Brocade Communications Systems, Inc. Brocade FastIron ICX Series Switch/Router 08.0.40 Security Target

Version 0.6
January 15, 2016

Prepared for:

Brocade Communications Systems, Inc.

130 Holger Way
San Jose, CA 95134

Prepared By:

Gossamer Laboratories

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the Brocade Communications Systems, Inc. Brocade FastIron ICX Series Switch/Router 08.0.40.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***/selected-assignment/***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- The NDPP uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

Terminology

User	Any entity (human or otherwise) outside the TOE that interacts with the TOE.
Unauthorized User	An entity that interacts (or attempts to interact) with the TOE Security Function (TSF) in an unapproved manner.
Authorized Administrator	A role with which a trusted TOE user is associated to administer both the functionality and security parameters of the TOE and its operational Environment. Such users are trusted not to compromise the security policy enforced by the TOE.
TOE User	Any person who interacts with the TOE.

External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Authentication data	Information used to verify the claimed identity of a user.
Object	An entity within the TOE Security Function (TSF) Scope of Control (TSC) that contains or receives information and upon which subjects perform operations.
Subject	An entity within the TSC that causes operations to be performed.
Authorized User	A user who may, in accordance with the TOE Security Policy (TSP), perform an operation.

1.1 Security Target Reference

ST Title – Brocade Communications Systems, Inc. Brocade FastIron ICX Series Switch/Router 08.0.40

ST Version – Version 0.6

ST Date – January 15, 2016

1.2 TOE Reference

TOE Identification – Brocade Communications Systems, Inc. Brocade FastIron ICX Series Switch/Router 08.0.40, including the following series and models

- ICX Series Hardware Platforms
    a. ICX-7250 (ICX 7250-24P, ICX 7250-48P)
    b. ICX 7750 (ICX 7750-48F, ICX 7750-48C, ICX 7750-26Q)
    c. ICX 7450 (ICX 7450-24-E, ICX 7450-24P-EP, ICX 7450-48-E, ICX 7450-48P-E, ICX 7450-48F-EF)

TOE Developer – Brocade Communications Systems, Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is the Brocade FastIron ICX Series Switch/Router 08.0.40 family of products.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. Optionally, a number of co-located appliances can be connected in order to work as a unit with a common security policy. The embedded software is a version of Brocades' proprietary Multiservice IronWare software. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances.

All TOE appliances are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance

with the evaluated configuration (using the Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide) prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH. This remote management interface is protected using encryption as explained later in this ST.

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations, i.e. PowerPC etc.
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

1.4 TOE Description

The Target of Evaluation (TOE) is the Brocade FastIron ICX Series Switch/Router 08.0.40 including the following series and models

- ICX Series Hardware Platforms
    a. ICX-7250 (ICX 7250-24P, ICX 7250-48P)
    b. ICX 7750 (ICX 7750-48F, ICX 7750-48C, ICX 7750-26Q)
    c. ICX 7450 (ICX 7450-24-E, ICX 7450-24P-EP, ICX 7450-48-E, ICX 7450-48P-E, ICX 7450-48F-EF)

The following links offer additional information about each series of the TOE:

- **ICX Series**

  http://www.brocade.com/products/all/switches/product-details/icx-6610-switch/index.page

  http://www.brocade.com/products/all/switches/product-details/icx-6430-and-6450-switches/index.page

  http://www.brocade.com/products/all/switches/product-details/icx-6650-switch/index.page

  http://www.brocade.com/downloads/documents/data_sheets/product_data_sheets/icx-6610-switch-ds.pdf

While there are different models in the three series, they differ primarily in physical form factor, number and types of connections and slots, and relative performance. The ICX Series possesses between 24 and 80 10/100/1000 Mbps RJ-45 ports, and the presence of "F" in the model number indicates 100/1000 Mbps SFP ports instead of RJ-45 ports and the presence of "P" indicates that the RJ-45 ports are PoE+. While there are some functional differences among the families, they each provide the same security characteristics as claimed in this security target.

The different series have differing CPUs as described below

- The ICX 7250 Series utilizes a Dual-core ARM Cortex A9 1GHz
- The ICX 7750 Series utilizes a Freescale P2041, 1.5 GHz CPU
- The ICX 7450 Series utilizes a Dual-core ARM Cortex A9 1GHz

1.4.1 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance the Brocade IOS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions). IOS enforces applicable security policies on network information flowing through the hardware appliance.

The basic start-up operation of the TOE is as follows:

1. At system startup the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap.
2. The operating system reads the configuration parameters from the configuration file in non-volatile memory and then builds the necessary data structures in dynamic memory and begins operation.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface.

1.4.1.1 Physical Boundaries

Each TOE appliance runs a version of the Brocades software and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can be configured to synchronize its internal clock using an NTP server in the operational environment.

The use of external authentication services such as RADIUS or TACACS/TACACS+ is excluded from the evaluated configuration as the FastIron family devices provide no TLS encryption for external authentication servers.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the Brocade FastIron ICX Series Switch/Router 08.0.40: The TOE logical boundary consists of the security functionality of the products summarized in the following subsections:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

Note that use of the following features is limited in the evaluated TOE:

1. The use of SNMP has **not** been subject to evaluation. Note that SNMP can be used only to monitor and not modify any security related configuration settings.
2. The *Strict Password Enforcement* setting is assumed to be **enabled** in the evaluated configuration.
3. The TOE will be operated in Common Criteria mode (a more restricted mode than FIPS mode).

Given that this Security Target conforms to the NDPP, the security claims focus on the TOE as a secure network infrastructure device and do not focus on other key functions provided by the TOE, such as controlling the flow of network packets among the attached networks. However, those functions can be freely used without affecting the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

The TOE includes the ability to communicate with a SYSLOG server in its environment to access its services. The TOE is designed to interact with each of those servers in accordance with their respective protocols, including security capabilities where applicable.

1.4.1.2.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

1.4.1.2.2 Cryptographic support

The TOE is a FIPS-certified cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH and TLS.

1.4.1.2.3 User data protection

The TOE performs a wide variety of network switching and routing functions, passing network traffic among its various network connections. While implementing applicable network protocols associated with network traffic routing, the TOE is carefully designed to ensure that it doesn't inadvertently reuse data found in network traffic. This is accomplished primarily by controlling the size of all buffers, fully overwriting buffer contents, and zero-padding of memory structures and buffers when necessary

1.4.1.2.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules. It provides the ability to both assign attributes (user names, passwords and privilege levels) and to authenticate users against these attributes.

1.4.1.2.5 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management since the Super User allows for complete read-and-write access to the system.

1.4.1.2.6 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

Note that the TOE is a single appliance or a closely grouped (e.g., in the same rack) collection of appliances acting as a unit. As such, no intra-TOE communication is subject to any risks that may require special protection (e.g., cryptographic mechanisms).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

1.4.1.2.7 TOE access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

1.4.1.2.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access to ensure both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs.

1.4.2 TOE Documentation

Brocade offers a series of documents that describe the installation of the FastIron switch/router products as well as guidance for subsequent use and administration of the applicable security features. The following list of documents was examined as part of the evaluation:

- FastIron Ethernet Switch Administration Guide Supporting FastIron Software Release 08.040, Part Number: 53-1004000-01, 18 December 2015
- FastIron Ethernet Switch Security Configuration Guide Supporting FastIron Software Release 08.0.40, Part Number: 53-1003907-0118 December 2015
- FastIron FIPS and Common Criteria Configuration Guide, Supporting FastIron Software Release 08.0.30, 53-1003636-01, 27 July 2015

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.
    - Part 3 Conformant
- The ST conforms to the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014.
- Package Claims:
    - Assurance Level: EAL 1 conformant

      The NDPP defines assurance activities beyond the scope for EAL 1, and this Security Target includes them to ensure that they are within scope of the corresponding evaluation. However, at the present time, international recognition of the evaluation results are limited to defined assurance packages, such as EAL1, and does not extend to Scheme-defined assurance extensions or refinements.

2.1 Conformance Rationale

The ST conforms to the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the NDPP.

3. Security Objectives

The Security Problem Definition may be found in the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014, and this section reproduces only the corresponding Security Objectives for convenience. The NDPP offers additional information about the identified security objectives, but that has not been reproduced here and the NDPP should be consulted if there is interest in that material.

In general, the NDPP has presented a Security Objectives appropriate for network infrastructure devices and as such are applicable to the Brocade FastIron ICX Series Switch/Router 08.0.40.

3.1 Security Objectives for the Environment

OE.NO_GENERAL_PURPOSE
There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.TRUSTED_ADMIN
TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDPP. The NDPP defines the following extended SFRs and since they are not redefined in this ST the NDPP should be consulted for more information in regard to those CC extensions.

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FCS_SSH_EXT.1: Explicit: SSH
- FCS_TLS_EXT.1: Explicit: TLS
- FIA_PMG_EXT.1: Password Management
- FIA_UIA_EXT.1: User Identification and Authentication
- FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014. The refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the NDPP made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDPP which includes all the SARs for EAL1 as defined in the CC. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the NDPP that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL1 assurance requirements alone. As such, those assurance activities have been reproduced in this ST to ensure they are included within the scope of the evaluation effort.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the FastIron Switch/Router Family TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1: Explicit: SSH
	FCS_TLS_EXT.1: Explicit: TLS
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination

	FTA_SSL.4: User-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel
	FTP_TRP.1: Trusted Path

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions;
d) Specifically defined auditable events listed in Table 1 (in the NDPP).

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of Table 1 (in the NDPP).

5.1.1.2 User Identity Association (FAU_GEN.2)

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 External Audit Trail Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1

The TSF shall be able to [***transmit the generated audit data to an external IT entity***] using a trusted channel implementing the [***TLS***] protocol.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1)

FCS_CKM.1.1

Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [

- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;***
- ***NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' for RSA-based key establishment schemes]***

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

5.1.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1

The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.1.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1(1).1

Refinement: The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in [***CBC***] and cryptographic key sizes 128-bits and 256-bits that meets the following:

- FIPS PUB 197, 'Advanced Encryption Standard (AES)'
- [***NIST SP 800-38A***].

5.1.2.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1(2).1

Refinement: The TSF shall perform cryptographic signature services in accordance with a [***(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater***] that meets the following:
[***Case: RSA Digital Signature Algorithm - FIPS PUB 186-2 or FIPS PUB 186-3, 'Digital Signature Standard'***].

5.1.2.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1(3).1

Refinement: The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256,***] and message digest sizes [***160, 256***] bits that meet the following: FIPS Pub 180-3, 'Secure Hash Standard.'

5.1.2.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4))

FCS_COP.1(4).1

Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1, SHA-256***], key size [**equal to the digest size**], and message digest sizes [***160, 256***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

5.1.2.7 Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with [***NIST Special Publication 800-90 using [CTR_DRBG (AES)]***] seeded by an entropy source that accumulated entropy from [***a software-based noise source***].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

5.1.2.8 Explicit: SSH (FCS_SSH_EXT.1)

FCS_SSH_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [***no other RFCs***].

FCS_SSH_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [**256K**] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [***no other algorithms***].

FCS_SSH_EXT.1.5

The TSF shall ensure that the SSH transport implementation uses [***SSH_RSA***] and [***no other public key algorithms***] as its public key algorithm(s).

FCS_SSH_EXT.1.6

The TSF shall ensure that data integrity algorithms used in SSH transport connection is [***HMAC-SHA1***].

FCS_SSH_EXT.1.7

The TSF shall ensure that diffie-hellman-group14-sha1 and [***no other methods***] are the only allowed key exchange methods used for the SSH protocol.

5.1.2.9 Explicit: TLS (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1

The TSF shall implement one or more of the following protocols [***TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)***] supporting the following ciphersuites:
Mandatory Ciphersuites:
- TLS_RSA_WITH_AES_128_CBC_SHA
Optional Ciphersuites:
- [***TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,***

5.1.3 User data protection (FDP)

5.1.3.1 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.1.4 Identification and authentication (FIA)

5.1.4.1 Password Management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:
1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: [***!, @, #, $, %, ^, &, *, (,), [“‘”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “[”, “\”, “]”, “_”, “`”, “{”, “}”, and “~”]***];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.

5.1.4.2 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.4.3 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism, [***[SSH public-key-based authentication mechanism]***] to perform administrative user authentication.

5.1.4.4 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:
- Display the warning banner in accordance with FTA_TAB.1;
- [***[network routing services]***].

FIA_UIA_EXT.1.2

The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.1.5 Security management (FMT)

5.1.5.1 Management of TSF Data (for general TSF data) (FMT_MTD.1)

FMT_MTD.1.1

The TSF shall restrict the ability to manage the TSF data to the Security Administrators.

5.1.5.2 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- [***- Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1,***
- Ability to configure the cryptographic functionality].

5.1.5.3 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR.2.1

The TSF shall maintain the roles: Authorized Administrator.

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions
- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Extended: Protection of Administrator Passwords (FPT_APW_EXT.1)

FPT_APW_EXT.1.1

The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext passwords.

5.1.6.2 Extended: Protection of TSF Data (for reading of all symmetric keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1

The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.6.3 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.1.6.4 TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1

The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.1.6.5 Extended: Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1

The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2

The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3

The TSF shall provide a means to verify firmware/software updates to the TOE using a [***digital signature mechanism***] prior to installing those updates.

5.1.7 TOE access (FTA)

5.1.7.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1

Refinement: The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.7.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.7.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.7.4 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1

Refinement: Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.8 Trusted path/channels (FTP)

5.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1

Refinement: The TSF shall use [***SSH, TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***[TOE update server]***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2

The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server, retrieving a firmware update**].

5.1.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1

Refinement: The TSF shall use [***SSH***] provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2

Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 1 components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM coverage
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

Table 2 EAL 1 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic functional specification (ADV_FSP.1)

ADV_FSP.1.1d
The developer shall provide a functional specification.

ADV_FSP.1.2d
The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c
The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c
The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c
The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4c
The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e
The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d
The developer shall provide operational user guidance.

AGD_OPE.1.1c
The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c
The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c
The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c
The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c
The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c
The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1d

The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3 Requirement Dependency Rationale

As can be seen in the following table all of the SFR and SAR dependencies are satisfied in this ST.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UIA_EXT.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1(*) and FCS_CKM_EXT.4
FCS_CKM_EXT.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(4)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_RBG_EXT.1	none	none
FCS_SSH_EXT.1	FCS_COP.1	FCS_COP.1(*)
FCS_TLS_EXT.1	FCS_COP.1	FCS_COP.1(*)
FDP_RIP.2	none	none
FIA_PMG_EXT.1	none	none
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UAU_EXT.2	none	none
FIA_UIA_EXT.1	none	none
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.2 and FMT_SMF.1
FMT_SMF.1	none	none

FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FPT_APW_EXT.1	none	none
FPT_SKP_EXT.1	none	none
FPT_STM.1	none	none
FPT_TST_EXT.1	none	none
FPT_TUD_EXT.1	none	none
FTA_SSL.3	none	none
FTA_SSL.4	none	none
FTA_SSL_EXT.1	none	none
FTA_TAB.1	none	none
FTP_ITC.1	none	none
FTP_TRP.1	none	none
ADV_FSP.1	none	none
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1
AGD_PRE.1	none	none
ALC_CMC.1	ALC_CMS.1	ALC_CMS.1
ALC_CMS.1	none	none
ATE_IND.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1
AVA_VAN.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1

Table 3 Requirement Dependencies

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security Audit

The TOE is designed to produce syslog conformant messages in a number of circumstances including warnings about the device itself (such as temperature, power failures, etc.) as well as security relevant events (the success and failure login of the user, regardless of the authentication mechanism; changing a user's password; and adding and deleting user accounts). In each case the audit record includes the time and date, identification of the responsible subject (e.g., by network address or user ID), the type of event, the outcome of the event, and other information depending on the event type.

The audit records are stored in a log (internal to the TOE appliance) that is protected so that only an authorized TOE User can read (for which tools accessible via the CLI are provided). The protection results from the fact that the logs can be accessed only after a user logs in (see section 6.4 below).

The log stores up to 50 entries after which the audit entries will be overwritten, oldest first. The administrator (with Super User privilege) can (and should) choose to configure one or more external syslog servers where the TOE will simultaneously send a copy of the audit records. The TOE can be configured to use TLS (using any of the supported ciphersuites) to protect audit logs exported to an external server.

The TOE includes a hardware clock that is used to provide reliable time information for the audit records it generates.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in Table 1 (in the NDPP). Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in Table 1 (in the NDPP).
- FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server. This communication is protected with the use of TLS.

6.2 Cryptographic support

The TOE includes a FIPS 140 certified crypto module providing supporting cryptographic functions. The evaluated configuration requires that the TOE be configured in Common Criteria mode to ensure FIPS certified functions are used.

The following functions have been FIPS certified in accordance with the identified standards.

Functions	Standards	ICX 7250/7450	ICX 7750
Encryption/Decryption			
• AES CBC (128 and 256 bits)	FIPS Pub 197 NIST SP 800-38A	2981	2787
Cryptographic signature services			
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS Pub 186-2	1565	1387
Cryptographic hashing			
• SHA-1, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 256, 384, and 512 bits)	FIPS Pub 180-3	2505	2258
Keyed-hash message authentication			
• HMAC-SHA-1(digest size 160)	FIPS Pub 198-1 FIPS Pub 180-3	1890	1674
Random bit generation			
• CTR_DRBG with sw & hw based noise sources with a minimum of 256 bits of non-determinism	NIST SP 800-90	569	437
Key Derivation Functions			
• TLS and SSH	NIST SP 800-135	390	391

Table 4 Cryptographic Functions

While the TOE generally fulfills all of the NIST SP 800-56B requirements without extensions, the following table specifically identifies the "should", "should not", and "shall not" conditions from the publication along with an indication of how the TOE conforms to those conditions.

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented?	Rationale for deviation
5.6	Should	Yes	Not applicable
5.8	shall not	No	Not applicable
5.9	shall not (first occurrence)	No	Not applicable
5.9	shall not (second occurrence)	No	Not applicable
6.1	should not	No	Not applicable
6.1	should (first occurrence)	Yes	Not applicable
6.1	should (second occurrence)	Yes	Not applicable
6.1	should (third occurrence)	Yes	Not applicable
6.1	should (fourth occurrence)	Yes	Not applicable
6.1	shall not (first occurrence)	No	Not applicable
6.1	shall not (second occurrence)	No	Not applicable
6.2.3	Should	Yes	Not applicable
6.5.1	Should	Yes	Not applicable

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented?	Rationale for deviation
6.5.2	Should	Yes	Not applicable
6.5.2.1	Should	Yes	Not applicable
6.6	shall not	No	Not applicable
7.1.2	Should	Yes	Not applicable
7.2.1.3	Should	Yes	Not applicable
7.2.1.3	should not	No	Not applicable
7.2.2.3	should (first occurrence)	Yes	Not applicable
7.2.2.3	should (second occurrence)	Yes	Not applicable
7.2.2.3	should (third occurrence)	Yes	Not applicable
7.2.2.3	should (fourth occurrence)	Yes	Not applicable
7.2.2.3	should not	No	Not applicable
7.2.2.3	shall not	No	Not applicable
7.2.3.3	should (first occurrence)	Yes	Not applicable
7.2.3.3	should (second occurrence)	Yes	Not applicable
7.2.3.3	should (third occurrence)	Yes	Not applicable
7.2.3.3	should (fourth occurrence)	Yes	Not applicable
7.2.3.3	should (fifth occurrence)	Yes	Not applicable
7.2.3.3	should not	No	Not applicable
8	Should	Yes	Not applicable
8.3.2	should not	No	Not applicable

Table 5 NIST SP800-56B Conformance

The TOE provides RFC compliant TLS and SSH implementations with no security related extensions.

The TOE uses a software-based random bit generator that complies with Special Publication 800-90 using CTR_DRBG when operating in the FIPS mode. AES-256 is used in conjunction with a minimum of 256 bits of entropy accumulated from the processing stack, hardware serial numbers, and the low-order bits from the current time of day.

The TOE supports the following secret keys, private keys and CSPs:

Key or CSP:	Zeroized upon:	Stored in:	Zeroized by:
SSH host RSA private key	Command	Flash	Overwriting once with zeros
SSH host RSA public key	Command	Flash	Overwriting once with zeros
SSH client RSA public key	Command	Flash	Overwriting once with zeros
SSH session key	End of session	RAM	Overwriting once with zeros
TLS host RSA private key	Command	Flash	Overwriting once with zeros
TLS host RSA digital certificate	Command	Flash	Overwriting once with zeros
TLS pre-master secret	Handshake done	RAM	Overwriting once with zeros
TLS session key	Close of session	RAM	Overwriting once with zeros
DH Private Exponent	New key exchange	RAM	Overwritten with new value
DH Public Key	Not applicable	RAM	Public value
User Password	Command	Flash	Overwriting once with zeros
Port Administrator Password	Command	Flash	Overwriting once with zeros
Crypto Officer Password	Command	Flash	Overwriting once with zeros
Firmware Integrity / Load RSA public key	Not applicable	Flash	Public value
DRBG Seed	Every 100ms	RAM	Overwritten with new value
DRBG Value V	Every 100ms	RAM	Overwritten with new value
DRBG Constant C	Every 100ms	RAM	Overwritten with new value

Table 6 Keys and CSPs

The TOE stores all persistent secret and private keys in FLASH and store all ephemeral keys in RAM (as indicated in the above table). Additionally, the TOE is designed to zeroize secret and private keys when they are no longer required by the TOE as detailed below. The TOE's zeroization has been subjected to FIPS 140 validation. Note that zeroization occurs as follows: 1) when deleted from FLASH, the previous value is overwritten once with zeroes; 2) when added or changed in FLASH, any old value is overwritten completely with the new value; and, 3) the zeroization of values in RAM is achieved by overwriting once with zeroes.

The TOE supports the following zeroization methods for its secret keys, private keys and CSPs (note that no public keys appear in this list; they are public and thus need not be zeroizeable). For any given CSP in the table above, there may be multiple zeroization methods available.

- command: *fips zeroize all* - The device zeros out the shared secrets use by various networking protocols including host access passwords, SSH host keys, and TLS host keys with the digital signature.
- command: *no fips enable* or *no fips enable common-criteria* - Zeroizes shared secrets, SSH and TLS host keys, and the TLS certificate *based on the configured FIPS policy*. Either of these commands will take the TOE out of its evaluated configuration and zeroize the secrets assuming a default FIPS policy. An administrator can use the prior command, *fips zeroize all*, to conclusively zeroize all CSPs, secret, and private keys, irrespective of the configured FIPS policy.
- The SSH session key is transient. It zeroized at the end of a session and recreated at the beginning of a new session.
- The TLS pre-master secret is generated during the TLS handshake. It is destroyed after it is used.
- The TLS session key is generated for every TLS session. The TLS session key is deleted after the session is closed.
- The DRBG seed is recomputed periodically on 100 millisecond intervals.
- The DH private exponent is generated at the beginning of DH KEX. A new random number overwrites the memory location used to store the value each time a new session is initiated.
- For SSH, the RSA private key is stored in a locally generated file on flash during the key generation process. The file is removed during zeroization. The *crypto key zeroize* command removes the keys.
- For TLS, the RSA private key is stored in a locally generated file on flash during the key generation process. The private and public key data is overwritten with space characters during zeroization. The *crypto-ssl zeroize* command zeroes out the RSA key pair.

These supporting cryptographic functions are included to support the SSHv2 (compliant with RFCs 4251, 4252, 4253, and 4254) and TLSv1.0 (compliant with RFC 2246), TLS v1.1 (RFC4346), and TLS v1.2 (RFC 5246) secure communication protocols.

The TOE supports TLSv1.0, v1.1, and v1.2 with the cipher suites described in section 5.1.2.9.

The TOE supports SSHv2 with AES (CBC) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1, and RSA (with diffie-hellman-group14-sha1 for the key exchange method). While other ciphers and hashes are implemented in the product, they are disabled while the TOE is operating in Common Criteria or FIPS mode.

The TOE allows users to perform SSHv2 authentication using password based authentication and allows users to upload a public key for SSHv2 public key client authentication. The TOE's SSHv2 implementation limits SSH packets to a size of 256K bytes. Whenever the timeout period or authentication retry limit is reached, the TOE closes the applicable TCP connection and releases the SSH session resources. As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately decrypted. However, if it is not complete when the buffer becomes full (256K bytes) the packet will be dropped and the connection terminated.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: See Table 5 NIST SP800-56B Conformance above.

- FCS_CKM_EXT.4: Keys are zeroized when they are no longer needed by the TOE.
- FCS_COP.1(1): See Table 4 Cryptographic Functionsabove.
- FCS_COP.1(2): See Table 4 Cryptographic Functionsabove.
- FCS_COP.1(3): See Table 4 Cryptographic Functionsabove.
- FCS_COP.1(4): See Table 4 Cryptographic Functionsabove.
- FCS_RBG_EXT.1: See Table 4 Cryptographic Functionsabove.
- FCS_SSH_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above.

6.3 User data protection

The TOE is designed to ensure its own internal integrity as well as to protect user data from potential, unintended reuse by clearing resources (e.g., memory) as they are allocated to create objects used in the implementation of the TOE operations. Note that volatile memory is the primary resource involved in normal TOE execution while its persistent storage is based on non-volatile flash memory.

When the TOE sends a network packet, it must request a buffer from the buffer pool. After using a buffer, the TOE releases the buffer back to the buffer pool. In response to a request, the buffer pool will return a buffer and its length, where the length is greater than or equal to that requested. The TOE will compare the length of the returned buffer to that which it requested (the size of the packet), overwrite the returned buffer with packet data (destroying any residual data present in the buffer), and, if the provided buffer exceeds the requested size of the packet, overwrite any extra space with zeros (thus ensuring that no residual data can leak from the TOE).

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_RIP.2: The TOE always overwrites resources when allocated for use in objects.

6.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except to display a message of the day banner and to permit network routing services without identification or authentication. The TOE allows both unauthenticated network routing services to route network traffic through the TOE as well as unauthenticated network routing protocol traffic destined to the TOE (including DNS, ARP, ICMP, BootP, DHCP, RIP, OSPF, BGP, VRRP, VRRP-E, Multi-VRF) but does not include any management configuration of the TOE's network routing services. The TOE authenticates TOE Users against their user name, password and privilege level.

The Authorized Administrator with Super User privilege represents the "administrator" referred to in the security requirements of the protection profile. Other accounts with privileges other than Super User were not tested during the evaluation. The Authorized Administrator with Super User privilege defines local user (or TOE User) accounts and assigns passwords and privilege levels to the accounts. Each user account has a user name, password, and a privilege level associated with it. There is a default privilege level account associated with each privilege level and each has its own password. It is up to the Authorized Administrator with Super User privilege to decide whether or how to use these legacy accounts. Note however, that each has an identity, password, and privilege level.

The user roles offered by the TOE are categorized differently when described in FIPS documentation. Specifically, the Authorized Administrator with Super User privilege equates to the FIPS Crypto Officer Role, the Port Configuration User equates to the FIPS Port Configuration Administrator Role (and has write access to the interface configuration mode only), and a user with read-only privileges and no configuration mode access equates to the FIPS User Role.

While the Authorized Administrator with Super User privilege can create or otherwise modify accounts freely, other users cannot change their own (or any other) security attributes. Note that the TOE supports a password enforcement configuration where the minimum password length can be set by an administrator up to 48 characters.

Passwords can be created using any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1).

Additional authentication mechanisms can also be configured by an Authorized Administrator using an Authentication Method List. This allows some flexibility in setting up authentication mechanisms when desired. The available mechanisms include the Local Password for the Super User Privilege level and the SSH public key authentication mechanism. An administrator can create users, associate passwords with user accounts, and can also set the privilege level associated with a user. Users, after authenticating, may upload a public key to be used with SSH client public key authentication. When authentication succeeds, the TOE looks up the user's defined privilege level, assigns that to the user's session, and presents the user with a command prompt (the "#" character, e.g., "`Brocade(config)#`").

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above.
- FIA_UAU.7: The TOE does not echo passwords as they are entered; rather '*' characters are echoed when entering passwords.
- FIA_UAU_EXT.2: The TOE can be configured to utilize local password-based authentication and SSH public-key-based authentication mechanisms.
- FIA_UIA_EXT.1: The TOE doesn't offer any services or access to its functions, except for the switching/routing of network traffic and displaying a message of the day banner, without requiring a user to be identified and authenticated.

6.5 Security management

The TOE associates each defined user account with a privilege level. The most privileged level is Super User (with regards to the requirements in this Security Target users with lesser privilege levels are referred to collectively simply as TOE users since such users do not have complete read-and-write access to the system). Again, as stated in section 6.4, other accounts with privileges other than Super User were not tested during the evaluation. The TOE implements an internal access control mechanism that bases decisions about the use of functions and access to TOE data on those privilege levels. In this manner, the TOE is able to ensure that only the Authorized Administrator with Super User privilege can access audit configuration data, information flow policy ACLs, user and administrator security attributes (including passwords and privilege levels), authentication method lists, the logon failure threshold, the remote access user list; and cryptographic support settings.

Other than the Super User level, the TOE implements a Read Only level where only basic commands can be issued and no changes can be made and a Port Configuration level where non-security device parameters can be managed. Collectively, this ST refers to all users of the TOE as "TOE Users" where the "Authorized Administrator with Super User privilege" is a subset of that broader role.

The TOE offers command line functions which are accessible via the CLI. The CLI is a text based interface which can be accessed from a directly connected terminal or via a remote terminal using SSH. These command line functions can be used to effectively manage every security policy, as well as the non-security relevant aspects of the TOE.

Note that the TOE does not offer a Web Management Interface when configured for Common Criteria Mode. When running in Common Criteria Mode, the TOE only offers a CLI access from a directly connected terminal or via a remote terminal using SSH.

The following table provides the list of security-related commands used to configure or examine the TOE security settings. The services listed here reflect the minimal set needed to properly configure the TOE to comply with the requires of the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014.

Command	Tested Command Variantts	Description
write	write memory	Write to persistent storage
crypto	crypto key generate	Invoke cryptographic functions

Command	Tested Command Variantts	Description
openssl	openssl s_server	Configure secure connections (e.g., with syslog)
logging	logging host <ip-address> ssl-port <port>	Configure the audit logging host
boot	boot system flash <primary or secondary>	Boot the selected flash image
console	console timeout <time>	Manage console properties
banner	banner motd +	Manage the login banner
exit	exit	Logout or exit current session
ntp	ntp	Switch to ntp configuration mode
config	config t	Switch to configuration mode
username	username <user> password	Manage user accounts
clock	clock set <time>	Manage the internal clock
server	server <ntp server ip> minpoll <time>	Configure external services
crypto-ssl	crypto-ssl certificate generate	Manage web server properties
fips	fips enable common-criteria fips show fips zeroize all	Manage FIPS and Common Criteria configuration
ip	ip ssh pub-key-file ip ssh idle-time <time>	Manage ip connection (e.g., ssh) configuration
aaa	aaa authentication	Configure the aaa authentication functions
enable	enable aaa enable password-min-length 15 enable user password-masking	Enable console login features
show	show flash show ver show clock show ip client-pub-key show ip ssl show logging show run | <options>	Show identified configuration information

Table 7 Security Related Configuration Commands

The TOE also provides a comprehensive set of network routing configuration commands. These commands were not exercised as the above services in Table 7 represent the minimum set of commands needed to for proper configuration.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MTD.1: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Authorized Administrator with Super User privilege (aka Security Administrator).
- FMT_SMF.1: The TOE includes the functions necessary to enable/disable available network services, to manage the cryptomodule and associated functions, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.2: The TOE includes roles associated with privileges. 'Authorized Administrator with Super User privilege' corresponds to the required 'Authorized Administrator' also referred to as 'Security Administrator' in some requirements.

6.6 Protection of the TSF

The TOE is an appliance and as such is designed to work independent of other components to a large extent. Secure communication with third-party peers as addressed in section 6.8, Trusted path/channels, and secure communication among multiple instances of the TOE is limited to a direct link between clustered switch appliances. Normally clustered components are co-located and connected via a link that would not be exposed outside of the same physical environment. As such, no additional protection (e.g., encryption) should be necessary in most operational environments.

While the administrative interface is function rich, the TOE is designed specifically to not provide access to locally stored passwords (which can be administratively configured to be protected by MD-5, SHA-1, or SHA-256) and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE. The TOE is a hardware appliance that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The TOE can be configured to periodically synchronize its clock with a time server, but the TOE can only ensure its own reliability and not that of an external time mechanism. The TOE also implements the timing elements through timeout functionality due to inactivity for terminating both local and remote sessions. Note that the clock is used primarily to provide timestamp for audit records, but is also used to supporting timing elements of cryptographic functions.

The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. An administrator can configure the TOE to reboot or to stop, with errors displayed, when an error is encountered. When operating in FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self-testing. The module performs Cryptographic algorithm known answer tests, firmware integrity tests using RSA signature verification and conditional self-tests for DRBG, Hardware RNG, Pair-wise consistency tests on generation of RSA keys, and a Firmware load test (RSA signature verification). Upon failing any of its FIPS mode power-on self-tests, the TOE will refuse to boot.

The TOE supports loading a new software image manually by the administrator using CLI commands. From the CLI, an administrator can use SCP in order to download a software image, and the TOE, prior to actually installing and using the new software image, will verify its digital certificate using the public key in the certificate configured in the TOE. An unverified image cannot be installed. Note that the TOE comes preinstalled with an applicable Brocade public certificate.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password. Furthermore, locally defined passwords are not stored in plaintext form.
- FPT_STM.1: The TOE includes its own hardware clock.
- FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics that will serve to ensure the TOE is functioning properly. The tests include ensure memory and flash can be accessed as expected, to ensure that software checksums are correct, and also to test the presence and function of plugged devices.
- FPT_TUD_EXT.1: The TOE provides function to query the version and upgrade the software embedded in the TOE appliance. When installing updated software, digital signatures are used to authenticate the update to ensure it is the update intended and originated by Brocade.

6.7 TOE access

The TOE can be configured to display an administrator-configured message of the day banner that will be displayed before authentication is completed (before the user enters his password). The banner will be displayed when accessing the TOE via the console or SSH interfaces.

The TOE can be configured by an administrator to set a session timeout value (any value up to 240 minutes, with 0 disabling the timeout) – the default timeout is disabled. A session (local or remote) that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. Upon exceeding the session timeout (if set), the TOE logs the user off, but leaves the user's console displaying the last contents.

The user will be required to login in after any session has been terminated due to inactivity or after voluntary termination. Of course, administrators can logout of local or remote sessions at any time.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4: The TOE provides the function to logout (or terminate) the both local and remote user sessions as directed by the user.
- FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE, allowing administrators to terminate their session prior to performing any functions.

6.8 Trusted path/channels

The TOE implements SSHv2, which is required to be used for remote administration. When an administrator attempts to connect to the TOE, the TOE attempts to negotiate a session. If the session cannot be negotiated, the connection is dropped..

When a client attempts to connect using SSH, the TOE and the client will negotiate the most secure algorithms available at both ends to protect that session. SSH_RSA is the only public key authentication algorithm used by the SSH transport implementation, and DH group 14 is the only Diffie-Hellman group the TOE supports when configured in Common Criteria mode.

In each case, AES-CBC with 128-bit or 256-bit keys is implemented for encryption and decryption and RSA using up to 2048-bit keys are implemented for key exchange and authentication (i.e., distribution).

Remote connections to SYSLOG servers are protected using TLS (as specified earlier).

In all cases, the endpoints are assured by virtue of the certificates installed, trusted, and reviewable when connecting and by virtue of user authentication.

The TOE update service is secured using SCP, as when operating in FIPS (or Common Criteria) Mode, the TOE prevents the use of TFTP to retrieve a new TOE firmware image.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that any authentication operations and exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides SSH, based on its embedded cryptomodule, to ensure secure remote administration. The administrator can initiate the remote session, the remote session is secured (disclosure and modification) using FIPS certified cryptographic operations, and all remote security management functions require the use of one of these secure channels.