FIPS 140-2 SECURITY POLICY

NetScreen-5XT

Version 4.0.0r7.3 P/N 093-0608-000 Rev. B

Copyright Notice

Table of Contents

A. Scope of Document

The NetScreen-5XT is an Internet security device that integrates firewall, virtual private networking (VPN), and traffic shaping functions.

Through the VPN, the NetScreen-5XT provides the following:

- IPSec standard security
- Data Encryption Standard (DES), triple-DES, and Advanced Encryption Standard (AES) key management

  Note: *DES is used for legacy systems.*

- Manual and automated IKE (ISAKMP)
- Use of RSA and DSA certificates

The NetScreen-5XT also provides an interface for a user to configure or set policies through the Console or Network ports.

The general components of the NetScreen-5XT include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC (GigaScreen version 2), 10/100 Mbps Ethernet interface, and console interface. The entire case is defined as the cryptographic boundary of the modules. The NetScreen-5XT's physical configuration is defined as a multi-chip standalone module.

B. Security Level

The NetScreen-5XT meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

C. ROLES AND SERVICES

The NetScreen-5XT supports 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 up to 4 concurrent Admin users, either in a User Role or in a Read-Only Role.

The NetScreen-5XT provides the following services:

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

The NetScreen-5XT supports 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) 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-5XT provides a number of interfaces:

- The NetScreen-5XT has five Ethernet autosensing interfaces (RJ-45). One is for the Untrusted network, and four, labeled 1, 2, 3, and 4, are for the Trusted network. These interfaces are the network ports. Each port has two LEDs that indicate port status:
  - The bottom LED indicates the bandwidth: the LED on means 100 Mbps, the LED off means 10 Mbps.
  - The top LED indicates Ethernet connectivity and activity: the LED on and blinking means the port is active (transmitting and receiving data), the LED off means the port is inactive.
- Console port – RJ-45 serial port connector.
- Modem port – RJ-45 serial port connector. Disabled in FIPS mode.
- Power interface: AC or DC.
- The module has two status LEDs.
  - Power status LED: Illuminates solid green when power is supplied to the NetScreen-5XT.
  - Module status LED: Illuminates blinking green when the module is operational, dark or red when the module is not operational, solid amber when the unit is rebooting, or solid green when the module is initializing.
- 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.

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-4.0 firmware to 4.0 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 AES for VPN to manual key only; IKE is disabled for AES
   - 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.
- Telnet and HTTP (WebUI) are 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 alphanumberic 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 unauthorized 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-5XT does not employ a maintenance interface or have a maintenance role.
- When in FIPS mode, the WebUI of the NetScreen-5XT 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-5XT provides a Show Status service via the GET service.
- The NetScreen-5XT cannot be accessed until the initialization process is complete.
- The NetScreen-5XT implements the following power-up self-tests:

  Device Specific Self-Tests:

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

  Algorithm Self-Tests:

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

- The NetScreen-5XT implements the following conditional tests:
  - PRNG continuous test
  - Hardware RNG 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

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), 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-5XT 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. The user can be authenticated via a RADIUS server. The RADIUS server provides an external database for user role administrators. The NetScreen-5XT 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 64. This number is shared with other TCP connections.
- Telnet can only come through VPN with AES encryption.
- There are a maximum of 2 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-5XT's chips are production-grade quality and include standard passivation techniques.
- The NetScreen-5XT is contained within a metal production-grade enclosure.

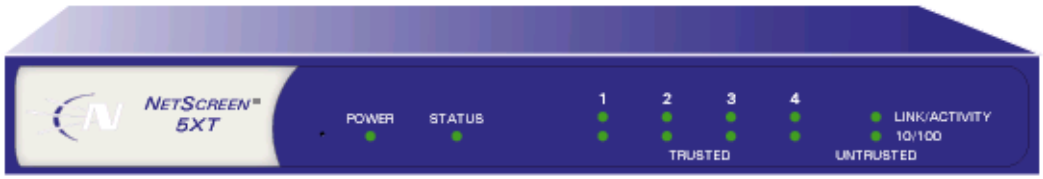

Figure 1 Front of the NetScreen 5XT Device

- The enclosures are opaque to visible spectrum radiation.

- The enclosure includes a removable cover and is protected by a tamper-evident seal. The location of the tamper evident seal is shown in Figure 1.

Figure 2 Tamper-Evident Seal

- The source code is annotated with detailed comments.
- Ninety-two percent of the software within a cryptographic module is 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-5XT does not use third party applications.
- The NetScreen-5XT 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 and Clear commands, except the RNG key.
- The NetScreen-5XT does not perform key archiving.
- Algorithms included in the NetScreen-5XT are:
  - FIPS Approved:

    DSA/SHA1

    TDES (CBC)

DES (CBC)

AES (CBC)

SHA-1-HMAC

RSA Sign/Verify (PKCS #1)

RSA Encrypt/Decrypt (used for key wrapping only)

– Non-FIPS Approved:

MD5

DH

- The NetScreen-5XT conforms to FCC part 15, class B.
- 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 NetScreen Technologies, Inc. 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 NetScreen Technologies, Inc. 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.
- VPN with AES encryption is manual key only. In other words, IKE is disabled for the VPN using AES.
- 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.

F. FIPS CERTIFICATE VERIFICATION

In FIPS mode, if the signing CA certificate cannot be found in the NetScreen-5XT 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 CSPs of the module, providing information on generation, destruction and usage. They also correlate the User roles and the Crypto-Officer roles to the set of services to which they have privileges.

The matrices use the following convention:

- G: Generate
- D: Delete
- U: Usage
- N/A: Not Available

Crypto-Officer

CSP \ Services	Set	Unset	Clear	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*	D†	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

* 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

CSP \ Services	Set	Unset	Clear	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*	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

* 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

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 Password	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

Glossary

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

Authentication. Administrator authentication ensures the user identity by validating user name and password. Data authentication ensures data is from a legitimate source, and its content has not been altered. The algorithms used in data authentication include DSA signature check in the firmware download or IKE exchange, and the keyed hash algorithm SHA-1-HMAC used in IKE exchange or IPSEC data integrity check.

CLI. The command line interface.

DHCP. The Dynamic Host Configuration Protocol used to dynamically assign IP addresses to networked computers.

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

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.

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. Secured Command Shell, using SSH to encrypt telnet traffic.

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.)

Index

S

T

U

V