# Global Information Assurance Certification Paper

# Basic Fibre Channel Storage Area Network Security

By
Bryan "E" Embry

GIAC Security Essentials Certification (GSEC)
Practical Assignment: Version 1.4c, Option 1
Date Submitted: 27 Jan 05

## Abstract

World events have contributed to a heightened sense of security with regard to computer information. The majority of information pertaining to computer information security relates to host systems and the TCP/IP networks that connect them. However, Fibre Channel Storage Area Networks (FC SAN's) have rapidly evolved as peers to their cousin TCP/IP networks. A Fibre Channel SAN can be very complex in nature and a basic understanding of how to secure a Fibre Channel SAN is of vital importance in order to protect computer information. In this document, I will briefly discuss what a SAN is along with the fundamental building blocks used to build a SAN. I will then discuss some basic methods to help secure a SAN.

## 1.0 What is a Fibre Channel SAN (Storage Area Network)?

A Fibre Channel Storage Area Network (SAN) is a specialized high performance network that is used to connect host systems to storage devices using a protocol called Fibre Channel (FC). For brevity in this document, I will refer to a Fibre Channel Storage Area Network simply as a "SAN". Before we delve into the basic concepts of securing a SAN, it would be helpful to first have a basic understanding of what a SAN is. To illuminate what a SAN is, lets first examine the model of how host systems access and store data without using SAN technology. Once this model is examined, we can then explain what a SAN is by comparison and contrast.

### 1.1 Data Access and Data Storage WITHOUT Using SAN Technology

In this model of data access and storage, host systems access and store data by reading and writing data to their own internal storage disk(s) or to a directly connected external storage device such as a storage array. While this model provides basic data access and storage functionality for computer data and information, it has several limitations. These limitations are discussed below.

### 1.2 Scalability

In this model, hosts are limited in the amount of storage space they can access since the amount of storage space accessible to a host is contingent upon how many internal disk drives the host computer can support or how many direct connections a host can make to external storage devices. External, direct connections to storage devices are accomplished through the use of HBA's (Host Bus Adapters) and cables. The number of HBA's that can be installed in a particular host is limited to the number of available card slots in that host which limits the storage scalability of a that host.

### 1.3 Distance Limitations

Distance limitations are also inherent in this model of directly connecting host systems to external storage devices. Many of these host systems use SCSI (Small Computer System Interface) cables to directly connect hosts to storage devices. Unfortunately, SCSI cabling technology only supports distances up to several meters in length which requires storage devices to be in relative close proximity to their host machines.

### 1.4 Performance Limitations

Accessing storage arrays through the use of SCSI cabling is subject to the performance limitations of SCSI cabling technology. SCSI transfer speeds using these cables normally have performance in the Mbit/s range which is order of magnitudes slower than the speeds achievable in a SAN environment.

### 1.5 Host to Storage Availability

Having more than one data path from a host to a storage array improves the data availability between a host and its associated storage array. With multiple data paths, if a single path were to fail, data between the host and the storage array can potentially travel down an alternate path improving availability and fault tolerance. When direct connecting hosts and storage arrays, achieving path redundancy is usually more difficult because the number of direct connections that can be made are more limited.

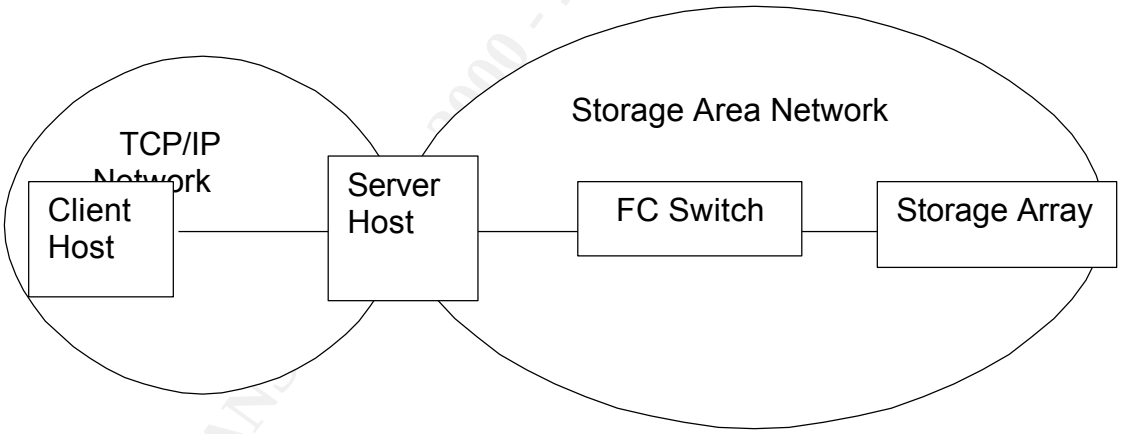
## 1.6 The SAN (Storage Area Network) Model

A SAN largely overcomes the limitations discussed in the model above by employing FC (Fibre Channel) protocols and technology. FC technology facilitates Gbit/s transfer speeds between hosts and storage devices over distances up to kilometers in length[7]. These long distances are achieved through the use of fiber optic cabling which is flexible and immune to the effects of EMI (Electro Magnetic Interference). Also, in the specifications of the Fibre Channel protocol, World Wide Numbers (WWN's) are used to uniquely identify devices on a SAN such as hosts, FC switches, and storage devices such as storage arrays and tape devices[6]. Although it is not practical, in theory, a Fibre

Channel SAN environment can support millions of hosts and storage devices. To understand more about what a SAN is, it is important to know some of the components that make up a SAN. Below are the key components that make up a SAN.

### 1.7 Host Systems

Host systems which are usually servers read, write and process the data and information in a SAN environment. These hosts use FC Host Bus Adapters (HBA's) to provide a physical connection point into a SAN. In a SAN environment, hosts and storage devices are interconnected through the use of fiber optic technology and FC switches. FC switches which are the glue used to build a SAN environment will be discussed later in this document. These hosts are often servers ie.(web servers, database servers) and provide services to other client hosts which are not part of the SAN environment, but have a need to access the data or information stored in the SAN. For example, a client host at a travel agency may access flight information by accessing a remote server in a SAN environment with a database containing flight information. This server would be connected to a storage device such as a storage array using SAN technology with FC switches and fiber optic cabling. In this example, the client host is NOT considered part of the SAN, but the server and storage array which are connected to the FC switch IS considered part of the SAN.




### 1.8 Fibre Channel (FC) Host Bus Adapters (HBA's)

HBA's in a SAN environment are Fibre Channel (FC) cards that are installed in host systems in order to allow a host to connect to a SAN. Since SAN's employ Fibre Channel (FC) technology, a host connecting to a SAN must use a FC HBA along with fiber optic cables to connect to a SAN. The fiber optic technology used in a SAN greatly improves on the distance limitations inherent in the use of SCSI cabling technology since hosts and storage devices in a SAN can span kilometers as opposed to just a few meters. Unique WWN's are assigned to each of these HBA's by their vendors. The unique WWN's assigned to these

HBA's provide hosts with a unique and identifiable connection point into a SAN. The task of securing a SAN relies heavily upon keeping track of these WWN's. Some vendors that produce FC HBA's for use in host systems include Qlogic and Emulex.

### 1.9 FC Storage Devices

FC storage devices used in a SAN are normally storage arrays and tape backup devices that employ FC technology. These storage devices can easily be scaled to support terabytes of data and beyond and are connected to FC switches in order to build a SAN. Storage arrays contain many high capacity disks that are usually configured using RAID (Redundant Array of Independent Disks) technology. RAID configurations are often implemented to facilitate high availability and fault tolerance in mission critical environments. However, RAID is beyond the scope of this document and will not be discussed. The storage space on these disk drives are logically configured and presented as uniquely identified LUN's (Logical Unit Number) to hosts in a SAN environment. Hosts use these LUN's to store data and information on them. Storage arrays can be quite complex in nature and many have redundant RAID controllers to provide ongoing availability in a SAN environment in the case of a single controller failure. There are many vendors that sell FC storage arrays. Some of these vendors include Sun Microsystems, Hitachi, EMC, Network Appliance, IBM and HP.

### 1.10 Fibre Channel (FC) Switches

Fibre Channel (FC) switches are the core building blocks used to interconnect hosts and FC storage devices. These switches are conceptually similar to TCP/IP switches but instead use FC protocols. These switches provide high performance connectivity in the Gbit/s range between hosts and storage devices on a SAN. Although it is possible to directly connect a host to a storage device using FC technology, a SAN is built by connecting hosts and storage devices via a FC switch. This type of connectivity is referred to as a "SAN fabric" and more complex SAN fabrics can be created by interconnecting FC switches with each other. SAN fabrics can be built that exponentially overcome the scalability limitations discussed in the non-SAN model where hosts are directly connected to their storage devices. FC switches also implement a number of security features which can help protect a SAN from unauthorized access and use. Some vendors that sell FC switches include Qlogic, Brocade, and McData.

## 2.0 Basic Security and SAN's

Using the components described above, SAN fabrics can be built that can easily support the interconnectivity of a large number of hosts and storage devices.

With this magnitude of scalability, it is easy to imagine the security implications involved in this scenario. How can we go about securing and protecting a SAN? A word to the wise, “build security into your SAN along the way”. This approach is much easier than trying to secure a SAN after it has been completely built. The next several sections in this document will address some basic concepts that can be used to help secure and protect your SAN.

### 2.1 Physical Security Policies

Implementing physical security policies is for obvious reasons an important practice in any SAN environment. Keeping storage devices, their associated hosts and switches in secure server rooms with controlled access is paramount in order to help protect the data and information on a SAN from unauthorized access. Physical security will also help prevent having unauthorized devices such as unknown hosts and unknown FC switches from being attached to a SAN and potentially accessing the data and information stored on that SAN. Policies should also be implemented to address the proper disposal of disk drives. The storage arrays in a SAN environment contain many disk drives. Consequently, disk drive failures are inevitable and properly disposing a failed disk drive is needed in order to prevent compromising sensitive data.

### 2.2 Using Passwords

Normally, SAN devices such as hosts, storage devices and FC switches are connected to a terminal concentrator and/or TCP/IP network through the use of serial ports and/or TCP/IP interfaces. This allows system administrators to perform maintenance and monitoring functions on SAN devices. In order to prevent unauthorized users from accessing SAN devices, it is essential to establish password protection on your SAN devices. While passwords are extremely effective, it is important to make sure these passwords are periodically changed and known only by authorized personnel. Having more than one trusted user with password knowledge is generally good practice since there have been many situations where the password was known only by a single person and that person was unavailable during a disaster or security incident.

### 2.3 Monitoring the SAN

Many SAN devices such as FC switches and storage arrays incorporate monitoring software in order to monitor their health and status. Normally this monitoring software is installed on a host system which uses a TCP/IP interface to periodically poll the TCP/IP interfaces on these SAN devices in order to obtain their status. This monitoring software on the host should be set up to continually log the status information of the SAN devices to a log file. Having effective log files are paramount in determining if a breach of your SAN has occurred and can be very useful in reconstructing events leading up to a SAN security breach.

## 2.4 Connecting a SAN to a Private TCP/IP Network

Although connecting the TCP/IP interface of a SAN device to a TCP/IP network is often needed in order to monitor its health and status, connecting SAN devices to the same TCP/IP network used by enduser host systems on a company network often presents its own unique problems. For example, many SAN devices such as storage arrays and switches employ a small, scaled down operating system which allows you to log into that SAN device to enter configuration and status commands through its TCP/IP interface. These smaller, scaled down operating systems often contain TCP/IP stacks and buffers that have been scaled down for basic TCP/IP functionality. Consequently, a problem may arise when third party security scanning software is used on that same TCP/IP network. Security scanning software is often used to probe host systems on a TCP/IP network for vulnerabilities. If these SAN devices are directly connected to that same network, many times, the security scanning software will hang or lock up these SAN devices after probing them. This hang condition often occurs because the scaled down TCP/IP functionality on these SAN devices often lack the robustness found in the TCP/IP code of a full blown operating system used by a host system. One solution to this situation is to place SAN devices on a private TCP/IP network which is not being probed by security scanning software. Placing these SAN devices on a private network also reduces their vulnerability of being attacked by malicious hackers.

## 2.5 Securing your SANS using Zoning

One of the basic building blocks of a SAN is a Fibre Channel (FC) switch. FC switches provide scalability in a SAN environment by allowing multiple nodes such as hosts and FC storage devices to be interconnected. Recall, this is referred to as a “SAN Fabric” and FC switches can be also interconnected with other FC switches to create more complex SAN fabrics with exponentially more nodes. Connecting multiple hosts with multiple storage arrays using FC switches also creates security implications. To illustrate, suppose a single SAN fabric has one storage array containing proprietary engineering information and another storage array with sensitive HR (Human Resources) information. How do we keep the engineering host(s) which are a part of this SAN fabric from accessing the HR information and the HR hosts which are also part of this same SAN fabric from accessing the engineering information? Using “zones” provides us with a solution to keep the engineering host(s) and their logically associated storage array(s) segregated from the HR host(s) and their logically associated storage array(s)[3]. From our own intuition, a “zone” is an area that has been partitioned and segregated from other areas so it can be used for a specific purpose and this is how zones are used in a SAN fabric. Zones are configured on FC switches and are normally configured by logging into a FC switch or accessing the FC switch through the use of switch management software. The two types of zoning are “Hard Zoning” and “Soft Zoning” and are discussed

below.

### 2.5.1 Hard Zoning

FC switches have physical FC ports on them used to interconnect other FC nodes such as storage devices and hosts. FC switches usually contain 8 ports, 16 ports, 32 ports and more. “Hard Zoning” is a method where a subset of the physical ports on an FC switch can be partitioned and grouped together. For example, on a 16 port FC switch, you may want to group ports 0-7 into a single hard zone and group ports 8-15 into another hard zone. In this configuration, only the devices physically connected to ports 0-7 on the FC switch are visible and accessible to each other. None of the devices physically connected to ports 0-7 would be able to see and access the devices connected to ports 8-15 on the same FC switch. The reverse is also true. The devices physically connected to ports 8-15 on that same FC switch would be visible and accessible to each other but would not be able to see and access the devices connected to ports 0-7 on the same FC switch. Hard zones in a FC switch cannot overlap and any FC device wishing to access the devices in a particular hard zone must be physically connected to one of the switch ports included in that hard zone. Hard zoning is the most secure method of zoning since it is based on the underlying switch circuitry. The FC switch itself simply maintains a table of the hardware ports grouped in a defined hard zone. FC frames originating from outside of a particular hard zone destined to the devices in that hard zone are simply dropped. Creating hard zones are an effective way to keep hosts and storage arrays with a similar purpose logically grouped together while preventing them from being accessed by other hosts. A drawback to hard zoning is its lack of flexibility. For instance, if a particular device needs to be moved to a different zone, this would require either physically reconnecting that device to a different port on an FC switch or reconfiguring the hard zone itself using the switch management software.

### 2.5.2 Soft Zoning

Another method of zoning is “Soft Zoning” which is also used to logically control the access between hosts and storage devices. All FC nodes are uniquely identified using a WWN (World Wide Name). Theoretically, no two FC nodes share the same WWN. When setting up a soft zone on a FC switch, WWN’s associated with devices are logically grouped together. For example, the WWN of a storage array containing HR data can be logically grouped with the WWN of the HR host(s) that need access to that data. Soft zoning has more flexibility than hard zoning because the zones are created using the WWN’s of devices and not the physical ports on a FC switch. This allows you to logically associate storage arrays and hosts so they can see and access each other regardless of which physical port on the FC switch they are connected to. Soft zones can also overlap which means that a particular device can reside in more than one soft zone simultaneously. A common example for using overlapping in a soft zone is

placing a FC tape backup device in two soft zones simultaneously so the devices in each soft zone can utilize the FC tape backup device. Soft zones can also span across FC switches that are interconnected.

### 2.6 Securing SAN Storage Access using LUN Filtering

Recall that a storage array contains many physical disk drives. A LUN (Logical Unit Number) is used by a host operating system to uniquely address a logical area of disk space on a storage device such as a storage array. A LUN normally identifies a partition on a single disk drive or a partition on a RAID set composed of several disk drives. Storage arrays can be configured with hundreds of partitions that are each accessed by hosts using unique LUN's. One method of providing controlled access to data and information on storage arrays is through the use of LUN filtering, sometimes called "LUN masking". LUN filtering is a method where the LUN's on a storage array are assigned to specific host connections. For example, suppose a storage array with a RAID set has been configured with two partitions. These two partitions would ultimately be presented as two individual LUN's to the host connections on a SAN. For simplicity, lets designate these two LUN's as LUN 1 and LUN 2. Using LUN filtering, it is possible to configure LUN 1 to be accessible only by host A and to configure LUN 2 to be accessible only by host B. This is accomplished through the use of WWN's. Recall that each host connection in a SAN environment is identified using the WWN assigned to its HBA. With this in mind, it is possible to configure a LUN to only be accessible by the WWN's of HBA's belonging to specific hosts. For example, you can designate LUN 1 to be accessible only by the WWN belonging to the HBA on host A and LUN 2 to be accessible only by the WWN belonging to HBA on host B. Using LUN filtering, a single storage array with one LUN containing HR information and another LUN containing engineering information can be secured by assigning each LUN only to a host that needs access to that information. The configuring of LUN filters in a SAN environment is normally accomplished on the storage array itself.

### 2.7 Protecting the Ports on your FC Switch

The hardware ports on a FC switch can also present a vulnerability to a SAN environment. Each port on a FC switch has the ability to operate in one of several modes. For instance, a single port can be designated as an F-port which would be used to connect a fabric device such as a host or storage array to the FC switch or a port could be configured as an E-port which would be used to interconnect two FC switches to build a larger SAN fabric. There are several other port modes that can also be configured such as a G-port. A G-port is considered a universal port, which will automatically and dynamically adjust its mode to support a particular device that has been attached to it such as a host, storage array, or even another FC switch. A vulnerability in this scenario exists when an unauthorized device is connected to a SAN environment. For example, connecting an unauthorized FC switch to a SAN could potentially provide an

entry point to access the information stored on that SAN. To help protect against this kind of vulnerability, it is important to make sure ports on a switch are configured into a mode that supports the type of device that you intend to connect to those ports. As an example, if you know beforehand that you will only be connecting hosts and storage devices to your FC switch, then it is best to configure those ports as F-ports and not as E-ports or G-ports. This will help prevent someone from connecting an unauthorized FC switch to your SAN and accessing your stored information. Other ports on a FC switch that are not being used should be temporarily disabled until they are needed[2].

### 2.8 SAN Fabric Security with FC Switch Operating Systems

FC switches have a small Operating System (OS) used to manage the switch itself and many vendors are including features in their switch OS's to make a SAN fabric more secure. One example would be Brocades "Secure Fabric OS"[5]. Secure Fabric OS provides a number of features such as the ability to set up "trusted switches". These trusted switches are given the responsibility of managing the configuration and security parameters of all other switches in the SAN fabric[5]. These trusted switches provide a central point of management for the other switches in a SAN fabric and are recognized by these other switches through the use of an authentication process. This authentication process can help protect a SAN from the threat of WWN spoofing where an attacker assumes the WWN of one FC switch to gain access to another FC switch[4]. Also, centrally managing a SAN fabric helps enhance the security of a SAN by providing a limited point of management access which reduces the overall vulnerability points in the entire SAN. Other vendors such as Qlogic and McData are implementing their own security features into their FC switch OS's. The drawback of many of these switch OS's lies in the area of compatibility and interoperability. Usually, the security features designed into a FC switch provided by one vendor are not compatible or interoperable with the security features designed into the FC switches provided by another vendor. This often forces a customer to purchase all of their FC switches from a single vendor.

### 2.9 Protecting Data at Rest and Data in Flight

So far, the methods we have discussed include using passwords, zoning, and port protection which are designed to safeguard against unauthorized access to your SAN. However, following the concept of providing protection through layering, further protection of data and information stored in a SAN can be provided through the use of encryption. The data in a SAN is either "at rest" when it is physically stored on a storage device such as a storage array or tape device or the data is considered "in flight" when it is in transit across a SAN. Using encryption techniques to protect data at rest or in flight is a powerful way to protect the confidentiality of data stored in a SAN in the case where that information is accessed or intercepted by an attacker.

### 2.10 Perimeter Protection of a SAN

Although a SAN is a specialized type of network unto itself, in order for endusers to access the data or information stored in a SAN, the SAN information itself must ultimately be accessible via the use of an outside TCP/IP network. Recall, that enduser client hosts which are not part of a SAN normally use a TCP/IP network to access a server which is directly connected to and part of a SAN. This opens up a whole realm of potential vulnerabilities in a SAN. One of the most obvious vulnerabilities lies with the server connected to the SAN itself. Access to SAN information or data as well as storage devices and FC switches may be obtained if any of these servers are compromised or breached. In light of this, securing the TCP/IP network that is used to access your SAN is vitally important and using firewalls along with intrusion detection and intrusion prevention systems must be considered[1].

## Conclusion

SAN technology has enjoyed explosive growth in the last five years and will continue to grow for years to come. As SAN's continue to grow in size and complexity, more vulnerabilities in the SAN environment will continue to surface[4]. Knowing this, it is paramount to build security into a SAN during each step of its implementation and understanding the foundational concepts of a SAN and some of the basic methods of securing a SAN are no longer an afterthought and must be taken seriously in order to protect vital information[8].

## List of References:

[1] Clark, Elizabeth. "Fibre Channel San Security." Network Magazine. 4 Sep 2002. <http://www.networkmagazine.com/article/NMG20020826S0012>.

[2] InformationWeek. "Storage Security Best Practices." storagepipeline. 4 Aug 2003. <http://www.storagepipeline.com/showArticle.jhtml?articleID=12808179>.

[3] Chudnow, Christine Taylor. "Fibre Channel security." Computer Technology Review. Mar 2003. <http://www.findarticles.com/p/articles/mi_m0BRZ/is_3_23/ai_99751348>.

[4] Scheier, Robert. "Time to prepare for SAN security." SearchSecurity.com. 18 Sep 2002. <http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci851338,00.html >.

[5] Brocade. "Secure Fabric OS, A comprehensive security architecture for SAN fabrics." <http://www.brocade.com/san/pdf/datasheets/SecureFabric_DS_04_lr.pdf>, 2004.

[6] Chris Beauchamp, Josh Judd, and Benjamin Kuo. Building Sans with Brocade. Rockland: Syngress Publishing, 2001.

[7] Benner, Allen F. Fibre Channel for SANs. New York: McGraw-Hill, 2001.

[8] Leyden, John. "Myth of storage security savaged." The Register. 24 Jan 2002. <http://www.theregister.co.uk/2002/01/24/myth_of_storage_security_savaged/>.