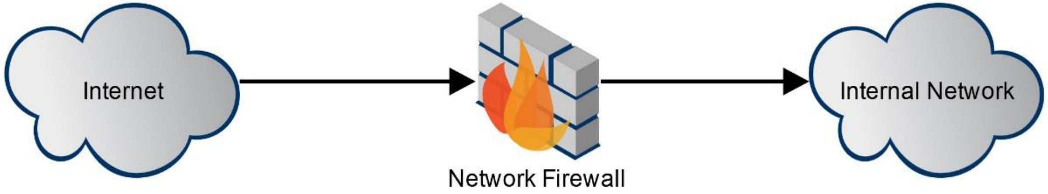
Firewalls

- Firewalls are the foundation of a defense-in-depth network security strategy.
- They're designed to protect organizations from network-based attacks.
- Firewalls do this by filtering data packets that go through them.
- They can be a standalone network device or software on a computer system, meaning **network-based** (hardware) or **host-based** (software).



3 Common Types of Firewalls

- **1st Generation**: Packet Filtering Firewalls
- **2nd Generation**: Circuit-Level Firewalls
- **3rd Generation**: Application-Level Firewalls

1st Gen: Packet Filtering Firewalls

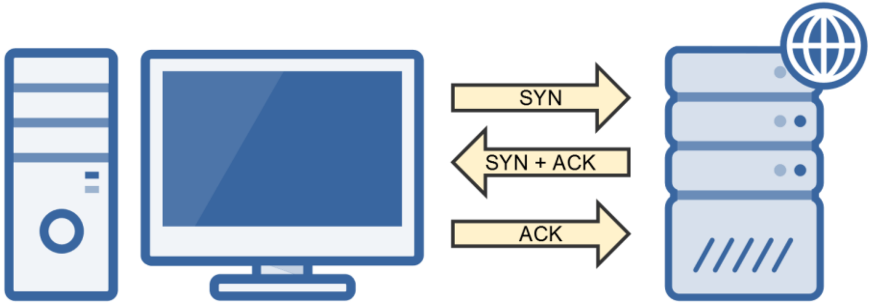
- 1st generation and most basic type of firewall.
- They inspect all data packets that attempt to traverse it, and based on predefined rules, packets are either allowed or denied.
- These predefined rules are commonly called an Access Control List (ACL).
- Considered Stateless Firewalls.

- Packet filtering rules are common TCP/IP packet attributes:
- **IP Address**
  - Source IP Address
  - Destination IP Address
- **TCP/UDP Port**
  - Source TCP/UDP Port
  - Destination TCP/UDP Port
- **Inbound or Outbound**
  - Inbound Firewall Network Interface
  - Outbound Firewall Network Interface

INSTRUCTOR
ALTON

2nd Gen: Stateful Inspection Firewalls

- Operate at the Transport Layer of the OSI Model (Layer 4) and monitor TCP sessions.
- Determine the legitimacy of a requested session by monitoring the 3-way handshake between packets.
- Valid TCP sessions are allowed to pass, while invalid and terminated sessions are not.
  - Hackers can alter the 3-way handshake process for malicious reasons.
  - If the firewall believes an attack is occurring, it will block the traffic.



3rd Gen: Application-Level Firewalls

- Also known as proxy servers, these firewalls operate at the Application Layer of the OSI Model (Layer 7).
- Specifically, proxy servers can provide the following services:
    - **Filter**: Filters packets based on an application or service (FTP, SMTP, etc.).
    - **Caching**: Provides caching services, for example:
        - ✓ When you request a page from a website, the proxy server will retrieve it and then cache it in its memory.
        - ✓ The next time someone requests that website, the proxy server can retrieve it from its cache.
        - ✓ This saves Internet bandwidth.
    - **Logging**: Has the ability to log user activity for auditing purposes.