Cisco MDS 9000 Family SAN-OS Release 3.2(2c)

August 2008
Version: 3.0

Table of Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

List of Tables

List of Figures

Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.2 of the Common Criteria [CC]. Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional requirements: The allowable operations defined in paragraph 4.4.1.3.4 of Part 1 of the CC [CC1] are refinement, selection, assignment and iteration.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment value(s)] and a red text color.
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text.
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined italicized text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the CC an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

All operations described above are used in this Security Target. Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

References

The following documentation was used to prepare this ST:

[CC]	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
[CC1]	Common Criteria Part 1: Introduction and General Model, Version 2.2, CCIB-2004-01-001, January 2004.
[CC2]	Common Criteria Part 2: Security Functional Requirements, Version 2.2, CCIB-2004-01-002, January 2004.
[CC3]	Common Criteria Part 3: Security Assurance Requirements, Version 2.2, CCIB-2004-01-003, January 2004.
[CEM]	Common Evaluation Methodology Part 2: Evaluation Methodology, Version 2.2, CCIMB-2004-01-004, January 2004.

Introduction

This introductory section presents *security target (ST)* identification information and an overview of the ST. A statement of Common Criteria conformance is also provided.

Acronyms

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
CC	Common Criteria
CLI	Command Line Interface
CUP	Control Unit Port
DH-CHAP	Diffie Hellmann – Challenge Handshake Authentication Protocol
EAL	Evaluation Assurance Level
EMS	Element Management System
FCIP	Fibre Channel over IP
FCP	Fibre Channel Protocol
FC-SP	Fibre Channel – Security Protocol
FICON	IBM Fiber Connection
GUI	Graphical user Interface
IP	Internet Protocol
IPFC	IP over Fibre Channel
iSCSI	Small Computer System Interface over IP
IT	Information Technology
LUN	Logical Unit Number
OOB	Out of Band
PP	Protection Profile
RADIUS	Remote Access Dial-In User Service
RBAC	Role Based Access Control
SAN	Storage Area Network
SF	Security Function
SFP	Security Function Policy
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

VSAN	Virtual Storage Area Network
WWN	World Wide Name

ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets an **Evaluation Assurance Level (EAL) 3** level of assurance for the TOE augmented with the assurance component ALC_FLR.1.

ST Title:	Cisco MDS 9000 Family SAN-OS Release 3.2(2c) Security Target
TOE Identification:	Cisco MDS 9000 Family with SAN-OS Release 3.2(2c). Specific hardware models include: • Cisco MDS 9509 Multilayer Director (DS-C9509) • Cisco MDS 9506 Multilayer Director (DS-C9506) • Cisco MDS 9513 Multilayer Director (DS-C9513) • Cisco MDS 9216 Multilayer Fabric Switch (DS-C9216-K9) • Cisco MDS 9216A Multilayer Fabric Switch (DS-C9216A-K9) • Cisco MDS 9216i Multilayer Fabric Switch (DS-C9216i-K9) • Cisco MDS 9140 Multilayer Fabric Switch (DS-C9140-K9) • Cisco MDS 9120 Multilayer Fabric Switch (DS-C9120-K9) The following expansion modules may be used in models with expansion slots: • Cisco MDS 9500 Series Supervisor Module (DS-X9530) • Cisco MDS 9500 Series Supervisor 2 Module (DS-X9530-SF2-K9) • Cisco MDS 9000 Family Multiprotocol Services Module (DS-X9302-14K9) • Cisco MDS 9000 Family Storage Services Module (DS-X9032-SSM) • Cisco MDS 9000 IP Storage Services Modules (DS-X9304-SMIP, DS-X9308-SMIP) • Cisco MDS 9000 Family Fibre Channel Switching Modules (DS-X9016, DS-X9032)
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256 (including CCIMB final interpretations as of 30 July 2004).
ST Evaluation:	National Information Assurance Partnership
Author(s):	Cisco Systems, Inc.
Keywords:	Cisco MDS 9000, SAN, VSAN

Security Target Overview

The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches targets enterprise and service provider storage network environments. The Cisco MDS 9000 Family products also target heterogeneous storage area networks where the overall storage environment consists of multiple vendors' products. In those environments, the Cisco MDS 9000 Family products can serve as a centralized system to provide interconnection and advanced services.

The Cisco MDS 9000 Family of switches consists of the Cisco MDS 9500 Series of Multilayer Directors, the Cisco MDS 9216 Multilayer Fabric Switch and the Cisco MDS 9100 Series of fixed configuration fabric switches.

Figure 1 The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches

Common Criteria Conformance

The TOE is conformant with Parts 2 and 3 of the CC, version 2.2 [CC2, CC3]. This includes all CCIMB interpretations finalized on or before 30 January 2004.

TOE Description

The Target of Evaluation (TOE) is a Storage Area Network (SAN) solution consisting of the SAN-OS operating system running on the Cisco MDS 9000 family of Multilayer Directors and Fabric Switches. The SAN-OS software is the same base system software used throughout the entire Cisco MDS 9000 product line. The Cisco MDS 9000 family of switches provides the infrastructure that ties together file servers and back end storage.

A Storage Area Network (SAN) is a high-speed network of shared storage devices. A storage device is a machine that contains nothing but a disk or disks for storing data. A SAN's architecture works in a way that makes all storage devices available to all servers on a LAN or WAN. As more storage devices are added to a SAN, they too will be accessible from any server in the larger network. A SAN can provide a number of different storage components, including mainframe disk, tape and RAID.

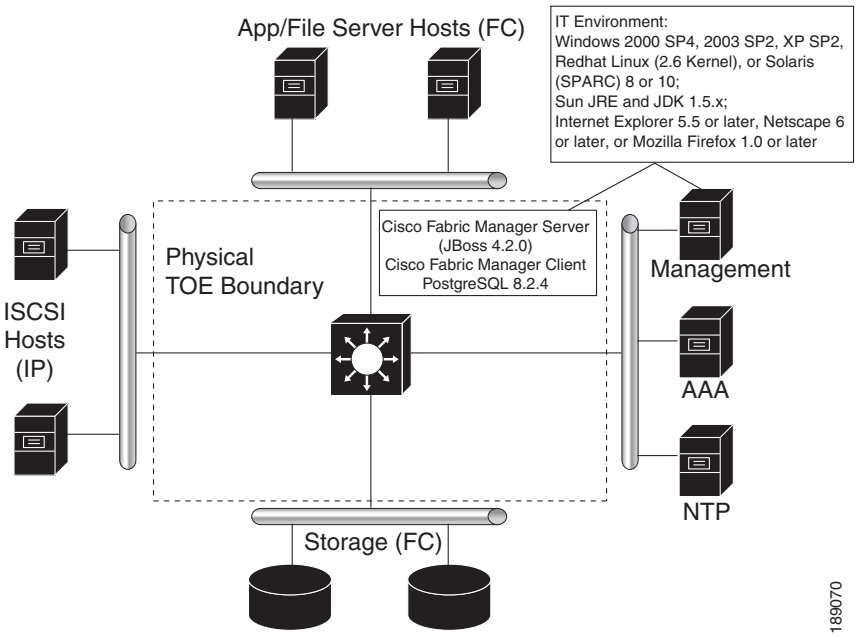
The Cisco SAN-OS supports a collection of SAN specific protocols for communication between the users and subjects: the Fibre Channel Protocol (FCP) and Small Computer System Interface over IP (iSCSI)).

It is important to note that the use of iSCSI is not available using the Cisco 9100 family of fabric switches, and may only be achieved using a TOE configuration which includes the IP Storage Services or the Multiprotocol Services Modules.

Physical Scope

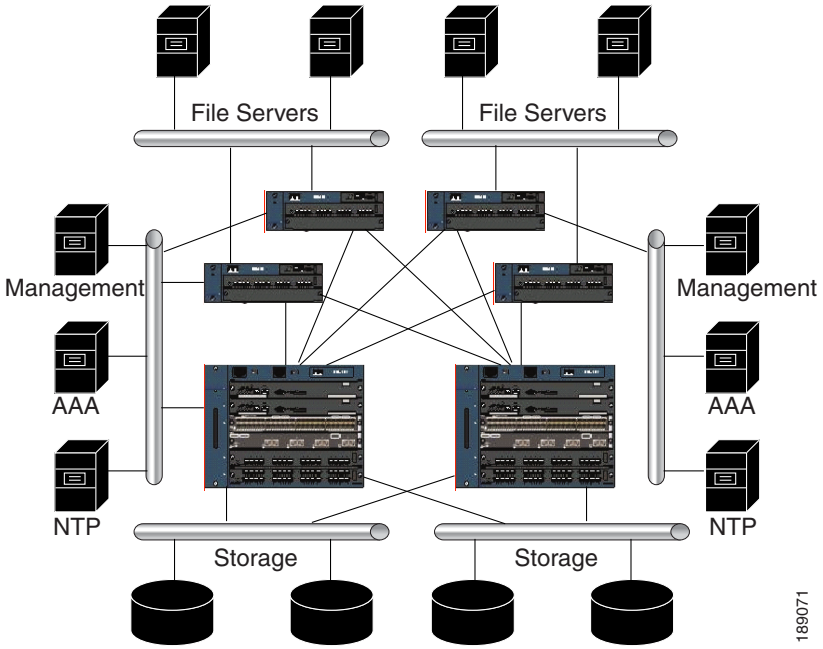
A functioning SAN requires three components for operation: switches, storage and servers. The physical boundary of the TOE is limited to the devices that provide the fabric and the devices that assist in administering the switches. The servers that access the data and the storage devices (disk, tape) and the iSCSI hosts are considered a portion of the environment. The IP network is a protected network that provides the IP communications for the iSCSI protocol. Other components in the TOE environment include those devices on the Management LAN. The Management LAN is a protected network that provides NTP and AAA services as well as access to the TOEs management functions via a Management Workstation. Communications between the servers that access the data and the storage devices is considered in-band. Communications between the Management LAN and the switch fabric is considered out-of-band. There is an option for enabling of in-band management, where a VSAN that is used to communicate management info is created, but this is excluded in the evaluated configuration.

Figure 2 Physical Scope of the TOE



It should be noted that the above diagram allows for multiple File Servers and, storage devices and Cisco MDS 9000 Series Multilayer Switches. The reason for this is to allow for redundancy and scalability that may be required in certain environments. The minimal TOE configuration is considered to be a single file server, storage device and Cisco MDS 9000 Fabric switch, configured as shown in Figure 2. Figure 3 shows an example configuration which utilizes redundancy, such that there is no single point of failure in the SAN solution. The use of redundancy is within the scope of evaluation, but is not considered a security function. The connection of TOE instances to a Management LAN has been left of this diagram for complexity reasons.

Figure 3 Example use of TOE instances in a redundancy configuration



The above figure shows the use of several interconnected Cisco MDS 9000 family fabric switches. Due to the nature of the traffic being handled by these switches, they may be sequentially interconnected in order to allow for data flows between the file servers and the storage devices. This functionality has no impact on the secure function of the TOE providing that all TOE instances have been configured correctly.

For administration the TOE provides the Cisco Fabric Manager, including the Fabric Manager client, server, and Device Manager. These components are installed on the Management Workstation.

The TOE does not allow any users other then administrative users.

Table 1 Physical Scope of the TOE

Physical TOE Components	Hardware/Software Component Description
Software	SAN-OS Maintenance Release 3.2(2c), including Fabric Manager for SANOS 3.2(2c). Fabric Manager 3.2(2c) includes: Fabric Manager Server Fabric Manager Client Performance Manager Device Manager Fabric Manager Web Services Fabric Manager also relies on the PostgreSQL, version 8.2.4 DBMS package, that is included on the Fabric Manager distribution CD and is within the TOE boundary. Fabric Manager also uses JBoss 4.2.0.

Table 1 Physical Scope of the TOE

Physical TOE Components	Hardware/Software Component Description
MDS 9509 Multilayer Director	Cisco MDS 9509 multilayer directors contain two slots for supervisor modules and 7 slots for switching or services modules providing up to 224 ports (32 ports x 7 slots).
MDS 9506 Multilayer Director	Cisco MDS 9506 multilayer directors contain two slots for supervisor modules and 4 slots for switching or services modules providing up to 128 ports (32 ports x 4 slots).
MDS 9513 Multilayer Director	Cisco MDS 9513 multilayer directors contain two slots for supervisor modules and 11 slot s for switching or services modules providing up to 352 ports (32 ports x 11 slots).
MDS 9216 Multilayer Fabric Switch	Cisco MDS 9216 multilayer fabric switches contain one fixed integrated supervisor module with 16 Fibre Channel ports and an expansion slot which can support up to 32 additional ports (for a total of 48 ports).
MDS 9216A Multilayer Fabric Switch	Cisco MDS 9216A multilayer fabric switches contain one fixed integrated supervisor module with 16 Fibre Channel ports and an expansion slot which can support up to 48 additional ports (for a total of 64 ports).
MDS 9216i Multilayer Fabric Switch	Cisco MDS 9216i multilayer fabric switches support 14 2-Gbps Fibre Channel interfaces for high-performance storage area network (SAN) connectivity and Small Computer System Interface over IP (iSCSI) storage services and an expansion slot which can support up to 48 additional ports (for a total of 62 ports).
MDS 9140 Multilayer Fabric Switch	Cisco MDS 9140 multilayer switches contains 40 ports (8 full rate ports, 32 host-optimized ports)
MDS 9120 Multilayer Fabric Switch	Cisco MDS 9120 multilayer switches contains 20 ports (4 full rate ports, 16 host-optimized ports)
Ethernet, Fibre Channel, Serial Port	These components make up the physical connectivity layer to the TOE. The Ethernet and Fibre Channel interfaces are used to connect to the switch fabric or to server / device components. The serial port is used for local administrative access.
Cisco MDS 9500 Series Supervisor Module	The Cisco MDS 9500 Series Supervisor Module is designed to allow for non-disruptive software upgrades and hardware redundancy for maximum availability and performance. This module may be used with the MDS 9509 and 9506 Multilayer Directors.
Cisco MDS 9500 Series Supervisor 2 Module	The Cisco MDS 9500 Series Supervisor 2 Module is designed to allow for non-disruptive software upgrades and hardware redundancy for maximum availability and performance. This module may be used with any of the 9500 Multilayer Directors.

Table 1 Physical Scope of the TOE

Physical TOE Components	Hardware/Software Component Description
Cisco MDS 9000 Family Multiprotocol Services Module	This Module offers fourteen 2-Gbps Fibre Channel interfaces and two Gigabit Ethernet ports. The module enables Small Computer System Interface over IP (iSCSI) for Ethernet attached servers without sacrificing Fibre Channel port density. This module may be used with the MDS 9509 and 9506 Multilayer Directors, as well as the MDS 9216 Multilayer Fabric Switch.
Cisco MDS 9000 Family Storage Services Module	This module provides the same features as the Cisco MDS 9000 Family Fibre Channel Switching Module, but additionally has the capability to perform Fibre Channel Write Acceleration and Network-Accelerated Serverless Backup. This module may be used with the MDS 9509 and 9506 Multilayer Directors, as well as the MDS 9216 Multilayer Fabric Switch, but the Fibre Channel Write Acceleration and Network-Accelerated Serverless Backup features are not able to be used in the evaluated configuration as they require a separate boot image to be installed on the SSM card.
Cisco MDS 9000 IP Storage Services Modules	A module that provides four or eight gigabit Ethernet ports for use with iSCSI. This module expands the number of ethernet ports that may be utilised by the switch. This module may be used with the MDS 9509 and 9506 Multilayer Directors, as well as the MDS 9216 Multilayer Fabric Switch.
Cisco MDS 9000 Family Fibre Channel Switching Modules	A basic 16 or 32 port fiber channel switching module. This module expands the number of fiber channel ports that may be utilised by the switch. This module may be used with the MDS 9509 and 9506 Multilayer Directors, as well as the MDS 9216 Multilayer Fabric Switch.

Logical Scope

The logical boundary is drawn around the hardware and software that make up the TOE. The TOE has many functions and features that enhance its ability as a SAN product (such as failover/redundancy), but do not affect security. These features of the TOE exist, but are not relied upon to enforce any security policy or function. The features documented below are specifically relied upon by the TOE.

The TOE provides a number of security-related services. This includes traffic and device isolation obtained through the deployment of VSANs, switch and host authentication, role-based access control, port access control and fabric binding, device access control through zoning, secure management session authentication through SSHv2 and SNMPv3, secure management access via IP-based access control lists, security audit, and support for remote authentication, authorization and accounting (AAA) services (i.e. RADIUS and TACACS+).

Identification & Authentication

Switch and Host Authentication

The TOE allows fabric-wide authentication from one switch to another switch or from a switch to a host. These switch and host authentications are performed locally within each switch. Authentication between devices is performed using the Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP). Fibre Channel-level authentication allows only authorized devices to be added to a fabric, thus preventing unauthorized devices from accessing the switch.

Host authentication may also be performed for iSCSI hosts that request access to storage within the SAN. It is important to note that the use of iSCSI may only be achieved using a TOE configuration which includes the IP Storage Services Module or the Multiprotocol Services Module. Each switch uses its internal authentication mechanisms or RADIUS/TACACS+ can be leveraged for centralized switch and host authentication via the client modules in the SAN-OS software.

Administrative Control

The network-admin (sw) role has the ability to specify the switch shell timeout (all sessions) and switch session timeout (current session). The network-admin (sw) role also has the ability to view and monitor the list of switch logged in users, log off a user, and specify an account timeout period upon creation of the user's account. The network-admin(FM) role and network-admin(sw) role depending on FM authentication mode selected, as shown in the table in SM.ROLE – Security Management Roles have the ability to view and monitor the list of logged in Fabric Manager users and log off a user. The network-admin (FM) also has the responsibility during installation of the TOE for setting the initial communication parameters that will be used to establish connections with the Fabric Manager database.

Authenticated management user sessions

Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE. Public key-based authentication is supported by the TOE through SSH.

RADIUS / TACACS+ Support

The RADIUS / TACACS+ services are supported by the TOE through a component (client module) of SAN-OS. Through this module, client security management can be centralized including the specification of the RADIUS or TACACS+ pre-shared keys, server time-out intervals, and the display of server details. AAA event messages generated by the client module are recorded in the audit log and stored on the switch's local disk. The Fabric Manager also interfaces with RADIUS/TACACS+ services for authentication purposes when RADIUS/ TACACS+ is selected as the FM authentication mode. These settings are configurable through the Fabric Manager Client and Fabric Manager Web Client.

Switch Security

Port Security

The TOE can bind entities to fiber channel ports using the port, node or switch World Wide Name (an entity may be a host(server), target(storage device) or switch), thus preventing unauthorized access to a switch port.

Fabric Binding

Fabric binding extends port security by binding inter-switch links within the SAN, thus preventing unauthorized switches from joining the fabric or disrupting current fabric operations. Fabric binding policies are enforced based on identities authenticated by DHCHAP.

IP-based Access Control Lists

IP-ACLs restrict IP-related Cisco MDS 9000 out-of-band (i.e. Ethernet based) management traffic based on IP addresses (Layer 3 and Layer 4 information). An IP filter contains rules for matching an IP packet based on the protocol, address, and port. IP-ACLs are configurable on the management interface.

VSAN (Traffic Isolation)

Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between user groups. This ensures the confidentiality of data traversing the VSAN from users and devices belonging to other VSANs. It should be noted that devices, such as file servers and tape storage devices are not part of the TOE but part of the TOE environment and may be configured to participate in a VSAN. Each network interface of a device connected to the TOE may only participate in a single VSAN.

Virtual SAN (VSAN) technology partitions a single physical SAN into multiple VSANs. VSAN capabilities allow the Cisco SAN-OS to logically divide a large physical fabric into separate isolated environments to improve Fibre Channel SAN scalability, availability, manageability, and network security. For FICON, VSANs ensure that there is true hardware-based separation of FICON and open systems.-11

Each VSAN is a logically and functionally separate SAN with its own set of Fibre Channel fabric services. This partitioning of fabric services greatly reduces network instability by containing fabric reconfigurations and error conditions within an individual VSAN. The strict traffic segregation provided by VSANs helps ensure that the control and data traffic of a given VSAN is confined within its own domain, increasing SAN security.

Data traffic can be transported between specific hosts and targets on different VSANs using Inter-VSAN Routing without merging VSANs into a single logical fabric. Fibre Channel control traffic does not flow between VSANs, nor can initiators access any resources aside from the ones designated with Inter-VSAN Routing. This enables the TOE to share resources like tape libraries while reducing the risk of compromise from other VSAN users.

Access Control

Role Based Access Control

Role-based authorization limits access to management operations by assigning users to roles. This kind of authorization restricts an administrator to management operations based on the roles to which they have been added. When an administrator executes a command, performs command completion, obtains context sensitive help, or attempts to access a privileged web page, the switch and Fabric Manager software allow the operation to progress if the administrator has permission to access that command or page. On the switch each role can contain multiple users and each user can be a member of multiple roles. Up to 64 different switch user-defined roles can be created, each role may have zero or more members.

The TOE has default roles: network-admin (sw), network-operator (sw), network-admin (FM), and network-operator (FM). Only the network-admin (sw) has write access to the security functions on the switch. The network-admin (sw) role has write access to the configuration of the switch. The

network-admin(FM) role and network-admin(sw) role depending on FM authentication mode selected, as shown in the table in Security Management (SM).1 have write acces to the configuration of the Fabric Manager. The network-admin(sw) and network-admin(FM) roles are able to create FM User roles. The network-admin(sw) role are able to create switch user roles.

Note For a complete description of TOE roles and privileges see Table 13.

Zoning

Zoning provides a means of restricting visibility and connectivity between devices connected to a common Fibre Channel SAN. To avoid any compromise of critical data within the SAN, zoning allows the user to overlay a security map dictating which devices, namely hosts (servers), can see which targets (storage devices) thereby reducing the risk of data loss.

Zoning enables the switch administrator to set up access control between storage devices or user groups.

Zoning is enforced by examining the source-destination ID field (which can be a WWN, IP address, Fibre Channel Identifier, etc). Logical Unit Number (LUN) zoning ensures that LUNs are accessible only by specific hosts.

Zoning also was not designed to address availability or scalability of a Fibre Channel infrastructure. Therefore while zoning provides a necessary service within a fabric, the use of VSANs along with zoning provides an optimal solution.

Audit

The accounting and system message logs record all switch user actions such as login and logout, and configuration commands executed by the user. The accounting and system message logs are stored on the local disk of the switch for later review and analysis. Unauthorized access to ports on the TOE and AAA events generated by the TOEs internal authentication server are also recorded in the accounting and system message logs. The Fabric Manager Server and Web Server logs are a separate component, which can be viewed from the Fabric Manager Web Client while the Accounting and System Message Logs exist on the MDS switches. These logs record login/logout events to the Fabric Manager Server and Web Server.

Note that although the switches can be configured to send log events to a syslog service listening on the Fabric Manager, that this functionality was not evaluated and cannot be enabled in the evaluated configuration.

Management

The TOE is managed by the Cisco Fabric Manager / Device Manager software accessed via the management workstation, or through the CLI using SSH or a serial connection.

Management interfaces supported by each instance of a switch in the TOE include:

- Command Line Interface (CLI) through a serial port or an SSH session over Out-of-band (OOB) management port
- OOB Ethernet management, through a supervisor module front panel Ethernet port
- SNMPv3 over OOB management port (for Fabric Manager and Device Manager access)

Management interfaces supported by the Fabric Manager in the TOE include:

- A local Fabric Manager Web Client and an out-of-band Fabric Manager Client

CLI

The CLI allows the user to type and execute commands at the switch prompt. The CLI parser provides command help, command completion, and keyboard sequences that allow users to access previously executed commands from the buffer history. The CLI may be accessed via SSH or directly through the serial port on the TOE. The CLI adheres to the same syntax to that of the Cisco IOS CLI.

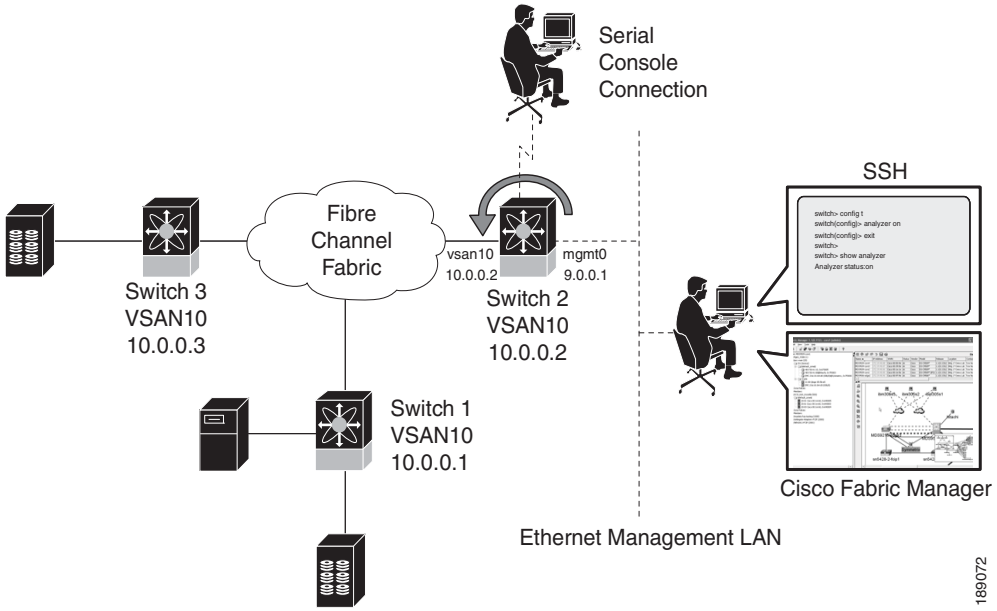
Cisco Fabric Manager

The Cisco Fabric Manager is a Java and SNMPv3-based network fabric and device management tool with a Graphical User Interface that displays real-time views of your network fabric and installed devices. The Cisco Fabric Manager provides three views for managing your network fabric:

- The Device View displays a continuously updated physical picture of device configuration and health conditions for a single switch.
- The Fabric View displays a view of your network fabric, including multiple switches.
- The Summary presents real-time performance statistics all active ports and channels.

The Cisco Fabric Manager provides an alternative to the CLI for most switch configuration commands.

Figure 4 TOE Administration Scenarios



Features Outside of Scope

Current software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- IPFC and In-band Management of the TOE switches
- FCIP
- Switch Command Line Interface (only as accessed through the Fabric Manager Client and Device Manager)

  This Command Line Interface Tool is available from the pull-down menus of the Fabric Manager Client and Device Manager.
- IPSec
- Certificate Authorities and Digital Certificates
- SAN Extension Tuner
- FICON
- Cisco Storage Media Encryption
- Cisco Data Mobility Manager
- Oracle Database
- JBoss jmx-console
- JBoss web-console
- Use of Intelligent Storage Services:

  - SCSI Flow Services and Statistics
  - Fibre Channel Write Acceleration
  - SANTap
  - Network-Accelerated Serverless Backup (NASB)
  - Network-Hosted Storage Applications with the Fabric Application Interface Standard (FAIS)-based Intelligent Storage Application Programming Interface (ISAPI). This is an API Cisco provides on the SSM.

Note that the Intelligent Storage Services (ISS) capabilities mentioned above are available on the -port Fibre Channel Storage Services Module (SSM) but require a separate boot image to be installed on the SSM. This is not allowed in the evaluated configuration.

IT Environment

The TOE boundary does not include the following IT Environment Components:

- Hardware platform for the Fabric Manager, which can be any of the following:
  - Windows 2000 SP4, 2003 SP2, XP SP2
  - Redhat Linux (2.6 Kernel)
  - Solaris (SPARC) 8 and 10
- Sun JRE and JDK 1.5.x
- Internet Browser:
  - Internet Explorer 5.5 or later
  - Netscape 6 or later
  - Mozilla Firefox 1.0 or later

Services Provided by the TOE environment

The following services are provided by the TOE environment:

- AAA server functionality
- Storage of Fabric Manager, its logs, its database, and configuration files (on host OS)
- NTP server functionality
- A management workstation suitable to access the configuration interfaces of the TOE via SSH or Cisco Fabric Manager (Web Application)
- FICON, a high-speed input/output (I/O) interface for mainframe connections to storage devices.
- The switch to host DHCHAP authentication requires an HBA adapter that is FC-SP compliant and supports DHCHAP authentication.

TOE DATA

Data in the TOE is categorized as either user data or TSF data. The following sections identify the data included in the TOE.

TSF Data

The TSF data produced and maintained by the TOE are audit records, MDS time, user identification and authentication credentials for both MDS and Fabric Manager and MDS and Fabric Manager security roles. The Fabric Manager related TSF data (identification and authentication credentials and security role definitions) are stored in the Fabric Manager Database, although these credentials are only used to authenticate to Fabric Manager if all of the configured MDS authentication switches are not available. In addition, SNMP user credentials for the switch are cached in the Fabric Manager Database.

The security attributes of the TOE used to support the SFRs identified in this ST are:

1. Authentication credentials (password)
2. User identifiers (user name)
3. SNMP Manager credentials (SNMPv3 security model and level attributes and SNMP IP address, and authentication and privacy password)
4. User assigned Access Levels (role)

The SNMPv3 security level attributes define how the authentication and encryption algorithms will be applied to SNMP packets. The security level attributes define if no authentication or encryption will be applied; if only authentication will be applied; or if both authentication and encryption will be applied to SNMP packets. The evaluated configuration requires both authentication and encryption. The security model of SNMPv3 is a user based security model which defines per user, username and authentication and privacy password and the security level attributes that are used for the specific user when they carry out SNMP requests.

A security role is assigned to a user when their user account is created on the switch. Switch role definitions control access to management of VSANs and also control access to commands from the CLI.

User Data

There is no user data maintained or stored by the TOE. Since the TOE is a managed switch, user data passes through the TOE in the data payload of networking packets. This data is not stored or managed by the TOE.

TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.

Secure Usage Assumptions

The following assumptions relate to the operation of the TOE:

Table 2 Secure Usage Assumptions

Name	Description
A.NOEVIL	Network administrators and operators of the TOE are assumed to be non-hostile, trusted to perform their duties in a secure manner, and expected to follow all security policies and procedures applicable to their deployment.
A.PHYSICAL	Internetworking equipment containing the TOE is assumed to be in a physically secure environment.
A.ZONECONNECT	Interconnected switches within the same management zone as the TOE are assumed to have protection against unauthorized access.
A.NETPROTECT	Data traversing the VSAN across different environment locations is assumed to be protected from threats of unauthorized disclosure and unauthorized modification.
A.PERSONNEL	It is assumed that administrators, operators and maintainers have been trained sufficiently to configure, operate, and maintain the TOE in a secure and trusted manner in accordance with the guidance documentation.
A.TIMESOURCE	Clock sources external to the scope of the TOE are stored in a secure location, and configured accurately so as to provide a trusted clock source for the TOE's internal clock.
A.VSANTIMESYNC	All network devices within the VSAN will be configured to the same external clock.
A.MANAGEMENTLAN	The Management LAN is protected. All services such as AAA or NTP provided by the management LAN, and all devices attached to the management LAN are trusted to perform in a secure manner.
A.PASSWORD	Administrators shall ensure that all users of the TOE use passwords that conform to the complexity requirements as described in the evaluated guidance documentation.
A.HOSTOS	The host operating system of the Fabric Manager is assumed to provide protection to files that are stored on it such that they cannot be deleted or altered without authorization.

Threats to Security

Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

Threats Addressed by the TOE

In general, the threat agent includes, but is not limited to: 1) people with TOE access who are expected to possess “low” expertise, resources, and motivation, or 2) failure of the TOE.

The TOE addresses the following threats:

Table 3 Threats Countered by the TOE

Name	Description
T.USERATTACK	An unauthorized individual may gain access to the TOE and compromise its security functions by altering its configuration and/ or audit records.
T.EXCEEDPRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in the illegal modification of the TOE configuration.
T.VSANCOMPROMISE	An unauthorized user, switch, host or device within the SAN fabric may gain access to a VSAN they are not a member of, and view traffic belonging to that VSAN.
T.ZONECOMPROMISE	An unauthorized user or device within a VSAN may gain access to a zone they are not a member of, and view traffic belonging to that zone.
T.SWITCHCOMPROMISE	An unauthorized switch or host within the SAN fabric may gain access to a switch or host they are not permitted to access, and view the traffic destined for that switch or host.
T.NODETECT	An unauthorized user, switch, host or device attempts to mount an attack against the TOE security functions without detection.

Threats Addressed by the Operating Environment

The TOE operational environment addresses the following threats:

Table 4 Threats Countered by the TOE Operating Environment

Name	Description
TE.BADTIME	An authorized user is unable to determine the sequence of events in the audit trail due to an incorrect or inaccurate time-stamp.
TE.BADAAA	A compromised AAA service allows unauthorized persons access to the TOE configuration.
TE.BADMANAGEMENT	Equipment on the management LAN is used to mount an attack against the TOE.

Security Objectives

The security objectives are a concise statement of the intended response to the security problem. These objectives indicate, at a high level, how the security problem, as characterized in the "Security Environment" section of the ST, is to be addressed. Just as some threats are to be addressed by the TOE and others by its intended environment, some security objectives are for the TOE and others are for its environment. These two classes of security objectives are discussed separately.

Security Objectives for the TOE

The security objectives for the TOE are as described in the following table.

Table 5 Security Objectives for the TOE

Name	Description
O.SECUREOPERATE	The TOE shall prevent unauthorized modification to its security functions and configuration data.
O.MONITOR	The TOE shall provide the capability to monitor and provide limited control over user sessions.
O.VSANPROTECT	The TOE shall prevent unauthorized disclosure of VSAN traffic from those users and devices belonging to other VSANs within the SAN fabric.
O.VSANACCESS	The TOE shall ensure that only those authorized users, switches, hosts and devices within the SAN fabric are granted access to the appropriate VSAN.
O.SWITCHACCESS	The TOE shall ensure that only those authorized switches and hosts are granted access to the appropriate switches and hosts within the SAN fabric.
O.ZONEACCESS	The TOE shall ensure that only those authorized devices and user groups within the same VSAN are granted access to the appropriate zone.

Table 5 Security Objectives for the TOE

Name	Description
O.PRIVILEGE	The TOE shall ensure that authorized users do not exceed their assigned privileges (or roles).
O.AUDIT	The TOE shall record the necessary events to ensure that all users of the TOE are held accountable for their actions.

Security Objectives for the TOE Environment

The security objectives for the TOE environment are as described in the following table.

Table 6 Security Objectives for the Environment

Name	Description
OE.SECUREMANAGE	Those responsible for the operation of the TOE and interconnected switches shall ensure that the TOE environment is physically secure, and management and configuration of the security functions of the TOE are: a) initiated from a management station connected to a protected network, b) undertaken by trusted staff trained in the secure operation of the TOE, and c) performed securely through the creation of strong passwords in accordance with industry best practices d) configured to interface only to trusted clock sources.
OE.TRAFFICPROTECT	Those responsible for the operation of the TOE and the traffic between interconnected entities belonging to the same VSAN (but located in different physical environments) shall ensure that adequate security controls have been deployed to protect against threats of unauthorized disclosure and unauthorized modification.
OE.AAA	When the TOE is configured to use an external AAA server, the IT Environment will provide trusted authentication and authorization services for use with the TOE. The protocols that may be used for these services are restricted to either RADIUS or TACACS+.
OE.TIME	The Fabric Manager portion of the TOE will utilize a reliable time stamp from the environment, and the switch portions of the TOE will have access to a reliable time source from the environment.
OE.FMSTORAGE	Those responsible for the operation of the TOE and its environment will ensure that protected storage of the Fabric Manager configuration files, audit logs, and database is provided on the host operating system.

IT Security Requirements

TOE Security Functional Requirements

This section contains the functional requirements for the TOE. The functional requirements are listed in summary form in the table below.

Table 7 TOE Security Functional Requirements

No.	Component	Component
Class FAU: Audit		
	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Security audit review
Class FCS: Cryptographic Support		
	FCS_CKM.1(1)	Cryptographic key generation (SSH)
	FCS_CKM.1(2)	Cryptographic key generation (DES)
	FCS_CKM.1(3)	Cryptographic key generation (Blowfish)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1 (1)	Cryptographic operation (Local Password Encryption, Database Password Encryption, and Database Initial
	FCS_COP.1 (2)	Cryptographic operation (FM Local Database Password Encryption)
	FCS_COP.1 (3)	Cryptographic operation (Database End-User Password Encryption)
	FCS_COP.1 (4)	Cryptographic operation (DH-CHAP)
	FCS_COP.1 (5)	Cryptographic operation (SSH)
Class FDP: User Data Protection		
	FDP_IFC.1(1)	Subset Information flow control – Zone Policy
	FDP_IFF.1(1)	Simple Security Attributes – Zone Policy
	FDP_IFC.1(2)	Subset Information flow control – IP ACLs
	FDP_IFF.1(2)	Simple Security Attributes – IP ACLs
	FDP_IFC.1(3)	Subset Information flow control – VSAN
	FDP_IFF.1(3)	Simple Security Attributes – VSAN
Class FIA: Identification and Authentication		
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5(1)	Multiple authentication mechanisms

Table 7 TOE Security Functional Requirements

No.	Component	Component
	FIA_UID.2(1)	User identification before any action
Class FMT: Security Management		
	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SAE.1	Time-limited authorization
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FMT_SMR.3	Assuming roles
Class FPT: Protection of the TSF		
	FPT_SEP.1(1)	TSF Domain Separation
	FPT_STM_SWT_EXP.1	Reliable Time Stamps
	FPT_RVM.1(1)	Non-bypassability of the TSP
Class FTA: TOE Access		
	FTA_SSL_SWI_EXP.3	TSF-initiated termination
	FTA_TSE.1	TOE session establishment
Class FTP: Trusted path/channel		
	FTP_ITC.1	Inter-TSF trusted channel

The following sections contain the functional components from the Common Criteria Part 2 [CC2] (CC) with the operations completed. The standard CC text is in regular font; the text inserted by the Security Target (ST) author is in accordance with the conventions described in at the beginning of this document.

Security Audit (FAU)

Audit Data Generation (FAU_GEN.1)

Hierarchical to: No other components.

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

[The events listed in Table 8: Audit Events, below].

s

Table 8 Audit Event

Component	Audit Events Generated
Switch	• Login and logout events of users; • Configuration commands executed by the switch user; • Intrusion attempts on the TOE fiber channel switch ports; and • AAA events from external RADIUS and TACACS+ servers
Fabric Manager	• Login and logout events of users

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [no other audit relevant information].

Dependencies: FPT_STM_SWT_EXP.1 Reliable time stamps

Application Note: There are two audit generation mechanisms on the TOE. One on the switch and one on the Fabric Manager.

Security Audit Review (FAU_SAR.1)

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [the Role listed in Table 9: Audit Review Privileges] with the capability to read [the Privileges listed in Table 9: Audit Review Privileges] from the audit records.

Table 9 Audit Review Privileges

Role	Privileges
Network-admin(sw) and other switch based customized user roles with privileged access	All switch audit information All Fabric Manager audit information depending on FM authentication mode selected, as shown in Table 13
Network-operator(sw)	All switch audit information
Network-admin(FM)	All Fabric Manager audit information
Network-operator(FM)	None

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit Data Generation

Cryptographic Support (FCS)

Cryptographic Key Generation (FCS_CKM.1 (1)) – SSH

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic **public/private** keys in accordance with a specified cryptographic key generation algorithm [RSA, DSA] and specified cryptographic key sizes [1024, 2048] that meet the following: [RSA Encryption Standard (PKCS#1), Digital Signature Standard(FIPS-186)].
Dependencies:	FCS_COP.1 Cryptographic operation
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.2 Secure security attributes

Cryptographic Key Generation (FCS_CKM.1 (2)) – DES

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [DES] and specified cryptographic key sizes [56 bit] that meet the following: [FIPS PUB 46-3].
Dependencies:	FCS_COP.1 Cryptographic operation
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.2 Secure security attributes

Cryptographic Key Generation (FCS_CKM.1 (3)) – Blowfish

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Blowfish] and specified cryptographic key sizes [128] that meet the following: [not applicable].
Dependencies:	FCS_COP.1 Cryptographic operation
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.2 Secure security attributes

Cryptographic Key Destruction (FCS_CKM.4)

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [no specified standard].
Dependencies:	FCS_CKM.1 Cryptographic key generation
	FMT_MSA.2 Secure security attributes

Cryptographic Operation (FCS_COP.1 (1)) – Local Password Encryption, Database Password Encryption, and Database Initial Connection Encryption

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [local password hashing on the switch, local password hashing of the database password on the database, and hashing of the database password between Fabric Manager and the PostgreSQL database] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [none] that meet the following: [RFC 1321].
Dependencies:	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.2 Secure security attributes

Cryptographic Operation (FCS_COP.1 (2)) – FM Local Database Password Encryption

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [local database password encryption on the Fabric Manager] in accordance with a specified cryptographic algorithm [Blowfish] and cryptographic key sizes [128] that meet the following: [none].
Dependencies:	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.2 Secure security attributes

Cryptographic Operation (FCS_COP.1 (3)) – Database End-User Password Encryption

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [local end-user password encryption in the PostgreSQL database] in accordance with a specified cryptographic algorithm [DES] and cryptographic key sizes [56 bits] that meet the following: [FIPS PUB 46-3].
Dependencies:	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.2 Secure security attributes

Cryptographic Operation (FCS_COP.1 (4)) – DH-CHAP

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [hashing on the shared secret password for DHCHAP authentication] in accordance with a specified cryptographic algorithm [MD5 or SHA-1] and cryptographic key sizes [none] that meet the following: [RFC 1321 or 3174].
Dependencies:	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.2 Secure security attributes

Cryptographic Operation (FCS_COP.1 (5)) – SSH Authentication

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [session key encryption/decryption] in accordance with a specified cryptographic algorithm [RSA, DSA] and cryptographic key sizes [1024, 2048] that meet the following: [RSA Encryption Standard (PKCS#1), Digital Signature Standard (FIPS-186-2)].
Dependencies:	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

User Data Protection (FDP)

Subset Information Flow Control (FDP_IFC.1(1)) – Zone Policy

Hierarchical to:	No other components.
FDP_IFC.1.1(1)	The TSF shall enforce the [Zone information flow control SFP] on [Subjects: Host, switch and storage devices Information: IP or FCP SCSI requests and responses within the Zone Operations: Permit or Deny SCSI requests and responses].
Dependencies:	FDP_IFF.1(1) Simple Security Attributes

Simple Security Attributes (FDP_IFF.1(1)) – Zone Policy

Hierarchical to:	No other components.
FDP_IFF.1.1(1)	The TSF shall enforce the [Zone information flow control SFP] based on the following types of subject and information security attributes: [Subject Security Attributes: Source and destination Zone member identifiers: – Port, node or switch World Wide Name (WWN) – IP address – Fiber Channel Identifier (FC ID) – Interface and domain ID – Logical Unit Number (LUN) – iSCSI qualified name (IQN) – Symbolic-node-name (IQN) Information Security Attributes: source ID, and destination ID].
FDP_IFF.1.2(1)	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [traffic to and from switches, hosts and storage devices within the Zone as identified by the information security attributes must be explicitly permitted by the Zone policy settings as identified by the subject security attributes].

FDP_IFF.1.3(1) The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4(1) The TSF shall provide the following [none].

FDP_IFF.1.5(1) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6(1) The TSF shall explicitly deny an information flow based on the following rules [none].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

Subset Information Flow Control (FDP_IFC.1(2)) – IP ACLs

Hierarchical to: No other components.

FDP_IFC.1.1(2) The TSF shall enforce the [information flow control SFP] on

[Subjects: MDS switch network interfaces

Information: IP packets

Operations: IP traffic filtering].

Dependencies: FDP_IFF.1(2) Simple Security Attributes

Simple Security Attributes (FDP_IFF.1(2)) – IP ACLs

Hierarchical to: No other components.

FDP_IFF.1.1(2) The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes:

[Subject Security Attributes: IP address

Information Security Attributes:

- Source IP address;
- Destination IP address;
- Source port number; and
- Destination port number
- IP Protocol
- ICMP message type
- ICMP message code
- Type of service (TOS)].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [traffic to and from switches (information security attributes) must be explicitly permitted by the policy settings (subject security attributes)].

FDP_IFF.1.3(2) The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4(2) The TSF shall provide the following [none].

FDP_IFF.1.5(2) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6(2) The TSF shall explicitly deny an information flow based on the following rules [none].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

Subset Information Flow Control (FDP_IFC.1(3)) – VSAN

Hierarchical to: No other components.

FDP_IFC.1.1(3) The TSF shall enforce the [VSAN information flow control SFP] on

[Subjects: Switch network interfaces

Information: FC-2 Frames

Operations: Permit or Deny FC Frames].

Dependencies: FDP_IFF.1(3) Simple Security Attributes

Simple Security Attributes (FDP_IFF.1(3)) – VSAN

Hierarchical to: No other components.

FDP_IFF.1.1(3) The TSF shall enforce the [VSAN information flow control SFP] based on the following types of subject and information security attributes:

[Subject Security Attributes: Receiving/transmitting VSAN interface

Information Security Attributes: VSAN ID].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [if the VSAN interfaces (subjects) are configured to be in the same VSAN].

FDP_IFF.1.3(3) The TSF shall enforce the [information flow so that only frames contain a matching VSAN ID in the header will be forwarded to the appropriate VSAN interfaces].

FDP_IFF.1.4(3) The TSF shall provide the following [none].

FDP_IFF.1.5(3) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6(3) The TSF shall explicitly deny an information flow based on the following rules [packets associated with a VSAN will not be forwarded to VSAN interfaces (subjects) not configured to be in that VSAN].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

Identification and Authentication (FIA)

User Attribute Definition (FIA_ATD.1)

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- [Username;

- Password;
- Assigned role(s)].

Dependencies: No dependencies.

User Authentication before any Action (FIA_UAU.2)

Hierarchical to: FIA_UAU.1

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.

Dependencies: FIA_UID.1 Timing of Identification

Multiple Authentication Mechanisms (FIA_UAU.5(1))

Hierarchical to: No other components

FIA_UAU.5.1 The TSF shall provide [

- User name and password combination (for CLI, SNMP, and FM users);
- Device name and password combination (for DH-CHAP);
- iSCSI host name and password combination (for CHAP); and
- User name and password or SSH key (for SSH users), and
- use of external RADIUS and TACACS+ authentication mechanisms as indicated in FIA_UAU.5(2)]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any **entity's** claimed identity according to the [

- For a user: SSH key or user name and password;
- For a iSCSI host: the iSCSI host must be authenticated to connect to the TOE via CHAP; and
- For a device: the device must be authenticated to connect to the TOE via DH-CHAP
- For authentication set to use RADIUS or TACACS+: the rules as specified in FIA_UAU.5.2(2)].

Dependencies: No dependencies

Application Note: There is also an option for authentication to RADIUS and TACACS+ servers for user, device, or host authentication. This functionality is covered by FIA_UAU.5(2) on the IT environment.

User Identification before any Action (FIA_UID.2(1))

Hierarchical to: FIA_UID.1

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.

Dependencies: No dependencies.

Application Note: There is also an option for authentication to RADIUS and TACACS+ servers for user, device, or host authentication. This functionality is covered by FIA_UID.2(2) on the IT environment.

Security Management (FMT)

Management of Security Functions Behaviour (FMT_MOF.1)

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable, **and** modify the behavior of* the functions [listed in Table 10: Functions of Roles] to [the Role listed in Table 10: Functions of Roles].

Table 10 Functions of Roles

Functions	Role
• Create, modify and delete FM user accounts • Create and assign FM security roles • View logged in FM Client users • Logout an FM Client user • Add or Remove a fabric from the list of monitored fabrics • View zone, VSAN, and Fabric Membership • Review FM Server logs • Configure RADIUS and TACACS+ parameters on FM • Configure initial database communication parameters	Network-Admin(FM)
• View the TOE configuration (on the FM) including Health, Performance, Inventory and Custom Reports for fabrics that have already been discovered	Network-Operator(FM)

Table 10 Functions of Roles

Functions	Role
• Add or Remove a fabric from the list of monitored fabrics • Add or remove switches, hosts and/or devices to the fabric • Bind entities to a fiber channel port • Bind inter-switch links within a VSAN • Change the default security parameters on the switch • Configure ACLs between devices and user groups within the same VSAN • Configure RADIUS and TACACS+ parameters on the FM • Configure RADIUS and TACACS+ parameters on the switch • Create, modify and delete FM User accounts • Create, modify and delete switch user accounts • Create and assign switch security roles • Create and assign FM security roles • Create and modify IP-based ACLs to restrict management traffic • Logout a FM Client user • Logout a switch user • Review audit events on the switch • Review FM Server logs • Specify CLI session and shell timeout periods • View logged in switch users • View logged in FM Client users • View zone, VSAN, and Fabric Membership	Network-Admin(sw) and other switch based customized user roles with privileged access
• Review of audit events on the switch • View zone, VSAN, Fabric and switch configuration	Network-operator(sw)

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

Management of Security Attributes (FMT_MSA.1)

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [Zone, IP ACL's and VSAN information flow control SFP's] to restrict the ability to *modify* ***and*** *delete* the security attributes [of VSANs, Zones and IP ACLs,] to [the network-admin (sw) role (or other switch based

customized roles with privileged access)].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

Application Note: This SFR covers specification of rules for all three iterations of FDP_IFF.1

Secure Security Attributes (FMT_MSA.2)

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model

FDP_IFC.1 Subset information flow control

FMT_MSA.1 Management of Security Attributes

FMT_SMR.1 Security Roles

Static Attribute Initialization (FMT_MSA.3)

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [Zone, IP ACL's and VSAN information flow control SFP's] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [network-admin role (sw) (and other switch based customized user roles with privileged access)] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of Security Attributes

FMT_SMR.1 Security Roles

Management of TSF Data (FMT_MTD.1)

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to *modify, delete* ***and*** *clear* the [TSF Data listed in Table 11: TSF Data and Roles] to [the Role listed in Table 11: TSF Data and Roles].

Table 11 TSF Data and Roles

TSF Data	Role
Switch configuration	Network-admin(sw) and other switch based customized user roles with privileged access
None	Network-operator(sw)
Fabric Manager configuration	Network-admin(FM), Network-admin(sw) depending on FM authentication mode selected, as shown in the table in SM.ROLE – Security Management Roles
None	Network-operator(FM)

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

Time-limited Authorization (FMT_SAE.1)

Hierarchical to: FMT_SMR.1

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [DH-CHAP authentication timeout value] to [the network-admin role (sw) (and other switch based customized user roles with privileged access)].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [reject the DH-CHAP authentication attempt] after the expiration time for the indicated security attribute has passed.

Dependencies: FMT_SMR.1 Security Roles

FPT_STM_SWT_EXP.1 Reliable Time Stamps

Specification of Management Functions (FMT_SMF.1)

Hierarchical to: No other components.

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

- Add or Remove a fabric from the list of monitored fabrics
- Add or remove switches, hosts and/or devices to the fabric
- Bind entities to a fiber channel port
- Bind inter-switch links within a VSAN
- Change the default security parameters on the switch
- Configure ACLs between devices and user groups within the same VSAN
- Configure initial database communication parameters

- Configure RADIUS and TACACS+ parameters on the FM
- Configure RADIUS and TACACS+ parameters on the switch
- Create, modify and delete FM User accounts
- Create, modify and delete switch user accounts
- Create and assign switch security roles
- Create and assign FM security roles
- Create and modify IP-based ACLs to restrict management traffic
- Logout a FM Client user
- Logout a switch user
- Review audit events on the switch
- Review FM Server logs
- Specify CLI session and shell timeout periods
- View logged in switch users
- View logged in FM Client users
- View the TOE configuration (on the FM) including Health, Performance, Inventory and Custom Reports for fabrics that have already been discovered
- View zone, VSAN, and Fabric Membership].

Dependencies: No Dependencies

Security Roles (FMT_SMR.1)

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the roles: [network-operator (sw), network-admin (sw), other switch based customized user roles with privileged access, network-admin (FM), network-operator (FM)].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of Identification

Assuming Roles (FMT_SMR.3)

Hierarchical to: No other components.

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: [network-admin (sw), network-operator (sw), other switch based customized user roles with privileged access, network-admin (FM), network-operator (FM)].

Dependencies: FMT_SMR.1 Security Roles

Protection of the TSF (FPT)

TSF Domain Separation (FPT_SEP.1(1))

Hierarchical to: No other components.

FPT_SEP.1.1(1) The TSF shall maintain a security domain for is own execution that protects it from

interference and tampering by untrusted subjects.

FPT_SEP.1.2(1) The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

Switch Reliable Time Stamps (FPT_STM_SWT_EXP.1)

Hierarchical to: No other components.

FPT_STM_SWT_EXP.1.1 The TSF shall be able to provide reliable time stamps for the MDS switch component use.

Dependencies: No dependencies.

Non-bypassability of the TSP (FPT_RVM.1(1))

Hierarchical to: No other components.

FPT_RVM.1.1(1) The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

TOE Access (FTA)

TSF-initiated Termination (FTA_SSL_SWI_EXP.3)

Hierarchical to: No other components.

FTA_SSL_SWI_EXP.3.1 The TSF shall terminate an interactive *Switch CLI* session after a

- [configurable Shell and Session timeout period of 1 to 525,600 minutes (as specified by the switch administrator in the TOE configuration)]

time interval of user inactivity.

Dependencies: No dependencies

TOE Session Establishment (FTA_TSE.1)

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [

- Any user account defined with the expired flag set on a switch.
- Any user account defined with the force session termination flag set on a switch; or
- Any Switch, Host and Devices within the fabric, based one or more of the following:
  - The failed DH-CHAP authentication attempts attribute;
  - Unauthorized Port, node or switch World Wide Name (WWN);
  - Unauthorized source/destination IP address;
  - Unauthorized source/destination TCP/UDP port number;
  - Unauthorized FC ID

–Unauthorized Interface and domain ID; and

–Unauthorized Logical Unit Number (LUN)].

Dependencies: No dependencies.

Trusted Path/Channels (FTP)

Inter-TSF Trusted Channel (FTP_ITC.1)

Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF **or** the remote trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [IP packet flows (management and VSAN traffic)].

Dependencies: No dependencies.

TOE Security Assurance Requirements

This section contains the assurance requirements for the TOE as specified by the CC for EAL 3 augmented with the assurance component ALC_FLR.1. The assurance requirements are listed in summary form in the table below.

Table 12 TOE Security Assurance Requirements

No.	Component	Component Name
Class ACM: Configuration management		
1	ACM_CAP.3	Configuration items
2	ACM_SCP.1	TOE Configuration Management Coverage
Class ADO: Delivery and Operation		
3	ADO_DEL.1	Delivery procedures
4	ADO_IGS.1	Installation, generation and start-up
Class ADV: Development		
5	ADV_FSP.1	Informal functional specification
6	ADV_HLD.2	Security enforcing high level design
7	ADV_RCR.1	Informal representational correspondence
Class AGD: Guidance documents		
8	AGD_ADM.1	Administrator guidance
9	AGD_USR.1	User guidance
Class ALC: Life Cycle Support		
10	ALC_DVS.1	Identification of security measures
11	ALC_FLR.1	Basic Flaw Remediation
Class ATE: Tests		
12	ATE_COV.2	Evidence of coverage
13	ATE_DPT.1	Testing: high level design
14	ATE_FUN.1	Functional testing
15	ATE_IND.2	Independent testing- sample
Class AVA: Vulnerability Assessment		
16	AVA_MSU.1	Examination of guidance
17	AVA_SOF.1	Strength of TOE security function evaluation
18	AVA_VLA.1	Developer vulnerability analysis

Configuration Management (ACM)

Authorization Controls (ACM_CAP.3)

Dependencies:	ACM_SCP.1 TOE CM Coverage
	ALC_DVS.1 Identification of security measures
ACM_CAP.3.1D	The developer shall provide a reference for the TOE.
ACM_CAP.3.2D	The developer shall use a CM system.
ACM_CAP.3.3D	The developer shall provide CM documentation.
ACM_CAP.3.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2C	The TOE shall be labeled with its reference.
ACM_CAP.3.3C	The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4C	The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.6C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.7C	The CM system shall uniquely identify all configuration items.
ACM_CAP.3.8C	The CM plan shall describe how the CM system is used.
ACM_CAP.3.9C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10C	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11C	The CM documentation shall provide measures such that only authorized changes are made to the configuration items.

TOE CM Coverage (ACM_SCP.1)

Dependencies:	ACM_CAP.3 Authorization Controls
ACM_SCP.1.1D	The developer shall provide a list of configuration items for the TOE.
ACM_SCP.1.1C	The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

Delivery and Operation (ADO)

Delivery Procedures (ADO_DEL.1)

Dependencies:	No dependencies
ADO_DEL.1.1D	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D	The developer shall use the delivery procedures.

ADO_DEL.1.1C	The delivery documentation shall describe all the procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Installation, Generation, and Start-Up Procedures (ADO_IGS.1)

Dependencies:	No dependencies
ADO_IGS.1.1D	The developer shall document procedures necessary for the secure generation, and start-up of the TOE.
ADO_IGS.1.1C	The installation, generation, and stat-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Development (ADV)

Informal Functional Specification (ADV_FSP.1)

Dependencies:	No dependencies
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C	The functional specification shall be internally consistent.
ADV_FSP.1.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C	The functional specification shall completely represent the TSF.

Security Enforcing High Level Design (ADV_HLD.2)

Dependencies:	ADV_FSP.1 Informal functional specification ADV_RCR.1 Informal correspondence demonstration
ADV_HLD.2.1D	The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1C	The presentation of the high level design shall be informal.
ADV_HLD.2.2C	The high level design shall be internally consistent.
ADV_HLD.2.3C	The high level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4C	The high level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5C	The high level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6C	The high level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7C	The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8C	The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error

messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Informal Correspondence Demonstration (ADV_RCR.1)

Dependencies: No dependencies

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent parts of TSF representation that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely verified in the less abstract TSF representation.

Guidance Documents (AGD)

Administrator Guidance (AGD_ADM.1)

Dependencies: ADV_FSP.1 Informal functional specification

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrator personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values, as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

User Guidance (AGD_USR.1)

Dependencies: ADV_FSP.1 Informal functional specification

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrator users of the System TOE.

AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the System TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of the TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Life Cycle Support (ALC)

Identification of Security Measures (ALC_DVS.1)

Dependencies:	ADO_IGS
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.1.2C	The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Basic Flaw Remediation (ALC_FLR.1)

Dependencies:	None
ALC_FLR.1.1D	The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.1.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.1.2C	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.1.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.1.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Tests (ATE)

Analysis of Coverage (ATE_COV.2)

Dependencies:	ADV_FSP.1 Informal functional specification

	ATE_FUN.1 Functional testing
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 identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2C	The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Testing: High-level Design (ATE_DPT.1)

Dependencies:	ADV_HLD.1 Descriptive high-level design
	ATE_FUN.1 Functional testing
ATE_DPT.1.1D	The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1C	The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Functional Testing (ATE_FUN.1)

Dependencies:	No dependencies.
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, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each test security function behaved as specified.

Independent Testing – Sample (ATE_IND.2)

Dependencies:	ADV_FSP.1 Informal functional specification
	AGD_USR.1 User guidance
	ATE_FUN.1 Functional testing
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.

Vulnerability Assessment (AVA)

Examination of Guidance (AVA_MSU.1)

Dependencies:	ADO_IGS.1 Installation, generation, and start-up procedures
	ADV_FSP.1 Informal functional specification
	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
AVA_MSU.1.1D	The developer shall provide guidance documentation.
AVA_MSU.1.1C	The guidance documentation 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.
AVA_MSU.1.2C	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3C	The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4C	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Strength of TOE Security Function Evaluation (AVA_SOF.1)

Dependencies:	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high level design
AVA_SOF.1.1D	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the SPP/SST.

Developer Vulnerability Analysis (AVA_VLA.1)

Dependencies:	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high level design
	AGD_USR.1 User guidance
AVA_VLA.1.1D	The developer shall perform a vulnerability analysis.
AVA_VLA.1.2D	The developer shall provide vulnerability analysis documentation
AVA_VLA.1.1C	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways n which a user can violate the TSP.
AVA_VLA.1.2C	The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment of the TOE.

Security Requirements for the IT Environment

Protected Audit Trail Storage (FAU_STG.1)

Hierarchical to: No other components

FAU_STG.1.1 The ~~TSF~~ **TOE environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The ~~TSF~~ **TOE environment** shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: This SFR covers the protection of the Fabric Manager logs on the host Operating System.

Multiple Authentication Mechanisms (FIA_UAU.5 (2))

Hierarchical to: No other components

FIA_UAU.5.1(2) The ~~TSF~~ **TOE environment** shall provide

- [User name and password combination (for CLI, SNMP, and FM users)
- Device name and password combination (for DH-CHAP);
- iSCSI host name and password combination (for CHAP);]

to support user authentication.

FIA_UAU.5.2(2) The ~~TSF~~ **TOE environment** shall authenticate any **entity's** claimed identity according to the

- [For a user: RADIUS and TACACS+ user name and password;
- For a iSCSI host: the iSCSI host must be authenticated to connect to the TOE via CHAP; and
- For a device: the device must be authenticated to connect to the TOE via DH-CHAP].

Dependencies: No dependencies

Application Note: This SFR covers the RADIUS and TACACS+ functionality that can be used to authenticate users, devices, and hosts.

User Identification before any Action (FIA_UID.2 (2))

Hierarchical to: FIA_UID.1

FIA_UID.2.1(2) The ~~TSF~~ **TOE environment** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application Note: This SFR covers the RADIUS and TACACS+ functionality that can be used to authenticate users, devices, or hosts.

FPT_STM_ENV_EXP.1 Environment Reliable Time Stamps

Hierarchical to: No other components.

FPT_STM_ENV_EXP.1 The IT environment shall be able to provide reliable time stamps for the Fabric Manager's use and an optional NTP time-source for the switch.

Dependencies: No dependencies.

TSF Domain Separation (FPT_SEP.1(2))

Hierarchical to: No other components.

FPT_SEP.1.1(2) The ~~TSF~~ **IT environment** shall maintain a security domain for is own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2) The ~~TSF~~ **IT environment** shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

Non-bypassability of the TSP (FPT_RVM.1(2))

Hierarchical to: No other components.

FPT_RVM.1.1(2) The ~~TSF~~ **IT environment** shall ensure that TSP enforcement functions are invoked nd succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

Protection of the Fabric Manager (FPT_STG_ENV_EXP.1)

Hierarchical to: No other components.

FPT_STG_ENV_EXP.1 The TOE environment shall protect the Fabric Manager configuration files and database TOE data from unauthorized deletion.

Dependencies: No dependencies.

Security Requirements for the Non-IT Environment

The TOE has no security requirements for the non-IT environment.

TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

IT Security Functions

This section presents the security functions implemented by the TOE.

Security Management (SM)

SM.ROLE – Security Management Roles

The TOE has default switch management user roles: network-admin (sw), network-operator (sw). The network-admin (sw) role has permission to execute all commands and make configuration changes on the switch and Fabric Manager depending on FM authentication mode selected, as shown in the table below, including the creation and customization of up to 64 additional switch roles. The network-operator (sw) role only has permission to view the switch configuration and audit events. The network-operator (sw) cannot make any configuration changes to the switch.

The switch roles network-admin (sw) and network-operator (sw) cannot be changed or deleted. However, customized roles can be created to assign to switch users requiring similar privileges to the network-admin(sw) and network-operator(sw) roles.

Additionally, the TOE has default Fabric Manager user roles: network-admin (FM) and network-operator (FM). The network-admin (FM) role has permission to make configuration changes on the Fabric Manager, including the addition of FM user roles. The network-operator (FM) role only has permission to view the configuration on the Fabric Manager, including Health, Performance, Inventory and Custom Reports for fabrics that have already been discovered.

The Fabric Manager credentials and roles are stored in the Fabric Manager Database (PostgreSQL). The network-admin (FM) has the responsibility for setting the initial communication parameters with the database during installation. These parameters specify which database is to be opened, and the connection parameters become a static part of the configuration. There is no mechanism on the TOE for changing the settings after installation. In addition, SNMP user credentials for the switch are cached in the Fabric Manager Database. The FM Web Client, FM Java Client and Device Manager all use the stored SNMP credentials to affect changes on the switch(s); it presents them on behalf of the admin when config changes are made to the switch.

In Table 16 an FM Authentication Method is listed, as it determines many of the privileges that are available to the roles on the TOE. The Fabric Manager allows local, MDS, or RADIUS/TACACS+ authentication. The Local setting utilizes the local Fabric Manager Database for authentication, the MDS setting uses TOE switches for authentication, and the RADIUS/TACACS+ setting uses external AAA servers for authentication. The table below also specifies the permissions granted to roles based on authentication modes.

Table 13 Role Permissions Division

network-admin(sw)	network-operator(sw)	network-admin(fm)	network-operator(fm)	Permission	FM Client auth modes	CLI auth modes	DM auth modes	FM Web auth modes
Yes				• Create, modify and delete switch user accounts	All	All	All	
Yes				• Create and assign switch security roles	All	All	All	
Yes				• Change the default security parameters	All	All	All	

Table 13 Role Permissions Division

network-admin(sw)	network-operator(sw)	network-admin(fm)	network-operator(fm)	Permission	FM Client auth modes	CLI auth modes	DM auth modes	FM Web auth modes
Yes				• Specify CLI session and shell timeout periods	All	All		
Yes				• View logged in switch users	All	All		
Yes				• Logout a switch user	All	All		
Yes				• Bind entities to a fiber channel port	All	All	All	
Yes				• Bind inter-switch links within a VSAN	All	All	All	
Yes				• Add or remove switches, hosts and/or devices to the fabric	All	All	All	
Yes				• Create and modify IP-based ACLs to restrict management traffic	All	All	All	
Yes				• Configure ACLs between devices and user groups within the same VSAN	All	All	All	
Yes				• Configure RADIUS and TACACS+ parameters on the switch	All	All	All	
Yes	Yes			• Review audit events on the switch	All	All	All	
Yes		Yes		• Create, modify and delete FM user accounts	All			All
Yes		Yes		• View logged in FM Client users	All			All
Yes		Yes		• Logout an FM Client user	All			All
Yes		Yes		• Add or Remove a fabric from the list of monitored fabrics	All			All
Yes		Yes		• Create and assign FM security roles				All
Yes	Yes	Yes		• View zone, VSAN, and Fabric Membership	All	All		All

Table 13 Role Permissions Division

network-admin(sw)	network-operator(sw)	network-admin(fm)	network-operator(fm)	Permission	FM Client auth modes	CLI auth modes	DM auth modes	FM Web auth modes
Yes		Yes		• Configure RADIUS and TACACS+ parameters on the FM				All
Yes		Yes		• Review FM Server logs				All
		Yes		• Configure initial database communication parameters				All
		Yes	Yes	• View the TOE configuration (on the FM) including Health, Performance, Inventory and Custom Reports for fabrics that have already been discovered.				Local only

SM.NETWORK-ADMIN – Network-Admin Roles

The network-admin(sw) role has responsibility for the security of the switches within the TOE through the ability to change the default security values. The network-admin (FM) role has responsibility for the security of the Fabric Manager.

The network-admin(sw) and network-admin(FM) roles have permissions on the TOE as defined in Table 13.

Device Access Control (AC)

AC.PORT – Port Security

Port security allows the network-admin (sw) role to configure the TOE to reject login requests from unauthorized Fiber Channel devices (Nx ports) and switches (xE ports). Port security is enforced by the TOE by configuring the devices and switch port interfaces through which each device or switch is connected. The port world wide name (pWWN) or the node world wide name (nWWN) is used to specify the Nx port connection for each device. The switch world wide name (sWWN) is used to specify the xE port connection for each switch. Each Nx and xE port can be configured to restrict a single port or a range of ports. Enforcement of port security policies are done on every activation and when the port initially becomes active. The port security feature requires all devices connecting to a switch to be part of the port security active database. The software uses this active database to enforce authorization.

AC.FABRICBIND – Fabric Binding Security

Fabric binding extends port security by binding inter-switch links within the SAN, thus preventing unauthorized switches from joining the fabric or disrupting current fabric operations. Fabric binding policies are enforced based on identities authenticated by DHCHAP.

AC.ZONES – Zone Security

Zoning enables the network-admin (sw) role to set up access control between storage devices or user groups within the same VSAN. Access to a zone is enforced by examining the source-destination ID field. Zone membership criteria is based on WWNs or FC IDs, including:

- Port world wide name (pWWN)
- Fabric pWWN
- FC ID
- Interface and switch WWN (sWWN)
- Interface and domain ID
- Domain ID and port number
- IP address
- iSCSI qualified name (IQN)
- Symbolic-node-name (IQN)

The table below shows the combinations of the attributes listed above that can be used with hosts, switches, and storage devices.

Table 14 Zone Subjects to Attributes Mapping

Zone Membership IDs	**Subject**		
	Host	Switch	Storage Device
pWWN	x	x	x
Fabric pWWN (fwwn)		x	
FC ID	x	x	x
Interface and sWWN		x	
Interface and domain ID		x	
Domain ID and port num		x	
IP address	x		x
iSCSI qualified name (IQN)	x		x
Symbolic-node-name (IQN)	x		x

A zone may consist of multiple zone members. Members in a zone can access each other; members in different zones cannot access each other. If zoning is not activated, all devices are members of the default zone. If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone.

Note Hard zoning is enforced by the hardware on each frame sent by an Nx port. As frames enter the switch, source-destination IDs are compared with permitted combinations to allow the frame at wirespeed. Hard zoning is applied to all forms of zoning.
Hard zoning enforces zoning restrictions on every frame, and prevents unauthorized access.

AC.LUNZONES – LUN Zone Security

Storage devices with multiple Logical Unit Numbers (LUNs) may be zoned separately via LUN Zoning. LUN zoning enables the network-admin (sw) role to restrict access to specific LUNs associated with a device. This type of zoning allows greater access granularity within a storage device.

AC.IPACL – IP Access Control Lists

IP-ACLs restrict IP-related Cisco MDS 9000 out-of-band (i.e. Ethernet based) management traffic based on IP address and port number. An IP-ACL is a sequential collection of permit and deny conditions that apply to IP flows. Traffic is tested against the conditions in the list. The first match determines if the software accepts or rejects the rule. An IP filter contains rules for matching traffic based on the protocol, address, port, ICMP type, and type of service (TOS). See . IP-ACLs allow the network-admin (sw) to permit or deny traffic per interface by these filtering types.

The network-admin (sw) role can specify IP-ACLs using an assigned name. Each IP-ACL can have a maximum of 256 entries. Each entry is a unique filter applied to a specified interface. Each switch can have a maximum of 64 IP-ACLs. Traffic coming into the switch is compared to IP-ACL entries based on the order that the entries occur in the switch. New statements are added to the end of the list. The TOE keeps looking until it has a match. If no matches are found when the switch reaches the end of the list, the traffic is denied. There is an *implied deny* for traffic that is not permitted. A single-entry IP-ACL with only one deny rule has the effect of denying all traffic.

IP-ACLs are only configurable on the management interface by the network-admin (sw) role.

Table 15 Access Control List Filters

Filter Type	Accepted Values	
IP Protocol	Integer (0-256)	
	Name (e.g., IP, TCP, UDP, ICMP, etc.)	
Address	Source	
	Source Wildcard	
	Destination	
	Destination Wildcard	
TCP/UDP Ports	Name	Number (0-65535)
UDP	dns	53
	tftp	69
	ntp	123
	radius accounting	1646 or 1813
	radius authentication	1645 or 1812
	snmp	161
	snmp-trap	162
	syslog	514

Table 15 Access Control List Filters

Filter Type	Accepted Values	
TCP	ftp	20
	ftp-data	21
	ssh	22
	telnet	23
	smtp	25
	tacacs-ds	65
	www	80
	sftp	115
	http	143
	wbem-http	5988
	wbem-https	5989
ICMP message	Type:	Code:
	echo	8
	echo-reply	0
	destination unreachable	3
	traceroute	30
	time exceeded	11
TOS	Name	Level (0-15)
	max-reliability	
	max-throughput	
	min-delay	
	min-monetary-cost	
	normal	

Accounting, System Message, and Fabric Manager Logs (AL)

AL.AUDIT – Accounting, System Message, and Fabric Manager Logs

The accounting and system message logs on the switch record the start-up and shutdown of the audit functions, all user actions on the switch such as login and logout and configuration commands executed by the user. Unauthorized access attempts to switch ports and channels on the TOE are also recorded in the system message log. The TOE records the date and time of each event, the type of event, the involved subject identity and the outcome of the event. The accounting and system message logs are generated and stored on the switch for later review and analysis.

Logged messages for switch events can be directed to the switch console, local disk or to a syslog server in the IT Environment using the SYSLOG protocol. Only the network-admin(sw) and network-operator(sw) roles can view the accounting and system message logs and review the audit messages stored in the switch buffer on the TOE and act upon them as required.

Log messages on Fabric Manager are generated by the Fabric Manager and stored in the Fabric Manager Server Logs, which can be viewed by the network-admin(sw) depending on FM authentication method selected (and shown in), network-admin(FM) role, and authenticated users on the host Operating System. Protection of these logs is provided by the host Operating System.

Session Control and Monitoring (CM)

CM.CONTROLS – Session Controls

The network-admin (sw) role can configure the shell session timeout value that specifies the lifetime of all terminal sessions on the TOE. When the time limit is exceeded the shell exits and closes that session. The default is 30 minutes. The network-admin (sw) role can configure different timeout values for a console or a virtual terminal line (VTY) session.

The network-admin (sw) role can also configure the terminal session timeout value that specifies the automatic logout time for the current terminal session on that switch. When the time limit configured by this command is exceeded, the switch closes that session and exits. The default is 30 minutes.

CM.MONITOR – User Sessions

The network-admin (sw) and network-admin (FM) role can display a list of all logged in users, and has the ability to terminate a user session. In addition, the network-admin (sw) role can, on the switch, specify an account timeout period upon creation of the user's account, display a user's profile details, and view a user's command history through the accounting log.

Encryption Services (ES)

ES.ENCRYPT – Password Encryption

When the TOE maintains the user name and password locally (whether on the switch or in the PostgreSQL database for Fabric Manager) it stores the password information in encrypted form. Specifically, on the switch a user's password is passed through a one-way hash algorithm (MD5) and the output value stored in the password file against the user's name. In the PostgreSQL database for Fabric Manager, DES encryption is used to encrypt the username and password for end users of Fabric Manager (the credentials in the FMUSERS and SNMPUSERS table).

The TOE also uses encryption to protect the initial connection data that is transferred between the Fabric Manager and the PostgreSQL database. This initial connection data contains a username and password that selects the correct PostgreSQL database and allows access to the database. Note that only the password is encrypted during the communications. This password is protected by Blowfish encryption where it is stored on the Fabric Manager, MD5 hashing before it is transferred in the connection request to the database, and MD5 hashing within the database itself.

Note that the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

ES.SSH – SSH Key Generation, Destruction & Authentication Support

A host key pair must be generated before enabling the SSH service on the TOE. The number of bits specified for the host key pair include 1024 and 2048. The TOE implements DSA and RSA cryptographic algorithms for key generation. Both SSH versions 1 and 2 have been implemented by the TOE. However, only SSH Version 2 is to be used in accordance with the evaluated configuration. A

separate SSH key with the same parameters may also be assigned to each user for secure remote management sessions. SSH keys bound to a particular user may be deleted. Key destruction is performed using an overwrite method of the keys stored on the local disk.

In order to support the authentication of a user, the TOE performs session key encryption based on the user's public key stored in the user's profile. This 'session key' is then sent back to the user where it is decrypted and verified by the SSH host to ensure its authenticity. Once the secure session is established, the user then submits his login credentials securely over the SSH tunnel to gain access to the TOE (refer to IA.LOCAL).

Note that the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

ES.DH-CHAP – Hashed Shared Secret Password

DH-CHAP authentication in each direction requires a shared secret password between the connected devices. This shared secret password is hashed using a negotiated hash algorithm before performing authentication. Supported hash algorithms include MD5 and SHA-1.

Note that the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

Identification and Authentication (IA)

IA.USERS – User Types

The TOE maintains user profiles on both the switch and the Fabric Manager. Authentication information, user name, user password, and role membership are stored in the user profile. The user profile on the switch also contains password expiration date, SNMP security parameters that determine the way their SNMP session is established and maintained (e.g. session encryption parameters), a SSH key for secure remote management access to the TOE and an optional expiry date for their account. Only SNMP Version 3 is to be used in accordance with the evaluated configuration.

IA.LOCAL – Local Identification & Authentication

The TOE enforces individual identification and authentication on all users attempting to access the TOE. Users with management access must successfully authenticate themselves using a unique user name and password combination prior to performing any actions on the TOE. The username and password of Fabric Manager users are also stored locally on the Fabric Manager database (the PostgreSQL database) that is within the TOE. The TOE maintains the user name and password locally and stores the password information in encrypted form. Both SNMP and the CLI have common role management and share the same credentials, user names and user passwords on the switch.

Several of the authentication mechanisms and interfaces will fail over or fallback to local authentication from the Fabric Manager local database if the selected method is not available. Note that this fallback does not alter the FM Authentication Mode setting in the Fabric Manager. The following table shows where, based on FM Authentication mode selected, credentials are stored, and whether fallback to Local authentication occurs.

Table 16 Authentication Storage and Fallback Capabilities

FM Authentication Method	Associated Role(s)	Management Interfaces that can be accessed	Where I&A credentials are stored	Other Authentication Credentials to Fallback To
MDS	network-admin(sw)	Command Line Interface	Locally on the switch[1]	None.
		Fabric Manager Web Client	Locally on the switch	Local network-admin(FM) credentials if none of the authentication switches are available
		Fabric Manager Client	Locally on the switch for initial authentication. Once authenticated to the switch the Fabric must be authenticated: which uses the SNMP credentials stored in the PostgreSQL database if the switch was previously discovered and authenticated; if the fabric has not been previously discovered, in order to do initial discovery the network-admin(sw) credentials must be provided.	Local network-admin(FM) credentials if none of the authentication switches are available. This will only open the client, however. The network-admin(sw) credentials must be provided to discover new fabrics.
		Device Manager	Locally on the switch	None.
MDS	network-operator(sw)	Command Line Interface, Fabric Manager Client, Device Manager	Same as for network-admin(sw) in MDS authentication mode	Local network-admin(FM) credentials if none of the authentication switches are available with the exception of Device Manager, which has no fallback.

Table 16 Authentication Storage and Fallback Capabilities

FM Authentication Method	Associated Role(s)	Management Interfaces that can be accessed	Where I&A credentials are stored	Other Authentication Credentials to Fallback To
MDS	network-admin(FM)	Fabric Manager Web Client	In the PostgreSQL database	None. (This is the role that is used for fallback.)
		Fabric Manager Client	In the PostgreSQL database	
MDS	network-operator(FM)	No interface available	N/A	N/A
Local	network-admin(sw)	Command Line Interface	Locally on the switch	None
		Device Manager	Locally on the switch	None
Local	network-operator(sw)	Command Line Interface	Locally on the switch	None
Local	network-admin(FM)	Fabric Manager Web Client	In the PostgreSQL database	None
		Fabric Manager Client	In the PostgreSQL database	None
Local	network-operator(FM)	Fabric Manager Web Client	In the PostgreSQL database	None

Table 16 Authentication Storage and Fallback Capabilities

FM Authentication Method	Associated Role(s)	Management Interfaces that can be accessed	Where I&A credentials are stored	Other Authentication Credentials to Fallback To
RADIUS/ TACACS+	network-admin(sw)	Command Line Interface	Locally on the switch	None.
		Fabric Manager Web Client	Locally on the switch	Local network-admin(FM) credentials if none of the authentication servers are available
		Fabric Manager Client	Locally on the switch for initial authentication. Once authenticated to the switch the Fabric must be authenticated: which uses the SNMP credentials stored in the PostgreSQL database if the switch was previously discovered and authenticated; if the fabric has not been previously discovered, in order to do initial discovery the network-admin(sw) credentials must be provided.	Local network-admin(FM) credentials if none of the authentication servers are available
		Device Manager	Locally on the switch	None.
RADIUS/ TACACS+	network-operator(sw)	Command Line Interface, Fabric Manager Client, Device Manager	Same as for network-admin(sw) in RADIUS/ TACACS+ authentication mode	Local network-admin(FM) credentials if none of the authentication servers are available with the exception of Device Manager, which has no fallback.

Table 16 Authentication Storage and Fallback Capabilities

FM Authentication Method	Associated Role(s)	Management Interfaces that can be accessed	Where I&A credentials are stored	Other Authentication Credentials to Fallback To
RADIUS/ TACACS+	network-admin(FM)	Fabric Manager Web Client	External RADIUS/ TACACS+ server; For Fallback: In the PostgreSQL database	None. (This is the role that is used for fallback.)
		Fabric Manager Client	External RADIUS/ TACACS+ server; For Fallback: In the PostgreSQL database	
RADIUS/ TACACS+	network-operator(FM)	Fabric Manager Web Client	External RADIUS/ TACACS+ server; For Fallback: In the PostgreSQL database	None.

1. Note that the local switch authentication is unaffected by the FM authentication setting. The switch can be configured to utilize an external RADIUS/ TACACS+ server for authentication. If this setting is configured, all places where this table says "Locally on the switch" would instead be "External RADIUS/ TACACS+ server" and the associated fallback is to the local switch.

IA.SWITCH&HOST- Switch and Host Authentication

The TOE allows fabric-wide authentication from one switch to another switch or from a switch to a host. These switch and host authentications are performed locally in each switch. Authentication between devices is performed using the Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) as part of the FC-SP protocol suite. Fiber Channel-level authentication allows only authenticated devices to be added to a fabric, thus preventing unauthorized devices from accessing the switch.

Host authentication may also be performed for iSCSI hosts that request access to storage within the SAN.

RADIUS/TACACS+ can also be leveraged for centralized switch and host authentication via the client modules. The RADIUS/TACACS+ server(s) exist in the TOE environment.

DH-CHAP Authentication

DH-CHAP is a mandatory password-based, key-exchange authentication protocol that supports both switch-to-switch and host-to-switch authentication. DH-CHAP authentication in each direction requires a shared secret password between the connected devices. The network-admin (sw) role can configure passwords in the local authentication database for other devices in a fabric. These other devices are identified by their device name, which is also known as the switch World Wide Name (WWN) or device WWN. The password is restricted to 64 characters and can be specified in clear text (0) or in encrypted text (7)[1]. If the clear text (0) option is used the password is entered in clear text from the administrative session. If the encrypted text (7) option is used, the password is encrypted prior to entry.

During the DH-CHAP protocol exchange if the TOE does not receive the expected DH-CHAP message within a specified time interval, authentication failure is assumed. The time ranges from 20 (no authentication is performed) to 1000 seconds. The default is 30 seconds.

1. The shared secret password should be encrypted in accordance with the evaluated configuration.

iSCSI (CHAP) Authentication

The IP Storage Services and Multiprotocol Services Modules supports the iSCSI authentication mechanism to authenticate iSCSI hosts that request access to storage. When iSCSI authentication is enabled, the iSCSI hosts must provide user name and password information each time an iSCSI session is established. During an iSCSI login, both the iSCSI initiator and target have the option to authenticate each other. By default, the IPS module allows either CHAP authentication or no authentication from iSCSI hosts. Please note that CHAP authentication is always to be used in accordance with the evaluated configuration. The IPS module verifies the iSCSI host authentication using the local password database, TACACS+, or RADIUS.

IA.LOGIN – Authenticated Sessions

Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE. Public key-based authentication is supported by the TOE through SSH for remote management access. For the Fabric Manager Web Services administrative username and password requirements apply.

IA.EXTERNAL – RADIUS / TACACS+ Client Support

The RADIUS and TACACS+ services for authentication for the switch are supported by the TOE through a client module. Through this client security management can be managed including the specification of the RADIUS or TACACS+ pre-shared key, server time-out interval and the display of server details. AAA event messages generated by the client are also recorded in the accounting log. For the Fabric Manager, RADIUS and TACAC+ services are configured through the Fabric Manager clients and supported through the Fabric Manager Server.

Access Control (ACC)

ACC.RBAC – Role Based Access Control

For switch security management via the CLI and SNMPv3 interface, up to 64 user-defined switch roles can be created. Privileges and actions on the switch can be associated with the user-roles on the switch and assigned to one or more VSANs.

The TOE has default switch roles: network-admin (sw), network-operator (sw), default-role (sw). Only the network-admin (sw) has write access to the switch security functions and configuration and is able to create switch user roles.

The TOE has default Fabric Manager roles: network-admin (FM) and network-operator (FM). Only the network-admin (sw) and network-admin (FM) have write access to the Fabric Manager security functions and configuration and are able to create FM user roles.

Confidentiality (CO)

CO.VSAN – VSAN Traffic Flow Control

VSANs provide isolation among devices that are physically connected to the same fabric. The underlying VSAN implementation allows the network-admin (sw) role to create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FCIDs) to be used simultaneously in different VSANs.

Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between the data traversing separate VSANs. This ensures the traffic flow control of data traversing the VSAN from users and devices belonging to other VSANs.Each separate virtual fabric is isolated from one another using a hardware-based frame tagging mechanism on VSAN member ports and EISL links. The Enhanced ISL (EISL) link type includes added tagging information for each frame within the fabric which allows for VSAN membership enforcement at each switch source port and destination port within a VSAN. Membership is defined using a unique VSAN ID.

Self-Protection of the TOE (SP)

SP.DOMAIN – Domain Separation and Non-bypassability

The switch component of the TOE is hardware appliance in which all operations in the TOE scope are protected from interference and tampering by untrusted subjects, with all administration and configuration operations performed within the physical boundary of the TOE. Also, all TSP enforcement functions must be invoked and succeed prior to functions within the TSC proceeding. The TOE has been designed so that all locally maintained TSF data and switch data can only be manipulated via the CLI or SNMPv3 interfaces. All line cards that are included in the TOE rely on the main MDS switch for power, memory management, and access control. In order to access any functionality of the line cards, the Identification & Authentication mechanisms of the switch must be invoked and succeed. In addition, the line cards use a central memory pool that is managed by the switch. No processes outside of the TOE are allowed direct access to this memory. Finally, the line cards enforce IP-ACLs, Zone policies and VSAN policies at their interfaces before traffic passes into the switch. This design, combined with the fact that only a user with the 'network-admin' roles or a similarly privileged user defined role may access the TOE security functions, provides a distinct protected domain for the TSF.

The Fabric Manager portion of the TOE (including its configuration files, logs, and PostgreSQL database) relies on the host OS in the IT environment for protection from interference and tampering and to ensure that TSP enforcement functions must be invoked.

SP.TIMESOURCE – Reliable Time Source

The TOE maintains real time on the switch using an internal hardware clock that can interface to the Network Time Protocol (NTP) for a time source. The host operating system in the IT environment maintains real time for the Fabric Manager, and its database, using an internal hardware clock.

Assurance Measures

The TOE claims to satisfy the assurance requirements for the Common Criteria Evaluation Assurance Level EAL3 (CC EAL3) augmented with the assurance component ALC_FLR.1. This section identifies the Configuration Management, System Development Procedures, System Test Documentation and System Installation and Guidance Documentation measures applied by TOE to satisfy the CC EAL3 and ALC_FLR.1 assurance requirements defined in the CC Part3 [CC3].

Table 17 Assurance Measures

Assurance Measure Label	Assurance Measure Description
CM_DEL	Configuration management and delivery documentation includes: a description of the method used to uniquely identify the configuration items; a configuration management plan describing how the configuration management system is used to maintain the configuration items, ensuring that only authorized changes are permitted;. The Configuration Management and Delivery documentation also provides all required information that describes all procedures necessary to maintain security for the distribution of the TOE to a user's site, and on the flaw remediation measures in place to support the TOE. Evidence title(s): Cisco's MDS 9000 Configuration Management Plan and Delivery Procedures
CL	A configuration list, which is a description of the configuration items comprising the TOE and provides evidence that the TOE implementation representation, design documentation, test documentation, guidance documentation and configuration management documentation are tracked by the CM systems Evidence title(s): Cisco MDS 9000 Specific Configuration Items List and Delivery Procedures
FSP	Functional specification that describes the TSF and its external interfaces and the purpose and method of use of external TSF interfaces, including details of effects, exceptions and error messages. Evidence title(s): Cisco MDS 9000 Functional Specification
HLD	High-level design that describes the structure of the TSF in terms of sub-systems and describes the security functionality provided by each sub-system. It should also describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages as appropriate. An indication of whether each subsystem is TSP-enforcing is also required. Additional mappings and analysis are presented in the FSP document for the TOE Summary Specification to TOE Security Functions. Evidence title(s): Cisco MDS 9000 High Level Design
RCR	Representation correspondence analysis that, for each adjacent pair TSF representations, demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. Evidence title(s): Cisco MDS 9000 Representation Correspondence

Table 17 Assurance Measures

Assurance Measure Label	Assurance Measure Description
AGD	Administrator guidance that describes the administrative functions and interfaces available to the administrator of the TOE, describes the steps necessary for the secure installation, generation and startup of the TOE, describes how to administer the TOE in a secure manner, describes warnings about functions and privileges that should be controlled in a secure processing environment, describes all assumptions about user behavior relevant to secure operation, describes all security parameters under the control of the administrator, and describes each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. Evidence title(s): Cisco MDS 9000 Administrator Guidance
DEV_SEC	Documentation on the security of the development environment describing all 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. Evidence should also be provided demonstrating that the security measures are being applied in practice. Evidence title(s): Cisco MDS 9000 Development Security
COV-DPT	The COV-DPT documentation provides: Analysis that demonstrates the correspondence between the tests identified in the test documentation and the TSF is complete and as described in the functional specification. Analysis that demonstrates that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design. Test documentation consisting of test plans, test procedure descriptions, expected test results and actual test results. The test plan identifies the security functions to be tested and the goal of the tests to be performed. The test procedure descriptions identify the tests to be performed, and describes the scenario(s) for testing each security function. The expected test results show the anticipated outputs from successful test execution. The actual test results demonstrate that each tested security function behaved as specified. Evidence title(s): Cisco MDS 9000 Test Coverage and Depth **Note** This evidence is contained within the Cisco MDS 9000 Functional Test Plan.
TEST_EQUIP	The TOE and necessary supporting infrastructure suitable for testing.
VLA_SOF	A vulnerability analysis that shows that for all identified vulnerabilities, the vulnerability cannot be exploited in the intended environment of the TOE. For each mechanism identified in the Security Target, an analysis shows that the claimed strength of TOE security function meets or exceeds the minimum strength level defined in the Security Target. Evidence title(s): Cisco MDS 9000 Vulnerability Analysis and Strength of Function

PP Claims

This Security Target does not claim conformance to a PP.

Rationale

Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are suitable, that is they are sufficient to address the security needs, and that they are necessary, ie, there are no redundant security objectives.

All Assumptions, Threats and Policies Addressed

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

- The first section (Table 18, Mapping of Assumptions, Threats, and OSPs to Security Objectives) shows that all of the secure usage assumptions, threats to security, and organizational security policies have been addressed.
- The second section (Table 19, Mapping of Security Objectives to Threats, Policies and Assumptions) shows that each security objective counters at least one assumption, policy, or threat.

Table 18 Mapping of Assumptions, Threats, and OSPs to Security Objectives

Threat/Policy/Assumption Label	Associated Security Objective
A.NOEVIL	O.SECUREOPERATE O.MONITOR O.AUDIT OE.SECUREMANAGE
A.PHYSICAL	OE.SECUREMANAGE
A.ZONECONNECT	OE.SECUREMANAGE OE.TRAFFICPROTECT
A.NETPROTECT	OE.TRAFFICPROTECT O.VSANPROTECT
A.PERSONNEL	O.MONITOR O.AUDIT O.PRIVILEGE
A.TIMESOURCE	OE.SECUREMANAGE

Table 18 Mapping of Assumptions, Threats, and OSPs to Security Objectives

Threat/Policy/Assumption Label	Associated Security Objective
T.USERATTACK	O.SECUREOPERATE O.VSANPROTECT O.VSANACCESS O.ZONEACCESS O.PRIVILEGE OE.AAA
T.EXCEEDPRIV	O.PRIVILEGE O.SECUREOPERATE O.AUDIT OE.AAA
T.VSANCOMPROMISE	O.SECUREOPERATE O.PRIVILEGE O.VSANPROTECT O.VSANACCESS OE.TRAFFICPROTECT
T.ZONECOMPROMISE	O.SECUREOPERATE O.PRIVILEGE O.ZONEACCESS OE.TRAFFICPROTECT
T.SWITCHCOMPROMISE	O.SECUREOPERATE O.PRIVILEGE O.SWITCHACCESS
T.NODETECT	O.MONITOR O.AUDIT OE.SECUREMANAGE

Table 19 shows that there are no unnecessary IT security objectives.

Table 19 Mapping of Security Objectives to Threats, Policies and Assumptions

Objective Label	Threat / Policy/ Assumption
O.SECUREOPERATE	A.NOEVIL T.USERATTACK T.EXCEEDPRIV T.VSANCOMPROMISE T.ZONECOMPROMISE T.SWITCHCOMPROMISE
O.MONITOR	A.NOEVIL A.PERSONNEL T.NORESPONSE T.NODETECT
O.VSANPROTECT	T.USERATTACK T.VSANCOMPROMISE
O.VSANACCESS	T.USERATTACK T.VSANCOMPROMISE
O.SWITCHACCESS	T.SWITCHCOMPROMISE
O.ZONEACCESS	T.USERATTACK T.ZONECOMPROMISE
O.PRIVILEGE	A.PERSONNEL T.USERATTACK T.EXCEEDPRIV T.VSANCOMPROMISE T.ZONECOMPROMISE T.SWITCHCOMPROMISE
O.AUDIT	A.NOEVIL A.PERSONNEL T.EXCEEDPRIV T.NODETECT
OE.SECUREMANAGE	A.NOEVIL A.PHYSICAL A.ZONECONNECT A.TIMESOURCE A.NOACCESS A.PASSWORD T.NODETECT

Table 19 Mapping of Security Objectives to Threats, Policies and Assumptions

Objective Label	Threat / Policy/ Assumption
OE.TRAFFICPROTECT	A.ZONECONNECT A.NETPROTECT T.VSANCOMPROMISE T.ZONECOMPROMISE
OE.AAA	A.PASSWORD T.USERATTACK T.EXCEEDPRIV
OE.TIME	TE.BADTIME
OE.FMSTORAGE	A.HOSTOS T.USERATTACK

Security Objectives are Sufficient

The following arguments are provided in Table 20 to demonstrate the sufficiency of the Security Objectives outlined above.

Table 20 Sufficiency of Security Objectives

Assumption/Threat/Policy	Argument to Support Security Objective Sufficiency
A.NOEVIL	This assumption is upheld by the following security objectives: O.SECUREOPERATE ensures that changes to the security functions and configuration data that has not been authorized will not succeed O.MONITOR provides a function whereby the user's session may be monitored and controlled as to detect and prevent unauthorized activity O.AUDIT provides for the recording of security-relevant events and associating users with those events so that users can be accountable for their actions OE.SECUREMANAGE ensures that the TOE environment is sited in a secure location and managed from within the protected network. It also ensures that TOE administrators receive appropriate training to enable them to operate the TOE securely.
A.PHYSICAL	This assumption is upheld by the security objective OE.SECUREMANAGE, which ensures that the TOE is located in a physically secure environment.
A.ZONECONNECT	This assumption is upheld by the following security objectives: OE.SECUREMANAGE, which ensures that the TOE environment (where interconnected switches may be present) is physically secure from unauthorized access. OE.TRAFFICPROTECT ensures that traffic traveling over unprotected communication paths within the SAN fabric is adequately protected through other means

Table 20 Sufficiency of Security Objectives

Assumption/Threat/Policy	Argument to Support Security Objective Sufficiency
A.NETPROTECT	This assumption is upheld by the following security objectives: OE.TRAFFICPROTECT which ensures that the traffic between interconnected entities located in different physical environments is protected against unauthorized disclosure and unauthorized modification O.VSANPROTECT ensures that users and devices belonging to a VSAN within the SAN fabric cannot view the traffic on other VSANs for which they do not have membership to access
A.PASSWORD	This assumption requires for the use of compliant passwords in the authentication of the users, switches, hosts and devices to the TOE and is upheld by OE.SECUREMANAGE which ensures that access to the TOE is performed securely through the creation of strong passwords in accordance with industry best practices. This assumption is also upheld by OE.AAA which provides trusted authentication and authorization services.
A.PERSONNEL	This assumption is upheld by the following security objectives: O.MONITOR as the actions of all personnel operating the TOE can be monitored by the TOE O.AUDIT provides for the recording of security-relevant events and associating personnel with those events O.PRIVILEGE ensures that all personnel operating the TOE do not exceed their assigned privilege
A.TIMESOURCE	This assumption is upheld by the security objective OE.SECUREMANAGE, which ensures that the TOE is configured to interface only to trusted clock sources.
A.HOSTOS	This assumption is upheld by the security objective OE.FMSTORAGE, which ensures that the IT environment provides protection to the Fabric Manager, configuration files, audit information, and database.

Table 20 Sufficiency of Security Objectives

Assumption/Threat/Policy	Argument to Support Security Objective Sufficiency
T.USERATTACK	The threat of a user-initiated attack on the TOE is countered by the following security objectives: O.SECUREOPERATE ensures that changes to the security functions and configuration data that has not been authorized will not succeed O.VSANPROTECT ensures that users belonging to a VSAN within the SAN fabric cannot view the traffic on other VSANs for which they do not have membership to access O.VSANACCESS ensures that only those authorized users within the SAN fabric are granted access to the appropriate VSAN O.ZONEACCESS ensures that only those user groups within the same VSAN are granted access to the appropriate zone O.PRIVILEGE ensures that the user is only permitted to perform the security functions corresponding to their assigned privilege or role OE.AAA provides trusted authentication and authorization services to ensure only authorised administrators perform configuration activities upon the TOE. OE.FMSTORAGE provides protection for the TOE configuration files, audit events, and database that are stored in the IT environment.
T.EXCEEDPRIV	The threat of an authorized user exceeding his/her privileges and subsequently illegally modifying the TOE configuration is countered by the following security objectives: O.PRIVILEGE ensures that the user is only permitted to perform the security functions corresponding to their assigned privilege or role O.SECUREOPERATE ensures that changes to the security functions and configuration data that has not been authorized will not succeed O.AUDIT provides for the recording of security-relevant events and associating users (and their privileges) with those events OE.AAA provides trusted authentication and authorization services to ensure only authorised administrators perform configuration activities upon the TOE.

Table 20 Sufficiency of Security Objectives

Assumption/Threat/Policy	Argument to Support Security Objective Sufficiency
T.VSANCOMPROMISE	The threat of an unauthorized user, switch, host or device within the SAN fabric gaining access to a VSAN they are not a member of and viewing traffic belonging to that VSAN is countered by the following security objectives: O.SECUREOPERATE ensures that any changes initiated from a user who has not been authorized (and therefore does not have the appropriate privilege) will not succeed O.PRIVILEGE ensures that the user is only permitted to perform the security functions corresponding to their assigned privilege or role O.VSANPROTECT ensures that users and devices belonging to a VSAN within the SAN fabric cannot view the traffic on other VSANs for which they do not have membership to access O.VSANACCESS ensures that only those authorized users, switches, hosts and devices within the SAN fabric are granted access to the appropriate VSAN OE.TRAFFICPROTECT ensures that traffic traveling over unprotected communication paths within the SAN fabric is adequately protected through other means
T.ZONECOMPROMISE	The threat of an unauthorized user or device within a VSAN gaining access to a zone they are not a member of and subsequently viewing the traffic belonging to that zone is countered by the following security objectives: O.SECUREOPERATE ensures that any changes initiated from a user who has not been authorized (and therefore does not have the appropriate privilege) will not succeed O.PRIVILEGE ensures that the user is only permitted to perform the security functions corresponding to their assigned privilege or role O.ZONEACCESS ensures that only those user groups and devices within the same VSAN are granted access to the appropriate zone OE.TRAFFICPROTECT ensures that traffic traveling over unprotected communication paths within the SAN fabric is adequately protected through other means

Table 20 Sufficiency of Security Objectives

Assumption/Threat/Policy	Argument to Support Security Objective Sufficiency
T.SWITCHCOMPROMISE	The threat of an unauthorized switch or host within the SAN fabric gaining access to a switch or host they are not permitted to access and subsequently viewing the traffic destined for that switch or host is countered by the following security objectives: O.SECUREOPERATE ensures that any changes initiated from a user who has not been authorized (and therefore does not have the appropriate privilege) will not succeed O.PRIVILEGE ensures that the user is only permitted to perform the security functions corresponding to their assigned privilege or role O.SWITCHACCESS ensures that only those authorized switches and hosts are granted access to the appropriate switches and hosts within the SAN fabric
T.NODETECT	The threat of an attack on the TOE security functions by an unauthorized user, switch, host or device succeeding without detection by the TOE is countered by the following security objectives: O.MONITOR ensures that the TOE has implemented the necessary security functions to monitor and provide limited control over user sessions. O.AUDIT ensures that all security-relevant events that may indicate an attack on the TOE security functions are recorded and that information recorded is sufficient to hold users accountable for their security-relevant actions OE.SECUREMANAGE, which ensures that operators of the TOE receive appropriate training for the secure management and operation of the TOE.

Security Requirements Rationale

Suitability of the Security Requirements

The purpose of this section is to show that the identified security requirements are suitable to meet the security objectives. and show that each security requirement is necessary, that is, each security objective is addressed by at least one security requirement or assumption and vice versa.

Security Objectives for the TOE are satisfied by Common Criteria functional components. Security Objectives for the Environment are satisfied by TOE secure usage assumptions with the exception of OE.AAA which is satisfied by the environmental SFRs FIA_UAU.5(2) and FIA_UID.2(2).

Table 21 Mapping of Security Objectives to Security Requirements

Security Objectives	Security Requirements
O.SECUREOPERATE	FCS_CKM.1(1) through (3), FCS_CKM.4, FCS_COP.1(1) through (3), FCS_COP.1(5), FDP_IFC.1(2), FDP_IFF.1(2), FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(3), FDP_IFF.1(3), FIA_ATD.1, FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2(1), FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FPT_SEP.1(1), FPT_RVM.1(1), FTA_SSL_SWI_EXP.3, FTA_TSE.1
O.MONITOR	FAU_GEN.1, FAU_SAR.1, FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1, FTA_SSL_SWI_EXP.3, FTA_TSE.1
O.VSANPROTECT	FDP_IFC.1(3), FDP_IFF.1(3), FTP_ITC.1
O.VSANACCESS	FCS_COP.1(4), FDP_IFC.1(3), FDP_IFF.1(3), FIA_ATD.1, FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2(1), FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SAE.1, FMT_SMF.1, FMT_SMR.1, FMT_SMR.3, FPT_SEP.1(1), FPT_RVM.1(1), FTA_TSE.1, FTP_ITC.1
O.SWITCHACCESS	FAU_GEN.1, FAU_SAR.1, FCS_COP.1(4), FDP_IFC.1(3), FDP_IFF.1(3), FIA_UAU.5(1), FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SAE.1, FMT_SMF.1, FPT_SEP.1(1), FPT_RVM.1(1), FTA_TSE.1
O.ZONEACCESS	FDP_IFC.1(1), FDP_IFF.1(1), FIA_ATD.1, FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2(1), FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_SMR.3, FPT_SEP.1(1), FPT_RVM.1(1)
O.PRIVILEGE	FDP_IFC.1(1), FDP_IFF.1(1), FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_SMR.3, FTA_TSE.1
O.AUDIT	FAU_GEN.1, FAU_SAR.1, FIA_UAU.2, FIA_UID.2(1), FMT_MOF.1, FPT_STM_SWT_EXP.1

Table 22 Mapping of Environmental Security Objectives to Assumptions

Environmental Objectives	Assumptions
OE.SECUREMANAGE	A.PHYSICAL, A.PERSONNEL, A.TIMESOURCE, A.PASSWORD.
OE.TRAFFICPROTECT	A.NETPROTECT
OE.AAA	A.PASSWORD
OE.FMSTORAGE	A.HOSTOS

Table 23 Mapping of Security Requirements to Security Objectives

Security Requirements	Security Objectives
FAU_GEN.1	O.MONITOR, O.AUDIT, O.SWITCHACCESS
FAU_SAR.1	O.MONITOR, O.SWITCHACCESS, O.AUDIT
FAU_STG.1	OE.FMSTORAGE
FCS_CKM.1(1) through (3)	O.SECUREOPERATE
FCS_CKM.4	O.SECUREOPERATE
FCS_COP.1 (1) through (3)	O.SECUREOPERATE
FCS_COP.1 (4)	O.VSANACCESS, O.SWITCHACCESS
FCS_COP.1 (5)	O.SECUREOPERATE
FDP_IFC.1(1)	O.SECUREOPERATE, O.ZONEACCESS
FDP_IFF.1(1)	O.SECUREOPERATE, O.ZONEACCESS
FDP_IFC.1(2)	O.SECUREOPERATE
FDP_IFF.1(3)	O.SECUREOPERATE
FDP_IFC.1(3)	O.SECUREOPERATE, O.VSANPROTECT, O.VSANACCESS, O.SWITCHACCESS
FDP_IFF.1(3)	O.SECUREOPERATE, O.VSANPROTECT, O.VSANACCESS, O.SWITCHACCESS
FIA_ATD.1	O.SECUREOPERATE, O.MONITOR, O.VSANACCESS, O.ZONEACCESS, O.PRIVILEGE
FIA_UAU.2	O.SECUREOPERATE, O.VSANACCESS, O.ZONEACCESS, O.AUDIT
FIA_UAU.5(1)	O.SECUREOPERATE, O.VSANACCESS, O.SWITCHACCESS, O.ZONEACCESS
FIA_UAU.5(2)	OE.AAA
FIA_UID.2(1)	O.SECUREOPERATE, O.VSANACCESS, O.ZONEACCESS, O.AUDIT
FIA_UID.2(2)	OE.AAA
FMT_MOF.1	O.SECUREOPERATE, O.MONITOR, O.VSANACCESS, O.SWITCHACCESS, O.ZONEACCESS, O.PRIVILEGE, O.AUDIT
FMT_MSA.1	O.SECUREOPERATE, O.MONITOR, O.VSANACCESS, O.SWITCHACCESS, O.ZONEACCESS, O.PRIVILEGE
FMT_MSA.2	O.SECUREOPERATE, O.MONITOR, O.VSANACCESS, O.SWITCHACCESS, O.ZONEACCESS, O.PRIVILEGE
FMT_MSA.3	O.SECUREOPERATE, O.MONITOR, O.VSANACCESS, O.SWITCHACCESS, O.ZONEACCESS
FMT_MTD.1	O.SECUREOPERATE, O.VSANACCESS, O.SWITCHACCESS, O.ZONEACCESS, O.PRIVILEGE
FMT_SAE.1	O.VSANACCESS, O.SWITCHACCESS

Table 23 Mapping of Security Requirements to Security Objectives

Security Requirements	Security Objectives
FMT_SMF.1	O.SECUREOPERATE, O.MONITOR, O.VSANACCESS, O.SWITCHACCESS, O.ZONEACCESS, O.PRIVILEGE
FMT_SMR.1	O.VSANACCESS, O.ZONEACCESS, O.PRIVILEGE
FMT_SMR.3	O.VSANACCESS, O.ZONEACCESS, O.PRIVILEGE
FPT_SEP.1(1)	O.VSANACCESS, O.SECUREOPERATE, O.SWITCHACCESS, O.ZONEACCESS
FPT_RVM.1(1)	O.VSANACCESS, O.SECUREOPERATE, O.SWITCHACCESS, O.ZONEACCESS
FPT_STM_SWT_EXP.1	O.AUDIT
FPT_STM_ENV_EXP.1	OE.TIME
FPT_TAB.1	O.SECUREOPERATE, O.PRIVILEGE,
FTA_TSE.1	O.SECUREOPERATE, O.MONITOR O.VSANACCESS, O.SWITCHACCESS, O.PRIVILEGE,
FTA_SSL_SWI_EXP.3	O.SECUREOPERATE, O.MONITOR
FTP_ITC.1	O.VSANACCESS, O.VSANPROTECT
FPT_RVM.1 (2)	OE.SECUREMANAGE
FPT_SEP.1 (2)	OE.SECUREMANAGE
FPT_STG_ENV_EXP.1	OE.FMSTORAGE

Table 24 Mapping of Assumptions to Environmental Objectives

Assumptions	Environmental Objectives
A.PHYSICAL	OE.SECUREMANAGE
A.PERSONNEL	OE.SECUREMANAGE
A.TIMESOURCE	OE.SECUREMANAGE
A.PASSWORD	OE.SECUREMANAGE, OE.AAA
A.NETPROTECT	OE.TRAFFICPROTECT
A.HOSTOS	OE.FMSTORAGE

Sufficiency of the Security Requirements

The following table shows that security requirements are sufficient to satisfy the TOE security objectives, whether in a principal or supporting role.

Table 25 Sufficiency of Security Requirements

Objectives	Argument to Support Sufficiency of Security Requirements
O.SECUREOPERATE	The objective to prevent unauthorized changes to the TOE security functions and configuration data is met by the following security requirements: • FCS_CKM.1(1) generates the SSH key pair to be used in the secure authentication of users prior to accessing the security functions and configuration • FCS_CKM.1(2) generates the DES key to be used to protect end-user passwords that are stored in the PostgreSQL database. • FCS_CKM.1(3) generates the Blowfish key to be used to protect the database password that is stored in the Fabric Manager configuration files. • FCS_CKM.4 ensures that the cryptographic keys used to authenticate to the TOE are destroyed appropriately • FCS_COP.1 (1) through (3) ensures that the local password entries are encrypted as to prevent illegitimate access to the TOE via a compromised password file and ensures that the connection data transferred between the Fabric Manager and the PostgreSQL database are not passed in the clear. • FCS_COP.1 (5) ensures that SSH session key encryption is performed in accordance with the OpenSSH v2 standard in support of remote user or host authentication to the TOE • FDP_IFC.1(1) requires that all switches, devices and hosts actions resulting in the access to the Zone controlled to prevent unauthorized Zone activity • FDP_IFF.1(1)supports FDP_IFC.1(1) by ensuring that access to the Zone is done so in accordance with the rules of the Zone access control policy • FDP_IFC.1(2) requires that all IP packets that flow through the TOE are subject to inspection prior to being forwarded. • FDP_IFF.1(2) supports FDP_IFC.1(2) by ensuring that IP packets flowing through the TOE do so in accordance with the rules of the information flow control policy • FDP_IFC.1(3) requires that all switches, devices and hosts actions resulting in the access to the VSAN security functions are controlled to prevent unauthorizey attributes are restrictive in nature as to enforce the access control and information flow control security policies for the TOE

Objectives	Argument to Support Sufficiency of Security Requirements
	• FDP_IFF.1(3)supports FDP_IFC.1(3) by ensuring that access to the VSAN is done so in accordance with the rules of the VSAN access control policy • FIA_ATD.1 ensures that user credentials are maintained by the TOE so they can be used for the identification and authentication of users prior to gaining access to the TOE security functions and configuration • FIA_UAU.2, FIA_UID.2(1) provide support for meeting this objective by requiring identification and authentication of all users prior to gaining access to the TOE • FIA_UAU.5(1) specifies the different authentication mechanisms used by the users, switches, devices and hosts to access each instance of the TOE • FMT_MOF.1 requires that the ability to manage the security functions and access the configuration is restricted to users with a privileged role • FMT_MSA.1 specifies that only users with a privileged role can manage the TOE security functions and related configuration data • FMT_MSA.2 specifies that only secure attributes will be used for the TOE security function configuration • FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control and information flow control security policies for the TOE • FMT_MTD.1 specifies that only users with a privileged role can manage the TOE configuration • FMT_SMF.1 specifies the management capabilities of the TSF to include security functions that can create, modify and delete the configuration data • FPT_SEP.1(1) ensures that the a separate execution domain is maintained by the TOE to avoid intentional (or otherwise) tampering with the TOE security functions and configuration data by un-trusted agents • FPT_RVM.1(1) ensures that the TSP enforcement functions cannot be bypassed • FTA_SSL_SWI_EXP.3 ensures the termination of an interactive CLI session in order to mitigate session hijacking of a user terminal left unattended • FTA_TSE.1 allows the TOE to deny session establishment for all users, switches, hosts and devices based on pre-defined conditions

Objectives	Argument to Support Sufficiency of Security Requirements
O.MONITOR	The objective to ensure that the TOE provides the capability to monitor and provide limited control over user sessions is met by the following security requirements: • FAU_GEN.1 requires the capability to generate records of security-relevant events, which can be used to detect suspicious user activity • FAU_SAR.1 requires that authorized users will have the capability to read and interpret data stored in the audit logs such that security breeches can be traced to user sessions • FIA_ATD.1 ensures that user credentials are maintained by the TOE so they can be used for the identification and authentication of users prior to gaining access to the TOE • FMT_MOF.1 supports this objective by giving users with a privileged role the ability to manage the security functions that control user privileges, session control and monitoring parameters • FMT_MSA.1 supports this objective by giving users with a privileged role to manage the TOE security functions that control and monitor user sessions • FMT_MSA.2 specifies that only secure attributes will be used for the TOE security function configuration • FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy and control user sessions • FMT_SMF.1 supports the security management functions relevant to the TOE, including the configuration of control and user monitoring parameters • FTA_SSL_SWI_EXP.3 ensures the termination of a user session after a pre-determined time period has elapsed • FTA_TSE.1 will deny a user permission to establish a session when their user account has expired
O.VSANPROTECT	The objective to ensure that the TOE will prevent unauthorized disclosure of VSAN traffic from those users and devices belonging to other VSANs within the SAN fabric is met by the following security requirements: • FDP_IFC.1(3) requires that all switches, devices and hosts actions resulting in the access to the VSAN traffic are controlled to prevent unauthorized access • FDP_IFF.1(3) supports FDP_IFC.1(3) by ensuring that access to the VSAN traffic is done so in accordance with the rules of the VSAN Information Flow Control policy

Objectives	Argument to Support Sufficiency of Security Requirements
	• FTP_ITC.1 ensures that a distinct protected communications channel is established between the TOE and each remote trusted IT product.
O.VSANACCESS	The objective to ensure that the TOE will only permit those authorized users, switches, hosts and devices within the SAN fabric access to the appropriate VSAN is met by the following security requirements: • FCS_COP.1 (4) ensures that hashing on the shared secret between switches and devices is performed in support of the DH-CHAP authentication protocol to prevent illegitimate access to the TOE via a compromised shared secret • FDP_IFC.1(3) requires that all switches, devices and hosts actions resulting in the access to the VSAN traffic are controlled to prevent unauthorized access • FDP_IFF.1(3) supports FDP_IFC.1(3) by ensuring that access to the VSAN traffic is done so in accordance with the rules of the VSAN Information Flow Control policy • FIA_ATD.1 ensures that user credentials are maintained by the TOE so they can be used for the identification and authentication of users prior to gaining access to the TOE • FIA_UAU.2, FIA_UID.2(1) provide support for meeting this objective by requiring identification and authentication of all users prior to gaining access to the TOE • FIA_UAU.5(1) specifies the different authentication mechanisms used by the users, switches, devices and hosts to access each instance of the TOE • FMT_MOF.1 requires that the ability to manage the security functions and access the configuration is restricted to users with a privileged role (which includes granting access to the VSAN) • FMT_MSA.1 specifies that only users with a privileged role can manage the TOE security functions and related configuration data that control access to the VSAN • FMT_MSA.2 specifies that only secure attributes will be used for the TOE security function configuration • FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control and information flow control security policies for the TOE • FMT_MTD.1 specifies that only users with a privileged role can manage the TOE configuration (which includes granting access to the VSAN) • FMT_SAE.1 allows a user with a privileged role to specify a timeout value for DH-CHAP authentication and reject the attempt to join the VSAN after the timeout period has expired

Objective	Argument to Support Sufficeincy of Security Requirements
	• FMT_SMF.1 specifies the management capabilities of the TSF to include security functions that can create, modify and delete the configuration data (which includes granting access to the VSAN) • FMT_SMR.1 requires that the TOE be able to maintain the roles and to be able to associate users with their roles (a role can determine which VSAN a user belongs to) • FMT_SMR.3 requires that an explicit request is performed for those users assuming a privileged role • FPT_SEP.1(1) ensures that a separate execution domain is maintained by the TOE to help prevent unauthorized access to the TOE (which includes the access control lists for each VSAN) • FPT_RVM.1(1) ensures that the TSP enforcement functions cannot be bypassed • FTA_TSE.1 allows the TOE to deny session establishment (within a VSAN) for all users, switches, hosts and devices based on pre-defined conditions • FTP_ITC.1 ensures that a distinct protected communications channel is established between the TOE and each remote trusted IT product.
O.SWITCHACCESS	The objective to ensure that the TOE will only permit those authorized switches and hosts within the SAN fabric to access other switches and hosts is met by the following security requirements: • FAU_GEN.1 supports this objective by recording intrusion attempts on the TOE fiber channel switch ports in the audit trail • FAU_SAR.1 supports FAU_GEN.1 by ensuring that authorized users will have the capability to read and interpret data stored in the audit logs such that security breeches can be detected • FCS_COP.1 (4) ensures that hashing on the shared secret between switches and hosts is performed in support of the DH-CHAP authentication protocol to prevent illegitimate access to the TOE via a compromised shared secret • FDP_IFC.1(3) requires that all switch, device and host actions resulting in the access to another switch, device or host are controlled to prevent unauthorized access • FDP_IFF.1(3) supports FDP_IFC.1(3) by ensuring that switch, device or host access to another switch, device or host is done so in accordance with the rules of the access control policy • FIA_UAU.5(1) specifies the different authentication mechanisms used by the switches and hosts to access each instance of the TOE

Objective	Argument to Support Sufficeincy of Security Requirements
	• FMT_MOF.1 requires that the ability to manage the security functions and access the configuration is restricted to users with a privileged role (which includes granting access to the VSAN) • FMT_MSA.1 specifies that only users with a privileged role can manage the TOE security functions and related configuration data that control the access parameters to other switches and hosts • FMT_MSA.2 specifies that only secure attributes will be used for the TOE security function configuration • FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control security policy for the TOE • FMT_MTD.1 specifies that only users with a privileged role can manage the TOE configuration (which includes managing the access parameters to other switches and hosts) • FMT_SAE.1 allows a user with a privileged role to specify a timeout value for DH-CHAP authentication and reject the attempt to join the VSAN after the timeout period has expired • FMT_SMF.1 specifies the management capabilities of the TSF to include security functions that can create, modify and delete the configuration data (which includes managing the access parameters to other switches and hosts) • FPT_SEP.1(1) ensures that the a separate execution domain is maintained by the TOE to help prevent unauthorized access to the TOE (which includes the access parameters to other switches and hosts) • FPT_RVM.1(1) ensures that the TSP enforcement functions cannot be bypassed • FTA_TSE.1 allows the TOE to deny session establishment for all interconnected switches and hosts to the TOE based on pre-defined conditions
O.ZONEACCESS	The objective to ensure that the TOE will only permit those authorized devices and user groups within the same VSAN to access a zone is met by the following security requirements: • FDP_IFC.1(1) requires that all devices and user group actions resulting in the access to a Zone are controlled to prevent unauthorized access • FDP_IFF.1(1) supports FDP_IFC.1(1) by ensuring that device and user group access to a Zone is done so in accordance with the rules of the Zone Information Flow Control policy • FIA_ATD.1 ensures that user credentials are maintained by the TOE so they can be used for the identification and authentication of users prior to gaining access to the TOE (which are also used to grant access to a zone)

Objectives	Argument to Support Sufficiency of Security Requirements
	• FIA_UAU.2, FIA_UID.2(1) provide support for meeting this objective by requiring identification and authentication of all users prior to gaining access to the TOE (or zones) • FIA_UAU.5(1) specifies the different authentication mechanisms used by the users and devices to access each instance of the TOE (and zones) • FMT_MOF.1 requires that the ability to manage the security functions and access the configuration is restricted to users with a privileged role (which includes granting access to the zone) • FMT_MSA.1 specifies that only users with a privileged role can manage the TOE security functions and related configuration data that control the zone access control lists • FMT_MSA.2 specifies that only secure attributes will be used for the TOE security function configuration • FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control security policy for the TOE • FMT_MTD.1 specifies that only users with a privileged role can manage the TOE configuration (which includes managing the zone access control lists) • FMT_SMF.1 specifies the management capabilities of the TSF to include security functions that can create, modify and delete the configuration data (which includes managing the zone access control lists) • FMT_SMR.1 requires that the TOE be able to maintain the roles and to be able to associate users with their roles (a role can determine which zone a user belongs to) • FMT_SMR.3 requires that an explicit request is performed for those users assuming a privileged role • FPT_SEP.1(1) ensures that the a separate execution domain is maintained by the TOE to help prevent unauthorized access to the TOE (which includes the zone access control lists) • FPT_RVM.1(1) ensures that the TSP enforcement functions cannot be bypassed
O.PRIVILEGE	The objective to ensure that authorized users do not exceed their privileges (or roles) is met by the following security requirements: • FIA_ATD.1 associates the user security role with their user identity which then determines the user's set of privileges

Objectives	Argument to Support Sufficiency of Security Requirements
	• FMT_MOF.1 requires that the ability to access the security functions that control user privileges, session control and monitoring parameters is restricted to users with a privileged role • FMT_MSA.1 specifies that only users with a privileged role can access the TOE security functions and related configuration data • FMT_MSA.2 specifies that only secure attributes will be used for the TOE security function configuration • FMT_MTD.1 specifies that only users with a privileged role can access the TOE configuration • FMT_SMF.1 details the security management functions relevant to the TOE, including the configuration of user roles (which determine the user privileges) • FMT_SMR.3 requires that an explicit request is performed for those users assuming a privileged role (network-admin (sw), network-operator (sw), customized switch role with privileged access, network-admin (FM), or network-operator (FM)) • FTA_TSE.1 will deny a user permission to establish a session when their user account has expired
O.AUDIT	The objective to provide the means of detecting and recording security relevant events is met by the following security requirements: • FAU_GEN.1 requires the capability to generate records of security-relevant events, including configuration commands executed by the user in order to be able to hold a user accountable for their actions • FAU_SAR.1 requires that authorized users will have the capability to read and interpret data stored in the audit logs such that security breeches can be detected • FIA_UAU.2, FIA_UAU.2 support FAU_GEN.1 by requiring the TOE to enforce identification and authentication of all users • FMT_MOF.1 require that that the ability to manage the audit functions be restricted to users with a privileged role • FPT_STM_SWT_EXP.1 requires the provision of reliable time stamps that can be associated with security-relevant events
OE.AAA	The objective to provide trusted remote authentication and authorization services for use with the TOE via the RADIUS or TACACS+ protocols are met by the following security requirements for the IT environment: • FIA_UID.2(2) provides support for meeting this objective by requiring identification of all users prior to gaining access to the TOE • FIA_UAU.5(2) specifies the different remote authentication mechanisms available to be used by the users, switches, devices and hosts to access each instance of the TOE.

Objectives	Argument to Support Sufficiency of Security Requirements
OE.TIME	The objective to provide time services in the environment is supported by the following security requirement for the IT environment: • FPT_STM_ENV_EXP.1 provides support for meeting this objective by requiring a timestamp on the host OS and an optional time-source in the environment.
OE.SECUREMANAGE	The objective to provide secure management of the TOE and interconnected switches in the environment is supported by the following security requirement for the IT environment: • FPT_SEP.1(1) provides support for meeting this objective by requiring the IT environment to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. • FPT_RVM.1(1) ensures that the TSP enforcement functions cannot be bypassed
OE.FMSTORAGE	The objective to provide secure storage of the TOE Fabric Manager configuration files, audit data, and database that is stored in the environment is supported by the following security requirement for the IT environment: • FAU_STG.1 ensures that unauthorized modification and deletion of records on the host OS is not allowed. • FPT_STG_ENV_EXP.1 ensures that the host OS provides protection to the FM configuration files and database.

Satisfaction of Dependencies

Table 25 shows the dependencies between the functional and assurance requirements. All of the dependencies are satisfied. Note that:

(H) indicates that the dependency is satisfied through the inclusion of a component that is hierarchical to the one required; and

(*) indicates that the TOE does not satisfy this dependency. Refer to the supporting rationale following .

Table 26 Dependency Analysis

Component Reference	Requirement	Dependencies	Mapping
Functional Requirements			
	FAU_GEN.1	FPT_STM_SWT_EXP.1	29
	FAU_SAR.1	FAU_GEN.1	1
	FCS_CKM.1(1) through (3)	FCS_COP.1, FCS_CKM.4, FMT_MSA.2*	7, 4, *
	FCS_CKM.4	FCS_CKM.1, FMT_MSA.2*	3, *

Table 26 Dependency Analysis

Component Reference	Requirement	Dependencies	Mapping
	FCS_COP.1 (1) through (3)	FCS_CKM.1*, FCS_CKM.4*, FMT_MSA.2*	*, *, *
	FCS_COP.1 (4)	FCS_CKM.1*, FCS_CKM.4*, FMT_MSA.2*	*, *, *
	FCS_COP.1 (5)	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2*	3, 4, *
	FDP_IFC.1(1)	FDP_IFF.1(1)	9
	FDP_IFF.1(1)	FDP_IFC.1(1), FMT_MSA.3	8, 22
	FDP_IFC.1(2)	FDP_IFF.1(2)	11
	FDP_IFF.1(2)	FDP_IFC.1(2), FMT_MSA.3	10, 22
	FDP_IFC.1(3)	FDP_IFF.1(3)	13
	FDP_IFF.1(3)	FDP_IFC.1(3), FMT_MSA.3	12, 22
	FAU_STG.1	FAU_GEN.1	1
	FIA_ATD.1	None	-
	FIA_UAU.2	FIA_UID.1	18(H)
	FIA_UAU.5(1) and (2)	None	-
	FIA_UID.2(1) and (2)	None	-
	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	26, 25
	FMT_MSA.1	FDP_IFC.1(1), FMT_SMR.1, FMT_SMF.1	8, 26, 25
	FMT_MSA.2	ADV_SPM*, FDP_IFC.1(1), FMT_MSA.1, FMT_SMR.1	*, 8, 20, 26
	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	20, 26
	FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	26, 25
	FMT_SAE.1	FMT_SMR.1, FPT_STM_SWT_EXP.1	26, 29
	FMT_SMF.1	None	-
	FMT_SMR.1	FIA_UID.1	18(H)
	FMT_SMR.3	FMT_SMR.1	26
	FPT_SEP.1, FPT_RVM.1	None	-
	FPT_STM_SWT_EXP.1	None	-
	FTA_SSL_SWI_EXP.3	None	-
	FTA_TSE.1	None	-
	FTP_ITC.1	None	-
Assurance Requirements			

Table 26 Dependency Analysis

Component Reference	Requirement	Dependencies	Mapping
	ACM_CAP.3	ACM_SCP.1, ALC_DVS.1	34, 42
	ACM_SCP.1	ACM_CAP.3	33
	ADO_DEL.1	None	-
	ADO_IGS.1	AGD_ADM.1	40
	ADV_FSP.1	ADV_RCR.1	39
	ADV_HLD.2	ADV_FSP.1, ADV_RCR.1	37, 39
	ADV_RCR.1	None	-
	AGD_ADM.1	ADV_FSP.1	37
	AGD_USR.1	ADV_FSP.1	37
	ALC_DVS.1	None	-
	ALC_FLR.1	None	-
	ATE_COV.2	ADV_FSP.1, ATE_FUN.1	37, 46
	ATE_DPT.1	ADV_HLD.1, ATE_FUN.1	38, 46
	ATE_FUN.1	None	-
	ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	37, 40, 41, 46
	AVA_MSU.1	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1	36, 37, 40, 41
	AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	37, 38
	AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	37, 38, 40, 41

The following dependencies are not satisfied in this Security Target:

- ADV_SPM.1
- FCS_CKM.1 and FCS CKM.4 (for FCS_COP.1 (1) and FCS_COP.1 (4) only)

ADV_SPM.1 is identified as a dependency of FMT_MSA.2, which in turn is identified as a dependency for FCS_CKM.1(1) through (3), FCS_CKM.4, FCS_COP.1 (1)through (5). The intent of FMT_MSA.2 is that values for security attributes must not violate the TSP. In the context of the FCS family, FMT_MSA.2 requires that the combination of cryptographic security attributes such as key length, key validity period and key use (e.g. digital signature, key encryption, data encryption) may only be set to values which maintain the 'secure state' of the TOE. By ensuring that the TOE configuration is configured in accordance with the evaluated guidance and is suitably password protected in accordance with the secure usage assumptions A.PERSONNEL and A.PASSWORD, the security attributes of the TOE will be set to values which maintain a secure state; therefore, the dependency of FMT_MSA.2 on ADV_SPM.1 is satisfied (as per Section H2, paragraph 1015 of CC v2.2 part 2).

FCS_CKM.1 and FCS_CKM.4 is identified as a dependency for FCS_COP.1 (1) and FCS_COP.1 (4). The cryptographic operations 'Local Database Password Encryption and Database Initial Connection Encryption' and 'hashing on the shared secret password' are implemented by the one-way functions MD5 and SHA-1 that do not require cryptographic keys for operation. Therefore, the requirements FCS_COP.1 (1) and FCS_COP.1 (4) are met without satisfying this dependency.

Rationale for Explicitly Stated Security Requirements

The table below presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Table 27 Explicitly Stated Requirement Rationale

Explicit Requirement	Identifier	Rationale
FPT_STM_SWT_EXP.1.1	Switch Reliable Time Stamps	This requirement is necessary because the CC version of FPT_STM.1 does not specify portions of the TOE. This is specific to the MDS switch component. This requirement is split between the TOE and the environment.
FTA_SSL_SWI_EXP.3	TSF-initiated termination	This requirement is necessary because the CC version of FTA_SSL.1 does not specify portions of the TOE. This is specific to the MDS switch component.
FPT_STM_ENV_EXP.1.1	Environment Reliable Time Stamps	This requirement is necessary because the CC version of FPT_STM.1 does not allow the time stamp source to be split. This is specific to the host OS for the Fabric Manager in the TOE environment. This requirement is split between the TOE and the environment.
FPT_STG_ENV_EXP.1	Protection of the Fabric Manager	This requirement is necessary because no CC FPT requirements exist for protection of configuration files and the storage database on a host OS.

TOE Summary Specification Rationale

IT Security Functions Satisfy the SFRs

This section shows that each SFR is mapped to at least one IT security function and each IT security function is mapped to at least one SFR.

Table 28 Mapping of SFRs to IT Security Functions

Security Functional Requirement	IT Security Function
FAU_GEN.1	AL.AUDIT, SP.TIMESOURCE
FAU_SAR.1	AL.AUDIT
FCS_CKM.1(1)	ES.SSH
FCS_CKM.1(2) and (3)	ES.ENCRYPT
FCS_CKM.4	ES.SSH
FCS_COP.1 (1) through (3)	ES.ENCRYPT

Table 28 Mapping of SFRs to IT Security Functions

Security Functional Requirement	IT Security Function
FCS_COP.1 (4)	ES.DH-CHAP
FCS_COP.1 (5)	ES.SSH, IA.LOGIN
FDP_IFC.1(1)	AC.ZONES, AC.LUNZONES
FDP_IFF.1(1)	AC.ZONES, AC.LUNZONES
FDP_IFC.1(2)	AC.IPACL
FDP_IFF.1(2)	AC.IPACL
FDP_IFC.1(3)	CO.VSAN, SM.NETWORK-ADMIN
FDP_IFF.1(3)	CO.VSAN, SM.NETWORK-ADMIN
FIA_ATD.1	SM.ROLE, IA.USERS, ACC.RBAC
FIA_UAU.2	IA.LOCAL, IA.LOGIN
FIA_UAU.5(1)	IA.LOCAL, IA.LOGIN, IA.SWITCH&HOST, ES.SSH
FIA_UID.2(1)	IA.LOCAL, IA.LOGIN
FMT_MOF.1	SM.ROLE, SM.NETWORK-ADMIN
FMT_MSA.1	SM.ROLE, SM.NETWORK-ADMIN, ACC.RBAC
FMT_MSA.2	SM.ROLE, SM.NETWORK-ADMIN, ACC.RBAC
FMT_MSA.3	SM.ROLE, SM.NETWORK-ADMIN
FMT_MTD.1	SM.ROLE, SM.NETWORK-ADMIN
FMT_SAE.1	SM.NETWORK-ADMIN, IA.SWITCH&HOST, ACC.RBAC
FMT_SMF.1	SM.NETWORK-ADMIN
FMT_SMR.1	SM.ROLE, ACC.RBAC, IA.EXTERNAL
FMT_SMR.3	SM.ROLE, SM.NETWORK-ADMIN, IA.EXTERNAL
FPT_SEP.1(1)	SM.NETWORK-ADMIN, SP.DOMAIN
FPT_RVM.1(1)	SM.NETWORK-ADMIN, SP.DOMAIN
FPT_STM_SWT_EXP.1	SP.TIMESOURCE
FTA_SSL_SWI_EXP.3	CM.CONTROLS
FTA_TSE.1	CM.MONITOR, AC.PORT, AC.FABRICBIND, AC.ZONES, AC.LUNZONES, AC.IPACL
FTP_ITC.1	AC.PORT, AC.FABRICBIND, AC.ZONES, AC.LUNZONES, AC.IPACL

Table 29 Mapping of IT Security Functions to SFRs

IT Security Function	Security Functional Requirement
SM.ROLE	FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1, FMT_SMR.3
SM.NETWORK-ADMIN	FDP_IFC.1(3), FDP_IFF.1(3), FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SAE.1, FMT_SMF.1, FPT_SEP.1(1), FPT_RVM.1(1), FMT_SMR.3
AC.PORT	FDP_IFC.1(1), FDP_IFF.1(1), FTA_TSE.1, FTP_ITC.1
AC.FABRICBIND	FTA_TSE.1, FTP_ITC.1
AC.ZONES	FDP_IFC.1(1), FDP_IFF.1(1), FTA_TSE.1, FTP_ITC.1
AC.LUNZONES	FDP_IFC.1(1), FDP_IFF.1(1), FTA_TSE.1, FTP_ITC.1
AC.IPACL	FDP_IFC.1(2), FDP_IFF.1(2), FTA_TSE.1, FTP_ITC.1
ACC.RBAC	FIA_ATD.1, FMT_MSA.1, FMT_MSA.2, FMT_SMR.1, FMT_SAE.1
AL.AUDIT	FAU_GEN.1, FAU_SAR.1,
CM.CONTROLS	FTA_SSL_SWI_EXP.3
CM.MONITOR	FTA_TSE.1
ES.ENCRYPT	FCS_CKM.1(1) through (3), FCS_COP.1 (1) through (3)
ES.SSH	FCS_CKM.1(1), FCS_CKM.4, FCS_COP.1 (5), FIA_UAU.5(1)
ES.DH-CHAP	FCS_COP.1 (4)
IA.USERS	FIA_ATD.1
IA.LOCAL	FIA_UAU.2, FIA_UID.2(1), FIA_UAU.5(1)
IA.SWITCH&HOST	FIA_UAU.5(1), FMT_SAE.1
IA.LOGIN	FCS_COP.1(5), FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2(1)
IA.EXTERNAL	FMT_SMR.1, FMT_SMR.3
CO.VSAN	FDP_IFC.1(3), FDP_IFF.1(3)
SP.DOMAIN	FPT_SEP.1(1), FPT_RVM.1(1)
SP.TIMESOURCE	FAU_GEN.1, FPT_STM_SWT_EXP.1

IT Security Function Suitability

This section provides appropriate justification that the IT Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

Table 30 Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FAU_GEN.1	This TOE SFR is satisfied by the security functions AL.AUDIT and SP.TIMESOURCE as: AL.AUDIT provides for the generation of security-relevant audit records that are written to the accounting log. The accounting log represents a subset of the system log that stores all systems events and messages. SP.TIMESOURCE supports this requirement by providing a reliable timestamp for each audit record in the accounting log.
FAU_SAR.1	This TOE SFR is satisfied by the security function AL.AUDIT as: AL.AUDIT provides the capability to review the audit records stored in the accounting log. The accounting log is stored locally on the TOE.
FCS_CKM.1(1)	This TOE SFR is satisfied by the security function ES.SSH as: ES.SSH provides the mechanism to generate the public and private keys for hosts and users requiring secure access to the TOE via the OpenSSH Version 2 protocol.
FCS_CKM.1(2)	This TOE SFR is satisfied by the security function ES.ENCRYPT as: ES.ENCRYPT provides the mechanism to generate the keys for use in encrypting end-user passwords stored in the PostgreSQL database with the DES algorithm.
FCS_CKM.1(3)	This TOE SFR is satisfied by the security function ES.ENCRYPT as: ES.ENCRYPT provides the mechanism to generate the keys for use in encrypting the database password stored in the Fabric Manager configuration files with the Blowfish algorithm
FCS_CKM.4	This TOE SFR is satisfied by the security function ES.SSH as: ES.SSH provides the capability to delete all cryptographic keys used by the TOE by overwriting the key data stored on the local disk.
FCS_COP.1 (1)	This TOE SFR is satisfied by the security function ES.ENCRYPT as: ES.ENCRYPT implements the one-way hash algorithm (MD5) used to encrypt each user's password stored in the local password file on the local switch and the local database password on the database. The TOE also uses MD5 hashing to encrypt the initial connection data that is transferred between the Fabric Manager and the PostgreSQL database.
FCS_COP.1 (2)	This TOE SFR is satisfied by the security function ES.ENCRYPT as: ES.ENCRYPT implements the Blowfish algorithm to encrypt the database password where it is locally stored within the Fabric Manager configuration files.

Table 30 Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FCS_COP.1 (3)	This TOE SFR is satisfied by the security function ES.ENCRYPT as: ES.ENCRYPT implements the DES algorithm to encrypt each end-user's password stored in FMUSERS and SNMPUSERS tables in the PostgreSQL database.
FCS_COP.1 (4)	This TOE SFR is satisfied by the security function ES.DH-CHAP as: ES.DH-CHAP implements the one-way hash algorithm (MD5 or SHA-1) used to encrypt the shared secret password used to establish the identities of switches and hosts using the DH-CHAP authentication protocol.
FCS_COP.1 (5)	This TOE SFR is satisfied by the security functions ES.SSH and IA.LOGIN as: ES.SSH implements the cryptographic operation responsible for performing session key encryption and decryption based on the user or host public key stored in the corresponding profile or hosts file. Encryption and decryption of the session key is required for each end point during an SSH session so that the authenticity of the user or host can be verified. IA.LOGIN enforces the use of SSH for remote management.
FDP_IFC.1(1)	This TOE SFR is satisfied by the security functions AC.ZONES and AC.LUNZONES as: AC.ZONES allows the TOE privileged user to create and maintain zones to set up access control between storage devices or user groups within the same VSAN based on WWN port and switch credentials, FC ID, interface and domain IDs and IP addresses AC.LUNZONES allows the TOE privileged user to create and maintain zones to set up access control between storage devices using their logical unit number (LUN)
FDP_IFF.1(1)	This TOE SFR is satisfied by the security functions AC.ZONES and AC.LUNZONESas: AC.ZONES allows the TOE privileged user to create and maintain zones to set up access control between storage devices or user groups within the same VSAN based on WWN port and switch credentials, FC ID, interface and domain IDs and IP addresses AC.LUNZONES allows the TOE privileged user to create and maintain zones to set up access control between storage devices using their logical unit number (LUN)
FDP_IFC.1(2)	This TOE SFR is satisfied by the security function AC.IPACL as: AC.IPACL allows the TOE privileged user to create and maintain IP-based access control lists for management traffic traveling over Ethernet and/or IP over Fibre Channel to enter or exit the TOE based on a list of permit and deny operations
FDP_IFF.1(2)	This TOE SFR is satisfied by the security function AC.IPACL as: AC.IPACL permits or denies IP-based management traffic to enter or exit the TOE based on pre-defined IP access control lists

Table 30 Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FDP_IFC.1(3)	This TOE SFR is satisfied by the security functions CO.VSAN and SM.NETWORK-ADMIN as: CO.VSAN provides the traffic isolation feature of VSAN implementation that allows each network fabric to separate from each other using a hardware-based tagging mechanism on VSAN member ports and EISL links, resulting in the absolute separation of user groups. SM.NETWORK-ADMIN allows users with the network-admin (sw) role to create multiple logical SANs (i.e. VSANs) over the common network infrastructure
FDP_IFF.1(3)	This TOE SFR is satisfied by the security functions CO.VSAN and SM.NETWORK-ADMIN as: CO.VSAN provides the traffic isolation feature of VSAN implementation that allows each network fabric to separate from each other using a hardware-based tagging mechanism on VSAN member ports and EISL links, resulting in the absolute separation of user groups. SM.NETWORK-ADMIN allows users with the network-admin (sw) role to create multiple logical SANs (i.e. VSANs) over the common network infrastructure
FIA_ATD.1	This TOE SFR is satisfied by the security functions SM.ROLE ,IA.USERS and ACC.RBAC as: SM.ROLE creates and maintains the roles assigned to each user within the SAN fabric that is used in the identification and authentication of users IA.USERS creates and maintain the identities and passwords of the users which are used as the primary credentials for user identification and authentication ACC.RBAC implements role based access control based on user roles maintained by SM.ROLE
FIA_UAU.2	This TOE SFR is satisfied by the security functions IA.LOCAL and IA.LOGIN as: IA.LOCAL allows for users to be identified and authenticated prior to allowing any TSF mediated actions to be performed. IA.LOGIN ensures that each user must be successfully authenticated prior to accessing the TSF mediated functions of the TOE.

Table 30 Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FIA_UAU.5(1)	This TOE SFR is satisfied by the security functions IA.LOCAL, IA.LOGIN, IA.SWITCH&HOST and ES.SSH as: IA.LOCAL provides the local authentication mechanism for each CLI or SNMP user based on the username and password combination IA.LOGIN enforces the use of the Identification and Authentication mechanisms of the TOE. IA. SWITCH&HOST provides the authentication mechanism to support switch to switch or switch to host authentication based on the shared secret password and iSCSI host authentication when requesting access to storage devices within the SAN fabric ES.SSH supports the authentication mechanism by performing session key encryption and decryption based on the user or host public key to enable secure remote management access to the TOE
FIA_UID.2(1)	This TOE SFR is satisfied by the security functions IA.LOCAL and IA.LOGIN as: IA.LOCAL allows for users to be identified and authenticated prior to allowing any TSF mediated actions to be performed. IA.LOGIN ensures that each user must be successfully authenticated prior to accessing the TSF mediated functions of the TOE.
FMT_MOF.1	This TOE SFR is satisfied by the security functions SM.ROLE and SM.NETWORK-ADMIN as: SM.ROLE ensures that only those users with privileged roles may access the security management functions of the TOE SM.NETWORK-ADMIN role is the main switch role with full access to the TOE security management functions and configuration.
FMT_MSA.1	This TOE SFR is satisfied by the security functions SM.ROLE, SM.NETWORK-ADMIN and ACC.RBAC as: SM.ROLE ensures that only those users with privileged roles may access the security management functions of the TOE altering the access control and information flow control policies SM.NETWORK-ADMIN role is the main switch role with full access to the TOE security management functions and configuration. ACC.RBAC enforces role based access to the TSF configuration.

Table 30 Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FMT_MSA.2	This TOE SFR is satisfied by the security functions SM.ROLE and SM.NETWORK-ADMIN: SM.ROLE ensures that only those users with privileged roles may access the security management functions of the TOE altering the access control and information flow control policies SM.NETWORK-ADMIN role is the main switch role with full access to the TOE security management functions and configuration. ACC.RBAC enforces role based access to the TSF configuration so that only the trusted administrator roles may configure the TOE.
FMT_MSA.3	This TOE SFR is satisfied by the security functions SM.ROLE and SM.NETWORK-ADMIN as: SM.ROLE ensures that only those users with privileged roles may access the security management functions of the TOE and specify restrictive default values for security attributes SM.NETWORK-ADMIN role is the main switch role with full access to the TOE security management functions and configuration.
FMT_MTD.1	This TOE SFR is satisfied by the security functions SM.ROLE and SM.NETWORK-ADMIN as: SM.ROLE ensures that only those users with privileged roles may access the security management functions of the TOE that access the TSF configuration SM.NETWORK-ADMIN role is the main switch role with full access to the TOE security management functions and configuration.
FMT_SAE.1	This TOE SFR is satisfied by the security functions SM.NETWORK-ADMIN, IA. SWITCH&HOST and ACC.RBAC as: SM.NETWORK-ADMIN role is the main switch role with full access to the TOE security management functions and configuration including specifying the default timeout value for DH-CHAP authentication between switches and hosts IA.SWITCH&HOST provides the authentication mechanism to support switch to switch or switch to host authentication and implements a forced timeout value during the DH-CHAP authentication attempt ACC.RBAC enforces role based access control, restricting the capability to configure DH-CHAP authentication timeout values to users associated with the network-admin (sw) role or an appropriately privileged user role.
FMT_SMF.1	This TOE SFR is satisfied by the security functions SM.NETWORK-ADMIN as: SM.NETWORK-ADMIN role performs all of the security management functions for the TOE

Table 30 Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FMT_SMR.1	This TOE SFR is satisfied by the security functions SM.ROLE, ACC.RBAC, and IA.EXTERNAL as: SM.ROLE ensures that only those users with privileged roles may access the security management functions of the TOE that access the TSF configuration, and associate users with their roles ACC.RBAC implements role based access control based on user roles maintained by SM.ROLE IA.EXTERNAL allows for users authenticated by the remote AAA service to be associated with user roles.
FMT_SMR.3	This TOE SFR is satisfied by the security functions SM.ROLE, SM.NETWORK-ADMIN and IA.EXTERNAL as: SM.ROLE ensures that only those users with privileged roles may access the security management functions of the TOE that access the TSF configuration SM.NETWORK-ADMIN role is the main switch role with full access to the TOE security management functions and configuration. IA.EXTERNAL allows for users authenticated by the remote AAA service to be associated with privileged user roles.
FPT_SEP.1(1)	This TOE SFR is satisfied by the security functions SM.NETWORK-ADMIN and SP.DOMAIN as: The TOE provides protection mechanisms for its security functions, such as the restricted ability that only users with a privileged role can perform administrative actions on the TOE (SM.NETWORK-ADMIN). Another protection mechanism is that on the switch all functions of the TOE are confined to the device itself (SP.DOMAIN). The TOE is completely self-contained, and therefore, maintains its own execution domain. Protection of the Fabric Manager is provided by the host OS.
FPT_RVM.1(1)	This TOE SFR is satisfied by the security functions SM.NETWORK-ADMIN and SP.DOMAIN as: The TOE provides protection mechanisms for its security functions, such as the restricted role mechanism that requires that the identification and authentication mechanism be invoked and succeed prior to performing administrative actions on the TOE (SM.NETWORK-ADMIN). Another protection mechanism is that on the switch all functions of the TOE are confined to the device itself (SP.DOMAIN). The TOE is completely self-contained, and therefore, requires enforcement of the TSP prior to execution of functionality. Protection of the Fabric Manager is provided by the host OS.
FPT_STM_SWT_EXP.1	This TOE SFR is satisfied by the security function SP.TIMESOURCE as: SP.TIMESOURCE internal time source security function is used to ensure that each audited event contains a date and time stamp for that event. The TOE time source may be synchronized with an external NTP server.

Table 30 Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FTA_SSL_SWI_EXP.3	This TOE SFR is satisfied by the security function CM.CONTROLS as: CM.CONTROLS allows the TOE to enforce the shell and terminal session timeout values (default of 30 minutes) so that when the time period has elapsed the user or terminal session is terminated.
FTA_TSE.1	This TOE SFR is satisfied by the security functions CM.MONITOR, AC.PORT, AC.FABRICBIND, AC.ZONES, AC.LUNZONES, and AC.IPACL as: CM.MONITOR allows the TOE to enforce an expiry date on a user's account to prevent further access and therefore session establishment AC.PORT allows the TOE to reject session establishment based on the switch WWN identifiers for each port AC.FABRICBIND allows the TOE to reject session establishment for interconnected switches based on the identities authenticated by DH-CHAP AC.ZONES allows the TOE to reject session establishment for devices and use groups based on WWN port and switch credentials, FC ID, interface and domain IDs and IP addresses AC.LUNZONES allows the TOE to reject session establishment for storage devices based on their logical unit number AC.IPACL allows the TOE to reject session establishment for management traffic traveling over Ethernet and/or IP over Fibre Channel based on the source/destination IP address and TCP/UDP number
FTP_ITC.1	This TOE SFR is satisfied by the security functions AC.PORT, AC.FABRICBIND, AC.ZONES, AC.LUNZONES, and AC.IPACL as: AC.PORT allows the TOE privileged user to create and maintain access control lists to its ports based on switch WWN identifiers for each port. AC.FABRICBIND allows the TOE privileged user to create and maintain access control permissions to bind interconnected switches (instances of the TOE) based on the identities authenticated by DH-CHAP AC.ZONES allows the TOE privileged user to create and maintain zones to set up access control between storage devices or user groups within the same VSAN based on WWN port and switch credentials, FC ID, interface and domain IDs and IP addresses AC.LUNZONES allows the TOE privileged user to create and maintain zones to set up access control between storage devices using their logical unit number (LUN) AC.IPACL allows the TOE privileged user to create and maintain IP-based access control lists for management traffic traveling over Ethernet and/or IP over Fibre Channel based on the source/destination IP address and TCP/UDP number

Demonstration of Mutual Support

The mutual supportiveness of the TOE security functional requirements and security functions can be demonstrated by an analysis of those requirements that help prevent bypass, tampering, and de-activation of the SFRs. It can also be demonstrated by determining which requirements and functions enable the detection of these types of attacks and by referring to the results of the previous analyses performed in this chapter. The results of this combined analysis are presented below.

Help Prevent Bypassing of Other SFRs

FIA_UID.2(1), FIA_UID.2(2), and FIA_UAU.2 support other functions that allow user access to the assets by restricting actions that the user can take before being authorized.

The management functions FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FMT_SMR.3 support all other SFRs by restricting the ability to change security management functions to a user with a privileged role (e.g. network-admin roles), exclusively, ensuring that other users cannot circumvent the SFRs.

FMT_MOF.1, FMT_MSA.2, FMT_MSA.3, FMT_SMR.3, limit the acceptable values for secure access and security data, and protects the SFRs dependent on those values from being bypassed.

Help Prevent Tampering of Other SFRs

FIA_UID.2(1), FIA_UID.2(2), and FIA_UAU.2 support other actions that allow the user access to the TOE by restricting the actions that the user can take before being authorized.

FIA_ATD.1 and FMT_MSA.1 support all other SFRs by restricting the ability to change privileges and associated management functions to authorized users, thus ensuring that other users cannot tamper with these SFRs.

FTA_TSE.1 and FTA_SSL_SWI_EXP.3support all other SFRs by denying system access and session establishment by restricting unauthorized user access and session inactivity levels.

Help Prevent de-activation of Other SFRs

The access control actions governed by FDP_IFC.1 and FDP_IFF.1 act together with other SFRs to provide control of allowed data access and traffic flow, preventing unauthorized de-activation of SFRs.

FMT_MSA.1 supports all other SFRs by restricting the ability to change privileges and associated management functions to authorized users, thus ensuring that other users cannot tamper with these SFRs.

FMT_MOF.1, FMT_MSA.2, FMT_MSA.3, FMT_SMR.3, limit the acceptable values for secure access and security data, and protects the SFRs dependent on those values from being bypassed.

FIA_UID.2(1), FIA_UID.2(2), and FIA_UAU.2 support other actions that allow the user access to the TOE by restricting the actions that the user can take before being authenticated.

Other Analyses Performed

The dependency analysis provided at and the analyses provided in, and Table 29 demonstrate that the IT security functions work together to satisfy the TSFs, that is, they demonstrate mutual support between function components.

By definition, all assurance requirements support all SFRs since they provide confidence in the correct implementation and operation of the SFRs.

This analysis of the security functional and assurance requirements demonstrates that there are no conflicts between requirements. Therefore, the security requirements together form a mutually supportive and consistent whole.

Assurance Security Requirements Rationale

The table below shows that all Security Assurance Requirements (SARs) are met by the assurance measures.

Table 31 Mapping of SARs to Assurance Measures

Security Assurance Requirements	Assurance Measures
ACM_CAP.3	CM-DEL
ACM_SCP.1	CL
ADO_DEL.1	CM-DEL
ADO_IGS.1	AGD
ADV_FSP.1	FSP
ADV_HLD.2	HLD
ADV_RCR.1	RCR
AGD_ADM.1	AGD
AGD_USR.1	AGD
ALC_DVS.1	DEV_SEC
ALC_FLR.1	CM-DEL
ATE_COV.2	COV-DPT
ATE_DPT.1	COV-DPT
ATE_FUN.1	COV-DPT
ATE_IND.2	COV-DPT
AVA_MSU.1	AGD
AVA_SOF.1	VLA-SOF
AVA_VLA.1	VLA-SOF

Given that all security assurance requirements are met by at least one assurance measure and that the implementation of each assurance measure will be the subject of evaluation activities, it is concluded that all of the assurance measures will meet all of the security assurance requirements.

Since non-administrative users have no direct interaction with the TOE, no non-administrative user guidance is required. Therefore the assurance requirement AGD_USR.1 does not apply to this evaluation.

CC EAL3 provides design information down to the High-Level Design, which is sufficient for the completion of an analysis of the strength of function, independent, and developer testing of security functions and includes analysis of obvious vulnerabilities for the TOE. Additionally, ALC_FLR.1 provides for basic flaw remediation allowing for identified security flaws in the TOE to be updated in a controlled manner. Therefore CC EAL3 provides consumers with a low to moderate level of independently assured security services and is considered an appropriate level of assurance for the TOE.

Strength of Function Claims

The minimum Strength of Function for the TOE is **SOF-Basic**.

The security functional requirements FIA_UAU.2 and FIA_UAU.5(1) provide the basis for the password mechanism. Passwords are inherently probabilistic and as such require a strength of function claim. The strength of function of the password in the TOE is SOF-Basic. The strength of function claim is based on the correct administration of the TOE. The assumptions to support the SOF claim are A.NOEVIL and A.PERSONNEL. These assumptions ensure that the TOE is configured correctly and that administrators are trusted personnel and assume the organization has appropriate security policies in place to protect its assets.

The TOE security function for the identification & authentication mechanisms (IA.LOCAL, IA.USERS, IA.SWITCH&HOST and IA.LOGIN) inherits the SOF claim above, as it implements the password requirements from the relevant security functional requirements identified above.

The security functional requirements FIA_UAU.5(1), FCS_COP.1 (1) through (3), FCS_COP.1 (4) and FCS_COP.1(5) specify several cryptographic-based mechanisms used to hash the shared secret password for the DH-CHAP and CHAP authentication protocols, or to hash or encrypt the password entries stored in the local password files. Determination of the strength of function for cryptographic functions is out of scope of the Common Criteria. Therefore, no SOF claim for these requirements (and their corresponding security functions) has been specified for this TOE.

The minimum strength claim for SOF-Basic is appropriate for this TOE as it is sufficient to protect against an attacker with a low attack potential, i.e. attackers with high resources, high skill and low motivation. Additionally, it is consistent with the evaluation level of EAL 3 and the testing that is carried out for that level of assurance.

Rationale for Extensions

This ST does not contain any extended or explicitly stated security requirements.

PP Claims Rationale

This ST makes no PP conformance claim therefore no rationale is required.

Appendix A – Switch Modules in the Scope of Evaluation

The following table shows the various modules that may be optionally included in a switch whilst running in the evaluated configuration.

Module	Related Documentation
Cisco MDS 9500 Series Supervisor Module	Cisco MDS 9500 Series Supervisor Module Data Sheet
Cisco MDS 9000 Family Multiprotocol Services Module	Cisco MDS 9000 Family Multiprotocol Services Module Data Sheet
Cisco MDS 9000 Family Storage Services Module	Cisco MDS 9000 Family Storage Services Module Data Sheet
Cisco MDS 9000 IP Storage Services Modules	Cisco MDS 9000 IP Storage Services Modules Data Sheet
Cisco MDS 9000 Family Fibre Channel Switching Modules	Cisco MDS 9000 Family Fibre Channel Switching Modules Data Sheet

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html