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 of storage networking solutions 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 2/4/8/16-Gbps modules is 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 rates 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 communicate 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 below illustrates the Cisco TrustSec Fibre Channel Link Encryption feature.
Cisco TrustSec Fibre Channel Link Encryption with hardware and software integration using Cisco MDS 9000 family of storage networking solutions 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 the Cisco MDS 9000 family.

To perform encryption between 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 (SAs) per switch. Security key management is not required, as they are stored locally on.

**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 Series Multilayer Switches. For 16-Gbps modules such as the DS-X9448-768K9, the minimum requirement is Cisco MDS NX-OS Software Release 6.2(9). For 32-Gbps modules such as the DS-X9648-1536K9, the minimum NX-OS software release requirement is 8.1(1). Note that Cisco TrustSec is supported only on E-ports configured between supported Cisco MDS 9000 Series Multilayer switches.
Supported hardware

Following Cisco MDS 9500 and 9700 Series Multilayer Directors switching modules and MDS 9000 Fibre Channel Fabric Switches support Cisco TrustSec Fibre Channel Link Encryption:

- 4/44-port 1/2/4/8-Gbps Fibre Channel switching module (DS-X9248-48K9)
- 48-port 1/2/4/8-Gbps Fibre Channel switching module (DS-X9248-96K9)
- 24-port 1/2/4/8-Gbps Fibre Channel switching module (DS-X9224-96K9)
- 48-port 8-Gbps Advanced Fibre Channel switching module (DS-X9248-256K9)
- 32-port 8-Gbps Advanced Fibre Channel switching module (DS-X9232-256K9)
- 48-port 2/4/8/16-Gbps Fibre Channel switching module (DS-X9448-768K9)
- 48-port 4/8/16/32-Gbps Fibre Channel switching module (DS-X9648-1536K9)
- Cisco MDS 9000 24/10-Port SAN Extension Module (DS-X9334-K9)
- Cisco MDS 9396S 16-Gbps 96-Port Fibre Channel Fabric Switch
- Cisco MDS 9132T 32-Gbps 32-Port Fibre Channel Fabric Switch
- Cisco MDS 9148T 32-Gbps 48-Port Fibre Channel Fabric Switch
- Cisco MDS 9396T 32-Gbps 96-Port Fibre Channel Fabric Switch

Supported ports across different modules

The Cisco TrustSec Fibre Channel Link Encryption feature is supported on selected ports out of each port group on modules and/or switches. Here is the list of ports where this feature can be enabled:

- 48-port 32-Gbps Fibre Channel Switching Module (DS-X9648-1536K9) – supported on ports 9-12, 25-28, and 41-44
- Cisco MDS 9132T Fibre Channel Switch – supported on ports 9-12 and 25-28
- Cisco MDS 9148T Fibre Channel Switch – supported on ports 9-12, 25-28, and 41-44
- Cisco MDS 9396T Fibre Channel Switch – supported on 9-12, 25-28, 41-44, 57-60, 73-76, and 89-92 ports

License information

The Cisco TrustSec Fibre Channel Link Encryption feature is included with the Cisco MDS 9000 Enterprise license package. Customers who already have an installed Cisco MDS 9000 Enterprise license can use this feature; no additional licenses are required. Customers can also try this feature without purchasing an enterprise license for a period of 120 days. More details about the Cisco MDS 9000 Enterprise license package can be found here.
For more information

- For more information about how to configure Cisco TrustSec encryption, please visit Configuring Cisco TrustSec Fibre Channel Link Encryption Guide

- To learn more about Cisco storage solutions for the data center, visit https://www.cisco.com/c/en/us/products/storage-networking/index.html