Webserver-DMZ

Overview

The objective of this project was to deploy and secure a web server within the DMZ network using **Nginx**, update **firewall rules** to block traffic to the webserver from **pfSense** Inside network, and integrate **Splunk Enterprise** for centralized log collection and analysis from the webserver-dmz.
This setup demonstrates how enterprise environments segment network zones, restrict access, and monitor server activity through centralized SIEM tools.

Implementation Steps

1. Create WebServer-DMZ Virtual Machine

- Opened **VirtualBox** and cloned the existing **Client2-DMZ** virtual machine.
- Selected **Machine → Clone**, renamed the new VM to **WebServer-DMZ**, and reinitialized all MAC addresses.
- Once the cloning process completed, powered on the new VM.

Hostname Configuration

- Opened Terminal and updated host identifiers: *#sudo nano /etc/hostname #sudo nano /etc/hosts*
- Replaced all instances of **client2-dmz** with **webserver-dmz**.
- Applied the new hostname immediately with: *#sudo hostname webserver-dmz*

---

2. Assign a Static IP Address to WebServer-DMZ

- Accessed the **Networking** icon (top-right of Ubuntu-webserver).
- Navigated to **Edit Connections → Wired Connection 1 → Edit → IPv4 Settings tab**.
- Changed the method from *Automatic (DHCP)* to *Manual*.
- Entered the following network details:
- Address: **192.168.4.55**
- Netmask: **255.255.255.0**
- Gateway: **192.168.4.1**
- DNS: **8.8.8.8**
- Saved and closed the settings window.
- Applied changes in Terminal:

~sudo ifconfig enp0s3 down
~sudo ifconfig enp0s3 up

~ifconfig

- Verified that enp0s3 displayed the correct IP (**192.168.4.55**).

---

3. Install and Configure Nginx

- Installed Nginx web server by following the DigitalOcean Nginx Installation Guide.
- Verified installation by visiting:
- http://192.168.4.55
- A successful setup displayed the **"Welcome to Nginx"** default web page, confirming that the server was running correctly.

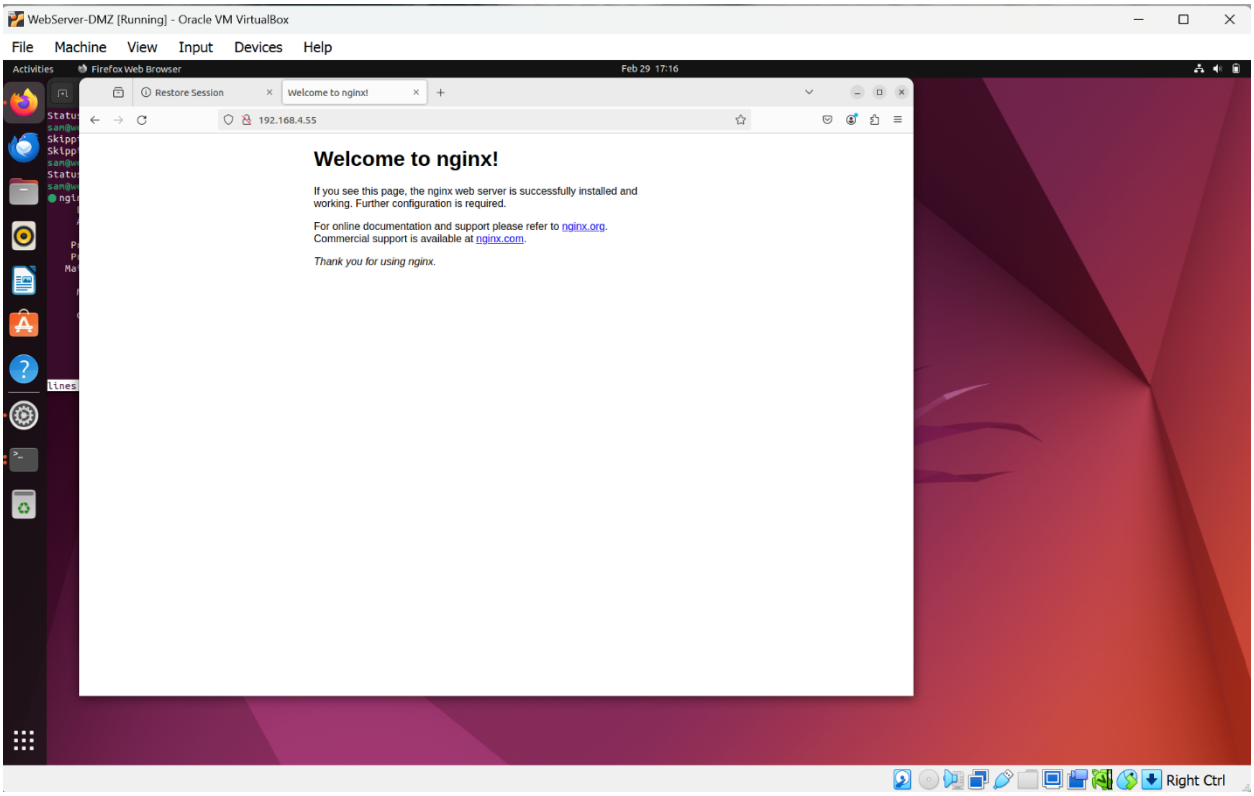

Figure 1/Nginx

---

4. Test Connectivity from the Inside Network

- Ensured that **Outside-Firewall**, **Inside-Firewall**, and **WebServer-DMZ** were active.
- From **Client3-Inside**, ran network validation commands:
- ping 192.168.4.55
- traceroute 192.168.4.55
- nmap 192.168.4.55

- Results confirmed the following:
    - Ping and traceroute succeeded.
    - nmap scan showed port 80 as **open**, verifying that HTTP access was active from the internal network.

---

5. Modify Inside-Firewall Rules (pfSense)

- Accessed the **Inside-Firewall** via browser at http://192.168.2.1.
- Navigated to **Firewall → Rules → LAN → Add Rule to Bottom**.

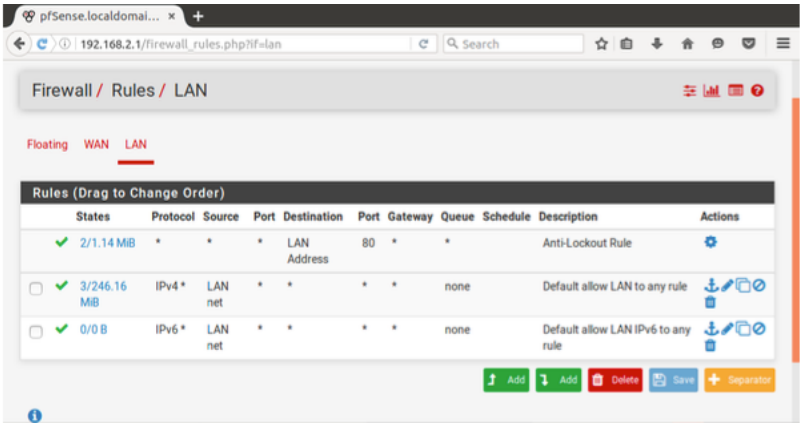

Figure 2/Rules

- Configured the rule as follows:
- Action: Block
- Protocol: TCP
- Destination: 192.168.4.55
- Port: 80 (HTTP)
- Log: Enabled
- Description: Block access to webserver-dmz
- Saved and applied changes.
- Moved the new rule into the second position under LAN rules.

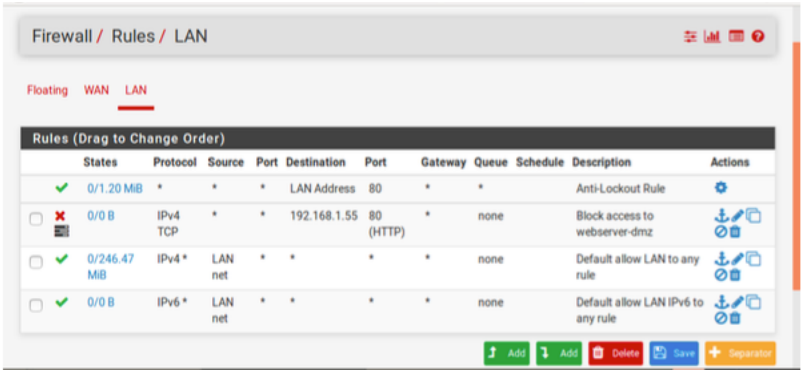

Figure 3/Rules update

Re-Testing:

- From **Client3-Inside**, re-ran connectivity tests.
  - Ping and traceroute still worked.
  - nmap showed port 80 as **filtered**.
  - Browser access to http://192.168.4.55 was **blocked**, confirming the rule worked as intended.
  - Alternatively, tested *wget 192.168.4.55* which kept getting "connection timeout"

---

6. Configure Splunk Enterprise for Web Logs

- On **Splunk-DMZ**, opened **http://localhost:8000** and logged in as admin.
- Navigated to:
  Settings → Forwarding and Receiving → Configure Receiving → New → Port: 9997

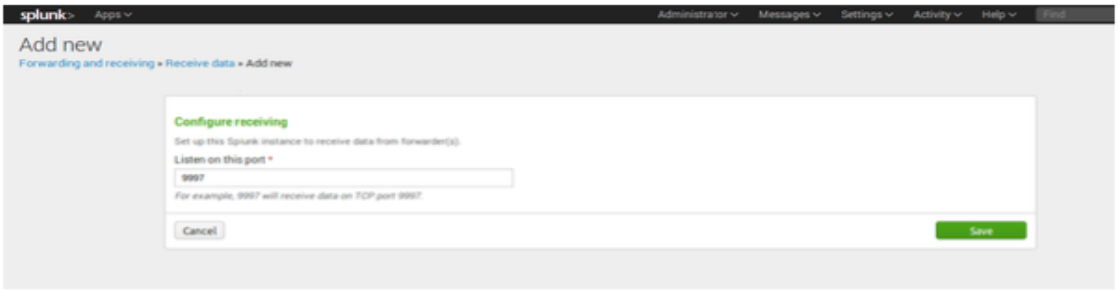

Figure 4/Splunk1

- Created a new index for the web server logs:
  Settings → Indexes → New Index → Name: webserver

---

7. Configure Splunk Universal Forwarder on WebServer-DMZ

- Downloaded and installed the **Splunk Universal Forwarder** package:
- *~sudo dpkg -i splunkforwarder-6.5.2-67571ef4b87d-linux-2.6-amd64.deb*
- Enabled Splunk Forwarder to auto-start on boot:
- *~cd /opt/splunkforwarder/bin/*
- *~sudo ./splunk enable boot-start*
- *~sudo systemctl start SplunkForwarder*
- Configured Splunk Forwarder to send logs to Splunk-DMZ:
- *~sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.4.20:9997*
- Added monitored Nginx log files:
- *~sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/nginx/access.log -index webserver -sourcetype webserver_access*
- *~sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/nginx/error.log -index webserver -sourcetype webserver_errors*

---

8. Verify Log Data in Splunk

- Logged into **Splunk Enterprise** and ran the query:
- index=webserver
- Verified that both **access** and **error logs** were successfully ingested from **WebServer-DMZ**.

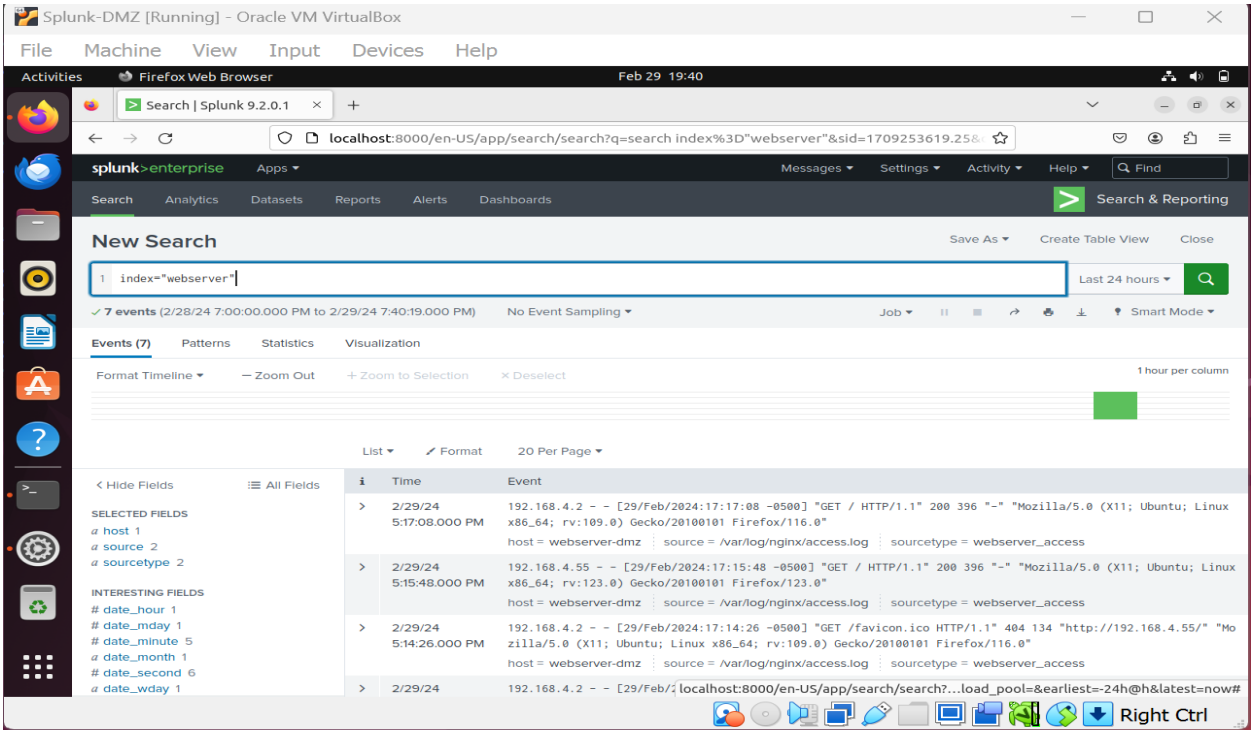

Figure 5/Splunk