



**STORAGE AREA
NETWORK**

The Growing Need for Security in Storage Area Networks

New features in Brocade Fabric OS 6.1 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® 6.1 and the latest generation of Brocade SAN switches and directors.

OVERVIEW

As today's IT organizations face 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 size and extend across multiple sites. A 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 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 measures need to balance the probability of a 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 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).

Some legislation, such as the California Senate Bill (SB) 1386 and similar laws in approximately 40 states, requires organizations to disclose security breaches of confidential personal information about their state residents. This means that a security breach might become public information 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 data within a SAN environment.

Since 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, Brocade developed a special licensed version of Fabric OS designed to meet the specific requirements of the most security-sensitive environments. For instance, Brocade 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 the FC-SP/FC-SEC standard).

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. All of the security features that were previously licensed have been replaced with more powerful and flexible functionality in the standard Fabric OS (version 5.3.0 and later), which does not require a license. Figure 1 shows the security technologies that organizations can utilize in a typical Brocade SAN environment.

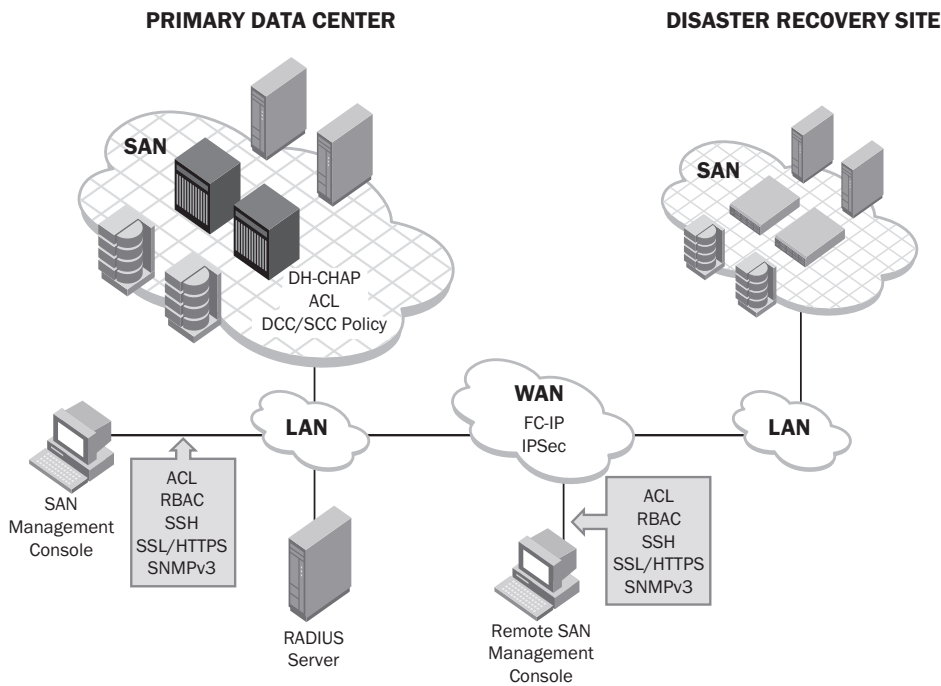


Figure 1.
Key technologies for
securing SAN environments.

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 threats that are most likely to be exploited within their own environments and weigh the cost of implementing the appropriate countermeasures to mitigate or eliminate the risk attributed to a threat. In a SAN environment, the most vulnerable points of exposure usually involve 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 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 employees or contractors who have something to gain from exploiting a weakness in the system. These threats are the most difficult to manage and control since they involve people who have legitimate access to 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 evidence for any potential criminal or civil investigation.

To help prevent malicious attacks, organizations should plan to:

- **Limit administrator responsibilities:** Organizations can restrict responsibilities by assigning a different user name to each SAN administrator and a specific role using Role-Based Access Controls (RBAC).
- **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 a timestamp and reports them in a format consistent with the Distributed Management Task Force (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 time-synchronized so they can be analyzed and contrasted 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, Brocade has developed routing capabilities, known as Fibre Channel Routing, that enable select devices in physically distinct fabrics to securely communicate with each other without merging the switches 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 a combination of features such as Virtual Fabrics, RBAC, hardware-enforced zoning, Registered State Change Notification (RSCN) aggregation and suppression, and ACLs. The Brocade Virtual Fabric feature can partition a 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, undocumented or non-existent operational procedures, a bypass of operational procedures, fatigue caused by long or nighttime working hours, misidentification of hardware, and simple mistakes. The key to minimizing the risks of this type of threat is to develop solid, well-documented operational procedures and restrict administrator privileges to only the tasks that are required for a particular administrator's job functions. Organizations should not grant additional privileges to a trusted, long-term, or favored administrator when those privileges are not required for that administrator's job functions.

Organizations can utilize several techniques to create a safe and reliable SAN environment. For example, they should persistently disable all unused Fibre Channel switch ports. This approach prevents problems arising from administrators inserting unconfigured Host Bus Adapters (HBAs) into a fabric that might send RSCNs to other devices or the whole fabric with the potential result being an application disruption or total SAN outage. Similarly, organizations should configure all Fibre Channel ports so that they cannot act as E_Ports to form an ISL with another switch. This method helps prevent the accidental or unauthorized addition of a switch to a fabric unless the ISL ports are explicitly enabled as E_Ports by an administrator with the appropriate privileges.

PROTECTING MANAGEMENT INTERFACES

The first line of defense in protecting SAN data and devices is physical security. Organizations should physically lock buildings while restricting and monitoring access to data centers and even racks within the data center. Guards, cameras, bio-identification, motion sensors, infrared sensors, door sensors, and other monitors can track who has physical access to IT devices at any given time. This level of physical security is critical, not only for data security, but for system availability and change control procedures. By recording who accessed what—and when—organizations can reduce their troubleshooting time and costs as well as their Mean Time To Repair (MTTR).

As described previously, the greatest potential points of exploitation in a SAN are the management interfaces: entry points that outside attackers typically attempt to compromise. Organizations should employ reliable overall IP network security best practices to isolate the management interfaces and ensure that they are accessible only to the appropriate staff on the IP network. The next potential threat for an outside attacker is the act of discovering the SAN switch devices on the IP network. Organizations can minimize this threat by disabling any unused management interfaces or protocols, such as telnet, SNMP, or HTTP.

Brocade has disabled any unnecessary IP services and requires authentication for Brocade Web Tools before a user can view any information, even read-only data. In many cases, organizations should use more secure protocols such as SSHv2 and SSL/HTTPS to encrypt the login conversations. When managing their switches with SNMP, organizations should also use SNMPv3 since it supports encrypted community strings along with many other capabilities.

If an attacker knows the IP address of a SAN switch, the user authentication process or login is the next line of defense. 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. Keeping default passwords, changing the default passwords only slightly, and using easy-to-discover passwords (for example, the word “Brocade” or a user name) constitute the most common security hole with SAN devices and IT devices in general. Fabric OS enables policies that require passwords to have a minimum length and automatically expire after a certain amount of time—and require users to change default passwords at login. Lastly, organizations can set policies to lock down an account automatically after any excessive unsuccessful login attempts.

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 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. 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 internal management requirements.

SAN administrators can create up to 255 customized user accounts, with each account having specific roles defined by RBAC. Organizations should assign a unique user name 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 manage both passwords and user names on each switch locally or through a centralized access control administration method such as the RADIUS authentication protocol or the Lightweight Directory Access Protocol (LDAP).

Organizations can also employ Brocade Virtual Fabrics so administrators have access only to the groups of SAN ports, WWNs, and switches that their job function requires. Within a Virtual Fabric, an administrator should have the correct RBAC. Organizations can use Virtual Fabrics and RBAC in conjunction to limit an administrator to just the portions of the SAN and the amount of control that is necessary. Providing full administrative authority and a complete view of the SAN for administrators who do not need that level of access exposes the organization to accidental or malicious attacks that can cause downtime or data loss.

FIBRE CHANNEL SECURITY AND CONFIGURATION METHODS

RSCN is required for a SAN to properly function, but RSCNs can potentially be disruptive if not managed properly by the SAN switch. Brocade switches forward RSCNs only to zones with devices affected by the addition or removal of a device. Also, Brocade switches forward only one RSCN if identical RSCNs occur within a half-second window, an approach that limits the impact of a device sending hundreds or thousands of RSCNs per second. 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 used by one host from being accessed by another host. This was not a significant issue at the time due to the limited scale of the original SANs. Over time, this became a security risk as SANs became larger, more complex, and mission-critical to most data centers. To help secure particular devices and data, Brocade invented the concept of “zoning,” or restricting device communication only to member devices within a given zone. Today, zoning plays an integral role in SAN security.

For Brocade switches, there are two ways to identify zone members, and zone enforcement is performed either in the switch’s Name Server or within the switch’s ASICs. Identification methods include Domain Port (DP) and port World-Wide Name (pWWN). DP is the switch domain ID and the switch port number while pWWN is the storage or host port WWN. Brocade recommends pWWN identification because of the management flexibility it provides, and several advanced Brocade features require pWWN zoning.

Brocade switches that operate at 2 Gbit/sec or faster speeds enforce *both DP and pWWN zones* in hardware. This was not the case in Brocade 1 Gbit/sec switches, and users frequently chose DP identification because it was the only hardware-enforced zoning method at the time. Now, a zone with all DP identification or all pWWN identification uses the more secure hardware enforcement.

However, there are some cases when mixing identification methods results in software enforcement. These cases include mixing DP and pWWN identification within a zone or using a DP identification for one zone and the pWWN attached to that DP in another zone. For this reason, Brocade recommends using the same zoning identification method (preferably pWWN) across the entire SAN to ensure that:

- All zoning is hardware-enforced
- Advanced features such as Fibre Channel Routing are usable
- Zoning management methods are consistent

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, helps contain RSCNs, and makes the SAN much easier to manage and troubleshoot. 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. By default, 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, HBA drivers can have difficulty discovering an entire SAN. The Default Zoning feature ensures that devices not already assigned to an active zone will be assigned to the Default Zone and will not be seen by other devices when an administrator disables a zoning configuration.

For superior protection of hosts and switches, organizations can use DH-CHAP authentication to provide a strong authentication when adding new switches or hosts to an existing fabric. This is the strongest anti-WWN spoofing method available and should be used in conjunction with Device Connection Control (DCC) policies described below.

ADDITIONAL BROCADE FIBRE CHANNEL SECURITY FEATURES

Brocade has developed several additional security features to further strengthen SAN fabrics. Brocade previously offered a special licensed version of Fabric OS that enabled organizations to authenticate switches, restrict device access, control management interface access, and utilize a single point of control for fabric management. These security features are now included in the base Fabric OS in version 5.3.0 and later. The security features introduced in Fabric OS 5.3.0 include:

- **Fabric Configuration Server (FCS) policy:** Identifies one switch as the primary point of control (the FCS) 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 allowed 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.
- **IP filters:** Replace the previously licensed Management Access Control (MAC) policy. They have firewall-like properties and are used to block or control access to the IP management interface.

The appendix highlights some of the key security features available for Brocade Fibre Channel switches running Fabric OS 6.1.

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 native Fibre Channel over dark fiber or Wave Division Multiplexing (WDM), but this technology is limited to distances of several hundred kilometers. For longer distances, organizations can connect their SANs through technology that allows Fibre Channel communication over IP using protocols such as FCIP and iFCP over WAN links, 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 as well as a disruption of service to physically cut the cable and tap into it. To prevent this difficult tapping process, organizations can protect dark fiber cables in pressurized tubes by monitoring gas pressure changes that would indicate physical tampering. However, this is extremely rare and usually implemented only in governmental security organizations.

A more common precaution is to isolate the SAN fabrics electronically at each physical site instead of merging them into a single fabric. Because a single fabric is a single point of failure, isolating the fabrics also eliminates the risk of disruption from a dark fiber cable cut. 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 a routed zone, which enables selective node communication while keeping each site's fabric isolated.

Securing a SAN connection across a TCP/IP transport requires extra considerations since IP is much easier to access than dark fiber. 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 also contain hardware encryption chips that employ IP Security (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, AES-128, or AES-256 as an encryption algorithm, which is offered on the Brocade 7500 and Brocade FR4-18i.

INTRUSION DETECTION AND INCIDENT RESPONSE

If an organization detects 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.

FABRIC-BASED ENCRYPTION FOR DATA AT REST

A new platform from Brocade ensures data confidentiality for data at rest with fabric-based encryption. The first release of the Brocade Encryption Switch and FS8-18 Encryption Blade for the Brocade DCX™ Backbone is the fastest way to encrypt data on enterprise disk media with up to 96 Gbit/sec of encryption processing power. This new technology enables enterprises to encrypt specific or all disk data to prevent accidental data leaks when disk drives are replaced or disk arrays refreshed and to protect enterprises from data theft.

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 without compromising management efficiency. Today's IT organizations should utilize these solutions to develop a solid SAN security strategy, strengthen their SAN infrastructures, perform periodical SAN security assessments, and implement new security technologies as they become available.

For more information about Brocade security solutions, visit www.brocade.com. To learn how Brocade Services offerings can enhance security throughout the data center fabric, visit www.brocade.com/services-support.

APPENDIX.
BROCADE FABRIC OS SAN SECURITY FEATURES

The following table identifies the current and past security-related features available on Brocade SAN switches and in which version of Fabric OS they became available.

* **Security Level:** B = Basic, I = Intermediate, A = Advanced, O = Optional

Security Feature	Fabric OS 2.x	Fabric OS 3.x	Fabric OS 4.x/5.x/6.x	Security Level*
SSH (AES, 3DES, RSA)	2.6	3.1.0	4.1.1	I
SSH Public Key uthentication	-	-	6.1	A
TLS/SSL (AES, 3DES, RC4/RSA)	-	N/A	4.4	I
HTTPS (AES, 3DES, RC4/RSA)	-	N/A	4.4	I
PEAP/TLS	-	-	5.3	A
SNMPv3 (AES, 3DES)	-	-	4.4 (DES)	I
NTP (to synchronize timestamps)	2.6.1	3.2	4.2	B
NTP (up to 8 NTP servers)	-	-	5.3	B
PKI Digital Certificates (SLAP/RSA); Not factory-shipped since May 15, 2005	2.6	3.1.0	4.1	A
DH-CHAP (E_Ports, switch binding)	-	3.1.0	4.4	A
DH-CHAP (F_Ports, port binding)	-	-	5.3	A
MS-CHAPv2	-	-	5.3	A
Secure RPC (for Brocade API using SSL)	-	-	4.4	A
Secure File Copy (SCP) for configUp/Download	-	-	4.4	I
Secure File Copy (SCP) for firmwareDownload	-	-	5.3	I
Secure File Copy (SCP) for supportSave	-	-	5.3	I
SecTelnet	2.6	3.1	4.1	I
Telnet disable	-	-	4.4	I
Telnet timeout	2.6	3.1	4.1	B
IP filters (block listeners)	-	-	4.1	B
Secure passwords (centralized control via RADIUS/CHAP)	-	3.2	4.4	A
LDAP	-	-	6.0	A
Multiple User Accounts (MUA—up to 15)	-	3.2	4.4	I
Multiple User Accounts (MUA—up to 255)	-	-	5.2	I
Role-Based Access Controls (RBAC) Admin, User, Switch Admin Roles	-	-	5.0.1	I
Operator, Zone Manager, Fabric Admin, Basic Admin Roles (RBAC) added	-	-	5.2	I
Security Admin Role (RBAC) added	-	-	5.3	I
Admin lockout policy	-	-	5.3	I
Boot PROM password reset	-	-	4.1	A
Password hardening policies	-	-	5.1	B
Upfront login in Web Tools	-	-	5.0.1 Default in 5.2	B

Security Feature	Fabric OS 2.x	Fabric OS 3.x	Fabric OS 4.x/5.x/6.x	Security Level*
Login banner	2.6	3.1	4.1	B
Monitor attempted security breaches (via Audit Logging)	-	-	5.2	A
Monitor attempted security breaches (via Fabric Watch—Security Class)	-	-	4.4	A
Fibre Channel Security Policies – Device Connection Control/Switch Connection Control (DCC/SCC) policies	Secure Fabric OS only	Secure Fabric OS only	5.2	A
Management access controls (IP filters in Fabric OS 5.3)	Secure Fabric OS only	Secure Fabric OS only	5.3	A
Trusted Switch (FCS) central security management	2.6	3.1	4.1	A
FCS Policy (without Secure Fabric OS)	-	-	5.3	A
AUTH policy	-	-	5.3	-
Management access controls (SNMP, Telnet, FTP, Serial Port, Front Panel)	Secure Fabric OS 2.6	Secure Fabric OS 3.1	Secure Fabric OS 4.1	A
Hardware-enforced zoning by WWN and Domain/Port ID	(Port-based only)	3.0	4.0	B
Default zoning	-	-	5.1	I
Insistent Domain IDs	-	-	4.2	I
RSCN suppression/aggregation	-	3.1	4.1	B
Configurable RSCN suppression by port	-	-	5.0.1	O
Event auditing	-	-	5.2	I
Change tracking	2.4	3.0	4.0	I
Firmware change alerts in Fabric Manager	-	-	4.4	A
E_Port disable (portCfgEPort)	2.6	3.2	4.2	I
Persistent port disable (E/F/FL/Ex/M_Ports)	2.6.1	3.2	4.2	I
Administrative Domains	-	-	5.2	A
IPSec (Brocade 7500 only)	-	-	5.2	O
IPv6	-	-	5.3	O
Security database size increased to 1 MB (from 256 K)	-	-	6.0	-
FIPS mode (140-2 level 2)	-	-	6.0	A
USB port disable/enable	-	-	6.0	B

Corporate Headquarters

San Jose, CA USA
T: +1-408-333-8000
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

© 2008 Brocade Communications Systems, Inc. All Rights Reserved. 09/08 GA-WP-862-04

Brocade, the B-wing symbol, DCX, Fabric OS, File Lifecycle Manager, MyView, and StorageX are registered trademarks, and DCFM and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in 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