

NetScreen Release Notes

Product: NetScreen-Remote

Version: NetScreen-Remote 8.3

Release Status: Release

Part Number: 093-1116-000, Rev. A

Date: 12-8-03

Contents

1. ["Version Summary on page 2](#)
2. ["New Features and Enhancements on page 2](#)
 - 2.1 ["New Features in NetScreen-Remote 8.3 on page 2](#)
 - 2.2 ["New Features in NetScreen-Remote 8.2 on page 2](#)
 - 2.3 ["New Features in NetScreen-Remote 8.1 on page 3](#)
 - 2.4 ["New Features in NetScreen-Remote 8.0 on page 4](#)
3. ["Changes to Default Behavior on page 5](#)
4. ["Addressed Issues on page 5](#)
 - 4.1 ["Addressed Issues in NetScreen-Remote 8.3 on page 5](#)
 - 4.2 ["Addressed Issues from NetScreen-Remote 8.2 on page 7](#)
 - 4.3 ["Addressed Issues from NetScreen-Remote 8.0r1 on page 11](#)
5. ["Known Issues on page 11](#)
 - 5.1 ["Compatibility Issues in NetScreen-Remote 8.3 on page 11](#)
 - 5.1.1 ["Platform Compatibility on page 12](#)
 - 5.1.2 ["Common Compatibility and Configuration Issues on page 13](#)
 - 5.1.3 ["Common Compatibility Notes on page 14](#)
 - 5.2 ["Known Issues from NetScreen-Remote 8.3 on page 17](#)
 - 5.2.1 ["Known Issues from NetScreen-Remote 8.2 on page 19](#)
6. ["Getting Help on page 22](#)

1. Version Summary

NetScreen-Remote 8.3 is a the latest release version of NetScreen-Remote, a Virtual Private Network remote access client for connecting client PCs or laptops to any IP network through a VPN connection to a NetScreen device or other secure communications with other devices running NetScreen-Remote. It supports industry-standard IPSec, L2TP, and IKE protocols for tunneling and transport layer security as well as key exchange. It is ideal for road warrior access on laptops to networks from remote locations and supports any Internet ISP through modem, DSL, or wireless access-point.

The NetScreen-Remote Installation Guide and NetScreen-Remote Administrator Guide describe the configuration and setup of the NetScreen Remote Security Client.

2. New Features and Enhancements

The following sections provide an overview of new features that were introduced in each version of NetScreen-Remote as well as existing features that were enhanced.

2.1 New Features in NetScreen-Remote 8.3

NetScreen-Remote 8.3 is a maintenance release.

2.2 New Features in NetScreen-Remote 8.2

The following are new features introduced in NetScreen-Remote 8.2.

- **Added support for AES Encryption** - 8.2 provides support for AES-128, AES-192 and AES-256 for Phase I and Phase II. (Note this feature cannot be managed by NetScreen-Global PRO)
- **New Sygate Personal Firewall code** - This version includes build 1152s of Sygate Security Agent (Sygate Personal Firewall SE) which addresses the following issues:
 - **NetBIOS Protection now user-selectable** - The NetBIOS Protection options in the Personal Firewall are now user-selectable. The user may disable NetBIOS Protection if desired or if they encounter problems mapping network drives over a VPN.

- **Personal Firewall cannot be bypassed** - An attack was reported where an attacker could potentially bypass any personal firewall software and execute malicious code. This affected NetScreen-Remote 8.3 and previous versions, as well as other 3rd party Personal Firewall products. This release of the Personal Firewall contains fixes which prevent a thread from being created, which could potentially execute malicious code.

2.3 New Features in NetScreen-Remote 8.1

The following are new features introduced in NetScreen-Remote Client 8.1.

- **Manual Connection Button:** Normally, the client automatically initiates a VPN connection when traffic matches a defined Remote Party. Customers have asked for a more “user oriented” session establishment where the user selects a “connect to...” button to initiate a VPN connection to the gateway. New “connect to...” and “disconnect from ...” buttons are being added to the system tray icon. The manual connection feature also provides an option to inhibit automatic connections, providing more intuitive operation for users that have a direct connection to their corporate network while in the office and use a VPN connection for remote access to the same network.
- **URL Policy Retrieval:** URL Policy Retrieval allows the user to configure the client with a Policy URL. The policy that is in the web address of a policy file which can be retrieved automatically via HTTP by the client. The policy file is retrieved periodically at an interval determined by a registry setting.
- **NAT-T Draft 2 Support:** This release adds support for the latest IETF NAT Traversal (NAT-T) draft. Draft 2 enhances the ability of IPSec sessions to transit IPSec-aware NAT devices, such as those commonly found in SOHO installations. This release maintains backward compatibility with NAT-T draft 1 implementations.
- **Maintenance Release:** Bug fixes as listed in the Addressed Issues section.

2.4 New Features in NetScreen-Remote 8.0

The following are new features introduced in NetScreen-Remote 8.0.

- **Extended Authentication (XAUTH)** – NetScreen-Remote 8.0 provides support for extended authentication that allows NetScreen devices to integrate with legacy authentication services (RADIUS, LDAP, SecureID, NT Domain, Active Directory) and prompt the user for passwords or token credentials. *This feature must be used with NetScreen ScreenOS 4.0 or later for full compatibility.*
- **Optional Posture Assessment** – When NetScreen-Remote is used with the NetScreen-Global PRO line of Security management systems, the Global PRO administrator may enforce posture assessment on the NetScreen-Remote Security Client. If the personal firewall software is not installed, not functioning or has been compromised in any way, the VPN policies are not downloaded to the client, eliminating the possibility of compromised machines gaining VPN access.
- **Optional Policy Purge** – When used with the NetScreen-Global PRO line of Security management systems, VPN policies are purged from the NetScreen-Remote system upon logout from the VPN - this behavior is now optional in this release and is enforced by the NetScreen-Global PRO administrator.
- **Improved Windows XP Support** – NetScreen-Remote contains drivers signed by Microsoft that are used during installation. As a result the install process on Windows XP machines has been improved. This version now also supports Windows XP Home Edition in addition to Windows XP Professional.
- **File-based IPSec Logging** – IPSec logging can now be file-based. The feature is disabled by default as it is intended for troubleshooting purposes. The feature can be enabled in the Security Policy Editor-> Options->Global Options-> Enable IPSec Logging. The logging file, isakmp.log, is located in NetScreen-Remote's Program files home directory. The log file default max size is 100K which can be changed by adding a LOGMAXFILEKB registry to NetScreen-Remote's ACL key. Default max size is checked when the IPSEC logging function is enabled/disabled or when the machine is re-booted (i.e. the log file if larger then 1LOGMAXFILEKB will be cleared).

3. Changes to Default Behavior

There are no changes to the default behavior of NetScreen-Remote in this release.

4. Addressed Issues

The following sections identify which major bugs have been fixed in each release of NetScreen-Remote. If there is no subsection for a particular NetScreen-Remote release, that release included no addressed issues.

4.1 Addressed Issues in NetScreen-Remote 8.3

- **QA018746** – On Windows NT, the virtual adapter connector may have been created with PPTP port spec.
- **QA004752** – Some Maximum Transmission Unit (MTU) settings would result in packet loss on the NetScreen-Remote device.
- **QA004751** – Multiple quick modes during a virtual adapter session with the WINS configuration did not work properly.
- **QA004750** – The NetScreen-Remote client did not handle mode configuration collisions correctly on Windows XP.
- **QA004749** – The NetScreen-Remote client popup menu sometimes was missing lower manual connection.
- **QA004748** – The NetScreen-Remote client packet log sometimes contained extraneous characters.
- **QA004747** – The NetScreen-Remote client did not guard against attribute payload overflow.
- **QA004746** – The NetScreen-Remote client did not guard against buffer overflow in HASH_R processing.
- **QA004745** – The NetScreen-Remote client did not guard for NAT-D payload overflow.
- **7018** – When configuring a VPN resource with a service group in Global PRO, when the software transmitted to the NetScreen-Remote environment that no services were configured.
- **5457** – The client loaded the wrong SPI number when proposals for AH and ESP were in the same policy.
- **5458** – The IPSecMon monitoring utility failed when retrieving policy or certificates.
- **5454** – The SPDEdit facility incorrectly chose the first certificate with the same label, regardless of the container ID.

- **5443** – The SPDedit Other Connection ID type when set to Any Gateway IP Address remained enabled after clearing the Connect Using checkbox.
- **5438** – You could not save any changes or add a remote gateway associated with a Ghost save and remote gateway buttons after importing an unlocked policy over a locked policy.
- **5367** – Auto-retrieval of an MSCEP certificate did not work.
- **5221** – The **vpn.exe** executable file causes a fatal application error when running **vpn.bat** from a command prompt.
- **5183** – The system was unable to release and renew IP addresses or renewals of DHCP leases,
- **4733** – Windows 2000 and Windows XP DNE MTU Adjust does not accommodate enough overhead for all connection types.
- **4721** – RSA Secure-ID Passcode was truncated for Secure ID.
- **4705** – The Secure All types of manual connections to the 2nd or 3rd connection tried to establish a connection to the first connection.
- **4704** – Windows 2000 and XP Net Login Error 5719 in event viewer caused single sign-on applications to fail.
- **4679** – CA certificates imported into the personal certificate store with Internet Explorer caused Certificate Manager to crash when opening the personal CA certificate.
- **4678** – Multiple XAUTH prompts were presented to the user when XAUTH was not completed.
- **4677** – Quick Mode started before the extended authentication process completed.
- **4676** – The interface detection mechanism failed on RAS devices introduced after the reboot.
- **4668** – The NSIadapssl32v30.dll dynamic link file included with the NetScreen-Remote client was not compatible with Sun or IPlanet 5.1 or later.
- **4667** – NetScreen-Remote clients using VRS (internal IP) with no virtual adapter could not pass fragmented UDP traffic.
- **4556** – The remote gateway connections were not recognized in manual connections.
- **4173** – TDES and DES with manual keys failed with all hash algorithm and generated the following error message:
Error importing outbound key entry.
- **4170** – In a remote party ID with the connection using setting checked, the wrong default ID types were listed.

- **4162** – You could not maintain a virtual adapter while processing initial contact and while it was in responder mode.
- **4161** – NetScreen-Remote has eliminated residual active virtual adapters that have no SA.
- **4103** – You could not enter and save PSK on Windows XP.
- **4005** – NetScreen-Remote has a mechanism that prevents the creation of duplicate connection names.

4.2 Addressed Issues from NetScreen-Remote 8.2

- **5445** – Remote gateway failed when using Autocert and more than one certificate listed in SafeNet Certificate Manager.
- **5441** – Autocert with My ID set to IPV4 could lead to a misconfigured Filter Table Rules with an IP of all 0's and a mask of all 1's
- **5440** – Autocertificate with My ID set to IPV4 now only selects certificates with IPV4 information in it.
- **5437** – The Secure All and Secure Other Connections environments displayed the manual connect option when first selected.
- **5435** – Virtual adapter settings were not retained when they were moved within various screens in the policy editor without an administrator first saving the settings.
- **5436** – Unknown ID type reported in the log environment when switching connection from secure to block and back to secure.
- **5434** – A certificate-based VPN PM registration did not work.
- **5428** – The sub Certificate Authority Certificate Retrieval in Certificate Manager only retrieves a portion of a certificate string.
- **5423** – Log reports DNS, ALT DNS were generated and the Private DNS was assigned after the virtual adapter was created.
- **5420** – The system improperly displayed messages when failing over to a remote gateway using a hostname.
- **5419** – The SPDedit Gateway IP address box remained enabled after you unchecked the Connect Using checkbox.
- **5411** – When attempting to save a pre-shared key on a Windows XP platform, the NetScreen-Remote device displayed the following message:
Can not enter and save Pre-Shared Key on XP, error encrypting PSK.

- **5404** – You could not retrieve a CA certificate from Certificate Manager when logged on as a regular Windows 2000 and Windows NT user. Placement of certificate in local device store is now a configurable option in the Certificate Manager.
- **5402** – Default settings were not changed for a new connection to 3DES / SHA1 / DH Group 2.
- **5437** – The Secure All and Secure Other Connections environments displayed the manual connect option when first selected.
- **5435** – Virtual adapter settings were not retained when they were moved within various screens in the policy editor without an administrator first saving the settings.
- **5419** – The SPDedit Gateway IP address box remained enabled after you unchecked the Connect Using checkbox.
- **5400** – The system did not recognize insertion/removal of the remote access (RAS) devices.
- **5386** – The system did not search all root stores for a CRL if none are located in the specified root certificate store.
- **5385** – The client did not properly enforce the validation of the ID specified in the client and the one sent from the gateway when using certificates.
- **5384** – Realtek 8139 NIC did not get responses to 1460 byte pings.
- **5383** – When using an operating system developed in the German language, the NetScreen-Remote device displayed the following message:

```
Can not use the SafeNet Virtual Adapter on German OSs
```
- **5359** – The system was unable to locate the **vapnt.sys** file during the installation.
- **5322** – The "route addition failure" message occurred when failing over to a remote gateway when the primary Gateway did not require a route addition.
- **5321** – Second key requests were generated when failing over to a remote gateway/subnetwork connection creating a dynamic entry with a mask of all ones.
- **5320** – Proper routes were not added to connections using virtual adapter and remote gateway when recovering back to the primary gateway from a remote gateway connection using a virtual adapter.
- **5315** – An SCEP request failed and Certificate Manager would close when logged on as a regular user on Windows NT, Windows 2000 and Windows XP.
- **5229** – The connection failed over to the remote gateway when the hostname was not found.

- **5212** – Certification Revocation List (CRL) imports failed to import on W2K when you logged on as a regular user.
- **5209** – Custom installs were not supported on systems that did not have a C: drive.
- **5208** – Secure Gateway Tunnel information was lost when connections were set to blocked and then back to secure.
- **5202** – CERT Vulnerability VU#287771: Large number of payloads and a large SPI value forced the system to fail. The failure ID was IREIKE.
- **5185** – Entering a connection name with 93 characters or more caused the policy editor not to open and caused invalid page faults when running on the Windows 98 platform.
- **5165** – Using the AOL dialup environment, the virtual adapter connections failed with errors because they were unable to determine a tunnel gateway.
- **5158** – Users without administrator privileges could not open the policy editor on non-English versions of Windows 2000.
- **5139** – The virtual adapter failed to build if the DUN connection was configured to only be used by one person.
- **5137** – If Microsoft DUN was configured with an alternate phone number, the virtual adapter would not be built.
- **5104** – The remote gateway name field did not limit the amount of characters entered and caused SPDEdit to crash when saving the remote gateway with large names.
- **4992** – Viewing the log debug message **recv fail rlen -1** resulted in the user being unable to establish a VPN connection over a modem.
- **4966** – The system could not map drives to Windows NT or Windows 2000 servers on Windows XP and Windows 2000 clients using the virtual adapter.
- **4964** – Users had full control of Certificate Manager with fully locked policies.
- **4962** – The system could not export PKCS12 certificates to the default path **C:\Temp\Cert.p12** if the **Temp** directory did not exist.
- **4943** – A connection displayed incorrectly when changing from a secure connection using gateway to the Blocked setting.
- **4936** – Connections with the gateway hostname and ID type **Any** used a previously entered gateway IP address for session establishment.
- **4935** – No attempt was made to resolve the gateway hostname if the ID type was set to the **Any** setting and you selected the gateway hostname.
- **4929** – On Windows XP, importing a PKCS12 file from the command line failed.

- **4892** – Internet PPPoE client did not work with NetScreen-Remote when using the virtual adapter.
- **4857** – The **CMD.exe** executable program failed at times when working with SPDedit on systems that had their policy loading from a floppy disk.
- **4797** – If a policy was locked and you accessed the global policy settings, the SPDedit facility failed.
- **4791** – The system could not initiate Aggressive Mode when set to Autocert.
- **4735** – IKE traffic would not occur after a policy was imported through the GUI.
- **4734** – A secure gateway tunnel domain name or IP address changed when a connection was set to Blocked and then changed back to Secure.
- **4711** – When you edited the IP address in the right control region and then changed connections, the system lost edits.
- **4672** – Session establishment with the virtual adapter failed on initial use.
- **3972** – An L2TP connection mislabeled the adapter in Windows 2000 and Windows ME.
- **5458** – The IPSecMon monitoring utility failed when retrieving policy or certificates.
- **5457** – The client loaded the wrong SPI number when proposals for AH and ESP were in the same policy.
- **5454** – The SPDEdit facility incorrectly chose the first certificate with the same label, regardless of the container ID.
- **5443** – The SPDedit Other Connection ID type when set to Any Gateway IP Address remained enabled after clearing the Connect Using checkbox.
- **5438** – You could not save any changes or add a remote gateway associated with a Ghost save and remote gateway buttons after importing an unlocked policy over a locked policy.
- **5367** – Auto-retrieval of an MSCEP certificate did not work.
- **5221** – The VPN.exe executable file causes a fatal application error when running VPN.bat from a command prompt.
- **5183** – The system was unable to release and renew IP addresses or renewals of DHCP leases.
- **4892** – An Enternet PPPoE client did not work with a NetScreen-Remote client when using the virtual adapter.
- **4858** – Prompts for Double and Triple XAUTH occurred on connections that failed over to a remote gateway.

4.3 Addressed Issues from NetScreen-Remote 8.0r1

- **4879** – FTP puts and large pings failed with native Windows XP PPPoE broadband connections.
- **4852** – You needed to disable the Windows XP firewall for IKE to work since the key request from the driver to the service was blocked.
- **4849** – You needed to load a driver to improve performance of secure domain logon.
- **4848** – You could not select the option to install an L2TP tunnel over a virtual adapter on Windows 98 systems without the ndiswan utility.
- **4695** – If the Windows 9x platform device was configured with a static DNS address (i.e. not through DHCP) and an IPSec session with the virtual adapter was established, the DNS assignment through the virtual adapter did not take effect.
- **4634** – Warning messages during a client installation about the NetScreen-Remote virtual adapter and DNE were not signed by Microsoft.
- **4593** – The IFconfig utility included with NetScreen-Remote was not compatible with Windows XP Pro and Windows XP Home.
- **4460** – Help was in the "always on top" state when not minimized. This state did not allow you to view system Help and configure the system simultaneously.

5. Known Issues

This section describes known issues with the current release.

- The first set of issues describes known compatibility issues with other products, including but not limited to specific NetScreen appliances, other versions of ScreenOS, Internet browsers, NetScreen management software and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.
- The second set describes deviations from intended product behavior as identified by NetScreen Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

5.1 Compatibility Issues in NetScreen-Remote 8.3

Below are the known compatibility issues at the time of this release. Whenever possible, a work-around (starting with "W/A:") has been provided for your convenience.

5.1.1 Platform Compatibility

- **Windows XP Internet Connection Firewall With Virtual Adapter** – You must configure on your virtual adapter a firewall with the Windows XP Internet Connection Firewall if the connection used to create a virtual adapter or the device is dropping packets.
- **Driver Signing Warnings on Windows XP with Security Patch MS02-50** – Earlier versions of the MS02-50 security patch on Windows XP caused unsigned driver messages when installing the NetScreen-Remote client.

W/A: Download the latest MS02-50 patch from the following page on the Microsoft web site:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-050.asp>

- **ScreenOS Compatibility** – It is highly recommended that you use this version of NetScreen-Remote in conjunction with ScreenOS 3.0r2 or later for full compatibility with all new features. If you do not plan on using some features full compatibility with previous versions of ScreenOS is supported. Below is a compatibility matrix of ScreenOS versions required to use certain features in NetScreen-Remote.

Feature	Available Platforms	NAT-Traversal	L2TP
ScreenOS 4.0.0r9	5XP/5XT/25/50/204/208/500/5000	Yes	Yes
ScreenOS 3.0.3r4	5XP/5XT/25/50/100/500	Yes	Yes
ScreenOS 3.1.0r9	204/208/500	Yes	Yes
ScreenOS 3.1.0r4	5200 Only	Yes	Yes
ScreenOS 2.6.1r8	5/5XP/10/100/500	No	Yes
ScreenOS 2.8.1r1	1000	No	No

- **Global PRO Compatibility** – If using VPN Policy Management, NetScreen-Global PRO or Global PRO Express version 3.0.1 or greater is required. This release is synchronized with Global-PRO 4.0r1 release, and will upgrade or downgrade automatically to other releases of Global-PRO.

- **Windows OS Compatibility** – This version of NetScreen-Remote has been tested and is compatible with Windows 95 (Version 4.00.950 B, 4.00.950C) with winsock2 DLL, Internet Explorer 4.0 or greater and DUN 1.3 Upgrade, Windows 98 (98, 98 SE), Windows NT 4.0 Workstation (SP4, SP5, SP6), Windows Me, Windows 2000 Professional, Windows XP Professional and Windows XP Home Edition. Due to non-Y2K compliance, the following versions are no longer tested or supported: Windows 95 (Version 4.00.950, 4.00.950a) and Windows NT 4.0 SP3 or earlier.

5.1.2 Common Compatibility and Configuration Issues

Please read [Section 1. “Version Summary”](#) in regards to recommended versions of ScreenOS and Windows OS for full compatibility with this version of NetScreen-Remote. This section contains common compatibility and configuration issues encountered as well as configuration requirements under certain circumstances.

- **Windows 95B Compatibility Issues** – Under certain circumstances NetScreen-Remote Login will not load on Windows 95B Machines; after a system reboot, the application loads properly.
- **File Clearing Issues** – Installation of NetScreen-Remote may not clear all files if installed in a non-default directory. You must manually delete the files after uninstalling in this environment.
- **PKCS7 Support Issues** – PKCS7 is not supported when used with Global PRO. PKCS7 Certificate Chains not supported. Also, PKCS7 must be used with Aggressive mode. When using standalone NetScreen-Remote (without Global-PRO Integration) clients must connect to NetScreen device using Aggressive mode. Main mode fails if using PKCS7 Certificate chains.
- **Hub and Spoke VPN Limitations** – If using Hub and Spoke VPNs with NetScreen-Remote 7, you must use L2TP Over IPSec. Native NetScreen-Remote IPSec does not support the Hub and Spoke VPN feature. Please refer to the product documentation for information on setting up L2TP Functionality with NetScreen-Remote.
- **TCP Ports Not Open to Global-PRO for NetScreen-Remote** – You must open the following ports on the Global-PRO appliance from NetScreen-Remote Clients: TCP/1099, TCP/11111, TCP 42496, TCP/11112. It is also recommended that you create a service-book entry for the protocols above.
- **NAT-Traversal Requires ScreenOS 3.0r2 or Later** – For full compatibility, it is recommended that you use NAT-Traversal with ScreenOS 3.0r2 or later. You must also enable the NetScreen device.

- **User Configured Incorrect DN field in Client's Certificate Request** – When creating a certificate-request on the NetScreen-Remote Client, it is important that IP Address, Email, FQDN and/or Distinguished Name defined in the client's certificate request matches how the user is identified in Global PRO. For example, if email identity johndoe@netscreen.com is used in Global PRO as a users IKE Identity, the client's certificate DN must contain this valid email address johndoe@netscreen.com - otherwise authentication fails.
- **User Configures Incorrect Date/Time Setting when using Certificates** – When creating a certificate request, it is important to verify the date/time of the machine requesting the certificate is valid. If the time of the machine is fast, then the time and date stamped on the certificate may not yet be valid. It is also important to verify time-zone information is correct for both NetScreen-Remote Clients and the NetScreen device.
- **Network Interface Card (NIC) Compatibility** – NetScreen-Remote should be compatible with all NDIS compliant Ethernet NICs (NICs tested for NetScreen-Remote). Only plug and play on Windows 95, 98, ME and 2000 is supported. Plug and play on notebook computers running Windows NT is not supported. Co-existence (i.e. encryption over the dial-up adapter) with Token Ring cards is supported.

5.1.3 Common Compatibility Notes

These compatibility items require the specified workaround to be performed for proper operation:

- **New Virtual Adapter features will not be updated for users performing an upgrade** – New routing information is not added to the existing Virtual Adapter connection in the Dialup Networking properties environment.
W/A: Delete any virtual adapter connections from the Dialup Networking environment. A new virtual adapter connection will be created on the next connection that utilizes the virtual adapter with all of the new settings.
- **Automatic Certificate selection may not work in aggressive mode** – Since Aggressive Mode sends an ID payload in the first initiator packet, and no explicit certificate is selected, the session may fail. The client makes a best guess and selects the first certificate that meets the specified ID type (DN, e-mail, IP address, etc.). This certificate may or may not be a valid certificate.
W/A: Manually select the certificate when using Aggressive Mode or limit your certificates to one in NetScreen-Remote Certificate Manager.

- **NetScreen-Remote is incompatible with the AT&T Dialers VPN component** – The VPN component included with the AT&T dialer is incompatible with DNE components of NetScreen-Remote (all versions).

W/A: Uncheck the VPN component during the installation of the AT&T dialer

- **Sony PCG-SRX77P laptop with an integrated modem and NIC** – NetScreen-Remote will not install properly on Sony PCG-SRX77P laptop PCs with the on-board network interface card enabled.

W/A: To use NetScreen-Remote on this device, disable the onboard network interface card and use an external network interface card.

- **Dell Laptop with PCMCIA - INTEL PRO-100 SR Combo Mobile Adapter** – NetScreen-Remote will not install properly on Dell laptop PCs with the PCMCIA Intel PRO 100-SR Combo network interface card.

W/A: You must use another network interface card in these systems.

- **Windows 95 systems may crash while loading NetScreen-Remote Login** – On some Windows 95 systems the Authenticate and Go NetScreen-Remote Login application will randomly exit with an error message until the system is rebooted.

W/A: Reboot your windows 95 system.

- **Point-to-Point Protocol (PPPoE) software for DSL connections must be installed and operational before NetScreen-Remote is installed** – The installation of PPPoE software on a system that has NetScreen-Remote installed will remove some network components.

W/A: If the system does not have NetScreen-Remote installed, install the PPPoE software first, and then install NetScreen-Remote. If the system already has NetScreen-Remote installed, uninstall NetScreen-Remote, choose the Save Policy and Certificates option, and then after rebooting, install the PPPoE software. As a last step, reinstall NetScreen-Remote.

- **DNE and Microsoft's Internet Connection Sharing for Windows 98 Second edition are incompatible** – If you attempt to install DNE over ICS or vice versa, a dialog displays and DNE will not install, or be automatically uninstalled. To check for ICS, look for the following key:

HKEY_LOCAL_MACHINE\Enum\Network\ICSHAREP

W/A: If this key is present, inform the user to remove ICS and try the installation again.

- **3Com Smart Agent Software Compatibility** – You cannot install NetScreen-Remote properly if 3Com's Smart Agent software is loaded on the device before installing NetScreen-Remote.

W/A: Smart Agent software must be installed after NetScreen-Remote.

- **Windows NT Plug and Play Drivers** – Laptops running NT where the manufacturer has tried to create "plug and play" support through a custom utility may experience problems. Windows NT does not support plug and play functionality and DNE cannot work with these custom, non-standard, non-NDIS-compliant utilities. NetScreen-Remote supports plug and play functionality on Windows 95 and Windows 98.

W/A: In the case of the laptop utilities, you must disable the utility and get the latest network interface card driver from the vendor (not the special pre-packaged one that the laptop vendor supplies with the utility).

- **Windows NT disabled protocols are enabled when DNE is installed** – On Windows NT 4.0 only, if you have disabled protocols, after they are installed, the protocols become enabled.

W/A: Disable the protocols through the Network Control panel or remove the protocols.

- **NetScreen-Remote is incompatible with Earthlink software** – Incompatibility with Earthlink Internet Software version 5.02.

W/A: You still can access Earthlink via a standard dial-up networking configuration. To access this environment, uninstall the Earthlink software. Earthlink Technical Support has been made aware of the situation and can assist in setting up a standard dial-up configuration for access to Earthlink.

- **On 95/98/ME, the Entegra USB has problems with suspend/standby** – The Entegra USB has problems when returning from suspend mode in that the interface is not always present.

W/A: Unplug the adapter and plug it back in.

- **AOL 6.0 Compatibility** – AOL6.0 software has installation problems on Windows 95/98/SE/ME platforms with DNE. The AOL installation continuously reinstall TCP and ask to be restarted. To work around this problem, boot into safe mode, remove DNE, and continue on with the AOL installation. After AOL is installed, reinstall DNE. AOL will still ask to be restarted on every startup. Select 'No' and AOL will work properly.

W/A: Upgrade to AOL 7.0. On Windows XP using native XP PPPoE connections a repair of the NetScreen-Remote client from Add/Remove Programs is required if an AOL 7.0 upgrade is performed with the NetScreen-Remote client already installed. The repair option from Add/Remove programs for the NetScreen-Remote client will correct the PPPoE settings that AOL overwrites.

5.2 Known Issues from NetScreen-Remote 8.3

The following are known deficiencies in features at the time of this release. Whenever possible, a workaround is suggested following the description of the problem. Workaround information starts with "W/A:." If there is no subsection for a particular ScreenOS release, no new known issues were identified for that release.

- **15456** – When running NetScreen-Remote over the Microsoft Windows 98 platform, If you enable the Phase 2 Rekey feature on the NetScreen device and if the Phase 1 modes of the NetScreen device and NetScreen remote client do not match, the NetScreen Remote software can cause an error.
- **15391** – When you set the tunnel using the redundant gateway, and you try to disconnect a tunnel in the gateway, the disconnection process may fail. NetScreen-Remote software displays the following message:

Unrecognized connection name.

W/A: Disconnect all tunnels to disconnect the tunnel.

- **15108** – If you configure a tunnel with a protocol set to UDP and the port set to TFTP traffic, the TFTP file transfer fails. NetScreen-Remote software displays the following message:

Inbound packet failed validation.

- **15068** – When you configure an L2TP over IPSec tunnel with the SA Lifetimes feature configured, the device drops packets after the expiration of the SA Lifetimes setting. The packet loss occurs because the client appears to be sending unencrypted Phase 2 (Quick Mode) packets.
- **15066** – In an instance where you have enabled a Phase II Rekey setting on the NetScreen device with the Phase 1 mode on the NetScreen device and no remote client, the client can go into an inoperable state where it cannot connect or disconnect.

W/A: Use the **unset zone zone block** command to remove intra-zone traffic blocking.

- **14679** – When you have two IKE proposals and you try to remove the first proposal, NetScreen-Remote software removes the proposal, but does not refresh the status on the screen.

W/A: You need to click on another icon on the left side of the NetScreen-Remote IKE Proposal dialog box. When you refresh the dialog box, NetScreen-Remote indicates the software removed the proposal.

The following are known issues from the SafeNet known issues documentation.

- **QA018812** – Windows XP logoff causes intermittent **ifcfg.exe** application errors. When logging off on Windows XP, you may intermittently receive application errors associated with the interface configuration **ifcfg.exe** executable file.
- **5446** – If logged on as a Non Administrator, the Import Personal Certification dialog box remains open with no prompt or error message after attempting to place the certificate in the local device store due to the check box.
- **5444** – If logged on as a non-administrator, the Import Personal Certificate window remains open with no prompt or error message after attempting to place the certificate in the local device store, which is the default setting in the Advanced Properties environment.
- **5395** – The route adding operation fails when using the virtual adapter and both peers undergo a Network Address Translation (NAT) operation and the private IP address on both networks are the same. In an environment where a NAT operation has occurred, if both private networks have the same address space, the phase 1 completes as expected. But when the route adding process occurs, it fails with error code 0000003A.
- **5318** – The logging facility reports an error associated with an Internet interface on connections that have remote gateways specified. The message displayed is:

Error updating filter record

- **5317** – The manual connection on Windows 9x platforms to a remote subnetwork (or range) specified with an address, reports a failure with Request Local Address functions. This problem is because Windows 9x does not generate traffic to such addresses.
- **4933** – The NetScreen-Remote device fails when trying to map a drive over a secure Point-to-Point-Protocol-Over-Ethernet (PPPoE). connection may require a system restart.

- **4687** – When attempting to create a dialup virtual adapter session with only one dialup adapter present on the NetScreen device, the IPSec SA completes even though the virtual adapter has not been added. The log shows a virtual interface constructed, but no message the virtual adapter added.
- **4657** – If you enter an underscore character in an SCEP request to SMC in the Common Name field, the Common Name may be corrupted after retrieval. The Common name retrieved is a # sign followed by a long numeric string.
- **4606** – When selecting the Device Connection Authentication and Remote Upgrade option for a NetScreen-Remote client installation on a Windows 2000 platform, the NetScreen device displays the following error message:

Digital Signature not Found for Crypto OSD Adapter

- **4506** – If the Internet interface in the MY ID section of a connection is set to a value other than Any, virtual adapter connections will fail with the following errors:
 - Failure finding or creating filter entry
 - Key download failed.
 - Error downloading key.
 - Failed loading the keys.

5.2.1 Known Issues from NetScreen-Remote 8.2

- **5446** – If logged on as Non-Admin the Import Personal Certificate window remains open with no prompt or error message after attempting to place the certificate in the local machine store due to the check box.

W/A: The check box for Place certificate in local machine store should be unchecked if logged on as non-admin when importing a personal certificate.

- **5444** – If logged on as Non-Admin the Import Personal Certificate window remains open with no prompt or error message after attempting to place the certificate in the local machine store, which is the default setting in advance properties.

W/A: Open the advance tab in the SCEP request form and uncheck the box to place certificate in local machine store if logged on as non-admin when importing a personal certificate.

- **5443** – SPDedit Other Connections Secure connection with Connect Using checked. Set "ID Type" to "Any" then uncheck the Connect Using checkbox. Save the policy then close and reopen the SPDedit utility. The Gateway IP Address remains enabled.

W/A: Check "Connect Using" set "ID type" to "IP Address" uncheck "Connect Using" and save the policy.

- **5438** – Unable to save policy from GUI after importing unlocked policy over a locked policy.

W/A: Close and reopen the SPDedit utility or close the SPDedit utility and save it at the prompt.

- **5395** – In an environment that has undergone a Network Address Translation (NAT) , if both private networks have the same address space (In the test it is 172.16.x.x 255.255.0.0), the phase 1 completes as expected however, when the mode config attributes are applied, the virtual adapter is created, but when the route add is issued (route add 10.100.200.254 mask 255.255.255.255 172.16.50.1) it fails with error code (0000003A).

W/A: If the virtual adapter is not used the connection works as expected. If the mode config address and the physical address are not on the same logical subnet, then the virtual adapter works as expected.

- **5318** – Log viewer reports "Error updating filter record" when specifying an Internet Interface on connections that have remote gateway's specified.

W/A: Do not specify an Internet Interface on connections that have remote gateway's, use the manual connect only option or specify "Any" for the Internet interface setting.

- **5317** – Manual connect on 9x platforms to a remote subnet (or range) specified with an address which is apparently (by address class) a subnet address will report a RequestLocalAddress failure. (This is because 9X will not generate traffic to such addresses.)

W/A: Initiate traffic to establish the tunnel such as a ping, WEB, Mail or FTP traffic.

- **5311** – Manual disconnects from a 2nd remote gateway reports unable to disconnect. Disconnecting from the 1st remote gateway works as expected.

W/A: Use the Disconnect All option from the tray icon when connections have failed over to a 2nd remote gateway.

- **4933** – System hangs when trying to map a drive over a secure PPPoE connection and may require a system restart.

W/A: The client will Map drives using RASPPPoE software. Free download link, <http://user.cs.tu-berlin.de/~normanb/#Download>

- **4858** – Double and Triple XAuth prompt occurs on connections that failover to a remote gateway with virtual adapter connections. Remaining key request from the primary Gateway trigger a second rekey to the failover Gateway when using virtual adapter.

W/A: Lower the retransmit interval from 15 seconds to 5 seconds in Global Policy Settings of Policy Editor.

- **4778** – Policy entry for SENDCERT_TYPE not honored by IKE. This allows the client to send a pkcs7 certificate chain even when the peer requests an x509 certificate.

W/A: Either the gateway should send a PKCS#7 certificate request or the gateway should be able to verify the chain itself, if it asks for a x509 certificate and the client responds with one.

- **4687** – When attempting a dial-up virtual adapter session with only one dial-up adapter present on the machine (i.e., improper configuration), the IPsec SA completes even though the virtual adapter is not added. The log shows a virtual interface constructed but no message for virtual adapter added.

W/A: Verify that two dial-up adapters are present on the machine before attempting dial-up virtual adapter sessions.

- **4679** – If a connection configured to use a selected certificate is changed to use preshared key, if the change is not saved and the focus is changed to another connection and then back to the MYID page, the ID has reverted back to the certificate. This does not happen when changing from Autocert to preshared key.

W/A: Save policy after making these changes or correct the connections MYID by editing or re-importing the policy if this condition occurs.

- **4506** – If the Internet Interface in the MY ID section of a connection is set to something other than Any, a virtual adapter connections will fail with the following: 15:26:52.998 Failure finding or creating filter entry 15:26:53.008 Failure finding or creating filter entry 15:26:53.008 Key download failed. 15:26:53.008 Error downloading key. 15:26:53.008 Failed loading the keys

W/A: Set the Internet Interface for the effective connection to Any or set virtual adapter to disabled.

- **3700** – When requesting an SCEP certificate, the CA accepts a valid request, but upon retrieval the Certificate Manager cannot decrypt the reply with his private key because the Private key was generated with a Microsoft Base CSP or an RSA Keon CSP on Win 95, 98, NT (works on Windows 2000). However, file based certificates can still be imported.

W/A: Install IE 5.5+ and the request and retrieval will work properly.

- **3641** – On Windows 2000 and Windows XP, the dial-up adapter is not available in the drop down list until the dial connection is established. The PPP adapter is not available in the drop down list under the MY IDENTITY - INTERFACES on Windows 2000 until the dial connection is made.

W/A: Once the dialup connection is made, you can choose the proper adapter. After you disconnect, the interface selection defaults back to ANY.

- **3531** – Sometimes on Windows 98 you are unable to import or export a PKCS#12 certificate/key file due to the following leftover registry key: HKEY_CURRENT_USER\Software\Microsoft\Cryptography\UserKeys\IRENULLKEY.

W/A: Delete the following registry key:
"HKEY_CURRENT_USER\Software\Microsoft\Cryptography\UserKeys\
" and delete the "IRENULLKEY."

6. Getting Help

For more information, please send e-mail to support@netscreen.com, or call us at 1-800-638-8296.

NetScreen occasionally provides maintenance releases for ScreenOS software. You can download software updates at www.netscreen.com/support.

For further assistance with NetScreen products, visit

www.netscreen.com/services/contact_tac

NetScreen occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your device with NetScreen at the following address:

www.netscreen.com/cso

Copyright © 2003 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10,

NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com

