

# *FIPS 140-2 SECURITY POLICY*

*Juniper Networks*

*NetScreen-5400*

HW P/N NS-5400 VERSION 3010 FW VERSIONS SCREENOS 5.0.0R9.H, SCREENOS 5.0.0R9A.H AND SCREENOS 5.0.0R9B.H

## Copyright Notice

Copyright © 2005 Juniper Networks, Inc. May be reproduced only in its original entirety [without revision].

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

## 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 ..... 4
- B. Security Level ..... 5
- C. Roles and Services ..... 5
- D. Interfaces ..... 6
- E. Setting FIPS mode ..... 8
- F. Other Parameters ..... 10
- G. FIPS Certificate Verification ..... 14
- H. Critical Security Parameter (CSP) Definitions ..... 14
- I. Public Key Definitions ..... 14
- J. Matrix Creation of Critical Security Parameter (CSP) versus the Services (Roles & Identity)..... 15
- K. Definitions List ..... 17

## A. Scope of Document

The Juniper Networks NetScreen-5400 is an internet security device that integrates firewall, virtual private networking (VPN) and traffic shaping functionalities. The model number is NetScreen-5400 and includes interface options listed in Table 1.

Part Number	Model	Interface Option	Power Supply
NS-5400-P00A-S00	NS-5400	2G24FE SPM	AC
NS-5400-P00D-S00	NS-5400	2G24FE SPM	DC
NS-5400-P01A-S00	NS-5400	8G SPM	AC
NS-5400-P01D-S00	NS-5400	8G SPM	DC
NS-5000-8G	8G SPM	-CARD ONLY-	N/A
NS-2G24FE	2G SPM	-CARD ONLY-	N/A

Table 1 – List of 5400 part numbers

Through the VPN, the NetScreen-5400 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)
- The use of RSA and DSA certificates

The NetScreen-5400 also provides an interface for users to configure or set policies through the console or network ports.

The general components of the NetScreen-5400 include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASICs (GigaScreen version 2 and GigaScreen II), 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-5400's physical configuration is defined as a multi-chip standalone module.

## B. Security Level

The NetScreen-5400 meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 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	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

## C. Roles and Services

TheNetScreen-5400 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-5400 provides the following services:

- Clear/Delete: Clear dynamic system info
- Exec: Exec system commands
- Exit: Exit command console
- Get: Get system information
- Ping: Ping other host
- Reset: Reset system
- Save: Save command
- Set: Configure system parameters
- Trace-route: Trace route
- Unset: Unconfigure system parameters

The NetScreen-5400 supports both role-based and identity-based authentication.

- All roles can be authenticated locally (within NS-5400); 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 User Role.

## D. Interfaces

- The NetScreen-5400 can accept up to three of two network interface cards.

The network interface card options are:

1. 8GSPM: The 8GSPM provides eight Gigabit Ethernet mini-Gigabit Interface Converter (GBIC) ports (labeled 1-8) using hot-swappable transceivers. The 8GSPM delivers up to 4 Gigabits per-second (Gbps) of firewall and up to 2 Gbps of Virtual Private Network (VPN) capacity.

2. The 2G24FE Secure Port Module (SPM) deploys two 1-Gigabit Ethernet ports (labeled 1,2) and 24 FE ports (labeled 1-24) with up to 2 Gbps of firewall and up to 1 Gbps of VPN process capacity. This total consists of one aggregate interface for the two 1-Gigabit ports, and five aggregate interfaces for the 24 10/100 Ethernet ports.

- Console port: RJ-45 interface for Control input and status output.
- Modem port: RJ-45. Disabled in FIPS mode.
- MGT port: Control input. 10/100 Mbps ethernet for management traffic. It has 2 link lights (LEDs) to indicate the port status. The right LED indicates the link status. If the LED is on, this means the link is up. If the LED is off, this means the link is down. The left LED indicates the ethernet activity. If the LED is on and is blinking, this means the port is active (transmitting/receiving data). If the LED is off, this means the port is inactive.
- HA1/HA2 port: For status output. Dual mini-GBIC ports for failover.
- Compact flash: Image input. Interface for a memory flash card.
- Power interface: For system power, AC or DC.
- The management module has six types of indicators, all for status output:
  - CPU utilization: Consists of an array of 5 LEDs that indicate the current level of CPU utilization. Utilization is defined as the amount of traffic detected on the interface at any given time. The CPU utilization LEDs represent the following percentages of utilization: 5%, 10%, 25%, 50%, and 90%. When all LEDs are dark, this indicates CPU utilization is less than 5%.
  - One Power status LED: Illuminates solid green when the power is supplied to the NetScreen-5400.
  - One Module status LED: Illuminates blinking green when the module is operational or amber when the unit is booting up.
  - System Alarm LED: Illuminates red when a critical alarm occurs, such as a hardware or software failure, or a firewall attack; illuminates amber when a major alarm occurs, such as "low memory;" is dark when there are no alarms.
  - HA LED: Illuminates green if the unit is the master, amber if the unit is the slave, and is dark if HA is not configured.
  - Compact Flash LED: Illuminates green if the compact flash card is installed in the compact flash slot, blinking green if the compact flash card is active, and is dark if the slot is empty.
- The secure port module has two LEDs, each for status output.
  - One power status LED: Illuminates solid green when the power is supplied to the NetScreen-5400.
  - One module status LED: Illuminates blinking green when the module is operational or amber when the unit is booting up.
- The fan tray has a status output LED: Illuminates solid green when the fan is operational, and is dark when it is not operational.

- Hardware reset button: After the user follows the sequence: insert for 5 seconds, release for 5 seconds, insert for 5 seconds, and release for 5 seconds, the device will erase all configurations and be restored to the default factory settings.

## 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. 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 "set FIPS-mode enable" through the CLI.

Special note for firmware upgrade: if a pre-5.0 firmware is upgraded to 5.0 FIPS version and above, even if the box is previously in FIPS mode, please re-enable FIPS again by issuing the commands "unset FIPS-mode enable," "set FIPS-mode enable," followed by rebooting the box.

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 management via Telnet, HTTP (WebUI) and NetScreen Security Manager (NSM) only through a VPN with 256-bit AES encryption
- Enforce management via SSH only when using 3DES
- Disable 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, NSM and HTTP (WEB UI) are allowed only through a VPN with 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 cryptographic 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 endorsed 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-5400 does not employ a maintenance interface or have a maintenance role.
- When in FIPS mode, the NetScreen-5400 WebUI only displays options that comply with the requirements of FIPS 140-2.
- The output data path is logically disconnected from the circuitry and processes performing key generation or key zeroization.
- The NetScreen-5400 provides a Show Status service via the GET service.
- The NetScreen-5400 cannot be accessed until the initialization process is complete.
- The NetScreen-5400 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 KAT

- TDES, CBC mode, encrypt/decrypt KAT
- SHA-1 KAT
- RSA (encryption and signature) KAT
- ANSI X9.31 DRNG KAT
- DSA Sign/Verify KAT
- AES, CBC mode, encrypt/decrypt KAT
- HMAC-SHA-1 KAT
- DH key agreement test
- The NetScreen-5400 implements the following conditional 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)
- The internal packaging cannot show damage or evidence of tampering. The plastic bag should not have a large hole and the label that seals the plastic bag should not be detached or missing. If the bag or the seal are damaged in any way, this may be evidence of tampering

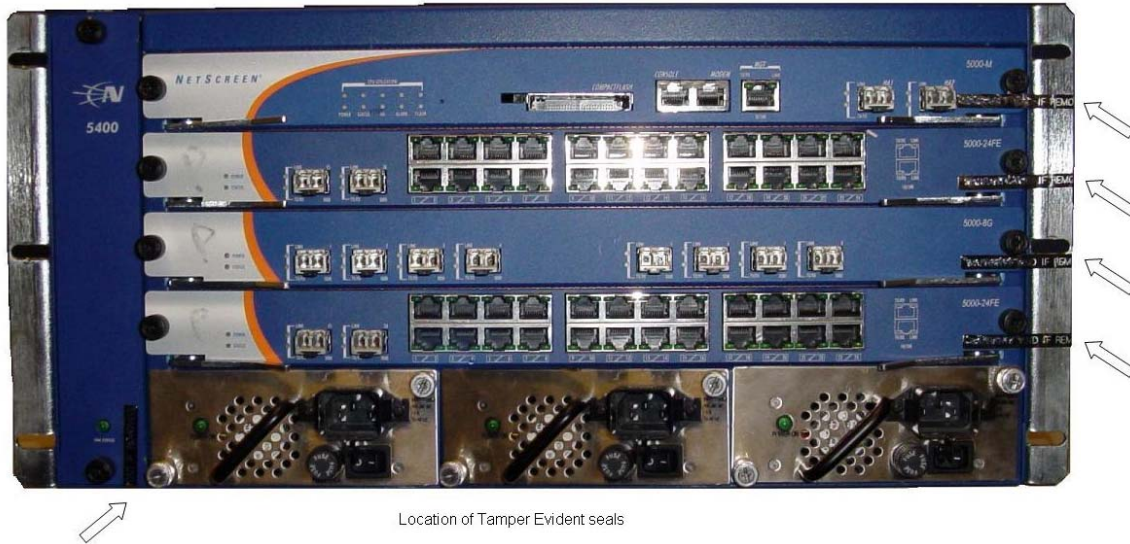
## F. Other Parameters

Also note that:

- The firmware can be loaded through the 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-5400 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-5400 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.

- 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 first time an operator logs on to the module, the operator uses the default user name and password, which are both "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 only come through a VPN with AES encryption. The default page time-out is 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.
- There are a maximum of 22 sessions shared between Telnet and SSH.
- Upon a Telnet and console login failure, the next prompt will not come up for an estimated 5 seconds.
- The NetScreen-5400's chips are production-grade quality and include standard passivation techniques.
- The NetScreen-5400 is contained within a metal production-grade enclosure.



**Figure 1: Tamper Evident Mechanisms, Front of the NetScreen-5400**

- The enclosures are opaque to visible spectrum radiation.
- The enclosure includes a removable cover and is protected by tamper evident seals. These seals also cover the power block at the back and front of the units. The locations of the tamper evident seals are shown in Figure 1.
- 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.
- The NetScreen-5400 includes the following algorithms:
  - 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-5400 conforms to FCC part 15, class A.
- Upon the 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.
- Upon the 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 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, 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 will be logged.
- A VPN with AES encryption is manual key or IKE.
- HA traffic encryption is 256 bit AES.
- If a VPN uses 3DES Encryption, the key exchange protocol IKE is enforced to use group 5 only.
- SHA-1 algorithm on GigaScreen II has the limitation that it cannot hash more than 8K of data. Other ASIC chips have no such limitation.
- 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, during the loading of the X509 certificate, if the signing CA certificate cannot be found in the NetScreen-5400, 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.

## 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.
- HA Key: AES Encryption key for HA data.
- 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 matrixes 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 3: 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
HA Key	G	D	N/A	N/A	U	U	N/A	N/A	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 4: User and VSYS User

**User and VSYS 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
HA Key	G	D	N/A	N/A	U	U	N/A	N/A	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 5: Read-Only User and VSYS Read-Only User

**Read-Only User and VSYS 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
HA 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  
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  
SDRAM – Synchronous Dynamic Random Access Memory  
SSH – Secure Shell  
TCP – Transmission Control Protocol  
TFTP – Trivial File Transfer Protocol  
VPN – Virtual Private Networking