Brocade Directors and Switches Security Target

Version Number	Publication Date
3.1	11/26/2013

Table of Contents

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 conformance claims, and the ST organization. The TOE is the Brocade Directors and Switches provided by Brocade Communications Systems, Inc. Brocade Directors and Switches are 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 Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by the TOE and the environment, and the organizational policy that the TOE must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and environment that supports the TOE, and details the assurance requirements.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

Security Target Title – Brocade Directors and Switches Security Target

Security Target Version – Version 3.1

Security Target Date – November 26, 2013

TOE Identification –

- Director Blade[1] Models: FC8-16, FC8-32, FC8-48, FC8-64, FC16-32, FC16-48, CP8, CR8, CR4S-8, CR16-4, CR16-8, FCOE10-24, FS8-18, FX8-24
- Director Models: DCX, DCX-4S, DCX 8510-4, DCX 8510-8
- Switch Appliance Models: 300, 5100, 5300, 6510, 6520, 7800, 8000, BES
- Embedded Blades[2]: 5410, 5424, 5450, 5460, 5470, 5480, 5431, 6547 and M6505
- Software: FabricOS version 7.2.0.a

Models FS8-18 and BES switch appliance support the user data encryption function.

TOE Guidance Documents –

- Brocade - FabricOS Administrator's Guide – Publication #53-1002920-01, 26-July 2013

[1] A blade refers to a purpose-built component that is installed in a Brocade director.
[2] An embedded blade is a Brocade switch in a blade form factor that may be installed in any blade server product.

- Brocade – FabricOS Command Reference – Publication #53-1002921-01, 26-July 2013
- Brocade – FabricOS Message Reference – Publication #53-1002929-01, 26-July 2013

TOE Developer – Brocade Communications Systems, Inc.

Evaluation Sponsor – Brocade Communications Systems, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 4, September 2012.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012.
  - Part 3 Conformant
  - Assurance Level: EAL-4 augmented with ALC_FLR.2

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.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.

1.4 Acronyms and Terminology

This section defines the acronyms and terms used throughout this document.

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

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

2. TOE Description

The Target of Evaluation (TOE) is the Brocade Directors and Switches hardware appliances running FabricOS version 7.2.0a. The various models of the TOE mentioned in Section 1.1 differ in performance, form factor and number of ports, but all run the same FabricOS version 7.2.0a software. The TOE is available in three form factors: a rack-mount Director chassis with a variable number of blades, a self-contained switch appliance device and embedded blades acting as a switch.

Director models are composed of blades of several types. A 'director blade model' is either a control blade (CP4 or CP8), a core switch blade (CR8 or CR4S-8, CR16-4, CR16-8), a port blade (FC4-16, FC4-32, FC4-48, FC8-16, FC8-32, FC8-48, FC8-64, FC16-32, FC16-48) or an application blade (FC4-16IP, FX8-24, FCOE10-24, FS8-18). Control blades contain the control plane for the chassis. A core switch blade contains the ASICs for switching between port blades. A port blades support various numbers of ports and speeds. Application blades provide additional capabilities such as FC over Ethernet or encryption. The DCX, DCX-4S, DCX 8510-4 and DCX 8510-8 require at least one control blade and one core blade to make the director operational.

Director Model	Blades
DCX	CP8, CR8, FC8-16, FC8-32, FC8-48, FC8-64, FX8-24, FCOE10-24, FS8-18
DCX-4S	CP8, CR4S-8, FC8-16, FC8-32, FC8-48, FC8-64, FC10-6, FX8-24, FCOE10-24, FS8-18
DCX 8510-4	CP8, CR16-4, FC8-64, FC16-32, FC16-48, FX8-24, FS8-18
DCX 8510-8	CP8, CR16-8, FC8-64, FC16-32, FC16-48, FX8-24, FS8-18

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

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

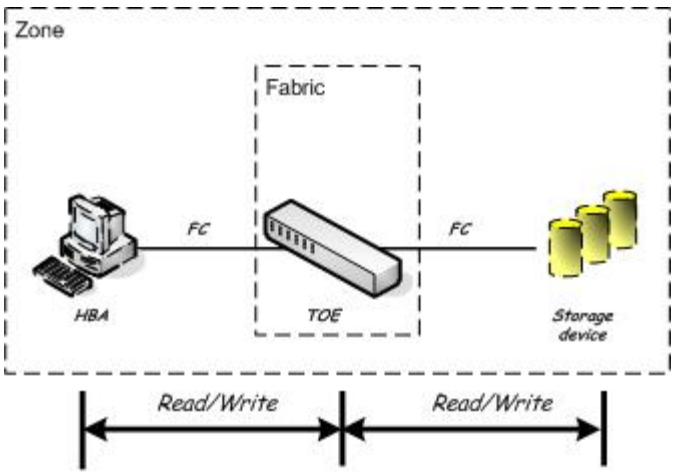


Figure 1: Host bus adapters can only access storage devices that are members of the same zone.

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

The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

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

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

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

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

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

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

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

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

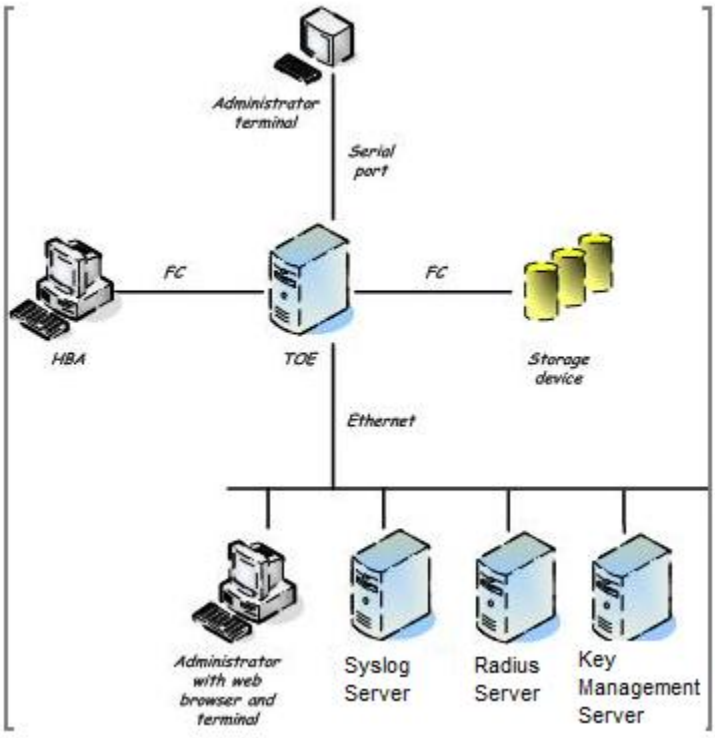


Figure 2: Administrators can access the TOE using a serial terminal or across a network. Audit records are sent to a syslog server.

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

2.2 TOE Architecture

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

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

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

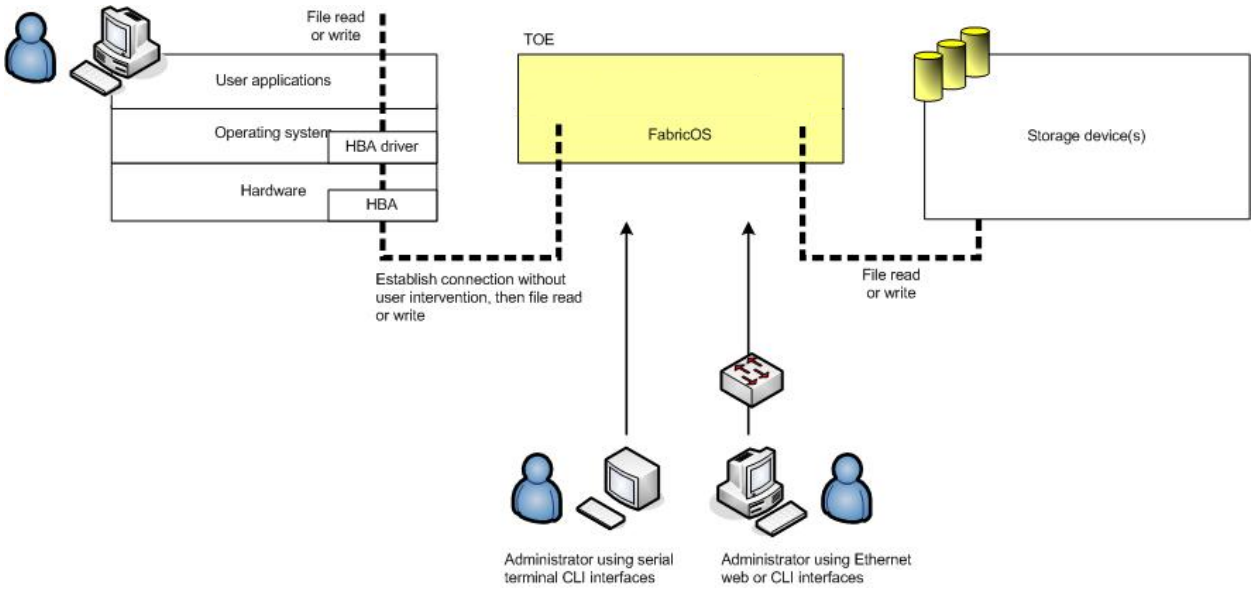


Figure 3: TOE and environment components.

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

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

2.2.1 Physical Boundaries

The components that make up the TOE are identified in Section 1.1 above.

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

any other components in the environment to provide security-related services. 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)
    - 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)
- RFC 2625 IP and ARP Over FC
- RFC 2837 Fabric Element MIB
- MIB-FA INCITS TR-32: 2003
- 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

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF

- Trusted path

There is no distinction between the product and the TOE.

2.2.2.1 Security audit

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

2.2.2.2 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[3] 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.

Some models of the TOE support encryption of user data for specified storage devices. A storage device configured to host encrypted data receives only encrypted data from the TOE and the TOE decrypts data received from the storage device. The encryption of the data exchanged between the TOE and an encrypted storage device is called "user data encryption". A CryptoTarget container is a configuration of "virtual devices" that is created for each storage device hosted on the TOE. A LUN is simply a number assigned to an addressable logical unit within a storage device. A CryptoTarget container identifies individual LUNs within a storage device as either encrypted or cleartext.

2.2.2.3 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.

2.2.2.4 Security management

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

2.2.2.5 Protection of the TSF

Protection of the TSF is provided primarily by virtue of the fact that the TOE is a hardware appliance that is physically protected in the environment. On most models, the TOE does not encrypt data written to or read from storage devices by host bus adapters. Encryption of this data is called "user data encryption" and is available only on a subset of the models of the TOE being evaluated (see 6.1.2.1 for more details). 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 SSH or HTTPS. Further, TOE requires administrators to login after a SSH or HTTPS connection has been established. The TOE provides a reliable time stamp for audit records.

---

[3] When more than one instance of the TOE is interconnected (i.e. installed and configured to work together), they are referred to collectively as a "SAN fabric" or simply a "fabric."

2.2.2.6 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.[4]

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

2.2.2.7 Trusted Path

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

2.3 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. See section 1.1 for the applicable guidance documentation included in the TOE.

[4] While the mechanism is built from a general purpose firewall capability of the underlying FabricOS, limitations on functionality provided to the end user limit its use to providing restrictions on administrative connectivity.

3. Security Environment

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-4) 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.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NETWORK	The environment will 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.

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 provide guidance and mechanisms to allow administrators to effectively manage the TOE and its security functions, to ensure that only authorized administrators are able to access such certain functionality, and to ensure that communication between the TOE and the administrator is protected.
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.NETWORK	The Environment will protect network communication to and from the TOE from unauthorized disclosure or modification.
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.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
FCS: Cryptographic Support	FCS_COP.1(1): Cryptographic Operation for Trusted Path
	FCS_COP.1(2): Cryptographic Operation for User Data Encryption
	FCS_CKM.1(1): Cryptographic key generation
	FCS_CKM.1(2): Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
FDP: User data protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	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(1): Management of security attributes
	FMT_MSA.1(2): Management of security attributes
	FMT_MSA.3(1): Static attribute initialization
	FMT_MSA.3(2): Static attribute initialization
	FMT_MTD.1(1): Management of TSF data
	FMT_MTD.1(2): Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps
FTA: TOE access	FTA_MCS.1: Basic limitation on multiple concurrent sessions
	FTA_TSE.1: TOE session establishment
FTP: Trusted Path	FTP_TRP.1: Trusted path

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**the events listed in the table below**].

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, 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

5.1.2 Cryptographic Support

5.1.2.1 Cryptographic operation for trusted path (FCS_COP.1(1))

FCS_COP.1.1(1)The TSF shall perform [**SSH and SSL trusted path operations**] in accordance with a specified cryptographic algorithm [**shown in column 1 of the table below**] and cryptographic key sizes [**shown in column 2 of the table below**] that meet the following: [**shown in column 3 of the table below**].

Algorithm	Key Sizes	Standards
HMAC-SHA1	160 bit	FIPS 198
3DES-CBC	168 bit	FIPS 46-3
AES128-CBC	128 bit	FIPS 197
AES192-CBC,	192 bit	FIPS 197
AES256-CBC	256 bit	FIPS 197
TLS/AES128	128 bit	FIPS 197

5.1.2.2 Cryptographic operation for user data encryption (FCS_COP.1(2))

FCS_COP.1.1(2) The TSF shall perform [**user data encryption**] in accordance with a specified cryptographic algorithm [**AES256**] and cryptographic key sizes [**256 bit**] that meet the following: [**FIPS 197**].

5.1.2.3 Cryptographic key generation (FCS_CKM.1(1))

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**pseudo random key generation**] and specified cryptographic key sizes [**128, 160, 168, 192 and 256 bits**] that meet the following: [**ANSI X9.31 DRNG**].

5.1.2.4 Cryptographic key generation (FCS_CKM.1(2))

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**pseudo random key generation**] and specified cryptographic key sizes [**256-bit**] that meet the following: [**ANSI X9.31 DRNG**].

5.1.2.5 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**].

5.1.3 User data protection (FDP)

5.1.3.1 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**

].

5.1.3.2 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:**

1. **storage device address;**
2. **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 **[no additional rules].**

5.1.3.3 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 **For models of the product supporting user data encryption,** the TSF shall enforce the [**encrypted user data SFP**] on [

a.) **Subjects: host bus adapters;**

b.) **Information: data frames read / written by a host bus adapter from / to a storage device; and**

c.) **Operation: block-read and block-write**

].

5.1.3.4 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 **For models of the product supporting user data encryption,** the TSF shall enforce the [**encrypted user data SFP**] based on the following types of subject and information security attributes: [

a.) **Subjects security attributes:**

1. **host bus adapter port number;**

b.) **Information security attributes:**

1. **storage device port number;**
2. **LUN and**
3. **storage device CryptoTarget container membership**

].

FDP_IFF.1.2 **For models of the product supporting user data encryption,** the TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a.) **the CryptoTarget container membership for the storage device includes the HBA port number and indicates the LUN should be encrypted, then the TOE will**

1. **encrypt blocks written from the HBA to the LUN on the storage device port; or**

2. **decrypt blocks read from the storage device port before sending the data frames to the HBA;**

b.) **the CryptoTarget container membership for the storage device includes the HBA port number and indicates the LUN should be encrypted, then the TOE will NOT**

1. **encrypt blocks written from the HBA to the LUN to the storage device port; or**
2. **decrypt blocks read from the storage device port before sending the data frames to the HBA;**

].

FDP_IFF.1.3 **For models of the product supporting user data encryption,** the TSF shall enforce the [**no additional SPF rules**].

FDP_IFF.1.4 **For models of the product supporting user data encryption,** the TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5 **For models of the product supporting user data encryption,** the TSF shall explicitly deny an information flow based on the following rules: [**none**].

5.1.4 Identification and authentication (FIA)

5.1.4.1 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**].

5.1.4.2 User attribute definition (FIA_ATD.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**

].

5.1.4.3 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**].

5.1.4.4 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-mediated actions on behalf of that user.

5.1.4.5 Multiple authentication mechanisms(FIA_UAU.5)

FIA_UAU.5.1 The TSF shall allow [**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 [**administrator configured order of authentication providers**].

5.1.4.6 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security management (FMT)

5.1.5.1 Management of security attributes (FMT_MSA.1(1))

FMT_MSA.1.1(1) The TSF shall enforce the [**SAN Fabric SFP**] to restrict the ability to [***[add or remove members of a zone***]] 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, factory**].

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

5.1.5.2 Management of security attributes (FMT_MSA.1(2))

FMT_MSA.1.1(2) **For models of the product supporting user data encryption,** the TSF shall enforce the [**encrypted user data SFP**] to restrict the ability to [***[manage]***] the security attributes [

- **host bus adapter port number;**
- **host bus adapter CryptoTarget container membership;**
- **LUN encryption status;**
- **storage device port number; and**
- **storage device CryptoTarget container membership**]

to [**users possessing one of the following administrative roles: Admin, SecurityAdmin, FabricAdmin, Root Factory**].

5.1.5.3 Static attribute initialization (FMT_MSA.3(1))

FMT_MSA.3.1(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(1) The TSF shall allow the [**no user**] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4 Static attribute initialization (FMT_MSA.3(2))

FMT_MSA.3.1(2) **For models of the product supporting user data encryption,** the TSF shall enforce the [**encrypted user data SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) **For models of the product supporting user data encryption,** the TSF shall allow the [**no user**] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.5 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**

]

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

5.1.5.6 Management of TSF data (FMT_MTD.1(2))

FMT_MTD.1.1(2) 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, factory**].

5.1.5.7 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:[

- **manage the attributes of the encrypted user data SFP**
- **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,**
- **specify the presumed source address and service permitted from which remote users connect to the TOEquery, modify, delete, and assign the user identity and role; and**

set and reset passwords of users possessing administrative roles.].

5.1.5.8 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**
- **factory**

].

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.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.7 TOE access (FTA)

5.1.7.1 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 [**4**] sessions per user.

5.1.7.2 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**].

5.1.8 Trusted Path (FTP)

5.1.8.1 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]***].

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL-4 components and ALC_FLR.2, as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

EAL-4 augmented was selected as the assurance level because the TOE is a commercial product whose users require a moderate to high level of independently assured security. ALC_FLR.2 was selected to exceed EAL-4 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 little attack potential. As such, EAL-4 is appropriate to provide the assurance necessary to counter the limited potential for attack.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.4: Complete functional specification
	ADV_IMP.1: Implementation representation of the TSF
	ADV_TDS.3: Basic modular design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.4: Production support, acceptance procedures and automation
	ALC_CMS.4: Problem tracking CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.2: Testing: security enforcing modules
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3: Focused vulnerability analysis

Table 2 EAL-4 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 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.

5.2.1.2 Complete functional specification (ADV_FSP.4)

ADV_FSP.4.1d The developer shall provide a functional specification.
ADV_FSP.4.2d The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.4.1c The functional specification shall completely represent the TSF.
ADV_FSP.4.2c The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.4.3c The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.4.4c The functional specification shall describe all actions associated with each TSFI.
ADV_FSP.4.5c The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.
ADV_FSP.4.6c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.4.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 Implementation representation of the TSF (ADV_IMP.1)

ADV_IMP.1.1d The developer shall make available the implementation representation for the entire TSF.
ADV_IMP.1.2d The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.
ADV_IMP.1.1c The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2c The implementation representation shall be in the form used by the development personnel.
ADV_IMP.1.3c The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.
ADV_IMP.1.1e The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

5.2.1.4 Basic modular design (ADV_TDS.3)

ADV_TDS.3.1d The developer shall provide the design of the TOE.
ADV_TDS.3.2d 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.3.1c The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.3.2c The design shall describe the TSF in terms of modules.
ADV_TDS.3.3c The design shall identify all subsystems of the TSF.
ADV_TDS.3.4c The design shall provide a description of each subsystem of the TSF.
ADV_TDS.3.5c The design shall provide a description of the interactions among all subsystems of the TSF.
ADV_TDS.3.6c The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.
ADV_TDS.3.7c The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.
ADV_TDS.3.8c The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.
ADV_TDS.3.9c The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.
ADV_TDS.3.10c The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

ADV_TDS.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

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

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

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

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

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

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

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

AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.

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

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Production support, acceptance procedures and automation (ALC_CMC.4)

ALC_CMC.4.1d The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2d The developer shall provide the CM documentation.

ALC_CMC.4.3d The developer shall use a CM system.

ALC_CMC.4.1c The TOE shall be labelled with its unique reference.

ALC_CMC.4.2c The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3c The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4c The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5c The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6c The CM documentation shall include a CM plan.
ALC_CMC.4.7c The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8c The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9c The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10c The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.
ALC_CMC.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 Problem tracking CM coverage (ALC_CMS.4)

ALC_CMS.4.1d The developer shall provide a configuration list for the TOE.
ALC_CMS.4.1c The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.
ALC_CMS.4.2c The configuration list shall uniquely identify the configuration items.
ALC_CMS.4.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document 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.

5.2.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.
ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.2.3.5 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall 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 documentation 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 corrected and the correction 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.

5.2.3.6 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1d The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2d The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1c The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2c The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

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

5.2.3.7 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1d The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2d The developer shall document the selected implementation-dependent options of each development tool.

ALC_TAT.1.1c Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2c The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3c The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

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

5.2.4 Tests (ATE)

5.2.4.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.

ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

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

5.2.4.2 Testing: security enforcing modules (ATE_DPT.2)

ATE_DPT.2.1d The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1c The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

ATE_DPT.2.2c The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3c The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

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

5.2.4.3 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.
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.

5.2.4.4 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 interfaces to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Focused vulnerability analysis (AVA_VAN.3)

AVA_VAN.3.1d The developer shall provide the TOE for testing.
AVA_VAN.3.1c The TOE shall be suitable for testing.
AVA_VAN.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.3.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.3.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.
AVA_VAN.3.4e 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 Enhanced-Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 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)
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

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

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

  Each audit record contains the following fields:

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

  For example:

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

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

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

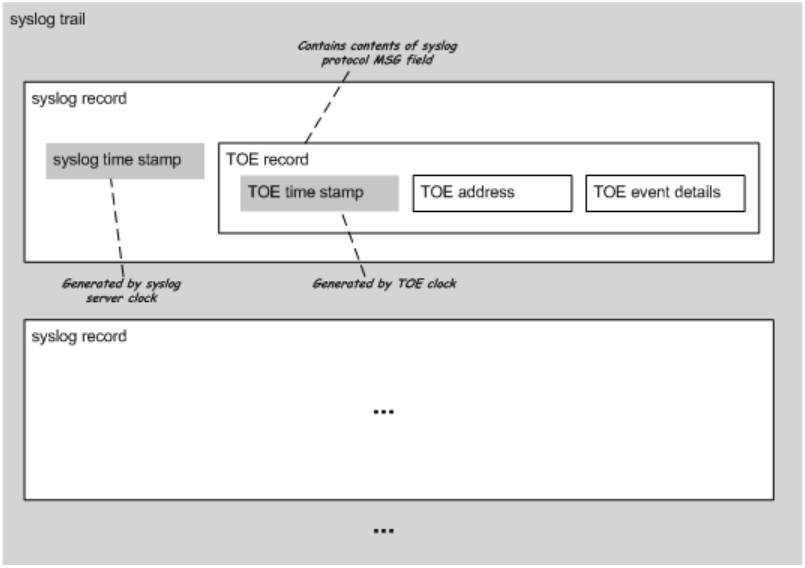


Figure 4: TOE and environment audit record components.

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

For example:

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

The 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.

6.1.2 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/FCIP-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.

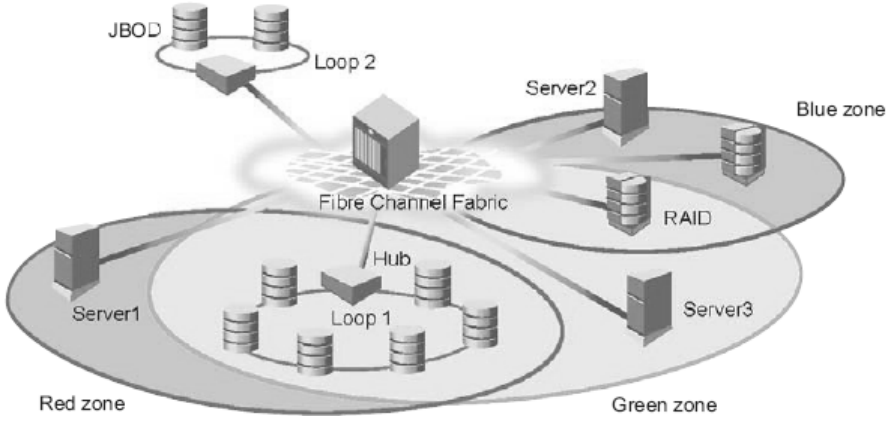
Zoning works by checking each frame before it is delivered to a zone member and discarding it if there is a zone mismatch. The TOE monitors HBA communications and blocks any frames that do not comply with the zone configuration. Zoning prevents users from even discovering the existence of unauthorized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



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/FCIP-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/FCIP 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/FCIP 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.

6.1.2.1 User Data Encryption

Some models of the TOE support encryption of user data for specified storage devices. Only the BES switch applicance and FS8-18 director blade models support the user data encryption feature. User data is encrypted using the AES256-XTS or AES256-GCM. The encryption component within the BES and FS8-18 products has received FIPS 140-2 Level 3 certification (certificate 1796).

A storage device configured to host encrypted data receives only encrypted data from the TOE and the TOE decrypts data received from the storage device.

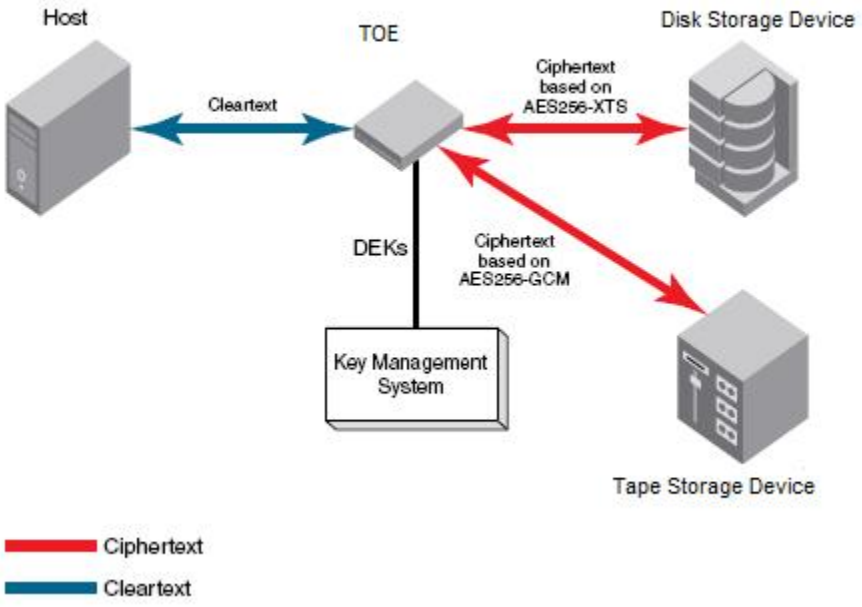


Figure 5: User Data Encryption

6.1.2.1.1 Key Management System

The user data encryption mechanism is transparent to the FC routing and zone enforcement mechanisms and is subject to all FC routing and zone enforcement configuration.

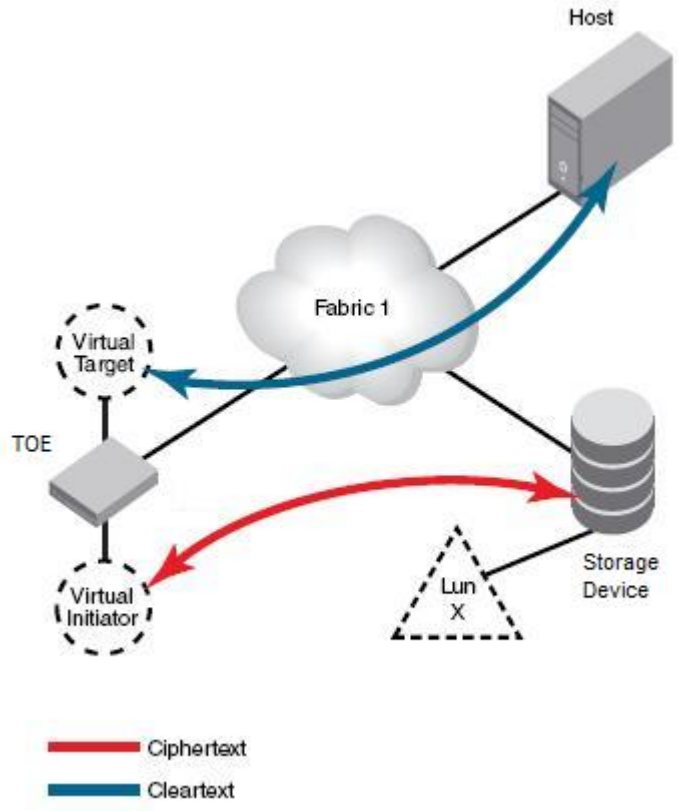


Figure 6: User Data Flow for User Data Encryption SFP

Data encryption keys (DEKs) are generated by the TOE. Data is encrypted and decrypted using the same DEK. A DEK must be preserved at least long enough to decrypt the ciphertext that it created. The length of time data is stored before it is retrieved can vary greatly, and some data may be stored for years or decades before it is accessed. Key management systems provide life cycle management for all DEKs created by the encryption engine. Key management systems are provided by third party vendors.

A DEK is created by an encryption engine, distributed, and stored in a key vault. The key is used to encrypt and decrypt data at least once, and possibly many times. The TOE zeroizes a DEK when the key is no longer needed.

6.1.2.1.2 CryptoTarget Container

A CryptoTarget container is a configuration of "virtual devices" that is created for each storage device hosted on the TOE. The CryptoTarget container holds the configuration infomation for a single storage device, including DEK, associated hosts (a.k.a., initiators) and storage device settings. A CryptoTarget container virtualizes the interfaces between the storage devices and hosts to provide a transparent encryption function.

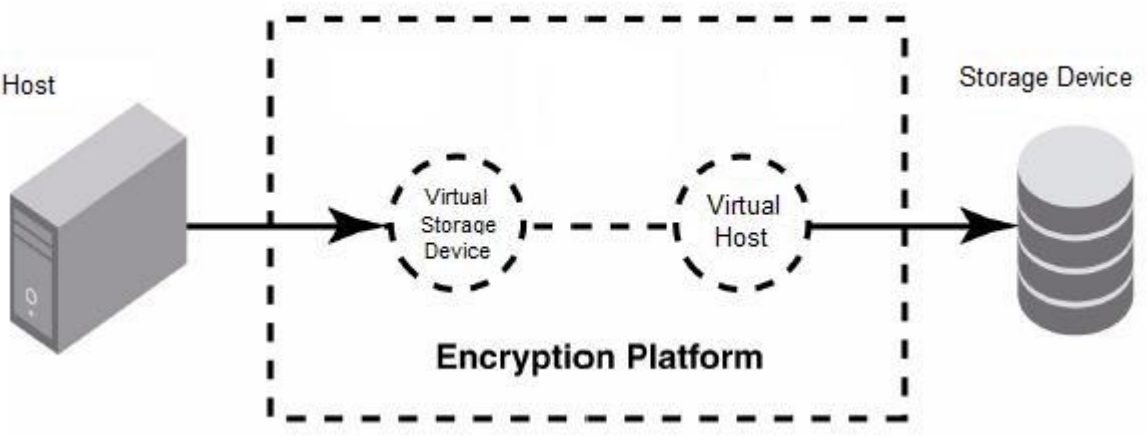


Figure 7: CryptoTarget Container

Within a storage device for which a CryptoTarget container has been defined, encryption policies must be configured for all LUNs that reside on the storage device. Encryption policies include specifying whether encryption will be applied to the LUN, whether existing data on the LUN should be encrypted and rekey policies.

The TOE will encrypt data sent to (and decrypt data received from) a specific LUN on a storage device when the HBA (identified by a port number) involved in the data transfer is an initiator in the CryptoTarget for the storage device. CryptoTarget membership determines the set of initiators associated with the CryptoTarget container. If an initiator is not a member in the CryptoTarget container for a given storage device, the data exchanged between that initiator and the storage device is not encrypted/decrypted.

CryptoTarget membership does not grant an HBA access to a storage device. An HBA must have access to a storage device in accordance with the SAN Fabric SFP.

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.
- FDP_IFC.1, FDP_IFF.1: Some models of the TOE provides the ability to encrypt user data to, or decrypt user data from, a storage device.
- FCS_COP.1(2): Some models of the TOE support encryption of user data using 256-bit AES that meets FIPS 197. The models of the TOE that support user data encryption have a FIPS 140-2 Level 3 certificate (1796).
- FCS_CKM.1(2): The TOE generates 256-bit keys for use with AES256-XTS or AES256-GCM in accordance with the TOE's FIPS 140-2 Level 3 certificate (1796).

6.1.3 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, Factory, Admin, FabricAdmin, SecurityAdmin, SwitchAdmin, BasicSwitchAdmin, ZoneAdmin, Operator and User. There are four pre-defined administrator accounts called "root", "factory", "admin" and "user", each of which is assigned the respective role of the same name, e.g. the "admin" account is assigned the Admin role. Note that neither the account called "user" nor any account that is assigned the User role, corresponds to a host bus adapter that is attempting to access a storage device, rather a User-role account corresponds to an administrative user that can view but not change configuration settings. The internal

FabricOS root account is disabled during TOE configuration, since it allows access to the operating system. This FabricOS 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: The TOE maintains security attributes for administrative users.
- 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 authentication mechanism and also permits authentication to occur using a third-party RADIUS or LDAP Server. The order in which these authentication providers is checked is determined by an administrator.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified. Administrative users are identified using user identifiers.

6.1.4 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
- factory – can perform all administrative commands

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

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

- FMT_MSA.1(1): The ability to modify host bus adapters and storage devices zone membership is limited to users possessing the admin, zoneAdmin, fabricAdmin, root, or factory role; the root role (account) is disabled during TOE configuration. Zone membership is defined by the default zone and zone configuration.
- FMT_MSA.1(2): The ability to modify the configuration of the user data encryption SFP defined between host bus adapters and storage devices is limited to users possessing the Admin, SecurityAdmin, FabricAdmin, Root and Factory roles.
- FMT_MSA.3(1): By default, host bus adapters do not have access to storage devices.
- FMT_MSA.3(2): By default, encryption is not performed on the transmission of user data between a host bus adapter and a storage device.
- 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, SecurityAdmin, root, factory; 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, root, and factory may set any account's password; the root role (account) is disabled during TOE configuration..
- FMT_SMF.1: The TOE provides administrative interfaces to manage the encrypted user data policy, to modify 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.

6.1.5 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.

For most models, the TOE does not encrypt data written to or read from storage devices by host bus adapters. For these models, 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. On those models providing user data encryption, data is protected from disclosure when it is written to or read from storage devices by host bus adapters. 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 SSH and HTTPS. Further, TOE requires administrators to login after a SSH or HTTPS 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 SSH, the SSL switch certificate is the one that is presented to the calling application in the environment. The SSL cipher list is configured as follows:

- ALL – all ciphers suites except the eNULL ciphers which must be explicitly enabled
- ADH – anonymous DH cipher suites.
- EXPORT56 – 56 bit export encryption algorithms. In OpenSSL 0.9.8d and later the set of 56 bit export ciphers is empty unless OpenSSL has been explicitly configured with support for experimental ciphers.
- RC4 – cipher suites using RC4.
- RSA cipher suites using RSA key exchange.
- HIGH – ``high" encryption cipher suites. This currently means those with key lengths larger than 128 bits, and some cipher suites with 128-bit keys.
- MEDIUM – "medium" encryption cipher suites, currently some of those using 128 bit encryption.
- LOW – "low" encryption cipher suites, currently those using 64 or 56 bit encryption algorithms but excluding export cipher suites.
- ssl2 – only include SSL v2 ciphers.

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 generates time stamps to support the auditing function.

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

- FPT_STM.1: The TOE generates time stamps for use in audit records.

6.1.6 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 is two (2), while all other roles have a maximum of four (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., SSH) being used to establish the connection. The TOE also denies logon when authentication credentials have expired.

6.1.7 Trusted Path

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

During TOE installation, a 1024-bit RSA key pair and then a corresponding PKCS#10 certificate request is generated. The TOE provides command-line interfaces to generate new keys and certificate requests. 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. After a key pair is generated, after a certificate request is generated using the new keys, the certificate request is sent to a CA in the environment. After the CA creates the certificate, the certificate is imported into the TOE using additional command-line interfaces. This certificate is called the "SSL switch certificate". There are also interfaces to import the issuing CA's certificate. The TOE also clears keys associated with SSL and SSH functions from internal memory when the key is no longer needed.

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, 3DES-CBC, AES128-CBC, AES192-CBC, AES256-CBC, TLS/AES128. Additionally, the DCX-4S, DCX, DCX 8510-4, DCX 8510-8, 6510, 7800 and 8000 products have received FIPS 140-2 Level 2 certification (1796), while the encryption component within the BES and FS8-18 products have received FIPS 140-2 Level 3 certification (pending). The TOE zeroizes keys used in for the trusted path mechanism and DEKs when the key is no longer needed.

In the evaluated configuration, the TOE must be configured to operate in "FIPS mode" to enforce various constraints including use of Approved crypto algorithms and disabling the root account. However, only a subset of the TOE models have also received FIPS 140-2 certification. The TOE models that have received FIPS 140-2 certification (pending) are: 6510, 7800, DCX, DCX-4S, DCX 8510-4, DCX 8510-8. All TOE models execute the same version of FOS and support the same "FIPS mode" behavior and must be configured to operate in "FIPS mode", regardless of whether the TOE model has received FIPS 140-2 certification.
The following table correlates algorithms, key lengths and standards for the algorithms used to support SSH and HTTPS.

Algorithm	Key Sizes	Standards	Certificate #
HMAC-SHA1	160 bit	FIPS 198	397, 933, 934
3DES-CBC	168 bit	FIPS 46-3	652, 1043
AES128-CBC	128 bit	FIPS 197	1796,1595, 1596
AES192-CBC	192 bit	FIPS 197	1796,1595, 1596
AES256-CBC	256 bit	FIPS 197	1796, 1595, 1596
TLS/AES128	128 bit	FIPS 197	1796, 1595, 1596

Table 3 Trusted Path Algorithms, Key Sizes, Standards and Certificate Numbers

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_COP.1(1): The TOE uses SSH and HTTPS to provide a trusted path for use by administrators. These operations are performed using the algorithms and bit sizes specified above.
- FCS_CKM.1(1): The TOE generates new RSA keys based upon ANSI X9.331 DRNG for keys shown in Table 3.
- FCS_CKM.4: The TOE clears a DEK and clears keys associated with SSL and SSH functions from internal memory when the key is no longer needed.
- FTP_TRP.1: The TOE uses SSH and HTTPS to provide a trusted path to its terminal-based management interfaces to protect the communication from disclosure and modification.

7. Protection Profile Claims

There is no Protection Profile claim.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

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

8.1.1 Security Objectives Rationale for the TOE and Environment

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

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GNEERATION	O.MANAGE	O.TOE_PROTECTION	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION	OE.CONFIG	OE.NETWORK	OE.PHYCAL
T.ACCOUNTABILITY			x							
T.ADMIN_ERROR		x		x						
T.MASQERADE						x	x			
T.TSF_COMPROMISE					x					
T.UNAUTH_ACCESS	x									
A.LOCATE										x
A.NETWORK									x	
A.NO_EVIL								x		

Table 4 Environment to Objective Correspondence

8.1.1.1 T.ACCOUNTABILITY

A user may not be held accountable for their actions.

This Threat is countered by ensuring that:

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

8.1.1.2 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.

8.1.1.3 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.

8.1.1.4 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.

8.1.1.5 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.

8.1.1.6 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.

8.1.1.7 A.NETWORK

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

8.1.1.8 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

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 5** indicates the requirements that effectively satisfy the individual objectives.

8.2.1 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_GNEERATION	O.MANAGE	O.TOE_PROTECTION	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION
FAU_GEN.1			x				
FCS_COP.1(1)					x		
FCS_COP.1(2)					x		
FCS_CKM.1(1)					x		
FCS_CKM.1(2)					x		
FCS_CKM.4					x		
FDP_ACC.1	x						
FDP_ACF.1	x						
FDP_IFC.1	x						
FDP_IFF.1	x						
FIA_AFL.1						x	
FIA_ATD.1						x	x
FIA_SOS.1						x	
FIA_UAU.2						x	
FIA_UAU.5						x	
FIA_UID.2							x
FMT_MSA.1(1)				x			
FMT_MSA.1(2)				x			

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GNEERATION	O.MANAGE	O.TOE_PROTECTION	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION
FMT_MSA.3 (1)				x			
FMT_MSA.3 (2)				x			
FMT_MTD.1(1)				x			
FMT_MTD.1(2)				x			
FMT_SMF.1				x			
FMT_SMR.1		x		x			
FPT_STM.1			x				
FTA_MCS.1				x			
FTA_TSE.1				x			
FTP_TRP.1				x			
ADV_ARC.1					x		

Table 5 Objective to Requirement Correspondence

8.2.1.1 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.
- FDP_IFC.1, FDP_IFF.1: For models of the product supporting user data encryption the TOE provides the ability to encrypt/decrypt block-read and block-write operations to connected storage devices that are initiated by the host bus adapter.

8.2.1.2 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.

8.2.1.3 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.
- FPT_STM.1: The TOE provides time stamps for its own use.

8.2.1.4 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(1): The ability to modify host bus adapters and storage devices zone membership is limited to users possessing the admin, zoneAdmin, fabricAdmin, root, or factory role.
- FMT_MSA.1(2): The ability to modify the configuration of the user data encryption SFP defined between host bus adapters and storage devices is limited to users possessing the Admin, SecurityAdmin and FabricAdmin, Root and Factory roles
- FMT_MSA.3(1): By default, host bus adapters do not have access to storage devices.
- FMT_MSA.3(2): By default, encryption is not performed on the transmission of user data between a host bus adapter and a storage device.
- 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, factory.
- FMT_MTD.1(2): Administrators can set their own passwords. The administrative roles admin, Security Admin, root and factory may set any account's password.
- 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.
- 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.

8.2.1.5 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(1): The TOE utilizes cryptography to as part of the trusted path mechanism that protects communications during administrative sessions.
- FCS_COP.1(2): In selected models, the TOE utilizes cryptography to protect user data transmitted to and stored on storage devices.
- FCS_CKM.1(1): The TOE generates keys for use with the trusted path mechanims.
- FCS_CKM.1(2): The TOE generates keys for use with the user data encryption mechanims.
- FCS_CKM.4: The TOE zeroizes keys used in for the trusted path mechanism when the key is no longer needed.
- ADV_ARC.1; requires that the TSF be able to protect itself from tampering and that the security mechanisms in the TSF cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF executables, TSF data or TSF-protected data.

8.2.1.6 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.
- 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.

8.2.1.7 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.

8.3 Security Assurance Requirements Rationale

EAL-4 augmented was selected as the assurance level because the TOE is a commercial product whose users require a moderate to high level of independently assured security. ALC_FLR.2 was selected to exceed EAL-4 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 little attack potential. As such, EAL-4 is appropriate to provide the assurance necessary to counter the basic potential for attack.

8.4 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-4 (i.e., ALC_FLR.2) that has been added for this product has been included in this analysis.

Only FCS_COP.1(2) has unsatisfied dependencies which are justified below this table.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FCS_COP.1(1)	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]; and FCS_CKM.4	FCS_CKM.1(1), and FCS_CKM.4
FCS_COP.1(2)	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]; and FCS_CKM.4	none
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1 and FCS_CKM.4	FCS_COP.1(1) and FCS_CKM.4
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1 and FCS_CKM.4	FCS_COP.1(2) and FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1	FCS_CKM.1
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(1)
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MSA.3(2)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2

ST Requirement	CC Dependencies	ST Dependencies
FIA_ATD.1	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 (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.2
FMT_MSA.1(2)	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.1
FMT_MSA.3 (1)	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MSA.3 (2)	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	none	none
FTA_MCS.1	FIA_UID.1	FIA_UID.2
FTA_TSE.1	none	none
FTP_TRP.1	none	none
ALC_FLR.2	none	none

Table 6 CC Dependencies vs. ST Dependencies

8.5 Extended Requirements Rationale

There are no extended requirements.

8.6 TOE Summary Specification Rationale

Each subsection in Section 6, 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 6 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE Access	Trusted path
FAU_GEN.1	x						
FCS_COP.1(1)							x
FCS_COP.1(2)		x					
FCS_CKM.1(1)							x
FCS_CKM.1(2)		x					
FCS_CKM.4							x
FDP_ACC.1		x					
FDP_ACF.1		x					
FDP_IFC.1		x					
FDP_IFF.1		x					
FIA_AFL.1			x				
FIA_ATD.1			x				
FIA_SOS.1			x				
FIA_UAU.2			x				
FIA_UAU.5			x				
FIA_UID.2			x				
FMT_MSA.1(1)				x			
FMT_MSA.1(2)				x			
FMT_MSA.3(1)				x			
FMT_MSA.3(1)				x			
FMT_MTD.1				x			
FMT_SMF.1				x			
FMT_SMR.1				x			
FPT_STM.1					x		
FTA_MCS.1						x	
FTA_TSE.1						x	
FTP_TRP.1							x

Table 7 Security Functions vs. Requirements Mapping

8.7 PP Claims Rationale

See Section 7, Protection Profile Claims.