FIPS 140-2 SECURITY POLICY

Juniper Networks

NetScreen-500

P/N NS-500 VERSION 4110 FW VERSION SCREENOS 5.0 R9

Copyright Notice

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-500 is an Internet security device that integrates firewall, virtual private networking (VPN) and traffic shaping functionalities.

Through the VPN, the NetScreen-500 provides the following:

- IPSec standard security
- Data Encryption Standard (DES), triple-DES and Advanced Encryption Standard (AES) key management

  Note: DES is only used for legacy systems
- Manual and automated IKE (ISAKMP)
- Use of RSA and DSA certificates

The NetScreen-500 also provides an interface for users to configure or set policies through the console or network ports.

The general components of the NetScreen-500 include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC (GigaScreen), 10/100 Mbps ethernet interface, GBIC network interface, console interface, backplane, redundant power supplies and fan tray. The entire case is defined as the cryptographic boundary of the modules. The NetScreen-500's physical configuration is defined as a multi-chip standalone module.

B. Security Level

The NetScreen-500 meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1: 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	2
Self-Tests	2

Design Assurance	2
Mitigation of Other Attacks	N/A

C. Roles and Services

TheNetScreen-500 supports five 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.
- VSYS User Role: This role has the same operations as the User Role above, except that a VSYS user only operates within a particular virtual system. See the *NetScreen Concept and Examples ScreenOS Reference Guide* for more information about virtual systems.
- VSYS Read-Only User Role: This role has the same operations as the Read-Only User Role above, except that a VSYS read-only user only operates within a particular virtual system. See the *NetScreen Concept and Examples ScreenOS Reference Guide* for more information about virtual systems.

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

  The root administrator can create a virtual system (vsys) administrator for each vsys, if the device has multiple virtual systems configured. The vsys administrator can function in either the "user" role or "read-only" role. A virtual system is the architecture that enables the device to respond with a different set of configurations for each vsys administrator. Therefore, a single box can appear to be several logical "virtual systems."

  The NetScreen-500 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-500 supports both role-based and identity-based authentication.

- All roles can be authenticated locally (within the NS-500); 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 Crypto-Officer (local database), the User Role (local database), the Read-Only User Role (local database), VSYS User Role, and VSYS Read-Only Role User Role.

D. Interfaces

The NetScreen-500 provides a number of interfaces:

- LCD and Control Pad: A display with control keys that can be used to perform basic configurations and to view status reports through the LCD and control pad. The LCD displays two lines, each line capable of displaying up to 16 characters (Control Input, Status Output).
- Two to four network cards. These may be either 10/100 Base T or GBIC interfaces (Data Input, Data Output, Control, Status).
- HA-1: dedicated RJ-45 used for failover processing (Data Input, Data Output, Control, Status).
- HA-2: backup dedicated RJ-45 used for failover processing if HA-1 fails (Data Input, Data Output, Control, Status).
- MGT: dedicated RJ-45 used exclusively for management traffic, such as Telnet, SCS, or HTTP (Control, Status).
- Console port: DB9 serial port connector (Control, Status).
- Modem port: DB9 serial port connector. Disabled in FIPS mode.
- PCMCIA interface for a memory flash card (Data Input).
- Up to two power interfaces.
- 22 LED status interfaces: 12 general, 4-interface module, and 6 port LEDs (Status). The following sections describe these LEDs.

Table 2: Twelve General LEDs:

LED	Purpose	Color	Meaning

STATUS	System status	Blinking amber	Booting up normally
		Blinking green	Normal operation
ALARM	System alarm	Red	Critical alarm - failure of hardware component or software module (such as a cryptographic algorithm)
		Green	No alarm condition present
		Amber	Major alarm: ○ Low memory (<10% remaining) ○ High CPU utilization (>90%) ○ Log memory full ○ Sessions full ○ Maximum number of VPN tunnels reached ○ Firewall attacks detected ○ HA status changed or redundant group member not found
		Dark	No alarm
PWR1	Power Supply #1	Green	Power supply #1 is functioning correctly
		Red	Power supply failure, or bay is empty
PWR2	Power Supply #2	Green	Power supply #1 is functioning correctly
		Red	Power supply failure, or bay is empty
FAN	Fan status	Green	All fans functioning properly
		Red	One or more fans failed
TEMP	Temperature	Green	Temperature is within safety range
		Red	Outside safety range
HA	High Availability	Green	Unit is master
		Blinking green	Redundant group member cannot be found
		Amber	Unit is slave
		Dark	HA not configured
FW	Firewall alarm	Green	No alarm attacks
		Red	Firewall alarm/event has occurred
VPN	VPN activity	Blinking green	VPN activity - encrypting/decrypting traffic
		Blinking yellow	VPN drops or denies traffic
		Red	VPN tunnels have reached 90%of the maximum number of simultaneously active IPSec SAs.
		Dark	No VPN defined or no tunnels active
SESSION	Firewall session utilization	Green	Sessions are < 70% utilization
		Yellow	Sessions are between 70% and 90% utilization.
		Red	Sessions are >90% utilization.
PCMCIA	PC card status	Green	PC card is installed in PCMCIA slot.
		Blinking green	PC card is active

		Red	PC card is >90% full or read/write activity has failed.
		Dark	PCMCIA slot is empty.
SHAPE	Traffic shaping	Green	Traffic shaping in operation
		Blinking green	Traffic shaping transmits packets
		Blinking yellow	Traffic shaping drops packets
		Red	Configured guaranteed bandwidth > available interface bandwidth
		Dark	No traffic shaping configured

- Four module status LEDs: Illuminates green to correspond to the position of the installed interface modules (Status):

Green: Card operational
Blinking Red: Card failed
Dark: No card

- Six network status LEDs for the MGT, HA-1 and HA-2 ports. Each Ethernet port has two LEDs: the left LED indicates 10Mbps or 100Mbps; the right LED indicates link and network activity (Status).

E. Setting FIPS Mode

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

The commands "get config", or "get system" indicate if the system is in FIPS mode.

The module can be set to FIPS mode only through the CLI. To set the module to FIPS mode, execute "set FIPS-mode enable" through the CLI.

Special note for firmware upgrade: if pre-5.0 firmware is upgraded to FIPS version 5.0 or higher, re-enable FIPS again by issuing the commands "unset FIPS-mode enable", "set FIPS-mode enable", and reboot the device. You must do this even if the device was previously in FIPS mode.

This command will perform the following:

- Disable administration via SSL
- Disable the loading and output of the configuration file from the TFTP server
- Disable the Global reporting agent
- Disable administration via SNMP
- Disable the debug service
- Disable the modem port
- Enforce HTTP only through VPN with AES encryption
- Enforce Telnet only through VPN with AES encryption

- Enforce SCS to use only 3DES to manage the box
- Disable the MD5 algorithm

Execute the "save" command.

Execute the "reset" command.

Please note the following:

- Configure the HA encryption key before using the HA link.
- Telnet and HTTP (WEB UI) are allowed only through VPN with AES encryption.
- The derivation of keys for ESP-Encryption and ESP-Authentication using a user's password is in non-FIPS mode.
- 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/(626) + 1/ 626) + 1/(626) = 3/(626), which is far less than 1/100,000.
- DSA-signed firmware image cryptographic strength analysis: the firmware is signed by a well-protected DSA private key. The generated signature is attached to the firmware. In order for the device to accept an authorized 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 administrator password is not echoed during entry.
- The NetScreen-500 does not employ a maintenance interface or have a maintenance role.

- When in FIPS mode, the NetScreen-500 WebUI only displays options that comply with FIPS regulations.
- The output data path is logically disconnected from the circuitry and processes performing key generation, or key zeroization.
- The NetScreen-500 provides a Show Status service via the GET service.
- The NetScreen-500 cannot be accessed until the initialization process is complete.
- The NetScreen-500 implements the following power-up self-tests:

Device Specific Self-Tests:

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

Algorithm Self-Tests:

- DES, CBC mode, encrypt/decrypt KAT
- TDES, CBC mode, encrypt/decrypt KAT
- SHA-1 KAT
- RSA (encryption and signature)
- DSA Sign/Verify
- Exponentiation
- AES, CBC mode, encrypt/decrypt KAT
- HMAC-SHA-1
- ANSI X9.31 DRNG KAT

The NetScreen-500 implements the following conditional tests:

- DRNG continuous test
- Hardware RNG continuous test
- SCS key agreement test
- DH key agreement test
- DSA pair-wise consistency test
- RSA pair-wise consistency test
- Bypass test
- Firmware download DSA signature test (Software Load Test)

Other Parameters

Note the following:

- A pair-wise consistency test for the DH, DSA and RSA (encryption and signature) key-pairs is employed.
- The firmware can be loaded using the Trivial File Transfer Protocol (TFTP) or the PCMCIA port, where a firmware load test is performed via a DSA signature.
- Keys are generated using a FIPS approved pseudo random number generator per ANSI X9.31, Appendix C.
- 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.
- In FIPS mode, only FIPS-approved algorithms are used.
- The NetScreen-500 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. 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-500 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 has to be at least 6 characters.
- The operator must enter the user name and password. All logins through a TCP connection disconnect after three consecutive login failures, and an alarm is logged.
- A separate session is assigned to each successful administrator login.
- The password is not echoed during the administrator login.
- SCS uses 3DES encryption only.
- 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: (1) "set admin" and "unset admin". These two services allow the Crypto-Officer to create a new user, change a current user's user name and password, or delete an existing user. (2) "set FIPS enable" and "unset FIPS enable". These two services allow the Crypto-Officer to switch between FIPS mode and default mode.
- HTTP can come through the VPN only with AES encryption. The default page timeout is set to 10 minutes; this is user configurable. The maximum number of HTTP connections, i.e., 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 2048. This number is shared with other TCP connections.

- Telnet can come through the VPN with AES encryption only.
- There are a maximum of 22 sessions shared between Telnet and SCS.
- Upon a telnet or console login failure, the next prompt will not come up for an estimated 5 seconds.
- The NetScreen-500's chips are production-grade quality and include standard passivation techniques.
- The NetScreen-500 is contained within a metal production-grade enclosure.

Figure 1: Front of the NetScreen-500 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

- The source code is annotated with detailed comments.
- The Netscreen-500 does not use third party applications.
- The NetScreen-500 generates an Initial Vector (IV) using a FIPS approved pseudo random number generator for the beginning of a session. The IV is incremented by one for each packet belonging to this session.

- IKE, Diffie-Hellman (DH), and RSA encryption are employed for public key- based key distribution techniques, which are commercially available public key methods.
- The policy is associated with keys located in the modules. The private/public key pair of the module is located at a certain and exact memory location of the flash.
- All keys are stored in plain text.
- All keys and unprotected security parameters can be zeroized through the Unset,Clear and Delete commands, except the PRNG key.
- The NetScreen-500 does not perform key archiving.
- The NetScreen-500 includes the following algorithms:
    - FIPS Approved:

      DSA

      SHA-1

      TDES (CBC)

      DES (CBC) (for legacy systems only)

      AES (CBC)

      HMAC-SHA-1

      RSA Sign/Verify (PKCS #1)

      ANSI X9.31 DRNG
    - Non-FIPS Approved:

      MD5

      DH (key agreement)

      RSA Encrypt/Decrypt (used for key wrapping only)
- The NetScreen-500 conforms to FCC part 15, class A.
- 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 Juniper Networks 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, SCS key agreement 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 Juniper Networks 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, SCS can use 3DES only to encrypt/decrypt commands. Also if the command from SCS is to set or get the AES manual key, it will fail and a message is logged.
- HA traffic encryption is 256 bit AES.
- 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.

F. FIPS Certificate Verification

In FIPS mode, during the loading of the X509 certificate, if the signing CA certificate cannot be found in the NetScreen-500, the following message is displayed on the console:

> 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]?

Where x is one of (0, 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F).

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

G. Critical Security Parameter (CSP) Definitions

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

- IPSEC Manual Key: DES, TDES, and AES for user traffic encryption. It is from user input.
- IPSEC Session Key: DES, TDES, and AES for user traffic encryption. It is generated by the IKE key exchange.
- IKE Pre-Shared Key:User input data to generate IKE session key and SHA-1-HMAC key.

- IKE Session Key: DES, TDES, AES for peer-to-peer IKE message encryption.
- User Name and Password: Crypto-Officer and Users' user names and passwords.
- SCS Server/Host Key: RSA keypairs used in secure command shell (equivalent to SSH).
- SCS Session Key: Encryption key to encrypt telnet commands by using 3DES only.
- DSA Public Key: Firmware-download authentication key.
- HA Key: AES Encryption key for HA data.
- IKE DSA Key: DSA key pair used in IKE identity authentication.
- IKE RSA Key: RSA key pair used in IKE identity authentication.
- PRNG Algorithm Key: ANSI X9.31 algorithm key required to generate pseudo-random numbers. These items are stored in volatile RAM and in non-volatile flash memory.
- SHA-1-HMAC Key: IPSEC authentication key between end users, and IKE authentication between two peers.

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

The following matrix defines the set of services to the CSPs of the module, providing information on generation, destruction and usage. It also correlates 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 3: Crypto-Officer

CSP \ Services	Set	Unset	Clear/ Delete	Get	Exec	Save	Ping	Reset	Exit	Trace-route
IPSEC Manual Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IPSEC Session Key	G	D	N/A	U	N/A	N/A	N/A	D	N/A	N/A
IKE Pre-shared Key	G	D	N/A	U	G	U	N/A	N/A	N/A	N/A
IKE Session	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A

Key										
User Name and Password	G1	D2	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SCS Server/Host Key	G	D	D	U	G	U	N/A	D (Server Key)	N/A	N/A
SCS Session Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
DSA Public Key	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
HA Key	G	D	N/A	N/A	U	U	N/A	N/A	N/A	N/A
IKE DSA Key	N/A	D	N/A	N/A	G,D,U	N/A	N/A	N/A	N/A	N/A
IKE RSA 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
SHA-1-HMAC Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A

Table 4: User and VSYS User

CSP \ Services	Set	Unset	Clear/ Delete	Get	Exec	Save	Ping	Reset	Exit	Trace-route
IPSEC Manual Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IPSEC Session Key	G	D	N/A	U	N/A	N/A	N/A	D	N/A	N/A
IKE Pre-shared Key	G	D	N/A	U	G	U	N/A	N/A	N/A	N/A
IKE Session Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
User Name and Password	G3	N/A	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SCS Server/Host Key	G	D	D	U	G	U	N/A	D (Server Key)	N/A	N/A
SCS Session Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
DSA Public Key	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
HA Key	G	D	N/A	N/A	U	U	N/A	N/A	N/A	N/A
IKE DSA Key	N/A	D	N/A	N/A	G,D,U	N/A	N/A	N/A	N/A	N/A
IKE RSA 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
SHA-1-HMAC Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A

Table 5: Read-Only User and VSYS Read-Only User

CSP \ Services	Get	Ping	Exit	Trace-route
IPSEC Manual Key	U	N/A	N/A	N/A

IPSEC Session Key	U	N/A	N/A	N/A
IKE Pre-shared Key	U	N/A	N/A	N/A
IKE Session Key	N/A	N/A	N/A	N/A
User Name and Password	U	N/A	N/A	N/A
SCS Server/Host Key	U	N/A	N/A	N/A
SCS Session Key	N/A	N/A	N/A	N/A
DSA Public Key	N/A	N/A	N/A	N/A
HA Key	N/A	N/A	N/A	N/A
IKE DSA Key	N/A	N/A	N/A	N/A
IKE RSA Key	N/A	N/A	N/A	N/A
PRNG Algorithm Key	N/A	N/A	N/A	N/A
SHA-1-HMAC Key	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.

H. Definitions List

AES – Advance Encryption Standard
CLI – Command Line Interface
CSP – Critical Security Parameter
DES – Data Encryption Standard
DH – Diffie-Hellman
DRNG – Deterministic RNG
HA – High Availability
IPSec – Internet Protocol Security
IV – Initial Vector
KAT – Known Answer Test
NS – NetScreen
PRNG – Pseudo RNG
RNG – Random Number Generator
ROM – Read Only Memory
RSA – Rivest Shamir Adelman Algorithm
SCS – Structured Cabling System
SDRAM – Synchronous Dynamic Random Access Memory

TCP – Transmission Control Protocol
TFTP – Trivial File Transfer Protocol
VPN – Virtual Private Networking