

SANRAD White Paper:
SANRAD's Solution as Part of a Layered Security
Approach to IP-SANs
WP 007-01

SANRAD
US Tel: +1- 800-471-2616
International Tel: +972-3-767-4800

Copyright SANRAD 2004

All rights reserved. The copyright and all intellectual property rights in this article belong to SANRAD. It is strictly forbidden to copy, duplicate or otherwise use this article or any part thereof in any way shape or form without the prior written consent of SANRAD.

Table of Contents

INTRODUCTION	3
OVERVIEW OF AN IP-SAN	4
THE LAN PERIMETER	5
INTER-LAN COMMUNICATIONS	6
ISCSI INITIATOR AUTHORIZATION	7
ISCSI INITIATOR AUTHENTICATION	8
SUMMARY	9

Table of Figures

FIGURE 1. SANRAD V-SWITCH IN AN IP-SAN.....	4
FIGURE 2. FIREWALL SECURITY	5
FIGURE 3. VPN SECURITY.....	6
FIGURE 4. ACL SECURITY	7
FIGURE 5. CHAP SECURITY	8

Introduction

As the need for information storage and backup continues to rise exponentially, many companies have migrated away from FC-SANs and NAS and begun investigating and implementing more cost-effective IP-SANs. IP-SANs are storage networks connected over IP networks with information packets being sent within a SCSI command between an iSCSI initiator and iSCSI target. The average company has an IP-based infrastructure already in place and established IT guidelines, making the implementation of an IP-SAN easy and affordable.

However, specifically because IP-SANs may use the Internet – hailed as THE open world medium for information and idea exchange – some companies hesitate. Send my confidential company information via the Internet? Is it secure? How do I know that the right people will get the right information? How do I identify the right people?

These are legitimate questions that some insight into the available Internet, iSCSI and SAN technologies can answer.

This paper looks at each layer of the IP-SAN; the connections between iSCSI targets & initiators and what can be done to ensure information security in each layer. This paper presents four IP-SAN layers:

- LAN Perimeter
- Inter-LAN Communications
- Initiator Authorization
- Initiator Authentication

Your IP-SAN security should not be left to any one layer. In this paper, we'll examine an iSCSI command as it makes its way through each layer: what it can encounter and how SANRAD's V-Switch fits in. With an understanding of the layers of an IP-SAN and how to protect them, you'll know how to recognize the right people and get them the right data.

Overview of an IP-SAN

Before we examine each IP-SAN layer, first let's begin with an understanding of a standard IP-SAN topology.

An IP-SAN has three main types of components: storage devices, hosts and switches. The storage devices and hosts sit at opposite ends of the SAN and are connected in the middle through the IP network switches. iSCSI initiators in the host connect through the IP switch to iSCSI targets in the storage devices to access information.

Certain companies, such as SANRAD, have developed products – software, hardware or a combination – to enable virtualisation of physical storage into customized, sizable virtual volumes. Virtualisation can increase security in an IP-SAN by enabling unique partitioning of physical storage and applying rules for access to each partition. Throughout this paper, we will consider the added security value of SANRAD's V-Switch in an IP-SAN. The SANRAD V-Switch sits in the data path between the storage devices and the IP network switch.

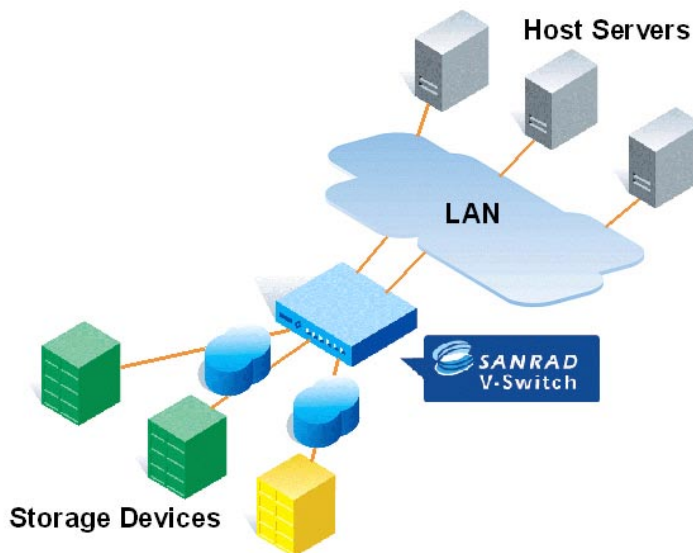


Figure 1. SANRAD V-Switch in an IP-SAN

The LAN Perimeter

The first layer of protection in your IP-SAN is the wall separating the internal network or Local Area Network (LAN) from the outside networks. This wall is the gateway through which information enters and leaves your LAN. Controlling this perimeter controls information access and flow.

SECURE TECHNOLOGY: FIREWALL

A firewall usually sits on the perimeter between the internal and external networks. A firewall provides traffic control between these two networks. A firewall can be closed to stop all traffic flow or selectively opened at specific locations to allow specific IP traffic through.

The iSCSI initiator login attempt trying to pass through the firewall must be on the firewall's list of IPs allowed to cross the firewall. If it is, it also must enter through correct port and be of the correct protocol. All firewalls should also have some method for authentication.

V-SWITCH

The V-Switch supports alternate iSCSI communication port configurations. A port other than the standard iSCSI port can be used for iSCSI communications, making unauthorized login attempts harder.

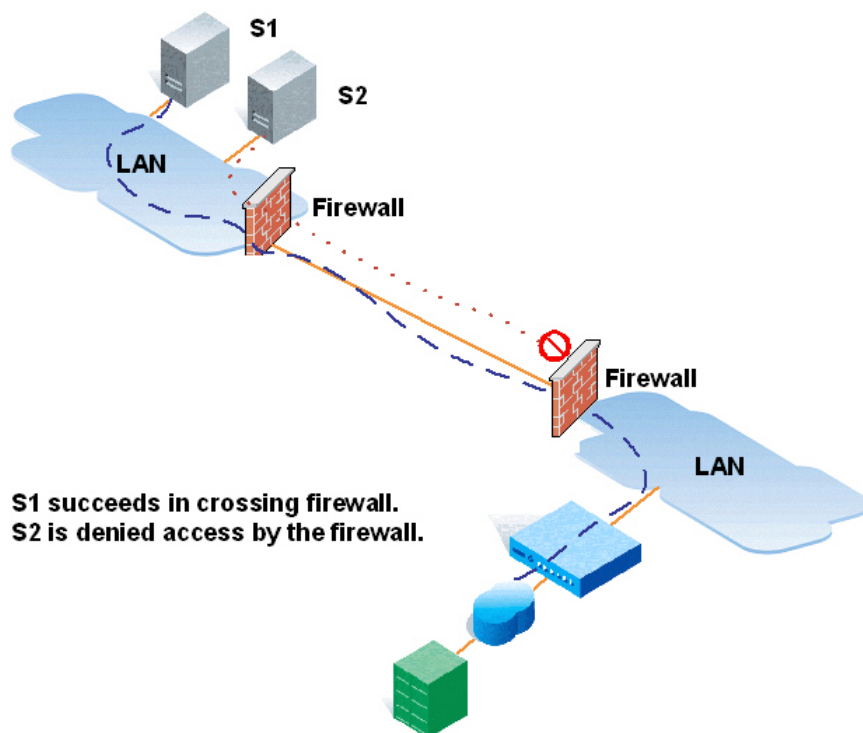


Figure 2. Firewall Security

Inter-LAN Communications

If you can close your LAN to outside networks, your information will be more secure. However, most companies need to be connected to outside networks. Isolation isn't an option. When information crosses through the private-public border, it can lose the security it enjoyed in a LAN. You cannot build a wall around information as it travels between networks but you can create secure tunnels and encrypt the information during its journey.

SECURE TECHNOLOGY: VIRTUAL PRIVATE NETWORK

A Virtual Private Network (VPN) creates a secure transport tunnel for data in motion between two LANs using high-level encryption. A VPN appliance is placed at the public-private border of each LAN. Encryption keys and groups are then configured for point-to-point encryption-decoding to guard against eavesdropping.

When the iSCSI initiator login attempt passes through the firewall and travels to another LAN, it is encrypted by the VPN as it leaves its LAN and is decoded by the VPN at the entrance to the second LAN.

V-SWITCH

The V-Switch supports VPN tunnelling appliances and methods, allowing information flowing through the V-Switch to be encrypted during 'public' travel between LANs.

The iSCSI initiator login attempt that made it successfully through the firewall arrives securely to the V-Switch's LAN.

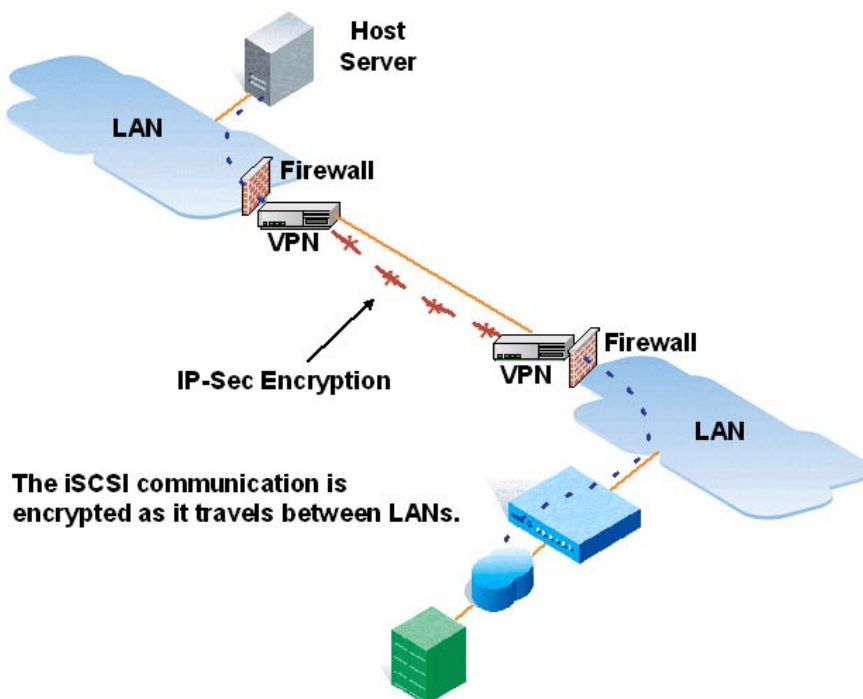


Figure 3. VPN Security

iSCSI Initiator Authorization

You have implemented security measures in two layers of your IP-SAN. An iSCSI initiator login attempt has qualified for access at each network layer. It is now at the specific iSCSI target device. Does the device allow anyone who can find it to log in? At this point, each device is on its own.

SECURE TECHNOLOGY: ACL

Certain devices support the creation of an Access Control List (ACL) for a target to establish which iSCSI initiators are allowed or denied access to it. Besides determining which iSCSI initiators can access the device, the type of access can also be set: read-write or read-only.

V-SWITCH

The V-Switch supports ACL configuration on a per-target per-initiator basis. The V-Switch ACL uses the iSCSI initiator's WWUI to identify it. More than one initiator can be allowed access to a target and each initiator's access rights can be independently configured. Access to a target can also be denied to an iSCSI initiator.

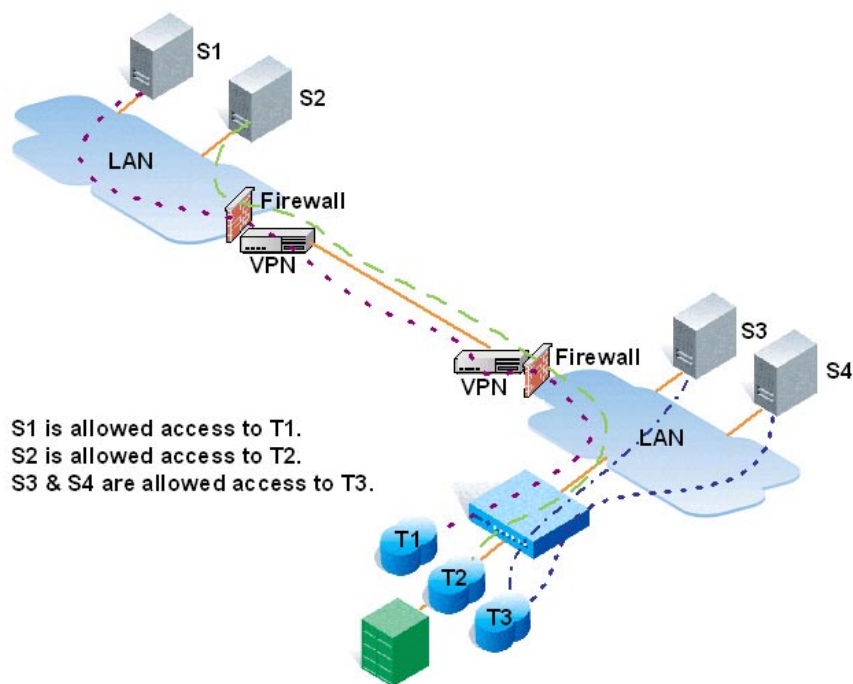


Figure 4. ACL Security

iSCSI Initiator Authentication

An iSCSI initiator login attempt seems to come from an ACL-approved source. But how do you know that the iSCSI initiator really is who it says it is? How do you know it isn't an impostor? What if your club – iSCSI target – had a secret handshake that all members needed to know to gain admittance? Something more elaborate and foolproof than, "Joe sent me."

SECURE TECHNOLOGY: CHAP AUTHENTICATION

Challenge-Handshake Authentication Protocol (CHAP) is an authentication protocol that can be used to authenticate iSCSI initiators at target login. The iSCSI target server sends an encrypted user name + password challenge to the initiator. The initiator must answer the challenge. Without the correct answer, the iSCSI session login attempt is terminated.

V-SWITCH

The V-Switch ACL supports CHAP and SRP authentication for its iSCSI targets. The user name + password are configured and stored on the V-Switch. As an additional safety measure, the V-Switch includes a RADIUS client for supporting a RADIUS server. Instead of storing the user name and password together on the V-Switch, the user password can be stored on the RADIUS server.

- 1 - The initiator attempts to login.
- 2 - V-Switch sends user name + password to RADIUS server.
- 3 - RADIUS server verifies user password.
- 4 - V-Switch logs initiator in and opens session.

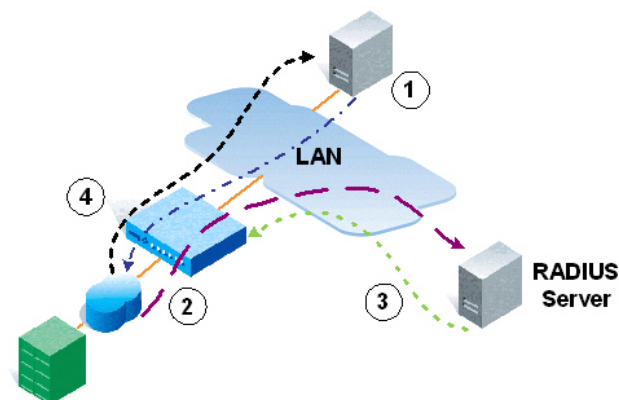


Figure 5. CHAP Security

Summary

IP-SANs answer the growing need for more cost-effective and secure SAN implementations. Using readily available IP security technologies, you can secure your data transfer over the IP network without increasing the cost of ownership of an IP-SAN. Using the SANRAD V-Switch, you can add initiator authorization and authentication to your existing security measures.

SANRAD plans to incorporate IP-Sec encryption technologies into the V-Switch to provide its customers with full data encryption within the LAN. SANRAD is also developing technologies to protect your data at rest against theft of the physical storage disks.

SANRAD
US Tel: +1- 866-301-8155
International Tel: +972-3-767-4800
info@SANRAD.com

Copyright SANRAD 2004

All rights reserved. The copyright and all intellectual property rights in this article belong to SANRAD. It is strictly forbidden to copy, duplicate or otherwise use this article or any part thereof in any way shape or form without the prior written consent of SANRAD.