

WatchGuard® VPN Guide

WatchGuard Firebox® System 6.0



Notice to Users

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

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2002 WatchGuard Technologies, Inc. All rights reserved.

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

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

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

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

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

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

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

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

© 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
- THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

All rights reserved.

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

The implementation was written so as to conform with Netscapes SSL.

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

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

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

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

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

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

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

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

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

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

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

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

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

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

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

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

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

The Apache Software License, Version 1.1
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

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

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

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

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.
Part No: 1200148

WatchGuard Technologies, Inc. VPN Manager Software End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This VPN Manager End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD optional software product for the WatchGuard Firebox System you have purchased, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "OPTIONAL SOFTWARE PRODUCT"). WATCHGUARD is willing to license the OPTIONAL SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing, activating or using the OPTIONAL SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the OPTIONAL SOFTWARE PRODUCT to you, and you will not have any rights in the OPTIONAL SOFTWARE PRODUCT. In that case, promptly return the OPTIONAL SOFTWARE PRODUCT/license key certificate, along with proof of payment, to the authorized dealer from whom you obtained the OPTIONAL SOFTWARE PRODUCT/license key certificate for a full refund of the price you paid.

1. **Ownership and License.** The OPTIONAL SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement

and NOT an agreement for sale. All title and copyrights in and to the OPTIONAL SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the OPTIONAL SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the OPTIONAL SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the OPTIONAL SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the OPTIONAL SOFTWARE PRODUCT:

(A) You may install and use the OPTIONAL SOFTWARE PRODUCT on that number of WATCHGUARD hardware products (or manage that number of WATCHGUARD hardware products) at any one time as permitted in the license key certificate that you have purchased and may install and use the OPTIONAL SOFTWARE PRODUCT on multiple workstation computers. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the OPTIONAL SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(B) To use the OPTIONAL SOFTWARE PRODUCT on more WATCHGUARD hardware products than provided for in Section 2(A), you must license additional copies of the OPTIONAL SOFTWARE PRODUCT as required.

(C) In addition to the copies described in Section 2(A), you may make a single copy of the OPTIONAL SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the OPTIONAL SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the OPTIONAL SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the OPTIONAL SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the OPTIONAL SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the OPTIONAL SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the OPTIONAL SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to us with a dated proof of purchase.

(B) OPTIONAL SOFTWARE PRODUCT. The OPTIONAL SOFTWARE PRODUCT will materially conform to the documentation that accompanies it or its license key certificate. If the OPTIONAL SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the OPTIONAL SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the OPTIONAL SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE OPTIONAL SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE OPTIONAL SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION,

ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE OPTIONAL SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE OPTIONAL SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE OPTIONAL SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5.United States Government Restricted Rights. The OPTIONAL SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

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

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

8.Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the OPTIONAL SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the OPTIONAL SOFTWARE PRODUCT AND BY USING THE OPTIONAL SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD

Contents

CHAPTER 1 Introduction to VPN Technology	1
Tunneling Protocols	2
IPSec	2
PPTP	3
Encryption	3
Authentication	4
Extended authentication	4
Internet Key Exchange (IKE)	4
WatchGuard VPN Solutions	5
Mobile User VPN	6
RUVPN with PPTP	7
RUVPN with extended authentication	8
Branch Office Virtual Private Network (BOVPN)	8
CHAPTER 2 Designing a VPN Environment	13
Selecting an Authentication Method	13
Selecting an Encryption and Data Integrity Method	14
IP Addressing	14
NAT and VPNs	15
Access Control	15

Split Tunneling	16
Network Topology	16
Meshed networks	16
Hub-and-spoke networks	18
Determining Which WatchGuard VPN Solution to Use	19
VPN Installation Services	21
VPN Scenarios	21
Large company with branch offices: VPN Manager	22
Medium-sized company with main office and auxiliary office: BOVPN with Basic DVCP	22
Small company with telecommuters: MUVPN	23
Company with remote employees: MUVPN with extended authentication	24
CHAPTER 3 Activating the Certificate Authority on the Firebox	27
Public Key Cryptography and Digital Certificates	27
PKI in a WatchGuard VPN	28
Defining a Firebox as a DVCP Server and CA	31
Managing the Certificate Authority	34
Managing certificates from the CA Manager	36
Restarting the CA	36
CHAPTER 4 Configuring RUVPN with PPTP	39
Configuration Checklist	39
Encryption levels	40
Configuring WINS and DNS Servers	41
Adding New Users to Authentication Groups	42
Configuring Services to Allow Incoming RUVPN Traffic	44
By individual service	44
Using the Any service	45
Activating RUVPN with PPTP	46
Enabling Extended Authentication	46
Entering IP Addresses for RUVPN Sessions	47
Configuring Debugging Options	47
Preparing the Client Computers	48

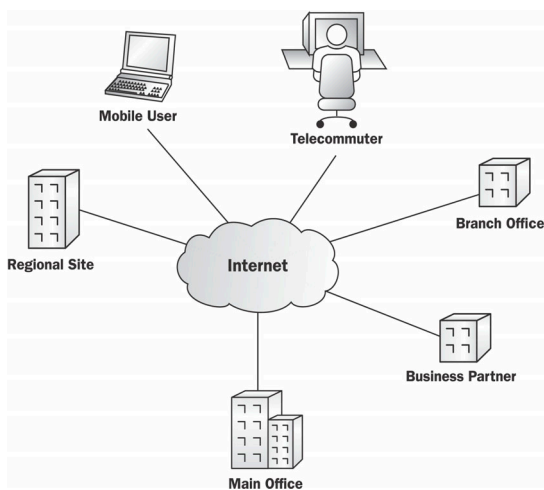
Installing MSDUN and Service Packs	48
Windows 98 Platform Preparation	49
Windows NT Platform Preparation	51
Windows 2000 Platform Preparation	53
Windows XP Platform Preparation	54
Starting RUVPN with PPTP	55
Running RUVPN and Accessing the Internet	55
Making Outbound PPTP Connections From Behind a Firebox	56
CHAPTER 5 Preparing to Use MUVPN	57
Purchasing a Mobile User VPN license	57
Entering License Keys	58
Configuring WINS and DNS Servers	59
Preparing Mobile User VPN Profiles	59
Defining a User for a Firebox Authenticated Group	60
Modifying an existing Mobile User VPN entry	62
Allowing Internet access through MUVPN tunnels	63
Defining an Extended Authentication Group	63
Setting Advanced Preferences	66
Configuring Services to Allow Incoming MUVPN Traffic	67
By individual service	68
Using the Any service	69
Regenerating End-User Profiles	69
Saving the Profile to a Firebox	69
Distributing the Software and Profiles	70
Making Outbound IPSec Connections From Behind a Firebox	71
Configuring Debugging Options for MUVPN	71
Terminating IPSec Connections	72
CHAPTER 6 Configuring BOVPN with Basic DVCP ..	73
Configuration Checklist	73
Creating a Tunnel to a Device	74
Editing a tunnel to a device	76

Removing a tunnel to a device	76
Configuring Logging for a DVCP Server	77
CHAPTER 7 Configuring BOVPN with Manual IPSec	79
Configuration Checklist	79
Configuring a Gateway	80
Creating a Tunnel with Manual Security	83
Creating a Tunnel with Dynamic Key Negotiation	86
Creating a Routing Policy	88
Changing IPSec policy order	90
Configuring multiple policies per tunnel	90
Configuring services for BOVPN with IPSec	90
CHAPTER 8 Configuring IPSec Tunnels with VPN Manager	93
Defining a Firebox as a DVCP Server and CA	94
Installing VPN Manager	94
Launching VPN Manager	95
Adding Devices to VPN Manager (Dynamic Devices Only)	95
Updating a device's settings	96
Defining a Firebox as a DVCP Client (Dynamic Fireboxes Only)	97
Adding Policy Templates	98
Adding resources to a policy template	99
Adding Security Templates	99
Creating Tunnels Between Devices	100
Drag-and-drop tunnel creation	100
Menu-driven tunnel creation	101
Enabling a SOHO Single-Host Tunnel	102
Editing a Tunnel	104
Removing Tunnels and Devices from VPN Manager	105
Removing a tunnel	105
Removing a device	105
Allowing Remote Access to the DVCP Server	106

CHAPTER 9 Monitoring VPN Devices and Tunnels	107
Monitoring VPNs from Control Center	107
Branch Office VPN tunnels	108
MUVPN and RUVPN tunnels	109
Monitoring VPNs through VPN Manager	110
Opening the VPN Manager Display	110
Device Status	110
Connection status	111
Tunnel status	112
Log server status	112
Creating a custom view	113
CHAPTER 10 Managing the SOHO with VPN Manager	115
Importing Certificates	115
MS Internet Explorer 5.5 and 6.0	116
Netscape Communicator 4.79	117
Netscape 6	117
Accessing the SOHO	118
System Status	119
Network	119
Administration	119
Firewall	120
Logging	120
WebBlocker	120
VPN	120
Removing Certificates	121
MS Internet Explorer 5.5 and 6.0	121
Netscape Navigator 4.79	122
Netscape 6	122
 Index	 123

Introduction to VPN Technology

The Internet is a technical and social development that puts a multitude of information at your fingertips. On this worldwide system of networks, a user at one computer can get information from any other computer. The benefits of using the Internet to exchange information and conduct business are enormous. Unfortunately, so are the risks. Because data packets traveling the Internet are transported in plain text, potentially anyone can read them and place the security of your network in jeopardy.



Virtual private networking technology counters this threat by using the Internet's vast capabilities while reducing its security risk. A virtual private network (VPN) allows communication to flow across the Internet between two networks or between a host and a network in a secure manner. The networks and hosts at the endpoints of a VPN are typically corporate headquarters, branch offices, remote users, telecommuters, and traveling employees. User authentication verifies the identity of both the sender and the receiver. Data sent by way of the Internet is encrypted such that only the sender and the receiver of the message can see it in a clearly readable state.

For more information on VPN technology, see the online support resources at <http://support.watchguard.com>. The main page contains links to basic FAQs, advanced FAQs, and the WatchGuard User's Forum.

Tunneling Protocols

Tunneling—the foundation of VPN implementations—is the transmission of private data through a public network, generally the Internet. Tunneling involves encrypting and encapsulating data and protocol information within units called IP packets. The “tunnel” is the path that the IP packets travel over the Internet. A tunnel is also defined by its start and end points, the type of authentication and encryption used, and the users allowed to use it.

Tunneling protocols provide the infrastructure of virtual private networking. These sets of rules govern how data transmission occurs. Two tunneling protocols widely in use today are Internet Protocol Security (IPSec) and Point-to-Point-Tunneling Protocol (PPTP).

IPSec

The Internet Engineering Task Force (IETF) developed the IPSec protocol suite as a security mechanism to ensure the confidentiality and authenticity of IP packets. IPSec functionality is based on modern cryptographic technologies, providing extremely strong data authentication and privacy. IPSec makes secure communication possible over the Internet, and IPSec standards allow interoperability between VPN solutions.

A major benefit of IPSec is its interoperability. Instead of specifying a proprietary method for performing authentication and encryption, it works with many systems and standards.

IPSec includes two protocols to deal with issues of data integrity and confidentiality when securing data across the Internet. The AH (Authentication Header) protocol handles data integrity, and the ESP (Encapsulated Security Payload) protocol solves both data integrity and confidentiality issues.

PPTP

PPTP is a widely accepted networking technology that supports VPNs, allowing remote users to access corporate networks securely across the Microsoft Windows operating systems and other point-to-point protocol (PPP)-enabled systems. Although PPTP is not as secure as IPSec, it provides a low-cost, private connection to a corporate network that is easy to implement.

Encryption

In general, intruders can intercept transmitted packets in a network fairly easily and read their contents. VPNs use encryption to keep data confidential as it passes over the Internet to the authorized recipient.

Encryption level is determined by the length of the encryption key. The longer the key, the stronger the encryption level, and the greater the measure of security provided. The level of encryption used in a particular instance depends on the performance and security requirements of the tunnel. Stronger encryption provides a greater level of security but impacts performance. For general-purpose tunnels, over which no sensitive data is to be passed, base encryption provides adequate security with good throughput. For administrative and transactional connections, where exposure of data carries a high risk, strong encryption is recommended.

Within a VPN, after the end points on a tunnel agree upon an encryption scheme, the tunnel initiator encrypts the packet and encapsulates it in an

IP packet. The tunnel terminator recovers the packet, removes the IP information, and then decrypts the packet.

Authentication

An important aspect of security for a VPN is confirming the identity of all communicating parties. Two ways of ensuring identity are password authentication (also called shared secrets) and digital certificates. A shared secret is a passphrase or password that is the same on both ends of a tunnel. The data is encrypted using a session key, which is derived from the shared secret. The gateways can encrypt and decrypt the data correctly only if they share the same secret. Digital certificates use public key-based cryptography to provide identification and authentication of end gateways.

For more information on certificates, see Chapter 3, “Activating the Certificate Authority on the Firebox.”

In addition to identifying the user, authentication also defines the resources a user can access. A user must present specified credentials before being allowed access to certain locations on the network.

Extended authentication

Authentication can either take place through a firewall or through an external authentication server such as Remote Authentication Dial-In User Service (RADIUS). An authentication server is a trusted third party that provides authentication services to other systems on a network.

Internet Key Exchange (IKE)

As the number of VPN tunnels between Fireboxes and other IPSec-compliant devices grow, maintaining the large number of session keys used by tunnels becomes a challenge. Keys must also change frequently to ensure the security of each VPN connection.

Internet Key Exchange (IKE)—the key management protocol used with IPSec—automates the process of negotiating and changing keys. IKE implements a security protocol called Internet Security Association and Key Management Protocol (ISAKMP), which uses a two-phase process for establishing an IPSec tunnel. During Phase 1, two gateways establish a secure, authenticated channel for communication. Phase 2 involves an exchange of keys to determine how the data between the two will be encrypted.

Diffie-Hellman is an algorithm used in IKE to negotiate keys required for data encryption. Diffie-Hellman groups are collections of parameters used to achieve the negotiation. These groups allow two peer systems that have no prior knowledge of one another to publicly exchange and agree on a shared secret key. Group 1 is a 768-bit prime modulus group, and group 2 is a 1024-bit prime modulus group—the difference is in the number of bits used for exponentiation to generate private and public keys. Group 2 is more secure than group 1, but requires more time to compute the keys.

WatchGuard VPN Solutions

The WatchGuard Firebox System offers several methods to provide secure tunnels:

- Mobile User VPN
- Remote User VPN with PPTP
- Branch Office VPN with Basic DVCP
- Branch Office VPN with Manual IPSec
- IPSec tunneling with VPN Manager

WatchGuard offers three different levels of encryption: base, medium, and strong. Base encryption uses a 56-bit encryption key for the Data Encryption Service (DES) algorithm to encrypt data. Medium encryption uses a 112-bit key for TripleDES, and strong encryption uses a 168-bit key for TripleDES.

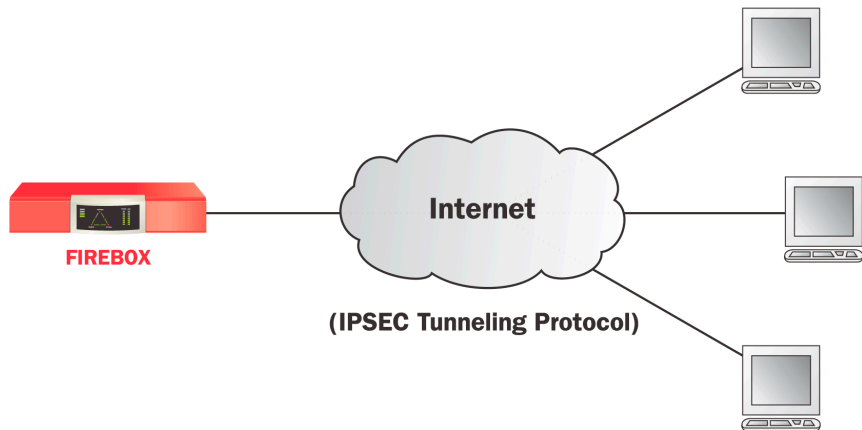
Mobile User VPN

Telecommuters working from home and traveling employees who need corporate network access are common fixtures in today's business environment. Mobile User VPN (MUVPN) creates an IPSec tunnel between an unsecured remote host and your trusted and optional networks using a standard Internet dial-up or broadband connection without compromising security. This type of VPN requires only one Firebox for the private network and the Mobile User VPN software module, which is an optional feature of the WatchGuard Firebox System.

MUVPN uses IPSec with DES or 3DES-CBC to encrypt incoming traffic and MD5 or SHA-1 to authenticate data packets. You create a security policy configuration and distribute it along with the MUVPN software to each telecommuter. After the software is installed on the telecommuters' computers, they have a secure way to access corporate resources. MUVPN users can modify their security policy, or you can restrict them such that they have read-only access to the policy.

Certificate-based authentication is supported for MUVPN tunnels. This functionality requires that you configure a Firebox as a DVCP server. DVCP is described in "BOVPN with Basic DVCP" on page 9.

Mobile User VPN is available on all Firebox models including the SOHO. Firebox 1000 and 2500 each include a five-user license, and the Firebox 4500 includes a 20-user license. Additional licenses can be added in 5-, 20-, 50-, and 100-pack increments. Large enterprise site licenses are also available.



MUVPN tunnels

MUVPN with extended authentication

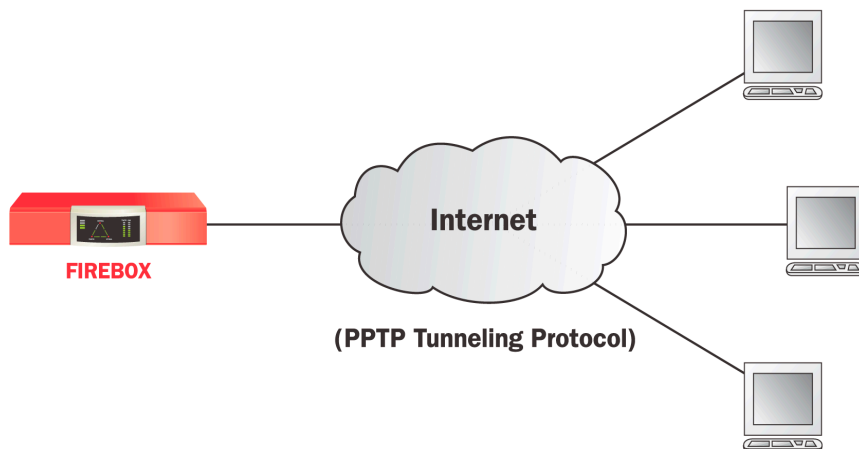
Using MUVPN with extended authentication, users can authenticate to a Windows NT or RADIUS authentication server. Instead of validating against its own data, the Firebox validates users against the third-party server. No usernames or passwords need to be configured on the Firebox.

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.

RUVPN with PPTP

Remote User VPN (RUVPN) fulfills the same purpose as MUVPN by allowing a remote user to connect to the main office by way of the Internet. However, RUVPN provides a way for telecommuters or travelling employees to connect to the Firebox Trusted network using PPTP instead of IPSec.

RUVPN with PPTP is included with the basic WatchGuard Firebox System package. It supports up to 50 concurrent sessions per Firebox and works with any Firebox encryption level.



RUVPN with PPTP tunnels

RUVPN with extended authentication

Using RUVPN with extended authentication, users can authenticate to a RADIUS authentication server. Instead of validating against its own data, the Firebox validates users against the third-party authentication server instead. No usernames or passwords need to be loaded onto the Firebox.

Branch Office Virtual Private Network (BOVPN)

Many companies have geographically separated offices that need to pass data to one another or access a common database. For example, in a retail chain, each location may need to check inventory in the same centrally located warehouse.

Because branch office communications involve sensitive company data, secure exchange of information is particularly important. Using WatchGuard Branch Office VPN (BOVPN), you can connect two or more locations over the Internet while still protecting the resources of your trusted and optional networks. WatchGuard BOVPN creates a secure

tunnel between two networks protected by the WatchGuard Firebox System or between a Firebox and another IPSec-compliant device.

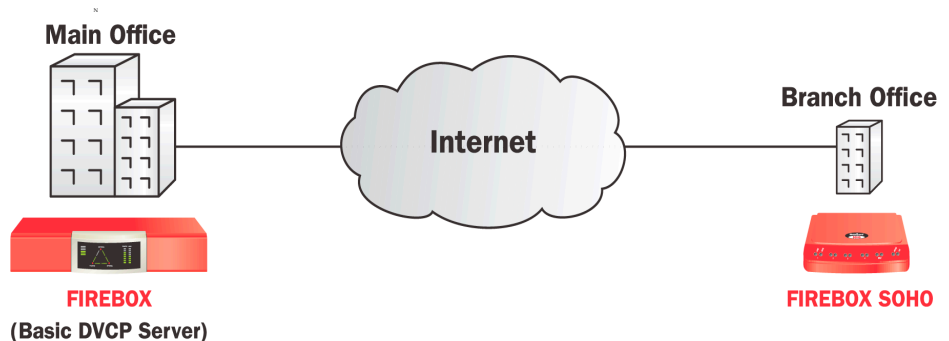
Certificate-based authentication is supported for BOVPN tunnels. This functionality requires that you configure a Firebox as a DVCP server and a certificate authority, as described in the next section and in Chapter 3, “Activating the Certificate Authority on the Firebox.”

BOVPN with Basic DVCP

Dynamic VPN Configuration Protocol (DVCP) is a WatchGuard client server embedded in every WatchGuard Firebox. DVCP simplifies the creation of IPSec tunnels and keeps the user from creating unworkable configurations.

The primary mode of DVCP—Basic DVCP—is used to establish secure IPSec tunnels between Fireboxes and SOHOs. (Standard DVCP establishes tunnels between devices in VPN Manager, as described in “IPSec tunnels with VPN Manager” on page 10.)

BOVPN with Basic DVCP requires that you define a Firebox as a DVCP server. This server sits at the center of a distributed array of DVCP clients—SOHOs and SOHO | Telecommuters. The DVCP server maintains the connections between two devices by storing all policy information—including network address range and tunnel properties such as encryption, timeouts, and authentication. DVCP clients can retrieve this information from the server. The only information clients need to maintain is an identification name, shared key, and the IP address of the server’s External interface.

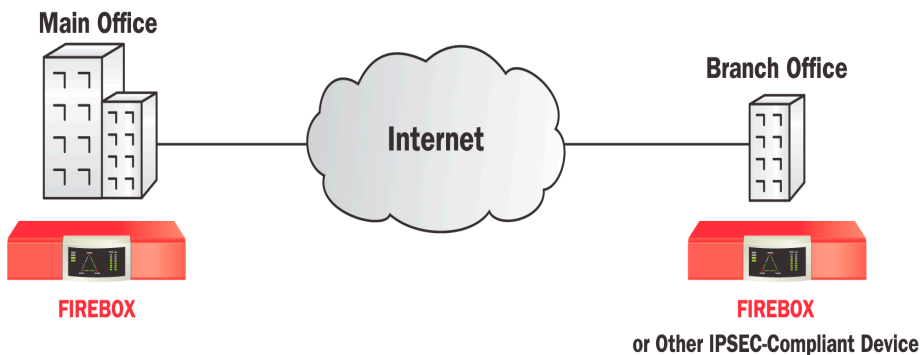


BOVPN with Basic DVCP

BOVPN with Manual IPsec

This BOVPN method uses IPsec to establish encrypted tunnels between a Firebox and any other IPsec-compliant security device, regardless of brand, that may be in service protecting branch office, trading partner, or supplier locations. BOVPN with IPsec is available with the WatchGuard medium encryption version at DES (56-bit) strength, and with the WatchGuard strong encryption versions at both DES (56-bit) and TripleDES (168-bit) strengths.

A main advantage of BOVPN with manual IPsec is that you can order and prioritize routing policies to specify which VPN tunnel to use for certain traffic. For example, you can use DES encryption for VPN traffic originating from your sales team, and the stronger TripleDES encryption for all data transmitted from your finance department.



BOVPN with Manual IPsec

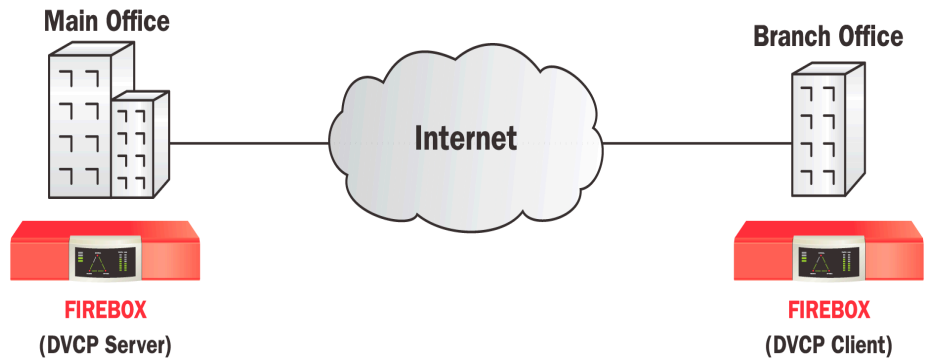
IPsec tunnels with VPN Manager

With VPN Manager, you create fully authenticated and encrypted IPsec tunnels using a simple drag-and-drop or menu interface. VPN Manager uses DVCP to securely transmit IPsec VPN configuration information between Fireboxes. Using DVCP, administrators define each configuration aspect of the VPN—such as encryption algorithms and how often encryption keys are negotiated—and then store these settings on a centrally located DVCP server. When a Firebox is installed and initialized, a software client on the Firebox contacts the DVCP server to obtain IPsec policy information.

Using VPN Manager, you can simultaneously configure, manage, and monitor all of the WatchGuard appliances throughout the enterprise. The software eliminates the need for Internet security expertise among branch offices and remote users. Instead, remote users simply plug in the appliance and the administrator at the headquarters does all the rest. If certificates are used for tunnel authentication, all you need to do is configure the Firebox as a certificate authority. The details of certificate generation and distribution are automatically managed by DVCP.

NOTE

The Firebox Model 700 does not support VPN Manager.



BOVPN with VPN Manager

Designing a VPN Environment

VPN tunnels introduce an additional layer of complexity to the security aspects of your network. When you set up a VPN environment, you are expanding your security perimeter to vulnerable settings such as hotel rooms, airports, and employees' homes. And your company's network security is only as strong as its weakest link.

Another primary concern when deploying VPNs, which must often be balanced with security concerns, is performance. Many of the most secure options available for VPNs come at a high performance cost.

Selecting an Authentication Method

A primary element of a VPN is its method of user authentication. You can use either shared keys or digital certificates to authenticate VPN users. Shared secrets are passwords that must be provided to users. They offer an easy way to quickly set up VPNs to a small number of remote employees, although large numbers of passwords are difficult to manage. To maintain as much security as possible using this method, users should choose strong passwords, passwords should be aged quickly, and users should be locked out after three failed login attempts.

When using RUVPN with PPTP or MUVPN, it is especially important to use strong passwords. Compromising the security of VPN endpoints could jeopardize the security of the main network. If, for example, a traveling employee's laptop were stolen, a thief who was able to crack the password would have instant access to the corporate network.

Digital certificates are electronic documents that prove a user's identity. (For a detailed discussion of certificates, see "Public Key Cryptography and Digital Certificates" on page 27.) Certificates are managed by a trusted third party called a certificate authority (CA). In the WatchGuard Firebox System, a Firebox can be configured to function as a CA. This method of authentication is more secure and scalable than shared secrets.

Selecting an Encryption and Data Integrity Method

Consider both security and performance when choosing encryption and data integrity methods. Out of the two types of encryption supported—DES and TripleDES—the strongest is TripleDES, which is recommended for any sensitive data. Although DES requires less computing time for encryption and decryption, it is recommended only where strong security is not necessary or where use of strong encryption is prevented by export restrictions.

Data integrity ensures that the data received by a VPN endpoint has not been altered while in transit. Two types of data authentication are supported: 128-bit strength Message Digest 5 (MD5-HMAC) and 160-bit strength secure hash algorithm (SHA-HMAC). Because SHA-HMAC has a greater bit strength, it is considered more secure to a small degree, although it may place a slightly heavier load on the processor. However, both MD5 and SHA are considered secure and are used extensively.

IP Addressing

Proper IP addressing is important when creating a VPN. To maintain scalability and performance, branch offices should use a subnet of the corporate network.

For MUVPN and RUVPN tunnels, the safest method is to define a “placeholder” secondary network, define a range of addresses for it, and choose an IP address from that network range. This allows you to draw from a range of addresses that do not clash with real host addresses in use behind the Firebox. Using this method, you must also configure the client computer to use the default gateway on the remote host. For information on defining a secondary network, see the *WatchGuard Firebox System User Guide*. For information on IP addressing with PPTP tunnels, see the following FAQ:

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

NAT and VPNs

Implementing NAT within an IPSec VPN can require some adjustments. By definition, NAT changes an IP packet’s address information. The packet will then fail its data integrity check under the AH protocol, which requires that every bit in the datagram remain unchanged. When using NAT within a tunnel created using BOVPN with Manual IPSec, you must make sure you specify ESP as an authentication method instead of AH. (With all other types of IPSec tunnels, ESP is always used as the authentication method.)

Traffic through an IPSec VPN can be masqueraded if necessary using any type of NAT supported by the Firebox. One scenario in which this would be useful is if a VPN exists between two networks that have the same IP address range on their trusted networks. 1-to-1 NAT could be used so each could choose a unique network.

The other scenario for using NAT within VPNs is to use IPSec and PPTP passthrough, as described in “Making Outbound IPSec Connections From Behind a Firebox” on page 71 and “Making Outbound PPTP Connections From Behind a Firebox” on page 56.

Access Control

VPNs allow users with varying degrees of trust to access corporate resources. Consider which type of access is appropriate for a given type of

user. For example, you might have a group of contract employees you want to restrict to just one network while granting your sales force access to all networks.

Different VPN applications may also determine your level of trust. Branch office VPNs, because they have a firewall device at both ends of the tunnel, are more secure than MUVPN and RUVPN, which are protected at only one end. And branch office VPNs involve devices with static IP addresses while the addressing of remote users' and telecommuters' workstations is generally dynamic.

Split Tunneling

Split tunneling refers to a remote user or site accessing the Internet on the same machine as the VPN connection but without placing the Internet traffic inside the tunnel. Browsing the Web occurs directly through the user's ISP. This exposes the system to attack because the Internet traffic is not filtered or encrypted.

However, despite the security risks of split tunneling, it does offer performance advantages. 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. One solution is to allow split tunneling but require that remote users have personal firewalls for machines residing behind the VPN endpoint.

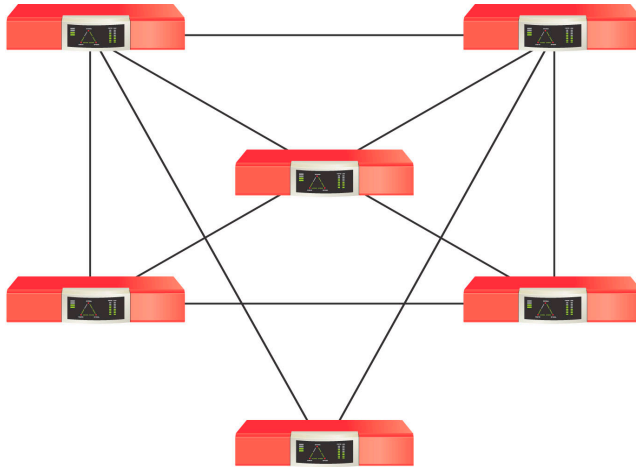
Network Topology

You can configure the VPN to support both mesh and hub-and-spoke configurations. The topology you select determines the types and number of connections that are established, the flow of data, and the flow of routing traffic.

Meshed networks

In a fully meshed topology, as shown in the following figure, all servers are interconnected to form a web, or mesh, with only one hop to any VPN

member. Communication can occur between every member of the VPN, whether required or not.



Fully meshed network

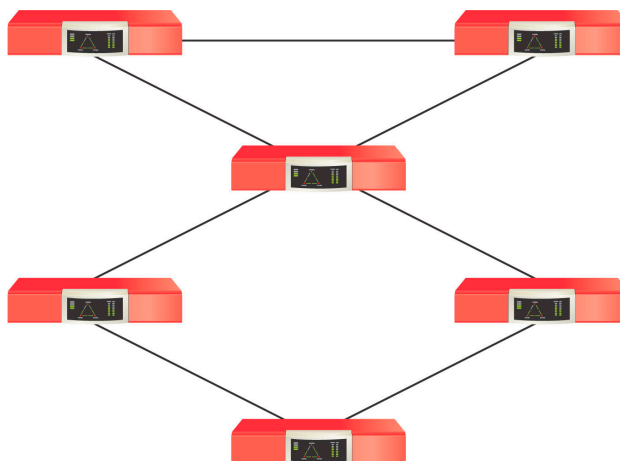
This topology is the most fault-tolerant. If a VPN member goes down, only the connection to that member's protected network is lost. However, this topology has more routing traffic because each VPN member must send updates to every other member. Also, routing loops in a mesh topology can require a significant amount of time to be resolved.

The security of the system as a whole can be maintained and monitored from multiple locations, each deploying a large scale Firebox. This configuration is used by larger enterprises with substantial branch offices, each requiring the higher capacity firewall. Smaller offices and remote users are connected using MUVPN, RUVPN, or SOHOs.

The main issue with fully meshed networks is scalability. Because every device in the network must communicate with every other device, the number of tunnels required quickly becomes immense. Maintaining such a large number of tunnels can also have a considerable impact on performance. The following equation shows the number of tunnels required for this configuration:

$$[(\text{number of devices})^2 = \text{number of tunnels}]$$

Partially meshed networks, as shown in the following figure, have only the inter-spoke communications they need and are therefore more scalable than fully meshed networks. A limiting factor in all meshed networks is the number of tunnels that can be supported without overloading the CPU.



Partially meshed network

Hub-and-spoke networks

In a hub-and-spoke configuration, as shown in the following figure, all VPN tunnels terminate at one end of a centrally located and managed firewall appliance. This configuration is frequently used by smaller enterprises with a central Firebox and many distributed remote users connecting with MUVPN, RUVPN, or SOHOs.

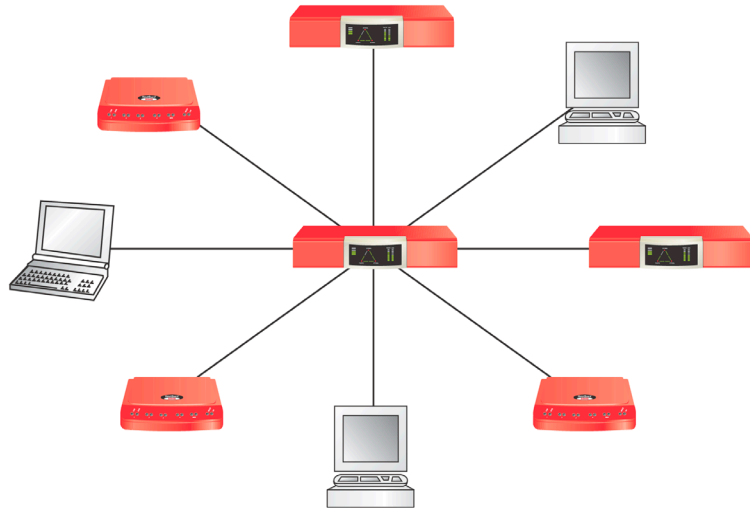
The master server is the central hub of this topology, with all communications radiating outward to other servers and returning to the master server.

In terms of routing traffic, hub-and-spoke is the least traffic-intensive topology, but the master server is the single point of failure. If the master server goes down, an encrypted tunnel cannot be established to any slave server and the ability to send encrypted data to all protected networks is lost.

Hub-and-spoke is far more scalable than meshed with a much more manageable number of tunnels, as shown in the following equation:

$$[(\text{number of devices}) - 1 = \text{number of tunnels}]$$

The hub site can be expanded as spoke capacity requirements increase. However, because all traffic travels through the hub, this setup requires considerable bandwidth.



Hub-and-spoke network

Determining Which WatchGuard VPN Solution to Use

The five different WatchGuard VPN solutions are each designed for particular applications and setups.

Use BOVPN with Basic DVCP if:

- You are creating tunnels between a Firebox at your main office and dynamically addressed SOHOs at your branch offices.
- The branch offices do not need to communicate with each other.
- You need only very simple tunnels.

Use BOVPN with Manual IPsec if:

- You are creating tunnels between a Firebox and a non-WatchGuard, IPsec-compliant device.
- You want to assign different routing policies to different tunnels.
- You want to restrict the type of traffic that passes through the tunnel.

Use IPsec tunnels with VPN Manager if:

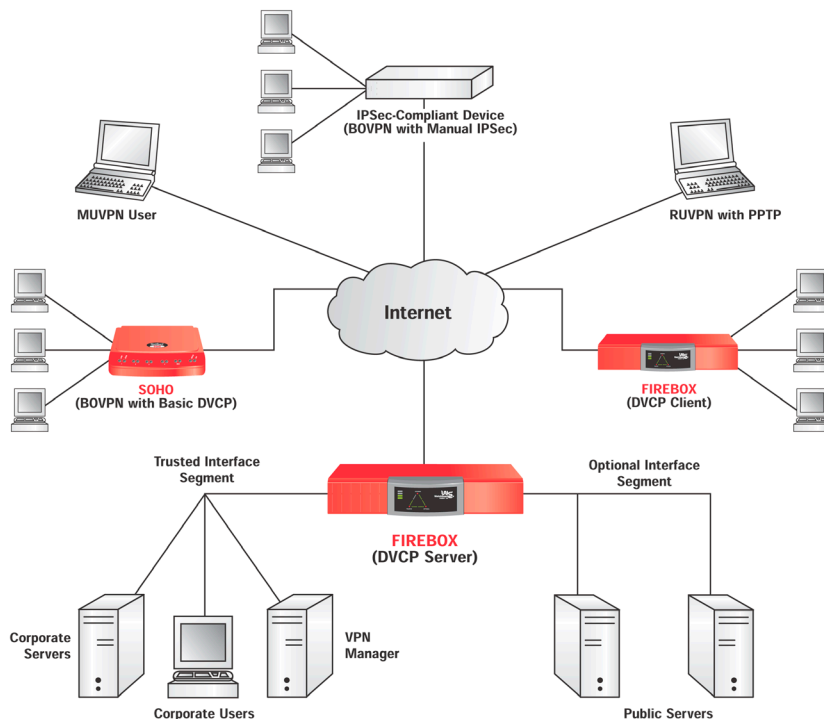
- You are creating tunnels between two or more Fireboxes.
- You want to assign different routing policies to different tunnels.
- Participating client devices are dynamically addressed.
- You have a large number of tunnels to set up.

Use MUVPN if:

- You have mobile users who need to connect securely to a Firebox or SOHO.

Use RUVPN with PPTP if:

- You have mobile users who want to connect to the Firebox using PPTP.



WatchGuard VPN Solutions

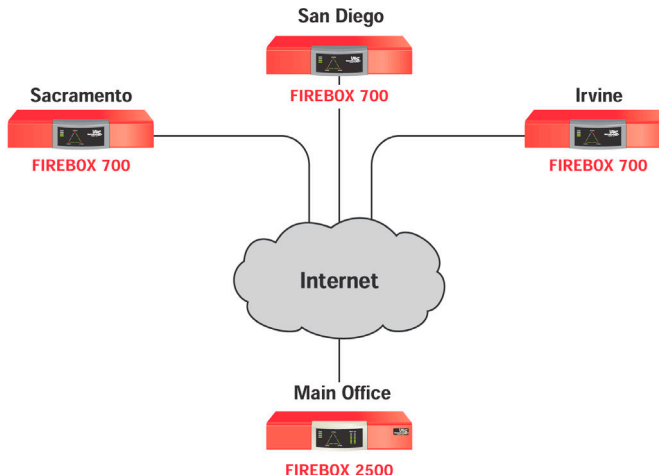
VPN Installation Services

WatchGuard Remote VPN Installation Services are designed to provide you with comprehensive assistance for basic VPN installation, at extra cost. You can schedule a dedicated two-hour time slot with one of our WatchGuard technicians to review your VPN policy, help you configure, and test your VPN configuration. This service assumes you have already properly installed and configured your Fireboxes.

VPN Scenarios

This section describes four different types of enterprises and the VPN solutions that best fit each one.

Large company with branch offices: VPN Manager



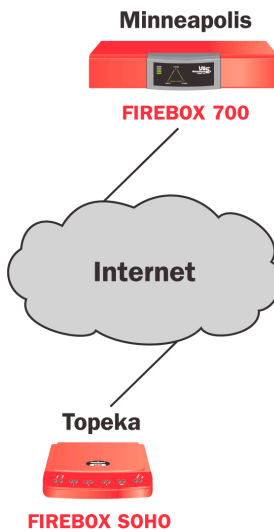
Gallatin Corporation has a main office with about 300 users in Los Angeles and branch offices of around 100 users each in Sacramento, San Diego, and Irvine. All locations have high-speed Internet access, and employees at all locations need secure connections to all other locations.

This enterprise uses Fireboxes at each location and VPN Manager to connect the locations to each other. Each office connects to all other offices, and all users at each office have access to the shared files at all the other locations. The Firebox at headquarters is the DVCP server and the Fireboxes at the branch offices are DVCP clients. Service interruptions occasionally occur with Gallatin's Internet service provider, which renders the Firebox at headquarters unavailable, but the tunnels among the other locations remain in place.

Medium-sized company with main office and auxiliary office: BOVPN with Basic DVCP

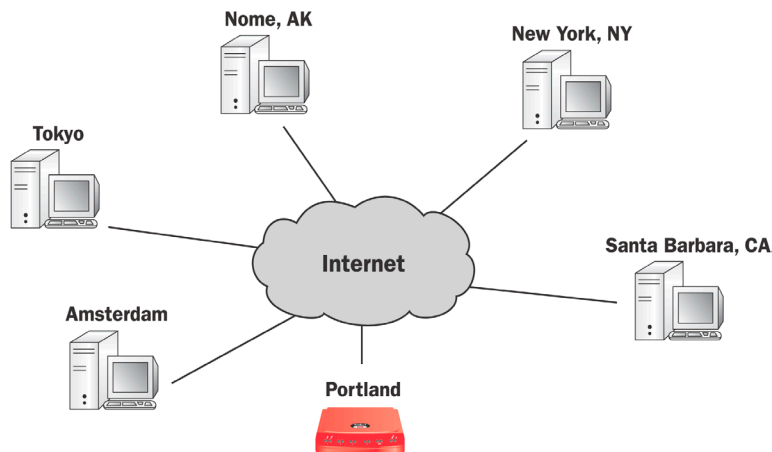
Arrington's Plumbing Supply has a main office in Minneapolis, Minnesota and a distribution center in Topeka, Kansas. The main office has a Firebox 700 on a T1 connection and the distribution center has a SOHO ltc. The two offices have secure access to one another using Basic DVCP, which allows the SOHO to establish a VPN with the Firebox

despite the SOHO's public IP address changing from time to time. The eight employees at the distribution center can access all shared files at headquarters, and headquarters can access the inventory computers in Topeka.



Small company with telecommuters: MUVPN

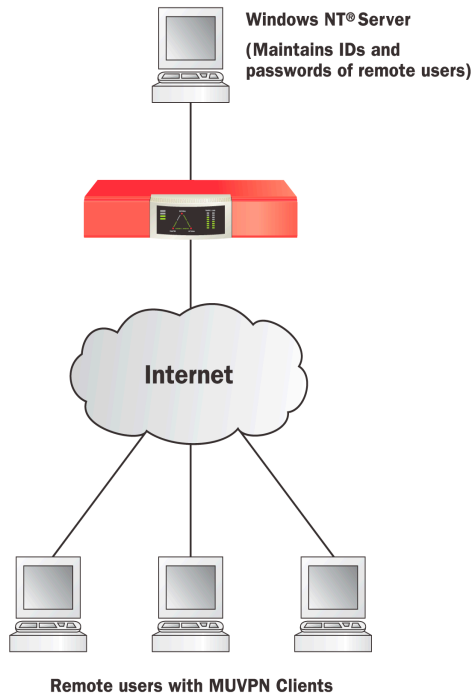
River Rock Press is a small publishing house serving a speciality market. It has an office with six employees in Portland, Oregon and five editors who live all over the world. The main office uses a SOHO for firewalling and as a VPN gateway, and the five editors each use a Mobile User VPN client to securely connect to the River Rock Information Center in Portland. The editors are able to securely exchange information any time their computers are connected to the Internet, regardless of the type of Internet connections they have at each location.



Company with remote employees: MUVPN with extended authentication

BizMentors, Inc employs 35 trainers to deliver courses in business-related topics at client companies' facilities. BizMentor's 75 salespeople need up-to-the minute information on the trainers' schedules to avoid scheduling conflicts. This information is kept current on a database located in BizMentors' data center. The data center uses a Firebox, and each salesperson uses an MUVPN client to access the inventory and price database. A Windows NT server at the data center is used to authenticate all remote users.

Normally, the ID and password information must be entered and maintained on both the Firebox and the Windows NT server. However, using extended authentication, all IDs and passwords are validated against the Windows NT server and do not need to be loaded onto the Firebox. All salespersons can log into the corporate network with the ID and password they normally use when inside the network. The Firebox validates the ID and password against the Windows NT server instead of its own internal data.



Activating the Certificate Authority on the Firebox

All WatchGuard tunnels created using IPSec can be authenticated using either shared secrets or *digital certificates*. A certificate is an electronic document containing a public key which provides proof that the key belongs to a legitimate party and has not been compromised. Certificates are issued to clients by a trusted third party called a certificate authority (CA). In the WatchGuard Firebox System, a Firebox that is configured as a DVCP server also functions as a CA.

Certificates provide a stronger and more scalable means of authentication than shared secrets. Although many CAs in the marketplace are complex to deploy, the WatchGuard CA is easily configured and performs authentication functions with minimal input required by the user.

CAs are part of a system of key generation, key management, and certification called a Public Key Infrastructure (PKI). The PKI provides for certificate and directory services that can generate, distribute, store, and—when necessary, revoke the certificates.

Public Key Cryptography and Digital Certificates

A central fixture of a PKI is an information protection method called *public key cryptography*. This cryptographic system involves two

mathematically related keys, known as a key pair. One key, the private key, is kept secret by the owner of the key. The other key, known as the public key, may be distributed far and wide by its owner. The keys in the key pair are complementary. Only the private key can decrypt information encrypted with the public key. And only the public key verifies information signed with the private key.

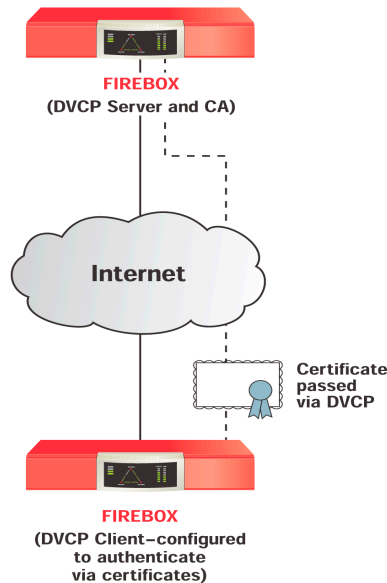
The integrity and identity of public keys is maintained using digital certificates. A root certificate, which contains the public key of the CA, ensures that the client certificates are valid.

Certificates have a fixed lifetime that is determined when they are issued. However, certificates are sometimes revoked before the expiration date and time that was originally set for them. To keep track of which certificates are no longer valid, the CA maintains an online, up-to-date listing of revoked certificates called a certificate revocation list (CRL). Before validating a certificate, the CRL is checked to make sure the certificate has not been revoked.

PKI in a WatchGuard VPN

For authenticating by way of certificates, the Firebox must be configured as a DVCP server, which automatically activates the CA on the Firebox. Each DVCP client authenticates to the DVCP server. The CA determines that the client is legitimate and then returns a certificate to the client.

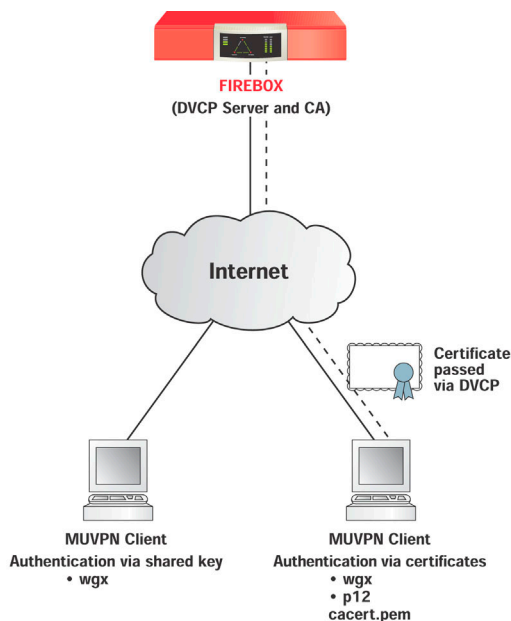
The CA can be configured in several ways. A common structure, shown in the following figure, includes a Firebox as a DVCP server that is managing a DVCP client. The DVCP server can also manage a number of DVCP clients known as a DVCP cluster. The CA component of the DVCP server is active regardless of whether either Firebox authenticates through certificates. The authentication method is determined by settings in the DVCP clients. In the example below, one DVCP client authenticates using certificates. When the client contacts the server, the CA downloads a certificate to the Firebox using DVCP.



DVCP server/CA with DVCP client

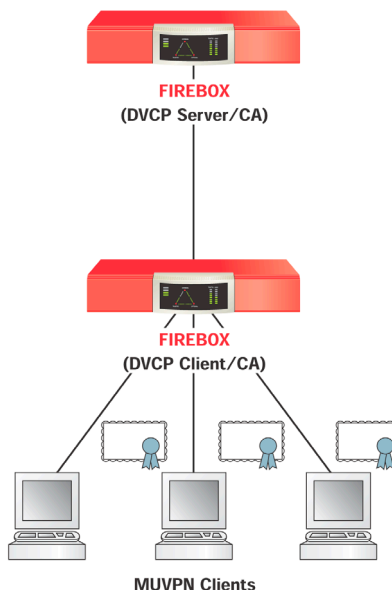
The following figure shows a Firebox that is not part of a DVCP cluster. Instead, the Firebox functions as a CA for MUVPN users. In this example, one MUVPN user is authenticating through certificates and the other by shared key. Because MUVPN clients are not DVCP clients, they authenticate to the Firebox, and Control Center creates a request for a certificate. After the CA issues the certificate, Control Center packages the certificate for transport to the MUVPN client.

The Firebox administrator provides each MUVPN user with a collection of settings called an MUVPN end-user profile. Users who are authenticating with shared keys receive one file, `.wgx`. Users authenticating with certificates receive a `.wgx` file along with two other files: `cacert.pem`, which contains the root certificate; and `.p12`, the client certificate. When the MUVPN user authenticating by way of certificates opens the `.wgx` file, the root and client certificates contained in the `cacert.pem` and `.p12` files are automatically loaded.



DVCP server/CA with MUVPN clients

Another configuration, shown in the following figure, involves a DVCP server/CA at a company's main office and a Firebox as a DVCP client at a branch office. The branch office supports mobile users authenticating by way of certificates. This scenario comprises two CAs—a principal CA and a subordinate one.



DVCP server/CA, DVCP client/CA, and MUVPN clients

Defining a Firebox as a DVCP Server and CA

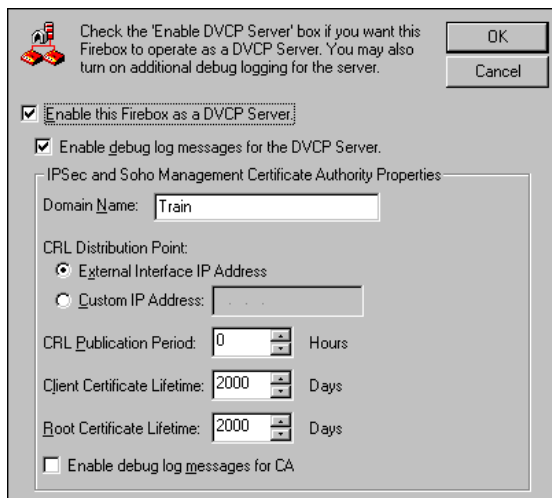
When you designate a Firebox as a DVCP server, you also enable it as a certificate authority. You can configure a DVCP server from either Policy Manager or VPN Manager.

NOTE

Only a Firebox with a static IP address can be defined as a DVCP server.

Using Policy Manager

- 1 Open Control Center and connect to the Firebox you want to define as an DVCP Server.
- 2 From Policy Manager, select **Network ⇒ DVCP Server**.
The DVCP Server Properties window appears, as shown in the following figure.



- 3 Select the checkbox marked **Enable this Firebox as a DVCP Server**.
- 4 If you want to enable debug logging for the server, select the checkbox marked **Enable Debug Log Messages for the DVCP Server**.
- 5 Enter the domain name for the IPSec and SOHO Management Certificate Authority Properties.
- 6 Select the Certificate Revocation List (CRL) end point.
This is either an external interface IP address or custom IP address.
- 7 Enter the CRL Publication period in hours.
This is the period of time a particular CRL is available.
- 8 Enter the client certificate lifetime in days.
- 9 Enter the root (CA) certificate lifetime in days.
- 10 Select the box **Enable debug log messages for CA** to have these messages sent to the WSEP log host.

NOTE

Make sure you set CA properties correctly. Changing CA properties after initial setup will invalidate all certificates.

- 11 Click **OK**.

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

Using VPN Manager

- 1 Open VPN Manager and select **File** ⇒ **New**.
The New Server dialog box appears, as shown in the following figure.

A DVCP Server manages any DVCP Clients you create.
Enter the name, type, passphrases and license key for the new Server.

Display Name:

Hostname/IP Address:

Status Passphrase:

Configuration Passphrase:

License Key:

OK Cancel Help

- 2 Enter the following:

Display Name

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

Host Name or IP Address

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

Status Pass Phrase

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

Configuration Pass Phrase

This is the current configuration (read/write) passphrase. This is also the passphrase used when configuring a device that is inserted into VPN Manager.

License Key

The key listed on your VPN Manager License Key Certificate.

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

NOTE

If you are configuring BOVPN tunnels using certificates for authentication, you must use the WatchGuard Security Event Processor (WSEP) for logging. Because certificates use timestamps, all devices in a VPN using certificates for authentication must be using the same timekeeping method.

Managing the Certificate Authority

You can manage various aspects of the certificate authority on the Firebox using the Web-based CA manager.

- 1 After activating the CA on the Firebox, access the Web-based Certificate Authority Settings pages. You can do this from several locations:
 - From the Control Center Main Menu, select **Tools** ⇒ **Advanced** ⇒ **CA Manager**.
 - From VPN Manager, select **Resources** ⇒ **CA Manager**.
 - From VPN Manager, click the CA Manager icon (shown at right).



VPN Manager and Control Center must first be connected to the Firebox designated as a DVCP server.

- 2 Enter the Firebox configuration passphrase when prompted.
The main menu of the Certificate Authority Settings pages appears.
- 3 From the main menu, select the page you want as follows:

Generate a New Certificate

Enter a subject common name, organizational unit, password, and certificate lifetime to generate a new certificate.

- For MUVPN users, the common name should match the username of the remote user.
- For Firebox users, the common name should match the Firebox identifier (normally, its IP address).

- For a generic certificate, the common name is the name of the user.

NOTE

Enter the organizational unit specification only if you are generating certificates for MUVPN users. It is not used with other types of VPN tunnels. The unit name should appear in the following format:

GW:< *vpn gateway name*>

where is the value of config.watchguard.id in the gateway Firebox's configuration file.

Publish a Certificate Revocation List (CRL)

Force the CA to publish the CRL to all certificate-holding clients.

Publish the CA Certificate

Print a copy of the CA (root) certificate to the screen so you can manually save it to the client.

Find and Manage Certificates

Specify the serial number, subject common name, or subject organizational unit of a certificate to be located in the database. Also, instead of a particular certificate, you can specify that only valid, revoked, or expired certificates are located. The results of the search are displayed on the List Certificates page, as described below.

List and Manage Certificates

View a list of certificates currently in the database and select certificates to be published, revoked, reinstated, or destroyed. For information on performing these actions on certificates, see the next section.

Upload CA Credentials

Use this page to force the certificate authority on a particular Firebox to become subordinate to the master CA. The master CA will generate a private key and certificate for the Firebox. Enter the name of the credentials file containing the key and certificate (or click Browse to locate it) to be uploaded to the Firebox.

Upload Certificate Request

Use this page to import a certificate request from a third party. Specify the subject common name and organizational unit. Enter or browse to locate the certificate signing request file.

Managing certificates from the CA Manager

You use the List and Manage Certificates page to publish, revoke, reinstate, or destroy certificates:

- 1 From the List and Manage Certificates page, click the serial number of the certificate on which you want to perform the action.
The certificate data appears.
- 2 From the **Choose Action** drop list, select from the following choices and then click **GO**:

Publish (PEM)

Publishes the certificate in Privacy Enhanced Mail (PEM) format, which uses a protocol to provide secure Internet mail. This option allows you to save the certificate to a file and upload it to a third-party device.

Publish (PKC12)

Publishes the certificate in PKCS12 format, which is used by most Web browsers. This option allows you to save the certificate to a file and upload it to a third-party device.

Revoke

Revokes a certificate. This action does not publish a CRL.

Reinstate

Reinstates a previously revoked certificate.

Destroy

Destroys a certificate.

Restarting the CA

When the CA root certificate expires, you must restart the CA to force it to reissue a new root certificate.

From Control Center:

- 1 Click the Control Center Main Menu button (shown at right). Select **Management** $\Rightarrow$ **Restart CA**.
- 2 When asked to confirm, click **Yes**.
- 3 Enter the Firebox configuration (read/write) passphrase.
- 4 When prompted, click **Yes**.



Configuring RUVPN with PPTP

Remote User Virtual Private Networking (RUVPN) uses Point-to-Point Tunneling Protocol (PPTP) to establish a secure connection between an unsecured remote host and a protected network. It supports up to 50 concurrent sessions per Firebox and works with any Firebox encryption level. RUVPN requires configuration of both the Firebox and the end-user remote host computers.

RUVPN users can authenticate either to the Firebox or to a RADIUS authentication server.

Configuration Checklist

Before configuring a Firebox to use RUVPN, gather this information:

- The IP addresses to assign to the remote client during RUVPN sessions. **These IP addresses cannot be addresses that are currently used in the network.** The safest way to allocate addresses for RUVPN users is to define a “placeholder” secondary network, define a range of addresses for it, and choose an IP address from that network range. For more information, see “IP Addressing” on page 14.
- The IP addresses of the DNS and WINS servers in the trusted network that perform IP address lookup on host alias names.

- The usernames and passwords of those authorized to connect to the Firebox using RUVPN.

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 56-bit (medium) encryption.

For RUVPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. U.S. domestic versions of Windows XP ship with 128-bit encryption enabled by default, but earlier versions of Windows may require a strong encryption patch, available from Microsoft. The Firebox always attempts to negotiate 128-bit encryption first, and drops down (if enabled) to 40-bit if the client is unable to negotiate the 128-bit encrypted connection. For information on how to enable the drop to 40-bit, see “Activating RUVPN with PPTP” on page 46. For more information on encryption levels and PPTP tunnels, see the following FAQ: https://support.watchguard.com/AdvancedFaqs/pptp_tunnelencryp.asp

If you live outside the U.S. and you need to activate strong encryption on your LiveSecurity Service account, send an email to supportid@watchguard.com and include in the request:

- Your active LiveSecurity Service key number
- Date purchased
- The name of your company
- Mailing address
- Telephone contact number and name
- Email address to respond to

If you live in the U.S., you must download either the medium or strong encryption software from your archive page in the LiveSecurity Service Web site. Go to www.watchguard.com, click **Support**, log into your LiveSecurity Service account, and then click **Latest Software**.

After you have downloaded or activated the medium or strong encryption software, you must download the medium or strong encryption version of the Firebox software, uninstall the original

encryption software, and finally, install the medium or strong encryption software from the downloaded file.

NOTE

If you want to retain your current Firebox configuration when performing the uninstall/reinstall, do not set up the Firebox with the QuickSetup Wizard when reinstalling. Instead, open Control Center, connect to the Firebox, and save the current configuration file. Configurations generated with any encryption version are compatible.

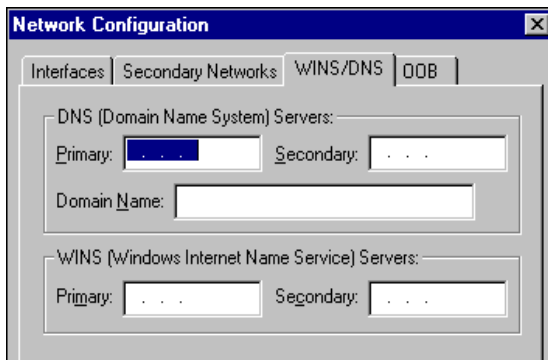
Configuring WINS and DNS Servers

RUVPN 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.



Adding New Users to Authentication Groups

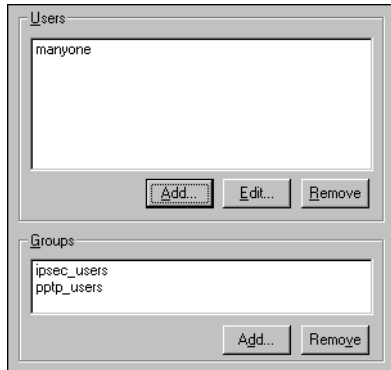
All RUVPN users must be placed in a built-in Firebox authentication group called `pptp_users`. This group, which contains the usernames and passwords of RUVPN users, is used to configure the allowed services for incoming traffic, as described in the next section.

To gain access to Internet services (such as outgoing HTTP or outgoing FTP), the remote user provides authenticating data in the form of a username and password, and the WatchGuard Firebox System software authenticates the user to the Firebox.

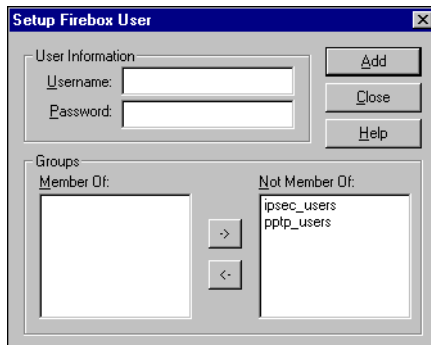
For more information on Firebox groups, see the “Creating Aliases and Implementing Authentication” chapter in the WatchGuard Firebox System *User Guide*.

From Policy Manager:

- 1 Select **Setup** ⇒ **Authentication Servers**.
The Authentication Servers dialog box appears.
- 2 Click the **Firebox Users** tab.
The information on the tab appears as shown in the following figure.



- 3 To add a new user, click the **Add** button beneath the **Users** list. The Setup Firebox User dialog box appears, as shown below.



- 4 Enter a username and password for the new user.
- 5 Select **pptp_users** in the **Not Member Of** list, and then click the left-pointing arrow to move the name to the **Member Of** list. Click **Add**. The user is added to the User list. The Setup Remote User dialog box remains open and cleared for entry of another user.
- 6 To close the **Setup Remote User** dialog box after you have finished adding new users, click **Close**. The Firebox Users tab appears with a list of the newly configured users.
- 7 When you finish adding all users you want to add, click **OK**. The users and groups can now be used to configure services, as explained in the next section.

Configuring Services to Allow Incoming RUVPN Traffic

By default, RUVPN 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 or the entire pptp_users group to service icons in the Services Arena.

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

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:

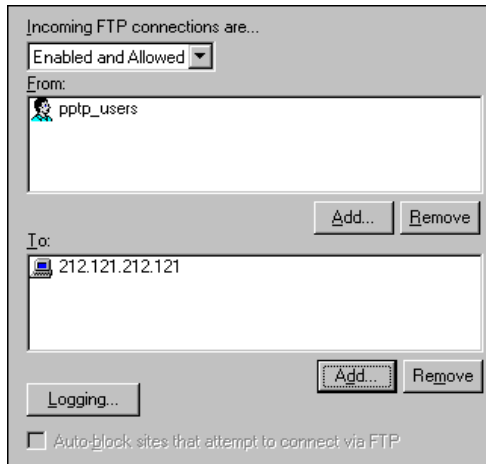
Incoming

- Enabled and allowed
- From: pptp_users
- To: Trusted, Optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: Trusted, Optional, network or host IP address, or alias
- To: pptp_users

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



Using the Any service

Add the Any service with the following properties:

Incoming

- Enabled and allowed
- From: pptp_users
- To: Trusted, Optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: Trusted, Optional, network or host IP address, or alias
- To: pptp_users

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

NOTE

If you want to use WebBlocker to control remote users' Web access, add pptp_users to whichever proxy service controls WebBlocker (such as Proxied-HTTP) instead of the Any service.

Activating RUVPN with PPTP

The next step in configuring RUVPN with PPTP is activating the feature. Activating RUVPN with PPTP adds the `wg_pptp` service icon to the Services Arena, which sets default properties for PPTP connections and the traffic flowing to and from them. The `wg_pptp` service rarely requires modification, and WatchGuard recommends leaving it in its default settings. From Policy Manager:

- 1 Select **Network** ⇒ **Remote User**. Click the **PPTP** tab.
- 2 Enable the checkbox marked **Activate Remote User**.
- 3 If necessary, enable the checkbox marked **Enable Drop from 128-bit to 40-bit**.

In general, this checkbox is used only by international customers.



Enabling Extended Authentication

RUVPN with extended authentication allows users to authenticate to a RADIUS authentication server instead of to the Firebox. For more information on extended authentication, see “Extended authentication” on page 4.

- 1 Enable the checkbox marked **Use RADIUS Authentication to authenticate remote users**, as shown in the previous figure.
- 2 Configure the RADIUS server using the **Authentication Servers** dialog box, as described in the WatchGuard Firebox System *User Guide*.
- 3 On the RADIUS server, add the user to the `pptp_users` group.

Entering IP Addresses for RUVPN Sessions

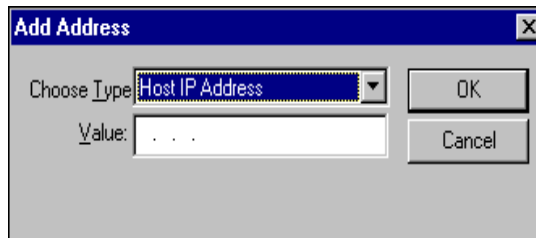
RUVPN with PPTP supports 50 concurrent sessions, although you can configure a virtually unlimited number of client computers. The Firebox dynamically assigns an open IP address to each incoming RUVPN session from a pool of available addresses until this number is reached. After the user closes a session, the address reverts to the available pool and is assigned to the next user who logs in.

For more information on assigning IP addresses to RUVPN clients, see “IP Addressing” on page 14.

From the PPTP tab on the **Remote User Setup** dialog box:

- 1 Click **Add**.

The Add Address dialog box, as shown below, appears.



- 2 Use the **Choose Type** drop list to select either a host or network. You can configure up to 50 addresses. If you select a network address, RUVPN with PPTP will use the first 50 addresses in the subnet.
- 3 In the **Value** field, enter the host or network address in slash notation. Click **OK**.
Enter unused IP addresses that the Firebox can dynamically assign to clients during RUVPN with PPTP sessions. The IP address appears in the list of addresses available to remote clients.
- 4 Repeat the add process until all addresses for use with RUVPN with PPTP are configured.

Configuring Debugging Options

WatchGuard offers a selection of logging options 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 RUVPN problems.

- 1 From Policy Manager, click **Network** ⇒ **Remote User VPN**.
The Remote User Setup window appears with the Mobile User VPN tab selected.
- 2 Select the **PPTP** tab.
- 3 Click **Logging**.
The PPTP Logging dialog box appears.
- 4 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.
- 5 Click **OK**. Save the configuration file to the Firebox.

Preparing the Client Computers

Every computer used as an RUVPN with PPTP remote host must first be prepared with the following:

- Operating system software
- Device drivers
- Internet service provider (ISP) account
- Public IP address

After you have obtained these basic requirements, follow the procedures in this section to perform the following:

- Install the required version of Microsoft Dial-Up Networking and any required service packs
- Prepare the operating system for VPN connections
- Install a VPN adapter (not required for all operating systems)

Installing MSDUN and Service Packs

The client computer may need MSDUN (Microsoft Dial-Up Networking) upgrades installed and other extensions and service packs for proper configuration. Currently, RUVPN with PPTP requires these upgrades according to platform:

Encryption	Platform	Application
Both	Windows 95	MSDUN 1.3
Both	Windows 98	MSDUN 4.0
Base	Windows 98 SE	Second Edition
Strong	Windows 98 SE	MSDUN 128-bit
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2

*40-bit encryption is the default for Windows 2000. If you are upgrading from Windows 98, in which you had set strong encryption, Windows 2000 will automatically define strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center Web site at:

<http://www.microsoft.com/downloads/search.asp>

Windows 98 Platform Preparation

To prepare a Windows 98 remote host, you enter a name for the remote client, the name of the domain you are connecting to, and, optionally, a description for the computer. You must also verify that certain supporting software is installed.

From the Windows Desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click **Network**.
- 2 Verify that Client for Microsoft Networks is installed.
If Client for Microsoft Networks is not installed, you must install it. For instructions, see "Installing Client for Microsoft Networks" on page 50.
- 3 Click the **Identification** tab.
- 4 Enter a name for the remote client.
This must be a unique name on the remote network.
- 5 Enter the domain name you are connecting to.
This should be the same as the "Log on to Windows NT domain" value.

- 6 Enter a description for your computer (optional).
- 7 Verify that Dial-Up Adapter #2 (VPN Support) is installed.
If you do not have Dial-Up Adapter #2 (VPN Support), you must install it. For instructions, see "Installing Dial-Up Adapter #2 (VPN Support)" on page 50.
- 8 Click **OK**. Click **OK** to close and save changes.
- 9 Restart the machine.

Installing Client for Microsoft Networks

From the **Networks** dialog box:

- 1 Click the **Configuration** tab. Click **Add**.
- 2 Select **Client**. Click **Add**.
- 3 Select **Microsoft** from the list on the left. Select **Client for Microsoft Networks** from the list on the right. Click **OK**.
- 4 Select **Client for Microsoft Networks**.
- 5 Click **Properties**.
- 6 Enable the **Logon and Restore Network Connections** checkbox.
- 7 Proceed with Step 3 of "Windows 98 platform preparation."

Installing Dial-Up Adapter #2 (VPN Support)

- 1 Click **Add**.
- 2 Select **Adapter**. Click **Add**.
- 3 Select **Microsoft** from the list on the left. Select **Dial-Up Adapter** from the list on the right. Click **OK**.
- 4 Proceed with Step 8 of "Windows 98 platform preparation."

Installing a VPN adapter on Windows 98

In addition to basic platform preparation, RUVPN with PPTP requires the installation and configuration of a VPN adapter.

From the desktop of the client computer:

- 1 Double-click **My Computer**. Double-click **Dial-Up Networking**.
Or, click Start and point to Settings. Click Dial-Up Network and Connections.
- 2 Double-click **Make New Connection**.
- 3 Enter a "friendly" name for the connection.

- 4 Select the device **Microsoft VPN Adapter**. Click **Next**.
- 5 Enter the host name or IP address of the Firebox External interface. Click **Next**.
- 6 Click **Finish**.
- 7 Right-click the new connection. Click **Properties**.
- 8 Click the **Server Types** tab. Enable the following options:
 - Log on to network—Required for MS Networking but not for TCP/IP—only connections such as Telnet
 - Enable software compression
 - Require encrypted password
 - Require data encryption
 - TCP/IP
- 9 Click **TCP/IP Settings**. Enable the following options:
 - Server-assigned IP address
 - Server-assigned name server
 - Use IP header compression
 - Use default gateway on remote network; enable this option only if you have multiple networks behind the firewall or if you have assigned the pool from a “placeholder” secondary network, as described in “Entering IP Addresses for RUVPN Sessions” on page 47.
- 10 Click **OK**. Click **OK** again.
- 11 Restart the computer.

Windows NT Platform Preparation

To prepare a Windows NT remote host, you must specify PPTP as your protocol, choose the number of VPNs, and set up remote access.

From the Windows NT Desktop of the client computer:

- 1 Click **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click **Network**.
- 2 Click the **Protocols** tab.
- 3 Click **Add**.

- 4 Select **Point To Point Tunneling Protocol**.
- 5 Choose the number of VPNs.
Unless a separate host will be connecting to this machine, you need only one VPN.
- 6 In the **Remote Access Setup** box, click **Add**.
- 7 Select **VPN** on the left. Select **VPN2-RASPPTM** on the right.
- 8 Click **Configure** for the newly added device.
- 9 Click **Dial Out Only**. Click **Continue**.
- 10 Click **OK**.
- 11 Restart the machine.

Adding a domain name to a Windows NT workstation

Often, remote clients need to connect to a domain behind the firewall. To do this, the remote client must recognize the domains to which they belong. Adding a domain requires the installation of the Computer Browser Network Service. From the Windows NT Desktop:

To install a Computer Browser Service

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click **Network**.
The Network dialog box appears.
- 2 Click the **Services** tab.
- 3 Click **Add**.
- 4 Select **Computer Browser**.
- 5 Browse to locate the installation directory. Click **OK**.
- 6 Restart the workstation.

To add a new domain

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click **Network**.
The Network dialog box appears.
- 2 Click the **Protocols** tab.
- 3 Select **Computer Browser**. Click **Properties**.
- 4 Add the remote network domain name.
You can add multiple domain names during the same configuration session.
- 5 Click **OK**.
- 6 Reboot the workstation.

Installing a VPN adapter on Windows NT

In addition to basic platform preparation, RUVPN with PPTP requires the installation and configuration of a VPN adapter.

From the Windows NT Desktop of the remote host:

- 1 Double-click **My Computer**.
- 2 Double-click **Dial-Up Networking**.
If you have not already configured an entry, Windows guides you through the creation of a dial-up configuration. When it prompts for a phone number, enter the host name or IP address of the Firebox. When complete, you should see a Dial-Up Networking dialog box with the default button Dial.
- 3 Select **New** to make a new connection. If you are prompted to use the wizard, enter a friendly connection name and enable the **I Know All About** checkbox.
- 4 Under the **Basic** tab, configure the following settings:
 - **Phone Number**: Firebox IP address
 - **Entry Name**: Connect to RUVPN (or your preferred alternative)
 - **Dial Using**: RASPPTPM (VPN1) adapter
 - **Use Another Port if Busy**: enabled
- 5 Click the **Server** tab. Configure the following settings:
 - **PPP**: Windows NT, Windows 95 Plus, Internet
 - **TCP/IP**: enabled
 - **Enable Software Compression**: enabled
- 6 Click the **Security** tab. Configure the following settings:
 - **Accept Only Microsoft Encrypted Authentication**: enabled
 - **Require Data Encryption**: enabled
- 7 Click **OK**.

Windows 2000 Platform Preparation

To prepare a Windows 2000 remote host, you must configure the network connection. (Because the PPTP functionality is built into Windows 2000, you do not need to install a VPN adapter as you would for the Windows 98 and Windows NT platforms.)

From the Windows Desktop of the client computer:

- 1 Select **Start** ⇒ **Settings** ⇒ **Dial-Up Network and Connections** ⇒ **Make New Connection**.
The Network Connection wizard appears.
- 2 Click **Next**.
- 3 Select **Connect to a private network through the Internet**. Click **Next**.
- 4 Enter the host name or IP address of the Firebox External interface.
Click **Next**.
- 5 Select whether the connection is for all users or only the currently logged-on user. Click **Next**.
- 6 Enter a name you want to use for the new connection, such as "Connect with RUVPN." Click **Finish**.

Windows XP Platform Preparation

To prepare a Windows XP remote host, you must configure the network connection. (Because the PPTP functionality is built into Windows XP, you do not need to install a VPN adapter as you would for the Windows 98 and Windows NT platforms.)

From the Windows Desktop of the client computer:

- 1 Select **Start** ⇒ **Control Panel** ⇒ **Network and Internet Connections**.
The Network Connection wizard appears.
- 2 Click **Next**.
- 3 Select **Connect to the network at my workplace**. Click **Next**.
- 4 Select **Virtual Private Connection**. Click **Next**.
- 5 Enter a name you want to use for the new connection, such as "Connect with RUVPN." Click **Next**.
- 6 Select **Automatically dial this initial connection**. Click **Next**.
- 7 Enter the host name or IP address of the Firebox External interface.
Click **Next**.
- 8 Click **Finish**.

Starting RUVPN with PPTP

The connect process is identical regardless of the Windows platform. From the Windows Desktop:

- 1 Establish an Internet connection through either Dial-Up Networking or directly through a LAN or WAN.
- 2 Double-click **My Computer**. Double-click **Dial-Up Networking**.
- 3 Double-click the dial-up networking connection you made for your PPTP connection to the Firebox.
- 4 Enter the remote client username and password.
These were assigned when you added the user to the pptp_users group, as described in "Adding New Users to Authentication Groups" on page 42.
- 5 Click **Connect**.

Running RUVPN and Accessing the Internet

You can enable remote users to access the Internet through a RUVPN tunnel. However, this option has certain security implications, as described in "Split Tunneling" on page 16.

- 1 When you are setting up your connection on the client computer, enable the checkbox marked **Use default gateway on remote network**. In Windows 98 and Windows NT, this checkbox is located on the **TCP/IP Settings** dialog box. In Windows 2000 and Windows XP, it is located on the **Advanced TCP/IP Settings** dialog box.
- 2 On the Firebox, create a dynamic NAT entry from VPN to External. If you want to specify that only certain PPTP users have this ability, create entries from <virtual IP address> to External.
- 3 Configure your Any service to allow incoming connections from pptp_users to External. However, if you want to use WebBlocker to control remote users' Web access, add pptp_users to whichever proxy service controls WebBlocker (such as Proxied-HTTP) instead of the Any service.

Making Outbound PPTP Connections From Behind a Firebox

You may have occasions in which a user wants to make PPTP 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 PPTP connections to his or her network using PPTP. For the local Firebox to properly handle the outgoing PPTP connection, a PPTP service must be set up as follows:

- 1 Enable the PPTP service. (For information on enabling services, see Chapter 8, “Configuring Filtered Services” in the WatchGuard Firebox System *User Guide*.)
- 2 Select **Setup** ⇒ **NAT**, and make sure the checkbox marked **Enable Dynamic NAT** is enabled. This is the default for a Firebox in routed mode.

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

Preparing to Use MUVPN

Like RUVPN with PPTP, Mobile User VPN (MUVPN) requires configuration of both the Firebox and the remote client computers. However, unlike RUVPN with PPTP, 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 *Mobile User VPN Administration Guide* and the operating system-specific MUVPN end-user brochures. However, this chapter provides the Firebox procedures you need to perform before using these other guides.

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.

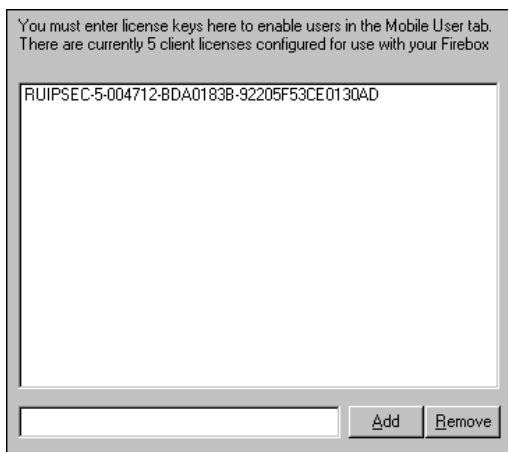
A license is available through your local reseller or at:

<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. For more information on encryption, see “Encryption levels” on page 40.

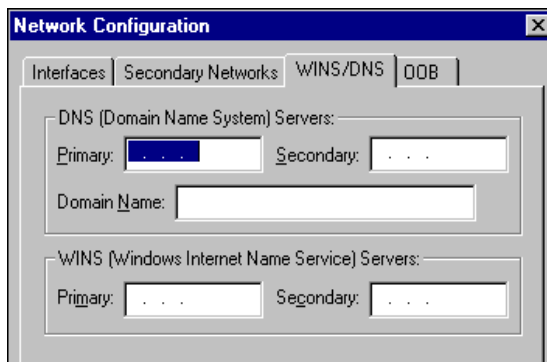
Configuring WINS and DNS Servers

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 66.

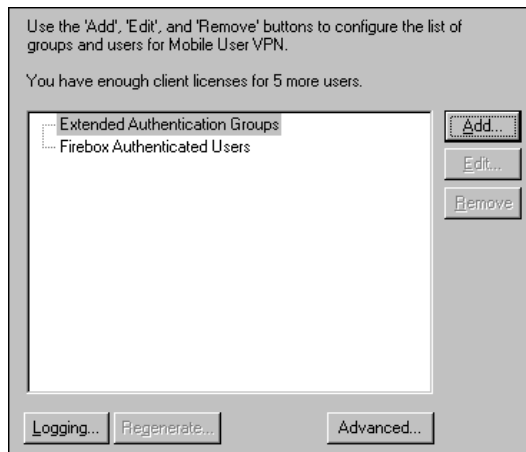
The IPSec client allows for the deployment of the software in situations where the client does not have a static IP address—such as with a DSL connection. This is the default profile and allows for the conversion of existing profiles (with the .exp extension) to the newer version (with the .wgx extension). 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 in “Defining an Extended Authentication Group” on page 63 instead.)

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. **Click Next.**
This key will be used to negotiate the encryption and/or authentication for the MUVPN tunnel.
- 5 Select whether you will use the shared key or a certificate for authentication. **Click Next.**
- 6 If you specified certificates, enter the configuration passphrase of your certificate authority. **Click Next.**
- 7 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.
- 8 If you plan to use a virtual adapter and route all of the remote user's Internet traffic through the IPsec tunnel, enable the checkbox marked **Use default gateway on remote network**. For more information on this option, see "Allowing Internet access through MUVPN tunnels" on page 63.

NOTE

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

- 9 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, as described in "IP Addressing" on page 14.
- 10 Select an authentication method and encryption method for this mobile user's connections. Enter a key expiration time in kilobytes or hours.

Authentication

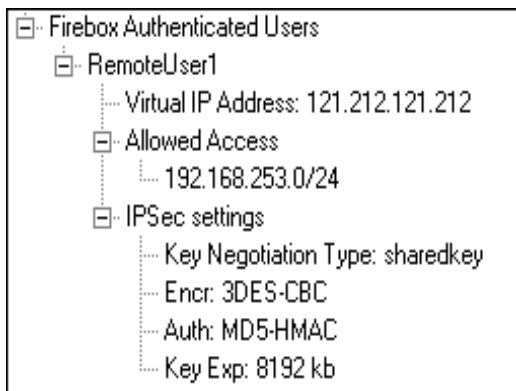
MD5-HMAC (128-bit algorithm) or SHA1-HMAC (160-bit algorithm)

Encryption

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

11 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 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 security implications, as described in “Split Tunneling” on page 16.

- 1 When you are running the MUVPN wizard, enable the checkbox marked **Use default gateway on remote network** on the network resource screen.
- 2 Create a dynamic NAT entry from VPN to External. If you want to specify that only certain MUVPN users have this ability, create entries from <virtual IP address> to External.
- 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.

Defining an Extended Authentication Group

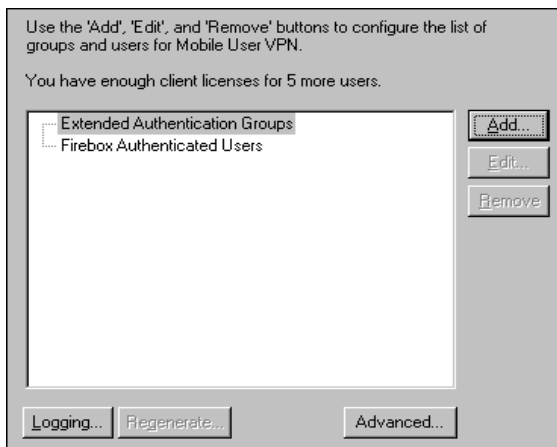
MUVPN with extended authentication allows users to authenticate to a Windows NT or RADIUS authentication server instead of to the Firebox. For more information on extended authentication, see “MUVPN with extended authentication” on page 7.

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.

From Policy Manager:

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

The Mobile User VPN information appears, as shown below.



- 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 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 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, enable 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, as described in "IP Addressing" on page 14). 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 arrives earliest.

Authentication

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

Encryption

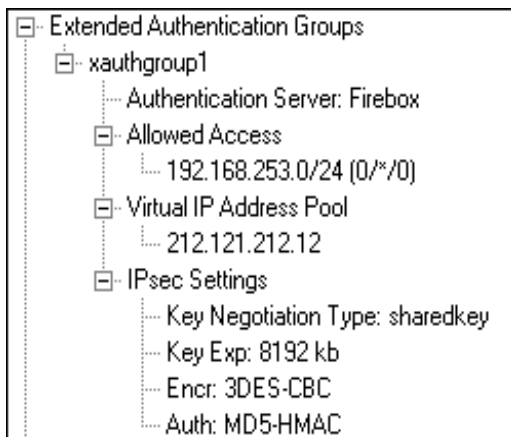
None (no encryption), DES-CBC (56-bit), or 3DES-CBC (168-bit)

- 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.

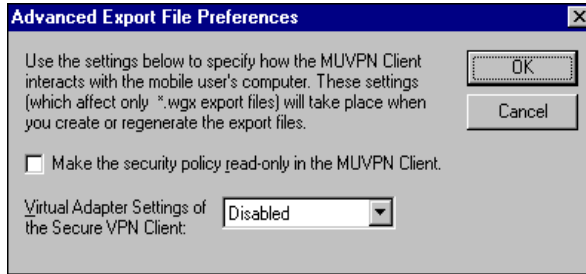


Setting Advanced Preferences

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, enable 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

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.

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:

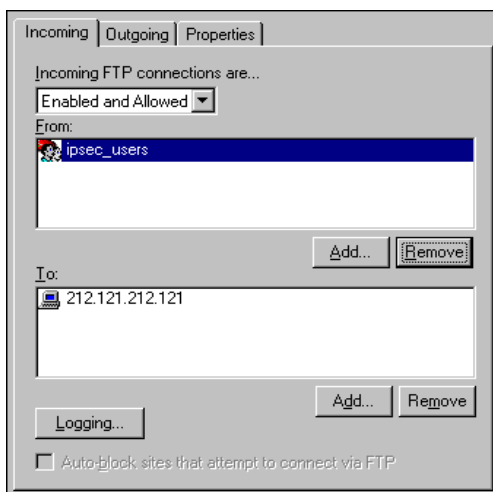
Incoming

- Enabled and allowed
- From: ipsec_users or extended authentication group
- To: Trusted, Optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: Trusted, Optional, 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.



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, Optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: Trusted, Optional, network or host IP address, or alias
- To: ipsec_users or extended authentication group

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. From the **File** menu, select **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 (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, an IPSec service must be set up as follows:

- 1 Enable the IPSec service. (For information on enabling services, see Chapter 8, “Configuring Filtered Services” in the WatchGuard Firebox System *User Guide*.)
- 2 Select **Setup** ⇒ **NAT**, and make sure the checkbox marked **Enable Dynamic NAT** is enabled. This is the default for a Firebox in routed mode.
- 3 Run the MUVPN Wizard and make sure ESP is specified instead of AH for tunnel protection. AH is incompatible with NAT.

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 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.

Configuring BOVPN with Basic DVCP

Dynamic VPN Configuration Protocol (DVCP) is the WatchGuard-proprietary protocol that easily creates IPSec tunnels. The type of DVCP described in this chapter is known as Basic DVCP, which can establish VPN tunnels between devices in a hub-and-spoke formation.

The Basic DVCP server is a Firebox that sits at the center of a distributed array of DVCP clients. This server maintains the connections between two devices by storing all policy information—including network address range and tunnel properties such as encryption, timeouts, and authentication. DVCP clients can retrieve this information from the server. The only information clients need to maintain is an identification name, shared key, and the IP address of the server's External interface.

You use the DVCP Client Wizard to configure a Firebox as a DVCP server and create tunnels to each client device. The clients then contact the server and automatically download the information needed for them to connect securely.

Configuration Checklist

Before implementing BOVPN with DVCP, gather the following information:

- IP address of the Firebox that will act as the Basic DVCP server.
- IP network addresses for the networks communicating with one another.
- A common passphrase, known as a shared secret.

Creating a Tunnel to a Device

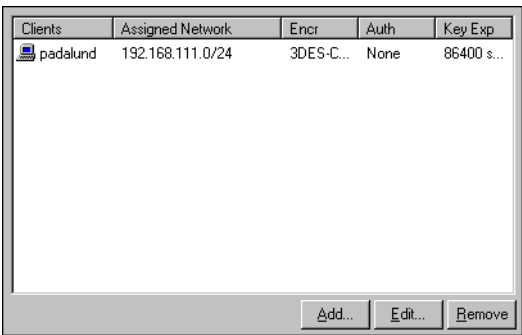
Use the following procedure to create a tunnel to a device.

The tunnels you create to SOHO clients must be completely distinct from any tunnel created for branch office VPN, regardless of whether they are being managed through DVCP or manually (as described in the next chapter). The networks on the trusted side of the SOHO cannot be the same as any other SOHO's trusted network (unless you are using a Telecommuter tunnel).

From Policy Manager:

- 1 Select **Network** ⇒ **Branch Office VPN** ⇒ **Basic DVCP Server**.

The Basic DVCP Server Configuration dialog box appears, showing the clients configured to use DVCP as shown in the following figure.



Clients	Assigned Network	Encr	Auth	Key Exp
 padalund	192.168.111.0/24	3DES-C...	None	86400 s...

Buttons: Add... Edit... Remove

- 2 Click **Add**.
The DVCP Client Wizard launches.
- 3 Enter a distinctive name for the DVCP client.
The client name appears in the Basic DVCP Server Configuration dialog box as well as the Firebox and Tunnel Status display in Control Center.
- 4 Enter the shared key that the client and server will use for encryption.
Click **Next**.

- 5 Enter the IP address of the network or host that the DVCP client will be able to access.
- 6 Select a client type and then enter the virtual network or IP address this client will use for connections. Click **Next**.

Telecommuter IP Address

The SOHO is assigned a single IP address. This is the device's virtual IP address on the Trusted network of the Firebox to which the device will be allowed access.

Private Network

The device is assigned an entire network.

- 7 Use the **Type** drop list to select an encryption type:

ESP (Encapsulated Security Payload)

Performs encryption and/or authentication

AH (Authentication Header)

Performs authentication only

- 8 Use the **Authentication** drop list to select an authentication method:

None

No authentication

MD5-HMAC

128-bit algorithm

SHA1-HMAC

160-bit algorithm

- 9 If you chose **ESP** in the **Type** drop list, see the **Encryption** drop list to select an encryption method:

None

No encryption

DES-CBC

56-bit encryption

3DES-CBC

168-bit encryption

- 10 Enter a key expiration time in kilobytes, hours, or both.
If you specify both, the key expires at whichever time arrives earliest.

11 Click **Next**. Click **Finish**. Save the configuration to the Firebox.

The new policy appears in the **Basic DVCP Server Configuration** dialog box. The WatchGuard device can now be connected, powered on, and configured. As part of the configuration process, it will automatically download the appropriate tunnel information. You must provide the DVCP client administrator with the client name, shared key, and the IP address of the server's external interface.

Editing a tunnel to a device

You can change the following properties of a DVCP tunnel without forcing the client to reboot:

- Identification name
- Shared key
- Encryption/authentication level
- Timeouts

You can also change the network range of a WatchGuard client. However, when you save the configuration to the server, it automatically triggers the client to reboot and load the new policy.

From Policy Manager:

1 Select **Network** ⇒ **Branch Office VPN** ⇒ **Basic DVCP Server**.

The Basic DVCP Server Configuration dialog box appears

2 Select the DVCP client you want to edit. Click **Edit**.

The DVCP Client Wizard opens and displays the tunnel properties.

3 Use the **Next** and **Back** buttons to move through the DVCP Client Wizard and reconfigure tunnel properties. When complete, click **Finish**.

4 Save the configuration to the Firebox.

The next time the client contacts the server, it automatically notes the tunnel policy change and downloads the modifications. If the network address range on a client has changed, the client automatically restarts.

Removing a tunnel to a device

When a tunnel is removed, the DVCP client can no longer communicate with the server. The next time the DVCP client tries to contact the server,

contact will be denied. If these settings were never manually configured, the client will use 192.168.111.0/24 as the DVCP network range.

From Policy Manager:

- 1 Select **Network** ⇒ **Branch Office VPN** ⇒ **Basic DVCP**.
- 2 Select the tunnel policy. Click **Remove**.
The policy is removed from the DVCP Configuration dialog box.

Configuring Logging for a DVCP Server

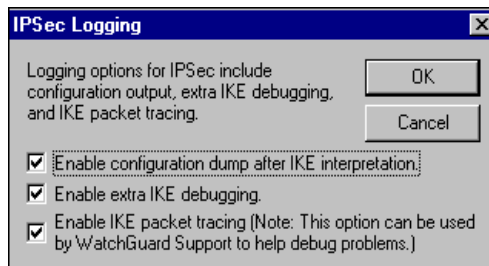
You can set several logging options for IPSec, including:

- Configuration dump after IKE interpretation
- IKE debugging messages
- Trace of IKE packets and their movements

Note, however, that these logging options can generate a high volume of traffic and can affect VPN performance. This is particularly true of tracing the IKE packets. Enable these options only to troubleshoot problems.

From Policy Manager:

- 1 Select **Network** ⇒ **Branch Office VPN** ⇒ **Basic DVCP**.
The Basic DVCP Server Configuration dialog box appears.
- 2 Click the **Logging** button at the right of the dialog box.
The IPSec Logging dialog box, as shown below, appears.



- 3 Enable the checkbox or checkboxes for the logging options you want. Save the configuration to the Firebox.

Configuring BOVPN with Manual IPSec

Branch Office VPN (BOVPN) with Manual IPSec establishes encrypted tunnels between a Firebox and any other IPSec-compliant security device, regardless of brand, that may be in service protecting branch office, trading partner, or supplier locations.

BOVPN with IPSec is available with the WatchGuard medium encryption version at DES (56-bit) strength, and with the WatchGuard strong encryption versions at both DES (56-bit) and TripleDES (168-bit) strengths.

NOTE

Manual IPSec tunnels are not supported to Fireboxes that are configured as DHCP or PPPoE clients (have dynamically assigned external IP addresses).

Configuration Checklist

Before implementing BOVPN with IPSec, gather the following information:

- IP address of both ends of the tunnel

- Policy endpoints—IP addresses of specific hosts or networks participating in the tunnel
- Encryption method (both ends of the tunnel must use the same encryption method)
- Authentication method

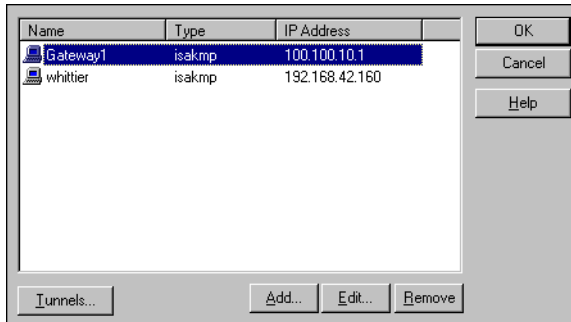
Configuring a Gateway

A gateway specifies a point of connection for one or more tunnels. The standard specified for a gateway, such as ISAKMP automated key negotiation, becomes the standard for tunnels created with the device at the other end of the tunnel.

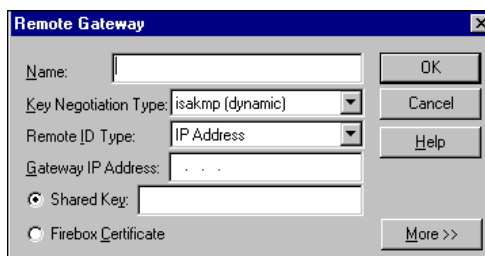
Adding a gateway

From Policy Manager:

- 1 Select **Network** ⇒ **Branch Office VPN** ⇒ **Manual IPSec**.
The IPSec Configuration dialog box appears.
- 2 Click **Gateways**.
The Configure Gateways dialog box appears, as shown in the following figure.



- 3 To add a gateway, click **Add**.
The Remote Gateway dialog box appears, as shown below.



- 4 Enter the gateway name.
This name identifies a gateway only within Policy Manager.
- 5 Use the **Key Negotiation Type** drop list to select either **ISAKMP (dynamic)** or **Manual**.
- 6 Use the **Remote ID Type** drop list to select either IP Address, Domain Name, User Name, or SDN.
Domain name and user name are simply labels you apply to designate the domain or user at the VPN endpoint. When the Firebox attempts to contact the VPN endpoint, it looks for these names.
SDN stands for Subject's Distinguished Name, which is the identifier of the certificate that will be used to authenticate the remote gateway for Phase 1 IKE.

NOTE

For VPNs using WatchGuard devices, WatchGuard recommends using the default value in the Remote ID Type field. If this value needs to be changed for interoperability, consult the appropriate interoperability document for information on the values you should use in this field.

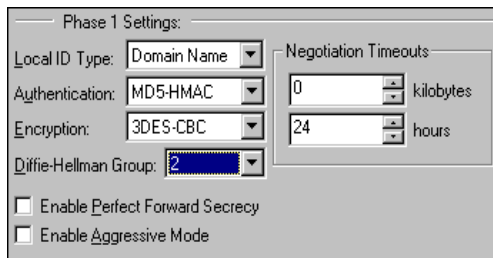
- 7 Enter the gateway IP address or identifier according to your previous selection.
- 8 Select either the Shared Key or Firebox Certificate option to specify the authentication method to be used. If you select Shared Key, enter the shared key.
These options are available only for ISAKMP-negotiated gateways. The same key must be entered at the remote device.

NOTE

If you select to authenticate using certificates, the certificate authority must be active on the Firebox. For information on activating the CA, see Chapter 3, “Activating the Certificate Authority on the Firebox.” In addition, if you use certificates, you must use the WatchGuard Security Event Processor for logging.

- 9 If you want to define Phase 1 settings, click **More**.

The Phase 1 settings fields appear, as shown in the following figure. Phase 1 refers to the initial phase of the IKE negotiation. It involves authentication, session negotiation, and key exchange.



- 10 In the **Local ID Type** drop list, specify IP Address, Domain Name, User Name, or SDN.

Domain name and user name are simply labels you apply to designate the domain or user at the VPN endpoint. When the Firebox attempts to contact the VPN endpoint, it looks for these names.

SDN stands for Subject's Distinguished Name, which is the identifier of the certificate that will be used to authenticate the remote gateway for Phase 1 IKE.

NOTE

For VPNs using WatchGuard devices, WatchGuard recommends using the default value in the Local ID Type field, which is the external IP address of the Firebox. If this value needs to be changed for interoperability, consult the appropriate interoperability document for information on the values you should use in this field.

- 11 In the **Authentication** field, specify the type of authentication: SHA1-HMAC or MD5-HMAC.
- 12 In the **Encryption** field, enter the type of encryption: DES-CBC or 3DES-CBC.

- 13 In the **Diffie-Hellman group** field, specify the group. WatchGuard supports groups 1 & 2.
Diffie-Hellman refers to a mathematical technique for securely negotiating secret keys over a public medium. Diffie-Hellman groups are collections of parameters used to achieve this. Group 2 is more secure than group 1, but requires more time to compute the keys.
- 14 If you choose, select the checkbox marked **Enable Perfect Forward Secrecy**.
When this option is selected, each new key that is negotiated is derived by a new Diffie-Hellman exchange instead of from only one Diffie-Hellman exchange. Enabling this option provides more security, but requires more time because of the additional exchange.
- 15 If you choose, select the checkbox marked **Enable Aggressive Mode**.
Mode refers to an exchange of messages in Phase 1. Main Mode is the default.
- 16 Specify negotiation timeouts in either kilobytes, hours, or both.
If you specify both, the timeout occurs at whichever time arrives earliest.
- 17 When you finish adding gateways, click **OK** to return to the **IPSec Configuration** dialog box.

Editing and removing a gateway

To edit a gateway, from the **Configure Gateways** dialog box:

- 1 Select the gateway and click **Edit**.
The Remote Gateway dialog box appears.
- 2 Make changes according to your security policy preferences and click **OK**.

To remove a gateway, from the **Configure Gateways** dialog box:

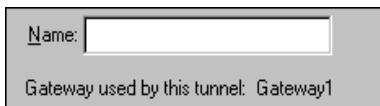
- Select the gateway and click **Remove**.

Creating a Tunnel with Manual Security

The following describes how to configure a tunnel using a gateway with the manual key negotiation type. From the **IPSec configuration** dialog box:

- 1 Click **Tunnels**.
The Configure Tunnels dialog box appears.
- 2 Click **Add**.
The Select Gateway dialog box appears.

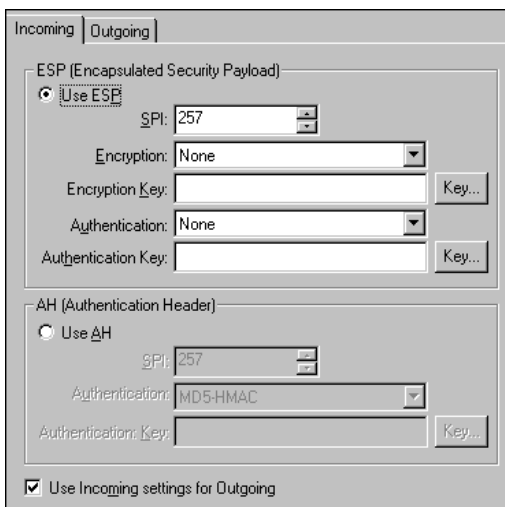
- 3 Select a remote gateway with manual key negotiation type to associate with this tunnel (the key negotiation type is displayed in the **Type** column at the **Configure Tunnels** dialog box). Click **OK**.
The Identity tab of the Configure Tunnel dialog box appears, as shown in the following figure.



Name:

Gateway used by this tunnel: Gateway1

- 4 Type a tunnel name.
Policy Manager uses the tunnel name as an identifier.
- 5 Click the **Manual Security** tab. Click **Settings**.
The Incoming tab of the Security Association Setup dialog box appears.
- 6 Click the **Phase 2 Settings** tab.
The Phase 2 settings fields appear, as shown in the following figure.



Incoming | Outgoing

ESP (Encapsulated Security Payload)

☒ Use ESP

SPI: 257

Encryption: None

Encryption Key: Key...

Authentication: None

Authentication Key: Key...

AH (Authentication Header)

☐ Use AH

SPI: 257

Authentication: MD5-HMAC

Authentication Key: Key...

☒ Use Incoming settings for Outgoing

- 7 Click either the ESP or AH security method option. Configure the chosen security method.
The difference between the two is that ESP can provide both authentication and encryption while AH provides authentication only. Also, ESP authentication does not cover the encapsulated IP header while AH does.
For more information on configuring these security methods, see "Using Encapsulated Security Protocol (ESP)" on page 85 and "Using Authenticated Headers (AH)" on page 85.

- 8 To use the same settings for both incoming and outgoing traffic, enable the **Use Incoming Settings for Outgoing** checkbox.
If you enable this checkbox, you are done with the Security Association Setup dialog box and can proceed to the next step. If you clear this checkbox, click the Outgoing tab and configure the security associations for outgoing traffic. The fields have the same rules and parameter ranges as the Incoming tab.
- 9 Click **OK**.
The Configure Tunnels dialog box appears displaying the newly created tunnel. Repeat the tunnel creation procedure until you have created all tunnels for this particular gateway.
- 10 After you add all tunnels for this gateway, click **OK**.
The Configure Gateways dialog box appears.
- 11 To configure more tunnels for another gateway, click **Tunnels**. Select a new gateway and repeat the tunnel creation procedure for that gateway.
- 12 When all the tunnels are created, click **OK**.

Using Encapsulated Security Protocol (ESP)

- 1 Type or use the SPI scroll control to identify the Security Parameter Index (SPI).
You must select a number between 257 and 1023.
- 2 Use the **Encryption** drop list to select an encryption algorithm.
Options include: None (no encryption), DES-CBC (56-bit), and 3DES-CBC (168-bit).
- 3 If you selected DES-CBC or 3DES-CBC, click **Key**.
- 4 Type a passphrase for generating a key. Click **OK**.
The passphrase appears in the Encryption Key field. You cannot enter a key here directly.
- 5 Use the **Authentication** drop list to select an authentication algorithm.
Options include: None (no authentication), MD5-HMAC (128-bit algorithm), or SHA1-HMAC (160-bit algorithm).
- 6 If you selected MD5-HMAC or SHA1-HMAC, click **Key**.
- 7 Type a passphrase for generating a key. Click **OK**.
The passphrase appears in the Authentication Key field. You cannot enter a key here directly.

Using Authenticated Headers (AH)

- 1 Type or use the SPI scroll control to identify the Security Parameter Index (SPI).
You must select a number between 257 and 1023.

- 2 Use the **Authentication** drop list to select an authentication method. Options include: MD5-HMAC (128-bit algorithm) or SHA1-HMAC (160-bit algorithm).
- 3 Click **Key**. Enter a passphrase for generating a key. Click **OK**.
The passphrase appears in the Authentication Key field. You cannot enter a key here directly.

NOTE

If both ends of the tunnel have Fireboxes, the remote administrator can also enter the encryption and authentication passphrases. If the remote firewall host is an IPSec-compliant device of another manufacturer, the remote system administrator must enter the literal keys displayed in the Security Association Setup dialog box when setting up the remote IPSec-compliant device.

Creating a Tunnel with Dynamic Key Negotiation

The following describes how to configure a tunnel using a gateway with the Internet Security Association and Key Management Protocol (ISAKMP) key negotiation type. ISAKMP is a protocol for authenticating communication between two devices. This process involves defining how the entities will use security services such as encryption, and how to generate the keys that will be used to convert the encrypted data back into plain text.

From the **IPSec Configuration** dialog box:

- 1 Click **Tunnels**.
The Configure Tunnels dialog box appears.
- 2 Click **Add**.
- 3 Click a gateway with ISAKMP (dynamic) key negotiation type to associate with this tunnel. Click **OK**.
- 4 Type a tunnel name.
Policy Manager uses the tunnel name as an identifier.
- 5 Click the **Phase 2 Settings** tab.
The Phase 2 fields appear, as shown in the following figure.

Security Association Proposal (SAP)

Type: ESP (Encapsulated Security Payload)

Authentication: SHA1-HMAC

Encryption: 3DES-CBC

☒ Force key expiration:

every 8192 kilobytes

every 24 hours

- 6 Use the **Type** drop list to select a Security Association Proposal (SAP) type.
Options include: Encapsulated Security Payload (ESP) or Authenticated Headers (AH).
- 7 Use the **Authentication** drop list to select an authentication method.
Options include: None (no authentication), MD5-HMAC (128-bit algorithm), and SHA1-HMAC (160-bit authentication algorithm).
- 8 Use the **Encryption** drop list to select an encryption method.
Options include: None (no encryption), DES-CBC (56-bit), and 3DES-CBC (168-bit encryption).
- 9 To have a new key generated periodically, enable the **Force Key Expiration** checkbox.
With this option, transparent to the user, the ISAKMP controller generates and negotiates a new key for the session. For no key expiration, enter 0 (zero) here. If you enable the Force Key Expiration checkbox, set the number of kilobytes transferred or hours passed in the session before a new key is generated for continuation of the VPN session.
- 10 Click **OK**.
The Configure Tunnels dialog box appears displaying the newly created tunnel. Repeat the tunnel creation procedure until you have created all tunnels for this gateway.
- 11 After you add all tunnels for this gateway, click **OK**.
The Configure Gateways dialog box appears.
- 12 To configure more tunnels for another gateway, click **Tunnels**. Select a new gateway and repeat the tunnel creation procedure for that gateway.
- 13 When all tunnels are created, click **OK**.

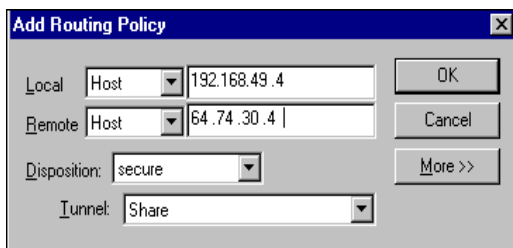
Creating a Routing Policy

Routing policies are sets of rules, much like packet filter rules, for defining how outgoing IPSec packets are built. They also determine whether incoming IPSec packets can be accepted. Policies are defined by their endpoints. These are not the same as tunnel or gateway endpoints—endpoints that define policies are the specific hosts or networks attached to the tunnel's Fireboxes (or other IPSec-compliant devices) that communicate through the tunnel.

From the **IPSec Configuration** dialog box:

- 1 Click **Add**.

The Add Routing Policy dialog box appears, as shown below.



- 2 Use the **Local** drop list to select the tunnel type of the IP address behind the local Firebox.
The tunnel type can be an entire network or a single host.
- 3 Enter the IP or network address in slash notation for the local host or network.
- 4 Use the **Remote** drop list to select the tunnel type of the IP address of the remote Firebox or IPSec-compliant device.
- 5 Enter the IP address or network address in slash notation for the remote host or network.
- 6 Use the **Disposition** drop list to select a bypass rule for the tunnel:

Secure

IPSec encrypts all traffic that matches the rule in associated tunnel policies.

Block

IPSec does not allow traffic that matches the rule in associated tunnel policies.

Bypass

IPSec passes traffic that matches this rule without encryption; that is, this traffic will “bypass” the IPSec routing policy.

NOTE

For every tunnel created to a dropped-in device, you must create a host policy for both sides’ external IP addresses that has protection set to Bypass. Otherwise, traffic to and from the dropped-in device’s external IP address will conflict with any network policy associated with the VPN. In addition, make sure Bypass policies are at the top of the policy list or move them accordingly, as explained in “Changing IPSec policy order” on page 90.

- 7 If you chose **Secure** as your disposition, use the **Tunnel** drop list to select a configured tunnel.

To configure a new tunnel, see “Creating a Tunnel with Manual Security” on page 83 or “Creating a Tunnel with Dynamic Key Negotiation” on page 86. To display additional information about the selected tunnel, click **More**.

- 8 If you want to restrict the policy to a specific source port, destination port, or protocol, click **More**.

The fields for ports and protocol appear, as shown below.



The image shows a configuration window with three fields: "Dst Port:" with a text input containing "0", "Protocol:" with a dropdown menu showing "*", and "Src Port:" with a text input containing "0".

- 9 To restrict the policy to a single destination port, in the **Dst Port** field, enter the remote host port.

The remote host port number is optional. The port number is the port to which WatchGuard sends communication for the policy. To enable communications to all ports, enter zero (0).

- 10 Use the **Protocol** drop list to limit the protocol used by the policy.

Options include: * (specify ports but not protocol), TCP, and UDP.

- 11 To restrict the policy to a single source port, in the **Src Port** field, enter the local host port.

The local host port number is optional. The port number is the port from which WatchGuard sends all communication for the policy. To enable communication from all ports, enter zero (0).

12 Click **OK**.

The IPSec Configuration dialog box appears listing the newly created policy. Policies are listed in the order in which they were created. To change the order, see the next section.

Changing IPSec policy order

WatchGuard handles policies in the order listed, from top to bottom, on the **IPSec Configuration** dialog box. Initially, the policies are listed in the order created. You must manually reorder the policies from more specific to less specific to ensure that sensitive connections are routed along the higher-security tunnels. In general, WatchGuard recommends the following policy order:

- Host to host
- Host to network
- Network to host
- Network to network

Policies must be set to the same order at both ends of the tunnel.

From the **IPSec Configuration** dialog box:

- To move a policy up in the list, click the policy. Click **Move Up**.
- To move a policy down in the list, click the policy. Click **Move Down**.

Configuring multiple policies per tunnel

If you use two or more policies for a tunnel, the order must be identical on each Firebox. For example, suppose Firebox1 and Firebox2 have a tunnel defined between them and both Fireboxes have Policy A and Policy B. For the tunnel to operate, both Fireboxes must define Policy A followed by Policy B. If, instead, one Firebox has Policy A defined first and the other has Policy B defined first, the tunnel will not operate.

Configuring services for BOVPN with IPSec

Access control is a critical part of configuring a secure VPN environment. If machines on the branch office VPN network are compromised, attackers obtain a secure tunnel to the Trusted network.

Users on the remote Firebox are technically outside the Trusted network; you must therefore configure the Firebox to allow traffic through the VPN

connection. A quick method is to create a host alias corresponding to the VPN remote networks and hosts. Then, use either the host alias or individually enter the remote VPN networks and hosts when configuring the following service properties:

Incoming

- Enabled and Allowed
- From: Remote VPN network, hosts, or host alias
- To: Trusted or selected hosts

Outgoing

- Enabled and Allowed
- From: Trusted network or selected hosts
- To: Remote VPN network, hosts, or host alias

For more information on configuring services, see the “Configuring Filtered Services” chapter in the WatchGuard Firebox System *User Guide*.

Allow VPN access to any services

To allow all traffic from VPN connections, add the Any service to the Services Arena and configure it as described above.

Allow VPN access to selective services

To allow traffic from VPN connections only for specific services, add each service to the Services Arena and configure each as described above.

Configuring IPSec Tunnels with VPN Manager

WatchGuard VPN Manager offers speed and reliability through drag-and-drop tunnel creation, automatic wizard launching, and the application of templates. With VPN Manager, you create fully authenticated and encrypted IPSec tunnels in minutes, and you can be assured that they do not clash with other tunnels or security policies.

From the same GUI, you can then administer and monitor the tunnels and view the status of the various components and tunnels at a glance. For more information on monitoring tunnels using VPN Manager, see Chapter 9, “Monitoring VPN Tunnels.”

VPN Manager also provides a secure way to remotely manage SOHOs. For more information, see Chapter 10, “Managing the SOHO with VPN Manager.”

Steps in creating VPNs using VPN Manager

To configure VPN Manager you must:

- Designate a Firebox as a DVCP server and Certificate Authority (CA)
- (Dynamic devices only) Add Fireboxes or SOHOs as devices to the VPN Manager device list
- (Dynamic devices only) Configure the Firebox as a DVCP client
- Build policy templates to designate which networks are accessible through VPN tunnels
- Build security templates to set encryption level and authentication type
- Create tunnels between devices

Defining a Firebox as a DVCP Server and CA

The first step in setting up a VPN tunnel using VPN Manager is defining a Firebox as a DVCP server. This automatically activates the certificate authority on the Firebox, whether you choose to authenticate by way of certificates or shared keys.

For information on defining the Firebox as a DVCP server and CA, see Chapter 3, “Activating the Certificate Authority on the Firebox.”

Installing VPN Manager

VPN Manager is bundled with the WatchGuard Firebox System software, but it is available for use only if you enable the VPN Manager checkbox when installing WFS and enter your license key.

- 1 Insert the WatchGuard Firebox System CD.
If the installation wizard does not start automatically, double-click install.exe in the root directory of the CD.
- 2 On the Select Components screen of the installation wizard, click the checkbox marked **VPN Manager**.
- 3 Enter the VPN Manager license key found on your license key certificate.

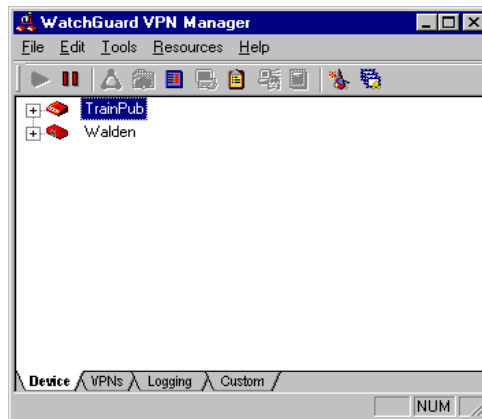
If you have already installed the WatchGuard Firebox System and forgot to click the checkbox marked **VPN Manager**, or if you purchased the option after the initial install, rerun the setup program and select the correct checkbox.

Launching VPN Manager

If you have already installed VPN Manager, start the application as follows:

- 1 **Start ⇒ Programs ⇒ WatchGuard ⇒ VPN Manager.**
- 2 When prompted, enter the configuration passphrase the Firebox functioning as your DVCP server.

The VPN Manager UI appears, as shown in the following figure.



Adding Devices to VPN Manager (Dynamic Devices Only)

If the devices enabled as DVCP clients use dynamic IP addresses, you must manually add them to your VPN configuration. This step is unnecessary if you are using static devices.

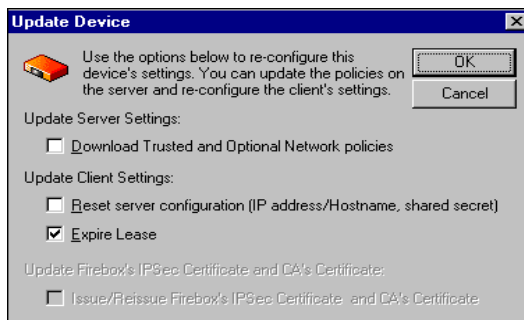
From VPN Manager:

- 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 status and configuration passphrases.
- 7 If you specified a device type with a dynamic IP address, enter the shared secret. Click **Next**.
- 8 Specify the default method used to authenticate tunnels with this Firebox: autogenerated shared key or Firebox certificate (RSA signature). Click **Next**.
If the Firebox is running WFS 5.0 or earlier, the certificate option is not supported.
If you select to authenticate using certificates, you must use the WatchGuard Security Event Processor for logging.
- 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 page is optional.
- 11 The wizard then displays a page describing what the steps will be performed next. 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.

Updating a device's settings

You can use the **Update Device** dialog box to reconfigure the settings of a selected device.

- 1 From the **VPNs** tab, right-click a device and select **Update Device**.
The Update Device dialog box appears, as shown in the following figure.



- 2 Change the settings as desired. The issue/reissue option forces a reissue of both the client and the root certificate. This is generally not necessary because a new certificate is downloaded every time the device is restarted.

Defining a Firebox as a DVCP Client (Dynamic Fireboxes Only)

If you are creating a tunnel to a Firebox with a dynamic IP address, you must define it as a DVCP client to enable VPN Manager to contact it.

From Policy Manager:

- 1 Select **Network** ⇒ **DVCP Client**.
- 2 Enable the checkbox marked **Enable this Firebox as a DVCP Client**.
- 3 In the **Firebox Name** field, specify the name of the Firebox.
- 4 To log messages for the DVCP client, enable the checkbox marked **Enable debug log messages for the DVCP Client**.
- 5 To add DVCP servers that the client can communicate with, click **Add**.
- 6 Enter the IP address. Enter the shared secret. Click **OK**.
- 7 Reboot the Firebox.
The Firebox contacts the DVCP server.

Adding Policy Templates

One of the benefits of a VPN is that you can define (and limit) the networks 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 Select 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 (shown at right).

The Device Policy dialog box for that device appears, as shown in the following figure.

The Device Policy dialog box is shown. It has a title bar and a main area. At the top left, there is a document icon and a text box with the following text: "A policy defines which hosts and/or networks behind a device are shared and secured. Use this page to add, edit, or remove resources for this device." To the right of this text are three buttons: "OK", "Cancel", and "Help". Below the text box is a "Policy Name:" label followed by a text box containing "policy_00002". Below that is a "Type:" label followed by a dropdown menu showing "Branch Office Tunnel". Below the dropdown is a "Resources:" label followed by a large empty text box. At the bottom of the dialog are three buttons: "Add...", "Edit...", and "Remove".

- 3 Enter a policy name of your choosing.
- 4 Specify whether the tunnel is a branch office tunnel or a telecommuter tunnel (if the device is a SOHO).
- 5 If you are defining a policy template for a Telecommuter tunnel, enter an unused IP address from the Firebox's Trusted network. Enter the IP address of the machine behind the SOHO that will use this tunnel.
- 6 Click **OK**.

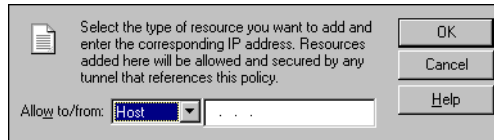
The policy template is defined and is now available in the VPN Wizard when creating a VPN tunnel involving that device.

Adding resources to a policy template

From the **Device Policy** dialog box:

- 1 Click **Add**.

The Resource dialog box appears, as shown in the following figure.



- 2 Select the type of resource you want and enter its IP address. Click **OK**.

Adding Security Templates

A security template specifies the encryption level and authentication type for a tunnel.

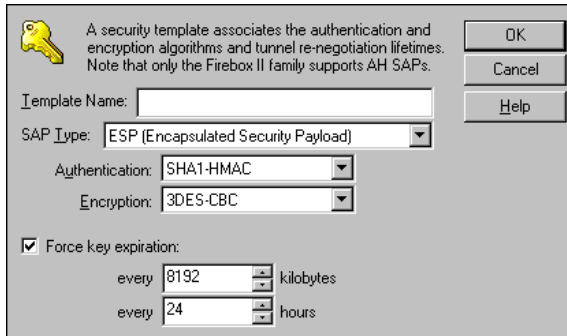
Default security templates are provided for available encryption levels. You can also create new templates. A variety of security templates makes it easy to match the appropriate level of encryption and type of authentication to the tunnel created with the Configuration wizard.

From the VPN Manager display:

- 1 Click the **VPN** tab.
- 2 Right-click anywhere in the window, and select **Insert Security Template** or click the Insert Security Template icon (shown at right).

The Security Template dialog box appears, as shown in the following figure.





A security template associates the authentication and encryption algorithms and tunnel re-negotiation lifetimes. Note that only the Firebox II family supports AH SAPs.

Template Name:

SAP Type:

Authentication:

Encryption:

☒ Force key expiration:

every kilobytes

every hours

OK Cancel Help

- 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, hours, or both. If you specify both, the key expires at whichever time arrives earliest. 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**.

Creating Tunnels Between Devices

You can define a tunnel either using the drag-and-drop method or the VPN Manager Configuration Wizard.

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 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 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

This method is the only one you can use to create tunnels for dynamically addressed SOHO devices.

From VPN Manager:

- 1 Click the **VPNs** tab.
- 2 Select **Edit ⇒ Create a New VPN** or click the Create New VPN icon (shown at right).
This launches the VPN Manager Wizard.



- 3 **Click Next.**
The wizard displays two listboxes that each list all the devices registered in VPN Manager.
- 4 Select a device from each listbox to be the endpoints of the tunnel you are creating.
- 5 Select the policy templates for each device's end of the tunnel.
The listbox displays any templates added to VPN Manager.
- 6 **Click Next.**
The wizard displays the Security Template dialog box.
- 7 Choose the appropriate security template for this VPN. **Click Next.**
The wizard displays the DVCP configuration.
- 8 Select 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 wait until a given device's lease expires, at which time VPN Manager automatically uploads the new configuration.

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 network). This tunnel is called a SOHO Telecommuter tunnel and is useful for situations where an employee sets up a home configuration such that his or her family's network is behind a SOHO, but only one computer—the telecommuter's—is allowed access to corporate resources available through 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 **Remote Gateways VPN** from the menu on the left.
- 3 Select **VPN Manager Telecommuter** from the drop list.

4 Click **Enable Remote Gateway**.

5 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.

Unique Name or ID

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

Local Address Allowed to Use VPN

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

6 Click **Submit**.

Creating a Policy for a Telecommuter

A SOHO enabled for a VPN Manager Telecommuter tunnel does not have an associated policy. You must create a policy for this device in 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.

Editing a Tunnel

All tunnels you have created are visible on the **VPNs** tab of VPN Manager. VPN Manager allows you to edit the tunnel name, security template, endpoints, and the policy used.

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**.

The Device Properties dialog box appears, as shown in the following figure.

A DVCP Device can participate in VPNs as defined by the list of tunnels. VPN Manager can also provide real-time status of all configured devices.

Display Name: test(Server)

Firebox Type: Firebox

Hostname/IP Address: 192.168.49.4

Status Passphrase: *****

Configuration Passphrase: *****

Shared Secret:

Lease Time: 60 minutes

IPSec Tunnel Authentication: Shared Key

If this device has WINS and/or DNS servers you want to share with remote devices, you can enter them here.

WINS Primary: . . . WINS Secondary: . . .

DNS Primary: . . . DNS Secondary: . . .

Domain Suffix:

Contact Information:

Contact List...

- 4 Click **OK** to save the change.
When the tunnel is renegotiated, the changes are applied.

Removing Tunnels and Devices from VPN Manager

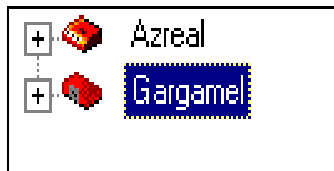
To remove a device from VPN Manager, you must first delete any tunnels for which that device is an endpoint.

Removing a tunnel

- 1 From VPN Manager, click the **VPNs** tab.
- 2 Expand the **Managed VPNs** folder to reveal the tunnel to be deleted.
- 3 Right-click the tunnel.
- 4 Select **Remove**. When asked to confirm, click **Yes**.
- 5 When prompted to issue a restart command to the devices affected by this removal, click **Yes**.

Removing a device

- 1 From VPN Manager, click either the **Devices** or **VPNs** tab.
Either the Devices tab (left figure below) or the VPNs tab (right figure below) appears.



Device tab (left) and VPN tab (right)

- 2 If you are using the **VPNs** tab, expand the **Devices** folder to reveal the device to be deleted.
- 3 Right-click the device.
- 4 Select **Remove**. When asked to confirm, click **Yes**.

Allowing Remote Access to the DVCP Server

When running VPN Manager on a remote host, external from the Firebox designated as the DVCP server, you must allow incoming access.

From Policy Manager:

- 1 Double-click the WatchGuard icon, shown at right, in the Services Arena.
- 2 On the **Incoming** tab, beneath the **From** field, click **Add**.
The Add Address dialog box appears.
- 3 Click **Add Other**.
The Add Member dialog box appears.
- 4 From the **Choose Type** drop list, click **Host IP Address**.
- 5 Enter the IP address of the VPN Manager station in the **Value** field. Click **OK**.
- 6 Under **To**, click **Add**.
The Add Address dialog box appears.
- 7 Click **Firebox**. Click **Add**. Click **OK**.

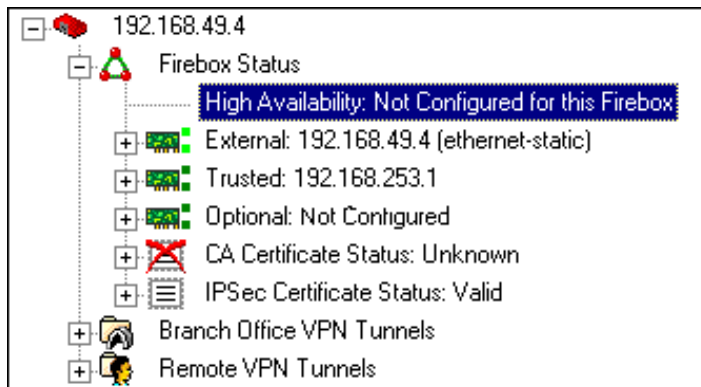


Monitoring VPN Devices and Tunnels

To properly manage a VPN environment, you need real-time information on its components. Current status of all VPN devices and tunnels appears on Control Center and on the VPN Manager display. You can use this information to determine current device status, to diagnose problems, and to plan how various devices need to be configured or reconfigured.

Monitoring VPNs from Control Center

The section in Control Center directly below the front panel shows the current status of the branch office, RUVPN, and MUVPN tunnels (both RUVPN and MUVPN tunnels are grouped under the Remote VPN Tunnels heading). The following figure shows the tunnel status information in Control Center, located beneath the information on Firebox status.



Expanding and collapsing the display

To expand a branch of the display, click the plus sign (+) next to the entry, or double-click the name of the entry. To collapse a branch, click the minus sign (–) next to the entry. A lack of either a plus or minus sign indicates that there is no further information about the entry.

Red exclamation point

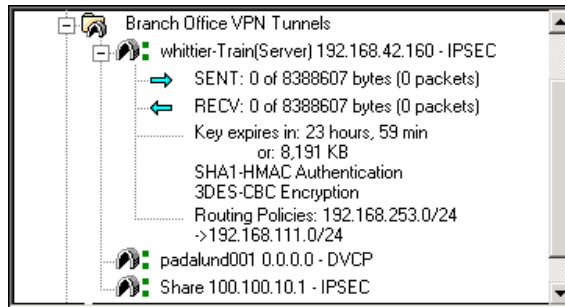
A red exclamation point appearing next to a device or tunnel indicates that something within its branch is not functioning properly. For example, a red exclamation point next to the Firebox entry indicates that the Firebox is not communicating with either the WatchGuard Security Event Processor or Management Station. A red exclamation point next to a tunnel listing indicates a tunnel is down.

When you expand an entry with a red exclamation point, another exclamation point appears next to the specific device or tunnel with the problem. Use this feature to rapidly identify and locate problems in your VPN network.

Branch Office VPN tunnels

The first piece of VPN information displayed in Control Center is the status of branch office VPN tunnels. The figure below shows an expanded entry for a BOVPN tunnel. The information displayed, from top to bottom, is:

- The name assigned to the tunnel during its creation, along with the IP address of the destination IPsec device (such as another Firebox, SOHO, or SOHO | tc), and the tunnel type (IPsec or DVCP). If the tunnel is DVCP, the IP address refers to the entire remote network address rather than that of the Firebox or equivalent IPsec device.



- The amount of data sent and received on that tunnel in both bytes and packets.
- The time at which the key expires and the tunnel is renegotiated. Express expiration time as a time deadline or in bytes passed. DVCP tunnels configured for both traffic and time deadline expiration thresholds display both; this type of tunnel expires when either event occurs first (time runs out or bytes are passed).
- Authentication and encryption levels set for that tunnel.
- Routing policies for the tunnel.

MUVPN and RUVPN tunnels

Following the branch office VPN tunnels is an entry for Mobile User VPN or RUVPN with PPTP tunnels.

If the tunnel is Mobile User VPN, the branch displays the same statistics as for the DVCP or IPsec Branch Office VPN described previously. The entry shows the tunnel name, followed by the destination IP address, followed by the tunnel type. Below are the packet statistics, followed by the key expiration, authentication, and encryption specifications.

If the tunnel is RUVPN with PPTP, the display shows only the quantity of sent and received packets. Byte count and total byte count are not applicable to PPTP tunnel types.

Monitoring VPNs through VPN Manager

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.

The VPN Manager main window 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. The information that appears 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.

Opening the VPN Manager Display

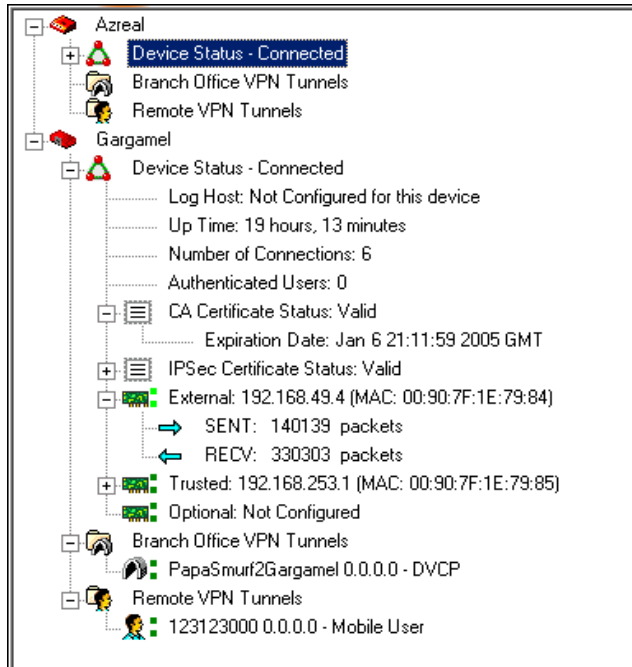
To open VPN Manager, from the Windows interface:

- 1 Select **Start** ⇒ **Programs** ⇒ **WatchGuard** ⇒ **VPN Manager**. You may be prompted for the configuration passphrase of the Firebox designated as your DVCP server.

VPN Manager connects to the DVCP server and displays the VPN and device configuration, distributed appropriately among the four tabs on the display.

Device Status

Click the **Devices** tab of the VPN Manager display to view the real-time status of all devices being managed by DVCP. An example of the information shown on this tab appears in the figure below.



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.

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 VPN Manager.

Yellow exclamation point

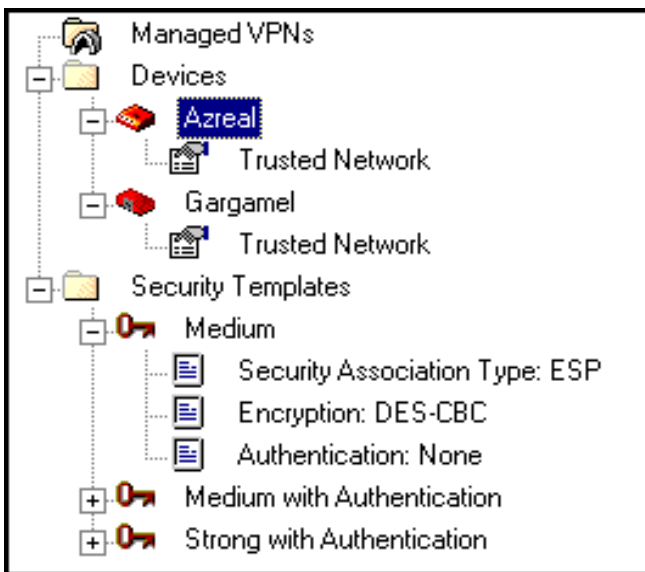
Questionable operation. VPN Manager is trying to contact the device. The exclamation point will either resolve or turn red.

Red exclamation point

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

Tunnel status

Click the **VPNs** tab of the VPN Manager display to view the IPsec tunnels configured. This portion of the display, as shown in the following figure, includes information on devices and security templates, including security association type, encryption types, and authentication type.



Log server status

Click the **Logging** tab of the VPN Manager display to view log servers in the VPN environment. The list of servers in use is compiled from the

configuration files of the devices under management. The display also lists devices for which logging is not configured. (Logging for devices is configured in Policy Manager, as described in the WatchGuard Firebox System User Guide.)



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.

For example, suppose your enterprise is very large, consisting of a hundred or more devices. You could use the custom view to group devices into manageable units according to variables such as region, business affiliation, operating units, and so on.

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** option.
The device appears on the Custom tab. You can select the device name and drag it to a new location in the window, or into a folder.

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. Enter a name for the folder.

Managing the SOHO with VPN Manager

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 from his or her home.

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)—the industry-standard method for protecting Internet communication.

Importing Certificates

When you define a Firebox as a DVCP server, a certificate file is created and stored in the directory where you installed the WatchGuard Firebox System software. For example, a path of a certificate file might appear as follows:

```
c:\Program Files\WatchGuard\Certificates\[DVCP Server's  
IP Address]\SOHO-Admin.p12
```

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

MS Internet Explorer 5.5 and 6.0

From the VPN Manager desktop:

- 1 Launch the browser and select **Tools** ⇒ **Internet Options**.
The Internet Options window appears.
- 2 Click the **Content** tab. Click **Certificates**.
The Certificates window appears.
- 3 Click the **Personal** tab. Click **Import**.
The Certificate Import Wizard appears.
- 4 Click **Next**.
- 5 Browse to the file location, select it, and click **Open**.
- 6 Click **Next**.
- 7 Enter the configuration passphrase of the DVCP server and click **OK**.
- 8 Click **Next**.
- 9 Enable the **Automatically select the certificate store based on the type of certificate** option, and then click **Next**.
- 10 Click **Finish**.
A window appears indicating that the certificate has been successfully imported.

Troubleshooting tips

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

- Verify that you have the strong encryption (128-bit) version of Internet Explorer.
- Verify that you have the correct password for the .p12 (or .pfx) file. This must be the configuration passphrase of the Firebox that is acting as your DVCP server.
- Verify that the certificate file is not zero (0) length. If it is, delete the file, disconnect from VPN Manager, and run it again.
- Sometimes, at installation, Internet Explorer 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

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

Netscape Communicator 4.79

From the VPN Manager desktop:

- 1 Launch the browser and select **Communicator** ⇒ **Tools** ⇒ **Security Info**.
The Security Info window appears.
- 2 From the navigation menu on the left, select **Certificates** ⇒ **Yours**.
- 3 Click **Import a Certificate**.
The File to Import window appears.
- 4 Browse to the file location, select it, and click **Open**.
The Password Entry Dialog box appears.
- 5 Enter the configuration passphrase of the DVCP server and click **OK**.
A window appears indicating that the certificate has been successfully imported.
- 6 Click **OK** to return to the Certificates window.
The imported certificate appears within the appropriate field.
- 7 Click **OK** to return to the browser.

Netscape 6

From the VPN Manager desktop:

- 1 Launch the browser and select **Tasks** ⇒ **Privacy and Security** ⇒ **Security Manager**.
The Netscape Personal Security Manager window appears.
- 2 Click the **Certificates** tab.
- 3 From the navigation menu on the left, click **Mine**.
- 4 Click **Restore**.
The File Name to Restore window appears.
- 5 Browse to the file location, select it, and click **Open**.
The Password window appears.
- 6 Enter the configuration passphrase of the DVCP server and click **OK**.
A window appears indicating that the certificate has been successfully restored.
- 7 Click **OK** to return to the Personal Security Manager window.
The imported certificate appears within the appropriate field.
- 8 Click **Close** to return to the browser.

Troubleshooting tips

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

- Verify that you have the strong encryption (128-bit) version of Netscape.
- Verify that you have the correct password for the .p12 (or .pfx) file. This must be the configuration passphrase of the Firebox that is your DVCP server.
- Verify that the certificate file is not zero (0) length. If it is, delete the file, disconnect from VPN Manager, and run it again.

Accessing the SOHO

Now that you have imported the proper certificate into your browser, you are ready to use VPN Manager to remotely access the device to monitor and manage the SOHO.

You cannot use the same browser to access the SOHO as the one used to access the CA Manager. For more information on accessing the CA Manager, see “Managing the Certificate Authority” on page 34. You must close the CA Manager browser before attempting to access the SOHO from VPN Manager.

From VPN Manager:

- 1 Select the SOHO device you want to access 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**.
- 3 Click **OK**.
The SOHO System Status page appears.

All SOHO management functions that would normally be available locally through a Web browser are now available remotely and securely.

System Status

The System Status page is effectively the configuration home page of the SOHO. A variety of information is revealed to provide a comprehensive display of the SOHO configuration:

- The firmware version
- A few of the SOHO features and their status as Enabled or Disabled
- Upgrade options and their status
- Configuration information for both the Trusted and External networks
- Firewall settings (Incoming and Outgoing services)
- A reboot button to restart the SOHO

Network

From the Navigation bar on the left, click Network to:

- Configure the SOHO network settings for both the External and Trusted Networks
- Configure static routes in order to pass traffic to networks on separate segments
- View a variety of network statistics to assist in monitoring data traffic as well as troubleshooting potential problems

Administration

From the Navigation bar on the left, click **Administration** to:

- Enable System Security passphrases and allow Remote Management
- Enable VPN Manager access
- Update the SOHO from a non-Windows operating system
- Upgrade the SOHO features
- View the configuration file as text

System security and remote management

Here you enable system security, assign an administrator name to the device, and set the passphrases.

You can also enable the SOHO for remote management. This allows you to connect to the unit remotely using the WatchGuard Remote Management VPN client. Set the virtual IP address to be provided to your remote computer upon connection as well as the authentication and encryption algorithms used to secure the connection.

Firewall

From the Navigation bar on the left, click **Firewall** to:

- Configure the incoming and outgoing services.
- Define blocked sites
- Enable various firewall options, such as:
 - Do not respond to Ping requests received on External Network
 - Do not allow FTP access to Trusted Network interface
 - Disable SOCKS proxy
 - Log all allowed outbound access
- Configure a DMZ for a single host

Logging

From the Navigation bar on the left, click **Logging** to:

- View the SOHO Event Log—this displays various log entry messages
- Configure the SOHO to send logs to a WSEP (WatchGuard Security Event Processor)
- Configure the SOHO to send logs to a Syslog server
- Configure the System Time

WebBlocker

From the Navigation bar on the left, click **WebBlocker** to enable and configure this feature. WebBlocker filters your users' access to Web sites by category.

VPN

From the Navigation bar on the left, click **VPN** to:

- Configure remote gateways to create BOVPN tunnels between the SOHO and other IPSec-compliant devices
- Configure MUVPN clients to create Mobile User VPN tunnels to the SOHO
- View various statistics regarding existing tunnels

Removing Certificates

Certain situations might require you to update the certificates that VPN Manager uses. For example, if the configuration passphrase of the Firebox defined as the DVCP server is changed or if you are reinstalling the DVCP server, you will need to update the certificates. The certificates must be removed, and then new certificates must be generated and used.

MS Internet Explorer 5.5 and 6.0

From the VPN Manager desktop:

- 1 Launch the browser and select **Tools ⇒ Internet Options**.
The Internet Options window appears.
- 2 Click the **Content** tab. Click **Certificates**.
The Certificates window appears.
- 3 Select the certificate or certificates you want to remove.
- 4 Click **Remove**.
A warning window appears.
- 5 Click **Yes**.
The selected certificates are deleted from the browser.
- 6 Click **Close** and then click **OK** to return to the browser.

After you have removed the certificates from your browser, you must delete them from your computer.

From VPN Manager:

- Select **File ⇒ SOHO Management ⇒ Clean up on PC**.

Netscape Navigator 4.79

From the VPN Manager desktop:

- 1 Launch the browser and select **Communicator** ⇒ **Tools** ⇒ **Security Info**.
The Security Info window appears.
- 2 From the navigation menu on the left, select **Certificates** ⇒ **Yours**.
- 3 Select the certificate or certificates you want to remove.
- 4 Click **Delete**.
A warning window appears.
- 5 Click **OK**.
The selected certificates are deleted from the browser.
- 6 Click **OK** to return to the browser.

After you have removed the certificates from your browser, you must delete them from your computer.

From VPN Manager:

- Select **File** ⇒ **SOHO Management** ⇒ **Clean up on PC**.

Netscape 6

From the VPN Manager desktop:

- 1 Launch the browser and select **Tasks** ⇒ **Privacy and Security** ⇒ **Security Manager**.
The Netscape Personal Security Manager window appears.
- 2 Click the **Certificates** tab.
- 3 From the navigation menu on the left, select **Mine**.
- 4 Select the certificate or certificates you want to remove.
- 5 Click **Delete**.
A warning window appears.
- 6 Click **Delete**.
The selected certificates are deleted from your browser.
- 7 Click **Close** to return to the browser.

After you have removed the certificates from your browser, you must delete them from your computer. From VPN Manager:

- Select **File** ⇒ **SOHO Management** ⇒ **Clean up on PC**.

Index

.exp files 60
.p12 file 29, 70
.wgx files 29, 59, 60

A

Add Address dialog box 47, 106
Add Member dialog box 106
Add Routing Policy dialog box 88
Advanced Export File Preferences dialog box 66
Advanced Mobile User VPN Policy Configuration dialog box 65
Aggressive Mode 83
AH
 configuring 85
 described 3, 84
Any service
 and MUVPN 68, 69
 and RUVPN 45
Authenticated Headers. See AH
authentication
 DES, TripleDES 5
 described 4
 for VPNs, viewing 109
 selecting method for 13
authentication server
 described 4
 specifying 64
 types supported 46, 63
Authentication Servers dialog box 42
authentication, extended. See extended authentication

B

Basic DVCP Server Configuration dialog box 74, 76, 77
BOVPN
 and certificate-based authentication 9
 described 8
 monitoring tunnels 108
BOVPN with Basic DVCP
 creating tunnel to SOHO 74
 modifying tunnels 76

 removing tunnels 76
 requirements for 73
 scenario 22
 setting encryption type 75
 setting logging options for 77
 specifying authentication method 75
 specifying encryption 74
 specifying key expiration time 75
 when to use 19
BOVPN with Manual IPsec
 adding gateways 80
 advantages of 10
 allowing access to services 91
 changing IPsec policy order 90
 configuring a gateway 80
 configuring a tunnel with manual security 83
 configuring AH 85
 configuring key negotiation type 81
 configuring services for 90
 configuring tunnels with dynamic key negotiation 86
 creating routing policies 88
 described 10, 79
 editing gateways 83
 editing, removing gateways 83
 enabling Aggressive Mode 83
 enabling Perfect Forward Secrecy 83
 encryption levels 10, 79
 Phase 1 settings 82
 Phase 2 settings 84, 86
 requirements for 79
 selecting bypass rule 88
 specifying authentication method 81, 82
 specifying Diffie-Hellman group 83
 specifying encryption 82
 using certificates 82
 using Encapsulated Security Protocol 85
 when to use 20
BOVPN with VPN Manager
 adding devices to 95
 adding policy templates 98
 adding security templates 99
 allowing remote access to DVCP server 106
 creating tunnels 100, 101
 defining Firebox as DVCP client 97
 described 10
 editing tunnels 104
 enabling SOHO single-host tunnel 102
 removing devices and tunnels 105
 scenario 22
 when to use 20
branch office VPN. See BOVPN
bypass rules for tunnels 88

C

- CA. See certificate authority
- cacert.pem 29, 70
- certificate authority
 - described 14, 27
 - designating as subordinate 35
 - designating Firebox as 31
 - enabling debug log messages for 32
 - Firebox as, scenarios 30
 - managing 34
 - restarting 36
 - scenarios 28
- certificate revocation list (CRL)
 - described 28
 - publication period for 32
 - publishing 35
 - selecting endpoint for 32
- certificates
 - and logging 34
 - described 4, 14, 28
 - destroying 36
 - files in end-user profile 70
 - generating new 34
 - importing to VPN Manager 115
 - listing current 35
 - publishing 36
 - reinstating 36
 - removing 121
 - revoking 36
 - searching for 35
 - setting lifetimes of 32
- certificates, root. See root certificate
- Client for Microsoft Networks, installing 50
- Configure Gateways dialog box 80, 83
- Configure Tunnels dialog box 83, 86
- Control Center
 - components of 107
 - monitoring VPNs from 107
- Control Center Main Menu button 37
- CRL. See certificate revocation list

D

- debug logging, enabling for DVCP server 32
- DES 5, 14
- Device Policy dialog box 98, 99
- Device Properties dialog box 104
- devices
 - adding to VPN Manager 95
 - dynamic 95

- removing from VPN Manager 105
- updating settings of 96
- viewing connection status of 111
- viewing status 110
- dialog boxes
 - Add Address 47
 - Add Routing Policy 88
 - Advanced Export File Preferences 66
 - Authentication Servers 42
 - Basic DVCP Server Configuration 74, 76, 77
 - Configure Gateways 80, 83
 - Configure Tunnels 83, 86
 - Device Policy 98
 - Device Properties 104
 - IPSec Configuration 80, 83, 88
 - IPSec Logging 71, 77
 - New Server 33
 - Remote Gateway 80
 - Remote User Setup 47
 - Resource 99
 - Security Policy 101
 - Security Template 99, 102
 - Select Gateway 83
 - Setup Firebox User 43
 - Setup Remote User 43
 - Update Device 96
- Dial-Up Adapter #2, installing 50
- Diffie-Hellman
 - described 5
 - groups 5, 83
- digital certificates. See certificates
- DNS servers, configuring 41, 59
- DVCP
 - and certificates 11
 - and VPN Manager 10
 - basic 9
 - described 9, 73
- DVCP Client Wizard 73, 74, 76
- DVCP clients
 - defining Fireboxes as 97
 - described 73
 - SOHOs as 74
- DVCP cluster 28
- DVCP server
 - allowing remote access to 106
 - as CA 28
 - described 9, 73
 - enabling debug logging 32
 - friendly name for 33
 - setting logging options for 77
- dynamic security, configuring a tunnel with 86
- Dynamic VPN Configuration Protocol. See DVCP

E

Encapsulated Security Protocol. See ESP encryption

- activating strong 40
- and MUVPN 58
- and RUVPN with PPTP 40
- described 3, 5
- for VPNs, viewing 109
- levels of 3, 5, 40

end-user profiles for MUVPN users

- described 57
- distributing to remote users 70
- locking 66
- preparing 59
- regenerating 69
- saving 69

ESP

- configuring 85
- described 3, 84

extended authentication

- defining groups for 46, 63
- described 4, 7, 8
- specifying authentication method for 64
- specifying server 64

F

Fireboxes

- as CAs 14
- configuring for MUVPN 57
- configuring for RUVPN with PPTP 39
- defining as DVCP clients 97
- defining as DVCP server 31
- designating as CA 28, 31
- designating as DVCP server 94
- making outbound connections behind 56

fully meshed topology 16

G

gateways

- adding 80
- configuring 80
- described 80
- editing 83

groups, authentication 42

H

hub and spoke configuration 18

hub-and-spoke configuration 18

I

IKE

- and Diffie-Hellman group 83
- and Phase 1 settings 82
- described 4, 5
- logging options for 77
- phase 1,2 5

Internet

- accessing through IPSec tunnel 63
- accessing through PPTP tunnel 55
- accessing through tunnel 16

Internet Key Exchange. See IKE

Internet Security Association and Key Management Protocol. See ISAKMP

IP addresses

- and VPN design 14
- entering for RUVPN with PPTP 47

IPSec

- benefits of 3
- changing policy order 90
- described 2
- logging options for 77
- with VPN 9

IPSec Configuration dialog box 80, 83, 88

IPSec Logging dialog box 71, 77

ISAKMP

- and Diffie-Hellman groups 83
- and gateways 81
- described 5, 86

K

key pairs 28

L

log servers, viewing 112

logging

- for CA 32
- for DVCP server 77

M

- manual security, configuring tunnels with 83
- MD5-HMAC 14, 61, 75
- meshed topology 16
- Mobile User VPN wizard 61, 62, 64
- Mobile User VPN. See MUVPN
- MSDUN, and RUVPN 48
- MUVPN
 - allowing Internet access through 63
 - and certificates, scenarios 29
 - and IP addressing 15
 - and virtual adapters 67
 - authentication for 6, 57
 - configuring debugging options 71
 - configuring services to allow 67
 - configuring shared servers for 59
 - defining new user 60
 - described 6, 57
 - distributing end-user profiles 70
 - encryption levels for 6, 58
 - end-user profiles. See end-user profiles for MUVPN users
 - entering license keys 58
 - making outbound connections behind Firebox 71
 - modifying existing user 62
 - monitoring tunnels 109
 - preparing configuration files for 59
 - preparing end-user profiles 59
 - purchasing license for 57
 - scenario 23, 29
 - setting encryption for 61
 - specifying authentication method 61, 64
 - types of licenses for 6
 - when to use 20
 - with extended authentication 7, 24, 63

N

- NAT, and VPNs 15
- Network Connection wizard 54
- network topology
 - described 16
 - fully meshed 16
 - hub-and-spoke 18
 - partially meshed 18
- New Server dialog box 33

P

- partially meshed networks 18
- password authentication 4
- passwords
 - and security of VPN endpoints 14
 - described 4
- PEM format 36
- Perfect Forward Secrecy 83
- Phase 1
 - described 5
 - settings 82
- Phase 2
 - described 5
 - settings 84, 86
- PKCS12 format 36
- PKI 27
- policy templates
 - adding 98
 - adding resources to 99
- PPTP 3
- PPTP. See also RUVPN with PPTP
- pptp_users 42
- private key, public key 28
- public key cryptography 27
- Public Key Infrastructure (PKI) 27

R

- red exclamation point
 - in Control Center display 108
 - in VPN Manager display 112
- Remote Gateway dialog box 80
- Remote User Setup dialog box 47
- Remote User VPN. See RUVPN with PPTP
- Resource dialog box 99
- root certificate
 - described 28
 - publishing 35
 - reissuing 36
 - setting lifetime for 32
- routing policies
 - changing order of 90
 - configuring multiple 90
 - creating 88
 - described 10, 88
- RUVPN with PPTP
 - accessing the Internet with 55
 - activating 46
 - adding a domain name for NT 52

- and authentication groups 42
- and MSDUN 48
- and the Any service 45
- configuration checklist 39
- configuring debugging options 47
- configuring services to allow 44
- configuring shared servers for 41
- described 7, 39
- encryption levels 40
- entering IP addresses for 47
- installing client for Microsoft Networks 50
- installing Dial-Up Adapter #2 50
- IP addressing 15, 39
- making outbound connections behind a Firebox 56
- monitoring tunnels 109
- preparing client computers for 48
- preparing Windows 2000 remote host 53
- preparing Windows 98 remote host 49
- preparing Windows NT remote host 51
- preparing Windows XP remote host 54
- running 55
- starting 55
- system requirements for 49
- when to use 20
- with extended authentication 8

S

- Security Parameter Index (SPI) 85
- Security Policy dialog box 101
- Security Template dialog box 99, 102
- security templates, adding 99
- Select Gateway dialog box 83
- services
 - allowing VPN access to 91
 - configuring for BOVPN with Manual IPSec 90
 - configuring to allow MUVPN traffic 67
 - configuring to allow RUVPN traffic 44
- Setup Firebox User dialog box 43
- Setup Remote User dialog box 43
- SHA1-HMAC 61, 75
- SHA-HMAC 14
- shared secrets 4, 13
- SOHOs
 - as DVCP clients 74
 - creating tunnels for dynamic 101
 - creating tunnels to 74
 - remote management of 120
 - remotely accessing 118
 - single-host tunnels 102

- split tunneling
 - described 16
 - with PPTP, enabling 55

T

- Technical Support, VPN Installation Services 21
- TripleDES 5, 14
- tunneling protocols 2
- tunnels
 - and gateways 80
 - bypass rules for 88
 - configuring with dynamic security 86
 - configuring with manual security 83
 - created to dropped-in devices 89
 - creating to SOHOs 74
 - creating with Basic DVCP 74
 - creating with VPN Manager 93, 100
 - described 2
 - drag-and-drop creation 100
 - editing 104
 - menu-driven creation 101
 - modifying Basic DVCP 76
 - monitoring 108
 - multiple policies for 90
 - removing from VPN Manager 105
 - SOHO single-host 102
 - viewing 112

U

- Update Device dialog box 96
- Use Incoming Settings for Outgoing checkbox 85

V

- virtual adapter for MUVPN users 67
- VPN Installation Services 21
- VPN Manager
 - adding devices 95
 - and authentication via certificates 11
 - and DVCP 10
 - certificates in 115
 - creating custom view 113
 - described 10, 93
 - launching 95
 - opening UI 110
 - physical description 110
 - removing certificates 121

- UI 110
- viewing device status 110
- viewing log servers 112
- viewing tunnels 112
- VPNs
 - access control for 15
 - and IP addressing 14
 - and IPsec 9
 - and NAT 15
 - authentication methods for 13
 - described 2
 - design considerations 13, 14, 16, 17, 18, 21
 - monitoring 107
 - monitoring from Control Center 107
 - monitoring with VPN Manager 110
 - network topology 16
 - scenarios 21
 - split tunneling 16
 - terminating 72
 - WatchGuard solutions 19

W

- WatchGuard Security Event Processor, and certificates 34
- wg_pptp service icon 46
- Windows 2000, preparing for RUVPN with PPTP 53
- Windows 98
 - installing VPN adapter on 50
 - preparing for RUVPN with PPTP 49
- Windows NT
 - adding a domain name 52
 - installing a VPN adapter on 53
 - preparing for RUVPN with PPTP 51
- Windows XP, preparing for RUVPN with PPTP 54
- WINS servers, configuring 41, 59

X

XAUTH. See extended authentication

Y

- yellow exclamation point, in VPN Manager display 112