



By Robert Winter  
Dan McConnell

# SECURITY THROUGH MATURITY: A BRIEF ON SECURING iSCSI NETWORKS

Internet SCSI (iSCSI) offers a scalable, simplified, cost-effective way to implement storage area networks (SANs) using standard Ethernet components. By understanding the core elements of network security, key differences between iSCSI and Fibre Channel, and best practices for securing iSCSI networks, administrators can implement robust, secure iSCSI SANs.

Internet SCSI (iSCSI) can provide a number of advantages in enterprise storage area network (SAN) infrastructures—offering similar scalability, availability, and manageability as Fibre Channel in a cost-effective way, and enabling IT administrators to work with standard, familiar Ethernet components rather than specialized Fibre Channel equipment. iSCSI-capable Dell™ EqualLogic™ PS Series, Dell PowerVault™, and Dell/EMC storage systems can provide a simplified, scalable way to implement iSCSI SANs.

The underlying technologies—the iSCSI protocol, Ethernet, and TCP/IP transport—help provide a well-known, mature, and cost-effective security infrastructure for iSCSI SANs. Understanding the core elements of effective security strategies, the differences between iSCSI and Fibre Channel security, and best practices for iSCSI security can help administrators create robust, secure iSCSI SAN deployments.

## CORE ELEMENTS OF EFFECTIVE SECURITY

Storage-based security can be grouped into two distinct areas, referred to as data at rest (DAR) and data in flight (DIF). Both DAR and DIF have security strategies that include elements of authentication, authorization, and data coherence. Because DAR refers to data contained within a physical device and DIF refers to data moving between devices, not all of these elements need be present at the same time,

and each may have differing levels of implementation in a given environment.

### Data-at-rest and data-in-flight security

DAR provides security for a physical storage device by encrypting data and providing secure access to data on the device—helping prevent unauthorized data access even if the device is removed from its secure infrastructure. DIF provides network-oriented security, including encryption of packet, or *protocol data unit* (PDU), contents to help ensure payload confidentiality; PDU hashing to help ensure delivery integrity; and secure access to network entities.

DAR security may not be required if physical access to storage devices is strictly controlled, while DIF security may not be required for a SAN that is isolated from other networks. DIF security is recommended if the transported data supports public or shared access, such as remote storage replication over a public network for backup or disaster recovery. An effective security strategy should evaluate the needs of the specific environment and provide guidance on implementation.

### Authentication, authorization, and data coherence

In iSCSI environments, *authentication* refers to the login phase authentication of the initiator, or the mutual authentication of the initiator and target. Several

#### Related Categories:

Best practices

Fibre Channel

Internet SCSI (iSCSI)

Network security

Security

Storage

Storage area network (SAN)

Visit [DELL.COM/PowerSolutions](http://DELL.COM/PowerSolutions) for the complete category index.

cryptographic techniques are possible for iSCSI authentication: Kerberos V5 (KRB5), Simple Public-Key Generic Security Services Application Programming Interface (GSS-API) Mechanism 1 (SPKM1), Simple Public-Key GSS-API Mechanism 2 (SPKM2), Secure Remote Password (SRP), and Challenge Handshake Authentication Protocol (CHAP). CHAP is by far the most common method and is required for iSCSI devices to implement. It uses one-way, three-phase authentication for targets authenticating initiators and for initiators authenticating targets, which is generally sufficient for the majority of storage environments.

*Authorization* defines allowed actions. Access control, implemented in most types of networks using access control lists (ACLs), provides authorization of communication channel access based on information contained in PDUs, such as IP address, iSCSI Qualified Name (IQN), virtual LAN (VLAN), and other parameters (also called *n*-tuples). Authorization can be as simple as permitting access to resources from well-known *n*-tuples unique to an iSCSI session, or may include additional layers of authorization that further restrict user access to not only devices but also services.

*Data coherence* preserves data confidentiality and integrity. Confidentiality is commonly termed encryption, and helps ensure that the data payload is transmitted securely. Integrity is commonly termed hashing, and helps ensure that information received has not been modified. iSCSI data confidentiality provides encryption of information over an iSCSI frame. iSCSI data integrity may be provided at five levels: the Ethernet, TCP, IP, iSCSI, and IP Security (IPsec) checksums. In Ethernet, the checksum is also called the frame check sequence (FCS) and is a 32-bit cyclic redundancy check (CRC). The iSCSI checksum is also called the iSCSI digest, and may cover multiple iSCSI PDUs.

## COMPARISON OF iSCSI AND FIBRE CHANNEL SECURITY

iSCSI provides a more mature security solution set than Fibre Channel. iSCSI security

today is managed at the endpoints (initiator and target) by way of robust authentication and authorization techniques.

Fibre Channel security is managed in the network and the endpoints, which makes it more difficult to manage than iSCSI and creates additional challenges for security management. The vast majority of critical communications today occur over TCP/IP and not over Fibre Channel. TCP/IP-based security has thus by necessity become increasingly mature over decades of development. Because iSCSI is defined and transported over TCP/IP, it can make comprehensive use of the deep, robust pool of available security technologies and strategies that enable solutions across the authorization, authentication, and data coherence security elements. Fibre Channel, in contrast, has only recently proposed a solution for data coherence: Fibre Channel Security Protocol (FC-SP). Although this proposal borrows from many of the base technologies that IPsec uses, it is not yet deployable and does not therefore have the necessary maturity of the iSCSI solution set. It will likely take years of trial and error before appropriate operational security strategies are developed across Fibre Channel to cover all key security elements. Figure 1 shows the iSCSI

and Fibre Channel protocol layers, and Figure 2 summarizes the basic components of iSCSI and Fibre Channel security.

Fibre Channel, which is not a generally well-known or widely used protocol, offers a policy of *security through obscurity*. iSCSI, which runs over well-established protocols, provides *security through maturity* using robust security protocols and techniques. iSCSI therefore can also continue to evolve by taking advantage of the work being done on both Ethernet and TCP/IP standards.

### Passive, active, and operational attacks

Attacks on SANs, such as iSCSI or Fibre Channel SANs, typically fall into one of three categories: passive, active, and operational. A *passive attack* is based on snooping of clear-text information in the packet stream, with *n*-tuples comprising IP addresses, Media Access Control (MAC) addresses, World Wide Names (WWNs), IQNs, VLANs, TCP port numbers, and other parameters. Attacks can occur using individual management interfaces on switches or through mirrored switch ports, which can access data on other ports. SANs can also be vulnerable to a passive attack if the attackers have physical access to the fabric cabling.

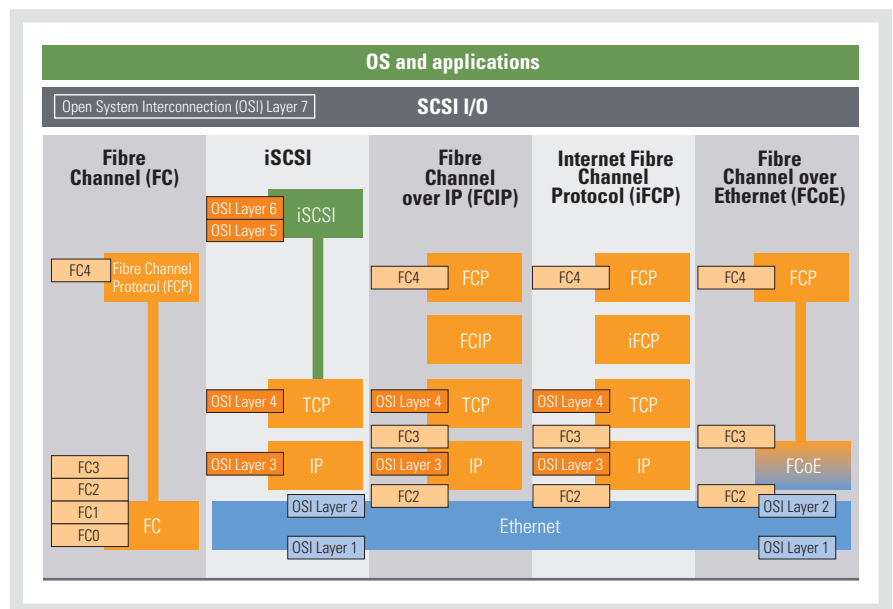


Figure 1. iSCSI and Fibre Channel protocol layers

In an *active attack*, those attempting to obtain access typically terminate or intercept a communication endpoint (either an initiator or target) with equipment that they control, and then misrepresent that equipment as the original endpoint. This type of attack can occur only if the attackers have access to the physical or logical network and can thereby intercept the packet streams. Another form of active attack can flood packets to iSCSI or Fibre Channel endpoints, preventing timely access to the network by valid traffic.

An *operational attack* misuses a management portal on an infrastructure component, which might be an initiator, target, or switch. Ethernet and Fibre Channel switches may host an HTTP service, a Simple Network Management Protocol (SNMP) agent, or a Common Information Model (CIM) agent, and these management portals therefore require protection. Another type of attack is a break-in to the server. The underlying storage protocol cannot protect that server's data further, but it is still important that this infected server not be able to access resources that do not belong to it.

**Domain isolation and IPsec**

*Domain isolation* can help easily resolve many of the vulnerabilities described in the preceding section. This isolation can take two forms: physical and logical. Physical isolation means that the SAN is entirely

closed and has no connection to the rest of the network; this approach can be somewhat impractical, but is a common implementation for Fibre Channel SANs. Logical segmentation can be implemented in iSCSI using VLANs, which are commonly used to isolate management portals across different infrastructures and can also be used to protect access to data types within the same SAN. Fibre Channel supports the similar concept of zoning as well as virtual SANs (VSANs), although VSANs were only recently introduced.

IPsec can provide highly flexible DIF security for iSCSI. Because Fibre Channel is not IP based, it must use non-IPsec methods to create secure tunnels between Fibre Channel SANs or perform translation between IP and Fibre Channel networks. IPsec is designed to be completely transparent to iSCSI protocol operation and provides mechanisms for implementing strong authentication, authorization, and data coherence. It uses two protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is designed to provide authentication and integrity of IP packets, but does not provide confidentiality for the payload; ESP is designed to provide integrity and confidentiality for the payload as well as a form of authentication.

Each of these protocols can operate in either tunnel mode or transport mode (see Figure 3). Tunnel mode is typically used to help ensure the confidentiality of

the original IP header and payload between endpoints (such as gateways) connecting two domains, often when data must leave the secure confines of a LAN or wide area network (WAN) and travel between hosts over a public network such as the Internet. Transport mode can provide end-to-end confidentiality but does not encrypt the original IP header, and can thus allow the packet to participate in normal routing operations for the domain.

**BEST PRACTICES FOR iSCSI SECURITY**

Following best practices appropriate for specific deployments or usage models can help organizations secure their iSCSI SANs as part of a comprehensive enterprise security strategy. This section outlines a few of the recommended practices that administrators should consider.

**Isolate the iSCSI domain.** Because iSCSI SANs can be switched within Ethernet LANs or routed through IP subnets, iSCSI can exist in mixed-traffic networks. Enterprise data centers typically segment different kinds of network traffic by either department or application type. Providing similar segmentation for iSCSI storage traffic through domain isolation—using either physical isolation or logical segmentation—can help secure the iSCSI SAN from other traffic.

**Consolidate and secure management portals.** Networks often include many management consoles, with switches, hosts, and routers having their own management agents or applications. Best practices recommend limiting the number of management portals and restricting access to them so that only one console has overall control of a particular iSCSI SAN domain. This primary management portal should be accessed using robust security pathways, such as virtual private networks (VPNs), especially if the access is external to the network.

**Disable unused switch and router features.** Ethernet switches may include features that are unnecessary in an iSCSI

	iSCSI	Fibre Channel
<b>Authentication</b>	CHAP	CHAP, FC-SP, Fibre Channel Authentication Protocol (FCAP)
<b>Authorization</b>	IQNs, ACLs	WWNs, ACLs
<b>Confidentiality</b>	IPsec ESP and AH protocols in tunnel or transport mode	FC-SP (based on some aspects of IPsec)
<b>Integrity</b>	Ethernet CRC (within LAN), TCP checksum (end to end), IP checksum (end to end), iSCSI digest (end to end), IPsec ESP and AH protocols in tunnel or transport mode	CRC (end to end)
<b>Segmentation</b>	VLANs, IP subnets, Internet Storage Name Service (iSNS)	VSANs, Fibre Channel name services

Figure 2. Comparison of iSCSI and Fibre Channel security components

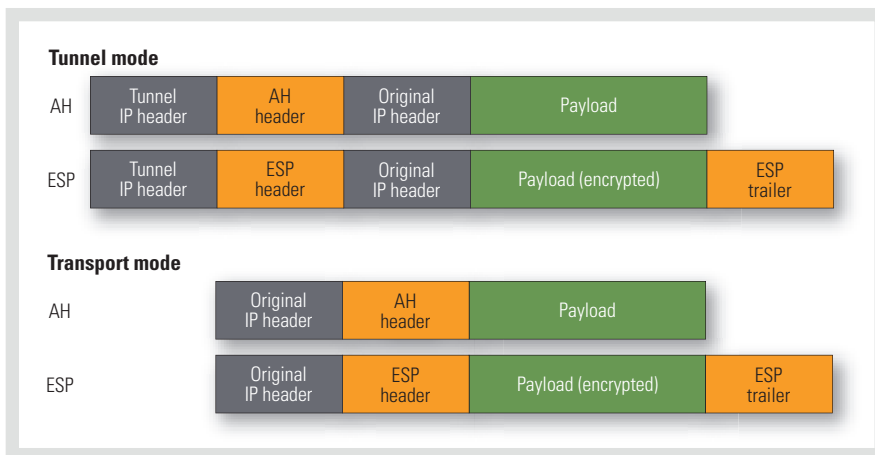


Figure 3. IPsec headers in tunnel mode or transport mode

SAN. For example, switches may include up to four management portals—SNMP agent, HTTP server, Telnet command-line interface (CLI) access, and serial CLI access—but obviously not all of these portals are required. Based on the best practice of using a single primary management console, administrators should lock down these portals so that they can access only the primary management console’s IP address or configured VLAN. They should also typically turn off port mirroring and other features that may be unnecessary, such as Layer 3 routing on switches used only as Layer 2 devices.

**Use access control lists for authorization.** ACLs, a common feature of Ethernet switches, match iSCSI PDUs based on a defined  $n$ -tuple. ACLs can limit access to particular switch ports based on administrator-defined restrictions, with  $n$ -tuples that do not represent membership in the iSCSI SAN then being rejected by the switch. ACLs provide a powerful way to control network access to services, and best practices recommend using them as a network resource access authorization technique.

**Use CHAP when possible.** CHAP is used by VPNs and the Microsoft® Windows® OS, and is commonly supported by iSCSI devices. CHAP can have the target authenticate the initiator but also enables targets and initiators to authenticate each other. iSCSI SAN deployments should generally

employ the strongest authentication method available, using CHAP when possible for entity authentication.

**Use IPsec when appropriate.** Although technical and operational concerns may limit its deployment today, when practical, administrators should use IPsec in its minimal required configuration—ESP in tunnel mode between security domains—for data coherence. Typical deployments focus on environments in which data leaves the local data center security domain, and generally employ a security or VPN appliance for using IPsec between data centers.

**Define a practical and secure key management strategy.** Organizations should define practical and secure key management strategies that fit their needs and resources. Keys for CHAP, DAR, and DIF encryption require careful management—lost keys, for example, may make data inaccessible. Organizations typically develop their own key management strategies and guard them closely, because exposing these strategies can represent a security threat. Best practices recommend that key management strategies include the following minimum elements:

- **Enterprise-wide policy:** The policy should be well-known, enforceable, and consistent across the enterprise. Separate internal groups should not develop their own policies.

- **Secure key creation:** Enabling secure key creation can be difficult, but using purpose-built hardware based on Federal Information Processing Standard (FIPS) 140-2 Level 3 encryption can help simplify this task.
- **Key revocation:** Key revocation policies should cover key aging, key reuse, and re-encryption of old data with new keys.
- **Key escrow:** Keys should be maintained securely between employers and employees such that employees do not have complete ownership or knowledge of the keys. A secure third party might be used to implement this mechanism.
- **Key distribution:** Key distribution may be as simple as having a dedicated organization within an enterprise that manually distributes and manages keys, or as complex as a full Public Key Infrastructure (PKI) implementation.

## ROBUST, SECURE iSCSI DEPLOYMENTS

Strong security does not necessarily mean expensive security. By taking advantage of the maturity of Ethernet and TCP/IP technologies that serve as the basis for iSCSI networking and following key iSCSI best practices, administrators can cost-effectively implement robust, secure iSCSI SANs as part of a comprehensive enterprise security strategy. [🔗](#)

**Robert Winter** is a network technologist in the Dell Office of the CTO.

**Dan McConnell** is a product marketing strategist in the Dell Enterprise Storage Group.

**MORE**

**ONLINE**

[DELL.COM/PowerSolutions](http://DELL.COM/PowerSolutions)

---

**QUICK LINK**

**Dell iSCSI storage solutions:**  
[DELL.COM/iSCSI](http://DELL.COM/iSCSI)