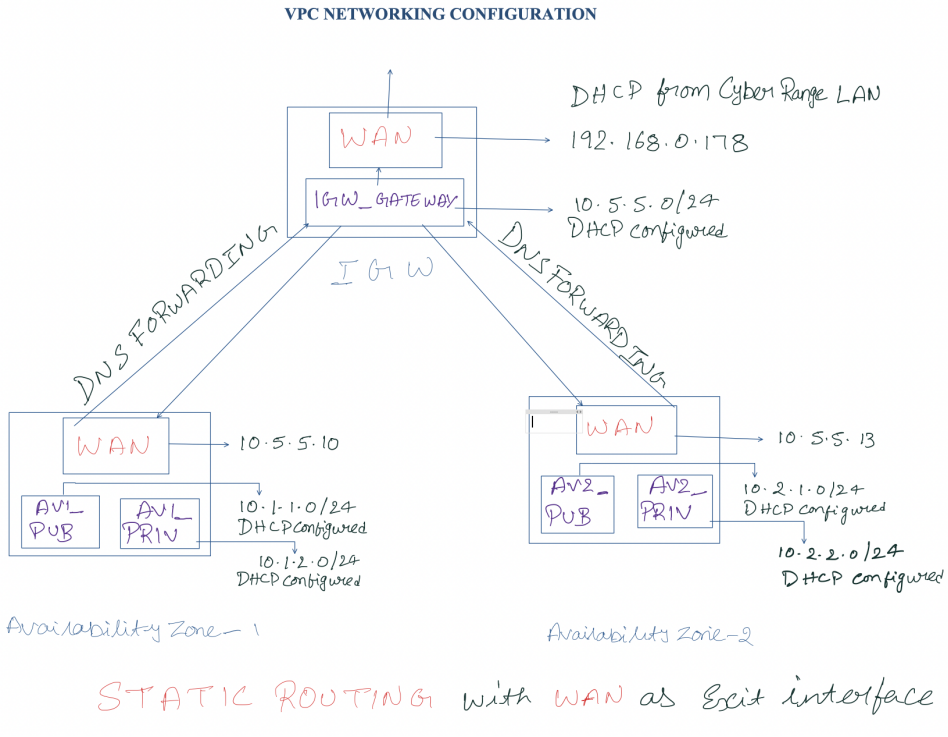
Virtual Private Cloud Networking on PfSense

SCENARIO

You need to set up a isolated infrastructure similar to that of a AWS VPC with multiple availability zones that should be able to communicate with one another There should be a public and private subnet in each of the availability zone. The devices in the publicly and private subnets of their respective zones should be able to communicate with one another. Each zone should route through one ingress/egress point, additionally basic firewalls should be implemented throughout the system. For this exercise a minimum of 2 availability zones should be implemented to demonstrate functionality. Any additional zones are repetitive and do not add much for the additional complexity.

IMPLEMENTATION

To solve the above task, we are going to have multiple network interfaces as shown in the figure below. The IGW pfSense will be the primary pfsense since it handles perimeter firewall, DNS and the routing of packets.



STEP-1: Creating Virtual Interfaces

To implement the above network map, the first step would be create virtual networks on XOA or any hypervisor so that we can attach machines to a particular network. They are named as follows in this case:

- IGW_Gateway
- AV1_PUB (Availability Zone - 1 Public Subnet)
- AV1_PRIV (Availability Zone - 1 Private Subnet)
- AV2_PUB (Availability Zone - 2 Public Subnet)
- AV2_PRIV (Availability Zone - 2 Private Subnet)

STEP-2: Creating Virtual Machines

Create 3 virtual machines and attach the network interfaces as follows to create availability zones and create multiple private networks to isolate devices connected to those networks from being directly accessible from outside.

VIrtual Machine -1 (IGW): The main Internet Gateway router or it can also be termed as the edge router. This is where the traffic comes in from outside and the traffic from internal network goes out. The availability zones would be connected to the IGW_Gateway which makes the availability zones directly connected networks to the IGW. We need two interfaces on this router. The first network interface would be a bridged network while the other one would be a virtual interface which acts as IGW_Gateway.

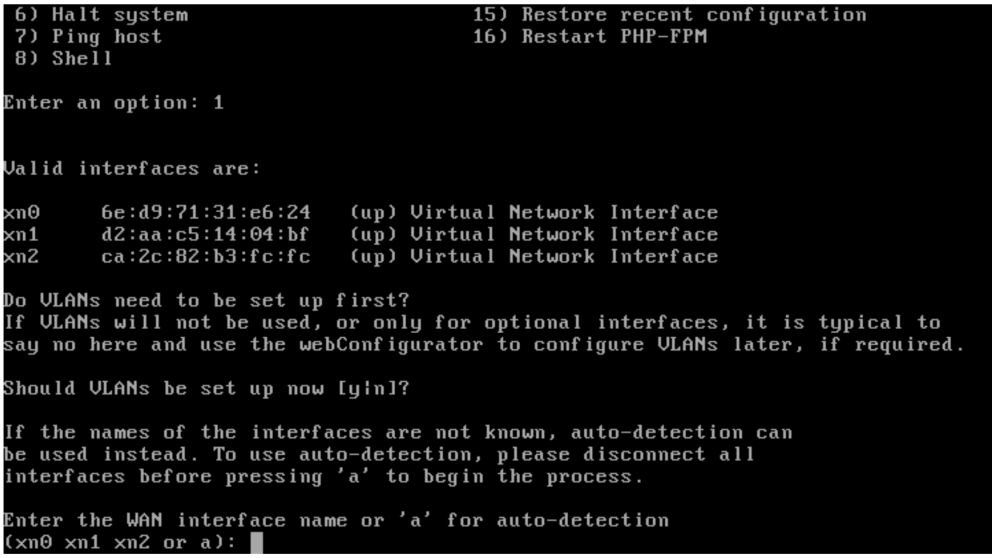
VIrtual Machine -2 (AV1): This will be the first availability zone. Create a pfsense virtual machine and attach the networks *IGW_Gateway, AV1_PUB,AV1_PRIV* to the machine. We are going to configure these virtual interfaces to solve for certain network functionalities.

VIrtual Machine -3 (AV2): This will be the second availability zone. Create a pfsense virtual machine and attach the networks *IGW_Gateway, AV2_PUB,AV2_PRIV* to the machine.

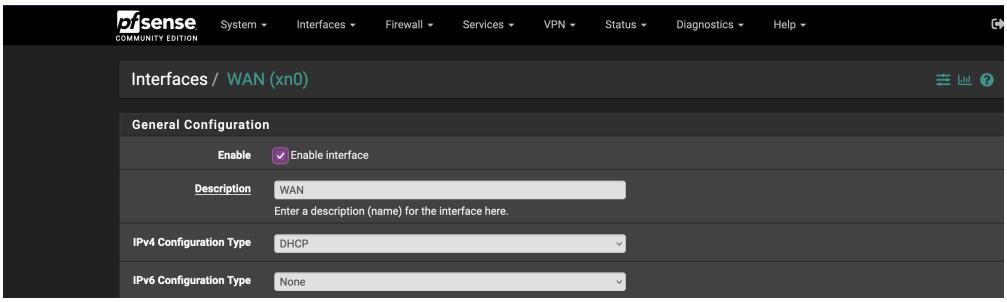
We are going to configure this in a top-down approach which means that we are going to configure the IGW router first and then configure the availability zones.

STEP-3: Configuring the IGW Router

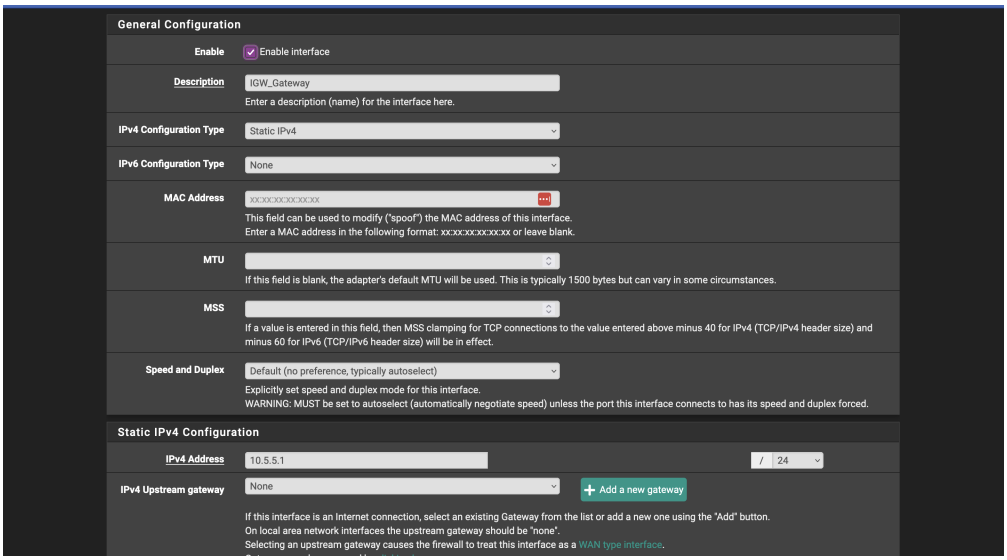
- Once pfsense is installed, open the console and assign the WAN and LAN interfaces to their physical interfaces respectively (Select option 1 in the shell to assign network interfaces). Note that the virtual interfaces are also considered a physical interface as shown in the image below.



- Once you assign interfaces, the WAN would already get an IP address from the DHCP server.
- From the pfsense console, grab the IP address of the WAN interface and enter it into the browser which gives you the access to the pfsense web console which is where you can make changes.
- Post entering the default credentials, it redirects you to a setup page where you can configure the IP addresses of the interfaces. It should show up a WAN interface and the data should be auto populated since pfsense already has a WAN address and if it does not, follow the next step
- Configure WAN on the IGW pfSense using DHCP to get an IP from the school. Unchecked "Reserved Networks options". We would get an IP from the Cyber Range LAN which is a 192.168.0.0/21 network.

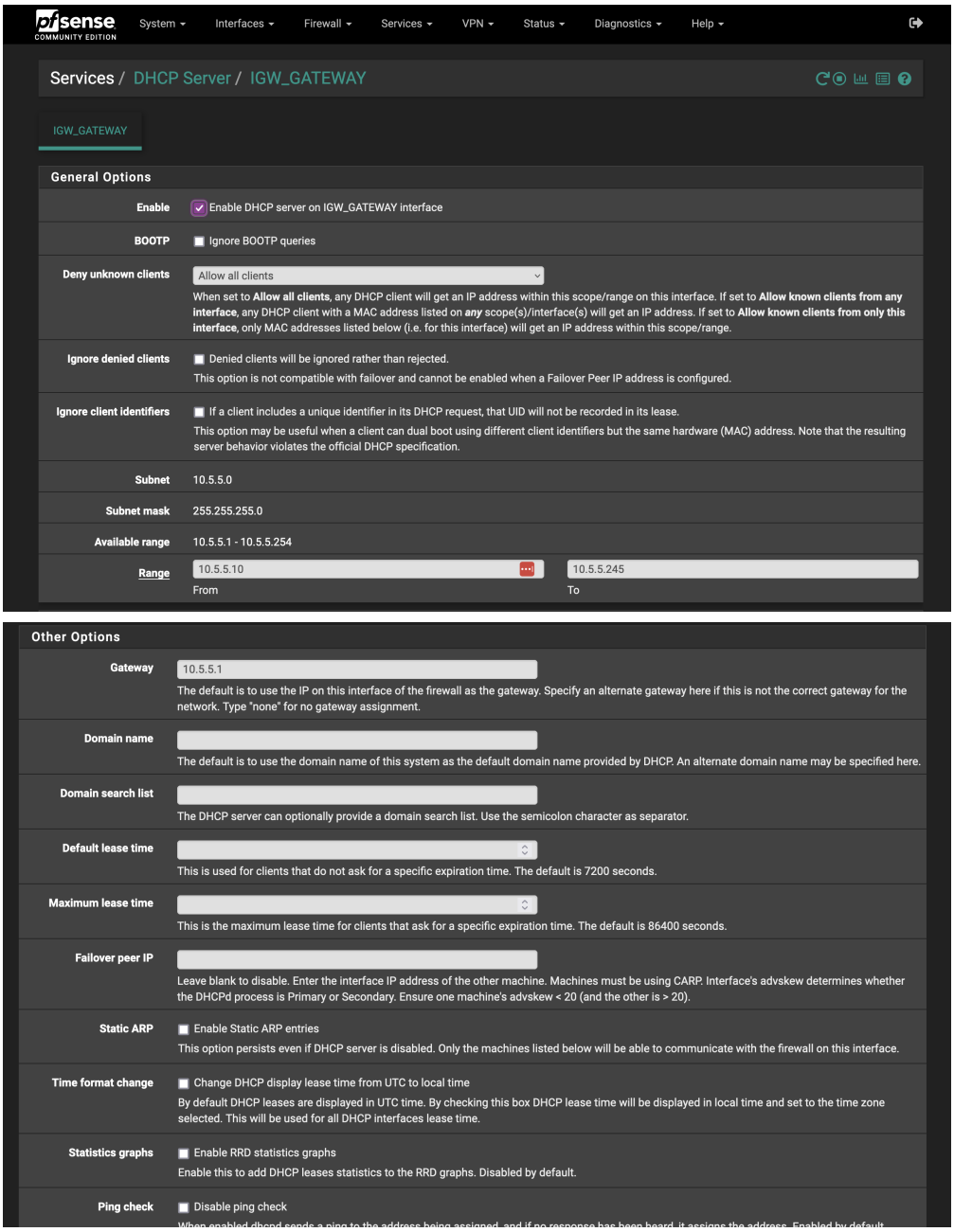


- Configure LAN (IGW Gateway) - Setup a static IPv4 with IPv6 disabled. The network it is on is 10.5.5.0/24. The IP of the interface is 10.5.5.1 and it is also the gateway. The IPv4 upstream gateway should be set to none.



STEP-4: Configuring DHCP on IGW

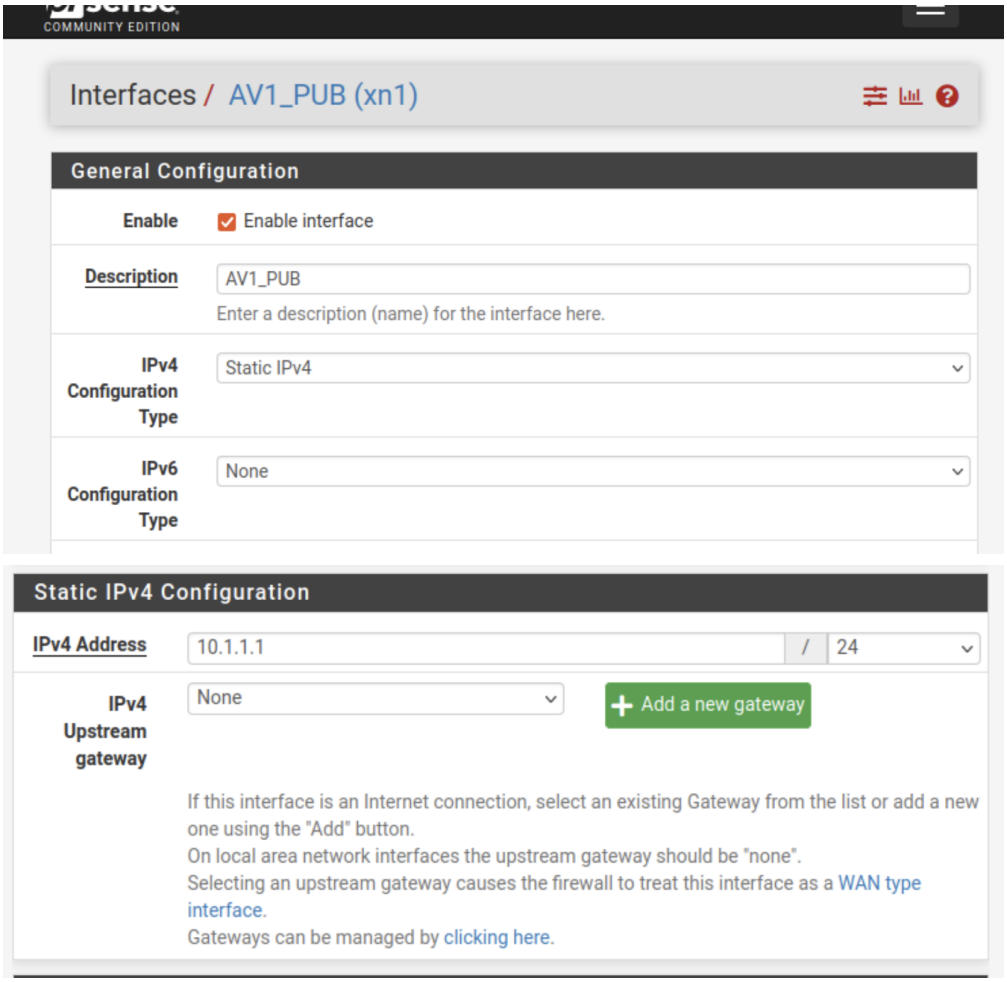
- Configure DHCP on the LAN interface by navigating to Services > DHCP Server. Enable the DHCP on the interface and the available range for DHCP is 10.5.5.10 - 10.5.5.240. A rule of thumb is that for any network interface, the gateway would be the IP address of the network interface itself and in this case the IP address is 10.5.5.1. Enter this as the gateway when configuring the DHCP.



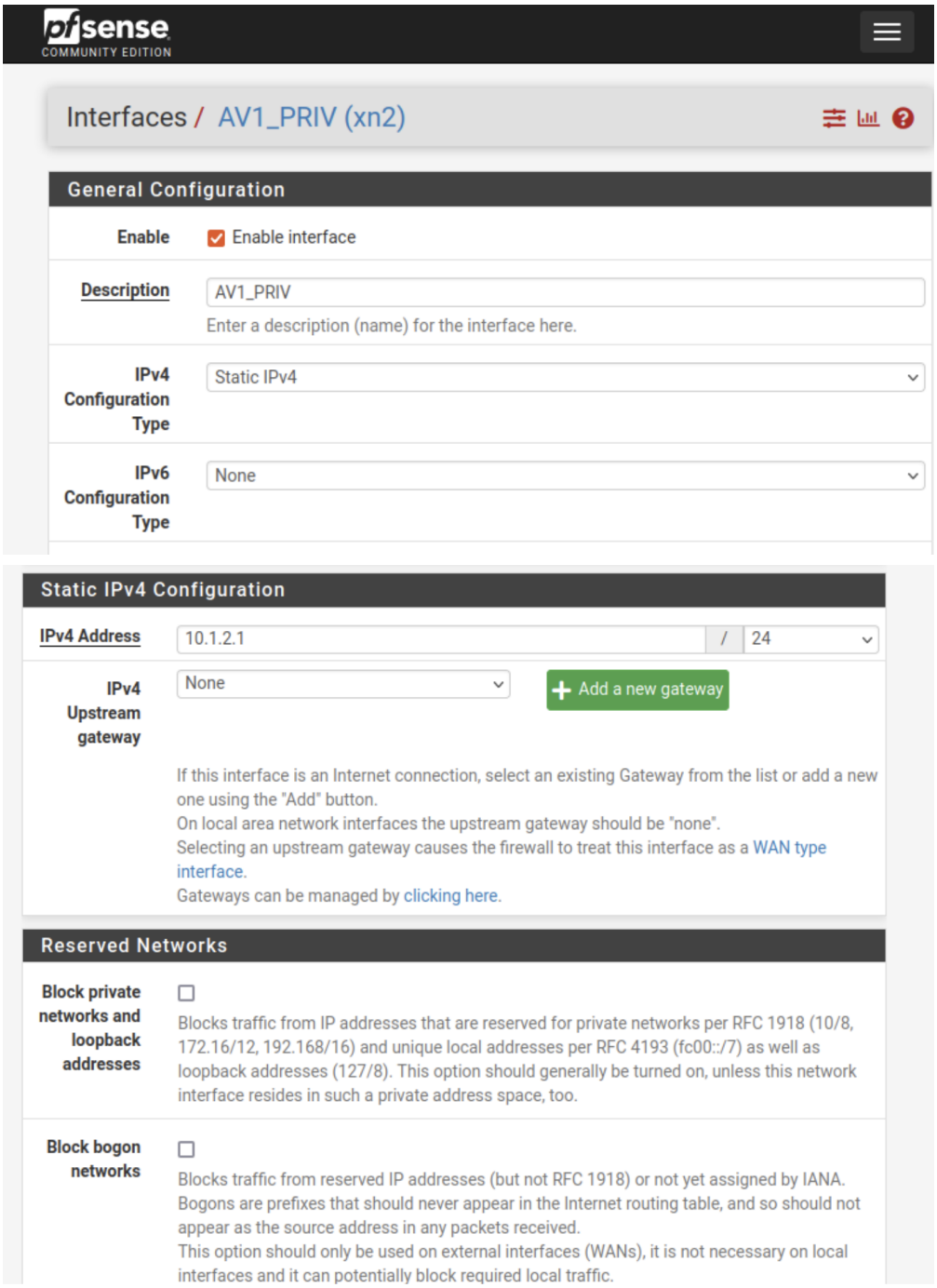
- Once the DHCP is enabled, we can connect devices to IGW_Gateway and the devices will get a 10.5.5.0/24 IP address.

STEP-5: Configuring the AV-1 Router

- Follow the same process as we did for IGW Router - Assign interfaces. Once the interfaces are assigned, the IP address of the WAN would be 10.5.5.10 since that is the first available address for IGW_Gateway.
- Since our local machine is on a different network than the WAN of AV-1, we would need another device which is on the same network to access the Web Configuration page of pfsense and hence we connect another machine to the IGW_Gateway and access the web configuration page for AV-1.
- Configure the LAN as AV1_PUB and assign it an IP address of 10.1.1.1. The CIDR would be 10.1.1.0/24.

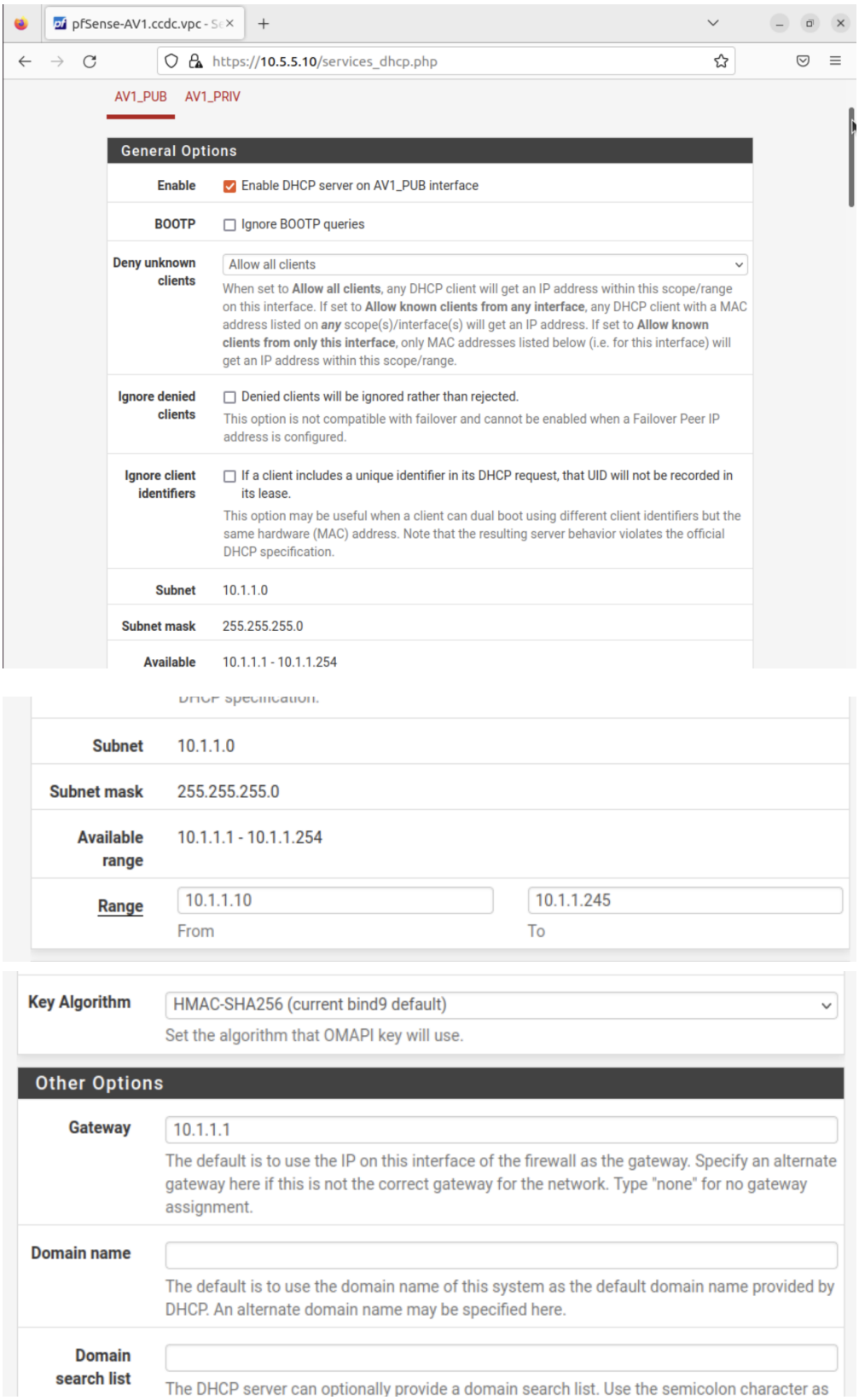


- Configure OPT1 as AV1_PRIV and assign it an IP address of 10.1.2.1. The CIDR would be 10.1.2.0/24.

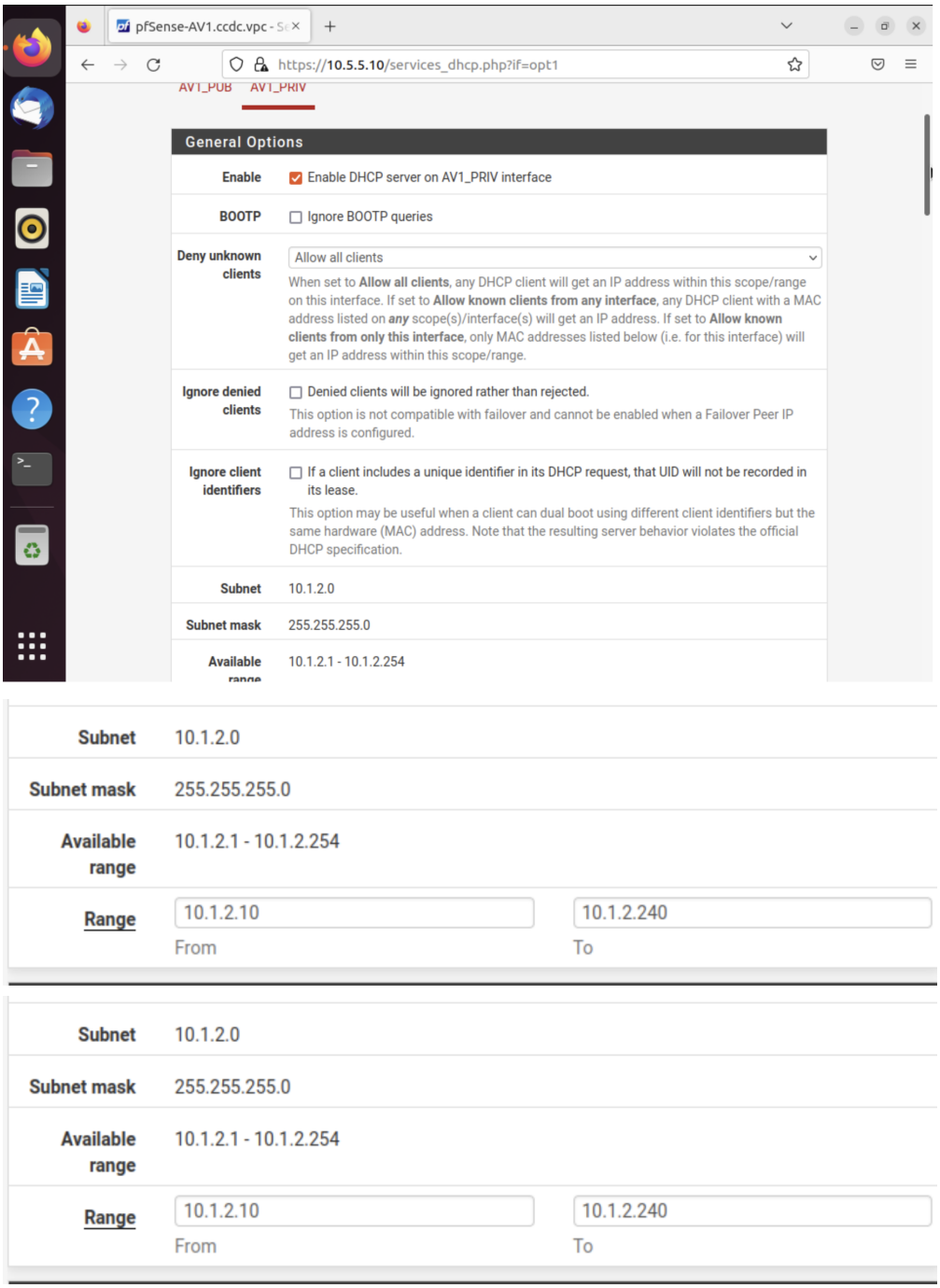


STEP-6: Configuring DHCP on AV1

- Configure DHCP on LAN and OPT1 interfaces by navigating to ***Services > DHCP Server***. Enable the DHCP on the interfaces and leave the IP range as is. The Gateways would be 10.1.1.1 and 10.1.2.1 respectively.



- DHCP AV1_PRIV

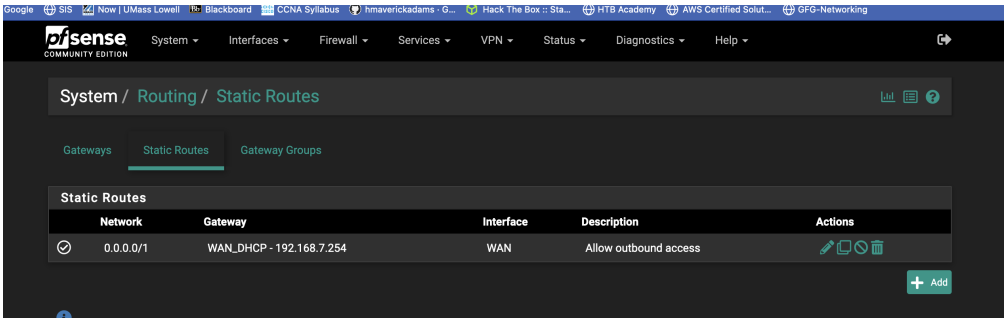


We now have IP addresses configured for network interfaces and a DHCP server which would give devices connecting to the network, a specific IP address. However, there is no access to the internet from any of the internal networks, no one can reach these networks from the outside and to solve this, we need to configure Routing and Firewall to send packets out to the internet and let network packets into the network.

STEP-7: Configuring Routing on IGW

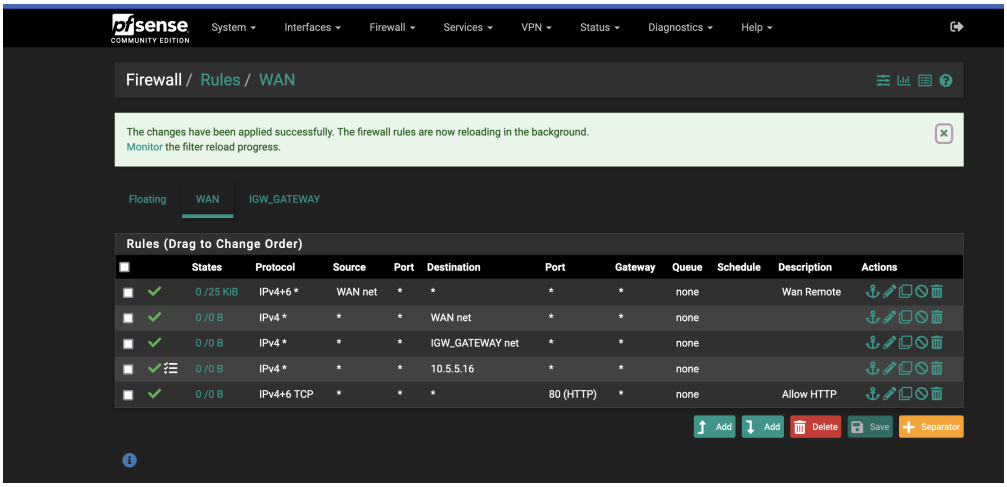
- Navigate to ***System > Routing > Static Routes***
- Add a new static route to a 0.0.0.0/1 network which essentially means any IP address and any subnet mask.
- Select the interface as WAN and the gateway to be the DHCP Gateway.
- Save the settings and we now have a static route to anywhere on the internet.

The WAN gets an IP via the DHCP and the gateway is configured by the network administrator of the school. The gateway in this case is 192.168.7.254.

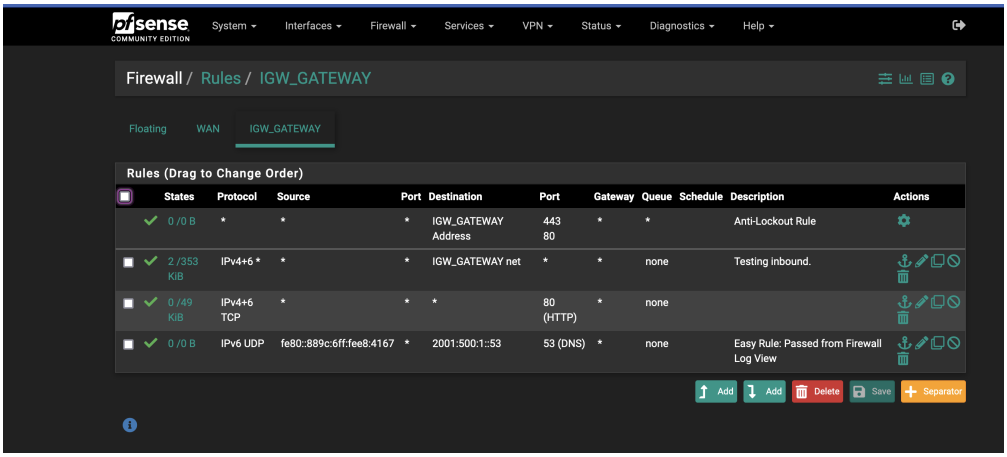


STEP-8: Configuring Firewall on IGW

- Navigate to ***Firewall > Rules > WAN***
- Add an rule which allows all protocols from the source WAN_net to any destination.
- Add two new rules that allows incoming request to IGW_Gateway network and the WAN network.



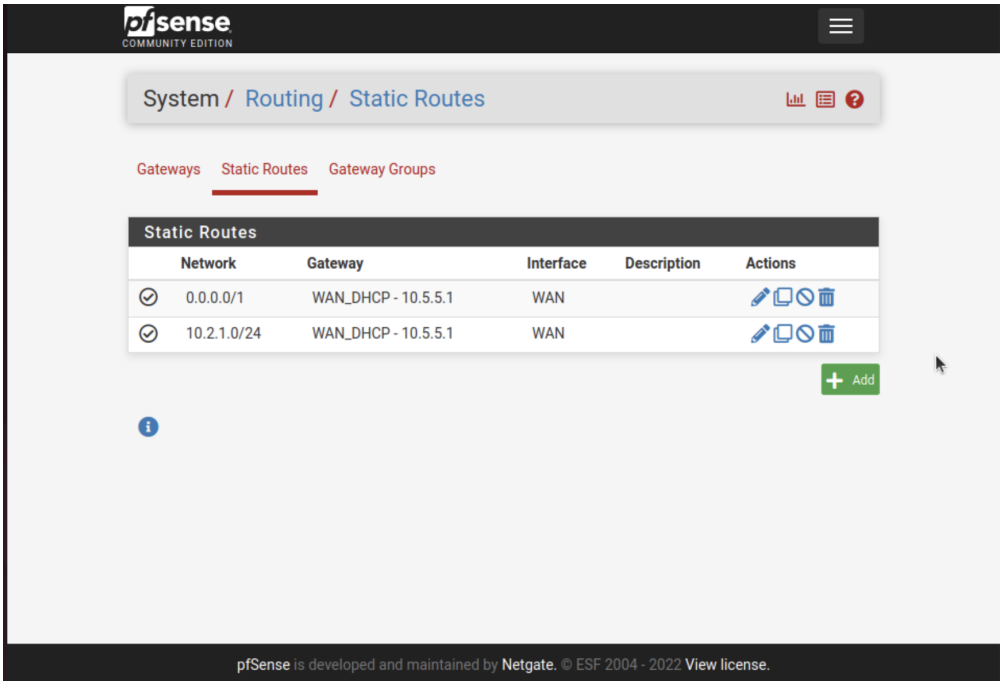
- Navigate to IGW_Gateway firewall rules and add the outbound rules which allow access to the internet and allow packets coming into the IGW_Gateway network.



STEP-9: Routing on Availability Zone - 1

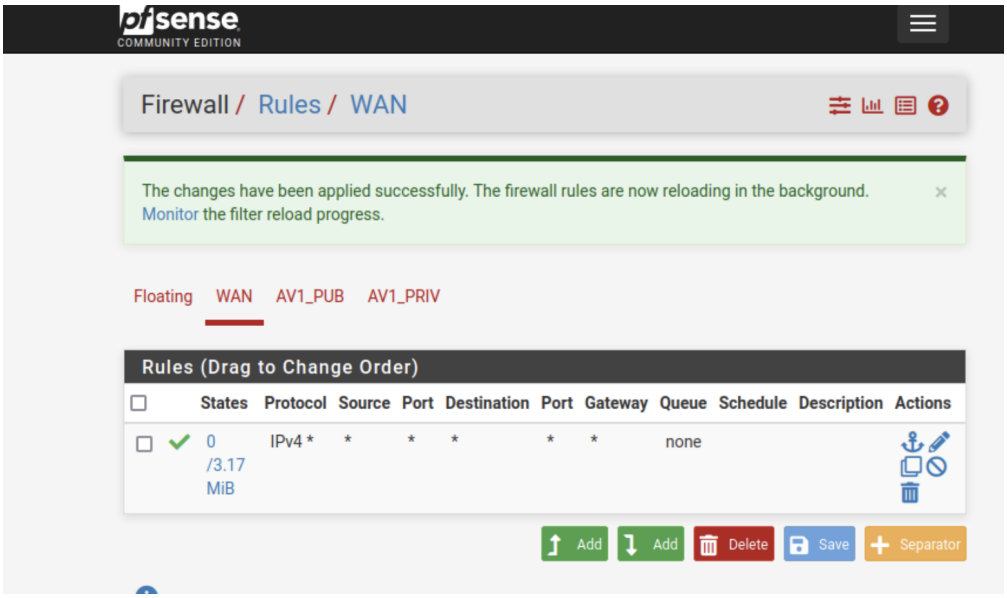
- Navigate to ***System > Routing > Static Routes***.
- Add a new static route to a 0.0.0.0/1 network which essentially means any IP address and any subnet mask.
- Select the interface as WAN and the gateway to be the DHCP Gateway which in this case is 10.5.5.1. This is the gateway that we have specified while configuring the DHCP server on the IGW_Gateway.

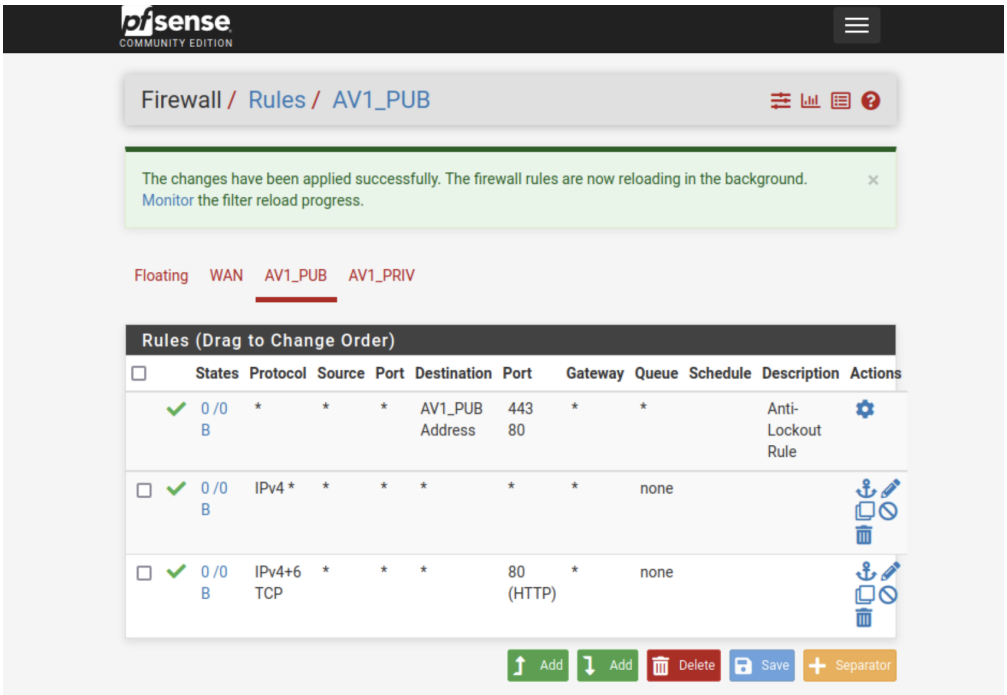
- Save the settings and we now have a route to the internet via the IGW. Any network packet that is going out of the WAN interface will be forwarded to 10.5.5.1 as we have specified in the static route.



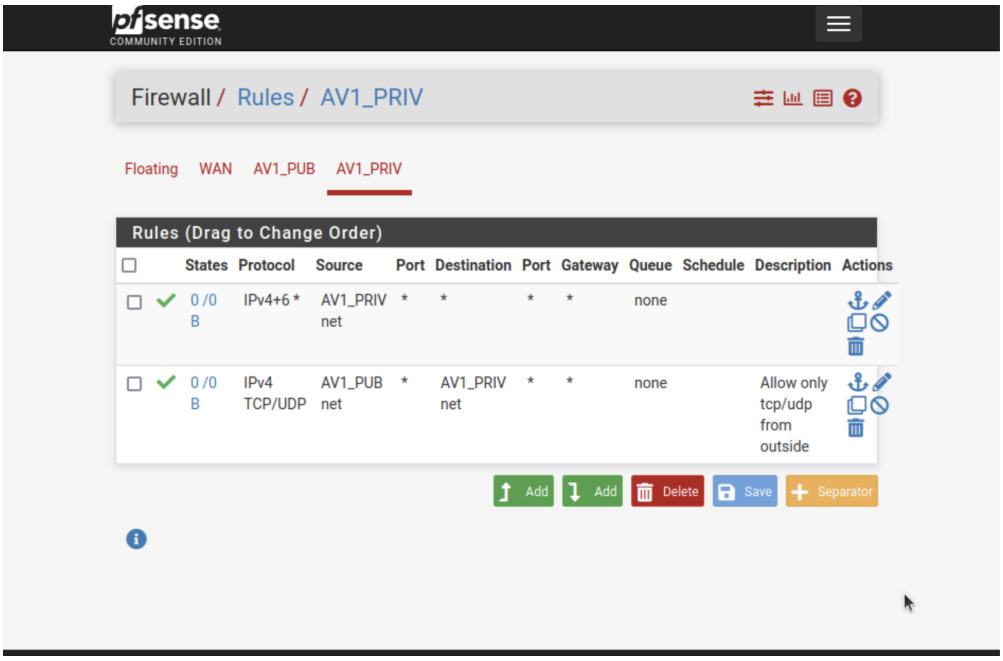
STEP-10: Firewall on Availability Zone - 1

- Navigate to ***Firewall > Rules > WAN***
- You can add lenient rules here since this is going to be an internal network and the IGW does all the filtering initially and hence add an "any any" rule on the WAN and AV1_PUB that passes all the traffic.





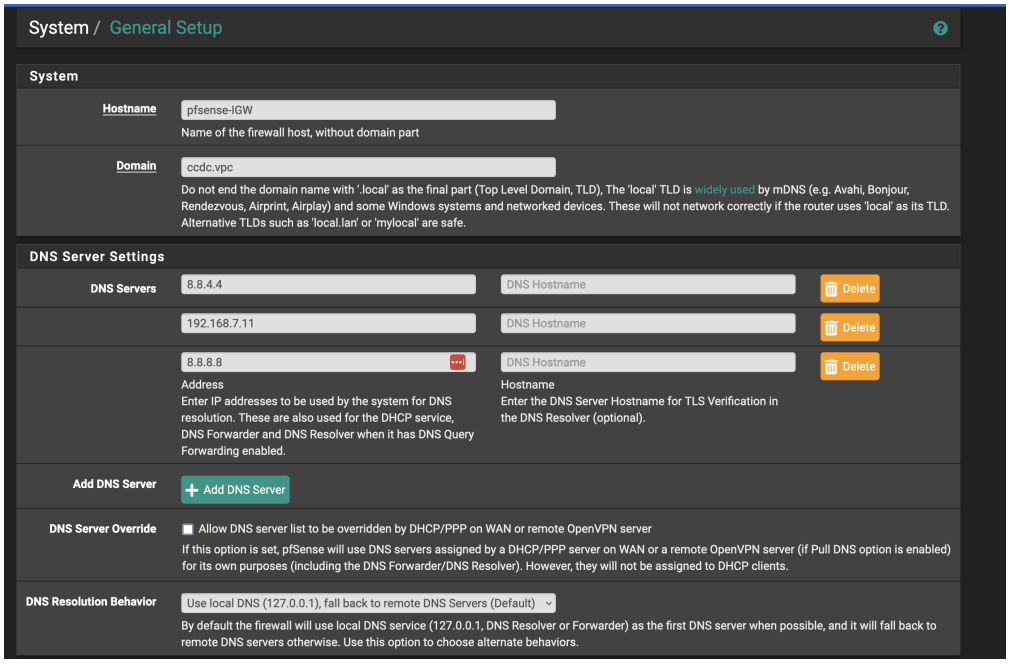
- On AV1_PRIV, add a rule that passes incoming data from AV1_Pub network since we want the private subnet to be isolated from the outside.



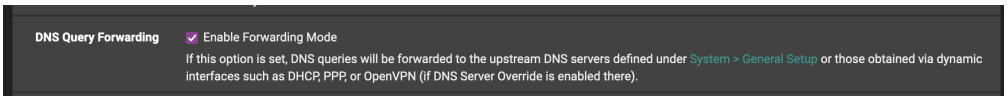
Note: The setup for Availability Zone - 2 would be similar to what has been for Availability Zone -1 except for changes in IP addresses.

STEP-11: DNS Configuration on IGW

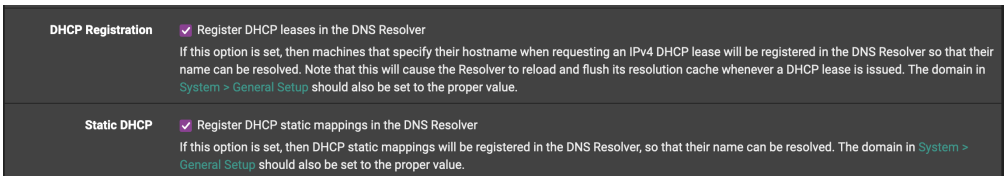
- In order to configure DNS for our networks, we would need DNS servers and hence we are using external DNS servers including the in-house DNS server.
- Navigate to ***System > General Setup > DNS Server Settings*** and enter the external DNS server addresses as below.



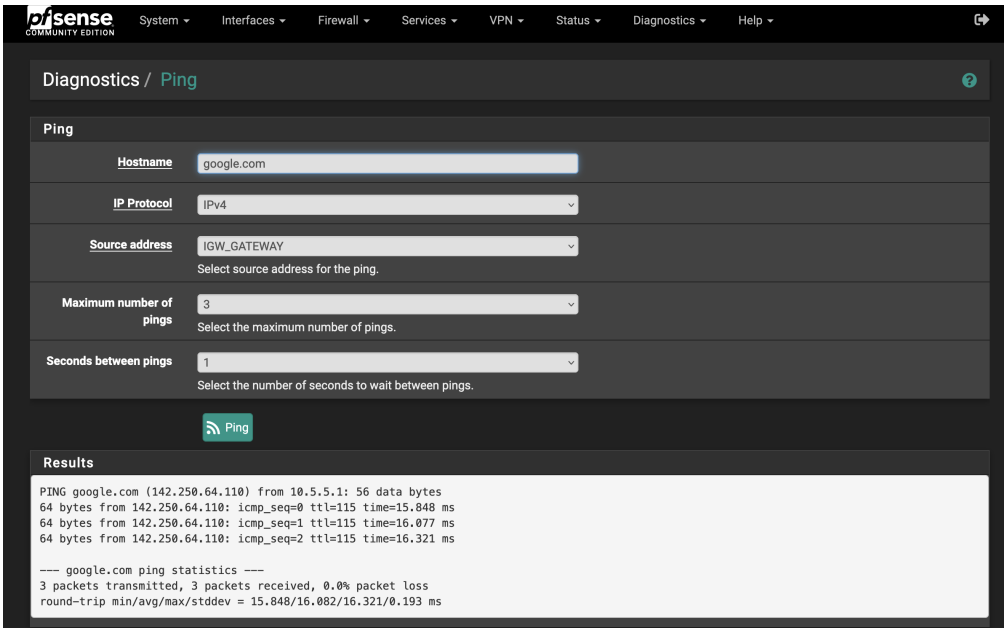
- We have specified DNS servers that the pfSense system uses to resolve DNS requests. However, we need to configure the pfsense to use these servers we have specified and to do that, we navigate to ***Services > DNS Resolver***.
- Enable the DNS Resolver and scroll down to select **"Enable Forwarding Mode"** under DNS Query Forwarding. This is the configuration change that enables pfsense to use the external DNS servers that we have already specified under General Settings.



- If you are looking at resolving internal hostnames, select the options as below.

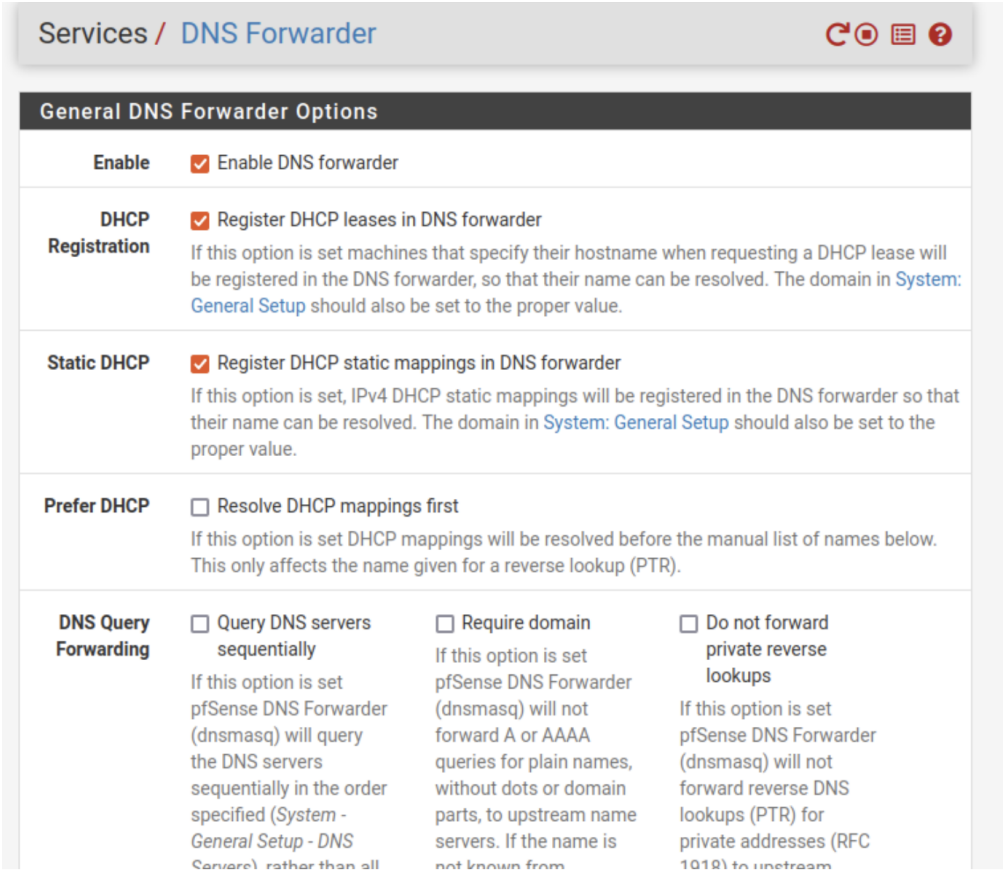


- Save the DNS Resolver settings and your networks should be able to resolve hostnames
- Navigate to ***Diagnostics > Ping*** and ping any hostname that you would like to resolve.

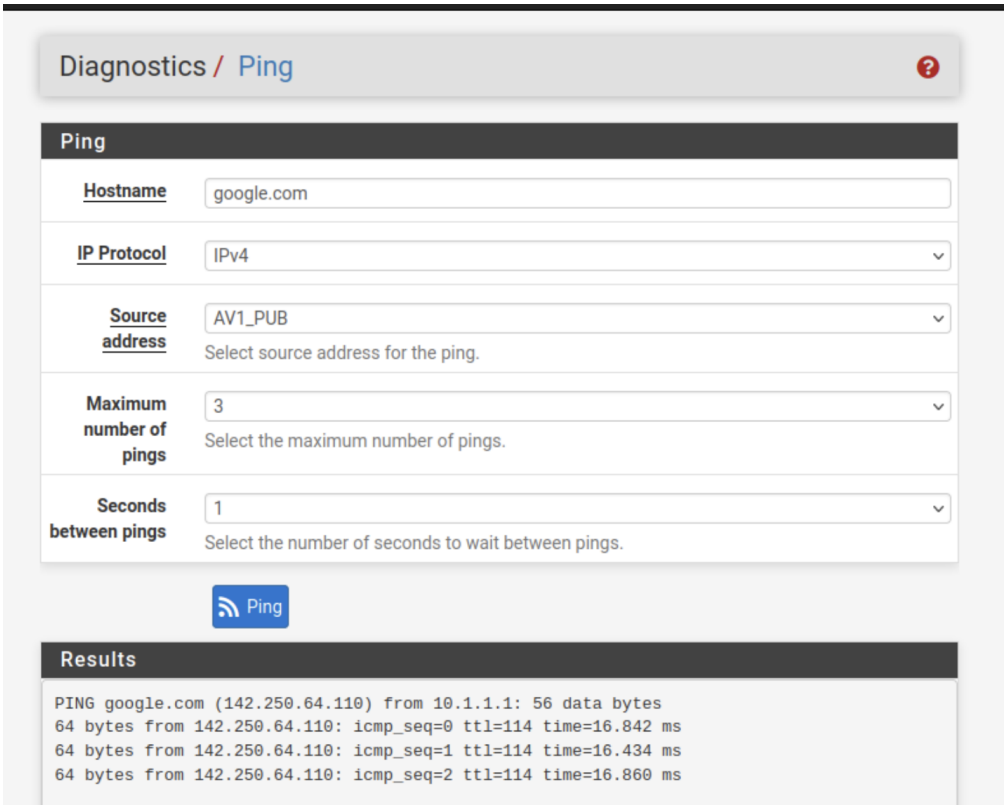


STEP-12: DNS on Availability Zone - 1

- To solve for DNS on this zone, the idea is to forward the DNS requests to the IGW_Gateway and the IGW router will handle the resolution of DNS requests.
- List the IP address of the IGW_Gateway which is 10.5.5.1 in the System > General Setup > DNS Server Settings field
- ***Navigate to Services > DNS Resolver*** and disable the DNS resolver. We can directly use the DNS Forwarder to forward the requests to 10.5.5.1.



- Navigate to Diagnostics > Ping and ping any hostname that you would like to resolve.



The above guide helps replicate a Virtual Private Cloud like networking architecture using PfSense. The firewall rules and IP addresses can be modified as deemed fit.