

FIPS 140-2 Security Policy

Juniper Networks

Netscreen-5200

VERSION 5.0.0r9 P/N 093-1395-000 REV. E

Copyright Notice

Copyright © 2005 Juniper Networks, Inc. All rights reserved.

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.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

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.....	5
B. SECURITY LEVEL	6
C. ROLES AND SERVICES	6
D. INTERFACES.....	8
E. SETTING FIPS MODE.....	10
F. FIPS CERTIFICATE VERIFICATION.....	12
G. CRITICAL SECURITY PARAMETER (CSP) DEFINITIONS.....	12
H. MATRIX CREATION OF CRITICAL SECURITY PARAMETER (CSP) VERSUS THE SERVICES (ROLES & IDENTITY).....	13
I. OTHER PARAMETERS	15
J. ACCRONYM LIST.....	19

A. SCOPE OF DOCUMENT

The Juniper Networks NetScreen-5200 is an internet security device that integrates firewall, virtual private networking (VPN), and traffic-shaping functionalities. The model number is NetScreen-5200 and includes the interface options listed in Table 1.

Table 1: List of Netscreen-5200 Part Numbers

Part Number	Model	Interface Option	Power Supply
NS-5200-P00A-S00	NS-5200	2G24FE SPM	AC
NS-5200-P00D-S00	NS-5200	2G24FE SPM	DC
NS-5200-P01A-S00	NS-5200	8G SPM	AC
NS-5200-P01D-S00	NS-5200	8G SPM	DC
NS-5000-8G	8G SPM	-CARD ONLY-	N/A
NS-2G24FE	2G SPM	-CARD ONLY-	N/A

Through the VPN, the NetScreen-5200 provides the following:

- IPSec standard security
- Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES) key management
- Manual and automated IKE (ISAKMP)
- Use of RSA and DSA certificates

The NetScreen-5200 also provides an interface for users to configure or set policies through the console or network ports.

The general components of the NetScreen-5200 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 device is defined as the cryptographic boundary of the modules. The physical configuration of the NetScreen-5200 is defined as a multi-chip standalone device.

B. SECURITY LEVEL

The NetScreen-5200 meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 2: Device 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

The NetScreen-5200 supports five 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 and change the device to operate in FIPS mode.
- **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.
- **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.
- **VSYS User:** This role has the same operations as the User, listed previously, except that a VSYS User only operates within a particular virtual system. See the *NetScreen Concepts & Examples ScreenOS Reference Guide* for more information about virtual systems.
- **VSYS Read-Only User:** This role has the same operations as the Read-Only User, listed previously, except that a VSYS Read-Only User only operates within a particular virtual system. See the *NetScreen Concepts & Examples ScreenOS Reference Guide* for more information about virtual systems.

The device allows concurrent Admin users, either in User or Read-Only User roles.

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 or read-only roles. 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-5200 provides the following services:

- Clear/Delete: Clear dynamic system info
- Execute: Execute system commands
- Exit: Exit command console
- Get (Show Status): Display 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
- Network Traffic: The VPN and networking services available to an operator
- Unset: Unconfigure system parameters. The NetScreen-5200 support both role-based and identity-based authentication.
- Role-based authentication provides an admin name and a password, but the actual authentication occurs at a RADIUS server. This is only available to User Role (Admin).
- All other forms of authentication (local database) are classified as identity-based.
- The device supports identity-based authentication for the Crypto-Officer Role (local database), the User Role (local database), and the Read-Only Role (local database).

D. INTERFACES

The NetScreen-5200 can accept one of two network interface cards.

The network interface card options are:

- **8GSPM:** The 8G Secure Port Module (SPM) 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.
- **2G24FE:** The 2G24 Fast Ethernet (FE) 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.

The NetScreen-5200 provides a number of interfaces:

- **Console port:** RJ-45 interface for Control input and status output.
- **Modem port:** RJ-45 serial port connector. This port is 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 adapter:** For system power, AC or DC.

Table 3: Six General LEDs

LED	Purpose	Color	Meaning
CPU Utilization	System CPU Utilization	Green	Consists of an array of five LEDs that indicate the current level of CPU utilization. Utilization is defined as the amount of traffic detected on the device at any given time. The CPU utilization LEDs represent the following percentages of possible utilization: 5%, 10%, 25%, 50%, and 90%.
		Off	When all are off, there is less than 5% CPU usage.
POWER	System Power	Green	Indicates the system is receiving power.
		Red	Indicates there is an error with the power.
		Off	Indicates the system is not receiving power.

LED	Purpose	Color	Meaning
STATUS	System Status	Blinking amber	Indicates the system is booting up
		Blinking green	Indicates the system is operational
ALARM	System Alarm	Red	Indicates a critical alarm, for example failure of hardware component or software device (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
		Off	No alarm
HA	High Availability	Green	Unit is the master device
		Blinking green	Redundant group member cannot be found
		Amber	Unit is the backup device
		Off	HA is not configured
FLASH	Flash Memory Card	Green	Indicates flash card is installed
		Blinking green	Indicates flash card is active
		Off	Indicates that the flash card slot is empty

- The SPM has two Status LEDs:
 - **Power:** Illuminates solid green when the power is supplied to the NetScreen-5200.
 - **Module:** Illuminates blinking green when the module is operational or amber when the unit is booting up.
 - **Fan Status LED:** Illuminates solid green when the fan is operational, and is off when it is not operational.
 - **Hardware reset button:** After the user follows the reset device sequence, the device erases all configurations and is restored to its default factory settings.

E. SETTING FIPS MODE

By default, FIPS mode is disabled.

For firmware upgrading: If pre-5.0 firmware is upgraded to FIPS version 5.0 or higher, you must reset the device to run in FIPS mode. You must do this even if the device was previously set to run in FIPS mode.

The commands **get config** and **get system** display which mode is running on the device.

The device can be set to FIPS mode only through the CLI.

To set the device to run in FIPS mode, do the following:

1. Type **set FIPS-mode enable** at the command prompt.

This command performs the following:

- Disables administration through SSL
- Disables the loading and output of the configuration file from the TFTP server
- Disables the Global reporting agent
- Disables administration through SNMP
- Disables the debug service
- Disables the modem port
- Enforces HTTP only through VPN with AES encryption
- Enforces Telnet only through VPN with AES encryption
- Enforces SSH to use only Triple-DES to manage the box
- Disables the MD5 algorithm

2. Type **save** at the command prompt.

3. Type **reset** at the command prompt.

Note the following:

- Configure the HA encryption key before using the HA link.
- Telnet and HTTP (WebUI) 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.
- Admin 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 is 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 are dropped for one minute.

- If there are multiple login failure retries within one minute and since the user is locked out after three continuous 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 $1/(2320)$, which is far less than $1/1,000,000$.
- The image download takes at least 23 seconds, so there can be no more than three download tries within one minute. The random success rate for multiple retries is $1/(2320) + 1/(2320) + 1/(2320) = 3/(2320)$, 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-5200 does not employ a maintenance interface or have a maintenance role.
- When in FIPS mode, the NetScreen-5200 WebUI only displays options that comply with FIPS regulations.
- The output data path is disconnected from the circuitry and processes performing key generation or key zeroization.
- The NetScreen-5200 provides a Show Status service when using the **get** CLI command.
- The NetScreen-5200 cannot be accessed until the initialization process is complete.
- The NetScreen-5200 implements the following startup self-tests:

Device Specific Self-Tests:

- Boot ROM firmware-self-test is via DSA signature
- SDRAM read/write check
- FLASH test

Algorithm Self-Tests:

- DES, CBC mode, encrypt/decrypt (for legacy systems only)
- Triple-DES, CBC mode, encrypt/decrypt
- SHA-1
- RSA (encryption and signature)
- DSA Sign/Verify
- Exponentiation
- AES, CBC mode, encrypt/decrypt
- SHA-1-HMAC
- Bypass test
- ANSI X9.31 KAT

The NetScreen-5200 implements the following conditional tests:

- PRNG continuous test
- Hardware RNG continuous test
- SSH key agreement test
- DH key agreement test
- DSA pair-wise consistency test
- RSA pair-wise consistency test
- Bypass test
- Firmware download DSA signature test

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-5200, the following message is displayed on the console, 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.

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. This key is generated by the user's input.
- **IPSEC Session Key:** DES, TDES, and AES for user traffic encryption. This key 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.
- **Admin Name and Password:** Crypto-Officer and Users' admin names and passwords.
- **SSH Server/Host Key:** RSA key pairs used in secure command shell.
- **SSH Session Key:** Encryption key to encrypt Telnet commands by using Triple-DES 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.

H. 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 device, providing information on generation, destruction, and usage. It also correlates the User and 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 4: 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 Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
Admin Name and Password	G ¹	D ²	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SSH Server/Host Key	G	D	D	U	G	U	N/A	D	N/A	N/A
SSH 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

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

² The Crypto-Officer is authorized to remove all authorized operators.

CSP \ Services	Set	Unset	Clear/ Delete	Get	Exec	Save	Ping	Reset	Exit	Trace-route
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: User and VSYS User Roles

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
Admin Name and Password	G ³	N/A	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SSH Server/Host Key	G	D	D	U	G	U	N/A	D	N/A	N/A
SSH 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 6: Read-Only and VSYS Read-Only User Roles

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
Admin Name and Password	U	N/A	N/A	N/A
SSH Server/Host Key	U	N/A	N/A	N/A
SSH 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

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

CSP \ Services	Get	Ping	Exit	Trace-route
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

I. OTHER PARAMETERS

Note the following:

- A pair-wise consistency test for DH, DSA, and RSA (encryption and signature) key-pairs is employed.
- The firmware can be loaded through 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 device'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-5200 enforces both identity-based and role-based authentication. Based on their identity, the operator assumes the correct role.
- Operators must be authenticated using admin names and passwords. Authentication occurs locally. The user can be authenticated via a RADIUS server, which provides an external database for user role administrators. The NetScreen-5200 acts as a RADIUS proxy, forwarding the authentication request to the RADIUS server. The RADIUS server replies with an accept or reject message. See the log for authenticated logins. The RADIUS shared secret has to be at least six characters long.
- The operator must enter the admin 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.
- SSH uses Triple-DES encryption only.
- The Crypto-Officer is provided with the same set of services as the user with four additional CLI commands:

set admin and **unset admin** CLI commands. These two commands allow the Crypto-Officer to create a new user, change a current user's admin name and password, or delete an existing user.

set **FIPS-mode enable** and **unset FIPS-mode enable** CLI commands. 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 setting is user configurable. The maximum number of HTTP connections, that is, 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 only come through a VPN with AES encryption.
- There are a maximum of 22 sessions shared between Telnet and SSH.
- Upon a Telnet or console login failure, the next prompt does not display for an estimated five seconds.
- The chips in the NetScreen-5200 are production-grade quality and include standard passivation techniques.
- The NetScreen-5200 is contained within a metal production-grade enclosure.



Location of Tamper Evident Seals

Figure 1: Tamper Evident Mechanisms, Front of NS-5200

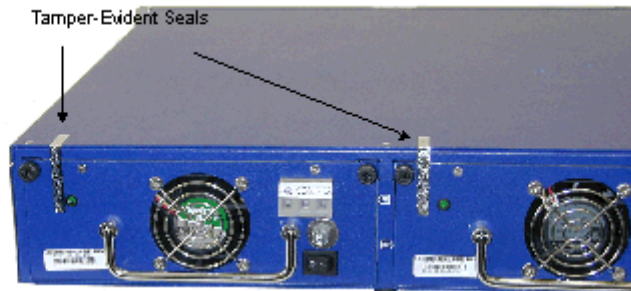


Figure 2: Tamper Evident Mechanisms, Rear of NS-5200

- 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 and 2.

Removing the cover damages the tamper evident seals. You should place new seals as follows:

1. Thoroughly clean the areas on which you will place the labels with isopropyl alcohol.
 2. Peel off the labels and apply them to the locations shown in Figure 1 and 2.
 3. Allow the adhesives to cure for 24 hours before they function as tamper evident seals.
- The NetScreen-5200 has 92% of the software within a cryptographic device, which was implemented using a high-level language (C); 5% is written in assembly due to performance issues; and 3% are Web page files, such as HTML and GIF, for the WebUI.
 - The Netscreen-5200 does not use third-party applications.
 - The NetScreen-5200 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.
 - Internet Key Exchange (IKE), Diffie-Hellman (DH), and Rivest Shamir Adelman Algorithm (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 device. The private/public key pair of the device 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**, **delete**, and **clear** commands, except for the RNG key.
 - The NetScreen-5200 does not perform key archiving.
 - The NetScreen-5200 includes the following algorithms:

FIPS Approved:

DSA/SHA1

TDES (CBC)

DES (CBC)

AES (CBC)

SHA-1-HMAC

RSA Sign/Verify (PKCS #1)

ANSI X9.31

RSA Encrypt/Decrypt (used for key wrapping only)

Non-FIPS Approved:

MD5

DH

- The NetScreen-5200 conforms to FCC part 15, class A.
- Upon the failure of any startup self-test, the device enters and stays in either the Algorithm Error State or Device specific error state, depending on the self-test failure. The failure causes the console to display error messages and the Status LED to flash red. It is the responsibility of the Crypto-Officer to return the device to Juniper Networks for further analysis.
- Upon the failure of any conditional test, the device enters and stays in a permanent error state, depending on the type of failure. The failure causes the console to display error messages and the Status LED to flash red. It is the responsibility of the Crypto-Officer to return the device to Juniper Networks for further analysis.
- On shutdown, previous authentications are erased from memory and need to be re-authenticated at startup.
- Bypass tests are performed as a conditional test and at device startup. Bypass state occurs when the administrator configures the device 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 occur:

- A non-VPN policy is matched for this traffic
- A routing table entry exists for the traffic that matches this non-VPN policy.
- In FIPS mode, SSH can use Triple-DES 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.
- HA traffic encryption is 256-bit AES.
- If a VPN uses Triple-DES encryption, the key exchange protocol IKE is enforced to use group five 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.

J. ACCRONYM 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
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