

Security Overview

The Cisco MDS 9000 NX-OS software supports advanced and configurable security features that provide security within a Storage Area Network (SAN). These features protect your network against deliberate or unintentional disruptions from internal or external threats. Cisco MDS 9000 NX-OS hardware also provides intrinsic security capabilities, notably anti-counterfait technology and secure boot. The Cisco NX-OS operating system also receives regular updates in terms of known vulnerabilities, as determined by Cisco Product Security Incident Response Team. For more information, see PSIRT. For this reason, Cisco NX-OS can be considered a hardened operating system.

This chapter includes the following sections:

- FIPS, on page 1
- Users and Common Roles, on page 2
- AAA Options, on page 2
- IP ACLs, on page 2
- PKI, on page 3
- Information About SSH Services, on page 3
- IPsec, on page 3
- FC-SP and DHCHAP, on page 3
- Port Security, on page 4
- Fibre Channel Common Transport Management Server Query, on page 4
- Fabric Binding, on page 4
- TrustSec Fibre Channel Link Encryption, on page 4

FIPS

The Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module should be a set of hardware, software, firmware, or some combination that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary. FIPS specifies certain crypto algorithms as secure, and it also identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

For more information on configuring FIPS, see Configuring FIPS.

Users and Common Roles

Role-based access control (RBAC) limits access to switch operations by assigning users to roles. All management access within the Cisco MDS 9000 Family is based upon roles. Users are restricted to performing the management operations that are explicitly permitted, by the roles to which they belong. For example, one user might have an administrator role on a specific VSAN.

For information on configuring users and common roles, see Common Roles.

AAA Options

RADIUS and TACACS+

The authentication, authorization, and accounting (AAA) feature verifies the identity of, grants access to, and tracks the actions of users managing a switch. All Cisco MDS 9000 Family switches can use RADIUS and TACACS+ protocols to communicate with remote AAA servers. This combination of MDS 9000 with AAA servers provides a centralized user account management capability.

If MDS 9000 switches is acting as a network access server, then the communication between your network access server and the RADIUS or TACACS+ security server is through AAA.

The chapters in this guide describe the following features:

- Switch AAA functionalities—A function by which you can configure AAA switch functionalities on any switch in the Cisco MDS 9000 Family, using the command-line interface (CLI) or Simple Network Management Protocol (SNMP).
- RADIUS—A distributed client and server system implemented through AAA that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco MDS 9000 switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.
- TACACS+—A security application that provides a centralized AAA solutions with validation of users who are attempting to gain access to an MDS 9000 switch. TACACS+ services are maintained in a database on a TACACS+ daemon that typically runs on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.

For information on configuring RADIUS and TACACS+, see Configuring Security Features on an External AAA Server.

IP ACLs

IP access control lists (ACLs) provide basic network security on the out-of-band management Ethernet interface and the in-band IP management Interface. The Cisco MDS 9000 Family switches use IP ACLs to restrict traffic from unknown and untrusted sources and restrict network use based on user identity or device type.

For information on configuring IP ACLs, see Configuring IPv4 and IPv6 Access Control Lists.

PKI

The Public Key Infrastructure (PKI) allows an MDS 9000 switch to obtain and use digital certificates for secure communication in the network. PKI support provides manageability and scalability for applications that support digital certificates, such as IPsec, IKE, and SSH.

For information on configuring PKI, see Configuring Certificate Authorities and Digital Certificates.

Information About SSH Services

Secure Shell (SSH) is a protocol that provides a secure, remote connection to the Cisco NX-OS CLI. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. You can use SSH keys for the following SSH options:

- SSH2 using RSA
- SSH2 using DSA

Starting from Cisco MDS NX-OS Release 8.2(1), SHA2 fingerprint hashing is supported on all Cisco MDS devices by default.

A secure SSH connection, with a RSA key is available as default on all Cisco MDS 9000 Series Switches. If you require a secure SSH connection with a DSA key, you need to disable the default SSH connection, generate a dsa key, and then enable the SSH connection (see the Generating the SSH Server Key Pair section).

Use the **ssh key** command to generate a server key.



Caution If you are logging in to a switch through SSH and you have issued the **aaa authentication login default none** command, you must enter one or more keystrokes to log in. If you press the **Enter** without entering at least one keystroke, your log in will be rejected.

For more information about configuring SSH services, see Configuring SSH Services and Telnet

IPsec

IP Security (IPsec) protocol is a framework of open standards by the Internet Engineering Task Force (IETF) that provides data confidentiality, data integrity, and data origin authentication between participating peers. IPsec provides security services at the IP layer, including protecting one or more data flows between a pair of hosts, a pair of security gateways, or a security gateway and a host.

For information on configuring IPsec, see Configuring IPSec Network Security.

FC-SP and DHCHAP

Fibre Channel Security Protocol (FC-SP) capabilities provide switch to switch and hosts to switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol that provides authentication between Cisco MDS

9000 Family switches and other devices. DHCHAP consists of the CHAP protocol combined with the Diffie-Hellman exchange.

With FC-SP, switches, storage devices, and hosts are able to prove their identity through a reliable and manageable authentication mechanism. With FC-SP, Fibre Channel traffic can be secured on a frame-by-frame basis to prevent snooping and hijacking, even over untrusted links. A consistent set of policies and management actions are propagated through the fabric to provide a uniform level of security across the entire fabric. The current implementation is aligned to FC-SP-2 version.

For more information on configuring FS-SP and DHCHAP, see Configuring FC-SP and DHCHAP.

Port Security

The port security feature prevents unauthorized access to a switch port by binding specific world-wide names (WWNs) to specific switch ports.

When port security is enabled on a switch port, the devices connecting to that port must be in the port security database and must be listed in the database as bound to a given port. If both of these criteria are not met, the port will not achieve an operationally active state and the devices connected to the port will be denied access to the SAN.

For information on configuring port security, see About Port Security.

Fibre Channel Common Transport Management Server Query

With the FC-CT query management feature, an administrator can configure the network in such a manner that only a storage administrator or a network administrator can send queries to a switch and access information such as devices that are logged into the fabric, switches in the fabric, how they are connected, how many ports each switch has and where each port is connected, configured zone information and privilege to add or delete zone and zone sets, and Host Bus Adapter (HBA) details of all the hosts connected in the fabric and so on.

For information on configuring fabric binding, see About Fibre Channel Common Transport.

Fabric Binding

The fabric binding feature ensures Inter-Switch Links (ISLs) are enabled only between specified switches in the fabric binding configuration. This feature helps prevent unauthorized switches from joining the fabric or disrupting the current fabric operations. This feature uses the Exchange Fabric Membership Data (EEMD) protocol to ensure that the list of authorized switches is identical in all of the switches in a fabric. Fabric binding is optional for Opens Systems while it is mandatory for FICON deployments.

For information on configuring fabric binding, see About Fabric Binding.

TrustSec Fibre Channel Link Encryption

Cisco TrustSec Fibre Channel Link Encryption is an extension of the Fibre Channel-Security Protocol (FC-SP) feature and uses the existing FC-SP architecture to provide integrity and confidentiality of transactions. Encryption is added to the peer authentication capability to provide security and prevent unwanted traffic

interception. Peer authentication is implemented according to the FC-SP standard using the Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) protocol.

For information on configuring TrustSec Fibre Channel Link Encryption, see About Fibre Channel Common Transport.