FIPS 140-2 SECURITY POLICY

Juniper Networks

NetScreen-5XT

HW P/N NS-5XT VERSION 1010 FW VERSIONS SCREENOS 5.0.0R9.H, SCREENOS 5.0.0R9A.H AND SCREENOS 5.0.0R9B.H

Copyright Notice

Juniper Networks, Inc.

ATTN: General Counsel

1194 N. Mathilda Ave.Sunnyvale, CA 95014

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Consult the dealer or an experienced radio/TV technician for help.

Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

TABLE OF CONTENTS

A. Scope of Document

The Juniper Networks NetScreen-5XT is an Internet security device that integrates firewall, virtual private networking (VPN), and traffic shaping functions.

Through the VPN, the NetScreen-5XT provides the following:

- IPSec standard security
- Data security using the Data Encryption Standard (DES), Triple-DES and Advanced Encryption Standard (AES) algorithms

Note: DES - for legacy systems only; transitional phase only - valid until May 19, 2007

- Manual and automated IKE (ISAKMP)
- Use of RSA and DSA certificates

The NetScreen-5XT also provides an interface for a user to configure or set policies through the Console or Network ports.

The general components of the NetScreen-5XT include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC (GigaScreen version 2), 10/100 Mbps Ethernet interface, and console interface. The entire case is defined as the cryptographic boundary of the modules. The NetScreen-5XT's physical configuration is defined as a multi-chip standalone module.

B. Security Level

The NetScreen-5XT meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Module Security Level Specification

Security Requirements Section	**Level**
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

C. Roles and Services

The NetScreen-5XT supports three distinct roles:

- Cryptographic Officer Role (Root): The module allows one Crypto-Officer. This role is assigned to the first operator who logs on to the module using the default user name and password. Only the Crypto-Officer can create other administrators, and change to FIPS mode.
- User Role (Admin): The Admin user can configure specific security policies. These policies provide the module with information on how to operate (for example, configure access policies and VPN encryption with Triple-DES).
- Read-Only User Role (Admin): This role can only perform a limited set of services to retrieve information or status. This role cannot perform services to configure the box.

The module allows concurrent Admin users, either in a User Role or in a Read- Only Role.

The NetScreen-5XT provides the following services:

- **Clear/Delete**: Clear dynamic system info
- **Exec**: Exec system commands
- **Exit**: Exit command console
- **Get (Show Status)**: Get system information
- **Ping**: Ping other host
- **Reset (Self-Tests)**: Reset system
- **Save**: Save command
- **Set**: Configure system parameters
- **Trace-route**: Trace route
- **Unset**: Unconfigure system parameters

The NetScreen-5XT supports both role-based and identity-based authentication.

- All roles can be authenticated locally (within the NS-5XT); optionally, the module supports authentication via a RADIUS server for only the User role. Authentication by use of the RADIUS server is viewed as role-based authentication; all other methods of authentication are identity-based.
- All other forms of authentication (local database) are classified as identity- based.
- The module supports identity-based authentication for the Cryptographic Officer Role (local database), the User Role (local database), and the Read-Only Role (local database).

D. Interfaces

The NetScreen-5XT provides a number of interfaces:

- The NetScreen-5XT has five Ethernet autosensing interfaces (RJ-45) (Data Input, Data Output, Control, Status). One is for the Untrusted network, and four, labeled 1, 2, 3, and 4, are for the Trusted network. These interfaces are the network ports. Each port has two LEDs that indicate port status:
  - The bottom LED indicates the bandwidth: the LED on means 100 Mbps, the LED off means 10 Mbps (Status Output)
  - The top LED indicates Ethernet connectivity and activity: the LED on and blinking means the port is active (transmitting and receiving data), the LED off

means the port is inactive (Status Output)

- Console port – RJ-45 serial port connector (Data Input, Data Output, Status, Control).
- Modem port – RJ-45 serial port connector. Disabled in FIPS mode.
- Power interface: AC or DC.
- The module has two status LEDs.
  - Power status LED: Illuminates solid green when power is supplied to the NetScreen-5XT (Status Output).
  - Module status LED: Illuminates blinking green when the module is operational, dark or red when the module is not operational, solid amber when the unit is rebooting, or solid green when the module is initializing (Status Output).
- Hardware reset button: After the user follows this sequence—press for 5 seconds, release for 5 seconds, press again for 5 seconds, and release again for 5 seconds—the device erases all configurations and restores the default factory settings (Control Input).

E. Setting FIPS Mode

By default, the module is in non-FIPS mode on the first power-up.

The CLI commands **get config** or **get system** show if the system is in FIPS mode.

1. The module can be set to FIPS mode only through the CLI. The module must be zeroized when toggling between FIPS and non-FIPS mode of operation. It is suggested that the module's configuration be saved prior to switching modes. To set the module to FIPS mode, execute the **set FIPS-mode enable** command through the CLI.

Note: *If you upgrade pre-5.0 firmware to 5.0 version FIPS or later, you must re-enable FIPS mode again even if the device was previously in FIPS mode. To re-enable FIPS mode, issue the commands* **unset FIPS-mode enable**, *then* **set FIPS-mode enable**, *before rebooting the device.*

The **set FIPS-mode enable** command performs the following:

- Disables administration via SSL
- Disables loading and output of configuration files from the TFTP server
- Disables the NetScreen-Global PRO reporting agent
- Disables administration via SNMP
- Disables debug service
- Disables the Modem port
- Enforces management via Telnet, HTTP (WebUI), and NetScreen Security Manager only through a VPN with 256-bit AES encryption
- Enforces management via SSH only when using 3DES
- Disables the MD5 algorithm

2. Execute the **save** command.
3. Execute the **reset** command.

Note the following:

- Telnet, NSM and HTTP (WebUI) are only allowed through a VPN tunnel with 256-

bit AES encryption.

- User names and passwords are case-sensitive. The password consists of at least six alphanumeric characters. Since there are 26 uppercase letters, 26 lowercase letters, and 10 digits, the total number of available characters is 62. The probability of someone guessing a password is $1/(62^{6}) = 1/56{,}800{,}235{,}584$, which is far less than a 1/1,000,000 random success rate. If three login attempts from the console fail consecutively, the console will be disabled for one minute. If three login attempts from Telnet or the WebUI (through VPN with AES encryption) fail consecutively, any login attempts from that source will be dropped for one minute.
- If there are multiple login failure retries within one minute and since the user is locked out after three contiguous login failures, the random success rate for multiple retries is $1/(62^{6}) + 1/ 62^{6}) + 1/(62^{6}) = 3/(62^{6})$, which is far less than 1/100,000.
- DSA-signed firmware image cyrptographic strength analysis: the firmware is signed by a DSA private key, which is in the sole possession of Juniper Networks. The generated signature is attached to the firmware. In order for the device to accept an image, the image has to have a correct 40-byte (320-bit) signature. The probability of someone guessing a signature correctly is $1/(2^{320})$, which is far less than 1/1,000,000.
- The image download takes at least 23 seconds, so there can be no more than 3 download tries within one minute. Therefore, the random success rate for multiple retries is $1/(2^{320}) + 1/(2^{320}) + 1/(2^{320}) = 3/(2^{320})$, which is far less than 1/100,000.
- In order for authentication data to be protected against disclosure, substitution and modification, the operator password is not echoed during entry.
- The NetScreen-5XT does not employ a maintenance interface or have a maintenance role.
- When in FIPS mode, the WebUI of the NetScreen-5XT only displays options that comply with the requirements of FIPS 140-2.
- The output data path is logically disconnected from the circuitry and processes that perform key generation or key zeroization.
- The NetScreen-5XT provides a Show Status service via the GET service.
- The NetScreen-5XT cannot be accessed until the initialization process is complete.
- The NetScreen-5XT implements the following power-up self-tests:

  Device Specific Self-Tests:

  - Boot ROM firmware-self-test is via DSA signature (Software Integrity Test)
  - SDRAM read/write check
  - FLASH test

  Algorithm Self-Tests:

  - DES, CBC mode, encrypt/decrypt (for legacy systems only) KAT
  - 3DES, CBC mode, encrypt/decrypt KAT
  - SHA-1 KAT
  - RSA (encryption and signature) KAT
  - DSA Sign/Verify KAT
  - AES, CBC mode, encrypt/decrypt KAT
  - HMAC-SHA-1 KAT
  - DH key agreement test

  - ANSI X9.31 DRNG KAT
- The NetScreen-5XT implements the following conditional self-tests:
  - DRNG continuous test
  - Hardware RNG continuous test
  - DSA pairwise consistency test
  - RSA pairwise consistency test
  - Bypass test
  - Firmware download DSA signature test (Software Load Test)

F. Other Parameters

Note the following:

- Firmware can be loaded through Trivial File Transfer Protocol (TFTP), where a firmware load test is performed via a DSA signature.
- Keys are generated using the FIPS-approved ANSI X9.31 pseudo random number generator.
- For every usage of the module's random number generator, a continuous RNG self-test is performed. Note that this is performed on both the FIPS-approved RNG and non-FIPS-approved RNG.
- The NetScreen-5XT enforces both identity-based and role-based authentication. Based on their identity, the operator assumes the correct role.
- Operators must be authenticated using user names and passwords. Alternatively, the CO may also be authenticated via digital signature verification during the download of a new firmware image. Authentication will occur locally. As an option, the user can be authenticated via a RADIUS server. The RADIUS server provides an external database for user role administrators. The NetScreen-5XT acts as a RADIUS proxy, forwarding the authentication request to the RADIUS server. The RADIUS server replies with either an accept or reject message. See the log for authenticated logins. The RADIUS shared secret must be at least 6 characters.
- All logins through a TCP connection disconnect upon three consecutive login failures and an alarm is logged.
- A separate session is assigned to each successful administrator login.
- The first time an operator logs on to the module, the operator uses the default user name and password which is netscreen, netscreen. This user is assigned the Crypto-Officer role.

The Crypto-Officer is provided with the same set of services as the user, with four additional services:

  - **set admin** and **unset admin** allow the Crypto-Officer to create a new user, change a current user's user name and password, or delete an existing user.
  - **set FIPS enable** and **unset FIPS enable** allow the Crypto-Officer to switch between FIPS mode and the default mode.

- HTTP can only come through VPN with AES encryption. The page time-out is set to 10 minutes by default; this setting can be user configured. The maximum number of HTTP connections, or the maximum number of concurrent WebUI logins, depends on how many TCP sockets are currently available in the system. The maximum number of available TCP sockets is 64. This number is shared with other TCP connections.
- Telnet can only come through VPN with AES encryption.
- There are a maximum of two sessions shared between Telnet and SSH.

- Upon a Telnet or console login failure, the next prompt will not come up for an estimated 5 seconds.
- The NetScreen-5XT's chips are production-grade quality and include standard passivation techniques.
- The NetScreen-5XT is contained within a metal production-grade enclosure.

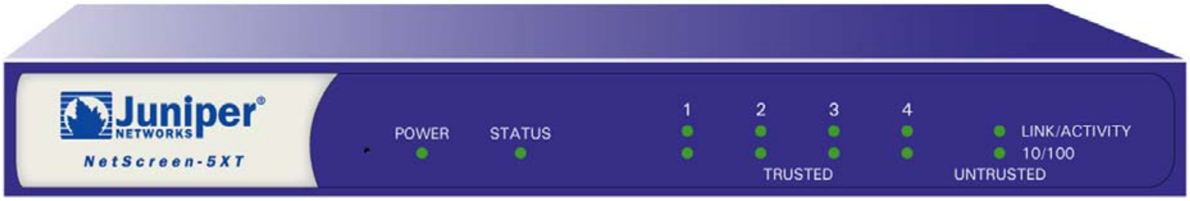

Figure 1: Front of the NS-5XT device

- The enclosures are opaque to visible spectrum radiation.
- The enclosure includes a removable cover and is protected by a tamper-evident seal. The location of the tamper evident seal is shown in Figure 2.

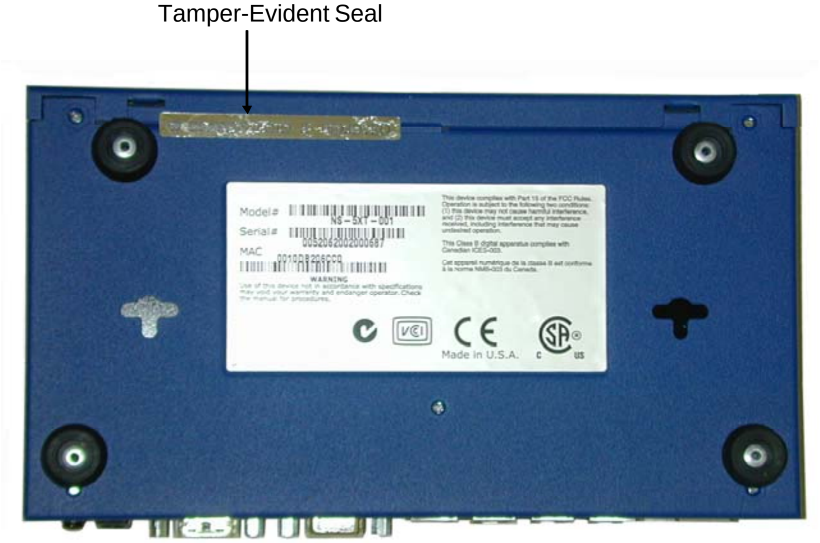

Figure 2 Tamper-Evident Seal

- IKE, Diffie-Hellman (DH), and RSA encryption are employed for public key- based key distribution techniques, which are commercially available public key methods and are known to provide at least 80-bits of strength as implemented.
- All keys and unprotected security parameters can be zeroized through the Unset, Clear, Delete, and Reset commands. Pressing the hardware reset button will also cause the zeroization of all plaintext CSPs.
- Algorithms included in the NetScreen-5XT are:

- FIPS Approved:

  DSA

  SHA-1

  TDES (CBC)

  DES (CBC) (transitional phase only valid until May 19, 2007)

  AES (CBC)

  HMAC-SHA-1

  RSA Sign/Verify (PKCS #1)

  ANSI X9.31 DRNG

- Non-FIPS Approved:

  MD5

  DH (key agreement, key establishment methodology provides 80 bits of encryption strength)

  RSA Encrypt/Decrypt (used for key wrapping only, key establishment methodology provides 80 bits of encryption strength)

- The NetScreen-5XT conforms to FCC part 15, class B.
- On failure of any power-up self-test, the module enters and stays in either the Algorithm Error State, or Device specific error state, depending on the self-test failure. The console displays error messages and the status LED flashes red. It is the responsibility of the Crypto-Officer to return the module to NetScreen Technologies, Inc. for further analysis.
- On failure of any conditional test, the module enters and stays in a permanent error state, depending on the type of failure: Bypass test failure, DH key agreement test failure, DSA pair-wise test failure, or RSA pair-wise agreement test failure. The console displays error messages and the status LED flashes red. It is the responsibility of the Crypto- Officer to return the module to NetScreen Technologies, Inc. for further analysis.
- On power down, previous authentications are erased from memory and need to be re-authenticated again on power-up.
- Bypass tests are performed at power-up, and as a conditional test. Bypass state occurs when the administrator configures the box with a non-VPN policy and traffic matching this policy arrives at the network port. The bypass enabled status can be found by retrieving the entire policy list. Two internal actions must exist in order for bypass to happen: (1) a non-VPN policy is matched for this traffic, and (2) a routing table entry exists for the traffic that matches this non-VPN policy.
- In FIPS mode, SSH can use 3DES only to encrypt/decrypt commands. Also, if the command from SSH is to set or get the AES manual key, it will fail and a message is logged.
- If the VPN uses 3DES Encryption, the key exchange protocol IKE is enforced to use group 5 only.
- The module is not designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

G. FIPS Certificate Verification

In FIPS mode, if the signing CA certificate cannot be found in the NetScreen-5XT during the loading of the X509 certificate, the following message appears (where x is one of 0, 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F):

```
Please contact your CA's administrator to verify the following finger print (in HEX) of the CA
cert...

xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Do you want to accept this certificate y/[n]?
```

Based on the result of the CA certificate fingerprint checking, the Crypto-Officer accepts or denies the loaded certificates.

H. Critical Security Parameter (CSP) Definitions

Below is a list of Critical Security Parameter (CSP) definitions:

- IPSEC HMAC SHA-1 Key: Used by IPsec for data integrity.
- IPSEC ESP Key: DES, TDES, and AES for user traffic encryption.
- IKE Pre-Shared Key: Used during the IKE protocol to establish cryptographic keys to be used by IKE.
- IKE Encryption Key: DES, TDES, and AES for peer-to-peer IKE message encryption.
- IKE HMAC SHA-1 Key: Used by IKE for data integrity.
- Password: Crypto-Officer and User passwords.
- SSH Server/Host DSA Private Key: Used to create digital signatures.
- SSH Encryption Key: TDES encryption key to encrypt telnet commands.
- SSH HMAC SHA-1 Key: Used by SSH for data integrity.
- IKE RSA/DSA Private Key: DSA/RSA key used in IKE identity authentication.
- PRNG Algorithm Key: ANSI X9.31 algorithm key required to generate pseudo-random numbers.
- Diffie Hellman Private Key Components: Used during the DH key agreement protocol.

I. Public Key Definitions

Below is a list of the public keys utilized by the module:

- Firmware Authentication Key: Used by the device to verify DSA signatures over firmware images.
- CA DSA/RSA Public Key: Used by IKE to authenticate a peer's certificate.
- Local DSA/RSA Public Key: Used by the IKE peer to verify digital signatures.
- SSH Server/Host DSA Public Key: Used by the SSH client to verify digital signatures.
- SSH Client DSA Public Key: Used by the device to verify digital signatures.
- Diffie Hellman Public Key Components: Used by the DH Key Agreement protocol.

J. Matrix Creation of Critical Security Parameter (CSP) versus the Services (Roles & Identity)

The following matrices define the set of services to the CSPs of the module, providing information on generation, destruction and usage. They also correlate the User roles and the Crypto-Officer roles to the set of services to which they have privileges.

The matrices use the following convention:

- G: Generate
- D: Delete
- U: Usage
- N/A: Not Available

Table 1: Crypto-Officer

Crypto-Officer

CSP \ Services	Set	Unset	Clear/Delete	Get	Exec	Save	Ping	Reset	Exit	Trace-route
IPSEC HMAC SHA-1 Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IPSEC ESP Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IKE Pre-shared Key	G	D	N/A	U	G	U	N/A	N/A	N/A	N/A
IKE Encryption Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
IKE HMAC SHA-1 Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
Password	G1	D2	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SSH Server/Host DSA Private Key	G	D	D	U	G	U	N/A	D (Server Key)	N/A	N/A
SSH Encryption Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
SSH HMAC SHA-1 Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
IKE RSA/DSA Private Key	N/A	D	N/A	N/A	G,D,U	N/A	N/A	N/A	N/A	N/A
PRNG Algorithm Key	N/A	N/A	N/A	N/A	G,U	N/A	N/A	D	N/A	N/A
Diffie Hellman Private Key Components	G	N/A	N/A	N/A	N/A	N/A	N/A	D	N/A	N/A

Table 2: User

User

CSP \ Services	Set	Unset	Clear/Delete	Get	Exec	Save	Ping	Reset	Exit	Trace-route
IPSEC HMAC SHA-1 Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IPSEC ESP Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IKE Pre-shared Key	G	D	N/A	U	G	U	N/A	N/A	N/A	N/A
IKE Encryption Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
IKE HMAC SHA-1 Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
Password	G3	N/A	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SSH Server/Host DSA Private Key	G	D	D	U	G	U	N/A	D (Server Key)	N/A	N/A
SSH Encryption Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
SSH HMAC SHA-1 Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
IKE RSA/DSA Private Key	N/A	D	N/A	N/A	G,D,U	N/A	N/A	N/A	N/A	N/A
PRNG Algorithm Key	N/A	N/A	N/A	N/A	G,U	N/A	N/A	D	N/A	N/A
Diffie Hellman Private Key Components	G	N/A	N/A	N/A	N/A	N/A	N/A	D	N/A	N/A

Table 3: Read-Only User

Read-Only User

CSP \ Services	Get	Ping	Exit	Trace-route
IPSEC HMAC SHA-1 Key	U	N/A	N/A	N/A
IPSEC ESP Key	U	N/A	N/A	N/A
IKE Pre-shared Key	U	N/A	N/A	N/A
IKE Encryption Key	N/A	N/A	N/A	N/A
IKE HMAC SHA-1 Key	N/A	N/A	N/A	N/A
Password	U	N/A	N/A	N/A
SSH Server/Host DSA Private Key	U	N/A	N/A	N/A
SSH Encryption Key	N/A	N/A	N/A	N/A
SSH HMAC SHA-1 Key	N/A	N/A	N/A	N/A
IKE RSA/DSA Private Key	N/A	N/A	N/A	N/A
PRNG Algorithm Key	N/A	N/A	N/A	N/A
Diffie Hellman Private Key Components	N/A	N/A	N/A	N/A

1. The Crypto-Officer is authorized to change all authorized operators' user names and passwords, but the user is only allowed to change his/her own user name and password
2. The Crypto-Officer is authorized to remove all authorized operators.
3. The Crypto-Officer is authorized to change all authorized operators' user names and passwords, but the user is only allowed to change his/her own user name and password.

K. Definitions List

AES – Advance Encryption Standard

CLI – Command Line Interface

CSP – Critical Security Parameter

DES – Data Encryption Standard

DH – Diffie-Hellman

DRNG – Deterministic RNG

IPSec – Internet Protocol Security

IV – Initial Vector

KAT – Known Answer Test

NS – NetScreen

NSM – NetScreen Security Manager

PRNG – Pseudo RNG

RNG – Random Number Generator

ROM – Read Only Memory

RSA – Rivest Shamir Adelman Algorithm

SDRAM – Synchronous Dynamic Random Access Memory

SSH – Secure Shell protocol

TCP – Transmission Control Protocol

TFTP – Trivial File Transfer Protocol

VPN – Virtual Private Networking