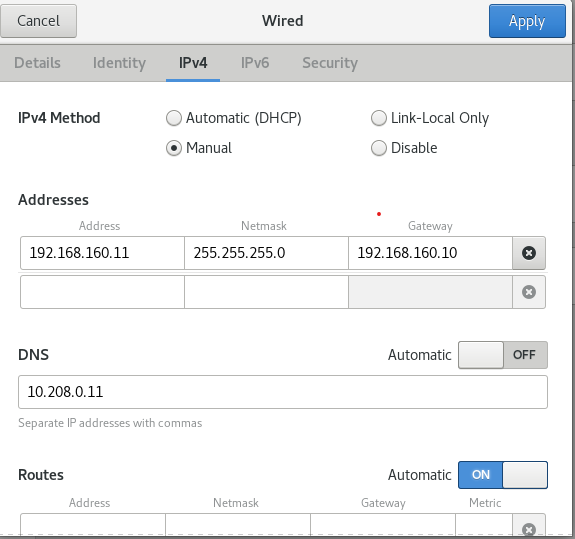
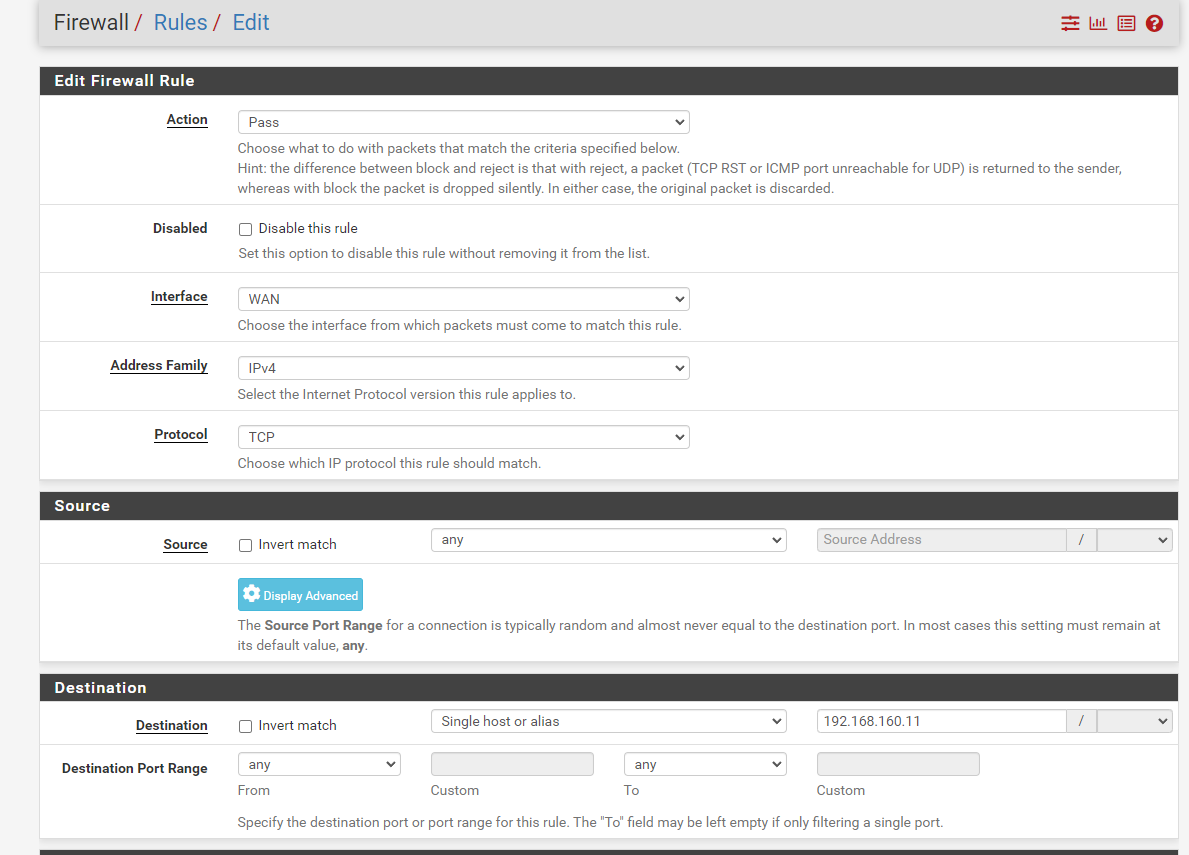
**Question.4) Configure SNORT to detect outgoing SSH requests**

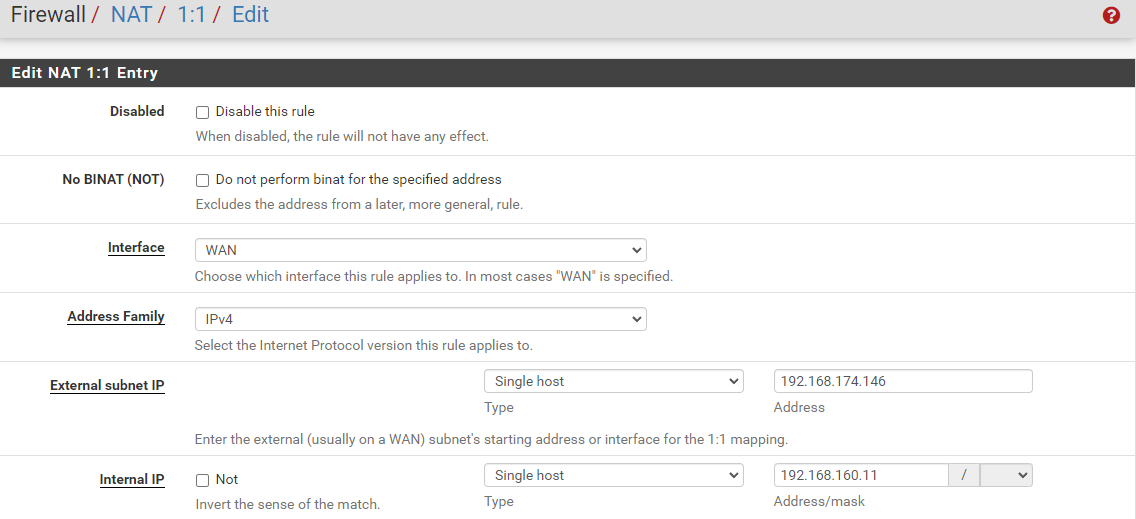
**Answer:-**

****

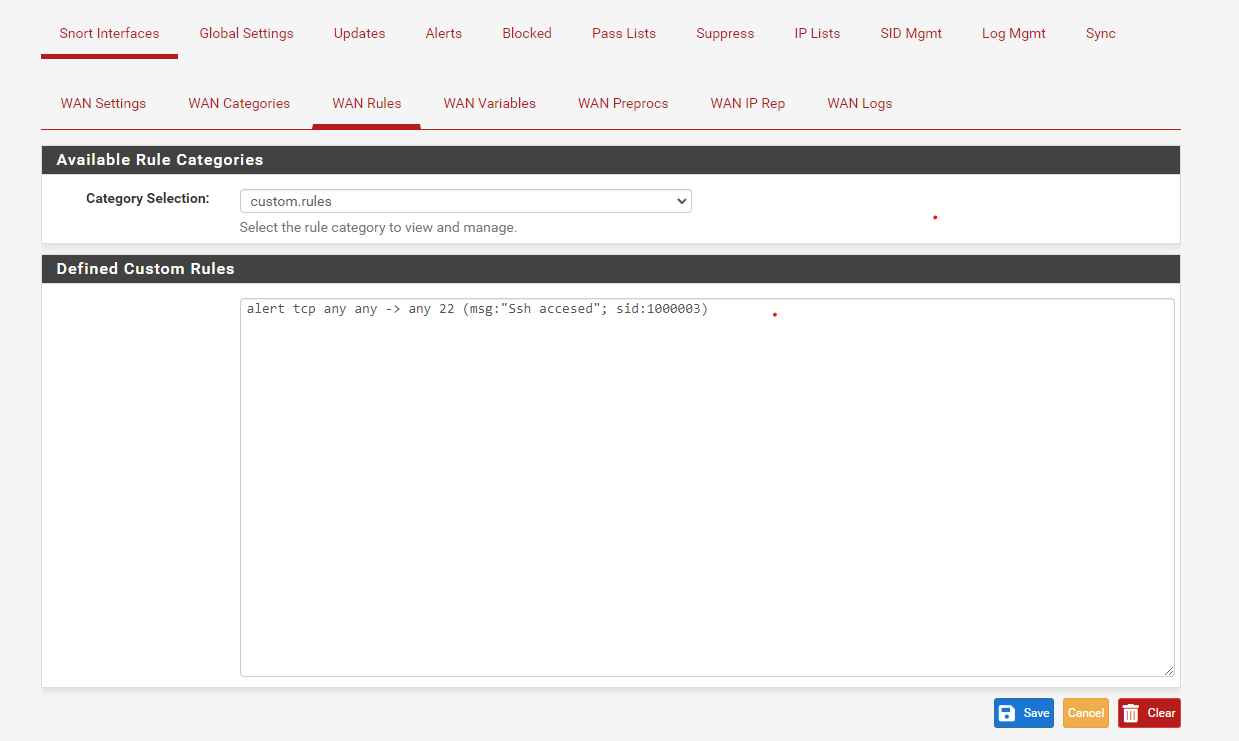
**Fig:-Client Machine setup**

****

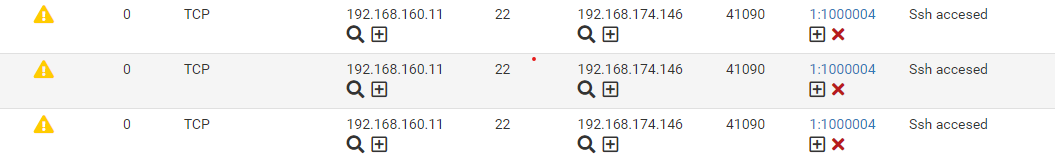
**Fig :- Adding Client machine ip in Destination (192.168.160.11)**

****

**Fig:- NAT 1:1 Mapping**

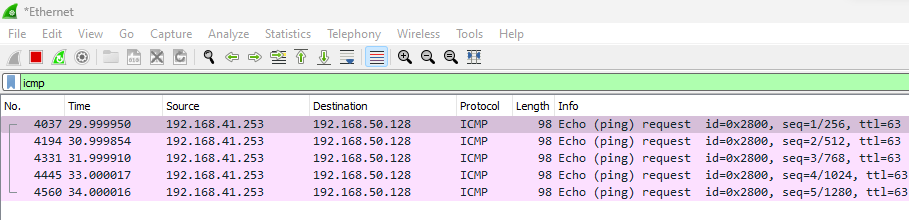
****

**Fig :- Applying Snort custom rule in WAN Rules**

****

**Fig:- Snort Alert received**

**Q.2) Set up Wireshark to capture icmp traffic from local machine**

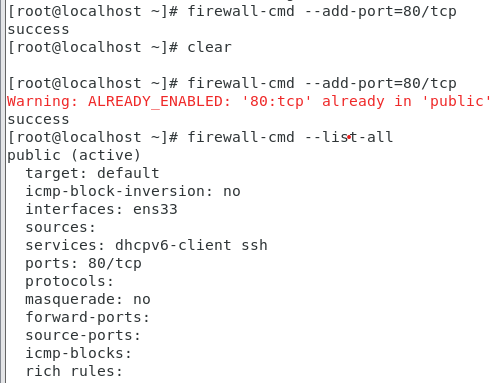
****

**Local Machine ip :- 192.168.41.253**

**Destination machine ip:- 192.168.50.128**

**Q.1) Write a rule in firewalld**

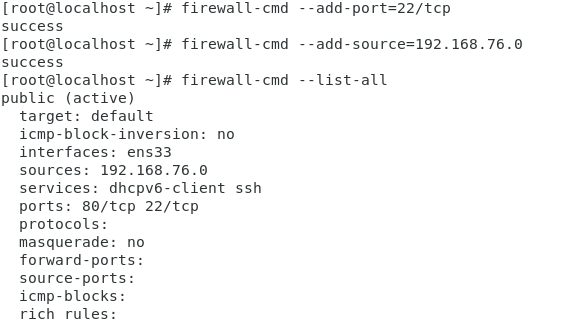
**b) Allow web server access from any ip address**

****

**c) allow ssh from 192.168.76.0/24**

**answer:-**

firewall-cmd --add-rich-rule='rule family=ipv4 source address=192.168.76.0/24 service name=ssh log prefix="SSH Access" level="notice" accept'

****

**a)Allow ICMP from any port**

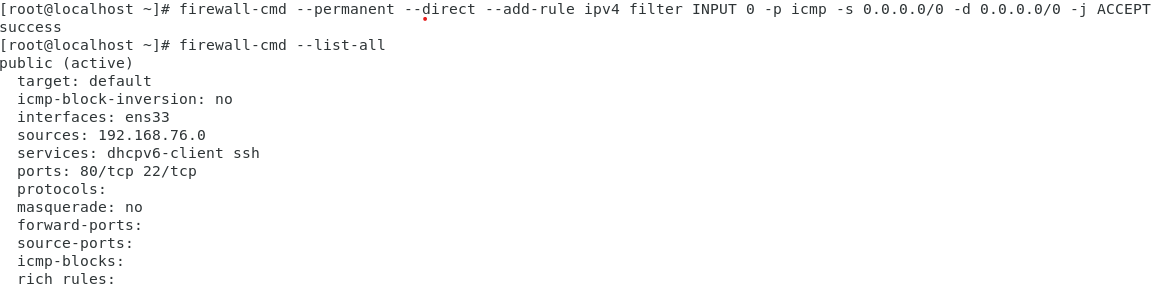
**answer:-**

firewall-cmd --permanent --add-icmp-block-inversion

firewall-cmd --permanent --add-icmp-block=echo-reply

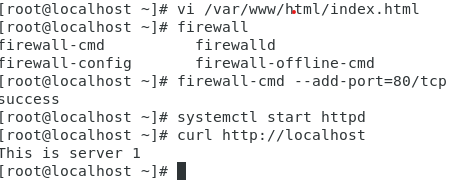
firewall-cmd --permanent --add-icmp-block=echo-request

firewall-cmd --reload

****

**Q3.) Set up reverse proxy using nginx**

**Creating server1**

****

**Creating server 2**

****

**Server1:-**

yum install httpd

vim /var/www/html/index.html

“This is server 1”

firewall-cmd --add-port=80/tcp

systemctl start httpd

curl http://localhost

vi /etc/hosts

ip a

vi /etc/hosts

reboot

systemctl start httpd

**Server2:-**

yum install httpd

vim /var/www/html/index.html

“This is server 2”

firewall-cmd --add-port=80/tcp

systemctl start httpd

curl http://localhost

vi /etc/hosts

ip a

vi /etc/hosts

reboot

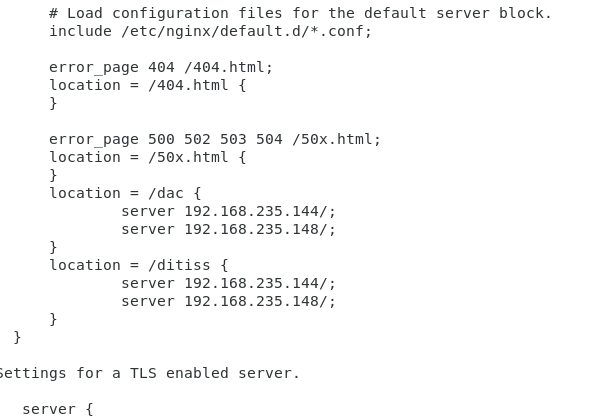
systemctl start httpd

**nginx-client:-**

**yum install nginx**

**vi /etc/nginx/nginx.conf**

**Making following changes in nginx.conf file, please refer following screenshot , I have added two locations /dac and /ditiss**

****

**Systemctl start nginx**

**Systemctl enable nginx**