3.3 IP Security

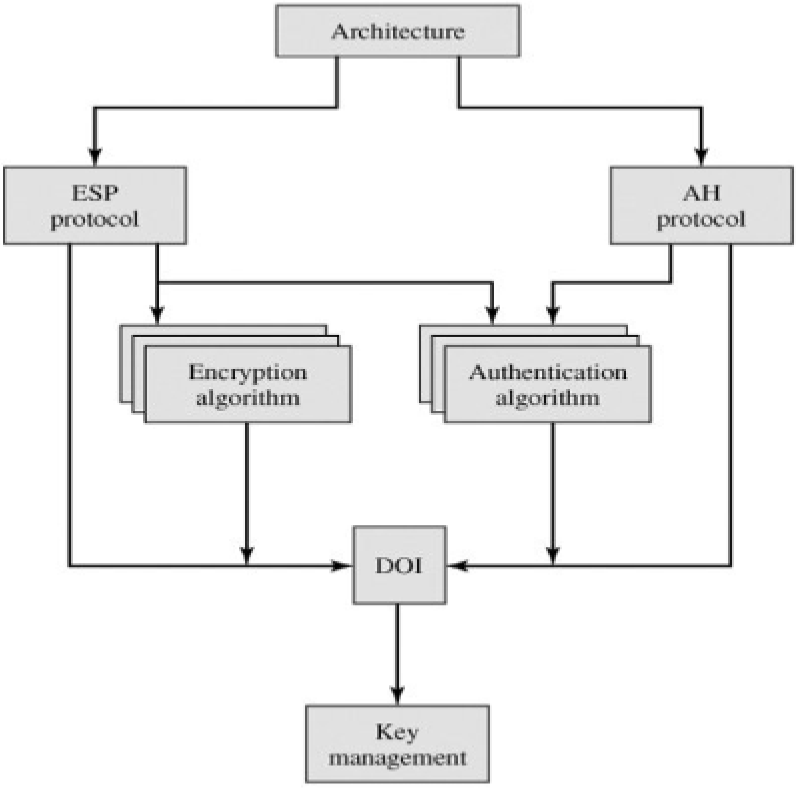
IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples are

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

IP Security Architecture

The IPSec specification consists of numerous documents. The most important of these, issued in November of 1998, are

RFC 2401: An overview of a security architecture
RFC 2402: Description of a packet authentication extension to IPv4 and IPv6
RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
RFC 2408: Specification of key management capabilities



IPSec Document Overview

Architecture: Covers the general concepts, security requirements, definitions, and mechanisms defining IPSec technology.

Encapsulating Security Payload (ESP): Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.

Authentication Header (AH): Covers the packet format and general issues related to the use of AH for packet authentication.

Encryption Algorithm: A set of documents that describe how various encryption algorithms are used for ESP.

Authentication Algorithm: A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.

Key Management: Documents that describe key management schemes.

Domain of Interpretation (DOI): This document contains values needed for other documents to relate to each other.

IPSec Services

IPSec provides security services at the IP layer by enabling a system to select required security protocols.

Two protocols are used to provide security:

- Authentication protocol
- Encryption/authentication protocol (ESP).

The services are

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Security Associations

An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If security exchange is needed in both directions then two-way security association is needed. A security association is uniquely identified by three parameters:

Security Parameters Index (SPI): A bit string assigned to this SA.

IP Destination Address: Only unicast addresses are allowed.

Security Protocol Identifier: This indicates whether the association is an AH or ESP security association

SA Parameters

A security association is normally defined by the following parameters:

Sequence Number Counter: A 32-bit value used to generate the Sequence Number field in AH or ESP headers.

Sequence Counter Overflow: A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA.

Anti-Replay Window: Used to determine whether an inbound AH or ESP packet is a replay or not.

AH Information: Specifies an authentication related parameters like authentication algorithm, authentication key, and key lifetimes.

ESP Information: Specifies the encryption and authentication algorithm, keys, initialization values, key lifetimes

Lifetime of this SA: This is the time interval after which SA must be replaced with a new SA.

IPSec Protocol Mode: This parameter specifies the mode of transfer.

Path MTU: Specifies the maximum transmission unit.

SA Selectors

IPSec provides the user with flexibility in the way in which IPSec services are applied to IP traffic. The means by which IP traffic is related to specific SAs is the nominal Security Policy Database (SPD). SPD contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic. Each SPD entry is defined by a set of IP and upper-layer protocol field values, called selectors. These selectors are used to filter outgoing traffic in order to map it into a particular SA.

The following selectors determine an SPD entry:

- Destination IP Address
- Source IP Address
- UserID
- Data Sensitivity Level
- Transport Layer Protocol
- Source and Destination Ports

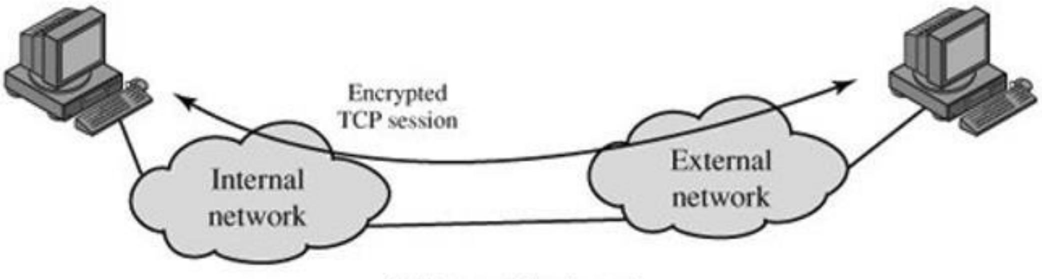
Modes of Transfer

- Transport Mode
- Tunnel Mode

Transport Mode

Transport mode provides protection primarily for upper-layer protocols. The transport mode protection

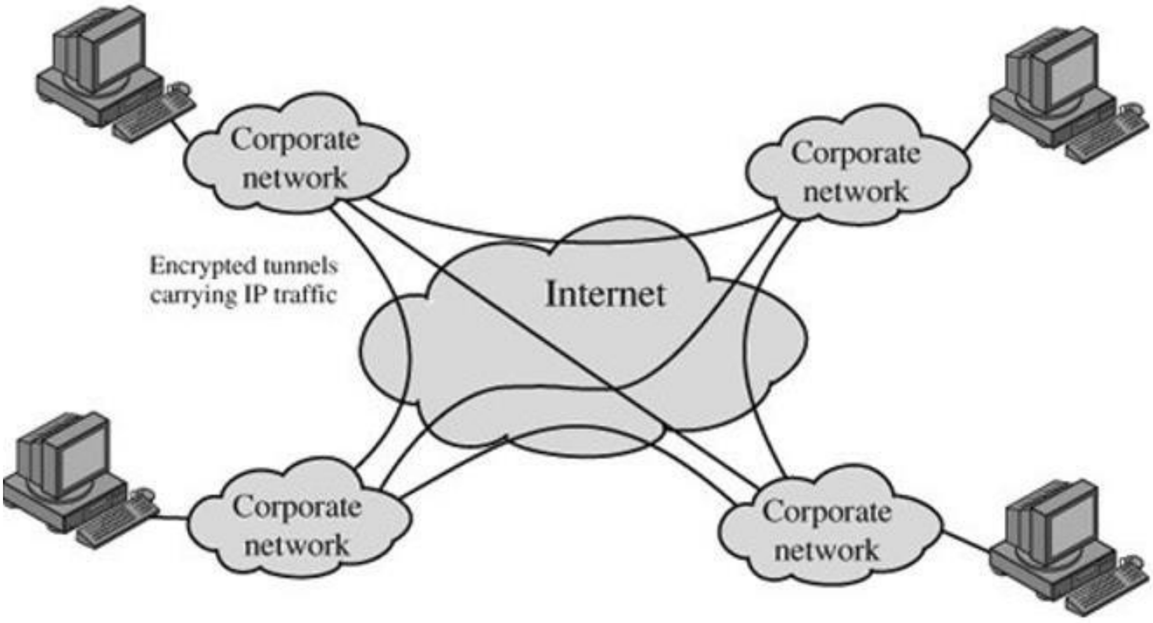
extends to the payload of an IP packet. Transport mode is used for end to end connections.



(a) Transport-level security

Tunnel Mode

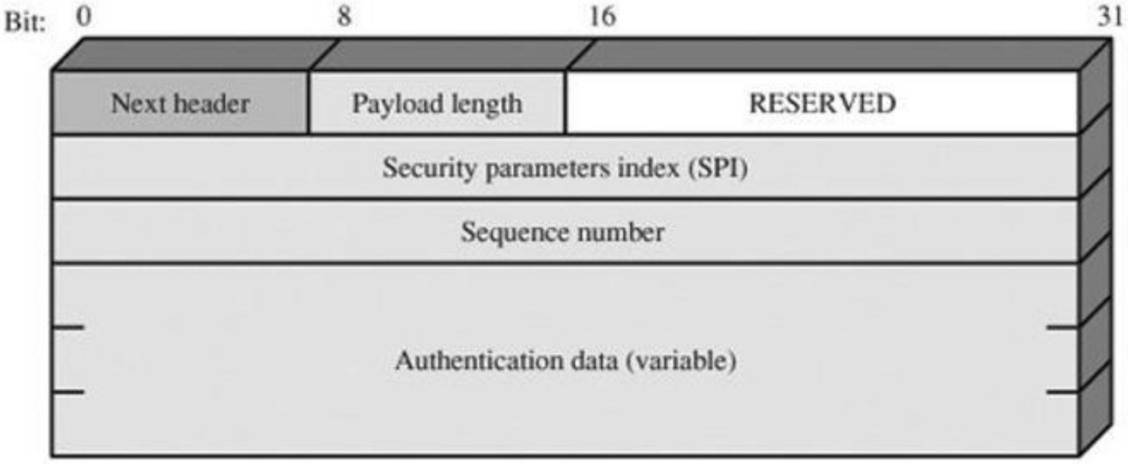
Tunnel mode provides protection to the entire IP packet. Tunnel mode authenticates the entire inner IP and selected portion of outer IP header, IP V6 extension header.



(b) A virtual private network via tunnel mode

AUTHENTICATION HEADER

The Authentication Header provides data integrity and authentication of IP packets. The data integrity assures that modification during transit is not possible. The authentication enables the system to authenticate the user and prevents the address spoofing attacks.


Bit: 0
8
16
31
Next header
Payload length
RESERVED
Security parameters index (SPI)
Sequence number
Authentication data (variable)

The Authentication Header consists of the following fields

Next Header (8 bits): Identifies the type of header immediately following this header.

Payload Length (8 bits): Length of Authentication Header in 32-bit words, minus 2.

Reserved (16 bits): For future use.

Security Parameters Index (32 bits): Identifies a security association.

Sequence Number (32 bits): A monotonically increasing counter value.

Authentication Data (variable): A variable-length which contains the Integrity Check Value.

Anti-Replay Service

A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The Sequence Number field is designed to overcome such attacks.

Generation of sequence number by the sender

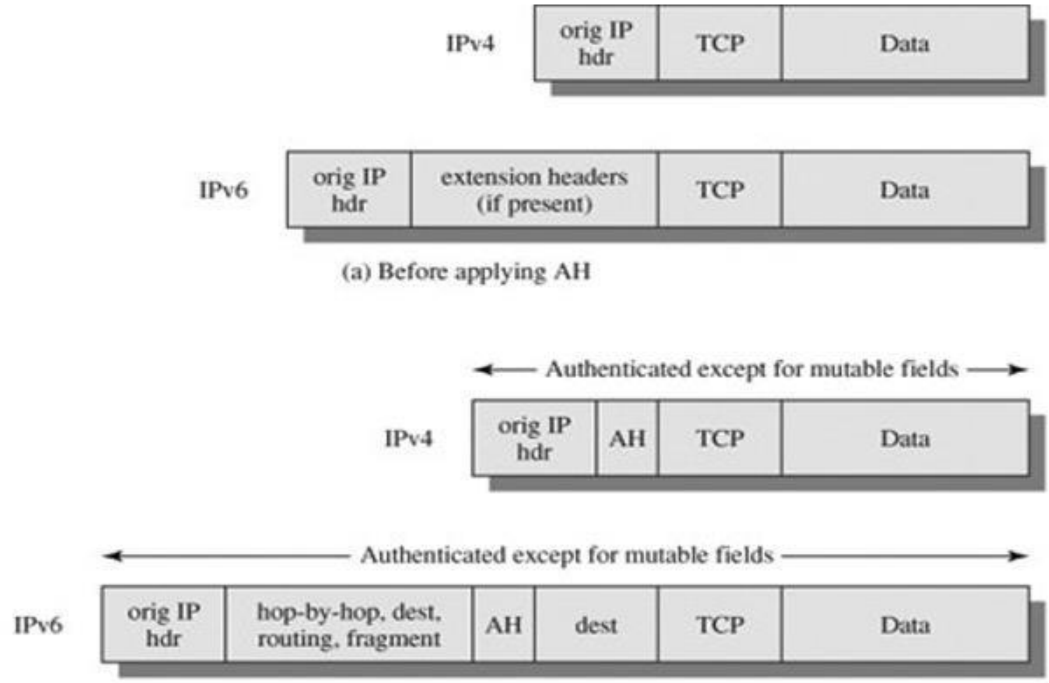
When a new SA is established, the sender initializes a sequence number counter to 0. Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field. Thus, the first value to be used is 1. If anti-replay is enabled the sender must not allow the sequence number field to come back to 0, after cycle past 232 -1. If the limit of 232-1 is reached, the sender should terminate this SA and negotiate a new SA with a new key.

For any incoming packet, the processing

1. If the received packet falls within the window and is new, the MAC is generated.
2. If the packet is authenticated, the corresponding slot in the window is marked as received.
3. If the received packet is to the left of the window, or if authentication fails, the packet is discarded.

Transport mode AH

The AH is inserted after the original IP header and before the IP payload.

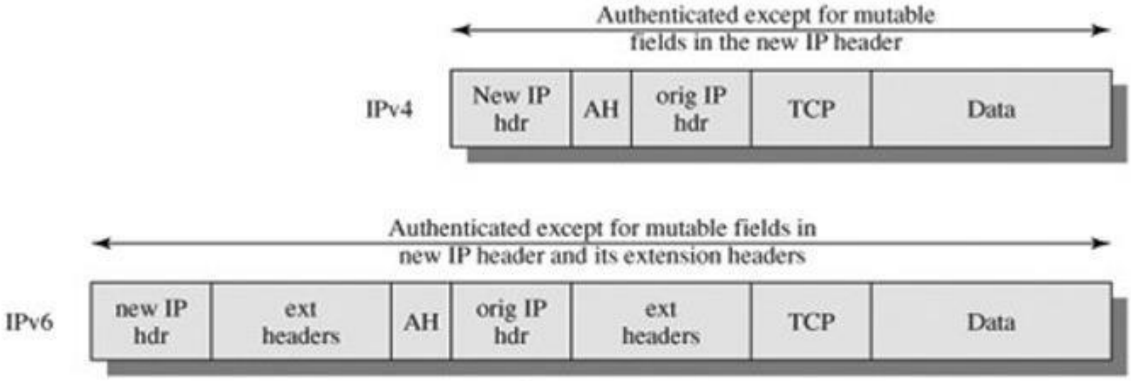

IPv4
orig IP hdr
TCP
Data
IPv6
orig IP hdr
extension headers (if present)
TCP
Data
Authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
Authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

(a) Before applying AH

(b) Transport mode

Tunnel Mode of AH

The entire original IP packet is authenticated and the AH is inserted between the orginal IP header and new IP header.


Authenticated except for mutable fields in the new IP header
IPv4
New IP hdr
AH
orig IP hdr
TCP
Data
Authenticated except for mutable fields in new IP header and its extension headers
IPv6
new IP hdr
ext headers
AH
orig IP hdr
ext headers
TCP
Data

(c) Tunnel mode