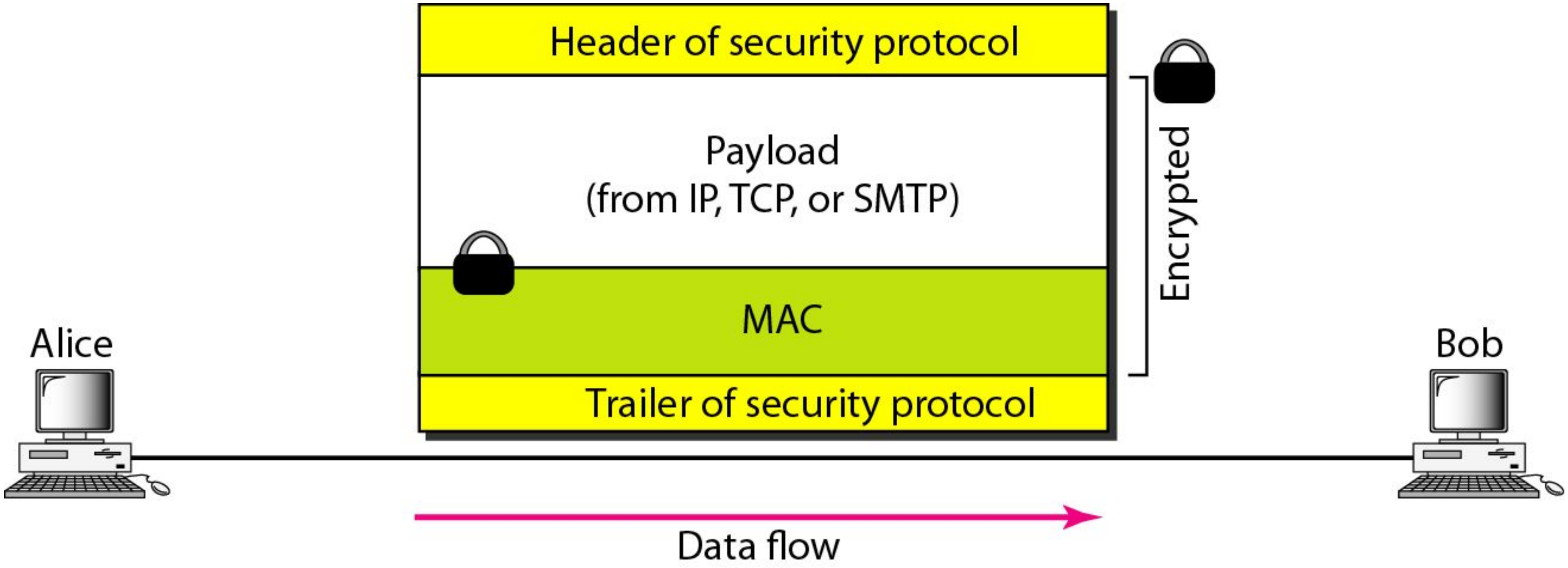
Security in the Internet: IPSec, SSL/TLS, PGP, VPN, and Firewalls

Common structure of three security protocols



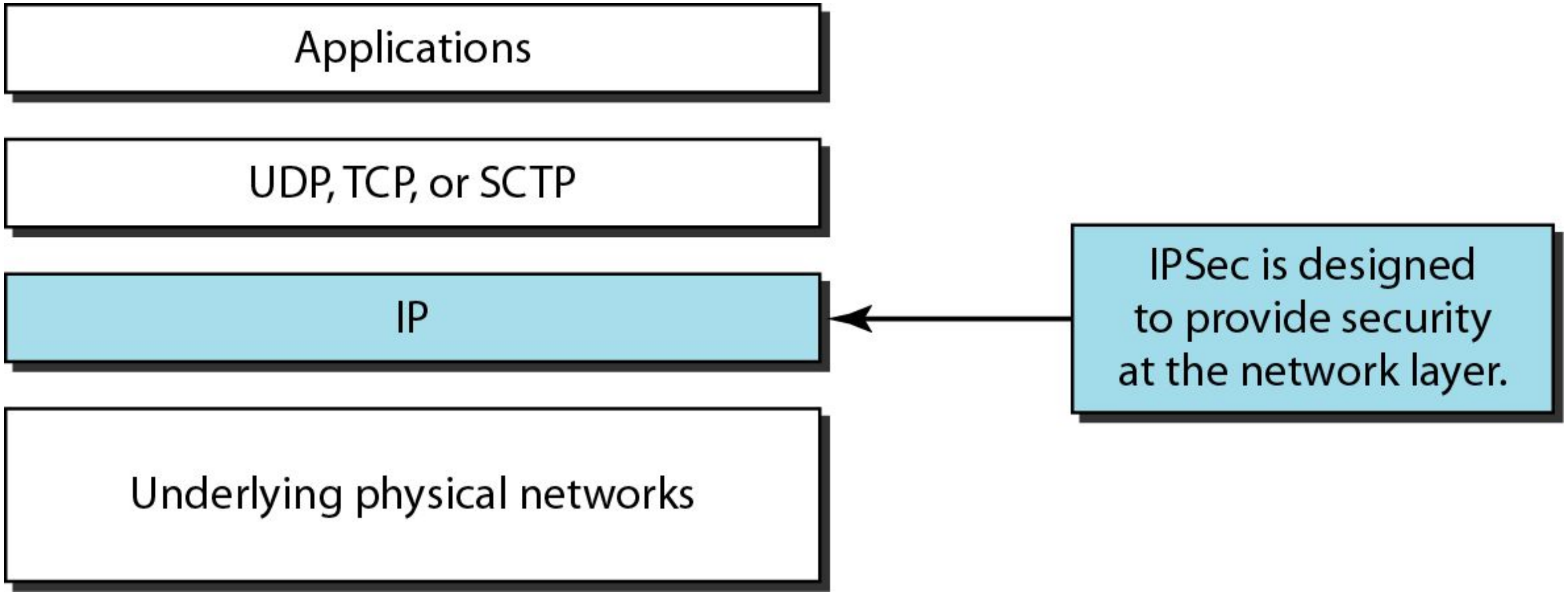
IPSecurity (IPSec)

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

Topics discussed in this section:

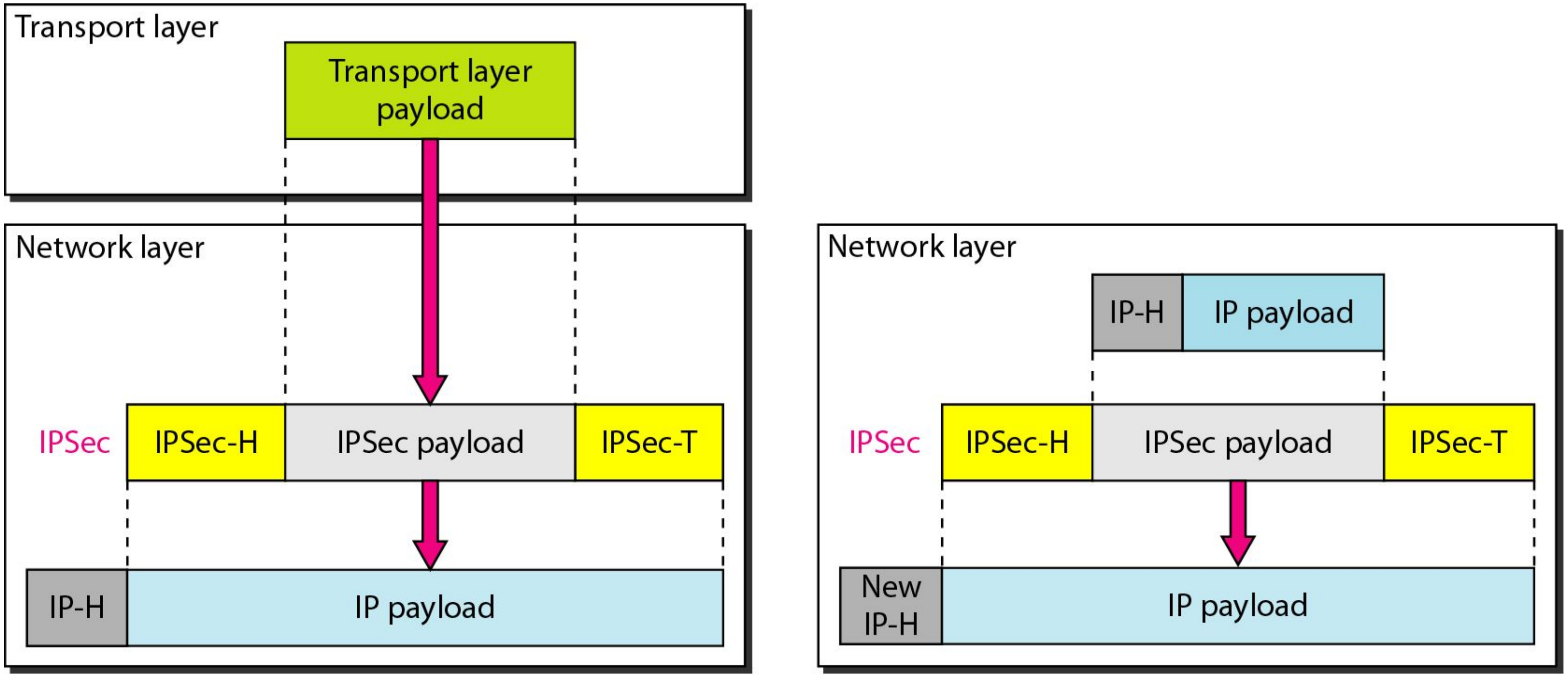
- Two Modes
- Two Security Protocols
- Security Association
- Internet Key Exchange (IKE)
- Virtual Private Network

TCP/IP protocol suite and IPSec


Applications
UDP, TCP, or SCTP
IP
Underlying physical networks
IPSec is designed to provide security at the network layer.

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

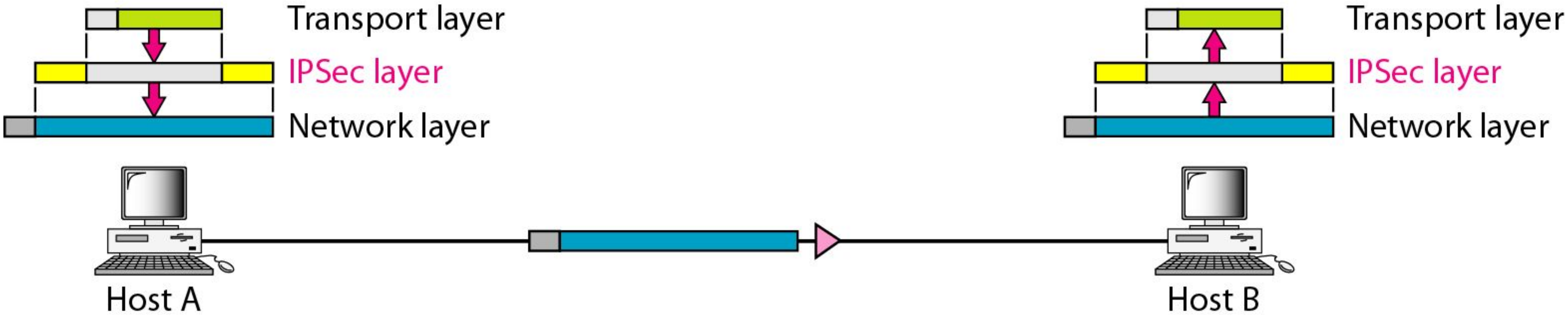
Transport mode and tunnel modes of IPSec protocol



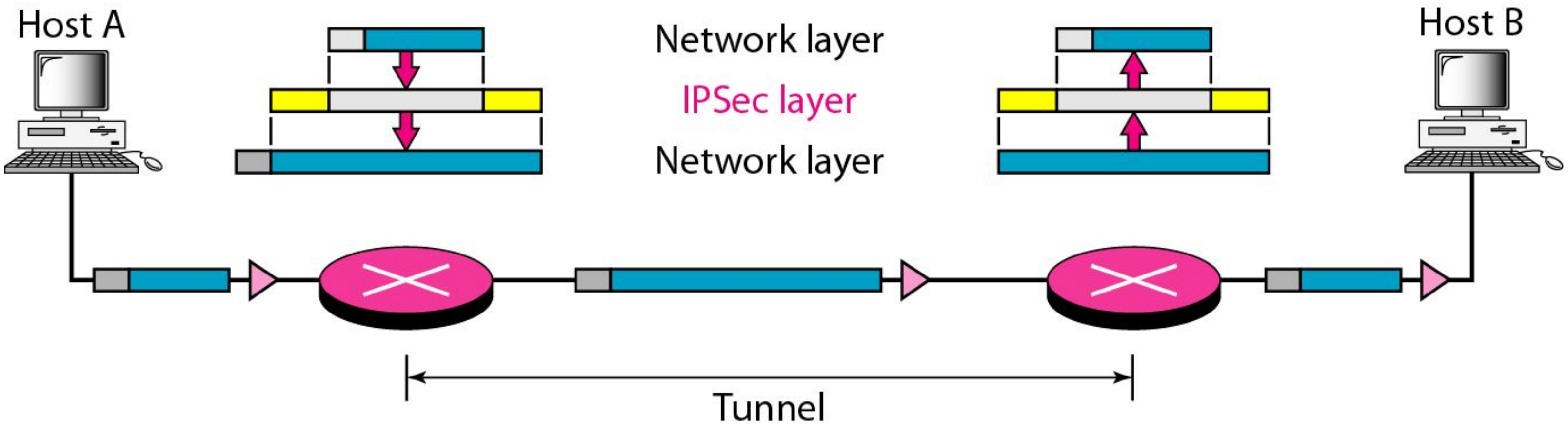
a. Transport mode

b. Tunnel mode

Transport mode in action

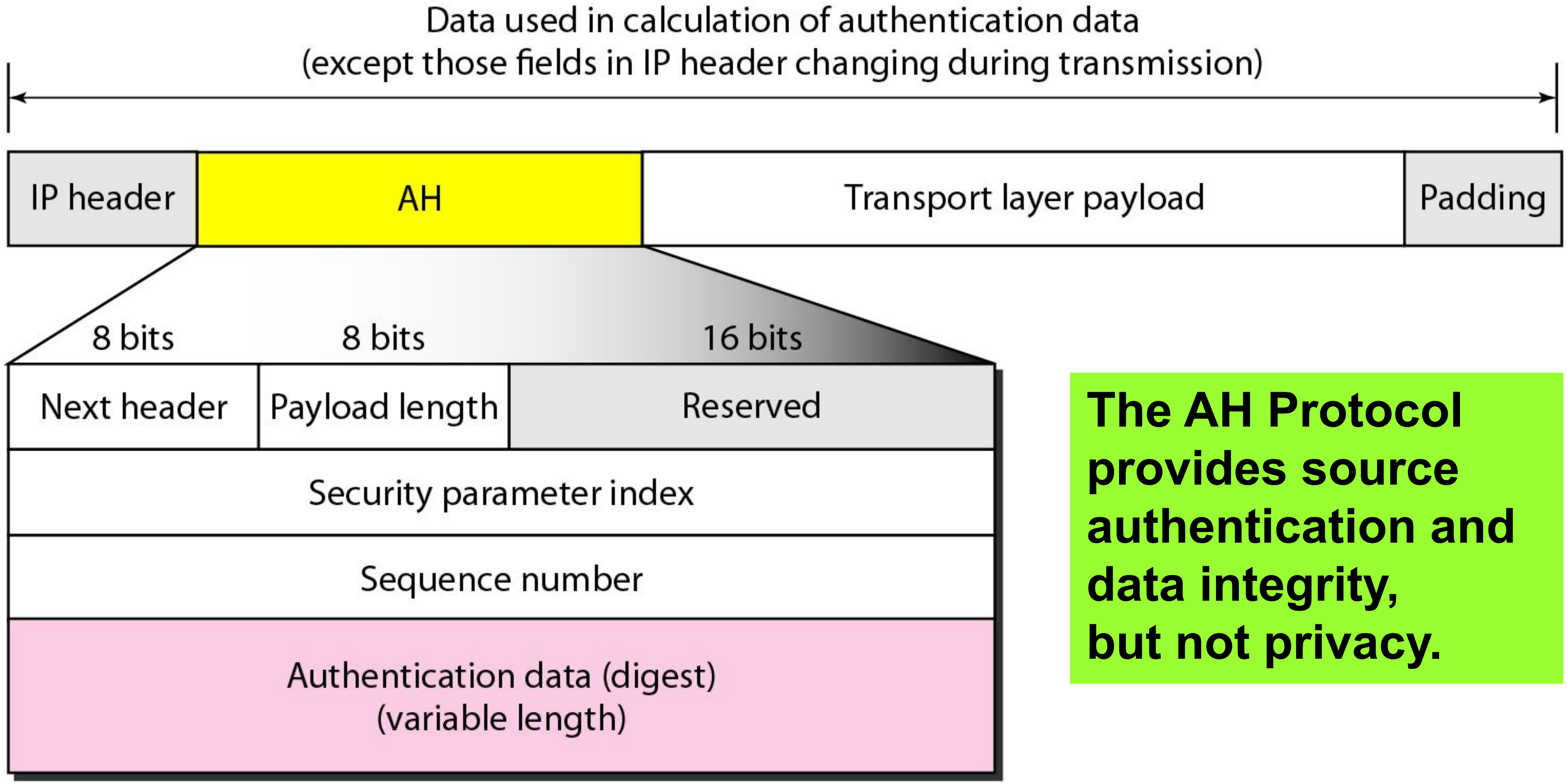


Tunnel mode in action



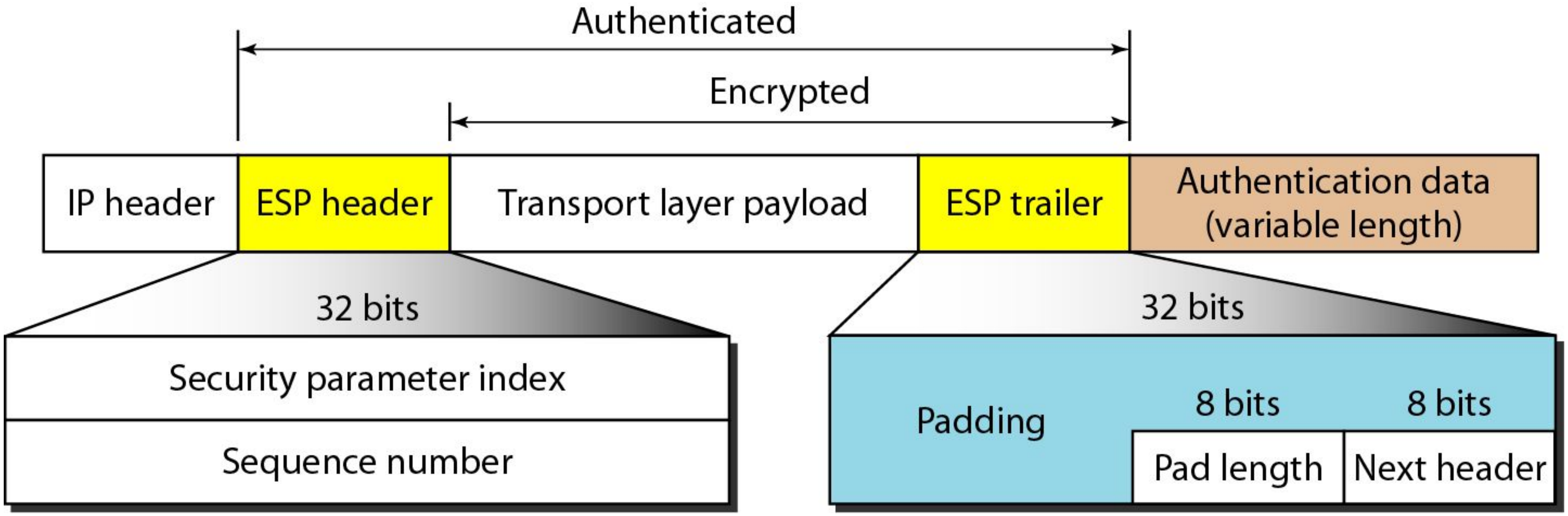
IPSec in tunnel mode protects the original IP header.

Authentication Header (AH) Protocol



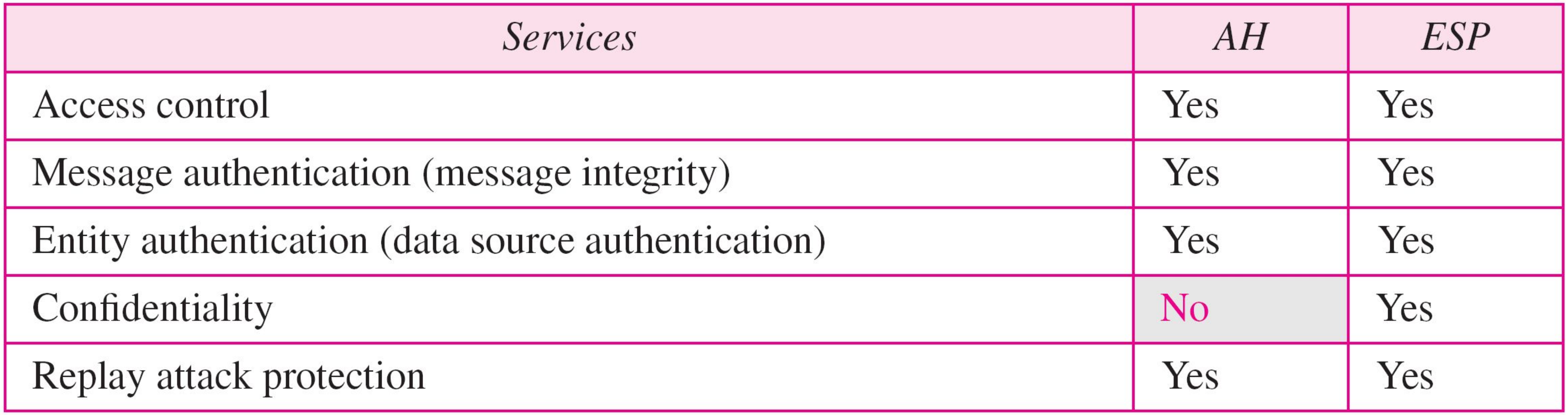
The AH Protocol provides source authentication and data integrity, but not privacy.

Encapsulating Security Payload (ESP) Protocol



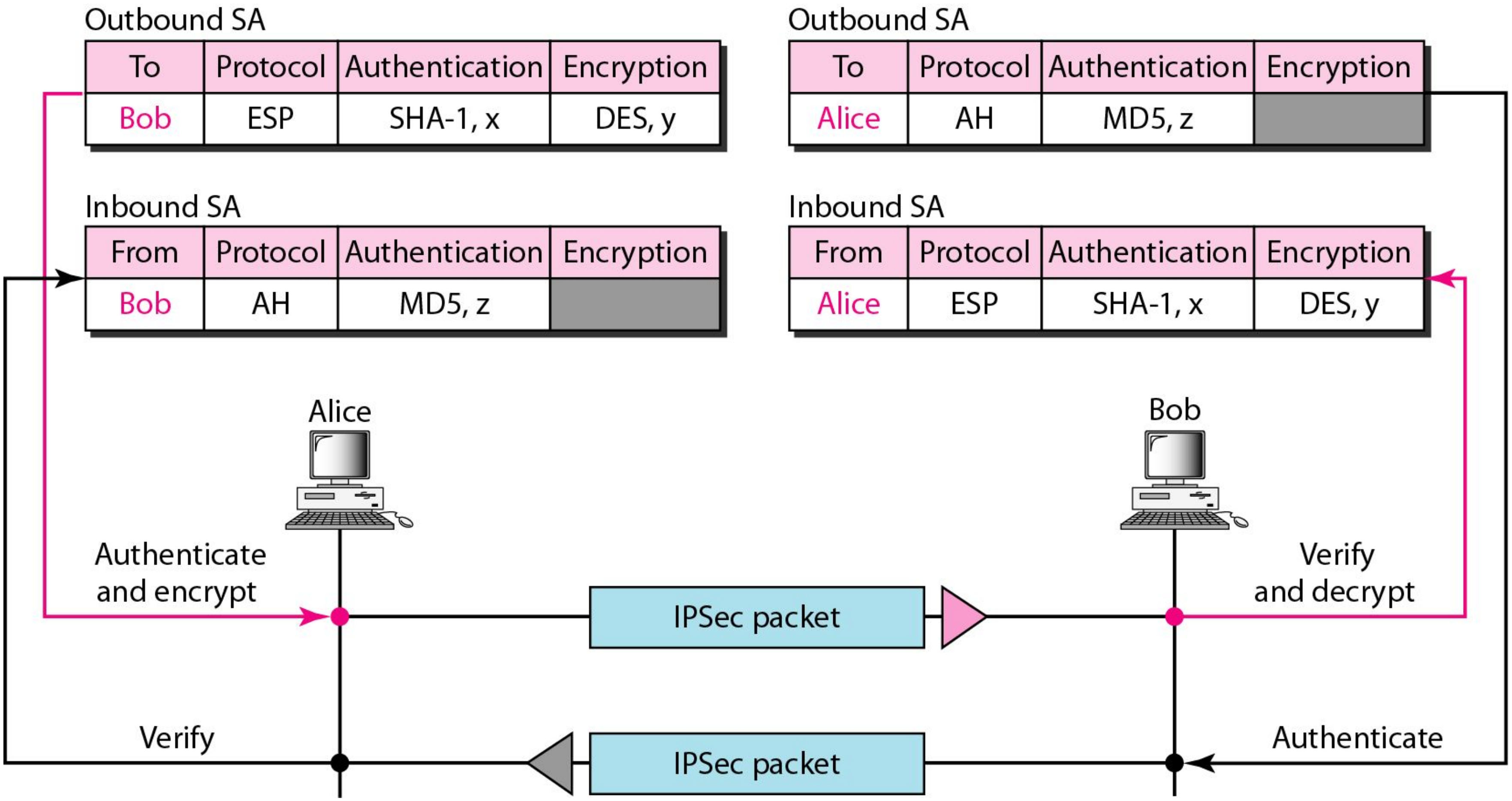
ESP provides source authentication, data integrity, and privacy.

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

Simple inbound and outbound security associations



Outbound SA

To	Protocol	Authentication	Encryption
Bob	ESP	SHA-1, x	DES, y

Inbound SA

From	Protocol	Authentication	Encryption
Bob	AH	MD5, z	▨

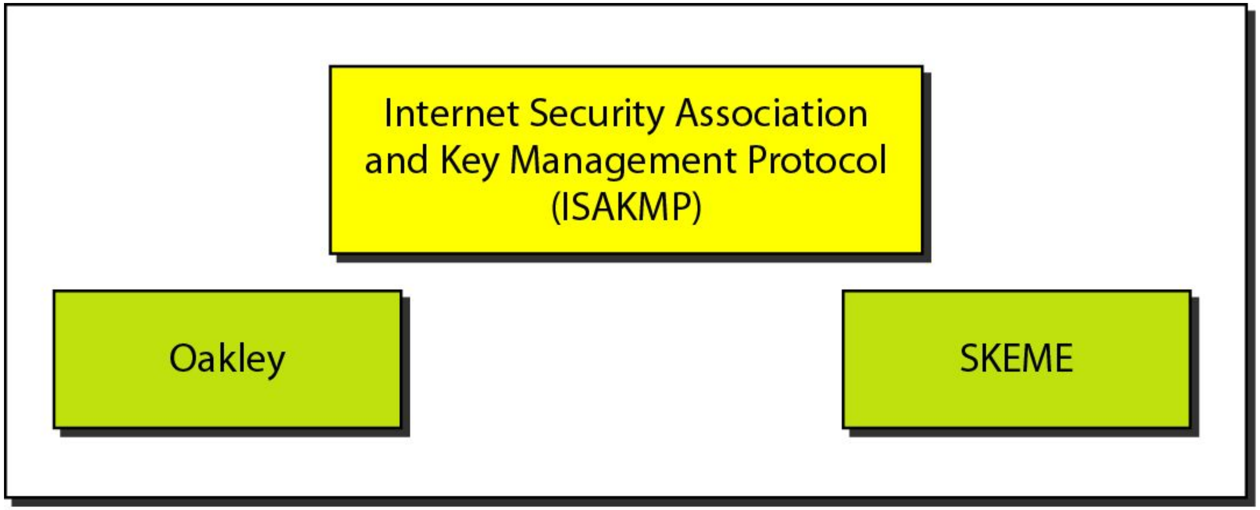
Outbound SA

To	Protocol	Authentication	Encryption
Alice	AH	MD5, z	▨

Inbound SA

From	Protocol	Authentication	Encryption
Alice	ESP	SHA-1, x	DES, y

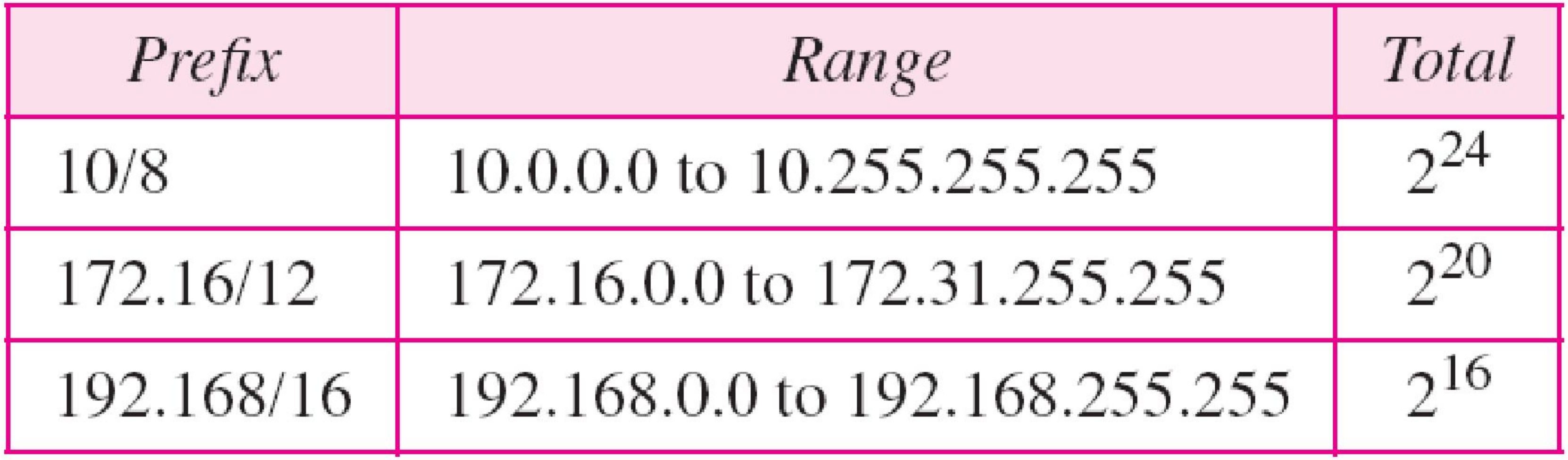
IKE components


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

Internet Key Exchange (IKE)

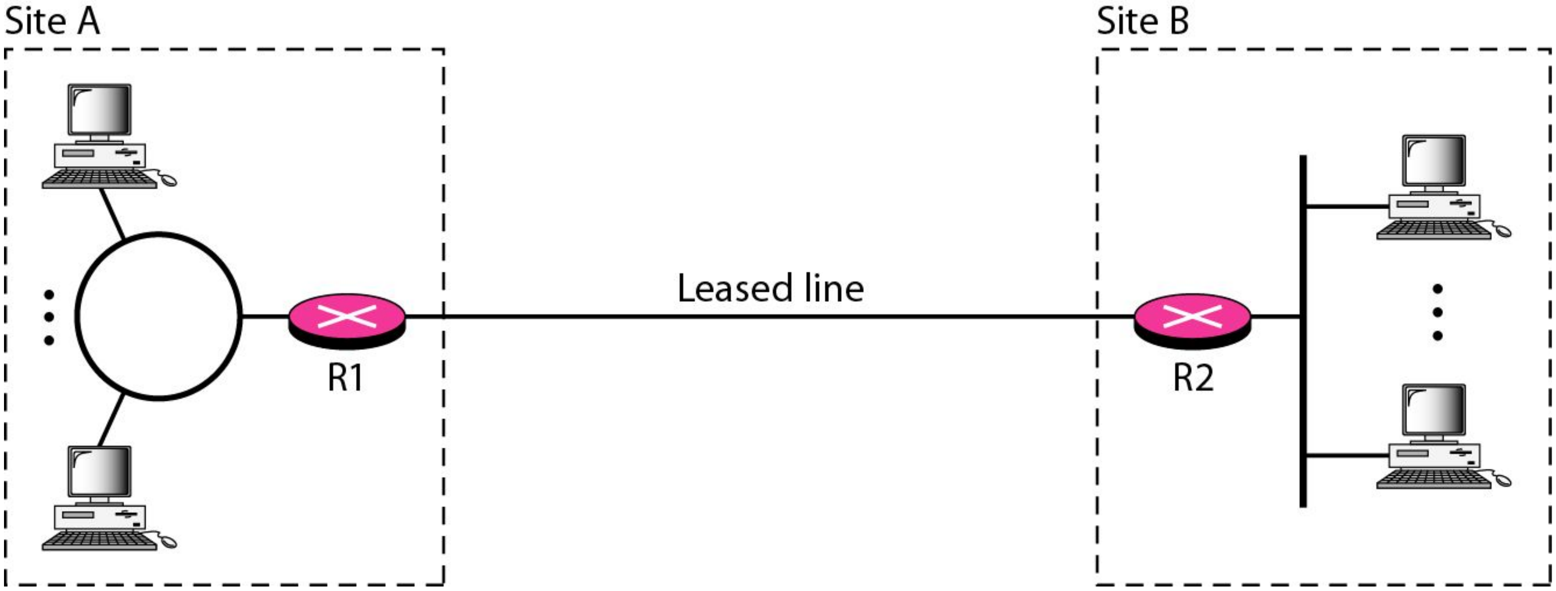
IKE creates SAs for IPSec.

Addresses for private networks

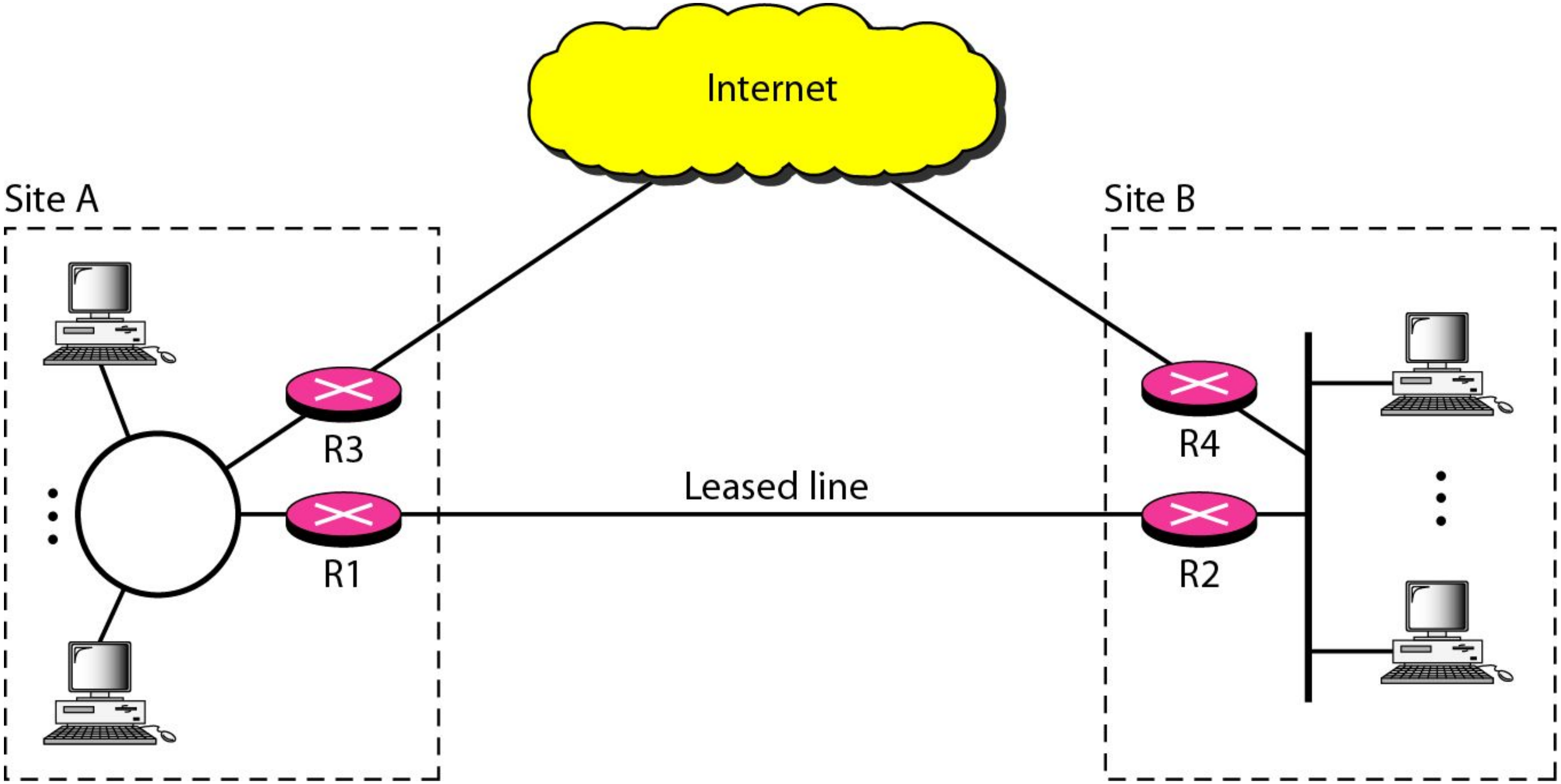


Prefix	*Range*	*Total*
10/8	10.0.0.0 to 10.255.255.255	2^{24}
172.16/12	172.16.0.0 to 172.31.255.255	2^{20}
192.168/16	192.168.0.0 to 192.168.255.255	2^{16}

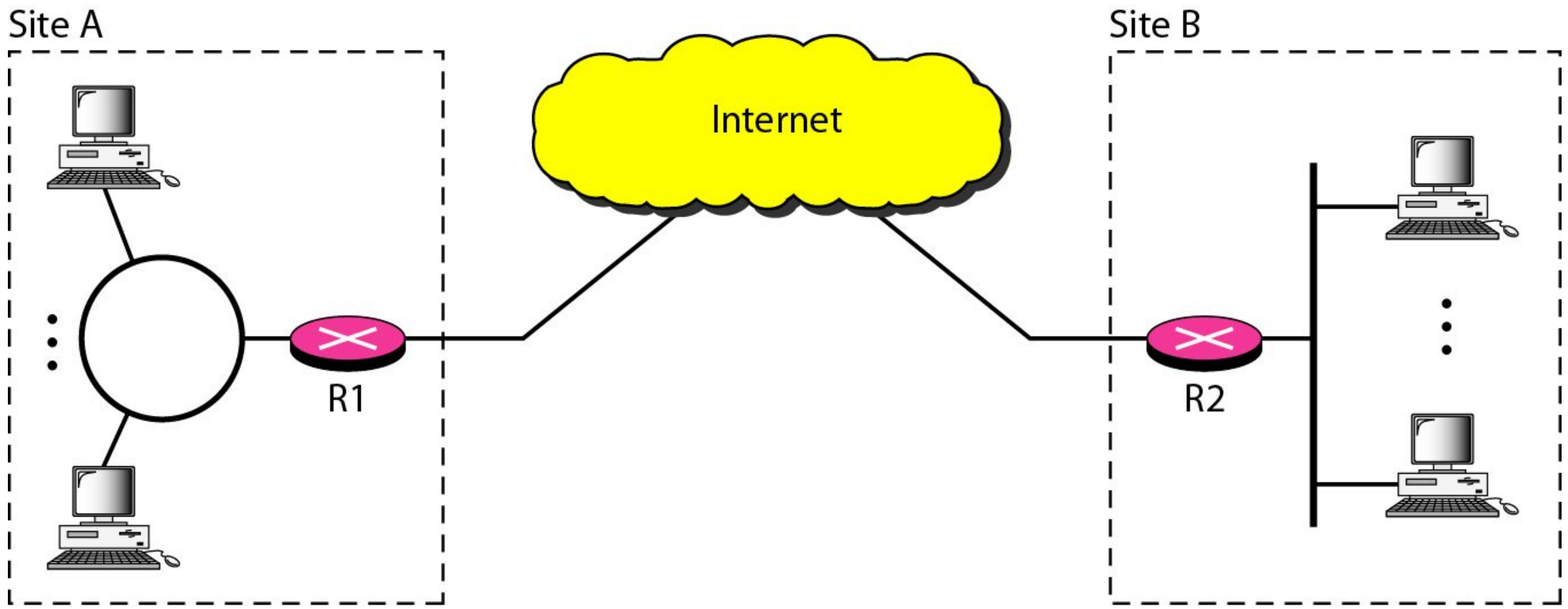
Private network



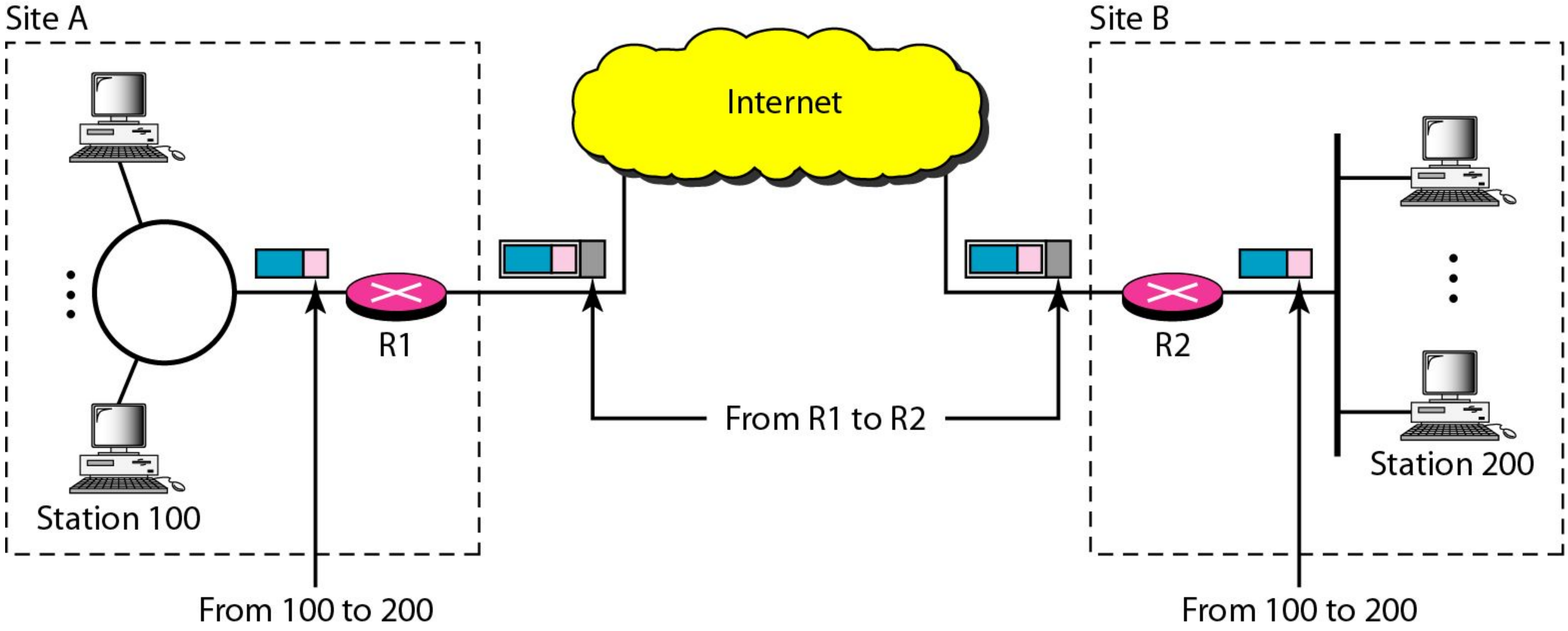
Hybrid network



Virtual private network



Addressing in a VPN



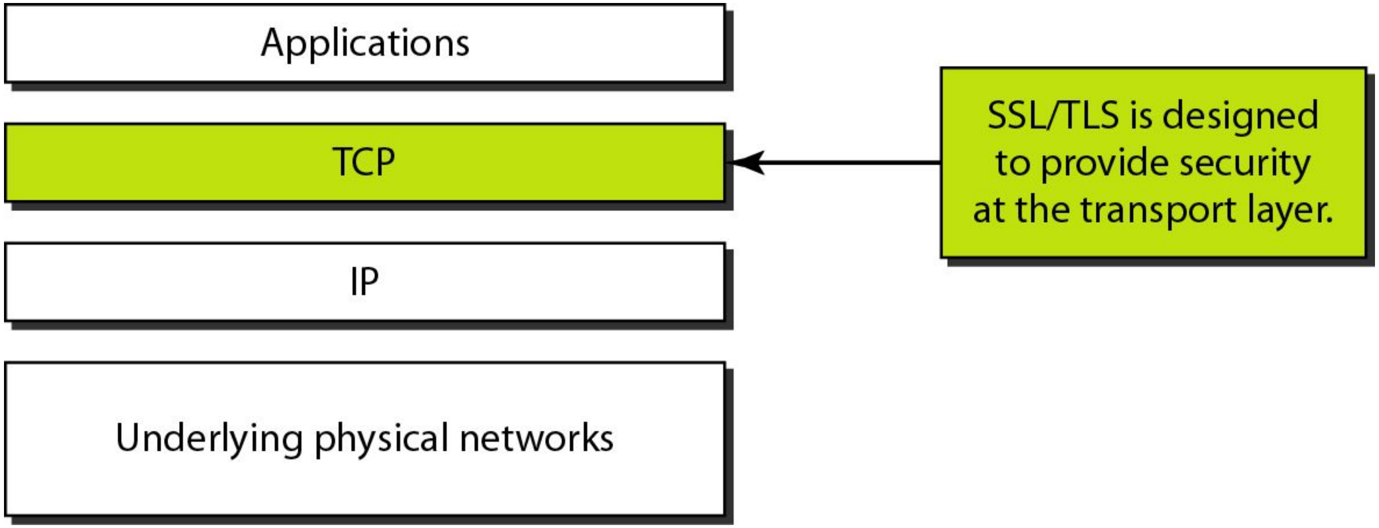
SSL/TLS

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. The latter is actually an IETF version of the former.

Topics discussed in this section:

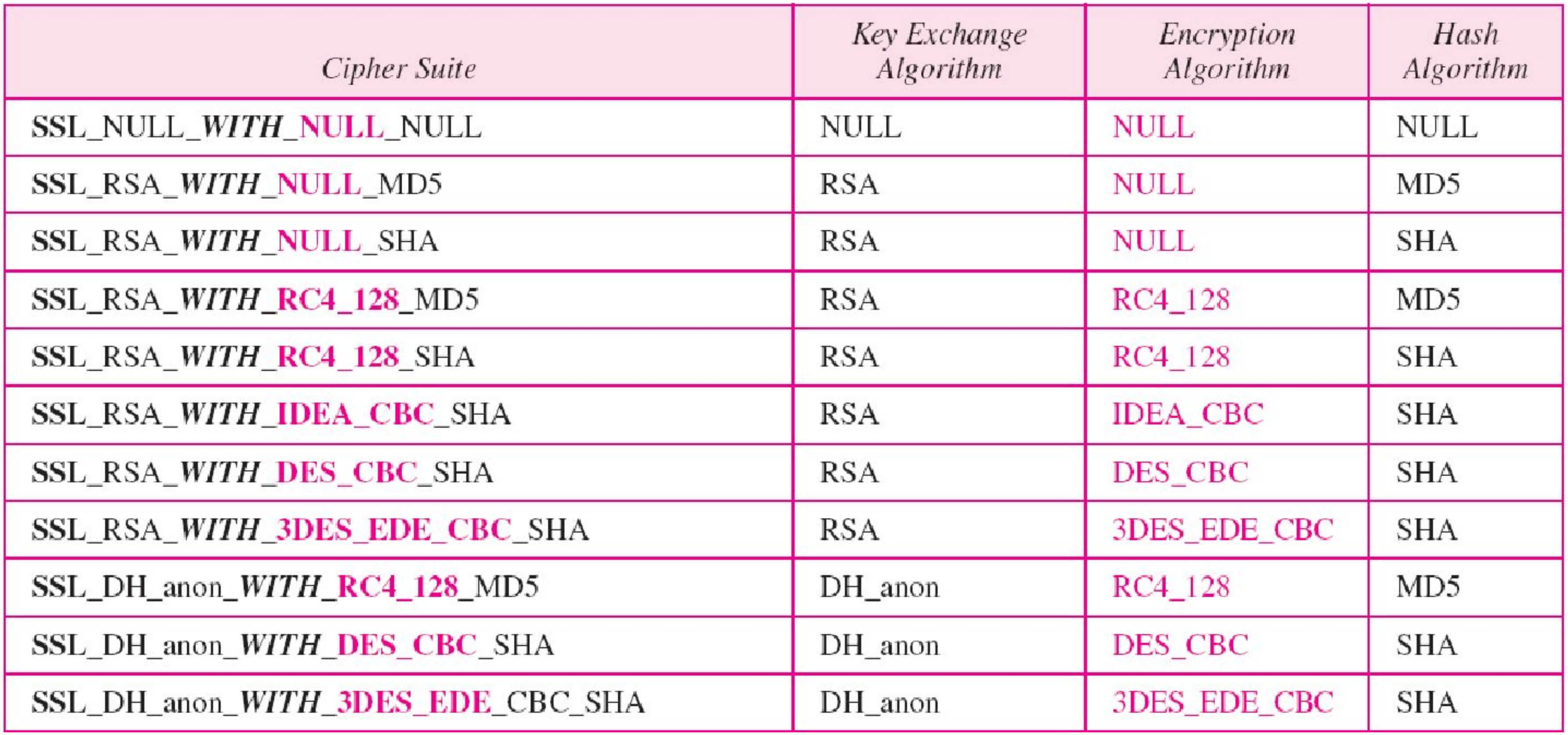
- SSL Services
- Security Parameters
- Sessions and Connections
- Four Protocols
- Transport Layer Security

Location of SSL and TLS in the Internet model



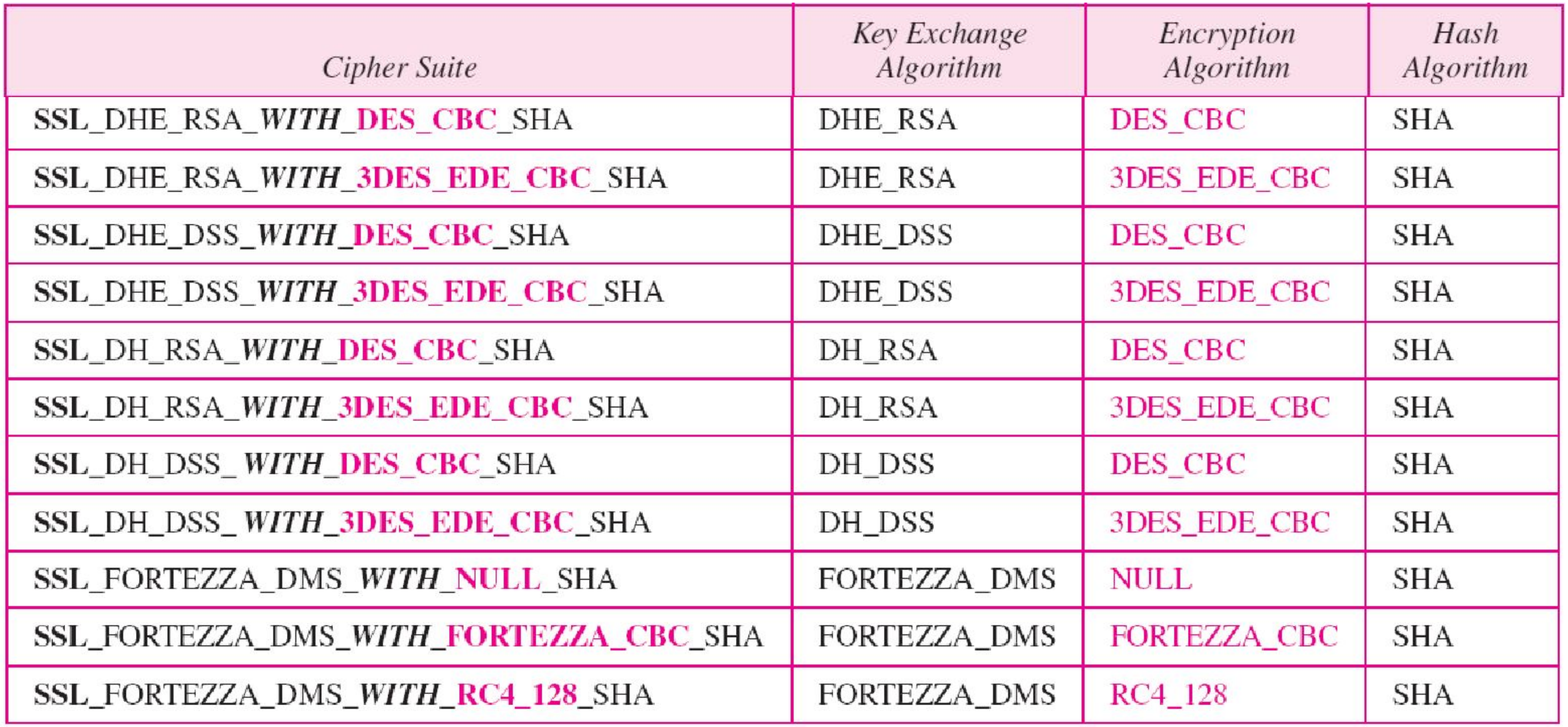
SSL/TLS is designed to provide security at the transport layer.

SSL cipher suite list



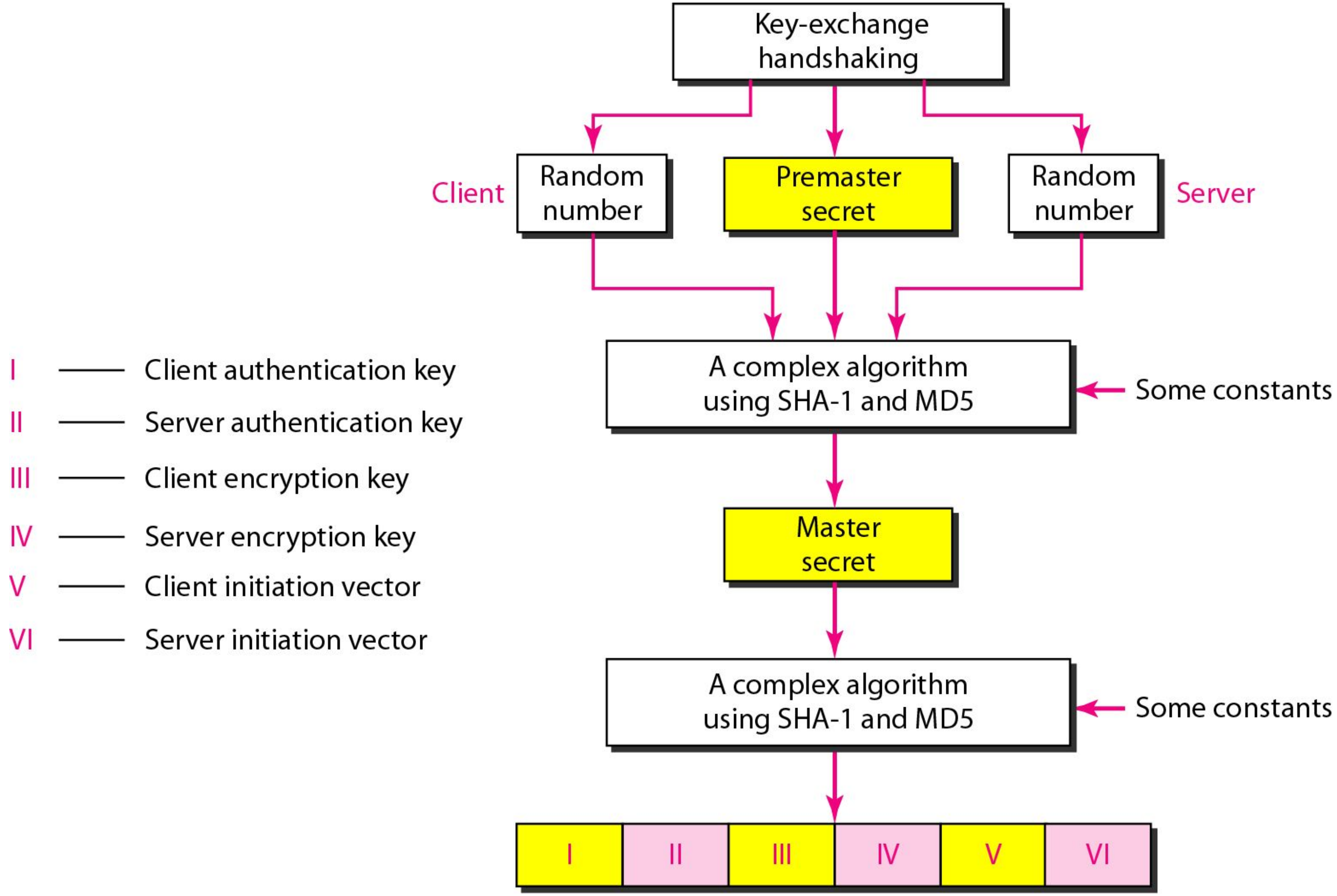
Cipher Suite	*Key Exchange Algorithm*	*Encryption Algorithm*	*Hash Algorithm*
SSL_NULL_***WITH***_**NULL**_NULL	NULL	NULL	NULL
SSL_RSA_***WITH***_**NULL**_MD5	RSA	NULL	MD5
SSL_RSA_***WITH***_**NULL**_SHA	RSA	NULL	SHA
SSL_RSA_***WITH***_**RC4_128**_MD5	RSA	RC4_128	MD5
SSL_RSA_***WITH***_**RC4_128**_SHA	RSA	RC4_128	SHA
SSL_RSA_***WITH***_**IDEA_CBC**_SHA	RSA	IDEA_CBC	SHA
SSL_RSA_***WITH***_**DES_CBC**_SHA	RSA	DES_CBC	SHA
SSL_RSA_***WITH***_**3DES_EDE_CBC**_SHA	RSA	3DES_EDE_CBC	SHA
SSL_DH_anon_***WITH***_**RC4_128**_MD5	DH_anon	RC4_128	MD5
SSL_DH_anon_***WITH***_**DES_CBC**_SHA	DH_anon	DES_CBC	SHA
SSL_DH_anon_***WITH***_**3DES_EDE**_CBC_SHA	DH_anon	3DES_EDE_CBC	SHA

SSL cipher suite list (continued)



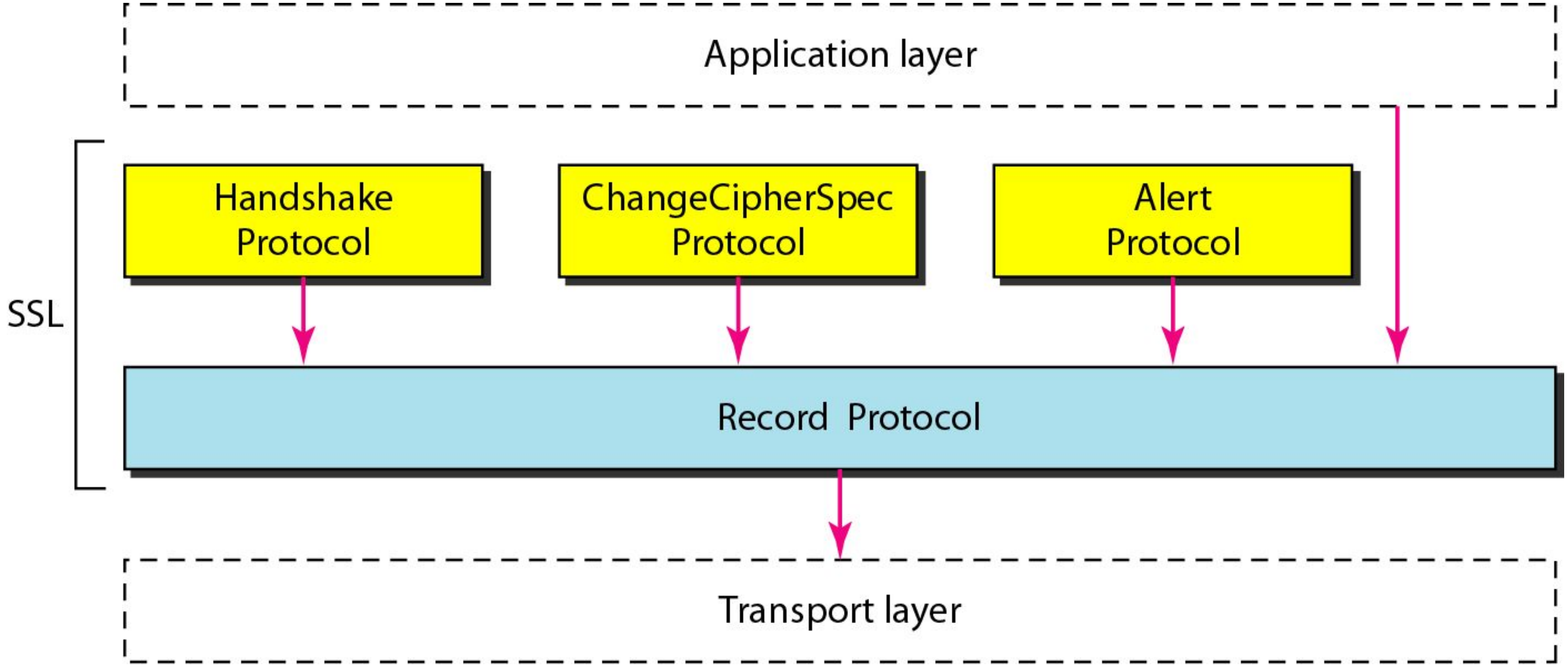
Cipher Suite	Key Exchange Algorithm	Encryption Algorithm	Hash Algorithm
SSL_DHE_RSA_*WITH*_DES_CBC_SHA	DHE_RSA	DES_CBC	SHA
SSL_DHE_RSA_*WITH*_3DES_EDE_CBC_SHA	DHE_RSA	3DES_EDE_CBC	SHA
SSL_DHE_DSS_*WITH*_DES_CBC_SHA	DHE_DSS	DES_CBC	SHA
SSL_DHE_DSS_*WITH*_3DES_EDE_CBC_SHA	DHE_DSS	3DES_EDE_CBC	SHA
SSL_DH_RSA_*WITH*_DES_CBC_SHA	DH_RSA	DES_CBC	SHA
SSL_DH_RSA_*WITH*_3DES_EDE_CBC_SHA	DH_RSA	3DES_EDE_CBC	SHA
SSL_DH_DSS_ *WITH*_DES_CBC_SHA	DH_DSS	DES_CBC	SHA
SSL_DH_DSS_ *WITH*_3DES_EDE_CBC_SHA	DH_DSS	3DES_EDE_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_NULL_SHA	FORTEZZA_DMS	NULL	SHA
SSL_FORTEZZA_DMS_*WITH*_FORTEZZA_CBC_SHA	FORTEZZA_DMS	FORTEZZA_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_RC4_128_SHA	FORTEZZA_DMS	RC4_128	SHA

Creation of cryptographic secrets in SSL

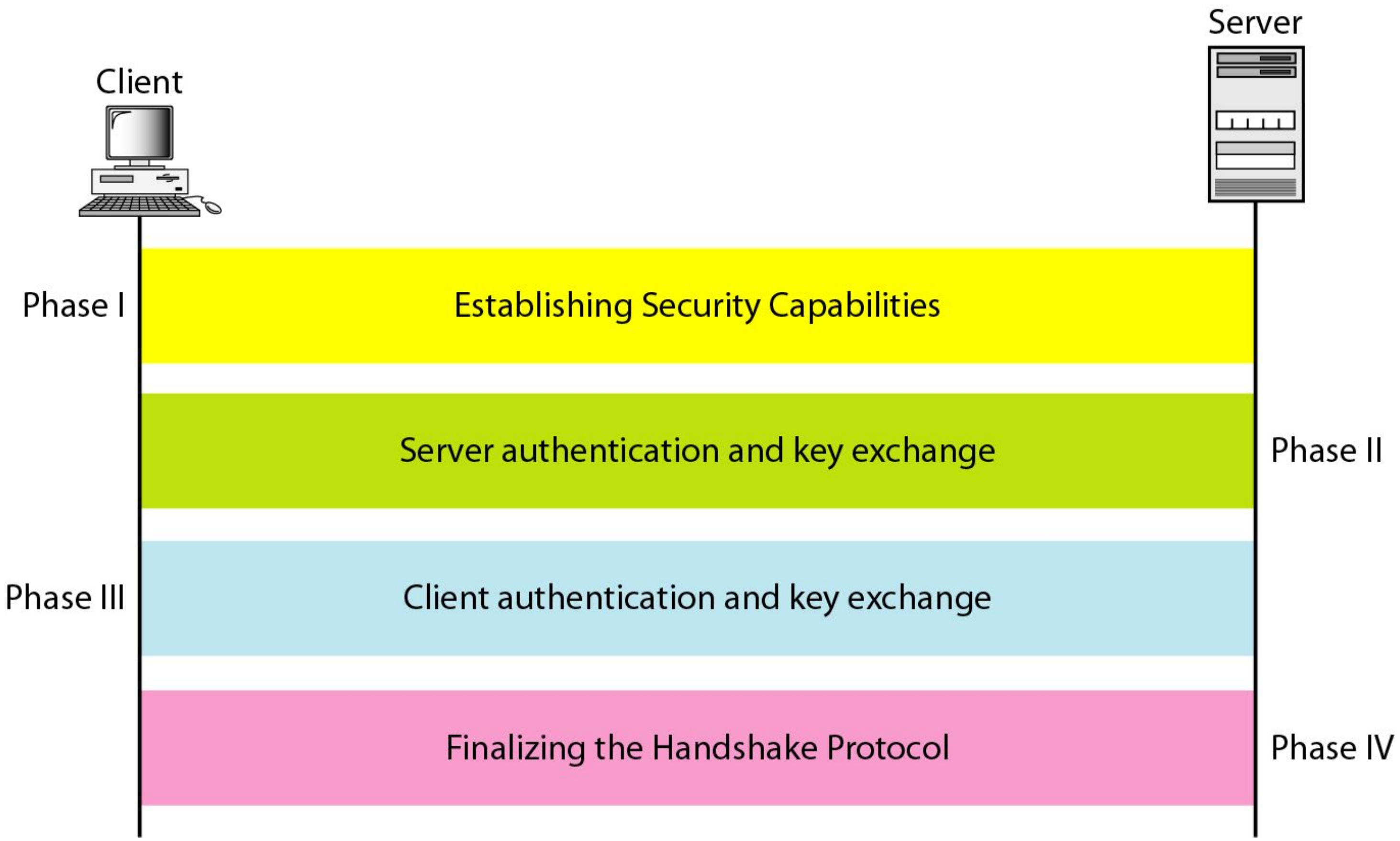


I	Client authentication key
II	Server authentication key
III	Client encryption key
IV	Server encryption key
V	Client initiation vector
VI	Server initiation vector

Four SSL protocols

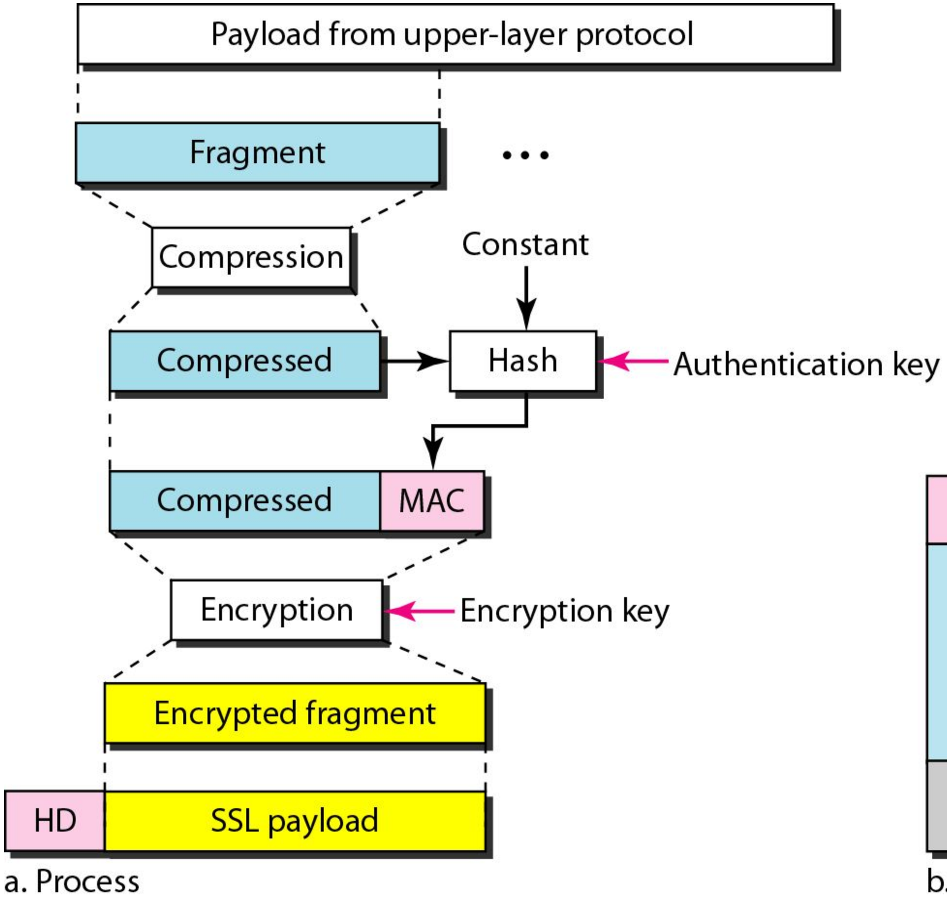


Handshake Protocol

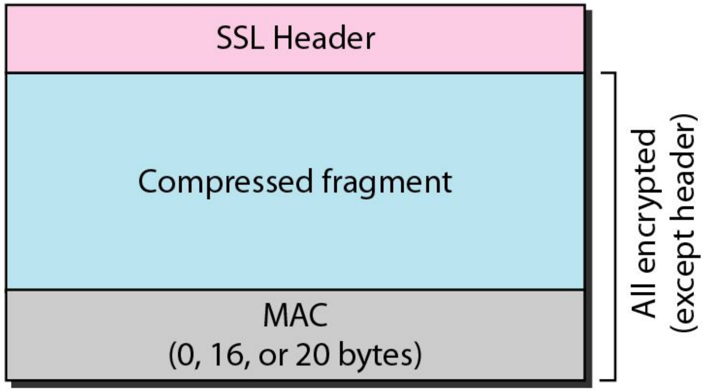


Server
Client
Phase I
Establishing Security Capabilities
Server authentication and key exchange
Phase II
Phase III
Client authentication and key exchange
Finalizing the Handshake Protocol
Phase IV

Processing done by the Record Protocol



a. Process



b. Packet

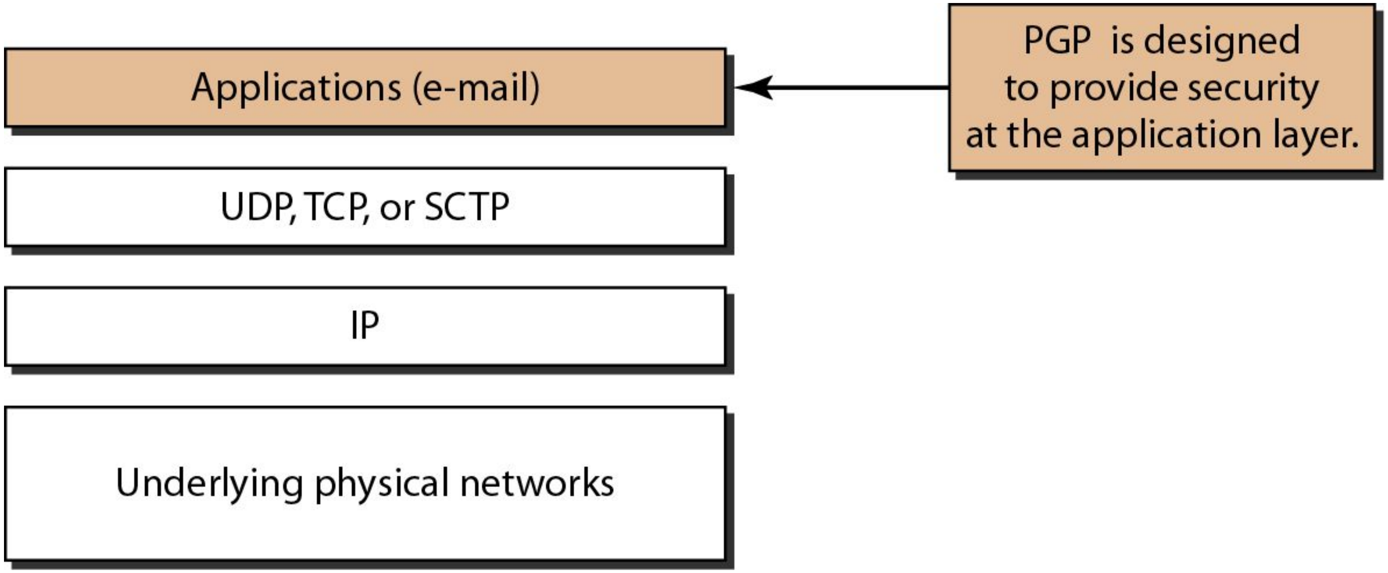
PGP

One of the protocols to provide security at the application layer is Pretty Good Privacy (PGP). PGP is designed to create authenticated and confidential e-mails.

Topics discussed in this section:

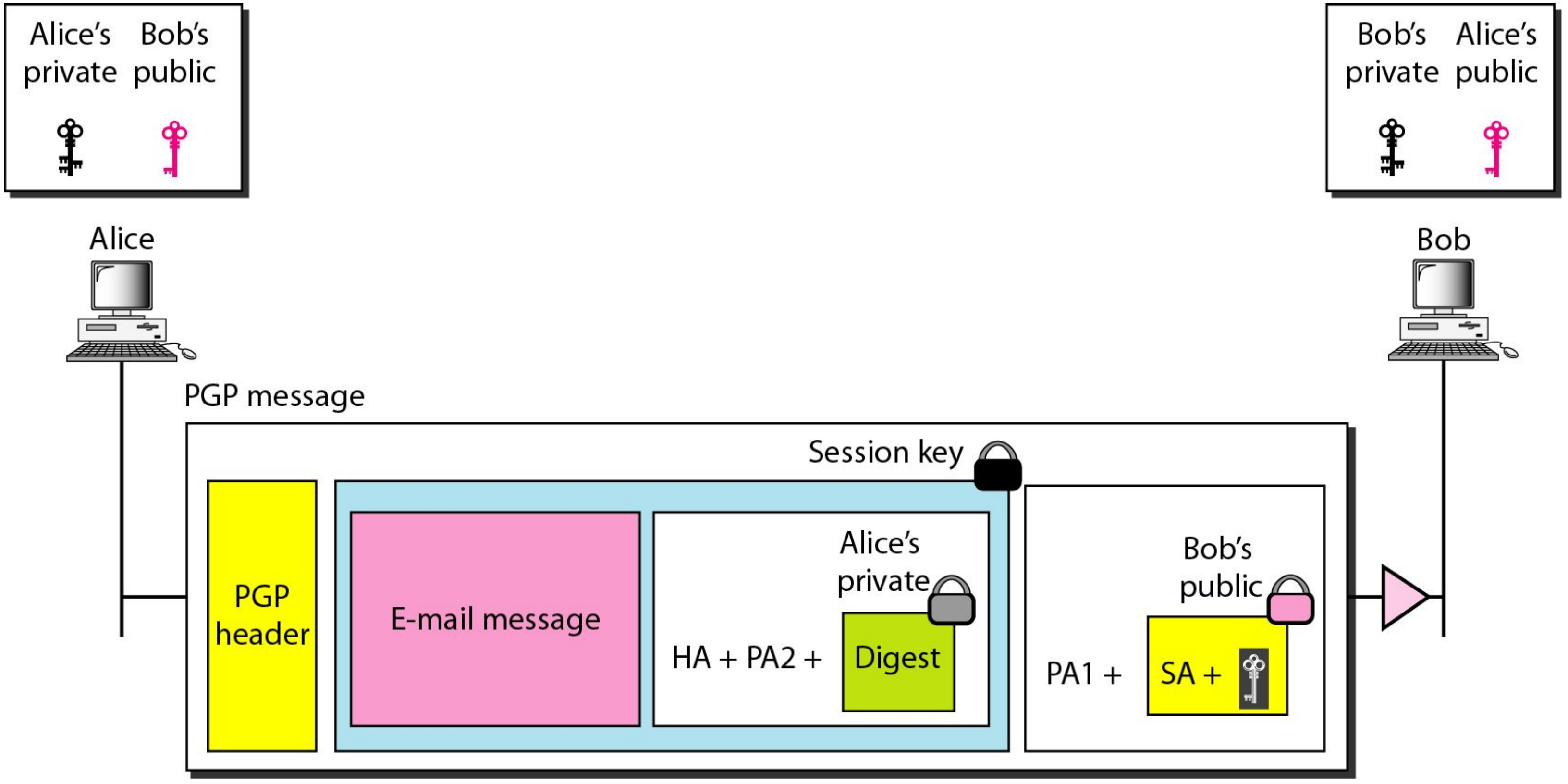
- Security Parameters
- Services
- A Scenario
  PGP Algorithms
- Key Rings
- PGP Certificates

Position of PGP in the TCP/IP protocol suite


Applications (e-mail)
UDP, TCP, or SCTP
IP
Underlying physical networks
PGP is designed to provide security at the application layer.

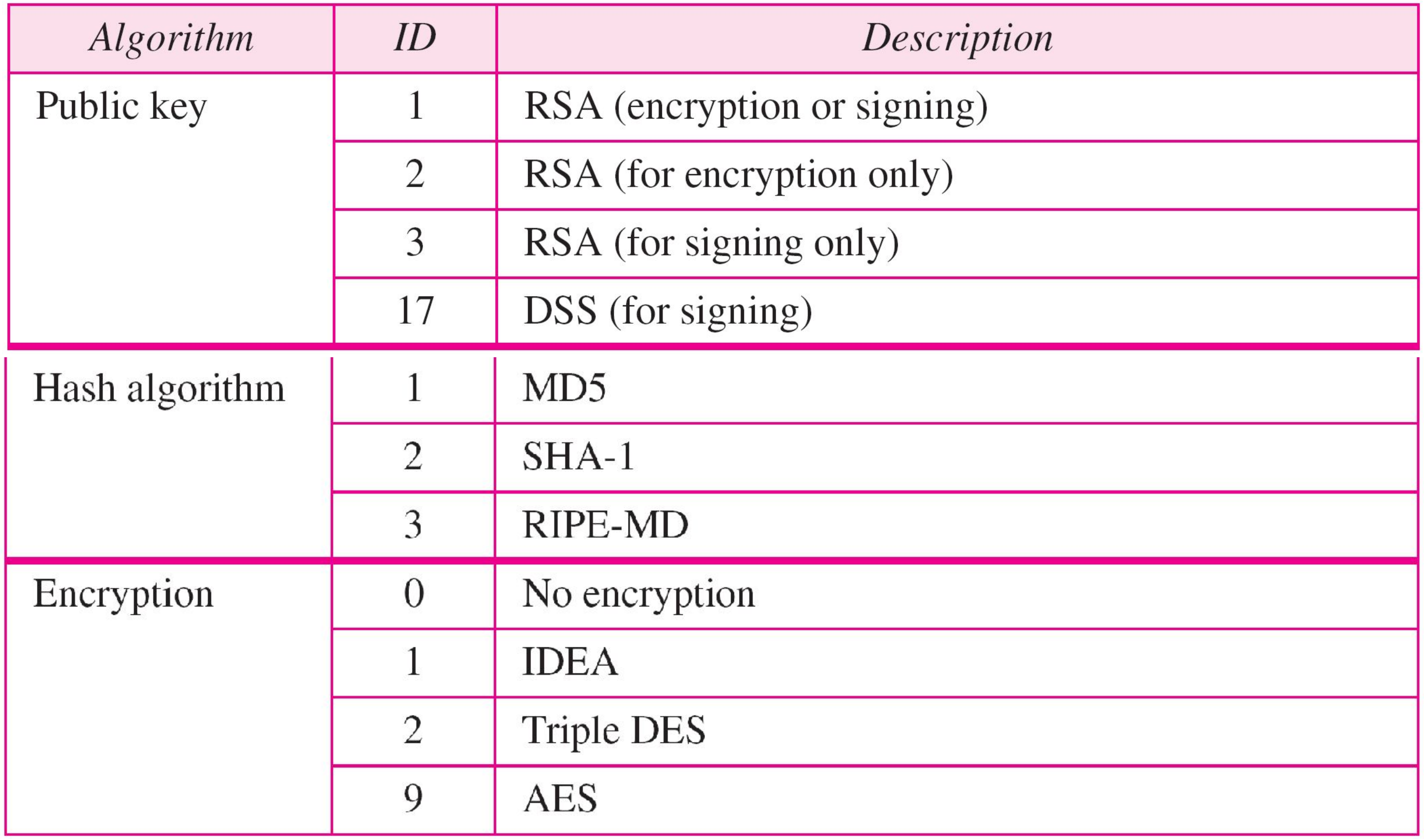
In PGP, the sender of the message needs to include the identifiers of the algorithms used in the message as well as the values of the keys.

A scenario in which an e-mail message is authenticated and encrypted



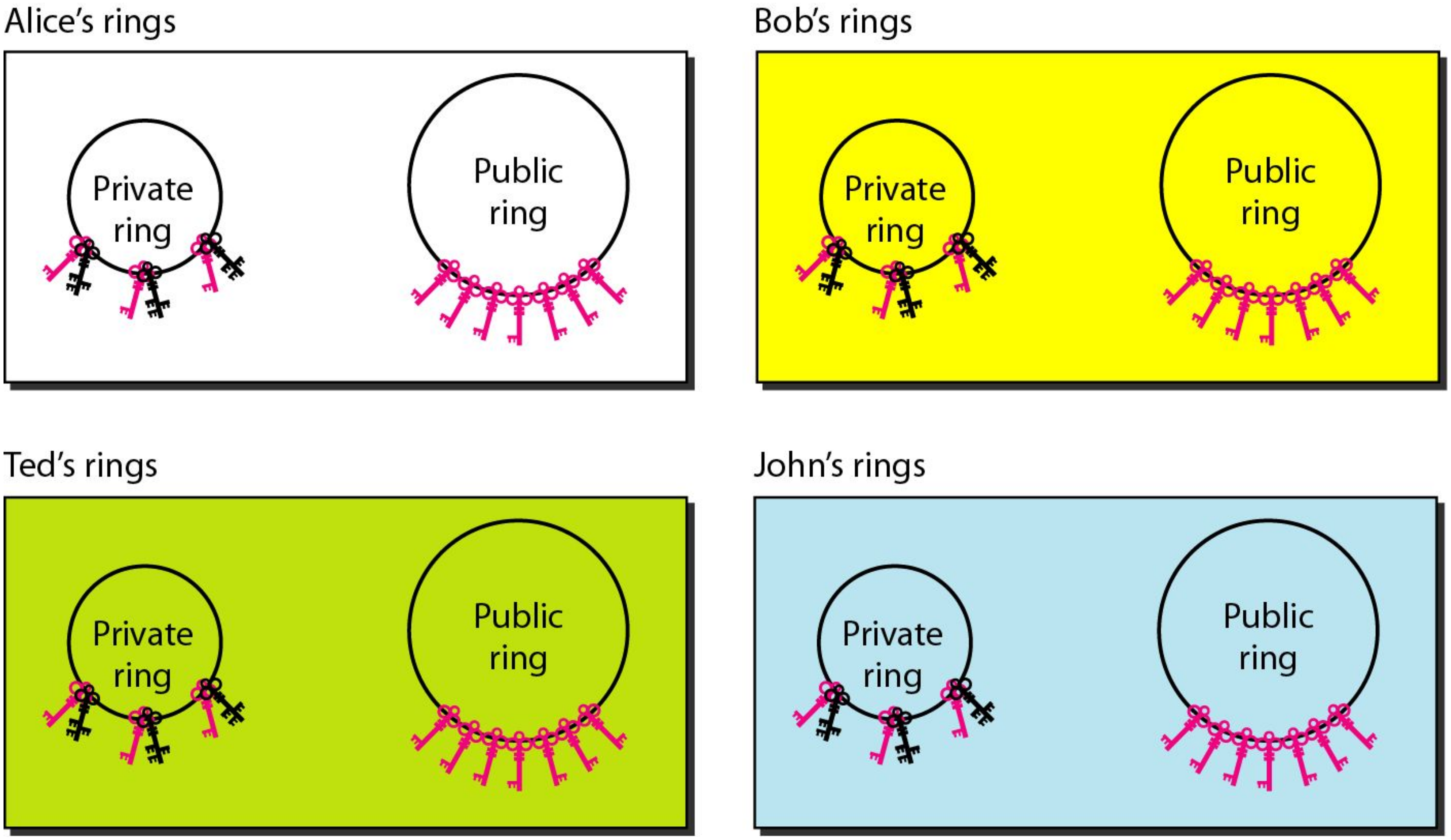
PA1: Public-key algorithm 1 (for encrypting session key)
PA2: Public-key algorithm (for encrypting the digest)
SA: Symmetric-key algorithm identification (for encrypting message and digest)
HA: Hash algorithm identification (for creating digest)

PGP Algorithms



Algorithm	*ID*	*Description*
Public key	1	RSA (encryption or signing)
	2	RSA (for encryption only)
	3	RSA (for signing only)
	17	DSS (for signing)
Hash algorithm	1	MD5
	2	SHA-1
	3	RIPE-MD
Encryption	0	No encryption
	1	IDEA
	2	Triple DES
	9	AES

Rings


Alice's rings
Private ring
Public ring
Bob's rings
Private ring
Public ring
Ted's rings
Private ring
Public ring
John's rings
Private ring
Public ring

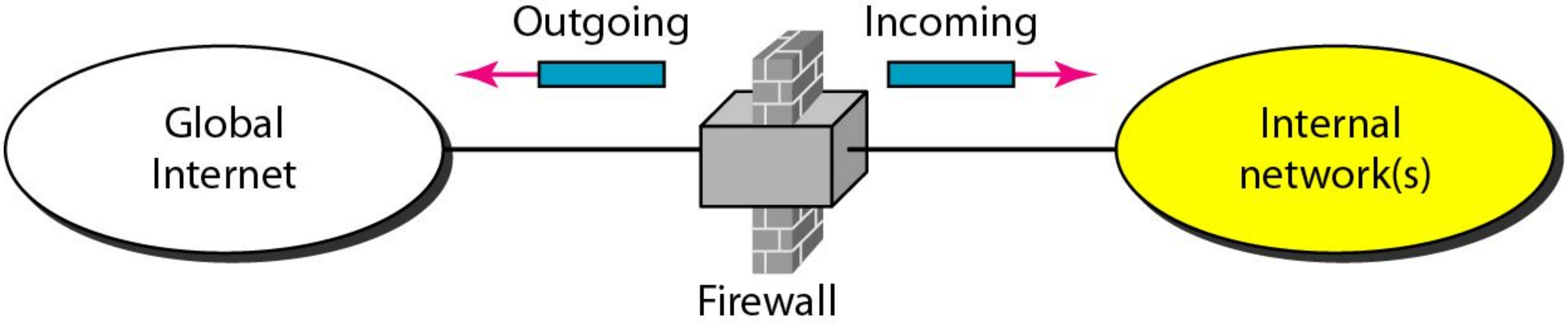
FIREWALLS

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 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.

Topics discussed in this section:

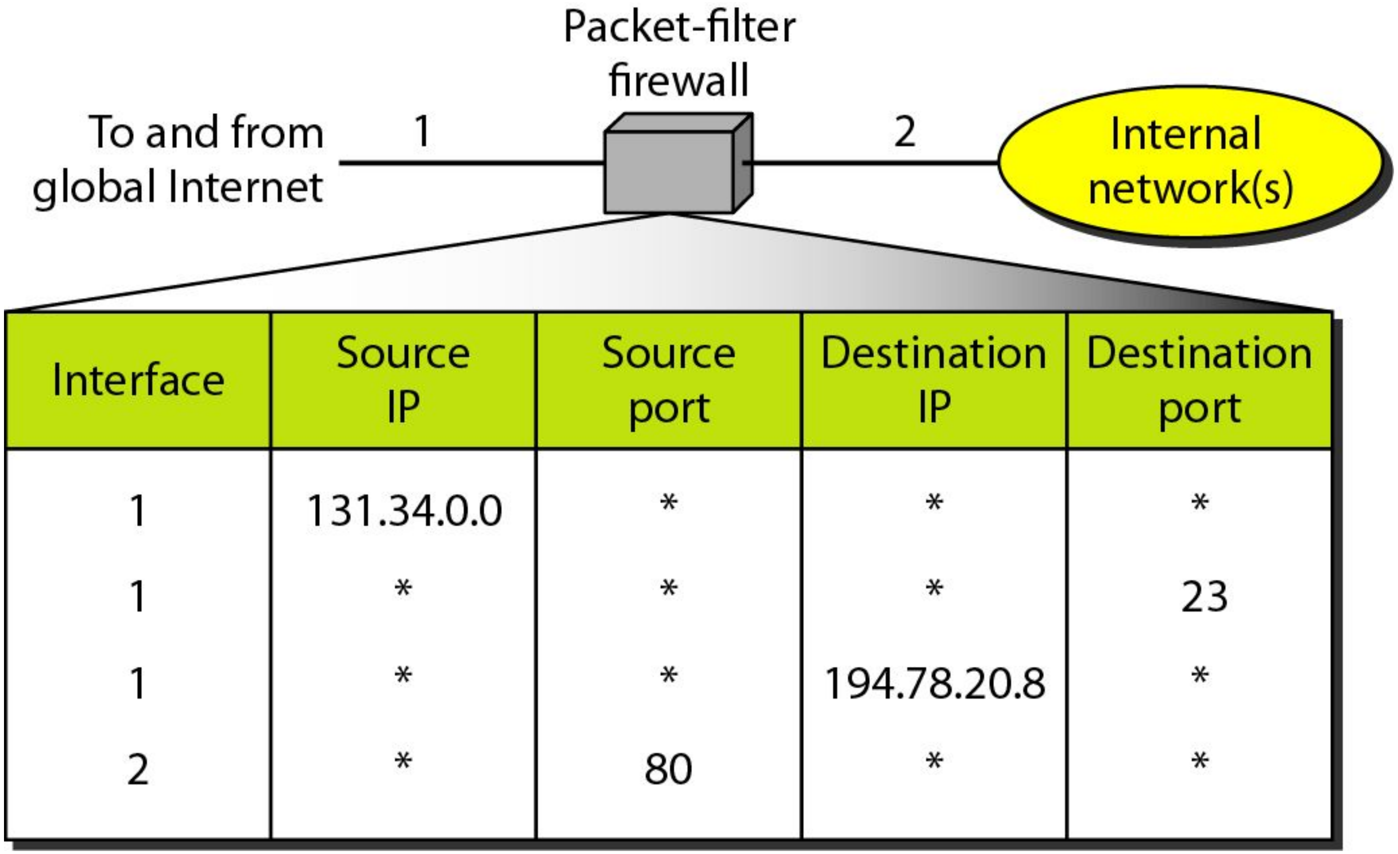
- **Packet-Filter Firewall**
- **Proxy Firewall**

Firewall



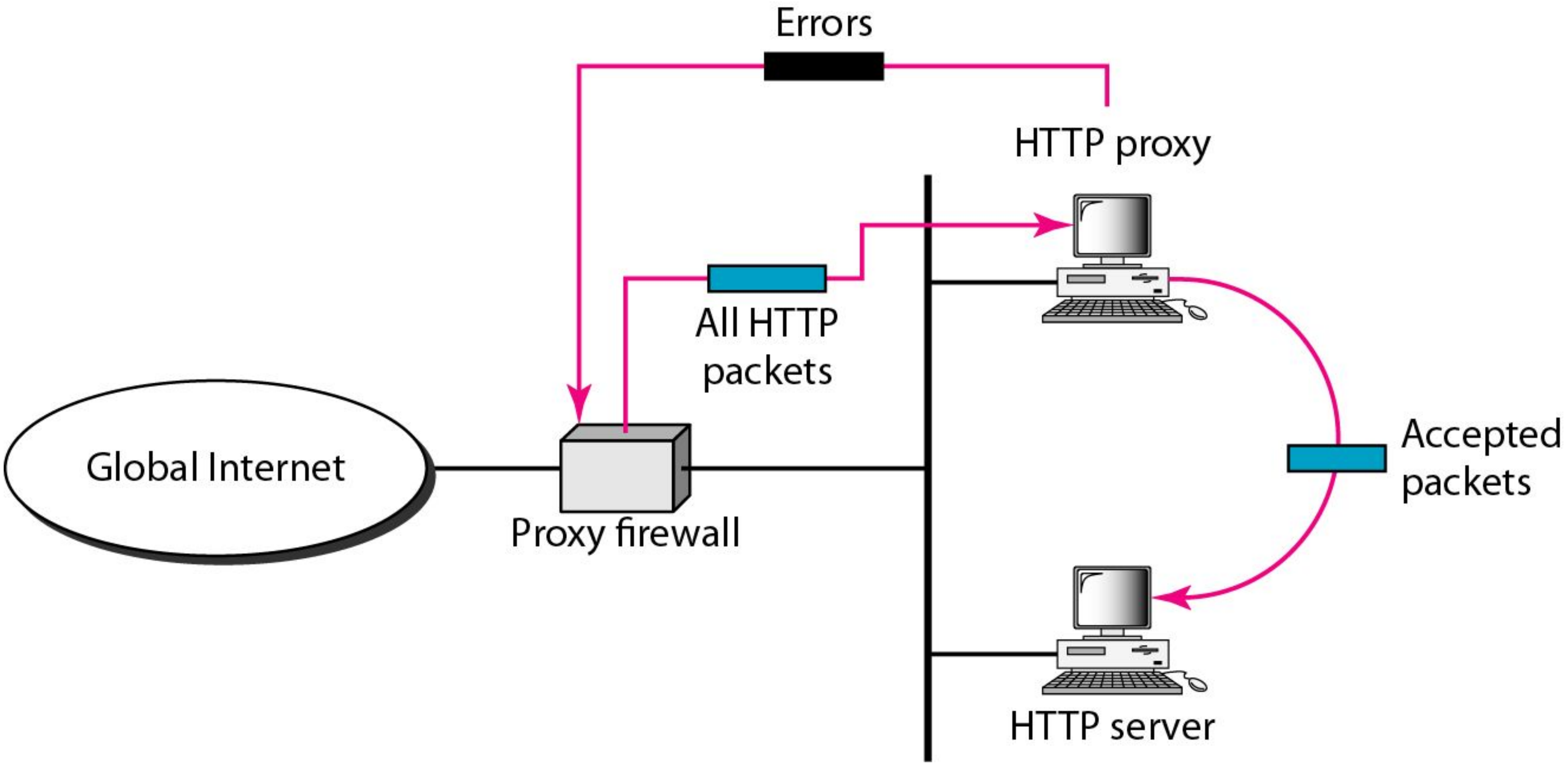
A packet-filter firewall filters at the network or transport layer.

Packet-filter firewall



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

Proxy firewall



A proxy firewall filters at the application layer.