White Paper

Cisco TrustSec Fibre Channel Link Encryption

What You Will Learn

Data integrity and confidentiality is a top priority for Cisco's customers. Storage networks may span large areas or multiple sites, and relying solely on physical security is not practical. Two requirements that are essential for secure communications are authentication and encryption.

Current Cisco® MDS 9000 Family switches support peer authentication according to the Fibre Channel Security Protocol (FC-SP) standard using the Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP), but this process does not prevent unwanted activities such as traffic interception. To help ensure data integrity and privacy, data must be encrypted.

Cisco TrustSec® Fibre Channel Link Encryption addresses customer needs for data integrity and privacy.

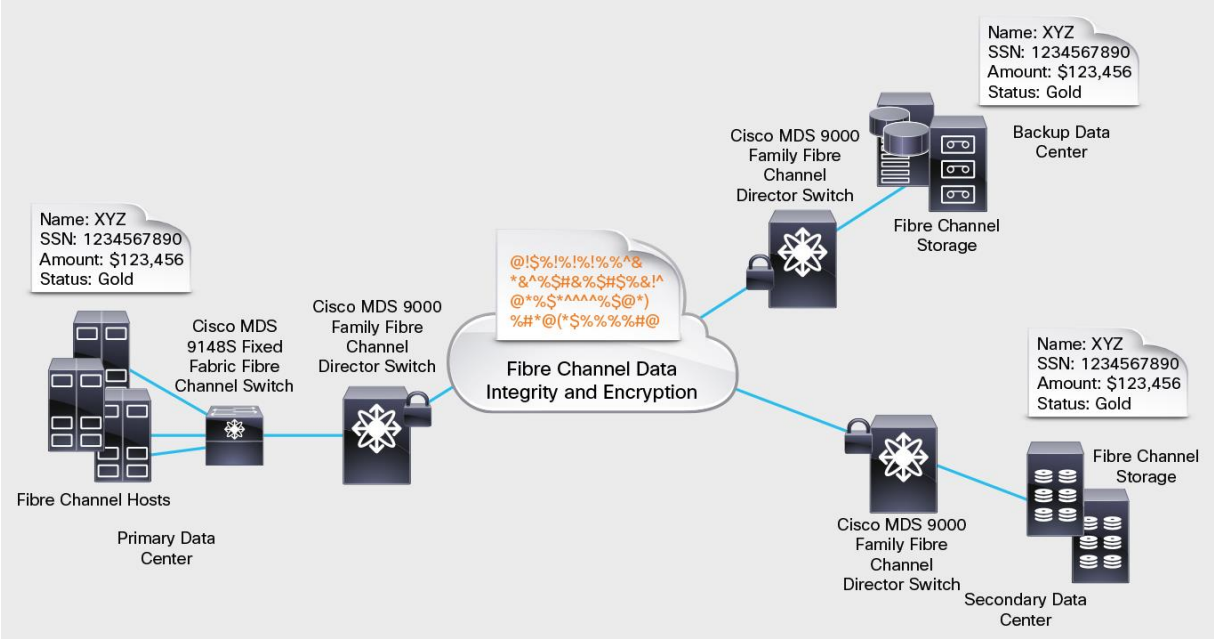
Cisco TrustSec Fibre Channel Link Encryption Overview

Cisco TrustSec Fibre Channel Link Encryption is an extension of the FC-SP standard and uses the existing FC-SP architecture. Starting with Cisco MDS 9000 NX-OS Software Release 4.2(1), Fibre Channel data traveling between E-ports on 1/2/4/8-Gbps modules and NX-OS Software Release 6.2(9) on 2/4/8/10/16-Gbps modules may be encrypted. Cisco uses the 128-bit Advanced Encryption Standard (AES) encryption algorithm and enables either AES-Galois/Counter Mode (GCM) or AES-Galois Message Authentication Code (AES-GMAC). AES-GCM encrypts and authenticates frames, and AES-GMAC authenticates only the frames that are being passed between the two peers. Encryption is performed at line rate by encapsulating frames at egress with encryption using the GCM authentication mode with 128-bit AES encryption. At ingress, frames are decrypted and authenticated with integrity checks.

There are two primary use cases for Cisco TrustSec Fibre Channel Link Encryption. In the first use case, customers are communicating outside the data center over native Fibre Channel (for example, dark fiber, Coarse Wavelength- Division Multiplexing [CWDM], or Dense Wavelength-Division Multiplexing [DWDM]). In the second use case, encryption is performed within the data center for security-focused customers such as defense and intelligence services. This feature is competitively unique and should provide a clear differentiator for campus and metropolitan-area network (MAN) deployments and high-security accounts.

Figure 1 illustrates the Cisco TrustSec Fibre Channel Link Encryption feature.

Figure 1. Cisco TrustSec Fibre Channel Link Encryption



Cisco TrustSec Fibre Channel Link Encryption with hardware and software integration using the Cisco MDS 9000 MDS Family provides an easier solution for link-to-link encryption. Cisco TrustSec Fibre Channel Link Encryption is configured and provisioned using Cisco MDS NX-OS Software and Cisco Data Center Network Manager (DCNM), the same software used to manage other data center products such as Cisco MDS 9000 Family and Cisco Nexus® Family products.

To perform encryption between the switches, a security association needs to be established. An administrator must manually configure the security association before the encryption can take place. The security association includes parameters such as encryption keys and salt (A 32-bit hexadecimal number that is used during encryption and decryption) are required for encryption. We can set up to 2000 security associations per switch. Key management is not required, and keys are stored locally on the switch.

Required Software

To use Cisco TrustSec Fibre Channel Link Encryption, Cisco MDS 9000 NX-OS Software Release 4.2(1) or later must be installed on the Cisco MDS 9000 Family switches. For 16-Gbps modules such as the DS-X9448-768K9, the minimum OS software release required is Cisco MDS NX-OS Software Release 6.2(9). Note that Cisco TrustSec is supported only on E-ports configured between Cisco MDS 9000 Family switches.

Supported Hardware

Cisco TrustSec Fibre Channel Link Encryption is supported only on the following Cisco MDS 9500 and 9700 Series Multilayer Directors switching modules:

- 48-port 2/4/8/16-Gbps Fibre Channel switching module (DS-X9448-768K9)
- 32-port 8-Gbps Advanced Fibre Channel switching module (DS-X9232-256K9)
- 48-port 8-Gbps Advanced Fibre Channel switching module (DS-X9248-256K9)
- 24-port 1/2/4/8-Gbps Fibre Channel switching module (DS-X9224-96K9)
- 48-port 1/2/4/8-Gbps Fibre Channel switching module (DS-X9248-96K9)
- 4/44-port 1/2/4/8-Gbps Fibre Channel switching module (DS-X9248-48K9)

License Information

The Cisco TrustSec Fibre Channel Link Encryption feature is included with the Cisco MDS 9000 Enterprise license. Customers who already have an installed Cisco MDS 9000 Enterprise license can use this feature; no additional licenses are required.

For More Information

- For more information about how to configure Cisco TrustSec encryption, please visit Configuring Cisco TrustSec Fibre Channel Link Encryption.
- To learn more about Cisco storage solutions for the data center, visit http://www.cisco.com/go/storage.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-545124-01 08/14