5.5.2 Firewall Facts

A *firewall* is a device or software running on a device that inspects network traffic and allows or blocks traffic based on a set of rules.

- A network-based firewall inspects traffic as it flows between networks. For example, you can install a network-based firewall on the edge of your private network that connects to the internet to protect against attacks from internet hosts. Network-based firewalls are typically dedicated hardware devices.
- A host-based or application-based firewall inspects traffic received by a host. Use a host-based firewall to protect against attacks when there is no network-based firewall, such as when you connect to the internet from a public location. Host-based firewalls are typically software programs. A host-based firewall can be configured to meet the security requirements of the specific host and add an additional layer of security even when a network firewall has been implemented.
- Firewalls use filtering rules, sometimes called access control lists (ACLs), to identify allowed and blocked traffic. A rule identifies traffic characteristics, such as:
  - 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
- Firewalls can protect against external attacks.
- Firewalls don't offer protection against all attacks (for example, spoofed email messages).
- A firewall can impede network availability because it adds processing to network traffic, or might drop network traffic when overloaded.

The following table explains different firewall types:

Type	Characteristics
Packet Filtering	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: - Operates up to OSI layer 3 (Network layer) - Uses access control lists (ACLs) or filter rules to control traffic - Offers high performance because it only examines addressing information in the packet header - Can be implemented using features that are included in most routers - Is not very intelligent, so it is subject to DoS and buffer overflow attacks - 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 each packet without considering whether the packet is part of a valid and active session.
Stateful	The stateful inspection firewall (also known as *circuit-level proxy* or *gateway*) makes decisions about which traffic to allow based on virtual circuits or sessions. The firewall is considered stateful because it keeps track of the state of a session. A stateful inspection firewall: - Operates up to OSI Layer 5 (Session layer) - Keeps track of known connections and sessions in a *session table* (also referred to as a state table) - Allows only valid packets within approved sessions - Verifies that packets are properly sequenced - Ensures that the TCP three-way handshake process occurs only when appropriate - Can filter traffic that uses dynamic ports because the firewall matches the session information, not the port numbers, for filtering In general, stateful inspection firewalls are slower than packet filtering firewalls. If only the session state is being used for filtering, a stateful inspection firewall can be faster after the initial session table has been created.
Application	An Application-layer firewall (also referred to as an Application-level gateway or proxy) makes security decisions based on information contained within the data portion of a packet. An Application-level gateway: - Operates up to OSI Layer 7 (Application layer) - Stops each packet at the firewall and inspects it, so there is no IP forwarding - Inspects encrypted packets, such as in SSL inspection - Examines the entire content (not just individual packets) - Understands or interfaces with the application-layer protocol - Can filter based on user, group, and data such as URLs within an HTTP request - Is the slowest form of firewall because entire messages are reassembled at the Application layer A *proxy server* is a device that stands as an intermediary between a secure private network and the public and is a specific implementation of an Application-level firewall. With a proxy, every packet is stopped and inspected at the firewall, which causes a break between the client and the source server. Proxies can be configured to: - Control both inbound and outbound traffic

	▪ Increase performance by caching heavily accessed content (content is retrieved from the proxy cache instead of the original server) ▪ Filter content ▪ Shield or hide a private network. ▪ Restrict access by user or by specific websites ▪ Allows inspection of encrypted packets, such as SSL inspection

Most newer firewalls have flood guard protections built into their feature sets. A flood guard protects against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which are the main types of DoS flood attacks. SYN floods, ping floods, UDP floods, and port floods. The following table explains a few common firewall security features:

Feature	Characteristics
Block ping to WAN	This feature helps prevent attackers from discovering your network through ICMP Echo (ping) requests.
Stealth Mode	This feature will prevent the response to port scans from the WAN. This protects against port floods.
TCP Flood	This feature will drop all invalid TCP packets. This protects your network from SYN flood attacks.
UDP Flood	This feature helps prevent UDP flood attacks by metering the number of simultaneous, active UDP connections from a single computer on the internal network.
ICMP Notification	This feature can silently block the sending of ICMP Notifications. Some protocols may require these notifications.
Fragmented Packets	This feature will block the sending of fragmented IP packets.
SYN Flood Detect Rate	To help prevent SYN floods, this feature monitors the rate of SYN packets during a configuration time period. Too many SYN packets will cause the firewall to determine that a SYN flood is occurring and to trigger the appropriate response.
Echo Storm Detect Rate	To help prevent ping floods, this feature monitors the rate of echo pings during a configuration time period. Too many pings will cause the firewall to determine that a ping flood is occurring and to trigger the appropriate response
ICMP Flood Detect Rate	This feature monitors non-ping ICMP packets. Too many will case the firewall to determine that a ICMP flood is occurring and trigger the appropriate response.

Be aware of the following when managing firewalls:

- When designing firewall packet filters, a common practice is to close all ports, opening only those ports necessary for accessing the resources behind the firewall.
- If a host cannot communicate on the network or if specific types of traffic (such as ICMP or Remote Desktop connection) don't work on a host, check the host firewall settings to make sure that the traffic type is allowed.
- Firewalls typically create log entries when packets are blocked by firewall rules. You can examine these logs to help troubleshoot communication problems or identify potential attacks (such as DoS attacks).
