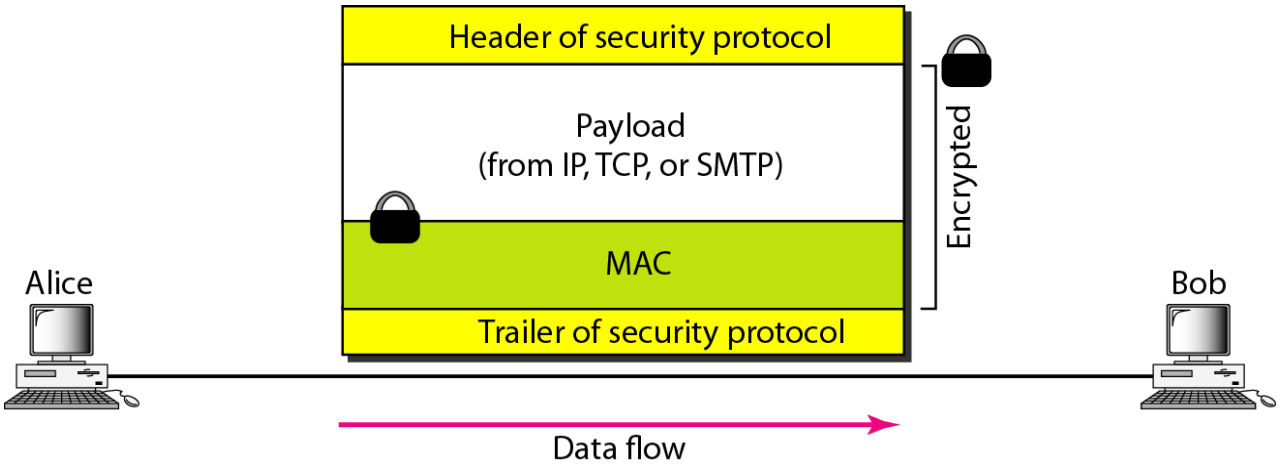
Data Communications and Networking Fourth Edition

Forouzan

Chapter 32

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

Figure 32.1 *Common structure of three security protocols*



32-1 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

Figure 32.2 *TCP/IP protocol suite and IPSec*

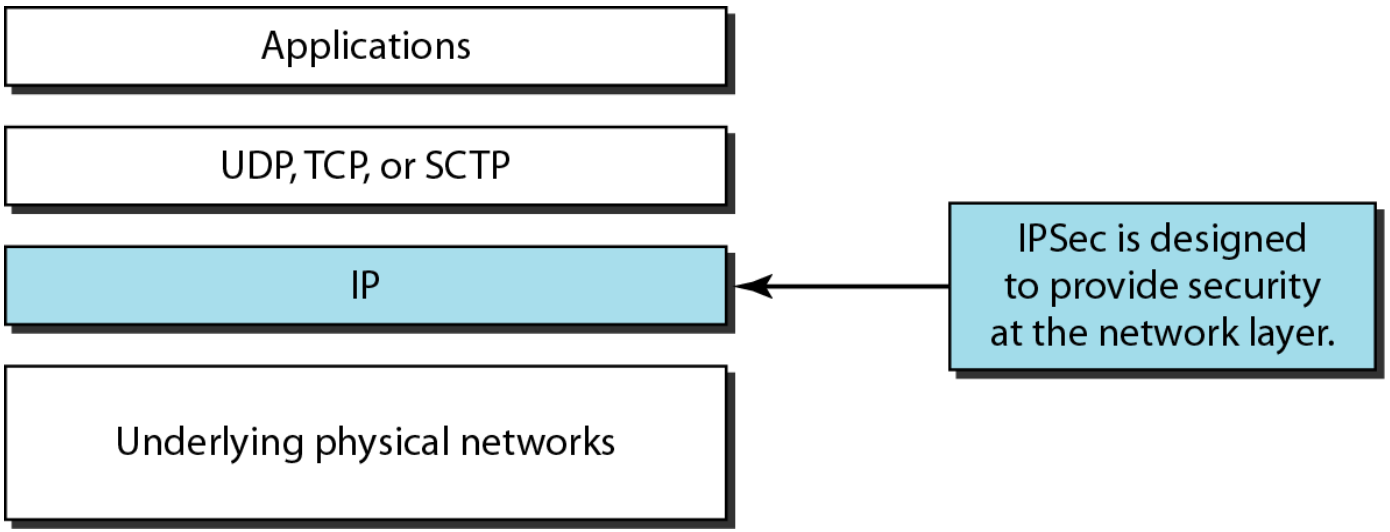
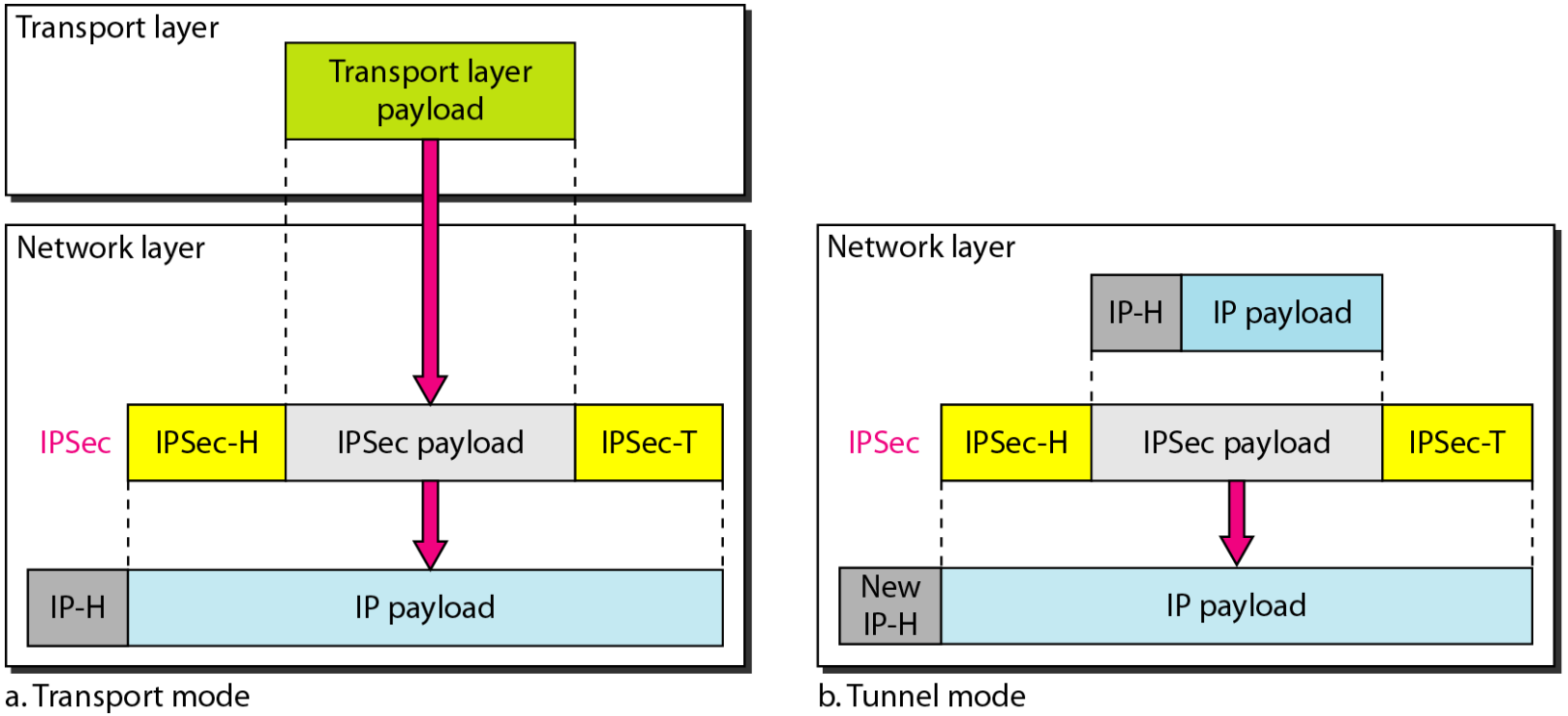


Figure 32.3 *Transport mode and tunnel modes of IPSec protocol*



Note

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

Figure 32.4 *Transport mode in action*

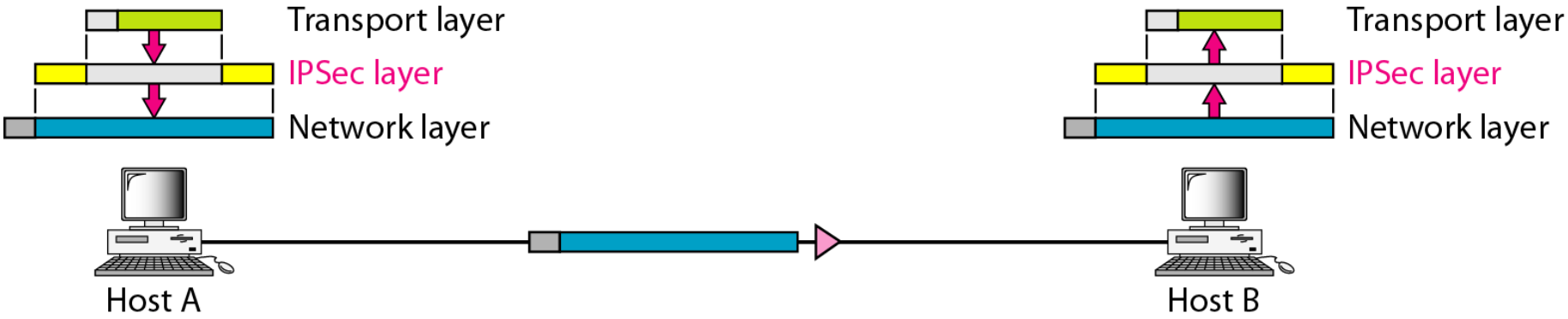
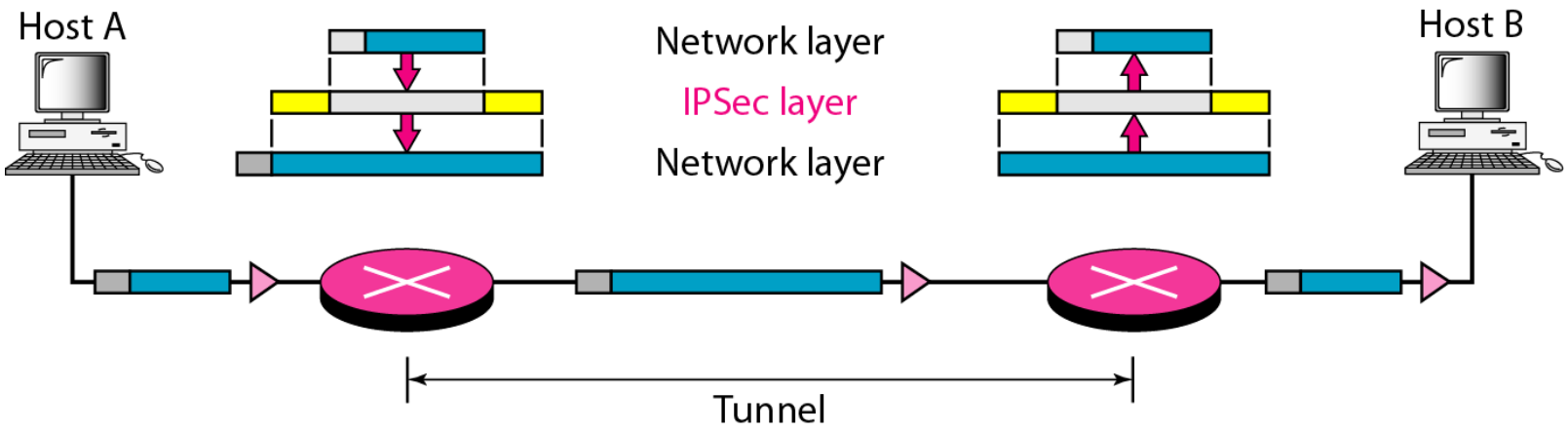


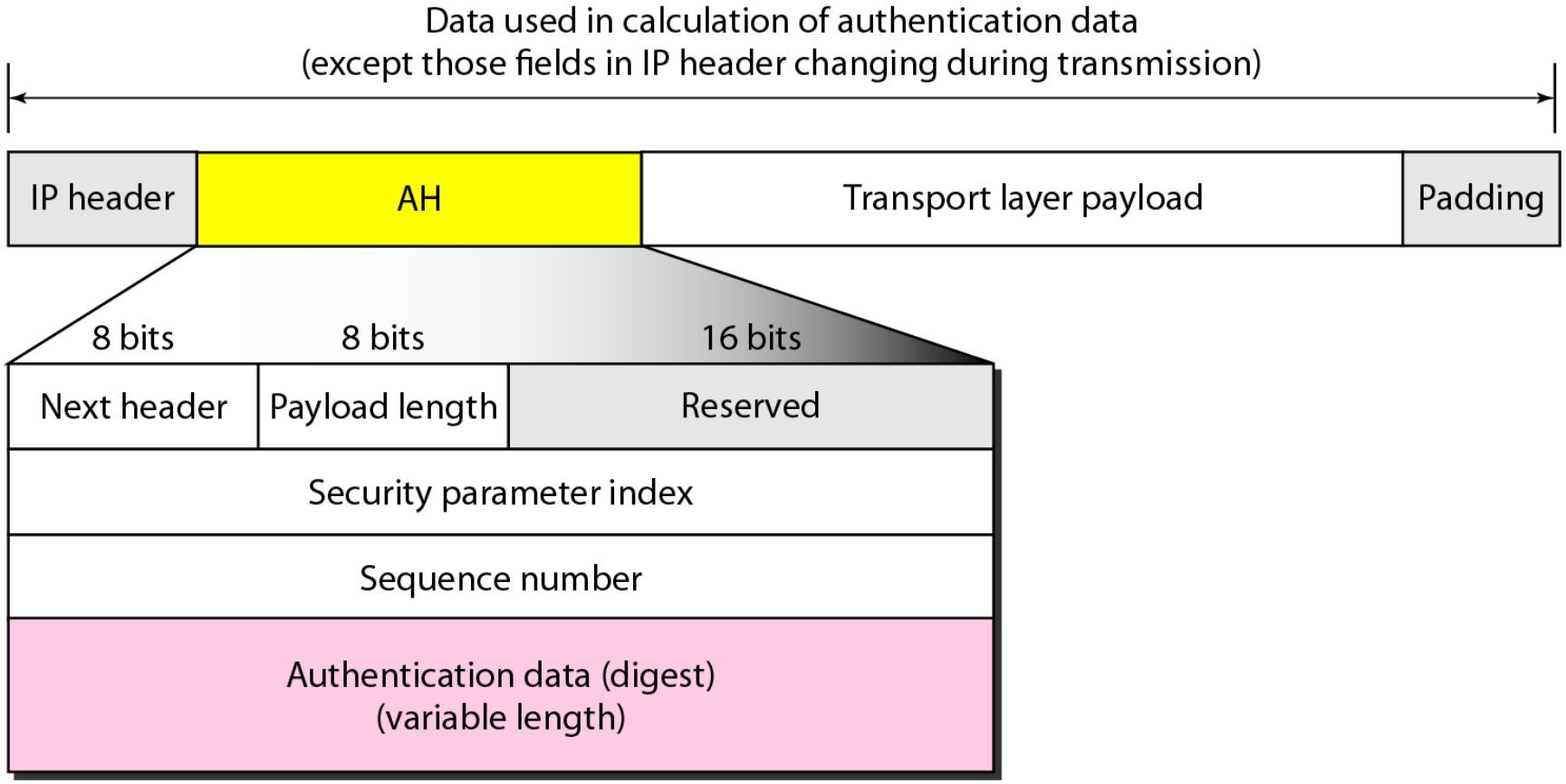
Figure 32.5 *Tunnel mode in action*



Note

IPSec in tunnel mode protects the original IP header.

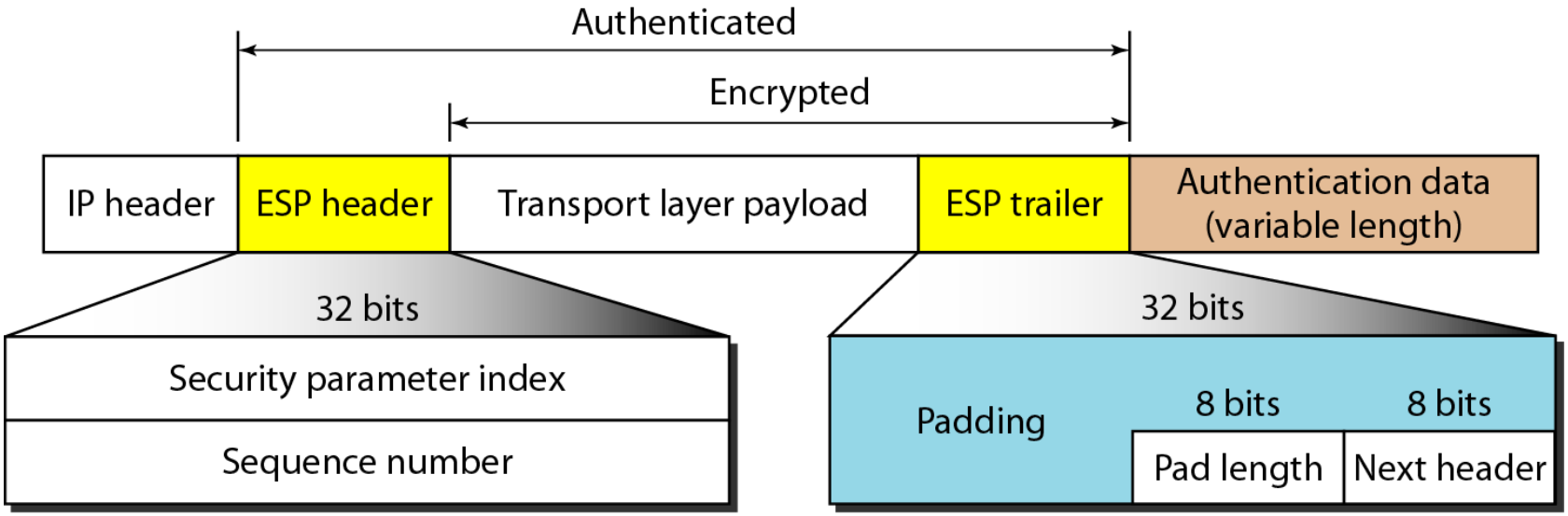
Figure 32.6 *Authentication Header (AH) Protocol in transport mode*



Note

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

Figure 32.7 *Encapsulating Security Payload (ESP) Protocol in transport mode*



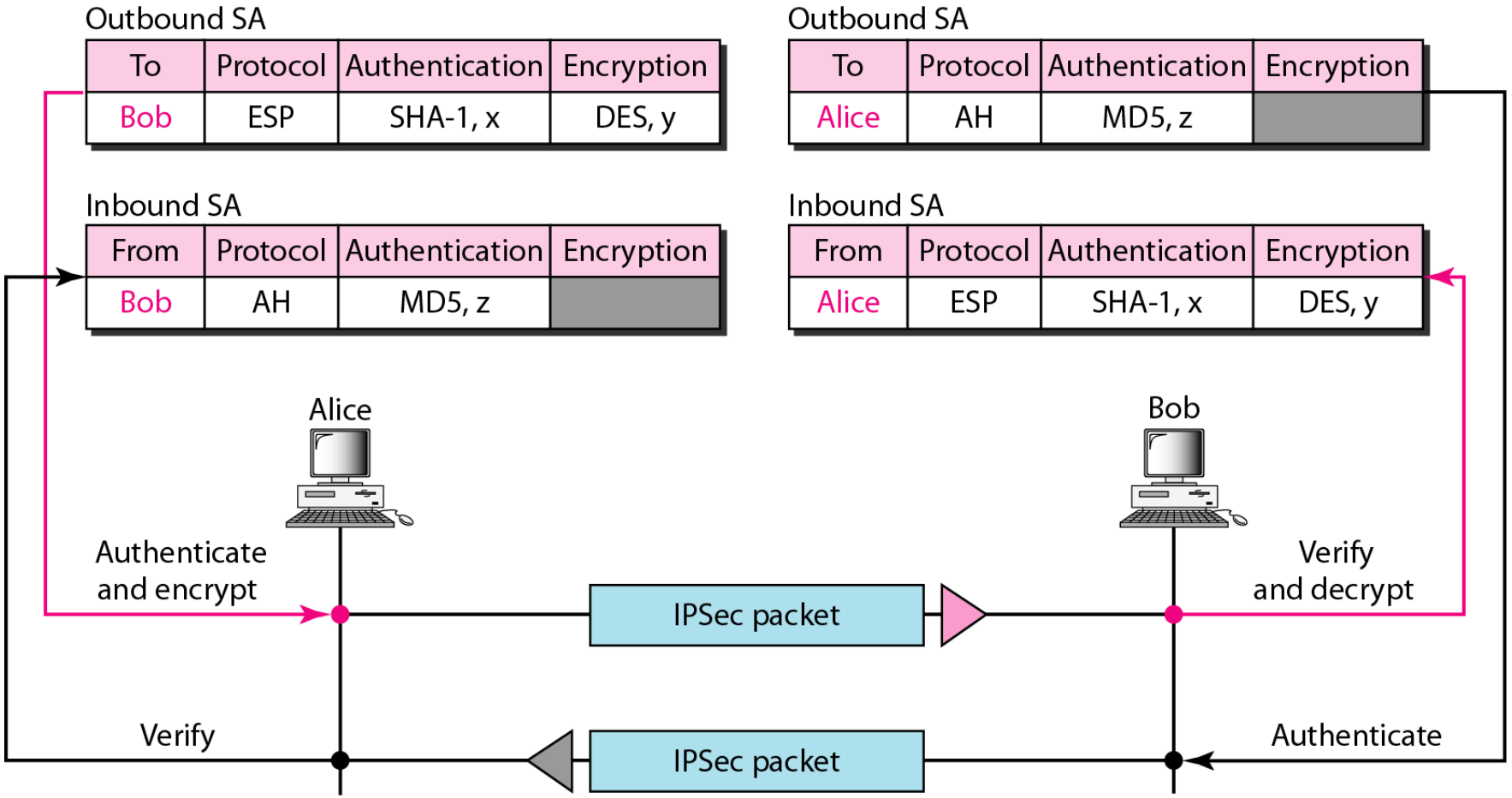
Note

ESP provides source authentication, data integrity, and privacy.

Table 32.1 *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

Figure 32.8 *Simple inbound and outbound security associations*



Note

IKE creates SAs for IPSec.

Figure 32.9 *IKE components*

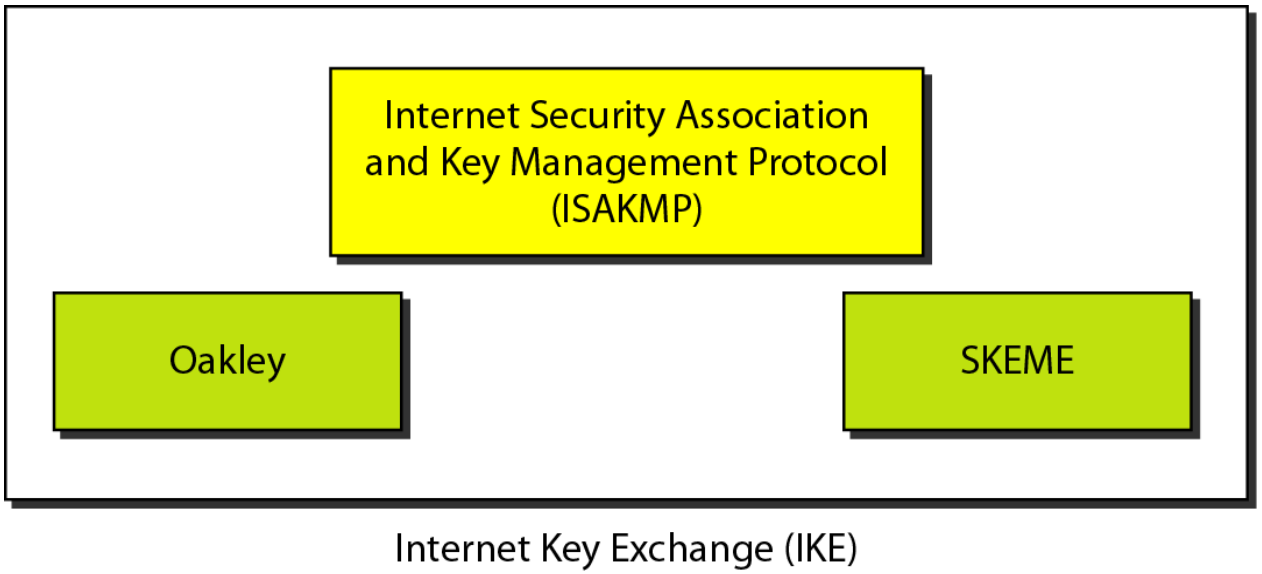


Table 32.2 ***Addresses for private networks***

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}

Figure 32.10 *Private network*

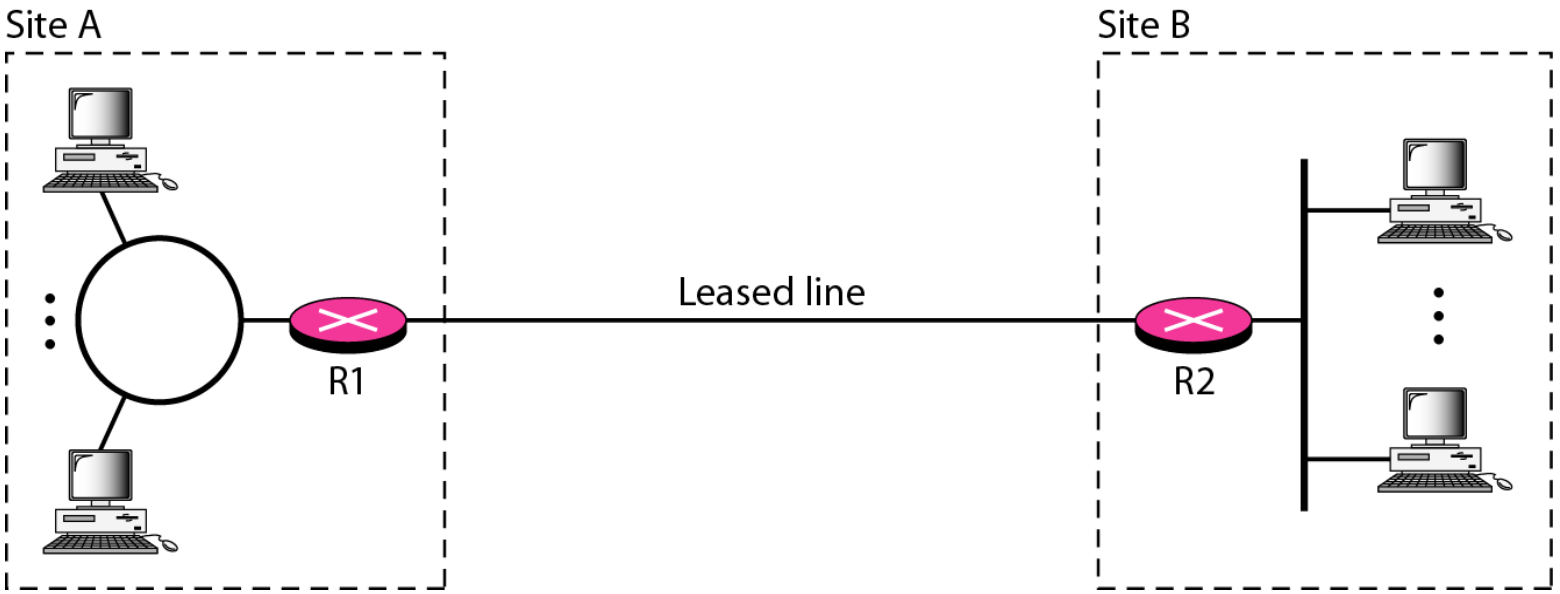


Figure 32.11 *Hybrid network*

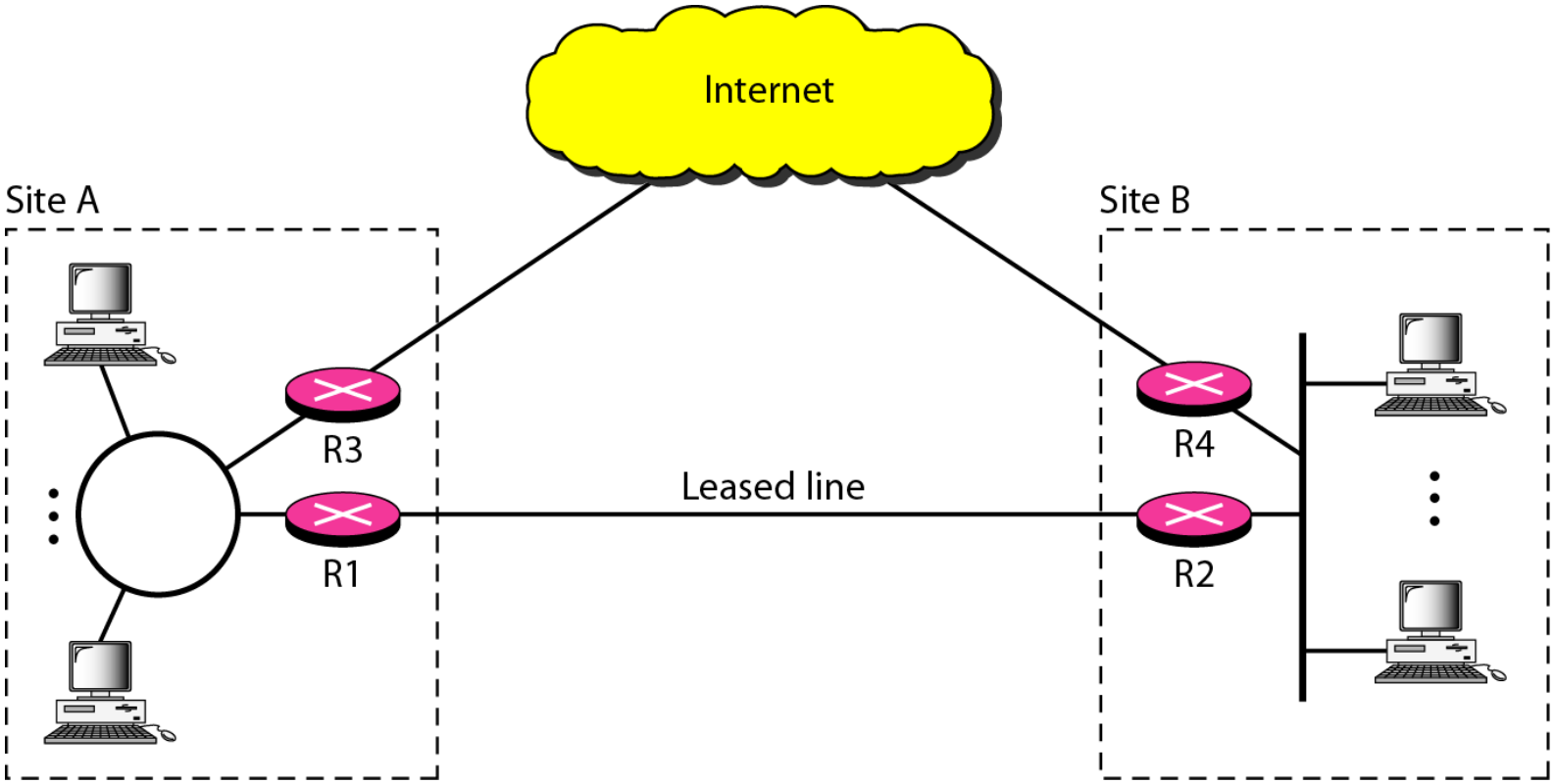


Figure 32.12 *Virtual private network*

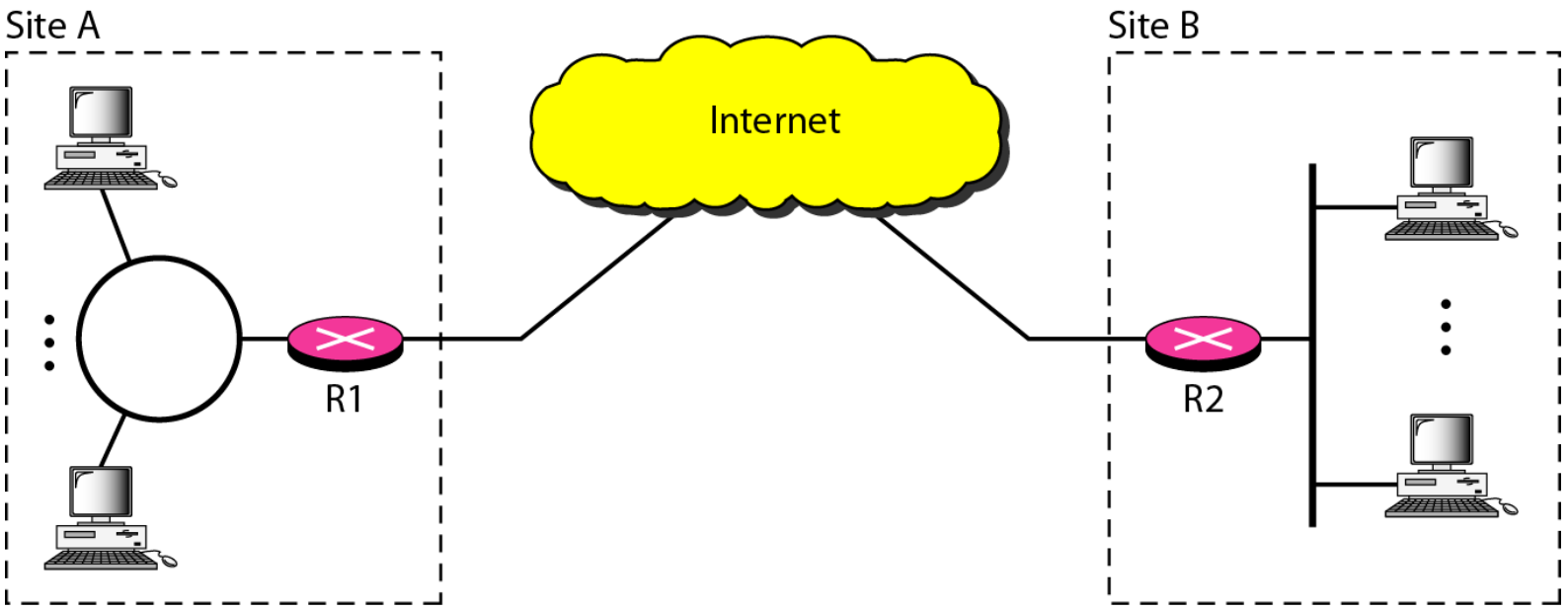
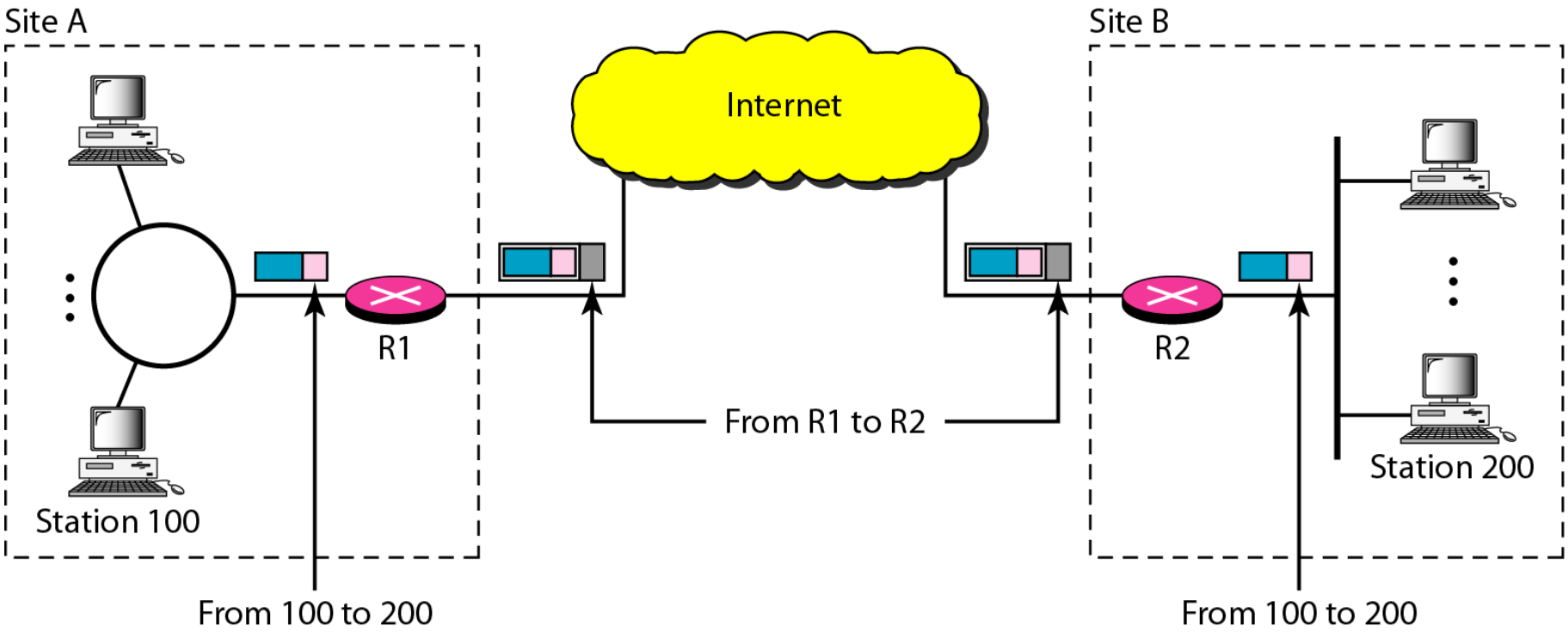


Figure 32.13 *Addressing in a VPN*



32-2 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

Figure 32.14 *Location of SSL and TLS in the Internet model*

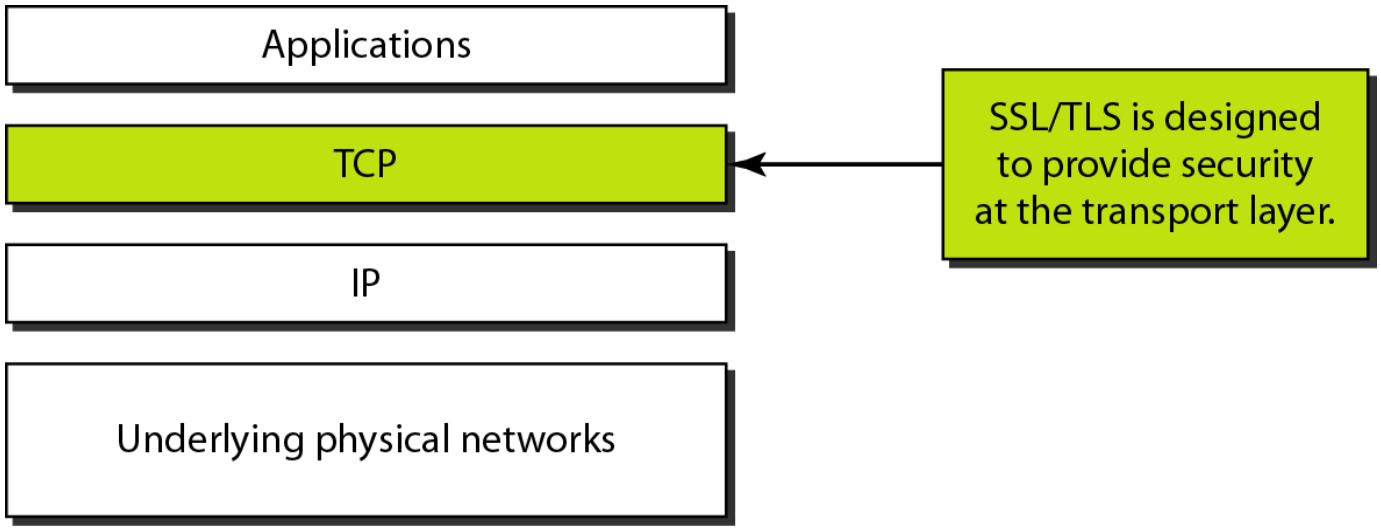


Table 32.3 *SSL cipher suite list*

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

Table 32.3 *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

Note

The client and the server have six different cryptography secrets.

Figure 32.15 *Creation of cryptographic secrets in SSL*

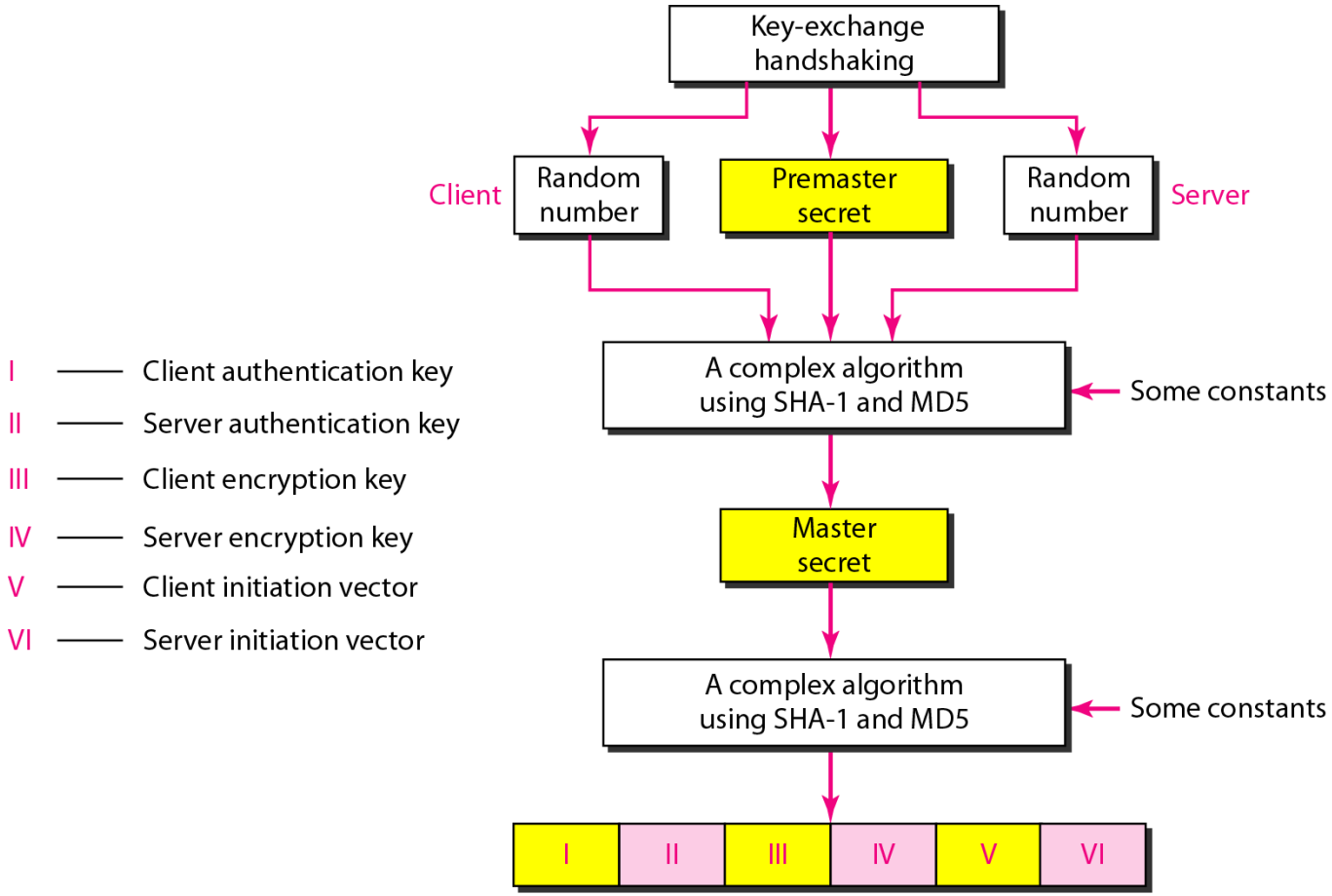


Figure 32.16 *Four SSL protocols*

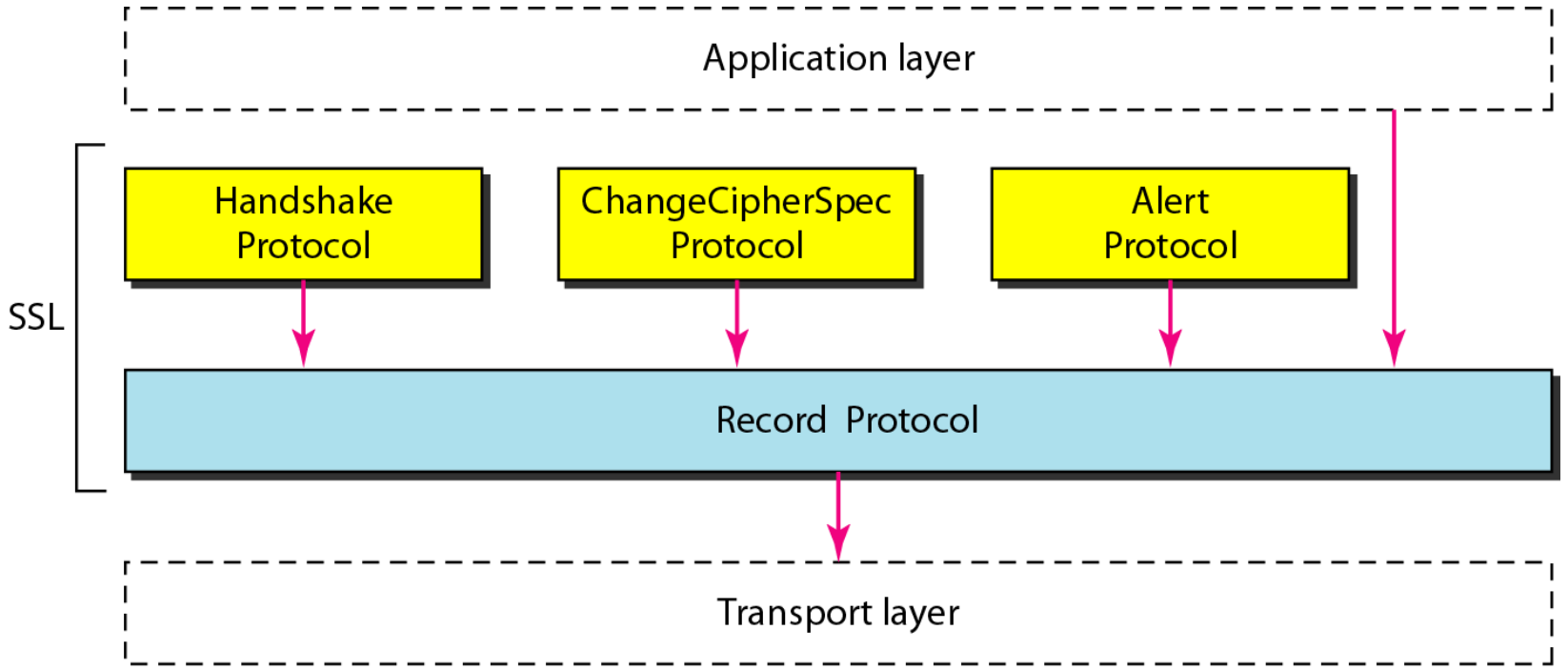


Figure 32.17 *Handshake Protocol*

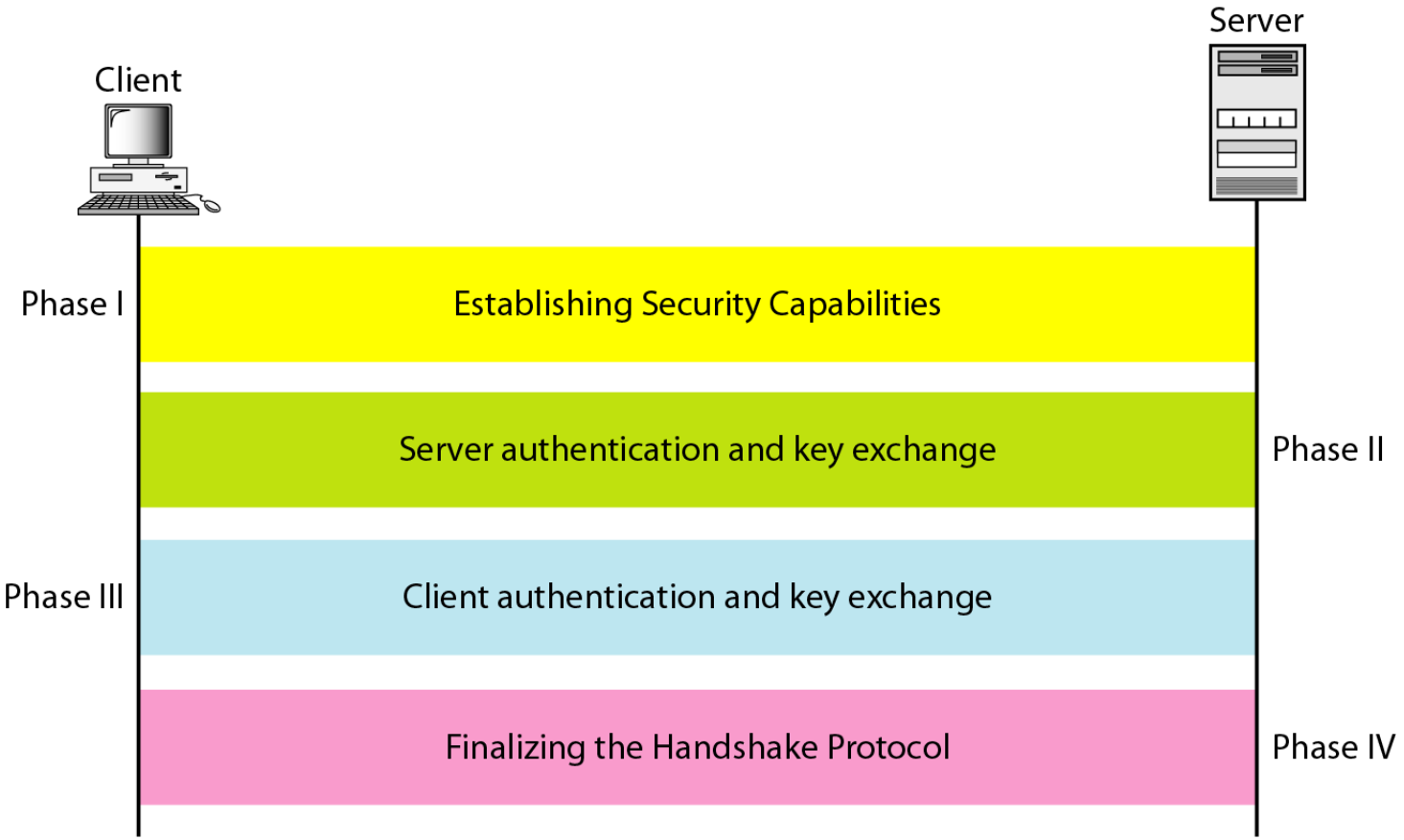
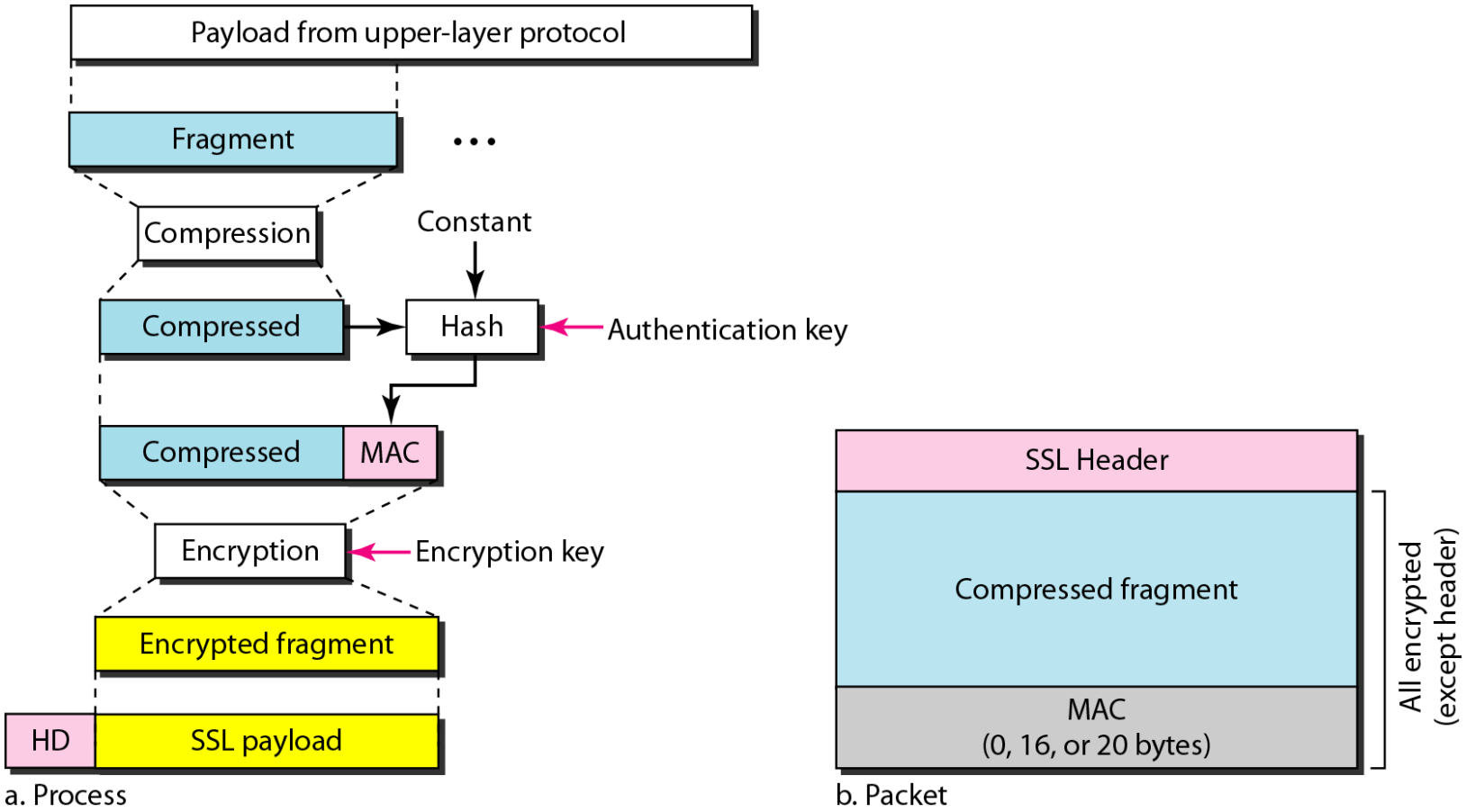


Figure 32.18 *Processing done by the Record Protocol*



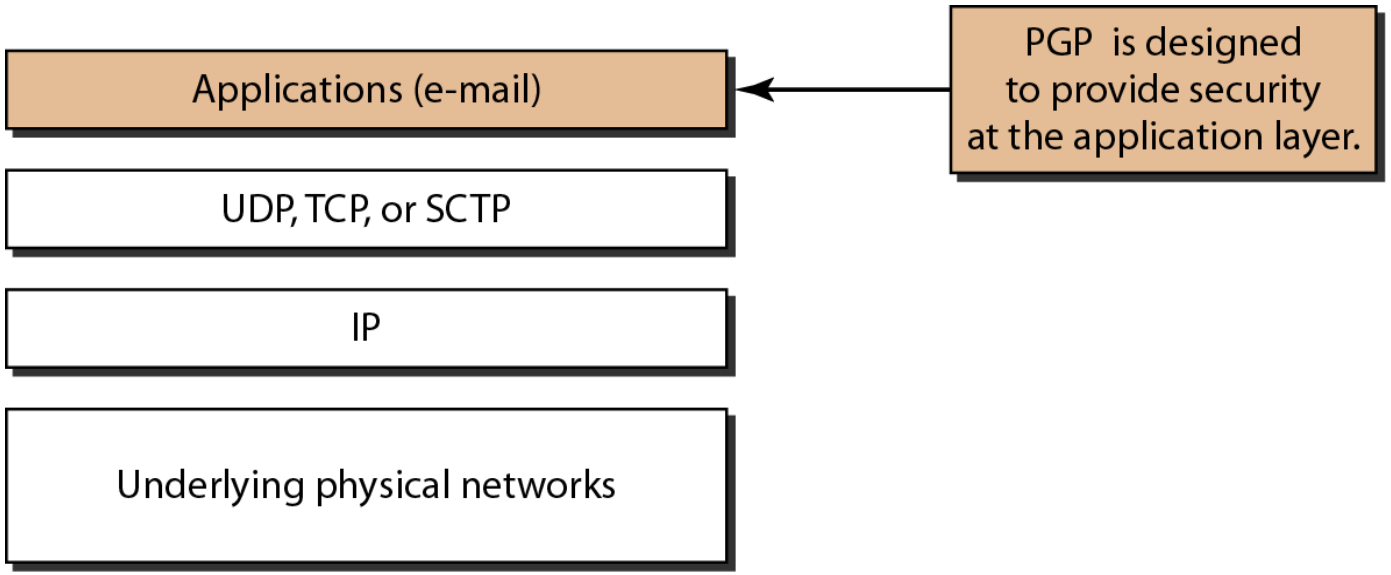
32-3 PGP

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

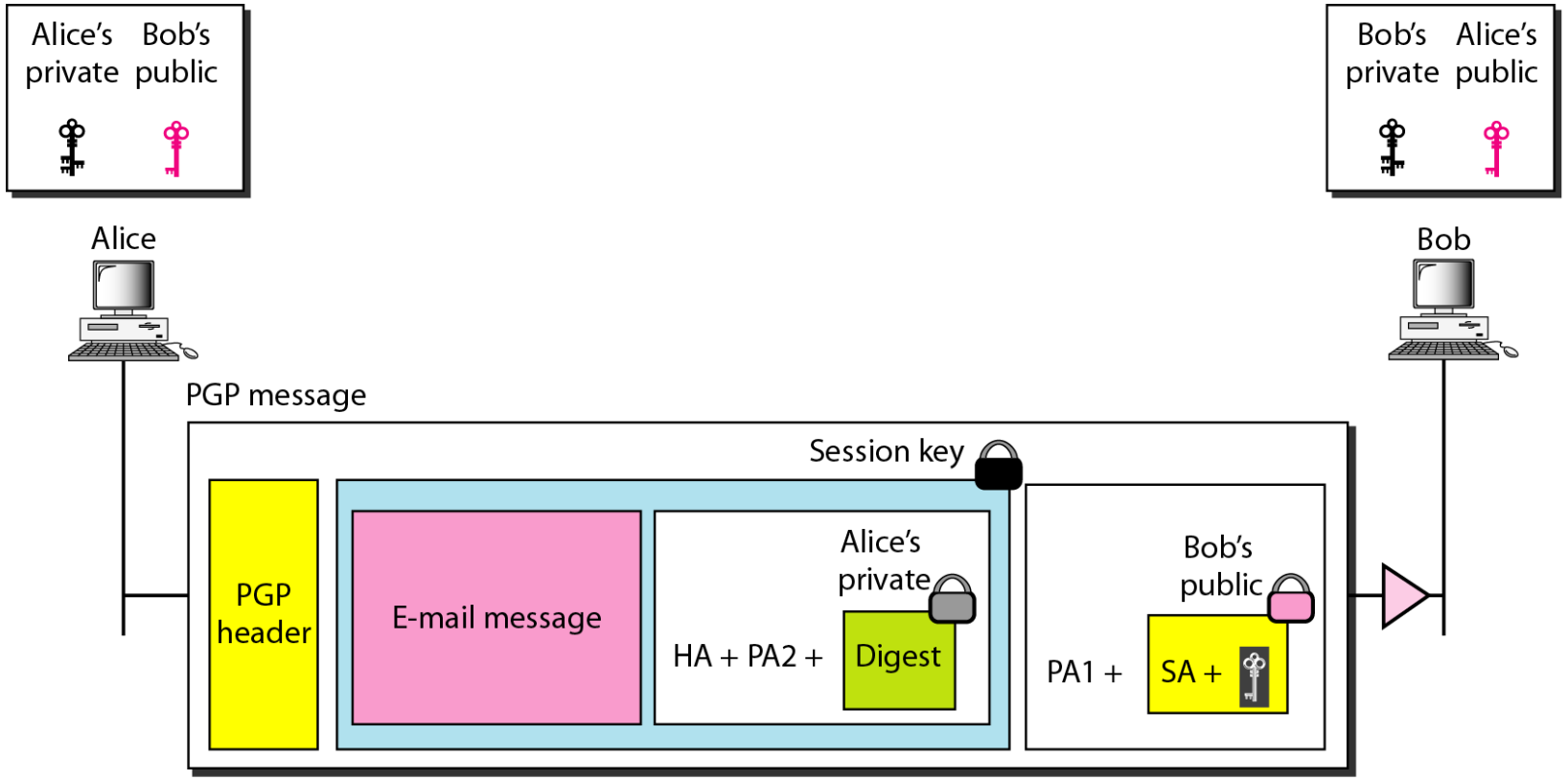
Figure 32.19 *Position of PGP in the TCP/IP protocol suite*



Note

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.

Figure 32.20 *A scenario in which an e-mail message is authenticated and encrypted*

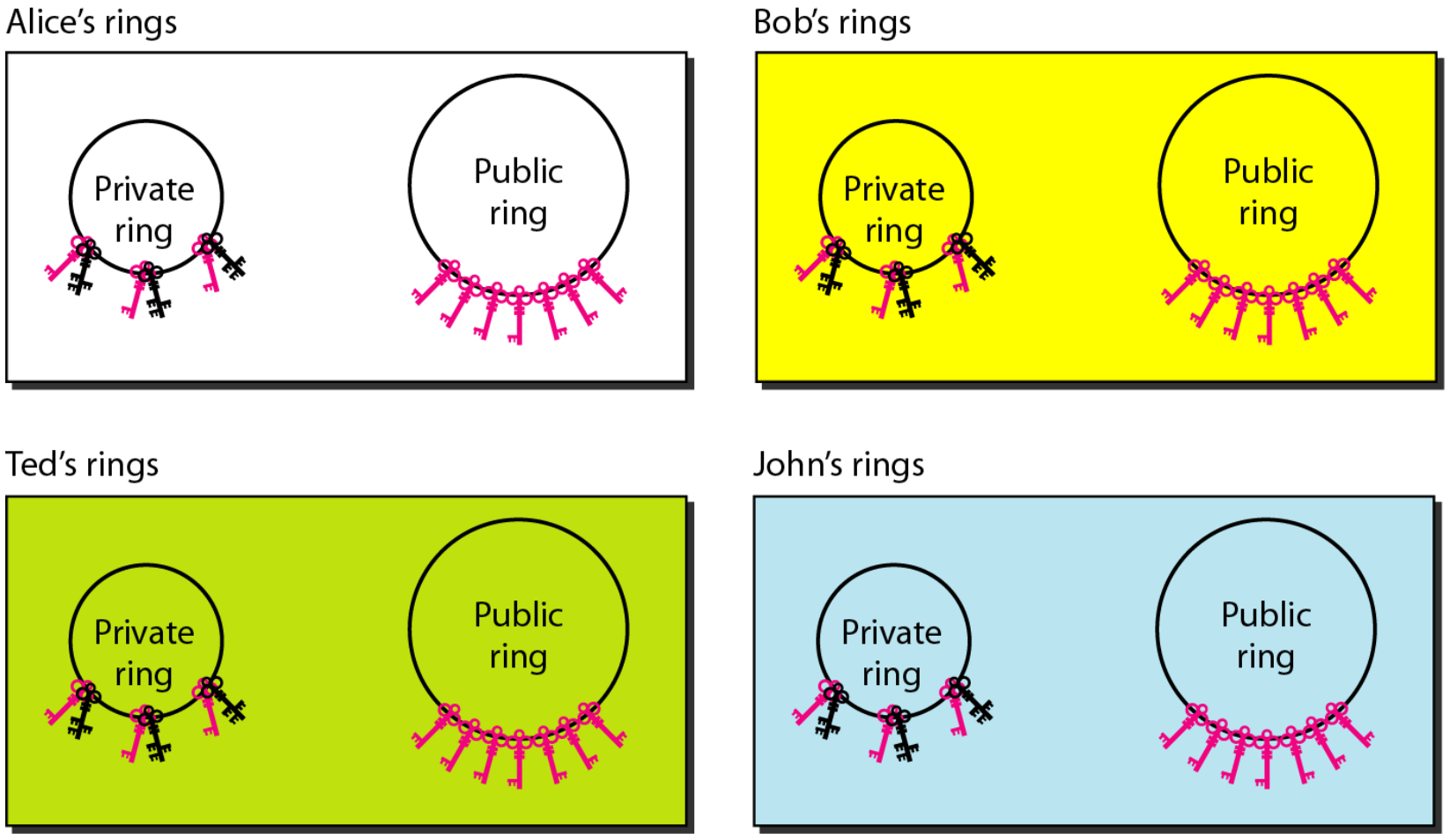


PA1: Public-key algorithm 1 (for encrypting session key)
PA2: Public-key algorithm (for encrypting the digest)
SA: Symmetric-key algorithm identification (for encrypting message and digest)
HA: Hash algorithm identification (for creating digest)

Table 32.4 *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

Figure 32.21 *Rings*



Note

In PGP, there can be multiple paths from fully or partially trusted authorities to any subject.

32-4 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

Figure 32.22 *Firewall*

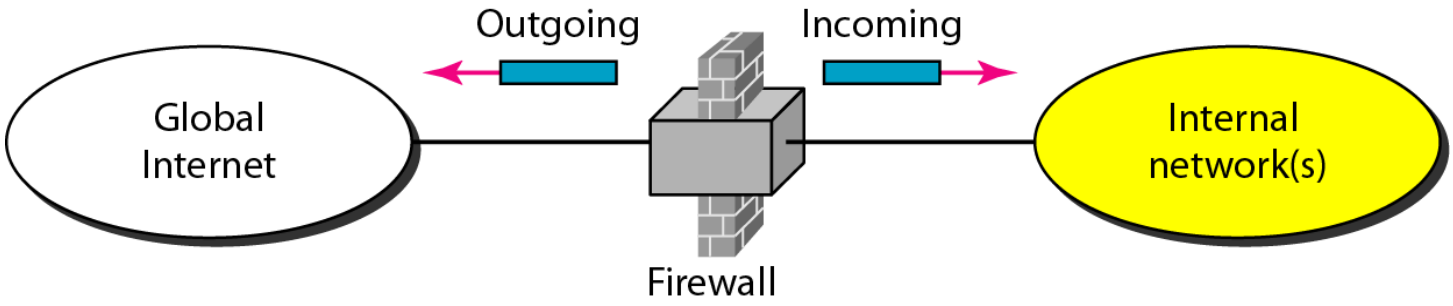
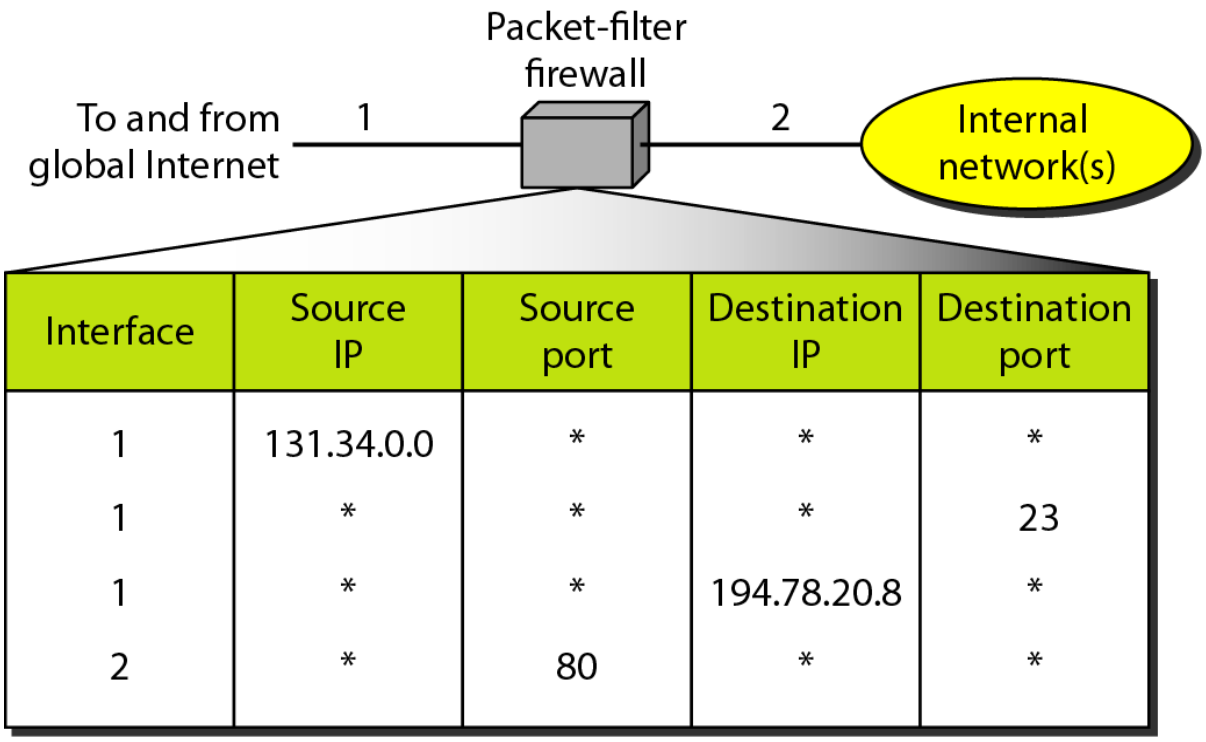


Figure 32.23 *Packet-filter firewall*

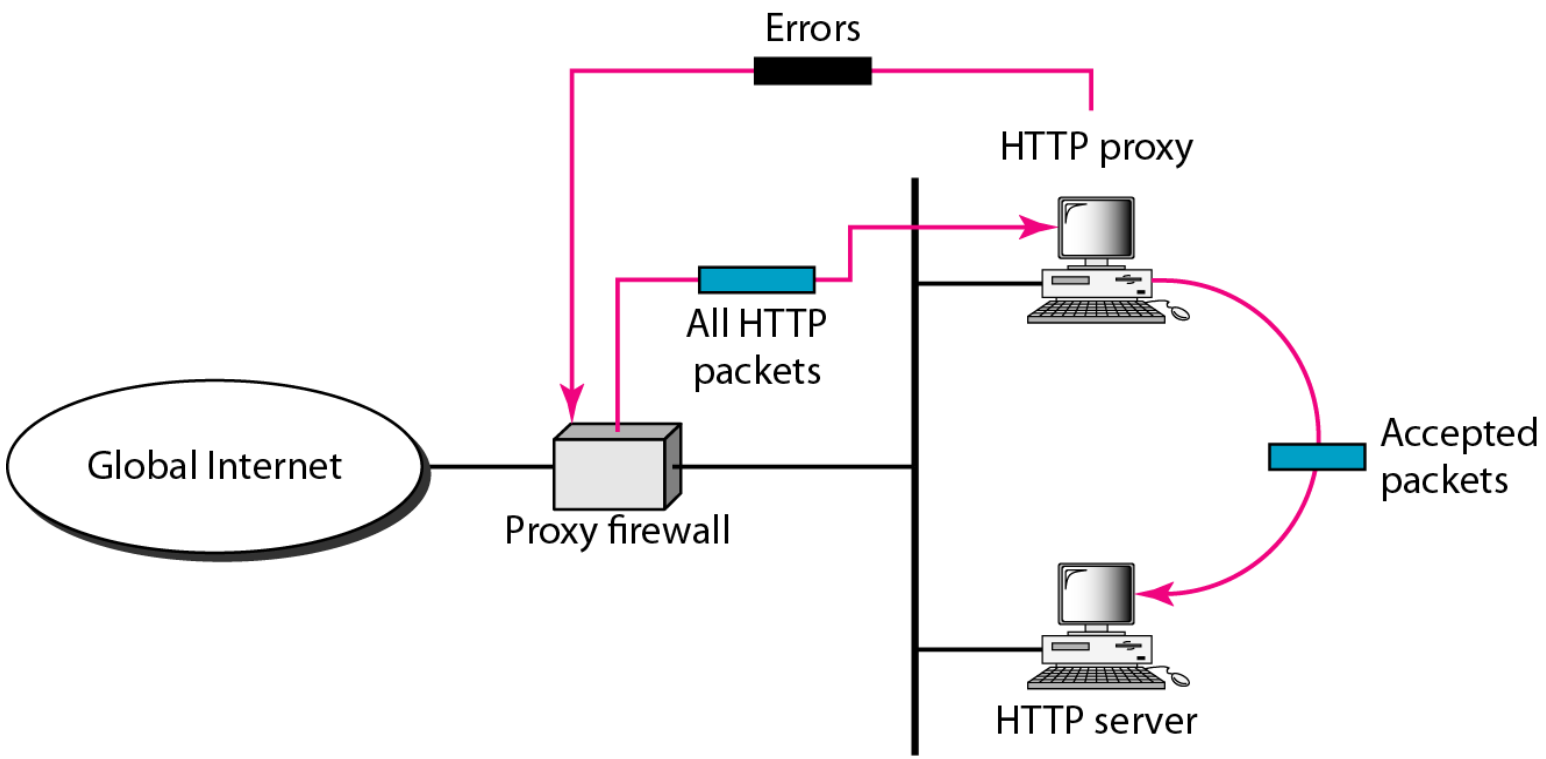


Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Note

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

Figure 32.24 *Proxy firewall*



Note

A proxy firewall filters at the application layer.