6. IP Security 4

Thursday, March 4, 2021 1:04 PM

Transport mode
- Encrypts payload
- Host-to-host
- Also maintains integrity of the payload

IP Header	Data

IP header	ESP/AH	Data

-original header remains
Actual SIP & DIP is visible

Best protection: hiding the source and destination IP (can be done in VPN)

Tunnel mode:

IP header	Data

New IP header	ESP/AH	IP header	Data

R1 and R2 connected via the internet (multiple intermediate routers).
In tunnel mode, the source and destination addresses of the **routers** is added to the packet as new IP header.

The actual source and destination addresses are hidden in the packet and are encrypted along with the data
--> virtual private mode
Intruders cannot detect actual sender and receiver
Firewall-to-firewalll

New packet in tunnel mode AH

SIP	DIP	AH header	IP header	TCP	Data

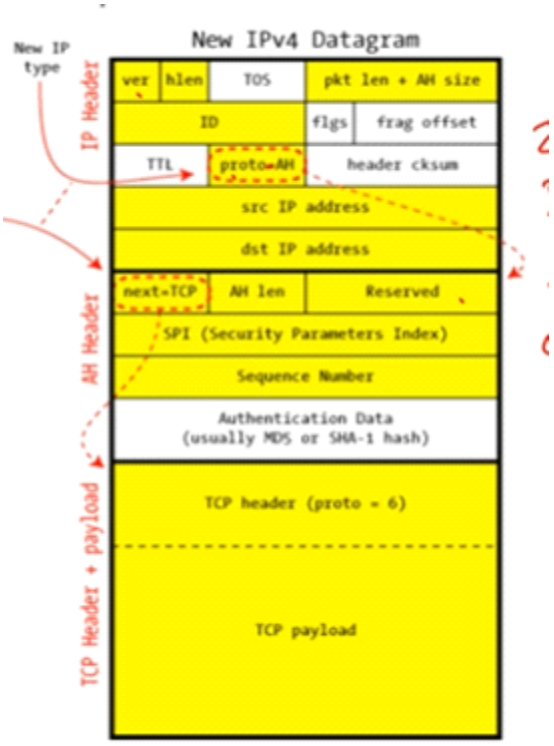
Integrity provided for all mutable and immutable fields

Receiver decode s

IP datagram (IP layer)
Segment (transport layer)

IPv4 header in AH transport mode

IP header	AH header	TCP header + payload



Yellow-> protected by Authentication data

Handshaking between two points to ensure algorithms for digest and encryption