WatchGuard® Firebox® SOHO 6 User Guide

SOHO 6 - firmware version 6.3

Certifications and Notices

FCC Certification

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

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

CE Notice

The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU).

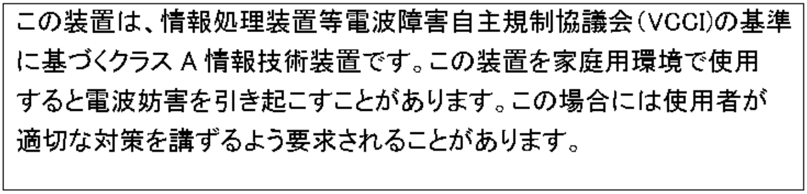
CE

Industry Canada

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

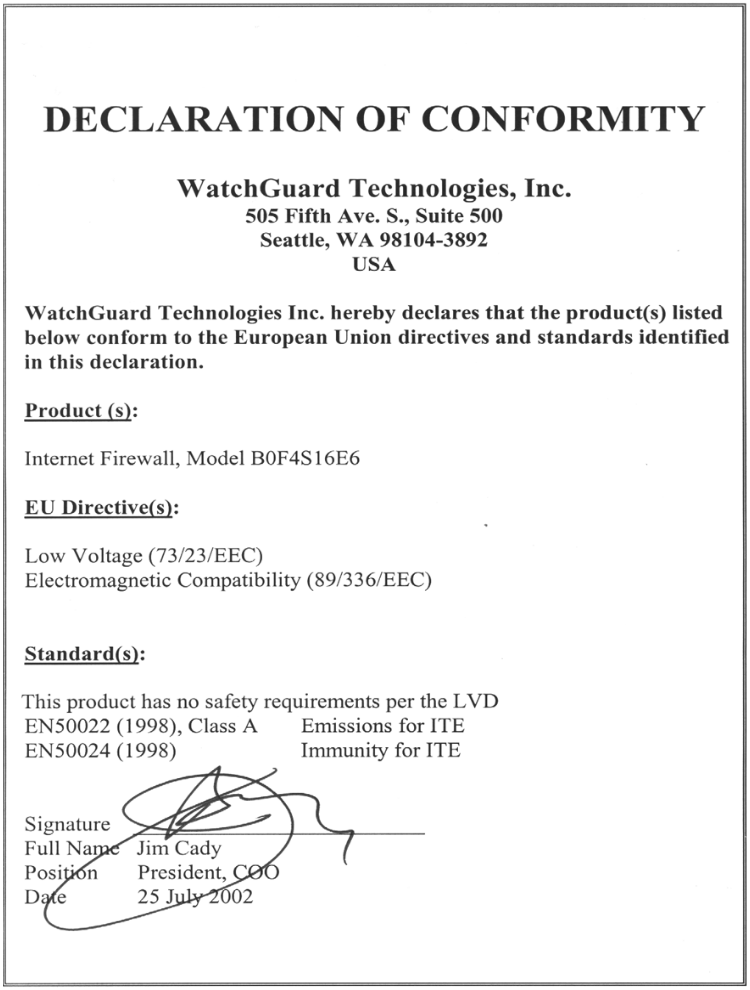
Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel broulleur du Canada.

VCCI Notice Class A ITE



この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Declaration of Conformity



DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product (s):

Internet Firewall, Model B0F4S16E6

EU Directive(s):

Low Voltage (73/23/EEC)
Electromagnetic Compatibility (89/336/EEC)

Standard(s):

This product has no safety requirements per the LVD

EN50022 (1998), Class A	Emissions for ITE
EN50024 (1998)	Immunity for ITE

Signature
Full Name Jim Cady
Position President, COO
Date 25 July 2002

WATCHGUARD SOHO SOFTWARE END-USER LICENSE AGREEMENT

WATCHGUARD SOHO SOFTWARE
END-USER LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE
This WatchGuard SOHO Software 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 SOHO software product, which includes computer software (whether installed separately on a computer workstation or on the WatchGuard hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity service (or its equivalent) (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 licensors. 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 use the SOFTWARE PRODUCT solely for the purpose of operating the SOHO hardware product in accordance with the SOHO or user documentation.

If you are accessing the SOFTWARE PRODUCT via a Web based installer program, you are granted the following additional rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any computer with an associated connection to the SOHO hardware product in accordance with the SOHO user documentation;

(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 that each computer on which you install the SOFTWARE PRODUCT has an associated connection to the same SOHO hardware product ; 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 us 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 they will provide you with a new version of the SOFTWARE PRODUCT or a full refund at their 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 AND 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 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 (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 WILL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD 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 HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS WILL 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 subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Incorporated, 505 5th Ave. 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 SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS EULA ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS EULA; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS EULA AND PERFORM ITS OBLIGATIONS UNDER THIS EULA AND; (C) THIS EULA AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS EULA DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY.
No change or modification of this EULA will be valid unless it is in writing, and is signed by WATCHGUARD.

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or

Copyright, Trademark, and Patent Information

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

Software Version Number: 6.3
Part No 0814-000

Abbreviations Used in this Guide

3DES	Triple Data Encryption Standard
DES	Data Encryption Standard
DNS	Domain Name Service
DHCP	Dynamic Host Control Protocol
DSL	Digital Subscriber Line
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
MAC	Media Access Control
MUVPN	Mobile User Virtual Private Network
NAT	Network Address Translation
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WSEP	WatchGuard Security Event Processor

Contents

CHAPTER 1

Introduction

The purpose of this guide is to help users of the WatchGuard® Firebox® SOHO 6 and Firebox® SOHO 6tc set up and configure these appliances for secure access to the Internet.

In this guide, the name SOHO 6 refers to both the SOHO 6 as well as the SOHO 6tc. The only difference between these two appliances is the VPN feature. VPN is available as an upgrade option for the SOHO 6. The SOHO 6tc includes the VPN upgrade option.

The SOHO 6 provides security when your computer is connected to the Internet with a high-speed cable modem, DSL modem, leased line, or ISDN.

The newest installation and user information is available from the WatchGuard Web site:

http://support.watchguard.com/sohoresources/

The following conventions are used in this guide:

- Within procedures, visual elements of the user interface, such as buttons, menu items, dialog boxes, fields, and tabs, appear in boldface.
- Menu items separated by arrows (⇒) are selected in sequence from subsequent menus. For example, **File ⇒Open ⇒Configuration File** means to select **Open** from the **File** menu, and then **Configuration File** from the **Open** menu.
- URLs and email addresses appear in sans serif font; for example, wg-users@watchguard.com
- Code, messages, and file names appear in monospace font; for example: `.wgl` and `.idx` files
- In command syntax, variables appear in italics; for example: fbidsmate *import_passphrase*
- Optional command parameters appear in square brackets.

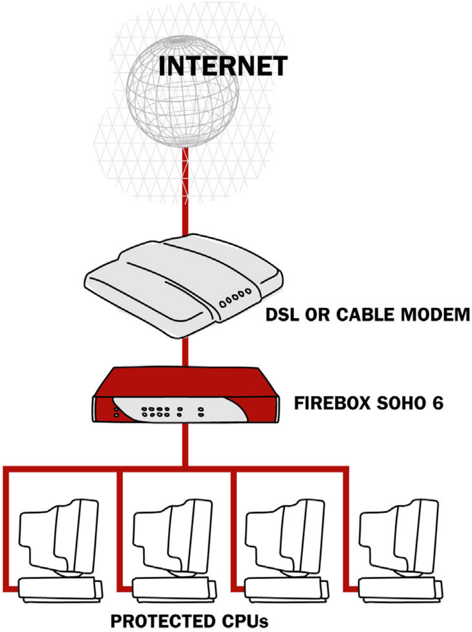
Package Contents

Make sure that the package contains all of these items:

- *SOHO 6 QuickStart Guide*
- User Guide
- LiveSecurity Service® activation card
- Hardware Warranty Card
- AC adapter (12 V, 1.0-1.2 A)
- Straight-through Ethernet cable
- SOHO 6 security appliance

How a Firewall Works

The Internet connects your network to resources. Some examples of resources are the World Wide Web, email, and video/audio conferencing. A connection to the Internet can be dangerous to the privacy and the security of your network. A firewall divides your internal network from the Internet to reduce this danger. The appliances on the trusted side of your SOHO 6 firewall are protected. The illustration below shows how the SOHO 6 physically divides your trusted network from the Internet.



The SOHO 6 controls all traffic between the external network (the Internet) and the trusted network (your computers). All suspicious traffic is stopped. The rules and policies that identify the suspicious traffic are shown in “Configuring Incoming and Outgoing Services” on page 62.

How Information Travels on the Internet

The data that is sent through the Internet is divided into packets. To make sure that the packets are received at the destination, information is added to the packets. The protocols for sending and receiving these packets are called TCP and IP. TCP disassembles and reassembles the data; for example, data that may consist of an email message or a program file. IP adds information to the packets that includes the destination and the handling requirements.

IP addresses

An IP address identifies a computer on the Internet that sends and receives packets. Each computer on the Internet has an address. The SOHO 6 is also a computer and has an IP address. When you configure a service behind a firewall, you must include the trusted network IP address for the computer that supplies the service.

A URL (Uniform Resource Locator) identifies each IP address on the Internet. An example of a URL is:

http://www.watchguard.com/.

Protocols

A protocol defines how a packet is assembled and transmitted through a network. The most frequently used protocols are TCP and UDP (User Datagram Protocol). There are other IP protocols that are less frequently used.

Port numbers

During the communication between computers, port numbers identify which programs or applications are connected.

How the SOHO 6 Processes Information

Services

A service is the group of protocols and port numbers for a specified program or type of application. The standard configuration of the SOHO 6 contains the correct settings for many standard services.

Network Address Translation (NAT)

All connections from the trusted network to the external network through a SOHO 6 use dynamic NAT. Dynamic NAT prevents the private IP addresses from your trusted network from being sent through the Internet.

The SOHO 6 replaces the private IP addresses with the public IP address to protect the trusted network. Each packet sent through the Internet contains IP address information. Packets sent through the SOHO 6 with dynamic NAT include only the public IP address of the SOHO 6 and not the private IP address of the computer in the trusted network. Because only the IP address of the SOHO 6 is sent to the external network, unauthorized access by the computers in the public network to the computers in the trusted network is prevented.

SOHO 6 Hardware Description

The hardware of the SOHO 6 uses newer technology than earlier SOHO models.

Faster Processor

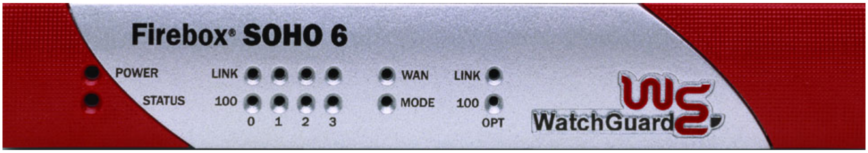
The SOHO 6 has a new network processor that runs at a speed of 150 MHz. Ethernet and encryption technology are included.

Ethernet ports

The SOHO 6 has six 10/100 Base TX ports. The Ethernet ports have the labels 0 through 3, OPT and WAN.

SOHO 6 front and rear views

There are 14 indicator lights on the front panel of the SOHO 6. The illustration below shows the front view.



PWR

PWR is lit while the SOHO 6 is connected to a power supply.

Status

Status is lit while a management connection is in use.

Link

Link indicators are lit while there is an active physical connection to the related Ethernet port. A link indicator flashes when data flows through the Ethernet port.

100

The 100 indicator is lit when a port is in use at 100 Mb. The 100 indicator is *not* lit when a port is in use at 10 Mb.

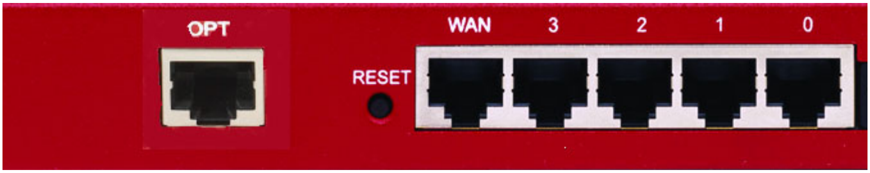
WAN

WAN is lit while there is an active physical connection to the WAN port. The indicator flashes when data flows through the port.

Mode

Mode is lit while there is a connection to the Internet.

There are six Ethernet ports, a reset button, and a power input on the rear of the SOHO 6. The picture below shows the rear view.



OPT port

The OPT port is for the optional network interface. This interface is activated when you purchase the Dual ISP Port upgrade or the VPNforce™ Port upgrade. See “Configuring the OPT Port Upgrades” on page 43 for more information about the Dual ISP Port upgrade and the VPNforce Port upgrade.

Note

The OPT port is only for the Dual ISP Port upgrade or VPNforce Port upgrade. You cannot use the OPT port as an Ethernet port on the trusted network.

RESET button

Push the reset button to reset the SOHO 6 to the factory default configuration. See “Resetting the SOHO 6 to the factory default settings” on page 26 for more information about this procedure.

WAN port

The WAN port is for the external network interface.

Four numbered ports (0-3)

These Ethernet ports are for the trusted network interface.

Power input

Connect the power input to a power supply using the 12-volt AC adapter supplied with the SOHO 6.

Hardware operating specifications

Before installing your SOHO 6, you should also be aware of its operating parameters:

Operating temperature	0 to 40 degrees C
Storage termperature	-10 to 70 degrees C
Operating humidity	10% to 85%
Storage humidity	5% to 90%

CHAPTER 2 Installation

The SOHO 6 protects computers that are connected to it by Ethernet cable. Follow the procedures in this chapter to install the SOHO 6 in your network.

To install the SOHO 6, you must complete the following steps:

- Identify and record your TCP/IP settings.
- Disable the HTTP proxy setting of your Web browser.
- Enable your computer for DHCP.
- Make a physical connection between the SOHO 6 and your network.

See the SOHO 6 *QuickStart Guide* included with the SOHO 6 for a summary of this information.

Before you Begin

Before you install the SOHO 6, you must have the following:

- A computer with a 10/100BaseT Ethernet I/O card installed and a Web browser, such as Netscape or Internet Explorer.
- A functional Internet connection—this connection must be a cable or DSL modem with a 10/100BaseT port, an ISDN router, or a direct LAN connection. If the Internet connection is not functional, call your Internet Service Provider (ISP).
- Two straight-through Ethernet network cables with RJ45 connectors. Crossover cables, which are often red or orange in color, are not satisfactory. The SOHO 6 package includes one cable—a second cable may have been supplied with your modem; if not, you will need to purchase a second cable. Make sure that the cables are of sufficient length to connect the modem or router to the SOHO 6 and the SOHO 6 to your computer.
- The method of network address assignment used by your ISP. The possible methods are static addressing, DHCP, or PPPoE. Call your ISP to determine the method used, if necessary.
- The SOHO 6 serial number—found on the bottom of the appliance.

Examining and recording the current TCP/IP settings

Examine the current TCP/IP settings of your computer, and record the settings in the table “TCP/IP Settings” on page 14. Follow the instructions for the operating system that is installed on your computer.

Microsoft Windows 2000 and Windows XP

1 Select **Start** ⇒**Programs** ⇒**Accessories** ⇒**Command Prompt**.

2 At the prompt, type `ipconfig /all` and then press **Enter**.

3 Record the TCP/IP settings in the table provided.

4 Click **Cancel**.

Microsoft Windows NT

1 Select **Start** ⇒**Programs** ⇒**Command Prompt**.

2 At the prompt, type `ipconfig /all` and then press **Enter**.

3 Record the TCP/IP settings in the table provided.

4 Click **Cancel**.

Microsoft Windows 95, 98, or ME

1 Select **Start** ⇒**Run**.

2 Type: `winipcfg`

3 Click **OK**.

4 Select the **Ethernet Adapter**.

5 Record the TCP/IP settings in the table provided.

6 Click **Cancel**.

Macintosh

1 Select the **Apple** menu ⇒**Control Panels** ⇒**TCP/IP**.

2 Record the TCP/IP settings in the table provided.

3 Close the window.

Other operating systems (Unix, Linux)

1 Consult your operating system guide to locate the TCP/IP settings.

2 Record the TCP/IP settings in the table provided.

3 Exit the TCP/IP configuration screen.

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

NOTE

If you must connect more than one computer to the trusted network behind the SOHO 6, determine the TCP/IP settings for each computer.

Disabling the HTTP proxy setting of your Web browser

To configure a SOHO 6, you must access the configuration pages in the SOHO 6 with your browser. If the HTTP proxy setting in your browser is enabled, you cannot open these pages to complete the configuration procedure.

If the HTTP proxy setting is enabled, the browser only sees Web pages found on the Internet, and not pages in other locations. If the HTTP proxy setting is disabled, you can open the configuration pages in the SOHO 6 and Web pages on the Internet.

The following instructions show how to disable the HTTP proxy setting in three browser applications. If a different browser is used, use the help menus of the browser program to find the necessary information.

Netscape 4.7

1 Open Netscape.

2 Select **Edit** ⇒**Preferences**.
The Preferences window appears.

3 A list of options is shown at the left side of the window. Click the **+** symbol to the left of the **Advanced** option to expand the list.

4 Click **Proxies**.

5 Make sure the **Direct Connection to the Internet** option is selected.

6 Click **OK**.

Netscape 6.x

1 Open Netscape.

2 Select **Edit** ⇒**Preferences**.
The Preferences window appears.

3 A list of options is shown at the left side of the window. Click the arrow symbol to the left of the **Advanced** heading to expand the list.

4 Click **Proxies**.

5 Make sure the **Direct Connection to the Internet** option is selected.

6 Click **OK**.

Internet Explorer 5.0, 5.5, and 6.0

1 Open Internet Explorer.

2 Select **Tools ⇒Internet Options**.
The Internet Options window appears.

3 Click the **Advanced** tab.

4 Scroll down the page to **HTTP 1.1 Settings**.

5 Clear all of the checkboxes.

6 Click **OK**.

Enabling your computer for DHCP

To open the configuration pages for the SOHO 6, configure your computer to receive its IP address through DHCP. See "Network addressing" on page 31 for more information about network addressing and DHCP.

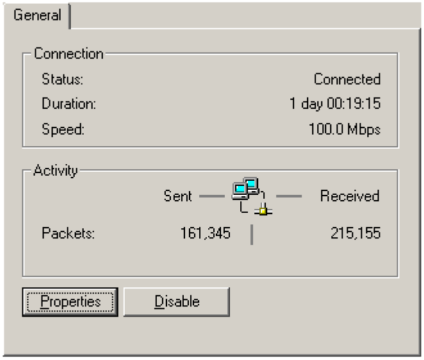
NOTE

These configuration instructions are for the Windows 2000 operating system.

1 Select **Start ⇒Settings ⇒Control Panel**.
The Control Panel window appears.

2 Double-click the **Network & Dial-up Connections** icon.

3 Double-click the connection you use to connect to the Internet.
The network connection dialog box appears.



Connection

Status: Connected

Duration: 1 day 00:19:15

Speed: 100.0 Mbps

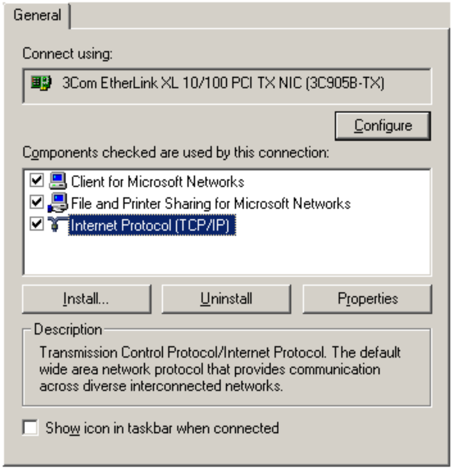
Activity

Sent — Received

Packets: 161,345 215,155

4 Click **Properties**.

The network connection properties dialog box appears.



Connect using:

3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)

Components checked are used by this connection:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

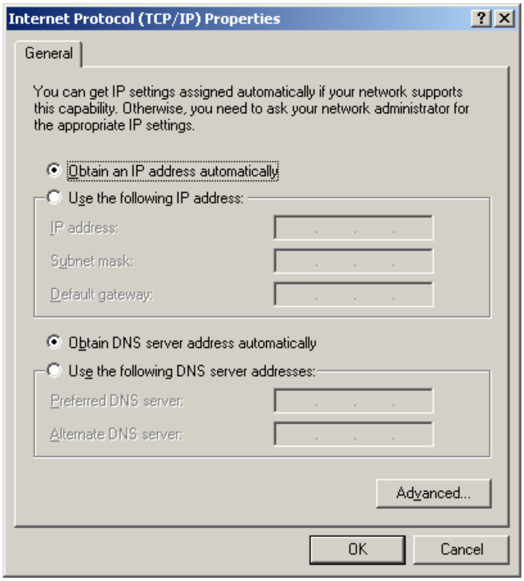
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in taskbar when connected

5 Double-click the **Internet Protocol (TCP/IP)** component.

The Internet Protocol (TCP/IP) Properties dialog box appears.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

6 Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** checkboxes.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.

8 Click **OK** again to close the network connection Properties dialog box. Click **Close** to close the network connection dialog box. Close the Control Panel window.

Physically Connecting to the SOHO 6

The SOHO 6 protects one computer or a multi-computer network. The SOHO 6 also functions as a hub to connect other appliances.

Cabling the SOHO 6 for one to four appliances

A maximum of four computers, printers, scanners, or other network peripherals can connect directly to the SOHO 6. These connections use the four numbered Ethernet ports (labeled 0-3). To connect a maximum of four appliances, use the SOHO 6 as a network hub.

1 Shut down your computer.

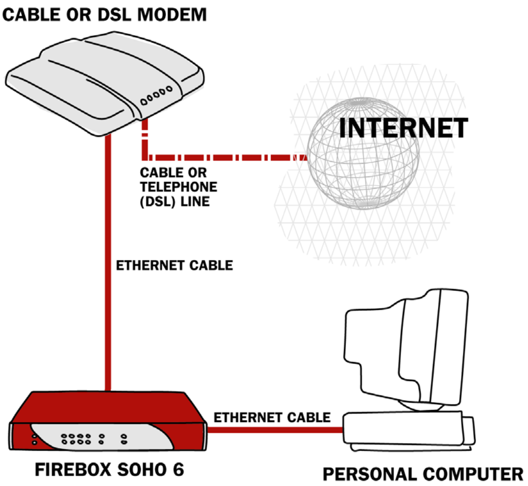
2 If you connect to the Internet through a DSL modem or cable modem, disconnect the power supply to this device.

3 Disconnect the Ethernet cable that connects your DSL modem, cable modem, or other Internet connection to your computer. Connect this cable to the WAN port on the SOHO 6.

   The SOHO 6 is connected directly to the modem or other Internet connection.

4 Connect one end of the straight-through Ethernet cable supplied with your SOHO 6 to one of the four numbered Ethernet ports (labeled 0-3) on the SOHO 6. Connect the other end to the Ethernet port of your computer.

   The SOHO 6 is connected to the Internet and your computer.



5 If you connect to the Internet through a DSL modem or cable modem, reconnect the power supply to this device. The indicator lights flash and then stop. The modem is ready for use.

6 Attach the AC adapter to the SOHO 6. Connect the AC adapter to a power source.

7 Restart the computer.

See “Factory Default Settings” on page 25 for the factory default configuration options. See “External Network Configuration” on page 31 and “Configuring the Trusted Network” on page 36 for special configurations.

Cabling the SOHO 6 for more than four appliances

Although the SOHO 6 has only four numbered Ethernet ports (labeled 0-3), you can connect more than four appliances. Use one or more network hubs to make more connections.

The base model SOHO 6 includes a ten-seat license. This license allows a maximum of ten appliances on the trusted network to connect to the Internet at the same time. There can be more than ten appliances on the trusted network, but the SOHO 6 will only allow ten Internet connections. A seat is in use when an appliance connects to the Internet and is free when the connection is broken. License upgrades are available from the WatchGuard Web site:

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

To connect more than four appliances to the SOHO 6, these items are necessary:

- An Ethernet hub
- A straight-through Ethernet cable, with RJ-45 connectors, for each computer
- A straight-through Ethernet cable to connect each hub to the SOHO 6

To connect more than four appliances to the SOHO 6, follow these steps:

1 Shut down your computer. If you connect to the Internet through a DSL modem or cable modem, disconnect the power supply from this device.

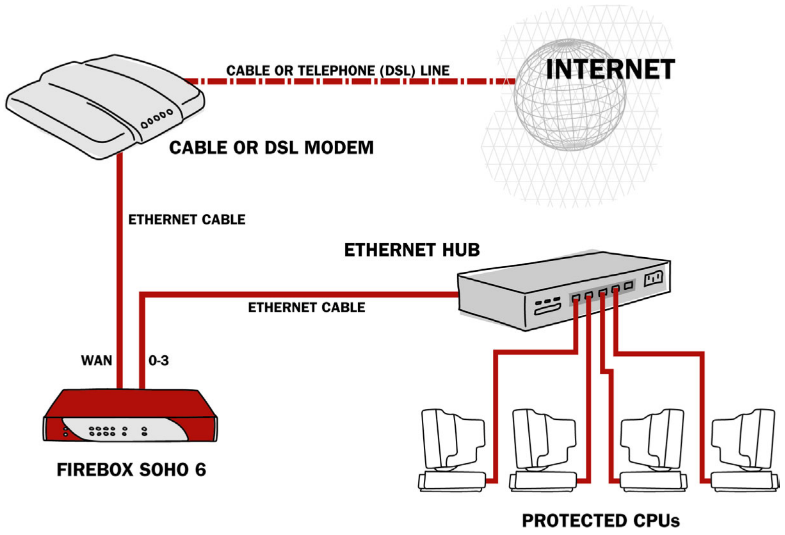
2 Disconnect the Ethernet cable that runs from your DSL modem, cable modem, or other Internet connection to your computer. Connect the Ethernet cable to the WAN port on the SOHO 6.

 The SOHO 6 is connected directly to the modem or other Internet connection.

3 Connect one end of the straight-through Ethernet cable supplied with your SOHO 6 to one of the four numbered Ethernet ports (labeled 0-3) on the SOHO 6. Connect the other end to the uplink port of the Ethernet hub.

 The SOHO 6 is connected to the Internet and your Ethernet hub.

4 Connect an Ethernet cable between each of the computers and an uplink port on the Ethernet hub.



5 If you connect to the Internet through a DSL modem or cable modem, reconnect the power supply to this device. The indicator lights flash and then stop. The modem is ready for use.

6 Attach the AC adapter to the SOHO 6. Connect the AC adapter to a power supply.

7 Restart your computer.

See “Factory Default Settings” on page 25 for the factory default configuration options. See “External Network Configuration” on page 31 and “Configuring the Trusted Network” on page 36 for special configurations.

CHAPTER 3

SOHO 6 Basics

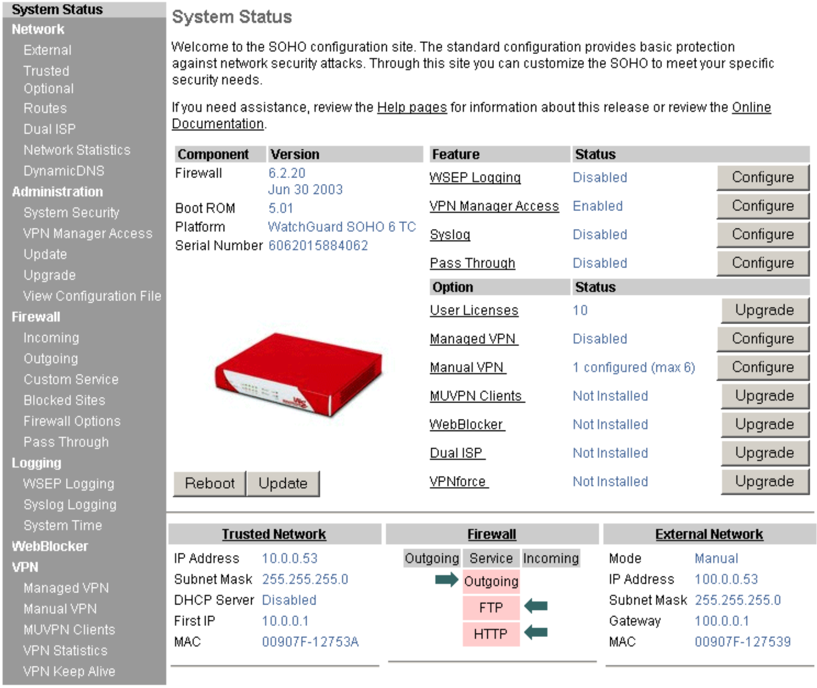
The configuration of the SOHO 6 is made through Web pages contained in the software of the SOHO 6. You can connect to these configuration pages with your Web browser.

SOHO 6 System Status Page

Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.

The default IP address is: `http://192.168.111.1`

The System Status page appears.



System Status

Welcome to the SOHO configuration site. The standard configuration provides basic protection against network security attacks. Through this site you can customize the SOHO to meet your specific security needs.

If you need assistance, review the Help pages for information about this release or review the Online Documentation.

Component	Version
Firewall	6.2.20 Jun 30 2003
Boot ROM	5.01
Platform	WatchGuard SOHO 6 TC
Serial Number	6062015884062

Feature	Status	
WSEP Logging	Disabled	Configure
VPN Manager Access	Enabled	Configure
Syslog	Disabled	Configure
Pass Through	Disabled	Configure
Option	**Status**	
User Licenses	10	Upgrade
Managed VPN	Disabled	Configure
Manual VPN	1 configured (max 6)	Configure
MUVPN Clients	Not Installed	Upgrade
WebBlocker	Not Installed	Upgrade
Dual ISP	Not Installed	Upgrade
VPNforce	Not Installed	Upgrade

Trusted Network	
IP Address	10.0.0.53
Subnet Mask	255.255.255.0
DHCP Server	Disabled
First IP	10.0.0.1
MAC	00907F-12753A

Firewall		
Outgoing	Service	Incoming
→	Outgoing	
	FTP	←
	HTTP	←

External Network	
Mode	Manual
IP Address	100.0.0.53
Subnet Mask	255.255.255.0
Gateway	100.0.0.1
MAC	00907F-127539

The System Status page is the main configuration page of the SOHO 6. A display of information about the SOHO 6 configuration is shown. This information includes the following:

- The firmware version
- The serial number of the appliance
- The status of the following SOHO 6 features:
  - WSEP Logging
  - VPN Manager Access
  - Syslog
  - Pass Through

- The status of the upgrade options
- Configuration information for the trusted network and the external network
- Configuration information for firewall settings (incoming services and outgoing services)
- A reboot button to restart the SOHO 6

NOTE

If the external network is configured to use the PPPoE protocol, the System Status page displays a connect button or a disconnect button. Use these buttons to start or terminate the PPPoE connection.

Factory Default Settings

The default network settings and configuration settings for the SOHO 6 are as follows:

External network

The external network settings use DHCP.

Trusted network

The default IP address for the trusted network is 192.168.111.0.

The IP addresses for the computers on the trusted network are assigned through DHCP.

Firewall settings

All incoming services are blocked.

An outgoing service allows all outbound traffic.

All of the firewall options are disabled.

The DMZ pass-through is disabled.

System Security

The System Security is disabled. The system administrator name and system administrator passphrase are not set. All computers on the trusted network can access the configuration pages.

SOHO 6 Remote Management is disabled.

VPN Manager Access is disabled.

The remote logging is not configured.

WebBlocker

The WebBlocker is disabled and the settings are not configured.

Upgrade Options

The upgrade options are disabled until the license keys are entered into the configuration page.

Resetting the SOHO 6 to the factory default settings

Reset the SOHO 6 to the factory default settings if it is not possible to correct a configuration problem. A reset to the factory default settings is required if the system security passphrase is unknown or the firmware of the SOHO 6 is damaged by a power interruption. Follow these steps to reset the SOHO 6 to the factory default settings:

1 Disconnect the power supply.

2 Press and hold the reset button.

3 Connect the power supply.

4 Continue holding the button until the red LED on the front of the SOHO 6 goes on and then off.

5 Disconnect the power supply.

6 Connect the power supply.
The PWR indicator is on and the reset is complete.

The base model SOHO 6

The base model SOHO 6 includes a ten-seat license. This license allows a maximum of ten computers on the trusted network to connect to the Internet at the same time. There can be more than ten computers on the trusted network, but the SOHO 6 will only allow ten Internet connections. See "Cabling the SOHO 6 for more than four appliances" on page 20 for additional information.

Registering Your SOHO 6 and Activating the LiveSecurity Service

After the SOHO 6 is installed and configured, register the SOHO 6 and activate your LiveSecurity Service subscription. LiveSecurity Service provides threat alert notifications, security advice, free virus protection, software updates, technical support by Web or telephone, and access to online help resources and the WatchGuard user forum. A subscription to the LiveSecurity Service is required to get the license keys for the upgrades that you purchase.

You must have the serial number of your SOHO 6 to register. The SOHO 6 serial number is located on the bottom of the appliance. Record the serial number in the table below:

Serial Number:	

Register your SOHO 6 with the LiveSecurity Service at the WatchGuard Web site:

http://www.watchguard.com/activate

NOTE

To activate the LiveSecurity Service, your browser must have JavaScript enabled.

If you have a user profile on the WatchGuard Web site, enter your user name and password. If you do not have a user profile on the WatchGuard Web site, create a new account. Select your product and follow the instructions for product activation.

Record your LiveSecurity Service user profile information in the table below:

User name:	
Password:	

Keep this information confidential.

Rebootting the SOHO 6

To reboot a SOHO 6 located on the local network, use one of these methods:

NOTE

The SOHO 6 requires 30 seconds to reboot. The Mode indicator on the front of the SOHO 6 will go off and then come on.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 Click **Reboot**.

OR

1 Disconnect and reconnect the power supply.

To reboot a SOHO 6 located on a remote system, use one of these methods:

NOTE

The remote SOHO 6 must be configured to allow incoming HTTP (Web) or FTP traffic from the Internet. See "Configuring Incoming and Outgoing Services" on page 62 for information about how to configure a SOHO 6 to receive incoming traffic.

1 Type the external network IP address of the remote SOHO 6 in your browser window to connect to the System Status page of the remote SOHO 6.

2 Click **Reboot**.

OR

1 Send an FTP command to the remote SOHO 6. Use an FTP program to connect to the remote SOHO 6, and enter the command:

```
quote rebt
```

CHAPTER 4

Configure the Network Interfaces

External Network Configuration

When you configure the external network, you select the method of communication between the SOHO 6 and the ISP. Make this selection based on the method of network address distribution in use by your ISP. The possible methods are static addressing, DHCP, or PPPoE.

Network addressing

To connect to a TCP/IP network, each computer must have an IP address. The assignment of IP addresses is dynamic or static.

- If the assignment is dynamic, the ISP assigns a different IP address to a computer each time the computer connects to the network. When the computer disconnects, the IP address is made available to a different computer.

- If the assignment is static, all computers on the network have a permanently assigned IP address. There are no computers that have the same IP address.

Most ISPs make dynamic IP address assignments through DHCP (Dynamic Host Configuration Protocol). When a computer connects to the network, a DHCP server at the ISP assigns that computer an IP address. The manual assignment of IP addresses is not necessary with this system.

Some ISPs assign the IP addresses through PPPoE (Point-to-Point Protocol over Ethernet). PPPoE emulates a standard dial-up connection to provide some of the features of Ethernet and PPP. This system allows the ISP to use the billing, authentication, and security systems designed for dial-up, DSL modem, and cable modem service. When the SOHO 6 is configured to use PPPoE, a button on the System Status page controls the connection to the external network.

Your ISP can tell you how their system assigns the IP addresses.

Configuring the SOHO 6 external network for dynamic addressing

The default configuration sets the SOHO 6 to get the external address information through DHCP. If your ISP supports this method, the SOHO 6 gets IP address information from the ISP when the SOHO 6 reboots and connects to the Internet. The SOHO 6 does not require any additional configuration.

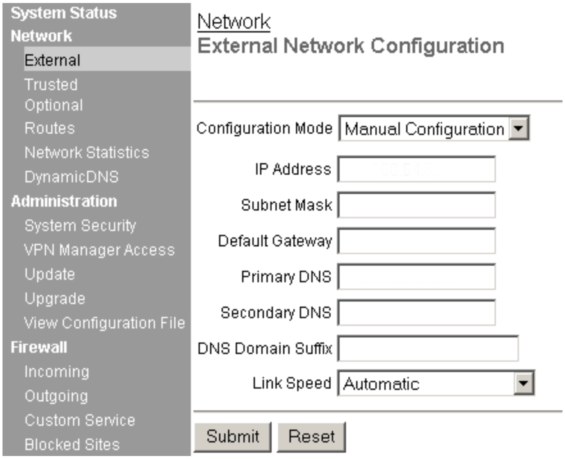
Configuring the SOHO 6 external network for static addressing

If your ISP assigns static IP addresses, you must move the IP address data from your computer to the SOHO 6. This configuration causes the ISP to communicate with the SOHO 6 and not your computer.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network** ⇒**External**.
The External Network Configuration page opens.

3 From the **Configuration Mode** drop-down list, select **Manual Configuration**.
The page refreshes.



Configuration Mode: Manual Configuration

Link Speed: Automatic

4 Type the TCP/IP settings you recorded from your computer during the installation process. Refer to the table, “TCP/IP Settings” on page 14.

5 Click **Submit**.
The configuration change is saved to the SOHO 6.

Configuring the SOHO 6 external network for PPPoE

If your ISP assigns IP addresses through PPPoE, your PPPoE login name and password are required to configure the SOHO 6.

To configure the SOHO 6 for PPPoE:

1 Open your Web browser and click **Stop**.

Because the Internet connection is not configured, the browser cannot load your home page from the Internet. The browser can open the configuration pages in the SOHO 6.

2 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.

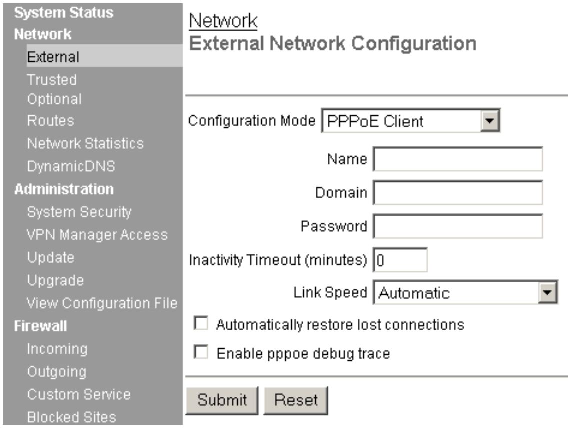
The default IP address is: http://192.168.111.1

3 From the navigation bar at left, select **Network** ⇒**External**.

The External Network Configuration page opens.

4 From the **Configuration Mode** drop-down list, select **PPPoE Client**.

The page refreshes.



External Network Configuration

Configuration Mode: PPPoE Client

Name:

Domain:

Password:

Inactivity Timeout (minutes): 0

Link Speed: Automatic

□ Automatically restore lost connections

□ Enable pppoe debug trace

5 Type the PPPoE login name and domain as well as the PPPoE password supplied by your ISP in the applicable fields.

6 Type the time delay before inactive TCP connections are disconnected.

7 Select the **Automatically restore lost connections** checkbox.

This option keeps a constant flow of traffic between the SOHO 6 and the PPPoE server. This option allows the SOHO 6 to keep the PPPoE connection open during a period of frequent packet loss. If the flow of traffic stops, the SOHO 6 reboots. A reboot frequently restores the connection. The ISP sees this constant flow of traffic as a continuous connection. The regulations and billing policy of the ISP determine if you can use this option. Watchguard Technical Support uses this feature as a solution to some problems.

8 Select the **Enable PPPoE debug trace** checkbox to activate PPPoE debug trace.

9 Click **Submit**.

The configuration change is saved to the SOHO 6.

Setting the SOHO 6 external network link speed

The SOHO 6 automatically uses the highest possible link speed (100Mbps full-duplex) for the external network by default. If the highest speed is unavailable, the SOHO 6 tries slower speeds until it establishes a connection. However, you can manually set the connection speed of the external network. Before you set the connection speed, you need to know whether your connection is full-duplex or half-duplex. Full-duplex connections can send and receive data at the same time, while half-duplex connections can only transmit and receive data sequentially.

NOTE

Make sure you check with your ISP to verify your link speed and whether your connection is half- or full-duplex. Setting the link speed incorrectly can cause connection problems.

To set the external network link speed:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network ⇒External**.
The External Network Configuration page opens.

3 From the **Link Speed** drop-down list, select the link speed you want.

4 Click **Submit**.

Configuring the Trusted Network

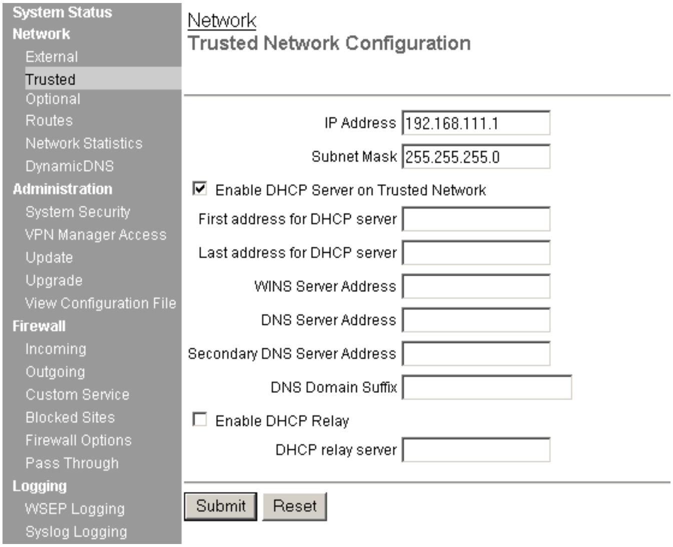
The DHCP Server option sets the SOHO 6 to assign IP addresses to the computers on the trusted network. The SOHO 6 uses DHCP to make the assignments. When the SOHO 6 receives a request from a new computer on the trusted network, the SOHO 6 assigns the computer an IP address. If you use a DHCP server to assign IP addresses, enable the DHCP Relay option. This option causes the SOHO 6 to forward the DHCP request to the specified DHCP server.

Configuring DHCP server and DHCP relay

To configure DHCP server:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network ⇒Trusted**.
The Trusted Network configuration page opens.



Network
Trusted Network Configuration

IP Address 192.168.111.1

Subnet Mask 255.255.255.0

☑ Enable DHCP Server on Trusted Network

First address for DHCP server

Last address for DHCP server

WINS Server Address

DNS Server Address

Secondary DNS Server Address

DNS Domain Suffix

☐ Enable DHCP Relay

DHCP relay server

3 Type the IP address and the subnet mask in the applicable fields.

4 Select the **Enable DHCP Server on the Trusted Network** checkbox.

5 Type the first IP address that is available for the computers that connect to the trusted network in the applicable fields.

6 Type the WINS Server address, DNS Server primary address, DNS Server secondary address, and DNS Domain server suffix in the applicable fields.

7 To configure the DHCP relay server, select the **Enable DHCP Relay checkbox**.

8 Type the IP address of the DHCP relay server in the applicable field.

9 Click **Submit.**

10 Reboot the SOHO 6.

The SOHO 6 will send all DHCP requests to the specified, remote DHCP server and relay the resulting IP addresses to the computers connected to the trusted network. If the SOHO 6 is unable to contact the specified, remote DHCP server in 30 second, it will revert to using its own DHCP server to respond to computer on the trusteed network.

Configuring additional computers on the trusted network

The SOHO 6 accepts the direct connection of a maximum of four computers, printers, scanners, or other network peripherals. The use of one or more 10BaseT Ethernet hubs with RJ-45 connectors allows the connection of additional appliances.

Follow these steps to add a computer to the trusted network:

1 Make sure that the computer has an Ethernet card installed.

2 Shut down the computer.

3 Connect the computer to the network as shown in “Cabling the SOHO 6 for more than four appliances” on page 20.

4 Restart the computer.

5 Set the computer to get its address through DHCP as shown in “Enabling your computer for DHCP” on page 16.

6 Shut down and restart the computer.

Configuring the trusted network with static addresses

To disable the SOHO 6 DHCP server and make static address assignments, follow these steps:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.

The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network** ⇒**Trusted**.

The Trusted Network configuration page opens.

3 Type the IP address and the subnet mask in the applicable fields.

4 Clear the **Enable DHCP Server on the Trusted Network** checkbox.

5 Click **Submit.**

6 Reboot the SOHO 6 as necessary.

7 Configure the appliances on the trusted network with static addresses.

Configuring Static Routes

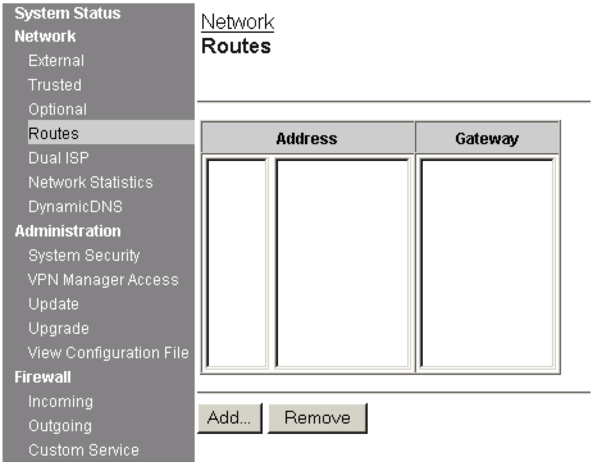
To send the specified packets to different segments of the trusted network connected through a router or switch, configure static routes.

Follow these instructions to configure static routes:

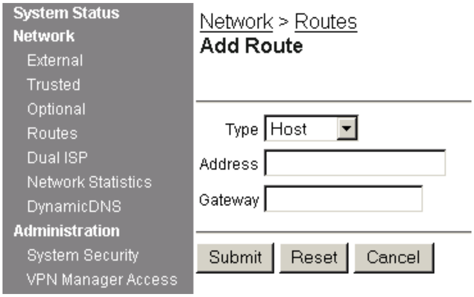
1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.

The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network** ⇒**Routes**.
The Routes page opens.



3 Click **Add**.
The Add Route page opens.



Type Host
Address
Gateway

4 From the **Type** drop-down list, select either **Host** or **Network**.

5 Type the IP address and the gateway of the route in the applicable fields.
The gateway of the route is the local interface of the router.

6 Click **Submit**.

To remove a route, select the route and click **Remove**.

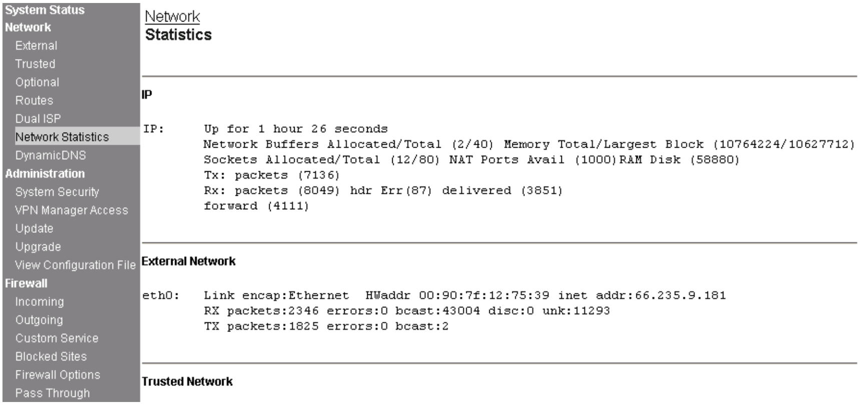
Viewing Network Statistics

The Network Statistics page gives information about network performance. This page is useful during troubleshooting.

Follow these instructions to access the Network Statistics page:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
  The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network ⇒Network Statistics**.
  The Network Statistics page opens.



Network
Statistics

IP

```
IP:      Up for 1 hour 26 seconds
         Network Buffers Allocated/Total (2/40) Memory Total/Largest Block (10764224/10627712)
         Sockets Allocated/Total (12/80) NAT Ports Avail (1000)RAM Disk (58880)
         Tx: packets (7136)
         Rx: packets (8049) hdr Err(87) delivered (3851)
         forward (4111)
```

External Network

```
eth0:    Link encap:Ethernet  HWaddr 00:90:7f:12:75:39 inet addr:66.235.9.181
         RX packets:2346 errors:0 bcast:43004 disc:0 unk:11293
         TX packets:1825 errors:0 bcast:2
```

Trusted Network

Configuring the Dynamic DNS Service

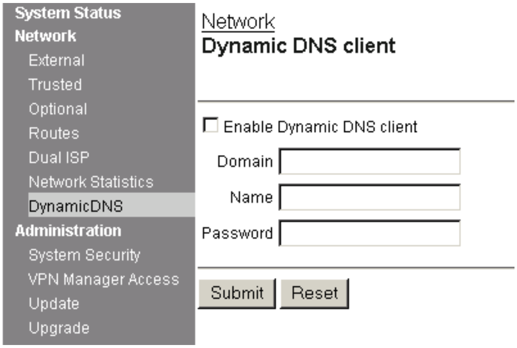
This feature allows you to register the external IP address of the SOHO 6 with the dynamic DNS (Domain Name Server) service DynDNS.org. A dynamic DNS service makes sure that the IP address attached to your domain name is changed when your ISP assigns you a new IP address.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

NOTE

WatchGuard is not affiliated with dyndns.org.

2 From the navigation bar at left, select **Network ⇒DynamicDNS**.
The Dynamic DNS client page opens.



Network
Dynamic DNS client

□ Enable Dynamic DNS client

Domain

Name

Password

3 Select the **Enable Dynamic DNS client** checkbox.

4 Type the domain, name, and password in the applicable fields.

NOTE

The SOHO 6 receives the IP address of members.dyndns.org when it connects to the time server.

5 Click **Submit**.

Configuring the OPT Port Upgrades

The optional (OPT) port of the SOHO 6 supports two upgrades:

- Dual ISP Port upgrade
- VPNforce Port upgrade

To upgrade the SOHO 6, purchase an additional license and activate the new upgrade option. See “Activating the SOHO 6 Upgrade Options” on page 56 for more information about how to upgrade the SOHO 6.

NOTE

The OPT port is only for the Dual ISP Port upgrade or VPNforce Port upgrade. You cannot use the OPT port as an Ethernet port on the trusted network.

Configuring the Dual ISP Port

The Dual ISP Port upgrade adds redundant support for the external interface. With this upgrade installed, the SOHO 6 starts a connection through the optional port when the primary external port connection fails.

There are no new policy definitions needed. The optional interface uses the same policy definitions as the external interface.

The SOHO 6 uses two methods to determine if the external interface connection is down:

- The status of the link to the nearest router
- A ping to a specified location

The SOHO 6 pings the default gateway or the location selected by the administrator. If there is no response, the SOHO 6 switches to the secondary external network connection.

When this upgrade option is activated, these actions automatically occur:

- If the external connection fails, the optional port (OPT) connection is opened and used.
- If the optional port (OPT) connection fails, the external port (EXT) connection is opened and used.
- If the external port (EXT) and optional port (OPT) connections fail, the SOHO 6 tries both ports until a connection is made.

When the optional port (OPT) is in use, the SOHO 6 does not switch back to the external port (EXT) unless PPPoE is used to assign IP addresses. After the SOHO 6 switches to the optional port (OPT), the administrator must change the configuration back to the external port (EXT) when the connection is restored.

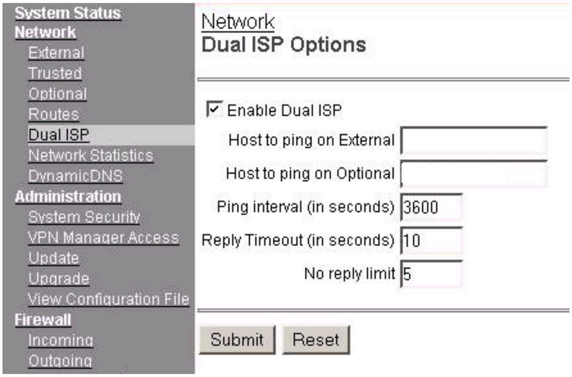
If you use PPPoE, you can set an inactivity timeout that disables inactive TCP connections during periods of inactivity. See “Configuring the SOHO 6 external network for PPPoE” on page 34 for PPPoE configuration information. If your external connection fails, the optional port connection is started and used. The optional port (OPT) is used until the TCP connection becomes inactive (timeout). When the traffic continues, the SOHO 6 connects through the external port (EXT) first. If a connection is made, the external port (EXT) is used. If the external port (EXT) is not available, the SOHO 6 connects through the optional port (OPT).

After you upgrade the SOHO 6 to activate this upgrade option, follow these instructions to complete the configuration:

1 Connect one end of a straight-through Ethernet cable to the optional port (OPT), and connect the other end to the source of the secondary external network connection. This connection can be a DSL modem, a cable modem, or a hub.

2 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

3 From the navigation bar at left, select
Network ⇒**Dual ISP**.
The Dual ISP Options page opens.



Network
Dual ISP Options

☑ Enable Dual ISP

Host to ping on External	
Host to ping on Optional	
Ping interval (in seconds)	3600
Reply Timeout (in seconds)	10
No reply limit	5

4 Select the **Enable Dual ISP** check box.

5 Type the IP addresses for the external and optional interfaces in the applicable fields.

6 Type the number of seconds between pings and the number of seconds to wait for a reply in the applicable fields.

7 Type the limit number of pings before timeout in the applicable field.

8 Click **Submit**.

Configuring the VPNforce™ Port

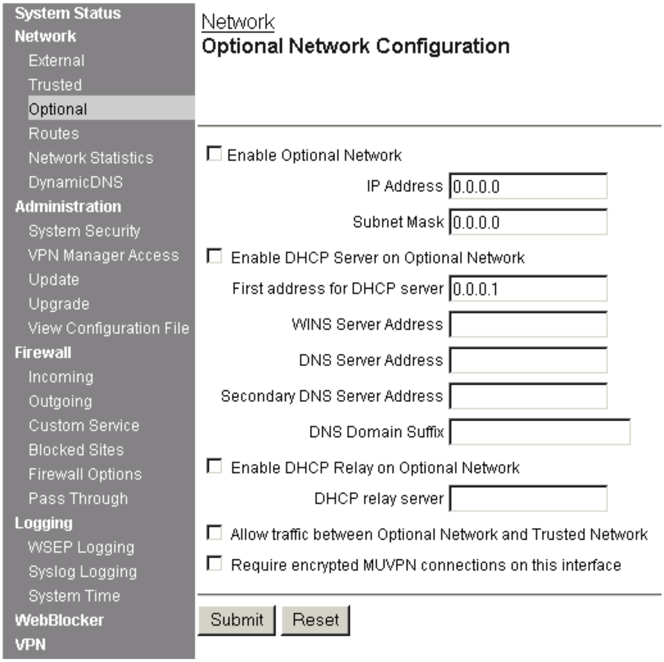
The VPNforce Port upgrade activates the SOHO 6 optional port (OPT) for connection to a second network on the trusted side. This option extends the protection of the firewall to include a telecommuter or a network in a remote office. The new users have secure access to the corporate network and protected access to the Internet.

When the optional port (OPT) is used for VPNforce, a new network is made that is separate from the network used by the trusted network. The default IP address for the network attached to the optional port is 192.168.112.0.

After you upgrade the SOHO 6 to activate this upgrade option, follow these instructions to complete the configuration:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network** ⇒**Optional**.
The Optional Network Configuration page opens.



Network

Optional Network Configuration

□ Enable Optional Network

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

□ Enable DHCP Server on Optional Network

First address for DHCP server 0.0.0.1

WINS Server Address

DNS Server Address

Secondary DNS Server Address

DNS Domain Suffix

□ Enable DHCP Relay on Optional Network

DHCP relay server

□ Allow traffic between Optional Network and Trusted Network

□ Require encrypted MUVPN connections on this interface

3 To enable VPNforce, select the **Enable Optional Network** checkbox.

4 Type the IP address, DHCP Server, and DHCP Relay for the optional interface in the applicable fields.

This is the same process for configuring the trusted network. See "Configuring the Trusted Network" on page 36 for additional instructions about these fields.

5 To allow traffic between the optional network and trusted network, select the **Allow traffic between Optional Network and Trusted Network** checkbox.

6 To require encrypted MUVPN connections on this interface, select the **Require Encrypted MUVPN connections on this interface** check box.

7 Click **Submit**.

CHAPTER 5

Administrative Options

Use the SOHO 6 Administration page to configure access to the SOHO 6. The System Security, SOHO 6 Remote Management feature, and VPN Manager Access are configured from the Administration page. The firmware updates, upgrade activation, and display of the SOHO 6 configuration file in a text format are done from the Administration page.

The System Security Page

The System Security page contains the settings that control access to the configuration of the SOHO 6. Set a system administrator name and passphrase to limit access to the configuration pages. Enable remote management to allow the configuration of the SOHO 6 from the external network.

System security

A passphrase prevents access to the configuration of the SOHO 6 by an unauthorized user on the trusted network. The use of a passphrase is important to the security of your network.

Note

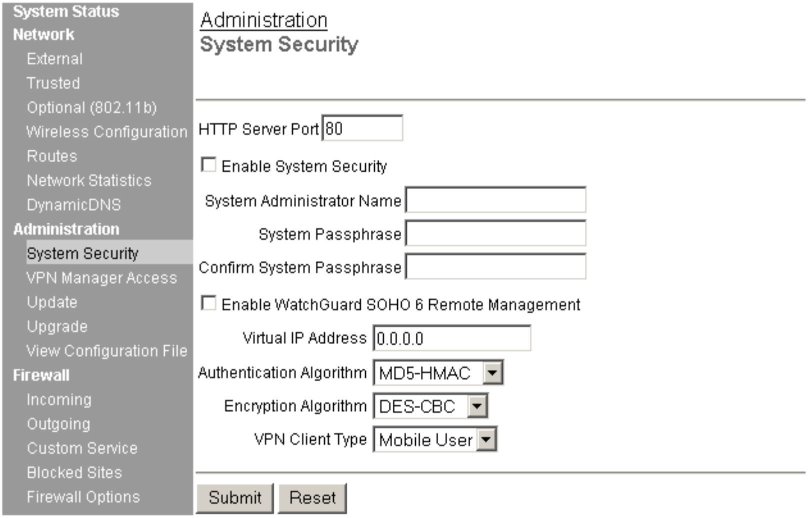
Record the system administrator name and passphrase in a safe location. When system security is enabled, the system administrator name and passphrase are required to access the configuration pages. If the system administrator name and passphrase are unknown, you must reset the SOHO 6 to the factory default settings. See "Factory Default Settings" on page 25 for additional information.

Change the System Administrator passphrase every month. Select a combination of eight letters, numbers, and symbols. Do not use an English or foreign word. Use at least one special symbol, a number, and a mixture of upper case and lower case letters for increased security.

Follow these instructions to enable system security:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Administration** =>**System Security**.
The System Security page opens.



Administration
System Security

HTTP Server Port 80

□ Enable System Security

System Administrator Name

System Passphrase

Confirm System Passphrase

□ Enable WatchGuard SOHO 6 Remote Management

Virtual IP Address 0.0.0.0

Authentication Algorithm MD5-HMAC

Encryption Algorithm DES-CBC

VPN Client Type Mobile User

3 Verify that the **HTTP Server Port** is set to 80.

4 Select the **Enable System Security** checkbox.

5 Type a system administrator name and passphrase and then type the passphrase again to confirm it in the applicable fields.

6 Click **Submit**.

SOHO 6 Remote Management

Both the SOHO 6 and SOHO 6tc include the SOHO 6 Remote Management feature. This feature allows a remote computer on an unsecured network to manage the SOHO 6 with a secure connection. The secure connection is achieved through the use of the MUVPN client or Pocket PC client software application on the remote computer. Both of these client software applications use the Internet Protocol Security (IPSec) standard.

Here is an example of how the Remote Management feature can be used. First, the remote computer connects to the SOHO 6 through a standard Internet connection. Then the MUVPN client software is activated. Finally, the MUVPN client creates an encrypted tunnel to the SOHO 6. The remote computer can now access the configuration pages of the SOHO 6 without compromising security.

Here is another example of how the Remote Management feature can be used. Use a Pocket PC to connect to the SOHO 6 through the Internet. The Pocket PC client software creates an encrypted tunnel to the SOHO 6. The remote computer can now access the configuration pages of the SOHO 6 without compromising security."System security" on page 50

1 First, follow the instructions in "System security" on page 50.

2 Select the **Enable SOHO 6 Remote Management** checkbox.

3 Type the Virtual IP address in the applicable field.
  This address is used by the remote management computer to connect to the SOHO 6.

4 Select an authentication algorithm from the **Authentication Algorithm** drop-down list.
  The selections are MD5-HMAC (128-bit authentication) or SHA1-HMAC (160-bit authentication).

5 Select an encryption algorithm from the **Encryption Algorithm** drop-down list.
  The selections are DES-CBC or 3DES-CBC.

6 Select the VPN client type from the **VPN Client Type** drop-down list.
  The selections are Mobile User (MUVPN) or Pocket PC.

7 Click **Submit**.

8 Install and configure the MUVPN client on the remote computer.
  For this information, see Chapter 10 "MUVPN Clients" on page 105.

9 After you have installed and configured the MUVPN client, connect to the Internet using Dial-Up Networking or a LAN or WAN connection.

From the Windows desktop system tray, follow these steps:

10 Verify that the MUVPN client has been activated. If the MUVPN client has not been activated, right-click the icon and select **Activate Security Policy**.

For information on how to determine the status of the MUVPN icon, see "The MUVPN client icon" on page 133.

11 Right-click the icon and select **Connect**.

The WatchGuard Mobile User Connect window appears.

12 Click **Yes**.

13 Type the IP address of the SOHO 6 external network in your browser window to connect to the System Status page.

Setting up VPN Manager Access

The VPN Manager Access page configures the SOHO 6 to allow remote configuration of the SOHO 6 by the WatchGuard VPN Manager software. The WatchGuard VPN Manager software configures and manages VPN tunnels.

The VPN Manager software is a separate product and must run on a WatchGuard Firebox II/III. Additional information about the VPN Manager product is available on the WatchGuard Web site:

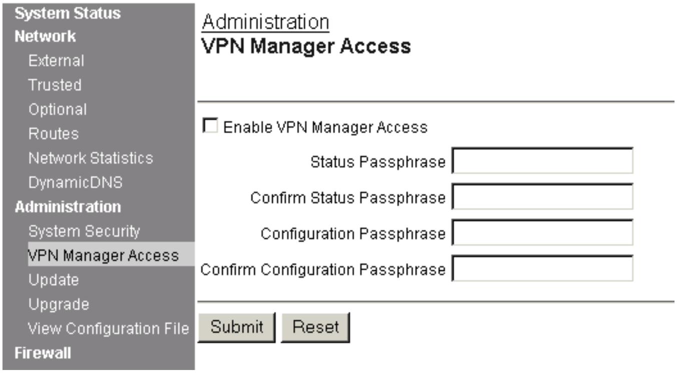
https://www.watchguard.com/products/vpnmanager.asp

Follow these instructions to configure VPN Manager access:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.

The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Administration** ⇒**VPN Manager Access**.
The VPN Manager Access page opens.



Administration

VPN Manager Access

□ Enable VPN Manager Access

Status Passphrase

Confirm Status Passphrase

Configuration Passphrase

Confirm Configuration Passphrase

3 Select the **Enable VPN Manager Access** checkbox.

4 Type the status passphrase and then type it again to confirm in the applicable fields.

5 Type the configuration passphrase and then type it again to confirm in the applicable fields.

NOTE

These passphrases *must* match the passphrases used in the VPN Manager software or the connection will fail.

6 Click **Submit**.

Updating the Firmware

Check regularly for SOHO 6 firmware updates on the WatchGuard Web site:

http://www.watchguard.com/support/sohoresources/

Download the files that contain the firmware update. Save the files on your computer.

Follow these instructions to transfer the new firmware to your SOHO 6:

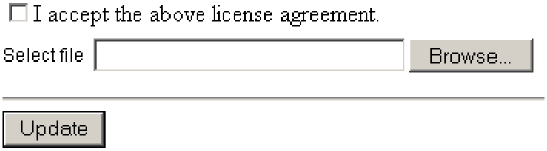
1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Administration ⇒Update**.
The Update page opens.

NOTE

If you configure your SOHO 6 from a computer that does not use the Windows operating system, such as Macintosh or Linux, you must update your firmware with this procedure. The WatchGuard installation programs supplied on CD-ROM are compatible only with Windows platforms.

3 Read the end-user license agreement. Then select the **I accept the above license agreement** checkbox at the bottom of the page.



4 Type the location of the firmware files on your computer or click **Browse** and locate the firmware files on your computer.

5 Click **Update**.
Follow the instructions provided by the update wizard.

NOTE

The update wizard requests a user name and password. Type the system administrator name and passphrase configured on the System Security page. The default values are "user" and "pass".

Activating the SOHO 6 Upgrade Options

Every SOHO 6 includes the software for all upgrade options. To activate an upgrade option, you must enter a license key in the configuration of the SOHO 6. To receive a license key, purchase and activate an upgrade option at the LiveSecurity Service Web site. See "Registering Your SOHO 6 and Activating the LiveSecurity Service" on page 27 for more information.

Follow these steps to activate an upgrade option:

1 Go to the upgrade page of the WatchGuard Web site:
http://www.watchguard.com/upgrade

2 Type your user name and password in the applicable fields.

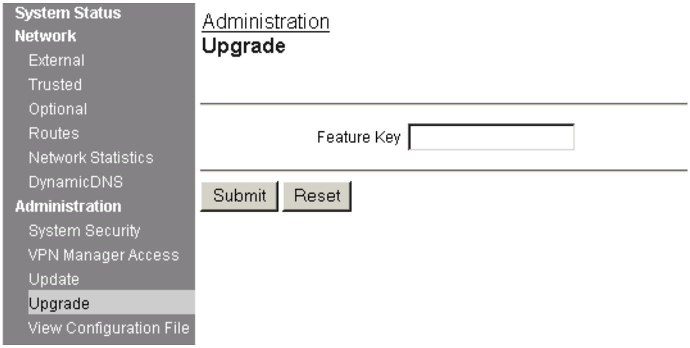
3 Click **Log In**.

4 Follow the instructions provided on the Web site to activate your license key.

5 Copy the feature key from the LiveSecurity Service Web site.

6 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

7 From the navigation bar at left, select **Administration** ⇒**Upgrade**.
The Upgrade page opens.



8 Paste the **Feature Key** in the applicable field.

9 Click **Submit**.

Upgrade options

Seat licenses

A seat license upgrade allows more connections between the trusted network and the external network. For example, a 25-seat license allows 25 connections instead of the standard 10 connections.

Dual ISP Port

The Dual ISP Port upgrade adds redundant support for the external interface.

VPNforce Port

The VPNforce Port upgrade activates the SOHO 6 optional port (OPT) for connection to a second network on the trusted side. This option extends the protection of the firewall to include a telecommuter or a network in a remote office.

IPSec Virtual Private Networking (VPN)

The VPN upgrade is necessary to configure virtual private networking. The SOHO 6tc includes a VPN upgrade license key. The SOHO 6 does not include a VPN upgrade license key.

WebBlocker

The WebBlocker upgrade enables the Web filtering option.

MUVPN Clients

The MUVPN Clients upgrade allows remote users to connect to the SOHO 6 through a secure (IPSec) VPN tunnel. These users have access to trusted network resources.

LiveSecurity Service subscription renewals

Purchase a LiveSecurity subscription renewal for a period of one or two years from your reseller or the WatchGuard online store. Go to the renew page of the WatchGuard Web site to purchase or activate a subscription renewal:

http://www.watchguard.com/renew/

Follow the instructions on the Web site.

Viewing the Configuration File

The contents of the SOHO 6 configuration file is available in text format from the View Configuration File page.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Administration ⇒View Configuration File**.
The View Configuration File page opens.

CHAPTER 6

Configure the Firewall Settings

Firewall Settings

The configuration settings of the SOHO 6 control the flow of traffic between the trusted network and the external network. The configuration you select depends on the types of risks that are acceptable for the trusted network.

The SOHO 6 lists many standard services on the configuration page. A service is the combination of protocol and port numbers for a type of application or communication.

Configuring Incoming and Outgoing Services

The default configuration of the SOHO 6 prevents the transmission of all packets from the external network to the trusted network. Change the configuration to select the types of traffic that are permitted. For example, to operate a Web server behind the SOHO 6, add an incoming Web service.

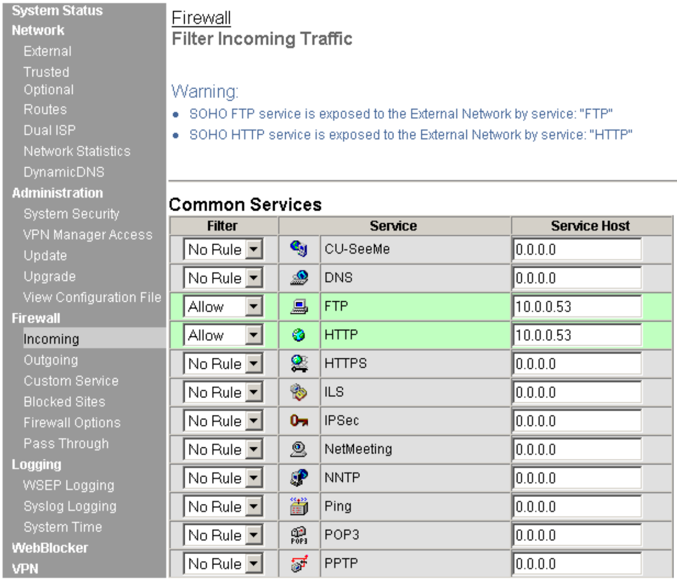
Select carefully the number and the types of services that you add. The added services decrease the security of your network. Compare the value of access to each service against the security risk caused by that service.

Common services

Follow these steps to change the configuration of the incoming filters for common services:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Firewall** ⇒**Incoming** or **Outgoing**.
The Filter Traffic page opens.



Firewall
Filter Incoming Traffic

Warning:

- SOHO FTP service is exposed to the External Network by service: "FTP"
- SOHO HTTP service is exposed to the External Network by service: "HTTP"

Common Services

Filter	Service	Service Host
No Rule	CU-SeeMe	0.0.0.0
No Rule	DNS	0.0.0.0
Allow	FTP	10.0.0.53
Allow	HTTP	10.0.0.53
No Rule	HTTPS	0.0.0.0
No Rule	ILS	0.0.0.0
No Rule	IPSec	0.0.0.0
No Rule	NetMeeting	0.0.0.0
No Rule	NNTP	0.0.0.0
No Rule	Ping	0.0.0.0
No Rule	POP3	0.0.0.0
No Rule	PPTP	0.0.0.0

3 Locate a pre-configured service, such as FTP, Web, or Telnet. Then select either **Allow** or **Deny** from the drop-down list.

The previous illustration shows the HTTP service configured to allow incoming traffic.

4 Type the trusted network IP address of the computer to which this rule applies in the applicable field.

The illustration shows the HTTP service configured to allow incoming traffic to the computer with IP address 192.168.111.2.

5 Click **Submit**.

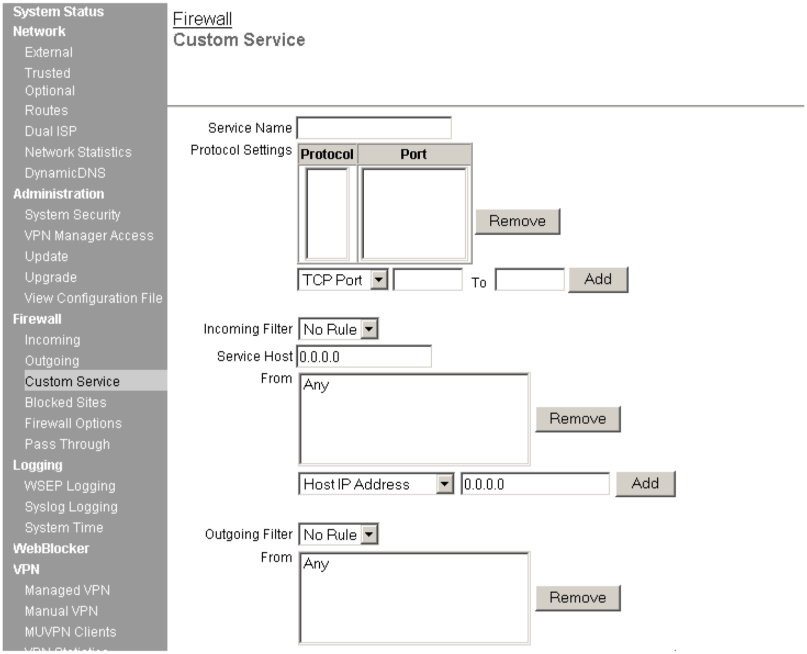
Creating a custom service

If you need to allow a service that is not listed in the common services, configure a custom service based on a TCP port, a UDP port, or a protocol.

Follow these steps to configure a custom service:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Firewall** ⇒**Custom Service**.
The Custom Service page opens.



Firewall
Custom Service

Service Name
Protocol Settings

Protocol	Port

TCP Port

Incoming Filter: No Rule
Service Host: 0.0.0.0
From: Any
Host IP Address: 0.0.0.0

Outgoing Filter: No Rule
From: Any

3 Type a name for the service in the **Service name** field.

4 Select **TCP Port**, **UDP Port**, or **Protocol** from the drop-down list below the **Protocol Settings**.
The Custom Service page refreshes.

5 In the fields separated by the word **To**, type the port number or the range of port numbers, or type the protocol number.

NOTE

For a TCP port or a UDP port, specify a port number. For a protocol, specify a protocol number. You cannot specify a port number for a protocol.

6 Click **Add**.

The following steps determine how the service is filtered.

7 Select **Allow** or **Deny** from the **Incoming Filter** and **Outgoing Filter** drop-down lists.

8 Select **Host IP Address**, **Network IP Address**, or **Host Range** from the drop-down list at the bottom of the page.

The Custom Service page refreshes.

9 Type a single host IP address, a network IP address, or the start and end of a range of host IP addresses in the applicable address field.

10 Click **Add**.

Repeat the previous three steps until all of the address information for this custom service is set.

11 Click **Submit**.

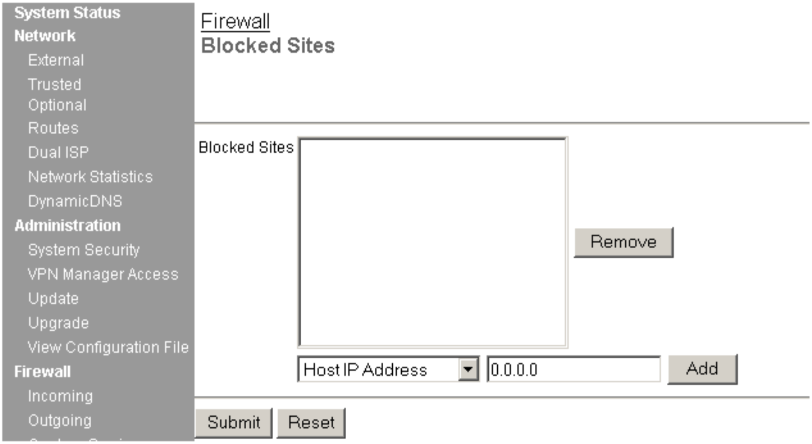
Blocking External Sites

The default configuration of the SOHO 6:

- Allows the transmission of all packets from the trusted network to the external network
- Prevents the transmission of all packets from the external network to the trusted network

You can change the configuration to prevent access to specified Internet sites. Follow these steps to configure the blocked sites:

1 From the navigation bar at left, select **Firewall** ⇒**Blocked Sites**.
The Blocked Sites page opens.



2 Select either **Host IP Address**, **Network IP Address**, or **Host Range** from the drop-down list.
The Blocked Sites page refreshes.

3 Type a single host IP address, a network IP address, or the start and end of a range of host IP addresses in the applicable address field.

4 Click **Add**.
The address information appears in the Blocked Sites field.

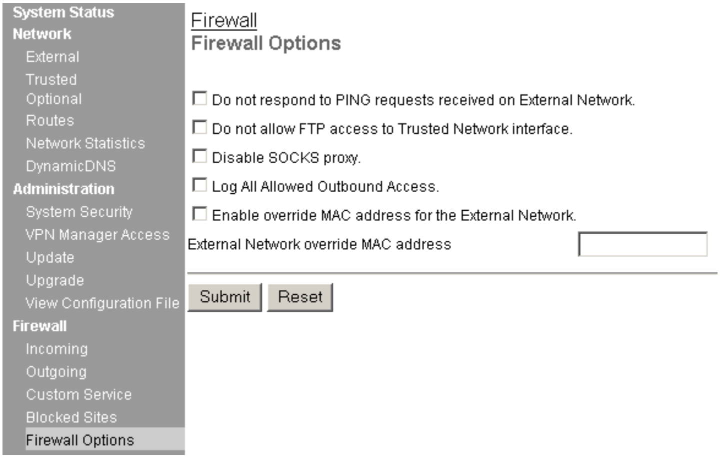
5 Click **Submit**.

Firewall Options

The previous sections described how to allow or deny complete classes of services. The Firewall Options page allows the configuration of general security policies.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Firewall ⇒Firewall Options**.
The Firewall Options page opens.



Firewall
Firewall Options

□ Do not respond to PING requests received on External Network.
□ Do not allow FTP access to Trusted Network interface.
□ Disable SOCKS proxy.
□ Log All Allowed Outbound Access.
□ Enable override MAC address for the External Network.
External Network override MAC address

Responding to ping requests from the external network

You can configure the SOHO 6 to deny all ping packets received on the external interface.

1 Select the **Do not respond to PING requests received on External Network checkbox**.

2 Click **Submit**.

Denying FTP access to the trusted network interface

You can configure the SOHO 6 to prevent FTP access to the computers on the trusted network by the computers on the external network.

1 Select the **Do not allow FTP access to Trusted Network** checkbox.

2 Click **Submit**.

SOCKS implementation for the SOHO 6

The SOHO 6 functions as a SOCKS network proxy server. An application that uses more than one socket connection and implements the SOCKS version 5 protocol can communicate through the SOHO 6. SOCKS supplies a secure, two-way communication channel between a computer on the external network and a computer on the trusted network. To use a SOCKS-compatible application, configure the application with the necessary information about the SOHO 6.

The SOHO 6 supports SOCKS version 5 only. The SOHO 6 does not support authentication or DNS (Domain Name System) resolution.

NOTE

Configure the SOCKS-compatible application to connect to IP addresses and not to domain names. Applications that can only reference domain names are not compatible with the SOHO 6.

Some SOCKS-compatible applications that function correctly when used through the SOHO 6 are ICQ, IRC, and AOL Messenger.

NOTE

When a computer in the trusted network uses a SOCKS-compatible application, other users on the trusted network have free access to the SOCKS proxy on that computer. Disable SOCKS on the SOHO 6 to prevent this security risk. See "Disabling SOCKS on the SOHO 6" on page 69.

Configuring your SOCKS application

To allow a SOCKS-compatible application on a computer in the trusted network to communicate with a computer on the external network, configure the application as described below. To make these settings, refer to the user's guide for the application.

NOTE

The SOHO 6 uses port 1080 to communicate with a computer that uses a SOCKS-compatible application. Make sure that port 1080 is not in use by other applications on the computer.

- If there is a selection of protocols or SOCKS versions, select SOCKS version 5.
- Select port 1080.
- Set the SOCKS proxy to the URL or IP address of the SOHO 6. The default IP address is: http://192.168.111.1.

Disabling SOCKS on the SOHO 6

After a SOCKS-compatible application has connected through the SOHO 6, the SOCKS port stays open. After the application terminates, the SOCKS port is available to anyone on your trusted network. The following steps prevent this security problem.

When the SOCKS-compatible application is not in use:

1. Select the **Disable SOCKS proxy** checkbox.
   This disables the SOCKS proxy feature of the SOHO 6.
2. Click **Submit**.

To use the SOCKS-compatible application:

1. Clear the **Disable SOCKS proxy** checkbox.
   This enables the SOHO 6 SOCKS proxy server.
2. Click **Submit**.
   This disables the SOHO 6 SOCKS proxy server.

Logging all allowed outbound traffic

When in the default configuration, the SOHO 6 only records unusual events. For example, all denied traffic is recorded in the log file. You can change the configuration of the SOHO 6 to record all outbound traffic events.

NOTE

This option records an large number of log entries. WatchGuard recommends that you use this option as a problem-solving aid only.

Follow these steps to enable this option:

1. Select the **Log All Allowed Outbound Access** checkbox.
2. Click **Submit**.

Enabling the MAC Address Override for the External Network

If your ISP requires a MAC address, enable this option. The SOHO 6 will use its own MAC address for the trusted network. You can enter a new MAC address for use on the external network.

Follow these steps to enable this option:

1. Select the **Enable override MAC address for the External Network** checkbox.
2. Type the new MAC address for the SOHO 6 external network in the applicable field.
3. Click **Submit**.

NOTE

If the **MAC address for the external network** field is cleared and the SOHO 6 is rebooted, the SOHO 6 is reset to the factory-default MAC address for the external network.

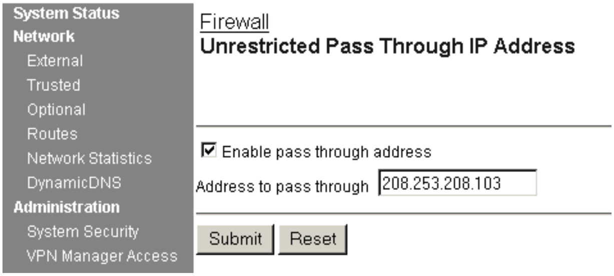
To prevent MAC address collisions, the SOHO 6 searches the external network periodically for the override MAC address. If the SOHO 6 finds a device that uses the same MAC address, the SOHO 6 resets to the factory-default external MAC address and reboots.

Creating an Unrestricted Pass Through

The SOHO 6 can allow traffic to flow from the external network to a computer on the trusted network that has a public IP address.

Follow these steps to configure a pass through:

1. Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
   The default IP address is: http://192.168.111.1
2. From the navigation bar at left, select
   Firewall ⇒Pass Through.
   The Unrestricted Pass Through IP Address page opens.



Unrestricted Pass Through IP Address

☑ Enable pass through address

Address to pass through 208.253.208.103

3 Select the **Enable pass through address** checkbox.

4 Type the IP address of the computer to connect to the pass through in the applicable field.

This must be a public IP address.

5 Click **Submit**.

NOTE

A pass through connection decreases the security of the trusted network, because the computer with the pass through connection is on the same Ethernet segment as the trusted network. Do not use a pass through connection unless the effect of the pass through connection on the security of the trusted network is known.

CHAPTER 7

Configure Logging

The SOHO 6 logging feature records a log of the events related to the security of the trusted, external, and optional networks. Communication with the WatchGuard WebBlocker database and incoming traffic are examples of events that are recorded. The log records the events that show possible security problems. A denied packet is the most important type of event to log. A sequence of denied packets can show that an unauthorized person tried to access your network.

NOTE

The records in the SOHO 6 log are erased if the power supply is disconnected.

Viewing SOHO 6 Log Messages

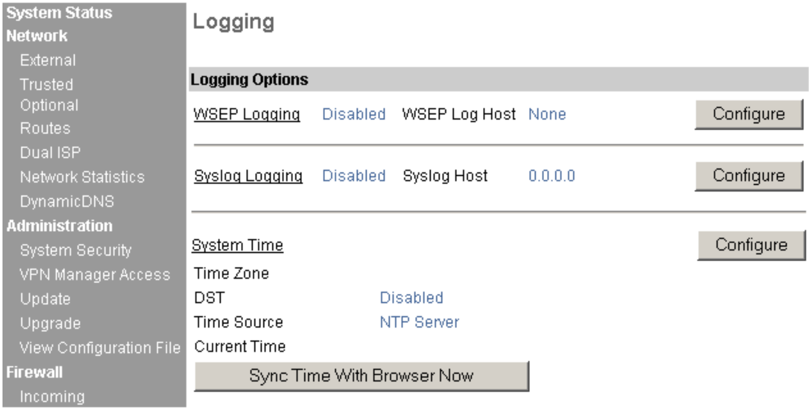
The SOHO 6 event log records a maximum of 150 log messages. If a new entry is added when the event log is full, the oldest log message is removed.

The log messages include the time synchronizations between the SOHO 6 and the WatchGuard Time Server, packets discarded because of a packet handling violation, duplicate messages, return error messages, and IPSec messages.

The following procedure shows how to view the event log:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Logging**.
The Logging page opens with the Event Log at the bottom of the page.



Logging

Logging Options

WSEP Logging Disabled WSEP Log Host None

Syslog Logging Disabled Syslog Host 0.0.0.0

System Time

Time Zone

DST Disabled

Time Source NTP Server

Current Time

NOTE

The newest entry is shown at the top of the event log.

This option synchronizes the clock of the SOHO 6 to your computer:

- Click **Sync Time with Browser now**.

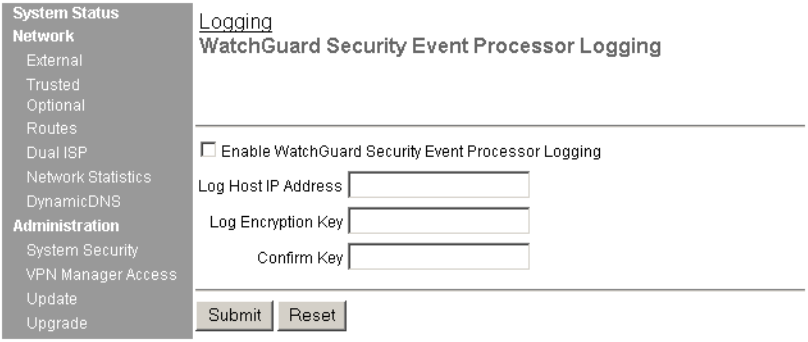
The SOHO 6 synchronizes the time at startup.

Setting up Logging to a WatchGuard Security Event Processor Log Host

The WSEP (WatchGuard Security Event Processor) is an application that is available with the *WatchGuard Firebox System* package used by a Firebox II/III. The WSEP application runs on a computer that functions as the log host. The WSEP application records log messages sent from the Firebox II/III. If you have a Firebox II/III, configure the WSEP to accept the log messages from your SOHO 6. Then follow these instructions to send your event logs to the WSEP.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select
Logging ⇒WSEP Logging.
The WatchGuard Security Event Processor page opens.



Logging
WatchGuard Security Event Processor Logging

□ Enable WatchGuard Security Event Processor Logging

Log Host IP Address

Log Encryption Key

Confirm Key

3 Select the **Enable WatchGuard Security Event Processor Logging** checkbox.

4 Type the IP address of the WSEP server that is your log host in the applicable field.

5 Type a passphrase in the **Log Encryption Key** field and confirm the passphrase in the **Confirm Key** field.

6 Click **Submit**.

NOTE

Use the same encryption key recorded in the WSEP application.

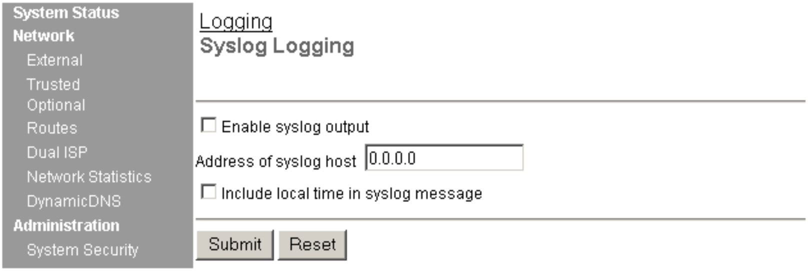
Setting up Logging to a Syslog Host

This option sends the SOHO 6 log entries to a Syslog host.

Follow these steps to configure a Syslog Host:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Logging ⇒Syslog Logging**.
The Syslog Logging page opens.



Logging
Syslog Logging

□ Enable syslog output

Address of syslog host 0.0.0.0

□ Include local time in syslog message

3 Select the **Enable syslog output** checkbox.

4 Type the IP address of the Syslog server in the applicable field.

5 Click **Submit**.

This option includes the local time from your browser in the Syslog messages:

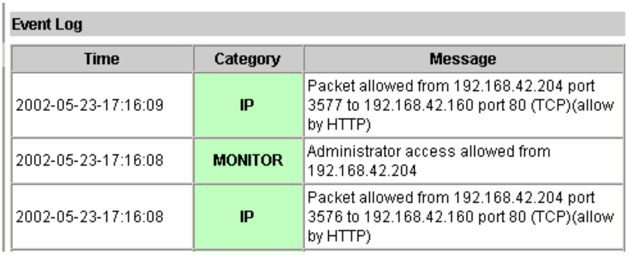
- Select the **Include local time in syslog message** checkbox.

NOTE

Syslog traffic is not encrypted. Syslog messages that are sent through the Internet decrease the security of the trusted network. Use a VPN tunnel to increase the security of Syslog message traffic. If the Syslog messages are sent through a VPN tunnel, the data is encrypted with IPSec technology.

Setting the System Time

The SOHO 6 records the time of each log entry.



Event Log

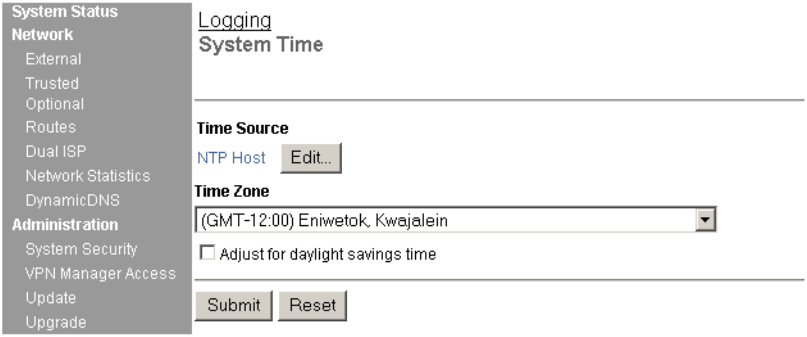
Time	Category	Message
2002-05-23-17:16:09	IP	Packet allowed from 192.168.42.204 port 3577 to 192.168.42.160 port 80 (TCP)(allow by HTTP)
2002-05-23-17:16:08	MONITOR	Administrator access allowed from 192.168.42.204
2002-05-23-17:16:08	IP	Packet allowed from 192.168.42.204 port 3576 to 192.168.42.160 port 80 (TCP)(allow by HTTP)

The time recorded in the log entries is from the SOHO 6 system clock.

Follow these steps to set the system time:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Logging ⇒System Time**.
The System Time page opens.



System Time

Time Source

NTP Host

Time Zone

(GMT-12:00) Eniwetok, Kwajalein

□ Adjust for daylight savings time

3 Select a time zone from the drop-down list.

4 Select the **Adjust for daylight savings time** checkbox.

5 Click **Submit**.

CHAPTER 8

SOHO 6 WebBlocker

WebBlocker is an option for the SOHO 6 that allows the system administrator to control which Web sites the users can access.

How WebBlocker Works

WebBlocker uses a database of Web site addresses, which is owned and maintained by SurfControl. The database shows the type of content found on thousands of Web sites. WatchGuard puts the newest version of the SurfControl database on the WebBlocker server at regular intervals.

WebBlocker checks each Web site request by users in the trusted network. The SOHO 6 sends to the database a request for the type of content found on the Web site. The SOHO 6 uses the rules shown below to control the access to Web sites:

Web site not in the WebBlocker database

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

Web site in the WebBlocker database

If the site is in the WatchGuard WebBlocker database, the SOHO 6 examines the configuration to see if that type of site is permitted. When the type of site is not permitted, the user is told that the site is not available. If the type of site is permitted, the Web browser opens the page.

WatchGuard WebBlocker database unavailable

If the WatchGuard WebBlocker database is not available, the user is told that the Web site is not available. The database is not available if the SOHO 6 cannot connect to the WatchGuard server.

WebBlocker users and groups

- **Groups**

  A group is a set of users on the trusted network.

- **Users**

  Users are persons that use the computers on the trusted network.

Bypassing the SOHO 6 WebBlocker

The SOHO 6 WebBlocker configuration page includes a full access password field. Give this password to those users of the trusted network allowed to bypass WebBlocker. When a site is blocked, the user can supply the full access password to access the Web site. After the user supplies the password, the user can access all Web sites until the password expires or the browser is closed.

Purchasing and Activating the SOHO 6 WebBlocker

To use WatchGuard SOHO 6 WebBlocker, you must purchase and enable the WebBlocker upgrade license key. See “Activating the SOHO 6 Upgrade Options” on page 56 for information about upgrade license keys.

Configuring the SOHO 6 WebBlocker

Use the SOHO 6 configuration pages to configure WebBlocker/

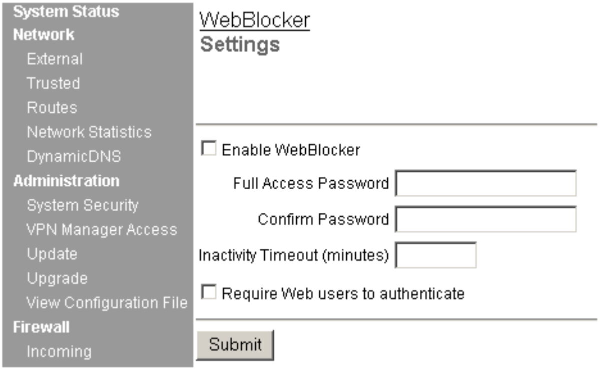
WebBlocker settings

Use the WebBlocker settings page to:

- Activate WebBlocker
- Set the full access password
- Set the inactivity timeout
- Require that your Web users authenticate

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **WebBlocker** ⇒**Settings**.
The WebBlocker Settings page opens.



□ Enable WebBlocker

Full Access Password

Confirm Password

Inactivity Timeout (minutes)

□ Require Web users to authenticate

3 Select the **Enable WebBlocker** checkbox.

4 Type a passphrase in the **Full Access Password** field.

The full access password allows a user to access all Web sites until the password expires or the browser is closed.

5 Type a value, in minutes, in the **Inactivity Timeout field**.

The inactivity timeout disconnects Internet connections that are inactive for the set number of minutes.

6 To set WebBlocker to use groups and users, select the **Require Web users to authenticate checkbox**.

7 Click **Submit**.

Creating WebBlocker groups and users

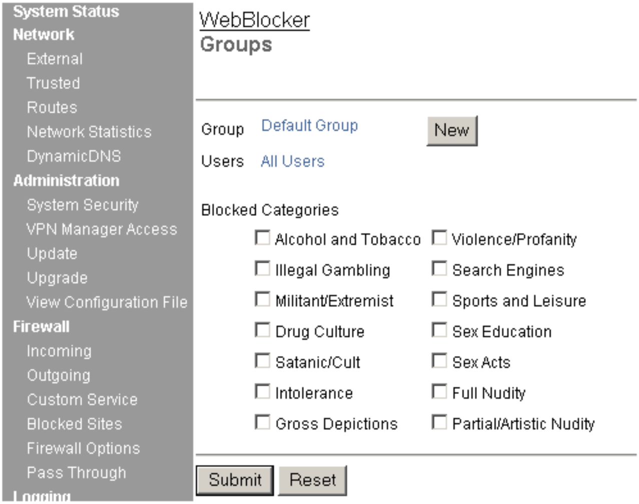
Follow these instructions to create WebBlocker groups:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.

The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **WebBlocker** ⇒**Groups**.

The WebBlocker Groups page opens.



WebBlocker

Groups

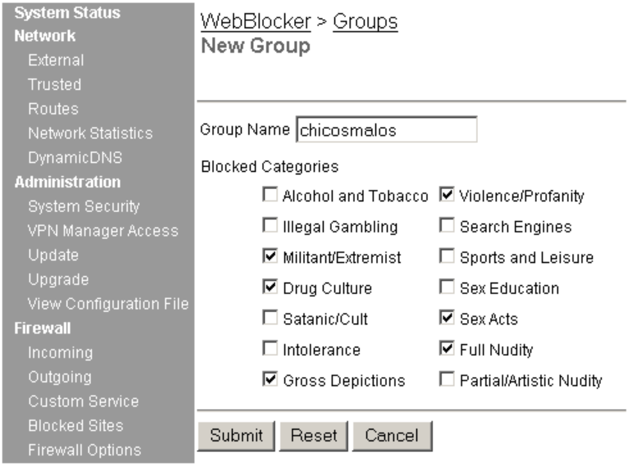
Group Default Group

Users All Users

Blocked Categories

□ Alcohol and Tobacco	□ Violence/Profanity
□ Illegal Gambling	□ Search Engines
□ Militant/Extremist	□ Sports and Leisure
□ Drug Culture	□ Sex Education
□ Satanic/Cult	□ Sex Acts
□ Intolerance	□ Full Nudity
□ Gross Depictions	□ Partial/Artistic Nudity

3 Click **New** to create a group name and profile.



WebBlocker > Groups

New Group

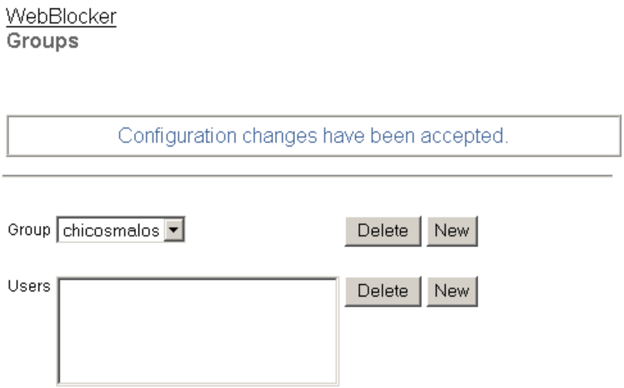
Group Name chicosmalos

Blocked Categories

□ Alcohol and Tobacco	☑ Violence/Profanity
□ Illegal Gambling	□ Search Engines
☑ Militant/Extremist	□ Sports and Leisure
☑ Drug Culture	□ Sex Education
□ Satanic/Cult	☑ Sex Acts
□ Intolerance	☑ Full Nudity
☑ Gross Depictions	□ Partial/Artistic Nudity

4 Define a **Group Name** and select the types of content to filter for this group.

5 Click **Submit.**
A New Groups page opens that shows the configuration changes.



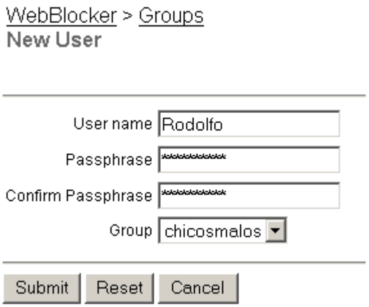
WebBlocker
Groups

Configuration changes have been accepted.

Group: chicosmalos

Users:

6 To the right of the **Users** field, click **New**.
The New User page opens.



WebBlocker > Groups
New User

User name: Rodolfo
Passphrase: **********
Confirm Passphrase: **********
Group: chicosmalos

7 Type a new user name and passphrase and then type the passphrase again to confirm in the applicable fields.

8 Use the **Group** drop-down list to assign the new user to a given group.

9 Click **Submit**.

NOTE

To remove a user or group, make a selection and click **Delete**.

WebBlocker Categories

The WebBlocker database contains the following 14 categories:

NOTE

A Web site is only added to a category if the contents of the Web site advocate the subject matter of the category. Web sites that provide opinion or educational material about the subject matter of the category are not included. 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. This category includes substances that are 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 blocked 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 appliances, 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.

CHAPTER 9

VPN—Virtual Private Networking

This chapter explains how to use the Branch Office VPN upgrade option for the SOHO 6.

Why Create a Virtual Private Network?

Use a VPN tunnel to make an inexpensive and secure connection between the computers in two separate locations. Expensive, dedicated point-to-point connections are not necessary for a VPN connection. A VPN tunnel gives the security necessary to use the public Internet for a virtual private connection.

What You Need

- A SOHO 6 with the VPN upgrade option installed and another IPSec-compatible appliance.

NOTE

IPSec-compatible appliances include the Firebox SOHO 6, the Firebox II/III, and the Firebox Vclass.

- The data from your ISP about the Internet connections for each of the two IPSec-compatible appliances:
    - IP address
    - Primary DNS IP address (optional)
    - A secondary DNS address (optional)
    - Domain name (optional)
- The network addresses and subnet masks for the two trusted networks.

NOTE

The trusted networks at the either ends of the VPN tunnel must have different network addresses.

If the appliances that connect through the VPN tunnel are not configured correctly, the VPN tunnel will not function. WatchGuard recommends that you make a record of the configuration information in the following format.

IP Address Table (example):

Item	Description	Assigned By
External IP Address	The IP address that identifies the IPSec-compatible appliance to the Internet. **Site A:** 207.168.55.2 **Site B:** 68.130.44.15	ISP
External Subnet Mask	The bitmask that shows which part of the IP address identifies the local network. For example, a class C address includes 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	An address used to identify a local network. A local network address cannot be used as an external IP address. WatchGuard recommends that you use an address from one of the reserved ranges: 10.0.0.0/8 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0 **Site A:** 192.168.111.0/24 **Site B:** 192.168.222.0/24	You
Shared Secret	The shared secret is a passphrase used by two IPSec-compatible appliances to encrypt and decrypt the data that goes through the VPN tunnel. The two appliances use the same passphrase. If the appliances do not have the same passphrase, they cannot encrypt and decrypt the data correctly. Use a passphrase that contains numbers, symbols, lowercase letters, and uppercase letters for better security. For example, "Gu4c4mo!3" is better than "guacamole".	You

	Site A: OurLittleSecret **Site B:** OurLittleSecret	
Encryption Method	DES uses 56-bit encryption. 3DES uses 168-bit encryption. The 3DES encryption method gives better security, but decreases the speed of communication. The two IPSec-compatible appliances must use the same encryption method. **Site A:** 3DES **Site B:** 3DES	You
Authentication	The two IPSec-compatible appliances must use the same authentication method. **Site A:** MD5 (or SHA1) **Site B:** MD5 (or SHA1)	You

Enabling the VPN upgrade

To activate an upgrade option, you must enter a license key in the configuration of the SOHO 6. To receive a license key, purchase and activate an upgrade option at the LiveSecurity Service Web site.

To activate the VPN upgrade, these items are necessary:

- A SOHO 6 that is installed and configured
- A connection to the Internet
- A VPN upgrade license key

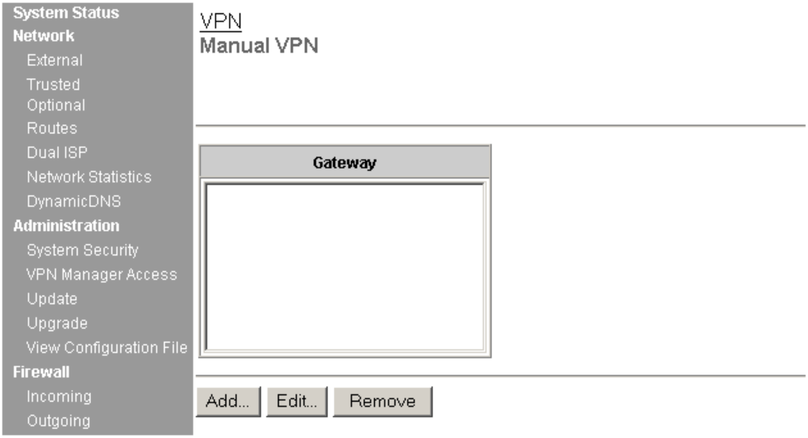
Setting Up Multiple SOHO 6 to SOHO 6 VPN Tunnels

An administrator of a SOHO 6 can configure a maximum of six VPN tunnels to other SOHO 6 devices. The VPN Manager software can configure a larger number of SOHO 6 to SOHO 6 tunnels.

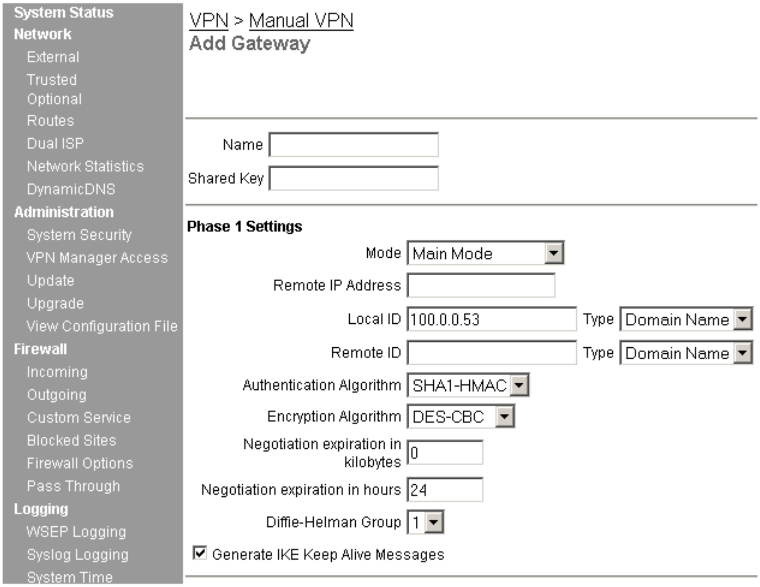
To define multiple VPN tunnels to other SOHO 6 appliances, follow these steps:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **VPN** ⇒**Manual VPN**.
The Manual VPN page opens.



3 Click **Add**.
The Add Gateway page opens.



VPN > Manual VPN

Add Gateway

Name

Shared Key

Phase 1 Settings

Mode: Main Mode

Remote IP Address

Local ID: 100.0.0.53 Type: Domain Name

Remote ID Type: Domain Name

Authentication Algorithm: SHA1-HMAC

Encryption Algorithm: DES-CBC

Negotiation expiration in kilobytes: 0

Negotiation expiration in hours: 24

Diffie-Helman Group: 1

☑ Generate IKE Keep Alive Messages

4 Type the **Name** and **Shared Secret** for the VPN tunnel.

The shared secret is a passphrase used by two IPSec-compatible appliances to encrypt and decrypt the data that goes through the VPN tunnel. The two appliances use the same passphrase. If the appliances do not have the same passphrase, they cannot encrypt and decrypt the data correctly.

5 Use the default **Phase 1** settings or change the settings as necessary.

To modify Phase 1 settings, complete the following steps:

NOTE

The Phase 1 settings must be the same on both appliances.

6 Select the negotiation **Mode** for **Phase 1** from the drop-down list. The mode selections are **Main** and **Aggressive**. If the

external IP address is dynamic, select **Aggressive Mode**. If the external IP address is static, use either mode.

7 Select the **Local ID** type and the **Remote ID** type from the drop-down list. These must match the settings used on the remote gateway.

- If you select **Main Mode**, the **Local ID** type and the **Remote ID** type must contain IP addresses.
- If you select **Aggressive Mode**, the **Remote ID** type may be an IP address or a domain name. If your external IP address is static, the **Local ID** type must be an IP address. If your external IP address is dynamic, the **Local ID** type may be either a domain name or an IP address.

8 From the **Authentication Algorithm** drop-down list, select the type of authentication.

The options are MD5-HMAC (128-bit authentication) or SHA1-HMAC (160-bit authentication).

9 From the **Encryption Algorithm** drop-down list, select the type of encryption.

The options are DES-CBC or 3DES-CBC.

10 Type the number of kilobytes and the number of hours until negotiation expiration in the applicable fields.

11 From the **Diffie-Hellman Group** drop-down list, select the group number. WatchGuard supports group 1 and group 2.

Diffie-Hellman is a mathematical technique used to securely negotiate secret keys through a public network. Diffie-Hellman groups are collections of parameters used to achieve this. Group 2 is more secure than group 1, but more time is required to calculate group 2 secret keys.

12 Select the **Generate IKE Keep Alive Messages** checkbox to keep the VPN tunnel open when there is no communication. Short packets are sent across the VPN tunnel at regular

intervals to maintain the connection. If the tunnel connection closes, the SOHO 6 does a rekey to open the tunnel again.

The Generate IKE Keep Alive Messages checkbox is selected in the default configuration.

Use the default Phase 2 settings, or change the Phase 2 settings as shown below:

NOTE

Make sure that the Phase 2 settings are the same on both appliances.

13 From the **Authentication Algorithm** drop-down list, select the type of authentication.

14 From the **Encryption Algorithm** drop-down list, select the type of encryption.

15 Select the **Enable Perfect Forward Secrecy checkbox**, if necessary.

When this option is selected, each new key that is negotiated is derived by a new Diffie-Hellman exchange instead of from only one Diffie-Hellman exchange. This option gives more security, but increases the time necessary for the communication because of the additional exchange.

16 Type the number of kilobytes and the number of hours until negotiation expiration in the applicable fields.

17 Type the IP address of the local network and the remote network that must use Phase 2 negotiation.

18 Click **Submit**.

Creating a VPN Tunnel to a SOHO 6 with an IPSec-Compliant Appliance

Instructions that tell how to configure a VPN tunnel between a SOHO 6 and another IPSec-compatible appliance are available from the WatchGuard Web site:

https://www.watchguard.com/support/AdvancedFaqs/sointerop_main.asp

Special considerations

Think about these points before you configure your WatchGuard SOHO 6 VPN network:

- You can connect a maximum of six SOHO 6 appliances together in a star configuration. To configure more VPN tunnels, a WatchGuard Firebox II/III with WatchGuard VPN Manager is necessary.
- WatchGuard reccomends that both of the VPN appliances have a static IP address. Configuring a VPN tunnel between two appliances using dynamic IP addresses, can pose several problems. See "Network addressing" on page 31 for more information about dynamic IP addresses. However, these issues can be resolved by using Dynamic DNS. For information on configuring the Dynamic DNS feature, see "Configuring the Dynamic DNS Service" on page 42.
- Both appliances must use the same encryption method; either DES or 3DES.
- When two Microsoft Windows NT networks are connected, the two networks must be in the same Microsoft Windows domain or be trusted domains. This is a Microsoft Networking design implementation and not a limitation of the SOHO 6.

Configuring Split Tunneling

The split tunneling feature allows the system administrator to direct all Internet traffic from the trusted network through the VPN tunnel. Without split tunneling, only traffic directed to the other end of the VPN tunnel is sent through the tunnel and the traffic for other Internet addresses is sent directly to the Internet. Split tunneling allows the control of access to Internet Web sites from one location.

To set up split tunneling follow these steps:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **VPN** ⇒**Manual VPN**.
The Manual VPN page opens.

3 Click **Add**.
The Add Gateway page opens.

4 Configure the gateway.
See "Setting Up Multiple SOHO 6 to SOHO 6 VPN Tunnels" on page 95 for information about the Add Gateway page.

5 Type the network IP address of the local network and remote networks in the applicable fields.

6 Click **Submit**.

Using MUVPN Clients

The MUVPN Clients upgrade allows remote users to connect to the SOHO 6 through a secure (IPSec) VPN tunnel. The remote user gains access to the local trusted network and the networks connected by VPN tunnels to the local SOHO 6. The SOHO 6 also allows users on the trusted network to access the networks connected by VPN tunnels to the local SOHO 6. If you purchase the VPNforce Port upgrade, you also receive one MUVPN connection to the optional network. Additional VPNforce Port user licenses can be purchased.

Viewing the VPN Statistics

The SOHO 6 has a configuration page that displays VPN statistics. Use this page to monitor VPN traffic and to solve problems with the VPN configuration.

To view the VPN Statistics page:

1. Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
   The default IP address is: http://192.168.111.1
2. From the navigation bar at left, select **VPN ⇒VPN Statistics**.
   The VPN Statistics page opens.

Frequently Asked Questions

Why do I need a static external address?

To make a VPN connection, each of the appliances must know the IP address of the other appliance. If the addresses are dynamic, these addresses can change. A changing address prevents a connection between the two appliances. However, this issue can be resolved by using Dynamic DNS. For information on configuring the Dynamic DNS feature, see “Configuring the Dynamic DNS Service” on page 42.

How do I get a static external IP address?

The external IP address for your computer or network is assigned by your ISP. Many ISPs use dynamic IP addresses so that their network is easier to configure and to make the connection of a Web server to their network more difficult. Most ISPs supply a static IP address as an optional service.

How do I troubleshoot the connection?

If you can ping the remote SOHO 6 and the computers on the remote network, the VPN tunnel functions correctly. The configuration of the network software or the applications are possible causes of other problems.

Why is ping not working?

If you cannot ping the local network address of the remote SOHO 6, follow these steps:

1 Ping the external address of the remote SOHO 6.

For example, at Site A, ping 68.130.44.15 (Site B). If the ping does not come back, make sure the external network settings of Site B are correct. If the settings are correct, make sure that the computers at Site B have access to the Internet. If this procedure does not give a solution, speak to a service person at your ISP.

2 If you can ping the external address of each SOHO 6, try to ping a local address in the remote network.

From Site A, ping 192.168.111.1. If the VPN tunnel functions correctly, the remote SOHO 6 sends the ping back. If the ping does not come back, make sure the local settings are correct. Make sure that the local DHCP address ranges for the two networks connected by the VPN tunnel do not use any of the same IP addresses. The two networks connected by the tunnel must not use the same IP addresses.

How do I obtain a VPN upgrade license key?

You can purchase a license key for an upgrade from the WatchGuard Web site:

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

How do I enable a VPN tunnel?

The instructions to help you enable a VPN tunnel are available from the WatchGuard Web site:

https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

CHAPTER 10 MUVPN Clients

The MUVPN client is a software application that is installed on a remote computer. This application makes a secure connection from the remote computer to your protected network through an unsecured network. The MUVPN client uses Internet Protocol Security (IPSec) to guarantee the security of the connection.

The following is an example of how the MUVPN client can be used. First, the MUVPN client is installed on the remote computer. Then a connection to the Internet is established on the remote computer. The user starts the MUVPN client, which creates an encrypted tunnel to the SOHO 6. The SOHO 6 connects the user to the trusted network. The employee now has remote access to the internal network and does not compromise the security of the network. You do not need a successful connection on the external interface to create MUVPN connections.

ZoneAlarm®, a personal firewall software application, is included as an optional feature with the MUVPN client. ZoneAlarm provides additional security for the remote users of your network by acting as a software firewall.

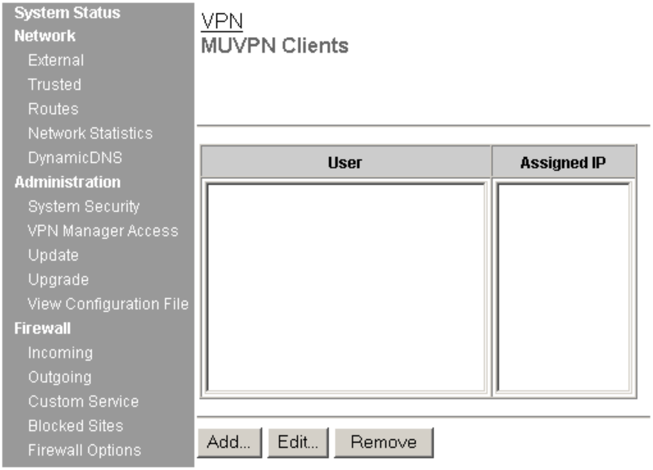
This chapter shows how to install and configure the MUVPN client on a remote computer. This chapter also includes information about the features of the ZoneAlarm personal firewall.

Configuring the SOHO 6 for MUVPN Clients

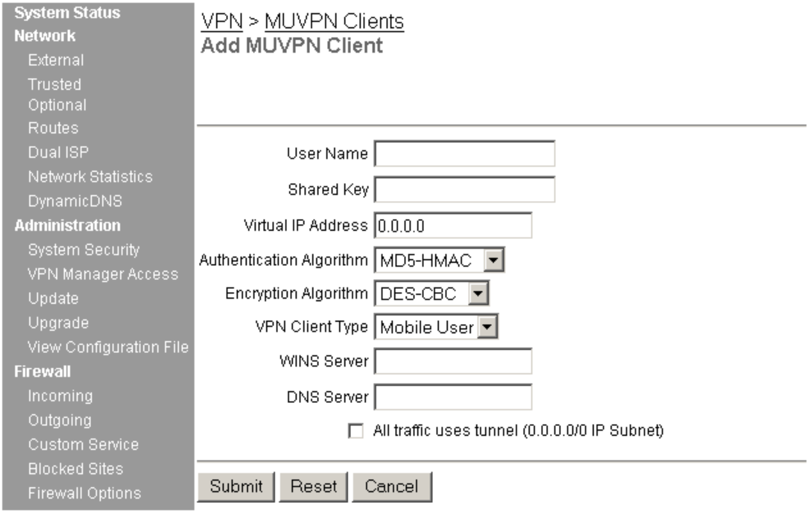
Follow these steps to configure your SOHO 6 for MUVPN clients:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default trusted IP address is 192.168.111.1

2 From the navigation bar at left, select **VPN** ⇒**MUVPN Clients**.
The MUVPN Clients page appears.



3 Click **Add**.
The Add MUVPN Client page appears.



VPN > MUVPN Clients

Add MUVPN Client

User Name	
Shared Key	
Virtual IP Address	0.0.0.0
Authentication Algorithm	MD5-HMAC
Encryption Algorithm	DES-CBC
VPN Client Type	Mobile User
WINS Server	
DNS Server	

□ All traffic uses tunnel (0.0.0.0/0 IP Subnet)

4 Type a user name and a shared key in the applicable fields.

The user name is used as the e-mail address and the passphrase is used as the pre-shared key for the MUVPN client.

5 Type the virtual IP address in the applicable field.

The virual IP address is the same as the IP address on the Trusted Network Configuration page. This address is used by the remote computer to connect to the SOHO 6.

6 From the **Authentication Algorithm** drop-down list, select the type of authentication.

The options are MD5-HMAC and SHA1-HMAC.

7 From the **Encryption Algorithm** drop-down list, select the type of encryption.

The options are DES-CBC and 3DES-CBC.

8 Select **Mobile User** from the **VPN Client Type** drop-down list.

9 Click **Submit**.

Preparing the Remote Computers to Use the MUVPN Client

The MUVPN client is only compatible with Windows operating systems. The MUVPN client can only be installed on computers that meet these system requirements:

System requirements

- A computer with a Pentium processor (or equivalent)
- Compatible operating systems and minimum RAM:
    - Microsoft Windows 98: 32 MB
    - Microsoft Windows ME: 64 MB
    - Microsoft Windows NT 4.0 Workstation: 32 MB
    - Microsoft Windows 2000 Professional: 64 MB
    - Microsoft Windows XP: 64 MB
- The latest service packs for each operating system are recommended, but not required
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Microsoft Internet Explorer 5.0 or later
- An Internet service provider account
- A dial-up or broadband (DSL or cable modem) connection

To use Windows file and print sharing through a MUVPN tunnel, the remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the SOHO 6. To communicate with these servers, the remote computer must have the proper Windows components installed and configured.

NOTE

You cannot use the MUVPN virtual adapter. Make sure this is disabled.

Windows 98/ME operating system setup

This section describes how to install and configure the network components that are required for the Windows 98/ME operating system. These components must be installed before the MUVPN client will function correctly on a Windows 98/ME computer.

NOTE

The Mobile User VPN Adapter supports L2TP.

Configuring network names

From the Windows desktop:

1 Select **Start** ⇒**Settings** ⇒**Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Make sure the Client for Microsoft Networks is installed.
The Client for Microsoft Networks must be installed before you continue with this procedure. For instructions, see "Installing the Client for Microsoft Networks" on page 110.

4 Click the **Identification** tab.

5 Type a name for the remote computer in the applicable field.
This name must be unique on the remote network.

6 Type the domain name for this connection in the applicable field.

7 Enter a description for the remote computer in the applicable field.
This step is optional.

8 Click **OK** to close the Network window.
Click Cancel if you do not want to save the changes.

9 Reboot the computer.

Installing the Client for Microsoft Networks

The Client for Microsoft Networks must be installed before you can configure network names. If the Client for Microsoft Networks is not installed, follow these steps.

From the Network window:

1 Click the **Configuration** tab and then click **Add**.
The Select Network Component Type window appears.

2 Select **Client** and then click **Add**.
The Select Network Client window appears.

3 Select **Microsoft** from the list at left. Select **Client for Microsoft Networks** from the list at right and then click **OK**.

4 Select **Client for Microsoft Networks** and then click **Properties**.

5 Select the **Log on to Windows NT domain** checkbox.

6 Type the domain name in the **Windows NT Domain** text field.
Examples of typical domain names are "sales", "office", and "warehouse".

7 Select the **Logon and Restore Network Connections** checkbox.

Installing Dial-Up Networking

Dial-Up Networking must be installed before the Mobile User VPN Adapter can be installed. If Dial-up Networking is not installed, follow these steps.

From the Windows desktop:

1 Select **Start** ⇒**Settings** ⇒**Control Panel**.

2 Double-click the **Add/Remove Programs** icon.
The Add/Remove Properties window appears.

3 Click the **Windows Setup** tab.

The Windows Setup dialog box appears. The operating system searches for installed components.

4 Select the **Communications** checkbox and then click **OK**.

The Copying Files dialog box appears. The operating system copies the necessary files.

5 The Dial-Up Networking Setup window appears. Click **OK** to restart the computer.

The computer reboots.

The Dial-up Networking component of Windows 98 must be updated with the 1.4 patch. This update is available from the Microsoft Web site.

Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the SOHO 6.

From the Windows desktop:

1 Select **Start** ⇒**Settings** ⇒**Control Panel**.

2 Double-click the **Network** icon.

The Network window appears.

3 Select the network component **TCP/IP** ⇒**Dial-Up Adapter** and then click **Properties**.

The TCP/IP Properties Information window appears.

4 Click **OK**.

5 Click the **DNS Configuration** tab and then select the **Enable DNS** checkbox.

6 Type the IP address of the DNS server in the **DNS Server Search Order** text field. Click **Add**.

If you have multiple remote DNS servers, repeat steps 5 and 6.

NOTE

The DNS server on the private network behind the SOHO 6 must be the first server in the list.

7 Click the **WINS Configuration** tab and then select the **Enable WINS Resolution** checkbox.

8 Type the IP address of the WINS server in the **WINS Server Search Order** text field and then click **Add**.

If you have multiple remote WINS servers, repeat steps 7 and 8.

9 Click **OK** to close the TCP/IP Properties window. Click **OK** to close the Network window.

The System Settings Change dialog box appears.

10 Click **Yes** to restart the computer.

The computer reboots.

Windows NT operating system setup

This section describes how to install and configure the network components that are required for the Windows NT operating system. These components must be installed before the MUVPN client will function correctly on a Windows NT computer.

NOTE

The Mobile User VPN Adapter supports L2TP.

Installing Remote Access Services on Windows NT

Remote Access Services (RAS) must be installed before the Mobile User VPN Adapter can be installed. If RAS is not installed, follow these steps.

Follow the Windows desktop:

1 Select **Start** ⇒**Settings** ⇒**Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Click the **Services** tab and then click **Add**.

4 Select **Remote Access Services** from the list and then click **OK**.

5 Enter the path to the Windows NT install files or insert your system installation CD and then click **OK**.
The Remote Access Setup window appears.

6 Click **Yes** to add a RAS device, such as a modem, and then click **Add**.

7 Complete the Install New Modem wizard.

NOTE

If there is no modem installed, you can select the **Don't detect my modem; I will select it from a list** checkbox. Select the standard 28800 modem. To install RAS, Windows NT requires at least one RAS device, such as a modem, to be installed. If a modem is not available, **a serial cable between two computers** can be selected.

8 Select the modem added in the previous step from the Add RAS Device window.

9 Click **OK**, click **Continue** and then click **Close**.

10 Reboot the computer.

Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the SOHO 6.

From the Windows desktop:

1 Select **Start** ⇒**Settings** ⇒**Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Click the **Protocols** tab and then select the **TCP/IP** protocol.

4 Click **Properties**.
The Microsoft TCP/IP Properties window appears.

5 Click the **DNS** tab and then click **Add**.

6 Enter the IP address of your DNS server in the applicable field.
To add additional DNS servers, repeat steps 5 and 6.

NOTE

The DNS server on the private network behind the SOHO 6 must be the first server in the list.

7 Click the **WINS Address** tab, type the IP address of your WINS server in the applicable field, and then click **OK**.
To add additional WINS servers, repeat this step.

8 Click **Close** to close the Network window.
The Network Settings Change dialog box appears.

9 Click **Yes** to restart the computer.
The computer reboots.

Windows 2000 operating system setup

This section describes how to install and configure the network components that are required for the Windows 2000 operating system. These components must be installed before the MUVPN client will function correctly on a Windows 2000 computer.

From the Windows desktop:

1 Select **Start** ⇒**Settings** ⇒**Network and Dial-up Connections**.

2 Select the dial-up connection you use to access the Internet.
The connection window appears.

3 Click **Properties** and the click the **Networking** tab.

4 Make sure the following components are installed and enabled:

- Internet Protocol (TCP/IP)

- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) network component

From the connection window, Networking tab:

1. Click **Install**.
   The Select Network Component Type window appears.
2. Double-click the **Protocol** network component.
   The Select Network Protocol window appears.
3. Select the **Internet Protocol (TCP/IP)** network protocol and then click **OK**.

Installing the File and Printer Sharing for Microsoft Networks

From the connection window, Networking tab:

1. Click **Install**.
   The Select Network Component Type window appears.
2. Double-click the **Services** network component.
   The Select Network Service window appears.
3. Select the **File and Printer Sharing for Microsoft Networks** network service and then click **OK**.

Installing the Client for Microsoft Networks

From the connection window, Networking tab:

1. Click **Install**.
   The Select Network Component Type window appears.
2. Double-click the **Client** network component.
   The Select Network Protocol window appears.
3. Select the **Client for Microsoft Networks** network client and then click **OK**.

Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the SOHO 6.

From the connection window, Networking tab:

1 Select the **Internet Protocol (TCP/IP)** component and then click **Properties**.

The Internet Protocol (TCP/IP) Properties window appears.

2 Click **Advanced**.

The Advanced TCP/IP Settings window appears.

3 Click the **DNS** tab and then, from the section labeled **DNS server addresses, in order of use**, click **Add**.

The TCP/IP DNS Server window appears.

4 Enter the IP address of the DNS server in the applicable field and then click **Add**.

To add additional DNS servers, repeat steps 3 and 4.

NOTE

The DNS server on the private network behind the SOHO 6 must be the first server in the list.

5 Select the **Append these DNS suffixes (in order)** checkbox and then click **Add**.

The TCP/IP Domain Suffix window appears.

6 Enter the Domain suffix in the applicable field.

To add additional DNS suffixes, go back to step 5.

7 Click the **WINS** tab and then, from the section labeled **WINS addresses, in order of use**, click **Add**.

The TCP/IP WINS Server window appears.

8 Enter the IP address of the WINS server in the applicable field and then click **Add**.

To add additional WINS servers, repeat steps 7 and 8.

9 Click **OK** to close the Advanced TCP/IP Settings window, click **OK** to close the Internet Protocol (TCP/IP) Properties window, and then click **OK**.

10 Click **Cancel** to close the connection window.

Windows XP operating system setup

This section describes how to install and configure the network components that are required for the Windows XP operating system. These components must be installed before the MUVPN Client will function correctly on a Windows XP computer.

From the Windows desktop:

1 Select **Start** ⇒**Control Panel**
The Control Panel window appears.

2 Double-click the **Network Connections** icon.

3 Double-click the connection you use to access the Internet.
The connection window appears.

4 Click **Properties** and then click the **Networking** tab.

5 Make sure the following components are installed and enabled:

- Internet Protocol (TCP/IP)
- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) Network Component

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Protocol** network component.
The Select Network Protocol window appears.

3 Select the **Internet Protocol (TCP/IP)** network protocol and then click **OK**.

Installing the File and Printer Sharing for Microsoft Networks

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Services** network component.
The Select Network Service window appears.

3 Select the **File and Printer Sharing for Microsoft Networks** network service and then click **OK**.

Installing the Client for Microsoft Networks

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Client** network component.
The Select Network Protocol window appears.

3 Select the **Client for Microsoft Networks** network client and then click **OK**.

Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the SOHO 6.

From the connection window, Networking tab:

1 Select the **Internet Protocol (TCP/IP)** component.

2 Click **Properties**.
The Internet Protocol (TCP/IP) Properties window appears.

3 Click **Advanced**.

The Advanced TCP/IP Settings window appears.

4 Click the **DNS** tab and then, from the section labeled **DNS server addresses, in order of use**, click **Add**.

The TCP/IP DNS Server window appears.

5 Enter the IP address of the DNS server in the applicable field and then click **Add**.

To add additional DNS servers, repeat steps 4 and 5.

NOTE

The DNS server on the private network behind the SOHO 6 must be the first server in the list.

6 Select the **Append these DNS suffixes (in order)** checkbox and then click **Add**.

The TCP/IP Domain Suffix window appears.

7 Enter the domain suffix in the applicable field.

To add additional DNS suffixes, go back to step 6.

8 Click the **WINS** tab and then, from the section labeled **WINS addresses, in order of use**, click **Add**.

The TCP/IP WINS Server window appears.

9 Enter the IP address of the WINS server in the applicable field and then click **Add**.

To add additional WINS servers, repeat steps 8 and 9.

10 Click **OK** to close the Advanced TCP/IP Settings window, click **OK** to close the Internet Protocol (TCP/IP) Properties window, and then click **OK**.

11 Click **Cancel** to close the connection window.

Installing and Configuring the MUVPN Client

The MUVPN installation files are available at the WatchGuard Web site:

http://www.watchguard.com/support

NOTE

To install and configure the MUVPN client, you must have local administrator rights on the remote computer.

Installing the MUVPN client

Follow these steps to install the MUVPN client:

1 Copy the MUVPN installation file to the remote computer.

2 Double-click the MUVPN installation file to start the InstallShield wizard.

If you accidentally skip a step, click cancel and start the installation again.

3 Click **Next**.

If the InstallShield stops because read-only files are detected, click Yes to continue the installation.

4 A welcome message is displayed. Click **Next**.

The Software License Agreement is displayed.

5 Click **Yes** to accept the terms of the License Agreement.

The Setup Type window appears.

6 Select the type of installation. WatchGuard recommends that you use the Typical installation. Click **Next**.

7 On a Windows 2000 computer, the InstallShield will detect the Windows 2000 L2TP component. If the component is installed, the InstallShield does not install it again. Click **OK** to continue.

The Select Components window appears.

8 Do not change the default selections. Click **Next**.

The Start Copying Files window appears.

9 Click **Next** to install the files.

When the `dni_vapmp` file is installed, a command prompt window appears. This is normal. When the file has been installed, the command prompt window will close and the process will continue.

10 When the InstallShield wizard is complete, click **Finish**.

11 The InstallShield wizard searches for a user profile file. Click **Next** to skip this step. The user profile file does not need to be installed.

An information dialog box appears.

12 Click **OK** to continue the installation.

13 The installation of the MUVPN client is complete. Make sure the option **Yes, I want to restart my computer now** is selected. Click **Finish**.

The computer reboots.

NOTE

The ZoneAlarm personal firewall may prevent the connection to the network after the computer is restarted. If this occurs, log on to the computer locally the first time after installation. For more information regarding ZoneAlarm, see "The ZoneAlarm Personal Firewall" on page 139.

Configuring the MUVPN client

When the computer restarts, the WatchGuard Policy Import window opens. Click **Cancel**.

From the Windows desktop system tray:

1 Right-click the MUVPN client icon and then select **Activate Security Policy**.

2 Double-click the MUVPN client icon.

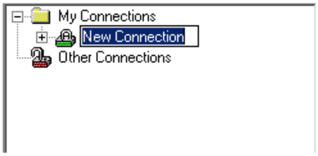
The Security Policy Editor window appears.

NOTE

The ZoneAlarm personal firewall may display alert messages. For more information regarding ZoneAlarm see "The ZoneAlarm Personal Firewall" on page 139.

3 Select **Edit** ⇒**Add** ⇒**Connection**.

A **New Connection** appears in the Network Security Policy field at left. The Connection Security, Remote Party Identity, and Addressing settings appear at right.



4 Type a unique name for the new connection.

If this will be a unique policy for a specific user, enter a unique name to identify the policy. For example, you may want to include the name of the user.

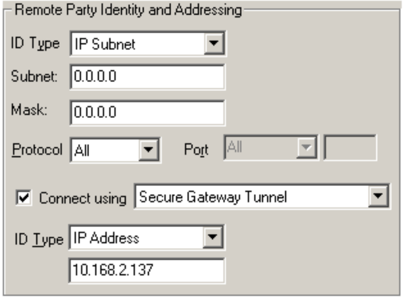
5 Select the **Secure** option.

This is the default setting.

6 Select the **Only Connect Manually** checkbox.

7 Select the **IP Subnet** option from the **ID Type** drop-down list.

The Remote Party Identity and Addressing fields are updated.



Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 0.0.0.0

Mask: 0.0.0.0

Protocol: All　Port: All

☑ Connect using: Secure Gateway Tunnel

ID Type: IP Address

10.168.2.137

8 When you set the **Subnet** and **Mask** addresses, you define whether or not an MUVPN user can access the Internet through the tunnel. If you want to access only the Trusted network, type the trusted network address in both the **Subnet** and **Mask** fields. If you want to access both the Trusted network and the Internet, type 0.0.0.0 in both the **Subnet** and **Mask** fields.

NOTE

The addresses you type in the Subnet and Mask fields must be identical to the Virtual IP Address you typed on the Add MUVPN Client page. See "Configuring the SOHO 6 for MUVPN Clients" on page 106.

9 Select **All** from the **Protocol** drop-down list.
This is the default setting.

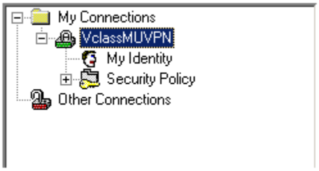
10 Select the **Connect using** checkbox and then select **Secure Gateway Tunnel** from the **Connect using** drop-down list.

11 Select **IP Address** from the **ID Type** drop-down list and then type the IP address of the external interface in the applicable field.

Defining the My Identity settings

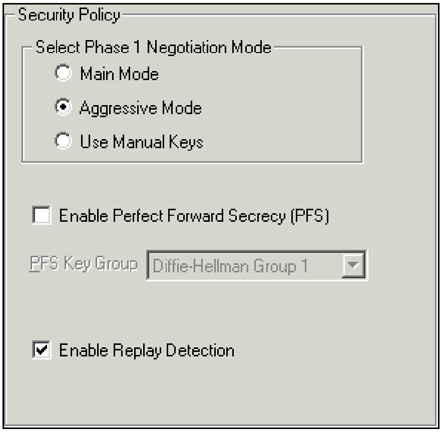
To define the My Identity settings, follow these steps.

1. Expand the **Network Security Policy** to display the new entry.
   The My Identity and Security Policy entries appear.



My Connections
VclassMUVPN
My Identity
Security Policy
Other Connections

2. Select **Security Policy**.
   The Security Policy dialog box appears.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

● Aggressive Mode

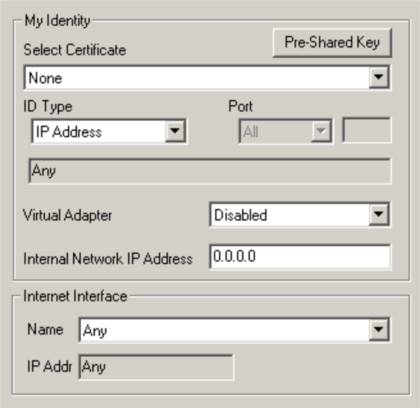
○ Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

☑ Enable Replay Detection

3. Select **Aggressive Mode**. Make sure the **Enable Perfect Forward Secrecy (PFS)** checkbox is clear and the **Enable Replay Detection** checkbox is selected.
4. Close the Security Policy dialog box.
5. Select **My Identity**.
   The My Identity and Internet Interface settings appear to the right.



My Identity

Select Certificate: None

Pre-Shared Key

ID Type: IP Address

Port: All

Any

Virtual Adapter: Disabled

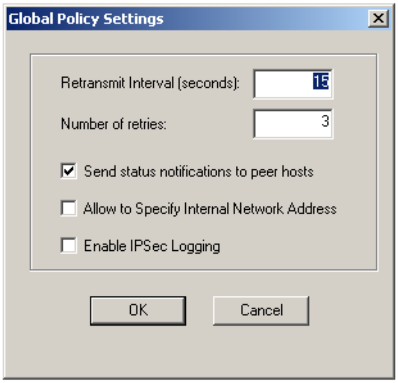
Internal Network IP Address: 0.0.0.0

Internet Interface

Name: Any

IP Addr: Any

6 Select **Options** ⇒**Global Policy Settings**.
The Global Policy Settings window appears.



Global Policy Settings

Retransmit Interval (seconds): 15

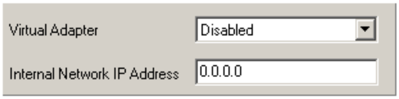
Number of retries: 3

☑ Send status notifications to peer hosts

☐ Allow to Specify Internal Network Address

☐ Enable IPSec Logging

7 Select the **Allow to Specify Internal Network Address** checkbox and then click **OK**.
The Internal Network IP Address field appears in the My Identity section.



Virtual Adapter: Disabled

Internal Network IP Address: 0.0.0.0

8 Select **None** from the **Select Certificate** drop-down list.

9 Select **E-mail Address** from the **ID Type** drop-down list and then enter the user name defined on the SOHO 6 in the applicable field.

10 Select **Disabled** from the **Virtual Adapter** drop-down list.

11 Type `0.0.0.0` in the **Internal Network IP Address** field if this value does not appear by default.

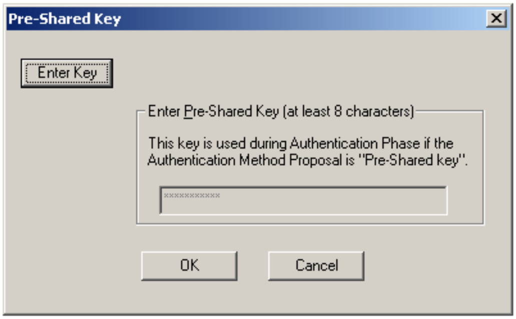
The default value is `0.0.0.0`.

12 Select **Any** from the **Name** drop-down list.

This is the default setting.

13 Click **Pre-Shared Key**.

The Pre-Shared Key dialog box appears.



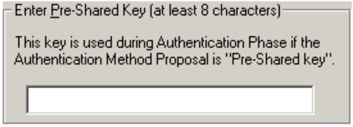
Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

xxxxxxxxxxxx

14 Click **Enter Key**.

The text field is enabled.



Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

15 Type the exact text of the MUVPN client passphrase entered on the SOHO 6 and then click **OK**.

NOTE

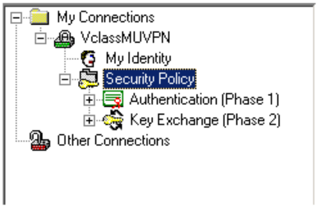
Both the pre-shared key and the e-mail address must exactly match the system passphrase and system administrator name settings of the SOHO 6. If they do not match, the connection will fail.

Defining Phase 1 and Phase 2 settings

Follow these steps to define the Phase 1 and Phase 2 settings. These values must match the settings of the SOHO 6.

1 From the **Network Security Policy** field, expand **Security Policy**.

Both Phase 1 and Phase 2 negotiations appear.

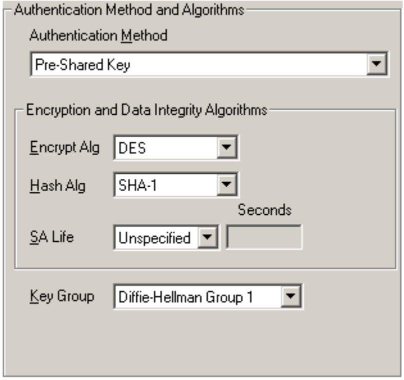


2 Expand **Authentication (Phase 1)**.

A Proposal entry appears.

3 Select **Proposal 1**.

The Authentication Method and Algorithms settings appear to the right.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: DES

Hash Alg: SHA-1

SA Life: Unspecified, Seconds:

Key Group: Diffie-Hellman Group 1

4 Select **Pre-Shared** Key from the **Authentication Method** drop-down list.

NOTE

Phase 1 values must be as specified in the following steps. Phase 2 values must match the settings of the Firebox SOHO 6.

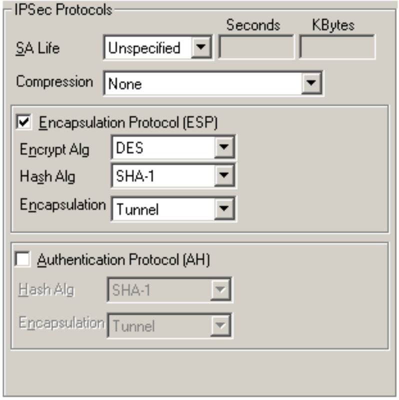
5 Select **DES** from the **Encrypt Alg** drop-down list and then select **SHA-1** from the **Hash Alg** drop-down list.

6 Select **Unspecified** from the **SA Life** drop-down list.
This is the default setting.

7 Select **Diffie-Hellman Group 1** from the **Key Group** drop-down list.

8 Expand **Key Exchange (Phase 2)**.
A Proposal entry appears.

9 Select **Proposal 1**.
The IPSec Protocols settings appear to the right.



IPSec Protocols

SA Life: Unspecified — Seconds: — KBytes:

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

10 Select **Both** from the **SA Life** drop-down list.

11 Type `86400` in the **Seconds** field and `8192` in the **KBytes** field.

12 Select **None** from the **Compression** drop-down list.
This is the default setting. The SOHO 6 does not support compression.

13 Select the **Encapsulation Protocol (ESP)** checkbox.

14 Select a value for the **Encrypt Alg** and **Hash Alg** drop-down lists.

NOTE

The encrypted and hash values must match the settings of the SOHO 6. If the settings do not match, the connection will fail.

15 Select **Tunnel** from the **Encapsulation** drop-down list.
This is the default setting.

16 Make sure the **Authentication Protocol (AH)** checkbox is not selected.

17 Select **File** ⇒**Save** or click the button shown at the right. 💾

Uninstalling the MUVPN client

Follow these directions to uninstall the MUVPN client. WatchGuard recommends that you use the Windows Add/ Remove Programs tool.

Disconnect all existing tunnels and dial-up connections. Reboot the remote computer. Perform these steps from the Windows desktop:

1 Select **Start ⇒Settings ⇒Control Panel.**

The Control Panel window appears.

2 Double-click the **Add/Remove Programs** icon.

The Add/Remove Programs window appears.

3 Select **Mobile User VPN** and then click **Change/Remove**.

The InstallShield wizard appears.

4 Select **Remove** and then click **Next**.

The Confirm File Deletion dialog box appears.

5 Click **OK** to remove all of the components.

When the `dni_vapmp` file is removed, a command prompt window appears. This is normal. When the file has been removed, the command prompt window will close and the process will continue.

The Uninstall Security Policy dialog box appears.

6 Click **Yes** to delete the Security Policy Personal Certificates and the Private/Public Keys.

The InstallShield Wizard window appears.

7 Select the **Yes, I want to restart my computer now**. Click the **Finish** option.

The computer will reboot.

NOTE

The ZoneAlarm personal firewall settings are stored in the following directories by default.

Windows 98: `c:\windows\internet logs\`
Windows NT and 2000: `c:\winnt\internet logs\`
Windows XP: `c:\windows\internet logs`

To remove these settings, delete the contents of the appropriate directory.

8 When the computer has restarted, select **Start** ⇒**Programs**.

9 Right-click **Mobile User VPN** and select **Delete** to remove this selection from your Start menu.

Configuring the SOHO 6 for MUVPN Clients Using Pocket PC

In order to create a MUVPN tunnel between the SOHO 6 and your Pocket PC, you must configure the MUVPN Clients feature on the SOHO 6.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default trusted IP address is 192.168.111.1

2 From the navigation bar at left, select **VPN** ⇒**MUVPN Clients**.
The MUVPN Clients page appears.

3 Click **Add**.
The Add MUVPN Client page appears.

4 Type a user name and a shared key in the applicable fields.
The user name is used as the e-mail address and the passphrase is used as the pre-shared key for the MUVPN client.

5 Type the virtual IP address in the applicable field.

The virual IP address is the same as the IP address on the Trusted Network Configuration page. This address is used by the remote computer to connect to the SOHO 6.

6 From the **Authentication Algorithm** drop-down list, select the type of authentication.

The options are MD5-HMAC and SHA1-HMAC.

7 From the **Encryption Algorithm** drop-down list, select the type of encryption.

The options are DES-CBC and 3DES-CBC.

8 Select **Pocket PC** from the **VPN Client Type** drop-down list.

9 Click **Submit**.

For additional information about configuring your Pocket PC to serve as an MUVPN client, go to the WatchGuard Web site:

https://www.watchguard.com/support/sohoresources/soinstallhelp.asp

Connecting and Disconnecting the MUVPN Client

The MUVPN client software makes a secure connection from a remote computer to your protected network through the Internet. To establish this connection, you must connect to the Internet and use the MUVPN client to connect to the protected network.

Connecting the MUVPN client

1 Connect to the Internet through a Dial-Up Networking connection, a LAN connection, or a WAN connection.

From the Windows desktop system tray:

2 If the MUVPN client is not active, right-click the icon and select **Activate Security Policy**.

For information about how to determine the status of the MUVPN icon, see "The MUVPN client icon" on page 133.

From the Windows desktop:

3 Select **Start** ⇒**Programs** ⇒**Mobile User VPN** ⇒**Connect**.

The WatchGuard Mobile User Connect window appears.

4 Click **Yes**.

The MUVPN client icon

The MUVPN icon appears in the Windows desktop system tray. The icon image provides information about the status of the connection.

Deactivated

The MUVPN Security Policy is deactivated. This icon may appear if the Windows operating system did not start a required MUVPN service. If this occurs, the remote computer must be restarted. If the problem continues, reinstall the MUVPN client.

Activated

The MUVPN client is ready to establish a secure, MUVPN tunnel connection.

Activated and Transmitting Unsecured Data

The MUVPN client is ready to establish a secure, MUVPN tunnel connection. The red bar on the right of the icon indicates that the client is transmitting unsecured data.

Activated and Connected

The MUVPN client has established at least one secure, MUVPN tunnel connection, but is not transmitting data.

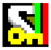
Activated, Connected and Transmitting Unsecured Data

The MUVPN client has established at least one secure, MUVPN tunnel connection. The red bar on the right of the icon indicates that the client is only transmitting unsecured data.

Activated, Connected and Transmitting Secured Data

The MUVPN client has established at least one secure, MUVPN tunnel connection. The green bar on the right of the icon indicates that the client is only transmitting secured data.

Activated, Connected and Transmitting both Secured and Unsecured Data



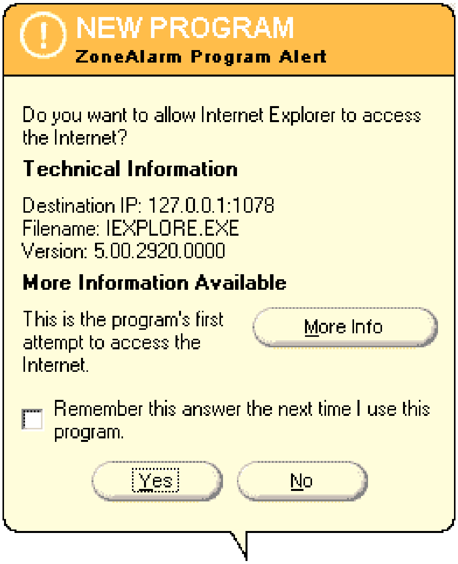
The MUVPN client has established at least one secure, MUVPN tunnel connection. The red and green bars on the right of the icon indicate that the client is transmitting both secured and unsecured data.

Allowing the MUVPN client through the personal firewall

The following programs are associated with the MUVPN client. To establish the MUVPN tunnel, you must allow these programs through the personal firewall:

- MuvpnConnect.exe
- IreIKE.exe

The personal firewall will detect when these programs attempt to access the Internet. A New Program alert window appears to request access for the MuvpnConnect.exe program.



NEW PROGRAM
ZoneAlarm Program Alert

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:1078
Filename: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

□ Remember this answer the next time I use this program.

From the New Program alert window:

1 Select the **Remember this answer the next time I use this program** checkbox and the click **Yes**.

With the option selected, the ZoneAlarm personal firewall will allow this program to access the Internet each time you attempt to make a MUVPN connection.

The New Program alert window appears to request access for the IreIKE.exe program.

2 Set the **Remember this answer the next time I use this program** check box and then click **Yes**.

With the option selected, the ZoneAlarm personal firewall will allow this program to access the Internet each time you attempt to make a MUVPN connection.

Disconnecting the MUVPN client

From the Windows desktop system tray:

1 Right-click the MUVPN client icon and then select **Deactivate Security Policy**.

The MUVPN client icon with a red bar is displayed to indicate that the transmitted data is not secure.

If the ZoneAlarm personal firewall is active, deactivate it now.

From the Windows desktop system tray:

1 Right-click the ZoneAlarm icon shown at right. ZA

2 Select **Shutdown ZoneAlarm**.

The ZoneAlarm window appears.

3 Click **Yes**.

Monitoring the MUVPN Client Connection

The Log Viewer and the Connection Monitor are installed with the MUVPN client. These tools can be used to monitor the MUVPN connection and to diagnose problems that may occur.

Using the Log Viewer

The Log Viewer displays the communications log. This log shows the events that occurred during the connection of the MUVPN tunnel.

From the Windows desktop system tray:

1 Right-click the **Mobile User VPN** client icon.

2 Select **Log Viewer**.
The Log Viewer window appears.

Using the Connection Monitor

The Connection Monitor displays statistical and diagnostic information for each active connection in the security policy. This display shows the security policy settings and the security association (SA) information. The displayed information is determined during the phase 1 IKE negotiations and the phase 2 IPSec negotiations.

From the Windows desktop system tray:

1 Right-click the **Mobile User VPN** client icon.

2 Select **Connection Monitor**.
The Connection Monitor window appears.

An icon appears to the left of the connection name:

- SA indicates that the connection only has a phase 1 SA. A phase 1 SA is assigned in the following situations:
    - for a connection to a secure gateway tunnel

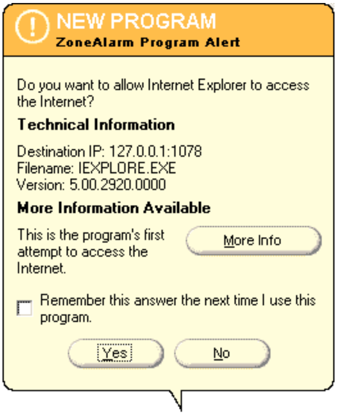
  - when a phase 2 SA connection has not yet been made
  - when a phase 2 SA connection cannot be made
- A key indicates that the connection has a phase 2 SA. This connection may also have a phase 1 SA.
- An animated black line underneath a key indicates that the client is processing secure IP traffic for the connection.
- A single SA icon with several key icons above it indicates a single phase 1 SA to a gateway that protects multiple phase 2 SAs.

The ZoneAlarm Personal Firewall

A personal firewall is a barrier between your computer and the outside world. A computer is most vulnerable at the connection points. These connection points are called ports. Without ports, your computer cannot connect to the Internet.

ZoneAlarm protects these ports by following a simple rule: Block all incoming and outgoing traffic unless you explicitly allow that traffic for trusted programs.

When you use ZoneAlarm you often see New Program alert windows similar to the following image.


NEW PROGRAM
ZoneAlarm Program Alert

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:1078
Filename: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

□ Remember this answer the next time I use this program.

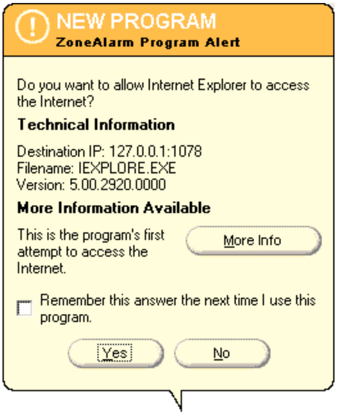
This alert appears whenever one of your programs attempts to access the Internet or your local network. This alert ensures that no information leaves your computer without your authorization.

The ZoneAlarm personal firewall provides a brief tutorial after the MUVPN client is installed. Follow the tutorial to learn how to use this program.

For more information about the features and configuration of ZoneAlarm, please refer to the ZoneAlarm help system. To access the help system, select **Start** ⇒**Programs** ⇒**Zone Labs** ⇒ **ZoneAlarm Help**.

Allowing traffic through ZoneAlarm

When an application requires access through the ZoneAlarm personal firewall, a New Program alert will be displayed on the Windows desktop. This alert tells the user which program requires access. The name of the program may not clearly indicate which application requires access.



Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:1078
Filename: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

□ Remember this answer the next time I use this program.

In the example above, the Internet Explorer Web browser application has been launched. The application attempts to access the user’s home page. The program that actually needs to pass through the firewall is “IEXPLORE.EXE”.

To allow this program access to the Internet each time the application is started, select the **Remember the answer each time I use this program** checkbox.

Here is a list of some programs that need to pass through the ZoneAlarm personal firewall when you use their associated applications.

Programs That *Must* Be Allowed	
MUVPN client	IreIKE.exe MuvpnConnect.exe
MUVPN Connection Monitor	CmonApp.exe
MUVPN Log Viewer	ViewLog.exe
Programs That *May* be Allowed	
MS Outlook	OUTLOOK.exe
MS Internet Explorer	IEXPLORE.exe
Netscape 6.1	netscp6.exe
Opera Web browser	Opera.exe
Standard Windows network applications	lsass.exe services.exe svchost.exe winlogon.exe

Shutting down ZoneAlarm

From the Windows desktop system tray:

1 Right-click the ZoneAlarm icon shown at right. ZA

2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.

3 Click **Yes**.

Uninstalling ZoneAlarm

From the Windows desktop:

1 Select **Start** ⇒**Programs** ⇒**Zone Labs** ⇒**Uninstall ZoneAlarm**.
The Confirm Uninstall dialog box appears.

2 Click **Yes**.
The ZoneLabs TrueVector service dialog box appears.

3 Click **Yes**.

The Select Uninstall Method window appears.

4 Make sure **Automatic** is selected and then click **Next**.

5 Click **Finish**.

NOTE

The Remove Shared Component window may appear. During the initial installation of ZoneAlarm, some files were installed that could be shared by other programs on the system. Click Yes to All to completely remove all of these files.

6 The Install window appears and prompts you to restart the computer. Click **OK** to reboot your system.

Troubleshooting Tips

Additional information about how to configure the MUVPN client is available from the WatchGuard Web site:

www.watchguard.com/support

The answers to several frequently asked questions about the MUVPN client are answered below.

My computer hangs immediately after installing the MUVPN client...

This problem may be caused by one of the following two problems:

- The ZoneAlarm personal firewall application is disrupting the normal traffic on the local network.
- The MUVPN client is active and is unsuccessfully attempting to create VPN tunnels.

When the MUVPN client is not in use, both ZoneAlarm and the MUVPN client should be deactivated.

From the Windows desktop system tray:

1 Reboot your computer.

1 Right-click the MUVPN client icon and then select **Deactivate Security Policy**.
The MUVPN client icon with a red bar is displayed to indicate that the Security Policy has been deactivated.

1 Right-click the ZoneAlarm icon shown at right. ZA

2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.

3 Click **Yes**.

I have to enter my network login information even when I'm not connected to the network...

When you start your computer, you are prompted to enter your Windows network user name, password and domain. It is very important that you enter this information correctly, just as you would at the office. Windows stores the information for use by network adapters and network applications. Later, when you connect to your ISP and start the MUVPN client, your computer uses the stored information to connect to the company network.

I am not prompted for my user name and password when I turn my computer on...

This is probably caused by the ZoneAlarm personal firewall application. This program is very good at what it does. ZoneAlarm keeps your computer secure from unauthorized incoming and outgoing traffic. Unfortunately, it may prevent your computer from broadcasting its network information. This prevents the transmission of the login information. Make sure you deactivate ZoneAlarm each time you disconnect the MUVPN connection.

Is the MUVPN tunnel working?

The MUVPN client icon appears in the Windows desktop system tray once the application has been launched. The MUVPN client displays a key in the icon when the client is connected.

To test the connection, ping a computer on your company network.

- Select **Start** ⇒**Run** and then type `ping` followed by the IP address of a computer on your company network.

My mapped drives have a red X through them...

Windows 98/ME, NT, and 2000 verify and map network drives automatically when the computer starts. Because you cannot establish a remote session with the company network before the computer starts, this process fails. This causes a red X to appear on the drive icons. To correct this problem, establish a MUVPN tunnel and open the network drive. The red X for that drive should disappear.

How do I map a network drive?

Due to a Windows operating system limitation, mapped network drives must be remapped when you work remotely. To remap a network drive from the Windows desktop:

1 Right-click **Network Neighborhood**.

2 Select **Map Network Drive**.
The Map Network Drive window appears.

3 Use the drop-down list to select a drive letter.
Select a drive from the drop-down list or type a network drive path.

4 Click **OK**.

The mapped drive appears in the My Computer window. Even if you select the **Reconnect at Logon** checkbox, the mapped drive will only appear the next time you start your computer if the computer is directly connected to the network.

I am sometimes prompted for a password when I am browsing the company network...

Due to a Windows networking limitation, remote user virtual private networking products can allow access only to a single network domain. If your company has multiple networks connected together, you will only be able to browse your own domain. If you try to connect to other domains, a password prompt will appear. Unfortunately, even providing the correct information will not allow you to access these additional networks.

It takes a *really* long time to shut down the computer after using the MUVPN client...

If you access a mapped network drive during an MUVPN session, the Windows operating system will wait for a signal from the network before the shutdown can be completed.

I lost the connection to my ISP, and now I can't use the company network...

If your Internet connection is interrupted, the connection to the MUVPN tunnel may be lost. Follow the procedure to close the tunnel. Reconnect to the Internet. Restart the MUVPN client.

CHAPTER 11

Using VPNforce

The VPNforce^{tm} upgrade activates the SOHO 6 optional interface. The optional interface is labeled OPT on the SOHO 6 appliance. The optional interface provides remote users with a separate network, called the optional network, behind the SOHO 6. The optional network has secure access to the corporate network. The trusted network is only used for non-corporate functions.

The optional network can also be used with the MUVPN client to enforce corporate security policies.

Using VPNforce to Connect to your Corporate Network

This upgrade option provides remote users with a separate network, called the optional network, behind the SOHO 6. The optional network has secure access to the corporate network. The trusted network is only used for non-corporate functions.

NOTE

To use this upgrade option, you must access your corporate network through a VPN tunnel from the SOHO 6 to a WatchGuard Firebox appliance or other IPSec compliant appliance. For information about the VPN upgrade option, see "VPN—Virtual Private Networking" on page 91.

Configuring the Optional Network

The VPNforce upgrade activates the SOHO 6 optional interface. This upgrade option provides remote users with a separate network, called the optional network, behind the SOHO 6. The optional network has secure access to the corporate network. The trusted network is only used for non-corporate functions.

You must activate the upgrade option before you can configure the optional network on the SOHO 6. For additional information see "Activating the SOHO 6 Upgrade Options" on page 56.

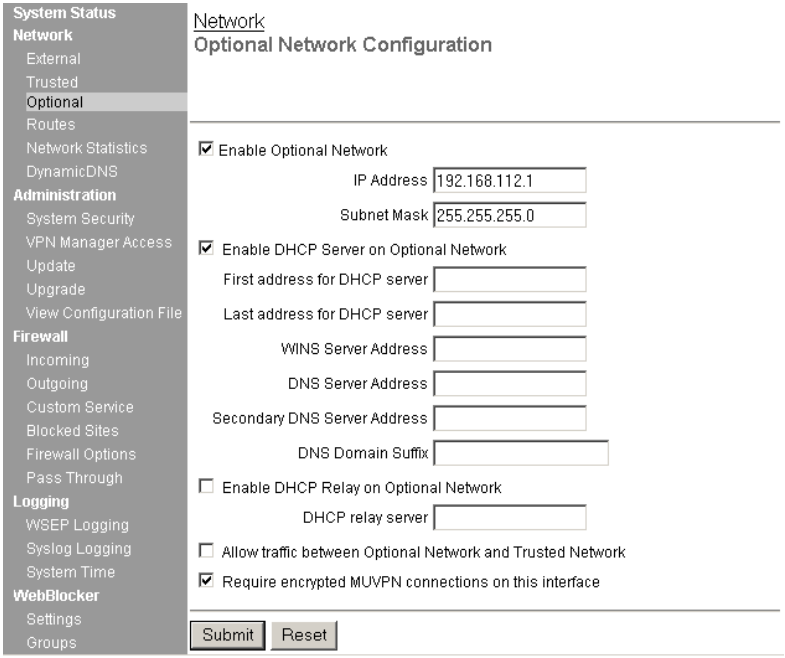
When the optional interface is activated with this upgrade, a new subnet is defined. The subnet for the optional interface is separate from the subnet for the trusted interface. By default, the subnet for the optional interface is 192.168.112.0/24.

1 With your Web browser, go to the System Status page using the IP address of the Trusted interface.

  The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Network ⇒Optional**.

  The Optional Network Configuration page appears.



Network

Optional Network Configuration

☑ Enable Optional Network

IP Address 192.168.112.1

Subnet Mask 255.255.255.0

☑ Enable DHCP Server on Optional Network

First address for DHCP server

Last address for DHCP server

WINS Server Address

DNS Server Address

Secondary DNS Server Address

DNS Domain Suffix

☐ Enable DHCP Relay on Optional Network

DHCP relay server

☐ Allow traffic between Optional Network and Trusted Network

☑ Require encrypted MUVPN connections on this interface

3 Select the **Enable Optional Network** checkbox.

4 Type the IP address and the subnet mask of the optional interface in the appropriate fields.

Make sure that this network is different from that of the trusted network.

5 To configure the DHCP server, select the **Enable DHCP Server on the Optional Network** checkbox.

6 Type the first IP address the DHCP server will hand out to computers connected to the optional network in the applicable field.

7 Type the **WINS Server Address**, **DNS Server Address** (including the **Secondary DNS Server Address** if appropriate), and **DNS Domain Suffix** in the applicable fields.

These fields are optional.

8 To configure the DHCP relay server, select the **Enable DHCP Relay checkbox**.

9 Type the IP address of the DHCP relay server in the applicable field.

10 Click **Submit.**

The SOHO 6 will send all DHCP requests to the specified, remote DHCP server and relay the resulting IP addresses to the computers connected to the optional network. If the SOHO 6 is unable to contact the specified, remote DHCP server in 30 second, it will revert to using its own DHCP server to respond to computer on the optional network.

11 To allow traffic between the Optional and Trusted network, select the **Allow traffic between Optional Network and Trusted Network** checkbox.

Enabling this option eliminates the security between the two networks.

12 Select the **Require encrypted MUVPN connections on this interface** checkbox.

13 Click **Submit**.

The page refreshes and you are prompted to reboot the SOHO 6 to activate the changes.

14 Click **Reboot**.

15 Connect one end of a straight-through Ethernet cable into the Ethernet port labeled OPT on the SOHO 6. Connect the other end into the uplink port of the hub.

16 Connect Ethernet cables to the uplink ports of the hub and to the Ethernet ports of each of your computers.

Using VPNforce and the MUVPN Client Upgrades to Enforce Your Corporate Policy

If you want to require remote users to use the MUVPN client to connect to the protected network, you must perform the procedures in this section. These procedures will also allow you to enforce your corporate security policies for remote users. The first procedure describes how to configure the SOHO 6. The second procedure describes how to configure the MUVPN clients.

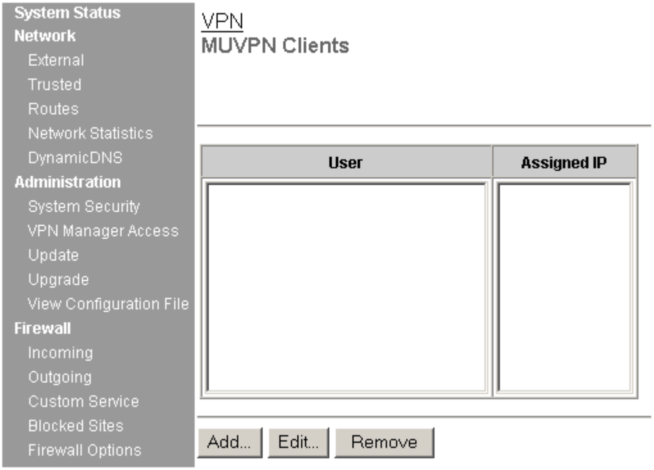
You must activate the upgrade option before you can configure the MUVPN clients on the SOHO 6. For additional information see "Activating the SOHO 6 Upgrade Options" on page 56.

Configuring the SOHO 6

Follow these steps to configure your SOHO 6:

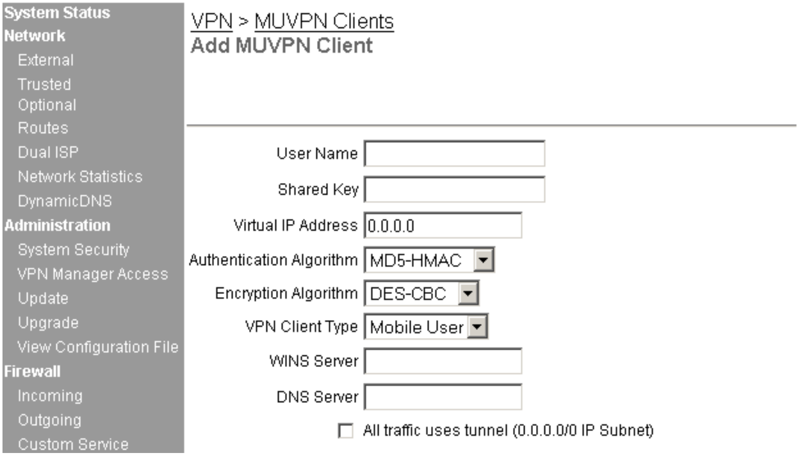
1 With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **VPN** ⇒**MUVPN Clients**.
The MUVPN Clients page appears.



3 Click the **Add** button.

The Edit MUVPN Client page appears.



Add MUVPN Client

User Name	
Shared Key	
Virtual IP Address	0.0.0.0
Authentication Algorithm	MD5-HMAC
Encryption Algorithm	DES-CBC
VPN Client Type	Mobile User
WINS Server	
DNS Server	

☐ All traffic uses tunnel (0.0.0.0/0 IP Subnet)

4 Type a user name and a passphrase in the applicable fields.

The user name is used as the e-mail address and the passphrase is used as the pre-shared key for the MUVPN client.

5 Type an unused IP address from the trusted network, which will be used by the MUVPN client computer when connecting to the SOHO 6 in the **Virtual IP Address** field.

6 Select **MD5-HMAC** from the **Authentication Algorithm** drop list.

7 Select **DES-CBC** from the **Encryption Algorithm** drop list.

8 Select **Mobile User** from the **VPN Client Type** drop list.

9 Select the **All traffic uses tunnel (0.0.0.0/0 Subnet)** checkbox.

10 Click **Submit**.

The page refreshes and you are prompted to reboot the SOHO 6 to activate the changes.

11 Click **Reboot**.

12 Connect one end of a straight-through Ethernet cable into the Ethernet port labeled OPT on the SOHO 6. Connect the other end into the uplink port of the hub.

13 Connect Ethernet cables to the uplink ports of the hub and to the Ethernet ports of each of your computers.

Configuring the MUVPN client

Before configuring the MUVPN client, you must first install it on your computer. For information on installing the client, see “Installing and Configuring the MUVPN Client” on page 120.

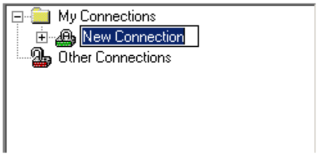
Follow these procedures to create a MUVPN security policy:

1 Right-click the MUVPN client icon and select **Security Policy Editor**.

The Security Policy Editor dialog box appears.

2 Select **Edit** ⇒**Add** ⇒**Connection**.

A New Connection appears in the Network Security Policy field on the left side and the and the Connection Security and Remote Party Identity and Addressing settings appear on the right side.



3 Type a unique name for the new connection.

If this will be a unique policy for a specific user, enter a unique name to help identify it. For example, you may want to include the actual name of the end user.

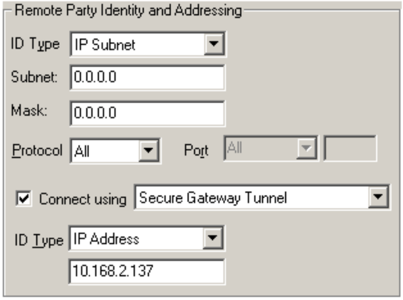
4 Select the **Secure** option.

This is the default setting.

5 Select the **Only Connect Manually** checkbox.

6 Select the **IP Subnet** option from the **ID Type** drop list.

The Remote Part Identity and Addressing settings refresh to display the appropriate fields.



Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 0.0.0.0

Mask: 0.0.0.0

Protocol: All   Port: All

☑ Connect using: Secure Gateway Tunnel

ID Type: IP Address

10.168.2.137

7 Type 0.0.0.0 in both the **Subnet** and **Mask** fields.

These are the default values.

8 Select **All** from the **Protocol** drop list.

This is the default setting.

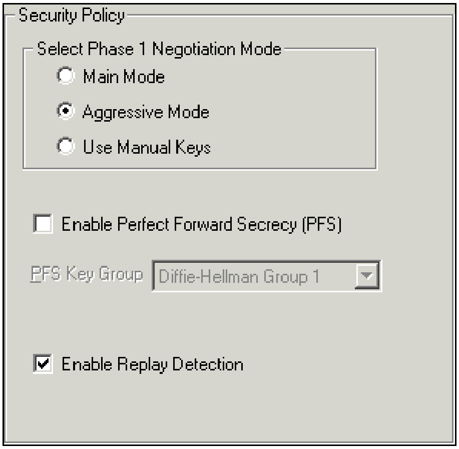
9 Select the **Connect using** checkbox and select **Secure Gateway Tunnel** from the drop list.

10 Select **IP Address** from the **ID Type** drop list and then type the IP address of the Optional interface in the available field.

Defining the Security Policy settings

Follow these instructions to define the Security Policy settings.

1 From the **Network Security Policy** field, select **Security Policy**.
The Security Policy settings appear to the right.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode
● Aggressive Mode
○ Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

☑ Enable Replay Detection

2 Select the **Aggressive Mode** option.

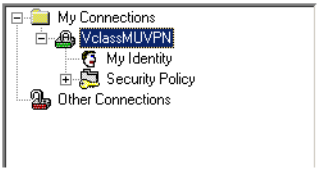
3 Verify that the **Enable Perfect Forward Secrecy (PFS)** checkbox is not selected.

4 Select the **Enable Replay Detection** checkbox.

Defining the My Identity settings

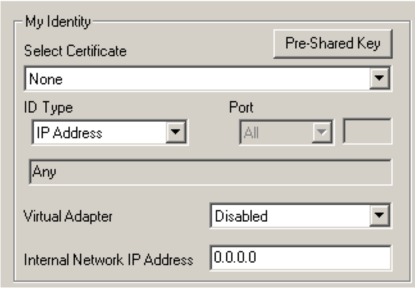
Follow these instructions to define the My Identity settings.

1 From the **Network Security Policy** field, expand the new entry.
The My Identity and Security Policy entries appear.



2 Select **My Identity**.

The My Identity and Internet Interface settings appear to the right.


My Identity

Select Certificate

None

ID Type

IP Address

Port

All

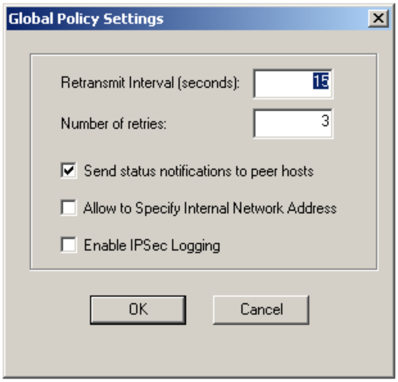
Any

Virtual Adapter: Disabled

Internal Network IP Address: 0.0.0.0

3 Select **Options** ⇒**Global Policy Settings**.

The Global Policy Settings dialog box appears.


Global Policy Settings

Retransmit Interval (seconds): 15

Number of retries: 3

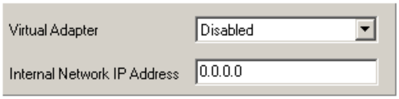
☑ Send status notifications to peer hosts

☐ Allow to Specify Internal Network Address

☐ Enable IPSec Logging

4 Select the **Allow to Specify Internal Network Address** checkbox and then click **OK**.

The Internal Network IP Address field appears among the My Identity settings.



Virtual Adapter: Disabled

Internal Network IP Address: 0.0.0.0

5 Select **None** from the **Select Certificate** drop list.

6 Select **E-mail Address** from the **ID Type** drop list and then enter the username defined on the SOHO 6 in the available field.

7 Select **Disabled** from the **Virtual Adapter** drop list.

8 Type `0.0.0.0` in the **Internal Network IP Address** field.

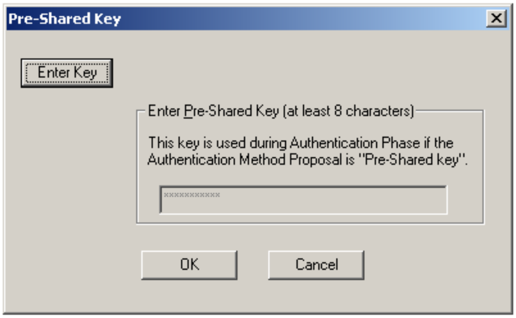
This value appears by default.

9 Select **Any** from the **Name** drop list.

This is the default setting.

10 Click **Pre-Shared Key**.

The Pre-Shared Key dialog box appears.



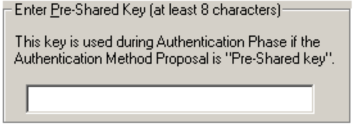
Pre-Shared Key

Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

11 Click **Enter Key**.

The text entry field is activated.



Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

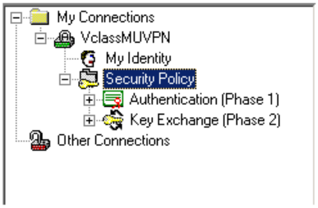
12 Type the exact text of the MUVPN client passphrase entered on the Firebox SOHO 6 appliance and then click **OK**.

Defining Phase 1 and Phase 2 settings

Follow these instructions to define the Phase 1 and Phase 2 settings. Make certain that settings match exactly with those on the Firebox SOHO 6 appliance.

1 From the **Network Security Policy** field, expand **Security Policy**.

Both Phase 1 and Phase 2 negotiations appear.

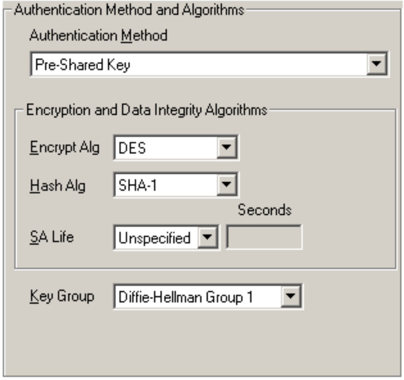


2 Expand **Authentication (Phase 1)**.

A Proposal entry appears.

3 Select **Proposal 1**.

The Authentication Method and Algorithms settings appear to the right.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: DES

Hash Alg: SHA-1

SA Life: Unspecified

Seconds:

Key Group: Diffie-Hellman Group 1

4 Select **Pre-Shared** Key from the **Authentication Method** drop list.

NOTE

These values must match exactly those entered in the Firebox SOHO 6 appliance.

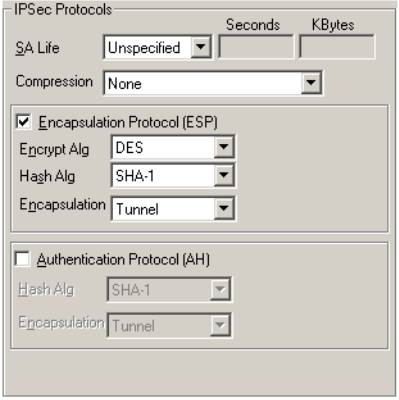
5 Select **DES** from the **Encrypt Alg** drop list and select **SHA-1** from the **Hash Alg** drop list.

6 Select **Unspecified** from the **SA Life** drop list.
This is the default setting.

7 Select **Diffie-Hellman Group 1** from the **Key Group** drop list.

8 Expand **Key Exchange (Phase 2)**.
A Proposal entry appears.

9 Select **Proposal 1**.
The IPSec Protocols settings appear to the right.



IPSec Protocols

SA Life: Unspecified (Seconds: blank, KBytes: blank)

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

10. Select **Both** from the **SA Life** drop list and then type `86400` in the **Seconds** field and `8192` in the **KBytes** field.
11. Select **None** from the **Compression** drop list.

    This is the default setting. The SOHO 6 Firebox appliance does not support compression.
12. Select the **Encapsulation (ESP)** checkbox and then select a value for the **Encrypt Alg** and **Hash Alg** drop lists.
13. Select **DES** from the **Encrypt Alg** drop list and select **MD5** from the **Hash Alg** drop list.
14. Select **Tunnel** from the **Encapsulation** drop list.

    This is the default setting.
15. Verify that the **Authentication Protocol (AH)** checkbox is *not* selected.
16. After you have finished, select **File ⇒Save** or click the button at right. 💾

Using the MUVPN client to Secure a Wireless Network

The VPNforce upgrade and the MUVPN client can also be used to prevent wireless "drive by" hacking. This configuration requires an Ethernet connection from the wireless access point (WAP) to the OPT port on the SOHO 6.

Follow these instructions to complete the configuration:

1 Identify the Ethernet cable that connects your DSL/cable modem to the WAN port of your WAP.

2 Disconnect this cable from the WAN port of your WAP.

3 Connect this cable to the WAN port of the SOHO 6.

4 Connect one end of a straight-through Ethernet cable to the OPT port of the SOHO 6.

5 Connect the other end of the straight-through Ethernet cable to one of the LAN ports of your WAP.

6 Configure your WAP as a bridge. To do so, disable the DHCP server on the LAN ports of the appliance. Refer to the user documentation of your WAP for additional information.

7 Connect an Ethernet cable from a computer to the SOHO 6 to access the configuration pages.

8 Configure the MUVPN clients upgrade on the SOHO 6 and install and configure the MUVPN client on your computers. For additional information, see “Using VPNforce and the MUVPN Client Upgrades to Enforce Your Corporate Policy” on page 151.

CHAPTER 12

Support Resources

Troubleshooting Tips

If you have problems during the installation and the configuration of your SOHO 6, refer to this information.

General

What do the PWR, Status, and Mode lights signify on the SOHO 6?

When the PWR light is lit, the SOHO 6 is connected to a power source. When the Status light is lit, there is a management connection to the SOHO 6. When the MODE light is lit, the SOHO 6 is operational.

If the PWR light *blinks*:

> The SOHO 6 is running from its backup flash memory. You can connect to the SOHO 6 from a computer attached to one of the four Ethernet ports (labeled 0-3) to configure the SOHO 6.

If the Mode light is *blinks*:

The SOHO 6 cannot connect to the external network. Possible causes of this problem include:

- The SOHO 6 did not receive an IP address for the external interface from the DHCP server.
- The WAN port is not connected to another appliance.
- The connection to the external interface is defective.
- The appliance to which the external interface of the SOHO 6 is connected is not operating correctly.

How do I register my SOHO 6 with the LiveSecurity Service?

See “Registering Your SOHO 6 and Activating the LiveSecurity Service” on page 27.

How do I restart my SOHO 6?

See “Rebootting the SOHO 6” on page 28.

How do I reset my System Security password, if I forgot or lost it?

See “Resetting the SOHO 6 to the factory default settings” on page 26.

How does the seat limitation on the SOHO 6 work?

See “Cabling the SOHO 6 for more than four appliances” on page 20.

What is a SOHO 6 feature key?

See “Activating the SOHO 6 Upgrade Options” on page 56.

I can't get a certain SOHO 6 feature to work with a DSL modem.

Some DSL routers implement NAT firewalls. An external network connection through an appliance that supplies NAT causes problems with WebBlocker and the performance of IPSec. When a SOHO 6 connects to the external network through a DSL router, set the DSL router to operate as a bridge only.

How do I install and configure the SOHO 6 using a Macintosh (or other) operating system?

The installation instructions for the Macintosh and other operating systems are available from the WatchGuard Web site:

`https://www.watchguard.com/support/sohoresources/soinstallhelp.asp`

How do I know whether the cables are connected correctly to my SOHO 6?

The front panel of the SOHO 6 has fourteen indicators. The WAN indicator shows if the SOHO 6 is connected to the modem; if this indicator is not lit, the SOHO 6 is not connected.

- Make sure that the cable is connected from the SOHO 6 to the modem.
- Make sure the Internet connection is active.

The link indicators (0-3) are for the four Ethernet ports of the trusted network. These indicators show if the SOHO 6 is connected to a computer or hub. If the indicators are not lit, the SOHO 6 is not connected to the computer or hub. Make sure that the cable is connected and the computer or hub is connected to a power supply.

I can connect to the System Status page; why can't I browse the Internet?

If you can access the configuration pages, but not the Internet, there is a problem with the connection from the SOHO 6 to the Internet.

- Make sure the cable modem or DSL modem is connected to the SOHO 6 and the power supply.
- Make sure the link light on the modem and the WAN indicator on the SOHO 6 are lit.

Speak with your ISP if the problem is not corrected.

How can I see the MAC address of my SOHO 6?

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
  The default IP address is: http://192.168.111.1

2 At the bottom of the System Status page, the External network header is shown on the right side. The MAC address or addresses are shown.
  Record these addresses before you call Technical Support.

Configuration

Where are the SOHO 6 settings stored?

The configuration parameters are stored in memory of the SOHO 6.

How do I set up DHCP on the trusted network of the SOHO 6?

1 Make sure your computer is configured to use DHCP. See "Enabling your computer for DHCP" on page 16 for additional information.

2 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

3 From the navigation bar at left, select
Network ⇒ **Trusted**.

4 Clear the **Enable DHCP Server** check box.

5 Click **Submit**.

How do I change to a static, trusted IP address?

To use a static IP address, select a network IP range and subnet mask for the trusted network.

The network IP ranges and subnet masks in the table below are reserved for private networks in compliance with RFC 1918. Replace the Xs in the network IP address with a number between 1 and 254. The subnet mask does 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, follow these steps:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select
Network ⇒ **Trusted**.

3 Select the **Enable DHCP Server** check box.

4 Click **Submit**.

5 Type the information in the applicable fields.

6 Click **Submit**.

How do I set up and disable WebBlocker?

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **WebBlocker** ⇒**Settings**.
The WebBlocker Settings page opens.

3 Select the **Enable WebBlocker** check box.

4 Type a passphrase in the **Full Access Password** field.

5 Type the number of minutes for the inactivity timeout in the applicable field.

To disable WebBlocker, clear the **Enable WebBlocker** check box.

How do I allow incoming services such as POP3, Telnet, and Web (HTTP)?

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Firewall** ⇒**Incoming**.
The Filter Incoming Traffic page opens.

3 Select the pre-configured service to allow.

4 Select **Allow** from the drop-down list.

5 Type the trusted network IP address of the computer hosting the service.

6 Click **Submit**.

How do I allow incoming IP, or uncommon TCP and UDP protocols?

Record the IP address of the computer that is to receive the incoming data and the number of the new IP protocol. Follow these steps:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the SOHO 6.
The default IP address is: http://192.168.111.1

2 From the navigation bar at left, select **Firewall** ⇒**Custom Service**.
The Custom Service page opens.

3 Beneath the **Protocol Settings** fields, select **TCP Port**, **UDP Port** or **Protocol** from the drop-down list.
The Custom Service page refreshes.

4 Type a name for the service in the **Service** field.

5 Type the new protocol number in the **Protocol** field.

6 Click **Submit**.

7 From the navigation bar at left, select **Firewall** ⇒**Incoming**.
The Firewall Incoming Traffic page opens.

8 At the bottom of the page, locate the new service under the **Custom Service** list and select **Allow** from the drop-down list.

9 Type the IP address of the computer that is to receive the incoming data in the **Service Host** field.

10 Click **Submit**.

How do I create a back up of my configuration?

It is often a good idea to back up your configuration in the event that it is corrupted or that you lose your system administrator name and passphrase. Follow these steps to create a back up of the

SOHO 6 configuration file. These steps apply to using a command prompt with Windows 2000 or XP.

1 Configure the firewall settings of the SOHO 6 to allow an incoming FTP service to the trusted IP address of the appliance.

   For information on configuring an incoming service, see Chapter 6 "Configure the Firewall Settings" on page 61.

2 Select **Start** ⇒**Programs** ⇒**Accessories** ⇒**Command Prompt**.

   A command prompt window appears.

3 At the prompt, type `ftp` and then the IP address of the trusted network.

   The default IP address is: `192.168.111.1`

4 Press **Enter**.

5 You are then prompted for the username and password. Type the system administrator name and passphrase configured on the system security page. For information on configuring the system security page, see "System security" on page 50.

   The default values are "user" and "pass".

6 Respond to the ftp prompt as follows:

   ftp> `bin`

   ftp> `get wg.cfg`

   The wg.cfg file is downloaded to the directory of the original command prompt.

   ftp> `bye`

   The original command prompt reappears.

7 Type `exit` at the prompt and then press **Enter**.

   The command prompt window closes.

VPN Management

See "What You Need" on page 91.

Make sure that the two appliances use the same encryption and authentication method.

How do I set up my SOHO 6 for VPN Manager Access?

This requires the add-on product, WatchGuard VPN Manager, which is purchased separately and used with the WatchGuard Firebox System software. Purchase VPN Manager through the WatchGuard Web site:

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

For more information on how to allow VPN Manager access to a SOHO 6, see the *VPN Guide*.

How do I set up VPN to a SOHO 6?

Information about how to configure a VPN tunnel between a SOHO 6 and another IPSec-compliant appliance is available from the WatchGuard Web site:

https://www.watchguard.com/support/AdvancedFaqs/sointerop_main.asp

1 Log in to the site.

2 Download the file you need.

3 Follow the instructions to configure your VPN tunnel.

Contacting Technical Support

(877) 232-3531	United States end-user support
(206) 521-8375	United States authorized reseller support
(360) 482-1083	International support

Online documentation and FAQs

Documentation in PDF format, tutorials, and FAQs are available on the WatchGuard Web Site:

https://support.watchguard.com/AdvancedFaqs/

Special notices

The online help system is not yet available on the WatchGuard Web site. Click on the **Help** link at the top of the System Status page to connect to the WatchGuard Product Documentation page, which has links to more information sources.

Index