

INSIDE-FIREWALL

Overview

The objective of this project was to extend the existing DMZ network by introducing an **inside firewall** and an **internal client3-inside machine**, while also updating **Splunk-DMZ** to receive firewall logs. This setup strengthened the segmentation between external, DMZ, and internal networks and provided additional visibility into network traffic.

The implementation included:

- Creating and configuring a **pfSense inside firewall**.
- Deploying a **Client3-Inside VM** to represent an internal host.
- Updating **Splunk-DMZ** to ingest logs from the pfSense firewalls.
- Verifying the new network and DHCP configuration.

Environment Setup

1. pfSense – Inside Firewall

- **VM Creation**
 - Cloned from existing *Outside-Firewall* VM in VirtualBox.

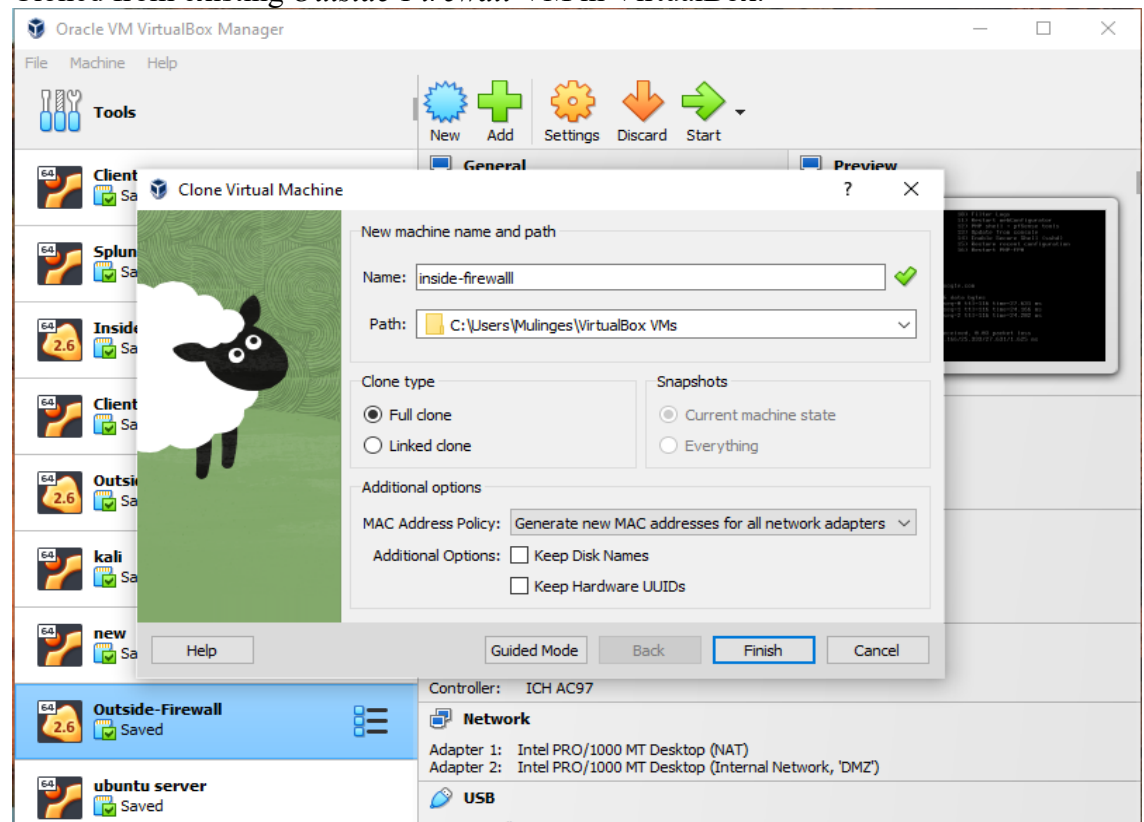


Figure 1/clone

- Name: *Inside-Firewall*.
- Clone type: Full Clone with a MAC address policy to generate new MAC addresses.
- **Networking**
 - Configured the networking for the new Vm by clicking the **Settings** button from the main window of the VirtualBox then navigated to **Network** and changed the network adapters below.
 - Adapter 1: Enabled and attached to Internal Network with an option of *DMZ*.

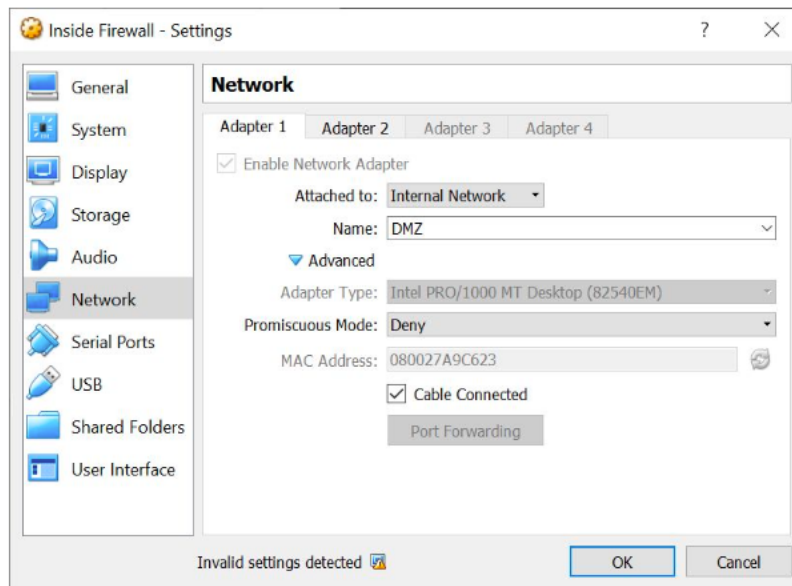


Figure 2/DMZ

- Adapter 2: Enabled and attached to Internal Network which I changed from intent to *Inside*. This presented the internal network that other VMs were attached to (Vms created later).

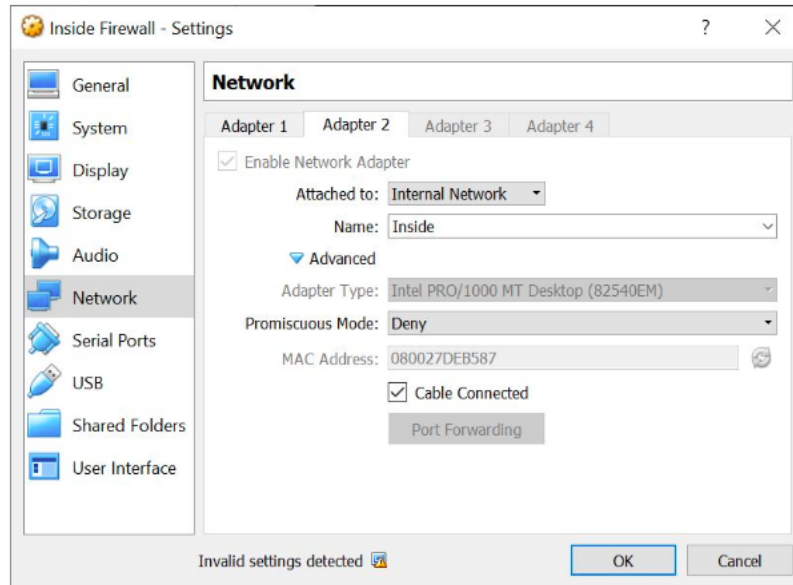


Figure 3/Inside Network

- **Interface Configuration-** I rebooted the VM (inside firewall) and choose **option 2** from the text-based menu and I populated it as follows:
 - WAN (em0):
 - WAN IPv4: **192.168.4.2**
 - Subnet Mask: **/24**
 - WAN upstream Gateway: **192.168.4.1** (Outside-Firewall LAN)
 - Enable the DHCP server: **N(no)**
 - Revert to HTTP as the webConfigurator protocol: **N(no)**
 - LAN (em1):
 - LAN IPv4: **192.168.2.1**
 - Subnet Mask: **/24**
 - DHCP enabled **Y (yes)**
 - Range: **192.168.2.100 – 192.168.2.200**
 - Revert to HTTP as the webConfigurator protocol: **N (no)**

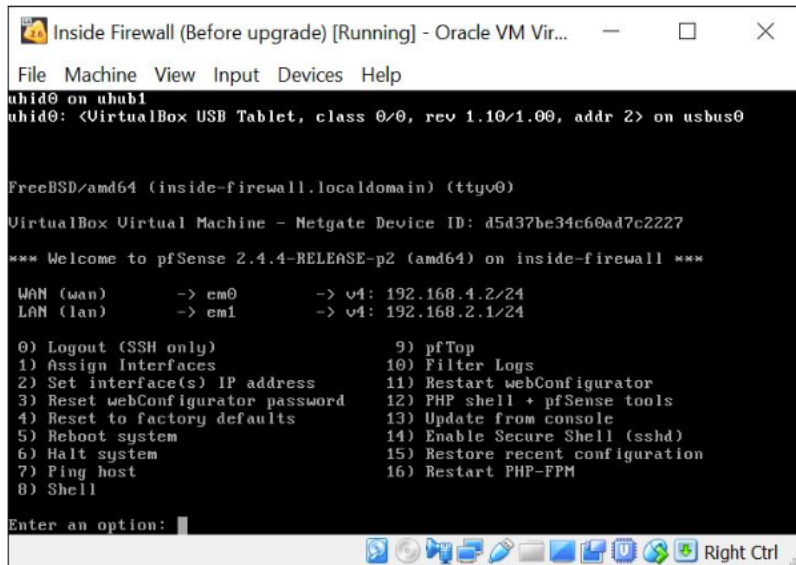


Figure 4/Inside Firewall

- **Verification**
 - Confirmed pfSense booted with the correct IP assignments.
 - Accessed pfSense webConfigurator at: **http://192.168.2.1**.
 - Logged in with default credentials **admin/pfsense**.

CLIENT3-INSIDE

- Cloned the existing Ubuntu VM (**Client1**) to create **Client3-Inside** using the same steps shown in the previous cloning lab.
- Reinitialized MAC addresses to avoid conflicts.
- Powered off the original VM before cloning to ensure consistency.

Network Configuration

- Modified Client3-Inside's **Adapter 1** settings in VirtualBox:
 - Changed from NAT → **Internal Network**.
 - Assigned to the **Inside** network segment.
 - Set **Promiscuous Mode** = **Allow VMs** to enable packet sniffing.

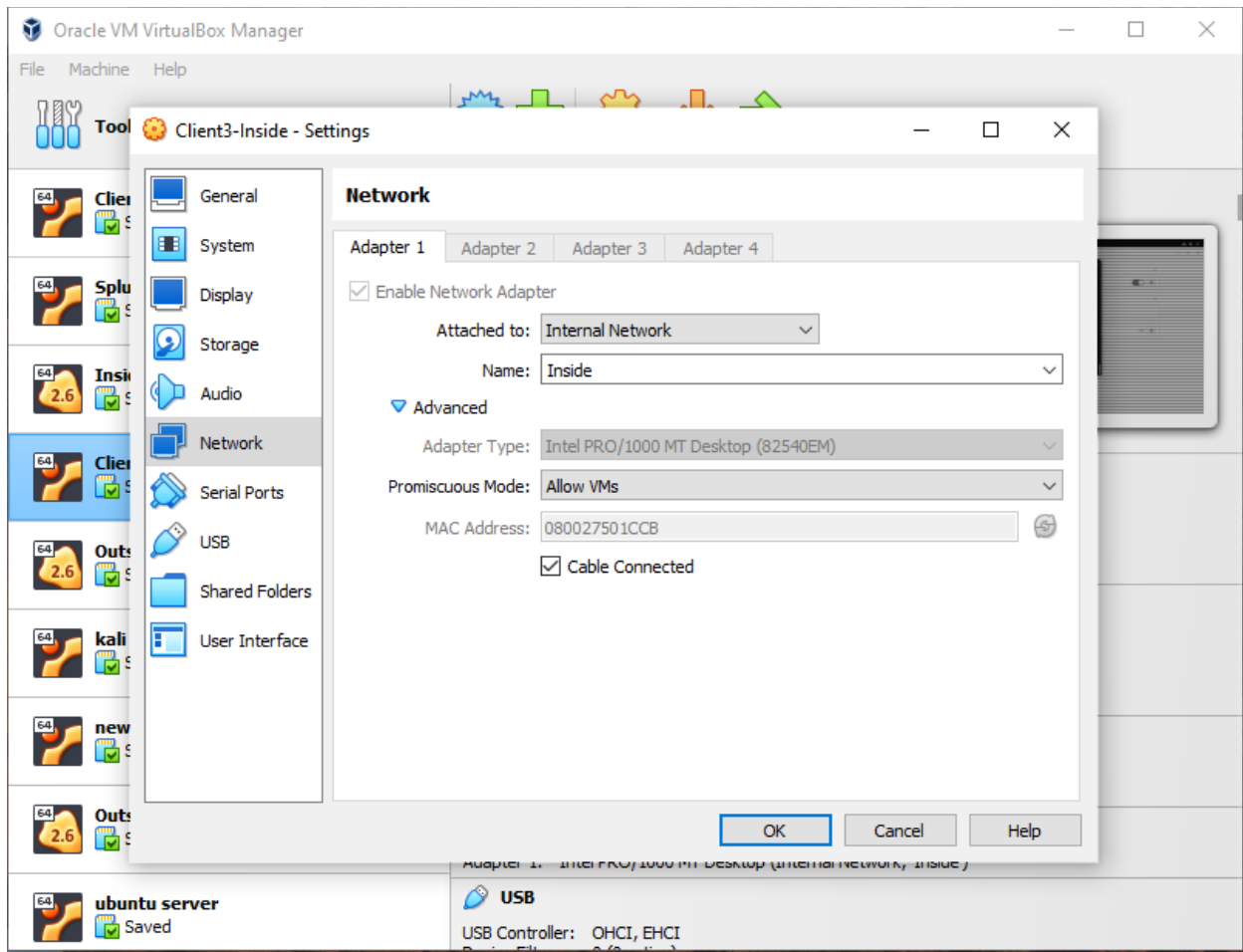






Figure 5/Client3

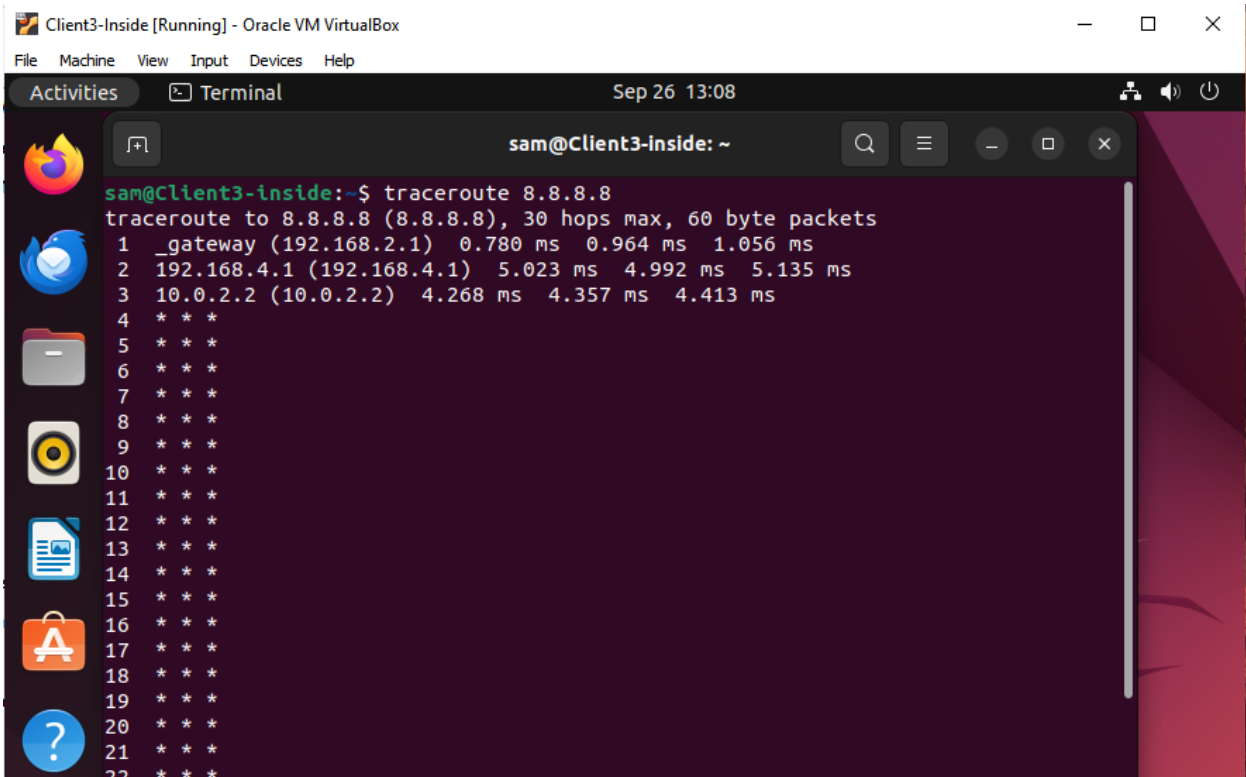
Ubuntu Network Setup

- Booted Client3-inside VM
- Verified network adapter under Ubuntu Network Manager.
- Configured **IPv4 to Automatic (DHCP)** to obtain an IP address from pfSense.
- Restarted the network interface using the following commands on my terminal:
- ***sudo ifconfig enp0s3 down***
- ***sudo ifconfig enp0s3 up***
- ***ifconfig*** -to confirm the correct Ip address

Connectivity Testing

- Verified connectivity to the **pfSense firewall**:
- pinged 192.168.2.1
- Accessed pfSense web interface via browser at:
http://192.168.2.1 → Successfully reached login page (admin/pfsense).
- Conducted additional network tests:

- ping 192.168.2.1  Inside firewall reachable.
- ping 192.168.4.1  Upstream gateway reachable.
- ping 8.8.8.8  Internet connectivity verified (IP-based, DNS configuration pending).
- traceroute 8.8.8.8  Confirmed correct routing path:
 - Hop 1 → **192.168.2.1 (Inside firewall)**
 - Hop 2 → **192.168.4.1 (Outside gateway)**



The screenshot shows a terminal window titled "Client3-Inside [Running] - Oracle VM VirtualBox". The terminal output displays the command `traceroute 8.8.8.8` and its results. The output shows the path from the local host to 8.8.8.8, with the first two hops being 192.168.2.1 and 192.168.4.1, which correspond to the firewall and gateway mentioned in the list above. The output also shows the number of hops, the IP address of the gateway, and the round-trip time in milliseconds for each hop.

```
sam@Client3-Inside:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 _gateway (192.168.2.1)  0.780 ms  0.964 ms  1.056 ms
 2 192.168.4.1 (192.168.4.1)  5.023 ms  4.992 ms  5.135 ms
 3 10.0.2.2 (10.0.2.2)  4.268 ms  4.357 ms  4.413 ms
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
```

Figure 6/Traceroute

Splunk-DMZ

Overview

The objective of this project was to configure the **Splunk-DMZ virtual machine** by assigning it a static IP address and connecting it to the **DMZ VLAN** within VirtualBox. This setup allows the Splunk instance to collect and analyze log data from both internal and external firewalls, establishing a centralized log management platform within the enterprise lab environment.

Implementation Steps

1. Update VLAN Configuration on VirtualBox for Splunk-DMZ

- Opened **VirtualBox** and selected the **splunk-dmz** virtual machine.
- Clicked **Settings** → **Network**.
- Under **Adapter 1**, confirmed that it was **Enabled** and changed:
 - **Attached To:** Internal Network
 - **Name:** DMZ
- This configuration connected Splunk-DMZ to the same **DMZ VLAN** network.

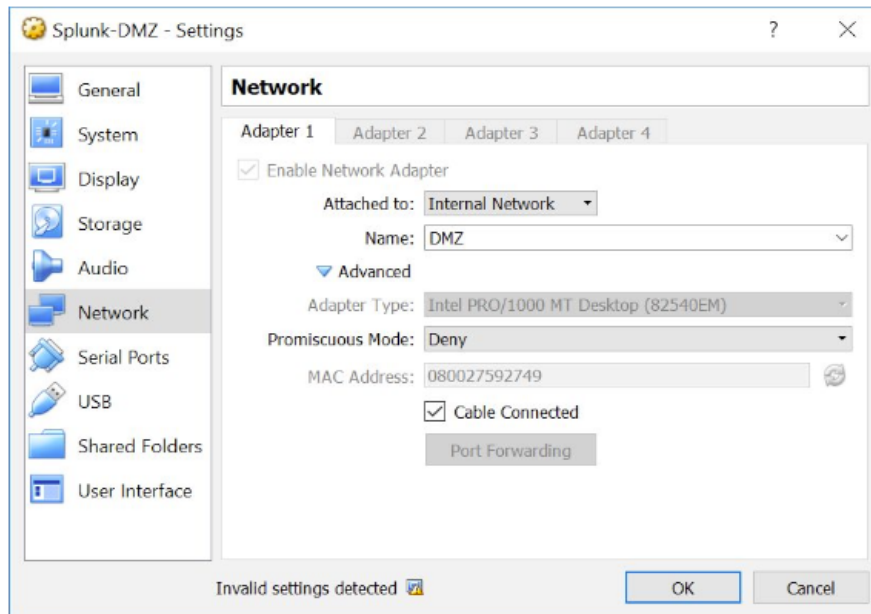


Figure 7/Splunk-dmz

2. Assign a Static IP Address in Ubuntu (Splunk-DMZ VM)

- Booted into the **Splunk-DMZ virtual machine**.
- Accessed the network settings through the **Networking icon** (top-right of the Ubuntu interface).
- Chose **Edit Connections** → **Wired Connection 1** → **Edit** → **IPv4 Settings tab**.
- Changed **Method** from *Automatic (DHCP)* to *Manual*.
- Entered the following network configuration:
 - **Address:** 192.168.4.20
 - **Netmask:** 255.255.255.0
 - **Gateway:** 192.168.4.1
 - **DNS Server:** 8.8.8.8
- Saved and closed the network settings window.

3. Verify and Apply Network Configuration

- Opened a **Terminal window** and executed the following commands to apply changes:

```
~sudo ifconfig enp0s3 down  
~sudo ifconfig enp0s3 up  
~ifconfig
```

- Verified that the **interface enp0s3** displayed the correct static IP address: 192.168.4.20.
-

4. Validate Connectivity

- Confirmed network connectivity by successfully pinging:
 - **Gateway (pfSense Outside Firewall):** ping 192.168.4.1
 - **External DNS (Google DNS):** ping 8.8.8.8
- Verified stable connectivity between **Splunk-DMZ** and other devices on the DMZ network.

Configure syslog input

Overview

The objective of this project was to configure **Splunk Enterprise** to collect and analyze **syslog data** from both the **Outside Firewall** and **Inside Firewall** pfSense systems. Also modify the virtual machine's IP address. This step enhances visibility into network traffic and security events, providing centralized log management for enterprise security monitoring.

Implementation Steps

1. Configure Syslog Input in Splunk

- Logged into **Splunk Enterprise GUI** at <http://localhost:8000>.
- Navigated to: **Settings** → **Data** → **Data Inputs** → **Local Inputs** → **TCP**.
- Added a new **TCP Syslog input**:
 - Port: **514**
 - Source name override: **syslog**
 - Source type: **Operating System** → **Syslog**
 - App context: **Search & Reporting**
 - Method: **IP**
 - Index: **Created new index** → **syslog**

Add Data Select Source Input Settings Review Done < Submit >

Review

Input Type	TCP Port
Port Number	514
Source name override	syslog
Restrict to Host	N/A
Source Type	syslog
App Context	search
Host	(IP address of the remote server)
Index	syslog

Figure 8/TCP Port

- Repeated the steps to configure a **UDP Syslog input** on port **514**, pointing to the same **syslog index**.

Add Data Select Source Input Settings Review Done < Submit >

Review

Input Type	UDP Port
Port Number	514
Source name override	syslog
Restrict to Host	N/A
Source Type	syslog
App Context	search
Host	(IP address of the remote server)
Index	syslog

Figure 9/UDP port

2. Configure Outside Firewall (pfSense) for Remote Logging

- Did the following steps from a web browser inside **Client2**.
- Accessed the Outside Firewall at <http://192.168.4.1>.
- Navigated to: **Status** → **System Logs** → **Settings**.
- Enabled **remote syslog logging**.

- Configured the **remote syslog server = 192.168.4.20 (Splunk-DMZ IP)**.
- Initially set logging to **forward everything**.
- Verified that syslog messages started flowing to Splunk.

3. View Syslog in Splunk

- Inside the Splunk Enterprise web GUI opened **Apps → Search and Reporting**.
- Ran initial search: **index=syslog**

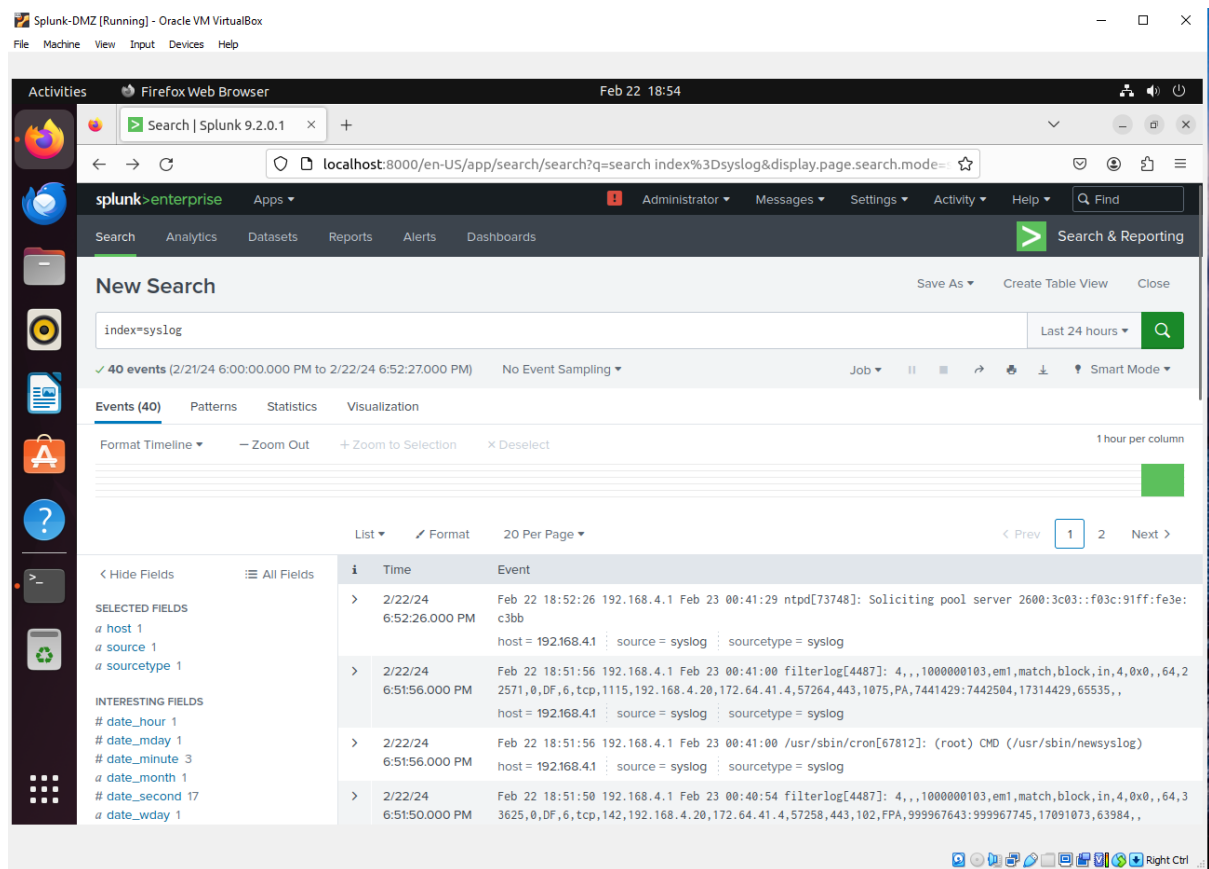


Figure 10/syslog

- Ran visualization query: index=syslog | chart count by host

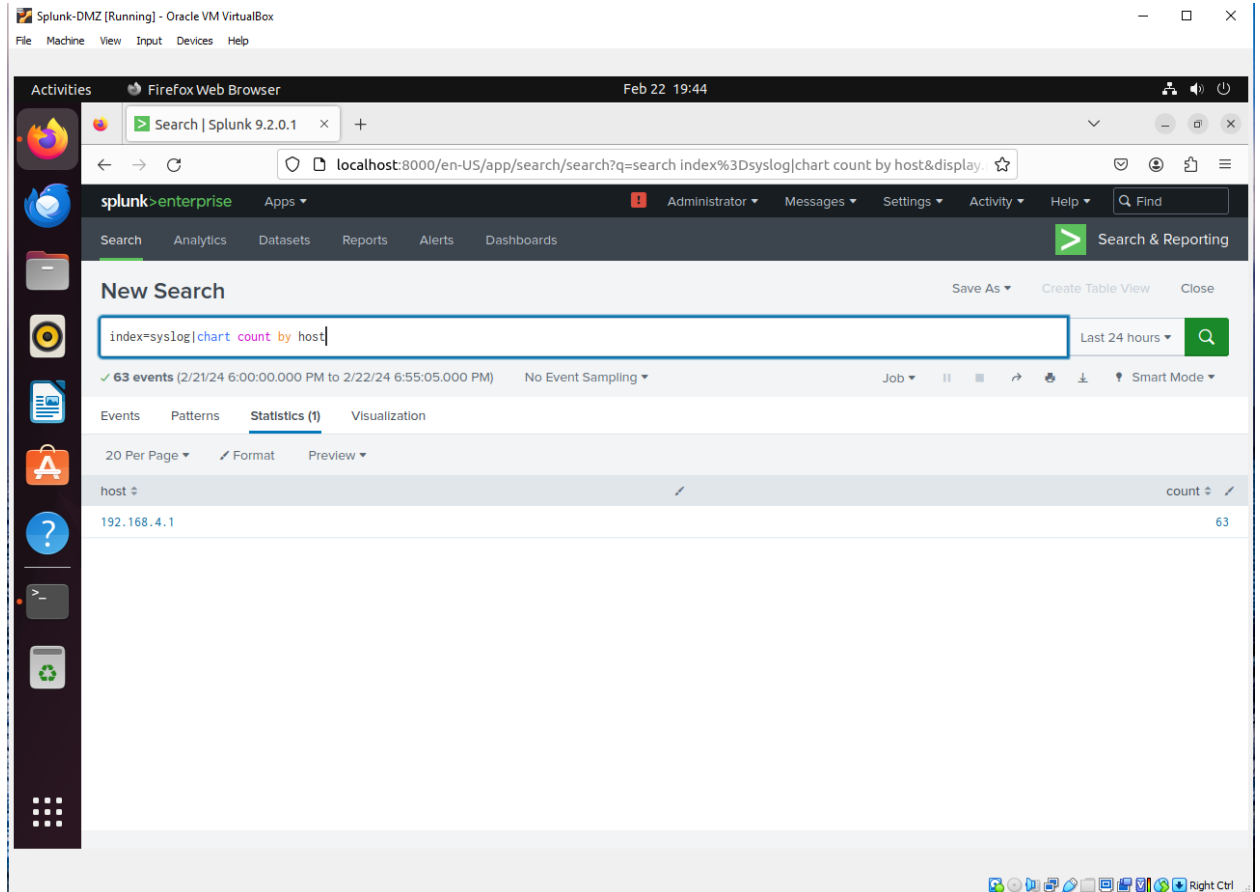


Figure 11/chart count

- Used the **Visualize** tab to generate charts and graphs of log activity.

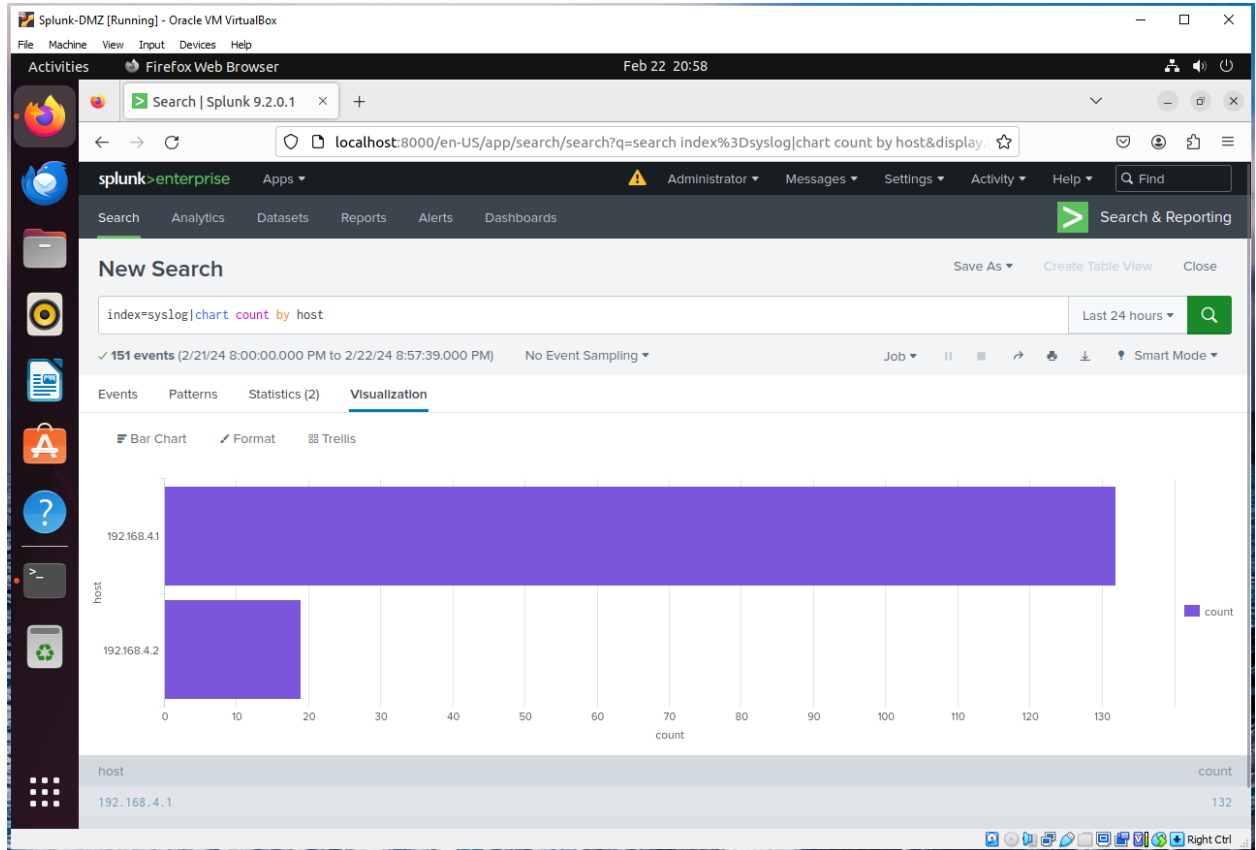


Figure 12/Visualization

4. Reduce Log Volume on Outside Firewall

- Adjusted syslog forwarding to reduce Splunk license usage (limited to 500MB/day).
- Modified **Status** → **System Logs** → **Settings**:
 - Disabled “Everything”.
 - Enabled only:
 - **Firewall Events**
 - **VPN Events**.
- Saved settings to ensure only relevant logs were forwarded.

5. Configure Inside Firewall (pfSense) for Remote Logging

- Followed the same procedure that I had used earlier to “configure Outside-Firewall for Remote logging” but this time on the Inside-Firewall.
- From **Client3-Inside**, accessed the Inside Firewall web GUI: <http://192.168.2.1>.

- Configured the Inside Firewall to forward logs to the **Splunk-DMZ server**.
-

6. Verify Multi-Source Syslog Data in Splunk

- In Splunk, reran:
- `index=syslog | chart count by host`
- Confirmed that logs were now being received from **both Outside and Inside firewalls**.
- Visualizations demonstrated successful multi-host log aggregation in Splunk.