

WatchGuard® VPN Manager Guide

VPN Manager 5.0



Copyright

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

Notice to Users

Information in this document is subject to change and revision without notice. This documentation and the software described herein is subject to and may only be used and copied as outlined in the Firebox System software end-user license agreement. No part of this manual may be reproduced by any means, electronic or mechanical, for any purpose other than the purchaser's personal use, without prior written permission from WatchGuard Technologies, Inc.

TRADEMARK NOTES

WatchGuard and LiveSecurity are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and other countries. Firebox, DVCP, and Designing peace of mind are trademarks of WatchGuard Technologies, Inc. All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Part No: 1200148

Contents

Chapter 1: Introduction to VPN Manager	1
What is VPN Manager?	2
<i>Centrally managing devices</i>	2
<i>Virtual private networking and IPSec</i>	2
Physical Description	3
VPN Manager Features	3
How Does DVCP Work?	4
<i>Configuring VPN Manager</i>	4
<i>DVCP device and tunnel management</i>	5
Planning your Internet Distributed Enterprise (IDE)	5
Chapter 2: Setting Up a Firebox as a DVCP Server	7
Chapter 3: Setting Up Certificates on Web Browsers	9
Enabling Web-based Management	10
Importing a Certificate for Microsoft Internet Explorer 5	10
<i>Troubleshooting IE 5.0 certificate setup</i>	11
Certificate Import Process for Netscape 4.75	11
<i>Troubleshooting Netscape 4.75 certificate setup</i>	11
Resetting Certificates	12
Removing Certificates	13
Chapter 4: Adding Devices to VPN Manager	15
Enabling Fireboxes as DVCP Clients	15
<i>Enabling SOHOs as DVCP clients</i>	16
Adding Devices to VPN Manager	17
Removing a Device from VPN Manager	18
<i>Removing Fireboxes</i>	18
<i>Removing SOHOs</i>	18

Chapter 5: Creating Tunnels Between Devices	21
Adding Policy Templates	22
Adding Security Templates	23
Connecting Devices	23
<i>Drag-and-drop tunnel creation</i>	23
<i>Menu-driven tunnel creation</i>	24
Enabling a SOHO Single-Host Tunnel	25
Removing or Changing a Tunnel	27
<i>Editing a tunnel</i>	27
<i>Removing a tunnel</i>	28
<i>Editing a policy template</i>	28
Chapter 6: Using the VPN Manager User Interface	29
Opening the VPN Manager Display	29
Viewing Device Status	30
<i>Tree-view structure</i>	30
<i>Connection status</i>	30
<i>Context menu options</i>	31
Viewing Tunnels	32
Viewing Log Servers	33
Creating a Custom View	33
Launching Applications from VPN Manager	34
Chapter 7: Using Remote Administration	35
Starting the Remote Management Feature	35
<i>System administration</i>	36
<i>Services</i>	37
<i>Private network</i>	37
<i>Public network</i>	37
<i>System information</i>	38
Index	39

Introduction to VPN Manager

A virtual private network (VPN) is a private network created by exchanging encrypted data between a branch or home office and a corporate network by way of the Internet. Today, many businesses are looking at VPN technology as a cost-effective way to bring together remote offices and telecommuters.

WatchGuard VPN Manager offers an unprecedented level of convenience and control for creating IPSec tunnels and virtual private networks (VPNs) simply and quickly. VPN Manager provides an intuitive graphical user interface (GUI) for rapidly creating IPSec tunnels of varying types of authentication and levels of encryption. Rather than configuring multiple dialog boxes and multi-tab tools, VPN Manager offers speed and reliability through drag-and-drop tunnel creation, automatic wizard launching, and the application of templates. This eliminates the time-consuming, error-prone processes typically associated with the creation of IPSec VPNs. With VPN Manager, you can actually create fully authenticated and encrypted tunnels in minutes, and be assured that they do not clash with other tunnels or security policies.

From the same graphical user interface, you can then administer and monitor the network of created tunnels and know the status of the various components and tunnels at a glance. VPN Manager configures and manages any combination of the WatchGuard Firebox family of appliances.

The WatchGuard Knowledge Base contains extensive information on VPN technology. To access the Knowledge Base, go to the following Web site and log into the LiveSecurity Service:

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

What is VPN Manager?

VPN Manager is a centralized point for creating and managing the network security of an Internet Distributed Enterprise (IDE). An IDE is an organization that uses the Internet extension to conduct business. It usually consists of multiple locations behind security devices, connected by VPNs. VPN Manager administers and monitors an enterprise's sum total of Fireboxes, Event Processors, networks, and VPN tunnels. VPN Manager also has the controls to launch the applications of the WatchGuard Firebox System.

Centrally managing devices

VPN Manager is a powerful tool for: viewing all VPN connections; determining their status; configuring or reconfiguring either or both ends of the tunnels that it monitors and controls; and configuring Fireboxes from a single control center. One of the most innovative features in VPN Manager is its drag-and-drop graphical user interface for creating IPSec tunnels. The key to this drag-and-drop convenience is the underlying technology, the WatchGuard proprietary DVCP (Dynamic VPN Configuration Protocol).

Virtual private networking and IPSec

DVCP eliminates much of the confusion of creating IPSec tunnels, and keeps the operator from creating unworkable configurations.

VPN Manager consists of several parts: a client (referred to as VPN Manager), a server (a Firebox that you designate and activate as the DVCP server), and WatchGuard security appliances.

Physical Description

VPN Manager is a Microsoft Windows NT 4.0, Windows 98, and Windows 2000 application with a toolbar at the top and a main window that consists of four tabbed tree-view windows.

The four tabs and descriptions of the information they contain are:

Device View

A status page for all devices in VPN Manager. This includes the log host, MAC address, and IP address for the interfaces for each device as well as the status of all VPN tunnels currently configured in VPN Manager.

VPN View

Displays status information on current VPN tunnels, their endpoints, and their security parameters.

Logging View

Displays the logging status for devices managed by VPN Manager.

Custom View

Provides a means for you to create a custom view of the devices managed by VPN Manager.

All devices and VPNs are managed through VPN Manager. It can also launch all other programs associated with the WatchGuard Firebox System.

A DVCP server must run on a WatchGuard Firebox (not a SOHO). The server provides centralized storage of all configured devices under management and builds VPNs quickly and interactively for those devices.

The log server consists of the Event Processor, the reporting processes, and their associated supporting files. The VPN Manager's Log Server View provides centralized management of log servers currently in use.

VPN Manager Features

VPN Manager allows you to:

- Configure and monitor multiple Firebox devices

- Configure and monitor multiple SOHO devices
- Create and view contact and location information for each device
- Customize the view of devices and device properties to suit an environment and implementation
- Associate devices in a GUI to create drag-and-drop VPNs without error or confusion
- Centralize management of distributed log servers

How Does DVCP Work?

WatchGuard's DVCP automates the creation of IPSec VPNs. The user interfaces for configuring DVCP tunnels are templates, automated wizards, and point-and-click GUIs. Configurations of various types and levels of authentication and strengths of encryption reside in templates that are selected and applied to the IPSec tunnels you create.

DVCP servers act as information/configuration servers for all the devices inserted into the VPN Manager environment. Upon booting to an operational state, a DVCP client will query the DVCP server for its DVCP information. When the client receives the DVCP information, it restores connections to all tunnel endpoints specified in the DVCP configuration.

After you have configured VPN Manager by supplying the name or IP address of each Firebox you want to monitor, you can then drag and drop one device upon another in the GUI, which then launches a tunnel creation wizard that already knows the IP addresses and read-write passwords of the two devices, based on their registration information. The wizard creates the tunnel based on this information along with the security template that you designate for that purpose. The security templates contain specific authentication and encryption combinations that you select and apply according to the security you want for the tunnel you are creating.

Configuring VPN Manager

Configuring VPN Manager involves:

- Designating a Firebox as a DVCP server

- Adding Fireboxes as devices to the VPN Manager device list
- Creating tunnels — virtual private network connections between devices

When the VPN Manager starts (after configuration), it downloads the lists of configured devices and configured security templates, policy templates, and tunnels. It distributes this information among the appropriate tabs of its display. VPN Manager then gets the current status of the devices in each VPN.

DVCP device and tunnel management

VPN Manager maintains an open connection to the DVCP server. VPN Manager downloads the DVCP configuration at startup and sends a modified configuration when a user makes changes. VPN Manager also accounts for lost connections with an easy reconnect method, remembering its state if it was in the middle of a transaction.

When you make configuration changes via VPN Manager, VPN Manager stores the updated configuration. When the new configuration is saved to the DVCP server, VPN Manager notifies the devices involved that a new configuration exists and forces it to expire its lease/lookup and use the new configuration.

Planning your Internet Distributed Enterprise (IDE)

The remainder of this user guide discusses how to use VPN Manager to create, configure, and administer virtual private networks and tunnel combinations. However, before you configure your IDE, plan your configuration and gather the information you will need to do the following:

- Organize your IDE by domains (sites). Each domain should contain a Firebox or SOHO.
- Make sure you know which devices need to have tunnels between them and what level of encryption and method of authentication to use for each tunnel. The level of encryption and authentication has a direct effect on the performance of the

VPN tunnel because of hardware resources. Consider security and performance when choosing the level of encryption and authentication.

- Assign names to each tunnel and to each VPN. Logical names for tunnels and devices are recommended.
- Make sure that you have the IP addresses or DNS names, and monitoring (read-only) and configuration (read-write) passphrases for all the Fireboxes to be managed by VPN Manager.

Setting Up a Firebox as a DVCP Server

DVCP is a protocol developed by WatchGuard to make VPN configuration and monitoring simple and straightforward. A DVCP server is a Firebox that is responsible for maintaining the VPN configuration for the devices specified in VPN Manager. After you have installed VPN Manager, one of your first tasks is choosing a Firebox within your IDE to be the DVCP server. The Firebox that is physically closest to the VPN Manager workstation is probably the best candidate for the DVCP server.

To access the VPN Manager interface, select **Start ⇒ Programs ⇒ WatchGuardTools ⇒ VPN Manager**.

From VPN Manager:

- 1 Select **Tools ⇒ Policy Manager**.
The WatchGuard Policy Manager appears.
- 2 Select **Network ⇒ Enhanced DVCP Server**.
The DVCP Server Setup window appears.
- 3 Click the checkbox labeled **Enable this Firebox as a DVCP Server**.
- 4 Enter a name in the **Domain Name** field and click **OK**.
You can name the domain anything you want. After you click OK, the display returns to the Policy Manager.

- 5 From Policy Manager, select **File** ⇒ **Save** ⇒ **To Firebox**, create or verify the name for the configuration file, and enter the designated Firebox's read-write passphrase.

This saves the new configuration to the Firebox. The Firebox can now function as a DVCP server, but it has not been activated yet.

- 6 Select the VPN Manager window.
- 7 Select **File** ⇒ **New**.

The New Server dialog box appears.

- 8 Enter the following:

Display Name

A friendly name of your choosing. This will become the name of the Firebox acting as the DVCP server.

Firebox Type

Select the device type that describes the DVCP server device from the drop-down list.

Enter the Host Name or IP Address

This is either the device's DNS name or its IP address.

Status Pass Phrase

This is the current monitoring (read-only) passphrase.

Configuration Pass Phrase

This is the current configuration (read-write) passphrase. This will also be the passphrase needed when configuring a device to be inserted into VPN Manager.

License Key

Enter the key listed on your VPN Manager License Key Certificate.

- 9 Click **OK**.
A message appears confirming the DVCP server setup.
- 10 Click **OK**.
The Firebox reboots. It is now activated as a DVCP server.

Setting Up Certificates on Web Browsers

Certificates are an important component of the secure exchange of information across the Internet. A *certificate* is a file that establishes secure network connections by confirming your identity. A *certificate authority* is a trusted entity that issues certificates and guarantees the identity of the individual granted the certificate.

Certain transactions in VPN Manager, such as managing a WatchGuard SOHO remotely, require your Web browser to have certificates enabled. To maintain security in an open environment such as the Internet, the browser uses both a WatchGuard-proprietary encrypted socket protocol and Secure Sockets Layer (SSL), which is the industry-standard method for protecting Internet communication.

The DVCP server, which acts as the certificate authority for the DVCP environment, creates certificates for the SOHO when the device is inserted into the VPN Manager environment. The certificate file is stored in the installation directory of the WatchGuard software (c:\program files\watchguard\certificates\).

Enabling Web-based Management

When you configure a DVCP server, a certificate file is created and sorted in the directory where you installed WatchGuard. For example:

c:\Program Files\WatchGuard\Certificates\[*DVCP Server's IP Address*]\SOHOAdmin

This file must be imported by the browsers that will be used to contact and configure the SOHOs in your IDE.

Importing a Certificate for Microsoft Internet Explorer 5

To configure a Microsoft IE 5.0 Web browser as an administration tool:

- 1 Open an IE 5.0 browser.
- 2 Select **Tools** ⇒ **Internet Options**.
The Internet Options tool appears.
- 3 Click the **Content** tab.
- 4 Click **Certificates**.
The Certificate Manager screen appears.
- 5 Select the **Personal** tab and click **Import**.
This activates the import wizard.
- 6 Click **Next**.
You are prompted for the file name.
- 7 Type the full path to the file, or browse to it. Click **Next**.
- 8 Type the password that encrypts the certificate file.
This is the same as the DVCP server's read-write key.
- 9 Click **Next**.
You are prompted to select a certificate store.
- 10 Let the default selection stand. Click **Next**.
- 11 Click **Finish**.
This screen completes the import process. If you are prompted to accept a certificate as trusted, click Yes.
You should get a message indicating that import is successful.
The imported certificate should show in the Certificate Manager.
The browser is now ready to be enabled for SSL client authentication.
- 12 Select the certificate and click **Advanced**.
You are presented with a list of certificate purposes.

- 13 Check **Client authentication**.
- 14 Click **OK**. Click **Close**. Click **OK** again.

Troubleshooting IE 5.0 certificate setup

If any of the preceding steps fail, check the following:

- Make sure you have the strong encryption (128-bit) version of IE.
- Make sure you have the right password for the .p12 (or .pfx) file. This must be the read-write password of the Firebox that is your DVCP server.
- Make sure the certificate file is not 0 length. If it is, delete it and run VPN Manager again.
- Sometimes, at installation, IE5 does not enable strong encryption. You can check this by looking in the registry. Look at
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Defaults\Provides\001

It should be set to Microsoft Enhanced Cryptographic Provider v1.0. If not, edit the line to fix it manually, and restart the browser.

Certificate Import Process for Netscape 4.75

- 1 Open the Netscape 4.75 browser and click **Security**.
- 2 On the left-side menu, find the **Certificates** heading and click **Yours**.
- 3 Click **Import a Certificate**.
- 4 Browse to the file location and click **Open**.
The Password Entry dialog box appears.
- 5 Enter the read-write password of the DVCP server and click **OK**.
A screen appears that says your certificate has been successfully imported.

Troubleshooting Netscape 4.75 certificate setup

- Make sure you have the strong encryption (128-bit) version of Netscape.

- Make sure you have the right password for the .p12 (or .pfx) file. This must be the read-write password of the Firebox that is your DVCP server.
- Make sure the certificate file is not 0 length. If it is, delete it and run VPN Manager again.

Resetting Certificates

Certain situations might require you to update the certificates that VPN Manager uses. For example, if the Firebox's configuration passphrase is changed, you will need to update the certificate that VPN Manager uses for management sessions. The certificates need to be removed, then new certificates will be generated and used instead. To remove the old certificates, first, in your browser:

- 1 Select **Tools** ⇒ **Internet Options**.
The Internet Options dialog box appears.
- 2 Select the **Control** tab.
- 3 Click **Certificates**.
The Certificates dialog box appears.
- 4 Highlight the certificate or certificates to remove.
- 5 Click **Remove**.
The selected certificates will be deleted from your browser.

After you have removed the old certificates from your browser, in the VPN Manager:

- 1 Select **File** ⇒ **Certificates** ⇒ **Clean up on PC**.
This will delete the VPN Manager's certificates on the computer on which VPN Manager is installed.

Removing Certificates

When you are reinstalling the DVCP server, the certificates associated with the deleted DVCP server must be removed. From the browser in which the certificates were installed:

- 1 Select **Tools ⇒ Internet Options**.
The Internet Options dialog box appears.
- 2 Select the **Control** tab.
- 3 Click **Certificates**.
The Certificates dialog box appears.
- 4 Highlight the certificate or certificates to remove.
- 5 Click **Remove**.
The selected certificates will be deleted from your browser.

After you have removed the old certificates from your browser, in the VPN Manager:

- 1 Select **File ⇒ Certificates ⇒ Clean up on PC**.
This will delete the VPN Manager's certificates on the computer on which VPN Manager is installed.
- 2 Select **File ⇒ Certificates ⇒ Clean up on DVCP Server**.
This will delete the VPN Manager's certificates on the Firebox designated as the DVCP server.
The Firebox reboots and then reconnects to the VPN Manager, entering its certificates in the VPN Manager's Certificates folder.

Adding Devices to VPN Manager

The first step in creating tunnels between devices is to enable each device as a DVCP client. Next, you add the devices to VPN Manager for use as VPN endpoints. VPN Manager makes adding devices straightforward and error-free by launching a wizard to configure each device. For each device, you must know its name or IP address and its configuration (read-write) passphrase.

Enabling Fireboxes as DVCP Clients

VPN Manager automatically configures the DVCP server Firebox as a DVCP client. The only prerequisite is that the WatchGuard service be configured to allow incoming connections from the DVCP server to the Firebox (DVCP client).

From Policy Manager:

- 1 Select the WatchGuard icon in the Services Arena.
- 2 Click **Edit ⇒ Modify Service**.
- 3 Under **From**, click **Add**.
The Add Address dialog box appears.
- 4 Click **Add Other**.
The Add Member dialog box appears.

- 5 From the **Choose Type** drop list, click **Host IP Address**.
- 6 Enter the IP address of the DVCP server in the **Value** box. Click **OK**.
- 7 Under **To**, click **Add**.
The Add Address dialog box appears.
- 8 Click **Firebox**.
The Add Member dialog box appears.
- 9 Click **Add**.
- 10 Click **OK**.

Enabling SOHOs as DVCP clients

NOTE

For a SOHO to be configured as a DVCP client for VPN tunnels, it must have the VPN feature enabled.

To enable a SOHO with a static (not DHCP or PPPoE) IP address as a DVCP client, on the SOHO:

- 1 Browse to the WatchGuard **SOHO Configuration** menu.
The default configuration IP address is 192.168.111.1.
- 2 Click **System Administration**.
The System Administration page appears.
- 3 Click **Remote Configuration**.
The Remote Configuration page appears.
- 4 Enter a read-write and read-only passphrase.
The read-write and read-only passphrases will be used by the DVCP server to communicate with the SOHO.

To enable a SOHO with a dynamically assigned (DHCP or PPPoE) IP address as a DVCP client, on the SOHO:

- 1 Browse to the WatchGuard **SOHO Configuration** menu.
The default configuration IP address is 192.168.111.1.
- 2 Click **Virtual Private Networking**.
The Virtual Private Networking page appears.
- 3 Select **VPN Manager SOHO** from the drop list.
- 4 Click **Configure**.
The VPN Manager SOHO page appears.

5 Check **Enable IPsec Network**.

6 Enter the following:

DVCP Server Address

Enter the IP address of the DVCP server (defined in VPN Manager) to which this device will be a client.

User ID

Use the IP address or any identifying name or number. The same ID must be entered in the VPN Manager when adding the device.

Shared Secret

Enter a passphrase for use between the client and server. The same secret must be entered in the VPN Manager when adding the device.

Adding Devices to VPN Manager

After enabling the devices as DVCP clients, you can now add them to your VPN configuration.

From VPN Manager:

- 1 Select either the **Device** or the **VPNs** tab. Select **Edit ⇒ Insert Device**. The WatchGuard Device wizard appears.
- 2 Click **Next**.
- 3 Enter a display name for the device.
This is a name of your own choosing. It is not tied to the device's DNS name.
- 4 From the **Device Type** drop list, select the device type.
- 5 Enter the host name or IP address.
This is the DNS name, not the name you entered in Step 3.
- 6 Enter the monitoring (read-only) and configuration (read-write) passphrases.
These must be at least seven characters long.
- 7 Set the **Initial Lease Time-out**, if necessary.
This is the amount of time that the configuration is run before the device contacts the DVCP server to see if its configuration has changed.
- 8 Click **Next**.
The wizard displays the DNS and WINS settings for the DHCP window.

- 9 Enter any WINS or DNS server IP addresses you want in your configuration. Click **Next**.
If you are not using DNS or WINS servers, ignore this page, and click Next. The wizard displays the Contact Information page.
- 10 Enter any contact information you want for contacting administrators of this Firebox. Click **Next**.
The information on this panel is optional. The wizard displays the Gather Information and Configure Device information panel.
- 11 Click **Next**.
When finished, the wizard displays the message "New Device Successfully Changed."
- 12 Click **Close**.
The wizard uploads the new configuration to the DVCP server and exits.

Removing a Device from VPN Manager

Removing a device from VPN Manager does not remove it from its associated tunnels. To remove it completely from VPN Manager, you will also have to delete any tunnels for which that device is an endpoint.

Removing Fireboxes

From Policy Manager:

- 1 Select **Network** ⇒ **Enhanced DVCP Client**.
The Enhanced DVCP Client Setup dialog box appears.
- 2 Disable the **Enable This Firebox as a DVCP Client** checkbox.
- 3 Click **OK**.

Removing SOHOs

In VPN Manager, in the **VPNs** tab:

- 1 Expand the **Devices** folder to reveal the SOHO device to be deleted.
- 2 Right-click the device.
- 3 Select **Remove**.

NOTE

Tunnels associated with a deleted device are not deleted from the VPNs tab view. Before deleting the device, manually delete any tunnels associated with a deleted device.

Creating Tunnels Between Devices

A tunnel enables one network to send its data by way of another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

After devices are added to VPN Manager, tunnels can be configured between them. VPN Manager uses a graphical interface that launches the VPN Manager Configuration wizard, which knows the endpoint device IP addresses and their read-write passwords. The wizard uses templates to simplify tunnel creation. The policy template defines what resources will be accessible through the tunnel, to the other endpoint. The security template defines the encryption level and authentication method to be used. When you finish the wizard, it creates the new tunnel.

NOTE

A SOHO device, with VPN enabled, can be configured for a maximum of five tunnels.

Adding Policy Templates

One of the benefits of a VPN is that you can define (and limit) the networks that are accessible through the tunnel: A VPN can be created between only two hosts or between multiple networks — or any combination in between. To define the networks available through a given VPN device, you create policy templates. By default, VPN Manager provides a Trusted network policy template, which allows access to the Trusted network behind the VPN device to which the policy is applied. To create a policy template, on the VPNs tab:

- 1 Highlight the device for which you want to define a policy template.
- 2 Right-click and select **Insert Policy** or click the Insert Policy Template icon.
The Device Policy dialog box for that device appears.
- 3 Enter a policy name of your choosing.
- 4 Configure the networks accessible through this policy template. This is also known as the bypass rule (the type of IPSec policy applied to the VPN tunnel):
 - **Block** — IPSec will not allow traffic that matches the rule in associated tunnel policies.
 - **Bypass** — IPSec will not encrypt any traffic between the two hosts (this cannot be used if the hosts are networks).
 - **Secure** — IPSec will encrypt all traffic that matches the rule in associated tunnel policies.
- 5 Click **Add** to define the accessible resources for the device.
The Resource dialog box appears.
- 6 Select the type of resource (host or network) from the **Allow To/From** menu.
- 7 Enter the resource's IP address (for host) or network address (for network). Click **OK**.
- 8 Click **OK**.
The policy template has been defined. It can now be selected in the VPN wizard when creating a VPN tunnel involving that device.

Adding Security Templates

Default security templates are provided for available encryption levels. New templates can also be created. A variety of security templates makes it easy to match the appropriate level of encryption and type of authentication to the tunnel created with the Configuration wizard.

From the VPN Manager display:

- 1 Click the **VPN** tab.
- 2 Right-click anywhere in the window, and select **Insert Security Template**.
The Security Template dialog box appears.
- 3 Enter the template name, SAP (security authorization packet) type (either ESP or AH), authentication, and encryption.
- 4 If you want to force key expiration, enable the corresponding checkbox, and then specify either kilobytes or hours.
The security template has been defined. It can now be selected in the VPN wizard when creating a VPN tunnel involving that device.
- 5 Click **OK**.

Connecting Devices

There is more than one way to designate endpoints in a tunnel and work through the VPN Manager Configuration wizard. Here are two ways to create a tunnel.

Drag-and-drop tunnel creation

NOTE

This method cannot be used to create tunnels for dynamically addressed SOHO devices.

From VPN Manager:

- 1 Click the **Device** tab.

- 2 Click the device name of one of the tunnel endpoints to highlight it and drag it to the device name of the other tunnel endpoint.
This launches the VPN Manager Configuration wizard, starting with the dialog box that shows (in two list boxes) the two endpoint devices you selected using drag-and-drop.
- 3 For each device (endpoint), select a policy template from the drop list.
The policy template determines the resources available through the tunnel. Resources can be a network or a host.
The listbox displays any policy templates you have added to VPN Manager.
- 4 Click **Next**.
The wizard displays the Security Policy dialog box.
- 5 Select the security template appropriate for the level of security and type of authentication to be applied to this tunnel.
The listbox displays any templates you have added to VPN Manager.
- 6 Click **Next**.
The wizard displays the DVCP configuration.
- 7 Enable the checkbox labeled **Restart devices now to download VPN configuration**. Click **Finish** to restart the devices and deploy the VPN tunnel.

NOTE

If you are configuring a large number of devices, you can delay restarting the devices until you have created all the tunnels. To restart any device, right-click it and select Restart. Or you can wait until a given device's lease expires, at which time VPN Manager uploads the new configuration automatically.

Menu-driven tunnel creation

NOTE

This method must be used to create tunnels for dynamically addressed SOHO devices.

Follow these steps from VPN Manager:

- 1 Click the **VPNs** tab.

- 2 **Select Edit => Create a New VPN.**
This launches the VPN Manager Configuration wizard.
- 3 **Click Next.**
The wizard displays two listboxes that each list all the devices registered in VPN Manager. You will be selecting one device from each listbox as endpoints of a tunnel.
- 4 **Select a device from each listbox as endpoints of the tunnel you are setting up.**
- 5 **Select the policy templates for each device's end of the tunnel.**
The listbox displays any templates that you have added to VPN Manager.
- 6 **Click Next.**
The wizard displays the Security Template dialog box.
- 7 **Choose the security template you want for this VPN. Click Next.**
The wizard displays the DVCP configuration.
- 8 **Enable the checkbox labeled **Restart devices now to download VPN configuration**. Click **Finish** to restart the devices and deploy the VPN tunnel.**

NOTE

If you are configuring a large number of devices, you can delay restarting the devices until you have created all the tunnels. To restart any device, right-click it and select Restart. Or you can wait until a given device's lease expires, at which time VPN Manager uploads the new configuration automatically.

Enabling a SOHO Single-Host Tunnel

Any SOHO (static or dynamic) can be configured for a tunnel that allows only one host behind the SOHO to connect to another endpoint (host or networks). This tunnel is called a SOHO Telecommuter tunnel and is useful for situations where an entire family's network is behind a SOHO, but only one computer — the telecommuter — should be allowed access to corporate resources available via the tunnel. On the SOHO:

- 1 **Browse to the WatchGuard **SOHO Configuration** menu.**
The default configuration IP address is 192.168.111.1.

- 2 Click **Virtual Private Networking**.
The Virtual Private Networking page appears.
- 3 Select **VPN Manager Telecommuter** from the drop list.
- 4 Click **Configure**.
The VPN Manager Telecommuter page appears.
- 5 Check **Enable IPSec Network**.
- 6 Enter the following:

DVCP Server Address

Enter the IP address of the DVCP server (defined in VPN Manager) to which this device will be a client.

User ID

Use the IP address or any identifying name or number. The same ID must be entered in the VPN Manager when adding the device.

Shared Secret

Enter a passphrase for use between the client and server. The same secret must be entered in the VPN Manager when adding the device.

Private IP Allowed to Use VPN

Enter the IP address of the trusted host behind the SOHO (the telecommuter's computer).

Creating a Policy for a Telecommuter

A SOHO that has been enabled for a VPN Manager Telecommuter tunnel does not have an associated policy. A policy must be created for this device in the VPN Manager. On the VPNs tab:

- 1 Under the **Devices** folder, select the device.
- 2 Right-click the device and select **Insert Policy**.
The Device Policy dialog box appears.
- 3 Enter the following:

Policy Name

Enter a friendly name of your choosing.

Type

Select **Telecommuter Tunnel** from the drop list.

Virtual IP Address Behind the Firebox

Enter a free IP address on the Trusted network of the remote Firebox to which the SOHO is connecting.

Private IP Allowed to Use Tunnel

Enter the IP address of the trusted host behind the SOHO (the telecommuter's computer). Use the same address entered on the SOHO VPN configuration.

Removing or Changing a Tunnel

After a tunnel has been created, it will be visible on the VPNs tab of the VPN Manager. The VPN Manager allows tunnel resources on an existing VPN to be edited. You may also want to remove a tunnel that is no longer used.

Editing a tunnel

The VPN Manager allows the tunnel name, security template, endpoints, and the policy used to be edited on an existing tunnel. On the VPNs tab:

- 1 Expand the tree to show the device and its policy that you want to edit.
- 2 Highlight the tunnel that you want to edit.
- 3 Right-click and select **Properties**.
- 4 You can modify:

VPN Tunnel

The name used to identify this tunnel

Security Template

Used to define the security for this tunnel

Devices

Defined as endpoints for this tunnel

Policy Template

Used to define the resources available (for a given endpoint of this tunnel)

- 5 Click **OK** to save the change.
When the tunnel is renegotiated, the changes will be applied.

Removing a tunnel

To remove a tunnel, on the VPNs tab:

- 1 Highlight the tunnel on the **VPNs** tab.
- 2 Select **Edit => Remove**.

Editing a policy template

If resources defined for a given endpoint and/or tunnel need to be altered, you can do so without having to delete the tunnel. To edit the policy, on the VPNs tab:

- 1 Under the **Devices** folder, select a policy.
- 2 Right-click and select **Properties**.
The Policy dialog box appears.
- 3 You can modify the resources in the following ways:

Edit

To alter an already-defined resource

Add

To add a new resource

Remove

To delete an already-defined resource

Using the VPN Manager User Interface

You use the VPN Manager user interface to view real-time information on all managed devices simultaneously. This information is used to determine current device status, to diagnose problems, and to plan how various devices need to be configured or reconfigured.

Opening the VPN Manager Display

To open VPN Manager, from the Windows interface:

- 1 Select **Start ⇒ Programs ⇒ WatchGuard ⇒ VPN Manager**.
This displays a blank VPN Manager user interface:
- 2 Select **File ⇒ Connect** or select the Connect icon from the toolbar.
- 3 Enter the name or IP address of the DVCP server and the Firebox read-write password. Click **OK**.
VPN Manager connects to the DVCP server and displays the VPN and device configuration, distributed appropriately among the four tabs on the display.

Viewing Device Status

Click the **Devices** tab of the VPN Manager Display to view the real-time status of all devices being managed by DVCP.

Tree-view structure

All devices appear in a tree-view structure. When the box next to an entry contains a plus sign (+), the tree is collapsed. To expand it, click the plus sign. The tree view expands at that entry to display the properties of that device.

To collapse the display, click the minus sign (–) next to a device. The expanded tree disappears, leaving a single-line entry for that device.

The display is structured as follows:

- Device Name
- Statistics folder
- Log Host
- Up Time
- Number of connections
- Authenticated Users
- External MAC
- # of packets sent
- # of packets received
- Trusted MAC
- # of packets sent
- # of packets received
- Optional MAC
- # of packets sent
- # of packets received

- Branch Office VPN Tunnel folder
- Tunnel Name/Encryption
- Bytes Sent
- Bytes Received
- Renegotiation
- Authentication
- Remote User VPN Folder

Connection status

The top level of the tree view for each device will show a red, yellow, or no exclamation point. The exclamation point (or lack of it) provides the

device's status, even when the tree view is not expanded. The statuses indicated are as follows:

No exclamation point

Normal operation. The device is connected to the VPN Manager.

Yellow exclamation point

Questionable operation. VPN Manager is trying to contact the device. The exclamation point will either resolve or turn red.

Red exclamation point

Failed operation. The device is no longer connected to the VPN Manager. Right-click the device, and select **Resume Connection**. If this fails to resolve the situation, examine the devices for other problems.

Context menu options

Right-clicking a device in the Device tab presents the following functionality:

Create a new VPN

Another means of starting the VPN wizard, to quickly create a VPN between identified devices.

Update Device

Allows updating of network policies, resetting of the DVCP server configuration, and expiration of the lease.

Insert Device

Allows configuration of a new device to be added to the VPN Manager view.

Remove

Remove the selected device.

Properties

View the properties of the selected device, as configured in the VPN Manager's Device wizard.

Pause/Resume Connection

Pause or resume VPN Manager's connection and any tunnels to the device (available option depends on device status).

Policy Manager

Open Policy Manager for the device selected.

SOHO Configuration

Open the SOHO device's configuration (for SOHO devices only).

Firebox Monitors

View Firebox Monitors for the device selected.

Log Viewer

View LogViewer for the device selected.

HostWatch

View HostWatch for the device selected.

Historical Reports

View Historical Reports for the device selected.

Front Panel

View the Security Triangle Display for the device selected.

Copy to Custom tab

Copy the device to the Custom tab view.

Viewing Tunnels

Click the VPNs tab of the VPN Manager Display to view IPsec tunnels configured for devices under management. This portion of the display shows the currently configured VPN tunnels, devices, and default security templates for each of the available encryption levels.

The display is structured as follows:

- Managed VPNs folder
- List of managed tunnels
- Endpoint device names and related policies
- Devices folder
- Device Name
- Associated Policies
- Security Templates folder
- List of security templates
- Security Association Type
- Encryption Type
- Authentication Type

Viewing Log Servers

Click the Logging tab of the VPN Manager Display to view log servers in the IDE. The list of servers in use is compiled from the configuration files of the devices under management.

The display is structured as follows:

- Log Servers Folder
- Log Server Name or IP
- Log Server's Associated Device(s)
- Devices Not Currently Logging
- Associated Device(s)

Creating a Custom View

The Custom tab of the VPN Manager Display allows the creation of a customized workspace, optimized to your specific needs. Any of the resources in the Devices view can be listed on the Custom tab by tunnel location, level of encryption, device type used, and so on. The Firebox devices themselves (with all their corresponding settings and tunnel statistics), individual device statistics, individual tunnels, and individual remote users from any device can all be monitored. You can also create folders to group information in a way that is meaningful for your own environment.

To add devices to the **Custom** tab:

- 1 In the **Device** tab of the VPN Manager display, right-click the device you want to add to the **Custom** tab.
- 2 Select the **Copy to Custom** tab.
- 3 On the **Custom** tab, drag and drop the device into the desired location or folder in the tree view.

To add a folder on the **Custom** tab:

- 1 Right-click in the **Custom** tab window.
- 2 Select **Add New Folder**.
- 3 Double-click the name of the folder to select it.
- 4 Type a name of your choosing.
- 5 Click elsewhere to save the change.

Launching Applications from VPN Manager

Use the VPN Manager display to launch all WatchGuard Firebox System applications: Policy Manager, LogViewer, Report Generator, and WatchGuard Security Event Processor.

To launch any of these applications:

- 1 On the toolbar of the VPN Manager display, click the appropriate icon.

These are identical to the ones in the Control Center.

You can also select Tools => *Application*, where *Application* is the program you want to launch.

Using Remote Administration

VPN Manager allows you to manage and configure devices remotely. This is especially helpful when working with a SOHO to set up a tunnel for an employee working offsite at a distant office or their home.

To manage a SOHO remotely, you need to have certificates enabled on your Web browser. For more information, see Chapter 3, “Setting Up Certificates on Web Browsers.”

Starting the Remote Management Feature

- 1 From the toolbar on the VPN Manager display, highlight the device you want to monitor and then click the SOHO Management icon on the toolbar (to the right of the Policy Manager icon).
The Client Authentication dialog box appears.
- 2 Select the certificate for this device and click **OK**.
A dialog box appears telling you that an application is requesting access to a protected item.
- 3 Click **OK**.
The Remote Management screen appears in your Web browser.

System administration

The System Administration section allows you to:

- Configure system passwords
- Configure remote logging and configuration
- Configure DMZ settings
- View the configuration of the device

System password

To view system password options, click **System Password**. Here you set the password for the SOHO and assign an administrator's name to the device.

Remote logging

To view remote logging options, click **Remote Logging**.

To activate this option:

- 1 Click **Enable Remote Logging**.
- 2 Enter the log server IP address and the passphrase. Click **Submit**.

Remote configuration

To view remote configuration options, click **Remote Configuration**. To enable this option, enter the passphrases and click **Submit**.

DMZ settings

To view DMZ settings, click **DMZ Settings**.

The demilitarized zone (DMZ) is an open area of your network where you allow information to pass unrestricted. To enable the option for this device, enter the information and click **Submit**.

View configuration

To view the configuration file for this device, click **View configuration**.

The detail of the configuration file is shown.

Services

To configure services for this device, click **Services**. The services screen appears.

Incoming services

Click **Allowed Incoming Services**.

Allowed incoming services

At this point you can either add or remove a service. To add a service click **Add a Service**. All the services listed in the Firebox System 5.0 Policy Manager are also available for this device. The difference is that you do not have the device directly in front of you. Click any of the selections to add them to this device.

Block outgoing services

You also have the option to block outgoing services on this device. Services such as SMB Networking, TCP or UDP services, and protocols can be blocked from here. You can also remove any blocking that was set up.

The default for blocking outgoing services is like that for the Firebox: no services are automatically blocked. You must specifically designate which services to block.

Private network

To view the private network settings click **Private Network**. The Private Network screen appears and lists the settings for the private network you are using.

Public network

To view the public network settings, click **Public Network**. You see this screen and the details of the public network.

If this device is connected using a PPOE client (this is generally a DSL connection) the PPOE information is completed.

System information

To view the system information for this device, click **System Information**. This screen provides links to features and the software version this device is using, network statistics, and the event log.

Features and Version Information

This screen details the firmware installed on this device. You also see whether or not WebBlocker is enabled.

Network Statistics

This screen details information about the network you are using. The IP address, public, and private networks are listed.

Event log

This screen shows behind-the-scenes detail for this device.

Index

C

- certificate authority 9
- certificates
 - described 9
 - for IE 5.0 10
 - for Netscape 4.75 11
 - removing 13
 - resetting 12

D

- devices
 - adding 15, 17
 - connecting 23
 - connecting to a tunnel 23
 - managing remotely 35
 - removing 18
 - viewing status 30
- dialog boxes
 - Enhanced DVCP Client Setup 18
 - New Server 8
 - Security Policy 24
 - Security Template 25
- DVCP
 - described 2, 7
 - device and tunnel management 5
 - how it works 4
 - server 5, 7, 9
- DVCP clients
 - enabling Fireboxes as 15
 - enabling SOHOs as 16
- Dynamic VPN Configuration Protocol. See DVCP

E

- Enhanced DVCP Client Setup dialog box 18

F

- Fireboxes
 - defining as DVCP servers 7
 - designating as DVCP server 4
 - enabling as DVCP clients 15

I

- IDE 2, 33
 - described 2
 - planning 5
- IE 5.0
 - enable strong encryption 11
 - importing certificate 10
- Internet Distributed Enterprise. See IDE.
- IPSec, with DVCP 4
- IPSec tunnels 1

L

- log servers, viewing 33

N

- New Server dialog box 8

P

- policy templates
 - adding 22
 - editing 28

R

- remote management 35

S

- Security Policy dialog box 24
- Security Template dialog box 25
- security templates, adding 23
- SOHOs

- enabling as DVCP clients 16
- managing remotely 35
- maximum tunnels 21
- tunnels 25

structure of VPN Manager display 30

W

Web-based management 10

T

tunnels

- changing 27
- creating 1
- described 21
- drag-and-drop creation 23
- editing 27
- IPSec 1
- menu-driven creation 24
- removing 28
- SOHO maximum 21
- SOHO single-host 25
- viewing 32
- with DVCP 4

V

virtual private networks. See VPNs

VPN Manager 1

- adding devices 15, 17
- adding policy templates 22
- and IDE 5
- appliances 2
- certificates in 9
- configuration 5
- configuring 4
- described 1
- description 2
- display structure 30
- features of 3
- launching applications 34
- opening UI 29
- physical description 3
- removing or changing a tunnel 27
- viewing device status 30
- viewing log servers 33
- viewing tunnels 32

VPNs

- centrally managing devices 2
- described 1
