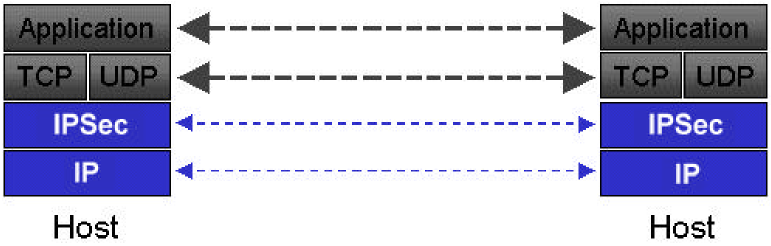
Hardware Implementation of IPSec:
Performance implications

Dr. Sara Bitan, Chief Technology Officer, RADGUARD

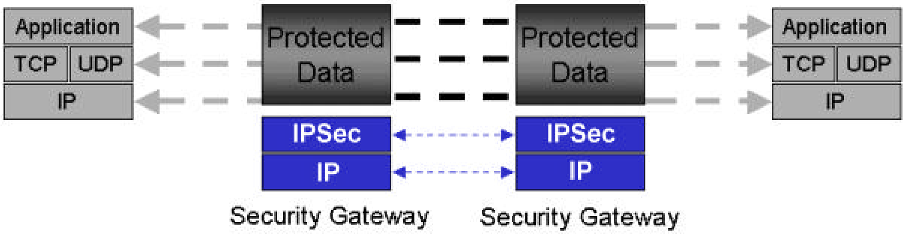
The Internet Protocol Security (IPSec) standard is quickly becoming the workhorse for interoperable network encryption. As a result of the US automotive industry's embracing of IPSec for use in the path-breaking Automotive Network eXchange (ANX) program, IPSec has gained acceptance among vendors of encryption gear throughout the world and has become a requirement of many institutions looking to implement Virtual Private Network (VPN) solutions in their networks.

IPSec is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies ways for securing private information transmitted over public networks. Services supported by IPSec include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering) and replay protection (defense against unauthorized re-sending of data). IPSec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPSec key management protocol, is a series of steps that establishes keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet Engineering Task Force (IETF), IPSec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to interoperate.

IPSec works in two ways. The first, transport mode, is the native way. As shown below, it is the direct relaying of IPSec protected data from host to host. It is used in devices that incorporate IPSec into the way they stack TCP/IP data: for example a laptop outfitted with client encryption.



The second IPSec method is tunnel mode. Here, IP traffic generated by hosts without IPSec support is captured from the wire by a security device, or gateway. As shown in the diagram below, the gateway encapsulates the entire IP packet with IPSec encryption, including the original IP header. It then adds a new IP header to the data packet and sends it across the public network to a second gateway, where the information is decrypted and sent in its original form to the designated recipient.



Tunneling, the focus of this article, is performed by a VPN device which resides at the entrance/exit points of a network. The device modifies (encrypts and authenticates) outgoing traffic and decrypts and authenticates incoming data according to the methods outlined by IPSec.

Tunneling is used to created secure VPNs. It enables distributed private networks to communicate securely over untrusted, public networks. When using tunneling over the Internet, companies can build secure wide area networks (WANs), intranets and extranets at a fraction of the cost associated with traditional methods. VPNs implemented in non-Internet environments, such as frame relay networks, provide comprehensive protection for mission critical applications. In all its configurations, tunneling is a money saving technology, both in terms of reduced communications costs and prevented security breaches.

Today, VPN tunneling is moving from the technological periphery to the networking core. In principle, tunneling represents an effective solution for any organization, large or small, looking to use public backbones to link two or more private networks securely. In practice, VPN tunnels are being built by two kinds of users. The first is made up of smaller companies who see VPNs as an easy and cost-effective way to build a multi-site network. This segment focuses on Internet-based VPNs, which include only a handful of gateways per network.

The second group comprises technology visionaries: large companies who look to tunneling as the communications paradigm of the future. For the visionaries, VPNs represent an effective way to reduce communications while simultaneously securing their existing networks. Tunneled networks for these users can include hundreds of sites and can be structured as hybrid topologies: i.e. a combination of different backbones—Internet and Frame Relay—in one secure communications environment. Examples of companies which fit the visionaries profile are members of the US automotive industry (the Big Three as well as their suppliers and distributors), financial institutions (banks, insurance companies) and R&D divisions of multinational firms.

In production networks of both large and small varieties, the immense amount of data flowing through IPSec gateways can place significant strain on its resources. As the final point of a network, every bit of information leaving or entering the network, even that which is not protected, must be processed to some degree by the VPN device. In order to prevent the gateway from degrading the performance of the network, the gateway must be designed to operate as close to wire speed as possible.

When evaluating the performance of a network device, there are two parameters that are of importance: latency and throughput. Latency is the time it takes for data to pass from source to destination. In terms of a security gateway's relationship to the network it protects, latency is the additional time needed for information to be processed by the gateway before it enters/exits the network. A slow gateway will affect the performance of a network, a wire speed device will operate transparently.

Throughput, or bandwidth, is the number of packets a device can handle in a single unit of time. Throughput becomes important if the bandwidth of a network is wider than its VPN gateway. In such a scenario, the gateway will not be able to process all data. Some packets will be discarded, resulting in potential interruptions to UDP and even TCP.

The relationship between latency and throughput is not straightforward. A device may operate slowly, but at very wide bandwidths, just as a narrow pipeline may operate quickly. With IPSec processing, however, latency and throughput can be correlative. Software VPN solutions--which rely on a CPU burdened with other tasks, such as network management--may introduce significant latency, which in turn may limit throughput. It is precisely for this reason that hardware has become the method of choice for virtual private networking.

Hardware VPN devices provide effective means for accelerating the two distinct, yet related aspects of secure tunneling: IPSec processing and IKE key management.

1. IPSec Processing

IPSec processing differs significantly from normal gateway functions, such as routing or network address translation (NAT). IPSec's digital signature and encryption features are applied to every bit of a data packet, as compared to most gateway functions which only affect packet headers. In addition, the algorithms used in IPSec's keys are far more computation intensive than router processing. In order to cope with the strains of these tasks, IPSec hardware devices, such as those developed by RADGUARD, use individual, dedicated processors to divide IPSec into separate functions – header computation (tunneling and creation of the new IPSec header) and cryptographic processing. With this division of labor, IPSec implementation by hardware allows for the parallel processing of IPSec's component elements. Encryption/decryption, digital signature, and next packet processing are performed independently and at the same time. This off-loads tasks from the VPN device's main CPU, hence increasing bandwidth and reducing latency.

2. Internet Key Exchange

IKE is based on two public key algorithms—the Diffie-Hellman key agreement protocol and the RSA digital signature/encryption algorithm—both of which are based on modular exponentiation. IKE itself is divided into two stages. Main mode, the first phase, contains at least three modular exponentiations, while the second, quick mode, contains one (when perfect forward secrecy is used). Modular exponentiation is resource intensive. It involves complicated, long numbers and multi-precision arithmetic. Using dedicated hardware for modular exponentiation increases the speed of key exchange by several orders of magnitude. It significantly reduces device latency and improves throughput.

Using hardware to perform IKE is advantageous from the network perspective as well. IKE allows network managers to divide their VPN sites into multiple sub-networks (subnets), with each pair of subnets connected via a separate secure channel, or security association (SA) in IPSec terminology. Parallel processing, as made possible by hardware IKE implementation, increases dramatically the number of simultaneous SAs that a security gateway is able to maintain. A software device, operating at peak performance, can maintain dozens of simultaneous SAs per unit of time. A hardware system, in comparison, can maintain thousands. And in the real world, where VPNs can include dozens if not hundreds of security gateways (behind each of which can operate dozens of subnets), the ability to process simultaneously thousands of unique SAs becomes a fundamental requirement.

Hardware IKE implementation, thus, not only reduces latency and increases the bandwidth of VPN devices, but it also directly contributes to the expanded communications potential of the networks security gateways defend.

In recent weeks, the IETF met in Chicago and discussed, among other things, the future of IPSec. In principle, the work of the IPSec team has been completed. Protocol standardization has been achieved and the infrastructure has been built for VPNs to function effectively in production networks. The IETF realized, however, that continued development of IPSec is required to address a number of issues that remain unresolved. As a result, a new committee, entitled "IPSecond," was formed, whose goals are to further improve IPSec and make it even more suitable for universal implementation. The working group's targets include: remote IPSec client support (mobile IP, DHCP); IPSec over non-IP protocols; tunnel end-point (security gateway) discovery; security policy definition; and quality of service (QoS) issues.

As the IETF works to improve IPSec and organizations of all sizes make the transition to secure VPNs, it is clear that hardware-based solutions will have an important role to play in the dynamic secure networking market. In an era of the "virtual office" and the multinational corporation, the ability to link geographically separated offices securely is a business necessity. As we have seen, hardware IPSec implementation provides an effective method for securing wide area links without limiting bandwidth or adding latency. It makes it possible for virtual private networking to realize its potential of improving communications through advanced network security.