NETSCREEN-100

Cryptographic Module
Security Policy

Version 0.3   P/N 093-0074-000   Rev. A

Copyright Notice

Table of Contents

A.   Scope of Document

The NetScreen-100 is an Internet security device integrating firewall, virtual private networking (VPN) and traffic shaping functionalities.

Through the VPN, the NetScreen-100 provides the following:

- IPSec standard security

- Data Encryption Standard (DES) and triple-DES encryption key management, and

- manual and automated IKE (ISAKMP)

The NetScreen-100 also provides an interface for a user to configure or set policies through the Secure Command Shell (SCS, SSH Version 1 compatible), which provides DES or TDES encryption.

The general components of the NetScreen-100 include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC, a power supply and a fan. The entire case is defined as the cryptographic boundary of the modules. The NetScreen-100's physical configuration is defined as multi-chip standalone modules.

B.   Security Level

The NetScreen-100 meets the overall requirements applicable to Level 2 security of FIPS 140-1.

Table 1: Module Security Level Specification

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

C. Roles and Services

TheNetScreen-100 supports two distinct roles:

<u>Cryptographic Officer Role (Root)</u>: 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.

<u>User Role (Admin)</u>: The module allows up to 19 users. Each entity is authenticated using identity-based authentication via user name and 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).

- The NetScreen-100 provides 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 dhcp client renew**: Renews the lease for an IP address from a DHCP server
    - **Exec ntp update**: Immediately updates the NetScreen device clock using Network Time Protocol
    - **Exec pki dsa new <key length>**: Generate the DSA key pair
    - **Exit**: Logs out from a login session
    - **Ping**: Checks the network connection to another system
    - **Reset**: Reboots the device
    - **Save**: Saves the configuration data
    - **Exec DNS**: Refreshes all DNS entries.
    - **Exec Software-Key**: Sets the feature configurations.
    - **Exec Trace-Route**: Trace routes other hosts.
    - **Policy Enforcement**: The state of the module in terms of how to handle the packets

D.   Interfaces

- The NetScreen-100 provides a number of interfaces:

  - Three Ethernet autosensing interfaces (RJ45) labelled Trusted, Untrusted and DMZ. These interfaces are the network ports.
  - Console port: DB25 serial port connector.
  - PCMCIA interface for a memory flash card.
  - Power interface.
  - Eight LED status interfaces.

    (a)   <u>One Power status LED</u>: Illuminates solid green when power is supplied to the NetScreen-100.

    (b)   <u>One Module status LED</u>: Illuminates solid green when the NetScreen-100 is first powered up and the units first perform diagnostics. During start-up, 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.

    (c)   <u>Six Network status LEDs (for the Trusted, Untrusted, and DMZ ports)</u>: Each Ethernet port has two LEDs: The left LED indicates 10Mbps or 100Mbps; the right LED indicates link and network activity.

Setting FIPS Mode

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

To set the module to FIPS mode:

- Assign a system IP address

- Enable the Secure Communication Shell (SCS) for management access on at least one of the interfaces

Execute "set fips-mode enable". This command will perform the following:

- Disable the console port for administration usage. The status can still be displayed on the console and newly signed firmware can still be loaded from the console.

- Inhibit the output of unprotected configuration data.

- Disable administration via the web (i.e., HTTP and HTTPS)

- Disable the TFTP client except the "save image-key tftp" and the "save software from tftp"

- Disable administration via telnet

- Disable administration via Global

- Disable administration via Global PRO

- Disable administration via SNMP

- Disable RADIUS Server

- Disable debug service

Execute the "save" command.

Execute the "reset" command.

Please note the following:

- In FIPS mode, the secure (encrypted) mode of communication must be enforced through the trusted, untrusted, or DMZ port via SCS (SSH compatible).

- 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-100 does not employ a maintenance interface or have a maintenance role.

- The output data path is logically disconnected from the circuitry and processes performing key generation, manual key entry or key zeroization.

- The NetScreen-100 provides a Show Status service via the GET service.

- The NetScreen-100 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
– TDES, CBC mode, encrypt/decrypt
– SHA-1
– RSA (encryption and signature)
– DSA Sign/Verify
– Exponentiation

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 PCMCIA 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.

• The NetScreen-100 enforces identity-based authentication. Based on their identity, the operator assumes the correct role.

• 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-100 allows up to five concurrent operators via SSH.

• 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 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 NetScreen-100's chips are production-grade quality and include standard passivation techniques.

- The NetScreen-100 is 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. In addition to the tamper evident seal, a red tamper evident varnish is applied to the screw that secures the enclosure. The locations of the tamper evident seal and varnish are shown in Figure 1.
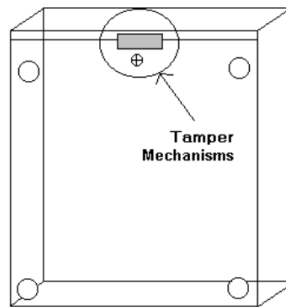

Figure 1 - Tamper Evident Mechanisms

- 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-100 does not use third party applications.

- The NetScreen-100 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.

- Pre-shared keys are manually distributed through the Secure Command Shell. These are entered electronically and encrypted.

- 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-100 does not perform key archiving.

- Algorithms included in the NetScreen-100 are:

  - RC2
  - RC4
  - MD5
  - SHA-1
  - RSA (encryption and signature)
  - DSA
  - TDES (CBC)
  - DES (CBC)
  - DH
  - HMAC
  - Blowfish

- The NetScreen-100 conforms 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.

- Only DSA certificates can be used in FIPS mode. The user can only use pre-shared keys in the IKE process if DSA certificates are not available.

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-100, the following message is displayed at the SCS console:

```
      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]?
```

Where x is one of (0, 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F).

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, 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 and Users' 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

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

The following matrix defines the set of services to the Security Relevant Data Items (SRDIs) of the module, providing information on generation, destruction and usage. It also correlates the User roles and the Crypto-Officer roles to the set of services it has privileges to.

Roles	Crypto-Officer/User													
SRDI \ Services	Set	Unset	Clear	Get	Policy Enforce-ment	Save	Exec DHCP Client Renew	Exec PKI DSA New	Exit	Ping	Reset	Exec DNS	Exec Software Key	Exec Trace-Route
IPSEC Manual Key	Set	D	N/A	U	U	U	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Roles	**Crypto-Officer/User**													
IPSEC Session Key	N/A	N/A	D	U	G.U	N/A	N/A	N/A	N/A	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	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	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	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	N/A	N/A	N/A	N/A
SCS DES Key	U	U	U	U	U	U	U	U	U	U	U	U	U	U
DSA Key	N/A	N/A	D	N/A	U	U	N/A	G	N/A	N/A	N/A	N/A	N/A	N/A

- G: Generate

- D: Destroy

- U: Usage

    *G: The Crypto-Officer is authorized to change all authorized operator's user names and passwords, but the user is only allowed to change his/her own user name and password.

    *D: The Crypto-Officer is authorized to remove all authorized operators.

Index

S

SCS DES Key 8, 9
SCS Server/Host Key 8, 9
Secure Command Shell
    (SCS) 1
Security Relevant Data Items (SRDIs) 9
self-tests
    device specific 4
services
    clear 2
    exec dhcp client renew 2
    exec ntp update 2
    exec pki dsa new 2
    exit 2
    get 2
    ping 2
    policy enforcement 2
    reset 2
    save 2
    set 2
    unset 2

SRDI Services 9
SRDIs 9

T

tamper evident mechanism 6
tamper evident seal 6
TFTP 5
Triple-DES 1
Trivial File Transfer Protocol (TFTP) 5

U

user name 8
user password 8
User Role 2

V

virtual private networking (VPN) 1
VPN 1