Edmira XHAFERRA[1]
Kristel BOZHIQI[1]
Charles RAPOZO[2]

FOCUS "SECURITY" OF STORAGE AREA NETWORK (SAN)

Abstract

The Storage Area Network (SAN) is a space-saving storage technology to manage data securely. The amount of data that needs to be stored is growing, and this is due to the growing number of users of Information Technology all over the world. In this paper we will see what this technology is, the basic components that are involved in its construction, the protocols that are being used, and will address security issues in SAN.SAN, provides storage space management and maintains fast data up. Security has been and remains the top priority for any campaign that works with sensitive information and data, another element should be SANs. The vulnerability assessment is one of the critical requirements to make data storage a system safe. Knowledge about security elements and solutions can help data storage administrators to increase the security level and reliability of networks.

Keywords: *SAN, DAS, NAS, SCSI and FCIP*

1 Faculty of Information Technology, "Aleksander Moisiu" University, Durres, Albania
2 Faculty of Engineering, University of Zimbabwe

1. Introduction

Information and data are essential (vital for any company, business or ordinary customer today. It seems that the demand for information storage increases almost twice as much as the growth of storage capacities. Moreover, we have a situation where this capacity can not to grow sensibly. The traditional way of storing information is using a server, each containing its storage and these storage spaces are accessible directly from the server and can't be shared with other servers, this is called Direct Attached Storage (DAS). Powerful companies that need more storage space will use not one but some servers and each has its own space to store it. management and the second part of the memory that was left unused to any server was very difficult to be exploited by the servers Creating a common storage space that can be accessed by all servers, and here we refer not only to a collection of hard drives but to some processes that govern how storage is accessible from the server. This type of storage space is called Networked Storage.

2. Technology DAS, SAN, NAS

There are three main technologies that share storage in the Direct Attached Storage (DAS), Storage Area Network (SAN) and Network Attached Storage (NAS) network. Let's look at their physical connections with servers to better understand the differences between them.

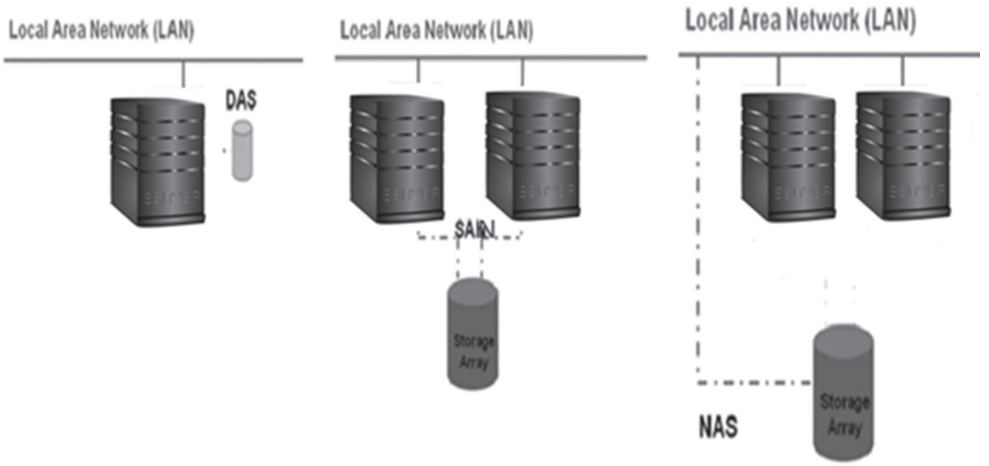

Figure 1. Technology DAS, SAN and NAS

Direct Attached Storage (DAS) is a dedicated disk that connects directly to the server, and uses the "point to point" link to the server. In fact, point to point connectivity is the simplest way of communication that exists in information retention systems. Access to data storage in DAS is done directly through the server. The disadvantage is that if the server is closed or shut down, applications and users working in DAS do not have access to this data. DAS can be a good solution for small companies as data storage management becomes more difficult with increased data storage volume.

Network Attached Storages (NAS) is defined as one or several Hard Disks together connected to the network. NAS is the storage of data that is connected to a shared network and is directly accessible over the local area network (LAN) from any of the users or servers that are attached to the network and functions as a file server that stores and shares network data. The main function of NAS is to share network files so send or receive via TCP / IP protocols.

NAS uses different protocols for different operating systems, which are: Network File System (NFS) belonging to the Unix operating system and Common Internet File System (CIFS) used for the Windows operating system.

Usage of files on NAS is done over local network speed (LAN) and file access sometimes becomes impossible from delays or network barriers. So because of the needs of companies to use better performance devices and to transfer larger amounts of data such as the appearance of movies or online transactions, it was downloaded from the NAS to SAN, which is compatible with MAC, Unix and Linux windows.

Storage Area Network (SAN) if we refer to Figures 1, it is defined as a network consisting of several computers, servers and devices that are interconnected to one another. This infrastructure allows different devices to communicate with one another.

SAN is one of the data storage technologies currently used in different network sizes for storing and accessing data at greater and more reliable speeds. The operation of each network storage area is based on the basic communication elements that manages physical connections, management layers for possible connection organization, computer system, and devices for safe and reliable data storage. The SAN manages the data at the block level, so it's not at the file level for tracing and distributing free disk space to the data. SANs are also used to make a high-speed connection between storage and servers.

Various SAN servers can use different operating systems such as Windows, Unix, and Linux. With the help of various communication techniques and communication protocols such as iSCSI and FCIP, SAN allows storage and storage of data at long-range high speeds.

3. SAN components

SAN members such as servers and network clients need access to the same data at the same time. The file system is the technology used to access multiple servers for the same data at the same time in the SAN.

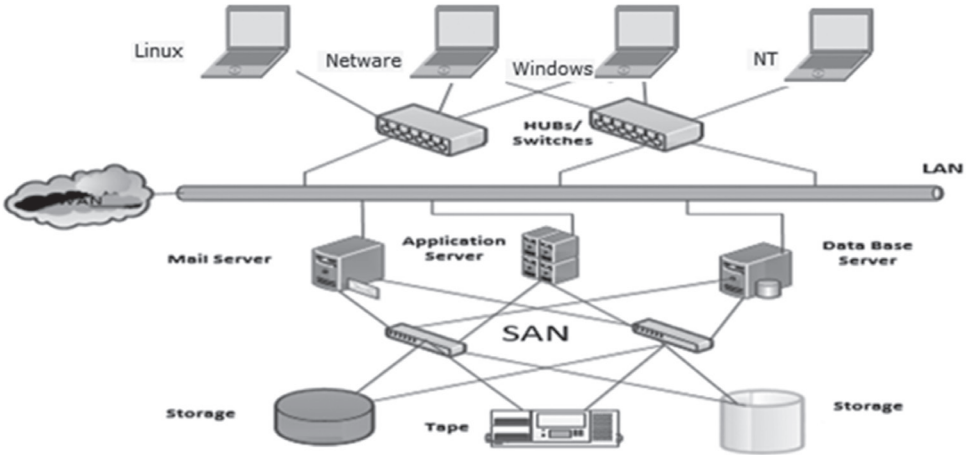

Figure 2. SAN components

Any storage device that connects to a server or computer can not do anything alone, so the file system connects between the drive blocks and the operating system that is available to modify or create and modify any disk file. Each file system has the information table about the status of the disk blocks for managing and sharing the disk blocks.

If a node in a network fails or has a functional problem, other nodes on the network can continue accessing the data blocks without any problems.

4. Storage Area Network security issues

Maintaining and availability of data is an important issue in the IT world today. To increase the level of security in the SAN we have to verify the security risks and weaknesses in maintaining data and communication between SAN elements in order to take measures to increase security. The methods of access control in SAN are:

Authentication, which is used to identify the person, software, and hardware that should have permission to use the system. Most people working in storage sites feel that security exists in another network area and that there is no need

to worry about security features in new storage technologies such as SANs. Authentication does not exist naturally in SAN, but exists through some other applications such as SAN management programs and applications that have access to SAN control. Certain identification models such as Diffie-Hellman-Chalenge Handshake Protocol (DH-CHAP), Fiber Channel Authentication Protocol (FCAP) and Fiber Channel Security Protocol (FCSP) provide security for different types of connections such as switch-to-switch connections, node-to-node and node-to-switch connection.

Authorization, which is used to verify the access level to the device in a SAN and is provided by the WWN of the node or gate known as WWNN and WWPN.

Encryption, which does not exist on most data storage devices but is provided using some third-party apps, but there is generally no encryption method from layer 0 to layer 4 in FC.

Availability, where availability control of the equipment is the same as Quolity of Service QoS and exists in the second layer of FC known as the frame error path. Availability and ability to detect and control errors is one of the essential tasks for implementing a SAN.

5. Possible solutions for securing data in SANs

Data to be protected are divided into two groups:

1. Data In Fly DIF
2. Data At Rest DAR

In flight data, we mention data and information transmitted as packets from source to target. The Protocol Data Unit (PDU) protects the data during transmission and is known as the data security in the flight. Break data is also known as maintaining secure data on disks like encrypting stored data or secure application and accessing data stored on disks. Regardless of data sharing, where data was shared as Data In Fly and Data At Rest, the security of these data consists of two main components that are:

1. Confidentiality of data
2. Integrity of data

Confidentiality of data is recognized as a guarantee for information regarding access by unauthorized persons to these data, while data integrity has the responsibility of data security guarantee not to apply any change or corruption after retention of data in disk. Securing data in the SAN can be made possible

based on a logical security split that takes place in two directions:

- Provision of physical equipment consisting of SAN (factory-level security)
- Providing Data

Provision of physical hardware is based on several components: Fiber Channel Authentication Protocol (FCAP), fiber channel zoning, masking of logical unit, port connection, etc.

5.1 Data Encryption

Data encryption is one of the simplest ways to secure data. Regardless of whether the data is stolen, lost or secured in some way, they can not be read without the correct encryption key. Data encryption has been used to exchange information safely and securely for many centuries. It transforms data that is unprotected into encrypted data using a keystroke and is difficult to break and return to comprehensible text without the help of this browser.

The two most important types of encryption are:

1. Symmetric encryption
2. Asymmetric Encryption

In symmetric encryption, the same secret or password that is used to encrypt a message decrypts the encrypted corresponding text. This algorithm is the simplest and the most efficient way to implement a secure communication.

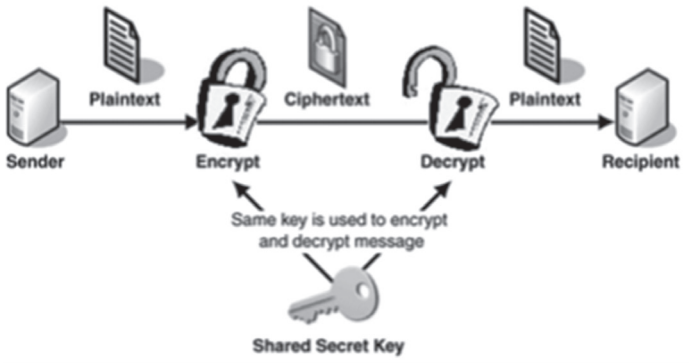

Figure 3. Symmetric Data Encryption

In a non-encrypted encryption a key is used to encrypt a message, and another key is used to decrypt encrypted encrypted text. Asymmetric encryption is also known as “public-key encryption”

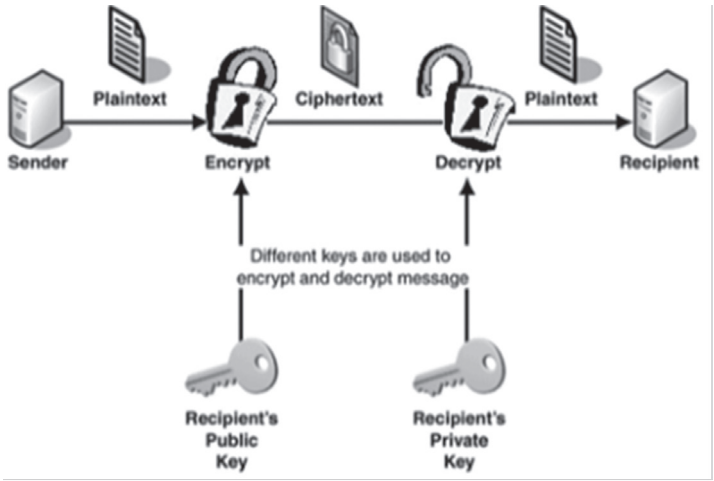

Figure 4. Non-metric data encryption

Some encryption algorithms that are even more popular nowadays are:

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Diffie-Hellman
- Triple Data Encryption Standard (3DES)

The main methods used as standard for data security are: Fiber Channel Password Authentication Protocol (FCPAP), Diffie Hellman - Challenge Handshake Authenticaton Protocol (DH-CHAP) and Fiber Channel Security (FC Sec).

5.2 Security solutions in iSCSI SAN

Authentication, authorization, and encryption are the three basic security elements in the SAN. Authentication on iSCSI SAN is provided using the Challenge Hand Shake Protocol (CHAP). For authorization control, SAN uses the name of the initiating node. Encryption uses IP Sec and Secure Socket Layer (SSL). Most SAN vendors believe that SAN is not a tangible technology because it works on Gigabit Ethernet infrastructure and is also a point-to-point technology, so attackers are not capable of hacking and hacking SANs and this occurs only if they have physical access to the SAN equipment.

iSCSI SAN has basic identification elements such as iSCSI Qualified Name (IQN), LUN, and iSCSI Simple Name Services (iSNS) server. IQN is an iSCSI initiating client identifier that acts as a MAC address in the Network Interface Card (NIC). The only authorization method available to iSCSI SAN is IQN

that is not a secure method. They are a fake and can not be a good method of authorization.

LUN is a logical part of storage devices. Each information storage device is divided into several LUNs where each LUN functions as a logical disk partition on the computer desktop. ISCSI works on the TCP 3260 port. The ISNS server is located on any iSCSI device or operating system. Each iSCSI or target initiator is registered on the ISNS server. ISNS is responsible for informing customers about available iSCSI networking equipment and customer information for various security settings that are used in SAN for communication with targets. The ISNS server works on the TCP 3205 port.

6. Conclusions

The SAN architecture is built to make the connection between servers and shared storage fast, reliable, easy, and secure.

Networking Components: The SAN can be built based on the use of fiber optics or Gigabit Ethernet according to the SAN architecture and the connection protocol. Other SAN components are hubs, connectors, switches, and routers.

Data storage systems do not have any security features, and this lack of security makes storage more vulnerable to various attacks. The best way to have SAN security is the combination of authentication, authorization, and data encryption. The result also shows that the most vulnerable part of security in the storage space are internal people, who are people who have access to information storage devices and their management consoles.

Security solutions in iSCSI SAN consist of different authentication methods such as DH-CHAP, RADIUS server and Kerberos v5. The best result is when combining these authentication methods with an encryption method like IP Sec. There are several specific security solutions in the FC SAN such as zoning (strong or soft zoning), LUN masking, and gateway connectivity.

It’s the security, the performance and the seriousness that make SAN a good choice for data retention on networks.

Reference

1. T. Clark, designing storage area network, second edition. Addison wesley, 2003.
2. C. Brooks, H. Dachuan, D.jackson, M. A.miller, and M. Rosichini, IBM total storage SAN filesystem, Fourth edition. IBM, 2006.
3. H. Dwivedi, Securing storage: A practical guide to SAN and NAS security, First edition. 2012.
4. Ofj\sc [11] EMC best practice for performance and availability of storages, Whitepaper, Corporate Headquarters, march 2011, http:/ / www.emc.com.
5. iSCSI vs. fibre channel explained , fibre channel takes rightful place beside fibre channel, S.J.Bigelow, 13 July 2007, http:/ / www.cuttedge.com.
6. Network work research centre, TCP offload engine (TOE), network buzz issue, 2009, http:/ / www.networkworld.com/ .
7. Open filer information and configuration, G.Porter, December 2010, http:/ / greg.porter.name/ wiki/
8. ISCSI Security (Insecure SCSI), H.Dwivedi, Fall 2005, https:/ / www. blackhat.com/ .
9. iSCSI vs. FC SANs ,three reasons not choose sides, position paper, November 2010, http:/ / www.davenportgroup.com/
10. Storage performance, R. Lucchsi, 2008 , Network Industry Association (SNIA), www.snia.org.