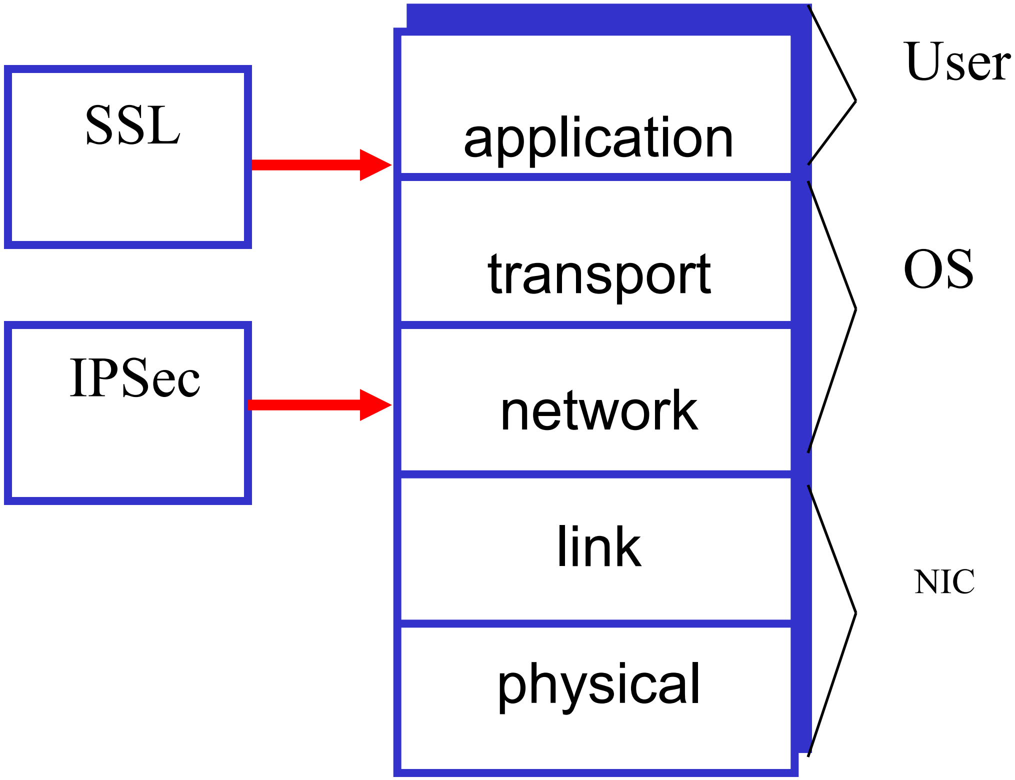
IPSec Part I: AH and ESP

- Readings
  - Sections 16.0, 16.1, 16.2, 16.5, 16.12
  - Chapter 17

Internet Security Protocols

- IPSec and SSL
- IPSec lives at the network layer
- SSL lives between application and transport layers



SSL vs. IPSec

- SSL/TLS
  - Lives at socket layer (part of user space)
  - Has encryption, integrity, authentication, etc.
  - Has a simpler specification
- IPSec
  - Lives at the network layer (part of the OS)
  - Has encryption, integrity, authentication, etc.
  - Is overly complex (including serious flaws)

SSL vs. IPSec

- IPSec implementation
  - Requires changes to OS, but no changes to applications
- SSL implementation
  - Requires changes to applications, but no changes to OS
- SSL built into Web application early on (Netscape)
- IPSec used in VPN applications (secure tunnel)
- Reluctance to retrofit applications for SSL
- Reluctance to use IPSec due to complexity and interoperability issues
- Result? **Internet less secure than it should be!**

IPSec and Complexity

- IPSec is a complex protocol
- Over-engineered
  - Lots of generally useless extra features
- Flawed
  - Some serious security flaws
- Interoperability is serious challenge
  - Defeats the purpose of having a standard!
- Complex

What is IPSec?

- Protocols and mechanisms to
  - support security at the network layer (IP layer)
- Implemented on end hosts and gateways
- Security Policies and SPD (security policy database)
  - Rules to decide if an IP packet (datagram) needs to be processed and how
- Security Association (SA) & SAD (SA database)
  - Information about the unique security connection
  - Separate associations in each direction (outbound, inbound)
  - SA is uniquely defined by:
    - SPI (security parameters index)
    - Destination IP address
    - IPSec Protocol (ESP or AH)

Components of IPSec

- Two parts to IPSec
- **IKE:** Internet Key Exchange
  - Mutual authentication
  - Establish shared symmetric key
  - Two "phases"
- **ESP/AH**
  - After SA (symmetric key) has been established
  - ESP: Encapsulating Security Payload — for encryption and/or integrity of IP packets
  - AH: Authentication Header — integrity only

Services Provided by IPSec

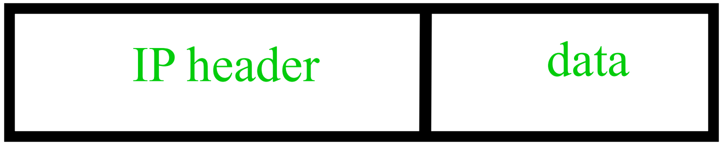
- Data content confidentiality
- Connectionless integrity
- Data origin authentication
- Replay protection
- Privacy
- Traffic flow masking

IPSec Architecture

- Security Policies
  - define treatment of traffic
- Security Associations between nodes components
- Security Protocols
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Key Management
  - Internet Key Exchange (IKE)
- Algorithms for authentication and encryption

IP Review

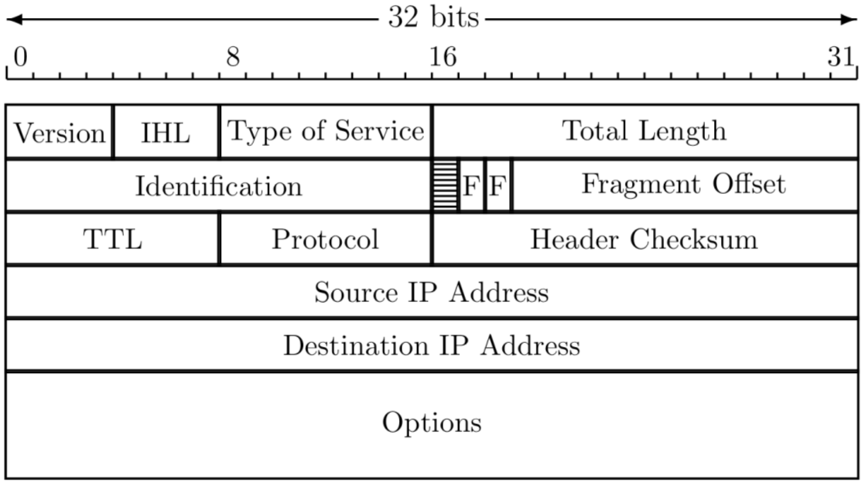
- IP datagram is of form



IP header

data

- Where IP header is



32 bits

0 8 16 31

Version | IHL | Type of Service | Total Length

Identification | F | F | Fragment Offset

TTL | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options

Fields of the IP Packet

- *Version*: the version number of the protocol. Version = 4 for IPv4.
- *Header length*: the length of the header in 4 byte words. Header length = 5 if options are not used.
- *Service type*: 3 bits of precedence (rarely used) 4 bits DTRM representing delay, throughput, reliability, and monetary cost. Field generally ignored. Last bit is 0.
- *Total length*: length in bytes of the header plus data. Maximum size is 65,535 bytes.
- *Identification, flags, fragment offset*: used for fragmentation and reassembly (offset in 8 byte chunks)
- *Time to live (TTL)*: Originally seconds, now usually hop count. Source sets it (often 30 used). Each router must decrement by at least 1. When 0 packet discarded.

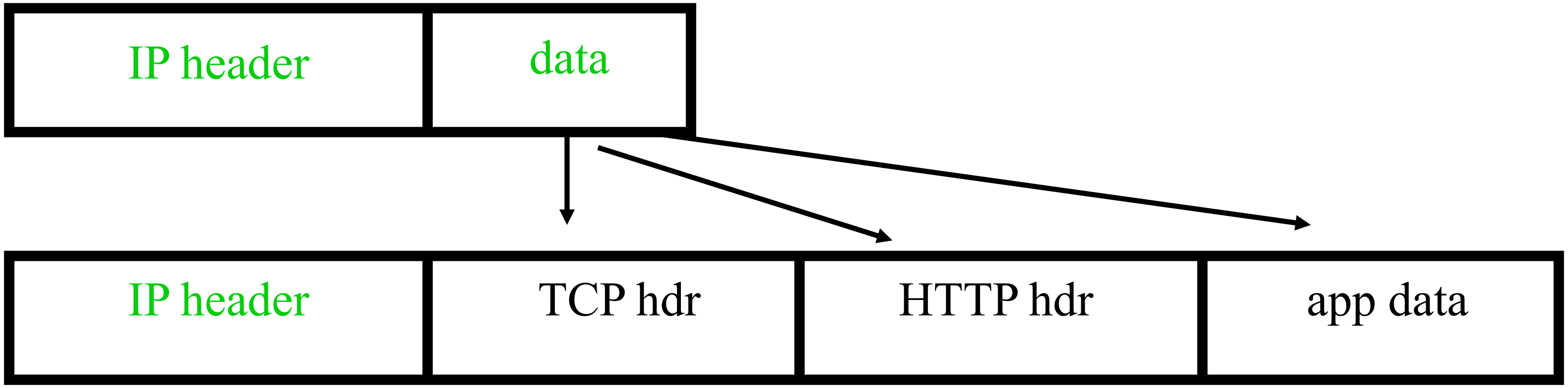
Protocol Field Values

- Protocol = 1, ICMP, Internet Control Message Protocol
- Protocol = 6, TCP
- Protocol = 17, UDP
- Protocol = 4, IP in IP encapsulation
- Protocol = 8, EGP, Exterior Gateway Protocol
- Protocol = 9, IGRP, Interior Gateway Routing Protocol
- Protocol =89, OSPF, Open Shortest Path First Routing P.
- Protocol = 50, ESP, Encapsulating Security Payload
- Protocol = 51, AH, Authentication Header

- Check file /etc/protocols for more protocols

IP and TCP

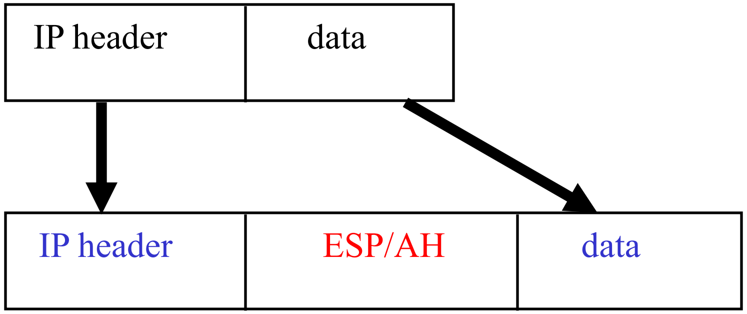
- Consider HTTP traffic (over TCP)
- IP encapsulates TCP
- TCP encapsulates HTTP



- IP data includes TCP header, etc.

IPSec Transport Mode

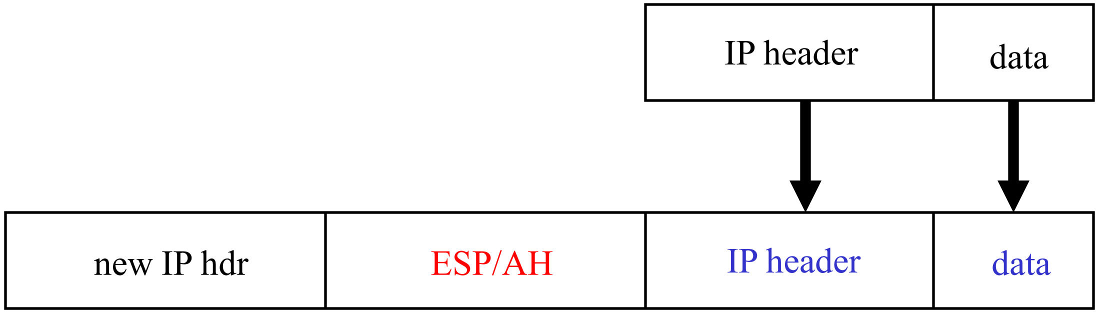
- IPSec **Transport Mode**



- Transport mode designed for host-to-host
- Transport mode is efficient
  - Adds minimal amount of extra header
- The original header remains
  - Passive attackers can see who is talking

IPSec Tunnel Mode

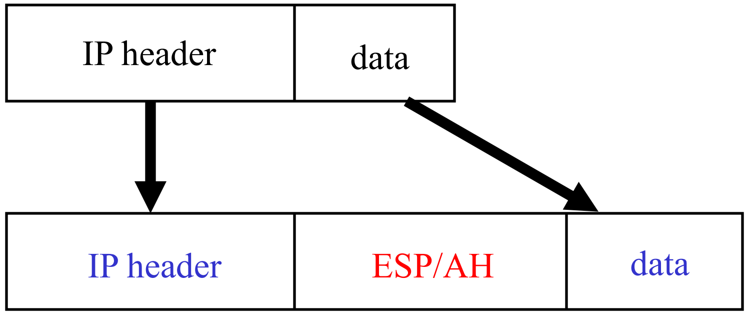
- IPSec Tunnel Mode



- Tunnel mode for firewall to firewall traffic
- Original IP packet encapsulated in IPSec
- Original IP header not visible to attacker (if ESP is used)
  - New header from firewall to firewall
  - Attacker does not know which hosts are talking

Comparison of IPSec Modes

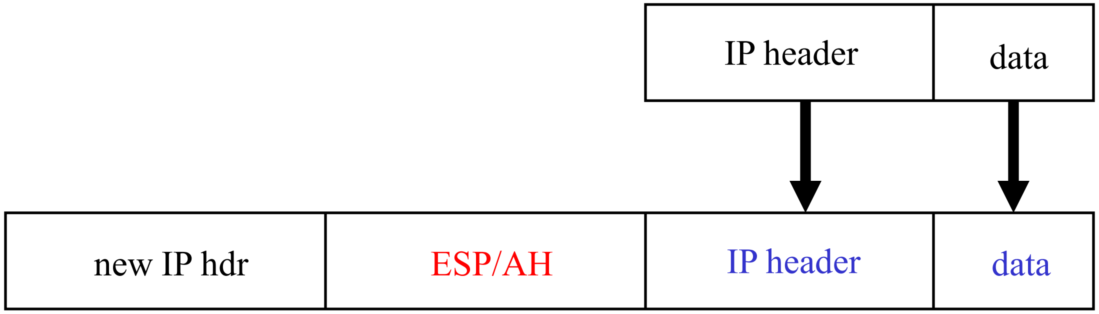
- Transport Mode



IP header
data

IP header
ESP/AH
data

- Tunnel Mode



IP header
data

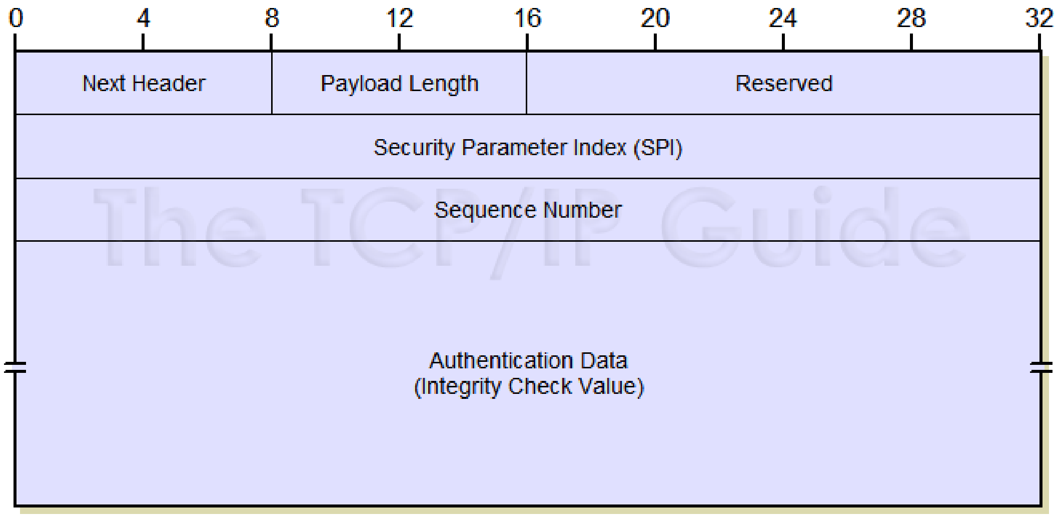
new IP hdr
ESP/AH
IP header
data

- Transport Mode
  - Host-to-host
- Tunnel Mode
  - Firewall-to-firewall
- Transport mode not necessary
- Transport mode is more efficient

Authentication Header (AH)

- RFC 4302 (IP Authentication Header)
- The IP AH is used to provide
  - Connectionless integrity
  - Data origin authentication
  - Protection against replays.
- AH provides authentication for as much of the IP header as possible, but cannot all be protected by AH.
- Data privacy is not provided by AH (all data is in the clear)

IPSec AH Header



Next Header | Payload Length | Reserved

Security Parameter Index (SPI)

Sequence Number

Authentication Data
(Integrity Check Value)

Next Header: protocol type of following payload

Payload Length: length (in 32 bit words) of the AH Header minus 2 (note that it is actually the AH header length, instead of payload length)

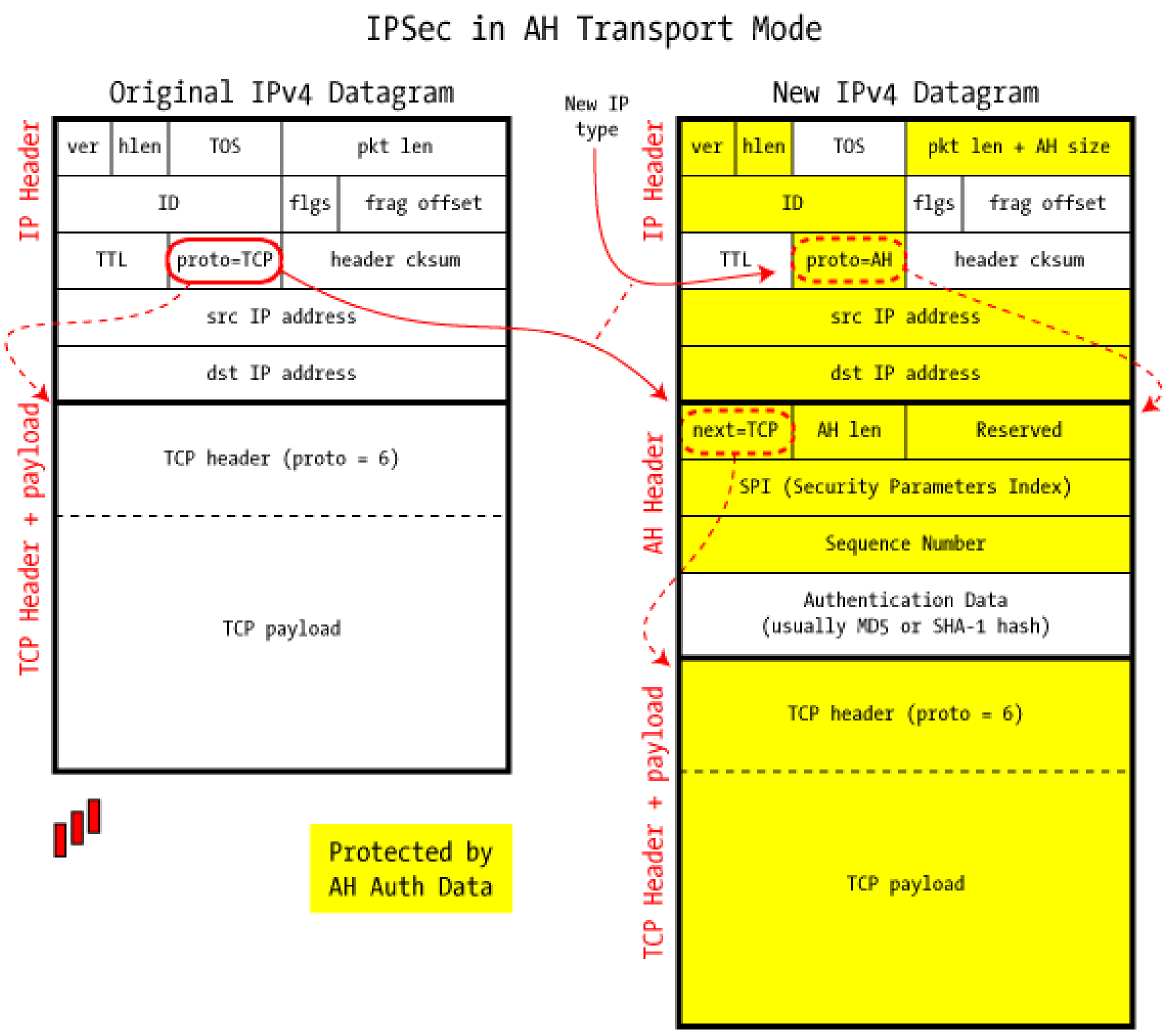
Sequence Number: monotonically increasing number

Authentication Data: Integrity check value (ICV) over most of the packet

IPSec in AH Transport Mode

- AH covers all immutable fields of IP & AH headers and payload by computing a MAC.
- Does not cover
  - IP Header: TOS, flags, frag offset, TTL, header checksum, (Note: covers pkt len modified value)
  - AH Header: Authentication Data
- Modification of the IP Header
  - protocol field changed to AH = 51
    - current value of protocol field inserted into IPSec Header
  - Packet length field changed

AH in Transport Mode



IPSec in AH Transport Mode

Original IPv4 Datagram

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=TCP | header cksum

src IP address

dst IP address

TCP header (proto = 6)

TCP payload

New IPv4 Datagram

ver | hlen | TOS | pkt len + AH size

ID | flgs | frag offset

TTL | proto=AH | header cksum

src IP address

dst IP address

next=TCP | AH len | Reserved

SPI (Security Parameters Index)

Sequence Number

Authentication Data
(usually MD5 or SHA-1 hash)

TCP header (proto = 6)

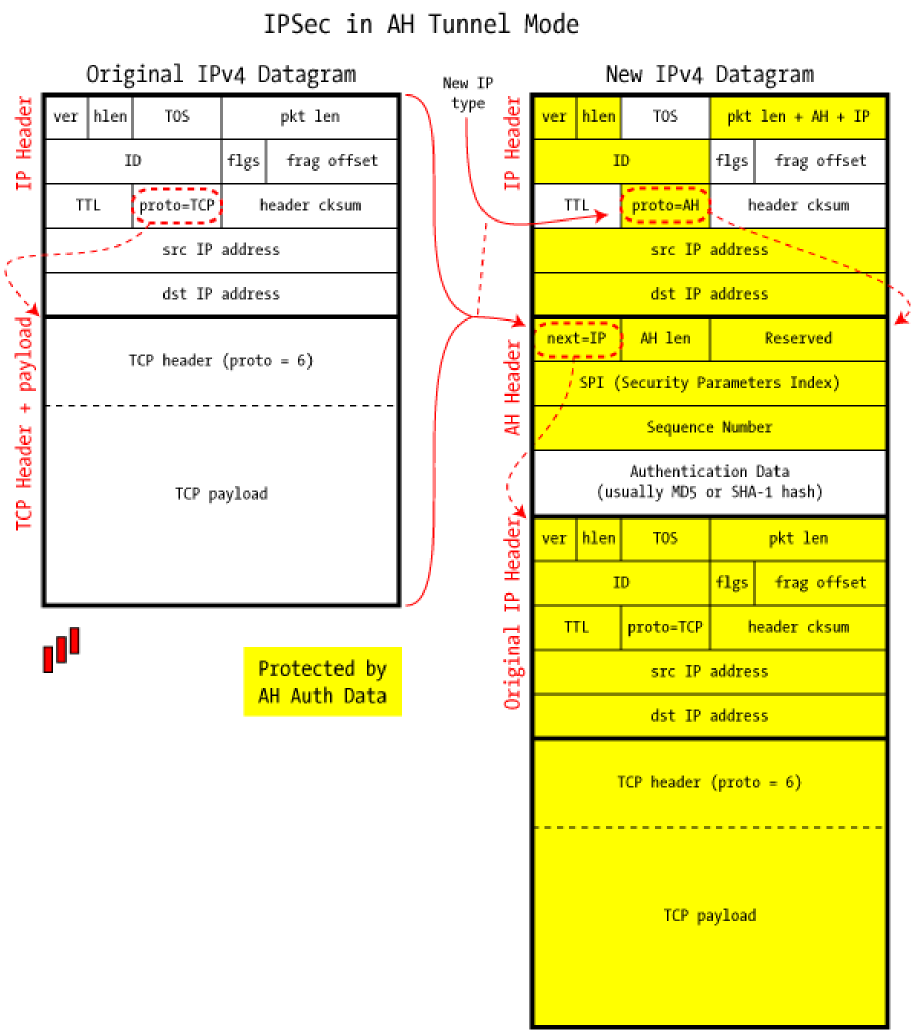
TCP payload

Protected by
AH Auth Data

IPSec in AH Tunnel Mode

- AH covers all immutable fields of the headers and payload
- Does not cover
  - IP Header: TOS, flags, frag offset, TTL, header checksum
  - AH Header: Authentication Data
- New IP Header is created with appropriate source and destination IP addresses
  - protocol field set to AH = 51
- IPSec Header
  - next field is set to IP = 4

IPSec in AH Tunnel Mode



Notes on AH

- HMAC incorporates a secret key
- Exact authentication function and keys negotiated by end points
- Tunnel Mode vs. Transport Mode identified by the next header type in the IPSec Header (also true of ESP)
  - if 4 then must be Tunnel mode
  - else Transport mode
- AH is incompatible with NAT / PAT devices
  - Network Address Translation
  - Port address translation
  - change of (private) source address, for example, at a NAT box does not allow re-computation of the HMAC by the destination

Encapsulating Security Payload (ESP)

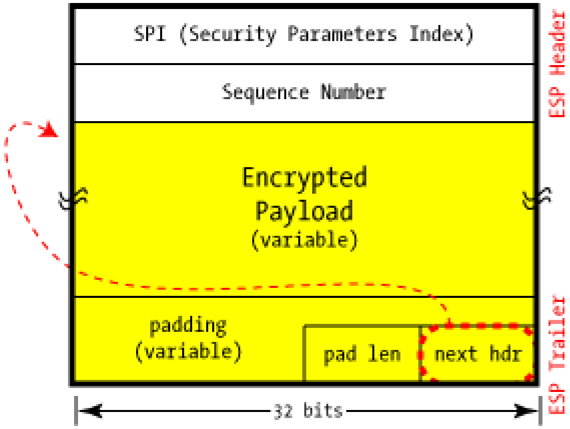
- RFC 4303 (IP Encapsulating Security Payload)
- ESP allows for encryption, as well as authentication.
  - Both are optional, defined by the SPI and policies.
    - A null encryption algorithm was proposed
  - Thus AH in a sense is not needed
  - Protocol type in IP header is set to 50
- ESP does not protect the IP header, only the payload
  - in tunnel mode original packet is encrypted
  - In transport mode original packet data is encrypted
  - This includes higher level protocols and ports. (NATs and firewalls may need this information).
- ESP header is actually a header plus a trailer as it "surrounds" the packet data
- Can actually combine AH and ESP but rarely done

ESP (Cont’d)

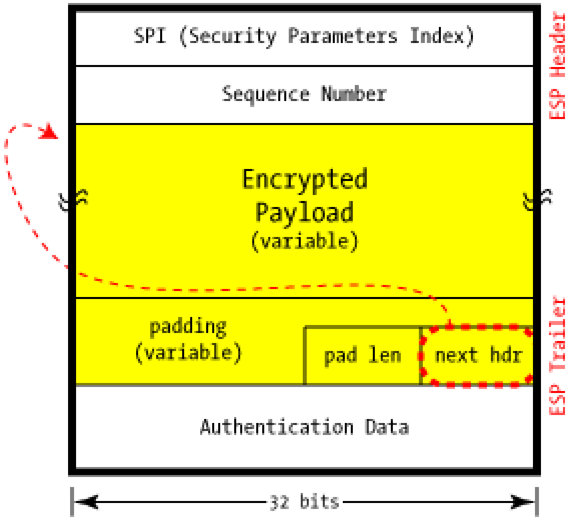
- Services provided include:
  - Confidentiality
  - Data origin authentication
  - Connectionless integrity
  - Anti-replay service
  - Limited traffic flow confidentiality
- Security services can be provided between
  - A pair of communicating hosts
  - A pair of security gateways
  - A security gateway and a host

ESP Header

ESP w/o Authentication



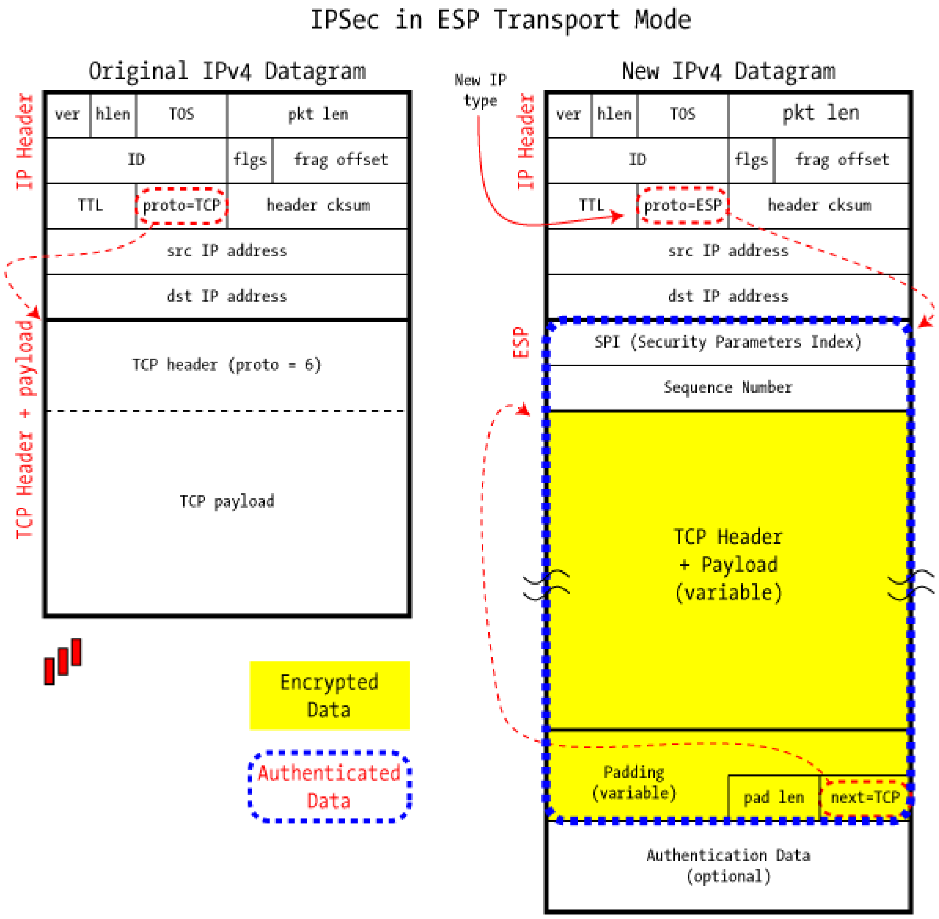
ESP with Authentication



Notes on ESP

- The “header” fields
  - SPI
  - Sequence Number
- The “data” part
  - Optionally may have an IV added (in clear if necessary)
  - Has variable length padding
    - Sometimes needed for encryption
    - Sometimes masks encryption
    - Sometimes used to mask traffic flow
- The “trailer” part
  - Padding length
  - Next header
    - In tunnel mode would be set to 4
    - In transport mode would be set to original packet data
- ESP can also have NAT/PAT problems
  - If transport layer information is used.

IPSec in ESP Transport Mode



IPSec in ESP Transport Mode

Original IPv4 Datagram

IP Header

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=TCP | header cksum

src IP address

dst IP address

TCP Header + payload

TCP header (proto = 6)

TCP payload

Encrypted Data

Authenticated Data

New IPv4 Datagram

New IP type

IP Header

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=ESP | header cksum

src IP address

dst IP address

ESP

SPI (Security Parameters Index)

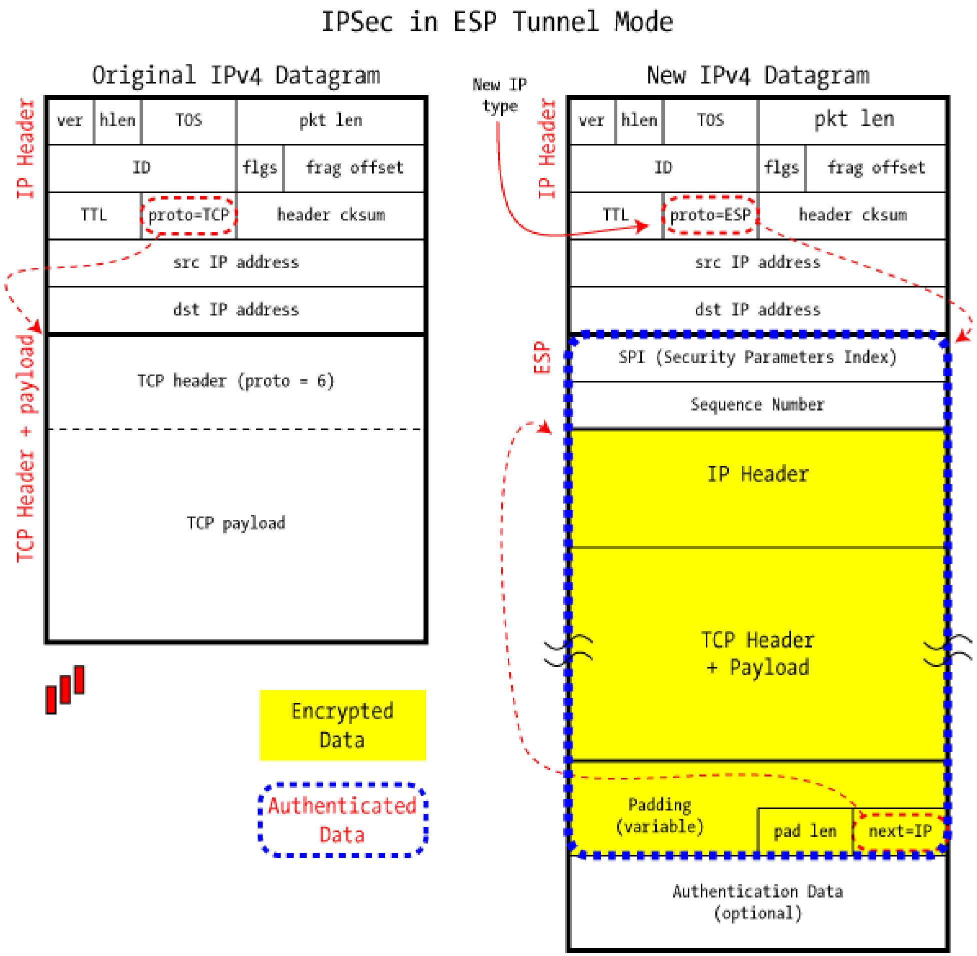
Sequence Number

TCP Header + Payload (variable)

Padding (variable) | pad len | next=TCP

Authentication Data (optional)

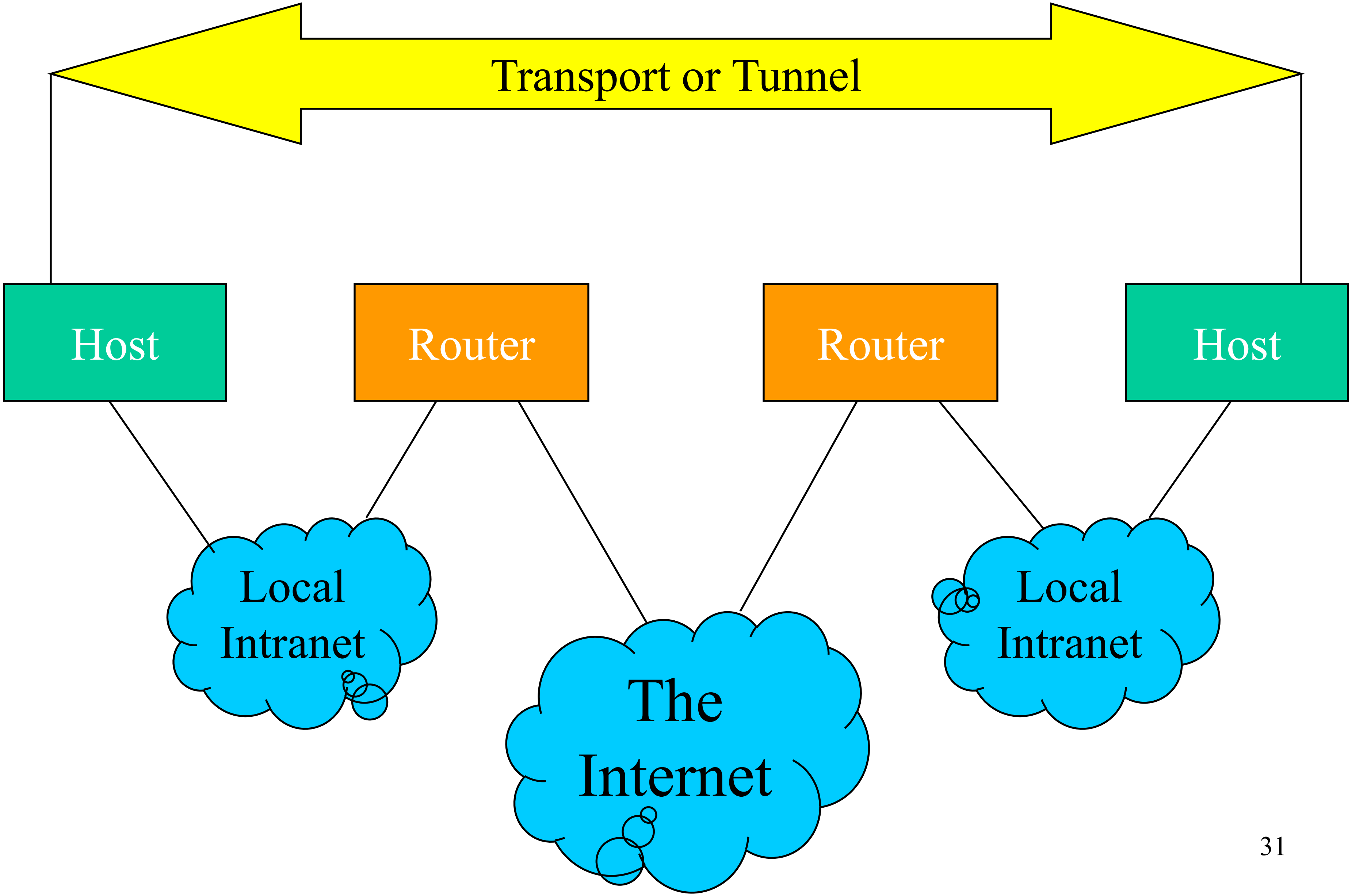
IPSec in ESP Tunnel Mode



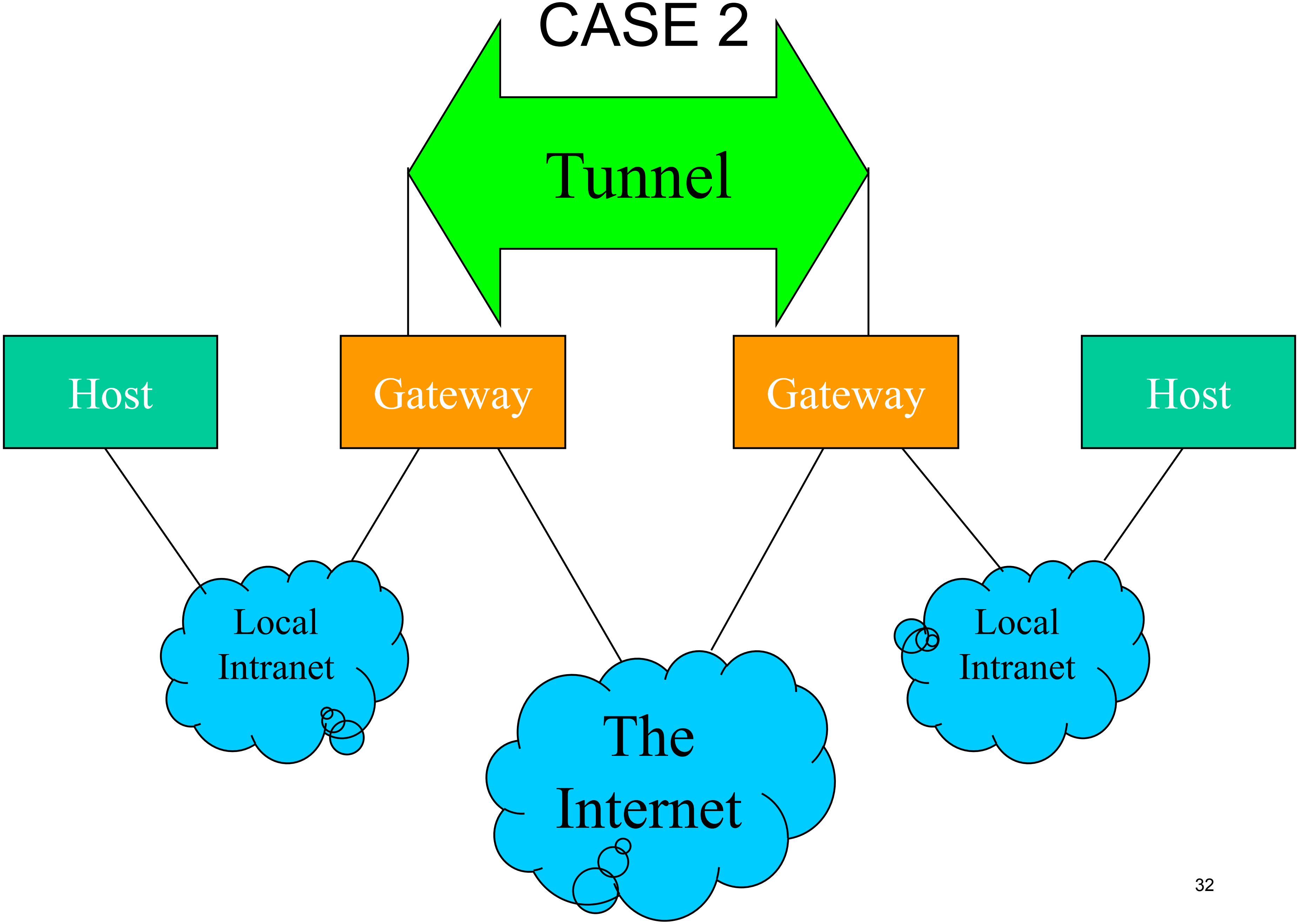
Some Example Configurations Using IPSec

- Case 1: Host to host secured service
  - End to end (transport or tunnel)
- Case 2: Gateway to Gateway secured service
  - such as VPN (virtual private network)
- Case 3. Host to gateway secured tunnel and separate secured host to host such as dialing in to a gateway

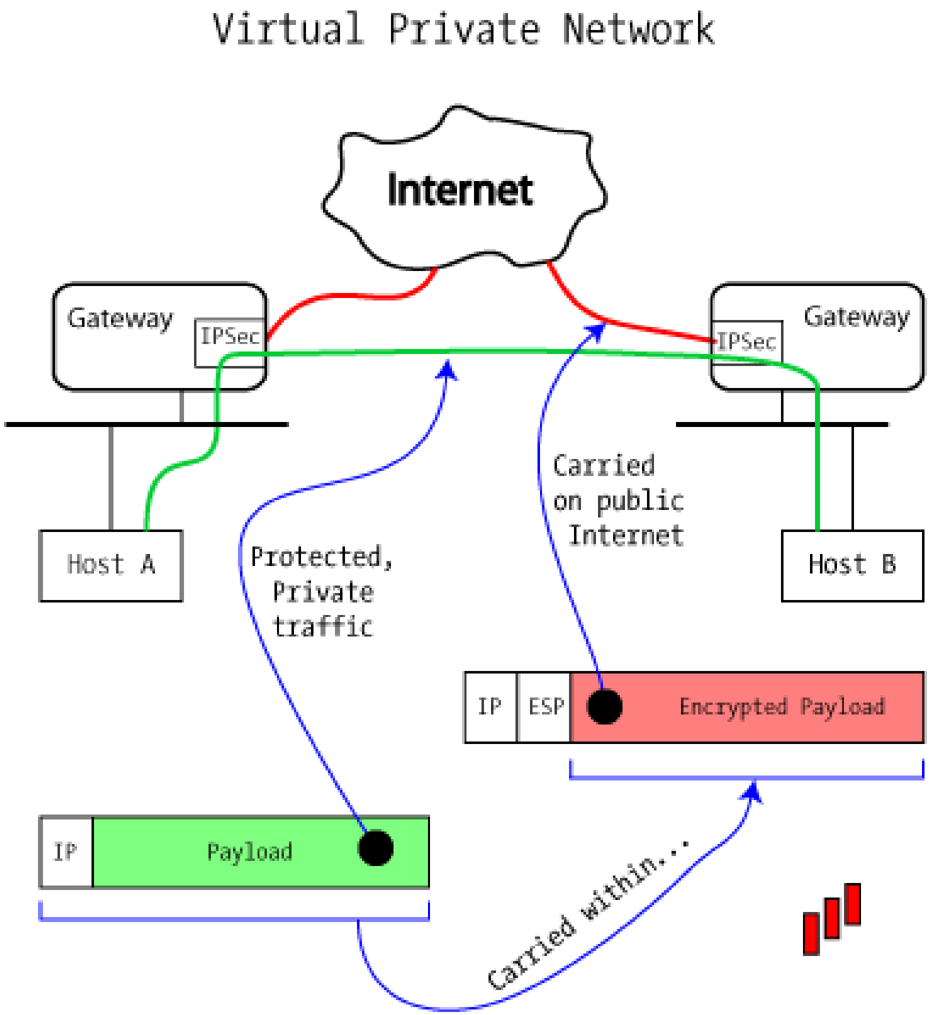
CASE 1


Transport or Tunnel
Host
Router
Router
Host
Local Intranet
The Internet
Local Intranet

CASE 2

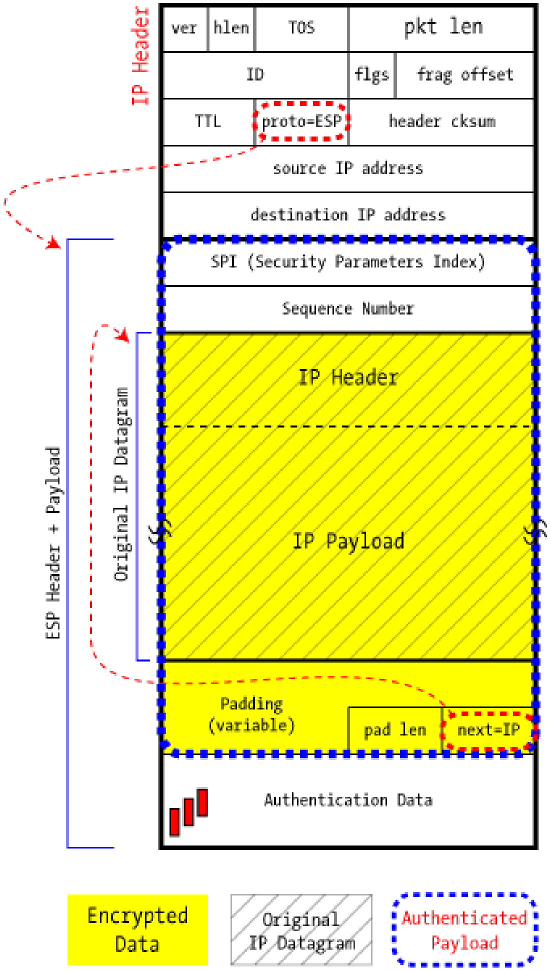

Tunnel
Host
Gateway
Gateway
Host
Local Intranet
The Internet
Local Intranet

Traditional VPN



Traditional VPN

ESP+Auth+Tunnel Mode
- Traditional VPN



IP Header

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=ESP | header cksum

source IP address

destination IP address

ESP Header + Payload

SPI (Security Parameters Index)

Sequence Number

Original IP Datagram

IP Header

IP Payload

Padding (variable) | pad len | next=IP

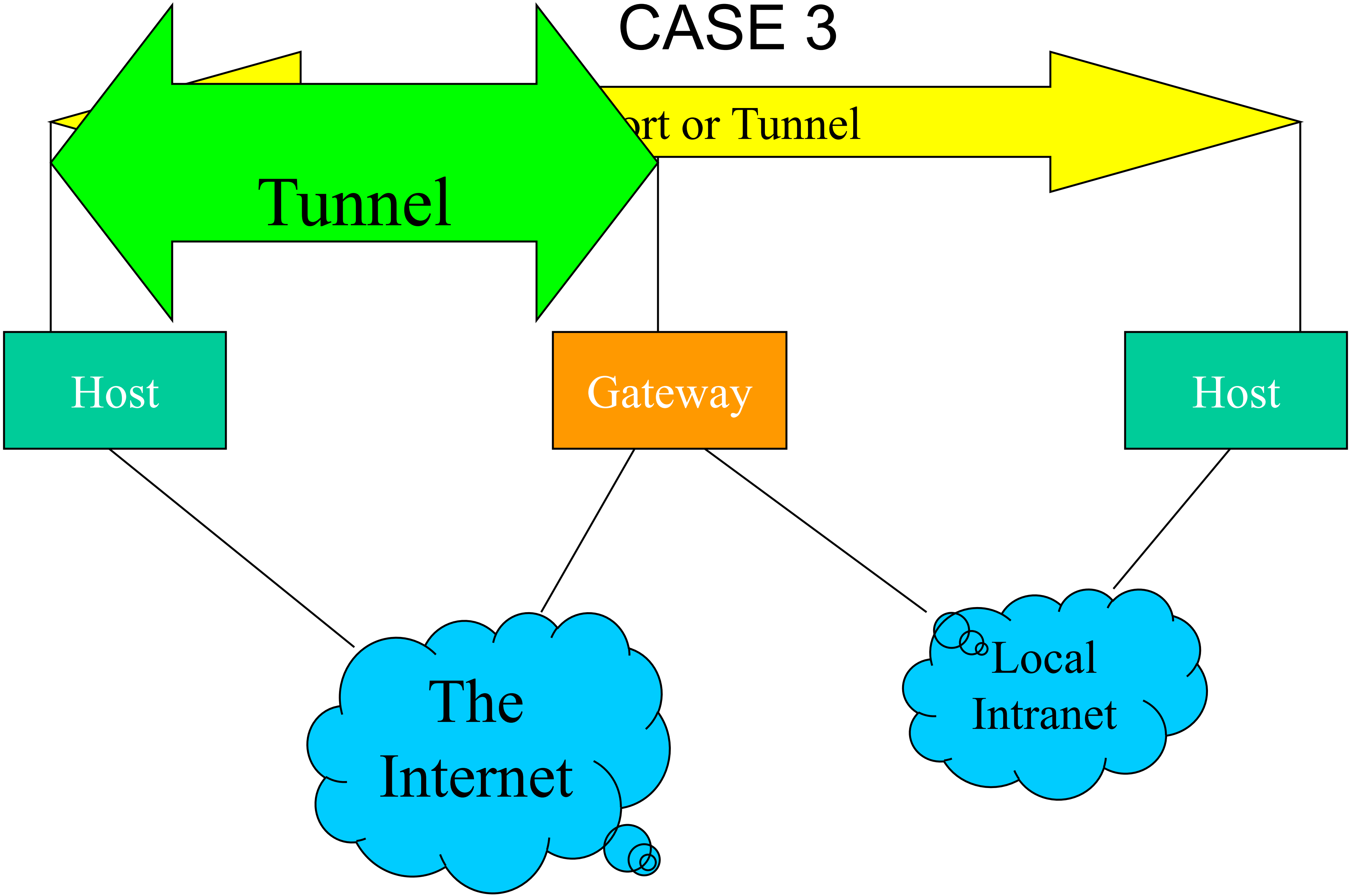
Authentication Data

Encrypted Data

Original IP Datagram

Authenticated Payload

CASE 3


rt or Tunnel
Tunnel
Host
Gateway
Host
The Internet
Local Intranet

SAD and SPD

- The IPSec protocol maintains two databases for both endpoints:
  - Security association database. Indexed by SPI’s, contains the information needed to encapsulate packets for one association: cryptographic algorithms, keys, sequence numbers, etc.
  - Security policy database: Allows for implementation of packet filtering policies. Defines whether or not to accept non-protected packets, what to require, etc.

Security Association Database

- Sequence number
- Sequence number overflow
- Anti-replay window
- AH information
  - Algorithms, initialization values, keys, etc.
- ESP information
  - Algorithms, initialization values, keys, etc.
- SA lifetime
- IPSec protocol mode
- Tunnel destination
- Path MTU (max packet size)

Security Policy Database

- Defines:
  - Traffic to be protected
  - How to protect it
- Must be consulted for each packet entering or leaving the IP stack
- Three possible actions
  - Discard
  - Bypass IPSec
  - Apply IPSec

Security Associations

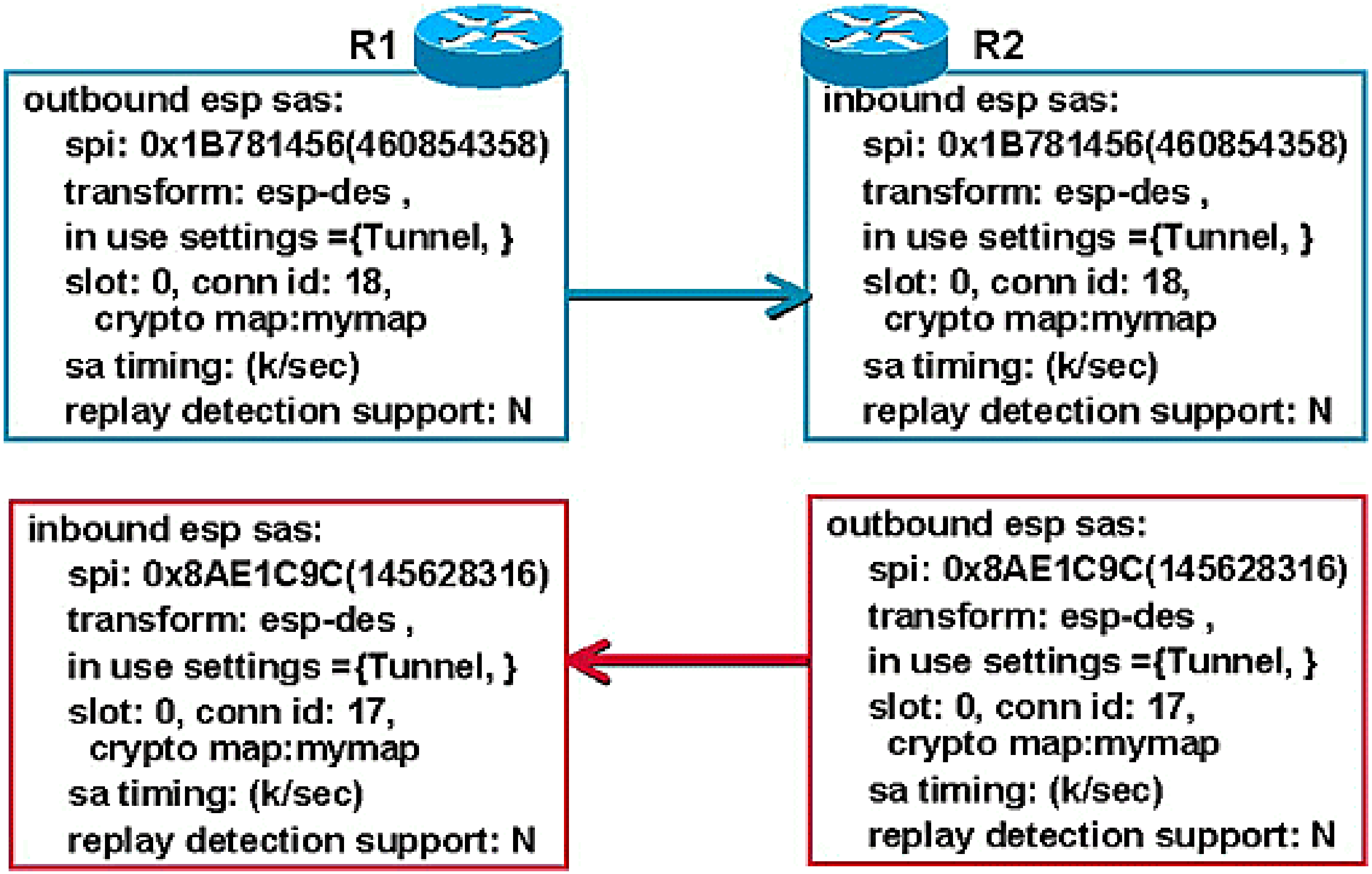
- An IPSec protected connection is called a *security association*
- The SPI used in identifying the SA is normally chosen by the receiving system (destination)
- Basic Processing
  - for outbound packets, a packet’s selector is used to determine the processing to be applied to the packet
  - More complex than for inbound where the received SPI, destination address and protocol type uniquely point to an SA

Some Security Association Selectors

- Destination IP address
- Source IP address
- Name
- Next layer protocol

- RFC 4301

SAs between two Cisco Routers



R1

```
outbound esp sas:
   spi: 0x1B781456(460854358)
   transform: esp-des ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 18,
     crypto map:mymap
   sa timing: (k/sec)
   replay detection support: N
```

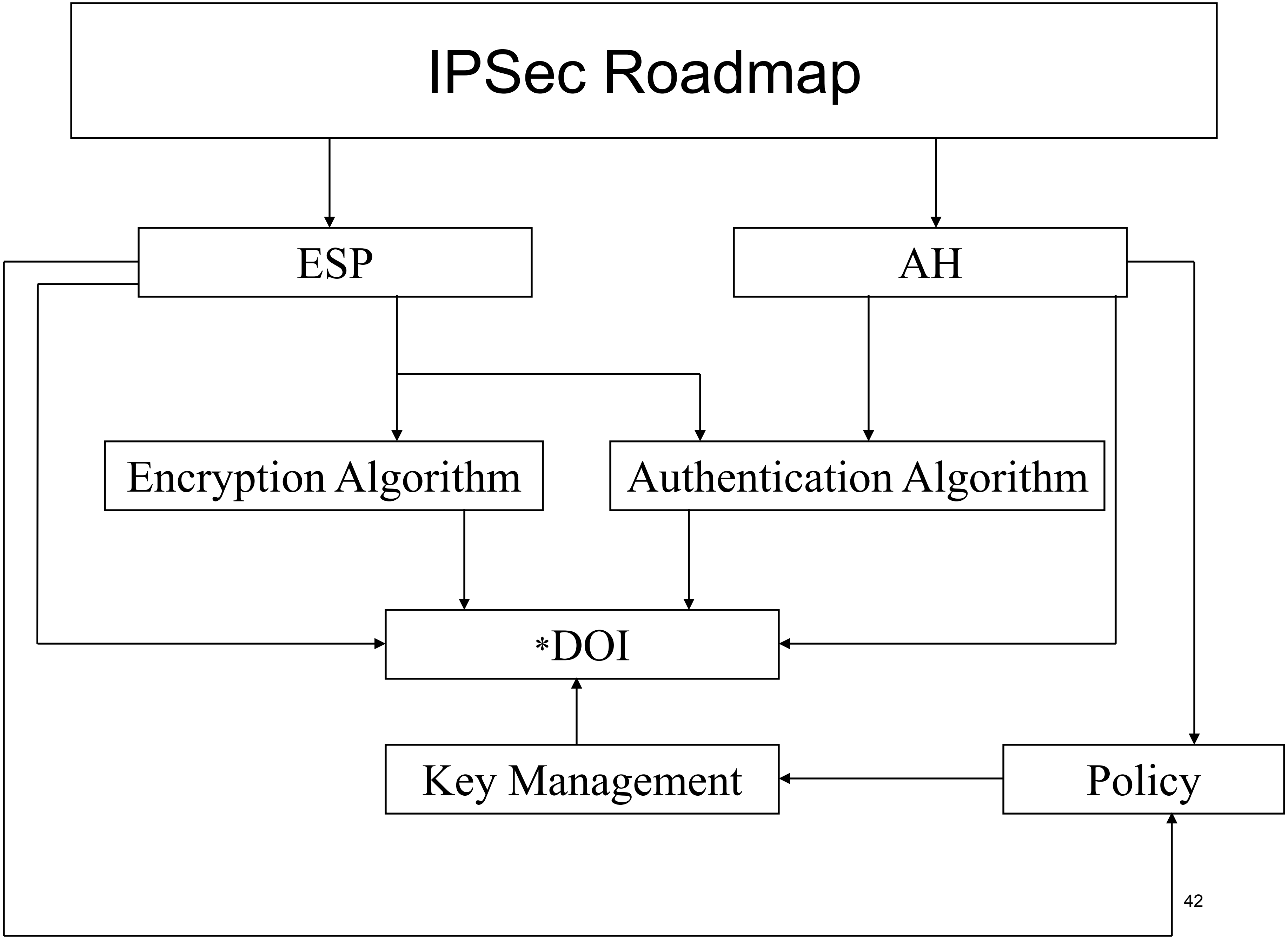
R2

```
inbound esp sas:
   spi: 0x1B781456(460854358)
   transform: esp-des ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 18,
     crypto map:mymap
   sa timing: (k/sec)
   replay detection support: N
```

```
inbound esp sas:
   spi: 0x8AE1C9C(145628316)
   transform: esp-des ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 17,
     crypto map:mymap
   sa timing: (k/sec)
   replay detection support: N
```

```
outbound esp sas:
   spi: 0x8AE1C9C(145628316)
   transform: esp-des ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 17,
     crypto map:mymap
   sa timing: (k/sec)
   replay detection support: N
```

IPSec Roadmap



*Domain of Interpretation

Readings Assignment

- Chapter 18