# Demilitarized Zone (DMZ) Network Configuration in pfSense Firewall

A Demilitarized Zone (DMZ) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, typically the internet. The primary purpose of a DMZ is to add an extra layer of security to an organization's local area network (LAN); an external network node can access only what is exposed in the DMZ, while the rest of the network remains protected.

## Steps to Configure a DMZ in pfSense

Identify the interfaces you will use for the WAN, LAN, and DMZ. For this example:

WAN (Wide Area Network) interface connected to the internet.

LAN (Local Area Network) interface connected to the internal network.

DMZ interface for external-facing services.

Navigate to Interfaces > Assignments.

Add a new interface by selecting an available network port and clicking the add button.

Click on the newly created interface to configure it.

Enable the interface and assign it a name (e.g., DMZ).

Set the IPv4 Configuration Type to "Static IPv4".

Assign an IP address for the DMZ network (e.g., 192.168.3.100/24).

Save and apply the changes.

## Configuring Firewall Rules:

Go to Firewall > Rules and select the DMZ tab.

Click the add button to create a new rule.

Configure the rule to allow traffic from the DMZ to the WAN if needed (e.g., allowing HTTP/HTTPS traffic):

Action: Pass

Interface: DMZ

Protocol: TCP

Source: DMZ net

Destination: Any

Destination Port Range: HTTP (80) / HTTPS (443)

Save and apply the changes.

Add a rule to allow specific traffic from the DMZ to the LAN if necessary, but be restrictive to minimize security risks.

Ensure the default deny rule is in place for all other traffic.

## NAT Configuration:

Navigate to Firewall > NAT > Outbound.

If using Automatic NAT, pfSense will automatically create the necessary rules. For manual control, switch to Manual Outbound NAT rule generation.

Add a new outbound NAT rule for the DMZ network:

Interface: WAN

Source: DMZ net

Source Port: Any

Destination: Any

Destination Port: Any

Translation / target: Interface address (for NAT)

Save and apply the changes.

Install and configure the necessary services (e.g., web servers, mail servers) on hosts within the DMZ network.

Ensure these hosts have the appropriate static IP addresses within the DMZ subnet.