Server Setup: Setting up the Network

Branson Bailey

Home Lab Project

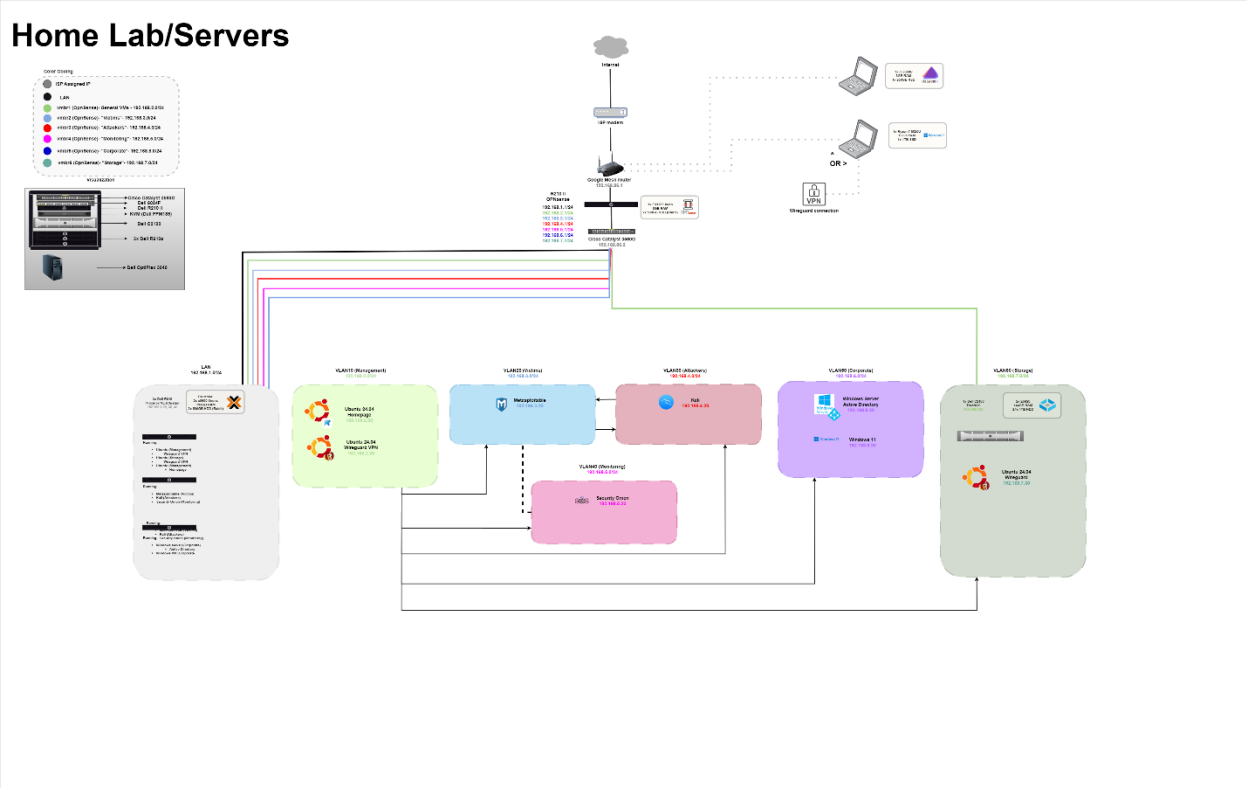
10 December 2024

Table of Contents

Project Focus

The focus of this project is to deploy OPNsense (24.7) in my home lab environment on an R210 II. This will provide the networking foundation for all of my future home lab activities.

Attached below is a basic overview of the desired network topology for my home lab setup:

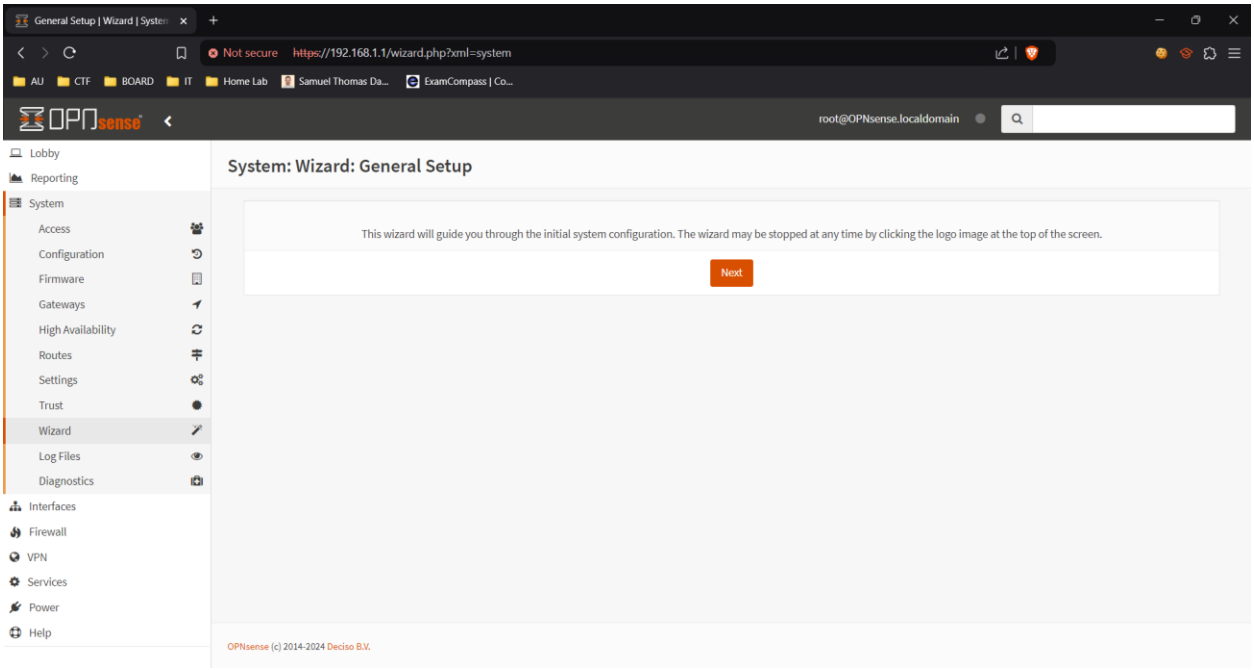


End-Goal Network Topology

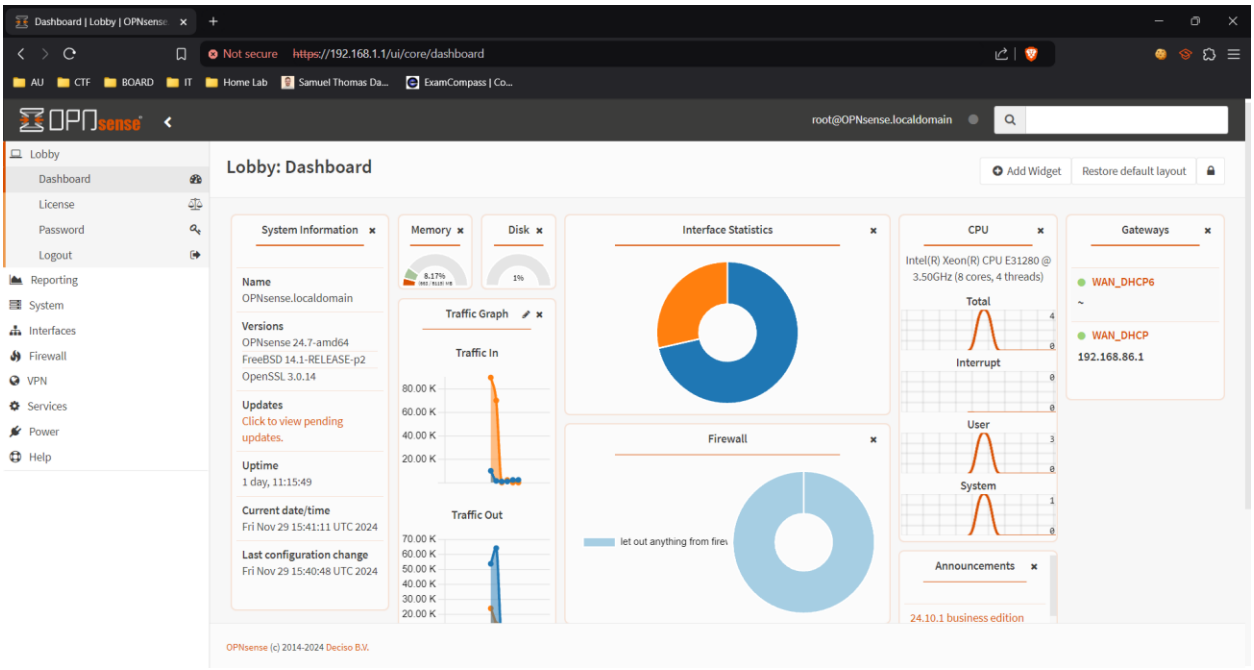
Network Setup Process

In this part, I will display the process of setting up the network in OPNsense. This writeup will begin on the web access site after doing some basic configuration in the CLI.

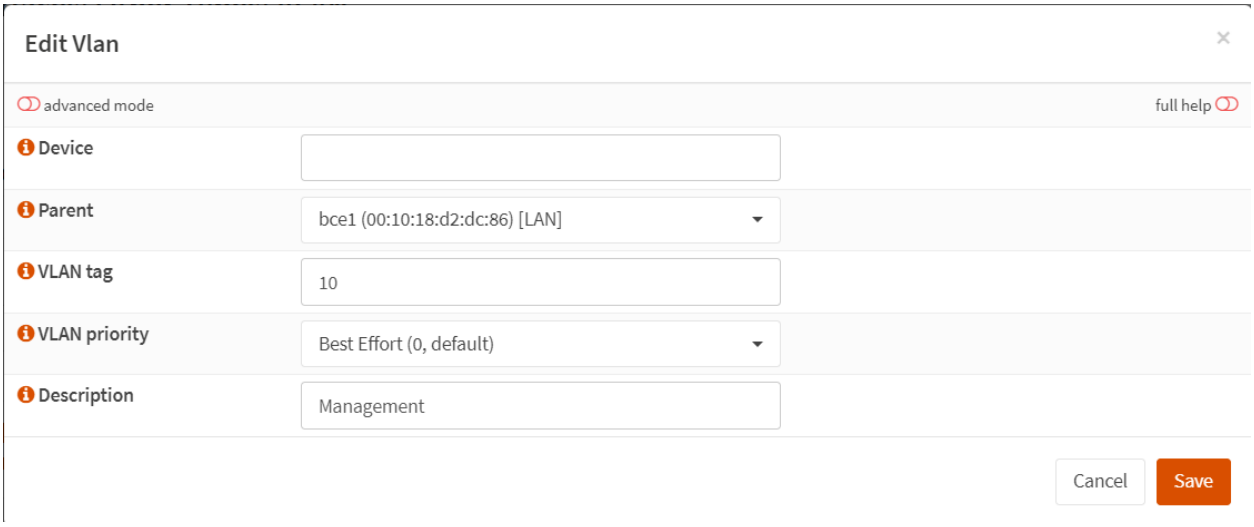
Link to image download: https://opnsense.org/download/



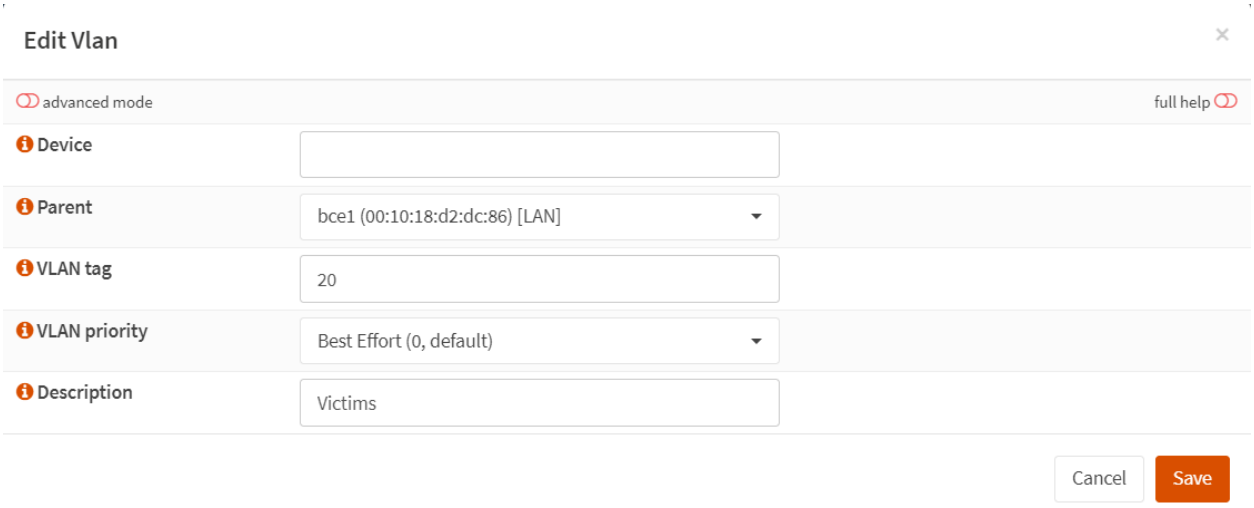
Here is the initial screen you are greeted with!



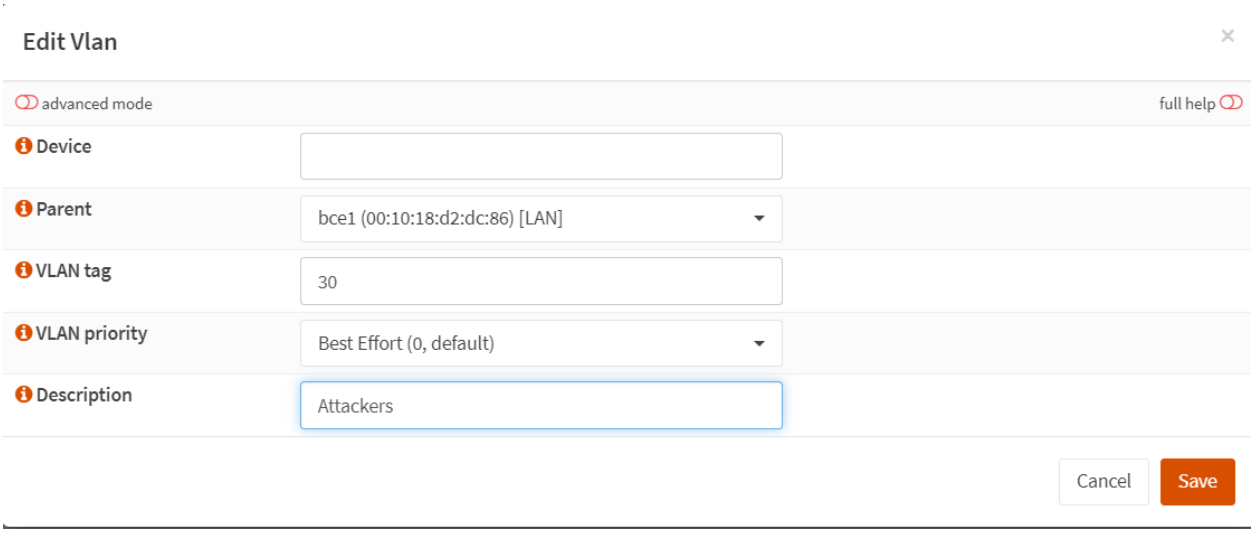
This is what the dashboard looks like. Here you can see general information about the node



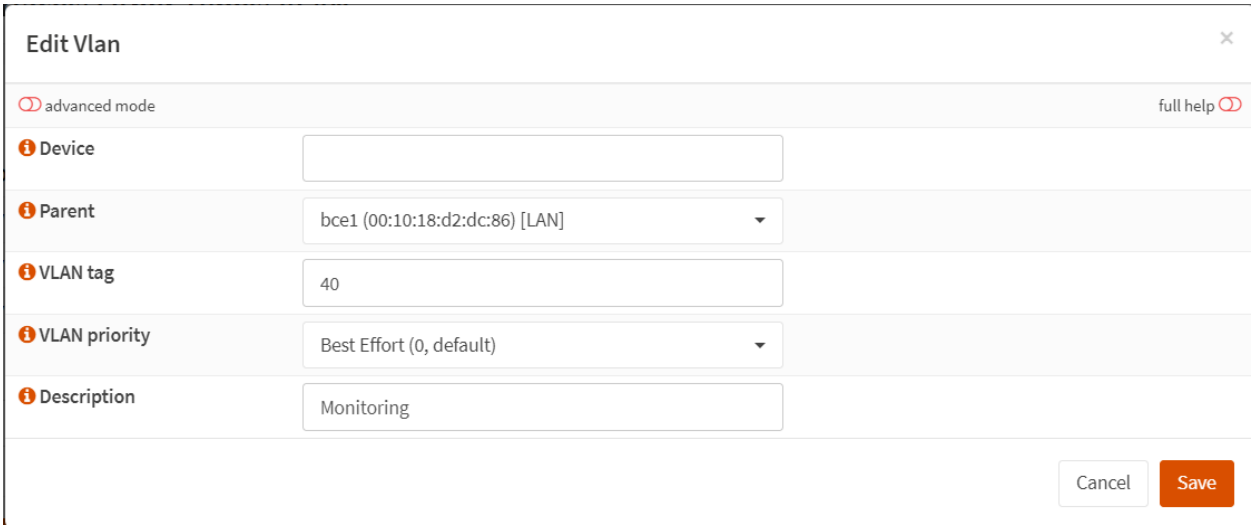
Here I am setting up the Management VLAN



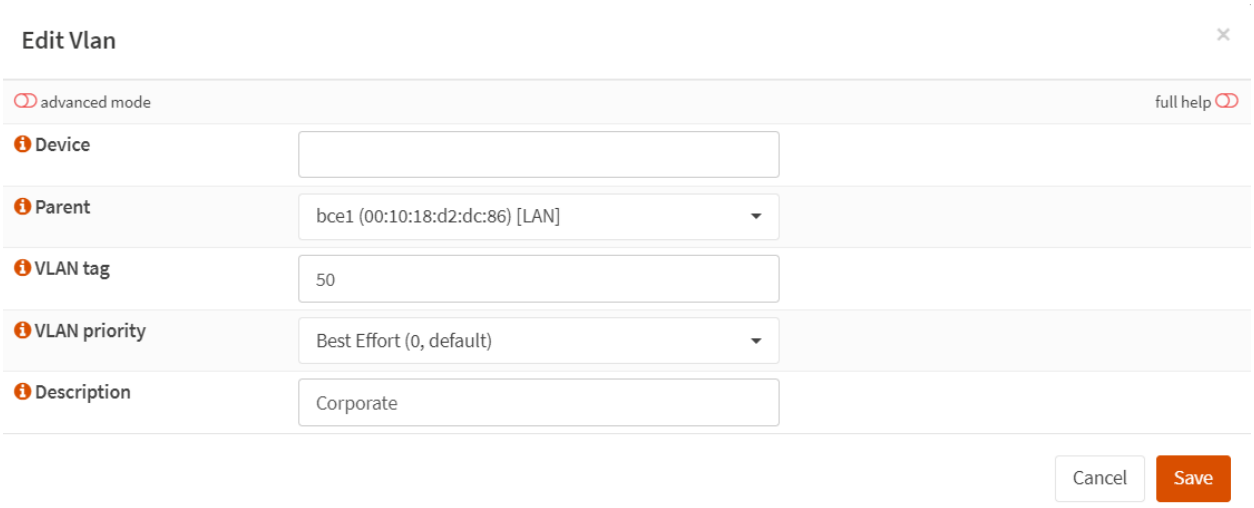
Here I am setting up the Victims VLAN



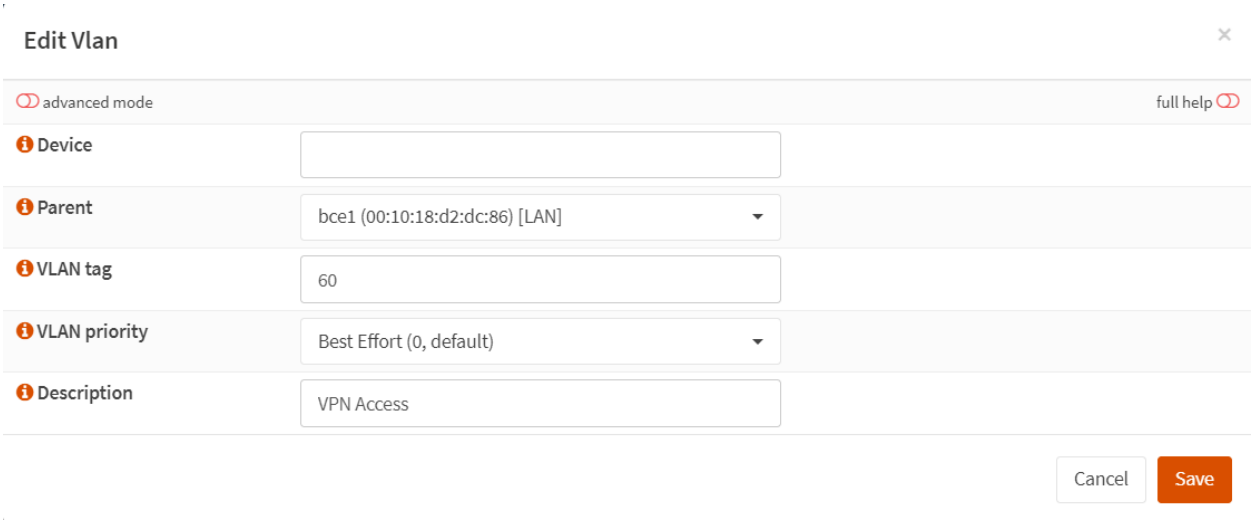
Here I am setting up the Attackers VLAN



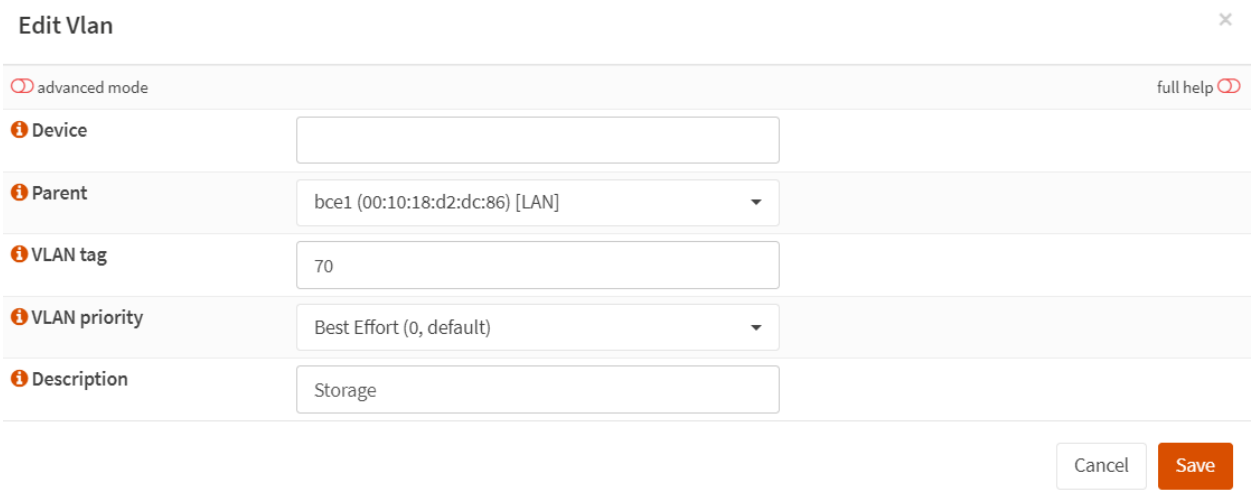
Here I am setting up the Monitoring VLAN



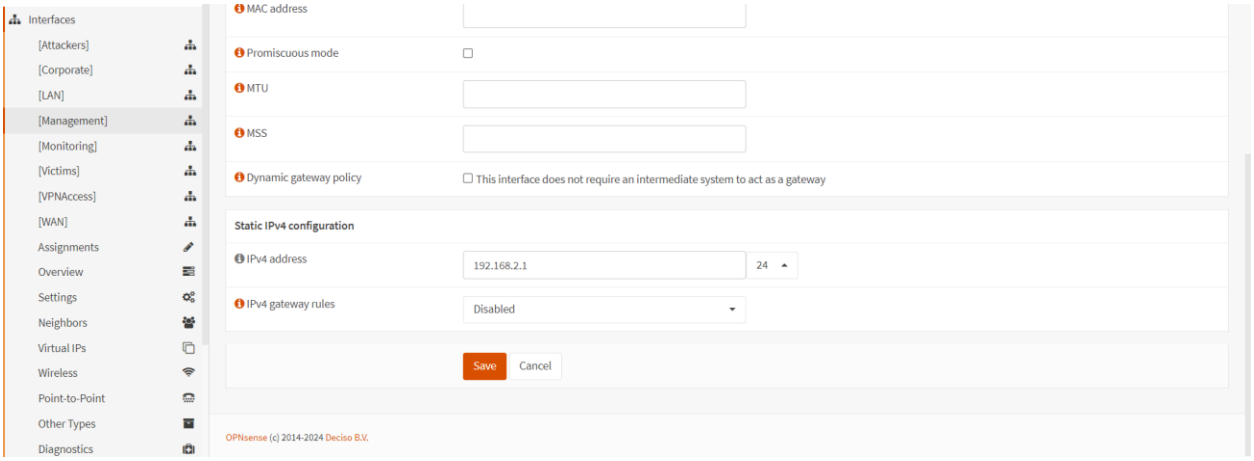
Here I am setting up the Corporate VLAN



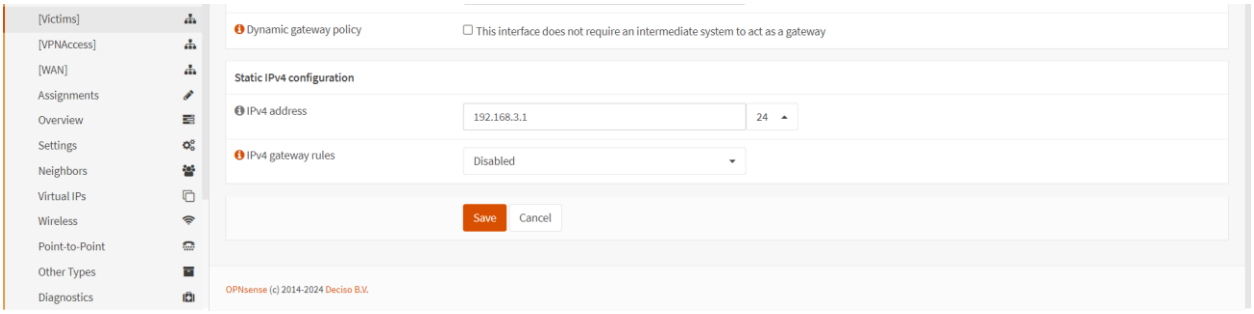
Here I am setting up the VPN Access VLAN



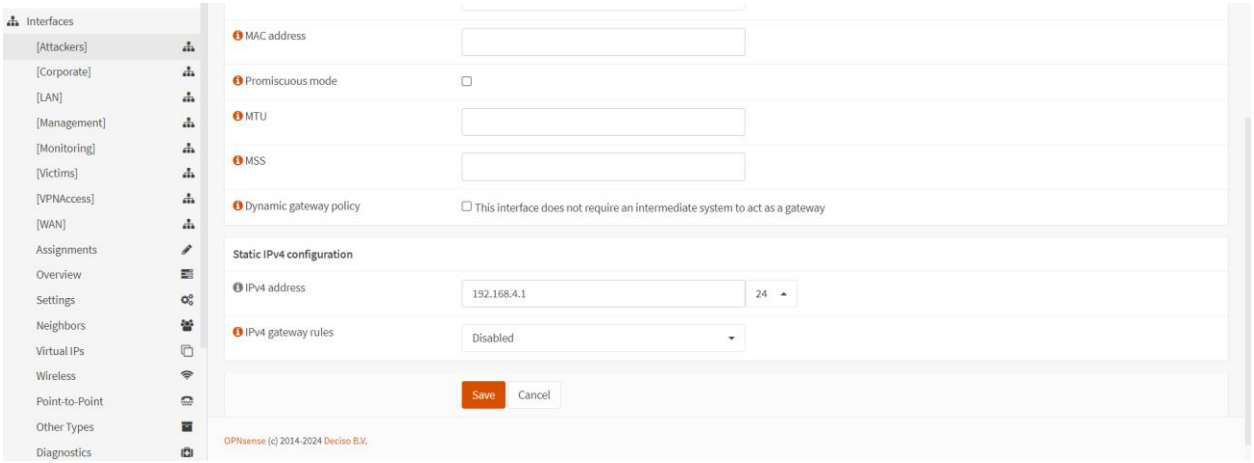
Here I am setting up the Storage VLAN



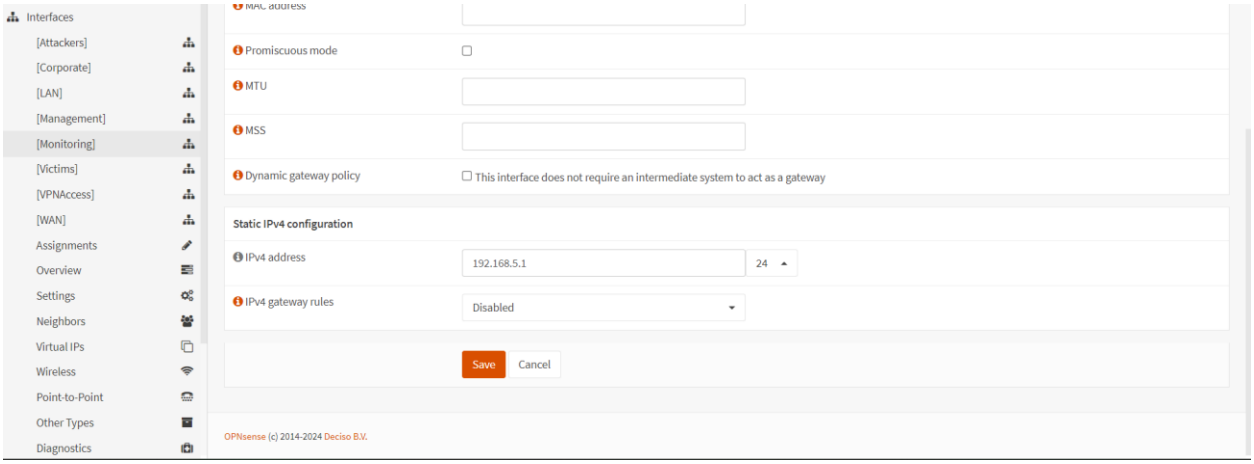
Here I am configuring the interface for the Management VLAN



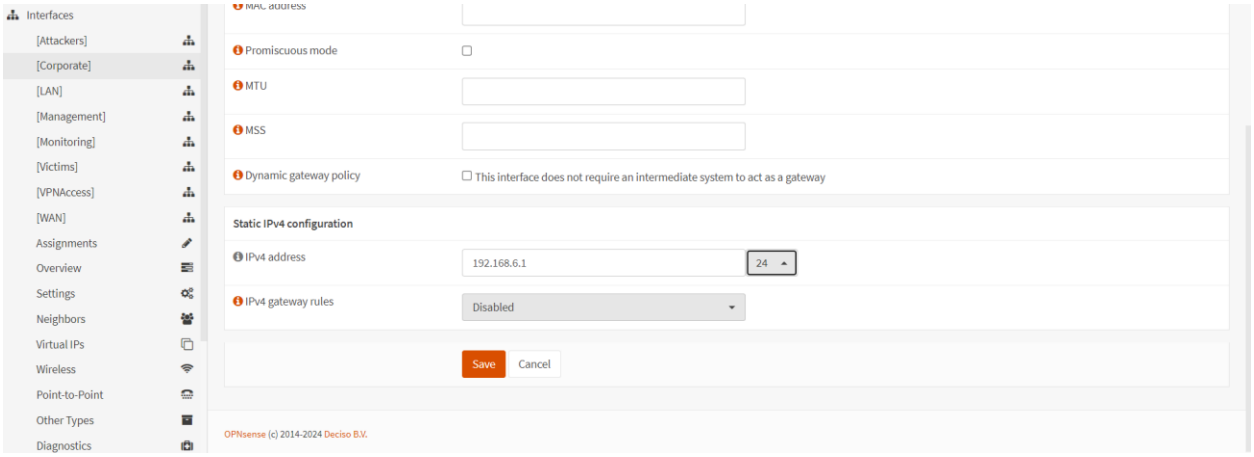
Here I am configuring the interface for the Victims VLAN



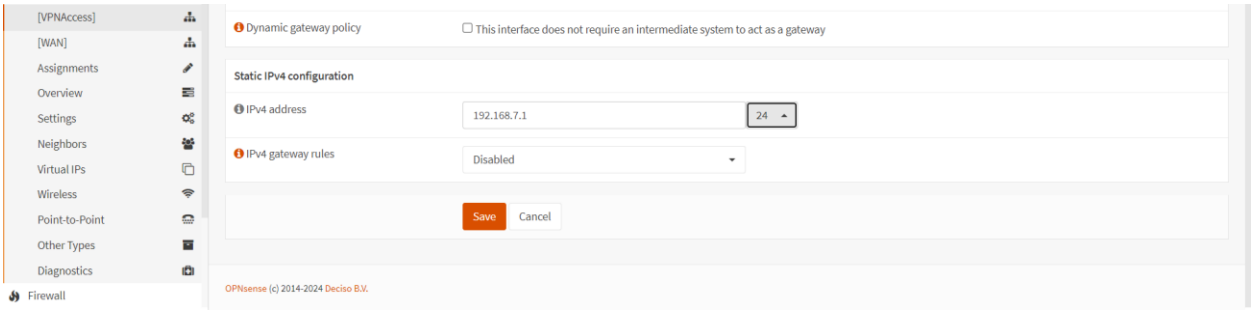
Here I am configuring the interface for the Attackers VLAN



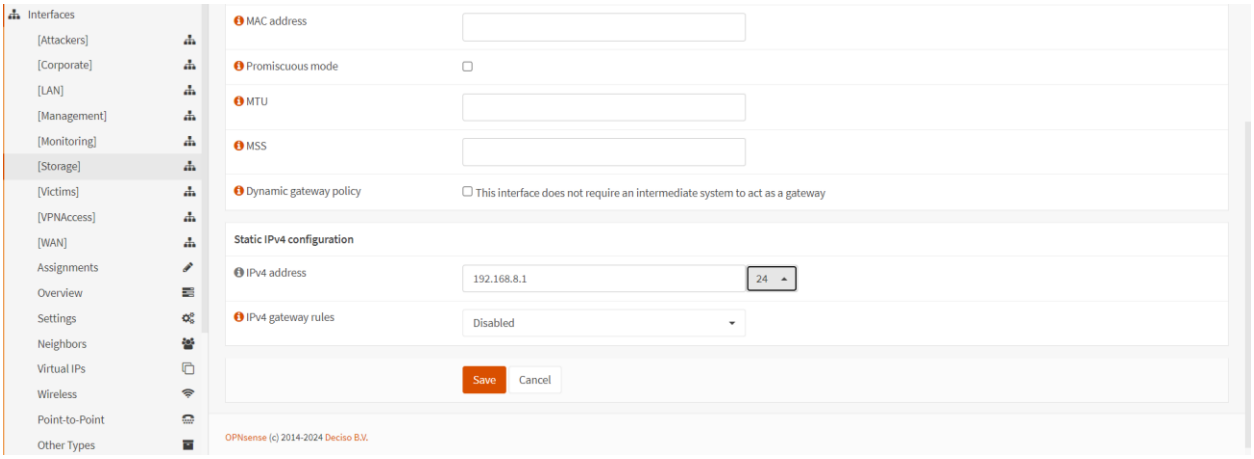
Here I am configuring the interface for the Monitoring VLAN



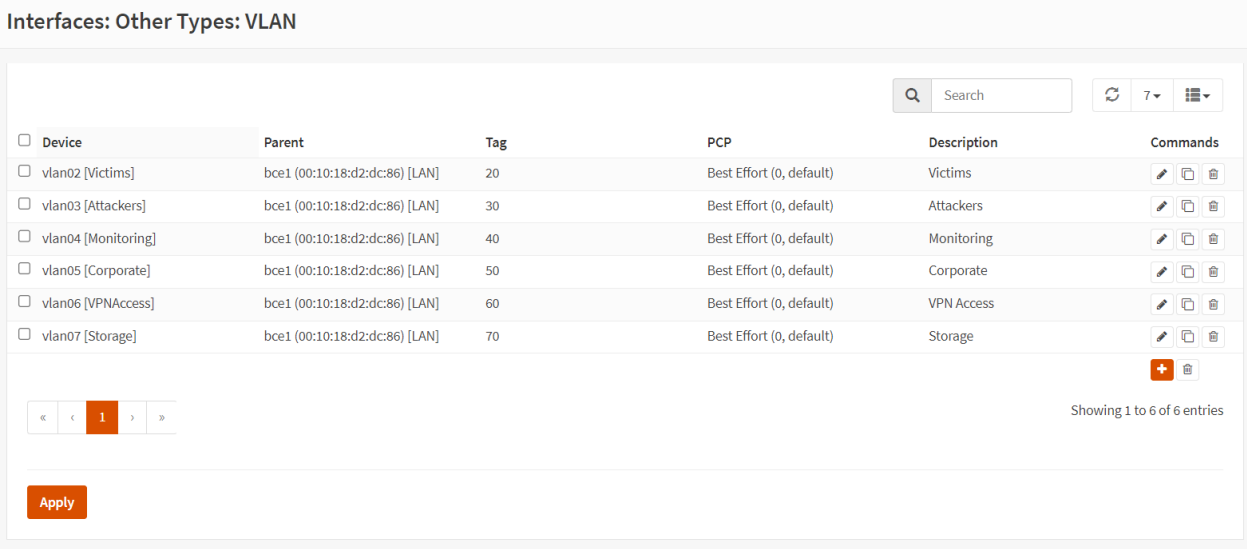
Here I am configuring the interface for the Corporate VLAN



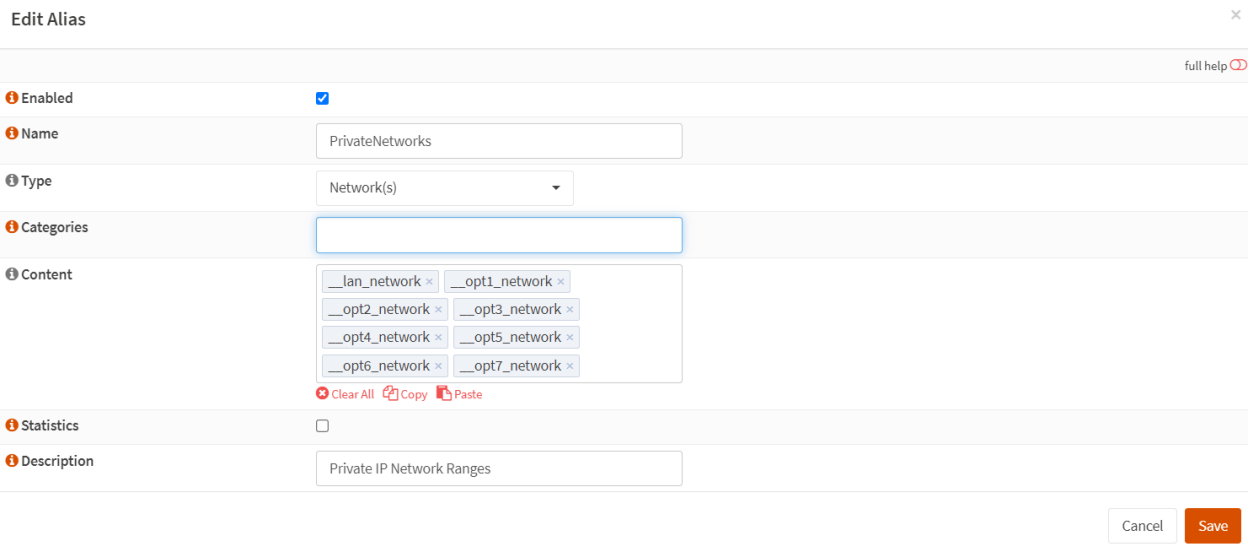
Here I am configuring the interface for the VPN Access VLAN



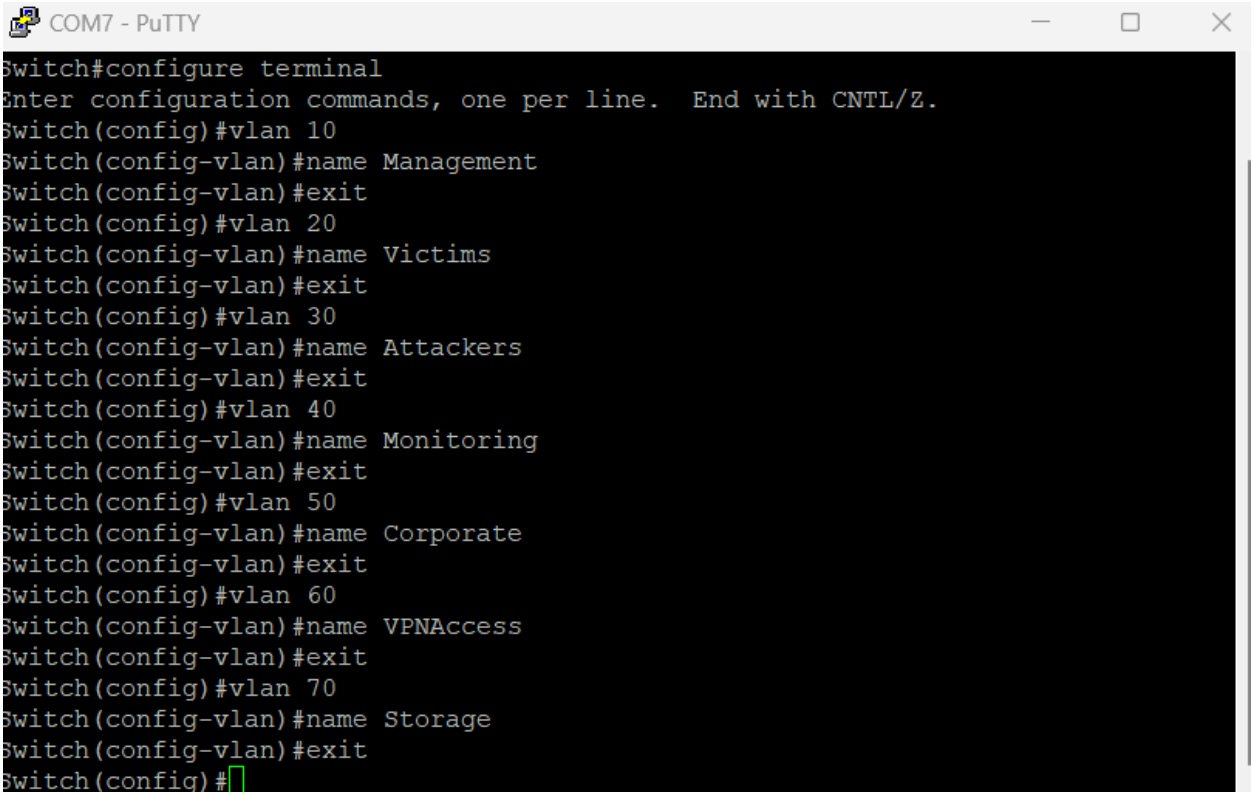
Here I am configuring the interface for the Storage VLAN



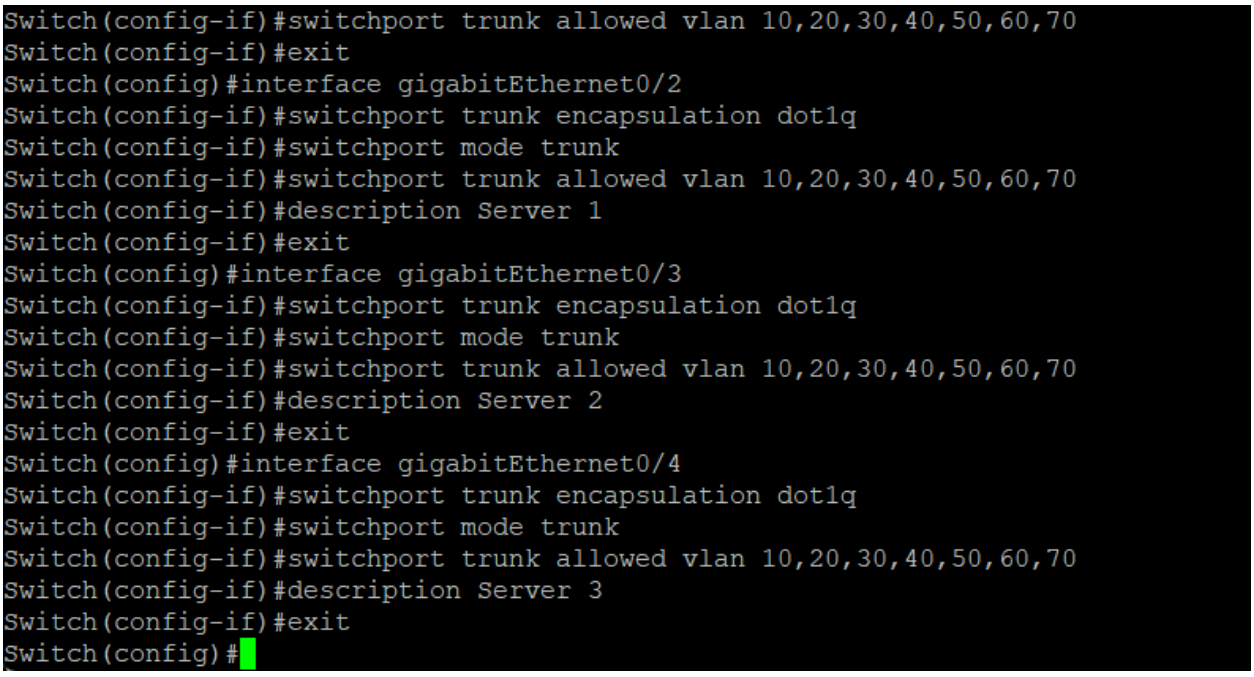
Here are all of the interfaces



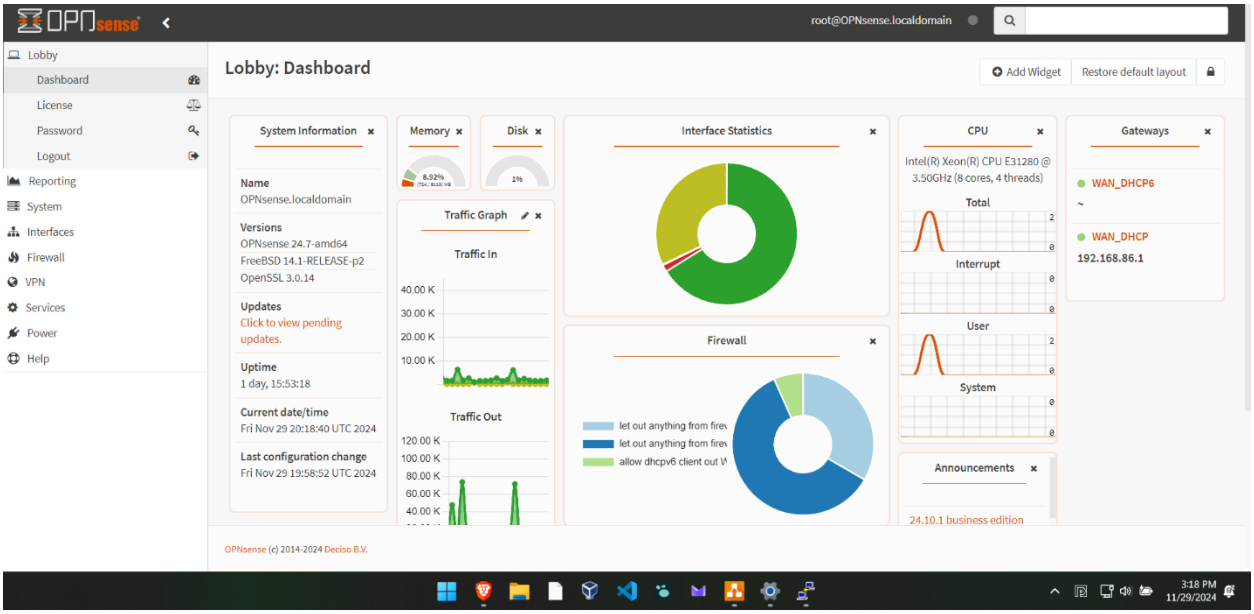
Here I am setting up an alias for all of my VLANS. This will make some of the firewall configurations later easier.



Next, I created the VLANS on my cisco switch



Next, I configured the ports on the switch as trunk ports so that the networks from OPNsense would carry over properly



Ensuring the sensors work properly

Write-up & Summary

In this project section, I successfully configured a multi-layered network environment using OPNsense installed on a Dell PowerEdge R210 II, and a Cisco 3560G switch to enable trunking for VLANs. OPNsense is set up with multiple network zones corresponding to a VLAN, and tagged appropriately in the switch. The Dell R210 II serves as the core router/firewall, and the switch's trunk ports ensure that traffic from these VLANs is properly carried to connected devices across the network.

The switch is configured with trunk ports to allow all VLAN traffic to pass through the router/firewall. For example, the Victims and Attackers zones are isolated for controlled experiments and simulations, this setup allows those firewall rules to be applied easier. This setup acts as the foundation for a segmented and secure network environment.

In the next section, I will configure the firewall to secure the setup and allow communication between the subnets.

References

Draw.io - free flowchart maker and diagrams online. Flowchart Maker & Online Diagram Software. (n.d.). https://app.diagrams.net/

OPNsense® a true open source security platform and more - OPNsense® is a true open source firewall and more. (2024, July 31). OPNsense® Is a True Open Source Firewall and More. https://opnsense.org/