

**STORAGE AREA
NETWORK**

The Growing Need for Security in Storage Area Networks

New features in Brocade Fabric OS 5.2 help increase SAN security in enterprise environments to better protect sensitive data.

Today's IT organizations face unprecedented security threats as well as a wide range of industry regulations and government legislation designed to ensure that critical data is well protected. This paper describes key aspects of Storage Area Network (SAN) security and how Brocade® solutions help these organizations better secure their Fibre Channel SAN environments and the data stored within. This paper also includes recommendations on how to increase SAN security by utilizing the capabilities in Brocade Fabric OS® 5.2 and the latest generation of Brocade SAN switches and directors.

OVERVIEW

As today's IT organizations face more and more security threats and a growing amount of industry and government regulations, securing SAN environments has become an increasingly important aspect of overall data security. This is especially the case as SANs continue to grow in both size and importance—and extend across multiple sites. Another key factor in security is that many SANs use more than just the Fibre Channel protocol, with many different protocols now carrying storage traffic in and out of the SAN. Some are upper-level protocols such as FICON®, while others run over IP, such as FCIP for tunneling Fibre Channel between sites and iSCSI for fanning out to low-cost servers.

At a basic level, security is a delicate balance between the impact of a threat, the probability of the threat occurring, the impact of a security breach, and the cost of implementing countermeasures. The tolerated risk level varies significantly from one organization to another and depends on several factors.

The acceptable risk level is sometimes dictated by legislation in certain countries or for specific industries such as the case with the U.S. Health Insurance Portability and Accountability Act (HIPAA) guidelines for the healthcare industry, Gramm-Leach Bliley Act (GLBA) for the financial and insurance industries, and the Payment Card Industry Data Security Standard (PCI DSS) for companies dealing with credit card transactions. Other countries and regions also regulate the privacy of information, as is the case with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the European Union (EU) Data Protection Directive (EU Directive 95/46/EC).

In fact, some legislation, such as the California Senate Bill (SB) 1386, requires organizations to disclose security breaches of confidential personal information about California residents. This means that a security breach might become public domain and have serious business consequences due to compromised confidential data.

Regardless of the specific legislation, the more valuable the data is to an organization, the lower the tolerated risk level will be when it comes to protecting it. This trend is only likely to continue, especially as data security becomes an increasingly global issue.

THE IMPORTANCE OF SAN SECURITY

Although SAN security is a specialized field dealing with issues specific to the storage industry, it follows the same established principles found in all modern IT security. It involves a continuous process of evaluating an environment's current state of security against the constant changes brought about by innovations in technology and an increase in awareness concerning security issues. As a result, a SAN security strategy is integral to an overall IT security strategy and should address all possible threats facing a shared storage pool.

Since the introduction of Secure Fabric OS® in 2001, Brocade has been a leader in Fibre Channel SAN security. Based on several years of real-world experience deploying SANs of varying sizes and architectures, Secure Fabric OS was designed to meet the specific requirements of the most security-sensitive environments. For instance, Secure Fabric OS introduced the first Access Control Lists (ACLs) in the Fibre Channel industry and provided the first Fibre Channel authentication mechanism using PKI, which has since been replaced with the standards-based DH-CHAP (part of FC-SP).

Brocade has continued to introduce new security features to help ensure that SAN infrastructures and the data residing within them remain secure and highly available. Several of these features are now standard in the base Fabric OS, and Fabric OS 5.2.0 provides even more features, such as the Switch Connection Control (SCC) and Device Connection Control (DCC) policies, which are necessary components in the implementation of FICON solutions. Figure 1 shows the security technologies that organizations can utilize in a typical Brocade SAN environment.

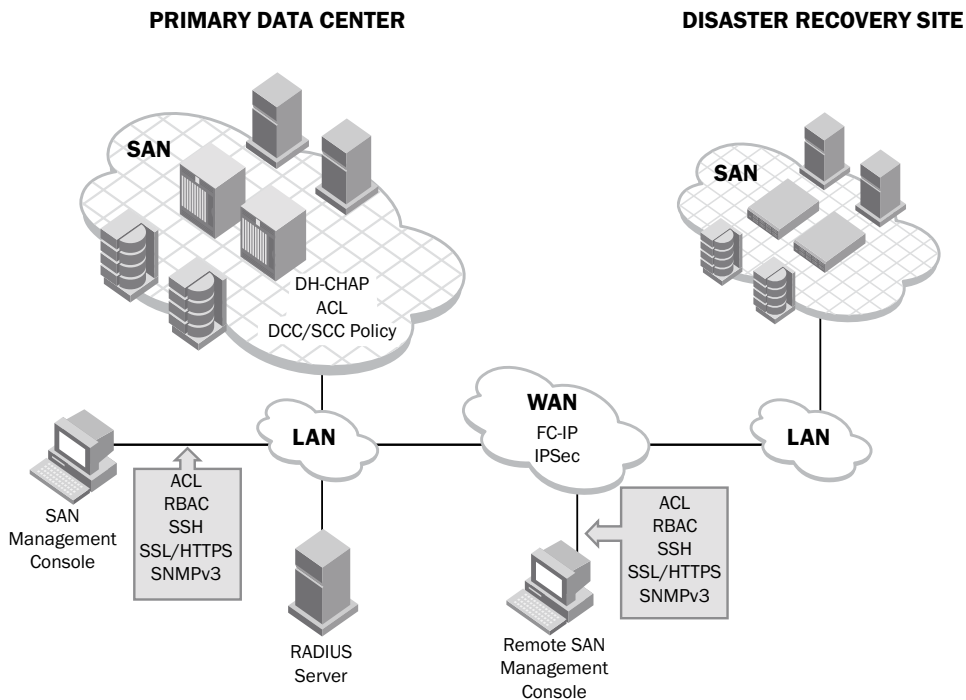


Figure 1. Key technologies for securing SAN environments.

THE PRIMARY THREATS TO A SAN

SAN security involves more than just guarding against a malicious outsider with sophisticated hacking tools and the intent to destroy or steal data. In fact, most IT security threats are based on internal threats from insiders. As a result, best-practice IT security strives to maintain five basic objectives: availability, integrity, authentication, confidentiality, and non-repudiation of data. At a minimum:

- Data must always be available to authorized users whenever it is needed.
- In order to maintain its integrity, data must not be modified in any way.
- Sensitive data such as personal information, intellectual property, and data pertaining to national security must remain strictly confidential.

These objectives provide a foundation for protecting against the numerous types of threats and attacks that can be executed against a storage environment. The U.S. National Security Agency's Information Assurance Technical Framework (IATF) considers five classes of threat agents, as shown in Table 1.

Table 1.
Classes of Threat Agents.

Attack	Description
Passive	Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information (such as passwords). Passive intercept of network operations can give adversaries indications and warnings of impending actions. Passive attacks can result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These include attacks mounted against a network backbone, exploitation of information in transit, electronic penetrations into an enclave, or attacks on an authorized remote user when attempting to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-in	Close-in attacks are where an unauthorized individual is in physical close proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close proximity is achieved through surreptitious entry, open access, or both.
Insider	Insider attacks can be malicious or non-malicious. Malicious insiders have the intent to eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentionally circumventing security for non-malicious reasons such as to "get the job done."
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product, such as a back door to gain unauthorized access to information or a system function at a later date.

In terms of storage and SAN environments, most security threats fall into three categories:

1. Malicious outsider threats
2. Malicious insider threats
3. Non-malicious insider threats

Given the wide range of potential threats to a storage environment, organizations should first identify the threat agents that are most likely to occur within their own environments and weigh the cost of implementing the appropriate countermeasures to mitigate or eliminate the risk of an attack. In a SAN environment, the most vulnerable points of exposure are usually the people managing the SAN and the management interfaces to the infrastructure hardware. Outsider attacks typically target the management interfaces since they utilize the TCP/IP protocol, which is well known to hackers.

PROTECTING A SAN FROM INTERNAL THREATS

Because it is well established that the majority of security threats stem from insiders, a basic SAN security strategy should likely focus primarily on this type of threat agent. These types of threats fall into two distinct groups: malicious and non-malicious threats.

Malicious Insider Threats

Malicious insider threats typically involve disgruntled employees or contractors. These threats are the most difficult to manage and control since they involve people who have legitimate access to and privileges on the affected systems. The key to mitigating risks from this type of threat is to limit the privileges a specific individual has and to distribute workload and responsibilities among multiple administrators. In the event that a security incident occurs, it is also important to have a proper incident response procedure in place, with clear methods to track administrator activities and provide an evidence trail for any potential criminal investigation or civil pursuit.

To help prevent malicious attacks, organizations should plan to:

- **Limit administrator responsibilities:** Organizations can restrict responsibilities by assigning a different username to each SAN administrator and a specific role using Role-Based Access Controls (RBACs).
- **Isolate particularly sensitive environments:** Another common technique is to physically segregate the most security-sensitive environments from other systems. One way to accomplish this is to isolate them into different physical SAN fabrics composed of distinctly separate switches. This method is particularly useful for government agencies and commercial projects requiring the highest level of confidentiality.
- **Track SAN administrator activities:** Organizations can also use the Event Auditing and Track Changes features that enable Brocade SAN switches to maintain logs for security-related events within a fabric. The Event Auditing feature tracks a wide range of events with an accurate timestamp and reports them in a format consistent with the DMTF standard. Organizations can configure several other log files for Brocade switches, including separate log servers such as the syslog, RASlog, and system message log. For the best results, organizations should set up syslog servers as well as Network Time Protocol (NTP) servers. Syslog is easy to use, runs on virtually any platform, and is free in a variety of versions. Brocade supports sending various alerts (security, configuration, and so on) to the syslog. These logs contain timestamps that organizations can then synchronize using NTP to ensure that all system logs are in perfect time synchronization in case an incident occurs.

One of the drawbacks of physically separating devices, however, is losing the ability to share valuable resources with systems outside the isolated fabric. To overcome this predicament, Brocade has developed routing capabilities, known as Logical SANs (LSANs), that enable devices in physically distinct fabrics to communicate with each other without merging everything into a single fabric. This technique enables secure device sharing while simultaneously increasing resource utilization for a higher ROI.

For less security-sensitive environments, organizations can use other methods to isolate data and devices from unauthorized devices and personnel while still gaining the benefits of a shared network. One such method employs features such as domains/Virtual Fabrics, RBAC, zoning, Registered State Change Notification (RSCN) aggregation and suppression, and ACLs. In addition, the Brocade Virtual Fabric feature can partition a given fabric into separate logical segments. For instance, a SAN administrator might have full authority over one or multiple Virtual Fabrics but might be restricted to a lesser role for other Virtual Fabrics.

Non-Malicious Insider Threats

Non-malicious insider threats are probably the most common cause of service disruptions within a SAN. Several factors can contribute to this problem, including lack of knowledge and training, lack of operational procedures, a bypass of operational procedures, fatigue caused by long working hours, misidentification of hardware, and plain ordinary mistakes. The key to minimizing the risks of this type of threat is to develop solid operational procedures and restrict administrator privileges except for the most trusted and experienced administrators.

Organizations can utilize several techniques to create a relatively foolproof SAN environment. For example, they can persistently disable all Fibre Channel ports that are not being used. This approach prevents problems arising from administrators inserting unconfigured HBAs into a fabric that might send RSCNs to other devices or flood the fabric with the potential result being a SAN outage. Similarly, organizations should configure all Fibre Channel ports such that they cannot act as E_Ports. This method helps prevent the accidental or unauthorized addition of a switch to a fabric unless explicitly enabled as an E_Port by an administrator with the appropriate privileges.

PROTECTING MANAGEMENT INTERFACES

As described earlier, the greatest potential points of exploitation in a SAN are the management interfaces, the entry points that outside attackers typically attempt to compromise. The first line of defense in protecting management interfaces is the user authentication process or login. When it comes to password policies, organizations should treat Fibre Channel switches just like any other hosts. Brocade has implemented features to prevent unauthorized users from obtaining too much information on a fabric, such as an upfront login in Brocade Web Tools to prompt for a username and password before displaying any information about a switch or fabric.

In addition, Brocade uses well-known and predefined user accounts for roots, administrators, and users. As always, organizations should modify the well-known default passwords for all of these accounts. Moreover, passwords should have a minimum length and automatically expire after a certain amount of time, and users should be required to change passwords at login. Lastly, any excessive unsuccessful login attempts should lock down an account automatically.

The Brocade Multi-User Account (MUA) feature allows up to 255 customized user accounts, with each account having specific roles defined by RBACs. Organizations should assign a unique username to each person who has legitimate access to the SAN infrastructure. Doing so can improve troubleshooting and change tracking while clearly defining each administrator's appropriate role and authorization rights. Organizations can locally manage both passwords and usernames on each switch or through a centralized access control administration method such as the RADIUS authentication protocol.

Once administrators are logged into a telnet or SSH session, most organizations display a standard welcome message or banner at system login. Although this type of login banner might not be a major deterrent, it can help minimize liability and provide legal support in the event of a security breach, and it should be a standard practice for any IT security strategy.

Securing Management Access

Every organization obviously has its own requirements and acceptable risk levels when it comes to SAN security. And although they can secure Brocade SAN switches to a very high degree, organizations usually do so at the expense of manageability due to additional overhead and restrictions on the management tools that can be used. As a result, each organization must balance security and usability based on its own unique requirements.

Brocade switches can be made extremely secure by disabling TCP/IP ports and services such as SNMP, telnet, and HTTP. In many cases, organizations should replace these services with more secure protocols such as SSHv2 and SSL/HTTPS to encrypt the login conversations. When managing their switches with SNMP, organizations should use SNMPv3 since it supports encrypted community strings along with many other features.

FIBRE CHANNEL SECURITY AND CONFIGURATION METHODS

Proper configuration of a SAN is essential to protecting the integrity and availability of data in storage pools. The Fibre Channel protocol itself has some inherent functionality that can be disruptive if not configured properly, and RSCNs are the best example of this. To overcome this challenge, Brocade switches are designed to contain RSCNs only for the devices affected within a zone by the addition or removal of a device. Furthermore, organizations can entirely suppress RSCNs on specific ports. Some applications, particularly in the video imaging and multimedia industries as well as tape backups, actually require this capability.

Zoning with Brocade

When SANs first emerged more than a decade ago, there was no real access control mechanism to protect storage owned by one host from being accessed by another host. This was not a significant issue at the time since it simplified management. Over time, however, it began posing a security risk as SANs evolved. To help secure particular devices and data, Brocade developed the concept of “zoning,” or restricting device sharing and access only to member devices within a given zone. Today, zoning plays an integral role in SAN security.

Two different types of zoning are possible: “soft” zoning and “hard” zoning. These terms generally refer to how zoning rules are enforced. Soft zoning, or software-enforced zoning, enforces zoning rules based on the information presented by the Name Server. This is sometimes called WWN-based zoning since the Name Server is the central repository of WWNs in a fabric. (Note that software-enforced zoning is generally considered less secure than hard zoning because of the potential for WWN spoofing.)

In contrast, hard zoning, or hardware-enforced zoning, indicates that the hardware or ASIC enforces the zoning rules. The term “port-based zoning” typically indicates hard zoning. Today, all Brocade 2 and 4 Gbit/sec products utilize hardware-enforced zoning, whether the zone members are defined using the domain/port ID, WWN, or a combination of both.

As a security best practice, organizations should utilize single-initiator zones. That means each zone should have only one host, although it can have multiple storage nodes. Single HBA zoning improves security and helps contain RSCNs—in addition to making the SAN much easier to manage and less prone to disruptions. An extension of this best practice for mixed disk and tape traffic on the same HBA is to utilize two zones for each HBA: one for disk nodes and one for tape nodes. This approach isolates the disk and tape devices even though they continue to communicate through the same HBA.

Another best practice is to activate “default zoning,” which is available in Fabric OS 5.1.0 and later versions. If no zones are defined or the current zoning configuration is disabled, all devices can see each other in the SAN. This can create a variety of problems. First, the SAN is more vulnerable from a security perspective. Second, several HBA drivers have difficulty discovering an entire SAN. The default zoning capability helps ensure that devices not already assigned to an active zone will be assigned to the default zone and ultimately will not be seen by other devices when an administrator performs a “cfgDisable” operation.

ADDITIONAL BROCADE FIBRE CHANNEL SECURITY FEATURES

Brocade has developed several additional security features to further strengthen SAN fabrics. Introduced in 2001, Secure Fabric OS enables organizations to authenticate switches, control device access, control management interface access, and utilize a single point of control to manage a fabric. Additional security features include:

- **Fabric Configuration Server (FCS) policy:** Identifies one switch as the primary FCS or primary point of control to manage all switches within a fabric. Administrators must perform any changes to zoning, user accounts, passwords, or policies via the primary FCS, thereby reducing the number of possible entry points for a potential attacker.
- **Switch Connection Control (SCC) policy:** Enables the highest level of security within a Fibre Channel fabric by authenticating switches before they can join a fabric. This policy prevents the unauthorized addition of a new switch to an existing secure fabric unless an administrator has explicitly defined it in the SCC policy.
- **Device Connection Control (DCC) policy:** Specifies which devices can participate in a fabric and locks them down to a specific port within the fabric to prevent the addition of a device to an unauthorized port. Organizations can use this policy as a WWN spoofing countermeasure by preventing a device that is configured to mimic an existing device from joining a fabric unless the device being spoofed is first disconnected then physically replaced with an unauthorized device.

Both the DCC and SCC policies are now available in the base Fabric OS. Table 2 highlights some of the other key security features available for Brocade Fibre Channel switches running Fabric OS 5.2.0.

Brocade Security Features	
<ul style="list-style-type: none"> • DH-CHAP • SSHv2 (using AES, 3DES, RSA) • SSL (using AES, 3DES, RSA) • HTTPS (using AES) • SNMPv3 • FC-SP • Secure RPC • Secure file copy (SCP) • Telnet disable • Telnet timeout • IP filters (block listeners) • Secure passwords (centralized control via RADIUS/CHAP) • Multiple User Accounts (MUAs), up to 255 • Role-Based Access Controls (RBACs) • Administrative Domains/Virtual Fabrics • Boot PROM password reset • Password hardening policies • Upfront login in Web Tools • Login banner 	<ul style="list-style-type: none"> • Monitoring of attempted security breaches (via audit logging) • Monitoring of attempted security breaches (via Fabric Watch Security Class) • Fibre Channel security policies: DCC and SCC • Trusted Switch (FCS) for central security management • Management access controls (SNMPv3, Telnet, FTP, serial port, front panel) • Hardware-enforced zoning by WWN and/or domain/port ID • Default zoning • RSCN suppression and aggregation • Configurable RSCN suppression by port • NTPv3 (to synchronize timestamps) • Event auditing • Change tracking • Firmware change alerts in Fabric Manager • Persistent port disable • Persistent domain ID • E_Port disable

Table 2.
Brocade Security Features.

SECURING LONG-DISTANCE SAN CONNECTIVITY

In recent years, disaster recovery and business continuity have taken center stage with most IT organizations as a way to protect their critical data and prevent potential business outages. Storage networks have played a prominent role in this trend, with data replication, remote mirroring, and remote backup some of the most commonly deployed solutions that utilize long-distance SAN connectivity. Today's organizations typically use two implementations to exchange data between SANs over longer distances where cost, distance, and performance are the primary factors in deciding what technology to employ.

The fastest—and most expensive—method to exchange data over distance is with dark fiber, but this technology is limited to distances of approximately 100 kilometers. For longer distances, organizations can connect their SANs through bridging technology between Fibre Channel and IP—using protocols such as FCIP and IPFC over standard lines such as T3 and OC3, for example.

Securing a dark fiber connection is similar to the techniques described earlier. However, intercepting communications on a dark fiber requires expensive specialized equipment and requires a disruption of service to physically cut the cable to tap into it. Encrypting data across dark fiber might be considered an excessive measure given the low probability of this threat from occurring without being detected.

The only additional precaution with this type of solution is to isolate the SAN fabrics at each physical site instead of merging them into a single fabric. Because a fabric itself can be viewed as a single point of failure, isolating the fabrics would also eliminate this particular risk. Organizations can implement SAN routing technology via the Brocade 7500 Switch or the Brocade 48000 Director (using the Brocade FR4-18i routing blade) as part of an LSAN.

Securing a SAN connection across a TCP/IP transport, however, does require some extra considerations since it is much easier to access. Again, the Brocade 7500 can provide a high-performance FCIP long-distance solution with built-in hardware compression, Fast Write, and Tape Pipelining features for higher performance. The Brocade 7500 and Brocade FR4-18i blade also contain hardware encryption chips that employ IPSec to secure the FCIP channel between sites. The IPSec protocol is an accepted networking standard and is commonly used to encrypt data across TCP/IP connections. Moreover, IPSec enables organizations to choose either 3DES or AES-256 as an encryption algorithm.

INTRUSION DETECTION AND INCIDENT RESPONSE

If an organization does detect a security incident, the first step is to identify whether a breach actually has occurred in the timeliest manner possible. Organizations can use several methods to generate security-related alerts in Brocade SAN environments. Events such as invalid logins, attempts at connecting unauthorized devices into ports, time servers being out of sync, and the use of illegal commands for a user's authorized level are all items that the Brocade Fabric Watch utility can monitor automatically. Organizations can configure several events and parameters in the Fabric Watch Security Class and generate an alert in the form of an SNMP trap or an e-mail sent to the appropriate personnel.

Another best-practice method is to analyze the various log files on a regular basis and look for any anomalies. These logs include the syslog, RASlog, Audit Events log, and Track Changes log. These files can also provide critical forensic evidence in the event of a SAN security incident and should be protected using adequate backup techniques.

Developing a reliable SAN incident response procedure with clearly defined steps is critical in minimizing further damage and eventually prosecuting an attacker on criminal charges or pursuing an attacker in a civil suit. To increase the probability of success for such cases, organizations must be sure to exercise due diligence and follow appropriate measures to gather evidence and maintain the evidence trail even prior to an incident occurring.

SUMMARY

In the past few years, SAN security has gained a considerable amount of visibility and is clearly on the minds of C-level executives today. Brocade understands the importance of data security and has been at the forefront of improving SAN security with the right solutions for safely managing and protecting data. Today's IT organizations can utilize these solutions to develop a solid SAN security strategy, strengthen their SAN infrastructures, perform periodical SAN security audits, and implement new security technologies as they become available.

For more information, visit www.brocade.com.

Corporate Headquarters

San Jose, CA USA
T: (408) 333-8000
info@brocade.com

European Headquarters

Geneva, Switzerland
T: +41 22 799 56 40
emea-info@brocade.com

Asia Pacific Headquarters

Singapore
T: +65-6538-4700
apac-info@brocade.com

© 2007 Brocade Communications Systems, Inc. All Rights Reserved. 01/07 GA-WP-862-01

Brocade, the Brocade B-weave logo, Fabric OS, File Lifecycle Manager, MyView, Secure Fabric OS, SilkWorm, and StorageX are registered trademarks and the Brocade B-wing symbol and Tapestry are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON is a registered trademark of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.



BROCADE