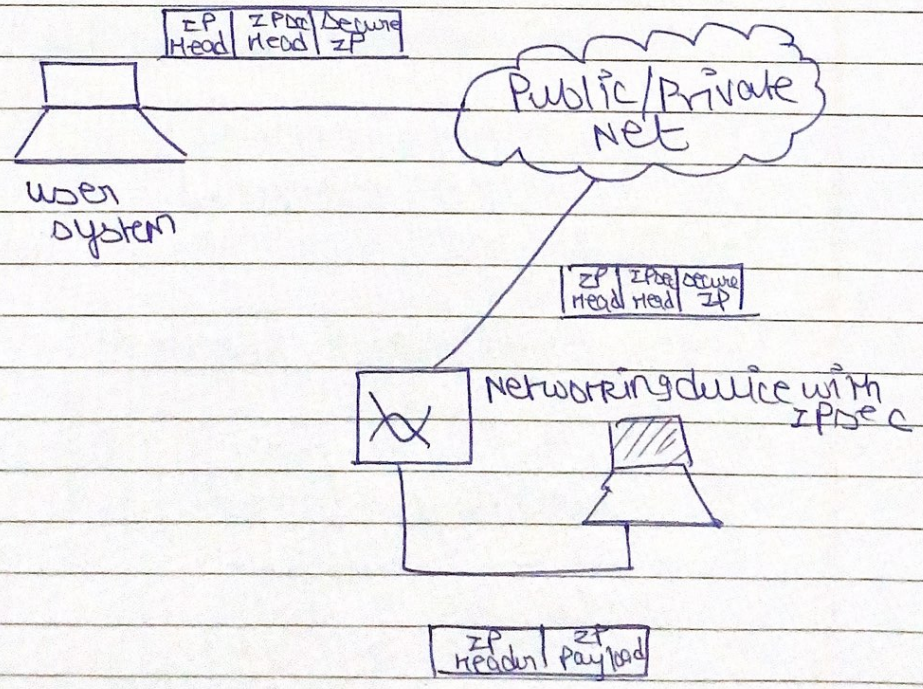
DATE
PAGE No.

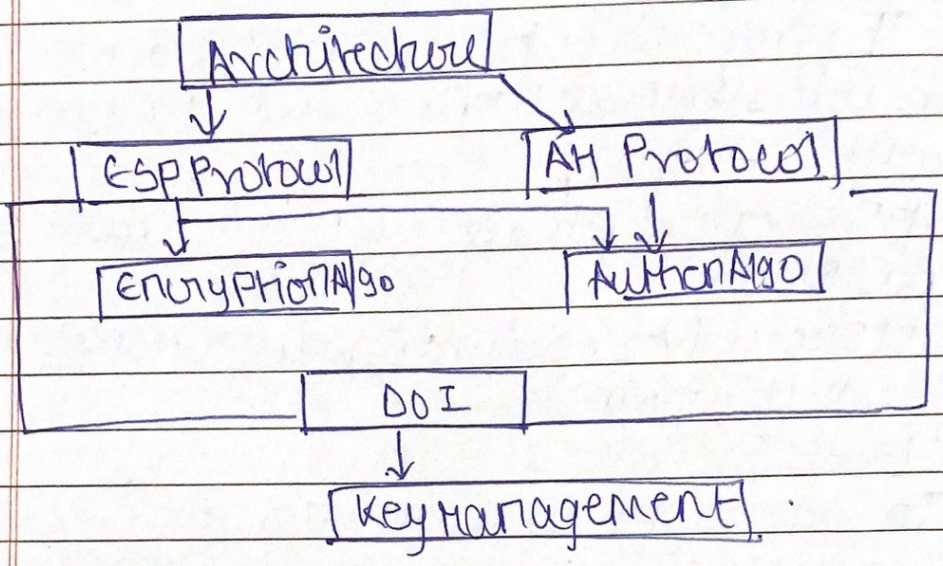
IPsec

a) IETF protocol between 2 points across IP
b) provides data authentication, integrity & confidentiality
c) defines encrypted decrypted & authenticated packets
d) protocols (for security key exchange & key mgmnt)

Uses

a) To encrypt application layer
b) provide security for routers across the internet.
c) provide authentication w/o encryption (data is originating from known sender)
d) IPsec tunnelling (two points, encrypted data transfer similar to VPN)



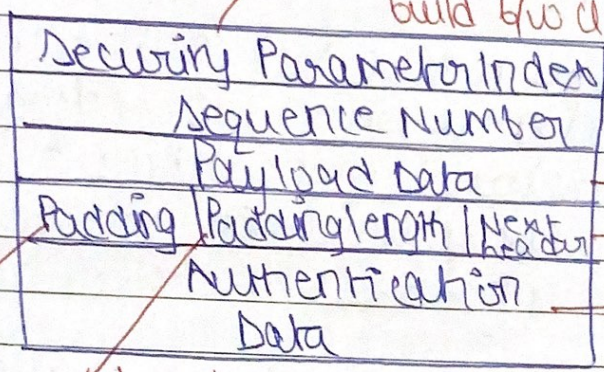


→ Confidentiality
→ Authentication
→ Integrity.

DATE
PAGE No.

ESP Protocol

↳ provides confidentiality service



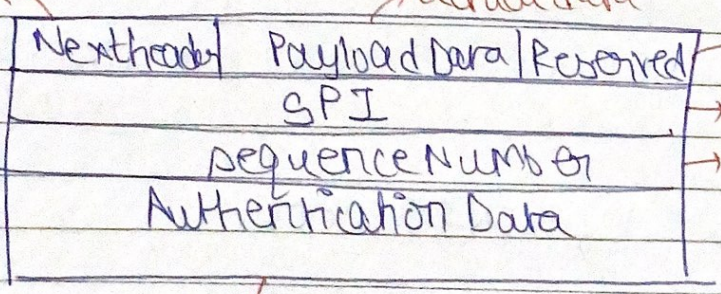
Key Management
↳ defines how keys are exchanged

Encryption Algo → contains algorithm used for ESP (documents)

Authentication Header Protocol

↳ authentication along with integrity
↳ covers packet format & general issues related to use.

DOI
↳ identifier supporting AH & ESP
→ document related to each other



optional field

Authentication Algo
↳ document containing authentication also used for Authentication

DATE
PAGE No.

Securing Association

↳ securing parameters that dictates how IPSec processes a packet

↳ rules to use for authentication and encryption algorithms, key exchange mechanisms & secure communication between two parties.

↳ simplex connection that allows two host to communicate securely

↳ SA is one way relationship b/w sender & receiver that affords security for traffic

Parameters

↳ SPI → select SA for receiving system under which packet is processed
↳ IP Destination Address destination endpoint
↳ Securing Protocol Identifier.
↓
tell whether association is an AH or ESP securing

↳ SPI Counter

↳ Path MTU
↳ ESP Info

DATE
PAGE No.

Security Policy Database

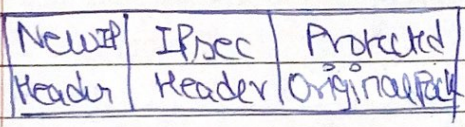
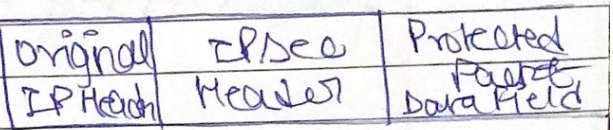
1. Set of rules determining whether a packet is subject to IPsec & govern processing details

2. each entry → policy (how traffic is processed)

3. Three ways of IPsec Processing (for inbound & outbound packets)
   - discard
   - perform
   - bypass

4. Selector → A selector is a set of IP & upper layer protocol fields which map traffic flow to a security policy

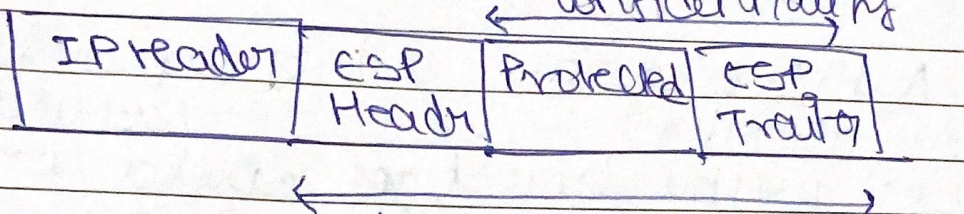
5. Selector Fields
   - source address
   - destination address
   - transport layer protocol
   - source & destination protocol ports
   - user ID

Tunnel Mode	Transport Mode
a) IP address is IPsec gateway address Host IP address is not revealed	a) IP address of destination is actual address (vulnerable to scanning)
b) 	b) 
c) Two IP headers sent. Inner IP packet determines IPsec policy & protects	c) IP addresses in the outer header used to determine policy
d) Policy enforced on the contents of inner IP	d) IP header, next header & any ports supported by next header can be used to determine IPsec policy.
e) original packet is inside or can say encapsulated in new packet.	e) depending on the protocol used a new AH or ESP header is created & inserted after ~~new~~ original IP header
f) NAT is supported	f) NAT is not supported
g) Eg Cisco routers/ ASA firewalls	g) Telnet or Remote Desktop session.

DATE
PAGE No.

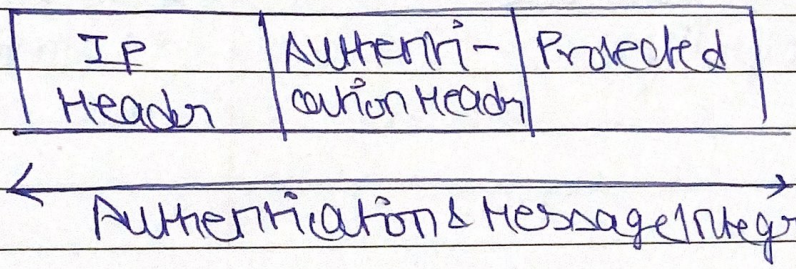
IP Header Protection

ESP



Protocol = 51

AH



Ipsec Security Protocols

Authentication Header

- uses keyhash mechanism
- All data in cleartext

Encapsulating Security Payload

- Data confidential
- Data payload encrypted

Similarities

- Ensures data integrity
- also ensures data integrity.

Differences

- does not provide confidentiality
- provides optional replay protect
- provides data origin authentication
- provides confidentiality
- Anti replay protection
- does provide but optional.

Date:
Page No.

IPV4 and IPV6

version → of Protocol
header → length
low delay, → high output
header + → data

Version (4)	HLEN (4)	Type of service (8)	Total length (16)
packet-id for identity. Identification (16) bits group of frag. units	3 flag one Flag (3) bit	no. of data bytes Fragment offset (13) of particular datagram	ahead
TTL (8)	name of Protocol (8)	Header checksum (16)	
Sender	Source IP address (32)		
Receiver	Destination IP address (32)		
	options + Padding		

datagram lifetime

checking errors in datagram header

helps to handle priority of packet

Date.
Page No.

↑ least priority discarded

↑ if congestion

Version (4)	Priority / Traffic Class (8)	Flow Label (2)
Payload length (16)	Next header (8)	Hop limit (8)
Source Address (128)		
Destination (128)		
Extension headers ()		

Flow label: used to label packets belonging to the same flow in order to request special handling by IPv6 routers

Payload Length: total size of payload (total info contained

Next header: type of extension header (if present)

Hop limit: maximum no of hops allowed.

extension header: rectify limitations of the IP V4 option field, extension headers are introduced.