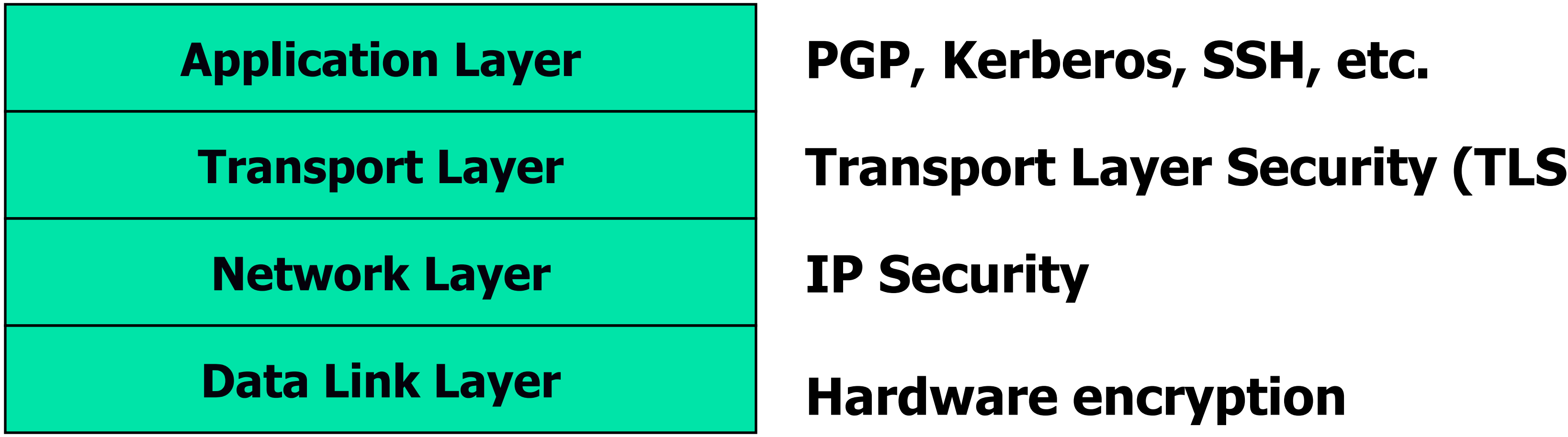
NETWORK LAYER SECURITY

IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.

IPSec helps create authenticated and confidential packets for the IP layer.

Security at What Level?



Application Layer	PGP, Kerberos, SSH, etc.
Transport Layer	Transport Layer Security (TLS
Network Layer	IP Security
Data Link Layer	Hardware encryption

Security at Application Layer

(PGP, Kerberos, SSH, etc.)

- Implemented in end-hosts
- Advantages
  - Extend application without involving operating system.
  - Application can understand the data and can provide the appropriate security.
- Disadvantages
  - Security mechanisms have to be designed independently of each application.

Security at Transport Layer

Transport Layer Security (TLS)

- Implemented in end-hosts
- Advantages
  - Existing applications get security seamlessly
- Disadvantages
  - Protocol specific

Security at Network Layer

IP Security (IPSec)

- Advantages
  - Provides seamless security to application and transport layers (ULPs).
  - Allows per flow or per connection security and thus allows for very fine-grained security control.
- Disadvantages
  - More difficult to to exercise on a per user basis on a multi-user machine.

Security at Data Link Layer

- (Hardware encryption)
- Need a dedicated link between host/routers.

- Advantages

- Speed.

- Disadvantages

- Not scalable.
- Need dedicated links.

IP Security (IPSec)

- IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF).

  Creates **secure, authenticated, reliable communications over IP networks**

IPSec Security Services

- Connectionless integrity

  Assurance that received traffic has not been modified. Integrity includes anti-reply defenses.

- Data origin authentication

  Assurance that traffic is sent by legitimate party or parties.

- Confidentiality (encryption)

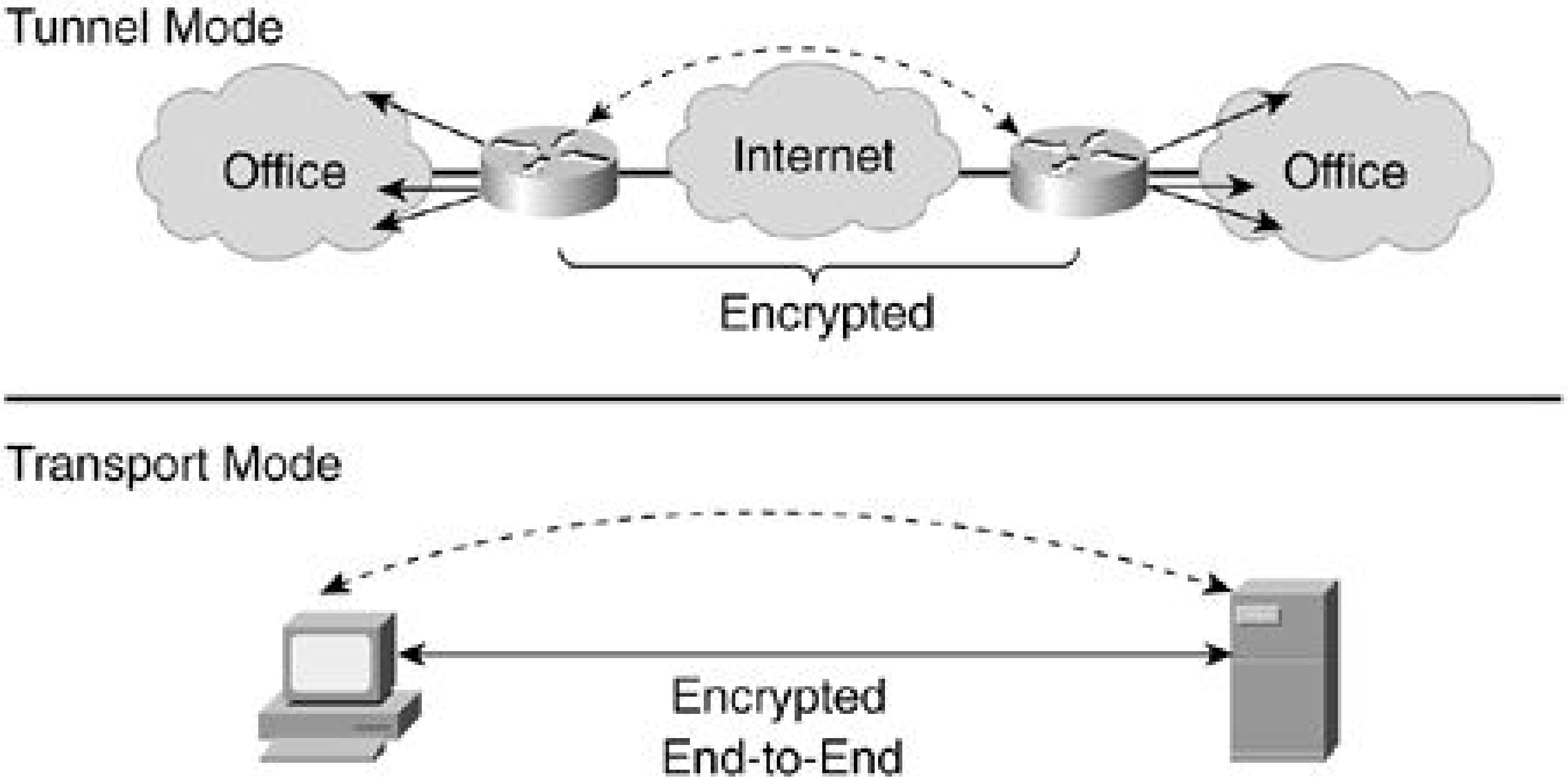
  Assurance that user's traffic is not examined by non-authorized parties.

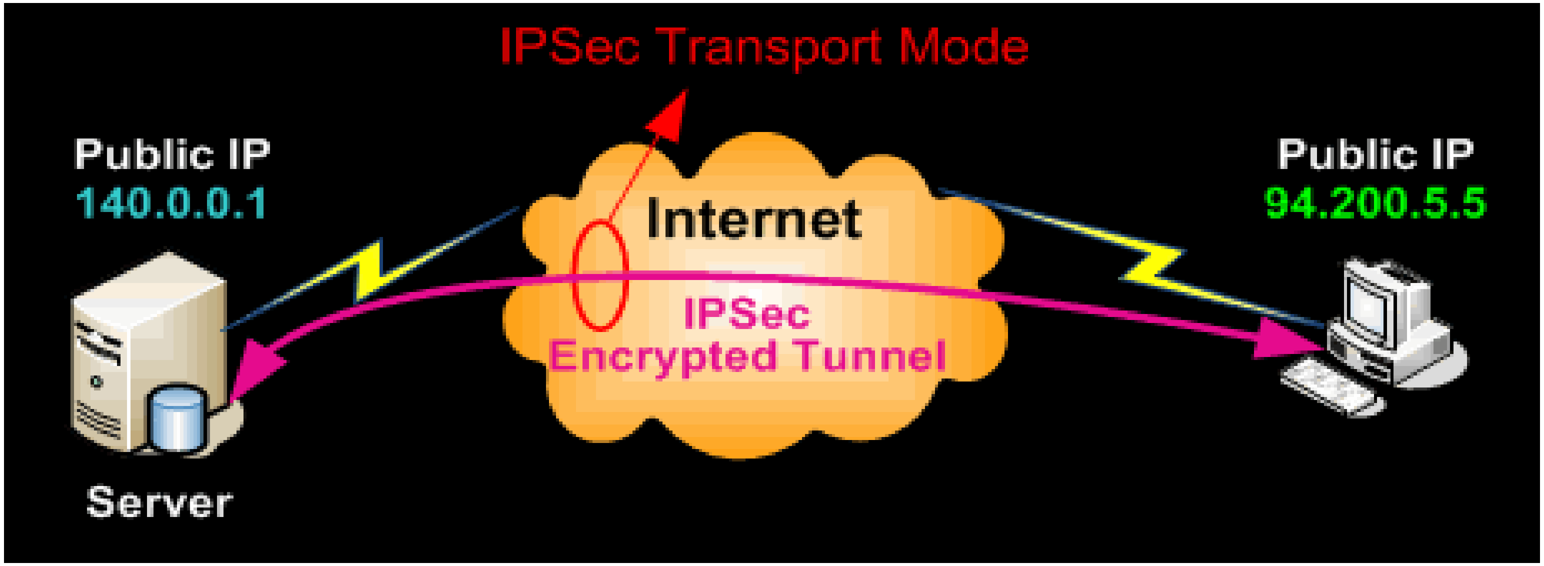
- Access control

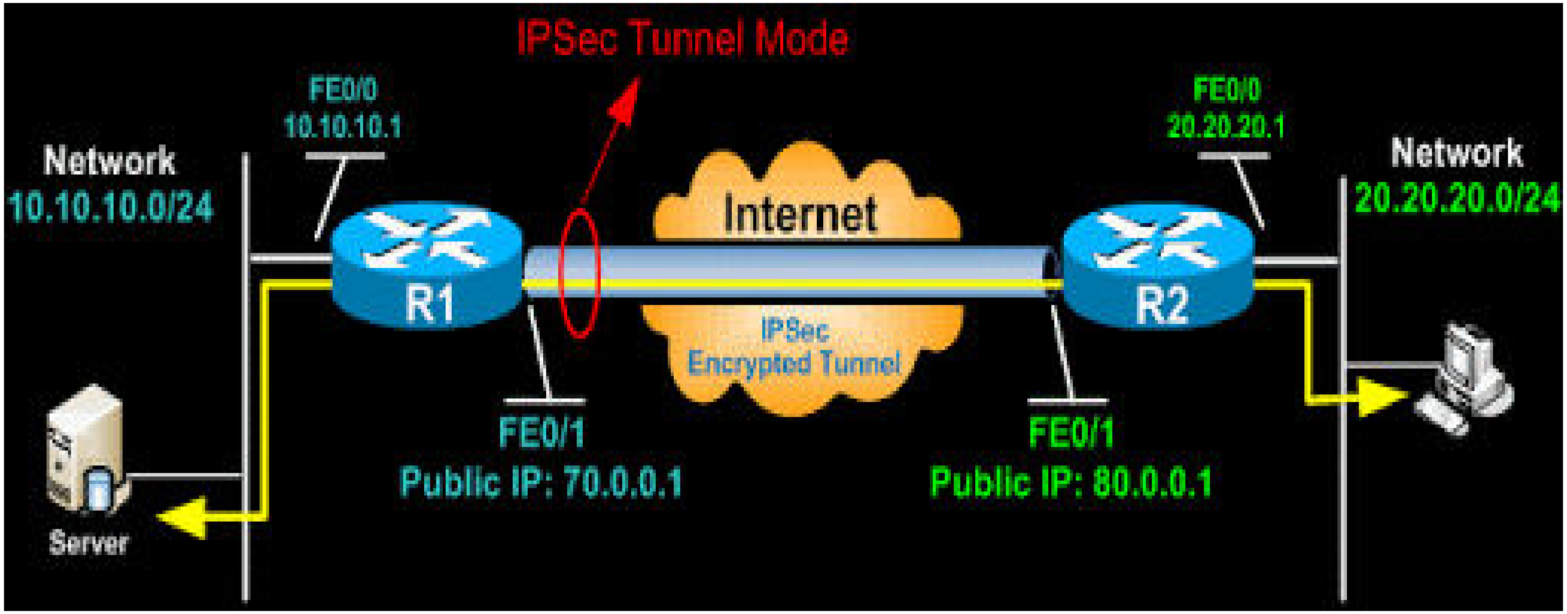
  Prevention of unauthorized use of a resource.

Links

- https://www.youtube.com/watch?v=oNmadn4gwWU


Tunnel Mode
Office
Internet
Office
Encrypted
Transport Mode
Encrypted
End-to-End


IPSec Transport Mode
Public IP
140.0.0.1
Internet
IPSec
Encrypted Tunnel
Public IP
94.200.5.5
Server

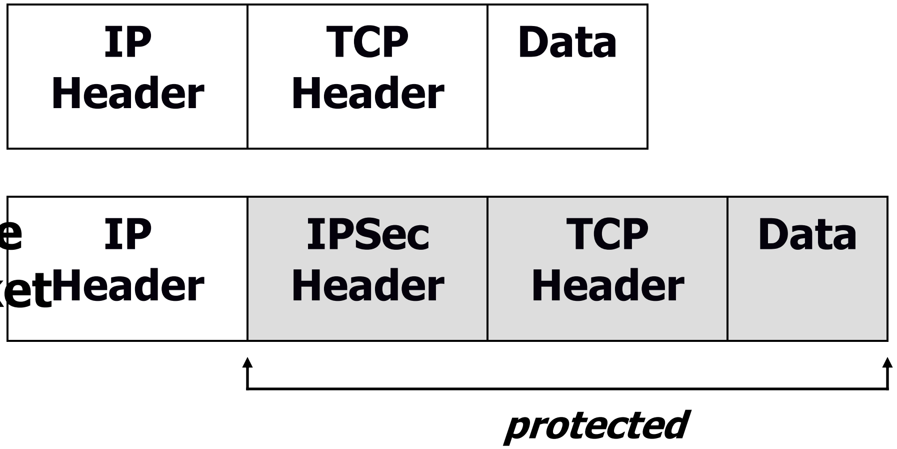

IPSec Tunnel Mode
FE0/0
10.10.10.1
Network
10.10.10.0/24
R1
Internet
IPSec
Encrypted Tunnel
R2
FE0/0
20.20.20.1
Network
20.20.20.0/24
FE0/1
Public IP: 70.0.0.1
FE0/1
Public IP: 80.0.0.1
Server

IPSec Modes of Operation

- Transport Mode: protect the upper layer protocols

Original IP Datagram

Transport Mode protected packet



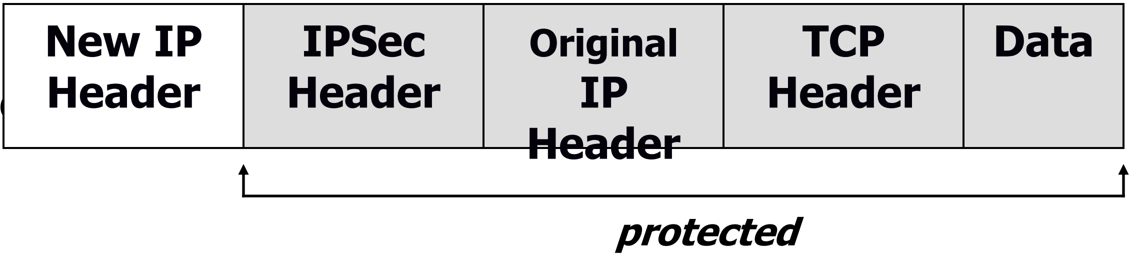
IP Header	TCP Header	Data

IP Header	IPSec Header	TCP Header	Data

protected

- **Tunnel Mode: protect the entire IP payload**

Tunnel Mode protected pack

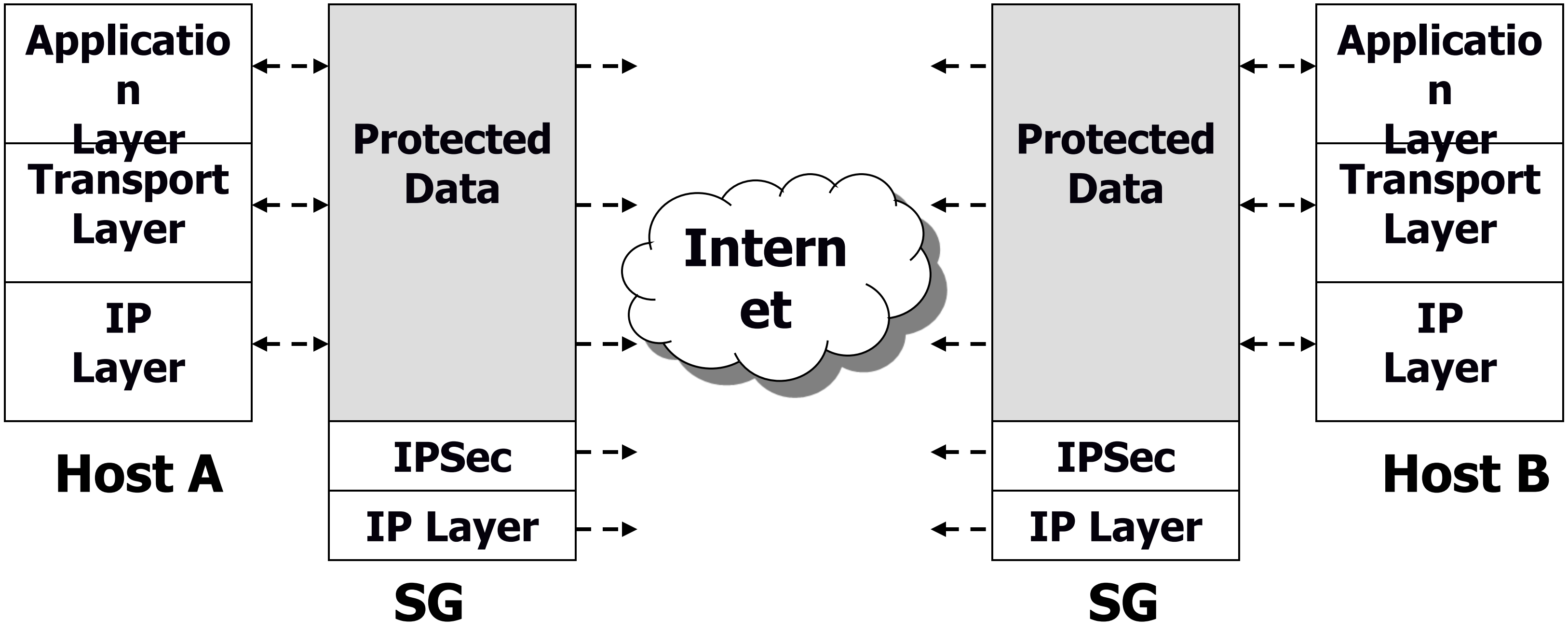


New IP Header	IPSec Header	Original IP Header	TCP Header	Data

protected

Tunnel Mode

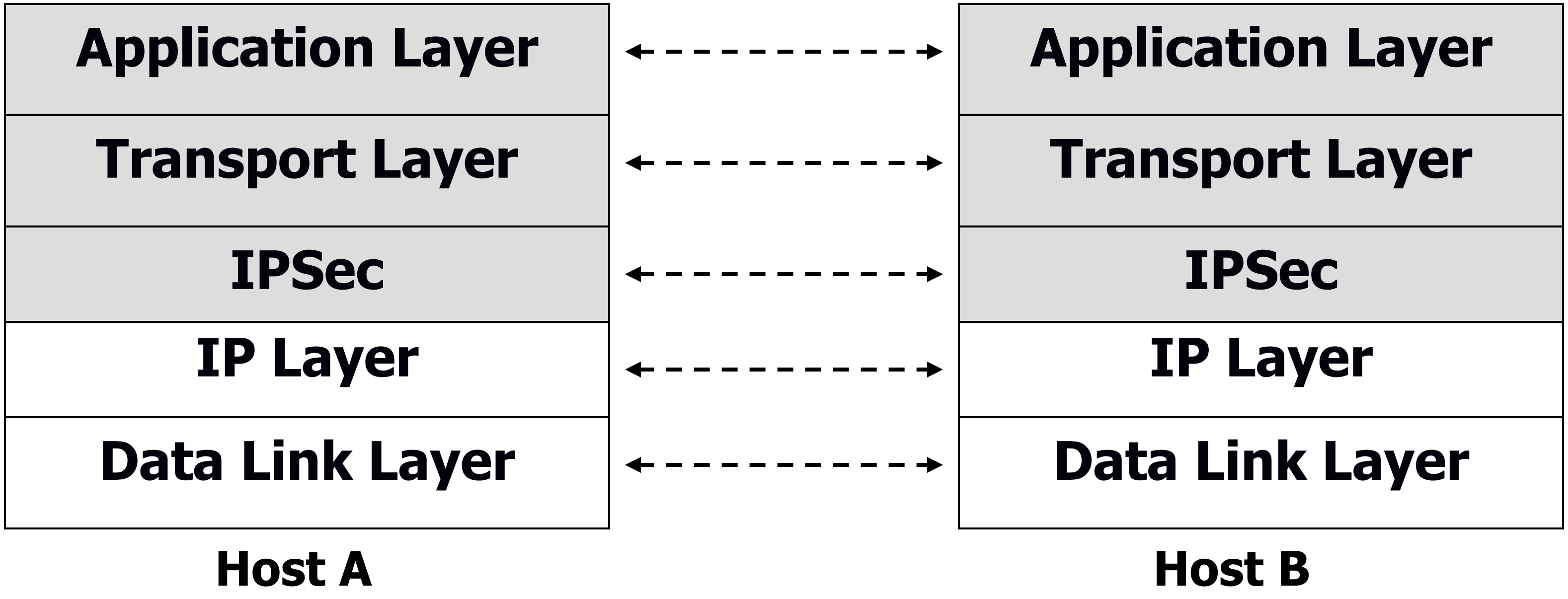
- Host-to-Network, Network-to-Network



SG = Security Gateway

Transport Mode

- Host-to-Host



Application Layer

Transport Layer

IPSec

IP Layer

Data Link Layer

Host A

Application Layer

Transport Layer

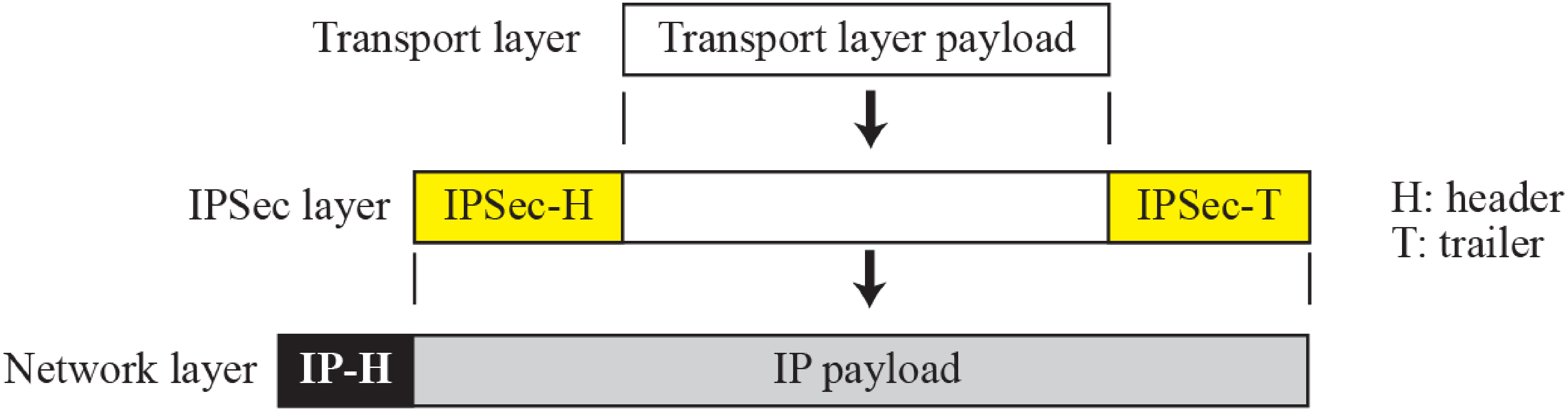
IPSec

IP Layer

Data Link Layer

Host B

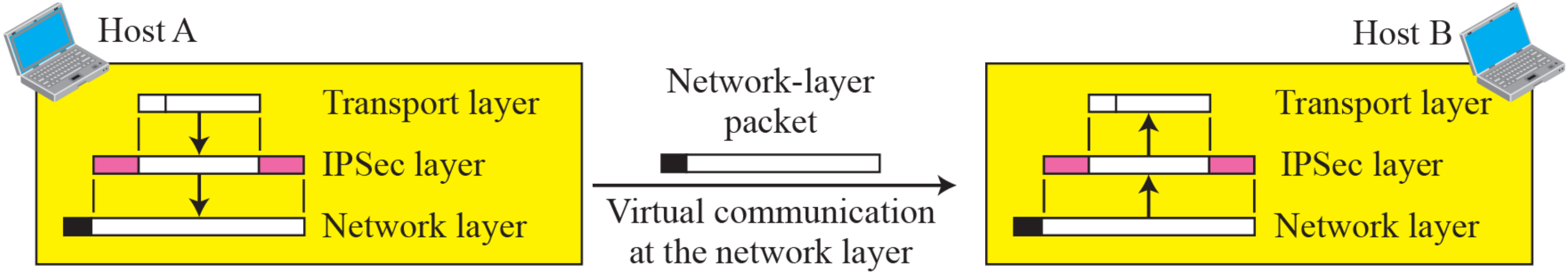
IPSec in transport mode



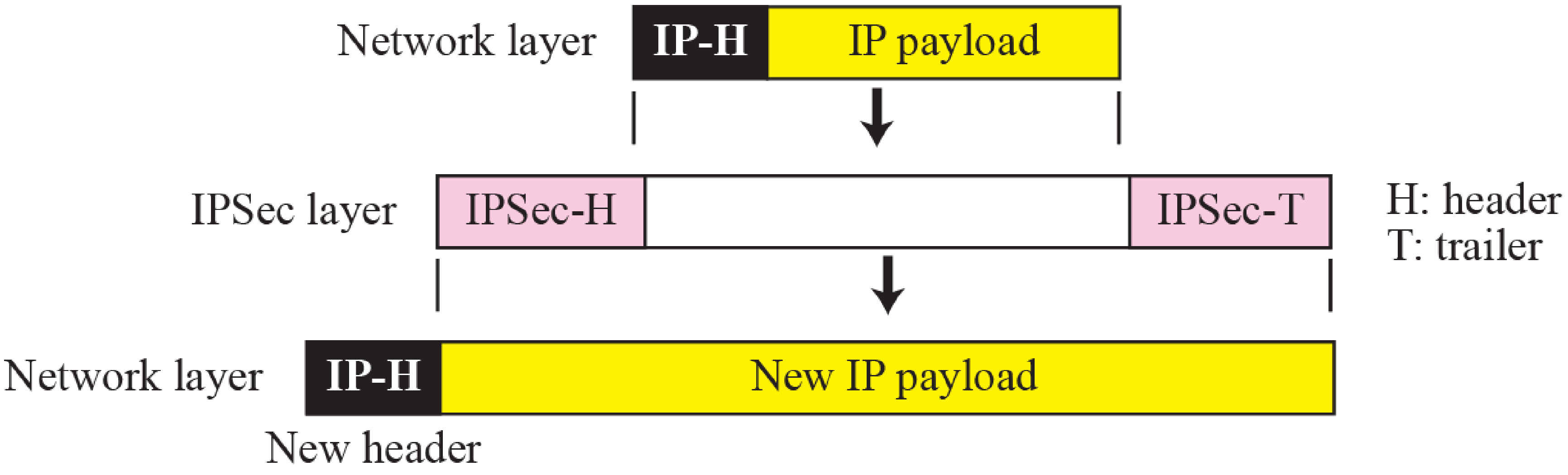
Note

IPSec in transport mode does not protect the IP header; it only protects the information coming from the transport layer.

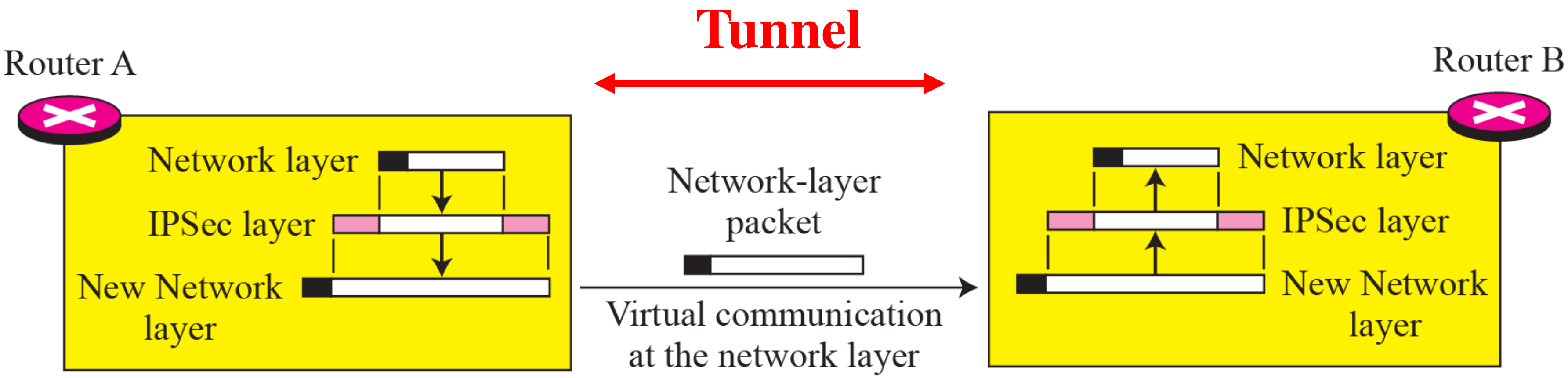
Transport mode in Action



IPSec in tunnel mode



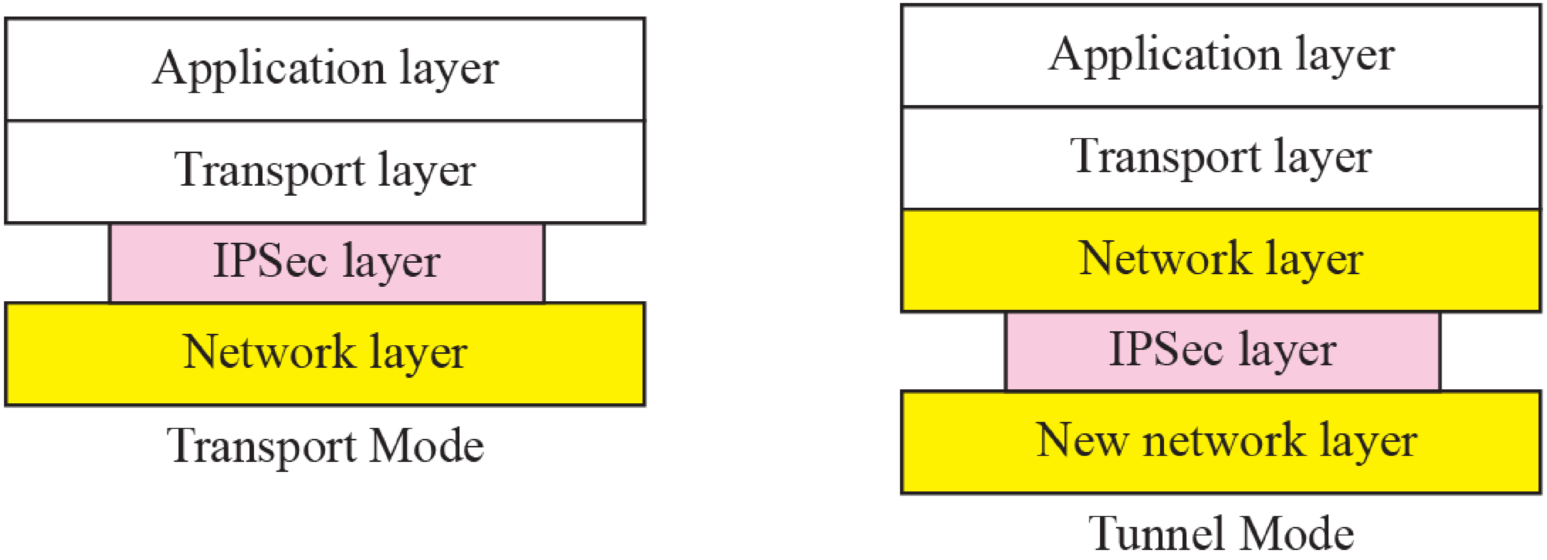
Tunnel-mode in action



Note

IPSec in tunnel mode protects the original IP header.

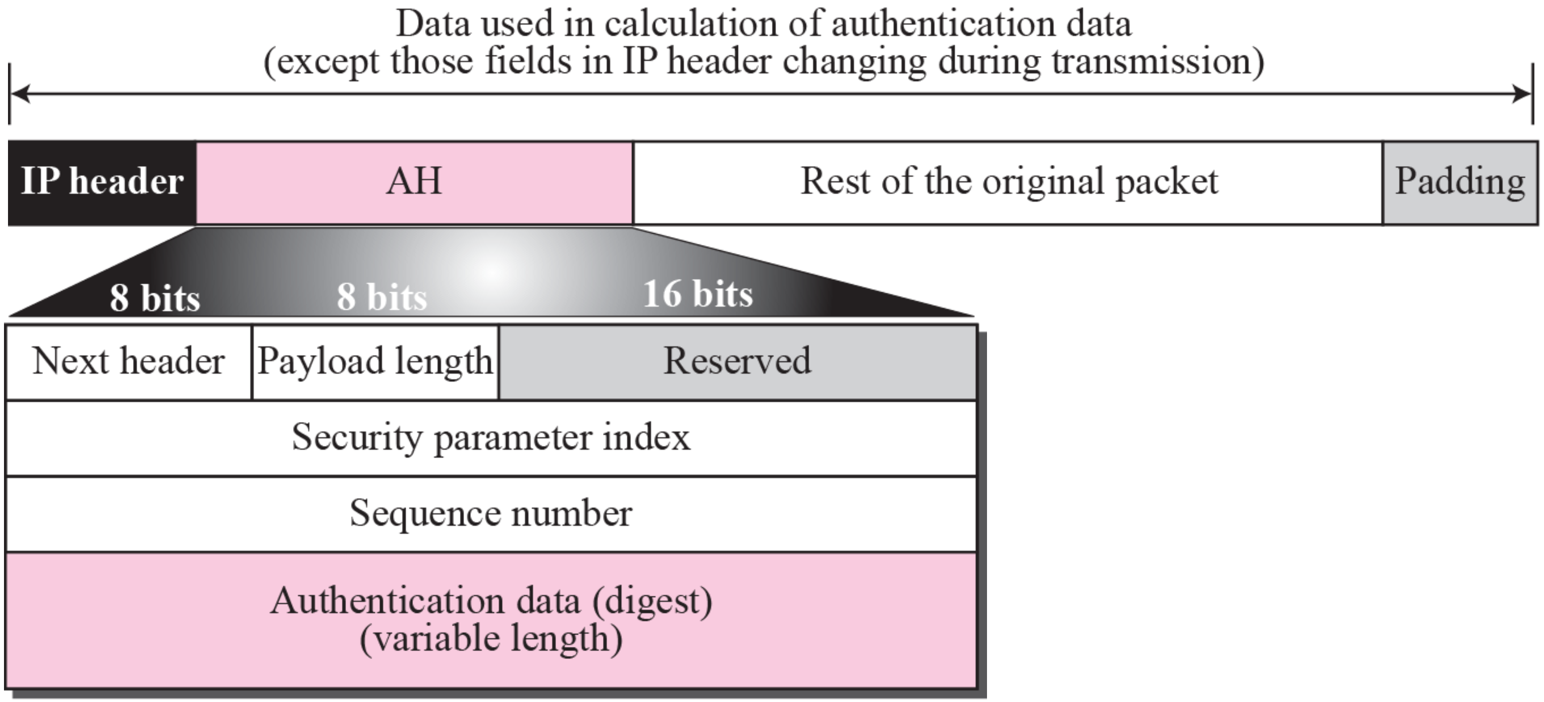
Transport mode versus tunnel mode



IPSec Security Protocols

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

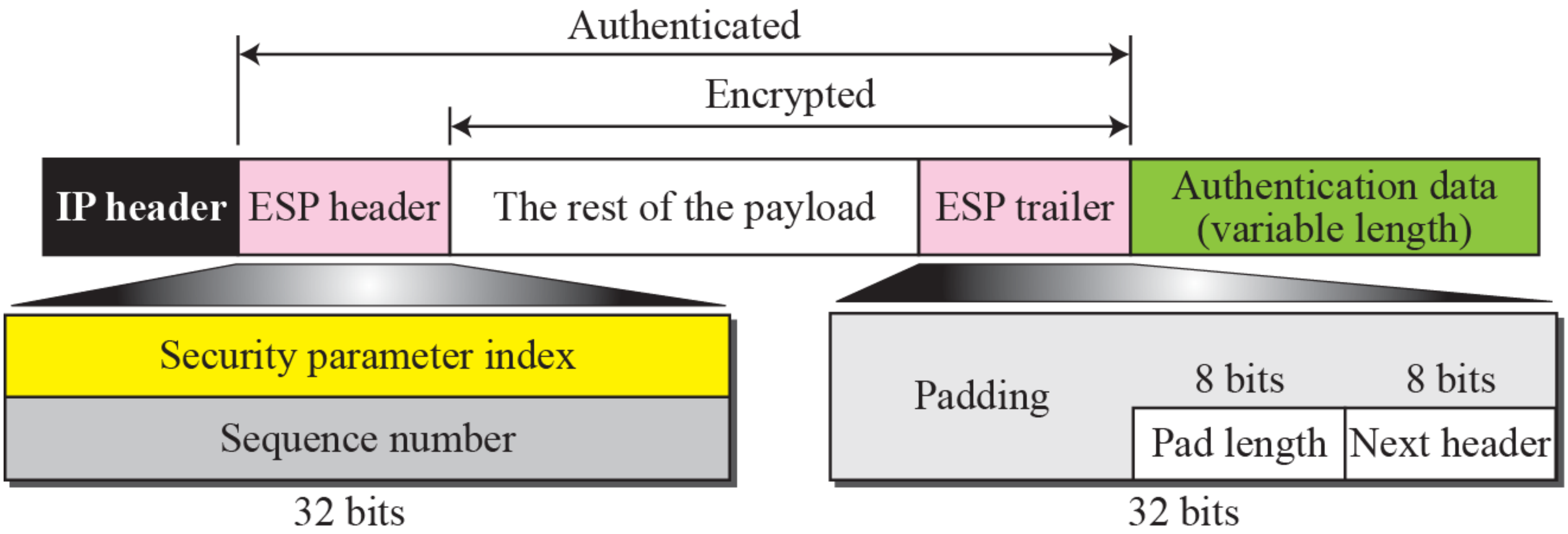
Authentication Header (AH) protocol


Data used in calculation of authentication data
(except those fields in IP header changing during transmission)
IP header
AH
Rest of the original packet
Padding
8 bits
8 bits
16 bits
Next header
Payload length
Reserved
Security parameter index
Sequence number
Authentication data (digest)
(variable length)

Note

The AH protocol provides source authentication and data integrity, but not privacy.

Encapsulating Security Payload (ESP)



Note

ESP provides source authentication, data integrity, and privacy.

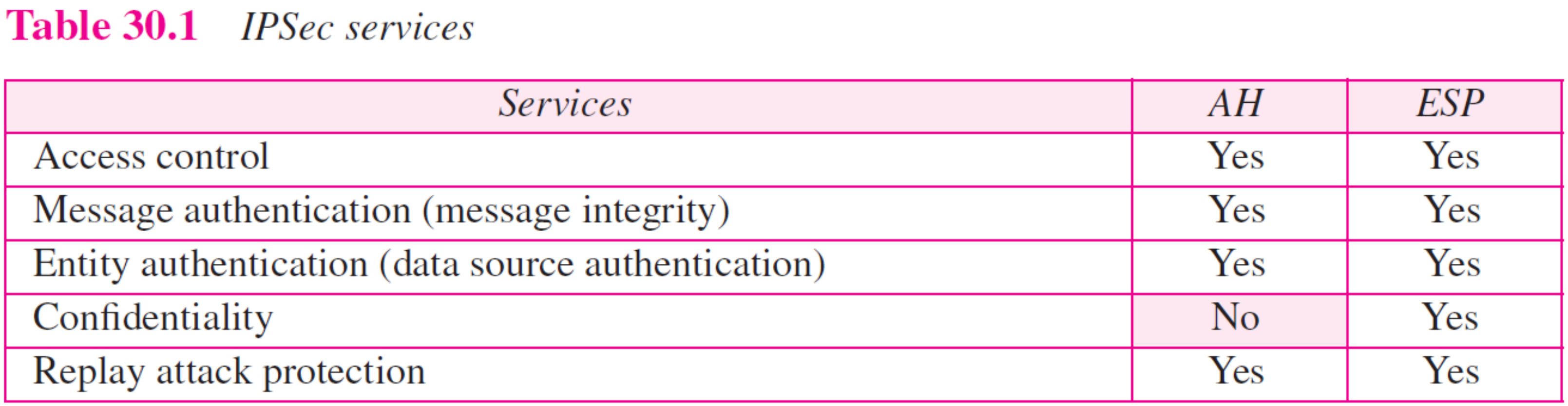


Table 30.1 *IPSec services*

Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

Security Parameter Index SPI

- The Security Parameter Index (SPI) is a very important element in the SA. An SPI is a 32-bit number that is used to uniquely identify a particular SA for any connected device.
- A Security Association (SA) is an agreement between two devices about how to protect information during communication.
- It also indicates the parameters, such as keys and algorithms.
- SPI provides a mechanism for the destination to identify which SA to use to check the security of the received packet.
- The SPI is provided to map the incoming packet to an SA at the destination
- The SPI is a 32-bit random number generated by the sender to identify the SA to the recipient.

Security Policy Database (SPD)

- IPSec Policies are maintained in the Security Policy Database (SPD).
- IPSec Policies define which traffic to be protected, how it is to be protected, and with whom to protect it.
- The sending host determines what policy is appropriate for the packet, depending on various "Selectors" by checking in the Security Policy Database (SPD).
- "Selectors" can include Source and Destination IP Addresses, Name (User ID ir a System Name), Transport Layer Protocols (TCP or UDP) or Source and Destination Ports.
- The Security Policy Database (SPD) indicates what the policy is for a particular packet. If the packet requires IPsec processing, it is passed to the IPsec module for the required processing.

Security Association Database (SAD)

- IPSec Security Associations are stored in the Security Association Database (SAD).
- Each Security Association has an entry in the Security Association Database (SAD).
- The Security Association entries in the Security Association Database (SAD) are indexed by the three Security Association properties.

  1) Destination IP address 2) IPSec protocol 3) Security Parameter Index (SPI).

Simple SA

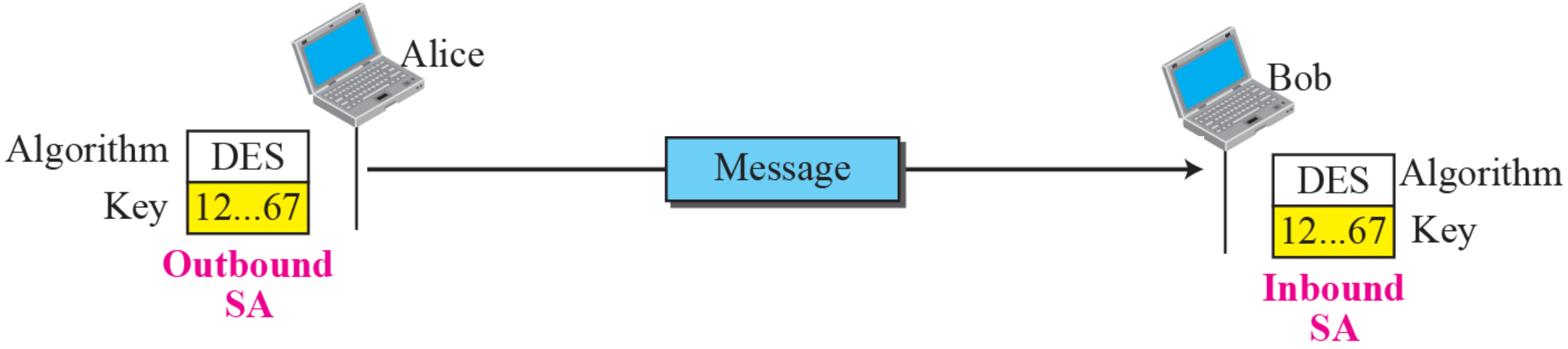

Alice
Algorithm
DES
Key
12...67
Outbound SA
Message
Bob
DES
Algorithm
12...67
Key
Inbound SA

Figure 30.9 *SAD*

Index	SN	OF	ARW	AH/ESP	LT	Mode	MTU
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							

Security Association Database

Legend:

SPI: Security Parameter Index
DA: Destination Address
AH/ESP: Information for either one
P: Protocol
Mode: IPSec Mode Flag

SN: Sequence Number
OF: Overflow Flag
ARW: Anti-Replay Window
LT: Lifetime
MTU: Path MTU

SPD

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	

Legend:

SA: Source Address

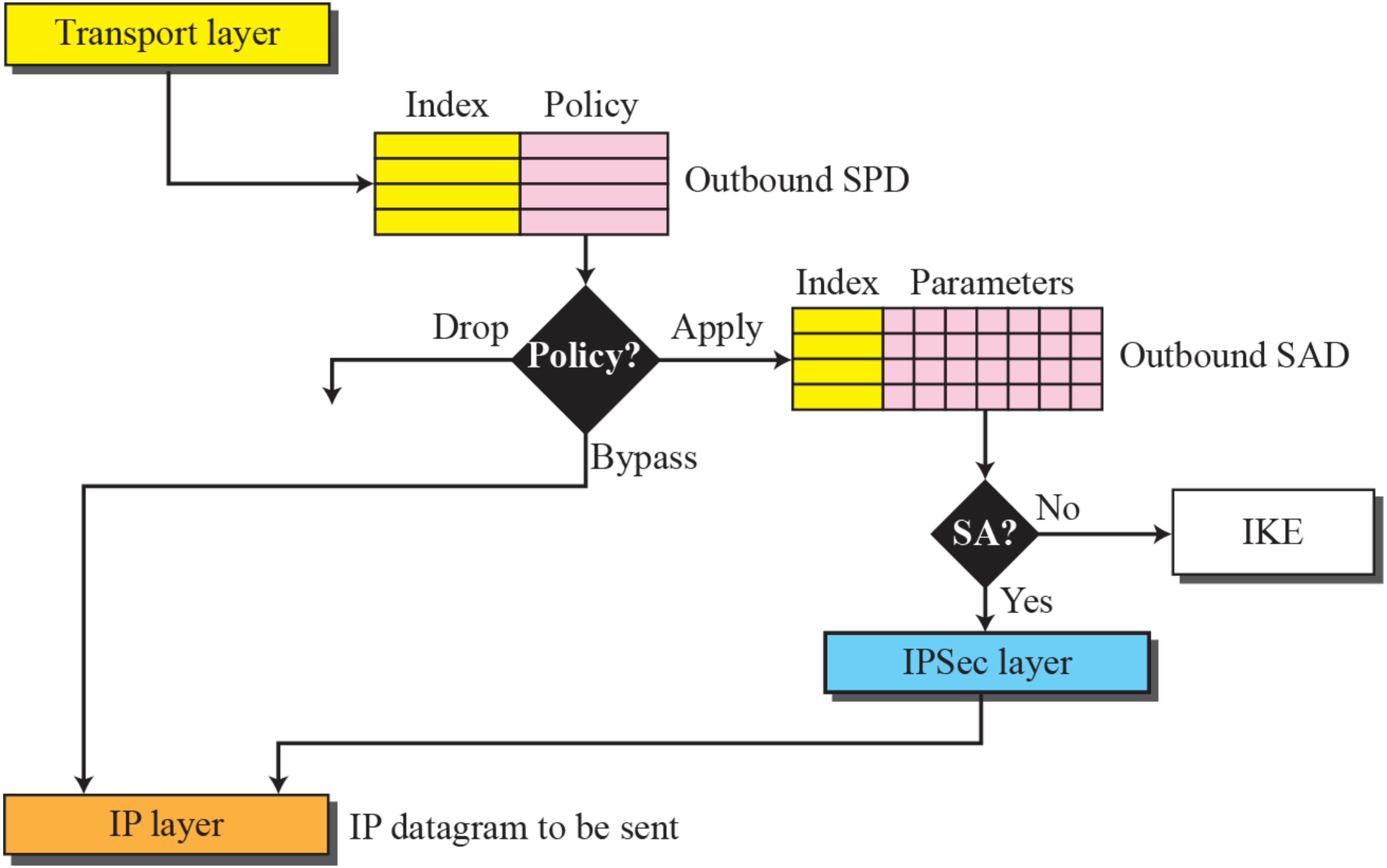
DA: Destination Address

P: Protocol

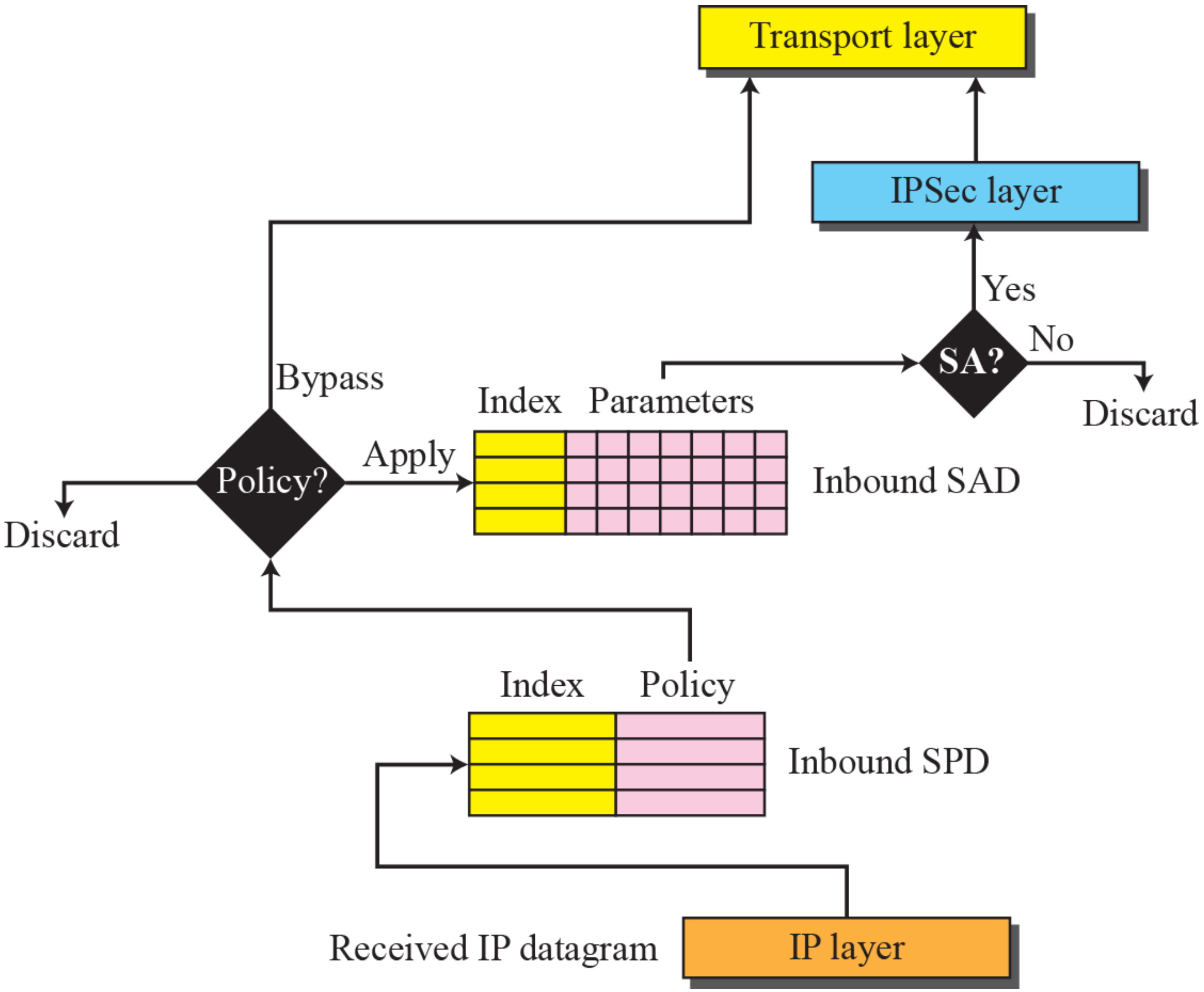
SPort: Source Port

DPort: Destination Port

Outbound processing



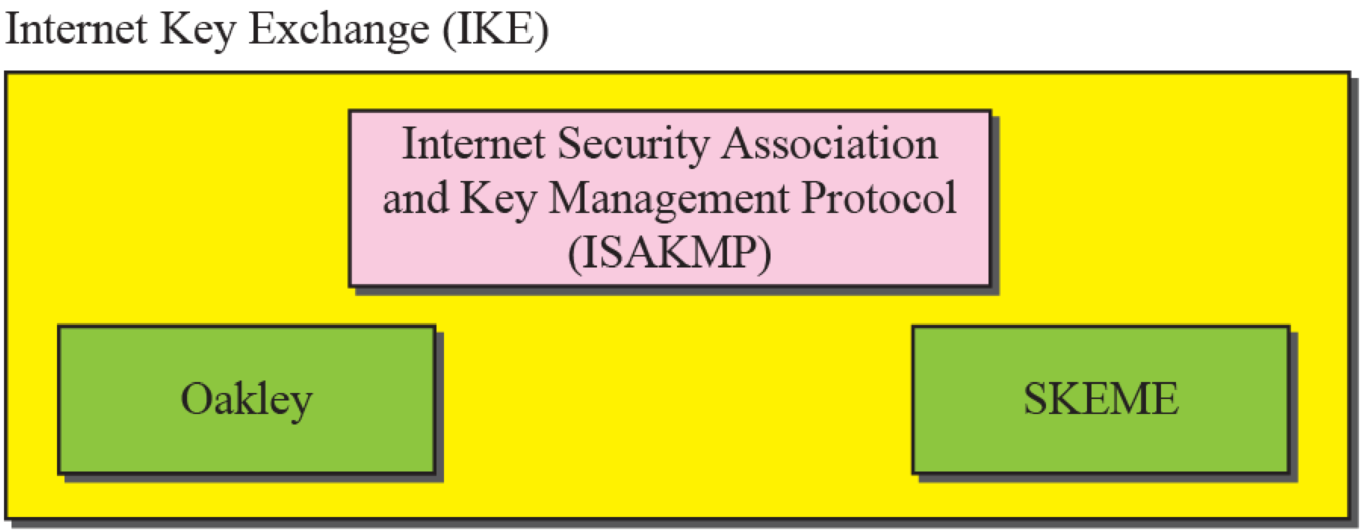
Inbound processing



Note

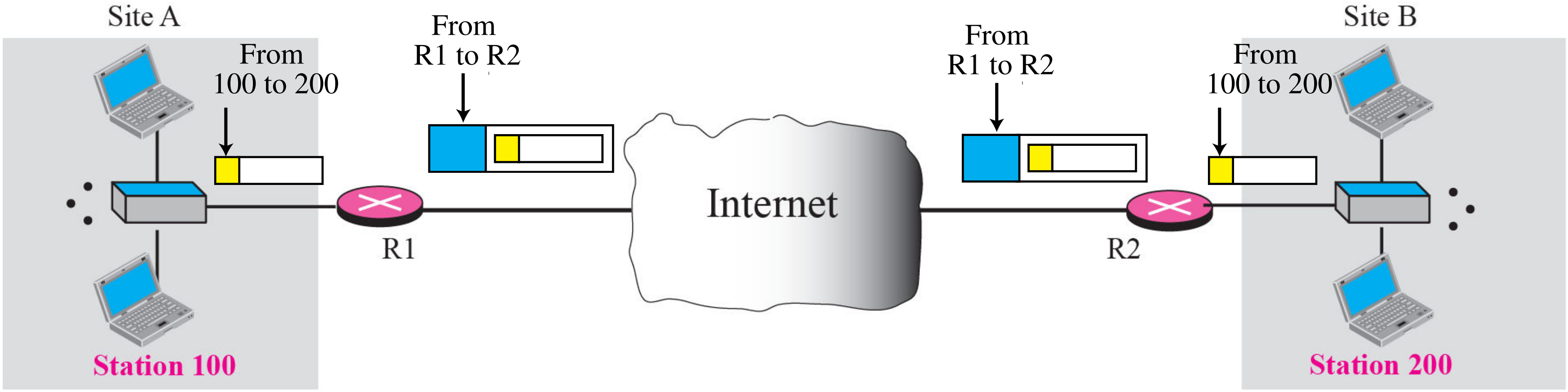
IKE creates SAs for IPSec.

Figure 30.13 *IKE components*



Internet Key Exchange (IKE)
Internet Security Association and Key Management Protocol (ISAKMP)
Oakley
SKEME

Figure 30.14 *Virtual private network*


Site A
From
100 to 200
From
R1 to R2
Internet
From
R1 to R2
Site B
From
100 to 200
R1
R2
Station 100
Station 200