CHAPTER 1

Product Overview

This chapter includes the following sections:

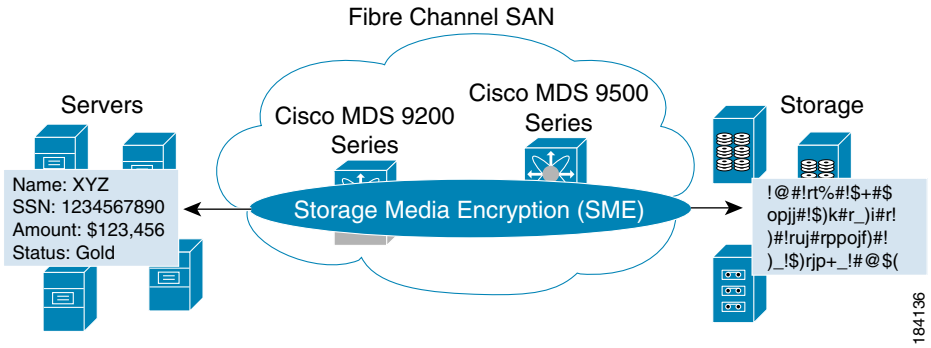
About Cisco Storage Media Encryption

The Cisco SME solution is a comprehensive network-integrated encryption service with enterprise-class key management that works transparently with existing and new SANs. The innovative Cisco network-integrated solution has numerous advantages over competitive solutions available today:

- Cisco SME installation and provisioning are both simple and nondisruptive. Unlike other solutions, Cisco SME does not require rewiring or SAN reconfiguration.
- Encryption engines are integrated on the Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) and the Cisco MDS 9222i Multiservice Module Switch, eliminating the need to purchase and manage extra switch ports, cables, and appliances.
- Traffic from any virtual SAN (VSAN) can be encrypted using Cisco SME, enabling flexible, automated load balancing through network traffic management across multiple SANs.
- No additional software is required for provisioning, key, and user role management; Cisco SME is integrated into Cisco Fabric Manager, therefore reducing operating expenses.

Figure 1-1 shows the integration of Cisco SME with SAN fabrics to offer seamless management of data encryption.

Figure 1-1 Cisco Storage Media Encryption



Cisco Storage Media Encryption Features

The Cisco MDS 9000 Family of intelligent directors and fabric switches provide an open, standards-based platform for hosting intelligent fabric applications and services. As a platform, the Cisco MDS 9000 family switches provide all essential features required to deliver secure, highly available, enterprise-class Fibre Channel storage area network (SAN) fabric services. Cisco has integrated encryption for data-at-rest as a transparent fabric service to take full advantage of this platform.

Cisco SME (SME) is a standards-based encryption solution for heterogeneous tape libraries and virtual tape libraries. Cisco SME is managed with Cisco Fabric Manager and a command-line interface (CLI) for unified SAN management and security provisioning. Cisco SME includes the following comprehensive built-in key management features:

Transparent Fabric Service

Cisco employs a Fibre Channel redirect scheme that automatically redirects the traffic flow to an MSM-18/4 module or an MDS 9222i switch any where in the fabric. There are no appliances in-line in the data path and there is no SAN rewiring or reconfiguration.

Encryption

Cisco SME uses strong, IEEE-compliant AES 256 encryption algorithms to protect data at rest. Advanced Cisco MDS 9000 SAN-OS Software security features, such as Secure Shell (SSH), Secure Sockets Layer (SSL), RADIUS, and Fibre Channel Security Protocol (FC-SP) provide the foundation for the secure FIPS Level 3 architecture.

Cisco SME uses the NIST approved random number standard to generate the keys for encryption

Encryption and compression services are transparent to the hosts and storage devices.

Cisco SME Roles

Cisco SME services include two configuration and security roles. Primary security roles for Cisco SME configuration are Cisco SME Administrators and Cisco SME Recovery Officers. Cisco SME Recovery Officers are also responsible for key recovery operations. The SAN administrator is assigned both roles by default. During Cisco SME configuration, additional Recovery Officers can be added.

The Cisco SME Administrator configures and maintains Cisco SME. This role can be filled by multiple storage network administrators who are responsible for the following:

- SAN administration
- Cisco SME provisioning and management

Cisco SME Recovery Officers play a critical role in recovering the key database of an archived cluster and they are responsible for protecting the master key. The role of the Cisco SME Recovery Officer separates master key management from Cisco SME administrations and operations. In some organizations, a security officer may be assigned to this role.

At the advanced security level, a quorum of Cisco SME Recovery Officers is required to perform recovery procedures. The default is 2 out of 5. In this case 2 of the 5 recovery officers are required to unlock the master key.

For additional information on Cisco SME Administrator and Cisco SME Recovery Officer roles, see Creating and Assigning Cisco SME Roles and Cisco SME Users, page 2-14.

Key Management

The Cisco Key Management Center (Cisco KMC) provides dedicated key management for Cisco SME, with support for single- and multi-site deployments. Cisco KMC provides essential features such as key archival, secure export and import, and key shredding.

Key management features include the following:

- Master key resides in smart cards
- Quorum (2 out of 5) of smart cards required to recover the master key
- Unique Key per Tape
- Keys reside in clear-text only inside a FIPS boundary
- Tape keys and intermediate keys are wrapped by the master key and archived at the Key Management Center
- Option to store Tape keys on tape media

The centralized key lifecycle management includes the following:

- Archive, Shred, Recover, and Distribute media keys

  - Integrated into Fabric Manager Server
  - Secure transport of keys
- End-to-end key management using HTTPS/SSL/SSH
  - Access controls and accounting
  - Use of existing AAA mechanisms

Clustering

Cluster technology provides reliability and availability, automated load balancing, failover capabilities, and a single point of management.

FC Redirect

Cisco SME performance can easily be scaled up by adding more Cisco MDS 9000 family switches or modules. The innovative Fibre Channel redirect capabilities in Cisco MDS 9000 SAN-OS enable traffic from any switch port to be encrypted without SAN reconfiguration or rewiring.

Server-Based Discovery for Provisioning Tapes

Cisco SME provides discovery of backend targets using the identity of the host during a session establishment.

Target-Based Load Balancing

The Cisco SME cluster consists of a set of switches (in a dual-fabric environment) running the Cisco SME application. Clustering offers target-based load balancing of Cisco SME application services. The cluster infrastructure allows the Cisco SME application to communicate and coordinate to maintain consistency and high availability.

Load balancing is achieved by distributing ownership of the various metadata objects throughout the cluster. Cisco SME assigns hosts to the available Cisco SME interfaces using the following algorithm:

- All hosts for a given target port are always assigned to the same Cisco SME interface.
- If a target port is connected to one of the Cisco SME switches, an interface is selected based on the load from the target-connected switch. That is, the target locality is considered when choosing a Cisco SME interface for a target.
- If a target is connected to a switch that has no Cisco SME interface, then the target is assigned to the least loaded available interface in the Cisco SME cluster.

In target-based load balancing, the load on an interface refers to the the number of targets assigned to that interface.

Caution The load balancing command is disruptive to traffic. Ensure that you execute this command at a scheduled downtime otherwise the existing traffic will be affected.

Cisco SME Terminology

The following Cisco SME-related terms are used in this book:

- Cisco SME interface—The security engine in the MSM-18/4 module or fixed slot of a Cisco MDS 9222i fabric switch. Each MSM-18/4 module and MDS 9222i switch has one security engine.
- Cisco SME cluster—A network of MDS switches that are configured to provide the Cisco SME functionality; each switch includes one or more MSM-18/4 modules and each module includes a security engine.
- Fabric—A physical fabric topology in the SAN as seen by Fabric Manager. There can be multiple VSANs (Logical Fabrics) within the physical fabric.
- Tape group—A backup environment in the SAN. This consists of all the tape backup servers and the tape libraries that they access.
- Tape device—A tape drive that is configured for encryption.
- Tape volumes—A physical tape cartridge identified by a barcode for a given use.
- Tape volume group—A logical set of tape volumes that are configured for a specific use, for example, a group of tape volumes used to backup a database.
- Key Management Center—A component in Fabric Manager Server that stores the encryption keys.
- Master Key—An encryption key generated when an Cisco SME cluster is created. The master key encrypts the tape volume keys and tape keys and it is required to decrypt those keys in order to retrieve encrypted data.
- Media Key—A key that is used for encrypting and authenticating the data on specific tapes.
- SmartCard—A card (approximately the size of a credit card) with a built-in microprocessor and memory used for authentication.
- Cisco SME Administrator—A network administrator who configures Cisco SME
- Cisco SME Recovery Officer—A data security officer entrusted with smart cards and the associated PINs. Each smart card stores a share of the cluster master key. Recovery officers must present their cards and PINs to recover the key database of an archived cluster. A quorum of recovery officers are required to execute this operation.

Supported Topologies

Cisco SME supports a single-fabric topology. The Cisco MSM-18/4 module and the MDS 9222i switch provides the Cisco SME engines used by Cisco SME to encrypt and compress data-at-rest. Multiple modules can be deployed in a Fibre Channel fabric to easily scale-up performance, to enable simplified load balancing, and to increase availability. In a typical configuration, one MSM-18/4 is required in each Cisco SME cluster.

Cisco SME clusters include designated backup servers, tape libraries, and one or more MDS switches running Cisco SAN-OS Release 3.2(2c). One cluster switch must include an MSM-18/4 module. With easy-to-use provisioning, traffic between any host and tape on the fabric can utilize the Cisco SME services.

Required Cisco SME engines are included in the following Cisco products:

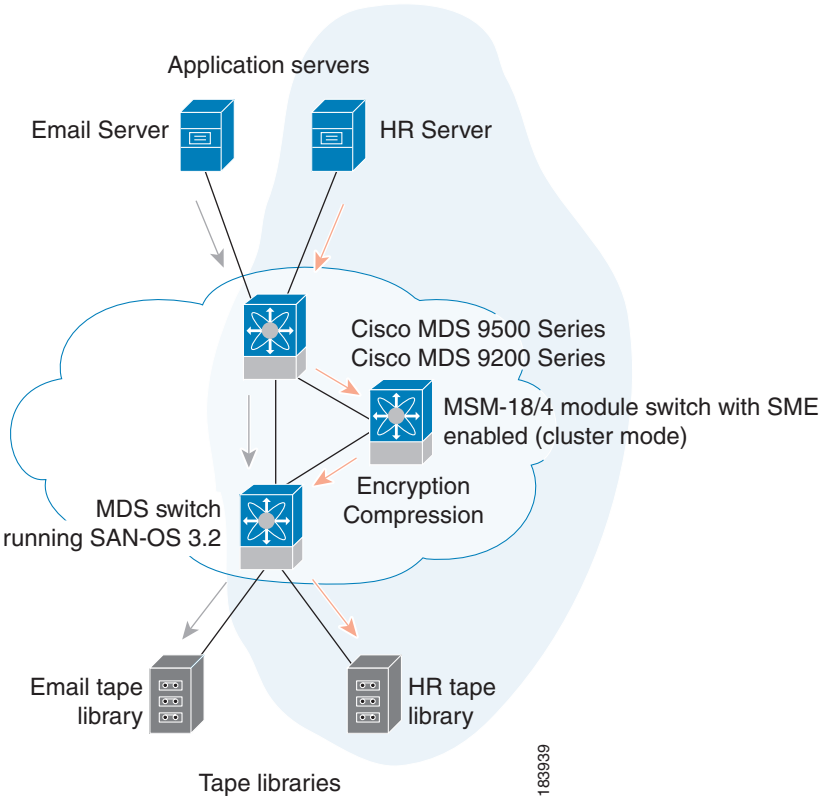
- Cisco MDS 9000 Family 18/4-port Multiservice Module (MSM-18/4)
- Cisco MDS 9222i Multiservice Module Switch

Single-Fabric Topology

Figure 1-2 shows a single-fabric topology in which the data from the HR server is forwarded to the Cisco MSM-18/4. The Cisco MSM-18/4 can be anywhere in the fabric. Cisco SME does a 1:1 mapping of the information from the host to the target and forwards the encrypted data to the dedicated HR tape. Cisco SME also tracks the barcodes on each encrypted tape and associates the barcodes with the host servers.

Figure 1-2 shows encrypted data from the HR server is compressed and stored in the HR tape library. Data from the Email server is not encrypted when backed up to the dedicated Email tape library.

Figure 1-2 Cisco Storage Media Encryption: Single-Fabric Topology



Note Tape devices should be connected to core switches like MDS 95XX/9216/9222i switch running SAN-OS 3.2(2).

Encryption and compression services are transparent to the hosts and storage devices. These services are available for devices in any Virtual SANs (VSANs) in a physical fabric and can be used without rezoning.

In Service Software Upgrade In Cisco SME

In-Service Software Upgrade (ISSU) is a comprehensive, transparent software upgrade capability which allows you to add new features and services without any disruption to the traffic.

In a cluster, which has the MDS 9222i switch as nodes, if the nodes are not able to communicate, then the node having the lowest node identifier (node ID) remains in the cluster while the other node leaves the cluster. However, when an ISSU is performed on a node having the lowest node identifier, a complete loss of the cluster results since both the nodes leave the cluster.

This undesirable situation is addressed in a two-node cluster as follows:

- The upgrading node sends a message to the other node of the intent to leave the cluster. The upgrading node can either be a master node or a slave node.
- The remaining node remains in the cluster and performs the role of the master node if it was a slave node. This node continues to remain in the cluster with the quorum intact.
- After the ISSU is completed and the switches boots up, the upgraded node rejoins the cluster as a slave node.

Note This feature is tied to the internals of ISSU logic and no additional command needs to be executed for this purpose.

Software and Hardware Requirements

This section includes the following topics:

Software Requirements

All MDS switches in the Cisco SME cluster must be running the current release of Fabric Manager and SAN-OS software. This includes the following:

- The Fabric Manager server must be running Fabric Manager 3.2(2).
- The Cisco MDS switches attached to tape devices must be running SAN-OS Release 3.2(2).
- All switches that include MSM-18/4 modules must be running SAN-OS Release 3.2(2) software.

Hardware Requirements

Cisco SME requires at least one encryption service engine in each cluster. The Cisco SME engines on the required modules provide the transparent encryption and compression services to the hosts and storage devices. To take full advantage of the standard and advanced security levels, a smart card reader is required.

For detailed information on required hardware and installing required hardware, refer to the specific installation guides. For information about ordering hardware, refer to http://www.cisco.com/en/US/ordering/index.shtml.

This section includes information about the following required hardware:

Cisco MDS 9000 Family 18/4-Port Multiservice Module (MSM-18/4)

The Cisco MDS 9000 Family 18/4-port Multiservice module (MSM-18/4) provides 18 autosensing 1-, 2-, and 4-Gbps Fibre Channel ports and four Gigabit Ethernet IP services ports. The MSM-18/4 module provides multiprotocol capabilities such as Fibre Channel, Fibre Channel over IP (FCIP), Small Computer System Interface over IP (iSCSI), IBM Fiber Connectivity (FICON), and FICON Control Unit Port (CUP) management.

The MSM-18/4 module provides 18 4-Gbps Fibre Channel interfaces for high-performance SAN and mainframe connectivity and four Gigabit Ethernet ports for FCIP and iSCSI storage services. Individual ports can be configured with hot-swappable shortwave, longwave, extended-reach, coarse wavelength-division multiplexing (CWDM) or dense wavelength-division multiplexing (DWDM) Small Form-Factor Pluggables (SFPs) for connectivity up to 125 miles (200 km).

The MSM-18/4 module can minimize latency for disk and tape through FCIP write acceleration and FCIP tape write and read acceleration. The MSM-18/4 module provides up to 16 virtual Inter-Switch Link (ISL) connections on the four 1-Gigabit Ethernet ports through tunneling, and provides up to 4095 buffer-to-buffer credits that can be assigned to a single Fibre Channel port.

The MSM-18/4 provides intelligent diagnostics, protocol decoding, and network analysis tools with the integrated Call Home capability.

Note Cisco MDS 9500 Series switches running Cisco MDS SAN-OS Release 3.2(1) or later support the MSM-18/4 and the MSFM-18/4 modules.

For additional information, refer to the *Cisco MDS 9500 Series Hardware Installation Guide*.

Cisco MDS 9222i Multiservice Modular Switch

The Cisco MDS 9222i Multiservice Modular switch includes an integrated supervisor module (in slot 1) that provides the control and management functions of the Cisco MDS 9222i Switch and it provides an 18-port Fibre Channel switching and 4-port Gigabit Ethernet IP services module. The Cisco MDS 9222i built-in supervisor module provides multiple communication and control paths to avoid a single point of failure. The Cisco MDS 9222i supervisor module has a PowerPC PowerQUICC III class processor, 1 GB of DRAM, and an internal CompactFlash card that provides 1 GB of storage for software images.

The Cisco MDS 9222i switch includes a modular expansion slot to host Cisco MDS 9000 Family Switching and Services Modules. For additional information, refer to the *Cisco MDS 9200 Series Hardware Installation Guide*.

Note The Cisco MDS 9222i switch requires MDS SAN-OS Release 3.2(2).

FC-Redirect-Capable Switches

Cisco SME requires that each target switch be FC-Redirect capable. FC-Redirect is not supported on the following switches:

- Cisco MDS 9124 switch
- Cisco MDS 9134 switch
- Cisco MDS 9020 switch

Note Tape devices and tape libariers are not supported in these edge switches.

Smart Card Readers

To employ standard and advanced security levels, Cisco SME requires the following:

- Smart Card Reader for Cisco SME (DS-SCR-K9)
- Smart Card for Cisco SME (DS-SC-K9)

The smart card reader is a USB device that is connected to a management workstation. The management workstation is used to configure the Cisco SME cluster. The smart card reader requires the smart card drivers that are included on the installation CD. These must be installed on the management workstation where the reader is attached.

Note The smart card reader is supported on Windows-only platforms.

Cisco Storage Media Encryption Security Overview

Cisco SME transparently encrypts and decrypts data inside the storage environment without slowing or disrupting business critical applications.

Cisco SME generates a master key, tape volume keys and tape keys. The keys are encrypted in a hierarchical order: the master key encrypts the tape volume keys and the tape keys. They are also copied to the key catalog on the Cisco KMC server for backup and archival. Eventually inactive keys are removed from the fabric, but they are retained in the Cisco KMC catalog. The keys can be retrieved automatically from the Cisco KMC by the Cisco SME services in the fabric if needed again.

A single Cisco KMC can be used as a centralized key repository for multiple fabrics with Cisco SME services if desired. Key catalog import and export capabilities are also provided to accommodate moving tape media to different fabrics in environments with multiple Cisco KMC servers. Backup applications can be used to archive the key catalogs for additional protection.

Additional Security Capabilities

Additional security capabilities offered by Cisco SAN-OS complete the Cisco SME solution. For example, RADIUS and TACACS+ servers can be used to authenticate, authorize, and provide accounting (AAA) for Cisco SME administrators. Management of Cisco SME can be limited to authorized administrators using role based access controls (RBAC). When communication take place, secure shell (SSHv2) protocol is used to provide message integrity and privacy.

The Cisco MDS 9000 Family is certified to meet Common Criteria (CC) EAL3 and Federal Information Processing Standard (FIPS) 140-2 level 2. To meet FIPS 140-2 level 3 Certification requirements for the critical Cisco SME services, the MSM-18/4 has the cryptographic engine and related memory devices encapsulated to prevent tampering. Any attempt at tampering the system is guaranteed to destroy the sensitive data. In addition, critical security parameters never leave the system unencrypted.