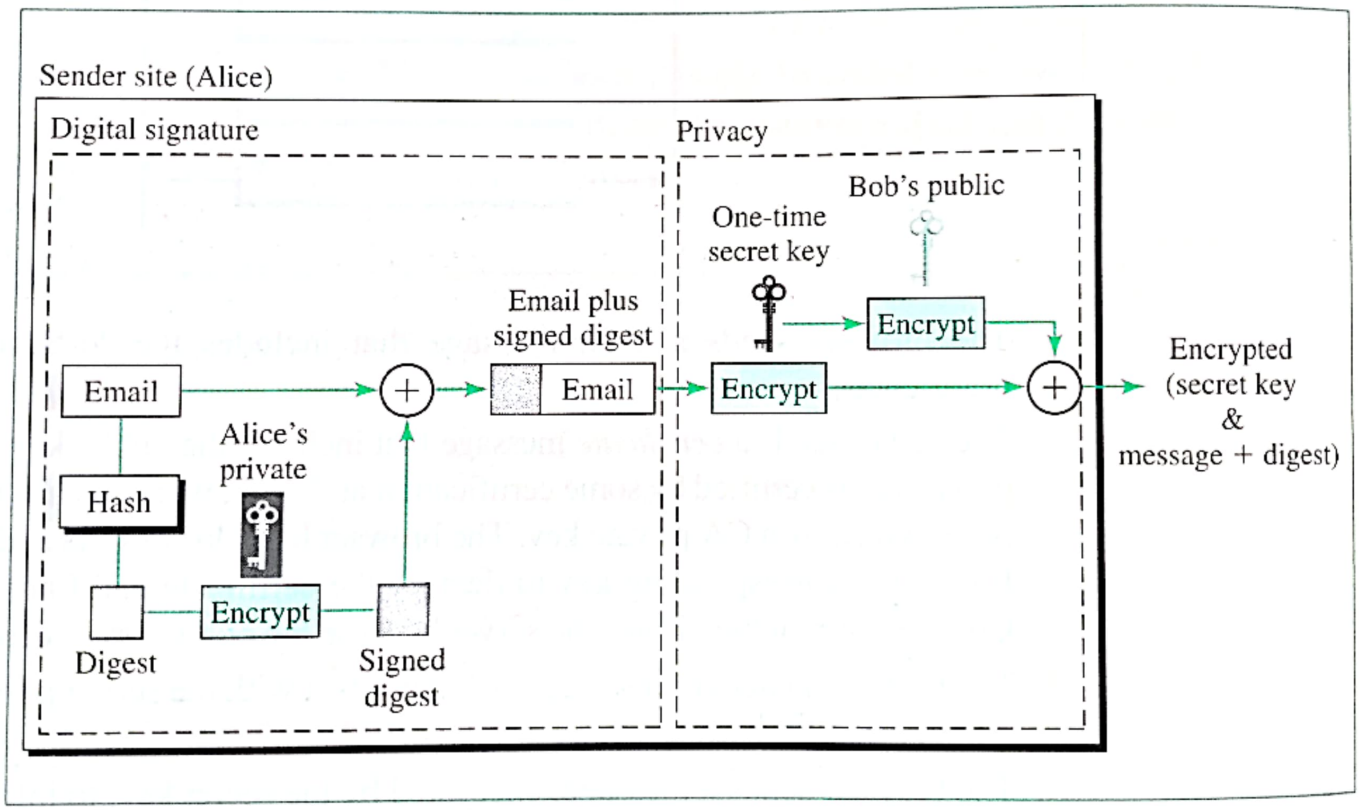
31.3 APPLICATION LAYER SECURITY: PGP

The implementation of security at the application layer is more feasible and simpler, particularly when the Internet communication involves only two parties, as in the case of email and TELNET. The sender and the receiver can agree to use the same protocol and to use any type of security services they desire. In this section, we discuss one protocol used at the application layer to provide security: PGP.

Pretty Good Privacy (PGP) was invented by Phil Zimmermann to provide all four aspects of security (privacy, integrity, authentication, and nonrepudiation) in the sending of email.

PGP uses digital signature (a combination of hashing and public-key encryption) to provide integrity, authentication, and nonrepudiation. It uses a combination of secret-key and public-key encryption to provide privacy. Specifically, it uses one hash function, one secret key, and two private-public key pairs. See Figure 31.7.

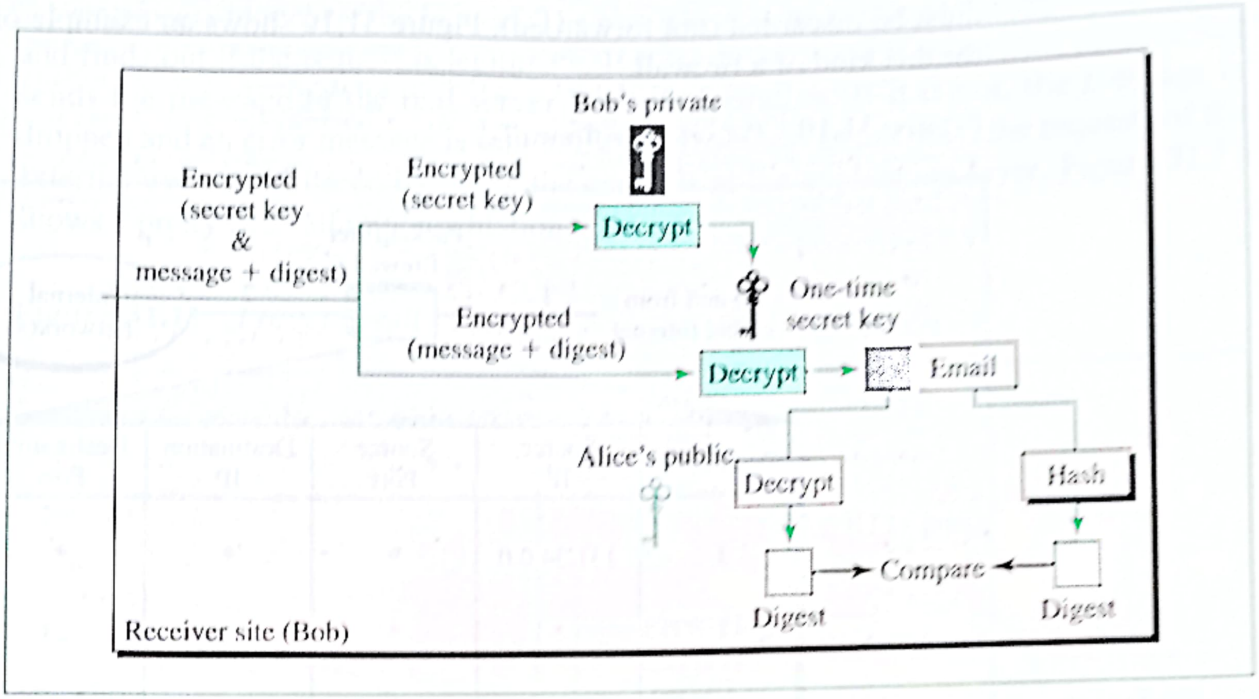
Figure 31.7 *PGP at the sender site*



The figure shows how PGP creates secure email at the sender site. The email message is hashed to create a digest. The digest is encrypted (signed) using Alice's private key. The message and the digest are encrypted using the one-time secret key created by Alice. The secret key is encrypted using Bob's public key and is sent together with the encrypted combination of message and digest.

Figure 31.8 shows how PGP uses hashing and a combination of three keys to extract the original message at the receiver site. The combination of encrypted secret key and message plus digest is received. The encrypted secret key first is decrypted (using Bob's private key) to get the one-time secret key created by Alice. The secret key then is used to decrypt the combination of the message plus digest.

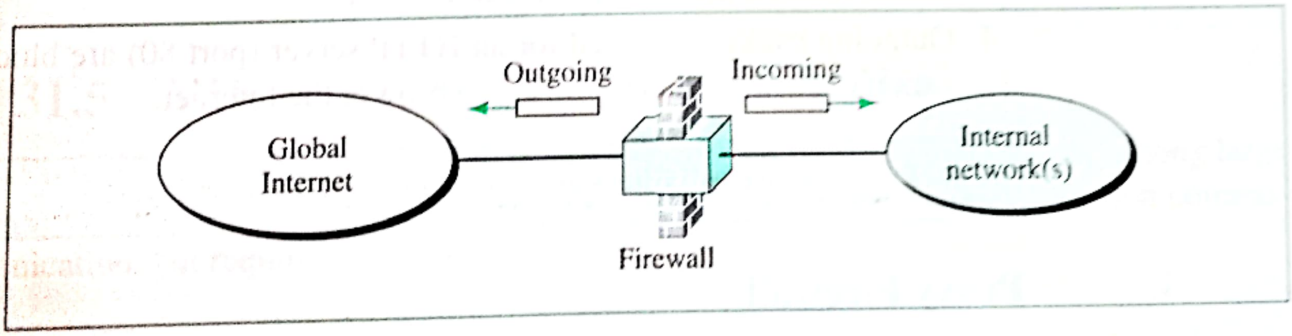
Figure 31.8 *PGP at the receiver site*



31.4 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 (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. Figure 31.9 shows a firewall.

Figure 31.9 *Firewall*



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.

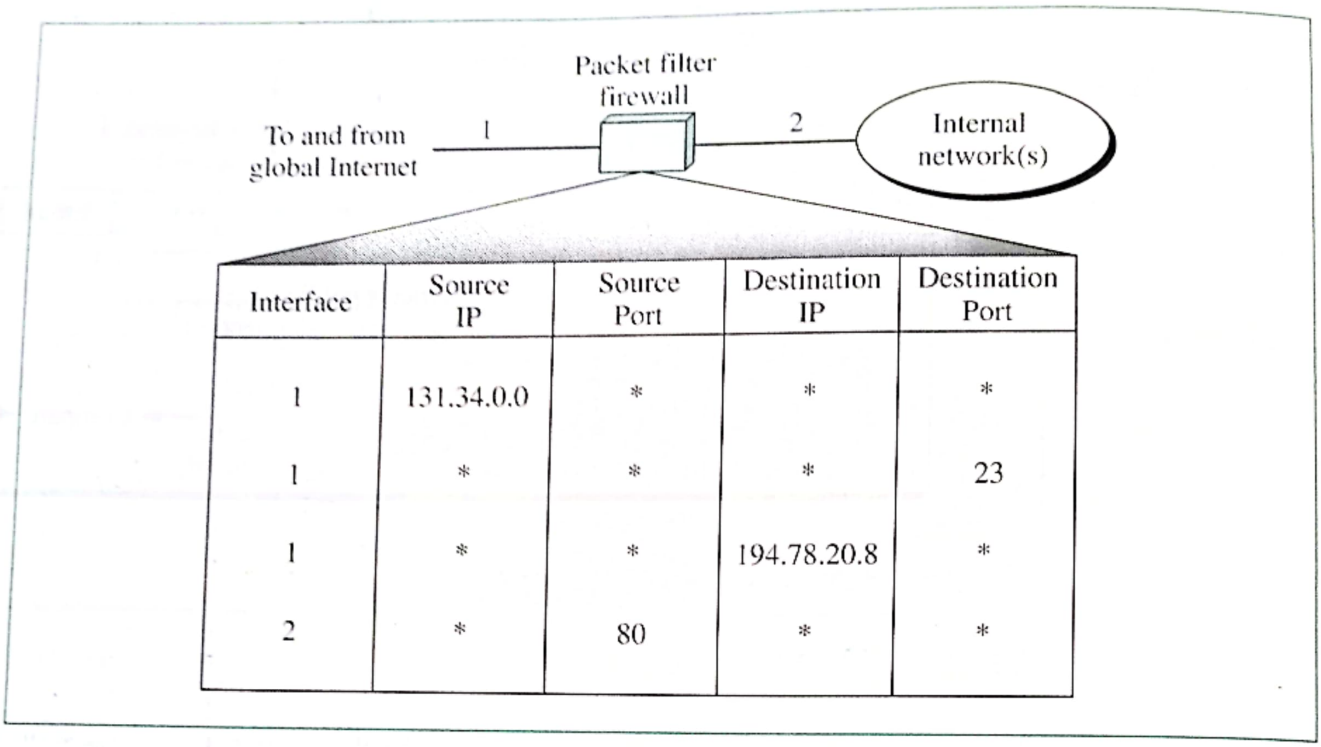
A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

Packet-Filter Firewall

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 packet must be discarded (not forwarded). Figure 31.10 shows an example of a filtering table for this kind of a firewall.

Figure 31.10 *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.

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

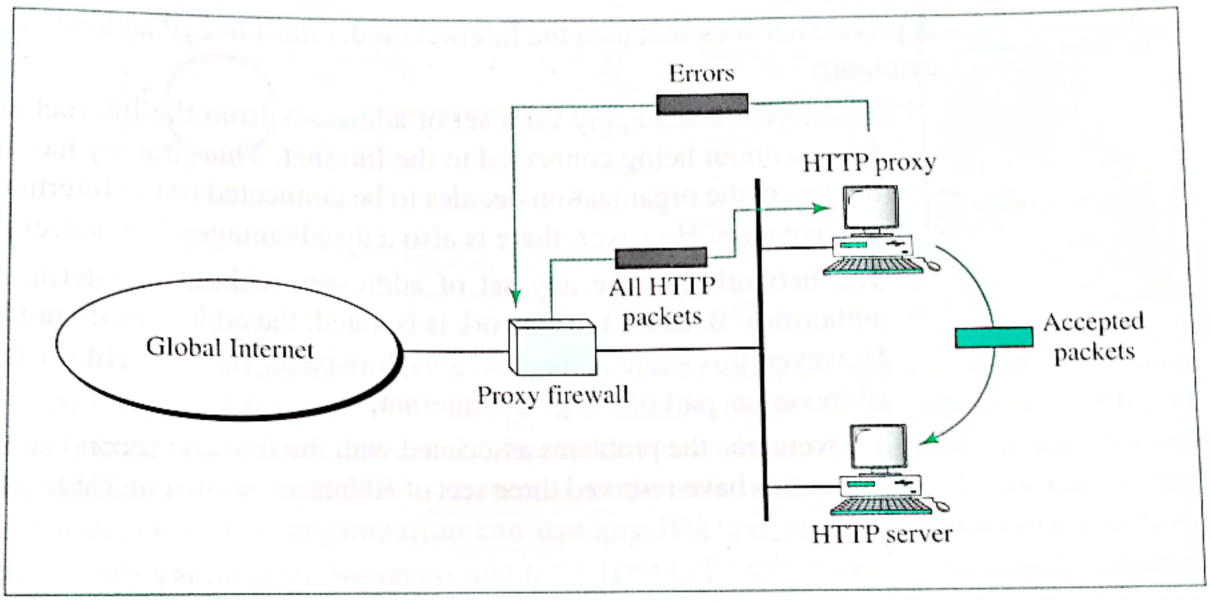
Proxy Firewall

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 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 computer (sometimes called an application gateway), which stands between the customer (user client) computer and the corporation

computer. When the user client process sends a message, the **proxy firewall** 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 31.11 shows a proxy firewall implementation.

Figure 31.11 *Proxy firewall*



A proxy firewall filters at the application layer.

31.5 VIRTUAL PRIVATE NETWORK

Virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and interorganization communication, but require privacy in their internal communication.

Private Networks

A private network is designed for use inside an organization. It allows access to shared resources and, at the same time, provides privacy. Before we discuss some aspects of these networks, let us define two commonly used related terms: *intranet* and *extranet*.

Intranet

An **intranet** is a private network (LAN) that uses the Internet model. However, access to the network is limited to the users inside the organization. The network uses application programs defined for the global Internet, such as HTTP, and may have Web servers, and so on.

Extranet

An **extranet** is the same as an intranet with one major difference: Some resources may be accessed by specific groups of users outside the organization under the control of the network administrator. For example, an organization may allow authorized customers access to product specifications, availability, and online ordering. A university or a college can allow distance learning students access to the computer lab after passwords have been checked.

Addressing

A private network that uses the Internet model must use IP addresses. Three choices are available:

1. The network can apply for a set of addresses from the Internet authorities and use them without being connected to the Internet. This strategy has an advantage. If in the future the organization decides to be connected to the Internet, it can do so with relative ease. However, there is also a disadvantage: The address space is wasted.
2. The network can use any set of addresses without registering with the Internet authorities. Because the network is isolated, the addresses do not have to be unique. However, this strategy has a serious drawback: Users might mistakenly confuse the addresses as part of the global Internet.
3. To overcome the problems associated with the first and second strategies, the Internet authorities have reserved three sets of addresses, shown in Table 31.1.

Table 31.1 *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}

Any organization can use an address out of this set without permission from the Internet authorities. Everybody knows that these reserved addresses are for private networks. They are unique inside the organization, but they are not unique globally. No router will forward a packet that has one of these addresses as the destination address.

Achieving Privacy

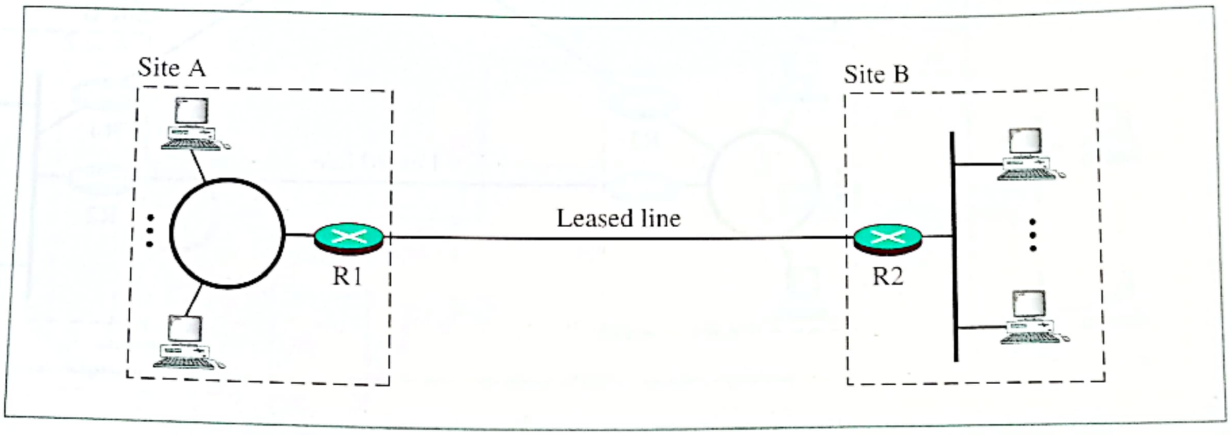
To achieve privacy, organizations can use one of three strategies: private networks, hybrid networks, and virtual private networks.

Private Networks

An organization that needs privacy when routing information inside the organization can use a **private network** as discussed previously. A small organization with one single site can use an isolated LAN. People inside the organization can send data to one another that totally remain inside the organization, secure from outsiders. A larger organization with

several sites can create a private internet. The LANs at different sites can be connected to each other using routers and leased lines. In other words, an internet can be made out of private LANs and private WANs. Figure 31.12 shows such a situation for an organization with two sites. The LANs are connected to each other using routers and one leased line.

Figure 31.12 *Private network*



In this situation, the organization has created a private internet that is totally isolated from the global Internet. For end-to-end communication between stations at different sites, the organization can use the Internet model. However, there is no need for the organization to apply for IP addresses with the Internet authorities. It can use private IP addresses. The organization can use any IP class and assign network and host addresses internally. Because the internet is private, duplication of addresses by another organization in the global Internet is not a problem.

Hybrid Networks

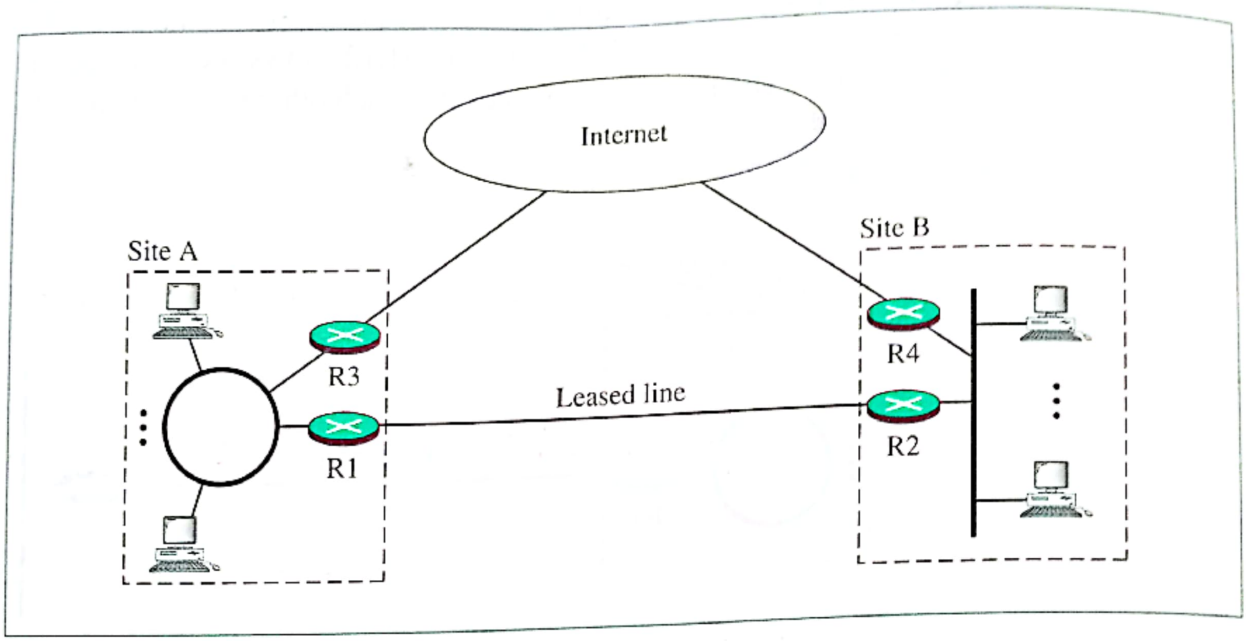
Today, most organizations need to have privacy in intraorganization data exchange, but, at the same time, they need to be connected to the global Internet for data exchange with other organizations. One solution is the use of a **hybrid network.** A hybrid network allows an organization to have its own private internet and, at the same time, access to the global Internet. Intraorganization data are routed through the private internet; interorganization data are routed through the global Internet. Figure 31.13 shows an example of this situation.

An organization with two sites uses routers R1 and R2 to connect the two sites privately through a leased line; it uses routers R3 and R4 to connect the two sites to the rest of the world. The organization uses global IP addresses for both types of communication. However, packets destined for internal recipients are routed only through routers R1 and R2. Routers R3 and R4 route the packets destined for outsiders.

Virtual Private Networks

Both private and hybrid networks have a major drawback: cost. Private wide-area networks (WANs) are expensive. To connect several sites, an organization needs several leased lines, which means a high monthly fee. One solution is to use the global Internet for both private and public communications. A technology called virtual private network (VPN) allows organizations to use the global Internet for both purposes.

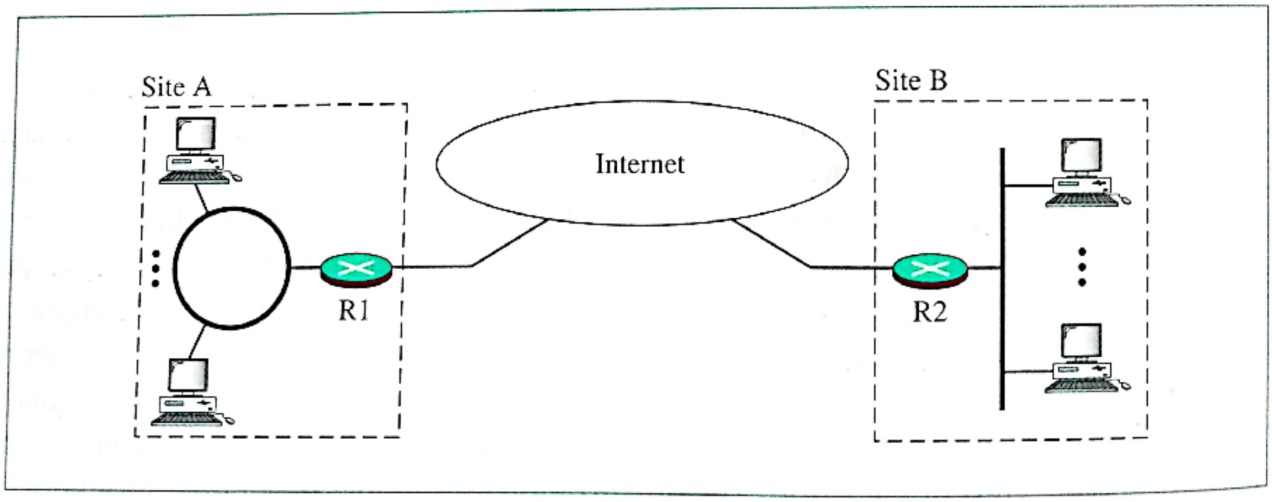
Figure 31.13 *Hybrid network*



VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.

Figure 31.14 shows the idea of a virtual private network. Routers R1 and R2 use VPN technology to guarantee privacy for the organization.

Figure 31.14 *Virtual private network*



VPN Technology

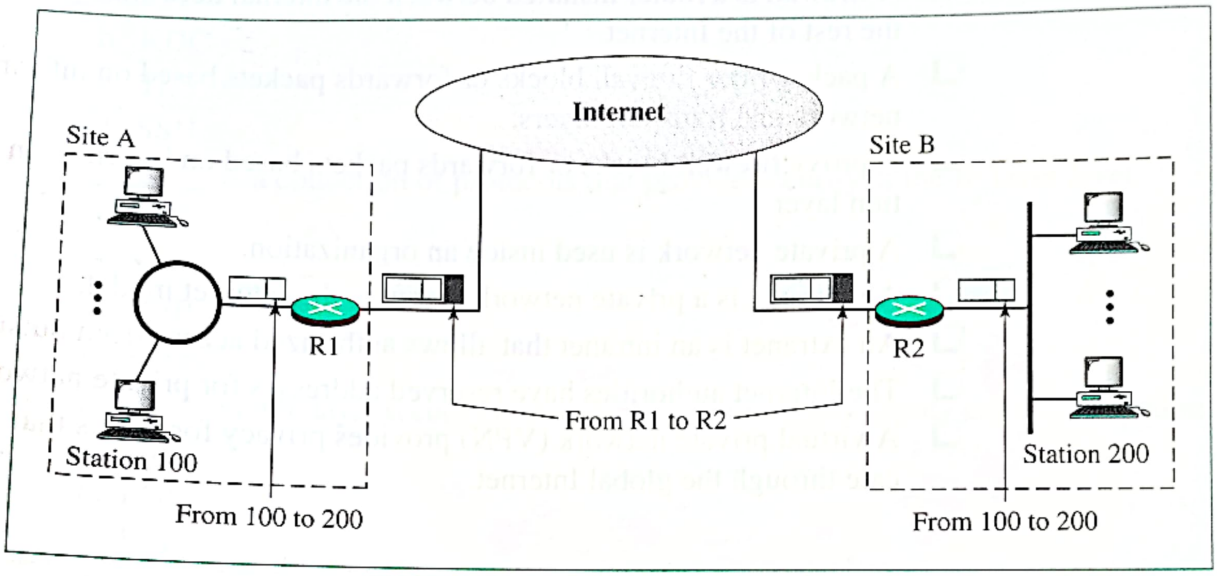
VPN technology uses IPSec in the tunnel mode to provide authentication, integrity, and privacy.

Tunneling

To guarantee privacy and other security measures for an organization, VPN can use the IPSec in the tunnel mode. In this mode, each IP datagram destined for private use in the

organization is encapsulated in another datagram. To use IPSec in the **tunneling** mode, the VPNs need to use two sets of addressing, as shown in Figure 31.15.

Figure 31.15 *Addressing in a VPN*



The public network (Internet) is responsible for carrying the packet from R1 to R2. Outsiders cannot decipher the contents of the packet or the source and destination addresses. Deciphering takes place at R2, which finds the destination address of the packet and delivers it.

31.6 KEY TERMS

Authentication Header (AH) protocol
data exchange protocol
Encapsulating Security Payload (ESP)
extranet
firewall
handshake protocol
hybrid network
intranet
IP Security (IPSec)
packet-filter firewall
Pretty Good Privacy (PGP)
private network
proxy firewall
Security Association (SA)
Transport Layer Security (TLS)
tunneling
virtual private network (VPN)

31.7 SUMMARY

- Security methods can be applied in the application layer, transport layer, and IP layer.
- IP Security (IPSec) is a collection of protocols designed by the IETF to provide security for an Internet packet.
- The Authentication Header protocol provides integrity and message authentication.
- The Encapsulating Security Payload protocol provides integrity, message authenti-