LAB 10 – Containerization+SIEM

By :- Faraz Ahmed

Table of Contents

1. GraylogServer Setup

- After installing basic GraylogServer and changing network configuration of that device, we enter “ip r” to check if the configurations are entered properly or not as highlighted in Figure 1.

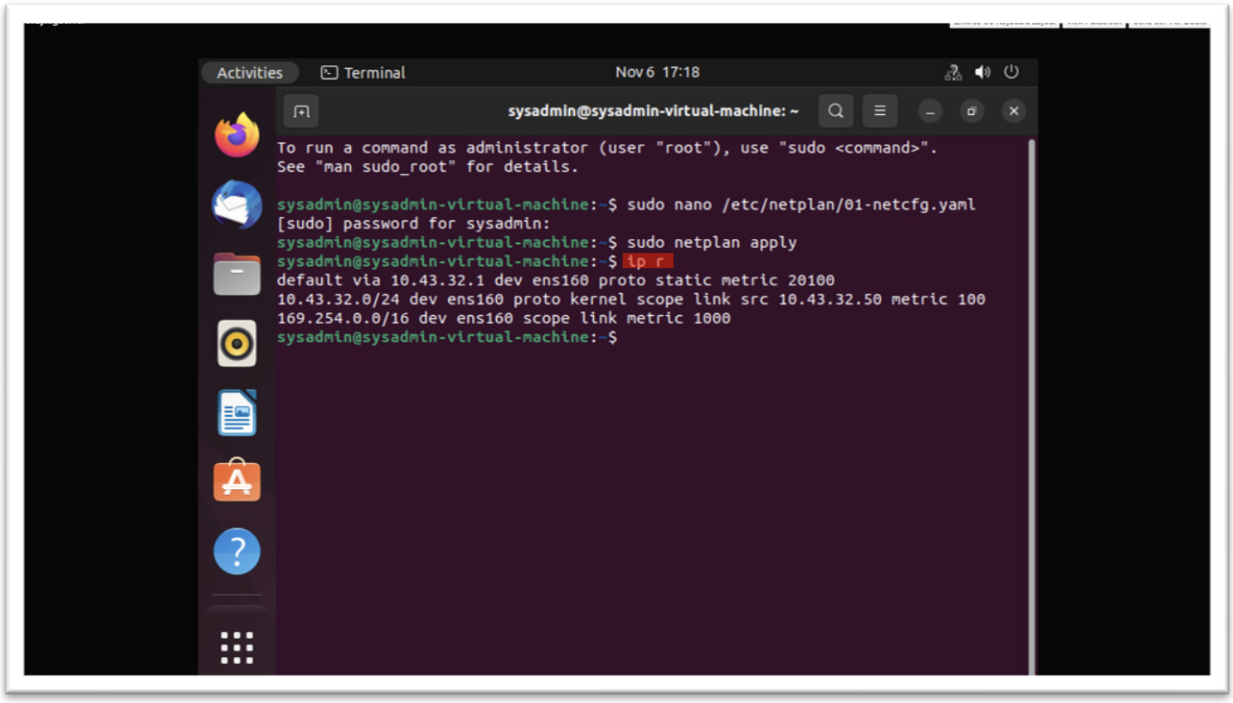

Figure 1: Screenshot of command “ip r” to check network configuration of GraylogServer.

- Now we enter command “sudo apt update” as highlighted below to update and upgrade the overall operating system in GraylogServer.

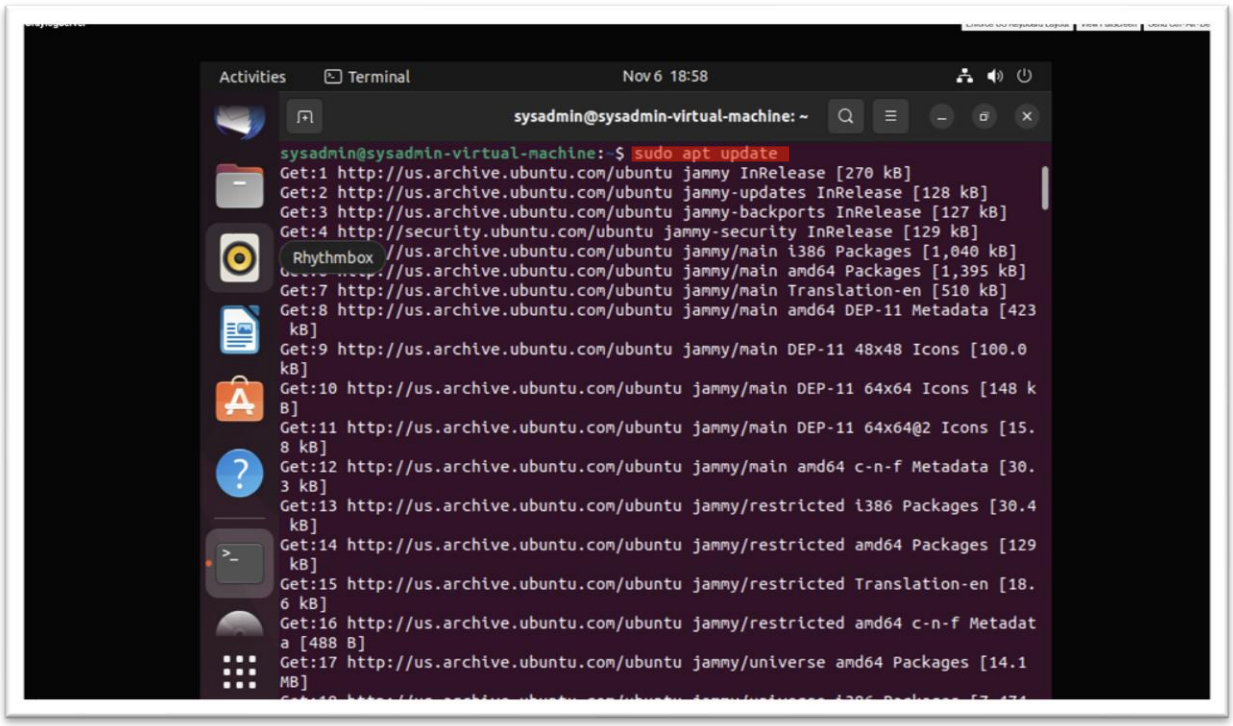

Figure 2: Screenshot of command “sudo apt update” to update O.S. of GraylogServer.

2. GraylogServer: Configure Graylog

- Then we install VMWare in GraylogServer and then enable it by inputting “sudo systemctl enable –now open-vm-tools”, then check the status by entering “systemctl status open-vm-tools” (as highlighted in figure 3) and from Figure 3 we can see that the VMWare is active and running.

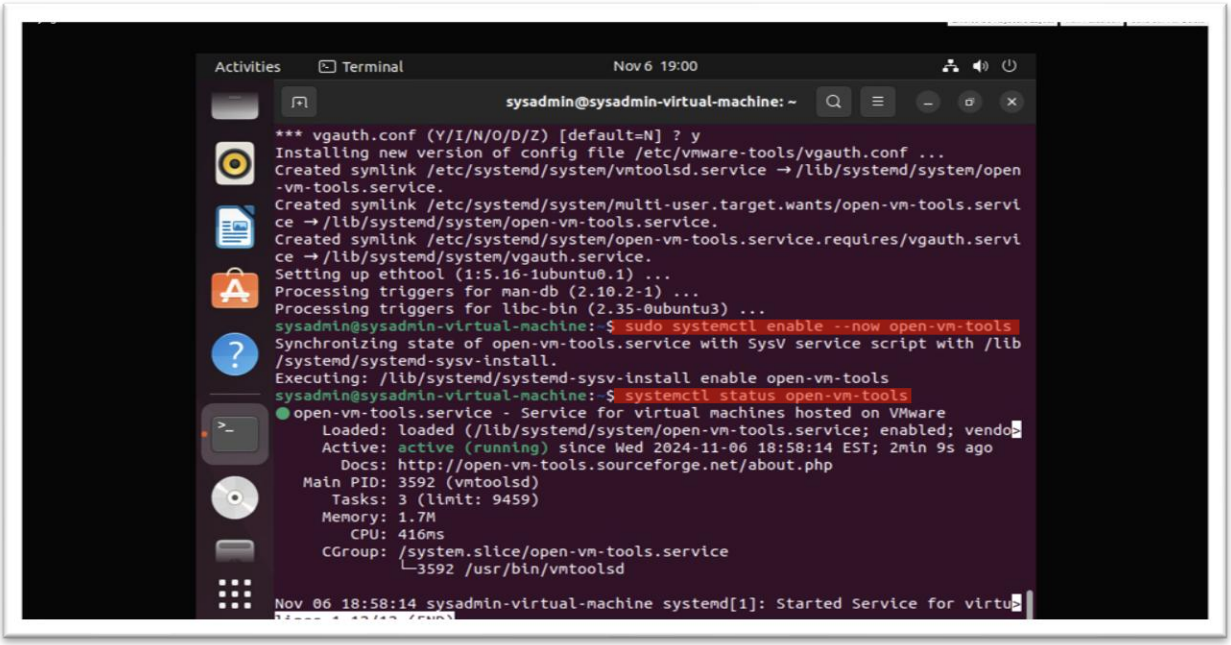

Figure 3: Screenshot of sudo systemctl enable –now open-vm-tools” to enable VMWare and “systemctl status open-vm-tools” to check the status of VMWare.

- By installing Docker, Docker compose and then Graylog using a docker compose .yaml file, we can access Graylog webpage using URL- http://10.43.32.50:9000 to enter admin as default username and password to open welcome page as shown in Figure 4.

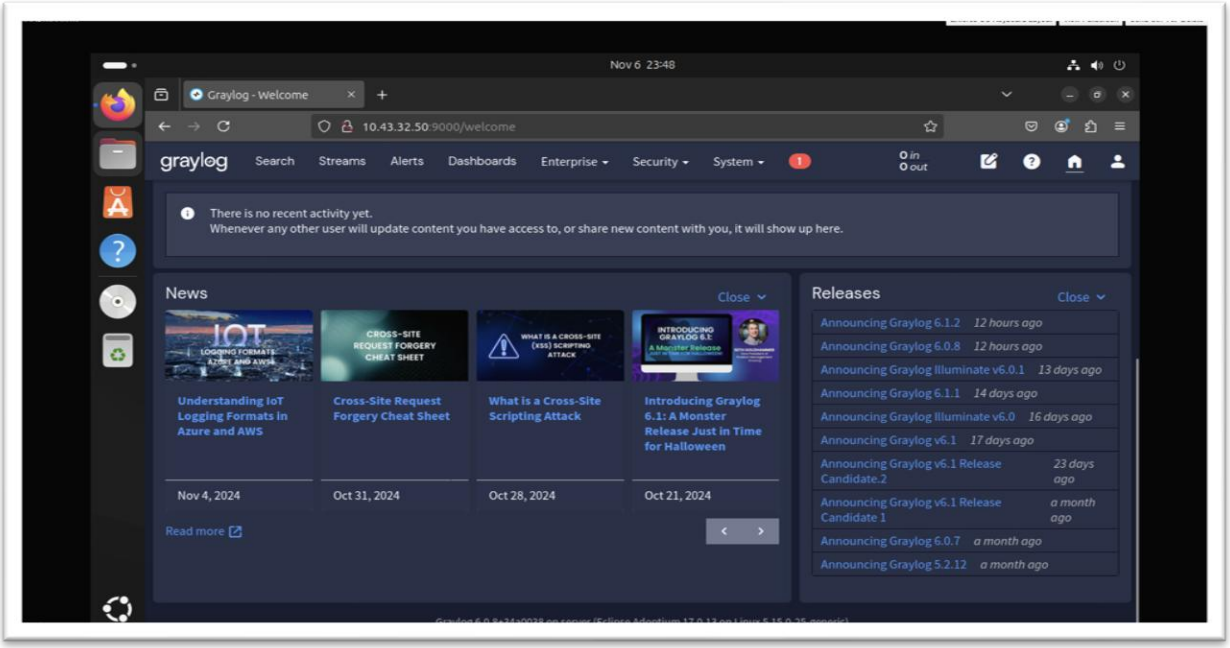

Figure 4: Screenshot of Welcome page of Graylog by entering “http://10.43.32.50:9000”.

3. Configure Graylog Forwarders

a. On Linux :-

- First we install rsyslog in Linux using command “sudo apt install rsyslog” as highlighted in Figure 5.

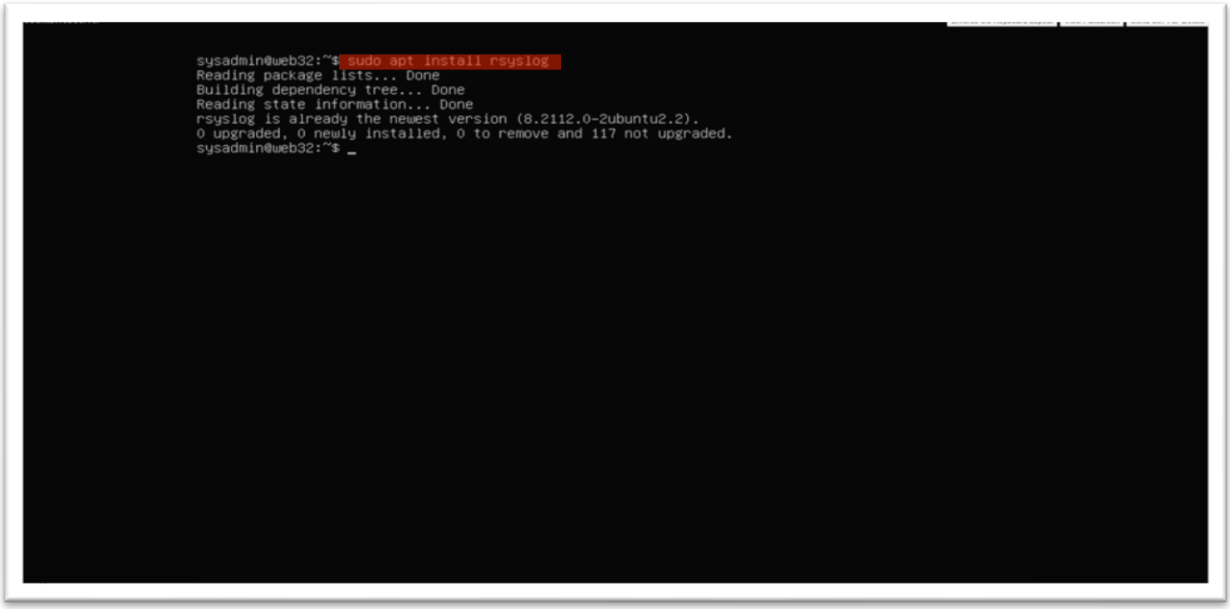

Figure 5: Screenshot of “sudo apt install rsyslog” to install rsyslog in Linux.

- After installing necessary files, we edit rsyslog configuration file using “sudo nano /etc/rsyslog.conf” and enter a new line - “*.* @10.43.32.50:5140;RSYSLOG_SyslogProtocol23Format” (as highlighted) and then Press CTRL+X then select Y to do Yes and then press Enter to exit the edit mode.

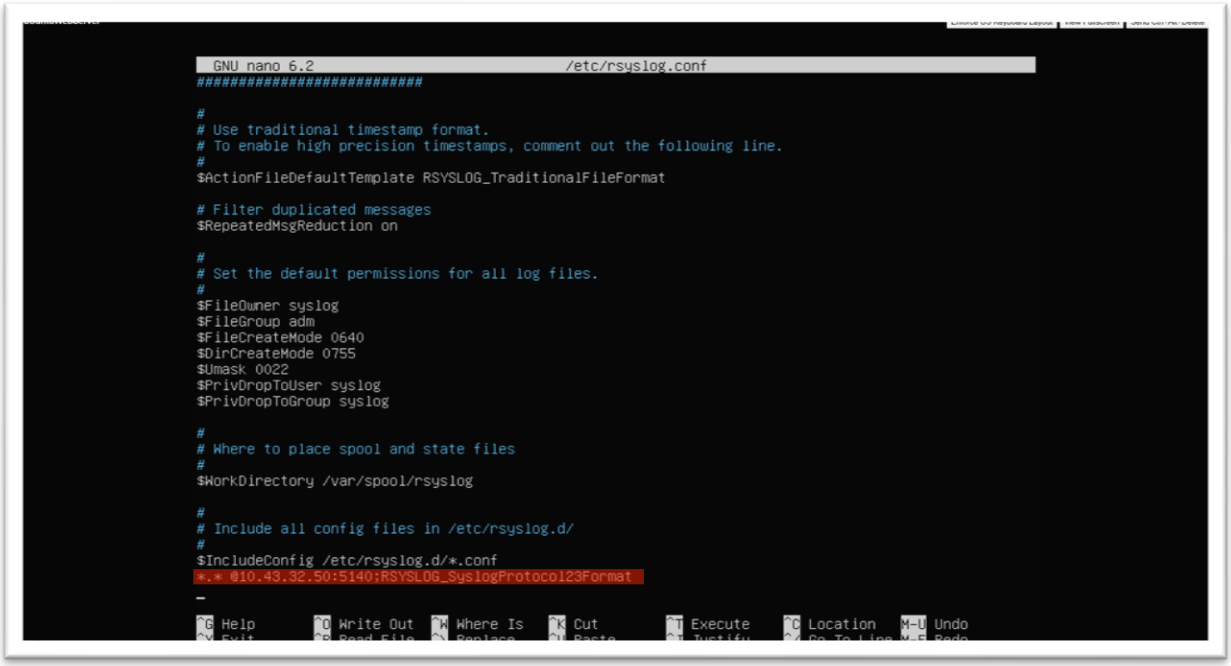

Figure 6: Screenshot of adding new line “*.* @10.43.32.50:5140;RSYSLOG_SyslogProtocol23Format” to edit rsyslog configuration.

- After that we will enter “sudo systemctl restart rsyslog” to start rsyslog services then enter “sudo systemctl status rsyslog” to check if rsyslog services are running or not as highlighted below.

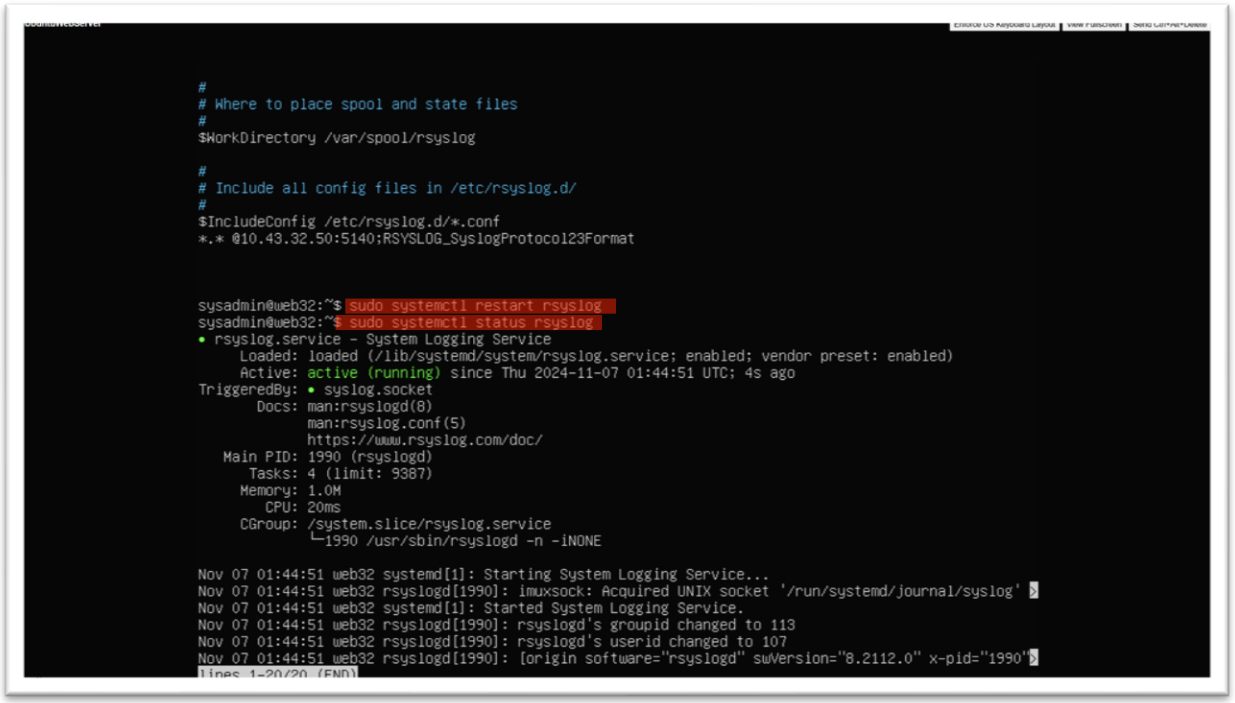

Figure 7: Screenshot of “sudo systemctl restart rsyslog” to restart rsyslog services and “sudo systemctl status rsyslog” to check if services is up and running or not.

b. On pfSenseRouter

- To configure rsyslog in pfSenseRouter, we navigate to “http://10.42.32.1” and go to Status → System Logs → Settings and under “Remote Logging Options” select Enable Remote Logging and enter GraylogServer’s IP- “10.43.3250:5140” and select Save.

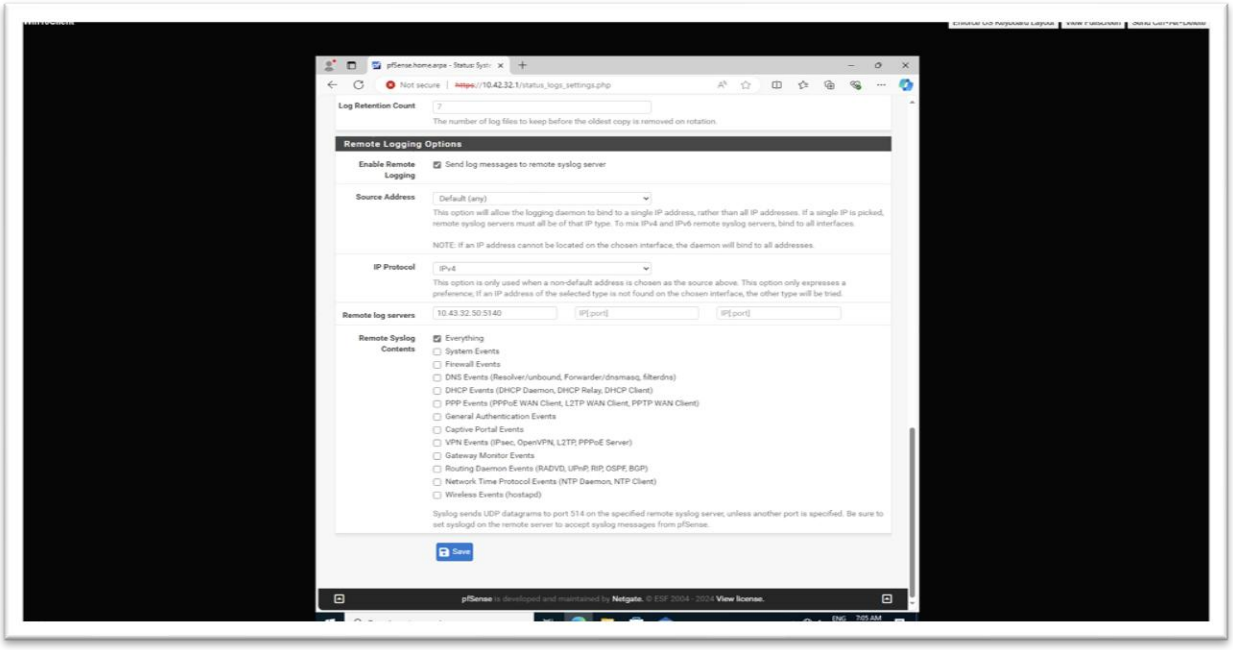

Figure 8: Screenshot of configure rsyslog in pfSenseRouter by “Enabling Remote Logging”.

4. Update Firewall Rules

- From Figure 9 we can see three highlighted firewall rules from which, first one is to “Allow HTTP access from UbuntuClient to GraylogServer” and second rule is “Allow traffic from AdminNet device to GraylogServer” and last one is “Block all other devices to access GraylogServer” to establish proper firewall rules.

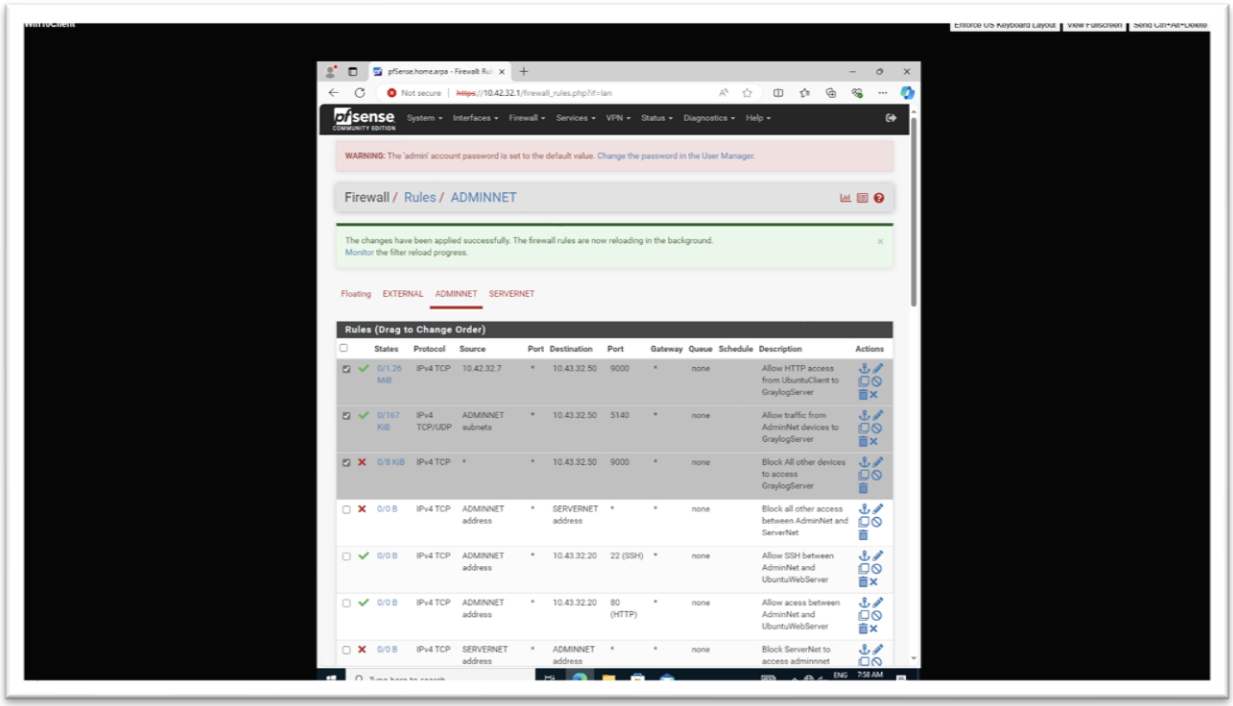

Figure 9: Screenshot of all three highlighted firewall rules.

5. Applied Graylog Capabilities

- ow we send SSH to UbuntuWebServer by entering SSH to their IP address like “ssh nonexistinguser@10.43.32.7”. Then we can note that the ssh was denied and fails. So, we can see the error message of SSH as shown in the Figure 10 in Graylog Web Server when we navigate to “Search → In search type- sysadmin and we can get the specific error of SSH.

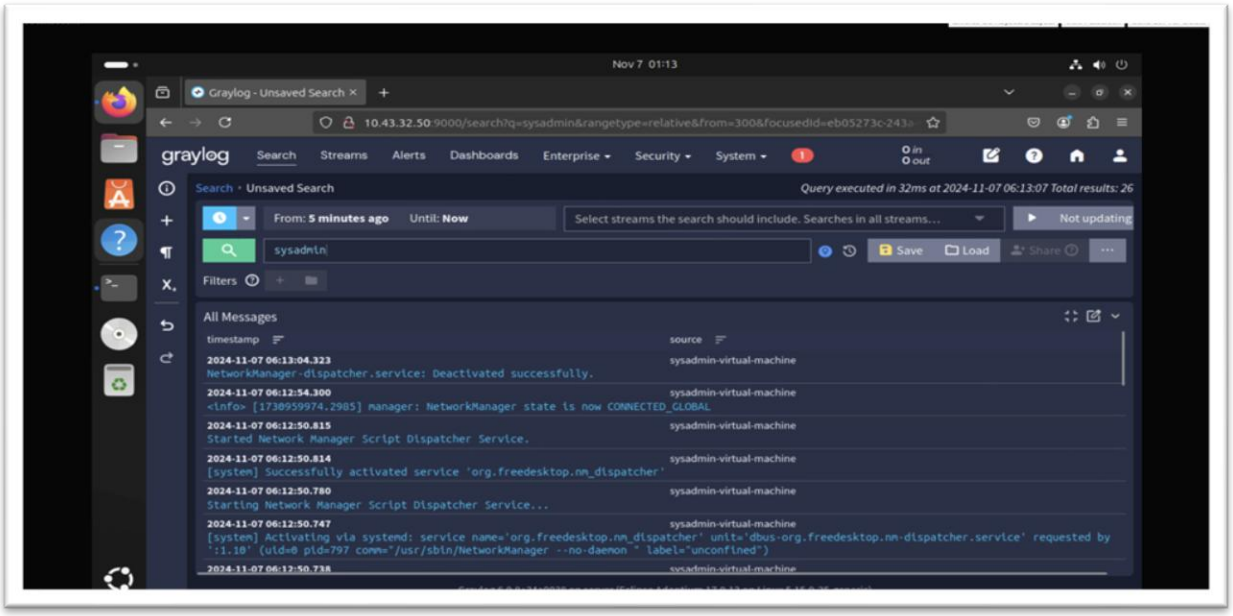

Figure 10: Screenshot of error message in “Search in Graylog Web Server”.

- Now after that we will navigate to Alerts → Events → Create new events (green button), then enter all the details for that event and press save to create it as a new alert for event. As we can see from Figure 11, alert for SSH failed for non-existent user on UbuntuWebServer (highlighted in Figure 11).

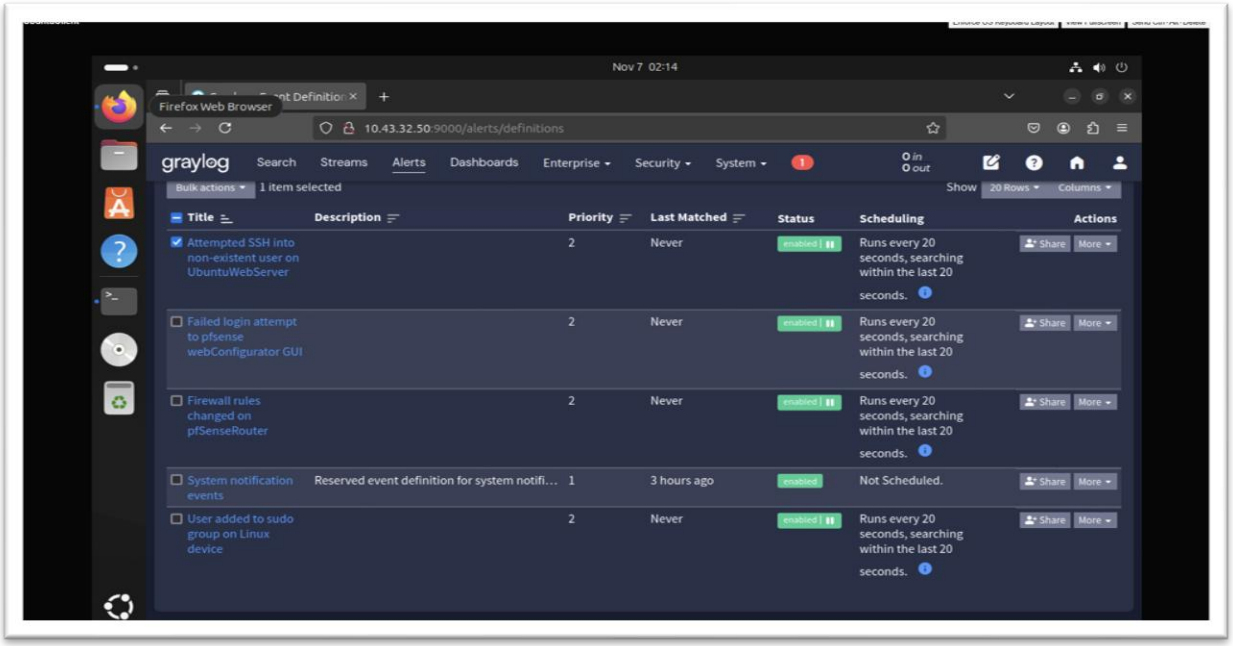

Figure 11: Screenshot of highlighted alert rule for “SSH for non-existent user on UbuntuWebServer”.

- So, we will do the same to make an alert rule for “Failed login attempts in pfsense webConfigurator GUI as shown in Figure 12.

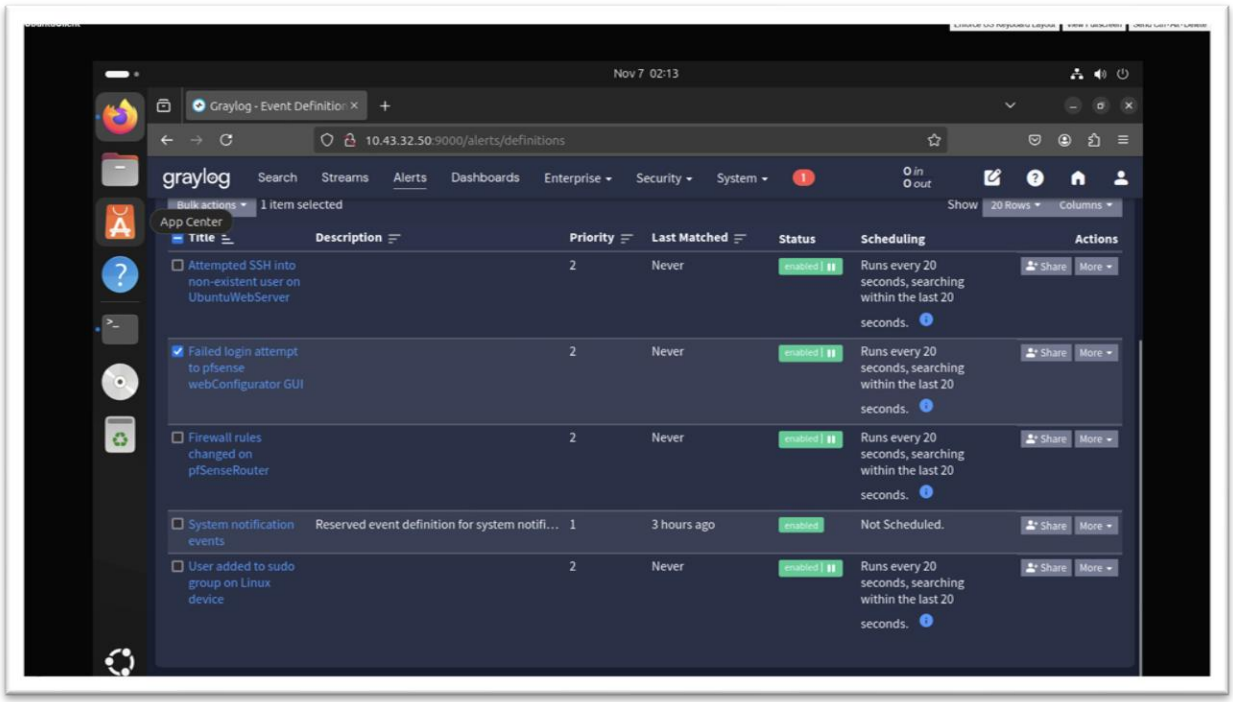

Figure 12: Screenshot of highlighted alert rule for “failed login attempt to pfsense GUI”.

- We will do the same to create alert rule for “firewall rules changed on pfSenseRouter” as shown in Figure 13.

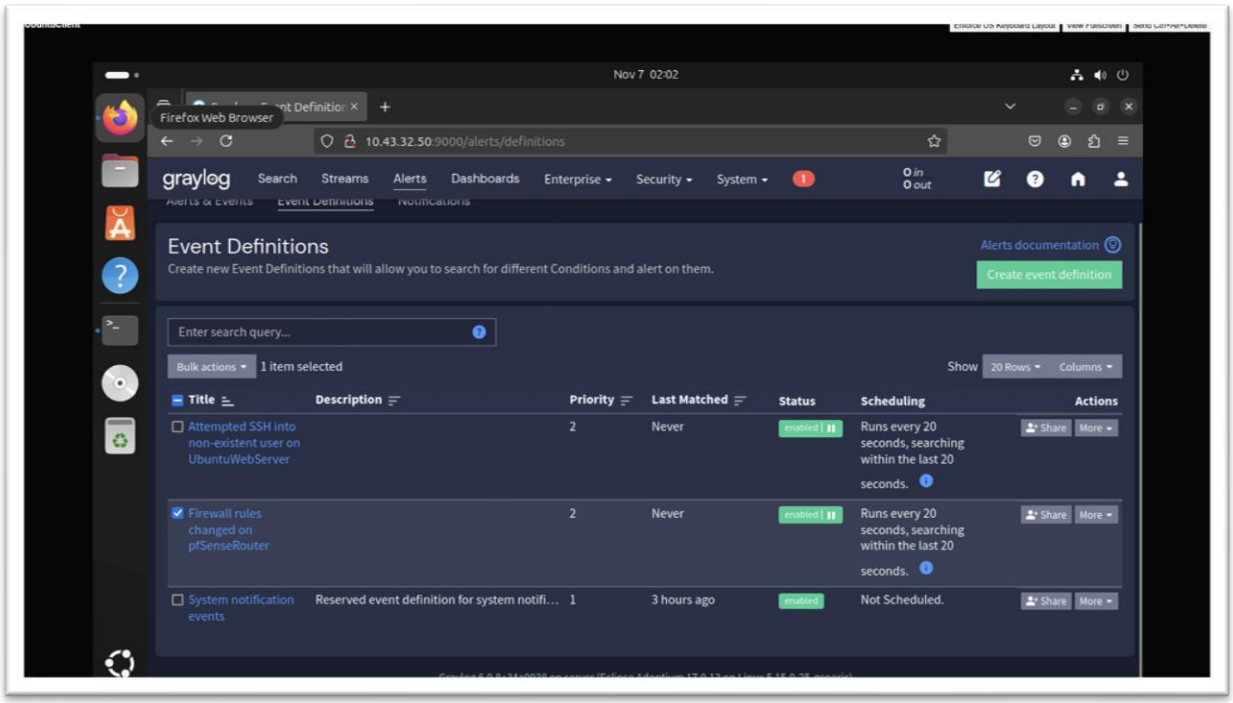

Figure 13: Screenshot of highlighted alert rule for “failed login attempt to pfsense GUI”.

- Now same we will do to create a new alert rule “user added to sudo group on Linux device” as shown in Figure 14.

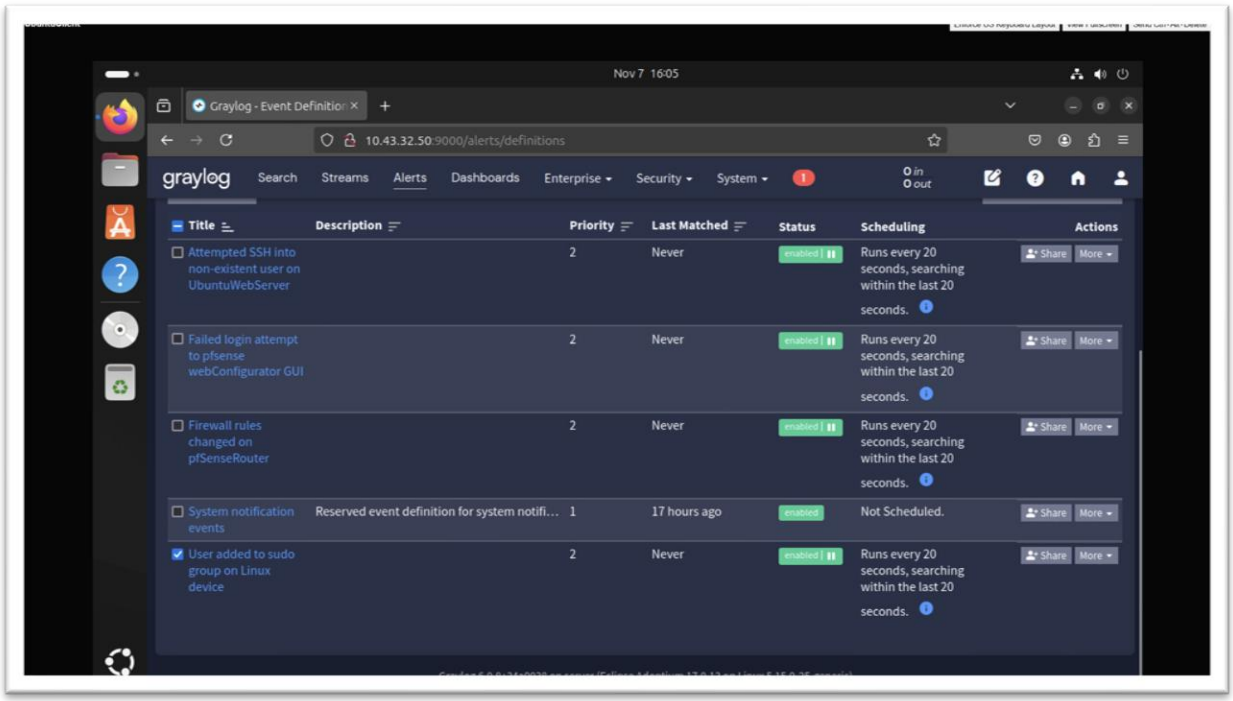

Figure 14: Screenshot of highlighted alert rule for “user added to sudo group on Linux device”.

6. Creating new alerts and a dashboard

- Navigate to “Dashboard option” and then select **“**Create a new dashboard” then add new “Events Overview” and add widgets to it by selecting plus symbol in the left and adding “time range by selecting drop down near clock icon”. Using this we can make a proper organized alert system and dashboard as shown in Figure 15.

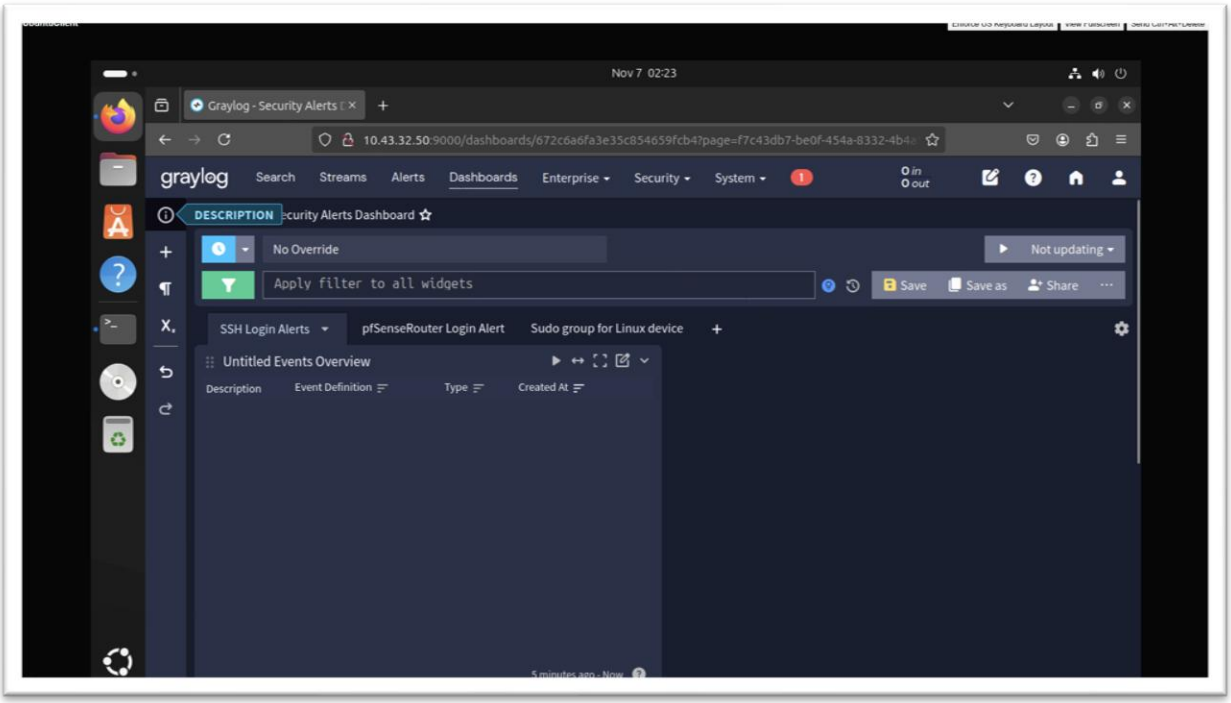

Figure 15: Screenshot of creating new dashboards and alerts in Graylog Web Server.

7. Update Topology

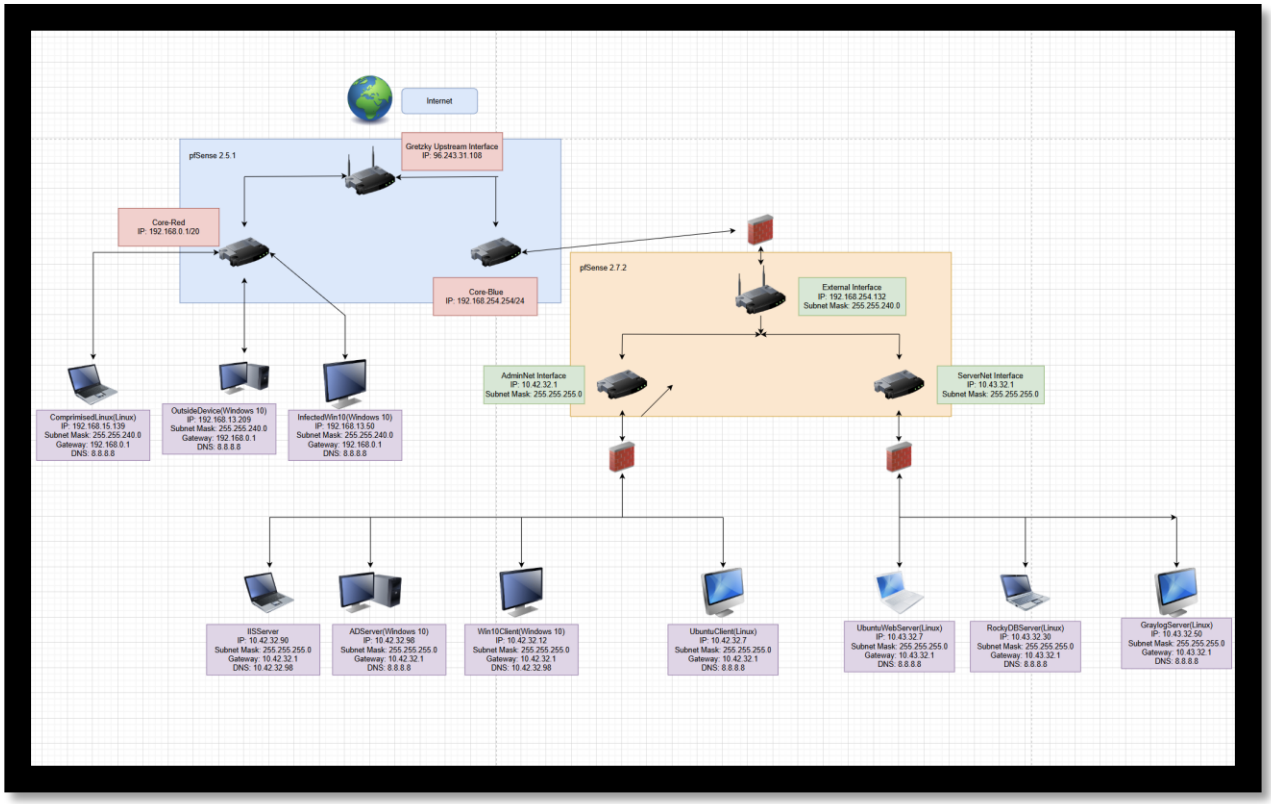

Figure 16: Screenshot of Updated Topology.