

Emulex LightPulse Fibre Channel HBA Family and Cisco MDS Family Solutions for Fabric Authentication

**A Technology Overview for
SAN Security using
Fibre Channel Security Protocol (FC-SP)**



Scope of this Paper:

This co-authored technology overview provides data center users with valuable information for understanding the benefits of FC-SP technology and practical use cases and deployment scenarios for maximizing these benefits.

This guide is intended to introduce the concepts of FC-SP using Emulex and Cisco products. General use cases are presented and possible benefits are mentioned. Actual customer configurations can vary widely along with results, and these deployment scenarios may not be possible or practical in any given case. Please consult with your Cisco or Emulex representative on specific questions based on your specific needs.

The capabilities described herein are not intended to imply specific product features or capabilities from Cisco or Emulex that may or may not be available at any time.

Introduction

Data security breaches are on the rise and not a week goes by without some kind of security incident in the headlines. Corporations are starting to realize that what they consider to be their greatest asset, their information, can also be a tremendous liability. Increasingly, data security and privacy regulations—such as Sarbanes-Oxley, and the Health Insurance Portability and Accountability Act (HIPAA)—are holding firms responsible for safeguarding their data and disclosing any incident. Regulatory compliance is putting the burden on corporations to exercise due diligence in deploying adequate security solutions. Additional pressure is fueled by the risk of negative public exposure and notification costs associated with a breach. The storage infrastructure must be secured from both inside and outside attackers, so it does not become a potential source of vulnerabilities. This is an essential addition to a data centric security strategy.

Storage security has often been overlooked as an area of concern but can have significant impact given how critical an asset data is to almost every organization. Storage security ranks with server and network security as a top-of-mind issue to IT management.

The increasing frequency of data security breaches has been chronicled on a global scale. In the United States alone, over 229 million records have been lost since January 2005 according to www.privacyrights.org. Identity theft has victimized well over 15 million consumers over the last year. A recent survey indicates that 19% of customers who were notified of a security breach took their business elsewhere. Another 40% were considering the same thing. Only 8% of consumers who receive a security breach notification did not blame the organization that suffered the breach. This is no theoretical exercise; information security breaches impact companies that experience them in terms of lost customers, lost market share, and the direct costs to comply with notification requirements. The negative impact of a breach can cost much more money than would an intelligent security investment.

In addition, the burden of regulatory compliance drives the need for storage-centric security. Chief level executives are looking to IT management for compliance solutions to minimize their legal liability and keep their companies off the front pages. In industries ranging from financial services to healthcare, investments in data availability and information privacy are at the heart of present and projected IT budgets.

The Value of Authentication for Fibre Channel Networks

The data center needs a cohesive and scalable security solution; one that is dynamically managed and interoperable with today's enterprise storage infrastructure. And in a world where server virtualization grows in popularity, the requirement for dynamic storage security and authentication solutions is compounded. There is, then, a need to secure the storage infrastructure and this white paper covers how Fibre Channel Authentication can improve an organization's security posture.

There is a new wave of better integrated, streamlined solutions from experienced mainstream vendors like Cisco and Emulex who are adding security features to their popular storage solutions. These new solutions are standards based and tightly integrated into the storage infrastructure, as opposed to being bolted on to it.

Some of the benefits of host-to-fabric and switch-to-switch authentication include:

- Integrates security into the end-point to provide strong server-to-switch authentication.
- Provides built-in security for the Fibre Channel Network to ensure that only authorized devices can access the fabric, and unauthorized devices cannot.
- Protects against pWWN spoofing, host masquerading and rogue/compromised servers that may be the launching point of an intrusion.
- Improves system stability and availability by reducing unplanned downtime due to administrative errors.

FC-SP Technology

The many standards that make up the Fibre Channel protocol are developed by the International Committee for Information Technology Standards (INCITS), an American National Standard Institute (ANSI) accredited standards committee. In 2002, INCITS began working on security protocols for Fibre Channel to address weaknesses in authenticating communication between devices on the SAN. ANSI/INCITS 426-2007 Fibre Channel Security Protocol (FC-SP) is the first fruit of this activity.

FC-SP is a new specification for Fibre Channel security, featuring device-to-device authentication, management of authentication passwords—known as shared secrets—data origin authentication, and anti-replay protection. These provisions safeguard SAN traffic against unauthorized access and help to prevent accidental configuration changes from interrupting application availability.

FC-SP has been drafted as a modular standard and defines different levels of compliance: to claim FC-SP Authentication Compliance (AUTH-A), a storage networking device, host bus adapter (HBA), or storage system, must support switch-to-switch, device-to-switch, and device-to-device authentication using the Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) with a NULL DH group. According to this profile, before allowing communication, FC-SP requires the devices to authenticate each other using a unique value, known as a shared secret.

To perform authentication, each fabric component must either know the shared secret associated with other entities with which it is communicating or rely on a third-party that knows the secret, such as a Remote Authentication Dial In User Service (RADIUS) server. Each device must also know, or be able to access, its own secret. This process eliminates the possibility of unauthenticated communication, and is effective in safeguarding the SAN against a network attack using a rogue server or switch capable of impersonating a valid device.

The authentication provided by the FC-SP AUTH-A compliant devices is of the utmost importance in the SAN, since many Fibre Channel specific access control mechanisms rely upon the device identity known as Port World Wide Name (pWWN). The pWWN, a sort of MAC address, is not intended to be secure and tamper-proof, and there are many management tools that allow changing the pWWN of a device, with a perfectly legitimate scope. The side effect of the relative ease of changing a pWWN is that the traditional Fibre Channel access control may be bypassed to reach an illegitimate goal.

Examples of traditional Fibre Channel access control functionalities that depend on the pWWN are:

- 1) Zoning, the basic tool in Fibre Channel to restrict the communication between a given group of devices.
- 2) Port Security, the ability to bind a specific device to a specific switch interface to minimize connection errors.
- 3) Logical Unit Number (LUN) mapping and masking, functionality built in the storage devices or servers to limit or profile the data access depending on what the host is authorized to access.

The deployment of FC-SP based authentication guarantees the effectiveness of the traditional Fibre Channel access control approach even if the attacker can use the pWWN of a valid device.

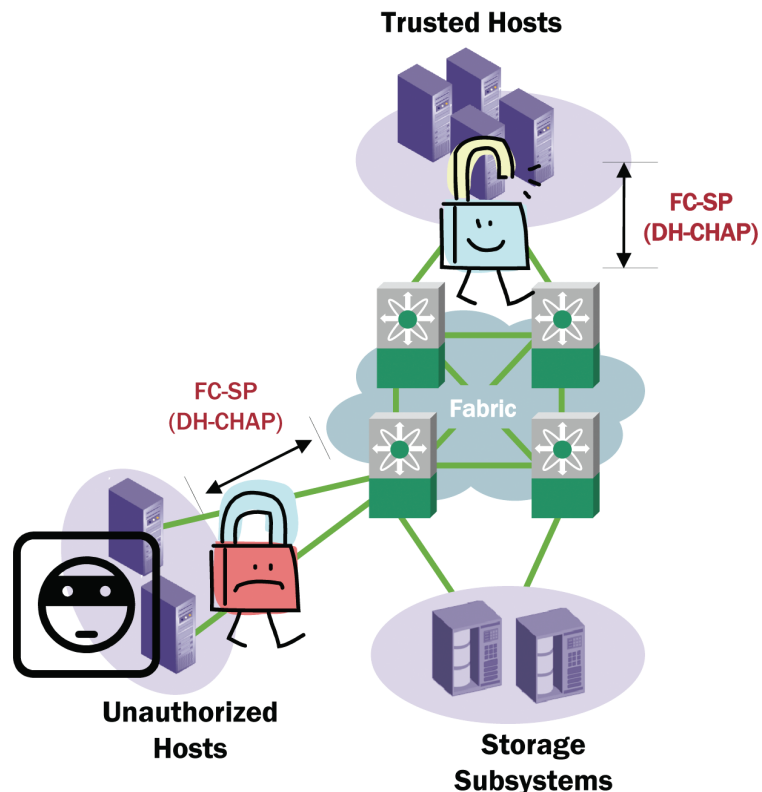


Figure 1: Host Threats Prevented by Implementation of DH-CHAP Authentication by the HBA

FC-SP is flexible, allowing devices that support the protocol to operate in a fabric that includes non-FC-SP compliant resources. Devices that support FC-SP generally turn the protocol off by default, allowing administrators to consciously map a security structure onto chosen components of the fabric.

Cisco Switch FC-SP Support

The Cisco MDS 9000 Family of Fibre Channel switches and directors provides an holistic approach to SAN security. Support for FC-SP authentication, fully integrated with Cisco's Authentication, Authorization, and Accounting (AAA) framework, provides the foundation for secure connectivity to the Fabric, and for secure switch to switch interconnection. The security of the control plane is ensured by the use of secure out-of band management protocols such as https, ssh (Secure Shell) and SNMPv3 that provide authentication, integrity protection and confidentiality.

Fabric connectivity security is referred as 'port security' when concerned about the connection of end devices to a fabric port, and it is referred as 'fabric binding' when concerned about switch to switch connections.

Both port security and fabric binding rely upon the support of FC-SP using DH-CHAP for switch-to-switch and device-to-switch authentication. A switch configured to require FC-SP authentication will only allow trusted devices to be connected to the fabric, preventing unauthorized access and protecting the stability of the fabric protocol and services.

By default, FC-SP is disabled in all Cisco MDS 9000 Family switches. Enabling the functionality allows each port to be configured with a different authentication mode. These modes are:

Mode	Description
On	Authentication is performed and if the connected device does not support FC-SP the link is moved to an isolated state
Auto-Active	Authentication is attempted, but access is allowed with or without corresponding FC-SP support in the connected device
Auto-Passive	The switch does not initiate authentication but will support FC-SP if a connected device tries to authenticate
Off	The switch does not support authentication and authentication attempts are sent an error message

If a port's mode is changed to anything other than off, the switch will automatically attempt to perform again the authentication procedure.

The Cisco MDS 9000 family of switches enforces a strong security policy for the FC-SP credentials used in a Fabric. All the FC-SP secrets must contain numbers and case sensitive letters only, and be between eight and 64 characters in length.

The Cisco MDS 9000 Family of switches can perform FC-SP authentication using an external authentication server that ties into Cisco's Authentication, Authorization, and Accounting (AAA) security framework. The use of a RADIUS or Terminal Access Controller Access-Control System Plus (TACACS+) server is recommended for fabrics with more than five switches.

For fabrics with fewer than five switches it's possible to manage FC-SP secrets locally in the fabric without the use of an external AAA server. There are three alternative approaches to locally manage these shared secret, from the least to the most secure:

- use the same shared secret for all the switches in the fabric.
- use a unique secret for each switch, with the list of all shared secrets available to every switch.
- use a different pair of shared secrets for each unique pair of switches in the fabric. An attacker compromising one switch will communicate only with the immediate neighbors of the compromised switch.

Emulex LightPulse Fibre Channel FC-SP Support

Emulex has taken the next step by extending authentication to the fabric edge, protecting access to critical enterprise data. Emulex security solutions provide protection from compromised management, LUN access violations, impersonation attacks, and human error. FC-SP is an important security technology that is supported at the end-point, improving security for the storage network as outlined below.






Threats			
Compromised management 	LUN access violation 	Impersonation attack 	Human error 
Typical Countermeasures			
<ul style="list-style-type: none"> • Authorization • Access control • Authentication 	<ul style="list-style-type: none"> • LUN masking on storage side • Access control 	<ul style="list-style-type: none"> • Authentication 	
Emulex Value-Add Security Capabilities			
<ul style="list-style-type: none"> • HBAnyware secure remote management • Authenticated CT 	<ul style="list-style-type: none"> • LUN masking on HBA • NPIV for zoning and masking at VM level 	<ul style="list-style-type: none"> • FC-SP compliance • DH-CHAP support 	

Figure 2: Simplified Threat Model and Defenses for HBA Security

FC-SP is an incremental layer of security supported by Emulex LightPulse HBAs that provides host to switch authentication services to ensure that only the hosts connected to a Fibre Channel network are authorized ones. Furthermore, FC-SP configurations need to be complementary with other HBA based access controls and HBA security parameters must be securely managed.

1. **Authenticated Fabric Access:** Integration of FC-SP into the Emulex's LightPulse Fibre Channel HBAs for host to fabric authentication protects the storage network from malicious attacks or incidents that may lead to a security breach. Furthermore, FC-SP protects the system from accidental misconfigurations that can also lead to data corruption, accidental access to sensitive data, or unplanned system downtime
2. **Complementary to Advanced HBA Access Controls – HBA based LUN Masking and NPIV:** Emulex LightPulse Fibre Channel HBA FC-SP deployments are complementary to current HBA access control techniques such as LUN Masking and NPIV (Network Port Identifier Virtualization) configurations. When FC-SP authentication is enabled, the authentication process occurs before other access control mechanisms are applied. Once FC-SP Authentication has been passed, the HBA joins the fabric in the same way as it did without authentication.
3. **HBA Management Access:** Along with improved security for Emulex's LightPulse HBAs is the need for secure management of the shared secret used for FC-SP Authentication. Emulex's HBAnyware provides remote management for configuration and operation of FC-SP. To make sure that the HBA configuration is not compromised, Emulex supports CT-Authentication to secure in-band management ensuring that only authorized administrators are able to manage the configuration. CT-Authentication is described in the following page.

End-Point Configuration of FC-SP parameters – An Example

Centralized management of HBAs can be shown with the Emulex HBAnyware management suite. The HBAnyware screen shot, in Figure 3, shows the details of the different parameters that can be configured for FC-SP authentication. FC-SP can be configured in an enabled, passive, or disabled mode, as described in the following table.

Mode	Description
Enabled mode	Forces connected devices to authenticate
Passive Mode	Advertizes the HBA's ability to authentication and will authenticate if requested
Disabled Mode	Turns off authentication

The bidirectional parameter enables the HBA to authenticate one direction, such as a server authenticating to a switch and bidirectional where each device authenticates each other. Depending on the FC-SP architecture, one-way authentication may make for an easier deployment without compromising security. Otherwise, two-way authentication may be more secure. FC-SP supports other link authentication features that are common in other network types. Parameters such as forced reauthentication, DH group priority, and Hash priorities can all be configured.

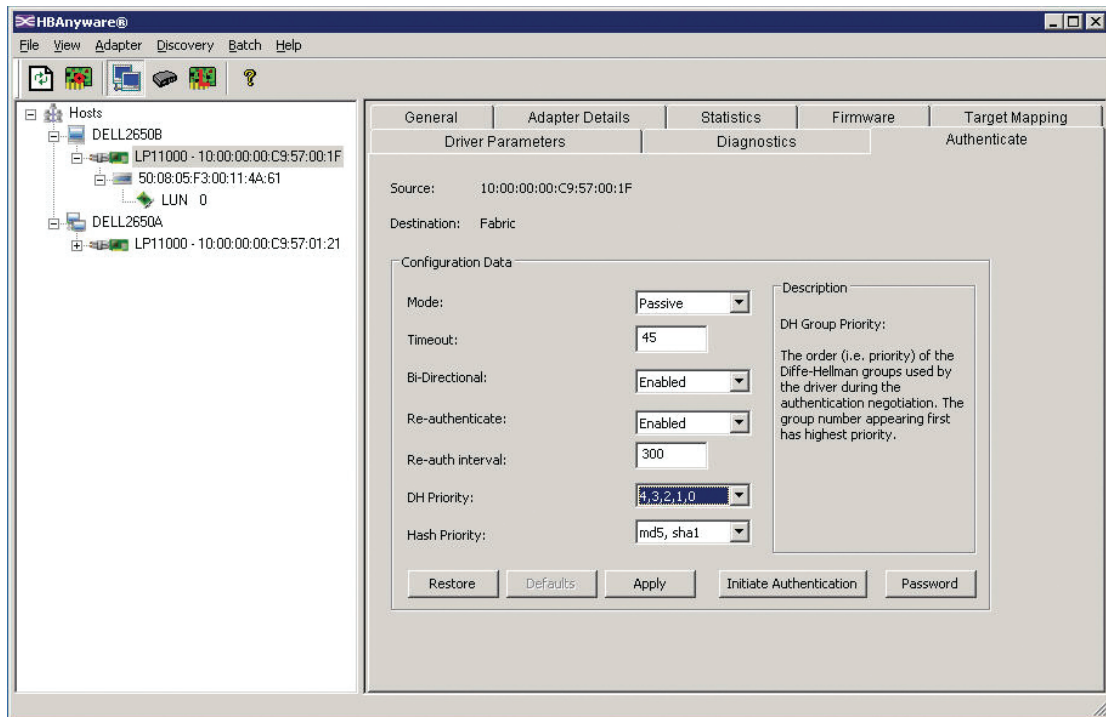


Figure 3: HBAnyware 3.3 Authenticate Screen provides an intuitive administrative interface for establishing DH-CHAP Authentication to the Fabric.

The shared secrets used for one-way or bidirectional authentication can be set from this screen via the password button. The 128 bit number that represents the password should be a random number, and it needs to match the password that is stored in the switch and corresponds to that specific HBA. Each HBA in the environment will need to be configured with its own secret. Furthermore, each HBA secret will need to be populated into each corresponding switch that the HBA is connected to. If a RADIUS server is incorporated into the environment, the HBA secrets will need to be populated into that database as well.

CT-Authentication

Remote in-band management access is protected by using CT-Authentication. With CT-Authentication, data center administrators can manage HBAs from a centralized management tool, and securely configure the HBA. Emulex HBAs support Authenticated Common Transport (Authenticated CT) protocol as defined in Fibre Channel Global Services 3 (FC-GS-3) specification.

Support of Authenticated CT satisfies the number one recommendation of the Storage Networking Industry Association's (SNIA) storage security initiative, calling for securing of the management path. More specifically Emulex HBAnywhere includes enhanced administrator validation for HBAs managed

both in-band and out-of band. Emulex's robust, secure remote management is based on security policies and allows for defined and enforceable access control lists and privileges. Authenticated CT support provides a more trusted methodology for managing HBAs when compared other options.

Conclusion

HBA authentication using the Fibre Channel Security Protocol (FC-SP) provides the mechanism for trusted servers to access the Fibre Channel network and denies access to the Fabric to unauthorized servers. FC-SP authentication is an additional layer of protection above and beyond physical security, fabric zoning, LUN masking, and NPIV.

FC-SP provides secure server to switch communication protocol that allows storage devices to prove to the requesting party that it has correctly identified that a particular node is the authorized node and communication with that node can be trusted. Authentication is done using the DH-CHAP protocol. Depending on the configuration, both the HBA and the switch can independently validate the identity of the other device. DH-CHAP prevents WWN spoofing (i.e. impersonation, masquerading attacks) and is designed to withstand replay, offline dictionary password lookup and challenge reflection attacks.

Cisco and Emulex are active and influential contributors to the FC-SP standard. As a sound storage security becomes a basic requirement in any data center, both companies are committed to deliver flexible and standards-based security technologies that will help mitigate data storage security risks and address threats in the Fibre Channel storage space.

Cisco and Emulex stand ready to supplement data center resources with the deep expertise and a wide range of products, to develop and deploy an interoperable, easy-to-use and cost effective storage security infrastructure.

For more information

To help you achieve your SAN security goals, please contact your Cisco or Emulex representative for information on Emulex LightPulse FC HBA and Cisco MDS Family products employing FC-SP authentication technology.

Cisco Systems, Inc. 170 West Tasman Drive, San Jose, CA 95134-1706 USA Tel 408-526-4000

www.cisco.com

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.

Emulex Corporation. 3333 Susan Street, Costa Mesa, CA 92626 USA Tel 714-662-5600 www.emulex.com

Copyright © 2007 Emulex. All rights reserved worldwide. No part of this document may be reproduced by any means or translated to any electronic medium without the prior written consent of Emulex.

Information furnished by Emulex is believed to be accurate and reliable. However, no responsibility is assumed by Emulex for its use; or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright or related rights of Emulex. Emulex, the Emulex logo, LightPulse and SLI are trademarks of Emulex.

