Other Useful Protocols

Internet Control Message Protocol (ICMP)
- It's the text messaging of network devices
- It's carried by IP but it's not used for data transfer
- Devices can request and reply to administrative requests (Even when things don't go well, i.e. error messages)

Generic Routing Encapsulation (GRE)
- Encapsulate traffic inside of IP
- It can be thought of as the tunnel between 2 endpoints
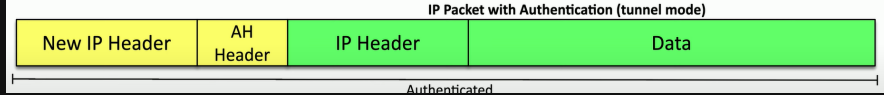- Not built-in encryption

Virtual Private Networks (VPN)
- Encrypts data that's transmitted over a public network
- Concentrator is used for encryption/decryption and it's often integrated into a firewall
- Many development options, for example, it can be implemented through a specialized hardware or it can be done through a software, etc..
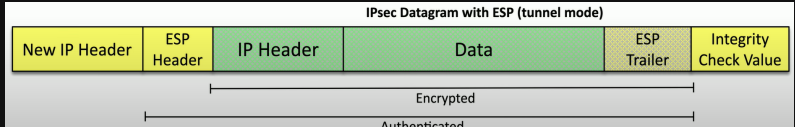
Internet Protocol Security (IPSec)
- Used for authentication and encryption
- Provides Confidentiality and Integrity (anti-replay)
- It's very standardized and very common

2 types of protocols used by IPSec

Authentication Header (AH)

IP Packet with Authentication (tunnel mode)

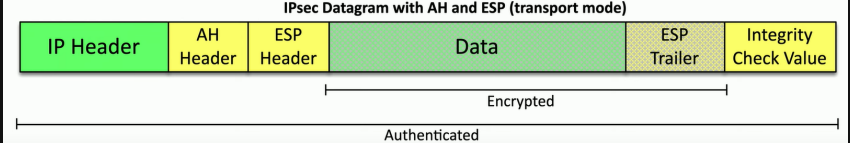| New IP Header	AH Header	IP Header	Data

Authenticated

The AH header includes a hash of the packet and a shared key
MD5, SHA1, or SHA2 are common

When the packet is received the packet is hash is recalculated and the hash is compared to the existent hash to validate the integrity of the packet
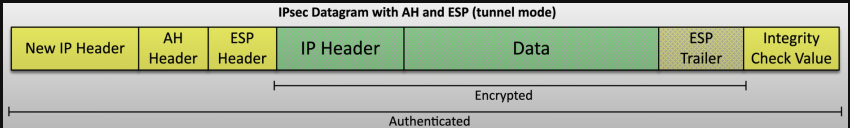
Encapsulation Security Payload (ESP)

IPsec Datagram with ESP (tunnel mode)

New IP Header	ESP Header	IP Header	Data	ESP Trailer	Integrity Check Value

Encrypted
Authenticated

MD5, SHA1, or SHA2 are common for hashing while 3DES or AES are common for encryption

Transport Mode

IPsec Datagram with AH and ESP (transport mode)

IP Header	AH Header	ESP Header	Data	ESP Trailer	Integrity Check Value

Encrypted
Authenticated

Transport Mode

Tunnel Mode

IPsec Datagram with AH and ESP (tunnel mode)

New IP Header	AH Header	ESP Header	IP Header	Data	ESP Trailer	Integrity Check Value

Encrypted
Authenticated

Tunnel Mode

Original packet

IP Header	Data

Transport mode

IP Header	IPsec Headers	Data	IPsec Trailers

Tunnel mode

New IP Header	IPsec Headers	IP Header	Data	IPsec Trailers
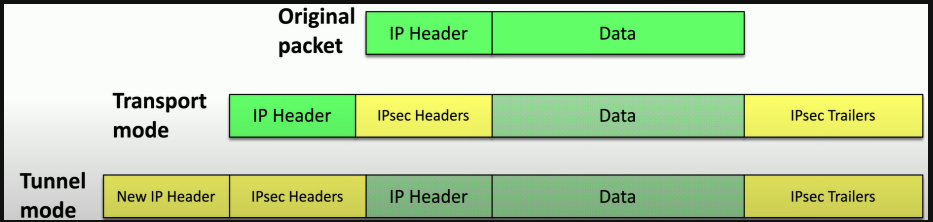
In Transport mode the IP header isn't secured this is why to have extra security in Tunnel mode, a new IP header is added