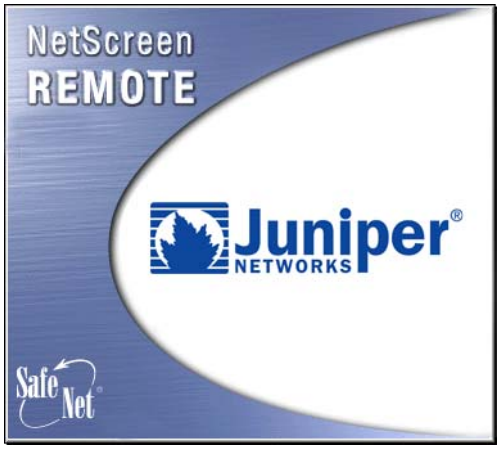
JUNIPER NETWORKS NETSCREEN-REMOTE SECURITY CLIENT INSTALLATION GUIDE



Version 8.6 P/N 093-1636-000 Rev. A

Licenses, Copyrights, and Trademarks

NETSCREEN-REMOTE 8.6 LICENSE AGREEMENT

PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THIS PRODUCT. BY INSTALLING AND OPERATING 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 ("Juniper"), 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 Juniper 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, Juniper 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 Juniper; 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 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.

Trademarks

Juniper Networks, NetScreen Technologies, Inc, the NetScreen 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.

Contents

Contents i

Preface

This installation guide is intended for Network Administrators to send to their end users along with the Juniper NetScreen-Remote Security Client software. If you need technical assistance with installing or using NetScreen-Remote Security Client, contact your Network Administrator or value-added reseller (VAR).

WHAT IS JUNIPER NETSCREEN-REMOTE SECURITY CLIENT?

Juniper NetScreen-Remote™ Security Client is a virtual private network (VPN) client that you can use to send and receive secure communications over the Internet, and it is also a security client that protects you and your computer from unwanted intruders. NetScreen-Remote Security Client is certified by the International Computer Security Association (ICSA) as an IPSec-compliant VPN solution.

When NetScreen-Remote Security Client operates on an unprotected public network, such as the Internet, it can create a VPN tunnel between an end user and a Juniper 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. NetScreen-Remote Security Client allows users to specify an internal network IP address to be sent for client-to-gateway communications.

NetScreen-Remote Security Client includes all the features of NetScreen-Remote VPN with the addition of an integrated personal firewall to provide additional security for mobile users. The NetScreen-Remote Security Client, which incorporates Sygate Technologies' award- winning personal firewall software, brings together numerous host-based security features with Juniper's VPN Client to protect mobile users systems from outside attacks, as well as targetted attacks against the VPN by Trojan applications.

NetScreen-Remote Security Client starts automatically each time the computer starts and runs transparently behind other software applications.

WHO SHOULD READ THIS GUIDE?

Any system administrator or person who is to install and initially set up the NetScreen-Remote Security Client. This guide describes how to install and set up NetScreen-Remote Security Client for VPN connections.

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.

USING THIS GUIDE

The following chapters are provided within this document:

Note

Note: The term “NetScreen-Remote” is used in chapters 1 through 4 and Chapter 7 to reference the VPN client component of the NetScreen-Remote Security Client product. “NetScreen-Remote Security Client” is used within chapters 5 and 6 to reference the firewall component of the of the NetScreen-Remote Security Client product.

Chapter 1, “Installation,” describes the NetScreen-Remote system prerequisites, how to update NetScreen-Remote Security Client from previous versions, and how to install the software, as well as how to modify this installation.

Chapter 2, “VPN Login/Logout,” describes how to login into your VPN with NetScreen-Remote Login, as well as log out of it.

Chapter 3, “Manually Loading Security Policies and Certificates,” provides instruction on how to back up existing security policies, load security policies, and load and verify certificates within NetScreen-Remote Security Client.

Chapter 4, “Configuring and Connecting to an L2TP VPN Connection,” explains how to configure L2TP VPN connections via Microsoft Dial-Up Networking. This chapter also describes how to connect to your L2TP VPN connection using Microsoft Dial-Up Networking.

Chapter 5, “Contacting Technical Support,” provides information on how to contact Technical Support.

RELATED PUBLICATIONS

Juniper Networks NetScreen-Remote Security Client Administrator's Guide

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

This chapter covers the following information:

System Prerequisites

Install the NetScreen-Remote in the following environment:

PC-compatible Computer	• Pentium processor or its equivalent
Operating System	• Microsoft Windows 2000 Professional or • Windows XP® Professional or Home Edition
Minimum RAM	• 64 MB RAM for Windows 2000 or Windows XP
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

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. If you do not have a previous version, go to the "Installation" section.

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

To manually uninstall a previous version of NetScreen-Remote:

Note: This procedure requires the PC/Laptop to be rebooted in order to finish the uninstall process. Please exit all other programs and appliations before proceeding.

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.

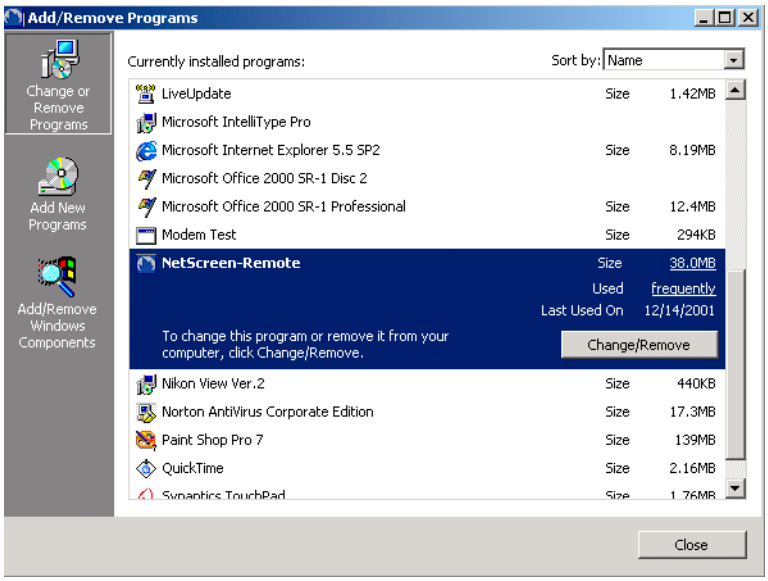


Figure 1-1 List of Installed Programs

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

   The following dialog box appears.

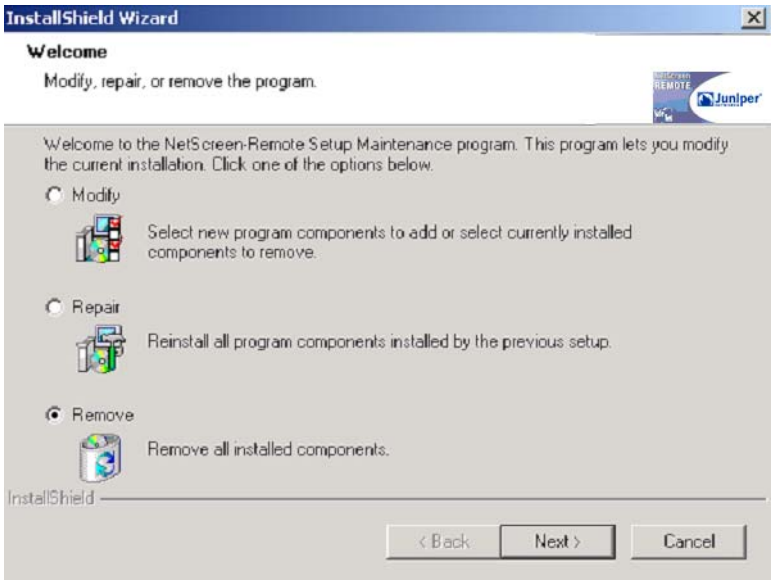


Figure 1-2 Modify, Repair, or Remove the Program

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

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

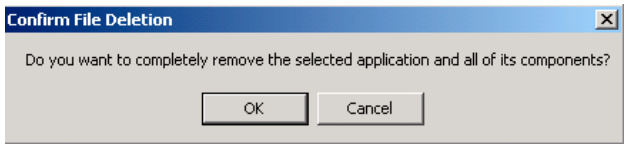


Figure 1-3 Deletion Confirmation Message

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

   The following alert box appears:

Figure 1-4 Delete Security Policy Alert Box

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

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

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

   A progress box appears.

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

INSTALLATION

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 or VPN client running at a time, running multiple firewalls and 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). The installation process requires the PC/Laptop to be rebooted at the end of the process.

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

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

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.

Note: When installing this product on Windows 2000 or Windows XP, administrator or its equivalent level of access is required.

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 NetScreen-Remote from a CD-ROM:

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

The following menu appears:

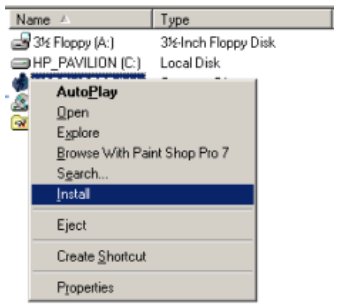


Figure 1-5 Select Install

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

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

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

—To install NetScreen-Remote from a website:

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

Continuing with Installation

The NetScreen-Remote setup application starts on your system:

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

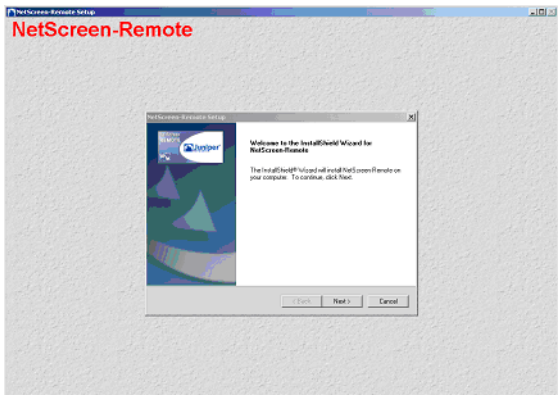


Figure 1-6 NetScreen-Remote Installation Welcome Screen

The Software License Agreement appears.

Figure 1-7 License Agreement

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

The **Setup Type** dialog box appears.

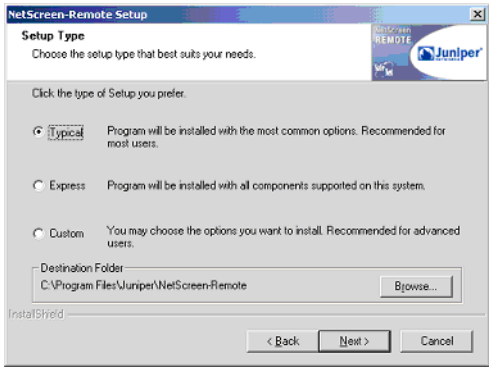


Figure 1-8 Installation Setup Type

3. Select one of these options:

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

   Express —Installs only the components that the system supports.

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

4. To install NetScreen-Remote in the default destination folder (C:\Program Files\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 1-9), and then click **Next**.

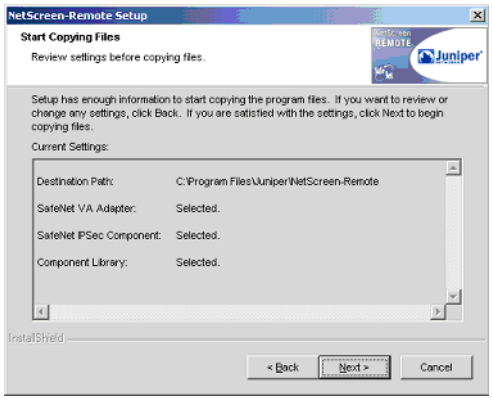


Figure 1-9 Start Copying Files

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

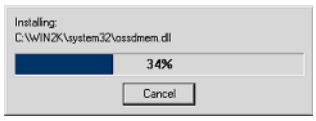


Figure 1-10 Device Reboot

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

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

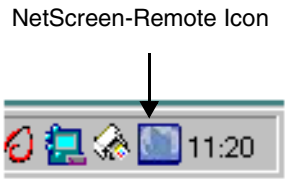


Figure 1-11 NetScreen-Remote icon on the Windows Taskbar

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 1-11. 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. 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.

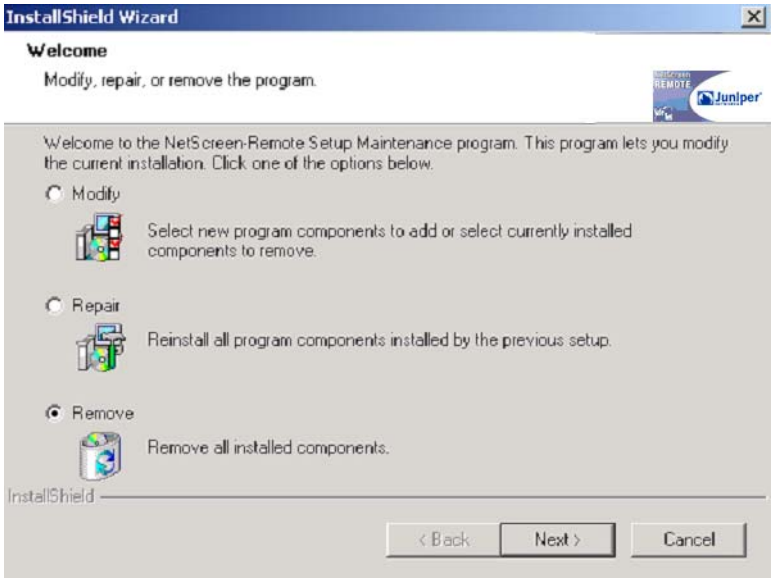


Figure 1-12 Modify, Repair, or Remove the Program

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.

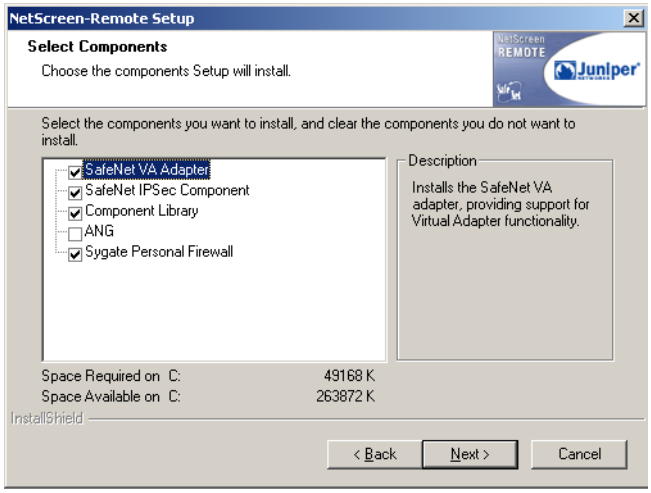


Figure 1-13 Select Components

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

   The re-installation procedure begins.

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

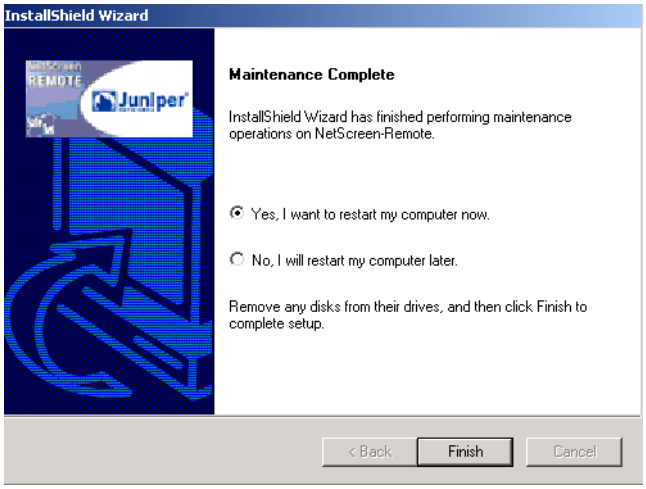


Figure 1-14 Maintenance Complete

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

2

VPN Login/Logout

This chapter covers the following information:

LOGGING INTO A VPN WITH NETSCREEN-REMOTE LOGIN FOR ANG USERS

In some circumstances, if you are an ANG user, you will use the NetScreen-Remote in a managed mode. If your Network Administrator has deployed a NetScreen-Global PRO line of security management systems, your NetScreen-Remote is designed to connect to the management system to authenticate your user identity. Once you have been successfully authenticated, NetScreen-Remote will download your VPN Security Policy and automatically install it onto your computer. After this occurs, you are able to access all VPN Network Resources.

Note: Logging in only applies to users who have to log into a Global PRO database.

To login and connect to your VPN:

1. On the Windows taskbar, click the **Start** button, and then click **NetScreen-Remote Login** to launch the NetScreen-Remote Login.

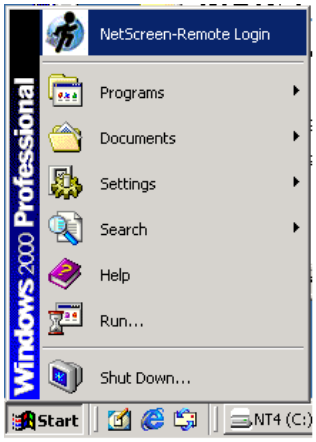


Figure 2-1 Launching NetScreen-Remote Login

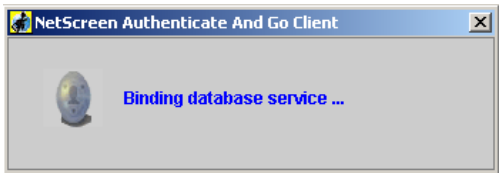


Figure 2-2 Initial Login Access Display

2. At the login screen, enter your user name and password.

If you do not know your user name and password, ask your Network Administrator for this information.

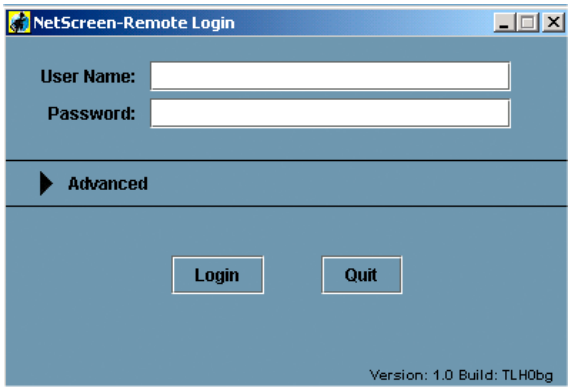


Figure 2-3 User Login

3. To select a predefined user profile, click **Advanced** and select the desired profile from the **Profile** box.

If multiple profiles are configured, these will be listed within the **Profile** box.

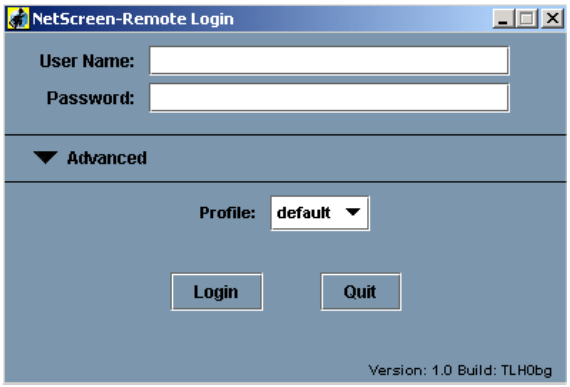


Figure 2-4 User Login Advanced

4. Click **Login**.

NetScreen-Remote authenticates you to the NetScreen-Global PRO management system.

Figure 2-5 Login Progress

5. During authentication, NetScreen-Remote may attempt to download new files from the NetScreen-Global PRO management system. This may periodically require you to re-start the NetScreen-Remote application to load updated files. If prompted to restart NetScreen-Remote, choose to re-start the application.

6. If NetScreen-Remote is configured to use a smart card, a prompt appears during user authentication prompting you to insert your smart card. Insert your smart card into the smart-card reader, if prompted. Once your card is inserted, you are prompted to enter your PIN. Enter your PIN and click **OK** to complete the login process.

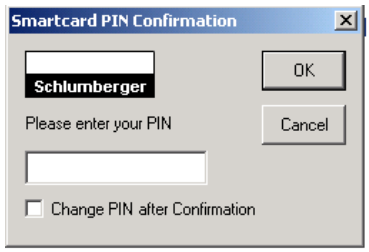


Figure 2-6 Smart-Card PIN Confirmation

Upon completion of the login process, the NetScreen-Remote Login icon appears in the bottom right of the screen:

LOGGING OUT OF A VPN

A user can log out of NetScreen-Remote by choosing the logoff button in the maximized application window. This will disconnect all VPN sessions and purge the security policy from your computer. Until you login again, you will not have access to your VPN resources.

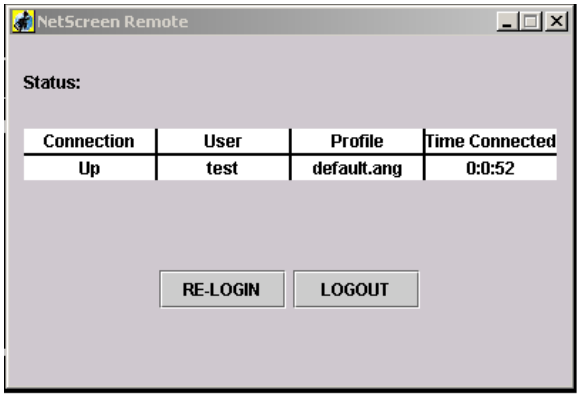


Figure 2-7 NetScreen-Remote Status Window

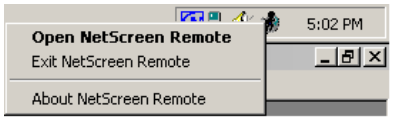


Figure 2-8 Exiting NetScreen-Remote

Alternatively, you may click the NetScreen-Remote icon within the taskbar and then click **Exit NetScreen Remote** to log out of NetScreen-Remote.

If you wish to login as another user, click **RE-LOGIN** on the NetScreen-Remote Status window.

3

Manually Loading Security Policies and Certificates

This chapter provides instruction on how to manually load security policies and certificates onto NetScreen-Remote. The following information is covered within this chapter:

- Manually Loading Security Policies
- Manually Loading Certificates
- Verifying Certificates

For more information about security policies and certificates, see the *NetScreen-Remote Security Client Administrator's Guide.* This administrator's guide covers these topics in greater detail.

MANUALLY LOADING SECURITY POLICIES

If you are not using NetScreen-Remote in a managed environment, or you do not have a NetScreen-Global PRO management system, it may be necessary to periodically install new security policies onto your system. In some circumstances, the Network Administrator distributes a default VPN configuration with the NetScreen-Remote software that includes a default security policy. During the installation of NetScreen-Remote, the default security policy is installed on your system and there is no need for you do anything further. The VPN configuration is permanently stored on your system, and you are able to access VPN resources transparently on demand without using NetScreen-Remote Login. However, if your Network Administrator has not provided a default security policy, or that policy has changed over time, it will be necessary to manually load the security policy. Security policies are distributed as regular files with *.SPD extensions.

Prior to loading security policies onto your computer, back up your existing security policy. Then proceed with loading your new security policies.

Backing up Security Policies

Loading a new security policy onto NetScreen-Remote will overwrite any existing security policy you may already have. Thus, back up your existing security policies prior to loading new security policies.

To back up 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 3-1 Export Security Policy

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

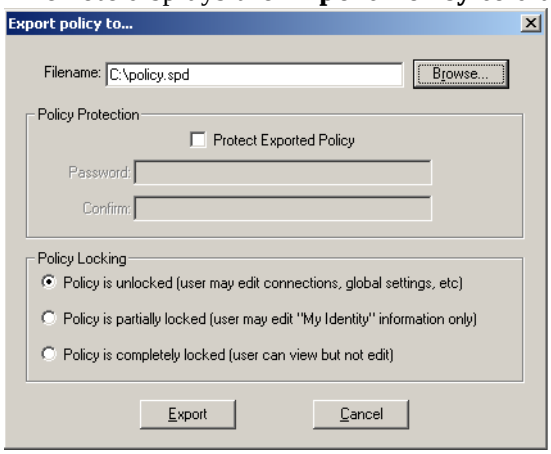


Figure 3-2 Export Policy To dialog box

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.

6. When you complete filling out this dialog box, click the Export button.

The **Save Existing Policy to** dialog box appears.

7. Locate a suitable location to save the file, name the file, and then click **save**.
8. On the **File** menu, click **Exit** to close the NetScreen-Remote Security Policy Editor.

You have completed saving your existing security policy.

Loading Security Policies

To load a security policy onto your computer:

1. Locate the security policy files on your computer.

The Security policies are distributed as regular files with *.SPD extensions.

2. Double-click a security policy file.

A message appears asking if you are sure you want to import the security policy to a given file destination.

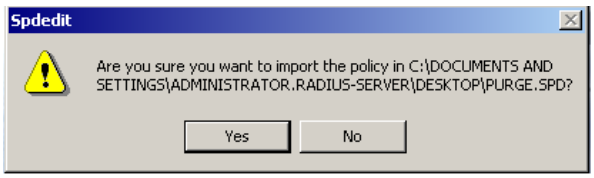


Figure 3-3 Loading a Security Policy

3. Click **Yes** to load the security policy.

The security policy is loaded onto your computer.

MANUALLY LOADING CERTIFICATES

If you are using a certificate-based VPN and do not already have a CA Certificate and a personal certificate loaded onto your system, it is necessary to load them onto your system prior to using NetScreen-Remote. In most circumstances you will need to load both a CA Certificate and a personal certificate onto NetScreen-Remote. Your Network Administrator should be able to provide you with these certificate files or instructions on how to download these certificates.

If you will be using a smart card, your personal certificate is loaded onto your card, and it may not be necessary to load a personal certificate, although you will still need a valid CA Certificate loaded onto your system.

To load CA Certificates or personal certificates onto your computer:

1. Locate the certificates on your computer.
2. Double-click the certificate file you want to load.

The **Certificate** dialog box appears with the certificate's information displayed in the **General** tab.

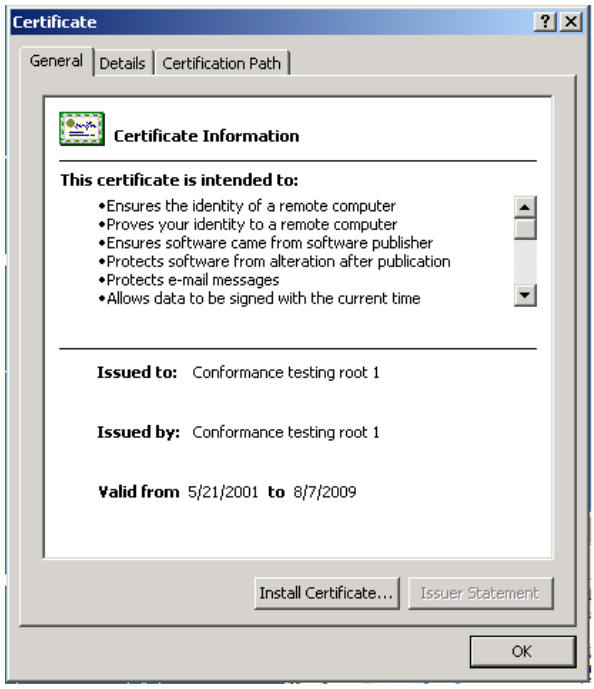


Figure 3-4 Loading Certificate

3. Click **Install Certificate,** and then click **OK** to load the certificate file.

You have completed loading the certificate file onto your computer. Repeat this procedure for each certificate you want to load onto your computer.

VERIFYING CERTIFICATES

After you load a CA and personal certificate on your computer, verify that it is a valid certificate with the Certificate Manager included with NetScreen-Remote.

To verify a CA or personal certificate is valid:

1. Click the NetScreen-Remote icon in the task bar to access the Certificate Manager.

The **NetScreen-Remote** menu appears.

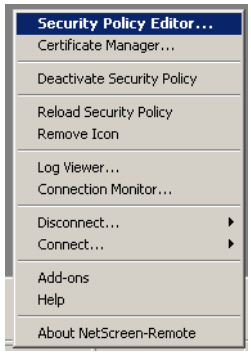


Figure 3-5 NetScreen-Remote Taskbar Menu

2. Click **Certificate Manager**.

The **Certificate Manager** dialog box appears. A list of your personal certificates with their associated descriptions display in the **My Certificates** tab. To verify a CA certificate, click on the **CA Certificates** tab.

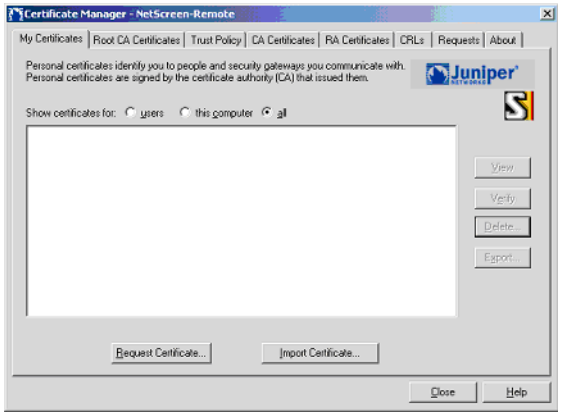


Figure 3-6 Certificate Manager

3. Select a certificate from the list, and then click **Verify**.

A message displays. If the message that displays indicates the certificate is valid, your certificate can be successfully read by the NetScreen-Remote software.

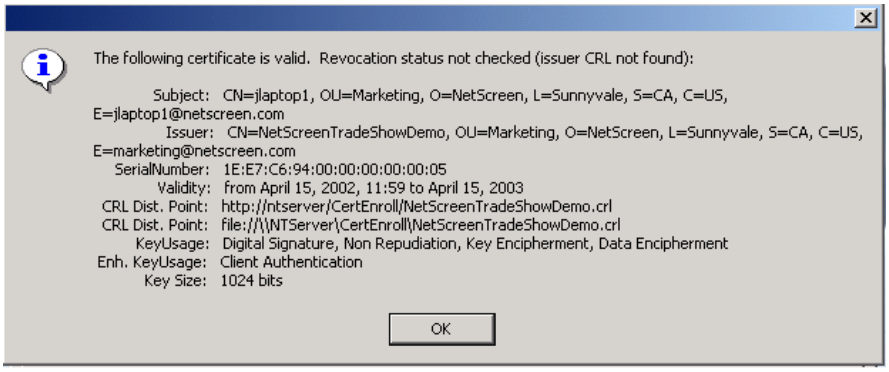


Figure 3-7 Valid Certificate

If the message that displays indicates a failure, your certificate is not valid. The failure occurred because the certificate cannot be read properly, it has expired, or it has been revoked. Contact your Network Administrator to obtain a new certificate and then repeat the procedures in the section Manually Loading Certificates.

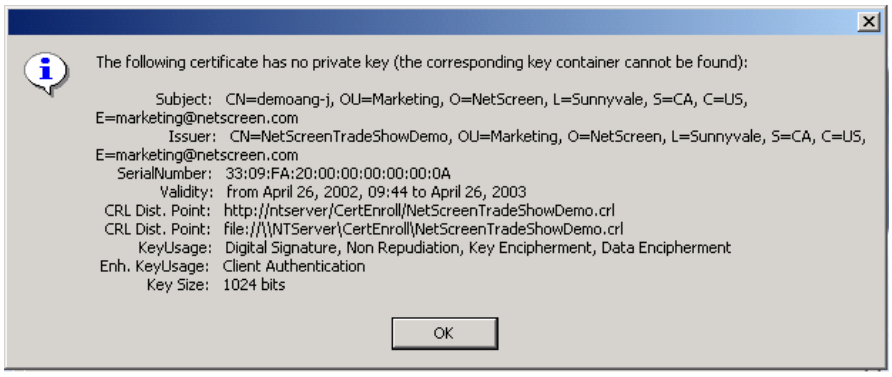


Figure 3-8 Certificate Not Valid

You have completed verifying whether your certificate is valid.

4

Configuring and Connecting to an L2TP VPN Connection

This chapter covers the following information:

CONFIGURING L2TP CONNECTION

If you will be connecting to a Layer Two Tunneling Protocol (L2TP) VPN Connection, you must configure the L2TP connection through your Microsoft Dial-Up Networking. Prior to configuring the L2TP connection, configure NetScreen-Remote for IPSec Transport mode connection to the NetScreen device.

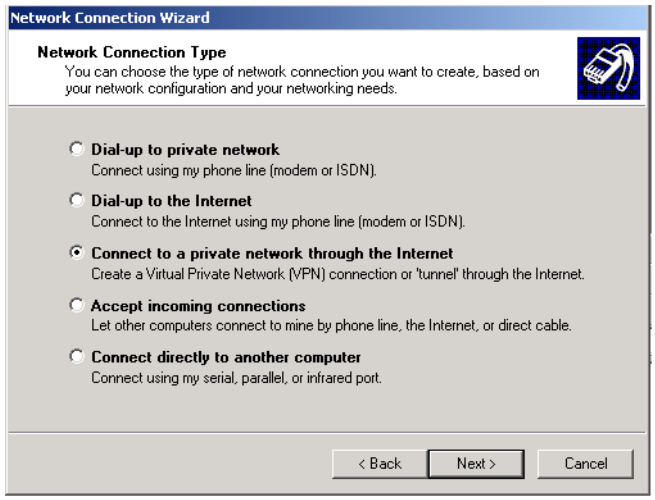
Note: The following procedure provides instruction on how to set up L2TP VPN connections on Windows 2000. A similar procedure is used to set up L2TP connections for Windows 95B, 98, ME, NT 4.0 and XP SP2.

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.



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.

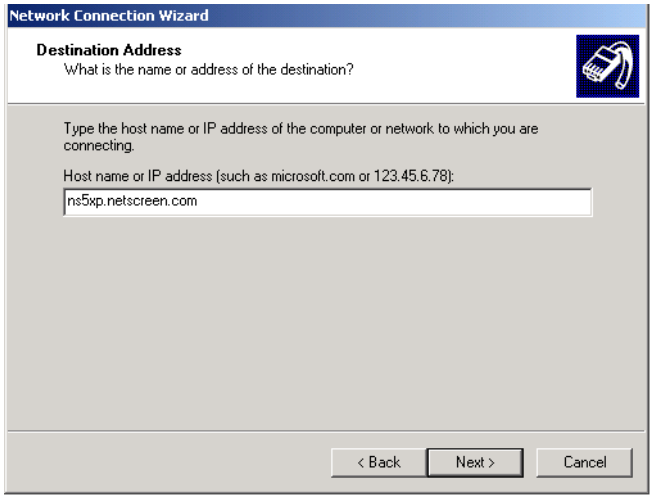


Figure 4-1 Destination Address dialog box

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.

Figure 4-2 Connect Virtual Private Connection

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

Your L2TP VPN connection will be established.

5

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

Index