



STORAGE AREA NETWORK

Technical Brief: Connecting Servers in a DMZ to a Fibre Channel SAN

A server connected to a Storage Area Network (SAN) can potentially see all of the connected storage devices and servers. This paper explores techniques for the secure configuration of a SAN with a Demilitarized Zone (DMZ).

BROCADE

CONTENTS

Introduction 3

Securing the Management Interfaces 3

Securing the Servers in the DMZ..... 4

Securing the Storage Devices..... 5

 Port Disable, Disable E_PORTS, Port ACLs..... 5

 Zoning..... 5

 LUN Masking..... 5

 Virtual Fabrics 6

Authentication of Servers..... 6

Use Case Scenarios 6

Auditing your SAN10

Best Practices.....10

Summary.....10

INTRODUCTION

A Demilitarized Zone (DMZ) is the part of the network that sits between the internal private network and the external network or Internet. The DMZ also acts as a buffer between the inside and outside networks where applications, such as e-mail, FTP, and web servers exchange information between both networks. This buffer is critical to preventing potential attackers from the outside network (the Internet) to communicate directly with any of the internal systems.

A separate network from the Local Area Network (LAN), a Storage Area Network (SAN) is used to exchange information between servers and storage devices, such as disk arrays and tape devices. SANs are currently implemented in the data center using two protocols: Fibre Channel (FC) and iSCSI. This paper focuses on FC SANs.

From a security perspective, there are critical concerns with connecting servers located in a DMZ, which are accessible from the Internet, to storage devices via a SAN. What are the risks involved with using a SAN with a DMZ and can the entire SAN be compromised by an outside attacker? Can this ever be done safely?

There are certainly risks involved in having a SAN in a DMZ, but with proper design and configuration it can be done with a high degree of safety. There are vulnerable SAN components, which must be properly secured before attempting this. It is important to note at this point that security is not always for preventing criminal activities originating from outside the bounds of the data center; it is also prudent to use various security measures to prevent unauthorized internal breaches and to prevent the impact of human error beyond a fixed scope.

A server that is connected to a SAN potentially can see all of the storage devices and servers connected to the SAN unless proper measures are taken to prevent it. This paper describes several techniques you can safely deploy to accomplish the secure configuration of a SAN with a DMZ.

NOTE: Brocade has created a detailed white paper on SAN security, "The Growing Need for Security in Storage Area Networks." Refer to this document for a more in-depth discussion of security in the SAN. (http://www.brocade.com/san/pdf/whitepapers/Growing_Need_for_SAN_Security_WP_01.pdf)

SECURING THE MANAGEMENT INTERFACES

Every FC switch or director has an Ethernet port used as a primary management interface. Switches are usually managed using a Command Line Interface (CLI) or a Graphical User Interface (GUI) via the Ethernet port using an IP address. It is extremely important to ensure that management interfaces are located on a network segment that is isolated from the Internet and, if necessary, the production network as well. The switch management interfaces should never be accessible from the Internet, at least not without a secure VPN (Virtual Private Network). This can be implemented in several ways using a one or more of the following technologies:

- A separate physical network
- Non-routable subnets
- Virtual LANs (VLANs), typically, a private VLAN
- Access Control Lists (ACL)
- Policy-Based Routing (PBR)
- Firewalls (implementing a VPN)

The management interfaces should also be used in conjunction with secure protocols such as SSH, SSL (HTTPS, SCP, SFTP), and SNMPv3. Conventional protocols such as telnet, HTTP, and SNMPv1/v2 exchange data in standard readable format and should be disabled once the secure protocols are configured. Information such as passwords and user IDs can easily be captured using network sniffing tools. Secure protocols such as SSH and SSL use encryption algorithms to protect unauthorized viewing of data, including passwords and user IDs.

User accounts and passwords are the first line of defense for a network device's management interface and are an important component in preventing unauthorized access. Assign separate accounts to each individual administrator who has access to the switches instead of a shared account among all or some administrators. Role Based Access Control (RBAC) is a feature that allows specific administrators specific rights under their user account on the network or a particular device.

The factory default passwords for all default accounts must be changed before a network device goes into production. This is usually done during the initial switch configuration. Companies should have policies requiring strong passwords and the periodic changing of those passwords. This includes:

- Forcing at least eight characters
- Using a combination of alphabetic, numeric and special characters
- Preventing the use of repeating characters and sequences
- Configuring a password expiration time for the number of unsuccessful login attempts, after which accounts are disabled

To simplify password management, create a single place to administer user names and passwords for all users and devices in large environments. Remote Authentication Dial In User Service (RADIUS) is such a tool. RADIUS provides a simple, centralized application to enable or disable user accounts and change passwords for all switches in a SAN.

SECURING THE SERVERS IN THE DMZ

The servers in the DMZ must also be secured using conventional security techniques such as firewalls, anti-virus software, and other methods. If a server in a DMZ is compromised and an attacker manages to gain control of the server, the attacker can access the storage devices attached to that server via the SAN. Since these servers are connected to the internal network, the internal network is now at risk of attack from a compromised server. Firewalls are commonly deployed to provide a barrier protecting the internal network.

Can an attacker use this system as a stepping stone into other storage devices and servers on the SAN? This is one of the greatest concerns expressed by security personnel when deciding whether a server in a DMZ should be connected to a SAN. Several methods that prevent attackers from using a server in a DMZ to gain access to other servers or devices connected to the SAN are discussed in the next section.

SECURING THE STORAGE DEVICES

There are several common techniques to prevent a server from being able to see or access storage that is not explicitly assigned to it.

Port Disable, Disable E_PORTS, Port ACLs

The initial step for controlling FC traffic and communication is to persistently disable any unused ports and persistently disable E_Ports on unused ports and host/storage ports. This prevents an unused port from having an unauthorized host attached and a host or storage port from being used to attach an unauthorized switch. Use port ACLs to lock a particular host or storage port to a port on the SAN switch. This prevents an unauthorized host from being attached to a port that is being used for an authorized host. While these port control methods add management steps to the configuration procedure for a DMZ switch, they significantly increase the security of the switch and impose very clear change control so the DMZ SAN does not have unexplained topology changes.

Zoning

The second technique, zoning, is implemented within an FC fabric. Zoning allows devices such as servers, disks, and tape drives to be grouped together and isolated from other devices. Devices can communicate only if they are within the same zone (though a device can be in multiple zones, which maximizes configuration flexibility). All SAN switches and directors are capable of hardware-enforced zoning, in which an ASIC allows or disallows devices to communicate as defined by the zoning configuration. Hardware enforcement is always done on Brocade switches if all zone identification in a zone configuration is D,P (port zoning) or pWWN (port WWN zoning). Mixing identification methods in a zone configuration can cause some of the zone enforcement to be the less secure Name Server enforcement. Brocade recommends using all pWWN when zoning to ensure that all zones are hardware enforced and to enable some advanced Brocade features such as Fibre Channel Routing.

LUN Masking

The third technique, LUN masking, can be implemented in the Host Bus Adapter (HBA) or in the disk controller. This technique is used to assign a specific LUN to a specific pWWN in the SAN. No other server will be able to see or access that LUN unless multiple LUN masking mappings are configured, typically on the storage subsystem. LUN masking is less effective if it is configured only on the server, because the masking can be disabled if the server is compromised. A server breach is more likely than a storage subsystem breach.

Virtual Fabrics

Finally, Virtual Fabrics (VF) are used to logically group switches, switch ports, and device pWWNs that should be managed separately from other components of the fabric in a physical fabric. Zoning groups devices that can communicate with each other compared to Virtual Fabrics, which group devices into managed units that each appear to be a SAN fabric. For example, you may want to create a Virtual Fabric to allow the UNIX environment to be managed separately from the Windows environment. You can assign privileges to a SAN administrator to manage the UNIX environment and different privileges to another SAN administrator to manage the Windows environment. The UNIX VF administrator cannot access or disrupt the devices in the Windows VF and vice-versa. Also, any changes made to the UNIX VF will not impact the Windows VF as long as each VF contains only switch ports and pWWN for devices.

AUTHENTICATION OF SERVERS

To further enhance security, use strong authentication mechanisms to authenticate servers joining a fabric. The ANSI T11 Technical Committee for FC has a standard in the approval phase that defines the use of an authentication protocol to authenticate end devices to switches. This protocol, Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) uses a public key cryptography to ensure that the pWWN of the HBA joining the fabric has not been spoofed and is in fact genuine. The pWWN on an HBA can usually be changed using tools provided by HBA manufacturers and it would be possible for someone to configure the HBA on a server to have the same pWWN as another server on the SAN. Use DH-CHAP and Port ACLs (discussed above) to prevent spoofing of a server HBA's pWWN.

USE CASE SCENARIOS

Another method to protect the production SAN is to simply use a separate physical SAN dedicated for the DMZ. A separate switch or director could be used to connect all servers within the DMZ. Storage devices could have dedicated ports attached to this switch or you could dedicate entire storage devices to the DMZ servers. This is probably the most secure solution but it requires dedicated hardware and decreases the level of storage centralization.

The following diagrams illustrate both improper and proper methods of connecting servers in a DMZ to a SAN.

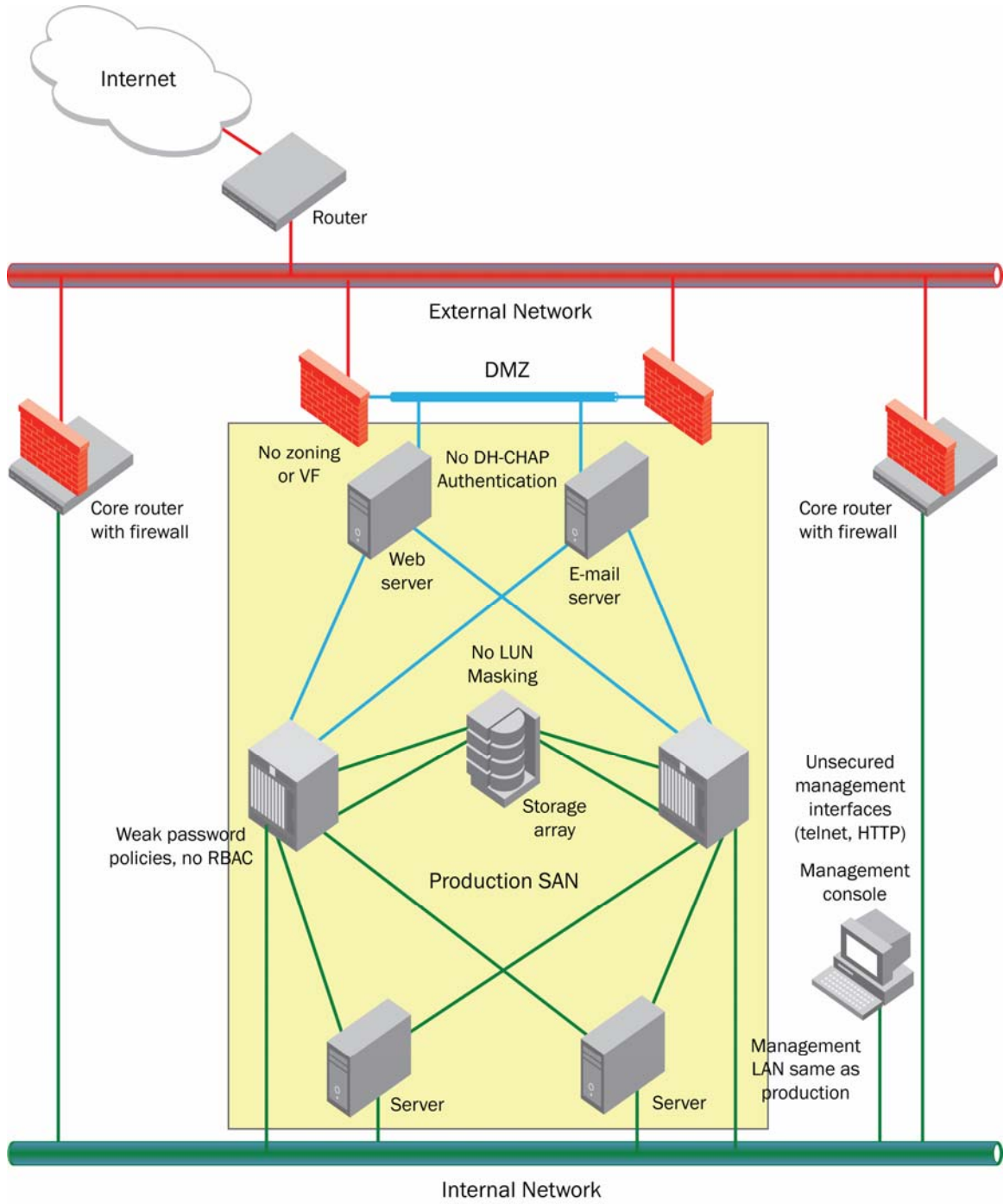


Figure 1. Improper method of connecting servers in a DMZ to a SAN

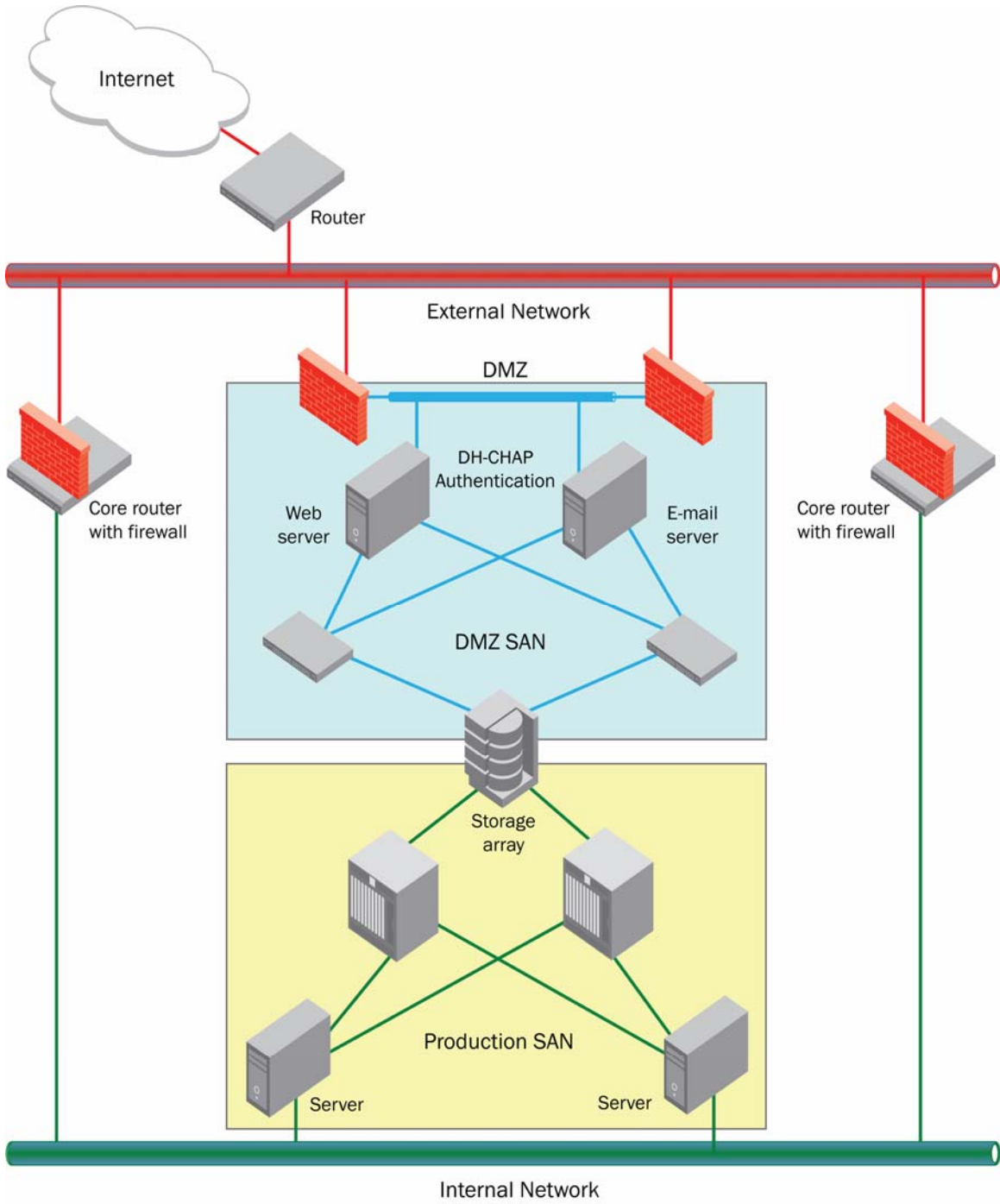


Figure 2. Separate physical SAN

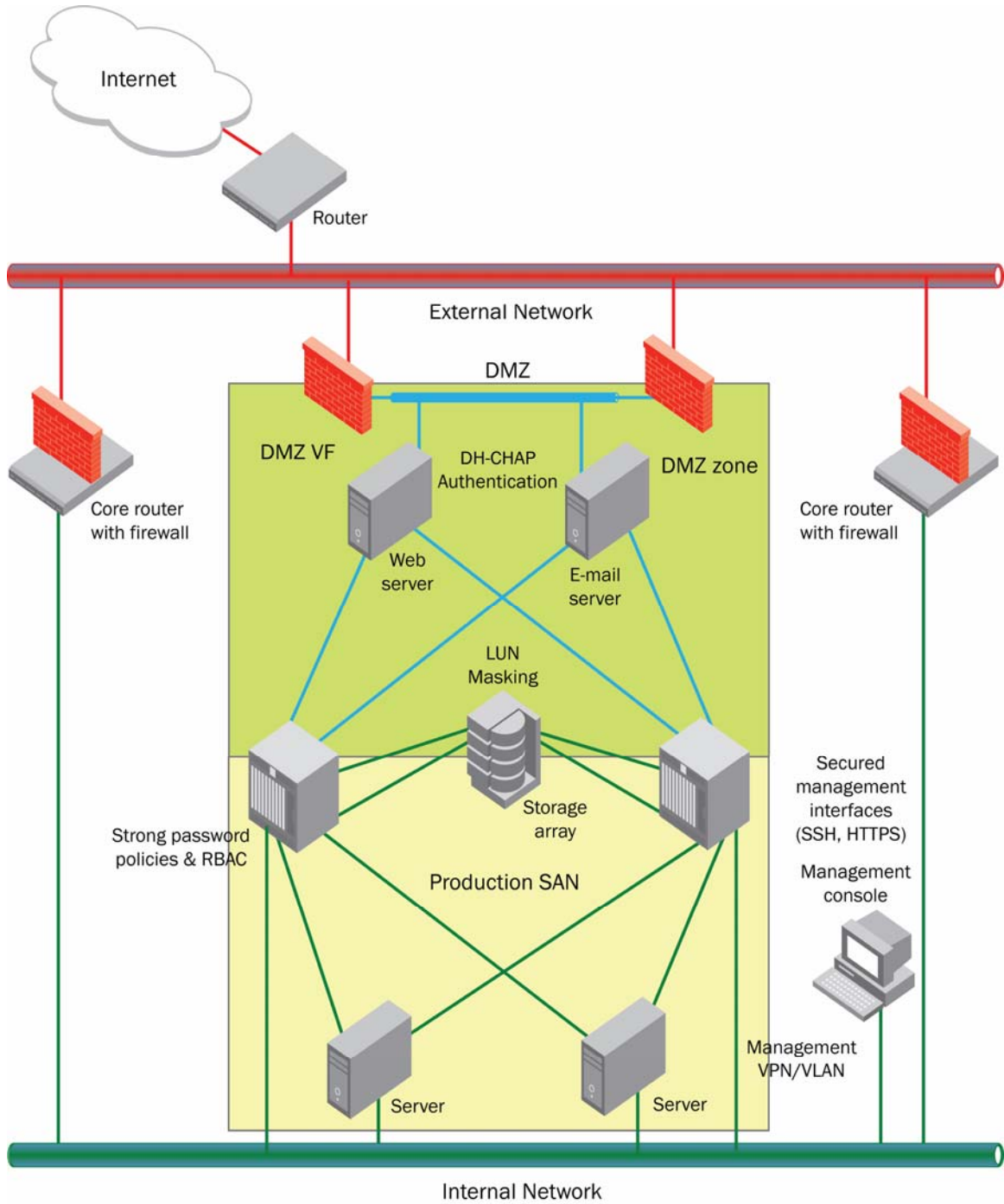


Figure 3. DMZ connected to a production SAN

AUDITING YOUR SAN

Network security has become more public and is often foremost in an IT manager's concerns. Most companies perform security audits on their networks on a regular basis but SANs are often overlooked. It is important to perform a SAN audit as well to ensure the protection of centralized data. SAN security audits should go beyond the technological components and include a review of SAN security policies, physical security, and incident response plans.

Brocade SAN Health™ Pro is a free SAN analysis tool that helps document and analyze a SAN to document the SAN topology and uncover misconfigurations. For more information go to <http://www.brocade.com/support/sanhealth.jsp>.

Brocade also offers a comprehensive SAN Security Audit via Brocade Professional Services. For more information go to <http://www.brocade.com/support/SANSecurityAudit.jsp>.

BEST PRACTICES

- √ Use a separate network, subnet, VLAN or VPN for management interfaces
- √ Use secure protocols to communicate using management interfaces and disable unused protocols
- √ Use strong password management policies and implement RADIUS
- √ Disable unused ports, disable E_Ports on all unused and node ports, and implement Ports ACLs
- √ Use hardware enforced zoning
- √ Use LUN masking
- √ Use DH-CHAP to authenticate servers
- √ Perform a security audit of your SAN

SUMMARY

As with any network, SANs have security vulnerabilities, but with proper design and configuration a SAN can be extremely secure. In order to safely connect servers in a DMZ to a SAN, there are several security precautions that must be taken. Several techniques have been outlined in this whitepaper, which when combined together, can provide a high level of protection to the production SAN in the event a server in the DMZ becomes compromised.

© 2007 Brocade Communications Systems, Inc. All Rights Reserved. 08/07 GA-TB-032-00

Brocade, the Brocade B-weave logo, Fabric OS, File Lifecycle Manager, MyView, SilkWorm, and StorageX are registered trademarks and the Brocade B-wing symbol, SAN Health, and Tapestry are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON is a registered trademark of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.