



Network Storage Group Host Products Technology Brief January 22, 2003

ISCSI SECURITY (IPSEC)

FC SANs have enjoyed an “inherent” security mechanism because they are typically physically isolated. Connecting to a FC SAN also requires unique expertise and equipment. Exposing valuable data storage on an Ethernet network is a different story. iSCSI is an exciting new protocol that enables high performance SANs over existing Ethernet networks promising lower total cost of ownership and ease of use. However, the ubiquity of Ethernet and the potential of having a data and storage area network on the same infrastructure have accelerated the SAN industry’s concern for end-to-end security.

Why is iSCSI Security Important?

There are several factors contributing to the security concerns of iSCSI. First and foremost is the fact that every laptop, PC, and server today can access an iSCSI network through a Gigabit Ethernet or even a 10/100 Mb Ethernet port. Almost every business in the country and now even homes have a working knowledge of how to configure and address an IP network. IP networks power the Internet providing worldwide addressability connecting millions of remote end nodes to a single network. The popularity of the Internet has driven a sophisticated niche industry of developing viruses, spying, and snooping software utilities that are available for free. In fact TCP/IP viruses, such as Melissa, Code Red, and Red Worm, are not only named, but even make the worldwide news! These factors combined with the future promise of running a SAN and LAN on the same Ethernet infrastructure to reap the benefits of pooled network bandwidth, lower equipment cost, and easy to manage systems, have driven the requirement for security in the iSCSI standard.

The iSCSI Protocol Security Requirement

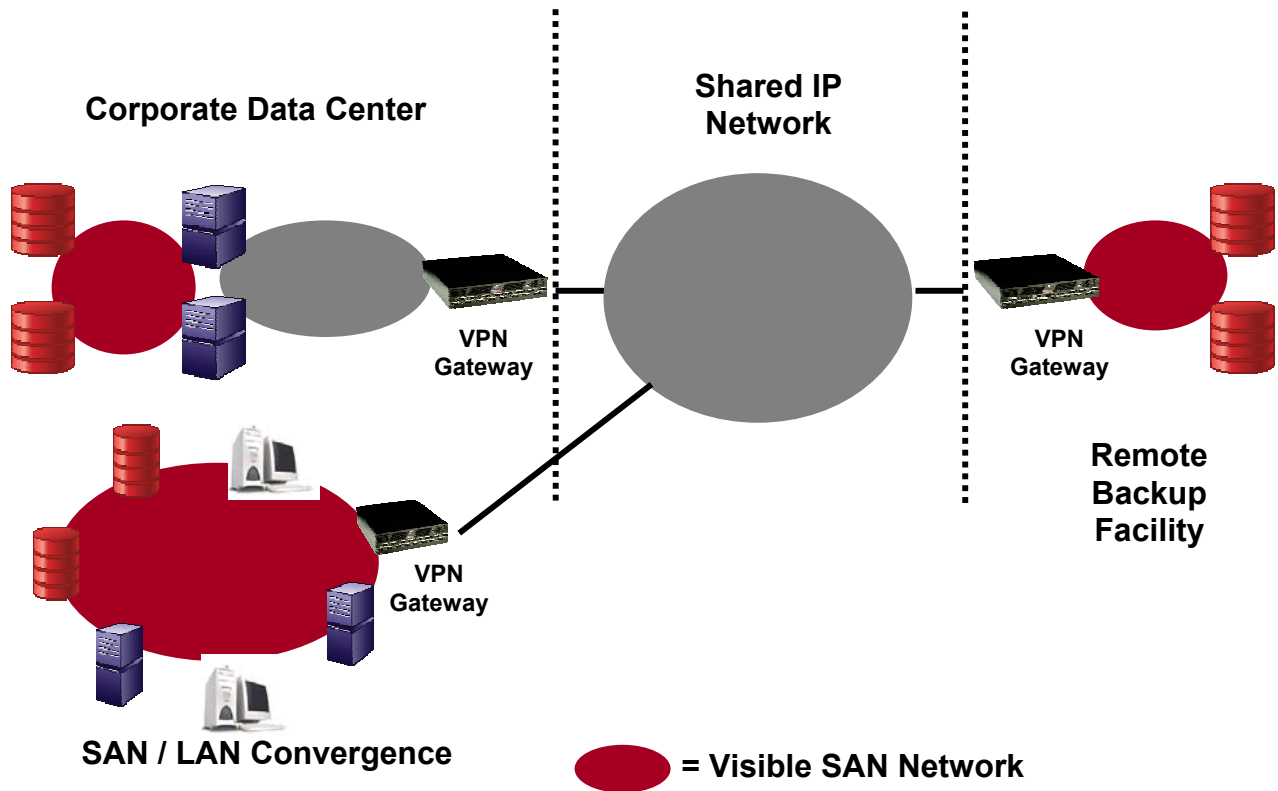
The IETF iSCSI standard includes optional provisions for full IPSEC which includes user authentication, message authentication, encryption, and key exchange functionality. iSCSI security functionality can be in Host Bus Adapters (HBAs) that are used in servers and storage systems, or dedicated security fabric appliances. During the initialization of an iSCSI network, end-nodes advertise their security capabilities and negotiate to the least common denominator of capability between communicating nodes. For example, if one end node has security and the other has no capability, the two will communicate to each other without security with the permission of both nodes. iSCSI is an application that runs with an existing network protocol, TCP/IP. As a result, iSCSI security leverages proven technology based on existing IPSEC standards, RFC 2401 and 2406, and does not have to reinvent the wheel. In fact, iSCSI security is based on the same technology used by traveling business people for connecting to corporate VPNs.

Secure iSCSI SAN Applications

Initial iSCSI SANs will be deployed physically isolated from the data network similar to FC. Since iSCSI runs over Ethernet, every computing device including servers, PCs, and laptops, can easily access an iSCSI SAN. This ease of access renders iSCSI SANs more susceptible to security breaches and puts data stored over an iSCSI network at risk. By using secure iSCSI HBAs, a physically isolated SAN can no longer be accessed without the proper authentication. Even if data

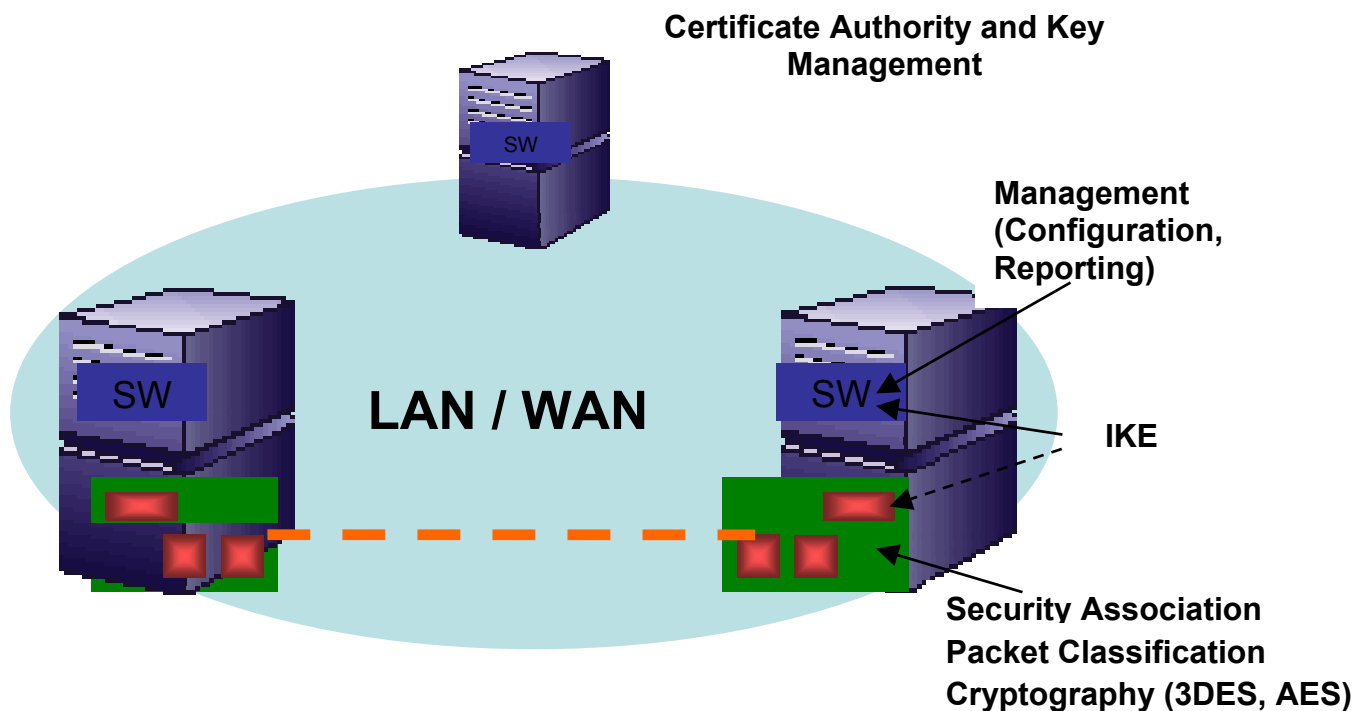
is illegally received or intercepted, the data would not be readable without the proper secret key and encryption algorithm.

The deployment of secure iSCSI HBAs and the ubiquity of TCP/IP enable new remote SAN applications, while providing end-to-end network security. Since iSCSI security is based on the same technology used for TCP/IP security today, a single SAN with secure iSCSI HBAs can easily span over a WAN with storage and servers in multiple locations. By providing security in end-node iSCSI HBAs, the storage network and data network can eventually converge to maximize network bandwidth usage, lower network management costs, and share the same switch fabric equipment, without the concern of security breaches and illegal access to information.



IPSEC Explained

IPSEC is a widely deployed technology standardized by the Internet Engineering Task Force (IETF), RFC 2401 and RFC 2406. IPSEC is an additional protocol layer on top of IP that interfaces transparently to the transport layer (TCP, UDP, etc...). The IPSEC function encapsulates IP packets with a new header and changes IP packets to provide end-to-end network security. The implementation of IPSEC involves several components:



User Authentication

User Authentication verifies that the end-node is who they claim to be. To ensure valid authentication, IPSEC uses electronic certificates that act as a birth certificate for nodes on the network. A public or internal company authority can administer these certificates.

Message Authentication

Message authentication ensures the integrity of information that is passed between nodes is accurate and has not been corrupted or tampered with.

Encryption

Encryption encodes the information so that even if it is accurate the information could not be read without the correct key and encryption algorithm to decode the information, providing full confidentiality between two communicating end nodes. Encryption algorithms are based on mathematical equations. With the advent of computers, encryption algorithms must guard against computers that can quickly try every possible key combination to breach security (also known as a brute force attack). To prevent this encryption mathematical computations are extremely complex and require significant processing to try a single combination. For instance, a \$200,000 server can try every combination and crack 56-bit 3DES in three days. As computer processing capabilities increase new encryption algorithms must be invented to ensure security. 3DES and AES are the encryption algorithms used in iSCSI to encode data. The computing power required to process,

3DES or AES, is approximately 2 to 3 times more than the processing required to offload TCP/IP for iSCSI.

Security Associations and Classification

Security associations define the policies and rules of communication between end nodes. Received packets of information must be classified by an end-node adapter to determine if the information can be accepted. Security associations are based on several parameters, including source/destination address, type of traffic, size of packet, encryption method, etc...

Key Exchange

Key Exchange (IKE) is the standard mechanism that enables two end nodes to provide each other with the proper key to successfully decode encrypted information. In the case of 3DES, the key is a 56-bit binary number that is only exchanged with an authenticated end node. The two most common ways for distributing keys are pre-shared keys or PKI (public key infrastructure). With pre-shared keys, keys are manually distributed to each end node and are practical only for IPSEC deployments with limited nodes. With PKI, keys are administered and initially generated by a certificate authority, allowing end nodes to be easily added and managed. PKI allows for the deployment of larger IPSEC networks. An independent company can administer certificates publicly or companies can purchase certificate authority software and administer certificates for their own secure network.

Policy Management and Reporting

Software is required to administer permissions and policies to govern the flow of information and data between nodes of the network. Typically the same software provides reports and statistics to monitor traffic flow and the status of the network. Reporting allows network managers to quickly and easily identify security breaches.

The Challenges of Implementing iSCSI Security

Including security in the iSCSI standard is only the first step to the successful adoption of secure iSCSI SANs. The complexity of iSCSI security poses several challenges to including IPSEC functionality in HBAs.

Hardware Acceleration is required for 1Gb IPSEC processing.

The performance of a secure iSCSI network must be similar or close to the performance of a non-secure iSCSI network. iSCSI employs the highest level of encryption, 3DES and AES, which requires a significant amount of computation to implement. In fact, the processing required can be anywhere from 2 to 3 times more than the processing of TCP/IP. Processing 3DES or AES in firmware or software at 1Gb data rates significantly degrades the performance of the network to the point where secure iSCSI SANs are impractical. State-based hardware dedicated to IPSEC processing is mandatory to support 1Gb secure iSCSI HBAs.

Standard IPSEC ASIC technology is too expensive.

Standard 1Gb IPSEC processing ASICs can cost several hundreds of dollars because they were designed for the VPN router market. VPN routers require IPSEC ASIC features that HBAs do not and are less cost sensitive. VPN routers can cost over \$100,000 and are purchased to handle the simultaneous processing of thousands of IPSEC connections. The use of standard IPSEC ASIC technology currently available to provide security would easily double if not triple the price of an iSCSI HBA. The adoption of iSCSI security is unlikely without affordable secure iSCSI HBAs. Significantly increasing the price of an adapter by adding security will leave secure iSCSI HBAs on the shelves.

Secure SANs must be easy to manage and configure.

Tools that can manage end node policies, access to storage, and detailed reports are required to successfully implement secure iSCSI networks. Management tools that incorporate the administration of IPSEC with SAN management are necessary for IT managers to deploy iSCSI security. If tools are difficult to use or if IPSEC and SANs are administered separately the cost to manage the network may hinder the adoption of secure iSCSI SANs.

Evaluating iSCSI Security Solutions

iSCSI HBAs and storage systems are available with and without IPSEC security. If security is required for your iSCSI deployment, there are several key criteria that are important in selecting the ideal solution.

Performance

Many products may offer support for IPSEC security with severely limited performance. Products that implement encryption or message authentication in software may support security, but are impractical because using these security features would drop performance to an unacceptable level. If enabling IPSEC security drops the throughput performance of a 1Gb iSCSI HBA to just 10Mb, why buy a 1Gb solution in the first place? Buying a 10/100 Mb iSCSI solution would be more practical and less expensive. Solutions that offer full 1Gb wire-speed support offload the most compute intensive functions of IPSEC with hardware. When purchasing iSCSI products be sure to find out if hardware is used to offload and accelerate the performance of IPSEC.

Price

Many iSCSI products that offer IPSEC security with the right performance are extremely expensive because they are using components that were originally developed for other applications, such as VPNs. Products using hardware technology optimized for secure iSCSI should be significantly less than 2 to 3 times the cost of an equivalent iSCSI product without security.

Experience with IPSEC Hardware and SAN I/O Technology

IPSEC is a complex technology with many software and hardware components. The combination of IPSEC and SAN technology requires new management tools and hardware to ensure that secure iSCSI SANs are easy to use. There are only a few vendors with a proven track record of delivering IPSEC and SAN I/O technology that have the experience required to develop secure iSCSI SAN products.

Now that SANs are mainstream and widely deployed, the concern for protecting data on storage networks has increased. IPSEC is a complex technology that is difficult and challenging to develop. When selecting iSCSI HBAs and storage systems for an iSCSI SAN, performance, affordability, and ease-of-use are key decision factors. Companies with a proven track record in both SAN I/O and high performance IPSEC products offer the best products for secure iSCSI SANs.