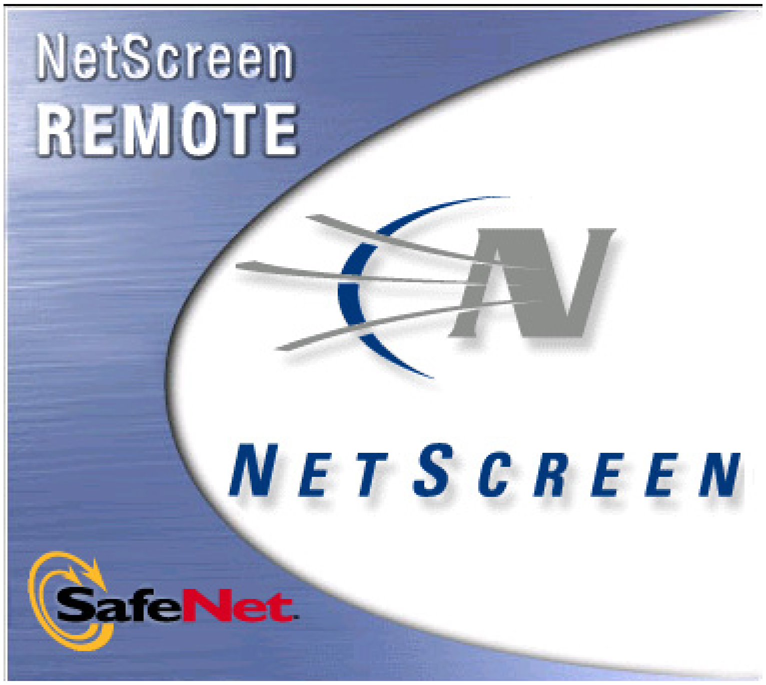
NETSCREEN-REMOTE VPN CLIENT ADMINISTRATOR'S GUIDE



Version 8.0 P/N 093-0267-000 Rev. A

Licenses, Copyrights, and Trademarks

THE SPECIFICATIONS REGARDING THE NETSCREEN PRODUCTS IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR USE AND APPLICATION OF ANY NETSCREEN PRODUCTS. NO PART OF THIS DOCUMENTATION MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT RECEIVING WRITTEN PERMISSION FROM NETSCREEN TECHNOLOGIES, INC.

NETSCREEN-REMOTE 8.0 LICENSE AGREEMENT

PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THIS PRODUCT. BY INSTALLING AND OPERATING NETSCREEN-REMOTE 8.0 ACCOMPANYING THIS AGREEMENT, YOU INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS AGREEMENT, ARE CONSENTING TO BE BOUND BY ITS TERMS, AND ARE BECOMING A PARTY TO THIS AGREEMENT. THIS AGREEMENT IS A VALID AND BINDING OBLIGATION ON YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS.

This is a license, not a sales agreement, between you, as an End User or as the Administrator (each as defined below), and NetScreen Technologies, Inc. ("NetScreen"), as the owner and provider of "NetScreen-Remote 8.0." NetScreen-Remote 8.0 consists of NetScreen proprietary software and third party software licensed or sublicensed, to you, as part of a single product, for use within a single network. "Administrator" means the individual or group within the purchasing organization that is responsible for managing network security access, including setting security policies, configuring NetScreen-Remote 8.0, and allowing End Users to download NetScreen-Remote 8.0 or otherwise installing NetScreen-Remote 8.0 on End User equipment. "End User" means your employees, contractors, and consultants performing services for you in connection with your network, authorized by the Administrator to install and use NetScreen-Remote 8.0 on a single computer subject to the terms and conditions of this license.

Any and all documentation and all software releases, corrections, updates, and enhancements that are or may be provided to you by NetScreen shall be considered part of NetScreen-Remote 8.0 and be subject to the terms of this Agreement.

1. License Grant. Subject to the terms of this Agreement, NetScreen grants you a limited, non-transferable, non-exclusive, revocable, license and right to:

a. Install and use, on a single computer for use by the Administrator, one (1) copy of NetScreen-Remote 8.0 to manage security policies for up to 10, 100, 1000 or more End Users, as indicated on the license certificate(s) provided to you by NetScreen; and

b. Download and install a single copy of NetScreen-Remote 8.0 on each of 10, 100, 200, 500, 1000 or more End User computers as indicated on the license certificate(s) provided to you by NetScreen.

Licenses that authorize use of NetScreen-Remote 8.0 with a greater number of End Users are available as upgrades and may be purchased from NetScreen as required by you. You must purchase all license upgrades separately. You shall ensure that End Users agree to be bound by the terms and conditions of this Agreement.

2. Use Within a Single System and Network. The foregoing license and rights are granted only to you for use by your Administrator and End Users. NetScreen-Remote 8.0 must be used in the manner set forth in the applicable documentation. NetScreen-Remote 8.0 is considered "in use" when its software is loaded into permanent or temporary memory (i.e. RAM). The Administrator may make one (1) copy of NetScreen-Remote 8.0 for backup and recovery purposes. Other than the rights explicitly granted herein, no right to copy, distribute, or sell, and no other right to install and use NetScreen-Remote 8.0, or any component thereof, is granted to you.

3. Limitation on Use.You are only licensing the rights set forth above to NetScreen-Remote 8.0. Except only as specifically described above, you may not engage in activity designed (or otherwise attempt), and if you are a corporation will use your best efforts to prevent your employees and contractors from engaging in activity designed (or otherwise attempting): (a) to modify, translate, reverse engineer, decompile, disassemble, create derivative works of, or distribute NetScreen-Remote 8.0 (or any component thereof) and the accompanying documentation; (b) to distribute, sell, transfer, sublicense, rent, or lease any rights in NetScreen-Remote 8.0 (or any component thereof) or accompanying documentation in any form to any person; or (c) to remove any proprietary notice, product identification, copyright notices, other notices or proprietary restrictions, labels, or trademarks on NetScreen-Remote 8.0, documentation, and containers. NetScreen-Remote 8.0 is not designed or intended for use in online control of aircraft, air traffic, aircraft navigation or aircraft communications; or in the development, design, construction, operation or maintenance of nuclear, chemical, or biological weapons of mass destruction or any nuclear facility. You warrant that you will not use or redistribute NetScreen-Remote 8.0 (or any component thereof) for such purposes.

4. Proprietary Rights. All rights, title and interest in and to, and all intellectual property rights, including copyrights, in and to NetScreen-Remote 8.0 and documentation, remain with NetScreen. You acknowledge that no title or interest in and to the intellectual property associated with or included in NetScreen-Remote 8.0 and NetScreen products is transferred to you and you will not acquire any rights to NetScreen-Remote 8.0 except for the license as specifically set forth herein.

5. Term and Termination. The term of the license is for the duration of NetScreen's copyright in NetScreen-Remote 8.0. NetScreen may terminate this Agreement immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will either destroy all copies of the documentation or return all materials to NetScreen. The provisions of this Agreement, other than the license granted in Section 1 ("License Grant") shall survive termination.

6. Limited Warranty. The sole warranty provided under this Agreement and with respect to the NetScreen-Remote 8.0 is set forth in NetScreen's Remote Warranty. THE NETSCREEN REMOTE WARRANTY CONTAINS IMPORTANT LIMITS ON YOUR WARRANTY RIGHTS. THE WARRANTIES AND LIABILITIES SET FORTH IN THE REMOTE WARRANTY ARE EXCLUSIVE AND ESTABLISH NETSCREEN'S ONLY OBLIGATIONS AND YOUR SOLE RIGHTS WITH RESPECT TO NETSCREEN-REMOTE 8.0 AND THIS AGREEMENT. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

7. Limitation of Liability. Your exclusive remedy for any claim in connection with NetScreen-Remote 8.0 and the entire liability of NetScreen are set forth in the NetScreen Remote Warranty. Except to the extent provided in the Remote Warranty, if any, IN NO EVENT WILL NETSCREEN OR ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR ANY LOSS OF USE, INTERRUPTION OF BUSINESS, LOST PROFITS OR LOST DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF NETSCREEN OR ITS AFFILIATE OR SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND WHETHER OR NOT ANY REMEDY PROVIDED SHOULD FAIL OF ITS ESSENTIAL PURPOSE. THE TOTAL CUMULATIVE LIABILITY TO YOU, FROM ALL CAUSES OF ACTION AND ALL THEORIES OF LIABILITY, WILL BE LIMITED TO AND WILL NOT EXCEED THE PURCHASE PRICE OF NETSCREEN-REMOTE 8.0 PAID BY YOU. YOU ACKNOWLEDGE THAT THE AMOUNT PAID FOR NETSCREEN-REMOTE 8.0 REFLECTS THIS ALLOCATION OF RISK.

8. Export Law Assurance. You understand that NetScreen-Remote 8.0 is subject to export control laws and regulations. YOU MAY NOT DOWNLOAD OR OTHERWISE EXPORT OR RE-EXPORT NETSCREEN-REMOTE 8.0 OR ANY UNDERLYING INFORMATION OR TECHNOLOGY, EVEN IF TO DO SO WOULD BE ALLOWED UNDER THIS AGREEMENT, EXCEPT IN STRICT COMPLIANCE WITH ALL UNITED STATES AND OTHER APPLICABLE LAWS AND REGULATIONS. Specifically, you agree that you are responsible for obtaining licenses to export, re-export, or import NetScreen-Remote 8.0. NetScreen-Remote 8.0 may not be downloaded, or NetScreen-Remote 8.0 otherwise exported or re-exported (i) into, or to a national or resident of, Cuba, Iraq, Iran, North Korea, Libya, Sudan, Syria, or any country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's lists of Specially Designated Nationals, Specially Designated Terrorists, or Specially Designated Narcotic Traffickers, or otherwise on the U.S. Commerce Department's Table of Denial Orders.

9. U.S. Government Restricted Rights. NetScreen-Remote 8.0 is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (OCT 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227-14(ALT III), as applicable.

10. Tax Liability. You agree to be responsible for the payment of any sales or use taxes imposed at any time whatsoever on this transaction.

11. General. If any provisions of this Agreement are held invalid, the remainder shall continue in full force and effect. The laws of the State of California, excluding the application of its conflicts of law rules shall govern this Agreement. The United Nations Convention on the Contracts for the International Sale of Goods will not govern this Agreement. This Agreement is the entire agreement between the parties as to the subject matter hereof and supersedes any other agreements, advertisements, or understandings with respect to NetScreen-Remote 8.0 and documentation. This Agreement may not be modified or altered, except by written amendment, which expressly refers to this Agreement and which, is duly executed by both parties.

You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.

THE SPECIFICATIONS REGARDING THE NETSCREEN PRODUCTS IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. ADMINISTRATORS AND END USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR USE AND APPLICATION OF ANY NETSCREEN PRODUCTS. NO PART OF THIS DOCUMENTATION MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT RECEIVING WRITTEN PERMISSION FROM NETSCREEN.

Copyright Notice

Trademarks

NetScreen Technologies, Inc, the NetScreen logo, NetScreen-Remote 8.0, NetScreen-Remote 8.0 Express, NetScreen-Remote, GigaScreen ASIC, and ScreenOS are trademarks and NetScreen is a registered trademark of NetScreen Technologies, Inc.

NETSCREEN-REMOTE 8.0 WARRANTY

Software Warranty. NetScreen Technologies, Inc. ("NetScreen") warrants that for a period of ninety (90) days from either software installation or sixty (60) days following shipment, whichever occurs first (the "Start Date"), the media on which the NetScreen software purchased by Customer ("Software") will be free from defects in materials and workmanship under normal use consistent with the instructions contained in the enclosed documentation. This limited warranty extends only to the original purchaser. Customer's sole and exclusive remedy and the entire liability of NetScreen, its suppliers and affiliates, under this warranty is, at NetScreen's option, either (i) to replace the media on which the Software is furnished with new media containing the Software; or (ii) to correct the reported defect through updates and fixes made generally available at www.netscreen.com/support. NetScreen makes no other warranty with respect to the Software, and specifically disclaims any warranty that the Software is error free or that Customer will be able to operate the Software without problems or interruptions.

Warranty Claims. For a period of ninety (90) days from the Start Date, NetScreen may provide Customers upgrades and fixes for the Software at www.netscreen.com/support. Customers may also send emails to support@netscreen.com to obtain technical support for a period of one (1) year from the Start Date.

Return Procedures. Customer must notify NetScreen of any defect in the Software within the warranty period and provide proper documentation and verification of defect. Customers should include Software product serial number in every service request. Within ten (10) business days of the date of notification, NetScreen will provide Customer with a Return Material Authorization ("RMA") number and the location to which Customer must return, at its cost, the defective Software. Customer is responsible for proper packaging of Software returned to NetScreen, including description of the failure, shipment to NetScreen's designated location, and return of Software within ten (10) days after issuance of the RMA number. In no event will NetScreen accept any returned Software that does not have a valid RMA number. Customer's failure to return Software within thirty (30) days of its receipt of an RMA may result in cancellation of the RMA. NetScreen does not accept responsibility for any Software lost in transit and recommends that the return be insured for the full value. NetScreen will use all reasonable efforts within five (5) days of receipt of defective Software to repair or replace such Software or refund Customer's purchase price. If a warranty claim is invalid for any reason, Customer will be charged at NetScreen's then-current rates for all services performed and expenses incurred by NetScreen.

Restrictions. No warranty will apply if the Software (i) has been altered, except by NetScreen; (ii) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by NetScreen; or (iii) has been subjected to abnormal physical, thermal or electrical stress, misuse, negligence, or accident. In addition, the Software is not designed or intended for use in (i) the design, construction, operation or maintenance of any nuclear facility, (ii) navigating or operating aircraft; or (iii) operating life-support or life-critical medical equipment, and NetScreen disclaims any express or implied warranty of fitness for such uses. NetScreen shall not be responsible for Customer's or any third party's software, firmware, information, or memory data contained in, sorted on, or integrated with any Software returned to NetScreen, whether under warranty or not. Customer is responsible for backing up its programs and data to protect against loss or corruption.

Disclaimer. EXCEPT AS EXPRESSLY SET FORTH ABOVE, NETSCREEN MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. FURTHER, NETSCREEN DOES NOT WARRANT THAT THE SOFTWARE IS ERROR FREE OR THAT BUYER WILL BE ABLE TO OPERATE THE SOFTWARE WITHOUT PROBLEMS OR INTERRUPTION.

Limitation of Liability. IN NO EVENT WILL NETSCREEN OR ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR ANY LOSS OF USE, INTERRUPTION OF BUSINESS, LOST PROFITS, OR LOST DATA, OR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OF ANY KIND REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF NETSCREEN OR ITS AFFILIATE OR SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND WHETHER OR NOT ANY REMEDY PROVIDED SHOULD FAIL OF ITS ESSENTIAL PURPOSE. THE TOTAL CUMULATIVE LIABILITY TO CUSTOMER, FROM ALL CAUSES OF ACTION AND ALL THEORIES OF LIABILITY, WILL BE LIMITED TO AND WILL NOT EXCEED THE PURCHASE PRICE OF THE SOFTWARE PAID BY CUSTOMER.

Contents

Preface

This manual provides network administrators with a guide to creating remote-access virtual private networks (VPNs) using NetScreen-Remote™ software. In it, you will learn installation, configuration, and deployment strategies.

What is NetScreen-Remote?

When NetScreen-Remote operates on any IP network, such as the Internet, it can create a VPN tunnel between an end user and a NetScreen security appliance. NetScreen-Remote software is a full-featured product ready for advanced IPSec communications that secures traffic sent from a desktop or laptop computer across a public or private TCP/IP network. It also intergrates with Microsoft (MS) Native L2TP protocols, and is compatible with most Certificate Authorities and MS CryptoAPI (MSCAPI) applications.

WHO SHOULD READ THIS GUIDE?

Any system administrator who has to design secure remote-access architecture using the NetScreen-Remote client, distribute the NetScreen-Remote software to a user base, and provide post-installation user support should read this guide. NetScreen-Remote is intended for use with NetScreen security appliances and systems. However, it will interoperate with other IPSec and L2TP-compliant devices.

ADMINISTRATOR DECISIONS

There are several things you must decide before configuring the NetScreen-Remote. The answers to these questions will determine your remote-access architecture, authentication, and deployment schemes.

Which end-user connection mechanisms will you use—fixed or dynamically assigned IP addresses? You will most likely be using **fixed IP addresses** in these cases:

- DSL user with fixed IP
- cable user with fixed IP
- one or two person office with fixed IP

You will most likely be using **dynamically assigned IP addresses** in these cases:

- cable or DSL with PPPoE or DHCP assignment of IP addresses
- traveling user using a dial-up connection
- Ethernet or wireless with DHCP

Will you require certificates, pre-shared key (AutoKey), or manual key for IPSec tunnel setup and authentication?

- **Certificates** are the most secure. The administrator can either obtain the certificate from a CA and send it to the user, or users can request their own certificate. (See Chapter 3.) Certificates can be loaded onto smart cards and these smart cards can distributed to the users.

  Will you acquire the certificate for the user, then distribute it to the user? Or will you instruct your end-users to generate and send certificate requests to the CA, then load the certificates themselves after receiving these from the CA?

  You can request the certificate using an on-line request process (certificate enrollment process or CEP). Or you can manually cut and paste the request to the CA (using PKCS 10 format).

- **Pre-shared key** is easier and faster to set up, but less secure, as the certificate’s initial key does not change. Also, if you revoke a user’s VPN access, you must change the pre-shared key. (See Chapter 5.)
- **Manual key**, used for testing, is another option. Because the keys are fixed and never change, if they are broken, they must be manually reassigned. This would mean a lot of re-configuration and is much less secure. (See Chapter 4.)

After you have made these decisions, configure a few NetScreen-Remote clients and NetScreen devices and try out the setup. When you are satisfied with the results, you are ready for deployment. (See Chapters 8 and 9.)

For more information, see Chapter 4 of the NetScreen Concepts and Examples ScreenOS Reference Guide, which describes these sample scenarios for using NetScreen-Remote.

Deactivating NetScreen-Remote

For easy transition between travel, home, and office use, one click is all it takes to deactivate or activate NetScreen-Remote. Right-click the NetScreen-Remote icon in the taskbar, and select Deactivate/Activate Security Policy from the pop-up menu. (The command toggles.)

Note: *You may wish to disable NetScreen-Remote whenever connected behind a NetScreen device or other VPN gateway.*

Using this Guide

Chapter 1, “Installation,” describes the prerequisites and installation procedure for NetScreen-Remote.

Chapter 2, “Interface” provides an overview of the layout, icons, and menus that appear in the interface.

Chapter 3, “Digital Certificates” explains how to obtain and manage certificates and certificate revocation lists (CRLs).

Chapter 4, “Configuring a VPN Tunnel with Pre-Shared Key” explains how to set up a VPN tunnel using a Pre-Shared Key with AutoKey Internet Key Exchange (IKE).

Chapter 5, “Configuring a VPN Tunnel with Digital Certificates” explains how to set up a VPN tunnel using digital certificates with AutoKey Internet Key Exchange (IKE).

Chapter 6, “Configuring a Manual Key VPN Tunnel” explains how to set up a VPN tunnel using Manual Keys.

Chapter 7, “Sample Scenarios” provides several typical scenarios for using NetScreen-Remote: from a hotel while on a business trip, from a home office, and in the corporate office (with the security feature deactivated).

Chapter 8,“Large Scale Distribution with NetScreen-Global PRO” describes the procedure for deploying large numbers of Security Clients in conjunction with NetScreen Global-PRO, using NetScreen-Remote Login.

Chapter 9,“Large Scale Distribution (Standalone Procedure)” describes the procedure to deploy Security Clients on a large scale in a stand-alone environment.

Appendix A,“Configuring a L2TP/IPSec” explains how to configure the L2TP VPN connection through your Microsoft Dial-Up Networking and how connect to the connection.

Appendix B, “Deploying NetScreen-Remote with Smart Cards” describes how to set up your smart card to interoperate with NetScreen-Remote and a NetScreen-Gateway.

Related Publications

The following are related publications:

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 4: VPNs

NetScreen Command Line Interface Reference Guide

Terminology

This manual uses Microsoft® Windows® terminology and concepts that are specific to the Internet. If you are unfamiliar with this terminology, please see your Microsoft Windows installation manual and the Help files that accompany your Web browser.

For More Information

For more information, see the HTML cover page that appears after you insert the NetScreen-Remote CD-ROM. The cover page contains a link to the release notes for NetScreen-Remote. If you have any questions regarding NetScreen-Remote, refer to the section, “Getting Help,” in the release notes or contact NetScreen Technical Support. NetScreen Technical support is available to registered users of NetScreen-Remote. You can contact them by one of the following ways:

- Web site: http:// support.netscreen.com
- E-mail: support@netscreen.com
- Fax: 1 (408) 730-6100
- Voice: 1-800-638-8296

Installation 1

The information contained in this chapter is repeated in the accompanying *NetScreen-Remote User's Installation Guide*. You can copy the *NetScreen-Remote User's Installation Guide* and distribute it to your end users with the NetScreen-Remote software.

If you plan to distribute many NetScreen-Remote clients, see Chapter 8, "Large Scale Distribution with NetScreen-Global PRO" or Chapter 9, "Large Scale Distribution (Standalone Procedure)" , for strategies and procedures that will help your deployment.

Silent installation assists in the mass deployment of the software to desktops. NetScreen-Remote installation should be able to be recorded by issuing the command setup -r. This should create an installation script that can be included with the install to create a silent install. The silent install is played back by issuing the command setup -s.

This chapter covers the following information:

- System Prerequisites
- Updating from Previous Versions
- Installation
- Modifying Installation

SYSTEM PREREQUISITES

Install the NetScreen-Remote client in the following environment:

PC-compatible Computer	• Pentium processor or its equivalent
Operating System	• Microsoft® Windows® 95 (build 950B and 950C only) or • Microsoft Windows 98 (98 and 98SE) or • Microsoft Windows 2000 Professional or • Windows NT® 4.0 (with Service Pack 4 or greater) or • Windows ME or • Windows XP® Professional or Home Edition
Minimum RAM	• 16 MB RAM for Windows 95 • 32 MB RAM for Windows 98 or Windows NT 4.0 • 64 MB RAM for Windows 2000 or Windows XP
Available Hard Disk Space	• Minimum 5 MB, Maximum 35 MB
Software Installation	• CD-ROM drive, network drive or web site
Communications Protocol	• IPSec and IKE L2TP with Windows 2000 (*Optional*) • Native Microsoft TCP/IP
Dial-up Connections	• Modem, internal or external (includes analog, DSL, and cable modems connecting to your PC via serial or USB port) • Native Microsoft Dial-up Networking • PPPoE drivers • Compatible with America Online® (AOL) 6.0 or greater

Network Connections	• Ethernet • Wireless Ethernet (802.11a/b)
Help-file Viewing	• Microsoft Internet Explorer® 4.0 or greater

Note: *NetScreen-Remote is not compatible with other VPN software. Uninstall the VPN software prior to using NetScreen-Remote.*

UPDATING FROM PREVIOUS VERSIONS

If you are upgrading to NetScreen-Remote from a previous version, *you must first uninstall the previous version*. If you do not need to uninstall a previous version, skip to “Installation” on page 1-6.

⚠ **Warning** *Failure to uninstall the previous version will cause system conflicts resulting in failure of your Windows operating system.*

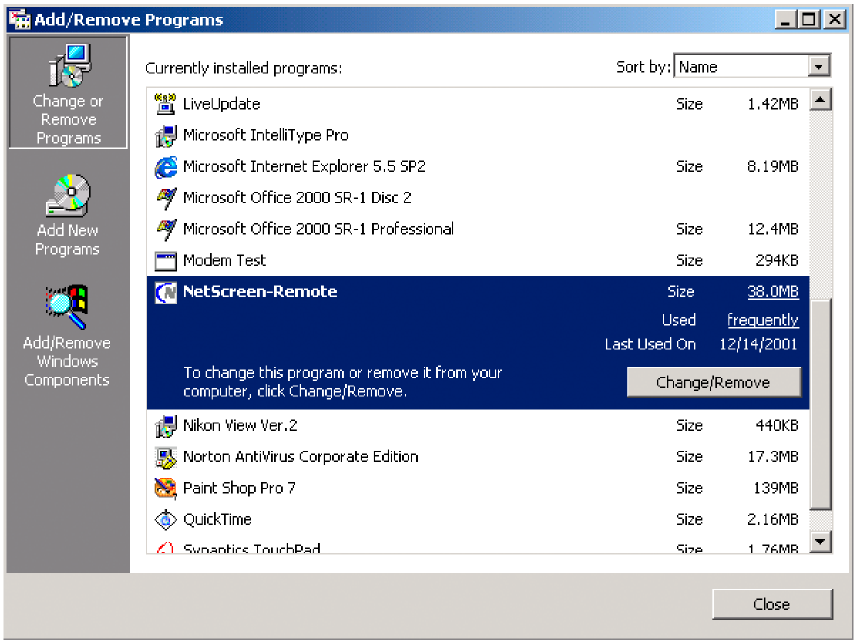
To uninstall a previous version of NetScreen-Remote:

1. Click **Start** on the Windows task bar, click **Settings**, and then click **Control Panel**.

   The Control Panel opens.

2. Double-click **Add/Remove Programs**.

   A list of installed programs appears.



Currently installed programs: Sort by: Name

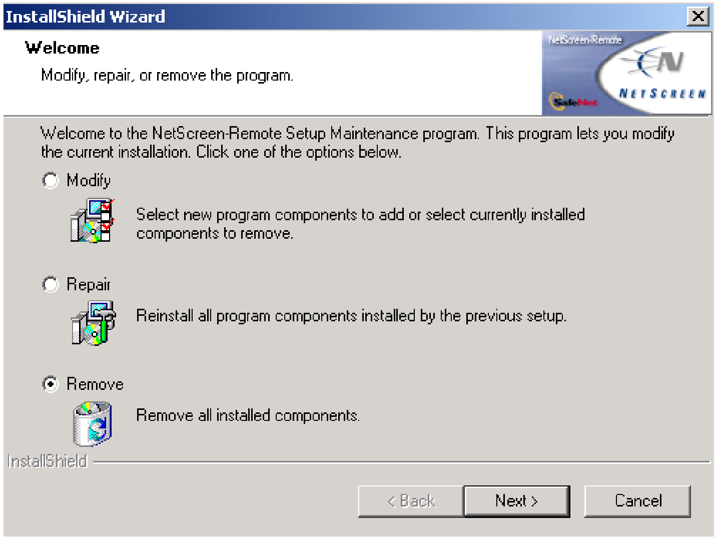
LiveUpdate	Size	1.42MB
Microsoft IntelliType Pro		
Microsoft Internet Explorer 5.5 SP2	Size	8.19MB
Microsoft Office 2000 SR-1 Disc 2		
Microsoft Office 2000 SR-1 Professional	Size	12.4MB
Modem Test	Size	294KB
NetScreen-Remote	Size	38.0MB
	Used	frequently
	Last Used On	12/14/2001
Nikon View Ver.2	Size	440KB
Norton AntiVirus Corporate Edition	Size	17.3MB
Paint Shop Pro 7	Size	139MB
QuickTime	Size	2.16MB
Synaptics TouchPad	Size	1.76MB

To change this program or remove it from your computer, click Change/Remove.

Figure 1-1 List of Installed Programs

3. From the list, select **NetScreen-Remote**.
4. Click **Change/Remove**.

   The following dialog box appears.



InstallShield Wizard

Welcome

Modify, repair, or remove the program.

Welcome to the NetScreen-Remote Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

○ Modify

Select new program components to add or select currently installed components to remove.

○ Repair

Reinstall all program components installed by the previous setup.

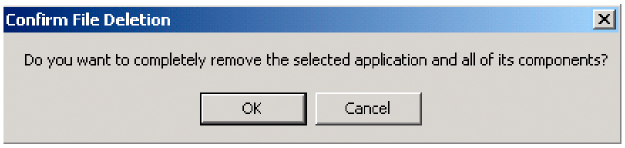
● Remove

Remove all installed components.

Figure 1-2 Modify, Repair, or Remove the Program

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

   You are asked if you want to completely remove the selected application and all of its components.



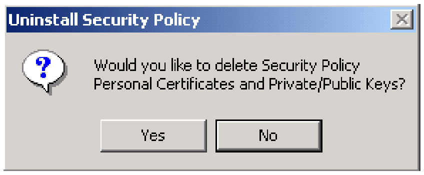
Confirm File Deletion

Do you want to completely remove the selected application and all of its components?

Figure 1-3 Deletion Confirmation Message

6. Click **OK** to confirm the deletion.

   The following alert box appears:



Uninstall Security Policy

Would you like to delete Security Policy Personal Certificates and Private/Public Keys?

Figure 1-4 Delete Security Policy Alert Box

This alert box gives you the opportunity to save your existing security policy. The items that you save are installed automatically during the new installation of NetScreen-Remote.

Note: *VPN connections are dependent on security policies, certificates, and keys. Once deleted, these may not be retrieved.*

7. Click **No** to keep your existing security policy.

   A progress box appears.

8. Click **OK** to acknowledge the successful uninstall.
9. Restart your computer.

INSTALLATION

Ensure that you have uninstalled any earlier version of NetScreen-Remote, as described in the previous section.

You can install NetScreen-Remote from a CD-ROM, a network drive share, or a website.

Starting Installation

Start your installation using one of the following three install methods and then proceed to the section “Continuing with Installation” on page 1-8:

—To install NetScreen-Remote from a CD-ROM:

1. With Microsoft Windows running and all other programs closed, insert the NetScreen-Remote CD into the CD-ROM drive.
2. Right-click **D:\**. (The D designates your CD-ROM drive, which could be designated differently depending on your computer’s setup.)

The following menu appears:

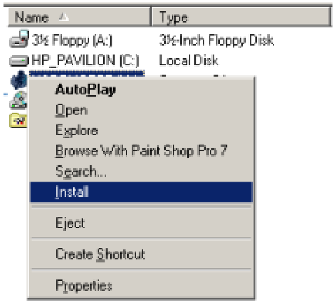


Figure 1-5 Select Install

3. Select **Install** from the menu to install NetScreen-Remote.
4. Go to the next section "Continuing with Installation."

—To install NetScreen-Remote from a network drive share:

1. Map to the network drive.
2. Locate the NetScreen-Remote files.
3. Double-click **setup.exe** to run the NetScreen-Remote setup application.
4. Go to the next section, "Continuing with Installation."

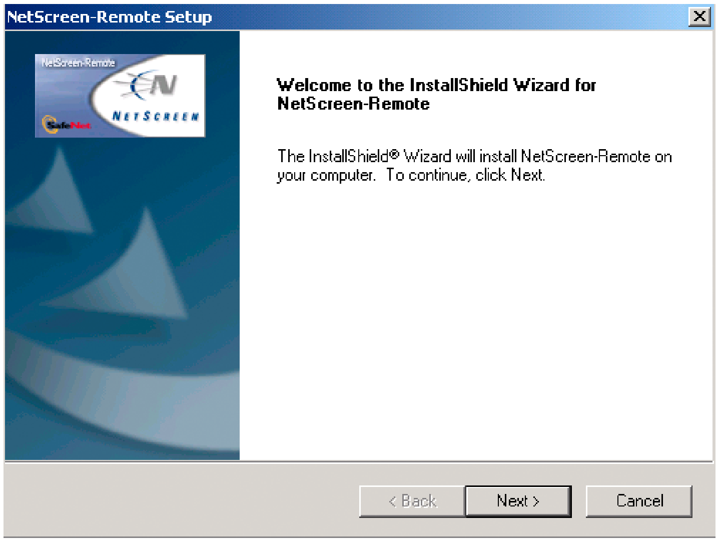
—To install NetScreen-Remote from a website:

1. Locate the NetScreen-Remote files on the website.
2. Select to download the **setup.exe** file and download the file.
3. After the file downloads, unzip the file to **C:\temp**.
4. Double-click **setup.exe** to run the NetScreen-Remote setup application.
5. Go to the next section, "Continuing with Installation."

Continuing with Installation

The NetScreen-Remote setup application starts on your system:

1. The InstallShield Wizard starts, as shown in Figure 1-6. Click **Next**.



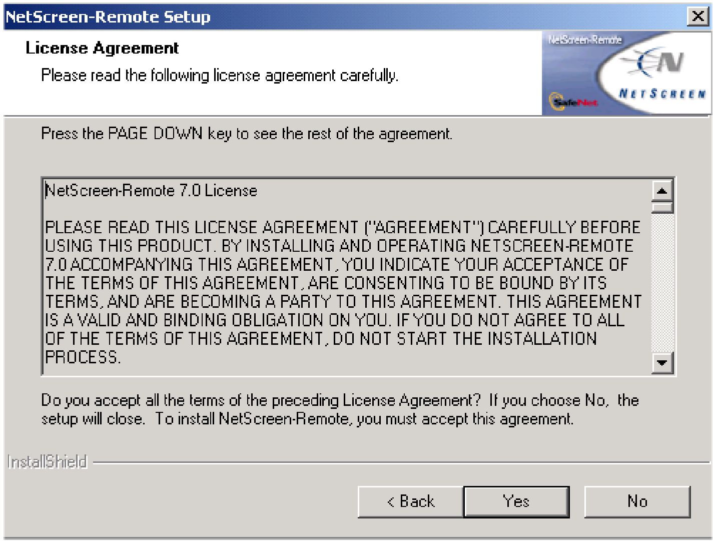
NetScreen-Remote Setup

Welcome to the InstallShield Wizard for NetScreen-Remote

The InstallShield® Wizard will install NetScreen-Remote on your computer. To continue, click Next.

Figure 1-6 NetScreen-Remote Installation Welcome Screen

The Software License Agreement appears.



NetScreen-Remote Setup

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

NetScreen-Remote 7.0 License

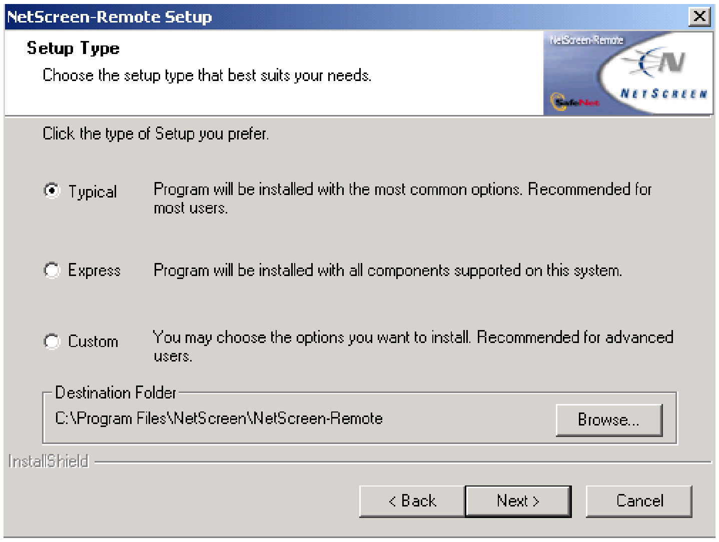
PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THIS PRODUCT. BY INSTALLING AND OPERATING NETSCREEN-REMOTE 7.0 ACCOMPANYING THIS AGREEMENT, YOU INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS AGREEMENT, ARE CONSENTING TO BE BOUND BY ITS TERMS, AND ARE BECOMING A PARTY TO THIS AGREEMENT. THIS AGREEMENT IS A VALID AND BINDING OBLIGATION ON YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS.

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install NetScreen-Remote, you must accept this agreement.

Figure 1-7 License Agreement

2. After reading the license agreement, click **Yes** to continue.

   The **Setup Type** dialog box appears.



NetScreen-Remote Setup

Setup Type

Choose the setup type that best suits your needs.

Click the type of Setup you prefer.

● Typical — Program will be installed with the most common options. Recommended for most users.

○ Express — Program will be installed with all components supported on this system.

○ Custom — You may choose the options you want to install. Recommended for advanced users.

Destination Folder

C:\Program Files\NetScreen\NetScreen-Remote

Figure 1-8 Installation Setup Type

3. Select one of these options:

   Typical —Recommended for most users; installs all VPN Client components.

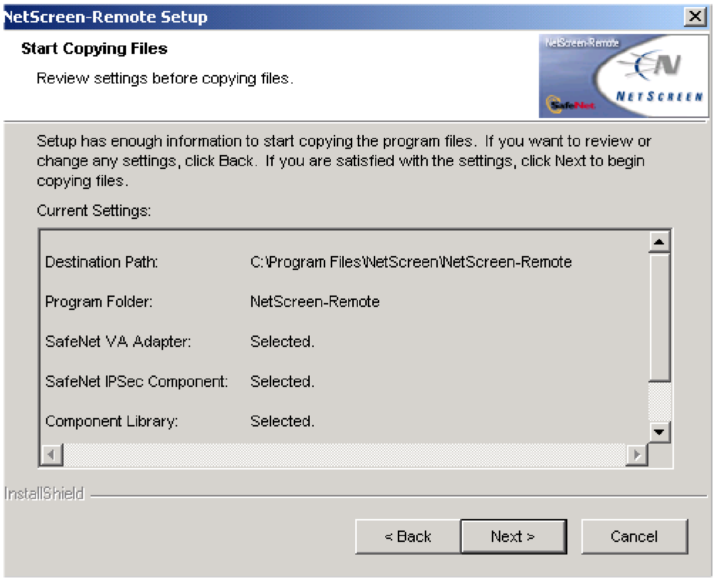
   Express —Installs only the components that the system supports.

   Custom —Enables you to select the components to install individually.

4. To install NetScreen-Remote in the default destination folder (C:\Program Files\NetScreen\NetScreen-Remote), click **Next**.

   To specify another destination folder, click **Browse**. In the **Choose Folder** dialog box, select the folder of your choice, and click **OK**. Then click **Next**.

5. Verify your selections in the window that appears (Figure 1-9), and then click **Next**.



NetScreen-Remote Setup

Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

Destination Path: C:\Program Files\NetScreen\NetScreen-Remote

Program Folder: NetScreen-Remote

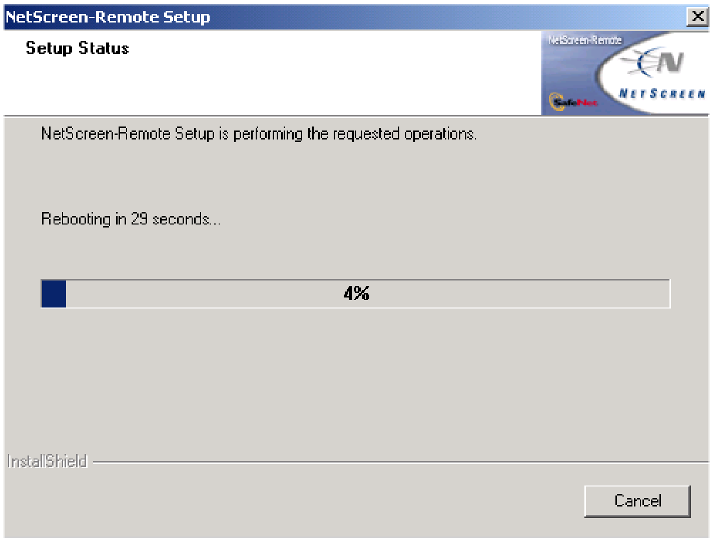
SafeNet VA Adapter: Selected.

SafeNet IPSec Component: Selected.

Component Library: Selected.

Figure 1-9 Start Copying Files

The NetScreen-Remote files are copied to the program folder that you specified. After all the files are copied, the following window appears:



Setup Status

NetScreen-Remote Setup is performing the requested operations.

Rebooting in 29 seconds...

4%

InstallShield

Figure 1-10 Device Reboot

Your computer automatically reboots after a successful installation. If you wish to abort the reboot process, click **cancel** before device timeout. If you log on to your computer with a password, you will need to re-enter it at the standard Windows login prompt.

After a successful installation, the NetScreen-Remote icon appears in the status area in the right corner of the Windows taskbar, as shown below.

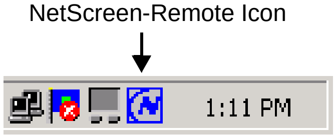


Figure 1-11 NetScreen-Remote icon on the Windows Taskbar

If you see the disabled NetScreen-Remote icon ☒ instead of the enabled NetScreen-Remote icon shown in Figure 1-11, review the system requirements in “System Prerequisites” on page 1-2 and ensure the system requirements for NetScreen-Remote are met. If the system requirements are met, follow the procedure in “Modifying Installation” on page 1-12 and select the **Repair** option to reinstall all program components during the initial setup and installation.

Modifying Installation

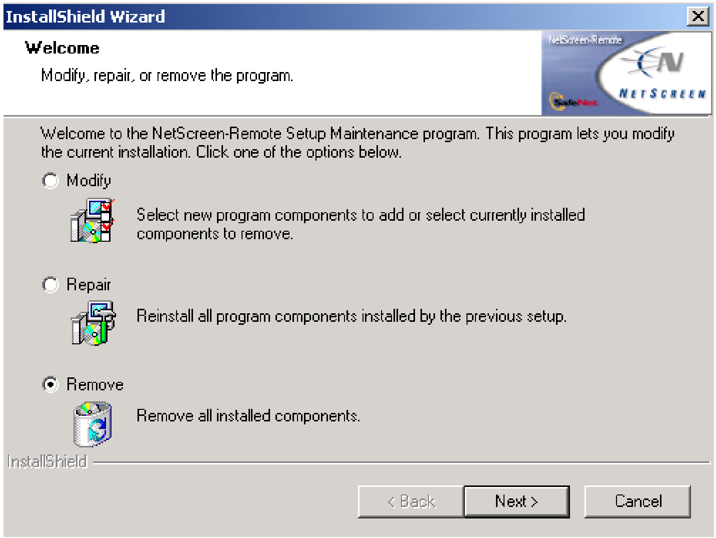
After the initial installation, you can add a new program component (modify the software) or reinstall all program components installed by the previous setup (repair the software). To do so:

1. Disable any virus-protection software that may be running on your computer.
2. On the Windows taskbar, click the **Start** button, click **Settings**, and then click **Control Panel**.

   The **Control Panel** opens.
3. Double-click **Add/Remove Programs**.

   The **Add/Remove Programs Properties** dialog box appears with a list of installed programs.
4. From the list, select **NetScreen-Remote**.
5. Click **Change/Remove**.

   The following **Welcome** dialog box appears.



Welcome

Modify, repair, or remove the program.

Welcome to the NetScreen-Remote Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

○ Modify

Select new program components to add or select currently installed components to remove.

○ Repair

Reinstall all program components installed by the previous setup.

● Remove

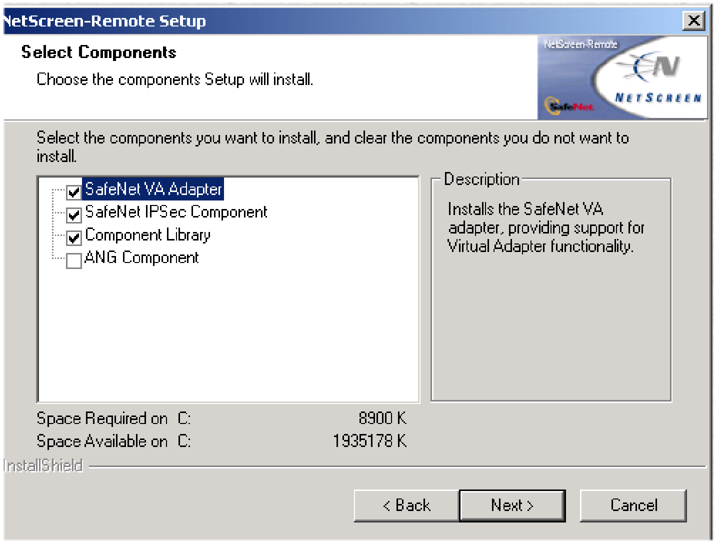
Remove all installed components.

Figure 1-12 Modify, Repair, or Remove the Program

6. To add or remove the Virtual Adapter, IPSec Client or another component, select **Modify**, and then click **Next**.

   If you want to reinstall the software, skip to Step 8.

The **Select Components** dialog box appears.



NetScreen-Remote Setup

Select Components

Choose the components Setup will install.

Select the components you want to install, and clear the components you do not want to install.

- ☑ SafeNet VA Adapter
- ☑ SafeNet IPSec Component
- ☑ Component Library
- □ ANG Component

Description

Installs the SafeNet VA adapter, providing support for Virtual Adapter functionality.

Space Required on C: 8900 K

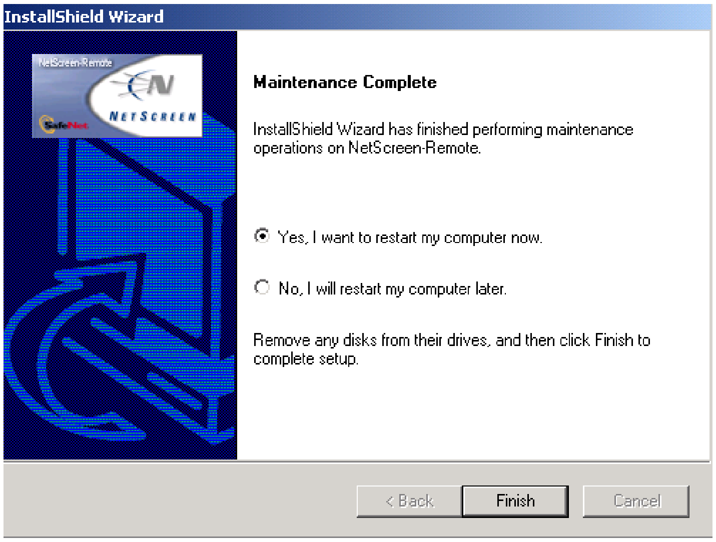
Space Available on C: 1935178 K

Figure 1-13 Select Components

7. Select the component to be installed, and then click **Next**. The installation procedure begins.
8. To reinstall the software, select **Repair**, and then click **Next**.

   The re-installation procedure begins.

   After either the installation or re-installation is complete, the **Maintenance Complete** dialog box appears.



Maintenance Complete

InstallShield Wizard has finished performing maintenance operations on NetScreen-Remote.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Figure 1-14 Maintenance Complete

9. Click **Yes, I want to restart my computer now**, and then click **Finish** to restart your computer immediately.

Interface 2

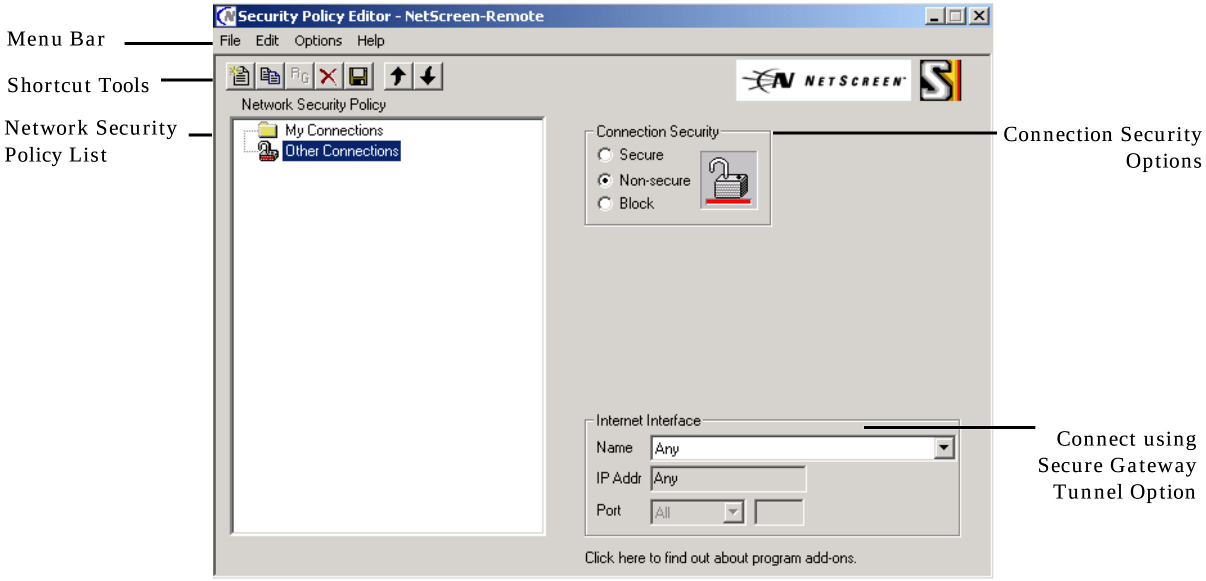
This chapter provides an overview of the layout, icons, and menus that appear in NetScreen-Remote.

NetScreen-Remote consists of these modules:

- Security Policy Editor: manually create connections and security policies
- Certificate Manager: manage and verify certificates
- NetScreen-Remote Login: authenticates user and downloads security policies.

Security Policy Editor

The Security Policy Editor, shown in Figure 2-1, is the software module within the NetScreen-Remote client where you manually create connections and security policies.



○ Secure
● Non-secure
○ Block

Name: Any
IP Addr: Any
Port: All

Click here to find out about program add-ons.

Figure 2-1 Security Policy Editor

The menu bar displays the four main menus of the Security Policy Editor. For a description of each menu, see “Menus” on page 2-4.

The shortcut toolbar contains tools for common commands. For a brief description of each icon on the toolbar, see “Shortcut Toolbar Icons” on page 2-9.

The Network Security Policy list displays a hierarchically ordered list of connections and their associated proposals. My Connections define the connection(s) that you create. The last connection in the list is Other Connections that tells NetScreen-Remote what to do with all connections not specifically defined. Connections are read in a top-down order similar to firewall rules.

The three Connection Security options refer to the type of security to apply to a connection:

Secure: 🔒 This option secures communication for the connection. (It is the equivalent of “tunnel” on other NetScreen products.)

Non-secure: 🔓 This option allows communication for the connection to pass through unsecured. (It is the equivalent of “permit” on other NetScreen products.)

Block: STOP This option does not allow any communication for the connection to pass through. (It is the equivalent of “deny” on other NetScreen products.)

Menus

The four main menus of the Security Policy Editor are:

- File
- Edit
- Options
- Help

The fifth main menu is the Taskbar icon (located on the taskbar). Its commands apply to both the Security Policy Editor and the Certificate Manager. For a description of its contents, see "Shortcut Menu" on page 2-22.

File Menu

The File menu contains commands for managing security policies and connections, saving any changes, and exiting from the Security Policy Editor.

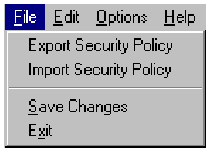


Figure 2-2 File Menu

Export Security Policy exports a security policy from NetScreen-Remote to the location you specify.

Import Security Policy imports a security policy to NetScreen-Remote.

Save Changes saves any changes that you made to your security policy.

Exit closes the Security Policy Editor after prompting you to save changes.

Edit Menu

The Edit menu contains commands for relocating connections or redundant gateways in the Network Security Policy list.

A *redundant gateway* is an alternate gateway to access your network that will establish a connection with the client if the primary gateway is busy, off-line, or unavailable. You can add up to 10 alternates for each secure connection. The first connection will always serve as the primary.

All redundant gateways must be configured with the same security policy information as the primary, except for the IP address, domain name, distinguished name, or pre-shared key (which must be unique to each device). Redundant gateways are used in the order in which they are listed in the top-down order.

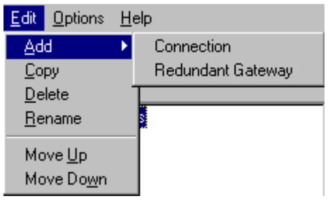


Figure 2-3 Edit Menu

Add adds a new connection or a new redundant gateway with the NetScreen-Remote default settings to the Network Security Policy list.

Copy copies a connection or redundant gateway from the Network Security Policy list.

Delete deletes a connection or redundant gateway from the Network Security Policy list.

You can disable all redundant gateways for a secure connection without deleting them. To do so, select the secure connection, and deselect the Connect using Secure Gateway Tunnel option. Then choose Save Changes from the File menu.

Move Up relocates a selected connection or redundant gateway one place higher in the Network Security Policy list.

Move Down relocates a selected connection or redundant gateway one place lower in the Network Security Policy list.

Options Menu

The commands in the Options menu affect elements of NetScreen-Remote in an overarching way.

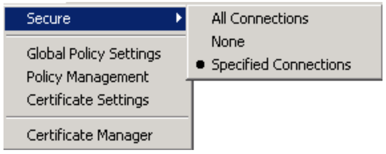


Figure 2-4 Options Menu

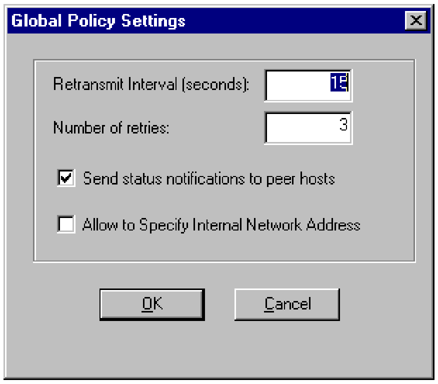
Secure specifies which connections are secure:

– All Connections: disables regular Internet while VPN is up.

– None: disables all VPN connections. Only regular traffic can pass.

– Specified Connections: allows VPN and regular to pass simultaneously.

Global Policy Settings opens the Global Policy Settings dialog box, in which you can set program preferences that affect all transmissions using NetScreen-Remote.


Global Policy Settings

Retransmit Interval (seconds): 15

Number of retries: 3

☑ Send status notifications to peer hosts

□ Allow to Specify Internal Network Address

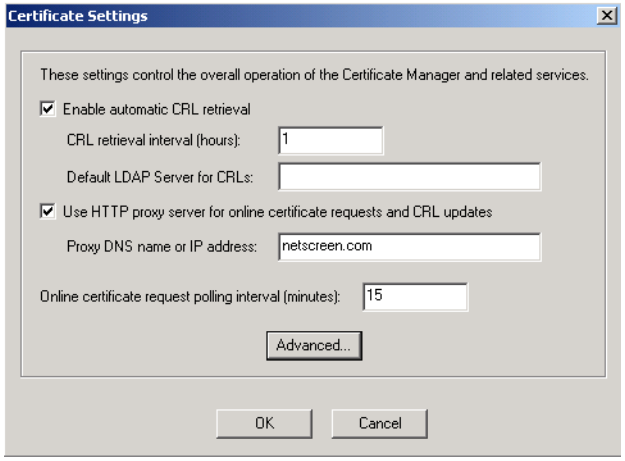
Figure 2-5 Global Policy Settings

You can select the following Global Policy settings:

- Retransmit Interval: the interval between no response and retry connection.
- Number of retries: the number of retries before failure or use of redundant gateway.
- Send status notifications to peer hosts: number of status equals the sent keepalive messages to keep VPN u
- Allow to Specify Internal Network Address: allows you to specify an IP address for the VPN traffic without using L2TP or XAuth.

Policy Management presents options used only in conjunction with the SafeNet/VPN Policy Manager, which contains detailed instructions on configuring these options.

Certificate Settings opens the Certificate Settings dialog box.



These settings control the overall operation of the Certificate Manager and related services.

☑ Enable automatic CRL retrieval

CRL retrieval interval (hours): 1

Default LDAP Server for CRLs:

☑ Use HTTP proxy server for online certificate requests and CRL updates

Proxy DNS name or IP address: netscreen.com

Online certificate request polling interval (minutes): 15

Figure 2-6 Certificate Settings

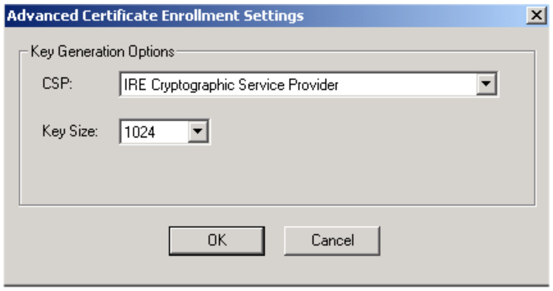
You can select the following Certificate Manager features:

- Enable the automatic retrieval of certificate revocation lists (CRLs) and specify the retrieval frequency (in hours) and the default LDAP server.
- Enable and specify an HTTP proxy server for on-line certificate requests using Certificate Enrollment Protocol (CEP) and CRL updates when connecting from a secure network to a certificate authority (CA) on the Internet.

Some networks have been designed to allow HTTP connections to exit from their private network by first being translated through an HTTP proxy. Select this option only if you use an HTTP proxy to make connections outside your private network and your CA is located outside your private network.

- Specify how often NetScreen-Remote checks (“polls”) for a response to a certificate request.

Advanced opens the Advanced Certificate Enrollment Settings dialog box:



CSP: IRE Cryptographic Service Provider

Key Size: 1024

CSP opens a drop-down menu with selections for a Cryptographic Service Provider (CSP):

IRE Cryptographic Service Provider;

Microsoft Base Cryptographic Provider v1.0;

Microsoft Enhanced Cryptographic Provider v1.0;

Microsoft Strong Cryptographic Provider; or

Schlumberger Cryptographic Service Provider. Use with Schlumberger smart cards.

DataKey CSP. Use with smart cards using DataKey drivers.

Key Size opens a drop-down menu with selections for a default key size: 512, 1024 or 2048. The default key size is 1024.

Certificate Manager opens the Certificate Manager, the module that allows you to manage personal certificates.

Help Menu

The Help menu offers access to the NetScreen-Remote Help files.

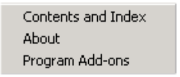


Figure 2-7 Help Menu

Contents and Index opens the Help files.

About displays the Security Policy Database Editor version and copyright information.

Program Add-Ons opens a browser window to SafeNet, Inc.

Shortcut Toolbar Icons

The tools in the shortcut toolbar carry out common commands in the Security Policy Editor.

Table 2-1 Shortcut Toolbar Icons

📄	**Add a New Connection:** creates a new connection.
📋	**Copy Selected Item:** copies a connection or a redundant gateway or a proposal.
RG	**RG:** adds a new redundant gateway.
✕	**Delete:** deletes a connection or a redundant gateway or a proposal.
💾	**Save:** saves the current Security Policy.
↑	**Move Up:** moves a selected connection or a redundant gateway or a proposal up one place on the Security Policy list.
↓	**Move Down:** moves a selected connection or a redundant gateway or a proposal down one place on the Security Policy list.

Certificate Manager

The Certificate Manager is the software module within NetScreen-Remote that allows you to request, import, store, view, verify, delete, and export personal certificates that you receive from certificate authorities (CAs).

> ***Note:*** On Windows 98+ to XP, certificates may also be loaded by double-clicking on the certificate itself or using your web browser. Certificate Manager need not be used on these systems unless you wish to verify a certificate.

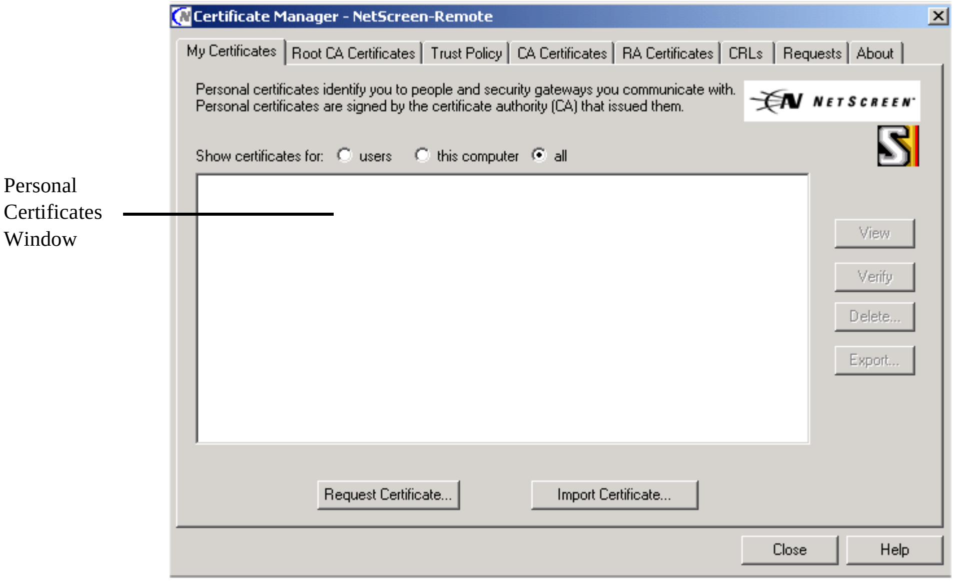
The Certificate Manager is organized into these six sections or pages:

- My Certificates
- CA Certificates
- RA Certificates
- CRLs
- Certificate Requests
- About

Click the tab for a specific page to access it.

My Certificates Page

The My Certificates page provides tools for managing personal certificates. A personal certificate verifies the identity of the individual using NetScreen-Remote.



Personal certificates identify you to people and security gateways you communicate with. Personal certificates are signed by the certificate authority (CA) that issued them.

Show certificates for: ○ users ○ this computer ● all

Figure 2-8 My Certificates Page

After highlighting a certificate in the personal certificates window, you can click the following buttons to perform the associated tasks:

> **View** opens the selected certificate for viewing. To close the certificate, click anywhere within the certificate displayed.
>
> **Verify** checks the validity status of the selected certificate.
>
> **Delete** removes the selected certificate from NetScreen-Remote.
>
> **Export** copies the selected certificate to a directory of your choice in a PKCS12 format.

Use the Request Certificate and Import Certificate buttons to obtain and induct new personal certificates into NetScreen-Remote:

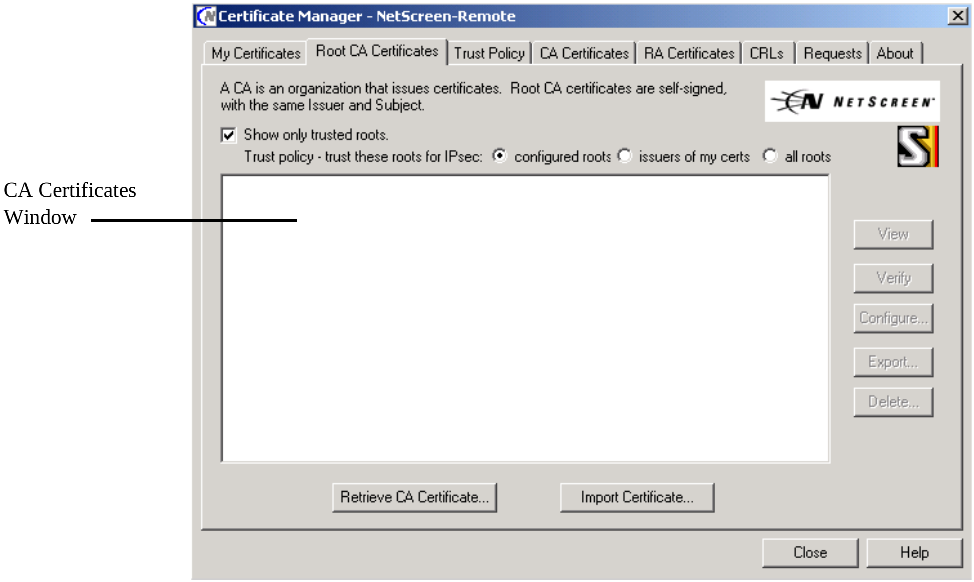
> **Request Certificate** provides a choice of dialog boxes for generating a PKCS10 request. You can use either the CEP, if you already have a CA certificate that supports CEP, or the cut-and-paste method, which is to cut and paste the Cert_Request into your CA certificate.

Import Certificate opens a dialog box for navigating to a personal certificate file on your computer, and then loading the certificate into NetScreen-Remote.

Note: *You can also double-click on the certificate file to import or load it into your computer.*

Root CA Certificates Page

The Root CA Certificates page provides tools for managing certificate authority (CA) certificates. A CA certificate verifies the identity of the authority that verifies personal and remote certificates.



A CA is an organization that issues certificates. Root CA certificates are self-signed, with the same Issuer and Subject.

☑ Show only trusted roots.

Trust policy - trust these roots for IPsec: ● configured roots ○ issuers of my certs ○ all roots

Figure 2-9 CA Certificates Page

After highlighting a certificate in the CA certificates window, you can click the following buttons to perform the associated tasks:

View opens the selected certificate for viewing. To close the certificate, click anywhere within the certificate displayed.

Verify checks the validity status of the selected certificate. If the certificate has expired, was revoked, or is corrupt, it will fail verification.

Configure opens the Configuration Parameters dialog box, allowing you to add details to a CA certificate. For example, if you obtained a CA certificate using the cut-and-paste method, you can add information enabling you to obtain a personal certificate online from that CA using the CEP.

Export copies the selected certificate to a directory of your choice in PKCs 12 format.

Delete removes the selected certificate from your system.

Retrieve CA Certificate opens the following dialog box for obtaining a digital certificate from a CA online via CEP.

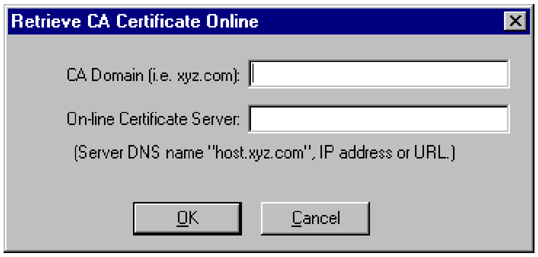

Retrieve CA Certificate Online
CA Domain (i.e. xyz.com):
On-line Certificate Server:
(Server DNS name "host.xyz.com", IP address or URL.)
OK
Cancel

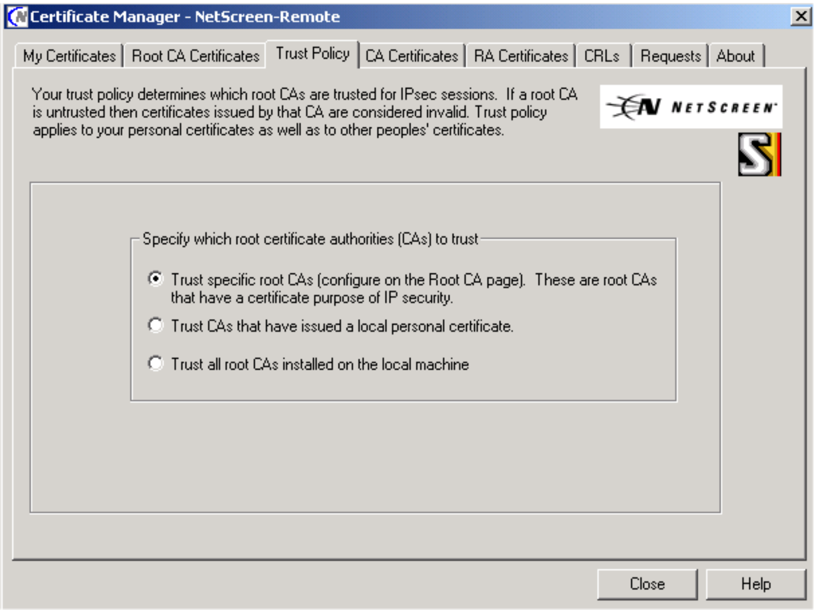
Figure 2-10 Retrieve CA Certificate Online

Import Certificate opens a dialog box for navigating to a personal certificate file on your computer and then loading the certificate into NetScreen-Remote.

Note: *Only the PKCS12 format and public key certificates are currently supported.*

Trust Policy

Your trust policy determines which root CAs are trusted for IPsec sessions. If a root CA is untrusted, then certificates issued by that CA are considered invalid. Trust policy applies to your personal certificates as well as to other people's certificates.



Certificate Manager - NetScreen-Remote

Your trust policy determines which root CAs are trusted for IPsec sessions. If a root CA is untrusted then certificates issued by that CA are considered invalid. Trust policy applies to your personal certificates as well as to other peoples' certificates.

Specify which root certificate authorities (CAs) to trust

● Trust specific root CAs (configure on the Root CA page). These are root CAs that have a certificate purpose of IP security.

○ Trust CAs that have issued a local personal certificate.

○ Trust all root CAs installed on the local machine

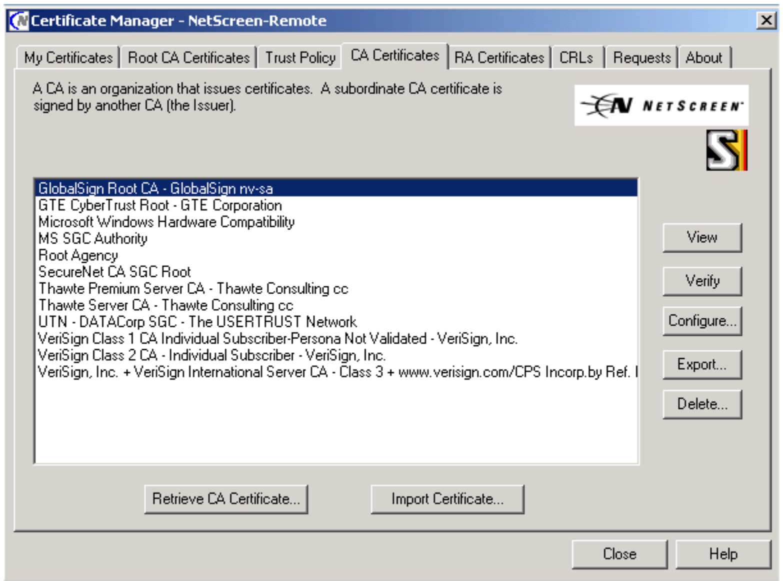
Figure 2-11 Trust Policy Menu

You can select the following Trust Policy features:

- Trust specific root CAs: use with private CAs that are loaded as root CA certificates.
- Trust CAs that have issued a local personal certificate: use with public CAs, such as VeriSign, Entrust. There is no need to load CA certificate into Root CA page.
- Trust all root CAs installed on the local machine: use with public CAs, such as VeriSign, Entrust. There is no need to load CA certificate into Root CA page.

CA Certificates

A CA is a trusted third party source that issues certificates. Examples of a CA are VeriSign and Entrust. A subordinate CA certificate is signed by another CA (the Issuer). For your convenience, common CA certificates have already been loaded.



A CA is an organization that issues certificates. A subordinate CA certificate is signed by another CA (the Issuer).

GlobalSign Root CA - GlobalSign nv-sa
GTE CyberTrust Root - GTE Corporation
Microsoft Windows Hardware Compatibility
MS SGC Authority
Root Agency
SecureNet CA SGC Root
Thawte Premium Server CA - Thawte Consulting cc
Thawte Server CA - Thawte Consulting cc
UTN - DATACorp SGC - The USERTRUST Network
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated - VeriSign, Inc.
VeriSign Class 2 CA - Individual Subscriber - VeriSign, Inc.
VeriSign, Inc. + VeriSign International Server CA - Class 3 + www.verisign.com/CPS Incorp.by Ref. I

Figure 2-12 CA Certificates

After highlighting a certificate in the CA certificates window, you can click the following buttons to perform the associated tasks:

View opens the selected certificate for viewing. To close the certificate, click anywhere within the certificate displayed.

Verify checks the validity status of the selected certificate.

Configure opens the Configuration Parameters dialog box, allowing you to add details to a CA certificate. For example, if you obtained a CA certificate using the cut-and-paste method, you can add information enabling you to obtain a personal certificate online from that CA using the CEP.

Export copies the selected certificate to a directory of your choice.

Delete removes the selected certificate from NetScreen-Remote.

Retrieve CA Certificate opens the following dialog box for obtaining a digital certificate from a CA online.

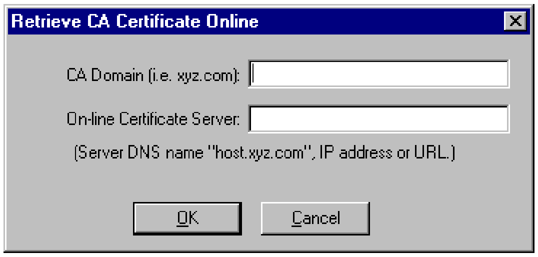

Retrieve CA Certificate Online
CA Domain (i.e. xyz.com):
On-line Certificate Server:
(Server DNS name "host.xyz.com", IP address or URL.)
OK
Cancel

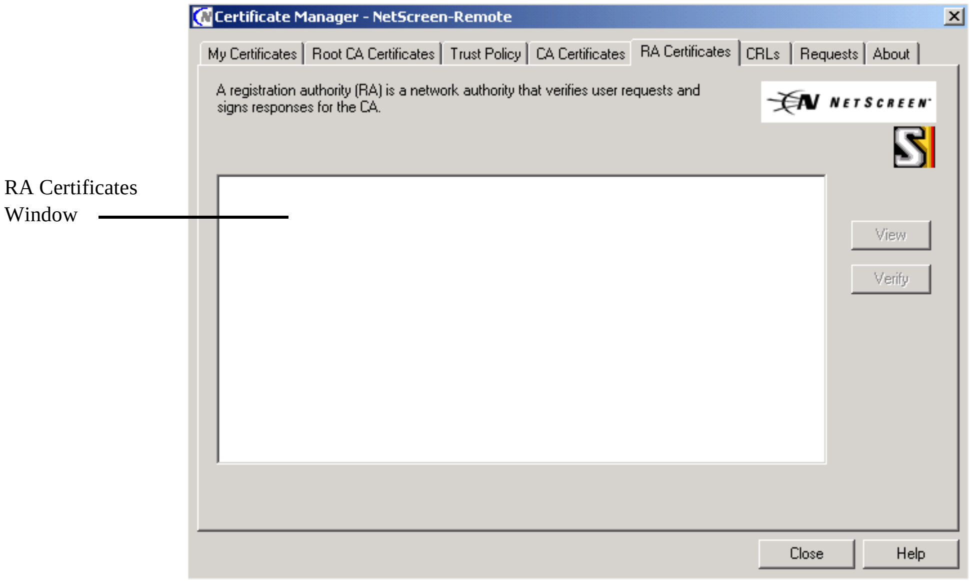
Figure 2-13 Retrieve CA Certificate Online

Import Certificate opens a dialog box for navigating to a digital certificate file on your computer and then loading the certificate into NetScreen-Remote.

RA Certificates Page

The RA Certificates page allows you to view and verify registered authority (RA) certificates. A registration authority is a subordinate-level server at the CA site that processes requests for personal certificates to the CA root server and forwards responses from the CA to the requesting parties. It is only used in the registration process.

> ***Note:*** *You will use an RA certificate, only if your CA requires one. In most cases, RA certificates are not used.*



A registration authority (RA) is a network authority that verifies user requests and signs responses for the CA.

Figure 2-14 RA Certificates Page

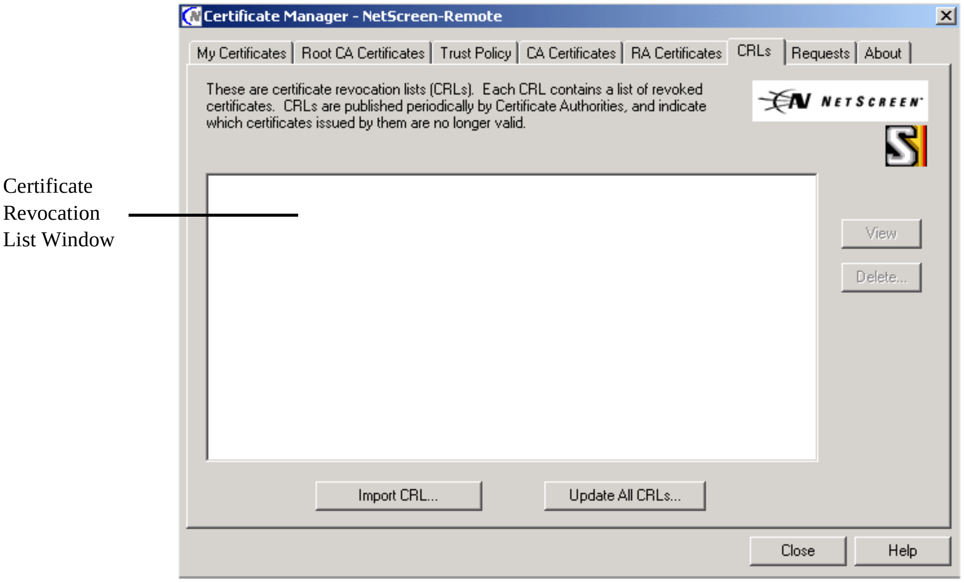
If a CA site is structured hierarchically and issues both a CA certificate and an RA certificate, it sends the RA certificate automatically with the requested CA certificate.

After highlighting a certificate in the RA certificates window, you can click the following buttons to perform the associated tasks:

> **View** opens the selected certificate for viewing. To close the certificate, click anywhere within the certificate displayed.
>
> **Verify** checks the validity status of the selected certificate.

CRLs Page

The CRLs page provides tools for importing, viewing, updating, and deleting certificate revocation lists (CRLs). A CRL is a list of revoked digital certificates. It is important to have the most recent CRL so that you know which certificates are no longer valid.



These are certificate revocation lists (CRLs). Each CRL contains a list of revoked certificates. CRLs are published periodically by Certificate Authorities, and indicate which certificates issued by them are no longer valid.

Figure 2-15 CRLs Page

After highlighting a CRL in the CRLs window, you can click the following buttons to perform the associated tasks:

View opens the selected CRL for viewing. To close the CRL, click anywhere within the CRL displayed.

Delete removes the selected CRL from NetScreen-Remote.

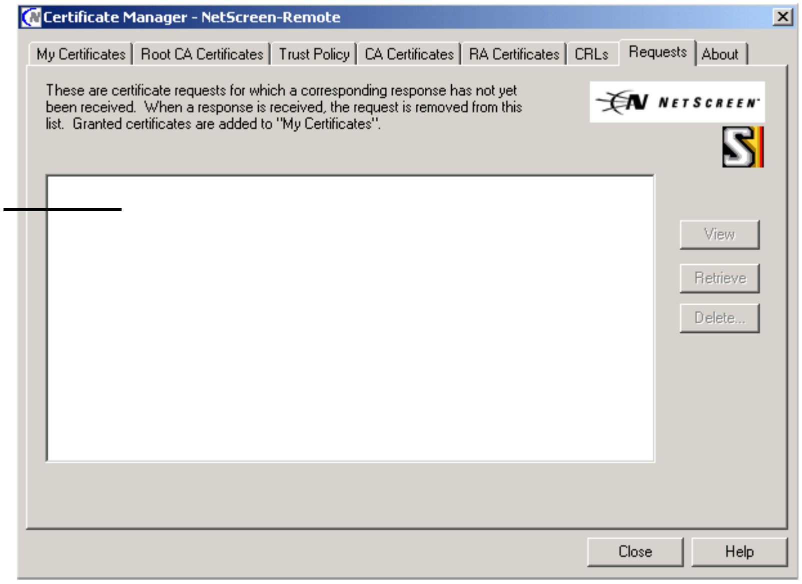
Import CRL opens a dialog box for navigating to a CRL file on your computer, and then loading the CRL into NetScreen-Remote.

Update All CRLs manually replaces all the CRLs in the Certificate Revocation List window with the latest versions available online from the respective CA servers.

Certificate Requests Page

The Certificate Requests page provides tools for viewing, retrieving, and deleting any pending personal certificate requests.

Depending on the CA contacted, a personal certificate request might take up to two or three days to process and approve. Once approved, you will be sent a file with your personal certificate. To load this file, either use the My Certificate page or double-click the file.



These are certificate requests for which a corresponding response has not yet been received. When a response is received, the request is removed from this list. Granted certificates are added to "My Certificates".

Figure 2-16 Certificate Requests Page

After highlighting a certificate request in the Pending Certificate Requests window, you can click the following buttons to perform the associated tasks:

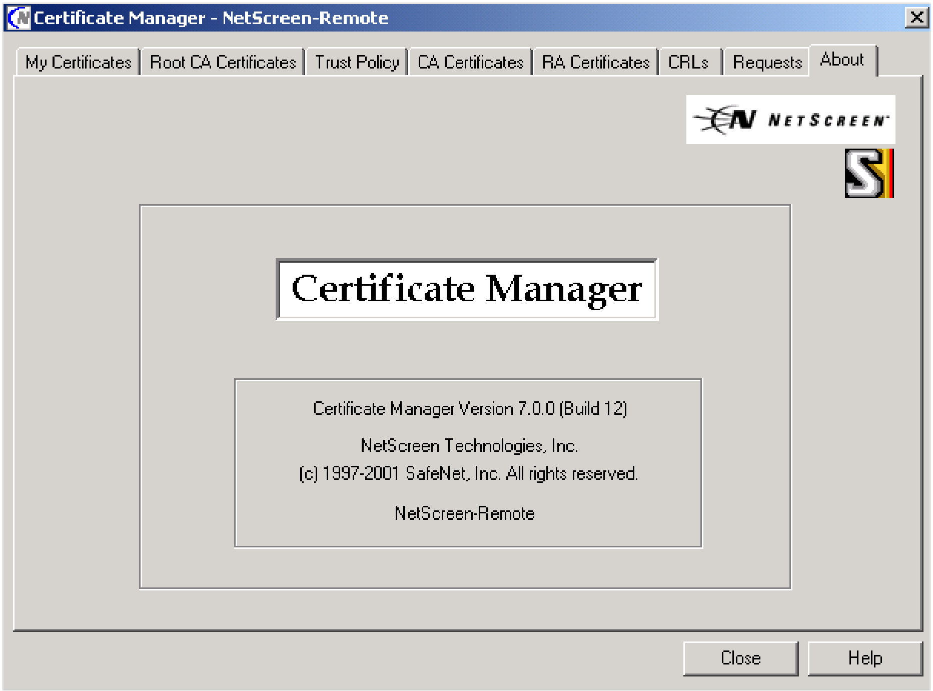
View opens the selected request for viewing.

Retrieve fetches a requested certificate from a CA when it becomes ready. The request disappears from the Pending Certificate Requests window, and the retrieved certificate appears in the My Certificates window.

Delete cancels the selected request and removes it from your system.

About Page

The About page shows the software version number, manufacturer, and copyright dates of the NetScreen-Remote Certificate Manager in use.



Certificate Manager Version 7.0.0 (Build 12)

NetScreen Technologies, Inc.

(c) 1997-2001 SafeNet, Inc. All rights reserved.

NetScreen-Remote

Figure 2-17 About NetScreen-Remote Screen

Desktop Taskbar Icons and Shortcut Menu

The NetScreen-Remote icon appears in the status area of the taskbar in the lower-right corner of the Windows desktop, as shown below.

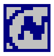


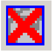
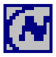
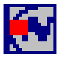
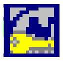
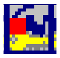
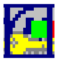
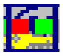
Figure 2-18 NetScreen-Remote Icon on the Windows Taskbar

The icon's appearance changes to indicate the current activity and state of NetScreen-Remote. Right-click this icon to invoke a shortcut menu.

NetScreen-Remote Icon

The NetScreen-Remote icon changes color and appearance to reflect the current activity and state of NetScreen-Remote, as shown in Table 2-2.

Table 2-2 Taskbar Icons

	**NetScreen-Remote logo (disabled)** Your Windows operating system did not start the Internet Key Exchange (IKE) service properly or NetScreen-Remote is disabled. If you see this icon, either try enabling NetScreen-Remote, if enabled, or restarting your computer. If neither work, you may need to reinstall the NetScreen-Remote software. See "Modifying Installation" on page 1-12.
	**NetScreen-Remote logo (enabled)** If you have successfully installed NetScreen-Remote, you see this icon before your computer establishes a connection or begins transmitting communications.
	**NetScreen-Remote logo (with red indicator)** Your computer has not established any secure connections and is transmitting nonsecured communications.
	**Yellow key with gray background** Your computer has established at least one secure connection but is not transmitting any communications.
	**Yellow key with red indicator** Your computer has established at least one secure connection and is transmitting only nonsecured communications.
	**Yellow with green indicator** Your computer has established at least one secure connection and is transmitting only secure communications.
	**Yellow with red/green indicator** Your computer has established at least one secure connection and is transmitting both secure and nonsecured communications.

Shortcut Menu

When you right-click the NetScreen-Remote icon on the Windows taskbar, the NetScreen-Remote shortcut menu pops up.

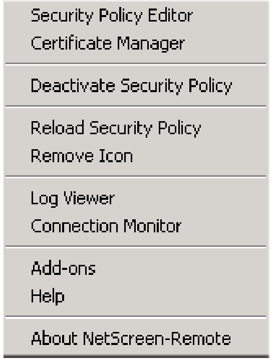


Figure 2-19 NetScreen-Remote Taskbar Shortcut Menu

Security Policy Editor opens the software module where you can manually create, store and export connections and security policies.

Certificate Manager opens the software module where you can manage certificates.

Activate/Deactivate Security Policy turns off the NetScreen-Remote so that no security policies are used. The **Deactivate Security Policy** command changes to **Activate Security Policy**.

Reload Security Policy replaces an existing security policy with a new security policy.

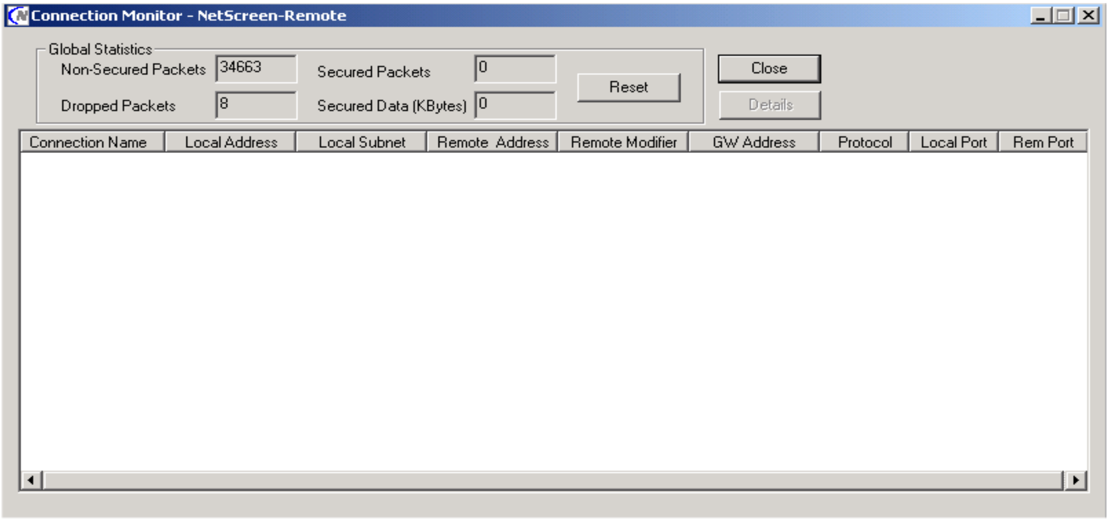
Saving changes to the security policy of an active connection terminates active connections. To delay implementing the changes until you end the currently active connection, click ***No*** *when NetScreen-Remote prompts you to reset your active connection. Then click* ***Reload Security Policy*** *to put the changes into effect.*

Remove Icon removes the NetScreen-Remote icon from the taskbar on your desktop. The icon reappears when you restart your computer.

Log Viewer opens the connection log, a diagnostic tool that lists Internet Key Exchange (IKE) negotiations as they occur.

NetScreen-Remote saves log information to a file called Connection.log in side NetScreen-Remote Directory; it is overwritten by ongoing IKE negotiations.

Connection Monitor opens a window that displays statistical and diagnostic information for each active connection in the security policy. To see details, select a connection, and click **Details**.



Connection Monitor - NetScreen-Remote

Global Statistics

Non-Secured Packets: 34663

Secured Packets: 0

Dropped Packets: 8

Secured Data (KBytes): 0

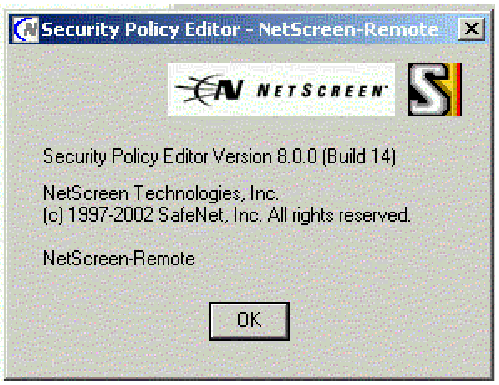
Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port

Figure 2-20 Connection Monitor

Add-ons opens the SafeNet, Inc. corporate web page.

Help opens the NetScreen-Remote Help file.

About NetScreen-Remote displays product version and copyright information.



Security Policy Editor Version 8.0.0 (Build 14)

NetScreen Technologies, Inc.
(c) 1997-2002 SafeNet, Inc. All rights reserved.

NetScreen-Remote

Figure 2-21 Product Version and Copyright Tab

Digital Certificates 3

A digital certificate is an electronic means for verifying one's identity through the word of a trusted third party, known as a Certificate Authority (CA). The CA server you use can be owned and operated by an independent CA (built-in support for Microsoft©, Verisign©, or Entrust©) or by your own organization, in which case you become your own CA. If you use an independent CA, you must contact them for the addresses of their CA and CRL servers (for obtaining certificates and certificate revocation lists), and for the information they require when submitting personal certificate requests. When you are your own CA, you make the rules.

To use a digital certificate to authenticate your identity when establishing a secure VPN connection, you must first do the following:

- Obtain a personal certificate from a CA, and load the certificate in your system through by using the Certificate Manager within NetScreen-Remote, or by double-clicking the certificate file.
- Obtain a CA certificate for the CA that issued the personal certificate (basically verifying the identity of the CA verifying you), and load the CA certificate in the Certificate Manager.
- Obtain a CRL, and load that in the Certificate Manager.

You can also view and verify Registration Authority (RA) certificates, and view and update CRLs.

This chapter covers the following information:

- Introduction to public key cryptography
- Obtaining certificates and CRLs
- Managing certificates, CRLs, and certificate requests

For information on using certificates when configuring VPN tunnels, see Chapter 5, "Configuring a VPN Tunnel with Digital Certificates."

Public Key Cryptography

In public key cryptography, a public/private key pair is used to encrypt and decrypt data. Data encrypted with a public key, which the owner makes available to the public, can only be decrypted with the corresponding private key, which the owner keeps secret and protected. For example, if Alice wants to send Bob an encrypted message, Alice can encrypt it with Bob's public key and send it to him. Bob then decrypts the message with his private key.

The reverse is also useful; that is, encrypting data with a private key and decrypting it with the corresponding public key. This is known as creating a digital signature. For example, if Alice wants to present her identity as the sender of a message, she can encrypt the message with her private key and send the message to Bob. Bob then decrypts the message with Alice's public key, thus verifying that Alice is indeed the sender.

Public/private key pairs also play an important role in the use of digital certificates. The procedure for signing a certificate (by a CA) and then verifying the signature works as follows (by the recipient):

Signing a Certificate

1. The Certificate Authority (CA) that issues a certificate hashes the certificate by using a hash algorithm (MD5 of SHA-1) to generate a digest.
2. The CA then "signs" the certificate by encrypting the digest with its private key. The result is a digital signature.
3. The CA then sends the digitally signed certificate to the person who requested it.

Verifying a Digital Signature

1. When the recipient gets the certificate, he or she also generates another digest by applying the same hash algorithm (MD5 of SHA-1) on the certificate file.
2. The recipient uses the CA's public key to decrypt the digital signature.
3. The recipient compares the decrypted digest with the digest he or she just generated. If the two digests match, the recipient can confirm the integrity of the CA's signature and, by extension, the integrity of the accompanying certificate.

Obtaining Certificates and CRLs

There are three methods for requesting a personal certificate:

- Online Enrollment Using a Web Browser.
- Manual (cut-and-paste) enrollment
- Certificate enrollment protocol (CEP)

Both methods are explained in the following sections. A CRL usually accompanies a retrieved personal certificate automatically. If it does not, you can download one from the certificate authority and then import it into the Certificate Manager.

Online Enrollment Using a Web Browser

With most CA systems, a user may request certificates online with an Online Enrollment form, or the Administrator may enroll on behalf of the user. The online enrollment process allows a user or administrator to either submit a certificate request or directly load a certificate onto a Smart-Card. Regardless of which method is chosen, once the certificate has been approved by the Administrator the user must login to the CA website and retrieve the certificate.

The CA certificate and CRL can also be loaded from the web browser into NetScreen-Remote.

Detailed information on how to submit web-based certificate requests can be found in the documentation for your CA system. NetScreen provides application-notes for various CA systems that are available from the NetScreen Technical Support site knowledgebase at http://support.netscreen.com. This is the preferred way of loading certificates if automatic enrollment via CEP is not available due to the ease-of-use by the end-user and administrator and lack of manual steps, such as saving and uploading files involved with other steps.

Manual (Cut-and-Paste) Enrollment

This procedure is also referred to as cut and paste or file-based method, because it requires you to transfer information manually to and from text files. CAs handle this method in various ways, but you always start with a certificate request file. NetScreen-Remote automatically generates the public/private key pair for you. The public key goes with your request; the private key resides on your hard drive and is kept confidential.

To obtain certificates through this method, perform this seven-step procedure, which is described in the following sections:

Step 1: Creating the Certificate Request

Step 2: Submitting the Request to Your CA

Step 3: Retrieving the Signed Certificate

Step 4: Retrieving the CA Certificate

Step 5: Importing the CA Certificate

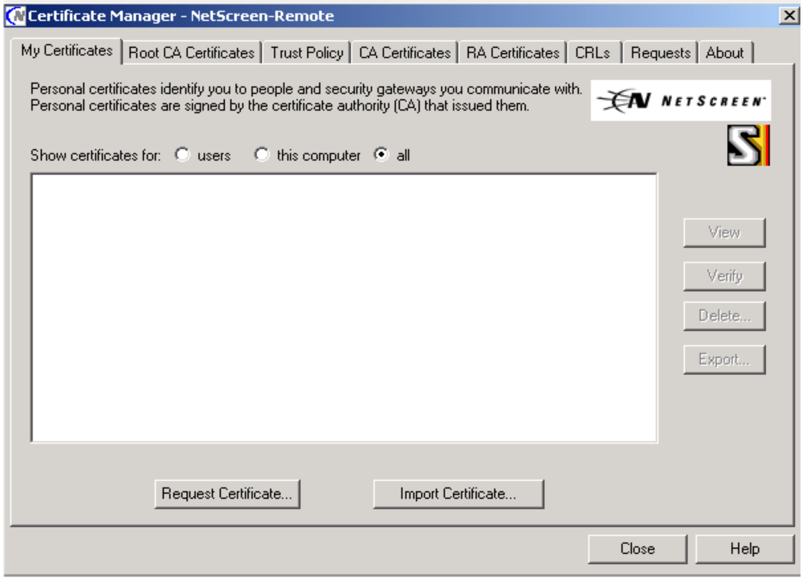
Step 6: Importing the Personal Certificate

Step 7: Obtaining the CRL

Step 1: Creating the Certificate Request

1. Open the Certificate Manager, using one of the following three methods:
   - Right-click the NetScreen/Soft-PK icon on the desktop taskbar, and then select **Certificate Manager**.
   - Double-click desktop taskbar, then click the **Options** menu, and choose **Certificate Manager**.
   - Click **Start** on the desktop taskbar, select **Programs**, then select **NetScreen-Remote**, and finally **Certificate Manager**.

   The Certificate Manager opens with the My Certificates page in front, as shown below. Any certificates you loaded are listed.



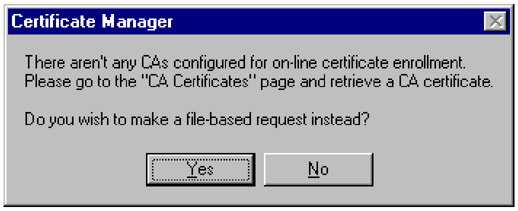
Personal certificates identify you to people and security gateways you communicate with. Personal certificates are signed by the certificate authority (CA) that issued them.

Show certificates for: ○ users ○ this computer ● all

Figure 3-1 My Certificates Menu

2. Click **Request Certificate**.

If you do not have a CA certificate loaded that supports online enrollment, this message appears:



Certificate Manager

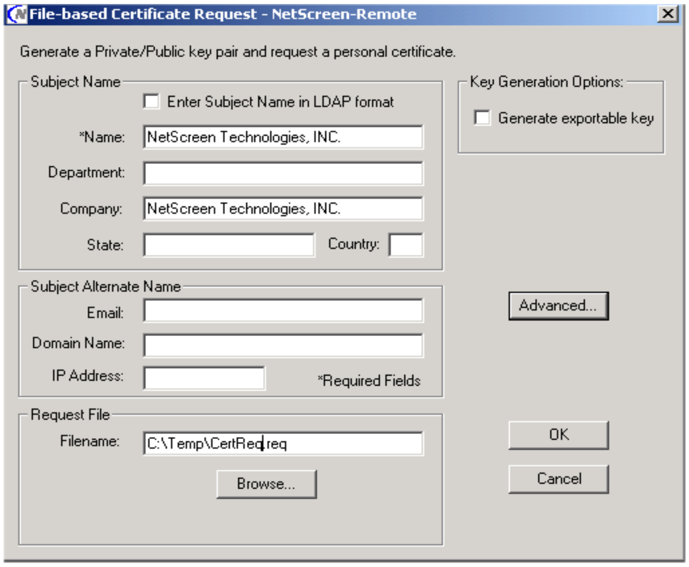
There aren't any CAs configured for on-line certificate enrollment.
Please go to the "CA Certificates" page and retrieve a CA certificate.

Do you wish to make a file-based request instead?

Figure 3-2 File-Based Request Message

3. Click **Yes** to make a file-based request.

   This dialog box appears:



File-based Certificate Request - NetScreen-Remote

Generate a Private/Public key pair and request a personal certificate.

Subject Name

☐ Enter Subject Name in LDAP format

*Name: NetScreen Technologies, INC.

Department:

Company: NetScreen Technologies, INC.

State: Country:

Key Generation Options:

☐ Generate exportable key

Subject Alternate Name

Email:

Domain Name:

IP Address:

*Required Fields

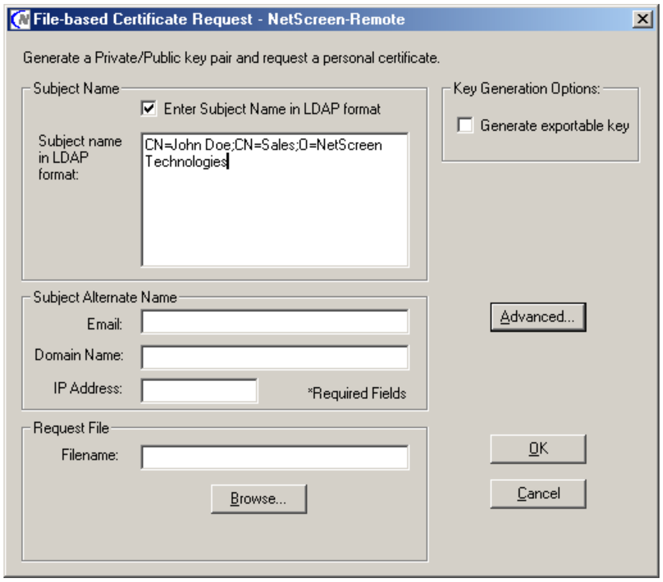
Request File

Filename: C:\Temp\CertReq.req

Figure 3-3 File-based Certificate Request

4. Complete the fields in the Subject Information area as required by your CA.

Note: *If your CA requires fields that are not shown or a different format, click Enter Subject Name in LDAP format and enter the full DN. For example, “CN=John Doe;CN=Sales;0=NetScreen.” See Figure 3-4.*



File-based Certificate Request - NetScreen-Remote

Generate a Private/Public key pair and request a personal certificate.

Subject Name

☑ Enter Subject Name in LDAP format

Subject name in LDAP format: CN=John Doe;CN=Sales;O=NetScreen Technologies

Key Generation Options:

□ Generate exportable key

Subject Alternate Name

Email:

Domain Name:

IP Address:

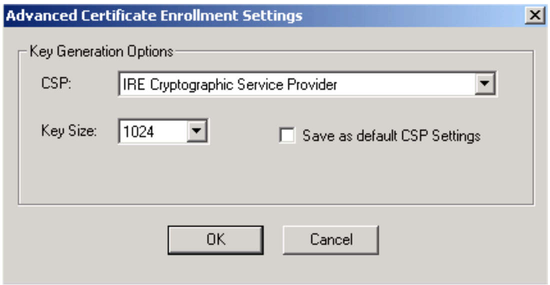
*Required Fields

Request File

Filename:

Figure 3-4 File-based Certificate Request - Subject Name in LDAP format

5. For advanced setting options, click **Advanced**.



Advanced Certificate Enrollment Settings

Key Generation Options

CSP: IRE Cryptographic Service Provider

Key Size: 1024

□ Save as default CSP Settings

Figure 3-5 Advanced Certificate Enrollment Settings Menu

Advanced opens a drop-down menu with selections for a Cryptographic Service Provider (CSP):

IRE Cryptographic Service Provider (default);

Microsoft Base Cryptographic Provider v1.0;

Microsoft Enhanced Cryptographic Provider v1.0;

Microsoft Strong Cryptographic Provider;

Schlumberger Cryptographic Service Provider (used for smart cards);

DataKey Cryptographic Service Provider (used for smart cards).

Key Size opens a drop-down menu with selections for key size: 512, 1024 or 2048.

Change the CSP setting only if you are using smart cards or your CA supports another CSP.

6. The default location for saving the Certificate Request File is C:\Temp, and the default filename is CertReq.req. To save the file in a different location, either type the location in the Filename field or click **Browse** and navigate to the folder of your choice. You can also rename the file.
7. If you want to be able to export the private key associated with the personal certificate you are now requesting, select **Generate exportable key**.

Note: *The* **Generate exportable key** *option may not work with all CSPs.*

8. Click **OK** to save the file.

Step 2: Submitting the Request to Your CA

You must submit your certificate request for approval next.

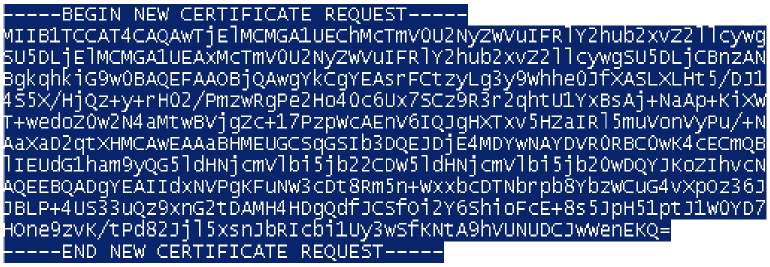
Note: *Some of the older CAs require steps 2-2 to 2-5.*

1. Go to a CA's website and follow their procedure for requesting a certificate until you reach the section where you are asked to provide your request. This usually involves submitting a saved certificate request to a website or e-mail address.

   NetScreen-Remote supports the following CAs

   – Baltimore
   – Entrust
   – IPlanet
   – Microsoft
   – RSA KeyOn
   – VeriSign
2. Using a text editor, open the certificate file that you created and saved in Step 1: Creating the Certificate Request.

3. Select the entire certificate request, taking care to select the entire text but not any blank spaces before or after the text, as shown below.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB1TCCAT4CAQAwTjElMCMGA1UEChMcTmV0U2NyZWVuIFRlY2hub2xvZ2llcywg
SU5DLjElMCMGA1UEAxMcTmV0U2NyZWVuIFRlY2hub2xvZ2llcywgSU5DLjCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAsrFCtzyLg3y9Whhe0JfXASLXLHt5/DJ1
4S5X/HjQz+y+rH02/PmzwRgPe2Ho40c6Ux7SCz9R3r2qhtU1YxBsAj+NaAp+KiXw
T+wedoZ0w2N4aMtwBVjgZc+17PzpWcAEnV6IQJgHXTxv5HZaIRl5muVonVyPu/+N
AaXaD2qtXHMCAwEAAaBHMEUGCSqGSIb3DQEJDjE4MDYwNAYDVR0RBC0wK4cECmQB
lIEUdG1ham9yQG5ldHNjcmVlbi5jb22CDW5ldHNjcmVlbi5jb20wDQYJKoZIhvcN
AQEEBQADgYEAIIdxNVPgKFuNW3cDt8Rm5n+WxxbcDTNbrpb8YbzWCuG4vXpOz36J
JBLP+4US33uQz9xnG2tDAMH4HDgQdfJCSfOi2Y6ShioFcE+8s5JpH51ptJ1W0YD7
HOne9zvK/tPd82Jjl5xsnJbRIcbi1Uy3wSfKNtA9hVUNUDCJwWenEKQ=
-----END NEW CERTIFICATE REQUEST-----
```

Figure 3-6 Selecting the Entire Certificate Request

4. Copy the selected text and paste it into the certificate request field on the website.
5. Submit the request in accordance with the CA's procedure.

   When your certificate request has been completely processed, the CA might display the certificate online or send it to you in an e-mail message.

Step 3: Retrieving the Signed Certificate

1. Select the entire certificate, taking care to select the entire text but not any blank spaces before or after the text, and copy it.
2. Paste the text into a simple text editor file.
3. Click **Save As**, and select **All Files (*.*).**
4. Name the file, and save it with the following extension: .cer

Step 4: Retrieving the CA Certificate

You must have both a personal certificate and a CA certificate from the CA that issued your personal certificate.

1. Return to the CA's website and follow the online procedure for requesting a CA certificate.
2. Copy the CA certificate and paste it into a text editor file.
3. Click **Save As**, and select **All Files (*.*).**
4. Name the file, and save it with the following extension: .cer

Step 5: Importing the CA Certificate

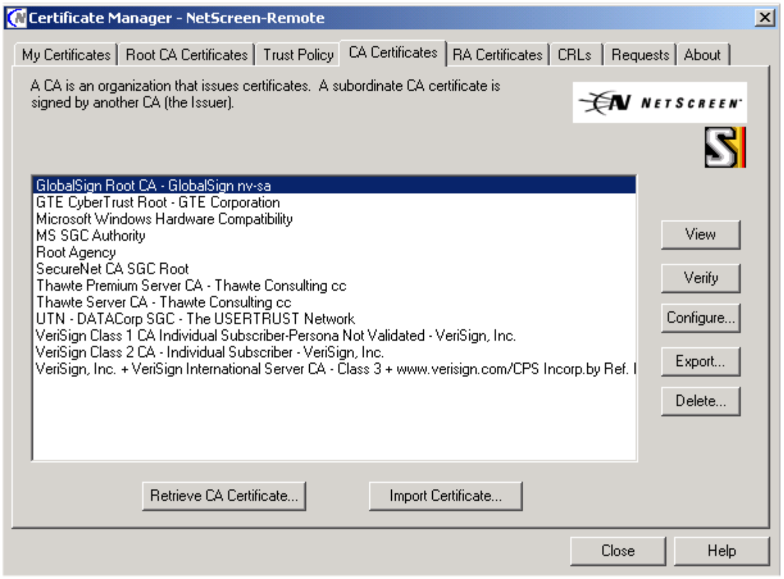
Note: *If you have Microsoft Windows 98, 98SE, ME, NT 4.0 or XP, you may skip the following procedure. You need only to double-click the CA certificate file to import it. If you have Microsoft Windows 95, you are required to go through the following procedure to import your CA certificate.*

1. In the Certificate Manager module of NetScreen-Remote, click the **CA Certificates** tab to bring that page to the front.
2. Click **Import Certificate**.

   The Open File dialog box appears.

3. Navigate to the file where you saved the CA certificate, and then click **Open**.

   The CA certificate is loaded and appears in the CA Certificate Window, as shown below.



A CA is an organization that issues certificates. A subordinate CA certificate is signed by another CA (the Issuer).

GlobalSign Root CA - GlobalSign nv-sa
GTE CyberTrust Root - GTE Corporation
Microsoft Windows Hardware Compatibility
MS SGC Authority
Root Agency
SecureNet CA SGC Root
Thawte Premium Server CA - Thawte Consulting cc
Thawte Server CA - Thawte Consulting cc
UTN - DATACorp SGC - The USERTRUST Network
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated - VeriSign, Inc.
VeriSign Class 2 CA - Individual Subscriber - VeriSign, Inc.
VeriSign, Inc. + VeriSign International Server CA - Class 3 + www.verisign.com/CPS Incorp.by Ref. I

Figure 3-7 Imported CA Certificate

Step 6: Importing the Personal Certificate

Note: *If you have Microsoft Windows 98, 98SE, ME, NT 4.0 or XP, you may skip the following procedure. You need only to double-click the CA certificate file to import it. If you have Microsoft Windows 95, you are required to go through the following procedure to import your CA certificate.*

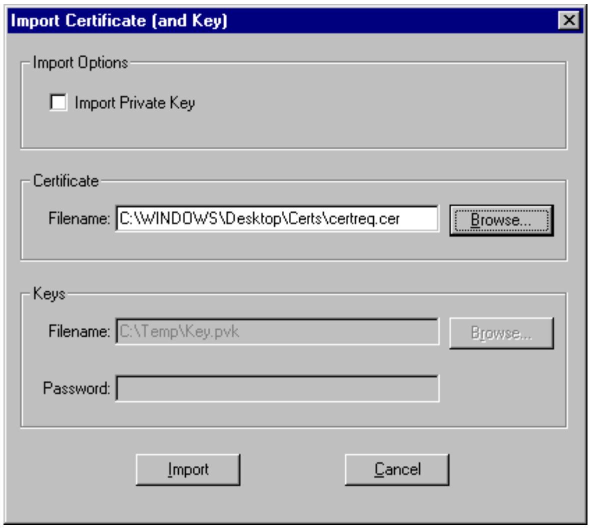
1. In Certificate Manager, click the **My Certificates** tab to bring that page to the front.
2. Click **Import Certificate**.

   The Import Certificate (and Key) dialog box appears.
3. Clear the **Import Private Key** check box.

   The Filename and Password fields in the Keys section become dimmed.
4. In the Certificate section, click **Browse** to navigate to the file where you saved the personal certificate.

   The Open File dialog box appears.
5. Navigate to the file where you saved the personal certificate, select the file, and then click **Open**.

   The selected file name and path appear in the Certificate Filename field. The Import Certificate (and Key) dialog box looks similar to that shown in Figure 3-8.



Import Certificate (and Key)

Import Options

□ Import Private Key

Certificate

Filename: C:\WINDOWS\Desktop\Certs\certreq.cer

Keys

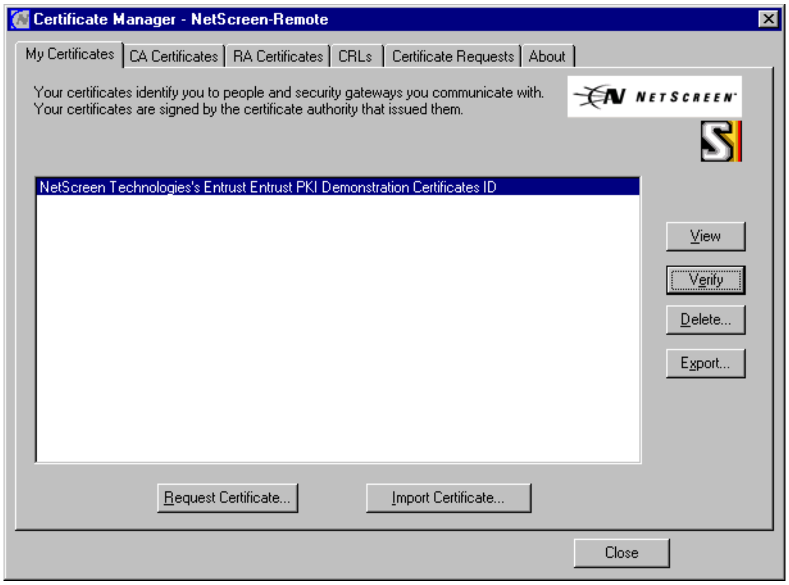
Filename: C:\Temp\Key.pvk

Password:

Figure 3-8 Import Certificate (and Key)

6. Click **Import**.

The personal certificate is loaded and appears in the Personal Certificates Window, as shown in Figure 3-9.



Your certificates identify you to people and security gateways you communicate with. Your certificates are signed by the certificate authority that issued them.

NetScreen Technologies's Entrust Entrust PKI Demonstration Certificates ID

Figure 3-9 Imported Personal Certificate

Step 7: Obtaining the CRL

A CRL is a list of certificates that the CA no longer recognizes as valid. Logically, any certificate issued by the CA that has not expired and is not on the CRL is valid.

Whenever you retrieve or import a personal certificate from a CA, it usually contains a CRL that imports directly into the Certificate Manager and can be viewed on the CRLs page. You usually need not configure or request anything.

If you have to obtain a CRL manually:

1. Download the CRL from the CA’s website, and save it locally.
2. On the CRLs page in the Certificate Manager, click **Import CRL**.

   The Import CRL dialog box appears.
3. Navigate to the CRL file that you downloaded, select the file, and click **Open**.

   A message appears, stating that the CRL has been successfully imported.
4. Click **OK** to acknowledge the message.

CEP Enrollment

The Certificate Enrollment Protocol (CEP) is a method for on-line enrollment. If you select a CA that supports this method, you must have their CA certificate before you can request a personal certificate online. In this case, you must know the certificate server DNS name or IP address in advance.

An advantage of CEP enrollment is that the CA automatically imports the CRL with the requested certificate. With the cut-and-paste method, you must download the CRL separately.

To obtain certificates through this method, perform the following two-step procedure:

Step 1: Retrieving the CA Certificate

Step 2: Retrieving a Personal Certificate

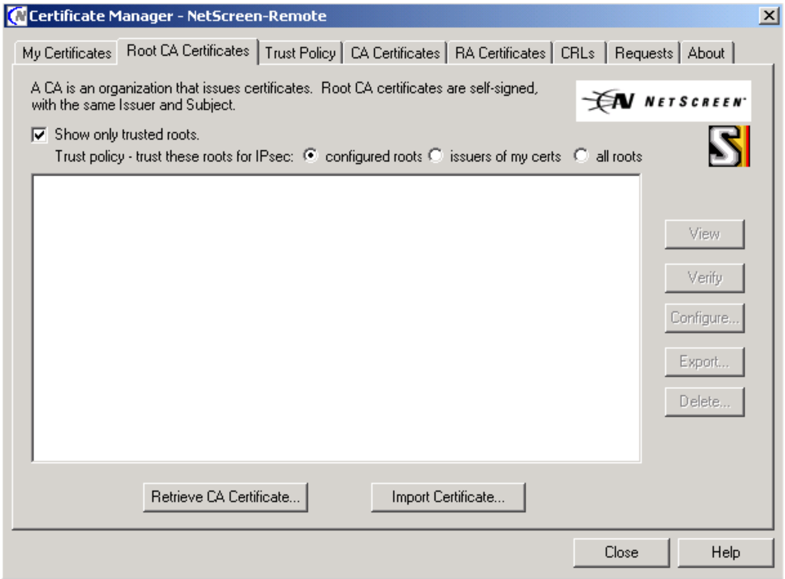
Step 1: Retrieving the CA Certificate

If you are on a network on the Trusted side of a NetScreen device and are attempting to use the CEP method to obtain a certificate from a CA on the Untrusted side (that is, on the Internet), then you must precede the retrieval procedure by enabling and specifying the DNS name or IP address of the proxy server for your network. To do this, use the Certificate Settings dialog box, shown on page 2-7 (choose Certificate Settings from the Option menu). If the CA server that you are using is on your network or if you are not requesting the certificate from a network inside a firewall, you can skip this preliminary step.

1. Log on to the Internet.
2. Open the Certificate Manager, using one of the following three methods:
   - Right-click the NetScreen/Soft-PK icon and select **Certificate Manager**.
   - Choose **Certificate Manager** from the Options menu.
   - Click **Start** on the desktop taskbar, then **Programs**, **NetScreen-Remote**, and **Certificate Manager**.

   The Certificate Manager opens with the My Certificates page in front.

3. Click the **CA Certificates** tab to bring that page forward, as shown in Figure 3-10.



A CA is an organization that issues certificates. Root CA certificates are self-signed, with the same Issuer and Subject.

☑ Show only trusted roots.

Trust policy - trust these roots for IPsec: ● configured roots ○ issuers of my certs ○ all roots

Figure 3-10 CA Certificates Page

4. Click **Retrieve CA Certificate**.

   This dialog box appears:

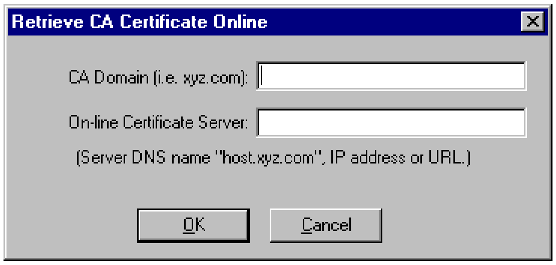

Retrieve CA Certificate Online
CA Domain (i.e. xyz.com):
On-line Certificate Server:
(Server DNS name "host.xyz.com", IP address or URL.)
OK
Cancel

Figure 3-11 Retrieve CA Certificate Online

5. In the CA Domain field, type the DNS name of the CA Authority, for example, entrust.com or verisign.com.

6. In the On-line Certificate Server field, type the complete IP or URL address of the certificate server.

   If the URL address of the CA certificate server ends with “cgi-bin/pkiclient.exe,” do not include the protocol connection at the beginning of the URL. If the URL address ends with anything else, you must include the protocol connection at the beginning of the URL.

7. Click **OK**.

   Within a few seconds, the Root Certificate Store message box appears, asking if you want to add the CA certificate to the Root Store.

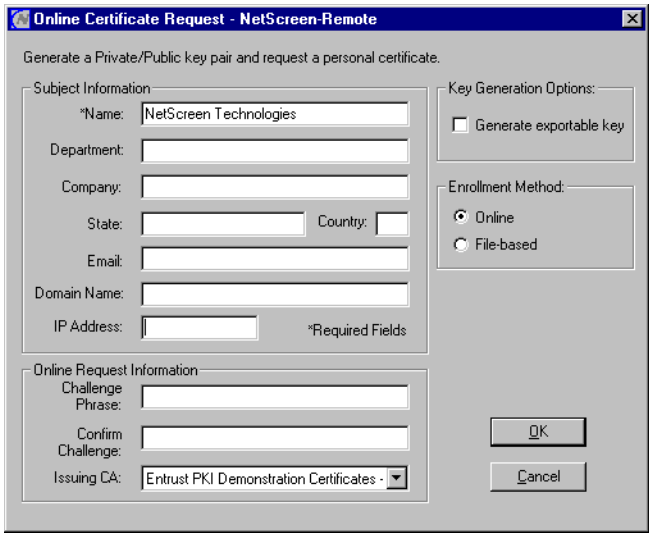
8. Click **Yes**.

   The CA’s digital certificate is now listed under CA Certificates.

Step 2: Retrieving a Personal Certificate

1. Click the **My Certificates** tab to bring that page to the front.
2. Click **Request Certificate**.

   This dialog box appears:



Online Certificate Request - NetScreen-Remote

Generate a Private/Public key pair and request a personal certificate.

Subject Information

*Name: NetScreen Technologies

Department:

Company:

State: Country:

Email:

Domain Name:

IP Address:

*Required Fields

Key Generation Options:

□ Generate exportable key

Enrollment Method:

● Online

○ File-based

Online Request Information

Challenge Phrase:

Confirm Challenge:

Issuing CA: Entrust PKI Demonstration Certificates -

Figure 3-12 On-line Certificate Request

3. In the Subject Information area, enter all relevant personal information.

   You might not need to fill in every field, depending on the requirements of the CA. The fields that one CA requires might not be required by another.

4. In the On-line Request Information area, make the following entries:
   - For the Challenge Phrase, type any combination of numbers or letters you choose. (For security reasons, only asterisks appear.)
   - For the Confirm Challenge, make the same entry as for the Challenge Phrase.
   - From the Issuing CA drop-down list, select a CA certificate.
5. If you want to be able to export the private key at a later time, select **Generate exportable key**.

   You will only be able to export the private key associated with the personal certificate you are now requesting if you select ***Generate exportable key*** *now. For security reasons, no one can change it later.*

6. In the Enrollment Method area, select **On-line**.
7. Click **OK**.

   NetScreen-Remote now generates a public/private key pair, and then it displays the On-line 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.

8. Click **OK** again.

   The certificate request appears on the Certificate Requests page.

9. Select the certificate request and click **Retrieve**.

   A message appears asking if you want to add this personal certificate.

10. Click **Yes**.

    The certificate request disappears from the Certificate Requests page, and the personal certificate now appears on the My Certificates page.

    The CRL usually accompanies the personal certificate automatically. If not, you can manually import it. For instructions, see "Step 7: Obtaining the CRL" on page 3-13.

11. To start using the certificate, you must first exit from NetScreen-Remote, and then open it again.

In the Security Policy Editor, you can now select the personal certificate in the Select Certificate field as a means for verifying your identity.

Managing Certificates, CRLs, and Certificate Requests

Personal and CA Certificates:
After you have loaded a personal or CA certificate in the Certificate Manager, you can view, verify, export, and delete it. (You can also configure a CA certificate obtained through the cut-and-paste enrollment method so that you can get a personal certificate using the CEP method from the same CA.)

RA Certificates:
A Registration Authority (RA) certificate automatically accompanies a CA certificate obtained from a CA structured hierarchically to include RAs. You can view and verify an RA certificate, but you can only delete it by deleting the CA certificate associated with it.

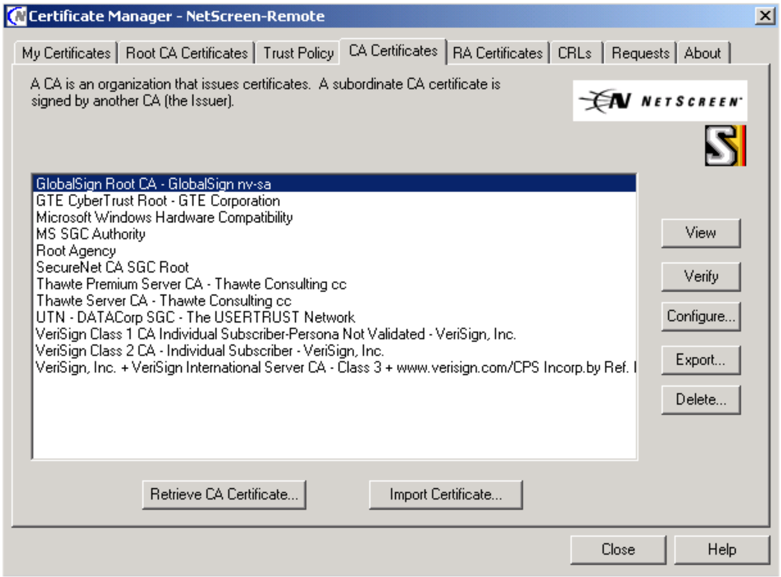
CRLs:
A CRL usually accompanies a personal certificate obtained on-line through the CEP method if the CRL distribution point is a valid URL. If you do not automatically receive one or if you obtain a personal certificate via the cut-and-paste method, you can download and import a CRL manually. Then you can view, update, and delete it.

Certificate Requests:
Some CAs approve certificate requests automatically, in which case the certificate becomes immediately available. Other CAs approve certificate requests manually and can take several days to process the request. During that waiting period, the pending certificate request is listed in the Certificate Requests window. Before the request is approved, you can view and delete it. Once the request is approved, you can then retrieve it for use.

Viewing Certificates, CRLs, and Certificate Requests

It is good practice to view your certificates to ensure that the information is accurate. In addition to personal and CA certificates, you can also view RA certificates, CRLs, and certificate requests.

Open the CA Certificates tab menu, as shown below:



A CA is an organization that issues certificates. A subordinate CA certificate is signed by another CA (the Issuer).

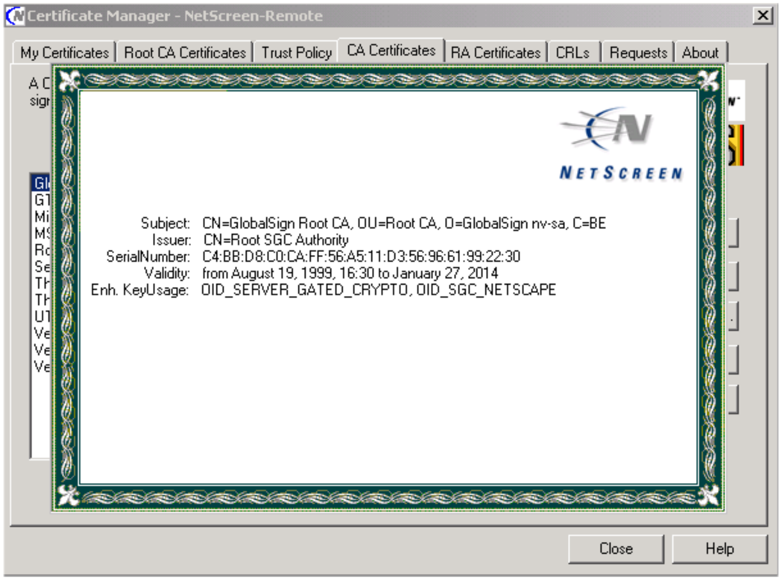
GlobalSign Root CA - GlobalSign nv-sa
GTE CyberTrust Root - GTE Corporation
Microsoft Windows Hardware Compatibility
MS SGC Authority
Root Agency
SecureNet CA SGC Root
Thawte Premium Server CA - Thawte Consulting cc
Thawte Server CA - Thawte Consulting cc
UTN - DATACorp SGC - The USERTRUST Network
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated - VeriSign, Inc.
VeriSign Class 2 CA - Individual Subscriber - VeriSign, Inc.
VeriSign, Inc. + VeriSign International Server CA - Class 3 + www.verisign.com/CPS Incorp.by Ref. I

Figure 3-13 CA Certificates Menu

1. Select the page with the item that you want to view by clicking its tab.

2. Select the item in the main window on that page, and click **View**, located on the right side of the page.

   The selected item appears, as shown below.



Subject: CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Issuer: CN=Root SGC Authority
SerialNumber: C4:BB:D8:C0:CA:FF:56:A5:11:D3:56:96:61:99:22:30
Validity: from August 19, 1999, 16:30 to January 27, 2014
Enh. KeyUsage: OID_SERVER_GATED_CRYPTO, OID_SGC_NETSCAPE

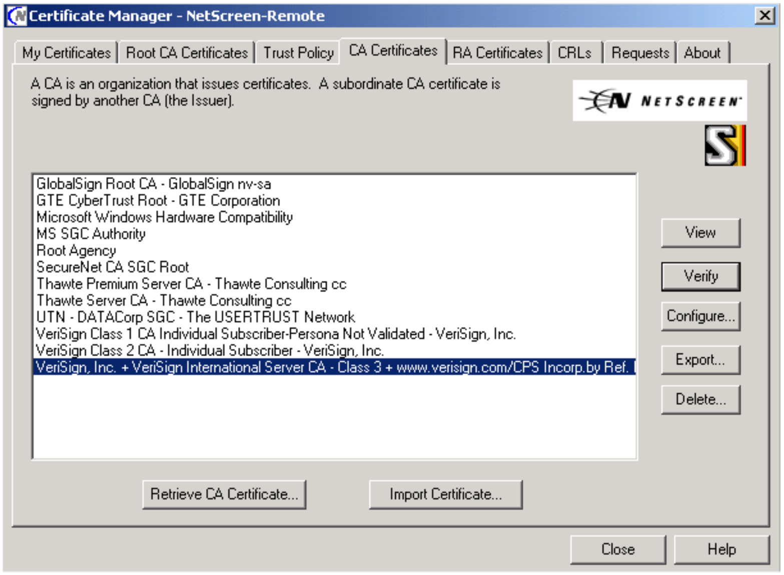
Figure 3-14 Certificate View Screen

3. To close a certificate, click it.

Verifying Certificates

To verify that a personal, CA, or RA certificate is valid:

1. Open the CA Certificates tab, and select the item that you want to verify by clicking its tab, as shown below:



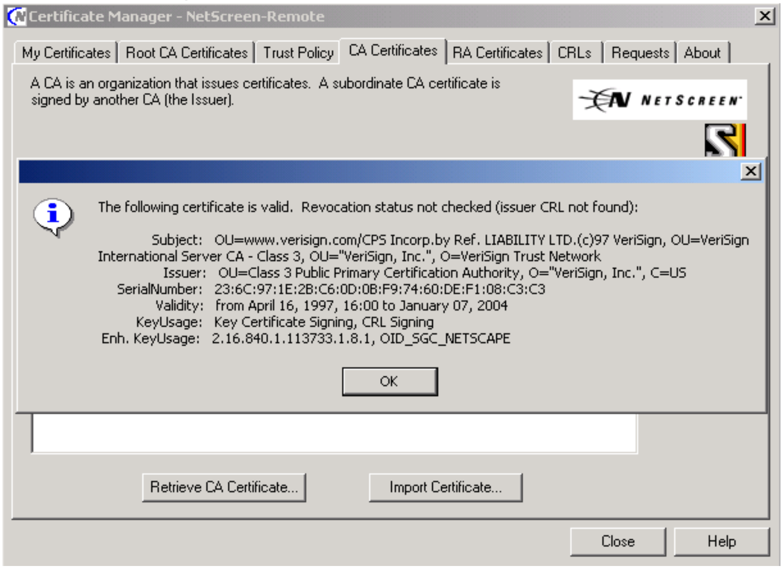
A CA is an organization that issues certificates. A subordinate CA certificate is signed by another CA (the Issuer).

GlobalSign Root CA - GlobalSign nv-sa
GTE CyberTrust Root - GTE Corporation
Microsoft Windows Hardware Compatibility
MS SGC Authority
Root Agency
SecureNet CA SGC Root
Thawte Premium Server CA - Thawte Consulting cc
Thawte Server CA - Thawte Consulting cc
UTN - DATACorp SGC - The USERTRUST Network
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated - VeriSign, Inc.
VeriSign Class 2 CA - Individual Subscriber - VeriSign, Inc.
VeriSign, Inc. + VeriSign International Server CA - Class 3 + www.verisign.com/CPS Incorp.by Ref.

Figure 3-15 CA Certificates Menu

2. Select the item in the main window, and then click **Verify**.

A property sheet for the selected item appears, detailing its properties and proclaiming it as valid or not, as shown below:



A CA is an organization that issues certificates. A subordinate CA certificate is signed by another CA (the Issuer).

The following certificate is valid. Revocation status not checked (issuer CRL not found):

```
       Subject:  OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign, OU=VeriSign
International Server CA - Class 3, OU="VeriSign, Inc.", O=VeriSign Trust Network
        Issuer:  OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
  SerialNumber:  23:6C:97:1E:2B:C6:0D:0B:F9:74:60:DE:F1:08:C3:C3
      Validity:  from April 16, 1997, 16:00 to January 07, 2004
      KeyUsage:  Key Certificate Signing, CRL Signing
 Enh. KeyUsage:  2.16.840.1.113733.1.8.1, OID_SGC_NETSCAPE
```

Figure 3-16 CA Certificates Verify Display

3. To close the property sheet, click **OK**.

Exporting Certificates

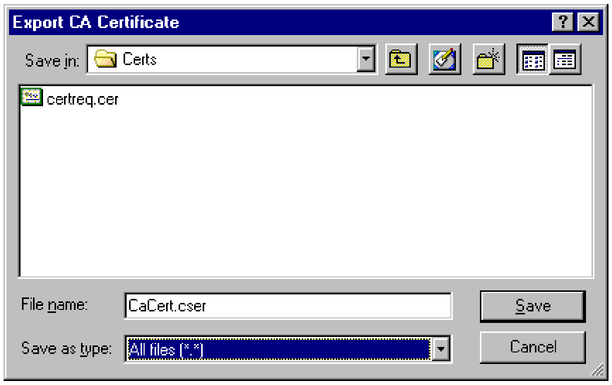
Exporting a certificate means copying it to an electronic file. You might export a certificate for reasons such as these:

- To transfer a certificate to another computer
- To create a backup copy

Always export the private key with the personal certificate. It is available for export only if you selected ***Generate exportable key*** *when you made the certificate request.*

1. Select the page with the certificate that you want to export.
2. Select the certificate in the main window, and then click **Export**.

   This dialog box appears:



File name: CaCert.cser

Save as type: All files (*.*)

Figure 3-17 Export CA Certificate

3. Navigate to the folder where you want to store a copy of the certificate, name the certificate file, and then click **Save**.

Deleting Certificates, CRLs, and Certificate Requests

To delete a certificate, CRL, or certificate request:

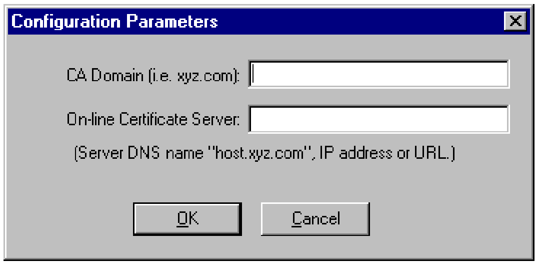
1. Select the page with the item that you want to delete.
2. Select the item in the main window on the page, and then click **Delete**.
3. You will be asked to confirm the deletion.
4. Click **Yes** to delete the selected item.

Configuring a CA Certificate

You can configure a CA certificate obtained through the cut-and-paste enrollment method to include the CA's domain name and the IP or URL address of the CA certificate server. Doing so enables you to obtain a personal certificate using the CEP method from the same CA in the future.

1. Click the **CA Certificates** tab to bring that page to the front.
2. Click **Configure**.

   This dialog box appears:



Configuration Parameters
CA Domain (i.e. xyz.com):
On-line Certificate Server:
(Server DNS name "host.xyz.com", IP address or URL.)
OK
Cancel

Figure 3-18 Configuration Parameters

3. In the CA Domain field, type the DNS name of the CA Authority, for example, entrust.com or verisign.com.
4. In the On-line Certificate Server field, type the complete IP or URL address of the certificate server.

If the URL address of the CA certificate server ends with "cgi-bin/pkiclient.exe," do not include the protocol connection at the beginning of the URL. If the URL address ends with anything else, you must include the protocol connection at the beginning of the URL.

5. Click **OK**.

Updating a CRL

NetScreen-Remote automatically updates CRLs obtained on-line through the CEP method once every 4 hours by default. You can specify a different interval (from 1 to 24 hours) for the automatic updates to occur. You can also update CRLs manually at any time.

To change the automatic CRL update interval:

1. In the Security Policy Editor, choose **Certificate Settings** from the Options menu.

   The Certificate Settings dialog box opens.

2. Select **Enable automatic CRL retrieval**.
3. In the CRL retrieval interval field, type a number between 1 and 24 to indicate the number of hours between each CRL update.
4. In the Default LDAP Server for CRLs field, type the complete URL address of the LDAP server for the CA. (Contact your CA for this information.)

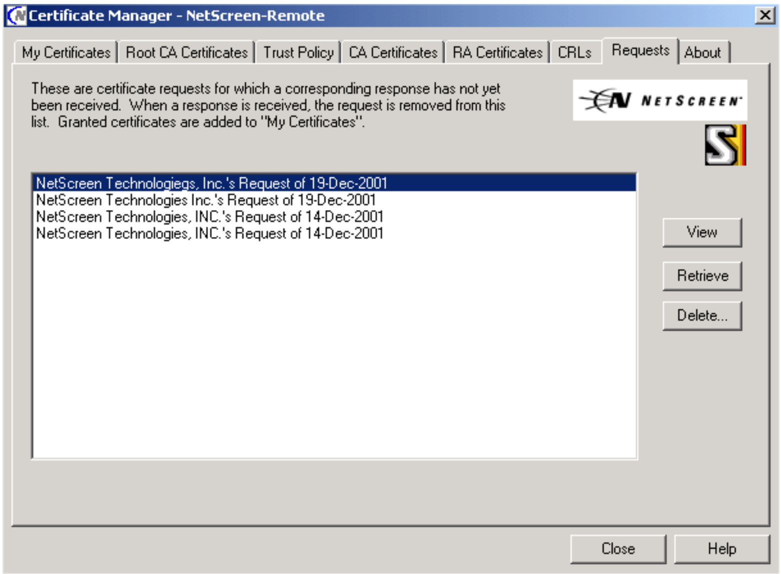
To update all the CRLs manually:

1. In the Certificate Manager, click the CRLs tab to bring that page forward.
2. Click **Update All CRLs**.

Retrieving Certificate Requests

Some CAs approve certificate requests automatically, in which case the certificate becomes immediately available. Other CAs approve certificate requests manually and can take several days to process the request. When the request is approved, the CA usually notifies the person making the request by e-mail or telephone, although sometimes it is the individual's responsibility to check with the CA to see if the certificate is ready. In either case, when you know that a request is ready, you can retrieve it.

1. Click the **Requests** tab to bring that page to the front, as shown below:



These are certificate requests for which a corresponding response has not yet been received. When a response is received, the request is removed from this list. Granted certificates are added to "My Certificates".

NetScreen Technologiegs, Inc.'s Request of 19-Dec-2001
NetScreen Technologies Inc.'s Request of 19-Dec-2001
NetScreen Technologies, INC.'s Request of 14-Dec-2001
NetScreen Technologies, INC.'s Request of 14-Dec-2001

Figure 3-19 Requests Menu

2. Select a pending request in the main window on that page.
3. Click **Retrieve**.

   NetScreen-Remote retrieves the certificate from the CA, and a prompt appears asking if you want to add this certificate.

4. Click **Yes**.

The certificate request disappears from the Certificate Request list, and the requested certificate appears in the list on either the CA Certificates or My Certificates page, as appropriate.

Configuring a VPN Tunnel with Pre-Shared Key 4

A Pre-Shared Key is a static key for both encryption and decryption that both participants must have before initiating communication. In this regard, the issue of secure key distribution is the same as that with a Manual Key. However, once distributed, a Pre-Shared Key, unlike a Manual Key, will change at predetermined intervals using the Internet Key Exchange (IKE) protocol. Frequently changing keys greatly improves security, and automatically doing so greatly reduces key-management responsibilities. However, changing keys increases traffic overhead; therefore, doing so too often can reduce data transmission efficiency.

This chapter explains the basics of configuring the NetScreen-Remote client for Pre-Shared Key operation. For additional information on setting up the security-gateway end of the tunnel with AutoKey (IKE) functionality, see Chapter 7, “Sample Scenarios” and the *NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 4: VPNs*.

As with Manual Keys, you must devise a means of securely distributing keys. Suggestions for securely transmitting keys are offered in Chapter 9, “Large Scale Distribution (Standalone Procedure).” Anyone with a valid ID and a Pre-Shared Key will be permitted access until the Pre-Shared Key is changed or user’s ID is disabled.

If you will be deploying NetScreen-Remote policies with NetScreen-Remote Global PRO, skip to Chapter 8, “Large Scale Distribution with NetScreen-Global PRO.” Chapters 4 to 7 do not apply to you.

Configuring the NetScreen-Remote Client

You can use a Pre-Shared Key operation when the NetScreen-Remote client has either a fixed or dynamically assigned IP address.

There are three steps to setting up NetScreen-Remote for a VPN tunnel with a Pre-Shared Key:

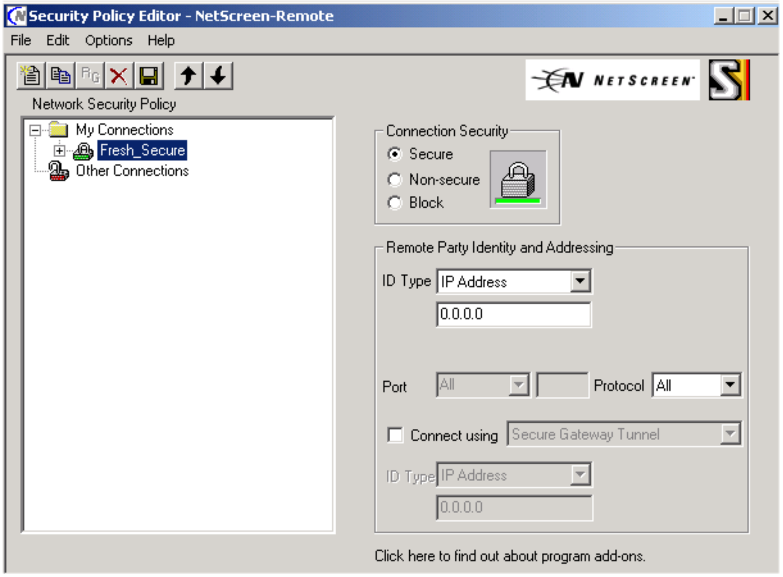
1. Creating a New Connection
2. Creating the Pre-Shared Key
3. Defining the IPSec Protocols

Step 1: Creating a New Connection

You begin by initiating a new connection. You then name the connection, define it as secure, and determine the identification and location of the other end of the eventual VPN tunnel.

1. Double-click the **NetScreen-Remote** icon, located on the Windows taskbar, to open the Security Policy Editor.
2. On the File menu, choose **New Connection**.

   A new Connection icon appears in the Network Security Policy list, as shown in Figure 4-1 on page 4-2.


Security Policy Editor - NetScreen-Remote
File
Edit
Options
Help
NETSCREEN
Network Security Policy
Click here to find out about program add-ons.

Network Security Policy
- My Connections
  - Fresh_Secure
- Other Connections

Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Address
0.0.0.0
Port: All
Protocol: All
☐ Connect using: Secure Gateway Tunnel
ID Type: IP Address
0.0.0.0

Figure 4-1 New Connection

3. Give the new connection a unique name.
4. In the Connection Security area (to the right of the Network Security Policy list), select **Secure**.
5. In the Remote Party Identity and Addressing area, select an identifier for the other party from the ID Type list, and enter the required information.

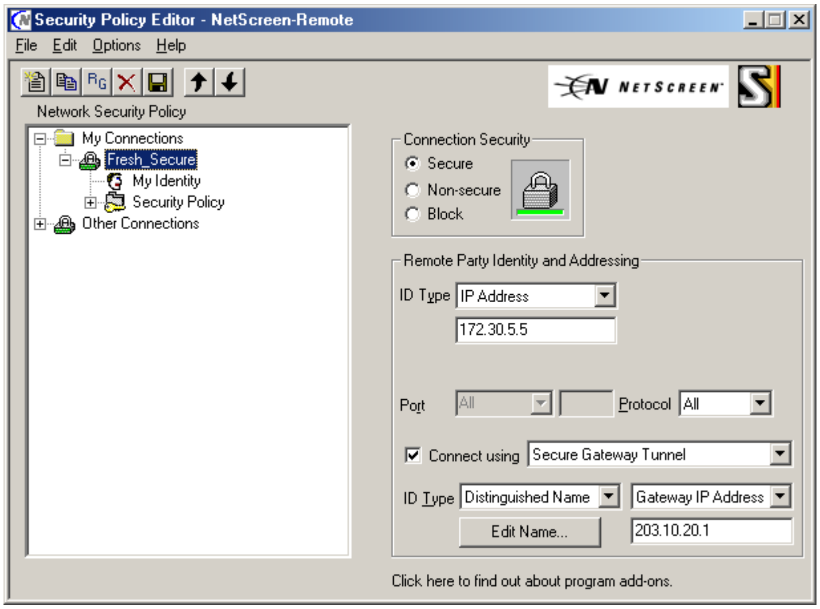
   Choose either IP Address or IP Subnet. Other choices will not work.

6. Define the protocol you want to use for the Connection: **All**, **TCP**, **UDP**, **ICMP**. The default is All.
7. If you are using tunnel mode to connect to a NetScreen device, select **Connect using Secure Gateway Tunnel**.

   The Secure Gateway Tunnel ID Type and IP Address fields become available.

8. For ID Type, select either **IP Address** or **Distinguished Name** as an identifier for the other party from the **ID Type** list, and enter the required information.

   If you select **Distinguished Name**, you must select either **Gateway IP address**, and enter the Gateway's IP address, or **Gateway Hostname** and enter the Gateway's hostname or Fully Qualified Domain Name (FQDN).



Security Policy Editor - NetScreen-Remote

Network Security Policy
- My Connections
  - Fresh_Secure
    - My Identity
    - Security Policy
- Other Connections

Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Address
172.30.5.5
Port: All
Protocol: All
☑ Connect using: Secure Gateway Tunnel
ID Type: Distinguished Name
Gateway IP Address: 203.10.20.1

Click here to find out about program add-ons.

Figure 4-2 Remote Party Identity and Addressing

Step 2: Creating the Pre-Shared Key

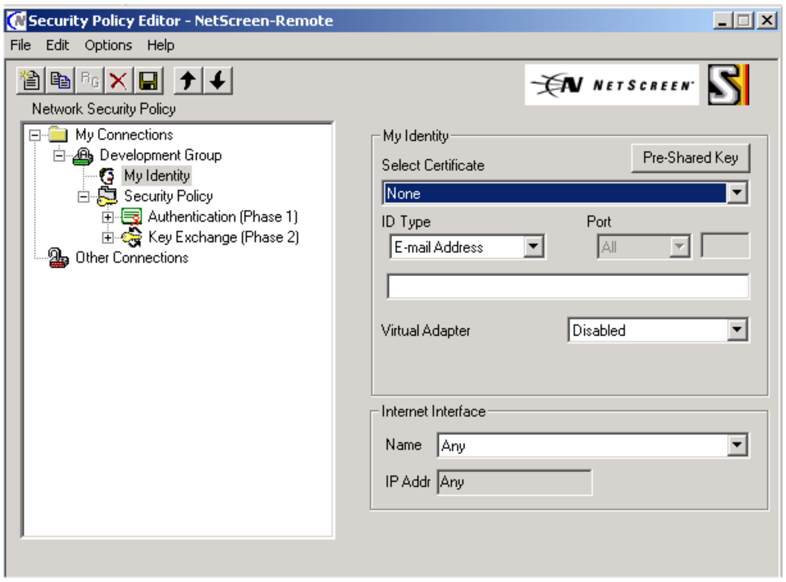
In Step 2, you create the Pre-Shared Key to be used in identifying the communicating parties during the Phase 1 negotiations.

1. Double-click the icon for the new connection.

   My Identity and Security Policy icons appear in the Network Security Policy list.

2. Click **My Identity**.

   The My Identity and Internet Interface areas appear to the right of the Network Security Policy list, as shown below.



Select Certificate: None

ID Type: E-mail Address

Port: All

Virtual Adapter: Disabled

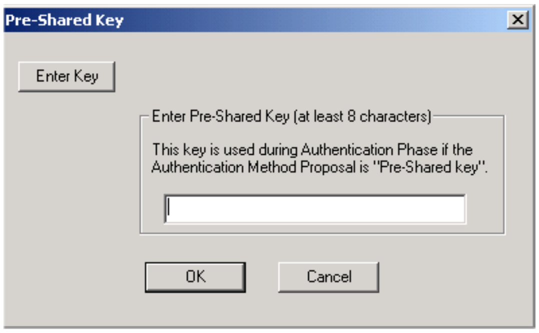
Name: Any

IP Addr: Any

Figure 4-3 My Identity and Internet Interface Areas

3. In the My Identity area, select **None** from the Select Certificate drop-down list.
4. Click **Pre-Shared Key**.

   The Pre-Shared Key dialog box appears, as shown in Figure 4-4.



Pre-Shared Key

Enter Key

Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

Figure 4-4 Pre-Shared Key

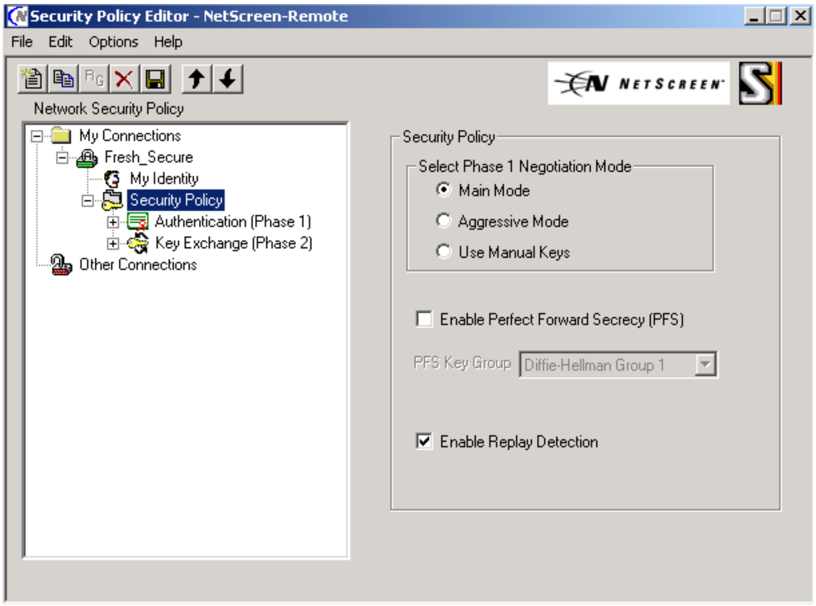
5. Click **Enter Key** to make the Pre-Shared Key field available.
6. Type a key with a length between 8 and 58 characters. A longer key length results in stronger encryption.
7. Click **OK** to save the entry.

Step 3: Defining the IPSec Protocols

In Step 3, you define the Internet Protocol Security (IPSec) protocols for securing the VPN tunnel.

1. Double-click **Security Policy** in the Network Security Policy list.

   The Security Policy area appears on the right, and the Authentication (Phase 1) icon and Key Exchange (Phase 2) icon appear in the Network Security Policy list, as shown below.



Network Security Policy

- My Connections
  - Fresh_Secure
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
      - Key Exchange (Phase 2)
- Other Connections

Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

○ Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

☑ Enable Replay Detection

Figure 4-5 Security Policy Area

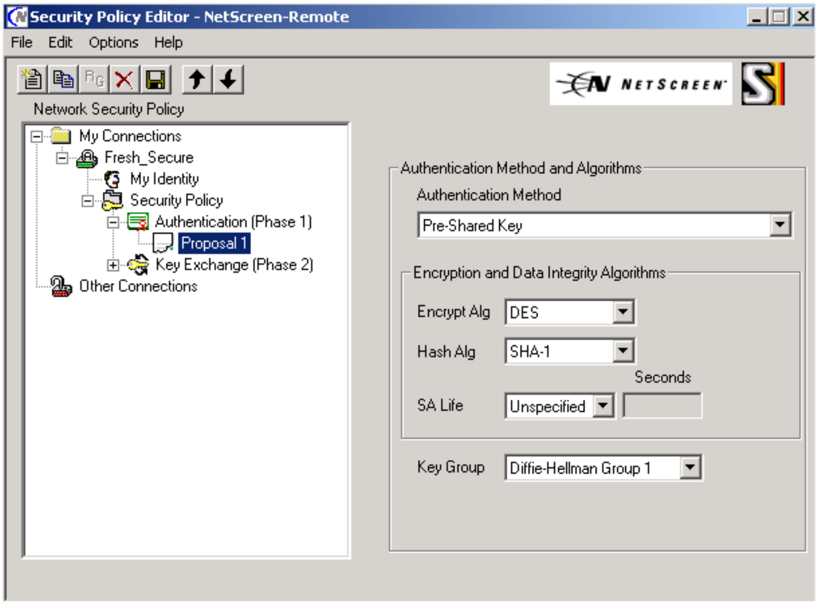
2. If you use another NetScreen product as the security gateway appliance at the other end of the VPN, select **Aggressive Mode** in the Security Policy area if you are using dynamic IP. (If you are using fixed IP, you can select Main Mode.)
3. Select **Enable Perfect Forward Secrecy (PFS)** and **Enable Replay Detection** if you want to employ these options.

   Perfect Forward Secrecy (PFS) is a method that allows the generation of a new encryption key independent from and unrelated to the preceding key.

   Replay Detection is a service in the Authentication Header that detects replay attacks, in which an attacker intercepts a sequence of packets, and then replays them later to gain access to network resources.
4. In the Network Security Policy list, double-click the **Authentication (Phase 1)** icon.

   Proposal 1 appears below the Authentication (Phase 1) icon.

5. Select **Proposal 1** to display the Authentication Method and Algorithms area, as shown below.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: DES

Hash Alg: SHA-1

SA Life: Unspecified Seconds

Key Group: Diffie-Hellman Group 1

Figure 4-6 Authentication Method and Algorithms Area

6. If you will be using XAuth, select **Pre-Share Key-Extended Authentication**.

   XAuth must also be enabled on the NetScreen device. XAuth allows password-prompt authentication in addition to Pre-shared Key. If enabled, you will be prompted for a password when initiating a VPN.

7. In the Authentication and Algorithms area, define the Encryption Algorithm, the Hash Algorithm, and the Security Association (SA) Life.

   To see brief descriptions of the choices in the Authentication Method and Algorithms area, see pages 6-7 and 6-8. Because you selected Pre-Shared Key, that is what appears in the Authentication Method field. Although there is a drop-down list, no other choices are available.

8. In the Key Group drop-down list, select **Diffie-Hellman Group 1**, **Diffie-Hellman Group 2**, or **Diffie-Hellman Group 5**.

   Diffie-Hellman is a key-generation protocol allowing the participants to agree on a key over an insecure channel.

9. Double-click the **Key Exchange (Phase 2)** icon.

Proposal 1 appears below the Key Exchange (Phase 2) icon.

10. Select **Proposal 1** to display the IPSec Protocols area.
11. In the IPSec Protocols area, define the **SA Life** (that is, the lifetime of the Security Association) in either seconds or bytes, or leave it as **Unspecified**.

    Unspecified lifetimes (Phase I and II) will cause NetScreen-Remote to accept the values proposed by the NetScreen device.
12. The Compression feature reduces packet sizes to expedite transmission. To enable compression, choose **Deflate** from the drop-down list; to disable it, choose **None**.

Other NetScreen products do not currently support compression. Because the devices on both ends of the VPN tunnel need to support this feature to be able to use it, leave the setting at ***None****.*

13. Select either **Encapsulation Protocol (ESP)** or **Authentication Protocol (AH)**, and specify the protocols that you want to use.

    ESP provides encryption, authentication, and an integrity check for IP datagrams

    AH provides authentication and an integrity check for IP datagrams

    If you select the **Connect using Secure Gateway Tunnel** check box when defining Remote Party Identity and Addressing, the encapsulation method must be **Tunnel**—no other option is available. If the other end of the VPN does not terminate at a gateway you can select either **Tunnel** or **Transport**, as in the case with L2TP/IPSec.

    To see brief descriptions of the protocols in the IPSec Protocols area, see page 6-7.
14. Click **Save** in the toolbar, or choose **Save Changes** from the File menu.

    The configuration for the NetScreen-Remote end of an eventual VPN tunnel using a Pre-Shared Key is complete.

To configure the NetScreen security gateway at the other end of a VPN tunnel for AutoKey IKE, refer to "Scenario 2: From Home with Pre-Shared Key" on page 7-21 and to the VPN section in the user guide for the specific NetScreen security appliance that you have.

Configuring a VPN Tunnel with Digital Certificates 5

Once configured, an AutoKey, unlike a Manual Key, can automatically change its keys at predetermined intervals using the Internet Key Exchange (IKE) protocol. Frequently changing keys greatly improves security, and automatically doing so greatly reduces key-management responsibilities.

Because digital certificates verify identity by way of a third party, you do not need to find a way to distribute keys securely prior to being able to set up a secure connection. Additionally, if you wish to revoke an individual user access, no changes need to be made on the NetScreen devices. Revoke the certification in your CA.

This chapter explains the basics of configuring the NetScreen-Remote client for IKE operation with digital certificates. For additional information on setting up the security-gateway end of the tunnel with AutoKey IKE functionality, see Chapter 7, "Sample Scenarios" and the *NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 4: VPNs*.

If you will be deploying NetScreen-Remote policies with NetScreen-Remote Global PRO, skip to Chapter 8, "Large Scale Distribution with NetScreen-Global PRO." Chapters 4 to 7 do not apply to you.

Configuring the Client

You can use an AutoKey IKE operation with digital certificates whether the NetScreen-Remote client has a fixed or dynamically assigned IP address.

There are three steps in setting up NetScreen-Remote for a VPN tunnel with a Pre-Shared Key:

1. Creating a New Connection
2. Configuring Identity
3. Defining the IPSec Protocols

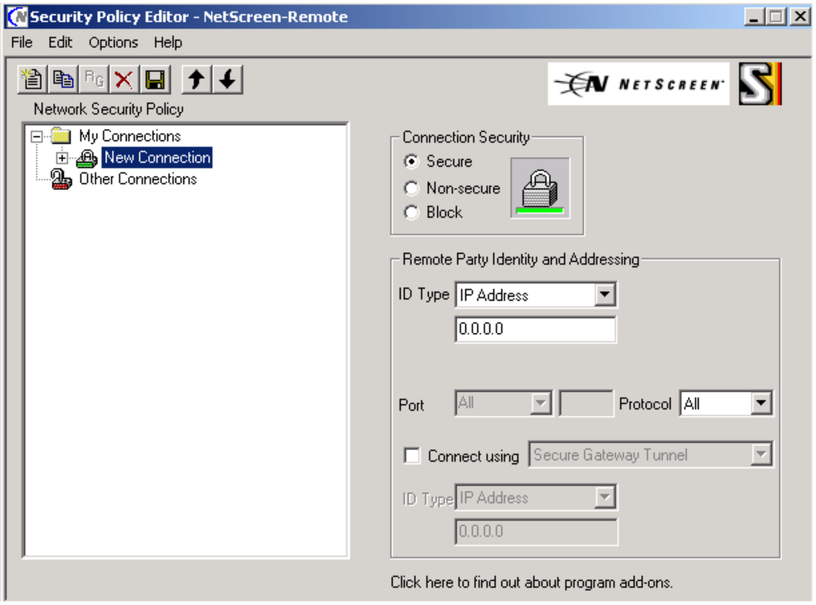
This assumes that you have already requested and installed your Local Certificate, CA Certificate, and CRL into the Certificate Manager.

Step 1: Creating a New Connection

You begin by initiating a new connection. You then name the connection, define it as secure, and determine the identification and location of the other end of the eventual VPN tunnel.

1. Double-click the **NetScreen-Remote** icon to open the Security Policy Editor.
2. On the File menu, choose **New Connection**.

A new connection icon appears, as shown below.



Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Address
0.0.0.0
Port: All
Protocol: All
☐ Connect using: Secure Gateway Tunnel
ID Type: IP Address
0.0.0.0

Click here to find out about program add-ons.

Figure 5-1 New Connection

3. Give the new Connection a unique name.
4. In the Connection Security area, select **Secure**.
5. In the Remote Party Identity and Addressing area, select an identifier for the other party from the ID Type list, and enter the required information.

   To see brief descriptions of the choices in the Remote Party Identity and Addressing area (as well as the restrictions), see “Step 1: Creating a New Connection” on page 6-2.

6. Define the protocol you want to use for the Connection: **All**, **TCP**, **UDP**, **ICMP**. The default is All.
7. If you are using tunnel mode to connect to a NetScreen device, select **Connect using Secure Gateway Tunnel**.

   The Secure Gateway Tunnel ID Type and IP Address fields become available.

8. For ID Type, select **Domain Name** from the ID Type list to identify the other party, then enter the domain name and correct IP address.

   Domain Name is the only option you can select.

Step 2: Configuring the Identity

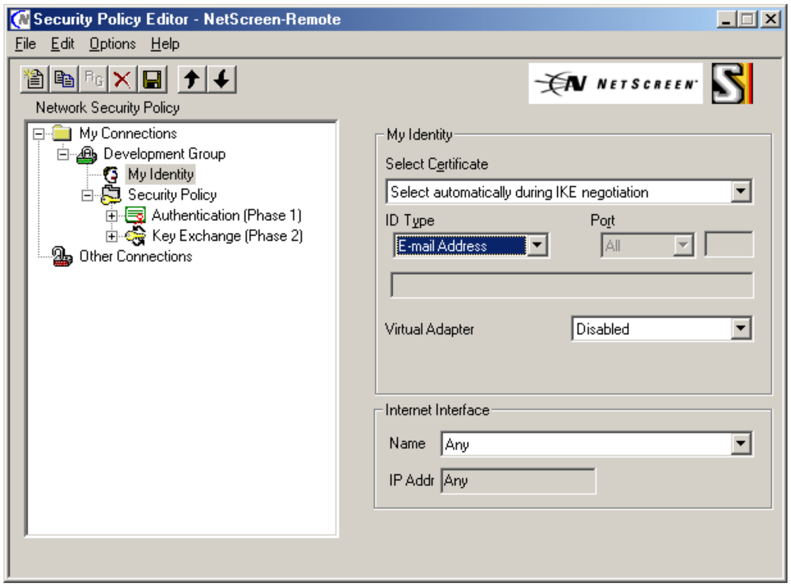
In Step 2, you configure your identity so that the party with whom you want to communicate can verify who you are.

1. Double-click the icon for the new connection.

   My Identity and Security Policy icons appear.

2. Select **My Identity**.

   The My Identity and Internet Interface areas appear, as shown below.



My Identity

Select Certificate: Select automatically during IKE negotiation

ID Type: E-mail Address

Port: All

Virtual Adapter: Disabled

Internet Interface

Name: Any

IP Addr: Any

Figure 5-2 My Identity and Internet Interface Areas

3. Select your certificate from the Select Certificate drop-down list.
4. For the ID Type, select one of these means of identifying yourself during the key exchange phase: **IP Address**, **Domain Name**, or **E-Mail Address**.

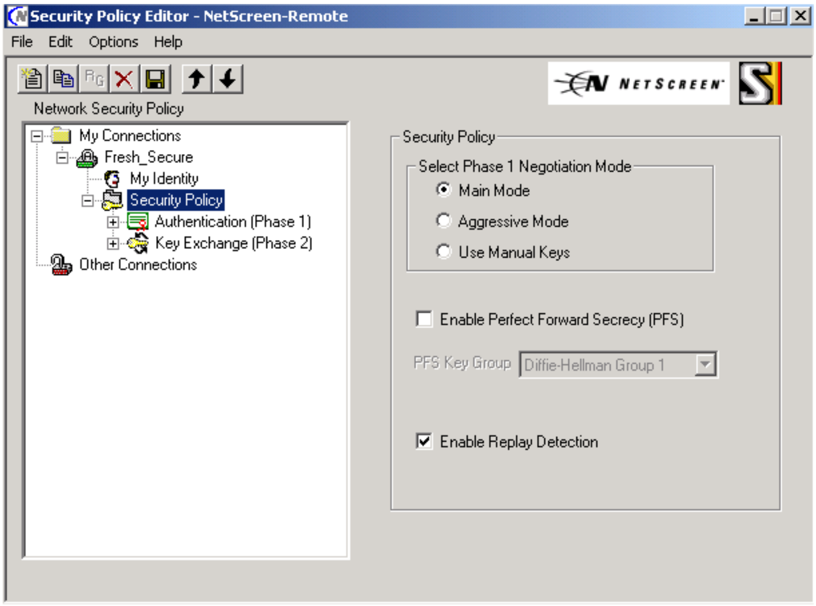
   If necessary, click **View** to display the information that is in your digital certificate.

Step 3: Defining the IPSec Protocols

In Step 3, you define the Internet Protocol Security (IPSec) protocols for securing the VPN tunnel.

1. Double-click **Security Policy** in the Network Security Policy list.

   The Security Policy area appears on the right, and the Authentication (Phase 1) icon and Key Exchange (Phase 2) icon appear in the Network Security Policy list, as shown below.



Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

○ Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

☑ Enable Replay Detection

Figure 5-3 Security Policy Area

2. Select **Aggressive Mode** or **Main Mode** in the Security Policy area.

   If using certificates, either the **Aggressive Mode** or the **Main Mode** can be used for the connection.

3. Select **Enable Perfect Forward Secrecy (PFS)** and **Enable Replay Detection** if you want to employ these options.

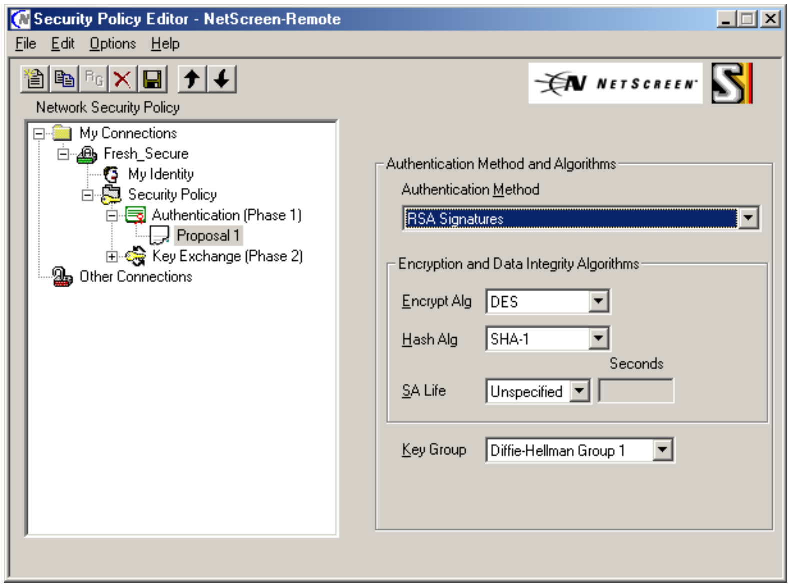
   Perfect Forward Secrecy (PFS) is a method that allows the generation of a new encryption key independent from and unrelated to the preceding key.

   Replay Detection is a service in the Authentication Header that detects replay attacks, in which an attacker intercepts a sequence of packets, and then replays them later to gain access to network resources.

4. In the Network Security Policy list, double-click **Authentication (Phase 1)**.

   Proposal 1 appears below the Authentication (Phase 1) icon.

5. Select **Proposal 1** to display the Authentication Method and Algorithms area, as shown below.



Authentication Method and Algorithms

Authentication Method: RSA Signatures

Encryption and Data Integrity Algorithms

Encrypt Alg: DES

Hash Alg: SHA-1

SA Life: Unspecified; Seconds:

Key Group: Diffie-Hellman Group 1

Figure 5-4 Authentication Method and Algorithms Area

6. In the Authentication and Algorithms area, define the Encryption Algorithm, the Hash Algorithm, and the Security Association (SA) Life.

   To see brief descriptions of the choices in the Authentication Method and Algorithms area, see pages 6-7 and 6-8.

   Because you selected a digital certificate, RSA Signatures is what appears in the Authentication Method field. Although there is a drop-down list, no other choices are available.

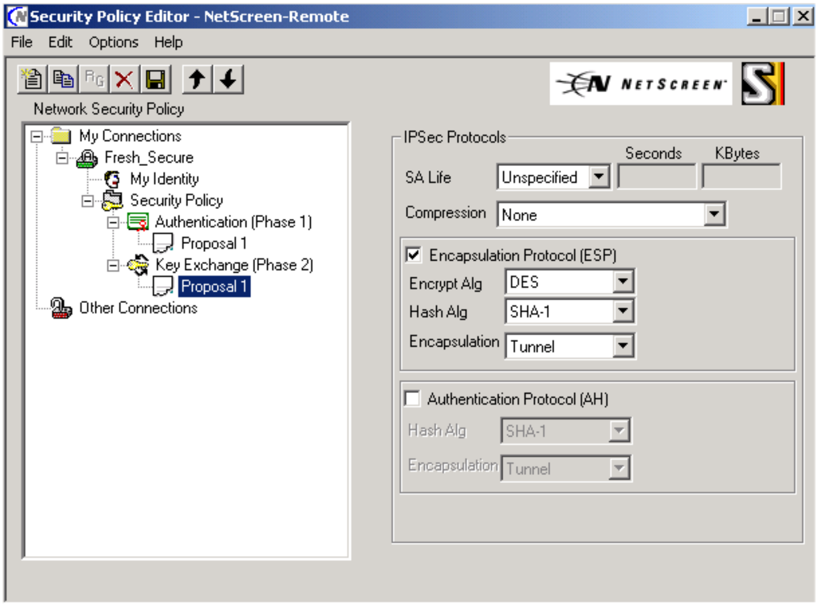
7. In the Key Group drop-down list, select either **Diffie-Hellman Group 1**, **Diffie-Hellman Group 2**, or **Diffie-Hellman Group 5**.

   Diffie-Hellman is a key-exchange protocol allowing the participants to agree on a key over an insecure channel.

8. In the Network Security Policy list, double-click **Key Exchange (Phase 2)**.

   Proposal 1 appears below the Key Exchange (Phase 2) icon.

9. Select **Proposal 1** to display the IPSec Protocols area, as shown below.



IPSec Protocols

SA Life: Unspecified (Seconds: , KBytes:)

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 5-5 IPSec Protocols Area

10. In the IPSec Protocols area, define the **SA Life** (that is, the lifetime of the Security Association) in either seconds or bytes, or leave it as **Unspecified**.

11. The Compression feature reduces packet sizes to expedite transmission. To enable compression, choose **Deflate** from the drop-down list; to disable it, choose **None**.

*Other NetScreen products do not currently support compression. Because the devices on both ends of the VPN tunnel need to support this feature to be able to use it, leave the setting at **None**.*

12. Select **Encapsulation Protocol (ESP)** or **Authentication Protocol (AH)**, and specify the protocols that you want to use:

    ESP provides encryption, authentication, and an integrity check for IP datagrams

    AH provides authentication and an integrity check for IP datagrams.

    If you select **Connect using Secure Gateway Tunnel** when defining Remote Party Identity and Addressing, the encapsulation method must be **Tunnel**—no other option is available. If the other end of the VPN does not terminate at a secure gateway, you can select either **Tunnel** or **Transport**, such as L2TP/IPSec.

    To see brief descriptions of the protocols in the IPSec Protocols area, see page 6-7.

13. Click **Save** on the toolbar or choose **Save Changes** from the File menu.

    The configuration for the NetScreen-Remote end of an eventual VPN tunnel using a digital Certificate is complete.

To configure the NetScreen security gateway at the other end of a VPN tunnel for AutoKey (IKE) with digital certificates, refer to "Scenario 3: From Home with Certificate" on page 7-45 and to the VPN section in the user guide for the specific NetScreen security appliance that you have.

Configuring a Manual Key VPN Tunnel 6

This chapter explains the basics of configuring the NetScreen-Remote client for Manual Key operation.

Manual Key is one method for setting up a VPN tunnel. As the name indicates, you manually set all elements of the connection at both ends of the tunnel. You must manually set the following:

- IP destination address (and, if applicable, secure gateway IP address and subnet mask)
- Security protocol (ESP or AH)
- Security parameter (Tunnel or Transport Mode)
- Authentication and encryption algorithms for the inbound and outbound keys (DES, 3DES, etc...)

Manual Key does not provide a means for automatic key management. That is, you must devise your own method for securely distributing and changing keys. Suggestions for securely transmitting keys are offered in Chapter 9, “Large Scale Distribution (Standalone Procedure)”

For information on setting up the security-gateway end of the tunnel, see Chapter 7, “Sample Scenarios.”

If you will be deploying NetScreen-Remote policies with NetScreen-Remote Global PRO, skip to Chapter 8, “Large Scale Distribution with NetScreen-Global PRO.” Chapters 4 through 7 do not apply to you.

Configuring the NetScreen-Remote Client

There are three steps to set up NetScreen-Remote for a Manual Key VPN tunnel:

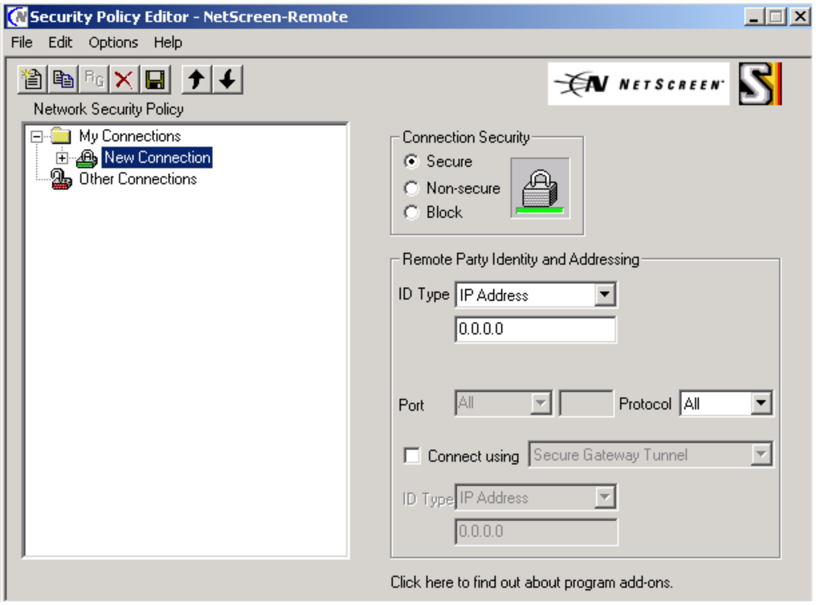
1. Creating a New Connection
2. Defining the IPSec Protocols
3. Creating the Inbound and Outbound Keys

Step 1: Creating a New Connection

You begin by initiating a new connection. You then name the connection, define its connection security, and determine the identification and location of the other end of the eventual VPN tunnel.

1. Double-click the **NetScreen-Remote** icon, located on the Windows taskbar, to open the Security Policy Editor.
2. On the Edit menu, choose **Add,** then select **Connection**.

   A new Connection icon appears in the Network Security Policy list, as shown below.



Connection Security: ● Secure ○ Non-secure ○ Block

Remote Party Identity and Addressing

ID Type: IP Address

0.0.0.0

Port: All

Protocol: All

□ Connect using: Secure Gateway Tunnel

ID Type: IP Address

0.0.0.0

Figure 6-1 New Connection

3. Give the new connection a unique name.
4. In the Connection Security area, select **Secure**.

5. In the Remote Party Identity and Addressing area, select an identifier for the other party from the ID Type list, and enter the required information.

   Your choices are:

   IP Address—Enter the destination IP address in the IP address field.

   Domain Name—Enter the domain name of the destination subnetwork.

   E-mail Address—Enter the destination e-mail address.

   IP Subnet—Enter the destination subnet IP address and subnet mask.

   IP Address Range—Enter the start and end of the destination IP address range.

   Distinguished Name—Click **Edit Name**, and enter information in the Subject Information fields. The information you enter is linked together to create the distinguished name of the destination.

   Entering an IP address or Domain Name separate from the gateway ID is an option.

6. Define the protocol you want to use for the connection.

   Your choices are:

   All—This choice allows the connection to use any IP protocol.

   TCP—Transmission Control Protocol, the protocol that controls data transfer on the Internet

   UDP—User Datagram Protocol, a protocol within the TCP/IP protocol suite that provides very few error recovery services (for example, a lost packet is simply ignored) and is used primarily for broadcasting

   ICMP—Internet Control Message Protocol, a protocol tightly integrated with the Internet Protocol (IP) that supports packets containing error, control, and informational messages related to network operations

   GRE—Generic Routing Encapsulation, a protocol that encapsulates the packets of one kind of protocol within GRE packets, which can then be contained within the packets of another kind of protocol

Note: *Additional protocols may be added by editing the services.txt file in the NetScreen-Remote directory.*

7. If your VPN will terminate tunnel mode to a NetScreen-Remote device, select **Connect using Secure Gateway Tunnel**.

   The Secure Gateway Tunnel ID Type and IP Address fields become available.

8. For ID Type, select an identifier for the other party from the ID Type list, and enter the required information.

   Your choices are:

   Any—Select Gateway IP Address or Gateway Hostname from the drop-down menu.

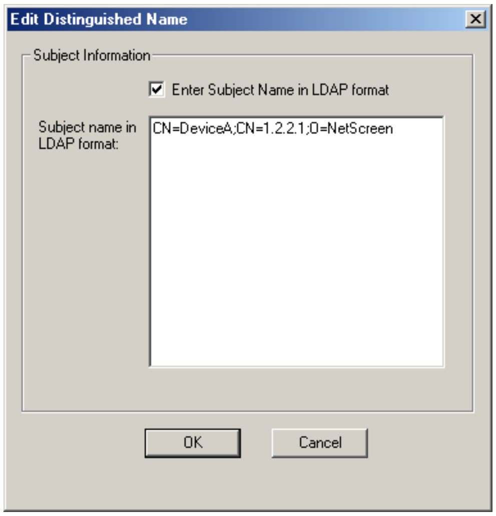
   IP Address—Enter the security gateway IP address in the IP address field.

   Domain Name—Enter the domain name of the security gateway.

   Distinguished Name—Click **Edit Name**, and enter information in the Subject Information fields. The information you enter is linked together to create the distinguished name of the security gateway.

   If preshared key IKE is used, only IP Address will work. If certificate IKE is used, only Domain Name with correct IP address will work.

   If your CA requires more fields, click **Enter Subject Name in LDAP format** and enter the entire **Distinguished Name**.



☑ Enter Subject Name in LDAP format

Subject name in LDAP format: CN=DeviceA;CN=1.2.2.1;O=NetScreen

Figure 6-2 Edit Distinguished Name - Subject Name in LDAP Format

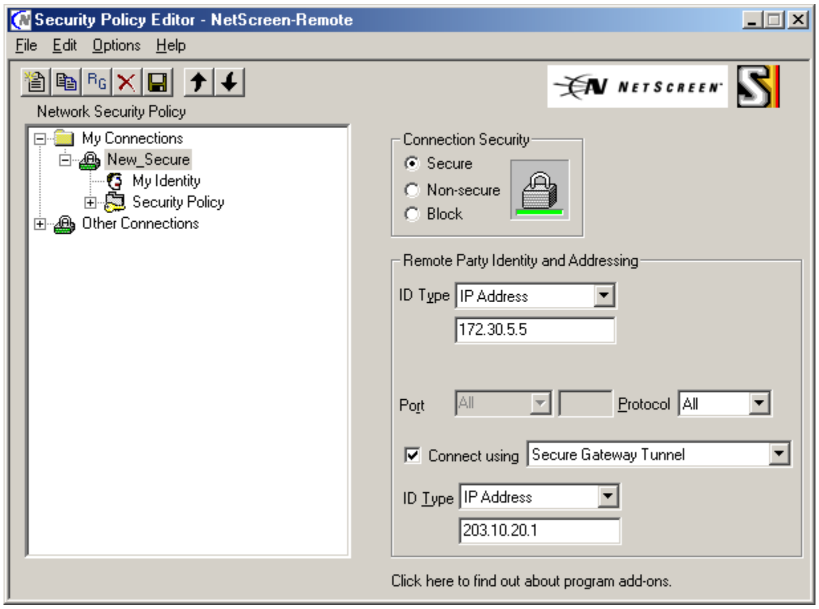
Step 2: Defining the IPSec Protocols

In this procedure, you specify that you will use Manual Keys, and then define the Internet Protocol Security (IPSec) protocols for securing the VPN tunnel.

> *Because the use of Manual Keys eliminates the Authentication phase of establishing a VPN tunnel, you do not need to set any identity authentication parameters.*

1. Double-click the icon of the new connection that you created in the previous procedure.

   Icons for My Identity and Security Policy appear in the Network Security Policy list, as shown below.



Network Security Policy

- My Connections
  - New_Secure
    - My Identity
    - Security Policy
- Other Connections

Connection Security

● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing

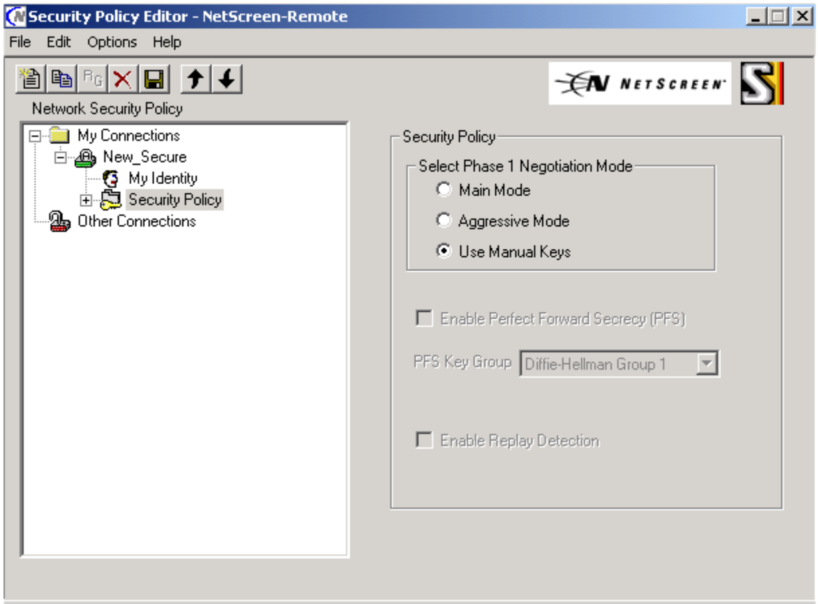
ID Type: IP Address
172.30.5.5
Port: All
Protocol: All
☑ Connect using: Secure Gateway Tunnel
ID Type: IP Address
203.10.20.1

Click here to find out about program add-ons.

Figure 6-3 My Identity and Security Policy Icons

2. Double-click the **Security Policy** icon.

The Security Policy area appears on the right, and icons for Authentication (Phase 1) and Key Exchange (Phase 2) appear in the Network Security Policy list, as shown below.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

○ Aggressive Mode

● Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

□ Enable Replay Detection

Figure 6-4 Security Policy

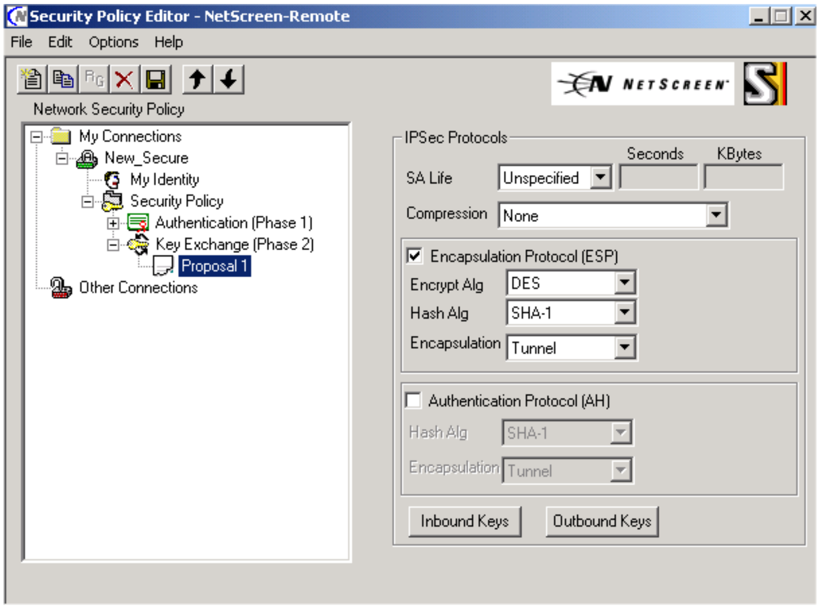
3. Select **Use Manual Keys** in the Security Policy area.

   The Enable Perfect Forward Secrecy (PFS) and Enable Replay Detection options become unavailable.

4. In the Network Security Policy list, double-click **Key Exchange (Phase 2)**.

   Proposal 1 appears in the Network Security Policy list.

5. Click **Proposal 1** to display the IPSec Protocols area, as shown below.



IPSec Protocols

Seconds KBytes

SA Life: Unspecified

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 6-5 IPSec Protocols

6. Because the Security Association (SA) life for Manual Keys is unlimited, leave SA Life set as **Unspecified**.

For security reasons, you should create new keys periodically. The longer that you use the same keys, the greater the chance a hacker has of cracking the keys.

7. To enable compression, choose **Deflate** from the drop-down list. To disable it, choose **None.**

NetScreen devices do not currently support compression. Because the devices on both ends of the VPN tunnel must support this feature to be able to use it, leave the setting at ***None****.*

8. Select **Encapsulation Protocol (ESP)** or **Authentication Protocol (AH)**.

   ESP, the default, provides encryption, authentication, and an integrity check for IP packets. It is the most widely used IPSec protocol.

AH provides authentication and an integrity check for IP packets

9. If you selected **Encapsulation Protocol (ESP)**, select one of the following from the Encryption Algorithm drop-down list:

   DES—Data Encryption Standard is a cryptographic block algorithm with a 56-bit key.

   Triple DES—This is a more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key.

   NULL—No cryptographic algorithm is applied. (NetScreen-Remote requires you to enter a key even if you select **NULL**. Because the key is not used, its content does not matter and can be anything.)

   In the Hash Algorithm drop-down list, select one of the following:

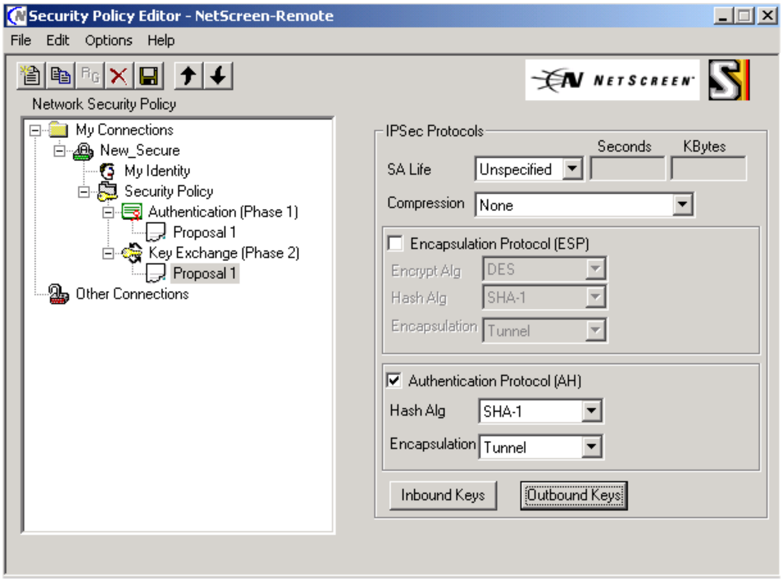
   MD5—Message Digest version 5 is an algorithm that produces a 128-bit message digest or hash from a message of arbitrary length. The resulting hash is used, like a fingerprint of the input, to verify authenticity.

   SHA-1—Secure Hash Algorithm-1 is an algorithm that produces a 160-bit hash from a message of arbitrary length. It is generally regarded as more secure than MD5 because of the larger hashes it produces.

   DES-MAC—Data Encryption Standard–Message Authentication Code is an authentication tag or checksum derived by using the final block of a DES-encrypted cipher text as the checksum.

   NetScreen devices do not support DES-MAC.

If you selected **Authentication Protocol (AH)**, select either **MD5** or **SHA-1** from the Hash Algorithm drop-down list.



SA Life: Unspecified

Compression: None

☐ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

☑ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 6-6 Security Policy Editor: Authentication Protocol (AH) Selected

Then select the Encapsulation method. If you select **Connect using Secure Gateway Tunnel** when defining Remote Party Identity and Addressing, the encapsulation method must be **Tunnel**—no other option is available. If the other end of the VPN does not terminate at a secure gateway, you can select either **Tunnel** or **Transport**, as in the case with L2TP/IPSec.

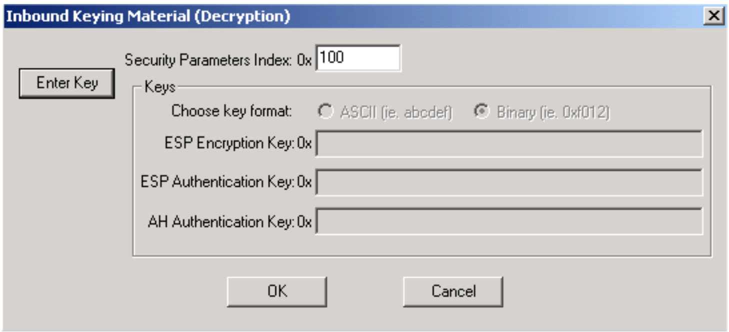
Step 3: Creating the Inbound and Outbound Keys

In this procedure, you create two pairs of keys: one pair to decrypt inbound messages and another pair to encrypt outbound messages. The remote endpoint will be configured to accept the same keys in the reverse direction.

Inbound Keys

1. Click **Inbound Keys** at the bottom of the Security Policy Editor window.

   The Inbound Keying Material (Decryption) dialog box appears.



Inbound Keying Material (Decryption)

Security Parameters Index: 0x 100

Keys

Choose key format: ○ ASCII (ie. abcdef) ● Binary (ie. 0xf012)

ESP Encryption Key: 0x

ESP Authentication Key: 0x

AH Authentication Key: 0x

Figure 6-7 Inbound Keying Material (Decryption)

2. Click **Enter Key** to open the Key fields.

   If you selected Encapsulation Protocol (ESP) in the IPSec Protocols area, only the ESP fields become available—the AH Authentication Key field remains dimmed. The reverse is true if you selected Authentication Protocol (AH).

3. In the Security Parameters Index (SPI) field, enter a unique identifying value of 8 hexadecimal characters.

   The NetScreen security gateway uses the SPI, which is carried in the header of the Security Protocol (ESP or AH), to identify the NetScreen-Remote user's VPN connection proposal. This allows the remote user to make a connection from either a fixed IP address or a dynamically assigned IP address.

4. For the key format, select either **ASCII** or **Binary**.

   ASCII—American Standard Code for Information Interchange is a binary coding system for the set of letters, numbers, and symbols on a standard keyboard.

   Binary—This base-16 (or hexadecimal) numbering system represents binary numbers with 16 characters: 1234567890abcdef.

⚠ **Caution** *If you enter a key in ASCII format, NetScreen-Remote automatically converts it into a corresponding binary code. However, the conversion process is different from that used by other NetScreen security devices, producing different binary codes. For the recommended procedure for creating manual keys, see "Scenario 1: On the Road with Manual Key" on page 7-3.*

5. Enter keys in the available Key fields, depending on the protocol you selected.

   The required key lengths are as follows:

	ASCII (Characters)	Binary (Hexadecimal Characters)
Encapsulation Security Protocol (ESP)		
Encryption Algorithm:		
DES	8	16
Triple DES	24	48
NULL	0	0
Hash Algorithm:		
MD5	16	32
SHA-1	20	40
DES-MAC	8	16
Authentication Protocol (AH)		
Hash Algorithm:		
MD5	16	32
SHA-1	20	40

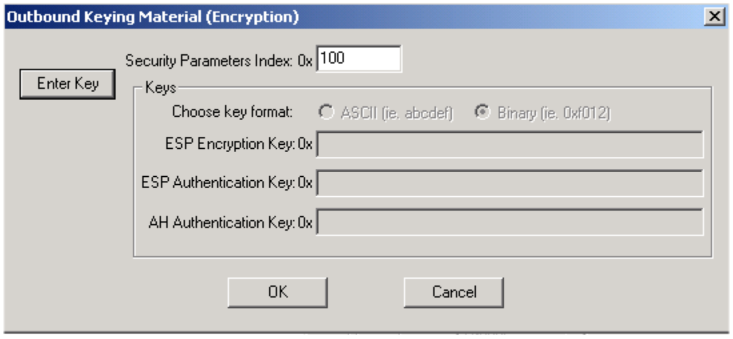
6. Click **OK** to save the settings.

   The Inbound Keying Material (Decryption) dialog box closes.

Outbound Keys

1. Click **Outbound Keys** at the bottom of the Security Policy Editor window.

   The Outbound Keying Material (Encryption) dialog box appears.



Security Parameters Index: 0x 100

Choose key format: ○ ASCII (ie. abcdef) ● Binary (ie. 0xf012)

ESP Encryption Key: 0x

ESP Authentication Key: 0x

AH Authentication Key: 0x

Figure 6-8 Outbound Keying Materials (Encryption)

2. Click **Enter Key** to activate the ESP Encryption Key and Authentication Key fields or the AH Authentication Key field, depending on which IPSec Protocol (ESP or AH) you selected.
3. In the Security Parameters Index (SPI) field, enter a unique identifying value of 8 hexadecimal characters.
4. For the key format, select either **ASCII** or **Binary**.
5. In the Key field(s), type the same key(s) that you used for the Inbound Keys.

If the other end of the VPN is another NetScreen product, the Inbound and Outbound Keys must be the same. Otherwise, they can be different.

6. Click **OK** to save the settings.

   The Outbound Keying Material (Encryption) dialog box closes.

7. Click the **Save** icon or choose **Save Changes** from the File menu.

   The configuration for the NetScreen-Remote end of a Manual Key VPN tunnel is complete.

To configure the NetScreen security gateway at the other end of a Manual Key VPN tunnel, refer to “Scenario 1: On the Road with Manual Key” on page 7-3 and to the VPN section in the user guide for the specific NetScreen security appliance that you have.

Sample Scenarios 7

The four sample scenarios in this chapter illustrate some of the possible uses of the NetScreen-Remote client to create secure virtual private network (VPN) tunnels with other NetScreen devices.

For more information regarding sample scenarios that illustrate uses of NetScreen-Remote client, see Chapter 4, “Policy Based VPNs,” of the *NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 4: VPNs.*

> ***Note:*** *For the most up-to-date ScreenOS graphics, see the latest versions of the ScreenOS user guides.*

If you will be deploying NetScreen-Remote policies with NetScreen-Remote Global PRO, skip to Chapter 8, “Large Scale Distribution with NetScreen-Global PRO.”

You can use the Manual Key method, the Pre-Shared Key/AutoKey IKE method and the Certificate/AutoKey IKE method to create a VPN tunnel from either dynamically assigned or fixed IP addresses.

The four scenarios are:

1. **On the Road with Manual Key:** You are at a hotel. From a dynamically assigned IP address, you create a Manual Key VPN tunnel to your company’s protected network (LAN).
2. **From Home with Pre-Shared Key (Fixed IP Address):** You are at your home office. From a fixed IP address, you create a Pre-Shared/AutoKey (IKE) VPN tunnel to a subnet on your company’s protected LAN.
3. **From Home with Certificate (Dynamic IP Address):** You are at your home office. From a dynamically assigned IP address, you create a Certificate/AutoKey IKE VPN tunnel to a computer on your company’s protected LAN.
4. **Back in the Office:** You have returned to your office. Now that your computer is behind the firewall, you no longer need to use a VPN tunnel, so you deactivate the security feature.

In scenario 1, the LAN is protected by the NetScreen-100. In scenarios 2 and 3, the LAN is protected by the NetScreen-5XP. For each scenario except the last, the following information is given:

- the data required to create a VPN tunnel

- how to configure the network security device and the remote client
- what happens when you initiate a connection

Scenario 1: On the Road with Manual Key

In this scenario, you are on a business trip. From your hotel, you want to create a VPN tunnel to your computer at your company's office. You are using the NetScreen-Remote client, and your company's network is protected by the NetScreen-100. The VPN tunnel that you create will secure the connection from your hotel to the company network, or more precisely, from your laptop to the NetScreen-100 device, as shown below.

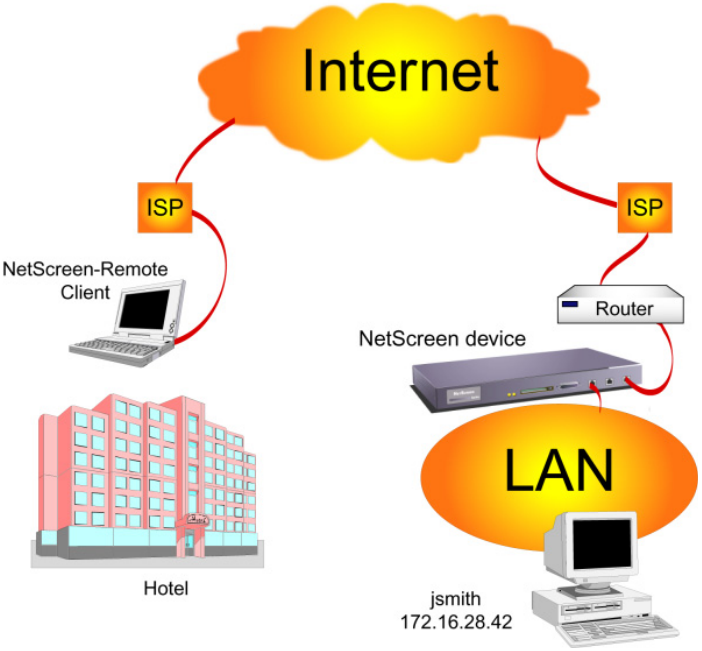


Figure 7-1 Hotel to Protected LAN

To set up the VPN tunnel, you must configure both the NetScreen-Remote client and the NetScreen-100 device. In this example, you will use the following settings:

- **Connection/User Name:** Joe/Joe
- **Connection Policy:** NetScreen-100, Encrypt; NetScreen-Remote, Secure
- **NetScreen-100 (Untrusted Port) IP Address:** 205.186.1.254
- **IP Address/Name of Computer on the LAN:** 172.16.28.42/jsmith
- **Remote Client IP Address:** Dynamically assigned by ISP
- **Negotiation Mode:** Manual Keys
- **IPSec Protocol:** Encapsulation Protocol (ESP)
- **Encryption Algorithm:** DES
- **Hash Algorithm:** MD5
- **Encapsulation Method:** Tunnel
- **Security Parameters Index (SPI):** 5555 (Inbound SPI on NetScreen-Remote; Remote SPI on the NetScreen-100); 6666 (Outbound; Local)
- **Inbound/Outbound ESP Encryption Key:** NetScreen123456NetScreen
- **Inbound/Outbound ESP Authentication Key:** NetScreen0123456
- **SA (Security Association) Life:** Unspecified

Setting Up the NetScreen-100

To create a successful VPN tunnel, you must set up the devices on both ends of the tunnel with identical VPN tunnel configurations.

There are two steps for setting up the NetScreen-100 for a Manual Key VPN tunnel:

1. Adding a new VPN dialup user to the User List

2. Adding a new Access Policy for the user

This example assumes the following:

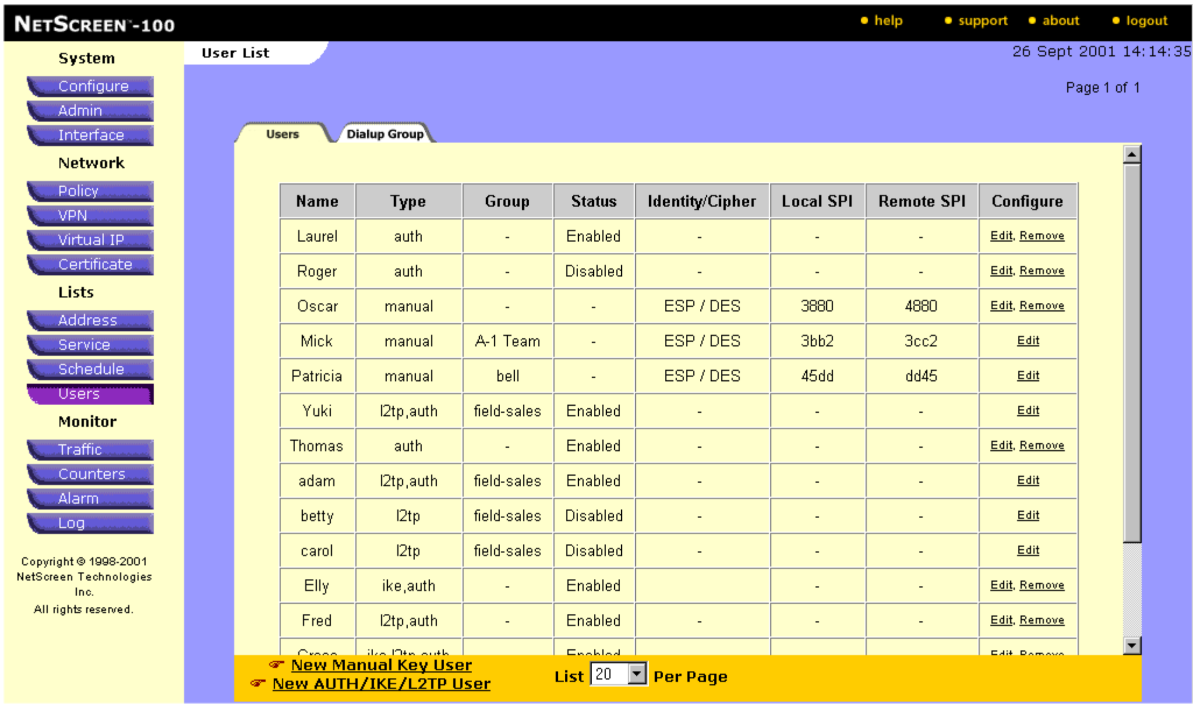
- *The protected LAN is already established.*
- *Your computer on the LAN has been assigned the IP Address 172.16.28.42, and it has a default gateway pointing to the Trusted port of the NetScreen-100 device.*
- *The IP address has been entered in the Trusted Address Book, and associated with the name "jsmith."*
- *The NetScreen-100 is operating in Network Address Translation (NAT) mode.*

Step 1: Adding a New VPN Dialup User

Before you can create an Access Policy for yourself, you must be listed in the User List.

1. Click the **Users** button, located under Lists in the menu column.

   The User Lists page appears, as shown below.



User List

26 Sept 2001 14:14:35

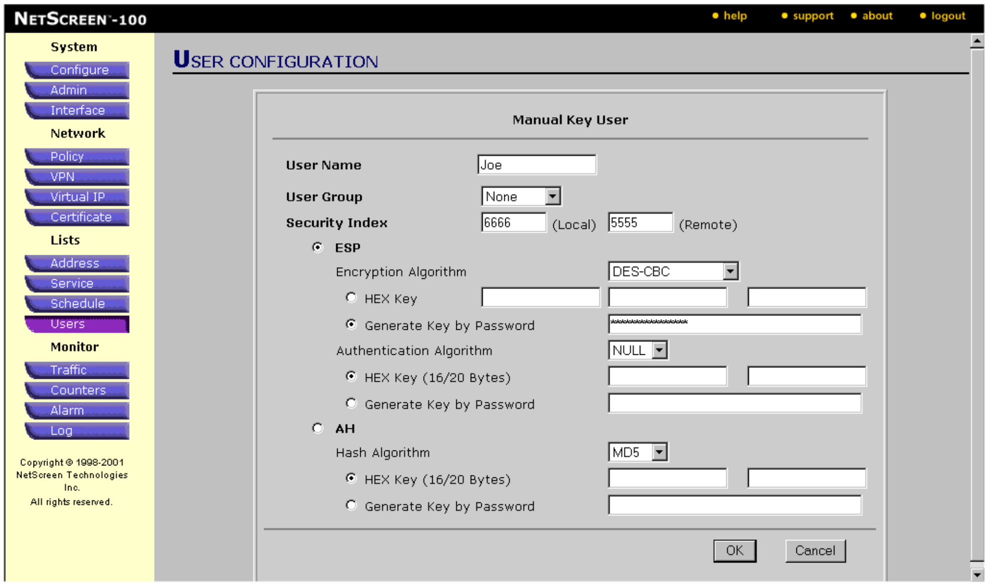
Page 1 of 1

Name	Type	Group	Status	Identity/Cipher	Local SPI	Remote SPI	Configure
Laurel	auth	-	Enabled	-	-	-	Edit, Remove
Roger	auth	-	Disabled	-	-	-	Edit, Remove
Oscar	manual	-	-	ESP / DES	3880	4880	Edit, Remove
Mick	manual	A-1 Team	-	ESP / DES	3bb2	3cc2	Edit
Patricia	manual	bell	-	ESP / DES	45dd	dd45	Edit
Yuki	l2tp,auth	field-sales	Enabled	-	-	-	Edit
Thomas	auth	-	Enabled	-	-	-	Edit, Remove
adam	l2tp,auth	field-sales	Enabled	-	-	-	Edit
betty	l2tp	field-sales	Disabled	-	-	-	Edit
carol	l2tp	field-sales	Disabled	-	-	-	Edit
Elly	ike,auth	-	Enabled		-	-	Edit, Remove
Fred	l2tp,auth	-	Enabled	-	-	-	Edit, Remove
Greg	ike,l2tp,auth		Enabled				Edit, Remove

Figure 7-2 User Lists Page

2. Click **New Manual Key User**, in the lower-left corner of the page.

The User Configuration dialog box appears, as shown below.



USER CONFIGURATION

Manual Key User

User Name: Joe

User Group: None

Security Index: 6666 (Local) 5555 (Remote)

● ESP

Encryption Algorithm: DES-CBC

○ HEX Key

● Generate Key by Password: ********************

Authentication Algorithm: NULL

● HEX Key (16/20 Bytes)

○ Generate Key by Password

○ AH

Hash Algorithm: MD5

● HEX Key (16/20 Bytes)

○ Generate Key by Password

Figure 7-3 User Configuration

3. In the User Name field, type **Joe**, and select **VPN Dialup User**.
4. In the VPN Dialup User section, enter the following information:
   - **User Group:** None
   - **Security Index:** 6666 (Local); 5555 (Remote)
   - **ESP-Encryption Algorithm:** DES-CBC

     Key: (Leave empty)

     Generate Key by Password: NetScreen123456NetScreen
   - **ESP-Authentication Method:** MD5

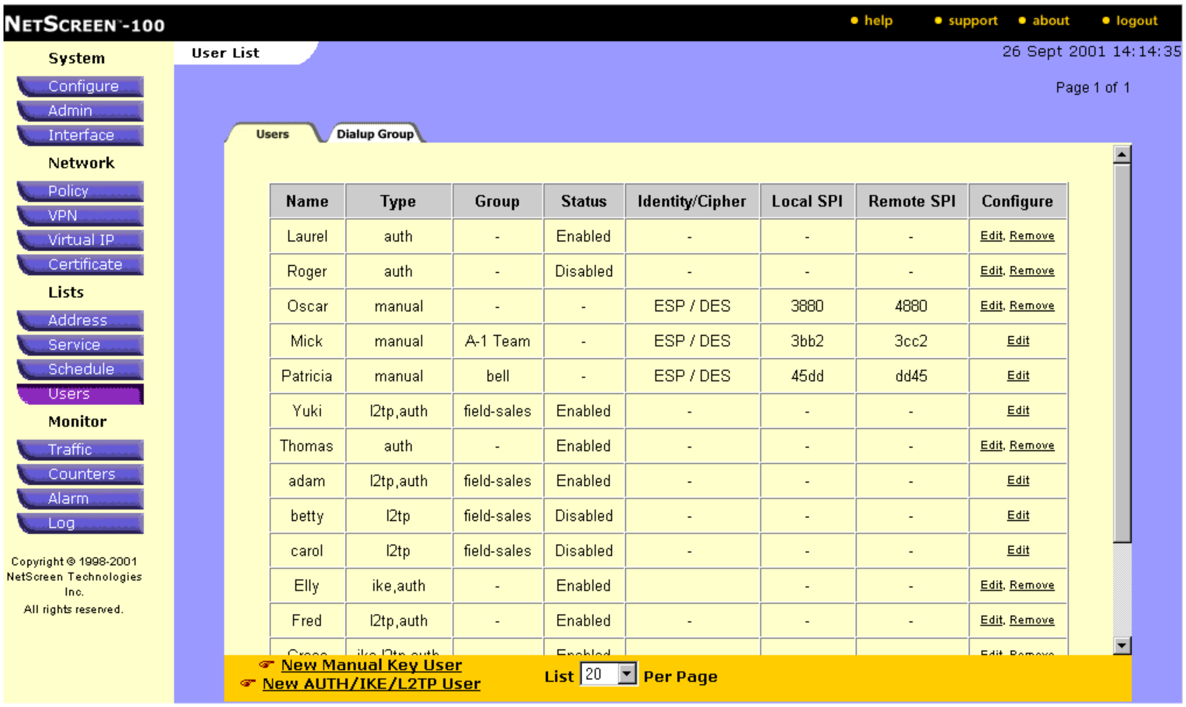
     Key: (Leave empty)

     Generate Key by Password: NetScreen0123456

The password can be up to 31 characters long.

5. Click **OK** to enter your settings.

   The Users List page appears, with the new user information listed, as shown below.



User List

26 Sept 2001 14:14:35

Page 1 of 1

Name	Type	Group	Status	Identity/Cipher	Local SPI	Remote SPI	Configure
Laurel	auth	-	Enabled	-	-	-	Edit, Remove
Roger	auth	-	Disabled	-	-	-	Edit, Remove
Oscar	manual	-	-	ESP / DES	3880	4880	Edit, Remove
Mick	manual	A-1 Team	-	ESP / DES	3bb2	3cc2	Edit
Patricia	manual	bell	-	ESP / DES	45dd	dd45	Edit
Yuki	l2tp,auth	field-sales	Enabled	-	-	-	Edit
Thomas	auth	-	Enabled	-	-	-	Edit, Remove
adam	l2tp,auth	field-sales	Enabled	-	-	-	Edit
betty	l2tp	field-sales	Disabled	-	-	-	Edit
carol	l2tp	field-sales	Disabled	-	-	-	Edit
Elly	ike,auth	-	Enabled		-	-	Edit, Remove
Fred	l2tp,auth	-	Enabled	-	-	-	Edit, Remove
Grace	ike,l2tp,auth		Enabled				Edit, Remove

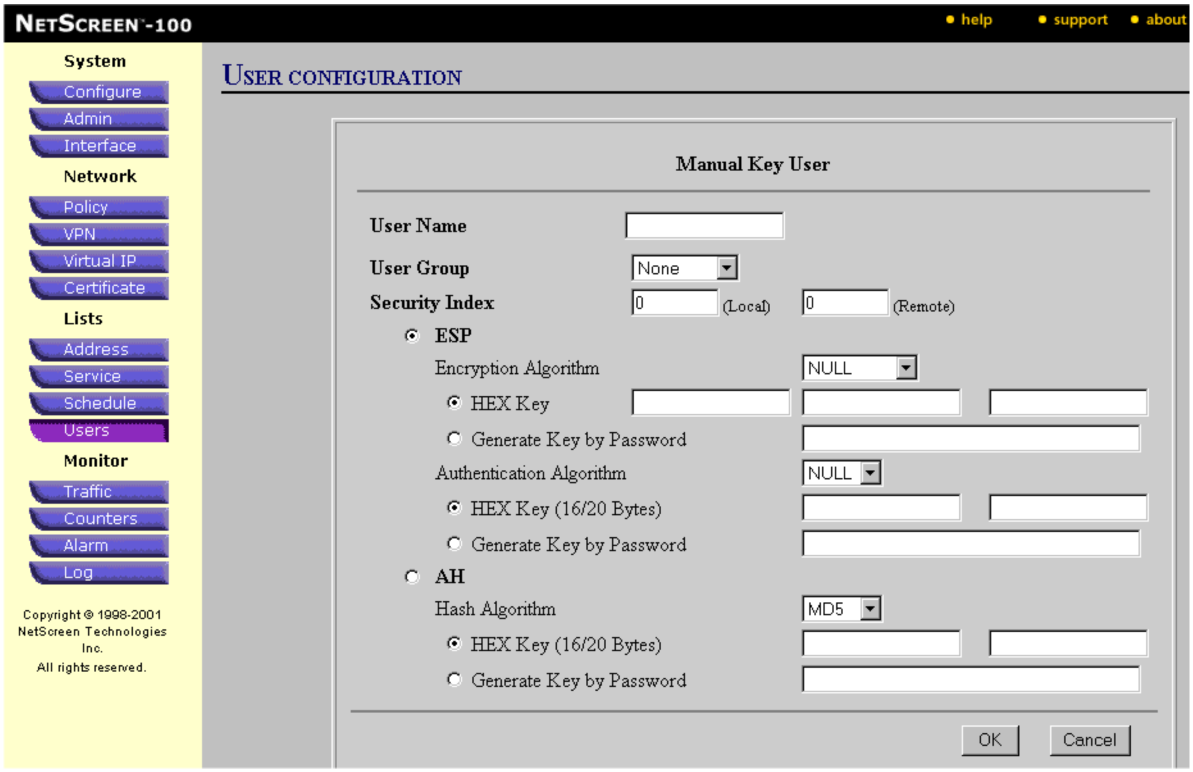
List 20 Per Page

Figure 7-4 Users List with New User Added

To remove a user from the Users List, you must first remove the Access Policy that is associated with him or her. Then return to the Users List page, and click ***Remove*** *in the row for the user you want to remove.*

6. To see the key in binary format, click **Edit** in the row for Joe.

The User Configuration dialog box reopens, displaying the generated key in binary format, as shown below.



Manual Key User

User Name

User Group: None

Security Index: 0 (Local) 0 (Remote)

● ESP

Encryption Algorithm: NULL

● HEX Key

○ Generate Key by Password

Authentication Algorithm: NULL

● HEX Key (16/20 Bytes)

○ Generate Key by Password

○ AH

Hash Algorithm: MD5

● HEX Key (16/20 Bytes)

○ Generate Key by Password

Figure 7-5 Keys in Binary Format

7. Record the keys.

   You need the keys in binary format to set up NetScreen-Remote.

Step 2: Creating an Access Policy

Now that you are listed in the Users List, you must create an Access Policy for yourself.

1. Click **Policy**, located under Network in the menu column.

   The Access Policies pages appear, with the Incoming Access Policies page in front.

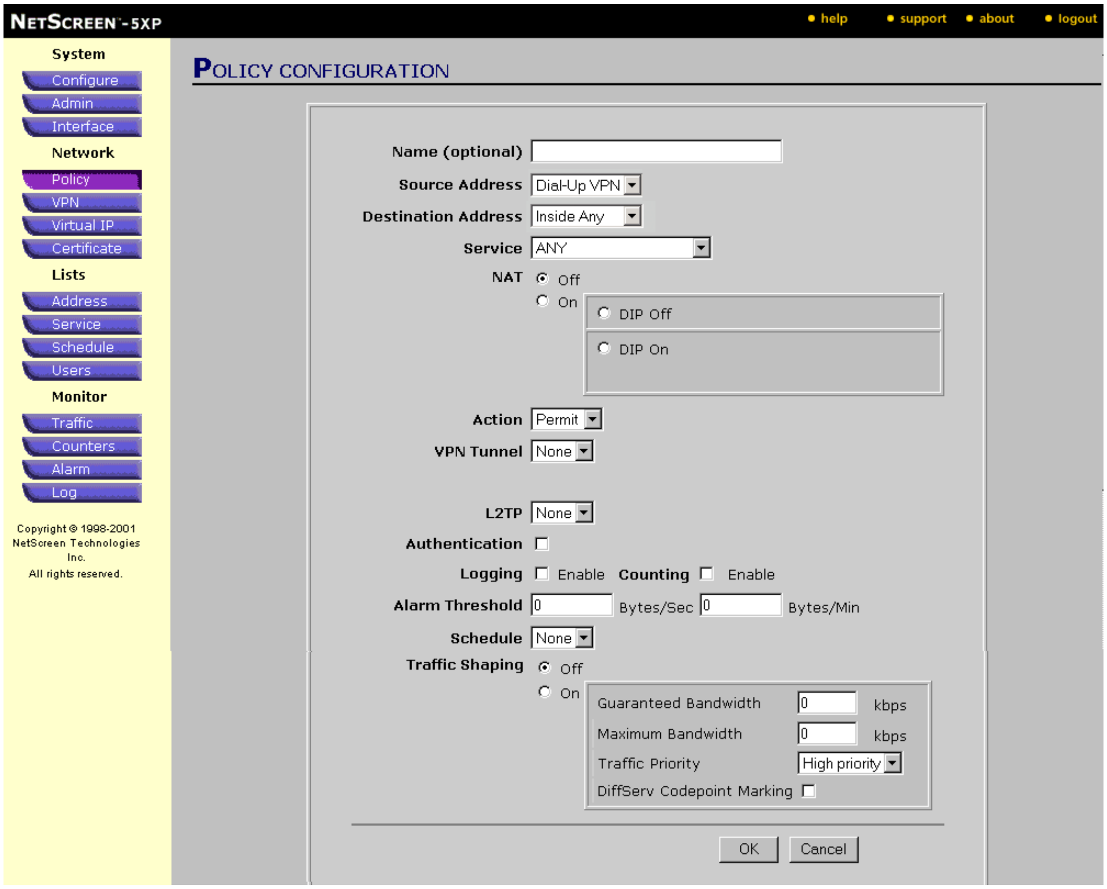
   Although VPN Access Policies are defined for Outgoing traffic, VPN Access Policies assume bidirectional traffic and that the destination address can also originate VPN sessions.

2. Click **New Policy**, located in the lower-left corner of the page.

   The Policy Configuration dialog box appears.

3. Enter the following information (shown in Figure 7-6):
   - **Name:** Joe's Policy
   - **Source Address:** jsmith (the name associated with IP address 172.16.28.42)
   - **Destination:** Dial-Up VPN
   - **Service:** Any
   - **Action:** Encrypt
   - **VPN Tunnel:** Dialup User – Joe

   Leave the remaining fields at their default values.



POLICY CONFIGURATION

Name (optional)
Source Address: Dial-Up VPN
Destination Address: Inside Any
Service: ANY
NAT: ● Off ○ On
○ DIP Off
○ DIP On
Action: Permit
VPN Tunnel: None
L2TP: None
Authentication □
Logging □ Enable Counting □ Enable
Alarm Threshold: 0 Bytes/Sec 0 Bytes/Min
Schedule: None
Traffic Shaping: ● Off ○ On
Guaranteed Bandwidth: 0 kbps
Maximum Bandwidth: 0 kbps
Traffic Priority: High priority
DiffServ Codepoint Marking □

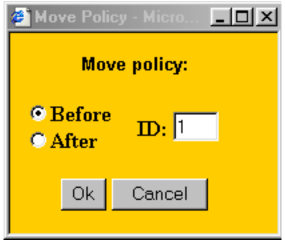
Figure 7-6 Policy Configuration Dialog Box with New Information

4. Click **OK** to enter your settings.

The Incoming Access Policies page appears, with the new Access Policy added.

5. Because the VPN Access Policy is more restrictive than the generic “Inside Any / Outside Any” policy, it needs to be at the top of the list of Access Policies. To change the position of an Access Policy, click the ↕ icon in the row for the Access Policy you want to move.

   The Move Policy dialog box appears.



Move policy:

● Before
○ After

ID: 1

Figure 7-7 Move Policy

6. Enter the new position for the Access Policy, and then click **OK** to save your settings.

*To change an existing Access Policy, click **Detail** in the row for the Access Policy that you want to change. The Policy Configuration dialog box for the selected Access Policy re-opens.*

*To remove an existing Access Policy, click **Remove** in the row for the Access Policy that you want to remove.*

The NetScreen security-appliance end of the eventual Manual Key VPN tunnel is complete.

Setting Up NetScreen-Remote

There are three steps to set up NetScreen-Remote for a Manual Key VPN tunnel:

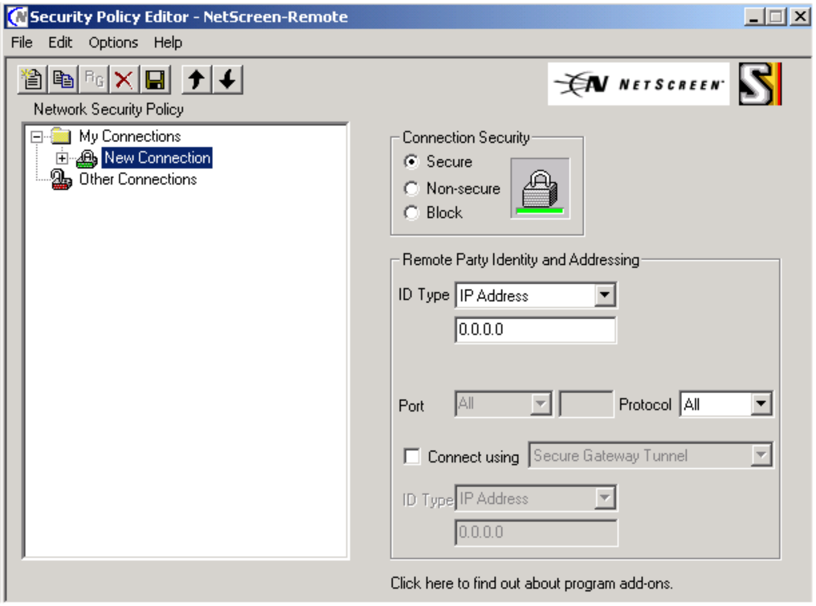
1. Creating a New Connection
2. Defining the IPSec Protocols
3. Creating the Inbound and Outbound Keys

Step 1: Creating a New Connection

You begin by initiating a new connection. You then name the connection, define it as secure, and determine the identification and location of the other end of the eventual VPN tunnel (that is, your computer on your company's protected network).

1. Double-click the **NetScreen-Remote** icon to open the Security Policy Editor.
2. On the File menu, choose **New Connection**.

   A new connection icon appears in the Network Security Policy list, as shown below.



Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Address
0.0.0.0
Port: All
Protocol: All
□ Connect using: Secure Gateway Tunnel
ID Type: IP Address
0.0.0.0

Figure 7-8 New Connection

3. Name the new connection **Joe**.

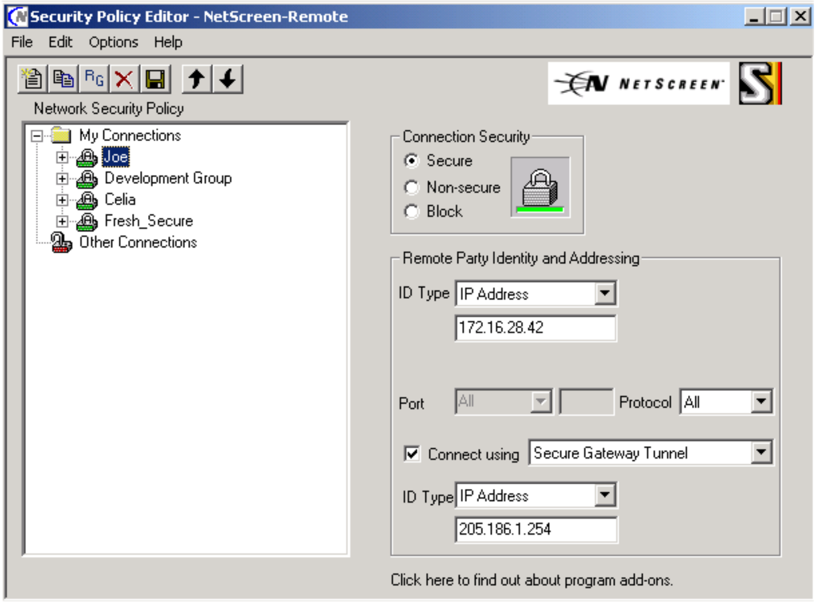
   This name does not have to be the same at both ends of the VPN tunnel.

4. In the Connection Security area, located to the right of the Network Security Policy list, select **Secure**.
5. In the Remote Party Identity and Addressing areas, select **IP Address**, and in the IP Address field, type **`172.16.28.42`**.
6. Leave Protocol set at **All**.
7. Select **Connect using Secure Gateway Tunnel**.

   The Secure Gateway Tunnel ID Type and IP Address fields become available.

8. For ID Type, choose **IP Address**, and in the IP Address field, type **`205.186.1.254`**.

   The completed Connection Security and Remote Party Identity and Addressing areas are shown below.



Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Address
172.16.28.42
Port: All
Protocol: All
☑ Connect using: Secure Gateway Tunnel
ID Type: IP Address
205.186.1.254

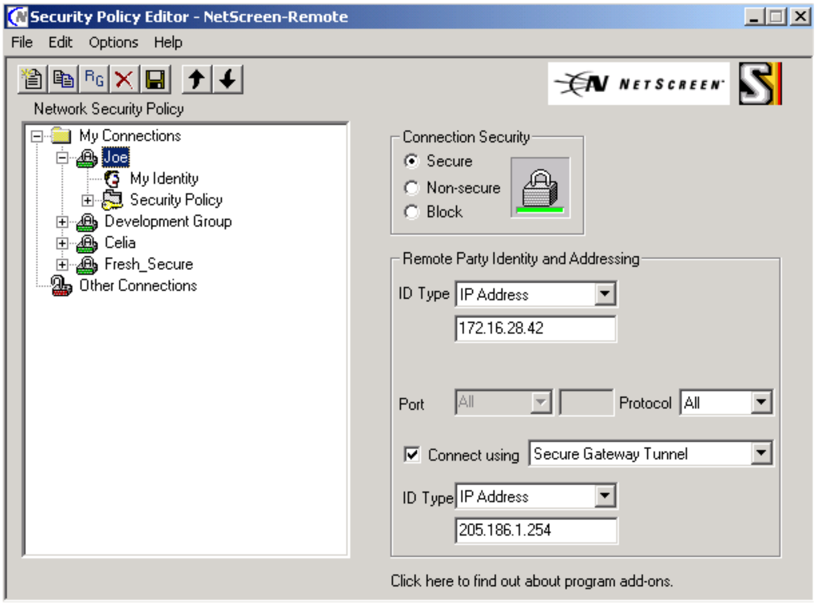
Figure 7-9 Connection Security, Remote Party Identity and Addressing

Step 2: Defining the IPSec Protocols

In Step 2, you specify that you will use Manual Keys. You then define the IPSec protocols for securing the VPN tunnel.

1. Double-click the **Joe** icon.

   My Identity and Security Policy icons appear in the Network Security Policy list.



Network Security Policy

- My Connections
  - Joe
    - My Identity
    - Security Policy
  - Development Group
  - Celia
  - Fresh_Secure
- Other Connections

Connection Security

● Secure

○ Non-secure

○ Block

Remote Party Identity and Addressing

ID Type: IP Address

172.16.28.42

Port: All

Protocol: All

☑ Connect using: Secure Gateway Tunnel

ID Type: IP Address

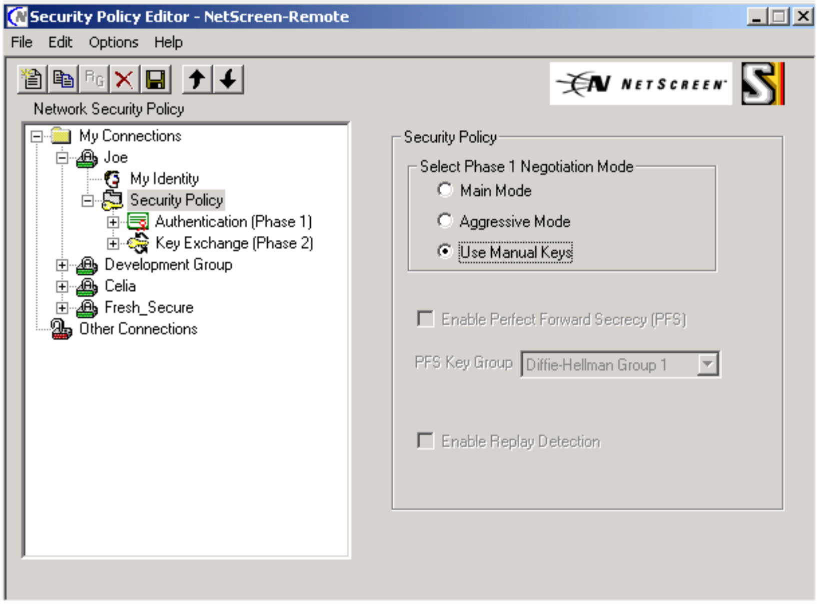
205.186.1.254

Click here to find out about program add-ons.

Figure 7-10 My Identity and Security Policy Icons

2. Double-click **Security Policy** in the Network Security Policy list.

   The Security Policy area appears on the right, and the Authentication (Phase 1) and Key Exchange (Phase 2) icons appear in the Network Security Policy list, as shown below.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

○ Aggressive Mode

● Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

□ Enable Replay Detection

Figure 7-11 Security Policy Area

3. Select **Use Manual Keys** in the Security Policy area.

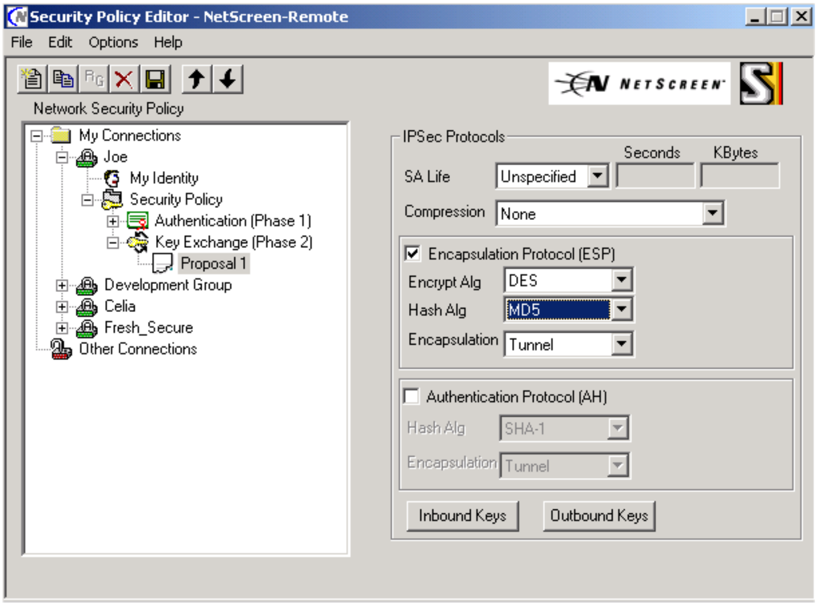
   The Enable Perfect Forward Secrecy (PFS) and Enable Replay Detection check boxes become unavailable.

4. Double-click **Key Exchange (Phase 2)**.

   Proposal 1 appears in the Network Security Policy list.

   Because the use of Manual Keys eliminates the Authentication phase (Phase 1) of establishing a VPN tunnel, you do not need to set any identity authentication parameters.

5. Select **Proposal 1** to display the IPSec Protocols area, as shown below.



IPSec Protocols

SA Life: Unspecified (Seconds, KBytes)

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: MD5

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 7-12 IPSec Protocols Area

6. Leave SA Life set as **Unspecified**.
7. Select **Encapsulation Protocol (ESP)**.
8. In the Encryption Algorithm drop-down list, select **DES**.
9. In the Hash Algorithm drop-down list, select **MD5**.
10. For the encapsulation method, select **Tunnel**.

Step 3: Creating the Inbound and Outbound Keys

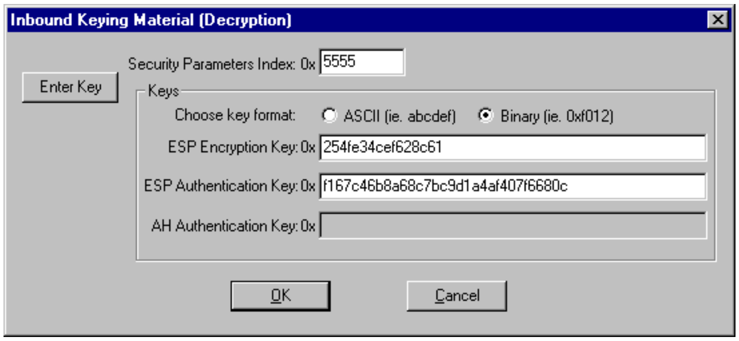
You will create two pairs of keys: one pair to decrypt inbound messages and another pair to encrypt outbound messages.

> *To ensure compatibility between NetScreen-Remote and the current version of other NetScreen products, use the same keys for both the Inbound and Outbound Keys.*

Inbound Keys

1. Click **Inbound Keys**, near the bottom of the Security Policy Editor.

   The Inbound Keying Material (Decryption) dialog box appears.



Inbound Keying Material (Decryption)

Security Parameters Index: 0x 5555

Keys

Choose key format: ○ ASCII (ie. abcdef) ● Binary (ie. 0xf012)

ESP Encryption Key: 0x 254fe34cef628c61

ESP Authentication Key: 0x f167c46b8a68c7bc9d1a4af407f6680c

AH Authentication Key: 0x

Figure 7-13 Inbound Keying Material (Decryption)

2. Click **Enter Key** to open the ESP Encryption Key and ESP Authentication Key fields.

   Because you selected Encapsulation Protocol (ESP) in the IPSec Protocols area, only the ESP fields become available. The AH Authentication Key field remains dimmed.

3. In the Security Parameters Index field, enter **5555**.
4. Select **Binary** as the key format.
5. In the ESP Encryption Key field, type in the key that you recorded when you set up the NetScreen-100: **`254fe34cef628c61`**

6. In the ESP Authentication Key field, type in the following key: **`f167c46b8a68c7bc9d1a4af407f6680c`**

The key length for a DES Encryption Key must be 16 hexadecimal characters. The key length for an MD5 Authentication Key must be 32 hexadecimal characters. For the key lengths for other IPSec protocols, see "Inbound Keys" on page 6-9.

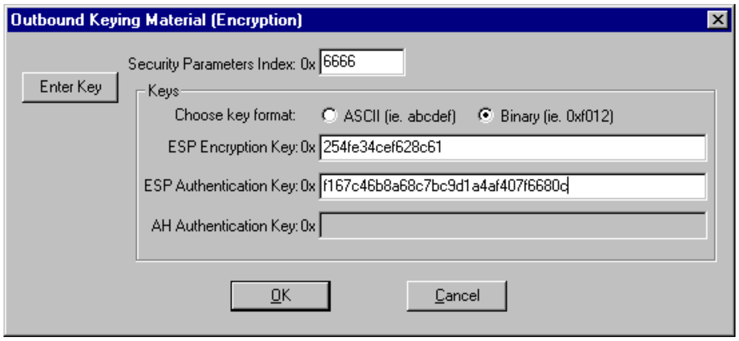
7. Click **OK** to save the settings.

   The Inbound Keying Material (Decryption) dialog box closes.

Outbound Keys

1. Click **Outbound Keys**, near the bottom of the Security Policy Editor.

   The Outbound Keying Material (Encryption) dialog box appears.



Outbound Keying Material (Encryption)

Security Parameters Index: 0x 6666

Keys

Choose key format: ○ ASCII (ie. abcdef) ● Binary (ie. 0xf012)

ESP Encryption Key: 0x 254fe34cef628c61

ESP Authentication Key: 0x f167c46b8a68c7bc9d1a4af407f6680c

AH Authentication Key: 0x

Figure 7-14 Outbound Keying Material (Encryption)

2. Click **Enter Key** to open the ESP Encryption Key and ESP Authentication Key fields.
3. In the Security Parameters Index field, enter **`6666`**.
4. Select **Binary**.
5. In the ESP Encryption Key field, type in the following key: **`254fe34cef628c61`**
6. In the ESP Authentication Key field, type in the following key: **`f167c46b8a68c7bc9d1a4af407f6680c`**

You must use the same keys as for the Inbound Keys.

7. Click **OK** to save the settings.

The Outbound Keying Material (Decryption) dialog box closes.

8. Click the **Save** icon on the toolbar or choose **Save Changes** from the File menu.

   The configuration for the NetScreen-Remote end of the eventual Manual Key VPN tunnel is complete.

Making a Connection

With both ends of the tunnel configured, you are ready to make a secure VPN tunnel connection.

1. Launch your Web browser.
2. Enter the IP address of your computer on the protected network: **`http://172.16.28.42`**

   NetScreen-Remote, which continually checks all IP addresses that you enter, recognizes this address as the one you configured for a secure connection. It routes the transmission to the security gateway (that is, the untrusted port of the NetScreen-100) and proposes the VPN tunnel connection.

   The NetScreen-100 responds to this proposal by checking its database until it finds the Access Policy defining the proposed connection as a VPN tunnel.

   With the settings at both ends in accord, NetScreen-Remote and the NetScreen-100 begin using the Manual Keys and the specified ESP encryption (DES) and authentication (MD5) algorithms to secure the connection.

   The VPN tunnel is established.

Scenario 2: From Home with Pre-Shared Key

In this scenario, you need to access your company's protected network (LAN) from your home office. You have a digital subscriber line (DSL), and your Internet service provider (ISP) has assigned you a fixed IP address.

You want to create a VPN tunnel to your company's LAN using the Pre-Shared Key/AutoKey IKE method. You are using the NetScreen-Remote client, and your company's network is protected by the NetScreen-5XP, which is configured for Network Address Translation (NAT). The VPN tunnel that you create will secure the connection from your computer to the NetScreen-5XP device, as shown below.

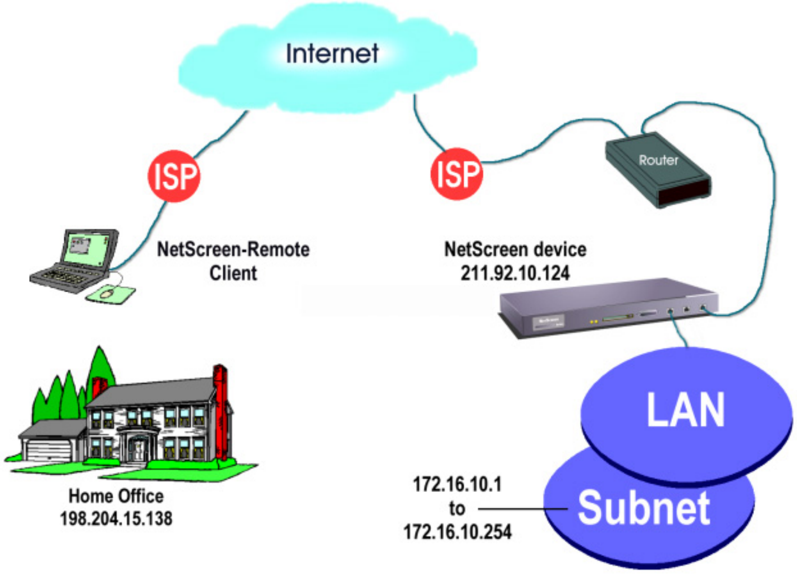

Internet
ISP
ISP
Router
NetScreen-Remote Client
NetScreen device 211.92.10.124
LAN
Home Office 198.204.15.138
172.16.10.1 to 172.16.10.254
Subnet

Figure 7-15 Home to Protected LAN using IKE with Pre-Shared Key

To set up the VPN tunnel, you must configure both the NetScreen-5XP device and the NetScreen-Remote client. In this example, you will use the following settings:

- **Connection/User Name:** Celia/Celia
- **Connection Policy:** NetScreen-5XP, Encrypt; NetScreen-Remote, Secure
- **NetScreen-5XP (Untrusted Port) IP Address:** 211.92.10.124
- **Network Subnet/Subnet Mask:** 172.16.10.0/255.255.255.0
- **NetScreen-Remote IP Address:** 198.204.15.138
  This is the address of Celia's home computer.
- **Negotiation Mode:** Pre-Shared Key/AutoKey (IKE)
- **Phase 1 Algorithm:** Diffie-Hellman Group 2
- **IPSec Protocol:** Encapsulation Protocol (ESP)
- **Encryption Algorithm:** DES
- **Hash Algorithm:** MD5
- **Encapsulation Method:** Tunnel
- **Pre-Shared Key:** NetScreenNetScreen
- **SA (Security Association) Life:** Unspecified
- **Key Life Time (Phase 2):** 3600 seconds

Setting Up the NetScreen-5

To create a successful VPN tunnel, you must set up the devices on both ends of the tunnel with identical configurations. With the NetScreen-5XP, you can configure up to 10 VPN tunnels.

There are four steps to set up the NetScreen-5XP for an AutoKey (IKE) VPN tunnel using a Pre-Shared Key:

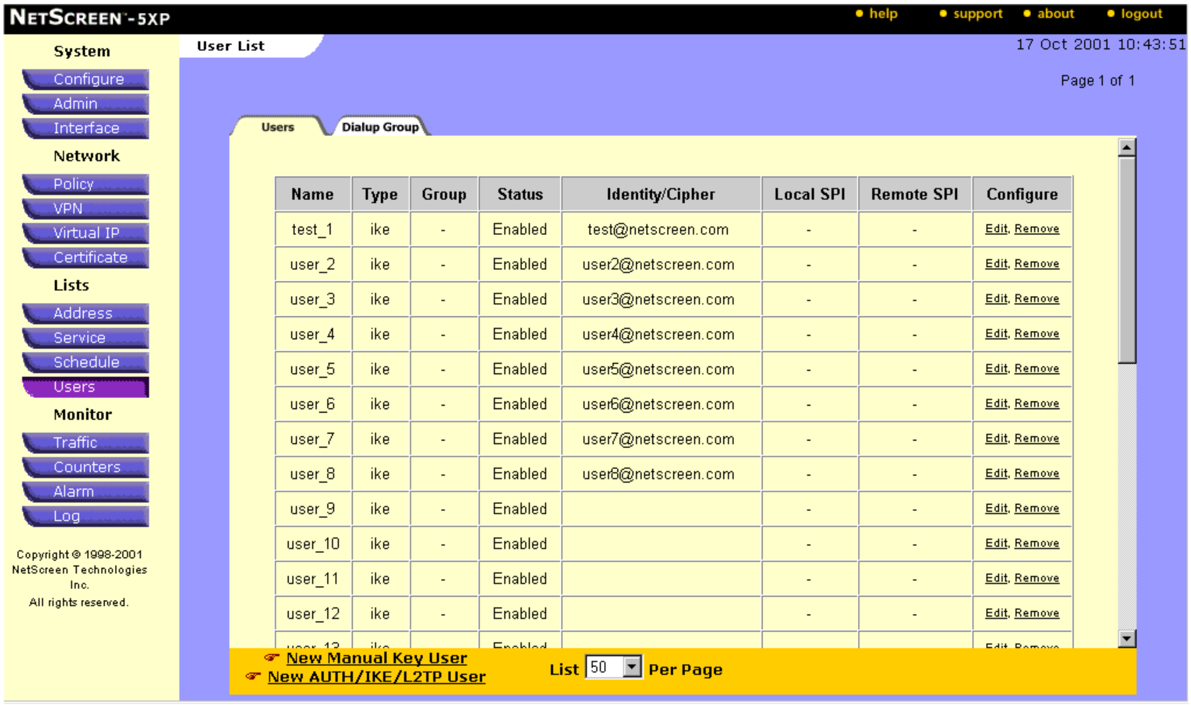
1. Adding an Entry to the Users List
2. Defining a Remote Gateway
3. Configuring an AutoKey IKE VPN
4. Defining a VPN Policy

Step 1: Adding an Entry to the Users List

At the company, you must first enter a User Name for your remote home computer in the NetScreen-5 User List.

1. Click **Users**, located under Lists in the menu column.

   The User Lists appear, with the Users page in front, as shown below.



17 Oct 2001 10:43:51

Page 1 of 1

Name	Type	Group	Status	Identity/Cipher	Local SPI	Remote SPI	Configure
test_1	ike	-	Enabled	test@netscreen.com	-	-	Edit, Remove
user_2	ike	-	Enabled	user2@netscreen.com	-	-	Edit, Remove
user_3	ike	-	Enabled	user3@netscreen.com	-	-	Edit, Remove
user_4	ike	-	Enabled	user4@netscreen.com	-	-	Edit, Remove
user_5	ike	-	Enabled	user5@netscreen.com	-	-	Edit, Remove
user_6	ike	-	Enabled	user6@netscreen.com	-	-	Edit, Remove
user_7	ike	-	Enabled	user7@netscreen.com	-	-	Edit, Remove
user_8	ike	-	Enabled	user8@netscreen.com	-	-	Edit, Remove
user_9	ike	-	Enabled		-	-	Edit, Remove
user_10	ike	-	Enabled		-	-	Edit, Remove
user_11	ike	-	Enabled		-	-	Edit, Remove
user_12	ike	-	Enabled		-	-	Edit, Remove
user_13	ike		Enabled				Edit, Remove

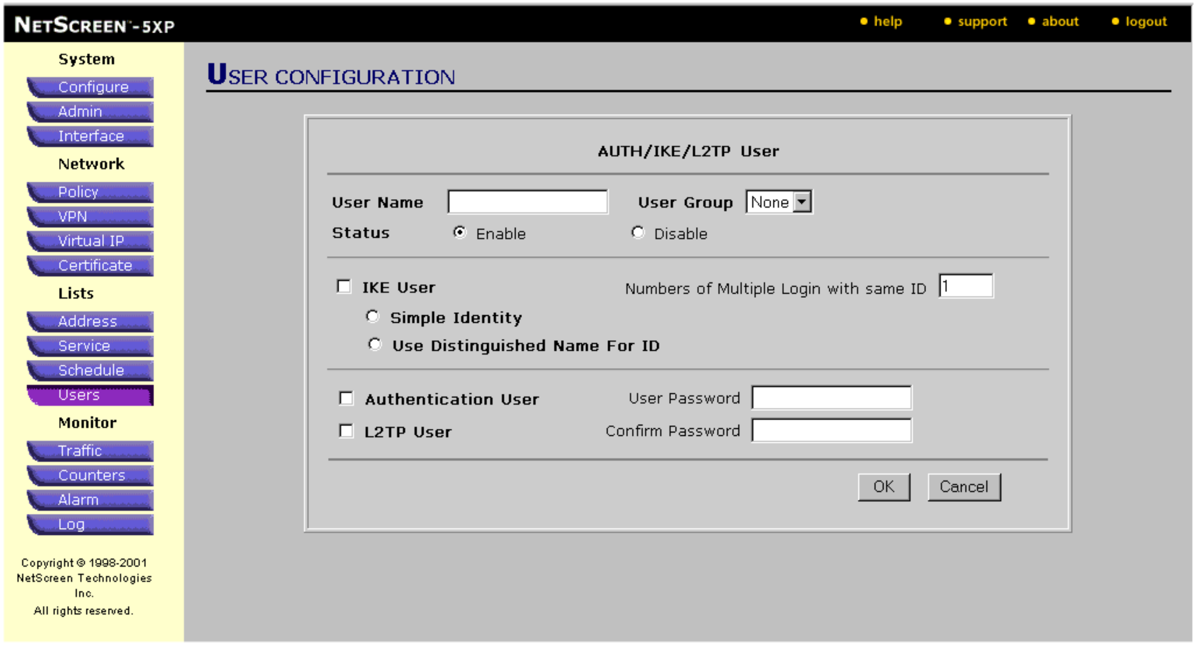
Figure 7-16 User List

2. Click **New User**, located at the bottom of the page.

   The User Configuration dialog box appears.

3. Enter the following information, as shown in Figure 7-17:
   - **User Name:** Celia
   - **IKE Dynamic Peer:** Select this option.
   - **User Group:** None
   - **Identity:** 198.204.15.138

   For **Identity**, when using a Pre-Shared Key, you can enter the User's IP address, fully qualified Domain Name, or E-mail address.



USER CONFIGURATION

AUTH/IKE/L2TP User

User Name ____ User Group None

Status ● Enable ○ Disable

□ IKE User Numbers of Multiple Login with same ID 1

○ Simple Identity

○ Use Distinguished Name For ID

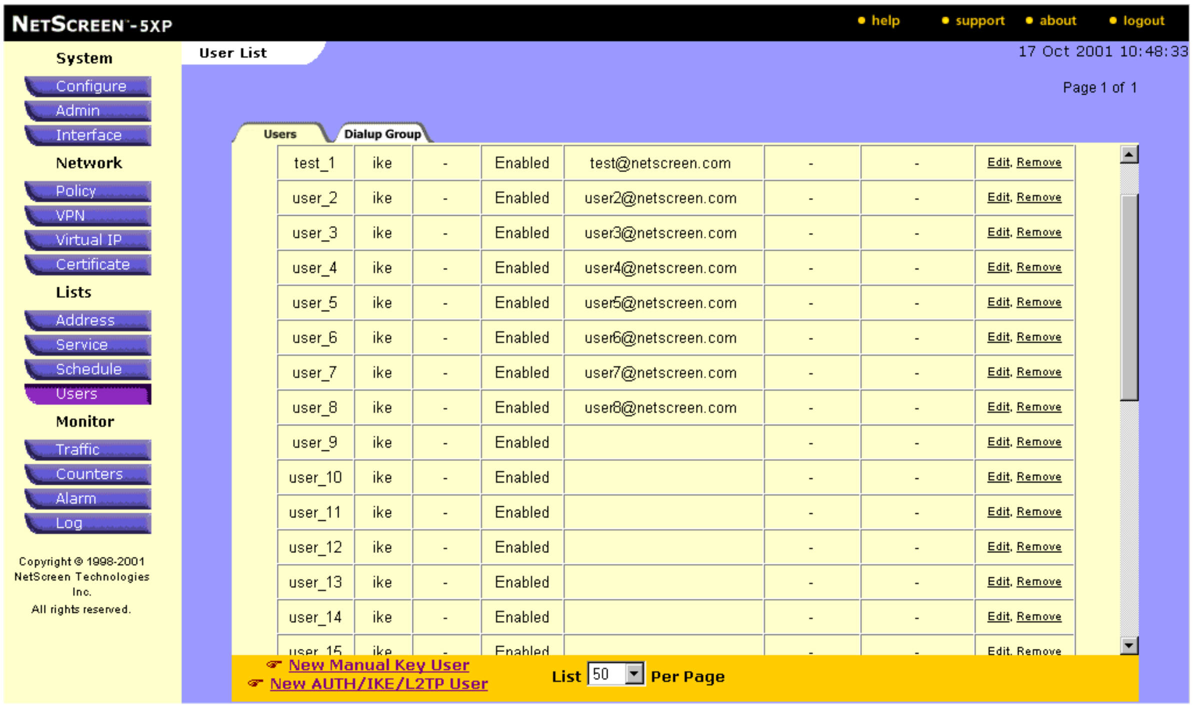
□ Authentication User User Password ____

□ L2TP User Confirm Password ____

Figure 7-17 User Configuration

4. To add this remote user, click **OK**.

   The Users List appears with the name of the new remote user, as shown below.



test_1	ike	-	Enabled	test@netscreen.com	-	-	Edit, Remove
user_2	ike	-	Enabled	user2@netscreen.com	-	-	Edit, Remove
user_3	ike	-	Enabled	user3@netscreen.com	-	-	Edit, Remove
user_4	ike	-	Enabled	user4@netscreen.com	-	-	Edit, Remove
user_5	ike	-	Enabled	user5@netscreen.com	-	-	Edit, Remove
user_6	ike	-	Enabled	user6@netscreen.com	-	-	Edit, Remove
user_7	ike	-	Enabled	user7@netscreen.com	-	-	Edit, Remove
user_8	ike	-	Enabled	user8@netscreen.com	-	-	Edit, Remove
user_9	ike	-	Enabled		-	-	Edit, Remove
user_10	ike	-	Enabled		-	-	Edit, Remove
user_11	ike	-	Enabled		-	-	Edit, Remove
user_12	ike	-	Enabled		-	-	Edit, Remove
user_13	ike	-	Enabled		-	-	Edit, Remove
user_14	ike	-	Enabled		-	-	Edit, Remove
user_15	ike	-	Enabled		-	-	Edit, Remove

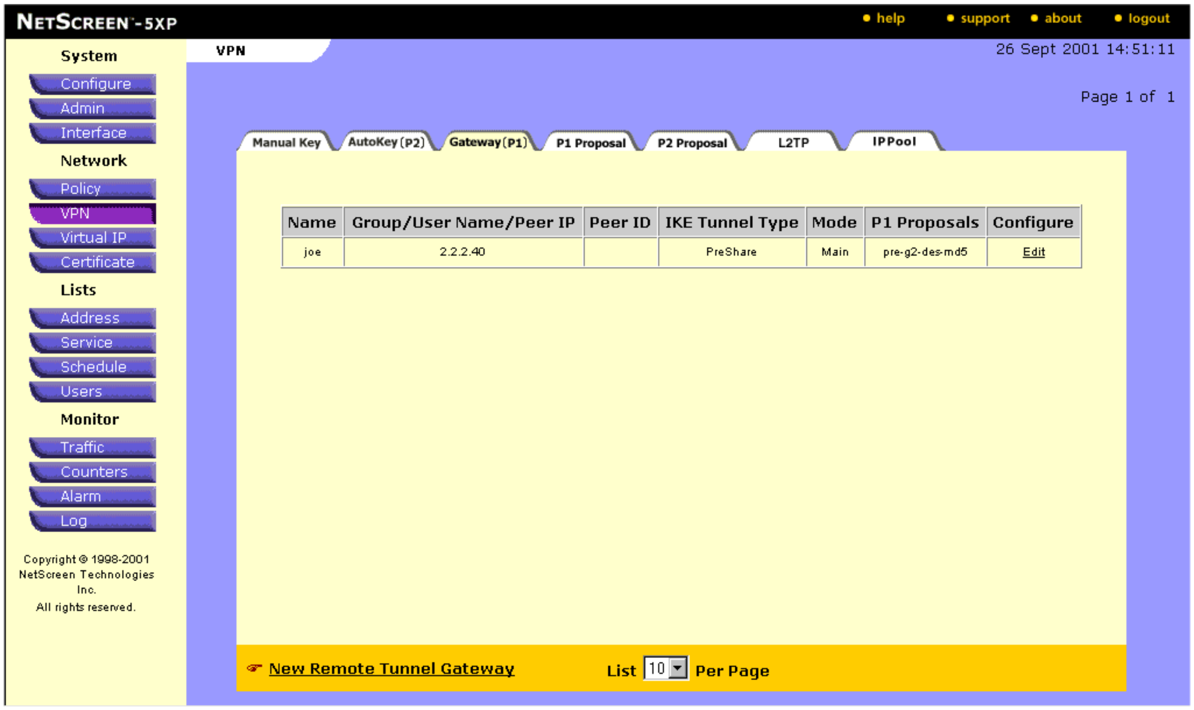
Figure 7-18 Users List

Step 2: Defining a Remote Gateway

Before you can set up an IKE tunnel for Dialup-to-LAN communication, you must define the remote gateway. This includes entering the preshared key and selecting an appropriate Phase 1 proposal for negotiating the building of the tunnel with the other end.

To create the gateway:

1. Click **VPN**, located under Network in the menu column.
2. Click the **Gateway** tab to bring that page forward.

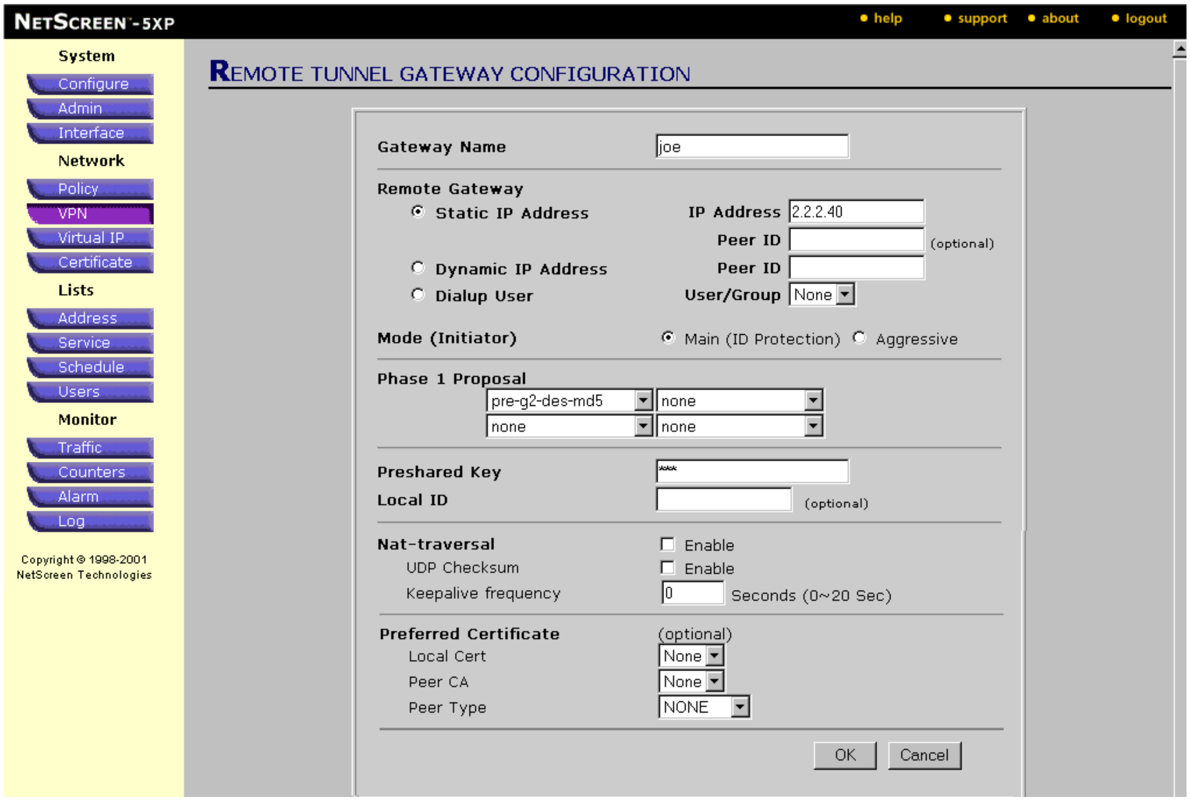


Name	Group/User Name/Peer IP	Peer ID	IKE Tunnel Type	Mode	P1 Proposals	Configure
joe	2.2.2.40		PreShare	Main	pre-g2-des-md5	Edit

Figure 7-19 Gateway Page

3. At the bottom of the page, click **New Remote Gateway** to display the New Remote Gateway Tunnel Configuration dialog box.

4. Enter the following information, as shown in Figure 7-20.
   - **Name:** Celia’s home-PC
   - **Pre-Shared Key:** NetScreenNetScreen
   - **Phase 1 Proposal:** pre-g2-des-md5
     To make configuration easier, the NetScreen-5 comes with a number of predefined Phase 1 proposals. However, the System Administrator can always create custom Phase 1 proposals.
   - **Remote Gateway/User - Dynamic IP address:** Select this option.
   - **Dynamic Peer/User/Group:** Dialup User - Celia.
     (*Celia* is the name you entered in the User List in the previous procedure.)



REMOTE TUNNEL GATEWAY CONFIGURATION

Gateway Name: joe

Remote Gateway
- ● Static IP Address — IP Address: 2.2.2.40; Peer ID: (optional)
- ○ Dynamic IP Address — Peer ID:
- ○ Dialup User — User/Group: None

Mode (Initiator): ● Main (ID Protection) ○ Aggressive

Phase 1 Proposal: pre-g2-des-md5 | none | none | none

Preshared Key: ***
Local ID: (optional)

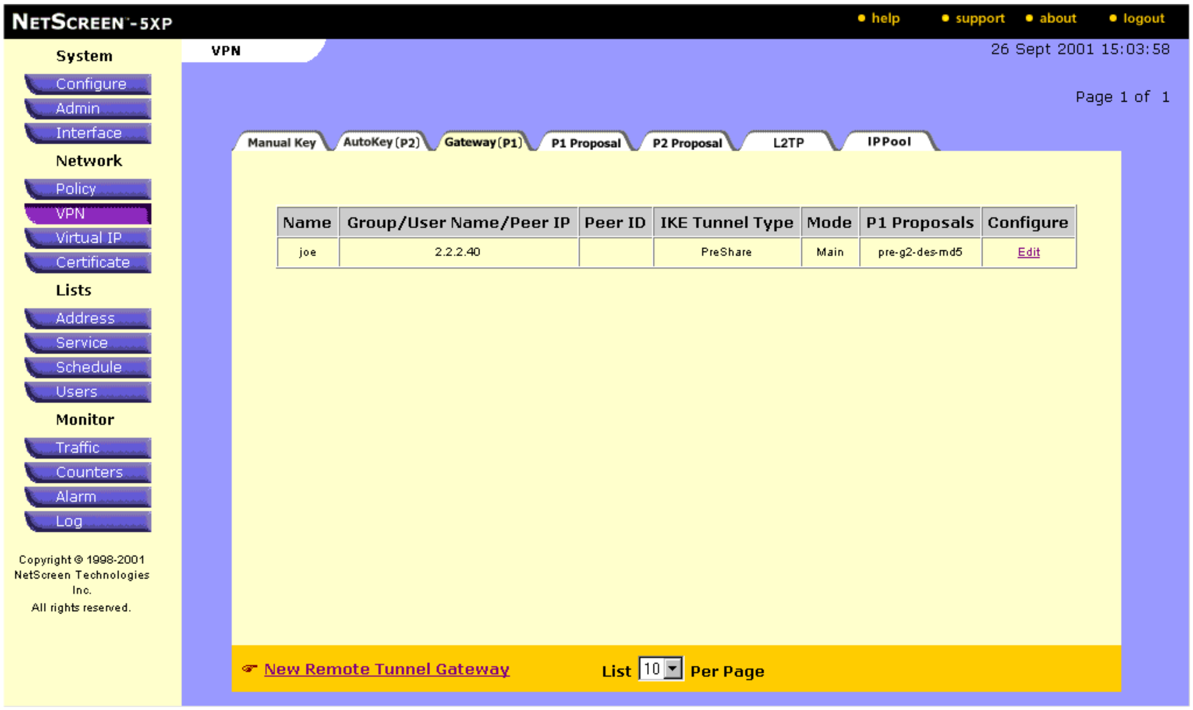
Nat-traversal: □ Enable
UDP Checksum: □ Enable
Keepalive frequency: 0 Seconds (0~20 Sec)

Preferred Certificate (optional)
Local Cert: None
Peer CA: None
Peer Type: NONE

Figure 7-20 New Remote Gateway Tunnel Configuration

5. Click **OK** to save the settings.

The Gateway Listings page appears with the new entry, as shown below.



26 Sept 2001 15:03:58

Page 1 of 1

Name	Group/User Name/Peer IP	Peer ID	IKE Tunnel Type	Mode	P1 Proposals	Configure
joe	2.2.2.40		PreShare	Main	pre-g2-des-md5	Edit

List 10 Per Page

Copyright © 1998-2001 NetScreen Technologies Inc.
All rights reserved.

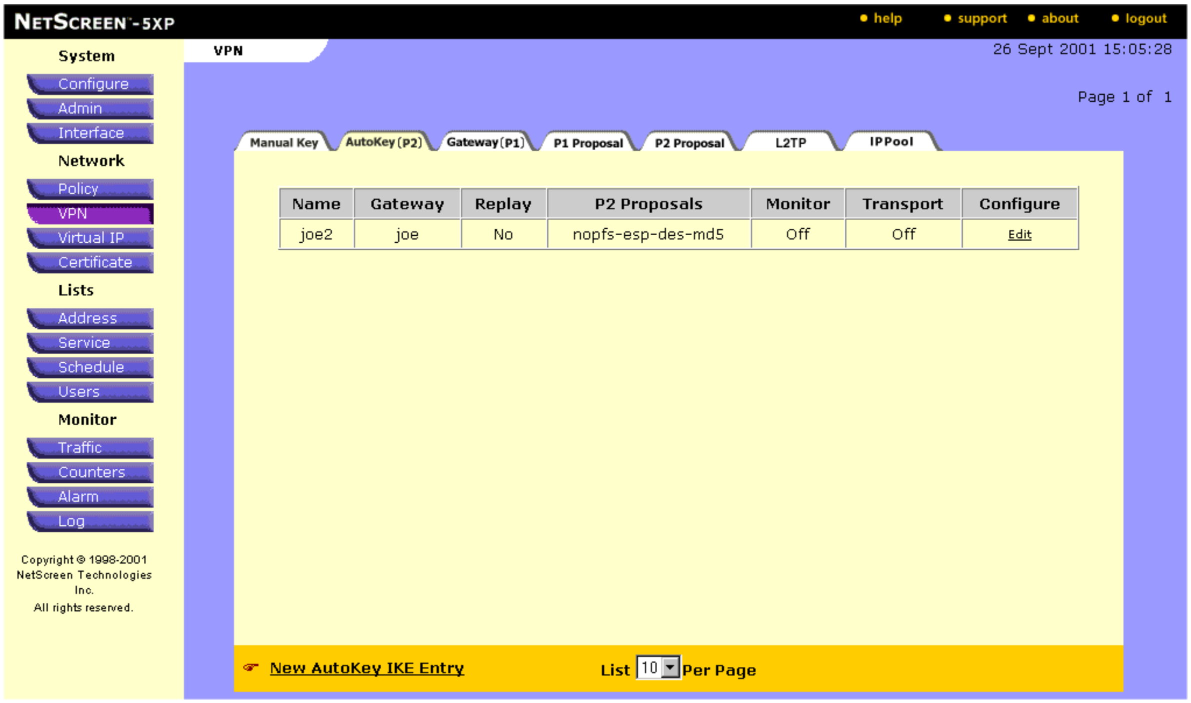
Figure 7-21 Gateway Listings Page with New Gateway Added

Step 3: Configuring an AutoKey IKE VPN Tunnel

So far, you have defined the new dialup user and the remote gateway. At this point, you must associate the remote gateway tunnel name with a Phase 2 proposal describing how the data passing through the tunnel is to be encrypted and decrypted.

1. Click **VPN**, located under Network in the menu column.

   The VPN pages appear, with the AutoKey IKE page in front.



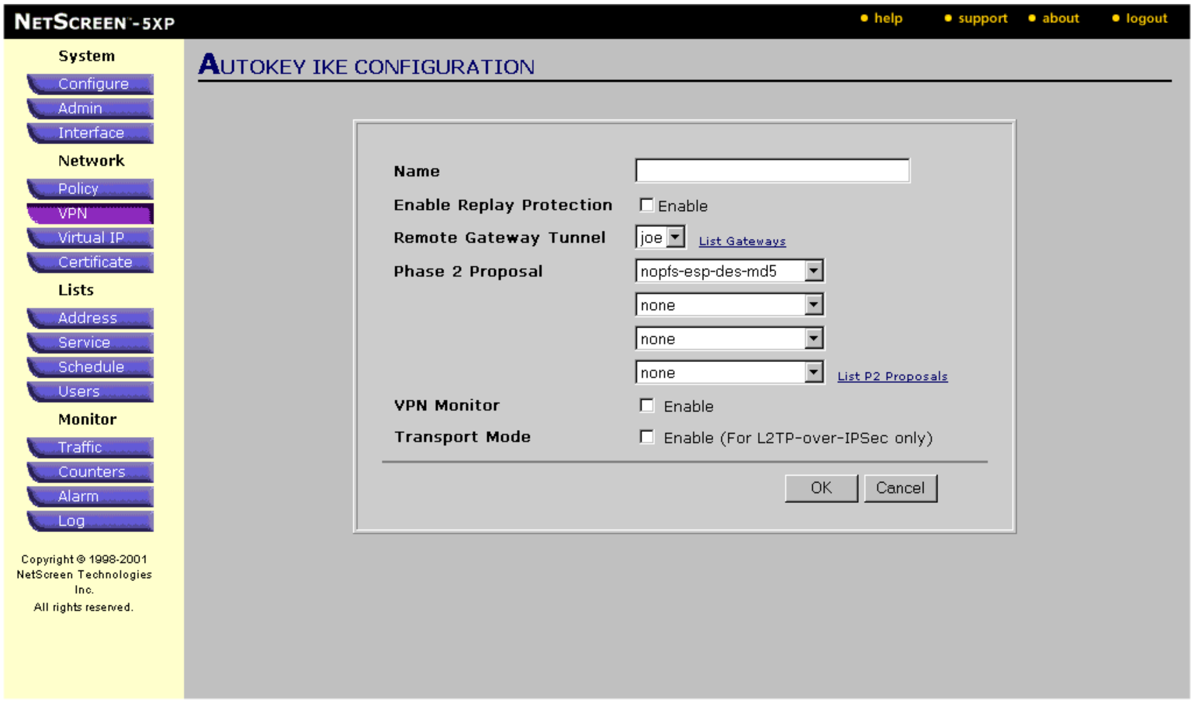
Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure
joe2	joe	No	nopfs-esp-des-md5	Off	Off	Edit

Figure 7-22 VPN AutoKey IKE Page

2. Click **New AutoKey IKE Entry**, located in the lower-left corner of the page.

   The New AutoKey IKE Configuration dialog box appears.

3. Enter the following information, as shown in Figure 7-23:
   - **Name:** Celia
   - **Remote Gateway Tunnel Name:** Celia’s home-PC
     This is the name you assigned when you created the new remote gateway in the previous procedure.
   - **Phase 2 Proposal:** nopfs-esp-des-md5
     To view the available predefined proposals in detail, click the **List Phase 2 Proposals** link. The default lifetime for the proposal selected in this particular scenario is 3600 (seconds).



AUTOKEY IKE CONFIGURATION

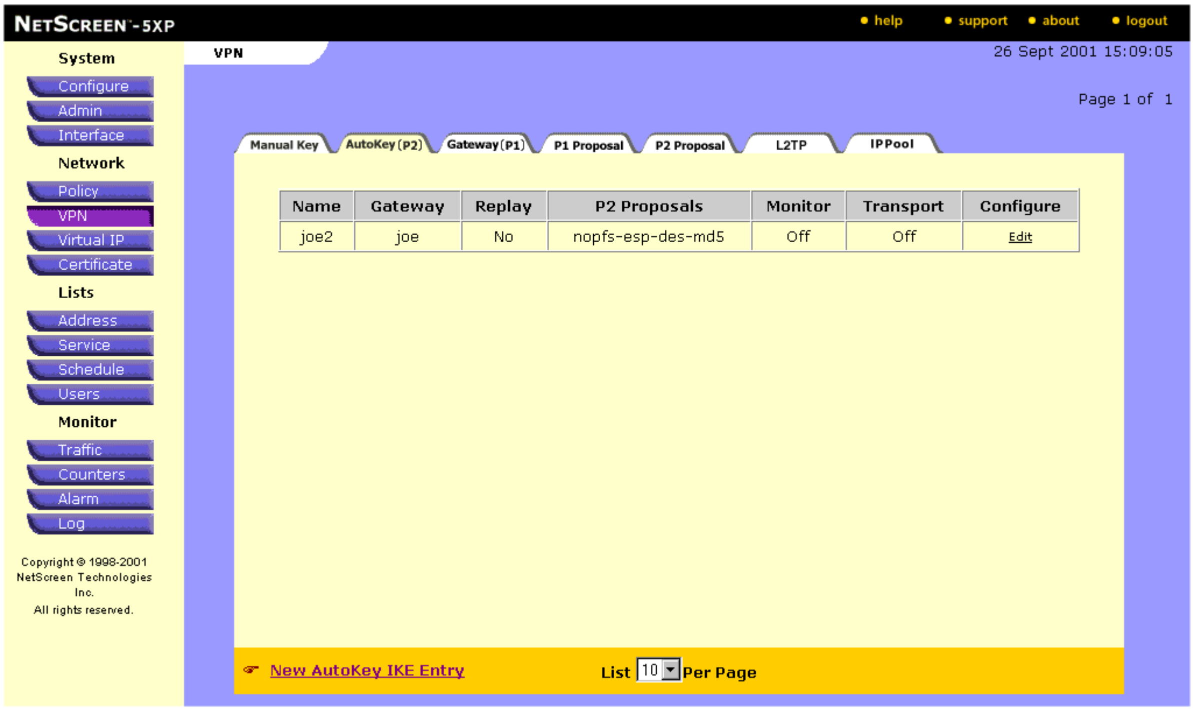
Name	
Enable Replay Protection	□ Enable
Remote Gateway Tunnel	joe ▾ List Gateways
Phase 2 Proposal	nopfs-esp-des-md5 ▾
	none ▾
	none ▾
	none ▾ List P2 Proposals
VPN Monitor	□ Enable
Transport Mode	□ Enable (For L2TP-over-IPSec only)

OK Cancel

Figure 7-23 New AutoKey IKE Configuration

4. Click **OK** to save the new entry.

The updated list of AutoKey IKE VPNs appears, as shown below.



26 Sept 2001 15:09:05

Page 1 of 1

Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure
joe2	joe	No	nopfs-esp-des-md5	Off	Off	Edit

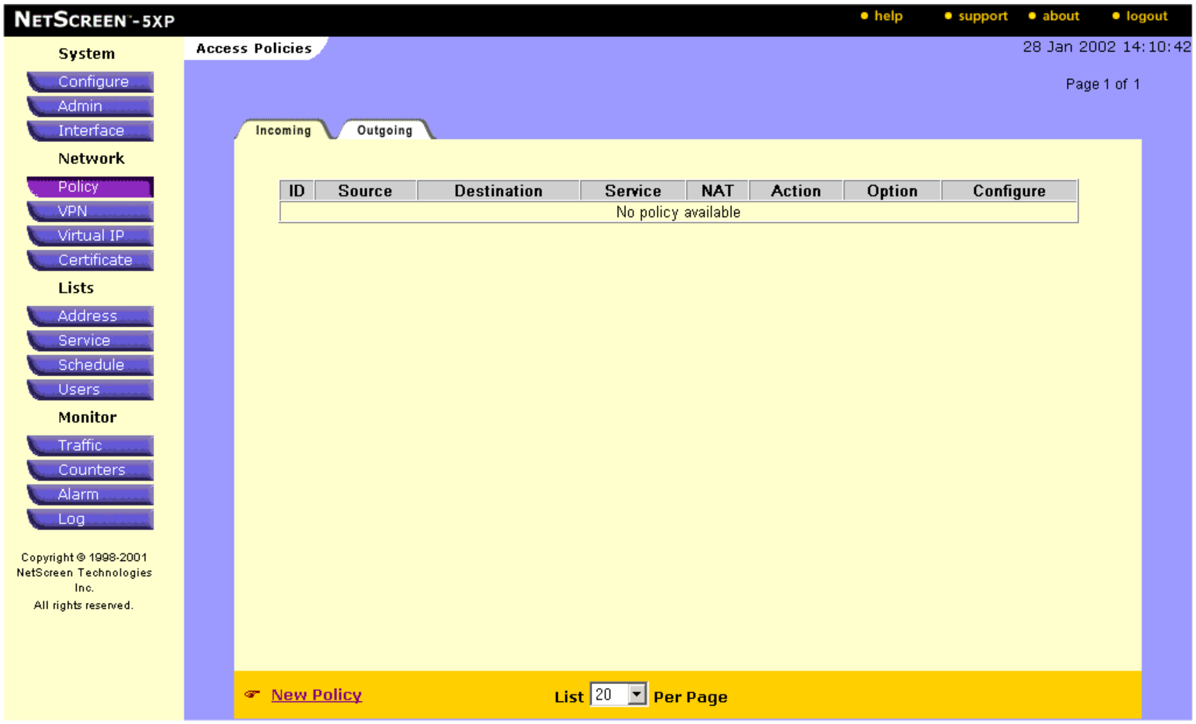
Figure 7-24 Updated List of AutoKey IKE VPNs

Step 4: Defining a VPN Access Policy

After you configure a VPN, you must define an Access Policy with the action set to *encrypt* and select the corresponding VPN tunnel.

1. Click **Policy**, located under Network in the menu column.

   The Access Policies pages appear, with the Incoming page in front.



28 Jan 2002 14:10:42

Page 1 of 1

ID	Source	Destination	Service	NAT	Action	Option	Configure
No policy available							

Figure 7-25 Outgoing Access Policies Page

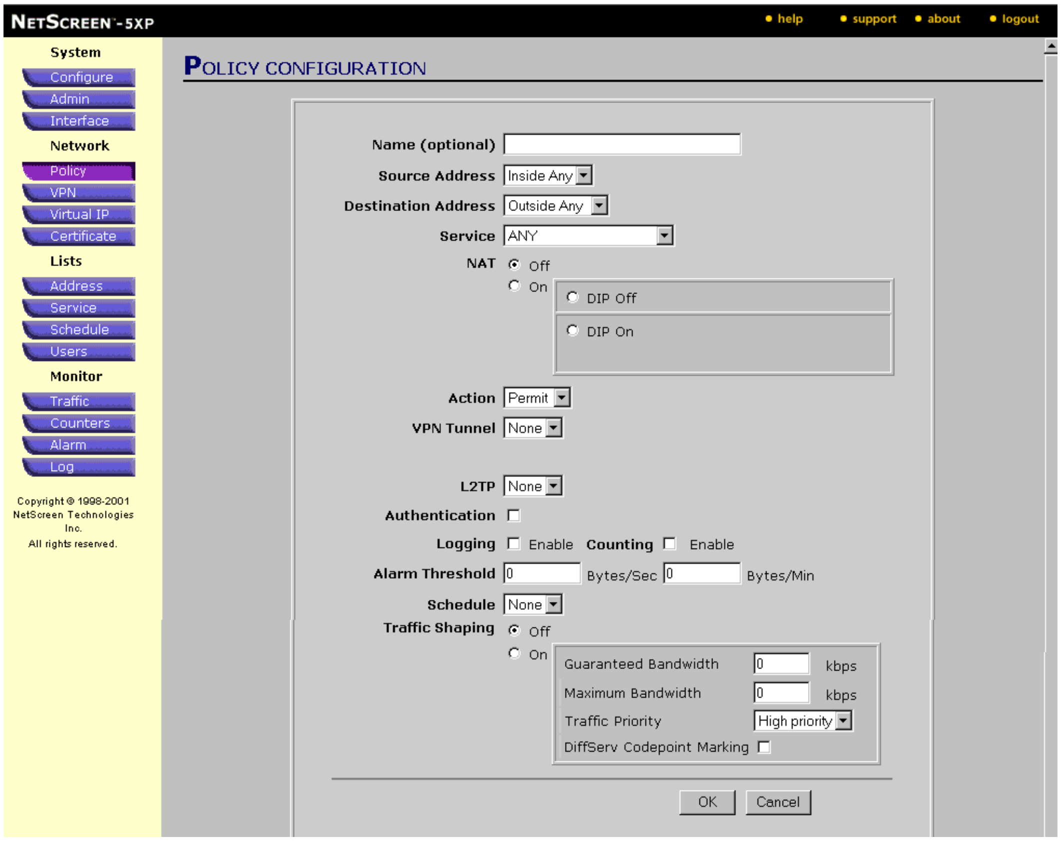
> *Although VPN Access Policies are defined for Outgoing traffic, VPN Access Policies assume bidirectional traffic and that the destination address can also originate VPN sessions.*

2. Click **New Policy**, located in the lower-left corner of the page.

   The Policy Configuration dialog box appears.

3. Enter the following information, as shown in Figure 7-26:
   - **Name:** Celia's Tunnel
   - **Source Address:** Inside Any
     To be more secure, you can first define a Trusted Address for a specific subnet, and then select that as the Source Address here.
   - **Destination Address:** Dial-Up VPN (from drop-down list)
   - **Service:** ANY
   - **Action:** Encrypt
   - **VPN Tunnel:** Celia

   Leave the remaining fields at their default values.



POLICY CONFIGURATION

Name (optional)

Source Address: Inside Any

Destination Address: Outside Any

Service: ANY

NAT ● Off ○ On
○ DIP Off
○ DIP On

Action: Permit

VPN Tunnel: None

L2TP: None

Authentication □

Logging □ Enable Counting □ Enable

Alarm Threshold 0 Bytes/Sec 0 Bytes/Min

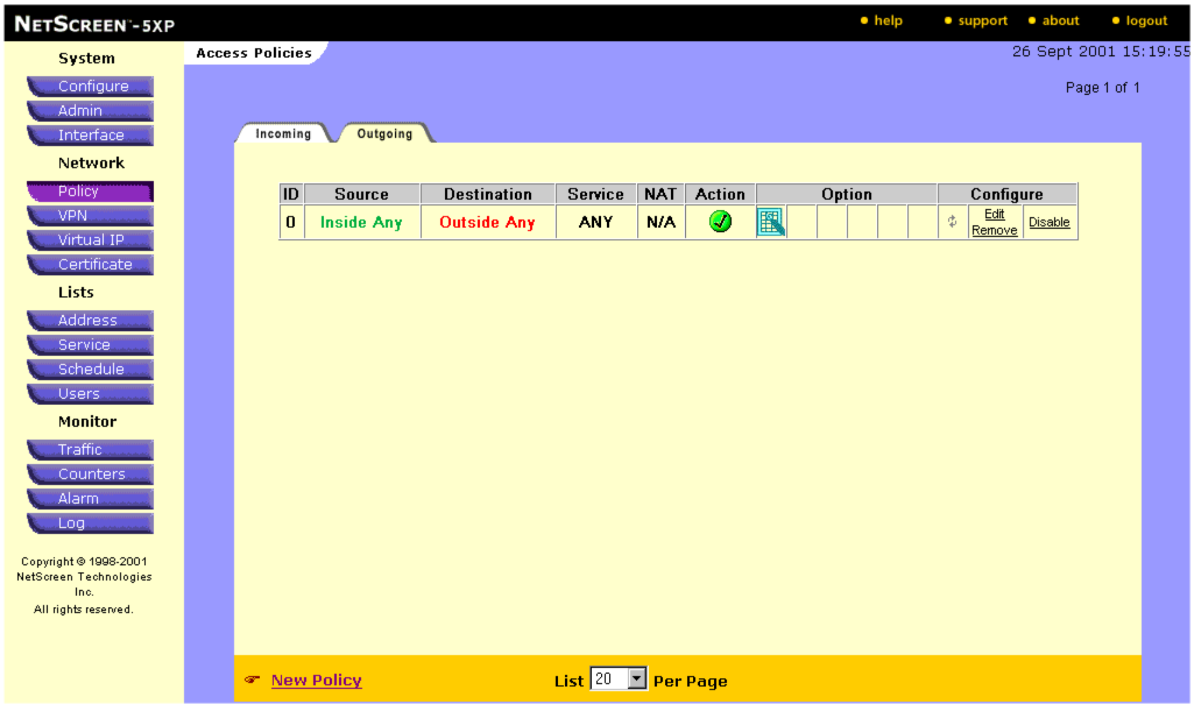
Schedule: None

Traffic Shaping ● Off ○ On
Guaranteed Bandwidth 0 kbps
Maximum Bandwidth 0 kbps
Traffic Priority: High priority
DiffServ Codepoint Marking □

Figure 7-26 Policy Configuration

4. Click **OK** to enter your settings.

The Outgoing Access Policies page appears, with the new Access Policy added, as shown below.



26 Sept 2001 15:19:55

Page 1 of 1

ID	Source	Destination	Service	NAT	Action	Option	Configure
0	Inside Any	Outside Any	ANY	N/A	✓	▦	⇕ Edit Remove Disable

List 20 Per Page

Figure 7-27 Outgoing Access Policies Page with New Policy

5. Because the VPN Access Policy is more restrictive than the generic “Inside Any / Outside Any” policy, it needs to be at the top of the list of Access Policies. To move the Access Policy to the top of the list, click the ⇕ icon in the row for the Access Policy that you want to move.

The Move Policy dialog box appears.

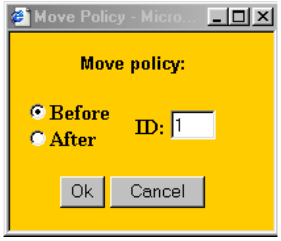
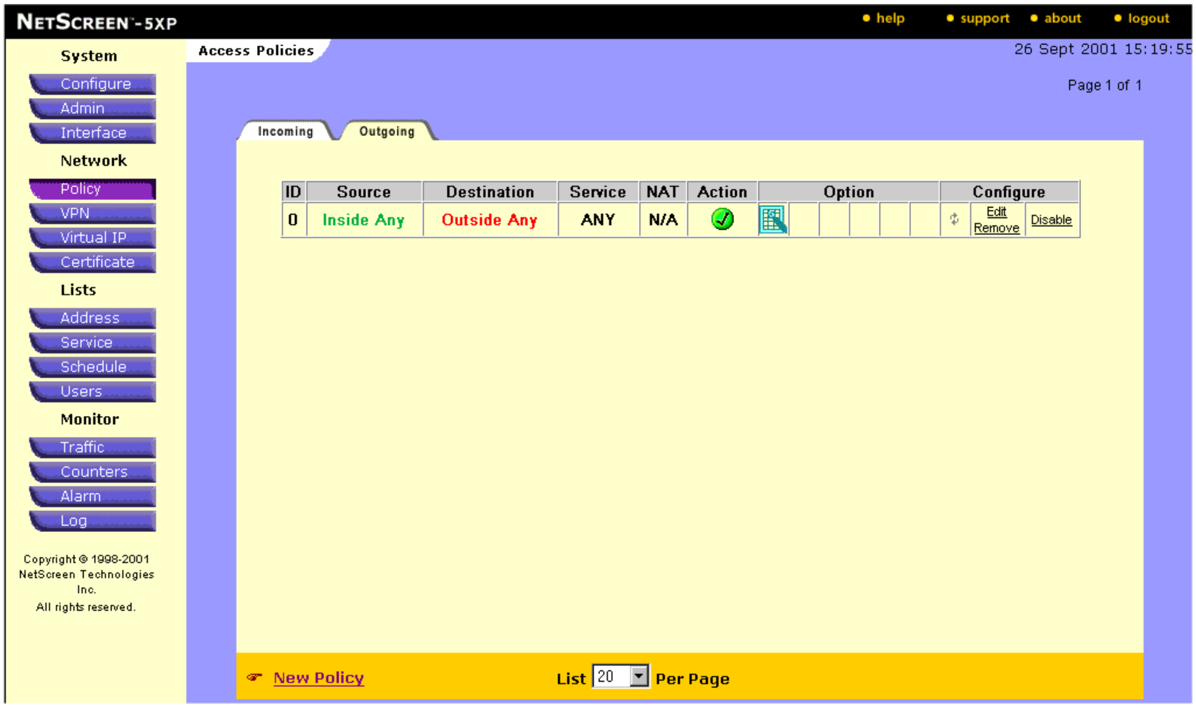


Figure 7-28 Move Policy

6. Enter the new position for the Access Policy, then click **OK**.

   The updated Outgoing Access Policy page appears, as shown below.



26 Sept 2001 15:19:55

Page 1 of 1

ID	Source	Destination	Service	NAT	Action	Option	Configure	
0	Inside Any	Outside Any	ANY	N/A	✓		Edit Remove	Disable

Figure 7-29 Updated Outgoing Access Policy List

The NetScreen security-appliance end of the eventual Pre-Shared/AutoKey IKE VPN tunnel is complete.

Setting Up NetScreen-Remote

There are three steps to setting up NetScreen-Remote for a Pre-Shared/AutoKey IKE VPN tunnel:

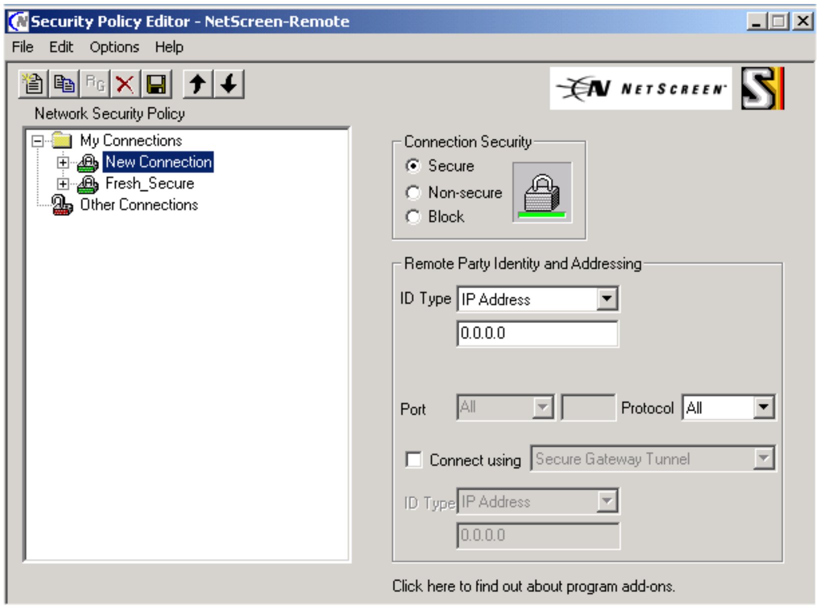
1. Creating a New Connection
2. Creating the Pre-Shared Key
3. Defining the IPSec Protocols

Step 1: Creating a New Connection

You begin by initiating a new connection. You then name the connection, define it as secure, and determine the identification and location of the other end of the eventual VPN tunnel (that is, the NetScreen-5 device protecting your company's network).

1. Double-click the **NetScreen-Remote** icon to open the Security Policy Editor.
2. On the File menu, choose **New Connection**.

   A new connection icon appears in the Network Security Policy list, as shown below.


Security Policy Editor - NetScreen-Remote
File
Edit
Options
Help
NETSCREEN
Network Security Policy
Click here to find out about program add-ons.

Network Security Policy:
- My Connections
  - New Connection
  - Fresh_Secure
- Other Connections

Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Address
0.0.0.0
Port: All
Protocol: All
□ Connect using: Secure Gateway Tunnel
ID Type: IP Address
0.0.0.0

Figure 7-30 New Connection

3. Name the new Connection **Celia**.
4. In the Connection Security area, located to the right of the Network Security Policy list, select **Secure**.
5. In the Remote Party Identity and Addressing area, select **IP Subnet** in the ID Type drop-down list.
6. In the Subnet field, type in **172.16.10.0**, and in the Mask field, type in **255.255.255.0**.

   This is the network subnet at the Company site.

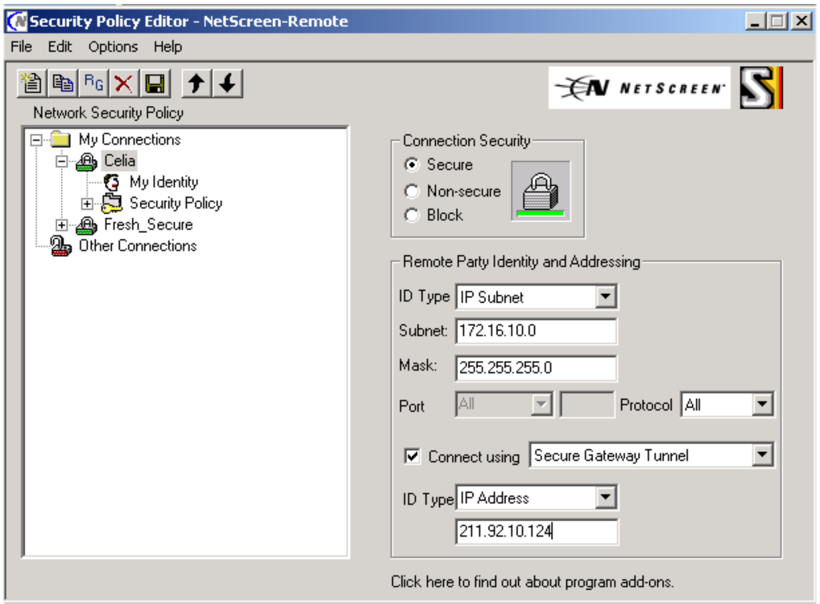
7. Leave Protocol set at **All**.
8. Select **Connect using Secure Gateway Tunnel**.

   The Secure Gateway Tunnel ID Type and IP Address fields become available.

9. For ID Type, choose **IP Address**, and in the IP Address field, type in **211.92.10.124**.

   This is the NS-5 Untrusted Port IP Address.

The completed Connection Security and Remote Party Identity and Addressing areas are shown below.



Connection Security

- ● Secure
- ○ Non-secure
- ○ Block

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 172.16.10.0

Mask: 255.255.255.0

Port: All

Protocol: All

☑ Connect using: Secure Gateway Tunnel

ID Type: IP Address

211.92.10.124

Click here to find out about program add-ons.

Figure 7-31 Connection Security, Remote Party Identity and Addressing

Step 2: Creating the Pre-Shared Key

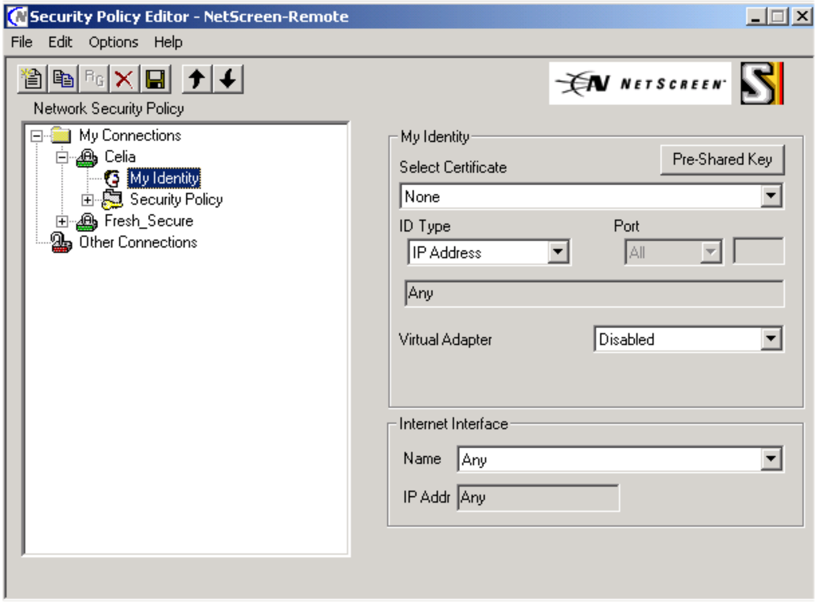
In this procedure, you create the Pre-Shared Key for encrypting communication.

1. Double-click the **Celia** icon.

   My Identity and Security Policy icons appear.

2. Click **My Identity**.

   The My Identity and Internet Interface areas appear to the right of the Network Security Policy list, as shown below.



Select Certificate: None

ID Type: IP Address

Port: All

Any

Virtual Adapter: Disabled

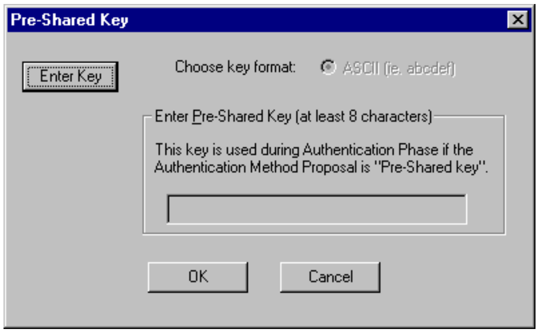
Name: Any

IP Addr: Any

Figure 7-32 My Identity and Internet Interface

3. In the My Identity area, select **None** from the Select Certificate drop-down list.
4. Click **Pre-Shared Key**.

The Pre-Shared Key dialog box appears.



Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

Figure 7-33 Pre-Shared Key

5. Click **Enter Key** to make the Pre-Shared Key field available.
6. Type in the following key: **`NetScreenNetScreen.`**

   The key length must be between 8 and 63 characters. A longer key length results in stronger encryption.

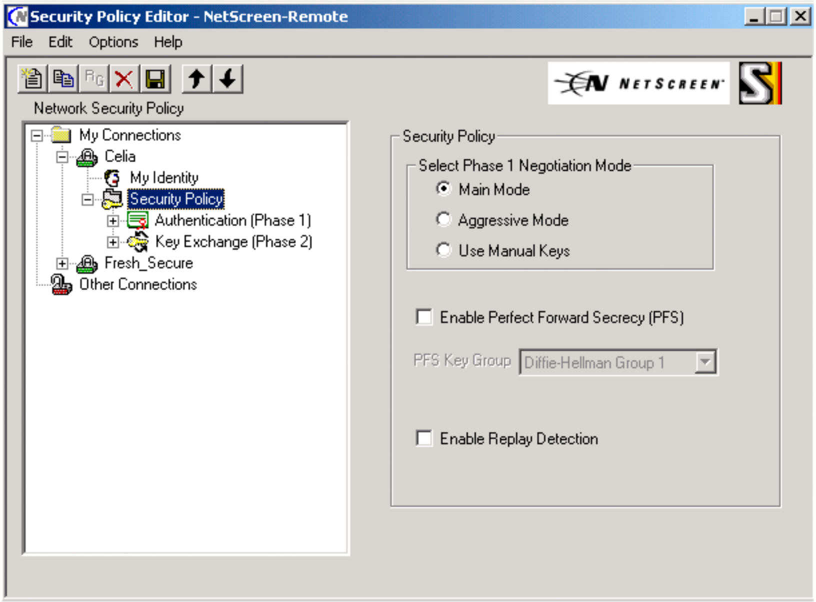
7. Click **OK** to save the entry.

Step 3: Defining the IPSec Protocols

In Step 3, you define the IPSec protocols for securing the VPN tunnel.

1. Double-click **Security Policy** in the Network Security Policy list.

   The Security Policy area appears on the right, and the Authentication (Phase 1) and Key Exchange (Phase 2) icons appear, as shown below.



Network Security Policy

- My Connections
  - Celia
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
      - Key Exchange (Phase 2)
  - Fresh_Secure
- Other Connections

Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

○ Use Manual Keys

☐ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

☐ Enable Replay Detection

Figure 7-34 Security Policy Area

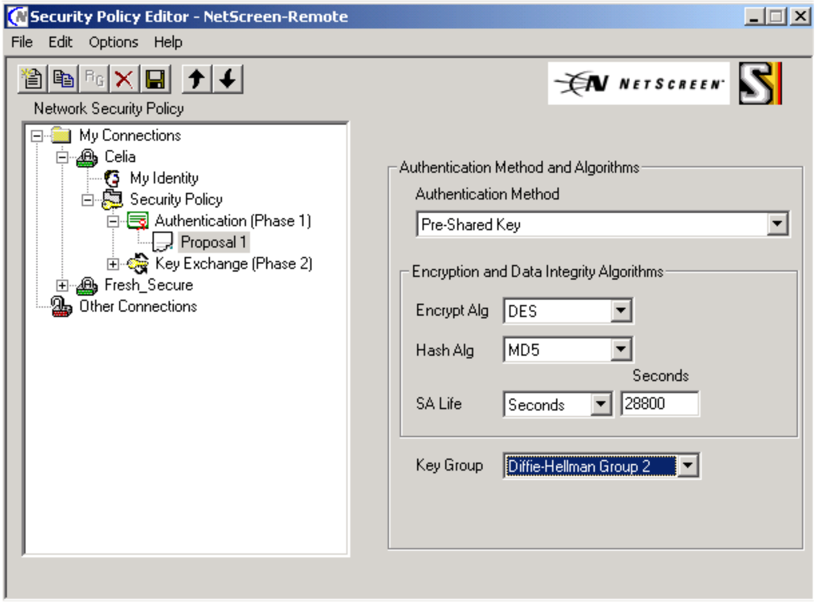
2. Select **Aggressive Mode** in the Security Policy area.
3. Double-click **Authentication (Phase 1)**.

   Proposal 1 appears below the Authentication (Phase 1) icon.

4. Select **Proposal 1** to display the Authentication Method and Algorithms area.

5. In the Authentication Method and Algorithms area, enter the following settings:
   - **Encryption Algorithm:** DES
   - **Hash Algorithm:** MD5
   - **SA Life:** Seconds
   - **Seconds:** 28800
   - **Key Group:** Diffie-Hellman Group 2

   The completed area is shown below.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: DES

Hash Alg: MD5

SA Life: Seconds — Seconds: 28800

Key Group: Diffie-Hellman Group 2

Figure 7-35 Authentication Method and Algorithms Area

Because you selected Pre-Shared Key, that is what appears in the Authentication Method field. Although there is a drop-down list, no other choices are available.

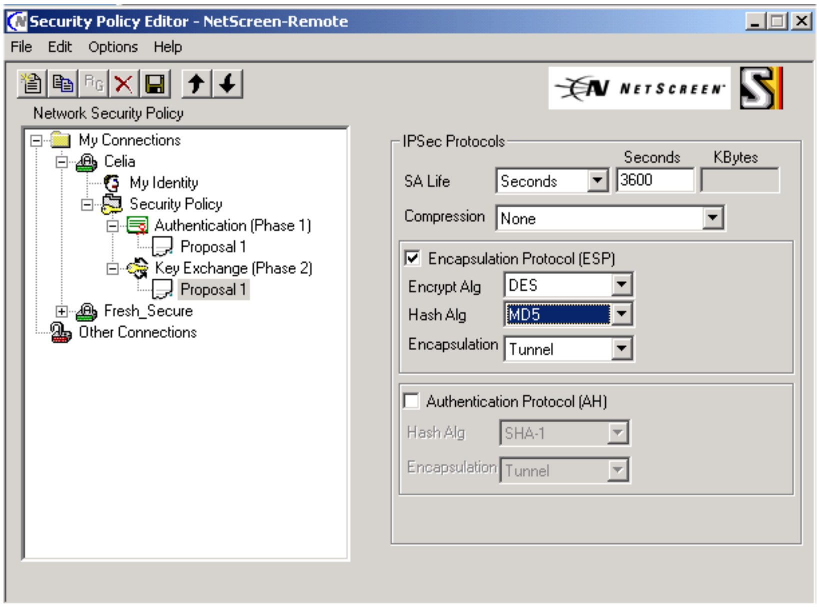
6. Double-click **Key Exchange (Phase 2)**.

   Proposal 1 appears below the Key Exchange (Phase 2) icon.

7. Select **Proposal 1** to display the IPSec Protocols area.

8. In the IPSec Protocols area, enter the following settings:
   - **SA life:** Seconds
   - **Seconds:** 3600
   - **Encapsulation Protocol (ESP)**: Select this option.
   - **Encryption Algorithm:** DES
   - **Hash Algorithm:** MD5
   - **Encapsulation:** Tunnel

   The completed IPSec Protocols area is shown below.



Network Security Policy

- My Connections
  - Celia
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
        - Proposal 1
  - Fresh_Secure
- Other Connections

IPSec Protocols

		Seconds	KBytes
SA Life	Seconds	3600	
Compression	None		

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: MD5

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 7-36 IPSec Protocols Area

9. Click the **Save** icon on the toolbar or choose **Save Changes** from the File menu.

   The NetScreen-Remote end of the eventual Pre-Shared/AutoKey IKE VPN tunnel is complete.

Making a Connection

With both ends of the tunnel configured, you are ready to make a secure VPN tunnel connection.

1. Launch your Web browser.
2. Enter an IP address within the network subnet, for example: **`http://172.16.10.250`**

   NetScreen-Remote, which continually checks all IP addresses that you enter, recognizes this address as the one you configured for a secure connection. It routes the transmission to the security gateway (that is, the Untrusted port of the NetScreen-5) and proposes the VPN tunnel connection.

   The NetScreen-5 responds to this proposal by checking its database until it finds the Access Policy defining the proposed connection as a VPN tunnel.

   With the settings at both ends in accord, NetScreen-Remote and the NetScreen-5 begin using the Pre-Shared Key and the specified ESP encryption (DES) and authentication (MD5) algorithms to secure the connection.

   The VPN tunnel is established.

   After encrypting the tunnel for an hour (3600 seconds), the key automatically changes to another, random key, using the AutoKey IKE function.

Scenario 3: From Home with Certificate

In this scenario, you need to access the company's protected network (LAN) from your laptop computer, which has a dynamically assigned IP address.

You want to create a VPN tunnel to your company's LAN using the Certificates/AutoKey (IKE) method. You are using the NetScreen-Remote client, and your company's network is protected by the NetScreen-5, which is configured for Network Address Translation (NAT). The VPN tunnel that you create will secure the connection from your computer to the NetScreen-5 device, as shown below.

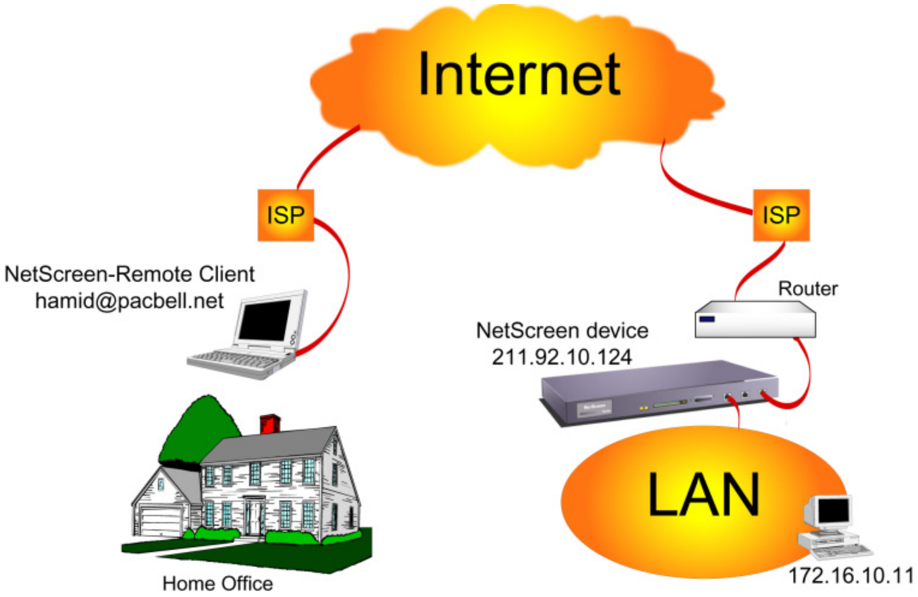


Figure 7-37 Home to Protected LAN using IKE with Certificates

To set up the VPN tunnel, you must configure both the NetScreen-5 device and the NetScreen-Remote client. In this example, you will use the following settings:

- **Connection/User Name:** Development Group/Hamid
- **Connection Policy:** NetScreen-5, Encrypt; NetScreen-Remote, Secure
- **NetScreen-5 (Untrusted Port) IP Address:** 211.92.10.124
- **IP Address/Subnet Mask on LAN:** 172.16.10.11/255.255.255.255
- **NetScreen-Remote Domain:** pacbell.net
- **Negotiation Mode:** Certificates/AutoKey (IKE)
- **Phase 1 Negotiation Mode:** Aggressive
- **IPSec Protocol:** Encapsulation Protocol (ESP)
- **Phase 1 Algorithm:** Diffie-Hellman Group 2
- **Encryption Algorithm:** Triple DES
- **Hash Algorithm:** SHA-1
- **Encapsulation Method:** Tunnel
- **SA (Security Association) Life:** Unspecified
- **Key Life Time:** 28800 seconds in Phase 1; 3600 seconds in Phase 2

Setting up the NetScreen-5

To create a successful VPN tunnel, you must set up the devices on both ends of the tunnel with identical configurations. With the NetScreen-5, you can set up to 10 VPN tunnels.

There are five tasks involved in setting up the NetScreen-5 for an AutoKey IKE VPN tunnel using certificates:

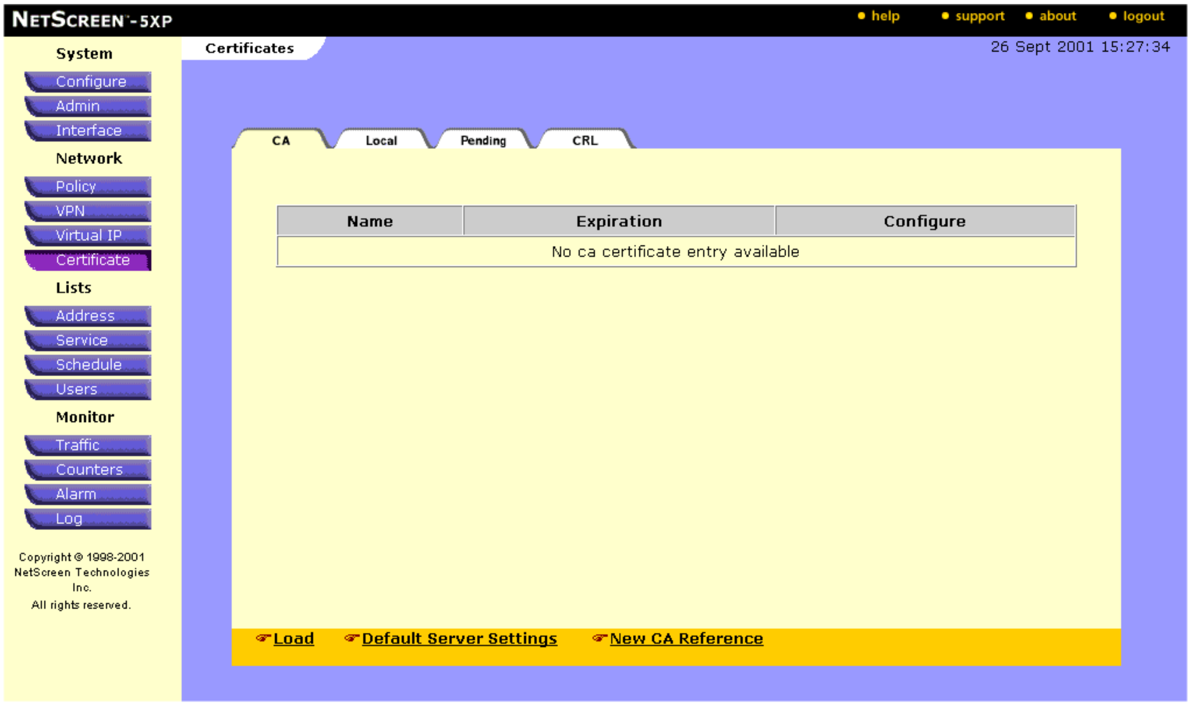
1. Checking for Certificates
2. Adding a Trusted Address to the Address Book
3. Adding an Entry to the Users List
4. Defining a Remote Gateway
5. Configuring an AutoKey IKE VPN Tunnel
6. Defining a VPN Access Policy

Step 1: Checking for Certificates

Before you can set up an AutoKey IKE VPN tunnel using certificates, you need to verify that two documents are already loaded into the NetScreen-5 device. These include a valid CA certificate and a valid local certificate (which serves as the device's identity and is the equivalent of a personal certificate on NetScreen-Remote).

To make sure that you have the required files:

1. Click **VPN**, located under Network in the menu column.
2. Click the **Certificates** tab to bring that page to the front.



Name	Expiration	Configure
No ca certificate entry available		

Figure 7-38 VPN Certificates List

- Verify that in the Type column, there is at least one CA certificate and one local certificate.
- Verify that the certificates are still current by checking the expiration dates.

With NetScreen v2.0, you cannot verify whether a CRL has been loaded into the NetScreen device. Check with your System Administrator to see if this has been done.

3. If there are no certificates listed, refer to the section on obtaining digital certificates in the *NetScreen-5 User's Guide* for instructions.

Step 2: Adding a Trusted Address to the Address Book

First, you must enter the IP address of the device to be the endpoint of the VPN tunnel on the Trusted side of the NetScreen-5.

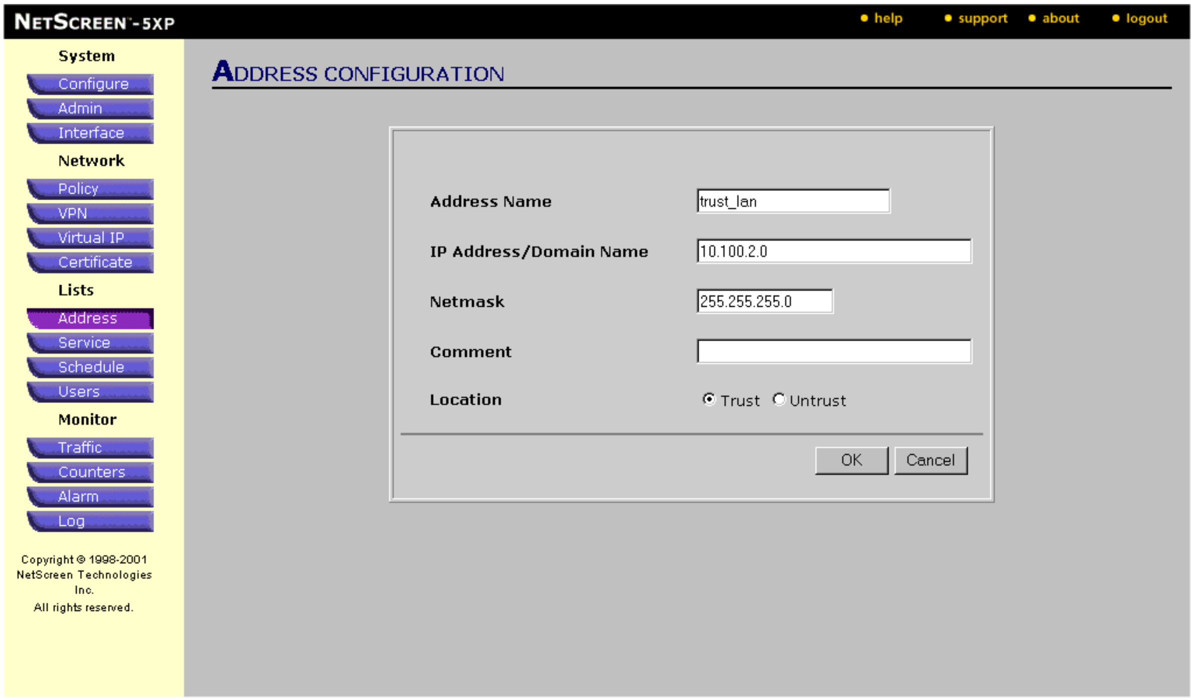
1. Click **Address**, located under Lists in the menu column.

   The Address Book appears, with the Trusted page in front.

2. Click **New Address**, located in the lower-left corner of the page.

   The Address Configuration dialog box appears.

3. Enter the following information, as shown in Figure 7-39.
   - **Address Name:** comp_11
   - **IP Address/Domain Name:** 172.16.10.11
   - **NetMask:** 255.255.255.255
   - Leave the Comment field empty, make sure that **Trust** is selected, and then click **OK** to save the configuration.



ADDRESS CONFIGURATION

Address Name	trust_lan
IP Address/Domain Name	10.100.2.0
Netmask	255.255.255.0
Comment	
Location	● Trust ○ Untrust

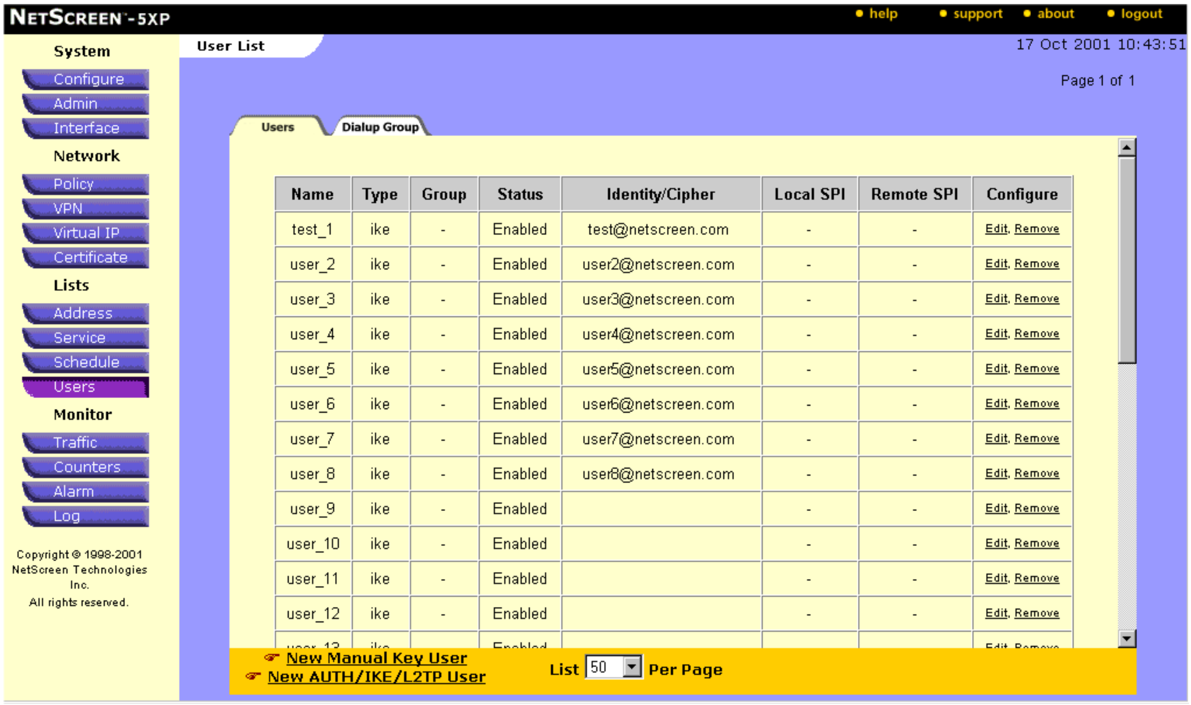
Figure 7-39 Address Configuration

Step 3: Adding an Entry to the Users List

Next, you must enter a user name for your remote home computer in the NetScreen-5 User List.

1. Click **Users**, located under Lists in the menu column.

   The Users and Dialup Group pages appear, with the Users page in front, as shown below.



Name	Type	Group	Status	Identity/Cipher	Local SPI	Remote SPI	Configure
test_1	ike	-	Enabled	test@netscreen.com	-	-	Edit, Remove
user_2	ike	-	Enabled	user2@netscreen.com	-	-	Edit, Remove
user_3	ike	-	Enabled	user3@netscreen.com	-	-	Edit, Remove
user_4	ike	-	Enabled	user4@netscreen.com	-	-	Edit, Remove
user_5	ike	-	Enabled	user5@netscreen.com	-	-	Edit, Remove
user_6	ike	-	Enabled	user6@netscreen.com	-	-	Edit, Remove
user_7	ike	-	Enabled	user7@netscreen.com	-	-	Edit, Remove
user_8	ike	-	Enabled	user8@netscreen.com	-	-	Edit, Remove
user_9	ike	-	Enabled		-	-	Edit, Remove
user_10	ike	-	Enabled		-	-	Edit, Remove
user_11	ike	-	Enabled		-	-	Edit, Remove
user_12	ike	-	Enabled		-	-	Edit, Remove
user_13	ike		Enabled				Edit, Remove

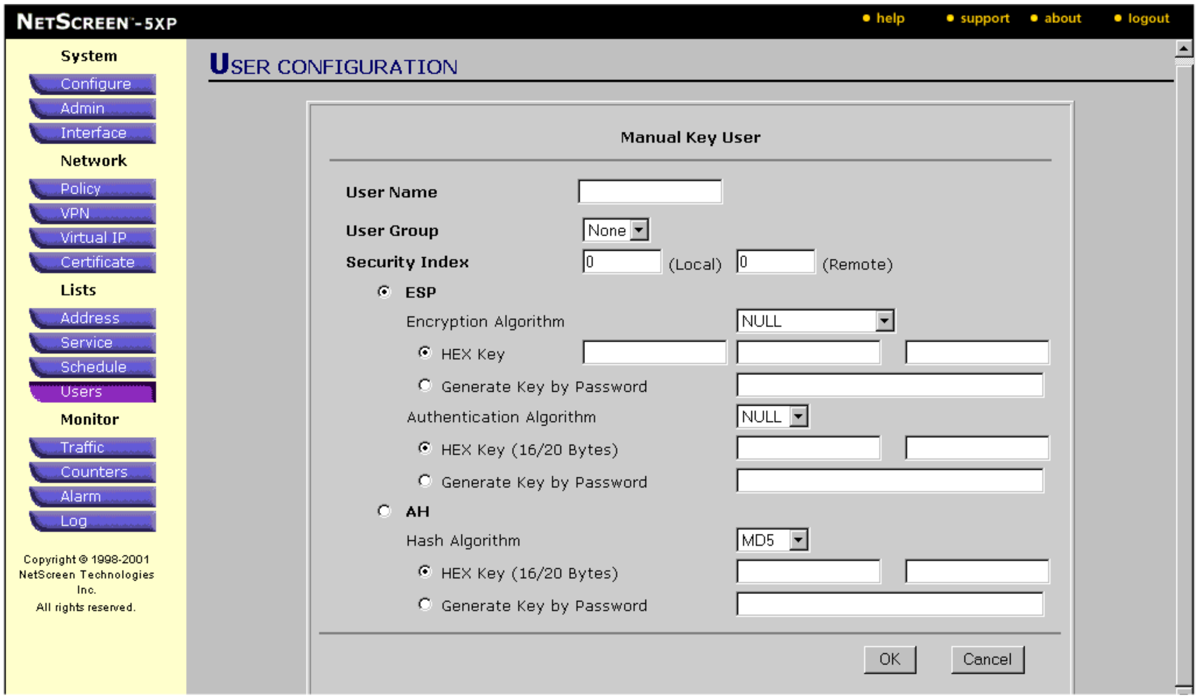
Figure 7-40 User Lists

2. Click **New User**, located at the bottom of the page.

   The User Configuration dialog box appears.

3. Enter the following information, as shown in Figure 7-41:
   - **User Name:** Hamid
   - **IKE Dynamic Peer:** Select this option.
   - **User Group:** None
   - **Identity:** pacbell.net

*For **Identity:** When using certificates, you must identify the device on which NetScreen-Remote is installed by its domain name.*



USER CONFIGURATION

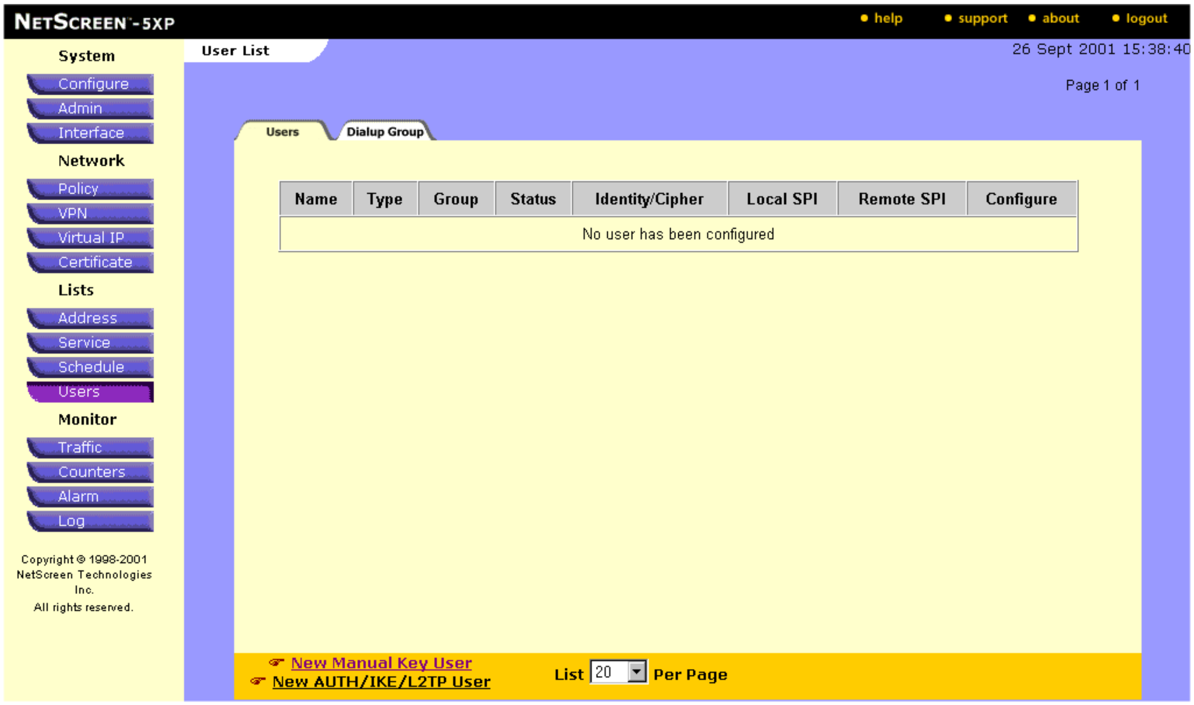
Manual Key User

User Name			
User Group	None		
Security Index	0 (Local)	0 (Remote)	
● ESP			
Encryption Algorithm		NULL	
● HEX Key			
○ Generate Key by Password			
Authentication Algorithm		NULL	
● HEX Key (16/20 Bytes)			
○ Generate Key by Password			
○ AH			
Hash Algorithm		MD5	
● HEX Key (16/20 Bytes)			
○ Generate Key by Password			

Figure 7-41 Users List

4. Leave everything else at the default values, and click **OK**, located at the bottom of the page.

The Users List appears with the name of the new remote user, as shown below.



User List

26 Sept 2001 15:38:40

Page 1 of 1

Name	Type	Group	Status	Identity/Cipher	Local SPI	Remote SPI	Configure
No user has been configured							

List 20 Per Page

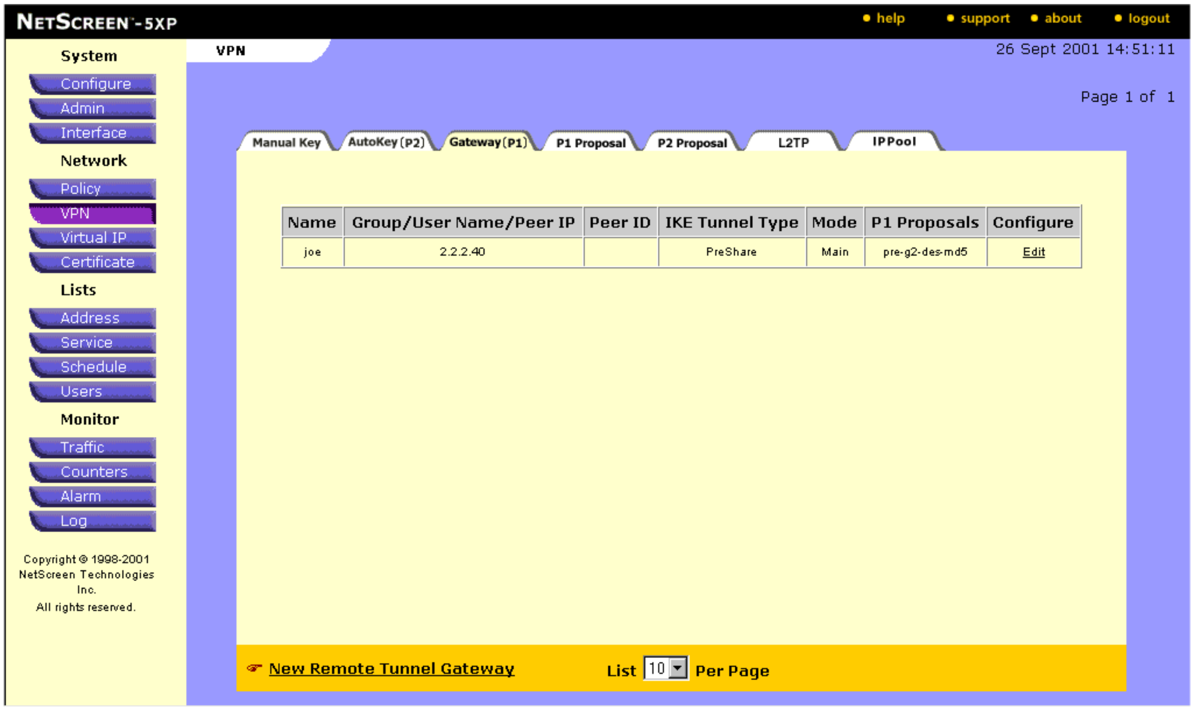
Figure 7-42 Users List

Step 4: Defining a Remote Gateway

Before you can set up an IKE tunnel for Dialup-to-LAN communication, you must define the remote gateway. This includes selecting an appropriate Phase 1 proposal for negotiating the building of the tunnel with the other end.

To create the gateway:

1. Click **VPN**, located under Network in the menu column.
2. Click the Gateway tab to bring the Gateways Listings page to the front, as shown below.

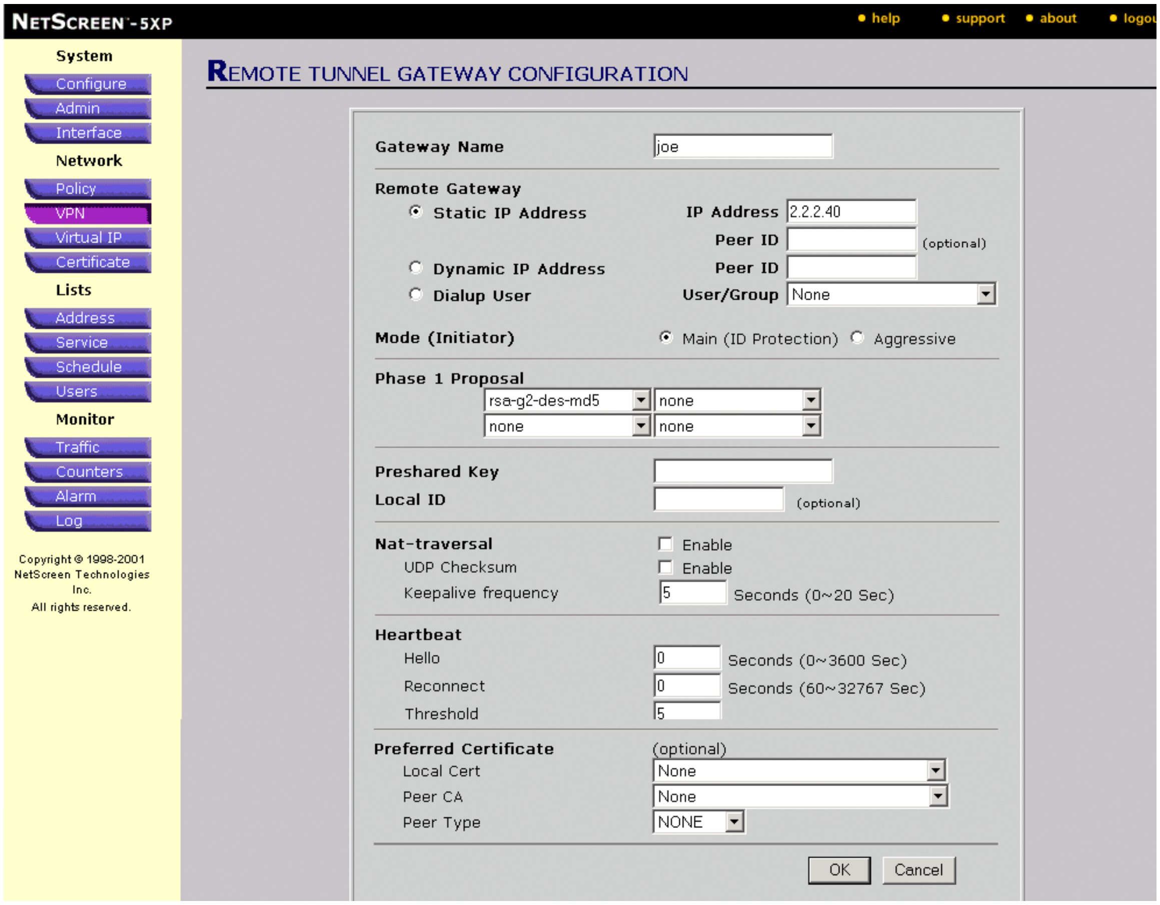


Name	Group/User Name/Peer IP	Peer ID	IKE Tunnel Type	Mode	P1 Proposals	Configure
joe	2.2.2.40		PreShare	Main	pre-g2-des-md5	Edit

Figure 7-43 Gateway Listings

3. At the bottom of the page, click **New Remote Gateway** to display the New Remote Gateway Tunnel Configuration dialog box.

4. Enter the following information, as shown in Figure 7-44.
   - **Name:** Hamid's home-PC
   - **Phase 1 Proposal:** rsa-g2-3des-sha
     To make configuration easier, the NetScreen-5 comes with a number of predefined Phase 1 proposals. This particular proposal uses Certificates, Diffie-Hellman Group 2 Perfect Forwarding Secrecy, and 3DES and SHA-1 for data encryption and authentication. The System Administrator can always create custom Phase 1 proposals.
   - **Mode:** Aggressive
   - **Remote Gateway/User - Dynamic IP address:** Select this option.
   - **Dynamic Peer/User/Group:** Dialup User - Hamid. *Hamid* is the name you entered in the User List in the last task.



REMOTE TUNNEL GATEWAY CONFIGURATION

Gateway Name: joe

Remote Gateway
- ● Static IP Address — IP Address: 2.2.2.40; Peer ID: (optional)
- ○ Dynamic IP Address — Peer ID:
- ○ Dialup User — User/Group: None

Mode (Initiator): ● Main (ID Protection) ○ Aggressive

Phase 1 Proposal: rsa-g2-des-md5; none; none; none

Preshared Key:
Local ID: (optional)

Nat-traversal: □ Enable
UDP Checksum: □ Enable
Keepalive frequency: 5 Seconds (0~20 Sec)

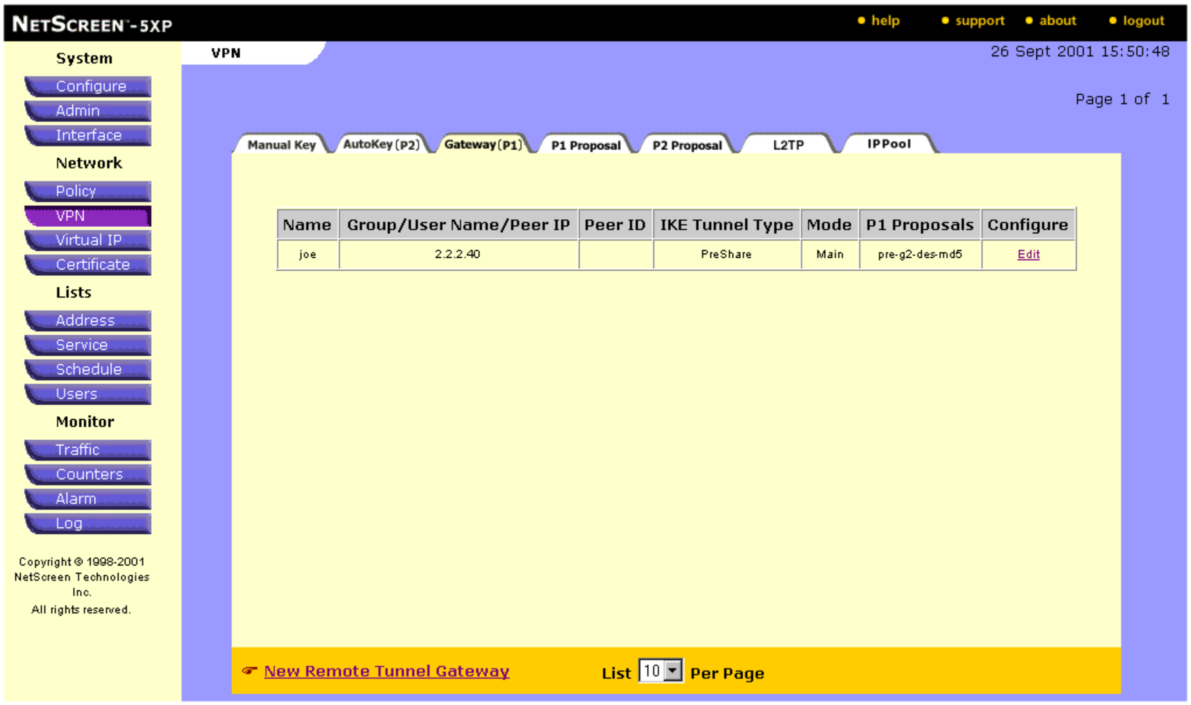
Heartbeat
Hello: 0 Seconds (0~3600 Sec)
Reconnect: 0 Seconds (60~32767 Sec)
Threshold: 5

Preferred Certificate (optional)
Local Cert: None
Peer CA: None
Peer Type: NONE

Figure 7-44 New Remote Gateway Tunnel Configuration

5. To save the settings, click **OK**.

The Gateway Listings page appears with the new entry, as shown below.



Name	Group/User Name/Peer IP	Peer ID	IKE Tunnel Type	Mode	P1 Proposals	Configure
joe	2.2.2.40		PreShare	Main	pre-g2-des-md5	Edit

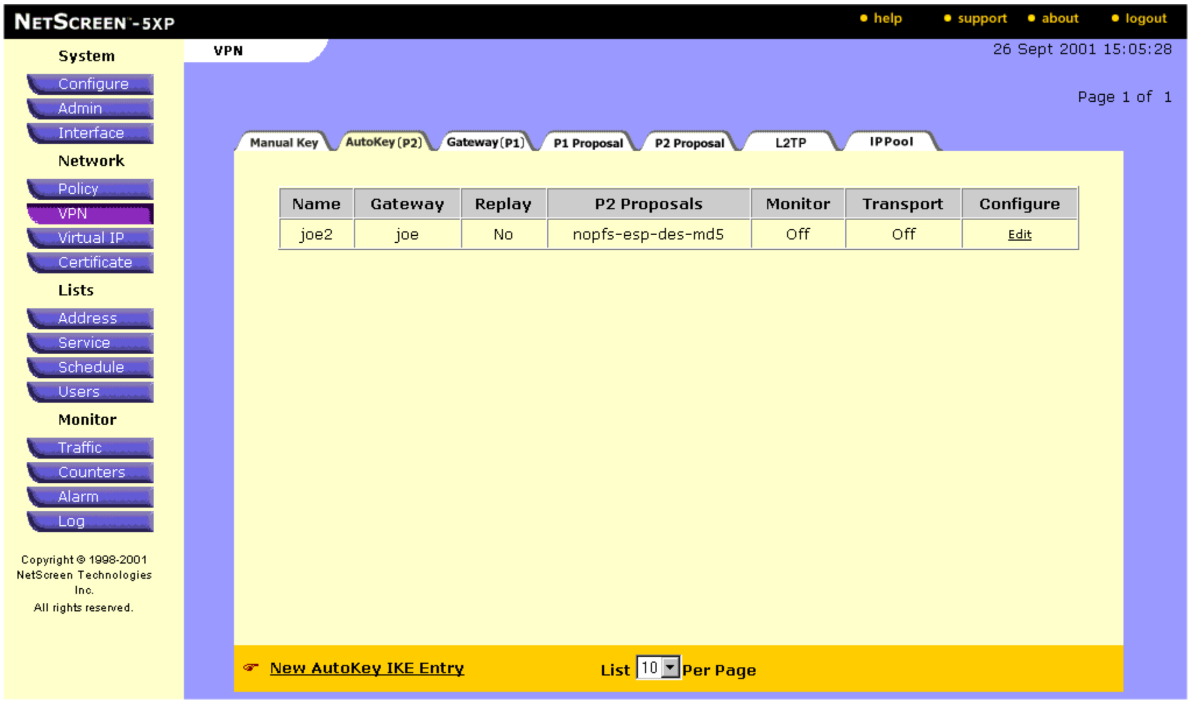
Figure 7-45 Gateway Listings with new gateway added

Step 5: Configuring an AutoKey IKE VPN Tunnel

So far, you have defined the new dialup user and the remote gateway. At this point, you must associate the remote gateway tunnel name with a Phase 2 Proposal describing how the data passing through the tunnel is to be encrypted and authorized.

1. Click **VPN**, located under Network in the menu column.

   The VPN pages appear with the AutoKey IKE page in front, as shown below.



26 Sept 2001 15:05:28

Page 1 of 1

Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure
joe2	joe	No	nopfs-esp-des-md5	Off	Off	Edit

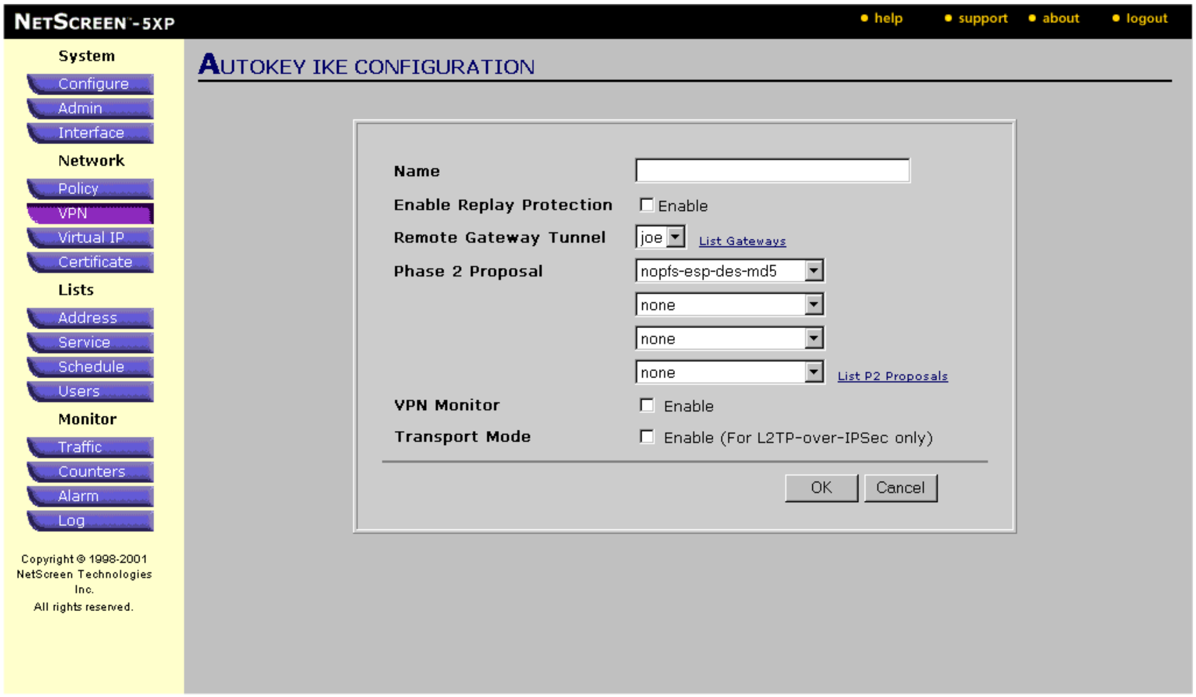
List 10 Per Page

Figure 7-46 VPN AutoKey IKE Page

2. Click **New AutoKey IKE Entry**, located in the lower-left corner of the page.

   The New AutoKey IKE Configuration dialog box appears.

3. Enter the following information, as shown in Figure 7-47:
   - **Name:** H-11
   - **Enable Replay Protection:** Select this option. This requires each IKE negotiation to have a sequence number.
   - **Remote Gateway Tunnel Name:** Hamid's home-PC, from the drop-down list. This is the name you assigned when you created the new remote gateway in the previous section.
   - **Phase 2 Proposal:** g2-esp-3des-sha
     This particular proposal uses Diffie-Hellman Group 2 with Perfect Forwarding Secrecy (PFS), and encapsulation with 3DES and SHA-1 for message encryption and authentication. To view the predefined proposals in detail, you can click on List Phase 2 Proposals. The default lifetime for the proposal selected in this particular scenario is 3600 seconds.



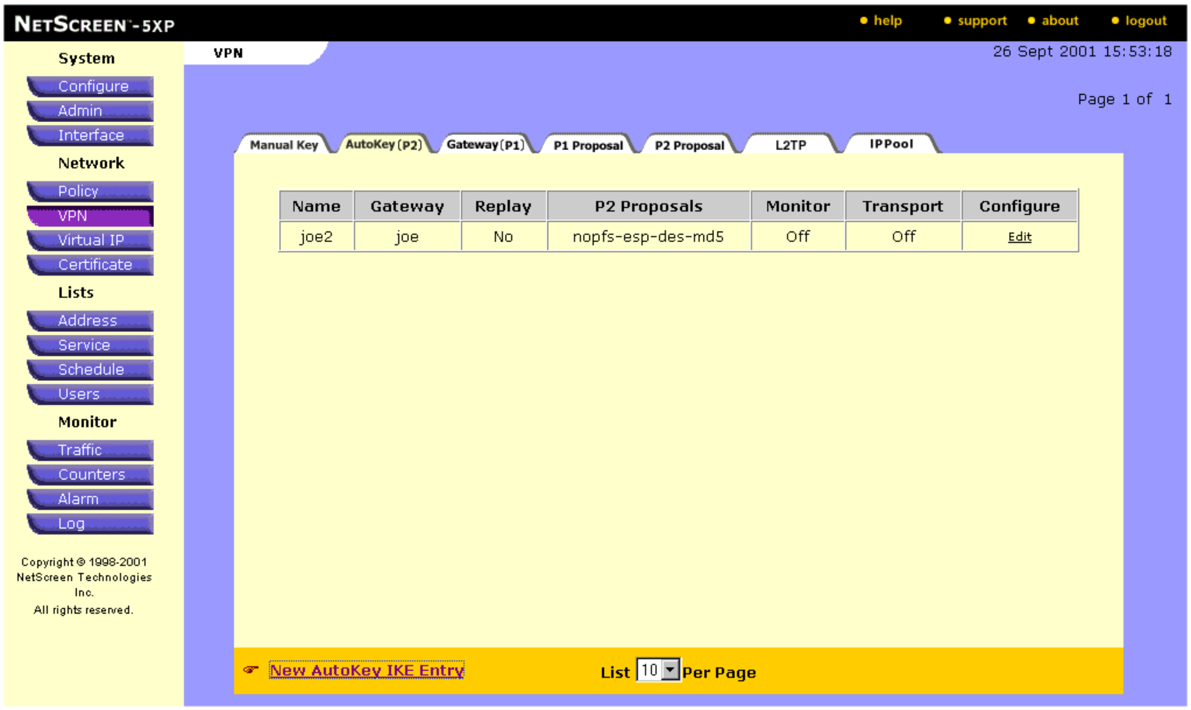
AUTOKEY IKE CONFIGURATION

Name	
Enable Replay Protection	□ Enable
Remote Gateway Tunnel	joe
Phase 2 Proposal	nopfs-esp-des-md5
	none
	none
	none
VPN Monitor	□ Enable
Transport Mode	□ Enable (For L2TP-over-IPSec only)

Figure 7-47 New AutoKey IKE Configuration

4. Click **OK** to save the new entry.

   The updated list of AutoKey IKE VPNs appears as shown below.



Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure
joe2	joe	No	nopfs-esp-des-md5	Off	Off	Edit

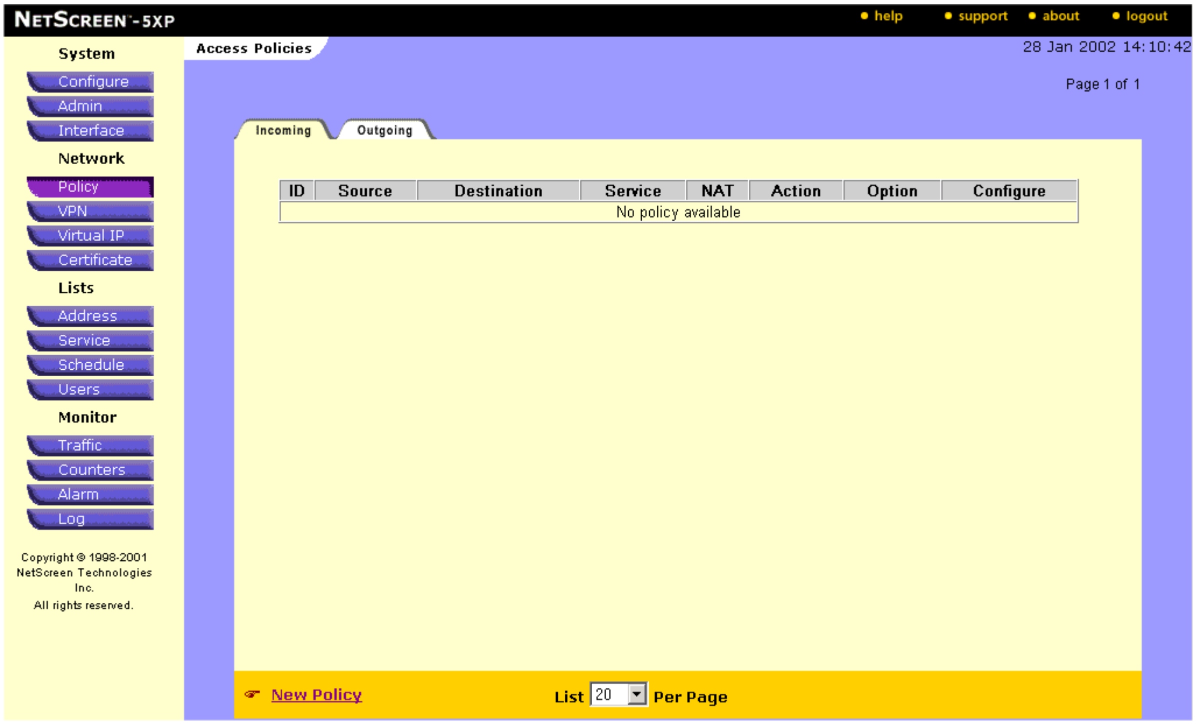
Figure 7-48 Updated List of AutoKey IKE VPNs

Step 6: Defining a VPN Access Policy

After you configure a VPN, you must define an Access Policy with the action set to *encrypt* and associate it with the VPN tunnel.

1. Click **Policy**, located under Network in the menu column.

   The Access Policies pages appear, as shown below.



ID	Source	Destination	Service	NAT	Action	Option	Configure
No policy available							

Figure 7-49 Access Policies Pages

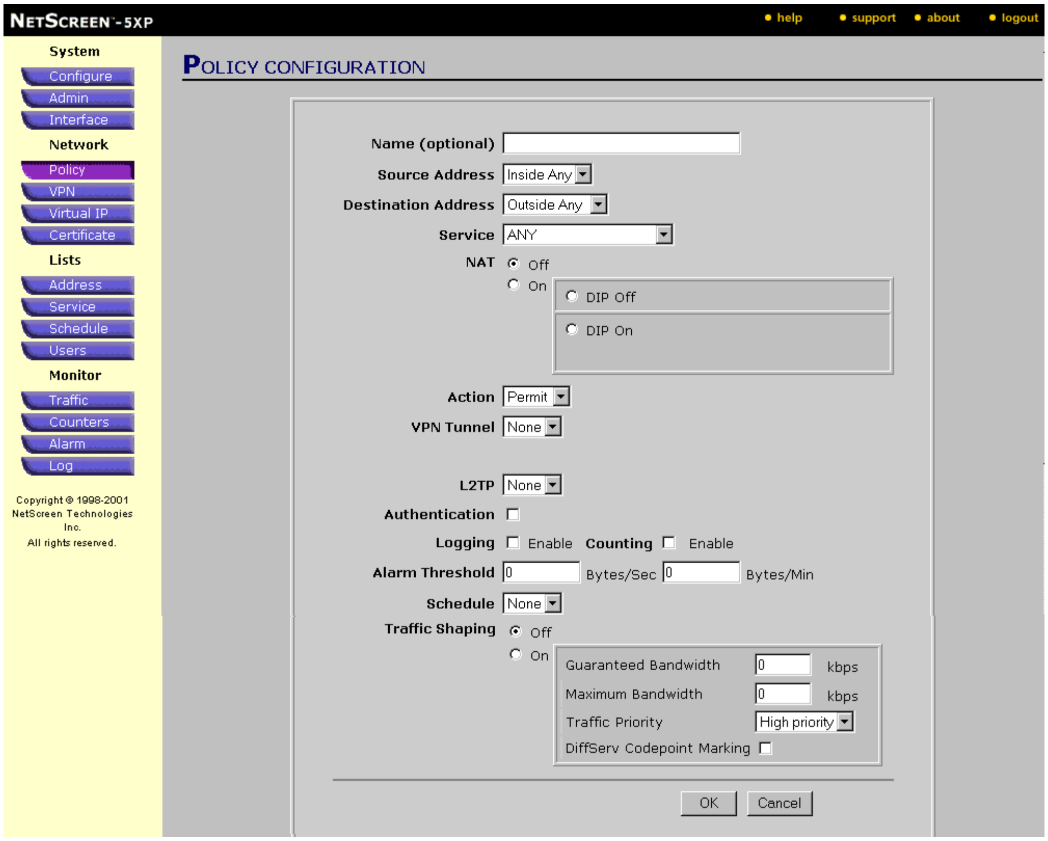
> *Although VPN Access Policies are defined for Outgoing traffic, VPN Access Policies assume bidirectional traffic and that the destination address can also originate VPN sessions.*

2. Click **New Policy**, located in the lower-left corner of the page.

   The Policy Configuration dialog box appears.

3. Enter the following information, as shown in Figure 7-50:
   - **Name (optional):** Hamid's Tunnel
   - **Source Address:** 172.16.10.11
   - **Destination Address:** Dial-Up VPN (from drop-down list)
   - **Service:** ANY
   - **Action:** Encrypt
   - **VPN Tunnel:** Hamid (from the drop-down list). This is the name you assigned to the new AutoKey IKE entry when you selected a Phase 2 Proposal in the last task.

   Leave the remaining fields at their default values.



POLICY CONFIGURATION

Name (optional)

Source Address: Inside Any

Destination Address: Outside Any

Service: ANY

NAT ● Off ○ On
○ DIP Off
○ DIP On

Action: Permit

VPN Tunnel: None

L2TP: None

Authentication □

Logging □ Enable Counting □ Enable

Alarm Threshold 0 Bytes/Sec 0 Bytes/Min

Schedule: None

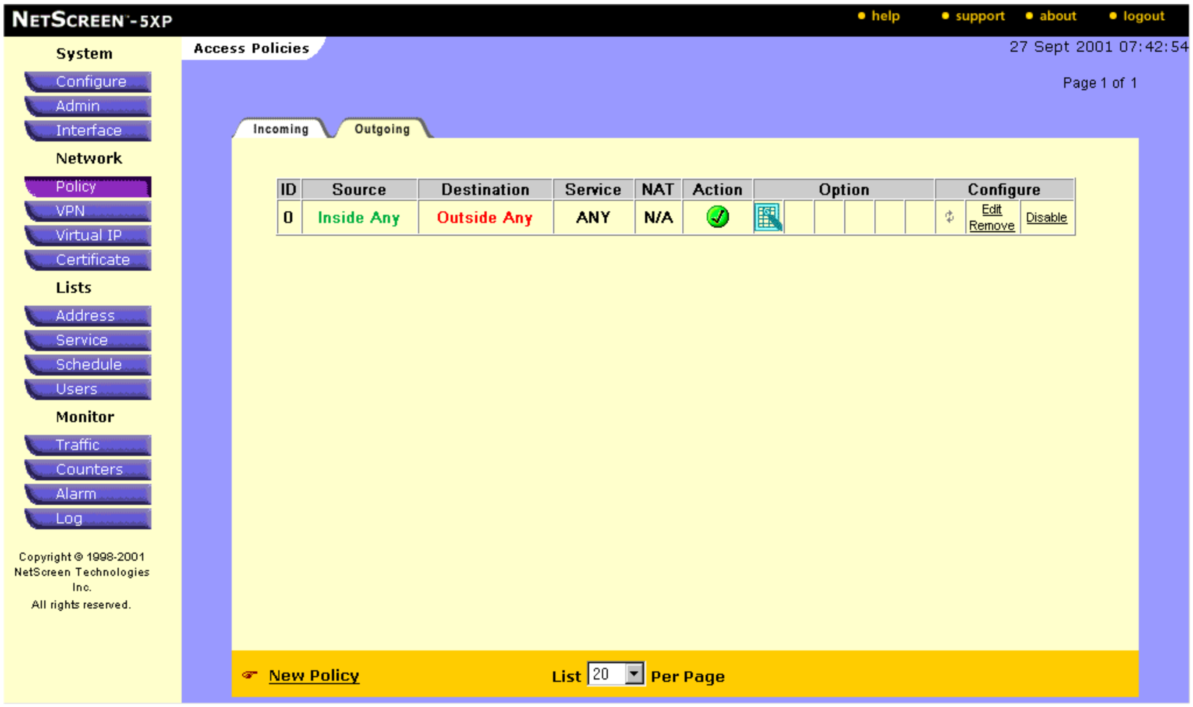
Traffic Shaping ● Off ○ On
Guaranteed Bandwidth 0 kbps
Maximum Bandwidth 0 kbps
Traffic Priority: High priority
DiffServ Codepoint Marking □

OK Cancel

Figure 7-50 Policy Configuration

4. Click **OK** to enter your settings.

The Outgoing Access Policies page appears with the new Access Policy added, as shown below.

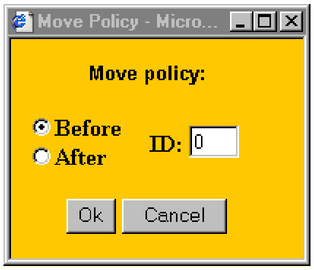


ID	Source	Destination	Service	NAT	Action	Option	Configure	
0	Inside Any	Outside Any	ANY	N/A	✓		Edit Remove	Disable

Figure 7-51 Outgoing Access Policies Page with New Access Policy

5. Since the VPN Access Policy is more restrictive than the generic "Inside Any /Outside Any" Access Policy, it needs to be at the top of the list of policies. To move the Access Policy to the top of the list, click the ↕ icon in the row for the Access Policy that you want to move.

The Move Policy dialog box appears.



Move policy:

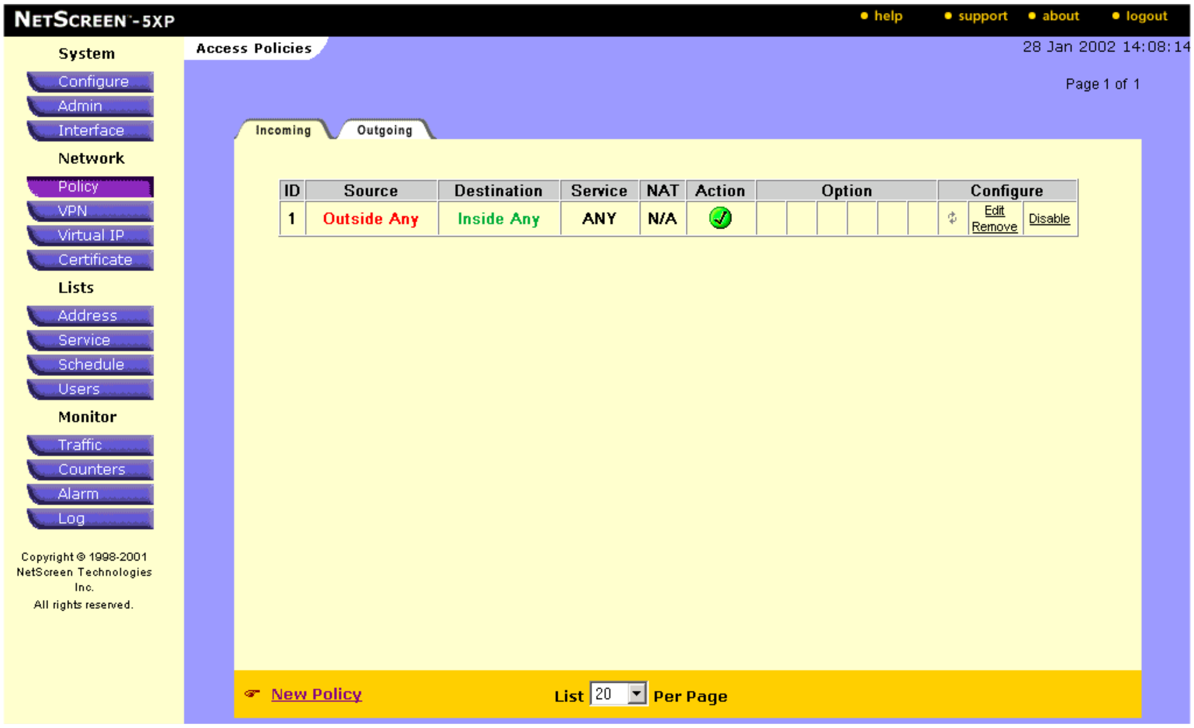
● Before
○ After

ID: 0

Figure 7-52 Move Policy

6. Fill in the information as needed to move the VPN Access Policy to the top, and then click **OK**.

   The updated Outgoing Access Policy page appears, as shown below.



Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

28 Jan 2002 14:08:14

Page 1 of 1

ID	Source	Destination	Service	NAT	Action	Option	Configure	
1	Outside Any	Inside Any	ANY	N/A	✓		Edit Remove	Disable

List 20 Per Page

Figure 7-53 Updated Outgoing Access Policy List

The NetScreen security-appliance end of the eventual Certificate/AutoKey (IKE) VPN tunnel is complete.

Setting up NetScreen-Remote

There are four steps to setting up NetScreen-Remote for a Pre-Shared/AutoKey IKE VPN tunnel:

1. Checking for Certificates
2. Creating a New Connection
3. Configuring Your Identity
4. Defining the IPSec Protocols

Step 1: Checking for Certificates

Before you can set up an AutoKey IKE VPN tunnel using certificates, you need to verify that all three of the following required files are already accessible in the Certificate Manager:

- A valid personal certificate (which serves as the device's identity)
- A valid CA certificate
- A certificate revocation list (CRL)

To make sure that you have the required files:

1. Right-click the **NetScreen-Remote** icon, located on the Windows taskbar.

   The NetScreen-Remote Shortcut menu appears, as shown below.

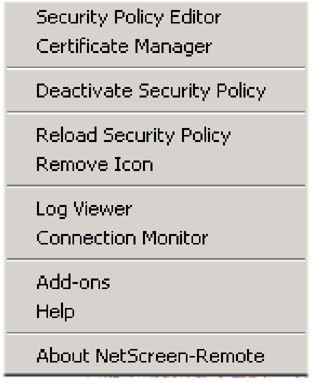
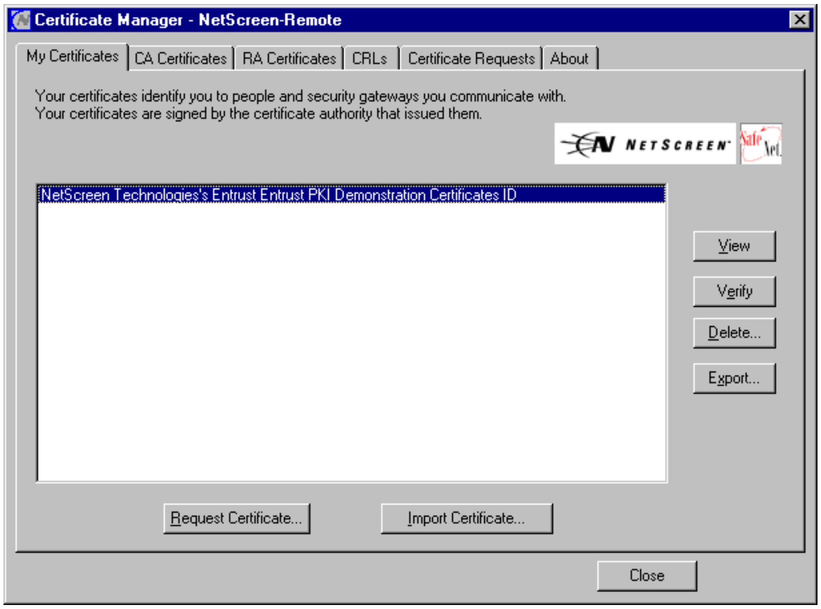


Figure 7-54 NetScreen-Remote Shortcut Menu

2. Choose **Certificate Manager**.

The Certificate Manager appears with My Certificates page in front, as shown below.



Your certificates identify you to people and security gateways you communicate with.
Your certificates are signed by the certificate authority that issued them.

NetScreen Technologies's Entrust Entrust PKI Demonstration Certificates ID

Figure 7-55 Certificate Manager

3. Make sure that a valid certificate is available by doing the following:
   - Select the Certificate you want to verify, and then click **View**.

     The personal certificate appears.
   - Check to see that the expiration date is still in the future.
4. Check for a valid CA Certificate and a valid CRL, using the same procedure outlined in step 3.

If no certificates or CRLs are listed, or if the certificate date is no longer valid, then see the instructions for obtaining certificates and CRLs in Chapter 3, "Digital Certificates" ."

Step 2: Creating a New Connection

You begin by initiating a new connection. You then name the connection, define it as secure, and determine the identification and location of the other end of the eventual VPN tunnel (that is, the NetScreen-5 device protecting your company's network).

1. Double-click the **NetScreen-Remote** icon, located on the Windows taskbar, to open the Security Policy Editor.
2. On the File menu, choose **New Connection**.

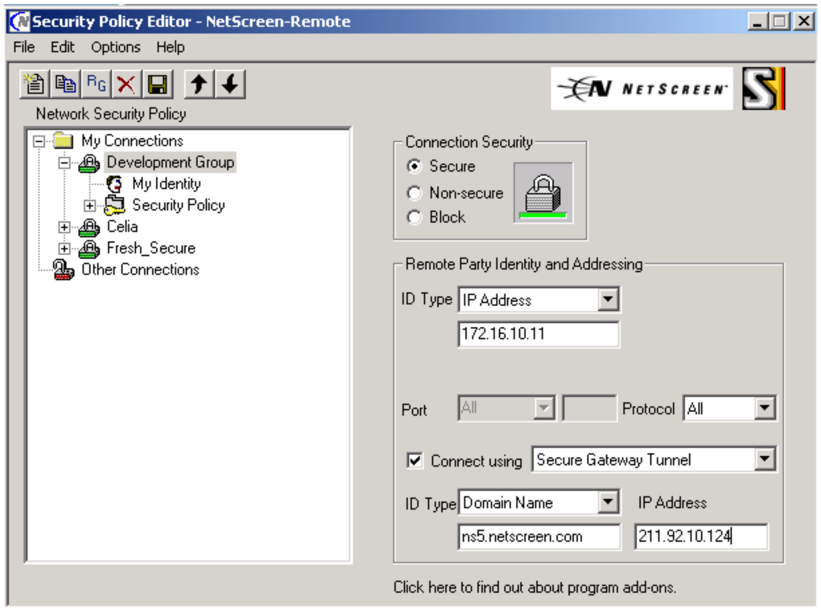
   A new connection icon appears in the Network Security Policy list.

3. Name the new connection **`Development Group`**.
4. In the Connection Security area to the right of the Network Security Policy list, select **Secure**.
5. In the Remote Party Identity and Addressing area, select **IP Address** in the ID Type drop-down list, and type **`172.16.10.11`** in the IP address field. (This is the endpoint of the VPN tunnel at the company site.)
6. Leave Protocol set at **All**.
7. Select **Connect using Secure Gateway Tunnel**.

   The Secure Gateway Tunnel ID Type and IP Address fields become available.

8. For ID Type, choose **Domain Name**, and type `ns5.netscreen.com` in the domain name field and `211.92.10.124` in the IP Address field. (This is the Untrusted port IP address of the NetScreen-5.)

   The completed Connection Security and Remote Party Identity and Addressing areas are shown below.



Connection Security

● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing

ID Type: IP Address
172.16.10.11
Port: All
Protocol: All
☑ Connect using: Secure Gateway Tunnel
ID Type: Domain Name
IP Address
ns5.netscreen.com
211.92.10.124

Figure 7-56 Connection Security, Remote Party Identity and Addressing

Step 3: Configuring Your Identity

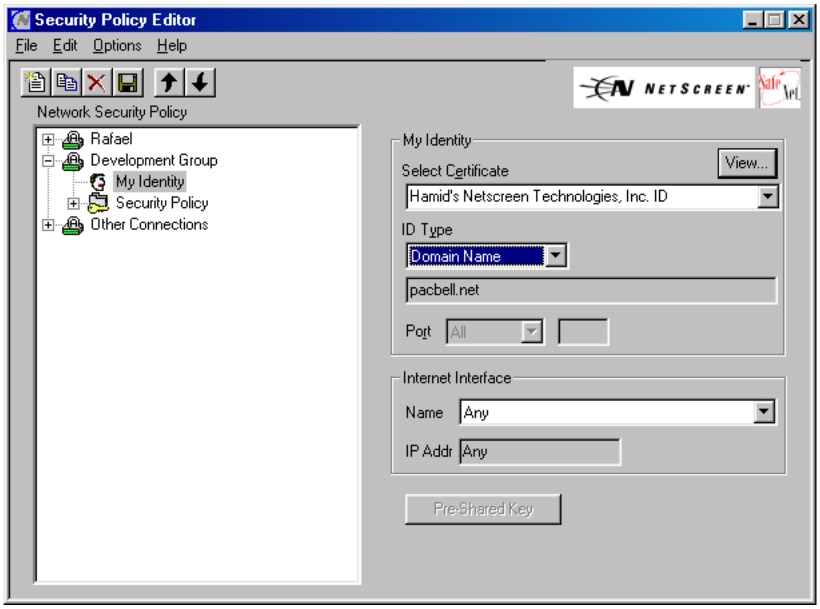
In this procedure, you configure your identity so that the party with whom you want to communicate can verify who you are. For this secure connection, you need to choose a digital certificate from the Certificate Manager.

1. Double-click the **Development Group** icon.

   The My Identity and Security Policy icons appear in the Network Security Policy list.

2. Click the **My Identity** icon.

   The My Identity and Internet Interface areas appear to the right of the Network Security Policy list, as shown below.



My Identity

Select Certificate: Hamid's Netscreen Technologies, Inc. ID

ID Type: Domain Name

pacbell.net

Port: All

Internet Interface

Name: Any

IP Addr: Any

Figure 7-57 My Identity and Internet Interface Areas

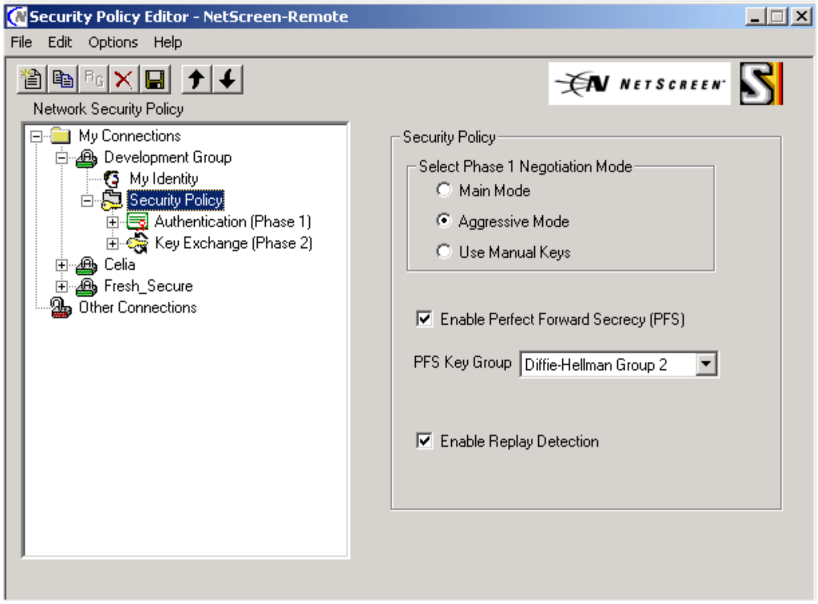
3. In the My Identity area, select a certificate from the Select Certificate drop-down list.
4. From the ID Type area, select **Domain Name**.
5. Save the entries.

Step 4: Defining the IPSec Protocols

In this procedure, you define the Internet Protocol Security (IPSec) protocols for securing the VPN tunnel.

1. Double-click the **Security Policy** icon in the Network Security Policy list.

   The Security Policy area appears on the right, and the Authentication (Phase 1) icon and Key Exchange (Phase 2) icon appear in the Network Security Policy list, as shown below.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

● Aggressive Mode

○ Use Manual Keys

☑ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

Figure 7-58 Security Policy Area

2. Select **Aggressive Mode** in the Security Policy area.

   This mode speeds the negotiation. As is necessary with a dialup client, identities are revealed before secure communications have been established, reducing the number of Phase 1 steps.

3. Uncheck the **Enable Perfect Forward Secrecy (PFS)** and **Enable Replay Detection** boxes.

4. In the Network Security Policy list, double-click the **Authentication (Phase 1)** icon.

   Proposal 1 appears below the Authentication (Phase 1) icon in the Network Security Policy list.

5. Click **Proposal 1** to display the Authentication Method and Algorithms area.

   The information you enter here must match the Phase 1 configuration you set up for the NetScreen-5 at the other end.

6. In the Authentication Method and Algorithms area, enter the following settings:

   – **Authentication Method:** RSA

   – **Encryption Algorithm:** Triple DES

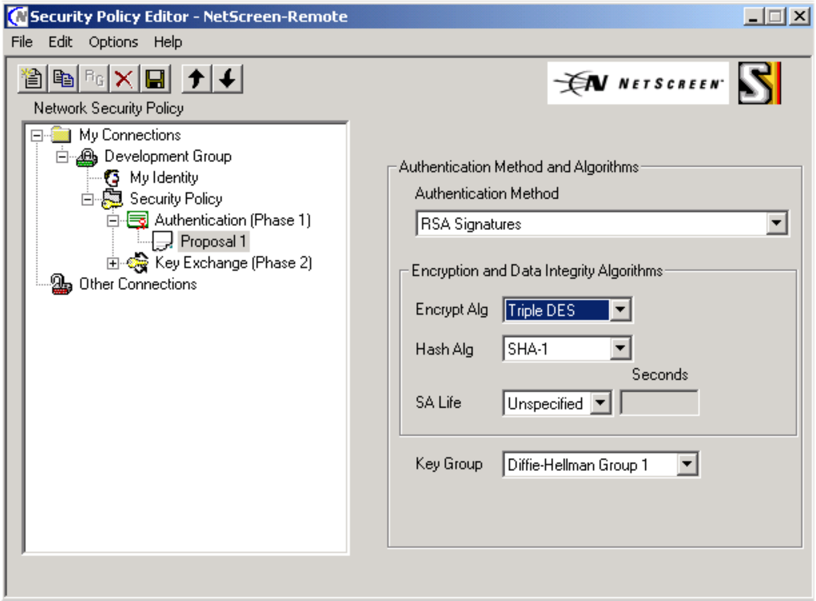
   – **Hash Algorithm:** SHA-1

   – **SA Life:** Seconds

   – **Seconds:** 28800

   – **Key Group:** Diffie-Hellman Group 2

   The completed Authentication Method and Algorithms area is shown below.



Authentication Method and Algorithms

Authentication Method: RSA Signatures

Encryption and Data Integrity Algorithms

Encrypt Alg: Triple DES

Hash Alg: SHA-1

SA Life: Unspecified

Seconds:

Key Group: Diffie-Hellman Group 1

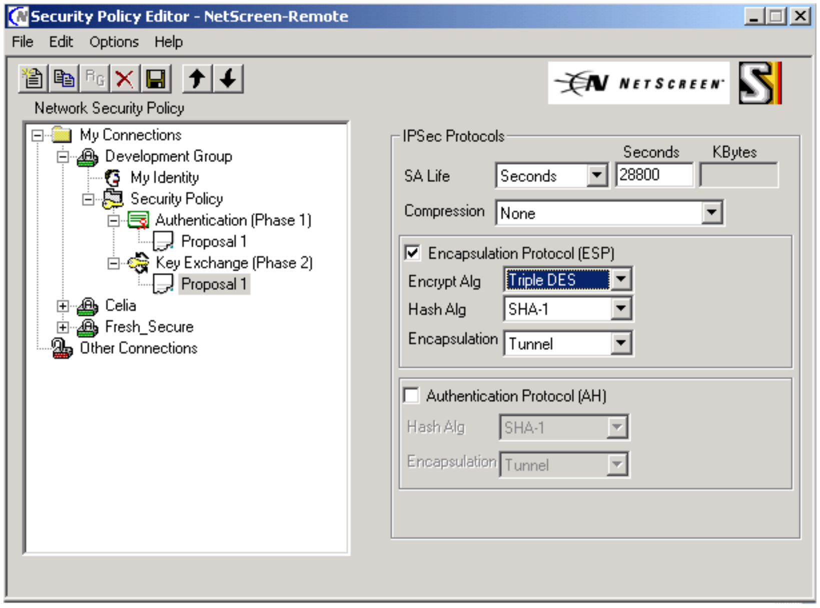
Figure 7-59 Completed Authentication Method and Algorithms Area

7. In the Network Security Policy list, double-click the **Key Exchange (Phase 2)** icon.

   Proposal 1 appears below the Key Exchange (Phase 2) icon in the Network Security Policy list. The information you enter here must match the Phase 2 configuration you set up for the NetScreen-5 at the other end.

8. Select **Proposal 1** to display the IPSec Protocols area.
9. In the IPSec Protocols area, enter the following settings:
   - **SA life:** Seconds
   - **Seconds:** 3600
   - **Encapsulation Protocol (ESP)**: Select this option.
   - **Encryption Algorithm:** Triple DES
   - **Hash Algorithm:** SHA-1
   - **Encapsulation:** Tunnel

   The completed IPSec Protocols area is shown below.



Network Security Policy

- My Connections
  - Development Group
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
        - Proposal 1
  - Celia
  - Fresh_Secure
- Other Connections

IPSec Protocols

SA Life: Seconds — Seconds: 28800 — KBytes:

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 7-60 Completed IPSec Protocols Area

10. Click the **Save** icon or choose **Save Changes** from the File menu.

    The NetScreen-Remote end of the eventual AutoKey (IKE) VPN tunnel is complete.

Making a Connection

With both ends of the tunnel configured, you are ready to make a secure VPN tunnel connection.

1. Launch your Web browser.
2. Enter an IP address within the network subnet, for example: **`http://172.16.10.250`**

   NetScreen-Remote, which continually checks all IP addresses that you enter, recognizes this address as the one you configured for a secure connection. It routes the transmission to the security gateway (that is, the untrusted port of the NetScreen-5) and proposes the VPN tunnel connection.

   The NetScreen-5 responds to this proposal by checking its database until it finds the Access Policy defining the proposed connection as a VPN tunnel.

   With the settings at both ends in accord, NetScreen-Remote and the NetScreen-5 begin using their local certificates and the specified ESP encryption (Triple DES) and authentication (SHA-1) algorithms to secure the connection.

   The VPN tunnel is established.

   After encrypting the tunnel for an hour (3600 seconds), the key automatically changes to another, random key, using the AutoKey IKE function.

Scenario 4: Back in the Office

In this scenario, you return to your office, where you want to connect to the company LAN with your laptop. Now that you are inside the firewall, you no longer need the security features of a VPN tunnel.

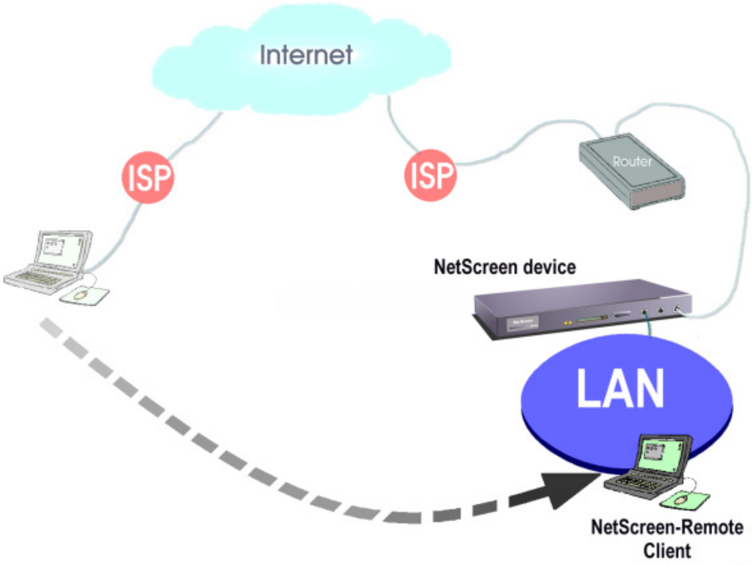


Figure 7-61 NetScreen-Remote Client Inside the Firewall

To use your laptop without the NetScreen-Remote security features, deactivate the Security Policy. Depending on the configuration, leaving NetScreen-Remote activated when within the firewall can result in being locked out of the local network.

1. Right-click the **NetScreen/SafeNet icon**, located on the taskbar in the lower-right corner of your desktop.

   The NetScreen-Remote shortcut menu appears.

2. Click **Deactivate Security Policy**.

   The NetScreen-Remote client stops monitoring your network activity.

To reactivate NetScreen-Remote, repeat the above steps, selecting ***Activate Security Policy*** *instead. (When NetScreen-Remote is deactivated, the* ***Deactivate Security Policy*** *command changes to* ***Activate Security Policy****.)*

Large Scale Distribution with NetScreen-Global PRO

8

VPN Policies for the NetScreen-Remote can be centrally managed with NetScreen-Global PRO. VPN policies for the NetScreen-Remote are configured from within Global-PRO. When the user logs in with their NetScreen-Remote, the user's VPN policy is sent using the NetScreen-Remote.

See the *Global-PRO Administrator's Guide* for information on how to configure VPN policies within Global-PRO for the NetScreen-Remote.

Deploying NetScreen-Remote clients on a large scale is a straight forward process. Basically, it consists of the following steps, which are described in this chapter:

- Centralizing Distribution of Common Files

  For ease of distribution, export the NetScreen-Remote installation files to a central location from which your users can access them, usually HTTP or Windows Drive Share.

- Repackaging The Installation for Use with NetScreen-Global PRO

  In some deployments of NetScreen-Remote, customizing or "repackaging" the installation package for easy distribution may be necessary.

- Using NetScreen-Remote Login

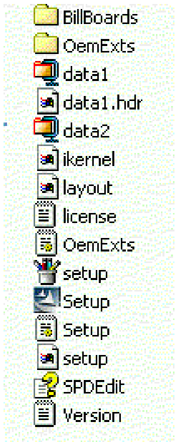
  Once invoked, a remote user must authenticate herself or himself with a User ID and Password. Only after the User ID and Password is verified against the Global-PRO Arbitrator will that user's VPN policy be downloaded into NetScreen-Remote.

- NetScreen-Remote Security Policy Editor — Display Only

  VPN policies downloaded from Global-PRO are locked and cannot be modified by the user.

Centralizing Distribution of Common Files

Each user needs to be able to download common NetScreen-Remote installation files. The complete set of software files is shown below.



BillBoards
OemExts
data1
data1.hdr
data2
ikernel
layout
license
OemExts
setup
Setup
Setup
setup
SPDEdit
Version

Figure 8-1 NetScreen-Remote Installation Software Files

Place NetScreen-Remote installation files on a website or a network drive share from which users can download these files.

Repackaging The Installation for Use with NetScreen-Global PRO

In some deployments of NetScreen-Remote, it may be beneficial for the administrator to customize or "repackage" the installation package for easy distribution in a specific environment. This is sometimes referred to as "Repackaging" the installation. Some of the reasons for repackaging the installation include:

- Defining Installation Parameters (e.g. Program Group, Install Path)
- Installing additional programs in-conjunction with NetScreen-Remote
- Hiding all end-user prompts during installation (Silent Install)
- Executing an automatic reboot after installation is complete
- Including default policy files or certificates
- Installing shortcuts in the start menu
- Hiding tray icons from the end-users
- Locking access to policy editor, certificate manager or log viewer

- Defining Global-PRO Servers for policy retrieval

Note: When deploying NetScreen-Remote with NetScreen-Global PRO, it is necessary to repackage the installation to include Global-PRO Server IP Address and other parameters in the Default.ANG file.

The first step to repackaging is to copy files from the read-only CD-ROM filesystem to a writable filesystem for modification. To ensure you copy all necessary files, a ZIP file of the NetScreen-Remote distribution on CD-ROM has ben created. First UnZip the file "NetScreen-Remote.ZIP" from the CD-ROM to suitable location for repackaging. Once the files have been copied to writable filesystem, a number of text-configuration files may be modified to change install behavior.

Software Distribution

After NetScreen-Remote has been repackaged for your environment, install files may be burned on to another CD-ROM for distribution to users. If you wish to automate your installs, installation files could be placed on a web page or network drive share from which end-users will have access to and called via a login script or batch file sent to the user.

Since it is possible to run the entire installation silently, that is with no user-interface, NetScreen-Remote could be installed distributed with any enterprise software management system (such as Microsoft's SMS) automatically or installed via login scripts or batch files.

Installation Configuration Files

Default.ANG

This file is located on the NetScreen-Remote program install directory inside the setup\OemExts\ANG directory and is used for NetScreen-Remote integration with NetScreen-Global PRO. You need to modify this file if you wish to connect your NetScreen-Remote Clients to Global-PRO Arbitrator for VPN policy retrieval. *If you are not using Global-PRO there is no need to modify this file.* The file only needs to be modified once for the entire NetScreen-Remote install base and may be used by all users connecting to that Global-PRO Arbitrator. This configuration file tells NetScreen-Remote where to contact your Global-PRO Arbitrator, which Policy Domain you are a member of and important certificate information used to authenticate the Global-PRO Server itself to ensure you are getting a VPN Policy from a valid Global-PRO Arbitrator.

Multiple *.ANG files may exist in the installation directory, each one will be installed with NetScreen-Remote as a separate profile, during login the user may select which profile they wish to use. The filename of the *.ANG file is used as the name for the profile. For example Corperate.ang would display as profile "Corporate" If a filename default.ang exists - it will always be used as the default connection profile.

Default.ANG Example:

```
#MON NOV 19 20:30:00 PDT 2001

LastUser=Guest
AngName=default.ang
DefaultSuffix=cn=users,cn=AcmeDomain,o=Global-PRO
PrependPrefix=cn=

[Arbitrator]
CertificateName=CN=2435823409852304985
ArbitratorAddress=10.150.42.100
ArbitratorPort=1099
SSL=true
retrycount=1
timeout=20

[Arbitrator]
CertificateName=CN=2344023985023934424
ArbitratorAddress=10.150.42.1098
ArbitratorPort=1099
SSL=true
retrycount=1
timeout=30
```

LastUser defines the username last used by the application, it is used by the program to internally to keep track of which user was used as last-login.

AngName defines the profile last used by the user, it is used by the program internally to keep track of which profile was used as last-login.

DefaultSuffix defines which LDAP Container / Global-PRO Policy Domain remote users for this profile are stored in. In most configurations you will use cn=users,cn=AcmeDomain,o=Global-PRO --where AcmeDomain is replaced with your Global-PRO Policy Domain name. These fields are case-sensitive. This field is required.

[*Arbitrator*] The Arbitrator Sections defines values for NetScreen Global-PRO Arbitrators. It is possible to have multiple Global-PRO Arbitrators defined for failover purposes. In the example above, we define only two servers, the first defined [Arbitrator] section is used for primary communications. However if a connection cannot be made before the timeout value is exceeded, NetScreen-Remote will failover to the next [Arbitrator] listed.

CertificateName is where the common-name (CN) of the Global-PRO Arbitrator certificate is defined. The Certificate Name (CN) is always equal to the serial number of your Global-PRO Arbitrator. NetScreen-Remote will always authenticate the Global-PRO Arbitrator first, to ensure you the user is sending their authentication credentials to a valid Global-PRO Arbitrator. This field is required.

ArbitratorAddress refers to the hostname or IP Address of the Global-PRO Arbitrator. This field is required.

ArbitratorPort refers to the TCP Port number of the Global-PRO Arbitrator. The default port is 1099. This field is required.

SSL must always be set to "true" as NetScreen-Global PRO will only accept connections from hosts via SSL. This field is required.

RetryCount defines the number of re-connect attempts NetScreen-Remote will attempt before failing over to the next Global-PRO Arbitrator. This field is required.

Timeout defines the number of seconds NetScreen-Remote will wait for a successful TCP connection to Global-PRO Arbitrator before attempting a retry.

OEMInstall.INI

This default OEMInstall.ini file is located in the installation directory within the /setup folder of NetScreen-Remote. You may modify some sections of this configuration file to customize the install for your environment. Environment variables defined on the local machine may be used inside this file. You should only modify sections outlined in bold. If other sections of this file (those labeled "Do not change") are modified, it may cause adverse effects to the installation of the software and/or target machine.

[OemExtensions]

RebootTimeout=30

The RebootTimeout key is to configure NetScreen-Remote installation processing to use a time-delayed reboot mechanism. When provided, the RebootTimeout key value specifies (in decimal) the number of seconds to wait before automatically rebooting the system when a reboot is required.

[DialogWelcome]

EnableDialog=Yes

The EnableDialog key of the DialogWelcome section may be used to enable or disable presentation of the Welcome Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

[DialogLicense]

EnableDialog=Yes

The EnableDialog key of the DialogLicense section may be used to enable or disable presentation of the License Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

[DialogDestPathandType]

EnableDialog=Yes

The EnableDialog key of the DialogDestPathandType section may be used to enable or disable presentation of the Destination Path and Setup Type Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

TargetDir="%ISV_PROGRAMFILES%\NetScreen\NetScreen-Remote"

The TargetDir key of the DialogDestPathandType section may be used to configured the default target directory for the installation. The default value for this is C:\Program Files\NetScreen\NetScreen-Remote.

[DialogProgramFolder]

EnableDialog=No

The EnableDialog key of the DialogProgramFolder section may be used to enable or disable presentation of the Program Folder Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "No".

AdministratorGroup=Yes

The AdministratorGroup key of the DialogProgramFolder section may be used to indicate the group to receive menu shortcuts created by NetScreen-Remote installation processing. Defined values of the AdministratorGroup Key are "Yes" and "No". The default value used when the AdministratorGroup Key does not exist is "Yes".

ProgramFolder="NetScreen-Remote"

The ProgramFolder key of the DialogProgramFolder section may be used to indicate the group to receive menu shortcuts created by NetScreen-Remote installation processing. As it is defined, the ProgramFolder key value contains the menu specification of the program group to contain the menu shortcuts. The default Program Group is "NetScreen-Remote"

[DialogSummary]

EnableDialog=Yes

The EnableDialog key of the DialogSummary section may be used to enable or disable presentation of the Summary Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

[EntriesStartup]

The EntriesStartup section of the Installation Configuration File contains information relating to the startup shortcuts created by the NetScreen-Remote installation process. The keys defined for the EntriesStartup section are detailed in the following subsections.

Certificate Manager=No

The "Certificate Manager" key of the EntriesStartup section may be used to enable or disable creation of the Certificate Manager shortcut by the NetScreen-Remote installation process. Defined values of the "Certificate Manager" key are "Yes" and "No". The default value used when the "Certificate Manager" key does not exist is "Yes".

Security Policy Editor=No

The "Security Policy Editor" key of the EntriesStartup section may be used to enable or disable creation of the Security Policy Editor shortcut by the NetScreen-Remote installation process. Defined values of the "Security Policy Editor" key are "Yes" and "No". The default value used when the "Security Policy Editor" key does not exist is "Yes".

Tray Icon=Yes

The "Tray Icon" key of the EntriesStartup section may be used to enable or disable creation of the Tray Icon shortcut by the NetScreen-Remote installation process. Defined values of the "Tray Icon" key are "Yes" and "No". The default value used when the "Tray Icon" key does not exist is "No".

Log Viewer=No

The "Log Viewer" key of the EntriesStartup section may be used to enable or disable creation of the Log Viewer shortcut by the NetScreen-Remote installation process. Defined values of the "Log Viewer" key are "Yes" and "No". The default value used when the "Log Viewer" key does not exist is "Yes".

Connection Monitor=No

The "Connection Monitor" key of the EntriesStartup section may be used to enable or disable creation of the Connection Monitor shortcut EntriesStartup the NetScreen-Remote installation process. Defined values of the "Connection Monitor" key are "Yes" and "No". The default value used when the "Connection Monitor" key does not exist is "Yes”.

Help=No

The "Help" key of the EntriesStartup section may be used to enable or disable creation of the Help shortcut by the NetScreen-Remote installation process. Defined values of the "Help" key are "Yes" and "No". The default value used when the "Help" key does not exist is "Yes".

L2TP Config Utility=No

The "L2TP Config Utility" key of the EntriesStartup section may be used to enable or disable creation of the L2TP Config Utility shortcut by the NetScreen-Remote installation process. Defined values of the "L2TP Config Utility" key are "Yes" and "No". The default value used when the "L2TP Config Utility" key does not exist is "Yes".

[EntriesMenu]

The EntriesMenu section of the Installation Configuration File contains information relating to the shortcuts displayed in Program group menus. The keys defined for the EntriesMenu section are detailed in the following subsections.

Certificate Manager=No

The "Certificate Manager" key of the EntriesMenu section may be used to enable or disable creation of the Certificate Manager shortcut by the NetScreen-Remote installation process. Defined values of the "Certificate Manager" key are "Yes" and "No". The default value used when the "Certificate Manager" key does not exist is "Yes".

Security Policy Editor=No

The "Security Policy Editor" key of the EntriesMenu section may be used to enable or disable creation of the Security Policy Editor shortcut by the NetScreen-Remote installation process. Defined values of the "Security Policy Editor" key are "Yes" and "No". The default value used when the "Security Policy Editor" key does not exist is "Yes".

Tray Icon=Yes

The "Tray Icon" key of the EntriesMenu section may be used to enable or disable creation of the Tray Icon shortcut by the NetScreen-Remote installation process. Defined values of the "Tray Icon" key are "Yes" and "No". The default value used when the "Tray Icon" key does not exist is "No".

Log Viewer=No

The "Log Viewer" key of the EntriesMenu section may be used to enable or disable creation of the Log Viewer shortcut by the NetScreen-Remote installation process. Defined values of the "Log Viewer" key are "Yes" and "No". The default value used when the "Log Viewer" key does not exist is "Yes".

Connection Monitor=No

The "Connection Monitor" key of the EntriesMenu section may be used to enable or disable creation of the Connection Monitor shortcut by the NetScreen-Remote installation process. Defined values of the "Connection Monitor" key are "Yes" and "No". The default value used when the "Connection Monitor" key does not exist is "Yes”.

Help=No

The "Help" key of the EntriesMenu section may be used to enable or disable creation of the Help shortcut by the NetScreen-Remote installation process. Defined values of the "Help" key are "Yes" and "No". The default value used when the "Help" key does not exist is "Yes".

L2TP Config Utility=No

The "L2TP Config Utility" key of the EntriesMenu section may be used to enable or disable creation of the L2TP Config Utility shortcut by the NetScreen-Remote installation process. Defined values of the "L2TP Config Utility" key are "Yes" and "No". The default value used when the "L2TP Config Utility" key does not exist is "Yes".

[EntriesPopup]

The EntriesPopup section of the Installation Configuration File contains information relating to the pop-up menu displayed by the Tray Icon application. The keys defined for the EntriesPopup section are detailed in the following subsections.

Certificate Manager=Yes

The "Certificate Manager" key of the EntriesPopup section may be used to enable or disable creation of the Certificate Manager shortcut by the NetScreen-Remote installation process. Defined values of the "Certificate Manager" key are "Yes" and "No". The default value used when the "Certificate Manager" key does not exist is "Yes".

Security Policy Editor=Yes

The "Security Policy Editor" key of the EntriesPopup section may be used to enable or disable creation of the Security Policy Editor shortcut by the NetScreen-Remote installation process. Defined values of the "Security Policy Editor" key are "Yes" and "No". The default value used when the "Security Policy Editor" key does not exist is "Yes".

Log Viewer=Yes

The "Log Viewer" key of the EntriesPopup section may be used to enable or disable creation of the Log Viewer shortcut by the NetScreen-Remote installation process. Defined values of the "Log Viewer" key are "Yes" and "No". The default value used when the "Log Viewer" key does not exist is "Yes".

Connection Monitor=Yes

The "Connection Monitor" key of the EntriesPopup section may be used to enable or disable creation of the Connection Monitor shortcut by the NetScreen-Remote installation process. Defined values of the "Connection Monitor" key are "Yes" and "No". The default value used when the "Connection Monitor" key does not exist is "Yes".

Help=Yes

The "Help" key of the EntriesPopup section may be used to enable or disable creation of the Help shortcut by the NetScreen-Remote installation process. Defined values of the "Help" key are "Yes" and "No". The default value used when the "Help" key does not exist is "Yes".

Executing a Custom Installation

If OemExts is not in the setup directory, you may have to first tell the NetScreen-Remote program the location of your configuration file. This location may be a local, relative path or a network path (e.g. \\serverA\config\install.ini) There are two ways to tell the NetScreen-Remote installer to use your custom configuration: A command-line argument to setup or in the setup.ini file. The command-line flag allows your install configuration file to reside in a separate location to your installation CD-ROM.

> ***Note:*** By default, NetScreen-Remote installer will use OEMInstall.ini file located in the setup directory of the CD-ROM for install configuration.

Command-Line

You can run Setup of NetScreen-Remote from the command-prompt or batch file with the path to the install configuration file. To use the local file install.ini for configuration:

```
setup.exe -xInstall.ini
```

To use a network file \\serverA\configs\OEMinstall.ini for configuration

```
Setup.exe -x\\serverA\configs\OEMinstall.ini
```

Defined in Setup.ini

In the setup.ini file on the install directory, you may also modify the "CmdLine=" line to define the location of the install configuration file. The following example would use the local file Install.ini for install configuration.

File: Setup.INI

```
[Startup]

CmdLine=-xInstall.ini# Define install file here

EnableLangDlg=Y         # Do not change

AppName=NetScreen-Remote# Do not change
```

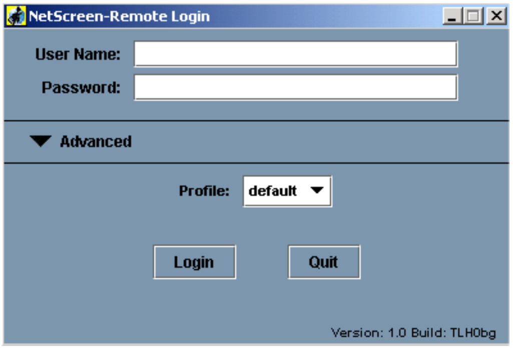
```
ProductGUID=2f931b84-0cee-11d1-aa7d-0080ad1ac47a# Do not change

[Languages]           # Do not changeDefault=0x0009# Do not
change

count=1                    # Do not change

key0=0x0009                # Do not change
```

Using NetScreen-Remote Login

To use NetScreen-Remote Login, you must have NetScreen Global-PRO properly installed and configured in a properly repackaged NetScreen Remote installation with valid Default.ANG. Once you successfully install NetScreen-Remote and reboot your machine to establish VPN tunnels, you must do the following:

- Launch NetScreen-Remote Login (Start->NetScreen-Remote Login)
- Enter a valid Username and Password
- Press **OK**

If you have configured multiple profiles, you may click on **Advanced** to select between them by selecting the desired profile in the drop-down Profile menu.



Profile: default

Version: 1.0 Build: TLH0bg

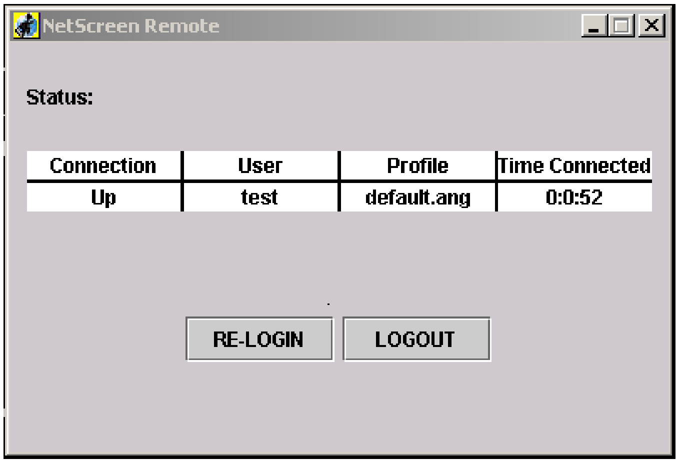
Figure 8-2 NetScreen-Remote Login - Advanced Settings

If your password is authenticated successfully, then your VPN policy will be automatically downloaded from the Global-PRO Arbitrator. This download will occur over a secure TLS channel using 3DES encryption – no VPN is required to use the NetScreen-Remote Login Connection Manager; however, proper ports must be open to the Global-PRO Arbitrator from all external firewalls. These ports are TCP/11111, TCP/1112, TCP/1099, and TCP/42496.

When one exits the NetScreen-Remote Login application, the VPN policy may be purged from NetScreen-Remote, a user will not be able to connect to the VPN again until they re-launch NetScreen-Remote Login Connection Manager and authenticate again. If the Global-PRO administrator has disabled policy purge, VPN polices will remain active upon logout and will be overwritten when the user logs in again.

VPN policy is user based, so if a user named Joe uses machine A to log into NetScreen-Remote Login, he will get the same VPN policy if he logs into machine B as Joe. Tying VPN policies to users as opposed to machines gives the administrator more flexibility when defining VPN access policies and gives the user the capability to login from anywhere without manually reconfiguring NetScreen-Remote.

If a user double-clicks on the NetScreen-Remote Login icon, their connect status and duration is displayed:



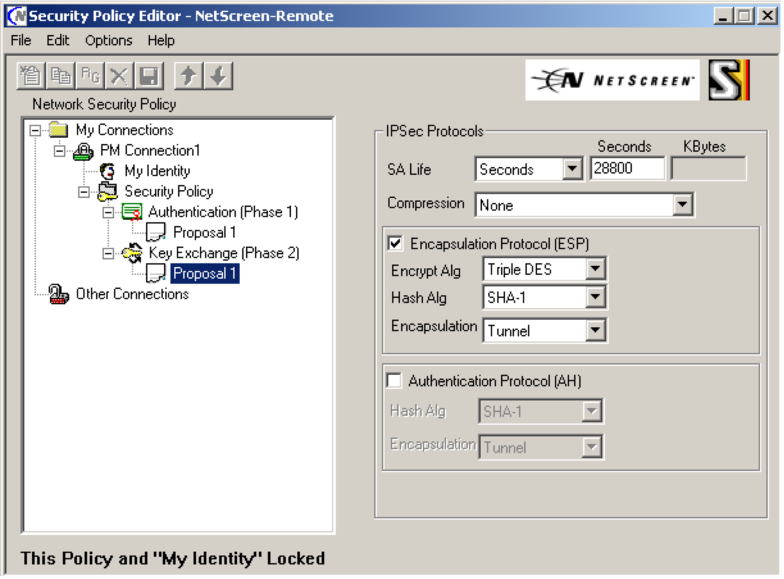
Status:

Connection	User	Profile	Time Connected
Up	test	default.ang	0:0:52

Figure 8-3 NetScreen-Remote Login Connection Status

NetScreen-Remote Security Policy Editor — Display Only

If a user opens the Security Policy Editor menu, she or he will find that the VPN policy is display-only, and cannot be modified by the user:



Security Policy Editor - NetScreen-Remote

Network Security Policy

- My Connections
  - PM Connection1
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
        - Proposal 1
- Other Connections

IPSec Protocols

SA Life: Seconds — Seconds: 28800 — KBytes:

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

This Policy and "My Identity" Locked

Figure 8-4 Security Policy Editor (Locked Screen)

VPN policies downloaded from Global-PRO are locked and cannot be modified by the NetScreen-Remote user.

9 Large Scale Distribution (Standalone Procedure)

NetScreen-Remote can be used in a stand-alone environment. VPN policies or “SPD” files must be generated and distributed to users manually. VPN policies or updates will not be automatically deployed to remote clients.

Deploying NetScreen-Remote clients on a large scale is a straightforward process. Basically, it consists of the following steps, which are described in this chapter:

- Centralizing Distribution of Common Files

  For ease of distribution, export the NetScreen-Remote installation files to a central location from which your users can access them, usually via File Transfer Protocol (FTP). Default policies and lock policies can also be configured and distributed in the form of common setup files.

- Repackaging The Installation

  In some deployments of NetScreen-Remote, customizing or "repackaging" the installation package for easy distribution may be necessary.

- Configuring the Connections

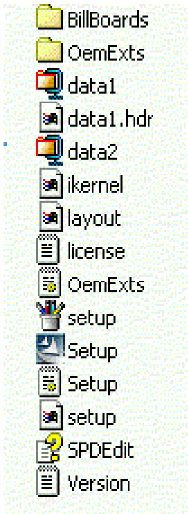
  Define the Security Policy for all users. Multiple sets can be created for user groups with different network requirements. For example, you may have a user who needs to be able to make VPN connections to their company headquarters, two satellite offices, and four vendors. Within each connection, the network administrator defines the specific Security Policy parameters of that connection.

- Exporting Policies and Delivering These to Users

  NetScreen recommends that you securely export and distribute the policy using a floppy disk or CD-ROM.

Centralizing Distribution of Common Files

Each user needs to be able to download common NetScreen-Remote installation files. The complete set of software files is shown below.



BillBoards
OemExts
data1
data1.hdr
data2
ikernel
layout
license
OemExts
setup
Setup
Setup
setup
SPDEdit
Version

Figure 9-1 NetScreen-Remote Installation Software Files

Place NetScreen-Remote installation files on a website or a network drive share from which users can download these files.

REPACKAGING THE INSTALLATION

In some deployments of NetScreen-Remote, it may be beneficial for the administrator to customize or "repackage" the installation package for easy distribution in a specific environment. This is sometimes referred to as "Repackaging" the installation. Some of the reasons for repackaging the installation include:

- Defining Installation Parameters (e.g. Program Group, Install Path)
- Installing additional programs in-conjunction with NetScreen-Remote
- Hiding all end-user prompts during installation (Silent Install)
- Executing an automatic reboot after installation is complete
- Including default policy files or certificates
- Installing shortcuts in the start menu

- Hiding tray icons from the end-users

Note: When deploying NetScreen-Remote with NetScreen-Global PRO, it is necessary to repackage the installation to include Global-PRO Server IP Address and other parameters in the Default.ANG file.

The first step to repackaging is to copy files from the read-only CD-ROM filesystem to a writable filesystem for modification. To ensure you copy all necessary files, a ZIP file of the NetScreen-Remote distribution on CD-ROM has ben created. First UnZip the file "NetScreen-Remote.ZIP" from the CD-ROM to suitable location for repackaging. Once the files have been copied to writable filesystem, a number of text-configuration files may be modified to change install behavior.

Default Installation Configuration File

OEMInstall.INI

This default OEMInstall.ini file is located in the installation directory in the /setup folder of the NetScreen-Remote.You may modify some sections of this configuration file to customize the install for your environment. Environment variables defined on the local machine may be used inside this file. You should only modify sections outlined in bold. If other sections of this file (those labeled "Do not change") are modified, it may cause adverse effects to the installation of the software and/or target machine.

[OemExtensions]

RebootTimeout=30

The RebootTimeout key is to configure NetScreen-Remote installation processing to use a time-delayed reboot mechanism. When provided, the RebootTimeout key value specifies (in decimal) the number of seconds to wait before automatically rebooting the system when a reboot is required.

[DialogWelcome]

EnableDialog=Yes

The EnableDialog key of the DialogWelcome section may be used to enable or disable presentation of the Welcome Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

[DialogLicense]

EnableDialog=Yes

The EnableDialog key of the DialogLicense section may be used to enable or disable presentation of the License Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

[DialogDestPathandType]

EnableDialog=Yes

The EnableDialog key of the DialogDestPathandType section may be used to enable or disable presentation of the Destination Path and Setup Type Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

TargetDir="%ISV_PROGRAMFILES%\NetScreen\NetScreen-Remote"

The TargetDir key of the DialogDestPathandType section may be used to configured the default target directory for the installation. The default value for this is C:\Program Files\NetScreen\NetScreen-Remote.

[DialogProgramFolder]

EnableDialog=No

The EnableDialog key of the DialogProgramFolder section may be used to enable or disable presentation of the Program Folder Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "No".

AdministratorGroup=Yes

The AdministratorGroup key of the DialogProgramFolder section may be used to indicate the group to receive menu shortcuts created by NetScreen-Remote installation processing. Defined values of the AdministratorGroup Key are "Yes" and "No". The default value used when the AdministratorGroup Key does not exist is "Yes".

ProgramFolder="NetScreen-Remote"

The ProgramFolder key of the DialogProgramFolder section may be used to indicate the group to receive menu shortcuts created by NetScreen-Remote installation processing. As it is defined, the ProgramFolder key value contains the menu specification of the program group to contain the menu shortcuts. The default Program Group is "NetScreen-Remote."

[DialogSummary]

EnableDialog=Yes

The EnableDialog key of the DialogSummary section may be used to enable or disable presentation of the Summary Dialog during NetScreen-Remote installation processing. Defined values of the EnableDialog Key are "Yes" and "No". The default value used when the EnableDialog Key does not exist is "Yes".

[EntriesStartup]

The EntriesStartup section of the Installation Configuration File contains information relating to the startup shortcuts created by the NetScreen-Remote installation process. The keys defined for the EntriesStartup section are detailed in the following subsections.

Certificate Manager=No

The "Certificate Manager" key of the EntriesStartup section may be used to enable or disable creation of the Certificate Manager shortcut by the NetScreen-Remote installation process. Defined values of the "Certificate Manager" key are "Yes" and "No". The default value used when the "Certificate Manager" key does not exist is "Yes".

Security Policy Editor=No

The "Security Policy Editor" key of the EntriesStartup section may be used to enable or disable creation of the Security Policy Editor shortcut by the NetScreen-Remote installation process. Defined values of the "Security Policy Editor" key are "Yes" and "No". The default value used when the "Security Policy Editor" key does not exist is "Yes".

Tray Icon=Yes

The "Tray Icon" key of the EntriesStartup section may be used to enable or disable creation of the Tray Icon shortcut by the NetScreen-Remote installation process. Defined values of the "Tray Icon" key are "Yes" and "No". The default value used when the "Tray Icon" key does not exist is "No".

Log Viewer=No

The "Log Viewer" key of the EntriesStartup section may be used to enable or disable creation of the Log Viewer shortcut by the NetScreen-Remote installation process. Defined values of the "Log Viewer" key are "Yes" and "No". The default value used when the "Log Viewer" key does not exist is "Yes".

Connection Monitor=No

The "Connection Monitor" key of the EntriesStartup section may be used to enable or disable creation of the Connection Monitor shortcut EntriesStartup the NetScreen-Remote installation process. Defined values of the "Connection Monitor" key are "Yes" and "No". The default value used when the "Connection Monitor" key does not exist is "Yes”.

Help=No

The "Help" key of the EntriesStartup section may be used to enable or disable creation of the Help shortcut by the NetScreen-Remote installation process. Defined values of the "Help" key are "Yes" and "No". The default value used when the "Help" key does not exist is "Yes".

L2TP Config Utility=No

The "L2TP Config Utility" key of the EntriesStartup section may be used to enable or disable creation of the L2TP Config Utility shortcut by the NetScreen-Remote installation process. Defined values of the "L2TP Config Utility" key are "Yes" and "No". The default value used when the "L2TP Config Utility" key does not exist is "Yes".

[EntriesMenu]

The EntriesMenu section of the Installation Configuration File contains information relating to the shortcuts displayed in Program group menus. The keys defined for the EntriesMenu section are detailed in the following subsections.

Certificate Manager=No

The "Certificate Manager" key of the EntriesMenu section may be used to enable or disable creation of the Certificate Manager shortcut by the NetScreen-Remote installation process. Defined values of the "Certificate Manager" key are "Yes" and "No". The default value used when the "Certificate Manager" key does not exist is "Yes".

Security Policy Editor=No

The "Security Policy Editor" key of the EntriesMenu section may be used to enable or disable creation of the Security Policy Editor shortcut by the NetScreen-Remote installation process. Defined values of the "Security Policy Editor" key are "Yes" and "No". The default value used when the "Security Policy Editor" key does not exist is "Yes".

Tray Icon=Yes

The "Tray Icon" key of the EntriesMenu section may be used to enable or disable creation of the Tray Icon shortcut by the NetScreen-Remote installation process. Defined values of the "Tray Icon" key are "Yes" and "No". The default value used when the "Tray Icon" key does not exist is "No".

Log Viewer=No

The "Log Viewer" key of the EntriesMenu section may be used to enable or disable creation of the Log Viewer shortcut by the NetScreen-Remote installation process. Defined values of the "Log Viewer" key are "Yes" and "No". The default value used when the "Log Viewer" key does not exist is "Yes".

Connection Monitor=No

The "Connection Monitor" key of the EntriesMenu section may be used to enable or disable creation of the Connection Monitor shortcut by the NetScreen-Remote installation process. Defined values of the "Connection Monitor" key are "Yes" and "No". The default value used when the "Connection Monitor" key does not exist is "Yes”.

Help=No

The "Help" key of the EntriesMenu section may be used to enable or disable creation of the Help shortcut by the NetScreen-Remote installation process. Defined values of the "Help" key are "Yes" and "No". The default value used when the "Help" key does not exist is "Yes".

L2TP Config Utility=No

The "L2TP Config Utility" key of the EntriesMenu section may be used to enable or disable creation of the L2TP Config Utility shortcut by the NetScreen-Remote installation process. Defined values of the "L2TP Config Utility" key are "Yes" and "No". The default value used when the "L2TP Config Utility" key does not exist is "Yes".

[EntriesPopup]

The EntriesPopup section of the Installation Configuration File contains information relating to the pop-up menu displayed by the Tray Icon application. The keys defined for the EntriesPopup section are detailed in the following subsections.

Certificate Manager=Yes

The "Certificate Manager" key of the EntriesPopup section may be used to enable or disable creation of the Certificate Manager shortcut by the NetScreen-Remote installation process. Defined values of the "Certificate Manager" key are "Yes" and "No". The default value used when the "Certificate Manager" key does not exist is "Yes".

Security Policy Editor=Yes

The "Security Policy Editor" key of the EntriesPopup section may be used to enable or disable creation of the Security Policy Editor shortcut by the NetScreen-Remote installation process. Defined values of the "Security Policy Editor" key are "Yes" and "No". The default value used when the "Security Policy Editor" key does not exist is "Yes".

Log Viewer=Yes

The "Log Viewer" key of the EntriesPopup section may be used to enable or disable creation of the Log Viewer shortcut by the NetScreen-Remote installation process. Defined values of the "Log Viewer" key are "Yes" and "No". The default value used when the "Log Viewer" key does not exist is "Yes".

Connection Monitor=Yes

The "Connection Monitor" key of the EntriesPopup section may be used to enable or disable creation of the Connection Monitor shortcut by the NetScreen-Remote installation process. Defined values of the "Connection Monitor" key are "Yes" and "No". The default value used when the "Connection Monitor" key does not exist is "Yes".

Help=Yes

The "Help" key of the EntriesPopup section may be used to enable or disable creation of the Help shortcut by the NetScreen-Remote installation process. Defined values of the "Help" key are "Yes" and "No". The default value used when the "Help" key does not exist is "Yes".

Executing a Custom Installation

If OemExts is not in the setup directory, you may have to first tell the NetScreen Remote program the location of your configuration file. This location may be a local, relative path or a network path (e.g. \\serverA\config\install.ini) There are two ways to tell the NetScreen-Remote installer to use your custom configuration: A command-line argument to setup or in the setup.ini file. The command-line flag allows your install configuration file to reside in a separate location to your installation CD-ROM.

> ***Note:*** By default, NetScreen-Remote installer will use OEMInstall.ini file located in the \setup directory of the CD-ROM for install configuration.

Command-Line

You can run Setup of NetScreen-Remote from the command-prompt or batch file with the path to the install configuration file. To use the local file install.ini for configuration:

```
setup.exe -xInstall.ini
```

To use a network file \\serverA\configs\OEMinstall.ini for configuration

```
Setup.exe -x\\serverA\configs\OEMinstall.ini
```

Defined in Setup.ini

In the setup.ini file on the install directory, you may also modify the "CmdLine=" line to define the location of the install configuration file. The following example would use the local file Install.ini for install configuration.

File: Setup.INI

```
[Startup]

CmdLine=-xInstall.ini# Define install file here

EnableLangDlg=Y         # Do not change

AppName=NetScreen-Remote# Do not change
```

```
ProductGUID=2f931b84-0cee-11d1-aa7d-0080ad1ac47a# Do not change

[Languages]            # Do not changeDefault=0x0009# Do not
change

count=1                         # Do not change

key0=0x0009                     # Do not change
```

Configuring the Connections

For each VPN tunnel for a given user, you need to configure at least one connection. For the configuration procedures for the three kinds of VPN connections possible, see the following chapters:

- Chapter 4, "Configuring a VPN Tunnel with Pre-Shared Key"
- Chapter 5, "Configuring a VPN Tunnel with Digital Certificates"
- Chapter 6, "Configuring a Manual Key VPN Tunnel"

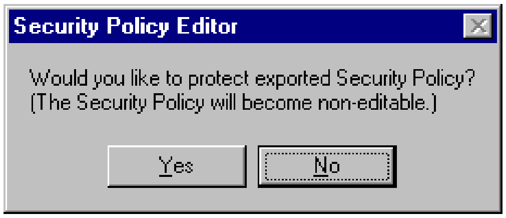
Note: *If using certificates, it is possible for all users with the same access rights to use the same SPD file if the group's IKE ID feature is used on the NetScreen device. For more information, see the NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 4: VPNs.*

Exporting Policies and Delivering These to Users

The network administrator needs to export each user's policy for subsequent distribution to that user.

1. In the Network Security Policy list, select a **policy** for distribution.
2. On the File menu, choose **Export Security Policy**.

   The Security Policy Editor options box appears.



Security Policy Editor

Would you like to protect exported Security Policy?
(The Security Policy will become non-editable.)

Figure 9-2 Security Policy Editor Options Box

3. Click **Yes** if you want to protect the exported Security Policy by making it non-editable, or click **No** if you want users to be able to edit it.

   The Save As dialog box appears.

4. Name the file, navigate to the directory where you want to keep it, and click **Save**.

Distribute each user's policy to them using the appropriate security measures.

You may also include a default policy with NetScreen-Remote install files by naming the file Default.spd and placing it in the NetScreen-Remote setup directory. After installation, these default settings will be used.

Configuring a L2TP/IPSec A

This appendix covers the following information:

- Configuring L2TP Connection
- Connecting to Your L2TP VPN

Configuring L2TP Connection

If you will be connecting to a Layer Two Tunneling Protocol (L2TP) VPN Connection, you must configure the L2TP connection through your Microsoft Dial-Up Networking. Prior to configuring the L2TP connection, configure NetScreen-Remote for IPSec Transport mode connection to the NetScreen device.

> ***Note:*** *The following procedure provides instruction on how to set up L2TP VPN connections on Windows 2000. A similar procedure is used to set up L2TP connections for Windows 95B, 98, ME, NT 4.0 and XP.*

To configure Microsoft Dial-Up Connection for a L2TP VPN connection:

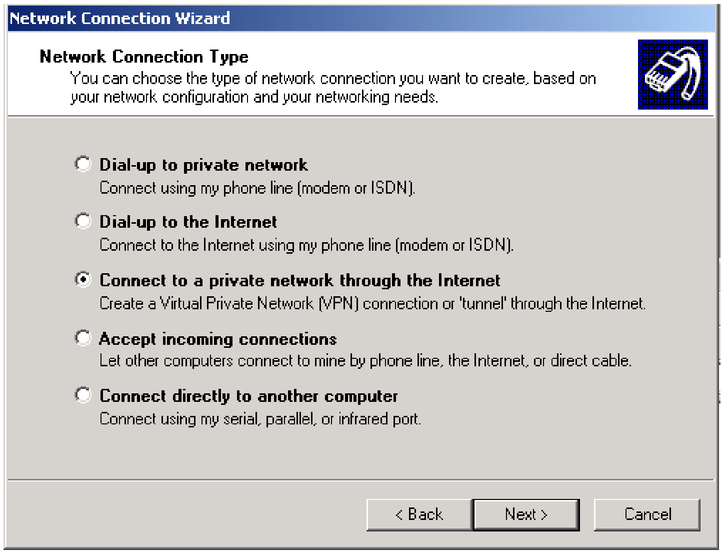
1. On the Windows taskbar, click the **Start** button, select **Programs**, select **Accessories**, select **Communications**, and then click **Network and Dial-Up Connections**.

   The **Dial-up Networking** dialog box appears.

2. Double-click the **Make New Connection** icon, and then click **Next**.

Figure 9-3 Make New Connection Icon

The **Network Connection Wizard** dialog box appears.



Network Connection Wizard

Network Connection Type

You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

● **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

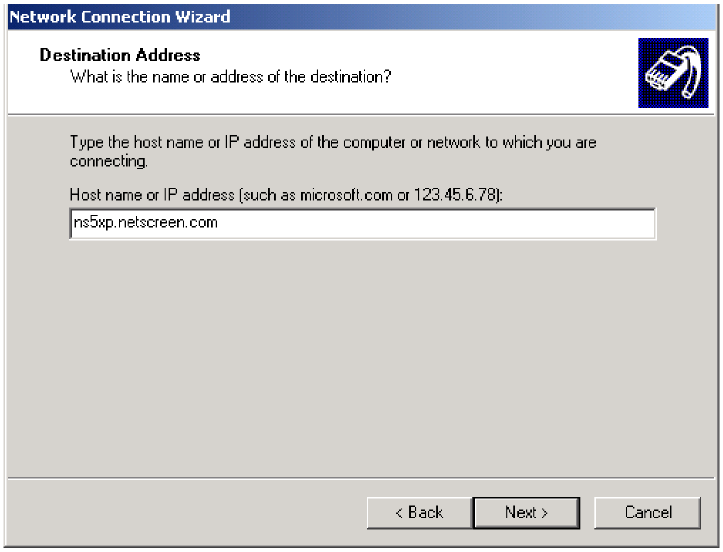
○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

Figure 9-4 Network Connection Wizard

3. Choose **connect to a private network through the Internet**, and then click **Next**.
4. If the physical connection is an Ethernet connection, select **Do not dial the initial connection**. If the physical connection is through an ISP, select **Automatically dial this initial connection**. Select the dial-up connection that connects you to your ISP, and then click **Next**.

   The **Destination Address** dialog box appears.



Network Connection Wizard

Destination Address

What is the name or address of the destination?

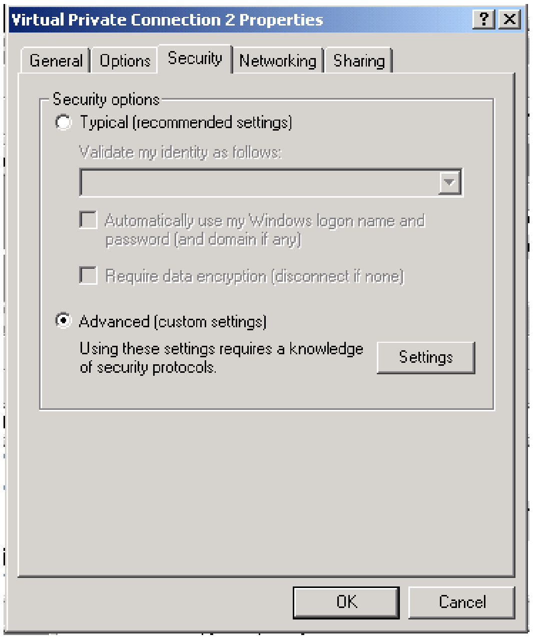
Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78): ns5xp.netscreen.com

Figure 9-5 Destination Address

5. In the **Host name or IP address** box, enter the IP address or hostname of NetScreen-Remote's Untrust interface, and then click **Next**.
6. Select either **For all users** or **For my user only** depending on your own need, and then click **Next**.
7. Enter the desired name for the connection, and then select **finish**.
8. Click the **Properties** tab.

   The following dialog box appears.



Security options

○ Typical (recommended settings)

Validate my identity as follows:

□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

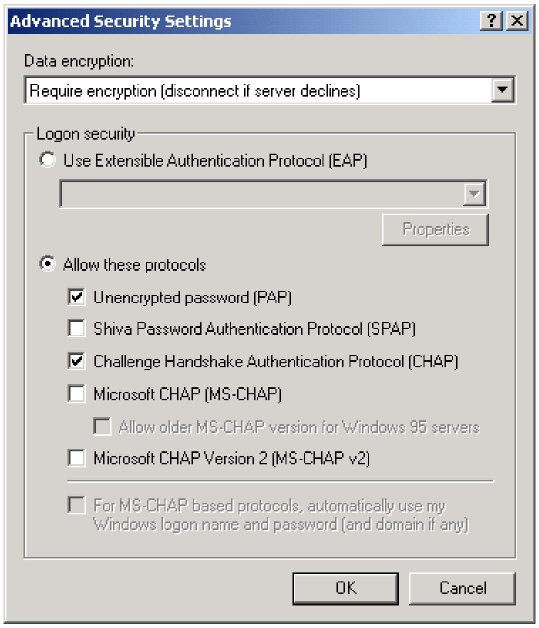
● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

Figure 9-6 Security Options

9. Click the **Security** tab, select **Advanced (custom settings)**, and then click **Settings**.

   The **Advanced Security Settings** dialog box appears.



Advanced Security Settings

Data encryption:

Require encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

☑ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP (MS-CHAP)

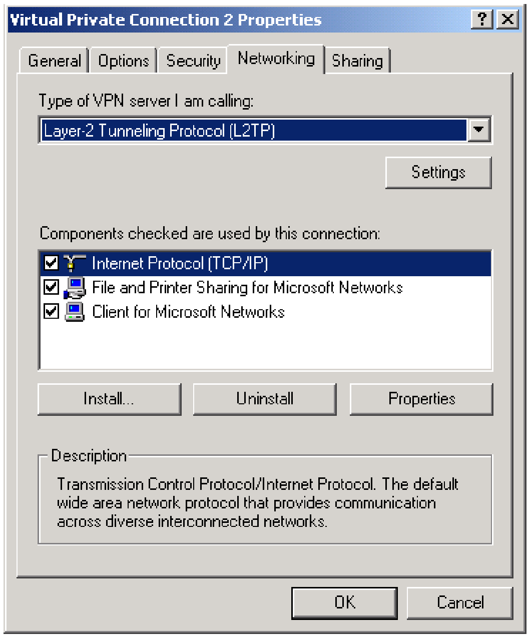
□ Allow older MS-CHAP version for Windows 95 servers

□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

Figure 9-7 Advanced Security Settings

10. In the **Data encryption** box, click **Optional encryption**.
11. Under **Logon security**, click **Allow these protocols,** and then click **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**. Click **OK**.



Type of VPN server I am calling:

Layer-2 Tunneling Protocol (L2TP)

Components checked are used by this connection:

☑ Internet Protocol (TCP/IP)
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 9-8 Networking

12. Click the **Networking** tab, and in the **Type of VPN server I am calling** box, click **Layer-2 Tunneling Protocol (L2TP)**. Click **OK**.

You have completed configuring Microsoft Dial-up Networking for a L2TP VPN connection. Go to the next section, “Connecting to Your L2TP VPN” for information on how to connect to your L2TP connection.

Connecting to Your L2TP VPN

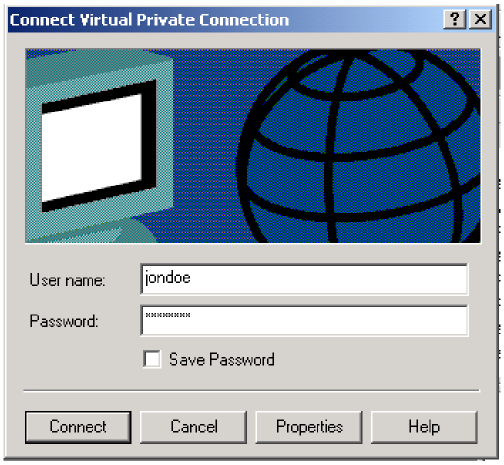
After you successfully configure your L2TP VPN connection via the Microsoft Dial-up Networking dialog box, you are able to connect to your L2TP VPN connection.

> ***Note:*** *Once your L2TP VPN connection has been established, it will remain active until idle-timeout, you shut down your computer, or you log off as a user. You may manually close your connection by clicking the* ***Network*** *icon in the taskbar, and then selecting* ***Disconnect.***

To connect to your L2TP VPN connection:

1. Double-click the Dial-up Connection you created.

   The **Connect Virtual Private Connection** dialog box appears.



User name: jondoe

Password: *********

□ Save Password

Figure 9-9 Connect Virtual Private Connection

2. Enter your user name and password, and then click **Connect**.

   Your L2TP VPN connection will be established.

Deploying NetScreen-Remote with Smart Cards B

This appendix describes the configuration steps for setting up a smart card to interoperate with NetScreen-Remote for the authentication of VPN sessions. A Schlumberger smart card is used to illustrate the configurations required on a smart card. The following sections are covered in this appendix:

- Smart Card Overview

  A brief overview of smart cards is provided.

- Generating and Loading a Private Key and Personal Certificate from Microsoft CA

  This describes how to generate and load a key pair and personal certificate on a smart card using the Microsoft Certificate Server, part of Windows 2000 Advanced Server. A similar process is required for all CAs, such as VeriSign and Entrust.

- Loading CA Certificate

  This describes how to load the CA certificate from a Microsoft Certificate Server on all computers you will use your smart card with NetScreen-Remote.

- Configuring NetScreen-Remote

  This section explains how to configure NetScreen-Remote to select which certificate to use during the IKE negotiation process with the NetScreen-Gateway, as well as the ID type to use when deploying NetScreen-Remote on a large scale using Group IKE IDs on the NetScreen-Gateway.

- Configuring the NetScreen-Gateway to Accept your Smart-Card Certificates

  This section explains how to configure a Group IKE ID on the NetScreen-Gateway. This configuration allows the gateway to accept the smart-card certificates.

SMART CARD OVERVIEW

A smart card is essentially a credit-card size unit with a memory chip for storing private keys and certificates; some units have built-in random number and certificate generation chips. Smart-card readers are available for virtually every PC. Most laptops use PCMCIA Smart-Card readers and desktops usually use USB or keyboard-based units. You can insert your smart card in any of these devices for authentication with NetScreen-Remote.

As mentioned, a smart card stores a private key in its own on-board memory. Most of the time, this key is encrypted with a password that the you select, or a default password that is assigned to the card. Most smart cards allow you to change this password after your keys have been generated.

Before installing NetScreen-Remote, install any software or drivers accompanying your smart card, and ensure the card is inserted into the unit and functioning.

GENERATING AND LOADING A PRIVATE KEY AND PERSONAL CERTIFICATE FROM MICROSOFT CA

Once your smart-card software is installed and operational, go to the Microsoft CA Server page to generate a private key and personal certificate. In this configuration example, a Schlumberger Smart-Card is used. Perform the following steps to generate a private key and personal certificate starting from the Microsoft CA Welcome page:

1. Click on **Request a certificate** in the **Select a task area**, and click **next**.

   The **Choose Request Type** dialog box appears.

2. Click on **Advanced request** then click **next**.

   The **Advanced Certificate Requests** dialog box appears.

3. If you are requesting a certificate for your own smart card, select **Submit a certificate request to this CA using a form**, and then click **next**. Skip to Step 5.

4. If you are enrolling on behalf of another user, select **Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station**, and then click **next**.

Note: In large deployments, the administrator may wish to generate key pairs on smart cards prior to deploying them to users. Most CA's allow you to enroll a certificate on a smart card on behalf of another user, including Microsoft CA. When you select this option, be sure to enter the user's correct information and tell the user the password you selected for their card, which they should later change.

5. Enter the following identifying information under Identifying Information area:
   – Name
   – E-Mail
   – Company
   – Department
   – City
   – State
   – Country/Region
6. Select **IPSec Certificate** from the **Intended Purpose** list.
7. Select **Schlumberger Cryptographic Service Provider** from the **CSP** list the **Key Options** area.

   In this example, a Schlumberger Smart-Card reader is used.
8. Accept the following default settings for the following in the **Key Options** area:
   – Key Usage: Both
   – Key Size: 1024
   – Create new key set
9. Click **Submit**.

   Your smart card now generates a private key and certificate request.
10. If your smart-card software prompts for your password or PIN during key generation, enter it.

    The default PIN on Schlumberger smart cards is 00000000. Your key will now be generated; this may take up to 2 minutes depending on the performance of your hardware.

11. If your Microsoft CA Server is configured to automatically approve certificates, the message “The certificate you requested was issued to you” displays on the **Certificate Issued** page. Click **Install this certificate**.

    If your CA does not auto-approve, you may have to wait for the administrator to approve your certificate request. After your administrator approves your certificate request, return to the CA Server web page and retrieve your certificate.

    After your certificate has successfully been installed, a message indicating this displays in the **Certificate Installed** page. Next, load your CA certificate. See the next section, “Loading CA Certificate.”

LOADING CA CERTIFICATE

In addition to loading your personal certificate, you also need to load the CA certificate on all computers you will use your smart card with NetScreen-Remote. Perform the following steps to load a CA certificate starting from the Microsoft CA Server Welcome page:

1. Click on **Retrieve the CA certificate or certificate revocation list** in the **Select a task area**, and click **next**.

   The **Retrieve The CA Certificate Or Certificate Revocation List** page appears.

2. Click **Install this CA certification path** link.

   After your CA certificate has been successfully installed, a message indicating this displays.

   Next, configure NetScreen-Remote to select which certificate and ID type to send to the NetScreen-Gateway. See the next section, “Configuring the NetScreen-Gateway to Accept your Smart-Card Certificates.”

CONFIGURING NETSCREEN-REMOTE

Once your personal and CA certificates have been loaded into your computer, configure NetScreen-Remote to select which certificate to use during the IKE negotiation process with the NetScreen-Gateway. “Configuring a VPN Tunnel with Digital Certificates” on page 5-1 describes how to configure NetScreen-Remote to use certificates. See this chapter for more information regarding the complete configuration of VPN tunnels using certificates. The procedure below provides a subset of the entire configuration for setting up VPN tunnels with certificates. The procedure below also provides the setting to select when deploying NetScreen-Remote on a large scale using Group IKE IDs on the NetScreen-Gateway.

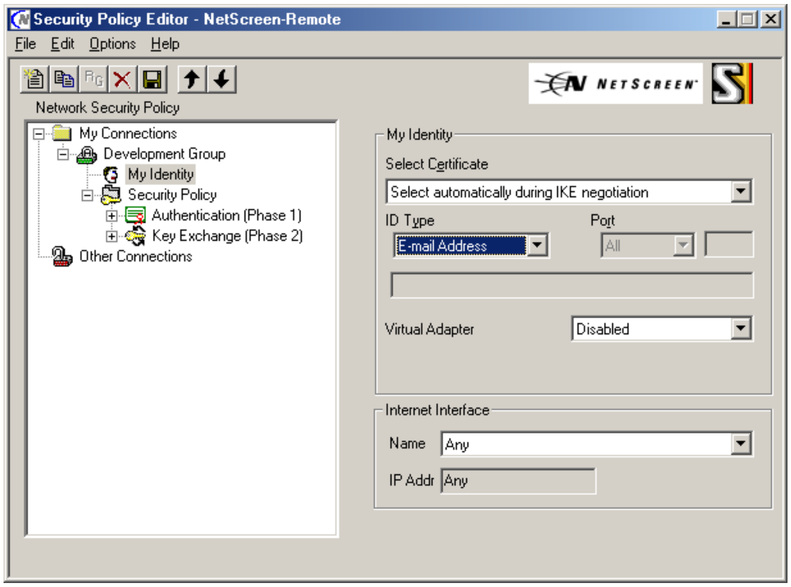
Perform the following steps to configure NetScreen-Remote to select the certificate and the ID type to send to the NetScreen-Gateway:

1. Double click on the NetScreen-Remote icon to launch the Security Policy Editor.
2. Double-click the icon for the new connection.

   My Identity and Security Policy icons appear.

3. Select **My Identity**.

   The My Identity and Internet Interface areas appear, as shown below.



My Identity

Select Certificate: Select automatically during IKE negotiation

ID Type: E-mail Address

Port: All

Virtual Adapter: Disabled

Internet Interface

Name: Any

IP Addr: Any

Figure 9-10 My Identity and Internet Interface Areas

4. Select **select automatically during IKE Negotiation** from the **Select Certificate** drop-down list.

   This will ensure that NetScreen-Remote will always send the local certificate that the NetScreen-Gateway will support.

5. For the **ID Type**, select one of these means of identifying yourself during the key exchange phase: **IP Address**, **Distinguished Name**, **Domain Name**, or **E-Mail Address**. If using Group IKE IDs on the NetScreen-Gateway, select **Distinguished Name** for the **ID Type**.

   The **Distinguished Name** ID type is recommended for large deployments.

If necessary, click **View** to display the information that is in your digital certificate.

6. Define the remainder of your security policy as described in "Configuring a VPN Tunnel with Digital Certificates."

Next, configure the NetScreen-Gateway to accept your smart-card certificates. See the next section, "Configuring the NetScreen-Gateway to Accept your Smart-Card Certificates."

CONFIGURING THE NETSCREEN-GATEWAY TO ACCEPT YOUR SMART-CARD CERTIFICATES

The easiest and most scalable way to support certificates for NetScreen-Remote features is with ScreenOS 3.0r1 or greater and Group IKE IDs feature. This ScreenOS feature only supports certificates and Distinguished Name identity types for clients connecting. The ScreenOS feature's previous requirement to add individual users to the NetScreen-Device is no longer required. Instead, this feature now allows groups of users to share a common IKE Identity when using certificates.

To configure a Group IKE ID on the NetScreen-Gateway, perform the following steps:

1. From the WebUI, select **Users** and then click **New IKE User** to define a new IKE User.
2. Click **Use Distinguished Name for ID** and fill in the appropriate fields. This will popup a list of Distinguished Name (DN) attributes you should define.

   In this example, configure a Group-IKE ID User Name of "Sales" where the NetScreen will permit any user whose signed certificate has the DN fields of OU=Sales and O=NetScreen and is signed by the proper CA. Any DN fields left empty will not be verified.
3. Enter the number of users in the **Number of Multiple Login with same ID** box who are allowed to login with the same ID simultaneously.

   In this example, 50 users may login to the "Sales" VPN using the certificates containing the specified DNs.

Note: To support multiple logins, the user "Sales" created must be added to a Dial-Up User Group. Create a User-Group called "Sales" and add user "Sales" as a member.

Next, define a VPN Tunnel for your Sales users by performing the following steps:

4. In the Remote Gateway area, click **Dialup User**.
5. Select the Dialup User - Sales (the group you previously created) from the User/Group list.
6. Select **Aggressive f**rom the **Mode (Initiator)** area.
7. Select **rsa-g2-des-sha** or some RSA-Certificate from the **Phase I Proposal** area.

   The remaining parameters are optional.

Next, create the necessary policies to permit the Sales-Group VPN to appropriate subnets. Usually this will be an incoming Dial-Up Any policy. See Chapter 4 of the NetScreen Concepts and Examples ScreenOS Reference Guide for an example of creating a Dial-Up policy.

After your policy is created, up to 50 users may login simultaneously with valid certificates containing OU=Sales and O=Netscreen within the DN fields. It is not necessary to add individual users to the NetScreen-Gateway. You need only approve or issue certificates to users for authentication purposes.

Index