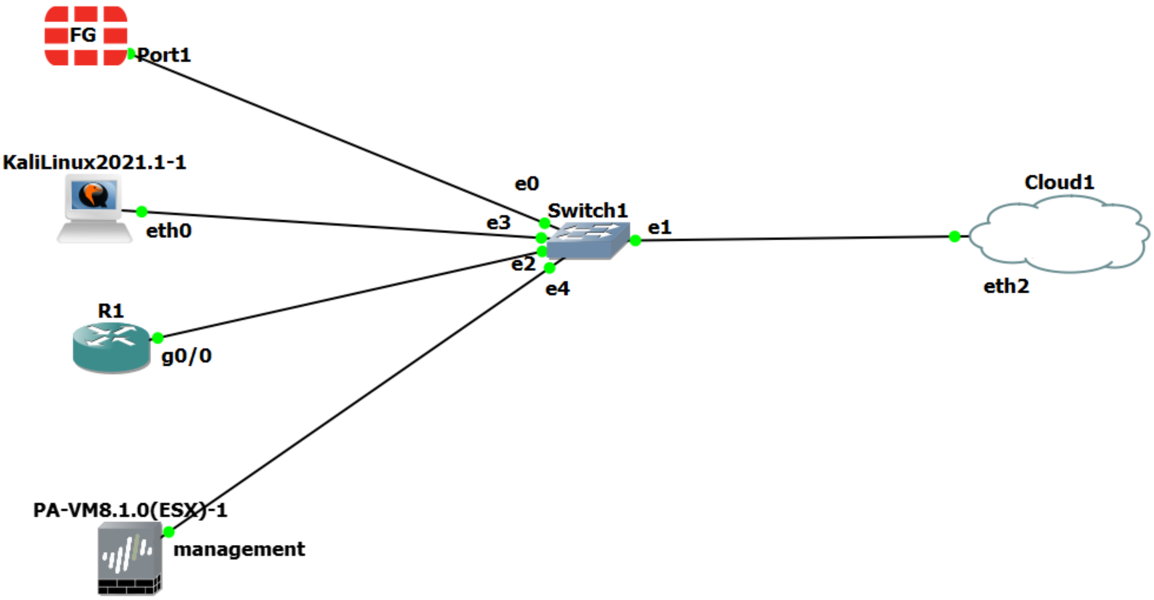

Based on the above diagram, configure the following steps:

1- (10%) Send Syslog from

- ✔ Kali(You can use any distributions) on port 5519,
- ✔ Cisco on port 5517 (Install Cisco App)
- ✔ Palo Alto on port 5518 (install Palo Alto App)
- ✔ FortiGate on Port 514 (install FortiGate App)

To Splunk, and create a single dashboard for all devices

2- (10%) Import the attached log on Splunk and show all queries in a single dashboard
https://drive.google.com/file/d/1uOcK8bQ_3JqECMp_3lGT2GZOFJ6toQxG/view?usp=drive_link

- count the number of failed password attempts for user root
- count the number of IP addresses and show the top 10.
- show top 5 port numbers used for ssh2
- show top 5 opened session usernames.

3- (10%) Send all step1 logs to PRTG software.

Evaluation:

- 30% configuration
- 10% Documentation

Time to Submit : Before Nov 22nd 2023