

Using Public Key Infrastructure with Interoperable IPSec/IKE Virtual Private Networks

a report by

Michael Spaulding

Senior Security Practitioner

Introduction

Many virtual private networks (VPNs) have core problems associated with them. Either the solution is proprietary, not allowing other vendors to operate with the product, or the security aspects are too weak for most corporations that are looking for a solution to their VPN needs. Therefore, the Internet Engineering Task Force (IETF) created Internet Protocol Security (IPSec) as a flexible, secure and interoperable standard. The standard is centred on interoperability and has gained wide acceptance by many hardware and software vendors.

Internet key exchange (IKE) is an automated key exchange mechanism that is used to facilitate the transfer of IPSec security associations (SAs). Internet Security Association and Key Management Protocol (ISAKMP) provides the standardised layout for negotiating SAs, the generation of cryptographic keys and the refreshing of the cryptographic keys, but is independent of the key determination mechanism that is used. The requirements for ISAKMP are strict due to the unsecured channel – the Internet – by which IPSec will transfer. The core requirements for ISAKMP are that only authenticated parties can be involved in key material exchanges and that it must provide key exchanges over links where no security can be assumed to exist.

Public key infrastructure (PKI) consists of systems that collaborate to provide and implement a public certificate system. The entire concept of PKI is based on the use of a certificate authority (CA). The CA is responsible for issuing, renewing and revoking certificates. Due to the sensitive information that is secured by the CA, trust is a critical issue. If a CA is compromised, many false certificates could be issued and many transactions nullified. Both parties in an IPSec VPN place trust in a CA, which validates both entities to confirm their identities.

IPSec

The benefits of IPSec are that it provides access control, connectionless integrity, data origin authentication, protection against replay attacks and

confidentiality for each IPSec packet. The benefits are achieved by using headers and trailers on each packet, which provide core pieces of information pertaining to authentication, data integrity and confidentiality. The authentication header (AH) addresses data origin authentication, data integrity and replay protection. The encapsulating security payload (ESP) header addresses the same features and also includes data confidentiality or encryption capabilities. By default, IPSec uses the AH as a minimum level for its capabilities. If data confidentiality is desired, the AH is replaced with an ESP header for the encryption feature and the authentication and data integrity components that the AH offer as well.

ESP refers to encryption. It is necessary to consider local, national and international law when developing an IPSec VPN strategy. Due to the concern that many governments place on encryption, powerful encryption algorithms, such as Triple Data Encryption Standards (TDES) or Ron's Code 4 (RC4), could be in violation of the law. This also has to be considered when developing a remote access solution with roaming users travelling internationally. A remote access solution, or any solution where encryption will travel over international boundaries, needs to consider the source and destination of the transmission.

SAs define the parameters for all IPSec communications. All SAs are identified with a security parameter index – a 32-bit value used to differentiate SAs with the same destination address and security protocol. The destination address and security protocol – AH or ESP – are also used to identify the SAs.

All IPSec traffic goes through a security policy database (SPD), which authorises services similar to an access control list (ACL) on a router. A selection of source and destination Internet Protocol (IP) also addresses the particular service that it will carry. IPSec also has a security association database that contains information for each SA, such as AH/ESP algorithms and keys, sequence numbers, protocol mode and SA lifetimes. This allows for complex configurations and for stronger encryption algorithms and data integrity hashes to be used before weaker algorithms and hashes.

Michael Spaulding is Senior Security Practitioner for Versign, Inc. He has held similar roles with Nationwide Insurance, Andersen Consulting and BMW. Hands-on experience is a strong attribute of Mr Spaulding's, having worked for US federal agencies, national and international telecoms providers and major financial institutions globally. His work experience has included firewalls, intrusion detection, penetration testing, security product evaluation and the design of security awareness programs.

The difficulty in using IPSec is that network address translation (NAT) has to be implemented on a vendor-by-vendor basis. When defining the protocol, the IETF did not address the issue of NAT because of IP version six (v6). Fortunately, IPSec is IPv6-compliant and was built to be forward-thinking. In the initial rollouts of IPSec with NAT, most vendors had difficulty with the data integrity hashes failing due to the manipulation of the packets with encryption/decryption processes. Packet filtering will not work properly on encrypted packets.

Internet Key Exchange (IKE)

IKE was created to be a means of automating key exchanges so that little human intervention was needed. Specifically, it is designed to address scalability concerns such as SA negotiations, key generation and refreshing of keys. IKE is also independent of the key determination mechanism.

ISAKMP comprises two phases. Phase one establishes a protection suite with a master key from which all subsequent keys will be derived. Phase one also uses public key cryptography for the authentication of both parties that are involved in the negotiation and generation of the ISAKMP SA and the keys used to protect ISAKMP messages in phase two. Phase one uses processor-intensive operations, therefore, it should be used less often. Phase two is less processor-intensive and should be performed more frequently. After phase one has been activated, phase two is used to establish the IPSec SA and generate and refresh keys for phase two only.

Phase one has two modes from which exchanges can occur – ‘main mode’ or ‘aggressive mode’. Main mode requires a six-message exchange between the initiator and responder, while the aggressive mode requires only a three-message exchange. Main mode is more secure and provides stronger authentication capabilities. Aggressive mode works more quickly than main mode. Phase two has only a quick mode as its method for message exchange. Quick mode is a three-message exchange that is used for the refreshing of key materials and for negotiation algorithms, data integrity hashes and features such as perfect forward secrecy (PFS).

IKE is a truly hybrid protocol within ISAKMP, which implements a subset of the Oakley Protocol and a subset of the secure key exchange mechanism (SKEME) protocol – specifically, the Oakley portions, which are identity protection, authentication and PFS. PFS is a means to prevent a phase-one key, if compromised, from being used to decrypt data. The only exposure that should occur is the data that is related to the phase-two key, limiting data exposure. SKEME provides anonymity, repudiation and quick

key refreshment. IKE provides automated authentication of IPSec peers, negotiations of IPSec SAs, the establishment of the IPSec keys and the enforcement of policies and key management over an unsecured, untrusted channel such as the Internet.

Public Key Aspects in VPNs

PKI aims to achieve a certain level of authentication by creating two-factor authentication. After binding a certificate to a person, computer or domain, a user can be required to be in possession of a certificate and know a password to the certificate in order to enable its use. In a remote-access scenario, certificates are a reasonable choice when compared with token-based systems, due to their cost and flexibility in architecture and use.

The process of using certificates in an IPSec-enabled VPN has some similarities with secure socket layers (SSLs) with client certificates enabled. Like a Web server, a firewall, router or switch would enrol for an IPSec server certificate. The CA or a local registration authority (LRA) would then authenticate the enrolment and, after completing the authentication process, would approve the IPSec server certificate for use, which would then be signed by the CA's root private key. The remote user would have a similar task and would also be authenticated and approved. Once both parties have IPSec certificates, a certificate-enabled VPN can be established. Often, the remote user will load some type of software, a client application or the operating system with IPSec capabilities to store and later establish the VPN.

The basis for deriving the shared secret is carried out by a Diffie-Hellman-style key exchange. The concept of the exchange is that it allows two users to establish a trusting relationship. Public keys are validated by a CA and a secret is established through a zero knowledge key exchange mechanism.

Conclusion

IPSec will enable multiple vendors to interact and enable secure VPNs. Digital certificates will address the concerns of scalability. PKI will also enable strong authentication of users and provide two-factor authentication in scenarios where users can utilise the Internet from remote locations worldwide. In the end, PKI-enabled IPSec VPNs will provide the necessary privacy, authentication and data integrity that companies and individuals are wanting desperately. ■

Additional Information

A longer version of this article may be found in the Reference Library of the CD-ROM accompanying this business briefing.