



Wire-Speed Network Security for IP Storage - Challenges and Solutions -

- Network security is critical to realizing the promise of broad-based deployment of IP Storage networking across enterprises, MANs, and WANs.

- IP Storage requires security solutions designed for the specific requirements of storage traffic.

- The NetOctave FlowThrough™ Security Architecture is optimized for wire-speed IPsec support for IP storage

The use of TCP/IP infrastructure promises flexible, cost-effective, and high-performance storage networking for a broad range of application environments. Three TCP/IP-based storage protocols, (*iSCSI*, *FCIP*, and *iFCP*) have been submitted to the Internet Engineering Task Force (IETF). Collectively, these protocols are grouped under the family name of *IP Storage*.

Network security is critical to the realization of the promise of broad-based deployment of IP Storage networking across enterprise networks, metropolitan-area networks (MANs), and wide-area networks (WANs). Enterprise-wide storage consolidation requires flexible and strong *authentication* and *data integrity* mechanisms. Storage Service Providers (SSPs) (who operate in the MAN environment) require a range of fine-grained IP Storage security capabilities. In the WAN arena, *data confidentiality* is a critical requirement for corporations to use shared public IP facilities for transport and outsourced storage of business-sensitive data. All of these requirements are met by the use of IP Security (IPsec) within the IP Storage protocols. Proper implementation of the IPsec protocol in IP Storage represents a critical challenge that will drive the rate of adoption of IP Storage.

The Challenges

Implementing wire-speed IPsec network security for IP Storage requires addressing a number of important challenges. Specifically,

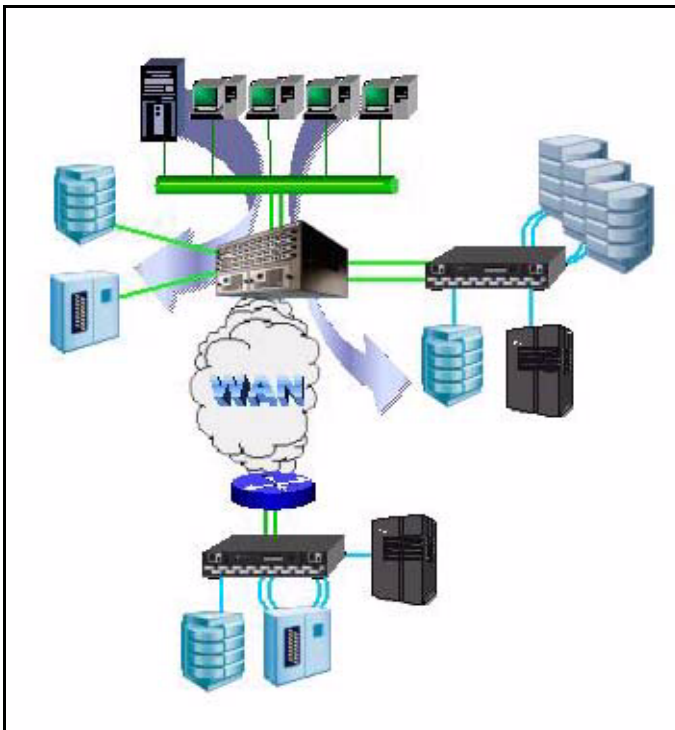
- ❑ The reliance of the three IP Storage protocols upon IPsec for security requires an optimized hardware solution for IPsec acceleration for IP Storage.
- ❑ The specific throughput, latency, and session traffic characteristics of IP Storage traffic require an order-of-magnitude efficiency improvement over current IPsec hardware and software solutions.
- ❑ IP Storage end-points use TCP/IP Offload Engine (TOE) components for low-latency processing of TCP/IP and lack the general-purpose packet handling capability provided by network processors. In this environment, IPsec acceleration hardware must incorporate the full range of IPsec functions, including cryptographic processing, security association handling, security policy management, and link layer adaptations.

Optimal support of IPsec in IP Storage devices requires a new generation of security processors that provide a self-contained solution for *in-line* acceleration of the full range of IPsec functions for multi-gigabit IP Storage flows.

Network Security for IP Storage

Today, the standard protocol for storage area networks (SANs) is Fibre Channel (FC) fabric technology. FC supports high levels of scalability, performance, and manageability, and helps overcome the distance limitations of previous connectivity protocols such as SCSI. While FC technology enables a flexible networked environment, optimized for server-to-storage data communications and high-speed server-to-server interconnectivity, there are a number of limitations that have hindered broad-based use of FC across corporations. For example, FC does not extend natively beyond 10 or 100 kilometers without the use of Wave Division Multiplexing (WDM) technology. Also, FC is severely limited by its lack of an internal security function. Security of Fibre Channel Storage Area Networks (FC SANs) is primarily addressed through physical security of the FC SAN infrastructure, which limits their deployment to high-end "glass house" environments. As a result, the storage network extension market is underserved.

The use of TCP/IP infrastructure promises flexible, cost-effective, and high-performance storage networking for a broad range of application environments. Current TCP/IP-based storage protocols in development and submitted to the IETF include *iSCSI*, *FCIP*, and *iFCP*. Collectively, these protocols are grouped under the family name of *IP Storage*. IP Storage is expected to drive the proliferation of a range of new classes of products. For example, a new generation of IP Storage Network Interface cards (NICs) and Host Bus Adapters (HBAs) is expected to emerge to enable servers with *iSCSI initiator* capabilities. Storage systems are expected to evolve to support *iSCSI target* functionality. In addition, next-generation storage networking switches are expected to offer IP Storage interfaces, including iSCSI and FCIP ports, as standard interfaces.



For enterprise end-users, IP Storage promises storage consolidation for hundreds to thousands of servers supporting low-end and mid-range applications. For Storage Service Providers (SSPs), IP Storage promises to enable efficient and secure sharing of storage resources among multiple customers. IP Storage also promises to enable storage SSPs and enterprises to leverage the ubiquity of IP for MAN/WAN networking for order of magnitude cost-effective storage area networking over distance.

Figure 1 Pervasive IP Storage Networking Across LAN/MAN/WAN Networks

Network security is critical to realizing the promise of broad-based deployment of IP Storage networking across enterprise, metropolitan (MAN), and wide-area networks (WAN). In an enterprise scenario, the opportunity to utilize iSCSI as the basis for enabling enterprise-wide storage consolidation requires:

- ❑ flexible and strong *authentication* or access control mechanisms to ensure only authorized users and hosts can access data and to prevent untrusted sources from launching attacks.
- ❑ *data integrity* mechanisms to address tampering or modification of data during transit. The ability of SSPs to capitalize on the opportunity to serve a range of different customers having varied security requirements assumes a range of fine-grained IP Storage security capabilities, while cost-effective SSP iSCSI-based storage networking presupposes the use of public IP MAN/WAN facilities for the transport of storage data.
- ❑ *data confidentiality* to enable corporations to use shared public IP facilities for transport and outsourced storage of business-sensitive data.

IP Storage Security Standards

IPsec is a framework of open security standards developed by the IETF. IPsec provides security for transmission of sensitive information over unprotected networks, such as shared enterprise, MANs, or WANs. IPsec products from a range of vendors have been successfully deployed for business-critical applications in enterprise and service provider networks, and have achieved a high degree of interoperability.

IPsec is also the foundation of network security capabilities of the IP Storage protocols. IPsec provides two key benefits as the underlying IP Storage security capability. First, as a broadly-supported standard, it will enable simplified interoperability across multi-vendor storage systems. Second, it will easily support the breadth of security requirements for the range of different IP Storage deployment scenarios.

IP Storage capabilities are envisioned for a range of product classes, including NICs, switches, and storage systems, which will be deployed in a number of scenarios, including enterprises and SSPs. Therefore, upcoming IP Storage protocol standards, including iSCSI, include mandatory support for a range of IPsec-based security capabilities; the actual use of which will be made by IP Storage end-points on a policy basis. These capabilities include¹:

- ❑ Mutual login between an iSCSI initiator and target during iSCSI session set-up as an *application-level* access control scheme. This step assumes the existence of a secure IPsec-based TCP connection between the iSCSI initiator and target.
- ❑ *Packet-level* IPsec-based robust data integrity checking to verify IP Storage commands and data have not been tampered with during transmission, as well as to address any errors that may have been introduced as IP Storage flows traverse intermediate TCP devices, such as TCP proxies and NAT devices, is critical.
- ❑ Flexible packet-level IPsec-based authentication or cryptographic verification of source/destination of IP packets is key to preventing malicious attacks to disrupt storage service delivery. In addition, IPsec-based authentication is a mandatory component of FCIP and iFCP protocols.
- ❑ IPsec-based *confidentiality* or protection against surreptitious monitoring of IP Storage traffic as it traverses public IP networks, including MAN/WAN networks, is a mandatory IP Storage requirement.

1. "Securing iSCSI, iFCP and FCIP", IETF Internet-Draft, 10/01

Implementing Security for IP Storage

Implementing wire-speed IPsec network security for IP Storage requires addressing a number of important challenges, which are outlined in the following sections.

Challenge 1 - IP Storage Traffic—Different Requirements from Network Data Traffic

IP Storage networking traffic is typically characterized by multi-gigabit level traffic flows between servers, storage networking switches, and storage systems. The intensive handshaking involved in the SCSI command set, the small blocks of data making up large portion of SAN traffic, and the high-performance caching schemes in storage systems combine to require an order of magnitude higher end-to-end latencies for IP Storage traffic than is required for pure data traffic. Additionally, there are significant specific differences between IP Storage and data traffic characteristics, which have important implications for the efficiency of implementing, wire-speed IPsec for IP Storage applications². These differences include:

- ❑ High relative percentage of large packets for IP Storage versus secure networking (6-8 million packets per second for IP Storage versus over 14 million for minimum packet size networking traffic).
- ❑ Low IP Storage session creation/teardown rates. Sessions between IP Storage end-points are typically long-lived to avoid latencies due to TCP “slow start” inefficiencies. As a result, Internet Key Exchange (IKE) acceleration can be handled in software rather than requiring a dedicated IKE accelerator.

Compared to VPN traffic, IP Storage traffic requires high throughput, but with fewer packets per second and lower session creation/teardown rates. Existing IPsec solutions will not provide the throughput required for storage systems, while new high-speed IPsec processors that are designed for VPN traffic will not work efficiently with IP Storage traffic.

Challenge 2 - Mandatory User of IPsec

The pervasive use of IPsec as the foundation of IP Storage security is the second important challenge to implementing IPsec for IP Storage. Unlike data networking protocols such as HTTP, SMTP, and FTP, which assume optional use of security on a per-client or per-network basis, IP Storage protocols assume a mandatory role of IPsec security. Specifically, the initial iSCSI login phase required for providing an application-level access control scheme assumes a secure IPsec-based TCP connection between the iSCSI initiator and target.

In addition, IPsec-based per-packet authentication, integrity checking, and confidentiality are supported to address threats such as masquerading, tampering of data during transit, IP session hijacking and acquisition of confidential data (Figure 2). The implication of such pervasive use of IPsec for all IP Storage deployments is that the IPsec architecture for IP Storage devices must have optimized support for IPsec as a mandatory wire-speed function.

2. NetOctave company internal analysis

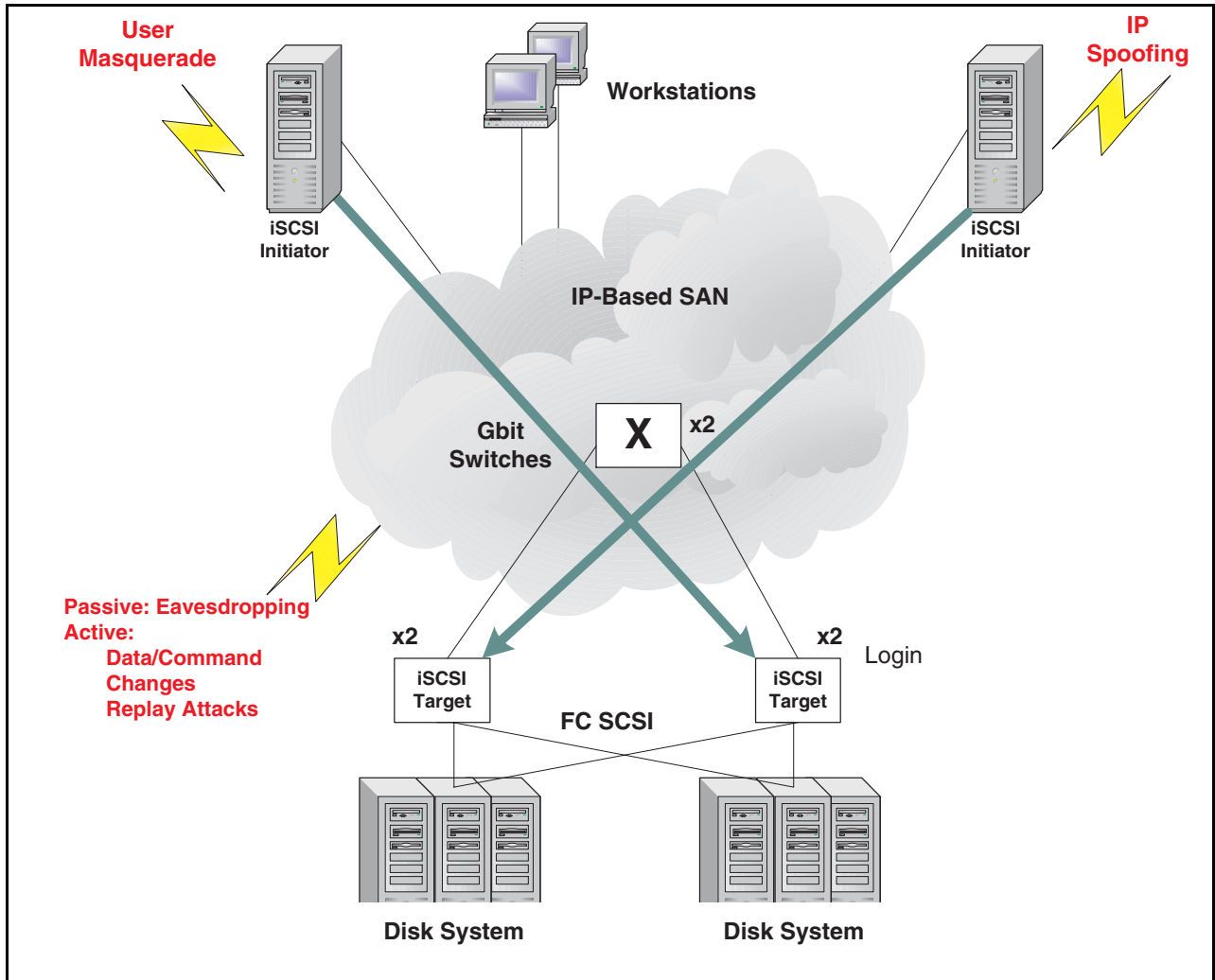


Figure 2 IP Storage Area Networking Security Threats

Challenge 3 - Emerging Architectures

The third key challenge for implementing IPsec for IP Storage is the emerging new hardware architecture for processing of TCP/IP and storage protocols, such as iSCSI, FCIP and iFCP, within IP Storage endpoints. Rather than employing a central processor or a network processor, IP Storage endpoints will employ TOE processors (sometimes called Storage Network Processors). However, the existing model of handling TCP/IP processing on the central processor in servers and GbE switches is not feasible for IP Storage networking. Estimates indicate that a 1 GHz microprocessor would be fully utilized processing TCP to drive a 1 Gbps line rate³.

At full utilization, the system CPU would be unavailable for other applications and unable to meet the latency requirements of IP Storage traffic. Instead, TOE components provide firmware or ASIC-based TCP/IP and, optionally, IP Storage protocol support. TOE products promise to enable iSCSI NICs and IP Storage networking switches, delivering equivalent CPU offload, throughput, and latency as existing Fibre Channel HBAs and fabric switches, and will be required for both the initiator or host and target side of IP Storage networking. The trend to offload TCP processing from the host CPU will become even greater as networking link rates evolve to 10 Gbps.

The absence of a general-purpose packet handling capability, such as that provided by network processors, and the use of TOE components for offloading of TCP and IP Storage protocols in IP Storage endpoints present an important challenge for implementing IPsec for IP Storage in that TOE components will not provide a general-purpose packet processing capability that could be used for processing of specific components of the IPsec protocol stack. This capability must be provided by the security processor.

The three main challenges presented by IP Storage traffic — high data-volume throughput with relatively low packets per second and session creation/teardown rates, the requirement to provide IPsec as an “always-on” function, and the limitations of the emerging IP Storage hardware architectures require a new approach to security processor design. Dedicated security processors that are designed specifically for IP Storage are required.

The Problem with Look-Aside Architectures

Wire-speed IPsec support in routers, firewalls and VPN gateways is typically implemented using a *look-aside* approach (Figure 3). In this type of architecture, IPsec encryption accelerators act as co-processors to network processors. The intelligence for managing the IPsec function and full IPsec protocol support, including packet processing, link layer adaptations, and Security Association (SA) handling, resides within the network processor.

The look-aside approach is sufficient for multi-megabit flows supported by IP security gateways (which provide optional support for IPsec), but it has severe limitations for multi-gigabit data flows. The look-aside approach places a significant burden on the network processor, and requires a high-bandwidth sideband interface for data transfer between the network processor and IPsec accelerator.

3. “IP Storage networking keeps enterprise on its TOEs,” ZDnet Enterprise, 10/3/01

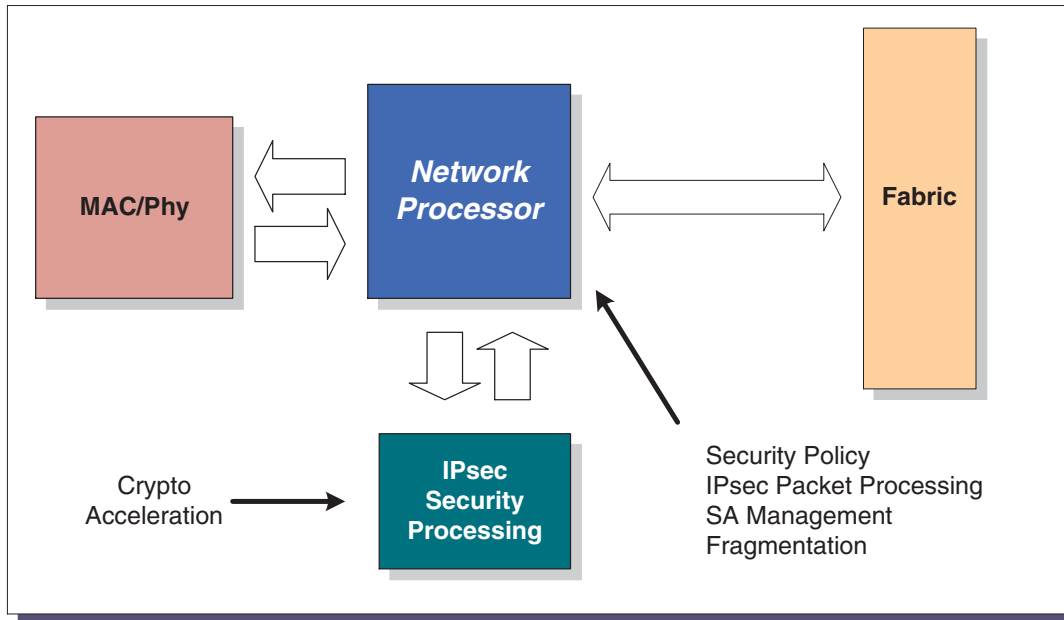


Figure 3 Traditional Architecture for IPsec Acceleration

The look-aside architecture is particularly unsuitable for IP Storage because of the mandatory requirement to encrypt traffic with IPsec. The processing burden from IPsec processing on a central processor would be extreme. Further, because IP Storage systems use TOE processors instead of network processors, the security processor must handle the entire IPsec protocol, and perform the decryption function before the TOE processing takes place.

Finally, the look-aside positioning of the security processor is not viable for the high data rates that are required for IP Storage applications. Neither network nor TOE processors have the high-bandwidth sideports that would be required to handle the required packet traffic. Modifying TOE designs to include such sideports would still provide an inefficient process, as packet traffic would have to enter the TOE processor, travel to the security processor for decryption, and then return to the TOE for TCP/IP processing.

In summary, optimal support of IPsec in IP Storage devices requires a new generation of security processors providing a self-contained solution for *in-line* acceleration of the full range of IPsec functions for multi-gigabit IP Storage flows.

The NetOctave FlowThrough™ Security Architecture - Optimized for Wire-Speed IPsec Support for IP Storage

NetOctave designed the FlowThrough™ Security Architecture in response to the problems associated with look-aside architectures. In the FlowThrough Security Architecture, the security processor is located in the data path, in front of the TOE (Figure 4). NetOctave's FlowThrough Security Architecture is the cornerstone of a new family of security acceleration solutions that fundamentally change the way wire-speed security is delivered for multi-gigabit latency-sensitive applications, such as IP Storage, that require mandatory IPsec support.

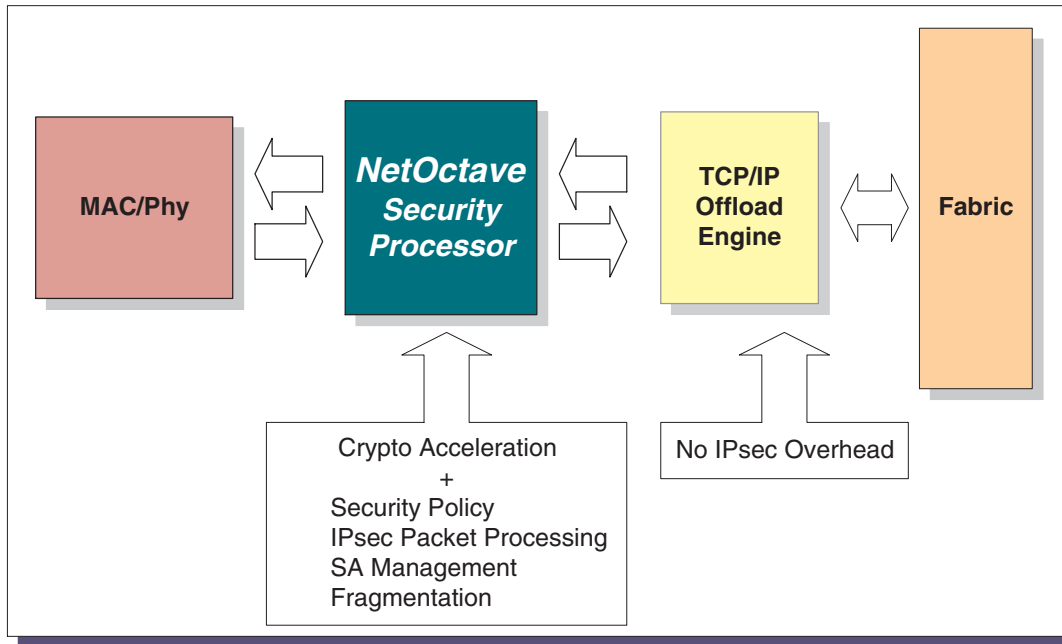


Figure 4 NetOctave FlowThrough™ Security Architecture for IP Storage

The FlowThrough architecture enables security processors that are located directly in the data path, eliminating the inefficiencies of existing “look-aside” security designs. Fundamental to the new architecture is the acceleration of the entire IPsec protocol — essential for when IPsec is implemented in conjunction with TOE elements in storage networking equipment. The new architecture incorporates packet processing, link layer adaptations for Packet over SONET and Ethernet, Security Association handling, and IPsec encryption/authentication functions into silicon-based products. NetOctave's FlowThrough Security Architecture enables high-performance, cost-effective security processors that provide wire-speed performance for encrypted traffic in IP Storage equipment.

About NetOctave

NetOctave is a fabless semiconductor company that provides silicon-based network security solutions for OEM customers. The Company's IPsec and SSL offerings are unique in their ability to support high connection rates and scale to multi-gigabit throughput rates, enabling wire-speed security in next-generation systems. The Company, funded by Intel® Communications Fund and Intersouth Partners, is headquartered in Research Triangle Park, North Carolina. NetOctave's Web site is at <http://www.netoctave.com>. For more information, please contact us at:

- 919.463.9903 by telephone
- info@netoctave.com by email