Date __/__/__

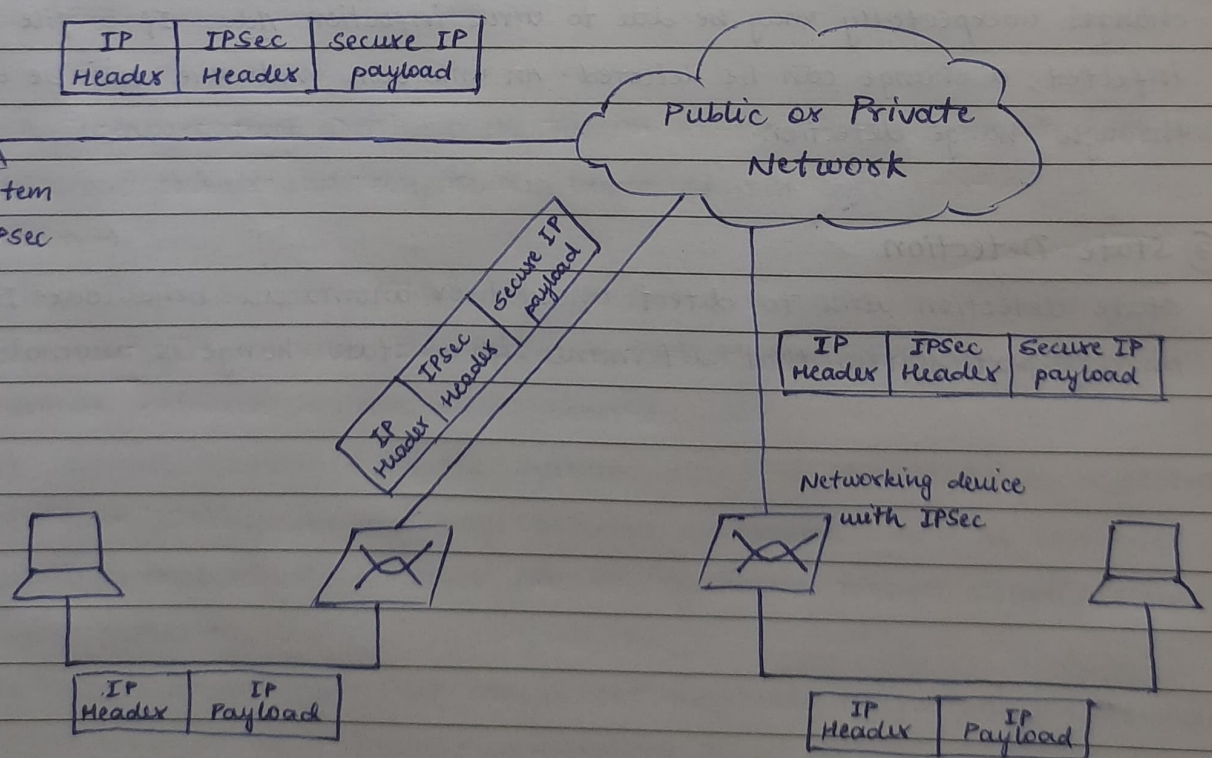
UNIT-2

IP SECURITY (IP Sec)

The IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for security key exchange and key management are defined in it.

Uses of IP Sec

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network (VPN) connection.

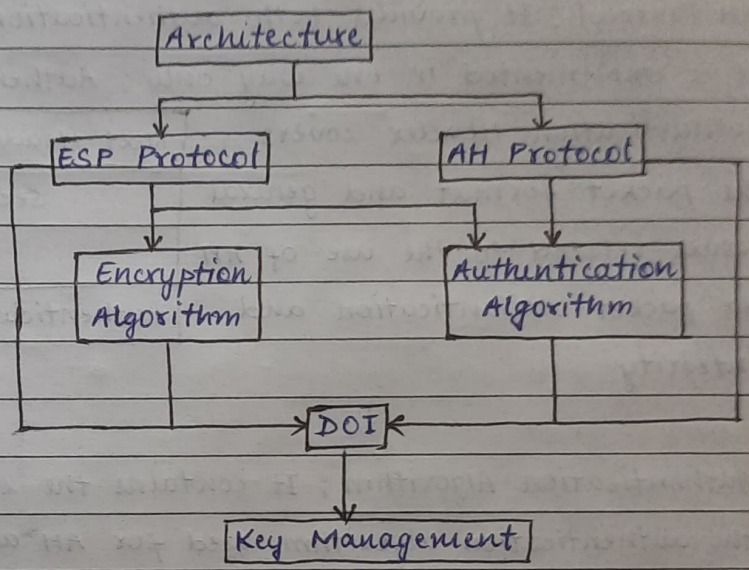


Date __/__/__

IPSec ARCHITECTURE

It uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec architecture includes protocols, algorithms, DOI and key management. All these components are very important in order to provide the 3 main service,

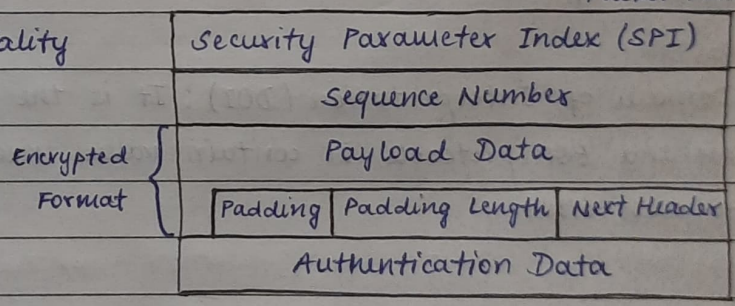
- Confidentiality
- Authentication
- Integrity



1) Architecture : The IPSec architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IPSec technology.

2) ESP Protocol : provides confidentiality service.

Packet Format



- SPI : This parameter is used be security association. It is used to give a unique number to the connection build between the client and server.
- Sequence No. : Unique sequence numbers are alloted to every packet so that on the receiver side packets can be arranged properly.
- Payload Data : It means the actual data or the actual message. The payload data is in an encrypted format to achieve confidentiality.
- Padding : Extra bits of space are added to the original message in order to ensure confidentiality. Padding length is the size of the added bits of space in the original message.
- Next Header : It means the next payload or next actual data.

Date / /

- Authentication Data: This field is optional in ESP protocol packet format.

3) Encryption Algorithm: The encryption algorithm is the document that describe various encryption algorithms used for ESP.

4) AH Protocol: It provides both authentication and integrity service. It is implemented in one way only: Authentication along with Integrity.

Authentication Header covers the packet format and general issues related to the use of AH for packet authentication and integrity.

Next Header	Payload Length	Reserved
Security Parameter Index (SPI)		
Sequence Number		
Authentication Data (Integrity Checksum)		

5) Authentication Algorithm: It contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP.

6) Domain of Interpretation (DOI): It is the identifier that supports both AH and ESP protocols. It contain values needed for documentation related to each other.

7) Key Management: It contains the document that describes how the keys are exchanged between sender and receiver.

SECURITY ASSOCIATIONS (SA)

A security association (SA) is a set of security parameters that dictates how IPsec processes a packet. The SA defines what rules to use for to use for authentication and encryption algorithms, key exchange mechanisms, and secure communication between two parties. SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. In other words, SA is a one-way relationship between sender &

receiver that affords security for traffic flow. It is defined by three parameters:

- SPI - The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- IP Destination Address - the address of the destination endpoint of the SA.
- Security Protocol Identifier - indicates whether the association is an AH or ESP security association.

some other parameters in SA -

- Sequence Number Counter
- Sequence Number Overflow
- Anti-Replay Window
- AH Information
- ESP Information
- Lifetime of SA
- IPSec Protocol Mode
- Path MTU

SECURITY POLICY DATABASE (SPD)

The SPD contains a set of rules that determines whether a packet is subject to IPsec processing and governs the processing details. Each entry in the SPD represents a policy that defines how the set of traffic covered under the policy will be processed. Any inbound or outbound packet is processed in one of the three ways: discard, perform IPsec processing, or bypass IPsec processing. A selector is a set of IP and upper layer protocol fields which map traffic flow to a security policy in the SPD. The possible fields for constructing the selector can be: source address, destination address, transport layer protocol, source & destination protocol ports, user ID.

Date / /

IPsec OPERATION : TUNNEL and TRANSPORT MODES

Destination IP address is actual address, vulnerable to scanning →

Transport Mode

Original IP Header	IPsec Header	Protected Packet Data Field

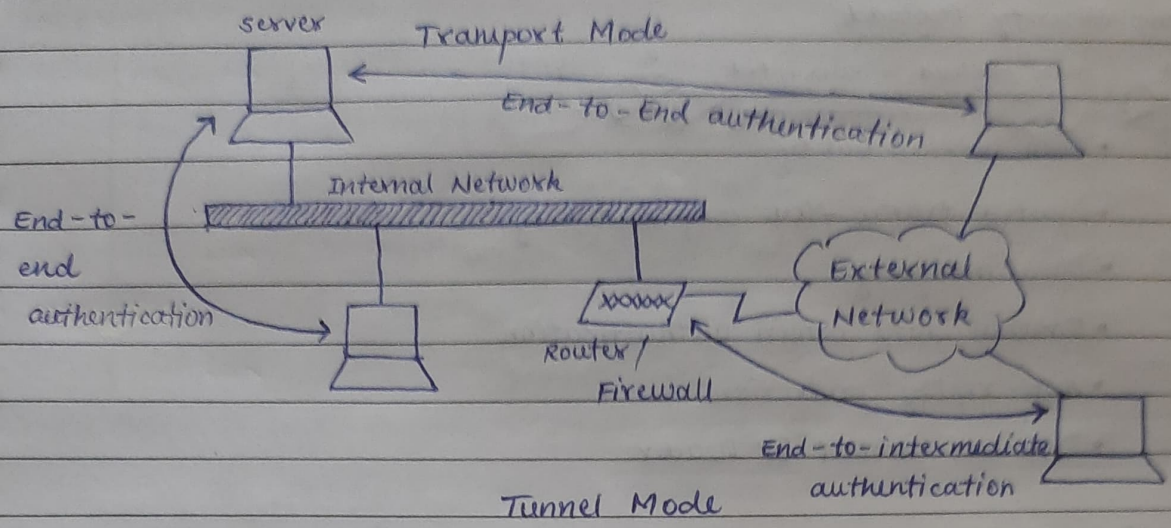
Destination IP address is IPsec gateway address. Host IP address is not revealed. →

Tunnel Mode

New IP Header	IPsec Header	Protected Original Packet

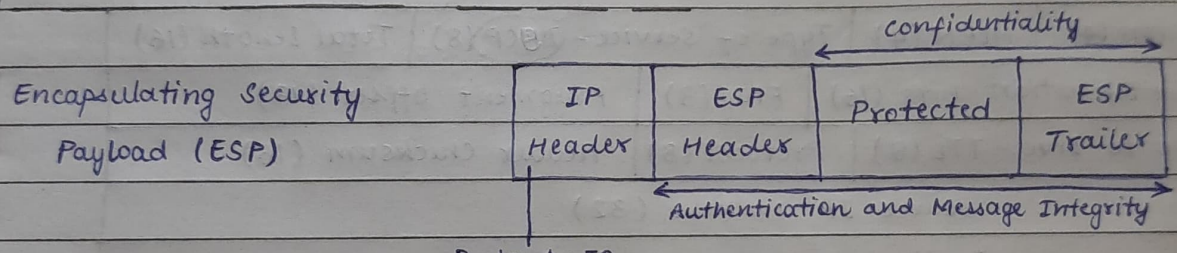
TUNNEL MODE	TRANSPORT MODE
Here two IP headers are sent. The inner IP packet determines the IPsec policy that protects its contents.	IP addresses in the outer header are used to determine the IPsec policy that will be applied to the packet.
IPsec policy is enforced on the contents of the inner IP packet.	The IP header, the next header, and any ports that the next header supports can be used to determine IPsec policy.
The original packet is encapsulated in a new IP packet (both its IP header and its payload).	Depending on the protocol used, a new AH or ESP header is created and inserted just after the original IP header.
NAT traversal is supported with the tunnel mode.	NAT traversal is not supported with the transport mode.
Eg: Cisco routers or ASA firewalls.	Eg: Telnet or Remote Desktop session.

Date __/__/__

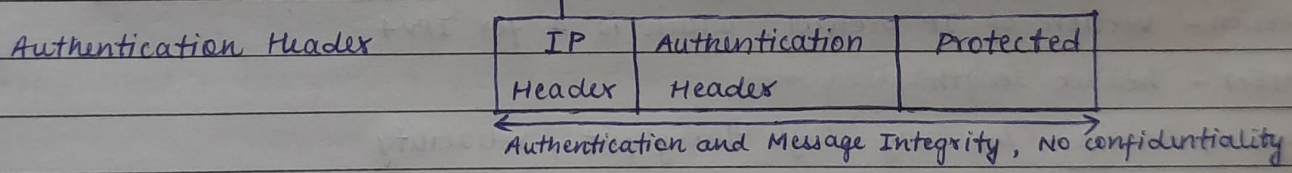


Tunnel Mode

IP HEADER PROTECTION : ESP and AH

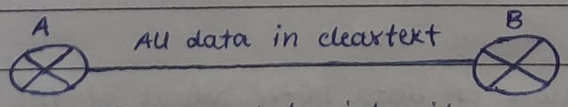


Protocol = 51



IPsec SECURITY PROTOCOLS

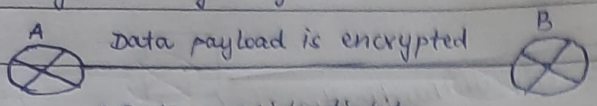
Authentication Header



- Ensures data integrity
- Uses keyed-hash mechanism
- Does not provide confidentiality (no encryption)
- Provides optional replay protection
- Provides origin authentication - ensures packets will definitely came from peer router

Date __/__/__

Encapsulating Security Payload



- Data confidentiality
- Limited traffic flow confidentiality
- Data integrity
- Optional data origin authentication
- Anti-replay protection
- Does not protect IP header

IPv4 and IPv6 HEADER

IPv4

→ Differentiated Services Code Points

Version (4)	HLEN (4)	Type of Service - DSCP (8)	Total Length (16)
Identification bits (16)	Flag (3)	Fragment Offset (13)	
Time to Live - TTL (8)	Protocol (8)	Header Checksum (16)	
Source IP address (32)			
Destination IP address (32)			
Options & Padding			

- Version - version of IP protocol, which is 4 for IPV4
- HLEN - header length
- Type of Service - low delay, high throughput, reliability
- Total Length - length of header + data (16 bits)
- Identification - unique packet id for identifying the group of fragments of a single IP datagram.
- Flags - 3 flags of 1 bit each
- Fragment Offset - represents the number of data bytes ahead of the particular fragment in the particular datagram.
- TTL - datagram's lifetime
- Protocol - name of the protocol to which the data is to be passed
- Header Checksum - checking errors in the datagram header
- Source IP address - sender's address
- Destination IP address - receiver's address

Date __/__/__

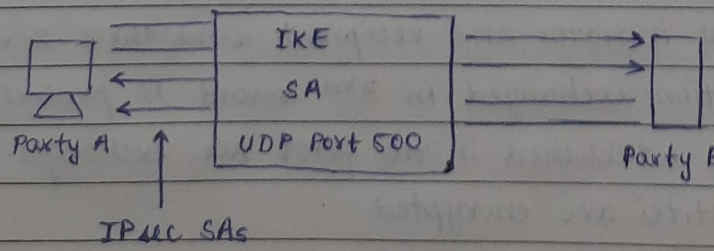
IPv6

Version (4)	Priority / Traffic Class (8)	Flow Label (20)
Payload Length (16)	Next Header (8)	Hop Limit (8)
Source Address (128)		
Destination Address (128)		
Extension Headers 1		
⋮		

- **Traffic Class** – It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.
- **Flow Label** – This field is used by the source to label the packets belonging to the same flow in order to request special handeling by intermediate IPv6 routers.
- **Payload Length** – This field indicates the total size of the payload which tells routers about the amount of information a particular packet contain in its payload.
- **Next Header** – This field indicates the type of extension header (if present) immediately following the IPv6 header.
- **Hop Limit** – This field is same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel.
- **Extension Header** – In order to rectify the limitations of the IPv4 option field, extension headers are introduced in IPv6.

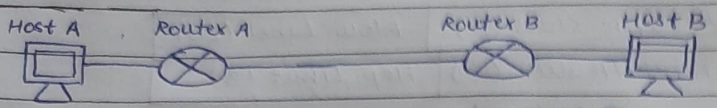
INTERNET KEY EXCHANGE (IKE)

IKE is a secure key management protocol that is used to set up a secure, authenticated communications channel between two devices.



Date __/__/__

PHASES OF IKE



1. Host A sends interesting traffic to Host B
2. Router A and B negotiate an IKE phase 1 session
3. Router A and B negotiate an IKE phase 2 session
4. Information is exchanged via the IPsec tunnel
5. The IPsec tunnel is terminated.

Two versions of IKE standards are available:
- IKEv1 - defined in RFC 2409
- IKEv2 - defined in RFC 7296

IKE PHASE-1

- Determine the following policy details:
  - Key distribution method
  - Authentication method
  - IPsec peer IP addresses and hostnames
  - IKE phase 1 policies for all peers
    - Encryption algorithm
    - Hash algorithm
    - IKE SA lifetime
- Goal: minimize misconfiguration

It establishes a bi-directional IKE SA aka ISAKMP security association.
Phase-1 has two modes:

1) Aggressive mode - In this mode, the initiator and recepient accomplish the same objectives as with main mode, but in only two exchanges, with a total of three messages. Because the participants identities are exchanged in the first two messages, aggressive mode does not provide identity protection.
2) Main mode - In this mode, the initiator and recepient send three 2-way exchanges. The information exchanged in 3rd round is protected by the encryption algorithm established in the first two exchanges. Thus, the participants identites are encrypted.

Date __/__/____

IKE PHASE-2

- Determine the following policy details :
  - IPsec algorithms and parameters for optimal security and performance
  - Transforms and if necessary, transform sets
  - IPsec peer details
  - IP address and applications of hosts to be protected
  - Manual or IKE-initiated SAs
- Goal : Minimize misconfiguration

ISAKMP is used to securely negotiate the IPsec pair of SAs.

Phase-2 has 1 mode :

1) Quick mode - It is similar to aggressive mode in phase-1, except negotiation must be protected within an IKE SA. Quick mode negotiates the SA for the data encryption and manages the key exchange for that IPsec SA.

Both phase uses Diffie-Hellman key exchange to establish shared key.

EXPECTATIONS FROM IKE

- Secrecy and authenticity
- Protection against replay attacks
- Scalability (being suitable for big network)
- Privacy and anonymity (protecting identity of players in the protocol)
- Protection against DOS.
- Efficiency (both computational and minimal in no. of messages)
- Independence of cryptographic algorithms
- Minimize protocol complexity
- Reliability