

VPN Administration Guide

Revision D

SafeNet SoftRemote Version 10.0

Sidewinder G₂ Version 6.0

Copyright

© 2003 Secure Computing Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Secure Computing Corporation.

Trademarks

Secure Computing, SafeWord, Sidewinder, SmartFilter, SofToken, Type Enforcement, and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. PremierAccess, G₂ Firewall, G₂ Enterprise Manager, Gauntlet, SecureOS, and MobilePass are trademarks Secure Computing Corporation. All other trademarks, tradenames, service marks, service names, product names, and images mentioned and/or used herein belong to their respective owners.

Software License Agreement

The following is a copy of the Software License Agreement as shown in the software:

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. BY CLICKING "I ACCEPT" BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. IF YOU DO NOT AGREE WITH THIS AGREEMENT, THEN CLICK "I DO NOT ACCEPT" BELOW AND RETURN ALL COPIES OF THE SOFTWARE AND DOCUMENTATION TO SECURE COMPUTING CORPORATION ("SECURE COMPUTING") OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

If this Software is being installed by a third party (for example, a value-added reseller, consultant, employee, or agent), such third party represents that it has the authority to bind the person or entity for whom the Software is being installed, and that its acceptance of this Agreement in the manner set forth above does bind such person or entity.

1. Grant of License. Secure Computing grants to you, and you accept, a non-exclusive, and non-transferable license (without right to sub-license) to use the Software Products as defined herein on a single machine.

2. Software Products. "Software Product(s)" means (i) the machine-readable object-code versions of the Software of Secure Computing contained in the media (the "Software"), (ii) the published user manuals and documentation that are made available for the Software (the "Documentation") and (iii) any updates or revisions of the Software or Documentation that you may receive (the "Update"). Under no circumstances will you receive any source code of the Software. Software Products provided for use as "backup" in the event of failure of a primary unit may be used only to replace the primary unit after a failure in fact occurs. They may not be used to provide any capability in addition to the functioning primary system that they backup.

3. Limitation of Use. You may not: 1) copy, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent, lease or sublicense all or any portion of the Software Product to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software Product in whole or in part; or 4) modify or prepare derivative works of the Software Products.

4. Limited Warranty and Remedies. Secure Computing warrants that the medium/media on which its Software is recorded is/are free from defects in material and workmanship under normal use and service for a period of ninety (90) days from the date of shipment to you.

Secure Computing does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The Software is furnished "AS IS" and without warranty as to the performance or results you may obtain by using the Software. The entire risk as to the results and performance of the Software is assumed by you. If you do not receive media which is free from defects in materials and workmanship during the 90-day warranty period, you will receive a refund for the amount paid for the Software Product returned.

5. Limitation Of Warranty And Remedies. THE WARRANTIES STATED HEREIN ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.

SECURE COMPUTING'S AND ITS LICENSORS ENTIRE LIABILITY UNDER, FOR BREACH OF, OR ARISING OUT OF THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE PRODUCT OR SERVICE THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR YOUR COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES WHETHER OR NOT SECURE COMPUTING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

6. Term and Termination. This license is effective until terminated. You may terminate it at any time by destroying the Software Product, including all computer programs and documentation, and erasing any copies residing on computer equipment. This Agreement also will automatically terminate if you do not comply with any terms or conditions of this Agreement. Upon such termination you agree to destroy the Software Product and erase all copies residing on computer equipment.

7. Ownership. This Software is licensed (not sold) to you. All intellectual property rights including trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights in or related to the Software Products are and will remain the property of Secure Computing or its licensors, whether or not specifically recognized or protected under local law. You will not remove any product identification, copyright notices, or other legends set forth on the Software Product.

8. Export Restrictions. You agree to comply with all applicable United States export control laws and regulations, including without limitation, the laws and regulations administered by the United States Department of Commerce and the United States Department of State.

9. U.S. Government Rights. Software Products furnished to the U.S. Government are provided on these commercial terms and conditions as set forth in DFARS 227.7202-1(a).

10. Entire Agreement. This Agreement is our offer to license the Software Product to you exclusively on the terms set forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have submitted (or hereafter submit) different, additional, or other alternative terms to Secure Computing or any reseller or authorized dealer, whether through a purchase order or otherwise, we object to and reject those terms. Without limiting the generality of the foregoing, to the extent that you have submitted a purchase order for the Software Product, any shipment to you of the Software Product is not an acceptance of your purchase order, but rather is a counteroffer subject to your acceptance of this Agreement without any objections or modifications by you. To the extent that we are deemed to have formed a contract with you related to the Software Product prior to your acceptance of this Agreement, this Agreement shall govern and shall be deemed to be a modification of any prior terms in their entirety.

11. General. Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing and signed by Secure Computing. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding shall not affect the validity of the other provisions of this Agreement. You may not assign this License or any associated transactions without the written consent of Secure Computing. This License shall be governed by and construed in accordance with the laws of California, without regard to its conflicts of laws provisions.

Other terms and conditions

This product contains software developed by the Net-SNMP project. Copyright © 1989, 1991, 1992 by Carnegie Mellon University. Copyright © 1996, 1998-2000 The Regents of the University of California. All Rights Reserved. Copyright © 2001-2002, Networks Associates Technology, Inc. All rights reserved. Portions of this code are copyright © 2001-2002, Cambridge Broadband Ltd. All rights reserved.

This product contains software developed through the Internet Software Consortium (<http://www.isc.org>). Copyright © 1996-2001 Internet Software Consortium. Portions Copyright © 1996-2001 Nominum, Inc.

This product contains software developed by Sendmail, Inc. Copyright © 1998-2001 Sendmail, Inc. All rights reserved.

This product includes software and algorithms developed by RSA Data Security Inc.

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

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>) Copyright © 1998-2000 The OpenSSL Project. All rights reserved.

This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).

This product utilizes MySQL (<http://www.mysql.com/>). Copyright © 1995, 1996, 2000 TcX AB & Monty Program KB & Detron Stockholm SWEDEN, Helsingfors FINLAND and Uppsala SWEDEN. All rights reserved.

This product incorporates compression code from the Info-ZIP group. There are no extra charges or costs due to the use of this code, and the original compression sources are freely available from <http://www.cdrom.com/pub/infozip/> or <ftp://ftp.cdrom.com/pub/infozip/> on the Internet.

This product includes software developed at the Information Technology Division, US Naval Research Laboratory. Copyright 1995 US Naval Research Laboratory (NRL). All Rights Reserved.

This product includes software developed by the University of California, Berkeley and its contributors. Copyright © 1991, 1992, 1993, 1994, 1995, 1996 Berkeley Software Design Inc. Copyright © 1997, 1998, 1999, 2000, 2001 Berkeley Software Design Inc. All rights reserved. Copyright © 2001 Wind River Systems, Inc. All rights reserved.

This product uses unmodified GNU software. GNU source code is available on request by contacting Secure Computing.

Pine and Pico are registered trademarks of the University of Washington. No commercial use of these trademarks may be made without prior written permission of the University of Washington. Pine, Pico, and Pilot software and its included text are Copyright 1989-1996 by the University of Washington.

Technical Support information

Secure Computing works closely with our Channel Partners to offer worldwide Technical Support services. If you purchased this product through a Secure Computing Channel Partner, please contact your reseller directly for support needs.

To contact Secure Computing Technical Support directly, telephone +1.800.700.8328 or +1.651.628.1500. If you prefer, send an e-mail to support@securecomputing.com. To inquire about obtaining a support contract, refer to our "Contact Secure" Web page for the latest information at www.securecomputing.com.

Customer Advocate information

To suggest enhancements in a product or service, or to request assistance in resolving a problem, please contact a Customer Advocate at +1.877.851.9080. If you prefer, send an e-mail to customer_advocate@securecomputing.com.

If you have comments or suggestions you would like to make regarding this document or any other Secure Computing document, please send an e-mail to techpubs@securecomputing.com.

Comments?

If you have comments or suggestions you would like to make regarding this document, please send an email to techpubs@securecomputing.com.

Printing history

Date	Part number	Software Release
March 2001	86-0935037-A	SoftPK 5.1.3 Build 4 and Sidewinder 5.1.0.02
February 2002	86-0935037-B	SoftRemote 7.0.1 and Sidewinder 5.2
June 2002	86-0935037-C	SoftRemote 8.0.1 and Sidewinder 5.2.1
May 2003	86-0935037-D	SoftRemote 10.0 and Sidewinder G ₂ Firewall 6.0

Table of Contents

Preface: About this Guide	ix
Who should read this guide?	ix
How this guide is organized	x
Where to find additional information	xi
Chapter 1: Getting Started	1-1
About SoftRemote & Sidewinder G ₂ VPNs	1-2
VPN requirements	1-3
Sidewinder G ₂ firewall requirements	1-3
SoftRemote requirements	1-4
Roadmap for deploying your VPNs	1-5
Chapter 2: Planning Your VPN Configuration	2-1
Identifying basic VPN connection needs	2-2
Identifying authentication requirements and configurations	2-3
Understanding pre-shared key authentication	2-3
Understanding Extended Authentication	2-4
Using digital certificate authentication	2-5
Determining where you will terminate your VPNs	2-8
Understanding Sidewinder G ₂ client address pools	2-10
Chapter 3: Configuring Sidewinder G₂ for	
SoftRemote Clients	3-1
Defining a virtual burb	3-2
Defining a client address pool	3-2
Enabling the VPN servers	3-4
Configuring rules & proxy entries for interburb passage	
of VPN connection traffic	3-6
Managing pre-shared keys (shared-passwords)	3-7
Managing Sidewinder G ₂ self-signed certificates	3-8
Creating & exporting a firewall self-signed certificate	3-8
Creating & exporting remote certificate(s)	3-10
Managing CA-based certificates	3-14

Requesting and retrieving a CA-issued root certificate	3-14
Requesting and retrieving a CA-issued firewall certificate . . .	3-15
Managing remote identities on Sidewinder G ₂	3-17
Determining identifying information for remote identities (certificates only)	3-17
Entering identifying information for remote identities (all) . . .	3-18
Configuring the VPN on Sidewinder G ₂	3-19

Chapter 4: Setting Up SoftRemote. 4-1

Managing SoftRemote deployment	4-2
SoftRemote installation and deployment notes	4-5
Installing SoftRemote	4-8
Starting SoftRemote	4-9
Determining VPN client status from icon variations	4-10
Determining ZoneAlarm status from icon variations	4-11
Disconnect/Connect SoftRemote VPN Client	4-12
Activating/Deactivating SoftRemote VPN client	4-13
SmartRemote Start menu options	4-14
Activating/Deactivating ZoneAlarm	4-14
Learning about the SoftRemote programs	4-15
About the Certificate Manager	4-16
Setting up a trust policy	4-16
Setting up Sidewinder G ₂ self-signed certificates	4-18
Setting up CA-based certificates	4-19
Managing certificates in SoftRemote	4-20
Importing CA root or firewall certificates in SoftRemote	4-20
Requesting and retrieving personal certificates in SoftRemote	4-22
Configuring a security policy in SoftRemote	4-25
Determining connection options	4-25
Setting up a Specified Connection policy	4-26
Setting up a Secure All Connections policy	4-34
Policy update distribution	4-35
VPN management command	4-36

Appendix A: Tips and Troubleshooting. A-1

SoftRemote Log Viewer	A-2
SoftRemote Connection Monitor	A-3
More about the Connection Monitor	A-4
To view the details	A-4
Common deployment issues	A-5
Upgrade tips	A-5
Connectivity troubleshooting	A-6

All Connections policy and Virtual Adapter settingA-7
Sidewinder G₂ troubleshooting commandsA-8
Working with Microsoft NetworkingA-8
ZoneAlarm troubleshooting resourcesA-11

P R E F A C E

About this Guide

This guide provides the information needed to set up connections between remote systems running SafeNet SoftRemote™ virtual private network (VPN) client software and systems on a network protected by Secure Computing's Sidewinder® G₂ firewall and VPN gateway. SafeNet SoftRemote is a Windows-compatible program that secures data communications sent from a desktop or laptop computer across either a public network or an existing corporate dial-up line. The software also includes the ZoneAlarm™ personal firewall for regulating external traffic coming in and out of the client system.

Note: *The SafeNet SoftRemote product is referred to as simply "SoftRemote" throughout the remainder of this document. When a feature or procedure relates only to the personal firewall, it is referred to as "ZoneAlarm."*



Important: *This guide describes administration of VPNs between SoftRemote Version 10.0 and Sidewinder G₂ Firewall Version 6.0. If you are working with a later version of either product, check our Web page at www.sidewinder.com for the latest documentation (select **Downloads & Activations** -> **Patches and Upgrades**).*

Who should read this guide?

This guide is written for the person assigned to manage Sidewinder G₂-based VPN connections with the SoftRemote VPN client. Administrating VPN connections requires that you perform procedures on both Sidewinder G₂ and SoftRemote to configure the gateway and pre-configure the VPN client security policy for each remote user (road warrior, telecommuter, etc.).

As a network administrator, you should read and understand all the procedures in this document. You will then be able to provide all remote users with the information, files, and software they need to set up SoftRemote software to communicate with your trusted network(s).

This guide assumes you are familiar with networks and network terminology. Because SoftRemote will require a security association with a Sidewinder G₂ firewall, you should be familiar with Sidewinder G₂ administration. Knowledge of the Internet and of Windows operating systems are also key requirements.

How this guide is organized

This guide contains the following chapters.

Chapter Title	Description
Chapter 1: Getting Started	Presents an overview of the SoftRemote and the Sidewinder G ₂ Firewall Virtual Private Network (VPN) environment, and describes the requirements. It includes a checklist to guide you through the basic steps to set up and deploy a VPN.
Chapter 2: Planning Your VPN Configuration	Provides information to help you understand key concepts and options that are related to a VPN connection.
Chapter 3: Configuring Sidewinder G2 for SoftRemote Clients	Provides a summary of Sidewinder G ₂ procedures associated with setting up and configuring SoftRemote connections in your network. Note: <i>Perform these procedures before you configure your SoftRemote clients.</i>
Chapter 4: Setting Up SoftRemote	Includes SoftRemote installation notes and describes the basic SoftRemote procedures for managing certificates and creating a customized SoftRemote security policy for your remote clients. This chapter summarizes the steps for preparing and deploying the SoftRemote software, digital certificate files, and security policy to your end users. It also includes basic information on the ZoneAlarm personal firewall. Note: <i>See the ZoneAlarm help files or Web site (www.zonealarm.com) for more detailed information.</i>
Appendix: Tips and Troubleshooting	Provides a summary of troubleshooting techniques available for resolving SoftRemote and Sidewinder G ₂ VPN connection problems.

Finding information

This guide is in electronic (softcopy) Adobe Acrobat portable documentation format (PDF) only and does not contain an index. However, you can use the Adobe Acrobat **Find** feature to search for every instance of any word or phrase that you want.

Viewing and printing this document online

When you view this document online in PDF format, you may find that the screen images are blurry. If you need to see the image more clearly, you can either enlarge it (which may not eliminate the blurriness) or you can print it. (The images are very clear when printed out.)

For the best results, print this PDF document using a PostScript printer driver.

- ◆ If your printer understands PostScript but does not have a PostScript driver installed, you need to install a PostScript driver. You can download one for your printer from www.adobe.com.
- ◆ If your printer is not a PostScript printer and this document does not print as expected, try one of the following:
 - If your printer has the option, **Print as Image**, enable this option and then try printing.
 - Print specific page(s) at a time rather than sending the entire document to the printer.

Where to find additional information

Refer to the following for related information.

- ◆ **About SoftRemote**

For additional information about configuring and troubleshooting SoftRemote software, refer to the online help that is integrated into the program's user interface. SoftRemote online help provides detailed step-by-step procedures for individual VPN client tasks.

- ◆ **About Sidewinder G₂**

For additional information about setting up VPN connections on a Sidewinder G₂ firewall, refer to Chapter 12 in the *Sidewinder G₂ Firewall Administration Guide*. In addition, be sure to review documentation associated with patch releases.

- ◆ **About ZoneAlarm**

For additional information about configuring and troubleshooting ZoneAlarm software, refer to the online help that is integrated into the program's user interface. ZoneAlarm online help provides detailed instructions for using basic and advanced features and troubleshooting for the personal firewall.

- ◆ **About digital certificates**

For information on digital certificates and Public Key Infrastructure (PKI) technology, see:

- *Understanding Public-Key Infrastructure*, by Carlisle Adams and Steve Lloyd (1999)

— *Internet X.509 Public Key Infrastructure, Certificate and CRL Profile*, RFC 2459, R. Housley, W. Ford, W. Polk, D. Solo (January 1999)

To contact Secure Computing directly or inquire about obtaining a support contract, refer to our Web site at **www.securecomputing.com**, and select "Contact Us." Or if you prefer, send us e-mail at **support@securecomputing.com** (be sure to include your customer ID and serial number in the e-mail).

CHAPTER 1

Getting Started

About this chapter

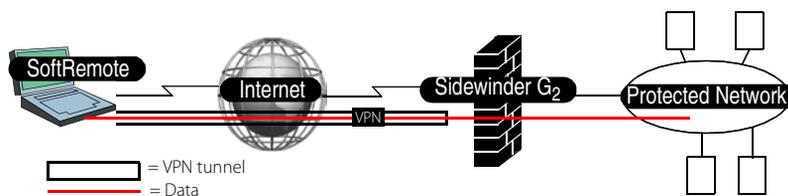
This chapter provides an overview of the SoftRemote™ and Sidewinder G₂ Firewall Virtual Private Network (VPN) environment and describes the requirements to set up secure connections in that environment. It includes a checklist to guide you through the basic steps to set up and deploy a VPN.

This chapter addresses the following topics:

- ◆ “About SoftRemote & Sidewinder G2 VPNs” on page 1-2
- ◆ “VPN requirements” on page 1-3
- ◆ “Roadmap for deploying your VPNs” on page 1-5

About SoftRemote & Sidewinder G₂ VPNs

Figure 1-1.
Sidewinder G₂ VPN
connection providing
secure data transmission
between a remote
system running
SoftRemote and your
internal network(s)



Note: In a VPN connection, keep in mind that the definition of "remote" depends on perspective. From the firewall's point of view, the remote end is a system connecting from the Internet. From the SoftRemote system's point of view, the remote end is the firewall (VPN gateway) and the protected network.

Using SoftRemote, a mobile employee or telecommuter can establish authenticated and encrypted access with networks protected by Secure Computing's fully IKE (Internet Key Exchange) compliant firewall. Remote users can access secure corporate resources using either public networks or corporate dial-up lines.

SoftRemote works in conjunction with ZoneAlarm to secure network communications. ZoneAlarm's purpose is to help regulate Internet traffic entering and exiting the remote user's system; however, it is not required for the VPN communication and therefore installing it is optional. Through SoftRemote, you may choose to make ZoneAlarm required or optional for your users. (See Chapter 4 for details.) Traffic can be split into two zones: local and Internet. This division allows users to exercise control over their traffic flow with trusted and untrusted sources. ZoneAlarm is configured at the application level, allowing certain programs access to the Internet while denying others.



Important: Consult the ZoneAlarm tutorial and online help files for a detailed description of the product's features, capabilities, and configuration options.

VPN requirements

To establish VPN communication between your firewall and SoftRemote clients, you must:

- ◆ Meet the system and network requirements found in Table 1-1 and Table 1-2.
- ◆ Design a matching security policy for the firewall gateway and the SoftRemote client.
- ◆ Configure your firewall with the proper VPN parameter settings and access rules.
- ◆ Configure the desired authentication methods— e.g. passwords and XAUTH, self-signed digital certificates, CA digital certificates, etc.

Before starting your VPN set up, ensure that your environment meets the requirements listed in this section.

Sidewinder G₂ firewall requirements

Your Sidewinder G₂ system and network must meet the basic requirements listed in Table 1-1.

Table 1-1. Requirements for running Sidewinder G₂'s VPN feature

Category	Requirement
Sidewinder G₂ firewall	<p>At least one installed and operational Sidewinder G₂ firewall with a VPN feature license.</p> <ul style="list-style-type: none"> ◆ Sidewinder Version 5.1 for basic functionality, or ◆ Sidewinder Version 5.2.1 or Sidewinder G₂ Firewall Version 6.0 for full features as documented in this guide <p>Note: You can protect more than one LAN with a single firewall.</p>
Network connection	A network infrastructure with a connection from Sidewinder G ₂ firewall to the Internet.

SoftRemote requirements

Each system on which SoftRemote will be installed must meet the requirements listed in Table 1-2.



Important: A remote system must only run one VPN client. If a VPN client program such as Soft-PK or SecureClient was previously installed on the remote system, ensure it is properly uninstalled before installing SoftRemote. See Chapter 4, “Setting Up SoftRemote”, for details.

Table 1-2. Requirements for running SoftRemote

Category	Requirement
Hardware	<ul style="list-style-type: none"> ◆ An IBM PC or compatible computer (portable or desktop) with at least a 75 MHz Pentium microprocessor (or equivalent). ◆ A non-encrypting modem (for use with Dial-Up Networking) or at least 1 NIC (e.g. Ethernet, ISDN). See http://www.ire.com/clientsupport/SafeNetClientNIClist.htm for compatible NICs. ◆ At least 10 MB of free hard disk space. ◆ The recommended system RAM size: <ul style="list-style-type: none"> — Windows 95: 16 MB — Windows 98, NT: 32 MB — Windows Me, 2000 Professional: 64 MB — Windows XP Home and Professional: 128 MB
Software	<ul style="list-style-type: none"> ◆ Microsoft Windows 95, 98, NT 4.0, Me, 2000 Professional, XP Home and Professional. ◆ Dial-Up Networking component of Microsoft Windows or LAN interface. ◆ If the remote system uses a modem, the end user must have a dial-up account with an Internet Service provider (ISP) or a private corporate dial-up account. <p>  Tip: Instruct SoftRemote users to follow the instructions provided by Microsoft to install Dial-Up Networking on their Windows PC. Also, create a Dial-Up Networking profile for the ISP used to gain access to the Internet. </p> <ul style="list-style-type: none"> ◆ To use help, Microsoft Internet Explorer 4.0 or later ◆ To use Microsoft Cryptographic Services (MS CSP), Microsoft Internet Explorer 5.0.1 or later ◆ To use certificates with keys larger than 1024, Microsoft Internet Explorer 5.5
Internet connection	Connection to the Internet (via a dial-up line, DSL, cable modem, ISDN, etc.)

Roadmap for deploying your VPNs

Because VPN connections are an integral component of your network security, we recommend that, as the network administrator, you carefully oversee the installation and configuration of the SoftRemote client(s). Setting up VPN connections using SoftRemote and Sidewinder G₂ requires that you perform procedures that will configure both the remote systems running SoftRemote AND your firewall.

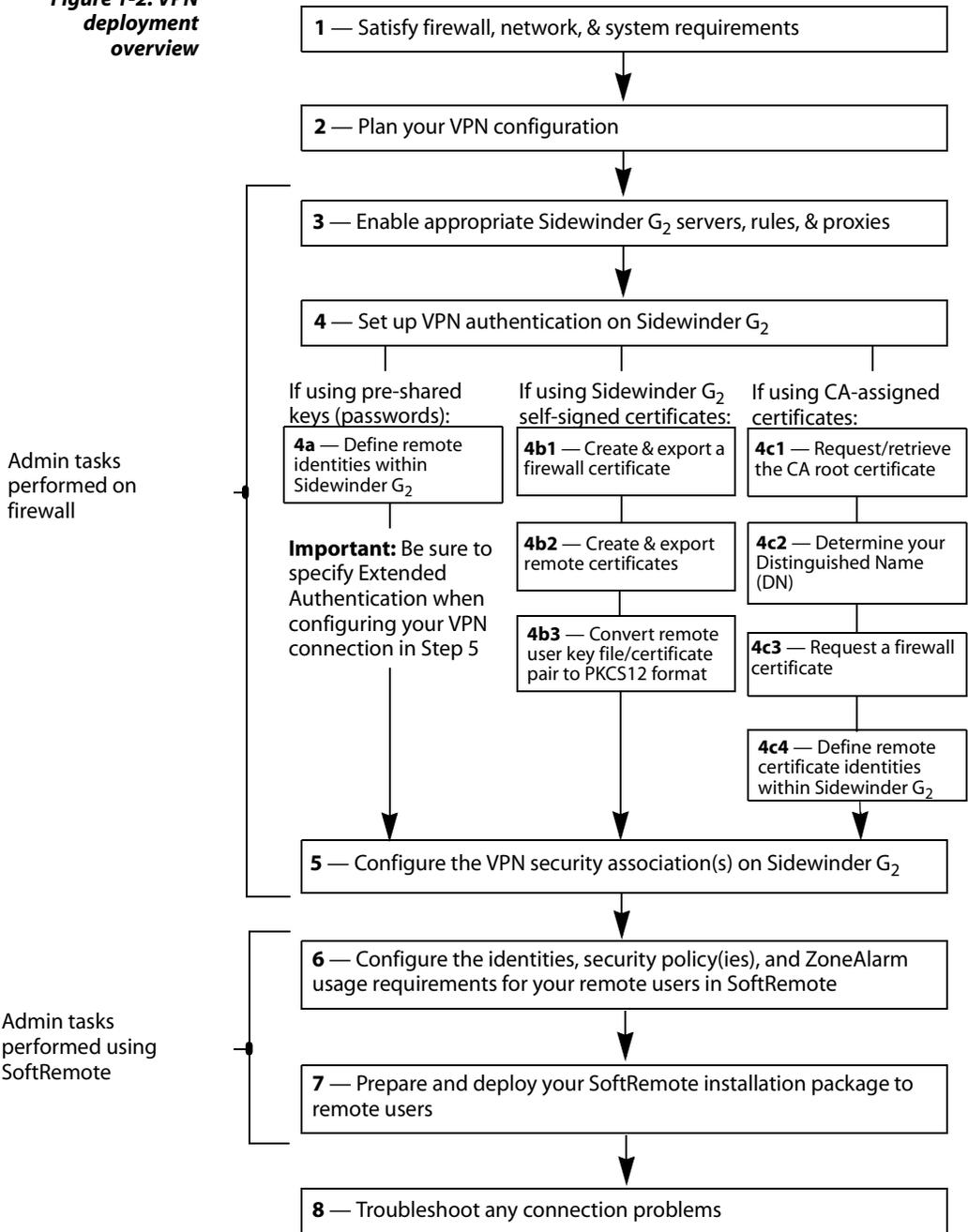
If done properly, administrators can do most of the VPN configuration for both SoftRemote and Sidewinder G₂ with little time dedicated to each end user machine and little effort required of the end users. Security policy and certificate files with specified names may be saved to an install image where they will be automatically imported as SoftRemote installs. Determine if your users will be required to install the VPN client with the personal firewall (SoftRemote-full), install the VPN client without the personal firewall (SoftRemoteLT), or if they will be able to choose. Then save the files you want auto-imported with the matching directory (full and/or SoftRemoteLT) on the deployment image. For example, you can set up a pre-shared password and create a security profile that you include with SoftRemote's installation files. If users can select whether or not they want the personal firewall, place the configuration file copies in both the full and VPN client only directories. The pre-shared password and policy will auto-import with the SoftRemote client. Users then simply need to configure the My Identity section using instructions you provide. See Chapter 4 for greater detail.



Tip: A separate *Secure Computing SoftRemote User's Guide* is **not** provided for end users of SoftRemote. Use Table 4-2, "SoftRemote install, deployment, and uninstall task summary," as a guideline for preparing instructions for your end users.

Figure 1-2 provides a graphical overview of the SoftRemote and Sidewinder G₂ VPN deployment process. Each of the tasks depicted in Figure 1-2 are also reflected in the checklist starting on page 1-7.

Figure 1-2. VPN deployment overview



SoftRemote deployment checklist

The following checklist identifies each major step involved in the set up and deployment of your SoftRemote software (as shown in Figure 1-2). You can use the checklist as a reference point and mark off each item as you complete it to ensure a successful VPN rollout.



Tip: Each step provides an overview of the task and points you to specific documentation for more detailed information.

1 — Satisfy firewall, network, & system requirements

- Firewall/network:** Verify that your firewall is at Version 5.1 or later, licensed for VPN, and that your network is fully operational.
- End-user systems:** Verify that each system on which SoftRemote will be installed meets the requirements as described on page 1-4.

2 — Plan your VPN configuration

- Review Chapter 2 in this guide to become familiar with key concepts and options that are available when setting up VPNs.
- Review Chapter 12 in the *Sidewinder G₂ Firewall Administration Guide* for additional background on VPN configuration.
- Review the *readme.txt* file located on the SoftRemote CD for additional information from Secure Computing.
- Determine the most effective authentication requirements for your situation.

3 — Enable appropriate Sidewinder G₂ servers, rules, & proxies

Note: For details, see “Enabling the VPN servers” on page 3-4 and “Configuring rules & proxy entries for interburb passage of VPN connection traffic” on page 3-6.

- CMD server:** The Certificate Management Daemon (CMD) server must be enabled before you can configure the certificate server.
- ISAKMP server:** The ISAKMP server must be enabled and set to listen on the appropriate burb (typically, this will be the **Internet** or **external burb**).
- ISAKMP rule:** At a minimum, you must define and enable a rule that allows ISAKMP traffic from the **Internet burb** (*desired source addresses*) to the **Internet burb** (*external IP address of the firewall*).

More...

- Other rules:** Depending on where you terminate your VPN connections on the firewall (e.g., in a virtual burb), you may need to create rules to allow traffic between burbs.
- Proxies:** Depending on where you terminate your VPN connections on Sidewinder G₂ (e.g., in a virtual burb), you may need to enable proxies to allow traffic between burbs.

4 — Create/request pre-shared keys or digital certificates on Sidewinder G₂

If using pre-shared keys (passwords):

- Use the **Admin Console** (known as **Cobra** in previous releases) to specify the client identity information within Sidewinder G₂. See “Managing pre-shared keys (shared-passwords)” on page 3-7 for details.

If using Sidewinder G₂ self-signed certificates:

- Use the **Admin Console** to create and export a firewall certificate. See “Creating & exporting a firewall self-signed certificate” on page 3-8 for details.
- Use the **Admin Console** to create and export remote certificates for each end user. See “Creating & exporting remote certificate(s)” on page 3-10 for details.
- Use a **command-line** utility on Sidewinder G₂ to convert the key/file certificate pair to PKCS12 format. See “Converting the certificate file/private key file pair to PKCS12 format” on page 3-12 for details.

If using a CA -assigned certificates:

- Use the **Admin Console** to define a CA and obtain the CA root certificate. See “Requesting and retrieving a CA-issued root certificate” on page 3-14 for details.
- Use the **Admin Console** to request a certificate for the firewall from the CA. See “Requesting and retrieving a CA-issued firewall certificate” on page 3-15 for details.
- Determine the identifying information (e.g., Distinguished Name settings) your clients will use in their personal certificates. See “Determining identifying information for remote identities (certificates only)” on page 3-17.

More...

For all authentication methods:

- Use the **Admin Console** to specify the client certificate identity information within Sidewinder G₂. See “Managing remote identities on Sidewinder G₂” on page 3-17 for details.

5 — Configure the VPN security association(s) on Sidewinder G₂

- Use the **Admin Console** to define the VPN security association configuration. See “Configuring the VPN on Sidewinder G₂” on page 3-19 for details.
- If necessary, enable Extended Authentication.

Note: Use of Extended Authentication is critical when using pre-shared key authentication.

6 — Configure the certificates/pre-shared keys and security policy(ies) for your remote users on SoftRemote

- Install your copy of **SoftRemote**. See “SoftRemote installation and deployment notes” on page 4-5 for details.
- If using Certificate Authority (CA) based or self-signed certificates, use **SoftRemote** to import and/or set up the certificates needed by each end user. See “About the Certificate Manager” on page 4-16 for details.
- If using a pre-shared key, set it up during this step. Use **SoftRemote** to create and save security policies that are customized for your end users. See “Configuring a security policy in SoftRemote” on page 4-25 for details.

7 — Prepare and deploy your SoftRemote installation package to remote users

- Determine the deployment method you will use based on your VPN configuration. For details, see “Managing SoftRemote deployment” on page 4-2.
- Prepare the files you will distribute to your end users. For details, see “Deployment Scenarios” on page 4-3.

More...

- ❑ Create SoftRemote installation and configuration instructions for your end users. For details, see “SoftRemote installation and deployment notes” on page 4-5.
 - ◆ If necessary, define configuration steps for the Windows Dial-Up Networking feature on each machine on which you are installing and using SoftRemote.
 - ◆ Specify the SoftRemote installation instructions.
 - ◆ Specify the instructions for importing, requesting, and/or setting up client certificates.
 - ◆ Specify the instructions for importing, updating, and /or activating a security policy.
 - ◆ Specify how and when to activate or deactivate the SoftRemote security policy.
 - ◆ Specify the guidelines for using ZoneAlarm.
- ❑ Distribute the SoftRemote deployment software and files to your end users.

8 — Troubleshoot any connection problems

- ❑ Use the **SoftRemote Log Viewer**. See “SoftRemote Log Viewer” on page App-2.
- ❑ Use the **SoftRemote Connection Monitor**. See “SoftRemote Connection Monitor” on page App-3.
- ❑ Use **Sidewinder G₂ firewall tools**. See “Sidewinder G₂ troubleshooting commands” on page App-8 and the *Sidewinder G₂ Firewall Administration Guide* for details.

CHAPTER 2

Planning Your VPN Configuration

About this chapter

This chapter provides information to help you understand key concepts and options that are related to a VPN connection. It addresses the following topics:

- ◆ “Identifying basic VPN connection needs” on page 2-2
- ◆ “Identifying authentication requirements and configurations” on page 2-3
- ◆ “Determining where you will terminate your VPNs” on page 2-8
- ◆ “Understanding Sidewinder G2 client address pools” on page 2-10

Identifying basic VPN connection needs

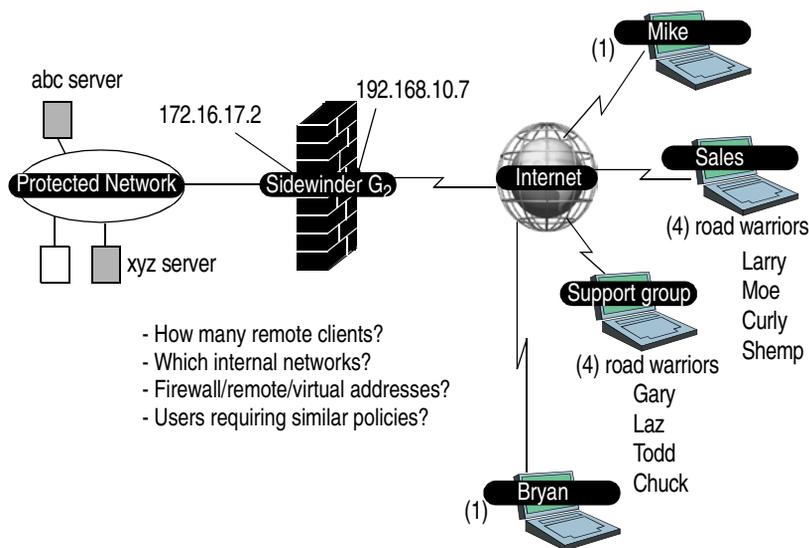
Before you actually begin to configure your Sidewinder G₂ or work with SoftRemote, ensure you have an understanding of the basic profile for your VPN connections.

Begin by doing the following:

- ◆ List the remote users that need a VPN connection
- ◆ List the internal/trusted systems to which users need access
- ◆ Identify groups of remote users who will have the same security policy
- ◆ Identify the important IP addresses

It may help to start a sketch that defines your basic requirements. Depending on your organization and network, this could be somewhat more complex than the diagram shown in Figure 2-1.

Figure 2-1.
Identify remote users and the target internal systems in a sample diagram



Identifying authentication requirements and configurations

Determine how you will identify and authenticate the parties in your VPN. Sidewinder G₂ and SoftRemote both support pre-shared key and digital certificate VPN configurations. In addition, when you use Sidewinder version 5.1.0.02 or later, you can set up Extended Authentication to provide increased security to your VPN network. Use the following table to help familiarize yourself with the basic characteristics of each authentication method.

Table 2-1. VPN configuration comparisons

Authentication Scenario	Attributes
Using pre-shared key and extended authentication (for a medium to large number of VPN clients)	<ul style="list-style-type: none"> ◆ Uses a client-configured password and strong authentication ◆ Single VPN association for all clients with same security policy ◆ Can make VPN deployment and management more efficient
Using self-signed certificates (for a small number of VPN clients)	<ul style="list-style-type: none"> ◆ No CA needed ◆ Requires a unique VPN association for each client ◆ Only for deployment to small number of users
Using CA-based certificates (for a medium to large number of VPN clients)	<ul style="list-style-type: none"> ◆ Uses a private or public CA ◆ Single VPN association for all clients with same security policy ◆ Can make VPN deployment and management more efficient

Understanding pre-shared key authentication

A pre-shared key (referred to as shared password by Sidewinder G₂) is an alphanumeric string—from eight to 80 characters—that can replace a digital certificate as the means of identifying a communicating party during a Phase 1 IKE negotiation. This key/password is called "pre-shared" because you must share it with another party before you can communicate with them over a secure VPN connection. The key/password is then configured into respective IPSec-compliant devices (e.g., firewall and software client). Using a pre-shared key/password for authentication is the easiest type of VPN association to configure.



Important: You should only use this method along with Extended Authentication.

Understanding Extended Authentication

In addition to the normal authentication checks inherent during the negotiation process at the start of every VPN association, Extended Authentication (XAUTH) goes one step further by requiring additional identity verification of the *person* requesting the VPN connection.

Depending on the extended authentication method you select, the person must provide a unique user name and password, a special passcode, or one-time password before the VPN association is established. For example, assume you configure a VPN association to use extended authentication and that you select the standard password process as the form of authentication. When a person attempts to establish a VPN connection, the firewall performs the standard VPN negotiations. In addition, the firewall issues a request for the proper user name and password. The person initiating the VPN connection request must then enter the proper user name and password at their workstation. The firewall must then verify the user's identity before the connection will be made.

The XAUTH option is most useful if you have travelling employees that connect remotely to your network using laptop computers. If a laptop computer is stolen, without extended authentication it might be possible for the thief to illegally access your network. This is because the information needed to establish the VPN connection (the shared password, certificate, etc.) is saved within the VPN client software. When the XAUTH option is used, however, the user is required to enter an additional piece of authentication information that is not saved on the computer—either a password, passcode, or PIN. This additional level of authentication renders the VPN capabilities of the laptop useless when in the hands of a thief.

Using digital certificate authentication

When using digital certificates (or "public key authentication"), each system in the VPN requires a unique **private key file** and a corresponding public key **certificate file**.

- ◆ **The private key file**

A private key file is unique to each system in the network and kept secret by the holder (VPN client, firewall, etc.). It is used to create digital signatures and, depending upon the algorithm, to decrypt data encrypted with the corresponding public key.

- ◆ **The certificate file (with public key)**

Certificates contain informational values such as the identity of the public key's owner, a copy of the public key itself (so others can encrypt messages or verify digital signatures), an expiration date, and the digital signature of the creating entity (CA or firewall).

When using Sidewinder G₂, the trusted source for authorizing key/certificate pairs can be the firewall itself through "self-signed" certificates, or a public or private Certificate Authority (CA) server (for example; Netscape, Baltimore, Entrust, etc.). Digital certificate implementations using Sidewinder G₂/SoftRemote follow the X.509 standard.



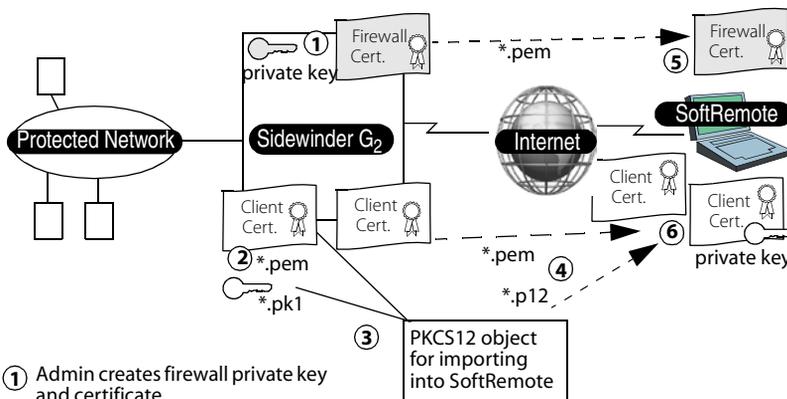
Important: You must configure the necessary certificates before you configure the VPN connection parameters on Sidewinder G₂ or SoftRemote.

Digital certificates have a validity period defined by an "effective" date and an "expiration date." Secure connections will not be established with an expired certificate. Be sure to have the issuing authority renew the certificate(s) prior to the expiration date and update the VPN equipment with these renewed certificates.

A closer look at self-signed certificates

A VPN implemented using Sidewinder G₂ self-signed certificates does not require an external certificate authority and is relatively easy to configure for a small number of clients. However, one security association must be configured on the firewall for each client. As the number of configured clients grows, so does the administrative effort. Figure 2-2 shows the certificates involved in a VPN using Sidewinder G₂ self-signed certificates.

Figure 2-2. Sidewinder G₂ self-signed certificate summary



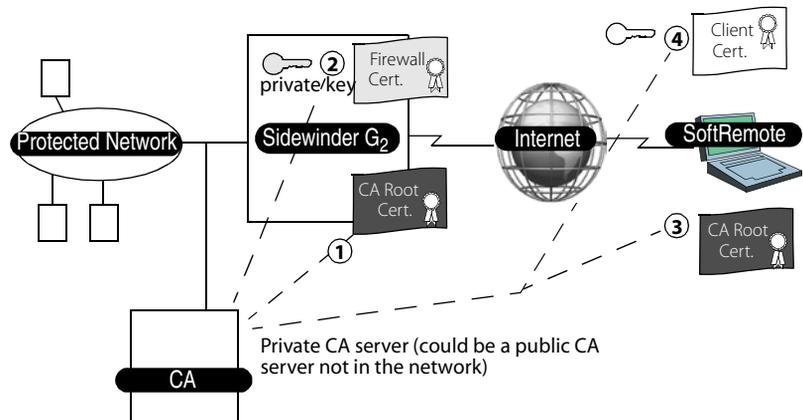
- ① Admin creates firewall private key and certificate
- ② Admin creates client private key/certificate pair(s)
- ③ Admin converts client private key & certificate files to PKCS12 object
- ④ Admin exports the certificate files and the PKCS12 object to transfer to the client
- ⑤ Firewall certificate imported to SoftRemote (private key remains on the firewall)
- ⑥ Client private key /certificate file (.p12) and client certificate (.pem) imported into SoftRemote. The .p12 file is imported as a user certificate. The .pem is imported as a trusted CA certificate.

Note: A self-signed certificate created on the firewall remains valid for five years (default setting) beginning from the date it is created.

A closer look at CA-based certificates

A VPN implemented using CA-based certificates requires access to a private or public CA. Each end point (client, firewall, etc.) in the VPN needs a local copy of the CA root certificate to verify signed certificates. In addition, each end-point retains its own private key file and public certificate. Figure 2-3 shows the certificates involved in a VPN using CA-based certificates.

Figure 2-3. CA-based digital certificate summary



- ① Admin requests CA root certificate
- ② Admin requests firewall certificate
- ③ Admin provides CA root certificate to client (or instructions to obtain it)
- ④ Admin provides client key/certificate to client (or instructions to obtain it)

Determining where you will terminate your VPNs

When you determine where you will terminate your VPN, you mark where traffic switches between clear text and encryption. Traffic is always encrypted between the two endpoints and then travels in clear text to its final destination. One endpoint is the VPN client on the remote machine. You can configure the other endpoint to terminate in any burb on the firewall. Terminating the VPN security association in any burb *except* the Internet burb ensures that traffic is inside a protected network when it is decrypted into clear text. For example, Figure 2-4 shows a VPN security association terminating in a trusted burb. In this case, you need no special rules or proxy controls other than an external-to-external ISAKMP rule.

 **Figure 2-4. VPN tunnel terminating on a trusted burb**

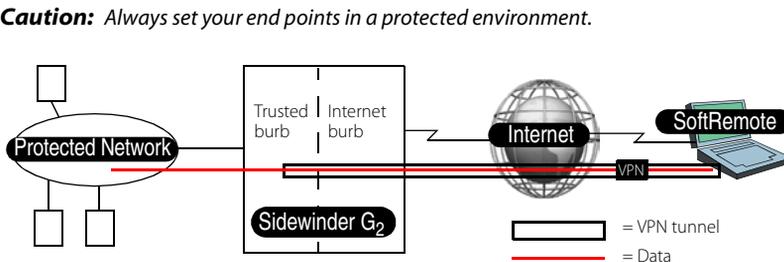
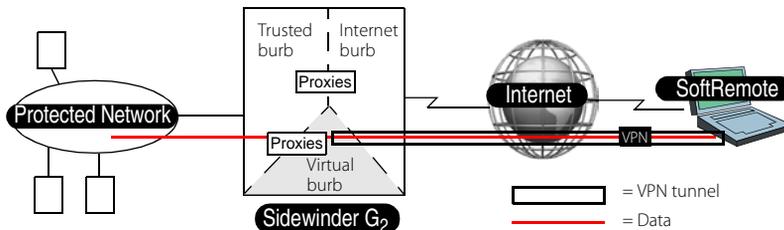


Figure 2-5 shows another option that allows you to terminate VPN traffic in a "virtual" burb. A virtual burb is a burb that does not contain a network interface card. The purpose of a virtual burb is two-fold: to serve as a protected logical endpoint for a VPN association and to facilitate policy control of the traffic after it is decrypted.

Figure 2-5. VPN tunnel terminating on a virtual burb



Terminating a VPN association in a virtual burb accomplishes two important goals:

- ◆ Separation of VPN traffic from non-VPN traffic.
- ◆ Enforcement of a security policy that applies strictly to your VPN users.

By terminating the VPN in a virtual burb you effectively isolate the VPN traffic from non-VPN traffic. Plus, you are able to configure a unique set of rules (via proxies and rules) for the virtual burb that allow you to control precisely what your VPN users can or cannot do.

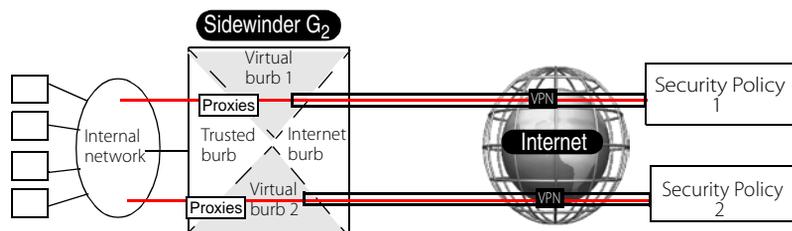
Note: The VPN implementation depicted in Figure 2-5 represents a "proxied" VPN because proxies must be used to move VPN data between burbs. The use of proxies enables you to control the resources that a VPN client has access to on your internal network.

Consider a VPN association that is implemented without the use of a virtual burb. Not only will VPN traffic mix with non-VPN traffic, but there is no way to enforce a different set of rules for the VPN traffic. This is because proxies and rules, the agents used to enforce the rules on a firewall, are applied on a burb basis and not to specific traffic within a burb.

Note: Do not terminate VPN connections in the Internet burb.

You can define up to nine physical and virtual burbs. For example, if you have two distinct types of VPN associations and you want to apply a different set of rules (security policy) to each type, simply create two virtual burbs, then configure the required proxies and rules for each virtual burb.

Figure 2-6. Virtual burb configuration for multiple security policies



One question that might come to mind when using a virtual burb is: "How does VPN traffic get to the virtual burb if it doesn't have a network card?" All VPN traffic originating from the Internet initially arrives via the network interface card in the Internet burb. A VPN security association, however, can internally route and logically terminate VPN traffic in any burb on the firewall. By defining a security association to terminate the VPN in a virtual burb, the VPN traffic is automatically routed to that virtual burb within the firewall. Thus, the trusted network now recognizes the virtual burb as the source burb for your VPN traffic. From the virtual burb, a proxy is needed to move the traffic to a trusted burb with network access.

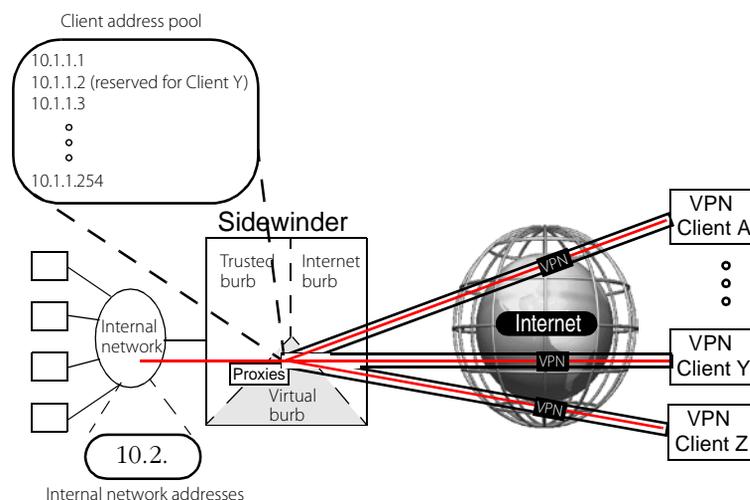


Important: Failure to enable or properly configure the necessary proxies and rules will result in connectivity and other problems. See “Configuring rules & proxy entries for interburb passage of VPN connection traffic” on page 3-6 for details.

Understanding Sidewinder G₂ client address pools

You may choose to implement your VPN using Sidewinder G₂ client address pools. Client address pools are reserved virtual IP addresses recognized as internal addresses of the trusted network. Addresses in this pool are configured on the firewall and assigned (or "pushed") to a VPN client (per VPN configuration) when the VPN connection is started. Client traffic within the protected network appears to come from the virtual IP address pool. On the protected network, only the firewall knows the client's real IP address.

Figure 2-7. VPN association implemented using a client address pool



Virtual IP address mappings using this client address pool.

VPN Client	Virtual IP Address
A	Next available within the pool
•	•
•	•
Y	10.1.1.2
Z	Next available within the pool

One of the reasons for using client address pools is that they simplify the management of VPN clients. They allow the firewall to manage certain configuration details on behalf of the client. This enables a

remote client to initiate a VPN connection without being preconfigured for all aspects of the connection.

Sidewinder G₂ uses the client address pool interface to manage a number of configuration parameters that are pushed to the remote client. The virtual IP address is one such parameter. Other important parameters are the IP addresses of the internal DNS and WINS servers that the client will need to function within the protected network. When leveraging these features of the client address pool interface, the client does not need to define a virtual IP for use in the VPN connection, nor does it need to concern itself with WINS and DNS issues on the trusted network. The DNS and WINS server IP addresses are pushed to the client with the virtual IP address.



Important: *The client machine's IP address should **not** match the internal network's subnet, as this configuration could cause internal routing and connectivity issues.*

In addition to simplifying the configuration process for your clients, client address pools give you the ability to place additional controls on VPN clients. From the firewall, you can do the following:

- ◆ Allow or restrict access on a client address pool basis.

For example, assume you create two client address pools. Client associations initiated from pool A might be granted access to certain networks that are off limits to clients from pool B.

- ◆ Allow or restrict access on a client basis.

This is done by assigning a specific IP address within a client address pool to a specific user by using the Fixed IP Map tab. The fixed addresses you specify must be within the range of available IP addresses as defined by the client address pools. By creating a network object for that IP address, you can then use the network object in a rule to allow or restrict the client's access to additional services.



Important: *When using client address pools, **only** select the Dynamic Restricted IP Client option on the Security Associations tab, regardless of how the client obtains its IP address.*

Note: *For more detailed information on client address pools, see the Sidewinder G₂ Firewall Administration Guide.*

Configuring Sidewinder G₂ for SoftRemote Clients

About this chapter

This chapter provides a summary of Sidewinder G₂ procedures for setting up and configuring SoftRemote connections in your network.

Note: For Enterprise Manager users, each procedure is described at the firewall level using the Admin Console.



Important: Perform these procedures before you configure your SoftRemote clients.

This chapter addresses the following topics:

- ◆ “Defining a virtual burb” on page 3-2
- ◆ “Enabling the VPN servers” on page 3-4
- ◆ “Configuring rules & proxy entries for interburb passage of VPN connection traffic” on page 3-6
- ◆ “Managing pre-shared keys (shared-passwords)” on page 3-7
- ◆ “Managing Sidewinder G2 self-signed certificates” on page 3-8
- ◆ “Managing CA-based certificates” on page 3-14
- ◆ “Managing remote identities on Sidewinder G2” on page 3-17
- ◆ “Configuring the VPN on Sidewinder G2” on page 3-19

Defining a virtual burb

If you have not done so, read the sections on virtual burbs in the previous chapter to help determine if your VPN configuration should include virtual burbs.

To create a virtual burb on the firewall for terminating a VPN, do the following:

1. Select **Firewall Administration -> Burb Configuration**.
2. Click **New** and create the new virtual burb.
3. Click the **Save**  icon.

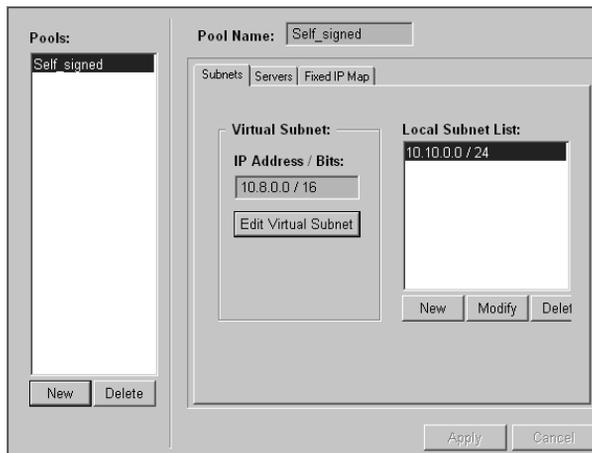
Defining a client address pool

If you have not done so, read the section on client address pools in the previous chapter to help determine if your VPN configuration should be set up using this virtual addressing tool.

To create a client address pool to apply virtual addresses to your incoming VPN connections, do the following from the Sidewinder G₂ Admin Console interface:

1. Select **VPN Configuration -> Client Address Pools**.

Figure 3-1. VPN Configuration -> Client Address Pools



2. Click **New**.
3. Enter a name in the **Enter New Pool Name** field.

4. In the Virtual Subnet Section, click **Edit Virtual Subnet**.
 - a. Enter the IP address to be used for virtual addressing.
 - b. Enter the number of bits in the netmask.
 - c. Click **OK**.



Caution: *Do not enter an existing subnet in your network in this window. Virtual addressing **only** works if the client address pool uses unassigned address space.*

5. In the Local Subnet List section, click **New**.
 - a. Enter the IP address of the subnet in your internal protected network that your SoftRemote users will access.
 - b. Enter the number of bits in the netmask.
 - c. Click **Add**, then click **Close**.
6. [Optional] If you would like to assign DNS or NBNS/WINS server information using the client address pool, click the **Servers** tab.
7. [Optional] In the DNS Servers section, click **New**.
 - a. Enter the IP address of the internal DNS server to which you want remote VPN users to connect.
 - b. Click **Add**.
8. [Optional] In the NBNS/WINS Servers section, click **New**.
 - a. Enter the IP address of the internal NBNS/WINS server to which you want remote VPN users to connect.
 - b. Click **Add**.
9. [Optional] If you would like specific remote users to always be assigned the same virtual address, click the **Fixed IP Map** tab.

Note: *For more information, click **Help** in the Admin Console.*

 - a. Click **New**.
 - b. Enter the IP address to be assigned to a specified client, then click **New**.
 - c. Enter the client identification string, then click **Add**. Repeat this process for each desired string.
 - d. Click **Close** on the smaller window, and then click **Close** on the larger window.
10. In the main section, click **Add**.

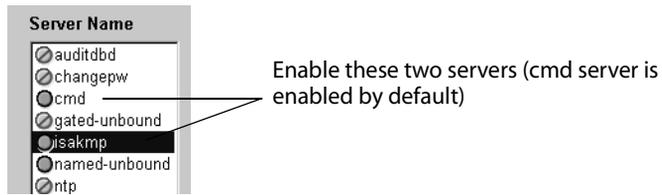
Enabling the VPN servers

Before you configure a VPN association on your firewall, you must first enable the firewall's CMD and ISAKMP servers. Next, set the firewall to listen for the ISAKMP server on the Internet burb.

Do the following from the Admin Console:

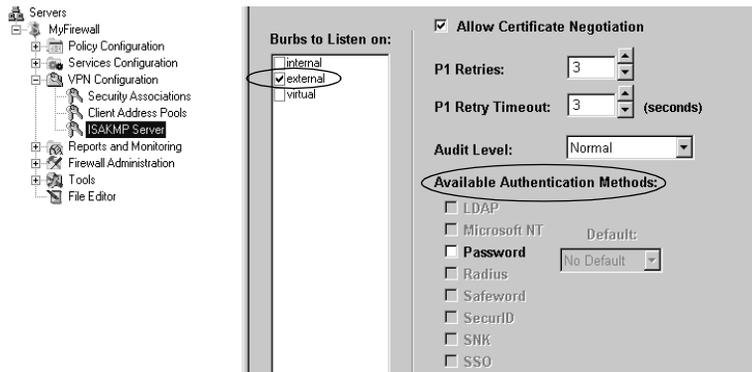
1. Enable the **cmd** and **isakmp** servers.
 - a. Select **Services Configuration -> Servers**.

Figure 3-2. Services Configuration -> Servers



- b. To enable a server, select it from the **Server Name** list and click **Enable**.
 - c. Click the **Save** icon.
2. Configure the ISAKMP server to listen on the appropriate burb.
 - a. Select **VPN Configuration -> ISAKMP Server**.

Figure 3-3. VPN Configuration -> ISAKMP Server

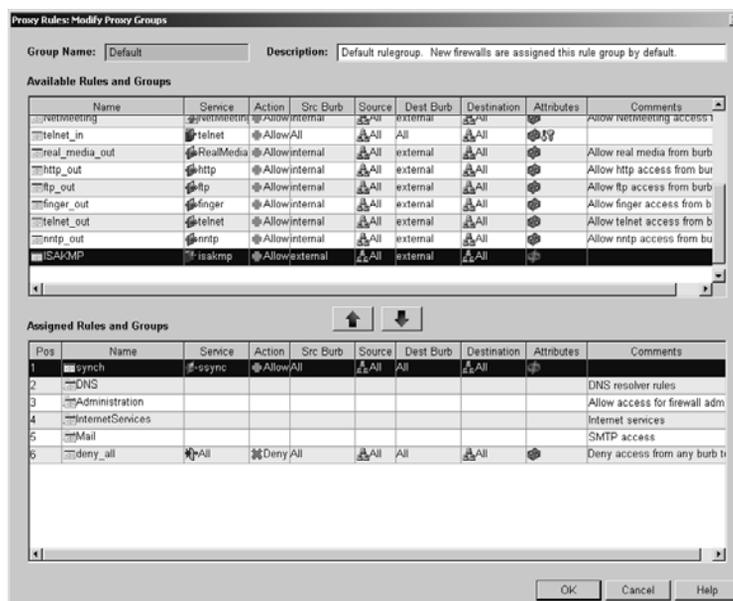


- b. In the **Bursts to Listen on** list column, click the burb name associated with the Internet burb.
 - c. In the **Available Authentication Method** fields, specify the method(s) to enable for Extended Authentication.
 - d. Click the **Save** icon.

Once the server is enabled and listening, you need a rule that allows external-to-external ISAKMP traffic. To create the new rule and then add it to your active rule group, do the following from the Sidewinder G₂ Admin Console:

1. Select **Policy Configuration -> Rules**. Leave the View Option on Proxy Rules.
2. Click **New** and then select **Proxy Rule**.
3. In the new window, enter the following information on the General tab:
 - ◆ Entry Name = (site dependent)
 - ◆ Agent = Server
 - ◆ Service = ISAKMP
 - ◆ Action = Allow
 - ◆ Audit Level = (site dependent)
 - ◆ Comments = (optional)
4. Click the **Source/Dest** tab and enter the following information:
 - ◆ Source burb = external (or site dependent name of external burb)
 - ◆ Source = (all source addresses, *)
 - ◆ Destination burb = external (or site dependent name of external burb)
 - ◆ Destination = (external IP of firewall)
5. Click **OK**.
6. Double click your active rule group.
The **Modify Proxy Groups** window opens.

**Figure 3-4. Proxy Rule:
Modify Proxy Groups**



7. Select the ISAMKP rule your newly created ISAKMP rule.
8. Click the down arrow and reposition rule above deny_all by dragging the rule up.



Important: Make sure your rule appears above any deny_all rules.

9. Click OK on the **Modify ProxyGroups** window, and then click the **Save** icon.

Configuring rules & proxy entries for interburb passage of VPN connection traffic

Depending on where you decide to terminate your VPN tunnel, you must ensure that you have the appropriate rules set up to allow/deny the appropriate proxy traffic. If using a virtual burb, you must ensure the desired proxies are enabled and the necessary proxy settings are configured in the active rule list. You may also need to add a static route to your internal router for traffic to reach the virtual subnet.

Note: Ensure you have defined appropriate network objects/groups. (See Chapter 5 in the Sidewinder G₂ Firewall Administration Guide for details.)

- ◆ Consult your company security policy to determine which users/user groups need access to which services and networks. Define (or ensure you have) rules that allow this type of access to and from any burbs you may have.

Note: For details about configuring and managing rules, see Chapter 6 in the

Sidewinder G₂ Firewall Administration Guide.

- ◆ If DNS is needed, assign DNS to listen for the virtual burb. At the command line, enter the following command:

```
cf dns add listen burb=burbname
```

where: *burbname* = the name you have assigned your virtual burb

Verify that DNS is listening on the virtual burb by typing the following command:

```
cf dns query
```

- ◆ Enable the desired proxies (HTTP, FTP, Telnet, SMTP, WINS, etc) in the appropriate burb(s). Select **Services Configuration -> Proxies**.

Note: For details about configuring and managing proxies, see Chapter 7 in the Sidewinder G₂ Firewall Administration Guide.

Managing pre-shared keys (shared-passwords)

The pre-shared key authentication option, when combined with strong extended authentication like SafeWord PremierAccess (one-time passwords), is a simple yet extremely secure configuration. You may create one generic client installation deployment for a group of like users. For example, you may create one security policy on SoftRemote, export it to an install image, and distribute that image to each member of your Sales team. Only one Security Association (SA) entry would be needed to govern the group's VPN connections.

When using pre-shared keys (passwords), you must define an identity "template" in the firewall that matches all possible client identities (or per group of entities) used by the remote entities in your VPN. To define remote identities on the firewall, you need to configure one tab from the Certificate Management section. See the procedure in "Managing remote identities on Sidewinder G₂" on page 3-17. Note that when working with pre-shared keys, the identity type should be a domain name or IP address and *not* a Distinguished Name. You only need to create and manage one password for all the remote entities for a given SA. The password and saved remote identity template are entered when setting up the related SA entry, as described in "Configuring the VPN on Sidewinder G₂" found on page 3-19.



Important: Be sure to specify Extended Authentication, as shown in Figure 3-10 "Password Options" on page 3-22.

Managing Sidewinder G₂ self-signed certificates

In a self-signed certificate configuration, Sidewinder G₂ creates and signs both the firewall certificate and the client certificate. Each certificate is signed with the private key associated with its own certificate identity. The firewall certificate then serves as the trust point for its own verification and the client (or remote) certificate serves as the trust point for its own verification. (Hence, "self-signed" authentication instead of authenticating against an external "certificate authority.") A copy of each certificate must reside on the firewall.

If you are using the firewall to generate certificates, use the following procedures to create and export self-signed certificates that identify the firewall and each remote client.



Tip: Typically, a VPN configuration using Sidewinder G₂ self-signed certificates is suitable if the number of clients is small.

Note: A Sidewinder G₂ self-signed certificate remains valid for five years beginning from the date it is created (default value).

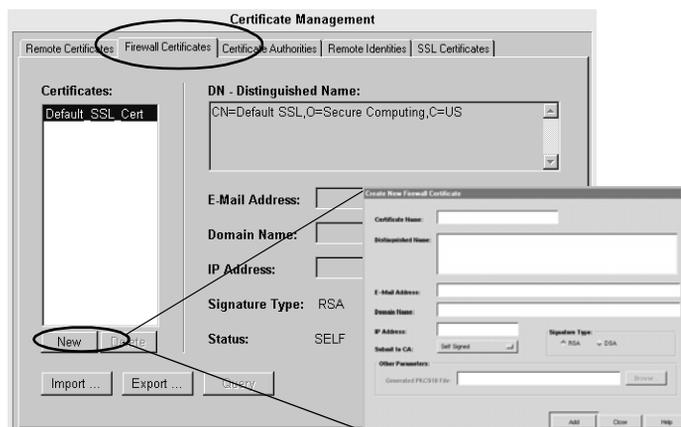
Creating & exporting a firewall self-signed certificate

Use the following procedure to create and export the firewall's self-signed certificate.

From the Sidewinder G₂ Admin Console:

1. Select **Services Configuration -> Certificate Management**.
2. Select the **Firewall Certificates** tab. Click **New**.

Figure 3-5.
Sidewinder Certificate Management: Create New Firewall Certificate window



- Specify the following Firewall Certificate settings.

Field	Setting
Certificate Name	Specify a name for the firewall certificate. Note: Use only alphanumeric characters plus the dash, dot, and underscore (-._). Do not begin the name with a dash (-).
Distinguished Name	Specify a set of data that identifies the firewall. Use the following format: cn=,ou=,o=,l=,st=,c= where: <ul style="list-style-type: none"> ◆ cn = common name ◆ ou = organizational unit ◆ o = organization ◆ l = locality ◆ st = state ◆ c = country <p> Important: The syntax for this field is very important. The order of the specified distinguished name fields must match the desired order to be listed in the certificate. The above entries should be separated by commas, and contain no spaces or special characters.</p>
E-Mail Address, Domain Name, IP Address	Optional fields used for identity information (in addition to DN).
Submit to CA	Select Self Signed .
Signature Type	Select RSA .

- Click **Add** to add the certificate to the Certificates list.
- Click **Close** to return to the Firewall Certificate window.
- Click **Export** and save the firewall certificate (containing the public key) to a file. Add a *.pem* extension (for example, "firewallcert.pem").
- Click **OK** when done.

Export the firewall certificate

If you are on the firewall local console, you may choose to copy the file to an MS-formatted diskette for deployment purposes. You can do this using the **mcopy** command. For example:

```
% mcopy filename a:filename
```

Creating & exporting remote certificate(s)

Client certificate and private key files are created on the firewall. The files are combined into a PKCS12-formatted object, which is then exported to the deployment media and imported into SoftRemote on the client machine. A copy of the certificate without the private key (*.pem) also needs to be exported and then imported into SoftRemote to act as a trust point. Another copy of the certificate will remain on the firewall to act as its trust point and verify the client certificate during the establishment of a VPN connection.

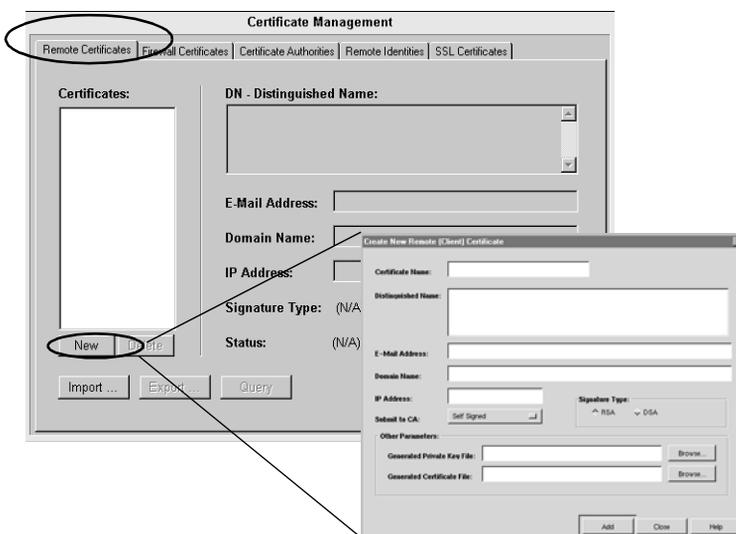
Use the following procedure on Sidewinder G₂ to create a self-signed certificate file (with its embedded public key) and a private key file for each of your SoftRemote clients. Once a pair of certificate/private key files are created for a unique client, you must use the firewall's `pkcs12_util` command to combine each file pair into a PKCS12-formatted object. Each PKCS12-formatted object must be distributed to the respective SoftRemote client.

From the Sidewinder G₂ Admin Console:

Note: The `pkcs12_util` must be run using the firewall's command line. If remotely administrating the firewall, you may accomplish this using a SSH, telnet, or remote Xterm session.

1. Select **Services Configuration -> Certificate Management**.
2. Select the **Remote Certificates** tab. Click **New**.

Figure 3-6.
Sidewinder Certificate
Management: Create
New Remote (Client)
certificate window



3. Specify the following Remote Certificate settings.

Field	Setting
Certificate Name	Specify a name for the remote certificate. Note: Use only alphanumeric characters plus the dash, dot, and underscore (-._). Do not begin the name with a dash (-).
Distinguished Name	Specify a set of data that identifies the client. Use the following format: cn=,ou=,o=,l=,st=,c= where: <ul style="list-style-type: none"> ◆ cn = common name ◆ ou = organizational unit ◆ o = organization ◆ l = locality ◆ st = state ◆ c = country Important: The syntax for this field is very important. The order of the specified distinguished name fields must match the desired order to be listed in the certificate. The above entries should be separated by commas, and contain no spaces or special characters.

More...

Field	Setting
E-Mail Address, Domain Name, IP Address	Optional fields for adding identification information (in addition to DN).
Submit to CA	Select Self Signed .
Signature Type	Select RSA .
Generated Private Key File	Click Browse and specify where you want to generate and save the private key associated with this certificate. You must use a <i>.pk1</i> extension (for example, " <i>clientprivate.pk1</i> ").  Important: The private key files must be created as <i>.pk1</i> objects. The conversion utility used starting in step 6 will not work with <i>.pk8</i> objects.
Generated Certificate File	Click Browse and specify where you want to generate and save this certificate. Use a <i>.pem</i> extension (for example, " <i>clientcert.pem</i> ").

Note: The generated private key and generated certificate files created above are needed to create a client private key file pair (a *.p12* file and a *.pem* file). These two client files are created with the firewall PKCS12 utility, as described in step 6 below.

4. Click **Add** to add the certificate to the Certificates list.
5. Click **Close** to return to the previous window.
6. To start the PKCS12 utility on the firewall, from the command line, enter the following command:

```
pkcs12_util
```

The utility will prompt you for the name and location of the private key file, for the name and location of the associated certificate file, and for the name and location in which to store the resulting PKCS12-formatted object.

The following message appears:

```
Please put file extensions on all file names.
Enter the name of the PKCS1 object (private key)
file:
```

7. Type the full path name of the private key file.

The following message appears:

```
Enter the name of the PEM signed public key
```

Converting the certificate file/private key file pair to PKCS12 format

(certificate) file:

8. Type the full path name of the associated certificate file.
The following message appears:

```
Enter the name of the output PKCS12 object (*.p12):
```

9. Type the full path name of the object file that will be created by the utility. Be sure to use a .p12 extension on the file name.

The following message appears:

```
pkcs12 encryption password for public key (it WILL be  
clear screen text):
```

10. Type a password for this PKCS12 object.

You apply a password to the object because the object contains both the public and private keys. The password can consist of any alphanumeric characters. The password will be needed when importing this object into a SoftRemote client.

Note: After typing the password, the utility creates the PKCS12 file in the directory you specified in step 9.

11. Return to **Step 1** and repeat for each remote client.

Once you have finished creating the PKCS12 object(s), copy each object (*.p12) and its corresponding certificate file (*.pem) to an accessible location for distribution to the appropriate SoftRemote client. If remotely administrating the firewall from a Windows machine, you may ftp the files to your PC and then save them to diskette. If on the firewall or a remote UNIX machine, you can do this using the **mcopy** command. (Repeat the entire command for each file.) For example:

```
% mcopy filename a:filename
```

**Copy the client key/
certificate object to a
diskette**

Managing CA-based certificates

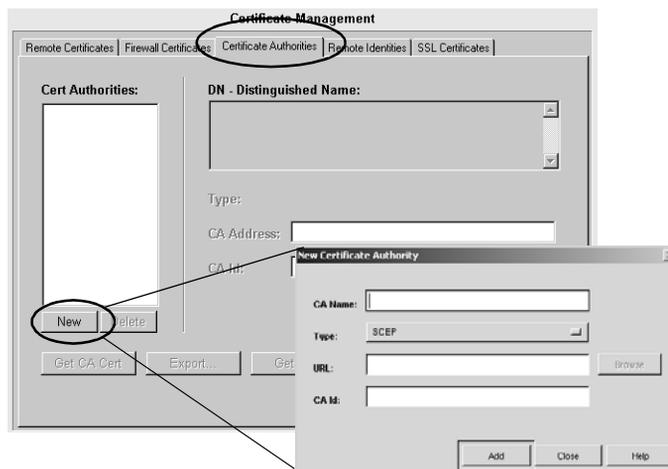
If you are using a CA to authorize certificates, use the following procedures to define the CA on the firewall, request the firewall and user certificates (if users will not be retrieving them), and define the remote identities of each client within the firewall (needed later when setting up your VPN connections). This procedure assumes you have already identified your desired Certificate Authority and made the necessary preparations.

Requesting and retrieving a CA-issued root certificate

To request a CA certificate for the firewall, do the following from the Admin Console.

1. Select **Services Configuration -> Certificate Management** and click the **Certificates Authorities** tab. Click **New**.

Figure 3-7.
Create New Certificate Authority window



2. In the **New Certificate Authority** window, specify the name, type, and location of the CA.

Note: Names must be unique and may be up to 255 characters. Use only alphanumeric characters plus the dash, dot, and underscore (-._). Do not begin the name with a dash (-). For SCEP, URLs must begin with "http://" to be accepted. Older versions of Netscape (e.g. Netscape 1.1) must end in '/cms/'.

3. Click **Add**, then click **Close**.
4. Click **Get CA Cert** to request the CA certificate and import it to the firewall.

- Click **Get CRL** to manually retrieve a new Certificate Revocation List (CRL) from the CA.

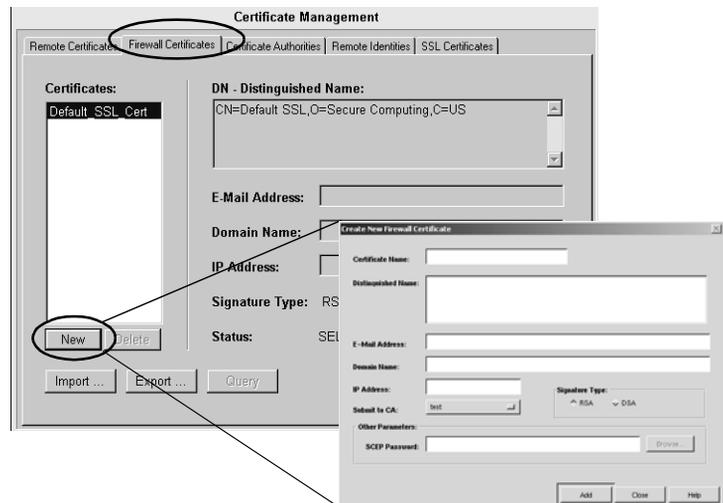
Note: *SoftRemote requires a copy of the CA root certificate. You may export it from the firewall with a .pem or .der extension, or simply retrieve another copy online using the SoftRemote client.*

Requesting and retrieving a CA-issued firewall certificate

To request a firewall certificate from a CA, do the following.

- Select **Services Configuration -> Certificate Management** and click the **Firewall Certificates** tab. Click **New**.

Figure 3-8.
Create New Firewall Certificates window



- Specify the firewall certificate information.

Field	Setting
Certificate Name	Specify a name for the firewall certificate. Note: Use only alphanumeric characters plus the dash, dot, and underscore (-._). Do not begin the name with a dash (-).

More...

Field	Setting
Distinguished Name	<p>Specify a set of data that identifies the firewall. Use the following format:</p> <p>cn=,ou=,o=,l=,st=,c=</p> <p>where:</p> <ul style="list-style-type: none"> ◆ cn = common name ◆ ou = organizational unit ◆ o = organization ◆ l = locality ◆ st = state ◆ c = country <p> Important: The syntax for this field is very important. The order of the specified distinguished name fields must match the desired order to be listed in the certificate. The above entries should be separated by commas, and contain no spaces or special characters.</p>
E-Mail Address, Domain Name, IP Address	Optional fields used for identity information (in addition to DN).
Submit to CA	Select the CA appropriate for your configuration.
Signature Type	Select RSA .
SCEP Password	Specify a password for managing the certificate (e.g., to revoke, etc.).

3. Click **Add** to send the enrollment request.



Important: After you send the enrollment request, the CA administrator must issue the certificate before you can continue.

4. On the Firewall Certificates tab, click **Query** to inquire about the status of your certificate request. If the enrollment request is accepted by the CA, the resulting certificate will be retrieved. (The firewall automatically queries the CA every 15 minutes to see if the request has been accepted. If the request has been accepted, the firewall will retrieve the resulting certificate.)
5. Record the firewall certificate's distinguished name information specified in step 2. This information must be entered into the security policy for each SoftRemote client.

Managing remote identities on Sidewinder G₂

In order to create a security association, you must define an identity "template" in the firewall that matches each possible group of remote identities that will be establishing a VPN under that security association. For example, "Sales" might be one group defined by a remote identity and given its own security association. If the group is using certificates, use Table 3-1 as a guideline for creating a distinguished name.



Caution: *If the group is using pre-shared keys, you should only enter a domain name or IP address and **not** a Distinguished Name.*

Determining identifying information for remote identities (certificates only)

Define the identifying information that will be used for each remote client certificate. Typically, these are the values entered in the Distinguished Name (DN) fields when defining a certificate. This information will be needed in either of the following scenarios:

- ◆ If you plan to direct remote users to request a remote certificate from the CA,
or
- ◆ If you plan to request remote certificates from the CA on behalf of the end-user.

Use Table 3-1 as a template for defining this information.



Tip: *An asterisk can be used as a wildcard when defining the fields on this window. For example; *, **O=acme**, **C=us** represents all users at ACME.*

Table 3-1. Client Distinguished Name (DN) information

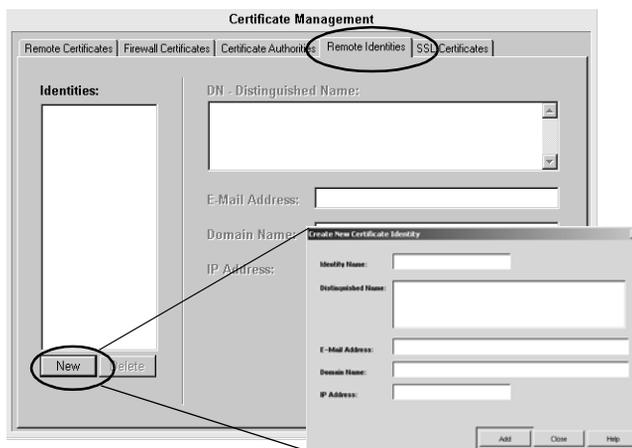
Distinguished Name fields	Record your information here
cn (common name)	
ou (organizational unit) Note: <i>SoftRemote lists this field as "Department."</i>	
o (organization) Note: <i>SoftRemote lists this field as "Company."</i>	
l (locality) Note: <i>SoftRemote lists this field as "City."</i>	
st (state)	
c (country)	

Entering identifying information for remote identities (all)

To define remote identities on the firewall, do the following.

1. Select **Services Configuration -> Certificate Management** and click the **Remote Identities** tab. Click **New**.

Figure 3-9.
Remote Identities defined on the firewall



2. In the Identity Name field, specify a name for the remote identities.

Note: Use only alphanumeric characters plus the dash, dot, and underscore (-._). Do not begin the name with a dash (-).

3. Select the identity type that best suits your authentication method:

- ◆ If using a pre-shared password/key, enter the appropriate information in either the E-mail Address, Domain Name, or IP Address field.
- ◆ If using certificates, specify a set of data that identifies the remote users in the Distinguished Name field.



Tip: Represent all users from a specific location one of two ways: One, the domain **acme.com** represents all users at ACME. Two, use an asterisk as a wildcard. For example: *, **O=acme, C=us**.

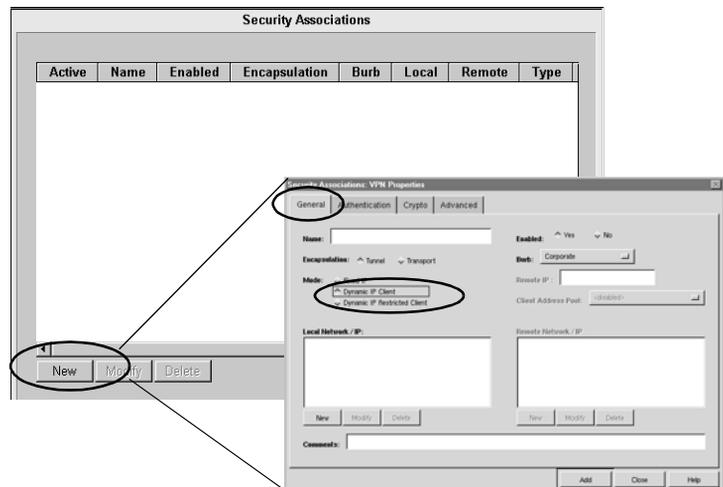
4. Click **Add**.

Configuring the VPN on Sidewinder G₂

Create a VPN security association for a **tunnel** VPN using your chosen method authentication. Do the following from the Sidewinder G₂ Admin Console:

1. Select **VPN Configuration -> Security Associations**. Click **New**.

Figure 3-10.
Sidewinder Security Associations window (defined VPNs)



2. Select the **General** tab and specify the following primary VPN settings.

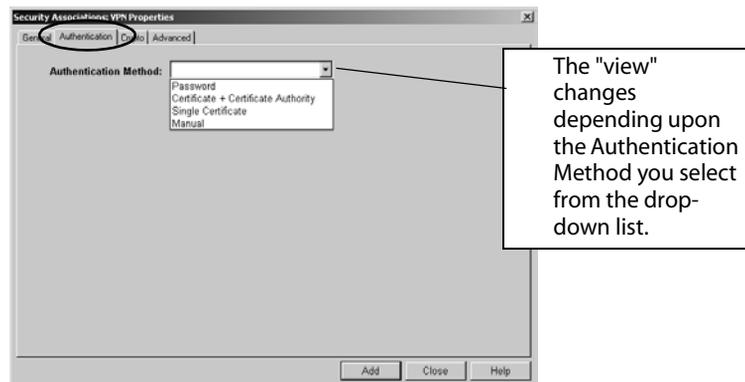
Field	Setting
Name	Enter a name for this VPN security association. Note: Use only alphanumeric characters plus the dash, dot, and underscore (-._). Do not begin the name with a dash (-).
Encapsulation	Select Tunnel . This is the more popular form of VPN encapsulation. Both the data and the source and destination IP addresses are encrypted within the encapsulated payload.
Enabled	Select Yes .
Burb	Click the drop-down list to assign this VPN to a burb. The firewall terminates each VPN in a burb, allowing you to apply access rules to the VPN if desired.
Mode	Select either Dynamic IP Client or Dynamic IP Restricted Client (the remote end is a device whose IP address is not fixed). Example: a salesperson that gains Internet access through an ISP using DHCP address assignment. Note: If selecting Dynamic IP Restricted Client , you will select either Client Address Pool (the firewall assigns the client a virtual IP address) or Dynamic Virtual Address Range (The firewall restricts client-configured virtual IP addresses).
Local Network/IP	Specify the network names or IP addresses to use as the destination for the client(s) in the VPN. Click the New button to specify the IP Address / Hostname and Number of bits in Netmask . The netmask specified identifies the network portion of the IP address. For example, if you specify a netmask of 24 with an IP address of 10.10.10.0, all IP addresses that begin with 10.10.10 are accepted. Note: If you are using Client Address Pools , the local network (destination for clients) is designated when configuring the client address pool. Note: If your client is configured for "All Connection", then enter 1.0.0.0/0 as your Local Network/IP.

More...

Field	Setting
If you selected Dynamic IP Restricted Client in the Mode field, you will need to define one of the following mutually exclusive options.	
Client Address Pool	Determine if you want remote clients to be assigned an IP addresses contained within one of the available client address pools. If so, use the drop-down list to select the client address pool you want to use. With this option, the firewall selects an IP address from the available pool and assigns it to the client for use during the VPN connection. Note: For information on creating Client Address Pools, see "Understanding Sidewinder G2 client address pools" on page 2-10 of this guide and Chapter 12 in the Sidewinder G ₂ Firewall Administration Guide.
Dynamic Virtual Address Range	Define the range of addresses a client can use when initiating a VPN connection. The addresses specified here do not represent a real network but are virtual addresses. With this option, the virtual IP address is configured at the client machine, and the firewall ensures that the addresses are within the approved address range.

3. Select the **Authentication** tab. Choose the authentication method appropriate for your configuration.

Figure 3-11.
Security Associations Properties, Authentication tab



- ◆ If you selected **Password** (Figure 3-12), specify the following password options.

Figure 3-12. "Password" options

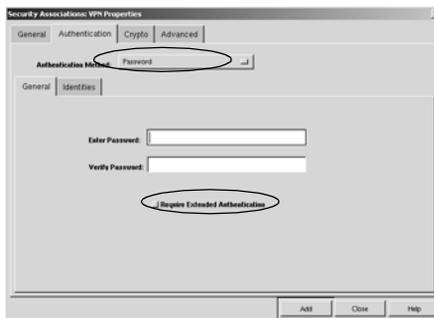


Table 3-2. Password options

	Field	Setting
General	Enter Password/ Reenter password	Enter and re-enter the password to be configured in the client security policy.
	Require Extended Authentication	Enable this check box if using Extended Authentication. Note: <i>Extended Authentication should always be used when shared-password authentication is used.</i>
Identities	Firewall Identity	Specify the identity to use when identifying the firewall to the remote client using a Fully Qualified Domain Name or an IP Address. E-mail is not recommended.
	Remote Identity	Specify the Remote Identities to recognize in VPN connections.

- ◆ If you selected **Single Certificate** (Figure 3-13), specify the following self-signed certificate options.

Figure 3-13.
"Single Certificate"
options

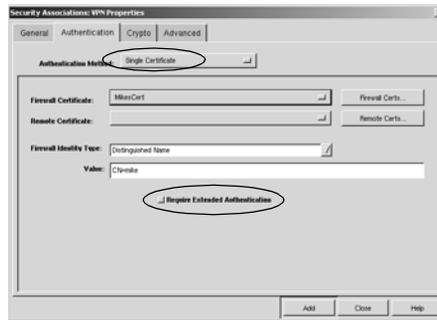


Table 3-3. Single Certificate (self-signed) options

Field	Setting
Firewall Certificate	Select the certificate used to authenticate the firewall to the remote client during the key exchange.
Remote Certificate	Select the certificate used on the remote end of the VPN from the list provided.
Firewall Identity Type	Select the identity type to use when identifying the firewall to the remote client. Note: <i>Distinguished Name is the default identity type. Other types will only be available if configured as part of the firewall certificate.</i>
Value	Contains the actual value used as the firewall identity. This field cannot be edited.
Require Extended Authentication	Enable this check box if using Extended Authentication.

- ◆ If you selected **Certificate & Certificate Authority** (Figure 3-14), specify the following CA certificate options.

Figure 3-14. "Certificate & Certificate Authority" options

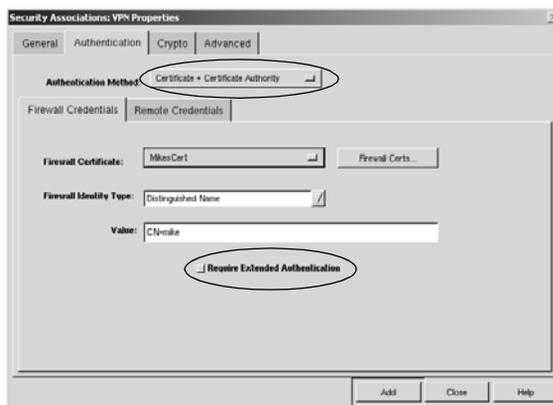


Table 3-4. Certificate + Certificate Authority options

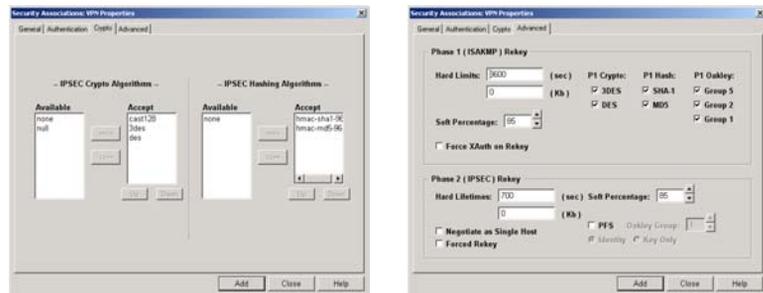
	Field	Setting
Firewall Credentials tab	Firewall Certificate	Select the certificate used to authenticate the firewall to the remote client during the key exchange.
	Firewall Identity Type	Select the identity type to use when identifying the firewall to the remote client.
	Value	Contains the actual value used as the firewall identity. This field cannot be edited.
	Require Extended Authentication	Enable this check box if using Extended Authentication.
Remote Credentials tab	Certificate Authorities	Move the certificate authority(ies) to trust for this VPN connection to the Trusted column. Note: Only remote certificates signed by listed CAs will be allowed to connect.
	Certificate Identities	Move the certificate identity(ies) to recognize in VPN connections to the Trusted column.

- ◆ [Conditional] If using aggressive mode, as is typical with connections configured for pre-shared passwords and extended authentication, specify the necessary settings. The encryption algorithms and rekey time limits need to match those configured in SoftRemote.



Tip: For Main Mode IKE configurations, you do not need to configure settings in the *Crypto* tab or *Advanced* tab windows. For details about those settings, refer to Chapter 12 in the Sidewinder G₂ Firewall Administration Guide.

Figure 3-15. “Crypto” and “Advanced” options



Save your settings!

4. Click **Add** to save the settings.
5. Click **Close**.

About this chapter

This chapter includes SoftRemote installation notes. It describes the basic SoftRemote procedures for managing certificates and passwords, creating a customized SoftRemote security policy for your remote clients, and configuring your ZoneAlarm personal firewall options.



Important: As network administrator, you need to install your own copy of SoftRemote and become familiar with the software before you deploy setup instructions and the SoftRemote software to each end user.

This chapter addresses the following topics:

- ◆ “Managing SoftRemote deployment” on page 4-2
- ◆ “SoftRemote installation and deployment notes” on page 4-5
- ◆ “Starting SoftRemote” on page 4-9
- ◆ “About the Certificate Manager” on page 4-16
- ◆ “Managing certificates in SoftRemote” on page 4-20
- ◆ “Configuring a security policy in SoftRemote” on page 4-25
- ◆ “Policy update distribution” on page 4-35
- ◆ “VPN management command” on page 4-36

Managing SoftRemote deployment

The best practice is to deploy the SoftRemote installation program with a customized security policy, including the necessary passwords and/or digital certificates and ZoneAlarm usage requirements. Custom installations are designed to make it easy to manage corporate security policies for tens, hundreds, or thousands of end users. During configuration you can set the interval and location to automatically pull subsequent policy updates see “Configuring a security policy in SoftRemote” on page 4-25.

Selecting a deployment strategy that compliments your authentication method and your end user population takes planning. Table 4-1 on page 4-3 is designed to help you analyze your options. As the administrator, you have the best understanding of your own environment, security policy, and resources. Brainstorm and problem-solve different deployment strategies ahead of time to determine which method best suits your needs. Keep in mind that scenarios discussed here are guidelines, not strict step-by-step instructions.

Along with the necessary software and configuration files, your deployment should provide specific SoftRemote installation and setup instructions for each end user. This facilitates management of corporate security policies for your end users and simplifies the deployment experience. Use the checklist provided in Table 4-2 on page 4-5 to help organize the tasks your users will need to perform.

Note: *When a filename is specified, such as IPSecPolicy.spd or CaCert.cser, you must use that filename for the file to auto-install. If the filename is represented by an *, you may choose your filename. You have more flexibility with naming conventions if you chose to have the files manually imported into a SoftRemote client.*

The security policies are exportable as fully locked, partially locked, or unlocked. Fully locked security policies will not allow the user to alter them, partially locked security policies allow the user to alter the **My Identity** portion of the policy only, and unlocked security policies are fully editable. In addition, you can password protect the security policies to enable encrypted policy postings and intransit privacy protection. The lock and password options are available when the security policy is initially exported from SoftRemote before being deployed to users.

Table 4-1 contains typical deployment scenarios, each with the overview configuration tasks, recommended deployment, and installation notes.

Table 4-1. Deployment Scenarios

Note: Your SoftRemote CD contains one directory that includes both the VPN client and Zone Alarm (SoftRemote), and another directory that includes only the VPN client (SoftRemote LT). You may choose to deploy only the desired product, or deploy both and then let each user decide which to one to install.

Scenario	SoftRemote Configuration	Recommended Deployment	Notes
Pre-shared key and extended authentication	Configure security policy including pre-shared key under My Identity on a SoftRemote client. Save file as <i>IPSecPolicy.spd</i> for auto-import, or <i>*.spd</i> for manual import.	<ul style="list-style-type: none"> ◆ Installation image <ul style="list-style-type: none"> — basic SoftRemote install package — <i>IPSecPolicy.spd</i> ◆ Provide end users with installation directions. 	<ul style="list-style-type: none"> ◆ Requires minimal user input during installation. ◆ Suitable for large deployments. ◆ Minimizes maintenance time and costs.
Self-signed firewall certificate and remote/personal certificate	<ol style="list-style-type: none"> 1. Configure the security policy and save as <i>IPSecPolicy.spd</i>. 2. Import firewall certificate with <i>*.pem</i> from accessible media. 3. Import the PKCS12 object (remote/personal certificate and key) with filename <i>*.p12</i> from accessible media. 4. Import the remote client certificate with <i>*.pem</i> from accessible media. 	<ul style="list-style-type: none"> ◆ Install image <ul style="list-style-type: none"> — basic SoftRemote install package ◆ Import from file: <ul style="list-style-type: none"> — <i>*.pem</i> (fw) — <i>*.p12</i> — <i>*.pem</i> (client) — <i>*.spd</i> ◆ Provide end users with installation directions and input information. 	<ul style="list-style-type: none"> ◆ Each client machine must have its own personal certificate. ◆ Auto-import is not a recommended option with this scenario, as file management of the individual certificates could be cumbersome.

More...

Scenario	SoftRemote Configuration	Recommended Deployment	Notes
CA certificate and personal certificate	<ol style="list-style-type: none"> 1. Request and retrieve a CA root certificate online using either the firewall or a SoftRemote client. Save file as <i>CACert.cser</i> for auto-import, <i>*.cser</i> or <i>*.pem</i> for manual import. 2. Configure security policy and save as <i>IPSecPolicy.spd</i>. 	<ul style="list-style-type: none"> ◆ Install image ◆ basic SoftRemote install package ◆ <i>CACert.cser</i> (if auto-importing) ◆ <i>IPSecPolicy.spd</i> ◆ If manually importing CA root certificate, import from file: <ul style="list-style-type: none"> ◆ <i>*.pem</i> ◆ Provide end users with installation directions and input information to request and retrieve their personal certificates online. 	<ul style="list-style-type: none"> ◆ If you chose to auto-import the <i>CaCert.cser</i>, a screen will appear after reboot (following the InstallShield Wizard) asking for the online personal certificate request information. Fill in the data at this point. SoftRemote will submit the certificate request to the CA and proceed with the install. ◆ Each client machine must have its own personal certificate.
Locked Policies and Automatic Policy updates	<ol style="list-style-type: none"> 1. Create and export new policy. 2. Policy includes interval to check for policy updates. 3. Policy includes URL to look for updates. 4. Password protect policy when exporting policy. 5. Lock policy when exporting policy. 	<ul style="list-style-type: none"> ◆ Locked policies used when Administrator wants to limit user policy editing capability. ◆ Automatic policy update enables convenient mechanism to deploy new policy to users. ◆ Policy protection provides privacy to policy update process. 	<ul style="list-style-type: none"> ◆ Policy locking and automatic updates are two separate features. ◆ Can be used with any of the above deployment scenarios.

SoftRemote installation and deployment notes

Use the Table 4-2 to guide you in preparing detailed installation instructions for your end users.

Table 4-2. SoftRemote install, deployment, and uninstall task summary

Task	Notes
Determine how to deploy SoftRemote to end users	<p>See scenario chart Table 4-1 on page 4-3 to help you decide which deployment option best suits your network environment.</p> <p>Based on your users' environment, include SoftRemote set up instructions for your end users from the following:</p> <ul style="list-style-type: none"> — specify dial-up network instructions — specify installation instructions — specify basic connection information — specify certificate import/request instructions — specify security policy import instructions — specify how and when to activate or deactivate the SoftRemote security policy — specify guidelines for using ZoneAlarm <p> Important: <i>If using Windows 9x and mode config (with client address pools), DNS may not automatically revert to dial-up provider values when the VPN stops. You will need to instruct users on how to break their ISP connection and reconnect to the ISP to reset the values. See the Appendix for more details.</i></p>
Prepare the client system for installation	<p>Prior to installing SoftRemote on any system, uninstall/remove any other VPN client programs that reside on the system. Also uninstall or disable any other personal firewalls that reside on the system. This includes uninstalling any resident copies of SecureClient or SoftPK software, and disabling the native XP Internet Connection Firewall.</p> <p> Important: <i>Failure to remove previous VPN client programs could result in very serious system problems.</i></p> <p>Uninstall using the Control Panel's Add/Remove program and reboot your computer before beginning the SoftRemote installation or upgrade.</p>

More...

Task	Notes
<p>Install SoftRemote</p> <p>Note: <i>If you are upgrading from a previous SoftRemote client, see the upgrade notes on page 4-7.</i></p>	<p>Note: <i>Do not have any other applications, including anti-virus software, open during the installation process.</i></p> <p>For Windows NT, 2000, or XP be sure to log in as Administrator or equivalent.</p> <p>To install SoftRemote, click the Install button on the autorun program from the SoftRemote CD. (If Autorun is disabled, you can also run the <i>setup.exe</i> program in the top-level SoftRemote directory of your choice—either the full SoftRemote product or SoftRemoteLT.)</p> <p>Select Custom install and check all three options on the Component Selection window.</p> <p>If you saved certificate or security policy files (using the filenames listed in Table 4-1) to the SoftRemote directory, they will auto-import during installation.</p> <p>See “Installing SoftRemote” on page 4-8 for details.</p> <p> Tip: <i>When setting up remote installations, you may elect to deploy the client install package to your end users via other means (e.g., provide a zip distribution or network-based installation).</i></p>
<p>If using ZoneAlarm, configure the personal firewall's settings</p>	<p>To configure ZoneAlarm, users respond to prompts triggered by traffic attempting to connect to the network. Consult the online help files for more information.</p> <p>To turn off ZoneAlarm, right click on the ZA icon in the system tray and select Shutdown ZoneAlarm.</p> <p>To require end users to use ZoneAlarm, go into SoftRemote's Security Policy Editor and select Options -> Firewall Settings. Then check “VPN connections require the firewall to be enabled.”</p> <p>To stop ZoneAlarm from loading at start up, go to Configure on the Control Center and uncheck “Load ZoneAlarm at start up.”</p> <p> Important: <i>To remove ZoneAlarm, use the uninstall utility included with the software. See “Activating/ Deactivating ZoneAlarm” on page 4-14 for more details.</i></p>
<p>Manage certificates in SoftRemote</p>	<p>If using digital certificate authentication, set up certificates using the Certificate Manager as described in “About the Certificate Manager” on page 4-16.</p>

More...

Task	Notes
Create security policies in SoftRemote	Before deploying SoftRemote, set up the appropriate information for the connection type, secure gateway tunnel, Phase 1 and Phase 2 settings, and the My Identity section as described in "Configuring a security policy in SoftRemote" on page 4-25.
Uninstall SoftRemote	<p>To remove SoftRemote, deactivate the client and then reboot. (It is important to have a clean reboot after your last use of SoftRemote's Virtual Adapter.) Shutdown the ZoneAlarm personal firewall.</p> <p>After you have logged in again, use the Add/Remove utility available in the Windows Control Panel. This process uninstalls both the VPN client and the ZoneAlarm personal firewall.</p> <p> Important: When you remove this software and its components, you have the option to keep your security policy, digital certificates, and private keys. This is recommended if you are uninstalling before an upgrade. The policy and certificates will be automatically pulled into the upgrade upon installation.</p>
Uninstall ZoneAlarm (only)	To remove ZoneAlarm, go to Start -> Programs -> Zone Labs -> Uninstall ZoneAlarm . Follow the instructions in the wizard. This process does not uninstall the VPN client.
Upgrade SoftRemote	<p>Before upgrading or reinstalling SoftRemote, uninstall any previous versions as noted above. Then proceed with the standard installation process.</p> <p> Tip: Save certificates and policy information when prompted during the uninstall process.</p>
Upgrading ZoneAlarm	Before upgrading, uninstall any previous versions as noted above. Then proceed with the standard installation process.

Installing SoftRemote

SoftRemote's initial installation is a simple process. The InstallShield Wizard leads you through the installation options.



Tip: *If you plan to distribute security policy or certificate files with your SoftRemote deployment, install the program on a Windows PC for use in creating those files for your end users.*

Do the following to start the application:

1. If you are installing this product on Windows NT or Windows 2000, log on as an administrator or its equivalent

2. Insert the product CD.

Note: *If auto-run is turned on, the SoftRemote 10 Set.up window will appear automatically and you may skip to the next set of steps.*

3. Click **Run** on the Start menu.

4. Click **Browse** and navigate first to the SoftRemote product CD, and then to the top-level *autorun.exe* file.

5. Click **Open**.

6. Click **OK** on the dialogue box to initiate the auto-run sequence, which brings up the SoftRemote 10.0 Setup window.

Once the SoftRemote 10.0 Setup window appears, do the following:

1. Select your installation configuration:

- ◆ Click **Install SoftRemote VPN and personal firewall** for the full SoftRemote installation option.
- ◆ Click **Install SoftRemote VPN client only** for the VPN client only SoftRemoteLT installation option.



Tip: *Click **SafeNet Notes** and **SCC Notes** to read the Release Notes.*

2. Click **Install SoftRemote**. After a moment, the InstallShield Wizard Welcome screen appears.

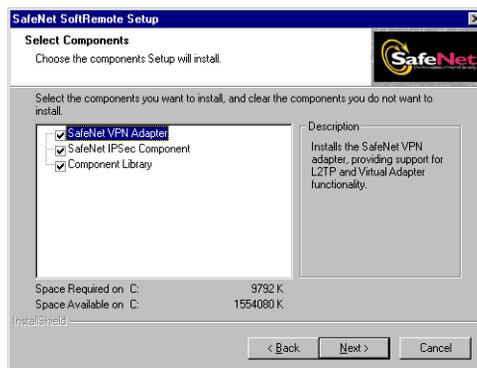
3. Click **Next**.

4. Read and understand the license agreement. Click **Yes** to continue.

5. Select **Custom**, and then click **Next**.

6. Ensure that all components are checked, and then click **Next**.

Note: The options will vary slightly depending on the Windows operating system used.



Note 1: The SafeNet VPN Adapter, which supports L2TP, requires the following network components to achieve full functionality as described here: Windows 95: *Dial-Up Networking with the Microsoft Dial-Up Networking 1.3 Upgrade*; Windows 98 and ME: *Dial-Up Networking*; Windows NT: *Remote Access Server (RAS)*.

Note 2: The Windows9x VPN Adapter option includes the VA Adapter, which you should include in the installation.

7. Review the settings, and then click **Next**. The InstallShield Wizard copies the necessary files.
8. Ensure that the **Yes, I want to restart my computer now** option is selected, and then click **Finish**.

Starting SoftRemote

SoftRemote starts automatically each time its host computer is started. It runs transparently at all times behind all other software applications, including the Windows login. The SoftRemote VPN client icon in the taskbar changes color and image to indicate the status of system communications. The ZoneAlarm icon switches from the ZoneAlarm icon to a lock to indicate whether or not Internet traffic is being allowed onto the system.

Note: If you do not want ZoneAlarm to automatically load at start up, go to Configure on the ZoneAlarm Control Center and uncheck "Load ZoneAlarm at start up."

Figure 4-1. SoftRemote icons in the Windows system tray



SoftRemote icons in taskbar

Determining VPN client status from icon variations

The following table summarizes all SoftRemote VPN client icon variations and their meaning.

Table 4-3. VPN client taskbar icons

Icon	Description
	Grey background/red line —Indicates Windows did not start the SoftRemote service properly or that your security policy is disabled.
	Yellow background —Indicates SoftRemote is installed correctly; no connection is established.
	Yellow and red background —Indicates a non-secure connection established; transmitting non-secure communications.
	Yellow key/dark green background —Indicates at least one secure connection established; no transmission.
	Yellow key/red background —Indicates at least one secure connection established; transmitting non-secure communications only.
	Yellow key/light green background —Indicates at least one secure connection established; transmitting secure communications only.
	Yellow key/red and light green background — Indicates at least one secure connection established; transmitting secure and non-secure communications.

In summary, **light green** means the computer is transmitting securely; **red** means it is transmitting unsecure communications. Both **red and light green** means that the computer is transmitting both secure and unsecure data simultaneously, on different connections.

Determining ZoneAlarm status from icon variations

The following table summarizes ZoneAlarm personal firewall icon variations and their meaning.

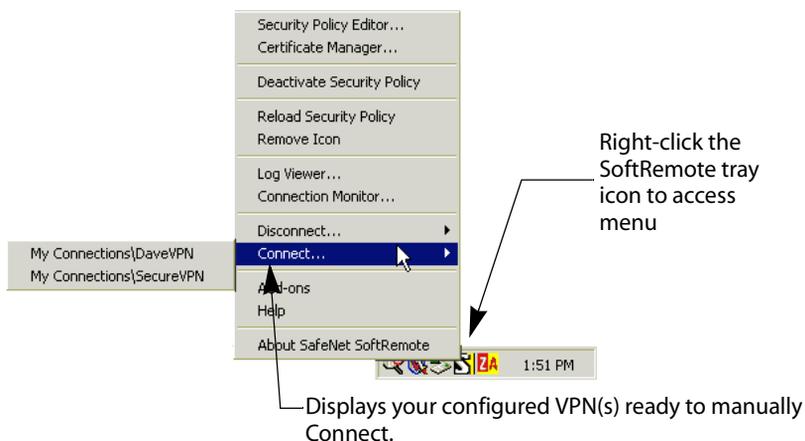
Table 4-4. ZoneAlarm icons

Icon	Description
	<p>ZoneAlarm — Indicates the ZoneAlarm application is installed. To display the ZoneAlarm control center window, right click and select Restore ZoneAlarm Control Center.</p>
	<p>Internet Activity Stopped — Indicates that Internet access is locked with High Security. A red closed lock indicates that traffic is blocked.</p>
	<p>Internet Activity — Indicates Internet activity as it happens. The original ZA icon image changes to this image when Internet traffic is being passed.</p>

Disconnect/Connect SoftRemote VPN Client

The SoftRemote VPN 'specified connections' can be manually connected or disconnected by a right-click on the SoftRemote icon in the taskbar. The popup menu displays the Connect and Disconnect VPN configurations as shown in Figure 4-2. A user can select the Connect option from the SoftRemote icon in the taskbar to display the configured VPN connections available for connection. From the displayed list, you can select the desired configured connection to initiate a VPN connection to the gateway. Conversely, a user can select the Disconnect option from the SoftRemote icon in the taskbar to display the active VPN connection. Then from this displayed list, you can select the desired connection to disconnect from the gateway.

Figure 4-2. SoftRemote system tray icon Connect/Disconnect options



Note: The manual connection feature is only available for 'specified connections'. The manual connection feature is not available for 'All Connection' policies.

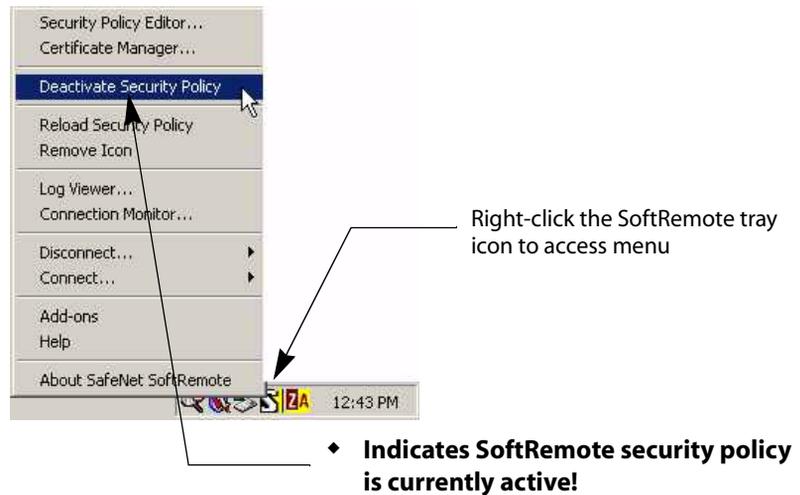
Activating/Deactivating SoftRemote VPN client

The SoftRemote security policy can be activated and deactivated by a right-click on the SoftRemote icon in the taskbar. This displays the Activate/Deactivate Security Policy menu option as shown in Figure 4-3. When deactivated, the option shows **Activate Security Policy**. When activated, the option shows **Deactivate Security Policy**.

To deactivate the SoftRemote security policy, click **Deactivate Security Policy**. This toggles the security policy to deactivate and the option menu displays **Activate Security Policy**.

To activate the SoftRemote security policy, click **Activate Security Policy**. This toggles the security policy to activate and the option menu displays **Deactivate Security Policy**.

Figure 4-3. SoftRemote system tray icon options



SmartRemote Start menu options

Figure 4-4 shows the program options that are available when you launch the SoftRemote user interface from the Start menu. This is a subset of the options available by right-clicking the SafeNet icon.

Figure 4-4. SoftRemote Start menu options



Activating/Deactivating ZoneAlarm

The ZoneAlarm user interface (known as the Control Center) defines how the personal firewall should handle alerts, locking policies, security settings, programs that want to access the Internet, and general configuration settings. ZoneAlarm is generally configured through pop-up queries to the user as applications attempt to access the network. Additionally, users may use the Control Center to configure, view, and modify the settings and zones.



Important: ZoneAlarm's security policy cannot be configured before installation. If you want user to set up ZoneAlarm to match your security policy, provide your users with instructions on how to set up ZoneAlarm.

As shown in Figure 4-5, you can right-click on the ZoneAlarm icon in the system tray to see all program options. Use this icon whenever you want to either modify or disable ZoneAlarm. ZoneAlarm is also activated and deactivated from the system tray menu. To make changes to your personal firewall policy, select Restore ZoneAlarm Control Center. See the program's online help for details on navigating the interface.

Figure 4-5. ZoneAlarm system tray icon options

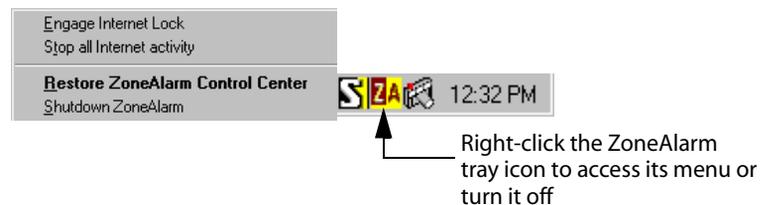


Figure 4-6 shows the program options that are available when you launch the ZoneAlarm Control Center from the Start menu.

Figure 4-6. ZoneAlarm Start menu options



Note: Use the utility provided with ZoneAlarm or the Control Panel's Add/Remove feature if you choose to uninstall the personal firewall program.

Learning about the SoftRemote programs

This section provides a brief description of the SoftRemote main program options, followed by important sub-options.



Tip: Browse the SoftRemote's comprehensive online help system to become familiar with client procedures and other detailed information.

◆ Security Policy Editor

The Security Policy Editor allows you to create, import, or export connection policies that define an IP data communications security policy.

◆ Certificate Manager

The Certificate Manager allows you to request, import, configure, and export the digital certificates received from certificate authorities (CAs) and trust points. To communicate securely using digital certificates, users must have two digital certificates: a root (CA or self-signed firewall) certificate and a personal certificate. This program allows you to define a trust policy that indicates which certificates to trust for IPSec sessions.

◆ Log Viewer

The Log Viewer displays the communications log, a diagnostic tool that lists the IKE negotiations that occur during the authentication and key generation phases.

◆ Connection Monitor

The Connection Monitor displays statistical and diagnostic information for each active secure connection in the security policy. This utility displays the actual security policy settings configured in the Security Policy Editor and the security association (SA) information

established during Phase 1 IKE negotiations and Phase 2 IPsec negotiations.

◆ **ZoneAlarm**

ZoneAlarm is a personal firewall that provides another level of control over Internet traffic that enters and exits the client system. Installing and requiring the use of ZoneAlarm are both optional.

About the Certificate Manager

If you are using digital certificate authentication in your VPN, you should provide your end users with the information and files needed to set up the necessary certificates on their SoftRemote client. You should also indicate what trust policy they will use, as this dictates which certificates will be considered valid or invalid. This section provides a basic overview of what you need to do and includes (or provides cross-reference to) the appropriate procedures.



Important: *The firewall self-signed or CA root certificate should always be present on the SoftRemote client before configuring the client certificate.*

Setting up a trust policy

Your trust policy determines which root CAs are trusted and therefore accepted for IPsec sessions and which ones are untrusted, or rejected. If a root CA is untrusted, certificates issued by this CA are considered invalid for IPsec. Your trust policy applies to your personal certificates as well as to remote parties' certificates. Your trust policy may be implemented using options on either the Trust Policy or Root CA Certificates tab and by using the Configuration Parameters dialogue box.

Note: *When self-signed certificates that are Certificate Authorities are imported at the VPN client, they are automatically considered trusted. Certificates that are imported through other means need to be manually configured to be trusted.*

Your trust policy is defined by selecting one of the following options:

- ◆ Root CAs specifically configured for IPsec communications (default)
- ◆ Root CAs that have issued a personal certificate to any of the computer's users
- ◆ All root CAs installed on your computer (the local machine)

You set your overall trust policy by selecting the appropriate radio button on either the Trust Policy tab (Figure 4-7) or on the Root CA Certificates tab (Figure 4-8).

Figure 4-7. SoftRemote Certificate Manager: Trust Policy tab



Figure 4-8. SoftRemote Certificate Manager: Root CA Certificates tab

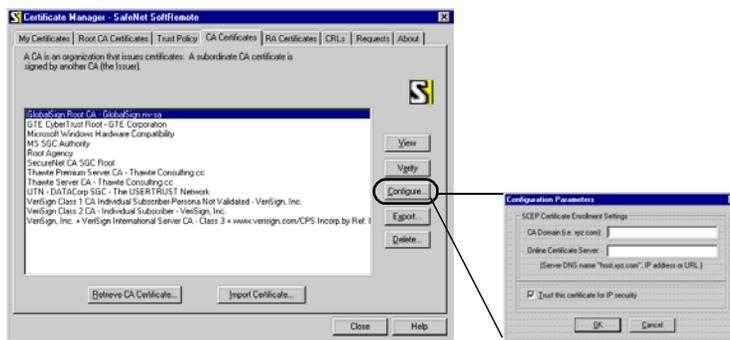


Caution: The options shown on the two tabs are directly linked. SoftRemote sets the trust policy according to the most recent change, regardless of where the change is made.

You may also set your trust policy on an individual root certificate basis. To trust a specific certificate, do the following:

1. In the Certificate Manager, ensure that the “Show only trusted roots” check box on the Root CA Certificates tab is **not** checked.
2. Click the tab that shows the certificate you want to configure:
 - ◆ Root CA Certificate
 - ◆ CA Certificates
3. Click the desired certificate to configure.
4. Click the **Configure** button. The Configuration Parameters dialog box opens.

Figure 4-9. SoftRemote Certificate Manager: Root CA Certificates tab



5. Specify that this certificate is trusted for IPSec communications by ensuring that the **Trust this certificate for IP security** check box is checked. The next time you view or verify this certificate, the ENH KeyUsage field will include this value: **IP security end system**.

Note: Only root certificates may be configured as part of the trust policy. Other associated certificates are trusted based on the status of their root certificate.

6. Click **OK**.

Setting up Sidewinder G₂ self-signed certificates

If you are using Sidewinder G₂ self-signed digital certificates, as the administrator, do the following:



Tip: In a VPN connection, keep in mind that the definition of "remote" depends on perspective. On the firewall, the end user's certificate is referred to as a "remote" certificate. On SoftRemote, it is referred to as a "personal" certificate. In this section, for clarity, it is referred to as the remote/personal certificate.

1. Prepare instructions to guide your end users through the following tasks:
 - a. Import the self-signed firewall certificate into the Root CA Certificates tab. See "Importing CA root or firewall certificates in SoftRemote" on page 4-20 for details.
 - b. Import the self-signed remote/personal certificate into the Root CA Certificates tab. See "Importing CA root or firewall certificates in SoftRemote" on page 4-20 for details.
 - c. Import the personal certificate -- the PKCS12 certificate and private key (text) into the My Certificates tab. See "Requesting and retrieving personal certificates in SoftRemote" on page 4-22 for

details.

2. Give these instructions to your end users.

Setting up CA-based certificates

If you are using CA-based digital certificates, the certificates may be requested either through Sidewinder G₂ or SoftRemote. If you want to include the CA root certificate with the installation image, follow the instructions for auto-import enrollment. If you want your users to import their own certificates online, follow the instructions for online enrollment.

For auto-import enrollment, do the following:

1. Import the CA root certificate, either created on the firewall or obtained online using SoftRemote, into the SoftRemote Certificate Manager. See “Importing CA root or firewall certificates in SoftRemote” on page 4-20 for details.

Note: You must import a copy of the CA root certificate into both the firewall and SoftRemote to successfully complete the VPN installation.

2. Export the CA root certificate file, naming it *CaCert.cser*, to the SoftRemote install image (in the same directory as the desired *setup.exe*). The CA root certificate will now auto-import during the SoftRemote installation on the client machine.
3. Prepare instructions for users to request and retrieve the personal certificate online. A copy of this procedure is provided later in this chapter. See “Requesting and retrieving personal certificates in SoftRemote” on page 4-22.
4. Give these instructions to your users with their SoftRemote installation.

For online enrollment, do the following:

1. Prepare instructions to guide your end users through the process of retrieving the CA root certificate online. See “Importing CA root or firewall certificates in SoftRemote” on page 4-20 for details.
2. Prepare instructions to guide your end users through the process of requesting and retrieving the personal certificate. See “Requesting and retrieving personal certificates in SoftRemote” on page 4-22 for details.
3. Give these instructions to your users with their SoftRemote installation.

Managing certificates in SoftRemote

The Certificate Manager module allows you to request, import, configure, and export digital certificates, and to define your trust policy. Review the previous section, “Setting up a trust policy” on page 4-16, if you are unfamiliar with the trust policy options presented in the Certificate Manager.

Importing CA root or firewall certificates in SoftRemote

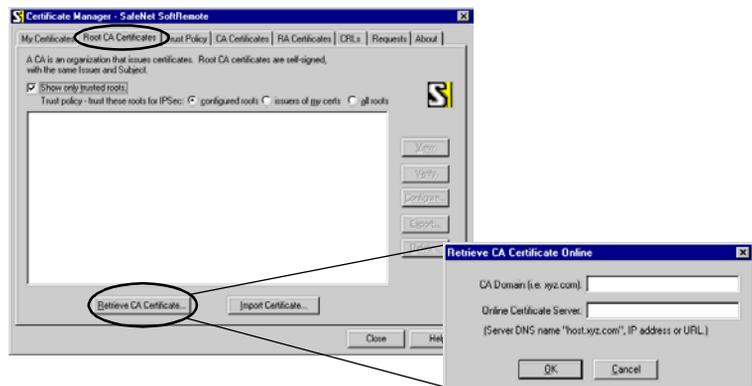
Use the following procedures to import a CA root, firewall self-signed, or client self-signed certificate into the SoftRemote system. These procedures are done at the client system and assume SoftRemote is already installed. The first set of instructions is for importing certificates online. The second set is for importing certificates from file.

Importing a CA root certificate online

Use the following procedures to request and retrieve a certificate online into the SoftRemote system. The client machine must have network access to the Certificate Authority.

1. Select **Start -> Programs -> SoftRemote -> Certificate Manager** (or right click the SafeNet icon and select Certificate Manager).
2. Click the **Root CA Certificates** tab.
3. Click **Retrieve CA Certificate...**. The Retrieve CA Certificate window appears.

Figure 4-10. SoftRemote Certificate Manager: Root CA Certificates tab, Retrieve CA Certificate



4. Enter the CA Domain and Online Certificate Server information.
5. Click **OK**.

Importing a CA root or firewall self-signed certificate from file



6. [Optional] From the Root CA Certificates tab, click **View** to see the information in the certificate.

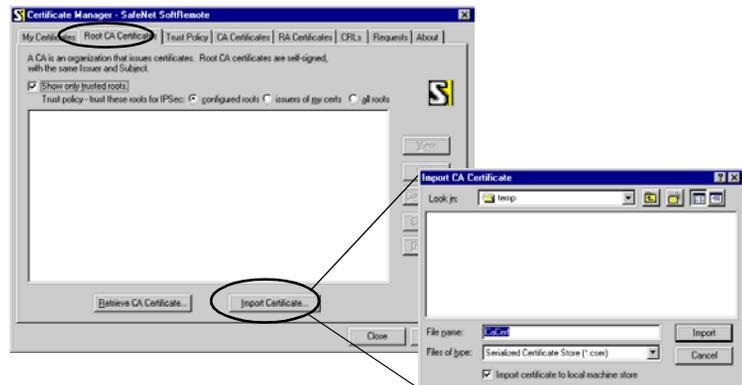
Note: The certificate will now be listed on the Root CA Certificates tab.

Use the following procedure to import a CA root, firewall self-signed, or client self-signed certificate from an accessible location (portable storage device or network) into the SoftRemote system. You must have created a file containing an exported certificate.

Important: If you are using self-signed certificates, you will need to import both the firewall and the personal certificate files into the Root CA Certificates tab.

1. Select **Start -> Programs -> SoftRemote -> Certificate Manager** (or right click the SafeNet icon and select Certificate Manager).
2. Click the **Root CA Certificates** tab.
3. Click **Import Certificate...**. The Import CA Certificate window appears.

Figure 4-11.
SoftRemote Certificate
Manager: CA Certificates
tab, Import CA
Certificate



4. From the **Files of type:** field, select **All Files (*.*)** and then navigate to display the files.
5. Browse to the appropriate *.pem (fw certificate) file and click **Open**. A window appears prompting you to confirm you want to import the selected certificate.

Note: SoftRemote supports other certificate files types, such as .der, .cser, .p7b, etc.

6. Click **Yes**.
7. [Optional] From the CA Root Certificates tab, click **View** to see the information in the certificate.

Requesting and retrieving personal certificates in SoftRemote

Use the following procedures to obtain personal certificates using the SoftRemote system. These procedures are done at the client system and assumes SoftRemote is already installed. They also assume that you have already retrieved the corresponding certificates for the firewall. The first set of instructions is for requesting and retrieving a certificate online. The second set is for importing a certificate from file.



Important: Self-signed personal certificates must be imported in both the My Certificates and the Root CA Certificates tabs.

Note: This procedure can be performed on behalf of the users by the administrator or performed by the end users at their machines. The exported certificate file may be used to import into a client machine (if created elsewhere) or saved as a backup.

Requesting and retrieving a personal certificate online

Use the following procedures to request and retrieve certificates online. The client machine must have network access to the Certificate Authority.

1. Select **Start -> Programs -> SoftRemote -> Certificate Manager** (or right click the SafeNet icon and select Certificate Manager).
2. Click the **My Certificates** tab.
3. Click **Request Certificate...** The Online Certificate Request dialog box appears.
4. [Optional] Select the **Generate Exportable Key** check box.

Figure 4-12. SoftRemote Certificate Manager: My Certificates tab, Online Certificate Request dialog box



Caution: You will only be able to export the private key associated with the personal certificate you are currently requesting if you check this option now. For security reasons, no one can change it later. Reasons you might want the exported key include using it with the installation, having users import the certificate and key, and having the key available for backup or recovery purposes.

5. If you did not obtain the root CA certificate through SoftRemote, click **Advanced** to set the certificate service provider address.
6. Under **Enrollment method**, click **Online**.
7. Under **Subject Name**, enter all relevant personal information, pressing the Tab key to move through the dialog box.
Note: *If you press **Enter**, the request will generate before you are finished.*
8. Under **Online Request Information**, enter or select these options:
 - a. In the **Challenge Phrase** box, enter any combination of numbers or letters you choose. For security reasons, only asterisks appear here.
 - b. In the **Confirm Challenge** box, enter the same phrase from the last step.
 - c. From the **Issuing CA** list, select a CA certificate.
Note: *Keep the challenge phrase that you entered on the enrollment form somewhere secure. This challenge phrase may be needed in the future to either restore or revoke the certificate.*
9. Click **OK**. Certificate Manager now generates a public/private key pair, and then displays the **Online Certificate Request** dialog box to indicate that it is waiting for a response from the CA. When the CA accepts your request, the **Certificate Manager** dialog box appears. Click **OK** again.
10. [Optional] To view your request, click the **Requests** tab. Select the request and click **View**. Click inside the certificate window to close it.
11. Get your CA administrator to approve your request.
12. Once your request is approved, select it under the **Requests** tab and click **Retrieve**.
13. Click **Yes** when the Certificate Manager dialog box asks if you want to add this personal certificate. The request disappears, but the personal certificate now appears under the **My Certificates** tab.
Tip: *You should select the new certificate and click **Verify** to verify it.*
14. In the **My Certificates** tab, select a personal certificate.
15. Click **Export**. The Export Certificate and Private Key dialog box appears.
16. In the **Filename** box, enter the drive, directory, and filename for the personal certificate file. The default setting is `C:\Temp\Cert.p12`.
Note: *The personal certificate file can be imported by the user or included for auto-import in the install image as "IpSecCerts.p12".*
17. In the **Password** box, type any password you choose.



Exporting a backup
personal certificate

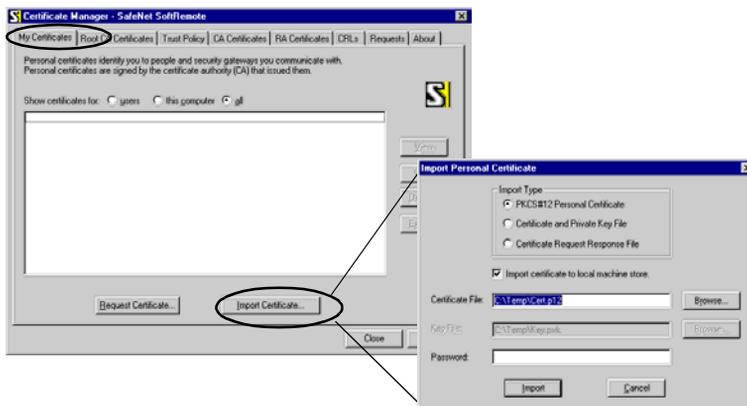
Importing a personal certificate from file

18. In the **Confirm Password** box, retype the password.

Use the following procedure to import a personal certificate from an accessible location (portable storage device or network) into the SoftRemote system. If the certificate is a self-signed certificate, you also need to import a copy into the Root CA Certificates tab.

1. Select **Start -> Programs -> SoftRemote -> Certificate Manager** (or right click the SafeNet icon and select Certificate Manager).
2. Click the **My Certificates** tab.
3. Click **Import Certificate...**

Figure 4-13.
My Certificates tab:
Import Certificate (and private Key) window



4. In the **Import Type** section, select **PKCS#12 Personal Certificate**.
5. Browse to the appropriate *.p12 file and click **Open**. The following window appears.
Note: The file type must be a PKCS12 object. PKCS8 and PKCS1 objects cannot be used.
6. Specify the password used when creating the .p12 file (step 17 on page 4-23). You will not be allowed to import the certificate without the proper password
Note: You must provide this password to the end user so they can later import this certificate file.
7. Click **Import**. A prompt appears to confirm you want to import the selected Personal Certificate.
8. Click **Yes**.
9. [Optional] From the **My Certificates** tab, click **View** to see the information

in the certificate.

10. If using self-signed certificates, click the **Root CA Certificates** tab.
11. Click **Import Certificate...** The Import CA Certificate window appears.
12. From the **Files of type:** field, select **All Files (*.*)** and then navigate to display the files.
13. Browse to the appropriate *.pem (client certificate) file and click **Open**. A window appears prompting you to confirm you want to import the selected certificate.
14. Click **Yes**.

Configuring a security policy in SoftRemote

As an administrator, you can configure end user security policies on your SoftRemote system, save them, and deploy them to your users. You have the options of locking security policy files so users cannot alter the policy and password encrypting them to protect privacy during policy posting and transit.

Determining connection options

When you configure a user policy on SoftRemote, you can specify to send all traffic over one VPN connection, or specify to send traffic over separate connections (some or all of which can be secured) for different traffic destinations. Multiple individual VPN tunnels are possible, as are a mix of VPN tunnels and unprotected connections. The individual connections are processed on a top-down basis. Traffic is handled by the first connection configuration that it matches.

Select **Options -> Secure** from the Security Policy Editor's main menu to choose between the options listed here.

- ◆ **Specified Connections** — This option allows you to configure multiple simultaneous connections. This option includes a default connection configuration, called "Other Connections," that controls traffic not covered by prior connection rules.

- ◆ **All Connections** — This allows you to configure one, and only one, connection that secures all IP communications through a connection to a specific gateway.

Note: Ensure that the firewall's Security Association information is also configured for securing all connections. See the information for configuring the Local Network/ IP field on page 3-20.

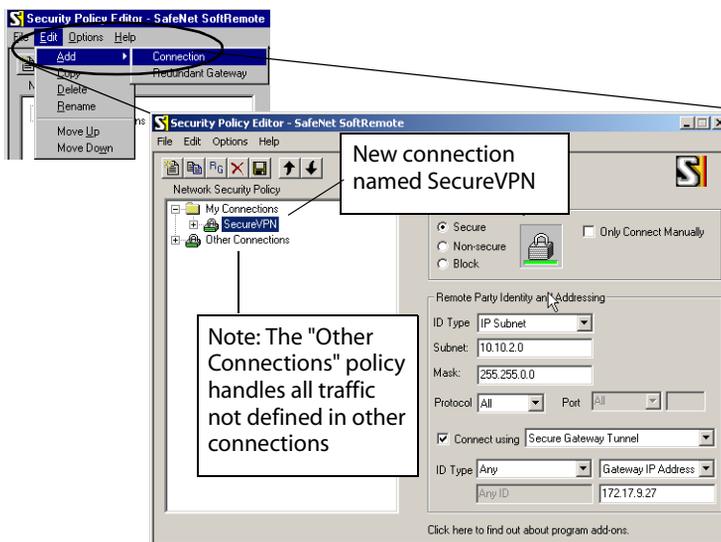
Setting up a Specified Connection policy

The first part of this section describes the setup of a multiple connection policy under the **Specified Connections** scenario. The connection settings you configure must coincide with configured settings/capabilities on the Sidewinder G₂ VPN Gateway.

Configuring a specified connection

1. Select **Start -> Programs -> SoftRemote -> Security Policy Editor** (or right click the SafeNet icon and select Security Policy Editor).
2. Select **Options-> Secure-> Specified Connections**.
3. Select **Edit -> Add -> Connection** to create a new connection.

Figure 4-14.
SoftRemote: Security Policy Editor



4. Specify a descriptive name for the connection. (The name "SecureVPN" is used in this example.)

5. Specify the connection type. In the **Connection Security** section, specify the setting that best fulfills your business need:
 - ◆ Non-secure mode—allows IP communications for this connection to pass through unsecured (unencrypted)
 - ◆ Secure mode—secures (encrypts) IP communications for this connection
 - ◆ Block mode—stops all IP communications for this connection from passing through
6. Specify the trusted network to which the client will be communicating. In the **Remote Party Identity and Addressing** fields:
 - ◆ Change the **ID Type** to **IP Subnet**.
 - ◆ Specify the **Subnet** and **Mask** of the trusted network on the inside of the firewall.

Note: *If this policy is configured for all connections, this field will be absent as all addresses are inherently included in this type of connection.*

7. Enable the **Connect using Secure Gateway Tunnel** box.
8. Specify the interface information for the Secure Gateway Tunnel that matches your authentication and network environment:
 - ◆ If using shared password: Set the **ID Type** to either **IP Address** or **Domain Name**
 - If you select IP Address, enter the IP address of the firewall's internet interface.
 - If you select Domain Name, enter the firewall's domain name in the field below. Then select either **Gateway IP Address** or **Gateway Hostname** (fully-qualified domain name) and enter the appropriate information in the field below.
 - ◆ If using digital certificates:
 - Set the **ID Type** to **Distinguished Name**.
 - Enter the **Gateway IP Address** or the **Gateway Hostname** (fully-qualified domain name) of the firewall's internet interface in the field below.
 - Click **Edit Name**, and then in the window that appears (Figure 4-15), enter the Distinguished Name information. Input all fields from the Firewall Certificate and click **OK**.

Figure 4-15. SoftRemote: Edit Distinguished Name window to specify Firewall public certificate



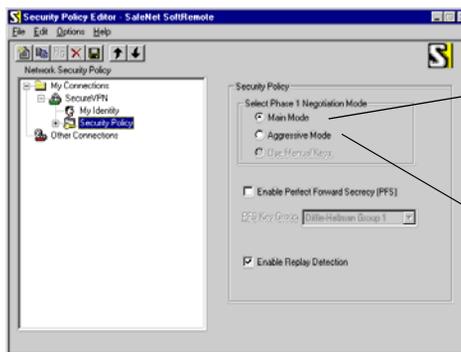
- ◆ If you want to accept any digital certificate from the gateway that resolves to a trusted Root CA certificate already configured on your SoftRemote client:
 - Set the **ID Type** to **Any**.
 - Enter the **Gateway IP Address** or the **Gateway Hostname** (fully-qualified domain name) of the firewall's internet interface in the field below.



Caution: In some instances data entered in the policy editor may be lost when changing screens without saving the data, therefore click the **Save** (floppy disk) icon before moving between policy editor screens.

9. Expand your new connection and then click on **Security Policy**. Select the Phase 1 Negotiation Mode.

Figure 4-16. SoftRemote: Security Policy fields

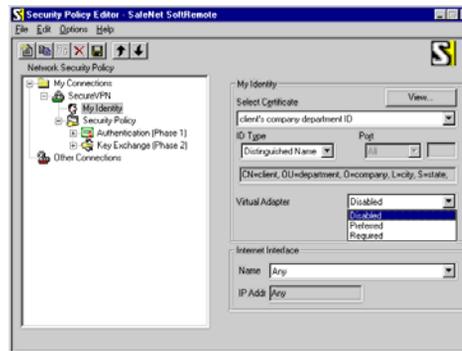


Use **Main Mode** for certificate-based or fixed IP address clients' VPNs

Use **Aggressive Mode** for pre-shared keys with dynamic client IP address

10. Specify how the user will be identified to the firewall. Select **My Identity**.

Figure 4-17.
SoftRemote: My Identity
fields



- a. Select the authentication method for this connection.
 - ◆ If using shared password:
 - From the Select Certificate drop-down list, select **None**.
 - Click **Pre-Shared Key** and enter the shared password.
 - [Conditional] If using aggressive mode, select **ID Type** and enter desired ID. The ID used (domain name or e-mail address) must match that configured for the remote identity on the firewall.
 - ◆ If using digital certificates, do one of the following:
 - Highlight the personal certificate previously imported from the drop-down list. Notice the ID Type automatically changes to Distinguished Name.
 - Highlight “Select automatically during IKE negotiation.”
 - Select **ID Type** and select your desired ID. Distinguished Name is the default, as all certificates use DN. You may choose any other listed ID Type, but certificates that do not contain that type of identity information will not be allowed.
- b. In the **Virtual Adapter** drop-down box, specify the status of the virtual adapter

Note: Save policy updates before moving to the next screen when changing this setting.

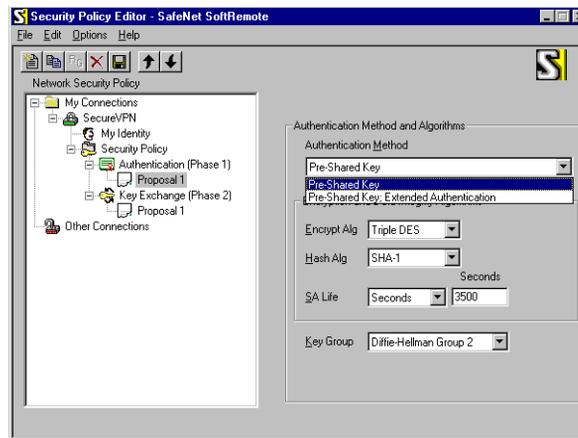
Status	Connection Type	Comments
Disabled	No virtual adapter is created. There is no WINS bind, and only variable DNS bind, which is platform dependent.	Requires manually creating WINS configuration information and requires manual configuration on Windows 2000 for DNS information.
Preferred	SoftRemote attempts to create a virtual adapter. If attempt fails, the connection is created as if in the Disabled option.	If the virtual adapter fails, SoftRemote loses WINS configuration information and may lose DNS configuration information sent from the VPN gateway.  Caution: If the configuration information is lost, you will have to configure it manually.
Required	SoftRemote attempts to create a virtual adapter upon VPN connection. Once the virtual adapter is successfully created, Soft Remote has WINS and DNS configuration information from the VPN connection gateway.	No connection is established if the virtual adapter is not created. Retries the VPN connection until the virtual adapter is successfully created.  Tip: This is the recommended deployment to ensure consistent behavior across platforms.

- c. In the **Internet Interface** selection drop-down box, specify which interface to use when creating the VPN connection. For our example, the default "Any" is adequate.
 - ◆ If your policy a virtual adapter, you must select **Any**.
 - ◆ If you would like your VPN to only initiate when the client machine is using a specific physical adapter, then identify that adapter here. (For example, if you want a VPN connection only when a dial-up adapter is used but not when a LAN adapter is used, select the dial-up adapter from the drop-down list.)

Note: On Windows 2000, dial-up adapters only appear in the drop-down menu when the dial-up connection is active. A selection that is made while the adapter is listed will persist and be recognized on the next connection attempt.

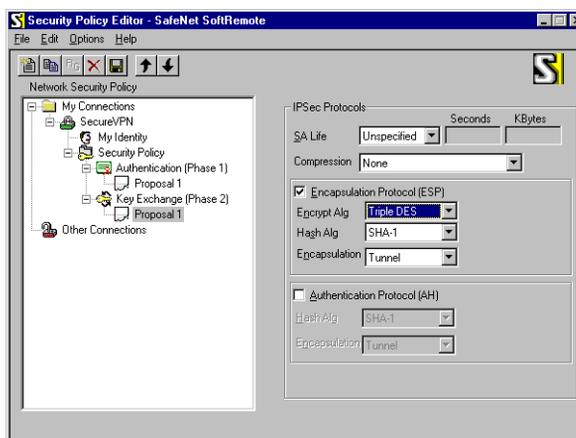
11. Specify the Authentication settings. Select **Security Policy -> Authentication (Phase 1) -> Proposal 1**.

Figure 4-18.
SoftRemote:
Authentication (Phase 1)
 -> **Proposal 1** fields



- a. In **Authentication Method** field, specify the method appropriate for your configuration. (For example, use **Pre-Shared Key** if using only password-based authentication, use **Pre-Shared Key: Extended Authentication** if using password-based authentication and extended authentication.)
 - b. In **Encryption and Data Integrity/Algorithms** fields:
 - ◆ **Encrypt Alg:** Select DES or **Triple-DES** (highest security).
 - ◆ **Hash Alg:** Select MD5 or **SHA-1** (highest security).
 - ◆ **SA Life:** Set this to **3500 seconds**, if you have not changed the default setting on the firewall. The number should be set to some period of time slightly shorter than is configured on the firewall SA definition (Advanced tab on the Sidewinder G₂ Admin Console). The Phase 1 Lifetime on the SoftRemote should NOT be left as Unspecified.
 - c. In **Key Group** field, select at least **Group 2**. (Group 5 is highest.)
12. Specify the Key Exchange settings. Select **Key Exchange (Phase 2)** -> **Proposal 1**.

Figure 4-19.
SoftRemote: Key
Exchange (Phase 2) ->
Proposal 1 fields



- ◆ **SA Life:** Select **Unspecified** to default to the firewall settings.
- ◆ **Compression should not be used.** Leave the default as None.
- ◆ **Encapsulation Protocol:** Select the **same settings** in the Encryption and Hash Algorithms fields as Phase I. **Do not change Tunnel Encapsulation.**
- ◆ **Do not use the Authentication Protocol (AH).** (Traffic will not be encrypted.)

13. Click the **Save** icon to save the policy on this system.

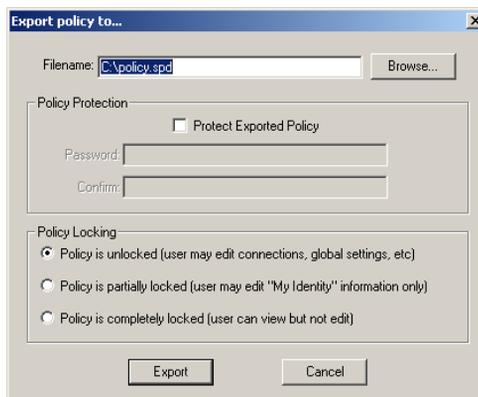


Important: You can export a policy without saving it, but the policy will not be saved and enforced on the system on which it was configured.

14. Select **File -> Export**.

The **Export policy to...** window appears.

Figure 4-20. Export
policy window



15. Specify the export settings.

- ◆ **Filename:** Specify the location of the exported file.
- ◆ **Protect Exported Policy:** Select to password protect the policy. The policy will be encrypted
- ◆ **Policy Locking:** Select one of the following settings:
 - **Policy is unlocked:** Select to allow the user to edit the policy.
 - **Policy is partially locked:** Select to allow the user to edit the **My Identity** information only.
 - **Policy is completely locked:** Select to allow the user to view the policy only.

Note: It is advisable to save an unlocked copy for administrator use. A non-protected policy may be imported over a protected policy, which allows you to begin editing again.

16. Provide a copy of this file to the appropriate end users.

The second part of this section describes how to configure the default connection, or the **Other Connections** portion, of the security policy. This connection is the last listed connection and handles any traffic that does not match an earlier connection.

Note: If *Other Connections* is a secured connection, the settings you configure must coincide with configured settings/capabilities on the Sidewinder G₂ VPN Gateway.

- ◆ This option includes a default connection configuration, called "Other Connections," that controls traffic not covered by prior connection rules.

Configuring other connections

1. Click on **Other Connections**.
2. Specify the connection type. In the **Connection Security** section, specify the setting that best fulfills your business need.
 - ◆ If you select Secure, configure this connection using the same steps as for the other secure connections. You do not need to specify the remote party identity (this field will not be available in the interface), as all packets not processed by another policy will be processed by this one.

A reciprocal VPN tunnel policy on sidewinder will need to identify protected networks as 1.0.0.0/0.
 - ◆ If you select Non-Secure, all traffic not that does not match earlier connection rules will be sent in clear text. Change the Internet Interface settings if the traffic should leave using a specific interface.
 - ◆ If you select the Block, all traffic not processed by another

connection will be blocked.

3. Click **Save**.

Setting up a Secure All Connections policy

In this connection option, one policy governs all traffic leaving the client machine.

1. Select **Start -> Programs -> SoftRemote -> Security Policy Editor** (or right click the SafeNet icon and select Security Policy Editor).
2. Select **Options-> Secure-> All Connections**.
3. Configure the security policy the way you would for a Specified Connection, starting with step 7 on page 4-27 (Enable the **Connect using Secure Gateway Tunnel** box) and continuing through step 16 on page 4-33.
 - ◆ The Remote Party Identity and address fields will not be available as all addresses are inherently included in this type of network.
 - ◆ The reciprocal policy in Sidewinder must identify the protected network as 1.0.0.0/0 to include all traffic.

Note: This is a 'All Connections' type policy, and therefore the Non-Secure and Block connection types are **not** available.



Important: When using Virtual Adapter and an 'All Connections' type policy, you may not have traffic enabled to 'All Connections'. To resolve this use the procedure provided in "All Connections policy and Virtual Adapter setting" on page A-7.

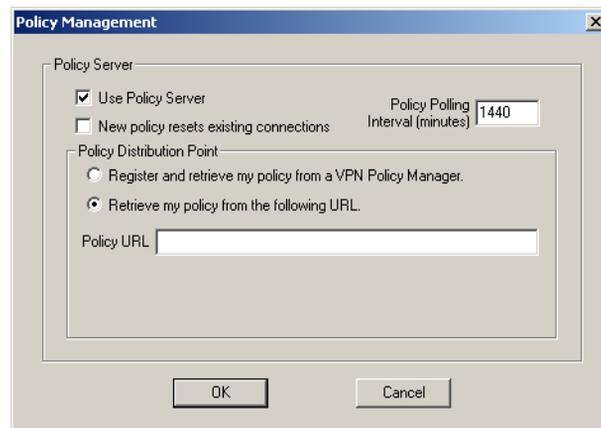
Policy update distribution

SoftRemote can be configured to periodically poll, or check for, and then retrieve a new security policy from a web address, or URL. The clients have several retrieval options which are configured using the **Policy Management** window in the **Secure Policy Editor**. Use the following procedure to configure policy updating options on the client.

1. Select **Start -> Programs -> SoftRemote -> Security Policy Editor** (or right click the **SoftRemote** icon and select **Security Policy Editor**).
2. Select **Options-> Policy Management**.

The **Policy Management** window displays.

Figure 4-21. Policy Management window



3. Select the **Policy Server** options as follows.
 - ◆ **Use Policy Server:** Select to set the options for policy distribution. When not selected, all of the options are grayed out.
 - ◆ **New policy resets existing connections:** Select to have SoftRemote reset all active connections when it retrieves a new policy. By default this box is clear, which means that SoftRemote does not drop all existing connections when it retrieves a new policy.
 - ◆ **Policy Polling Interval (minutes):** Enter how often SoftRemote polls and retrieves new policy. The minutes available are from **1** through **9999999**. The default is **1440** minutes (**24** hours).
 - ◆ **Retrieve my policy from the following URL:** Select this option to enter the web address of the security policy. When selected the **Policy URL:** text box appears, enter the URL here.
4. Click **OK**.

VPN management command

The VPN management command is a console application that provides command line support for the corresponding control functions in SoftRemote. The functions supported include: connect, disconnect, activate, deactivate, and reload. This allows you the use of batch files for these functions. You can create a batch file with the desired command in the SoftRemote install directory. You would then place a short cut to the file on your desktop to allow you to quickly execute the function.

The command format is:

```
VPN -activate
    -deactivate
    -connect connection_name
    -disconnect connection_name
```

where: *connection_name* is the name of your VPN connection.

Note: After you activate an 'All Connections' type policy, you must send traffic through the VPN to trigger SoftRemote to establish the configured connection. To do this, you might include a ping command to an internal address (behind the gateway).

APPENDIX A

Tips and Troubleshooting

About this appendix

This appendix provides a summary of troubleshooting techniques available for resolving SoftRemote and Sidewinder G₂ VPN connection problems. This appendix addresses the following topics:

- ◆ “SoftRemote Log Viewer” on page App-2
- ◆ “SoftRemote Connection Monitor” on page App-3
- ◆ “Common deployment issues” on page App-5
- ◆ “Upgrade tips” on page App-5
- ◆ “Connectivity troubleshooting” on page App-6
- ◆ “Sidewinder G2 troubleshooting commands” on page App-8
- ◆ “Working with Microsoft Networking” on page App-8
- ◆ “ZoneAlarm troubleshooting resources” on page App-11

SoftRemote Log Viewer

The Log Viewer displays the communications log, a diagnostic tool that lists the IKE negotiations that occur during the VPN set up negotiation. This is a very useful debugging tool when you cannot correctly establish a VPN connection.

There are times when a message may not show up in the log viewer. If you suspect that log entries are getting dropped, set the viewer to log to a file then read the file. To log to a file, open the policy editor select **Options -> Global Policy Settings** and select **Enable IPSec Logging**. The logging will be saved in the SoftRemote (SoftRemoteLT) install directory in the *isakmp.log* file.

Note: The Log Viewer shows only ISAKMP and IKE messages; it does not show audit messages for all traffic flow through the VPN.

To start the Log Viewer, click the Start menu or right-click the SoftRemote icon and then select the viewer from the displayed menu.

Figure A-1. Log Viewer window on SoftRemote



Important: This information is not saved. The Log Viewer content wraps after about 50 lines. Therefore, unless you freeze and save or print this information, it will be cleared by ongoing negotiations.

The following summarizes the tasks you can perform.

Button	Summary
Clear	Clears the communications log.  Important: You cannot retrieve this information once you clear it.
Freeze	Freezes/unfreezes the communications log. Because the communications log scrolls through IKE negotiations as they occur, you may need to freeze the log in order to save or print specific messages. Since this button acts as a toggle, once activated it will read UnFreeze until you click it again to restart the log.
Print	Print the current content in the communications log.  Tip: You may want to freeze the log before you attempt to print it.

More...

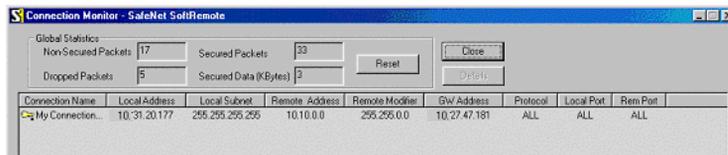
Button	Summary
Save	Save the current content in the communications log.  Tip: You may want to freeze the log before you attempt to save it.
Close	Closes the log viewer.

SoftRemote Connection Monitor

The Connection Monitor displays statistical and diagnostic information for each active connection in the security policy. This utility is designed to display the actual security policy settings configured in Security Policy Editor and the security association (SA) information established during Phase 1 IKE negotiations and Phase 2 IPsec negotiations.

To start the Connection Monitor, click the **Start** menu or right-click the SoftRemote icon and then select the Connection Monitor from the displayed menu.

Figure A-2. Connection Monitor window



You will see an icon to the left of the connection name:

- ◆ A **key** icon indicates that the connection has a Phase 2 IPsec SA. When there is a single Phase 1 SA to a gateway that is protecting multiple Phase 2 SAs, there will be a single Phase 1 connection with the SA icon and individual Phase 2 connections with the key icon listed above that entry.
- ◆ An **SA** icon indicates that the connection has only a Phase 1 IKE security association. This occurs when in the process of connecting to a secure gateway tunnel or when a Phase 2 IPsec SA fails to establish or has not been established yet.
- ◆ A **black mark** moving beneath the key icon indicates that the client is processing secure IP traffic for that connection.

More about the Connection Monitor

Global Statistics are not real-time operations; they are updated every five seconds.

Dropped Packets includes packets from connections that are configured as blocked.

Remote Modifier is either the remote party subnet mask or the end of the address range when IP Address Range is selected for the Remote Party Identity and Addressing ID Type.

To view the details

To see the details about a connection, click **Details**. The Security Association Details window appears as shown below.

Figure A-3. Connection Monitor Details window

The screenshot shows a window titled "Security Association Details" with a "Phase 2" tab selected. The window contains several fields for configuration and status:

Phase 2		Lifetime			
		Inbound	Outbound		
Enc Alg	3DES	Lcl Address	172.20.160.68	Expires at	11:11:36 5/12/03
Hash Alg	SHA-1	Rem Address	0.0.0.0	Data Secured	27484 b
SPI (inb)	6b34ef10	Encapsulation	TUNNEL	Data Remaining	Not in use
SPI (outb)	f280f8f2				Not in use

A "Close" button is located at the bottom right of the window.

You will see a Phase 1 tab and/or a Phase 2 tab; these tabs indicate that the selected connection has established SAs.

- ◆ To view Authentication (Phase 1) security associations negotiated by IKE, click the Phase 1 tab.
- ◆ To view Key Exchange (Phase 2) security associations negotiated by IPsec, click the Phase 2 tab.

Note: Certain fields are not populated in the Connection Monitor at this time. The unpopulated fields are targets for enhancements in future releases.

Common deployment issues

Listed here are some basic configuration issues you may encounter while preparing your SoftRemote deployment:

- ◆ If remotely administrating Sidewinder G₂ and you are using self-signed certificates, first ftp the proper **pk1* and **pem* files to the firewall. Then run the PKCS12 utility. Once completed, ftp the new **p12* file back to your remote console.
- ◆ When using self-signed certificates, make sure that the PKCS12 object file (**p12*), the corresponding personal certificate file (**pem*), and the corresponding firewall certificate file are imported into their proper tabs in SoftRemote's Certificate Manager. See "Setting up Sidewinder G2 self-signed certificates" on page 4-18 for details.
- ◆ When using CA certificates exported from the firewall and SoftRemote's auto-import feature during installation, do the following:
 - a. Request and retrieve the CA root certificate using the firewall.
 - b. Export the CA root certificate with a **.pem* file extension.
 - c. Import the file into the initial installation of the SoftRemote Certificate Manager, and then export the same file. This process changes the file format and extension to *.cser*, which allows you to rename the CA root certificate file *CACert.cser*.
 - d. Move the *CACert.cser* to your install image. The file will now automatically import during the installation process.

Upgrade tips

- ◆ Before upgrading, you must deactivate the client and then reboot. Once you finish the reboot, then uninstall the client. Reboot again, then install. Reboot one more time before you begin to use the client.

If the VA was used and you did not execute a clean reboot before uninstall, you may encounter problems from an incomplete VA uninstall. Call Secure Computing Support for assistance.
- ◆ The Original Windows installation media may be required during installation depending upon OS and configuration. Please have the CD or files ready prior to installation.
- ◆ If using self-signed certificates, when upgrading from Soft-PK to SoftRemote, your self-signed certificates need to be set explicitly as trusted CAs (not required on SoftPK). Immediately after

Connectivity troubleshooting

completing the upgrade, re-import the client certificates as CAs using the Certificate Manager and make sure they are set as trusted.

- ◆ If the settings in the Virtual Adapter are not updated per new installation, go to **Start -> Settings -> Network and Dial-up Connections** highlight and delete the SafeNet VA adapter entry. The entry will be re-installed with default settings when the next VA enabled connection is set up.

Check basic setup details if traffic is not being sent.

- ◆ Make sure you are using a non-encrypting modem.
- ◆ Make sure you are using a SafeNet SoftRemote supported NIC (Ethernet, ISDN, etc). See SafeNet's Web site at <http://www.ire.com/clientsupport/SafeNetClientNIClist.htm> for an updated list.
- ◆ Make sure the VPN servers and security associations on the firewall and the security policies on SoftRemote are enabled.
- ◆ Make sure that the client's virtual address is not configured to an address on the firewall's internal network.
- ◆ If you turned off ZoneAlarm and cannot start your VPN connection, check SoftRemote's **Security Policy Editor -> Options -> Firewall Settings**, and verify that "VPN connections require the firewall to be enabled" is unchecked.
- ◆ If you did not disable the Microsoft XP Internet Connective Firewall, you may experience some compatibility issues. Workarounds include:
 - Turn off the Native XP Firewall before installing SoftRemote and ZoneAlarm. If you will be using ZoneAlarm, do not turn the XP Firewall back on.
 - If you want to use the XP firewall, configure the XP firewall to allow two-way IKE traffic on port 500 UDP on the adapter used for your VPN traffic. Doing so allows rekeys initiated by a peer (the firewall). See the SafeNet SoftRemote Release Notes for instructions. (To access the release notes online, go to http://www.securedbysafenet.com/release_notes/SoftRemote/CS_Release_Bulletin_SoftRemote_10.0b4.htm)
- ◆ If you chose to leave the XP Internet Connective Firewall enabled

and are using the VA, you must ensure that both the SafeNet Virtual Adapter and the physical adapter are protected by the firewall. If one adapter is “firewalled” and the other is not, packets will not pass.

- ◆ If the Log Monitor indicates a Phase 1 Identity error, verify that all identity information (distinguished names and IP addresses) is entered correctly:
 - On SoftRemote **Security Policy Editor** -> *connection name* -> **Secure Gateway Tunnel** -> **ID Type**
 - On SoftRemote **Security Policy Editor** -> **My Identity**
 - On the Sidewinder G₂ Admin Console **Certificate Manager** -> *all tabs used in the security association*
- ◆ If the Log Monitor indicates a Phase 2 error, verify that the target networks are correctly configured on both Sidewinder G₂ and SoftRemote.
- ◆ If using digital certificates with keys of length 2048 bits or longer, you must have Internet Explorer Version 5.5 or better installed on the client machine.

All Connections policy and Virtual Adapter setting

When using an ‘All Connections’ type policy (forcing all external traffic through a tunnel to one gateway), and you are using the VA, then you may have to make a manual adjustment to the policy you distribute. The VA comes up without a **use default gateway** option activated when it should be activated. To correct this, it is best to force the setting in the policy (using the following procedure) and not involve the end user in the problem resolution.

1. Configure your policy and export it without locking or password protecting it.
2. Open the policy file with a text editor.
3. Locate the following line:


```
[HKEY_LOCAL_MACHINE\SOFTWARE\IRE\SafeNet\Soft-PK\ACL\0\MYID\VASUPPORT]
"VASUPPORT"=dword:00000002
```
4. Add the following line:


```
"VAUSEGW"=dword:00000002
```
5. The result should be as follows:

Sidewinder G₂ troubleshooting commands

```
[HKEY_LOCAL_MACHINE\SOFTWARE\IRE\SafeNet\Soft-PK\ACL\0\MYID\VASUPPORT]
"VASUPPORT"=dword:00000002
"VAUSEGW"=dword:00000002
```

6. Save the file then re-import it to the client.

Any client that you import this configuration file into will then have the **use default gateway** VA option set.

In addition to standard logging, the firewall performs auditing of certain system events which allows you to generate information on VPN connections. Table A-1 shows some useful commands to track VPN connections in real-time mode and check VPN settings/configuration.

Table A-1. Basic Sidewinder G₂ VPN troubleshooting commands

Commands
<p>tcpdump -npi ext_interface port 500 or proto 50</p> <p>To show IKE and IPSEC traffic arriving at the firewall.</p>
<p>cf ipsec q</p> <p>To review VPN policies on the firewall command line.</p>
<p>cf ipsec policydump</p> <p>To determine if VPN is active.</p>
<p>showaudit -v</p> <p>To show detailed audit trace information for VPN.</p>

Working with Microsoft Networking

Most end users will want to use SoftRemote to establish VPN connections to access internal Microsoft networks (NT servers, Exchange, etc.) and Web servers. DNS and WINS information must be correctly configured to work seamlessly in this environment.

The SoftRemote client supports receiving the DNS and WINS server information from Sidewinder G₂ to the client during the VPN connection initialization. To consistently and reliably communicate this information, enable the Virtual Adapter on the client. In the client configuration, set the Virtual Adapter option to “Required” in the My Identity screen on the client. The Virtual Adapter will start before the VPN initialization and will bind the DNS and WINS information sent to the client from Sidewinder G₂ for the duration of the VPN connection. A Virtual Adapter initialization failure results in an aborted VPN

initialization that usually self-corrects on the second try.

Note: *Windows 9x and NT are capable of receiving DNS information with the Virtual Adapter. However, the Windows 2000 Professional and both XP platforms require the Virtual Adapter. The Virtual Adapter is required for storage of WINS information on all platforms.*

If you are experiencing difficulties setting up WINS and DNS configuration information for your VPN connections, try some of the following options:



Tip: *Start by verifying that your WINS, DNS, and all other IP address settings are correct on both the client and the firewall.*

- ◆ If the client machine wants to connect to a WINS or DNS server, then the servers' IP addresses should be configured on the firewall in a client address pool, or manually configured in Network Properties on the client machine. Sidewinder G₂ cannot send DNS or WINS information if it is not sending a virtual IP address in a Client Address Pool.
- ◆ If the client machine is configured to accept WINS and DNS information but the information is not available on the machine, check these options:
 - Verify that the Client Address Pool settings used in the corresponding Sidewinder G₂ Security Association are correct. Change the appropriate settings, then restart your VPN client and try again.
 - Verify that the client's Virtual Adapter option is set to "Required."
- ◆ If the WINS information is correct, but the client is unable to authenticate to the primary domain controller (PDC), you may be experiencing one of several issues. For example:
 - If the VPN terminates in a protected burb with general traffic, the client may not be authenticating properly to the PDC. Connect the client machine to the local area network (LAN), start it, and verify the login. Disconnect it from the LAN and retry the VPN connection. The PDC should now respond correctly when connecting through a VPN connection.
 - If the VPN terminates in a virtual burb or burb separated from general traffic, your rules and proxies may be improperly configured. Watch the audit stream for netprobes or rules denies to help troubleshoot the problem source. You may

need to add or change entries to permit the traffic to flow through the firewall.

- ◆ If an end user wants to alternate between working on a LAN and over a VPN, then the user may need to establish a new connection with the local network after disconnecting from the VPN. The most reliable way to initialize into an MS network is to log out and then log into the network.
- ◆ If the client machine is Windows 9x or NT, has dial-up DNS, and is using mode config (to receive DNS information from a client address pool), the DNS values will not revert to the default when the VPN is disconnected. Provide users with instructions to reconnect to their ISP after disconnecting from the VPN to return to the original DNS values.
- ◆ If the client machine is Windows 2000 Professional, mode-config will not correctly set the DNS server identity on the client unless the Virtual Adapter Required option is set.
- ◆ If you want to allow Windows 2000 Professional systems to map drives in an NT domain, the Virtual Adapter must be configured manually to allow 'Client for MS Networking.' Also set 'Print and File Sharing for MS Networks.'

Note: Consult your Microsoft documentation for instructions.

- ◆ Ensure that you have "Virtual Private Networking" and "Dial Up Networking" installed. If they are not installed, do so at this time.

Note: Consult your Microsoft documentation for instructions.

ZoneAlarm troubleshooting resources

If ZoneAlarm is not passing traffic, check basic configuration details.

- ◆ Make sure the traffic or programs are allowed access to the Internet by using the Control Center Programs interface or checking "Remember this answer the next time I use this program" at the pop up window.
- ◆ Make sure ZoneAlarm is set to unlocked when you are planning on passing traffic.
- ◆ Make sure that you have your security settings (Low, Medium, High) at the proper level for your network environment.
- ◆ Make sure that your protected network is listed as a part of your local network by checking ZoneAlarm's Advanced tab.
- ◆ Change what traffic or programs are allowed or denied at any time by returning to the Control Center.



Tip: Enable the MailSafe protection feature available on the Security panel to quarantine e-mail script attachments.

For help with ZoneAlarm, use the following resources:

- ◆ Use the ZoneAlarm online help files
- ◆ Go to **Start -> Programs -> Zone Labs -> Readme.txt** for a list of known issues and helpful information
- ◆ Go to **<http://www.zonealarm.com/support>**

Troubleshooting

Part Number: 86-0935037-D

Software Version: SoftRemote 10.0 and Sidewinder G₂ 6.0

Product names used within are trademarks of their respective owners.

Copyright © 2003 Secure Computing Corporation. All rights reserved.