MK Mahwete

Setting Up UFW Firewall Rules

This document will take you through setting up firewall rules for your Splunk cluster enhances security by only allowing essential traffic between the VMs. we'll use **ufw** (Uncomplicated Firewall) on each VM.

Step 1: Verifying IP address and Port numbers

We need IP addresses of our 3 VMs and port numbers. From the setting Static IP document we can confirm the following IP addresses:

- Index IP: 192.168.122.10
- Search Head IP: 192.168.122.11
- Forward IP: 192.168.122.12

Port numbers:

- 9997 → Indexer receiving data from forwarder
- 8089 → Splunk management (used between Search Head & Indexer)
- 8000 → Splunk Web UI (optional for search head/indexer)
- 22 → SSH (optional for remote config)

>> $————————————————————————————[26 April 2025]

Step 2: Install and Enable UFW on all VMs

Now make sure that ufw is installed and if now, use the following command to install and enable ufw:

```
sudo apt install ufw -y
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

- After the installation is complete for all VMs set firewall rules for each VM

Index VM (192.168.122.10)

```
sudo ufw allow from 192.168.56.0/24 to any port 9997 proto tcp
sudo ufw allow from 192.168.56.11 to any port 8089 proto tcp

Allow Splunk Web UI
sudo ufw allow from 192.168.56.0/24 to any port 8000 proto tcp
```

```
Allow SSH from your host (optional)
sudo ufw allow from 192.168.56.1 to any port 22 proto tcp

sudo ufw enable
```

- Set search rules after completing the above commands or setting this ones

Search Head VM (192.168.122.11)

```
sudo ufw allow out to 192.168.56.10 port 8089 proto tcp

Allow Splunk Web UI
sudo ufw allow from 192.168.56.0/24 to any port 8000 proto tcp

Allow SSH from your host
sudo ufw allow from 192.168.56.1 to any port 22 proto tcp

sudo ufw enable
```

- Set forwarder rules after completing the above commands

Forwarder VM (192.168.56.12)

```
sudo ufw allow out to 192.168.56.10 port 9997 proto tcp

Allow SSH from host
sudo ufw allow from 192.168.56.1 to any port 22 proto tcp

sudo ufw enable
```

- Now check UFW status and rules if they are set correctly, then reload the ufw

```
sudo ufw status numbered
sudo ufw reload
```