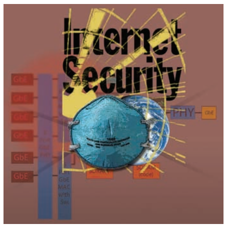
COVER FEATURE

Making the Gigabit IPsec VPN Architecture Secure



By placing the security processors directly in the data path to secure traffic without the aid of additional outside devices or software, the flow-through security device creates a virtual private network that maximizes network processing unit host offload with minimal system integration effort.

Robert Friend
Hifn

Classic corporate wide area networks typically maintain a high-speed connection to an Internet service provider that branch offices can use to connect to the corporate LAN from half a world away. Unfortunately, although they offer great accessibility, everyone using the Internet can see the traffic that passes between a remote office and corporate headquarters over these insecure Internet LAN connections.

A *virtual private network* uses the Internet Protocol security (IPsec) framework to provide confidentiality, data integrity, and end point authentication. These features protect corporate data from being viewed or tampered with while in transit over the Internet. Additionally, the VPN supports data compression, which increases Internet performance between sites.

Metropolitan area networks and *storage area networks* lead the trend toward gigabit Ethernet installations that seek to provide higher speed and better security. The decreasing cost of gigabit devices and their increasing availability in PCs are driving the use of gigabit MANs,[1] while increasing data rates drive the use of gigabit SANs as the bit rate to hard-disk media approaches 1 gigabit per second.

PERFORMANCE REQUIREMENTS

Chipset, network switch, and network interface card vendors continue to provide low-cost gigabit devices, while remote office/branch office and small to medium enterprise networking equipment is quickly migrating from 100 Mbps Ethernet to gigabit networking speeds. ROBO and SME equipment vendors are also adding security features to their products, including their gigabit offerings. Vendors already offer Internet Small Computer System Interface SAN equipment that runs at gigabit speeds and requires low latency. The IETF iSCSI and Fiber Channel over Internet Protocol standards require using IPsec to protect data in flight between SAN nodes.

The performance requirements only increase at the iSCSI SAN end points—iSCSI host bus adapters and target bus adapters—as they must also terminate the Transmission Control Protocol. Although the system designer usually offloads TCP termination to a TCP offload engine device that resides between the physical layer and the network processing unit, the NPU also can handle TCP offloading. TCP offloading typically consumes 1 Hz of NPU bandwidth per bit per second of network bandwidth; thus, terminating 1 Gbps of full-duplex TCP/IP network traffic requires 2 GHz of NPU bandwidth.[2] However, this bps/Hz tradeoff degrades at Gbps speeds due to increased memory transfer and interrupt handling overheads.

Thus, until now IPsec VPN implementations have either used software to perform all VPN functions or added a lookaside security processor that interfaces to the host network processing components through an auxiliary control bus, which removes it from the main dataflow path. The lookaside architecture offloads many compute-intensive IPsec and Internet Key Exchange operations, but lookaside

Published by the IEEE Computer Society

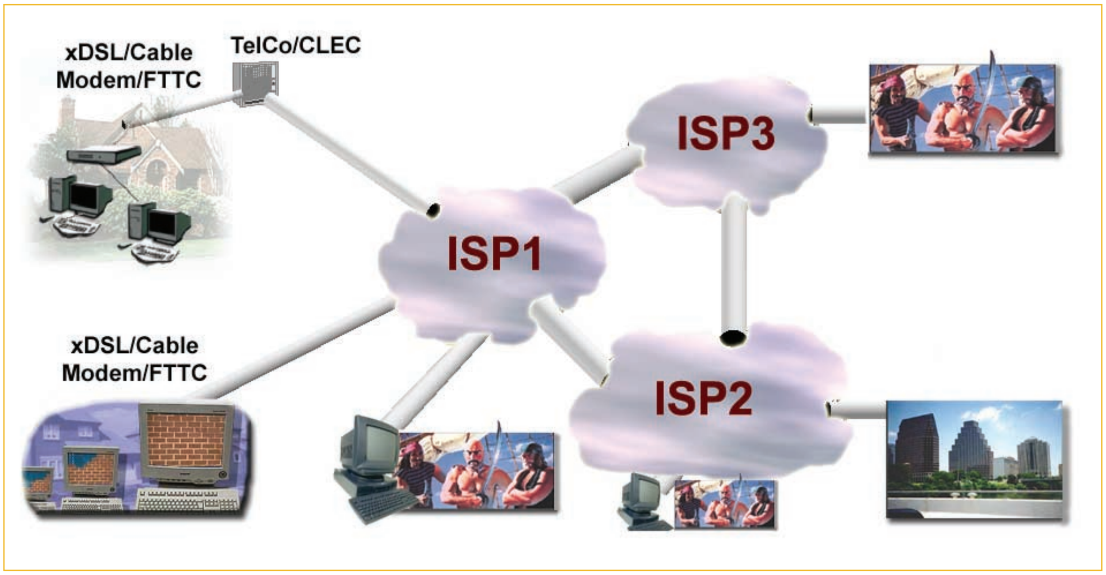


Figure 1. Corporate network data pirates. Threats can come from the remote local office's ISP, from the corporate ISP, or from any ISP across the world.

devices still require the network processing components to handle many packet parsing tasks specifically related to security functions. These devices also create a less efficient data movement architecture. Further, with a lookaside architecture, VPN designers take on more of the security design risk.

To provide network equipment manufacturers with a more complete, efficient, low-risk architecture that adds powerful security processing functionality, the design must place the security processors directly in the data path to secure traffic without the aid of outside devices or software. The flow-through security architecture allows adding security to a system in a way that provides maximum NPU offload with minimal system integration effort.

VPN SECURITY REQUIREMENTS

Anytime a network connection leaves the building, VPN security is required. However, since 80 percent of break-ins occur with insider assistance,[3-5] taking measures to protect sensitive information on the LAN is also a growing trend, especially when integrating SANs on the corporate backbone LAN.

Figure 1 shows that threats can come from the remote office via its local ISP, somewhere near the corporate headquarters via the corporate ISP, or across the world from any ISP. Thus, systems must protect data transmitted between corporate offices using the Internet.

A traditional site-to-site VPN is a static connection that securely extends the corporate LAN across the untrusted Internet to the remote office, where both end points consist of corporate VPN gateways. The VPN gateways decapsulate protected Internet traffic and present it to the local network as LAN traffic. Thus, the remote office appears to be part of the corporate network.

To protect corporate information as it moves across the Internet, between campus buildings, or inside the gigabit Ethernet LAN, OEM designers can use various options to implement gigabit IPsec security solutions. Comparing the cost and performance efficiencies of VPN implementations that use software-only or lookaside security processors with flow-through security processors provides a basis for choosing the best option. In addition to accelerating the VPN function to gigabit speeds, offloading the entire VPN functionality from the host NPU and freeing it to perform other security gateway functions becomes more critical at gigabit speeds.

LOOKASIDE ARCHITECTURE

Traditional security implementations are either NPU-based routers or Pentium-based appliances. In either implementation, the equipment contains minimal hardware for performing physical layer, media access control, and packet buffering. The security equipment also contains an NPU or a Pentium with a PCI chipset to handle all other functions such as firewalling, network address translation, VPN security, intrusion detection, virus detection, and quality of service.

When the VPN performance of next-generation designs drops to unacceptable levels, the options include migrating to a more expensive, higher-performing NPU or adding an additional NPU to offload some of the burden. Either option adds significantly more cost to the design.

The VPN function requires more NPU bandwidth than other security functions because most security processing analyzes certain fields in some headers of some packets. However, the VPN function requires the NPU to process every bit of every packet with compute-intensive encryption and authentication operations. Further, the Internet Key Exchange requires that the NPU perform compute-intensive public-key operations. Unfortunately, software-based VPNs cannot easily perform IKE

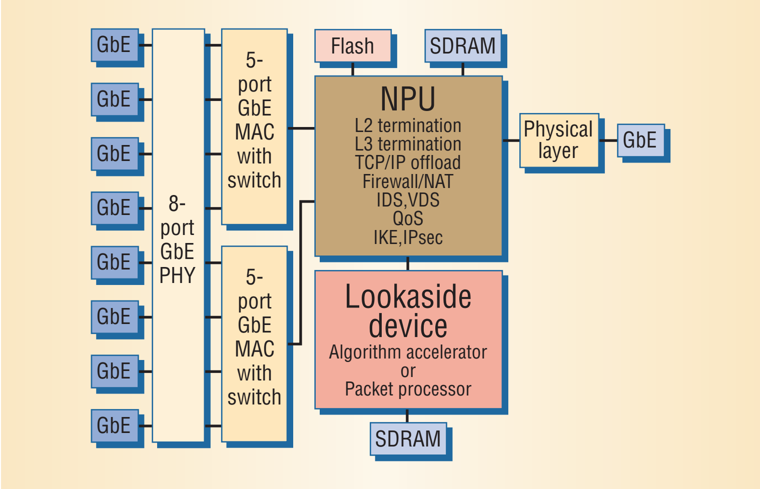


Figure 2. Lookaside security system concept. This simple hardware hookup adds lookaside security functionality to a network processing unit. In this case, the security coprocessor connects to the NPU through a separate control port outside the main dataflow path. PHY: physical layer.

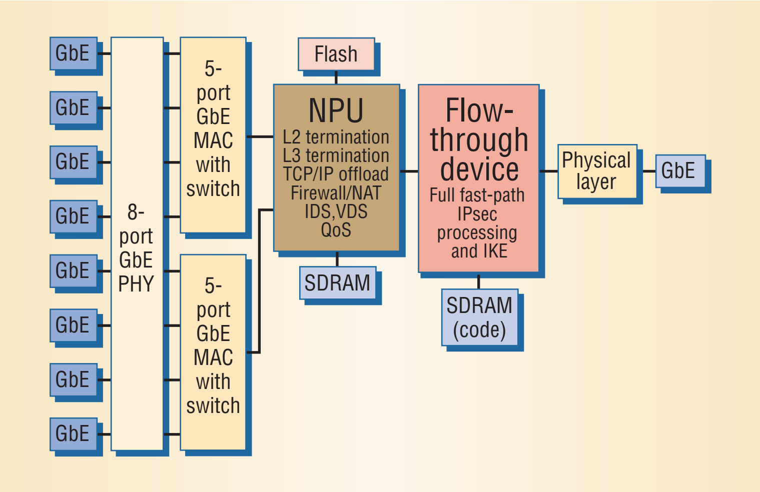


Figure 3. Flow-through security system concept. The architecture offloads all IP security and Internet Key Exchange processing. The flow-through IPsec device contains the security policy and security association databases and the IKE support, all on chip, and the network processing unit performs other security, networking, and quality-of-service functions. PHY: physical layer.

and IPsec VPN functions simultaneously: While the NPU performs IKE, IPsec processing performance temporarily degrades. Current software-based VPNs cannot operate cost-efficiently at gigabit speeds, so developers use security coprocessors to accelerate critical portions of IPsec processing.

Figure 2 shows the simple hardware hookup for adding lookaside security functionality to an NPU. In this case, the security coprocessor connects to the NPU through a separate control port outside the main dataflow path. This lookaside architecture provides the currently preferred option for adding security to VPN routers and appliances. The architecture requires that the NPU handle many IPsec packet parsing tasks and security functions, as well as the associated communication protocol and data movement functions, before handing packets to be processed to a security acceleration integrated circuit. While a lookaside security processor offloads the compute-intensive symmetric crypto and hashing functions, the remaining protocol processing and other ancillary IPsec functions can become a bottleneck on an NPU at gigabit speeds.

A lookaside architecture also requires additional bus bandwidth. Moving data from the NPU to the security processor and back doubles the NPU’s bus bandwidth by requiring two passes across its bus. A flow-through architecture cuts in half both the number of NPU data transfers and the bus bandwidth between the NPU and security processor because its outbound bus connects to another device, such as a network physical layer.

At a minimum, security gateways perform the firewall function and network address translation in addition to other compute-intensive functions, such as intrusion detection, virus detection, payload scanning, and some level of quality of service. Since packet classification is common to all these security functions, the security gateway designer can add other functions modularly and incrementally by enhancing the policy table, then incorporating additional software. However, at some point, the NPU resources will become exhausted and throughput performance will begin to degrade. Since VPN functionality is the most compute-intensive operation, especially at gigabit speeds, adding VPN hardware acceleration to a router or appliance with a firewall and NAT occurs first.

FLOW-THROUGH ARCHITECTURE

The flow-through security architecture provides the next-generation hardware implementation of the IPsec security protocol. This architecture locates the security processor in front of the network processor. The flow-through architecture encapsulates all IPsec VPN functionality and provides more system efficiency than the lookaside architecture. The flow-through security processor handles all the IPsec hardware and software functionality without any outside intervention, letting the NPU operate as if completely unaware of the VPN function.

Figure 3 shows the flow-through architecture, which offloads all IPsec and IKE processing. The flow-through IPsec device contains the security policy and security association databases and the IKE support, all on chip. The NPU can perform other security, networking, and QoS functions without requiring any modifications to the rest of the design. To insert the flow-through device, the system designer literally disconnects the hardware connection between the media access control and physical layer devices, then inserts the flow-through device in between. Thus, the flow-through device acts as a physical layer device to the host port and acts as a media access control device on the network side.

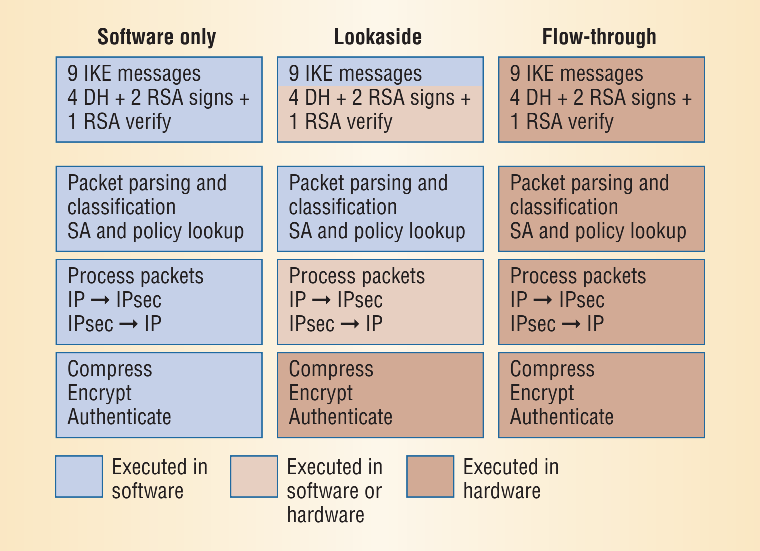
All packet processing and decryption functions for inbound traffic complete before the traffic reaches the network processor. The flow-through security processor's hardware interfaces feed the network or system processor at line rates. This enables predictable VPN performance independent of NPU bandwidth because the NPU only performs IPsec exception processing and policy configuration functions. The flow-through architecture reduces bus bandwidth because it does not require multiple lookaside bus transactions to and from the NPU.

The flow-through solution can aid the original equipment manufacturer in developing VPN equipment because the designer can integrate flow-through devices directly into the data path given that they barely disturb the rest of the system. This can decrease the system design effort required of OEM developers. Flow-through devices can further reduce design risk by incorporating an ICSA Labs certified IPsec/IKE solution, ensuring tested and certified interoperability.

Further, the flow-through solution can accelerate time to market by reducing the software effort to implement the IPsec and IKE protocols—there is no IPsec API to integrate into the system software for processing each IPsec packet. Additionally, the OEM developer doesn't need to maintain the IKE and IPsec software because the flow-through device already incorporates this. In addition, the OEM developer doesn't need to migrate to new IPsec standards because the flow-through device manufacturer supports standards upgrades. For IP storage equipment implementations, the flow-through device is located between a network's TCP offload engine and the physical layer device.

GIGABIT IPSEC ARCHITECTURE COMPARISON

Typical VPN implementations are either PC-based or extensions to routers. Without hardware acceleration, either the Pentium device or the network processor must perform the VPN function. IPsec requires protocol and packet processing in addition to packet encryption and authentication. Similarly, IKE requires message processing in addition to public-key cryptography. However, the cryptographic functions are compute-intensive and thus require a relatively large amount of CPU bandwidth just for encryption and authentication.



Software only	Lookaside	Flow-through
□ 9 IKE messages 4 DH + 2 RSA signs + 1 RSA verify	□ 9 IKE messages ▨ 4 DH + 2 RSA signs + 1 RSA verify	■ 9 IKE messages 4 DH + 2 RSA signs + 1 RSA verify
□ Packet parsing and classification SA and policy lookup	□ Packet parsing and classification SA and policy lookup	■ Packet parsing and classification SA and policy lookup
□ Process packets IP → IPsec IPsec → IP	▨ Process packets IP → IPsec IPsec → IP	■ Process packets IP → IPsec IPsec → IP
□ Compress Encrypt Authenticate	■ Compress Encrypt Authenticate	■ Compress Encrypt Authenticate

□ Executed in software
▨ Executed in software or hardware
■ Executed in hardware

Figure 4. Functional comparison of using a lookaside or flow-through approach to adding Internet Key Exchange and IPsec functionality to a software-only virtual private network system.

Lookaside IPsec algorithm accelerators for implementing gigabit line speeds hit the market in the late 1990s. However, merely accelerating the cryptographic functions still burdened the host CPU or NPU, hampering scalability. Manufacturers started shipping lookaside packet processors in 2000 to alleviate the additional CPU burden of transforming IP packets into IPsec packets, and vice versa. However, this still required the router or appliance vendor to have expert IPsec knowledge. In addition, the I/O bus connecting the CPU to the lookaside security processor must provide double the required throughput to facilitate input and output traffic. Flow-through processors completely offload the host CPU or NPU from any IPsec or IKE processing, thus alleviating technical constraints and facilitating the design process.

Figure 4 compares the host NPU burden required for adding IKE and IPsec VPN functionality to traditional software-only, lookaside, and flow-through systems.

In the lookaside system, the network processor parses and classifies inbound packets, looks up security policy and security associations, and removes IPsec headers as needed before either decoding the encrypted packet in software or forwarding it to the lookaside security processor for decryption and authentication. In the flow-through architecture, all IPsec processing occurs in hardware at line speed. Outbound traffic follows a similar process, only in reverse.

IKE involves more than just modular exponentiation: A single IKE transaction also requires forming nine messages, negotiating security policies, setting up the security association database entry, and performing Diffie-Hellman and RSA public-key operations. Most lookaside security processors

Table 1. Processing costs of adding IP security measures.

Processor	Cryptography (AES/SHA-1)	IPsec protocol and packet processing	IKE protocol and public-key processing	Total Pentium bandwidth	Pentium cost*	Multigigabit security processor cost	Total VPN cost
Software only	7.6 GHz	1 GHz	2.5 GHz	11.1 GHz	$851	$0	$851
Lookaside	0.0 GHz	1 GHz	0.1 GHz	1.1 GHz	$84	$150	$234
Flow-through	0.0 GHz	0 GHz	0.0 GHz	0.0 GHz	$0	$100	$100

*Assumes that a 3-GHz Pentium costs $230.

accelerate the public-key operations, but leave the IKE protocol processing to the host NPU.

IPsec is more than just advanced encryption standard (AES) and secure hash algorithm (SHA-1) as it also requires packet parsing and classification, security policy and storage area lookup, creating and checking security headers, checking security association lifetimes, and updating flow statistics. Most lookaside security processors relegate these tasks to the host NPU.

In Figure 4, the lookaside column represents the functionality of traditional security product offerings from algorithm accelerator or packet processing vendors. Algorithm accelerators only perform encryption and authentication algorithms, and some vendors also support IPComp compression. Packet processors additionally convert from IP packets into IPsec packets, and vice versa.

Some lookaside crypto devices also offer public-key acceleration hardware. Because lookaside devices only offer a portion of the total IPsec and IKE processing functionality in hardware, they might not solve the problem of performing IKE and IPsec concurrently.

In the lookaside configuration, the system processor handles some of the VPN protocol processing tasks, which means that the OEM developer must develop, port, and integrate a significant amount of IPsec and IKE software. Even downloading free IPsec and IKE software from the Web requires the OEM developer to port, integrate, and maintain this software. Thus, incorporating VPN functionality at line speed adds significant software complexity, time to market, engineering risk, and development resource load. Because flow-through processors encapsulate the entire IPsec solution in a single chip, their use can significantly reduce both the knowledge required to incorporate IPsec into a product and the time and risk associated with the development process.

PERFORMANCE AND COST ANALYSIS

Table 1 shows both the processor offload benefits and real dollar cost savings of adding IPsec hardware processors to Pentium-based appliances.[6] The computations were derived using a generic 1-GHz Pentium bandwidth unit to measure the amount of CPU bandwidth required to perform various IPsec functions in software, in order to support a full-duplex gigabit channel that delivers 2 Gbps.

The cryptographic cost for optimized AES-128 assembly code is approximately 280 clocks per 16-byte block,[7] while SHA-1 is 830 clocks per 64-byte block.[8] Converting to Pentium clocks per bit, these measurements yield approximately 3.8 clocks per bit per second, or 7.6 GHz of Pentium bandwidth to support a 2-Gbps channel. Because IPsec protocol processing and packet processing costs vary greatly depending on many factors including the number of security associations, security policies, and lookup implementations and whether an algorithm accelerator or packet processor is used, we estimate that 2 Gbps requires 500 MHz to 1.5 GHz of Pentium bandwidth.

Looked at another way, this calculation approximates 500 to 1,500 clocks per packet for a processing rate of 1 million packets per second. One million packets per second provides line speed processing bandwidth down to a 250-byte packet size, minus the interpacket gap, for a full-duplex gigabit line. Forming an IKE main mode tunnel requires one Diffie-Hellman key agreement (consisting of two exponentiations), one RSA private key, and two RSA public-key operations. Forming an IKE quick mode tunnel requires one Diffie-Hellman operation. We estimate that forming 100 main-mode and quick-mode tunnels per second provides enough key-generation rate to support a gigabit remote-access VPN. Coincidentally, one IKE main-mode and 300 IKE quick-mode tunnels per second require the same amount of public-key software processing.

A 2.1-GHz Pentium 4 requires 4.65 ms for RSA private-key processing, 0.19 ms for 1,024-bit RSA public-key operations, and 3.69 ms for 1,024-bit Diffie-Hellman key agreement computations.[9] Sustaining 100 tunnels per second in software requires approximately 2.5 GHz of Pentium bandwidth. IKE message processing is negligible, requiring less than 100 MHz of Pentium processing to maintain the 100 tunnel/sec IKE main-mode and quick-mode tunnel establishment rate.

Lookaside security processors provide a significant improvement in both CPU offload and cost. However, flow-through processors completely offload the host CPU from IPsec, providing significant additional cost savings compared to looka-

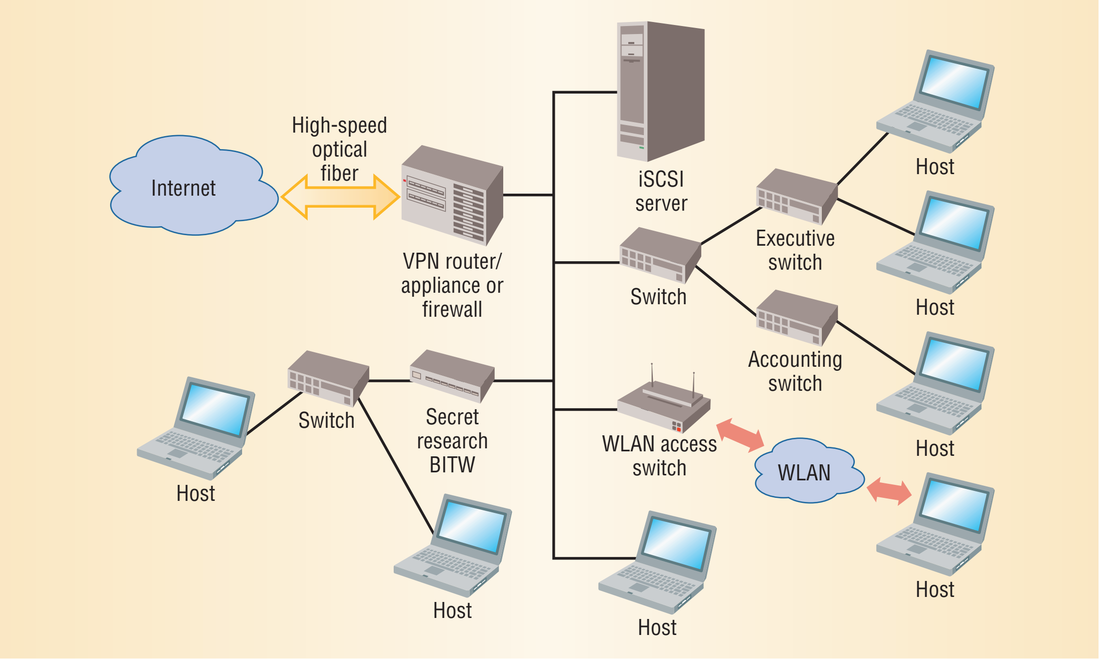


Figure 5. Flow-through security applications in a corporate network. The flow-through architecture can be adapted to boxes, such as gigabit switches and routers; boards, such as network interface cards or line cards; or anywhere a gigabit Ethernet physical layer is located. BITW: Bump in the wire network security.

side processors. This same analysis can be applied to the offload and cost benefits of NPU-based routers by converting a Pentium's processing power in MIPS to an NPU's processing power.

FLOW-THROUGH SECURITY APPLICATIONS

A flow-through architecture reduces the complexity of adding VPN functionality to firewall appliances and iSCSI SANs, and reduces the host system's processing burden. Figure 5 shows some typical corporate network applications for incorporating flow-through security, such as site-to-site or remote-access VPNs located at the edges of the network or between buildings in a MAN configuration.

Sensitive internal LAN segments such as executive, financial, and human resources are also candidate applications, as the flow-through architecture allows the protection normally located at the network edge to migrate inside the LAN to secure networking applications such as iSCSI SANs, WLAN switches, and departmental switches. This protects sensitive connections deeper in the corporate network, providing enhanced security all the way to the subnet. Thus, any system in the corporate network can include IPsec VPN functionality to protect connections that traverse the internal LAN as well as those that extend across the Internet.

When architecting network appliances, the manufacturer must decide whether to buy or design a security solution. OEMs purchase many of the appliance's security software elements, such as the firewall, network address translation/port address translation, intrusion detection, virus detection, and VPNs. The critical difference with the VPN solution is the amount of NPU bandwidth required to support this function at line speed, especially as the gigabit Ethernet becomes ubiquitous.

Engineers also must consider how to incorporate flow-through security solutions in OEM designs when the silicon device is not yet available. To alleviate this concern, the flow-through silicon vendor could first ship a "pass-through" device—printed circuit boards that connect the host port to the network port—that emulates the flow-through security chip in form and fit, only without the security function. Then the OEM can develop and debug the board prior to and independent from flow-through silicon delivery.

The flow-through architecture is targeted more to interface line cards than to service cards. In large switch and routing equipment, interface line cards provide cable connections carrying data to and from the box, while service cards provide services to the data as it traverses inside the box. A backplane bus connects interface line cards to service cards. In the interface line card, each port would have an associated flow-through device. Incoming data would be classified and decoded as it enters the box and heads to the backplane, and data outbound from the backplane would be classified and encoded just prior to exiting the box.

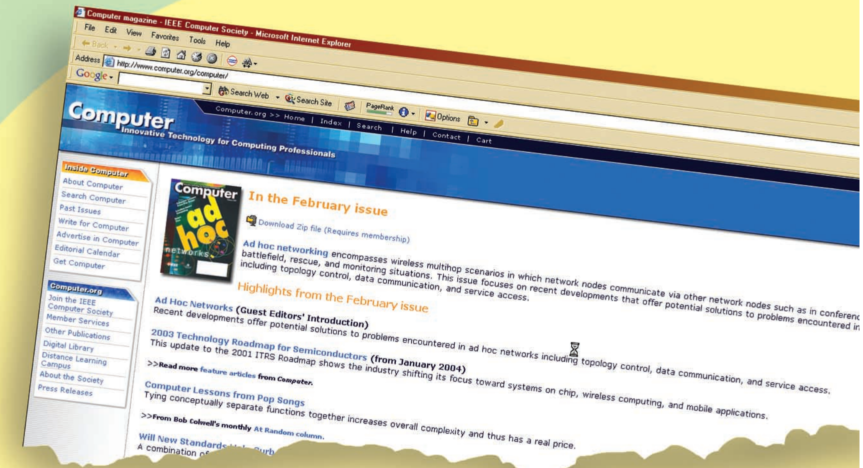
In the service card application, data enters and leaves the service card across the backplane, so the processing on a service card is naturally lookaside. The network processor would use the flow-through device functions in a lookaside architecture. The issue with this configuration is that the flow-through device requires twice as many interface connections to the network processor as the lookaside device.

Future enhancements for lookaside applications could include internally routing the data path connections inside the flow-through device to allow data to exit using the same interface through which it entered. Thus, a flow-through device's complete IKE and IPsec functionality could be packaged for a lookaside application with half the interfaces. While it would provide the same processor offload and development reduction benefits and the same level of integration of a flow-through device with a reduced pin count, this design would require fewer interface connections from the network processor. ■

References

1. "Gigabit Ethernet to Make Headway Despite User Reservations," *Network World High Speed LANs Newsletter*, 17 Feb. 2004; www.nwfusion.com/newsletters/lans/2004/0216lan1.html.
2. A.P. Foong et al., "TCP Performance Re-Visited;" www.cs.duke.edu/~jaidev/papers/ispass03.pdf.
3. Computer Security Institute, "2003 CSI/FBI Computer Crime and Security Survey;" www.gocsi.com.
4. E. Kabay, "Studies and Surveys of Computer Crime;" www2.norwich.edu/mkabay/methodology/crime_studies.htm.
5. D. Verton, "Analysts: Insiders May Pose Security Threat," *Computerworld*, 15 Oct. 2001; www.computerworld.com/securitytopics/security/story/0,10801,64774,00.html.
6. *Computer Edge Magazine*, 27 Feb. 2004; www.computoredge.com/sandiego/.
7. H. Lipmaa, "AES Candidates: A Survey of Implementations;" www.tcs.hut.fi/~helger/aes/rijndael.html.
8. A. Bosselaers, "Fast Implementations on the Pentium;" www.esat.kuleuven.ac.be/~bosselae/fast.html.
9. W. Dai, "Crypto++ 5.1 Benchmarks," 16 July 2003; www.eskimo.com/~weidai/benchmarks.html.

***Robert Friend** is a principal technologist at Hifn, where he evaluates next-generation protocols, technologies, and market segments. Friend is a member of the Internet Engineering Task Force, coauthor of RFC 1967, RFC 1974, RFC 2395, and a contributor to RFC 2118 and RFC 3078, and holds patent 4,920,339 for a switchable bus termination and address selector. Friend received a BS in electrical engineering from the University of California, Los Angeles. Contact him at rfriend@hifn.com.*



In the February issue

Download Zip file (Requires membership)

Ad hoc networking encompasses wireless multihop scenarios in which network nodes communicate via other network nodes such as in conferenc battlefield, rescue, and monitoring situations. This issue focuses on recent developments that offer potential solutions to problems encountered in including topology control, data communication, and service access.

Highlights from the February issue

Ad Hoc Networks (Guest Editors' Introduction)
Recent developments offer potential solutions to problems encountered in ad hoc networks including topology control, data communication, and service access.

2003 Technology Roadmap for Semiconductors (from January 2004)
This update to the 2001 ITRS Roadmap shows the industry shifting its focus toward systems on chip, wireless computing, and mobile applications.

>>Read more feature articles from Computer.

Computer Lessons from Pop Songs
Tying conceptually separate functions together increases overall complexity and thus has a real price.

>>From Bob Colwell's monthly At Random column.

Will New Standards
A combination