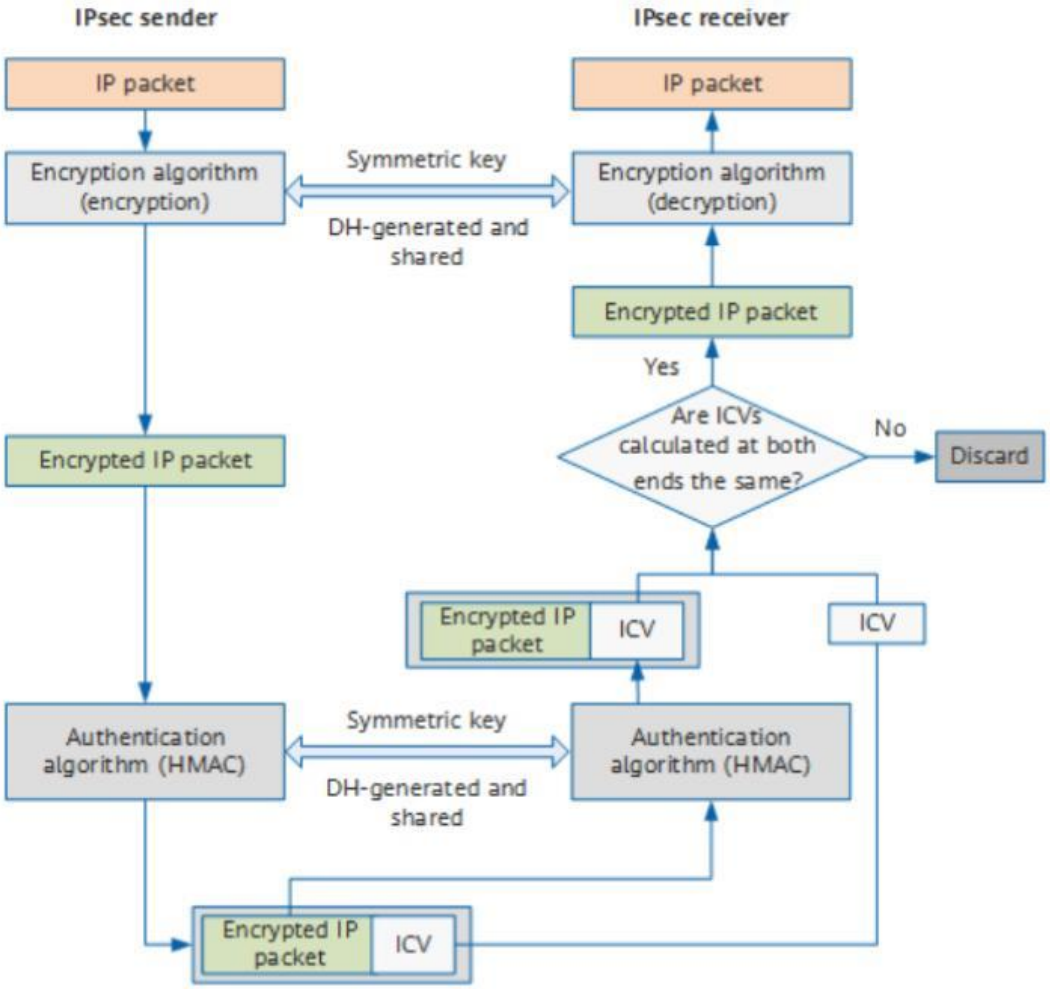
Lecture 15

In the previous lecture:

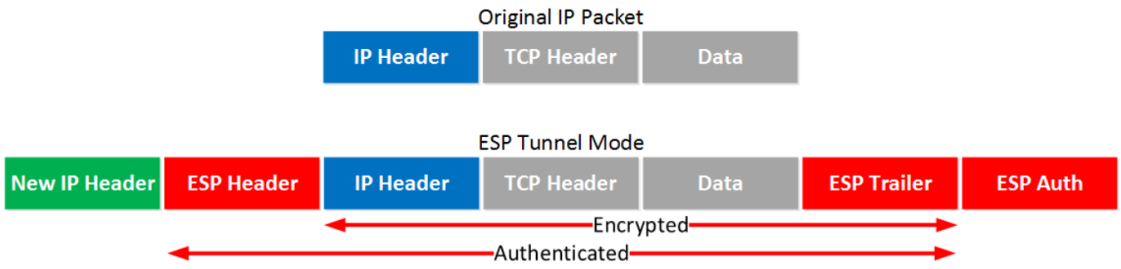


IPsec encryption and authentication process

In today's class: Details of (Encrypted IP Packet+ICV=IPsec packet)

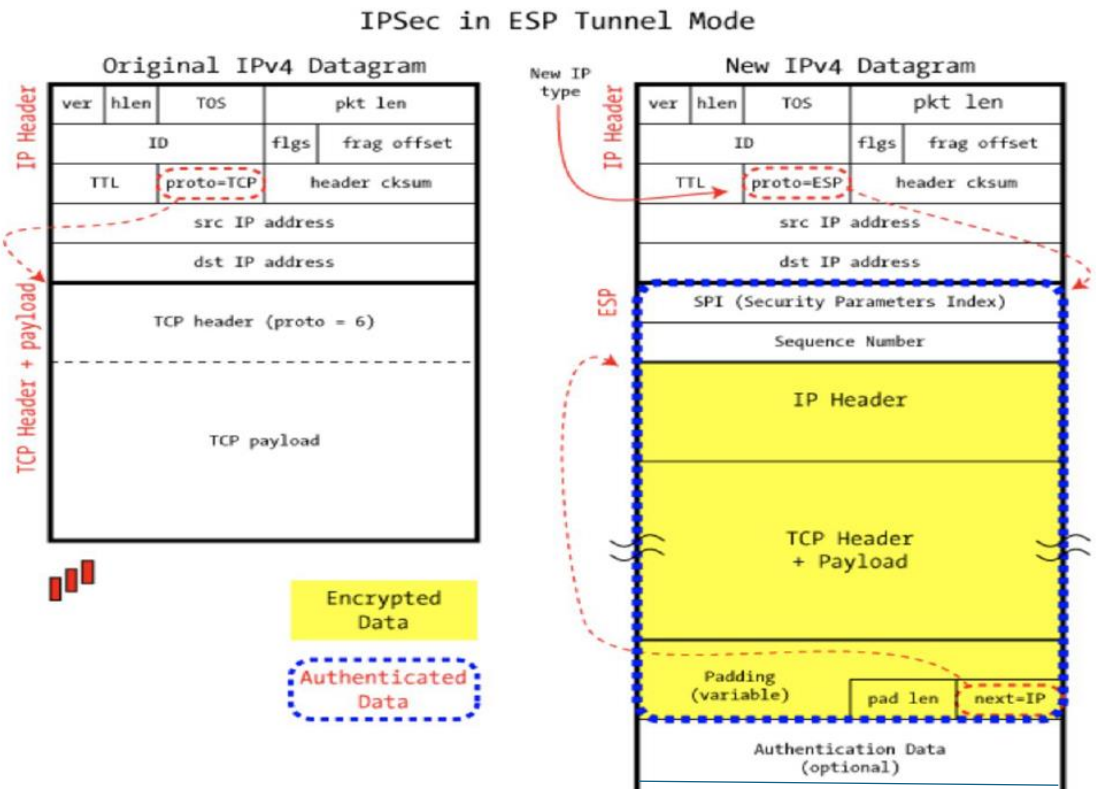
That is, How an IP packet is converted into an IPsec packet: There are various ways to do that. A good option is below.

IPsec in ESP (Encapsulating security payload) Tunnel mode



IPsec in ESP Tunnel mode (in more detail)

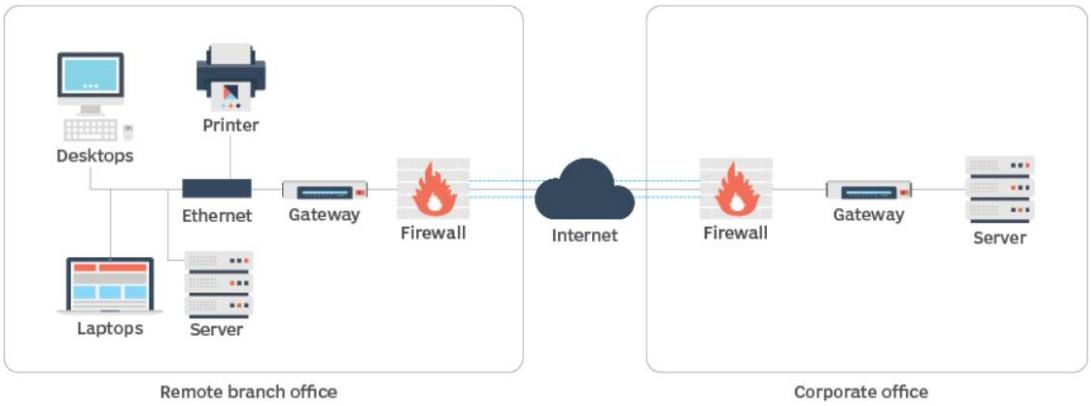
Data = TCP Payload



So far we talked about Router-to-router VPN (also known as gateway-to-gateway or site-to-site VPN). Picture as follows:

SITE-TO-SITE VPN

Site-to-site VPNs connect multiple networks to each other, typically a branch office to a company headquarters. In this setup, hosts do not have VPN client software; they send and receive TCP/IP traffic through a VPN gateway, which encapsulates and encrypts outbound traffic, sending it through a VPN tunnel over the internet to a peer VPN gateway at the target site. The peer VPN gateway decrypts the content and relays the packets to the target host.



There is another type of VPN. Known as Remote-access server. Picture as follows:

REMOTE ACCESS VPN

Remote access VPNs connect individual users to a corporate host network from any location. These VPNs require VPN client software at remote sites and at the host location. When a remote user sends traffic, VPN client software encapsulates and encrypts that traffic before sending it over the internet to a VPN gateway at the edge of the corporate network. Firewalls may also be present to further protect network traffic.