Brocade Communications Systems, Inc. Brocade Directors and Switches 7.3 (NDPP11e3) Security Target

Version 1.0
March 18, 2015

Prepared for:

Brocade Communications Systems, Inc.

130 Holger Way
San Jose, CA 95134

Prepared By:

www.gossamersec.com

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 Directors and Switches 7.3. The TOE is being evaluated as a network infrastructure device.

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.

Acronyms and Terminology

This following acronyms and terms are used throughout this document.

DEK	Data Encryption Key
FC	Fibre Channel
FCIP	Fibre Channel over IP
HBA	Host Bus Adapter

JBOD	Stands for "Just a Bunch of Disks", and it a way of connecting together a series of hard drives, combining multiple drives and capacities, into one drive
LUN	Logical Unit Number, used to refer to a logical device within a chain.
SAN	Storage Area Network

1.1 Security Target Reference

ST Title – Brocade Communications Systems, Inc. Brocade Directors and Switches 7.3

ST Version – Version 1.0

ST Date – March 18, 2015

1.2 TOE Reference

TOE Identification – Brocade Communications Systems, Inc. Brocade Communications Systems, Inc. Brocade Directors and Switches operating with FabricOS version 7.3.0a1, including the following series and models

- Director Blade[1] Models: FC8-16, FC8-32, FC8-48, FC8-64, FC16-32, FC16-48, CP8, CR8, CR4S-8, CR16-4, CR16-8, FX8-24
- Director Models: DCX, DCX-4S, DCX 8510-4, DCX 8510-8
- Switch Appliance Models: 300, 6510, 6520, 7800, 7840

TOE Developer – Brocade Communications Systems, Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is the Brocade Directors and Switches 7.3 family of products provided by Brocade Communications Systems, Inc. Brocade Directors and Switches 7.3 are hardware network devices that implement what is called a 'Storage Area Network' or 'SAN'. SANs provide connections between servers that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment.

1.4 TOE Description

The Target of Evaluation (TOE) is the Brocade Directors and Switches 7.3. The various models of the TOE identified below differ in performance, form factor and number of ports, but all run the same FabricOS version 7.3.0a1 software. The TOE is available in two form factors:

1. a rack-mount Director chassis with a variable number of blades, and
2. a self-contained switch appliance device

Director models are composed of blades of several types. A 'director blade model' is a control blade (CP8), a core switch blade (CR8 or CR4S-8, CR16-4, CR16-8), and port blades (FC8-16, FC8-32, FC8-48, FC8-64, FC16-32, FC16-48) or application blades (FX8-24). Control blades contain the control plane for the chassis. A core switch blade contains the ASICs for switching between port blades. A port blade supports various numbers of ports and speeds. Application blades provide additional capabilities such as FC over Ethernet. The DCX, DCX-4S, DCX 8510-4 and DCX 8510-8 require at least one control blade and one core blade to make the director operational.

Director Model	Blades

[1] A blade refers to a purpose-built component that is installed in a Brocade director.

DCX	CP8, CR8, FC8-16, FC8-32, FC8-48, FC8-64, FX8-24,
DCX-4S	CP8, CR4S-8, FC8-16, FC8-32, FC8-48, FC8-64, FX8-24
DCX 8510-4	CP8, CR16-4, FC8-64, FC16-32, FC16-48, FX8-24
DCX 8510-8	CP8, CR16-8, FC8-64, FC16-32, FC16-48, FX8-24

Brocade Directors and Switches are hardware appliances that implement what is called a "Storage Area Network" or "SAN". SANs provide physical connections between machines in the environment containing a type of network card called a Host Bus Adapter (HBA) that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment. The network connection between the storage devices in the environment, the TOE, and HBAs in the environment use high-speed network hardware. SANs are optimized to transfer large blocks of data between HBAs and storage devices. SANs can be used to replace or supplement server-attached storage solutions, for example.

The basic concept of operations from a *user's* perspective is depicted below. Actual implementation may interconnect multiple instances of TOE models.

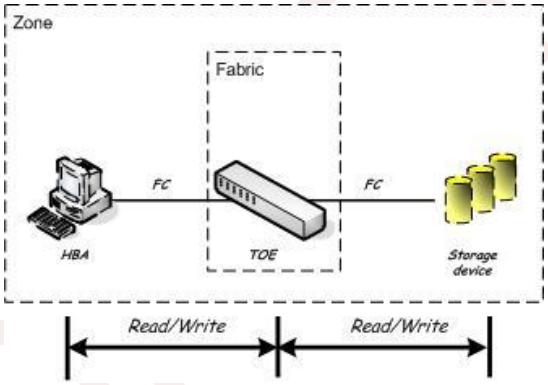

Figure 1: Host bus adapters can only access storage devices that are members of the same zone.

HBAs communicate with the TOE using Fibre Channel (FC) or FC over IP (FCIP) protocols. Storage devices in turn are physically connected to the TOE using FC/FCIP interfaces. When more than one instance of the TOE is interconnected (i.e. installed and configured to work together), they are referred to collectively as a "SAN fabric". A zone is a specified group of fabric-connected devices (called zone members) that have access to one another.

1.4.1 TOE Architecture

The TOE provides the ability to centralize the location of storage devices in a network in the environment. Instead of attaching disks or tapes to individual hosts in the environment, or for example attaching a disk or tape directly to the network, storage devices can be physically attached to the TOE, which can then be physically attached to host bus adapters in the environment. Host bus adapters that are connected to the TOE can then read from and write to storage devices that are attached to the TOE according to TOE configuration. Storage devices in the environment appear to the operating system running on the machine that the host bus adapter is installed in as local (i.e. directly-attached) devices.

More than one host bus adapter can share one or more storage devices that are attached to the TOE according to TOE configuration. Scalability is achieved by interconnecting multiple instances of TOE directors and switches to form a fabric that supports different numbers of host bus adapters and storage devices.

Directors and switches both can be used by host bus adapters to access storage devices using the TOE. Switch appliances provide a fixed number of physical interfaces to hosts and storage devices in the environment. Directors provide a configurable number of physical interfaces using a chassis architecture that supports the use of blades that can be installed in and removed from the director chassis according to administrator configuration.

There are administrative interfaces to manage TOE services that can be accessed using an Ethernet network, as well as interfaces that can be accessed using a directly-attached console as follows:

- Ethernet network-based web-based administrator console interfaces – Provides web-based administrator console interfaces called the "Brocade Advanced Web Tools."
- Ethernet network-based command-line administrator console interfaces – Provides command-line administrator console interfaces called the "FabricOS Command Line Interface."
- Serial terminal-based command-line administrator console interfaces – Provides command-line administrator console interfaces called the "FabricOS Command Line Interface."

There also exists administrative Ethernet network-based programmatic API interfaces that can be protected using SSL. The API interface is not supported in the evaluated configuration. Similarly, there exists a modem hardware component that is optional to the product that can be used in a similar manner as a serial console port, but it is disabled by virtue of not being physically installed during initial installation and configuration in the evaluated configuration.

The TOE can operate in either "Native Mode" or "Access Gateway Mode". Only Native mode is supported in the evaluated configuration. Access Gateway mode makes the switch function more like a "port aggregator" and in Access Gateway mode the product does not support the primary access control security functions (mainly zoning) claimed when operating in Native mode.

The basic concept of operations from an *administrator's* perspective is depicted below. While actual implementations may interconnect multiple instances of TOE models, each TOE device (i.e., instance of the TOE) is administered individually.

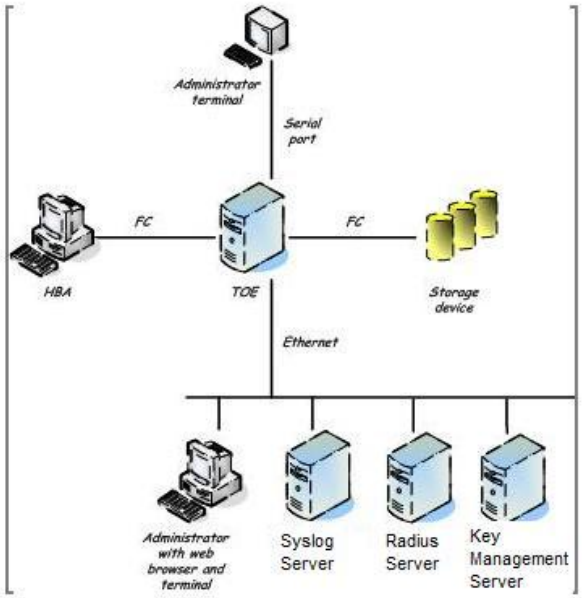

Figure 2: Administrators can access the TOE using a serial terminal or across a network. Audit records are sent to a syslog server.

Separate appliance ports are relied on to physically separate connected HBAs. The appliance's physical location between HBAs and storage devices is relied on to ensure TOE interfaces cannot be bypassed. The TOE encrypts commands sent from terminal applications by administrators using SSH for the command line interface and HTTPS for the Advanced Web Tools GUI interface. The TOE requires administrators to login before a SSH or HTTPS session is established.

1.4.1.1 Physical Boundaries

The TOE can be described in terms of the following components:

- Brocade Switch and Director appliances – One or more of each type are supported in the evaluated configuration. The evaluated configuration also supports one or more blades per director, depending on the number supported by a given director model.
- Brocade FabricOS operating system – Linux-based operating system that runs on Brocade switches and directors. FabricOS is comprised of user-space programs, kernel daemons and kernel modules loaded as proprietary components into LINUX. The base features of LINUX, including the file system, memory management, processor and I/O support infrastructure for FOS user-space programs, daemons, and kernel modules. Interprocess communication is handled through commonly mapped memory or shared PCI memory and semaphores as well as IOCTL parameter passing. LINUX provides access to memory or to make a standard IOCTL call, and all the contents of the buffers and IOCTL message blocks or other message blocks are proprietary to the FOS user-space programs, kernel modules and daemons. The FabricOS operating system is considered to include the OpenSSL crypto engine as internal functionality supporting TOE operation.

In its most basic form, the TOE in its intended environment of the TOE is depicted in the figure below.

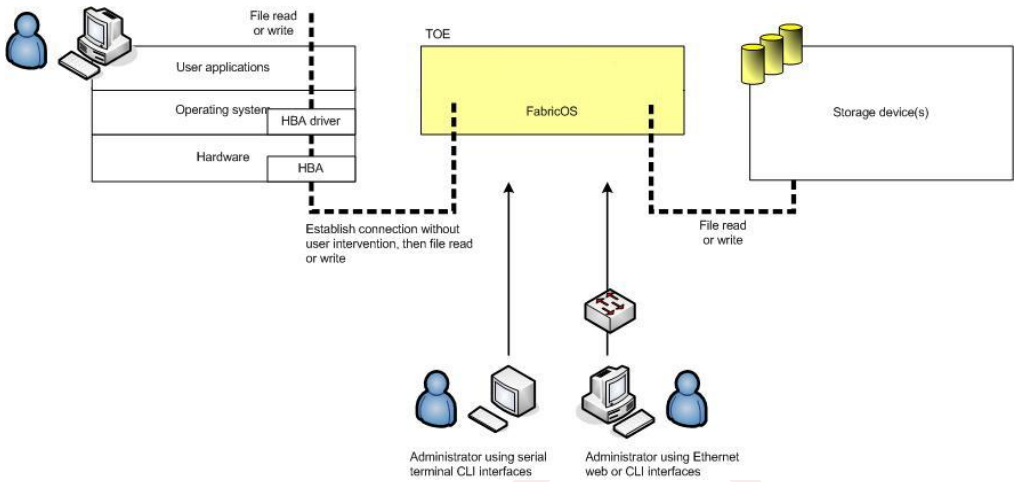

Figure 3: TOE and environment components.

The intended environment of the TOE can be described in terms of the following components:

- Host – A system in the environment that uses TOE SAN services.
- Host Bus Adapters (HBAs) – Provides physical network interfaces from host machines in the environment to the TOE. HBA drivers provide operating system interfaces on host machines in the environment to storage devices in the environment. Storage devices in the environment appear to the host operating system as local (i.e. directly-attached) devices.
- Storage device – A device used to store data (e.g. a disk or tape) that is connected to the TOE using a FC/FCIP connection and is accessed by a host using the TOE.
- Terminal application – Provides a runtime environment for console-based (i.e. SSH) client administrator console interfaces.
- Web browser – Provides a runtime environment for web-based (i.e. HTTPS) client administrator console interfaces.
- Syslog server – Provides logging to record auditable event information generated by the TOE. The syslog server is expected to protect audit information sent to it by the TOE and make that data available to administrators of the TOE.
- RADIUS/LDAP Server – An optional component that can perform authentication based on user credentials passed to it by the TOE. The TOE then enforces the authentication result returned by the RADIUS or LDAP Server.
- Certificate Authority (CA) – Provides digital certificates for SSH and HTTPS-based interfaces that are installed during initial TOE configuration. After installation, the CA no longer needs to be on the network for operation.
- Key management systems -- Provide life cycle management for all DEKs created by the encryption engine. Key management systems are provided by third party vendors and are not included in the scope of this evaluation.

The TOE relies on a syslog server in the environment to store and protect audit records that are generated by the TOE. The TOE can be configured to use a RADIUS or LDAP Server for authentication. The TOE does not rely on any other components in the environment to provide security-related services.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by Brocade Directors and Switches:

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

1.4.1.2.1 Security audit

The TOE generates audit events for numerous activities including policy enforcement, system management and authentication. A syslog server in the environment is relied on to store audit records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware. When the syslog server writes the audit record to the audit trail, it applies its own time stamp, placing the entire TOE-generated syslog protocol message MSG contents into an encapsulating syslog record.

1.4.1.2.2 Cryptographic support

The TOE contains FIPS-certified cryptographic implementations that provide 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

While implementing SAN and HBA protocols, the TOE is carefully designed to ensure that it doesn't inadvertently release or leak residual data. When the TOE allocates a new buffer for either an incoming or outgoing a network packet, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, and additional space will be overwritten (padded) with zeros before the packet is forwarded (either to an external network of HBA or written to a storage device) on both Ethernet and FiberChannel connections.

1.4.1.2.4 Identification and authentication

The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user, and an administrative role must be assigned. Either the TOE performs the validation of the login credentials or the information is passed to a RADIUS or LDAP Server to perform the validation and the TOE enforces the decision. The administrator can configure the order in which the external authentication provider and the local credentials are checked.

1.4.1.2.5 Security management

The TOE provides serial terminal (command line) and Ethernet network-based (command-line and web) management interfaces. Each of the three types of interfaces provides equivalent management functionality. The TOE provides administrative interfaces to configure hard zoning, as well as to set and reset administrator passwords. By default, host bus adapters do not have access to storage devices.

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, and 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 enforces a trusted path between the TOE administrators and the TOE using SSH and TLS/HTTPS connections for Ethernet connections from the Administrator terminal to the TOE. The TOE encrypts commands sent from terminal applications by administrators using SSH for the command line interface and TLS/HTTPS for the Advanced Web Tools GUI interface.

1.4.2 TOE Documentation

Brocade offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

- Brocade - FabricOS Administrator's Guide Supporting Fabric OS v7.3.0 – Publication #53-1003130-01, 13 October 2014
- Brocade – FabricOS Command Reference Supporting Fabric OS v7.3.0 – Publication #53-1003131-01, 27 June 2014
- Brocade – FabricOS Message Reference Supporting Fabric OS v7.3.0 – Publication #53-1003140-01, 01 July 2014
- Brocade – FabricOS Common Criteria Certification, draft version 10

Comment [A1]: This needs to be updated.

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 2012.
  - Part 3 Conformant
- 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

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 PP.

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 operational environment for reader convenience. The NDPP offers additional information about the identified security objectives, but that has not been reproduced here and the Protection Profile should be consulted if there is interest in that material.

In general, the NDPP has defined Security Objectives appropriate for network infrastructure devices and as such are applicable to the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014.

3.1 Security Objectives for the TOE

O.DISPLAY_BANNER
The TOE will display an advisory warning regarding use of the TOE.

O.PROTECTED_COMMUNICATIONS
The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

O.RESIDUAL_INFORMATION_CLEARING
The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

O.SESSION_LOCK
The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.

O.SYSTEM_MONITORING
The TOE will provide the capability to generate audit data and send those data to an external IT entity.

O.TOE_ADMINISTRATION
The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

O.TSF_SELF_TEST
The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

O.VERIFIABLE_UPDATES
The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

3.2 Security Objectives for the Operational 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 Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014 (NDPP11e3). The NDPP11e3 defines the following extended requirements and since they are not redefined in this ST the NDPP11e3 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_HTTPS_EXT.1: Explicit: HTTPS
- 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_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- 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 (NDPP11e3). The refinements and operations already performed in the PP are not identified (e.g., highlighted) here, rather the requirements have been copied from the PP and any residual operations have been completed herein. Of particular note, the PP 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 NDPP11e3 which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the PP that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 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 Brocade Communications Systems, Inc. Brocade Directors and Switches 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_HTTPS_EXT.1: Explicit: HTTPS
	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_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	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: Inter-TSF 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 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' for elliptic curve-based key establishment schemes and implementing 'NIST curves' P-256, P-384 and [P-521] (as defined in FIPS PUB 186-3, 'Digital Signature Standard');

- 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
(3) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater]
that meets the following:

[***Case: RSA Digital Signature***
Algorithm - FIPS PUB 186-2 or FIPS PUB 186-3, 'Digital Signature Standard'
Case: Elliptic Curve Digital Signature Algorithm
FIPS PUB 186-3, "Digital Signature Standard"
The TSF shall implement "NIST curves" P-256, P-384 and [P-521] (as defined in 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, SHA-512***] and message digest sizes [***160, 256, 512***] 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, SHA-512***], key size [**equal to the input block size**], and message digest sizes [***160, 256, 512***] 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 Explicit: HTTPS (FCS_HTTPS_EXT.1)

FCS_HTTPS_EXT.1.1
The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2
The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.1.2.8 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 [***FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using 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.

5.1.2.9 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, ECDSA-SHA2-NISTP256***] and [***no other 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, HMAC-SHA2-256, HMAC-SHA2-512***].
FCS_SSH_EXT.1.7
The TSF shall ensure that diffie-hellman-group14-sha1 and [***ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384, ECDH-SHA2-NISTP521***] are the only allowed key exchange methods used for the SSH protocol.

5.1.2.10 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_RSA_WITH_AES_128_CBC_SHA256,
TLS_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: [***!, @, #, $, %, ^, &, *, (,)***];
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 , external RADIUS server, and external LDAP server]***] 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 and SAN 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 [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***authentication server, [LDAP 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 [**transfer of audit records, verification of user identity via remote authentication server**].

5.1.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1

Refinement: The TSF shall use [***SSH, TLS/HTTPS***] 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.

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 generates audit records for start-up and shutdown of the TOE, all administrator actions, and for an unspecified level of audit (see table below for specific events). Audit records include date and time of the event, type of event, user identity that caused the event to be generated, and the outcome of the event. The TOE maintains a local audit log buffer that retains the last 256 messages persistently, overwriting the oldest events as necessary, and is only accessible by TOE administrators after logging in. The TOE sends audit records to a configured syslog server in the environment. The environment is relied on to provide interfaces to read from the audit trail. The auditable events include:

Requirement Component	Auditable event	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of the audit functions (specifically, of the TOE)	
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Failure to establish an SSH session. Establishment/Termination of an SSH session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FMT_SMF.1	All administrator actions	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session. *Not applicable since the TOE sessions cannot be locked.*	
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	
FTA_SSL.4	The termination of an interactive session.	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.

FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Syslog protocol messages containing audit records have three parts. The first part is called the PRI, the second part is the HEADER, and the third part is the MSG. The TOE generates syslog audit records as follows:

- The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the underlying TOE appliance hardware.

  Each audit record contains the following fields:

  AUDIT, <Timestamp generated by TOE>, <Event Identifier>, <Severity>, <Event Class>, <Username>/<Role>/<IP address>/<Interface>/<Application name>, <Admin Domain>/<Switch name>, <Reserved field for future expansion>, <Message>

  For example:

  AUDIT, 2006/12/10-09:54:03 (GMT), [SEC-1000], WARNING, SECURITY, JohnSmith/root/192.168.132.10/Telnet/CLI, Domain A/JohnsSwitch, , Incorrect password during login attempt

- The audit record is packaged into a syslog protocol message. The complete audit record is packaged into the syslog MSG part. The PRI and HEADER are then added.
- A network connection is established with the syslog server in the environment and the audit record is sent.

When the syslog server writes the audit record to the audit trail, it applies its own time stamp, placing the entire TOE-generated syslog protocol message MSG contents into an encapsulating syslog record, as depicted below.

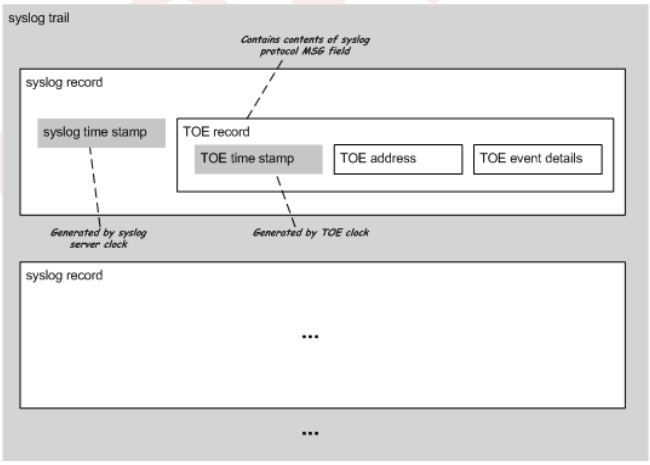

Figure 4: TOE and environment audit record components.

Since the time stamp applied by the TOE was included as part of the event details, the time stamp in the event details can be used to determine the order in which events occurred on the TOE. Similarly, the instance of the TOE that generated the record can be determined by examining the field containing the IP address of the TOE.

For example:

Jun 20 11:07:11 [10.33.8.20.2.2] raslogd: AUDIT, 2006/12/10-09:54:03 (GMT), [SEC-1000], WARNING, SECURITY, JohnSmith/root/192.168.132.10/Telnet/CLI, Domain A/JohnsSwitch, , Incorrect password during login attempt.

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

- FAU_GEN.1: The TOE generates audit events for the not specified level of audit. A syslog server in the environment is relied on to store audit records generated by the TOE.
- 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 cryptomodule providing supporting cryptographic functions. The evaluated configuration requires that the TOE be configured in FIPS mode to ensure FIPS certified functions are used.

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

Functions	Standards	Cert AMCC PPC 440EPX	PPC 400GPX and PPC 8548
Encryption/Decryption			
• AES CBC (128 and 256 bits)	FIPS Pub 197 NIST SP 800-38A	2876	2893
Cryptographic signature services			
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS Pub 186-4	1514	1523
• ECDSA Digital Signature Algorithm (P-256, 384, 521)	FIPS Pub 186-4	518	523
Cryptographic hashing			
• SHA-1/256/512 (digest sizes 160, 256, and 512 bits)	FIPS Pub 180-3	2417	2436
Keyed-hash message authentication			
• HMAC-SHA-1, HMAC_SHA2-256, HMAC-SHA2-512 (digest sizes 160, 256, and 512 bits)	FIPS Pub 198-1 FIPS Pub 180-3	1814	1829
Random bit generation			
• RNG with sw based noise sources	ANSI X9.31	1284	1289
Component Validation List			
• ECC CDH	NIST SP 800-56A	311	320
Key Derivation Functions			
• TLS and SSH	NIST SP 800-135	312	321

Table 3 Cryptographic Functions

The TOE generally fulfills all of the NIST SP 800-56A and SP 800-56B requirements without extensions. The TOE does not perform any operations marked as “shall not” or “should not” and performs all operations marked as “shall” or “should”. For elliptic curve and finite-field based key establishment, the TOE implements the following

sections of SP 800-56A: 5.6 and all subsections. For RSA key establishment, the TOE implements the following sections of SP 800-56B: 6 and all subsections.

The TOE uses a software-based random bit generator that complies with ANSI X9.31 using AES-256 when operating in the FIPS mode. AES-256 is used in conjunction with a minimum of 256 bits of entropy accumulated from the timing of disk I/O completion events and the low-order bits from the CPU clock.

Additionally, the TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. This function has also been subject to FIPS 140 certification. 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 following Critical Security Parameters are contained in the module:

- DH Private Keys for use with 2048 bit modulus in SSHv2 (FLASH)
- SSH Session Keys- 128 and 256 bit AES CBC (RAM)
- SSH Authentication Keys - 2048 bit RSA private/public key pair (FLASH)
- SSH KDF Internal State (RAM)
- SSH DH Shared Secret Key – 2048 bit key size (RAM)
- TLS Private Key (RSA 1024) (FLASH)
- TLS Pre-Master Secret – 48 byte key size (RAM)
- TLS Master Secret – 48 byte key size (RAM)
- TLS PRF Internal State (RAM)
- TLS Session Key – 128 bit AES (RAM)
- TLS Authentication Key for HMAC-SHA-1 (RAM)
- Approved RNG Seed Material (RAM)
- ANSI X9.31 DRNG Internal State (RAM)
- Passwords (FLASH)

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), TLSv1.1 (compliant with RFC 4346), and TLSv1.2 (compliant with RFC 5246) secure communication protocols.

The TOE supports TLSv1.0, TLSv1.1, and TLSv1.2 with AES (CBC) 128 or 256 bit ciphers, in conjunction with SHA-1 and SHA-256 and RSA. The following cipher suites are implemented by the TOE:

1. TLS_RSA_WITH_AES_128_CBC_SHA,
2. TLS_RSA_WITH_AES_256_CBC_SHA,
3. TLS_RSA_WITH_AES_128_CBC_SHA256, and
4. TLS_RSA_WITH_AES_256_CBC_SHA256.

The TOE supports SSHv2 with AES (CBC) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1, HMAC-SHA2-256, and HMAC-SHA2-512 and RSA and ECDH using the following key exchange methods.

1. diffie-hellman-group14-sha1,
2. ecdh-sha2-nistp256,
3. ecdh-sha2-nistp384,
4. ecdh-sha2-nistp521

The TOE also supports SSH_RSA and ecdsa-sha2-nistp256 for server authentication. While other ciphers and hashes are implemented in the product, they are disabled while the TOE is operating in FIPS mode.

The SSHv2 supports both public-key and password based authentication can be configured; and packets are limited to 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.

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

- FCS_CKM.1: See table above.
- FCS_CKM_EXT.4: See list above.
- FCS_COP.1(1): See table above.
- FCS_COP.1(2): See table above.
- FCS_COP.1(3): See table above.
- FCS_COP.1(4): See table above.
- FCS_HTTPS_EXT.1: The TOE implements HTTPS using TLS and compliant with RFC 2818.
- FCS_RBG_EXT.1: See table above.
- FCS_SSH_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above.
- FCS_TLS_EXT.1: The TOE supports TLS sessions for exporting audit data.

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 a network packet is sent, the buffer used by the packet is recalled and managed by the buffer pool. After that, if a new packet acquires a buffer from the buffer pool, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, and additional space will be overwritten (padded) with zeros before the packet is forwarded (either to an external network of HBA or written to a storage device) on both Ethernet and FiberChannel connections.

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 defines administrative users in terms of:

- user identity; and
- password; and
- role.

Role permissions determine the functions that administrators may perform. Nine roles, each with a fixed set of permissions, are supported: Root, Factory, Admin, FabricAdmin, SecurityAdmin, SwitchAdmin, BasicSwitchAdmin, ZoneAdmin, Operator and User. There are four pre-defined administrator accounts called “root”, “factory”, “admin” and “user”, each of which is assigned the respective role of the same name, e.g. the “admin” account is assigned the Admin role. Note that neither the account called “user” nor any account that is assigned the User role, corresponds to a host bus adapter that is attempting to access a storage device, rather a User-role account corresponds to an administrative user that can view but not change configuration settings. The internal

FabricOS root and factory accounts are disabled during TOE configuration, since they allow access to the operating system. Note that this FabricOS root account is not the same as the "Root" role.

The TOE authenticates administrative users accessing the TOE via the local console, SSH or web interface (HTTPS) in the same manner using either its own authentication mechanism or a RADIUS or LDAP Server. The TOE provides its own password authentication mechanism to authenticate administrative users. In order for an administrative user to access the TOE (i.e., to perform any functions except to see a configure login banner or to access network or SAN services), a user account including a user name and password must be created for the user, and an administrative role must be assigned. The TOE password authentication mechanism enforces password composition rules. Passwords must be between 8 and 40 characters; they can contain and must begin with an alphabetic (upper or lower case) character; they can include numeric characters and special characters such as !, @, #, $, %, ^, &, *, (, and); and they are case-sensitive. The TOE supports several password policies which apply only to accounts defined within the local user database. Among these policies is a minimum length setting that allows an administrator to configure a minimum password length (from 8 to 40 characters) that will be enforced by the TOE when passwords are changed.

In the case of RADIUS or LDAP Server authentication, the TOE passes the login credentials supplied to the RADIUS or LDAP Server for validation. If the RADIUS or LDAP Server returns a success value, the TOE matches the user name to a user name stored internally. The administrator can configure the order in which the external authentication provider and the local credentials are checked.

The TOE also supports the configuration of RSA and ECDSA certificates for users and once configured the user can login via SSH using the certificate rather than providing their password.

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

- FIA_PMG_EXT.1: The TOE supports passwords comprising upper and lower case alphabetic characters, numbers, and a set of special characters identified above. The TOE also allows administrator to defined a minimum password length between 8 and 40 characters..
- FIA_UAU.7: The TOE does not echo passwords as they are entered; rather either '*' or no characters are echoed when entering passwords.
- FIA_UAU_EXT.2: The TOE offers no TSF-mediated functions except display of a login banner and network and SAN services until the user is identified and authenticated.
- FIA_UIA_EXT.1: The TOE provides a password-based authentication mechanism, as well as public-key authentication for SSH, and also permits authentication to occur using a third-party RADIUS or LDAP Server. The order in which these authentication providers are checked is determined by an administrator.

6.5 Security management

The TOE defines the following administrative roles all of which are considered an 'authorized administrator', albeit with differing actual capabilities, for the purpose of evaluation:

- admin – can perform all administrative commands
- switchAdmin – can perform administrative commands except for those related to user management and zoning configuration commands
- operator – can perform administrative commands that do not affect security settings
- zoneAdmin – can perform administrative commands that only affect zoning configuration
- fabricAdmin – can perform administrative commands except for those related to user management

- basicSwitchAdmin – can be used to monitor system activity
- SecurityAdmin – can perform security-related configuration including user management and security policy configuration
- root – can perform all administrative commands and access the OS; this user account is disabled during TOE configuration
- factory – can perform all administrative commands

The TOE administrative interfaces consist of an Ethernet network-based interface and a serial terminal-based interface. Ethernet interfaces use a command-line interface called the "FabricOS Command Line Interface" or an HTTPS based interface known as Web Tools. The FabricOS Command Line Interface is reached using SSH or the serial interface, while Web Tools supports the use of hypertext transfer protocol over secure socket layer (HTTPS). Both network-based and terminal-based interfaces provide equivalent management functionality. The Ethernet (i.e., SSH) and serial terminal interfaces support the same command-line interface commands after a session has been established.

Once authenticated (none of these functions is available to any user before being identified an authenticated), authorized administrators have access to the following security 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 a login banner as well as network routing and SAN functions;
- Ability to configure the cryptographic functionality

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 administrators.
- FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified above.
- FMT_SMR.2: The TOE maintains administrative user roles.

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. 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 are protected using MD-5 hashing) 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 configured, 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 PRNG, 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 firmwareDownload command in order to download a new firmware 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. When a new firmware is downloaded, the new firmware always replaces the public key file on the switch with what is in the new firmware..

The TOE generates time stamps to support the auditing function.

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

- 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_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_STM.1: The TOE generates time stamps for use in audit records.
- 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 and banner that will be displayed before authentication is completed. In the case of the console and SSH, the message of the day is displayed before entering the user password and the banner is displayed afterwards. In the case of the web interface, the banner is displayed when connected a session.

The TOE can be configured by an administrator to set a session timeout value (with 0 disabling the timeout and no timeout by default). Note that there are two timeout values – one applies to the console and SSH and the other applies to the web interface. A session (local console or remote SSH or Web/HTTPS) 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 in the case of the console or SSH (web sessions change ot indicate an invalid session).

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.

6.8 Trusted path/channels

The TOE provides a trusted path for its remote administrative users accessing the TOE via the Ethernet ports provided on the TOE using either the command line interface using SSH or Advanced Web Tools using TLS/HTTPS. Note that local administrator access via the serial port is also allowed for command line access. However this access is protected by physical protection of the serial interface along with the TOE itself.

When an administrator attempts to connect to the TOE remotely, the TOE attempts to negotiate a session. If the session cannot be negotiated, the connection is dropped. When negotiating a TLS/HTTPS or SSH session, the TOE and the client application (SSH client or web browser) used by the administrator will negotiate the most secure algorithms available at both ends to protect that session. The available algorithms are identified in section 6.2 above.

Remote connections to 3rd party SYSLOG, RADIUS, and LDAP servers are supported for exporting audit records to an external audit server and for external user authentication. Communication with those external servers is 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 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 uses SSH and HTTPS to provide a trusted path for remote management interfaces to protect the communication from disclosure and modification.