pfSense Perimeter Firewall Configuration

Goal

Harden and manage perimeter access by configuring targeted firewall rules on a pfSense security appliance to support a DMZ-hosted web service.

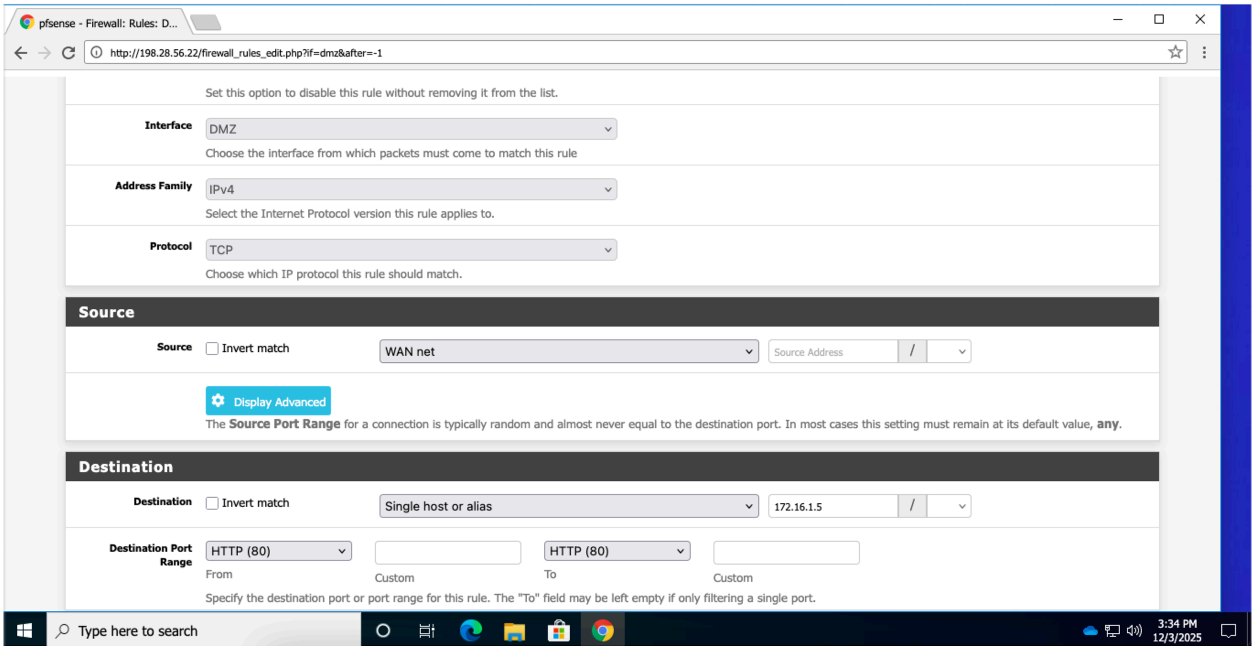
What I Implemented

1. Enabled External Access to a DMZ Web Server

Created dedicated firewall rules allowing inbound WAN traffic to reach a web server located in the DMZ:

- **HTTP (80) WAN → DMZ**
- **HTTPS (443) WAN → DMZ**
- Traffic restricted to a single host: **172.16.1.5**

Purpose:
Allows public web access while maintaining isolation between WAN, LAN, and DMZ segments.


pfsense - Firewall: Rules: D...
http://198.28.56.22/firewall_rules_edit.php?if=dmz&after=-1

Set this option to disable this rule without removing it from the list.

Interface DMZ
Choose the interface from which packets must come to match this rule

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source □ Invert match WAN net Source Address /

Display Advanced
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination □ Invert match Single host or alias 172.16.1.5 /

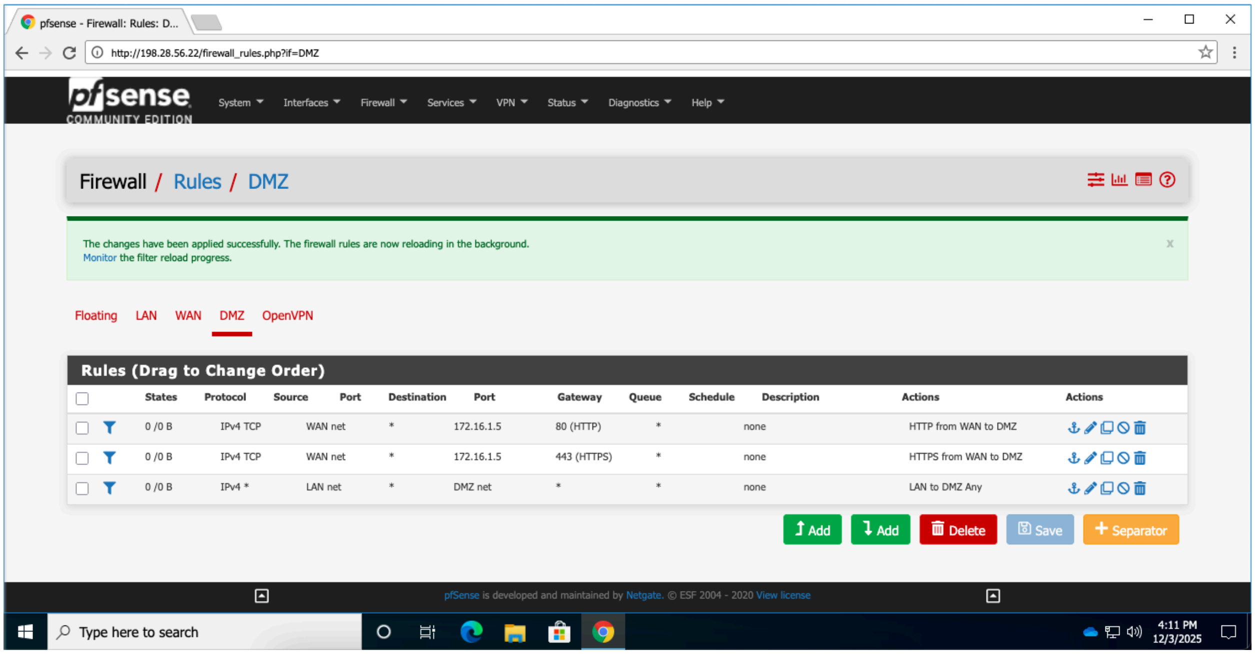
Destination Port Range HTTP (80) From; Custom; HTTP (80) To; Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

---

2. Configured Internal LAN → DMZ Trust Path

Added an internal rule to allow full LAN-originating traffic to the DMZ network.

Purpose:
Enables administrators and internal hosts to manage or support DMZ resources without weakening WAN-facing security controls.


pfsense - Firewall: Rules: D...
http://198.28.56.22/firewall_rules.php?if=DMZ
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating
LAN
WAN
DMZ
OpenVPN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□		0 /0 B	IPv4 TCP	WAN net	*	172.16.1.5	80 (HTTP)	*	none		HTTP from WAN to DMZ	
□		0 /0 B	IPv4 TCP	WAN net	*	172.16.1.5	443 (HTTPS)	*	none		HTTPS from WAN to DMZ	
□		0 /0 B	IPv4 *	LAN net	*	DMZ net	*	*	none		LAN to DMZ Any	

Add
Add
Delete
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license
Type here to search
4:11 PM
12/3/2025

Security Impact

This configuration builds a controlled perimeter for a public-facing web server while enforcing least privilege and maintaining strict WAN/LAN/DMZ segmentation. It reflects real-world firewall administration using pfSense, a widely adopted open-source network security platform.