NetScreen Release Notes Product: NetScreen-Remote
Version: Junip er Networks NetScreen-Remote 9.0
Release Status: Public
Part Number: 093-1474-000, Rev. G
Date: 12/12/2007

# 1. Contents

## 2. Version Summary

Juniper Networks NetScreen-Remote 8.8 is 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 Security Installation and Administrator Guides detail setup and configuration of NetScreen -Remote. For additional tips, see the NetScreen Knowledge Base located on the Juniper Networks customer support web page. Consult the online help document available through the NetScreen -Remote taskbar menu.

To go to the Juniper Networks and NetScreen-Remote support pages, use the following URLs:

http://www.juniper.net/support

http://nsremote-support.netscreen.com

## 2.1 Before Installing or Upgrading to this Version

When upgrading from an earlier version of the NetScreen -Remote VPN client, take these required steps before installing the client:

1. Uninstall the existing version through the Windows Control Panel **Add/Remove Programs** application.
2. Reboot the computer.

**Note**: The original Windows installation files may be required during installation, depending on the specific version of Windows and your configuration. Make sure that you have the CD-

ROMs or files available before you start the installation.

For more details on uninstalling the NetScreen-Remote application, please consult the Juniper Networks NetScreen-Remote 8.7 Administrators and Installation guides.

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

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

> **Note:** The original Windows installation files may be required during installation, depending on the specific version of Windows and your configuration. Make sure that you have the CDROMs or files available before you start the installation.

Consult the Known Limitations and Compatibility Issues sections in the Known Issues portion of this document for details on restrictions with NetScreen-Remote 9.0.

# 3. 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.

## 3.1 New Features and Enhancements in NetScreen-Remote 9.0

- 32-bit Vista Support
- Maintenance Release
- Added support for SafeNet Virtual Adapter (VA) on Microsoft Vista. This is the only change from the previous version.

## 3.2 New Features and Enhancements in NetScreen-Remote 8.8

There are no new features or enhancements in this release. This is a maintenance release.

## 3.3 New Features and Enhancements in NetScreen-Remote 8.7

There are no new features or enhancements in this release.

## 3.4 New Features and Enhancements in NetScreen-Remote 8.6

There are no new features or enhancements in this release.

## 3.5 New Features from NetScreen-Remote 8.5

The following are new features and enhancements introduced in NetScreen-Remote 8.5:

**Support for Windows XP SP2** – Note the following about NetScreen-Remote 8.5 support for Windows XP SP2:

The VPN client (NetScreen-Remote/SoftRemote) is now compatible with Windows XP SP2. NetScreen-Remote client versions 8.4 and earlier did not run correctly.

Sygate Personal Firewall is now compatible with Windows XP SP2.

**Note:** In Windows XP SP2 environments, this release of Sygate PFW

- does not write to the Windows Security Center
- does not disable the Windows Firewall

For additional information on setting up the security feature in a Windows XP SP2 environment, please consult the online support center at:

http://forums.sygate.com/vb/

**Support for Sygate Personal Firewall Version 5.5 Build 2710.** Online documentation is available at:

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

http://smb.sygate.com/support/documents/spf/SPF_WebHelp/SPF55.htm/

**New VPN Client Configuration Options.** The following new policy configuration options have been added to NetScreen-Remote.

**Note:** These options are not supported by the Juniper NetScreen Firewall/VPN devices. Please consult the Juniper NetScreen Firewall/VPN product information for the most current list of supported features.

- For the PFS Key group: Diffie-Hellman Group 14
- ESP Hash Algorithm: DES-MAC
- CSP Key size: 4096

## 3.6 New Features from NetScreen-Remote 8.4

The following are new features and enhancements introduced in NetScreen -Remote 8.4.

- Dead Peer Detection
- Enhanced Client Management
- Support Policy Based EMail ID Type
- Cached Certificate Request Submissions

It also contains the following SafeNet 10.3.3b4 components in it:

- SafeNet CSP Library (FIPS) v3.1.0b22
- SafeNet CSP Library (Non-FIPS) v3.0.1b22
- SafeNet Security Policy Editor v1.3.2 B02
- SafeNet Certificate Manager v1.3.2 B02
- Deterministic Networks (DNE) shim v2.20
- Layer 2 Tunneling Protocol (L2TP) v4.29

It also contains the following Sygate component in it:

- Sygate 5.5 Build v2634

## 3.7 New Features from NetScreen-Remote 8.3

NetScreen-Remote 8.3 is a maintenance release.

## 3.8 New Features from 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.

## 3.9 New Features from 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** – Allows the user to configure the client with aPolicy URL. The policy that is in the web address of a policy file which can beretrieved 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 IETFNAT 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.

## 3.10 New Features from 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 tointegrate with legacy authentication services (RADIUS, LDAP, SecureID, NT Domain, Active Directory) and prompt the user for passwords or tokencredentials. 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 compromisedmachines 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 nowoptional 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 XPProfessional.
- **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 maxsize 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).

# 4. Changes to Default Behavior

In NetScreen-Remote versions 8.4 and later, the Virtual Adapter Advanced TCP/IP properties option **use default gateway on remote network** is now checked by default. This may affect Internet access for the VPN user. For additionalinformation about Split Tunneling, please consult various Internet articles such as:

http://www.isaserver.org/tutorials/VPN Client Security Issues.html

# 5. 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.

## 5.1 Addressed Issues in NetScreen-Remote 9.0

- **QA032144** SoftRemote is not compatible with Windows Vista.
- **QA032116** Sub CA certificates causing issue with IKE authentication.
  Description:
  - 1. #defined REG_CACERTREQUESTS "CACERTREQUESTS" /* True to send CA cert request payloads, FALSE otherwise */
  - 2. #defined DEFAULT_REG_CACERTREQUESTS TRUE
- **QA032370** Sending Cert Requests for Intermediate CAs may lead to excessive number of request payloads.
- **QA032595** Log viewer reports “Too many timers” while there are numerous active tunnels and numerous tunnels are attempting to establish.
- **QA032900** Tunnel negotiation fails when aggressive mode is enabled and auto certificate selection is chosen.

## 5.2 Addressed Issues in NetScreen-Remote 8.8

- **QA023325** SECURE DOMAIN LOGON SHOULD HANDLE UNIQUE CERTIFICATE PIN NUMBERS

- **QA024279** ERROR MESSAGE "TOO MANY TIMERS" IN CLIENT LOG WHILE ESTABLISHING MULTIPLE TUNNELS CONCURRENTLY WITH IXVPN AT A RATE OF 2 TUNNELS AT A TIME OR MORE.
- **QA025065** MMC MAY NOT BE ABLE TO IMPORT CERTS EXPORTED BY CERTMGR
- **QA025268** RGW MAY CAUSE PH1 REUSE, LCLINSTMASK, LEGACY PEER, FW SETTING ISSUES
- **QA025270** IF A CONNECTION IS RE-USING PHASE-1 OF ANOTHER CONN, IT SHOULD MAKE SURE POLICY OPTIONS FOR BOTH CONNS MATCH EXACTLY
- **QA025272** FAILURE LOADING OR CREATING FILTER ENTRY MESSAGE IN LOG DISPLAY
- **QA025273** ONLY CONNECT MANUALLY IS PROCESSED, BUT NOT DISPLAYED IN SECURE ALL
- **QA025286** MANAGED POLICY PROCESSING DOESN'T DETECT CHANGES IN CEP SPECS
- **QA025383** CLIENT SHOULD RETURN SINGLE STATUS MSG (CONN_UP, DOWN ETC) FOR A CONN WITH MULTIPLE RGWS
- **QA025431** THE BEGINNING OF THE TEXT IN THE SECURE DOMAIN LOGON CERTIFICATE PIN PROMPT IS CUT OFF
- **QA025475** IN CASE OF SECURE DOMAIN LOGON WINDOWS LOGON PROCEEDS BEFORE CLIENT CONNECTION IS COMPLETED
- **QA025490** USER CANNOT COMPLETE SECURE DOMAIN LOGON AFTER ENTERING INCORRECT PIN WHEN USING AUTOMATIC CERTIFICATE SELECTION
- **QA025514** TEXT IS TRUNCATED IN ERROR MESSAGE GENERATED AFTER INCORRECT PIN IS ENTERED ON WINDOWS XP
- **QA025557** IREIKE CRASH
- **QA025656** CONNECT ON LOGON USING CERTPIN TAKES LONGER THAN NECESSARY TO LOGON EVEN WHEN (IN THE BACKGROUND) CLIENT HAS CONNECTED SUCCESFULLY TO REMOTE PARTY
- **QA025681** SECURE DOMAINLOGON DOES NOT WORK WITH CERTIFICATES NOT LOCATED ON SMART CARD
- **QA025689** CONNECTONLOGON FAILS WHEN USING CERTIFICATE ON SMART CARD
- **QA025793** DOUBLED PHASE 2 REKEY EXCHANGE AFTER PHASE 1 COLLISION
- **QA025804** INBOUND PH1 REKEYS MAY BE INAPPROPRIATELY DELETED
- **QA025791** GENERATED INVALID SPI NOTIFICATIONS HAVE THE SPI IN THE WRONG BYTE ORDER
- **QA025845** DATA-BASED KEY ANTICIPATION MAY STALL
- **QA025846** KEY ADDITION FOR A MANUAL CONNECTION IS NOT APPROPRIATE
- **QA025852** PHASE-2 REKEY DOES NOT WORK PROPERLY WHEN 2 OR MORE CONNS SHARE THE SAME PHASE-1
- **QA025856** IREIKE SERVICE MAY NOT ACCURATELY DETECT, CLEAR KEYS AT LOGOFF
- **QA025875** BAS-1: XAUTH PROMPTS SHOULD BE SQUELCHED WHILE USER IS

## 5.3 Addressed Issues in NetScreen-Remote 8.7

- **QA 024866** – CERT Advisory – PROTOS test-suite: C09-ISAKMP test suite causes IREIKE crash and buffer overflow.
- **QA025058** – IKE crash if DHCP address is released and renewed (with 'Secure All' connection) while XAuth prompt is open.
- **QA024486** – Cannot pass traffic when using null phase-2 encryption algorithm
- **QA024503** – Cannot pass traffic when using manual keys connections
- **QA023147** – IKE crashes after rekey when tunnel is established with NS25 VPN gateway
- **QA023326** – Can't receive multicast packet in the clear
- **QA024239** – IKE crash when using VADNSPrimary and VAWINSPrimary registry settings
- **QA023770** – Installation after GreenBorder Security Agent is installed causes BSOD
- **QA024248** – VPN Activate won't restore 'Secure All' configuration
- **QA024696** – Disabling network adapter (while secure connection is established) causes IKE to crash
- **QA024859** – In a multi-interface machine, wildcard char '!' does not function as expected
- **QA024243** – Client cannot pass secure traffic to site with matching subnet address when client is using the VA
- **QA023379** – IP subnet mask field cursor needs to be always be left-aligned
- **QA024254** – Internet interface pick list doesn't show NICs for non-admin users
- **QA024278** – Support refinement of adaptive filter to handle overlapping subnet cases
- **QA024978** – DNS-Enable/Disable list do not consider interface specific connections
- **QA024240** – User can create connection with no_name
- **QA024241** – User cannot copy proposal through Edit>Copy menu

## 5.4 Addressed Issues in NetScreen-Remote 8.6

- **QA022499** – Host machine displayed a blue screen when "other connections" was set to secure and the "manual only" word under ACL/0 was set to one.
- **QA019934** – Managed policy cert request entries were deleted when failed.
- **QA021546** – Current version of zone alarm bundled with SoftRemote client did not disable windows firewall which is enabled by default with the Windows XP SP2 installation.
- **QA022049** – Redundant gateway connections fail if they were not connected by the third redundant gateway.
- **QA022164** – Firewall was inappropriately disabled when policy was deactivated.
- **QA022436** – Viewing a root certificate, which was not highlighted crashed certmgr.
- **QA022557** – Excessive Phase 2 life time may have caused IREIKE service to crash during negotiations.
- **QA020701** – IRE CSP doesn't work with multi-processor systems.
- **4664** – Windows XP/2000 operating system ping replied to non-existing hosts on va connections; therefore, the client respond to all addresses on the vasubnet.
- **QA018846** – Filter rule instantiation for RAS, should allow configuration for VA connections.
- **QA021982** – Bypass connections require firewall affected the default connection.
- **QA022111** – Client log reported FW status disabled or enabled.
- **QA022112** – Rekeys failed with rgw connections that used a hostname for the gateway.
- **QA022160** – Free zone alarm bundle did not work on NT.
- **QA022421** – NEWPOLICYRESETSCONNS were not working.
- **QA022518** – Policy import was missing ACL global values if ACL key was missing.
- **QA022533** – In standard zone alarm build- "secure connections require firewall to be enabled" did not function.

- **QA022613** – XP SP2 reported no firewall when embedded firewall was present.
- **QA022642** – Imported a policy that did not have a LACTNETPROC value set; therefore, all connections were secured on activation.
- **QA022654** – VPN-Import did not process NEWPOLICYRESETSCONNECTIONS.
- **QA022699** – In standard zone alarm build non-secure traffic would not pass with the firewall enabled and “Non-secure connections require the FW to be enabled” was set to true.
- **QA022718** – Root certs were deleted after user replies “no” to the “you are about to delete this certificate. Are you sure?” prompt.
- **QA022803** – Key request were not initiated with or based on existing Phase 1.
- **QA020882** – Dialup connection with Windows XP using Windows XP firewall and SafeNet VA created a tunnel but did not pass secure traffic.
- **QA019896** – You had to de-select “Show only trusted roots” to configure/delete root certs in cert manager.
- **QA022028** – IREIKE reported 99% proc utilization after running a long time period with connect/ftp/disconnect to Cisco 2621.
- **QA022174** – Global policy settings dialog did not lock completely.
- **QA022572** – Local LBR, LSR connections only worked correctly in gateway mode.
- **QA022616** – Firewall uninstall required a reboot for SP2.
- **QA022618** – “ANY ID” box became editable when you chose “id type = any” for gateways (and RGW'S).
- **QA022549** – VPN -Import notified spdedit to update its display.
- **QA021863** – Traffic-based key requests to remote subnet overlapping physical subnet required arp response.
- **QA021864** – When mode config with VA overlapped a physical subnet, the traffic was not directed to the VA.
- **QA022472** – Supported subj_dn in XAUTHNAME policy item.
- **QA022725** – Maintained encrypted pre-shared key in memory.
- **QA021399** – Connections with an expired PH1 were not displayed on the disconnect menu.
- **QA021443** – Client was not interoperable with Keon CA.
- **QA021481** – LBR “Local Broadcast Relative” does not work on last octet only.
- **QA021482** – On Windows ME, VPN-deactivated results in an “already deactivated” message.

## 5.5 Addressed Issues in NetScreen-Remote 8.5

- **18996** – The automatic Sygate PFW Check feature was incompatible with NetScreen-Remote 8.4.
- **18745** – The Sygate Help/About page incorrectly displayed a copyright forthe 1997-2003 years. The copyright date should be 1997-2004.
- **18744** – The NetScreen-Remote home screen incorrectly displayed the NetScreen logo where it should have displayed the Juniper logo.
- **QA021443** – The client did not interoperate correctly with the Keon Certificate Authority.
- **QA021481** – The Local Broadcast Relative did not work on the last octet only.
- **QA021482** – On a Windows Millenium platform, the VPN deactivated results in an already deactivated message.
- **QA021399** – Connections with an expired PH1 incorrectly displayed on the Disconnect menu.
- **QA021220** – The System Tray NetScreen-Remote icon did not display after Windows Explorer terminated and restarted.
- **QA021213** – The Update command did not function properly.
- **QA021162** – Inappropriate Phase 1 sometimes initiated after an XAUTH dialog box was up.

- **QA021155** – The Authentication dialog box sometimes did not display.
- **QA021042** – The Virtual Adapter did not disconnect when the **ireike** objectrestarted.
- **SYG 10885** – With NetScreen-Remote 8.4 and Sygate 5.5b2634, logging into a Windows 2000 domain could take up to 15 minutes to complete.
- **N/A** – Incompatibility with NetScreen-Remote 8.4 (and earlier) and McAfee VirusScan Enterprise 8.0i when installed on Windows 2000 or XP.
- **N/A** – The NetScreen-Remote 8.4 documentation had not been completelyupgraded. Some areas contained screen shots and procedures from the WebUI in ScreenOS 3.x revisions.

## 5.6 Addressed Issues in NetScreen-Remote 8.4

- **19738/19908** – When attempting to establish a VPN, the Phase 2 renegotiation did not complete. Additionally, XAUTH processing did not complete in the allotted time.
- **19717** – The NetScreen-Remote system incorrectly displayed a Multiple XAUTH prompt when the machine was left idle and the policy was configured for RGW. When the device timed out, you were unable to log backinto the device.
- **19336** – NetScreen-Remote incorrectly sent an ARP (Address Resolution Protocol) packet to a local +1 IP address.
- **19323** – The Nokia PCMCIA GPRS Adapter D211 was incompatible with NetScreen-Remote.
- **N/A** – The system was unable to log back in after a timeout.
- **QA019598** – An SPD file could be incorrectly unlocked via command line.
- **QA4721** – You could not use RSA SecurID passcodes greater than 10 digits.
- **QA4612/QA4652/QA4661** – An error occurred when validating the proxy ID.
- **QA020611** – Under some conditions, packets failed because of validation errors.
- **QA020599** – Traffic initiated connections may have led to an inappropriate initiation of early manual-only connections.
- **QA020593** – When a remote party ID is set to an IP address range, the client incorrectly acted as a responder filter table.
- **QA020571** – The **spdedit.exe** file closed when more than 16 characters were entered in the gateway IP address.
- **QA020308** – CERTMGR incorrectly displayed the retrieve button enabled for file-based CERT requests.
- **QA020299** – IPSECON attempted to retrieve the CERT for file-based CERT requests. The log filled up with error messages.
- **QA020295** – Removing the IKEY 1000 while configured for SMARTCARD removal, did not clear the IPSec keys.
- **QA020243** – Certificate requests did not occur at the prescribed interval set by the CERT request polling interval.
- **QA020233** – Declining at the CERT Addition dialog box left a request in the request storage area.
- **QA020226** – The CERTMGR failed when generating a CERT request with SMARTCARD CSP w/o the reader card.
- **QA020155** – When changing policy from 'SECURE ALL CONNECTIONS' back to 'SPECIFIED CONNECTIONS', the 'OTHER CONNECTIONS' parameter remained set to secure.
- **QA020147** – IREIKE crash during startup when Other Connections were secure.
- **QA020085** – File copy traffic to mapped drive over secure connection causesclient to do excessive QM rekeys.
- **QA018812** – Windows XP logoff caused intermittent **ifcfg.exe** applicationerrors. When logging off on Windows XP, you intermittently received application errors associated with the interface configuration **ifcfg.exe** executable file.

## 5.7 Addressed Issues from 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 andESP 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 associatedwith 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 causedsingle 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 XAUTHwas not completed.
- **4677** – Quick Mode started before the extended authentication processcompleted.
- **4676** – The interface detection mechanism failed on RAS devices introduced after the reboot.
- **4668** – The NSladapssl32v30.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 andgenerated 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 initialcontact 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 ofduplicate connection names.

## 5.8 Addressed Issues from NetScreen-Remote 8.2

- **5445** – Remote gateway failed when using Autocert and more then 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 O's and a mask of all 1"s
- **5440** – Autocertificate with My ID set to IPV4 now only selects certificateswith 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 firstsaving 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 aremote gateway using a hostname.
- **5419** – The SPDedit Gateway IP address box remained enabled after youunchecked the Connect Using checkbox.
- **5411** – When attempting to save a pre-shared key on a Windows XPplatform, 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 inthe 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 firstsaving the settings.
- **5419** – The SPDedit Gateway IP address box remained enabled after youunchecked 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 W2Kwhen 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 theWindows 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 policyeditor 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 lockedpolicies.
- **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 linefailed.
- **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 aconnection 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 andESP were in the same policy.
- **5454** – The SPDEdit facility incorrectly chose the first certficate 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 associatedwith 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.

## 5.9 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.

# 6. Known Issues

This section describes known issues with the current release.

**Known Limitations** are issues that identify features that are not fullyfunctional at the present time, and will be unsupported for this release. NetScreen recommends that you do not use these features.

**Compatibility Issues** are known compatibility issues with other products,including but not limited to specific NetScreen appliances, other versions ofScreenOS, 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.

**Known Issues** are deviations from intended product behavior as identified by Juniper Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

## 6.1 Known Limitations

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

- **Windows XP Internet Connection Firewall with the Virtual Adapter**
  The SafeNet Virtual Adapter must be "firewalled" with the Windows XP Internet Connection Firewall if the connection used to create VA is Windows XP "firewalled"; otherwise, packets will not pass.

- **DNS resolution via a secure tunnel may require the full DNS name including DNS suffix.**
  **Description**: If the client is attempting to resolve a simple hostname via DNS utilizing the mode config DNS assigned address may fail because the locally configured DNS suffix may be appended.
  **Workaround**: In the adapters advanced TCP \ IP properties, append the desired DNS suffix in the DNS suffix search list.

- **PPPoE software for DSL connections must be installed and operational before the client is installed.**
  **Description**: Installing PPPoE software on a computer that already has the SoftRemote Client installed removes some network components.
  **Workaround**: If the computer does not have the SoftRemote client installed, install the PPPoE software before you install the SoftRemote client. If the client is already installed, remove the client and save the IPSec policy when prompted. After your computer reboots, install the PPPoE software, and then install the client again.

- **Compatibility issues with EarthLink software**
  **Description**: The client is incompatible with EarthLink Internet software, version 5.02.
  **Workaround**: EarthLink can still be accessed through a standard dial-up networking configuration. Uninstall the EarthLink software. EarthLink Technical Support is aware of the situation. Contact EarthLink for help in setting up a standard dial-up configuration for EarthLink access.

- **Compatibility issues with Sony Vaio and 3COM 3CCFE575CT CardBus PC Card**
  **Description**: The 3COM 3CXFE575CT 10/100 LAN CardBus PC Card is not compatible with Sony Vaio notebook computers. After the client is installed, the computer requires an Ethernet cable to be attached in order to boot. This NIC card works fine in other computers.
  **Workaround**: Use hardware profiles to disable the NIC card, or remove the NIC card when the computer is not attached to the network.

- **RequestLocalAddress failure and dialup interfaces are not detected properly in the Log Viewer on clients that also have the Nortel client installed and DN is bound to the Nortel IPSECSHM**
  **Description**: Cannot connect using Windows 2000 and XP RAS connections when DN is bound to the Nortel IPSECSHM.
  **Workaround**: In the Windows Device Manager, if the IPSECSHM - Deterministic Network Enhancer Miniport is disabled, the dialup interface will be detected properly and sessions will establish.

## 6.2 Known Limitations for NetScreen-Remote 8.8

These are the same as in the NetScreen -Remote 8.7 version. Please see the section 6.3 below.

## 6.3 Known Limitations for NetScreen-Remote 8.7

These are the same as in the NetScreen -Remote 8.6 version. Please see the section 6.3 below.

## 6.4 Known Limitations for NetScreen-Remote 8.6

The following are limitations in NetScreen-Remote 8.6:

**DNE Limitations and Workarounds** – The following are current issues with DNE 2.2.1 extracted from the DNE release notes.

- **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:** Clear the VPN component check box when installing the ATT dialer. When upgrading DNE on Windows 2000 (running "dneinst -install ..." when DNE is already installed), the DNE Network Adapters may be listed as "Deterministic Network Enhancer Miniport #2", instead of the normal listing of "Deterministic Network Enhancer Miniport -" followed by the name of the physical network adapter. This is a Windows bug fixed in Windows 2000 Service Pack 4.

- **Windows 2000/XP/2003 Task Offload**– With Task (IPSEC, Large TCP send, etc.) Offload capable network adapters, a plugin must be able to handle the additional attributes that are bundled with each packet. If a plugin is not capable of or do not want to deal with packet attributes, it should set the registry value: DisableTaskOffload to 1, located at: "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters".

- **AOL 6.0** – 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:** Boot into safe mode, remove DNE, and continue with the AOL install. After AOL is installed, reinstall DNE. AOL will still ask to be restarted on every startup; click No, and AOL will work normally.

  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.

- When upgrading DNE on Windows 2000 (running "dneinst -install ..." when DNE is already installed), the DNE Network Adapters may be listed as "Deterministic Network Enhancer Miniport #2", instead of the normal listing of "Deterministic Network Enhancer Miniport -" followed by the name of the physical network adapter.

  **W/A:** Install Windows 2000 Service Pack 4.

## 6.5 Known Limitations for NetScreen-Remote 8.5

The following are limitations in NetScreen-Remote 8.5:

**Manual Key Dial-up VPN Limitations** – Manual Key Dial-up VPNs are compatible with ScreenOS 4.x and earlier. ScreenOS 5.0 and later revisions do notsupport this configuration.

**No Support for DES-MAC** – ScreenOS only supports configurations for SHA-1 and MD5 security methods, although it does not support the DES-MAC method when connected to a Juniper firewall device.

**No Support for Diffie-Hellman Group 14** – While the Diffie-Hellman Group14 appears as an option in some lists in the NetScreen -Remote software, the product does not support it yet.

**New Key Length Support Limitations** – NetScreen-Remote now supports keylengths up to 4,096; although ScreenOS only supports key lengths up to 2,048.

**No Support for Silent Installation Running in Background** – Juniper supports a silent installation option, which hides all end user prompts during the installation. While this process may run in the foreground, Juniper does not support running the silent installation in the background, although it may run inthat mode. If it does run in the background, you do not see the initial splashscreens that launch as part of the installation process.

## 6.5 Known Limitations for NetScreen-Remote 8.4

The following are limitations in NetScreen-Remote 8.4:

**DNE Limitations and Workarounds** – The following are current issues with DNE 2.2.0 extracted from the DNE release notes.

- **Windows NT-Disabled Protocols Enabled With DNE Installed** – On Windows NT 4.0 only, if you install DNE with protocols disabled, then theprotocols become enabled.

  **W/A:** Disable the protocols through the Control Panel or remove the protocols after installing DNE.

- **Windows NT Plug and Play Drivers Issues** – Windows NT does not support Plug and Play, even on laptops whose manufacturers attempted tocreate Windows NT Plug and Play support through a custom utility. DNE does not work with custom, non -standard, or non-NDIS-compliant utilities.

**W/A:** Disable the utility and obtain the latest NIC driver from the vendor (not the special pre-packaged on that the laptop vendor supplies with the utility).

**Client Incompatible With the ATT Dialers' VPN Component** – The VPN component included with the ATT dialer is incompatible with DNE.

**W/A:** Clear the VPN component check box when installing the ATT dialer.

# 6.6 Compatibility Issues in NetScreen-Remote

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.

**Due to changes in the Microsoft Windows support, only Windows XP and Windows 2000 are supported. Defects will continue to be resolved on the other operating systems, but no new functionality will be supported.**
For questions regarding which operating systems Microsoft supports, please reference Microsoft’s product lifecycle at http://support.microsoft.com/gp/lifewin.

### 6.6.1 Supported Windows Versions

- Vista Business 32-bit
- Vista Enterprise 32-bit
- Vista Home Premium 32-bit
- Vista Ultimate 32-bit
- XP Home and Professional 32-bit
- 2000 Professional 32-bit

Juniper recommends installing the latest Windows service pack, dial-up networking upgrade, and Internet Explorer version.

### 6.6.2 Unsupported Windows Versions (Not Y2K-Compliant)

- Windows 95
- Windows 98
- Windows NT4.0
- Millennium
- Under certain circumstances NetScreen-Remote Login will not load on Windows 95B Machines; after a system reboot, the application loads properly.

### 6.6.3 Juniper NetScreen Platform

- **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.
- **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, andwill upgrade or downgrade automatically to other releases of Global-PRO.

### 6.6.4 Network Interface Card

This version should be compatible with all NDIS-compliant Ethernet network interface cards (NICs). Plug and play is supported on Windows 95, 98, Me, and 2000 only. Plug and play is not supported on notebook computers running Windows NT.

### 6.6.5 Common Compatibility and Configuration

Please refer to the different section under Platform Compatibility for detail on 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.

**Network Interface Cards**
This version should be compatible with all NDIS-compliant Ethernet network interface cards (NICs).

- **Installation Files for Different Windows Platforms** – For Windows 2000, Windows NT and Windows XP platforms, use the .exe installation file.
- **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 usedwith Aggressive mode. When using standalone NetScreen-Remote (withoutGlobal-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 upL2TP 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. Juniper Networks recommends that you create a service-book entry for the protocols above.
- **NAT-Traversal Requires ScreenOS 3.0r2 or Later** – For full compatibility, 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 Namedefined in the client's certificate request matches how the user is identifiedin 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

- that 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 2000is supported. Plug and play on notebook computers running Windows NT isnot supported. Co-existence (i.e. encryption over the dial-up adapter) withToken Ring cards is supported.
- **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

- **Nortel Contivity VPN Switch** – The elements of the Distinguished Name (DN) sent by the switch are not in the standard order expected by the client. When entering the DN in the Connect dialog box using the Nortel Contivity VPN Switch group, click Enter Subject Name in LDAP Format check box. Make sure that the order of the elements matches the order from the switch, for example:
- **W/A:** The Nortel switch's firmware version 3.5 or later, with Keep Alivesdisabled, is required. If a message regarding invalid hash length appears in the LogView, this means that the Keep Alive feature is enabled. The Keep Alives option is controlled through the IPSec section of the Group profile.The menu item in IPSec is called Enable Client Failover Tuning**.**
- **New Virtual Adapter Features Not Updated for Users Performing 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 Networkingenvironment. A new virtual adapter connection is created on the next connection that utilizes the virtual adapter with all of the new settings.
- **Errors When Gateway Sends Certificates With More Than 1,024 Bits Without Microsoft Enhanced CSP** – Log Viewer errors and connection failures occur on the client when the gateway sends certificates larger than 1,024 bits on computers that don’t have a 128-bit version of MicrosoftInternet Explorer installed. Log errors cannot acquire enhanced providerverify context, and signature verification fails.
- **W/A:** For gateways that send certificates larger than 1,024 bits to the client, upgrade to the 128-bit version of Internet Explorer, which includes theMicrosoft Enhanced CSP.
- **Automatic Certificate Selection May Not Work in Aggressive Mode** – Since Aggressive Mode sends an ID payload in the first initiator packet, andno explicit certificate is selected, the session may fail. The client makes abest 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 validcertificate.
- **W/A:** Manually select the certificate when using Aggressive Mode or limit your certificates to one in NetScreen-Remote Certificate Manager.
- **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.