The Internet Protocol Security (IPSec) Standard: Clearing up the Confusion

By Cary Hayward
Product Marketing Manager
RedCreek Communications

What is IPSec?

IPSec (Internet Protocol Security Standard) is a framework of open standards for ensuring secure private communications over public networks like the Internet. Based on standards developed by the Internet Engineering Task Force (IETF) IP Security Working Group, IPSec is an industry driven standard that ensures confidentiality, integrity, and authenticity of on an IP network. IPSec is a key component of this standards-based, flexible solution for deploying a network-wide security policy.

IPSec is like the "good housekeeping seal of approval" for privacy, integrity, and authentication. There are two significant benefits to IPSec compliance for the customer: enhanced security features and interoperability.

Enhanced security features give customers the comfort of knowing that IP based communications are using the most secure and comprehensive standard available today for encryption and authentication. Validation is evidenced by the IPSec endorsement by Cisco Systems and Microsoft Corporation on January 20, 1998.

Protocol interoperability means that an IPSec compliant unit will be able to exchange keys and encrypted communications with another IPSec compliant product. This means that the customer can use multiple IPSec vendors for multiple scenarios. IPSec compliance ensures that these two different products can negotiate and maintain a secure association with each other.

What is the ANX Role in IPSec?

The Automotive Network Exchange (ANX) is born out of the Automotive Industry Action Group (AIAG), a not-for-profit trade association based in Southfield, Michigan that has more than 1,200 North American auto and truck manufacturers and their suppliers as its members. ANX has brought attention to the emergence of IPSec as the standard for secure Internet communications by helping people understand the benefits of this TCP/IP based security standard.

When the acute need for a common standards-based network became evident, the ANX quickly looked to IPSec as the standard that would best meet automotive industry trading partner business requirements. The aim of ANX is to provide automotive trading partners with a secure network for electronic commerce and data transfer -- replacing the existing complex, redundant and costly connections throughout the automotive supply chain. By providing tunnel-like connections using the Internet, this IPSec secure virtual private network (VPN) will offer the auto industry significant savings which can ultimately be passed on to consumers as cars become cheaper to manufacture and sell. ANX is at the forefront of showing how IPSec would be a foundation for future network and applications growth.

The ANX is aggressively testing both equipment and service providers and has held four IPSec equipment-interoperability workshops over the past year involving more than 30 vendors. The purpose of the testing was to flush out problems in standard implementations by testing whether the vendors' implementations of the IPSec security standard in firewalls, routers, security hardware, and other devices will interoperate. With standards-based tools, ANX's participants will be able to pick security products that best meet their needs without being limited to a manufacturer's proprietary solution.

ANX was unveiled at AIAG's annual AUTO-TECH Conference and Exposition held in Detroit in August. The pilot was initiated in late 1997, with full ANX implementation beginning in 1998.

Representatives from Chrysler Corporation, Ford Motor Company, and General Motors Corporation interacted electronically with Tier One auto suppliers: Dana Corporation, Dofasco Inc. and UT Automotive, to exchange product engineering data. The first pilot program was initiated in late 1997 with several secure VPN vendors test interoperability of their IPSec solutions. Now that the ANX pilot has begun, the ANX has handed the torch to other vendors who are members of the IETF IPSec to continuing interoperability testing in 1998.

Cisco System's is scheduled to host the next set of IPSec interoperability trials in the first quarter of 1998. This much is clear, ANX has been a major contributor to the definition and roll-out of the IPSec standard.

RedCreek's Participation in the ANX Trials

RedCreek Communications has participated in the ANX sponsored interoperability testing meetings since March 1997 and will continue to be a participant in the Cisco Systems hosted IPSec testing as IPSec protocol interoperability moves forward in 1998.

At the September 22-26, 1997 ANX meeting held in the TimeStep Corporation offices in Kanata, Canada. RedCreek's testing focused on the IPSec Internet Protocol Encapsulated Security Protocol (IPESP) interoperability.

IPESP is the component of the IPSec standard that provides data confidentiality and integrity for IP datagrams. This protocol is used for gateway to gateway and remote system to gateway secure associations where the highest level of security is required. IPESP uses 40/56 bit DES or 112/168 bit Triple DES to encrypt the IP address of the sender along with the entire IP payload. The encrypted original IP datagram is then encapsulated in a new IP packet, using the IPSec gateway unit's IP address as the new source/destination of the packet. This mode provides the highest level of security between gateways as the payload information and the original IP header is encrypted and encapsulated.

At the September ANX meeting, RedCreek demonstrated IPESP interoperability with the following nine IPSec vendors:

- Ascend Communications
- Cisco Systems IOS
- CyLAN Technologies
- Frontier Technologies
- Hewlett Packard
- IBM
- Isolation Systems Ltd.
- Mentat
- Trusted Information Systems (TIS)

RedCreek continues to work closely with its strategic partners and customers in the area of IPSec interoperability between the scheduled ANX meetings.

What is Compliance with the IPSec Standard?

Customers, the trade press, analysts, and the marketing departments of VPN vendors have created confusion on the definition of IPSec Standard compliance. Conflicting and pervasive claims of "IPSec Compliance" by vendors in the network security marketplace have contributed also. Fueling this confusion is the fact that IPSec is comprised of multiple components, which add up to the umbrella Internet Engineering Task Force Internet Protocol Security (IPSec) standard. Each of these components (discussed below) are in various degrees of completion, all are labeled draft; therefore, depending on which vendor a customer asks, a person may get a different definition of what components comprise IPSec.

RedCreek and it's partners use the following encryption and authentication algorithms along with anti-replay services as mandatory components for "IPSec Compliance."

- Cipher encryption algorithm support of 40/56-bit DES and 112/168-bit Triple DES,
- Authentication support through Secure Hash Algorithm (SHA-1) and RSA (MD-5)

These encryption and authentication algorithms along with anti-replay services are selectable for the following IPSec secure VPN modes and Key Management schemes as appropriate:

- IPESP Tunnel Mode
- IPESP Transport Mode
- Authentication Header Transport Mode
- Authentication Header Tunnel Mode
- Manual Key
- ISAKMP/Oakley (Main Mode)
- ISAKMP/Oakley (Quick Mode)

An additional requirement for IPSec compliance is digital signature support of the Digital Signature Standard (DSS) and the RSA standard for digital signatures.

RedCreek and its partners recommend that customers use the list above as a checklist to verify IPSec compliance.

So What Does IPSec Compliance Mean for Customers?

From a customer's perspective IPSec brings two main benefits: strong standardized network security (privacy, integrity, and authentication) inherent with IPSec compliant products, and interoperability with other IPSec compliant vendors.

Security

The customer has the comfort of knowing that IP based communications passing over the network are using the most secure and comprehensive standard available today where encryption, authentication and data integrity are wrapped together. The validity of the IPSec standard as defined in the previous section, was demonstrated by industry leaders Cisco Systems and Microsoft Corporation in the Cisco press release on January 20, 1998. An exciting part of IPSec compliance is that it provides the first open roadmap for customers to integrate their own unique x.509 digital certificates into vendors IPSec compliant products for strong and transparent user authentication. This is where IPSec meets the Public Key Infrastructure (PKI).

The four components of IPSec security are:

Encryption & Encapsulation

The IPSec IPESP standard uses 40/56 bit DES or 112/168 bit Triple DES to encrypt the IP address of the sender along with the entire IP payload. This encrypted original IP datagram is then encapsulated in a new IP packet, using the IPSec VPN unit's IP address as the new source/destination of the packet. Besides the benefits discussed above, this mode provides the highest level of security between gateways as the payload information and the original IP header is encrypted and encapsulated. This offers protection against the most sophisticated man-in-the-middle attacks where datagrams are grabbed in transit between gateways and the hacker uses the source or destination IP address to mount attacks against the enterprise.

Authentication & Anti-Replay

The Secure Hash Algorithm (SHA-1) or MD-5 (RSA) ensure that the data stream is not changed or modified in transit. IPSec anti-replay service ensures that rogue packets are not inserted into the data stream. With anti-replay service, each IP datagram passing within the secure association is tagged with a sequence number. On the receiving end each datagram's sequence number is checked to see if it falls within a specified range. If an IP datagram tag number does not fall within the range, the datagram is blocked.

Key Management & Digital Signatures

ISAKMP/Oakley key management using Internet Security Association Key Management Protocol (ISAKMP) version 8 is the key management protocol that enables customers to use a single standard architecture to secure transactions with different vendor products that are fully IPSec compliant. Manual keying is also a feature of the IPSec standard that allows for "hardwired" interoperability between specific IPSec vendors. The Digital Signature Standard (DSS) and RSA provide proof of authorship for signatures on the digital certificate.

Support of Unique Digital Certificates

IPSec compliance allows for the import of a company's unique signed x.509 v.3 digital certificate into IPSec vendor's hardware and software client. This allows companies to integrate IPSec into their Public Key Infrastructure (PKI) programs for additional levels of user authentication and strong network security.

Interoperability

The second customer benefit is protocol interoperability between the various IPSec compliant products. Protocol interoperability means that a Ravlin unit will be able to exchange keys and encrypted communications with any other IPSec compliant product. Customers can use multiple IPSec vendors for multiple scenarios. For example, the customer may want to use Ravlin hardware for an extranet link to a supplier using Cisco PIX firewalls with integrated Ravlin IPSec PCI cards. IPSec compliance ensures that these two products can negotiate and maintain a secure association with each other.

RedCreek and IPSec

RedCreek Communications has been a leader in the development of the IPSec. In April 1997, RedCreek was the first company to ship the Internet Security Association Key Management Protocol (ISAKMP) in its Ravlin 4 and Ravlin 10 products. As described above, ISAKMP is a critical component of IPSec because it offers the unique scalability and secure privacy features previously unavailable to customers. RedCreek recognized this immediately and elected to implement ISAKMP into its products from the beginning. This early implementation allowed RedCreek to get feedback from customers prior to the ANX IPSec activities.

With the joint Cisco Systems/RedCreek press release announcing the integration of RedCreek's IPSec-compliant Virtual Private Network (VPN) technology into the Cisco PIX(TM) Firewall customers can see that a the world's largest networking vendor is now shipping a IPSec product. The Microsoft Corporation release the same day announcing their intention to integrate IPSec into the Windows NT 5.0 product further signaled clarity for customers considering IPSec. For RedCreek Communications this relationship with the world-wide leader in networking, Cisco Systems, is tangible proof of our IPSec leadership. For customers and partners of RedCreek, it means confidence that their network communications are secure.

2/22/98