8.1.2 Firewall Facts

A *firewall* is a software- or hardware-based network security system that allows or denies network traffic according to a set of rules. Firewalls can be categorized by their location on the network:

- A *network-based* firewall is installed on the edge of a private network or network segment.
  - Most network-based firewalls are considered *hardware* firewalls, even though they use a combination of hardware and software to protect the network from Internet attacks.
  - Network-based firewalls are more expensive and require more configuration than other types of firewalls, but they are much more robust and secure.
- A *host-based* firewall is installed on a single computer in a network.
  - Almost all host-based firewalls are *software* firewalls.
  - A host-based firewall can be used to protect a computer when no network-based firewall exists (e.g., when connected to a public network).
  - Host-based firewalls are less expensive and easier to use than network-based firewalls, but they don't offer the same level of protection or customization.

  A host-based firewall can be used in addition to a network-based firewall to provide multiple layers of protection.

- Firewalls use filtering rules, sometimes called *access control lists* (ACLs), to identify allowed and blocked traffic. A rule identifies characteristics of the traffic:
  - The interface the rule applies to
  - The direction of traffic (inbound or outbound)
  - Packet information such as the source or destination IP address or port number
  - The action to take when the traffic matches the filter criteria

  Each ACL has an *implicit deny*. This is a line at the end of the ACL stating that if a packet doesn't match any of the defined rules, then it will be dropped.

- Firewalls do not offer protection against all attacks (e.g., email spoofing).

The following table describes different firewall types:

Firewall Type	Characteristics
Packet filtering firewall	A *packet filtering firewall* makes decisions about which network traffic to allow by examining information in the IP packet header such as source and destination addresses, ports, and service protocols. A packet filtering firewall: - Uses ACLs or filter rules to control traffic. - Operates at OSI Layer 3 (Network layer). - Offers high performance because it examines only the addressing information in the packet header. - Can be implemented using features that are included in most routers. - Is a popular solution because it is easy to implement and maintain, has a minimal impact on system performance, and is fairly inexpensive. A packet filtering firewall is considered a *stateless* firewall because it examines each packet and uses rules to accept or reject it, without considering whether the packet is part of a valid and active session.
Circuit-level proxy	A *circuit-level proxy* or *gateway* makes decisions about which traffic to allow based on virtual circuits or sessions. A circuit-level gateway: - Operates at OSI Layer 5 (Session layer). - Keeps a table of known connections and sessions. Packets directed to known sessions are accepted. - Verifies that packets are properly sequenced. - Ensures that the TCP three-way handshake process occurs only when appropriate. - Does not filter packets. Instead, it allows or denies sessions. A circuit-level proxy is considered a *stateful* firewall because it keeps track of the state of a session. A circuit-level proxy can filter traffic that uses dynamic ports, because the firewall matches the session information for filtering and not the port numbers. In general, circuit-level proxies are slower than packet filtering firewalls. However, if only the session state is being used for filtering, a circuit-level gateway can be faster after the initial session information has been identified.
Application-level gateway	An *application-level gateway* is capable of filtering based on information contained within the data portion of a packet. An application-level gateway: - Examines the entirety of the content being transferred (not just individual packets). - Operates at OSI Layer 7 (Application layer). - Understands, or interfaces with, the application-layer protocol. - Can filter based on user, group, and data (e.g., URLs within an HTTP request). - Is the slowest form of firewall because entire messages are reassembled at the Application layer. One example of an application-level gateway is a *proxy server*. A proxy server is a device that stands as an intermediary between a secure private network and the public. Proxies can be configured to:

	▪ Control both inbound and outbound traffic. ▪ Increase performance by caching frequently accessed content. Content is retrieved from the proxy cache instead of the original server. ▪ Filter content and restrict access depending on the user or specific website. ▪ Shield or hide a private network. There are two different types of proxy servers: ▪ A *forward* proxy server handles requests from inside a private network out to the Internet. ▪ A *reverse* proxy server handles requests from the Internet to a server located inside a private network. A reverse proxy can perform load balancing, authentication, and caching. Oftentimes, reverse proxies work transparently, meaning that clients requesting specific resources don't know they are using a reverse proxy to access a server.
Unified threat management (UTM) device	A *unified threat management device* combines multiple security features into a single network appliance. A single UTM device can provide several security features: ▪ Firewall ▪ VPN ▪ Ant-spam ▪ Antivirus ▪ Load balancing By combining several services into one appliance, UTM devices make managing network security much easier. However, they also introduce a single point of failure—if the UTM fails, network security is lost. Additionally, UTM devices aren't as robust as other devices made for a specific use. Because of this, UTM devices are best suited for: ▪ Offices where space limits don't allow for multiple security appliances. ▪ Satellite offices that need to be managed remotely. Configuration changes need to be made on only one device, rather than multiple devices. ▪ Smaller businesses that wouldn't benefit from the robust features provided by specific security appliances.

A common method of using firewalls is to define various network *zones*. Each zone identifies a collection of users who have similar access needs. Firewalls are configured at the edge of these zones to filter incoming and outbound traffic. For example, you can define a zone that includes all hosts on your private network protected from the Internet, and you can define another zone within your network for controlled access to specific servers that hold sensitive information.