

WatchGuard® SOHO User Guide

SOHO and SOHO|tc 2.4



Registration and identification information

Please use this area to enter your SOHO information.

SOHO Serial Number:	
LiveSecurity User ID:	
Password:	

The SOHO serial number is located on the bottom of the SOHO. You create a LiveSecurity user ID and password when you register your WatchGuard SOHO or SOHO | tc. To register, after you install your SOHO, open your browser to <http://192.168.111.1/login.htm> and click **Click here to register your SOHO**.

Please keep this information in a secure place.

Copyright and patent information

Copyright © 1999-2001 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard and LiveSecurity are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and other countries. Firebox is a trademark of WatchGuard Technologies, Inc.

CyberPatrol is a registered trademark of SurfControl, Inc.
DocVer: B-2.4-User-2

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

WatchGuard® End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE

This WatchGuard End-User License Agreement (“EULA”) is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. (“WATCHGUARD”) for the WATCHGUARD software product you have purchased, which includes computer software and any separately installed components, and any updates or modifications thereto, and which may include associated media, printed materials, and on-line or electronic documentation (the “SOFTWARE PRODUCT”). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this EULA. Please read this EULA carefully. By installing or using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid.

- 1. OWNERSHIP AND LICENSE.** The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its suppliers. Your rights to use the SOFTWARE PRODUCT are as specified in this EULA, and WATCHGUARD retains all rights not expressly granted to you in this EULA. Nothing in this EULA constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.
- 2. PERMITTED USES.** You are granted the following rights to the SOFTWARE PRODUCT:
(A) You may install and use the SOFTWARE PRODUCT on any computer with an associated connection to the hardware product (the “Hardware”); (B) You may install and use the SOFTWARE PRODUCT on more than one computer at once without licensing an additional copy of the SOFTWARE PRODUCT for each additional computer on which you want to use it, provided each computer on which you install the SOFTWARE PRODUCT has an associated connection to the Hardware; and (C) You may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.
- 3. PROHIBITED USES.** You may not, without express written permission from WATCHGUARD: (A) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT; (B) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this EULA; (C) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective; (D) Sublicense, lend, lease or rent the SOFTWARE PRODUCT; or (E) Transfer this license to another party unless (i) the transfer is permanent, (ii) the third party recipient agrees to the terms of this EULA, and (iii) you do not retain any copies of the SOFTWARE PRODUCT.

4. LIMITED WARRANTY. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer; (A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD or the authorized dealer from whom you obtained the SOFTWARE PRODUCT with a dated proof of purchase; and (B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and your authorized dealer will provide you with a new version of the SOFTWARE PRODUCT or a full refund at its election.

DISCLAIMER AND RELEASE. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD OR ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THIS SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

LIMITATION OF LIABILITY. WATCHGUARD'S liability AND THE LIABILITY OF ITS LICENSORS (whether in contract, tort, or otherwise; and notwithstanding any fault, negligence, strict liability or product liability) with regard to THE SOFTWARE Product will in no event exceed the purchase price paid by you for such Product. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD OR ITS LICENSORS BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD AND ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF

SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed SOFTWARE PRODUCT and documentation are provided with Restricted Rights. Use, duplication or disclosure by the U.S Government or any agency or instrumentality thereof is subject to restrictions as set forth in DFARS 227.7202-3 (Commercial Computer Software) and DFARS 252.227-7015(b) (Technical Data-Commercial Items) -- Restricted Rights Clause at FAR 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Incorporated, 505 Fifth Avenue, South, Suite 500, Seattle, WA 98104.

6. EXPORT CONTROLS. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. TERMINATION. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this EULA, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. MISCELLANEOUS PROVISIONS. This EULA will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire EULA between us relating to the contents of this package, and supersedes any prior purchase order, communications, advertising or representations concerning the contents of this package AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this EULA will be valid unless it is in writing, and is signed by WATCHGUARD.

9. CANADIAN TRANSACTIONS. If you obtained this SOFTWARE PRODUCT in Canada, you agree to the following: The parties hereto have expressly required that the present EULA be drawn up in the English language. / Les parties aux presentes ont expressement exige que la presente conventions et ses Annexes soient redigees en la langue anglaise.

WatchGuard® Limited Hardware Warranty

This WatchGuard Limited Hardware Warranty (the "Warranty") applies to the enclosed WatchGuard hardware product (the "Hardware Product"). By using the HARDWARE Product, you agree to the terms hereof. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from whom you purchased the Hardware Product for a full refund. THIS WARRANTY DOES NOT APPLY TO THE WATCHGUARD SOFTWARE REQUIRED FOR OPERATION AND USE OF THE HARDWARE PRODUCT. PLEASE REFER TO THE ENCLOSED WATCHGUARD END-USER LICENSE AGREEMENT (THE "EULA") FOR THE SOFTWARE WARRANTY AND OTHER TERMS AND CONDITIONS ASSOCIATED WITH USE OF THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THE EULA, PLEASE RETURN THIS PACKAGE IN ACCORDANCE WITH THIS PARAGRAPH.

NOW, THEREFORE, WatchGuard Technologies and you agree as follows:

1. Limited Warranty. WatchGuard Technologies warrants that upon delivery and for one (1) year thereafter (as the same may be extended pursuant to Section 2 below, the "Warranty Period"): (a) the Hardware Product will be free from material defects in materials and workmanship, and (b) the Hardware Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard Technologies applicable specifications. This warranty does not apply to any Hardware Product that has been: (i) altered, repaired or modified by any party other than WatchGuard Technologies; or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Hardware Product from the manufacturers of Hardware Product components. However, you agree not to look to WatchGuard Technologies for, and hereby release WatchGuard Technologies from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.
2. Remedies. If any Hardware Product does not comply with WatchGuard Technologies warranties set forth in Section 1 above, WatchGuard Technologies will, at its option, either (a) repair the Hardware Product, or (b) replace the Hardware Product; provided, that you will be responsible for returning the Hardware Product to the place of purchase and for all costs of shipping and handling. As to any Hardware Product repaired or replaced by WatchGuard Technologies, the Warranty Period will end one (1) year after delivery of the repaired or replacement Hardware Product. Any Hardware Product, component, part or other item replaced by WatchGuard Technologies becomes the property of WatchGuard Technologies. WatchGuard Technologies shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Hardware Products.
3. Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD TECHNOLOGIES, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD TECHNOLOGIES AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD TECHNOLOGIES, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY

NONCONFORMANCE OR DEFECT IN THE HARDWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD TECHNOLOGIES AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE HARDWARE PRODUCT).

4. Limitation of Liability. WATCHGUARD TECHNOLOGIES' liability (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) with regard to any HARDWARE Product will in no event exceed the purchase price paid by you for such HARDWARE Product. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD TECHNOLOGIES BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY, FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE HARDWARE PRODUCT, EVEN IF WATCHGUARD TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. Miscellaneous Provisions. This Warranty will be governed by the laws of the state of Washington, without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sale of Goods, as amended, shall not apply. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard Technologies and you relating to the contents of this package, and supersedes any prior purchase order, communications, advertising or representations concerning the contents of this package AND BY USING THE HARDWARE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this Agreement will be valid unless it is in writing, and is signed by WatchGuard Technologies.

Welcome

Congratulations on purchasing the ideal solution for providing secure access to the Internet—the WatchGuard SOHO or WatchGuard SOHO | tc. Your new security device will give you peace of mind when connecting to the Internet using a high-speed cable or DSL modem, a leased line, or ISDN.

This User Guide applies to both the SOHO and SOHO | tc. The only difference between these two devices is the ability to create and use a Virtual Private Network (VPN). VPN can be added to the SOHO, while the SOHO | tc already has installed VPN capabilities.

In this guide, the name SOHO is used to refer to both the SOHO and SOHO | tc. The most current installation and user information is available on the Internet at:

<http://www.watchguard.com/pubs/install/index.asp>

Contacting Technical support

(877) 232-3531	U.S.; End-user support
(206) 521-8375	U.S.; Authorized Reseller support
(360) 482-1083	International support

Redeeming SOHO upgrade certificates

Once you have purchased an upgrade certificate, go to the following Web site:

<http://bisd.watchguard.com/soho/upgrade>

Please follow the instructions at this site to redeem your certificate and activate your upgrade. You do not need to have registered the unit and created a login prior to redeeming the certificate.

Using this guide

This manual assumes that you are familiar with your computer's operating system. If you have questions about navigating in your computer's environment, please refer to your system user manual.

The following conventions are used throughout this guide.

Convention	Indication
Bold type	Denotes menu commands, dialog box options, Web page options, Web page names. For example: "On the System Information page, select Disabled ."
CAUTION	Denotes a warning or precautionary information.
NOTE	Denotes important information, a helpful tip, or additional instructions.

Table of Contents

Table of Contents xi

CHAPTER 1 Installation	1
Before you begin	1
Performing manual installation	2
Physically connecting your SOHO	6
CHAPTER 2 Setting Up Your SOHO Network	11
How does a firewall work?	11
Configuring your external network	12
Configuring your trusted network	21
Changing the SOHO system name and password ..	22
Default factory settings	24
Troubleshooting installation and network configuration	26

CHAPTER 3	Configuring Services for a SOHO	37
	How does information travel on the internet?	37
	Allowing incoming services	39
	Blocking outgoing services	44
CHAPTER 4	Configuring Virtual Private Networking	49
	Why create a virtual private network?	49
	What you will need	50
	Special considerations	53
	Frequently asked questions	53
CHAPTER 5	Additional SOHO Features	57
	SOCKS for SOHO	57
	SOHO logging	60
	Rebooting a WatchGuard SOHO	61
CHAPTER 6	WatchGuard SOHO WebBlocker	63
	How WebBlocker works	63
	Purchasing and enabling SOHO WebBlocker	65
	Configuring the SOHO WebBlocker	66
	WebBlocker categories	71
	Searching for blocked sites	75
	Index	77

Before you begin

Pre-installation checklist

Before installing your new WatchGuard SOHO please ensure that you have:

- A 10BaseT Ethernet I/O network card installed in your computer.
- A cable or DSL modem with a 10BaseT port.
- Two Ethernet network cables with RJ45 connectors. These must *not* be “crossover cables” (which are usually red or orange). One cable is furnished with your unit. A second cable may have been supplied with your modem. If not, you will need to purchase a second Ethernet, RJ45 cable. Make sure that both cables are long enough to comfortably connect the modem to the SOHO and the SOHO to the computer in your individual office environment.

Performing manual installation

- An operational Internet connection. Setup of your SOHO requires access to the Internet. If your connection does not work, please contact your Internet service provider (ISP). When your connection has been established, you may proceed with installation and setup.
- If you have either a cable or DSL modem, consult the manual that came with your service, or call the ISP to find out whether your particular modem supports DHCP or PPPoE. You will need this information later in the installation process.
- If you are using PPPoE to connect to your local Internet service provider, the WatchGuard SOHO must be running firmware version 2.0 or later.
- An installed Web browser—either Netscape Navigator 4.5 (or higher) or Internet Explorer 4.0 (or higher).
- SOHO serial number.

Performing manual installation

Before you begin the installation process, connect to the Internet. You need to determine your current TCP/IP settings and disable your HTTP proxy.

NOTE

You must also know whether your ISP provides you with Dynamic or Static TCP/IP settings. For assistance in determining this, please see, “Network addressing” on page 12.

Determine your current TCP/IP settings

For your reference, record the computer's current TCP/IP settings in the chart provided at the end of this section. Different operating systems will supply different information. To locate your settings:

Microsoft Windows NT or 2000

- 1 Click **Start** ⇒ **Programs** ⇒ **Command Prompt**.
- 2 At the `C:\` prompt, enter `ipconfig/all`. Press **Enter**.
- 3 Enter your current TCP/IP settings in the chart provided below.
- 4 Click **Cancel**.

Microsoft Windows 95 or 98 or ME

- 1 Click **Start** ⇒ **Run**.
- 2 Type: `winiipcfg`. Click **OK**.
- 3 Select the "Ethernet Adapter."
Enter your current TCP/IP settings in the chart provided below.
- 4 Click **Cancel**.

Macintosh

- 1 Click **Apple menu** ⇒ **Control Panels** ⇒ **TCP/IP**.
- 2 Enter your current TCP/IP settings in the chart provided below.
- 3 Close the window.

Other operating systems (Unix, Linux)

- 1 Consult your operating system guide to locate the TCP/IP screen.
- 2 Enter settings in the chart provided below.

Performing manual installation

3 Exit the TCP/IP configuration screen.

TCP/IP Setting	Value
IP Address	. . .
Subnet Mask	. . .
Default Gateway	. . .
DHCP Enabled	Yes No
Primary WINS Server	. . .
Secondary WINS Server	. . .
DNS Server(s) Primary	. . .
Secondary	. . .

NOTE

If you are connecting more than one computer to the trusted network behind the SOHO, obtain the configuration TCP/IP information for each computer.

Disable your browser's HTTP proxy

To configure a WatchGuard SOHO after it is installed, you must be able to access the special configuration pages that reside on the SOHO. If the HTTP proxy in your browser is enabled, you can not access these pages, and you can not complete the configuration process.

With the HTTP proxy enabled, the browser automatically points itself to Web pages located on the Internet, and you cannot direct the browser to Web pages located in other places. Disabling the HTTP will not prevent you from accessing your favorite Web sites, but it will allow you to access the special configuration pages that reside only on the SOHO.

To disable the HTTP proxy in three commonly used browsers, see the instructions below. If your browser is not listed, see your browser Help menus to learn how to disable the HTTP proxy.

Netscape 4.5 or 4.7

- 1 Open Netscape.
- 2 Click **Edit** ⇒ **Preferences**.
The Preference dialog box appears.
- 3 Click the **+** before **Advanced** to expand the heading.
- 4 Click **Proxies**.
- 5 Select **Direct Connection to the Internet**.
- 6 Verify that the **Automatic Proxy Configuration** checkbox is enabled.
- 7 Click **OK** to save the settings.

Internet Explorer 4.0

- 1 Open Internet Explorer.
- 2 Click **View** ⇒ **Internet Options**.
- 3 Select the **Connections** tab.
- 4 Disable the checkbox **Access the Internet using a proxy server**.
- 5 Enable the checkbox **Connect to the Internet using a local area network**.

Physically connecting your SOHO

- 6 Click **Configure** at the bottom on the **Internet Options** screen.
- 7 Record the URL box information here: _____
- 8 Click **OK** to save settings.

Internet Explorer 5.0

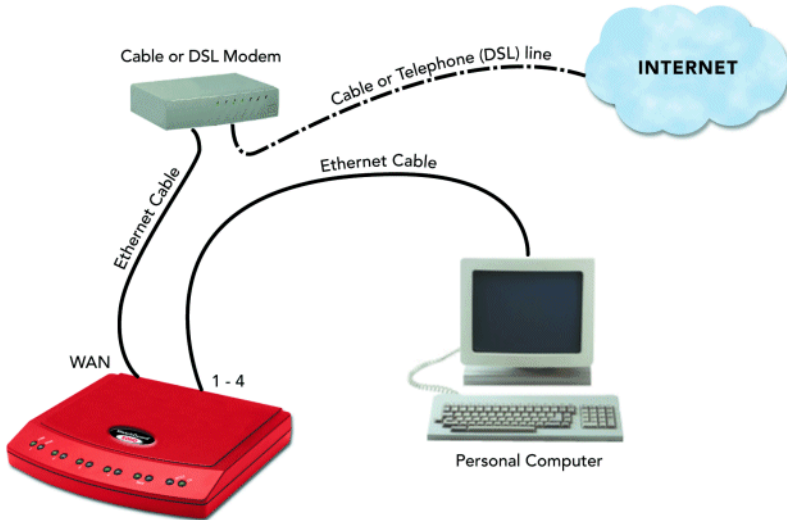
- 1 Open Internet Explorer.
- 2 Click **Tools** ⇒ **Internet Options**.
The Internet Options screen displays.
- 3 Click the **Advanced** tab.
- 4 Scroll down the page to **HTTP 1.1 Settings**.
- 5 Clear all checkboxes.
- 6 Click **OK** to save the settings.

Physically connecting your SOHO

Your WatchGuard SOHO can be used to protect a single computer or a multi-computer network. It can also function as a hub to connect a variety of other devices.

Cabling the SOHO for one to four devices

The SOHO has four (numbered 1-4) Ethernet ports. Each can be used to connect a variety of devices. These may include computers, printers, scanners, or other network peripherals. Your SOHO may replace an existing hub if you have no more than four devices to connect.



WatchGuard SOHO

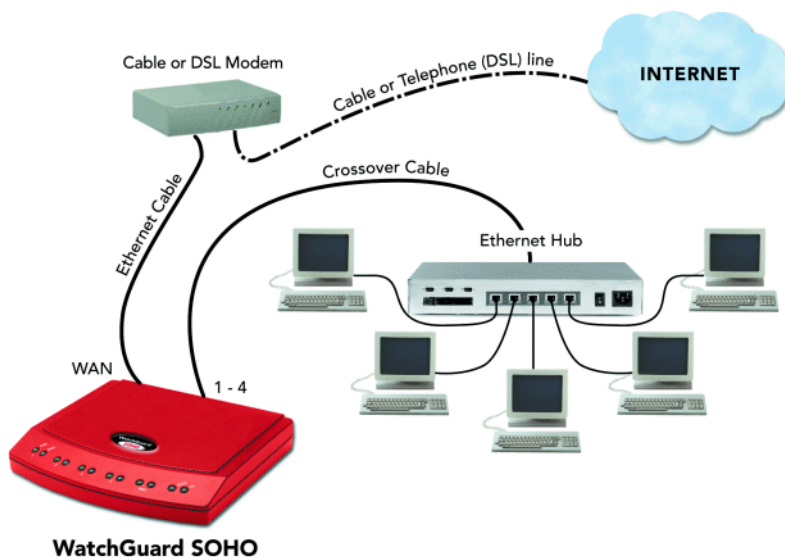
- 1 Complete the “Pre-installation checklist” on page 1.
- 1 Shut down your computer and unplug the power from your DSL or cable modem.
- 2 Unplug the Ethernet cable that is connected from your cable or DSL modem to your computer and plug it into the WAN port on the SOHO unit. The SOHO unit is now connected directly to the modem.
- 3 Plug the Ethernet cable supplied with your SOHO into any one of the four (numbered 1-4) Ethernet ports on the SOHO. Plug the other end into the Ethernet card installed in your computer. The SOHO unit will then be connected between your modem and computer.
- 4 Restore the power to your DSL or cable modem. Wait until the indicator lights of the cable modem have stopped flashing indicating that the cable modem is ready.

Physically connecting your SOHO

- 5 Attach the power cord to the SOHO and plug it into an outlet.
- 6 Restart your computer.
- 7 For information on the factory default configuration options, see “Default factory settings” on page 24. For specialized configurations, see “Configuring your external network” on page 12, as well as, “Configuring your trusted network” on page 21.

Cabling the SOHO for more than four computers

While there are only four (numbered 1-4) Ethernet ports on the back of the SOHO, you can connect many more devices to your SOHO using network hubs.



The SOHO and SOHO lite ship with a “10-seat” license. In other words, the SOHO allows up to ten computers on a network behind

the SOHO to access the Internet. More than ten computers can exist on the network and communicate with each other, but only the first ten which attempt to access the Internet will be allowed through the SOHO. If you would like to upgrade your SOHO to a twenty-five or fifty-seat user license, please visit:

<http://www.watchguard.com/sales/buyonline.asp>

- 1 Complete the “Pre-installation checklist” on page 1.
- 2 You will need these additional items:
 - One or more Ethernet hubs.
 - An Ethernet cable (with RJ-45 connectors) for each computer to connect to the SOHO.
 - An Ethernet cable to connect each hub to the SOHO.
- 3 Turn off your computer and unplug the power from the cable or DSL modem.
- 4 Unplug the Ethernet cable that is connected from your cable or DSL modem to your computer, and instead connect it from your modem to the WAN port on the SOHO.
This creates a connection between the SOHO and the modem.
- 5 Plug an Ethernet cable into any of the four (numbered 1-4) Ethernet ports on the SOHO. Plug the other end into an Ethernet hub.
- 6 Using Ethernet cables, connect the hub uplink port to the Ethernet card installed in each of your computers.
- 7 Turn on the power to your cable or DSL modem. Wait until the lights stop flashing, indicating that the modem is ready.
- 8 Attach the power cord to the SOHO and plug it into an outlet.
- 9 Restart your computer.

Setting Up Your SOHO Network

How does a firewall work?

Fundamentally, a firewall is a way of differentiating between, as well as protecting, “us” from “them”. On the external side of your SOHO firewall is the entire Internet. The Internet has many resources that you want to be able to reach, such as the Web, e-mail, and conferencing. It also presents dangers to the privacy and security of your computers. On the trusted side of your SOHO firewall are all the devices you want to protect from these dangers.

Using rules we will discuss in Chapter 3: “Configuring Services for a SOHO” on page 37, the WatchGuard SOHO evaluates all traffic between the external network (Internet) and the trusted network (your computers) and blocks any suspicious activity. In order for this to work as described, you must first configure both the external and trusted networks to work together and to talk to one another as well as the rest of the world.

NOTE

The configuration instructions in this chapter assume that you are using Windows 95/98/ME. If this is not the case, see your operating system help or user guide to locate the equivalent options and commands.

Configuring your external network

When you configure the external network, you establish how the SOHO communicates with your Internet service provider (ISP). This configuration is very much dependent on how your ISP distributes network addresses—using DHCP or PPPoE.

Network addressing

Each networked computer in the entire world must have an IP address to identify itself to other computers. The most common method to distribute IP addresses is to use Dynamic Host Configuration Protocol (DHCP). When you connect your computer to the network, a DHCP server at your ISP automatically assigns it a network IP address. This eliminates the ISP from having to manually assign and manage IP addresses.

IP address assignments can be either dynamic or static. With dynamic, your ISP assigns your computer a new address every time you connect. When you power down, you release the address, and it may be reassigned. An IP address that is static, on the other hand, belongs to your computer at all times whether or not you are currently using it. No other computer anywhere on the network shares the same address.

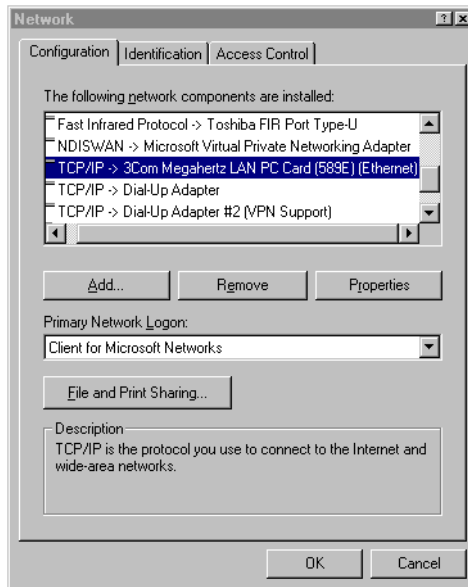
A third way of assigning addresses is called PPPoE (Point-to-Point Protocol over Ethernet). PPPoE combines some of the advantages

of Ethernet and PPP by simulating a standard Dial-Up connection. It is popular among many ISPs because it enables them to use existing Dial-Up infrastructure such as billing, authentication, and security for DSL and cable modems.

Determining whether your ISP uses dynamic or static addressing

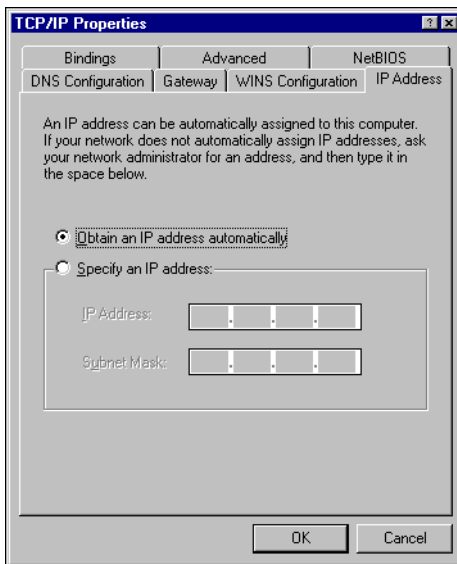
Most ISPs support both dynamic and static addressing. To determine if your connection to the Internet is dynamic or static:

- 1 Click **Start** ⇒ **Settings** ⇒ **Control Panel**.
The Control Panel window appears.
- 2 Double-click the **Network** icon.
The Network dialog box appears.



Configuring your external network

- 3 Scroll through the list of installed network components. Double-click the **TCP/IP** network component which is bound to your Ethernet card. Look for (Ethernet) in parentheses. The TCP/IP Properties dialog box appears.



- 4 If "Obtain an IP Address Automatically" is selected, your computer is configured for dynamic DHCP. If "Obtain an IP Address Automatically" is not checked, your computer is configured for static addressing.

Configuring the SOHO external network for dynamic addressing

Out of the box, the SOHO is configured to obtain its external address information automatically, using dynamic DHCP. So if your ISP assigns you an address automatically (or dynamically), the SOHO itself will obtain all the addressing information it needs

when it powers on and attempts to connect to the Internet. No further configuration of the SOHO is required. To complete the SOHO External Network configuration, see “Release and renew the IP configuration” on page 20.

Configuring the SOHO external network for static addressing

If you are assigned a static address, then you must transfer the permanent address assignment from your computer to the SOHO itself. Instead of communicating directly to your computer, the ISP will now communicate first through the SOHO. To do this you must both modify the static settings on your personal computer as well as enter the information into the SOHO Configuration pages.

NOTE

The SOHO supports a mini, onboard Web server which provides a Web interface for configuring the unit. Therefore, the SOHO configuration pages are reached via your Web browser. Simply point your Web browser to the internal, Trusted IP address of the SOHO to reach these Web pages.

On your computer:

- 1 Click **Start** ⇒ **Settings** ⇒ **Control Panel**.
The Control Panel window appears.
- 2 Double-click the **Network** icon.
The Network dialog box appears.
- 3 Double-click the **TCP/IP** network component which is bound to your Ethernet card. Look for **(Ethernet)** in parentheses.
The Properties window appears with the addressing information already filled in.

- 4 Select the **Obtain an IP address automatically** option. Click **OK**.
Reminder: The wording may differ slightly depending on the operating system. A similar option, however, is found on all platforms.
- 5 If prompted with “Do you want to enable DHCP?” click **Yes**.
- 6 Save the changes.
- 7 On most platforms, click **OK** until the Control Panel window closes.
- 8 Shut down and reboot the computer.

On the SOHO:

- 1 Open your Web browser. Click **Stop**.
At this point, the Internet connection is not fully configured, and the computer cannot load your home page from the Internet. However, the computer can access special configuration Web pages installed on the SOHO itself.
- 2 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 3 Click **External Network**.

Configuration: External Network

From the drop down list below, select the configuration method for the External Network interface and then push the "Configure" button to complete the configuration process.

The configuration method for your External Network interface depends upon your Internet Service Provider. If your ISP supports DHCP, then this information can be obtained automatically. For DHCP configuration select the "DHCP Client" option in the drop down list below.

If DHCP is not supported, then you must enter the information manually. For manual configuration select the "Manual Configuration" option in the drop down list below.

PPPoE is a protocol used in place of DHCP by many DSL service providers to deliver configuration information. If you have been assigned a login name and password, and you have DSL service, then you are probably using PPPoE. For PPPoE configuration select the "PPPoE Client" option in the drop down list below.



A screenshot of a web-based configuration interface. It features a dropdown menu with the text 'DHCP Client' and a small downward-pointing arrow on the right. Below the dropdown menu is a rectangular button with the text 'Configure'.

[[LiveSecurity Home](#)] [[Configuration Home](#)] [[Help](#)] [[Support](#)] [[About Us](#)]

- 4 From the drop list, select **Manual Configuration**.
- 5 Enter the TCP/IP settings you copied from the computer when you started the install process.
- 6 Click **Submit**.

To complete SOHO External Network configuration, see “Release and renew the IP configuration” on page 20.

Configuring SOHO external network for PPPoE

While less common, PPPoE is another method for an ISP to assign addresses. Check the information and manuals sent to you by your ISP to see if they use PPPoE. If you cannot find this information, contact your ISP and ask. You will need your PPPoE login name and password.

NOTE

If you are using PPPoE to connect to your ISP, the SOHO must be running firmware version 2.0 or later.

To configure the SOHO for PPPoE:

- 1 **Open your Web browser and click **Stop**.**
At this point, the Internet connection is not fully configured, and the computer cannot load your home page from the Internet. However, the computer can access special configuration Web pages installed on the SOHO itself.
- 2 **With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.**
For example, if using the default IP address, go to: <http://192.168.111.1>
- 3 **Click **External Network**.**
The External Network page appears.
- 4 **From the drop list, select **PPPoE Client**.**
The PPPoE Client configuration page appears.

The screenshot shows the WatchGuard configuration page for a PPPoE Client. The top navigation bar includes the WatchGuard logo and links for LIVESECURITY, LOCAL SETTINGS, HELP, SUPPORT, ABOUT US, and CONTACT US. The main content area is titled "Configuration: External Network -> PPPoE Client". Under the "PPPoE Client" heading, there are two input fields: "Name" with the value "rodolfo" and "Password" with masked characters. A checkbox labeled "Automatically restore lost connections" is checked. Below the form are "Submit" and "Reset" buttons. At the bottom, there are links for LiveSecurity Home, Configuration Home, Help, Support, and About Us.

5 Enter the PPPoE login name supplied by your ISP.

6 Enter the PPPoE password supplied by your ISP

7 Click **Automatically restore lost connections**.

This enables a constant flow of “heartbeat” traffic between the SOHO and the PPPoE server. In the event of routine packet loss, this option allows the SOHO to maintain its PPPoE connection. The SOHO may reboot to recover the PPPoE connection if the heartbeat fails. This provides for a more consistent Internet connection but will be seen as continuous traffic by the ISP and regulated as such.

8 Click **Submit**.

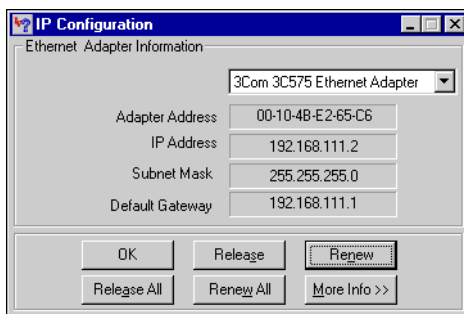
The configuration change is saved to the SOHO.

To complete SOHO External Network configuration, see “Release and renew the IP configuration” on page 20.

Release and renew the IP configuration

Regardless of what type of addressing your computer used originally, it will now obtain all of its information from the SOHO itself, using DHCP. To enable your computer to talk to the SOHO you must force it to release and renew all its IP configuration information. From your computer:

- 1 Click **Start** ⇒ **Programs** ⇒ **Command Prompt**.
- 2 At the **C:** prompt, enter `wi n i p c f g`. Press **Enter**.
The IP Configuration dialog box appears.
- 3 Verify that the information is displayed for "Ethernet Adapter," not for "PPP Adapter," which applies to a dial-up telephone modem.
- 4 Click the **Release** button. Then click the **Renew** button.
Your IP Configuration should look similar to the screenshot below. The values in the IP Configuration dialog box were obtained from the SOHO itself. The IP Address, Subnet Mask and Default Gateway entries must be completed and have the values displayed for address sharing to work as in the figure below. If you obtain different results, see "Troubleshooting installation and network configuration" on page 26.



Configuring your trusted network

Out of the box, the SOHO automatically uses DHCP to assign addresses to any computer on your trusted network. In other words, every time you connect a computer to the SOHO, either directly or through a hub, it automatically attempts to obtain its addresses from the SOHO itself.

NOTE

To disable the SOHO DHCP server and assign addresses statically on your trusted network, open the SOHO Configuration menu, click Trusted Network, and disable the checkbox labeled Enable DHCP Server. This is not recommended for most SOHO users.

Configure additional computers to the trusted network

Up to four computers can be plugged directly into the four (numbered 1-4) Ethernet ports of the SOHO. A larger number of computers can be networked together by using one or more readily available 10BaseT Ethernet hubs with RJ-45 connectors. The SOHO system will coexist with other communications over the same local area network, and you can mix computers with different operating systems. If you wish to add one or more computers to your trusted network:

- 1 Ensure that any additional computer has an Ethernet card installed. Shut the computer down, connect it to the network the same way you did in “Cabling the SOHO for more than four computers” on page 8. Restart the computer.
- 2 Set the computer to obtain its address dynamically.
see “Determining whether your ISP uses dynamic or static addressing” on page 13.
- 3 Turn off and restart the computer.

- 4 Release and renew the IP configuration.
see "Release and renew the IP configuration" on page 20.. The computer will then obtain its TCP/IP settings dynamically from the SOHO unit.

Changing the SOHO system name and password

Passwords are a barrier between your computer and anyone trying to break in. They are the first line of defense in computer security. They are, unfortunately, the most frequently overlooked of all security measures. The SOHO system name and password are designed to protect the SOHO configuration from being altered by someone on your trusted network. In other words, when you have configured a SOHO system name and password, no one in your office or home will be able to change (deliberately or accidentally) your firewall settings without the system name and password.

CAUTION

Take steps to ensure that you do not lose your system name and password. Once you have enabled password protection, there is no other means of accessing your SOHO settings. Should you forget your name and/or password, the only means of resetting requires reverting your SOHO to its factory settings;, please see "How do I reset the SOHO to factory defaults?" on page 32, you will then need to reconfigure your SOHO.

You should change your password at least once a month to be secure. A password should be a combination of letters, numbers, and symbols that do not spell out common words. It should contain at least one special character, number, and a mixture of

upper and lower case letters. To change the SOHO system password:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>. If this does not work, see "Troubleshooting installation and network configuration" on page 26.
- 2 Select **System Administration**.
The System Administration page appears.
- 3 Select **System Password**.
The System Password page appears.

Configuration: [System Administration](#) -> [Remote Configuration](#)

Registering your WatchGuard SOHO ensures that you will receive all LiveSecurity Alerts and software updates as soon as they are available. [Click here to register your SOHO](#) If you have already registered your SOHO, [Click here to update your information](#)

You may select a single name and password to protect your settings. If enabled, you will need to enter this name and password each time you want to change the configuration.

Enable Password

Name

Password

Retype Password

- 4 Check the **Enable Password** checkbox.
- 5 Enter the system user name in the **Name** field.
- 6 Enter the system password in the **Password** field.
- 7 Enter the system password again in the **Retype Password** field.

8 Click **Submit**.

The configuration change is saved to the SOHO and a password confirmation page appears. Click Configuration Home Page to return to the main menu.

Default factory settings

Your SOHO has the following default network and configuration settings:

External Network

External network settings use DHCP.

Trusted Network

- Trusted network IP address: 192.168.111.1.
- All computers on the trusted network automatically receive their addresses using dynamic DHCP.

Services

- All incoming services are blocked.
- All outgoing services are allowed.
- No DMZ pass-through address entered.

System Administration

- No system name or password—the onboard configuration pages are available to all on the trusted network.
- No remote logging is configured.
- Remote configuration is disabled.

The base model SOHO

The base model SOHO comes with a ten seat license—ten computers have access to the Internet through the SOHO.

Remember, while only four devices connect directly to the four (numbered 1-4) Ethernet ports, one or more of these devices can be a hub or router. Please see, “Cabling the SOHO for more than four computers” on page 8.

Upgrade certificates

Seat Licenses

The SOHO can be upgraded to provide for more seats than are available with the base model (for example, the 25 seat license certificate). These certificates must be purchased separately.

IPSec Virtual Private Networking (VPN)

The SOHO | tc comes with a VPN upgrade certificate, however you must first enable the VPN upgrade in order to configure virtual private networking. The SOHO does not come with the VPN upgrade certificate. It can be upgraded, but this certificate must be purchased separately.

WebBlocker

The SOHO can be upgraded to provide a web filtering option. This certificate must be purchased separately.

LiveSecurity Service Subscription Renewals

Subscriptions may be renewed for one or two years. You can purchase a renewal certificate from your reseller or buy it online. Log in to the LiveSecurity Service and click Subscription Renewals (even expired users can log in to renew their subscriptions) at:

<http://www.watchguard.com/support/>

Follow the instructions printed on the certificate to activate the renewal.

Troubleshooting installation and network configuration

The following information is offered to help overcome any minor difficulties that might occur when installing and setting up your SOHO.

General

What do the ON and MODE lights signify on the SOHO?

When the ON light is illuminated, the SOHO has power. When the MODE light is illuminated, the SOHO is operational.

If the ON light is *blinking* it is indicative of a couple of concerns:

- If the MODE light is off than the unit is running through it's boot process and the ON light will cease blinking when the process is complete.
- If the MODE light is illuminated then the unit is running from it's backup flash memory. You should be able to connect to the unit from a computer on of the four (numbered 1-4) Ethernet ports and reload the configuration. If the problem persists, please see "Contacting Technical support" on page viii.

If the MODE light is *blinking* it is indicative of a couple of concerns:

- The unit required a DHCP assigned IP address for the External interface (WAN port) but did not receive it.
- The External interface (WAN port) is not connected to another device, the physical connection is faulty, or the other device is not operating properly.

How do I register my SOHO?

Registering your WatchGuard SOHO ensures that you receive all LiveSecurity alerts and software updates as soon as they are available. The first year of service is free with purchase of the SOHO. To register your SOHO:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 Click **System Administration** and then click **System Password**.
- 3 Click **Click here to register your SOHO**.
- 4 Enter your information and then click **Save Profile**.

Configuration

Where are the SOHO settings stored?

The configuration parameters for the SOHO are stored in a file named `wg.cfg` in the SOHO.

How do I change to a DHCP trusted IP address?

- 1 Make sure your computer is set up to use DHCP dynamic addressing please see, “Release and renew the IP configuration” on page 20.
- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 Click **Trusted Network**.
- 3 Enable the checkbox labeled **Enable DHCP Server** and then click **Submit**.

- 4 Click **Reboot** and wait for the SOHO to finish rebooting. The MODE and ON light flash at different times during boot, which takes about a minute.

How do I change to a static trusted IP address?

Before you can use a static IP address, you must have a base Trusted IP address and subnet mask.

The following IP address ranges and subnet masks are set aside for private networks in compliance with RFC 1918. Replace the X in the network IP address with a number between 1 and 254. The subnet addresses do not need to be changed.

Network IP range	Subnet mask
10.x.x.x	255.0.0.0
172.16.x.x	255.240.0.0
192.168.x.x	255.255.0.0

To change to a static trusted IP address:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click **Trusted Network**, and disable the checkbox labeled **Enable DHCP Server**.
- 3 Enter the information in the appropriate fields. Click **Submit**.
- 4 Click **Reboot** and wait for the SOHO to finish rebooting. The MODE light on the front of the SOHO will turn off, then back on.

How do I allow any incoming service?

With the SOHO, you can allow any incoming service but doing this opens your network to the public.

CAUTION

This is a major security risk. For instructions on how to allow any incoming services, refer to "Adding the Any service" on page 42.

How do I allow incoming IP protocols?

You will need the IP address of the computer that will be receiving the incoming data and the IP protocol number that corresponds to the specific incoming IP protocol. To allow an incoming IP protocol:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click **Services** and then click **Allowed Incoming Services**.
- 3 Click **Add a Service** and then click **Add Other Service**.
- 4 In the protocol field, enter the protocol to allow.
- 5 Enter the IP address of the computer to receive incoming data for that protocol. Click **Submit**.

How do I set up and disable Web blocking?

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click **Services** and then click **Web Blocking**.
- 3 Enable the checkbox labeled **Enable Web Blocking**. Enter a password, time limit per session for your password, and enable the checkbox next to the type of sites you want blocked. To disable Web blocking, disable the checkbox labeled **Enable Web Blocking**.

How do I allow incoming services such as UDP, POP3, Telnet, and Web?

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click **Services** and then click **Allowed Incoming Services**.
- 3 Click **Add a Service** and then click the service you want to add. For UDP, you will need to select **UDP** on the **Forward** drop list and enter the range of port numbers in the port fields. For all other services, enter the IP address of the computer that needs the incoming service.
- 4 Click **Submit**.

VPN Management

Before setting up a VPN, you must have the following:

- Two properly configured and working SOHOs or one SOHO and one Firebox with the latest version of firmware. Each SOHO must have the VPN upgrade enabled.
- The static external IP address, the network address, and the subnet masks of both SOHOs. (The base trusted IP address of each SOHO must be static and unique.)
- The DNS and WINS server IP address, if used.
- The shared key (passphrase) for the tunnel.
- The same encryption method on each end of the tunnel (DES or 3DES).
- The same authentication method on each end (MD-5 or SHA-1).

How do I set up VPN between two SOHOs?

For detailed information on how to configure a VPN tunnel between two SOHO devices, download the SOHO to SOHO IPsec VPN Tunnel configuration instructions:

- 1 Using your Web browser, go to:
<http://www.watchguard.com/support>
- 2 Click **Interoperability** on the left of the page.
- 3 Click **VPN Configuration**.
- 4 Click **Configuring a SOHO to SOHO IPsec VPN Tunnel**.
- 5 Download and follow the instructions to configure your VPN tunnel.

Technical

How do I reboot my SOHO?

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click **System Information**.
- 3 Click **Features and Version Information**.
- 4 Click **Reboot** and wait for the SOHO to finish rebooting. The MODE light on the front of the SOHO will turn off, then back on.

NOTE

You can also reboot by removing the power source for ten seconds, and then restoring power.

How do I set up my SOHO for remote configuration?

This requires the add-on product, WatchGuard VPN Manager software, which is purchased separately. To purchase VPN Manager, use your Web browser to go to:

<https://www.watchguard.com/products/vpnmanager.asp>

For more information on how to remotely configure a SOHO, see the VPN Manager Guide.

How do I reset the SOHO to factory defaults?

To reset the SOHO to factory settings, disconnect the power, disconnect all cables, plug one end of an Ethernet cable into the WAN port and the other end into any of the four (numbered 1-4) Ethernet ports, reconnect the power, wait at least 90 seconds, and disconnect power. Your SOHO is now reset to factory defaults. Connect the cables in the original configuration and power up again.

How does the seat limitation on the SOHO work?

The default user license on the SOHO is 10. The first 10 computers on the network behind the SOHO to attempt to access the Internet are allowed through the SOHO. To clear the list of these first 10 computers you will need to reboot the SOHO.

How do I get to the SOHO Knowledge Base?

Using your Web browser, go to:

<http://www.watchguard.com/support>

Log in using your WatchGuard User Name and Password created when you registered. Click **Technical Support** and then click **Knowledge Base**.

I set a password on my unit, but I forgot it. Can you help?

If you forgot your password, you must reset the SOHO to its factory default. See question above on How do I reset the SOHO to factory defaults.

How do I install a SOHO using a Macintosh?

The process is essentially identical to installing on any other platform. Use the Installation chapter within this Guide. The one unique element for Macintosh users, determining your TCP/IP settings, can be found on page 3.

How do I know whether the cables are connected correctly to my SOHO?

There are twelve lights on the front of the SOHO grouped in pairs. The Link light labeled WAN tells you if your SOHO is connected to your modem. If this light is not illuminated, the SOHO is not connected to your modem. Check to make sure that both sides of the cable are connected and that your Internet connection is not down. The Link lights numbered 1 through 4 Ethernet ports for the Trusted network. They tell you if the SOHO is connected to a computer or hub. If the lights are not illuminated, the SOHO is not connected to the computer or hub. Check to make sure that both sides of the cable are connected and that the computer or hub has power.

I can connect to the configuration screen; why can't I browse the Internet?

This means that the SOHO is on, but something may be wrong with the connection from the SOHO to the Internet. Make sure the cable or DSL modem is connected correctly and has power. Also check the link light on your modem as well as the WAN link light

on the SOHO. If these are illuminated than your ISP may be temporarily down--you will need to call your ISP.

How do I register for Live Security?

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click on **LiveSecurity** in the top header and follow the instructions provided.

How can I see the MAC address of my SOHO?

A MAC (Medium Access Control) address is a unique number used to identify the actual physical hardware of an Ethernet device.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click on **System Information**.
- 3 Click on **Features and Version Information**.
- 4 You can view your MAC address from this page (it's recorded next to your External IP Address).

What is a SOHO feature key?

The feature key is an encrypted mask that tells the SOHO which features are enabled. It is stored with the configuration file of the SOHO.

I can't get a certain SOHO feature to work with a DSL modem.

Some DSL routers implement NAT firewalls. Running NAT in front of the SOHO causes problems with WebBlocker and the

performance of IPSec. When a SOHO is used in conjunction with a DSL router, the NAT feature of the DSL router should be set for bridge-only mode.

Configuring Services for a SOHO

How does information travel on the internet?

Each packet of information transported over the Internet must be packaged in a special way to ensure that it is able to travel from one computer to the next. A system called Internet Protocol (IP) takes chunks of information and wraps them up with a header identifying both where the information is going and how it should be handled enroute.

IP addresses

An IP address defines the specific computer on the Internet that should send or receive a packet. Every computer on the Internet has a unique address, including your SOHO device. When defining a service behind your firewall, you need to include the trusted network address for the machine hosting the application. On the Internet, IP addresses can be identified using either a string of numbers or a user-friendly domain name. For example, the IP

How does information travel on the internet?

address of the WatchGuard site is 209.191.160.60 while the domain name is www.watchguard.com.

Protocol

A protocol defines how a packet is bundled up and packaged for shipment across a network. The most commonly used protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). In addition, there are special protocols, such as IP, which are used less frequently.

Port number

The port number alerts the computers at both the sending and receiving end how to handle the packet.

Services

A service is the combination of protocol(s) and port numbers associated with a specific application or communication type. To facilitate configuration of your SOHO, WatchGuard lets you select pre-configured versions of several commonly used services.

WatchGuard SOHO services

The WatchGuard SOHO enables you to customize what is allowed both incoming and outgoing through your firewall. With this feature, you can narrowly define what kind of communication is permitted between computers on the Internet and computers on your trusted network.

To facilitate configuring your SOHO, WatchGuard identifies several commonly used services. A service is the combination of protocol(s) and port numbers associated with a specific application or communication type.

Allowing incoming services

By default, the security stance of the SOHO is to deny unsolicited incoming packets to computers on the trusted network protected by the SOHO firewall. You can, however, selectively open your network to certain types of Internet connectivity. For example, if you would like to set up a Web server behind the SOHO, you can add an incoming Web service.

It is important to remember that each service you add opens a small window into your trusted network and marginally reduces your security. This is the inherent trade-off between access and security.

Network address translation

All incoming connections through a SOHO automatically use a feature called dynamic network address translation (dynamic NAT). Without dynamic NAT, your trusted, private addresses would not be passed along the Internet to their destination.

Furthermore, the SOHO protects your trusted network by disguising private IP addresses. During an Internet connection, all traffic passed between computers includes their IP address information. However, due to the dynamic NAT feature, applications and servers on the Internet only see the public, external IP address of the SOHO itself and are never privy to the addresses in your trusted network address range when they exchange information with a computer behind your firewall.

Imagine that you install a computer behind the SOHO with the private IP address 192.168.111.12. If this address were broadcast to the Internet, hackers could easily direct an attack on the computer itself. Instead, the SOHO converts the address automatically to the public, external address of the SOHO. When a hacker tries to

violate the computer, they are stopped cold at the SOHO, never learning the true address of your computer.

Adding a pre-configured incoming service

Each service is defined by a combination of Internet protocols and port numbers to uniquely identify the connection type to applications and servers on the Internet. To facilitate configuring services, the WatchGuard SOHO Configuration pages include several of the most common types:

- FTP (File Transfer Protocol)
- Web (HTTP)
- Telnet
- POP3 (incoming e-mail)
- SSH

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 **Select Services.**
The Services menu appears.
- 3 **Select Allowed Incoming Services.**
The Incoming Services menu appears. In addition, a list of allowed incoming services is displayed beneath the menu identified by protocol, port number, and destination on the trusted network.
- 4 **Click Add a Service.**
The Add New Incoming Services menu appears.
- 5 **Select a pre-configured service type such as FTP, Web, or Telnet.**
A configuration page appears prompting for the location of the service on your trusted network.
- 6 **Enter the trusted network IP address of the computer hosting the service.**

7 Click **Submit**.

The configuration change is saved to the SOHO and the Show Incoming Rules page appears. The incoming service rules are identified by protocol, port, and destination on the trusted network.

Creating a custom incoming service

In addition to the pre-configured services provided by the WatchGuard SOHO Configuration interface, you can also create a custom service for a server on your trusted network. The limitations on the types of services you can add are as follows:

- Must use network address translation
- Must be a packet-filtering service (you cannot create custom proxy services)

Adding an incoming TCP or UDP service

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Select **Services**.
The Services menu appears.
- 3 Click **Allowed Incoming Services**. Click **Add a Service**.
The Add New Incoming Services menu appears.
- 4 Click **Add Other TCP or UDP Service**.
The New Port Forward configuration page appears.
- 5 Use the drop list to select a protocol type: TCP or UDP.
- 6 Enter the port number range in the port to port fields.
If configuring for a single port, enter the same port number in both fields. To determine the port number, open your Web browser to <http://help.livesecurity.com/lss/46/reference/ports4.htm>.
- 7 Enter the trusted network IP address of the computer hosting the service.
- 8 Enter a name for the service.

9 Click **Submit**.

The configuration change is saved to the SOHO, and the Show Incoming Rules page appears.

Adding an incoming service with another type of protocol

In addition to TCP and UDP, there are several other types of Internet protocols. To allow incoming service to these protocols, you must define both the protocol type and the internal destination. You cannot specify a port number. To allow an incoming service:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Select **Services**.
The Services menu appears.
- 3 Click **Allowed Incoming Services**. Click **Add a Service**.
The Add New Incoming Services menu appears.
- 4 Click **Add Other Service**.
The New Protocol Forward configuration page appears.
- 5 Enter the protocol name used to forward packets.
WatchGuard uses ICSA standards for protocol names.
- 6 Enter the trusted network IP address of the computer hosting this service.
- 7 Enter a name for the service.
- 8 Click **Submit**.
The configuration change is saved to the SOHO, and the Show Incoming Rules page appears.

Adding the Any service

In addition to specific protocols and ports, you can elect to send unidentified packets to a single server on your trusted network.

This enables you to open a hole in your firewall for services you would be unable to define using the standard service menus.

CAUTION

Unfortunately, the hole created using the Any service is indiscriminate. Any type of packet can enter through this service and be forwarded automatically to the trusted network address you provide. For security reasons, WatchGuard does not recommend enabling this feature.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 **Select Services.**
The Services menu appears.
- 3 **Click Allowed Incoming Services. Click Add a Service.**
The Add New Incoming Services menu appears.
- 4 **Click Add Any Service.**
The Any Service configuration menu appears.
- 5 Enter the trusted network IP address of the computer open to the Internet for any type of packet.
- 6 **Click Submit.**
The configuration change is saved to the SOHO, and the Show Incoming Rules page appears.

Removing an incoming service

You can remove a service no longer required by your network. You should do this any time you no longer support a particular type of incoming traffic, as the removal reduces any possible security weaknesses of the service. To remove an incoming service:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>

Blocking outgoing services

2 **Select Services.**

The Services menu appears.

3 **Click Allowed Incoming Services.**

The Incoming Services menu appears.

4 **Click Remove a Service.**

A list of existing, incoming services appears. Services are identified by protocol, port number, and destination address.

5 **Enable the checkbox next to the services you would like to remove.**

You can disable multiple services simultaneously.

6 **Click Submit.**

The selected service(s) are removed from the list. The list reappears. To return to the Configuration menu, click Configuration at the top of the page.

Blocking outgoing services

By default, the security stance of the SOHO is to allow all outgoing packets from computers on the trusted network protected by the SOHO firewall to the Internet. You can, however, selectively close your network to certain types of Internet connectivity. For example, one way to prevent users behind your firewall from transferring unsafe files from the Internet to the trusted network is to block all outgoing FTP.

It is important to remember that each service you block reduces accessibility to the files and destinations on the Internet. Again, this is representative of the inherent trade-off between access and security.

Blocking a TCP or UDP service

The two most commonly used network protocols are TCP and UDP. You can choose to block outgoing TCP or UDP traffic by port number or range.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 **Select Services.**
The Services menu appears.
- 3 **Select Blocked Outgoing Services.**
The Blocked Outgoing Services Menu appears. In addition, a list of blocked outgoing services is displayed beneath the menu identified by protocol and port number.
- 4 **Click Block TCP or UDP Service.**
The Block TCP or UDP Service menu appears.
- 5 Use the drop list to select a protocol type: TCP or UDP.
- 6 In the **From Port** field, enter the first port number to block. To block a single port, re-enter the port number in the **To Port** field. To block a range of port numbers, enter the last number in the range in the **To Port** field.
- 7 **Click Submit.**
The configuration change is saved to the SOHO, and the Blocked Service List page appears. The outgoing service is identified by protocol and port number range.

Blocking an alternative protocol

While less common, there are a number of other Internet protocols you may choose to block by name. The WatchGuard SOHO

currently only allows you to block non-TCP/UDP protocol on all ports.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 **Select Services.**
The Services menu appears.
- 3 **Click Blocked Outgoing Services.**
The Block Protocol page appears.
- 4 **Click Block IP Protocol.**
- 5 **Enter the name of the protocol.**
For example, IP.
- 6 **Click Submit.**
The configuration change is saved to the SOHO and the Blocked Service List page appears.

Removing a blocked outgoing service

At any time, you can reopen a service now required by your network. You should do this when you seek to open access to a particular type of outgoing traffic as the removal increases the accessibility for users on your trusted network to resources on the Internet. To allow an outgoing service that you had blocked:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 **Select Services.**
The Services menu appears.
- 3 **Click Blocked Outgoing Services.**
The Blocked Outgoing Services menu appears.
- 4 **Click Remove Blocked Service.**
A list of existing, outgoing blocked services appears. Services are identified by protocol and port number range.

- 5 Enable the checkbox next to the services you would like to remove from the list of blocked services.
You can disable blocking for multiple services simultaneously.
- 6 **Click Submit.**
The selected services are removed from the list. The list reappears. To return to the Configuration menu, click Configuration at the top of the page.

Configuring Virtual Private Networking

This chapter describes an optional feature of the WatchGuard SOHO: virtual private networking with IPSec.

The following WatchGuard SOHO products support IPSec tunnels:

- WatchGuard SOHO with VPN upgrade enabled
- WatchGuard SOHO|tc

Why create a virtual private network?

Virtual Private Networking (VPN) tunnels enable you to simply and securely connect computers in two locations without requiring expensive, dedicated point-to-point data connections. With VPN, you use low cost connections to the Internet to create a virtual connection between two branch offices. Unlike a simple, un-encrypted Internet connection, a VPN connection eliminates any

What you will need

significant risk of data being read or altered by outside users as it traverses the Internet.

What you will need

- 1 One WatchGuard SOHO with VPN and an IPSec-compliant device.
While you can create a SOHO to SOHO VPN, you can also create a VPN with a WatchGuard Firebox or other IPSec-compliant devices.
- 2 The following information from your Internet service provider for both devices:
 - Static IP address
 - Default gateway address
 - Primary domain name service (DNS) IP address
 - If available, a secondary DNS address
 - Domain name
- 3 Network addresses and subnet mask for networks. By default, the Trusted, network address of the SOHO is 192.168.111.0 and the subnet mask is 255.255.255.0.

NOTE

The internal networks on either end of the VPN tunnel must use different network addresses.

To create an IPSec tunnel between devices you must add information to the configuration files of each that is specific to the site, such as external and trusted IP addresses. It is imperative to keep these addresses straight. WatchGuard recommends making a table of IP addresses such as the one outlined below.

IP Address Table (example)

Item	Description	Assigned By
External IP Address	The IP address that identifies the SOHO to the Internet. Site A: 207.168.55.2 Site B: 68.130.44.15	ISP
External Subnet Mask	The overlay of bits that determines which part of the IP address identifies your network. For example, a Class C address licenses 256 addresses and has a netmask of 255.255.255.0. Site A: 255.255.255.0 Site B: 255.255.255.0	ISP
Local Network Address	A private network address used by an organization's local network for identifying itself within the network. A local network address cannot be used as an external IP address. WatchGuard recommends using an address from one of the reserved ranges: 10.0.0.0 — 255.0.0.0 172.16.0.0 — 255.240.0.0 192.168.0.0/16 — 255.255.0.0 Site A: 255.255.255.0 Site B: 255.255.255.0	You
Shared Secret	A phrase stored at both ends of the tunnel to authenticate the transmission as being from the claimed origin. The secret can be any phrase, but mixing numerical, special, alphabetical, and uppercase characters improves security. For example, "My1F@ult" is better than "myonefault" Site A: OurLittleSecret Site B: OurLittleSecret	You
Encryption Method	Encryption method determines the length in bits of the key used to encrypt and decrypt communication packets. DES is a 56-bit encryption; 3DES is 168-bit, and therefore much more secure. It is also slower. Either 3DES or DES may be selected as long as both sides use the same method. Site A: 3DES Site B: 3DES	You
Authentication	Both sides must use the same method. Site A: MD5 Site B: MD5	You

About the Feature Key

When you purchase a SOHO, the software for all upgrade options is provided with the unit regardless of whether you have actually purchased any of those options. The Feature Key which enables these software options is stored within the SOHO's configuration file. Once you have purchased an upgrade option and redeemed it, the Feature key stored on your unit is modified to enable the software upgrade.

Obtaining the VPN upgrade

If you purchased a WatchGuard SOHO and would like to purchase the VPN upgrade from a reseller or e-tailer, open your Web browser to:

<http://www.watchguard.com/sales/buyonline.asp>

Enabling the VPN upgrade

Whether you purchased a VPN upgrade separately or the SOHO I tc, which comes with the certificate enclosed, you must first enable the VPN upgrade before configuring virtual private networking. Enabling the VPN upgrade requires:

- An installed SOHO
- Internet connectivity
- A VPN upgrade certificate license

Step-by-step instructions for configuring a SOHO VPN tunnel

WatchGuard has developed a series of step-by-step instructions to facilitate configuration for a SOHO VPN tunnel to any of several other IPSec-compliant devices. To download these instructions, using your Web browser, go to:

<http://www.watchguard.com/support/interopvpn.asp>

Special considerations

Consider the following before configuring your WatchGuard SOHO VPN network:

- You can connect only two devices together: a WatchGuard SOHO and either another SOHO or another IPSec-compliant device. To set up multiple VPN tunnels, you will need to have at least one WatchGuard Firebox configured with the WatchGuard VPN Manager.
- Each device must be able to send messages to the other. If either device has a dynamically assigned Internet (IP) address (see “Network addressing” on page 12 for an explanation of dynamic IP addresses), it will not be able to find its remote counterpart.
- Both devices must be set to use the same encryption method. The two choices are DES or 3DES. When connecting two Windows NT networks, the two networks must be in the same Microsoft Windows domain or be trusted domains. This is a Microsoft Networking design implementation and is not a limitation of the SOHO device.

Frequently asked questions

Why do I need a static external address?

To create a VPN connection, one SOHO must be able to find its partner device. If the addresses were allowed to change, the SOHO could not find its remote computer.

How do I get a static external IP address?

Contact your ISP. Some systems, like many cable modem systems, use dynamically assigned addresses to simplify basic installations. Some providers may also use this feature to discourage users from creating Web servers. These providers usually offer a static IP address option.

How do I connect three or four offices together?

To connect more than two offices together, WatchGuard recommends designating one office the center of a “star” network configuration and upgrading it to a WatchGuard Firebox. You can then manage multiple tunnels to SOHOs or other IPSec compliant devices from the central Firebox.

How do I troubleshoot the connection?

If you can ping the remote SOHO and computers behind it, your VPN tunnel is up and running. Any remaining problems are probably caused by the MS Networking or the applications being used.

OK, ping is not working.

If you cannot ping the local network address of the remote SOHO, take the following steps to classify the problem:

- 1 Ping the external address of the remote SOHO.
For example, at Site A, ping 68.130.44.15 (Site B). You should get a reply. If not, verify the External Network Settings of Site B. If they are correct, verify that computers at Site B can access the internet. If you are still having trouble, contact your ISP.
- 2 Once you can ping the external address of each SOHO, try pinging the local address.
From Site A, ping 192.168.112.1. If the tunnel is up, you should get a reply from the remote SOHO. If not, re-check the Local Settings page.

Make sure that the local DHCP addresses ranges do not overlap. For example, IP addresses on either side of the tunnel must not be the same.

How do I obtain a VPN upgrade certificate?

Upgrade certificates come inside the box when you buy a WatchGuard SOHO I tc. They can also be purchased online. Using your Web browser, go to:

<http://www.watchguard.com/sales/buyonline.asp>

How do I enable a VPN Tunnel?

Full instructions for enabling a VPN tunnel can be found online. Using your Web browser, go to:

<http://www.watchguard.com/support/interopvpn.asp>

Additional SOHO Features

SOCKS for SOHO

SOCKS is a network proxy filter that works with SOCKS-aware applications such as ICQ. A typical SOCKS-dependent application requires that several sockets be opened and made available to the Internet. When a SOCKS-aware application (ICQ is SOCKS-aware) registers with the SOCKS server, SOCKS is able to manage the need of the application to have many ports open.

To use an application with SOCKS, the application must be configured with the SOCKS server information. The SOHO has limited SOCKS support included as of its version 2.0 firmware and later.

Setting up your SOCKS application for use with the SOHO requires no reconfiguration of the SOHO appliance itself. Your SOHO acts as the SOCKS proxy. You must, however, configure your application to be compliant with the SOHO implementation of SOCKS version 5.

SOHO SOCKS implementation

The SOHO SOCKS feature has the following characteristics and limitations:

- SOHO supports SOCKS version 5 only.
- It is a limited version of SOCKS and does not support authentication, nor does it support Domain Name System (DNS) resolution.

CAUTION

Configure the particular application so that it will *not* attempt to make DNS look-ups with SOCKS. However, some applications use only DNS through SOCKS and therefore will not function properly with the SOHO.

- Compatible SOCKS-aware applications that can be used through the SOHO include ICQ, IRC, and AOL Messenger.
- When you open a SOCKS application, it opens a “hole” in the SOHO firewall that is available to anyone on your trusted network. SOCKS applications therefore pose a significant security risk. To disable the port and close the security risk, see “Disabling SOCKS on the SOHO” on page 59.

Configuring your SOCKS application on the SOHO

Other than ensuring that port 1080 is open to run a SOCKS-dependent application, the rest of the configuration tasks must be done with the SOCKS-dependent application. Different applications may have variations in their settings, but you must configure the SOCKS-dependent application, using the application user interface, to certain parameters to enable the SOHO to pass SOCKS applications:

- If you can choose different services or versions of SOCKS, choose SOCKS version 5.
- Select port 1080 for the application
- For the SOCKS proxy, enter the URL or IP address of the SOHO trusted network. The default IP address is 192.168.111.0.

Disabling SOCKS on the SOHO

Once you have used a SOCKS-compliant application through the SOHO, the primary SOCKS port is available to anyone on your trusted network. You can, however, close this security gap between uses of SOCKS applications. To disable SOCKS:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Select **System Administration**.
The System Administration menu appears.
- 3 Select **Service Options**.
The Service Options menu appears.
- 4 Enable the checkbox next to the **Disable SOCKS proxy** selection.
This disables the SOHO from acting as a SOCKS proxy.
- 5 Click **Submit** to implement this configuration.

When you need to use SOCKS again, follow this procedure:

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Select **System Administration**.
The System Administration menu appears.

- 3 Select **Service Options**.
The **Service Options** menu appears.
- 4 Disable the checkbox next to the **Disable SOCKS proxy** selection.
This enables the SOHO to act as a SOCKS proxy.
- 5 Click **Submit** to register the change.
The SOHO is enabled again as a Proxy server and ready to pass SOCKS packets.

SOHO logging

The WatchGuard SOHO generates an ongoing activity log stored on the SOHO. This log stores a maximum of 150 messages. When it reaches its maximum, the oldest message is deleted.

The log messages may include time synchronizations between SOHO and the WatchGuard Key Server, discarded packets for a packet handling violation, duplicate messages, time-outs for attempting to open the WatchGuard Feature Key Server, or return error messages.

Viewing SOHO log messages

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click **System Information**.
The System page appears.
- 3 Click **Event Log**.
The Event Log page appears and the log file messages can be viewed.

Setting a remote log host

Setting a remote log host causes log messages to be transmitted to a WatchGuard log server with an account set up for your configuration. It has the advantages of saving local resources for other less memory-intensive tasks and puts the log host at the WatchGuard site where customer support can examine logs at your request to troubleshoot security problems.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 Click **System Administration**.
The System Administration menu appears.
- 3 Select **Remote Logging**.
The Secure Remote Logging page appears.
- 4 Check the box labeled **Enable Remote Logging**.
- 5 Enter the IP address of the WatchGuard log server that will be your remote secure log host.
- 6 In the **Pass Phrase** field, enter a pass phrase that will serve as a password to gain access to the log server.
- 7 In the **Retype Phrase** field, re-enter the pass phrase.
- 8 Click **Submit**.
This transmits your new user and log names to WatchGuard.

Rebooting a WatchGuard SOHO

To reboot a SOHO located on a local system, use one of the following methods:

- Using your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.

Click **System Information**, then click **Features and Version Information**. Click the **Reboot** button

- Unplug the SOHO and plug it back in

To reboot a SOHO located on a remote system, the SOHO must be configured to allow either incoming Web or FTP traffic to the trusted address of the SOHO. For information on configuring a SOHO to allow incoming traffic, see “Allowing incoming services” on page 39

You can than use one of the following methods:

- Open a special HTML page with the public, external SOHO IP address in the URL followed by `/rebootreq`. For example, `http://209.191.160.60/rebootreq`.
- Send an FTP command to the remote SOHO device. Use an FTP application to connect to the SOHO device, then enter the command: `quote rebt`

WatchGuard SOHO WebBlocker

WatchGuard SOHO WebBlocker is an optional feature of the WatchGuard SOHO and SOHO | tc that provides Web site filtering capabilities. It gives you precise control over the types of Web sites users on your trusted network are allowed to view.

How WebBlocker works

WebBlocker relies on a URL database, the CyberNOT list, a service of CyberPatrol, owned and maintained by SurfControl. The WebBlocker database contains many thousands of IP addresses and directories. These addresses are divided into categories based on content such as Drug Culture, Intolerance, or Sexual Acts.

WatchGuard updates the Webblocker server with a new database at regular intervals.

Once you have purchased and enabled WebBlocker, every time a user on your trusted network attempts to reach an Internet Web

site, the SOHO queries the WatchGuard database and determines whether or not to block the site. The SOHO considers the following conditions in determining whether or not to block the site:

Web site not in WebBlocker database

If the site is not in the WatchGuard WebBlocker database, the Web browser opens the page for viewing.

Web site in WebBlocker database

If the site is in the WatchGuard WebBlocker database, the SOHO checks whether or not you have chosen to block that type (or category) of site. When the category is blocked, the browser displays a page informing the user that the site is unavailable for viewing. If the category is not blocked, the Web browser opens the page for viewing.

WatchGuard WebBlocker database unavailable

If for any reason the WatchGuard WebBlocker database is unavailable (for example, if there is briefly a problem between your ISP and the nearest WatchGuard server), the browser displays a page informing the user that the site is unavailable for viewing.

WebBlocker Users and Groups

Groups

This feature allows you to create a group and prescribe a given web browsing profile by selecting the WebBlocker categories you want to prevent members of this group from browsing over the internet.

Users

This feature allows you to create an individual user account, with a unique username and password, and restrict their web browsing by assigning them to a given Group.

Bypassing the SOHO WebBlocker

Occasionally, you may want to allow select individuals to bypass the filtering functions of SOHO WebBlocker. For example, if you are using the SOHO at home as a telecommuter, you may want to block a category from your children while still retaining access for the adults in the household.

The SOHO WebBlocker configuration page includes a Full Access Password field. You can configure this password and give it to only those members of your trusted network who should be able to bypass WebBlocker. When a site is blocked or unavailable, the user has the option of entering the full access password. With the password entered, the browser displays the otherwise blocked site. After the password is entered, the user can browse any site on the Internet until either the Password Expiration duration passes or the individual closes the browser.

Purchasing and enabling SOHO WebBlocker

To use WatchGuard SOHO WebBlocker, you must first purchase and enable the WebBlocker upgrade certificate. You must then activate your LiveSecurity Subscription at:

<http://www.watchguard.com/support/>

After you have logged in, follow the instructions provided.

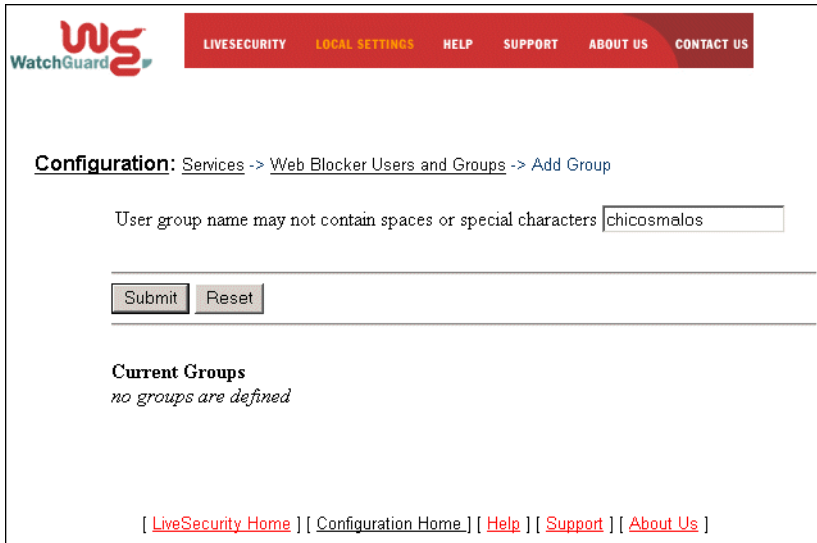
Configuring the SOHO WebBlocker

Use the WatchGuard SOHO Configuration pages to enable WebBlocker, create a full access password for bypassing WebBlocker, define an Inactivity Timeout which sets the duration that the full access password is valid, define the categories you want to block, and configure WebBlocker Groups and Users.

Add WebBlocker Groups

Follow the instructions below to add WebBlocker Groups. If you wish to use a global policy for all users, instead of creating separate group policies, ignore this section and follow the instructions to enable WebBlocker without selecting a Group.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click on **Services** and then click **WebBlocker Users and Groups**.
- 3 Select **Add Group** and enter a unique name for this group. In our example we have created the group "chicosmalos".



The screenshot shows the WatchGuard configuration interface. At the top left is the WatchGuard logo. To its right is a red navigation bar with the following links: LIVESECURITY, LOCAL SETTINGS, HELP, SUPPORT, ABOUT US, and CONTACT US. Below the navigation bar, the breadcrumb path is: **Configuration:** [Services](#) -> [Web Blocker Users and Groups](#) -> [Add Group](#). A text input field contains the name "chicosmaios". Above the field is a warning: "User group name may not contain spaces or special characters". Below the field are two buttons: "Submit" and "Reset". Underneath the buttons, the section "Current Groups" displays the message "no groups are defined". At the bottom of the page, there are links: [\[LiveSecurity Home \]](#) | [\[Configuration Home \]](#) | [\[Help \]](#) | [\[Support \]](#) | [\[About Us \]](#).

- 4 Click **Submit**.

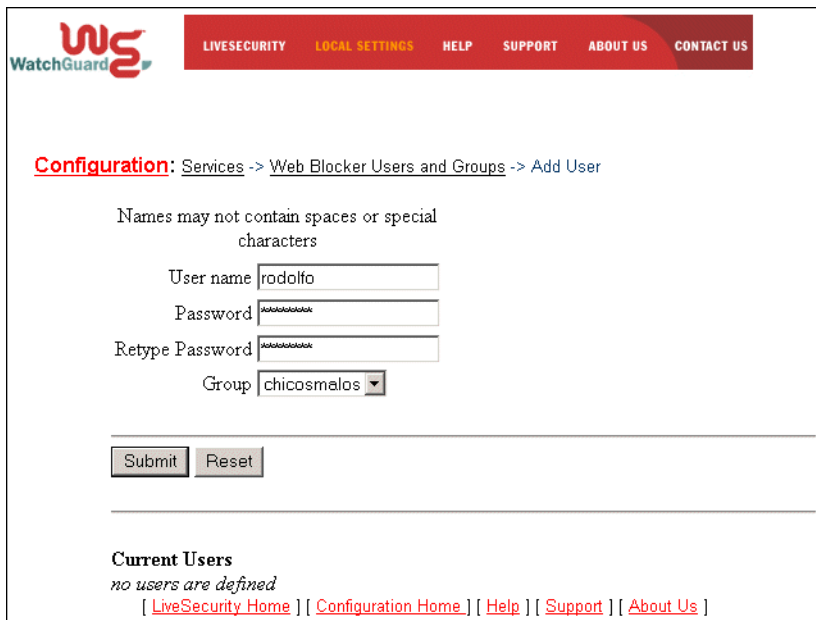
Add WebBlocker Users

Follow the instructions below to add WebBlocker Users. When creating users you must assign them to a pre-existing Group. Therefore, Groups must be created prior to adding a User.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 Click on **Services** and then click **WebBlocker Users and Groups**.
- 3 Select **Add Group**.

- 4 Enter a unique username and password. Use the drop down list to assign this User to a given Group.

In our example, we have assigned the User "rodolfo" to the Group "chicosmalos" created previously.



The screenshot shows the WatchGuard configuration interface. At the top left is the WatchGuard logo. A red navigation bar contains the following links: LIVESECURITY, LOCAL SETTINGS, HELP, SUPPORT, ABOUT US, and CONTACT US. Below the navigation bar, the breadcrumb path is: **Configuration:** Services -> Web Blocker Users and Groups -> Add User. A warning message states: "Names may not contain spaces or special characters". The form contains the following fields: "User name" with the value "rodolfo", "Password" and "Retype Password" both masked with asterisks, and a "Group" dropdown menu with "chicosmalos" selected. At the bottom of the form are "Submit" and "Reset" buttons. Below the form, the "Current Users" section shows "no users are defined" and a row of links: [[LiveSecurity Home](#)] [[Configuration Home](#)] [[Help](#)] [[Support](#)] [[About Us](#)]

Now that you have created a User and assigned them to a Group, the next step is to enable WebBlocker.

Enable WebBlocker

Follow the instructions below to enable WebBlocker, define the inactivity timeout value, require that your Web users authenticate (if you are using the Groups and Users feature option) and lastly, select the categories to be blocked for members of this Group.

- 1 Click **Configuration Home** and select **Services**.
The Services menu appears.

2 Select **WebBlocking**.

The WebBlocking configuration page appears. It provides controls for activating and controlling WebBlocker, as well as checkboxes to determine which content types can be accessed.

3 Enable the checkbox labeled **Enable WebBlocking**.

This turns on the SOHO WebBlocker.

4 Enter the full access password.

The full access password gives selected users a password that bypasses otherwise blocked sites.

5 Enter the Inactivity Timeout in minutes.

Setting the full access password inactivity timeout at, for example, 15 minutes, ensures that unattended Web browsers will be disconnected after sitting idle for 15 minutes. This ensures that only the individuals chosen to use the full access password will be able to browse otherwise blocked sites.

6 If you have defined WebBlocker Groups and Users, enable the **Require Web users to authenticate** checkbox.

7 If you have defined a WebBlocker Group, you can prescribe a given web browsing profile by selecting the WebBlocker categories you want to prevent members of this group from browsing over the internet. Once you have enabled the particular categories, select the group from the “Blocked Categories for group:” drop list.

In our example, we have selected the Group “chicosmalos” created previously.

Configuration: [Services](#) -> [Web Blocking](#)

WEB Blocker checks all outbound HTTP requests against a list of blocked sites and will deny attempts to access these sites.

Enable WebBlocker

Full Access Password

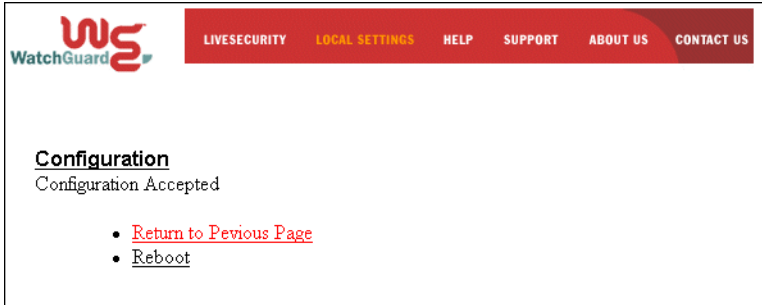
Inactivity Timeout (minutes)

Require Web users to authenticate

Blocked Categories for group

<input type="checkbox"/> Alcohol and Tobacco	<input type="checkbox"/> Violence/Profanity
<input checked="" type="checkbox"/> Illegal Gambling	<input checked="" type="checkbox"/> Search Engines
<input type="checkbox"/> Militant/Extremist	<input type="checkbox"/> Sports and Leisure
<input type="checkbox"/> Drug Culture	<input type="checkbox"/> Sex Education
<input type="checkbox"/> Satanic/Cult	<input checked="" type="checkbox"/> Sex Acts
<input type="checkbox"/> Intolerance	<input checked="" type="checkbox"/> Full Nudity
<input checked="" type="checkbox"/> Gross Depictions	<input checked="" type="checkbox"/> Partial/Artistic Nudity

- 8 Click the **Submit** button to register your changes.
- 9 Click the **Reboot** link at the Configuration Accepted page.



WebBlocker categories

WebBlocker relies on a URL database, the CyberNOT list, a service of CyberPatrol. The WebBlocker database contains many thousands of IP addresses and directories. These addresses are divided into categories based on content such as Drug Culture, Intolerance, or Sexual Acts. CyberPatrol constantly searches the Internet to update the list of blocked sites. The WebBlocker database contains the following 14 categories.

NOTE

In all of the categories sites to be blocked are selected by advocacy rather than opinion or educational material. For example, the Drugs/Drug Culture category blocks sites describing how to grow and use marijuana but does not block sites discussing the historical use of marijuana.

Alcohol/Tobacco

Pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.

Illegal Gambling

Pictures or text advocating materials or activities of a dubious nature that may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission), and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, online sports, or financial betting, including non-monetary dares.

Militant/Extremist

Pictures or text advocating extremely aggressive or combative behavior or advocacy of unlawful political measures. Topic includes groups that advocate violence as a means to achieve their goals. It also includes pages devoted to "how to" information on the making of weapons (for both lawful and unlawful reasons), ammunition, and pyrotechnics.

Drug Culture

Pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This does not include (that is, if selected these sites would not be WebBlocked under this category) currently illegal drugs legally prescribed for medicinal purposes (such as, drugs used to treat glaucoma or cancer).

Satanic/Cult

Pictures or text advocating devil worship, an affinity for evil, wickedness, or the advocacy to join a cult. A cult is defined as: A closed society that is headed by a single

individual where loyalty is demanded and leaving is punishable.

Intolerance

Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

Gross Depictions

Pictures or text describing anyone or anything that is either crudely vulgar, grossly deficient in civility or behavior, or shows scatological impropriety. Topic includes depictions of maiming, bloody figures, and indecent depiction of bodily functions.

Violence/Profanity

Pictures or text exposing extreme cruelty or profanity. Cruelty is defined as: Physical or emotional acts against any animal or person that are primarily intended to hurt or inflict pain. Topic includes obscene words, phrases, and profanity in either audio, text, or pictures.

Search Engines

Search engine sites such as AltaVista, InfoSeek, Yahoo!, and WebCrawler.

Sports and Leisure

Pictures or text describing sporting events, sports figures, or other entertainment activities.

Sex Education

Pictures or text advocating the proper use of contraceptives. Topic includes sites devoted to the explanation and description of condoms, oral

contraceptives, intrauterine devices, and other types of contraceptives. It also includes discussion sites devoted to conversations with partners about sexually transmitted diseases, pregnancy, and sexual boundaries. Not included in this category are commercial sites selling sexual paraphernalia (topics included under *Sexual Acts*).

Sexual Acts

Pictures or text exposing anyone or anything involved in explicit sexual acts and/or lewd and lascivious behavior. Topic includes masturbation, copulation, pedophilia, as well as intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian, or homosexual encounters. It also includes phone sex advertisements, dating services, adult personals, and sites devoted to selling pornographic CD-ROMs and videos.

Full Nudity

Pictures exposing any or all portions of human genitalia. Topic does *not* include sites categorized as Partial/Artistic Nudity containing partial nudity of a wholesome nature. For example, it does not include Web sites for publications such as *National Geographic* or *Smithsonian* magazine nor sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

Partial/Artistic Nudity

Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia which is handled under the Full Nudity category. Topic does not include swimsuits, including thongs.

Searching for blocked sites

To verify whether WebBlocker is blocking a site as part of a category block, visit the Search/Submit form on the Cyber Patrol Web site.

- 1 Using your Web browser, go to:
<http://www.cyberpatrol.com/cyberNOT/default.htm>
- 2 Scroll down to display the Cyber Patrol CyberNOT® Search Engine.
- 3 Type the URL of the site to check.
- 4 Click **Check if the URL is on the CyberNOT List**.
The search engine results notify you whether or not the site is on the CyberNOT list. Use this site also to suggest a new site for both the CyberNOT and CyberYES list, as well as to request a site review.

Index

A

Adding incoming services 41, 42
Allowing incoming services 39
Any service, adding 42

B

Blocked outgoing service, removing 46
blocked sites
 in WebBlocker 75
Blocking alternative protocols 45
Blocking outgoing services 44
Browser
 Internet Explorer
 disabling HTTP proxy 5
 Netscape 4.0
 disabling HTTP proxy 5
Browsers, supported 2

C

Cables, required 1
Cabling, new SOHO 6
Categories, WebBlocker 71
Changing
 names 22
 passwords 22
Checklist, pre-installation 1
Configure
 PPPoE client 17
 private network 24
 SOHO log host 60
Copyright Information ii
Custom incoming services, creating 41
Cyber Patrol, copyright information ii

D

Database
 WebBlocker 63
Default factory settings 24

Default gateway 50
Default IP address, SOHO 24
disabling HTTP proxy 5
Disabling SOCKS 58, 59
DNS service
 primary IP address 50
 secondary IP address 50
Domain name 50

E

Encryption, SOHO 53
External Network, default factory
 settings 24

F

Factory settings, default 24
Frequently asked questions 51

H

HTTP proxy
 disabling 4

I

ICQ, enable with SOCKS 57
ICQ, IRC, AOL Messenger 58
Identification Information ii
Implementing SOCKS 57
Incoming service
 adding 41, 42
 allowing 39
 creating custom 41
 removing 43
Information
 copyright ii
 identification ii
 patent ii

 registration ii
Installation
 cabling the SOHO 6
 manual 2
 pre-installation checklist 1
 TCP/IP setting 2
Introduction ix
 information & Internet 11, 38
 IP address 37
 port number 38
 protocol 38
 services 38
IP address 37
 reason for static 53
 static, obtaining 50
IP configuration, releasing and
 renewing 20

L

LED, troubleshooting 26
Link LED
 troubleshooting 26
Linux, setting TCP/IP 3
LiveSecurity
 User ID ii
Log host
 setting for SOHO 60
 setting remote 61

M

Macintosh, setting TCP/IP 3
Manual installation 2
Masquerading 39
Microsoft Windows NT, TCP/IP setting 2

N

Names, changing computer name 22
Network
 configure private 24

private network default factory settings 24
Network address 50
Network Address Translation 39

O

Outgoing services
 blocking 44
 blocking TCP 45
 blocking UDP 45

P

Part number, SOHO ii
Password
 changing 22
 saving ii
Patent Information ii
Ping 54
Port 1080, configuring for SOCKS 58
Port number, introduction 38
PPPoE, configuring client 17
Pre-configured service,
 adding 40
Pre-installation, checklist 1
Private network
 configure 24
 setting default factory settings 24
Protocol
 blocking alternative 45
Protocol, introduction 38
Proxy, disabling HTTP 4
Proxy, SOCKS 57

R

Registration Information ii
Releasing IP configuration 20
Remote Log Host, setting 61
Removing

 a blocked outgoing service 46
 an incoming service 43
Renewing IP configuration 20

S

Serial number, saving ii
Services
 adding any 42
 adding incoming 41, 42
 adding pre-configured 40
 allowing incoming 39
 blocking outgoing 44
 creating custom incoming 41
 removing 43
 removing a blocked 46
Services, introduction 38
SOCKS 57
 and ICQ 58
 and IRC 58
 configuring 58
 disabling 58, 59
 implementation 57
 security risk 58
 with SOHO version 2.0 57
SOCKS and AOL Messenger 58
SOHO
 default IP Address 58
Static IP address 50, 51
Static IP address, reason for 53
Subnet mask 50

T

TCP
 blocking outgoing 45
TCP, adding incoming 41
TCP/IP
 determining setting 2
 releasing IP configuration 20
 setting in Macintosh 3
 setting in Unix, Linux, etc. 3
 setting in Windows '95, '98 3
Troubleshooting 51

checking link LED 26
connecting more than two offices 54
pinging 54
static IP address 53

U

UDP
 adding incoming 41
 blocking outgoing 45
Unix, setting TCP/IP 3
URL database 63
Using the manual ix

V

Virtual Private Networking
 introduction 49

W

WebBlocker
 categories 71
 searching for blocked sites 75
 The Learning Company 71
Windows '95/'98/NT, disabling HTTP
 proxy 4