

- **Virtual Private Cloud Networking on PfSense**
 - **SCENARIO**
 - **IMPLEMENTATION**
 - **STEP-1:** Creating Virtual Interfaces
 - **STEP-2:** Creating Virtual Machines
 - **STEP-3:** Configuring the IGW Router
 - **STEP-4:** Configuring DHCP on IGW
 - **STEP-5:** Configuring the AV-1 Router
 - **STEP-6:** Configuring DHCP on AV1
 - **STEP-7:** Configuring Routing on IGW
 - **STEP-8:** Configuring Firewall on IGW
 - **STEP-9:** Routing on Availability Zone - 1
 - **STEP-10:** Firewall on Availability Zone - 1
 - **STEP-11:** DNS Configuration on IGW
 - **STEP-12:** DNS on Availability Zone - 1

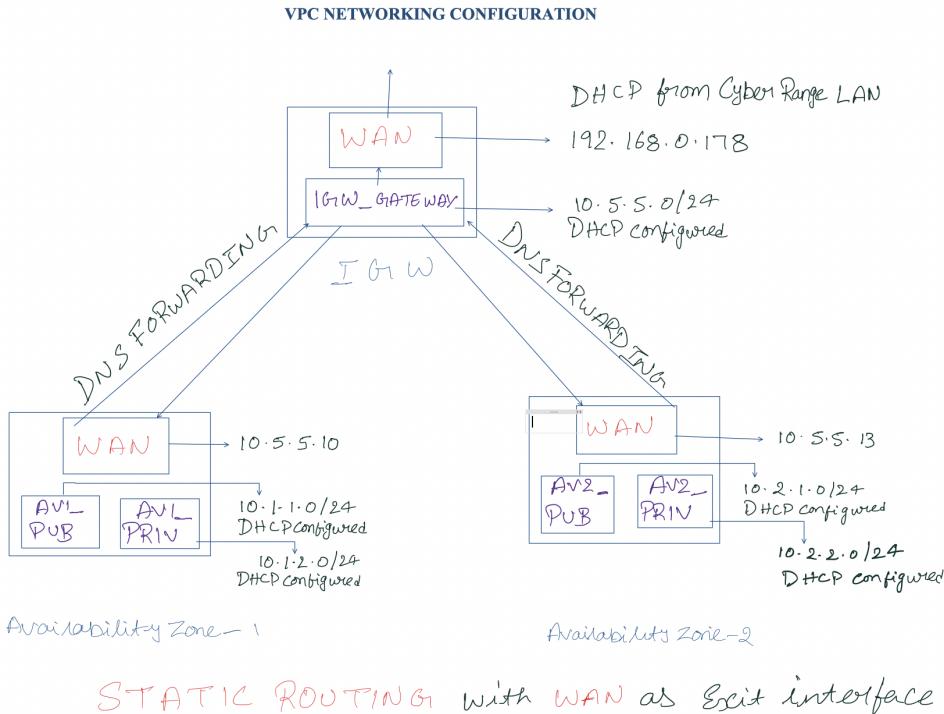
Virtual Private Cloud Networking on PfSense

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 to 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.

```

6) Halt system          15) Restore recent configuration
7) Ping host            16) Restart PHP-FPM
8) Shell

Enter an option: 1

Valid interfaces are:

xn0      6e:d9:71:31:e6:24  (up) Virtual Network Interface
xn1      d2:aa:c5:14:04:bf  (up) Virtual Network Interface
xn2      ca:2c:82:b3:fc:fc  (up) Virtual Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

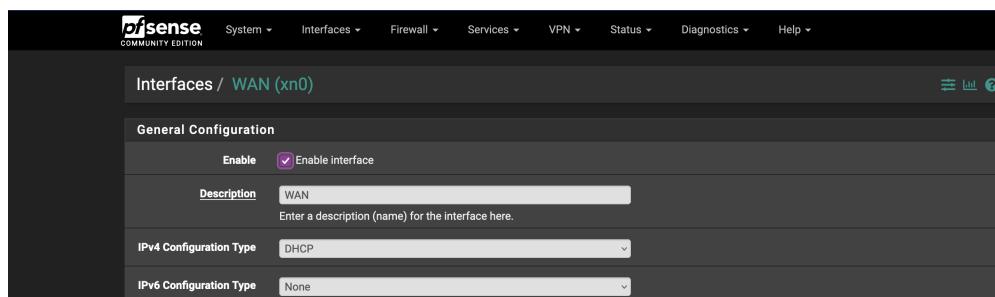
Should VLANs be set up now [y\?n]?

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(xn0 xn1 xn2 or a): 

```

- 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.

General Configuration

Enable: **Enable interface**

Description: **IGW_Gateway**
Enter a description (name) for the interface here.

IPv4 Configuration Type: **Static IPv4**

IPv6 Configuration Type: **None**

MAC Address: **xxxxxxxxxxxx** **...**
This field can be used to modify ('spoof') the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.

MTU: **1500**
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS: **1460**
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IP/6 header size) will be in effect.

Speed and Duplex: **Default (no preference, typically autoselect)**
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: **10.5.5.1** / **24**

IPv4 Upstream gateway: **None** **+ Add a new gateway**

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.

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.

The screenshot shows the pfSense web interface under the 'Services / DHCP Server / IGW_GATEWAY' path. The 'General Options' tab is selected. In the 'General Options' section, the 'Enable' checkbox is checked. Under 'Deny unknown clients', the dropdown is set to 'Allow all clients'. Under 'Ignore denied clients', the checkbox is unchecked. Under 'Ignore client identifiers', the checkbox is checked. The 'Subnet' is set to 10.5.5.0, 'Subnet mask' to 255.255.255.0, and 'Available range' to 10.5.5.1 - 10.5.5.254. The 'Range' field shows 'From' 10.5.5.10 and 'To' 10.5.5.245. In the 'Other Options' section, the 'Gateway' is set to 10.5.5.1. Other options like 'Domain name', 'Default lease time', and 'Maximum lease time' are also visible.

- 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.

The screenshot shows the Winbox interface for configuring the 'Interfaces / AV1_PUB (xn1)' interface. The 'General Configuration' section includes fields for 'Enable' (checked), 'Description' (AV1_PUB), and 'IPv4 Configuration Type' (Static IPv4). The 'IPv6 Configuration Type' is set to 'None'. In the 'Static IPv4 Configuration' section, the 'IPv4 Address' is set to 10.1.1.1 with a subnet mask of 24. The 'IPv4 Upstream gateway' dropdown is set to 'None', and there is a green button labeled '+ Add a new gateway'.

- 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.

General Configuration

- Enable:** Enable interface
- Description:** AV1_PRIV
Enter a description (name) for the interface here.
- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None

Static IPv4 Configuration

- IPv4 Address:** 10.1.2.1 / 24
- IPv4 Upstream gateway:** None [+ Add a new gateway](#)
- If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Reserved Networks

- Block private networks and loopback addresses:**
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
- Block bogon networks:**
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.

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.

The screenshot shows the pfSense DHCP configuration interface for the AV1_PRIV interface. The interface is divided into several sections:

- General Options:** Includes settings for enabling the DHCP server on the AV1_PUB interface, ignoring BOOTP queries, and defining client access rules (Allow all clients, Deny known clients from any interface, Allow known clients from only this interface). It also specifies the subnet (10.1.1.0), subnet mask (255.255.255.0), and available IP range (10.1.1.1 - 10.1.1.254).
- DHCP Specification:** Details the subnet (10.1.1.0), subnet mask (255.255.255.0), and available range (10.1.1.1 - 10.1.1.254).
- Key Algorithm:** Set to HMAC-SHA256 (current bind9 default). A note indicates this sets the algorithm for OMAPI key use.
- Other Options:** Includes fields for Gateway (10.1.1.1), Domain name, and Domain search list.

- DHCP AV1_PRIV

The screenshot shows the pfSense DHCP configuration interface. At the top, there are tabs for AV1_PUB and AV1_PRIV, with AV1_PRIV selected. The main section is titled "General Options". It includes fields for enabling the DHCP server on the AV1_PRIV interface (checked), ignoring BOOTP queries (unchecked), and client deny rules. The "Deny unknown clients" dropdown is set to "Allow all clients". Below this, there are sections for "Ignore denied clients" (unchecked) and "Ignore client identifiers" (unchecked). The subnet is set to 10.1.2.0, subnet mask to 255.255.255.0, and available range to 10.1.2.1 - 10.1.2.254. The "Range" fields show "From" as 10.1.2.10 and "To" as 10.1.2.240. Below this, there is another identical section for the same subnet and range.

Subnet	10.1.2.0	
Subnet mask	255.255.255.0	
Available range	10.1.2.1 - 10.1.2.254	
Range	10.1.2.10	10.1.2.240
	From	To

Subnet	10.1.2.0	
Subnet mask	255.255.255.0	
Available range	10.1.2.1 - 10.1.2.254	
Range	10.1.2.10	10.1.2.240
	From	To

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.

Network	Gateway	Interface	Description	Actions
0.0.0.1	WAN_DHCPC - 192.168.7.254	WAN	Allow outbound access	

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.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 25 KIB	IPv4+6 *	WAN net	*	*	*	*	*	none	Wan Remote	
0 / 0 B	IPv4 *	*	*	WAN net	*	*	*	none		
0 / 0 B	IPv4 *	*	*	IGW_GATEWAY net	*	*	*	none		
0 / 0 B	IPv4 *	*	*	10.5.5.16	*	*	*	none		
0 / 0 B	IPv4+6 TCP	*	*	*	80 (HTTP)	*	none	Allow HTTP		

- 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.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 0 B	*	*	*	IGW_GATEWAY Address	443	*	*	none	Anti-Lockout Rule	
2 / 353 KIB	IPv4+6 *	*	*	IGW_GATEWAY net	*	*	*	none	Testing inbound.	
0 / 49 KIB	IPv4+6 TCP	*	*	*	80 (HTTP)	*	*	none		
0 / 0 B	IPv6 UDP	fe80:889c:6ff:fee8:4167	*	2001:500:1::53	53 (DNS)	*	none	Easy Rule: Passed from Firewall Log View		

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.

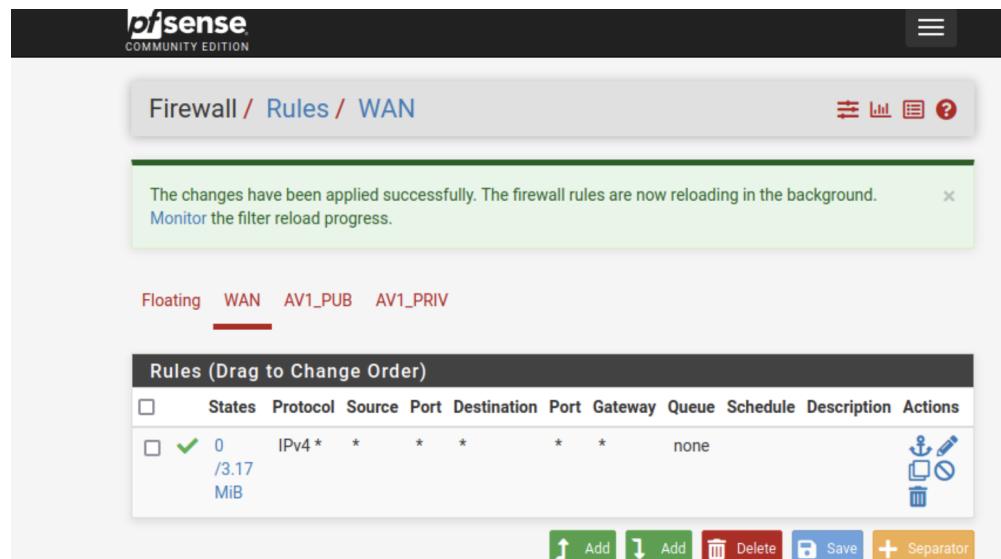
The screenshot shows the pfSense web interface with the title 'System / Routing / Static Routes'. The 'Static Routes' tab is selected. A table lists two static routes:

Network	Gateway	Interface	Description	Actions
0.0.0.0/1	WAN_DHCP - 10.5.5.1	WAN		
10.2.1.0/24	WAN_DHCP - 10.5.5.1	WAN		

Below the table is a green 'Add' button with a '+' icon. At the bottom of the page, there is a footer bar with the text 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.'

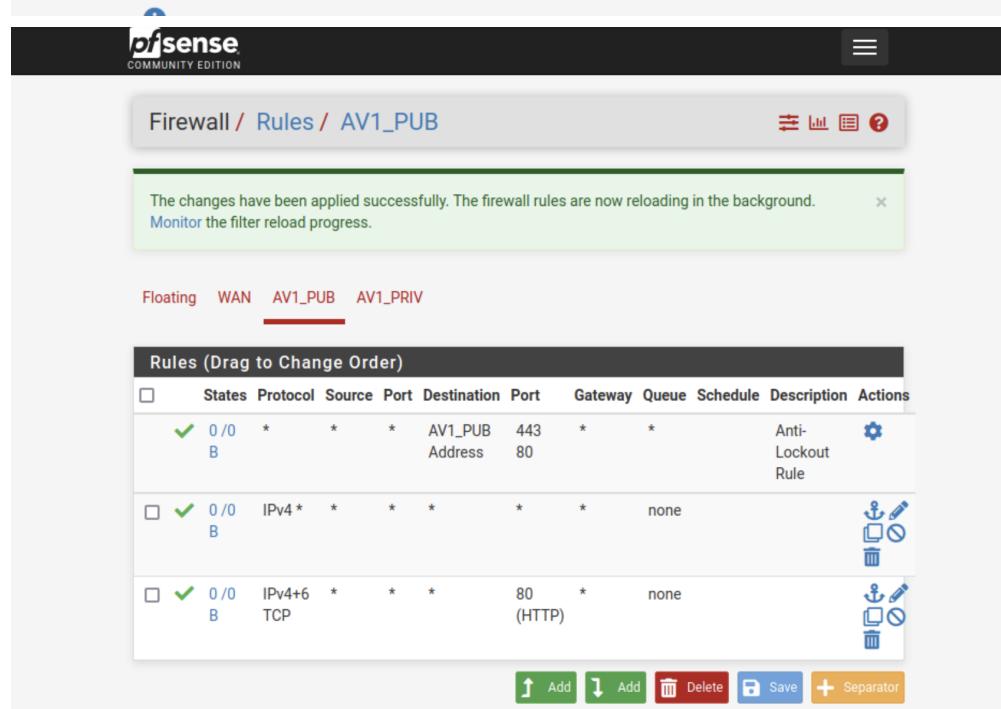
STEP-10: Firewall on Availability Zone - 1

- 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.



The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor](#) the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions			
<input checked="" type="checkbox"/> 0 /3.17	IPv4	*	*	*	*	*	*		none				



The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor](#) the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions			
<input checked="" type="checkbox"/> 0 /0		*	*	AV1_PUB	443	*	*		Anti-Lockout Rule				
<input checked="" type="checkbox"/> 0 /0	IPv4	*	*	*	*	*	*		none				
<input checked="" type="checkbox"/> 0 /0	IPv4+6	*	*	*	80	*			(HTTP)				

- 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.

DNS Query Forwarding **Enable Forwarding Mode**
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).

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

DHCP Registration **Register DHCP leases in the DNS Resolver**
If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in [System > General Setup](#) should also be set to the proper value.

Static DHCP **Register DHCP static mappings in the DNS Resolver**
If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

- 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.

Ping

Hostname: google.com

IP Protocol: IPv4

Source address: IGW_GATEWAY
Select source address for the ping.

Maximum number of pings: 3
Select the maximum number of pings.

Seconds between pings: 1
Select the number of seconds to wait between pings.

Results

```
PING google.com (142.250.64.110) from 10.5.5.1: 56 data bytes
64 bytes from 142.250.64.110: icmp_seq=0 ttl=115 time=15.848 ms
64 bytes from 142.250.64.110: icmp_seq=1 ttl=115 time=16.077 ms
64 bytes from 142.250.64.110: icmp_seq=2 ttl=115 time=16.321 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 15.848/16.082/16.321/0.193 ms
```

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.

General DNS Forwarder Options

Enable	<input checked="" type="checkbox"/> Enable DNS forwarder		
DHCP Registration	<input checked="" type="checkbox"/> Register DHCP leases in DNS forwarder If this option is set machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. The domain in System: General Setup should also be set to the proper value.		
Static DHCP	<input checked="" type="checkbox"/> Register DHCP static mappings in DNS forwarder If this option is set, IPv4 DHCP static mappings will be registered in the DNS forwarder so that their name can be resolved. The domain in System: General Setup should also be set to the proper value.		
Prefer DHCP	<input type="checkbox"/> Resolve DHCP mappings first If this option is set DHCP mappings will be resolved before the manual list of names below. This only affects the name given for a reverse lookup (PTR).		
DNS Query Forwarding	<input type="checkbox"/> Query DNS servers sequentially If this option is set pfSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (System - General Setup - DNS Servers) rather than all	<input type="checkbox"/> Require domain If this option is set pfSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from	<input type="checkbox"/> Do not forward private reverse lookups If this option is set pfSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1912) to upstream

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

Ping

Hostname	google.com
IP Protocol	IPv4
Source address	AV1_PUB
Select source address for the ping.	
Maximum number of pings	3
Select the maximum number of pings.	
Seconds between pings	1
Select the number of seconds to wait between pings.	

Results

```
PING google.com (142.250.64.110) from 10.1.1.1: 56 data bytes
64 bytes from 142.250.64.110: icmp_seq=0 ttl=114 time=16.842 ms
64 bytes from 142.250.64.110: icmp_seq=1 ttl=114 time=16.434 ms
64 bytes from 142.250.64.110: icmp_seq=2 ttl=114 time=16.860 ms
```

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.