NETSCREEN-200 SERIES DEVICES

Cryptographic Module Security Policy

Version 3.1.0 P/N 093-0526-000 Rev. A

Copyright Notice

Table of Contents

A. Scope of Document

The NetScreen-200 series are Internet security devices integrating firewall, virtual private networking (VPN) and traffic shaping functionalities.

Through the VPN, the NetScreen-200 series devices provide the following:

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

The NetScreen-200 series devices also provide an interface for a user to locally configure or set policies through the Console, Modem or Network ports.

The general components of the NetScreen-200 series devices include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC, 10/100Base-T Ethernet interfaces, power supply, and two fans. The entire case is defined as the cryptographic boundary of the modules. The physical configuration of the NetScreen-200 series devices is defined as a multi-chip standalone module.

B. Security Level

The NetScreen-200 series devices meet the overall requirements applicable to Level 2 security of FIPS 140-1.

Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	2
Module Interfaces	2
Roles and Services	2
Finite State Machine	2
Physical Security	2
Software Security	3
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	2
Self-Test	2

C. ROLES AND SERVICES

The NetScreen-200 series devices 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.
- User Role (Admin) – Each entity is authenticated using a user name and a pass phrase. The Admin user can configure specific security policies. These policies provide the module with information on how to operate (e.g., configure access policies and VPN encryption with Triple-DES).
- Read-Only Role (Admin) – This role can only perform a limited set of services.

The module allows up to 20 users, either in a User Role or in a Read-Only Role.

The NetScreen-200 series devices provide the following services:

- **Set –** Writes configuration-to-configuration scripts.
- **Unset –** Clears or toggles off given configuration-to-configuration scripts.
- **Get –** Shows information about particular settings or runtime information.
- **Clear –** Erases some runtime memory.
- **Exec –** Executes or updates dynamic entries, such as DHCP, Time, DSA/RSA Key Pair, DNS entries, software key, and trace route.
- **Exit –** Logs out from a login session.
- **Ping –** Checks the network connection to another system.
- **Policy Enforcement –** The state of the module in terms of how to handle the packets.
- **Reset –** Reboots the device.
- **Save –** Saves the configuration data.

The NetScreen-200 series devices support both role-based and identity-based authentication.

- Role-based authentication provides a user 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) is classified as identity-based.
- The module supports identity-based authentication for the Cryptographic Officer Role (DSA signature and local database), the User Role (local database), and the Read-Only Role (local database).

D. INTERFACES

The NetScreen-200 series devices provide a number of interfaces:

- The NetScreen-204 has four Ethernet auto sensing interfaces (RJ45) labelled 1, 2, 3, and 4, while the NetScreen-208 has eight of them labelled 1, 2, 3, 4, 5, 6, 7, 8. These interfaces correspond to the network ports on the device. Each port has two LEDs that indicate port status:
  - The right LED indicates link status: a glowing LED means the link is up, a dark LED means the link is down.
  - The left LED indicates Ethernet activity: a blinking LED indicates traffic activity, and a dark LED indicates no traffic activity.
  - Auto-sensing and Auto-correcting to DCE and DTE
- Console port – RJ-45 serial port connector
- Modem port – RJ-45 serial port connector
- Compact flash interface for a flash memory card
- One power interface: AC or DC
- Six general LEDs:

LED	Purpose	Color	Meaning
POWER	Power Supply	green	Power supply is functioning correctly.
		dark	Power supply failure, power bay is empty, or power bay is occupied but not receiving power.
STATUS	System Status	solid green	At start-up and while performing diagnostics
		blinking orange	During start-up
		blinking green	During normal operation
		red	Error detected.
		yellow	Unit is writing to flash.
HA	High Availability Status	green	Unit is primary (master).
		blinking green	Redundant group member not found.
		amber	Unit is backup (slave).
		dark	HA not enabled.
ALARM	System Alarm	red	Critical alarm—failure of hardware component or software module (such as a cryptographic algorithm)

LED	Purpose	Color	Meaning
		amber	Major alarm: • Low memory (<10% remaining) • High CPU utilization (>90%) • Session full • Maximum number of VPN tunnels reached. • Firewall attacks detected. • HA status changed or redundant group member not found.
		dark	No alarms
SESSION	Session Utilization	dark	Normal operation*
		green	Sessions are >70% utilization.
		yellow	Sessions are between 70% and 90% utilization.
		red	Sessions are >90% utilization.
FLASH	Memory Card Status	solid green	The card is installed but there is no activity.
		blinking green	Read-write activity
		dark	Flash card slot is empty.

* The NetScreen-200 series devices support 128,000 concurrent sessions.

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

Setting FIPS Mode

By default, the first time you start the module, it is in non-FIPS mode.

The module can be set to FIPS mode only through the CLI. To set the module to FIPS mode:

1. Execute the “set fips-mode enable” command. This command performs the following:
   - Disable administration via SSL
   - Disable loading and output of configuration file from the TFTP server
   - Disable NetScreen-Global PRO reporting agent
   - Disable administration via SNMP
   - Disable debug service
   - Disable modem interface
   - Enforce HTTP WebUI only through VPN
   - Enforce Telnet only through VPN
   - Disable MD5 algorithm
2. Execute the “save” command.
3. Execute the “reset” command.

Please note the following:

- Configure the HA encryption key before using the HA link.
- When in FIPS mode, management via Telnet and HTTP (WebUI) is only allowed through a VPN tunnel.
- 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 NetScreen-200 series devices do not employ a maintenance interface or have a maintenance role.
- When in FIPS mode, the WebUI of the NetScreen-200 series devices only displays options that comply with FIPS regulations.
- The output data path is logically disconnected from the circuitry and processes performing key generation or key zeroization.
- The NetScreen-200 series devices provide a Show Status service via the GET service.
- The NetScreen-200 series devices implement the following power-up self-tests:

  Device Specific Self-Tests:

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

Algorithm Self-Tests:

- DES, CBC mode, encrypt/decrypt
- 3DES, CBC mode, encrypt/decrypt
- AES, CBC mode, encrypt/decrypt
- SHA-1
- RSA (encryption and signature)
- DSA Sign/Verify
- Exponentiation
- HMAC-SHA-1

Other Parameters

Note also that:

- A pair-wise consistency test for the DSA and RSA (encryption and signature) key-pairs is employed.
- Firmware can be loaded through Trivial File Transfer Protocol (TFTP) or the compact flash port, where a firmware loads test is performed via a DSA signature.
- Keys are generated using a FIPS approved pseudo random number generator per ANSI X9.17, Appendix C.
- For every usage of the FIPS-approved PRNG, a continuous PRNG self-test is performed.
- In FIPS mode, only FIPS-approved algorithms are used.
- Operators must be authenticated using user names and passwords. Authentication will occur locally. The user can be authenticated via a RADIUS server. The RADIUS server provides an external database for user role administrators. The NetScreen-200 series devices act as a RADIUS proxy, forwarding the authentication request to the RADIUS server. The RADIUS server replies with either an accept or reject message.
- The operator must enter the user name and password. All logins through a TCP connection disconnect upon three consecutive login failures and an alarm is logged.
- The NetScreen-200 series devices allow up to five concurrent operators via SCS.
- 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.
- HTTP can only come through VPN. By default, the page time-out is set to 10 minutes; this setting can be user-defined.
- Telnet can only come through VPN. The NetScreen-200 series devices allow up to 6 concurrent operators. In the event of a login failure, the next prompt appears approximately 5 seconds later.
- The Crypto-Officer is provided with the same set of services as the user with the exception of the set admin, unset admin, and unset all services. These services allow the Crypto-Officer to create a new user, change a current user's user name and password, or delete an existing user.

- The Crypto-Officer is authenticated via digital signature only when downloading new firmware.
- The chips for the NetScreen-200 series devices are production-grade quality and include standard passivation techniques.
- The NetScreen-200 series devices are contained within metal production-grade enclosure.
- The enclosures are opaque to visible spectrum radiation.
- The enclosure includes a removable cover and is protected by a tamper-evident seal. This seal also covers the power block at the back of the unit, see Figure 1 and Figure 2.

Figure 1 Tamper-Evident Seal on AC Interface

Figure 2 Tamper-Evident Seal on DC Interface

- The source code is annotated with detailed comments.
- Ninety-five percent of the software within a cryptographic module is implemented using a high-level language (i.e. C); 5% is written in assembly due to performance issues and unavailability of a high-level language.
- The NetScreen-200 series devices do not use third party applications.
- The NetScreen-200 series devices generate 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 and Clear commands.
- The NetScreen-200 series devices do not perform key archiving.
- Algorithms included in the NetScreen-200 series devices are:
  - MD5 (Not used in FIPS mode.)
  - SHA-1
  - RSA (encryption and signature)
  - DSA
  - 3DES (CBC)
  - DES (CBC)
  - AES (CBC)
  - DH
  - HMAC-SHA-1
  - RC2
  - RC4
- The NetScreen-200 series devices conform to FCC part 15, class A.
- On failure of any power-up self-test or conditional self-test, the module enters and stays in either the Algorithm Error State or the Device specific error state, depending on the self-test failure. The module then logs the error and the module status LED indicates that an error has occurred. It is the responsibility of the Crypto-Officer to return the module to NetScreen Technologies, Inc. for further analysis.
- The module supports traffic bypass.

E. FIPS CERTIFICATE VERIFICATION

In FIPS mode, during the loading of the X509 certificate, if the signing CA certificate cannot be found in the NetScreen-200 series devices, 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.

F. SECURITY RELEVANT DATA ITEM (SRDI) DEFINITIONS

Below is a list of Security Relevant Data Item (SRDI) definitions:

- IPSEC Manual Key – Between end users, there is no IKE process involved.
- IPSEC Session Key – Encryption key between end-users
- IKE Pre-shared Key – Pre-shared key for authentication between peer-to-peer
- IKE Session Key – Encryption key between peer-to-peer
- User Name and Password – Crypto-Officer's and Users' user names and passwords
- SCS Server/Host Key – RSA key pairs used in secure command shell (equivalent to SSH)
- SCS DES Key – Encryption key to communicate via SCS (SHS)
- DSA Public Key – Firmware-download authentication key
- HA Key – DES 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 X9.17 algorithm key required to generate pseudo-random numbers. These items are stored in volatile RAM.

Matrix Creation of Security Relevant Data Items (SRDIs) Versus the Services (Roles & Identity)

The following matrices define the set of services to the Security Relevant Data Items (SRDIs) 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

Crypto-Officer

SRDI \ Services	Set	Unset	Clear	Get	Policy Enforcement	Save	Exec	Exit	Ping	Reset
IPSEC Manual Key	G	D	N/A	U	U	U	N/A	N/A	N/A	N/A
IPSEC Session Key	N/A	N/A	D	U	G.U	N/A	N/A	N/A	N/A	N/A
IKE Pre-shared Key	G	D	N/A	U	U	U	N/A	N/A	N/A	N/A
IKE Session Key	N/A	N/A	D	U	G, U	N/A	N/A	N/A	N/A	N/A
User Name and Password	G*	D†	N/A	U	U	U	N/A	N/A	N/A	N/A
SCS Server/ Host Key	G	N/A	D	U	G, U	N/A	N/A	N/A	N/A	N/A
SCS DES Key	U	U	U	U	U	U	U	U	U	U
DSA Key	N/A	N/A	D	N/A	U	U	G	N/A	N/A	N/A
HA Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IKE DSA Key	U	U	D	U	U	U	G	N/A	N/A	N/A
IKE RSA Key	U	U	D	U	U	U	G	N/A	N/A	N/A
PRNG Key	N/A	N/A	D	N/A	U	N/A	N/A	N/A	N/A	N/A

* 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

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

User

SRDI \ Services	Set	Unset	Clear	Get	Policy Enforce-ment	Save	Exec	Exit	Ping	Reset
IPSEC Manual Key	G	D	N/A	U	U	U	N/A	N/A	N/A	N/A
IPSEC Session Key	N/A	N/A	D	U	G.U	N/A	N/A	N/A	N/A	N/A
IKE Pre-shared Key	G	D	N/A	U	U	U	N/A	N/A	N/A	N/A
IKE Session Key	N/A	N/A	D	U	G, U	N/A	N/A	N/A	N/A	N/A
User Name and Password	G*	N/A	N/A	U	U	U	N/A	N/A	N/A	N/A
SCS Server/ Host Key	G	N/A	D	U	G, U	N/A	N/A	N/A	N/A	N/A
SCS DES Key	U	U	U	U	U	U	U	U	U	U
DSA Key	N/A	N/A	D	N/A	U	U	G	N/A	N/A	N/A
HA Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A
IKE DSA Key	U	U	D	U	U	U	G	N/A	N/A	N/A
IKE RSA Key	U	U	D	U	U	U	G	N/A	N/A	N/A
PRNG Key	N/A	N/A	D	N/A	U	N/A	N/A	N/A	N/A	N/A

* 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.

Read-Only

SRDI \ Services	Get	Exit	Ping
IPSEC Manual Key	U	N/A	N/A
IPSEC Session Key	U	N/A	N/A
IKE Pre-shared Key	U	N/A	N/A
IKE Session Key	U	N/A	N/A
User Name and Password	U	N/A	N/A
SCS Server/Host Key	U	N/A	N/A
SCS DES Key	U	U	U
DSA Key	N/A	N/A	N/A
HA Key	U	N/A	N/A
IKE DSA Key	U	N/A	N/A
IKE RSA Key	U	N/A	N/A
PRNG Key	N/A	N/A	N/A

Glossary

A

Advanced Encryption Standard (AES). An emerging encryption standard which, when adopted by Internet infrastructures worldwide, will offer greater interoperability with other network security devices. This version of AES uses a 128-bit key.

Authentication Header (AH). See *ESP/AH*.

Authentication. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as DES, or on public-key systems using digital signatures.

CLI. The command line interface.

Data Encryption Standard (DES). A cryptographic block algorithm with a 56-bit key.

DNS. The Domain Name System maps domain names to IP addresses.

DHCP. The Dynamic Host Configuration Protocol used to dynamically assign IP addresses to computers part of the same network.

ESP/AH. The IP level security headers, AH and ESP, were originally proposed by the Network Working Group focused on IP security mechanisms, IPSec. The term IPSec is used loosely here to refer to packets, keys, and routes that are associated with these headers. The IP Authentication Header (AH) is used to provide authentication. The IP Encapsulating Security Header (ESP) is used to provide confidentiality to IP datagrams.

GBIC. A Gigabit Interface Connector (GBIC) is the kind of interface module card used on the NetScreen-200 series devices for connecting to a fiber optic network.

Internet Key Exchange (IKE). The method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

Internet Protocol (IP). An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

IP Security (IPSec). Security standard produced by the Internet Engineering Task Force (IETF). It is a protocol suite that provides everything you need for secure communications—authentication, integrity, and confidentiality—and makes key exchange practical even in larger networks. See also *DES-CBC, ESP/AH*.

ISAKMP. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. By itself, it does not establish session keys, however it can be used with various session key establishment protocols to provide a complete solution to Internet key management.

MD5. Message Digest (version) 5, an algorithm that produces a 128-bit message digest (or hash) from a message of arbitrary length. The resulting hash is used, like a “fingerprint” of the input, to verify authenticity.

RADIUS. Remote Authentication Dial-In User Service is a service for authenticating and authorizing dialup users.

SCS. You can administer the NetScreen device from a network connection using Secure Command Shell (SCS), which is SSH-compatible. You must have an SSH client that is compatible with version 1.5 of the SSH protocol. These clients are available for most operating systems, including Windows 95 and later, Linux, and UNIX. The NetScreen device communicates with the SSH client through its built-in SCS server, which provides device configuration and management services. SCS uses DES or triple DES to encrypt traffic without the need to establish a VPN.

SHA-1. Secure Hash Algorithm-1, an algorithm that produces a 160-bit hash from a message of arbitrary length. (It is generally regarded as more secure than MD5 because of the larger hashes it produces.)

Triple DES (3DES). Triple DES is the encryption algorithm defined in the ANSI X9.52 standard.

Virtual System. A feature unique to the NetScreen-1000, a Virtual System is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual Systems reside separately from each other in the same NetScreen-1000 device. Each one can be managed by its own Virtual System Administrator.

Index

R

S

T

U

V