

CS 646 Network Protocols Security

Team Members: Rasheed Azeez, Murali Badiger, and Shivam Patel
Spring 2018

Project 3

Task 1 – Basic Configuration

To accomplish the basic configuration task, VMware Workstation 14 Player was used. The following instances were installed:

- pfSense-CE-2.4.3 64 bit (2)
- Ubuntu 16.04.3 64 bit (2)

The names of each of the instances are

- Pfsense1. **This instance has two network interface cards (NIC) installed.**
- Pfsense2. **This instance has two network interface cards (NIC) installed.**
- Ubuntu1
- Ubuntu2

The following three virtual networks were configured as described by the parameters within the physical diagram:

- VMnet2 = 10.47.1.0/24
- VMnet3 = 10.47.3.0/24
- VMnet4 = 10.47.2.0/24

1. Ubuntu1 and pfsense1 LAN interface is connected to VMnet2.
2. Pfsense1 and pfsense2 WAN interfaces are connected to VMnet3.
3. Ubuntu2 and pfsense2 LAN interface is connected to VMnet4.



Welcome to VMware Workstation 14 Player



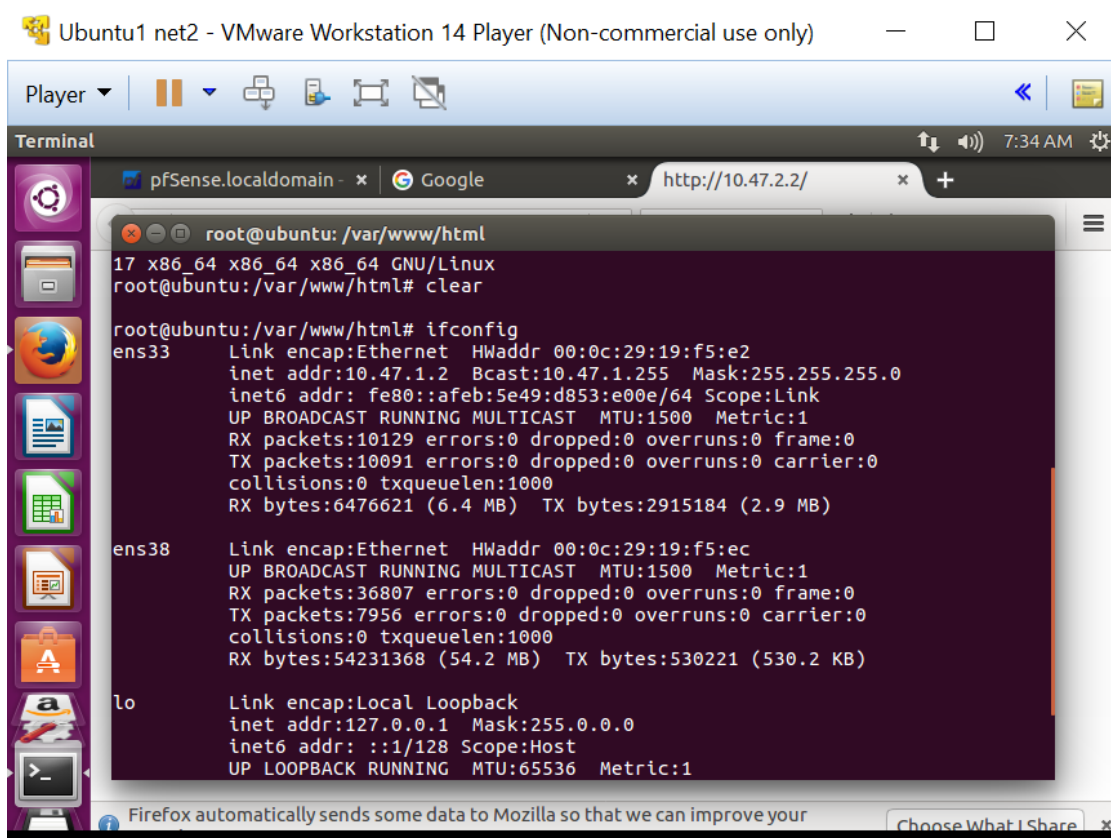
Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

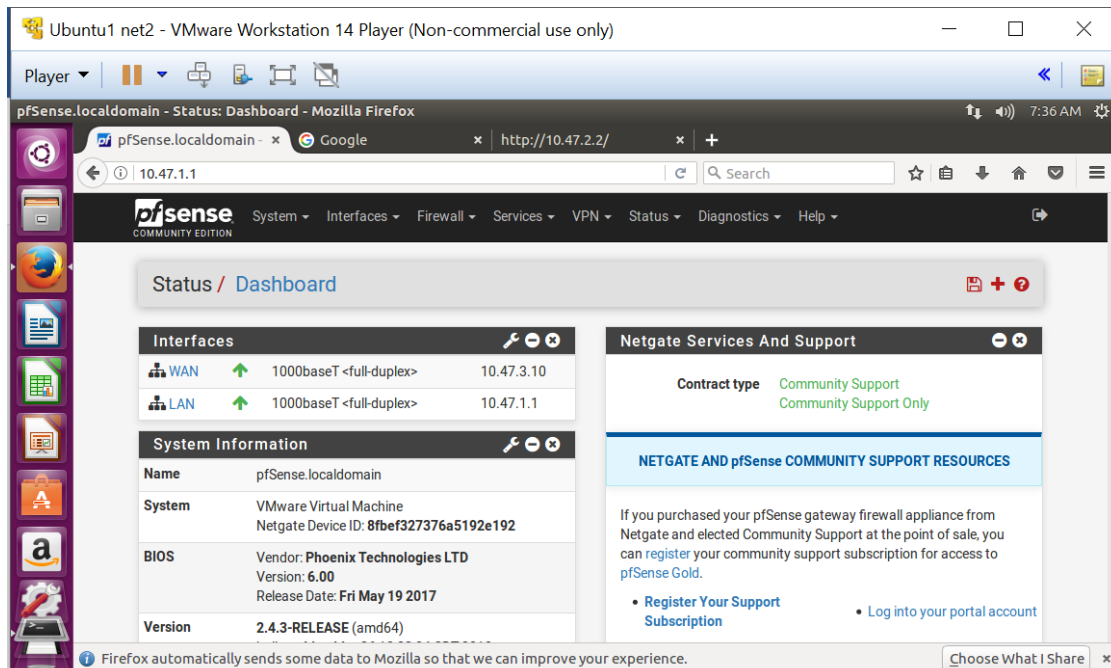


Open a Virtual Machine

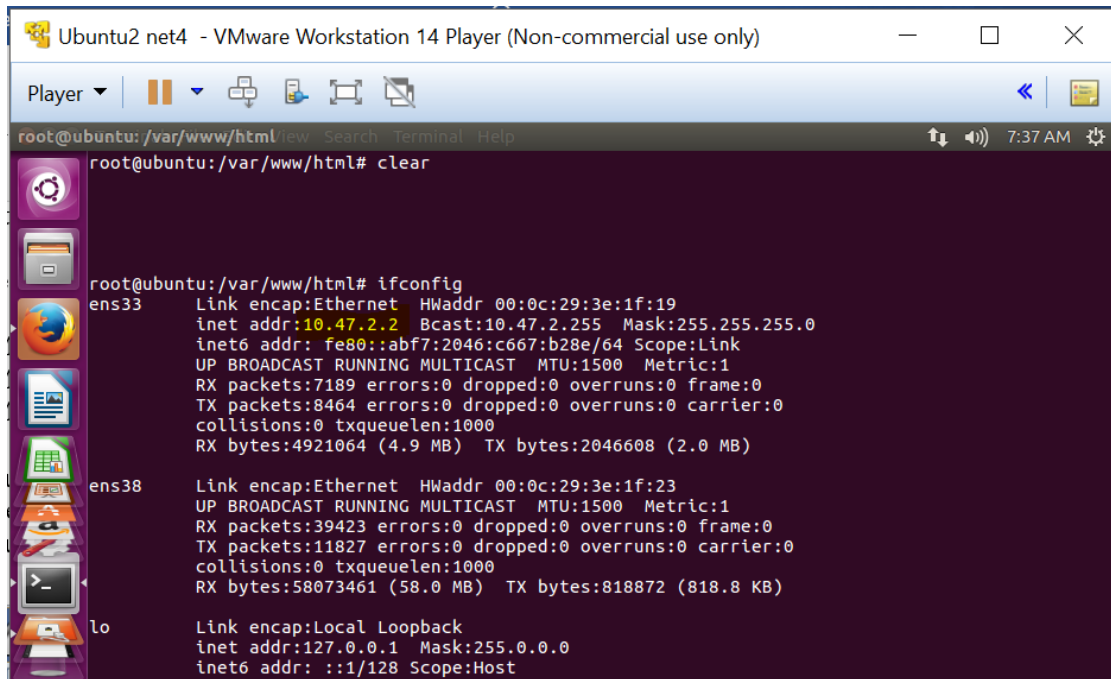
Screenshot 1: Ubuntu1 has 10.47.1.2



Screenshot 2: PfSense1



Screenshot 3: Ubuntu2



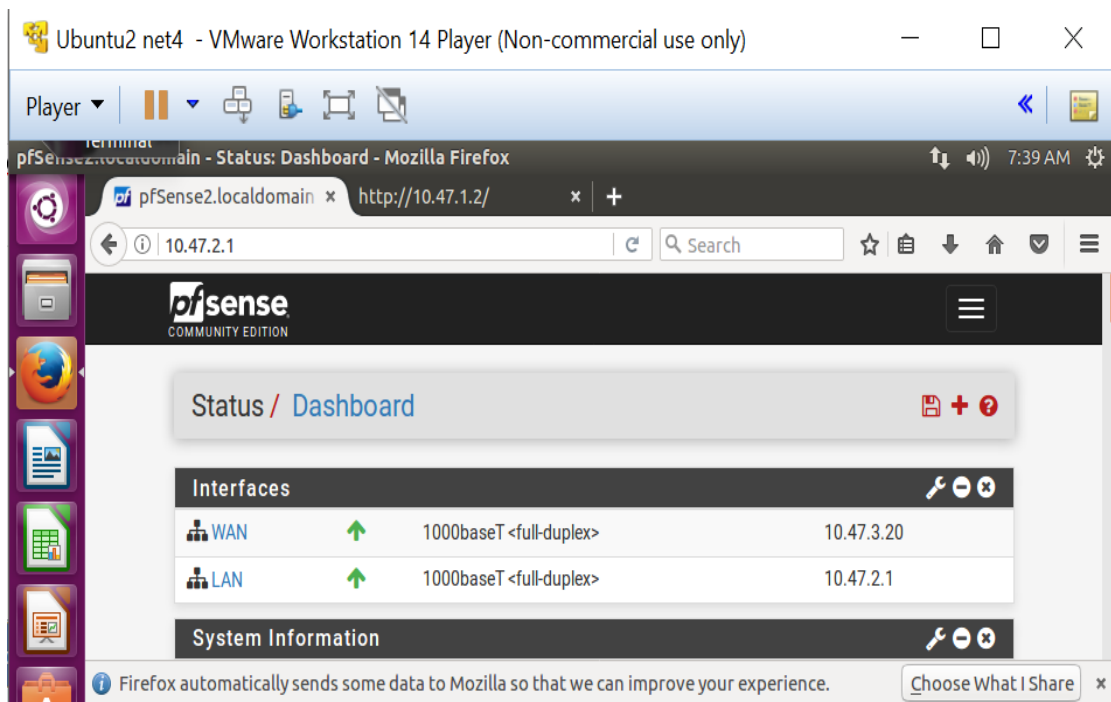
```
root@ubuntu:/var/www/html# clear

root@ubuntu:/var/www/html# ifconfig
ens33:  Link encap:Ethernet  HWaddr 00:0c:29:3e:1f:19
        inet addr:10.47.2.2  Bcast:10.47.2.255  Mask:255.255.255.0
        inet6 addr: fe80::abf7:2046:c667:b28e/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:7189 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8464 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:4921064 (4.9 MB)  TX bytes:2046608 (2.0 MB)

ens38:  Link encap:Ethernet  HWaddr 00:0c:29:3e:1f:23
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:39423 errors:0 dropped:0 overruns:0 frame:0
        TX packets:11827 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:58073461 (58.0 MB)  TX bytes:818872 (818.8 KB)

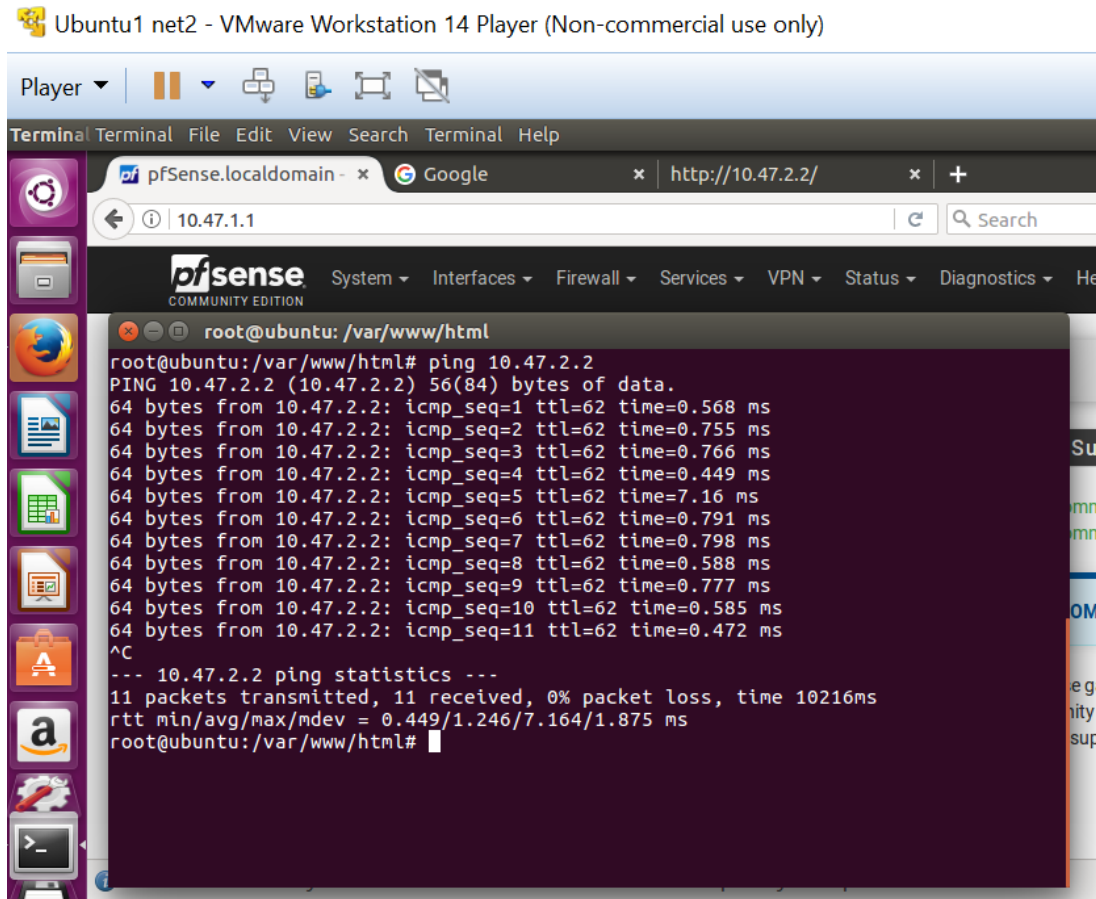
lo:     Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128  Scope:Host
```

Screenshot 4: pfsense2



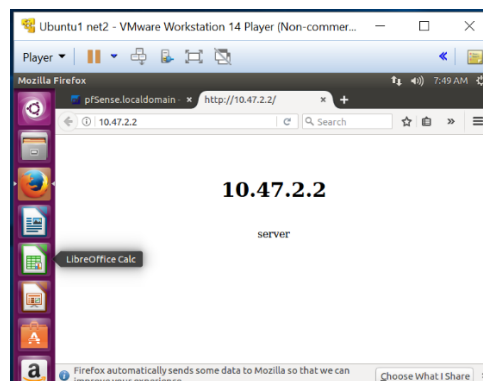
Currently, the firewall configurations are set to allow all connections. The screenshot below shows a ping command from the client machine (10.47.2.2) to the server (10.47.1.2). Please refer to the screenshot below for the results:

Screenshot 5: Ping Results from the client to the server



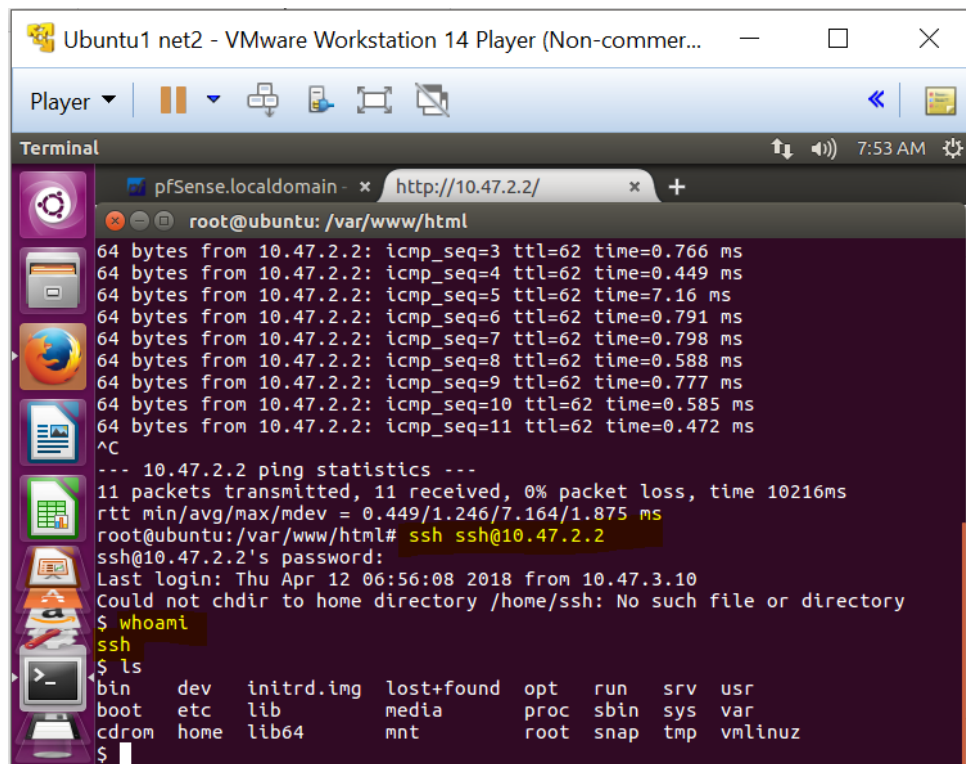
On Ubuntu, there is a server installed for the lab Apache2. The Secure Shell Hash (SSH) protocol was installed on this server. For SSH user, "SSH" was added. Below are screenshots for web and ssh server.

Screenshot 6: access server from client



The screenshot below shows the SSH session being established from Ubuntu1 to Ubuntu2.

Screenshot 8: SSH session

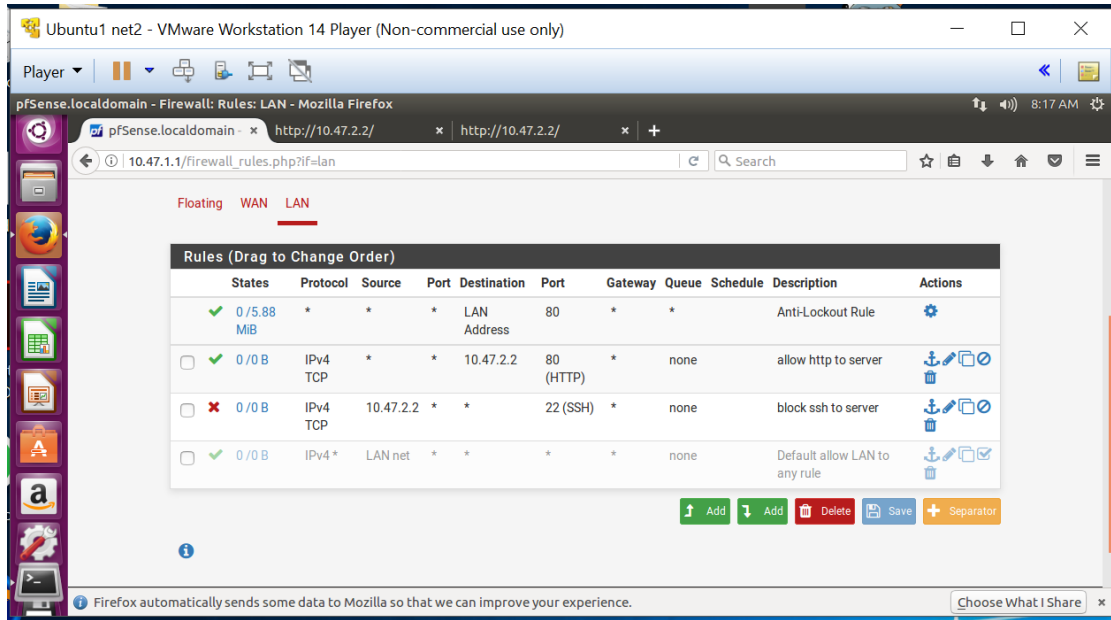


```
Ubuntu1 net2 - VMware Workstation 14 Player (Non-commer...
Player
Terminal
pfSense.localdomain - x http://10.47.2.2/ x +
root@ubuntu: /var/www/html
64 bytes from 10.47.2.2: icmp_seq=3 ttl=62 time=0.766 ms
64 bytes from 10.47.2.2: icmp_seq=4 ttl=62 time=0.449 ms
64 bytes from 10.47.2.2: icmp_seq=5 ttl=62 time=7.16 ms
64 bytes from 10.47.2.2: icmp_seq=6 ttl=62 time=0.791 ms
64 bytes from 10.47.2.2: icmp_seq=7 ttl=62 time=0.798 ms
64 bytes from 10.47.2.2: icmp_seq=8 ttl=62 time=0.588 ms
64 bytes from 10.47.2.2: icmp_seq=9 ttl=62 time=0.777 ms
64 bytes from 10.47.2.2: icmp_seq=10 ttl=62 time=0.585 ms
64 bytes from 10.47.2.2: icmp_seq=11 ttl=62 time=0.472 ms
^C
--- 10.47.2.2 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10216ms
rtt min/avg/max/mdev = 0.449/1.246/7.164/1.875 ms
root@ubuntu: /var/www/html# ssh ssh@10.47.2.2
ssh@10.47.2.2's password:
Last login: Thu Apr 12 06:56:08 2018 from 10.47.3.10
Could not chdir to home directory /home/ssh: No such file or directory
$ whoami
ssh
$ ls
bin      dev      initrd.img  lost+found  opt      run      srv      usr
boot    etc      lib         media       proc     sbin     sys      var
cdrom   home    lib64       mnt         root     snap     tmp      vmlinuz
$
```

Task 2 – Basic Security Configuration:

The following Local Area Network (LAN) configurations were established for Pfsense1:

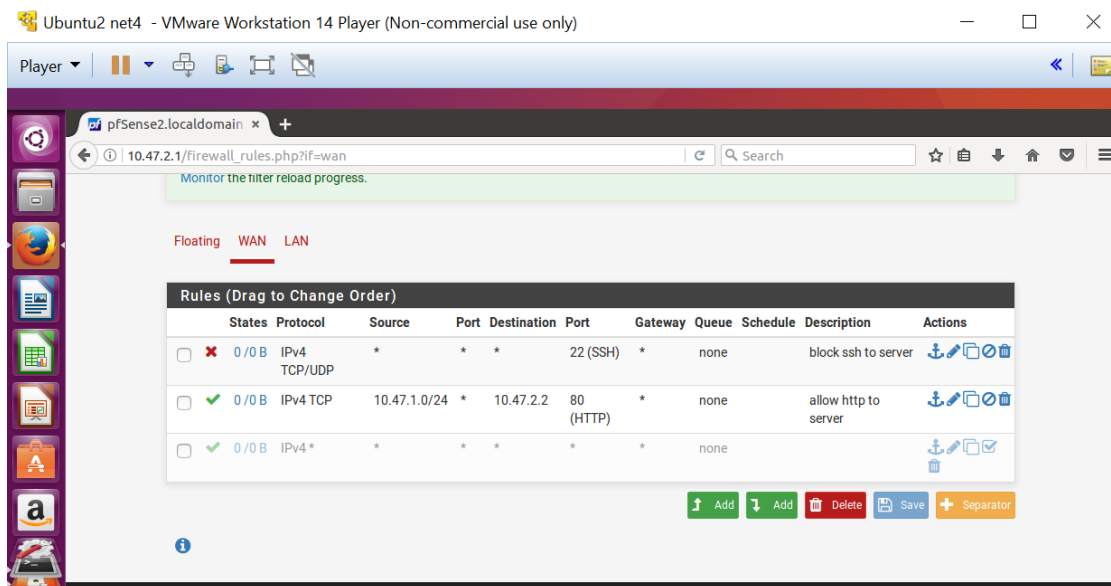
- Allows any clients/machines from the LAN to connect to 10.47.2.2 Port 80
- Disallows any clients/machines from the LAN to connect to 10.47.2.2 Port 22



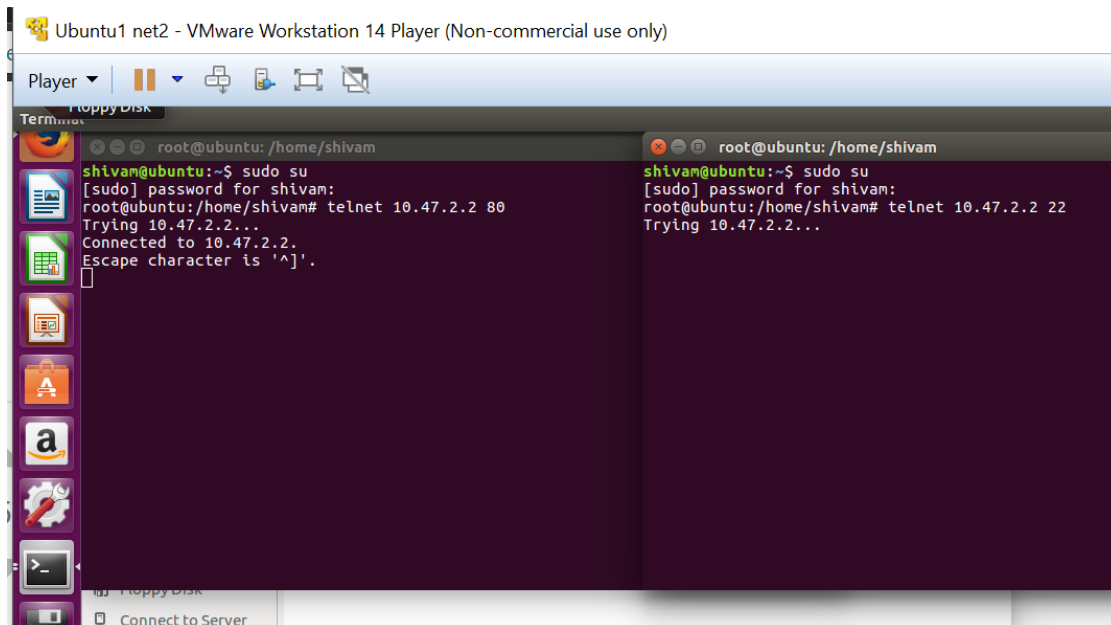
Screenshot 9: LAN Configurations on pfsense1

The following Wide Area Network (WAN) configurations were established for Pfsense2:

- Allows any clients/machines from the WAN to connect to 10.47.2.2 Port 80
- Disallows any clients/machines from the WAN to connect to 10.47.2.2 Port 22

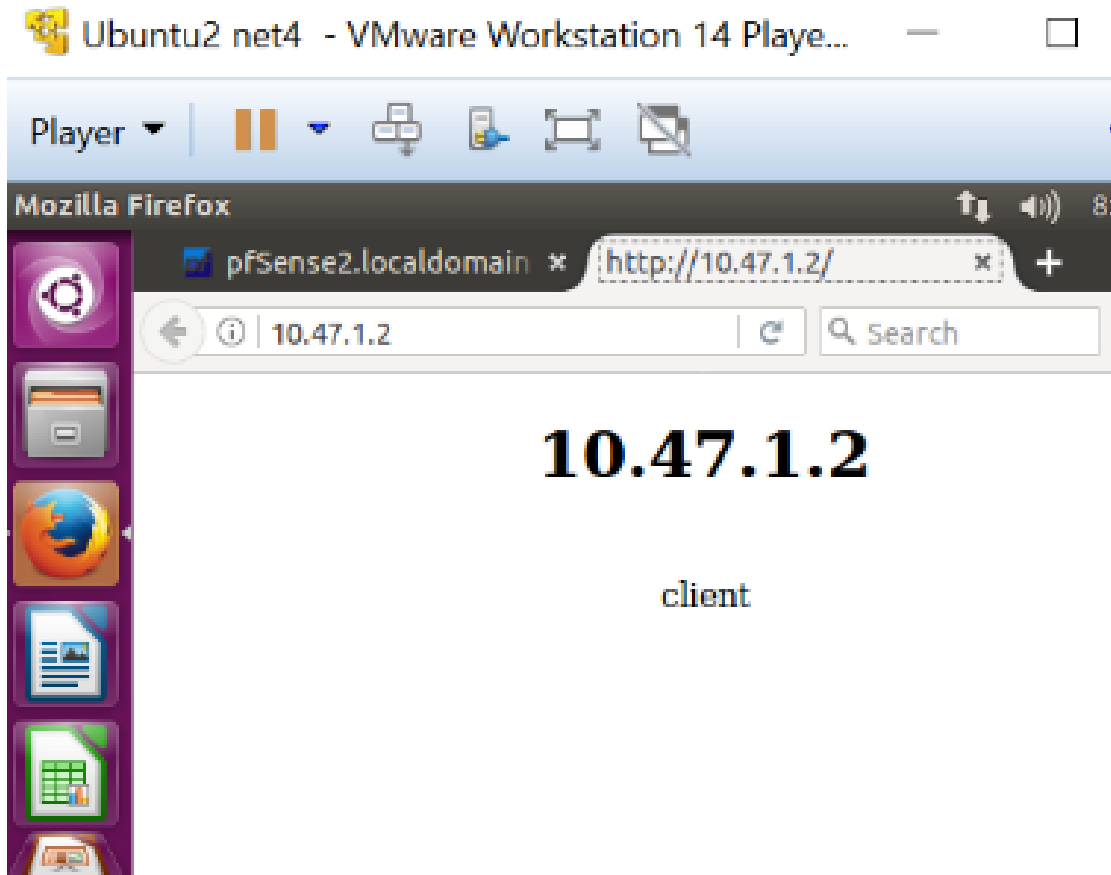


Screenshot 10: WAN Configurations on pfsense2



Screenshot 11: Telnet Sessions

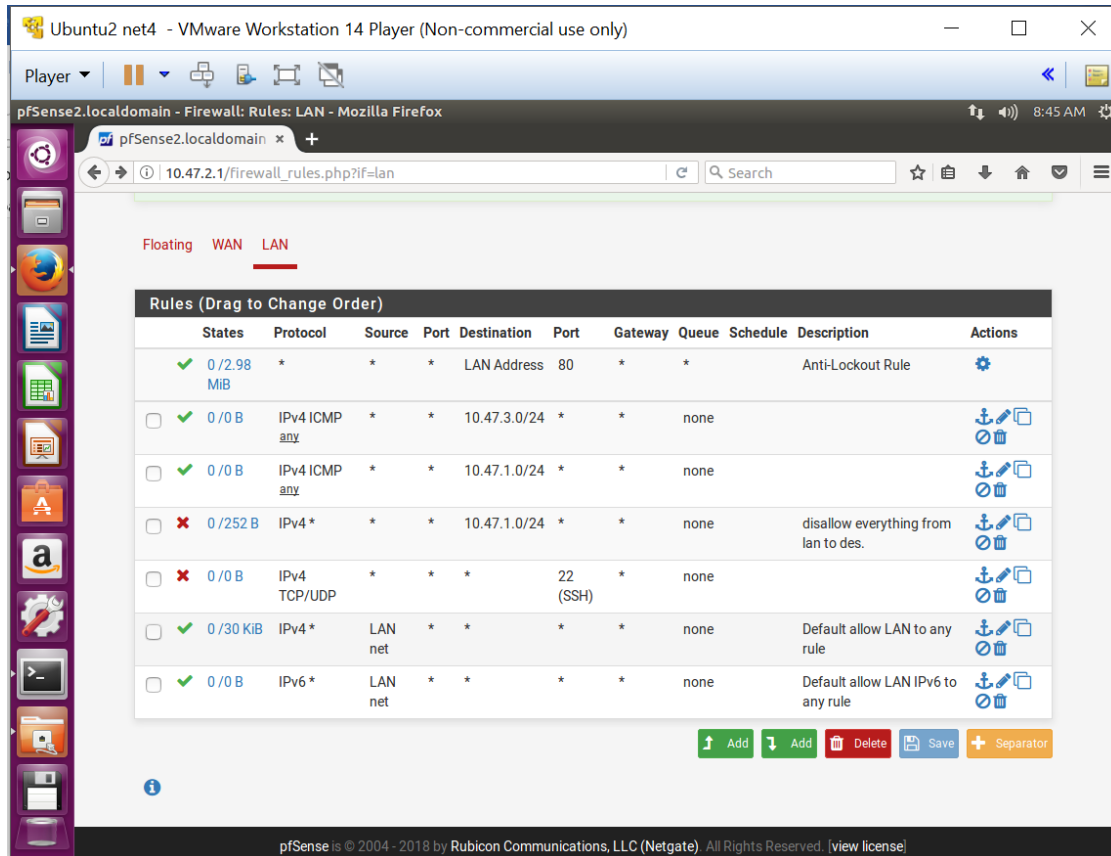
For demonstration, Apache2 and SSH was installed on the client machine.



Screenshot 12: Apache2 and SSH installed on client machine

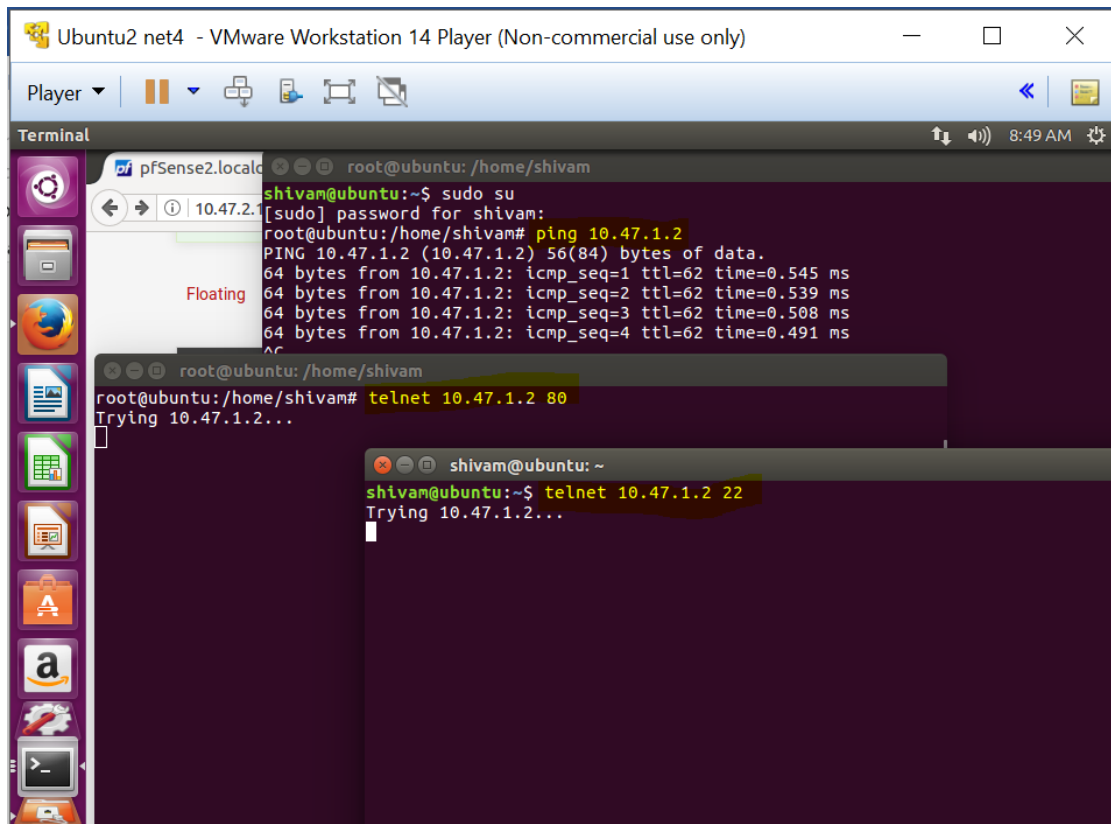
The following rule set was applied on Pfense2:

- The first rule is for the pfSense web interface, which is default.
- The second rule allows ICMP on the 10.47.3.0 network.
- The third rule allows ICMP on the 10.47.1.0 network.
- The fourth rule will disallow all other protocols



Screenshot 13: Rule set for Pfense2

The screenshot below illustrates that other than the ping command, no further access can be obtained.



Screenshot 14: http and ssh disallowed

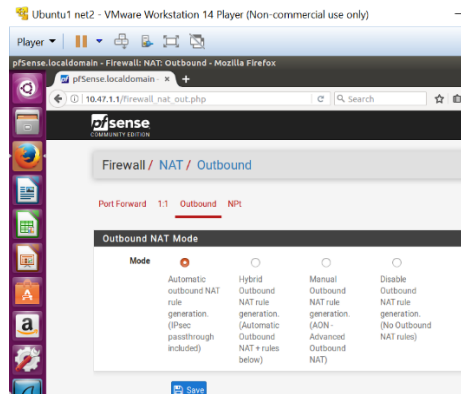
Task 3 – Basic Network Address Translation (NAT) Configuration:

NAT translates private addresses of LAN to external WAN Address.

For both pfsense NAT is set to Automatic Outbound NAT rule. Which translating our lan addresses to wan which are 10.47.3.10 and 10.47.3.20.

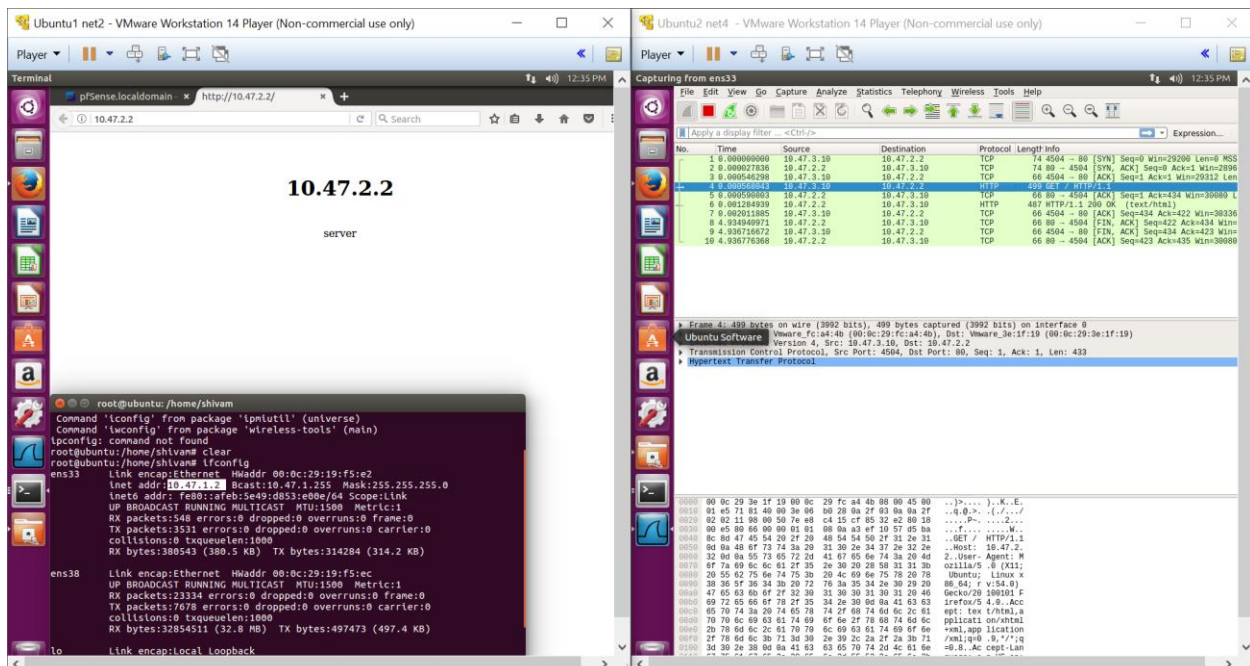
But still we are communicating with server with its private IP. Which is something that is not the case in real world because private addresses are not routable over WAN/public internet.

Screenshot 15: NAT auto outbound



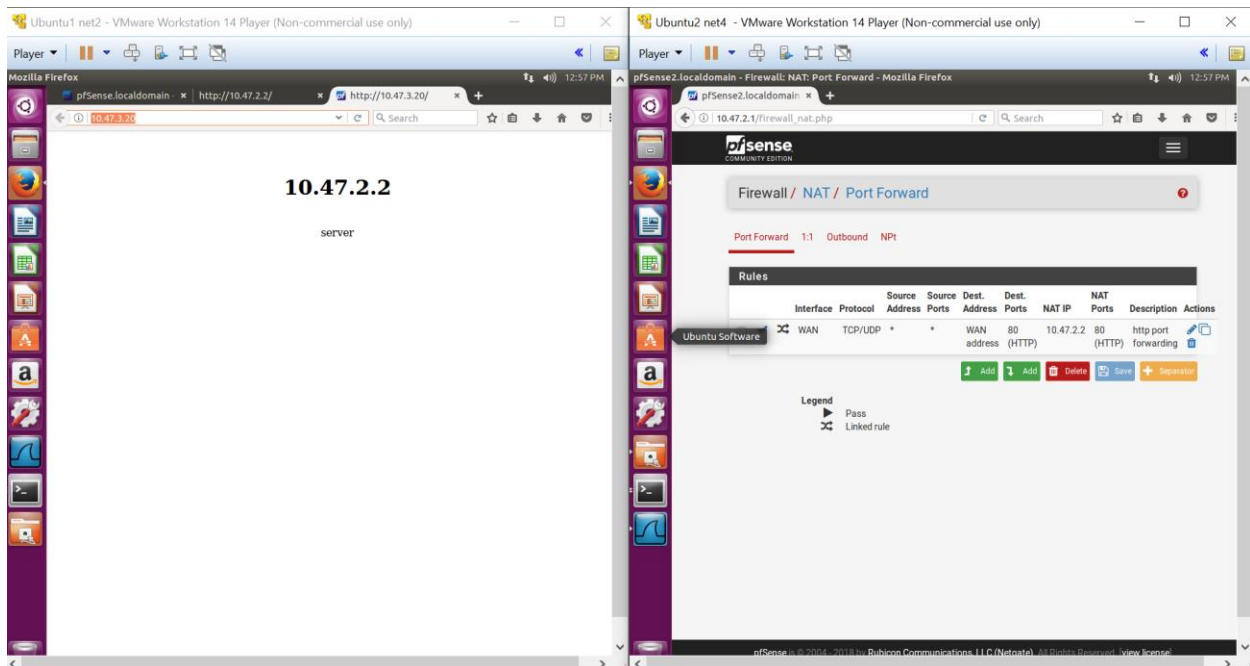
In wireshark source add is pfsense1's wan interface but the destination is server's private ip address but that's how we are accessing the server right now.

Screenshot 16: NAT on PFsense1 source is 10.47.3.10



We need to set up port forwarding on server side so that any request coming to pfsense2 port 80 can be forwarded to the server's port 80.

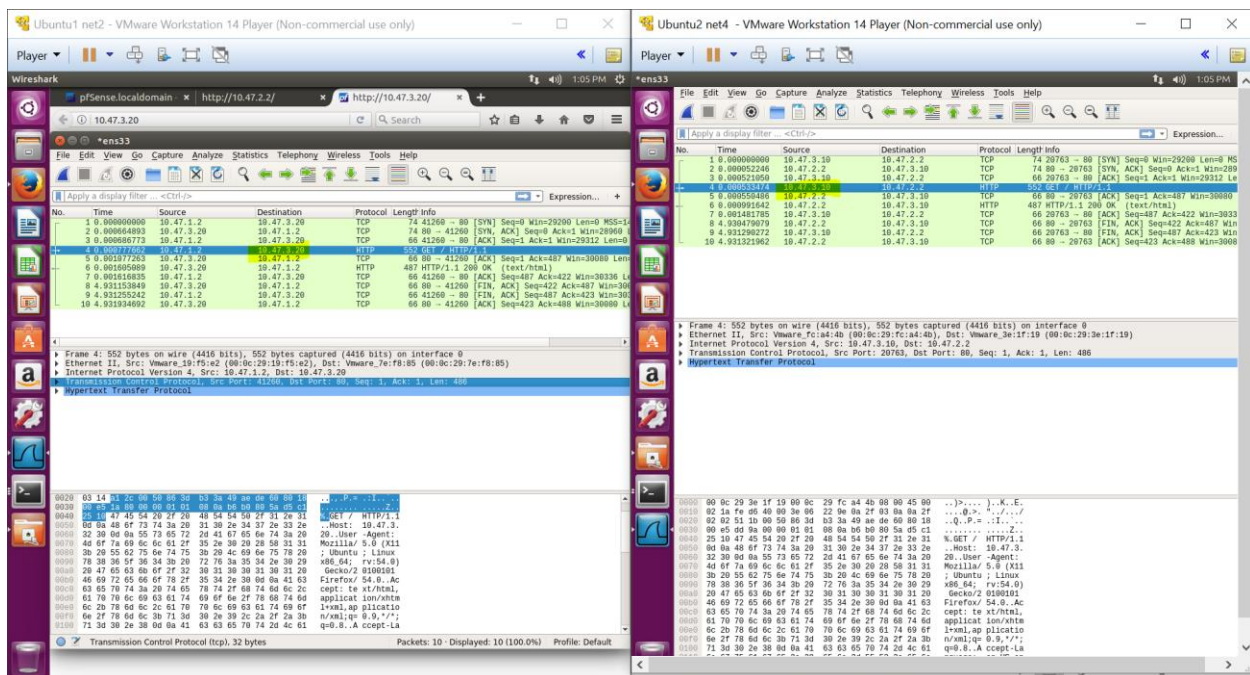
Screenshot 17:port-forwarding rule



As we can see we contacting 10.47.3.20 and its forwarding it to 10.47.2.2

Bellow is a screenshot showing Wireshark packet traces.

Screenshot 18:NAT working



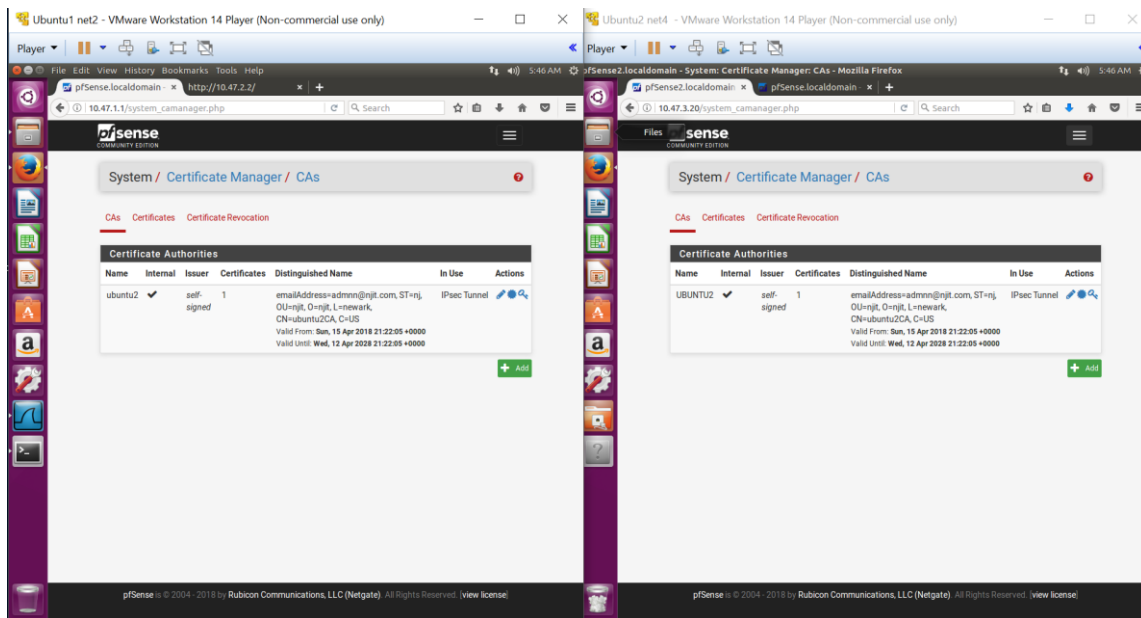
Task 4 – Basic Site-to-Site VPN Configuration:

For site to site secure VPN first we need to setup the certificates to use RSA instead we can use pre-shared key also but its not as secure as RSA.

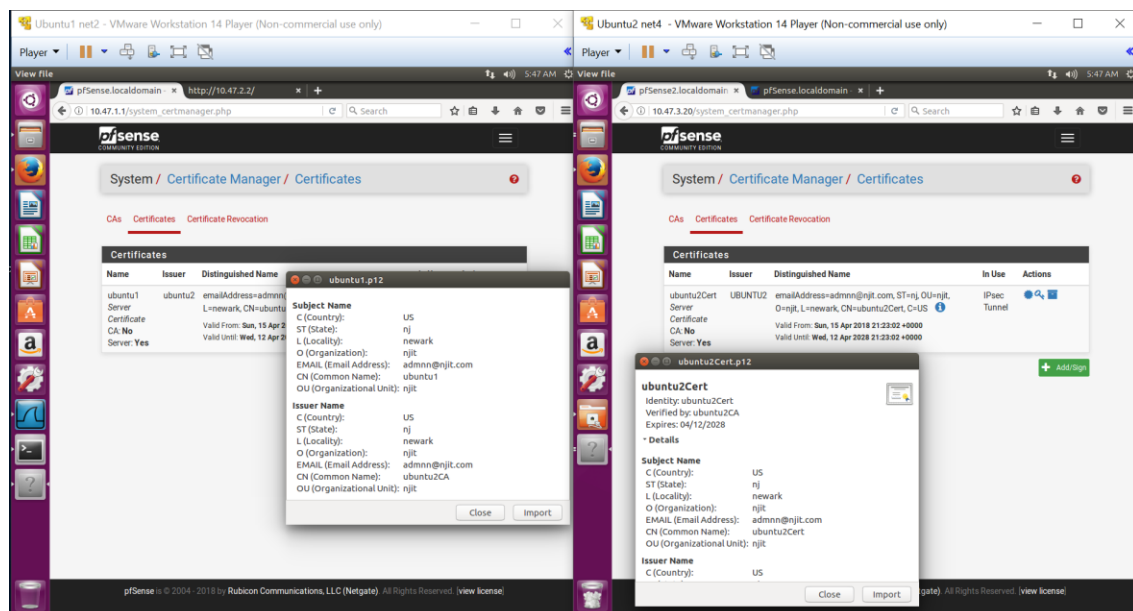
For mutual certificates we made rootCA in Pfsense2 and exported same rootCA to Pfsense1 so that both have same rootCA.

Then on both Pfsense we signed self-sign certificates with our rootCA. both have same rootCA so they will trust each other.

Screenshot 19: rootCA



Screenshot 20: Certificates on both pfsense signed with rootCA

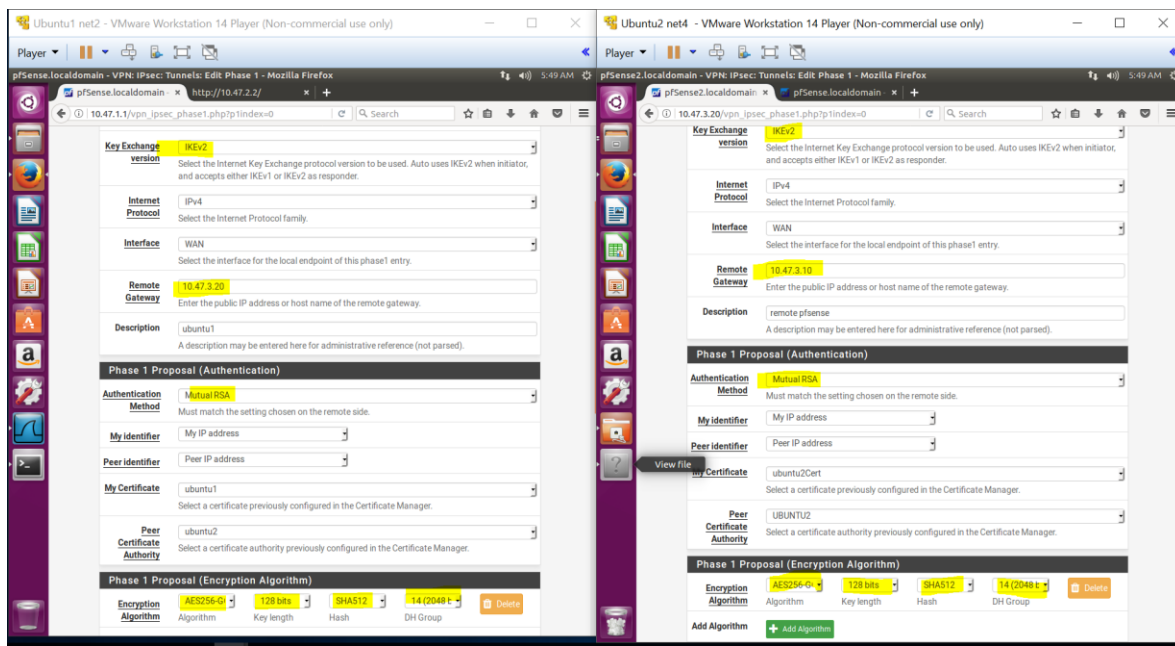


For VPN security association we have choose exactly same on both pfsense

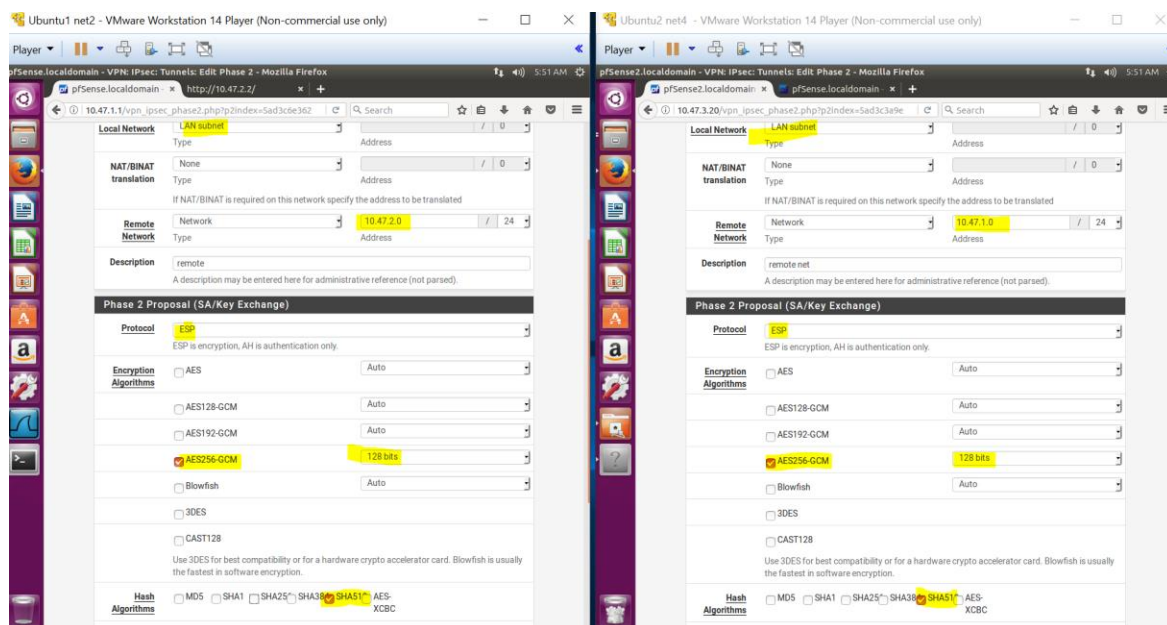
Key Exchange = IKEv2	Key Exchange = IKEv2
Remote getway 10.47.3.20	Remote getway 10.47.3.10
Aes256 128bit	Aes256 128bit
Sha512 DH Group 14	Sha512 DH Group 14

We can choose DHgroup 18 for even more secure connection but that may reduce the speed.

Screenshot 21: ipsec phase1 configurations

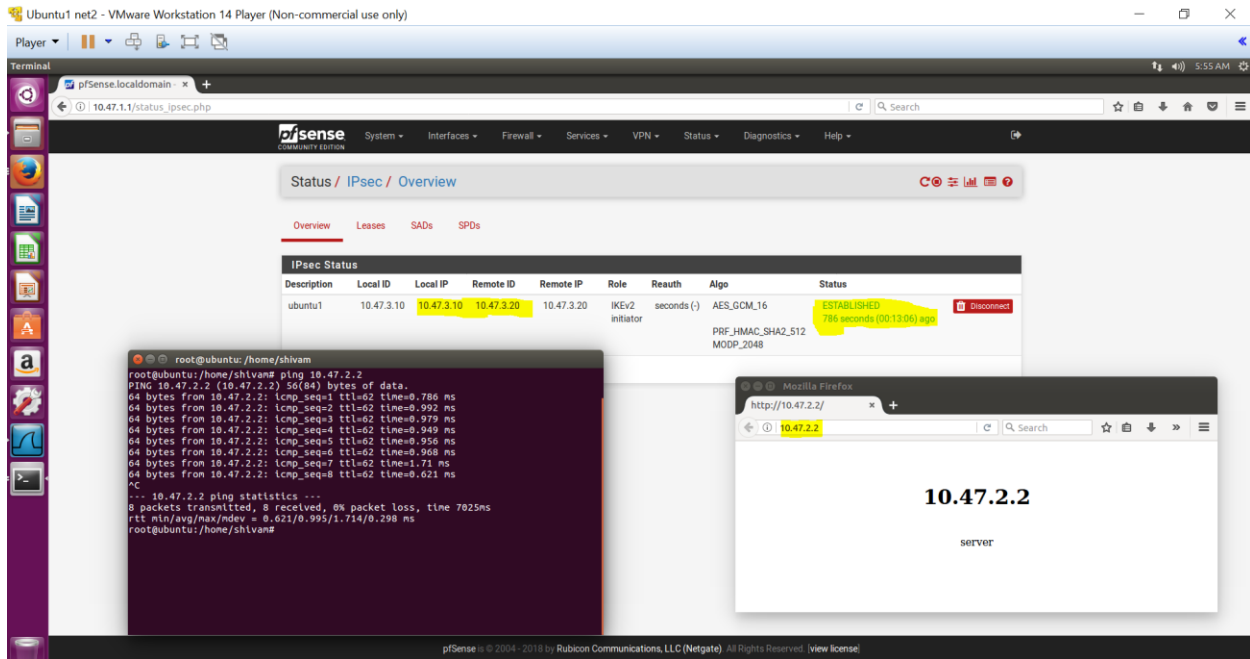


Screenshot 21: ipsec phase 2 configurations



For Phase2 we have selected ESP with AES 256 128 bit and hash algorithm SHA256

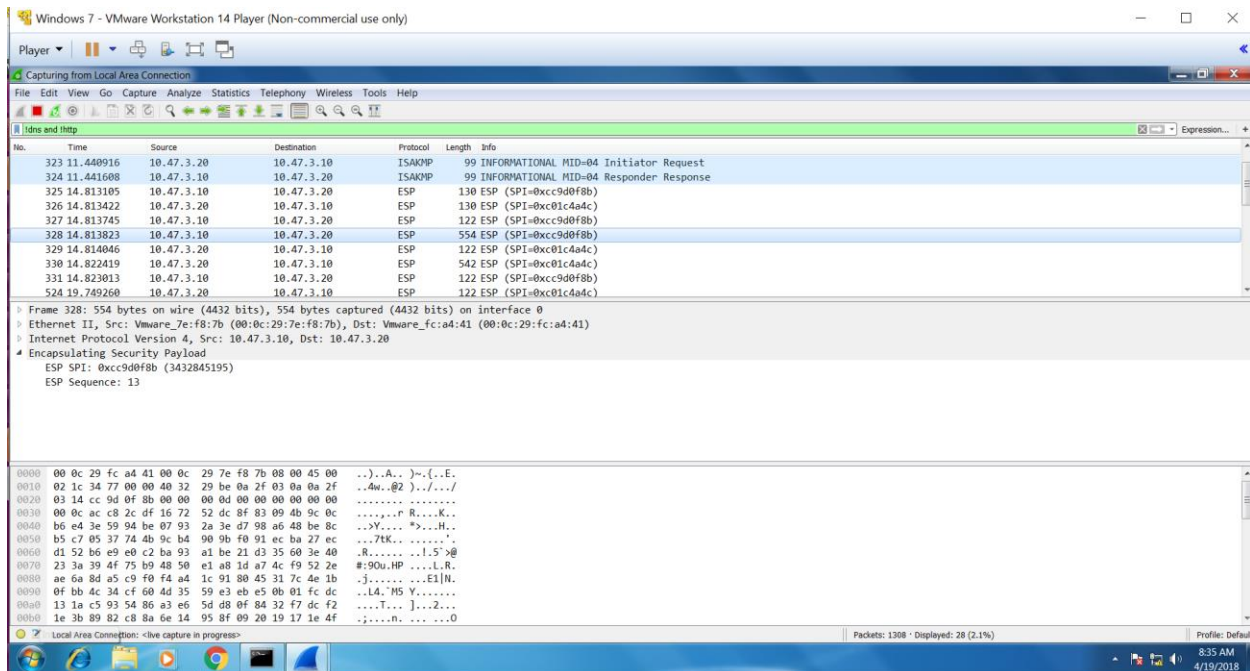
Screenshot 21: Screenshots below shows proof of vpn connection.



From client we are accessing server while VPN connection is being established

We have attached another windows7 machine for wireshark on wan 10.47.3.0 network to see VPN traffic.

Screenshot 22: see traffic from WAN



We can see the source and destination which are pfsense wan interfaces but nothing else all packets are encrypted