StorageWorks SAN by Compaq

Application Note -
SAN Security Overview

Part Number: AA-RQ6BA-TE

First Edition (October 2001)

Product Version: 1.0

Storage Area Networks are used to hold data in enterprise environments, where information security is a fundamental requirement. StoreageWorks SAN by Compaq products support information security by incorporating a set of technologies that control access to both the data stored in the SAN and the management interfaces to the SAN components. By using these products as summarized in this application note, the storage system manager can maximize the availability, integrity, and confidentiality of the data stored in StorageWorks SAN by Compaq storage systems.

For the latest version of this Application Note and other StorageWorks SAN by Compaq documentation, visit the Compaq storage website at:

http://www.compaq.com/san

COMPAQ

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Application Note - SAN Security Overview
First Edition (October 2001)
Part Number: AA-RQ6BA-TE

Application Note Contents

This application note covers the following topics:

- Introduction
- Summary of SAN Security Practices
    - — Table 1, How to Use SAN Security Features
- Security Features of StorageWorks SAN by Compaq Components
    - — 10/100 Ethernet
    - — Serial Line
    - — Host Bus Adapter
    - — Fibre Channel Switch
    - — Storage System
    - — StorageWorks Command Console Management Software
    - — SANworks SAN Management Appliance
- Conclusion

Intended Audience

This document is intended for customers who are considering security issues in the StorageWorks SAN by Compaq.

Introduction

Information security is a fundamental issue that must be dealt with while managing any data center. Compaq understands the importance and complexity of establishing and maintaining a secure information storage environment, and Compaq storage products are designed to make it easy to protect the availability, integrity, and confidentiality of the customer data that they hold.

This application note summarizes the data security features of StorageWorks SAN by Compaq products.

Refer to the *StorageWorks Heterogeneous Open SAN Design Reference Guide* (Second Edition, July 2001, Part Number AA-RMPNC-TE), available at:

http://www.compaq.com/products/storageworks/san/documentation.html

for additional information on this topic and on many related storage configuration topics.

Summary of SAN Security Practices

StorageWorks SAN by Compaq hardware and software components incorporate features that can be used to implement a secure data storage system. The following table shows the appropriate use of these security features in various environments.

Table 1: How to Use SAN Security Features

SAN Storage Security Feature	Departmental Storage System	Enterprise Storage System	Service Provider Storage System
Physical security of SAN environment.	Suggested. All personnel are employees.	Suggested. All personnel are employees.	Essential. Many personnel are competitors.
Controlled physical access to switch management using Front Panel Controls.	Suggested. Reduces risk of accidental problems.	Suggested. Reduces risk of accidental problems.	Optional. Switches are to be kept in a secure area.
Password protection on switch management using Telnet via in-band or out-of-band connections.	Essential. Avoid potential of remote access attempts over your network.	Essential. Avoid potential of remote access attempts over your network.	Essential. Avoid potential of remote access attempts over your network.
Disable switch management using SNMP via in-band or out-of-band connections.	Optional. SNMP is useful for system management, and SNMP only allows monitoring of system.	Optional. SNMP is useful for system management, and SNMP only allows monitoring of system.	Essential. Disable by use of license management on switch.
Disable switch management using SCSI Enclosure Services (SES) via in-band connections.	Optional. This tool is useful for system management.	Suggested. This tool is useful for system management, but it increases the inter-departmental risk.	Essential. Disable SES by use of license management on switch.
Disable web browser management interface.	Optional. Password protected.	Optional. Password protected.	Essential. Disable by use of license management on switch.

Table 1: How to Use SAN Security Features (Continued)

SAN Storage Security Feature	Departmental Storage System	Enterprise Storage System	Service Provider Storage System
Use of zones.	Optional. Use soft or hard zoning as required to manage Operating System conflicts.	Optional. Use soft or hard zoning as required to manage Operating System conflicts.	Optional. Use hard zoning as required to manage Operating System conflicts.
Use of SSP.	Essential. Use as required to manage access to data	Essential. Use as required to manage access to data	Essential. Use as required to manage access to data.
Controlled access to storage system management using serial line interface.	Optional. Risk from local access is low.	Suggested. Limit physical access to machine room.	Optional. Storage systems are physically secure in this environment.
Controlled access to storage system management using in-band interface.	Optional.	Optional.	Optional.
Restricted use of multiple switches.	Optional. No additional risk is added.	Optional. No additional risk is added.	Optional. No additional risk is added.
Restricted use of multiple storage systems.	Optional.	Optional.	Essential. Each customer must be located on a different HSG80 controller pair.
Restricted use of Management Appliance.	Optional. Appliance applications are password protected.	Optional. Appliance applications are password protected.	Optional. Appliance applications are password protected.
Use of logical unit visibility control on Modular Data Router tape controller.	Essential. Use as required to manage access to data.	Essential. Use as required to manage access to data.	Essential. Use as required to manage access to data.
Event logging enabled.	Essential. Needed to track possible intrusion attempts.	Essential. Needed to track possible intrusion attempts.	Essential. Needed to track possible intrusion attempts.

Security Features of StorageWorks SAN by Compaq Components

The components of a StorageWorks SAN by Compaq are shown in Figure 1.

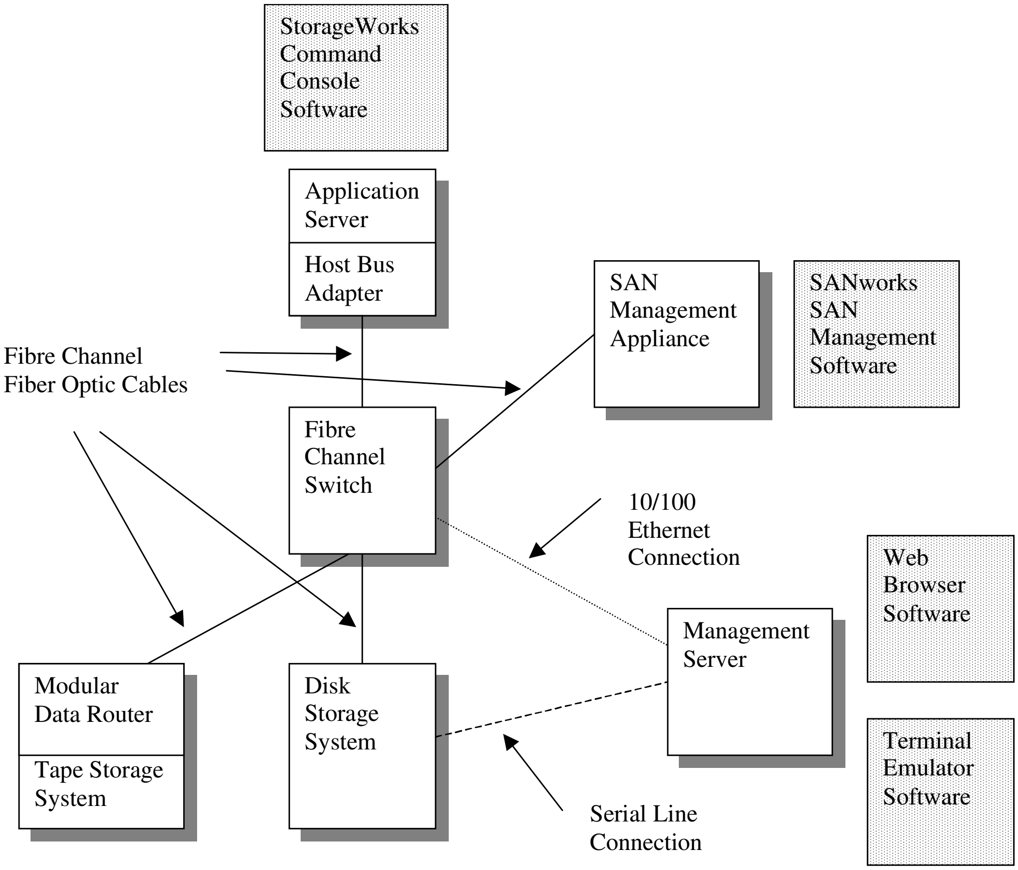

Figure 1: SAN Components

10/100 Ethernet

Because of the difficulty of securing a distributed system, the security of IP LANs is low. The system manager should verify that good passwords are in use on all the SAN components that are connected to a LAN, including the application servers, the SAN management appliance, the management server, and the Fibre Channel switches.

Serial Line

Serial line interfaces are used to connect a terminal (with its associated keyboard and display) to a server or other SAN component. The serial line protocol itself does not have any provision for access security.

The system manager should verify that good passwords are in use on all the SAN components that have serial line connections, or that these connection points are in a secure area.

Host Bus Adapter

The host bus adapter (HBA) is the basic interface between the SAN and each server. The microcode in an HBA can be changed by using a utility program. In the case of Windows NT, a microcode load can be done on an active system, and the server does not need to be re-booted to resume normal I/O activity. A new host bus adapter may be installed in an operational server.

In Fibre Channel there is no equivalent functionality to the “promiscuous” mode of operation that historically could be used on 10 Mbps CSMA/CD Ethernet networks. The security risk associated with HBAs in a Fibre Channel environment is low because the switches filter all traffic. Only traffic intended for a given server is communicated between the switch and that server’s HBAs.

If the operating system driver is changed, then the system must be rebooted. This minimizes the likelihood of undetected changes to driver software.

Fibre Channel Switch

Fibre Channel switches are connected together to form a SAN fabric. The switches are the foundation of the SAN system.

Switch Management Interfaces

The Fibre Channel switches in a Compaq Storage Area Network support several management interfaces. The interfaces and their security aspects are shown in the following table.

Table 2: SAN Switch Management Interface Security

Management Interface	Security Control Method
Front Panel Controls.	Interface supports only basic performance features, not data access management.
Telnet via in-band or out-of-band connections.	Password with several levels of access control.
SNMP via in-band or out-of-band connections, limited management capability.	Interface supports only monitoring and traps.
SCSI Enclosure Services (SES) via in-band connections.	Requires license to enable, physical security required.
Web browser via in-band or out-of-band connections.	Requires license to enable, password protected.

To maximize security in a SAN fabric, the system manager should verify that the switches are in a secure area, and that the SES management interface is disabled.

Switch Zones

The switches in a fabric cooperate to enforce data access zones. Servers are identified either by the switch port to which they are connected, or by their WWID. These two methods are called “hard zoning” and “soft zoning”, respectively.

The advantage of hard zoning is that it is enforced on a port-by-port basis by the switches in the fabric. The disadvantage is that if a server is moved from one port to another, the zone configuration must be changed to reflect the new connection topology. The advantage of soft zoning is that it is independent of port, so servers may be moved from one port to another without changing the zone settings. The disadvantage is that an HBA in a server could, at least theoretically, take on the WWID of another HBA and thus gain unauthorized access to the wrong zone.

The purpose of zones is to manage the interaction of servers in a SAN in order to prevent interference between the operating system drivers. In heterogeneous configurations the drivers may interfere with each other, and in homogeneous operating system environments the capacity of certain driver data tables may be exceeded. Zoning is used to manage these operational factors.

By properly configuring the zones in a SAN fabric, the system manager is able to control the access of servers to storage systems. It is not necessary to use a different fabric for each server or application.

Storage System

Products in the Compaq HSG series of RAID storage systems incorporate security controls on all the interfaces to the storage system.

Each storage system consists of a pair of HSG controllers, along with assorted supporting hardware.[1] The storage system is connected to one or more servers, and presents logical disks to those servers. Each logical disk has a logical unit number (LUN).

The Selective Storage Presentation (SSP) feature allows visibility of logical units to be restricted to a subset of the servers connected to the storage system.

Controller Management

Basic control of the storage system is performed using various buttons and lights on the front and rear panels of the RAID controller shelf. These controls allow the controllers to be halted or restarted. The controller microcode is stored on PCMCIA cards that are inserted into these panels.

One option for initial setup of the storage system as well as for ongoing operation is to use a serial line connection to each RAID controller. This connection is typically made between a controller and a terminal emulator program running on a nearby computer. All storage system management operations can be done using this interface. Physical access to the controller shelf must be maintained to avoid unauthorized use of this interface.

Another option for the initial setup and ongoing operation of the storage system is to use the in-band Fibre Channel management system. This system sends SCSI commands to logical units on the storage system to control the logical unit definitions and the SSP settings.

Data Access Control

The SSP feature of the storage system is the method used to control access to user data. Access is allowed to each logical unit by one or more servers.

The SSP settings may be controlled by any server having access to any logical unit on the storage system. This includes the SWCC agent, and the SAN Management Appliance, and could include a purpose-built intrusion application running on a server connected to the SAN. If a computing environment has multiple security domains then the domains must not coexist on a single storage system.

For example, consider the configuration shown in the following figure. Server A and Server B have access to logical unit D and logical unit E respectively. Server A and logical unit D are in one security domain, and Server B and logical unit E are in a separate security domain. Since both have access to Storage System C, then Server A may change the SSP settings to prevent Server B from accessing any logical units on the storage system.

[1] Refer to the HSG80 documentation for a complete description of the features of the Compaq family of storage systems.

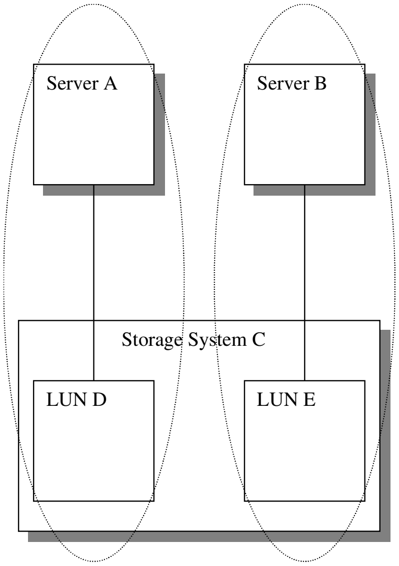

Figure 2: Multiple Security Domains on One Storage System

StorageWorks Command Console Management Software

StorageWorks Command Console (SWCC) is a client-server storage management software product that supports in-band management of Compaq storage systems. An agent program runs on a server and communicates with any storage system attached to that server. The SWCC client program runs on a second, remote server to provide the GUI. The two servers communicate by using a TCP/IP connection between the two servers.

The Command Scripter tool also uses the SWCC agent to communicate with storage systems.

User access to the SWCC agent is controlled by a username and password. Any SWCC client accessing the agent to perform management tasks will be asked for this password. The communications between the management station and the host servers connected to the storage controllers is protected by single-use key encryption. Also, remote configuration can be disabled.

Communication between the agent and the controller is done by using SCSI commands on the Fibre Channel connection between the server and the controller. The agent communicates with a logical unit on the controller.

SANworks SAN Management Appliance

Compaq offers an optional integrated SAN management system that uses an appliance connected to the Fibre Channel fabric. The SANworks SAN Management Appliance hosts web-based Open SAN Storage Management software. This software provides a wide variety of management tools.

Access to the Open SAN Management applications is controlled by a username and password method that uses the WEBM security model.

Conclusion

Compaq StorageWorks SAN products can be configured to provide a secure information storage environment. By using the guidelines suggested above, and by referring to the detailed information in the *StorageWorks Heterogeneous Open SAN Design Reference Guide* and in the product documentation, a system manager can insure that the highest possible level of data availability, integrity, and confidentiality is maintained.