FIPS 140-2 SECURITY POLICY

Juniper Networks

NetScreen 204/208

P/N NS-204 AND NS-208 VERSION 0110 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.

A. SCOPE OF DOCUMENT

The Juniper Networks NetScreen-204/208 is an Internet security device that integrates firewall, virtual private networking (VPN), and traffic shaping functions.

Through the VPN, the NetScreen-204/208 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-204/208 also provides an interface for a user to configure or set policies through the Console or Network ports.

The general components of the NetScreen-204/208 include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC (GigaScreen version 2), 10/100 Mbps Ethernet interface, console interface, and power supply. The entire case is defined as the cryptographic boundary of the modules. The NetScreen-204/208's physical configuration is defined as a multi-chip standalone module.

B. SECURITY LEVEL

The NetScreen-204/208 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

The NetScreen-204/208 support three distinct roles:

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

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

The NetScreen-204/208 provide 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-204/208 support both role-based and identity-based authentication.

- All roles can be authenticated locally (within the NS-204 and NS-208); optionally, the module supports authentication via a RADIUS server for only the User role. Authentication by use of the RADIUS server is viewed as role-based authentication; all other methods of authentication are identity-based.
- All other forms of authentication (local database) are classified as identity- based.
- The module supports identity-based authentication for the Cryptographic Officer Role (local database), the User Role (local database), and the Read-Only Role (local database).

D. INTERFACES

The NetScreen-204/208 provides a number of interfaces:

- The NetScreen-208 has eight Ethernet autosensing interfaces (RJ-45), labeled 1, 2, 3, 4, 5, 6, 7, and 8 (Data Input, Data Output, Control, Status). The NetScreen-

204 has four Ethernet autosensing interfaces (RJ-45) labeled 1, 2, 3, and 4 (Data Input, Data Output, Control, Status). These interfaces are the network ports. Each port has two LEDs that indicate port status:

- The right LED indicates the link status: the LED on means the link is up, the LED off means the link is down (Status Output).

- The left LED indicates Ethernet activity: the LED on and blinking means the port is active (transmitting and receiving data), the LED off means the port is inactive (Status Output).

- Console port – RJ-45 serial port connector (Data Input, Data Outpout, Status, Control).

- Modem port – RJ-45 serial port connector. Disabled in FIPS mode.

- Compact flash interface for a flash memory card (Data Input).

- Power interface: AC or DC.

- Six general LEDs:

  - One Power status LED: Illuminates solid green when power is supplied to the NetScreen-204/208 (Status Output).

  - One Module status LED: Illuminates solid green when the NetScreen-204/208 is first powered up and the unit performs diagnostics. During startup, the LED blinks orange, after which the LED starts to blink green. If an error is detected, then the LED illuminates red. The LED changes to yellow when the unit writes to flash (Status Output).

  - System Alarm LED: Illuminates red when a critical alarm occurs, such as the failure of a hardware component or software module (such as a cryptographic algorithm); illuminates green when no alarm condition is present; illuminates amber when a major alarm occurs. Major alarms include: low memory (less than10% remaining)
  high CPU utilization (more than 90%)
  session full
  maximum number of VPN tunnels reached
  firewall attacks detected
  HA status changes or a redundant group member is not found

    There is no illumination when there are no alarms (Status Output).

  - HA LED: Illuminates green if the unit is the master, blinking green if the redundant group member cannot be found, and amber if the unit is the slave. There is no illumination if HA is not configured (Status Output).

  - Session LED: Illuminates green if sessions are less than 70% utilized, yellow if sessions are between 70% and 90% utilized, and red if sessions are more than 90% utilized (Status Output).

  - Compact Flash LED: Illuminates green if a flash card is installed in the compact flash slot, blinking green if the compact flash card is active, and red if the compact flash card is more than 90% full or if read/write activity has failed. There is no illumination if the compact flash slot is empty(Status Output).

- Hardware reset button: After the user follows this sequence—press for 5 seconds, release for 5 seconds, press again for 5 seconds, and release again for 5 seconds—the device erases all configurations and restores the default factory settings (Control Input).

E. SETTING FIPS MODE

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

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

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

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

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

–   Disables administration via SSL

–   Disables loading and output of configuration files from the TFTP server

–   Disables the NetScreen-Global PRO reporting agent

–   Disables administration via SNMP

–   Disables debug service

–   Disables the Modem port

–   Enforces HTTP WebUI only through VPN with AES encryption

–   Enforces Telnet only through VPN with AES encryption

–   Enforces SCS to use only 3DES to manage the box

–   Disables the MD5 algorithm

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

Note the following:

*   Configure the HA encryption key before using the HA link.
*   Management via Telnet and HTTP (WebUI) is only allowed through a VPN tunnel 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 $1/(62^6) + 1/62^6) + 1/(62^6) = 3/(62^6)$, which is far less than 1/100,000.
*   DSA-signed firmware image cyrptographic strength analysis: the firmware is signed by a 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-204/208 does not employ a maintenance interface or have a maintenance role.

- When in FIPS mode, the WebUI of the NetScreen-204/208 only displays options that comply with FIPS regulations.

- The output data path is logically disconnected from the circuitry and processes that perform key generation or key zeroization.

- The NetScreen-204/208 provides a Show Status service via the GET service.

- The NetScreen-204/208 implements the following power-up self-tests:

  Device Specific Self-Tests:

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

  Algorithm Self-Tests:

  - DES, CBC mode, encrypt/decrypt (for legacy systems only) KAT
  - 3DES, CBC mode, encrypt/decrypt KAT
  - SHA-1 KAT
  - RSA (encryption and signature)
  - DSA Sign/Verify
  - Exponentiation
  - AES, CBC mode, encrypt/decrypt KAT
  - HMAC-SHA-1
  - ANSI X9.31 DRNG KAT

- The NetScreen-204/208 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.
- Firmware can be loaded through Trivial File Transfer Protocol (TFTP) or the Compact Flash Interface, 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-204/208 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-204/208 acts as a RADIUS proxy, forwarding the authentication request to the RADIUS server. The RADIUS server replies with either an accept or reject message. See the log for authenticated logins. The RADIUS shared secret must be at least 6 characters.
- The operator must enter a user name and password. All logins through a TCP connection disconnect upon three consecutive login failures and an alarm is logged.
- A separate session is assigned to each successful administrator login.
- The 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:
  - **set admin** and **unset admin** allow the Crypto-Officer to create a new user, change a current user's user name and password, or delete an existing user.
  - **set FIPS enable** and **unset FIPS enable** allow the Crypto-Officer to switch between FIPS mode and the default mode.
- HTTP can only come through VPN with AES encryption. The page time-out is set to 10 minutes by default; this setting can be user configured. The maximum number of HTTP connections, or the maximum number of concurrent WebUI logins, depends on how many TCP sockets are currently available in the system. The maximum number of available TCP sockets is 1024. This number is shared with other TCP connections.
- Telnet can only come through VPN with AES encryption.
- There are a maximum of 5 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-204/208's chips are production-grade quality and include standard passivation techniques.
- The NetScreen-204/208 is contained within a metal production-grade enclosure.

Figure 1: Front of the NS-204 device

Figure 2: Front of the NS-208 device

- The enclosures are opaque to visible spectrum radiation
- The enclosed includes a removeable cover and is protected by a tamper-evident seal. This seal also covers the power block at the back of the unit. The locations of the tamper evident seal are shown in Figure 3 and Figure 4.

Tamper-Evident Seal

Figure 3: Tamper evident seal on AC interface

Tamper-Evident Seal

Figure 4 Tamper-Evident Seal on DC Interface

- The NetScreen-204/208 does not use third party applications.
- The NetScreen-2004/208 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 plaintext.
- All keys and unprotected security parameters can be zeroized through the Unset, Clear and Delete commands, except the PRNG key.
- The NetScreen-204/208 does not perform key archiving.
- Algorithms included in the NetScreen-204/208 are:
  - 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-204/208 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, if the signing CA certificate cannot be found in the NetScreen-204/208 during the loading of the X509 certificate, the following message appears (where x is one of 0, 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F):

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


xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx


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

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

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 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 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 Key	N/A	N/A	D	N/A	N/A	N/A	N/A	D	N/A	N/A
User Name and Password	G[1]	D[2]	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

---

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 4: 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	G[3]	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

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 Pass- word	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

---

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