National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

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

Report Number: CCEVS-VR-VID10015-2008
Dated: 25 September 2008
Version: 1.1

**National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899**

**National Security Agency
Information Assurance Directorate
9800 Savage Road Suite 6757
Fort George Meade, MD 20755-6757**

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Cisco MDS 9000 Family with SAN-OS Release 3.2(2c) was performed by the ARCA Common Criteria Testing Laboratory in the United States and was completed on September 17, 2008. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, Evaluation Assurance Level 3, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 2.2.

The ARCA Common Criteria Testing Laboratory is an approved National Information Assurance Partnership (NIAP) Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 3 (EAL3) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of the Cisco MDS 9000 by any agency of the US Government and no warranty of the product is either expressed or implied.

The cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

1.1 Cisco MDS 9000 Functionality

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

1.2 Evaluation Details

Table 1 below provides the required evaluation identification details.

Item	Identification
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	Cisco MDS 9000 Family with SAN-OS Release 3.2(2c)
EAL	EAL3
Protection Profile	None
Security Target	Cisco MDS 9000 Family SAN-OS Release 3.2(2c) Security Target, Version 3.0, August 2008
Developer	Decisive Analytics/Cisco Systems
Evaluators	Rick West and Ken Dill ARCA CCTL 45901 Nokes Boulevard Sterling, VA 20166
Validators	Ken Eggers and John Nilles
Dates of Evaluation	20 July 2004 to 25 June 2008
Conformance Result	Part 2 extended; and Part 3 EAL 3 augmented with ALC_FLR.1.
Common Criteria (CC) Version	CC, version 2.2, January 2004

Table 1: Evaluation Details

1.3 Interpretations

Following is a table that defines which CCIMB Interpretations that were effective on or before the kick-off date July 20th 2004 were applied to this evaluation:

Number	Title
I-0432	List Of Subjects And Objects Refers To Types Thereof
I-0347	Including Sensitive Information In Audit Records
I-0420	Attribute Inheritance/Modification Rules Need To Be Included In Policy
I-0459	CM Systems May Have Varying Degrees Of Rigor And Function
I-0407	Empty Selections Or Assignments
I-0410	Auditing Of Subject Identity For Unsuccessful Logins
I-0414	Site-Configurable Prevention Of Audit Loss
I-0429	Selecting One Or More
I-0421	Application Notes In Protection Profiles Are Informative Only
I-0427	Identification Of Standards
I-0375	Elements Requiring Authentication Mechanism
I-0405	American English Is An Acceptable Refinement
I-0418	Evaluation Of The TOE Summary Specification:Part 1 Vs Part 3
I-0422	Clarification Of ``Audit Records''
I-0426	Content Of PP Claims Rationale
I-0378	Meaning Of Compliance Claims
I-0379	How To Require User/Admin Documentation For Functional Components

Table 2: Applicable International Interpretations

The Evaluation Team also complied with the CCEVS Precedents identified in Table 3

Precedent	**Precedent Title**
PD-106	Situations Where AGD_USR May Be Vacuously Satisfied
PD-90	TOE Labels
PD-84	Evaluation of TOE claiming compatibility with multiple IT environments
PD-63	What Information Must Be Provided in the TSS Rationale?
PD-62	What Must Be Tested for an ST Running On Multiple Platforms?
PD-56	Exhaustiveness of ATE_IND Testing
PD-54	What is an appropriate TOE Reference?
PD-8	When should monitoring of the public domain for new 'obvious vulnerabilities' cease?

Table 3: CCEVS Precedents Applied to the Evaluation

2. Identification of the TOE

The Target of Evaluation (TOE) is a Storage Area Network (SAN) solution consisting of the SAN-OS operating system running on the MDS 9000 family of Multilayer Directors and Fabric Switches. The MDS 9000 family of Directors and switches provides the infrastructure that ties together file servers and back end storage. The TOE includes Fabric Manager, a java based GUI for managing Directors/switches as an alternate to the CLI

The specific hardware and software that can be combined to form valid TOE configurations are identified below and described in section 5 of this document.

Hardware	Software
MDS 9506 Multilayer Director, MDS 9509 Multilayer Director, MDS 9513 Multilayer Director, MDS 9216 Multilayer Fabric Switch, MDS 9216A Multilayer Fabric Switch, MDS 9216i Multilayer Fabric Switch, MDS 9140 Multilayer Fabric Switch, MDS 9120 Multilayer Fabric Switch, Ethernet, Fibre Channel, Serial Port, Cisco MDS 9500 Series Supervisor Module, Cisco MDS 9500 Series Supervisor 2 Module, Cisco MDS 9000 Family Multiprotocol Services Module, Cisco MDS 9000 Family Storage Services Module, Cisco MDS 9000 IP Storage Services Modules, MDS 9000 Family Fibre Channel Switching Modules	SAN-OS Maintenance Release 3.2(2c), including Fabric Manager for SANOS 3.2(2c).

Table 4: Hardware and software that can be combined to form valid TOE configurations

3. Security Policy

The Security Functional Policies (SFPs) implemented by Cisco MDS 9000 are based on the following set of security policies:

- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Audit
- Cryptographic Support
- TOE Access
- Trusted Path/Channel

Note: Much of the description of the Cisco MDS 9000 security policy has been extracted and reworked from the Cisco MDS 9000 Security Target.

3.1 User Data Protection

3.1.1 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 and destination ID fields, which can be world wide names (WWNs), IP addresses, or Fibre Channel Identifiers. Logical Unit Number (LUN) zoning ensures that LUNs are accessible only by specific hosts.

Zoning 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 would be required to provide an optimal solution.

3.1.2 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. 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 IBM Fiber Connection (FICON), VSANs ensure that there is true hardware-based separation of FICON and open systems.

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.

3.1.3 IP-based Access Control Lists

IP-ACLs restrict IP-related 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.

3.2 Identification and Authentication

3.2.1 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 trusted 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.

3.2.2 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 Section 6.1.1.1 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.

3.2.3 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.

3.2.4 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.

3.3 Security 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.

3.3.1 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.

3.3.2 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 an alternative to the CLI for most switch configuration commands.

3.3.3 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 Section 6.1.1.1 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.

3.4 Protection of the TSF

3.4.1 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.

3.4.2 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.

3.5 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.

3.6 Cryptographic Support

3.6.1 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.

3.6.2 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.

3.6.3 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.

3.7 TOE Access

3.7.1 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.

3.7.2 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.

3.7.3 Port Security

The TOE can bind entities to fibre 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.

3.7.4 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.

3.8 Trusted Path/Channel

3.8.1 IP-based Access Control Lists

IP-ACLs restrict IP-related 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.

4. Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which the TOE is expected to operate.

4.1 Secure Usage Assumptions

The following assumptions are made in relation to the TOE:

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 trusted. 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.

Table 5: Secure Usage Assumptions

4.2 Threats to Security

The Threat agents against the TOE are attackers with expertise, resources, and motivation that combine to be a low attack potential. The TOE addresses the following threats:

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.

Table 6: Threats addressed by the TOE

5. Architectural Information

The following Physical Hardware and Software Included in the Target of Evaluation:

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.
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.
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 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
MDS 9000 Family Fibre Channel Switching Modules	A basic 16 or 32 port fibre channel switching module. This module expands the number of fibre 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.

Table 7: Architecture Details

6. Documentation

- Cisco MDS 9000 Family SAN-OS Release 3.2(2c) Security Target, Version 3.0, August 2008
- Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x Cisco MDS SAN-OS for Release 3.0(1) Through 3.2(2b), November 2007
- Cisco MDS 9000 Family Quick Configuration Guide
- Cisco MDS 9000 Family Command Reference, Cisco MDS SAN-OS Release 3.0(1) Through 3.2(2b), November 2007
- Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 3.x, Cisco MDS SAN-OS Release 3.0(3) Through 3.2(2b), November 2007
- Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide, November 2007
- Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.2(2c)
- Cisco MDS 9000 Family System Messages Reference, November 2007
- Cisco MDS 9000 Family MIB Quick Reference, November 2007
- Cisco MDS 9100 Series Hardware Installation Guide
- Cisco MDS 9216 Switch Hardware Installation Guide
- Cisco MDS 9500 Series Hardware Installation Guide
- Cisco MDS 9000 Family CWDM Passive Optical System Installation Note, June 2007
- Cisco MDS 9000 Family CWDM SFP Installation Note, June 2007
- Cisco MDS 9000 Family SSM Configuration Note, September 2007
- Cisco MDS 9000 Family Fabric Manager Server Database Schema - December 2006
- Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family
- Installation and Configuration for Common Criteria EAL3 Evaluated Cisco MDS 9000 Family – SAN-OS Release 3.2(2c), April 2008 Version 0-17

7. IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. The cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.1 Developer Testing

The developer performed a testing and coverage analysis, which examined each SFR and developed one or more Cisco test cases that verify the function or command requirement. These tests were documented in the EAL3 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions.

The developer testing addressed all the security functions claimed by the TOE. The developer used existing test cases to test the TOE. The evaluation team determined that the developer's test methodology met the coverage and depth requirements and that the actual test results matched the expected results.

The following hardware equivalence rationale addresses various TOE components and establishes what equivalent hardware is present in the test configuration and why that hardware subset is sufficient.

In the interests of efficiency, the evaluation team selected a subset of hardware platforms to test. The subset selected ensures that each software version is tested, and hardware product family is tested, though not all hardware models are tested. The rationale for this is that it is considered suitable that several versions TOE hardware that differ in non-security implementing functionality may be represented in the test setup by a TSF-equivalent component of TOE hardware. The TOE presents the same interfaces (TSFI) regardless of the hardware differences among different TOE models within each representative model set. Testing multiple configurations would not result in differences in test cases or procedures and would not yield different results. Some of the modules that are included in the TOE are available in several slot/performance backplane capacity configurations. In this situation, since the number of available interfaces does not impact of the security functionality of the TOE, modules of the same type but varying port density are considered equivalent from a security perspective.

The following hardware equivalence rationale addresses various TOE components and establishes what equivalent hardware is present in the test configuration and why that hardware subset is sufficient.

The subsets can be logically separated into 3 groupings:

Group A: 9506, 9509, 9513 Multi-layer Directors:

Group B: 9216, 9216A, 9216i Multi-layer Fabric Switch

Group C: 9100 Series Fabric Switches

Group	Model	Storage Networking Module	Tested by
A	9506	Cisco MDS 9000 Family 14/2-port Multiprotocol Services Module 16-port Fibre channel switching module	CCTL

		Supervisor-1 Module	
A	9509	IP Storage Services Module 16-port Fibre channel switching module Supervisor-1 Module	Vendor
A	9509	MDS 9000 1/2/4-Gbps 48-port Fibre Channel Switching Module Supervisor-1 Module	CCTL
	9513	16-port Fibre channel switching module Supervisor-1 Module	Vendor
	9513	24-port Fibre channel switching module 12-port Fibre channel switching module Supervisor-2 Module	CCTL
B	9216i	N/A (The 9216i module includes an integrated IP storage services module.)	Vendor and CCTL
C	Cisco 9100 Series	N/A	Vendor

Table 8: Hardware Subset Grouping

Hardware model group A

9506, 9509, 9513 Multi-layer Directors:

All hardware models in this group were tested.

Hardware model group B

9216i Multi-layer Fabric Switch:

All hardware models in this group were tested.

Hardware model group C

9100 Series Fabric Switches:

By selecting the 9140 TOE model, the evaluation team determined this group would be sufficiently tested. The 9120 is identical to the 9140, except it has fewer ports (20 versus 40). This was acceptable to the evaluation team.

Storage Networking Modules:

The storage networking modules in the TOE are categorized below:

- Cisco MDS 9500 Series Supervisor Module
- Cisco MDS 9500 Series Supervisor 2 Module
- Cisco MDS 9000 Family Multiprotocol Services Module
- Cisco MDS 9000 Family Storage Services Module
- Cisco MDS 9000 IP Storage Services Modules
- Cisco MDS 9000 Family Fibre Channel Switching Modules

The following modules were tested:

- Cisco MDS 9500 Series Supervisor Module
- Cisco MDS 9500 Series Supervisor 2 Module
- Cisco MDS 9000 Family Multiprotocol Services Module
- Cisco MDS 9000 IP Storage Services Modules
- Cisco MDS 9000 Family Fibre Channel Switching Modules

Features on the Cisco Multiprotocol Services Module (FC-IP and FICON) are disabled within the evaluated configuration.

Similarly, features on the IP Storage services module (FC-IP, Fibre Channel Write Acceleration, FICON) are disabled within the evaluated configuration.

This leaves the only difference among both modules to be Fibre channel port density.

The only module not tested was the Cisco MDS 9000 Family Storage Services Module.

This module, includes the following features:

- Fibre Channel switching.
- Fibre Channel Write Acceleration (FC-WA) and Small Computer System Interface (SCSI) flow-statistics monitoring.
- Network-Accelerated Serverless Backup with standards-based SCSI-2 EXTENDED COPY command.
- Network-Assisted Storage Applications with the SANTap protocol.
- Network-Hosted Storage Applications with the Fabric Application Interface Standard (FAIS)- based Intelligent Storage Application Programmatic Interface (ISAPI).

These features are further explained below:

1. Fibre Channel ports for native Fibre Channel communication;
2. The Fibre Channel Write Acceleration (FC-WA) and SCSI flow-statistics monitoring allows synchronous replication over greater distances by minimizing latency.
3. Network-Accelerated “serverless” Backup. This feature enables backup applications to use the network for data movement using the SCSI-2 Extended Copy command, thereby offloading I/O and processing from media servers.
4. Network-Assisted Storage Applications with the Cisco SANTap protocol. SANTap is a proprietary protocol that allows a storage appliance to get an I/O copy without impacting the integrity, availability, and performance of the primary I/O between servers and storage. The SSM intercepts I/O on the network and performs duplication for the purposes of secondary data processing functions such as data replication, continuous data protection, and data migration. Thus network-assisted storage applications can be deployed without appliances residing in the primary data path.
5. Network-Hosted Storage Applications with the Fabric Application Interface Standard (FAIS)- based Intelligent Storage Application Programming Interface (ISAPI). Cisco also provides an API that allows the SSM to be used for data-path transactions only

while control information flows through an external processor that the software vendor is responsible for maintaining. In this scenario, the SSM and external processor communicate either via an external IP network or in-band via IP over Fibre Channel.

Feature 1 above was sufficiently tested with the Fibre Channel Switching Modules.

Features 2-5 above are disabled within the TOE evaluated configuration. Therefore they do not impact the TSF and are not considered security relevant.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer.

The evaluation team performed a sample of the developer’s test suite and devised an independent set of team tests and penetration tests. The evaluation team reran a subset of the developer’s test suite that tested all of eight of the TSFs.

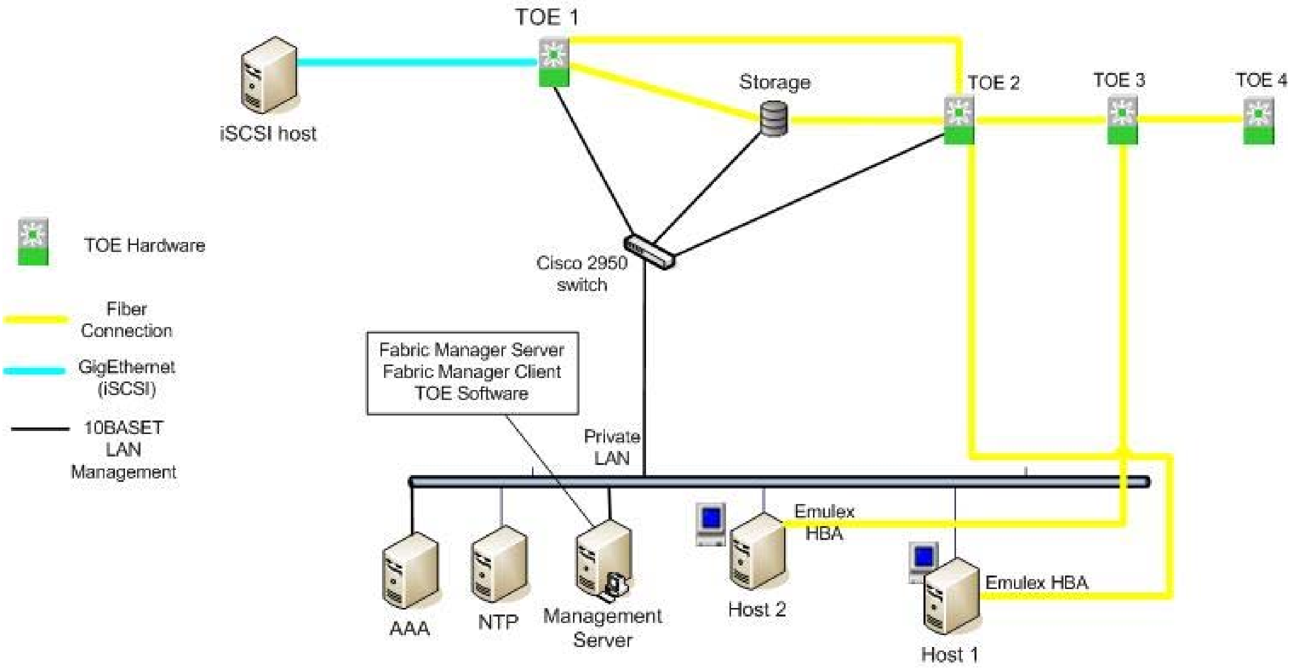
The evaluation team also performed a penetration flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR line by line to determine whether it was possible that the evaluated configuration could be susceptible to vulnerability. It’s to be noted that many of the functional testing concentrated on unauthorized access to a switch fabric or storage device. Therefore, a number of functional tests are also considered penetration tests. The evaluation team did construct and execute its own penetration tests below:

- Use a port scanner to check for open ports on the MDS switch and Fabric Manager using Nessus.
- Determine if the TOE will enforce CHAP authentication on all iSCSI requests.

8. Evaluated Configuration

The evaluated configuration was tested in the configuration identified in Figure 1, below. The evaluation results are valid for all configurations of the TOE identified in section 5 of this report

Figure 1: Testing Environment



Test models covered in team test activity

- **MDS 9506 Multilayer Director**
  Cisco MDS 9000 Multi-Protocol Services Module
  Cisco MDS 9500 Series Supervisor-1 Module
  24 port Fibre Channel Switching Modules

- **MDS 9509 Multilayer Director**
  Cisco MDS 9500 Series Supervisor-1 Module
  48 port Fibre Channel Switching Modules

- **MDS 9513 Multilayer Director**
  Cisco MDS 9500 Series Supervisor-2 Module
  12 port Fibre Channel Switching Modules
  24 port Fibre Channel Switching Modules

- **MDS 9216i Multilayer Fabric Switch** (Integrated Fibre Channel and IP storage services)

9. Results of the Evaluation

The Cisco MDS 9000 Family with SAN-OS Release 3.2(2c) satisfies all of the EAL3 assurance requirements against which it was evaluated. The Security Target provides a detailed description of how Cisco MDS 9000 meets each of the listed components.

10. List of 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

11. Validation Comments/Recommendations

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.