PART 1: Service chaining

Summary:

In this part, you will manage service chaining in OpenStack.

Section 1: In-network service chaining:

Create the service chaining in Figure 2 according to the lecture instructions.

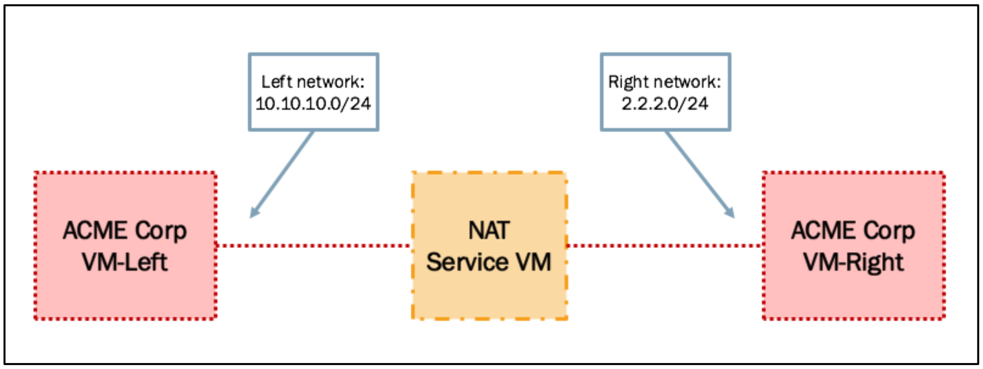
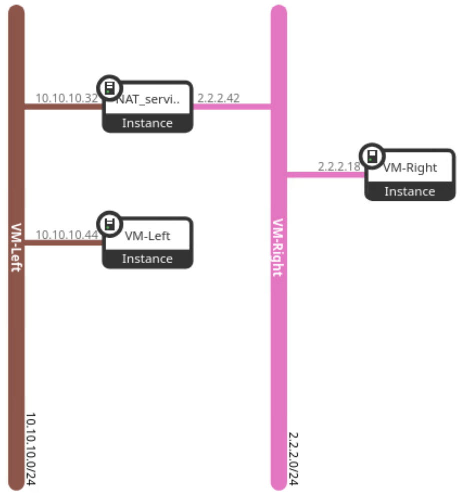


Figure 2. In-Network Service Chaining setup

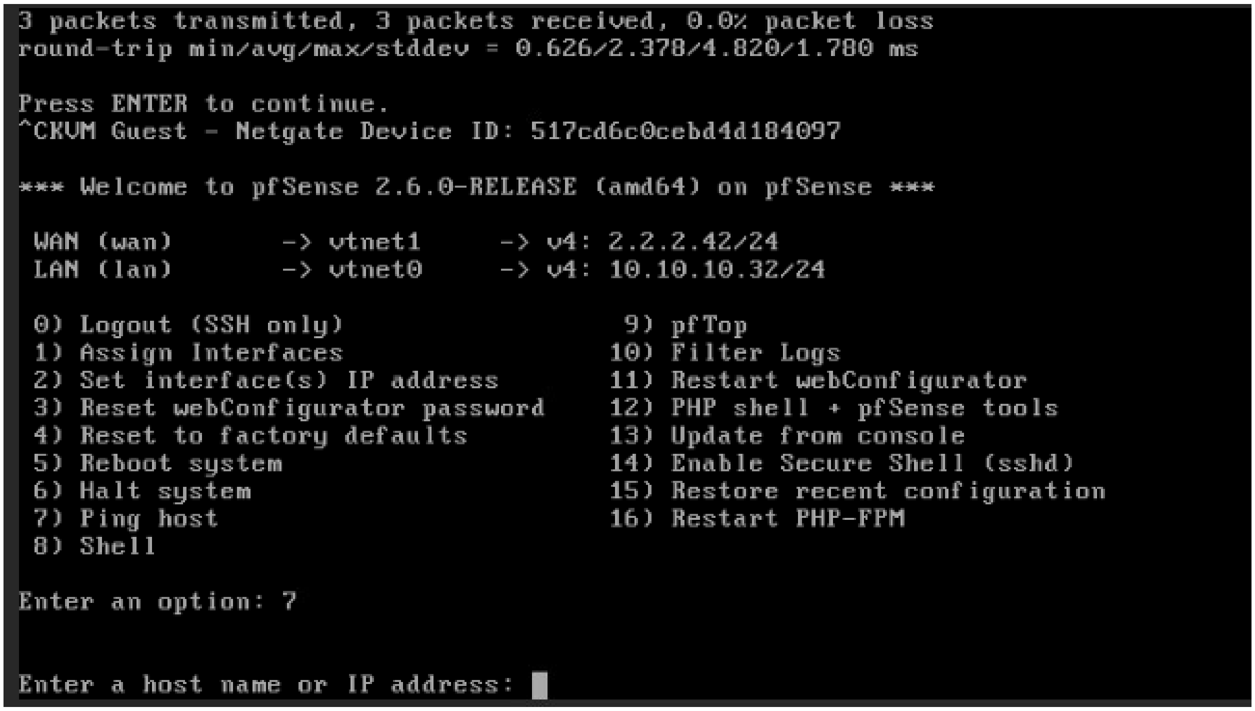
You can either create your own NAT VM appliance or download and use one from another source such as: pfSense.



For the NAT service, I used the pfsense VM. Installed from https://github.com/CloudSentralDotNet/iso_pfsense/releases.

Initial installation of pfsense is a bit weird because of the type of storage/drive we choose. But somehow got it installed.

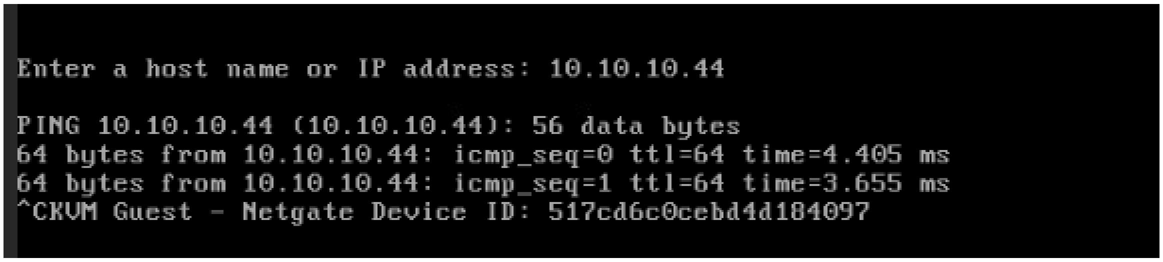
We need to first assign the wan and lan interfaces on the cli and then we can later change interfaces settings.



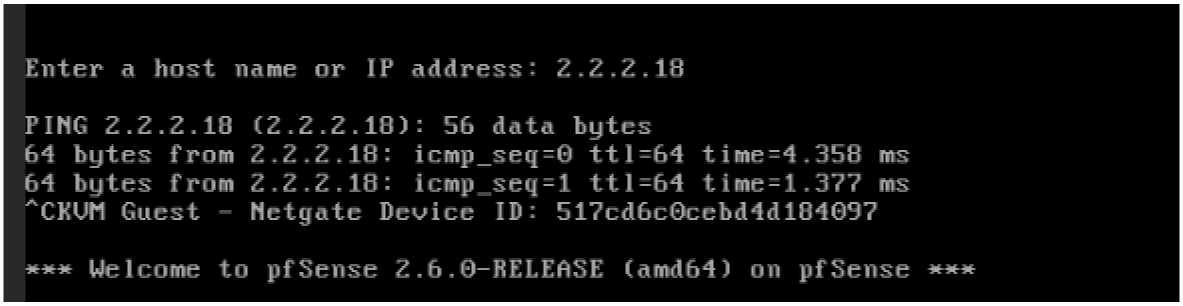
```
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.626/2.378/4.820/1.780 ms

Press ENTER to continue.
^CKVM Guest - Netgate Device ID: 517cd6c0cebd4d184097

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet1     -> v4: 2.2.2.42/24
 LAN (lan)       -> vtnet0     -> v4: 10.10.10.32/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 
```

MAKE SURE THAT THE INTERFACE(wan and lan) IP ADDRESSES MATCH WHAT OPENSTACK HAS ASSIGEND TO THE PFSENSE INTERFACES!

Ping Test



```
Enter a host name or IP address: 10.10.10.44

PING 10.10.10.44 (10.10.10.44): 56 data bytes
64 bytes from 10.10.10.44: icmp_seq=0 ttl=64 time=4.405 ms
64 bytes from 10.10.10.44: icmp_seq=1 ttl=64 time=3.655 ms
^CKVM Guest - Netgate Device ID: 517cd6c0cebd4d184097
```



```
Enter a host name or IP address: 2.2.2.18

PING 2.2.2.18 (2.2.2.18): 56 data bytes
64 bytes from 2.2.2.18: icmp_seq=0 ttl=64 time=4.358 ms
64 bytes from 2.2.2.18: icmp_seq=1 ttl=64 time=1.377 ms
^CKVM Guest - Netgate Device ID: 517cd6c0cebd4d184097

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
```

INTER-VN PINGS AND COMMUNICATION with single VM service chaining:

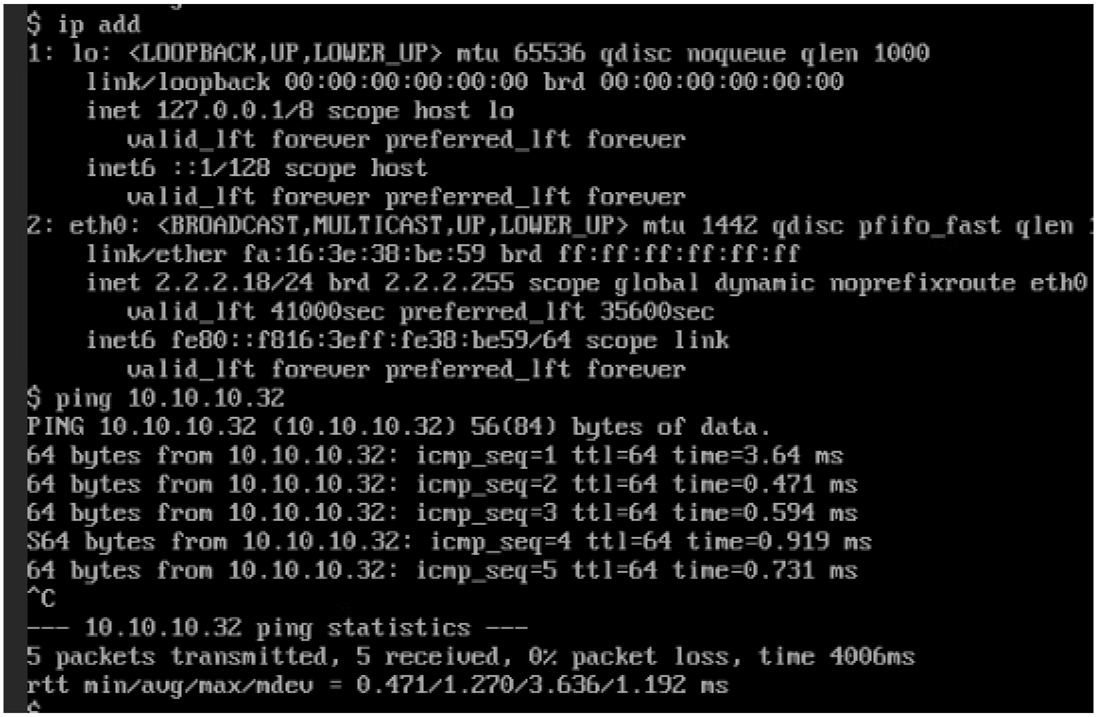
For Making inter-VN pings work via service chaining, You need to make sure that port security for all instance interfaces is TURNED OFF!

Pfsense VM is overly secure. Make sure you go to pfsense console and then run the command:

pfctl -d

to disable firewall temporarily

Ping Test from 2.2.2.0/24 network VM to 10.10.10.0/24 network VM:



```
$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen
    link/ether fa:16:3e:38:be:59 brd ff:ff:ff:ff:ff:ff
    inet 2.2.2.18/24 brd 2.2.2.255 scope global dynamic noprefixroute eth0
       valid_lft 41000sec preferred_lft 35600sec
    inet6 fe80::f816:3eff:fe38:be59/64 scope link
       valid_lft forever preferred_lft forever
$ ping 10.10.10.32
PING 10.10.10.32 (10.10.10.32) 56(84) bytes of data.
64 bytes from 10.10.10.32: icmp_seq=1 ttl=64 time=3.64 ms
64 bytes from 10.10.10.32: icmp_seq=2 ttl=64 time=0.471 ms
64 bytes from 10.10.10.32: icmp_seq=3 ttl=64 time=0.594 ms
S64 bytes from 10.10.10.32: icmp_seq=4 ttl=64 time=0.919 ms
64 bytes from 10.10.10.32: icmp_seq=5 ttl=64 time=0.731 ms
^C
--- 10.10.10.32 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.471/1.270/3.636/1.192 ms
$
```

Section 2: Transparent service chaining:

Add a Layer 2 firewall to the setup in Section 1. The firewall will block SSH protocol on port 22. The setup will look like Figure 3.

You may want to create your own Firewall VM or use the pfSense appliance mentioned in previous section.

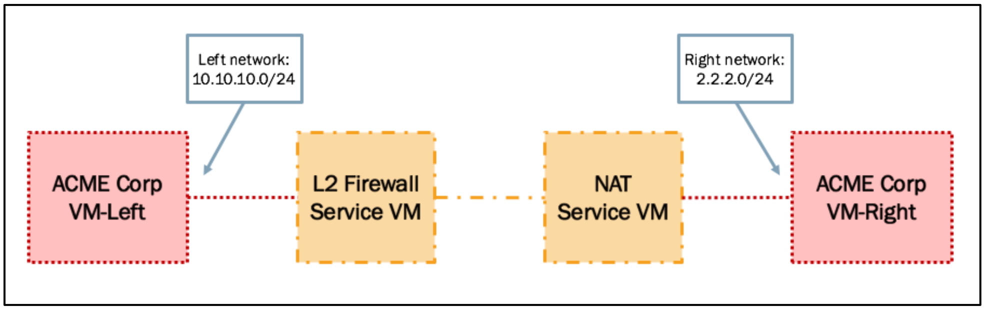
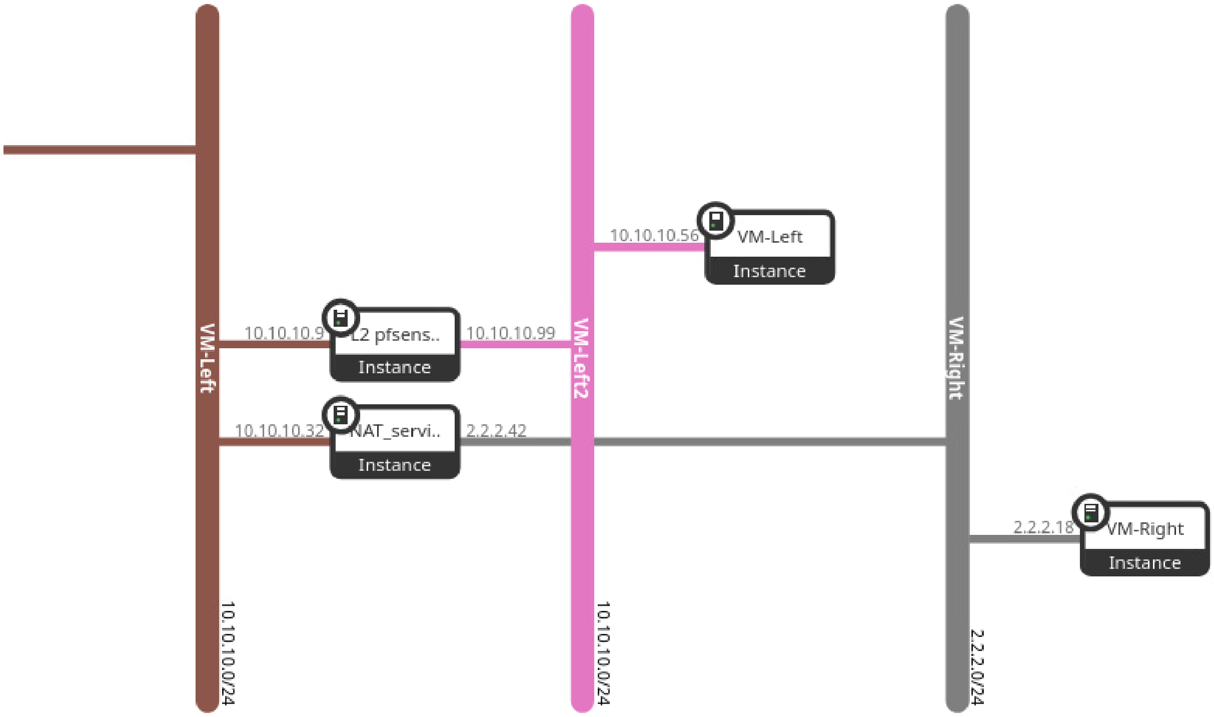


Figure 3. Service Chaining with L2 Firewall

Adding a transparent instance looks something like this:



Initial topology config:

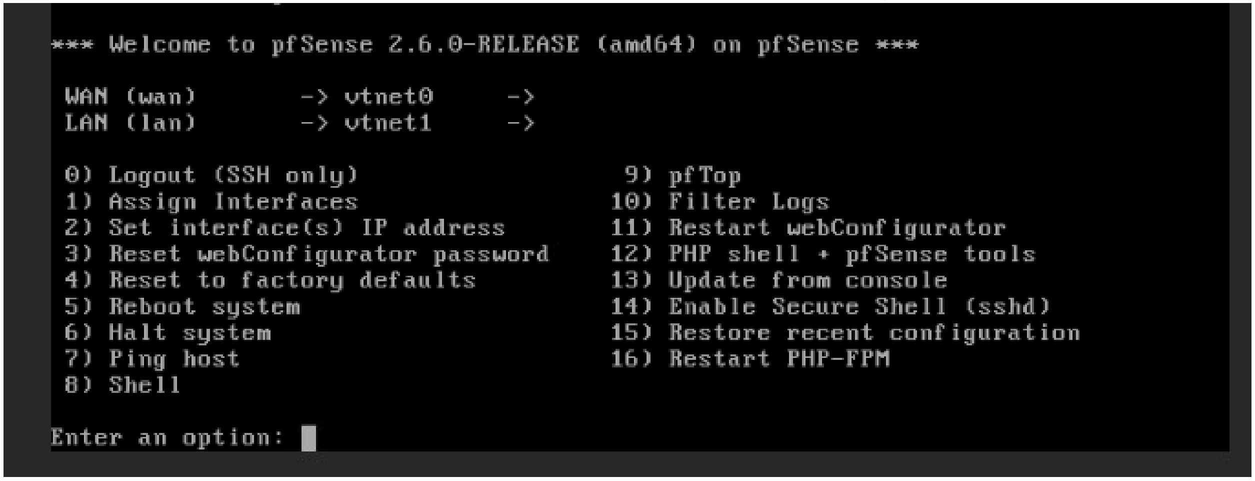
1. In the above topology we created two VNs with the same subnet(VM-left and VM-left2)
2. We will have to manually go to networks and put the new VN in the admin up state
3. Now, we add out VM left instance to VM-left2 VN and then add our transparent L2 firewall instance's interfaces to both VM-left and VM-left2 VNs. We are using pfsense for L2 transparent Instance and for the NAT_service
4. Now add NAT_service instance to the VM-left and VM-right VNs

Configs on VM-left

1. VM-left will be assigned with an IP address in the 10.10.10.0/24 subnet.
2. No additional configs required at this point of time
3. REMEMBER TO DISABLE PORT SECURITY on all interfaces for all devices
4. VM should have a default route or a static route to the 2.2.2.0/24 network via the NAT VM Ip address(10.10.10.32)

Configs on L2 Pfsense FW:

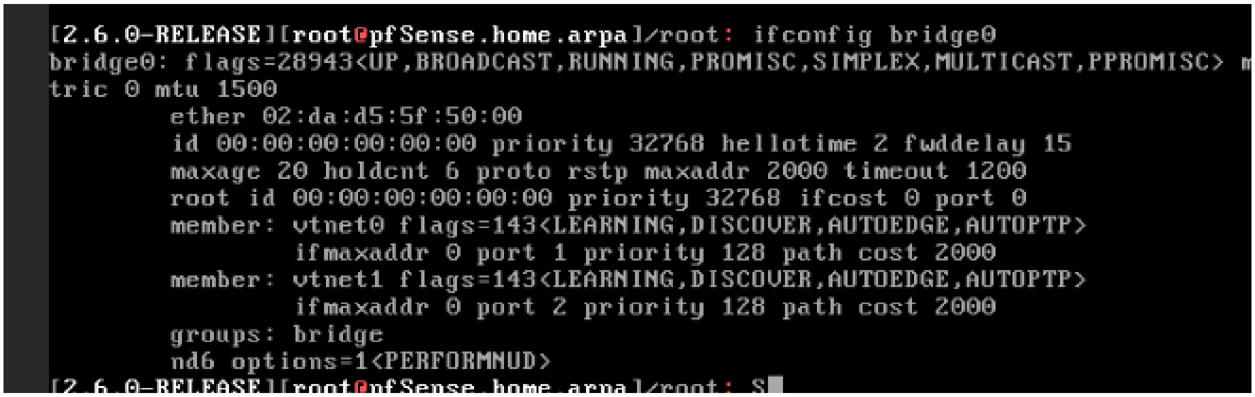
1. Openstack will try to assign IP addresses for both vtnet0 and vtnet1. Go to set interface Ip address and then just remove all Ip address mappings



```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     ->
 LAN (lan)       -> vtnet1     ->

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

2. Go to console and create a bridge interface between vtnet1 and vtnet0

```
ifconfig bridge0 create
ifconfig bridge0 addm vtnet0 addm vtnet1 up
```



```
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: ifconfig bridge0
bridge0: flags=28943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST,PPROMISC> m
tric 0 mtu 1500
        ether 02:da:d5:5f:50:00
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: vtnet0 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 1 priority 128 path cost 2000
        member: vtnet1 flags=143<LEARNING,DISCOVER,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 2 priority 128 path cost 2000
        groups: bridge
        nd6 options=1<PERFORMNUD>
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: $
```

Make sure vtnet0 and vtnet1 interfaces are added as members to the bridge interface bridge0

3. Temporarily Disable firewall on pfsense for sanity check:

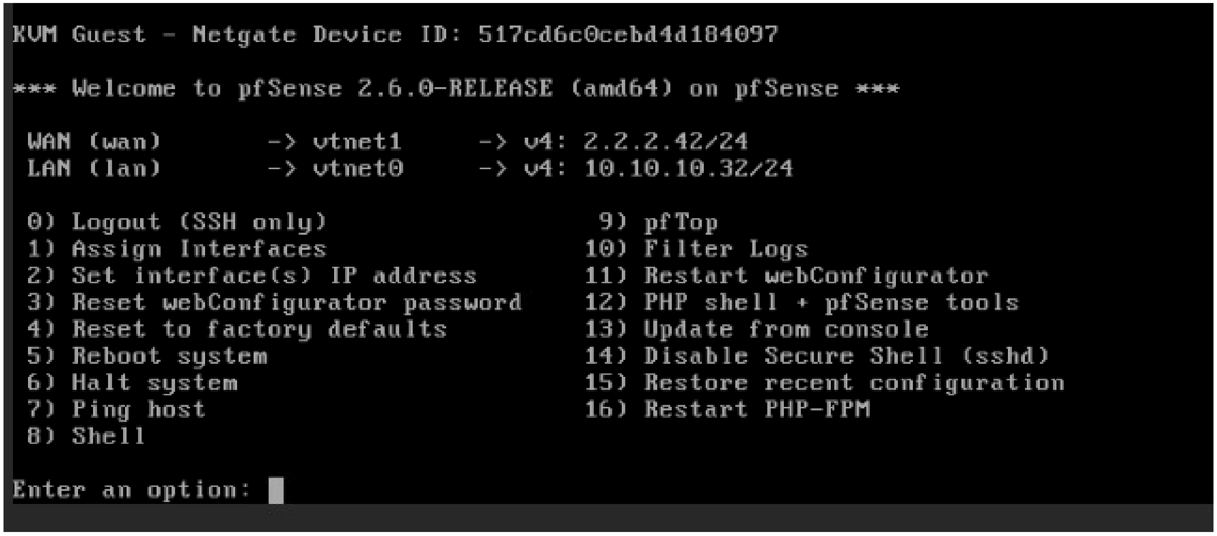
```
pfctl -d
```

4. Turn on promisc mode for all interfaces

```
Ifconfig bridge0 promisc
ifconfig vtnet0 promisc
ifconfig vtnet1 promisc
```

Configs on NAT service VM

1. One interface should be connected to the 2.2.2.0/24 VN(VM-right) and the other one connected to the VN connected to the 10.10.10.0/24 as shown in the diagram(VM-Left)
2. Disable Firewall using pfctl -d command
3. Make sure port security is turned off on all interfaces

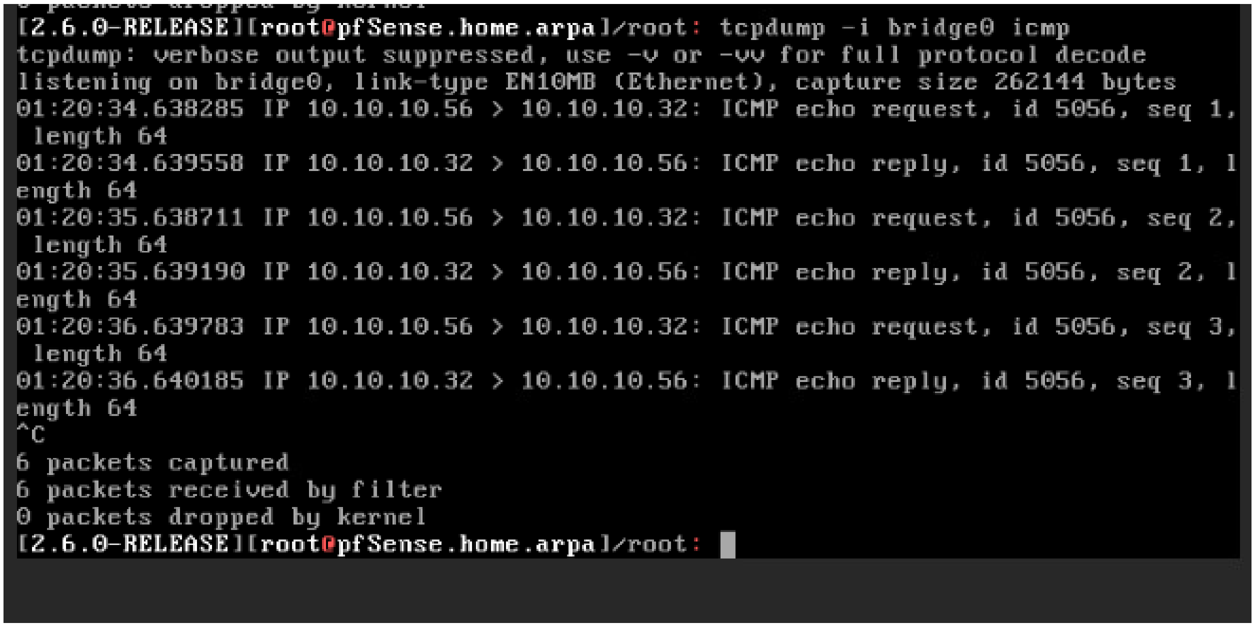


```
KVM Guest - Netgate Device ID: 517cd6c0cebd4d184097

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet1     -> v4: 2.2.2.42/24
 LAN (lan)       -> vtnet0     -> v4: 10.10.10.32/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Configs on VM-Right

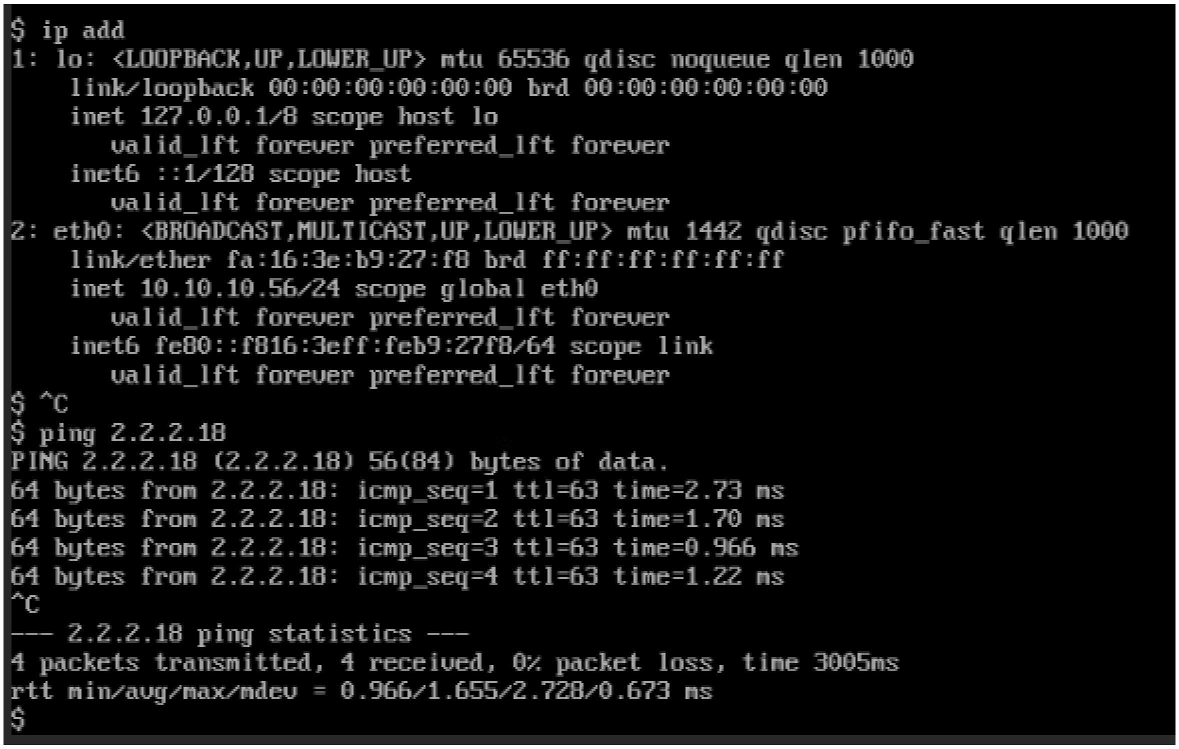
1. VM-Right will be assigned with an IP address in the 2.2.2.0/24 subnet.
2. REMEMBER TO DISABLE PORT SECURITY on all interfaces for all devices
3. VM should have a default route or a static route to the 10.10.10.0/24 network via the NAT VM Ip address(2.2.2.42)

The above configuration will make sure that the traffic passes through the L2 Transparent VM and not bypass it. In order to verify that it works, we can do a TCP dump on the Transparent instance on the bridge interface



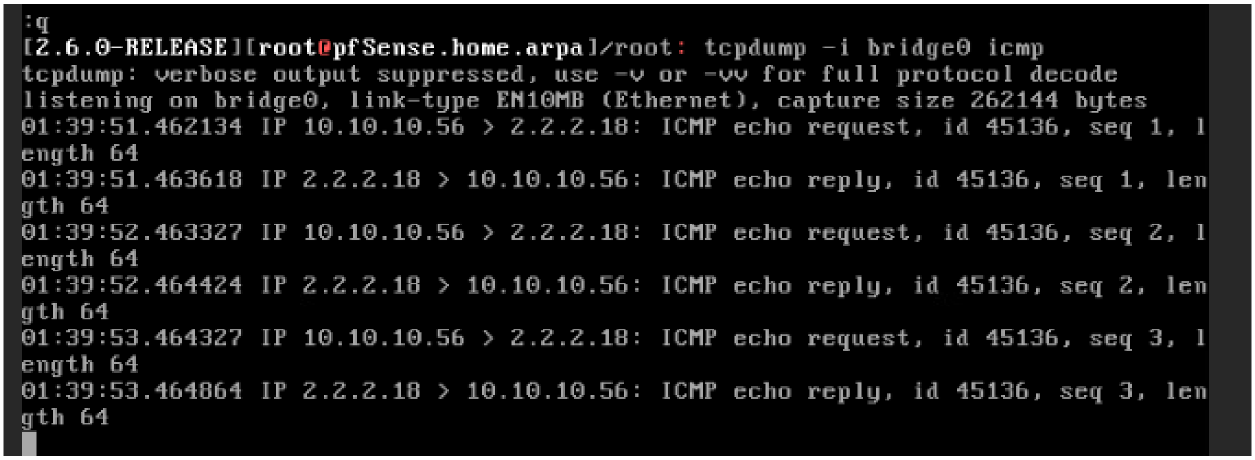
```
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: tcpdump -i bridge0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bridge0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:20:34.638285 IP 10.10.10.56 > 10.10.10.32: ICMP echo request, id 5056, seq 1,
 length 64
01:20:34.639558 IP 10.10.10.32 > 10.10.10.56: ICMP echo reply, id 5056, seq 1, l
ength 64
01:20:35.638711 IP 10.10.10.56 > 10.10.10.32: ICMP echo request, id 5056, seq 2,
 length 64
01:20:35.639190 IP 10.10.10.32 > 10.10.10.56: ICMP echo reply, id 5056, seq 2, l
ength 64
01:20:36.639783 IP 10.10.10.56 > 10.10.10.32: ICMP echo request, id 5056, seq 3,
 length 64
01:20:36.640185 IP 10.10.10.32 > 10.10.10.56: ICMP echo reply, id 5056, seq 3, l
ength 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[2.6.0-RELEASE][root@pfSense.home.arpa]/root:
```

Ping test between VM-left and VM-Right



```
$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:b9:27:f8 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.56/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:feb9:27f8/64 scope link
       valid_lft forever preferred_lft forever
$ ^C
$ ping 2.2.2.18
PING 2.2.2.18 (2.2.2.18) 56(84) bytes of data.
64 bytes from 2.2.2.18: icmp_seq=1 ttl=63 time=2.73 ms
64 bytes from 2.2.2.18: icmp_seq=2 ttl=63 time=1.70 ms
64 bytes from 2.2.2.18: icmp_seq=3 ttl=63 time=0.966 ms
64 bytes from 2.2.2.18: icmp_seq=4 ttl=63 time=1.22 ms
^C
--- 2.2.2.18 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.966/1.655/2.728/0.673 ms
$
```

Going through the transparent instance



```
:q
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: tcpdump -i bridge0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bridge0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:39:51.462134 IP 10.10.10.56 > 2.2.2.18: ICMP echo request, id 45136, seq 1, l
ength 64
01:39:51.463618 IP 2.2.2.18 > 10.10.10.56: ICMP echo reply, id 45136, seq 1, len
gth 64
01:39:52.463327 IP 10.10.10.56 > 2.2.2.18: ICMP echo request, id 45136, seq 2, l
ength 64
01:39:52.464424 IP 2.2.2.18 > 10.10.10.56: ICMP echo reply, id 45136, seq 2, len
gth 64
01:39:53.464327 IP 10.10.10.56 > 2.2.2.18: ICMP echo request, id 45136, seq 3, l
ength 64
01:39:53.464864 IP 2.2.2.18 > 10.10.10.56: ICMP echo reply, id 45136, seq 3, len
gth 64
```

Adding firewall rule in pfsense to block ssh traffic:

1. vi /cf/conf/config.xml
2. Add <filter> section with your rule:

```
<filter>
 <rule>
  <interface>bridge0</interface>
  <protocol>tcp</protocol>
  <source>any</source>
  <destination>any</destination>
  <port>22</port>
  <action>block</action>
 </rule>
</filter>
```

3. Reload pfSense:

```
/etc/rc.reload_all
```