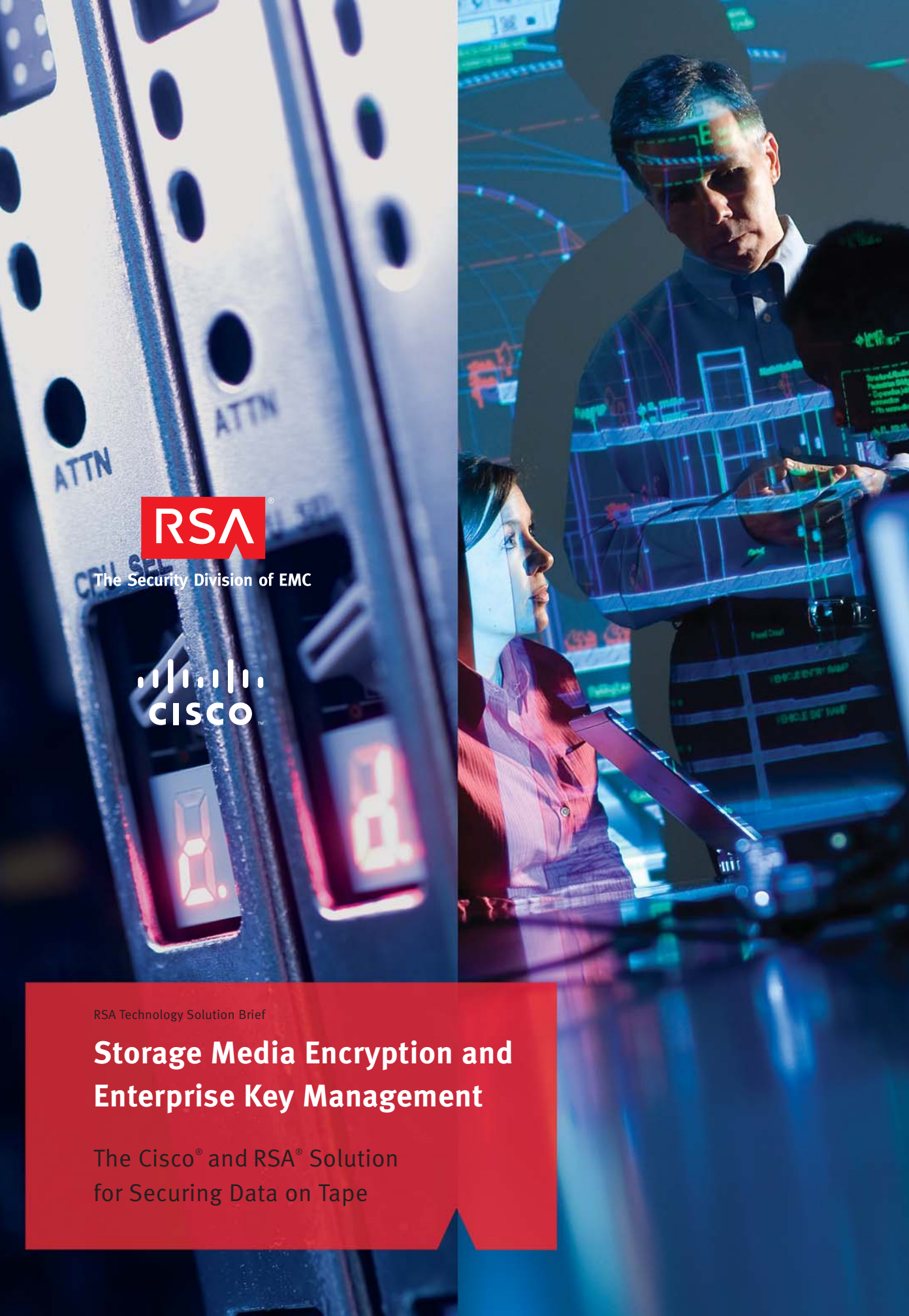


RSA Technology Solution Brief

Storage Media Encryption and Enterprise Key Management

The Cisco® and RSA® Solution for Securing Data on Tape

This paper discusses the solution provided by Cisco and RSA for securing data on tape through the use of Cisco® Storage Media Encryption and Enterprise Key Management.

Today's increasing requirements for application availability, combined with accelerating growth in the amount of data created and stored, dictates a paradigm shift for backup of large volumes of data – IT environments are faced with the combination of data growth and shrinking backup windows to get their backup completed – restore time objectives and restore point objectives are also becoming more stringent, increasing the importance of highly reliable, high-performance backup environments such as Virtual Tape Libraries and backup to disk.

As this transition occurs, however, magnetic tape continues to be commonly used for backup and distribution of large volumes of data. Until recently, tapes containing bulk data were rarely encrypted, as the risks associated with loss or theft of a tape were viewed as insufficient to warrant the costs in equipment, performance and operations that encryption could impose. Increasingly, however, the risks associated with bulk data loss are seen as much more serious, as a result of changes such as the following.

More stringent privacy regulations

Private data stored in electronic form are subject to privacy laws like the EU Directive on Privacy and Electronic Communication (2002), and the Japanese Bill to Protect Personal Data (2001). A growing number of U.S. states have privacy regulations in place, and several bills were introduced in the U.S. Congress in 2005. At the same time the Visa/Mastercard Payment Card Industry requirements and the Japan Bank Association's Data Protection Support standard are visible examples of data privacy demands on technologies.

Public disclosure of data breaches

The California Database Breach Act (California SB1386 / AB1298, 2003) requires that any data breach involving the private data of a California citizen is announced to the public. As a consequence, most of data breaches associated with lost/stolen clear text tapes require activities like alerting customers, providing credit monitoring, and damage control, with a potential loss of millions of dollars. Many other states have followed with their own regulations comparable to SB 1386.

Long-term data retention requirements

Government regulations like HIPAA and SEC 17a-4 demand long-term records retention for very long periods. Since tape media is often used for data archiving, tape encryption can be utilized to keep the data confidential and tamperproof.

Tape encryption can be seen as an insurance policy to deal with the threat of lost/stolen tapes. The combined offering of Cisco® Storage Media Encryption (SME) and RSA Key Manager for the Datacenter from RSA, the Security Division of EMC, provides an industry-leading offering for securing data on tape. The Cisco SME solution, integrated in a storage area network (SAN) based on the Cisco MDS 9000 family of switches and directors, compresses and encrypts the data being copied to physical tape or Virtual Tape Library (VTL). The actual cryptographic processing is performed in a distributed and scalable fashion on high-speed secure processors to reduce impact on backup windows. Enabling of encryption through the fabric manager is simple, ensuring minimal impact on operational processes and personnel.

RSA® Key Manager for the Datacenter complements Cisco® SME by providing centralized, enterprise-level key management that ensures the manageability, auditability and longevity of the encryption keys. The symmetric keys used in encryption are the most essential and sensitive pieces of information in the solution. They need to be protected so that the data encrypted with these keys cannot be decrypted by unauthorized users. The encryption keys must be preserved for as long as the encrypted data is preserved, or the encrypted data cannot be decrypted, and will therefore be unrecoverable if the key is no longer available. In addition, effective management of keys is essential when encrypted data is shared with partners, as well as in order to take advantage of such capabilities as shredding data by revocation of the key used to encrypt it.

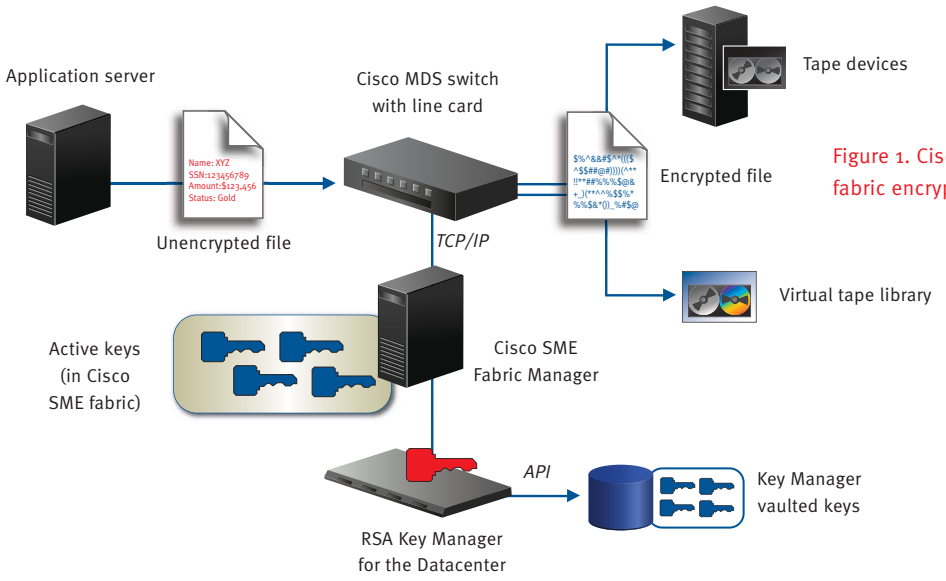


Figure 1. Cisco SME transparent fabric encryption service

Introduction

Cisco SME is a feature of Cisco MDS 9000 SAN-OS Software 3.2 that allows data stored on magnetic tape or VTLs to be encrypted, which protects that data in the event of physical loss or theft of the tapes. Without encryption, the data stored on tapes is accessible by anyone with the appropriate backup software.

As shown in Figure 1, encryption is performed by a line card as the data is sent by the backup host through the Cisco MDS 9000 family switch to the tape libraries. Cisco SME compresses it before encrypting it and committing it to tape. In some situations, backup software or the host's operating system may have already compressed the data, and therefore Cisco SME may or may not perform the compression.

Cisco SME is a transparent fabric service, meaning that it can be added to or removed from an existing fabric without significant disruption. In most cases, there is no need to re-cable or redesign a fabric. Customers who have an existing SAN fabric – with either Cisco MDS-9200 Series Multilayer Fabric Switches or Cisco MDS 9500 Series Multilayer Directors – can easily implement Cisco SME in their current environments. Fabrics with only Cisco MDS 9100 Series Multilayer Fabric Switches would require the addition of at least one Cisco MDS 9200 or 9500 Series switch to provide the encryption service.

As indicated in the illustration, key management is as important an element of the tape security solution as encryption. The integration of RSA Key Manager for the Datacenter with Cisco SME provides an industry-leading solution for securing data on tape, helping to ensure not only the effective protection of data through encryption but also the management of the keys used for encryption. This solution brief explores in detail both the encryption architecture and the key management architecture for Cisco SME with RSA Key Manager.

Encryption Architecture

Cisco SME provides a complete, integrated solution for encryption of data at rest on heterogeneous tape drives and VTLs. Storage in any virtual SAN (VSAN) can make full use of Cisco SME, providing exceptional flexibility for provisioning this transparent fabric service.

Interfaces enabled for Cisco SME, distributed in the various Cisco MDS 9000 family switches and directors in the SAN, intercept the traffic to a tape generated by a host and encrypt it before it reaches the target. Similarly, the traffic generated by the target designated for a host is intercepted by the Cisco SME interfaces and decrypted before it is forwarded to the host. The Cisco MDS 9000 family switches provide all the essential features required to deliver encryption within a secure, highly available, enterprise-class Fibre Channel SAN.

Cisco SME is managed with the Cisco Fabric Manager and a command-line interface (CLI). Cisco Fabric Manager provides unified SAN management and security provisioning as a single, logical SAN fabric feature.

Cisco SME Hardware

Tto implement Cisco SME in a fabric, at least one Cisco MDS 9000 18/4 Port Multi-services Module (MSM) is required in the fabric. The MSM line card contains the encryption engine, referred to as a Cisco SME interface, that is used to encrypt the data before it is stored on tape. It is recommended that multiple cards be implemented in a fabric to provide fault tolerance and increase throughput. The line card can be installed in a Cisco MDS 9216A or 9216i Multilayer Fabric Switch or a Cisco MDS 9506, 9509 or 9513 Multilayer Director. The Cisco MDS 9222i Multilayer Modular Switch comes standard with a hybrid supervisor and MSM in slot 1 (fixed slot) of the chassis.

This line card can perform all Cisco SME functions; therefore an additional Cisco MDS 9000 18/4 MSM line card is not required in a Cisco MDS-9222i. However, an additional Cisco MDS 9000 18/4-Port MSM can be installed in slot 2, providing increased throughput. A Cisco MDS 9000 18/4-Port MSM line card that is used for Cisco SME cannot be used for Internet Small Compute System Interface (iSCSI) services, as the port indices used for iSCSI are also used by Cisco SME and would therefore conflict. Nor is concurrent use of Fibre Channel over IP (FCIP) supported.

In some instances, regulatory code may require that not only that data be encrypted, but also that the encryption take place within a tamper-resistant cryptographic module. To address this requirement, Cisco SME provides a Federal Information Processing Standard (FIPS) 140-2 Level-3 architecture. Products are validated to be FIPS 140-2 compliant if they meet certain levels of protection of sensitive information. FIPS 140-2 Level 3 requires that identity-based authentication mechanisms be provided for administrative access and that the cryptography modules are encased in a hard opaque material to prevent tampering.

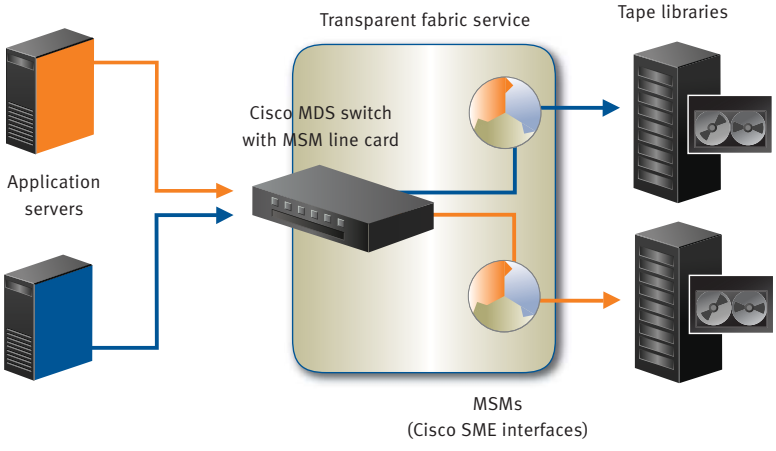


Figure 2. Cisco SME transparent fabric service automatically redirects encrypted traffic to the appropriate MSM.

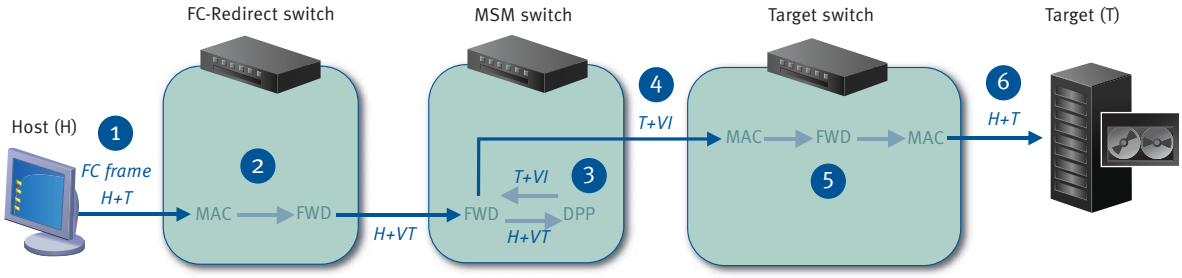


Figure 3. Packet Flow from Host to Tape

Cisco SME Transparent Fabric Service

Cisco SME is a transparent fabric service. This means that an MSM (such as the Cisco MDS 9000 18/4 Port MSM line card or MDS 9222i switch) can be deployed anywhere in the fabric. It does not need to be directly in the data path. It also means that cabling or configuration changes are not necessarily needed.

As shown in Figure 2, once Cisco SME is enabled, traffic that is being encrypted is automatically redirected to the appropriate MSM (Cisco SME interface) in the fabric using the FC-Redirect service. In the event of an MSM failure, traffic will be automatically redirected to a functional MSM.

FC-Redirect is the service that allows Cisco SME to function as a transparent fabric service. Essentially, its role is to create virtual targets for Cisco SME-enabled tape devices and virtual initiators for Cisco SME-enabled hosts. This allows the fabric to alter the flow of traffic so that it passes through an MSM to be encrypted before it is ultimately sent to the tape device for storage.

For FC-Redirect to function, several requirements must be met. First, any targets (tape devices) enabled for Cisco SME must be attached to a switch capable of FC-Redirect. This includes any switch or director in the Cisco MDS 9200 or 9500 Series that can support Cisco MDS 9000 SAN-OS Software 3.2. Cisco MDS 9124, 9134, 9120 20-Port and 9140 40-Port Multilayer Fabric Switches cannot be used to connect targets because they do not have the resources to support FC-Redirect. However, host devices can be connected to any supported Cisco MDS 9000 family switch.

The MSM on which Cisco SME is enabled creates a virtual initiator (VI) for each host and a virtual target (VT) for each target that is being serviced by Cisco SME. All VIs and VTs are created in the same VSAN as the target, and will be created in a default zone. Therefore, default zone permissions should be set to deny and nothing should be zoned with the VI and VT.

In order to propagate FC-Redirect information, Cisco Fabric Services should be enabled on all switches enabled for Cisco SME. FC-Redirect is a supervisor process and is maintained in the Permanent Storage Service (PSS), so that in the event of a Supervisor failure all state information is maintained.

In a normal environment, switches along the path between host (H) and tape (T) would simply forward the frames to the next switch in the path, based on FSPF routes. FC-Redirect changes how the frames are forwarded; this is seen in figure 3:

1. The Host sends a FC frame to the Target, just as it would if Cisco SME did not exist in the fabric.
2. The first FC-Redirect aware switch in the path receives the frame, and determines that the Target has been mapped to a Virtual Target. It then rewrites the frame header and sends it along to the new destination/target address, which resides on the switch containing the MSM.
3. The Cisco SME switch (with the MSM) receives the frame destined for the Virtual Target. It performs the encryption process on the data contained within the frame, compresses the data if possible, and rewrites the frame header replacing the Host/Initiator information with the Virtual Initiator Information and Virtual Target information with the Target (Tape device) information.

4. The Cisco SME switch sends the new frame to the target switch (where the target device is located).

5. The target switch receives the frame and discovers that it has been redirected. It again rewrites the frame header and replaces the Virtual Initiator information with the original Host information.

6. The target switch forwards the frame to the target device, where the encrypted data is written to tape.

Reply frames from the target follow the same process in reverse.

Cisco SME Management

The Cisco Fabric Manager Server (FMS) must be installed to manage any fabrics that are using Cisco SME. Management traffic for Cisco SME is conducted over a TCP/IP network, and is initiated by using a web browser to access the web server portion of the Cisco FMS. Cisco FMS licenses are not required to use only the Cisco SME management functionality.

Cisco FMS authenticates the user by using local credentials or a configured AAA server. When the Cisco SME tab is accessed, a secure shell (SSH) connection to the master switch in each managed fabric is established. Configuration messages are sent to the master switch in the appropriate cluster(s), and are then disseminated via the cluster communications mechanisms detailed below. SSH connections are established using the user's credentials, and are disconnected when the user logs off the Cisco Fabric Manager.

When Cisco SME is configured, two new roles are added to the security structure. The first is the Cisco SME administrator. This role is responsible for provisioning and management of the Cisco SME environment, including clusters, tape volume groups, tape devices, etc. This role can be restricted to the management of resources in specific VSANs. By default, all administrator-level users can fully manage Cisco SME.

The second role is the Cisco SME recovery officer. This role is responsible for as recovery in the event of a disaster. In an Advanced Security environment, several recovery officers are designated and a minimum of two are required to perform recovery. These new Cisco SME roles will work in conjunction with the existing storage administrator roles, which are responsible for provisioning and configuring storage resources.

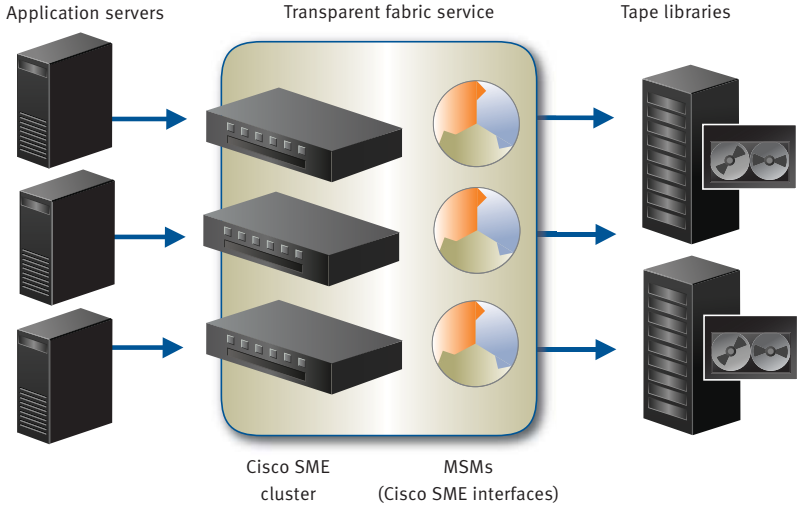
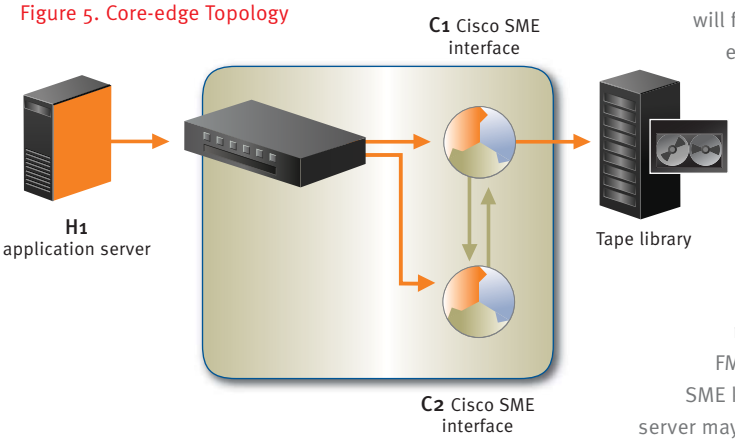


Figure 4. Cisco SME clusters provide a single point of management and consolidated resources.

Figure 5. Core-edge Topology



Cisco SME clusters, shown in Figure 4, provide a single point of management and consolidated resources. All switches containing MSMs with enabled Cisco SME interfaces in a fabric must belong to a single cluster. A Cisco SME cluster can be created with a single switch containing Cisco SME interfaces, or with multiple switches with Cisco SME interfaces. By having multiple Cisco SME interfaces in a cluster, encryption traffic is distributed among the various line cards providing load balancing. In addition, the failure of a single MSM will result in traffic being redirected to another MSM.

Cisco SME Topology

The current release of Cisco SME supports only a single fabric topology, meaning that Cisco SME clusters cannot span fabrics. Separate Cisco SME clusters can be implemented in each fabric but they will function as independent Cisco SME environments. Each fabric can have only one Cisco SME cluster, which can consist of up to four switches. Each switch has at least one MSM, but can have more than one.

Care must be taken with regards to the Cisco FMS in a Cisco SME environment. In addition to performing general fabric management and monitoring tasks, Cisco FMS is responsible for managing the Cisco SME keys. In a smaller environment, a single server may suffice as both the fabric manager server and the key management server. In larger environments, however, a separate fabric manager server dedicated to Cisco SME may be warranted.

Cisco SME supports a core-edge topology and an edge-core-edge topology. Figure 5 shows an example of a standard core-edge topology in which the tape devices are connected to multiple switches.

In this topology, because Cisco SME traffic does not follow FSPF routing algorithms, there is the chance that traffic will not take the shortest path to the target. As an example, traffic from Host H1 may travel to library L1 directly through switch C1 via its edge switch. However, it could just as easily travel through the edge switch to core switch C2, where Cisco SME encrypts the data and then forwards it to core switch C1 and finally to the destination tape device.

An alternative core-edge topology connects all tape devices to the same core switch. In that case, the Cisco SME should be installed in that same switch

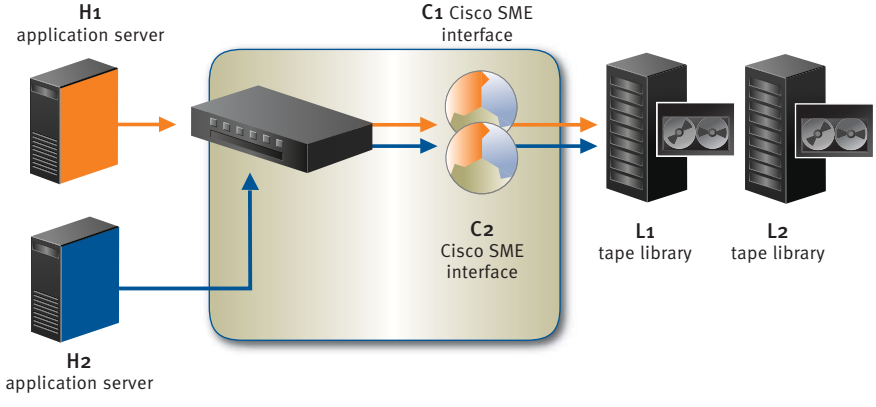


Figure 6. Edge-core-edge Topology

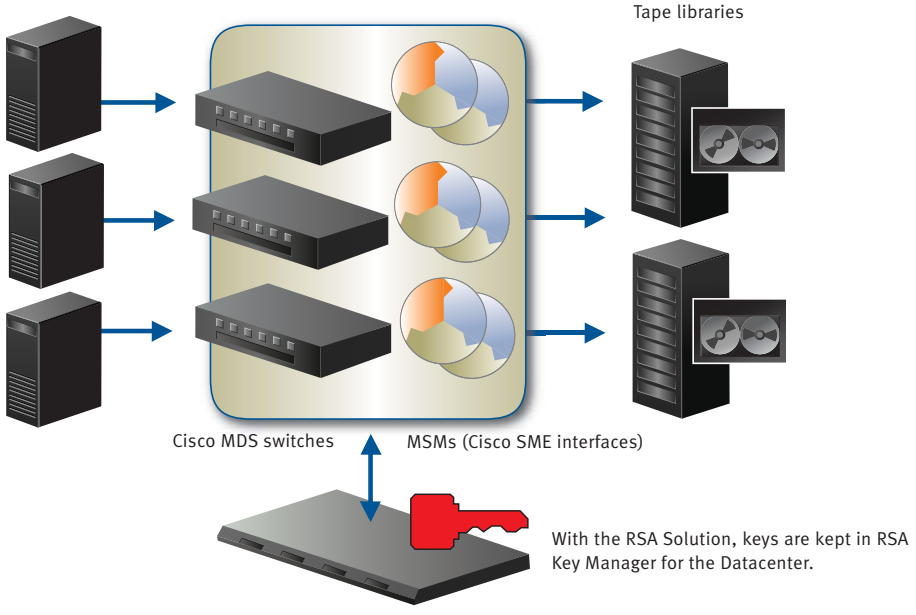


Figure 7. High Availability Configuration

and Cisco SME should be configured there as well. This allows the FC traffic to take the same path as if Cisco SME was not present

Cisco SME also supports an edge-core-edge topology, shown in Figure 6. In this topology, the MSMs are placed in the switch to which the libraries are connected. This reduces unnecessary routing of FC frames.

For the purposes of high availability (HA), multiple MSMs can be configured in a fabric, in different switches, as shown in Figure 7. This high-availability topology protects from both line card and switch failures.

Cisco SME Monitoring and Logging

The Cisco Fabric Manager plays an important role in monitoring the Cisco SME environment. For example, the Cisco Fabric Manager can be used to verify that a tape has been encrypted. Once a tape has been labeled and written, it appears in the active tab of the appropriate volume pool, identified by the tape barcode. The unique identifier for the encryption key used to encrypt the tape will also be displayed.

The monitoring capabilities in the Cisco Fabric Manager are complemented by logging capabilities. For example, if a tape does not appear in the Cisco Fabric Manager display, the user can verify that the data is being encrypted by examining the statistics for the appropriate Cisco SME interface. The log files are written to the Cisco MDS 9000 family directory. These files roll over periodically, so fmserver.log.1, fmserver.log.2, etc. may also be present and require inspection.

Cisco SME Configuration and Performance

Though encryption and compression consume processing power in the MSM, the Cisco SME solution nonetheless continues to deliver high performance, with each MSM supporting approximately 4 gigabits per second. For optimal performance with compression and encryption enabled, each MSM can be connected to up to eight tape drives (may be less depending on the type). Multiple MSMs can be configured in the Cisco MDS 9506, 9509 and 9513 Multilayer Directors, with up to four switches in a Cisco SME cluster.

Contact your EMC representative for the most up-to-date information on Cisco SME configuration and performance.

Key Management Architecture

The symmetric keys used in encryption, such as in the Cisco SME solution, are the most essential and sensitive piece of information in the solution. Not only do they need to be protected so that the data encrypted with these keys cannot be decrypted by unauthorized users, but they must be preserved for as long as the encrypted data is preserved, or the encrypted data cannot be decrypted and will therefore be unrecoverable if the key is no longer available.

The Cisco Key Management Center (KMC) interfaces directly with the MSMs, taking the critical role of immediately storing the cryptographic keys generated and used by the MSMs. These cryptographic keys include both the cipher keys, used to encrypt the data written to tape, and the key encryption keys used to protect the cipher keys from compromise.

As shown in the table, the enterprise key management solution provided by RSA Key Manager for the Datacenter, significantly extends the capabilities provided by the Cisco KMC.

Through these extended capabilities, RSA Key Manager for the Datacenter complements the capabilities of Cisco SME and Cisco KMC to provide the industry-leading solution for securing data on tape.

Cisco Key Management Center

Cisco KMC is the centralized management system that takes ownership of the lifecycle of keys used to encrypt and decrypt the data handled by Cisco SME. It includes three components:

– The Cisco SME web client is part of the Cisco Fabric Manager web client and is used to access a Cisco FMS via a standard web browser. It provides the front-end user interface for key management. It is launched by the security administrator and recovery officer from the workstations.

Cisco Key Management Center alone	Cisco KMC with RSA Key Manager for the Datacenter
Store up to 32,000 keys	Store millions of keys
Store attributes with the keys	Store attributes with the keys
Store key state	Store key state
Key access from multiple SANs	Key access from multiple SANs
Key access from multiple geographies	Key access from multiple geographies
	Enterprise database for key store
	Clustering for disaster recovery
	No single point of failure
	Database resilience
	Recommended for large number of keys
	Works with disk, database and application encryption

RSA Key Manager for the Datacenter significantly extends the capabilities provided by the Cisco KMC.

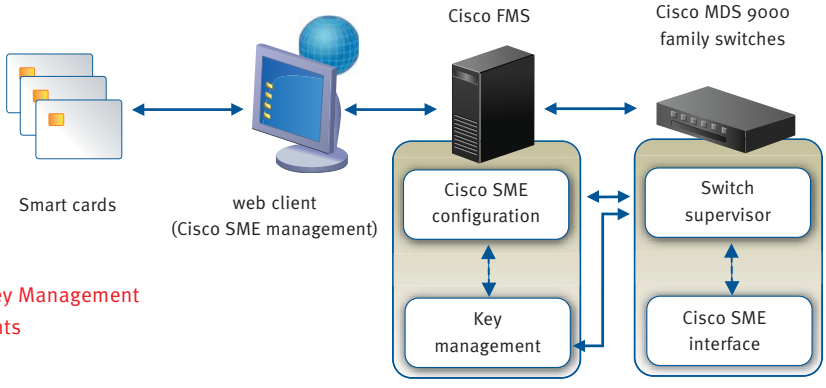


Figure 8. Cisco Key Management Center Components

– Smart cards can be used to store master keys for a cluster, and are accessed via a card reader which is attached to the workstation that is running the Cisco Fabric Manager web client. Smart cards can also be used to import and export Cisco SME information.

– The Cisco FMS manages the keys used in the Cisco SME environment. The key catalog database can be implemented in the Cisco FMS itself if an enterprise key manager is not being used. (see figure 8.)

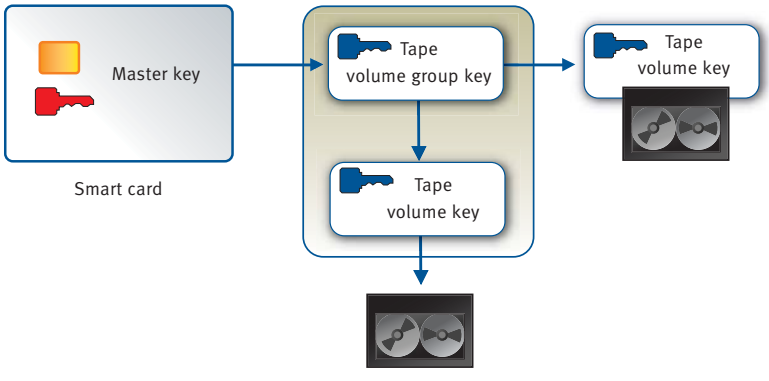
Communication among these components is secured through several mechanisms. Information passed between the Cisco Fabric Manager web client and the smart card reader is secured via a PIN that is required to access any information on the smart card.

Information between the web client and the Cisco FMS can be transmitted via the HTTPS protocol. Communication to the switches from Cisco FMS is performed using the SSH protocol.

Cisco SME uses three types of keys: the master key, tape volume group keys and tape keys. Each key in the hierarchy is wrapped, or encrypted, by the key directly above it; that is, the tape key is wrapped by the tape volume group key, which is wrapped by the master key – this key hierarchy is shown in Figure 9.

Tape keys can be stored either within the Cisco KMC or on the actual tape media. Storing the key on the media makes recovery simpler, because gaining access to the tape also grants access to the encrypted key. Tapes can also be assigned a unique key or they

Figure 9. Key Hierarchy



can all share the same key. Shared keys are less secure, as compromising a single tape compromises all tapes. In addition, if shared keys are used, then shredding of a single tape, such as to address a lost or misplaced tape, is not feasible. This is because destroying either the Tape Volume Group Key or the shared single encryption key will result in multiple tapes being destroyed.

Tape volume group keys are stored in the Cisco KMC and are unique to each tape volume group in each cluster.

The master key is unique for each Cisco SME cluster that is created. It is stored in the MSM and can be backed up in one of three ways:

– In Basic Mode, the key is saved to a text file that is secured by a password. This provides a very simple method to recover in the event of a failure, but is inherently less secure than the other methods.

– With Standard Security, the master key is stored on a smart card. If the master key is later needed, it can be retrieved by using a smart card reader attached to a management workstation. This is inherently more secure than the Basic method, as to compromise the key, someone would need to have physical access to the smart card, the reader as well as know the owner's PIN for the card. However, for those same reasons, recovery becomes more complex: for example, smart cards can be lost or PINs forgotten.

– With Advanced Mode, the key is written as "shares", which are distributed across five separate smart cards, some or all of which are required to recover the environment: for example, there is the option to require two or three of the five smart cards to recover the environment. While this is clearly the most secure environment, it also is the most complex and allows multiple of points of failure.

RSA Key Manager for the Datacenter

Key management has a great impact on both the effectiveness of encryption and on total cost of ownership for encryption solutions. There are three major reasons for this significant impact:

- The more that key management is split across different environments, the more difficult it is to align the configuration and operation of encryption in these environments with the security policies for the business. This is in part because enterprise key management systems such as RSA Key Manager implement policy-based control of how and where keys are used. But it is also because central, unified definition of key management makes it simpler to establish and maintain consistent control of keys across all environments in which encryption is performed.
- When key management is split across environments, a larger number of security experts are required for key management, often with the management cost further increased by a multiplication of tools that makes it difficult to share expertise and resources across these environments.
- When encrypted data needs to be shared between applications, groups or infrastructure, lack of centralized management for key sharing often means that data needs to be decrypted before sending it from one point to another and then re-encrypted at the destination, increasing both the cost of data sharing and the vulnerability of the data. Alternatively, if sharing of encrypted data is not supported by enterprise key management, expensive manual processes must be put in place to propagate the keys so that business processes will not be broken.

Using RSA Key Manager for the Datacenter to establish an enterprise key management environment, as shown in the Figure 10, addresses these issues to ensure both the cost effectiveness and the strength of encryption solutions.

Establishing effective data protection is possible only if the control mechanisms that an enterprise is using participate in well-understood security policies that reflect an accurate understanding of the enterprise's data, threats and risk model. Using an enterprise key management system that participates in centralized policy administration ensures that localized data protection enforcement is aligned with data protection policies. RSA Key Manager for the

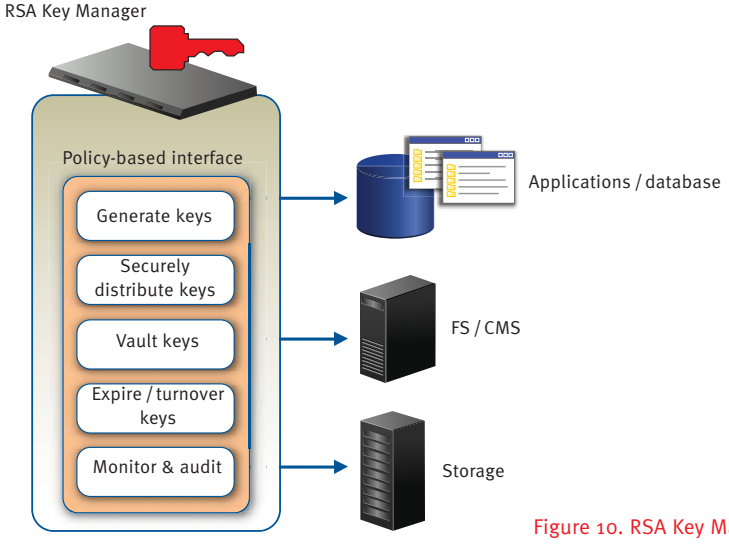


Figure 10. RSA Key Manager for the Datacenter

Datacenter provides this alignment of Cisco SME with enterprise security policy, helping to address the challenge of achieving effective and auditable security while optimizing accessibility to information and minimizing cost of operations.

The integration of RSA Key Manager with Cisco SME provides three major capabilities:

– Enterprise key management.

– Centralized vaulting and protection of keys.

– Comprehensive audit capabilities.

Enterprise key management in RSA Key Manager for the Datacenter ensures effective control of encryption, taking advantage of policy-based security rules to minimize the involvement of SAN administrators in key management. RSA Key Manager controls how long the key is available and where it is distributed, ensuring that policies regarding data availability are effectively and consistently enforced.

RSA recommends one key per tape. With the ability to manage millions of keys, RSA Key Manager for the Datacenter overcomes the limitations imposed by the Cisco KMC 32,000-key ceiling and can address an enterprise tape encryption environment and can manage keys from additional datacenter encryption sources, such as file systems, hosts, databases, and applications.

RSA Key Manager for the Datacenter provides centralized vaulting of the encryption keys for Cisco SME. Encryption keys are generated in the MSMs and vaulted in RSA Key Manager according to defined backup policies. Those keys can then be retrieved by the Cisco FMS when required for recovering data from a tape. This enables encryption deployments to scale while minimizing administrative costs and ensuring separation of duties.

RSA Key Manager for the Datacenter is required for the added benefit of replication over backup alone. This is a valuable feature, as the potential for keys to be lost between backups is greatly reduced when backup is augmented with replication. RSA Key Manager for the Datacenter incorporates Oracle® DataGuard 10G into the Key Manager server appliance, deployed in multiples of two in an active/passive configuration for redundancy.

With RSA Key Manager for the Datacenter, tape key distribution can be automated, and datacenter failover – a completely manual process without Key Manger – becomes a partially automated process. Here's how it works (assuming that every tape is assigned a unique key):

1) Datacenter 1

– Export the Key-Encrypting Key (KEK) to a smart card or to a password-protected file.

– Unwrap the Tape Key (by unwrapping the Volume Group Key with the Master Key)

– Export the keys to a text file, password protected

2) Datacenter 2

– Manually transport KEK and tape keys

– Import KEK

– Import tape keys from text file (previous step)

– Will automatically wrap keys as they are being imported

New keys would have to be moved as they are created.

Auditing of all encryption key usage activity ensures that security policies are enforced to meet compliance requirements. Vaulting of keys, restoring keys to Cisco SME interfaces, expiration or revocation of keys and distribution of keys across the enterprise can all be tracked in a secure log. This provides both the operational control and compliance visibility to ensure that encryption is being used effectively and according to defined security policies.

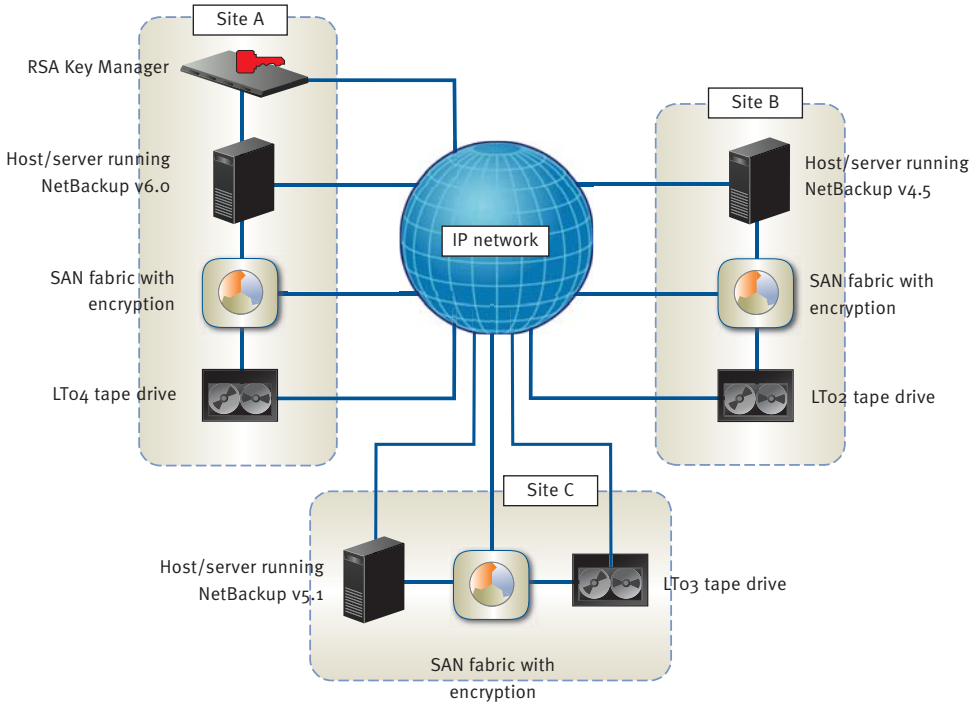
Because RSA Key Manager takes advantage of the enterprise key management interface provided by Cisco SME, deploying RSA Key Manager with Cisco SME is simple to set up. Those Cisco KMCs vaulting keys to RSA Key Manager or requesting archived keys from Key Manager are configured to communicate with a local or remote Key Manager.

Because the RSA Key Manager can be either local or remote, a single Key Manger server appliance can support complex topologies accommodating multiple geo-political areas and business units, as shown in Figure 11. Cisco Fabric Manager is used to enable RSA Key Manager for enterprise key management for Cisco SME.

Cisco SME is configured to use RSA Key Manager the first time the Cisco SME tab in the Cisco Fabric Manager web client is accessed. When the RSA Key Manager option is selected, additional information is required, as Cisco Fabric Manager must know how to access Key Manager. Additional information required is the IP Address of the Key Manager server appliance, the TCP port to access the services on the Key Manager (usually 443) and the PKI-based credentials used to gain access to Key Manager. Use of these credentials by Cisco SME and Key Manager ensures that attacks such as man-in-the-middle and injection are prevented.

Once the setup is completed, communication between the Cisco FMS and Key Manager is transparent. When the Cisco SME creates an encryption key for tape backup, the key is wrapped with the volume key, then with the master key for that Cisco KMC. The wrapped key is then immediately vaulted to RSA Key Manager via the Cisco SME application programming interface to ensure its availability for subsequent data restores. This is shown in Figure 12.

Figure 11. A single business unit or geo-political area utilizing Cisco SME and RSA Key Manager



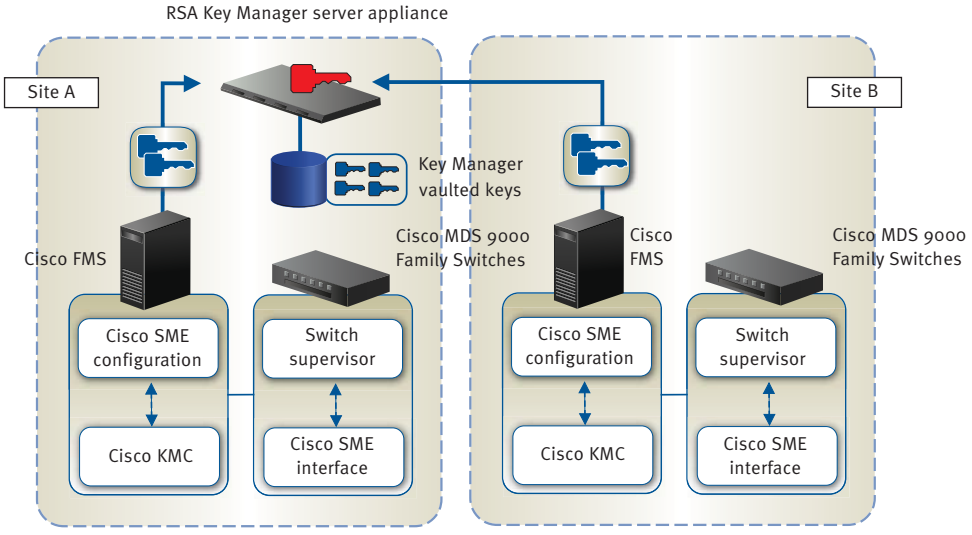


Figure 12. Vaulting Keys to RSA Key Manager for the Datacenter

When a tape is mounted for data restoration, the Cisco SME identifies the key required for decrypting that tape and the Cisco FMS requests the decryption key from RSA Key Manager via the application programming interface. Even for long-lived data retention, using RSA Key Manager with Cisco SME ensures that keys will be available without operator intervention or action.

Backup, archival and recovery of encryption keys in RSA Key Manager ensures that keys are available when needed. Business continuity can be enhanced through replication of keys across multiple active RSA Key Managers, while disaster recovery can be provided by export/import of keys to recovery sites.

RSA Key Manager for the Datacenter writes additional audit information to its own log file – beyond that provided by Cisco SME. Information written to the log file includes:

- Key-related events, such as a key is generated, a new key encryption key is generated, or a requested key is located.
- Key distribution events, such as a request is received for a new key or a key is sent to a client.
- Administrator events, such as an administrator initiates or terminates access to RSA Key Manager, a new key class is created, a new key policy is created or a new client entity is created.

In addition to this log, additional auditing information is provided by log files managed by related components, such as the database manager for the RSA Key Manager repository. Combined with the Cisco SME log files, the Key Manager audit capabilities provide a comprehensive view of key management activity in the Cisco SME environment.

Conclusion

Cisco and RSA are working together to reduce the cost, complexity and risks associated with storage media encryption. Cisco has moved storage encryption into the SAN – a highly scalable, reliable fabric service that minimizes deployment cost and disruption. RSA has provided enterprise-class encryption key management across the information technology stack. Together, RSA and Cisco provide an industy-leading, innovative and effective storage solution for addressing data protection via storage media encryption.

RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RKMCIS SB 0508

CISCO

RSA®
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com