**6.Security Technology: Firewalls and VPNs**

**Access control**

Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization—that is, information systems, restricted areas such as computer rooms, and the entire physical location. Access control is achieved by means of a combination of policies, programs, and technologies.

Access controls can be mandatory, nondiscretionary, or discretionary.

* **Mandatory access controls (MACs)** use data classification schemes; they give users and data owners limited control over access to information resources. In a data classification scheme, each collection of information is rated, and each user is rated to specify the level of information that user may access. These ratings are often referred to as sensitivity levels, and they indicate the level of confidentiality the information requires. A variation of this form of access control is called lattice-based access control, in which users are assigned a matrix of authorizations for particular areas of access.

The lattice structure contains subjects and objects, and the boundaries associated with each pair are demarcated. Lattice-based control specifies the level of access each subject has to each object. With this type of control, the column of attributes associated with a particular object (such as a printer) is referred to as an access control list (ACL). The row of attributes associated with a particular subject (such as a user) is referred to as a capabilities table.

* **Nondiscretionary controls** are a strictly-enforced version of MACs that are managed by a central authority in the organization and can be based on an individual’s role—role-based controls—or a specified set of tasks (subject- or object-based)—task-based controls. Role based controls are tied to the role a user performs in an organization, and task-based controls are tied to a particular assignment or responsibility.

The role and task controls make it easier to maintain the controls and restrictions associated with a particular role or task, especially if the individual performing the role or task changes often. Instead of constantly assigning and revoking the privileges of individuals who come and go, the administrator simply assigns the associated access rights to the role or task, and then whenever individuals are associated with that role or task, they automatically receive the corresponding access. When their turns are over, they are removed from the role or task and the access is revoked.

* **Discretionary access controls (DACs)** are implemented at the discretion or option of the data user. The ability to share resources in a peer-to-peer configuration allows users to control and possibly provide access to information or resources at their disposal. The users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access these resources.

For example, a user has a hard drive containing information to be shared with office coworkers. This user can elect to allow access to specific individuals by providing access, by name, in the share control function.

**All access control approaches rely on as the following mechanisms:**

* **Identification** is a mechanism whereby an unverified entity—called a supplicant—that seeks access to a resource proposes a label by which they are known to the system. The label applied to the supplicant is called an identifier (ID), and must be mapped to one and only one entity within the security domain.

Some organizations use composite identifiers, concatenating elements—department codes, random numbers, or special characters—to make unique identifiers within the security domain. Other organizations generate random IDs to protect the resources from potential attackers. Most organizations use a single piece of unique information, such as a complete name or the user’s first initial and surname.

* **Authentication** is the process of validating a supplicant’s purported identity. There are three widely used authentication mechanisms, or authentication factors:
* **Something a Supplicant Knows** This factor of authentication relies upon what the supplicant knows and can recall—for example, a password, passphrase, or other unique authentication code, such as a personal identification number (PIN).

A password is a private word or combination of characters that only the user should know. A password should be difficult to guess, which means it cannot be a series of letters or a word that is easily associated with the user, such as the name of the user’s spouse, child, or pet. Nor should a password be a series of numbers easily associated with the user, such as a phone number, Social Security number, or birth date. On the other hand, the password must be something the user can easily remember, which means it should be short or easily associated with something the user can remember.

A passphrase is a series of characters, typically longer than a password, from which a virtual password is derived. For example, while a typical password might be “23skedoo,” a typical passphrase might be “MayTheForceBeWithYouAlways,” represented as “MTFBWYA.”

* **Something a Supplicant Has** This authentication factor relies upon something a supplicant has and can produce when necessary. One example is dumb cards, such as ID cards or ATM cards with magnetic stripes containing the digital (and often encrypted) user PIN, against which the number a user input is compared. The smart card contains a computer chip that can verify and validate a number of pieces of information instead of just a PIN.

Another common device is the token, a card or key fob with a computer chip and a liquid crystal display that shows a computer-generated number used to support remote login authentication. Tokens are synchronous or asynchronous. Once synchronous tokens are synchronized with a server, both devices (server and token) use the same time or a time-based database to generate a number that must be entered during the user login phase. Asynchronous tokens, which don’t require that the server and tokens all maintain the same time setting, use a challenge/response system, in which the server challenges the supplicant during login with a numerical sequence. The supplicant places this sequence into the token and receives a response. The prospective user then enters the response into the system to gain access.

* **Something a Supplicant Is or Can Produce** This authentication factor relies upon individual characteristics, such as fingerprints, palm prints, hand topography, hand geometry, or retina and iris scans, or something a supplicant can produce on demand, such as voice patterns, signatures, or keyboard kinetic measurements.
* **Authorization** is the matching of an authenticated entity to a list of information assets and corresponding access levels. This list is usually an ACL or access control matrix.

**Authorization can be handled in one of three ways:**

* Authorization for each authenticated user, in which the system performs an authentication process to verify each entity and then grants access to resources for only that entity. This quickly becomes a complex and resource-intensive process in a computer system.
* Authorization for members of a group, in which the system matches authenticated entities to a list of group memberships, and then grants access to resources based on the group’s access rights. This is the most common authorization method.
* Authorization across multiple systems, in which a central authentication and authorization system verifies entity identity and grants it a set of credentials.

Authorization credentials (sometimes called authorization tickets) are issued by an authenticator and are honored by many or all systems within the authentication domain. Sometimes called single sign-on (SSO) or reduced sign-on, authorization credentials are becoming more common and are frequently enabled using a shared directory structure such as the Lightweight Directory Access Protocol (LDAP).

* **Accountability**, also known as auditability, ensures that all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Accountability is most often accomplished by means of system logs and database journals, and the auditing of these records.

Systems logs record specific information, such as failed access attempts and systems modifications. Logs have many uses, such as intrusion detection, determining the root cause of a system failure, or simply tracking the use of a particular resource.

**Firewalls**

A firewall in an information security program is similar to a building’s firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network (for example, the Internet), and the inside world, known as the trusted network. The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices.

**Firewalls can be categorized by processing mode, development era, or structure**.

* **Firewall Processing Modes**

Firewalls fall into five major processing-mode categories: packet-filtering firewalls, application gateways, circuit gateways, MAC layer firewalls, and hybrids.1 Hybrid firewalls use a combination of the other four modes, and in practice, most firewalls fall into this category, since most firewall implementations use multiple approaches.

**Protecting the Remote Connection**

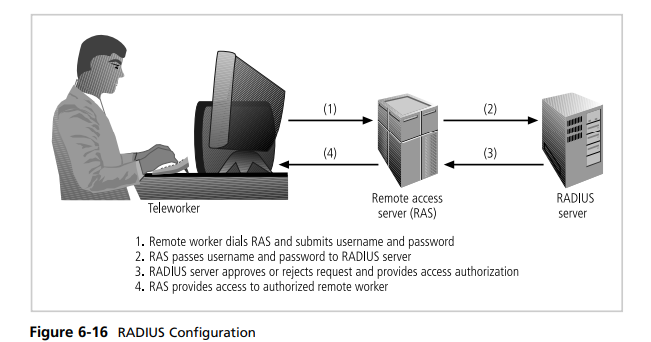
When connections are made between one network and another, the connections are arranged and managed carefully. Installing such network connections requires using leased lines or other data channels provided by common carriers, and therefore these connections are usually permanent and secured under the requirements of a formal service agreement. But when individuals—whether they be employees in their homes, contract workers hired for specific assignments, or other workers who are traveling—seek to connect to an organization’s network(s), a more flexible option must be provided. In the past, organizations provided these remote connections exclusively through dial-up services like Remote Authentication Service (RAS). Since the Internet has become more widespread in recent years, other options such as virtual private networks (VPNs) have become more popular.

**Remote Access**

Before the Internet emerged, organizations created private networks and allowed individuals and other organizations to connect to them using dial-up or leased line connections. The connections between company networks and the Internet use firewalls to safeguard that interface. It is a widely held view that these unsecured, dial-up connection points represent a substantial exposure to attack. An attacker who suspects that an organization has dial-up lines can use a device called a war dialer to locate the connection points.

A war dialer is an automatic phone-dialing program that dials every number in a configured range (e.g., 555-1000 to 555-2000), and checks to see if a person, answering machine, or modem picks up. If a modem answers, the war dialer program makes a note of the number and then moves to the next target number. The attacker then attempts to hack into the network via the identified modem connection using a variety of techniques. Dial-up network connectivity is usually less sophisticated than that deployed with Internet connections. For the most part, simple username and password schemes are the only means of authentication. However, some technologies, such as RADIUS systems, TACACS, and CHAP password systems, have improved the authentication process, and there are even systems now that use strong encryption.

* **RADIUS, TACACS, and Diameter** RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization’s network via a dial-up connection. Typical dial-up systems place the responsibility for the authentication of users on the system directly connected to the modems.
* **The Remote Authentication Dial-In User Service (RADIUS)** system centralizes the management of user authentication by placing the responsibility for authenticating each user in the central RADIUS server. When a remote access server (RAS) receives a request for a network connection from a dial-up client, it passes the request, along with the user’s credentials, to the RADIUS server. RADIUS then validates the credentials and passes the resulting decision (accept or deny) back to the accepting remote access server. Figure 6-16 shows the typical configuration of an RAS system.

****

* The **Diameter** protocol defines the minimum requirements for a system that provides authentication, authorization, and accounting (AAA) services and can go beyond these basics and add commands and/or object attributes. Diameter security uses existing encryption standards including Internet Protocol Security (IPSec) or Transport Layer Security (TLS), both well-regarded protocols, and its cryptographic capabilities are extensible and will be able to use future encryption protocols as they are implemented. Diameter capable devices are emerging into the marketplace and this protocol is expected to become the dominant form of AAA services.
* The **Terminal Access Controller Access Control System (TACACS)** is another remote access authorization system that is based on a client/server configuration. Like RADIUS, it contains a centralized database, and it validates the user’s credentials at this TACACS server. There are three versions of TACACS: TACACS, Extended TACACS, and TACACS+.

The original version combines authentication and authorization services. The extended version separates the steps needed to authenticate the individual or system attempting access from the steps needed to verify that the authenticated individual or system is allowed to make a given type of connection. The extended version keeps records for accountability, and to ensure that the access attempt is linked to a specific individual or system. The plus version uses dynamic passwords and incorporates two-factor authentication.

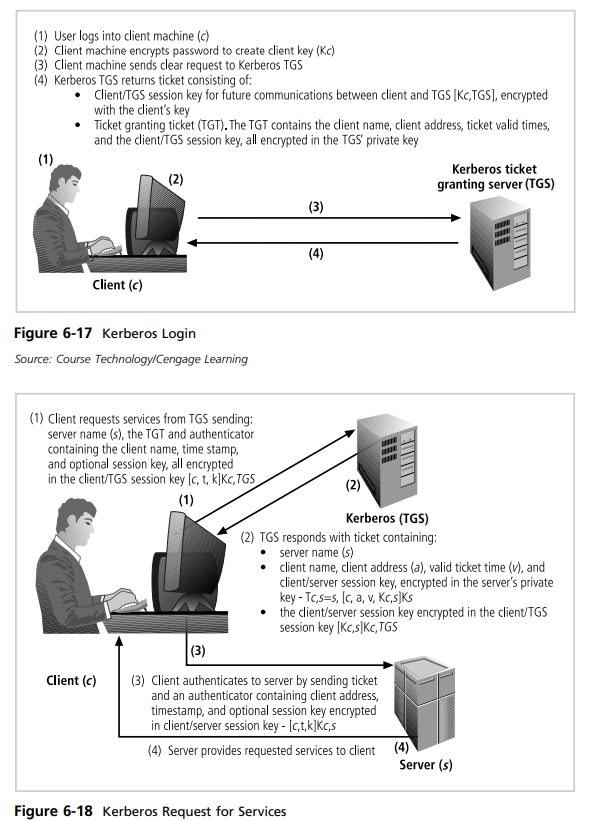
* **Securing Authentication with Kerberos** Two authentication systems can provide secure third-party authentication: Kerberos and SESAME.
* **Kerberos**—named after the threeheaded dog of Greek mythology (spelled Cerberus in Latin) that guards the gates to the underworld—uses symmetric key encryption to validate an individual user to various network resources. Kerberos keeps a database containing the private keys of clients and servers—in the case of a client, this key is simply the client’s encrypted password. Network services running on servers in the network register with Kerberos, as do the clients that use those services. The Kerberos system knows these private keys and can authenticate one network node (client or server) to another.

**Kerberos consists of three interacting services, all of which use a database library:**

1. Authentication server (AS), which is a Kerberos server that authenticates clients and servers.
2. Key Distribution Center (KDC), which generates and issues session keys.
3. Kerberos ticket granting service (TGS), which provides tickets to clients who request services. In Kerberos a ticket is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and therefore authorized to receive services. The ticket consists of the client’s name and network address, a ticket validation starting and ending time, and the session key, all encrypted in the private key of the server from which the client is requesting services

**Kerberos is based on the following principles:**

* The KDC knows the secret keys of all clients and servers on the network.
* The KDC initially exchanges information with the client and server by using these secret keys. Kerberos authenticates a client to a requested service on a server through TGS and by issuing temporary session keys for communications between the client and KDC, the server and KDC, and the client and server.
* Communications then take place between the client and server using these temporary session keys.

****

* **SESAME** The Secure European System for Applications in a Multivendor Environment (SESAME) is the result of a European research and development project partly funded by the European Commission. SESAME is similar to Kerberos in that the user is first authenticated to an authentication server and receives a token. The token is then presented to a privilege attribute server (instead of a ticket granting service as in Kerberos) as proof of identity to gain a privilege attribute certificate (PAC).

A PAC conforms to the standards of the European Computer Manufacturers Association (ECMA) and the International Organization for Standardization/International Telecommunications Union (ISO/ITU-T). SESAME uses public key encryption to distribute secret keys. SESAME also builds on the Kerberos model by adding additional and more sophisticated access control features, more scalable encryption systems, improved manageability, auditing features, and the option to delegate responsibility for allowing access.

**Virtual private networks** **(VPNs)**

Virtual private networks are implementations of cryptographic technology. A virtual private network (VPN) is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network.

The Virtual Private Network Consortium (VPNC) (www.vpnc. org) defines a VPN as “a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.” VPNs are commonly used to securely extend an organization’s internal network connections to remote locations.

**The VPNC defines three VPN technologies: trusted VPNs, secure VPNs, and hybrid VPNs.**

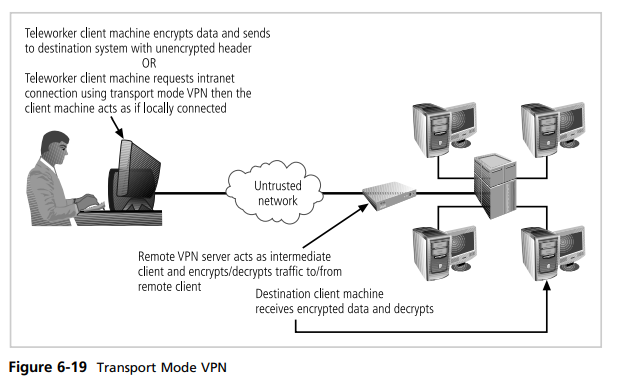
* **A trusted VPN**, also known as a legacy VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits. The organization must trust the service provider, who provides contractual assurance that no one else is allowed to use these circuits and that the circuits are properly maintained and protected—hence the name trusted VPN.
* **Secure VPNs** use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet.
* **A hybrid VPN** combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following, regardless of the specific technologies and protocols being used:

* **Encapsulation** of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network and be usable by the server network environment.
* **Encryption** of incoming and outgoing data to keep the data contents private while in transit over the public network, but usable by the client and server computers and/or the local networks on both ends of the VPN connection.
* **Authentication** of the remote computer and, perhaps, the remote user as well. Authentication and the subsequent authorization of the user to perform specific actions are predicated on accurate and reliable identification of the remote system and/or user.

A VPN allows a user to turn the Internet into a private network. an individual or organization can set up tunneling points across the Internet and send encrypted data back and forth, using the IP-packet-within-an-IP-packet method to transmit data safely and securely. VPNs are simple to set up and maintain and usually require only that the tunneling points be dual-homed—that is, connecting a private network to the Internet or to another outside connection point. There are a number of ways to implement a VPN. IPSec, the dominant protocol used in VPNs, uses either transport mode or tunnel mode. IPSec can be used as a stand-alone protocol, or coupled with the Layer Two Tunneling Protocol (L2TP).

* **Transport Mode** In transport mode, the data within an IP packet is encrypted, but the header information is not. This allows the user to establish a secure link directly with the remote host, encrypting only the data contents of the packet. The downside to this implementation is that packet eavesdroppers can still identify the destination system.

****

There are two popular uses for transport mode VPNs.

1. The first is the end-to-end transport of encrypted data. In this model, two end users can communicate directly, encrypting and decrypting their communications as needed. Each machine acts as the end node VPN server and client.
2. In the second, a remote access worker or teleworker connects to an office network over the Internet by connecting to a VPN server on the perimeter. This allows the teleworker’s system to work as if it were part of the local area network. The VPN server in this example acts as an intermediate node, encrypting traffic from the secure intranet and transmitting it to the remote client, and decrypting traffic from the remote client and transmitting it to its final destination.

This model frequently allows the remote system to act as its own VPN server, which is a weakness, since most work-at-home employees do not have the same level of physical and logical security they would have if they worked in the office.

* **Tunnel Mode** Tunnel mode establishes two perimeter tunnel servers that encrypt all traffic that will traverse an unsecured network. In tunnel mode, the entire client packet is encrypted and added as the data portion of a packet addressed from one tunneling server to another. The receiving server decrypts the packet and sends it to the final address. The primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.

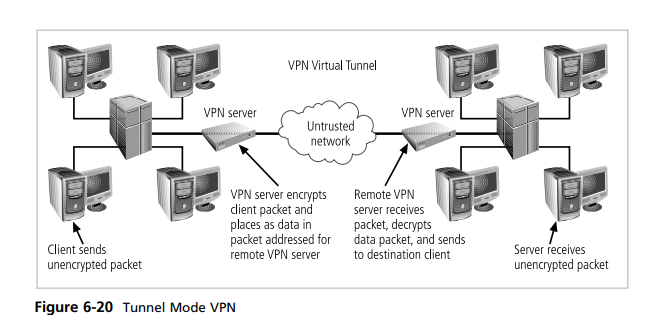
****

Figure 6-20 shows an example of tunnel mode VPN implementation. On the Figure 6-20 shows an example of tunnel mode VPN implementation. On the client end, a user with Windows 2000 or XP can establish a VPN by configuring his or her system to connect to a VPN server. The process is straightforward. First, connect to the Internet through an ISP or direct network connection. Second, establish the link with the remote VPN server.