optional network using IP address 111.222.121.3. There are no related networks.

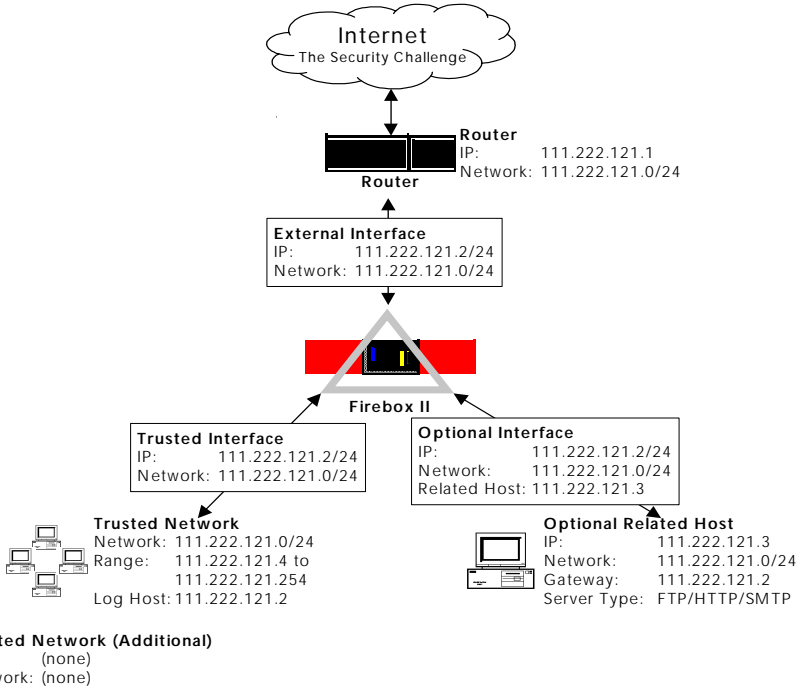


Table 1. Drop-In QuickSetup Wizard Data (Netmask /24)

Label	IP Addresses
Log Host	111.222.121.2
Default Gateway	111.222.121.1
Firebox Interface	111.222.121.2/24
SMTP Service	111.222.121.3

Policy Manager Configuration

- The Services Arena automatically contains icons for Filtered-HTTP, FTP, ping, SMTP (if you added it), and WatchGuard. Double-click the service and configure with the following settings:

Filtered-HTTP Incoming

- Enabled and Allowed
- From: Any
- To: 111.222.121.3

Filtered-HTTP Outgoing

- Enabled and Allowed
- From: Any
- To: Any

FTP Incoming

- Enabled and Allowed
- From: Any
- To: 111.222.121.3

FTP Outgoing

- Enabled and Allowed
- From: Any
- To: Any

- Configure the individual filter rules for FTP, SMTP incoming and outgoing, and HTTP proxy to your preference.
- Set the local time zone.
- Set the log encryption key for the primary log host.
- Save the new configuration to the Firebox.

Additional Configuration

- Go to all hosts on the Trusted network and configure the default gateway to 111.222.121.1.
- Open the WatchGuard Event Processor. Set the log encryption key to the same value as configured in the Policy Manager for the primary log host.

Drop-In Network Using Dynamic NAT

The drop-in network using dynamic NAT is very similar to the simple Drop-In network, with the addition of dynamic network address translation to hide (also known as “masquerading”) addresses on the Trusted network. To configure this type of network using the QuickSetup Wizard, do not check the Advanced checkbox on the first wizard screen.

When to Use

A drop-in network with dynamic NAT configuration works well when you want to “drop-in” the Firebox to an existing network and hide a private network behind either the Trusted or Optional interface.

Addressing

This example has an entry for 10.0.0.0/24 as a related network entry on the Trusted interface. It sets up the Trusted interface to accept packets for two networks, 111.222.121.0/24 and 10.0.0.0/24. Thus, machines on the 10.0.0.0/24 network use 10.0.0.1 as the default gateway while machines on the 111.222.121.0/24 network use 111.222.121.2 for their default gateway. The log host for this example is a randomly assigned machine on the Trusted network at 111.222.121.34. The SMTP/FTP/HTTP servers are on 111.222.121.3.

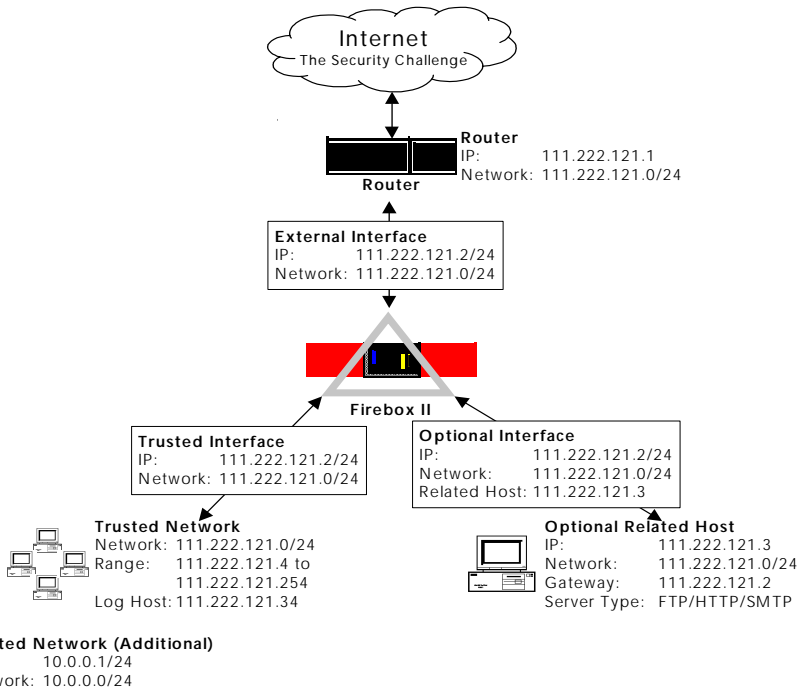


Table 2. Drop-In with Dynamic NAT QuickSetup Wizard Data

Label	IP Addresses
Log Host	111.222.121.34
Default Gateway	111.222.121.1
Firebox Interface	111.222.121.2/24
Related Network	10.0.0.1/24
SMTP Service	111.222.121.3

Policy Manager Configuration

- The Services Arena automatically contains icons for Filtered-HTTP, FTP, ping, SMTP (if you added it), and WatchGuard. Double-click the service and configure with the following settings:

Filtered-HTTP Incoming

- Enabled and Allowed
- From: Any
- To: 111.222.121.3

Filtered-HTTP Outgoing

- Enabled and Allowed
- From: Any
- To: Any

FTP Incoming

- Enabled and Allowed
- From: Any
- To: 111.222.121.3

FTP Outgoing

- Enabled and Allowed
- From: Any
- To: Any

- Configure the individual filter rules for FTP, SMTP incoming and outgoing, and HTTP proxy to your preference.
- Set the local time zone.
- Remove 10.0.0.0/8 from the Blocked Sites list.
- Remove the Management Station as the primary log host. Add the primary log host at 111.222.121.34. Set the log encryption key for the primary log host.
- Save the new configuration to the Firebox.

Additional Configuration

- Go to all hosts on the Trusted network and configure the default gateway to 111.222.121.1.
- Go to all hosts on the related network and configure the default gateway to 10.0.0.1.
- Install the WatchGuard Event Processor (WEP) on host 111.222.121.34. Open the WEP. Set the log encryption key to the same value as configured in the Policy Manager for the primary log host.

Subnetted Network

Subnetting involves taking an existing network (such as a 256-address Class C network) and subdividing it into two or more smaller networks. It enables the creation of a multiple network security configuration without the need to obtain additional IP network address ranges.

When to Use

A multiple network configuration works well when you want to subnet the external and trusted networks and, if you so do desire, the optional network. This separates the Firebox interfaces into distinct subnets, thus allowing you to easily track which machines reside on each network.

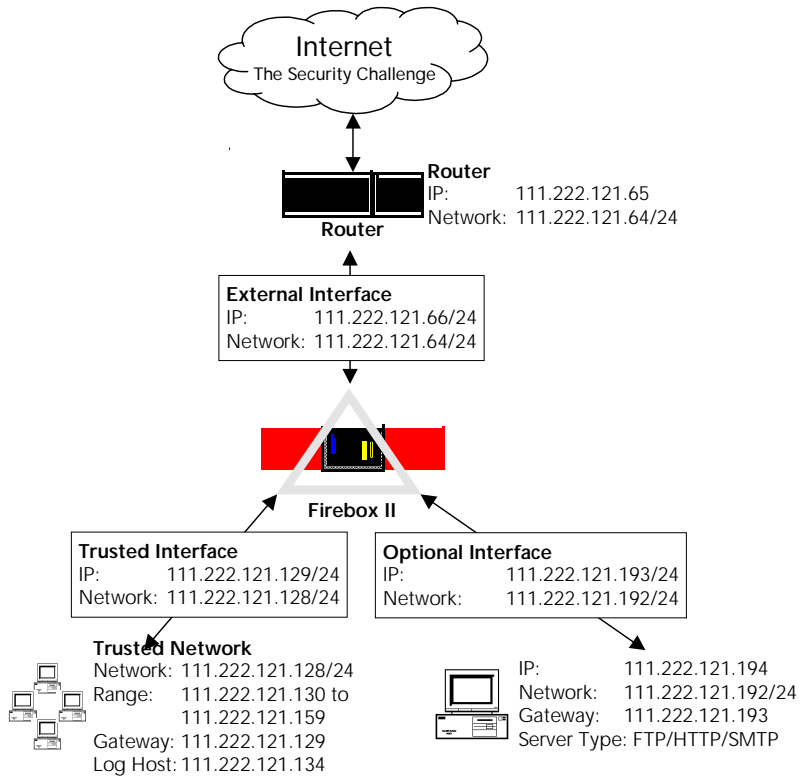
Addressing

In this multiple network configuration example, the interfaces on the Firebox are not on the same network. This translates into a multi-network configuration. To configure this type of network using the QuickSetup Wizard, check the Advanced checkbox on the first wizard screen. In a multiple network installation, you assign a different IP address to each of the Firebox interfaces. The log host for this example is a randomly assigned machine on the Trusted network with IP address 111.222.121.134. The SMTP/HTTP/FTP servers share a machine on the optional network at 111.222.121.194. There are no related networks.

In this example, we subdivide 111.222.121.0/24 into eight subnets:

1. 111.222.121.0 through 111.222.121.31
2. 111.222.121.32 through 111.222.121.63
3. 111.222.121.64 through 111.222.121.95
4. 111.222.121.96 through 111.222.121.127
5. 111.222.121.128 through 111.222.121.159
6. 111.222.121.160 through 111.222.121.191
7. 111.222.121.192 through 111.222.121.223
8. 111.222.121.224 through 111.222.121.254

Hosts on the Trusted network should have their default gateway set to the IP address of the Trusted network interface of the Firebox, 111.222.121.129/24. Hosts on the Optional network should have their default gateway set to the IP address of the Optional network interface of the Firebox, 111.222.121.193/24. Each network is now assigned a separate subnet. The Firebox assumes machines for each subnet are located off their respective interfaces with a default gateway matching the IP address of the interface.



Related Network (Additional)

IP: (none)
 Network: (none)

Table 3. Subnetted QuickSetup Wizard Data

Label	IP Addresses
Log Host	111.222.121.134
Default Gateway	111.222.121.65
External Interface	111.222.121.66/24
Trusted Interface	111.222.121.129/24
Optional Interface	111.222.121.193/24
FTP Service	111.222.121.194
HTTP Service	111.222.121.194
SMTP Service	111.222.121.194

Policy Manager Configuration

- Configure the individual filter rules for FTP, SMTP incoming and outgoing, and HTTP proxy to your preference.
- Set the local time zone.
- Remove the Management Station as the primary log host. Add the primary log host at 111.222.121.134. Set the log encryption key for the primary log host.
- Save the new configuration to the Firebox.

Additional Configuration

- Go to all hosts on the Trusted network and configure the default gateway to 111.222.121.129.
- Go to all hosts on the Optional network and configure the default gateway to 111.222.121.193.
- Install the WatchGuard Event Processor (WEP) on host 111.222.121.134. Open the WEP. Set the log encryption key to the same value as configured in the Policy Manager for the primary log host.

Subnetted Network Using Dynamic NAT

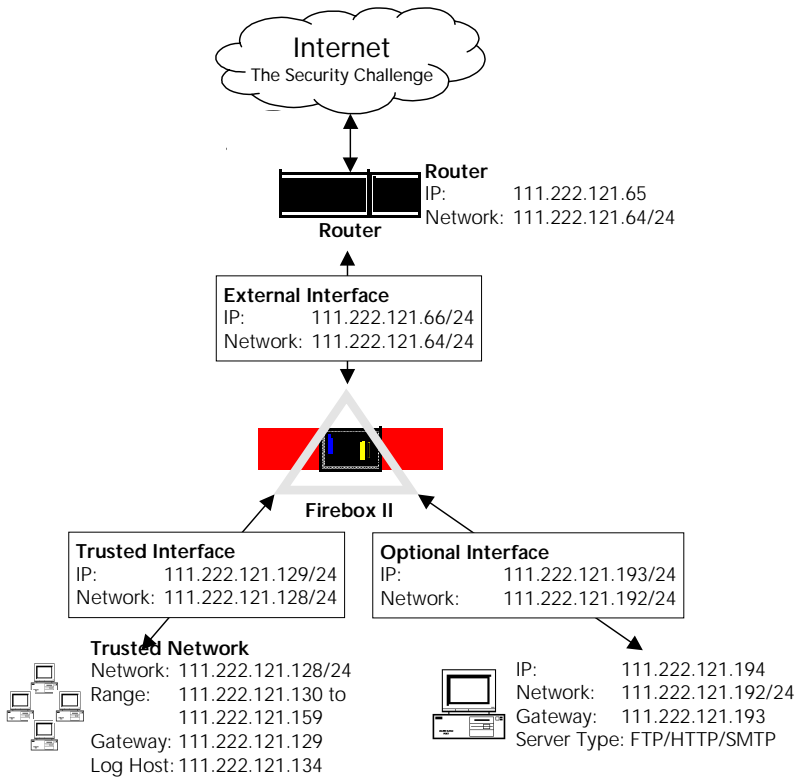
A subnet configuration using dynamic NAT is very similar to a simple subnet configuration except that it adds a network using incoming dynamic network address translation on the Trusted interface. Since the three interfaces are on different networks, we cannot assign them the same IP address. To configure this type of network using the QuickSetup Wizard, check the Advanced checkbox on the first wizard screen.

When to Use

A subnet configuration using dynamic NAT works well when you require different subnets on each Firebox interface, but you also wish to masquerade (hide) a private network behind either the Trusted or Optional interface.

Addressing

There is an entry for 10.0.0.1 as a related network on the Trusted interface. We are telling the Trusted interface to accept packets for two IP addresses, 111.222.121.129 and 10.0.0.1. Therefore, the default gateway for the machines on the related network is 10.0.0.1. Machines on the 111.222.121.129/24 network have a default gateway of 129. For this example, the SMTP/FTP/HTTP servers share IP address 111.222.121.193 and the log host is on the Trusted network at 111.222.121.134.



Related Network (Additional)

IP: 10.0.0.1/24
 Network: 10.0.0.0/24

Table 4. Subnetted Network with Dynamic NAT QuickSetup Wizard Data

Label	IP Addresses
Log Host	111.222.121.134
Default Gateway	111.222.121.65
External Interface	111.222.121.66/24
Trusted Interface	111.222.121.129/24
Optional Interface	111.222.121.193/24
Related Network	10.0.0.1/24
FTP Service	111.222.121.194
HTTP Service	111.222.121.194
SMTP Service	111.222.121.194

Policy Manager Configuration

- Configure the individual filter rules for FTP, SMTP incoming and outgoing, and HTTP proxy to your preference.
- Set the local time zone.
- Remove the Management Station as the primary log host. Add the primary log host at 111.222.121.134. Set the log encryption key for the primary log host.
- Remove 10.0.0.0/8 from the Blocked Sites list.
- Save the new configuration to the Firebox.

Additional Configuration

- Go to all hosts on the Trusted network and configure the default gateway to 111.222.121.129.
- Go to all hosts on the Optional network and configure the default gateway to 111.222.121.193.
- Go to all hosts on the related network and configure the default gateway to 10.0.0.1.
- Install the WatchGuard Event Processor (WEP) on host 111.222.121.134. Open the WEP. Set the log encryption key to the same value as configured in the Policy Manager for the primary log host.

Completing the Network Configuration Worksheet

We encourage you to complete the following network configuration worksheet before installing the WatchGuard LiveSecurity 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 your 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

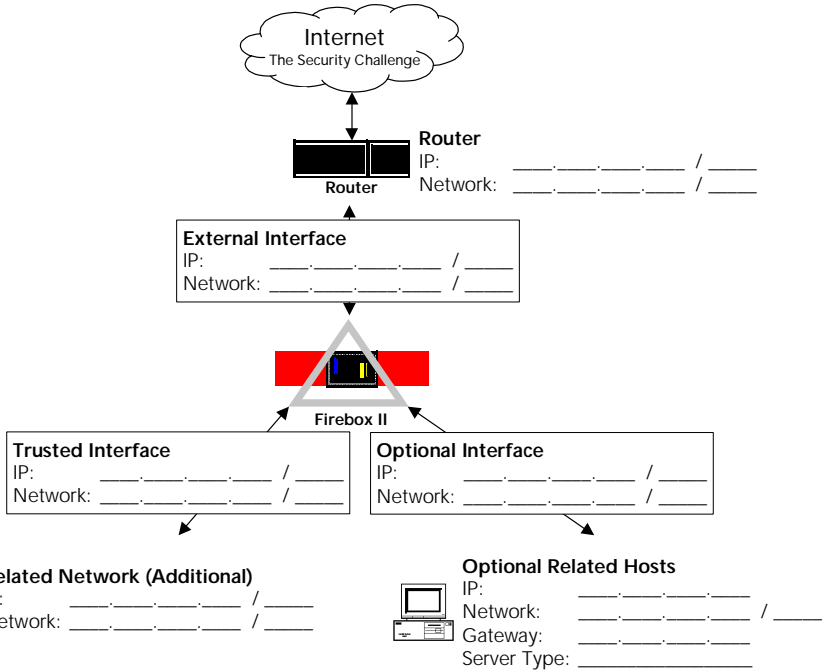


Table 5. Network Configuration Worksheet QuickSetup Wizard Data

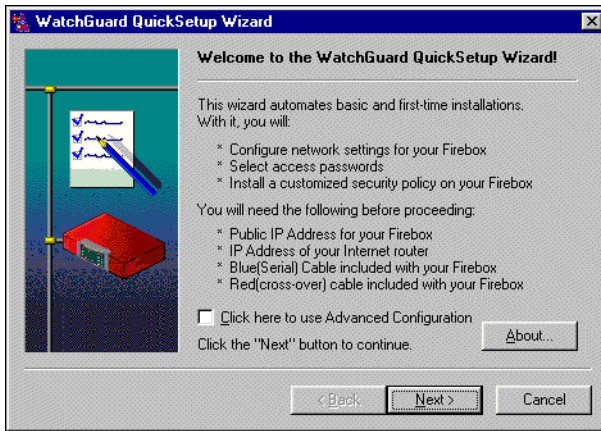
Label	IP Addresses
Log Host	_____
Default Gateway	_____
Firebox Interface (Basic)	_____ / _____
External Interface (Advanced)	_____ / _____
Trusted Interface (Advanced)	_____ / _____
Optional Interface (Advanced)	_____ / _____
Related Network	_____ / _____
SMTP Service	_____
HTTP Service	_____
FTP Service	_____

Running the QuickSetup Wizard

The final step of the WatchGuard LiveSecurity System installation is to run the QuickSetup Wizard. By default, the QuickSetup Wizard starts automatically after you complete installing the software. The QuickSetup Wizard creates a basic configuration file and saves it to the primary area of the Firebox flash disk. The Firebox loads the primary configuration file when it boots.

The QuickSetup Wizard also writes a basic configuration file called `wizard.cfg` to the hard drive of the Management Station. You must then expand the Firebox's basic configuration using the Policy Manager.

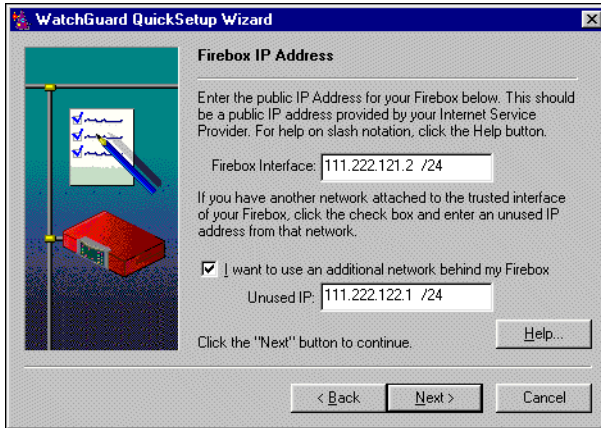
By default, the QuickSetup Wizard starts automatically after you complete installing the LiveSecurity System software. To manually start the QuickSetup Wizard from the Windows desktop, select Start ⇒ Programs ⇒ WatchGuard ⇒ QuickSetup Wizard.



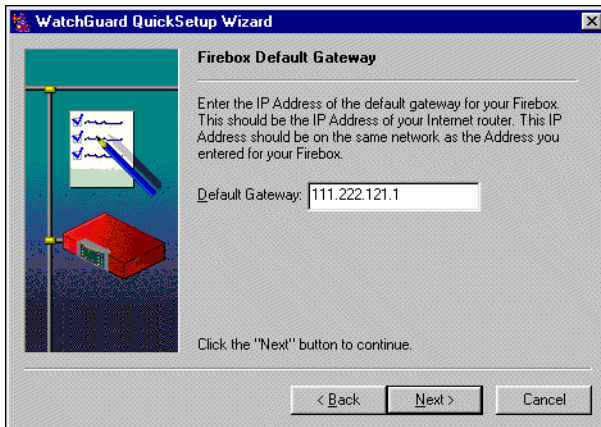
If you have not done so already, complete the Network Configuration Worksheet found on page 29. Select either a Basic (drop-in network) or Advanced (subnetted network).

Basic (Drop-In) Network Configuration

- a. Click Next. Enter the IP address for the Firebox interfaces.
In a drop-in configuration, all three interfaces share the same IP address.

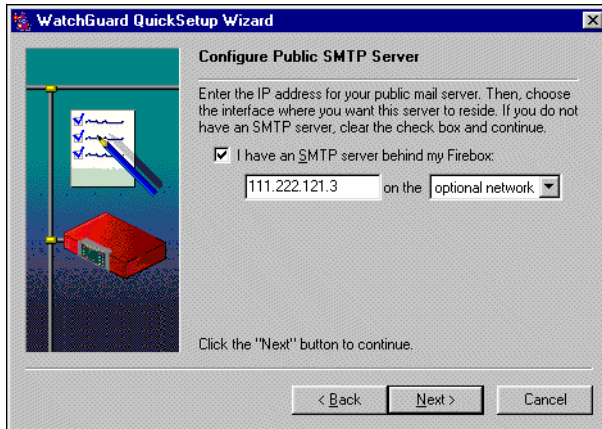


- b. If there is a related network on the Trusted interface using incoming network address translation, enable the "I want to use an additional network behind my Firebox" checkbox. Enter the address of the related network.
- c. Click Next. Enter the default gateway.

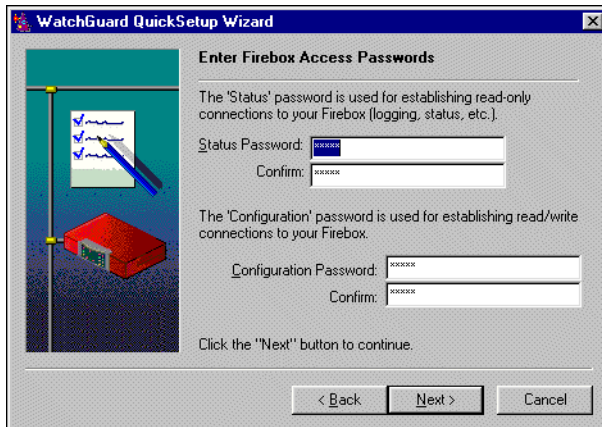


- d. Click Next. If you would like to configure an SMTP server, enable the "I have an SMTP server behind my Firebox" checkbox. Enter the

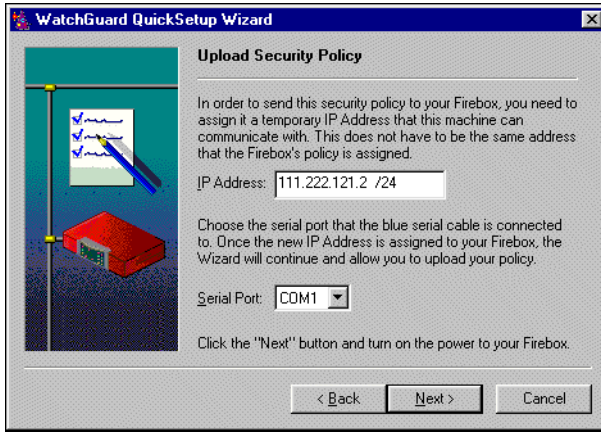
SMTP server IP address. Use the drop-list to select whether the server is on the trusted or optional network.



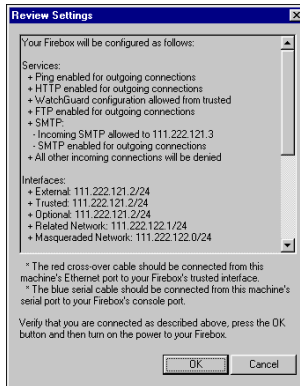
- e. Click Next. Enter the Firebox status (read-only) and configuration (read-write) passwords.
You must select two different values.



- f. Click Next. Enter an address the Firebox can use temporarily. Use the drop list to select the Serial port.



- g. Click Next.
The Review Settings dialog box appears.

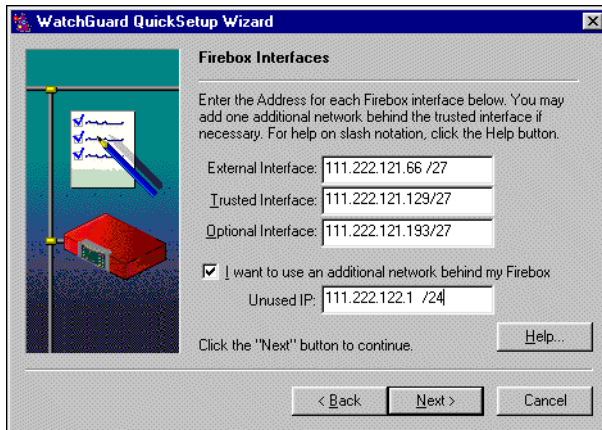


- h. Click OK.
The QuickSetup Wizard creates a basic configuration file.
- i. Turn the Firebox off and then on again.
The QuickSetup Wizard attempts to connect to the Firebox. When a connection is made, the wizard uploads a basic configuration file to the primary area of the Firebox flash disk and initializes the Firebox with the IP addresses you provided. When complete, the Firebox Sys B and Armed indicators light.

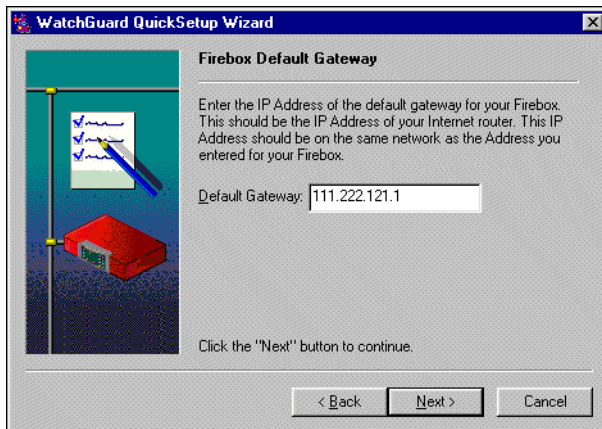
Advanced (Subnetted) Network Configuration

- a. Enable the Advanced Configuration checkbox.
- b. Click Next. Enter the IP address for each of the three Firebox interfaces.

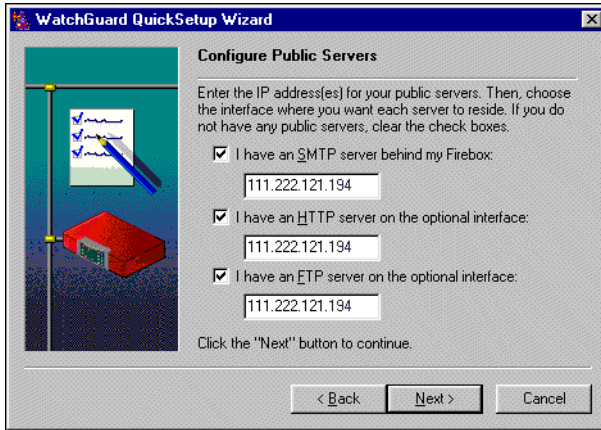
In an advanced (subnetted) configuration, the three Firebox interfaces use different addresses.



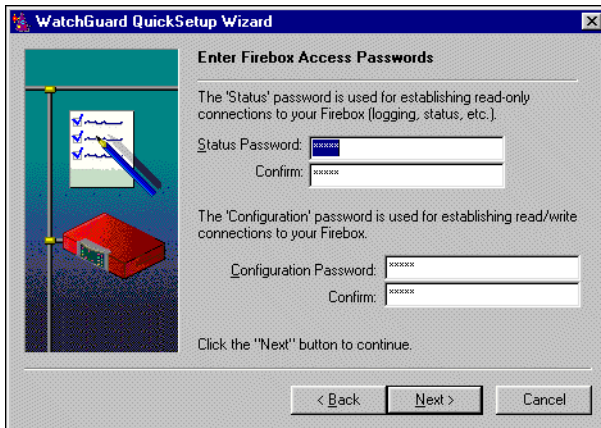
- c. If there is a related network on the Trusted interface using incoming network address translation, enable the "I want to use an additional network behind my Firebox" checkbox. Enter the address of the related network.
- d. Click Next. Enter the default gateway.



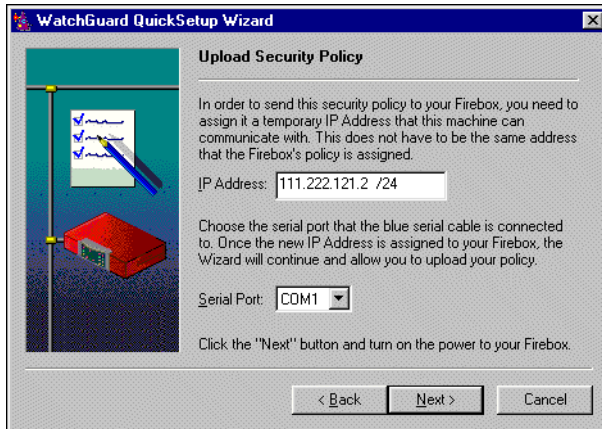
- e. Click Next. If you would like to configure an public servers, enable the appropriate checkbox and enter the server IP address.



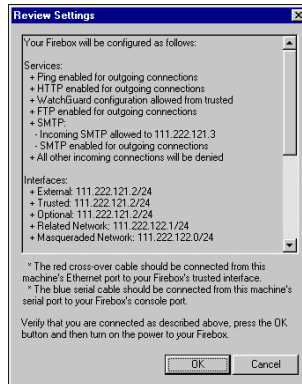
- f. Click Next. Enter the Firebox status (read-only) and configuration (read-write) passwords.
You must select two different values.



- g. Click Next. Enter an address the Firebox can use temporarily. Use the drop list to select the Serial port.



- h. Click Next.
The Review Settings dialog box appears.



- i. Click OK.
The QuickSetup Wizard creates a basic configuration file.
- j. Turn the Firebox off and then on again.
The QuickSetup Wizard attempts to connect to the Firebox. 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.

After You Install

Your Firebox can now communicate with the Management Station over your network.

- a. Complete the additional recommended configuration for your network type. See “Designing a Basic Network Configuration” on page 17.
- b. Disconnect the Firebox.
- c. Install the Firebox on your network.
The most common location is physically between the Internet router and connections to your trusted and optional networks.
- d. Connect your Ethernet lines to the Firebox Trusted, External, and Optional interfaces as appropriate.
Specific connections vary according to the simple or multiple network configuration created. You are not required to connect the Optional interface if it is not part of your network configuration.
- e. Reboot the Management Station.
If you have designated the Management Station as the primary log host, the WatchGuard Event Processor starts.
- f. Open the *User Guide* for additional configuration instructions.
- g. Using Adobe Acrobat Reader® you can print all or part of the *Reference Guide* and *Internet Security Handbook* for additional information.

