NETSCREEN-500

Cryptographic Module Security Policy

Version 2.6.1 P/N 093-0162-000 Rev. A

Copyright Notice

Table of Contents

A. Scope of Document 1

B. Security Level 1

C. Roles and Services 2

D. Interfaces 3

E. FIPS Certificate Verification 10

F. Security Relevant Data Item (SRDI) Definitions 11

Matrix Creation of Security Relevant Data Items (SRDIs) Versus the Services (Roles & Identity) 12

Glossary 17

Index i

A. Scope of Document

The NetScreen-500 is an Internet security device integrating firewall, virtual private networking (VPN) and traffic shaping functionalities.

Through the VPN, the NetScreen-500 provides the following:

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

The NetScreen-500 also provides an interface for a user to locally configure or set policies through the Console, Modem or Network ports.

The general components of the NetScreen-500 include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASIC, interface modules (ethernet 10/100-based or gigabit ethernet), two power supplies (one optional) and a fan tray. The entire case is defined as the cryptographic boundary of the modules. The NetScreen-500's physical configuration is defined as multi-chip standalone modules.

B. Security Level

The NetScreen-500 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	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-500 supports four 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 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).

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.

VSYS Role (Admin): The module allows up to one user per Virtual System that is created. Each entity is authenticated using 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-500 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
  - **Exit**: Logs out from a login session
  - **Ping**: Checks the network connection to another system
  - **Reset**: Reboots the device
  - **Save**: Saves the configuration data
  - **Enter VSYS**: Enters into a defined virtual system.
  - **Policy Enforcement**: The state of the module in terms of how to handle the packets
  - **Exec** - Executes or updates dynamic entries, such as DHCP, Time, DSA/RSA Key Pair, DNS entries, software key, trace route, and enter vsys.
- The NetScreen-500 supports both role-based and identity-based

authentication for each role.

- Role-based authentication provides a user name and password, but the actual authentication occurs at a RADIUS server.
- All other forms of authentication (DSA signature, local database) is classified as identity-based.

D. Interfaces

- The NetScreen-500 provides a number of interfaces:
  - LCD and Control Pad: A display with control keys that can be used to perform basic configurations and view status reports through the LCD and control pad. The LCD displays two lines, each line capable of displaying up to 16 characters.
  - Two to three Ethernet cards. These may be either 10/100 Base T or GBIC interfaces.
  - Three Ethernet autosensing interfaces (RJ45). These interfaces are the network ports.
    - HA-1: dedicated RJ45 used for fail-over processing.
    - HA-2: backup dedicated RJ45 used for fail-over processing if HA-1 fails.
    - MGT dedicated RJS
  - Console port: DB9 serial port connector.
  - Modem port: DB9 serial port connector.
  - PCMCIA interface for a memory flash card.
  - Up to two power interfaces.
  - 22 LED status interfaces: 12 general, 6 RJ 45 and 4 card LEDs.

(a) Twelve General LEDs:

LED	Purpose	Color	Meaning
STATUS	System Status	blinking amber	Booting up normally
		blinking green	Normal operation
ALARM	System Alarm	red	Critical alarm—failure of hardware component or software module (such as a cryptographic algorithm)
		green	No alarm condition present.

LED	Purpose	Color	Meaning
		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
		dark	No alarms
PWR 1	Power Supply #1	green	Power supply #1 is functioning correctly.
		red	Power supply #1 failure or power bay #1 is empty.
PWR 2	Power Supply #2	green	Power supply #2 is functioning correctly.
		red	Power supply #2 failure or power bay #2 is empty.
FAN	Fan Status	green	All fans functioning properly
		red	One or more fans failed.
TEMP	Temperature	green	Temperature is within safety range.
		red	Temperature is outside safety range.
HA	High Availability Status	green	Unit is master.
		blinking green	Redundant group member cannot be found.
		amber	Unit is slave.
		dark	HA not configured
FW	Firewall Alarm	green	No firewall attacks
		red	Firewall event/alarm has occurred.

LED	Purpose	Color	Meaning
VPN	VPN Activity	blinking green	VPN activity—encrypting/ decrypting traffic
		blinking yellow	VPN drops or denies traffic
		red	VPN tunnels have reached 90% of the maximum number of simultaneously active IPSec SAs.
		dark	No VPN defined or no tunnels active
SESSION	Session Utilization	green	Sessions are <70% utilization.
		yellow	Sessions are between 70% and 90% utilization.
		red	Sessions are >90% utilization.
PCMCIA	PC Card Status	green	PC card is installed in PCMCIA slot.
		blinking green	PC card is active.
		red	PC card is >90% full or read/write activity has failed.
		dark	PCMCIA slot is empty.
SHAPE	Traffic Shaping	green	Traffic shaping in operation
		blinking green	Traffic shaping transmits packets
		blinking yellow	Traffic shaping drops packets
		red	Configured guaranteed bandwidth > available interface bandwidth
		dark	No traffic shaping configured

(b) Four Module status LEDs: Illuminates green to correspond to the position of the installed interface modules:
Green: Card operational
Blinking Red: Card failed
Dark: No card

(c) Six Network status LEDs (for the MGT, HA-1 and HA-2 ports): 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.

The module can be set to FIPS mode only through the CLI. To set the module to FIPS mode, assign a system IP address.

Next, execute “set fips-mode enable”. This command will perform the following:

- Disable administration via SSL
- Disable loading configuration file from the TFTP server
- Disable administration via Global
- Disable administration via Global PRO
- Disable administration via SNMP
- Disable debug service
- Disable configuration information via LCD display

Execute the “save” command.

Execute the “reset” command.

Please note the following:

- Configure the HA encryption key before using the HA link.
- 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-500 does not employ a maintenance interface or have a maintenance role.

- When in FIPS mode, the NetScreen-500 WebUI only displays options that comply with FIPS regulations. (For example, the SSL, NS-Global, and NS-Global PRO management service options do not appear on the Interface Configuration page when FIPS mode is enabled.)
- The output data path is logically disconnected from the circuitry and processes performing key generation or key zeroization.
- The NetScreen-500 provides a Show Status service via the GET service.
- The NetScreen-500 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.
- 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-5XP acts 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-500 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.
- HTTP page time-out set to 10 minutes as default; this is user configurable.
- Telnet: The NetScreen-500 allows up to six concurrent operators. Upon a login failure, the next prompt will not come up for an estimated 10 seconds.
- VSYS is only able to configure policies related to a specific virtual system, and cannot clear or set any global variables.
- The Crypto-Officer is authenticated via digital signature only when downloading new firmware.
- The NetScreen-500's chips are production-grade quality and include standard passivation techniques.
- The NetScreen-500 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 a tamper evident seal, a red tamper evident varnish is applied to the screws that secures the enclosure. The location of the tamper evident seal and varnish is shown in Figure 1.

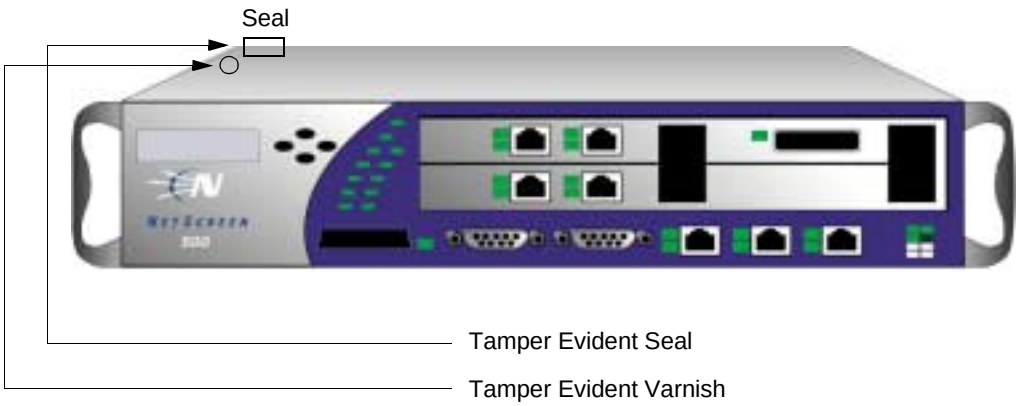

Figure 1 - Tamper Evident Mechanisms

- 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-500 does not use third party applications.
- The NetScreen-500 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.
- Electronically entered keys are input locally using a key loader.
- All keys and unprotected security parameters can be zeroized through the Unset and Clear commands.

- The NetScreen-500 does not perform key archiving.
- Algorithms included in the NetScreen-500 are:
  - RC2
  - RC4
  - MD5
  - SHA-1
  - RSA (encryption and signature)
  - DSA
  - TDES (CBC)
  - DES (CBC)
  - DH
  - HMAC
  - Blowfish
- The NetScreen-500 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.

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-500, the following message is displayed:

```
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, Users and VSYS 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.

Crypto-Officer

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

G: Generate D: Delete U: Usage

*G: 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.

*D: 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	Enter VSYS
IPSEC Manual Key	Set	D	N/A	U	U	U	N/A	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	N/A
IKE Pre-shared Key	G	D	N/A	U	U	U	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
User Name and Password	G*	N/A	N/A	U	U	U	N/A	N/A	N/A	N/A	U
SCS Server/Host Key	G	N/A	D	U	G, U	N/A	N/A	N/A	N/A	N/A	U
SCS DES Key	U	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	N/A
HA Key	G	D	N/A	U	N/A	U	N/A	N/A	N/A	N/A	N/A
IKE DSA Key	U	U	D	U	U	U	G	N/A	N/A	N/A	N/A
IKE RSA Key	U	U	D	U	U	U	G	N/A	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	N/A

G: Generate D: Delete U: Usage

*G: 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	Enter VSYS
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	U	N/A	N/A	N/A
User Name and Password	U	N/A	N/A	U
SCS Server/Host Key	U	N/A	N/A	U
SCS DES Key	U	U	U	U
DSA Key	N/A	N/A	N/A	N/A
HA Key	U	N/A	N/A	N/A
IKE DSA Key	U	N/A	N/A	N/A
IKE RSA Key	U	N/A	N/A	N/A
PRNG Key	N/A	N/A	N/A	N/A

G: Generate D: Delete U: Usage

VSYS

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

G: Generate D: Delete U: Usage

Glossary

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.

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

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

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-500 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.

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.)

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

A

algorithm
- error state 10
- self-tests 7

algorithms 10
- Blowfish 10
- DES 10
- DH 10
- DSA 10
- HMAC 10
- MD5 10
- RC2 10
- RC4 10
- RSA 10
- SHA-1 10
- TDES 10

ANSI X9.17 7

C

Console port 3
Cryptographic Officer 2

D

Data Encryption Standard (DES) 1
DHCP 17
DSA key 12, 13, 14, 15
DSA public key 11

E

EMI/EMC 1

F

FIPS 140-1 1
FIPS mode 6

H

HA Key 11
HA-1 3
HA-2 3

I

IKE 1
IKE DSA Key 11
IKE Pre-shared Key 11, 12, 13, 14, 15
IKE RSA Key 11
IKE Session Key 11, 12, 13, 14, 15
initial vector
- (IV) 9

IPSEC Manual Key 11, 12, 13, 14, 15
IPSEC Session Key 11, 12, 13, 14, 15
IPSec standard security 1
ISAKMP 1

L

LED status 3
LEDs
- ALARM 3
- FAN 4
- FW 4
- HA 4
- PCMCIA 5
- PWR 1 4
- PWR 2 4
- SESSION 5
- SHAPE 5
- STATUS 3
- TEMP 4

VPN 5

M

module specification
cryptographic algorithms 1
cryptographic module 1
finite state machine 1
key management 1
module interfaces 1
operating system security 1
physical security 1
roles and services 1
self-test 1
software security 1
module status 6

N

network ports 3
network status 6

P

PCMCIA interface 3
ping 2
power interface 3
PRNG Algorithm Key 11

R

Read-Only Role 2
RJ45 3

S

SCS DES Key 11, 12, 13, 14, 15
SCS Server/Host Key 11, 12, 13, 14, 15
Secure Command Shell
(SCS) 1
Security Relevant Data Items (SRDIs) 12
self-tests
device specific 7
services
clear 2
Enter VSYS 2
Exec 2
exit 2
get 2
ping 2
policy enforcement 2
reset 2
save 2
set 2
unset 2
SRDI Services 12, 13, 14, 15
SRDIs 12

T

tamper evident mechanism 9
tamper evident seal 9
TFTP 7
Triple-DES 1
Trivial File Transfer Protocol (TFTP) 7

U

user name 11
user password 11
User Role 2

V

virtual private networking (VPN) 1
VPN 1
VSYS Role (Admin) 2