11.2.2 Firewall Facts

A firewall can function as an IDS, but its main purpose is typically to establish a barrier between two networks to control traffic. A firewall is usually set up between the external and internal network, but can also be set up between internal networks.

This lesson covers the following topics:

- Firewall types
- Firewall technology
- Firewall identification
- Firewall limitations

Firewall Types

A firewall controls access to a network through a specific set of rules. Rules determine the traffic that is allowed to pass into, within, or out of the network. Most firewalls are configured to detect the type of traffic, the source and destination addresses, and ports. A firewall can be a hardware device or software program.

Hardware firewalls are physical devices usually placed at the junction or gateway between two networks, usually a private network and a public network, such as the internet. Hardware firewalls can be a standalone product or built into devices like broadband routers.

Software firewalls are generally used to protect individual hosts, but they can also be filters placed on devices, such as a router, to protect internal sections of a network.

Firewall Technology

As an ethical hacker and penetration tester, it is important to understand the different firewall architectures as well as the technologies they use and their limitations. The following table describes firewall technologies.

Technology	Description
Packet and content filtering	Packet filtering firewalls are the simplest and earliest type of firewall used. Packet filtering firewalls look at a packet's header information to determine legitimate traffic. Rules such as source and destination IP addresses, ports, protocols, and services are used to determine whether to allow or deny the packet entry. Be aware of the following: ▪ Packet filtering technology operates at Layers 3 and 4 of the OSI model. ▪ Packet filtering is a stateless form of inspection. It is a good first line of defense, but less secure than stateful inspection filters. ▪ Packet filtering is configured through access control lists (ACLs). ACLs enable the rule sets that determine whether to allow or block traffic. ▪ If traffic is not explicitly allowed within an ACL, by default, it is blocked.
Gateway	A firewall can be implemented on circuit-level gateways or application-level gateways. Both of these firewall designs sit between a host and a web server and communicate with the server on behalf of the host. They can also be used to cache frequently accessed websites for faster web page loading. ▪ Circuit-level gateways are a more complex form of firewall. Circuit-level gateways: ▪ Operate at Level 5 of the OSI model. ▪ Offer broader protection than an application firewall. ▪ Lack specific controls offered by Layer 7 firewalls. ▪ Store flow information for TCP connections and require client software to perform as a virtual circuit between systems. ▪ Application-level firewalls, also known as application gateways or proxy servers, can filter application-specific commands and can be configured as a web proxy. ▪ An Application-level firewall tends to be slower because of deep packet inspection at Layer 7. ▪ An Application-level firewall is capable of network address translation (NAT), translating non-routable IP addresses into routable ones.
Stateful inspection	Stateful firewalls, also referred to as stateful multilayer firewalls, determine the legitimacy of traffic based on the state of the connection from which the traffic originated. The stateful firewall maintains a state table that tracks the ongoing record of active connections.
Proxy servers	Proxy servers act as a proxy for internal hosts when connecting to the internet. ▪ Proxy servers prevent client systems from communicating directly with an outside source. This reduces exposure and risk. ▪ Proxy servers can also filter traffic by content. This means proxy servers can operate at Layer 7 of the OSI model. ▪ Proxy servers can also speed up browsing by caching frequently visited sites and resources.

Virtual private networks	A Virtual Private Network (VPN) is a network that provides secure access to a private network through the public network or internet. Virtual private networks offer secure connectivity between many entities, both internally and remotely. Their use of encryption provides an effective defense against sniffing.
Network address translation	Network address translation (NAT) separates IP addresses into two sets. This technology allows all internal traffic to share a single public IP when connecting to an outside entity.

Firewall Identification

After an attacker has identified a firewall and its rule set, the attacker can attempt to determine and exploit any weaknesses. The three primary methods of gathering firewall information are port scanning, banner grabbing, and firewalking.

Tool	Description
Port scanning	Port scanning is one of the most popular tools used to identify firewalls. It is also popular for determining the firewall's function. Port scanning is used to identify open ports and the services running. Open ports can be further probed to identify the version of services, which helps find vulnerabilities.
Banner grabbing	Banner grabbing, if not suppressed, is a simple method that helps identify the vendor of a firewall and the version of software it is running. Banner grabbing is a basic method to retrieve announcements provided by services in response to connection requests. The three main services that send out banners are FTP, Telnet, and web and email servers.
Firewalking	Firewalking is the process of probing a firewall to determine the configuration of ACLs by sending it TCP and UDP packets. This technique utilizes TTL values to determine gateway ACL filters and map networks by analyzing the IP packet responses. There are three components of firewalking: the host that sends the packets to the target, the gateway connected to the internet that the packets pass through, and the target system. Firewalk is a common firewall discovery tool. It works by crafting packets with a time-to-live (TTL) values set to expire one hop past the firewall. If the firewall allows the packet, it should forward the packet to the next hop, where the packet will expire and an ICMP time exceeded will be returned. When the firewall hop count is determined, the hacker begins the scan.

Firewall Limitations

Although firewalls provide a good first level of protection, they are not perfect. Some firewall limitations are:

- Firewalls can filter by an IP addresses, but cannot prevent spoofing.
- Firewalls can block specific ports and protocols, but cannot inspect a packet's payload.
- A packet filtering firewall does not detect or keep the connection state. This inability to keep up with the state status is a critical vulnerability because it means that packet filters cannot tell whether a connection was started inside or outside the organization.
- A firewall is unable to stop internal attacks or backdoors.
- A firewall cannot protect the network from social engineering and data-driven attacks, where the attacker sends malicious links and emails to employees inside the network.
- Firewalls and proxies are only as effective as their configurations; configurations are only as effective as the administrators creating them.
- Many firewall attacks are intended to evade firewalls, not assault them. Most attackers aim for softer targets. Firewall limitations help allow attackers identify network devices, which is key to initiating exploits.