IPSec

Executive Summary

Cisco Systems is taking a leadership role in developing the IP Security (IPSec) Protocol, a standards-based method of providing privacy, integrity, and authenticity to information transferred across IP networks. The Internet is rapidly changing the way we do business, but even the Internet's rapid growth has been slowed by a lack of security. The Internet is subject to many threats, including loss of privacy, loss of data integrity, identity spoofing, and denial-of-service. The goal of IPSec is to address all of these threats in the network infrastructure itself, without requiring expensive host and application modifications.

IPSec provides IP network-layer encryption. The standards define several new packet formats: the authentication header (AH) to provide data integrity and the encapsulating security payload (ESP) to provide confidentiality and data integrity. Key management and security associations, the IPSec parameters between two devices, are negotiated with the Internet Key Exchange (IKE, but previously known as the Internet Security Association Key Management Protocol or ISAKMP/Oakley). IKE can use digital certificates for device authentication to enable the creation of large encryption networks. Without digital certificate support, IPSec solutions will not scale to the Internet. The IPSec standards are currently in draft format, but are expected to become standards sometime in 1998.

Cisco will offer IPSec in both the Cisco IOS™ software and the PIX Firewall early in 1998. Cisco is also working with industry partners to ensure that IPSec is available on a wide range of systems, including Windows NT, Windows 95, and UNIX.

The Internet holds unlimited promise for changing the way we do business, but not without first addressing the security risks. IPSec provides a key piece of the solution, because it allows security to be embedded at the network layer. It will work in concert with other security mechanisms and help user organizations become global networked businesses.

Cisco Foundation for Network Services

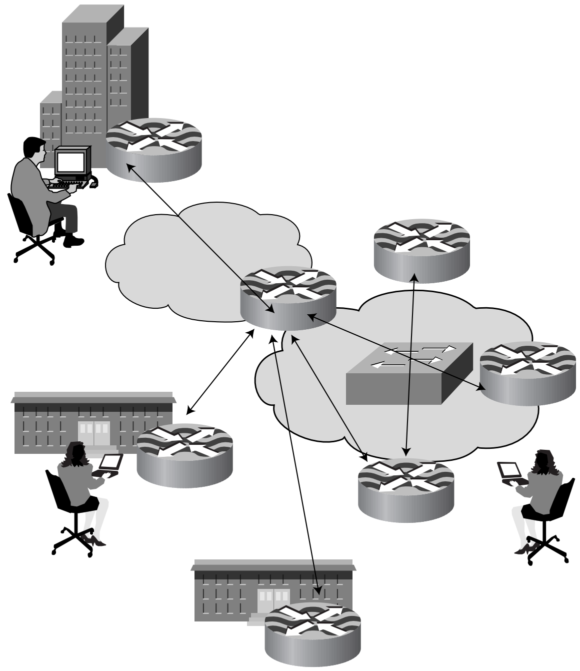
A secure network starts with a strong security policy that defines the freedom of access to information and dictates the deployment of security in the network. Cisco offers many technology solutions to choose from in building a custom security solution for Internet, extranet, intranet, and remote access networks. These scalable solutions seamlessly interoperate to deploy enterprise-wide network security. Cisco's offerings include comprehensive support for perimeter security, user authentication and accounting, and data privacy. Cisco's IPSec delivers a key technology component for providing this total security solution

Privacy, integrity, and authenticity technologies protect information transfer across links with network encryption, digital certification, and device authentication. Cisco is taking a leadership role in the IPSec standardization effort to ensure that the Internet provides a secure foundation for the growth of global networked businesses.

Enabling the Global Networked Business

The Internet is rapidly changing the way we do business. While the speed of communications is increasing, the costs are going down. This unprecedented potential for increased productivity will reward those who take advantage of it. The Internet enables such things as:

Figure 1 Extranets



- *Extranets*—Companies can easily create links with their suppliers and business partners (see Figure 1). Today, they must do so with dedicated leased lines or slow-speed dial lines. The Internet enables instant, on-demand high-speed communications.
- *Intranets*—Most large enterprises maintain unwieldy and costly wide-area networks. While the cost of dedicated lines has been greatly reduced, there is no question that the Internet offers a drastic cost savings.
- *Remote users*—The Internet provides a low-cost alternative for enabling remote users to access the corporate network. Rather than maintaining large modem banks and costly phone bills, the enterprise can enable remote users to access the network over the Internet. With just a local phone call to an Internet service provider, a user can have access to the corporate network.

These and other Internet applications are changing the way businesses communicate. The Internet provides the public communications infrastructure necessary to make this all possible. Unfortunately, the Internet is missing some key components, such as security, quality of service, reliability, and manageability. IPSec is one of the key technologies for providing security as a foundation network service.

Why Do We Need IPSec?

The Internet provides amazing opportunities, but not without some risk. Without the proper controls, your data is subject to several types of attacks. These problem areas are discussed in the sections that follow.

Loss of Privacy

A perpetrator may observe confidential data as it traverses the Internet. This ability is probably the largest inhibitor of business-to-business communications today. Without encryption, every message sent may be read by an unauthorized party as shown in Figure 2. The Computer Emergency Response Team Coordination Center (CERT CC) in its 1996 annual report at the following url:

(http://www.cert.org/pub/annual-reports/cert_rpt_96.html), listed packet sniffers as one of the most common incidents, saying:

“Intruders continued to install packet sniffers on root-compromised systems. These sniffers, used to collect account names and passwords, were frequently installed as part of a widely available kit that also replaced common system files with Trojan horse programs. These kits provided ‘cookbook’ directions that even novice, unskilled intruders could use to compromise systems.”

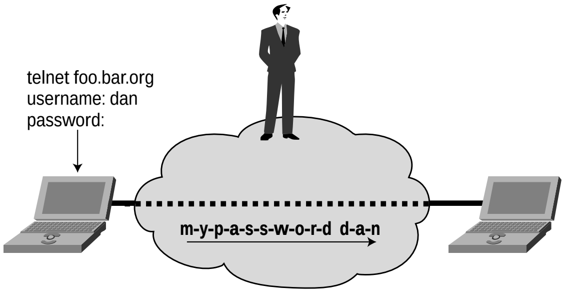


Figure 2 Packet Sniffing in Action

Loss of Data Integrity

Even for data that is not confidential, one must still take measures to ensure data integrity. For example, you may not care if anyone sees your routine business transaction, but you would certainly care if the transaction were modified. For example, if you were able to securely identify yourself to the your bank using digital certificates, you would still want to ensure that the transaction itself is not modified in some way, such as by changing the amount of the deposit as shown in Figure 3.

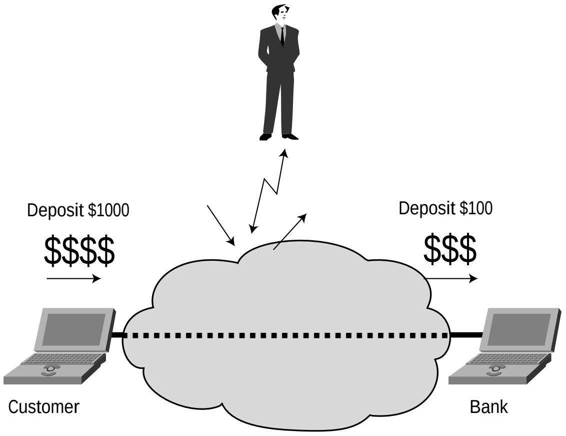


Figure 3 Data Integrity Ensures that Transactions are not Modified

Identity Spoofing

Moving beyond the protection of data itself, you must also be careful to protect your identity on the Internet. As shown in Figure 4, a crafty intruder may be able to impersonate you and have access to confidential information. Many security systems today rely on IP addresses to uniquely identify users. Unfortunately this system is quite easy to fool and has led to numerous break-ins. This was another vulnerability that CERT-CC pointed out in its 1996 annual report, saying:

"We continued to receive several reports each week of IP spoofing attacks. Intruders attacked by using automated tools that are becoming widespread on the Internet. Some sites incorrectly believed that they were blocking such spoofed packets, and others planned to block them but had not yet done so."

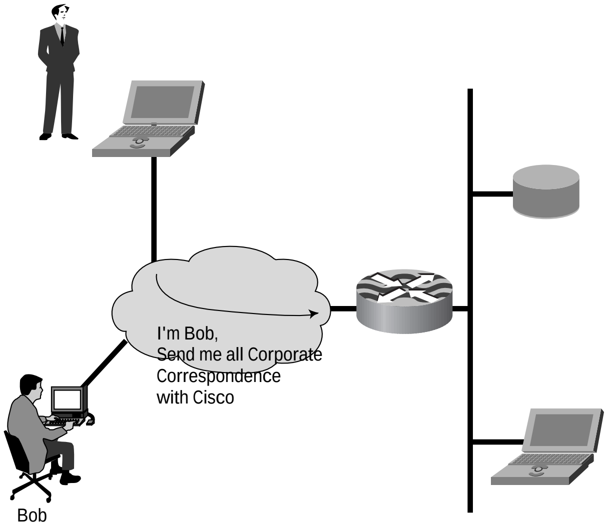


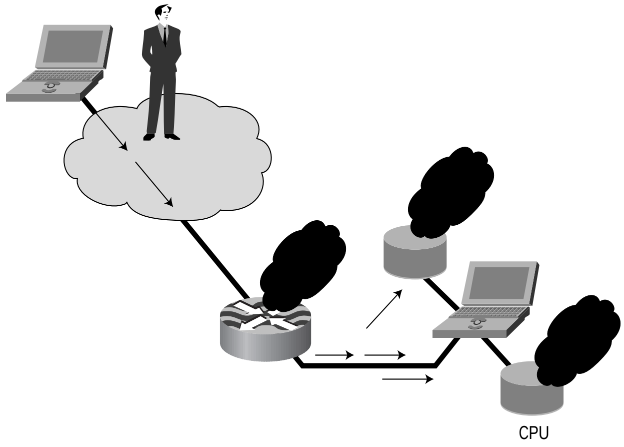
Figure 4 Identity Spoofing

Denial-of-service

As organizations take advantage of the Internet, they must take measures to ensure that their systems are available. Over the last several years attackers have found deficiencies in the TCP/IP protocol suite that allows them to arbitrarily cause computer systems to crash (see Figure 5). The CERT CC reported that:

"Instructions for executing denial-of-service attacks and programs for implementing such attacks were widely distributed this year. After this information was published, we noticed a significant and rapid increase in the number of denial-of-service attacks executed against sites."

Figure 5 Denial-of-service Attacks



IPSec: The Vision

Addressing the Threat

There are no simple answers to Internet security. All solutions require many elements, including a security policy and standards that define what you are trying to protect, a set of procedures to detail how to implement the policy, and a set of technologies that provides the protection.

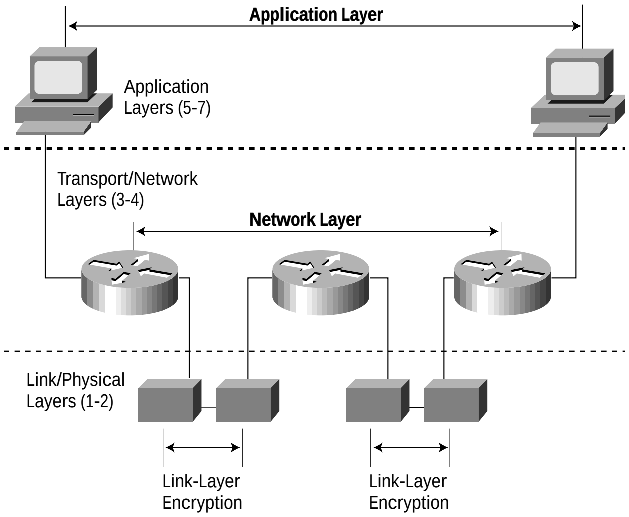
Confidentiality, integrity, and authentication are key services used to protect against the threats outlined in the previous section. Obviously, if data is encrypted while in transit, it is impossible for a perpetrator to observe or modify. The other threats, identity spoofing and denial-of-service, can be prevented with strong network-layer authentication. If devices can positively identify the source of data, then it is much harder to impersonate a friendly device and to anonymously implement a denial-of-service attack.

What Is IPSec?

IPSec is a framework of open standards for ensuring secure private communications over IP networks. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity, and authenticity of data communications across a public IP network. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

Encryption and authentication controls can be implemented at several layers in your computing infrastructure as shown in Figure 6.

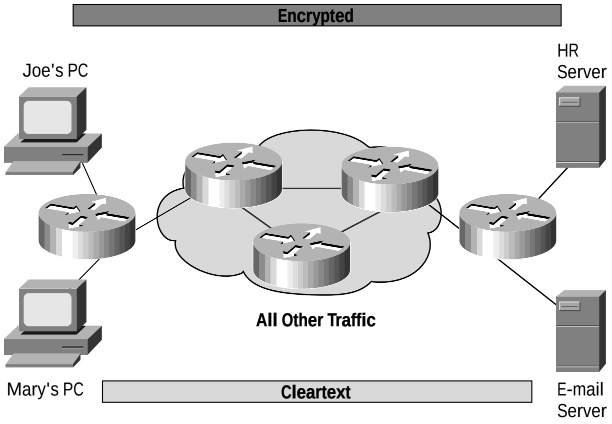
Figure 6 Encryption Implementation Locations



Before IPSec, networks were forced to deploy partial solutions that addressed only a portion of the problem. For example, the secure sockets layer (SSL) provides application encryption for Web browsers and other applications. SSL protects the confidentiality of data sent from each application that uses it, but it does not protect data sent from other applications. Every system and application must be protected with SSL for it to work.

Institutions such as the military have been using link-level encryption for years. With this scheme, every communications link is protected with a pair of encrypting devices-one on each end of the link. While this system provides excellent data protection, it is quite difficult to provision and manage. It also requires that each end of every link in the network is secure, because the data is in cleartext at these points. Of course, this scheme doesn’t work at all in the Internet, where possibly none of the intermediate links are accessible to you or trusted.

Figure 7 Network-Layer Encryption



The routers at the edge encrypt traffic from Joe's PC to the HR server and leave all other traffic unchanged.

IPSec implements network layer encryption and authentication as shown in Figure 7, providing an end-to-end security solution in the network architecture itself. Thus the end systems and applications do not need any changes to have the advantage of strong security. Because the encrypted packets look like ordinary IP packets, they can be easily routed through any IP network, such as the Internet, without any changes to the intermediate networking equipment. The only devices that know about the encryption are the end points. This feature greatly reduces both implementation and management costs.

IPSec Technologies

IPSec combines several different security technologies into a complete system to provide confidentiality, integrity, and authenticity. In particular, IPSec uses:

- Diffie-Hellman key exchange for deriving key material between peers on a public network
- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks
- Bulk encryption algorithms, such as DES, for encrypting the data
- Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication.
- Digital certificates signed by a certificate authority to act as digital ID cards.

Details of IPSec

IPSec combines the aforementioned security technologies into a complete system that provides confidentiality, integrity, and authenticity of IP datagrams. IPSec actually refers to several related protocols as defined in RFC 1825-1829 and several Internet drafts. These standards include:

- IP Security Protocol proper, which defines the information to add to an IP packet to enable confidentiality, integrity, and authenticity controls as well as defining how to encrypt the packet data.
- Internet Key Exchange, which negotiates the security association between two entities and exchanges key material. It is not necessary to use IKE, but manually configuring security associations is a difficult and manually intensive process. IKE should be used in most real-world applications to enable large-scale secure communications.

IPSec Packets

IPSec defines a new set of headers to be added to IP datagrams. These new headers are placed after the IP header and before the Layer 4 protocol (typically Transmission Control Protocol [TCP] or User Datagram Protocol [UDP]). These new headers provide information for securing the payload of the IP packet as follows:

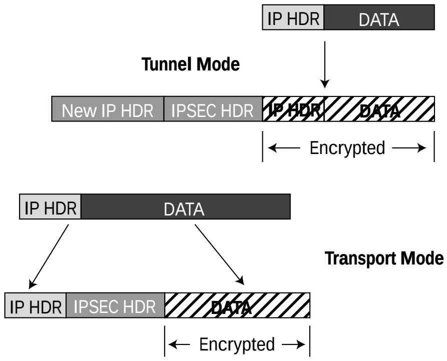
- *Authentication header (AH)*—This header, when added to an IP datagram, ensures the integrity and authenticity of the data, including the invariant fields in the outer IP header. It does not provide confidentiality protection. AH uses a keyed-hash function rather than digital signatures, because digital signature technology is too slow and would greatly reduce network throughput.
- *Encapsulating security payload (ESP)*—This header, when added to an IP datagram, protects the confidentiality, integrity, and authenticity of the data. If ESP is used to validate data integrity, it does not include the invariant fields in the IP header.

AH and ESP can be used independently or together, although for most applications just one of them is sufficient. For both of these protocols, IPSec does not define the specific security algorithms to use, but rather, provides an open framework for implementing industry-standard algorithms. Initially, most implementations of IPSec will support MD5 from RSA Data Security or the Secure Hash Algorithm (SHA) as defined by the U.S. government for integrity and authentication. The Data Encryption Standard (DES) is currently the most commonly offered bulk encryption algorithm, although RFCs are available that define how to use many other encryption systems, including IDEA, Blowfish, and RC4.

IPSec provides two modes of operation—transport and tunnel modes—as shown in Figure 8.

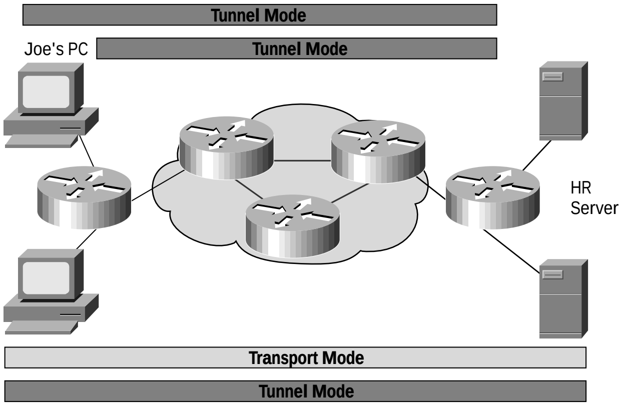
In transport mode, only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. This capability allows you to enable special processing (for example, quality of service) in the intermediate network based on the information in the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. Unfortunately, by passing the IP header in the clear, transport mode allows an attacker to perform some traffic analysis. For example, an attacker could see when Cisco's CEO sent a lot of packets to another CEO. However, the attacker would only know that IP packets were sent; the attacker would not be able to determine if they were e-mail or another application.

Figure 8 IPSec Tunnel and Transport Modes



In tunnel mode, the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. That is, the router performs encryption on behalf of the hosts. The source's router encrypts packets and forwards them along the IPSec tunnel. The destination's router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to enjoy the benefits of IP Security. Tunnel mode also protects against traffic analysis; with tunnel mode an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

Figure 9 Usage of IPSec Tunnel and Transport Modes.

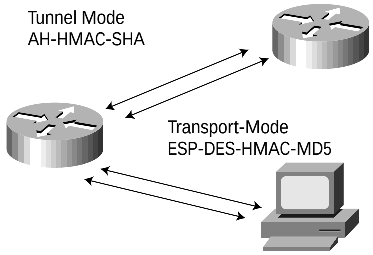


As defined by the IETF, IPSec transport mode can only be used when both the source and the destination systems understand IPSec as shown in Figure 9. In most cases, you deploy IPSec with tunnel mode. Doing so allows you to implement IPSec in the network architecture without modifying the operating system or any applications on your PCs, servers, and hosts.

Security Association

IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide either encryption, integrity and authenticity, or both. When the security service is determined, the two communicating nodes must determine exactly which algorithms to use (for example, DES or IDEA for encryption; MD5 or SHA for integrity). After deciding on the algorithms, the two devices must share session keys. As you can see, there is quite a bit of information to keep track of. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. A Security Association (SA) is a relationship between two or more entities that describes how the entities will use security services to communicate securely. The nomenclature gets a little confusing at times, because SAs are used for more than just IPSec. For example, IKE SAs describe the security parameters between two IKE devices. Further references to a security associations in the rest of this paper will specify whether they are IPSec or an IKE SA.

Figure 10 IPSec Security Associations



The security association is unidirectional, meaning that for each pair of communicating systems there are at least two security connections—one from A to B and one from B to A. The security association is uniquely identified by a randomly chosen unique number called the security parameter index (SPI) and the destination IP address of the destination. When a system sends a packet that requires IPSec protection, it looks up the security association in its database, applies the specified processing, and then inserts the SPI from the security association into the IPSec header. When the IPSec peer receives the packet, it looks up the security association in its database by destination address and SPI and then processes the packet as required. In summary, the security association is simply a statement of the negotiated security policy between two devices as shown in Figure 10.

Internet Key Management Protocol

IPSec assumes that a security association is in place, but it does not have a mechanism for creating that association. The IETF chose to break the process into two parts: IPSec provides the packet-level processing, while the Internet Key Management Protocol (IKMP) negotiates security associations. After considering several alternatives, including the Simple Key Internet Protocol (SKIP) and Photuris, the IETF chose IKE as the standard method of configuring security associations for IPSec.

IKE creates an authenticated, secure tunnel between two entities and then negotiates the security association for IPSec. This process requires that the two entities authenticate themselves to each other and establish shared keys.

Authentication

Both parties must be authenticated to each other. IKE is very flexible and supports multiple authentication methods. The two entities must agree on a common authentication protocol through a negotiation process. At this time, the following mechanisms are generally implemented:

- *Pre-shared keys*—The same key is pre-installed on each host. IKE peers authenticate each other by computing and sending a keyed hash of data that includes the preshared key. If the receiving peer is able to independently create the same hash using its preshared key, it knows that both parties must share the same secret, thus authenticating the other party.
- *Public key cryptography*—Each party generates a pseudo-random number (a nonce) and encrypts it in the other party's public key. The ability for each party to compute a keyed hash containing the other peer's nonce, decrypted with the local private key as well as other publicly and privately available information, authenticates the parties to each other. This system provides for deniable transactions. That is, either side of the exchange can plausibly deny that it took part in the exchange. Currently only the RSA public key algorithm is supported.
- *Digital signature*—Each device digitally signs a set of data and sends it to the other party. This method is similar to the previous one, except that it provides nonrepudiation. Currently both the RSA public key algorithm and the digital signature standard (DSS) are supported.

Both digital signature and public key cryptography require the use of digital certificates to validate the public/private key mapping. IKE allows the certificate to be accessed independently (for example, through DNSSEC) or by having the two devices explicitly exchange certificates as part of IKE.

Key Exchange

Both parties must have a shared session key in order to encrypt the IKE tunnel. The Diffie-Hellman protocol is used to agree on a common session key. The exchange is authenticated as described above to guard against "man-in-the-middle" attacks.

Using IKE with IPSec

These two steps, authentication and key exchange, create the IKE SA, a secure tunnel between the two devices. One side of the tunnel offers a set of algorithms, and the other side must then accept one of the offers or reject the entire connection. When the two sides have agreed on which algorithms to use, they must derive key material to use for IPSec with AH, ESP, or both together. IPSec uses a different shared key than IKE. The IPSec shared key can be derived by using Diffie-Hellman again to ensure perfect forward secrecy, or by refreshing the shared secret derived from the original Diffie-Hellman exchange that generated the IKE SA by hashing it with pseudo-random numbers (nonces). The first method provides greater security but is slower. After this is complete, the IPSec SA is established.

Figure 11 How IPSec uses IKE.

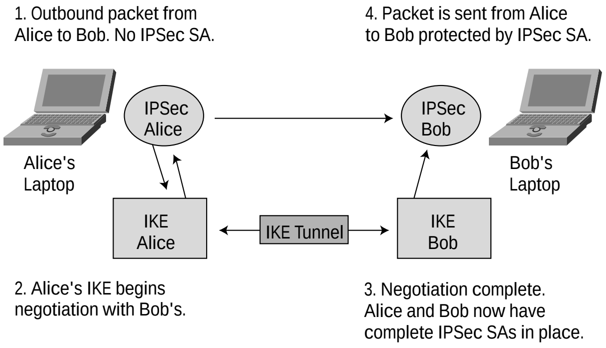
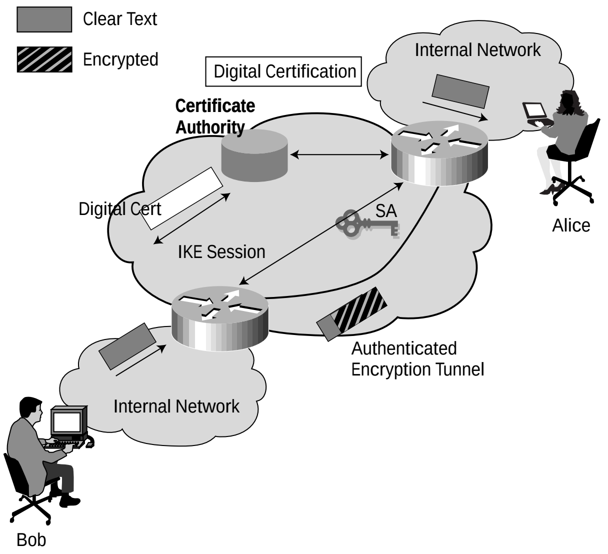

1. Outbound packet from Alice to Bob. No IPSec SA.
4. Packet is sent from Alice to Bob protected by IPSec SA.
IPSec Alice
IPSec Bob
Alice's Laptop
Bob's Laptop
IKE Alice
IKE Tunnel
IKE Bob
2. Alice's IKE begins negotiation with Bob's.
3. Negotiation complete. Alice and Bob now have complete IPSec SAs in place.

Figure 11 illustrates how IPSec uses IKE to set up a security association. Alice's first packet to Bob that should be encrypted triggers the IKE process. The IKE process builds a secure tunnel between Bob and Alice. The IPSec SA is negotiated over this tunnel. Alice can then use this SA to send secure data to Bob.

At this point you're probably trying to remember how all of this fits together, so an example may help. In Figure 12, Bob is trying to securely communicate with Alice. Bob sends his data toward Alice. When Bob's router sees the packet, it checks its security policy and realizes that the packet should be encrypted. The preconfigured security policy also says that Alice's router will be the other endpoint of the IPSec tunnel. Bob's router looks to see if it has an existing IPSec SA with Alice's router. If not, then it requests one from IKE. If the two routers already share an IKE SA, the IPSec SA can be quickly and immediately generated. If they do not share an IKE SA, one must first be created before negotiation of the IPSec SAs. As part of this process, the two routers exchange digital certificates. The certificates had to have been signed beforehand by a certificate authority that both Bob and Alice's routers trust. When the IKE session becomes active, the two routers can negotiate the IPSec SA. When the IPSec SA is set up, both routers will have agreed on an encryption algorithm (for example, DES) and an authentication algorithm (for example., MD5), and have a shared session key. Now, Bob's router can encrypt Bob's IP packet, place it into a new IPSec packet and send it to Alice's router. When Alice's router receives the IPSec packet, it looks up the IPSec SA, properly processes and unpacks the original datagram, and forwards it on to Alice. While this sounds complicated, it all happens automatically and transparently to both Alice and Bob.

Figure 12 IPSec and IKE in Practice



IETF Status

IPSec and IKE are standards-track protocols within the IETF. This means that they will eventually become Internet standards. However, today the standards are still evolving and are only in draft status. This means that while several vendors, including Cisco, have already demonstrated interoperable products, the standards may change in the future.

RFCs 1825 through 1829 describe the original IPSec protocol. These documents have been changed significantly, and new RFCs should appear shortly. The current drafts that describe IPSec and IKE are available at: http://www.ietf.org/html.charters/ipsec-charter.html.

Cisco and IPSec

Cisco's IPSec offering provides privacy, integrity, and authenticity for next-generation applications such as networked commerce. IPSec satisfies crucial requirements for transmission of sensitive information over the Internet. Cisco's unique end-to-end offering allows customers to implement IPsec transparently into their network infrastructures without affecting individual workstations or PCs.

Cisco is taking a leadership role in the IPSec standardization effort to ensure that the Internet provides a secure foundation for the growth of the global networked business.

IPSec is a key technology component of Cisco's end-to-end network service offerings. Working with its partners in the Enterprise Security Alliance, Cisco will ensure that IPSec is available for deployment wherever its customers need it. Cisco and its partners will offer IPSec across a wide range of platforms, including the Cisco IOS software, the Cisco PIX Firewall, Windows 95, Windows NT 4.0, Windows NT 5.0, and UNIX. Cisco is working closely with the IETF to ensure that IPSec is quickly standardized and is available on all other platforms.

Customers that implement Cisco's IPSec will be able to secure their network infrastructures without costly changes to every computer. When you deploy IPSec in your network, applications gain privacy, integrity, and authenticity controls without affecting individual users or applications. Application modifications are not required, eliminating the need to deploy and coordinate security on a per-application, per-computer, basis. This capability provides great cost savings, because only the infrastructure needs to be changed.

IPSec provides an excellent remote user solution. Remote clients can use IPSec clients on their PCs in combination with Layer 2 Transport Protocol (L2TP) to connect back to the enterprise network. The cost of remote access is decreased dramatically, and the security of the connection actually improves over that of dialup lines.

IPSec in Cisco IOS Software

Cisco's version of IPSec in the Cisco IOS software provides industry-leading capabilities while being fully interoperable with a wide range of other vendors. Through the auspices of the Automotive Network Exchange (ANX), Cisco has demonstrated interoperability of Cisco IOS IPSec. IPSec in Cisco IOS software offers the following advanced features:

- Embedded solution through a software-only upgrade does not require any modifications to the network, hosts, or applications.
- *Digital certificate support*—Cisco and Verisign have developed the certificate enrollment protocol (CEP), a protocol for communicating with certificate authorities. Several vendors, including Verisign and Entrust Technologies, will support Cisco CEP and be interoperable with Cisco devices.
- *Flexible security policy*—Extended access lists are used to selectively encrypt or authenticate datagrams. IP packets can be selected by any combination of source or destination addresses, Layer 4 protocols, and ports. Each encrypted stream can be separately authenticated and encrypted. For example, in Figure 12, if Alice is sending Web, e-mail, and telnet traffic to Bob, Alice's router may encrypt the Web traffic with one key, the telnet traffic with another key, and simply pass the e-mail traffic in the clear.
- *Part of a complete security solution*—Cisco IOS software provides many security features, including the Cisco IOS firewall feature set; authentication, access, and accounting (AAA); route authentication; and Kerberos.

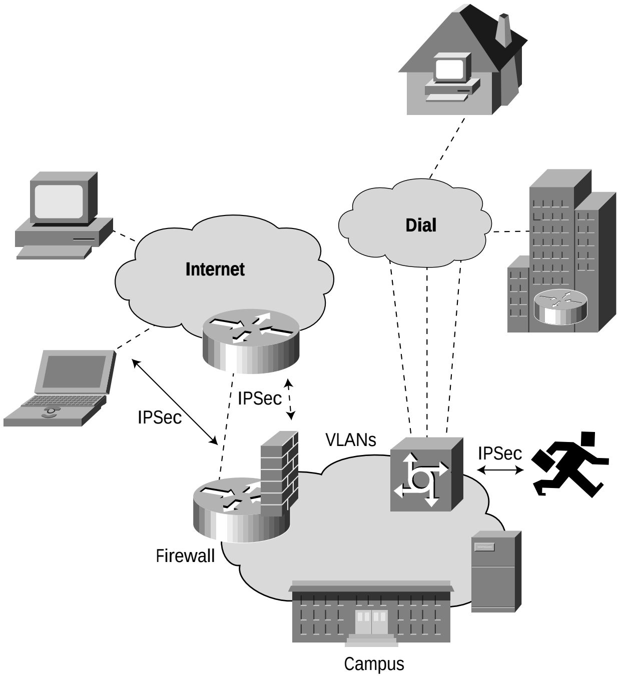
IPSec in Cisco IOS software supports the following standards:

- Current RFCs and Internet drafts for IPSec and IKE:
  - ESP is per draft-ietf-ipsec-esp-v2-04.txt
  - AH is per draft-ietf-ipsec-auth-header-05.txt
  - IKE is per draft-ietf-ipsec-ISAKMP/Oakley-07.txt
  - Entire IPSec implementation is per draft-ietf-ipsec-arch-sec-04.txt (Security Architecture for the Internet Protocol)
- IPSec and IKE denial-of-service encryption algorithms including:
  - DES-CBC with Explicit IV
  - 3DES-CBC with Explicit IV
  - 40-bit DES-CBC with Explicit IV
  - DES-CBC with Derived IV as specified in RFC 1829
- Authentication algorithms:
  - HMAC-MD5
  - HMAC-SHA
  - Keyed MD5 as specified in RFC 1828

IPSec and You

IPSec gives you the power to enable confidentiality, integrity, and authenticity in your network infrastructure. The Internet holds unlimited promise for changing the way we do business, but not without first addressing the security risks. IPSec provides a key piece of the solution, because it allows you to embed security at the network layer. It will work in concert with your other security mechanisms and help your organization become a global networked business.

Figure 13 IPSec everywhere.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at http://www.cisco.com.

Argentina · Australia · Austria · Belgium · Brazil · Canada · Chile · China (PRC) · Colombia · Costa Rica · Czech Republic · Denmark England · France · Germany · Greece · Hungary · India · Indonesia · Ireland · Israel · Italy · Japan · Korea · Luxembourg · Malaysia Mexico · The Netherlands · New Zealand · Norway · Peru · Philippines · Poland · Portugal · Russia · Saudi Arabia · Scotland · Singapore South Africa · Spain · Sweden · Switzerland · Taiwan, ROC · Thailand · Turkey · United Arab Emirates · United States · Venezuela