

IK2206 – Internet Security and Privacy

Chapter 17 – IPsec: AH and ESP

17.1 Overview of IPsec (READ)

17.1.1 Security Associations

What's an IPsec Security Association (SA)? What information is associated with an IPsec SA?
IPsec security association is a cryptographically protected connection. Associated with each end of the SA is a cryptographic key and other information such as the identity of the other end, the sequence number, and the cryptographic services being used (integrity only, encryption + integrity)

SA defined by SPI, destination address, flag for AH or ESP

How can a receiver (Bob) know which SA to use for an incoming packet? Is the Security Parameter Index (SPI) sent in clear or is it encrypted by IPsec?

The SPI Security Parameter Index enables the receiving system to select the SA under which a received packet will be processed.

?

17.1.2 Security Association Database

* What's an SA database? Who keeps such a database?

The database is maintained by a system which implements IPsec. It allows looking up how we have to transmit a packet to destination X. It provides the SPI, the key, the algorithms, the sequence number etc.

17.1.3 Security Policy Database

What's a policy database? What do you think it contains?

It is similar to a firewall but on the level of IPsec. In the database is specified which types of packets should be dropped completely, which should be forwarded, accepted without IPsec, and which should be protected by IPsec.

If Bob sends a packet to Alice (and the packet is to be protected by IPsec), will Bob's machine consult the policy database or SA database first?

? First the Security Policy Database, because the packet may be dropped.

17.1.4 AH and ESP

What security service(s) (encryption and/or integrity protection) is provided by AH? By ESP?
Authentication Header provides integrity protection only.

Encapsulating Security Payload provides encryption and/or integrity protection.

Can you find any advantage/disadvantage of AH as compared to ESP?

AH:

- + Firewall and routes can look at fields such as layer 4 ports in order to do packet filtering, content screening, or differential queuing.
- Not all fields in the IP Header are integrity protected (some of them are intended to be modified by routers)

ESP:

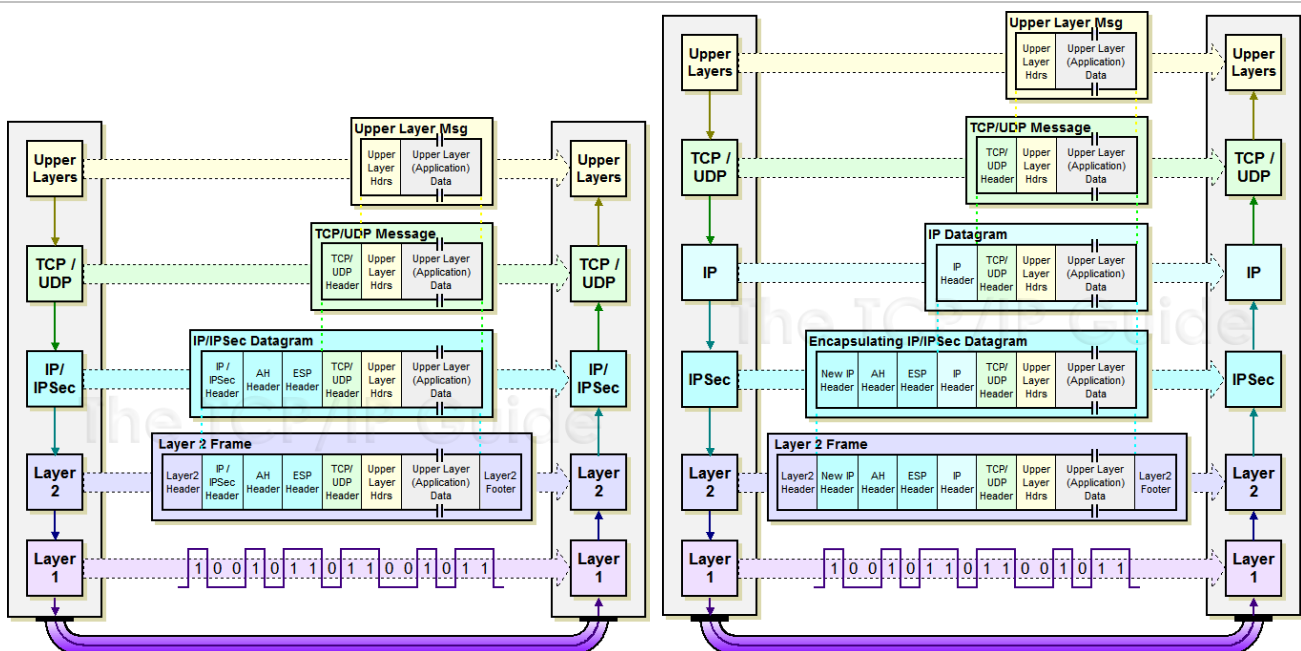
- + provides integrity and/or encryption
- Everything beyond the header is encrypted. Therefore, firewalls or routers can't read fields such as layer 4 information (=ports).
- Usually less efficient, since IP headers are stored twice.

17.1.5 Tunnel, Transport Mode

What's the difference between running IPsec in "transport mode" and "tunnel mode"? How does the packet format differ?

Transport mode refers to adding the IPsec information between the IP header and the remainder of the packet.

Tunnel mode refers to keeping the original IP packet intact and adding a new IP header and IPsec information (ESP or AH) outside.

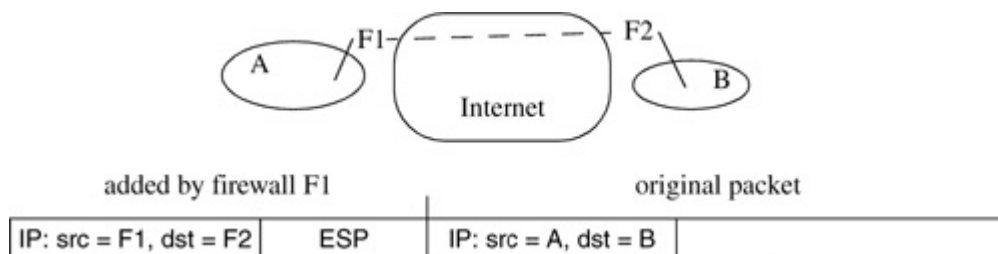


In what situations are "transport mode" and "tunnel mode" suitable? For end-to-end security between two hosts, or between security gateways (firewalls)? End-node to firewall?

- Transport mode is suitable for end-to-end security between two hosts.
- Tunnel mode is used in VPN constellations, where "firewall to firewall" or "endnode-to-firewall" communicate with each other.

What IP addresses are used in the "outer IP header" when running IPsec between firewalls?

In the outer IP header the IP address of the firewalls are used. For example: F1 and F2



If "tunnel mode" could be used instead of "transport mode" why do you think "transport mode" was included in the IPsec standard?

???

17.1.6 Why Protect the IP Header?

AH can be considered superior to ESP since it protects (parts of) the IP header. How would you argue against this?

ESP doesn't provide integrity for the IP header but this could be provided by ESP in tunnel mode.

17.2 IP and IPv6 (READ)

17.2.1 NAT (Network Address Translation)

Why is it difficult to run IPsec across NAT (and NAT) boxes?

An IPsec tunnel cannot go through a NAT box because the NAT box wants to update the IP addresses inside the encrypted data.

Why would one think of encapsulating IPsec on top of UDP? What the benefit of that? How much overhead is added?

There are carefully crafted configurations where IPsec can be used through NAT boxes by encapsulating IPsec packets inside UDP packets.

17.2.2 Firewalls

What may be the problem of running IPsec through Firewalls?

Security is strongest if done end-to-end. IPsec encrypts information on which firewalls like to base decisions, such as the PORT fields in the TCP header that can help them know whether the data is email or telnet.

What is meant with the term "firewall-friendly"? Can you give an example?

Firewall-friendly is the term for disguising traffic to look like something the firewall is configured to pass through. For instance, protocols are being defined to work on top of HTTP to make something like a file transfer.

17.2.3 IPv4 Header (READ BRIEFLY)

How can you know whether an IPv4 packet is protected with IPsec-ESP? IPsec-AH?

If the protocol field of the IP header contains 51 then the packet is protected with AH.

If the protocol field of the IP header contains 50 then the packet is protected with ESP.

What about the use of tunnel mode? What would the protocol field of the outer and inner IP header contain?

If TCP is used with IP using AH, for instance, then the protocol field in the IP header contains 51, and the protocol field in the AH header will be 6 (4 for IP) to indicate that TCP follows the AH header.

17.2.4 IPv6 Header (READ BRIEFLY)

As you will see in later sections the AH header looks much like a regular IPv6 extension header (while ESP does not), however, the interpretation of the "length of this header" field differs. How?

Length of this header is in units of 8-octet chunks, not counting the first 8-octet chunk. AH looks like an Ipv6 extension header, but its PAYLOAD LENGTH is a unit of 4-octet chunks instead of 8-octet chunks. (???)

17.3 AH (Authentication Header) (READ)

17.4 ESP (Encapsulation Security Payload) (READ)

What alternatives do you have if you want to encrypt a packet (ESP and/or AH)?

If you want integrity protection?

We could use AH or ESP

Both encryption and integrity protection?

We could use AH in combination with ESP or ESP only.

Why is it a bit strange to call ESP a "header"?

Headers are usually put to the beginning of the message. ESP puts information before and after the encrypted data.

Where is the payload?

The payload an ESP datagram is stored in a field called DATA.

- In tunnel mode, the payload starts with an IP header and IP payload.
- In transport mode, (when TCP is used on layer 4) the payload starts with a TCP header.

17.5 So, Do We Need AH? (READ)

17.6 Comparision of Encodings (READ)