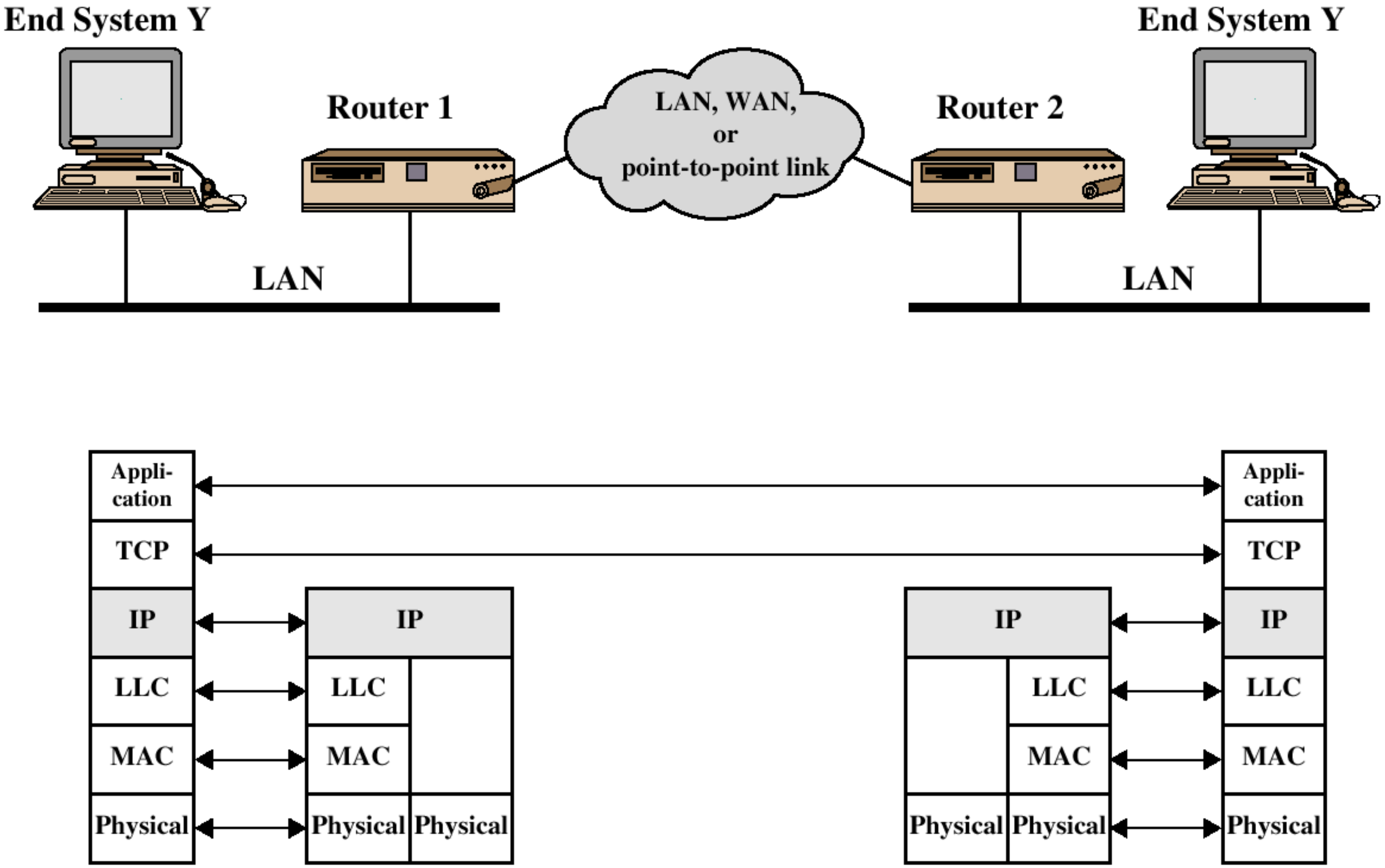
IPSec

Slides by Vitaly Shmatikov

UT Austin

TCP/IP Example

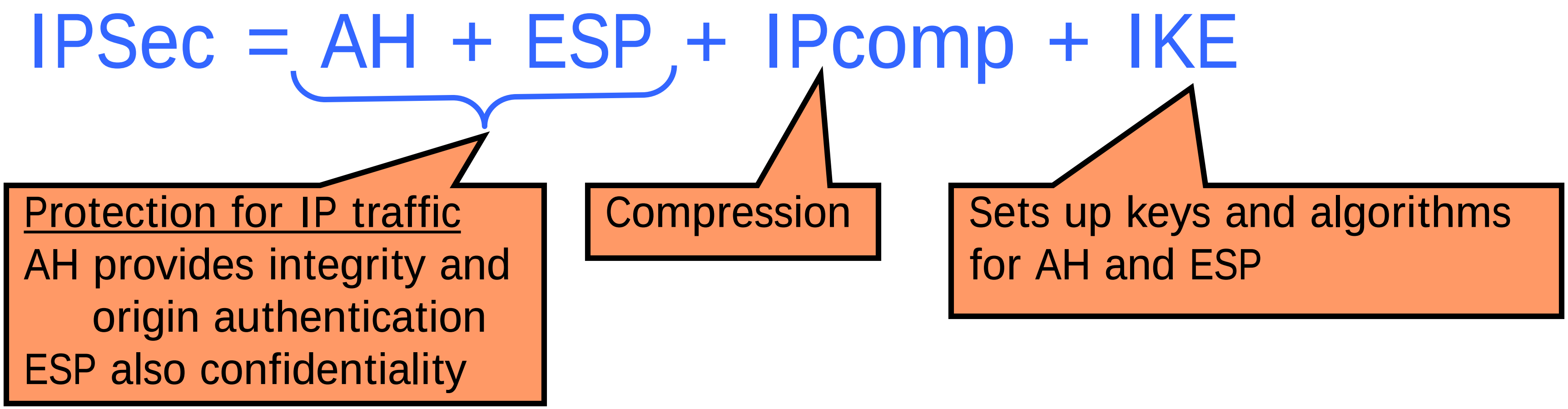


IP Security Issues

- 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

IPSec: Network Layer Security



IPSec = AH + ESP + IPcomp + IKE

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

Compression

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!

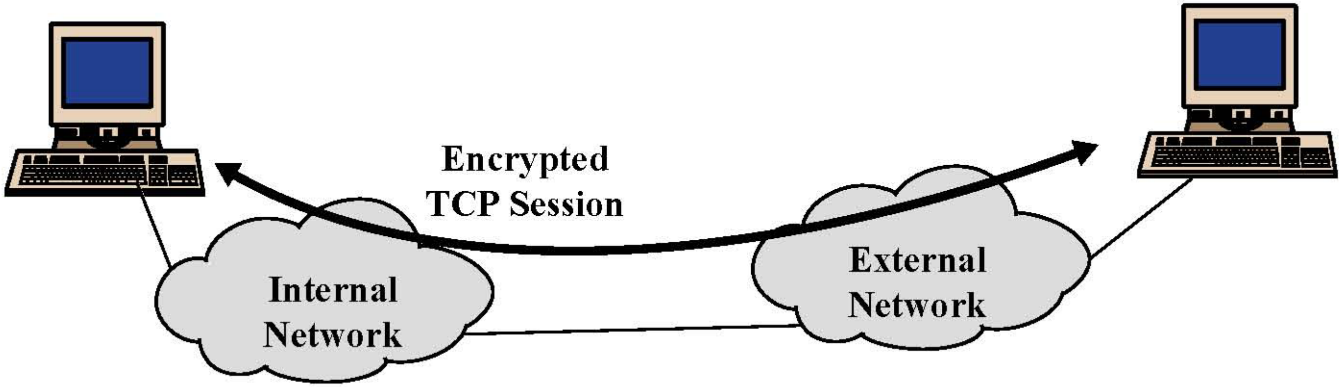
IPSec Security Services

- 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
  - Also partial protection against traffic analysis
- Authentication and encapsulation can be used separately or together
- Either provided in one of two modes
- These services are transparent to applications above transport (TCP/UDP) layer

IPSec Modes

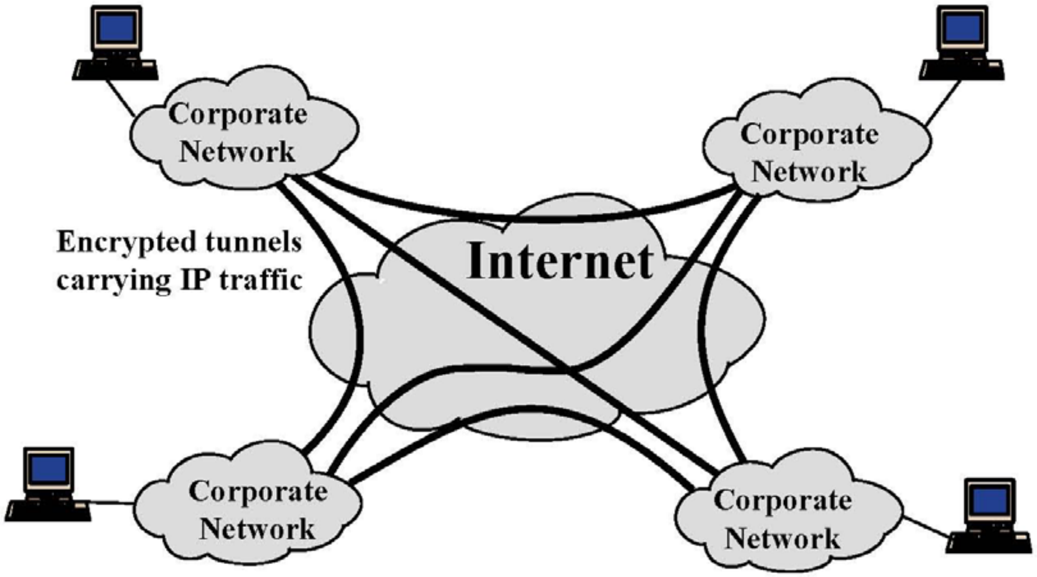
- Transport mode
  - Used to deliver services from host to host or from host to gateway
  - Usually within the same network, but can also be end-to-end across networks
- Tunnel mode
  - Used to deliver services from gateway to gateway or from host to gateway
  - Usually gateways owned by the same organization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

IPSec in Transport Mode



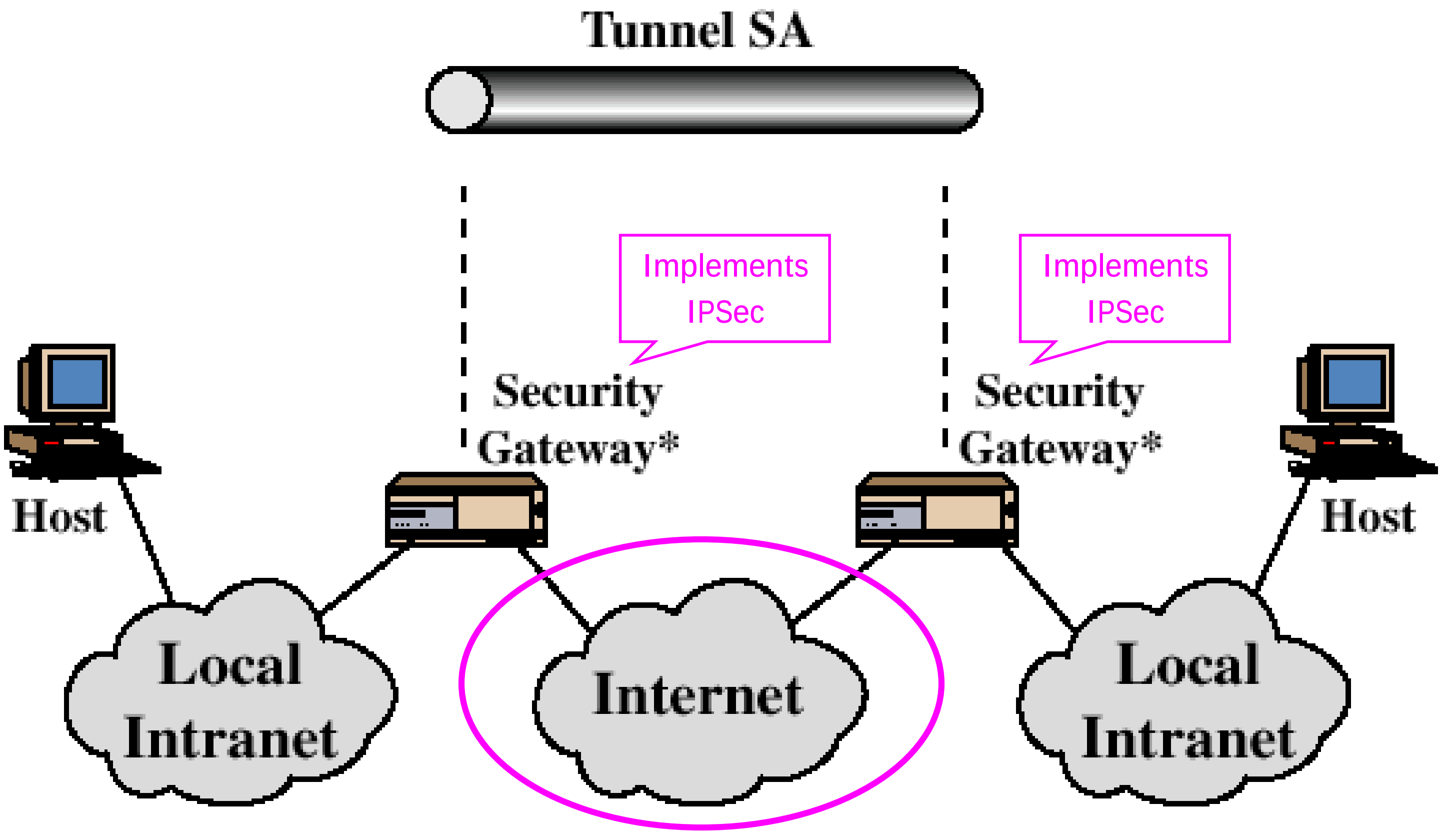
- End-to-end security between two hosts
  - Typically, client to gateway (e.g., PC to remote host)
- Requires IPSec support at each host

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

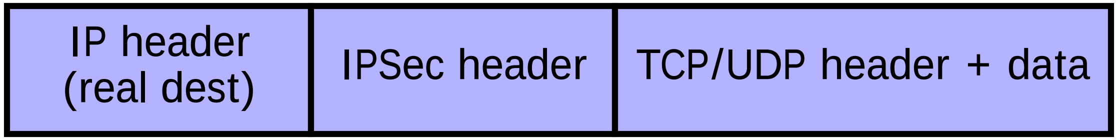
Tunnel Mode Illustration



IPSec protects communication on the insecure part of the network

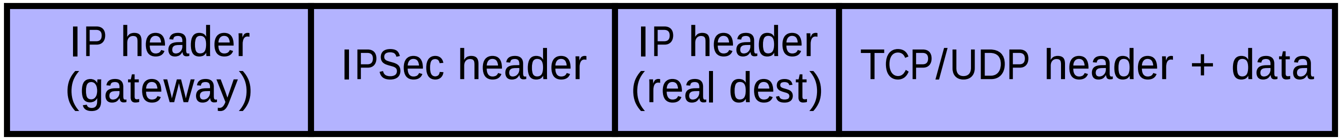
Transport Mode vs. Tunnel Mode

- Transport mode secures packet payload and leaves IP header unchanged



IP header (real dest) | IPSec header | TCP/UDP header + data

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



IP header (gateway) | IPSec header | IP header (real dest) | TCP/UDP header + data

Security Association (SA)

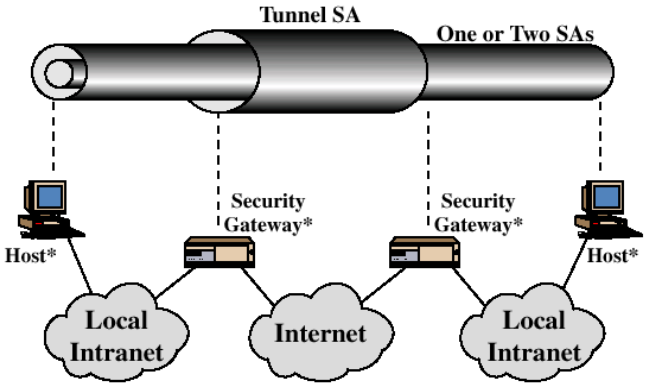
- One-way sender-recipient relationship
- SA determines how packets are processed
  - Cryptographic algorithms, keys, IVs, lifetimes, sequence numbers, mode (transport or tunnel) – read Kaufman!
- SA is uniquely identified by SPI (Security Parameters Index)...
  - Each IPSec keeps a database of SAs
  - SPI is sent with packet, tells recipient which SA to use
- ...destination IP address, and
- ...protocol identifier (AH or ESP)

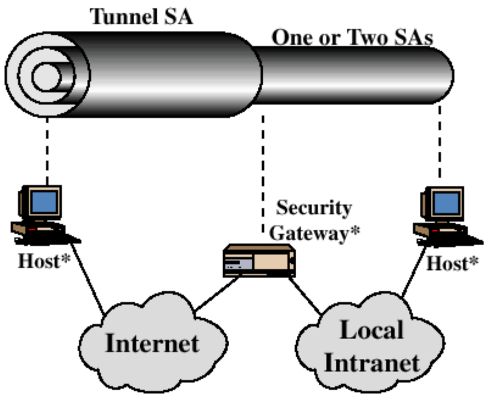
SA Components

- Each IPSec connection is viewed as one-way so two SAs required for a two-way conversation
  - Hence need for Security Parameter Index
- Security association (SA) defines
  - Protocol used (AH, ESP)
  - Mode (transport, tunnel)
  - Encryption or hashing algorithm to be used
  - Negotiated keys and key lifetimes
  - Lifetime of this SA
  - ... plus other info

Security Association Issues

- How is SA established?
  - How do parties negotiate a common set of cryptographic algorithms and keys to use?
- More than one SA can apply to a packet!
  - E.g., end-to-end authentication (AH) and additional encryption (ESP) on the public part of the network

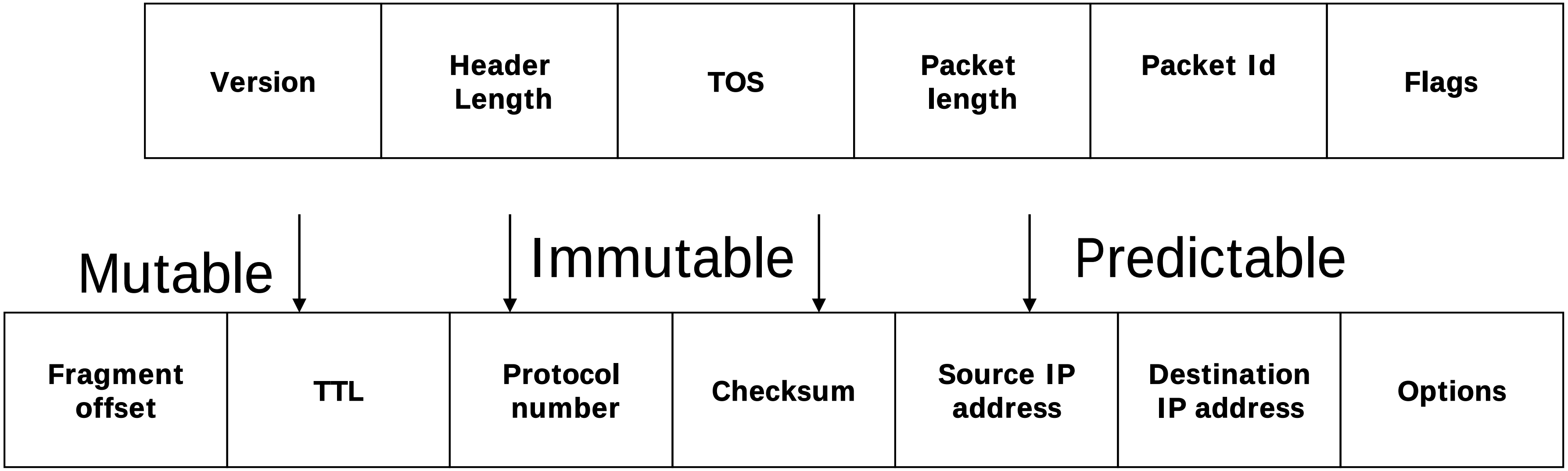




AH: Authentication Header

- Sender authentication
- Integrity for packet contents and IP header
- Sender and receiver must share a secret key
  - This key is used in HMAC computation
  - The key is set up by IKE key establishment protocol and recorded in the Security Association (SA)
    - SA also records protocol being used (AH) and mode (transport or tunnel) plus hashing algorithm used
    - MD5 or SHA-1 supported as hashing algorithms

IP Headers



Version

Header Length

TOS

Packet length

Packet Id

Flags

Mutable

Immutable

Predictable

Fragment offset

TTL

Protocol number

Checksum

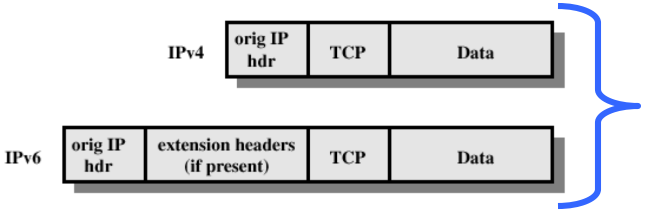
Source IP address

Destination IP address

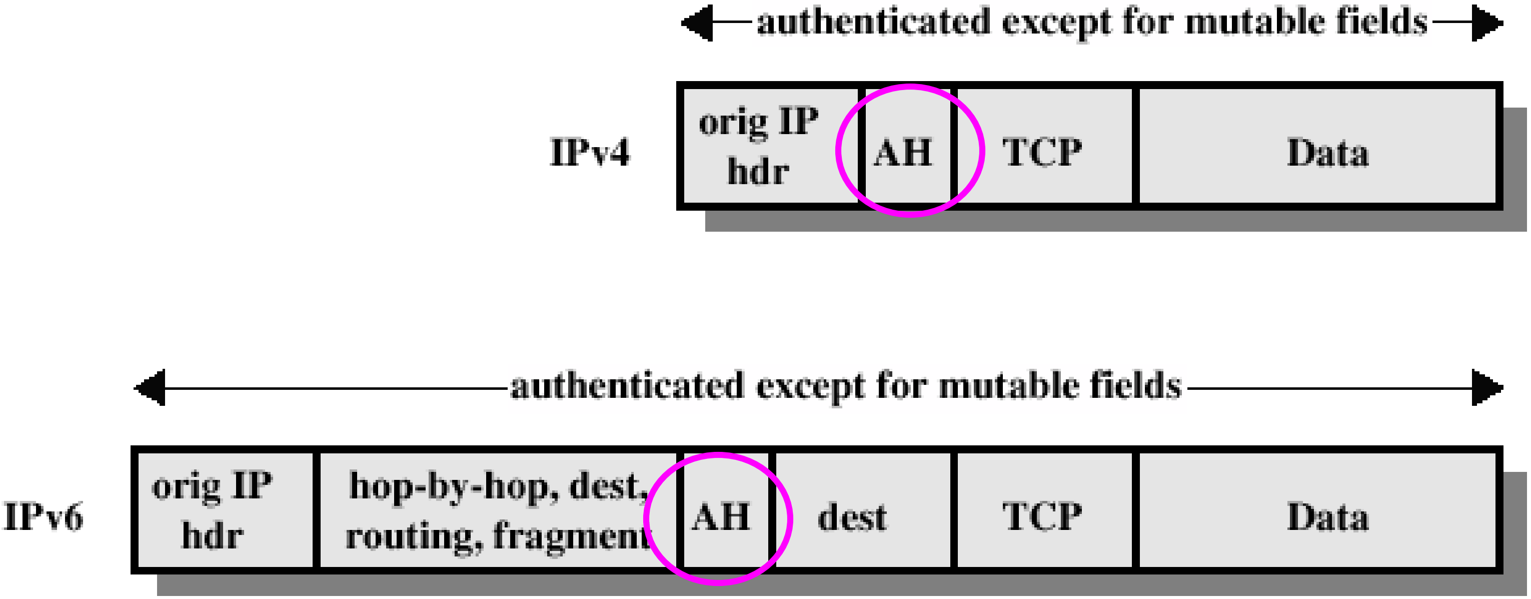
Options

AH sets mutable fields to zero and predictable fields to final value and then uses this header plus packet contents as input to HMAC

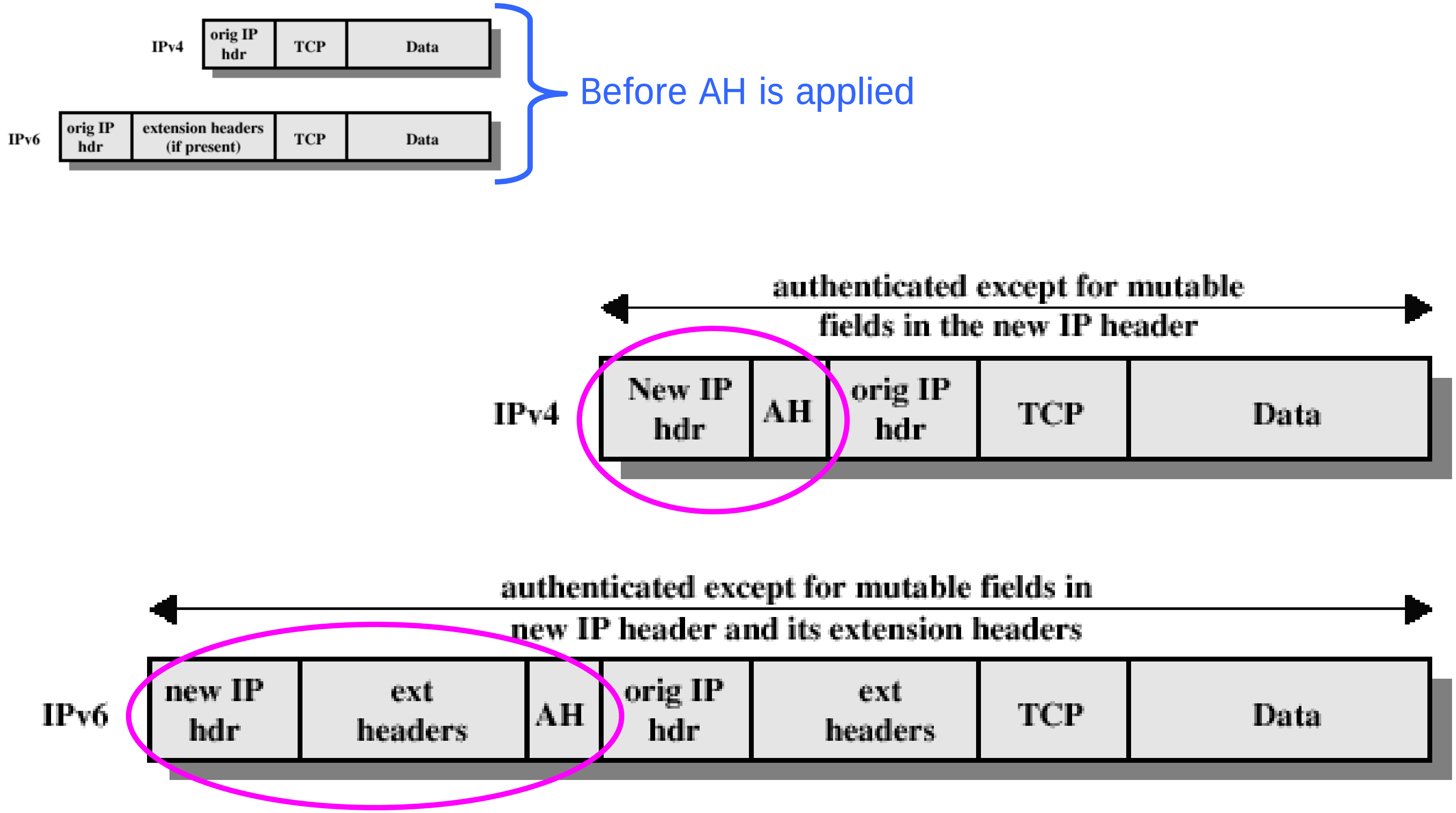
AH in Transport Mode



Before AH is applied


authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

AH in Tunnel Mode



IPv4

orig IP hdr | TCP | Data

IPv6

orig IP hdr | extension headers (if present) | TCP | Data

Before AH is applied

authenticated except for mutable fields in the new IP header

IPv4

New IP hdr | AH | orig IP hdr | TCP | Data

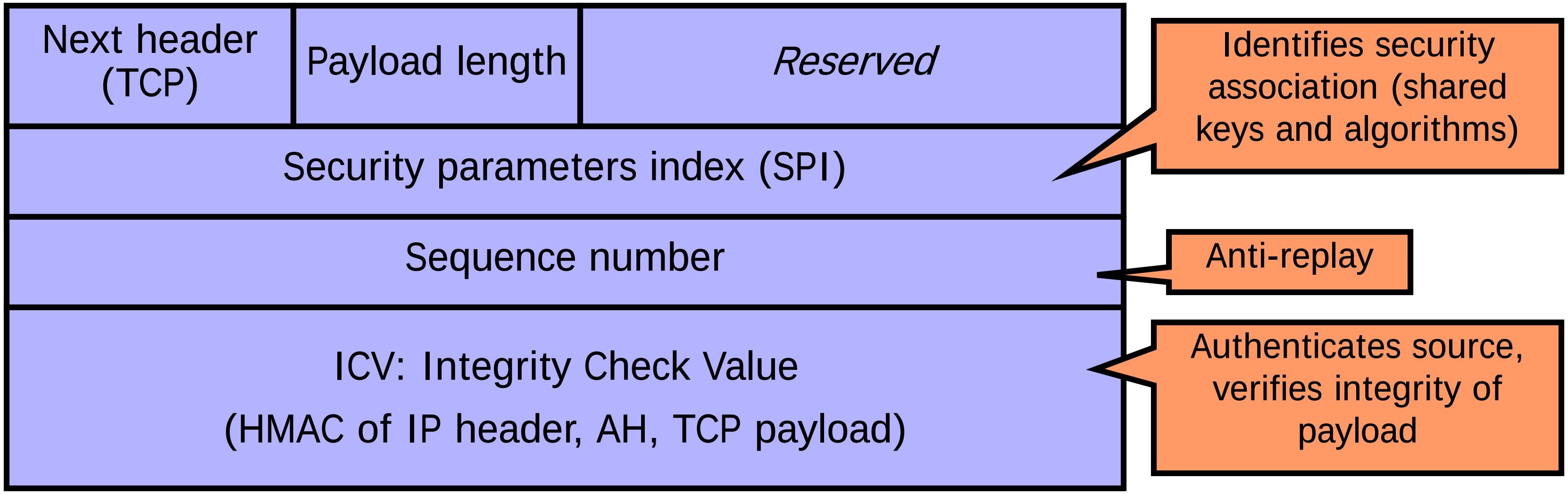
authenticated except for mutable fields in new IP header and its extension headers

IPv6

new IP hdr | ext headers | AH | orig IP hdr | ext headers | TCP | Data

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, TCP payload)

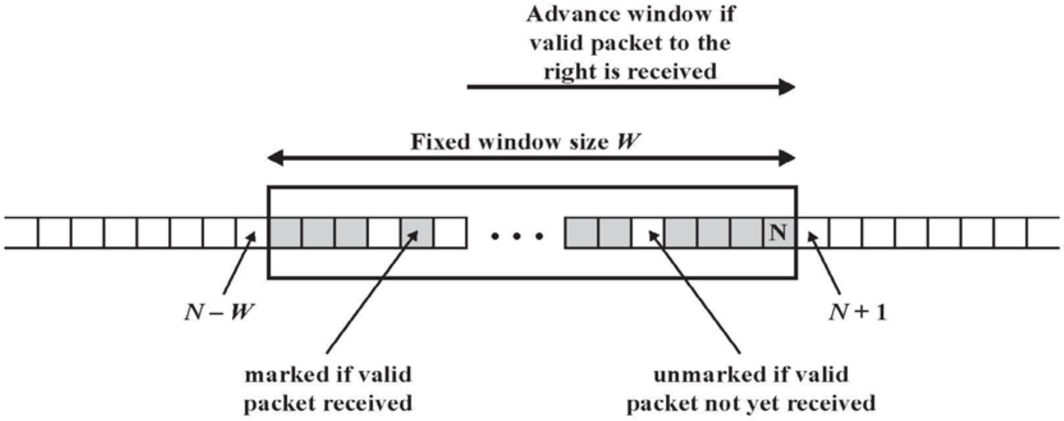
Identifies security association (shared keys and algorithms)

Anti-replay

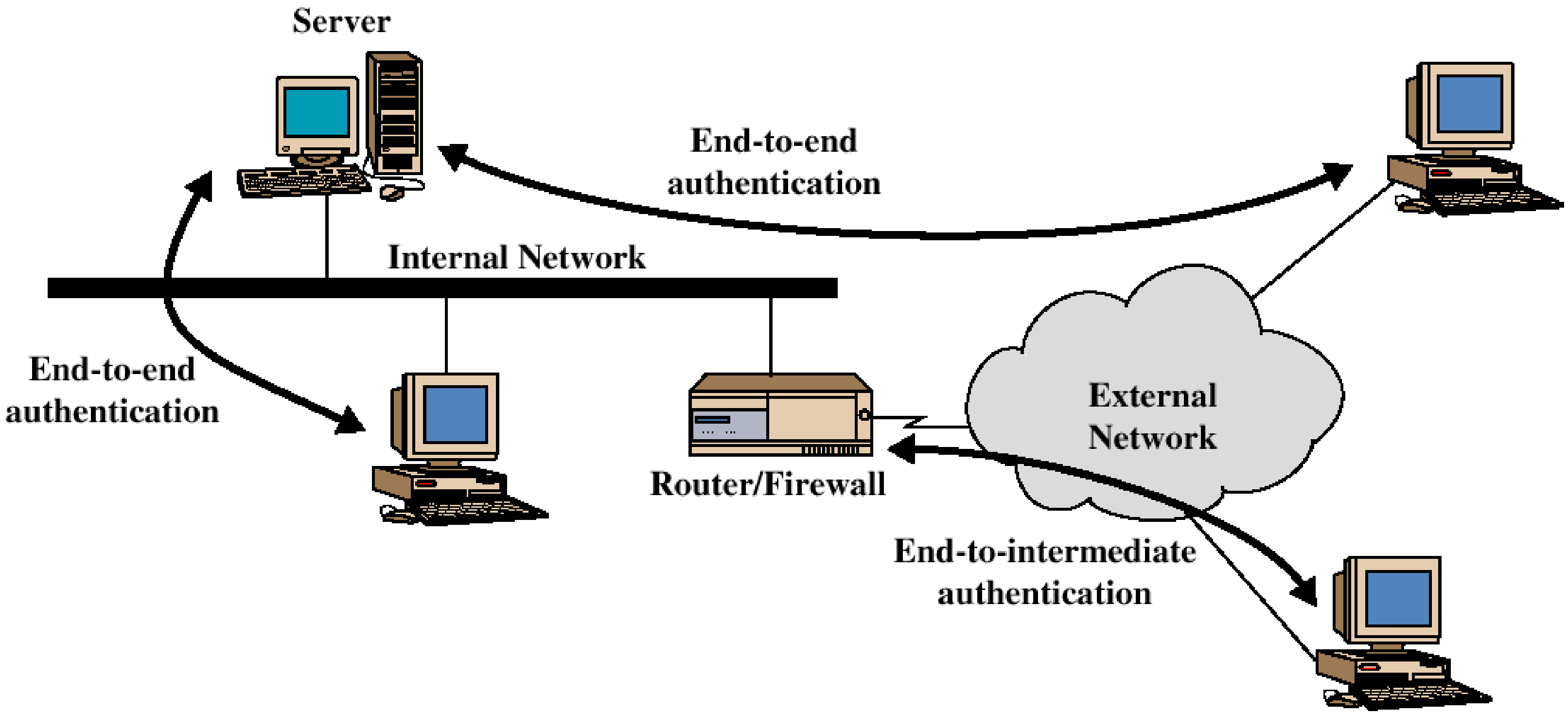
Authenticates source, verifies integrity of payload

Prevention of Replay Attacks

- When SA is established, sender initializes 32-bit counter to 0, increments by 1 for each packet
  - If wraps around 2^{32}-1, new SA must be established
- Recipient maintains a sliding 64-bit window
  - If a packet with high sequence number is received, do not advance window until packet is authenticated


Advance window if valid packet to the right is received
Fixed window size W
N
• • •
$N-W$
$N+1$
marked if valid packet received
unmarked if valid packet not yet received

Forms of AH-Based Authentication

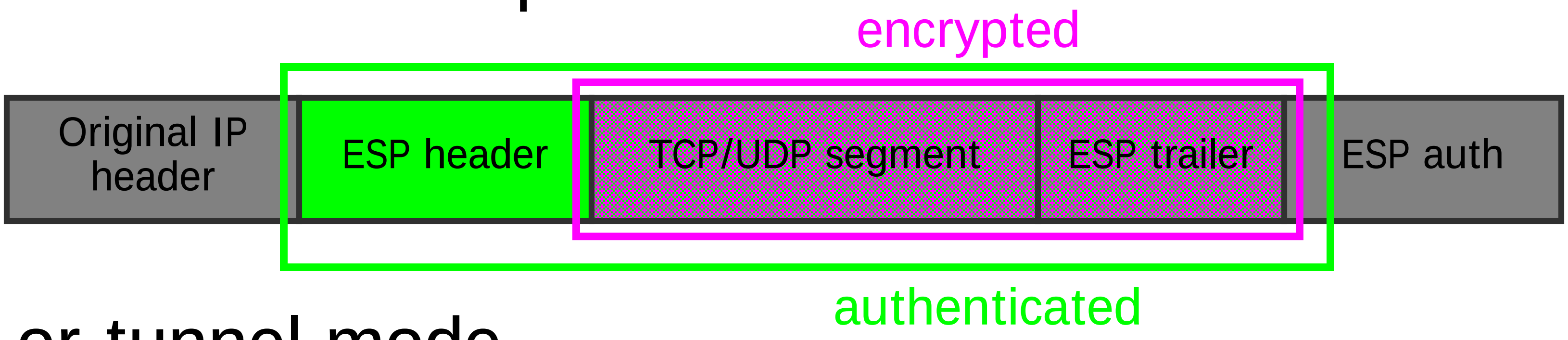

Server
End-to-end authentication
Internal Network
End-to-end authentication
Router/Firewall
External Network
End-to-intermediate authentication

ESP: Encapsulating Security Payload

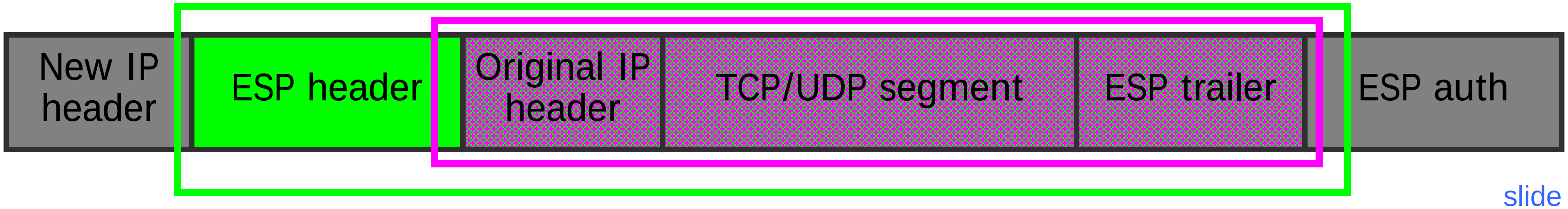
- Adds new header and trailer fields to packet
- Transport mode
  - Confidentiality of packet between two hosts
  - Complete hole through firewalls
  - Used sparingly
- Tunnel mode
  - Confidentiality of packet between two gateways or a host and a gateway
  - Implements VPN tunnels

ESP Security Guarantees

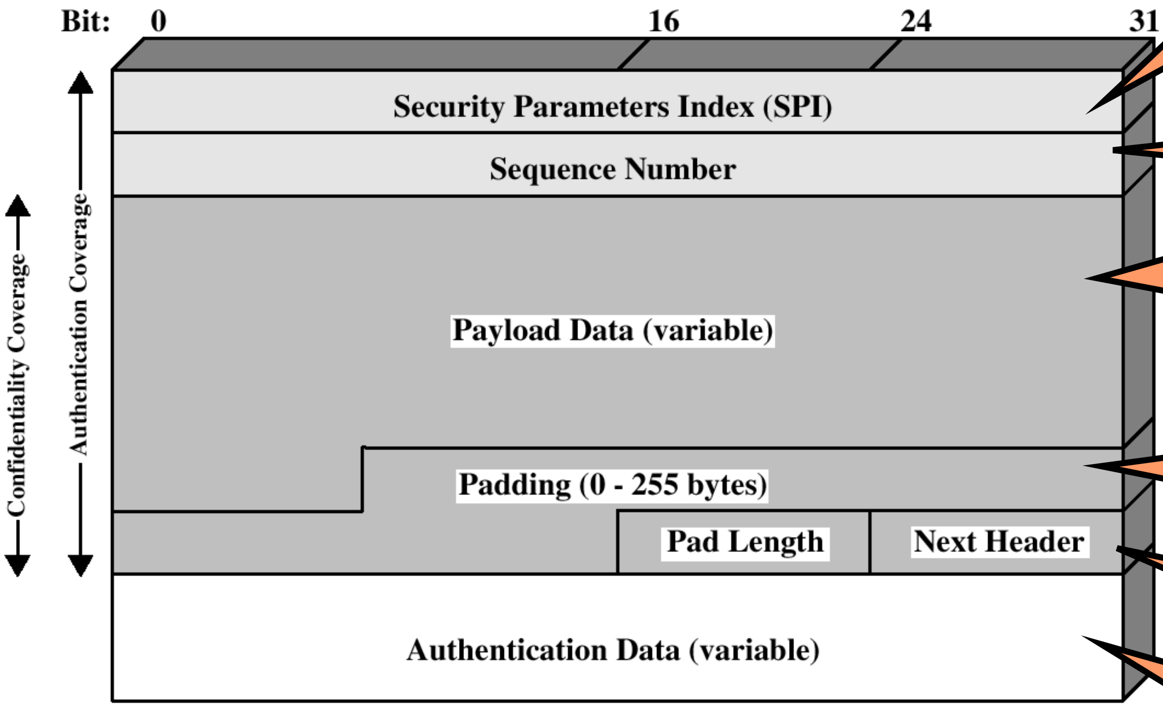
- Confidentiality and integrity for packet payload
  - Symmetric cipher negotiated as part of security assoc
- Optionally provides authentication (similar to AH)
- Can work in transport...



- ...or tunnel mode



ESP Packet



Identifies security association (shared keys and algorithms)

Anti-replay

TCP segment (transport mode) or entire IP packet (tunnel mode)

Pad to block size for cipher, also hide actual payload length

Type of payload

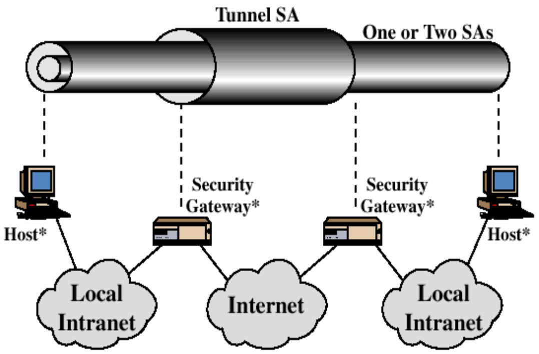
HMAC-based Integrity Check Value (similar to AH)

Virtual Private Networks (VPN)

- 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 VPN tunnel
  - Secure communication between parts of the same organization over public untrusted Internet

ESP Together With AH

- AH and ESP are often combined
- End-to-end AH in transport mode
  - Authenticate packet sources
- Gateway-to-gateway ESP in tunnel mode
  - Hide packet contents and addresses on the insecure part of the network
- Significant cryptographic overhead
  - Even with AH


Tunnel SA
One or Two SAs
Security Gateway*
Security Gateway*
Host*
Host*
Local Intranet
Internet
Local Intranet