

# **Storage Area Network (SAN) Security**

**Santhosh Kumar.M**

*MBA (Information Systems & Security)*

[ms.santhoshkumar@gmail.com](mailto:ms.santhoshkumar@gmail.com)

## Contents

---

<b>Introduction</b>	<b>3</b>
<b>Threats to a SAN</b>	<b>3</b>
<b>Security Mechanisms</b>	<b>4</b>
<b>Methodologies</b>	<b>6</b>
<b>Business Benefits</b>	<b>9</b>
<b>Summary</b>	<b>9</b>

### **Introduction**

A brief about SAN security and its importance

### **Threats to a SAN**

Commonly available threats to a SAN discusses here

### **Security Mechanisms**

Industry practices and mechanisms to be applied

### **Methodologies**

#### *Security Solutions*

Methodology to be followed

#### *Vendor Solutions*

SAN Security solutions

#### *Policy Documentation & Checklist*

Steps to be followed and documentation

### **Business Benefits**

Advantages of implementing SAN security

### **Summary**

Summary of the solutions discussed and best practices

## Introduction

*This white paper provides an overview of techniques & technologies that have evolved around security of Storage Area Network (SAN). I will discuss the importance of SAN security and why it is crucial for protecting a company's assets. This paper will touch upon common threats to a SAN and the precautions a business can take to protect itself. The main focus of this paper will be on securing a Storage Area Network by using commonly available security solutions and the solutions offered by SAN security vendors.*

*A Storage Area Network establishes a direct connection between storage element and servers or clients. This concept is similar to a Local Area Network (LAN) with the exception of allowing greater storage capacity and faster sub networks. A SANs device allows multiple direct host connections or connections through a fiber hub or switch.*

*The SAN is one of vast virtual pools of storage that can be accessed from any host connected to the network. In SAN theory, any host can get to any data within the SAN. It is an appealing vision, but from a security standpoint it is predicated on the idea that every attached host can be trusted, which may not be the case. Many SANs are only as secure as the hosts and clients attached to the storage network. If one of those systems is compromised, the data on the SAN becomes exposed. Fortunately, there are no known reports of SAN security problems to date. Most of the SAN implementations today are relatively small pilot projects. As such, they haven't attracted much attention beyond the small cadre of storage specialists who administer them. Also, these early SANs are buried deep within the organization – typically under lock and key in the data center.*

*Until now, SAN security has not been a major concern; rather it is more of a nagging issue. But as soon as organizations roll out their enterprise-wide SANs and load them up with all their stored information, SANs will become a much more tempting target. Security is one of the most neglected aspects of SANs. The common security issues are as follows:*

- ? Poor administration of the storage network.*
- ? Lack of a comprehensive security policy.*
- ? Absence of vulnerability analysis during the design and construction phase of the SAN.*

## Threats to a SAN

*Threats can be broken up into three basic levels. The first level of threats is unintentional and due to accidents or mistakes..The second level of threats is a simple malicious attack that uses existing equipment and possibly some easily obtained information. These attacks are..usually from internal sources. The third level of threat is the large scale attack that requires an uncommon level of sophistication and equipment to execute the attack. Third level attacks are extremely rare in SANs today and may take considerable knowledge and skill to execute.*

### Level One Threat

*Although level one threats are unintentional, they are just as serious, if not more so than the other threats because they are the most common in the workplace. Serious consequences can happen as a result of these mistakes, such as downtime and loss of revenue. Luckily for SAN administrators and for security concerns, level one threats are the easiest to prevent.*

*Simply plugging in a wrong cable, or for that matter unplugging a correct cable, can cause a level one threat. Therefore, the easiest way to avert this from happening is to limit physical access to the SAN environment. This is not only best practice for preventing accidents, but also for securing against malicious threats to the SAN.*

*Storage area network switches have an Ethernet port and serial port that can be used for management purposes. To further secure*

physical access to the SAN, one can "[create] a private network to manage the SAN that is separate from a company's Intranet. If the switch is connected to the company Intranet, Firewalls and Virtual Private Networks can restrict access to the Ethernet port." (McDATA, 2005, Unauthorized Access section, para)

#### Level Two Threats

Level Two threats usually involve internal sources. There are many motives behind these attacks such as a disgruntled employee looking to destroy information or someone looking to gain profit or an advantage from the information obtained.

Preventive measures used against Level One threats can help thwart off Level Two attacks. However, a person who "maliciously tries to steal data or cause disruption of service" (McDATA, 2005, Threat Level section, para. 3) is not only going to look for easily accessible information, but he or she may deceive in order to get that information.

There are numerous ways an intruder can swindle his or her way into getting information under false pretenses. Posing as an authorized user or device could result in gaining access to the SAN. This is also known as spoofing. "The way to prevent spoofing is by challenging the spoofer to give some unique information that only the authorized user should know." (McDATA, 2005, Spoofing section, para. 2). Verifying that the information given is genuine is referred to as authentication. Authentication requirements should not only apply to users, but also to the devices and applications. Authentication should be in place for user access to the management interface, management console access to the fabric, server access to the fabric, and switch access to the fabric.

#### Level Three Threats

It usually requires expensive equipment and a high level of skill to cause a Level Three threat. Even though these types of attacks are rare, they are the most taxing on a storage area network. These types of attacks

are usually from an external source and take a great amount of effort to execute. Therefore, these types of attacks are the hardest to defend against.

As mentioned earlier, using equipment to crack encrypted data would be an example of a Level Three threat. The only way to prevent this threat is take the necessary precautions to avoid data from being stolen. Physical and logical accesses, as discussed before, are crucial aspects that need to be addressed when taking into consideration security for a storage area network. Another example of a Level Three threat would be a Denial of Service attack.

## Security Mechanisms

There are two types of SAN

- ? Fibre Channel SAN
- ? iSCSI – IP SAN

Fibre Channel SAN topology is the high-speed storage option at a top dollar price. And until recently, a Fibre Channel SAN was the only option for networked storage. But with the advent of iSCSI, companies now have another SAN topology, called an IP SAN, which is more cost-effective than Fibre Channel. Though an IP SAN offers slower throughput than a Fibre Channel SAN, dedicated IP SANs running iSCSI are positioned to be the practical and economical alternative for many storage environments. Here we discuss the mechanisms used by SAN administrators Fibre channel & IP SAN

### Fibre Channel SAN security

In the past few years, Fibre Channel SANs have mainly been implemented in data centers, and quite often storage resources on those SANs house mission-critical data. For that reason, security has always been a key focus area for Fibre Channel networking. Fibre Channel SANs use zoning and LUN masking techniques to provide secure access to the storage resources. However, these technologies do not provide media security or encryption of the data at rest.

Zoning– A Fibre Channel SAN fabric consists of multiple elements (disk arrays, switches, host

bus adapters [HBAs], etc.) that enable the hosts to communicate over the Fibre Channel network. Zoning enables configuration of those elements into logical groups, ensuring that only members in those groups can communicate and access the specified storage resources.

There are two methods of zoning: hard zoning and soft zoning. Hard zoning, also referred to as port zoning, determines grouping by port level (i.e., only the host adapter attached to this port can talk to the array attached to this port). This is very effective but is inflexible if the network needs to be reconfigured.

Soft zoning is usually referred to as World Wide Name (WWN) zoning. Each element in a Fibre Channel fabric is identified by its WWN. WWN zoning uses the simple name server (SNS) in the switches to determine which WWN is allowed to communicate in a particular zone. This is a more flexible method of zoning, as zones don't have to be changed if the network is reconfigured. However, WWNs are subject to spoofing, so this is not as secure as port zoning.

LUN masking— Fibre Channel devices present their resources as logical unit numbers (LUNs). LUN masking essentially segments LUNs on a storage resource to specific servers. Masking is used when a number of servers are sharing the same storage resource (an array) but for one reason or another they should not have access to the same disks on that array. For example, say there is a 1TB array on the network, which is to be shared by Unix and NT servers. Because an NT server will assign a signature to any LUN it sees, it is important to mask the Unix LUNs off from the NT servers. With masking, the administrator can determine what LUNs (and thus what data) each server has access to.

Masking can be done from the host, HBA, switch, or storage array, depending on software support and how a user wants to manage masking procedures. HBA and controller-based

masking use a combination of WWN and LUN information to ensure secure access (e.g., only this LUN on this array with this WWN name can be accessed).

Combining zoning and LUN masking does provide a level of security from the perspective of what node should have access to what resources. But LUN masking and zoning do not solve the complete SAN security problem. They also have some drawbacks. Without effective authentication of ongoing traffic, for instance, there is the potential for hijacking. Hijacking occurs when the attacker slips in and takes over after the initial log-in has been authenticated.

### iSCSI – IP SAN security

iSCSI has yet to emerge as a significant storage networking technology for a number of reasons; however, the expectation is that iSCSI implementations will become more popular in the next few years.

The intent is for iSCSI to use the many aspects of IP network security, particularly IPsec. The IPsec standard defines multiple levels of security for transmitting data over the IP network. The key standards in IPsec that iSCSI will take advantage of are Authentication Headers (AH), which authenticate the original connection; Internet Key Exchange (IKE), which is an ongoing mutual authentication process for the duration of the connection; and the Encapsulating Security Protocol (ESP), which encrypts layer 4 and above data (the iSCSI protocol resides at layer 4). This level of protection is only for data in transit; the encryption does not transfer to the data at rest.

In addition, iSCSI transmission over the IP network can take advantage of all other network security measures such as VPNs and firewalls. Still, this is critical information as iSCSI packets contain the actual block location of data, so extra security measures should be considered.

### Multi-functional perspective

Because so many kinds of entities are involved in a SAN, it is useful to approach SAN security from a functional perspective rather than through the entities involved. This means starting with a list of functions that must be

achieved and applying that function list to all the entities rather than attempting to secure each entity separately. One such list of SAN security functions is the "Five A's": Authentication, access, audits, alarms and availability.

Authentication is making sure that only authorized personnel can access the SAN. This is usually implemented with a challenge-response protocol, most often based on userids and passwords. However other methods, such as biometrics, could be used.

Access is making sure that only the appropriate people gain access to the SAN and its information at the appropriate level. Here the technical issues loom larger than they do with authentication, and storage administrators have more control over the situation. The most basic part of access is determining and enforcing who will have access to what information and what privileges they will have with the data and the SAN itself.

Auditing access, configuration changes and user activity are important not only to detect security breaches, but to keep track of changes to the network and trends that may affect network performance. An effective auditing plan would include maintaining logs for access to the SAN, configuration changes and user activity.

Alarms are reactions to the results of the audits. They should vary from a simple, non-intrusive notification of minor incidents to full-blown crisis plans in the event of a major threat. It is especially important to set alarms that identify serious problems without crying wolf. Again, this takes study and planning on the part of the storage administrators. The first step in developing an effective alarm strategy involves determining what constitutes a normal pattern of activity on the SAN. In addition to traffic data, this could include use of administrative tools and making changes to the SAN.

Availability isn't usually considered as part of SAN security, but it has an important relation to it. Availability is primarily an architectural issue and refers to the degree of redundancy, fault tolerance and fail-over built into the SAN. However availability also involves disaster recovery and that is usually seen as part of security. In the security context, availability includes developing and maintaining an effective disaster recovery plan to handle incidents that could shut down the data center or destroy data. Disaster recovery requires careful planning and frequent practice to make sure the plan covers everything and will actually work when things go seriously wrong.

## Methodology

Authentication mechanisms range from a simple userid-password to multi-factor authentication. It depends on the organization to choose a solution considering the organizations size, criticality of the data and feasibility. For larger organizations or financial institutions with highly critical consumer data, out of band multi-factor authentication solutions that use one-time-password (OTP) authentication or etokens could be used. validID, an out-of-band authentication solution provided by ValidSoft - a leading global supplier of Strong Authentication and Transaction Verification solutions. Small and Medium enterprises which cannot afford an solution like validID, can implement a strong and frequently changed userid-password control.

Access control could be applied by the implementing the following controls,

- ? Storage Access Control
- ? Volume Access Control on the Host
- ? Configuration Access Control
- ? Storage Management Software Access Management
  - o Super User Access
- ? Proactive Detection of Access Violations

Hardening of platforms and encrypting passwords, messages and data moving over the SAN are powerful tools for defeating unauthorized access. Most SANs include at least some encryption features, however encryption may involve trading off speed for security. If it does and if encrypting everything at the same level of security imposes unacceptable performance penalties, the

administrator may want to establish an encryption hierarchy. For example passwords would have the strongest encryption protection, with management and administrative messages next and the data itself with the lowest level of protection.

Data Loss Prevention (DLP) solutions provided by Websense, Vontu (Symantec) could also be considered to implement access control depending on affordability.

Auditing should identify both normal and anomalous behavior and include procedures for reacting to violations. Like access control, auditing is usually a matter of inventorying the available tools and applying them effectively. All SANs have audit utilities and additional SAN auditing packages are available from vendors like LogLogic. Results of audit should be used to identify the loop holes which needs to be patched and the devices that need to be upgraded.

Alarms could be generated by either devices like IDS/IPS or log correlation engines. In both the cases, defining normality is an important factor in alarm generation. Here the SAN administrators need to generate a normal pattern and configure the system accordingly. Once 'normality' has been established, the next step is to determine how far the SAN activity should deviate from normal before it becomes cause to issue an alarm. Besides the obvious analysis of variance in the SAN activity parameters, this should include consideration of patterns of business activity and possibly external events. Moreover organizations that are more concerned about their security can implement Security Information and Event Management solutions from vendors like Arcsight, BT Counterpane and E-cop.

Availability could be addressed by taking regular backups of data or through mirroring. Large enterprises could afford to a DR site at a different geographic location or enable one of their branch locations to act as a DR site at the time of emergency. DR site

could also be taken on a leased basis from numerous vendors available in the market.

#### Vendors

Apart from the above specified control mechanisms, SAN security could be addressed by specific SAN security solutions available in the market.

1. McData SANtegrity Security Suite Software
2. Brocade Secure Fabric OS
3. Hifn 4300 HI PP III Storage Security Processor
4. HP StorageWorks Secure Fabric OS
5. Decru Dataform Security Appliances
6. Kasten Chase Assurency

Some of the basic functionalities of these solutions include

- ? Securing the SAN infrastructure from unauthorized / where devices (servers/hosts) can attach.
- ? Ensuring a secure means for distributing fabric wide security and Zoning information (trusted switch).
- ? Protecting sensitive management data against eavesdropping
- ? Creating a trusted SAN infrastructure
- ? Unauthenticated management and device level access.
- ? Sharing resources within the same fabric by tightly controlling

#### Policy Documentation & checklist

Proper documentation is an essential part of any complete security program. Security Policy and an Acceptable Use Policy documents are key references in defining security implementation and enforcement. These documents vary widely between organizations. Some might be quite comprehensive and detailed, while others might outline basic policies. What is important is that the documents be usable and that they enhance overall business effectiveness.

Security policies must provide more value than the cost and difficulty of implementing them. Other useful documents that play important roles in maintaining consistent processes and

supporting existing controls include, but are not limited to these topics:

- ? Change control policies
- ? Testing procedures
- ? Backup procedures
- ? Emergency procedures
- ? Disaster recovery plans
- ? Security incident policy

Other documentation targeting other specific aspects of the enterprise might be necessary. While not all of these processes fit directly under the umbrella of security, they serve to bolster the overall security infrastructure.

### Checklist

As a part of writing policies and documenting them, organizations can develop their own security checklist and use it for auditing purpose. The following checklist provides a broad range of platform-agnostic storage security essentials.

- ? Access controls - determines your policies and changes insecure access permissions (i.e., everyone having full access by default in Windows NT and 2000 and improperly configured NFS exports in UNIX)
- ? Unload unnecessary storage services related to NFS (i.e., mountd, statd, and lockd) if they're not needed and limit network-based permissions for NetWare volumes, Windows shares, etc. to a need-to-know basis from the get-go -- otherwise individual accountability and responsibility are out the window.
- ? Operating system, application and database-centric storage safeguards may not be enough so don't rely on them solely if the utmost in storage security is required. Consider enabling technology and vendor-specific storage controls as well as third-party add-ons if you're

not comfortable with your default setup.

- ? Accountability is another one of those storage security must-haves, so make sure audit logging is taking place where possible and practical.
- ? Most likely, you have bits and pieces (sometimes large chunks) of critical information that may not be adequately protected on workstations, servers and mobile devices (laptops, PDAs, smartphones, etc.) -- root this information out, take an inventory and put it in its place (or at least apply reasonable access controls to it where its currently located).
- ? Encrypting data in transit can help, but it's not everything (see Securing data at rest vs. data in transit), so don't rely on it exclusively.
- ? Use separate accounts for storage administration and maintenance with strong passwords for accountability purposes and to minimize the damage that can be done if a standard user account is compromised.
- ? Physical security is essential -- if that cannot be attained, then trying to reach a reasonable level of digital security is futile.
- ? Consider the various software-based storage encryption solutions for your critical systems (i.e., what NeoScale, Decru -- now NetApp, PGP and others are offering).
- ? Hardware-based drive encryption is coming of age on the client side, which can be a great way to lock things down at the lowest level.
- ? Develop your own internal storage security standards (i.e., encryption requirements, zoning configurations, access control methods, security architecture, etc.).
- ? Documented, maintained and enforced security policies that cover confidentiality, integrity and availability for storage-specific areas (where possible) are a must.
- ? Storage vendors are taking security more seriously and integrating better safeguards into their products (such as NetApp's recent acquisition of Decru) - demand these and use them where possible.

## Business Benefits

Storage security has become one of the hottest issues in IT, as high-profile database breaches and lost data tapes have catapulted the issue off the pages of trade journals and onto the nightly news. Companies report that just a single storage security incident can bring unwanted scrutiny and cost millions of dollars. Moreover from a business perspective, storage security should be evaluated as any other technology. So, first evaluate the critical assets of the corporation. When deciding to invest in technologies to secure those assets, try the following rules of thumb:

1. It should cost (significantly) less to secure an asset than the value of the asset.
2. It should (expectedly) cost more to steal the asset than the asset is worth

Along with other reasons mentioned in this paper, organizations are also being held responsible for the sensitive data they transmit and store with such laws as the Basel II, PCI -DSS, GBLA, Sarbanes-Oxley Act of 2002 and The Health Insurance Portability and Accountability Act of 1996.

## Summary

Storage area networks (SANs) are supposed to make data available to more users more easily, by linking multiple storage devices on a dedicated network. But, as so often happens, the needs for user access bumps up against the need to keep that data secure.

Currently, with most SANs in only limited use, the greatest risk isn't hacking but simple mistakes, such as a Windows and Unix server overwriting the same data. But as more users and administrators share space on SANs, it will become harder to secure the physical devices (such as RAID arrays or tape libraries) and logical resources (such as volumes on disks) within the SAN. Then there is the threat of

spoofing, where a hacker assumes the identity of a user or administrator to break into a storage network.

What follows is a breakdown of the areas of vulnerability and the tools storage managers have now (and can expect) to secure their SANs. These vulnerabilities include the user, the application server/host and the storage administrator.

*The user:* While not strictly part of the storage network, there's always a threat that a user with legitimate access to some data on a SAN could then surf through other data or use administrative tools to open the SAN to others. For now, storage managers have to rely on whatever authentication and access control (such as passwords) is applied at the application or network levels.

*The application server/host:* Again, basic security rules apply, such as updating all patches to the server and doing what you can to "harden" the operating system against attack

*The storage administrator:* With relatively small SAN deployments, many customers can keep SANs on separate networks, managed by consoles protected by locked doors accessible by only a few administrators. But as SANs serve more departments within an organization, more administrators will need various levels of administrative rights to them

The Storage Networking Industry Association (SNIA) [www.snia.org](http://www.snia.org) formed a working group focused on security- Storage Security Industry Forum (SSIF), but it is still a long way from defining effective standards and specifications. "We are trying to coordinate the efforts of the vendors and working with other groups within SNIA to pin down the terminology around security," reports Jim Hughes, the co-chairman of the security group.

Over time the working group hopes to come up with standards and specifications for such aspects of SAN security as authenticating end points to the Fibre Channel fabric and defining how switches will authenticate with each other. It is also working on encryption for data at rest, which refers to data that is stored on tape or disk rather than moving across the network

## References

- 1) The 5 A's of functional SAN security by Rick Cook

[http://searchstorage.techtarget.com/tip/1,289483,sid5\\_gci881954,00.html](http://searchstorage.techtarget.com/tip/1,289483,sid5_gci881954,00.html)

- 2) <http://www.sansecurity.com>
- 3) <http://www.snia.org/forums>

- 4) Time to prepare for SAN security Robert Scheier

[http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185\\_gci1294378,00.html](http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294378,00.html)

- 5) *Why you need (more) storage security* by Nancy Marrone

[http://www.infostor.com/article\\_display/why-you-need-more-storage-security/173322/s-articles/s-infostor/s-volume-7/s-issue-4/s-analyst-view/s-1.html](http://www.infostor.com/article_display/why-you-need-more-storage-security/173322/s-articles/s-infostor/s-volume-7/s-issue-4/s-analyst-view/s-1.html)