FIPS 140-2 Security Policy

Juniper Networks

NetScreen-5XT

Version 5.0.0r9 P/N 093-1392-000 Rev. D

Copyright Notice

Juniper Networks, Inc.

ATTN: General Counsel

1194 N. Mathilda Ave.Sunnyvale, CA 95014

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.

TABLE OF CONTENTS

A. SCOPE OF DOCUMENT

The Juniper Networks 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
- 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 device is defined as the cryptographic boundary of the modules. The physical configuration of the NetScreen-5XT is defined as a multi-chip standalone device.

B. SECURITY LEVEL

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

Table 1: Device 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 (Root):** The device allows one Crypto-Officer. This role is assigned to the first operator who logs on to the devices using the default admin name and password (netscreen, netscreen). Only the Crypto-Officer can create other administrators and change the device to operate in FIPS mode.
- **User (Admin):** This role can configure specific security policies. These policies provide the device with information on how to operate. For example, configuring access policies and VPN encryption with Triple-DES.
- **Read-Only User (Admin):** This role can only perform a limited set of services to retrieve information or status. This role cannot perform services to configure the device.

The device allows concurrent Admin users, either User or Read-Only User roles. The NetScreen-5XT provides the following services:

- Clear/Delete: Clear dynamic system info
- Execute: Execute system commands
- Exit: Exit command console
- Get (Show Status): Display 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
- Network Traffic: The VPN and networking services available to an operator
- Role-based authentication provides an admin name and a password, but the actual authentication occurs at a RADIUS server. This authentication is only available for the User Role (Admin).
- All other forms of authentication (local database) are classified as identity-based.
- The device supports identity-based authentication for the Crypto-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) (Data Input, Data Output, Control, and Status). 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:
  - Bottom LED: Indicates the bandwidth.

    On: 100 Mbps
    Off: 10 Mbps
  - Top LED: Indicates Ethernet connectivity and activity.

    On: Port is active (transmitting and receiving data)

    Off: Port is inactive
- **Console port:** RJ-45 serial port connector (Data Input, Data Outpout, Status, and Control).
- **Modem port:** RJ-45 serial port connector. This port is disabled in FIPS mode.
- **Power adapter:** AC or DC.
- The device has two status LEDs:
  - **Power:** Illuminates solid green when power is supplied to the NetScreen-5XT (Status Output).
  - **Status:** Illuminates blinking green when the device is operational, off or red when the device is not operational, solid amber when the device is rebooting, or solid green when the device is initializing (Status Output).
- **Hardware reset button:** The device erases all configurations and restores the default factory settings (Control Input). Refer to the *NetScreen-5XT User's Guide* for more device reset information.

E. Setting FIPS Mode

By default, FIPS mode is disabled.

For firmware upgrading: If pre-5.0 firmware is upgraded to FIPS version 5.0 or higher, you must reset the device to run in FIPS mode. You must do this even if the device was previously set to run in FIPS mode.

The commands **get config** and **get system** display which mode is running on the device.

The device can be set to FIPS mode only through the CLI.

To set the device to run in FIPS mode, do the following:

1. Type **set FIPS-mode enable** at the command prompt.

   This command performs the following:

   - Disables administration through SSL
   - Disables the loading and output of the configuration file from the TFTP server
   - Disables the Global reporting agent
   - Disables administration through SNMP
   - Disables the debug service
   - Disables the modem port
   - Enforces HTTP only through VPN with AES encryption
   - Enforces Telnet only through VPN with AES encryption
   - Enforces SSH to use only Triple-DES to manage the device
   - Disables the MD5 algorithm

2. Type **save** at the command prompt.

3. Type **reset** at the command prompt.

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.

- Admin names and passwords are case-sensitive. The password must consist 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 is 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 are dropped for one minute. If there are multiple login failure retries within one minute and since the user is locked out after three continuous 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 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 three 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 disconnected from the circuitry and processes that perform key generation or key zeroization.
- The NetScreen-5XT provides a show status service through the **get** CLI command.
- 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 done through DSA signature (Software Integrity Test)
    - SDRAM read/write check
    - FLASH test

    Algorithm Self-Tests:
    - DES, CBC mode, encrypt/decrypt (For legacy systems only)
    - Triple-DES, CBC mode, encrypt/decrypt
    - SHA-1
    - RSA (encryption and signature)
    - DSA Sign/Verify
    - Exponentiation
    - AES, CBC mode, encrypt/decrypt
    - SHA-1-HMAC
    - Bypass test

- ANSI X9.31 KAT

The NetScreen-5XT implements the following conditional self-tests:

- PRNG continuous test
- Hardware RNG continuous test
- SSH 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)

F. FIPS Certificate Verification

In FIPS mode, if the signing Certification Authority (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, Triple-DES, and AES for user traffic encryption. This key is generated by the user’s input.
- **IPSEC Session Key:** DES, Triple-DES, and AES for user traffic encryption. This key is generated by the IKE key exchange.
- **IKE Pre-Shared Key:** User input data used to generate IKE session key and SHA-1-HMAC key.
- **IKE Session Key:** DES, Triple-DES, AES for peer-to-peer IKE message encryption.
- **Admin Name and Password:** Crypto-Officer and Users’ admin names and passwords.
- **SSH Server/Host Key:** RSA keypairs used in secure command shell.

- **SSH Session Key:** Encryption key to encrypt Telnet commands by using Triple-DES 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.

H. Matrix Creation of Critical Security Parameter (CSP) versus the Services (Roles & Identity)

The following matrix defines the set of services to the CSPs of the device, providing information on generation, destruction, and usage. It also correlates the User and 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 2: 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
Admin Name and Password	G[1]	D[2]	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SSH Server/Host Key	G	D	D	U	G	U	N/A	D	N/A	N/A
SSH 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

[1] The Crypto-Officer is authorized to change all authorized operators' admin names and passwords, but the user is only allowed to change his/her own admin name and password.

[2] The Crypto-Officer is authorized to remove all authorized operators.

CSP \ Services	Set	Unset	Clear/ Delete	Get	Exec	Save	Ping	Reset	Exit	Trace - route
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 3: 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
Admin Name and Password	G[3]	N/A	N/A	U	N/A	U	N/A	N/A	N/A	N/A
SSH Server/Host Key	G	D	D	U	G	U	N/A	D	N/A	N/A
SSH 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

[3] The Crypto-Officer is authorized to change all authorized operators' admin names and passwords, but the user is only allowed to change his/her own admin name and password.

Table 5: 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
Admin Name and Password	U	N/A	N/A	N/A
SSH Server/Host Key	U	N/A	N/A	N/A
SSH 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

I. OTHER PARAMETERS

Note the following:

- A pair-wise consistency test for 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 through 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 device's random number generator, a continuous RNG self-test is performed. This test is performed on both the FIPS-approved RNG and non-FIPS-approved RNG.
- In FIPS mode, only FIPS-approved algorithms are used.
- Operators must be authenticated using admin names and passwords. Authentication occurs locally. The user can be authenticated through a RADIUS server, which 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 six characters long.
- A separate session is assigned to each successful administrator login.
- SSH uses Triple-DES encryption only.

- The Crypto-Officer is provided with the same set of services as the user, with four additional services:

  set admin and **unset admin** CLI commands allow the Crypto-Officer to create a new user, change a current user's admin name and password, or delete an existing user.

  set fips enable and **unset fips enable** CLI commands allow the Crypto-Officer to switch between FIPS mode and the default mode.

- HTTP can come through the VPN only with AES encryption. The default page timeout is set to 10 minutes; this setting is user configurable. The maximum number of HTTP connections, that is, 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 five sessions shared between Telnet and SSH.
- After a Telnet or console login failure has occured, the next prompt does not display for an estimated five seconds.
- The chips for the NetScreen-5XT are production-grade quality and include standard passivation techniques.

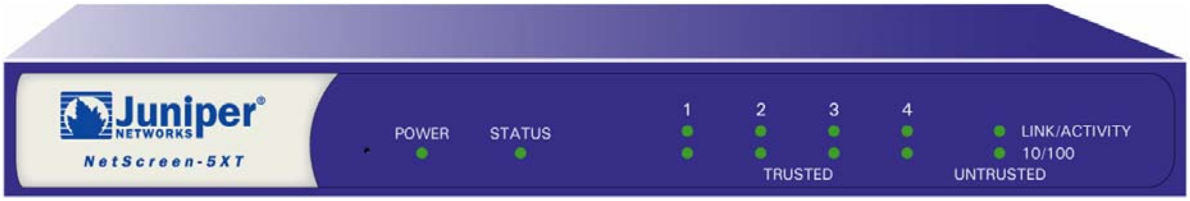

Figure 1: Front of the NetScreen-5XT Device

- The NetScreen-5XT is contained within a 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. The location of the tamper evident seal is shown in Figure 2.

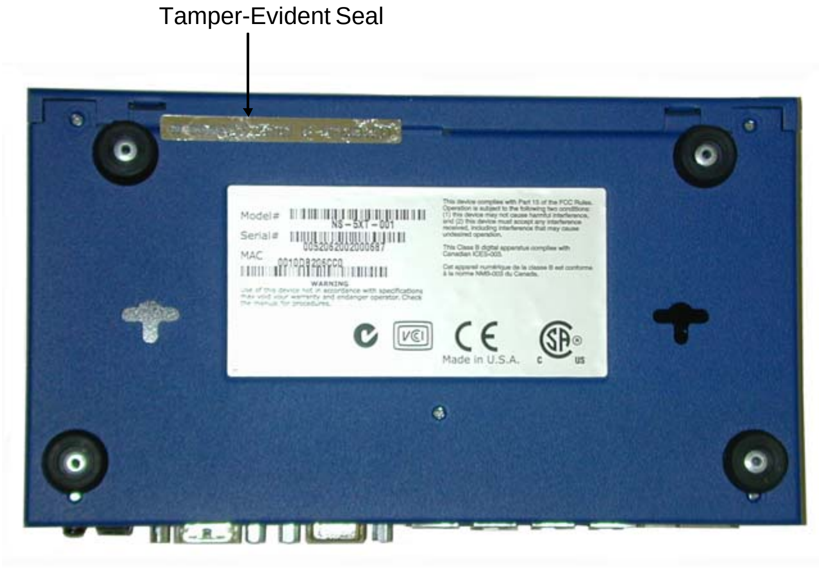

Figure 2. Tamper-Evident Seal

- The NetScreen-5XT has 92% of the software within a cryptographic module, which 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.
- Internet Key Exchange (IKE), Diffie-Hellman (DH), and Rivest Shamir Adelman Algorithm (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 devices. The private/public key pair of the device is located at a certain and exact memory location of the flash card.
- All keys are stored in plaintext.
- All keys and unprotected security parameters can be zeroized through the **unset**, **clear**, and **delete** CLI commands, except for the PRNG key.
- The NetScreen-5XT does not perform key archiving.
- Algorithms included in the NetScreen-5XT:

  FIPS Approved:

  Triple-DES (CBC)
  DSA/SHA
  DES (CBC) (For legacy systems only)
  AES (CBC)

SHA-1-HMAC

RSA Sign/Verify (PKCS #1)

RSA Encrypt/Decrypt (used for key wrapping only)

ANSI X9.31 PRNG

Non-FIPS Approved:

MD5

DH

- The NetScreen-5XT conforms to FCC part 15, class B.
- On failure of any power-up self-test, the device enters and stays in either the Algorithm Error State or Device specific error state, depending on the self-test failure. The failure causes the console to display error messages and the Status LED to flash red. It is the responsibility of the Crypto-Officer to return the device to Juniper Networks, Inc. for further analysis.
- On failure of any conditional test, the device enters and stays in a permanent error state, depending on the type of failure. The failure causes the console to display error messages and the Status LED to flash red. It is the responsibility of the Crypto-Officer to return the device to Juniper Networks, Inc. for further analysis.
- On shut-down, previous authentications are erased from memory and need to be re-authenticated when booting the device.
- Bypass tests are performed as a conditional test and at device startup. Bypass state occurs when the administrator configures the device 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 occur:

  - A non-VPN policy is matched for this traffic
  - A routing table entry exists for the traffic that matches this non-VPN policy.
- In FIPS mode, SSH can use Triple-DES only to encrypt/decrypt commands. Also, if the command from SSH 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 Triple-DES Encryption, the key exchange protocol IKE is enforced to use group five only.
- The device is not designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

J. ACCRONYM 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
PRNG – Pseudo RNG
RNG – Random Number Generator
ROM – Read Only Memory
RSA – Rivest Shamir Adelman Algorithm
SDRAM – Synchronous Dynamic Random Access Memory
SSH – Secure Shell Protocol
TCP – Transmission Control Protocol
TFTP – Trivial File Transfer Protocol
VPN – Virtual Private Networking