Cryptography

Figure 1 *Cryptography components*

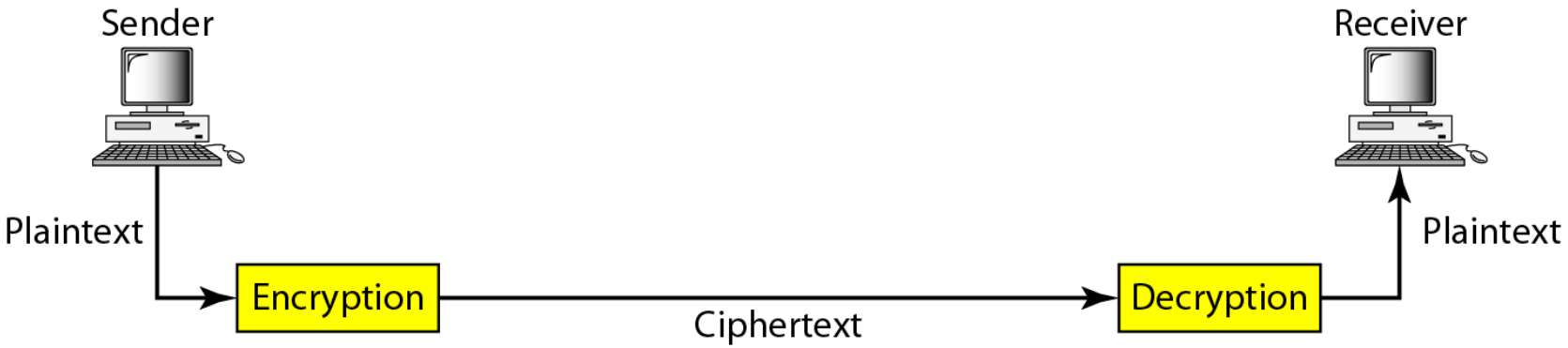


Figure 2 *Categories of cryptography*

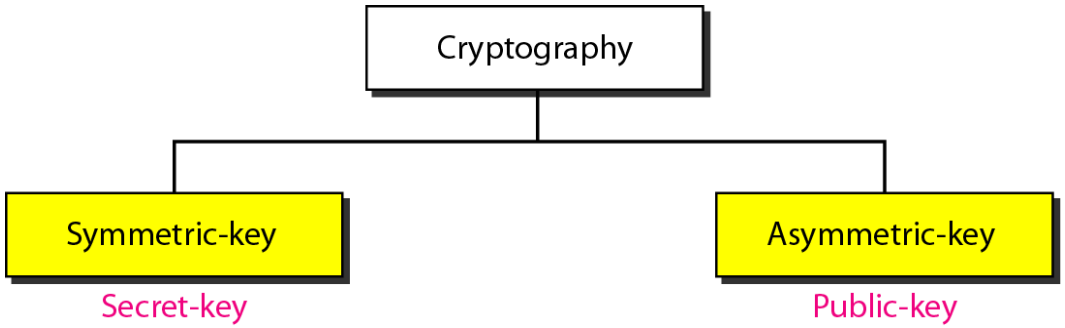


Figure 3 *Symmetric-key cryptography*

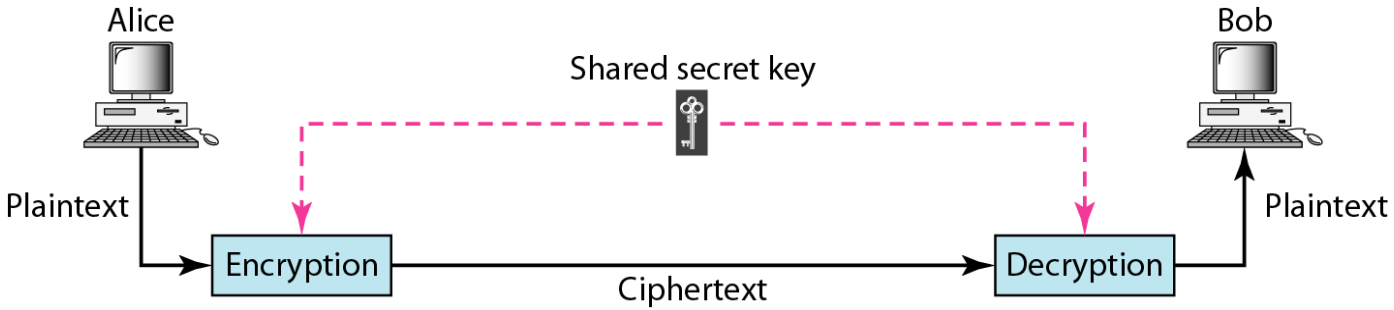


Figure 4 *Asymmetric-key cryptography*

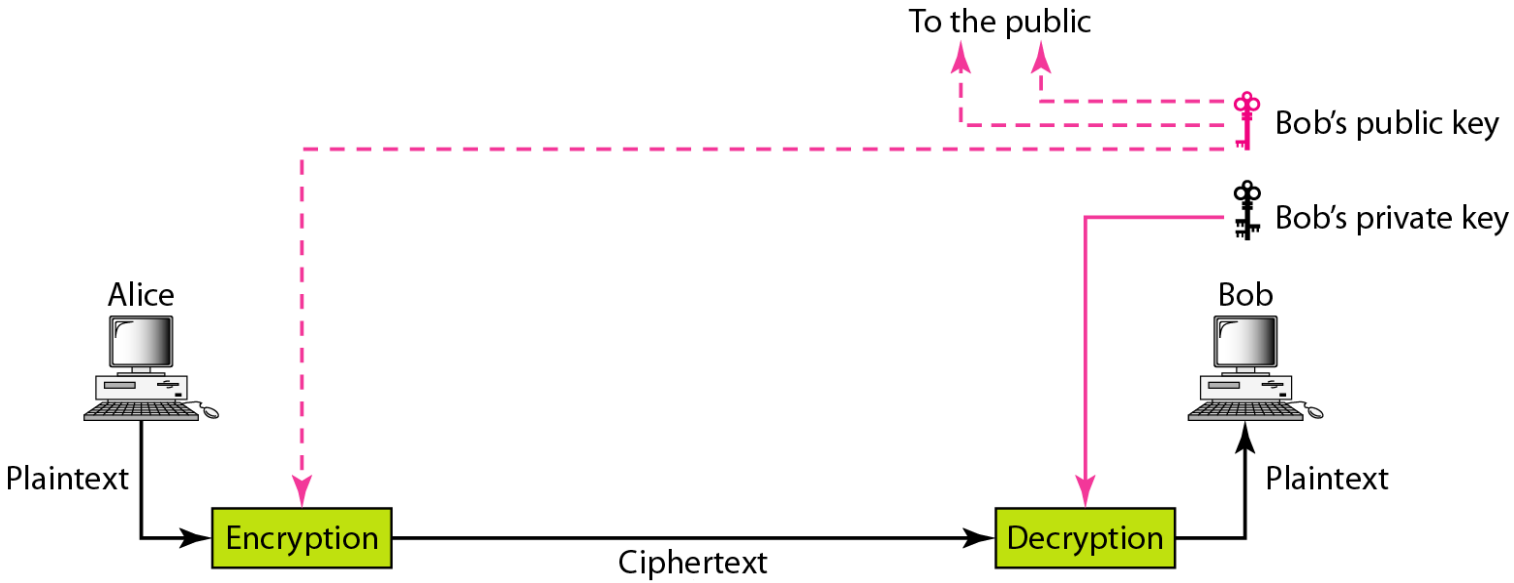
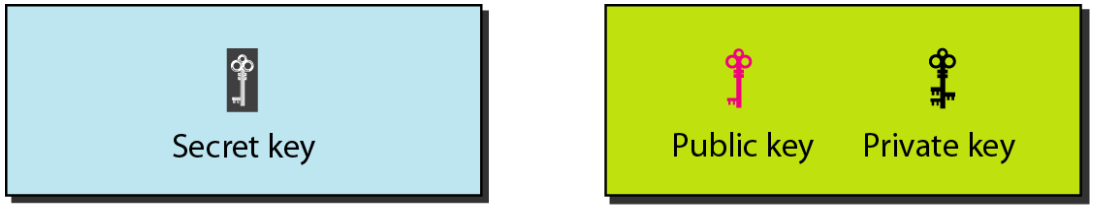


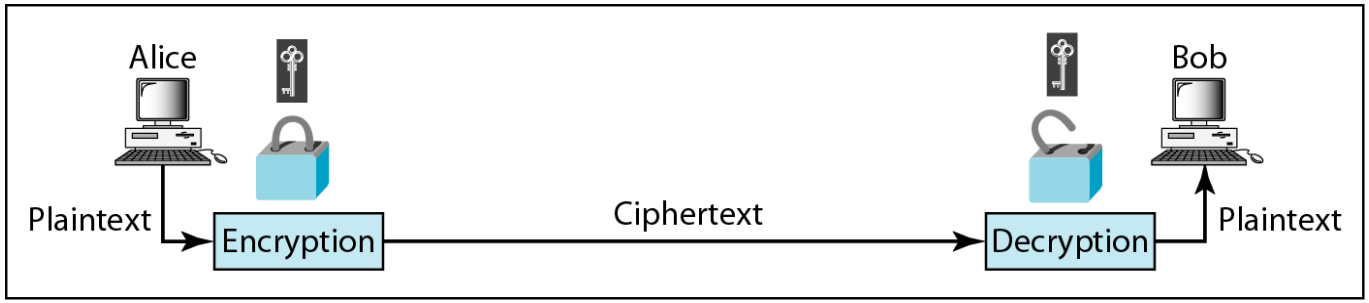
Figure 5 *Keys used in cryptography*



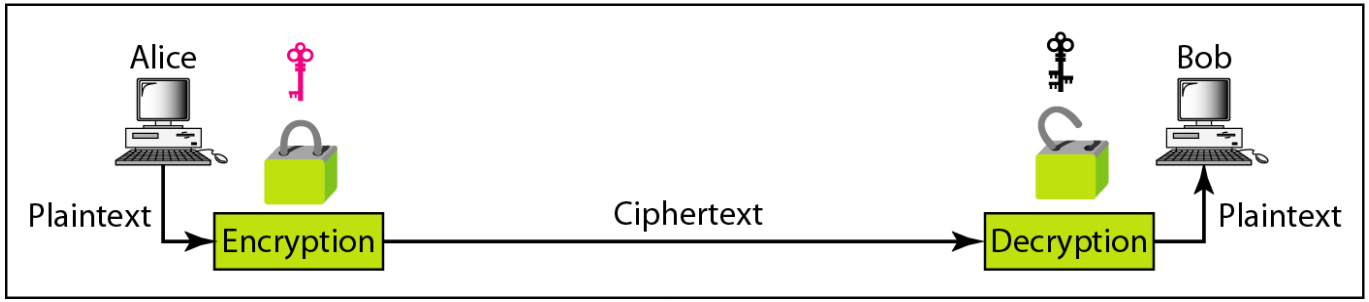
Symmetric-key cryptography

Asymmetric-key cryptography

Figure 6 *Comparison between two categories of cryptography*



a. Symmetric-key cryptography



b. Asymmetric-key cryptography

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

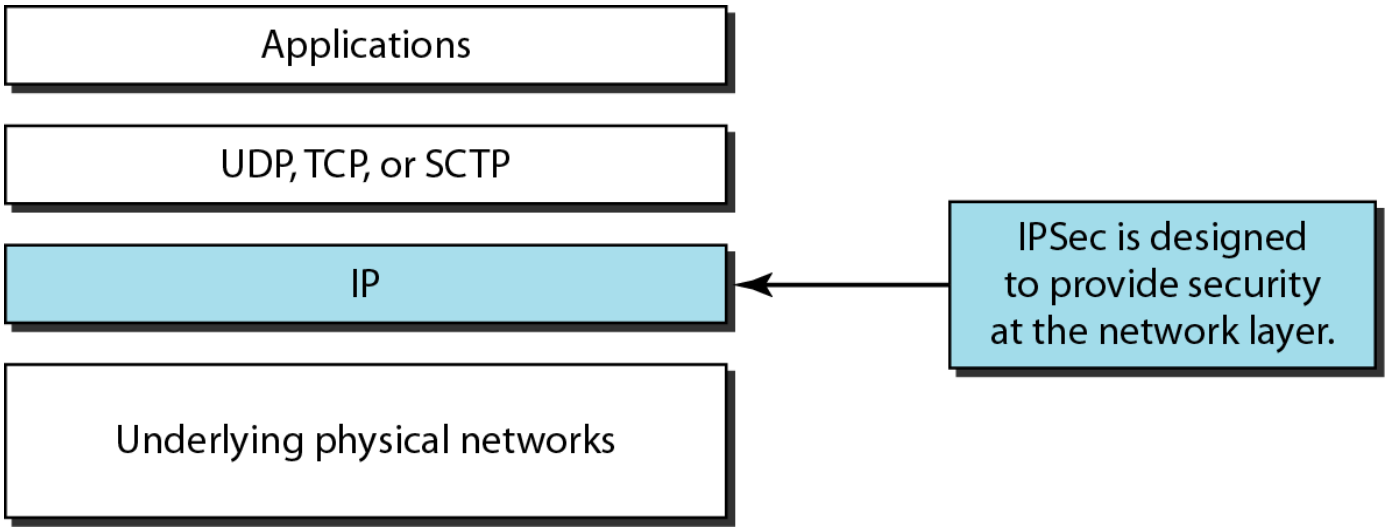
Internet security is normally applied at three layers in the Internet: the network layer, the transport layer, and the application layer.

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, such as routing protocols. Those applications that use the service of UDP can also benefit from this service because UDP is a connectionless protocol and transport-layer security protocols, as we discuss later, cannot be applied to UDP.

IPSec

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.

Figure 7 *TCP/IP protocol suite and IPSec*



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

Transport mode is normally used when we need host-to-host (end-to-end) protection of data. The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer. The receiving host uses IPSec to check the authentication and/or decrypt the **IP** packet and deliver it to the transport layer.

IPSec in tunnel mode protects the original IP header.

Tunnel mode is normally used between two routers, between a host and a router, or between a router and a host.

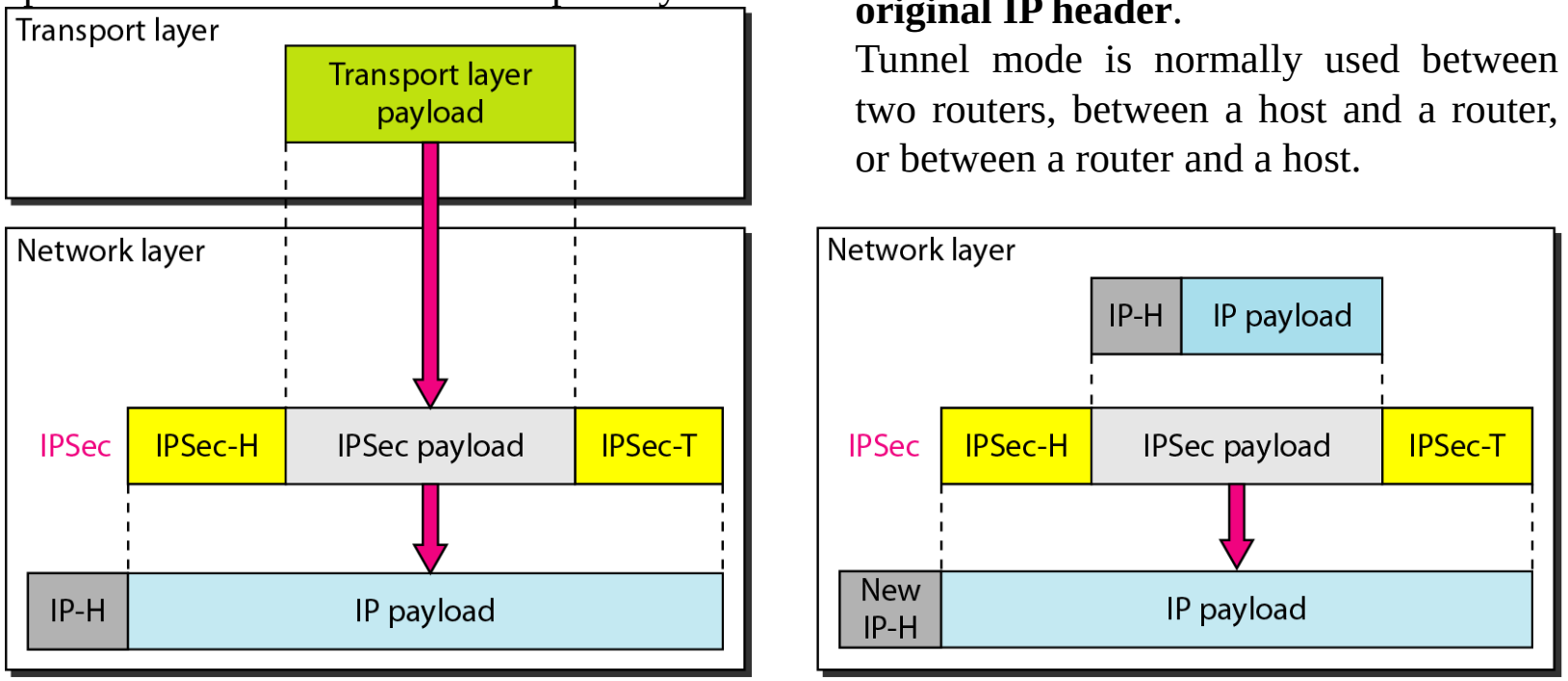


Figure 8 ***Transport mode and tunnel modes of IPSec protocol***

Figure 9 *Transport mode in action*

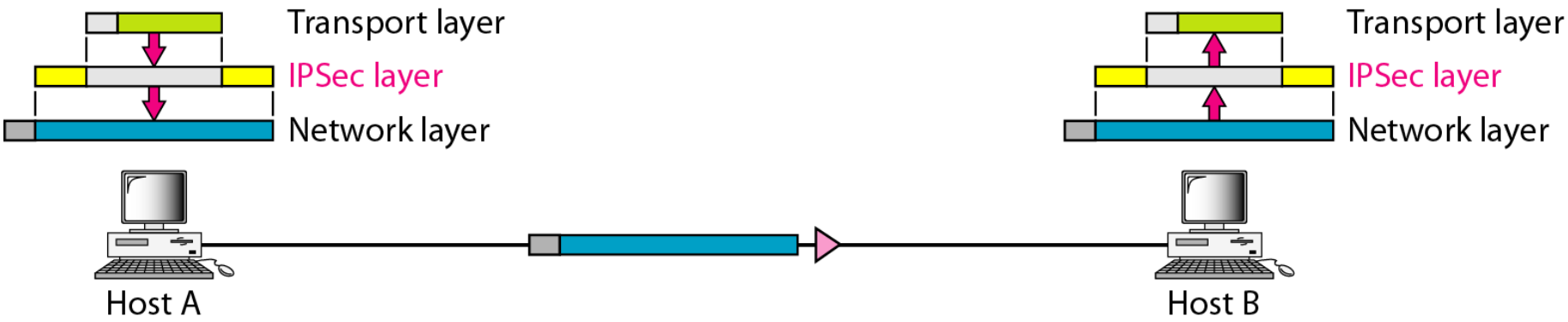
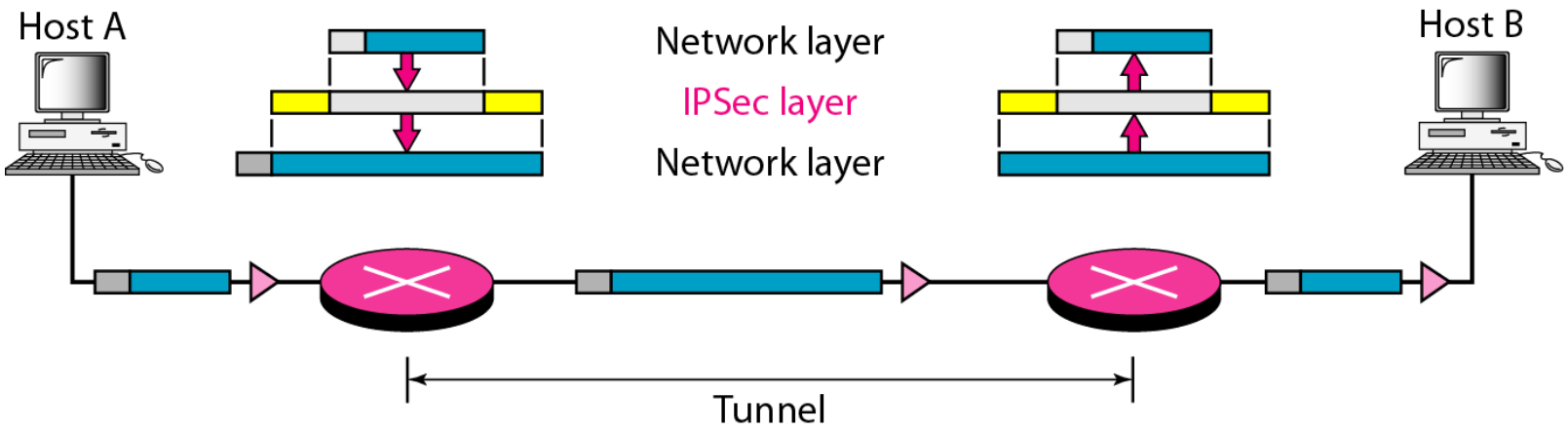


Figure 10 *Tunnel mode in action*



Note

IPSec in tunnel mode protects the original IP header.

Figure 11 *Private network*

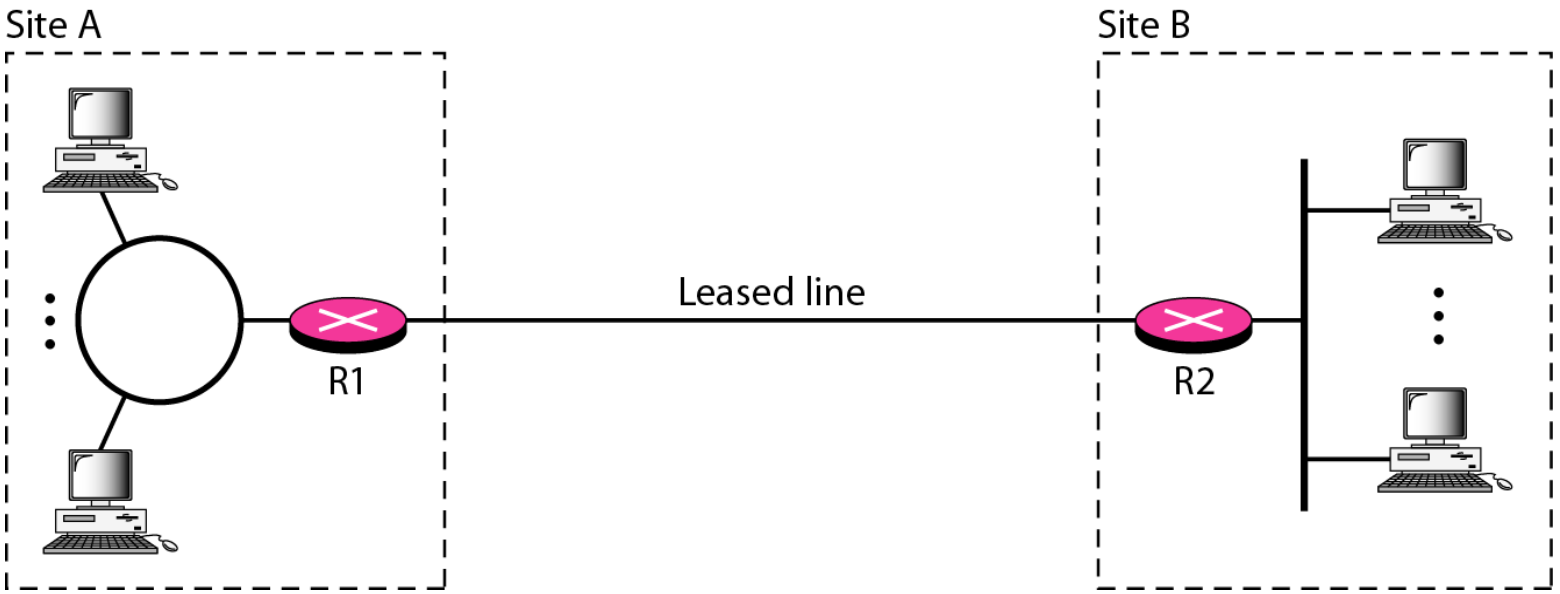


Figure 12 *Hybrid network*

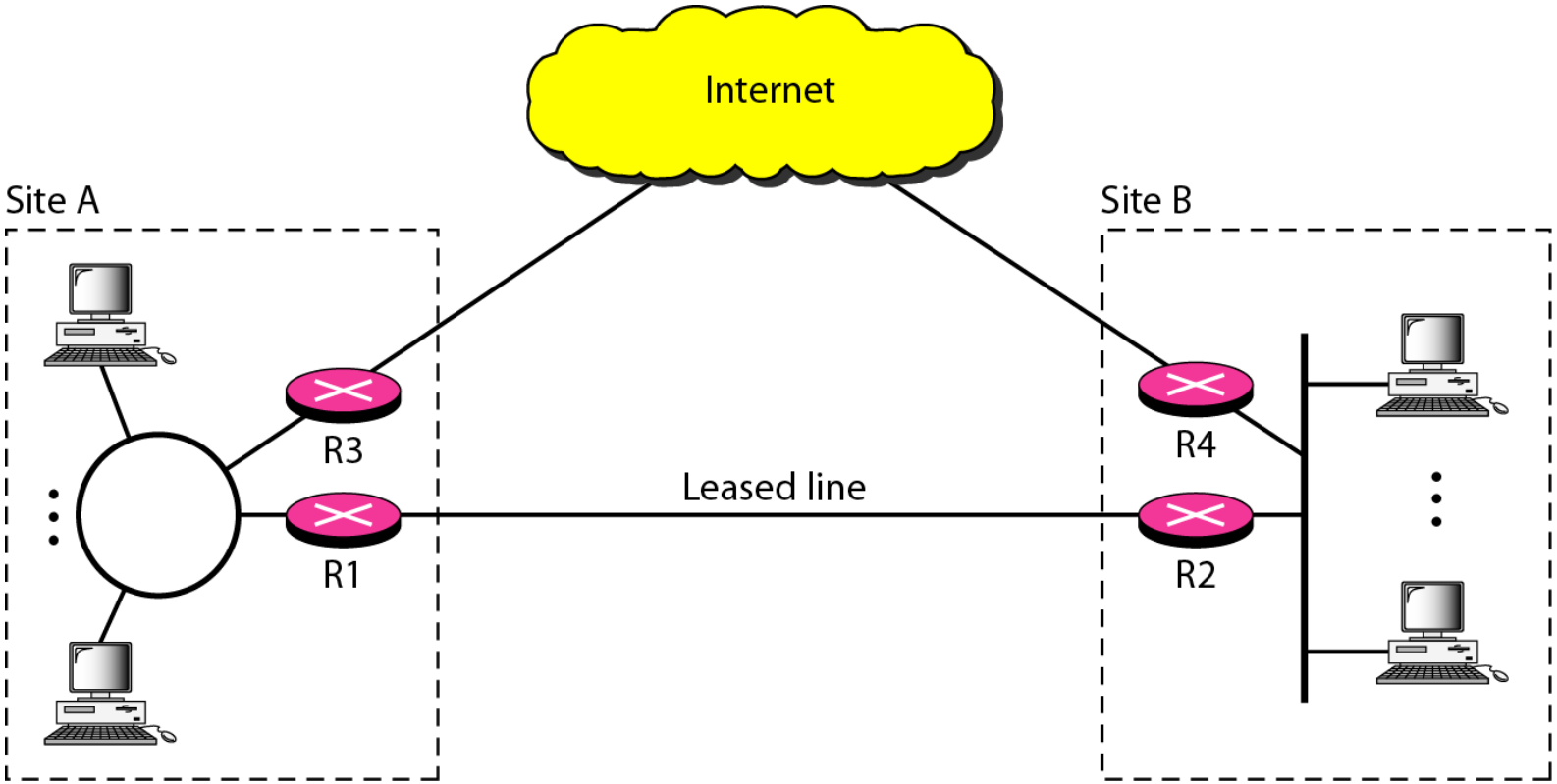


Figure 13 *Virtual private network*

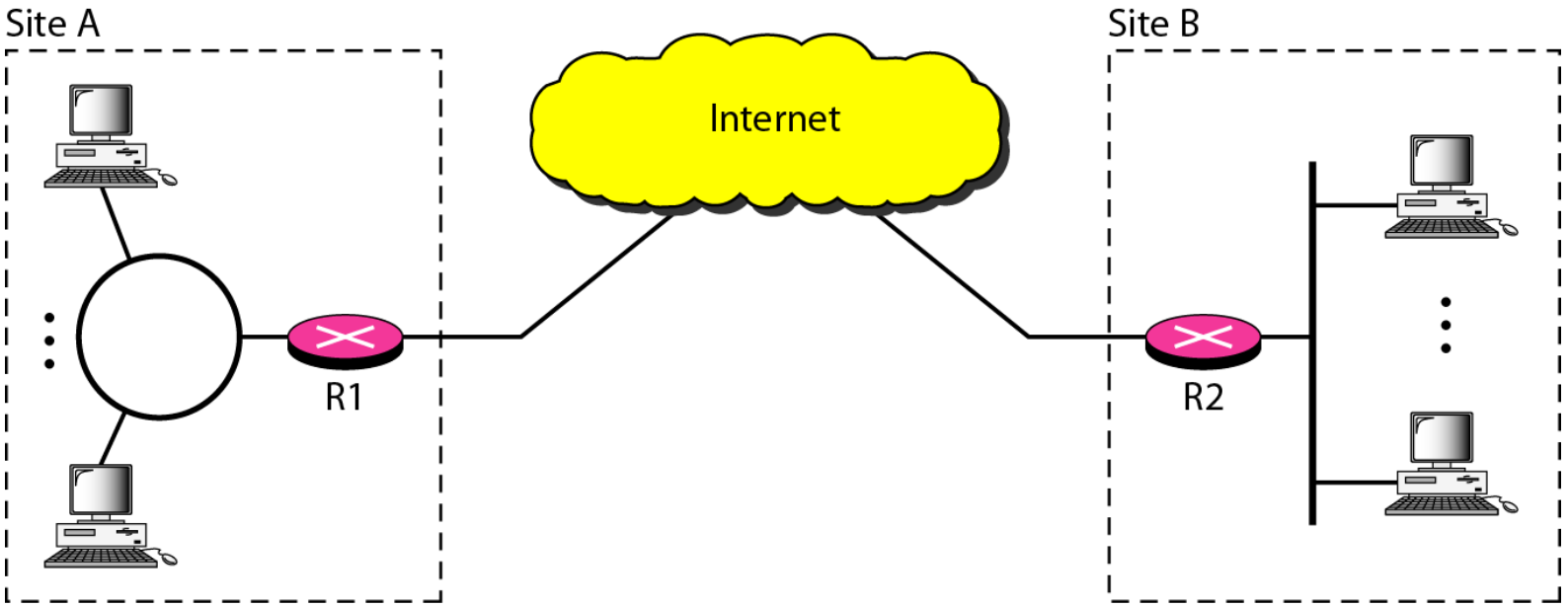
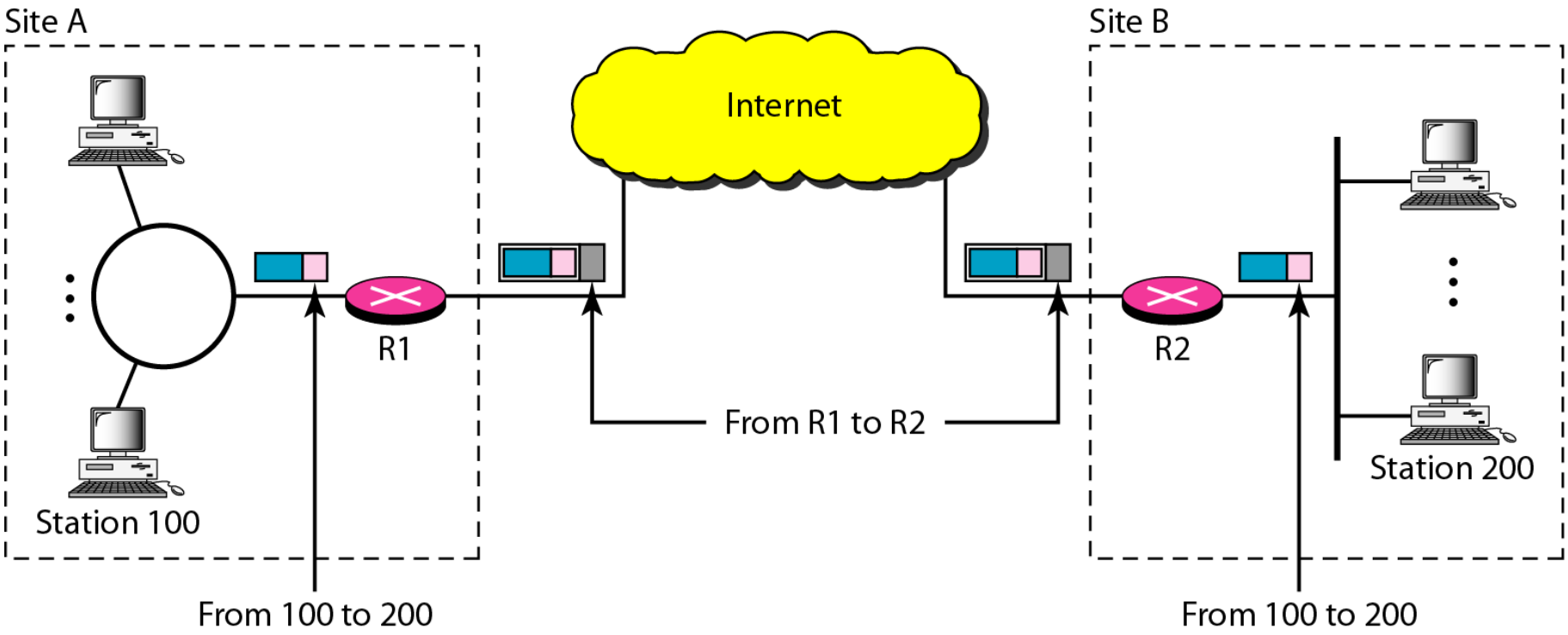


Figure 14 *Addressing in a VPN*



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.

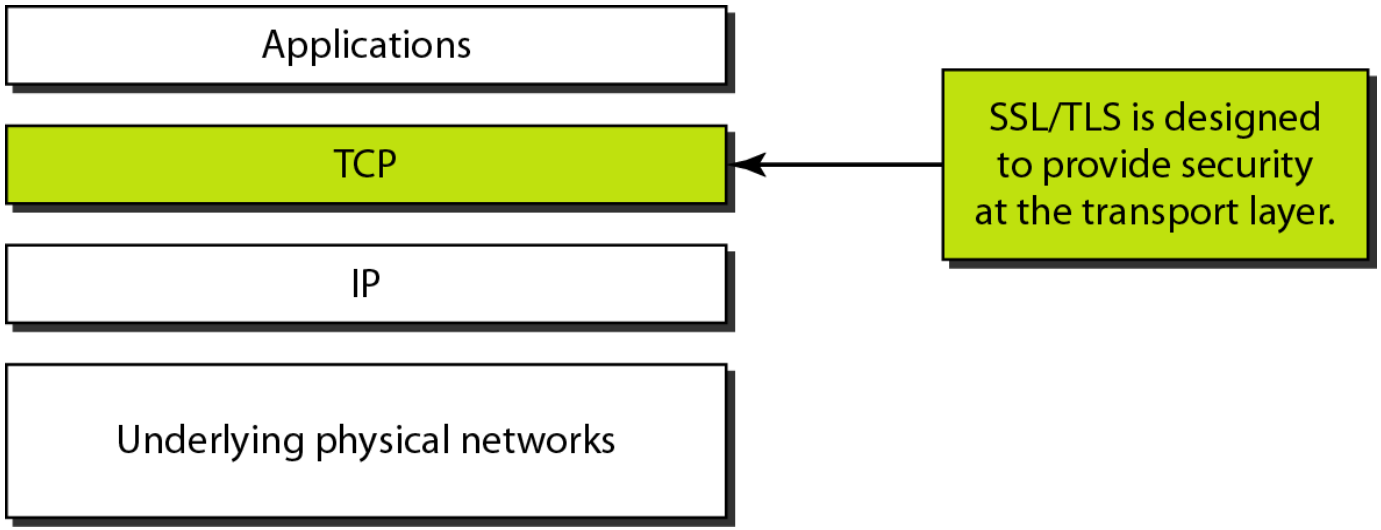


Figure 15 *Location of SSL and TLS in the Internet model*

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.

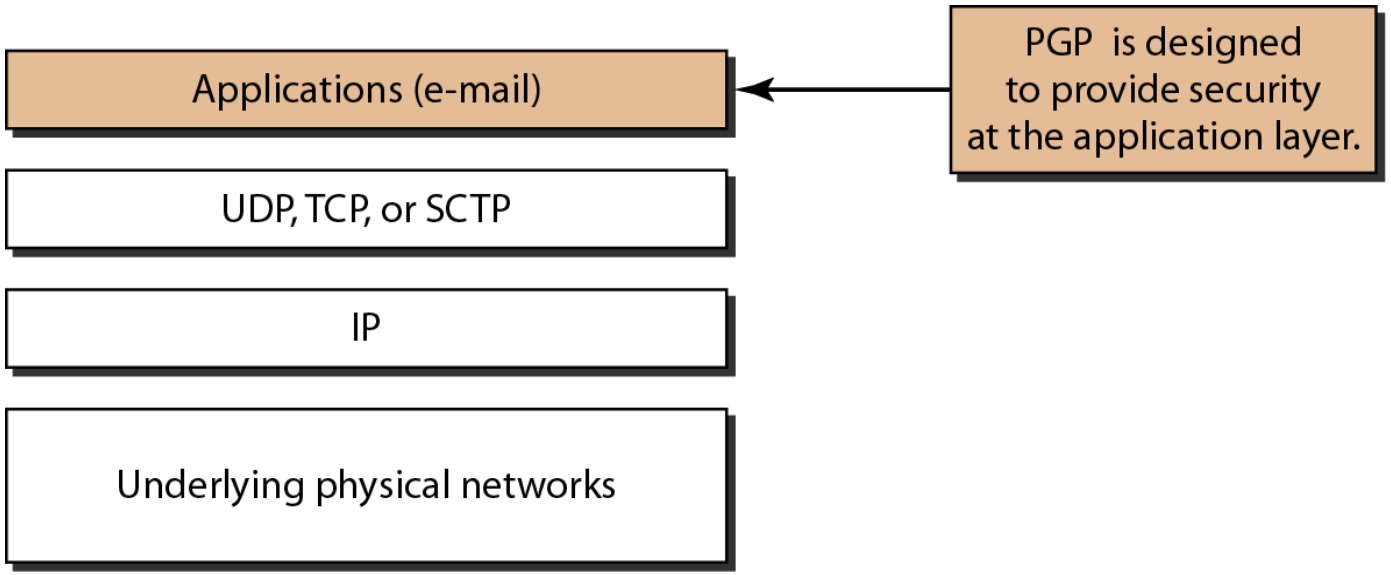


Figure 16 ***Position of PGP in the TCP/IP protocol suite***

Note

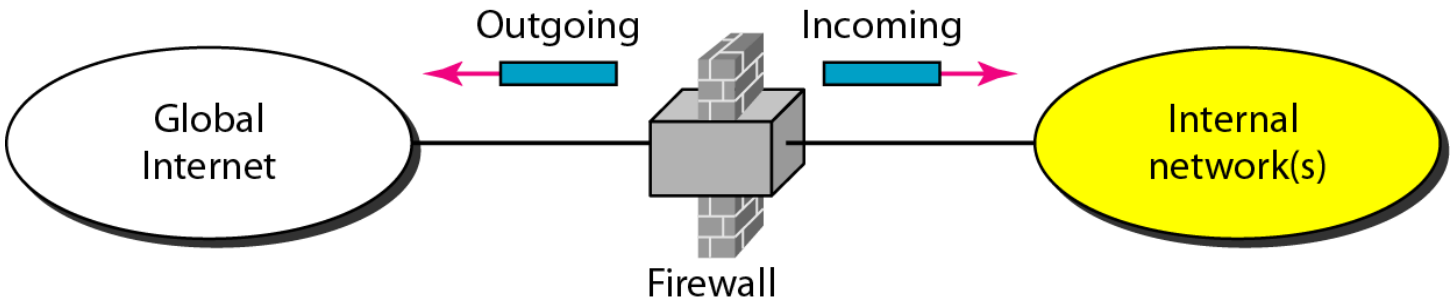
In PGP, the sender of the message needs to include the identifiers of the algorithms used in the message as well as the values of the keys.

Table *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

FIREWALLS

All previous security measures cannot prevent a person 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) or software 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.



For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization. A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

Note

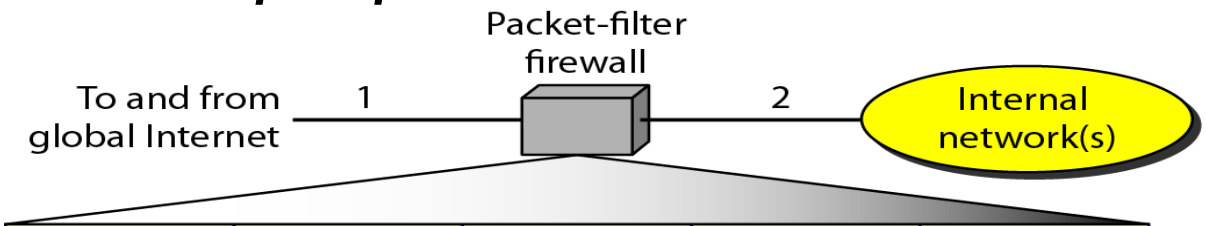
A packet-filter firewall filters at the network or transport layer.

Note

A proxy firewall filters at the application layer.

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). Figure 16 shows an example of a filtering table for this kind of a firewall.

Figure 16 *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	*	*

According to the figure, the following packets are filtered:

1. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the * (asterisk) means "any."
2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
3. Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.
4. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

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 policies regarding its web pages: only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked.

In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).

One solution is to install a proxy firewall (computer) (sometimes called an *application gateway),* which stands between the customer computer and the corporation computer. When the user client process sends a message, the application gateway runs a server process to receive the request. The server opens the packet at the application level and finds out if the request is legitimate. If it is, the server acts as a client process and sends the message to the real server in the corporation. If it is not, the message is dropped and an error message is sent to the external user. In this way, the requests of the external users are filtered based on the contents at the application layer. Figure 17 shows an application gateway implementation for HTTP.

Figure 17 *Proxy firewall*