FIREWALL

DEFINITION

A **firewall** is a security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules.

PURPOSE OF FIREWALLS

- Protecting against Unauthorized Access

- Monitoring and Controlling Network Traffic

- Establishing a Barrier between Trusted and Untrusted Networks

TYPES OF FIREWALLS

1. Packet Filtering Firewalls: Examines packets and decides whether to drop or forward them based on predefined rules.

2. Stateful Inspection Firewalls: Keeps track of the state of active connections and makes decisions based on the context of the traffic.

3. **Proxy Firewalls:** Acts as an intermediary between internal and external networks, forwarding requests and responses.

FIREWALL DEPLOYMENT LOCATIONS

1. **Network-based Firewalls**

   Placed at the network perimeter.

2. **Host-based Firewalls**

   Installed on individual devices.

3. **Cloud-based Firewalls**

   Protecting cloud infrastructure and services.

FIREWALL RULES AND POLICIES

1. **Inbound Rules**

   Control incoming traffic.

2. **Outbound Rules**

   Manage outgoing traffic.

3. **Default Rules**

   Define the baseline behavior for unspecified traffic.

COMMON FIREWALL SETTINGS

1. **Allow**

   Permits specified traffic.

2. **Block/Deny**

   Restricts specific traffic.

3. **Allow with Logging**

   Permits traffic and creates logs for analysis.

FIREWALL BEST PRACTICES

- Regularly Update Firewall Rules

- Monitor Firewall Logs

- Conduct Security Audits

CHALLENGES AND CONSIDERATIONS

1. **False Positives/Negatives**

   Balancing security and usability.

2. **Performance Impact**

   Considerations for large-scale networks.

3. **Evolving Threat Landscape**

   Adapting to new and emerging threats.

DMZ

The term **DMZ** which stands for the **demilitarized zone** is derived from a military term.

The nations at war with each other may set up a demilitarized zone usually through treaties. No country is permitted to have military forces in this stretch of land.

The most well-known one is the **Korean DMZ** currently taking place between **North** and **South Korea**. The purpose of the Korean DMZ is to protect both countries from strikes.

DMZ

- DMZ stands for Demilitarized Zone. It is a network segment used to host public facing servers.
- The DMZ isolates the public facing servers from internal servers.
- So, if the servers in DMZ are compromised, the attack doesn't spread to internal network.

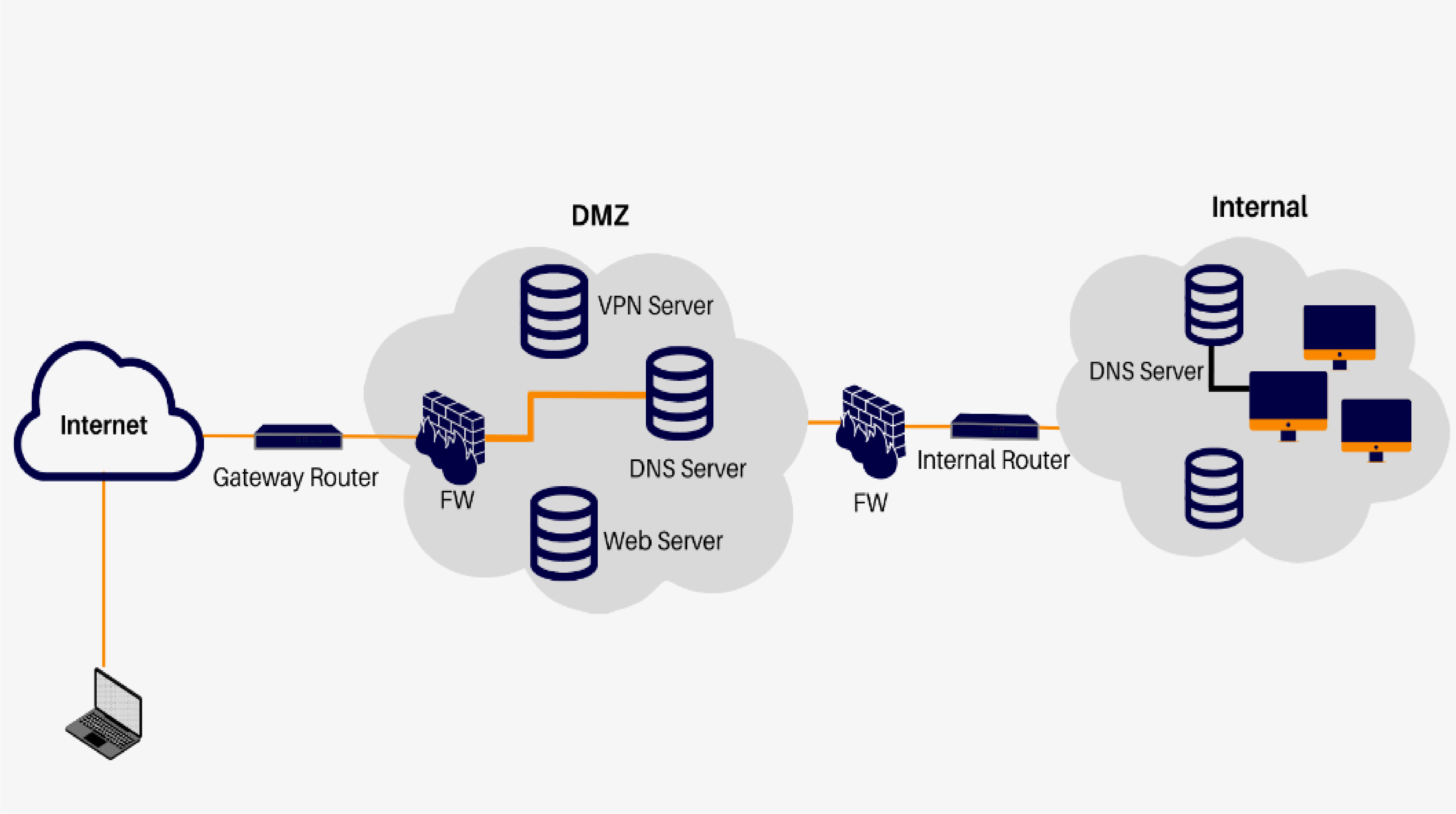
WHY USE A DMZ?

- **Protecting Internal Networks**

  Provides an additional layer of defense against external threats.

- **Hosting Publicly Accessible Services**

  Safely exposes services like web servers without exposing the entire internal network.


DMZ
Internal
VPN Server
Internet
DNS Server
Gateway Router
FW
DNS Server
FW
Internal Router
Web Server