Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1 Security Target

Version 0.5
January 20, 2023

Prepared for:

Brocade Communications Systems LLC (A Broadcom Limited Company)

1320 Ridder Park Dr
San Jose, CA 95131

Prepared By:

Gossamer Laboratories

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 Directors and Switches using Fabric OS v9.1.1 provided by Brocade Communication Systems LLC. The TOE is being evaluated as a network 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 parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - 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 …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1 Security Target

ST Version – Version 0.5

ST Date – January 20, 2023

1.2 TOE Reference

TOE Identification – Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1 including the following models:

- 7810
- G610
- G620
- G630
- G720
- G730
- X6-4
- X6-8
- X7-4
- X7-8

TOE Developer – Brocade Communications Systems LLC (A Broadcom Limited Company)

Evaluation Sponsor – Brocade Communications Systems LLC (A Broadcom Limited Company)

1.3 TOE Overview

The Target of Evaluation (TOE) is the Brocade Director and Switch family of products using Fabric OS v9.1.1. The TOE is a family of hardware network devices that create what is called a 'Storage Area Network' or 'SAN'. SANs provide switched connections between servers connected to the SAN and storage devices such as disk storage systems and tape libraries that are also connected to the SAN.

1.4 TOE Description

The Target of Evaluation (TOE) is the Brocade Director and Switch family of products using Fabric OS v9.1.1. The various models of the TOE differ in performance, form factor and number of ports, but all run the same Fabric OS version 9.1.1 software. The TOE is available in two form factors:

1. a rack-mount Director chassis with a variable number of replaceable modules or 'blades', and
2. a self-contained network switching appliance device

Brocade Directors and Switches are hardware appliances that create a "SAN". SANs enable connectivity between machines in the environment containing a type of network card called a Fibre Channel 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.

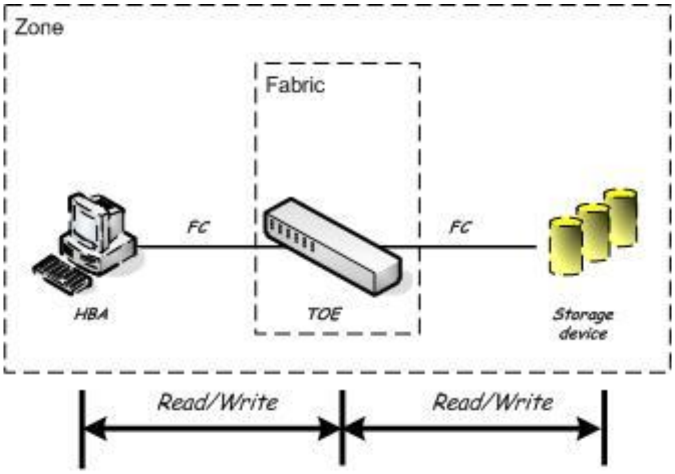

Figure 1: Host bus adapters can only access storage devices that are members of the same zone.

HBAs communicate with the TOE using FC or FC over IP (FCIP) protocols. Storage devices in turn are physically connected to the TOE using cabling connected to FC/FCIP interfaces.

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 HBAs in the environment. HBAs 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 HBA is installed in as local (i.e. directly-attached) devices.

More than one HBA 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 HBAs and storage devices.

Directors and switches both can be used by HBAs 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 command-line administrator console interfaces – Provides remote command-line administrator console interfaces called the “FabricOS Command Line Interface.”
- Serial terminal-based command-line administrator console interfaces – Provides local 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 TLS; that interface is called a REST API. 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.

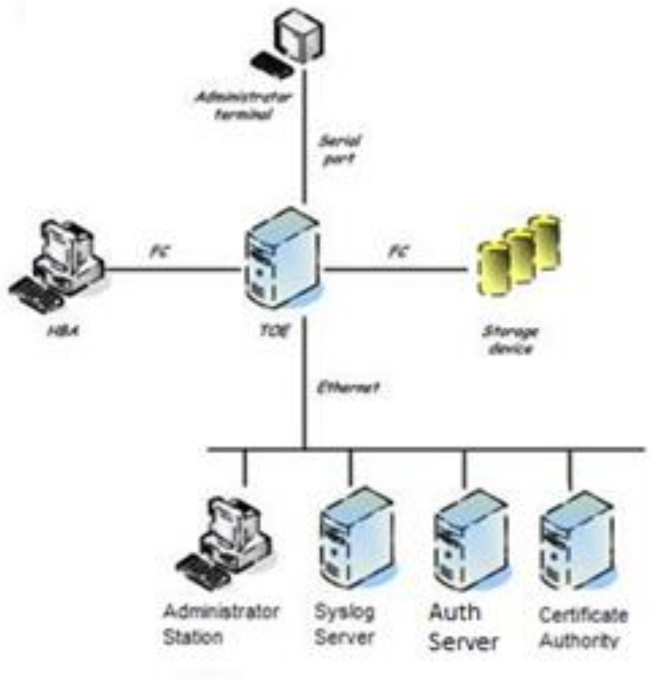

Figure 2: Administrators can access the TOE using a serial terminal or across a network. Audit records are sent to a syslog server.

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. The TOE requires administrators to login before an SSH session is established.

1.4.1.1 Physical Boundaries

The TOE consists of the following physical appliances and processors:

Hardware Model	Processor
G720	NXP Semiconductors T1042 (e5500 core)
G730	Intel(R) Atom(TM) CPU C3338R (2cores)
G610	NXP Semiconductors T1042 (e5500 core)
G620	NXP Semiconductors T1042 (e5500 core)
G630	NXP Semiconductors T1042 (e5500 core)
7810	NXP Semiconductors T1042 (e5500 core)
X6-4	NXP Semiconductors P4080 (e500mc core)
X6-8	NXP Semiconductors P4080 (e500mc core)
X7-4	NXP Semiconductors P4080 (e500mc core)
X7-8	NXP Semiconductors P4080 (e500mc core)

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

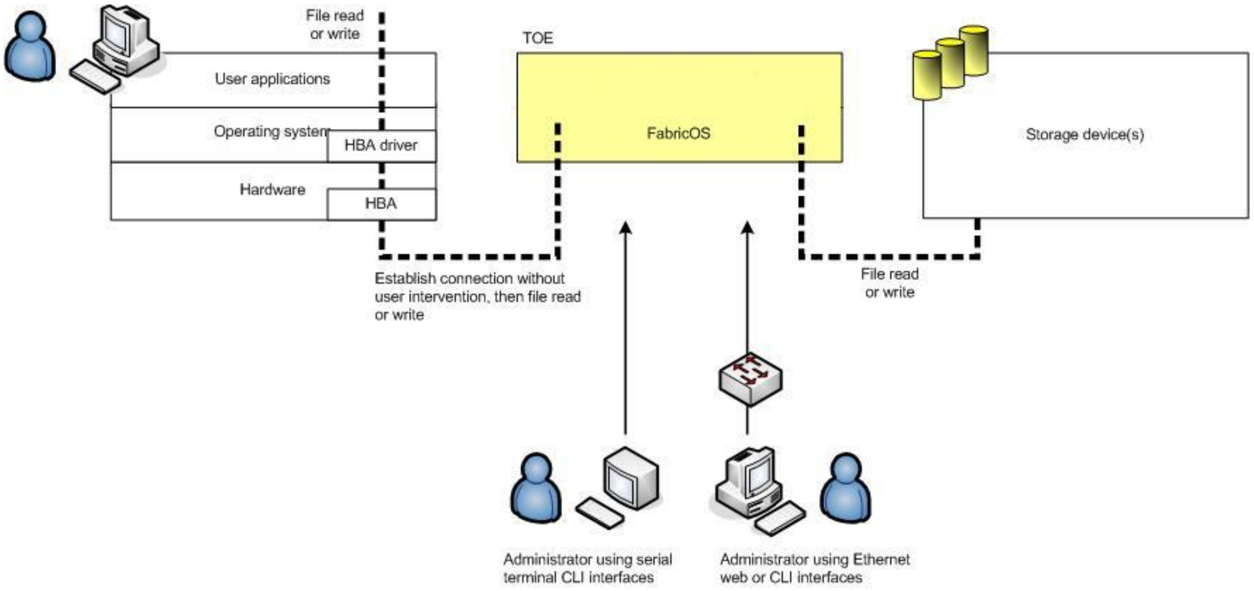

Figure 3: TOE and environment components.

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

- Host – A system in the environment that uses TOE Storage Area Network (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.
- NTP Server – Provides network time services to the TOE.
- LDAP Server – Provides authentication support for the TOE.
- 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.
- Certificate Authority (CA) – Provides digital certificates TLS-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 data encryption keys (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 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 the TOE.

- Security audit
- Cryptographic support
- 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 contents into an encapsulating syslog record.

1.4.1.2.2 Cryptographic support

The TOE contains CAVP tested 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 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 an external authentication server is called.

The TOE provides serial terminal (command line) and Ethernet network-based (command-line) management interfaces. The TOE provides administrative interfaces to set and reset administrator passwords.

1.4.1.2.4 Security Management

The TOE provides both serial terminal- and Ethernet network-based management interfaces. The TOE provides administrative interfaces to configure hard zoning, configure administrative interfaces, as well as to set and reset administrator passwords. By default, host bus adapters do not have access to storage devices.

1.4.1.2.5 Protection of the TSF

The TOE implements a number of features designed 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.

1.4.1.2.6 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.

1.4.1.2.7 Trusted path/channels

The TOE enforces a trusted path between the TOE administrators and the TOE using SSH 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. The TOE provides a TLS protected communication channel between itself and remote audit and authentication servers.

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® Fabric OS® Common Criteria User Guide, 9.1.x, 19 January 2023

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 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant
- Package Claims:
    - collaborative Protection Profile for Network Devices, Version 2.2e, 3/23/2020 (NDcPP22e)

Package	Technical Decision	Applied	Notes
CPP_ND_V2.2E	TD0670 – NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	
CPP_ND_V2.2E	TD0639 – NIT Technical Decision for Clarification for NTP MAC Keys	Yes	
CPP_ND_V2.2E	TD0638 – NIT Technical Decision for Key Pair Generation for Authentication	Yes	
CPP_ND_V2.2E	TD0636 – NIT Technical Decision for Clarification of Public Key User Authentication for SSH	No	Requirement not claimed
CPP_ND_V2.2E	TD0635 – NIT Technical Decision for TLS Server and Key Agreement Parameters	Yes	
CPP_ND_V2.2E	TD0634 – NIT Technical Decision for Clarification required for testing IPv6	Yes	
CPP_ND_V2.2E	TD0633 – NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	No	Requirement not claimed
CPP_ND_V2.2E	TD0632 – NIT Technical Decision for Consistency with Time Data for vNDs	Yes	
CPP_ND_V2.2E	TD0631 – NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	
CPP_ND_V2.2E	TD0592 – NIT Technical Decision for Local Storage of Audit Records	Yes	
CPP_ND_V2.2E	TD0591 – NIT Technical Decision for Virtual TOEs and hypervisors	Yes	
CPP_ND_V2.2E	TD0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
CPP_ND_V2.2E	TD0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
CPP_ND_V2.2E	TD0572 – NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Yes	
CPP_ND_V2.2E	TD0571 – NiT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	
CPP_ND_V2.2E	TD0570 – NiT Technical Decision for Clarification about FIA_AFL.1	Yes	

CPP_ND_V2.2E	TD0569 – NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	Yes	
CPP_ND_V2.2E	TD0564 – NiT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
CPP_ND_V2.2E	TD0563 – NiT Technical Decision for Clarification of audit date information	Yes	
CPP_ND_V2.2E	TD0556 – NIT Technical Decision for RFC 5077 question	Yes	
CPP_ND_V2.2E	TD0555 – NIT Technical Decision for RFC Reference incorrect in TLSS Test	Yes	
CPP_ND_V2.2E	TD0547 – NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
CPP_ND_V2.2E	TD0546 – NIT Technical Decision for DTLS – clarification of Application Note 63	No	Requirement not claimed
CPP_ND_V2.2E	TD0538 – NIT Technical Decision for Outdated link to allowed-with list	Yes	
CPP_ND_V2.2E	TD0537 – NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Yes	
CPP_ND_V2.2E	TD0536 – NIT Technical Decision for Update Verification Inconsistency	Yes	
CPP_ND_V2.2E	TD0528 – NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	Yes	
CPP_ND_V2.2E	TD0527 – Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	

2.1 Conformance Rationale

The ST conforms to the NDcPP22e. 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 NDcPP22e and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

In general, the NDcPP22e has defined Security Objectives appropriate for network devices and as such are applicable to the Directors and Switches TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.COMPONENTS_RUNNING (applies to distributed TOEs only)
For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.

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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

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

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.VM_CONFIGURATION (applies to vNDs only)
For vNDs, the Security Administrator ensures that the VS and VMs are configured to

- reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and
- Correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualization features such as cloning, save/restore, suspend/resume, and live migration.

If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e. The NDcPP22e defines the following extended requirements and since they are not redefined in this ST the NDcPP22e should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
- NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication - per TD0634
- NDcPP22e:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
- NDcPP22e:FIA_PMG_EXT.1: Password Management
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
- NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
- NDcPP22e:FPT_TST_EXT.1: TSF testing
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- NDcPP22e: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 NDcPP22e. The refinements and operations already performed in the NDcPP22e are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e and any residual operations have been completed herein. Of particular note, the NDcPP22e 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 NDcPP22e. The NDcPP22e should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Brocade Directors and Switches TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP22e:FAU_GEN.1: Audit Data Generation
	NDcPP22e:FAU_GEN.2: User identity association
	NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP22e:FCS_CKM.1: Cryptographic Key Generation
	NDcPP22e:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP22e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP22e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP22e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP22e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP22e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
	NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
	NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication - per TD0634
	NDcPP22e:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
FIA: Identification and authentication	NDcPP22e:FIA_AFL.1: Authentication Failure Management
	NDcPP22e:FIA_PMG_EXT.1: Password Management
	NDcPP22e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	NDcPP22e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP22e:FMT_MTD.1/CoreData: Management of TSF Data

	NDcPP22e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP22e:FMT_SMF.1: Specification of Management Functions - per TD0631
	NDcPP22e:FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
	NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
	NDcPP22e:FPT_TST_EXT.1: TSF testing
	NDcPP22e:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP22e:FTA_SSL.3: TSF-initiated Termination
	NDcPP22e:FTA_SSL.4: User-initiated Termination
	NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP22e:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel
	NDcPP22e:FTP_TRP.1/Admin: Trusted Path

Table 5-1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP22e:FAU_GEN.1)

NDcPP22e: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 comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***];

d) Specifically defined auditable events listed in Table 5-2.

Requirement	Auditable Events	Additional Content
NDcPP22e:FAU_GEN.1	None	None
NDcPP22e:FAU_GEN.2	None	None
NDcPP22e:FAU_STG_EXT.1	None	None
NDcPP22e:FCS_CKM.1	None	None
NDcPP22e:FCS_CKM.2	None	None
NDcPP22e:FCS_CKM.4	None	None
NDcPP22e:FCS_COP.1/DataEncryption	None	None
NDcPP22e:FCS_COP.1/Hash	None	None
NDcPP22e:FCS_COP.1/KeyedHash	None	None
NDcPP22e:FCS_COP.1/SigGen	None	None

NDcPP22e:FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
NDcPP22e:FCS_RBG_EXT.1	None	None
NDcPP22e:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
NDcPP22e:FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP22e:FCS_TLSC_EXT.2	None	None
NDcPP22e:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_PMG_EXT.1	None	None
NDcPP22e:FIA_UAU.7	None	None
NDcPP22e:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
NDcPP22e:FIA_X509_EXT.2	None	None
NDcPP22e:FIA_X509_EXT.3	None	None
NDcPP22e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
NDcPP22e:FMT_MTD.1/CoreData	None	None
NDcPP22e:FMT_MTD.1/CryptoKeys	None	None
NDcPP22e:FMT_SMF.1	All management activities of TSF data.	None
NDcPP22e:FMT_SMR.2	None	None
NDcPP22e:FPT_APW_EXT.1	None	None
NDcPP22e:FPT_SKP_EXT.1	None	None
NDcPP22e:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
NDcPP22e:FPT_TST_EXT.1	None	None
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None
NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	None
NDcPP22e:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The	None

	termination of a local session by the session locking mechanism.	
NDcPP22e:FTA_TAB.1	None	None
NDcPP22e: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.
NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None

Table 5-2 Auditable Events

NDcPP22e: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 cPP/ST, information specified in column three of Table 2.

5.1.1.2 User identity association (NDcPP22e:FAU_GEN.2)

NDcPP22e: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 Protected Audit Event Storage (NDcPP22e:FAU_STG_EXT.1)

NDcPP22e: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 according to FTP_ITC.1.

NDcPP22e:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition [***The TOE shall consist of a single standalone component that stores audit data locally,***]

NDcPP22e:FAU_STG_EXT.1.3

The TSF shall [***overwrite previous audit records according to the following rule: [overwrite oldest records first]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP22e:FCS_CKM.1)

NDcPP22e:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- ***RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,***
- ***ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,***
- ***FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1,***
- ***FFC Schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' and [RFC 3526]***].

5.1.2.2 Cryptographic Key Establishment (NDcPP22e:FCS_CKM.2)

NDcPP22e:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- ***RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, 'Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,***
- ***Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' (TD0581 applied),***
- ***Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography',,***
- ***FFC Schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' and [groups listed in RFC 3526] (TD0580 applied)***].

5.1.2.3 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4)

NDcPP22e:FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeroes]***];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [***logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes]***]

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP22e:FCS_COP.1/DataEncryption)

NDcPP22e:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, CTR, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772***].

5.1.2.5 Cryptographic Operation (Hash Algorithm) (NDcPP22e:FCS_COP.1/Hash)

NDcPP22e:FCS_COP.1.1/Hash

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 10118-3:2004.

5.1.2.6 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP22e:FCS_COP.1/KeyedHash)

NDcPP22e:FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and cryptographic key sizes [**equal to the input block size**] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.7 Cryptographic Operation (Signature Generation and Verification) (NDcPP22e:FCS_COP.1/SigGen)

NDcPP22e:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- ***RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits, 4096 bits],***
- ***Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256, 384, and 521 bits]***]

that meet the following: ***[***

- ***For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***
- ***For ECDSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST curves' [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4***].

5.1.2.8 NTP Protocol (NDcPP22e:FCS_NTP_EXT.1)

NDcPP22e:FCS_NTP_EXT.1.1

The TSF shall use only the following NTP version(s) [***NTP v4 (RFC 5905)***].

NDcPP22e:FCS_NTP_EXT.1.2

The TSF shall update its system time using [***Authentication using [SHA1, SHA256] as the message digest algorithm(s);***].

NDcPP22e:FCS_NTP_EXT.1.3

The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

NDcPP22e:FCS_NTP_EXT.1.4

The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.1.2.9 Random Bit Generation (NDcPP22e:FCS_RBG_EXT.1)

NDcPP22e:FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

NDcPP22e:FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[2] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.10 SSH Server Protocol - per TD0631 (NDcPP22e:FCS_SSHS_EXT.1)

NDcPP22e:FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [***4256, 4344, 5656, 6668, 8308 section 3.1, 8332***].

NDcPP22e:FCS_SSHS_EXT.1.2

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

NDcPP22e:FCS_SSHS_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [**262127**] bytes in an SSH transport connection are dropped.

NDcPP22e:FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com***].

NDcPP22e:FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [***ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp521***] as its public key algorithm(s) and rejects all other public key algorithms.

NDcPP22e:FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [***hmac-sha1, hmac-sha2-256, hmac-sha2-512***] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

NDcPP22e:FCS_SSHS_EXT.1.7

The TSF shall ensure that [***diffie-hellman-group14-sha1, ecdh-sha2-nistp256***] and [***diffie-hellman-group14-sha256, ecdh-sha2-nistp384, ecdh-sha2-nistp521***] are the only allowed key exchange methods used for the SSH protocol.

NDcPP22e:FCS_SSHS_EXT.1.8

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

5.1.2.11 TLS Client Protocol Without Mutual Authentication - per TD0634 (NDcPP22e:FCS_TLSC_EXT.1)

NDcPP22e:FCS_TLSC_EXT.1.1

The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]

and no other ciphersuites.

NDcPP22e:FCS_TLSC_EXT.1.2

The TSF shall verify that the presented identifier matches [***the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the CN or SAN]***.

NDcPP22e:FCS_TLSC_EXT.1.3

When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [***Not implement any administrator override mechanism***].

NDcPP22e:FCS_TLSC_EXT.1.4

The TSF shall [***present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1]***] in the Client Hello.

5.1.2.12 TLS Client Support for Mutual Authentication (NDcPP22e:FCS_TLSC_EXT.2)

NDcPP22e:FCS_TLSC_EXT.2.1

The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

NDcPP22e:FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [1-999] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

NDcPP22e:FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [

prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [an unlock operation] is taken by an Administrator,

prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

5.1.3.2 Password Management (NDcPP22e:FIA_PMG_EXT.1)

NDcPP22e:FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')'***];

b) Minimum password length shall be configurable to between [**8**] and [**40**] characters.

5.1.3.3 Protected Authentication Feedback (NDcPP22e:FIA_UAU.7)

NDcPP22e: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.

5.1.3.4 Password-based Authentication Mechanism (NDcPP22e:FIA_UAU_EXT.2)

NDcPP22e:FIA_UAU_EXT.2.1

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

5.1.3.5 User Identification and Authentication (NDcPP22e:FIA_UIA_EXT.1)

NDcPP22e: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]***].

NDcPP22e: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.

5.1.3.6 X.509 Certificate Validation (NDcPP22e:FIA_X509_EXT.1/Rev)

NDcPP22e:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [***the Online Certificate Status Protocol (OCSP) as specified in RFC 6960***]
- The TSF shall validate the extendedKeyUsage field according to the following rules:

o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.

o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

NDcPP22e:FIA_X509_EXT.1.2/Rev

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.1.3.7 X.509 Certificate Authentication (NDcPP22e:FIA_X509_EXT.2)

NDcPP22e:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***TLS***], and [***no additional uses***].

NDcPP22e:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***not accept the certificate***].

5.1.3.8 X.509 Certificate Requests (NDcPP22e:FIA_X509_EXT.3)

NDcPP22e:FIA_X509_EXT.3.1

The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization, Organizational Unit, Country***].

NDcPP22e:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (NDcPP22e:FMT_MOF.1/ManualUpdate)

NDcPP22e:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

5.1.4.2 Management of TSF Data (NDcPP22e:FMT_MTD.1/CoreData)

NDcPP22e:FMT_MTD.1.1/CoreData

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

5.1.4.3 Management of TSF Data (NDcPP22e:FMT_MTD.1/CryptoKeys)

NDcPP22e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.4 Specification of Management Functions - per TD0631 (NDcPP22e:FMT_SMF.1)

NDcPP22e: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 configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***Ability to manage the cryptographic keys,***
- Ability to configure the cryptographic functionality,
- Ability to configure thresholds for SSH rekeying,
- Ability to re-enable an Administrator account,
- Ability to configure NTP,
- Ability to configure the reference identifier for the peer,
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,
- Ability to import X509v3 certificates to the TOE's trust store,
- Ability to manage the trusted public keys database,
- Ability to set the time which is used for time-stamp].

5.1.4.5 Restrictions on Security Roles (NDcPP22e:FMT_SMR.2)

NDcPP22e:FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

NDcPP22e:FMT_SMR.2.2

The TSF shall be able to associate users with roles.

NDcPP22e:FMT_SMR.2.3

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

are satisfied.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Protection of Administrator Passwords (NDcPP22e:FPT_APW_EXT.1)

NDcPP22e:FPT_APW_EXT.1.1

The TSF shall store administrative passwords in non-plaintext form.

NDcPP22e:FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext administrative passwords.

5.1.5.2 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP22e:FPT_SKP_EXT.1)

NDcPP22e:FPT_SKP_EXT.1.1

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

5.1.5.3 Reliable Time Stamps - per TD0632 (NDcPP22e:FPT_STM_EXT.1)

NDcPP22e:FPT_STM_EXT.1.1

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

NDcPP22e:FPT_STM_EXT.1.2

The TSF shall [***allow the Security Administrator to set the time, synchronise time with an NTP server***].

5.1.5.4 TSF testing (NDcPP22e:FPT_TST_EXT.1)

NDcPP22e:FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [***during initial start-up (on power on), periodically during normal operation***] to demonstrate the correct operation of the TSF: [**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**].

5.1.5.5 Trusted update (NDcPP22e:FPT_TUD_EXT.1)

NDcPP22e:FPT_TUD_EXT.1.1

The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

NDcPP22e:FPT_TUD_EXT.1.2

The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

NDcPP22e:FPT_TUD_EXT.1.3

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

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (NDcPP22e:FTA_SSL.3)

NDcPP22e:FTA_SSL.3.1

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

5.1.6.2 User-initiated Termination (NDcPP22e:FTA_SSL.4)

NDcPP22e:FTA_SSL.4.1

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

5.1.6.3 TSF-initiated Session Locking (NDcPP22e:FTA_SSL_EXT.1)

NDcPP22e:FTA_SSL_EXT.1.1

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

5.1.6.4 Default TOE Access Banners (NDcPP22e:FTA_TAB.1)

NDcPP22e:FTA_TAB.1.1

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.

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Inter-TSF trusted channel (NDcPP22e:FTP_ITC.1)

NDcPP22e:FTP_ITC.1.1

The TSF shall be capable of using [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***authentication 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.

NDcPP22e:FTP_ITC.1.2

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

NDcPP22e: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**].

5.1.7.2 Trusted Path (NDcPP22e:FTP_TRP.1/Admin)

NDcPP22e:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***SSH***] to provide a communication path between itself and authorized 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 provides detection of modification of the channel data.

NDcPP22e:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP22e:FTP_TRP.1.3/Admin

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 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 5-3 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 categorization 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 fulfill 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
- 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 8191 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 those listed in Table 5-2.

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, 2022/09/28-12:28:44:094498 (GMT), [SEC-5075], INFO, SECURITY,
  admin/None/10.210.211.141/ssh/CLI,NA/sw0/FID 128, , Event: login, Status: failed, Info:
  Failed pubkey login attempt via REMOTE, IP Addr:190.2.2.2.
  ```

- 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 contents into an encapsulating syslog record, as depicted below.

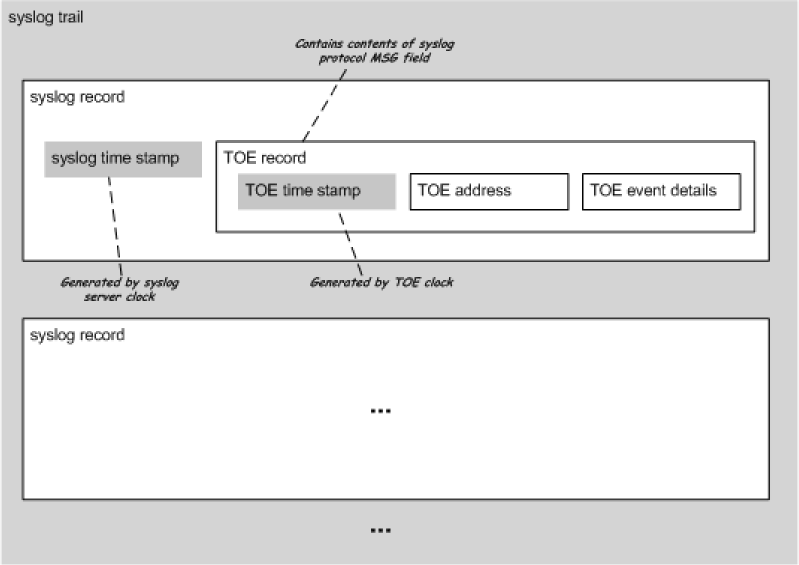

Figure 4: TOE and environment audit record components.

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.

The Security audit function satisfies the following security functional requirements:

- NDcPP22e: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. Within each audit event is date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in Table 5-2**Error! Reference source not found.**. For cryptographic keys, the act of importing, exporting or deleting a key is audited, the key is identified by name and the associated administrator account is identified.
- NDcPP22e: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.
- NDcPP22e: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 CAVP tested crypto library providing supporting cryptographic functions that runs within Fabric OS 9.1.1. The crypto library is referred to as the Brocade FOS Cryptographic library (a.k.a., Brocade Fabric OS FIPS Cryptographic Module). The evaluated configuration requires that the TOE be configured in FIPS mode to ensure CAVP tested functions are used. In FOS 9.1.1, by default, PAA is disabled in Intel Atom CPU C3338R.

Function	SFR	Standard	Certificate
Encryption/Decryption			
AES CBC/CTR/GCM (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A2604

Cryptographic hashing			
SHA-1/256/384/512 (digest sizes 160, 256, 384, and 512 bits)	FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A2604
Keyed-hash message authentication			
HMAC-SHA-1, HMAC_SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 (digest sizes 160, 256, 384 and 512 bits)	FCS_COP.1/KeyedHash	FIPS Pub 198-1	A2604
Cryptographic signature services			
RSA Digital Signature Algorithm (rDSA) (modulus 2048, 4096)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A2604
ECDSA Digital Signature Algorithm (P-256, P-384, P-521)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 14888-3	A2604
Random bit generation			
CTR_DRBG with software based noise sources	FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A2604
Key Generation			
RSA Key Generation (2048, 4096-bits)	FCS_CKM.1	FIPS Pub 186-4	A2604
ECDSA Key Generation with Curves P-256, P-384 and P-521	FCS_CKM.1	FIPS Pub 186-4	A2604
FFC Scheme DSA (2048-bit)	FCS_CKM.1	FIPS Pub 186-4	A2604
Key Establishment			
ECC Key Establishment with Curves P-256, P-384 and P-521	FCS_CKM.2	NIST SP 800-56A Rev 3	A2604
FFC Key Establishment (2048-bit)	FCS_CKM.2	NIST SP 800-56A Rev 3	A2604

Table 6-1 Cryptographic Functions

All cryptographic algorithm implementations are provided by the included Brocade FOS Cryptographic library. The TSF supports RSA key generation scheme using cryptographic key size of 2048-bit that meet the FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3; standard. The TSF also supports ECDSA (appendix B.4), FFC key generation (Appendix B.1) and FFC safe-primes key generation (RFC 3526). RSA key pairs can be generated during the creation of a Certificate Signing Request (CSR). The TOE follows NIST SP 800-56A Rev 3 ‘Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography’ key agreement scheme. The TOE acts as a recipient for RSA-based, ECC-based and FFC-safe-prime-based key establishment schemes because it is a server for the SSH management interface. It also acts as a sender for RSA-based, ECC-based, FFC-based and FFC-safe-prime-based key establishment schemes because it can be a TLS client to a syslog server and an LDAP server.

The following table outlines key establishment schemes used in the TOE:

Scheme	SFRs	Service
RSA key establishment	FCS_SSHS_EXT.1	Remote Administration
ECC key establishment	FCS_SSHS_EXT.1	Remote Administration
FFC Safe-primes key establishment	FCS_SSHS_EXT.1 (DH 14)	Remote Administration
RSA key establishment	FCS_TLSC_EXT.1	Remote Audit Server (syslog) Remote Auth Server (LDAP)
ECC key establishment	FCS_TLSC_EXT.1	Remote Audit Server (syslog) Remote Auth Server (LDAP)

FFC key establishment	FCS_TLSC_EXT.1	Remote Audit Server (syslog) Remote Auth Server (LDAP)
FFC Safe-primes key establishment	FCS_TLSC_EXT.1	Remote Audit Server (syslog) Remote Auth Server (LDAP)

Table 6-2 FOS Key Establishment Schemes

The TOE uses an SP 800-90A AES-256 CTR_DRBG. AES-256 is used in conjunction with a minimum of 256 bits of entropy accumulated from CPU jitter.

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. FLASH and RAM are accessible only through the restricted CLI command set, which can be used only after successful login to the TOE. Since this restricted CLI command set does not offer any commands to view raw FLASH or RAM, the CSP identified in Section 6.2 cannot be viewed even by administrative users.

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) (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)

The TOE is a TLS client to external audit and authentication servers when configured. The TLS client utilizes cryptographic functions to support the TLSv1.2 protocol that is compliant with RFC 5246. The TOE supports TLSv1.2 with client (mutual) authentication and is capable of providing a certificate in the TLS negotiation when the TLS server requests a certificate.

Certificates presented to the TLS server must match the reference identifier for the corresponding service. These reference identifiers must match the common name (or SAN values if present) and need to be a DNS value, an IPv4 address, or an IPv6 address. If a reference identifier is an IP address, the TOE reads the CN IP address in text format and gets peer host address from the TLS socket. The TLS socket returns a binary value in network byte order. The TOE converts this binary value to a canonical text format via INET system calls and compares the converted value to the text format of IP address obtained from CN. The TOE does support wildcards in certificates, and does not support certificate pinning.

The TOE rejects older versions of TLS and SSL. TLS v1.2 is supported with AES (CBC) 128 or 256 bit ciphers, in conjunction with SHA-1 and SHA-256 and RSA. Once configured per guidance, the TOE also presents the secp256r1, secp384r1 and secp521r1 curves in the Supported Elliptic Curves/Supported Groups Extension of a TLS Client Hello message.

The following cipher suites are implemented by the TOE:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

The TOE acts as an SSH server, using cryptographic functions to support the SSHv2 protocol which is compliant with RFCs 4251, 4252, 4253, 4254, 4256, 4344, 5656, 6668, 8308 section 3.1 and 8332.

No options included in the RFCs have been implemented. The TOE supports the encryption algorithms aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, and aes256-gcm@openssh.com to ensure confidentiality of an SSH session. The TOE supports password-based and public key based user authentication.

The TOE supports SSHv2 with AES (CBC/CTR/GCM modes) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1, HMAC-SHA2-256, and HMAC-SHA2-512 integrity algorithms as well as RSA and ECDH using the following key exchange methods:

- diffie-hellman-group14-sha1,
- diffie-hellman-group14-sha256
- ecdh-sha2-nistp256,
- ecdh-sha2-nistp384,
- ecdh-sha2-nistp512

While other ciphers and hashes are implemented in the product, they are disabled while the TOE is operating in FIPS mode. The TOE supports user and host public key authentication as follows:

- User public key authentication can be performed using ssh_rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 or ecdsa-sha2-nistp521 algorithms. Administrators must associate a public key with each user account that is authenticated with public-keys.
- TOE host public key authentication can be performed using ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp521 algorithms.

The TOE's SSHv2 supports both public-key and password based authentication. Either authentication approach can be configured. The maximum packet size accepted by the TOE SSH Server is limited to 262127 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 (262127 bytes) the packet will be dropped. The TOE initiates a session rekey after the configured rekey limit is reached. This limit is based on time and data, with a rekey triggered whenever either limit is reached. The time-based rekey can be configured by and administrator to values between 15 and 60 minutes. The data-based limit is not configurable and occurs before 1 gigabyte of traffic.

The Cryptographic support function satisfies the following security functional requirements:

- NDcPP22e:FCS_CKM.1: The TOE supports asymmetric key generation using RSA, ECC and FFC key establishment as part of TLS and SSH as described in the section above. The TOE acts as a client for TLS

(RSA, ECC, FFC and FFC Safe-prime) and a server for SSH (RSA, ECC and FFC Safe-prime). The TOE supports DH group 14 key establishment scheme that meets standard RFC 3526, section 3 for interoperability. RSA key pairs can be generated during the creation of a Certificate Signing Request (CSR). While the TOE can accept ECDSA certificates to authenticate its TLS peer, it does not generate ECC key pairs for a CSR.

- NDcPP22e:FCS_CKM.2: See Table 6-2 and NDcPP22e:FCS_CKM.1
- NDcPP22e:FCS_CKM.4: All memory is cleared by overwriting it with zeroes.
- NDcPP22e:FCS_COP.1/DataEncryption: The TOE provides symmetric encryption and decryption capabilities using AES in CBC, CTR and GCM mode (with 128 and 256 bit keysize) as described AES as specified in ISO 18033-3. AES is implemented in support of the following protocols: TLS, and SSH.
- NDcPP22e:FCS_COP.1/Hash: The TOE supports hashing using SHA-1, SHA-256, SHA-384 and SHA-512 validated conforming to FIPS 180-4, Secure Hash Standard (SHS). SHS hashing is used within several services including, NTP hashing, TLS, and SSH. SHA-256 is used in conjunction with RSA signatures for verification of software image integrity.
- NDcPP22e:FCS_COP.1/KeyedHash: The TOE supports keyed hash HMAC-SHA1, HMAC-SHA256, and HMAC-SHA384, HMAC-SHA512 conforming to ISO/IEC 9797-2:2011. Supported cryptographic key sizes: 160, 256, 384, 512 bits and message digest sizes: 160, 256, 384, 512 bits. Keyed hash use matches validated hash algorithms implemented by the module.
- NDcPP22e:FCS_COP.1/SigGen: The TOE supports RSA signature generation and verification according to RSASSA-PKCS1v1_5 with 2048-bit, and ECDSA signature generation and verification according to FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D with curves P-256/384/521.
- NDcPP22e:FCS_NTP_EXT.1: The TOE implements the NTPv4 protocol to synchronize with up to 8 external NTP time servers. The TOE authenticates time updates using an administrator-configured SHA1 or SHA256 message authentication. The TOE does not synchronize based on broadcast and multicast time updates. The TOE supports configuration of multiple simultaneous time servers and follows RFC 5905 algorithm to prioritize them
- NDcPP22e:FCS_RBG_EXT.1: The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90B.
- NDcPP22e:FCS_SSHS_EXT.1: The TOE supports SSHv2 as described above.
- NDcPP22e:FCS_TLSC_EXT.1/2: The TOE supports TLS v1.2 with the ciphersuites listed above for its syslog and LDAP connections.

6.3 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. Ten roles, each with a fixed set of permissions, are supported: Root, Factory, Admin, FabricAdmin, SecurityAdmin, SwitchAdmin, BasicSwitchAdmin, ZoneAdmin, Operator and User. There are three pre-defined administrator accounts called “maintenance”, “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 HBA 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 maintenance account is disabled during TOE configuration, since they allow access to the operating system.

TOE uses SSH to provide remote management Command Line Interface (CLI). The TOE authenticates administrative users accessing the TOE via this SSH interface as well as via the local console. The TOE authenticates administrative users with its own local authentication mechanism. This provides a password authentication mechanism that authenticates administrative users. In order for an administrative user to access the TOE (i.e., to perform any functions except to see a configured 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 to that account. The TOE password authentication mechanism enforces password composition rules. Passwords must be between 8 and 40 characters; they can contain 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. Additionally, the SSH interface supports public key authentication of administrative users. Administrative users are associated with a public key that must be verified during the authentication process. The TOE can also communicate with an LDAP server for authentication service.

A successful logon occurs when the user presents to the TOE a valid administrative user name along with either the correct password or verification of a public-key. 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.

Root certificates are loaded into the TOE during its initial configuration and the TOE uses the Root CA when verifying a certificate trust chain during TLS negotiations. Client identity certificates are loaded during TOE initial configuration and the TOE presents its identity certificate to the network peer during TLS negotiations protecting SYSLOG and LDAP connections. Certificates from the TLS peer are validated as part of the TLS authentication process for a network peer (i.e., syslog or LDAP). A certificate's trust chain is verified when it is first imported into the TOE. Certificates from peers are verified and if found not valid the associated TLS negotiation is rejected.

Additionally, the revocation status of a certificate is checked using OCSP. If the OCSP responder identified for a certificate cannot be reached to determine the revocation status of the certificate or the OCSP response is rejected as invalid, then the certificate is considered not valid and thus is not accepted. See below for additional checks performed as part of certificate validation.

The Identification and authentication function satisfies the following security functional requirements:

- NDcPP22e:FIA_AFL.1: A user in the Admin role can set a lockout failure count for remote login attempts. If the count is exceeded, the targeted account is locked. The TOE supports unlocking an account based on either a configured lockout duration or by explicit admin action. Remote login attempts using SSH are blocked entirely for an account when that account is locked. The admin’s valid password will allow[1] a successful login from the local console, even when the account is locked and admin lockout console access is enabled. This ensures that access to the TOE CLI is available at the local console despite the potential locking of all administrator accounts by a malicious remote attacker.

- NDcPP22e: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 define a minimum password length between 8 and 40 characters.

- NDcPP22e:FIA_UAU.7: The TOE does not echo passwords as they are entered; rather either ‘*’ or no characters are echoed when entering passwords.

- NDcPP22e: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.

- NDcPP22e:FIA_UIA_EXT.1: The TOE provides a password-based authentication mechanism, as well as public-key authentication for SSH.

- NDcPP22e:FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate validation. Certificates are validated as part of the authentication process for a network peer providing audit server functionality and

[1] The *adminlockout* console access feature must be enabled for this behavior.

authentication services. A certificate's trust chain is also validated when it is first imported into the TOE. In addition to a revocation check using OCSP, the following fields are verified as appropriate:

- Expiration – Current time must be within validity period of the certificate.
- Common Name - Needs to be FQDN device name or IP address. Wildcards are allowed only for 1 level of sub-domain and not allowed for the main domain.
- CA Field – Must be true if it is the certificate for a Certificate Authority (CA).
- Key Usage - CA Certificates must have "Certificate Sign", while identity certificates must have "Digital Signature" key usage.
- X509v3 Extended Key Usage - Must rightly indicate whether Certificate is for use as a "server" certificate or a "client" certificate. If incorrect, connection is not allowed.
- Authority Information Access - Must have valid OCSP server respond affirmatively. If this field is not present, an OCSP check is not performed.
- Subject Alternative Name - Not a mandatory attribute. If present, the values stored in this extension takes priority over the value within the CN field of the Subject attribute.
- Basics Constraints - Attribute must be present and must have CA flag set to TRUE in all CA certificates.

- NDcPP22e:FIA_X509_EXT.2: Administrators must install a trusted root CA certificate for a syslog peer and for an LDAP peer (both services must have a root CA defined, even if they are the same certificate). The TOE also must also have its own certificate installed for each of these services. Once defined these certificates are used to authenticate the corresponding peer. As described above, if the OCSP responder identified for a certificate cannot be reached to determine the revocation status of the certificate or the OCSP response is rejected as invalid, then the certificate is considered not valid.
- NDcPP22e:FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates.

6.4 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
- maintenance – can perform all administrative commands and access the OS; this user account is disabled during TOE configuration

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”. The FabricOS Command Line Interface is reached using SSH or the serial interface. 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 and authenticated), authorized administrators have access to the following security functions:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to manage the cryptographic keys,
- Ability to configure the cryptographic functionality,
- Ability to configure thresholds for SSH rekeying,
- Ability to re-enable an Administrator account,
- Ability to configure NTP,
- Ability to configure the reference identifier for the peer;,
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,
- Ability to import X509v3 certificates to the TOE's trust store,
- Ability to manage the trusted public keys database,
- Ability to set the time which is used for time-stamp.

The Security management function satisfies the following security functional requirements:

- NDcPP22e:FMT_MOF.1/ManualUpdate: Only the authorized administrator can update the TOE.
- NDcPP22e:FMT_MTD.1/CoreData: Only the authorized administrator can configure TSF-related functions.
- NDcPP22e:FMT_MTD.1/CryptoKeys: Cryptographic key related management is restricted to the authorized administrator. An administrator may generate and delete SSH host keys as well as keys associated with a CSR. The administrator may also import keys associated with CA certificates, as well as identity certificates that are used by the TOE.
- NDcPP22e:FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified above.
- NDcPP22e:FMT_SMR.2: The TOE maintains administrative user roles.

6.5 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 is 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 SHA-512 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 support 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 140-3 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 the 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 signature using the public key in 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 Protection of the TSF function satisfies the following security functional requirements:

- NDcPP22e: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.
- NDcPP22e:FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- NDcPP22e:FPT_STM_EXT.1: The TOE generates time stamps for use in audit records. The TOE can get time from an NTP server or can allow an administrator to set time manually. When time is manually configured, the TOE imposes restrictions upon the frequency and size of each change.
- NDcPP22e: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 ensure the TOE is functioning as expected.
- NDcPP22e: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, 4096-bit RSA key with SHA-256 digital signatures are used to authenticate the update to ensure it is the update intended and originated by Brocade.

6.6 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.

The TOE can be configured by an administrator to set a session timeout value (with 0 disabling the timeout and no timeout by default). A session (local console or remote SSH) 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.

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 satisfies the following security functional requirements:

- NDcPP22e:FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- NDcPP22e:FTA_SSL.4: The TOE provides the function to logout (or terminate) from the both local and remote user sessions as directed by the user.
- NDcPP22e:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.

- NDcPP22e:FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE.

6.7 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. 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 SSH session, the TOE and the client application (SSH client) 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 third-party SYSLOG 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 satisfies the following security functional requirements:

- NDcPP22e:FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that any LDAP authentication operations and exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification.
- NDcPP22e:FTP_TRP.1/Admin: The TOE uses SSH to provide a trusted path for remote management interfaces to protect the communication from disclosure and modification.