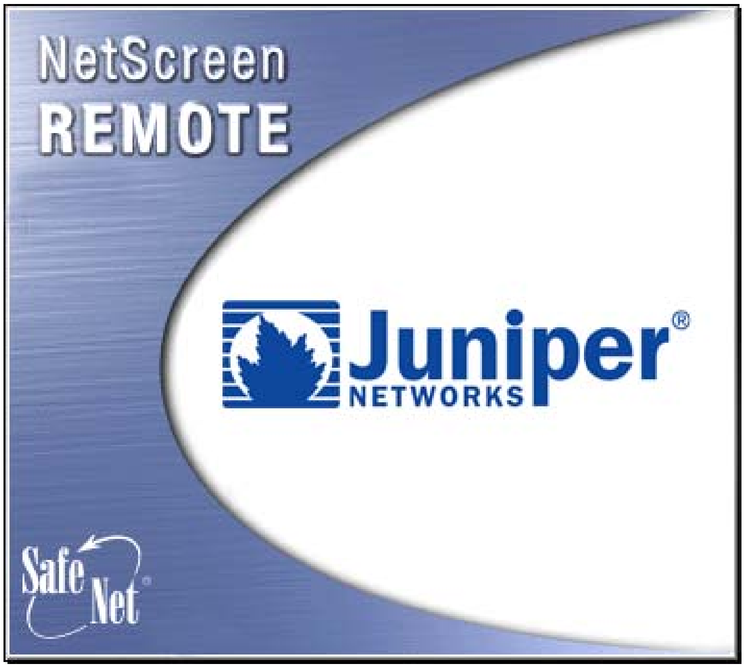
JUNIPER NETWORKS NETSCREEN-REMOTE SECURITY CLIENT ADMINISTRATOR'S GUIDE



Version 8.6 P/N 093-1637-000 Rev. A

Licenses, Copyrights, and Trademarks

THE SPECIFICATIONS REGARDING THE JUNIPER 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 JUNIPER 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 JUNIPER TECHNOLOGIES, INC.

JUNIPER NETSCREEN-REMOTE 8.6 LICENSE AGREEMENT

PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THIS PRODUCT. BY INSTALLING AND OPERATING JUNIPER NETSCREEN-REMOTE 8.6 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 Juniper Networks, as the owner and provider of "NetScreen-Remote 8.6." NetScreen-Remote 8.6 consists of Juniper 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 8.6, and allowing End Users to download NetScreen-Remote 8.6 or otherwise installing NetScreen-Remote 8.6 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 8.6 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 8.6 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 8.6 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 8.6 on each of 10, 100, 200, 500, 1000 or more End User computers as indicated on the license certificate(s) provided to you by Juniper.

Licenses that authorize use of NetScreen-Remote 8.6 with a greater number of End Users are available as upgrades and may be purchased from Juniper 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 8.6 must be used in the manner set forth in the applicable documentation. NetScreen-Remote 8.6 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 8.6 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 8.6, or any component thereof, is granted to you.

3. Limitation on Use.You are only licensing the rights set forth above to NetScreen-Remote 8.6. 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 8.6 (or any component thereof) and the accompanying documentation; (b) to distribute, sell, transfer, sublicense, rent, or lease any rights in NetScreen-Remote 8.6 (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 8.6, documentation, and containers. NetScreen-Remote 8.6 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 8.6 (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 8.6 and documentation, remain with Juniper. You acknowledge that no title or interest in and to the intellectual property associated with or included in NetScreen-Remote 8.6 and Juniper products is transferred to you and you will not acquire any rights to NetScreen-Remote 8.6 except for the license as specifically set forth herein.

5. Term and Termination. The term of the license is for the duration of Juniper's copyright in NetScreen-Remote 8.6. Juniper 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 Juniper. 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 8.6 is set forth in Juniper's Remote Warranty. THE JUNIPER NETSCREEN-REMOTE WARRANTY CONTAINS IMPORTANT LIMITS ON YOUR WARRANTY RIGHTS. THE WARRANTIES AND LIABILITIES SET FORTH IN THE REMOTE WARRANTY ARE EXCLUSIVE AND ESTABLISH JUNIPER'S ONLY OBLIGATIONS AND YOUR SOLE RIGHTS WITH RESPECT TO NETSCREEN-REMOTE 8.6 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 8.6 and the entire liability of Juniper are set forth in the NetScreen Remote Warranty. Except to the extent provided in the Remote Warranty, if any, IN NO EVENT WILL JUNIPER 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 JUNIPER 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 8.6 PAID BY YOU. YOU ACKNOWLEDGE THAT THE AMOUNT PAID FOR NETSCREEN-REMOTE 8.6 REFLECTS THIS ALLOCATION OF RISK.

8. Export Law Assurance. You understand that NetScreen-Remote 8.6 is subject to export control laws and regulations. YOU MAY NOT DOWNLOAD OR OTHERWISE EXPORT OR RE-EXPORT NETSCREEN-REMOTE 8.6 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 8.6. NetScreen-Remote 8.6 may not be downloaded, or NetScreen-Remote 8.6 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 8.6 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 8.6 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 JUNIPER 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 JUNIPER 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 JUNIPER.

Copyright Notice

Copyright © 1998-2004 Juniper Networks, Inc.

Copyright 2002 by Sygate Technologies, Inc. All rights reserved.

All rights reserved. Printed in USA.

Trademarks

Juniper Networks, the Juniper logo, NetScreen-Remote 8.6, NetScreen-Remote 8.6 Express, NetScreen-Remote, GigaScreen ASIC, and ScreenOS are trademarks and NetScreen is a registered trademark of NetScreen Technologies, Inc.

Sygate® is a registered trademark of Sygate Technologies, Inc. Microsoft is a registered trademark, and Windows, Windows ME, Windows 2000, Windows NT, Windows XP, and Windows 95/98 are trademarks of Microsoft Corporation. All other companies and product names are trademarks or registered trademarks of their respective holders.

JUNIPER NETSCREEN-REMOTE 8.6 WARRANTY

Software Warranty. Juniper Networks ("Juniper") 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 Juniper 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 Juniper, its suppliers and affiliates, under this warranty is, at Juniper'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.juniper.net/support. Juniper 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, Juniper may provide Customers upgrades and fixes for the Software at www.juniper.net/support. Customers may also send emails to support@juniper.net to obtain technical support for a period of one (1) year from the Start Date.

Return Procedures. Customer must notify Juniper 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, Juniper 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 Juniper, including description of the failure, shipment to Juniper's designated location, and return of Software within ten (10) days after issuance of the RMA number. In no event will Juniper 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. Juniper does not accept responsibility for any Software lost in transit and recommends that the return be insured for the full value. Juniper 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 Juniper's then-current rates for all services performed and expenses incurred by Juniper.

Restrictions. No warranty will apply if the Software (i) has been altered, except by Juniper; (ii) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Juniper; 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 Juniper disclaims any express or implied warranty of fitness for such uses. Juniper 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 Juniper, 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, JUNIPER 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, JUNIPER 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 JUNIPER 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 JUNIPER 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.

EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR USE AND APPLICATION OF ANY JUNIPER SECURITY 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 JUNIPER NETWORKS.

Table of Contents

Preface

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

What is Juniper NetScreen-Remote Security Client?

When the Juniper NetScreen-Remote Security Client operates on any IP network, such as the Internet, it can create a VPN tunnel between an end user and a Juniper NetScreen security appliance. The NetScreen-Remote Security Client 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 integrates with Microsoft (MS) Native L2TP protocols, and is compatible with most Certificate Authorities and MS CryptoAPI (MSCAPI) applications.

To simplify terminology, the NetScreen-Remote Security Client is referred to in this document as the "Security Client."

Who Should Read this Guide?

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

ASSUMPTIONS

This guide assumes that the user is familiar with the basic functioning of Windows operating systems, and standard Windows items, such as buttons, menus, toolbars, windows, etc.

Further, this guide assumes that the user has an Internet connection, whether through a private network, DSL connection, Ethernet, wireless Ethernet, dial-up modem, or some other form of connection.

TERMS

Depending on the kind of computing system that you use, you may connect to the Internet through a local area network (LAN), DSL, dial-up modem, or any number of other methods. The term “network connection” is used to refer to all of these different connection methods.

ADMINISTRATOR DECISIONS

There are several things you must decide before configuring the Security Client. 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 be 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 SCEP). 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.
- **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.

After you have made these decisions, configure a few Security Clients and Juniper 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 the VPN volume of the Juniper NetScreen Concepts and Examples ScreenOS Reference Guides, 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 the Security Client. Right-click the Security Client icon in the taskbar, and select Deactivate/Activate Security Policy from the pop-up menu. (The command toggles.)

Note ***Note:*** *You may wish to disable the Security Client whenever connected behind a Juniper device or other VPN gateway.*

Using this Guide

The following chapters are provided within this document:

Note ***Note:*** *The term "NetScreen-Remote" is used in chapters 1 through 9 and Appendices A and B to reference the VPN client component of the NetScreen-Remote Security Client product. "NetScreen-Remote Security Client" is used within this preface to reference the firewall component of the of the NetScreen-Remote Security Client product.*

Chapter 1, "Installation," describes the prerequisites and installation procedure for the Security Client.

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, "VPNs with Pre-Shared Keys" 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 links to several articles that demonstrate using NetScreen-Remote with various security components in various environments.

Chapter 8, "Large Scale Distribution with NetScreen-Global PRO" describes the procedure for deploying large numbers of Security Clients in conjunction with Juniper 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 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” provides an example of how to set up your smart card to interoperate with a Security Client and a Juniper NetScreen-Gateway.

Related Publications

The following are related publications:

Juniper Networks NetScreen Concepts and Examples ScreenOS Reference Guide (VPN volume)

Juniper Networks 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, 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 the Juniper Technical Assistance Center (JTAC). JTAC is available to users with valid service contracts of NetScreen-Remote. You can contact JTAC by one of the following ways:

- Phone: 1-888-314-JTAC (U.S., Canada, and Mexico)
- Phone: 408-745-9500
- Online Knowledge Base for NetScreen-Remote at

  http://nsremote-support.netscreen.com

1

Installation

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

> ***Note:*** *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.*
>
> *Note that Juniper supports a silent installation option which hides all end user prompts during the installation. This process may run in the foreground. Juniper does not support running the silent installation in the background, although it may run in that mode. If it does run in the background, you do not see the initial splash screens that launch as part of the installation process.*
>
> *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 in the following environment:

PC-compatible Computer	• Pentium processor or its equivalent
Operating System	• Windows XP® Professional or Home Edition • Microsoft Windows 2000 Professional or
Minimum RAM	• 64 MB RAM for Windows XP or Windows 2000
Available Hard Disk Space	• Minimum 5MB, 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, the installation program has been modified to automatically run the uninstall program if an earlier version is detected on the system. This eliminates the need to manually uninstall a previous version of software.

> ***Note:*** *Failure to uninstall the previous version will cause system conflicts resulting in failure of your Windows operating system.*

> ***Note:*** *At the end of the installation process, you need to reboot the device to complete the process.*

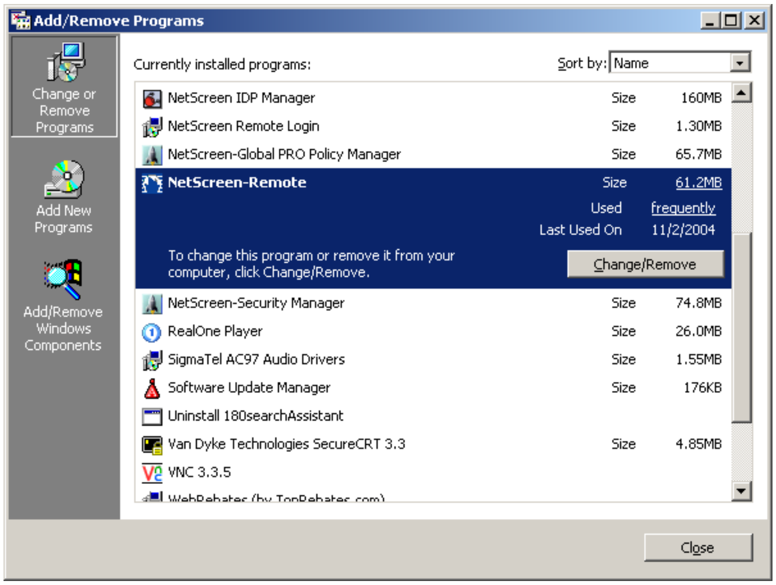
To manually uninstall a previous version of the NetScreen-Remote:

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

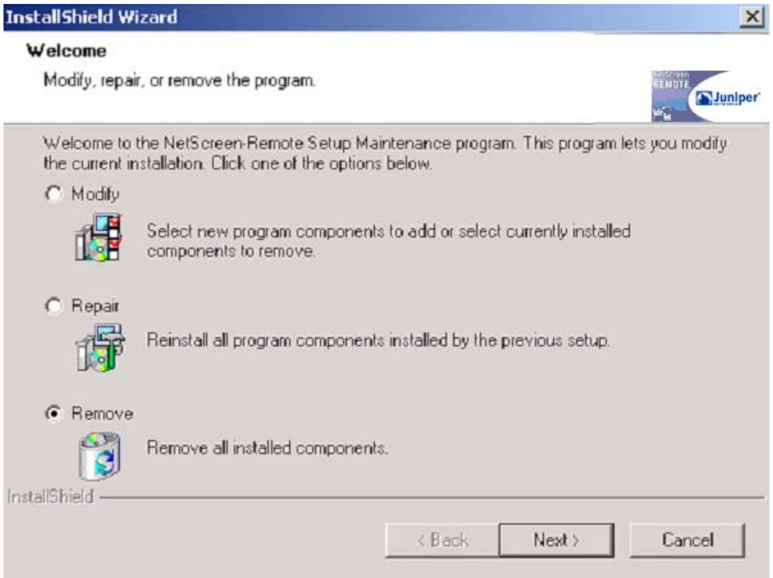
NetScreen IDP Manager	Size	160MB
NetScreen Remote Login	Size	1.30MB
NetScreen-Global PRO Policy Manager	Size	65.7MB
NetScreen-Remote	Size	61.2MB
	Used	frequently
	Last Used On	11/2/2004
NetScreen-Security Manager	Size	74.8MB
RealOne Player	Size	26.0MB
SigmaTel AC97 Audio Drivers	Size	1.55MB
Software Update Manager	Size	176KB
Uninstall 180searchAssistant		
Van Dyke Technologies SecureCRT 3.3	Size	4.85MB
VNC 3.3.5		
WebRebates (by TopRebates.com)		

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.

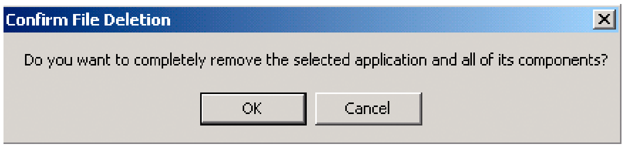
● Remove

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.



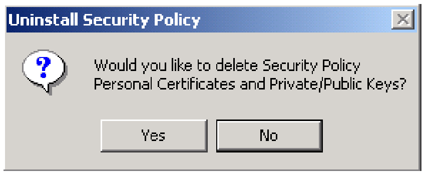
Confirm File Deletion

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 the 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

Before installing NetScreen-Remote, ensure that you have uninstalled all other vendor's firewall or VPN client software. While some computers can function with more that one firewall/VPN client running at a time, running multiple firewall/VPN clients will inevitably cause performance problems.

Also, before installing NetScreen-Remote, exit all other programs that access your network or Internet connection. This includes web browsers, email programs, instant messenger sessions, and media streaming applications (such as Internet radio broadcasts).

For Windows 2000, Windows NT and Windows XP users, use the .exe installation file. For Windows 98 and Windows ME users, use the .zip installation file.

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

You can install the 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 6:

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

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

1. Map to the network drive.
2. Locate the NetScreen-Remote files.
3. Copy setup.exe to a local area on the PC from the local copy.
4. Double-click **setup.exe** to run the NetScreen-Remote setup application.
5. Go to the next section, "Continuing with Installation."

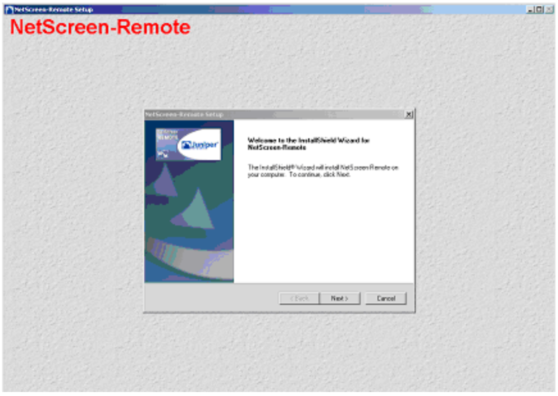
—To install the NetScreen-Remote from a website:

1. Locate the NetScreen-Remote files on the website.
2. Select to download the **setup.exe** file and download the file.
3. If the file is in a zip format, after the file downloads, unzip it 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 1-5. Click **Next**.

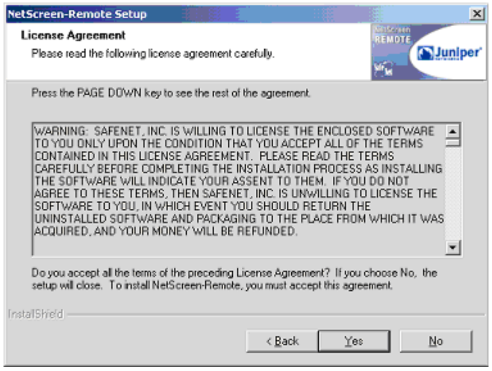


Welcome to the InstallShield Wizard for NetScreen-Remote

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

Figure 1-5 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.

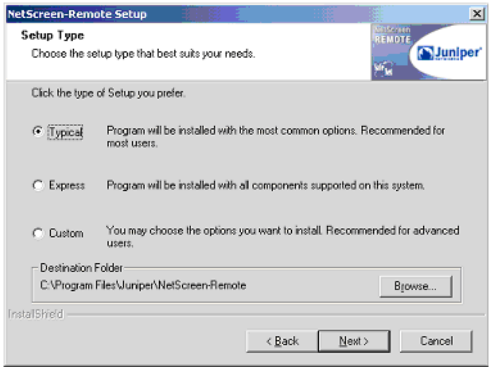
WARNING: SAFENET, INC. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SAFENET, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

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 1-6 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\Juniper\NetScreen-Remote

Figure 1-7 Installation Setup Type

3. Select one of these options:

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

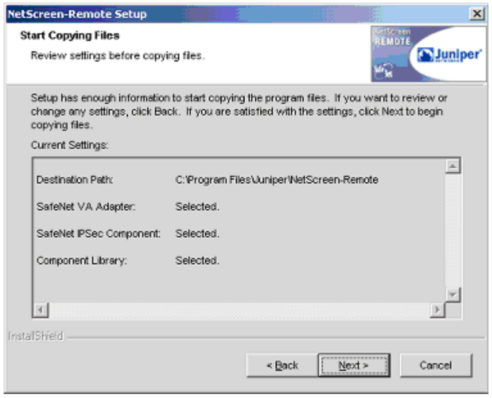
Express —Installs only the components that the system supports.

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

4. To install the NetScreen-Remote in the default destination folder (C:\Program Files\Juniper\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 1-8), and then click **Next**.



Start Copying Files

Review settings before copying files.

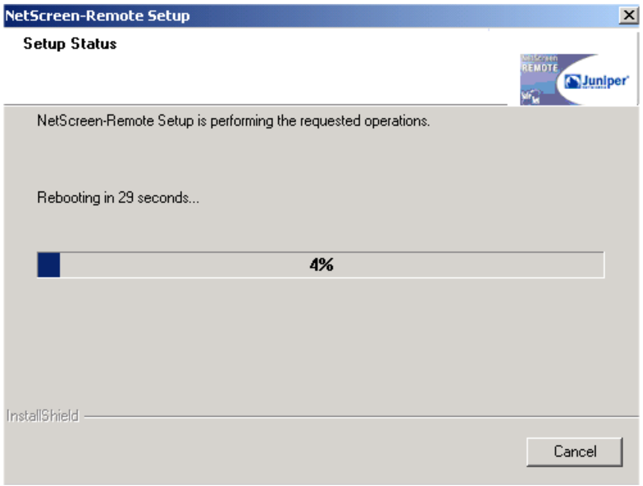
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

Destination Path:	C:\Program Files\Juniper\NetScreen-Remote
SafeNet VA Adapter:	Selected.
SafeNet IPSec Component:	Selected.
Component Library:	Selected.

Figure 1-8 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%

Figure 1-9 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.

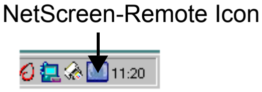


Figure 1-10 NetScreen-Remote icon on the Windows Taskbar

When you install the software, if it is a first-time installation, the NetScreen-Remote icon will be deactive instead of the active NetScreen-Remote icon shown in Figure 1-10. The appearance of the inactive NetScreen-Remote icon can be for one of several reasons, including:

-- You have not created any connections yet.

-- You installed the software incorrectly.

-- You configured NetScreen-Remote to be inactive at the time of bootup.

If you determined that the inactive status is because of a problem, follow the procedure in the “Modifying Installation” section later in the chapter 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**.

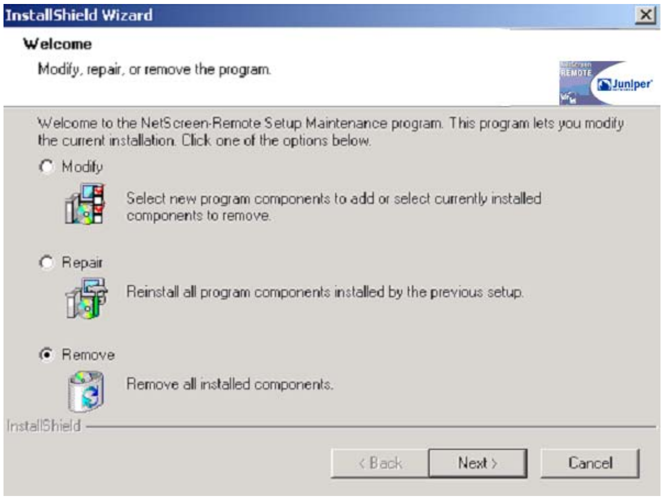
The **Control Panel** opens.

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.



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

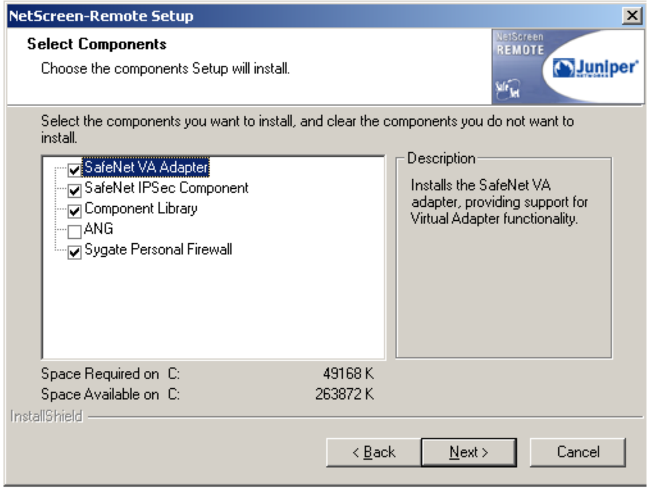
Remove all installed components.

Figure 1-11 Modify, Repair, or Remove the Program

6. To add or remove the Virtual Adapter, IPSec Client or other components 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
☑ Sygate Personal Firewall

Description

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

Space Required on C: 49168 K
Space Available on C: 263872 K

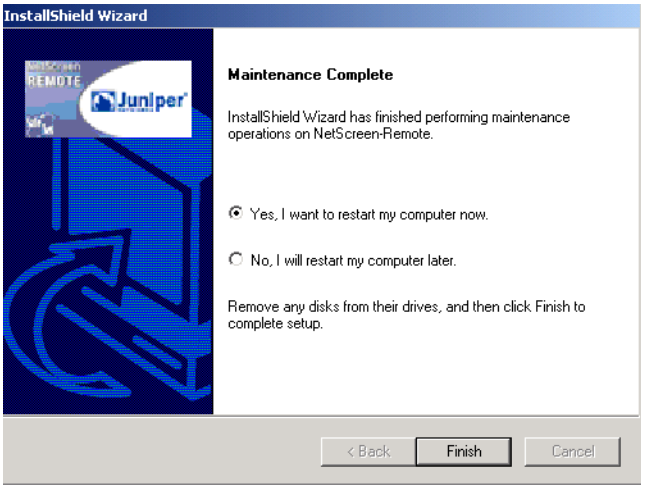
Figure 1-12 Select Components

7. Select the component to be installed, and then click **Next**. The installation procedure begins.
8. Note that if you select Sygate Personal Firewall, go to the following site to learn about Sygate Personal Firewall:

   http://smb.sygate.com/support/documents/spf/spf_install.htm
9. 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.


InstallShield Wizard

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 1-13 Maintenance Complete

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

2

Interface

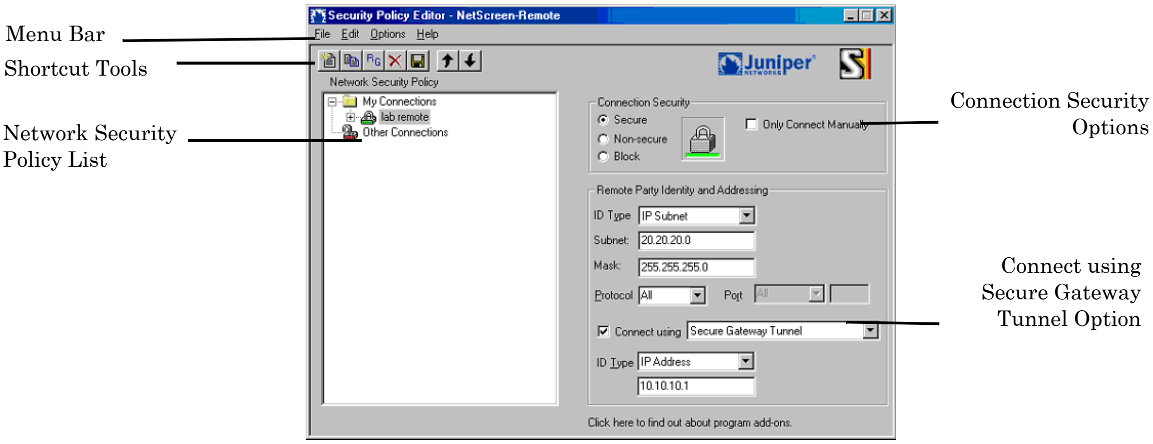
This chapter provides an overview of the layout, icons, and menus that appear in the NetScreen-Remote.

The NetScreen-Remote consists of these modules:

Security Policy Editor	Manually create connections and security policies.
Certificate Manager	Manage and verify certificates.
NetScreen-Remote Login policies	Authenticates user and downloads security.

Security Policy Editor

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


Menu Bar
Shortcut Tools
Network Security Policy List
Connection Security Options
Connect using Secure Gateway Tunnel Option
Security Policy Editor - NetScreen-Remote
File Edit Options Help
Juniper NETWORKS

Network Security Policy
- My Connections
  - lab remote
- Other Connections

Connection Security
- ● Secure
- ○ Non-secure
- ○ Block
- □ Only Connect Manually

Remote Party Identity and Addressing
- ID Type: IP Subnet
- Subnet: 20.20.20.0
- Mask: 255.255.255.0
- Protocol: All
- Port: All
- ☑ Connect using Secure Gateway Tunnel
- ID Type: IP Address
- 10.10.10.1

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 16.

The shortcut toolbar contains tools for common commands. For a brief description of each icon on the toolbar, see “Shortcut Toolbar Icons” on page 21.

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 the 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 Juniper products.)

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

Block: STOP
This option does not allow any communication for the connection to pass through. (It is the equivalent of “deny” on other Juniper 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 32.

File Menu

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

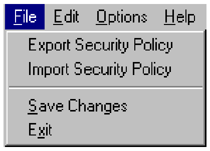


Figure 2-2 File Menu

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

Import Security Policy imports a security policy to the 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.

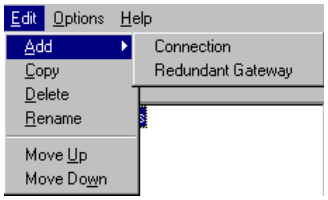


Figure 2-3 Edit Menu

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.

> ***Note:*** *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 within the Remote Party Identity and Addressing section of the Primary Gateway connection. Then choose Save Changes from the File menu.*

Rename enables you to provide another name for the connection or redundant gateway from the Network Security Policy list.

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 the NetScreen-Remote in an overarching way.

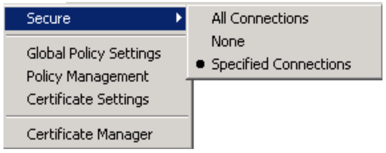
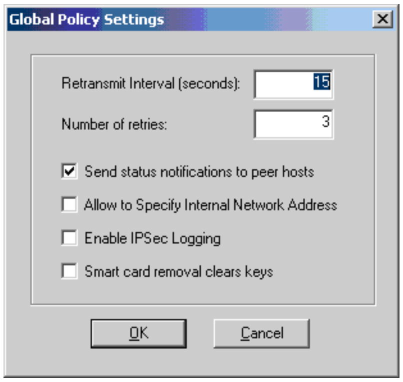


Figure 2-4 Options Menu

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 the NetScreen-Remote.



Retransmit Interval (seconds): 15

Number of retries: 3

☑ Send status notifications to peer hosts

□ Allow to Specify Internal Network Address

□ Enable IPSec Logging

□ Smart card removal clears keys

Figure 2-5 Global Policy Settings

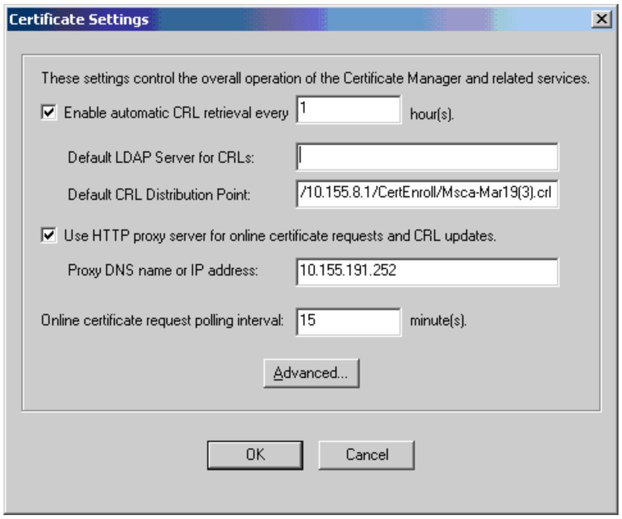
You can select the following Global Policy settings:

- **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:** sends status notifications to inform communicating parties what the time-out periods are and whether their security proposals have been accepted or rejected.
- **Allow to Specify Internal Network Address:** allows remote users to appear as internal users on a private network.

- **Enable IPSec Logging:** allows you to turn on logging for packets generated during the IPSec phase of a VPN tunnel connection.
- **Smart card removal clears keys:** allows security keys to be cleared when you remove the Smart card from the configuration.

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.



Certificate Settings

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

☑ Enable automatic CRL retrieval every 1 hour(s).

Default LDAP Server for CRLs:

Default CRL Distribution Point: /10.155.8.1/CertEnroll/Msca-Mar19(3).crl

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

Proxy DNS name or IP address: 10.155.191.252

Online certificate request polling interval: 15 minute(s).

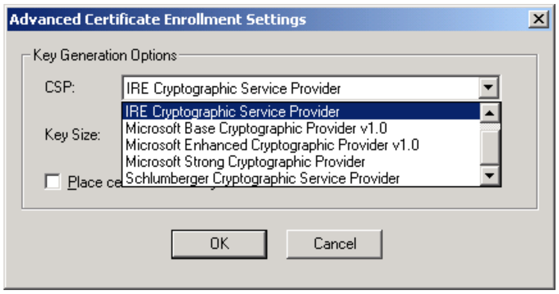
Figure 2-6 Certificate Settings

You can select the following Certificate Manager features:

- **Enable automatic CRL retrieval every** field enables you to perform automatic retrieval of certificate revocation lists (CRLs) and specify the retrieval frequency (in hours) and the default LDAP server.
- **Use HTTP proxy server for online certificate requests and CRL updates** enables you to specify an HTTP proxy server for on-line certificate requests using Certificate Enrollment Protocol (SCEP) 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 the NetScreen-Remote checks (“polls”) for a response to a certificate request.

Advanced opens the Advanced Certificate Enrollment Settings dialog box:


Advanced Certificate Enrollment Settings

Key Generation Options

CSP: IRE Cryptographic Service Provider

IRE Cryptographic Service Provider
Microsoft Base Cryptographic Provider v1.0
Microsoft Enhanced Cryptographic Provider v1.0
Microsoft Strong Cryptographic Provider
Schlumberger Cryptographic Service Provider
Key Size:
□ Place ce
OK
Cancel

Figure 2-7 Advanced Certificate Enrollment Settings dialog box

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

Gemplus GemSAFE Card CSP v1.0

IRE Cryptographic Service Provider

Microsoft Base Cyptographic Provider v1.0

Microsoft Enhanced Cryptographic Provider v1.0

Microsoft Strong Cryptographic Provider

Schlumberger Cryptographic Service Provider

Key Size opens a drop-down menu with selections for a default key size: 512, 1024, 2048, or 4096. The default key size is 1024.

Note: *ScreenOS does not support a key size of 4096.*

Place in Local Machine Store places the imported certificate in your - the logged-on user's - personal certificate store. Unless your network security administrator instructs you to change it, accept the default.

Save as Default CSP Settings saves the current settings for the certificate as the default configuration.

Certificate Manager opens the Certificate Manager, the module that allows you to manage personal certificates. Go to the Certificate Manager section for details on using Certificate Manager.

Help Menu

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

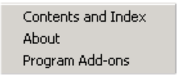


Figure 2-8 Help Menu

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 the 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 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.

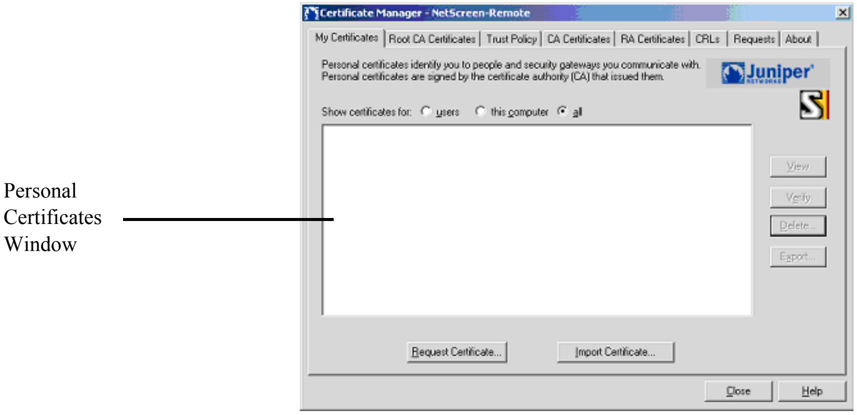
The Certificate Manager is organized into these six sections or pages:

- My Certificates
- Root CA Certificates
- Trust Policy
- CA Certificates
- RA Certificates
- CRLs
- 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 the NetScreen-Remote.



Certificate Manager - 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 2-9 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 the 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 the NetScreen-Remote:

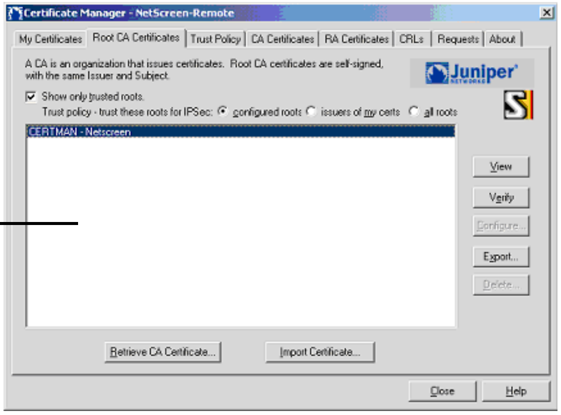
Request Certificate provides a choice of dialog boxes for generating a PKCS10 request. You can use either the SCEP, if you already have a CA certificate that supports SCEP, or the cut-and-paste method, which is to cut and paste the Cert_Request into your CA certificate.

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

CERTMAN - Netscreen

Root CA Certificates Window

Figure 2-10 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.

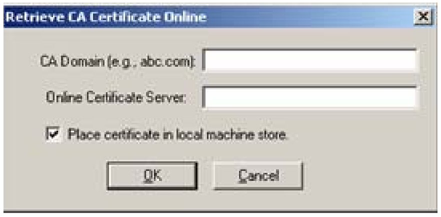
Verify checks the validity status of the selected certificate. If the certificate has expired, was revoked, or is corrupt, it fails verification.

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 SCEP.

Export copies the selected certificate to a directory of your choice in PKCS12 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 SCEP.



CA Domain (e.g., abc.com):

Online Certificate Server:

☑ Place certificate in local machine store.

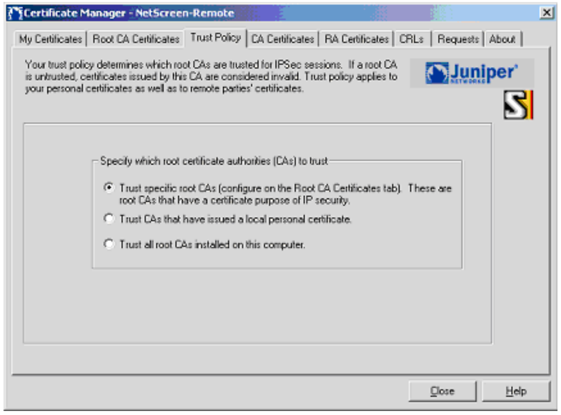
Figure 2-11 Retrieve CA Certificate Online

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

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

Trust Policy Page

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.



Your trust policy determines which root CAs are trusted for IPSec sessions. If a root CA is untrusted, certificates issued by this CA are considered invalid. Trust policy applies to your personal certificates as well as to remote parties' certificates.

Specify which root certificate authorities (CAs) to trust

- ● Trust specific root CAs (configure on the Root CA Certificates tab). 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 this computer.

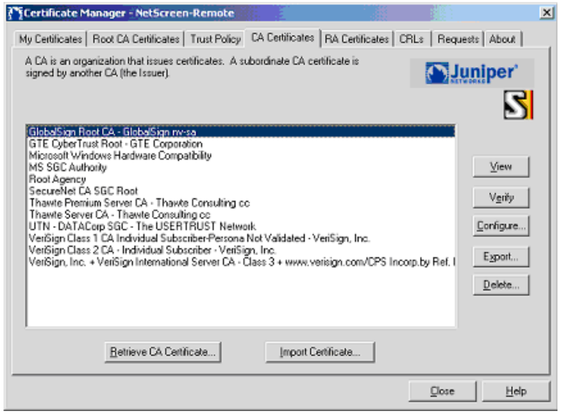
Figure 2-12 Trust Policy Menu

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 Page

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 2-13 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.

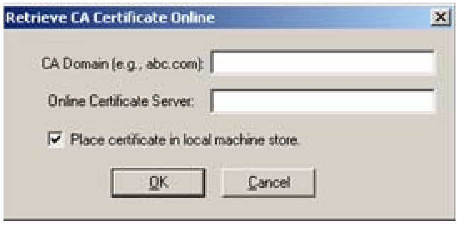
Verify checks the validity status of the selected certificate.

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 SCEP.

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

Delete removes the selected certificate from the 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 (e.g., abc.com):

Online Certificate Server:

☑ Place certificate in local machine store.

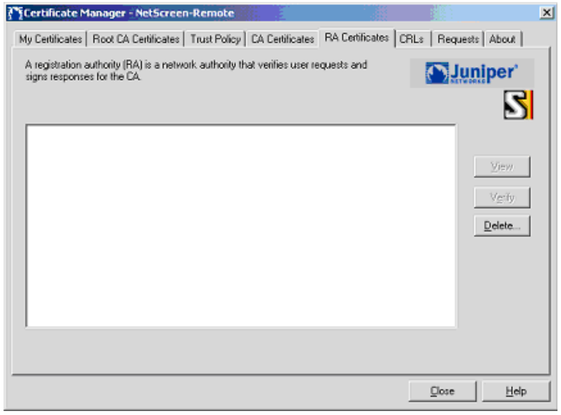
Figure 2-14 Retrieve CA Certificate Online

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



Certificate Manager - NetScreen-Remote

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

RA Certificates Window

Figure 2-15 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:

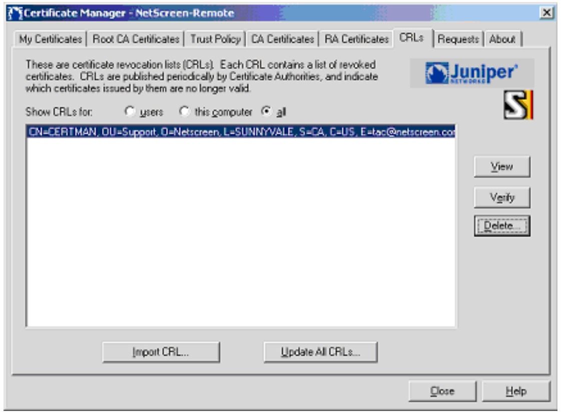
View opens the selected certificate for viewing. To close the certificate, click anywhere within the certificate displayed.

Verify checks the validity status of the selected certificate.

Delete removes the selected certificate from NetScreen-Remote.

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.

Show CRLs for: ○ users ○ this computer ● all

CN=CERTMAN, OU=Support, O=Netscreen, L=SUNNYVALE, S=CA, C=US, E=tac@netscreen.co

Certificate Revocation List Window

Figure 2-16 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.

Verify directs the client to check the validity dates and attempts to check the certificate against its CRL.

Delete removes the selected CRL from the NetScreen-Remote.

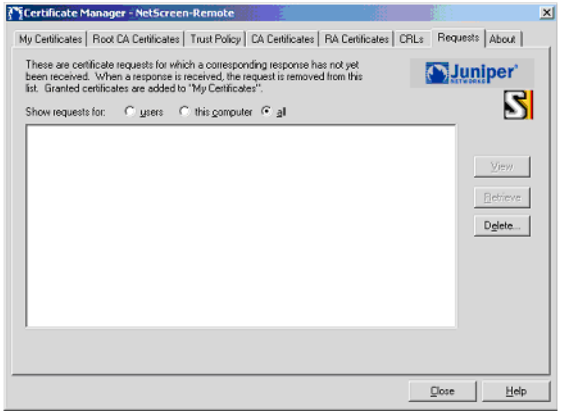
Import CRL opens a dialog box for navigating to a CRL file on your computer, and then loading the CRL into the NetScreen-Remote.

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.

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.



Pending Certificate Requests Window

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".

Show requests for: ○ users ○ this computer ● all

Figure 2-17 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:

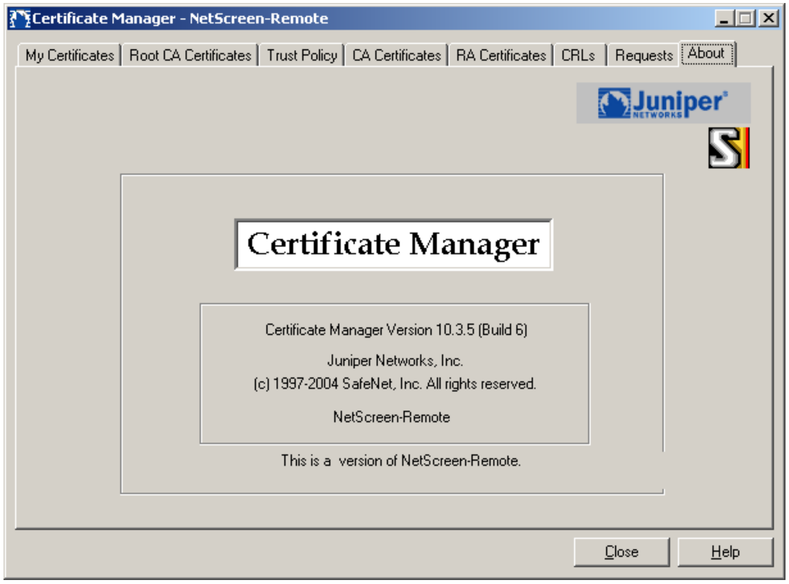
View opens the selected request for viewing.

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's Certificate Manager in use.



Certificate Manager Version 10.3.5 (Build 6)

Juniper Networks, Inc.
(c) 1997-2004 SafeNet, Inc. All rights reserved.

NetScreen-Remote

This is a version of NetScreen-Remote.

Figure 2-18 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 2-19 NetScreen-Remote Icon on the Windows Taskbar

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

NetScreen-Remote Icon

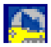
The NetScreen-Remote icon changes color and appearance to reflect the current activity and state of the NetScreen-Remote, as shown in Table 2-2.

Table 2-2 Taskbar Icons

NetScreen-Remote logo (disabled) The icon is grayed out. Either NetScreen-Remote is disabled or your Windows operating system did not start the Internet Key Exchange (IKE) service properly. If you see this icon, either try enabling the NetScreen-Remote, if disabled, or restarting your computer. If neither work, you may need to reinstall the NetScreen-Remote software. See "Modifying Installation" on page 10.

NetScreen-Remote logo (enabled) If you have successfully installed the 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.

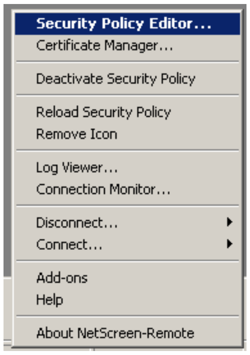


Figure 2-20 NetScreen-Remote Taskbar Shortcut Menu

- **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** toggles NetScreen-Remote on and off. When you activate NetScreen-Remote, the deactivated option displays. When you deactivate NetScreen-Remote, the activated option displays. turns off the NetScreen-Remote so that no security policies are used.
- **Reload Security Policy** replaces an existing security policy with a new security policy.

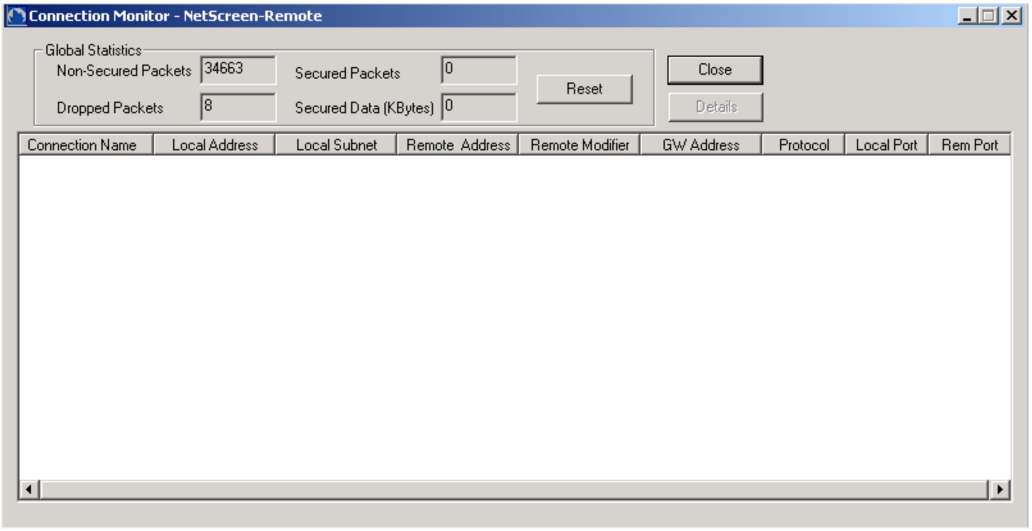
Saving changes to the security policy of an active connection terminates active connections. To delay implementing the changes until you end the currently active connection, click ***No*** *when the NetScreen-Remote prompts you to reset your active connection. Then click* ***Reload Security Policy***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

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

- **Connect** enables the NetScreen-Remote client to connect to a specific destination.

- **Disconnect** senables the NetScreen-Remote client to disconnect from a specific destination.
- **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

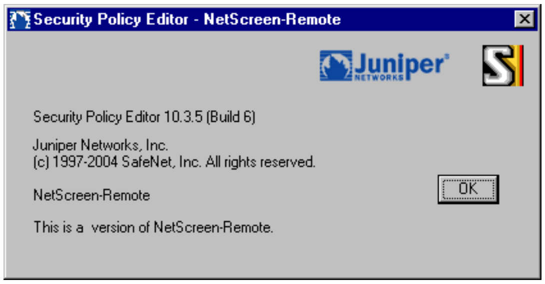
Secured Packets 0

Dropped Packets 8

Secured Data (KBytes) 0

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

- **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 - NetScreen-Remote

Security Policy Editor 10.3.5 (Build 6)

Juniper Networks, Inc.
(c) 1997-2004 SafeNet, Inc. All rights reserved.

NetScreen-Remote

This is a version of NetScreen-Remote.

3

Digital Certificates

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 the 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
- Simple Certificate Enrollment Protocol (SCEP)

Manual and SCEP 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 the NetScreen-Remote.

Detailed information on how to submit web-based certificate requests can be found in the documentation for your CA system. Juniper provides application notes on how to obtain certificates for various CA systems; these notes are available from the Juniper Technical Support site knowledgebase at http://www.juniper.net/support/. Online Enrollment via web browser is the preferred way of loading certificates, if automatic enrollment via SCEP 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 always start with a certificate request file. The 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

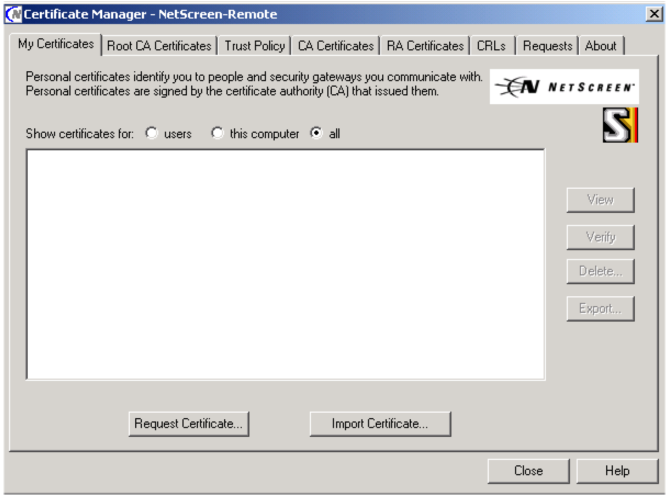
Step 6: Importing the Personal Certificate

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-Remote icon on the desktop taskbar, and then select **Certificate Manager**.
   - Double-click the NetScreen-Remote icon in the 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.



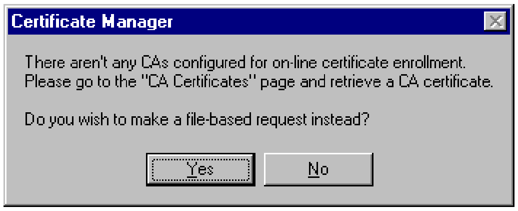
Personal certificates identify you to people and security gateways you communicate with. Personal certificates are signed by the certificate authority (CA) that issued them.

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

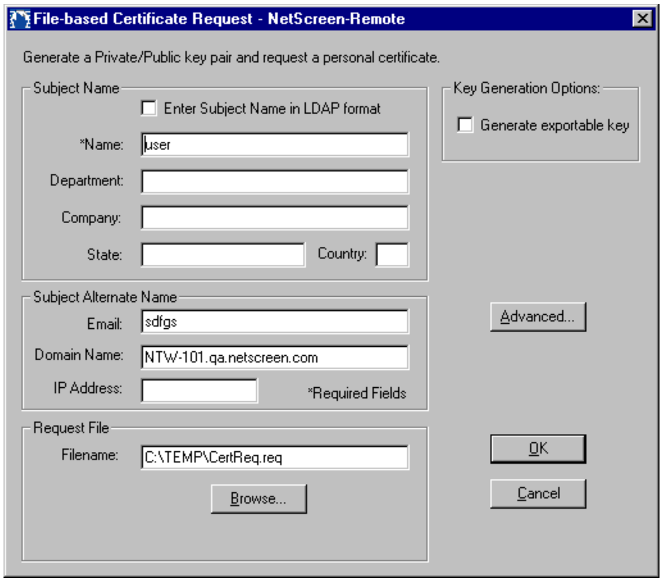
There aren't any CAs configured for on-line certificate enrollment.
Please go to the "CA Certificates" page and retrieve a CA certificate.

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: user

Department:

Company:

State: Country:

Key Generation Options:

□ Generate exportable key

Subject Alternate Name

Email: sdfgs

Domain Name: NTW-101.qa.netscreen.com

IP Address:

*Required Fields

Request File

Filename: C:\TEMP\CertReq.req

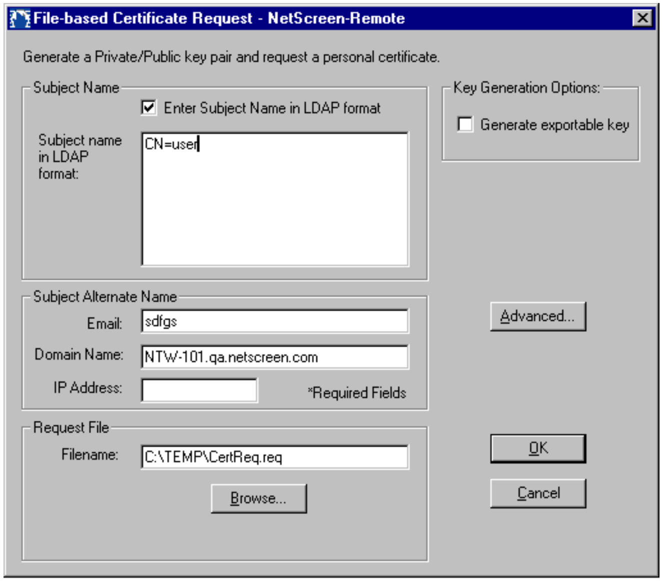
Figure 3-3 File-based Certificate Request

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=Juniper.” See Figure 3-4.*

> ***Note:*** *If you use NetScreen-Remote 8.2r1 or higher, do not enter a value for the IP address field. By entering a value in this field, the system generates a log error:*
>
> ***Invalid RSA signature***
>
> *If the error occurs, generate a new certificate request using a DNS name and/ or email address.*

Contact your CA to determine which fields are required. The Domain Name and/or Email must match the value configured for the user authentication on the NetScreen device.



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=user

Key Generation Options:

☐ Generate exportable key

Subject Alternate Name

Email: sdfgs

Domain Name: NTW-101.qa.netscreen.com

IP Address:

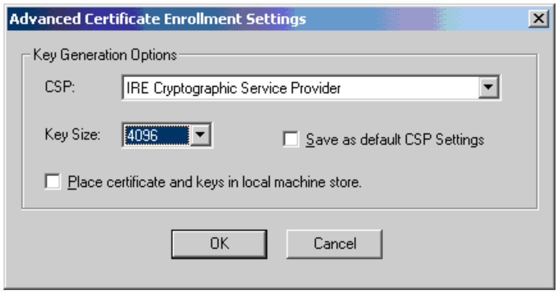
*Required Fields

Request File

Filename: C:\TEMP\CertReq.req

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: 4096

☐ Save as default CSP Settings

☐ Place certificate and keys in local machine store.

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, 2048, or 4096. NetScreen-Remote now supports key lengths up to 4,096. (Note that even though NetScreen-Remote software provides an option of a 4,096 key length, although NetScreen firewall/VPN devices are not compatible with this key length.)

Place certificate and keys in local machine store enables you to store the certificate on the local device.

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.*

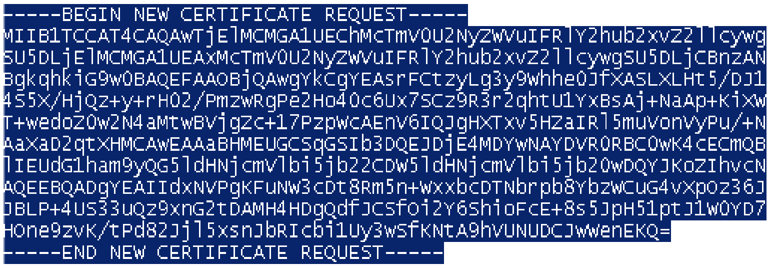
1. Go to a CA's website and follow their procedure for requesting a certificate until you reach the section where you are asked to provide your request. This usually involves submitting a saved certificate request to a website or e-mail address.

The 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

This is the step for retrieving the personal 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

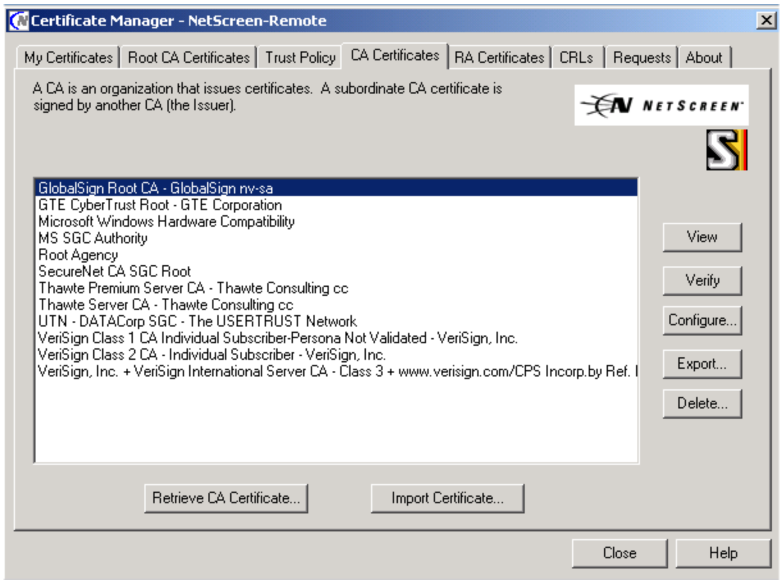
Note: *If you have Microsoft Windows XP, you may skip the following procedure. You need only to double-click the CA certificate file to import it. If you have Microsoft Windows 95, you are required to go through the following procedure to import your CA certificate.*

1. In the Certificate Manager module of the 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. l

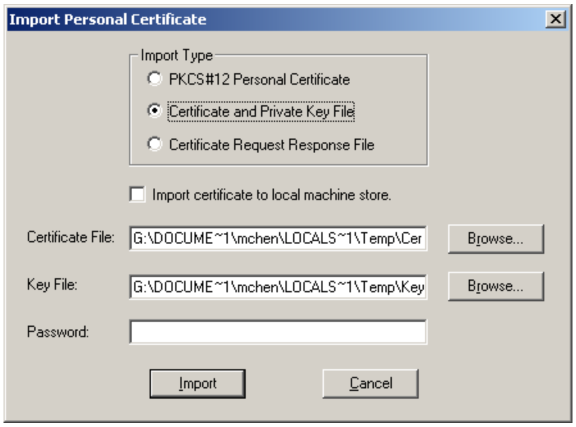
Figure 3-7 Imported CA Certificate

Step 6: Importing the Personal Certificate

> ***Note:*** *If you have Microsoft Windows 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 Personal Certificate dialog box appears.



Import Personal Certificate

Import Type

○ PKCS#12 Personal Certificate

● Certificate and Private Key File

○ Certificate Request Response File

□ Import certificate to local machine store.

Certificate File: G:\DOCUME~1\mchen\LOCALS~1\Temp\Cer

Key File: G:\DOCUME~1\mchen\LOCALS~1\Temp\Key

Password:

Figure 3-8 Import Personal Certificate

In the Import Type group select one of the following radio buttons:

- For general certificate importing of current and older certificate and key types, click the **Certificate and Private Key** option.

- For online certificate enrollment, click the **PKCS12 Personal Certificate** option.

- For a manual certificate request, click the **Certificate Request Response File**.

The import type you selected determines the devices available for you to complete.

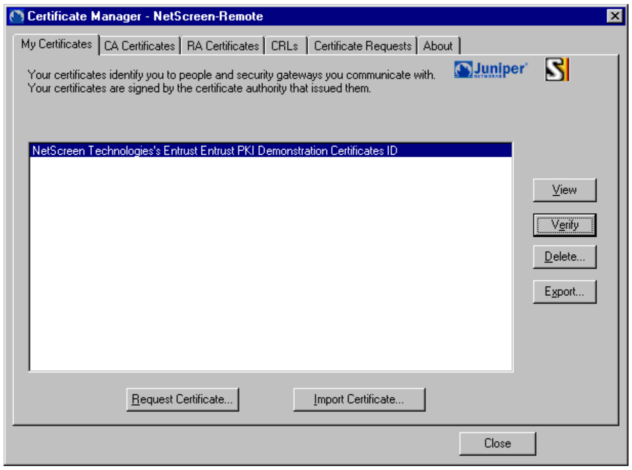
3. By default, the Import certificate to local machine store checkbox is clear which places the imported certificate in your-the logged-on user's-personal certificate store. Unless your network security administrator instructs you to change it, accept the default.

4. In the Certificate File box, type the drive, directory, and filename/file type of the personal certificate or certificate request response file to import or click Browse to locate it. The default certificate request response filename is **C:\temp_directory_for_OS\Cert.p7r.**
5. In the Key File box, type the drive, directory, and filename of the private key file to import or click Browse to locate it.
6. In the Password box, type the password used when the file was exported.
7. Unless your network security administrator advises you to change it, leave the Import certificate to local machine store checkbox selected.
8. Click **Import**.
9. When the key import confirmation message opens, click **Ok**.
10. When prompted to add this personal certificate, click **Yes**.

11. Click **Import**.

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

12. Double click on the certificate.



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.

SCEP Enrollment

The Simple Certificate Enrollment Protocol (SCEP) 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 SCEP 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

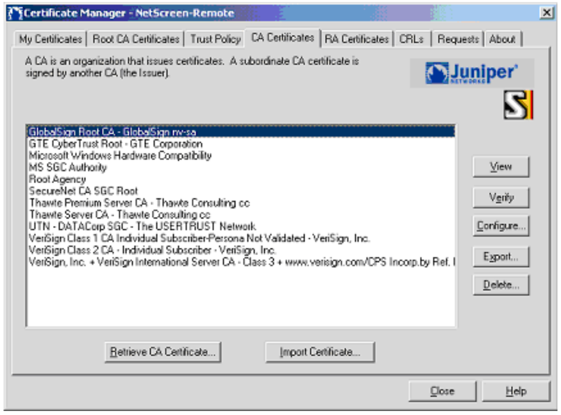
Step 1: Retrieving the CA Certificate

If you are on a network on the Trusted side of a Juniper Firewall/VPN device and are attempting to use the SCEP 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 2-19 (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-Remote 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. 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. l

Figure 3-10 CA Certificates Page

4. Click **Retrieve CA Certificate**.

The Retrieve CA Certificate Online dialog box appears:

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.

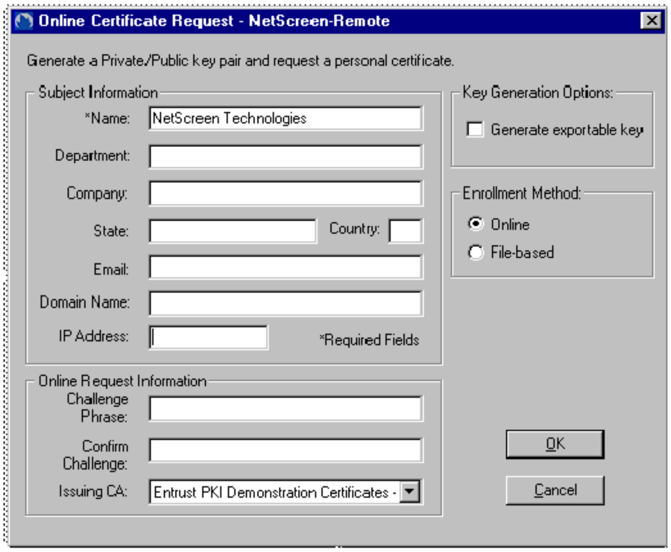
8. Click **Yes**.

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

Online Request Information

Challenge Phrase:

Confirm Challenge:

Issuing CA: Entrust PKI Demonstration Certificates -

Key Generation Options:

□ Generate exportable key

Enrollment Method:

● Online

○ File-based

Figure 3-11 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**.

The 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 46.*

11. To start using the certificate, you must first exit from the 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 SCEP 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.

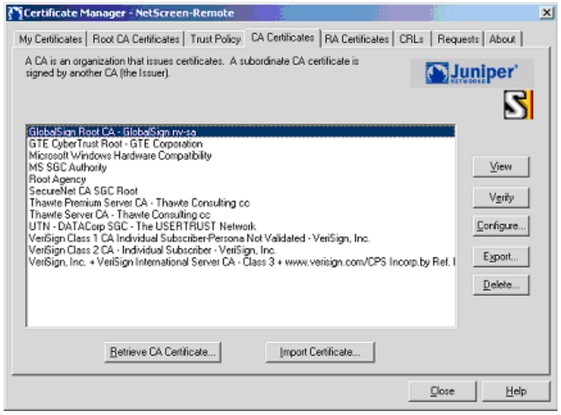
CRLs:
A CRL usually accompanies a personal certificate obtained on-line through the SCEP method if the CRL distribution point is a valid URL. If you do not automatically receive one or if you obtain a personal certificate via the cut-and-paste method, you can download and import a CRL manually. Then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



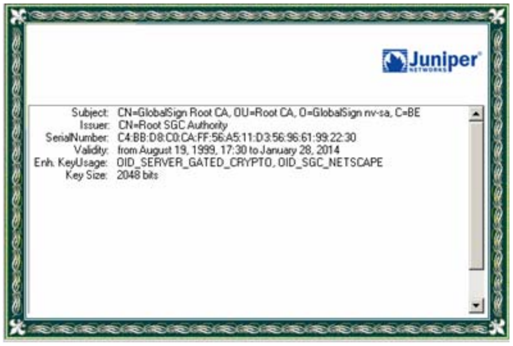
A CA is an organization that issues certificates. A subordinate CA certificate is signed by another CA (the Issuer).

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 3-12 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, 17:30 to January 28, 2014
Enh. KeyUsage:	OID_SERVER_GATED_CRYPTO, OID_SGC_NETSCAPE
Key Size:	2048 bits

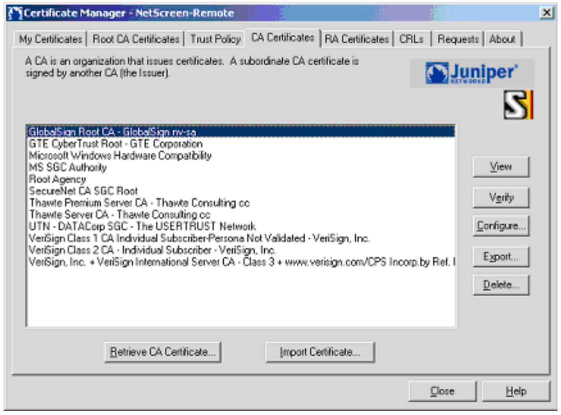
Figure 3-13 Certificate View Screen

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:



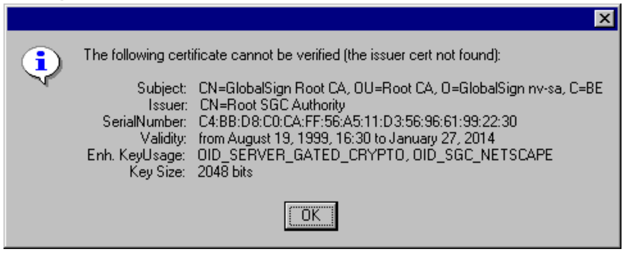
A CA is an organization that issues certificates. A subordinate CA certificate is signed by another CA (the Issuer).

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. I

Figure 3-14 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:



The following certificate cannot be verified (the issuer cert not found):

```
      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
     Key Size:  2048 bits
```

Figure 3-15 CA Certificates Verify Display

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

Exporting Certificates

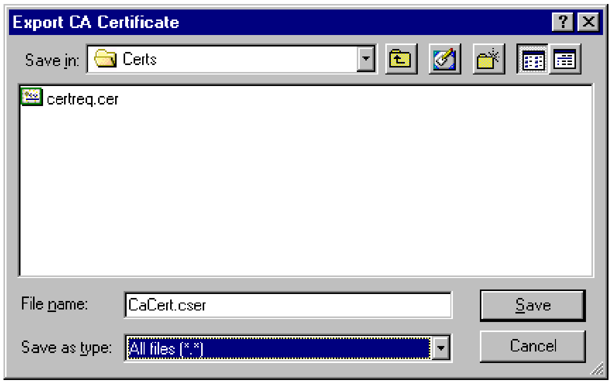
Exporting a certificate means copying it to an electronic file. You might export a certificate for reasons such as these:

- 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 3-16 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 SCEP 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:

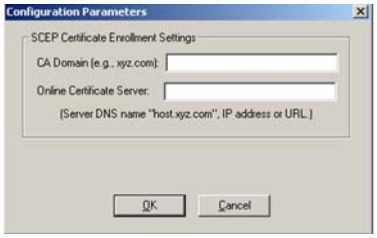

Configuration Parameters
SCEP Certificate Enrollment Settings
CA Domain (e.g., xyz.com):
Online Certificate Server:
(Server DNS name "host.xyz.com", IP address or URL.)
OK
Cancel

Figure 3-17 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

The NetScreen-Remote automatically updates CRLs obtained on-line through the SCEP 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.)

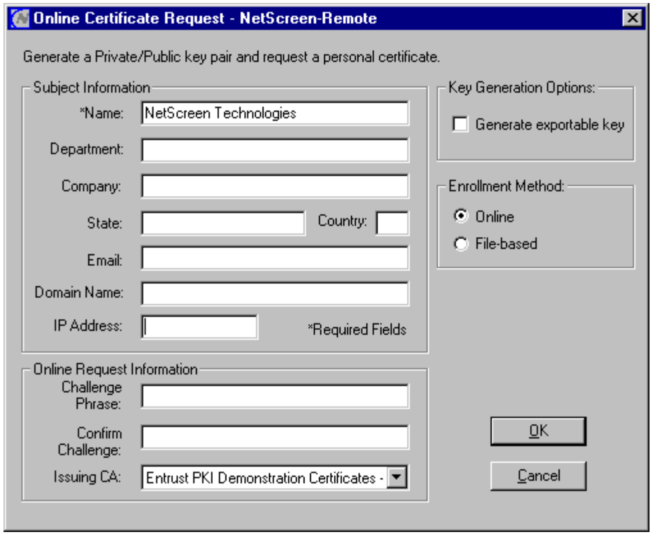
To update all the CRLs manually:

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:



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 3-18 Requests Menu

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

The 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.

4

VPNs with Pre-Shared Keys

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 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 VPN volume of the *Juniper Networks NetScreen Concepts and Examples ScreenOS Reference Guide*.

As with Manual Keys discussed in Chapter 6, “Configuring a Manual Key VPN Tunnel,” 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.

> ***Note:*** *The configuration in this section must match the one configured at the other tunnel endpoint.*

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 has either a fixed or dynamically assigned IP address.

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

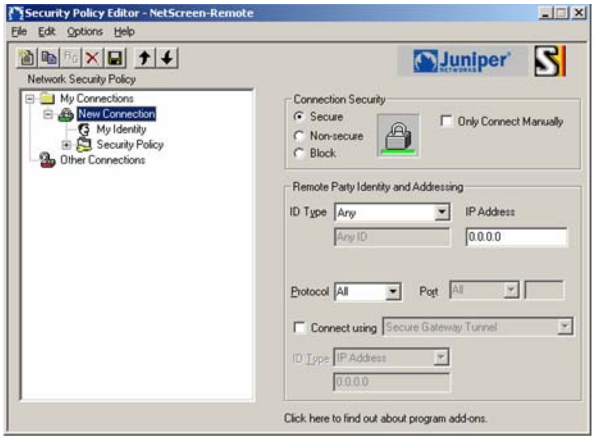
1. Creating a New Connection
2. Creating the Pre-Shared Key
3. Defining the IPSec Protocols

Step 1: Creating a New Connection

Begin by initiating a new connection. 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 **Edit**, then choose **Add**, and then click **New Connection**.

A New Connection icon appears in the Network Security Policy list, as shown in the following figure.



Connection Security
● Secure
○ Non-secure
○ Block
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: Any
Any ID
IP Address: 0.0.0.0
Protocol: All
Port: 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, GRE**. The default is **All**.

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

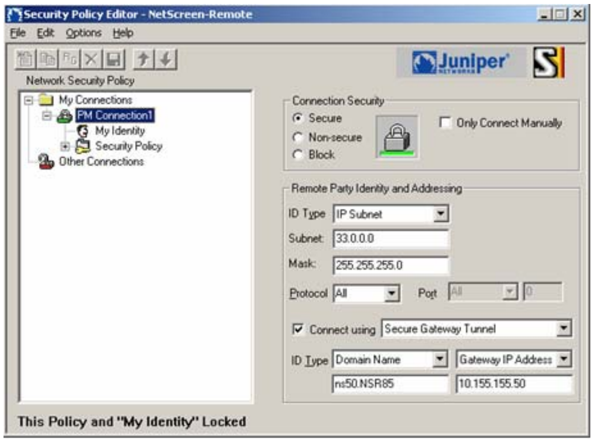
Note: *Additional protocols may be added by editing the services.txt file in the NetScreen-Remote directory.*

7. If you are using tunnel mode to connect to a Juniper Firewall/VPN 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).



Connection Security
- ● Secure
- ○ Non-secure
- ○ Block
- □ Only Connect Manually

Remote Party Identity and Addressing
- ID Type: IP Subnet
- Subnet: 33.0.0.0
- Mask: 255.255.255.0
- Protocol: All   Port: All   0
- ☑ Connect using: Secure Gateway Tunnel
- ID Type: Domain Name   Gateway IP Address
- ns50.NSR85   10.155.155.50

This Policy and "My Identity" Locked

Figure 4-2 Remote Party Identity and Addressing

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.

Step 2: Creating the Pre-Shared Key

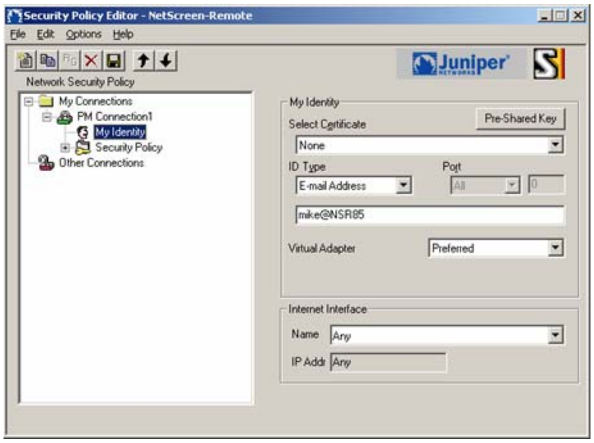
In Step 2, create the Pre-Shared Key to be used in identifying the communicating parties during the Phase 1 negotiations.

1. Double-click the icon for the new connection created in Step 1.

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.



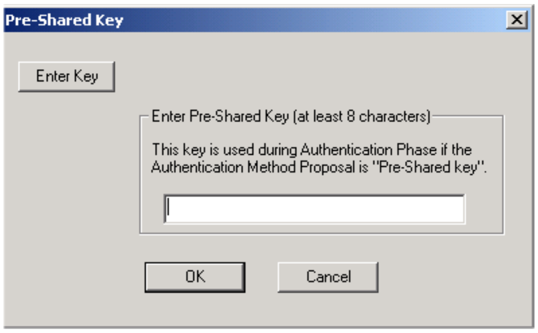
My Identity
- Select Certificate: None
- ID Type: E-mail Address   Port: All   0
- mike@NSR85
- Virtual Adapter: Preferred

Internet Interface
- 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.



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

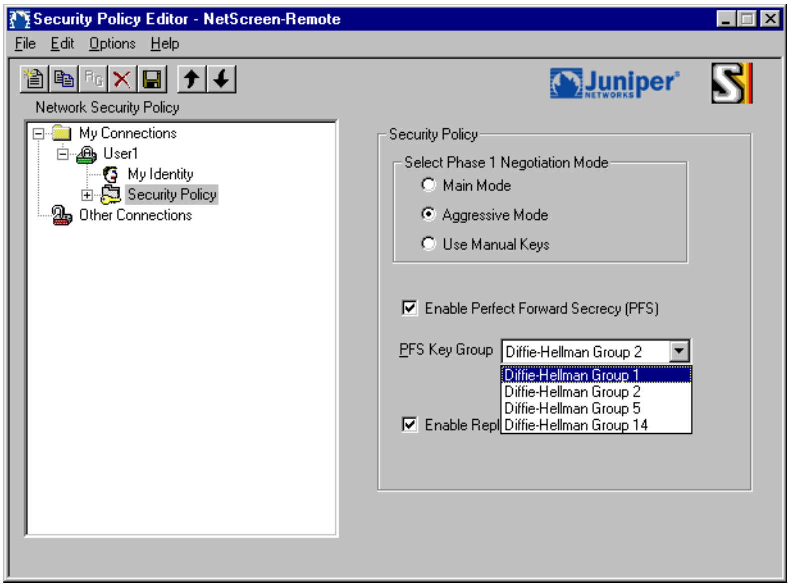
5. Click **Enter Key** to make the Pre-Shared Key field available.
6. Type a key with a length between 8 and 58 characters. A longer key length results in stronger encryption.
7. Click **OK** to save the entry.

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.



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

Diffie-Hellman Group 1
Diffie-Hellman Group 2
Diffie-Hellman Group 5
Diffie-Hellman Group 14

☑ Enable Repl

Figure 4-5 Security Policy Area

2. If you use another Juniper Firewall/VPN 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.

– In the **PFS Key Group** drop-down list, select either **Diffie-Hellman Group 1**, **Diffie-Hellman Group 2**, **Diffie-Hellman Group 5,** or **Diffie-Hellman Group 14**.

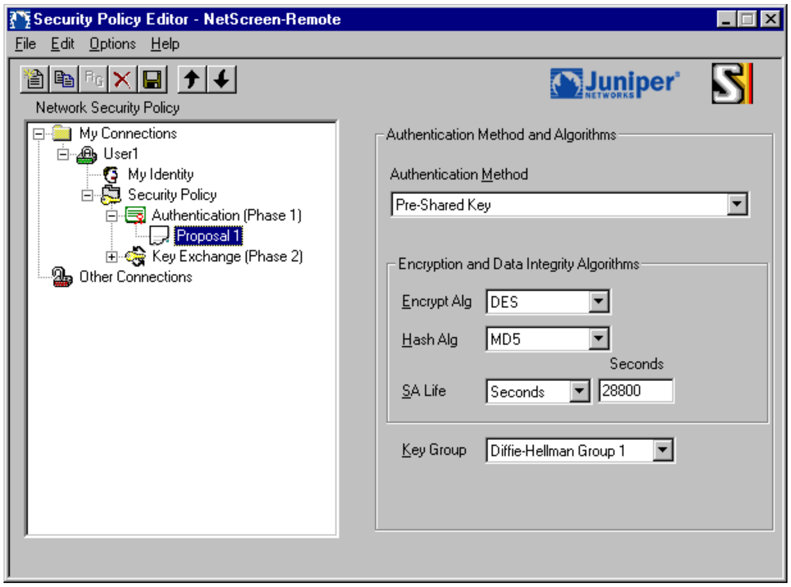
__Note:__ Juniper NetScreen firewall/VPN devices do not support Diffie Hellman Group 14.

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: MD5

SA Life: Seconds — Seconds: 28800

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**. If you will not be using XAuth, select Pre-Shared Key in the Authentication Method list.

XAuth must also be enabled on the Juniper Firewall/VPN 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. Brief descriptions of the protocols are:

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.

AES protocols — Provides maximum security for the key. The higher the AES value, the more secure the key is. AES values can be AES-128, the least secure, AES-192, medium security, and AES-256, the most secure.

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.

8. In the Key Group drop-down list, select **Diffie-Hellman Group 1**, **Diffie-Hellman Group 2**, **Diffie-Hellman Group 5,** or **Diffie-Hellman Group 14**.

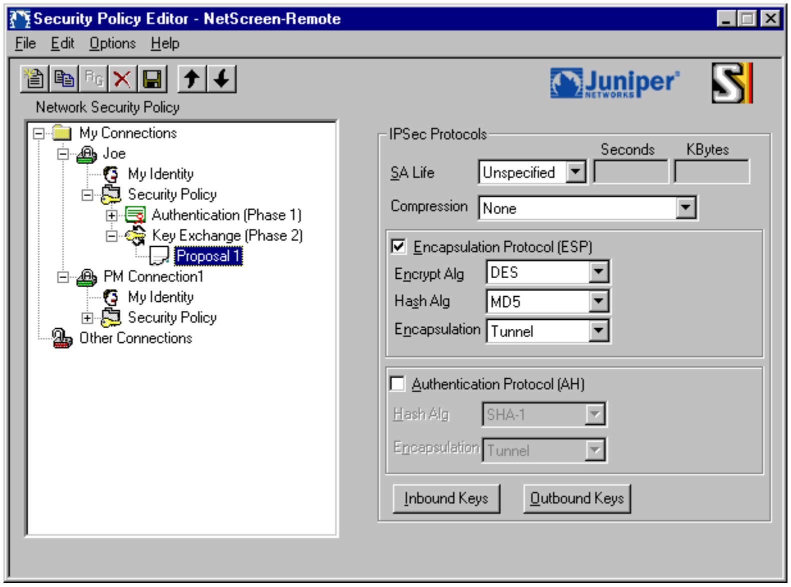
> ***Note:*** *Juniper NetScreen firewall/VPN devices do not support Diffie-Hellman Group 14.*

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.



SA Life: Unspecified

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: MD5

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 4-7 Phase 2 - Proposal 1

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 the NetScreen-Remote to accept the values proposed by the Juniper Firewall/VPN 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**.

__Note:__ Other Juniper Firewall/VPN 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.

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. Brief descriptions or protocols are provided here:

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. The following are descriptions of major protocols.

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.)

AES protocols — Provides maximum security for the key. The higher the AES value, the more secure the key is. AES values can be AES-128, the least secure, AES-192, medium security, and AES-256, the most secure.

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.

Juniper Firewall/VPN devices do not support DES-MAC.

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.

Note: *To configure the Juniper security gateway at the other end of a VPN tunnel for AutoKey IKE, refer to the first pre-shared key article referenced in Chapter 7 and to the VPN volume of the NetScreen Concepts & Examples ScreenOS Reference Guide.*

5

Configuring a VPN Tunnel with Digital Certificates

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 Juniper devices. Revoke the certification in your CA.

This chapter explains the basics of configuring the NetScreen-Remote 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, and the VPN volume of the *Juniper Networks NetScreen Concepts and Examples ScreenOS Reference Guide*.

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

There are three steps in setting up the NetScreen-Remote for a VPN tunnel with a Certificate:

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

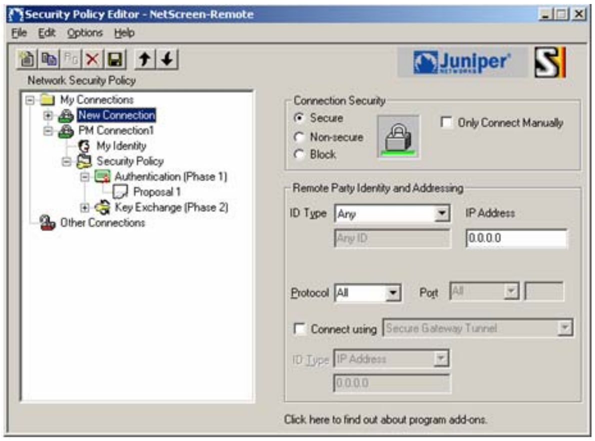
This assumes that you have already requested and installed your Local Certificate, CA Certificate, and CRL into the Certificate Manager.

Step 1: Creating a New Connection

Begin by initiating a new connection. 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, click **Edit**, then click **Add** and then click **New Connection**.

A new connection icon appears, as shown below.



Connection Security: ● Secure ○ Non-secure ○ Block □ Only Connect Manually

ID Type: Any — Any ID

IP Address: 0.0.0.0

Protocol: All Port: All

□ Connect using: Secure Gateway Tunnel

ID Type: IP Address — 0.0.0.0

Figure 5-1 New Connection

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

ID Type (first one) Indicates whether it is an IP Subnetwork Address or an Address Range which is a sequential collection of IP addresses (for example, 10.1.1.0 - 10.1.1.100) for the local node.

Protocol indicates the protocol you want to use for the connection: **All**, **TCP**, **UDP**, **ICMP, GRE**. The default is **All**.

> **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

Connect Using Secure Gateway Tunnel enables you to connect to a Juniper Firewall/VPN device if you are using tunnel mode.

ID Type enables you to identify the other party with an IP address, domain name, or distinguished name.

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.
6. Define the protocol you want to use for the Connection: **All**, **TCP**, **UDP**, **ICMP, GRE**. The default is **All**.
7. If you are using tunnel mode to connect to a Juniper Firewall/VPN 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.

Step 2: Configuring the Identity

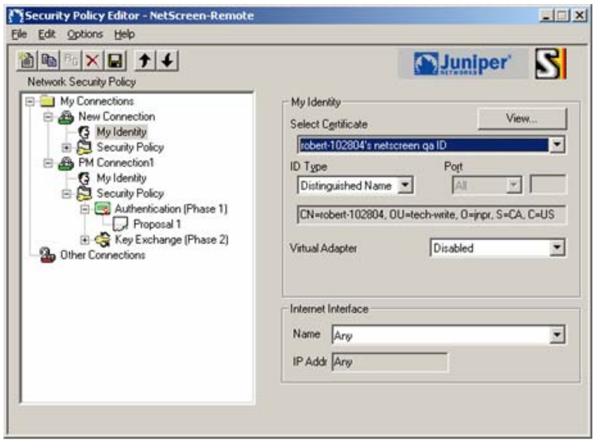
In Step 2, you configure your identity so that the party with whom you want to communicate can verify who you are.

1. Double-click the icon for the new connection created in Step 1.

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: robert-102804's netscreen qa ID

ID Type: Distinguished Name

Port: All

CN=robert-102804, OU=tech-write, O=jnpr, S=CA, C=US

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**.

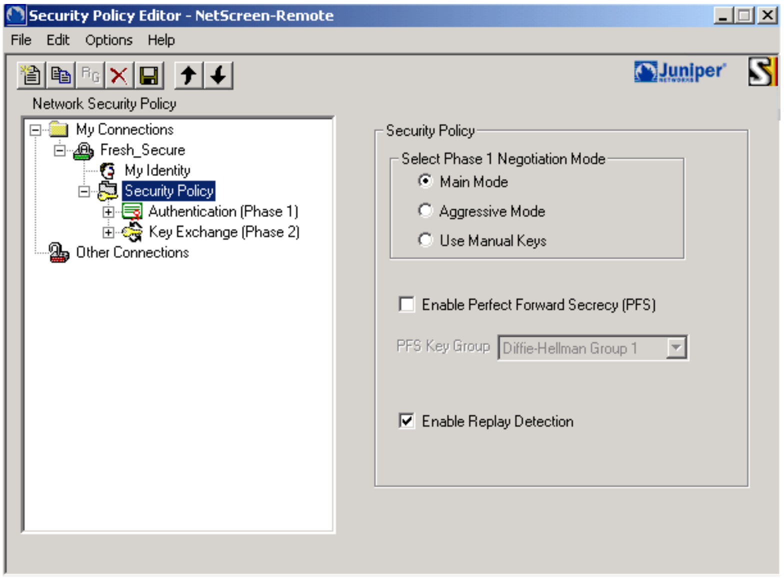
If necessary, click **View** to display the information that is in your digital certificate.

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.

– In the Key Group drop-down list, select either **Diffie-Hellman Group 1**, **Diffie-Hellman Group 2**, **Diffie-Hellman Group 5,** or **Diffie-Hellman Group 14**.

Note: *Juniper NetScreen Firewall/VPN devices do not support Diffie Hellman Group 14.*

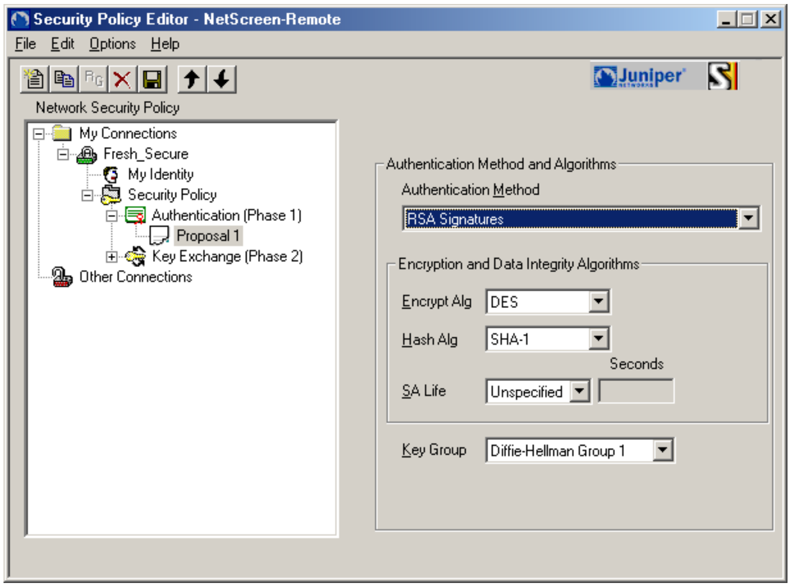
Replay Detection is a service in the Authentication Header that detects replay attacks, in which an attacker intercepts a sequence of packets, and then replays them later to gain access to network resources.

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

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

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.

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



Authentication Method: RSA Signatures

Encrypt Alg: DES

Hash Alg: SHA-1

SA Life: Unspecified

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.

The following are brief descriptions of the choices in the Authentication Method and Algorithms area.

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.

> ***Note:*** *Juniper Firewall/VPN devices do not support DES-MAC.*

7. In the Key Group drop-down list, select either **Diffie-Hellman Group 1**, **Diffie-Hellman Group 2**, **Diffie-Hellman Group 5,** or **Diffie-Hellman Group 14**.

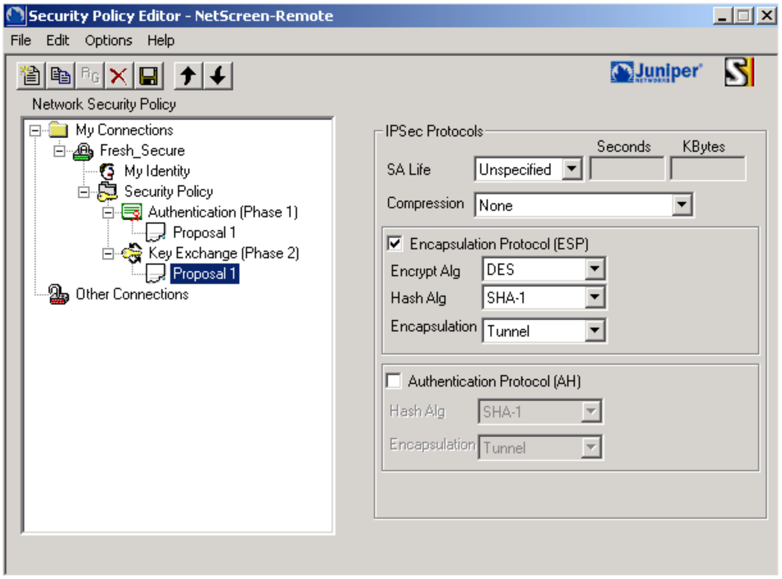
> ***Note:*** *Juniper NetScreen Firewall/VPN devices do not support Diffie Hellman Group 14.*

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.



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 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 Juniper Firewall/VPN 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 step 6.

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.

Note: *To configure the Juniper security gateway at the other end of a VPN tunnel for AutoKey IKE, refer to the first pre-shared key article referenced in Chapter 7 and to the VPN volume of the NetScreen Concepts & Examples ScreenOS Reference Guide.*

6

Configuring a Manual Key VPN Tunnel

This chapter explains the basics of configuring the NetScreen-Remote for Manual Key operation. The various options are described in this chapter including descriptions for null, md5, sha-1, etc.

> ***Note:*** *Manual Key Dial-up VPNs are compatible with ScreenOS 4.x and earlier. ScreenOS 5.0 and later revisions do not support this configuration.*

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,

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 to 7 do not apply to you.

Configuring the NetScreen-Remote

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

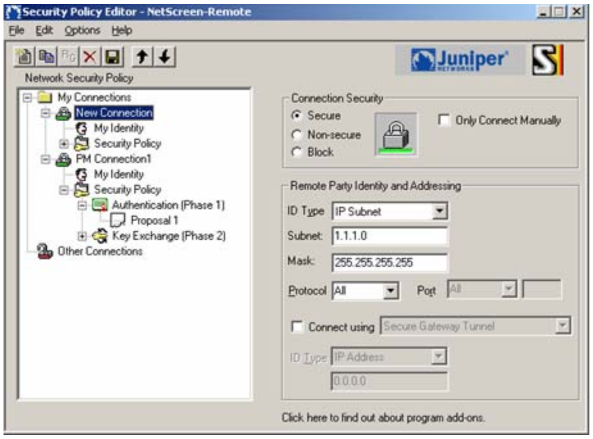
1. Creating a New Connection
2. Defining the IPSec Protocols
3. Creating the Inbound and Outbound Keys

Step 1: Creating a New Connection

Begin by initiating a new connection. 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
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 1.1.1.0
Mask: 255.255.255.255
Protocol: All
Port: 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 your CA requires more fields, click **Enter Subject Name in LDAP format** and enter the entire **Distinguished Name**.

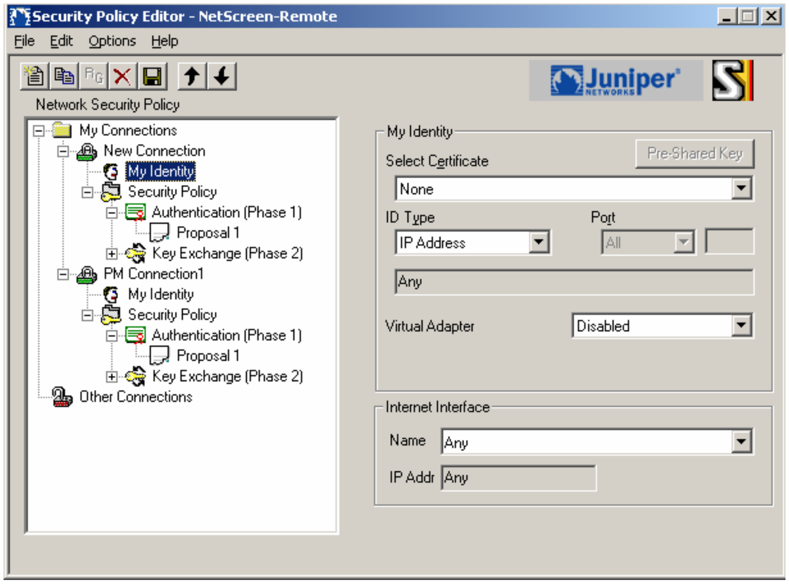
Step 2: Defining the IPSec Protocols

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.



Security Policy Editor - NetScreen-Remote

Network Security Policy

- My Connections
  - New Connection
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
  - PM Connection1
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
- Other Connections

My Identity

Select Certificate: None

ID Type: IP Address

Port: All

Any

Virtual Adapter: Disabled

Internet Interface

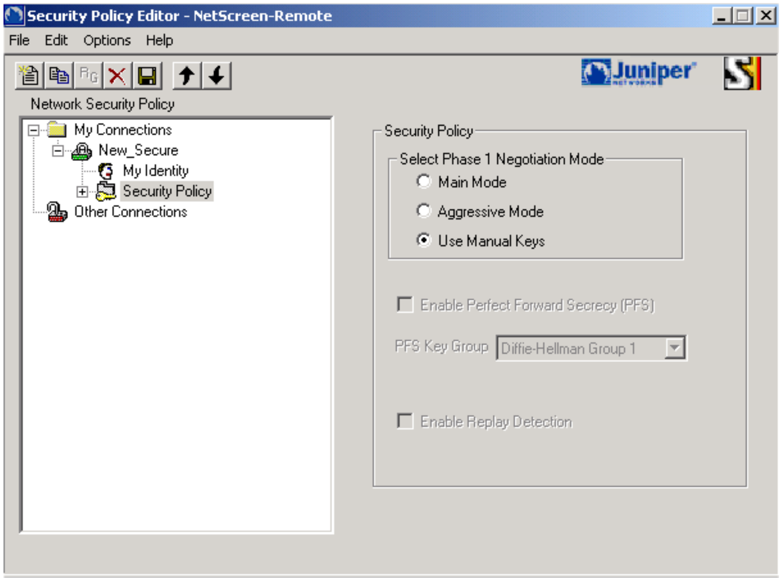
Name: Any

IP Addr: Any

Figure 6-2 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.



My Connections
New_Secure
My Identity
Security Policy
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 6-3 Security Policy

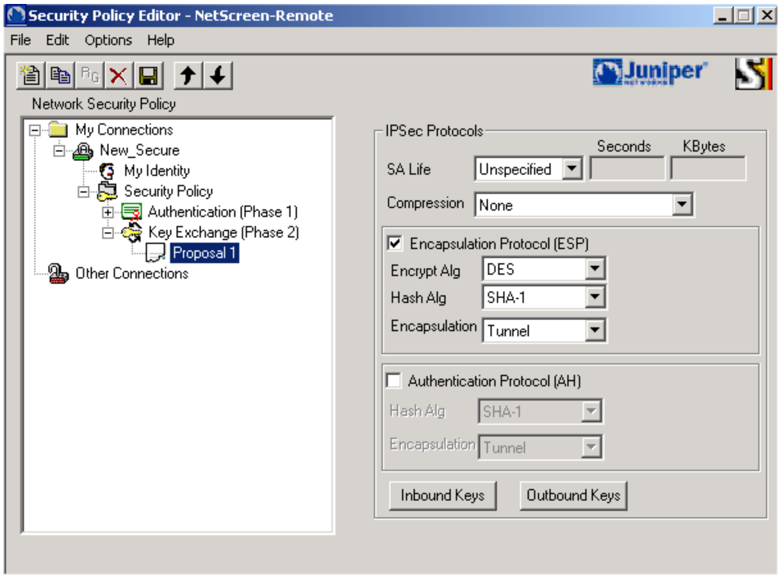
3. Select **Use Manual Keys** in the Security Policy area.

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.



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 6-4 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.**

Juniper Firewall/VPN 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.)

AES protocols — Provides maximum security for the key. The higher the AES value, the more secure the key is. AES values can be AES-128, the least secure, AES-192, medium security, and AES-256, the most secure.

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

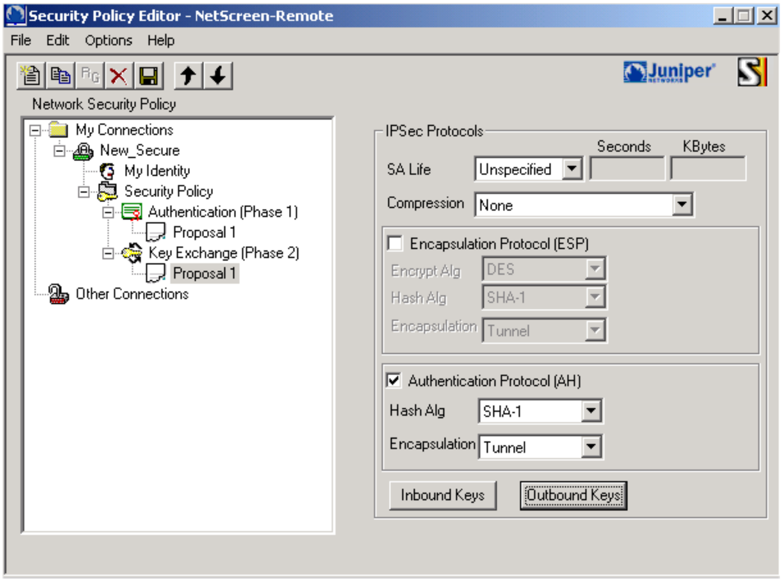
MD5—Message Digest version 5 is an algorithm that produces a 128-bit message digest or hash from a message of arbitrary length. The resulting hash is used, like a fingerprint of the input, to verify authenticity.

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.

Juniper Firewall/VPN 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 6-5 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.

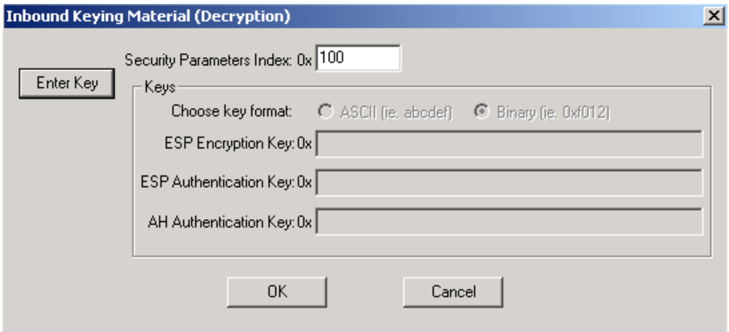
Step 3: Creating the Inbound and Outbound Keys

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)
Enter Key
Keys
ESP Encryption Key: 0x
ESP Authentication Key: 0x
AH Authentication Key: 0x
OK
Cancel

Security Parameters Index: 0x 100

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

Figure 6-6 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 Juniper 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.

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 Juniper security devices, producing different binary codes.

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
AES-128	16	32
AES-192	24	48
AES-256	32	64
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

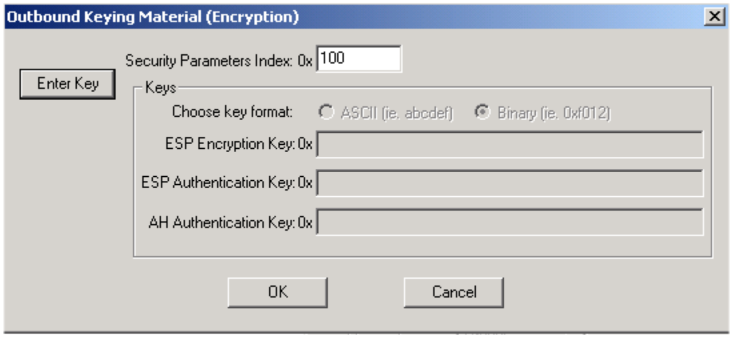
6. Click **OK** to save the settings.

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.


Outbound Keying Material (Encryption)

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 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**. Juniper recommends you do not select ASCII. See the note below.

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.

5. In the Key field(s), type the same key(s) that you used for the Inbound Keys.

> ***Note:*** *If the other end of the VPN is another Juniper Firewall/VPN 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.

> ***Note:*** *To configure the Juniper security gateway at the other end of a Manual Key VPN tunnel, refer to VPN volume in the NetScreen ScreenOS Concepts & Examples Guide.*

7

Sample Scenarios

This chapter provides sample scenarios for you to browse to gain an understanding of how you can use NetScreen-Remote with various security elements:

- Pre-Shared Keys
- Certificates
- XAuth
- IPSEc Tunnels
- Manual Keys
- NAT Traversal
- Central Site Traffic Control

Configuring a Dial-Up VPN with Pre-Shared Keys

Configuring a Dial-Up VPN Using Pre-Shared Keys

Article ID: ns4295

http://remote.support.netscreen.safeharbor.com/knowbase/root/public/ns4295.htm?

Configuring a Dial-up VPN Using Certificates

How Do I Configure a Dial-Up VPN Using Certificates?

Article ID: ns6228

http://remote.support.netscreen.safeharbor.com/knowbase/root/public/ns6228.htm?

Configuring a Dial-Up VPN with XAuth

Configuring the NetScreen-Remote Client to a NetScreen Device VPN With XAuth

Article ID: ns10160

http://remote.support.netscreen.safeharbor.com/knowbase/root/public/ns10160.htm?

Configuring L2TP Over IPSec Tunnel

Configuring L2TP Over an IPSec Tunnel

Article ID: ns10062

http://remote.support.netscreen.safeharbor.com/knowbase/root/public/ns10062.htm?

Configuring a Dial-Up VPN with Manual Key

Configuring a Manual Key Dial-Up VPN User

Article ID: ns10097

http://remote.support.netscreen.safeharbor.com/knowbase/root/public/ns10097.htm?

Configuring a Dial-Up VPN using NAT Traversal

Configuring Your NetScreen Device and NetScreen-Remote Client VPN Using NAT Traversal

Article ID: ns10150

http://remote.support.netscreen.safeharbor.com/knowbase/root/public/ns10150.htm?

Setting a Dial-Up VPN with Central Site Traffic Control

How Do I Force All Dial-Up VPN Traffic Through the Juniper NetScreen Firewall/VPN Device Before Going to the Internet?

Article ID: ns10446

http://remote.support.netscreen.safeharbor.com/knowbase/root/public/ns10446.htm?

8

Large Scale Distribution with NetScreen-Global PRO

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. The user logs in with their NetScreen-Remote login, the user's VPN. Global PRO pushes the SPD file into NetScreen-Remote. At this time, the VPN tunnel can be built.

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 the NetScreen-Remote, customizing or "repackaging" the installation package for easy distribution may be necessary.

- Using NetScreen-Remote Login

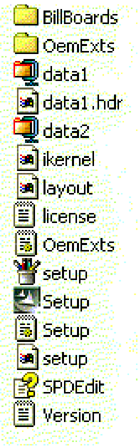
  Once invoked, a remote user must authenticate herself or himself with a User ID and Password. Only after the User ID and Password is verified against the Global-PRO Arbitrator will that user's VPN policy be downloaded into the NetScreen-Remote.

  - 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 the 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 the 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 the 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 the 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 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 the 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, the 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-Remotes 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 the 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 the 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=Policy Manager
PrependPrefix=cn=

[Arbitrator]
CertificateName=CN=2435823409852304985
ArbitratorAddress=10.150.42.100
ArbitratorPort=1099
SSL=true
retrycount=1
timeout=20
```

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 Juniper Networks 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, the 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. The 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 the NetScreen-Remote will attempt before failing over to the next Global-PRO Arbitrator. This field is required.

Timeout defines the number of seconds the 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 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 the 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 the 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 the 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 the 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%\Juniper\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\Juniper\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 the 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 the 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 the 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 the 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, the 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 the 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]

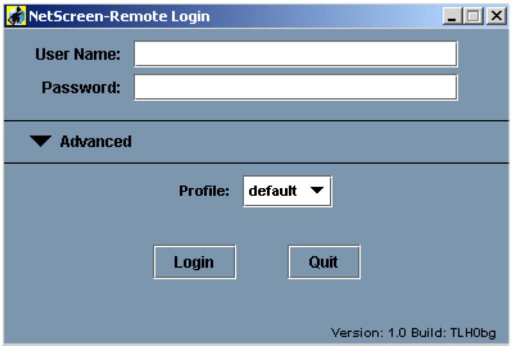
```
CmdLine=-xInstall.ini# Define install file here

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 the 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

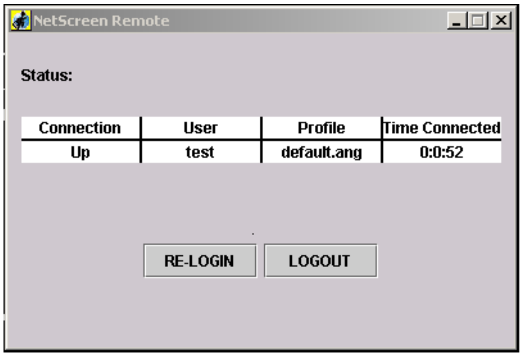
Figure 8-2 NetScreen-Remote Login - Advanced Settings

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 and a user will not be able to connect to the VPN again until they re-launch NetScreen-Remote Login 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. 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 the NetScreen-Remote.

If a user double-clicks on the NetScreen-Remote Login icon, their connect status and duration is displayed:



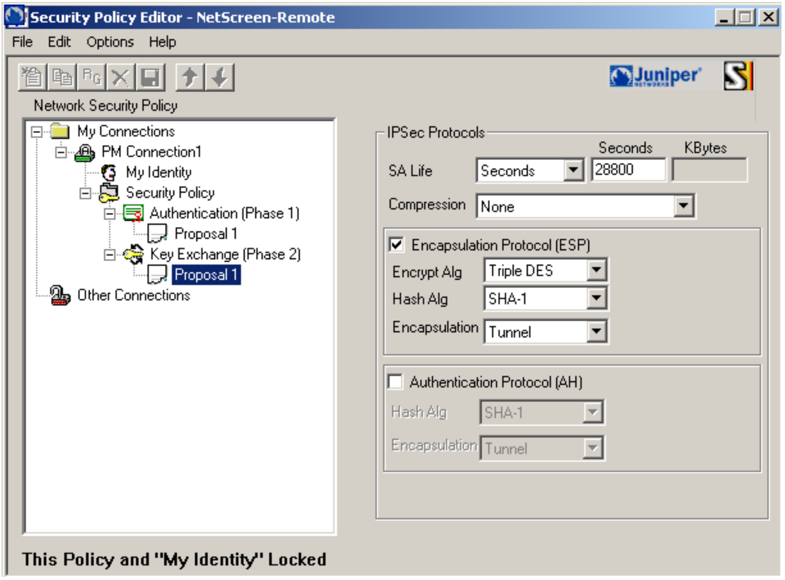
Status:

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:



		Seconds	KBytes
SA Life	Seconds	28800	
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

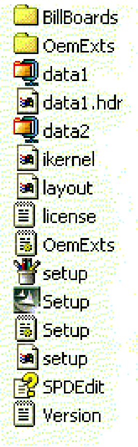
  Define the Security Policy for all users. Multiple sets can be created for user groups with different network requirements. For example, you may have a user who needs to be able to make VPN connections to their company headquarters, two satellite offices, and four vendors. Within each connection, the network administrator defines the specific Security Policy parameters of that connection.

- Exporting Policies and Delivering These to Users

  Juniper 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 in the foreground. NetScreen-Remote does not support background installations.)
- 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

oemexts.ini

This default oemexts.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%\Juniper\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\Juniper\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, “VPNs with Pre-Shared Keys”
- 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 Juniper device. For more information, see the VPN volume of the Juniper Networks NetScreen Concepts and Examples ScreenOS Reference Guide.*

Exporting Policies and Delivering These to Users

The network administrator needs to export each user’s policy for subsequent distribution to that user.

To export an existing security policy:

1. Double-click the NetScreen-Remote icon from the task bar.
2. From the File menu, click **Export Security Policy**.

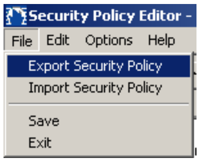
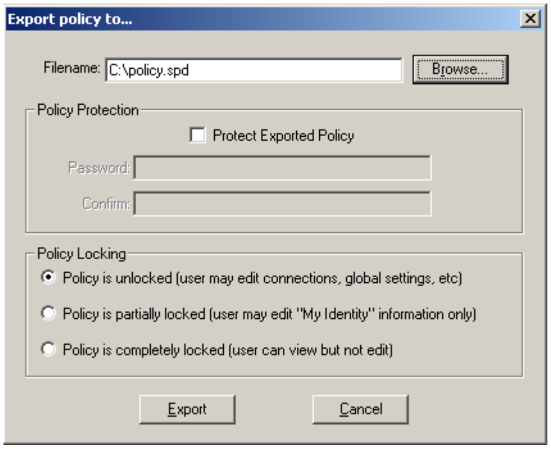


Figure 9-2 Export Security Policy

NetScreen-Remote displays the **Export Policy to** dialog box.



Filename: C:\policy.spd

Policy Protection

□ Protect Exported Policy

Password:

Confirm:

Policy Locking

● Policy is unlocked (user may edit connections, global settings, etc)

○ Policy is partially locked (user may edit "My Identity" information only)

○ Policy is completely locked (user can view but not edit)

Figure 9-3 Export Policy To dialog box

3. Click the Browse button and select a folder where you want to place the policy file.
4. To provide authentication for the policy, you can click on the Protect Exported Policy checkbox and type a string in the Password box and retype the string in the Confirm box. This provides password access to the file.
5. You can choose one of the three policy locking options. They are:

- Policy is unlocked where the user has privleges to edit connections and global settings.
- Policy is partically locked where the user may edit the “My Identity” information only.
- Policy is completely locked where the user can onlyv view the file, but not write to it.

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 **ipsecpolicy.spd** and placing it in the NetScreen-Remote setup directory. After installation, these default settings will be used.

10

Contacting Technical Support

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 the Juniper Technical Assistance Center (JTAC). JTAC is available to users with valid service contracts of NetScreen-Remote. You can contact JTAC by one of the following ways:

- Phone: 1-888-314-JTAC (U.S., Canada, and Mexico)
- Phone: 408-745-9500
- Online Knowledge Base for NetScreen-Remote at

  http://nsremote-support.netscreen.com

A

Conifguring L2TP

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 Juniper Firewall/VPN device.

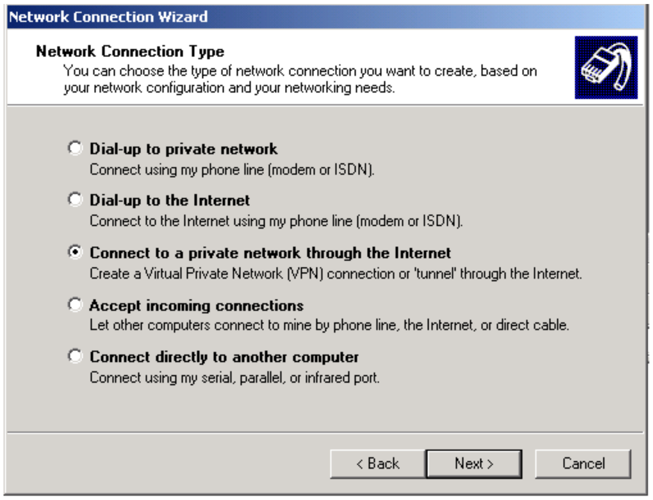
Note: *The following procedure provides instruction on how to set up L2TP VPN connections on Windows 2000. A similar procedure is used to set up L2TP connections for Windows XP SP2.*

Configuring an L2TP Connection for Windows 2000

To configure Microsoft Dial-Up Connection for a L2TP VPN connection for Windows 2000:

1. On the Windows desktop, click **Start**, then click **Settings**, then click **Network and Dial-up Connections**. The **Dial-Up Connections** dialog box displays.

2. Double click **Make New Connection**. The **Network Connection** wizard displays.



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.

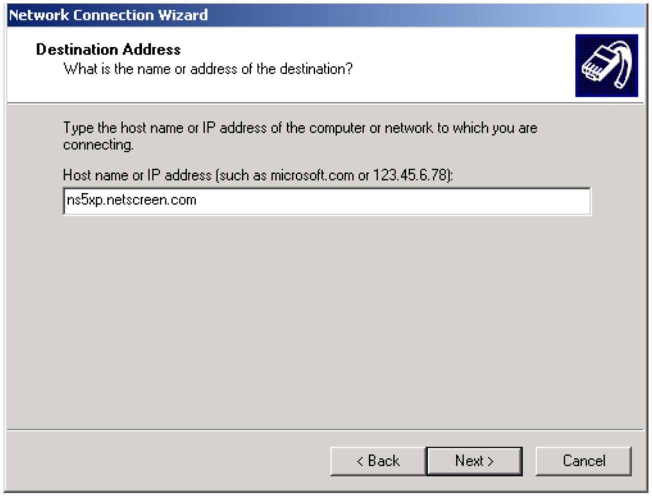
○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

Note: *If this is the first dial-up connection for your computer, you may be prompted to provide some preliminary data. Follow the prompts until you return to the Network Connection wizard.*

3. On the **Network Connection Type** page, go to the Select the devices to use in this connection list, and check as many of the check boxes that apply; you must select at least one. If you are not sure which ones to select, contact your network administrator.
4. Click **Next**.
5. On the **Public Network** page, click Do not dial the initial configuration.
6. Click **Next**.

7. On the **Destination Address** page, identify the remote party's L2TP server.



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 10-1 Destination Address dialog box

8. In the **Host name** or **IP address** box, type the IP address of the remote party's L2TP network server.
9. Click **Next**.
10. On the **Connection Availability** page, select whether to make this connection available to only you or all others who use your computer.
11. Ask your network administrator which option to select, and then click that option.
12. Click **Next**.
13. On the Completing the Network Connection wizard page, type the name for this connection. The default is **Virtual Private Connection**.
14. Click **Finish**.

Configuring an L2TP Connection for Windows XP

To configure Microsoft Dial-Up Connection for a L2TP VPN connection for Windows XP:

1. On the Windows desktop, click **Start**, then click **Settings**, then click **Network Connections**. The **Network Connections** window displays.
2. Double click **Make New Connection**. The Network Connection wizard displays.
3. Click **Next**. The **Network Connection Type** page opens.

Note: *If this is the first dial-up connection for your computer, you may be prompted to provide some preliminary data. Follow the prompts until you return to the Network Connection wizard.*

4. Click **Connect** to the network at my workplace.

5. Click **Next**. The **Network Connection** page displays.
6. Click **Virtual Private Network** connection.
7. Click **Next**. The **Connection Name** page opens.
8. In the **Workplace** box, type the name for this connection.
9. Click **Next**. The **VPN Server Selection** page displays.
10. Type the hostname or IP address of the remote party's L2TP server.
11. Click **Next**. The **Connection Availability** page displays.
12. For the **Create the connection for** option, accept the default, Anyone's use, or click **My use only**.
13. Click **Next**. The **Completing the New Connection** wizard page displays.
14. If you want to create a shortcut, select the **Add a shortcut to this connection to my desktop** checkbox.
15. Click **Finish**.

You have completed configuring Microsoft Dial-up Networking for an 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

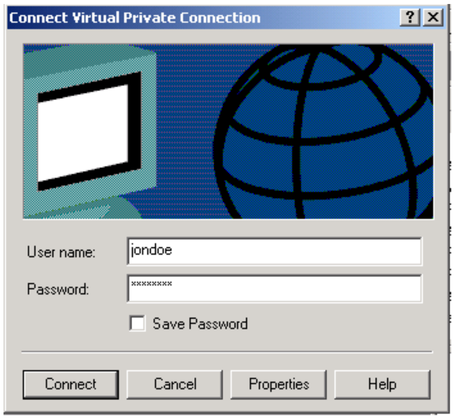
After you successfully configure your L2TP VPN connection via the Microsoft Dial-up Networking dialog box, you are able to connect to your L2TP VPN connection.

> ***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 10-2 Connect Virtual Private Connection

2. Enter your user name and password, and then click **Connect**.

Your L2TP VPN connection will be established.

B

Deploying NetScreen-Remote with Smart Cards

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-Remote, as well as the ID type to use when deploying NetScreen-Remote on a large scale using Group IKE IDs on the NetScreen-Remote.

- Configuring NetScreen-Remote to Accept your Smart-Card Certificates

  This section explains how to configure a Group IKE ID on the NetScreen-Remote. This configuration allows the product 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 NetScreen-Remote 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 NetScreen-Remote."Configuring a VPN Tunnel with Digital Certificates" on page 67 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 NetScreen-Remote.

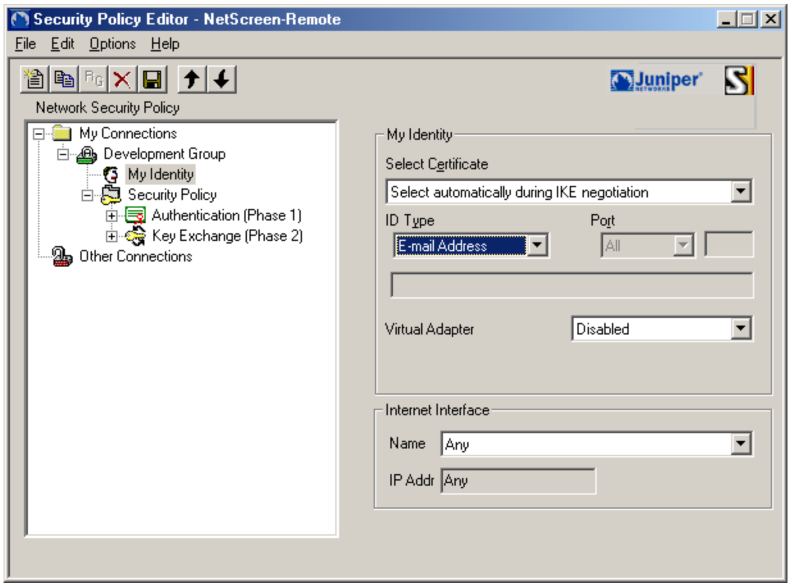
Perform the following steps to configure NetScreen-Remote to select the certificate and the ID type to send to the NetScreen-Remote:

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 10-3 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-Remote 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-Remote, 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-Remote to accept your smart-card certificates. See the next section, “Configuring NetScreen-Remote to Accept your Smart-Card Certificates.”

Configuring NetScreen-Remote 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 NetScreen-Remote, 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 Juniper Firewall/VPN device will permit any user whose signed certificate has the DN fields of OU=Sales and O=Juniper 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 *Juniper Networks 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=Juniper within the DN fields. It is not necessary to add individual users to NetScreen-Remote. You need only approve or issue certificates to users for authentication purposes.

Index