IPsec, tunneling, and VPNs
IV1013

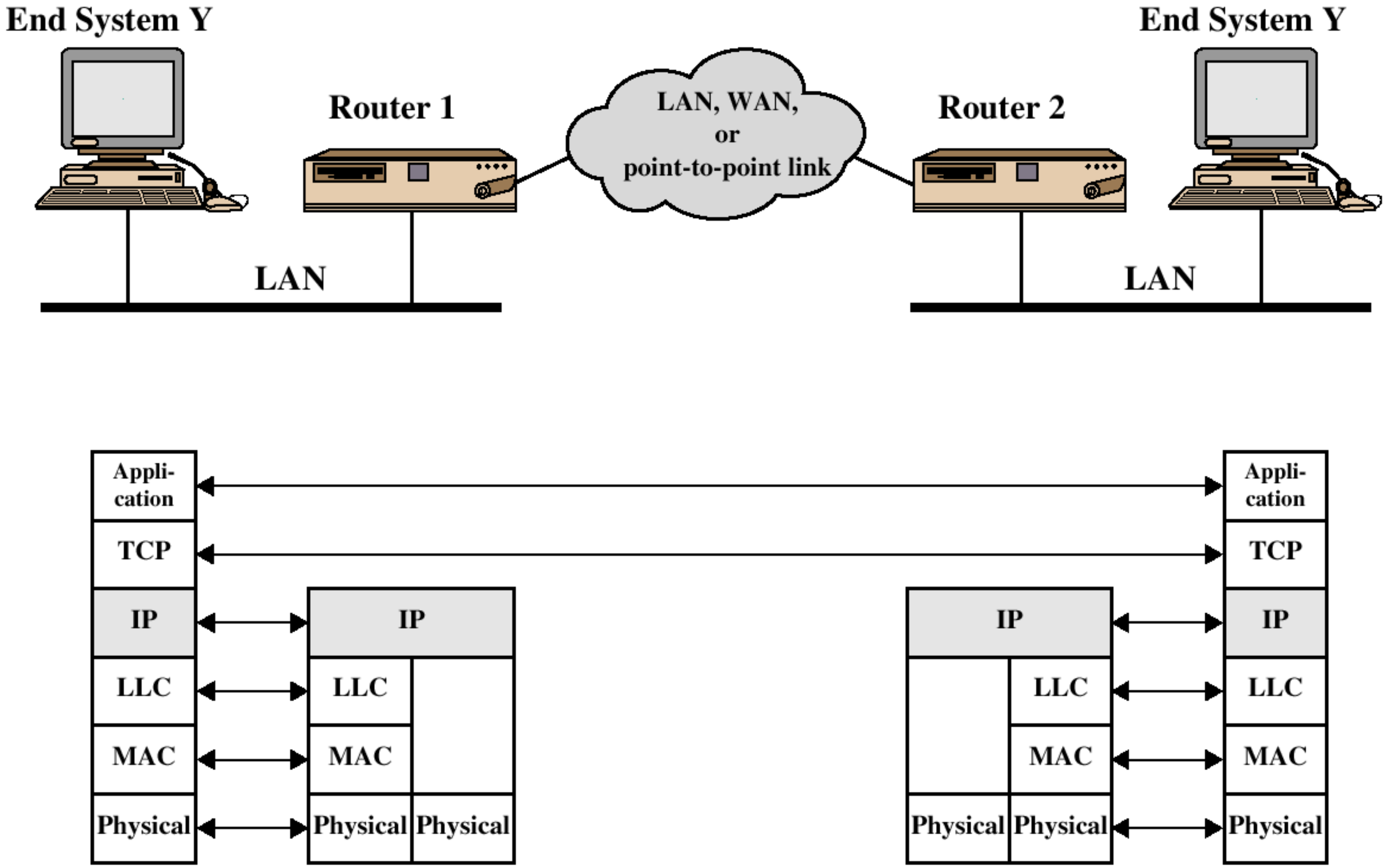
Markus Hidell, mahidell@kth.se
KTH School of ICT

Acknowledgements

- The presentation builds upon material from
  - Previous slides by Markus Hidell and Peter Sjödin
  - Material by Vitaly Shmatikov, Univ. of Texas
  - *Network Security Essentials*, 5th ed, William Stallings, Pearson
  - *Computer Networking: A Top Down Approach*, 5th ed, Jim Kurose, Keith Ross, Addison-Wesley
  - *TCP/IP Protocol Suite*, 4th ed, Behrouz Foruzan, McGraw-Hill

IPsec

TCP/IP



Appli-cation
TCP
IP
LLC
MAC
Physical

IP
LLC
MAC
Physical
Physical

IP
LLC
MAC
Physical
Physical

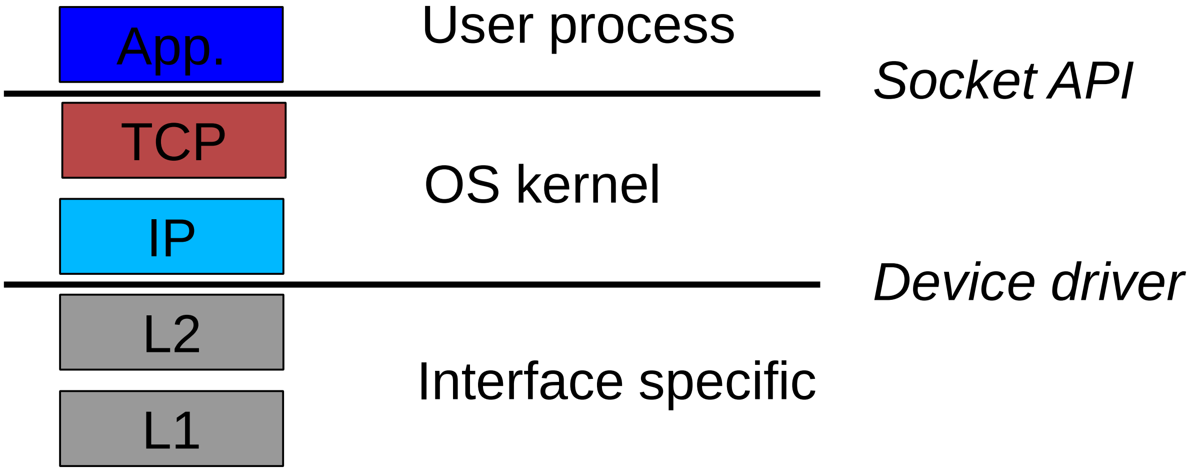
Appli-cation
TCP
IP
LLC
MAC
Physical

IP Security Issues

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service

- Many solutions are application-specific
  - TLS for Web, S/MIME for email, SSH for remote login
- IPsec aims to provide a framework of open standards for secure communications over IP
  - Protect every protocol running on top of IPv4 and IPv6

Operating System Layers



- SSL (Secure Socket Layer) changes the API to TCP/IP
  - Applications change, but OS doesn’t
  - TCP does not participate in the cryptography...(DoS attacks)
- IPsec implemented in OS
  - Applications and API remain unchanged (at least in theory)
- To make full use of IPSec, API and apps have to change!
  - and accordingly also the applications (pass on other IDs than IP addr)

Overview of IPsec

- Scope, see RFC 6071
    - IPSec and IKE Roadmap
- Authenticated Keying
    - Internet Key Exchange (IKE)
- Data Encapsulation
    - ESP: IP Encapsulating Security Payload (RFC 4303)
    - AH: IP Authentication Header (RFC 4302)
- Security Architecture (RFC 4301)
    - Tunnel/transport Mode
    - Databases (Security Association, Policy, Peer Authorization)

IPsec: Network Layer Security

IPsec = AH + ESP + IKE

Protection for IP traffic
AH provides integrity and origin authentication
ESP also confidentiality

Sets up keys and algorithms for AH and ESP

- AH and ESP rely on an existing security association
  - Idea: parties must share a set of secret keys and agree on each other's IP addresses and crypto algorithms
- Internet Key Exchange (IKE)
  - Goal: establish security association for AH and ESP
  - If IKE is broken, AH and ESP provide no protection!

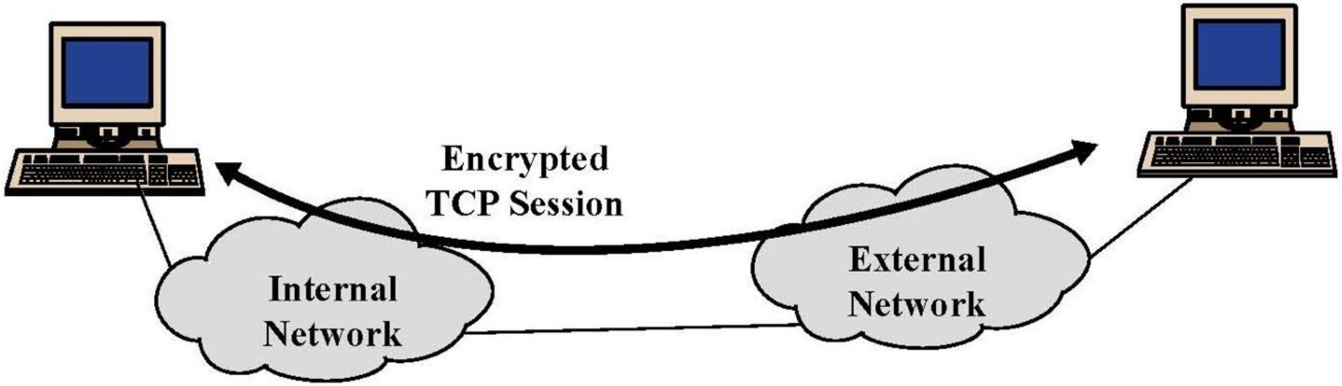
IPsec Security Services

- Authentication and integrity for packet sources
  - Ensures connectionless integrity (for a single packet) and partial sequence integrity (prevent packet replay)
- Confidentiality (encapsulation) for packet contents
- Access control
- Authentication and encapsulation can be used separately or together
- Either provided in one of two modes
  - Transport mode
  - Tunnel mode

IPsec Modes

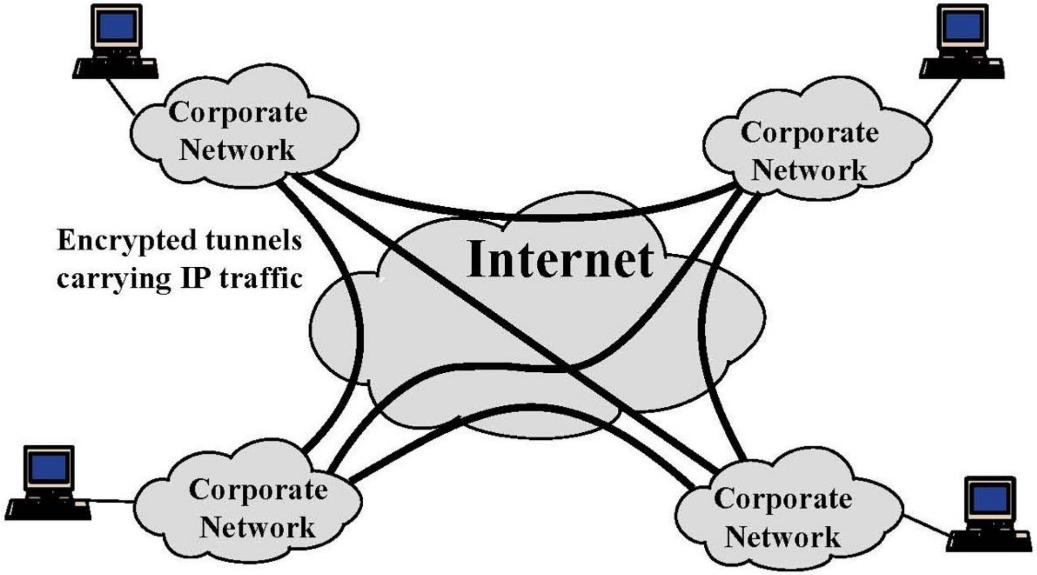
- Transport mode
  - Used to deliver services from host to host or from host to gateway
  - Usually within the same network, but can also be end-to-end across networks
- Tunnel mode
  - Used to deliver services from gateway to gateway or from host to gateway
  - Usually gateways owned by the same organization
    - With an insecure network in the middle

IPsec in Transport Mode



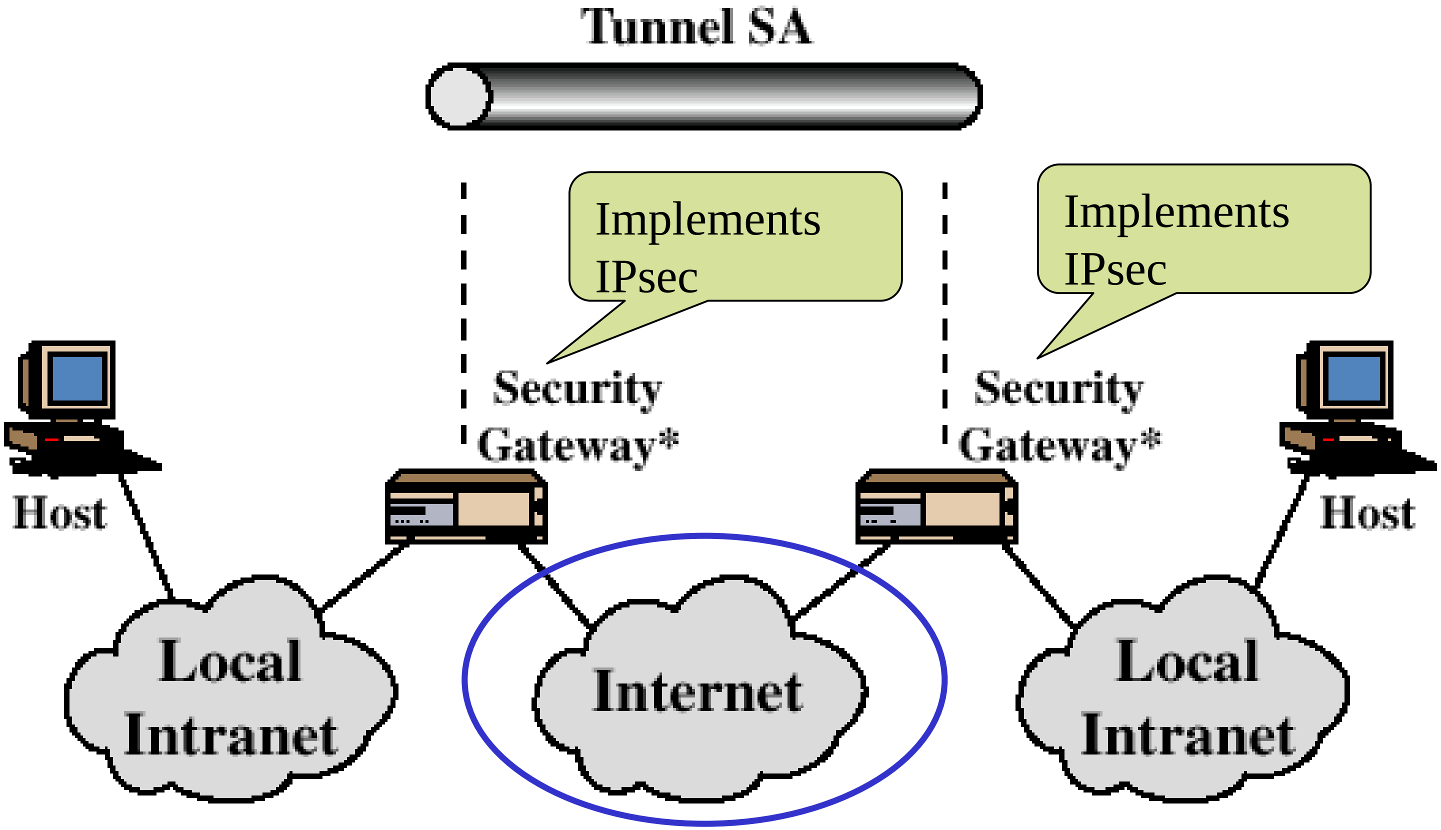
- End-to-end security between two hosts
- Requires IPsec support at each host

IPsec in Tunnel Mode



- Gateway-to-gateway security
  - Internal traffic behind gateways not protected
  - Typical application: virtual private network (VPN)
- Only requires IPsec support at gateways
  - API /application changes not an issue

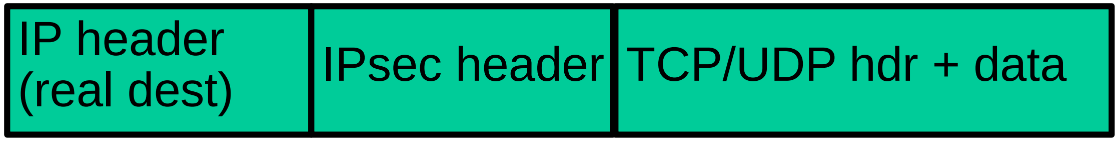
Tunnel Mode Illustration



IPsec protects communication on the insecure part of the network

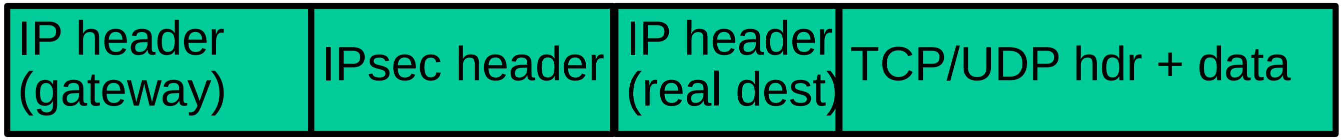
Transport Mode vs Tunnel Mode

- Transport mode secures packet payload and leaves IP header unchanged



IP header (real dest)	IPsec header	TCP/UDP hdr + data

- Tunnel mode encapsulates both IP header and payload into IPsec packets



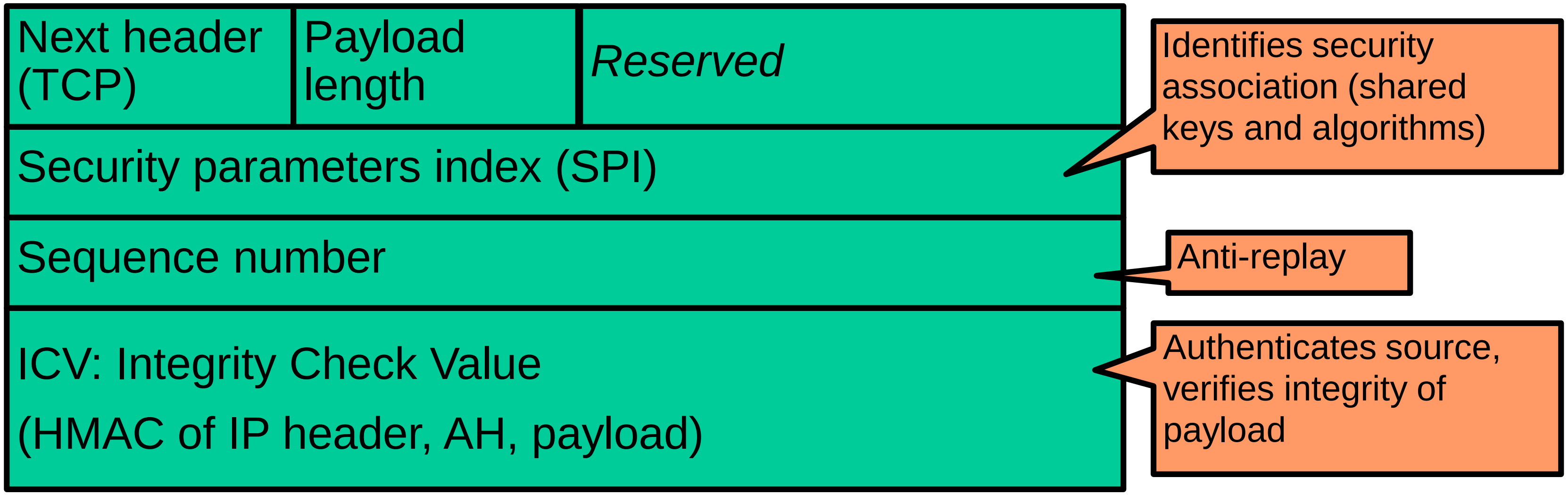
IP header (gateway)	IPsec header	IP header (real dest)	TCP/UDP hdr + data

Security Association (SA)

- One-way sender-recipient relationship
  - Manually configured or negotiated through IKE
- SA determines how packets are processed
  - Cryptographic algorithms, keys, AH/ESP, lifetimes, sequence numbers, mode (transport or tunnel)
- SA is uniquely identified by {SPI, dst IP addr, flag}
  - SPI: Security Parameter Index
    - Chosen by destination (unless traffic is multicast...)
  - Flag (security protocol identifier): ESP or AH
  - Each IPsec implementation keeps a database of SAs
  - SPI is sent with packet, tells recipient which SA to use

Authentication Header Format

- Provides integrity and origin authentication
- Authenticates portions of the IP header
- Anti-replay service (to counter denial of service)
- No confidentiality



Next header (TCP)

Payload length

Reserved

Security parameters index (SPI)

Sequence number

ICV: Integrity Check Value

(HMAC of IP header, AH, payload)

Identifies security association (shared keys and algorithms)

Anti-replay

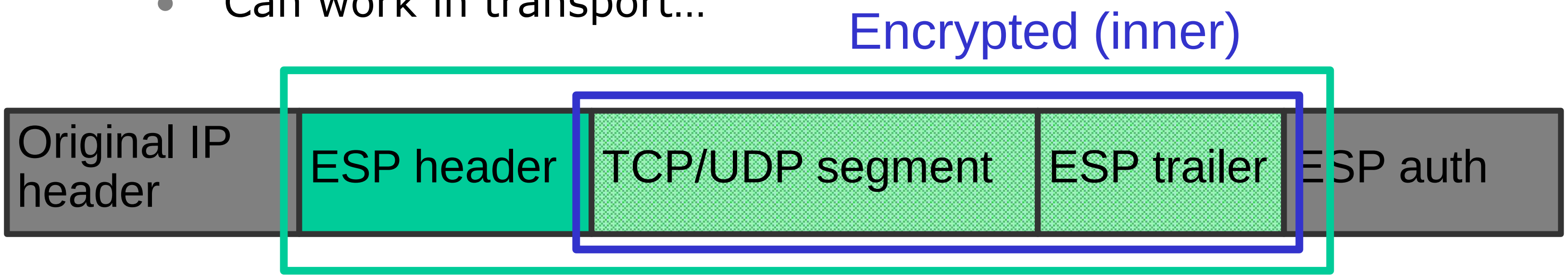
Authenticates source, verifies integrity of payload

ESP: Encapsulating Security Payload

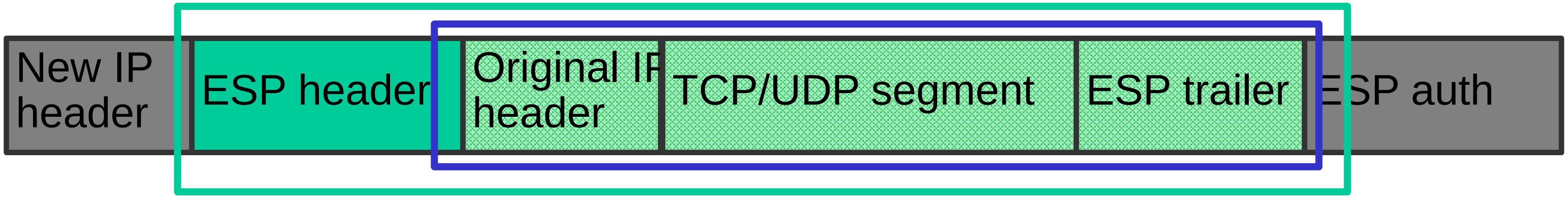
- RFC 4303
- Adds new header and trailer fields to packet
- Transport mode
  - Confidentiality of packet between two hosts
  - Complete hole through firewalls (for IPsec from a particular IP address)
  - Used sparingly
- Tunnel mode
  - Confidentiality of packet between two gateways or a host and a gateway
  - Implements VPN tunnels
  - FW filtering can be done on packets before they enter tunnel

ESP Security Guarantees

- Confidentiality and integrity for packet payload
  - Symmetric cipher negotiated as part of security assoc
- Optionally provides authentication (similar to AH)
- Can work in transport…



- …or tunnel mode (problem with NAT)

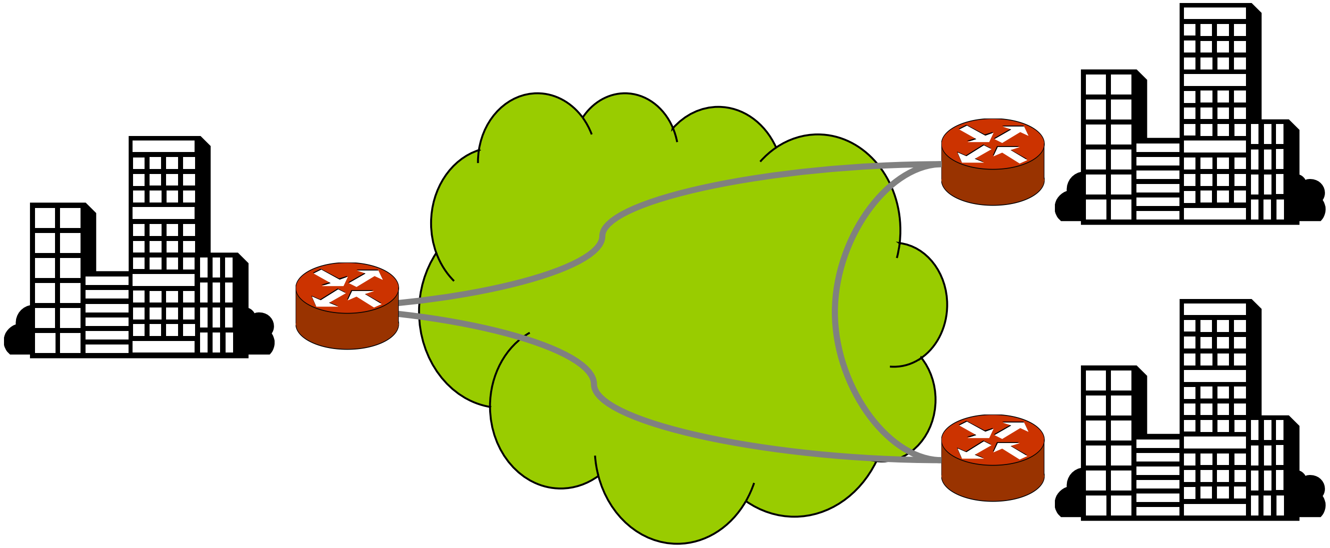


Tunnel Mode and NAT

- Tunnel mode can be problematic together with NAT
- If we set up a tunnel between our host and a public gateway, it won’t work:
  - Our private addresses will be in the original IP header
- It is OK to set up a tunnel between our host and a private intranet:
  - Private intranet addresses will be in the original IP header
  - New IP header will contain our home private address, which will be translated by the NAT

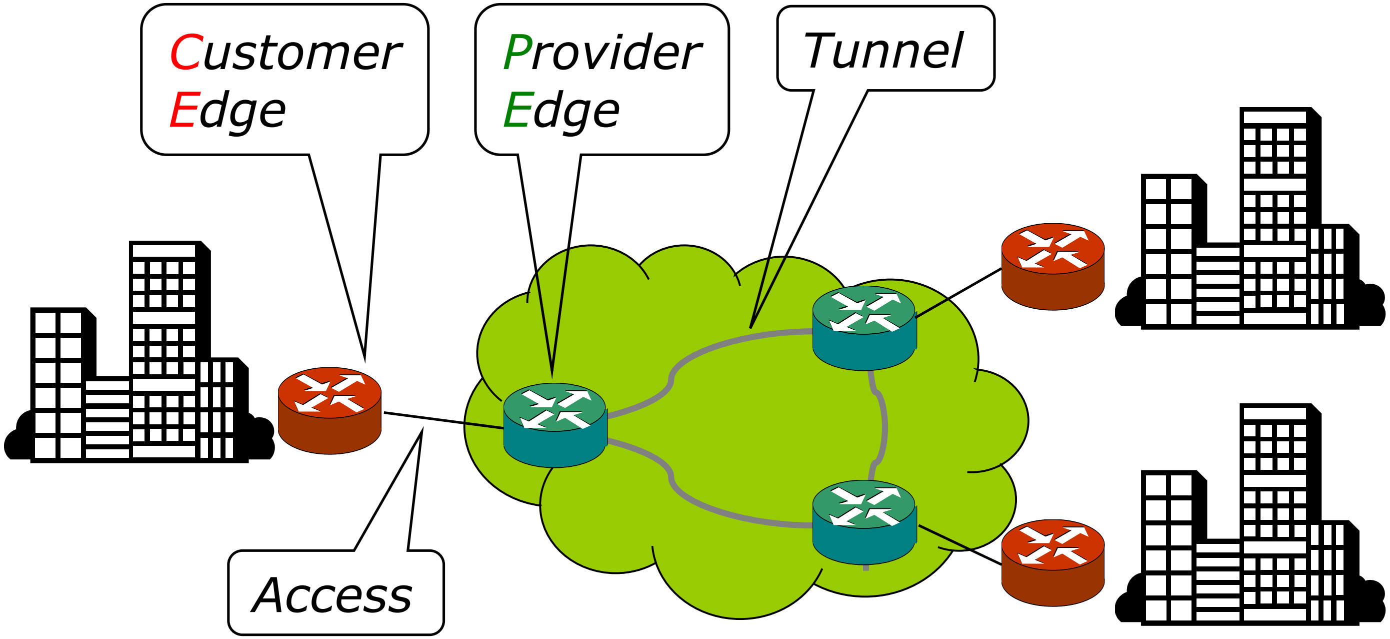
VPNs

Virtual Private Network



- Extensions of corporate network
- Over service provider’s infrastructure
  - “Provider provisioned”
- Resembles a true, physical network
  - Hence “virtual”

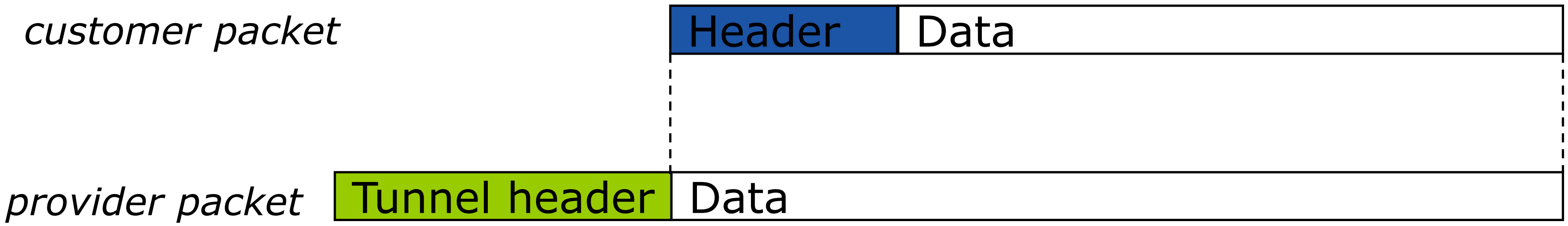
Basic Idea



- Data arrives from CE (Customer Edge) via access network
- Encapsulated by PE (Provider Edge) and sent over tunnel
- Decapsulated by receiving PE and sent over access network to CE

- Questions
  - How to tunnel packets?
  - Access method between PE and CE?
  - Service provided by PE to CE?

Tunneling



- Protocol encapsulation
  - customer (payload) protocol in provider (network) protocol
- Add a provider protocol header
  - IP, GRE, MPLS, L2TP, IPSec, …
- Customer packet carried **transparently** across provider's network
  - Any format possible!
- Source and destination addresses of tunnel header define tunnel endpoints
  - Configured for the tunnel
- Tunneling is used for many other purposes as well
  - IP multicast over non-multicast networks
  - IPv6 over IPv4 networks
  - …

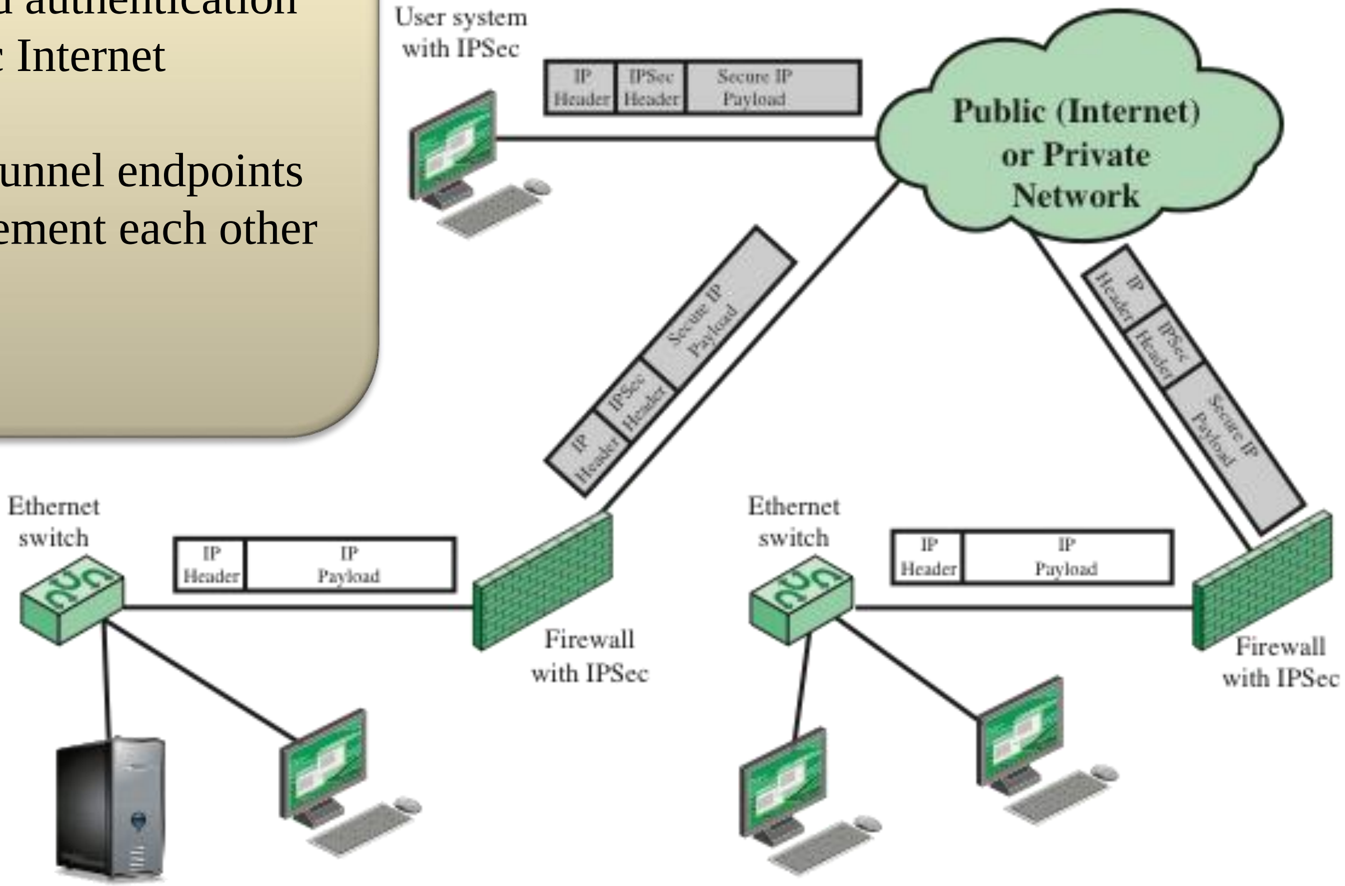
Secure VPNs

- IPsec ESP is often used to implement a VPN
  - Packets go from internal network to a gateway with TCP/IP headers for address in another network
  - Entire packet hidden by encryption
    - Including original headers so destination addresses are hidden
  - Receiving gateway decrypts packet and forwards original IP packet to receiving address in the network that it protects
- This is known as a IPsec VPN tunnel
  - Secure communication between parts of the same organization over public Internet
- The term IPsec VPN is sometimes used for secure VPNs in general
  - Even though they don’t use the IPsec protocols…

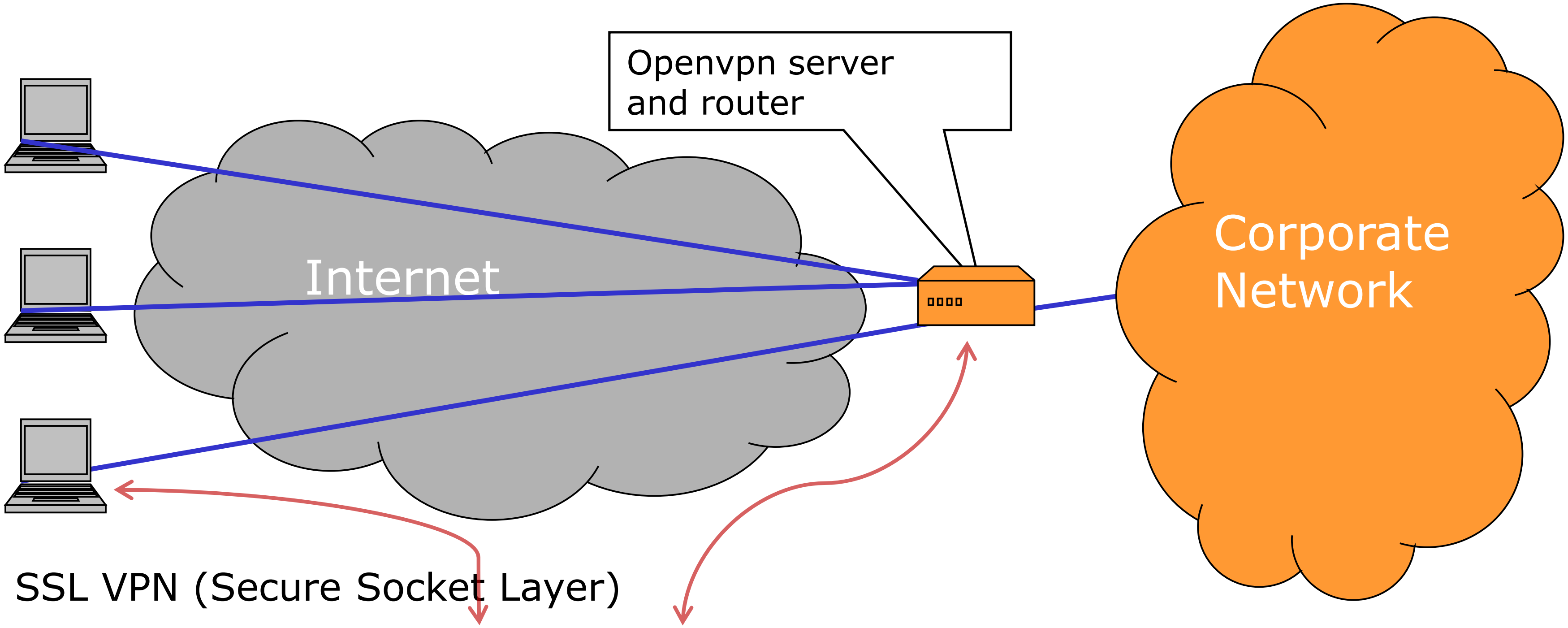
IPsec VPN

VPNs with IPsec tunnels
IPsec adds encryption and authentication
Protect traffic over public Internet

Firewalls with IPsec are tunnel endpoints
IPsec and firewall complement each other

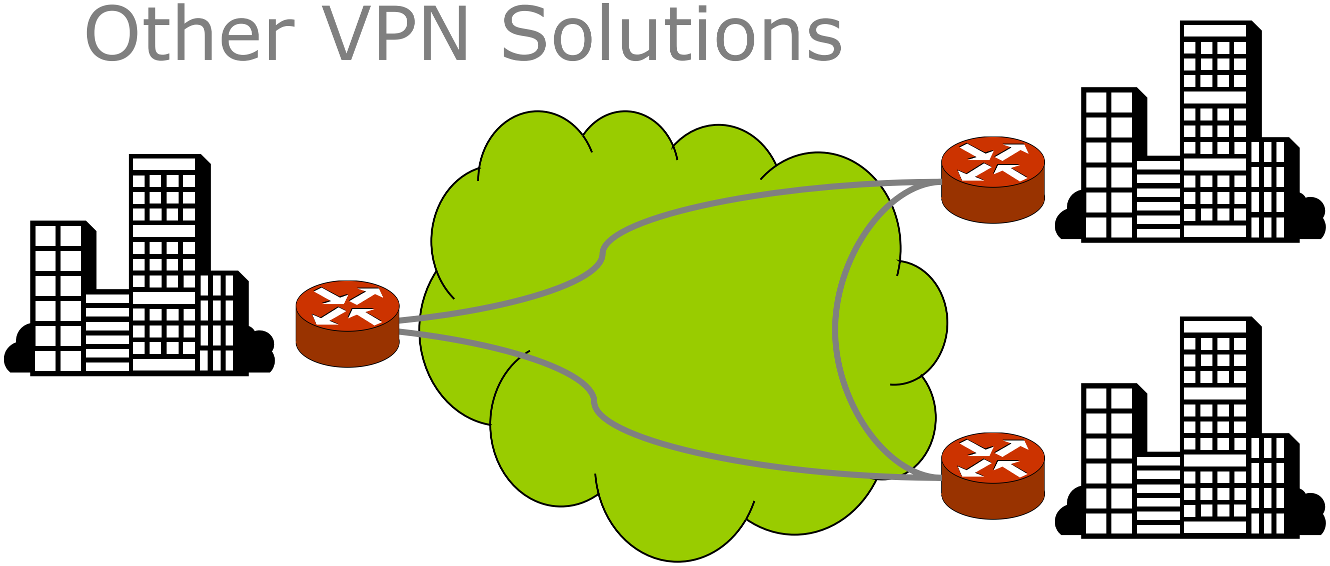


OpenVPN Network



- SSL VPN (Secure Socket Layer)
- Software running on hosts and server
  - Open source, www.openvpn.net
- **Virtual Layer 2 Network (Ethernet)**
- UDP tunnels over Internet as “cables”
- OpenVPN server works as an Ethernet switch
  - Built-in DHCP server
- A local network interface (Ethernet) on client as tunnel endpoint
  - “tap0” or similar

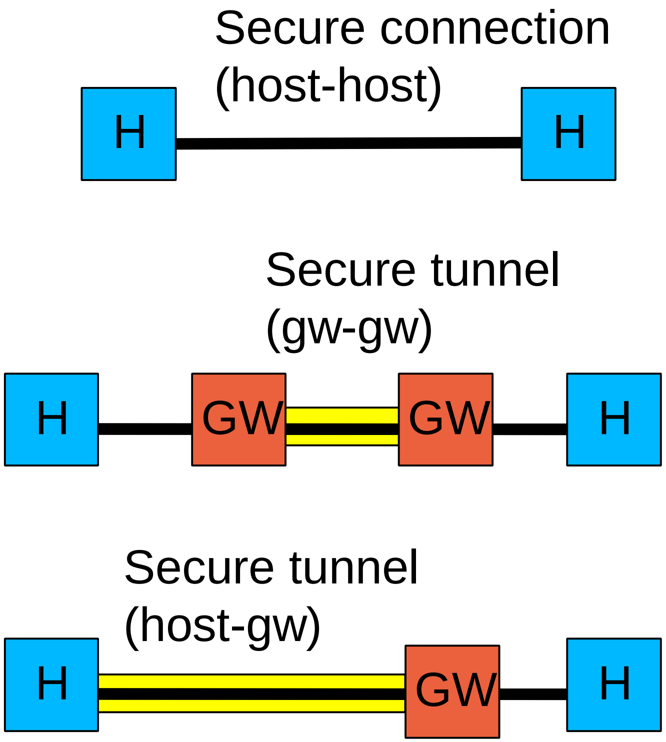
Other VPN Solutions



- PPTP—Point-to-Point Tunneling Protocol
  - Call control and management + PPP encapsulated in GRE, carried over IP
- L2TP—Layer 2 Tunneling Protocol
  - Dynamic setup, maintenance, and teardown of multiple layer 2 point-to-point tunnels
- PPTP and L2TP does not provide confidentiality and authentication themselves—rely on protocols being tunneled

IPsec Use Cases—Summary

- Host-Host
  - Transport mode
  - (Or tunnel mode)
- Gateway-Gateway
  - Tunnel mode
- Host-Gateway
  - Tunnel mode



ROYAL INSTITUTE
OF TECHNOLOGY

Thanks for listening