Global Information Assurance Certification Paper

SAN SECURITY:
Securing a Brocade SAN

By

Todd R. Einck

April 29, 2003

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b(Option 1)

Overview

Data is the lifeblood of an enterprise. Loss of data, loss of data availability, or compromise of confidentiality or integrity can prove catastrophic to an enterprise. Security of your networked data is becoming increasingly important. As new networked methods of storing data become more prevalent, there is an increase in exposure to security vulnerabilities. Fibre Channel Storage Area Networks (SANs) are one of the fastest growing network technologies that store data on target devices that are not directly attached to the application servers. Data is increasingly being stored and accessed outside the traditional data center boundaries. " As storage networks grow from isolated data center environments to IP-enabled networks spanning the world, users are starting to consider issues with security." [1. Kuo]

This paper will discuss the different aspects of securing a Brocade Fibre Channel Storage Area Network within the enterprise network environment. It will address security technologies that can be implemented in a SAN environment that is not utilizing the security product, as well as the additional features available in the Brocade Secure Fabric OS (SFOS) security product.

Security in Enterprise Networks

Storage Area Networks are comprised of an entire collection of devices that includes initiators (servers), targets (storage, including disks and tape), and the networked infrastructure (switches) that these are attached to. The initiators and targets communicate with each other over the underlying networked infrastructure. Each separate and distinct networked infrastructure is known as a fabric. An enterprise SAN may be comprised of more than one fabric and its attached devices.

When referencing SAN security, we are not only trying to prevent theft of the data, but in a more comprehensive sense, ensure confidentiality, integrity, and availability of the data. There are two aspects that must be mentioned when addressing availability. This first is to provide data access for the appropriate individuals. The second aspect is that the appropriate individuals have the data available when they require it.

Although many individuals do not immediately think about data availability when they are securing their fabrics, it is an important consideration. Proper design of the enterprise SAN can significantly increase the availability of data to the users. [2. Cook] In mission critical environments, it is a well-known principle to design the SAN with host and storage devices that are dual attached to two separate and distinct fabrics (also known as dual fabrics). Dual attachment of each host

and storage device to more than one fabric eliminates any single point of failure in the data path. Optimally, both I/O paths would be actively load balancing traffic on each of the fabrics. Dual fabrics afford the greatest availability of data during catastrophic events, human error (intentional and unintentional), or simply when configuration changes and testing to a fabric require downtime.

There is no magical silver bullet that will comprehensively secure your enterprise LAN and SAN environments. Security requires an effective combination of industry accepted LAN security practices layered with SAN security features. The security infrastructure must be viewed as a comprehensive strategy incorporating enforcement of security policies balancing between the needs of functionality and convenience versus security. All facets of security need to be addressed, implemented, and operating harmoniously. These combined layered elements will form a defense in depth (DiD) that may make other less hardened networks more appealing to the undirected hacker. It is paramount that fortification starts with basic physical security principles as the foundation to build upon. One aspect of physical security encompasses *what* individuals have physical access to *what* hardware, in *what* data centers, and at *what* times. Without effective physical security in the enterprise, all other security efforts cannot deliver effectively.

In addition to physically securing your networks, it is imperative to implement traditional IP network security technologies as a foundation in the enterprise network. It has been written that the biggest vulnerability in SAN security is the enterprise LAN security. [3. Cook] Traditional LAN security techniques include elements such as internal and external firewalls, host intrusion detection systems, network intrusion detection systems, anti-virus software, and up-to-date deployment of security service packs on Network Management Stations (NMS's) and application servers, among others. SAN security requires more than a sound LAN perimeter, it must include additional security elements in the core of the network to form a defense in depth.

Security in the SAN

To compliment the LAN technologies, there are several features that can be deployed on a Brocade SAN that do not require the Security product which will fortify the core of the network. These features include zoning, **portcfgeport**, **portcfgpersistentdisable**, **bannerset**, changing user login names, changing SNMP community strings, and adding SNMP ACL's for starters.

Zoning is the ability to partition a devices (hosts/storage) view of the other devices that exist in the fabric. During a standard Fibre Channel device login sequence, it is customary that initiators (hosts) query the Simple Name Server (SNS) to learn its view of the other devices (typically targets) in the fabric. The

fabric view returned to the initiator by the SNS can be tailored by implementing zoning. [4. Brocade] Zoning is typically implemented to partition heterogeneous operating environments and/or to separate organizations that are sharing the same networked infrastructure.

Zoning with the Brocade family of Fibre Channel switches can be enforced in two different ways. The first type of enforcement is known as 'soft' enforcement (also known as 'advisory', or Name Server assisted zoning). This occurs when the initiator queries the SNS to learn about the targets that it has access to. The SNS will reply to the inquiry with a list of the Port Identifiers (PID's; 24 bit FC addresses) of the devices that the initiator can communicate with. As indicated, this is only advisory. When implementing soft enforced zones, there are no additional mechanisms to insure that a device only tries to access the specified devices. Thus, in a soft enforced zone, if a rogue server generated frames for a target that it was not zoned with, the frames would successfully traverse the fabric to the target device. Flexibility in relocating hosts and targets within the fabric was originally why an administrator would configure zones that result in soft enforcement.

The second, more secure implementation of zoning enforcement is known as 'hardware' enforcement. The same SNS query process is still utilized under hard enforcement as was used in soft enforcement. The difference is that the zoning service will download the zoning table information to each Application Specific Integrated Circuit (ASIC) to be enforced as an ingress ACL at wire speed. Under 'hardware' enforcement, the ASIC will validate the Source ID (SID) of every inbound frame and confirm that the SID is a valid source address for this destination device. In this scenario, when a frame destined for the target device does not have a valid SID for that destination port, that frame will be dropped at the destination port.

There are two ways to identify a device within a fabric. The first is by its World Wide Name (WWN). This is very similar to a network interface cards IEEE MAC address. The second is by the devices location in the fabric based on what port it is connected to on which switch number (domain-id). SAN administrators can control what kind of zoning enforcement occurs in the fabric based on the types of zoning definitions that are implemented. Devices can be defined in a fabrics using its WWN, or the "domain-id,port" information. Enforcement is also impacted by the ASIC technology that is implement in each family of switches. Table 1 displays the type of zoning enforcement based on device definitions and which family of switch the devices are connected to.

Zoning Enforcement

	1GB ASIC SW2xxx *	2GB ASIC SW3xxx/ SW12000 **
Zone1="Dom1,Port2; Dom1,Port8"	Hard	Hard
Zone2="WWN1; WWN2; WWN3"	Soft	Hard
Zone3="Dom1,Port13; WWN9; "	Soft	Soft

* SilkWorm 1GB Family including 2010, 2040, 2050, 2100, 2210, 2240, 2250, 2400, 2800, 6400
** SilkWorm 2GB Family including 3200, 3800, 3900, 12000

Table 1

When administering zone configurations on a fabric that is not utilizing the Secure FOS, the SAN administrator can create, modify, delete, and enforce zones from any switch in the fabric that he has administrative access to. Configuring zoning is a fabric-wide event, and thus any zoning changes made on any switch will propagate to all other switches in that fabric.

In addition to partitioning a devices view with zoning, there exists another complimentary technology that is known as LUN Masking (Logical Unit Number), which and is commonly deployed in heterogeneous environments. "LUN Masking is the capability that allows a specific LUN to be exclusively assigned and accessed by a specific list of host connections. Usually only one host connection will access a LUN at a time. By implementing LUN Masking it is possible to reliably attach a single LUN to a single host connection. Most importantly, other host connections will not be able to access LUN's to which they are not assigned." [5.King] Today, LUN level technology is not implemented on the Fibre Channel network, instead it is implemented on the initiator and/or target device.

For legal defense reasons, it is recommended to implement a banner on all devices. The FOS command to do this is **bannerset.** It is prudent to mention in the banner text that "access to this system is for authorized users and authorized uses". The **bannerset** command can be invoked in two formats, interactively and non-interactively. The non-interactive option affords a maximum of less than 128 characters. The interactive mode allows a maximum of 1024 characters in the text message. A non-interactive example of the **bannerset** command is included in figure 1 below.

```
sw1:admin> bannerset "Use this banner to designate the site for authorized
users and uses only"
```

Figure 1

The banner text will be displayed to all telnet and HTTP login sessions as part of the initial screen presented to the user.

Another security aspect has to do with default passwords. When the administrator logs into a switch for the first time under the latest Fabric OSs, he will be prompted to change all the users default passwords. The administrator can choose to bypass this prompting, but it is not advised since default login and passwords to switches are well known and documented on the Internet. This password prompting will continue with each subsequent login, until all the user passwords are no longer the factory defaults.

The next feature is only available when the fabric is not operating in secure mode. The SAN administrator can change the user login names from the well-known defaults to names of his choice. This adds a layer of obscurity and may prove effective against novice hackers. The username change should not be considered an adequate defense mechanism all by itself. Recall the defense in depth principle?

It is possible to configure each port on a switch to be persistently disabled, or to only allow certain types of devices to connect to a port. Using the **portcfgeport** command on unpopulated switch ports will prevent a rogue switch from joining the existing fabric. This command does not prevent hosts or storage from attaching to the fabric on one of these open ports. If the objective is to prohibit any device from gaining access via an unused port, use the **portcfgpersistentdisable** (Figure 2) command on all unoccupied ports. This will disable the port, and it will remain disabled after subsequent switch reboots. Restricting device access at each port adds another complimentary defensive security layer.

```
RSLSW122:admin> portcfgpersistentdisable 7/0

RSLSW122:admin> switchshow
switchName:     RSLSW122
switchType:     10.0
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:00:60:69:80:04:5f
zoning:         OFF
switchBeacon:   OFF
blade7 Beacon:  OFF
blade8 Beacon:  OFF

Area Slot Port Media Speed State
=====================================
  0    7    0   id    N2   No_Sync   Disabled(Persistent)
  1    7    1   id    N2   No_Light
```

Figure 2

Brocade offers an error reporting strategy that allows the SAN administrator to designate up to six syslogd servers (**syslogdipadd**) to be specified for forwarding switch error log files. It is considered a best practice to forward switch error logs to syslogd servers for two reasons. The first reason is because the switch only retains a limited number of errors in the log file. The file is a first-in, first-out file, and when the file is full, the oldest messages drop from the file. The second reason to send error logs to external servers is to increase the chance of detection in the event that a hacker gains access to a switch, and is able to covers his tracks on the switch. One last note in reference to error logs is that it is imperative that there is time schedule into the daily routine to review log files. This is critical so an administrator can become familiar with what messages are considered normal, so he can better identify if something appears abnormal.

There are a few additional security topics worth mentioning. If SNMP is employed as part of the monitoring and alert strategy, the default version 1 community strings on all switches should be changed to values that are difficult to guess. These community strings behave like passwords, and the default v1 values are well known in the industry. To further limit access via SNMP, it is recommended to configure SNMP ACLs to explicitly define access of NMSs for SNMP monitoring and management. Lastly, utilize the **timeout** parameter to establish a telnet timeout value. All idle telnet sessions will automatically be closed after the designated period of time.

Integrating Secure Fabric OS in the SAN

Until now we have discussed ways to secure a fabric without incorporating the Brocade Secure Fabric OS into the overall security solution. The Secure Fabric OS product allows the administrator to develop policies and implement additional layers of control that complement the existing secure implementation. SFOS implements mutual authentication performed between all switches using standards-based public key technology (PKI) and digital certificates, in conjunction with policy-based security tools and controls. When implementing SFOS secure mode in a fabric, it is required that all switches in the fabric be running firmware that supports SFOS. The SFOS firmware is available across the SilkWorm product line and can be found in the FOS 2.6.x, FOS 3.1, and FOS 4.1 versions.

Prior to enabling secure mode some preparation steps need to be performed or validated. In addition to each switch running the SFOS firmware, all participating switches must have a valid digital certificate installed, valid PKI objects, and a zoning and security license. The simplest way to determine if your switch meets the requirements is to invoke **secmodeenable** from the command line. If the requirements are not met, you will receive a message indicating so. The following example informs the administrator that the digital certificate has not been installed. (Figure 3).

```
sw1:admin> secmodeenable
Require switch certificate and secure telnet to enable security
```

Figure 3

A “Field Upgrade Process” exists to walk an administrator through the steps necessary to prepare the switches for security. When all the switches in the fabric meet the secure mode requirements, the administrator can enable the Secure FOS feature. In order to enable security, the administrator must invoke **secmodeenable** from an application that affords secure management communications. The available options via telnet include SSHv2 (FOS 4.1), a Brocade provided Secure Telnet Client (SecTelnet), or direct-connect serial access. During the process of enabling security, the administrator is prompted for several items including designating ‘trusted’ switches and changing all user passwords. It is a SFOS requirement to change all user passwords by at least one character to enable security. The new password can range from eight to forty characters in length. The secure management channel client encrypts portions of each login session, including the user password, which, until now has likely been passed in clear text across the network. To ensure future administrative accessibility to the fabric, it is reasonable to escrow the newly

selected passwords according to company policies, or develop and implement such a policy to ensure safekeeping of the passwords.

If login usernames had been changed from the default values prior to entering secure mode, the usernames will be returned back to the factory defaults during the security enabling process. In addition, a single, fabric-wide login and password database will be propagated to all switches in the fabric and maintained at the designated 'trusted' switch.

Once enabled, the Secure FOS environment offers several additional security components. Cumulatively, these components are known as the Fabric Management Policy Set (FMPS) [6. Brocade]. The FMPS is comprised of the following components:

- **Fabric Configuration Server policy** (FCS_POLICY)
  One or more trusted switches that source all fabric configuration changes
- **Management Access Controls policies** (MAC Policies)
  A set of policies that use ACLs to control administrative access
- **Device Connection Control policies** (DCC Policies)
  Policies to explicitly define WWN access onto designated switch ports
- **Switch Connection Control policy** (SCC_POLICY)
  A policy that designates which switches can participate in a secure fabric
- **Secure Management Communications** (SMC)
  Encryption of certain user login authentication information

The only FMPS policy that is mandatory in a Secure FOS environment is the FCS_POLICY. This policy contains a list of one or more switches that are considered to be the most 'trusted' and physically secure in the enterprise environment. The first switch listed in the FCS_POLICY that is participating in the fabric is considered the Primary Fabric Configuration Server (PFCS). All other switches listed in this policy are considered Backup FCS (BFCS) switches. Upon failure of the PFCS, the first BFCS in the list that is participating in the fabric will assume the PFCS duties. When the original PFCS rejoins the fabric, it will become the PFCS again.

Recall that fabric administration of a non-SFOS fabric can occur from any switch in that fabric that the administrator has login access too. All fabric wide administrative changes made on any switch in the fabric would propagate to all other switches in the fabric. This means that any user with administrative access could update fabric-wide configurations, including zoning, from any switch in the fabric. In secure mode, fabric wide administration can only take place on the Primary FCS. The security policies, password, zoning, and SNMP configuration databases are maintained and controlled on PFCS. The PFCS will forward these updated databases out to all other switches in the fabric encrypted with its private key. Recipient switches use the PFCS's public key to decrypt and authenticate the information and implement the new configuration.

As mentioned earlier, to activate the security feature, the administrator would invoke **secmodeenable,** typically from the most trusted switch in the fabric. The first prompt that appears will request the administrator to enter the FCS list. When designating the FCS switches, it is possible to specify them by using the switch WWN, switch name, or the Domain Id. The switch name and Domain Id designations can only be specified if the switch is already present in the fabric. After specifying the FCS list and the new user passwords, the policy database will be created and propagated to all other switches in the fabric (Figure 4). This will immediately be followed by a 'fastboot' of all switches participating in the secure fabric and all secure telnet sessions will be terminated.

```
sw2:admin> secmodeenable

This is an interactive session to create a FCS list.

The new FCS list is empty.

Enter WWN, Domain, or switch name(Leave blank when done):
10:00:00:60:69:50:0a:3b
Switch WWN is 10:00:00:60:69:50:0a:3b.

The new FCS list:
  10:00:00:60:69:50:0a:3b

Enter WWN, Domain, or switch name(Leave blank when done):
10:00:00:60:69:30:16:b4
Switch WWN is 10:00:00:60:69:30:16:b4.

The new FCS list:
  10:00:00:60:69:50:0a:3b
  10:00:00:60:69:30:16:b4

Enter WWN, Domain, or switch name(Leave blank when done):
Are you done?  (yes, y, no, n): [no] y
Is the new FCS list correct?  (yes, y, no, n): [no] y
Each encryption/decryption of password takes a while
New FCS switch root password:
Re-enter new password:
New FCS switch factory password:
Re-enter new password:
New FCS switch admin password:
Re-enter new password:
New fabric wide user password:
Re-enter new password:
New Non FCS switch admin password:
Re-enter new password:
Saving passwd...done.
Saving Defined FMPS ...
done
Saving Active FMPS ...
done
Committing configuration...
done.
Secure mode is enabled.
```

Figure 4

After the switches reboot, invoke **secpolicydump** to view the current 'Defined' and 'Active' security policies. The policy database will consist only of the FCS_POLICY, as shown in Figure 5.

```
sw2:admin> secpolicydump

_____________________________________________________
                DEFINED POLICY SET

FCS_POLICY
   Pos    Primary WWN                       DId swName
   ____________________________________________________
     1    Yes     10:00:00:60:69:50:0a:3b    2 sw2
     2    No      10:00:00:60:69:30:16:b4    1 sw1

_____________________________________________________

_____________________________________________________
               ACTIVE POLICY SET

FCS_POLICY
   Pos    Primary WWN                       DId swName
   ____________________________________________________
     1    Yes     10:00:00:60:69:50:0a:3b    2 sw2
     2    No      10:00:00:60:69:30:16:b4    1 sw1

_____________________________________________________
```

Figure 5

As can be viewed above, the only policy that is implemented and enforced after enabling security in the fabric is the FCS_POLICY. All devices attached to the fabric will continue to operate as they did prior to enabling security, or until additional policies are defined and implemented.

It is recommended to limit the number of administrative touch points into any fabric. Management Access Control policies allow the administrator to explicitly permit or deny device access (by IP or WWN) into the network. MAC policies can be used to control both in-band and out-of-band access into the fabric. The policies that control out-of-band (i.e. IP over Ethernet) management access to the fabric include TELNET_POLICY, HTTP_POLICY, API_POLICY, RSNMP_POLICY, and the WSNMP_POLICY. The policies that control in-band (i.e. Fibre Channel) access are MS_POLICY, FRONTPANEL_POLICY, SERIAL_POLICY, and the SES_POLICY. Only one instance of each of these Management Access Control policies may exist in a fabric, and it is enforced fabric wide. Each of policies and what they control is listed in Figure 6 below.

MAC Policies

```
TELNET_POLICY       IP addresses of trusted management stations for telnet
HTTP_POLICY         IP's that are allowed to establish HTTP communications
API_POLICY          IP list of workstations that have API access in the fabric
RSNMP_POLICY        IP list of read-only SNMP NMS's
WSNMP_POLICY        IP list of SNMP NMS's that can perform writes in the fabric
FRONTPANEL_POLICY   WWN of SilkWorm 2800 switches that permit frontpanel access
SERIAL_POLICY       WWN of switches that permit serial access
MS_POLICY           Device port WWN which management server access is permitted
SES_POLICY          WWN of HBA allowing SCSI Enclosure Service administration
```

Figure 6

To create any MAC policy, the administrator must access the secure fabric via the Primary FCS switch using secure management communications. If the objective of the new policy is to limit telnet access from a specific set of management stations, then the IP of those stations will need to be explicitly defined in the TELNET_POLICY. In the example shown in Figure 7, only the two designated IP addresses will be permitted to access the secure fabric via telnet. Also note that it is necessary to explicitly activate the newly defined policy so it can be enforced.

```
sw2:admin> secpolicycreate "TELNET_POLICY", "10.255.252.106; 10.255.252.110"
TELNET_POLICY has been created.
sw2:admin> secpolicydump

_____________________________________________________
                DEFINED POLICY SET

FCS_POLICY
   Pos    Primary WWN                      DId swName
   _____________________________________________________
     1    Yes     10:00:00:60:69:50:0a:3b    2 sw2
     2    No      10:00:00:60:69:30:16:b4    1 sw1

TELNET_POLICY
   IpAddr
   _____________________________________________________
   10.255.252.106
   10.255.252.110


_____________________________________________________

_____________________________________________________
               ACTIVE POLICY SET

FCS_POLICY
   Pos    Primary WWN                      DId swName
   _____________________________________________________
     1    Yes     10:00:00:60:69:50:0a:3b    2 sw2
     2    No      10:00:00:60:69:30:16:b4    1 sw1


_____________________________________________________
```

```
sw2:admin> secpolicyactivate
About to overwrite the current Active Policy Set.
ARE YOU SURE  (yes, y, no, n): [no] y
Saving Defined FMPS ...
done
Saving Active FMPS ...
done
Committing configuration...done.
```

Figure 7

After configuring administrative access, it is time to design policies that designate what target and initiator devices are allowed to participate in the fabric. The administrator can introduce policies that specify which fibre channel devices can be attached to which port(s), on designated switches (Domain ID's). These policies are known as Device Connection Control policies (DCC_POLICY_xxx). Multiple DCC policies will likely exist in the fabric. A DCC policy can be created for each individual fibre channel device in the fabric, or a single policy may be designed to incorporate all information about all the devices in the entire fabric.

A good practice would be to start with a fabric-wide 'deny all' policy that would preclude any device that is not explicitly designated in some other DCC policy from joining the fabric. DCC policies that explicitly 'permit' devices take precedence over the 'deny all' policy. The DCC policies add an additional security layer in the event that an intruder with a rogue server gains physical access to the fabric. Upon attaching the rogue device to a port, the switch will check the device's WWN against the DCC policy database and disable that port if no policy explicitly allows that device WWN.

There are two scenarios that can impact the way an administrator might choose to implement a 'deny all' policy. The first scenario results from the fact that the enterprise fabric is already operational, and there are limited opportunities to take the fabric down. The second scenario is most likely to occur in an enterprise environment that the SAN is not currently in production.

Given the first scenario of a fully operational production fabric, it is reasonable for the administrator to create a 'deny all' policy that designates a bogus WWN as the only device that can connect to all switch ports in the entire fabric. An example of this policy is displayed in Figure 8.

```
sw2:admin> secpolicycreate "DCC_POLICY_Deny_All_Fabric",
"99:99:99:99:99:99:99:99; 1(*); 2(*)"
DCC_POLICY_Deny_All_Fabric has been created.

sw2:admin> secpolicydump "defined", "DCC_POLICY_Deny_All_Fabric"

_____________________________________________________
                DEFINED POLICY SET

DCC_POLICY_Deny_All_Fabric
   Type    WWN                     DId swName
   _____________________________________________________
   Switch  10:00:00:60:69:30:16:b4   1 sw1.
   =Port=> 0,1,2,3,4,5,6,7.
   Switch  10:00:00:60:69:50:0a:3b   2 sw2.
   =Port=> 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15.
   Device  99:99:99:99:99:99:99:99

_____________________________________________________
```

Figure 8

Note the DCC policy command line syntax, and policy database output. A device with WWN "99:99:99:99:99:99:99:99" is the only device that can be attached to any port (designated by the '*' in the command line) on either of the two switches in the fabric (switch Domain Id 1 and 2). Next, the administrator should immediately generate the 'permit' DCC policies for the legitimate fabric devices, prior to activating the DCC_POLICY_Deny_All_Fabric policy. An example of a single 'permit' DCC policy for the entire fabric that self populates with all valid device WWN's that currently exist in the fabric can be seen in Figure 9.

```
sw2:admin> secpolicycreate "DCC_POLICY_Production", "1[*]; 2[*]"
DCC_POLICY_Production has been created.


sw2:admin> secpolicydump "defined", " DCC_POLICY_Production "
sw2:admin> secpolicydump

_____________________________________________________
                DEFINED POLICY SET

DCC_POLICY_Production
   Type    WWN                     DId swName
   _____________________________________________________
   Switch  10:00:00:60:69:30:16:b4   1 sw1.
   =Port=> 0,1,2,3,4,5,6,7.
   Switch  10:00:00:60:69:50:0a:3b   2 sw2.
   =Port=> 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15.
   Device  10:00:00:00:c9:27:2c:c7
   Device  21:00:00:20:37:65:84:d8
   Device  21:00:00:20:37:87:48:c8
   Device  21:00:00:20:37:87:48:a5
   Device  21:00:00:20:37:87:48:ef

_____________________________________________________
```

Figure 9

The command line syntax for the above policy can be interpreted as follows. The use of the square brackets ([ ]) in the policy definition acts as a self-populating mechanism. Notice that no device WWNs are specified in the command line. The DCC_POLICY_Production policy will automatically be populated with the WWN's of all the devices that reside on any port in the entire fabric at the time of invocation. To interpret the policy database entry, read each policy entry from the bottom up. Notice that all five 'Device' WWNs could be attached to any switch port for the switches with Domain Id's 1 or 2.

Returning back to the second scenario for implementing a 'deny all' policy, recall that the administrator essentially has a brand new installation that has not been implemented in production. To generate a 'deny_all' policy under this scenario, the administrator can disconnect all fabric devices, or invoke a **portdisable** on every port that a device is attached to. This results in a fabric that has no devices operational in it. Now invoke the **secpolicycreate** command to create a policy that allows no devices on any port on any switch in the fabric. An example of this policy can be seen in Figure 10.

```
sw2:admin> secpolicycreate "DCC_POLICY_Deny_All_Fabric", "1[*]; 2[*]"
DCC_POLICY_Deny_All_Fabric has been created.

sw2:admin> secpolicydump "defined", "DCC_POLICY_Deny_All_Fabric"

_____________________________________________________
                DEFINED POLICY SET

DCC_POLICY_Deny_All_Fabric
   Type    WWN                    DId swName
   _____________________________________________________
   Switch  10:00:00:60:69:30:16:b4   1 sw1.
   =Port=> 0,1,2,3,4,5,6,7.
   Switch  10:00:00:60:69:50:0a:3b   2 sw2.
   =Port=> 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15.

_____________________________________________________
```

Figure 10

Notice in the above example that no devices are defined, and thus, no device can be attached to any port on any switch in the fabric. The 'deny all' policy should be used as a catchall for any ports that are not explicitly defined to allow designated devices. Remember not to activate the 'deny all' policy before creating the explicit permit policies, particularly if you are going to use the auto-populate syntax.

The last of the FMPS policy set is the Switch Connection Control Policy (SCC_POLICY). If this policy exists, it cannot be empty. It represents a list of all

the switches, by WWN, that can participate in the secure fabric. At a minimum, all designated FCS switches must be included in the member list. If an administrator inadvertently attempted to create an empty SCC_POLICY, the policy would automatically generate the entries to include all the FCS switches as members of the SCC_POLICY. It is critical to include all the non_FCS switches that reside in the fabric as members of the SCC_POLICY. Non-FCS switches are not considers trusted switches, and thus can never become the PFCS nor are they included in the FCS_POLICY. Any non-FCS switches that are not included in the SCC_POLICY will segment out of the fabric. Figures 11 and 12 show examples of the SCC policy.

```
sw2:admin> secpolicycreate "SCC_POLICY"
One or more non FCS switches are not in the SCC_POLICY.
They will be excluded from the fabric when activating the policy,
unless you add them by using secPolicyAdd command later.
ARE YOU SURE  (yes, y, no, n): [no] y
SCC_POLICY has been created.

sw2:admin> secpolicyshow "defined", "SCC_POLICY"

_____________________________________________________
                DEFINED POLICY SET

SCC_POLICY
   WWN                      DId swName
   _____________________________________________________
   10:00:00:60:69:50:0a:3b   2 sw2
   10:00:00:60:69:30:16:b4   1 sw1

_____________________________________________________
```

Figure 11

The syntax used in the above command line represents an attempt to create an SCC_POLICY that contains no entries. As can be viewed in the defined policy, the FCS switches are automatically included into the switch connection controls. Also note the prompting for the missing non-FCS switch. The administrator must ensure that all non-FCS switches in the fabric get included in the SCC_POLICY. In Figure 12 below, a new switch (sw3) is introduced into the secure fabric SCC policy.

```
sw2:admin> secpolicyadd "SCC_POLICY", "10:00:00:60:69:22:08:36"
Member(s) have been added to SCC_POLICY.

sw2:admin> secpolicyshow "defined", "SCC_POLICY"

_____________________________________________________
                DEFINED POLICY SET

SCC_POLICY
   WWN                       DId swName
   ___________________________________________________
   10:00:00:60:69:50:0a:3b   2 sw2
   10:00:00:60:69:30:16:b4   1 sw1
   10:00:00:60:69:22:08:36   3 sw3


_____________________________________________________
```

Figure 12

This new switch is a non-FCS switch that is identified by its WWN. Employing an SCC policy is strongly recommended, particularly in an environment that affords physically proximity of switches that are not intended to participating in the same fabric.

Recall that all secure fabric administration must originate from a management station utilizing secure management channels. The SecTelnet and SSHv2 clients encrypt portions of the login session. Additionally, management traffic that flows between the switches, travels in an encrypted format. Application data however, is not encrypted by the fabric. For the greatest security of application data, the encryption needs to originate at the source device, not at the edge of the fabric.

Lastly, some final comments regarding application data encryption. Data encryption can be broken into two categories, encryption of the “data at rest” and “data in flight”. [7. Clark] Solutions for encryption of the “data at rest” are already being implemented today. One of the notable issues with encrypting data on the disks is key management. Solutions that address encryption of “data in flight” at wire speed are fairly new to the marketplace, and typically involve a storage security appliance. [8. Komiega]

Summary

Storage Area Networks will continue to grow outside the traditional data center boundaries, which will increase the importance of security in the enterprise. An experienced administrator will leverage from all tools and techniques that are available to form a layered defense. Successful implementations of a comprehensive security framework must combine proven LAN security technologies with fibre channel SAN technologies, including the Secure Fabric OS features.

Acronyms

ASIC	Application Specific Integrated Circuit
ACL	Access Control List
BFCS	Backup Fabric Configuration Server
DCC	Device Connection Control
DiD	Defense in Depth
FC	Fibre Channel
FCS	Fabric Configuration Server
FMPS	Fabric Management Policy Set
HBA	Host Bus Adapter
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
LAN	Local Area Network
LUN	Logical Unit Number
MAC	Media Access Control
NMS	Network Management Station
PFCS	Primary Fabric Configuration Server
PID	Port Identifier; 24 bit address
PKI	Public Key Infrastructure
SAN	Storage Area Network
SCC	Switch Connection Control
SFOS	Secure Fabric Operating System
SID	Source Identifier; Source Port Identifier; 24 bit address
SMC	Secure Management Communications
SNMP	Simple Network Management Protocol
SSH	Secure Shell
WWN	World Wide Name

References

1. Kuo, Benjamin. "The road to practical SAN security" September 2002 URL: http://www.brocade.com/san/pdf/practical_SAN_security.pdf (12 January 2003)

2. Cook, Rick. "The 5 A's of functional SAN security" (24 February 2003) URL: http://searchstorage.techtarget.com/tip/0,289483,sid5_gci881954,00.html (27 February 2003)

3. Cook, Rick. "Save your SAN: Secure your LAN" (24 February 2003) URL: http://searchstorage.techtarget.com/tip/0,289483,sid5_gci881948,00.html (25 February 2003)

4. Brocade Communications White Paper. "Zoning Implementation Strategies for Brocade " (No date provided) URL: http://www.brocade.com/docHandler?docId=1120&docType=0&download=false (1 April 2003)

5. King, Bill "LUN Masking in a SAN", (1 July 2001) URL: http://www.qlogic.com/documents/datasheets/knowledge_data/whitepapers/whitepaper.lunmasking.pdf (5 April 2003)

6. Brocade Communications White Paper. "Advancing Security In Storage Area Networks" (No date provided) URL: http://www.brocade.com/docHandler?docId=1119&docType=0&download=false (16 March 2003)

7. Clark, Elizabeth "Emerging Technology: Storage Security – Under Lock and Key" (06 January 2003) URL: http://www.networkmagazine.com/article/NMG20021223S0004?ls=TW_012203 (17 April 2003)

8. Komiega, Kevin "New tool solves NAS, SAN security woes, company says" (14 October 2002) URL: http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci856720,00.html (05 April 2003)