FIPS 140-2 SECURITY POLICY

Juniper Networks, Inc.

SSG 520M and SSG 550M

HW P/N SSG-520M-SH, SSG-520M-SH-N, SSG-520M-SH-DC-N, SSG-520M-N-TAA, SSG-520M-SH-DC-N-TAA, SSG-550M-SH, SSG-550M-SH-N, SSG-550M-SH-DC-N, SSG-550M-N-TAA, SSG-550M-SH-DC-N-TAA
FW Version ScreenOS 6.3.0r6

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 JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

TABLE OF CONTENTS

Overview

The SSG 500 Series consists of high-performance security platforms for regional branch office and medium-sized, standalone businesses that want to stop internal and external attacks, prevent unauthorized access and achieve regulatory compliance. The SSG 550/ SSG 550M provides 1+ Gbps of stateful firewall performance and 600 Mbps of IPSec VPN performance, while the SSG 520/SSG 520M provides 650 Mbps of stateful firewall performance and 300 Mbps of IPSec VPN performance.

The general components of the SSG 520M and 550M include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC (Cavium Nitrox), 10/100 Mbps Ethernet interface, console interface, midplane and power supply.

The entire case is defined as the cryptographic boundary of the module. The SSG 500 series physical configuration is defined as a multi-chip standalone module. The chips are production-grade quality and include standard passivation techniques. The SSG 500 series conforms to FCC part 15, class B.

Fig. 1: SSG 520M

Fig. 2: SSG 550M

Validation Level

The following table lists the validation level for each FIPS 140-2 area.

Table 1: Module Validation Level

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

Roles and Services

The security appliance supports three distinct roles:

- **Cryptographic Officer (Root):** The device allows one Crypto-Officer. This role is assigned to the first operator who logs on to the device using the default admin name and password (netscreen, netscreen). Only the Crypto-Officer can create other administrators, change the device to operate in FIPS mode and apply the tamper-evident seals.
- **User (Admin):** This role can configure specific security policies. These policies provide the device with information on how to operate. For example, configuring access policies and VPN encryption with Triple-DES). This role does not have the ability to create other administrators.
- **Read-Only User (Admin):** This role can only perform a limited set of services to retrieve information or status. This role cannot perform services to configure the device.

The security appliance offers the following services:

- **Configuration:** Configure firewall policies (including the bypass service), VPN encryption and digital signature options, network interface options, routing tables, protocol support, authentication servers, logging options and system time. Clear dynamic system information such as statistics or VPN security associations.
- **Status:** View firewall policies, VPN configuration, traffic and performance statistics, firmware version, network interface status and system logs. Perform ping and trace-route.
- **Zeroize:** Overwrite all CSP values with three alternating bit patterns, then reset the configuration to the factory default values. Also occurs when placing the device into or removing it from FIPS mode.
- **Manage:** Create new users.
- **Self-tests:** Invoke cryptographic algorithm and system integrity self-tests.

The module allows concurrent Admin users, either User or Read-Only User roles. It provides the following services for each role:

Table 2: Roles and services summary

Service	Cryptographic Officer	User	Read-only User
Configure	Y	Y	N
Status	Y	Y	Y
Zeroize	Y	N	N
Manage	Y	N	N
Self-Tests	Y	Y	N
Tamper Seals	Y	N	N

The device does not employ a maintenance interface or have a maintenance role.

Authentication

The security appliance supports identity-based authentication. Operators must be authenticated using user names and passwords. All operators can be authenticated locally (within the security appliance). Based on his identity, an operator assumes the correct role.

The module supports identity-based authentication through the local database for the Cryptographic Officer Role, the User Role, and the Read-Only User Role.

In order for authentication data to be protected against disclosure, substitution and modification, passwords are not echoed during entry. A separate session is assigned to each successful administrator login. On power down, previous authentications are erased from memory and need to be re-authenticated again on power-up.

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.

Strength of Authentication

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. This also applies to the RADIUS shared secret, as well as authentication through the SSH protected channel.

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. Since a user is locked our after three contiguous login failures, the random success rate per minute is $1/(62^6) + 1/ (62^6) + 1/(62^6) = 3/(62^6)$, which is far less than 1/100,000.

Interfaces

The SSG 520M and SSG 550M provide a number of interfaces:

- Four Ethernet autosensing interfaces (RJ-45) (Data Input, Data Output, Control IN, Status OUT). These interfaces are network ports. Each port has two LEDs that indicate port status:

Table 3: SSG 520M and 550M Ethernet Port LEDs

Name	Color	State	Description
Status (left)	Green	Steady	Link up
		Off	Link down
TX/RX (right)	Green	Blinking	Indicates that traffic is passing through
		Off	Indicates that no traffic is passing through.

- Console port – RJ-45 serial port connector (Data Input, Data Output, Status IN, Control OUT). This port allows initial access to the Command Line Interface (CLI).
- Modem port – RJ-45 serial port connector. Disabled in FIPS mode.
- Power interface: AC or DC.
- The module has four status LEDs:

Table 4: Device Status LEDs

Name	Color	State	Description
Power	Green	Steady	Indicates that the unit is receiving power
		Off	Indicates that the unit is not receiving power
Status	Green	Off	Indicates that the system is starting or is powered off.
		Blinking	Indicates that the device is operating normally.
Alarm		Off	No alarm
	Amber	Steady	Major alarm: • Low memory (less than 10% remaining). • High CPU utilization (more than 90% in use). • Session full. • Maximum number of VPN tunnels reached. • HA status changed or redundant group member not found.
	Red	Steady	Critical alarm: • Failure of hardware component or software module. • Firewall attacks detected.
HA (High Availability)	Green	Steady	Unit is the primary (master) device.

	Amber	Steady	Unit is the secondary (backup) device.
		Off	HA is not enabled.

- 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).
- The SSG 520M and SSG 550M have six physical interface module (PIM) slots.
- Both modules were validated using only the fixed ethernet interfaces on the chassis.

Operation In FIPS Mode

Initial configuration

Connecting to the device

The security appliance provides an interface for an operator to configure the device through the Console or Network ports. For initial configuration, the operator must directly connect a VT-100 terminal or a non-networked device that can emulate a VT-100 terminal to the Console port via a serial cable.

By default, the security appliance is in non-FIPS mode on the first power-up. The first time an operator logs on to the appliance, the operator uses the default user name and password which is “netscreen”, “netscreen”. This user is assigned the Crypto-Officer role.

Once the device is operating in FIPS mode, the operator should perform the minimum configuration necessary to establish a management connection via SSH (i.e. configure a network interface and enable SSH management through that interface), then disable the console connection using the **set console disable** CLI command. If the console is re-enabled in FIPS mode, the device will automatically zeroize itself and return to non-FIPS mode.

Loading and authenticating firmware

Prior to placing the device in FIPS mode, the administrator must load the Juniper firmware authentication DSA public key, **imagekey.cer**, using the **save image-key** CLI command. When this public key is present on the device, the integrity and authenticity of the firmware is checked at system start and when firmware is loaded. If the DSA signature appended to the firmware is verified, the device allows it to be loaded.

If the device is not already running a FIPS validated version of the firmware, the administrator should load it using the **save software** CLI command. Loading a new version of firmware completely replaces any existing firmware.

The firmware is signed by a well-protected 1024 bit modulus DSA private key, which provides 80 bits of security. 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 signature.

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 $1/(2^{80}) + 1/(2^{80}) + 1/(2^{80}) = 3/(2^{80})$, which is far less than 1/100,000.

Enabling FIPS mode

The module can be set to FIPS mode only through the CLI. To set the module to FIPS mode, execute the **set FIPS-mode enable** command through the CLI. This command will zeroize and reset the device. When prompted, confirm that the configuration should be saved and the device reset.

Determining the current mode

To check whether the device is in FIPS mode, enter the **get system** CLI command:

```
ns-> get system
Product Name: ns5200
Serial Number: 0099122004000991, Control Number: 00000000, Mode: FIPS
Hardware Version: 0110(0)-(12), FPGA checksum: 00000000, VLAN1 IP (0.0.0.0)
Software Version: 6.3.0r6.0, Type: Firewall+VPN
Base Mac: 0010.db90.f770
File Name: ns5200.6.3.0r6.0, Checksum: 48e3d429
```

The current mode appears on the second line of the output.

Operating restrictions in FIPS mode

The security appliance automatically imposes the following restrictions when operating in FIPS mode:

- Disables administration via SSL
- Disables the import or export of configuration files
- Disables the SNMP Read-Write community
- Disables the USB and Modem ports
- Forces management via Telnet, HTTP (WebUI) and NetScreen Security Manager (NSM) only through a VPN with 256-bit AES encryption
- Forces SSHv2 management traffic to use Triple-DES encryption. (SSHv1 is disabled.)
- Disables the MD5 and DES algorithms
- Requires HA encryption to 256-bit AES.
- If a VPN is configured to use Triple-DES encryption, Diffie-Hellman Group 5 is required for key agreement. DH groups 1 and 2 are disabled.
- Prevents the operator from configuring a VPN whose strength is stronger then the security provided by the management connection:
    - For sessions via a directly connected serial cable, no strength restriction is applied.
    - For remote SSH connections (which are protected by Triple-DES encryption), the strength of the management connection is considered to be 112 bits. Therefore, the operator is prevented from configuring a VPN whose encryption algorithm has a strength greater than 112 bits, e.g. 128, 192 or 256 bit AES.
    - For remote telnet, WebUI or NSM connections, no strength restriction is applied, since these connections are already forced to pass through a 256-bit AES VPN.

Security rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

The cryptographic module provides identity-based authentication. Until the operator has been authenticated to the module to assume a valid role, the operator does not have access to any cryptographic services.

Data output is inhibited during key generation, self-tests, zeroization, and error states. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module. The module does not support a maintenance mode.

The module performs key agreement as per the guidelines in NIST SP 800-57.

Self tests

The security appliance implements the following power-up self-tests:

- Device Specific Self-Tests:
  - Boot ROM firmware self-test via DSA signature (Firmware Integrity Test)
- Critical Function Self-Tests:
  - SDRAM read/write check
  - FLASH test
- Algorithm Self-Tests:
  - Triple-DES, CBC mode, encrypt/decrypt KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - RSA (encrypt/decrypt and sign/verify) KAT
  - DSA Sign/Verify pairwise consistency test
  - ECDSA Sign/Verify pairwise consistency test
  - AES, CBC mode, encrypt/decrypt KAT
  - HMAC SHA-1 KAT, HMAC SHA-256 KAT
  - ANSI X9.31 DRNG KAT
  - RNG statistical (monobit, poker, runs and long runs) tests
  - DH exponentiation test
  - IKE v1/v2 Key Derivation Function KAT

The security appliance implements the following conditional tests:

- DRNG continuous test (both approved and non-approved RNG's)
- DSA pairwise consistency test
- ECDSA pairwise consistency test
- RSA pairwise consistency test
- Bypass test
- Firmware download DSA signature test (Firmware Load Test)
- DH pairwise consistency test
- Public key validation test

On failure of any self-test, the module enters and stays in a permanent error state with the following characteristics:

- The console displays an error message of the format: “XXX test failed: error code N”.
- The status LED flashes red.
- All traffic processing halts.

The module must be power cycled to return to operation.

Bypass tests are performed as a conditional test. The bypass state occurs when the administrator configures the module with a non-VPN policy and an incoming packet whose source address, destination address and service 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.

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.

At any time the cryptographic module is in an idle state, the operator may command the device to perform the self-tests.

FIPS Approved Algorithms

The following FIPS approved algorithms are supported by the security appliance:

- DSA , ECDSA Sign Verify
- SHA-1, SHA-256
- Triple-DES (CBC)
- AES (CBC)
- HMAC-SHA-1, HMAC-SHA-256
- RSA Sign/Verify (PKCS #1)
- ANSI X9.31 DRNG

The module supports the following communication protocols which are allowed in FIPS mode:

- SSL v3.1
- SSH v2
- IPSec

Non-FIPS Approved Algorithms

The following non-approved algorithms are allowed in FIPS mode:

- DH (key agreement, key establishment methodology provides 97 or 112 bits of strength)
- Elliptic Curve Diffie-Hellman (key establishment methodology provides 128 bits of strength)

- NDRNG

The following non-approved algorithms/protocols are disabled in FIPS mode:

- RSA encryption/decryption
- DES
- MD5
- SNMP v3

Zeroization

All keys and unprotected security parameters can be individually zeroized through the Unset, Clear, Delete, and Reset commands. Pressing the hardware reset button or issuing the **unset vendor-def** CLI command will cause the zeroization of all CSPs by reseting the device configuration to the factory default values.

Physical Security Policy

Before carrying out any steps to deploy a Juniper Networks security appliance, the end-user must verify the security of the product with the following observations:

1. Confirm that the product received matches the version that is validated as FIPS 140-2 compliant.

2. The outside packaging does not show damage or evidence that is has been opened. If the cardboard shows damage that would allow the device to be removed or exchanged, this may be evidence of tampering.

3. Each box is packaged with custom tape to indicate that the device was packaged by Juniper Networks or an authorized manufacturer. The tape is unique, with the words *Juniper Networks* printed repeatedly along the tape. If the tape is not present, the device may have been tampered with.

4. The internal packaging does not 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 seal are damaged in any way, the device may have been tampered with.

The security appliance is contained within a metal production-grade enclosure that is opaque to visible spectrum radiation. The enclosure includes a removable cover that must be protected by a tamper-evident seal.

The Cryptographic Officer is responsible for securing and having control at all times of any unused seals and the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

Tamper seals are applied in the same fashion regardless of the part number of the device.

Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper labels, opaque metal enclosure.	Upon receipt of the module and per security policy by the Cryptographic Officer.	Labels should be free of any tamper evidence.

Seals are available for order via part number JNPR-FIPS-TAMPER-LBLS. If a seal is missing or damaged, the device may have been tampered with. Tamper-evident seals should be applied as described below.

For all seal applications, the Cryptographic Officer should observe the following instructions.

- Handle the seals with care. Do not touch the adhesive side.
- All surfaces to which the seals are to be applied must be prepared by sanding lightly with 200 grit sandpaper to roughen the surface. Use an alcohol wipe to ensure that all surfaces are clean and clear of any residue.
- Apply with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

- If a seal must be removed, the surface should be prepared as described above prior to the application of a replacement seal.

Figure 3: Front of the SSG 520M and 550M devices

Figure 4: Rear detail of the SSG 520M

Figure 5: Rear detail of the SSG 550M device

Figure 6: Rear corner of the SSG 520M and 550M

Tamper-evident seals (14 for the SSG 520M, 13 for the SSG 550M) should be applied to:

- The front of the device as shown in Figure 3:
  - Label #1 applied vertically from the top of the chassis across the left edges of the slot covers numbered 1 and 2.
  - Label #2 applied vertically, overlapping with the last ¼ inch of label #1, covering the slot covers numbered 2 and 3, extending on to the front of the chassis.
  - Label #3 applied vertically from the top of the chassis across the right edges of the slot covers numered 1 and 2.
  - Label #4 applied vertically, overlapping with the last ¼ inch of label #3, covering the slot covers numbered 2 and 3, extending on to the front of the chassis.
  - Label #5 applied vertically from the top of the chassis across the left edges of the slot covers numbered 4 and 5.
  - Label #6 applied vertically, overlapping with the last ¼ inch of label #5, covering the slot covers numbered 5 and 6, extending on to the front of the chassis.
  - Label #7 applied vertically from the top of the chassis across the right edges of the slot covers numered 4 and 5.
  - Label #8 applied vertically, overlapping with the last ¼ inch of label #7, covering the slot covers numbered 5 and 6, extending on to the front of the chassis.
  - Label #9 applied horizontally from the left side of the chassis, extending toward the center of the removable ventilation cover.
  - Label #10 applied horizontally, extending across the right edge of the removable ventilation cover and on to the front of the chassis.
  - Label #11 applied horizontally to overlap labels numbered 9 and 10.
- The rear of the device:
  - For the SSG 520M, as shown in figure 4:
    - Label #12 applied vertically from the top of the removable cover extending on to the center of the power supply.
    - Label #13 applied vertically across the screw to the left of the power supply fan.
  - For the SSG 550M, as shown in figure 5:

- Label #12 applied vertically from the power supply cover extending on to the removable cover.

- The top of the removable cover, extending on to the side of the chassis opposite the power supply, as shown in figure 6. For the SSG 520M, this is label #14. For the SSG 550M, this is label #13.

The removable cover on both the SSG520M and SSG550M is a single piece covering the top of the unit and is fastened to the chassis by multiple retaining screws. Figure 7 depicts the device with the tamper seals removed and the cover partially removed. Please note that there are no user serviceable components inside the device.

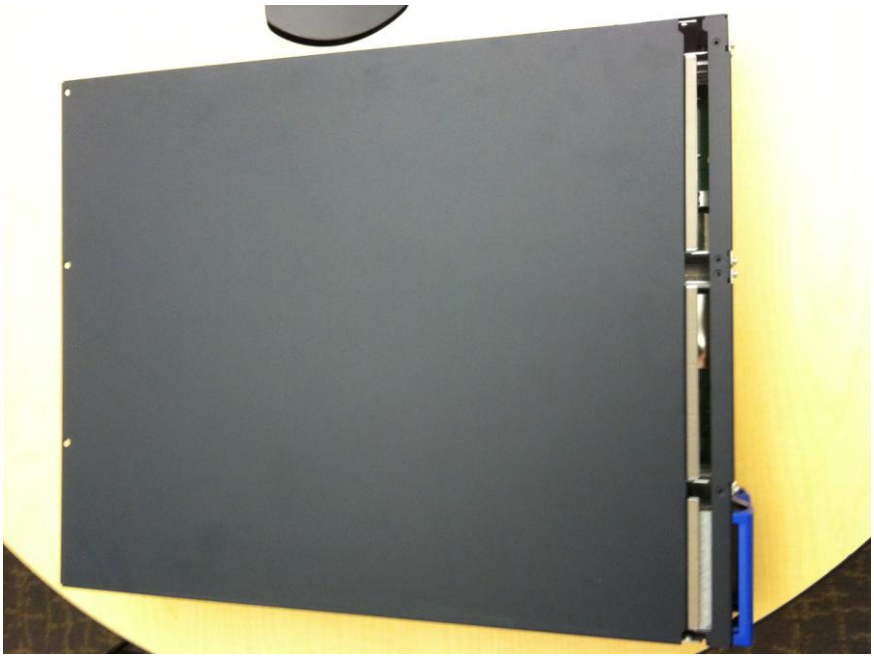

Figure 7: SSG 350M with the cover slid back

Cryptographic Algorithm Validation

Cryptographic algorithm validation certificate numbers for are listed in the table below:

Table 7: Algorithm Validation Certificates

Algorithm	Certificate Number
TDES	1063
AES	1622
DSA	509
SHA	1431
RNG	870
RSA	800
HMAC	953
ECDSA	207

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**: Triple-DES, 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**: Triple-DES, 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**: Triple-DES 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/ECDSA Private Key**: RSA/DSA/ECDSA key used in IKE identity authentication.
- **Diffie Hellman Private Key Components**: Used during the DH key agreement protocol.
- **PRNG Seed and Seed Key**: Used during the ANSI X9.31 generation of pseudo random numbers.
- **RADIUS Secret Key**: Used to authenticate exchanges with the RADIUS server

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/ECDSA 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.

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

The following matrices define the set of services to the CSP 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 A: Crypto-Officer

CSP \ Services	Configure	Status	Zeroize	Manage	Self-test
IPSEC HMAC SHA-1 Key	GD	U	D	N/A	N/A
IPSEC ESP Key	GD	U	D	N/A	N/A
IKE Pre-shared Key	GD	U	D	N/A	N/A
IKE Encryption Key	D	N/A	D	N/A	N/A
IKE HMAC SHA-1 Key	D	N/A	D	N/A	N/A
Password	G[1] D[2]	U	D	GD	N/A
SSH Server/Host DSA Private Key	GD	U	D	N/A	N/A
SSH Encryption Key	D	N/A	D	N/A	N/A
SSH HMAC SHA-1 Key	D	N/A	D	N/A	N/A
HA Key	GD	N/A	D	N/A	N/A
IKE RSA/DSA/ECDSA Private Key	GD	N/A	D	N/A	N/A
PRNG Seed and Seed Key	G	N/A	D	N/A	N/A
Diffie Hellman Private Key Components	G	N/A	D	N/A	N/A
RADIUS Secret Key	GD	U	G	N/A	N/A

Table B: User

CSP \ Services	Configure	Status	Self-test
IPSEC HMAC SHA-1 Key	GD	U	N/A
IPSEC ESP Key	GD	U	N/A
IKE Pre-shared Key	GD	U	N/A
IKE Encryption Key	D	N/A	N/A
IKE HMAC SHA-1 Key	D	N/A	N/A
Password	G[1] D	U	N/A
SSH Server/Host DSA Private Key	GD	U	N/A
SSH Encryption Key	D	N/A	N/A
SSH HMAC SHA-1 Key	D	N/A	N/A
HA Key	GD	N/A	N/A
IKE RSA/DSA/ECDSA Private Key	GD	N/A	N/A
PRNG Seed and Seed Key	G	N/A	N/A
Diffie Hellman Private Key Components	G	N/A	N/A
RADIUS Secret Key	GD	U	N/A

Table C: Read-Only User

CSP \ Services	Status
IPSEC HMAC SHA-1 Key	U
IPSEC ESP Key	U
IKE Pre-shared Key	U
IKE Encryption Key	N/A
IKE HMAC SHA-1 Key	N/A
Password	U
SSH Server/Host DSA Private Key	U
SSH Encryption Key	N/A
SSH HMAC SHA-1 Key	N/A
HA Key	N/A
IKE RSA/DSA/ECDSA Private Key	N/A
PRNG Seed and Seed Key	N/A
Diffie Hellman Private Key Components	N/A
RADIUS Secret Key	U

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.

Table D: How Keys Are Generated

CSP	Method of Generation
IPSEC HMAC SHA-1 Key	May be either entered directly at the CLI by the administrator, or generated internally via ANSI X9.31 RNG as a result of IKE protocol exchanges.
IPSEC ESP Key	“
IKE Pre-shared Key	Entered directly at the CLI by administrator
IKE Encryption Key	Internally via ANSI X9.31 RNG, as a result of IKE protocol exchanges
IKE HMAC SHA-1 Key	“
Password	Entered directly at the CLI by administrator
SSH Server/Host DSA Private Key	Internally via ANSI X9.31 RNG when DSA key-pair is generated.
SSH Encryption Key	Internally via ANSI X9.31 RNG, as a result of Diffie-Hellman key exchange during SSH session establishment.
SSH HMAC SHA-1 Key	“
HA Key	Entered directly at the CLI by administrator
IKE RSA/DSA/ECDSA Private Key	Internally via ANSI X9.31 RNG
Diffie Hellman Private Key Components	“
PRNG Seed and Seed Key	Initial generation via entropy gathered from a variety of internal sources.
RADIUS Secret Key	Entered directly at the CLI by administrator

Mitigation of Other Attacks Policy

The module is not designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

Definitions List

AES – Advanced Encryption Standard
CLI – Command Line Interface
CSP – Critical Security Parameter
DES – Data Encryption Standard
DH – Diffie-Hellman
DRNG – Deterministic RNG
GBIC - Gigabit Interface Converter
HA – High Availability
IPSec – Internet Protocol Security
IV – Initialization Vector
KAT – Known Answer Test
NS – NetScreen
NSM – NetScreen Security Manager
PIM - Physical Interface Module
PRNG – Pseudo RNG
RNG – Random Number Generator
ROM – Read Only Memory
RSA – Rivest Shamir Adelman Algorithm
SA – Security Association
SDRAM – Synchronous Dynamic Random Access Memory
SSH – Secure Shell protocol
TCP – Transmission Control Protocol
TFTP – Trivial File Transfer Protocol
VPN – Virtual Private Networking
VSYS – Virtual System