

IPsec

Internet Protocol Security

Internet Protocol Security

The standard Internet communication protocol is completely unprotected, allowing hosts to inspect or modify data in transit. Adding Interpeak IPsec to your system will resolve this limitation by providing strong encryption, integrity, authentication and replay protection.

Internet communication has no data security built-in, i.e. the protocol is completely unprotected. The application and user data is sent in clear text, hence all your information can be seen by any person, organisation, competitor etc. as the IP packets traverse the Internet. For example, your passwords are sent in the open and can be seen and used to hack your system.

The contents of the IP packets can be modified without the possibility of being detected. This matters when you do not care if anyone sees your information, but would certainly care if someone alters it.

Since packets can be forged, altered etc. it is possible to pose as someone or something else on the Internet. For example, you may only allow your operators to manage your systems, but without protection anyone could possibly do it. This is called Identity Spoofing, i.e. pretending to be someone else by creating IP packets with fake source address. Another bad scenario is that you or your systems could be fed forged important information from sources that you trust.

You also need ways to ensure that a transaction can only be carried out once, i.e. it should not be possible for someone to record a transaction, and

then replaying it verbatim, in order to get an effect of multiple transactions being received by the peer.

Add IPsec to Your System!

Adding IPsec to your system will take care of these threats because IPsec includes *strong encryption, integrity, authentication* and *replay protection*.

Strong Encryption—No one can read your information

Depending on the strength of the encryption algorithm, key length etc. it can be made very hard and costly to decrypt your information. Note that while there is no such thing as absolute security, it can be made extremely time-consuming, i.e. a brute force attack can be made virtually impossible.

Integrity—Modified packets are discarded

By calculating advanced cryptographic checksums on the data one can detect and log modified packets and throw them away.

Authentication—The peer identity is certified

Authentication can be used to sign your data so that others can verify that it is really you that sent it.

Replay Protection—Duplicate transactions are ignored

By using sequence numbers protected by cryptographic measures, duplicate packets can be detected and ignored.

- IPsec IPv4 Gateway and Host [RFC-2401].
- Tunnel/transport mode in any SA combination [RFC-2401].
- AH - IP Authentication Header [RFC-1826], [RFC-2402].
- ESP - IP Encapsulating Payload [RFC-1827], [RFC-2406].
- IPIP - IP in IP tunneling [RFC-1853].
- Bypass/apply/discard IP packet filtering with input/output selectors.
- SNMP/MIB support, "IPsec Monitoring MIB" [draft-ietf-ipsec-monitor-mib-03.txt]
- Key and SA management: "PF_KEY Key Management API", Version 2 [RFC-2367] + openbsd IKE extensions.
- Authentication transforms: HMAC-MD5-96 [RFC-2403], KDPK-MD5 [RFC-1828], HMAC-SHA-1-96 [RFC-2404], HMAC-RIPE-MD-160-96 [draft-ietf-ipsec-auth-hmac-ripemd-160-96-02], KDPK-SHA [RFC-1852]
- Encryption algorithms: ESP_NULL [RFC-2410], DES-CBC with explicit IV [RFC-2405], DES_IV64 [RFC-1829 using a 64-bit IV], 3DES [RFC-2451], CAST-128 [RFC-2144] & [RFC-2451], BLOWFISH [RFC-2451]
- Delivered in ANSI compliant "C" source code.
- Complete ready-to-run RTOS integration with examples, makefiles etc.

Interpeak IPsec features. A complete list of RFCs can be found on page 7.

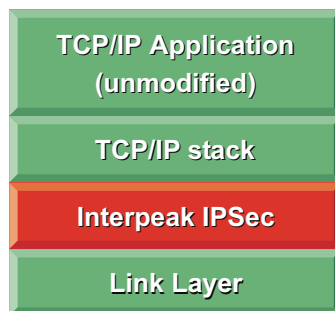
Main IPsec Advantages

Since IPsec is located at the network layer, no modifications to the TCP/IP applications are required in order to secure them. IPsec uses two new IP protocols, Encapsulating Security Payload (ESP) and Authentication Header (AH).

The way this works is that IPsec is inserted below the IP layer, between the TCP/IP kernel and the link modules. IPsec will insert the AH and ESP headers on all outgoing traffic that needs to be secured as well as parse and strip the IPsec headers for incoming IP packets. Applications that use BSD sockets (TCP/UDP/RAW IP) are all transparently and easily secured by including IPsec.

IETF Industry Standard

The industry has already introduced IPsec in full scale and its use is increasing fast. IPsec for Windows NT and 2000 is available from Microsoft. Other vendors have implemented IPsec for Win98, Win95 etc. Solaris 8, the latest SUN Solaris release, has IPsec built-in. IPsec can be added to Linux using a



The picture shows where Interpeak IPsec is inserted to protect a TCP/IP stack.

patch called *freeswan*. The BSD operating systems (OpenBSD, FreeBSD, NetBSD) all have IPsec built-in as well. Finally, basically all network companies that deliver routers, switches, gateways etc. now have IPsec built-in. Cisco, Nortel, etc. all advocate use of IPsec. It is clearly the emerging standard for IP Security.

The listed IPsec vendors including Interpeak IPsec are all compliant with the standards hence can communicate securely and interoperable with each other. The IPsec standard which is specified in about 20 RFC's is maintained by an IETF working group to ensure compatibility.

Configurable Security

IPsec uses a database called Security Policy Database (SPD) which contains information on what security needs to be applied to IP packets. The database uses selectors which can be source and destination IP address, source and destination UDP/TCP port, IP protocol numbers etc. Address ranges and wildcard selectors can be used for added flexibility.

For each outgoing or incoming IP packet the database is searched for a best match entry. If a match is found, the entry contains information on what encryption and authentication algorithms to use, algorithm key lengths, whether to tunnel the packet or not etc. An entry can also specify that no security is necessary. If no entry is found, the packet is discarded. Because of this design, IPsec can be configured to send some traffic unprotected, some partially

protected, and some strongly protected. For example, emails and telnet sessions can be sent encrypted, management could require authentication, HTML web traffic unprotected etc. Furthermore, security per application or service can be changed or added later simply by updating the security policy. Hence, IPsec can be added today, and turned on later when required. The performance penalty on unprotected traffic for including IPsec is less than 0.5% for input traffic and between 0.5% and 5% for output traffic, depending on output selectors and hooks.

Microsoft, HP,
Sun, Cisco,
Linux, BSD,
Telecom and
Datacom Vendors

IPsec vendors.

Versatile Security Solution

IPsec is a versatile security solution because it can perform different security mechanisms. *Authentication* is used to certify that a packet is from the correct sender, *encryption* to ensure data content confidentiality, *integrity* to make sure that the packets have not been modified in transit and *replay protection* to stop duplication of old transactions or thwart Denial of Service attacks.

Secure Sensitive Information

When IPsec is installed on two end hosts, communication security is achieved by having IPsec encrypt and authenticate sensitive information. Traffic that does not need to be encrypted can be sent without applying IPsec, for maximum performance.

Transport Mode

IPsec transport mode is used for host-to-host security and is slightly faster than tunnel mode since there is no need for an extra IP header. In transport

mode, the IPsec ESP/AH header(s) are inserted after the original IP header and prior to the transport layer headers and payload (TCP or UDP header).

The main advantage of IPsec in transport mode is that communication is secure the entire path to the remote system. It does not matter if insecure networks are between the two hosts.

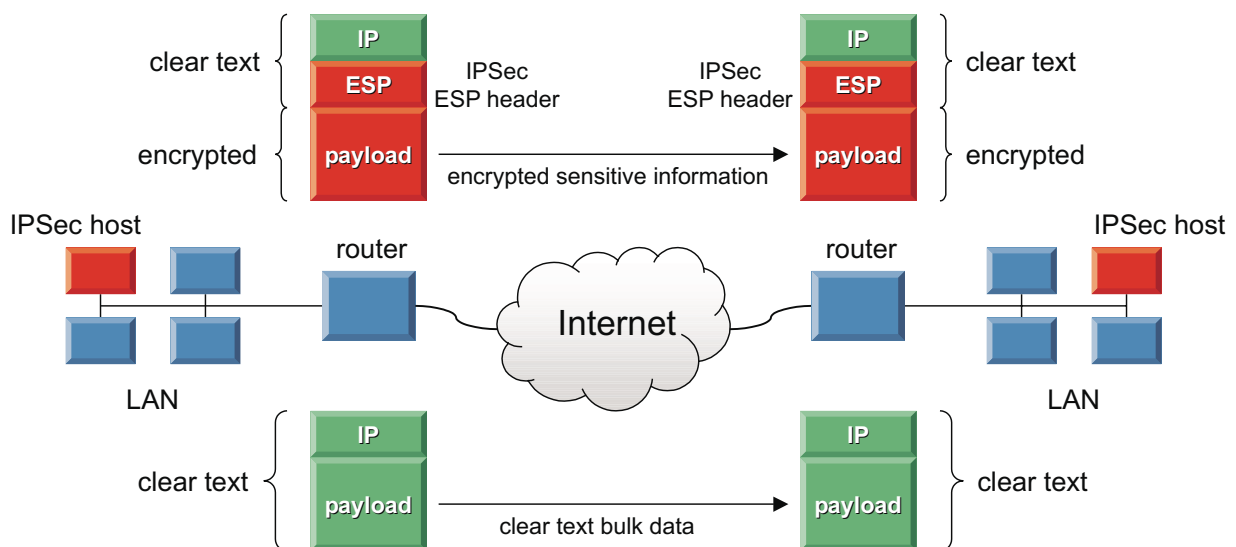
Tunnel Mode

In IPsec tunnel mode, an extra outer IP header is added before the IPsec header. In other words, the new IP

packet contains the IPsec ESP/AH header(s) followed by the original complete IP packet.

High Performance

Since IPsec can be configured per IP application and service, high performance can be achieved for applications that has a larger need for performance than security. The sensitive information can be encrypted and authenticated, and the bulk data where performance is more important and security is not an issue can travel in clear text.



The figure shows two IPsec hosts communicating with each other over the Internet, using the IPsec transport mode. The hosts can secure sensitive information by encrypting it using IPsec as well as send the bulk data unencrypted. Each host is using a policy database to make decisions on what traffic to encrypt and what traffic can be sent without IPsec being applied.

The top two IP packets show how sensitive information is encrypted by IPsec and an extra security header is inserted between the original payload and the IP header. The additional IPsec header (ESP—Encapsulating Secure Payload in this case) is added at the transmitting host for packets that need to be secured and the original payload is encrypted. The receiving end strips the IPsec ESP header and decrypts the payload before

handling the original IP packet and payload to the host TCP/IP stack.

With the strong encryption provided by Interpeak IPsec it is not possible for anyone to snoop and decipher the information sent between the two hosts. Also, it does not matter how many insecure routers the packets pass through, they remain protected the entire path. This set-up requires IPsec on both end systems, but does not require any IPsec on any of the systems between the two hosts.

The bottom IP packets show normal IP communication where no IPsec header is inserted. The bulk data travels unsecured between the two hosts the standard way. The advantage is that maximum performance can be achieved.

Virtual Private Networks

Two or more networks can be combined together to form a Virtual Private Network (VPN) by running IPsec in tunnel mode on the gateways. IP packets sent on the LAN are sent unencrypted. IP packets travelling between the networks are tunneled, encrypted by the local IPsec gateway and sent to the remote IPsec gateway.

In other words, the local gateway encrypts all outgoing IP packets and inserts them in new IP packets destined to the remote gateway. The receiving IPsec gateway unpacks and decrypts the original IP packets and transmits them on its LAN. The major advantage of this set-up, called IPsec tunnel mode, is that the end systems do not need to be modified to enjoy the benefits of IP Security.

IPsec 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.

Simplicity—Multiple targets are secured by a single IPsec gateway

The IPsec gateway performs the necessary encryption on behalf of the hosts. The source's IPsec gateway encrypts packets and forwards them along the IPsec tunnel. The hosts do not need to be modified at all, i.e. they do not even have to run IPsec.

High Performance—Traffic is only encrypted over insecure networks

Packets sent between the hosts on the LAN do not need encryption and are sent in clear text. Only IP packets that need to traverse the public and insecure Internet are encrypted and tunneled to the peer gateway which in turn unpacks the original packets and for-

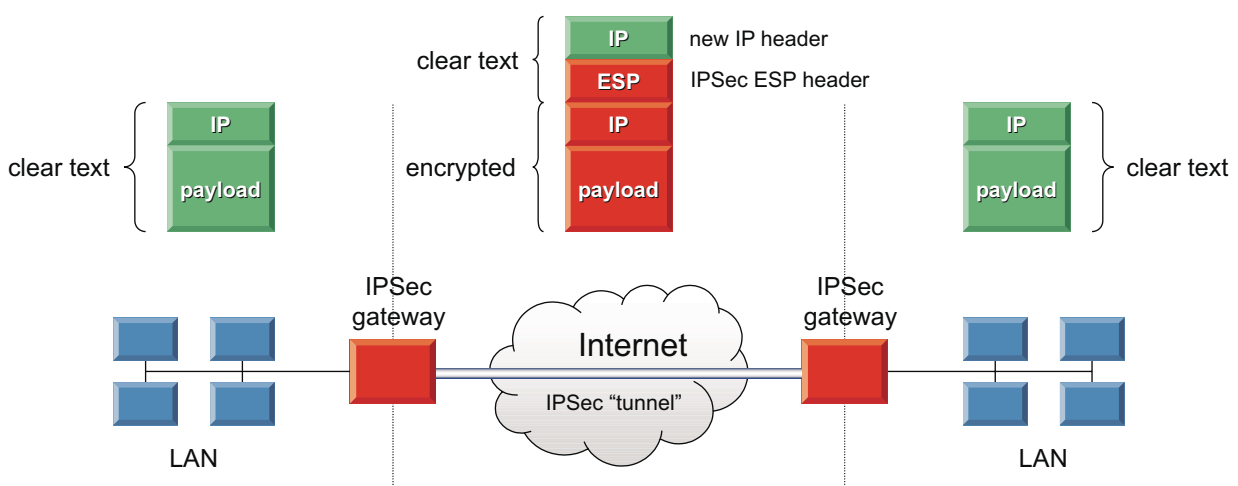
wards it once again in clear text. The advantage of this set-up is high performance since encryption is only applied between insecure networks.

Flexibility—Networks can be located at multiple sites

Since packets travelling between the gateways are tunneled, networks can be physically located at multiple sites. The two sites can share the same IP address network and hosts on both end can communicate securely with hosts on the other side just like if the remote host was on the local LAN.

Compatibility—Old systems can easily be secured

The old systems can be left unchanged and be secured by simply adding a IPsec gateway which secures the packets as they pass through. Even if one only has one host it can be simply secured by adding the IPsec gateway in front of it.



The picture shows two LANs, each with an intermediary IPsec gateway, that can communicate securely with each other using a VPN set-up which effectively combines the two networks into a virtual private network.

The IP packets on the left and right shows how an original IP packet is sent with the payload in clear text. The middle IP packet shows how the local IPsec gateway has added an outer IP

header + the IPsec header (ESP). The original IP packet is encrypted in full and inserted into the new IP packet which is forwarded to the remote IPsec gateway.

The receiving IPsec gateway unpacks, decrypts the original IP packet and forwards it on its local LAN. Routers on the insecure Internet can not see what is sent in the tunnel because all contents are encrypted. The virtual network is private!

RFC Conformance

Interpeak IPsec

RFC Conformance

- RFC 1826 IP Authentication Header [old AH]
 - RFC 1827 IP Encapsulating Security Payload (ESP) [old ESP]
 - RFC 1828 IP Authentication using Keyed MD5
 - RFC 1852 IP Authentication using Keyed SHA
 - RFC 1853 IPIP - IP in IP tunneling
 - RFC 2144 The CAST-128 Encryption Algorithm
 - RFC 2367 PF_KEY Key Management API, Version 2 [+openbsd ext]
 - RFC 2401 Security Architecture for the Internet Protocol
 - RFC 2402 AH - IP Authentication Header
 - RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
 - RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
 - RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
 - RFC 2406 ESP - IP Encapsulating Payload
 - RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec
 - RFC 2451 The ESP CBC-Mode Cipher Algorithms (blowfish, cast, des, 3des)
 - RFC 2857 HMAC-RIPE-MD-160-96
 - RFC 3566 The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
 - RFC 3602 The AES Cipher Algorithm and Its Use With IPsec
 - draft-ietf-ipsec-monitor-mib-03.txt
IPsec Monitoring MIB
 - draft-ietf-ipsec-udp-encaps-09.txt
UDP Encapsulation of IPsec ESP Packets
-

Interpeak Secure Networking Software

Interpeak provides state-of-the-art networking solutions specifically designed for embedded systems. The company's embedded networking and security software is currently used in thousands of applications across the globe.

Headquartered in Stockholm, Sweden, Interpeak operates through a global network of distribution channels and has its own sales and field application force dispersed in strategic locations worldwide, including the USA, Europe, and Asia. For additional information, please visit our homepage www.interpeak.com.

All Interpeak products are trademarks or registered trademarks of Interpeak AB. Other brand and product names are trademarks or registered trademarks of their respective holders. The information in this document has been carefully reviewed, and is believed to be accurate and reliable. However, Interpeak AB assumes no liabilities for inaccuracies in this document. Furthermore, Interpeak AB reserves the right to change specifications embodied in this document without prior notice.

Version 1.22-r5. Copyright © 2005, Interpeak AB. All rights reserved.