Chapter 32

Internet Security

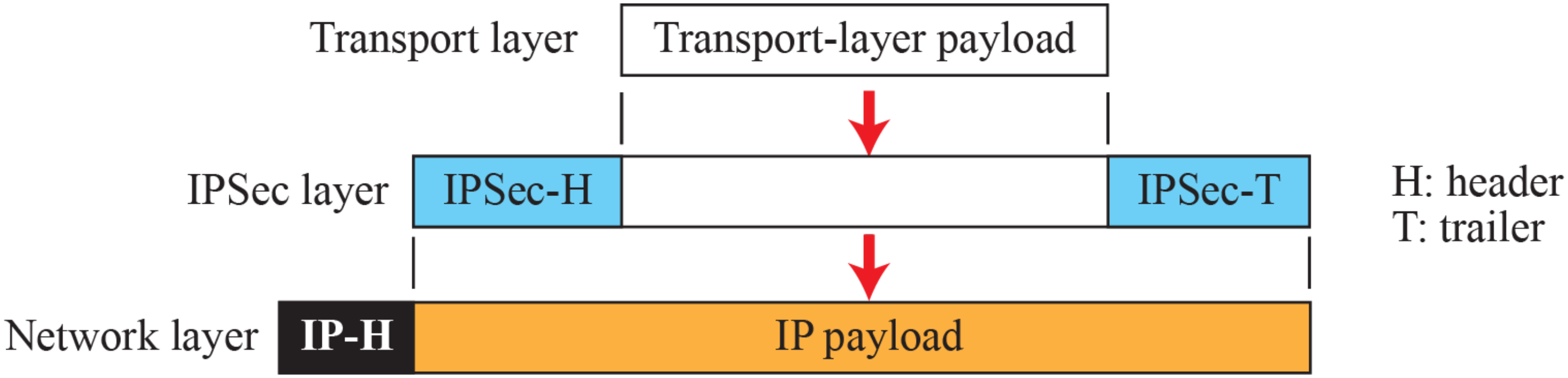
Objective

- Security at the network layer, IPSec: transport mode and tunnel mode.
- Security protocols at the transport layer, SSL.
- Security at the application layer: e-mail application

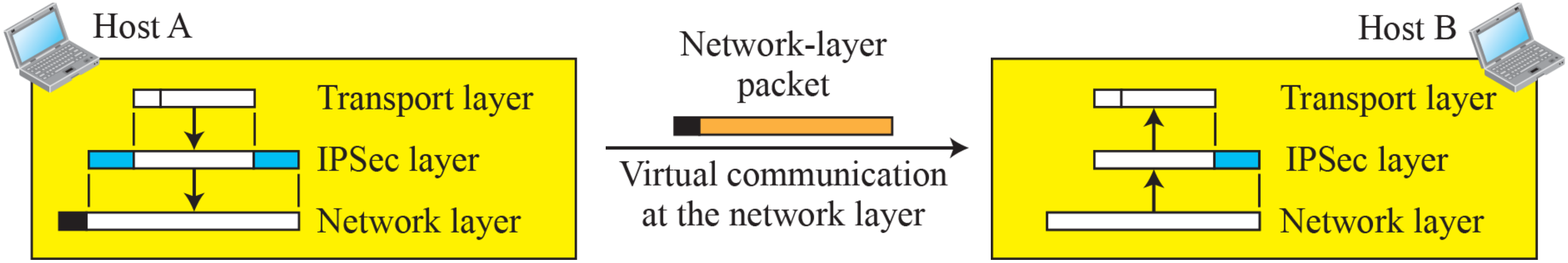
  PGP and S/MIME.
- Firewalls

NETWORK-LAYER SECURITY

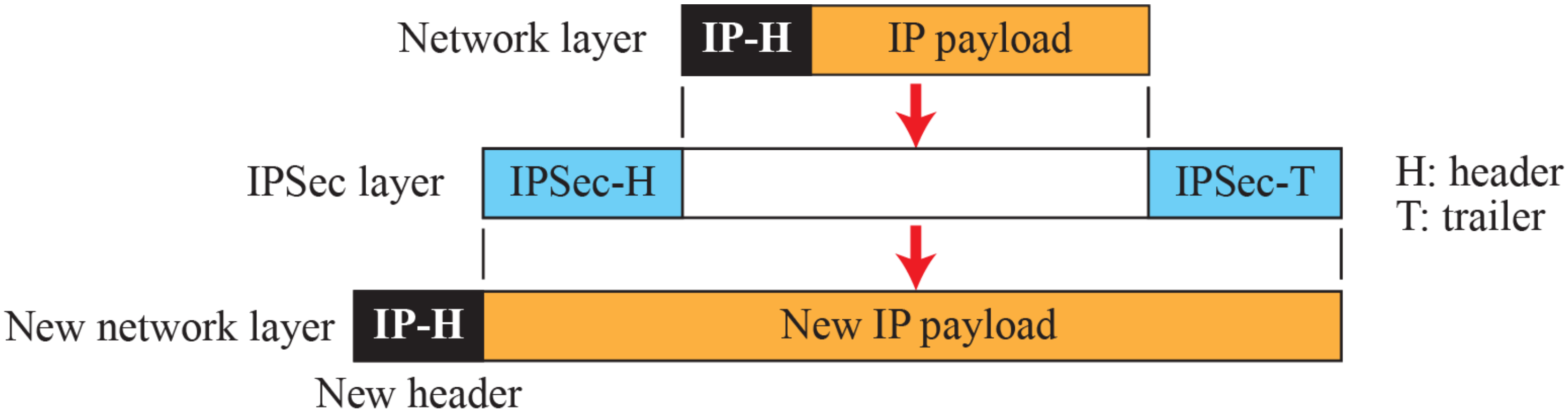
- Security at the network layer.
- At the network layer, security is applied between two hosts, two routers, or a host and a router.
- The purpose of network-layer security is to protect those applications that use the service of the network layer directly.
- IPSec operates in one of two different modes: transport mode or tunnel mode.



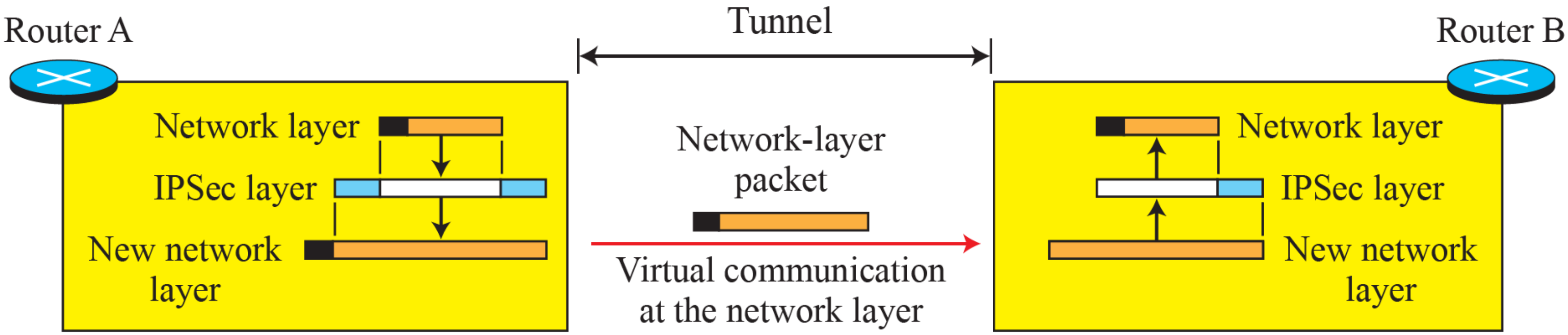
IPSec in transport mode



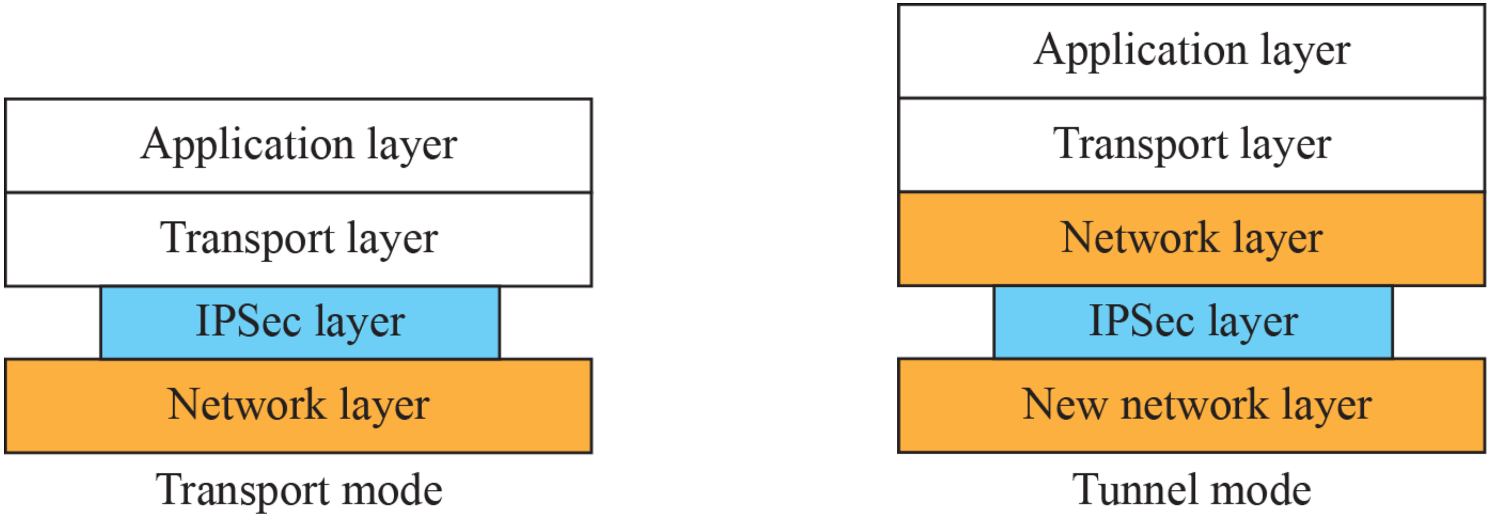
Transport mode in action



IPSec in tunnel mode



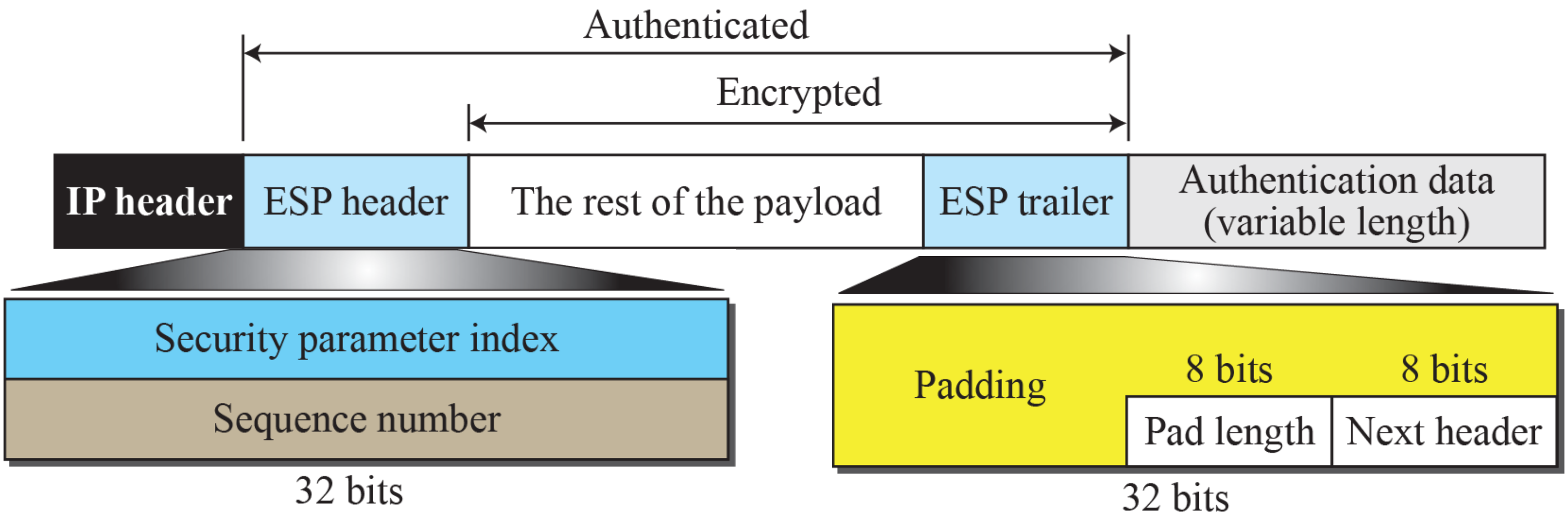
Tunnel mode in action



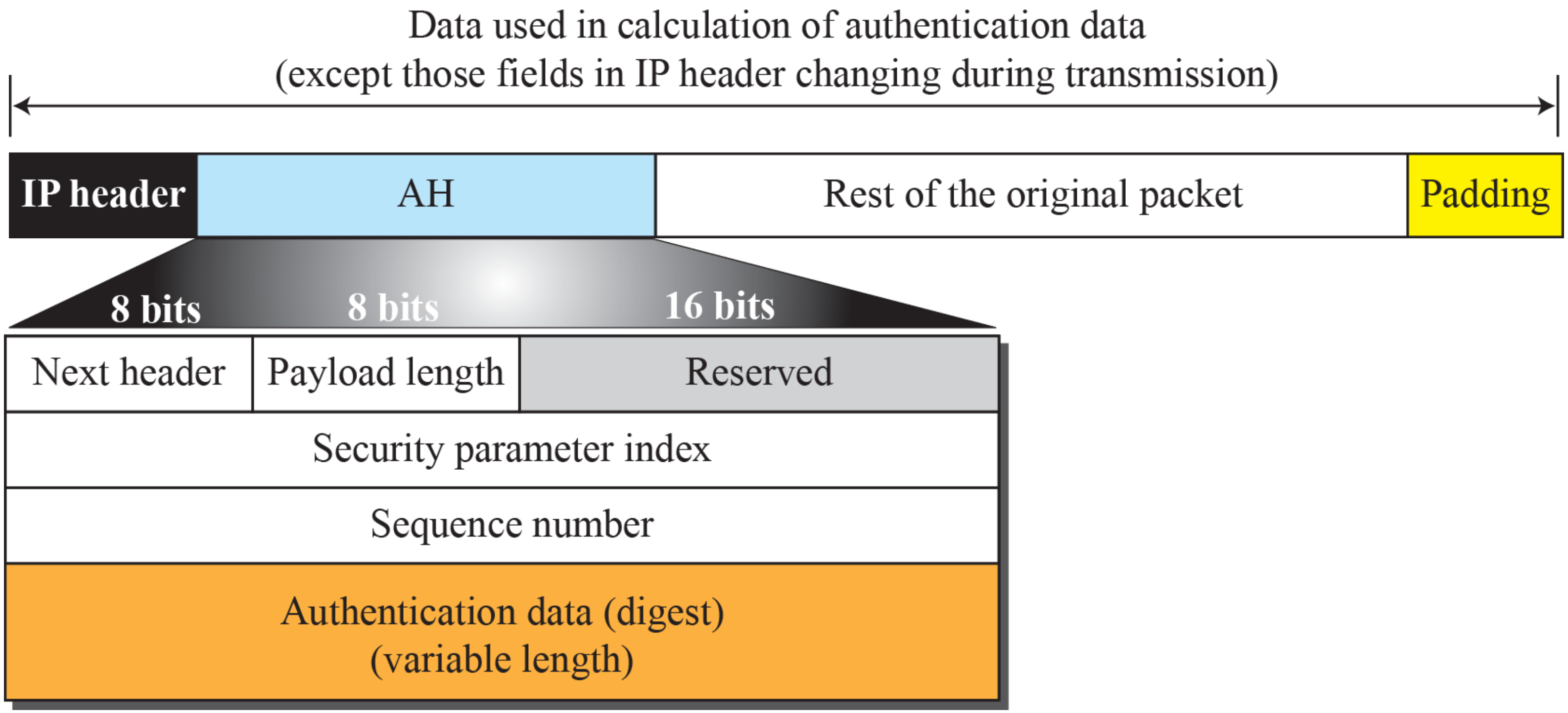
Transport mode versus tunnel mode

Two Security Protocols

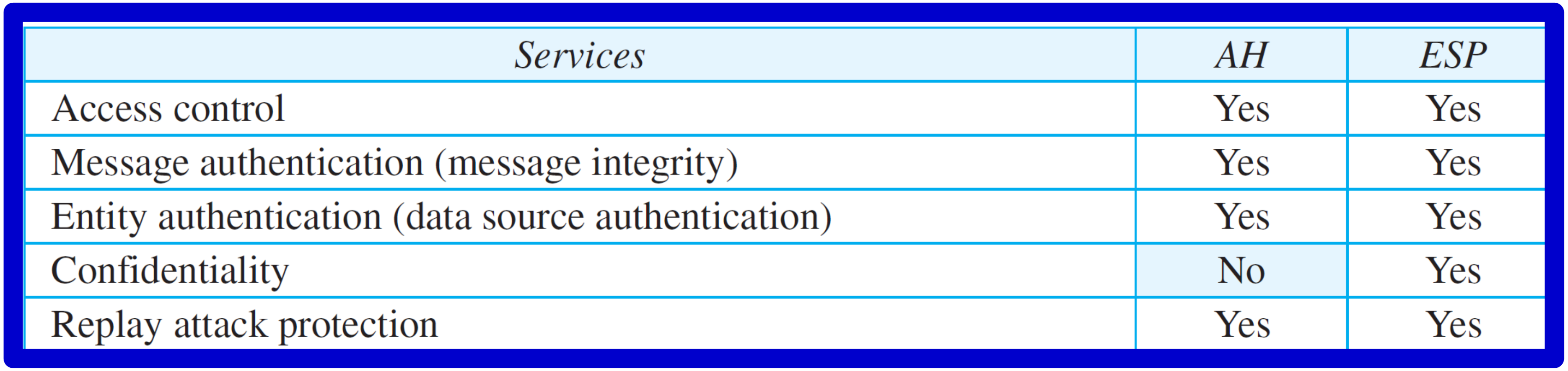
- IPSec defines two protocols, the Authentication Header (AH) Protocol and the Encapsulating Security Payload (ESP) Protocol, to provide authentication and/or encryption for packets at the IP level.



Encapsulating Security Payload (ESP)


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)

Authentication Header (AH) protocol

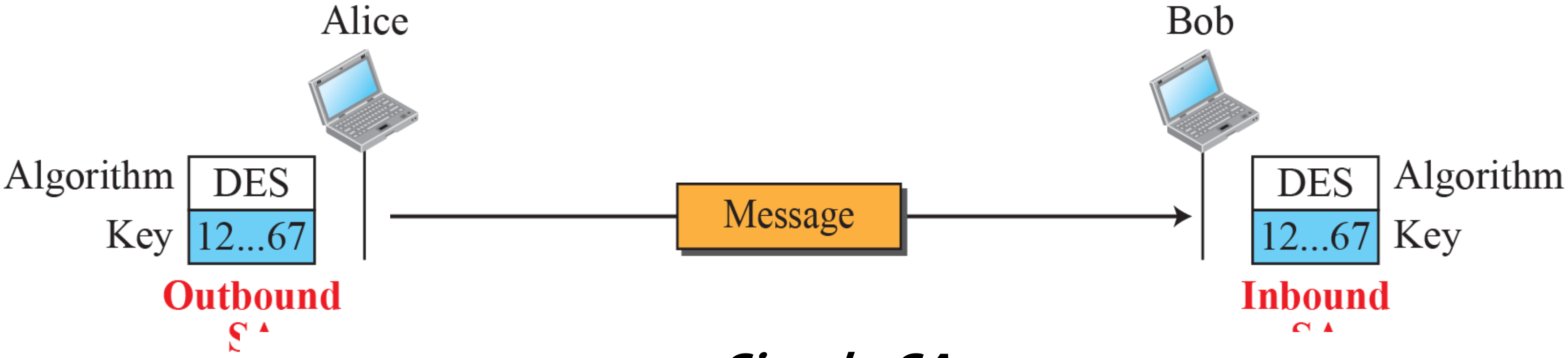


Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

IPSec services

Security Association

- Security Association is a very important aspect of IPSec.
- IPSec requires a logical relationship, called a Security Association (SA), between two hosts.
- The security association changes the connectionless service provided by IP to a connection-oriented service upon which we can apply security.



Simple SA

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

Security Association Database

SN: Sequence number
OF: Overflow flag
ARW: Anti-replay window
LT: Lifetime
MTU: Path MTU

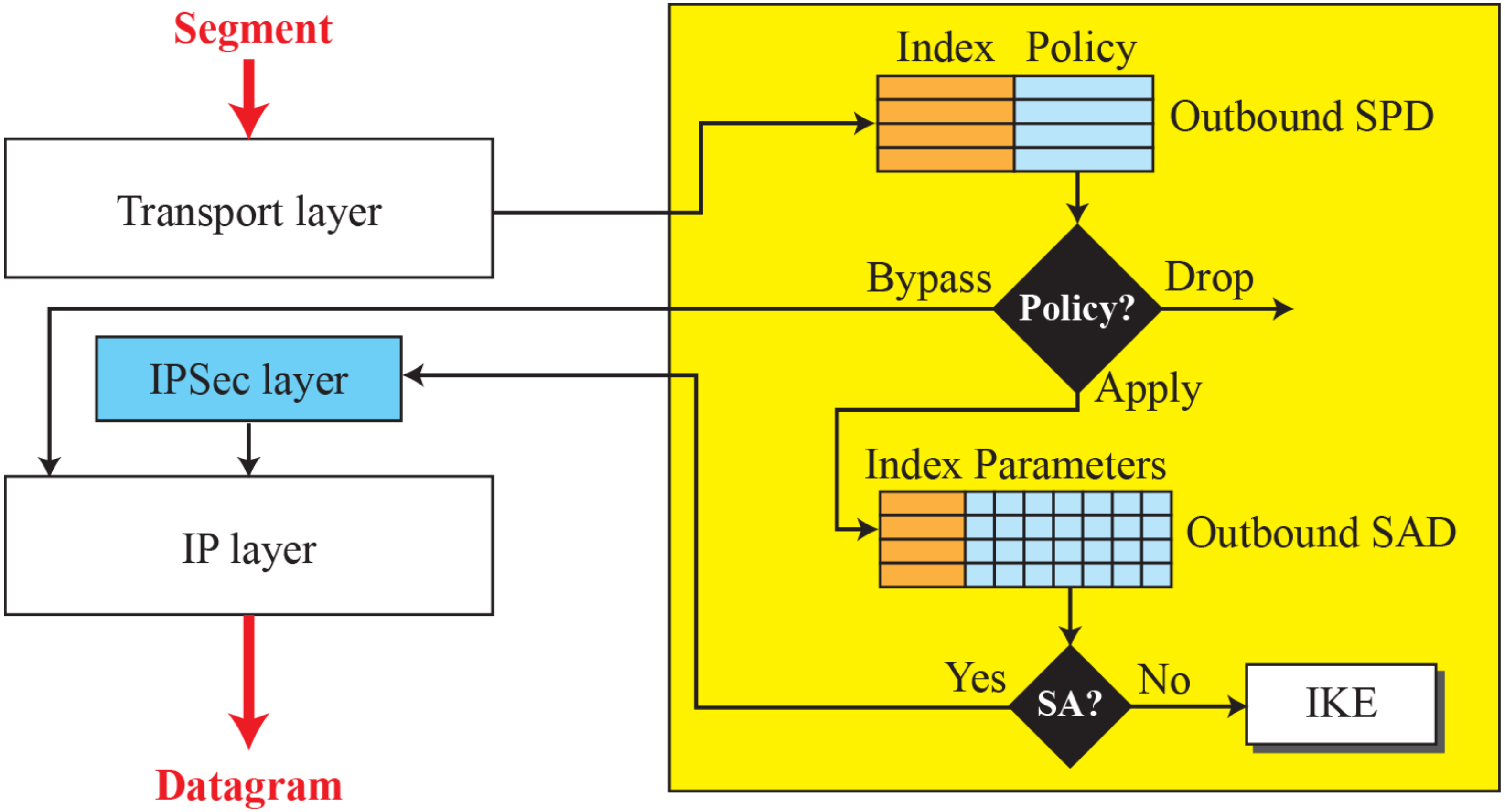
SPI: Security parameter index
DA: Destination address
AH/ESP: Information
P: Protocol
Mode: IPSec mode flag

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

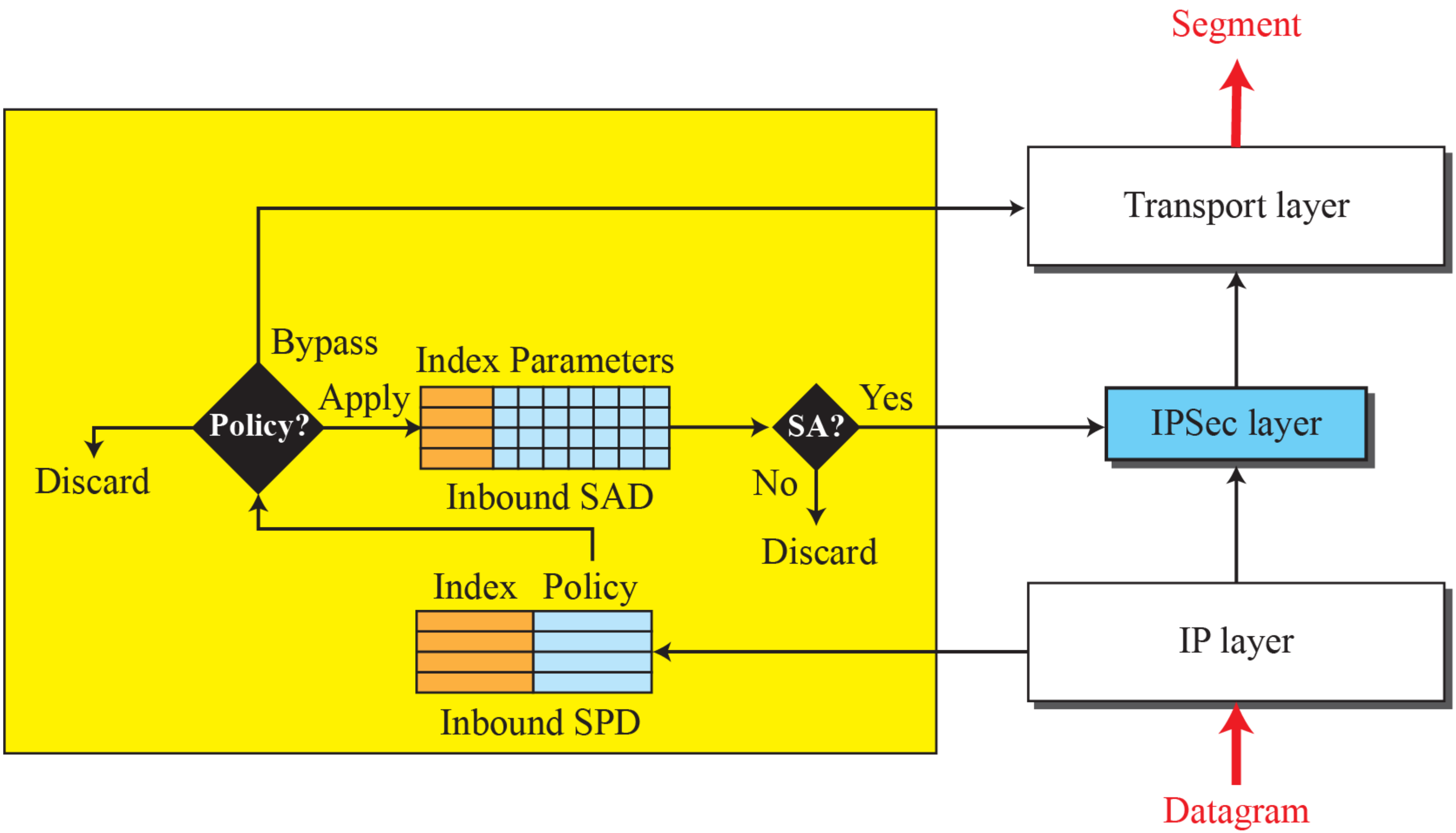
SA: Source address
DA: Destination address
P: Protocol

SPort: Source port
DPort: Destination port

Security Policy Database



Outbound processing



Inbound processing

Internet Key Exchange (IKE)

- The Internet Key Exchange (IKE) is a protocol designed to create both inbound and outbound Security Associations.

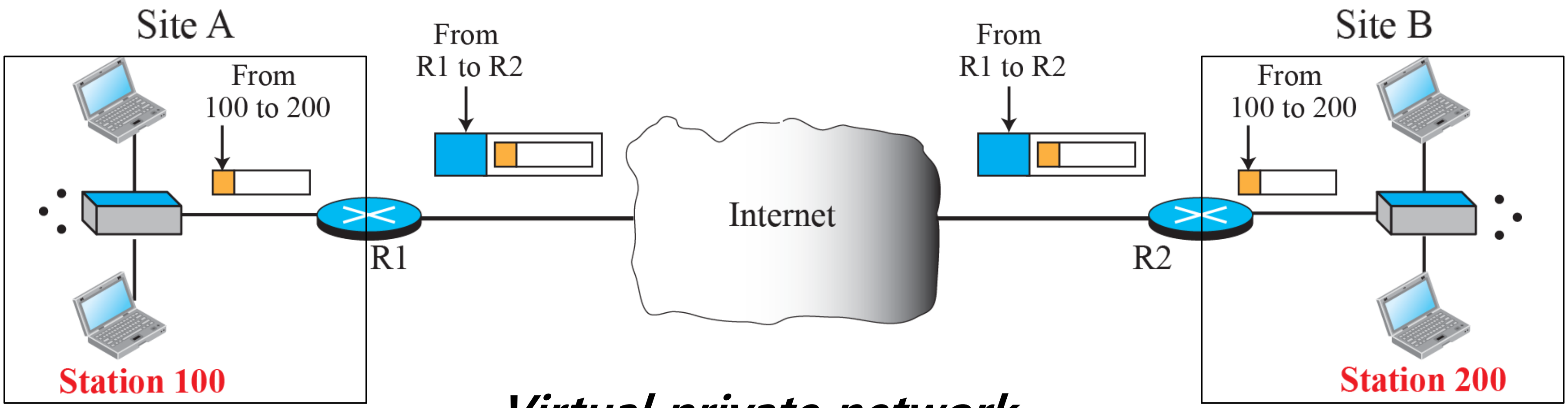
- When a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic.

- If there is no SA, IKE is called to establish one.

Virtual Private Network (VPN)

- One of the applications of IPSec is in virtual private networks.

- A virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and inter-organization communication, but require

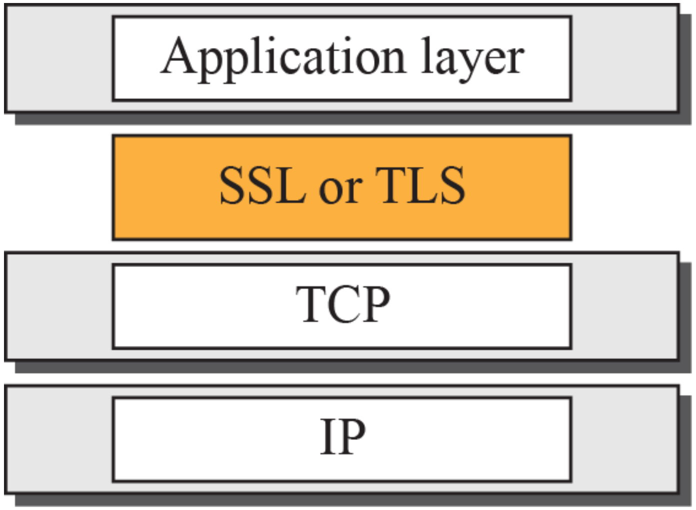


Virtual private network

TRANSPORT-LAYER SECURITY

- Security at the transport layer provides security for the application layer, which uses the services of TCP (or SCTP) as a connection-oriented protocol.

- Two protocols are dominant today for providing security at the transport layer: the Secure Sockets Layer (SSL) protocol and the Transport Layer Security (TLS) protocol.



SSL Architecture

- SSL is designed to provide security and compression services to data generated from the application layer.

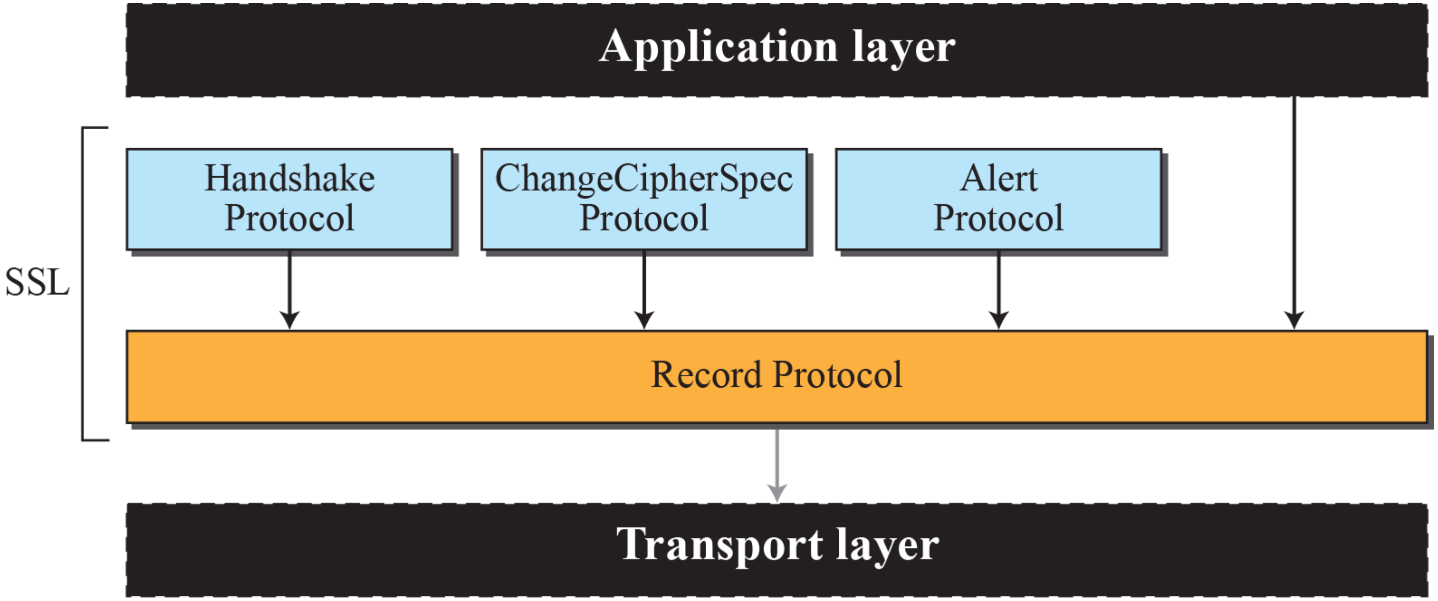
- Typically, SSL can receive data from any application-layer protocol, but usually the protocol is HTTP.

- The data received from the application is compressed (optional), signed, and encrypted.

- The data is then passed to a reliable transport-layer protocol such as TCP.

Four Protocols

- SSL defines four protocols in two layers.



Four SSL protocols

APPLICATION-LAYER SECURITY

- Two protocols providing security services for e-mails: Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME).

- Sending an e-mail is a one-time activity. The nature of this activity is different from SSL or IPSec.

- In those protocols, we assume that the two parties create a session between themselves and exchange data in both directions.

E-mail Security

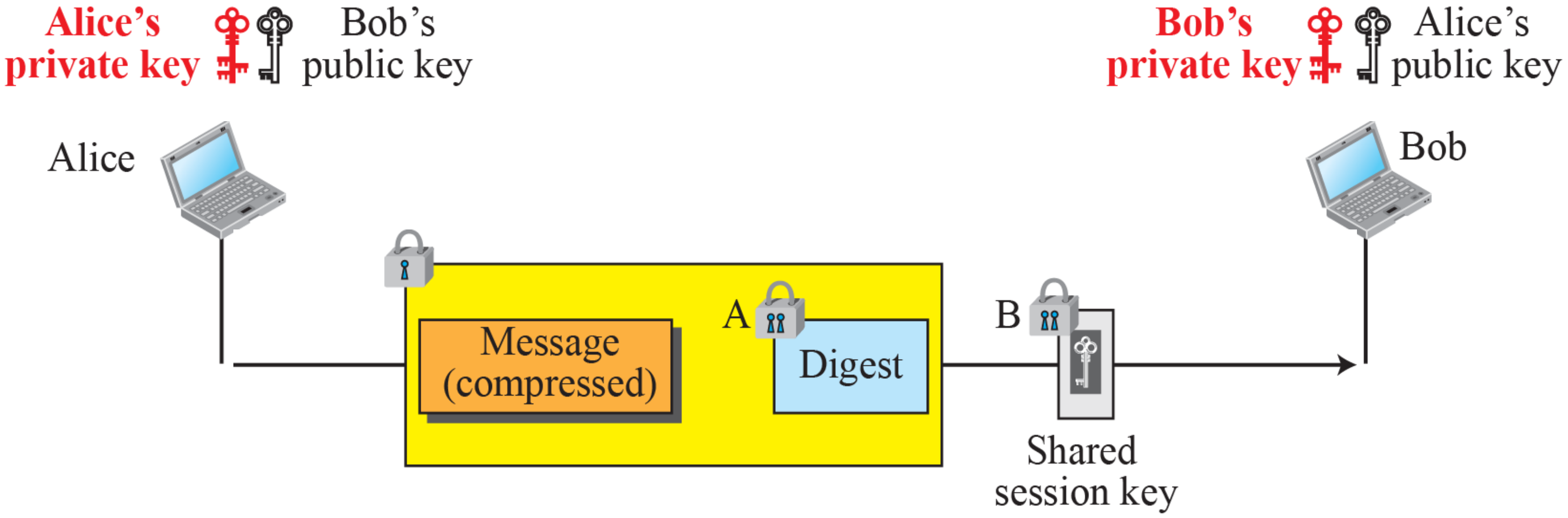
- In e-mail, there is no session. Alice and Bob cannot create a session.

- Alice sends a message to Bob; sometime later, Bob reads the message and may or may not send a reply.

Pretty Good Privacy (PGP)

- PGP was invented by Phil Zimmermann to provide e-mail with privacy, integrity, and authentication.

- PGP can be used to create secure e-mail messages.

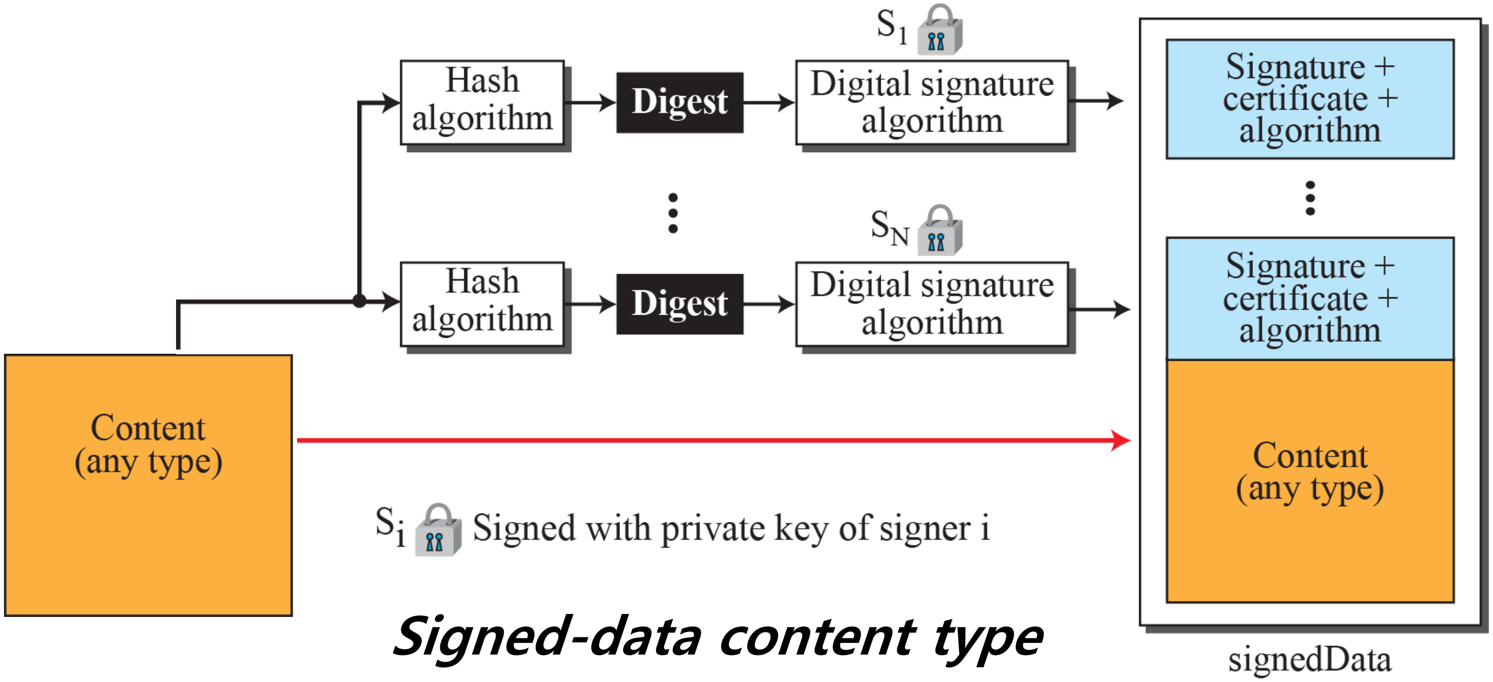


A confidential message

S/MIME

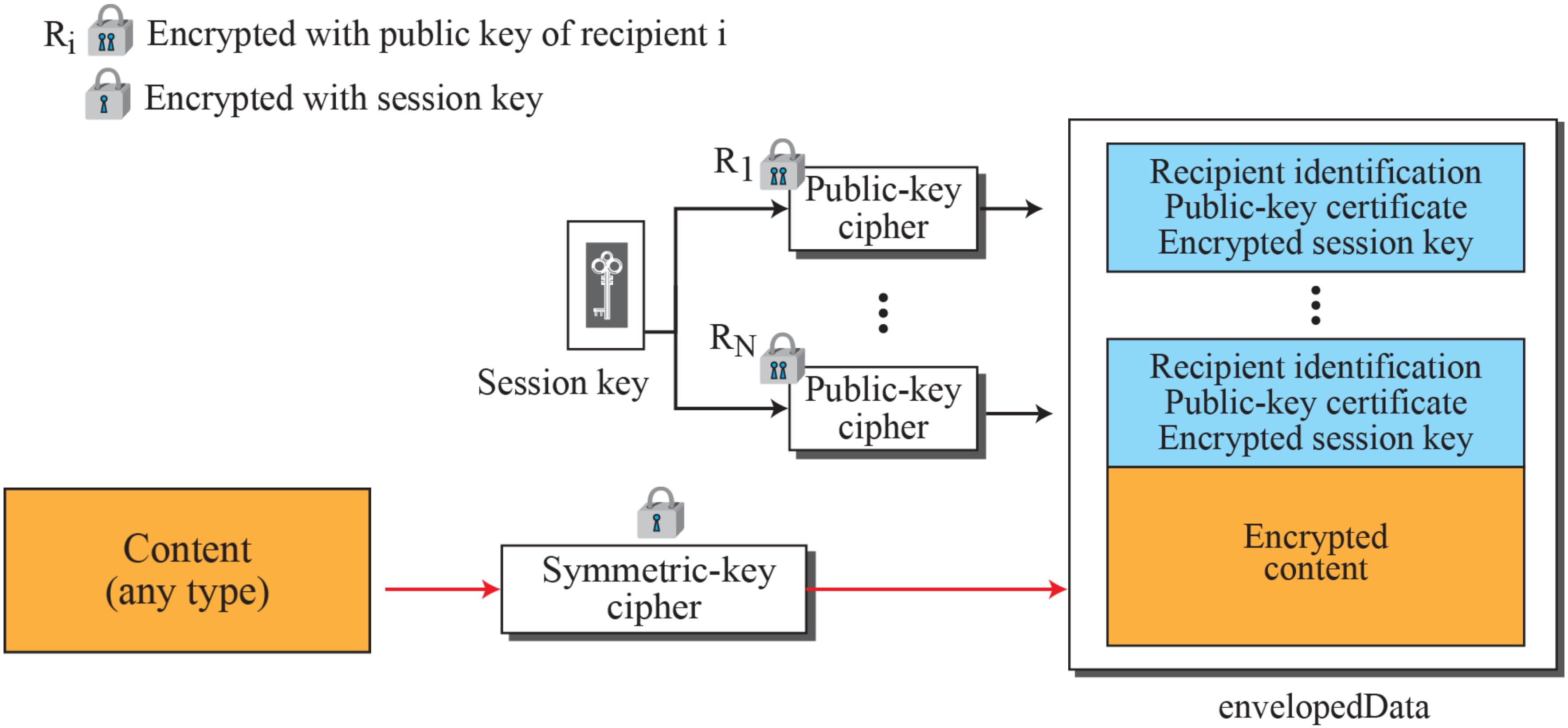
- Another security service designed for electronic mail is Secure/Multipurpose Internet Mail Extension (S/MIME).

- The protocol is an enhancement of the Multipurpose Internet Mail Extension (MIME) protocol.

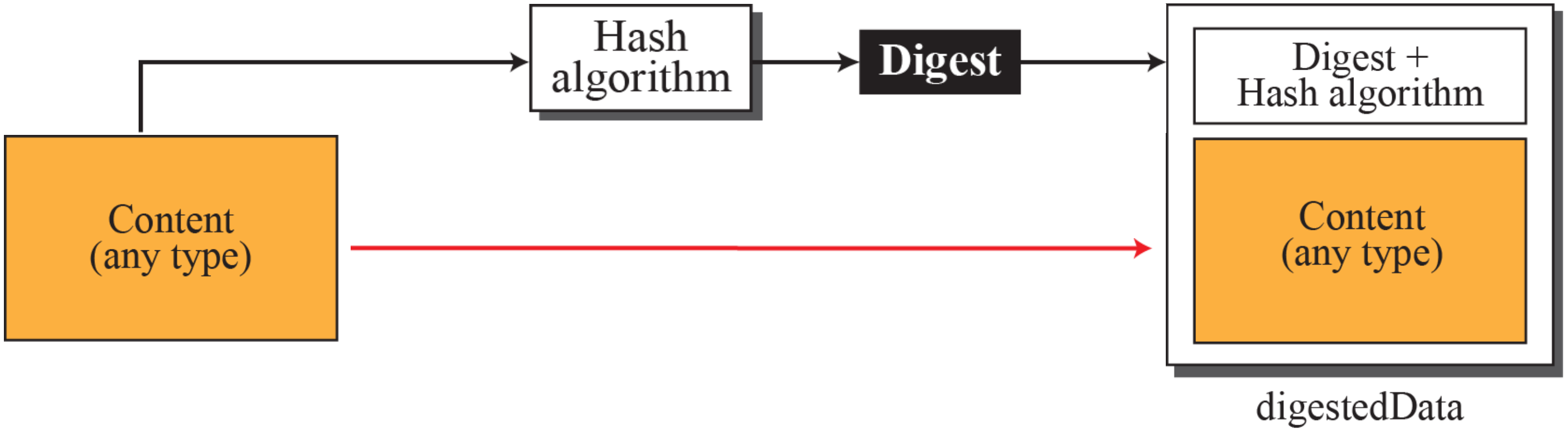


S_1
Hash algorithm
Digest
Digital signature algorithm
S_N
Hash algorithm
Digest
Digital signature algorithm
Signature + certificate + algorithm
Signature + certificate + algorithm
Content (any type)
Content (any type)
S_i Signed with private key of signer i
signedData

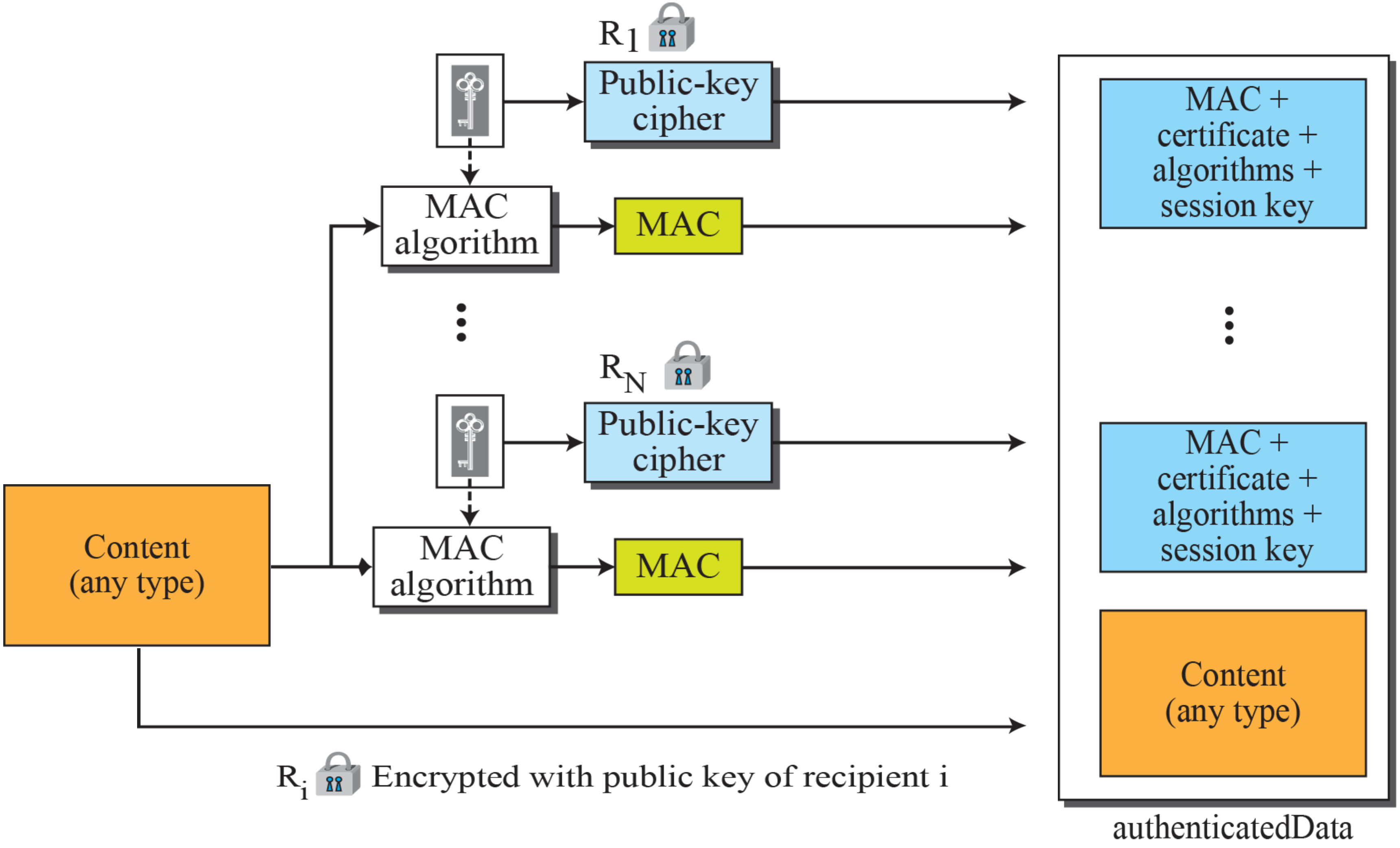
Signed-data content type



Enveloped-data content type



Digested-data content type


R1
Public-key cipher
MAC algorithm
MAC
MAC + certificate + algorithms + session key
RN
Public-key cipher
MAC algorithm
MAC
MAC + certificate + algorithms + session key
Content (any type)
Content (any type)
Ri Encrypted with public key of recipient i
authenticatedData

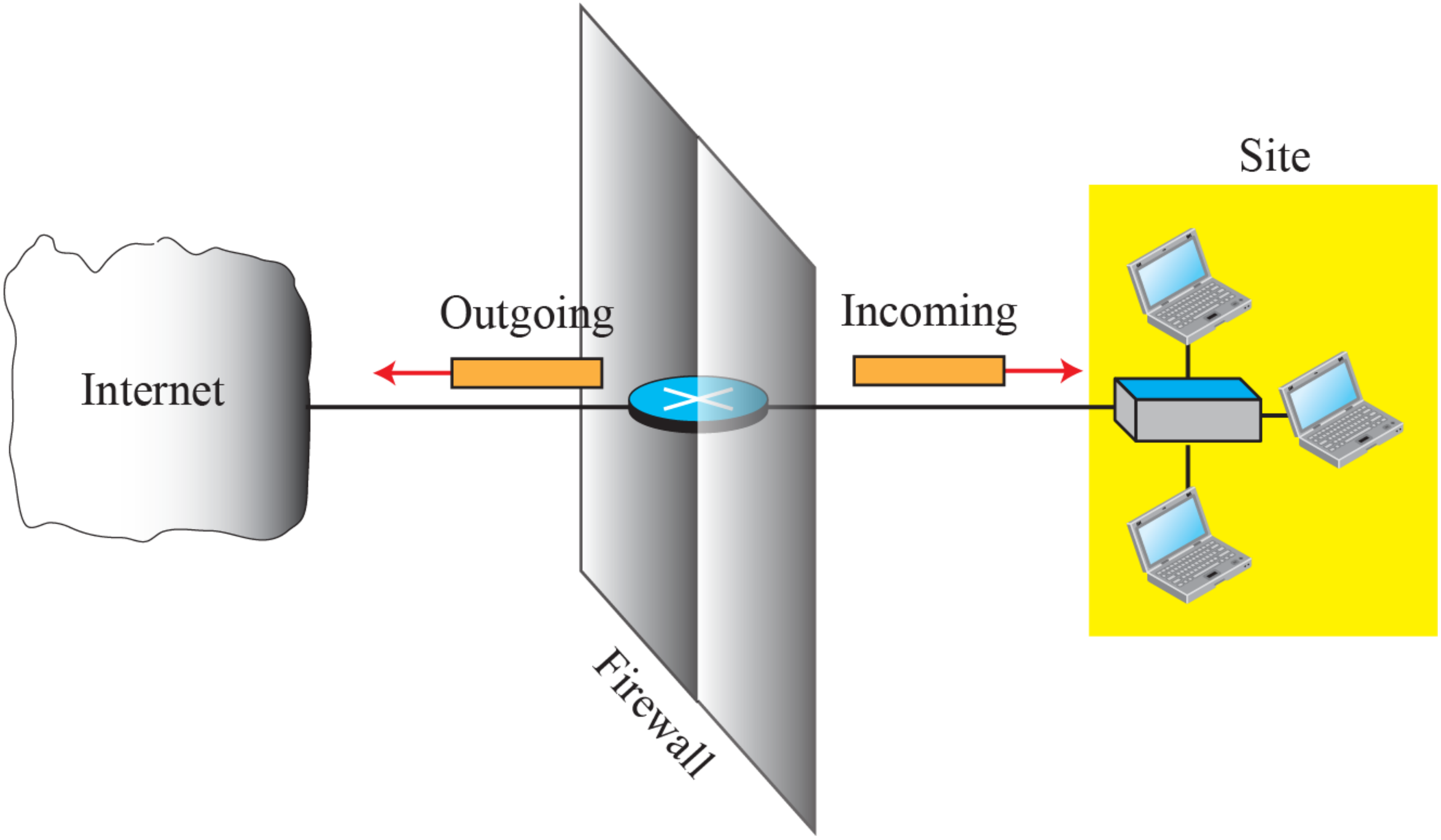
Authenticated-data content type

FIREWALLS

- All previous security measures cannot prevent Eve from sending a harmful message to a system.

- To control access to a system we need firewalls. A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet.

- It is designed to forward some packets and filter (not forward) others.



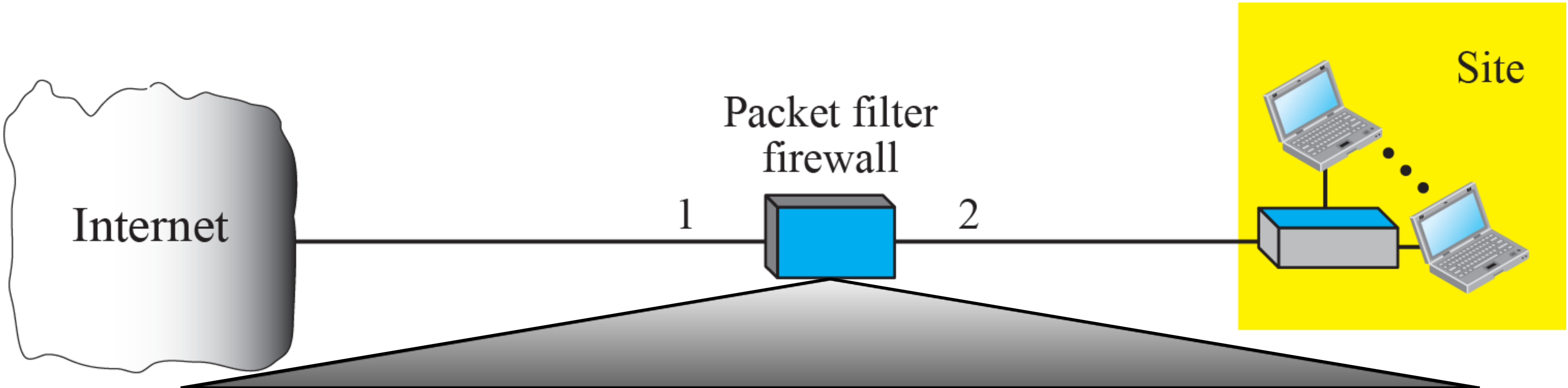
Firewall

Packet-Filter Firewalls

- A firewall can be used as a packet filter.

- It can forward or block packets based on the information in the network-layer and transport-layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP).

- A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded).



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

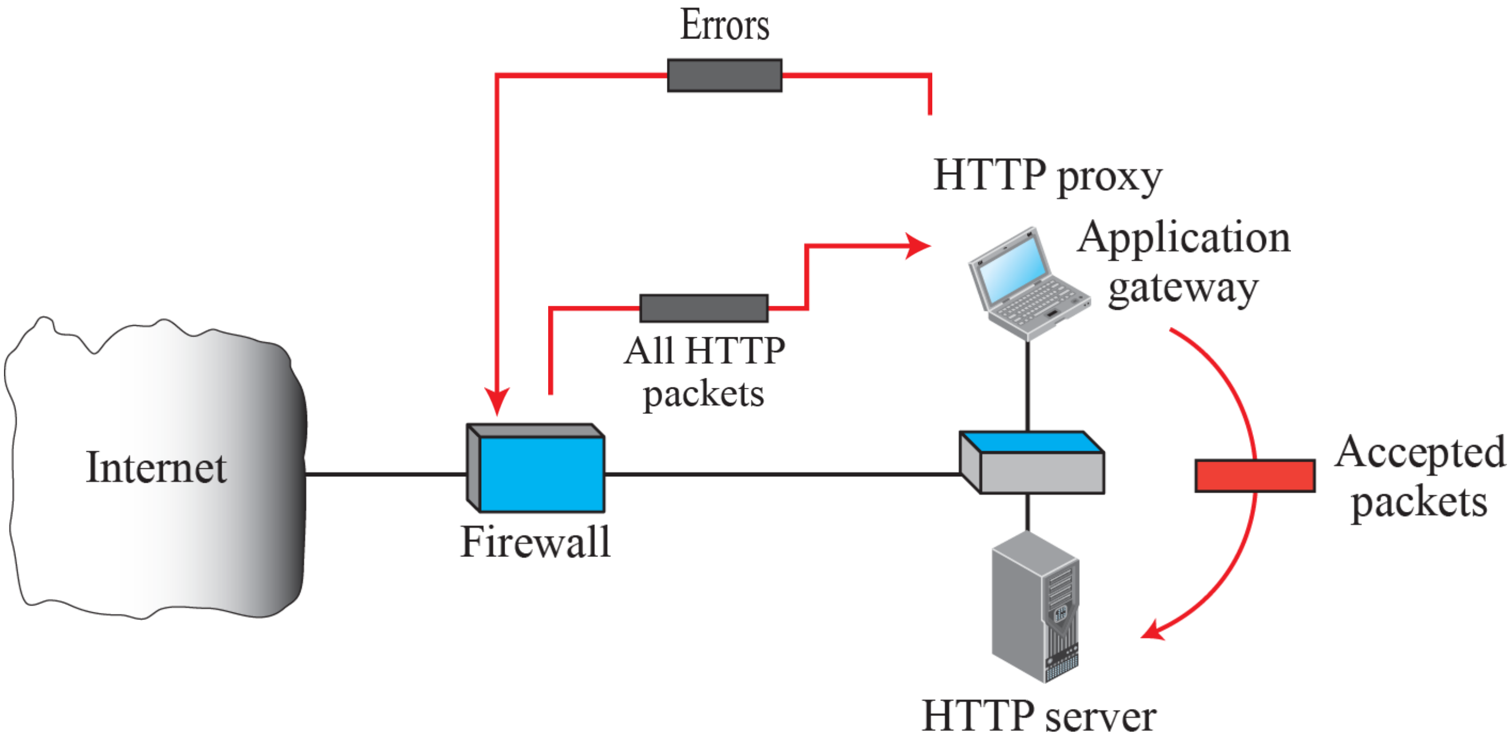
Packet-filter firewall

Proxy Firewall

- The packet-filter firewall is based on the information available in the network layer and transport layer headers (IP and TCP/UDP).

- However, sometimes we need to filter a message based on the information available in the message itself (at the application layer).

- As an example, assume that an organization wants to implement the following



Proxy firewall