Firewall Rules

Project Overview

The objective of this lab was to configure **DNS and firewall rules** on the Outside-Firewall (pfSense) and Webserver-DMZ virtual machines to enforce DNS traffic routing through a designated resolver. This ensured that all DNS queries from internal clients were directed exclusively to the **Outside-Firewall DNS server**, blocking all external DNS requests. The lab also integrated **Splunk-DMZ** for centralized monitoring and verification of firewall activities.

This project provided hands-on experience with **DNS resolution, pfSense firewall rule configuration, UFW (Uncomplicated Firewall)**, and **log analysis in Splunk Enterprise**.

Implementation Steps

1. Configure Splunk to Receive Firewall Logs

- Verified that Splunk was configured to receive **syslog data** from Outside-Firewall (from previous lab setup).
- Accessed pfSense at http://192.168.4.1 → **Status > System Logs > Settings**.
- Ensured **"Firewall Events"** was enabled to forward logs.
- Saved configuration.
- Confirmed that pfSense firewall messages were being sent to Splunk-DMZ.

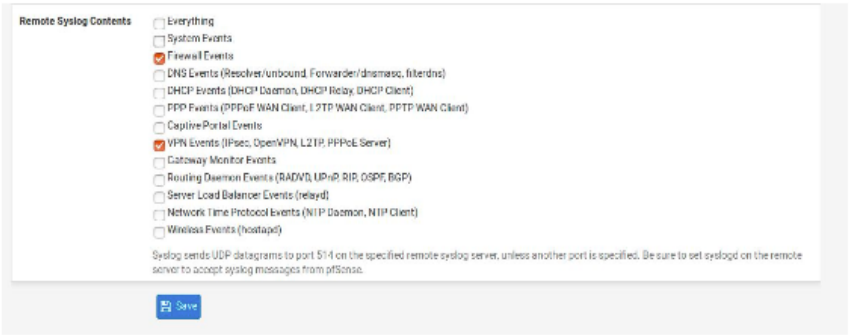

Figure 1/Rules

---

2. Configure Outside-Firewall as a DNS Resolver

- Accessed pfSense dashboard (System → General Setup).
- Updated general settings:
  - Hostname: pfsense-outside
  - DNS Server 1: 8.8.8.8

    - DNS Server Override: **Enabled**
    - Timezone: **EST**
- Saved changes.
- Enabled the DNS Resolver service via Services → DNS Resolver with the following configuration:
    - Enable DNS Resolver
    - Listen Port: 53
    - Network Interfaces: All
    - Outgoing Interfaces: All
    - System Domain Local Zone Type: Transparent
    - DNSSEC: Disabled
    - DNS Query Forwarding: Disabled
    - DHCP Registration: Unchecked
    - Static DHCP: Unchecked
- Saved and applied all changes.

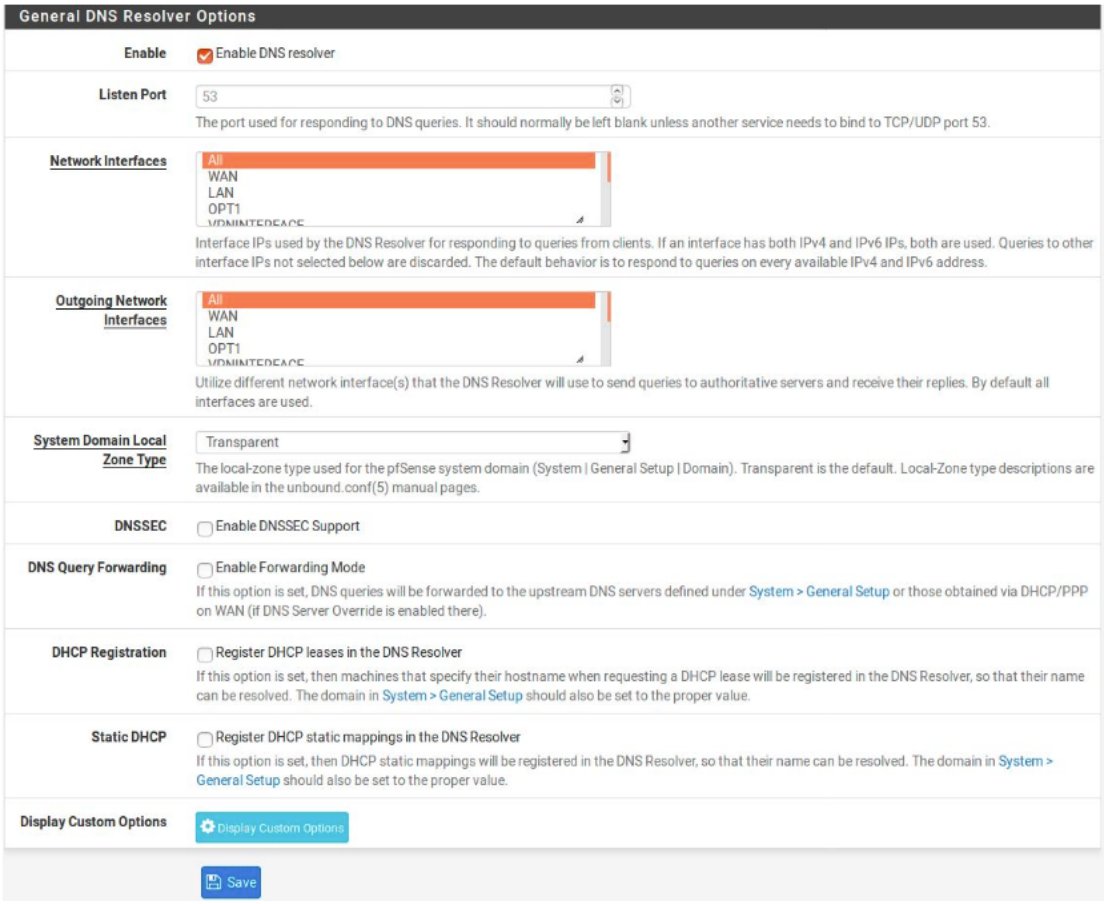

Figure 2/DNS

---

3. Validate DNS Resolver Functionality

- From **Client2-DMZ**, opened Terminal and entered nslookup.
- Tested DNS resolution using:
- yahoo.com

  Response confirmed proper DNS resolution via **Google DNS (8.8.8.8)**.

- Switched DNS server to pfSense:
- server 192.168.4.1
- cnn.com

  Verified successful DNS resolution via **Outside-Firewall DNS**.

---

4. Create Firewall Rules to Enforce DNS Policy

A. Add Reject Rule (Block all other DNS traffic)

- On client2-DMZ : Firefox → Outside-Firewall http://192.168.4.1
- Navigation: Firewall → Rules → LAN → Add Rule (Top of list)
- Configuration:
  - **Action:** Reject
  - **Protocol:** TCP/UDP
  - **Source:** Any
  - **Destination:** Any
  - **Destination Port Range:** 53 (DNS)
  - **Log:** Enabled
  - **Description:** Block access to external DNS servers
- Saved and applied changes.

B. Add Pass Rule (Allow DNS only to 192.168.4.1)

- Added another rule above the reject rule with the following configuration:
  - **Action:** Pass
  - **Interface:** LAN
  - **Protocol:** TCP/UDP
  - **Source:** Any
  - **Destination:** Single host 192.168.4.1
  - **Destination Port Range:** 53 (DNS)
  - **Log:** Disabled
  - **Description:** Allow access to Outside-Firewall DNS server
- Saved and applied changes.
- Verified that **Pass Rule precedes Reject Rule** in the list.

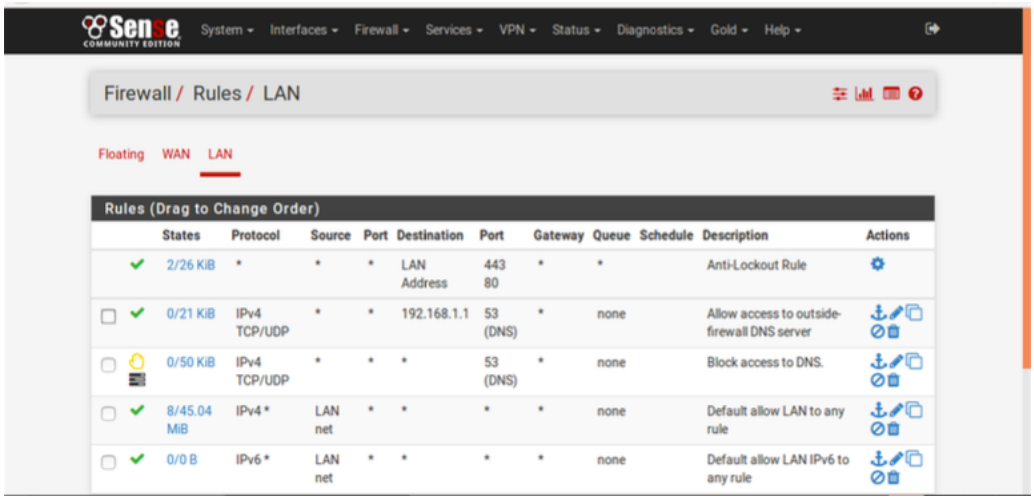

Figure 3/Firewall Rules

---

5. Test and Verify Firewall Behavior

- On **Client2-DMZ**, tested DNS queries again:
- nslookup
- yahoo.com # Expected: Fail (blocked by rule)
- server 192.168.4.1
- cnn.com # Expected: Success (allowed via pfSense DNS)
- Results confirmed that all DNS traffic outside 192.168.4.1 was blocked, enforcing secure DNS resolution.

---

6. Log Verification in Splunk

- Switched back to Splunk VM (192.168.4.20)
- Logged into **Splunk Enterprise** (https://localhost:8000).
- Verified DNS-related firewall events using:
- index=syslog 192.168.4.1
- Observed log entries showing blocked DNS attempts (e.g., failed query to yahoo.com), confirming that Splunk was receiving real-time firewall logs.

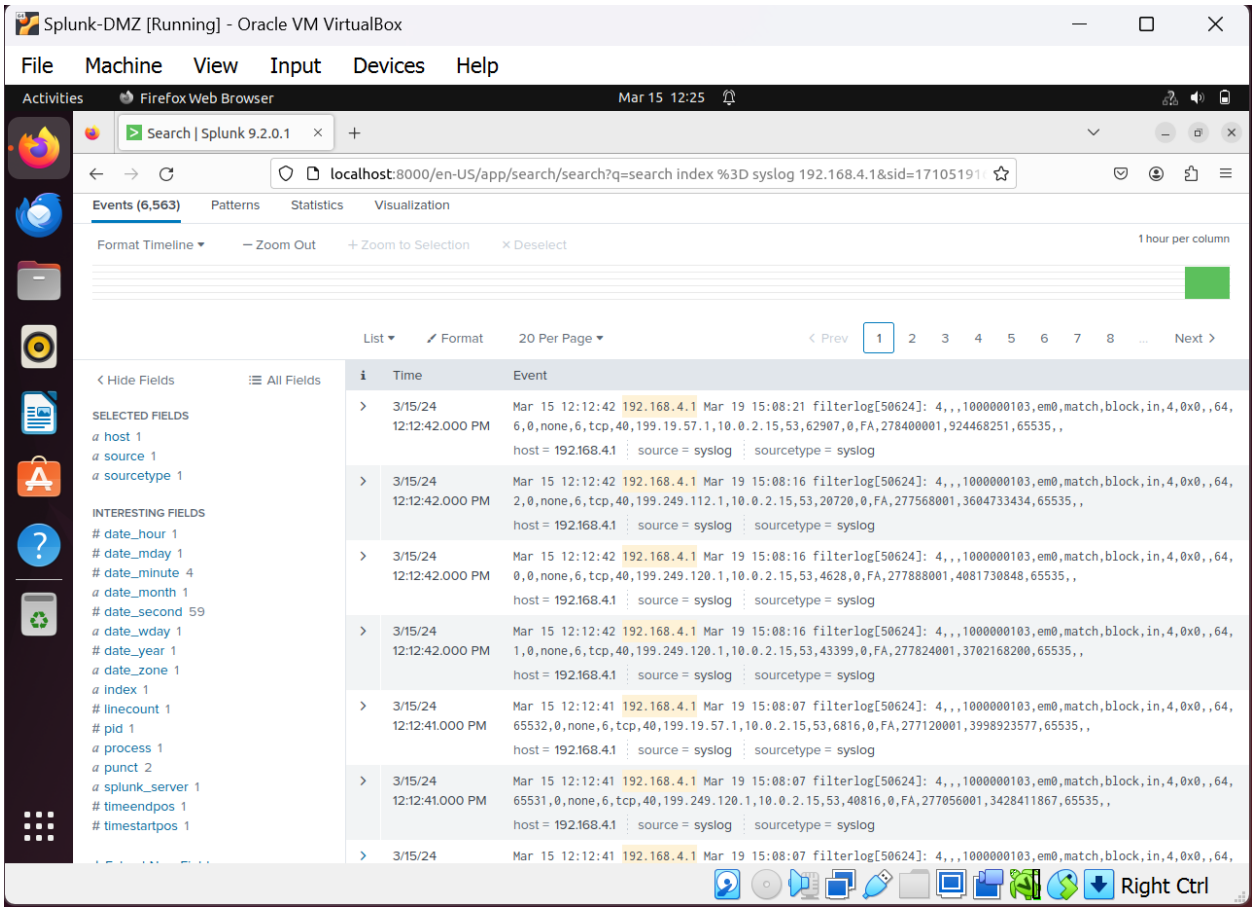

Figure 4/Syslog

7. Modify DNS Settings on Static Hosts

- Verified that all Ubuntu VMs with static IPs (e.g., **Client2-DMZ**) used the correct internal DNS server.
- Opened the **Network Settings** via the top-right networking icon in Ubuntu.
- Selected **Edit Connections → Wired Connection 1 (or 2) → Edit → IPv4 Settings** tab.
- Confirmed that **Method = Manual**.
- Updated **DNS Server** from 8.8.8.8 to 192.168.4.1.
- Saved and closed the settings window to apply the update.
- Ensured all static hosts pointed DNS traffic internally to the Outside-Firewall resolver.

---

8. Update DHCP Server Configuration on pfSense Firewalls

- Accessed **pfSense Dashboard → Services → DHCP Server** on both Inside and Outside Firewalls.

- Under the **Servers** section, confirmed that **192.168.4.1** was the only DNS server listed.
- Saved changes.
- Noted that the **Inside-Firewall** took slightly longer to boot due to the DNS timeout from the external block rule (cannot reach 8.8.8.8).
- Confirmed that **System → General Settings** on Inside-Firewall also referenced **192.168.4.1** as its DNS server.
- These adjustments standardized DNS resolution throughout the enterprise network.

---

3. Configure UFW on Webserver-DMZ

- Ensured **Outside-Firewall** and **Webserver-DMZ** VMs were powered on.
- Opened a Terminal window on **Webserver-DMZ** and installed the SSH server (if not already installed):
- sudo apt-get install ssh
- Enabled **UFW (Uncomplicated Firewall)**:
- sudo ufw enable
- Verified UFW status:
- sudo ufw status verbose
- Created a rule to **allow SSH access only from Client2-DMZ (192.168.4.50)**:
- sudo ufw allow from 192.168.4.50 to 192.168.4.55 port 22 proto tcp
- Verified that the new rule was successfully added:
- sudo ufw status verbose
- Confirmed that SSH access was restricted to the management host only.