Brocade Communications Systems LLC FabricOS Version 8.2.0a2 Running on Brocade Directors and Switches Security Target

Version 1.02
Date: September 24, 2019

Prepared for:

BROCADE
A BROADCOM INC. COMPANY

Brocade Communications Systems LLC

1320 Ridder Park Drive,
San Jose, CA 95131

Prepared By:

Gossamer Laboratories

www.gossamersec.com

LIST OF TABLES

LIST OF FIGURES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST acronyms and terminology, and the ST organization.

The TOE is the Brocade FabricOS Version 8.2.0a2 provided by Brocade Communications Systems LLC. The FabricOS software runs on the Brocade Directors and Switches hardware appliances. These Brocade appliances implement what is called a "Storage Area Network" or "SAN". SANs provide physical connections between servers that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- Extended Components Definition (Section 5)
- Security Requirements (Section 6)
- TOE Summary Specification (Section 7)

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 number enclosed in parenthesis 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, (1) and (2).
  - 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.

Acronyms and Terminology

This following acronyms and terms are used throughout this document.

FC	Fibre Channel
FCIP	Fibre Channel over IP
HBA	Host Bus Adapter
JBOD	Stands for "Just a Bunch of Disks", and it a way of connecting together a series of hard drives, combining multiple drives and capacities, into one drive

LUN	Logical Unit Number, used to refer to a logical device within a chain.
SAN	Storage Area Network
SSH	Secure Shell protocol
SSL	Secure Session Layer protocol
TLS	Transport Layer Security protocol

1.1 Security Target Reference

ST Title – Brocade Communications Systems LLC FabricOS Version 8.2.0a2 Running on Brocade Directors and Switches Security Target

ST Version – Version 1.02

ST Date – September 24, 2019

1.2 TOE Reference

TOE Identification – Brocade Communications Systems LLC, FabricOS Version 8.2.0a2 software running on Brocade Directors and Switches, including the following series and models:

- Gen 5 hardware (Gen5HW)
  - Director Blade[1] Models: FC16-32, FC16-48, FC16-64, CP8, CR16-4, CR16-8, FX8-24
  - Director Models: DCX 8510-4, DCX 8510-8
  - Switch Appliance Models: 6510, 6520 and 7840
- Gen 6 hardware (Gen6HW)
  - Director Blade Models: FC32-48, CPX6, CR32-4, CR32-8 and SX6
  - Director Models: X6-4, X6-8
  - Switch Appliance Models: G620 and G630

The TOE is the FabricOS software that is pre-installed on these hardware platforms.

TOE Guidance – Refer to section 1.4.2, “TOE Documentation” for applicable guidance documentation that are relevant to the evaluated configuration and use of the TOE. The evaluated versions of these documents are available at the TOE developer website (https://www.brocade.com).

TOE Developer – Brocade Communications Systems LLC

1.3 TOE Overview

The Target of Evaluation (TOE) is the Brocade FabricOS Version 8.2.0a2 running on Brocade Directors and Switches family of products configured as instructed by the preparatory documentation described in section 1.4.2 and provided by Brocade Communications Systems LLC Brocade FabricOS Version 8.2.0a2 running on Brocade Directors and Switches is a software solution utilizing hardware appliances that implement what is called a 'Storage Area Network' or 'SAN'. SANs provide physical connections between servers that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment. The TOE provides the following major security features:

- auditing of user activity,

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

- identification and authentication of users,
- management based upon user roles,
- a SAN access policy,
- restrictions upon TOE access,
- encryption supporting communication with network peers, and
- encryption supporting administrative trusted path.

1.3.1 Excluded Features

In order to facilitate evaluation some features of the Brocade FabricOS Version 8.2.0a2 software are not included in the scope of the TOE evaluation.

The following is a list of product features that are excluded from the evaluation and must be disabled[2] or not configured for use in the TOE configuration:

- Redundancy or encryption provided by processing of user data by ASICs is not evaluated.
- Fibre Channel over Ethernet (FCOE) cannot be configured to create SAN Ethernet Ports.
- Fibre Channel over IP (FCIP) cannot be configured for use over SAN Ethernet Ports.
- The TOE is configured to exclude the use of Elliptic-Curve Cryptographic algorithms for use with SSH by the use of certificates and keys defined using Elliptic-Curve Cryptographic algorithms.
- Web-based administrator console interfaces called the “Brocade Advanced Web Tools” cannot be used for administration of the TOE.
- The SNMP administrative interface cannot be used and must be disabled.
- Optional modem hardware for simulating a serial administration interface is not installed.
- The TOE cannot be operated in Access Gateway mode.
- Dynamic RBAC is not configured for use by administrators.
- Insecure protocols such as FTP and Telnet must not be used (or must be disabled) per instructions in guidance.
- IPsec features have not been evaluated and must be disabled per guidance instructions.
- Inflight encryption must be disabled.
- Only PEAP-MSCHAPv2 extension authentication protocols needs to be configured for RADIUS authentication.
- The REST API interface must not be used to access the TOE. REST interface must be disabled.

Additionally, the TOE cannot be configured to prevent the use of Elliptic-Curve Cryptographic algorithms supporting TLS other than by not creating (or deleting any existing) certificates and keys based on Elliptic-Curve Cryptographic algorithms. The Elliptic-Curve Cryptographic algorithms have not been evaluated.

Note that the Brocade Network Advisor is a management tool which utilizes the SNMP and web interfaces to communicate with the TOE. However, because both of those interfaces are excluded, then the Brocade Network Advisor is also excluded.

[2] Some features are disabled by virtue of not being configured for use by TOE administrators.

1.4 TOE Description

The Target of Evaluation (TOE) is the Brocade FabricOS Version 8.2.0a2 software configured as instructed by the preparatory documentation described in section 1.4.2. The TOE runs on Brocade Directors and Switches hardware appliances. The various models of the hardware supporting the TOE are mentioned in Section 1.2. These models differ in performance, form factor and number of ports. However, all models run the same Fabric OS Version 8.2.0a2 software. The Brocade Directors and Switches hardware appliances are available in two form factors:

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

Gen 5 Director models are composed of blades of several types. A 'director blade model' is either a control blade (CP8), a core switch blade (CR16-4, CR16-8), a port blade (FC16-32, FC16-48, FC16-64) or an extension blade (FX8-24). A core switch blade contains the ASICs for switching between port blades. Both port blades and an extension blades support various numbers of ports and speeds. The DCX 8510-4 and DCX 8510-8 require at least one control blade and one core blade to make the director operational.

Gen 6 Director models are composed of blades of several types. A 'director blade model' is a control blade (CPX6), a core switch blade (CR32-4 or CR32-8), and port blades (FC32-48) or application blades (SX6 FC-IP). Control blades contain the control plane for the chassis. A core switch blade contains the ASICs for switching between port blades. A port blade supports various numbers of ports and speeds. Application blades provide additional capabilities such as Fibre Channel (FC) over Ethernet. The X64 and X68 require at least one control blade and one core blade to make the director operational.

Director Model	Blades
DCX 8510-4	CP8, CR16-4, FC16-32, FC16-48, FC16-64, FX8-24
DCX 8510-8	CP8, CR16-8, FC16-32, FC16-48, FC16-64, FX8-24
X6-4	CPX6, CR32-4, FC32-48, SX6
X6-8	CPX6, CR32-8, FC32-48, SX6

The TOE running on the Brocade Directors and Switches implement what is called a "Storage Area Network" or "SAN". SANs provide physical connections between machines in the environment containing a type of network card called a Host Bus Adapter (HBA) that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment. The network connection between the storage devices in the environment, the hardware on which the TOE is running and the HBAs in the environment makes use of 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 for FabricOS user data activity from a user's perspective is depicted in Figure 1-1. Actual implementation may interconnect multiple instances of Brocade Directors and Switches running FabricOS. Refer to Figure 1-2 for a depiction of the typical Fibre Channel (FC) and internet protocol (IP) network connections.

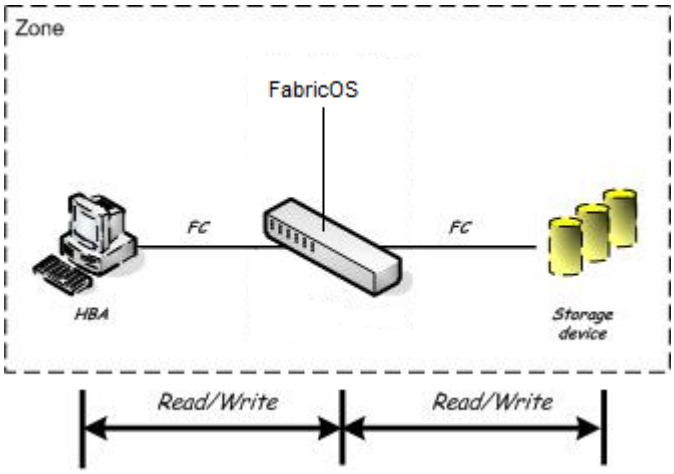

Figure 1-1: Host bus adapters can only access storage devices that are members of the same zone

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

The following section summarizes the TOE place in a SAN architecture.

1.4.1 TOE Architecture

A SAN 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 hardware running the TOE. These Brocade Directors and Switches can then be physically attached to host bus adapters in the environment. Host bus adapters that are connected to the hardware running the TOE can then read from and write to storage devices that are attached to the hardware running the TOE according to TOE configuration. Storage devices in the environment appear to the operating system running on the machine that the host bus adapter is installed in as local (i.e. directly-attached) devices.

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

Host bus adapters can access storage devices by communicating with the TOE. Switch appliances provide a fixed number of physical interfaces to other 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. The same TOE (FabricOS) runs on Brocade Switches and on Brocade Directors.

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 command-line administrator console interfaces called the "FabricOS Command Line Interface."
- Serial terminal-based command-line administrator console interfaces – Provides command-line administrator console interfaces called the "FabricOS Command Line Interface."

There 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.

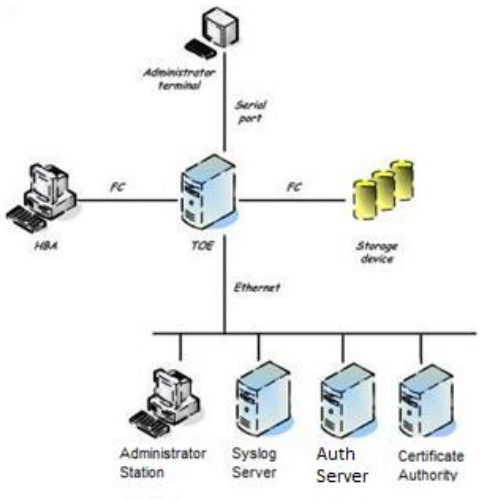

Figure 1-2: The TOE Network IT environment

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 a switch appliance 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 hardware running the TOE, each device running the TOE (i.e., instance of the TOE) is administered individually.

- 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 the TOE cannot be bypassed. The TOE encrypts commands sent from terminal applications by administrators using SSHv2 for the command line interface. The TOE requires administrators to login after an SSHv2 connection has been established.

Administration of the TOE occurs only on IP based networks or via the serial port. The exchange of user data between HBA, TOE and storage devices occurs only on Fibre Channel networks.

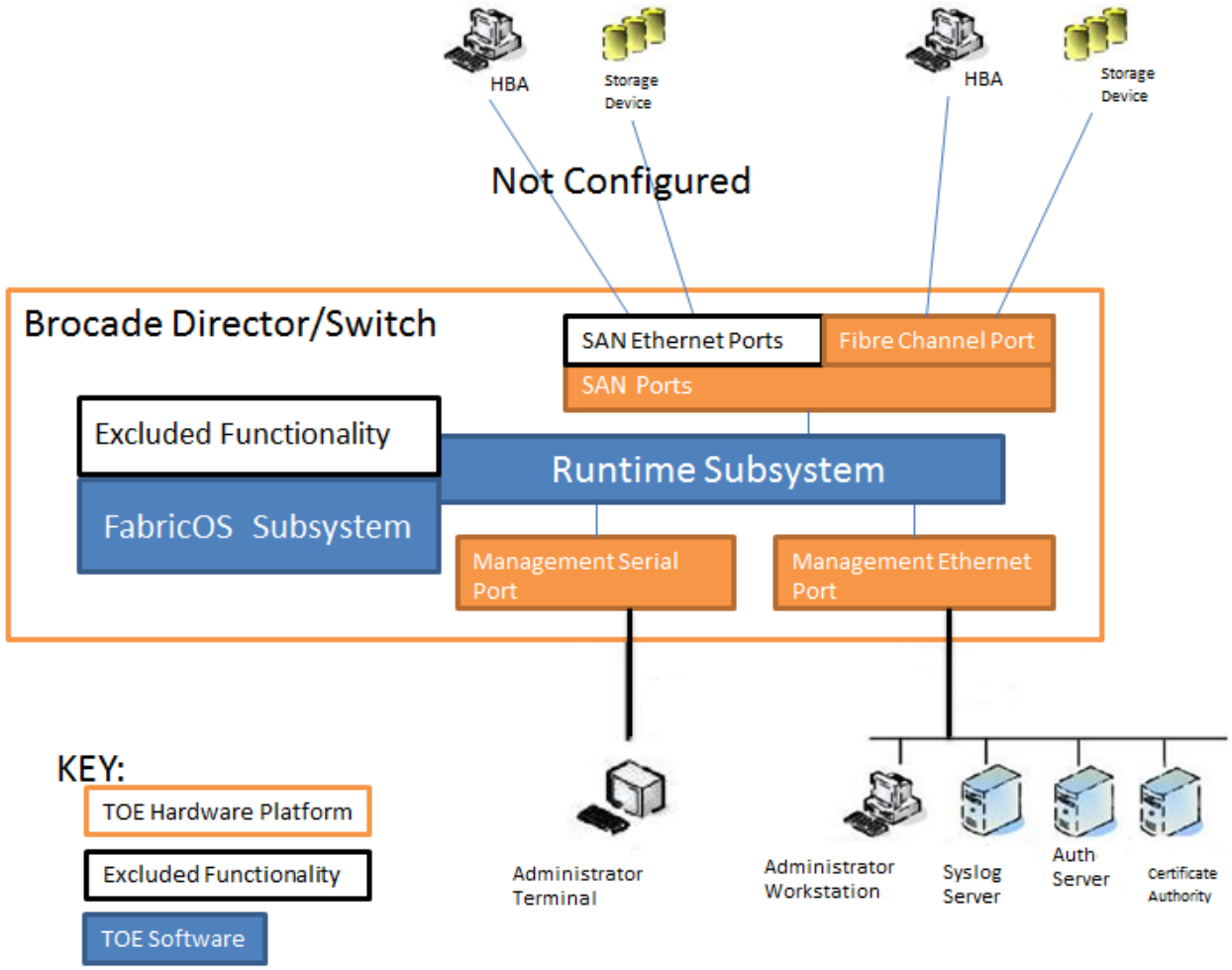

Figure 1-3: TOE Structure

Regarding the TOE internal architecture, the TOE is composed of two subsystems: FabricOS Subsystem and Runtime Subsystem. The Runtime Subsystem provides an execution environment for the FabricOS subsystem, logical representations of physical devices, and directly interacts with the physical hardware on which the TOE executes. Thus, the Runtime subsystem interacts with the physical devices (i.e., serial ports, Ethernet ports, and Fibre Channel ports) to facilitate use of those devices by the FabricOS Subsystem. As an example, the FabricOS subsystem defines and controls the network protocols used to communicate with administrator stations, and other management servers, while the Runtime subsystem provides the services that support the use of the physical connections on the Brocade Directors and Switches.

Figure 1-3 is a logical representation of the TOE software and its interaction with its own hardware platform and network IT environment. Excluded Functionality represented in this diagram are identified in section 1.3.1.

1.4.1.1 Physical Boundaries

The TOE is the Brocade FabricOS operating system configured as instructed by the preparatory documentation described in section 1.4.2 and running on Brocade Switch and Director Appliances. These components are further described as follows.

Brocade FabricOS operating system

The FabricOS is an operating system that runs on Brocade switches and directors with origins from Linux. FabricOS is comprised of user-space programs, kernel daemons and kernel modules loaded as proprietary components. Some base features of Linux were duplicated in FabricOS when FabricOS was created. These base features of FabricOS

include the file system, memory management, processor and I/O support infrastructure for FabricOS user-space programs, daemons, and kernel modules. Inter-process communication is handled through commonly mapped memory or shared PCI memory and semaphores as well as IOCTL parameter passing. FabricOS provides access to memory or to make a standard IOCTL call, and all the contents of the buffers and IOCTL message blocks or other message blocks are proprietary to the FabricOS user-space programs, kernel modules and daemons in the same manner as Linux. The FabricOS operating system includes the OpenSSL[3] crypto engine as internal functionality supporting TOE operation. All parts of FabricOS are considered TOE except that software directly supporting excluded functionality identified in section 1.3.1.

Brocade Switch and Director Appliances

One or more of each type of hardware appliance are supported in the evaluated configuration. The evaluated configuration also supports one or more blades per director, depending on the number supported by a given director model. These appliances are not the TOE, but rather are part of the TOE environment. They provide physical connections to a SAN which the TOE utilizes.

In its most basic form, the TOE in its intended environment is depicted in the Figure 1-2.

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

- Host – A system in the environment that uses TOE SAN services.
- Host Bus Adapters (HBAs) – Provides physical network interfaces from host machines in the environment to the TOE. HBA drivers provide operating system interfaces on host machines in the environment to storage devices in the environment. Storage devices in the environment appear to the host operating system as local (i.e. directly-attached) devices.
- Storage device – A device used to store data (e.g. a disk or tape) that is connected to the TOE using a FC connection and is accessed by a host using the TOE.
- Terminal application – Provides a runtime environment for console-based (e.g., SSHv2) client administrator console interfaces.
- Syslog server – Provides logging to record auditable event information generated by the TOE. The syslog server is expected to store audit information sent to it by the TOE and make that data available to administrators of the TOE.
- RADIUS/LDAP Server – An optional component that can perform authentication based on user credentials passed to it by the TOE. The TOE then enforces the authentication result returned by the RADIUS or LDAP Server.
- Certificate Authority (CA) – Provides digital certificates for TLS-based interfaces that are installed during initial TOE configuration. After installation, the CA no longer needs to be on the network for operation.

The TOE relies on a syslog server in the environment to store and protect audit records that are generated by the TOE. The TOE can be configured to use a RADIUS or LDAP Server for authentication. The TOE relies upon a certificate authority to generate certificates that are used by the TOE for host authentication. The TOE does not rely on any other components in the environment to provide security-related services. The TOE is interoperable with any adapter or device that is interoperable with one or more of the following standards:

- FC-AL-2 INCITS 332: 1999
- FC-GS-5 ANSI INCITS 427:2006 (includes the following.)
    - FC-GS-4 ANSI INCITS 387: 2004
- FC-IFR revision 1
- FC-SW-4 INCITS 418:2006 (includes the following)

[3] The TOE uses OpenSSL version 1.0.2h and the Known Answer Test code from OpenSSL version 1.0.2h. The TOE also includes a patch that prevents exploitation of the heartbleed bug.

  - FC-SW-3 INCITS 384: 2004
- FC-VI INCITS 357: 2002
- FC-TAPE INCITS TR-24: 1999
- FC-DA INCITS TR-36: 2004 (includes the following)
  - FC-FLA INCITS TR-20: 1998
  - FC-PLDA INCIT S TR-19: 1998
- FC-MI-2 ANSI/INCITS TR-39-2005
- FC-PI INCITS 352: 2002
- FC-PI-2 INCITS 404: 2005
- FC-FS-2 ANSI/INCITS 424:2006 (includes the following)
  - FC-FS INCITS 373: 2003
- FC-LS revision 1.51 (under development)
- FC-BB-3 INCITS 414: 2006 (includes the following)
  - FC-BB-2 INCITS 372: 2003
- FC-SB-3 INCITS 374: 2003 (replaces FC-SB ANSI X3.271: 1996; FC-SB-2 INCITS 374: 2001)
- FCP-2 INCITS 350: 2003 (replaces FCP ANSI X3.269: 1996)
- SNIA Storage Management Initiative Specification (SMI-S) Version 1.2 (includes the following)
  - SNIA Storage Management Initiative Specification (SMI-S) Version 1.02 (ANSI INCITS 388: 2004)
  - SNIA Storage Management Initiative Specification (SMI-S) Version 1.1.0

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- User data protection
- Identification and authentication
- Security management
- TOE Access
- Trusted path

This chapter also covers the topic of TSF protection.

There is no distinction between the product and the TOE.

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. TOE generated audit includes a message and timestamp. This is then sent to an external syslog server in the environment using the 'syslog protocol'.

1.4.1.2.2 User data protection

Host bus adapters can only access storage devices that are members of the same zone. The TOE enforces an access control policy called the SAN Fabric SFP to accomplish this. The SAN Fabric SFP is implemented using hardware-enforced zoning (also called "hard zoning" or simply "zoning") that prevents a host bus adapter from accessing a device the host bus adapter is not authorized to access. A zone is a region within the fabric where a specified group of fabric-connected devices (called zone members) have access to one another. Zone members do not have access to any devices outside the zone and devices outside the zone do not have access to devices inside the zone.

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 the information is passed to a RADIUS or LDAP Server to perform the validation and the TOE enforces the decision. The administrator can configure the order in which the external authentication provider and the local credentials are checked.

The TOE also can authenticate hosts acting as network peers that provide syslog, RADIUS or LDAP services. This authentication occurs using digital signature verifications based up certificates stored within the TOE and used during TLS session establishment.

1.4.1.2.4 Security management

The TOE provides both serial terminal- and Ethernet network-based management interfaces. Each of these types of interfaces provides equivalent management functionality. 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 TOE access

The TOE provides an IP Filter policy that is a set of rules applied to the IP management interfaces. These rules provide the ability to control how and to whom the TOE exposes the management services hosted on a switch. They cannot affect the management traffic that is initiated from a switch.

The TOE limits the number of concurrent login sessions for users, such that the number of simultaneous login sessions for each role is limited.

1.4.1.2.6 Trusted path

The TOE enforces a trusted path between the TOE administrators and the TOE using SSHv2 connections for Ethernet connections from the Administrator terminal to the TOE. The TOE encrypts commands sent from terminal applications by administrators using SSHv2 for the command line interface.

The TOE also enforces a trusted channel between the TOE and configured network peers that are providing syslog, RADIUS or LDAP services. This trusted channel utilizes TLSv1.2 to protect syslog and LDAP communications. The communication between the TOE and a RADIUS server utilizes TLS within the context of the RADIUS protocol.

FabricOS supports a REST interface. REST interface is disabled in the evaluation.

The TOE contains FIPS-certified cryptographic implementations that provide random bit generation, encryption/decryption, digital signature, secure hashing and key-hashing features in support of higher level cryptographic protocols including SSHv2 and TLSv1.2[4]. FabricOS also includes Elliptic-Curve cryptographic

[4] The FabricOS 8.2.0a2 BSI Configuration Guide describes the configuration and features that are included and available for use in a Common Criteria evaluated configuration of the TOE. This ST focuses on those features that are included for use in an evaluated configuration.

algorithms supporting TLSv1.2 which cannot be disabled, but which are not evaluated. Administrators are advised not to establish TLSv1.2 sessions to remote servers that require the use of Elliptic-Curve cryptographic algorithms.[5]

1.4.1.2.7 Protection of the TSF

Protection of the TSF is provided primarily by virtue of the fact that the TOE is running within a hardware appliance that is physically protected in the environment. The TOE does not encrypt data written to or read from storage devices by host bus adapters. The TOE relies instead on the environment to physically protect the network between the HBA and the TOE, and between the TOE and the storage device. 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 SSHv2. Further, TOE requires administrators to login after a SSHv2 connection has been established. The TOE utilizes a reliable time stamp for audit records that is provided by the real time clock in the Brocade Directors and Switches hardware appliances.

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 - Brocade Fabric OS - Administration Guide, 8.2.0a
  Technical Publication 53-1005237-05, 10 May 2018
- Brocade - Brocade Fabric OS Command Reference, 8.2.0a
  Technical Publication 53-1005241-04, 10 April 2018
- Brocade - Brocade Fabric OS Message Reference, 8.2.0a
  Technical Publication 53-1005249-04, 10 April 2018
- Brocade - Brocade Fabric OS 8.2.0a2 BSI Configuration Guide
  Technical Publication FOS-820X-BSI-UG100, 18 January 2019
- Brocade - Brocade Fabric OS Troubleshooting and Diagnostics Guide, 8.2.0
  Technical Publication 53-1005252-03, 10 April 2018

[5] FabricOS can be configured to prevent the use of Elliptic-Curve cryptographic algorithms with SSH.

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:
    - Assurance Level: EAL 2 augmented with ALC_FLR.2 conformant

2.1 Conformance Rationale

There is no Protection Profile claim.

3. Security Problem Definition

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL-2) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

T.ACCOUNTABILITY	A user may not be held accountable for their actions.
T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
T.TSF_COMPROMISE	A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTH_ACCESS	A user may gain unauthorized access (view, modify, delete) to a storage device.

3.2 Assumptions

A.ADMIN	An administrator should be a trustworthy and qualified person with sufficient administration skills.
A.AUDIT	The environment will provide a Syslog server and a means to present a readable view of the audit data.
A.AUTH_SVR	The authentication server will be capable of offering a password policy that requires password length, password strength and a restriction of failed login attempts that is consistent with the requirements of this Security Target.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MGMT_NET	The SSHv2 administration workstation, syslog server, and (when utilized) the authentication servers that are connected to the management network must be operated in a secure environment.
A.NETWORK	The environment will physically protect network communication to and from the TOE from unauthorized disclosure or modification.
A.NO_EVIL	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.
A.HARDWARE	The TOE is assumed to run on models of Brocade Directors and Switches that are listed in section 1.2. It is assumed that the following functionality is available to the TOE: a) Hardware real time clock b) A trustworthy bootloader

A.ORG_SUPPORT	The organization in which the TOE operates provides an appropriate cryptographic support infrastructure that is configured in a manner appropriate for the data processed by the TOE.

4. Security Objectives

This section summarizes the security objectives for the TOE and its environment.

4.1 Security Objectives for the TOE

O.ACCESS	The TOE will ensure that users gain only authorized access to the TOE and to the resources that the TOE controls.
O.ADMIN_ROLE	The TOE will provide authorized administrator roles to isolate administrative actions thus limiting the scope of errors that an administrator may cause.
O.AUDIT_GENERATION	The TOE will provide the capability to create records of security relevant events associated with users.
O.MANAGE	The TOE will allow administrators to effectively manage the TOE and its security functions, must ensure that only authorized administrators are able to access such functionality, and that communication between the TOE and the administrator is protected.
O.PROTECTED_COMM	The TOE will provide protected communication channels for administrators and authorized IT entities[6].
O.TOE_PROTECTION	The TOE will protect the TOE and its assets from external interference or tampering.
O.USER_AUTHENTICATION	The TOE will verify the claimed identity of users.
O.USER_IDENTIFICATION	The TOE will uniquely identify users.

4.2 Security Objectives for the Environment

OE.ADMIN	The environment will ensure that the administrators of the system are trustworthy and qualified personnel with sufficient administration skills.
OE.AUDIT	The environment will provide a Syslog server and a means to present a readable view of the audit data.
OE.AUTH_SVR	The authentication server will offer a password policy that requires password length, password strength and a restriction of failed login attempts that is consistent with the requirements of this Security Target.

[6] IT entities that a TOE is capable of communicating with are a syslog server, RADIUS server or LDAP server, as noted for FTP_ITC.1 application notes.

OE.PKI	The PKI associated with the trusted root certificates that are installed into the TOE utilize cryptographic algorithms and methods appropriate for the protection of the data processed by the TOE.
OE.NETWORK	The Environment will physically protect network communication to and from the TOE from unauthorized disclosure or modification.
OE.MGMT_NET	The SSHv2 administration workstation, syslog server, and (when utilized) the authentication servers that are connected to the management network are operated in a secure environment.
OE.CONFIG	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.
OE.PHYCAL	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
OE.HARDWARE	The TOE is assumed to run on models of Brocade Directors and Switches that are listed in section 1.2. In particular it is assumed that the following functionality is available to the TOE: a) Hardware real time clock b) A trustworthy bootloader

4.3 Security Objectives Rationale

This section shows that all secure usage assumptions, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

4.3.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats and usage assumptions by the security objectives.

	T.ACCOUNTABILITY	T.ADMIN_ERROR	T.MASQUERADE	T.TSF_COMPROMISE	T.UNAUTH_ACCESS	A.ADMIN	A.AUDIT	A. AUTH_SVR	A.LOCATE	A.NETWORK	A.MGMT_NET	A.NO_EVIL	A.HARDWARE	A.ORG_SUPPORT
O.ACCESS					X									
O.ADMIN_ROLE		X												
O.AUDIT_GENERATION	X													
O.MANAGE		X												
O.PROTECTED_COMM			X											
O.TOE_PROTECTION				X										
O.USER_AUTHENTICATION			X											
O.USER_IDENTIFICATION			X											
OE.ADMIN						X								
OE.AUDIT							X							

	T.ACCOUNTABILITY	T.ADMIN_ERROR	T.MASQUERADE	T.TSF_COMPROMISE	T.UNAUTH_ACCESS	A.ADMIN	A.AUDIT	A. AUTH_SVR	A.LOCATE	A.NETWORK	A.MGMT_NET	A.NO_EVIL	A.HARDWARE	A.ORG_SUPPORT
OE.AUTH_SVR								X						
OE.PKI														X
OE.CONFIG												X		
OE.NETWORK										X				
OE.MGMT_NET											X			
OE.PHYCAL									X					
OE.HARDWARE													X	

Table 4-1 Environment to Objective Correspondence

4.3.1.1 T.ACCOUNTABILITY

A user may not be held accountable for their actions.

This Threat is satisfied by ensuring that:

- O.AUDIT_GENERATION: The TOE will provide the capability to create records of security relevant events associated with users.

4.3.1.2 T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is countered by ensuring that:

- O.ADMIN_ROLE: The TOE will provide authorized administrator roles to isolate administrative actions thus limiting the scope of errors that an administrator may cause.
- O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions, must ensure that only authorized administrators are able to access such functionality, and that communication between the TOE and the administrator is protected.

4.3.1.3 T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

This Threat is countered by ensuring that:

- O.USER_AUTHENTICATION: The TOE will verify the claimed identity of users.
- O.USER_IDENTIFICATION: The TOE will uniquely identify users.
- O.PROTECTED_COMM: The TOE will provide protected communication channels for administrators and authorized IT entities.

4.3.1.4 T.TSF_COMPROMISE

A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

This Threat is countered by ensuring that:

- O.TOE_PROTECTION: The TOE will protect the TOE, and its assets from external interference or tampering.

4.3.1.5 T.UNAUTH_ACCESS

A user may gain unauthorized access (view, modify, delete) to a storage device.

This Threat is countered by ensuring that:

- O.ACCESS: The TOE will ensure that users gain only authorized access to the TOE and to the resources that the TOE controls.

4.3.1.6 A.ADMIN

An administrator should be a trustworthy and qualified person with sufficient administration skills.

This Assumption is satisfied by ensuring that:

- OE.ADMIN: The environment will ensure that the administrators of the system are trustworthy and qualified personnel with sufficient administration skills.

4.3.1.7 A.AUDIT

The environment will provide a Syslog server and a means to present a readable view of the audit data.

This Assumption is satisfied by ensuring that:

- OE.AUDIT: The environment will provide a Syslog server and a means to present a readable view of the audit data.

4.3.1.8 A.AUTH_SVR

The authentication server will be capable of offering a password policy that requires password length, password strength and a restriction of failed login attempts that is consistent with the requirements of this Security Target.

This Assumption is satisfied by ensuring that:

- OE.AUTH_SVR The authentication server will offer a password policy that requires password length, password strength and a restriction of failed login attempts that is consistent with the requirements of this Security Target.

4.3.1.9 A.LOCATE

The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

This Assumption is satisfied by ensuring that:

- OE.PHYCAL: The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.3.1.10 A.NETWORK

The Environment will physically protect network communication to and from the TOE from unauthorized disclosure or modification.

This Assumption is satisfied by ensuring that:

- OE.NETWORK: The Environment will physically protect network communication to and from the TOE from unauthorized disclosure or modification.

4.3.1.11 A.MGMT_NET

The SSHv2 administration workstation, syslog server, and (when utilized) the authentication servers that are connected to the management network must be operated in a secure environment.

This Assumption is satisfied by ensuring that:

- OE.MGMT_NETThe SSHv2 administration workstation, syslog server, and (when utilized) the authentication servers (i.e., RADIUS or LDAP) that are connected to the management network are operated in a secure environment.

4.3.1.12 A.NO_EVIL

The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

This Assumption is satisfied by ensuring that:

- OE.CONFIG: The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation

4.3.1.13 A.HARDWARE

The TOE is assumed to run on models of Brocade Directors and Switches that are listed in section 1.2. In particular it is assumed that the following functionality is available to the TOE:

a) Hardware real time clock
b) A trustworthy bootloader.

This Assumption is satisfied by ensuring that:

- OE.HARDWARE implements A.HARDWARE directly.

4.3.1.14 A.ORG_SUPPORT

The organization in which the TOE operates provides an appropriate cryptographic support infrastructure that is configured in a manner appropriate for the data processed by the TOE.

This Assumption is satisfied by ensuring that:

- OE.PKI: The PKI associated with the trusted root certificates that are installed into the TOE utilize cryptographic algorithms and methods appropriate for the protection of the data processed by the TOE.

5. Extended Components Definition

The iterations of the component FCS_RNG.1 is an extended component. The definition of the family FCS_RNG and its components can be found in the following document which is part of the BSI scheme document AIS 20/31:

- W. Killmann, W. Schindler, “A proposal for: Functionality classes for random number generators”, Version 2.0, September 1, 2011.

6. 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. This section also contains rationale for the SFRs and SARs. Finally, this section contains an analysis showing that all dependencies for the requirements included in the security target have been satisfied.

6.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the FabricOS Version 8.2.0a2 TOE running on the Brocade Directors and Switches.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
FCS: Cryptographic support	FCS_CKM.1(1): Cryptographic key generation for protected communication
	FCS_CKM.1(2): Cryptographic key generation for Host Authentication
	FCS_CKM.2: Cryptographic Key Distribution
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1(1): Cryptographic operation for cipher suites
	FCS_COP.1(2): Cryptographic Operation Payload Protection
	FCS_COP.1(3): Cryptographic Operations for Mutual Authentication
	FCS_COP.1(4) Cryptographic Operations for Key Agreement
	FCS_RNG.1: Random number generation for OpenSSL & OpenSSH (Class DRG.2)
FDP: User data protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1(1): User attribute definition: Administrators
	FIA_ATD.1(2): User attribute definition: Network Entities
	FIA_SOS.1: Verification of secrets
	FIA_UAU.2: User authentication before any action
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1: Management of security attributes for SAN Fabric Policy
	FMT_MSA.3: Static attribute initialisation for SAN Fabric Policy
	FMT_MTD.1(1): Management of TSF data
	FMT_MTD.1(2): Management of TSF data for a user password
	FMT_MTD.1(3): Management of TSF data for importing certificates
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FTA: TOE access	FTA_MCS.1: Basic limitation on multiple concurrent sessions
	FTA_TSE.1: TOE session establishment
FTP: Trusted path	FTP_ITC.1: Trusted Channel
	FTP_TRP.1: Trusted path

Table 6-1 TOE Security Functional Components

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and

shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**the events listed in** Table 6-2].

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 (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, [**no additional details**].

Requirement Component	Auditable event
FAU_GEN.1	start-up and shutdown of the audit functions (specifically, of the TOE)
FIA_AFL.1	Locking and unlocking of an account as a result of exceeding the maximum number of failed logons.
FIA_UAU.5	unsuccessful use of the authentication mechanism
FIA_UID.2	unsuccessful use of the user identification mechanism, including the user identity provided
FMT_SMF.1	use of the management functions (specifically, zone configuration, password management configuration, authentication attempts maximum configuration, TOE access filtering configuration, and setting user attributes)
FMT_SMR.1	modifications to the group of users that are part of a role

Table 6-2 Auditable Events

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation for protected communication (FCS_CKM.1(1))

FCS_CKM.1(1).1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**capable of generating a random bit sequences**] and specified cryptographic key sizes [

Key Sizes	Algorithm	Protocol
160 bit	HMAC-SHA1	SSHv2 and TLS
256-bit	HMAC-SHA256	SSHv2 and TLS
384-bit	HMAC-SHA384	TLS
512-bit	HMAC-SHA-512	SSHv2
128 bit	AES128-CBC	SSHv2 and TLS
256 bit	AES256-CBC	SSHv2 and TLS
128 bit	AES128-CTR	SSHv2
256 bit	AES256-CTR	SSHv2
256 bit	AES256-GCM	TLS

] that meet the following: [**keys are generated based on a random number generator which ensure entropy as defined by FCS_RNG.1(both iterations) and which satisfies the following:**

- **a) TLS: generation and exchange of session keys as defined in TLSv1.2 standard with the cipher suites defined in FCS_COP.1(1) and key derivation functions in FCS_COP.1(4),**
- **b) SSHv2: generation and exchange of session keys using the Diffie-Hellman key negotiation protocol as defined in RFC4253 defined in FCS_COP.1(1) and key derivation function FCS_COP.1(4).**

]

Application note: *For details of the SSH key generation and key negotiation process see section 8 of [RFC4253]. The evaluation will assess that the keys are generated in accordance with the requirements defined in [RFC4253].*

6.1.2.2 Cryptographic key generation for Host Authentication (FCS_CKM.1(2))

FCS_CKM.1(2).1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**capable of generating a random bit sequences for SSH Host Keys**] and specified cryptographic key sizes [**RSA keys of 2048 bits**] that meet the following: [**US NIST FIPS PUB 186-4].**

6.1.2.3 Cryptographic Key Distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**described in following table**] that meets the following: [**list of standard described in following table**].

Table 6-3 SSH & TLS Key Distribution

Key Distribution Method	Standard of Implementation	Key Size in bits
SSH: Key Exchange	DH ([HaC]) with Diffie-Hellman-group14-sha1from [RFC4253] (SSH v2.0), [RFC3526] (MODP)	plength = 2048
	DH ([HaC]) with diffie-Hellman-group-exchange-sha256 from [RFC4419] (SSH v2.0)	plength = 2048
TLS: encrypted exchange of pre-master secret	RSA-encryption RSAES-PKCS1-v1_5 (TLS_RSA) from [RFC5246] (TLS v1.2), [PKCS#1 v2.1]	modulus length = 2048
	DH ([HaC]) with group14 (TLS_DHE) from [RFC5246] (TLS v1.2)	modulus length = 2048

Application note *RSA public keys meeting the X.509 version 3 standard are generated external to the TOE and imported using the commands controlled by FMT_MTD.1(1).*

6.1.2.4 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroize**] that meets the following: [**none**].

6.1.2.5 Cryptographic Operation for Cipher Suites (FCS_COP.1(1))

FCS_COP.1(1).1

The TSF shall perform [**encryption, decryption, integrity verification, and peer authentication**] in accordance with a specified cryptographic algorithm [**associated with the cipher suites identified in the following list**] and cryptographic key sizes [**associated with the cipher suites identified in the following list**] that meet the following: [**protocols identified in the following list**].

a) **SSHv2 allowing the use of AES in CTR mode with 128 bits and 256 bits key sizes; AES in CBC mode with 128 bits and 256 bits key size;, and HMAC-SHA1, HMAC-SHA-256, or HMAC-SHA-512 defined by RFC 4253 (cipher suites: aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc);**
b) **TLSv1.2 allowing the use of the following cipher suites:**

i. **TLS_RSA_WITH_AES_128_CBC_SHA (number 002F)**
ii. **TLS_RSA_WITH_AES_256_CBC_SHA (number 0035)**
iii. **TLS_RSA_WITH_AES_128_CBC_SHA256 (number 003C)**
iv. **TLS_RSA_WITH_AES_256_CBC_SHA256 (number 003D)**
v. **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (number 009F)**

Application Note: *The two cipher suites (002F and 0035) do not work with TLSv1.2 and the RADIUS protocol. Using TLSv1.2 and RADIUS requires the use of the three cipher suites (003C, 003D and 009F).*

6.1.2.6 Cryptographic Operation Payload Protection (FCS_COP.1(2))

FCS_COP.1(2).1

The TSF shall perform [**cryptographic operations described in following table**] in accordance with a specified cryptographic algorithm [**cryptographic algorithm described in following table**] and cryptographic key sizes [**cryptographic key sizes described in following table**] that meet the following: [**list of standards described in following table**].

Table 6-4 SSH & TLS Payload Protection

Operation/ Purpose	Algorithm	Standard of Implementation	Key Size in bits
SSH Encryption and decryption	SSH: AES in CBC mode (aes128-cbc,aes256-cbc)	[FIPS-197] (AES), [SP 800-38A] (CBC), [RFC4253] (SSH v2.0)	|K| = 128, 256
	SSH: AES in CTR mode (aes128-ctr, and aes256-ctr)	[FIPS-197] (AES), [SP 800-38A] (CTR), [RFC4253] (SSH v2.0)	|K| = 128, 256
SSH Message authentication code generation and verification	SSH: HMAC with SHA-1, SHA-256, SHA-512 (hmac-sha1, hmac-sha2-256, hmac-sha2-512)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC4253] (SSH v2.0), [RFC6668] (SHA-2 for SSH)	|K| = 128, 256, 512
TLS Encryption and decryption	TLS: AES in CBC mode (AES_128_CBC, AES_256_CBC)	[FIPS-197] (AES), [SP 800-38A] (CBC), [RFC5246] (TLS v1.2)	|K| = 128, 256
	TLS: AES in GCM mode (AES_256_ GCM)	[FIPS-197] (AES), [SP 800-38D] (GCM), [RFC5246] (TLS v1.2)	|K| = 256
TLS Message authentication code generation and verification	TLS: HMAC with SHA-1, SHA-256, or SHA-384 (SHA1, SHA256, SHA-384)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	|K| = 128, 256, 384

6.1.2.7 Cryptographic Operations for Mutual Authentication (FCS_COP.1(3))

FCS_COP.1(3).1

The TSF shall perform [**cryptographic operations described in following table**] in accordance with a specified cryptographic algorithm **[cryptographic algorithm described in following**

table] and cryptographic key sizes [**cryptographic key sizes described in following table**] that meet the following: [**list of standards described in following table**].

Table 6-5 SSH & TLS Mutual Authentication

Operation/ Purpose	Authentication Mechanism	Standard of Implementation	Key Size in bits
SSH Server and client: Authentication of user	generation ("publickey": RSASSA-PKCS1-v1_5)	[PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC4252] (SSH-AUTH)	modulus length ≥ 2048
	Authentication based on user name and password ("password")	ch. 5 of [RFC4252] (SSH-AUTH)	Guess success probability $\varepsilon \leq 10^{-8}$
SSH Client: Authentication of host	RSA signature verification (RSASSA-PKCS1-v1_5 using SHA1(rsa2048-sha1))	[PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC4432] (RSA for SSH)	modulus length = 2048
TLS: Asymmetric authentication	Public-key-based authentication of the server using RSA-encryption RSAES-PKCS1-v1_5	[PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC5246] (TLS v1.2)	Modulus length = 2048

Application note: *RSA public keys meeting the X.509 version 3 standard are generated external to the TOE and imported using the commands controlled by FMT_MTD.1(1).*

Application Note: *The TOE enforces at minimum 1024 bit of modulus length.*

6.1.2.8 Cryptographic Operations for Key Agreement (FCS_COP.1(4))

FCS_COP.1(4).1

The TSF shall perform [**cryptographic operations described in following table**] in accordance with a specified cryptographic algorithm [**cryptographic algorithm described in following table**] and cryptographic key sizes [**cryptographic key sizes described in following table**] that meet the following: [**list of standards described in following table**].

Table 6-6 SSH and TLS Key Agreement

Operation/ Purpose	Algorithm	Standard of Implementation	Key Size in bits
SSH Key Derivation Function	SSH: PRF based on SHA-1 (diffie-hellman-group14-sha1)	[FIPS180-4] (SHA), [RFC4253] (SSH v2.0)	|K| = variable
	SSH: PRF based on SHA-256 (diffie-hellman-group-exchange-sha256)	[FIPS 180-4] (SHA256), [RFC4419] (SSH v2.0)	|K| = variable
	TLSv1.2: PRF based on HMAC with SHA-256 (tls_prf_sha256)[7]	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	|K| = variable

[7] the default TLS 1.2 Pseudorandom Function (PRF)

TLS Key Derivation Function	TLSv1.2: PRF based on HMAC with SHA-384 (tls_prf_sha384)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	|K| = variable

Application Note: *FCS_RNG.1 delivers the input for the key derivation function.*

6.1.2.9 Random Number Generation for OpenSSL & OpenSSH (Class DRG.2) (FCS_RNG.1)

FCS_RNG.1.1

For use by OpenSSH and OpenSSL, the TSF shall provide a [***deterministic***] random number generator that implements:

(DRG.2.1) If initialized with a random seed [***[that is provided through dev\random which is accumulated from timer interrupts]***], the internal state of the RNG shall [***have [at least 192 bits of entropy]***].

(DRG.2.2) The RNG provides forward secrecy.

(DRG.2.3) The RNG provides backward secrecy.

FCS_RNG.1.2

The TSF shall provide random numbers that meet

(DRG.2.4) The RNG, initialized with a random seed [on every request to X9.31/AES256 RNG], generates output for which [**at least 2^{14}**] strings of bit length 128 are mutually different with probability [**greater than or equal to 1 minus 2^{-8}**].

(DRG.2.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

Application Note: *The deterministic random number generator is based on ANSI X9.31. The internal state of the RNG has a length of 384 bits.*

Application Note: *This requirement is intended to describe the random number generation associated with the generation of TLS and SSH keys by the TOE. That is, the RNG is the deterministic random number generator used by OpenSSL and OpenSSH.*

Application Note: *The component FCS_RNG.1 is an extended component. The definition of the family FCS_RNG and its components can be found in the following document which is part of the BSI scheme document AIS 20/31:*

W. Killmann, W. Schindler, "A proposal for: Functionality classes for random number generators", Version 2.0, September 1, 2011.

6.1.3 User data protection (FDP)

6.1.3.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1

The TSF shall enforce the [**SAN Fabric SFP**] on [

a.) **subjects: host bus adapters**
b.) **objects: storage devices**
c.) **operations: block-read and block-write**

].

Application Note: *The subjects in the TOE are host bus adapters and the objects are storage devices. Operations mediated by the TOE are block-reads and block-writes. The TOE utilizes port*

number and zone membership of a host bus adapter as well as the storage device address and zone membership of the storage devices when enforcing its SAN Fabric SFP.

6.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1

The TSF shall enforce the [**SAN Fabric SFP**] to objects based on the following: [

a.) **subject security attributes:**

1. **port number;**
2. **zone membership**

b.) **storage device security attributes:**

3. **storage device address;**
4. **zone membership**

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**for any zone, if the subject port is a member of that zone and the device address is a member of that zone, then the operation is allowed**].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[no additional rules].**

6.1.4 Identification and authentication (FIA)

6.1.4.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1

The TSF shall detect when [***an administrator configurable positive integer within [1 to 999]***] unsuccessful authentication attempts occur related to [**user logon**].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [***met* or *surpassed***], the TSF shall [**lockout the account for an administrator configured time period**].

6.1.4.2 User attribute definition: Administrators (FIA_ATD.1(1))

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:[

a.) **the security attributes of users possessing administrative roles:**

- **user identity**
- **password**
- **role**

].

Application Note: *Human user authentication occurs only in the context of an SSH administrative session. Network Peer authentication can occur only over TLS protected communication pathways. FIA_UID.2 and FIA_UAU.2 use the generic term "user" to encompass both human users and network peers as users. The two iterations of FIA_ATD.1 define the different data stored by the TOE for these two types of user.*

6.1.4.3 User attribute definition: Network Entities (FIA_ATD.1(2))

FIA_ATD.1(2).1

The TSF shall maintain the following list of security attributes belonging to individual **TLS network peer** users: [

a) Network address/identifier of the TLS network peer; and

b) Public certificate of the TLS network peer.]

Application Note: *This requirement applies to users of the TOE that are actually network entities providing services to the TOE.*

Application Note: *The TOE may store either a network address or a DNS name for the network peer.*

Application Note: *Rather than storing certificates for individual peers, the TOE can store a trusted root certificate for an authority trusted that can sign peer certificates. A network peer may then be identified by virtue of the TOE verifying a the root of a trust chain for the certificate of a network peer.*

Application Note: *See also the application note for FIA_ATD.1(1).*

6.1.4.4 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [**an administrator specified overall minimum length and have a minimum number of specified character types**].

Application Note: *These limitations apply only for local identification and authentication. The limits may be different when using a RADIUS or LDAP server for identification and authentication*

6.1.4.5 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1

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

6.1.4.6 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1

The TSF shall provide [**local authentication, authentication by a third-party RADIUS and authentication by a third-party LDAP server**] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [**following:**

- **Human users are authenticated using the administrator configured order of authentication providers; and**
- **Network Peers are authenticated locally using certificates**].

6.1.4.7 User identification before any action (FIA_UID.2)

FIA_UID.2.1

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

6.1.5 Security management (FMT)

6.1.5.1 Management of security attributes for SAN Fabric Policy (FMT_MSA.1)

FMT_MSA.1.1

The TSF shall enforce the [**SAN Fabric SFP**] to restrict the ability to [***[add or remove members of a zone using***]] the security attributes [**host bus adapter port number; storage device port number; zone membership of a host bus adapter and zone membership of a storage device**] to [**users possessing one of the following administrative roles: admin, zoneAdmin, fabricAdmin, root**].

Application note: Host bus adapters and storage devices are referred to as members of a zone when they are added to a zone.

6.1.5.2 Static attribute initialization for SAN Fabric Policy (FMT_MSA.3)

FMT_MSA.3.1

The TSF shall enforce the [**SAN Fabric SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [**admin role**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.3 Management of TSF data (FMT_MTD.1(1))

FMT_MTD.1(1).1

The TSF shall restrict the ability to [***query, modify, delete, [and assign]***] the [

- **user identity,**
- **user role,**
- **minimum password length and minimum number of specified character types used in a password,**
- **number of unsuccessful authentication attempts that cause accounts to be locked,**
- **locked status of an account,**
- **order in which authentication providers are checked,**
- **presumed source address and service permitted from which remote users connect to the TOE,**
- **identify of network syslog, RADIUS and/or LDAP peers,**
- **cryptographic values associated with network peers,**
- **cryptographic values associated identifying the TOE.**

]

to [**users possessing one of the following administrative roles: admin, SecurityAdmin, root**].

Application note: The cryptographic values referenced above are those associated with the FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_COP.1(*) and FIA_ATD.1(2) requirements.

6.1.5.4 Management of TSF data for a user password (FMT_MTD.1(2))

FMT_MTD.1(2).1

The TSF shall restrict the ability to [***set***] the [**passwords**] to [**the administrative user associated with the password, and users possessing one of the following administrative roles: admin, SecurityAdmin, root**].

6.1.5.5 Management of TSF data for importing certificates (FMT_MTD.1(3))

FMT_MTD.1(3).1

The TSF shall restrict the ability to [***import***] the [**SSL switch certificate and root CA**

Certificates] to [**users possessing one of the following administrative roles: admin, SecurityAdmin, root**].

6.1.5.6 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:[

- **add or remove members of a zone;**
- **manage the minimum password length and minimum number of specified character types used in a password,**
- **manage the number of unsuccessful authentication attempts that cause accounts to be locked,**
- **manage the locked status of an account,**
- **specify the order in which authentication providers are checked,**
- **generate RSA Host Key pairs for use with SSH,**
- **export SSH public keys used to authenticate outbound SSH connections,**
- **import public keys to authenticate SSH users,**
- **import certificates for use with TLS,**
- **specify the presumed source address and service permitted from which remote users connect to the TOE; query, modify, delete, and assign the user identity and role; and set and reset passwords of users possessing administrative roles.].**

6.1.5.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the roles [**the following administrative roles:**

- **admin**
- **switchAdmin**
- **operator**
- **zoneAdmin**
- **fabricAdmin**
- **SecurityAdmin**
- **basicSwitchAdmin**
- **root**
- **user**

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application note: *Other than being able to log into TOE management interfaces and change their own passwords, users possessing the user administrative role can only access interfaces that provide the ability to monitor TOE performance.*

6.1.6 TOE access (FTA)

6.1.6.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2

The TSF shall enforce, by default, a limit of [**Four (4)**] sessions per user.

Application Note: *These limitations apply only for locally defined accounts undergoing identification and authentication. The limits may be different when using accounts defined under a RADIUS or LDAP server for identification and authentication*

6.1.6.2 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1

The TSF shall be able to deny session establishment based on [**authentication data expiration, presumed source address of the remote user and service being requested**].

6.1.7 Trusted path (FTP)

6.1.7.1 Trusted Channels to network peers (FTP_ITC.1)

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification ~~or~~ **and** disclosure **using TLSv1.2**.

FTP_ITC.1.2

The TSF shall permit the [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**transfer of audit records, verification of user identity via remote authentication server**].

Application Note: *The TOE supports trusted channels to network entities acting as a syslog server, RADIUS server or LDAP server. All such trusted channels are based upon TLS.*

Application Note: *The TOE is always the initiator of a TLS session (for syslog, RADIUS and LDAP). The TOE authenticates the remote TLS endpoint using the certificate associated with the target network peer (FIA_ATD.1(2)).*

Application Note: *The TOE authenticates itself to a syslog server via a certificate provided in the TLS exchange. The TOE utilizes authentication provided by the RADIUS and LDAP protocols to authenticate to a RADIUS and LDAP peer.*

6.1.7.2 Trusted path (FTP_TRP.1)

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***disclosure, modification***].

FTP_TRP.1.2

The TSF shall permit [***remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [***[administrator access of the TOE via Ethernet using SSH]***].

6.2 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.MANAGE	O.PROTECTED_COMM	O.TOE_PROTECTION	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION
FAU_GEN.1			X					
FCS_CKM.1(1)						X		
FCS_CKM.1(2)						X		
FCS_CKM.2						X		
FCS_CKM.4						X		
FCS_COP.1(1)						X		
FCS_COP.1(2)						X		
FCS_COP.1(3)						X		
FCS_COP.1(4)						X		
FCS_RNG.1						X		
FDP_ACC.1	X							
FDP_ACF.1	X							
FIA_AFL.1							X	
FIA_ATD.1(1)							X	X
FIA_ATD.1(2)					X			
FIA_SOS.1							X	
FIA_UAU.2							X	
FIA_UAU.5							X	
FIA_UID.2								X
FMT_MSA.1				X				
FMT_MSA.3				X				
FMT_MTD.1(1)				X				
FMT_MTD.1(2)				X				
FMT_MTD.1(3)				X				
FMT_SMF.1				X				
FMT_SMR.1		X		X				
FTA_MCS.1				X				
FTA_TSE.1				X				
FTP_ITC.1					X			
FTP_TRP.1				X				

Table 6-7 Objective to Requirement Correspondence

6.2.1 O.ACCESS

The TOE will ensure that users gain only authorized access to the TOE and to the resources that the TOE controls.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1, FDP_ACF.1: The TOE provides the ability to restrict block-read and block-write operations to connected storage devices that are initiated by host bus adapters. Host bus adapter can only access storage devices that are members of the same zone.

6.2.2 O.ADMIN_ROLE

The TOE will provide authorized administrator roles to isolate administrative actions thus limiting the scope of errors that an administrator may cause.

This TOE Security Objective is satisfied by ensuring that:

- FMT_SMR.1: The TOE maintains only administrative roles.

6.2.3 O.AUDIT_GENERATION

The TOE will provide the capability create records of security relevant events associated with users.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE generates audit events for the not specified level of audit.

6.2.4 O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, must ensure that only authorized administrators are able to access such functionality, and that communication between the TOE and the administrator is protected.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1: The ability to modify host bus adapters and storage devices zone membership is limited to users possessing the admin, zoneAdmin, fabricAdmin, or root roles.
- FMT_MSA.3: Once the TOE has been properly configured, host bus adapters do not have default access to storage devices. Only accounts with the admin role can specify the zone for new storage devices or HBAs.
- FMT_MTD.1(1): The ability to query, modify, delete, and assign administrative user security attributes is limited to users possessing one of the following administrative roles: admin, Security Admin, root.
- FMT_MTD.1(2): Administrators can set their own passwords. The administrative roles admin, Security Admin and root may set any account's password.
- FMT_MTD.1(3): Administrators can issue commands to import a certificate for use as the TOE certificate or import certificates for use as root CA certificates.
- FMT_SMF.1: The TOE provides administrative interfaces to modify and query host bus adapters and storage device zone membership, as well as to set and reset administrator passwords.
- FMT_SMR.1: The TOE maintains administrative user roles.
- FTA_MCS.1: The TOE limits the number of concurrent sessions a user can have based upon the user's role. This limitation applies only for local identification and authentication. The limits may be different when using a RADIUS or LDAP server for identification and authentication.
- FTA_TSE.1: The TOE limits the locations and services through which administrators can establish remote administrative sessions based upon the presumed source network location.
- FTP_TRP.1: The TOE provides a trusted path between itself and remote administrative users.

6.2.5 O.PROTECTED_COMM

The TOE will provide protected communication channels for administrators and authorized IT entities.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE maintains security attributes for authenticating network peers that act as a syslog server, RADIUS server or LDAP server.
- FTP_ITC.1: The TOE provides a trusted communication channel that utilizes TLS. This channel protects communication between the TOE itself and network peers providing syslog, RADIUS and LDAP services.

6.2.6 O.TOE_PROTECTION

The TOE will protect the TOE and its assets from external interference or tampering.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1(all iterations): The TOE utilizes cryptography to as part of the trusted path and trusted channel mechanisms that protects communications during administrative sessions as well as communication with network peers (i.e., syslog servers, RADIUS servers and LDAP servers).
- FCS_CKM.1(1) and FCS_CKM.1(2): The TOE generates keys for use with the trusted path and trusted channel mechanisms.
- FCS_CKM.2: The TOE distributes cryptographic keys in the context of a TLS handshake and negotiation of SSH symmetric session keys.
- FCS_CKM.4: The TOE zeroizes keys used in for the trusted path mechanism when the key is no longer needed.
- FCS_RNG.1: The TOE generates random numbers for use in key generation by OpenSSH and OpenSSL that is associated with the trusted channel and trusted path mechanisms.

6.2.7 O.USER_AUTHENTICATION

The TOE will verify the claimed identity of users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_AFL.1: The TOE locks user accounts as a result of too many failed logon attempts.
- FIA_ATD.1: The TOE maintains security attributes for administrative users.
- FIA_SOS.1: The TOE provides administratively defined constraints on user passwords. These constraints apply only for local identification and authentication. The constraints may be different when using a RADIUS or LDAP server for identification and authentication
- FIA_UAU.2: The TOE performs user authentication before allowing any other actions.
- FIA_UAU.5: The TOE supports the authentication of users via a local database of user accounts, via third-party RADIUS servers or via third-party LDAP servers.

6.2.8 O.USER_IDENTIFICATION

The TOE will uniquely identify users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE maintains security attributes for administrative users.

- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified. Administrative users are identified using user identifiers.

6.3 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 2 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 6-8 EAL 2 augmented with ALC_FLR.2 Assurance Components

6.3.1 Development (ADV)

6.3.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1d
The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2d
The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3d
The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1c
The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c
The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c
The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4c
The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5c
The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1e

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

6.3.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1d

The developer shall provide a functional specification.

ADV_FSP.2.2d

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

ADV_FSP.2.1c

The functional specification shall completely represent the TSF.

ADV_FSP.2.2c

The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3c

The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4c

For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5c

For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6c

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

ADV_FSP.2.1e

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

ADV_FSP.2.2e

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

6.3.1.3 Basic design (ADV_TDS.1)

ADV_TDS.1.1d

The developer shall provide the design of the TOE.

ADV_TDS.1.2d

The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1c

The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2c

The design shall identify all subsystems of the TSF.

ADV_TDS.1.3c

The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4c

The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.1.5c

The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6c

The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

ADV_TDS.1.1e

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

ADV_TDS.1.2e

The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.3.2 Guidance documents (AGD)

6.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

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

AGD_OPE.1.2c

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

AGD_OPE.1.3c

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

AGD_OPE.1.4c

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

AGD_OPE.1.5c

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

AGD_OPE.1.6c

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

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

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

6.3.2.2 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.

6.3.3 Life-cycle support (ALC)

6.3.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1d

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

ALC_CMC.2.2d

The developer shall provide the CM documentation.

ALC_CMC.2.3d

The developer shall use a CM system.

ALC_CMC.2.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.2.2c

The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3c

The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1e

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

6.3.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1c

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

ALC_CMS.2.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3c

For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1e

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

6.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d

The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2d

The developer shall use the delivery procedures.

ALC_DEL.1.1c

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1e

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

6.3.3.4 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d
The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2d
The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3d
The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1c
The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2c
The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3c
The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4c
The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5c
The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6c
The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7c
The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8c
The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.2.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.4 Tests (ATE)

6.3.4.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d
The developer shall provide evidence of the test coverage.

ATE_COV.1.1c
The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

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

6.3.4.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d
The developer shall test the TSF and document the results.

ATE_FUN.1.2d
The developer shall provide test documentation.
ATE_FUN.1.1c
The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2c
The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3c
The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4c
The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.4.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d
The developer shall provide the TOE for testing.
ATE_IND.2.1c
The TOE shall be suitable for testing.
ATE_IND.2.2c
The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e
The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e
The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.3.5 Vulnerability assessment (AVA)

6.3.5.1 Vulnerability analysis (AVA_VAN.2)

AVA_VAN.2.1d
The developer shall provide the TOE for testing.
AVA_VAN.2.1c
The TOE shall be suitable for testing.
AVA_VAN.2.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2e
The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3e
The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
AVA_VAN.2.4e
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.

6.4 Security Assurance Requirements Rationale

EAL-2 augmented was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. ALC_FLR.2 was selected to exceed EAL-2 assurance objectives in order to ensure that identified flaws are addressed. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a basic attack potential. As such, EAL-2 is appropriate to provide the assurance necessary to counter the basic potential for attack.

6.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE. The one additional assurance requirement beyond EAL-2 (i.e., ALC_FLR.2) that has been added for this product has been included in this analysis.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	OE.Hardware
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1(1) FCS_CKM.1(2), and FCS_CKM.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1(1) FCS_CKM.1(2), and FCS_CKM.4
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1(1) FCS_CKM.1(2), and FCS_CKM.4
FCS_COP.1(4)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1(1) FCS_CKM.1(2), and FCS_CKM.4
FCS_CKM.1(1)	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4) and FCS_CKM.4
FCS_CKM.1(2)	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1(3) and FCS_CKM.4
FCS_CKM.2	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1(1), FCS_CKM.1(2) and FCS_CKM.4
FCS_CKM.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1 and
FCS_RNG.1	None	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1(1)	none	none
FIA_ATD.1(2)	none	none
FIA_SOS.1	none	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	none
FIA_UID.2	none	none
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1, and FMT_SMR.1
FMT_MTD.1(1), FMT_MTD.1(2), and FMT_MTD.1(3)	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none

ST Requirement	CC Dependencies	ST Dependencies
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_MCS.1	FIA_UID.1	FIA_UID.2
FTA_TSE.1	none	none
FTP_ITC.1	none	none
FTP_TRP.1	none	none
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	ADV_FSP.2 and ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2
AGD_PRE.1	none	none
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2
ALC_CMS.2	none	none
ALC_DEL.1	none	none
ALC_FLR.2	none	none
ATE_COV.1	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1

Table 6-9 Requirement Dependencies

The TOE is assumed to run on models of Brocade Directors and Switches that are listed in section 1.2. In particular, it is assumed that a hardware real time clock is available to the TOE.

7. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- User data protection
- Identification and authentication
- Security management
- TOE access
- Trusted path

This chapter also includes Cryptographic mechanism references summary and covers the topics of TSF protection, identifies TOE assurance measures and provides TSS rationale mapping TOE security functions to requirements.

7.1 Security audit

The TOE generates audit records for start-up and shutdown of the TOE, and for an unspecified level of audit. 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 sends audit records to a syslog server in the environment. The environment is relied on to provide interfaces to read from the audit trail. The auditable events include:

Requirement Component	Auditable event
FAU_GEN.1	start-up and shutdown of the audit functions (specifically, of the TOE); The TOE auditing capability of the TOE is operational whenever the TOE is running. Thus, starting and stopping audit occurs only with the starting and stopping of the TOE. For controlled system shutdown/reloads, audits are generated indicating the planned action. When most system crashes occur, audits cannot be generated for the shutdown of auditing. Regardless of how the system stopped (planned shutdown or crash) an audit is generated indicating that the system is starting.
FIA_AFL.1	Locking and unlocking of an account as a result of exceeding the maximum number of failed logons.
FIA_UAU.2	Unsuccessful use of the authentication mechanism
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided
FMT_SMF.1	Use of the management functions (specifically, zone configuration, data encryption configuration, password management configuration, authentication attempts maximum configuration, TOE access filtering configuration, and setting user attributes)
FMT_SMR.1	Modifications to the group of users that are part of a role

Table 7-1 Requirement Component and Auditable event

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

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

  Each audit record contains the following fields:

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

For example:

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

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

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

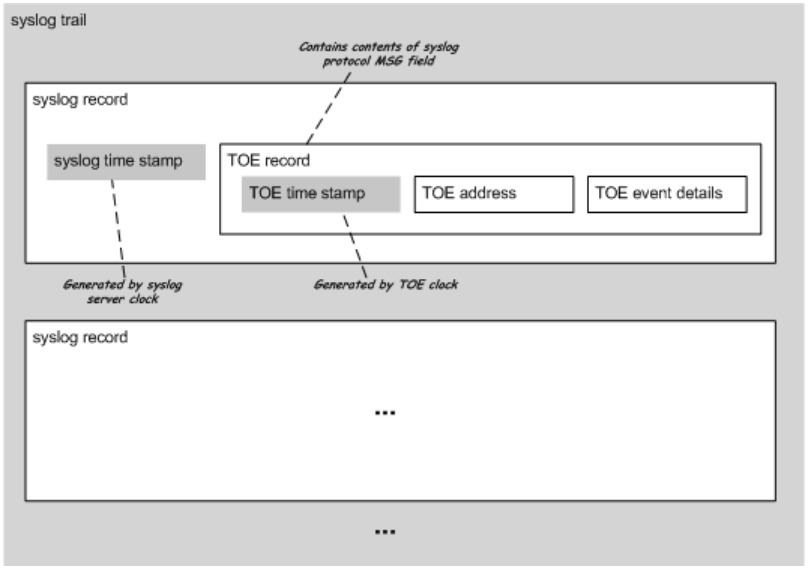

Figure 7-1: TOE and environment audit record components.

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

For example:

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

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

- FAU_GEN.1: The TOE generates audit events for the not specified level of audit. A syslog server in the environment is relied on to store audit records generated by the TOE.

7.2 User data protection

The evaluated configuration supports only interconnected TOE instances operated in a fabric switch mode.

The TOE defines host bus adapters in terms of port number and zone membership. The “port number” attribute that specifies a particular HBA host is semantically equivalent to the host address used to determine connectivity. The

"port number" specifies the specific physical port to which the HBA is connected. The unique host address obtained from the TOE when the HBA connects to the fabric also specifies the physical port to which the HBA is connected.

The first thing a host bus adapter must do is establish connectivity with at least one storage device located in the fabric. In order for a host bus adapter to access a storage device using the TOE, a port must be configured by an administrator to be a member of a zone of which a target storage device is already a member. After establishing a physical connection with the TOE, the HBA acquires what is called a SAN fabric address from the TOE, which is a 24-bit address format. Upon receiving an address, the HBA next registers itself with the TOE. The HBA then initiates FC[8]-protocol commands to establish connectivity with one or more targets located within the fabric. The TOE then determines whether or not to allow access to the storage device by comparing zone memberships.

The TOE implements the SAN Fabric SFP to restrict block-read and block-write operations to an HBA that is a member of the same zone as the object storage device. Host bus adapters can only access storage devices that are members of the same zone. Hardware-enforced zoning (also called "hard zoning" or simply "zoning") prevents a host bus adapter from accessing a device the host bus adapter is not authorized to access. The product also includes what is called soft zoning. Soft zoning does not restrict access to connected storage devices. If a host bus adapter has knowledge of the network address of a target device, the host bus adapter can read and write to it. That is why soft zoning is not supported in the evaluated configuration. Administrative guidance is relied on to warn against the use of soft zoning and it is not otherwise enabled by default in the evaluated configuration. A host bus adapter must be a member of a zone under hard zoning, configured by an administrator, before a host bus adapter can access a storage device.

Zoning works by checking each frame before it is delivered to a zone member and discarding it if there is a zone mismatch. The TOE monitors HBA communications and blocks any frames that do not comply with the zone configuration. Zoning prevents users from even discovering the existence of unauthorized target devices.

A zone is a region within the fabric where a specified group of fabric-connected devices (called zone members) have access to one another. Storage devices not explicitly defined in a zone are isolated, and host bus adapters in the zoned fabric do not have access to them.

- A group of one or more zones is called a *zone configuration*.
- The complete set of all zone members defined in a fabric is called the *defined zone configuration*.
- Zoning configuration procedures change zone objects in the defined configuration. When a configuration is enabled by an administrator, it becomes the *effective zone configuration*. The effective zone configuration is restored after a TOE reboot. This is also known as the *active zone configuration*.
- A copy of the defined zone configuration (plus the name of the effective zone configuration) can be saved by an administrator. The resulting *saved zone configuration* is restored after a switch reboot. If an administrator makes changes to the defined zone configuration but does not save them, there will be differences between the defined zone configuration and the saved zone configuration.
- A *default zone* is a zone that contains all ports that are not members of any zone in the active zone set.

A zone object is either an HBA or a disk. Any zone object connected to the fabric can be included in one or more zones. Zone objects can communicate only with other objects in the same zone. For example, consider the figure below, which shows:

- Three zones are configured, named Red, Green, and Blue.
- Server 1 can communicate only with the Loop 1 devices.
- Server 2 can communicate only with the RAID and Blue zone devices.
- Server 3 can communicate with the RAID device and the Loop1 device.
- The Loop 2 JBODs are not assigned to a zone; no other zoned fabric device can access them.

[8] Note that use of the FC over IP (FCIP) protocol is not included in an evaluated configuration.

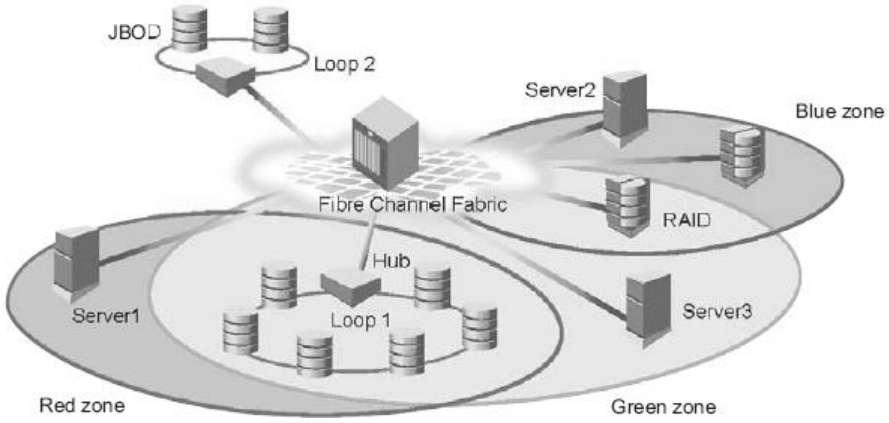

Figure 7-2: Sample Zones

The TOE determines whether or not to allow an HBA access to a storage device by comparing zone memberships. If access is permitted, the HBA is subsequently permitted to issue FC-protocol commands that correspond to disk read and write operations. If access is not permitted, a rejection command is returned to the HBA and any subsequent read or write operations from that HBA are discarded by the TOE.

When a host bus adapter performs a read or a write after the HBA has established a connection with a storage device using the TOE according to the SAN Fabric SFP, the HBA either breaks data blocks up into multiple data frames (in the case of a block-write operation) before sending the information to the TOE, or reassembles data frames into blocks (in the case of a block-read operation). When a write operation is performed, the storage device after the operation has completed transmits a single frame back through the TOE to the HBA to acknowledge that all data was received and written to the storage device.

When a host bus adapter performs a read to a target device for which it has established a connection, the HBA first issues the appropriate FC protocol command to the target at its defined 24-bit address. Next, the TOE inspects the user's HBA's Host address and target address within the frame to verify that connectivity is allowed via the current zoning configuration.

- If connectivity is allowed, then no further action is taken by the TOE besides ensuring that all of the frames are properly routed to their assigned destination based on their 24-bit destination address.
- If connectivity is not allowed, then the TOE sends a rejection command to the HBA and any subsequent read operations are rejected by the TOE.

Finally, the HBA collects all data frames and combines the data into the requested block for the host.

When a host bus adapter performs a write to a target device for which it has established a connection, the HBA first issues the appropriate FC protocol command to the target at its defined 24-bit address. Next, the TOE inspects the user's HBA's Host address and target address within the frame to verify that connectivity is allowed via the current zoning configuration.

- If connectivity is allowed, then no further action is taken by the TOE besides ensuring that all of the frames are properly routed to their assigned destination based on their 24-bit destination address.
- If connectivity is not allowed, then the TOE sends a rejection command to the HBA and any subsequent write operations are rejected by the TOE..

Next the HBA breaks up the data block to be written into multiple data frames, and transmits each one to the target. The TOE inspects the 24-bit address of each data frame, either allowing it to route properly, or rejecting it depending on the current zoning configuration.

Finally, the storage device transmits back a single frame acknowledging that all data was received and written to the storage media.

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

- FDP_ACC.1, FDP_ACF.1: The TOE provides the ability to restrict block-read and block-write operations to connected storage devices that are initiated by host bus adapters. Host bus adapter can only access storage devices that are members of the same zone.

7.3 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. Nine roles, each with a fixed set of permissions, are supported: Root, Admin, FabricAdmin, SecurityAdmin, SwitchAdmin, BasicSwitchAdmin, ZoneAdmin, Operator and User. There are three pre-defined administrator accounts called "root", "admin" and "user", each of which is assigned the respective role of the same name, e.g. the "admin" account is assigned the Admin role. Note that neither the account called "user" nor any account that is assigned the User role, corresponds to a host bus adapter that is attempting to access a storage device, rather a User-role account corresponds to an administrative user that can view but not change configuration settings. The root account is disabled during TOE configuration, since it allows access to the operating system. This root account is not the same as the "Root" role.

The TOE authenticates administrative users using either its own authentication mechanism or a RADIUS or LDAP Server. The TOE provides its own password authentication mechanism to authenticate administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user, and an administrative role must be assigned. The TOE password authentication mechanism enforces password composition rules. Passwords must be between 8 and 40 characters; they must begin with an alphabetical character; they can include numeric characters, the dot (.), and the underscore (_); they are case-sensitive. In the case of RADIUS or LDAP Server authentication, the TOE passes the login credentials supplied to the RADIUS or LDAP Server for validation. If the RADIUS or LDAP Server returns a success value, the TOE matches the user name to a user name stored internally. The administrator can configure the order in which the external authentication provider and the local credentials are checked.

The TOE supports several password policies which apply only to accounts defined within the local user database.

Password Strength

The password strength policy is enforced across all user accounts, and enforces a set of format rules to which new passwords must adhere. The password strength policy is enforced only when a new password is defined. The administrator can specify the number of lowercase, uppercase, digits, and punctuation that are required. The password strength policy can also specify the minimum length of a password.

Password History

The password history policy prevents users from recycling recently used passwords, and is enforced across all user accounts when users are setting their own passwords. The password history policy is enforced only when a new password is defined.

Specify the number of past password values that are disallowed when setting a new password.

Account Lockout

The account lockout policy disables a user account when that user exceeds a specified number of failed login attempts, and is enforced across all user accounts. Administrators configure this policy to either keep the account locked until explicit administrative action is taken to unlock it, or the locked account can be automatically unlocked after a specified period. Administrators can unlock a locked account at any time.

A failed login attempt counter is maintained for each user. The counters for all user accounts are reset to zero when the account lockout policy is enabled. The counter for an individual account is reset to zero when the account is unlocked after a lockout duration period expires.

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

- FIA_AFL.1: The TOE locks an account when the number of failed logon attempts exceeds an administrator specified value. The account cannot be used until it is unlocked by an administrator or after an administrator specified time period has elapsed.
- FIA_ATD.1(1): The TOE maintains security attributes for administrative users.
- FIA_ATD.1(2): The TOE maintains configuration information for each syslog server peer, RADIUS server peer, and LDAP server peer. This information contains and identifier for the network peer. In most cases, the TOE does not store a certificate for each peer, but instead saves a set of root-certificates belonging to trusted CA's. If the certificate presented by a peer through TLS negotiation matches the stored network identifier and has been signed by a trusted CA, then the authentication is considered valid.
- FIA_SOS.1: TOE supports several password policies that place constraints (see above) upon a user's selection of a password.
- FIA_UAU.2: The TOE offers no TSF-mediated functions until the user is authenticated.
- FIA_UAU.5: The TOE provides a password-based user authentication mechanism and also permits user authentication to occur using a third-party RADIUS or LDAP Server. The order in which these authentication providers are checked is determined by an administrator. Network peers are authenticated based upon the certificates that the TOE stores for the remote entities configured as syslog, RADIUS or LDAP servers.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified. Administrative users are identified using user identifiers.

7.4 Security management

The TOE defines the following administrative roles:

- admin – can perform all administrative commands
- switchAdmin – can perform administrative commands except for those related to user management and zoning configuration commands
- operator – can perform administrative commands that do not affect security settings
- zoneAdmin – can perform administrative commands that only affect zoning configuration
- fabricAdmin – can perform administrative commands except for those related to user management
- basicSwitchAdmin – can be used to monitor system activity
- SecurityAdmin – can perform security-related configuration including user management and security policy configuration
- root – can perform all administrative commands and access the OS; this user account is disabled during TOE configuration
- user – can view but not change configuration settings

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 SSHv2 or a terminal connected to a serial port. Both network-based and terminal-based interfaces provide equivalent management functionality. The Ethernet (i.e., SSHv2) and serial terminal interfaces support the same command-line interface commands after a session has been established.

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

- FMT_MSA.1: The ability to modify host bus adapters and storage devices zone membership is limited to users possessing the admin, zoneAdmin, fabricAdmin or root roles; the root role (account) is disabled during TOE configuration. Zone membership is defined by the default zone and zone configuration.
- FMT_MSA.3: By default, host bus adapters do not have access to storage devices. However, a device control policy can be used to specify alternate access permissions when new storage devices are connected to the TOE. The accounts with the admin role are allowed to specify device control policies.
- FMT_MTD.1(1): The ability to query, modify, delete, and assign administrative user, network peer and TOE security attributes is limited to users possessing one of the following administrative roles: admin, SecurityAdmin, root; the root role (account) is disabled during TOE configuration..
- FMT_MTD.1(2): Administrators can set their own passwords. The administrative roles admin, and Security Admin and root may set any account's password; the root role (account) is disabled during TOE configuration.
- FMT_MTD.1(3): Administrators can issue commands to import a certificate for use as the SSL Switch certificate or import certificates for use as root CA certificates.
- FMT_SMF.1: The TOE provides administrative interfaces to modify host bus adapters and storage device zone membership, to generate RSA Host Key pairs for use with SSH, to export SSH public keys and to import certificates for use with TLS as well as to set and reset administrator passwords.
- FMT_SMR.1: The TOE maintains administrative user roles.

7.5 TOE access

The IP Filter policy is a set of rules applied to the IP management interfaces as a packet filtering firewall. The IP Filter policy permits or denies traffic to go through the IP management interfaces according to the policy rules.

The TOE's password expiration policy forces expiration of a password after a configurable period of time, and is enforced across all user accounts. When a user's password expires, that user must change the password to complete the authentication process and open a new session. Password expiration does not disable or lock out the account.

The management channel is the communication established between the management workstation and the TOE. The TOE restricts user logon based upon the number of simultaneous login sessions allowed for each role when authenticated locally. The maximum number of simultaneous sessions for the admin role and all other roles is four[9] (4).

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

- FTA_MCS.1: The TOE restricts a user's concurrent sessions based upon the user's role using the limits stated in this section.
- FTA_TSE.1: The TOE restricts administrators from connecting based upon the source IP address and service (e.g., SSHv2) being used to establish the connection. The TOE also denies logon when authentication credentials have expired.

7.6 Trusted path

The TOE provides a trusted path for its remote administrative users accessing the TOE via the management ethernet ports provided on the Brocade Directors and Switches using the command line interface using SSHv2. Note that local

[9] When using RADIUS/LDAP for authentication the number of administrative sessions for each role is lifted, but due to the implementation, the TOE is still only able to support a total count of 32 sessions. This is a functional limitation, and not a security feature.

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.

The TOE uses TLSv1.2 as described below to protect the trusted channel between itself and external servers (i.e., syslog, LDAP and RADIUS).

The TOE implements the following protocols and cryptographic features meeting the identified standards and RFCs.[10]

Protocol or Cryptographic Algorithm	Standard or RFC
SSHv2	RFCs 4251, 4252 and 4253
TLS	TLSv1.2 (defined by RFC 5246).
HMAC	FIPS 198-1
SHA1	FIPS 180-4
HMAC-SHA1	FIPS 198-1
HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512	FIPS 180-2
RSA	FIPS PUB 186-4 and X.509v3

Table 7-2 Protocols / Cryptographic Algorithms and Standards / RFCs

The TOE utilizes certificates for TLS host authentication when TLSv1.2 is used to protect LDAP, RADIUS or Syslog communications. All certificates used by the TOE for this TLS host authentication must be imported into the TOE using the command-line interfaces. The lifetime of a key is determined solely by the frequency with which a site chooses to rekey. The private key is stored in persistent memory in the clear (the TOE will be located within controlled access facilities, which will prevent unauthorized physical access). The TOE uses the OpenSSL crypto engine to perform all cryptographic operations. There are also CLI commands to import an issuing CA's certificate rather than individual certificates for each server. The TOE clears keys associated with TLS and SSHv2 functions from internal memory when the key is no longer needed. The lifetime of a certificate is determined by the validity period for the certificate issued by the certifying authority. The validity period of the certificate used by the TOE for TLS is left to administrative discretion.

During TOE installation an RSA Host key pair is generated. The RSA Host key pair is composed of a public 2048 bit key and a private 2048 bit key. This key pair is used until the administrators choose to replace the key. Guidance instructs the administrator to only install certificates created entirely[11] with RSA 2048-bit key sizes and SHA256 hashing.

SSH and TLS session keys are used as long as the session remains open. Rekeying an SSH or TLS session requires closing one session and opening another by the administrator.

All Brocade switch products share the same underlying code base and implement a common set of cryptographic mechanisms to support trusted path. The algorithms available to support trusted path are HMAC-SHA1, AES128-CBC, AES256-CBC, TLS/AES128. The TOE zeroizes keys used in for the trusted path mechanism when the key is no longer needed.

The following table correlates algorithms, key lengths and standards for the algorithms used to support SSHv2 and TLS.

[10] Note that the TOE supports Elliptic-Curve cryptography; however, guidance instructs that it not be used in an evaluated configuration.
[11] That is, the same algorithm, hash and key size should be used for the certificate and for any CA key that signs the certificate.

Algorithm	Key Sizes	Standards	Certificate #
HMAC-SHA1	128 bit	FIPS 198-1	HMAC: 3328
HMAC-SHA-256	256 bit	FIPS 180-2	HMAC: 3328
HMAC-SHA-384	384bit	FIPS 180-2	HMAC: 3328
HMAC-SHA-512	512 bit	FIPS 180-2	HMAC:3328
AES128-CBC	128 bit	FIPS 197	AES: 5006
AES256-CBC	256 bit	FIPS 197	AES: 5006
AES-CTR	128, 256 bit	FIPS 197	AES: #C 195
AES-GCM	256 bit	FIPS 197	AES: #C 195
TLS/AES128	128 bit	FIPS 197	AES: 5006
RSA	2048 bit	FIPS 186-4	RSA: 2700

Table 7-3 Algorithms, Key Sizes, Standards and Certificate Numbers

The TOE supports SSHv2 with AES (CTR) 128 or 256 bit ciphers, and AES (CBC) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1, HMAC-SHA2-256, and HMAC-SHA2-512 and RSA using the diffie-hellman-group14-sha1 or diffie-hellman-group-exchange-sha256 key exchange methods.

NOTE: The TOE implementation of SSHv2 can be configured to utilize generation and exchange of session keys using either elliptic-curve, diffie-hellman-group14-sha1 or diffie-hellman-group-exchange-sha256 for key exchange. However, the evaluation guidance instructs the TOE be configured to accept and utilize only diffie-hellman-group14-sha1 or diffie-hellman-group-exchange-sha256.

The TOE provides TLSv1.2 and permits configuration using any of the following cipher suites:	
LDAP and SYSLOG only	TLS_RSA_WITH_AES_128_CBC_SHA (number 002F)
LDAP and SYSLOG only	TLS_RSA_WITH_AES_256_CBC_SHA (number 0035)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (number 003C)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (number 003D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (number 009F)
The TOE provides SSHv2 using the following cipher suites:	
	aes128-cbc
	aes256-cbc
	aes128-ctr
	aes256-ctr

Table 7-4 Cipher Suites supported for TLS and SSHv2

The application must be configured with the same issuing CA certificate in order to build a path and to verify the switch certificate's signature to establish the secure connection.

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

- FCS_CKM.1(1): The TOE generates new HMAC-SHA1, HMAC_SHA256, HMAC-SHA-512, and AES keys based upon the random numbers generated by FCS_RNG.1. These keys are used in support of TLSv1.2 and SSHv2.

- FCS_CKM.1(2): The TOE generates new RSA keys based upon ANSI X9.31 DRNG for keys shown in Table 7-3. The TOE generates candidate primes for RSA as per ANSI X9.31 for SSH host keys as defined within RFC4253. Brocade has obtained a CAVP algorithm for their implementation.
- FCS_CKM.2: The TOE distributes cryptographic keys in the context of a TLS handshake that is protected by RSA, and in the context of negotiation of SSH symmetric session keys using Diffie-Hellman key agreement. The TOE distribution methods meet the standards and key sizes shown in Table 6-3 SSH & TLS Key Distribution.
- FCS_CKM.4: The TOE clears keys associated with TLS and SSHv2 functions from internal memory when the key is no longer needed.
- FCS_COP.1(1): The TOE supports encryption, decryption, integrity verification, and peer authentication through SSHv2 and TLS using the ciphers identified in Table 7-4..
- FCS_COP.1(2): The TOE utilizes cryptographic operations for SSH user authentication as both a client and a server. The TOE also utilizes cryptographic operations for SSH host authentication of a remote peer. The TOE utilizes cryptographic operations during asymmetric authentication of a TLS server when establishing a TLS session. The authentication mechanisms, standards and key sizes used during these operations as defined in Table 6-4 SSH & TLS Payload Protection.
- FCS_COP.1(3): The TOE utilizes cryptographic authentication, meets standards and uses key sizes for the purposes shown by Table 6-5 SSH & TLS Mutual Authentication.
- FCS_COP.1(4): The TOE derives keys for SSH and TLS sessions using the algorithms and key sizes shown in Table 6-6 SSH and TLS Key Agreement while meeting the standards show in this table.
- FCS_RNG.1: A deterministic random number generator is implemented by the TSF. This RNG satisfies ANSI X9.31 AES 256 RNG and is used by OpenSSL for all random numbers needed for key generation supporting TLSv1.2. This same deterministic random number generator is used for all random numbers needed for key generation supporting SSHv2. .
- FTP_ITC.1: The TOE uses TLSv1.2 to provide protected communication pathways between the TOE and network peers that are providing Syslog, RADIUS and LDAP services. During TLS negotiation with a syslog server, the TOE authenticates itself to the syslog server by presenting a certificate. For TLS negotiation with a RADIUS or LDAP server, the TOE authenticates itself to the peer using mechanisms within the RADIUS and LDAP protocols.
- FTP_TRP.1: The TOE uses SSHv2 to provide a trusted path to its terminal-based management interfaces to protect the communication from disclosure and modification.

7.7 Protection of the TSF

The TOE maintains a security domain using appliance hardware. The use of a hardware appliance protects the TOE from external physical interference or tampering, including providing separate physical interfaces to separate hosts and storage devices. The TOE also relies upon being properly configured by administrators in accordance with the Common Criteria specific configuration guidance in FabricOS Version 8.2.0a2 BSI Configuration Guide.

The TOE does not encrypt data written to or read from storage devices by host bus adapters. The TOE relies instead on the environment to physically protect the network between the HBA and the TOE, and between the TOE and the storage device. 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 does encrypt commands sent from terminal applications by administrators using SSHv2. Further, TOE requires administrators to login after an SSHv2 connection has been established.

Administrators cannot bypass TOE functions because they are required to log in before the requested operation is allowed. When an administrator attempts to login using SSHv2, the RSA Host Key is used to authenticate the host and generate the diffie-hellman session keys that are presented to the calling application in the environment and is used to encrypt/decrypt traffic.

The application must be configured with the same issuing CA certificate in order to build a path and to verify the switch certificate's signature to establish the secure connection.

The TOE utilizes the reliable time stamp values obtained from the Brocade Directors and Switches hardware appliances.

7.8 Cryptographic Mechanism Documentation

Table listed below captures the cryptographic mechanisms (algorithms and communication protocols).

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authenticity	RSA signature verification for TLS RSAES-PKCS1-v1_5	[PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC5246] (TLS v1.2)	modulus length = 2048 bit	TLSv1.2 (RADIUS, LDAP, Syslog),	FCS_COP.1(3).1
2		RSA signature verification for SSH RSASSA-PKCS1-v1_5 (Authentication of SSH Host)	[PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC4252] (SSH-AUTH)	modulus length = 2048 bit	SSH	FCS_COP.1(3).1
3		Authentication based on user name and password for SSH	ch. 5 of [RFC4252] (SSH-AUTH)	Guess success probability ε ≤ 10-8	SSH	FCS_COP.1(3).1
4	Key agreement	Diffie-Hellman key agreement for SSH (Diffie-Hellman-group14-sha1)	DH [RFC4253] (SSH v2.0), [RFC3526] (MODP)	plength = 2048	SSH	FCS_CKM.2.1

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
5		Diffie-Hellman key agreement for SSH (diffie-hellman-group-exchange-sha256)	DH [RFC4419] (SSH v2.0)	plength = 2048	SSH	FCS_CKM.2.1
6		HMAC value generation for SSH (PRF) HMAC with SHA-1	[FIPS180-4] (SHA), [RFC4253] (SSH v2.0)	128 bit	SSH	FCS_COP.1(4).1 Pseudo-Random-Function (PRF) for key derivation diffie-hellman-group14-sha1
7		encrypted exchange of pre-master secret for TLS RSA-encryption RSAES-PKCS1-v1_5 (TLS_RSA)	[RFC5246] (TLS_RSA), [PKCS#1 v2.1]	2048-bit	TLSv1.2 (RADIUS, LDAP, syslog)	FCS_CKM.2.1
8		encrypted exchange of pre-master secret for TLS	DH ([HaC]) with group14 (TLS_DHE) from [RFC5246] (TLS v1.2)	2048-bit	TLSv1.2 (RADIUS, LDAP, syslog)	FCS_CKM.2.1
9		HMAC value generation for TLS (PRF) HMAC with SHA-256, SHA-384	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	256 bit and 384 bit	TLSv1.2 (RADIUS, LDAP, syslog)	FCS_COP.1(4).1 Pseudo-Random-Function (PRF) for key derivation tls_prf_sha256 tls_prf_sha384
10	Integrity	HMAC value generation and verification for SSH HMAC with SHA1, SHA-256, SHA-512	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC4253] (SSH v2.0), [RFC6668] (SHA-2 for SSH)	128, 256 bit and 512 bit	SSH	FCS_COP.1(2).1 hmac-sha1 hmac-sha2-256 hmac-sha2-512
11		HMAC value generation and verification for TLS HMAC with SHA-1, SHA-256,SHA-384	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	128 bit, 256 bit, and 384 bit	TLSv1.2 (RADIUS, LDAP, syslog)	FCS_COP.1(2).1

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
12	Confidentiality	symmetric encryption and decryption for SSH AES in CBC mode AES in CTR mode	[FIPS-197] (AES), [SP 800-38A] (CBC), [SP 800-38A] (CTR), [RFC4253] (SSH v2.0)	128 bit and 256 bit	SSH	FCS_COP.1(2).1 aes128-cbc aes256-cbc aes128-cttr aes256-ctr
13		symmetric encryption and decryption for TLS AES in CBC mode AES in GCM mode	[FIPS-197] (AES), [SP 800-38A] (CBC), [SP 800-38D] (GCM), [RFC5246] (TLS v1.2)	128 bit and 256 bit	TLSv1.2 (RADIUS, LDAP, syslog)	FCS_COP.1(2).1
14	Trusted Channel	SSHv2	[RFC4253]	-	SSH	FTP_ITC.1, FCS_COP.1(1).1 using the cipher suites aes128-cbc aes256-cbc aes128-cttr aes256-ctr
15		TLS v1.2[12]	[RFC5246]	-	TLSv1.2 (RADIUS, LDAP, Syslog),	FTP_ITC.1, FCS_COP.1(1).1 using the cipher suites TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
16	Cryptographic Primitive	Deterministic RNG DRG.2	AIS 20/31 RNG DRG.2	2048-bit	TLSv1.2 (RADIUS, LDAP, Syslog), SSH	FCS_RNG.1

Table 7-5 The cryptographic mechanisms (algorithms and communication protocols)

7.9 TOE Assurance Measures

The assurance measures provided by Brocade to meet the TOE Security Assurance Requirements defined within section 6.3 are identified in the following table.

[12] TLS v1.2 is using STARTTLS.

SAR	Assurance Measure
ADV_ARC.1	The architecture is described in the document entitled, "FabricOS running on Brocade Directors and Switches Security Architecture Document". This document describes the protection functionality provide by the TOE and the operational environment in which the TOE is intended to operate. In addition the initialization process for the TOE is described.
ADV_FSP.2	The functional specification, which described all TSFI, for the TOE is described in the document entitled, "FabricOS running on Brocade Directors and Switches Functional Specification". This document also traces functional specification to SFRs.
ADV_TDS.1	The TOE design specification is contained within the document entitled, "FabricOS running on Brocade Directors and Switches TOE Design Specification". This document describes the TOE structure.
AGD_OPE.1	A number of documents exist that provide operational guidance for the TOE system administrators. This includes guides that identify and explain the administration commands and parameters. These documents are enumerated in section 1.4.2.
AGD_PRE.1	A guide describing preparative procedures for configuring the TOE in a manner that is consistent with this Security Target is available. This preparative document is identified in section 1.4.2.
ALC_CMC.2 ALC_CMS.2 ALC_FLR.2	Brocade provided the document entitled, "Brocade Configuration Management Plan". This document identifies the TOE and describes the configuration management system used by Brocade to tracks hardware, software and document development. This document also contains a configuration item list. A chapter within this document is dedicated to bug tracking and resolution.
ALC_DEL.1	The TOE and the hardware platforms identified in this Security Target are delivered through sales channels controlled by Brocade. The TOE software is preinstalled upon the hardware.
ATE_COV.1	Brocade provided a test plan describing test cases that exercise the TOE security features described throughout this Security Target.
ATE_FUN.1	Testing has been performed upon the TOE as described in this Security Target. The tests and test results are documented and provided to the evaluation team.
ATE_IND.2	All of the required resources to perform the tests will be provided to the evaluation facility to perform testing. The evaluation facility will perform and document the tests they have created and performed as part of the evaluation technical report for testing. Due to the complexity of the test environment, testing will be performed using equipment at Brocade facilities.
AVA_VAN.2	Brocade provided equipment for testing and vulnerability analysis in support of the evaluation team's testing effort.

Table 7-6 The Security Assurance Requirements Measures

7.10 TOE Summary Specification Rationale

Each subsection in Section 7, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 7-7 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

	Security audit	User data protection	Identification and authentication	Security management	TOE access	Trusted path
FAU_GEN.1	X					
FCS_CKM.1 (1)						X
FCS_CKM.1 (2)						X
FCS_CKM.2						X
FCS_CKM.4						X
FCS_COP.1(1)						X
FCS_COP.1(2)						X
FCS_COP.1(3)						X
FCS_COP.1(4)						X
FCS_RNG.1						X
FCS_RNG.1(2)						X
FDP_ACC.1		X				
FDP_ACF.1		X				
FIA_AFL.1			X			
FIA_ATD.1(1)			X			
FIA_ATD.1(2)						X
FIA_SOS.1			X			
FIA_UAU.2			X			
FIA_UAU.5			X			
FIA_UID.2			X			
FMT_MSA.1				X		
FMT_MSA.3				X		
FMT_MTD.1				X		
FMT_MTD.1(2)				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FTA_MCS.1					X	
FTA_TSE.1					X	
FTP_ITC.1						X
FTP_TRP.1						X

Table 7-7 Security Functions vs. Requirements Mapping