V th module

# Electronic Mail Security

Two schemes used for email security :-

- ↳ PGP (Pretty Good Privacy)
- ↳ S/MIME (Secure/Multipurpose Internet Mail Extension)

## PGP

PGP is mainly used for personal email security. It is an effort of a single person Phil Zimmermann PGP provides confidentiality and authentication service that can be used for email and file storage application.

## Features :-

1). Uses best cryptographic mechanisms, includes RSA, DSS and DH for public key encryption. CAST-128, IDEA and 3DES for symmetric encryption. SHA-1 for hash coding.

2). Available free worldwide via the Internet.

3) Platform independent

4) low-cost

5) It was not developed by, nor is it controlled by government or standard organization.

6). PGP is now an Internet standard RFC3156.

## Operational Description

5 Services of PGP :-

1. Authentication
2. Confidentiality
3. Compression
4. Email compatibility
5. Segmentation.

## Authentication

The digital signature service provided by PGP is :-

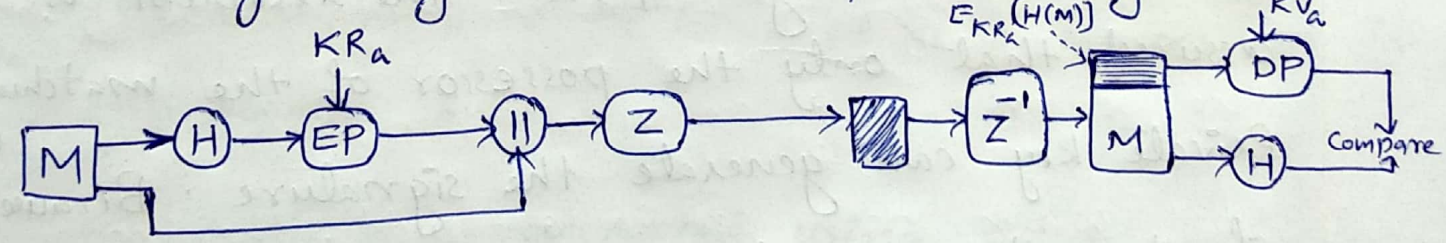



fig :- PGP authentication only.

Where :-

M - Plaintext Message
H - Hash function
EP - Public key encryption
DP - Public key decryption
$KR_a$ - Private key of user A
$KU_a$ - public key of user A
|| - Concatination
Z - Compression using ZIP algo
$Z^{-1}$ - Inverse Compression

Sequence is

1. Sender creates a message
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
4. The receiver uses RSA with sender's public key to decrypt and recovers the hash code.
5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match the message is accepted as authentic.

Here the combination of SHA-1 and RSA provides an effective digital signature scheme.

Due to the strength of RSA the recipient is assured that only the possessor of the matching Private key can generate the signature. Because of the strength of SHA-1 the recipient is assured that no one else could generate a new message that matches the hash code and hence the signature of the original message.

## 2. Confidentiality

In PGP Confidentiality is provided by encrypting message to be transmitted or to be stored locally as files.

Confidentiality service provided by PGP :-

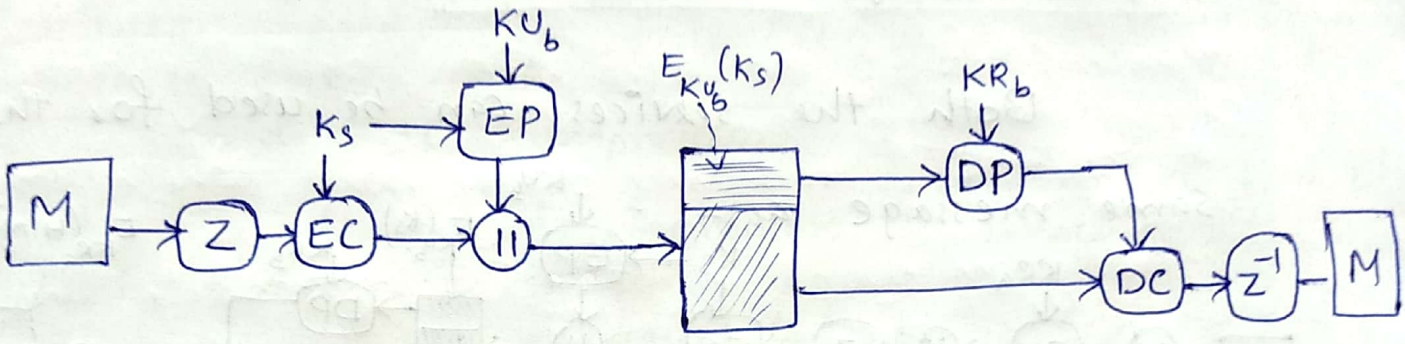



fig:- PGP Confidentiality only.

where :- EC - Symmetric Encryption
DC - Symmetric Decryption
Ks - Session key used in Symmetric Encryption algo.

The sequence is :-

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only
2. The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key
3. The session key is encrypted with RSA, using the recipient's public key, and is prepended to the message.

4. The receiver uses RSA with its private key to decrypt and recover the session key

5. The session key is used to decrypt the message.

## Confidentiality and Authentication

Both the services can be used for the same message as:-

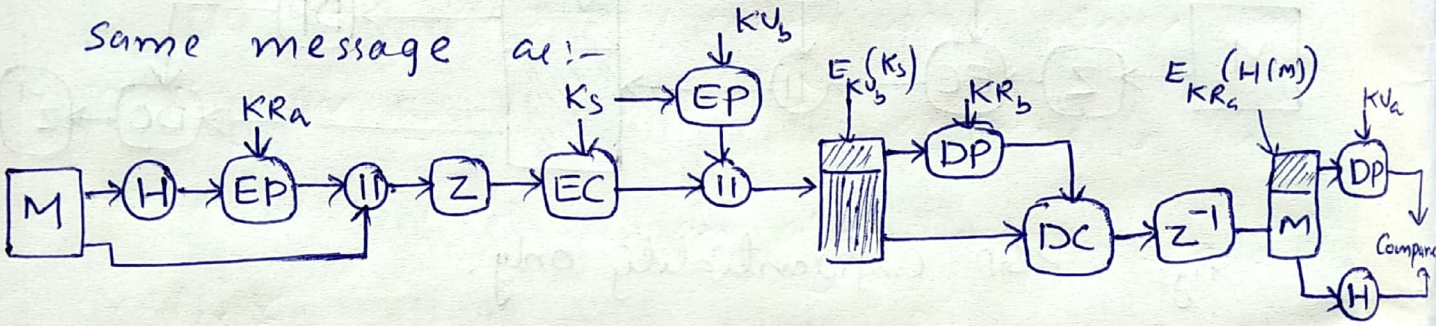



fig:- Confidentiality & authentication in PGP

Here first a signature is generated for the plaintext message and prepended to the message then the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES) and the session key is encrypted using RSA.

ie when both services are used, the sender first sign the message with its own private key, then encrypts the message with a session key and then encrypts the session key with the recipient's public key.

## 3. Compression

PGP compresses the message after applying signature but before encryption. This has the benifits of saving space both for e-mail transmission and for file storage. Compression algo used in PGP is **ZIP**.

Z - indicates compression
$Z^{-1}$ - indicates decompression

} placement of Z at $Z^{-1}$ is critical in algo:-

* (1) The signature is generated before compression for two reasons:-

a) It is preferable to sign an uncompressed message so it is free of the need for a compression algorithm for later verification.

b) Different version of PGP produce different compressed forms. Applying the hash function and signature after compression would constrains all PGP implementations to the same version of the compressed algorithm.

(2) Message encryption is applied after compression to strengthen cryptographic security. Because the compressed message has less redundancy than the original plaintext, cryptanalysis is difficult.

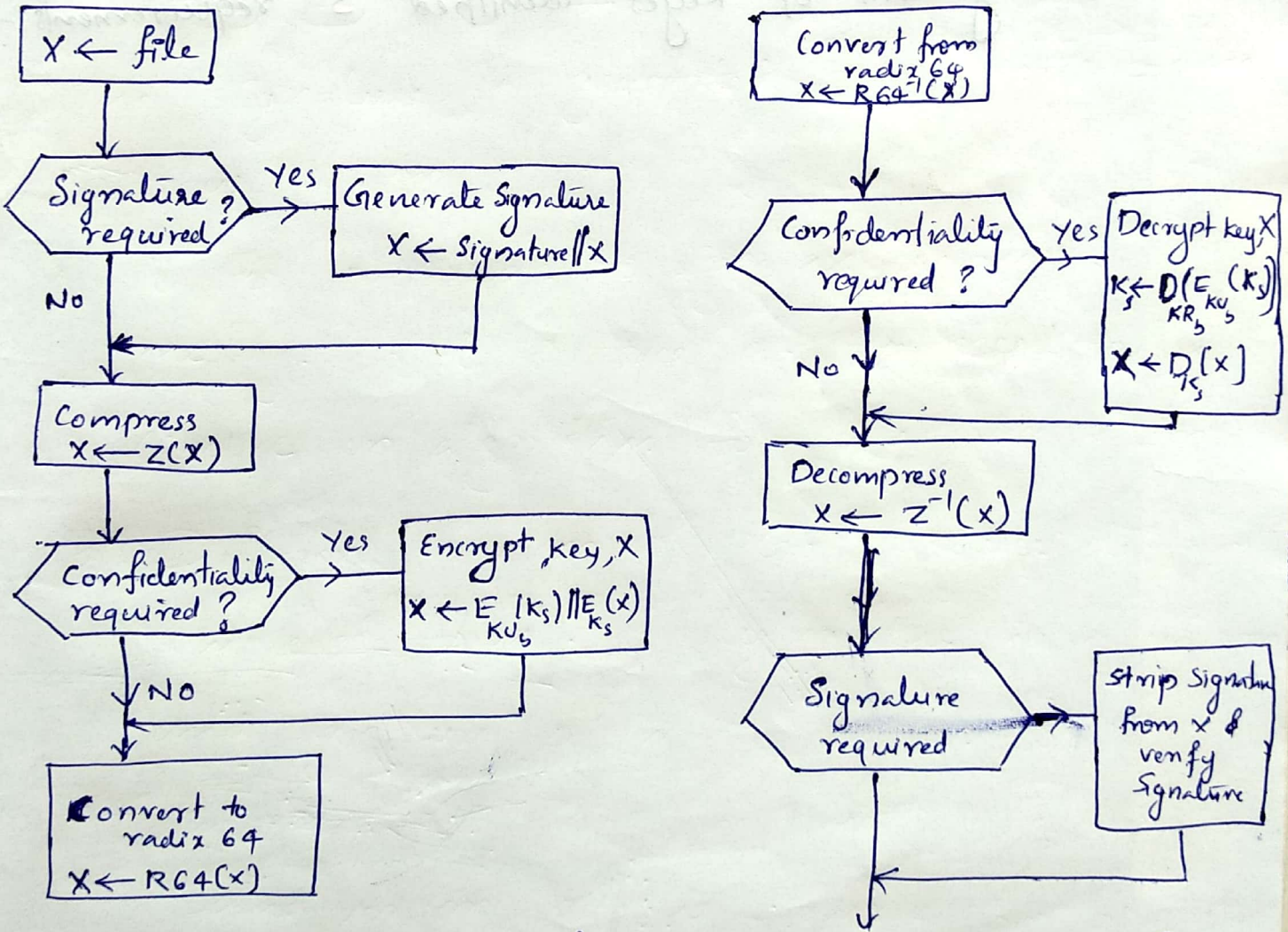
## 4. Email Compatibility

Many electronic mail systems only permit the use of blocks consisting of ASCII text. when PGP is used, at least part of the block to be transmitted is encrypted. This basically produce a sequence of arbitrary binary words which some mail system won't accept. To accomodate this restriction PGP uses an algorithm known as **radix 64** which maps 6 bits of binary data into 8 bit ASCII character. Unfortunately this expands the message by 33% however with the compression algorithm overall compression will be about one third.

## 5: Segmentation

Email facilities are often restricted to a maximum message length. for example, many of the facilities accessible throughout the internet impose a maximal length of 50,000 octets. Any msg longer than that must be broken up into smaller segments, each of which is mailed seperately.

To accomodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of the other processing including the radix-64 conversion. which is illustrated as follows:




(a) Transmission diagram (from A)

b) Reception diagram (to B)

fig:- Transmission & Reception of PGP messages.

→ IP Security

IP level security encompasses 3 functional areas:-

→ Authentication
→ confidentiality
→ Key Management.

(1) IP Security Overview

In IP-level security authentication and encryption are the necessary security feature which has been issued as IPV6.

Applications of IPSec

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

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

2

## Benifits of IPSec

→ when IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.

→ IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the internet into the organization.

→ IPSec is below the transport layer (TCP, UDP) and so is transparent to applications.

→ IPSec can be transparent to end users.

→ IPSec can provide security for individual users if needed.

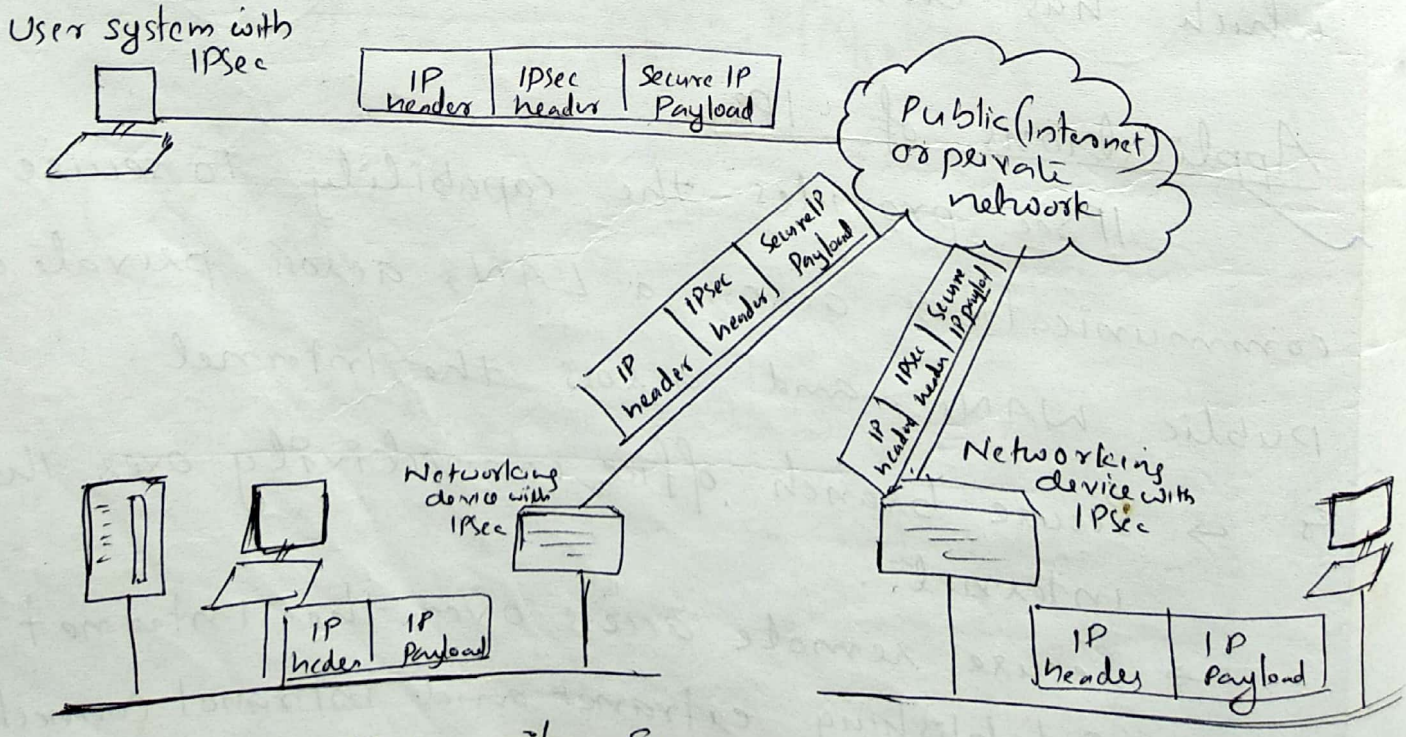



fig: An IP security Scenario

An Organization maintains LANs at dispersed locations. Nonsecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used. These protocols operate in networking devices, such as a routes or firewall, that connect each LAN to the outside world. The IPsec networking device ~~with~~ will typically encrypt and compress all traffic going into the WAN, and decrypt and decompress traffic coming from the WAN. these operations are transparent to workstations and servers on the LAN. Secure transmissions are also possible with individual users who dial into the WAN. Such user workstations must implement the IPsec protocol to provide security.

(2) IP Security Architecture

* Important

## IPSec Documents

The IPSec specifications consists of numerous documents. The most important documents are.

→ RFC 2401 :- An overview of 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.

In addition to these 4 RFC's, no. of additional documents are published and are divided into 7 groups:

1. Architecture :- Covers the general concepts, security requirements, definitions and mechanisms defining IP sec technology.

* 2. Encapsulating Security Payload (ESP) :- Covers the Packet format and general issues related to the use of the ESP for packet encryption.

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

4. Encryption algorithm :- A set of documents that describes how various encryption algorithms are used for ESP.

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

6. Key Management :- Documents that describes key management schemes.

7. Domain of Interpretation (DOI) :- Contains values needed for the other documents to relate to each other.

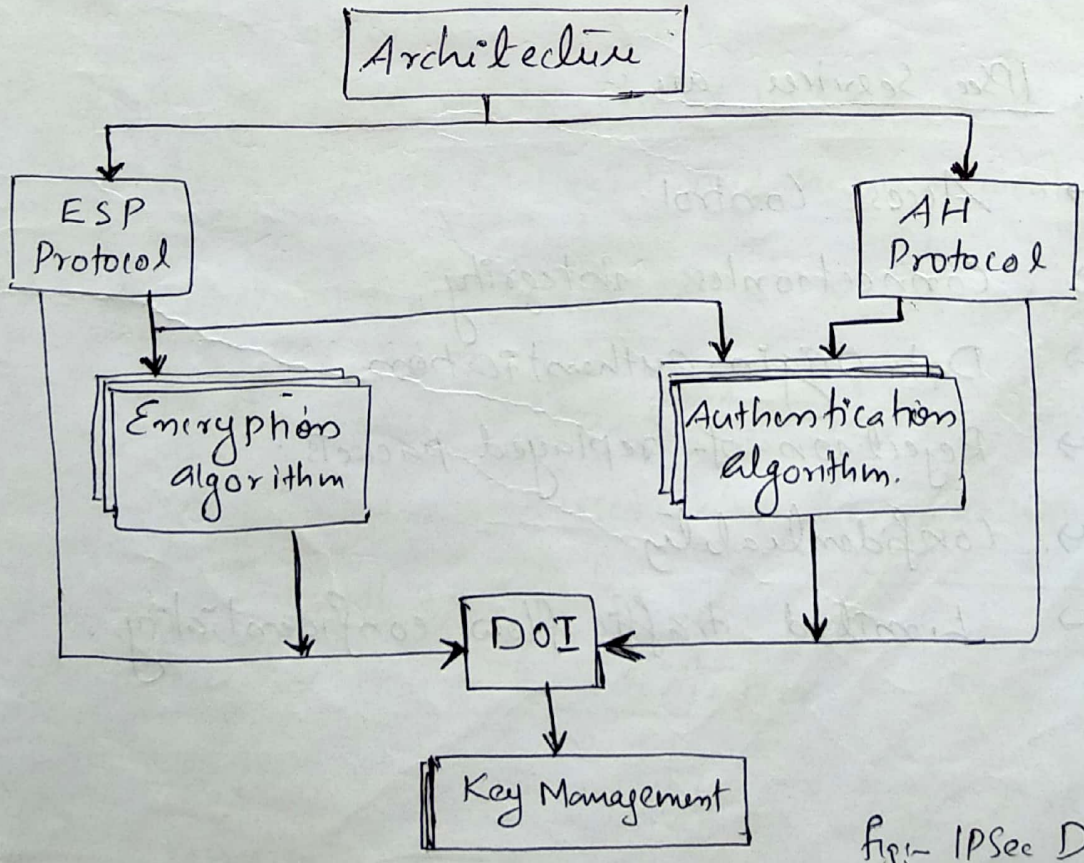



fig:- IPSec Document Overview.

6 IPSec Services

IPSec provides security services at the IP layer by enabling a system to select the required security protocols, determine algorithms to use for the services, and put in place any cryptographic keys required to provide the requested services.

Two protocols are used to provide security.

1) Authentication protocol by Authentication header (AH)
2) Combined encryption/authentication protocol by Encapsulating Security Payload (ESP)

The IPSec Services are :-

- Access Control
- Connectionless integrity
- Data Origin authentication
- Rejection of replayed packets.
- Confidentiality
- Limited traffic flow confidentiality.

# Security Associations (SA)

*: important

A key concept that appears in both authentication and confidentiality mechanisms for IP sec is the Security Associations (SA).

An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.

if a peer relationship is needed, for two-way secure exchange, then two security associations are required.

A security association is uniquely identified by 3 parameters :-

→ Security Parameter Index (SPI) :- A bit string assigned to this SA and having local significance only

↳ IP Destination Address :- ~~destination~~ address of the destination endpoint of the SA, which may be an end user stm or a ntwk system such as firewall or router.

→ Security Protocol Identifier :- This indicates whether the association is an AH or ESP security associations.

## SA Parameters

In each IPSec implementation, there is security association database that defines the parameters associated with each SA. Parameters are :-

→ Sequence Number Counter :- 32 bit value used to generate the sequence no field in AH or ESP headers.

→ Sequence Counter Overflow :- A flag indicating the overflow of the sequence no. counter.

→ Anti-Replay window :- Used to determine whether an inbound AH or ESP packet is a replay.

→ ESP information :- Encryption and authentication algorithm, keys, initialization values, key lifetime, and related parameters being used with ESP.

→ Lifetime of this Security Association :- A time interval or byte count after which an SA must be replaced with new SA.

→ IPSec Protocol Mode :- Tunnel or transport or wildcard mode.

→ Path MTU :- Any observed path for maximum transmision unit and aging variables.

a SA Selectors

The means by which IP traffic is related to specific SAs is the nominal Security Policy Database (SPD). An SPD contain entric 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.

Selectors are :-

- Destination IP address.
- Source IP address
- User ID
- Data sensitivity level
- Transport layer protocol
- IPsec Protocol (AH or ESP)
- Source and destination port
- IPV6 class
- IPv6 flow label
- IPV4 Type of service

X. important

10

# Transport and Tunnel Mode

Both AH and ESP support two modes of operation: Transport and tunnel mode.

## Transport Mode

Transport mode provides protection primarily for upper-layer protocols. ie transport mode protection extends to the payload of an IP packet. Transport mode is used for end-to-end communication between two hosts.

ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.

AH in transport mode authenticate the IP payload and selected portion of the IP header.

## Tunnel Mode

Tunnel mode provides protection to the entire IP packet. Tunnel mode is used when one or both ends of a SA is a security gateway, such as a firewall or router that implements IPSec.

ESP in tunnel mode encrypts and optionally authenticate the entire inner IP packet, including the inner IP header.

AH in tunnel mode authenticates the entire inner IP Packet and selected portions of the outer IP header.

## (3) Authentication Header (AH)

important

AH provides support for data integrity and authentication of IP packets. The data integrity features ensures that undetected modification to a packet's content in transit is not possible. The authentication feature enables an end system or network device to authenticate the user or application and filter traffic accordingly. It also prevents the address spoofing attacks and replay attacks.

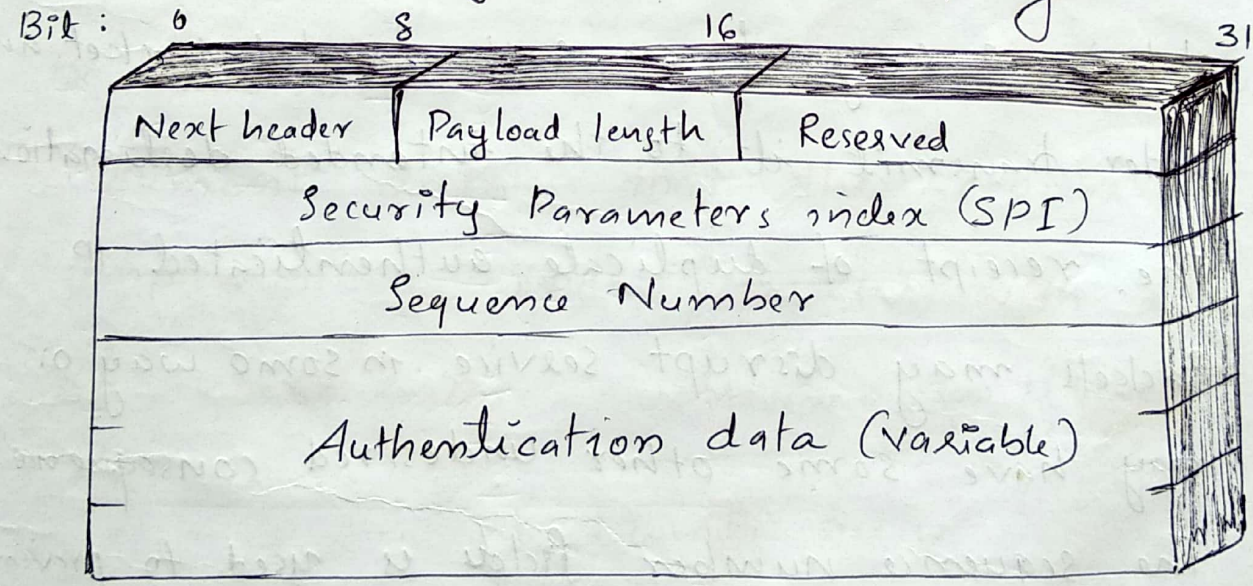



fig- IPSec Authentication Header.

Fields of AH are :-

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

→ Payload length (8 bits) :- Length of AH in 32 bit words minus 2.

19

↳ Reserved (16 bits) :- for future use.

↳ Security Parameter Index (SPI) (32 bits) :- Identifies the security association.

↳ Sequence number (32 bits) :- An increasing counter value.

↳ Authentication data (variable) :- A variable length field (integral no. of 32 bit) that contains the Integrity check Value (ICV) or MAC for this packet.

Anti-Replay Service

A replay attack is one which an attackes obtains a copy of an authenticated packet and later transmit it to the intended destination. The receipt of duplicate authenticated IP Packets may disrupt service in some way or may have some other undesired consequence. The sequence number field is used to prevent such attack.

Sequence Number generation and Processing is as follows:-

When a new SA is established, the sender initializes a sequence number counter

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 the limit of $2^{32}-1$ is reached, the sender should terminate this SA and negotiate a new SA with a new key.

Because IP is connectionless, unreliable-service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered. Therefore, the IPsec authentication document dictates that the receiver should implement a window of size W, with a default of W = 64. The

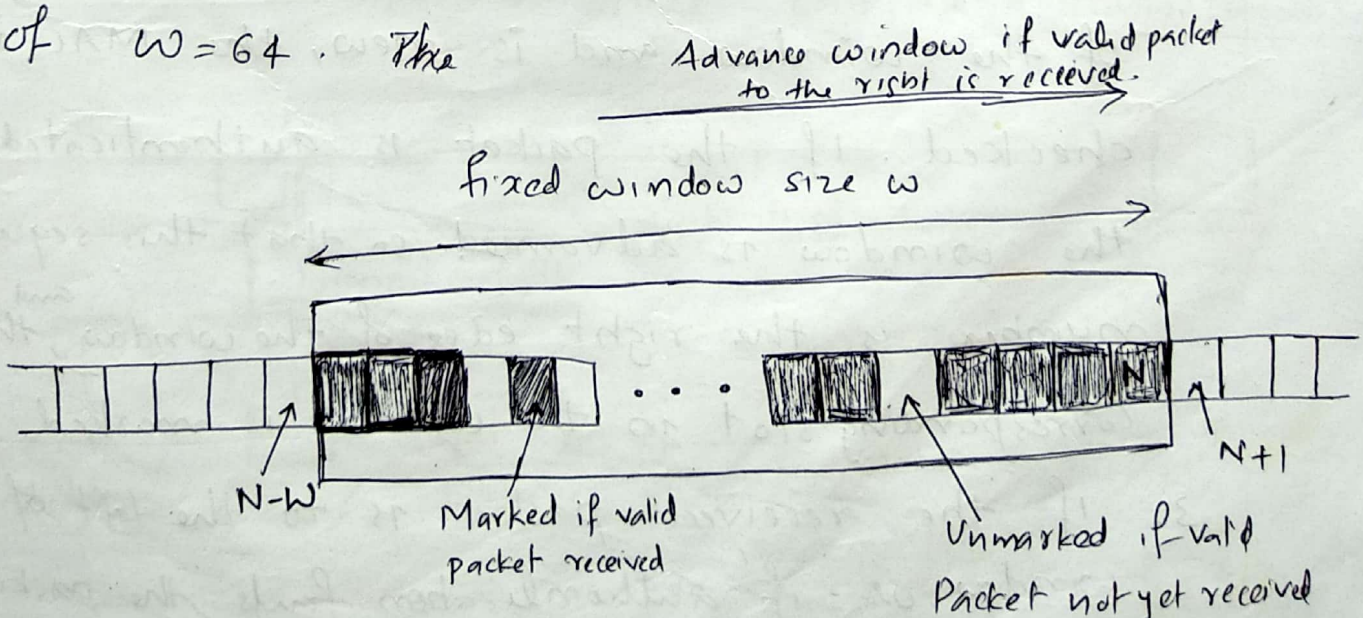



fig:- Anti Replay Mechanism.

The right edge of the window represents the highest sequence number, N, so far received for a valid packet. For any packet with a sequence number in the range from N-W+1 to N that has been correctly received, the corresponding slot in the window is mark.

The processing is as follows:-

1. if the received packet falls within the window and is new, the MAC is checked. if the packet is authenticated, the corresponding slot in the window is marked.

2. if the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked

3. if the received packet is to the left of the window, or if authentication fails, the packet is discarded, this is an auditable event,

## Transport and Tunnel Modes

There are two ways in which the IPSec authentication service can be used.

↳ Authentication is provided directly b/w a server and client workstations. the workstation can be either on the same network as the server or on an external network. As long as the workstation and the server share a protected secret key, the authentication process is secure. This case uses a transport mode SA

↳ A remote workstation authenticate itself to the corporate firewall, either for access to the entire internal network or because the requested server does not support the authentication feature. This case use a tunnel mode SA

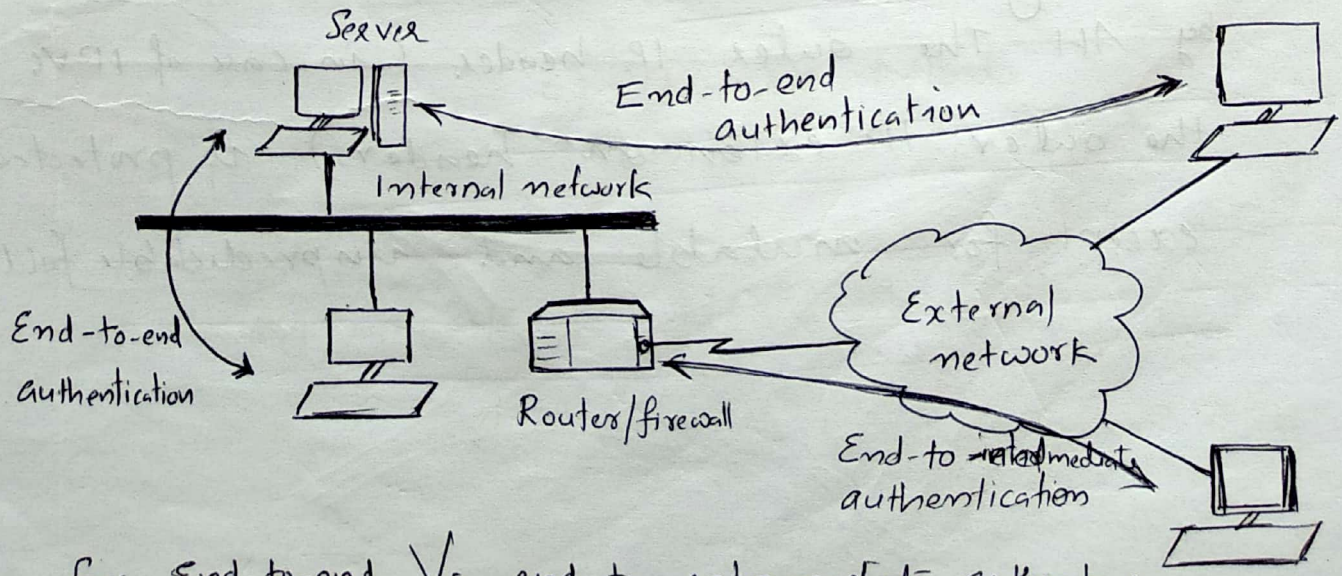


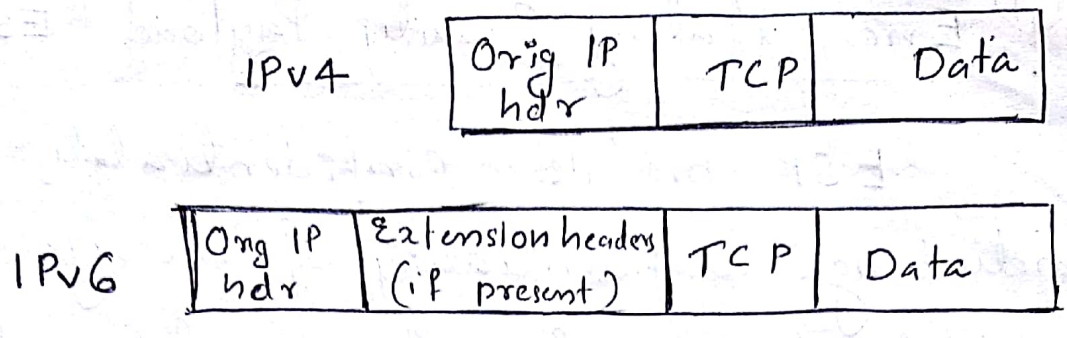

fig: End-to-end Vs end-to-intermediate authentication

## Scope of AH authentication

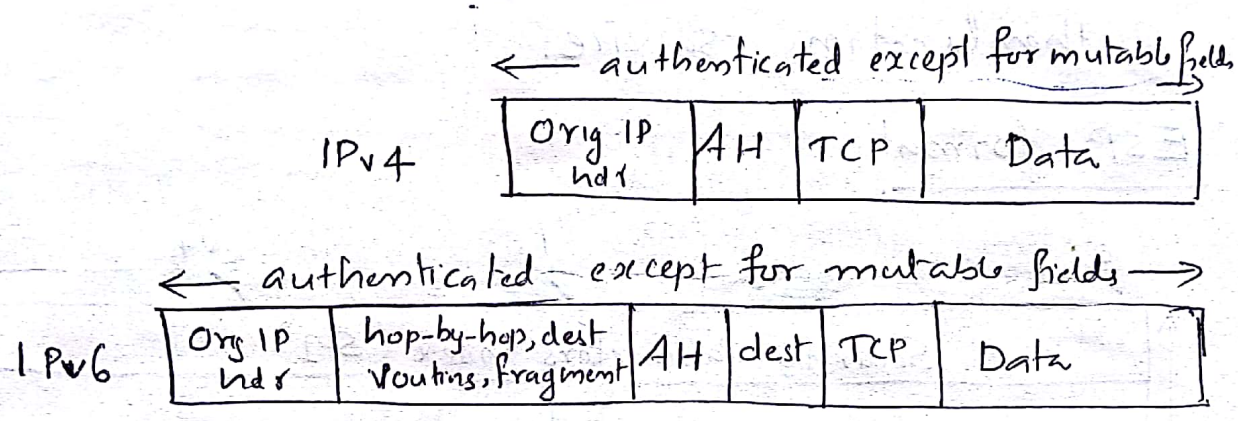
For transport mode AH using IPv4, the AH is inserted after the original IP header and before the IP payload. In IPV6, AH is viewed as an end-to-end pay load. ie it is not examined or processed by intermediate routers. therefore AH appears after the IPV6 base headers and the hop-by-hop, routing and fragment extension headers.

For tunnel mode AH, the entire original IP packet is authenticated, and the AH is inserted between the original IP header and a new outer IP header.

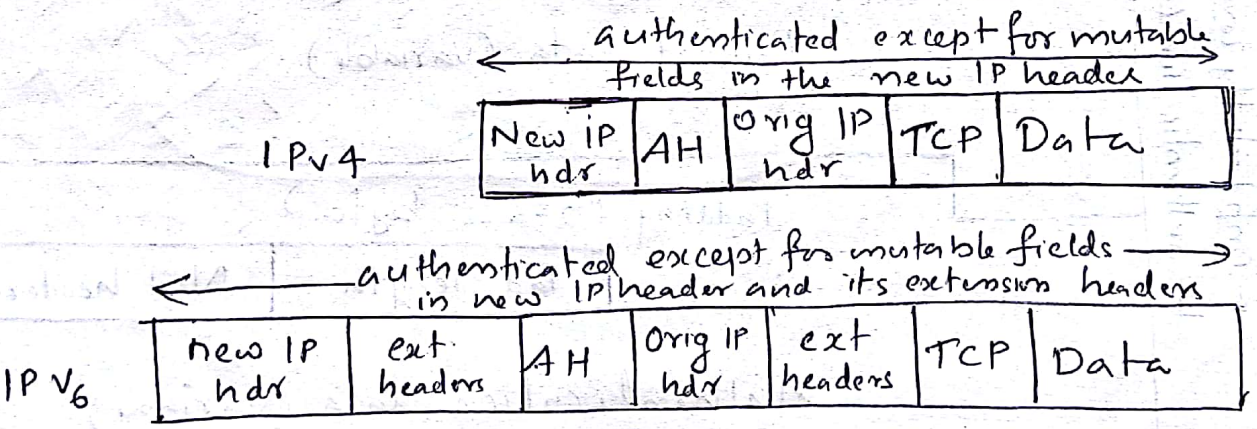
with tunnel mode, the entire inner IP packet, including the entire inner IP header is protected by AH. The outer IP header (in case of IPV6 the outer IP extension headers) is protected except for mutable and unpredictable fields.




a) Before applying AH.




b) Transport Mode.




c) Tunnel Mode.

Fig :- Scope of AH authentication.

# (4) Encapsulating Security Payload (ESP)

ESP provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide an authentication service.

## ESP format

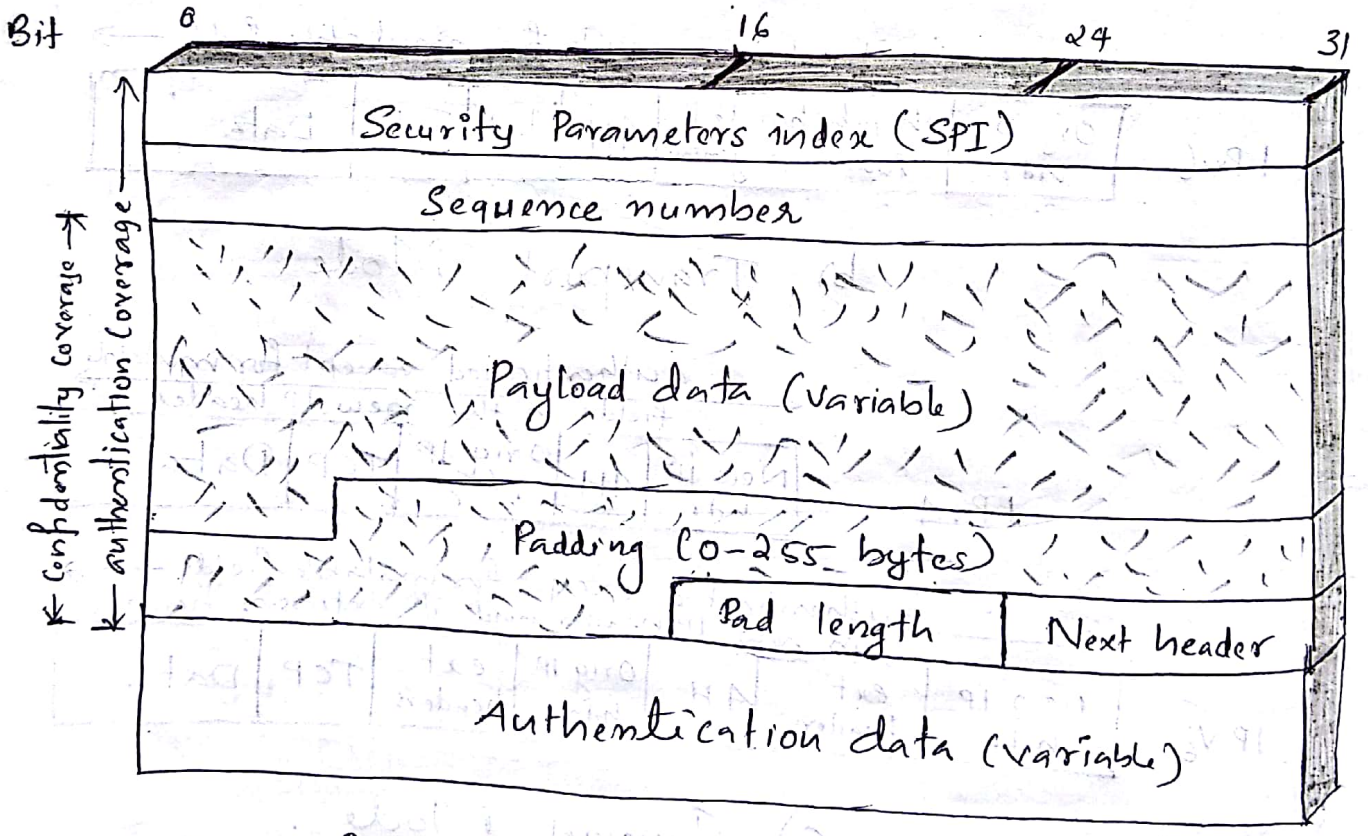



fig IPSec ESP format

ESP packets contains the following fields :-

→ Security Parameter Index (32 bits) :- identifies a SA

→ Sequence Number (32 bits) : An increasing counter value.

→ Payload Data (variable) :- This is a transport-level segment or IP packet that is protected by encryption.

→ Padding (0-255 bytes) :-

→ Pad length (8 bits) :- Indicates the no of pad bytes immediatly preceding this field.

→ Next header (8 bits) :- Identifies the type of data contained in the payload data field by identifying the first header in that payload.

→ Authentication Data (variable) :- It contains the integrity check value computed over the ESP Packet minus the Authentication Data field.

Encryption and authentication algorithms.

Encryption algorithms :-

→ DES in CBC mode
→ 3-key triple DES
→ RC5
→ IDEA
→ CAST
→ Blowfish.

authentication algorithms are :-

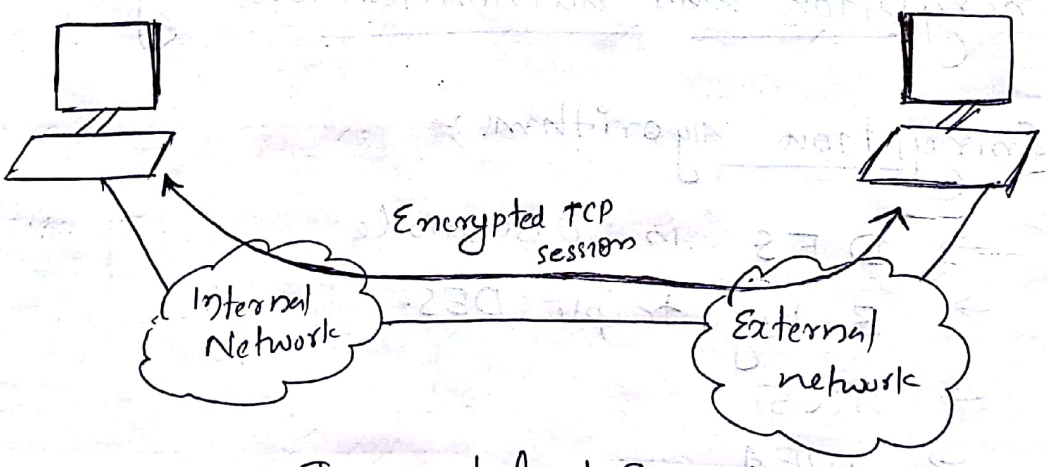
→ MAC with a default length of 96 bits.
→ HMAC-MD5-96.
→ HMAC-SHA-1-96.

16 Transport and Tunnel Mode

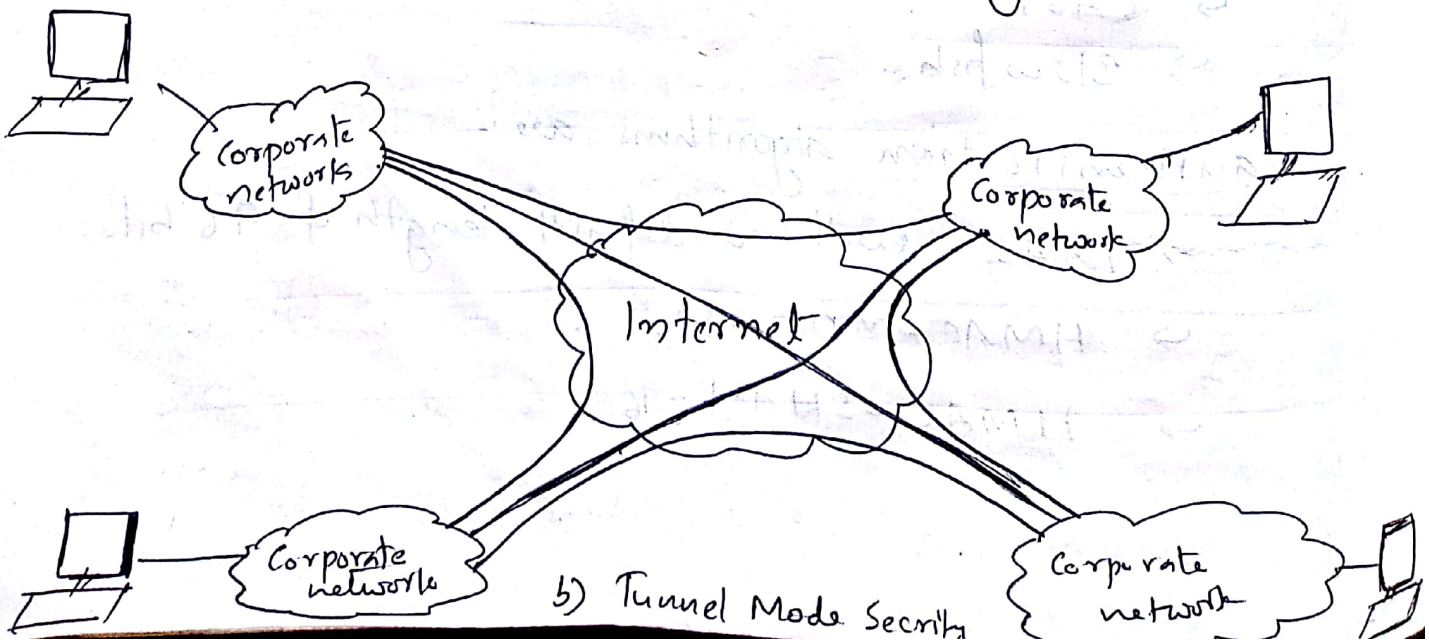
There are 2 ways in which the IPSec ESP service can be use.

→ Encryption is provided directly between two hosts. It is supported by transport mode SA.

→ Hosts on the internal networks use the Internet for transport of data but do not interact with other-internet based hosts. It is supported by tunnel mode SA. It is used to set up a virtual private network

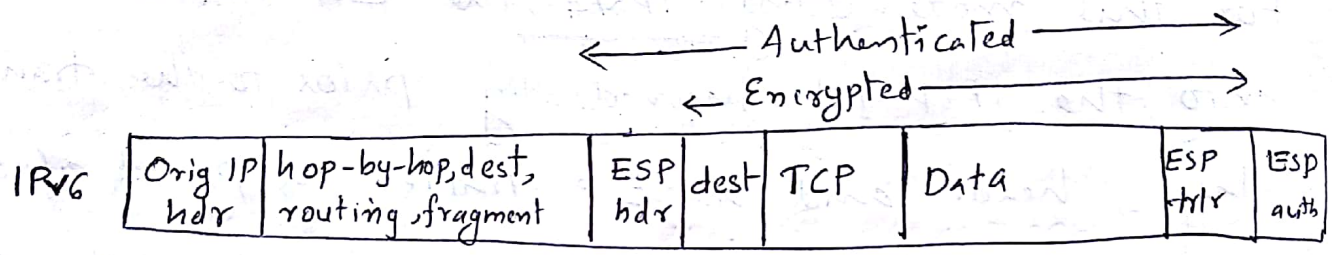



a) Transport level Security




b) Tunnel Mode Security

plus the destination options extension header if it occurs after the ESP header. Again the authentication covers the ciphertext plus the ESP header.




## Tunnel Mode ESP

Tunnel mode ESP is used to encrypt an entire IP packet. For this mode, the ESP header is prefixed to the packet and then the packet plus the ESP trailer is encrypted.

For IPv4 and IPv6 tunnel mode encryption and authentication is as follows:-

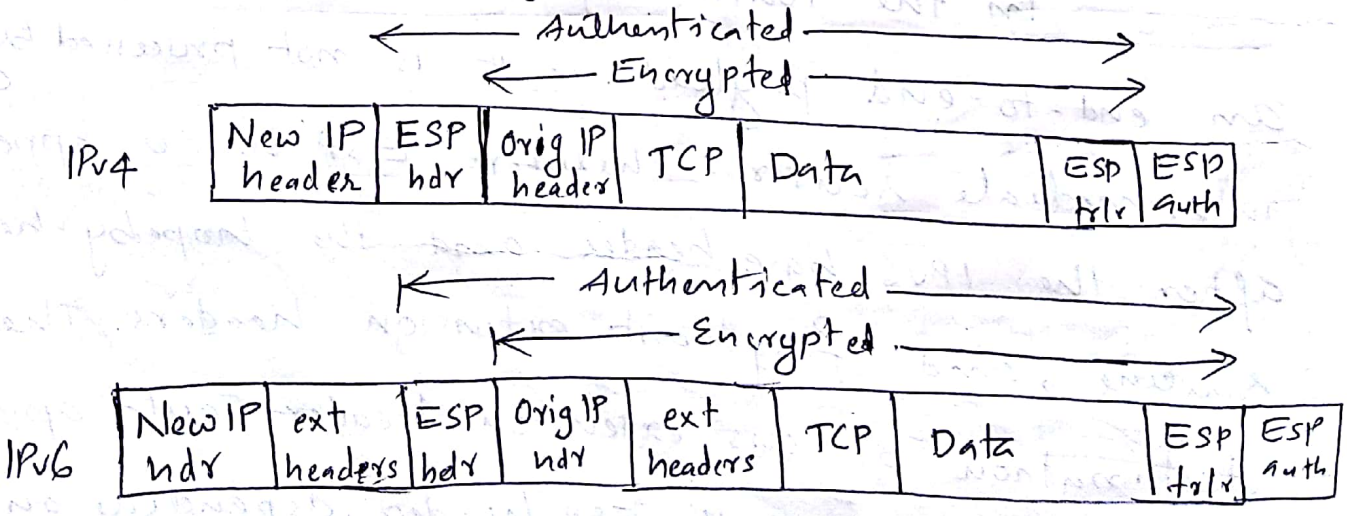
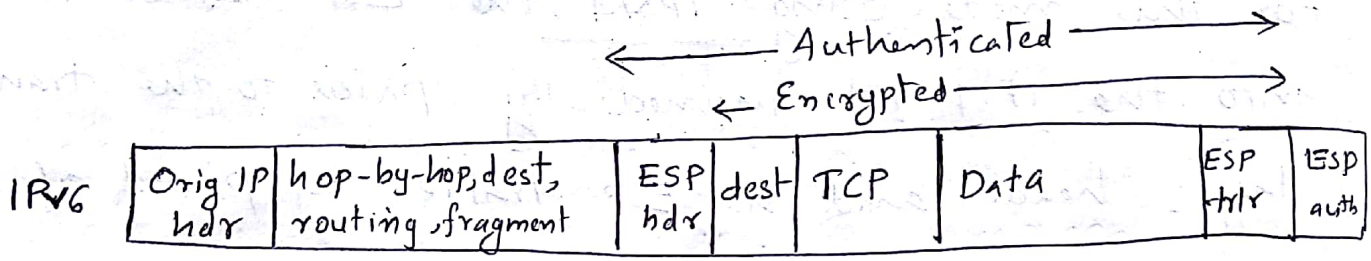



fig:- Tunnel Mode.

plus the destination options extension header if it occurs after the ESP header. Again the authentication covers the ciphertext plus the ESP header.




## Tunnel Mode ESP

Tunnel mode ESP is used to encrypt an entire IP packet. For this mode, the ESP header is prefixed to the packet and then the packet plus the ESP trailer is encrypted.

For IPv4 and IPv6 tunnel mode encryption and authentication is as follows:-

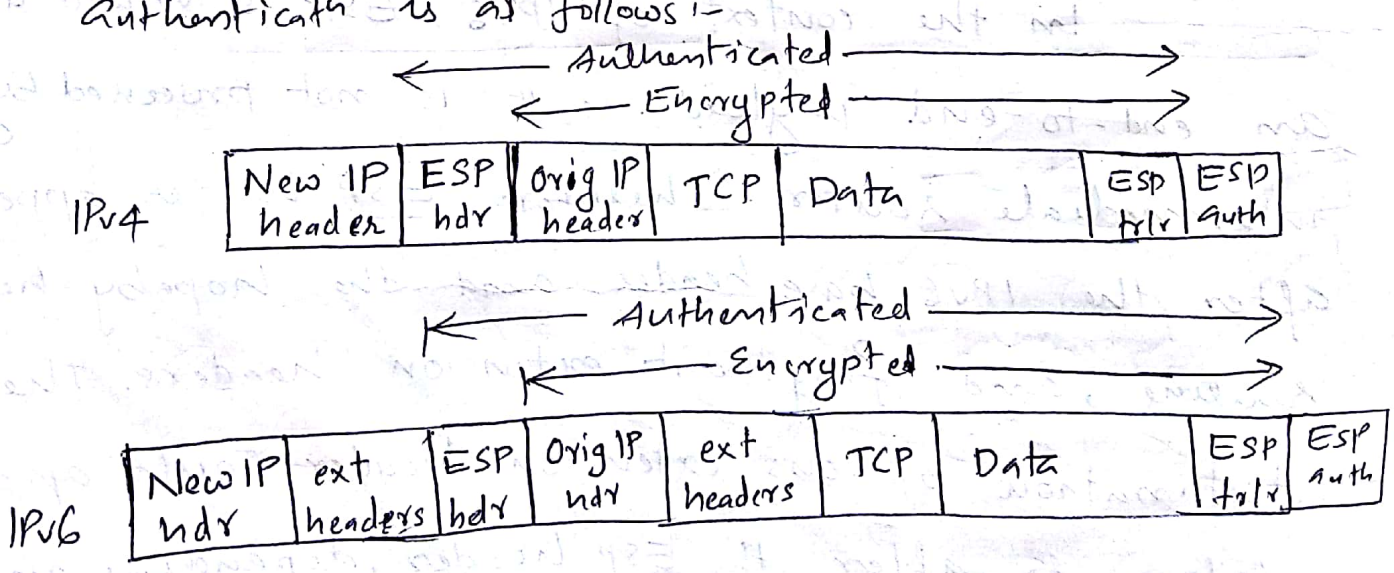



fig:- Tunnel Mode.

## (5) Combining Security Associations

An individual SA can implement either the AH or ESP protocol but not both. Sometimes a particular traffic flow will call for the services provided by both AH and ESP.

Security associations can be combined into bundles into two ways.

1) Transport adjacency : Refers to applying more than one security protocol to the same IP packet without invoking tunneling.

2) Iterated tunneling :- Refers to the applicatn of multiple layers of security protocols effected through IP tunneling.

### Basic Combinations of SA

The IPSec Architecture lists 4 examples of combinations of SAs.

Case 1 : Here all security is provided between end systems that implement IPSec. For any two end systems to communicate via an SA there must share the appropriate secret key.

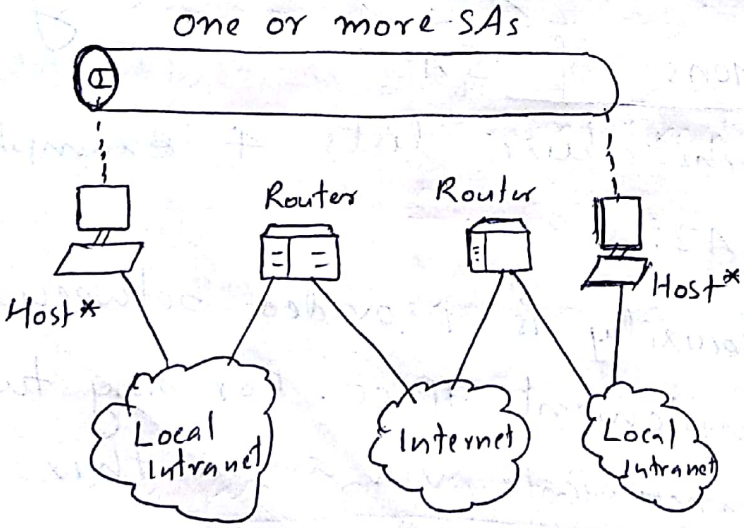
Possible Combinatn are :-

a) AH in transport mode
b) ESP in transport mode
c) AH followed by ESP in transport mode
d) any of a, b, c inside AH or ESP in tunnel mode

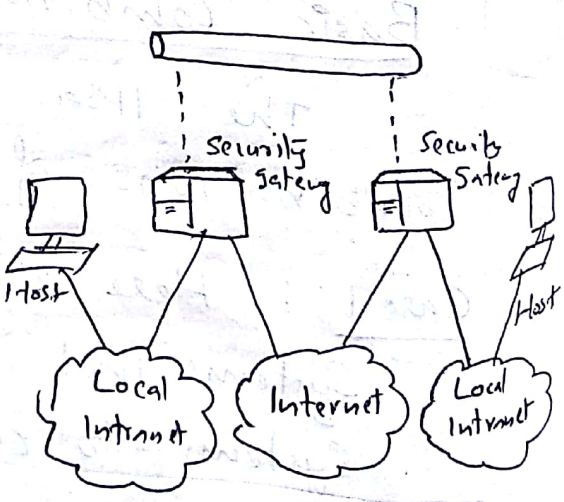
Case 2 : Here the security is provided only between gateways and no hosts implement IPSec. A single SA tunnel could only needed in this case. The tunnel could support AH, ESP or ESP with authentication option.

Case 3 : It build on case 2 by adding end-to-end security. All combinations for case 1 and 2 are allowed here.

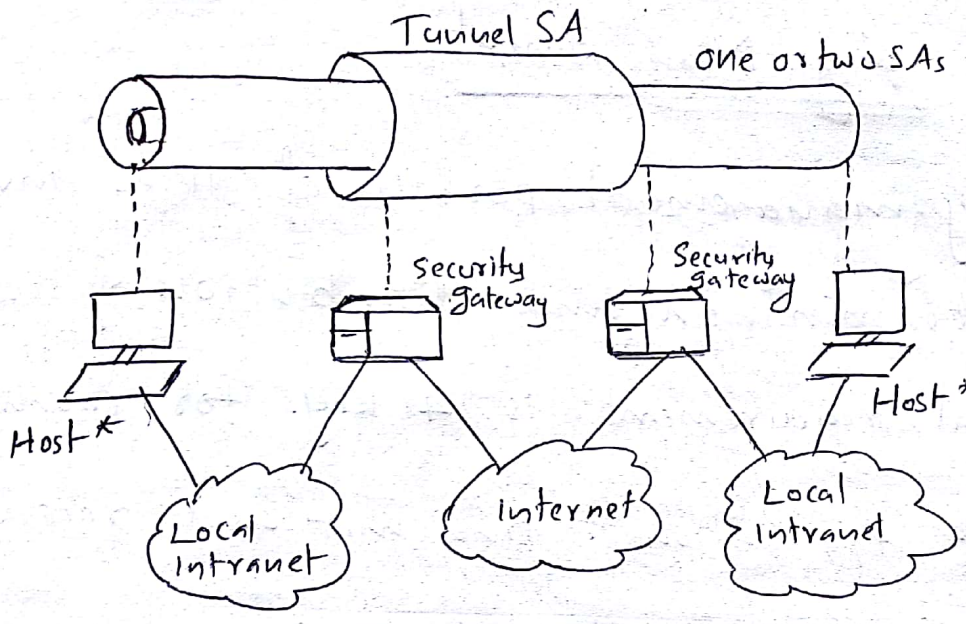
Case 4 : It provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall. Only tunnel mode is required.



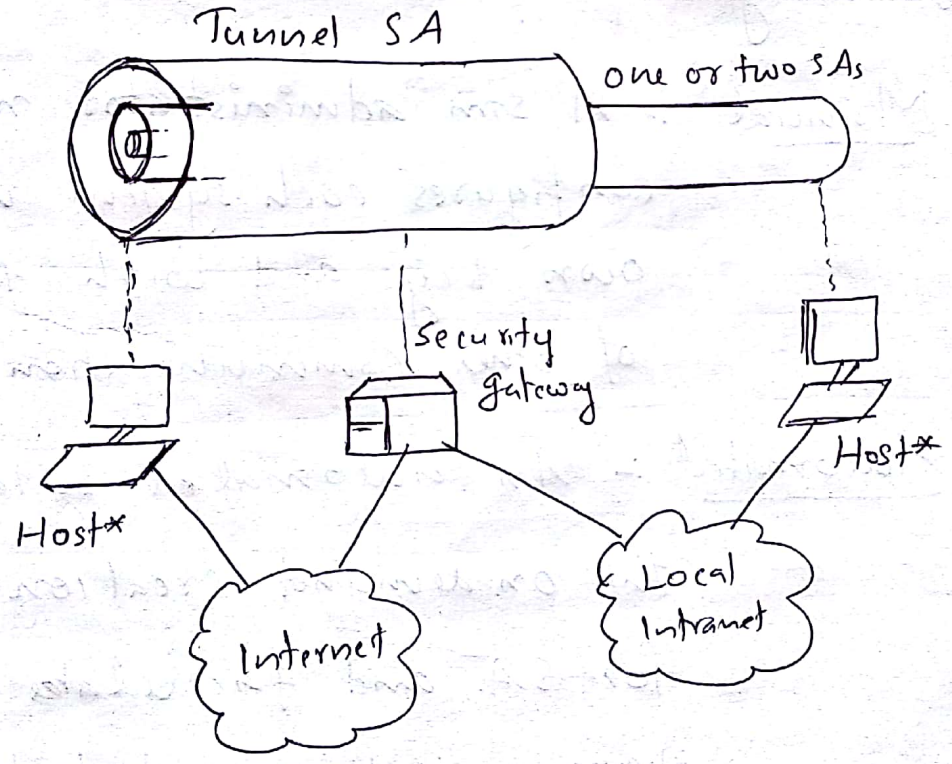

a) case 1




b) Case 2.




c) Case (3)




d) Case 4

* - denote Host that implements IPSec.

fig:- Basic Combinations of Security Associations.

(6) Key Management

Key management portion of IPSec involves the determination and distribution of secret keys. A typical requirement is 4 keys for communicath btw two applications: transmit and receive pairs for both AH and ESP.

IPSec architecture documents support 2 types of key management

→ Manual :- A stm administrator manually configures each system with its own keys and with the keys of other communication systems.

→ Automated :- An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.

There are 2 automated key management protocols

→ Oakley key Determination protocol

→ Internet Security Association and Key Management protocol (ISAKMP)