Securing IP Storage Networks

By Charles Baumert, Senior Director, Marketing, Cylink Corporation

Overview

Storage Networks are expected to capture more than half of the new storage deployments within the next few years, largely because they enable users to profit from a number of key business benefits. Multiple information resources can be consolidated for increased efficiencies and reduced costs. Members of an organization or a group of organizations can collaborate and share information, resulting in new opportunities to generate revenue. Information can be efficiently distributed within a network in order to improve service levels. Storage Networks can also be used as part of a Business Continuity program to provide back up information in the event that primary systems are disabled.

Storage Area Networks (SANs) were initially developed based on Fibre Channel (FC) technologies. The key benefit of FC networks is that they provide a high performance connection to storage that behaves like a dedicated link. The trade-off, however, is that they are not as widely implemented as IP networks. Organizations have to consider the costs of deploying a new infrastructure and acquiring a new set of skills to effectively manage and operate FC networks. To date, FC reach limitations and lack of interoperability between FC vendors have also been issues as customers strive to evolve from a centralized storage architecture to a more geographically distributed one that can provide additional benefits of efficiency and secure redundancy.

As an alternative, new technologies are being introduced that provide the ability to interconnect SANs using conventional Transmission Control Protocol/Internet Protocol (TCP/IP) and Ethernet networking. These technologies include Fibre Channel Internet Protocol (FCIP), Internet Fibre Channel Protocol (iFCP) and Internet Small Computer Systems Interface (iSCSI).

One of the key advantages of using the existing IP infrastructure is that these new technologies can leverage established security methods like IP Security (IPSec). Solutions are being deployed in networks today to provide the following:

Encryption – keeps important information confidential, private and within the control of the owning organization

Authentication – ensures that the identities of both the sender and the receiver of a communication are authentic before information is exchanged

Data Integrity – ensures the integrity of information during transmission

These proven capabilities can be used to prevent storage networks from being compromised and ensure that important information will not be stolen, deleted or maliciously altered.

Technologies for Securing IP Storage Networks

Baseline security for an IP Storage Network requires first that the local network segments be physically secure. Additional security can be provided by segregating storage resources and restricting access on the basis of operating system, department or shared storage access. Application-level technologies offer the potential of encrypting data at rest, while it is in the storage devices themselves.

Any rigorous security strategy, however, must also ensure that the data in transit between Storage Networks is protected. In an IP network this can be done with confidence, utilizing the well-established IPSec protocol. IPSec architecture and implementations for authentication and encryption are defined by IETF RFC documents 2401, 2402 and 2406 respectively.

Cylink has implemented a fully IPSec compliant design on its NetHawk VPN Encryptor. The product uses encapsulating security payload (ESP) to ensure data is undecipherable to an outsider and uses security associations based on tunneling mode. In tunneling mode, IP traffic issued from an individual host is encrypted by the VPN and then wrapped with an additional IP header addressed to the remote security gateway. At the end of the IPSec tunnel the traffic is decrypted and the original header is then used to route the traffic to its final destination. NetHawk currently uses strong Triple-DES encryption.

Authentication is achieved using X.509 digital certificates. Policy-based management of connections is provided and support for IKE simplifies the process of establishing connections between clients and gateways. In addition to authentication and encryption, NetHawk ensures maximum data integrity by making full use of the X.509v3 certificate format when exchanging data. Data recipients can be confident that what they receive is in fact what was originally sent. The bits that are used to ensure data integrity are themselves fully encrypted during transmission for additional security.

Cylink's powerful certificate-based network security manager, PrivaCy Manager, provides system scalability and centralized management of security devices. The manager also provides extensive reporting and logging capability.

Although VPN security capabilities can be added to other networking equipment such as routers or firewalls, there are risks that such an implementation opens up new security breaches and can potentially reduce performance. Highest levels of performance and security are provided with standalone encryption devices that can be separately managed from routers and firewalls.

Applying Security in IP Storage Networks

Cylink security solutions can readily be deployed in IP Storage Networks. This section will briefly describe each of the IP Storage Network technologies and show how NetHawk can be used to secure them.

Fibre Channel over IP (FCIP)

FCIP is a simple tunneling protocol for encapsulating entire Fibre Channel frames within TCP/IP. FCIP is used for connecting Fibre Channel SANs over distance to create a single larger Fibre Channel fabric.

Fibre Channel data at the source site is encapsulated in TCP/IP and sent across the network. At the receiving end, the TCP/IP headers are removed, and native FC traffic is provided to the destination switch. FCIP is fairly simple to deploy but uses TCP/IP only for intervening transport. Users are able to make use of their existing IP infrastructures but still need to contend with two disparate networks.

By deploying NetHawks at either end of the IP tunnel as shown in Figure 1, secure transport across the IP network is ensured.

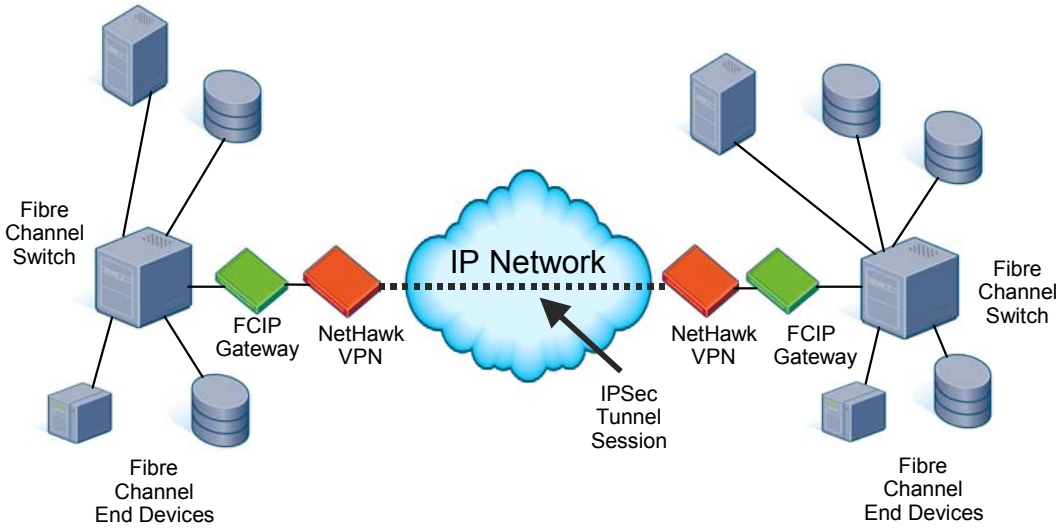

Figure 1. Securing an FCIP connection between two FC SANs

Hewlett Packard has certified Cylink's NetHawk to provide VPN encryption as part of their SANworks™ Data Replication Manager FC-IP solution. As part of the certification process, interoperability between NetHawk and FCIP gateways from CNT, SAN Valley Systems and SANcastle Technologies was verified.

Internet Fibre Channel Protocol (iFCP)

The iFCP protocol provides native TCP/IP connections between end devices. iFCP extends to the Fibre Channel end devices directly, eliminating the need for Fibre Channel switches and providing an IP storage switched network instead.

From an application standpoint, iFCP enables a much higher degree of interoperability for existing software and hardware products. Applications written for Fibre Channel SANs can run over iFCP-based SANs as well.

In an iFCP-based network, NetHawk can we used in front of the iFCP gateway to ensure security as shown in Figure 2.

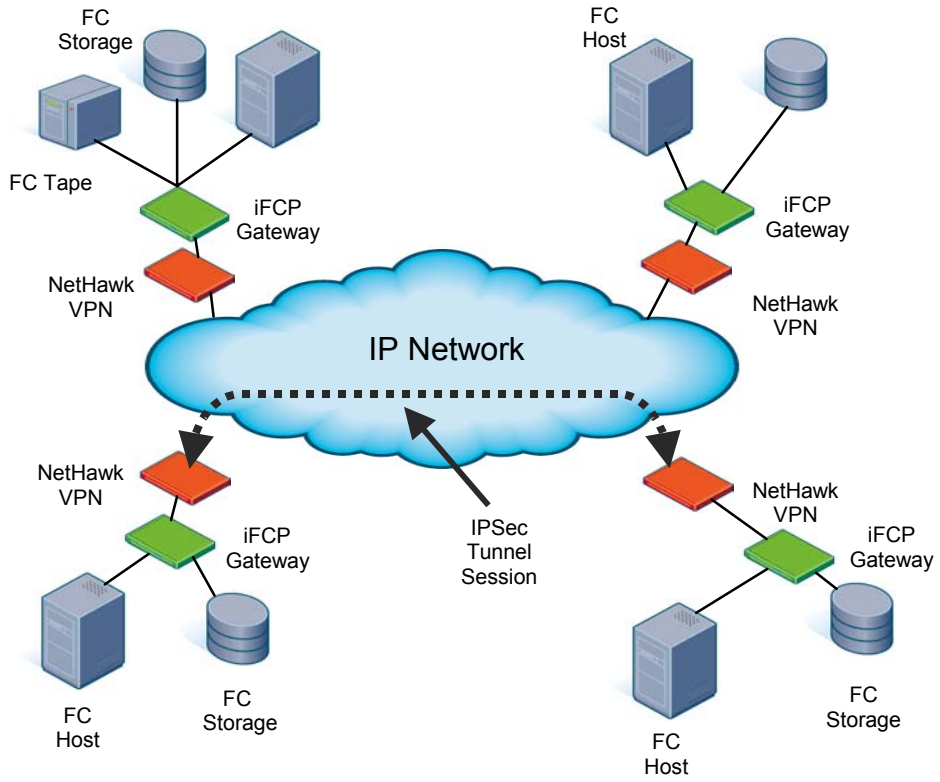

Figure 2. Securing an IP SAN that uses iFCP

Internet Small Computer Systems Interface (iSCSI)

The iSCSI protocol enables a homogeneous IP SAN solution. For some of the proponents of the developing iSCSI standard, FCIP and iFCP simply represent stepping stones on an evolutionary path that will lead from FC towards a ubiquitous IP SANs architecture. In all likelihood however, there will be a mix of FC, FCIP, iFCP and iSCSI solutions in the network for some years to come.

The iSCSI protocol encapsulates SCSI commands, status and data over TCP/IP and assumes that the storage end devices are native iSCSI. The iSCSI specification does not address FC end devices or the FC Protocol (FCP).

Figure 3 shows how NetHawk can be used to secure an iSCSI network.

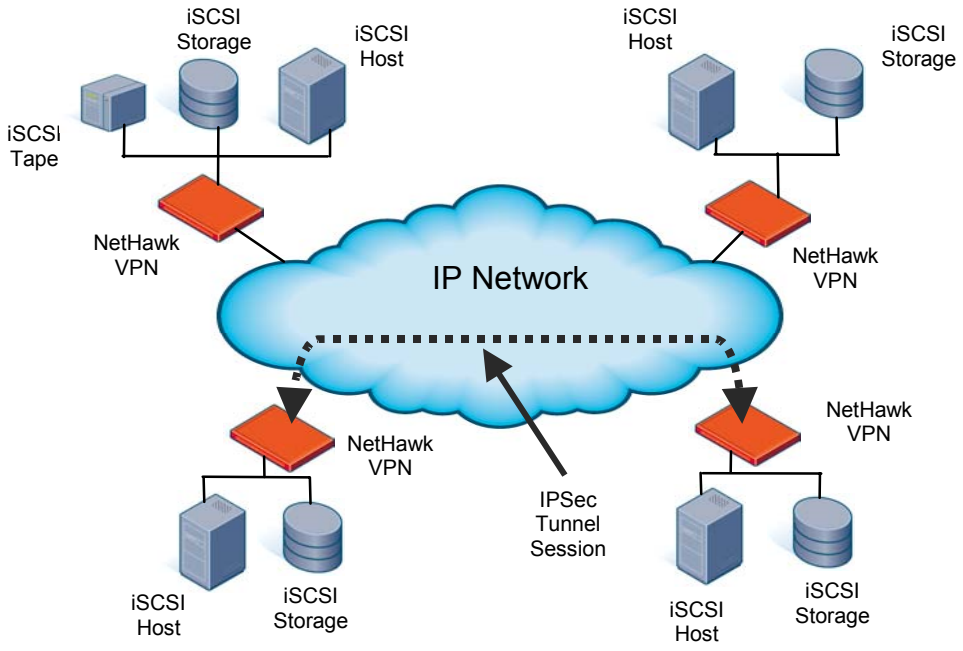

Figure 3. Securing an IP SAN that implements the iSCSI protocol end-to-end

A potential next step in iSCSI deployment will be the integration of IPSec functionality directly into the iSCSI host and storage devices as shown in Figure 4. Issues of cost, interoperability and security management will need to be addressed in order to make these solutions viable and scalable.

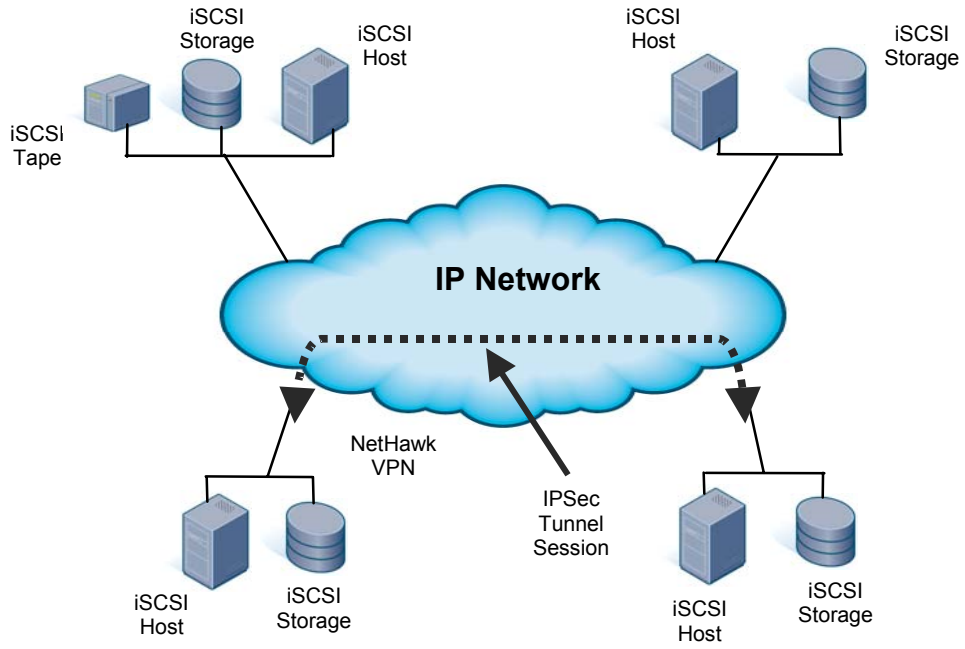

Figure 4. Securing an IP SAN that implements the iSCSI with IPSec integrated into the iSCSI devices

Key IPSec VPN Encryptor Features

The NetHawk family of encryptors has a number of features that are particularly important for use in an IP SAN environment.

Wire Speed Performance

Cylink's stand-alone NetHawk VPN appliance currently has a bandwidth capacity of 200 Mbps full duplex, and can support 20,000 simultaneous connections. Multiple NetHawks can be stacked in a load-balanced configuration to handle higher bandwidth requirements. Cylink is also developing a higher speed interface that will support a full Gigabit. Since NetHawk is a standalone device and does not need to share CPU processing power with an integrated networking device such as a router or firewall, it is able to maintain full wire speed performance under most conditions, which is not the case with integrated devices.

Failover

NetHawk's failover support ensures system reliability by allowing the network designer to build redundant NetHawks into a network. Up to four NetHawks may be used in a single protection configuration. The active and standby NetHawks are all configured with the same security policy by PrivaCy Manager. They are loosely coupled, each having an independent cryptographic identity and managing its own Security Associations (SAs).

One of the NetHawks is the active (Master) unit with all traffic going through it. In the event of a failure of the Master or certain link faults the next highest priority alternate NetHawk becomes Master and takes over all traffic. Remote NetHawks automatically learn that there is a new Master and direct traffic accordingly.

Load Balancing

NetHawk's load balancing feature ensures system availability in the event of fluctuation in system usage. In a load-balanced configuration, multiple NetHawks are deployed in parallel in a VLAN configuration. A stand-alone load balancer or a router with load balancing capability divides the amount of processing work between the VPN gateways and the router on a LAN so that processing is optimized and, in general, all users are served more quickly. Cylink plans to offer several variants of load balancing including stationary, round-robin, and load measure to ensure flexibility and scalability.

Manageability, Interoperability

Several characteristics of NetHawk make it easy to manage and deploy.

- Devices can be moved or redeployed throughout an evolving IP network. The same encryptors can be used in different applications as a network evolves from FCIP through iFCP to iSCSI.

- Cylink encryptors are compatible with MPLS, which can be used as a complementary technology to provide Quality of Service, and enhanced network performance.

- Privacy Manager enables users to establish security policies which automatically generate the rules for NetHawks. PrivaCy Manager also functions as the certificate authority.

In addition to managing NetHawk, PrivaCy Manager is also able to simultaneously manage the full line of Cylink encryptors including devices for ATM as well as Frame Relay and Leased Line networks. Thus, Cylink can be used to provide security throughout a company's network independent of the protocols being used.

About Cylink Corporation

Cylink develops, markets and supports a comprehensive portfolio of hardware and software security solutions for mission-critical private networks and business communications over the Internet. Founded in 1983, our solutions offer competitive advantages by lowering the cost of deploying and managing secure, reliable private networks, while enabling use of the Internet for trusted transactions with business partners and customers. Cylink's business solution focus areas include Secure Storage Area Networks

for Business Continuity and Disaster Recovery, Homeland Security including Critical Infrastructure Protection for Airports and First Responders, and Intellectual Property Protection. For more information about Cylink, please call (408) 855-6000 or visit www.cylink.com.

For additional information, contact Cylink at:

Corporate Headquarters
3131 Jay Street, Santa Clara, CA 95054
Phone USA & Canada: 800.533.3958
Phone Other Countries: 408.855.6000
Fax: 408.855.6100
Email: info@cylink.com
Website: www.cylink.com