

WatchGuard® Firebox® SOHO 6 MUVPN Clients Guide

SOHO 6.1



Using this Guide

To use this guide you need to be familiar with your computer's operating system. If you have questions about navigating in your computer's environment, please refer to your system user manual.

The following conventions are used in this guide.

Convention	Indication
Bold type	Menu commands, dialog box options, Web page options, Web page names. For example: "On the System Information page, select Disabled."
NOTE	Important information, a helpful tip or additional instructions.

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2002 WatchGuard Technologies, Inc. All rights reserved.
Firebox, Firebox 1000, Firebox 2500, Firebox 4500, Firebox II, Firebox II Plus, Firebox II FastVPN, Firebox III, Firebox SOHO, Firebox SOHO|tc, Firebox V100, Firebox V80, Firebox V60, Firebox V10, LiveSecurity, RapidStream, RapidCore, WatchGuard, WatchGuard Technologies, Inc., AppLock, AppLock/Web, Designing peace of mind, DVCP technology, Enforcer/MUVPN, FireChip, HackAdmin, HostWatch, LockSolid, RapidCare, SchoolMate, ServerLock, ServiceWatch, Smart Security. Simply Done., SpamScreen, Vcontroller are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

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

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

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

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

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

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

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

© 1998-2000 The OpenSSL Project. All rights reserved. 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 the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED 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 OpenSSL PROJECT OR ITS 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.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-1998 Eric Young (ey@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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 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 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 licence 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 licence [including the GNU Public Licence.]

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.
Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

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.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain 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/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED 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 RALF S. ENGELSCHALL OR HIS 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 Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

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. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED 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 APACHE SOFTWARE FOUNDATION OR ITS 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.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <<http://www.apache.org/>>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Part No

Contents

CHAPTER 1 Configure the SOHO 6	1
Redeem your SOHO 6 Upgrade Options	1
Configure the SOHO 6 for MUVPN Clients	3
CHAPTER 2 Preparation, Installation, and Connection	5
Prepare the Remote Computers	6
System requirements	6
Windows 98/ME operating system setup	7
Windows NT operating system setup	9
Windows 2000 operating system setup	11
Windows XP operating system setup	14
Install the MUVPN Client	17
Configuring the MUVPN Client	19
Uninstall the MUVPN client	23
Connect and Disconnect the MUVPN Client	24
Connecting the MUVPN Client	24
The Mobile User VPN client icon	24
Allowing the MUVPN client through the personal firewall	26
Disconnecting the MUVPN client	27
Monitor the MUVPN Client Connection	27
The Log Viewer	28

The Connection Monitor	28
CHAPTER 3 The ZoneAlarm Personal Firewall	31
ZoneAlarm Features	32
Allowing Traffic through ZoneAlarm	32
Shutting Down ZoneAlarm	34
Uninstalling ZoneAlarm	34
CHAPTER 4 Troubleshooting Tips	37
My computer is hung up just after installing the MUVPN client... ..	37
I have to enter my network log in information even when I'm not connected to the network... ..	38
I am <i>not</i> prompted for my user name and password when I turn my computer on... ..	38
Is the Mobile User VPN tunnel is working... ..	38
My mapped drives have a red X through them... ..	39
How to map a network drive	39
I sometimes get prompted for a password when I am browsing the company network... ..	39
It takes a really long time to shut down the computer after using Mobile User VPN... ..	40
I lost the connection to my ISP, and now I can't use the company network... ..	40

Configure the SOHO 6

This guide applies to both the SOHO 6™ and the SOHO 6t™—the name SOHO 6 is used to refer to both these devices throughout the guide. The only difference between them is the ability to create and use a Virtual Private Network (VPN) other than the MUVPN client. This VPN option can be added to the SOHO 6, while the SOHO 6t comes with the VPN option already installed and is used to create a Branch Office VPN tunnel between two IPsec compliant devices allowing data from an entire network rather than a single remote user.

This chapter describes how to configure a SOHO 6 for use with the WatchGuard® Mobile User VPN (MUVPN)™ client.

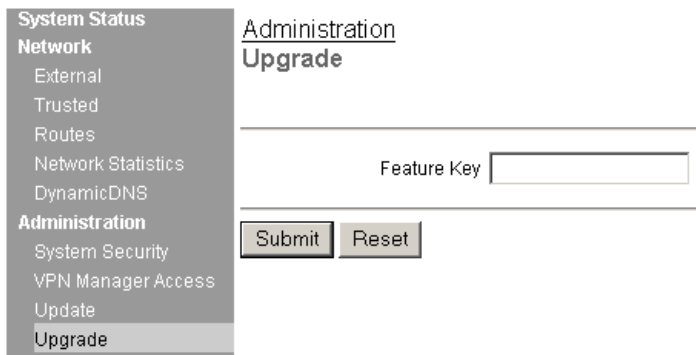
Redeem your SOHO 6 Upgrade Options

When you purchase a SOHO 6, the software for all upgrade options is provided with the unit regardless of whether you have actually purchased any of those options. The Feature Key that enables these software options is stored within the SOHO 6. Once you purchase an upgrade option and redeem it at the LiveSecurity Service Web site, you will receive a Feature Key, which you can then copy and paste into a SOHO 6 configuration page, to activate the software upgrade.

For information on registering your SOHO 6 with the LiveSecurity Service, see “Register your SOHO 6 and Activate the LiveSecurity Service” in the *Firebox SOHO 6 User Guide*.

Follow these steps to redeem your upgrade option license key:

- 1 With your Web browser, go to:
<http://www.watchguard.com/upgrade>
- 2 Click the **LiveSecurity** link at the top of the page and log into the site.
- 3 Follow the instructions provided on the site to redeem your upgrade license key.
- 4 Copy the Feature Key displayed at the LiveSecurity Service Web site.
- 5 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 6 From the navigation bar on the left side, select **Administration** ⇒ **Upgrade**.
The Upgrade page appears.



- 7 Paste the Feature Key in the appropriate field.
- 8 Click **Submit**.

Configure the SOHO 6 for MUVPN Clients

Flow 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.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 From the navigation bar on the right side, select **VPN ⇒ MUVPN Clients**.

The MUVPN Clients page appears.

The screenshot shows the MUVPN Clients configuration page. On the left is a navigation sidebar with the following items:

- System Status
- Network
 - External
 - Trusted
 - Routes
 - Network Statistics
 - DynamicDNS
- Administration
 - System Security
 - VPN Manager Access
 - Update
 - Upgrade
 - View Configuration File
- Firewall
 - Incoming
 - Outgoing
 - Custom Service
 - Blocked Sites
 - Firewall Options

The main content area is titled "VPN MUVPN Clients" and features a table with two columns: "User" and "Assigned IP". The table is currently empty. Below the table are three buttons: "Add...", "Edit...", and "Remove".

- 3 Click the **Add** button.

The Edit MUVPN Client page appears.

- 4 Enter a Username in the appropriate field.
This Username will be used as the E-mail Address when setting up the MUVPN client. In our example, Helmdog.
- 5 Enter a Passphrase in the appropriate field.
This passphrase will be used as the Pre-Shared Key when setting up the MUVPN client. In our example, pL4n3phr34k
- 6 Enter the Virtual IP address which will be used by the MUVPN computer when connecting to the SOHO 6 in the appropriate field.
In our example, 192.168.111.4.
- 7 Select the Authentication Algorithm.
In our example, SHA1-HMAC.
- 8 Select the Encryption Algorithm.
In our example, 3DECS-CBC.
- 9 From the **VPN Client Type** drop list, select Moible User.
- 10 Enable the **All traffic uses tunnel (0.0.0.0/0 Subnet)** checkbox to force all traffic from the MUVPN client to go through VPNforce IPsec tunnel.
- 11 Click the **Submit** button.

Preparation, Installation, and Connection

WatchGuard® Mobile User VPN (MUVPN)[™] client uses Internet Protocol Security (IPSec) to establish a secure connection over an unsecured network from a remote computer to your protected network.

For example, the MUVPN client is installed on an employee's computer, on the road or working from home. The employee establishes a standard Internet connection and activates the MUVPN client. The MUVPN client then creates an encrypted tunnel to your trusted network, protected behind a SOHO 6. The MUVPN client allows you to provide remote access to your internal networks without compromising security.

ZoneAlarm®, a personal firewall software application, is included as an optional feature with the MUVPN client to provide further security for your end users.

The purpose of this guide is to assist users of the SOHO 6 to set up the MUVPN client on an end-user's remote computer and to explain the features of the personal firewall.

Prepare the Remote Computers

The MUVPN client is only compatible with the Windows operating system. Every Windows system used as a MUVPN remote computer *must* have the following system requirements.

System requirements

- PC-compatible computer with 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 necessarily 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

Additionally, in order for Windows file and print sharing to occur through the MUVPN client tunnel each Windows operating system *must* have the proper components installed and configured to use the remote WINS and DNS servers on the trusted and optional networks behind the Firewall.

NOTE

You can not use the MUVPN client virtual adapter. Make sure this is disabled.

Windows 98/ME operating system setup

The following networking components *must* be configured and installed on a remote computer running Windows 98/ME in order for the MUVPN client to function properly.

Configuring networking names

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Verify that the Client for Microsoft Networks is installed.
If Client for Microsoft Networks is not installed, you *must* install it. For instructions, see the following section, "Installing the Client for Microsoft Networks".
- 3 Click the **Identification** tab.
- 4 Enter a name for the remote computer.
This *must* be a unique name on the remote network.
- 5 Enter the domain name you are connecting to.
This should be the same as the Logon to Windows NT domain value.
- 6 Enter a description for your computer (optional).
- 7 Click **OK**. Click **OK** to close and save changes to the Network control panel.
Click **Cancel** if you do not want to save any changes.
- 8 Reboot the machine.

Installing the Client for Microsoft Networks

From the Networks window:

- 1 Click the **Configuration** tab. Click **Add**.
The Select Network Component Type window appears.
- 2 Select **Client**. Click **Add**.
The Select Network Client window appears.
- 3 Select **Microsoft** from the list on the left. Select **Client for Microsoft Networks** from the list on the right. Click **OK**.
- 4 Select **Client for Microsoft Networks**.
- 5 Click **Properties**.
- 6 Enable the **Log on to Windows NT domain** option.

- 7 In the Windows NT Domain field, type the domain name.
For example, your domains might be sales, office, and warehouse.
- 8 Enable the **Logon and Restore Network Connections** option.

Installing Dial-Up Networking

The Mobile User VPN Adapter, which supports L2TP, installs only if Dial-up Networking is already installed on your computer. If Dial-up Networking is *not* installed, follow these instructions.

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Add/Remove Programs** icon.
The Add/Remove Properties window appears.
- 2 Click the **Windows Setup** tab.
The Windows Setup dialog box appears and searches for installed components.
- 3 Enable the **Communications** checkbox and click the **OK** button.
The Copying Files dialog box appears and copies the necessary files.
- 4 The Dial-Up Networking Setup dialog box appears and prompts you to restart the computer. Click the **OK** button.
The computer reboots.

Further, Windows 98 requires that the Dial-up Networking component be updated with the 1.4 patch. Please see the Microsoft Web site to receive this free update.

Configuring the WINS and DNS settings

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firewall.

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Select the network component **TCP/IP** ⇒ **Dial-Up Adapter**, then click the **Properties** button.
The TCP/IP Properties Information dialog box appears.
- 3 Click the **OK** button.
- 4 Click the **DNS Configuration** tab.
Verify that the Enable DNS option has been enabled.

- 5 Under the “DNS Server Search Order” heading, enter your DNS server IP address, then click the **Add** button.
If you have multiple remote DNS servers repeat this step.

NOTE

You *must* list the DNS server on the Private network behind the Firebox first.

- 6 Click the **WINS Configuration** tab.
- 7 Verify that the **Enable WINS Resolution option** has been enabled.
- 8 Under the “WINS Server Search Order” heading, enter your WINS server IP address, then click the **Add** button.
If you have multiple remote WINS servers repeat this step.
- 9 Click the **OK** button to close the TCP/IP Properties window.
- 10 Click the **OK** button to close the Network window.
The System Settings Change dialog box appears.
- 11 Click the **Yes** button to restart the computer and implement the changes.

Windows NT operating system setup

The following networking components *must* be installed and configured on a remote computer running Windows NT in order for the MUVPN client to function properly.

Installing Remote Access Services on Windows NT

The Mobile User VPN Adapter, which supports L2TP, installs only if the Remote Access Services (RAS) network component is already installed on the computer.

Follow the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
- 2 Select the **Services** tab.
- 3 Click the **Add** button.
- 4 Select **Remote Access Services** from the list, then click the **OK** button.

- 5 Enter the path to the Windows NT install files or insert your system installation CD, then click the **OK** button.
The Remote Access Setup dialog box appears.
- 6 Click the **Yes** button to add a RAS capable device and enable you to add a modem.
- 7 Click the **Add** button and complete the Install New Modem wizard.

NOTE

If there is no modem installed, you can enable the **Don't detect my modem; I will select it from a list** checkbox then add a Standard 28800 modem. Windows NT requires at least one RAS device such as a modem if the RAS component is installed. If no modems are available, a dial-up networking, serial cable between two computers can be selected.

- 8 Select the modem added in the last step in the Add RAS Device dialog box, then click the **OK** button.
- 9 Click the **Continue** button, then click the **Close** button.
- 10 Reboot your computer.

Configuring the WINS and DNS settings

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firebox.

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Click the **Protocols** tab.
- 3 Select the **TCP/IP** protocol and click the **Properties** button.
The Microsoft TCP/IP Properties window appears.
- 4 Click the **DNS** tab.
- 5 Click the **Add** button.
- 6 Enter your DNS server IP address in the appropriate field.
If you have multiple remote DNS servers repeat the previous three steps.

NOTE

You *must* list the DNS server on the Private network behind the Firebox first.

- 7 Click the **WINS Address** tab.
- 8 Enter your WINS server IP address in the appropriate field, then click the **OK** button.
If you have multiple remote WINS servers repeat this step.
- 9 Click the **Close** button to close the Network window.
The Network Settings Change dialog box appears.
- 10 Click the **Yes** button to restart the computer and implement the changes.

Windows 2000 operating system setup

The following networking components *must* be installed and configured on a remote computer running Windows 2000 in order for the MUVPN client to function properly.

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Select the **Networking** tab.
- 4 Verify that the following components are present and enabled:
 - Internet Protocol (TCP/IP)
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

Install these components if they are not already present.

Installing the Internet Protocol (TCP/IP) network component

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.

- 2 Click the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click the **Protocol** network component.
The Select Network Protocol window appears.
- 5 Select the **Internet Protocol (TCP/IP)** Network Protocol and then click the **OK** button.

Installing the File and Printer Sharing for Microsoft Networks

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click the **Services** network component.
The Select Network Service window appears.
- 5 Select the **File and Printer Sharing for Microsoft Networks** Network Service and then click the **OK** button.

Installing the Client for Microsoft Networks

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click the **Client** network component.
The Select Network Protocol window appears.
- 5 Select the **Client for Microsoft Networks** Network Client and then click the **OK** button.
- 6 Click the **Cancel** button to close the Select Network Component Type window.
- 7 Click the **OK** button to preserve the installed components.

- 8 Click the **Cancel** button to close the Dial-up connection window.

Configuring the WINS and DNS settings

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firebox.

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Click the **Networking** tab.
- 4 Select the **Internet Protocol (TCP/IP)** component, then click the **Properties** button.
The Internet Protocol (TCP/IP) Properties window appears.
- 5 Click the **Advanced** button.
The Advanced TCP/IP Settings window appears.
- 6 Click the **DNS** tab.
- 7 Under the “DNS server addresses, in order of use” heading, click the **Add** button.
The TCP/IP DNS Server window appears.
- 8 Enter your DNS server IP address in the appropriate field, then click the **Add** button.
If you have multiple remote DNS servers repeat the last two steps.

NOTE

You *must* list the DNS server on the Private network behind the Firebox first.

- 9 Enable the **Append these DNS suffixes (in order)** option.
- 10 Click the **Add** button.
The TCP/IP Domain Suffix window appears.
- 11 Enter your Domain suffix in the appropriate field.
If you have multiple DNS suffixes repeat the last two steps.
- 12 Click the **WINS** tab.

- 13 Under the “WINS addresses, in order of use” heading, click the **Add** button.
The TCP/IP WINS Server window appears.
- 14 Enter your WINS server IP address in the appropriate field, then click the **Add** button.
If you have multiple remote DNS servers repeat the last two steps.
- 15 Click the **OK** button to close the Advanced TCP/IP Settings window.
- 16 Click the **OK** button to close the Internet Protocol (TCP/IP) Properties window.
- 17 Click the **OK** button to close the next window.
- 18 Click the **Cancel** button again to close the Dial-up connection window.

Windows XP operating system setup

The following networking components **must** be installed and configured on a remote computer running Windows XP in order for the MUVPN client to function properly.

From the Windows desktop:

- 1 Select **Start** ⇒ **Control Panel** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Select the **Networking** tab.
- 4 Verify that the following components are present and enabled:
 - Internet Protocol (TCP/IP)
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

Install these components if they are not already present.

Installing the Internet Protocol (TCP/IP) Network Component

From the Windows desktop:

- 1 Select **Start** ⇒ **Control** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.

- 2 Click the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click the **Protocol** network component.
The Select Network Protocol window appears.
- 5 Select the **Internet Protocol (TCP/IP)** Network Protocol and then click the **OK** button.

Installing the File and Printer Sharing for Microsoft Networks

From the Windows desktop:

- 1 Select **Start** ⇒ **Control** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click the **Services** network component.
The Select Network Service window appears.
- 5 Select the **File and Printer Sharing for Microsoft Networks** Network Service and then click the **OK** button.

Installing the Client for Microsoft Networks

From the Windows desktop:

- 1 Select **Start** ⇒ **Control** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click the **Client** network component.
The Select Network Protocol window appears.
- 5 Select the **Client for Microsoft Networks** Network Client and then click the **OK** button.
- 6 Click the **Cancel** button to close the Select Network Component Type window.
- 7 Click the **OK** button to preserve the installed components.

- 8 Click the **Cancel** button to close the Dial-up connection window.

Configuring the WINS and DNS settings

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firebox.

From the Windows desktop:

- 1 Select **Start** ⇒ **Control Panel** ⇒ **Network Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click the **Properties** button.
- 3 Click the **Networking** tab.
- 4 Select the **Internet Protocol (TCP/IP)** component, then click the **Properties** button.
The Internet Protocol (TCP/IP) Properties window appears.
- 5 Click the **Advanced** button.
The Advanced TCP/IP Settings window appears.
- 6 Click the **DNS** tab.
- 7 Under the “DNS server addresses, in order of use” heading, click the **Add** button.
The TCP/IP DNS Server window appears.
- 8 Enter your DNS server IP address in the appropriate field, then click the **Add** button.
If you have multiple remote DNS servers repeat the last two steps.

NOTE

You *must* list the DNS server on the Private network behind the Firebox first.

- 9 Enable the **Append these DNS suffixes (in order)** option.
- 10 Click the **Add** button.
The TCP/IP Domain Suffix window appears.
- 11 Enter your **Domain suffix** in the appropriate field.
If you have multiple DNS suffixes repeat the last two steps.
- 12 Click the **WINS** tab.

- 13 Under the “WINS addresses, in order of use” heading, click the **Add** button.
The TCP/IP WINS Server window appears.
- 14 Enter your WINS server IP address in the appropriate field, then click the **Add** button.
If you have multiple remote WINS servers repeat the last two steps.
- 15 Click the **OK** button to close the Advanced TCP/IP Settings window.
- 16 Click the **OK** button to close the Internet Protocol (TCP/IP) Properties window.
- 17 Click the **OK** button to close the next window.
- 18 Click the **Cancel** button again to close the Dial-up connection window.

Install the MUVPN Client

Install the SOHO 6 MUVPN client software on each remote computer. The MUVPN installation files are available at the WatchGuard Web site:

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

The installation process consists of two parts: installing the client software on the remote computer and configuring the client.

NOTE

In order to perform the installation process successfully, you *must* log into the remote computer with local administrator rights.

Follow these steps to install the client:

- 1 Copy the MUVPN installation file to the remote computer.
- 2 Double-click the MUVPN installation file.
If at any time during the installation process you inadvertently skip a step, simply cancel the process and begin again.
- 3 The installation welcomes you to the InstallShield Wizard. Click the **Next** button.
During the Setup Status portion of the install procedure, the InstallShield may detect ReadOnly Files. If this occurs, click **Yes** for each event in order to continue the install.

- 4 The installation welcomes you again. Click the **Next** button.
The Software Licence Agreement appears.
- 5 Click the **Yes** button to accept the terms of the License Agreement and to continue with the installation.
The Setup Type window appears.
- 6 Select the type of setup. By default, Typical is enabled—this is the setup recommended by WatchGuard. Click the **Next** button.
- 7 If you are installing the client on a Windows 2000 host, the InstallShield detects the native Windows 2000 L2TP component. The client uses this component and does not need to install its own. Click the **OK** button to continue with the install.
The Select Components window appears.
- 8 Keep the default components and click the **Next** button.
The Start Copying Files window appears.
- 9 Click the **Next** button to begin copying files.
A command prompt window appears while the `dni_vapmp` file is installed—this is normal. When it is complete, the installation will continue.
- 10 When the InstallShield Wizard is complete, click the **Finish** button.
- 11 The InstallShield Wizard then searches for a User Profile file, click the **Next** button as this step is *not* necessary.
An Information dialog box appears.
- 12 Click the **OK** button to continue with the installation.
- 13 The InstallShield Wizard has completed the install of the SOHO 6 MUVPN client, verify that the option **Yes, I want to restart my computer now** is enabled and click the **Finish** button.
The computer reboots.

NOTE

The ZoneAlarm personal firewall may interfere with regular Local network traffic preventing access to network resources. If the remote computer is connected to the network after reboot, this may disrupt the network logon process. If in doubt, log on to the computer locally the first time after installation. For more information regarding ZoneAlarm, see Chapter 3 "The ZoneAlarm Personal Firewall" on page 33.

Configuring the MUVPN Client

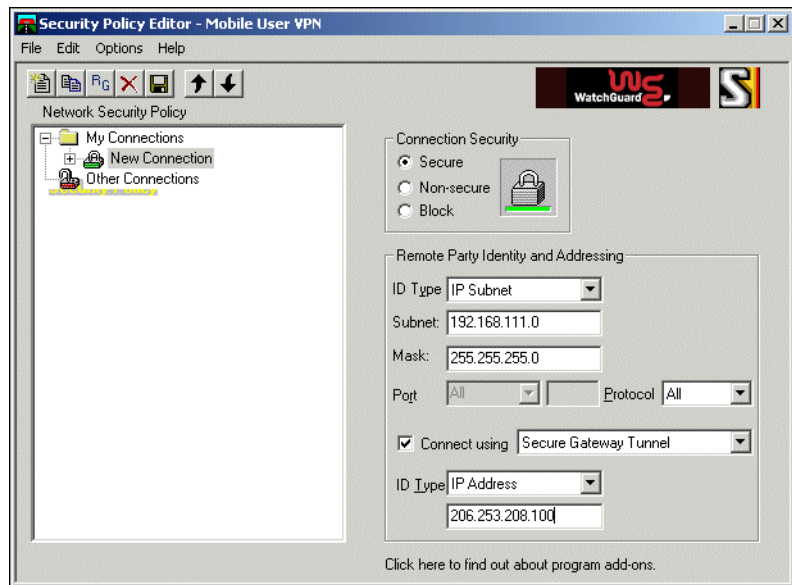
Once you have restarted the machine, the WatchGuard Policy Import dialog box appears. Click the **Cancel** button as this step is *not* necessary.

From the Windows desktop system tray:

- 1 Right-click on the **Mobile User VPN** client icon.
The Security Policy Editor window interface appears.
- 2 Select **Edit** ⇒ **Add** ⇒ **Connection**.
A New Connection will appear under the My Connections folder within the Network Security Policy field on the left side of the Editor.

NOTE

The ZoneAlarm personal firewall may immediately begin to display alerts on your Windows desktop. For more information regarding ZoneAlarm see "The ZoneAlarm Personal Firewall" on page 33.

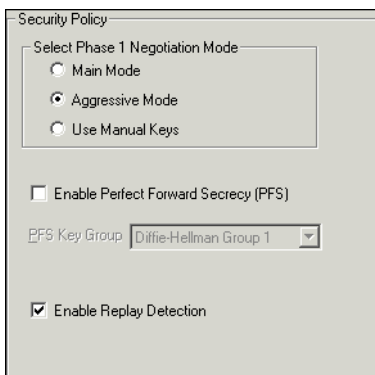


- 3 Under the Connection Security header on the right side of the Security Policy Editor window, enable the **Secure** option.
- 4 Under the Remote Party Identity and Addressing header, select **IP Subnet** from the ID Type drop list.

- 5 Enter the network IP Address of the Trusted Network behind the SOHO 6 in the field labeled “Subnet”.
In our example, 192.168.111.0.
- 6 Enter the Subnet Mask of the Trusted Network behind the SOHO 6 in the field labeled “Mask”.
In our example, 255.255.255.0.
- 7 From the Protocol drop list, verify that **All** has been selected.
- 8 Enable the **Connect using** checkbox and select **Secure Gateway Tunnel** from the drop list.
- 9 From the ID Type drop list, select **IP Address**.
- 10 Enter the External IP Address of the SOHO 6 in the appropriate field.
In our example, 206.253.208.100.
- 11 From the Network Security Policy on the left, expand **New Connection**.
My Identity and Security Policy should appear below New Connection.



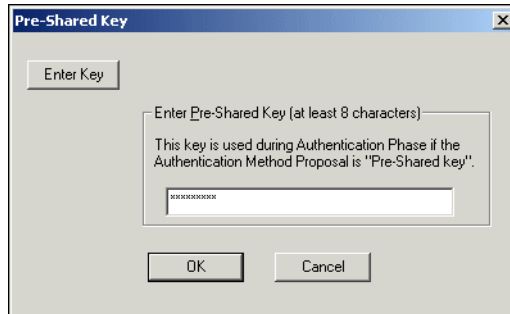
- 12 From the Network Security Policy, select **Security Policy**.
- 13 From the Select Phase 1 Negotiation Mode header, enable the **Aggressive Mode** option.



- 14 Select **My Identity**.

15 Click the **Pre-Shared Key** button.

The Pre-Shared Key window appears.



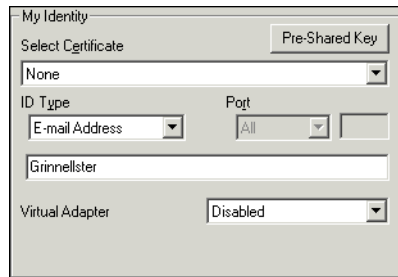
16 Click the **Enter Key** button.

17 Enter the same Passphrase configured on the SOHO 6 in the appropriate field.

In our example, pL4n3phr34k.

18 From the Select Certificate drop list, verify that **None** has been selected.

19 From the ID Type drop list, select **E-mail Address**.



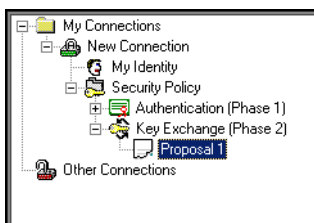
20 Enter the same Username configured on the SOHO 6.

In our example, Helmdog.

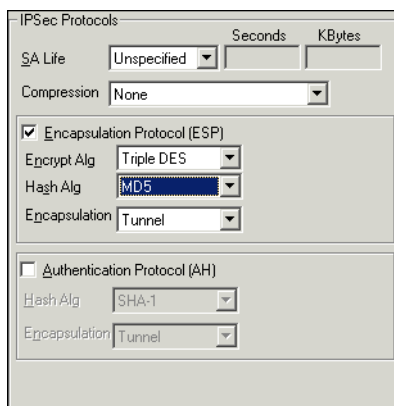
NOTE

Both the Pre-Shared Key and the E-mail Address, *must* exactly match the System Passphrase and System Administrator Name configured on the SOHO 6 or the connection will fail.

- 21 From the Virtual Adapter drop list, verify that **Disabled** has been selected.
- 22 From the Network Security Policy expand **Security Policy**, then expand **Key Exchange (Phase 2)**.
My Identity and Security Policy should appear below New Connection.



- 23 Select **Proposal 1**.
My Identity and Security Policy should appear below New Connection.
- 24 Verify that the **Encapsulation Protocol (ESP)** check box is enabled.



- 25 Set the Encrypt Alg and Hash Alg drop lists to the same values configured on the SOHO 6.
The "Hash Alg" setting refers to the "Authentication Algorithm" and the "Encrypt Alg" setting refers to the "Encryption Algorithm" settings on the SOHO 6. In our example, Triple DES and MD5.

NOTE

These two setting *must* exactly match those on the SOHO 6 or the connection will fail.

26 Select **File** ⇒ **Save Changes**.

Uninstall the MUVPN client

At some point, it may become necessary to completely uninstall the MUVPN client. WatchGuard recommends a complete uninstall using the Windows Add/Remove Programs tool.

First, disconnect all existing tunnels and dial-up connections and reboot the remote computer. Then, 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 click the **Change/Remove** button.
The InstallShield Wizard window appears.
- 4 Select **Remove**. Click the **Next** button.
The Confirm File Deletion dialog box appears.
- 5 Click the **OK** button to completely remove all of the components.
A command prompt window appears while the `dn1_vapmp` file is installed—this is normal. When it is complete, the installation will continue.
The Uninstall Security Policy dialog box appears.
- 6 Click the **Yes** button to delete the Security Policy Personal Certificates and Private/Public Keys.
The InstallShield Wizard window appears.
- 7 Verify that the option **Yes, I want to restart my computer now** is enabled and click **Finish**.
The computer will reboot.

NOTE

The ZoneAlarm personal firewall settings are preserved under the following default directories.

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

If you wish to disregard these settings, delete the contents.

- 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.

Connect and Disconnect the MUVPN Client

The MUVPN client enables the remote computer to establish a secure, encrypted connection to a protected network over the Internet. To do this, you *must* first connect to the Internet and then use the MUVPN client to connect to the protected network.

Connecting the MUVPN Client

- 1 First establish an Internet connection through either Dial-Up Networking or directly through a local area network (LAN) or wide area network (WAN).

From the Windows desktop system tray:

- 2 Verify the MUVPN client status—it *must* be activated. If it is not, right-click the icon and select **Activate Security Policy**.
For information on how to determine the status of the MUVPN icon, see the following section “The Mobile User VPN client icon”.

Then, from the Windows desktop:

- 3 Select **Start** ⇒ **Programs** ⇒ **Mobile User VPN** ⇒ **Connect**.
The WatchGuard Mobile User Connect window appears.
- 4 Click the **Yes** button.

The Mobile User VPN client icon

The Mobile User VPN icon exists in the Windows desktop system tray and displays several different status images. The following lists these images and provides a brief description of each.

Deactivated



The MUVPN Security Policy is deactivated or the Windows operating system did not start a necessary Mobile User VPN

service properly and the remote computer *must* be restarted (if this continues you may need to 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 has begun 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 transmitting only 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 transmitting only secured data.

Activated, Connected and Transmitting both Secure and Unsecured Data



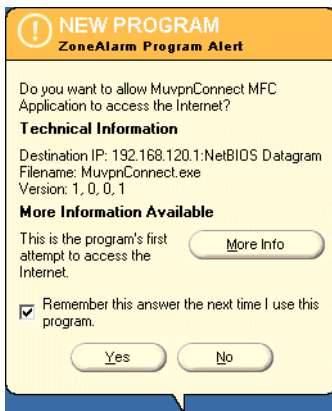
The MUVPN client has established at least one secure, MUVPN tunnel connection. The red and green bars on the right of the icon indicate that the client is transmitting both secured and unsecured data.

Allowing the MUVPN client through the personal firewall

There are a couple of programs associated with the MUVPN client, which you *must* allow through the personal firewall in order to establish the MUVPN tunnel:

- MuvpnConnect.exe
- IreIKE.exe

The personal firewall will detect the attempt of these programs to access the Internet. The New Program alert dialog box appears requesting access for the MuvpnConnect.exe program.



From the ZoneAlarm alert dialog box:

- 1 Enable the **Remember this answer the next time I use this program** option and click the **Yes** button.

This enables ZoneAlarm to allow the MuvpnConnect.exe program through each time you attempt to make a MUVPN connection.

The New Program alert dialog box appears requesting access for the IreIKE.exe program.

- 2 Enable the **Remember this answer the next time I use this program** option and click the **Yes** button.

This enables ZoneAlarm to allow the IreIKE.exe program through each time you attempt to make a MUVPN connection.

Disconnecting the MUVPN client

The MUVPN tunnel is independent of the Internet connection. Close the MUVPN tunnels when the remote computer encounters either of the following events.

- Loses the Internet connection
- No longer needs the MUVPN tunnel

From the Windows desktop system tray:

- 1 Right-click the **Mobile User VPN** client icon.
- 2 Select **Disconnect All**.

The MUVPN Client closes all tunnels. This process does not affect your connection to the Internet. You *must* disconnect from the Internet separately.

- 3 Right-click the **Mobile User VPN** client icon and select **Deactivate Security Policy**.

The MUVPN icon displays a red slash to indicate a deactivated Security Policy.

If you are using the ZoneAlarm personal firewall, deactivate this as well.

From the Windows desktop system tray:

- 1 Right-click the **ZoneAlarm** icon  and select **Shutdown ZoneAlarm**.

The ZoneAlarm dialog box appears.

- 2 Click the **Yes** button when prompted to quit ZoneAlarm.

Monitor the MUVPN Client Connection

There are two tools that accompany the MUVPN client which can be used to monitor your connection and diagnose problems that may occur: the Log Viewer and the Connection Monitor.

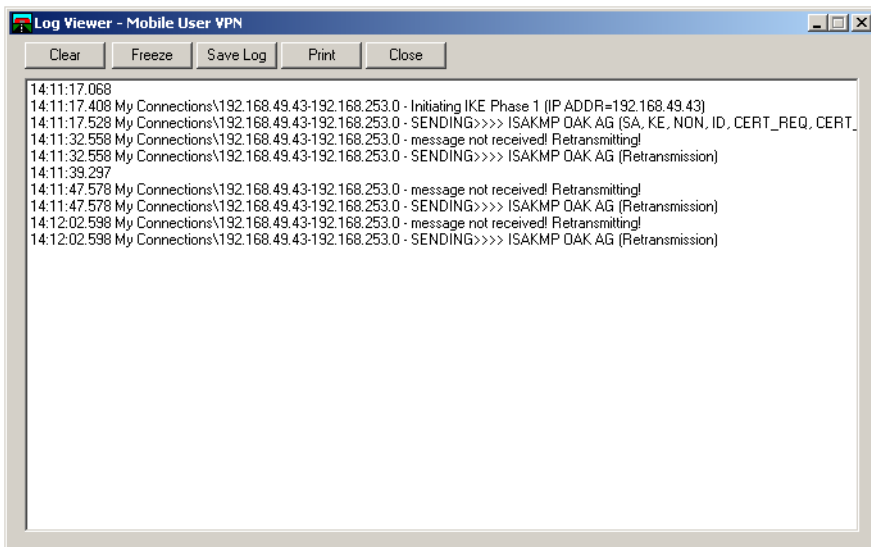
The Log Viewer

The LogViewer displays the communications log, a diagnostic tool that lists the negotiations that occur during the MUVPN client connection.

From the Windows desktop system tray:

- 1 Right-click the **Mobile User VPN** client icon.
- 2 Select **Log Viewer**.

The Log Viewer window appears.



The Connection Monitor

The Connection Monitor displays statistical and diagnostic information for each active connection in the security policy. This module shows the actual security policy settings and the security association (SA) information established during Phase 1 IKE negotiations and 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:

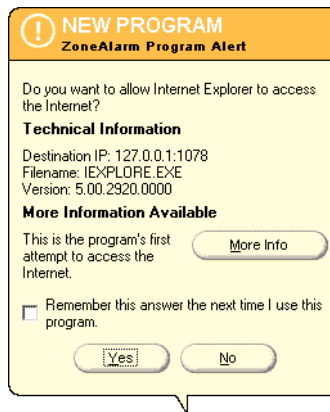
- SA indicates that the connection has only a Phase 1 IKE SA. This occurs when connecting to a secure gateway tunnel or when a Phase 2 IPsec SA fails to establish or has not been established yet.
- A key indicates that the connection has a Phase 2 IPsec SA, or both a Phase 1 and Phase 2 SA.
- A key with a black line moving below it indicates that the client is processing secure IP traffic for that connection.
- When a single Phase 1 SA to a gateway protects multiple Phase 2 SAs, there is a single Phase 1 connection with the SA icon and individual Phase 2 connections with the key icon displayed above that entry.

The ZoneAlarm Personal Firewall

A personal firewall is a barrier between your computer and the outside world. The computer is most vulnerable at its doors, called ports. Without ports, no connection to the Internet is possible.

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

When using ZoneAlarm, you often see Program Alert dialog boxes similar to the image below.



This alert appears whenever one of your programs (in this example, Internet Explorer) attempts to access the Internet or your local network. This powerful feature means no information leaves your computer unless you give it permission.

If you enable the “Remember the answer each time I use this program” checkbox you will only have to answer this question once for each program.

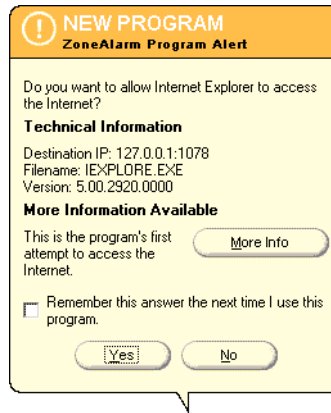
ZoneAlarm Features

The ZoneAlarm personal firewall provides a brief tutorial of the product immediately after installation of the MUVPN client. Carefully read each step to familiarize yourself with the application.

For more information on ZoneAlarm features and configuration, 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 Program Alert will be displayed on the Windows desktop informing the user which particular program needs access. Often, the program associated with the application is not readily indicative of the application the user is attempting to execute.



In the example above, the Internet Explorer Web browser application has been launched and is attempting to access the users home page. The program which actually needs to pass through the firewall is "IEXPLORE.EXE".

In order to allow this program access each time the application is executed, enable the **Remember the answer each time I use this program** checkbox.

Here is a list of a few essential programs which will need access through the ZoneAlarm personal firewall in order to operate some important applications.

Programs Which *Must* Be Allowed

<i>MUVPN client</i>	IreIKE.exe MuvpnConnect.exe
<i>MUVPN Connection Monitor</i>	CmonApp.exe
<i>MUVPN Log Viewer</i>	ViewLog.exe


Programs Which *May* be Allowed

<i>MS Outlook</i>	OUTLOOK.exe
-------------------	-------------

<i>MS Internet Explorer</i>	IEXPLORE.exe
Netscape 6.1	netscp6.exe
<i>Opera Web browser</i>	Opera.exe
<i>Standard Windows network applications</i>	lsass.exe services.exe svchost.exe winlogon.exe

Shutting Down ZoneAlarm

From the Windows desktop system tray:

- 1 Right-click on the **ZoneAlarm icon**  and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 2 Click the **Yes** button when prompted to quit ZoneAlarm.

Uninstalling ZoneAlarm

From the Windows desktop:

- 1 Select **Start** ⇒ **Programs** ⇒ **Zone Labs** ⇒ **Uninstall ZoneAlarm**.
The Confirm Uninstall dialog box appears.
- 2 Click the **Yes** button.
The ZoneLabs TrueVector service dialog box appears.
- 3 Click the **Yes** button to continue with uninstalling the TrueVector service and disable its Internet Security features.
The Select Uninstall Method window appears.
- 4 Verify that **Automatic** is selected and then click the **Next** button.
- 5 Click the **Finish** button to perform the uninstall.

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 the **Yes to All** button to completely remove all of these files.

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

Troubleshooting Tips

WatchGuard maintains a knowledge base on our Web site, including an In-Depth FAQ section on configuring and using the MUVPN client. This is available at:

www.watchguard.com/support

A few of the most common issues found in installing, configuring, and using the MUVPN client are described below.


My computer is hung up just after installing the MUVPN client...

This is most likely due to either the ZoneAlarm personal firewall application interfering with regular Local network traffic or it is because the MUVPN client is active and is unsuccessfully attempting to create VPN tunnels.

When the MUVPN client is not in use, ZoneAlarm should be shutdown and the client deactivated.

From the Windows desktop system tray:

- 1 First, reboot your computer.
- 2 Right-click on the Mobile User VPN client icon.

- 3 Select **Disconnect All**.
The MUVPN client closes all VPN tunnels.
- 4 Right-click on the Mobile User VPN client icon and select **Deactivate Security Policy**.
The MUVPN icon will display a red slash to indicate that the Security Policy has been deactivated.
- 5 Right-click on the ZoneAlarm icon  and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 6 Click the **Yes** button when prompted to quit ZoneAlarm.

I have to enter my network log in 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 if you were at the office connected to the network. Windows stores the information for use by network adapters and networked applications. Later, when you connect to your ISP and start the MUVPN client, your computer uses the stored user name, password, and domain to connect to the company network.

I am not prompted for my user name and password when I turn my computer on...

This is most likely due to the ZoneAlarm personal firewall application. This program is very good at what it does: keeping your computer secure from unauthorized incoming or outgoing traffic. Unfortunately, it may block your computer from broadcasting its network information thereby preventing the machine from sending the necessary login information. You should be certain to shut down ZoneAlarm each time you disconnect the MUVPN connection.

Is the Mobile User VPN tunnel is working...

The Mobile User VPN client icon, which appears in the Windows desktop system tray once it has been launched, will display a key within the icon once the client has connected.

To test the connection, ping a computer on your company network.

-
- Select **Start** ⇒ **Run**. Type `ping` and 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 verifies and maps network drives automatically when the computer starts. Because there is no way for you to establish a remote session with the company network before the computer actually starts, drive mapping fails during the boot process and a red X appears on the drive icon. Establish a MUVPN tunnel and open the network drive. The red X should disappear.

How to map a network drive

Due to a Windows operating system limitation, mapped network drives disappear when you work remotely. To remap a network drive from the Windows desktop:

- 1 Right-click on **Network Neighborhood**.
- 2 Select **Map Network Drive**.
The Map Network Drive dialog box appears.
- 3 Use the drop list to select a drive letter.
Either use the drop list or type a network drive path. For example:
`\\techsupport\share2\rodolfo`
- 4 Click **OK**.

The mapped drive appears in the My Computer window. Even if you enable the “Reconnect at Logon” checkbox, the mapped drive will not appear the next time you start your computer unless it is physically connected to the network.

I sometimes get prompted for a password when I am browsing the company network...

Due to a Windows networking limitation, remote user virtual private networking products only allow access to a single network domain. If your company is large enough to require subnetting (multiple networks connected together), you will only be able to browse your own domain. Attempts to access other domains will result in a password prompt. Unfortunately, even providing the correct information will not open these additional networks.

It takes a *really* long time to shut down the computer after using Mobile User VPN...

If you open and browse a mapped network drive during a MUVPN session, the Windows operating system waits for a signal from the network before it times out and completes the shut down cycle.

I lost the connection to my ISP, and now I can't use the company network...

If you lose Internet connection long enough, MUVPN also loses the secure tunnel. Follow the steps to close the tunnel. Then connect to the Internet and restart the MUVPN client.