

## **Server Setup: Setting up the Network**

Branson Bailey

Home Lab Project

10 December 2024

**Table of Contents**

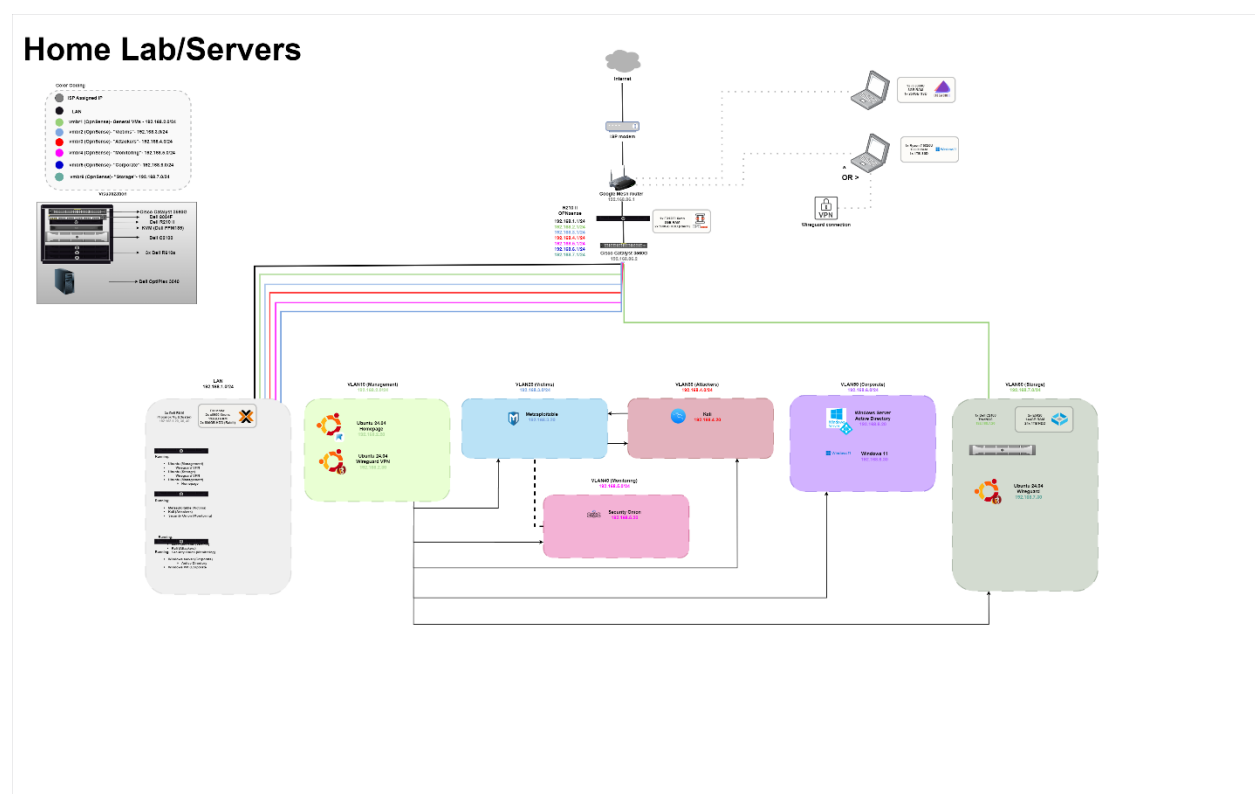
<b>Content</b>	<b>Page</b>
Cover Page	1
Table of contents	2
Project Focus	3
Network Setup Process	5
Write-up	14
References	15

## 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:

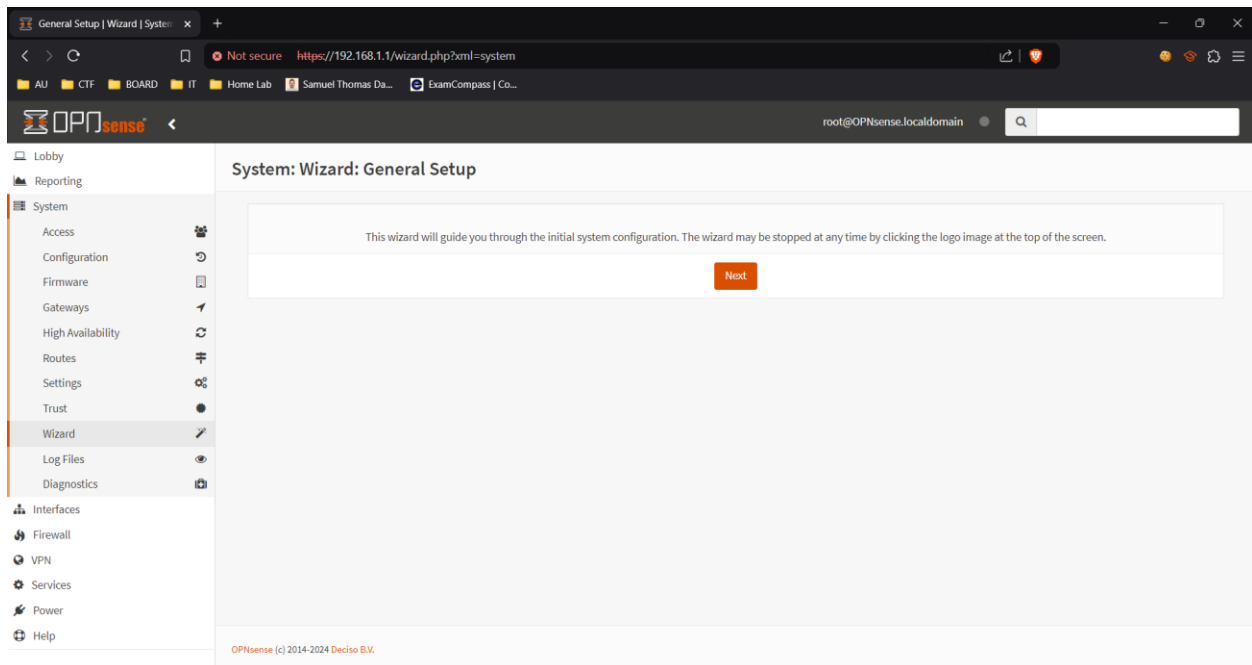


End-Goal Network Topology

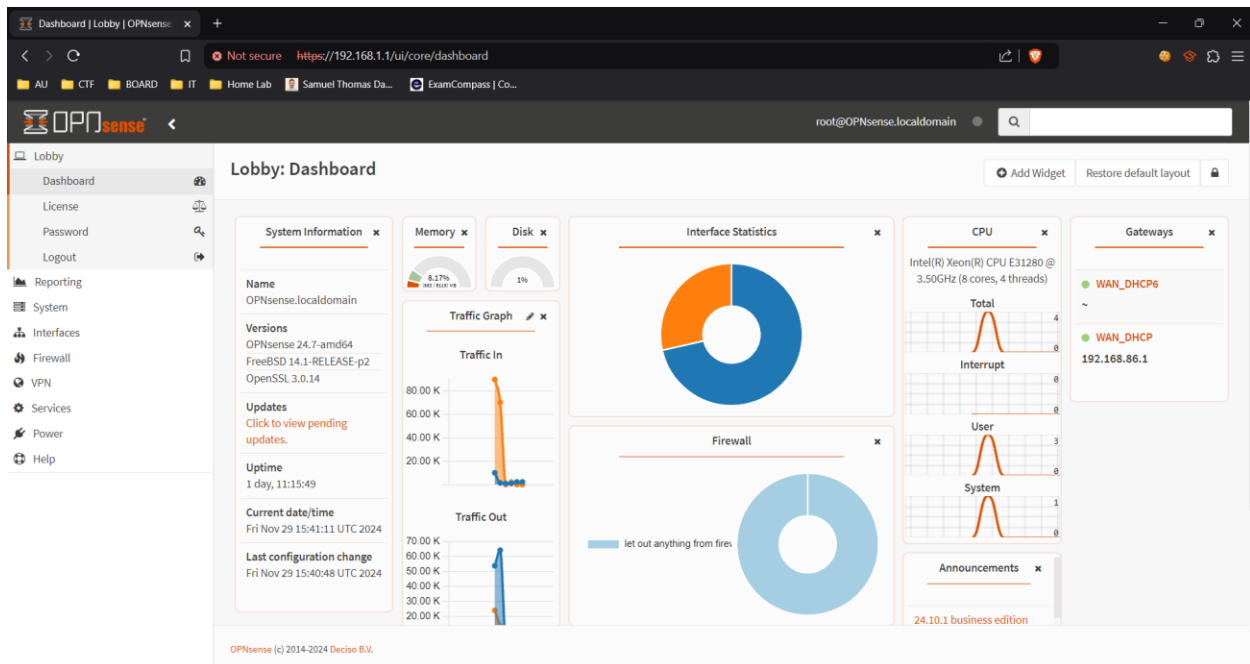
## Network Setup Process

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

### Edit Vlan

advanced mode

full help

Device	
Parent	bce1 (00:10:18:d2:dc:86) [LAN]
VLAN tag	10
VLAN priority	Best Effort (0, default)
Description	Management

Cancel

Save

Here I am setting up the Management VLAN

Edit Vlan

×

advanced mode

full help

<b>Device</b>	<input type="text"/>
<b>Parent</b>	bce1 (00:10:18:d2:dc:86) [LAN] ▼
<b>VLAN tag</b>	<input type="text" value="20"/>
<b>VLAN priority</b>	Best Effort (0, default) ▼
<b>Description</b>	<input type="text" value="Victims"/>

Cancel

Save

Here I am setting up the Victims VLAN

Edit Vlan

×

advanced mode

full help

<b>Device</b>	<input type="text"/>
<b>Parent</b>	bce1 (00:10:18:d2:dc:86) [LAN] ▼
<b>VLAN tag</b>	<input type="text" value="30"/>
<b>VLAN priority</b>	Best Effort (0, default) ▼
<b>Description</b>	<input type="text" value="Attackers"/>

Cancel

Save

Here I am setting up the Attackers VLAN

Edit Vlan

advanced mode

full help

Device

Parent

bce1 (00:10:18:d2:dc:86) [LAN]

VLAN tag

40

VLAN priority

Best Effort (0, default)

Description

Monitoring

Cancel

Save

Here I am setting up the Monitoring VLAN

Edit Vlan

advanced mode

full help

Device

Parent

bce1 (00:10:18:d2:dc:86) [LAN]

VLAN tag

50

VLAN priority

Best Effort (0, default)

Description

Corporate

Cancel

Save

Here I am setting up the Corporate VLAN

### Edit Vlan

×

advanced modefull help

<b>Device</b>	<input type="text"/>
<b>Parent</b>	bce1 (00:10:18:d2:dc:86) [LAN] ▼
<b>VLAN tag</b>	<input type="text" value="60"/>
<b>VLAN priority</b>	Best Effort (0, default) ▼
<b>Description</b>	<input type="text" value="VPN Access"/>

CancelSave

Here I am setting up the VPN Access VLAN

### Edit Vlan

×

advanced modefull help

<b>Device</b>	<input type="text"/>
<b>Parent</b>	bce1 (00:10:18:d2:dc:86) [LAN] ▼
<b>VLAN tag</b>	<input type="text" value="70"/>
<b>VLAN priority</b>	Best Effort (0, default) ▼
<b>Description</b>	<input type="text" value="Storage"/>

CancelSave

Here I am setting up the Storage VLAN

Interfaces

[Attackers]

[Corporate]

[LAN]

[Management]

[Monitoring]

[Victims]

[VPNAccess]

[WAN]

Assignments

Overview

Settings

Neighbors

Virtual IPs

Wireless

Point-to-Point

Other Types

Diagnostics

**MAC address**

**Promiscuous mode**

☐

**MTU**

**MSS**

**Dynamic gateway policy**

☐ This interface does not require an intermediate system to act as a gateway

**Static IPv4 configuration**

**IPv4 address**

24 ▲

**IPv4 gateway rules**

SaveCancel

OPNsense (c) 2014-2024 Deciso B.V.



Here I am configuring the interface for the Management VLAN

The screenshot shows the OPNsense web interface. On the left sidebar, the 'Settings' menu item is selected. The main content area displays the configuration for the 'Management' interface. At the top, there is a 'Dynamic gateway policy' section with a checkbox labeled 'This interface does not require an intermediate system to act as a gateway'. Below this is the 'Static IPv4 configuration' section, which includes an 'IPv4 address' field set to '192.168.3.1' and a '24' bit mask. The 'IPv4 gateway rules' are set to 'Disabled'. At the bottom of the configuration area are 'Save' and 'Cancel' buttons. The footer of the interface reads 'OPNsense (c) 2014-2024 Deciso B.V.'.

Here I am configuring the interface for the Victims VLAN

The screenshot shows the OPNsense web interface with the 'Victims' interface selected in the left sidebar. The configuration page for this interface is displayed. It includes a 'MAC address' field, a 'Promiscuous mode' checkbox, and fields for 'MTU' and 'MSS'. The 'Dynamic gateway policy' section is at the top with the checkbox 'This interface does not require an intermediate system to act as a gateway'. The 'Static IPv4 configuration' section shows the 'IPv4 address' as '192.168.4.1' with a '24' bit mask, and 'IPv4 gateway rules' set to 'Disabled'. 'Save' and 'Cancel' buttons are at the bottom. The footer indicates 'OPNsense (c) 2014-2024 Deciso B.V.'.

Here I am configuring the interface for the Attackers VLAN

The screenshot shows the OPNsense web interface with the 'Attackers' interface selected in the left sidebar. The configuration page for this interface is displayed. It includes a 'MAC address' field, a 'Promiscuous mode' checkbox, and fields for 'MTU' and 'MSS'. The 'Dynamic gateway policy' section is at the top with the checkbox 'This interface does not require an intermediate system to act as a gateway'. The 'Static IPv4 configuration' section shows the 'IPv4 address' as '192.168.5.1' with a '24' bit mask, and 'IPv4 gateway rules' set to 'Disabled'. 'Save' and 'Cancel' buttons are at the bottom. The footer indicates 'OPNsense (c) 2014-2024 Deciso B.V.'.

Here I am configuring the interface for the Monitoring VLAN

The screenshot shows the OPNsense web interface with the 'Interfaces' menu on the left. The 'Corporate' interface is selected. The configuration page displays the following settings:

- MAC address: [Empty field]
- Promiscuous mode: ☐
- MTU: [Empty field]
- MSS: [Empty field]
- Dynamic gateway policy: ☐ This interface does not require an intermediate system to act as a gateway
- Static IPv4 configuration:
  - IPv4 address: 192.168.6.1 (Subnet: 24)
  - IPv4 gateway rules: Disabled

At the bottom, there are 'Save' and 'Cancel' buttons. The footer indicates 'OPNsense (c) 2014-2024 Deciso B.V.'.

Here I am configuring the interface for the Corporate VLAN

The screenshot shows the OPNsense web interface with the 'VPNAccess' interface selected. The configuration page displays the following settings:

- Dynamic gateway policy: ☐ This interface does not require an intermediate system to act as a gateway
- Static IPv4 configuration:
  - IPv4 address: 192.168.7.1 (Subnet: 24)
  - IPv4 gateway rules: Disabled

At the bottom, there are 'Save' and 'Cancel' buttons. The footer indicates 'OPNsense (c) 2014-2024 Deciso B.V.'.

Here I am configuring the interface for the VPN Access VLAN

The screenshot shows the OPNsense web interface with the 'Storage' interface selected. The configuration page displays the following settings:

- MAC address: [Empty field]
- Promiscuous mode: ☐
- MTU: [Empty field]
- MSS: [Empty field]
- Dynamic gateway policy: ☐ This interface does not require an intermediate system to act as a gateway
- Static IPv4 configuration:
  - IPv4 address: 192.168.8.1 (Subnet: 24)
  - IPv4 gateway rules: Disabled

At the bottom, there are 'Save' and 'Cancel' buttons. The footer indicates 'OPNsense (c) 2014-2024 Deciso B.V.'.

Here I am configuring the interface for the Storage VLAN

## Interfaces: Other Types: VLAN

<div><div><div></div><div>Search</div></div><div><div></div><div>7</div><div></div></div></div>						
<input type="checkbox"/> Device	Parent	Tag	PCP	Description	Commands	
<input type="checkbox"/> vlan02 [Victims]	bce1 (00:10:18:d2:dc:86) [LAN]	20	Best Effort (0, default)	Victims	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/> vlan03 [Attackers]	bce1 (00:10:18:d2:dc:86) [LAN]	30	Best Effort (0, default)	Attackers	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/> vlan04 [Monitoring]	bce1 (00:10:18:d2:dc:86) [LAN]	40	Best Effort (0, default)	Monitoring	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/> vlan05 [Corporate]	bce1 (00:10:18:d2:dc:86) [LAN]	50	Best Effort (0, default)	Corporate	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/> vlan06 [VPNAccess]	bce1 (00:10:18:d2:dc:86) [LAN]	60	Best Effort (0, default)	VPN Access	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/> vlan07 [Storage]	bce1 (00:10:18:d2:dc:86) [LAN]	70	Best Effort (0, default)	Storage	<div><div></div><div></div><div></div></div>	
<div><div><div></div><div></div><div></div></div><div>Showing 1 to 6 of 6 entries</div></div>						
<div>Apply</div>						

Here are all of the interfaces

Edit Alias ×

full help

Enabled

☒

Name

PrivateNetworks

Type

Network(s)

Categories

Content

\_\_lan\_network ×

\_\_opt1\_network ×

\_\_opt2\_network ×

\_\_opt3\_network ×

\_\_opt4\_network ×

\_\_opt5\_network ×

\_\_opt6\_network ×

\_\_opt7\_network ×

Clear All

Copy

Paste

Statistics

☐

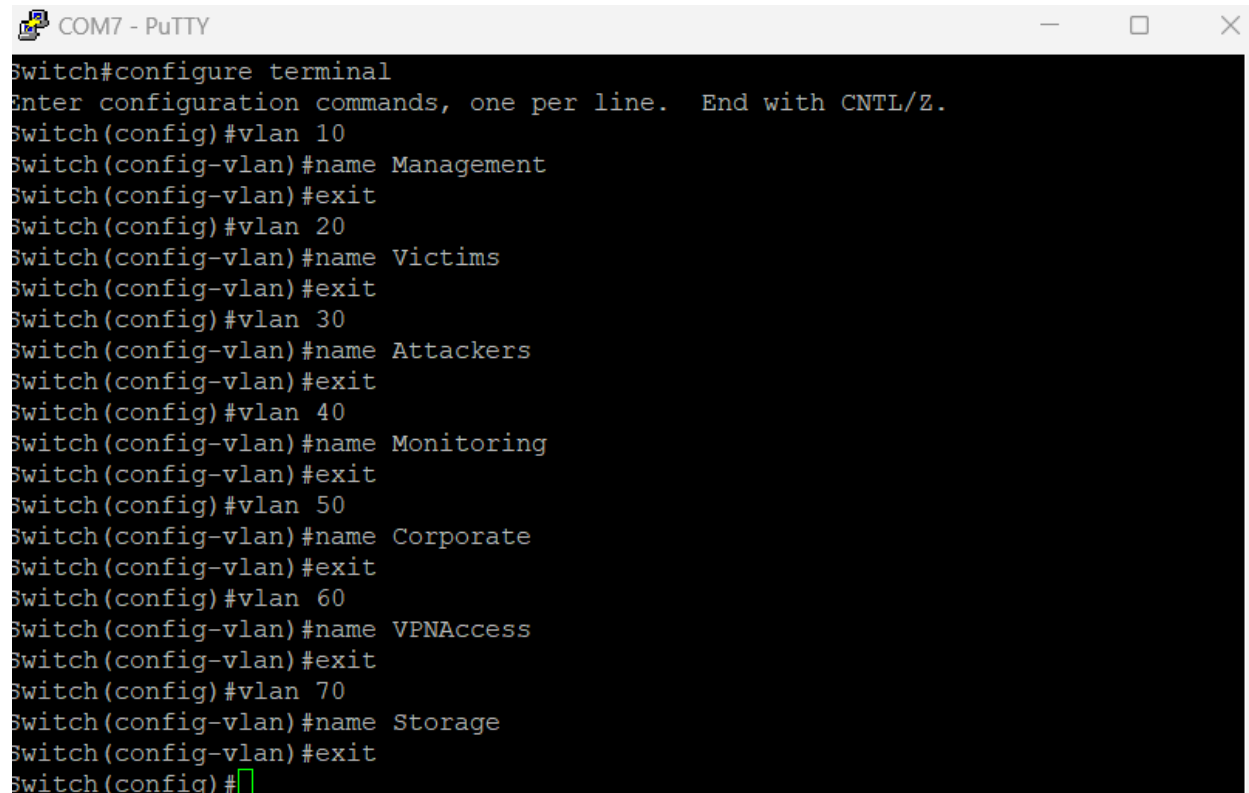
Description

Private IP Network Ranges

Cancel

Save

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

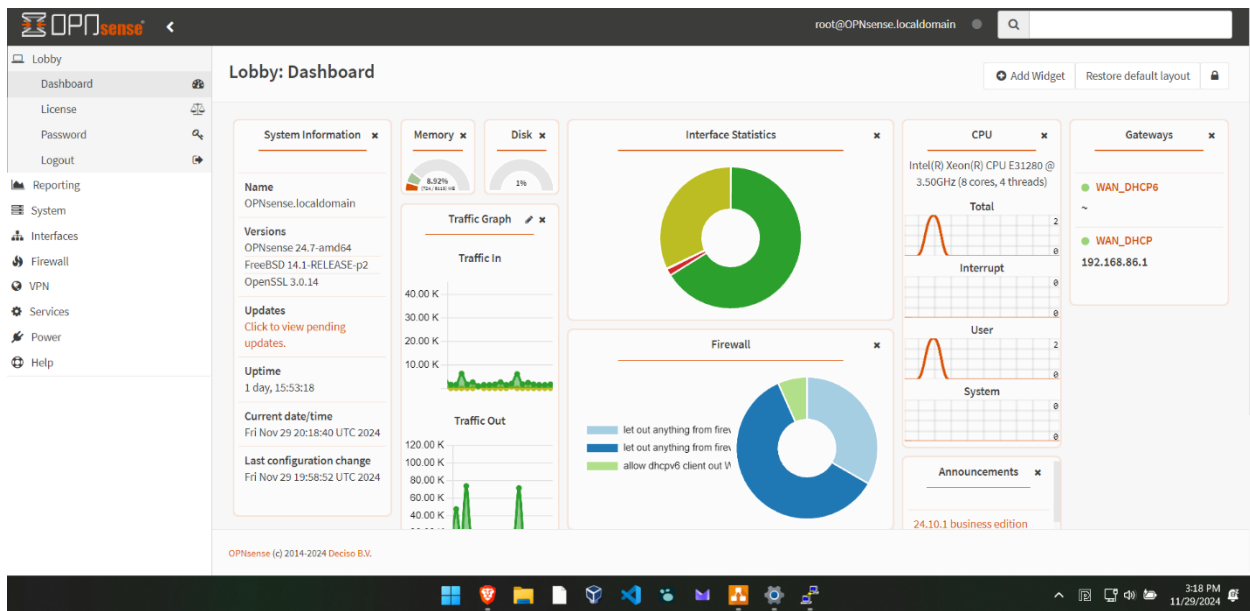


```
COM7 - PuTTY
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Victims
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Attackers
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name Monitoring
Switch(config-vlan)#exit
Switch(config)#vlan 50
Switch(config-vlan)#name Corporate
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)#name VPNAccess
Switch(config-vlan)#exit
Switch(config)#vlan 70
Switch(config-vlan)#name Storage
Switch(config-vlan)#exit
Switch(config)#
```

Next, I created the VLANs on my cisco switch

```
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70
Switch(config-if)#description Server 1
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet0/3
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70
Switch(config-if)#description Server 2
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet0/4
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70
Switch(config-if)#description Server 3
Switch(config-if)#exit
Switch(config)#
```

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/>*