

WatchGuard®

Mobile User VPN

Administration Guide

WatchGuard Mobile User VPN



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 - 2004 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*.

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

WFS Software Number v7.2

SafeNet Software Number v6.1.3

Contents

CHAPTER 1	Preparing the Firebox to Use MUVPN	1
	Purchasing a Mobile User VPN license	2
	Entering License Keys	2
	Configuring WINS and DNS Servers	3
	Preparing Mobile User VPN Profiles	4
	Defining a User for a Firebox Authenticated Group	4
	<i>Modifying an existing Mobile User VPN entry</i>	6
	<i>Allowing Internet access through MUVPN tunnels</i>	7
	Using Extended Authentication	8
	<i>Define an extended authentication group</i>	9
	Setting Advanced Preferences	11
	Configuring Services to Allow Incoming MUVPN Traffic	12
	<i>By individual service</i>	13
	<i>Using the Any service</i>	14
	Regenerating End-User Profiles	15
	Saving the Profile to a Firebox	15
	Distributing the Software and Profiles	15
	Making Outbound IPSec Connections From Behind a Firebox	16
	Configuring Debugging Options for MUVPN	17

Terminating Tunnels on Optional or Trusted Interfaces17
Terminating IPSec Connections17
CHAPTER 2 MUVPN Client Preparation, Installation, and Connection19
Prepare the Remote Computers20
<i>System requirements</i>20
<i>Windows NT operating system setup</i>21
<i>Windows 2000 operating system setup</i>22
<i>Windows XP operating system setup</i>26
<i>MUVPN client requirements</i>29
Install and Uninstall the MUVPN Client30
<i>Update the end-user profile</i>32
<i>Uninstall the MUVPN client</i>33
Connect and Disconnect the MUVPN Client34
<i>Connecting the MUVPN Client</i>34
<i>The Mobile User VPN client icon</i>35
<i>Allowing the MUVPN client through the personal firewall</i>37
<i>Disconnecting the MUVPN client</i>38
Monitor the MUVPN Client Connection38
<i>The Log Viewer</i>38
<i>The Connection Monitor</i>39
CHAPTER 3 The ZoneAlarm Personal Firewall41
ZoneAlarm Features42
Allowing Traffic through ZoneAlarm42
Shutting Down ZoneAlarm44
Uninstalling ZoneAlarm44
CHAPTER 4 Troubleshooting Tips for the MUVPN Client47
<i>My computer is hung up just after installing the MUVPN client...</i>47
<i>I have attempted to connect several times, but nothing is happening...</i>48
<i>I have to enter my network log in information even when I'm not connected to the network...</i>48
<i>I am not prompted for my user name and password when I turn my computer on...</i>48

<i>Is the Mobile User VPN tunnel working...</i>	49
<i>My mapped drives have a red X through them...</i>	49
<i>How to map a network drive...</i>	49
<i>I sometimes get prompted for a password when I am browsing the company network...</i>	49
<i>It takes a really long time to shut down the computer after using Mobile User VPN...</i>	50
<i>I lost the connection to my ISP, and now I can't use the company network...</i>	50
<i>No matter what I do, I can't use the company network...</i>	50
Index	51

Preparing the Firebox to Use MUVPN

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.

Mobile User VPN (MUVPN) requires configuration of both the Firebox and the remote client computers. The Firebox administrator has considerable control over the client configuration through a collection of settings called an end-user profile.

MUVPN users authenticate either to the Firebox or to a Windows NT or RADIUS authentication server. Authentication takes place either by using shared keys or certificates.

The complete procedure for using MUVPN is documented in the rest of this guide, and in the end-user brochures distributed for specific client operating systems. This chapter describes the Firebox procedures you need to perform before using the rest of this guide. For information specific to the SOHO 6, see the *SOHO 6 User Guide*.

NOTE

If you are creating an MUVPN tunnel to a SOHO 6, WatchGuard recommends that you obtain a static IP address. If you use a dynamically addressed SOHO 6, you must

reconfigure your MUVPN client every time the address changes.

Purchasing a Mobile User VPN license

WatchGuard Mobile User VPN is an optional feature of the WatchGuard Firebox System. Although the administrative tools to configure Mobile User VPN are automatically included in the Policy Manager software, you must purchase a license for each installation of the client software to activate the feature.

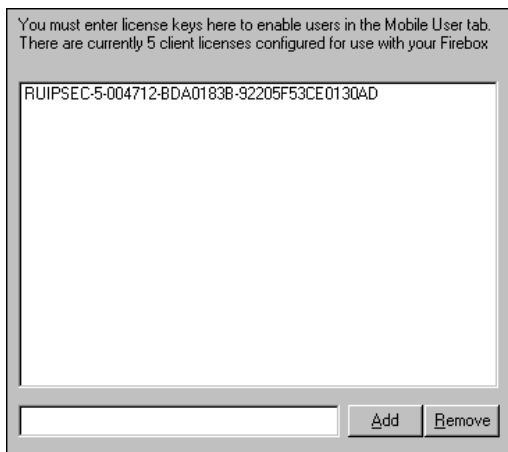
A license is available through your local reseller or at:
<http://www.watchguard.com/sales>

Entering License Keys

The first step in configuring the Firebox for MUVPN is to enter the license key or keys into the Firebox configuration file. The Firebox automatically restricts the number of Mobile User VPN connections to the sum of the number of seats each license key provides. From Policy Manager:

- 1 Select **Network > Remote User**. Click the **Mobile User Licenses** tab.

The Mobile User licenses information appears as shown below.



- 2 Enter the license key in the text field to the left of **Add**. Click **Add**.
The license key appears in the list of client licenses configured for use with the Firebox. Repeat the process until all your keys are added.

Encryption levels

Because of strict export restrictions placed on exported high encryption software, WatchGuard Firebox products are packaged with base encryption on the installation CD. You must use a higher encryption level when using MUVPN because the IPsec standard requires at least a 56-bit (medium) encryption.

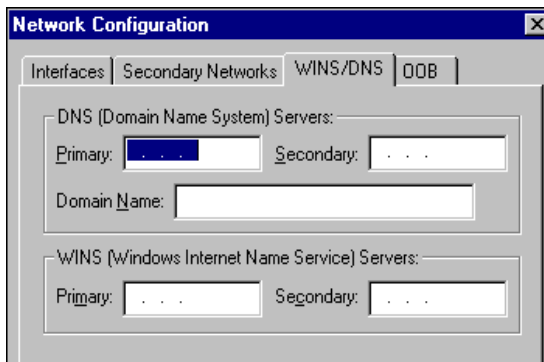
Configuring WINS and DNS Servers

RUVPN and MUVPN clients rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS translates host names into IP addresses, while WINS resolves NetBIOS names to IP addresses. These servers must be accessible from the Firebox trusted interface.

Make sure you use only an internal DNS server. Do not use external DNS servers.

From Policy Manager:

- 1 Select **Network > Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears, as shown in the following figure.
- 2 Enter primary and secondary addresses for the WINS and DNS servers. Enter a domain name for the DNS server.



Preparing Mobile User VPN Profiles

With Mobile User VPN, the network security administrator controls end-user profiles. Policy Manager is used to define the name of the end user and generate a profile with the extension `.wgx`. The `.wgx` file contains the shared key, user identification, IP addresses, and settings required to create a secure tunnel between the remote computer and the Firebox. This file is then encrypted with a key consisting of eight characters or greater which is known to the administrator and the remote user. When the `.wgx` file is installed in the remote client, this key is used to decrypt the file for use in the client software.

If you want to lock the profile for mobile users by making it read-only, see “Setting Advanced Preferences” on page 11.

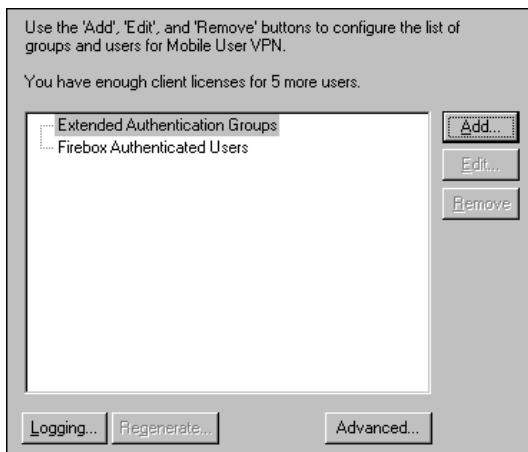
The IPSec client allows for the deployment of the software in situations where the client does not have a static IP address—such as with a DSL connection. This is the default profile and allows for the conversion of existing profiles (with the `.exp` extension) to the newer version (with the `.wgx` extension). New keys are generated as a part of this process; they must then be distributed to the users in the field.

Defining a User for a Firebox Authenticated Group

If the new user you are defining will use the Firebox for authentication, use the following procedure to define that user. If the new user will use a third-party authentication server for authentication, use the procedure described in “Using Extended Authentication” on page 8.

From Policy Manager:

- 1 Select **Network > Remote User**. Click the **Mobile User VPN** tab.
The Mobile User VPN information appears, as shown in the following figure.



- 2 Select **Firebox Authenticated Users**. Click **Add**. Click **Next**. The Mobile User VPN Wizard - Firebox Authenticated User appears.
- 3 Enter a username and passphrase.
- 4 Enter a shared key for the account.
This key will be used to negotiate the encryption and/or authentication for the MUVPN tunnel.
- 5 If you are connecting with a Pocket PC, select the appropriate checkbox. Click **Next**.
- 6 Select whether you will use the shared key or a certificate for authentication. Click **Next**.
- 7 If you specified certificates, enter the configuration passphrase of your certificate authority. Click **Next**.
- 8 Specify the network resource to which this user will be allowed access.
By default, the IP address of the Trusted network appears in the field marked Allow user access to.
- 9 If you plan to use a virtual adapter and route all of the remote user's Internet traffic through the IPsec tunnel, select the checkbox marked **Use default gateway on remote network**. This option also allows you to route MUVPN traffic through the HTTP proxies on the Firebox. For more information on this option, see "Allowing Internet access through MUVPN tunnels" on page 7.

NOTE

If you want to grant access to more than one network or host, use the procedure in the next section to modify the policy after finishing this wizard.

- 10 Specify a virtual IP address for this mobile user. Click **Next**. This can either be an unused IP address on the network you specified in the previous step or on a false network you have created.
- 11 Select an authentication method and encryption method for this mobile user's connections. Enter a key expiration time in kilobytes or hours.

Authentication

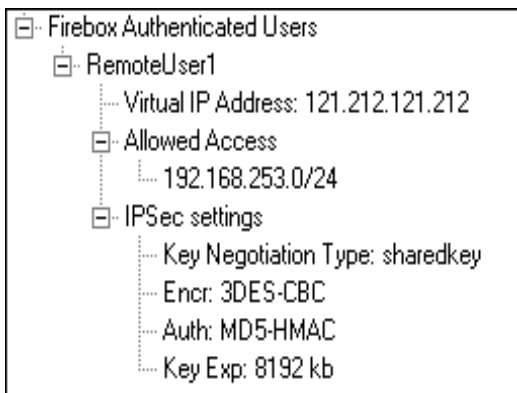
MD5-HMAC (128-bit algorithm) or SHA1-HMAC (160-bit algorithm)

Encryption

None (no encryption), DES-CBC (56-bit), or 3DES-CBC (168-bit)

- 12 Click **Next**. Click **Finish**.

The wizard closes and the username appears on the Mobile User VPN tab. If you expand the plus signs (+) next to the entries, you can view the information as shown in the following figure.



Modifying an existing Mobile User VPN entry

Use the Mobile User VPN wizard to generate a new .exp or .wgx file every time you want to change an end-user profile. Reasons to change a profile include:

- Modifying the shared key
- Adding access to additional hosts or networks
- Restricting access to a single destination port, source port, or protocol
- Modifying the encryption or authentication parameters

From Policy Manager:

- 1 Select **Network > Remote User**.
- 2 In the list of usernames and groups on the **Mobile User VPN** tab, click the username or group you want to change.
- 3 Click **Edit**.
The Mobile User VPN wizard appears, displaying the form containing the user or group name and passphrase.
- 4 Use **Next** to step through the wizard, modifying the end-user profile according to your security policy preferences.
- 5 To add access to a new network or host, proceed to the Allowed Resources and Virtual IP Address screen in the Mobile User VPN wizard. Click **Add**.
You can also use this screen to change the virtual IP address assigned to the remote user.
- 6 In the **Advanced Mobile User VPN Policy Configuration** dialog box, use the drop-down list to select **Network** or **Host**. Type the IP address. Use the **Dst Port**, **Protocol**, and **Src Port** options to restrict access. Click **OK**.
- 7 Step completely through the wizard to the final screen. Click **Finish**.
You must click Finish to create a new .wgx file and write the modified settings to the Firebox configuration file.
- 8 Click **OK**.

Allowing Internet access through MUVPN tunnels

You can enable remote users with virtual adapters to access the Internet through an MUVPN tunnel. However, this option has certain performance implications. For better performance, you can use *split tunneling*. Split tunneling refers to a remote user or site accessing the Internet on the same machine as the VPN connection, without placing the Internet traffic inside the tunnel. Browsing the Web occurs directly through the user's ISP.

However, split tunneling exposes the system to attack because the Internet traffic is not filtered or encrypted.

Despite the security risks of split tunneling, it offers a large performance boost compared to internet access over the MUVPN tunnel. When split tunneling is not allowed or supported, Internet-bound traffic must pass across the WAN bandwidth of the headend twice. This creates considerable load on the VPN headend.

NOTE

If you want the MUVPN client to be protected by WatchGuard's HTTP proxies, you cannot use split tunneling. In this scenario, you must allow internet access over the MUVPN tunnel, as described in this procedure. For additional information, see "Outgoing Configuration to allow MUVPN traffic over proxies" on page 14.

One recommended solution is to allow split tunneling, but require that remote users have personal firewalls for machines residing behind the VPN endpoint.

To allow internet access through the MUVPN tunnel:

- 1 When you are running the MUVPN wizard, select the checkbox marked **Use default gateway on remote network** on the network resource screen.
- 2 Create a dynamic NAT entry from VPN to the external interface. If you want to specify that only certain MUVPN users have this ability, create entries from <virtual IP address> to the external interface.
- 3 Add services as appropriate to allow outgoing connections for mobile users. Because you are allowing Internet access through the tunnel, you use the **Incoming** tab to configure outgoing traffic.

Using Extended Authentication

MUVPN with extended authentication allows users to authenticate to a Windows NT or RADIUS authentication server instead of to the Firebox. Instead of validating against its own data, the Firebox validates users against the third-party server. No usernames or passwords need to be configured on the Firebox.

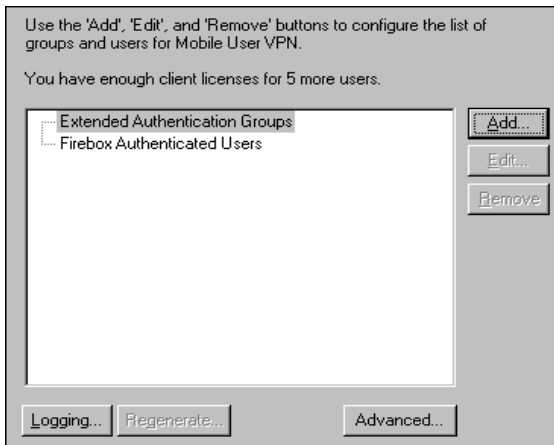
The advantage of MUVPN with extended authentication is that the network administrator does not have to continually synchronize user login information between the Firebox and the authentication server. MUVPN users log into the corporate network from remote locations using the same username and password they use when they are at their desks inside the company. If you want to use a third-party server for authentication, you must define an extended authentication group on the Firebox. The actual usernames and passwords for MUVPN users are stored on the authentication server itself and are not maintained by the Firebox.

Define an extended authentication group

From Policy Manager:

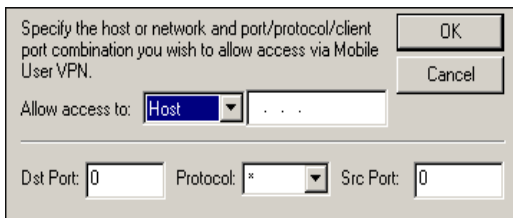
- 1 Select **Network > Remote User**. Click the **Mobile User VPN** tab.

The Mobile User VPN information appears, as shown in the following figure.



- 2 Select **Extended Authentication Groups**. Click **Add**. Click **Next**.
The Mobile User VPN Wizard - Extended Authentication Group appears.
- 3 Specify a name for the extended authentication group. Specify the passphrase used to encrypt the `.wgx` file for this group. Click **Next**.

- 4 Select an authentication server for this group from the drop-down list. Click **Next**.
The authentication server must already be set up using the Authentication Servers dialog box. For information on how to do this, see the WatchGuard Firebox System User Guide.
- 5 Select whether this group will use a shared key or a certificate for authentication. Click **Next**.
- 6 If you specified certificates, enter the configuration passphrase of your certificate authority, which is either the Firebox or a third-party CA device. Click **Next**.
If you specify the passphrase of the Firebox, CA must be active on the Firebox. For information on activating the CA, see Chapter 3, "Activating the Certificate Authority on the Firebox."
- 7 Specify the network resources to which this group will be allowed access. To add a new resource, click **Add**.
The Advanced Mobile User VPN Policy Configuration dialog box appears.



- 8 Use the **Allow Access to** drop-down list to select **Network** or **Host**. Type the IP address. Use the **Dst Port**, **Protocol**, and **Src Port** options to restrict access.
- 9 If you plan to use a virtual adapter and route all of the remote users' Internet traffic through the IPsec tunnel, select the checkbox marked **Use default gateway on remote network**. Click **Next**.
- 10 Specify the virtual IP address pool (these can be virtual IP addresses on a false network). To add addresses, click **Add** and enter an address or address range. Click **Next**.
- 11 Select an authentication method and encryption method for this group's connections. Enter a key expiration time in kilobytes, hours, or both.
If you specify both, the key expires at whichever time occurs earliest.

Authentication

MD5-HMAC (128-bit algorithm) or SHA1-HMAC (160-bit algorithm)

Encryption

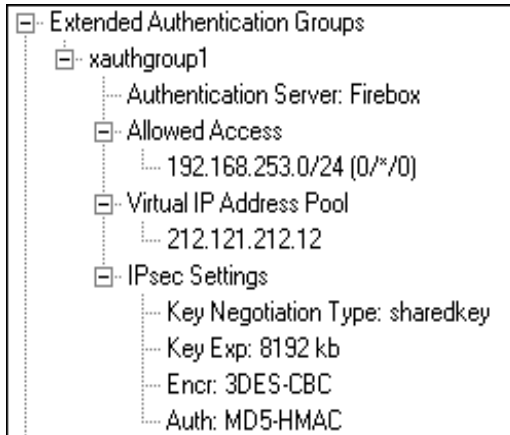
None (no encryption), DES-CBC (56-bit), or 3DES-CBC (168-bit)

- 12 Click **Next**. Click **Finish**.

The wizard closes and the group name appears on the Mobile User VPN tab. If you expand the plus signs (+) next to the entries, you can view the information as shown in the following figure.

Configuring the external authentication server

Define a group on the server that has the same name as the extended authentication remote gateway. All MUVPN users that authenticate to the server must belong to this group.



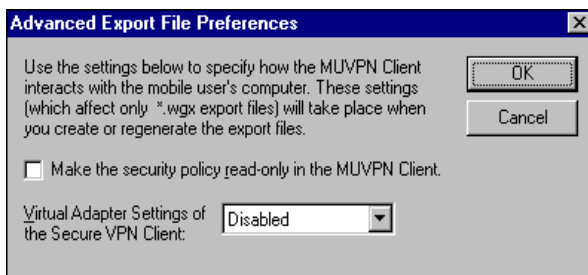
Setting Advanced Preferences

Advanced settings include specifying a virtual adapter rule and locking down the end-user profile so that users can view the settings but not change them. Locking down the profile is the recommended setting, because users generally cannot make

effective changes to the profile without making corresponding modifications to the Firebox.

- 1 Click **Advanced** on the **Mobile User VPN** tab.

The Advanced Export File Preferences dialog box appears, as shown in the following figure.



- 2 If you want to restrict mobile users such that they have read-only access to their profile, select the checkbox marked **Make the security policy read-only in the MUVPN client.**
- 3 A virtual adapter is used for assigning client IP addresses and network parameters such as WINS and DNS. Select the virtual adapter rule for the mobile user:

Disabled

(Recommended) The mobile user will not use a virtual adapter to connect to the MUVPN client.

Preferred

If the virtual adapter is already in use or otherwise unavailable, address assignment is performed without it.

Required

The mobile user must use a virtual adapter to connect to the MUVPN client.

Configuring Services to Allow Incoming MUVPN Traffic

By default, MUVPN users have no access privileges through a Firebox. To allow remote users to access machines behind the Firebox (on the trusted network, for example), you must either add their individual user names, extended authentication group

(for MUVPN users authenticating to an external server), or the `ipsec_users` group (for MUVPN users authenticating to the Firebox) to service icons in the Services Arena. Note that extended authentication groups must be added to services because these users are not members of `ipsec_users`.

WatchGuard recommends two methods for configuring services for MUVPN traffic: by individual service or by using the Any service. Configuring the Any service “opens a hole” through the Firebox, allowing all traffic to flow unfiltered between specific hosts.

To allow traffic to be filtered by WatchGuard’s proxies, follow this procedure, with the slight Service modifications shown at “Outgoing Configuration to allow MUVPN traffic over proxies” on page 14.

By individual service

In the Services Arena, double-click a service that you want to enable for your VPN users. Set the following properties on the service:

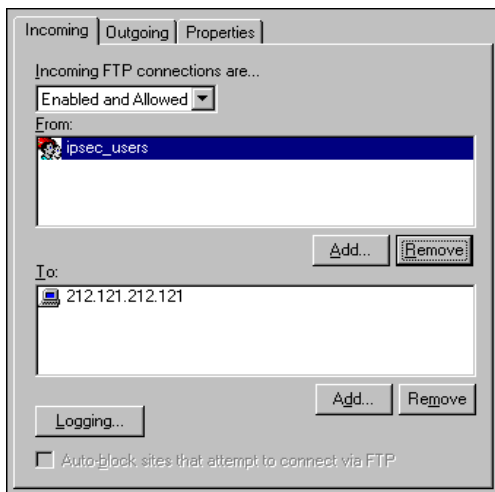
Incoming

- Enabled and allowed
- From: `ipsec_users` or extended authentication group
- To: trusted interface, optional interface, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted interface, optional interface, network or host IP address, or alias
- To: `ipsec_users` or extended authentication group

An example of how you might define incoming properties for a service appears on the following figure.



Outgoing Configuration to allow MUVPN traffic over proxies

The following Services configuration allows MUVPN traffic to be filtered by WatchGuard's proxies.

- Enabled and allowed
- From: ipsec_users, pptp_users, or extended authentication group
- To: trusted interface, optional interface, network or host IP address, or alias

Using the Any service

Add the Any service with the following properties:

Incoming

- Enabled and allowed
- From: ipsec_users or extended authentication group
- To: trusted interface, optional interface, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted interface, optional interface, network or host IP address, or alias

- To: ipsec_users or extended authentication group

NOTE

You cannot use the Any service to allow outgoing traffic To the external interface. Use the Outgoing service to allow outgoing traffic To the external interface.

Make sure you save your configuration file to the Firebox after making these changes.

Regenerating End-User Profiles

The WatchGuard MUVPN configuration gives you the ability to regenerate end-user profiles for your existing MUVPN users. You do not need to create a new profile when you regenerate. Regeneration creates new end-user profiles with the same settings for the current MUVPN users.

To generate new end-user profiles for current MUVPN users, on the **Mobile User VPN** tab, click **Regenerate**.

You can now distribute these end-user profiles as necessary.

Saving the Profile to a Firebox

To activate a new Mobile User profile, you must save the configuration file to the Firebox. Select **File > Save > To Firebox**.

Distributing the Software and Profiles

WatchGuard recommends distributing end-user profiles on a floppy disk or by encrypted email. Each client machine needs the following:

- Software installation package

The packages are located on the WatchGuard LiveSecurity Service Web site at:

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

Enter the site using your LiveSecurity Service user name and password. Click the **Latest Software** link, click **Add-ons/Upgrades** on the left side, and then click the **Mobile User VPN** link.

- The end-user profile
This file contains the user name, shared key, and settings that enable a remote computer to connect securely over the Internet to a protected, private computer network. The end-user profile has the filename *username.wgx*
- Two certificate files—if you are authenticating by way of certificates
These are the *.p12* file, an encrypted file containing the certificate, and *cacert.pem*, which contains the root Certificate Authority (CA) certificate.
- User documentation
End-user brochures developed by WatchGuard are located on the WatchGuard LiveSecurity Service Web site at: www.watchguard.com/support
Enter the site using your LiveSecurity user name and password. Click the **Product Documentation** link, and then click the **VPN** link.
- Shared key
To install the end-user profile, the user is prompted for a shared key. This key decrypts the file and imports the security policy into the MUVPN client. The key is set during the creation of the file in Policy Manager.

Making Outbound IPSec Connections From Behind a Firebox

You may have occasions in which a user wants to make IPSec connections to a Firebox from behind another Firebox. For example, if a mobile employee travels to a customer site that has a Firebox, he or she can make IPSec connections to his or her network using IPSec. For the local Firebox to properly handle the outgoing IPSec connection, you must set up the IPSec service. (For information on enabling services, see Chapter 8, “Configuring Filtered Services” in the WatchGuard Firebox System *User Guide*.)

Because the IPSec service enables a tunnel to the IPSec server and does not perform any security checks at the firewall, use of this service should be limited.

Configuring Debugging Options for MUVPN

WatchGuard offers a selection of logging options that you can set to gather information and help with future troubleshooting. Because enabling these debugging options can significantly increase log message volume and have potentially adverse impacts on Firebox performance, it is recommended that they be enabled only for troubleshooting MUVPN problems.

- 1 From Policy Manager, click **Network > Remote User VPN**.
The Remote User setup window appears with the Mobile User VPN tab selected.
- 2 Click **Logging**.
The IPSec Logging dialog box appears.
- 3 Click the logging options you want to activate.
For a description of each option, right-click it, and then click What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.
- 4 Click **OK**. Save the configuration file to the Firebox.

Terminating Tunnels on Optional or Trusted Interfaces

Because the Firebox can accept IKE traffic (IPSec key negotiation on the optional port), the IPSec peer can be connected directly to the optional port and can route traffic to the trusted network. To enable this feature, on the Safenet Client's security policy editor, set the IP address of the remote gateway to the Firebox's optional IP address.

Terminating IPSec Connections

In order to completely terminate VPN connections, the Firebox must be rebooted. Merely removing the IPSec service does not sever pre-established connections.

MUVPN Client Preparation, Installation, and Connection

The WatchGuard 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 company's trusted and optional networks, protected by a WatchGuard Firebox System. The MUVPN client allows you to provide remote access to your internal networks without compromising security.

You should have already configured the Firebox to work with MUVPN. If you have not, see the previous chapter, "Preparing the Firebox to Use MUVPN".

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 WatchGuard Firebox System to set up the MUVPN client on an end-user's remote computer and to explain the features of the personal firewall.

MUVPN Brochures

Along with this guide, WatchGuard has compiled end-user documentation regarding the preparation, installation, and connection of the Mobile User VPN Client as well as the usage

of the personal firewall. These brochures, customized separately for the supported Windows operating systems, are available on our Web site.

The brochures can be found on the WatchGuard Web site at:

www.watchguard.com/documentation

The rest of this chapter describes the basic tasks involved in preparing the remote computers to use the MUVPN client as well as the installation and connection procedures for the client.

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 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

However, if you plan to use the MUVPN client virtual adapter, the WINS and DNS settings are *not* configured on the client computers, but rather on the Firebox.

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 only if you do *not* plan to use the MUVPN client's virtual adapter.

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 only if you do *not* plan to use the MUVPN client's virtual adapter.

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 > Settings > 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 > Settings > 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 > Settings > 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 > Settings > 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 only if you do *not* plan to use the MUVPN client's virtual adapter.

From the Windows desktop:

- 1 Select **Start > Settings > 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.

MUVPN client requirements

In addition to basic operating system preparation, the MUVPN client requires the following, files, documentation, and pass-phrases.

MUVPN installation file

The installation files—one with the personal firewall (Muvpn.exe) and one without the personal firewall (MuvpnLite.exe)—are available from the WatchGuard Web site at:

www.watchguard.com/support

Enter the site using your LiveSecurity user name and password. Click the **Latest Software** link, then click **Add-ons/Upgrades** on the left side, and then the **Mobile User VPN** link.

The end-user profile

A file containing the user name, shared key, and settings that enable a remote computer to connect securely over the Internet to your trusted network. The end-user profile has the filename: *username.wgx*

The Policy Manager creates an end-user profile when you add a new MUVPN user to the Firebox. For more instructions on creating this file, see the WatchGuard *VPN Guide*, Chapter 5 “Preparing to Use MUVPN”.

Two certificates files—if you are authenticating by way of certificates.

The Policy Manager creates two files when the you select to authenticate using a certificate. These are the .p12 file, an encrypted file containing the certificate, and the cacert.pem file, which contains the root (CA or Certificate Authority) certificate.

For instructions on using certificates for authentication, see the *VPN Guide*, Chapter 5, subsection “Preparing Mobile User VPN Profiles.”

For more information regarding using certificates, see the *VPN Guide*, Chapter 3, “Activate the Certificate Authority on the Firebox.”

User documentation

End-user brochures developed by WatchGuard are located on the WatchGuard Web site at:

www.watchguard.com/support

Enter the site using your LiveSecurity user name and password. Click the **Product Documentation** link and then click the **VPN** link.

Shared Key

In order to install the end-user profile (the .wgx file), the user is prompted for a shared key. This key decrypts the file and imports the security policy into the MUVPN client. The key is set during the creation of the file at the Policy Manager.

NOTE

Write the shared key down and keep it in a secure place as it will be needed during the final steps of the installation process.

Username and Password—if you are authenticating by way of Extended Authentication.

You *must* supply the end user with the Username and Password for their authentication account. This is defined on the relevant authentication server.

For instructions on using Extended Authentication, see “Define an extended authentication group” on page 9

Install and Uninstall the MUVPN Client

The installation process consists of two parts: installing the client software on the remote computer and importing the end-user profile into 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 Copy the end-user profile (the .wgx file) to the remote computer's root directory.
If using certificates to authenticate, copy these files to the root directory as well.
- 3 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.
- 4 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.
- 5 The installation welcomes you again. Click the **Next** button.
The Software Licence Agreement appears.
- 6 Click the **Yes** button to accept the terms of the License Agreement and to continue with the installation.
The Setup Type window appears.
- 7 Select the type of setup. By default, Typical is enabled—this is the setup recommended by WatchGuard. Click the **Next** button.
- 8 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.
- 9 Keep the default components and click the **Next** button.
The Start Copying Files window appears.
- 10 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.
- 11 When the InstallShield Wizard is complete, click the **Finish** button.
- 12 The InstallShield Wizard then searches for the end-user profile (the .wgx file) at the computer's root directory, c:\, click the **Next** button. If the file was not copied to this default directory, you *must* use the Browse button to locate and select the proper folder.

- 13 The InstallShield Wizard has completed the install of the 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, see Chapter 2 "The ZoneAlarm Personal Firewall" on page 41.

Importing the end-user profile

Once you have restarted the machine, the WatchGuard Policy Import dialog box appears. Import the MUVPN end-user profile (the .wgx file) and provide the Shared Key used to decrypt the file.

- 1 The WatchGuard Policy Import window should locate the end-user profile (the .wgx file) in the directory specified during the installation.
If the WatchGuard Policy Import tool does not locate the .wgx file, click **Browse** and locate the file.
- 2 Enter the Shared key in the appropriate field and click the **OK** button.
- 3 You have finished setting up the MUVPN client. Click **OK**.
The remote computer is now ready to use MUVPN.

For instructions on how to reconfigure the MUVPN client with a new end-user profile, see "Update the end-user profile" on page 32.

NOTE

The ZoneAlarm personal firewall may immediately begin to display alerts on your Windows desktop. For more information regarding ZoneAlarm see the Chapter 2 "The ZoneAlarm Personal Firewall" on page 41.

Update the end-user profile

At some point, it may become necessary to reconfigure the MUVPN end-user profile (the .wgx file).

For example:

- The shared key changes
- The certificate files are reissued
- The Extended Authentication account is changed to a different server. For example, from NT authentication to RADIUS.
- The network configuration changes
- The remote computer is transferred to a new end-user

First, use the Policy Manager to edit and create a new MUVPN end-user profile (the .wgx file). For more information, see “Preparing the Firebox to Use MUVPN” on page 1.

From the remote computer:

- 1 Locate and double-click the end-user profile (the .wgx file) file.
If the WatchGuard Policy Import tool does not prompt you with the .wgx file to import, click **Browse** and locate the file.
- 2 Enter the Shared key in the appropriate field. Then click the **OK** button.
- 3 You have finished updating the MUVPN client. Click **OK**.
The remote computer is now ready to use MUVPN. The Security Policy is automatically activated.

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 `dni_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 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).

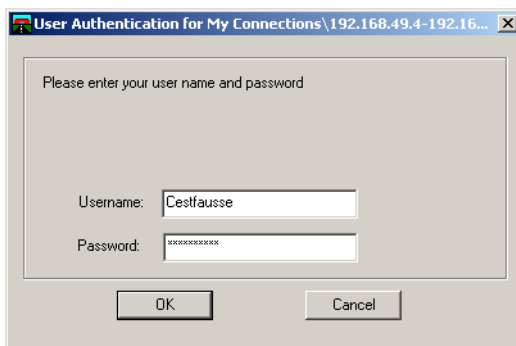
From the Windows desktop system tray:

- 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.

At this point, if you are using Extended Authentication, you will be prompted for the Username and Passphrase created previously on the authentication server. Enter these values and click **OK**.



For more information regarding Extended Authentication, see “Define an extended authentication group” on page 9.

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



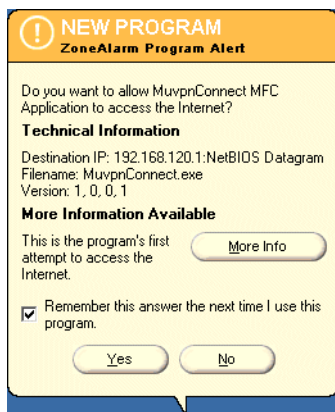
The MUVPN client has established at least one secure, MUVPN tunnel connection. The red and green bars on the right of the icon indicate that the client is transmitting both secured and unsecured data.

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 IrelKE.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

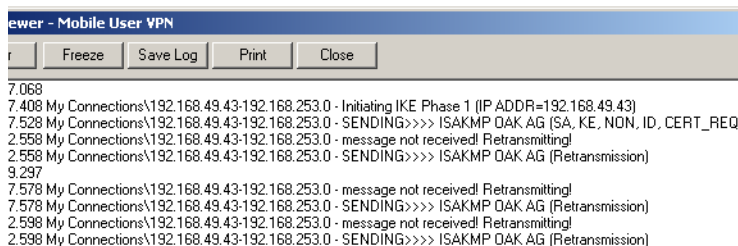
There are two tools that accompany the MUVPN client which can be used to monitor your connection and diagnose problems that may occur: the Log Viewer and the Connection Monitor.

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 is displayed on the Windows desktop informing the user which program needs access. Often, the program associated with the application is not indicative of the application the user is attempting to execute.



In the example above, the Internet Explorer Web browser application 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 the program access each time it is executed, enable the **Remember the answer the next time I use this program** checkbox.

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

Programs Which *Must* Be Allowed

<i>MUVPN client</i>	IrelKE.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
<i>Netscape 6 or 7</i>	netscp6.exe netscp.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 are installed that other programs on the system may share. 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 for the MUVPN Client

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, you should shut down ZoneAlarm and deactivate the client.

First, reboot your computer, then from the Windows desktop system tray:

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

The MUVPN client icon displays a red slash indicating that the Security Policy is deactivated.

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

I have attempted to connect several times, but nothing is happening...

The MUVPN client may have misloaded the end-user profile. Try reloading your security policy.

From the Windows desktop system tray:

- 1 Right-click the Mobile User VPN Client icon.
- 2 Select **Reload Policy**.
The MUVPN client reloads the end-user profile.
- 3 Now try to connect the client again.

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 and prevent the machine from sending the necessary login information. Be certain to shut down ZoneAlarm each time you disconnect the MUVPN connection.

Is the Mobile User VPN tunnel working...

The Mobile User VPN client icon, which appears in the Windows desktop system tray once it is launched, will display a key within the icon once the client is 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 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 **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, mobile 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 can only

browse your own domain. Attempts to access other domains result in a password prompt.

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 your 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.

No matter what I do, I can't use the company network...

There may be a problem with the end-user profile (the .wgx file) or shared passwords.

Index

Symbols

.exp files 4
.p12 file 16, 29
.wgx file 29
.wgx files 4

A

Advanced Export File Preferences
 dialog box 12
Advanced Mobile User VPN Policy
 Configuration dialog box 10
Any service
 and MUVPN 13, 14
authentication server
 specifying 10
 types supported 8
authentication, extended. See
 extended authentication

C

cacert.pem 16, 29

certificates
 files in end-user profile 16
certificates, files required if
 authenticating using 29
Client for Microsoft Networks
 installing on Windows 2000
 computers 24
Connection Monitor, monitoring
 MUVPN client through 39

D

dialog boxes
 Advanced Export File Preferences
 12
 IPSec Logging 17
DNS servers, configuring 3

E

encryption
 and MUVPN 3
end-user profile
 described 29
 importing 32

- updating 32
- end-user profiles for MUVPN users
 - described 1
 - distributing to remote users 15
 - locking 11
 - preparing 4
 - regenerating 15
 - saving 15
- extended authentication
 - defining groups for 8
 - specifying authentication method for 10
 - specifying server 10

F

- File and Printer Sharing for Microsoft Networks
 - and Windows 2000 23
 - and Windows XP 26
- Fireboxes
 - configuring for MUVPN 1

I

- Internet
 - accessing through IPSec tunnel 7
 - accessing through tunnel 7
- Internet Protocol (TCP/IP) Network Component
 - and Windows 2000 23
 - and Windows XP 26
- IPSec Logging dialog box 17

L

- LogViewer, monitoring MUVPN client through 38

M

- MD5-HMAC 6
- Mobile User VPN wizard 5, 7, 9

- Mobile User VPN. See MUVPN
- MUVPN
 - allowing Internet access through 7 and virtual adapters 12
 - authentication for 1
 - configuring debugging options 17
 - configuring services to allow 12
 - configuring shared servers for 3
 - connecting with Pocket PC 5
 - defining new user 4
 - described 1
 - disconnecting 38
 - distributing end-user profiles 15
 - encryption levels for 3
 - end-user profiles. See end-user profiles for MUVPN users
 - entering license keys 2
 - making outbound connections behind Firebox 16
 - modifying existing user 6
 - preparing configuration files for 4
 - preparing end-user profiles 4
 - purchasing license for 2
 - setting encryption for 6
 - specifying authentication method 5, 10
 - system requirements for 20
 - troubleshooting 49
 - with extended authentication 8
- MUVPN client
 - allowing through firewall 37
 - connecting using 34
 - files required to install 29
 - icon for 35
 - installing 29, 30
 - monitoring connection for 38
 - removing 33
- Muvpn.exe 29
- MuvpnLite.exe 29

O

- Outgoing service 15

P

Pocket PC 5

R

Remote Access Server, installing on
Windows NT 21

S

services

configuring to allow MUVPN traffic
12

SHA1-HMAC 6

shared key 30

split tunneling 7

described 7

system requirements 20

T

troubleshooting tips 47

V

virtual adapter for MUVPN users 12

VPNs

design considerations 7

split tunneling 7

terminating 17

W

Windows 2000

installing Client for Microsoft
Networks on 24

installing File and Printer Sharing
for Microsoft Networks on 23

installing Internet Protocol (TCP/IP)
Network Component on 23

WINS and DNS settings 24

Windows NT

installing Remote Access Server on
21

WINS and DNS settings 22

Windows XP

installing Client for Microsoft
Networks on 27

installing File and Printer Sharing
for Microsoft Networks on 26

installing Internet Protocol (TCP/IP)
Network Component on 26

WINS and DNS settings 27

WINS and DNS settings

on Windows 2000 computers 24

on Windows NT computers 22

on Windows XP computers 27

WINS servers, configuring 3

Z

ZoneAlarm

allowing MUVPN client through 37

described 19

troubleshooting 47

