Aalto University

Network Security: IPsec session protocol

Tuomas Aura

CS-E4300 Network security

Aalto University

Session protocol

- Encapsulated Security Payload (ESP) [RFC 4303]
  - Encryption and MAC for each IP packet
  - Optional replay protection with sequence numbers

Features to avoid:

- ESP with encryption only is insecure but allowed by some IPsec APIs
- Authentication Header (AH) – authentication only, no encryption
  - Do not use for new applications
  - Exists because of US export controls in the 1990s

Session protocol modes

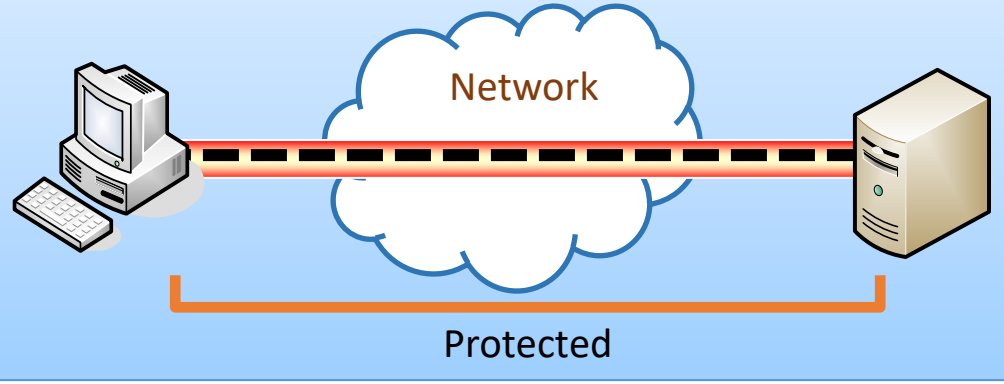
- Transport mode:
  - Host-to-host security
  - ESP header added between the original IP header and payload
- Tunnel mode:
  - Typically used for tunnels between security gateways to create a VPN
  - Entire original IP packet encapsulated in a new IP header plus ESP header
- In practice, IPsec is mainly used in tunnel mode

Transport and tunnel mode

Could be used for end-to-end protection of intranet traffic

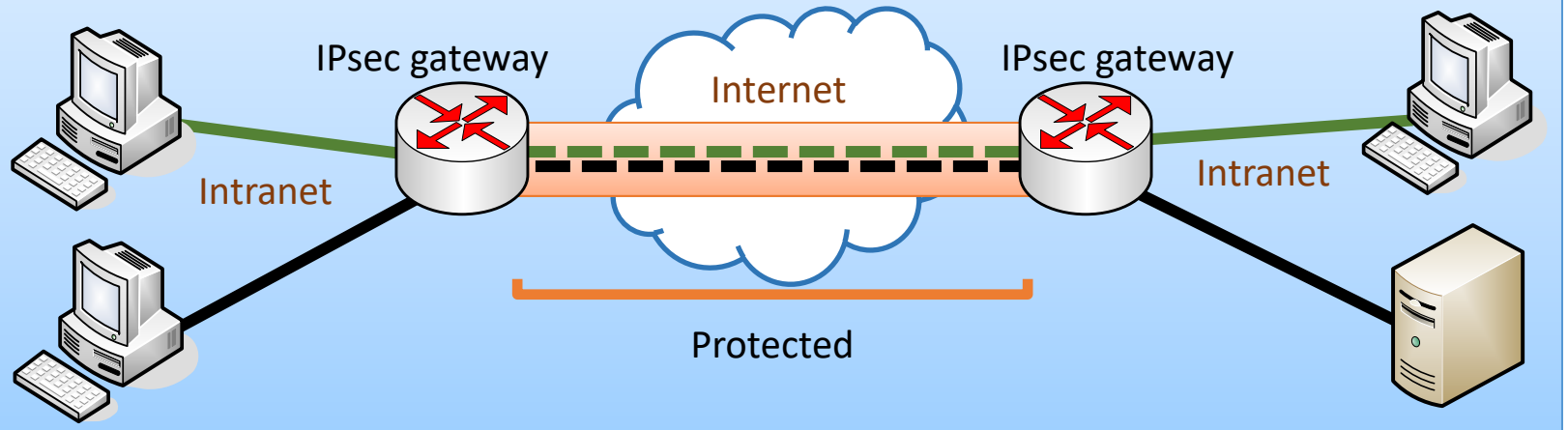
Transport mode

Encryption and/or authentication from end host to end host



Tunnel mode

Encryption and/or authentication between two gateways



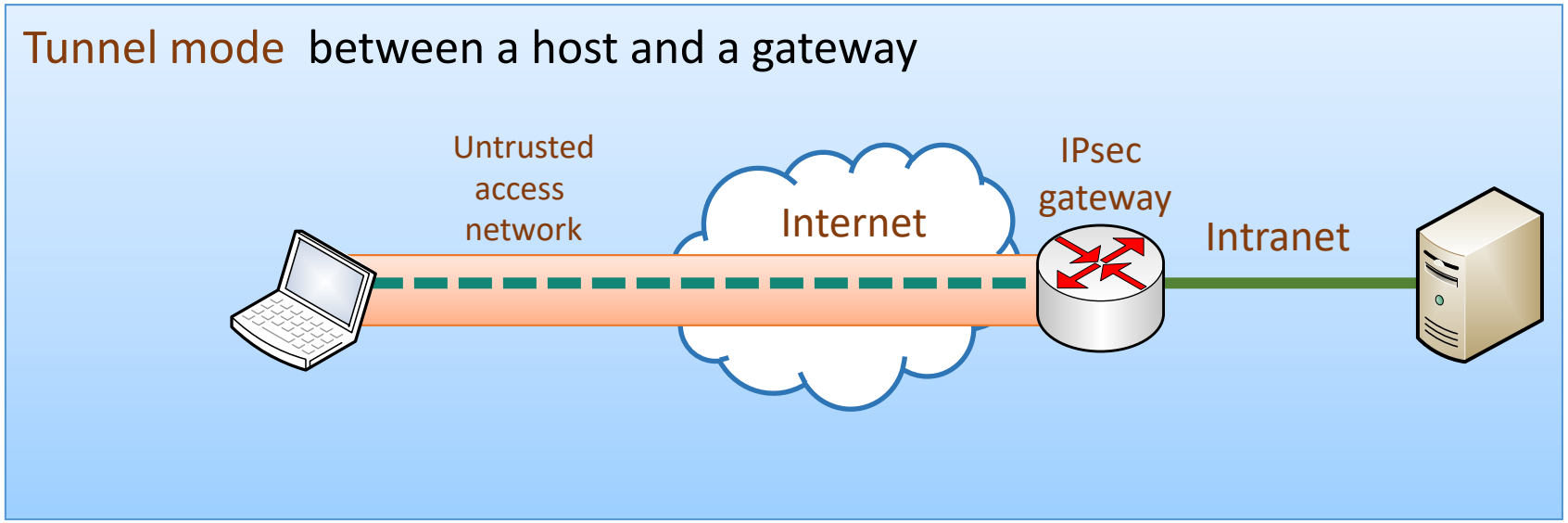
! Typical for site-to-site VPN

Gateway routers establish the IPsec tunnel; routing rules send traffic through the tunnel

Host-to-gateway VPN

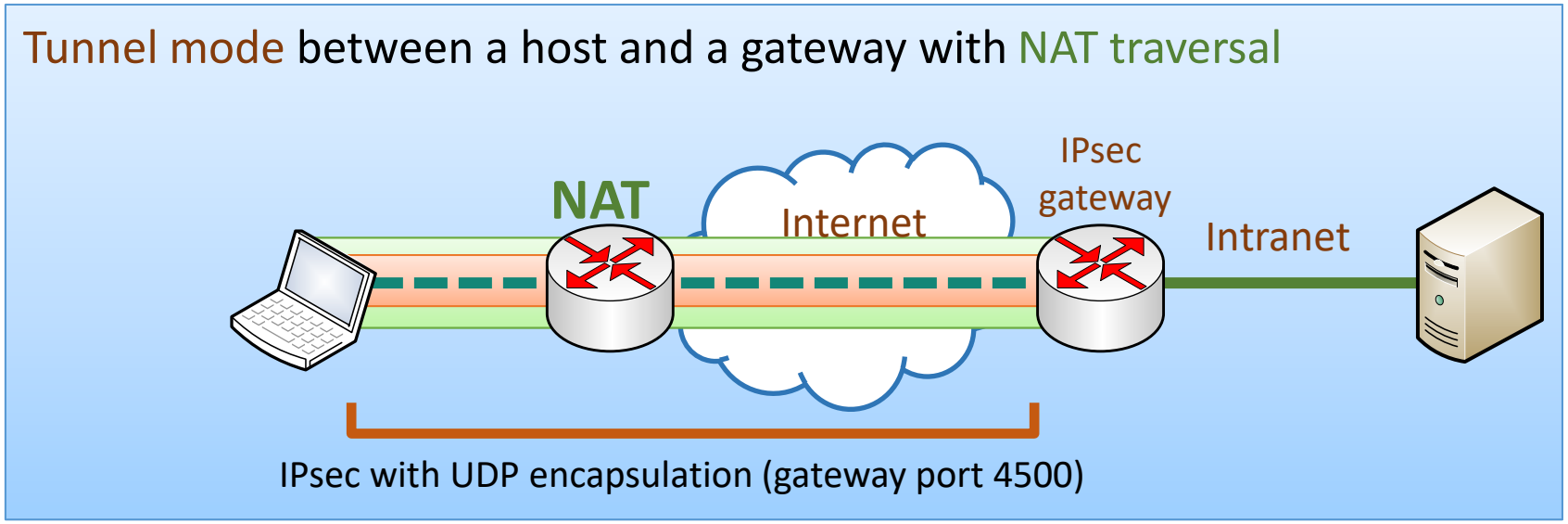
Mobile-user VPN back to office

without NAT



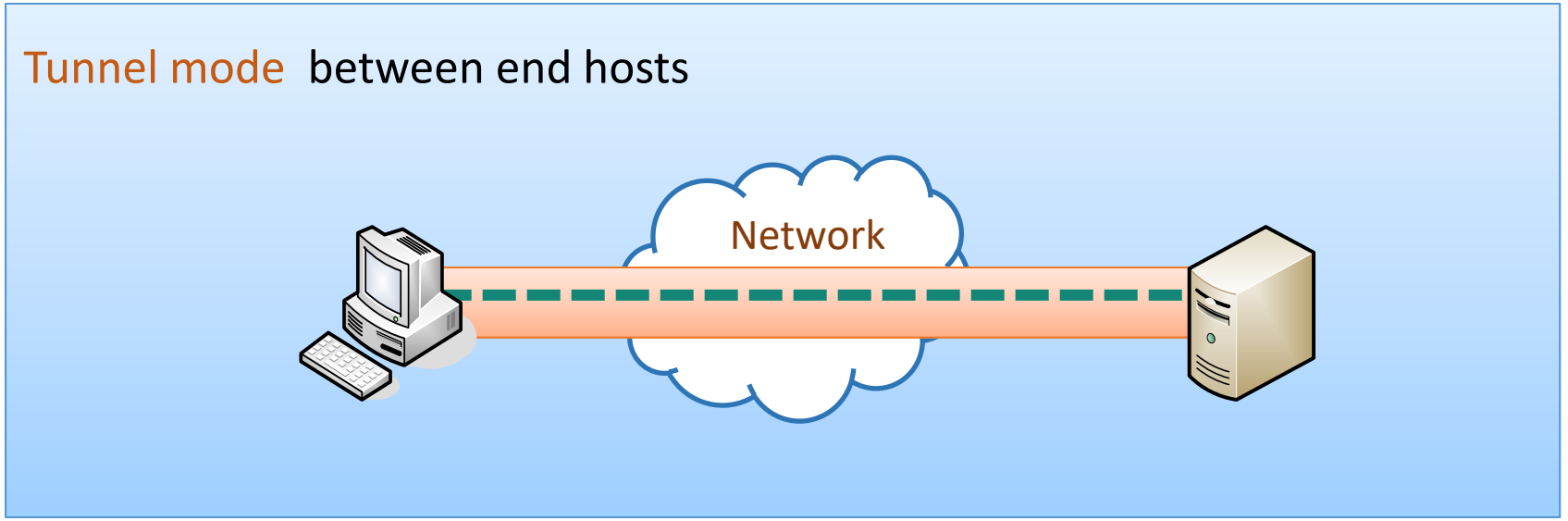
Host gets an IP address from the gateway router and becomes part of the intranet

! Typical scenario with NAT



Tunnel mode between hosts

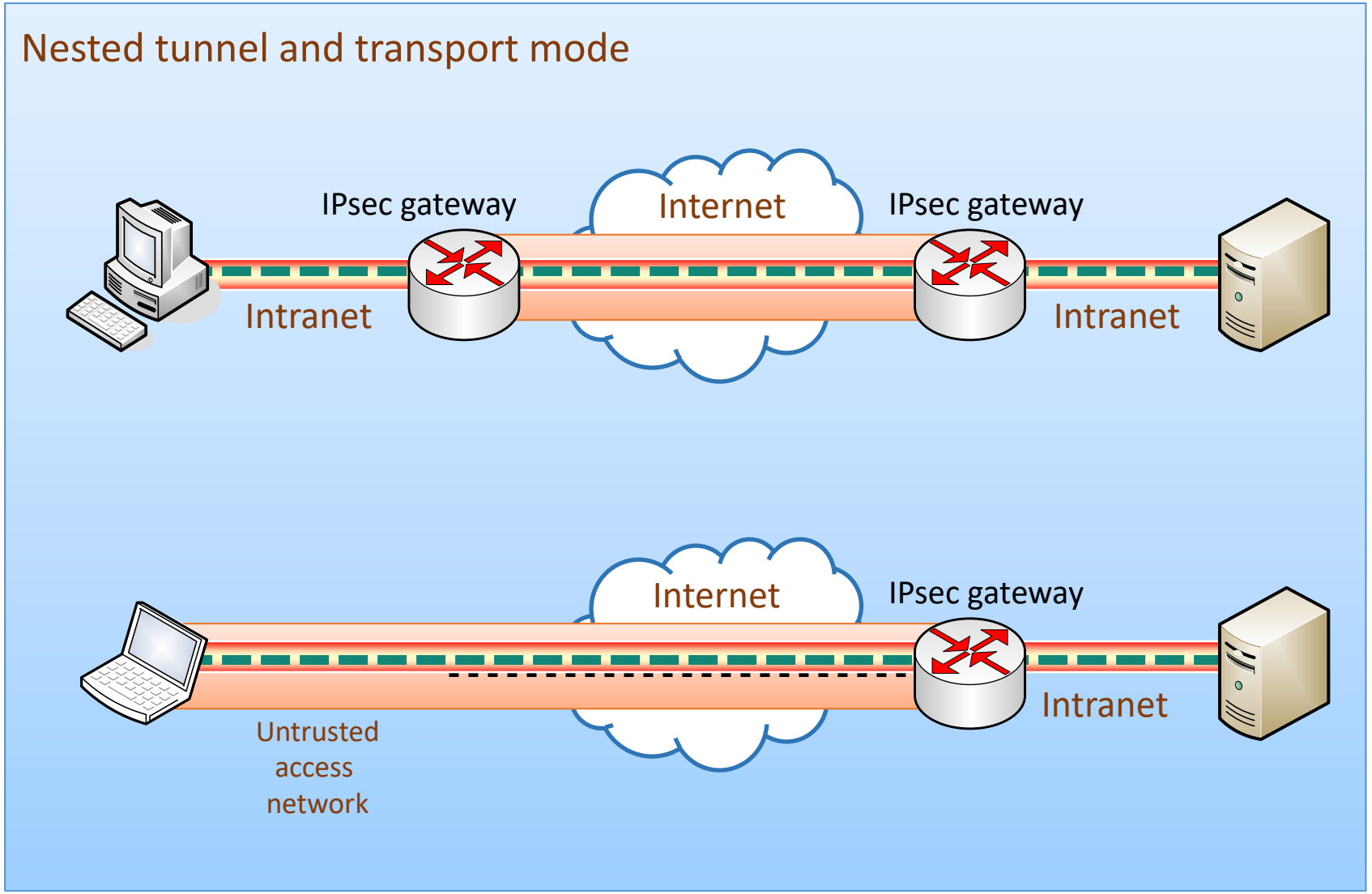
Security equivalent to transport mode



Nested protection

Combined VPN and end-to-end protection

– less common but possible

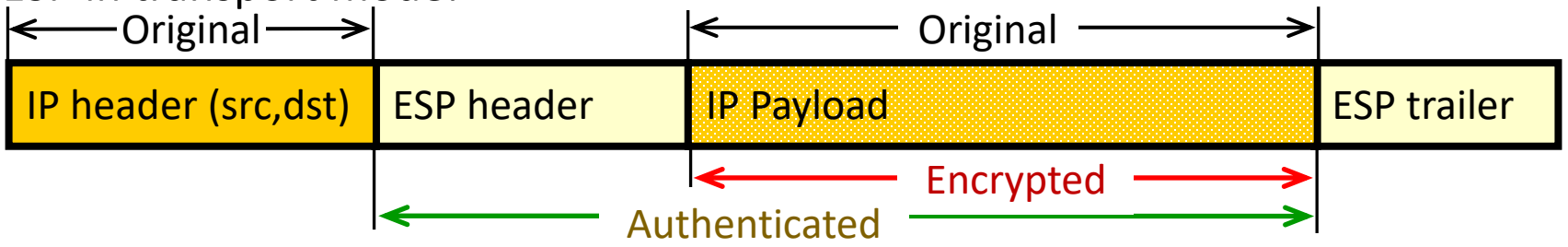


ESP packet formats

Original IP packet:

ESP header	=	SPI + sequence number
ESP trailer	=	padding + integrity check (HMAC)

ESP in transport mode:



ESP in tunnel mode:

ESP in tunnel mode with NAT traversal:

!

ESP tunnel headers

- Tunnel-mode ESP packet:

IP header(src gateway, dst gateway) |
UDP(gateway port 4500) |
ESP header(spi, sqn) |
IP header(src host, dst host) |
payload |
ESP trailer(padding, integrity check)

Outer IP header with gateway IP addresses

UDP header for NAT traversal

Security association identifier SPI, and optional sequence number for replay protection

Inner IP header with end-host IP addresses (=original IP header)

Original TCP/UDP/SCTP/ICMP

HMAC

Host-to-gateway VPN and IP addresses

- Tunnel-mode ESP packet:

IP header(src gateway, dst gateway) |
UDP(gateway port 4500) |
ESP header(spi, sqn) |
IP header(src host, dst host) |
payload |
ESP trailer(padding, integrity check)S

Outer IP header:

- Host's current IP address and the gateway IP addresses
- With NAT, the host's IP address changes on the way, and the UDP header is included

Inner IP header:

- Host's intranet address as the source or destination
- Intranet server IP address as the other endpoint