GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Storage Area Networks and Security

GIAC Security Essentials Certification (GSEC)
Practical Version 1.4, Option 1
April 5th, 2003
Neha Bhatt

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

What is a SAN? 3
SANs versus DAS and NAS 3
What is security? 4
Why is security important? 4
Types of attacks on Storage Area Networks 4
FIbre Channel vs IP 5
SANs Security Framework Proposed by Brocade Corporation 6
Security Domains 7
Security Framework-Evaluator Group 7
Outer Perimeter 8
Middle Perimeter 8
Inner Perimeter 8
Conclusion 11
REFERENCES 12

© SANS Institute 2003, Author retains full rights.

ABSTRACT

In this paper I will describe Storage Area Networks (SANs) including various terminology associated with SANs, a brief history about SANs security, and its variety of threats. The main focus will be on securing a SAN, in particular the various methods of defense in protecting the SANs. More specifically, emphasis will be placed on the proposed solutions of the Evaluator Group and Brocade Corporation. We will further explore the "inner layer" of defense including LUN Masking, Switch Zoning and security domains which are different methodologies involved in securing a SANs. In addition, a comparison of these two types of SAN interfaces, Fibre Channel, and IP will be discussed.

WHAT IS A SAN?

The need for storage of data and information as well as the increase of security awareness in the general population has brought the concept of a Storage Area Network to the forefront. A Storage Area Network establishes a direct connection between storage elements and servers or clients. [7] This concept is similar to a Local Area Network (LAN) with the exception of allowing greater storage capacity and faster subnetworks. A SANs device allows multiple direct host connections or connections through a fiber hub or switch. [1,6] The purpose of SANs is not confined to strict communication between storage and computers. Many institutes conduct administrative functions and other applications using SANs. The one characteristic a SAN is noted for and what separates it from other systems is its ability to universally connect with storage devices in computers. [10]

SANS VERSUS DAS AND NAS

In order to understand SANs, one must recognize the importance of the concept of other storage options. One of the more obsolete technologies is the Direct Attached Storage (DAS). The DAS system allows direct access by a given host to data. DAS was a viable alternative to mainframe in that it was faster, easier, and available at a lower cost. DAS capabilities were eventually too little for emerging technology. [6]

The rise of Network Attached Storage (NAS) and SANs were a byproduct of manufacturer discrepancies and their need to alleviate some vulnerabilities while advertising their strengths. NAS devices are similar to SANs devices in that they allow multiple host to share files using a common file protocol over a network connection. However, NAS can be limiting in that it can only support a certain number of operating systems. [6]

On the other hand, SANs support multiple operating systems and can be implemented using a "SAN Network architecture". This allows greater options and reliability when being used in long distance disaster recovery. [6] Whether using SANs or NAS one must understand security and possible threats to it.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

WHAT IS SECURITY?

Security is defined as the “management of a risk”. Risk is defined as the readiness of the information versus the exposure to theft, destruction, or alteration. Combined, a security risk is a seldom-used phrase in the IT world due to a lack of knowledge on execution of security features designed to protect information in SANs. This leads us into the importance of security as it applies to a SANs. [3]

WHY IS SECURITY IMPORTANT?

The rise of client/server networks throughout the 1990s produced greater difficulty in the effective security of data and applications. With the rise of the Internet into everyday life and business, the need for more advanced security came to the forefront. The task of securing information became greater than the need for obtaining data. Companies had to discover and manufacture advanced yet flexible security features to minimize the risks involved in data storage. [2]
The importance of security can be traced back to the 1970s and 1980s when network intrusions were limited to technically savvy individuals who could “reverse-engineer the system”. In the present day, sophisticated and automated tools allow for multiple types of intrusions due to the wide range of access points. [3]

According to Network Magazine “With more and more storage devices and networks becoming interconnected-not to mention the rise of IP-based storage security is becoming a topic of increasing concern”. In a recent question presented to its customers, EMC corporation acknowledged that most customers reaffirm their position about needing security however most have spent minimal to no time implementing security procedures. [4] The explosion of business activity and E-commerce has forced organizations to carefully balance expansion of enterprise with ability to protect information. [2]

According to Brocade corporation, “ Online expansion opens up a whole new world of possibilities-such as increased efficiency, reduced costs, improved enterprise communications, shorter time-to-market, and wider market reach”. This further stresses the need to construct a security framework to protect enterprise data. [2]

This can conclude that the need for security has not gone unnoticed but the inability to execute security practices that will cover all aspects in the ever-changing technology world still persists. Present-day companies and its professionals are in an everlasting campaign to guard data of large infrastructure IT companies. The most intense of these battles deals with the security of a SAN.

TYPES OF ATTACKS ON STORAGE AREA NETWORKS

There are several avenues of access into the storage device, a few of which will be explored here. The first type involves an intruder endeavoring to gain unauthorized

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

access, and the second is a Denial of Service attack (DOS). A DOS on any network will deny users from accessing that network. These attacks can be initiated from the inside or the outside [3].

Primary attacks involving unauthorized access are usually the result of non-system users gaining entry at a low level and then attempting to advance their status in the system. Reasons for this attack range from destruction of information, alteration of the data, and to view confidential and sensitive information. This can include changing switch configurations, corrupting or modifying sensitive data, or defacing of a Web site. In the very competitive world of business, this access can grant the user with sensitive business secrets that might be stored in a SAN-accessible device. [3,5]

The DOS attack is based on overloading its target system to impair its ability to communicate with the authorized user as well as delay response of the system to the requested command. This type may come from single or multiple systems and tend to focus on the perimeter technologies, which are ultimately the weakest link. [3] These various elements of attack are consistently improving in speed and method leaving the organization to plan and implement multiple strategies to offset the attacks. A proper security framework that balances protection of vital information without slowing core business procedures is imperative. [5]

FIBRE CHANNEL VS IP

Much has been said about Fibre Channel or IP storage networks as to which are the more secure networks. According to September 2002 Tutorial on Fibre Channel SAN security, Fibre Channel has been recognized as having greater security. However, debate continues about the attributes of the IP storage networks in that multiple security systems have been created and can be implemented in an IP network as opposed to a Fibre Channel. This has caused greater acceptance of the IP network [4].

Fibre Channel is often the choice of a manufacturers because of its ability to function and transmit information over a long distance using light to communicate. Many SAN manufacturers are currently utilizing the Fibre Channel method for product design which can connect directly to one another via FC-Hub, a Fibre Channel switch, or a combination of these two. Another option is to connect in a loop formation whereby a physical loop is formed to connect several devices. This loop resembles an FDDI ring in that the ring of devices reconfigures itself as more devices are added or subtracted or in case of a device failure. Fibre Channel switches provide a high-speed connection created in the point-to-point fashion. This method allows for not only faster communication but also a more efficient connection in that as the number of devices connected grows, the system itself stays compact unlike the loop formation which will increase in size as the devices added multiply. [6]

Due to Fibre Channel's high speed and large communication connections for Storage area networks, they are rapidly becoming the framework of choice. As storage capacity and the need for storage increases, the need for a more efficient SAN is necessary.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This means a growing complexity of the SAN due to the increased familiarity of the SANs network by the manufacturers and system administrators. The bottom line means a "highly available consolidated data access" brought about by the SAN. [8]

The perception of security offered by a Fibre Channel SANs as compared to other storage solutions is due to SANs network capability of devoting distinct communication between the storage system and its information recipient. As mentioned earlier, Fibre Channel SANs utilize optical Fibre which inhibits "sniffing". Furthermore, the chance of system compromise is diminished using Fibre Channel SANs that are not Internet linked as compared to an Internet connected storage system such as an IP based network. The security of a Fibre Channel SANs based on its ability to avoid network breaches contributes to its positive image. [7]

The inherent danger of Fibre Channel and IP networks, focusing mainly on the management interfaces, is the possibility for unauthorized access to the SAN. This is particularly important if the offender obtains access at the administrative level which allows a comprehensive interface with all other devices linked to the SAN. [7]

SANS SECURITY FRAMEWORK PROPOSED BY BROCADE CORPORATION

Flexible, yet powerful security components along with an efficient security framework lead to a highly secure SAN infrastructure. These components should include fabric configuration servers, management access controls, secure management communications, switch connection controls, and device connection controls. [2]

Fabric Configuration servers allow only secure trusted switches to access administrative functions which are sensitive. This mitigates the threat of corruption of security due to unauthorized management access. Additionally, the primary fabric configuration server concept helps eliminate unauthorized management requests from insecure switches. [2]

Management access controls secure the manager-to-fabric connection by controlling the HBA connection to the fabric. This will also allow for limitation of access by unidentified switches within the fabric by permitting organizations to disable control to selected management access points and/or restrict the access to a specific set of end points. [2]

Because WWN spoofing is a viable threat to SAN security, mainly due to the control methods used that request the WWN for access rights, device connection controls that secure the server are utilized to address this weakness. These controls also allow binding of a WWN to a specific port. This helps avoid other ports from finding the identity of the WWN. Better control over shared switch environments is enabled by this type of control. [2]

Switch connection controls let organizations limit connections to switches in the fabric. New switches must be authenticated before joining the fabric which is done using the switch's digital certificate or unique private key. This control provides specification for

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the switch list that is authorized while the digital authentication verifies that the WWN is correct and is a switch at all. [2]

Security Domains

Domains delineate the multiple categories of communication of the fabric security architecture that must be protected. These security domains must be placed by organizations in order to identify possible weak areas of the network. The domains include administrator-to-security management domain, host-to-switch domain, security management-to-fabric domain, and switch-to-switch domains. [11]

Administrator-to-security management domains consist of administrator access controls working in coincidence with management functions. This permits administrator-level functions to override and achieve control over security configurations. This is usually done by password access primarily. [2,11]
Host-to-Switch domains allow numerous switches to be joined with individual device ports utilizing access control lists or ACLs. Certain manufacturers provide controls that will facilitate binding the ACL and WWN which allows a secure connection during normal operation and management functions. [2,11]

Security management-to-Fabric Domains require encryption of data by a security management function with the switch's public key. This switch subsequently decrypts the data with its private key. This is a viable option for securing such things as a password leading to management communications. [2,11]

Switch-to-switch communication ensures that only authorized and authenticated switches can access a SAN fabric or a fabric zone. Digital certificates and ACLs initialize the switches of the security management functions and the switches impose the security policy. [2,11]

SECURITY FRAMEWORK-EVALUATOR GROUP

Mitigation of risk involving storage network security can also be attained by implementing a perimeter system of defense proposed by The Evaluator Group™. This method utilizes a multiple tiered security which deters intrusion as well as accentuates the technology being used to provide this perimeter. Because of the intimate connection between the various layers or perimeters, there must be a congruence of technologies allowing for proper communication between these perimeters. This must include technologies to conceal weaknesses that may be present in the outer, middle, and inner perimeters. [3]

Comprehensive security must allow for importance and distinction of each constituent involved in the internal network. However, all elements must allow for similar functionality in performing its primary functions. These functions consist of the following; integrity, availability, confidentiality, authentication, authorization, and accounting. The integrity of a system secures the network from improper modification.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Availability allows for accessibility of data in a timely manner. Confidentiality of a system protects the information from unauthorized exposure. Authentication verifies that use of resources are being utilized by an authorized entity. Authorization ensures limited access control to a system based on privileges and restrictions. Accounting provides a final security log of users according to the systems accessed and activities performed. [5]

Outer Perimeter

The initial security layer or the "outer perimeter" of an internal network system framework generally consists of firewalls, intrusion detection systems (IDS), and various other components [3]. A firewalls device allows traffic regulation between a secure area and a untrusted area contingent upon the security policies placed by the organization. The IDS red flags network patterns that may cause a conflict. This is accomplished by sensors which monitor data traffic. Host Based Intrusion Detection (HIDS) system and Network Based Intrusion Detection (NIDS) are the aforementioned sensors that comprise the IDS. This primary layer mitigates specific risks encountered by the SANs system. [5]

Middle Perimeter

The middle perimeter consists of securing the operating system. Depending on what Operating System (OS) that is running, the security setting range from security related patches and service packs, to setting domain security policies. [5]

Inner Perimeter

Security settings for internal storage are housed within this perimeter. It consists of management software, switch zoning and other fabric security settings, and LUN Masking; all of which are various methods of providing data access security for a Storage area Network. [1,4] This perimeter and its various techniques are discussed in greater detail below.

LUN Masking

This method of security for a SANs is necessary in that storage is made visible to any hosts connected to the SANs. This additional level of security is vital to allow only specific information to be made available to specific host devices. LUNs, Logical Unit Numbers, attempt to inhibit access to vital information by LUN masking. LUNs are defined as Small Computer System Interfaces (SCSI) identifier for a logical unit within a target device. LUNs are assigned in the Fibre channel world based on the system's WWNs. LUN masking may be implemented at multiple locations within the SAN which includes the storage arrays, bridges and routers, and HBAs. [7]

HBA implementation allows for limitation of commands by the software in the HBA. This will restrict visibility by the device driver to specific LUNs. This technique limits its

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

boundaries to the HBA in which it is within. Another area which LUNs may be installed is in a RAID subsystem which is a disk controller that operates a set of disk drives. This method establishes a table of port addresses within the RAID subsystem which allows certain addresses to utilize commands to a specific LUN or LUNs. [7]

LUN masking utilizes LUNs that are designated to certain hosts and allow the host server to only see the LUN that has been assigned to them. This tool may be used to limit access being attempted by multiple servers on a specific device. Restrictions to these servers can be made by the network administrator by confining the visibility of any information to an individual LUN or multiple LUNs. [4]

Standardizing the type of LUN masking that is occurring is essential in order to avoid multiple points of contention. Because multiple methods of LUN masking exist, it is prudent to explore the options and find which one works for your particular setting.

Zoning

Zone construction consists of servers and storage devices as part of a SAN fabric. They are able to access each other through port-to-port connections. Communication and recognition between devices in similar zones is possible however zone-to zone interaction is prohibited unless a specific configuration is acquired by one of the devices within that zone. Devices within a specific zone are called zone members and are identified by a port number or World Wide Name (WWN) which instantly identifies zone members by their 64-bit number. [9] Zones enhance the security of a network by preventing data loss through the control of the device access or their user groups. [8]

Zoning controls access to a SANs by directing and limiting access from a host device. Switches and hubs are utilized to support zoning to provide an additional degree of security. Zoning separates access to specified storage resources and limits it to only those who are authorized to access that particular zone. All communication within the zone is restricted to only those who have access to the zone. [7]

Zoning should be used by a SAN administrator to prevent failures of the system. It allows for multiple operating systems to function in the same environment. Proper segmentation of storage devices from those devices that are running the operating system is required. Furthermore, accessibility of data can be restricted by the administrator to certain users to prohibit sensitive information from being read by those who are not authorized to read it. [5]

Zoning creates barriers between devices that are using different operating systems which is critical in preventing corruption or loss of the data that may have been erroneously transferred between the devices. Additionally, zones allow for maintenance or other administrative functions to be performed distinctly without interruption to any of the other user groups. Temporary access to data may be authorized by the administrator for any specific reason as well as restoration of the restriction to return to normal activity. [8]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Types of Zoning

Hard Zoning

Zones may be utilized in numerous ways. One such way is known as switch zoning which is further divided into hard and soft zoning. Hard zoning, considered more secure than soft zoning, it defines zones based on the switch ports and reinforces soft zoning through hardware utilizing a router table. Hard zoning can be likened to complete restriction of access to data storage even if it is attempted by accident or intentionally. This security zoning method would not allow access in either case. Attempts at unauthorized access are prohibited by hard zoning because of its implementation in the system's circuitry and enforced by the system's routing table. The enforcement comes from using the physical fabric port number of a switch to generate the zones. This is contingent on the fact that there is actual, physical security on the switch is established. Hard zoning is simpler to design and manage and the hardware implements data transfers while ensuring unauthorized zone-to-zone traffic is prohibited. However, moving the devices to a different port will require alteration and modification of the policy. [5]

Soft Zoning

This security option is less secure than hard zoning in that it would restrict access to information without the proper authorization. However, unintentional attempts at access which accidentally "break the code" would allow unrestricted entry. Soft Zoning enforces zoning by using the name server and the WWN enforces the configuration policy. Based on the World Wide Names (WWNs), which are exclusive identifiers attached to a Fibre Channel device, soft zoning switches ensure that incoming frames are assigned to the same zone. Source and destination addresses (WWNs) must correspond or the switch will remove the frame that does not match. Soft zoning allows greater flexibility if a switch must be moved between different ports. This can be accomplished without altering the current zone. Devices can be moved to different switch ports without manual reconfiguration of any zones. [5] This generally means time will be saved by the SANs administrator which has constant device configuration changes occurring. The greater flexibility is offset by the insecurity of the soft zoning. Careful alteration of the frames can lead to access to switch zones that are previously off limits. [7]

The inherent weaknesses of soft zoning fuel the need to implement hard zoning devices. With soft zoning, the WWNs are able to be spoofed which will allow unrestricted access to resources. WWN changes, such as adding a new HBA card, require modification of the policy. Finally, incompatible HBAs can access the host directly because the switch does not control data transfers. [7]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Security concerns of ZONING

Even with all of the security measures offered by implemented zoning, SAN systems are still able to be exploited by certain risks. These risks include physical access, zone merging, and WWN spoofing issues. Attack on a SAN can occur physically by bypassing the hard zoning. This could be accomplished by physically changing the switch cable from a secure device to an insecure device. This can cause other problems if a switch change can join the switch into the fabric. Potential security issues exist because it is possible to incorporate switches and their zoning configurations into a SAN fabric. Once the zoning configuration has been compromised, the entire zoning is obsolete for the entire fabric. Whether by accident or deliberately, the zoning bypass can occur if the account password has been obtained and an adverse data element has been introduced by a switch into the fabric. WWN spoofing is a common method of attack in the IP world. This allows a rogue element to bypass the soft zoning in a SAN environment by deceiving the device as a different entity. A recommended way of securing the SAN even in the midst of zone bypassing, is to limit the number of switch-to-switch ports that are available or created. Another way is to disable those ports and switches that are not being utilized as ISL ports. As the required number of switches are increased, the port may be "re-enabled" in the fabric to accept it as an ISL. [5]

CONCLUSION

The advent of the SANs has brought about many changes to the IT industry allowing greater storage capacity and accessibility. As the positive changes have come about, so have the inherent risks to the SANs. The ever-changing SAN environment has inspired greater security measures that are not only more advanced technologically but also in terms of flexibility and scalability. The ability of the SAN to deliver shared storage in an open environment using numerous connectivity has caused organizations to put out well thought out security policies concerning the interaction of the devices to the SANs to ensure proper access. The limitless availability of connections for the SANs can also be a liability and data integrity must be protected. As we explored the many options of security throughout this paper, there were many advantages and disadvantages for each method. However one thing was clear; SAN security strategy must be designed and implemented utilizing multiple options instead of relying on simply one. Not doing so could be detrimental to the SAN fabric and data. Proper management of the SANs is an ongoing task to ensure that data quality has not been tampered with or that the level of security has not been compromised. This is crucial as the SANs infrastructure continues to evolve. As made evident by the Brocade and Evaluator proposed solutions, layers of defense are necessary in order to accomplish secure connections and allow for controlled access to information. Firewalls, IDSs, and various other components are but the first line of defense against tampering. Utilization of LUN masking, zoning provides a more granular line of defense using encryption, passwords, and device controls to cover up weaknesses as well permit authorized and authenticated access to a storage area network.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

REFERENCES

[1] EMC^2 "EMC SANS Product Description Guide"
URL:
http://www.emc.com/pdf/products/san_mgr/C997_san_manager_pdg.pdf

[2] Brocade Corporation. "Advancing Security in Storage Area Networks"
URL:
http://www.brocade.com/san/Feature_Stories/advancing_security.jsp

[3] Martin, D. Infostor Magazine "SANs Heighten Storage Security Requirements" January 2002
URL:
http://is.pennnet.com/Articles/Article_Display.cfm?Section=Archives&Subsection=Display&ARTICLE_ID=132420&KEYWORD=security

[4] Clark, E. Network Magazine "Emerging Technology: Storage Security – Under Lock and Key" January 2003
URL:
http://www.networkmagazine.com/article/NMG20021223S0004

[5] Brocade Communication System, Inc. "San Security: A Best Practices Guide"
URL:
http://www.brocadekorea.com/download/resource/SAN_Security_Practices_Guide.pdf

[6] Chirillo, J. Blaul, S. Storage Security. Indianapolis: Wiley Publishing, 2003

[7] Clark, E. Network Magazine "Fibre Channel SAN security" September 2002
URL:
http://www.networkmagazine.com/article/NMG20020826S0012

[8] O'Donnell, M. McData "Security in Switched Fibre Channel SANs"
URL:
http://www.mcdata.com/downloads/whitepapers/SecurityInSANs.pdf

[9] Datalink "Storage Area Networks: Data Security & Fabric Management" July 2002
URL:
http://www.storagesearch.com/datalink-art1.html

[10] Barker, R. Massiglia, P Storage Area Network Essentials New York Wiley Publishing 2002

[11] Vacca, J. "The Basics of SAN security – Part I" July 2002
URL:

© SANS Institute 2003, Author retains full rights.

http://www.enterprisestorageforum.com/sans/features/article.php/1431341

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.