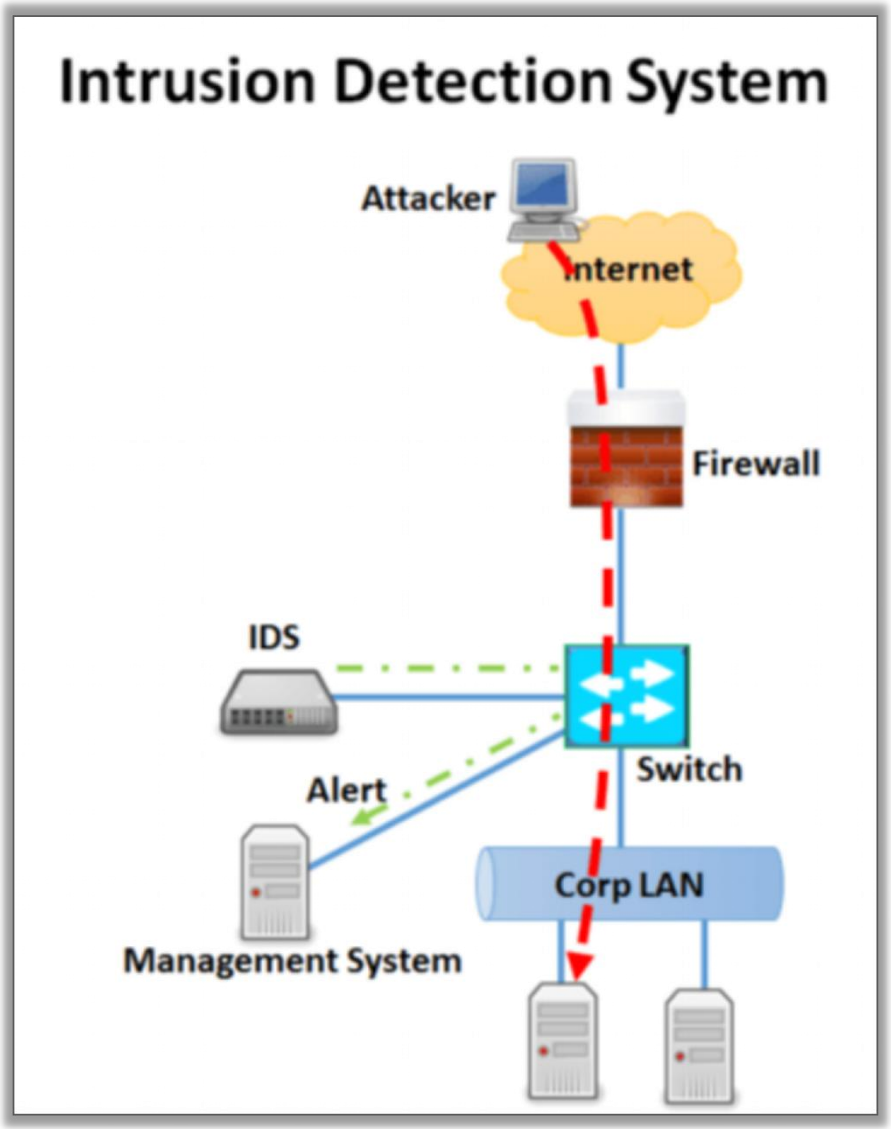
Intrusion Detection/Prevention Systems

Intrusion Detection Systems

- Intrusion Detection System (IDS)
  - Passive Monitoring
  - Hardware\software based
  - Uses attack signatures
  - Configuration
    - SPAN/Mirror Ports
    - Generates alerts (email)
    - After the fact response

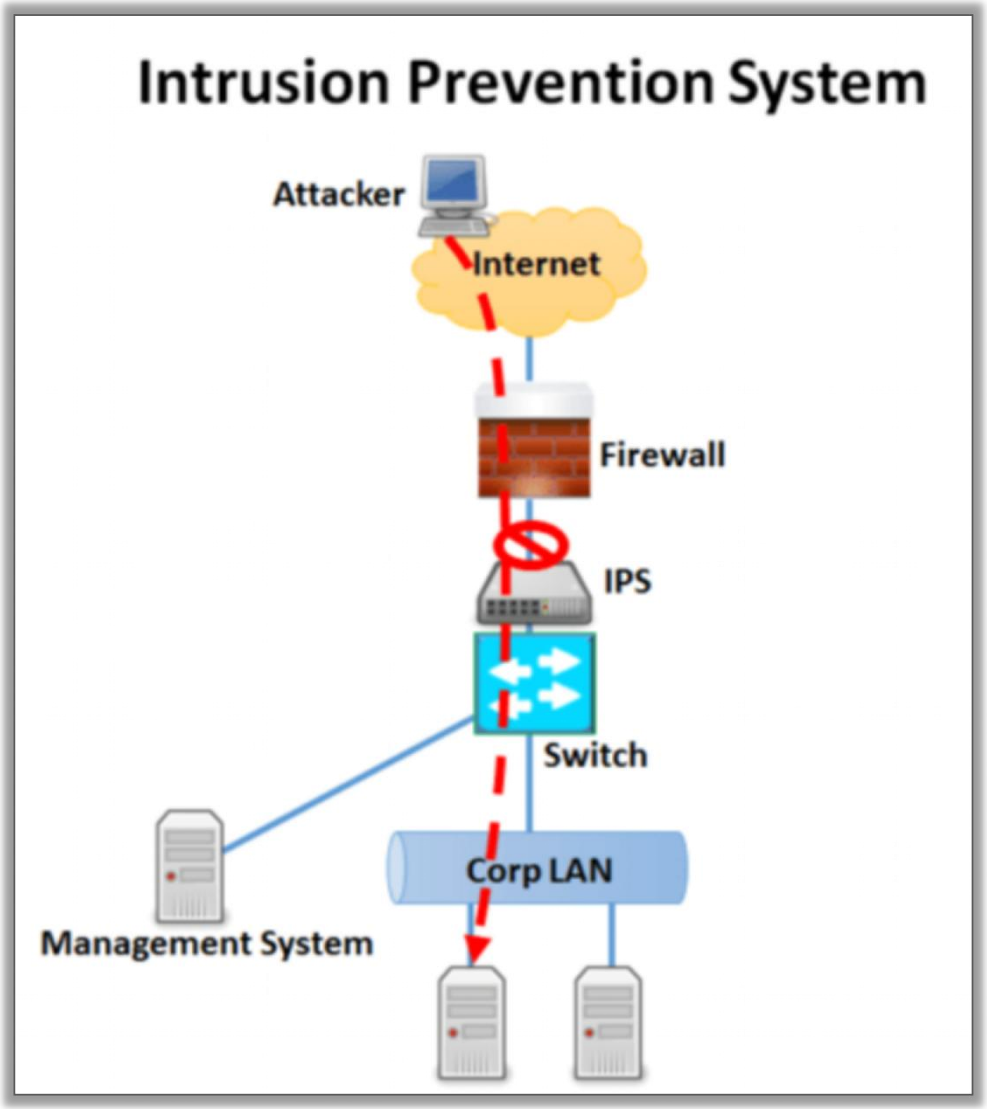
Intrusion Detection Systems



Intrusion Prevention Systems

- Intrusion Prevention System (IPS)
  - Also called Network Defense Systems (NDS)
  - Inline & active
  - Hardware\software based
  - Uses attack signatures
  - Configuration
    - Generates alerts (email)
    - Real time response

Intrusion Prevention Systems



⚙ How Does IDS Work?

• 📡**Traffic Collection**
•The IDS monitors **network packets** or **system logs**.
•It can work **in real-time**, collecting data from firewalls, routers, switches, or endpoints.

• 🔍**Analysis**
•The IDS analyzes traffic or logs using **two main detection methods**:

a. Signature-Based Detection

- •Compares incoming data to a **database of known threats** (like antivirus works).
- •Example: Matches known malware or attack patterns.

b. Anomaly-Based Detection

- •Learns what “normal” traffic looks like.
- •Flags **anything that deviates from that baseline**.
- •Example: If a user downloads 5GB of data at 3 AM and they never do that—IDS raises an alert.

⚙ How Does IPS Work?

- 🚨 **Alerting**
- If a potential threat is found, the IPS **generates an alert**.
- The alert may contain:
  - Type of threat
  - Source and destination IP
  - Time of detection
  - Severity level

- 🗂 **Logging**
- All findings are **logged** for further investigation or compliance.

UNIT:4 DEMILITARIZED ZONE

DMZ (Demilitarized Zone) — also known as:

- **Perimeter Network**
- **Screened Subnet**

Purpose:

- To add an **extra layer of security**.
- External users can **only access services in the DMZ**.
- The **internal network remains protected** by a firewall.

UNIT:4 DEMILITARIZED ZONE

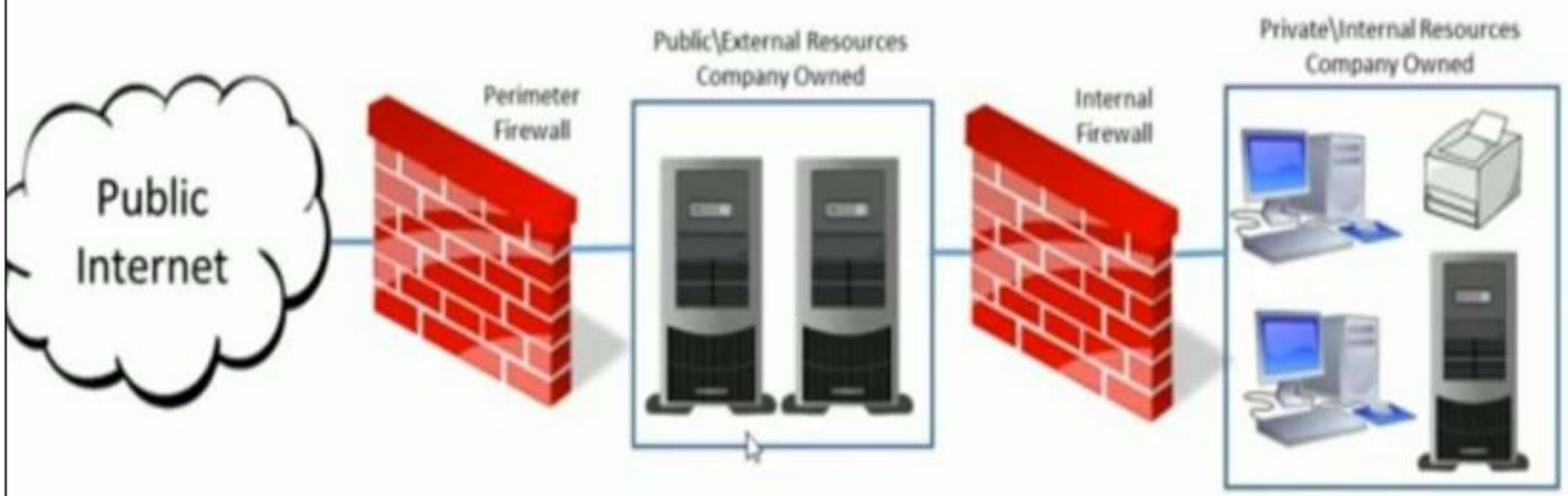
Dual-Firewall DMZ Configuration

- A **more secure approach** to creating a DMZ.
- Involves **two firewalls** with the DMZ positioned in between:
  - **Perimeter Firewall** (First Firewall):
    - Faces the **Internet**.
    - Allows only **external traffic to the DMZ**.
  - **Internal Firewall** (Second Firewall):
    - Faces the **Internal Network**.
    - Allows only **DMZ-to-Internal traffic** as needed.
- **Advantages:**
  - Provides extra **layered security**.
  - An attacker must **compromise both firewalls** to reach the internal network.
  - Enhances **control and monitoring** of traffic between zones.

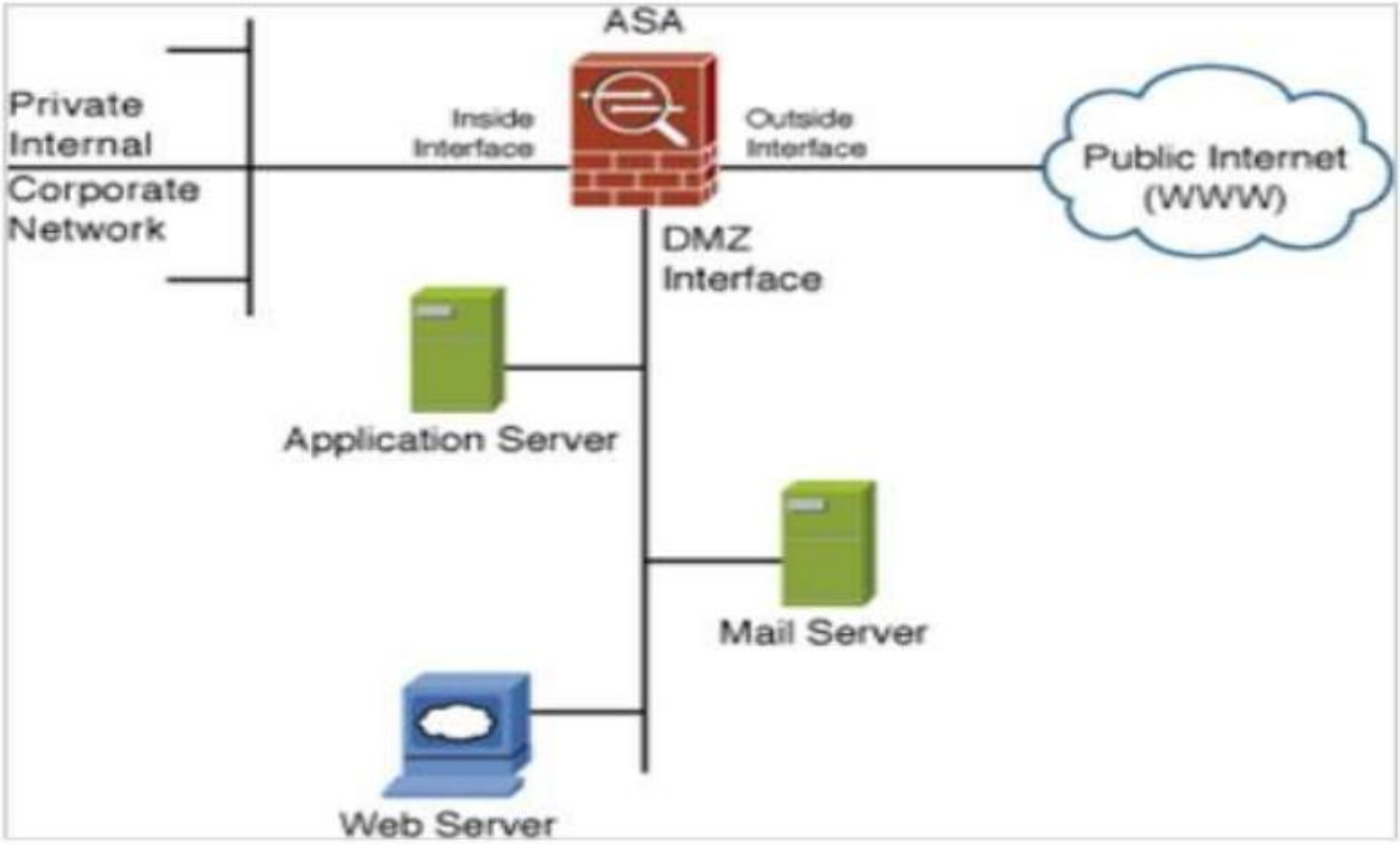
Single Firewall DMZ Configuration

- Uses **one firewall** with **at least three network interfaces**:
- **Interface 1**: Connects to the **External Network** (Internet via ISP).
- **Interface 2**: Connects to the **Internal Network** (LAN).
- **Interface 3**: Connects to the **DMZ Network**.
- Also known as a **3-legged firewall architecture**.
- Offers **simpler setup**, but **less secure** than dual-firewall design.
- Requires **careful firewall rule configuration** to ensure isolation between networks.

DMZ (Demilitarized Zone)



DMZ PLACEMENT AND FUNCTION



BENEFITS OF DMZ

Primary Benefit:

- Isolates all **internet-bound requests** to servers in the DMZ.
- Prevents direct access to the **internal network**.

Additional Security Advantages:

Auditing DMZ traffic

- Monitor and analyze external interactions.

Placing an IDS in the DMZ

- Detect suspicious activities targeting exposed services.

Limiting routing updates

- Better control of **routing behavior** across interfaces.

Hosting DNS in the DMZ

- Public-facing DNS services isolated from internal DNS servers.