1)

1. Write a set of iptables rules in the forward chain to allow RDP traffic from IP 196.1.113.4 only

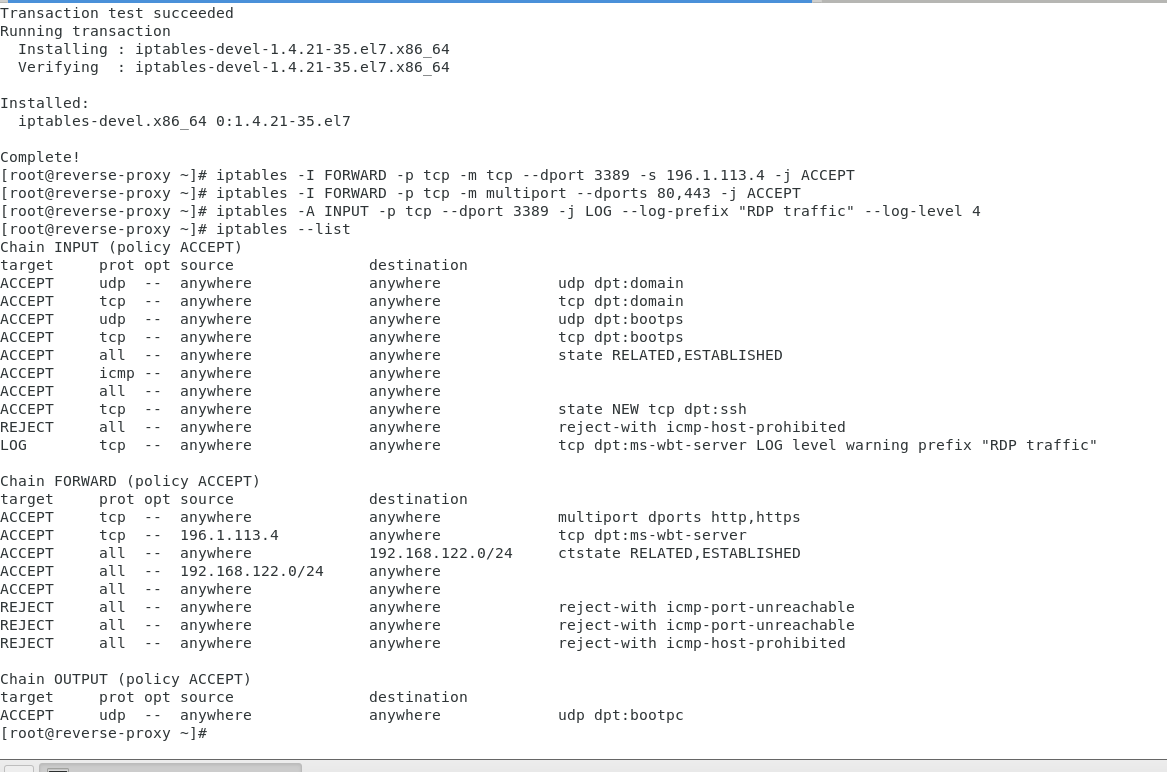
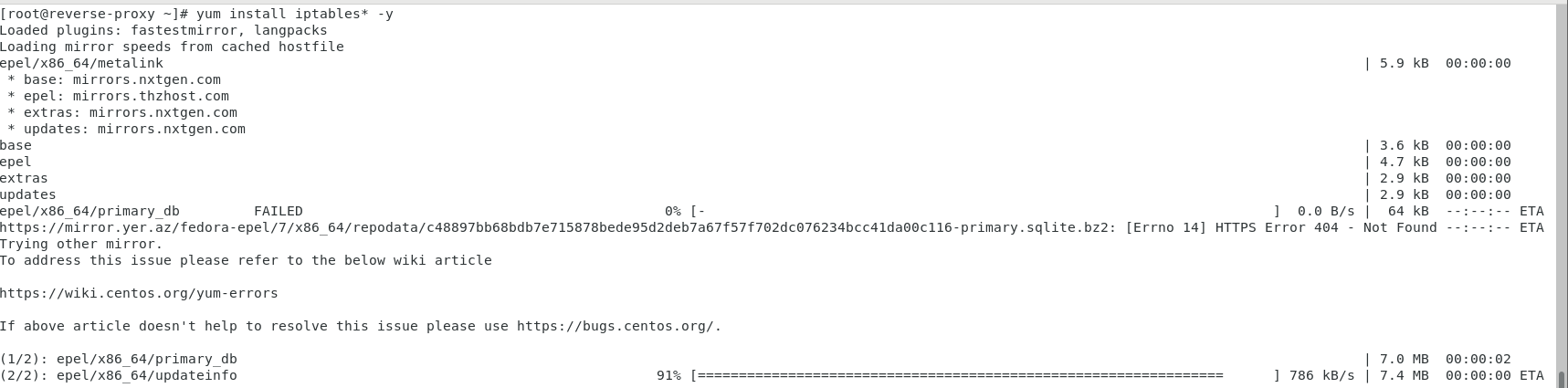
iptables -I FORWARD -p tcp -m tcp --dport 3389 -s 196.1.113.4 -j ACCEPT

1. Write a set of ip tables rules in the forward chain to allow incoming HTTP port 80 and HTTPS port 443 traffic to the web server

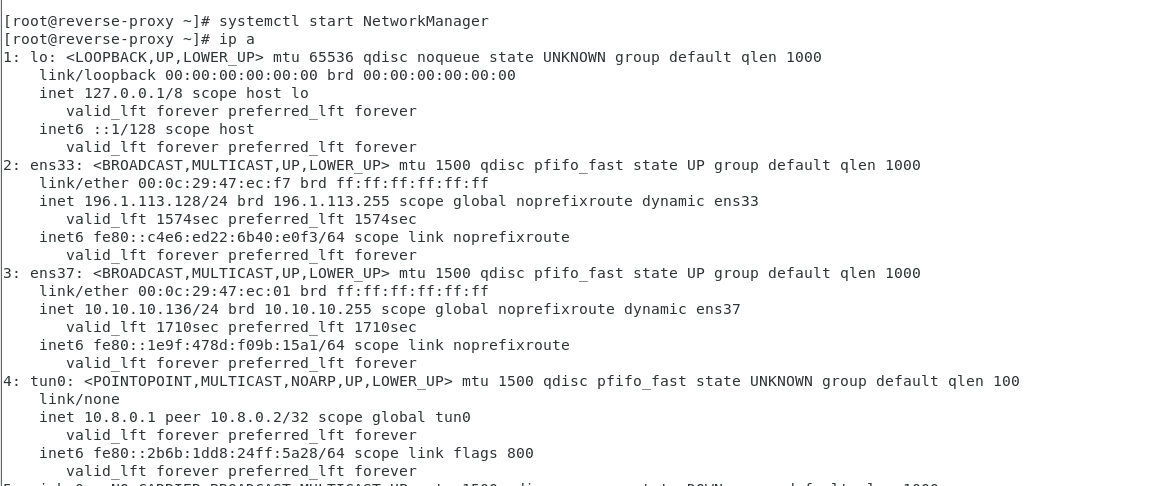
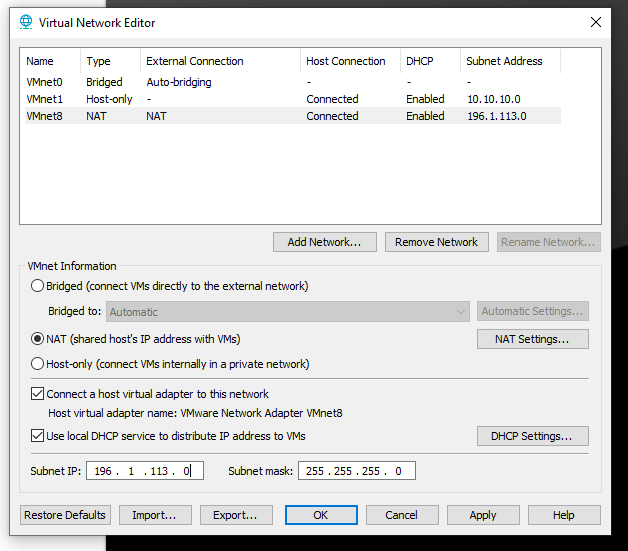
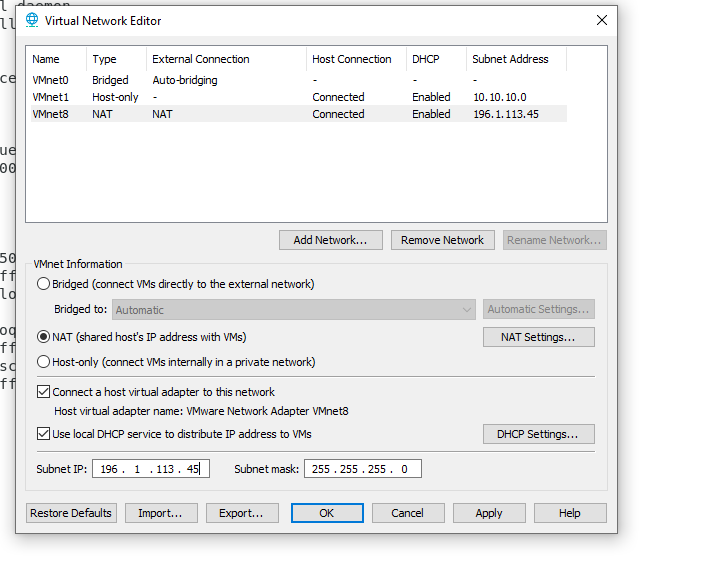
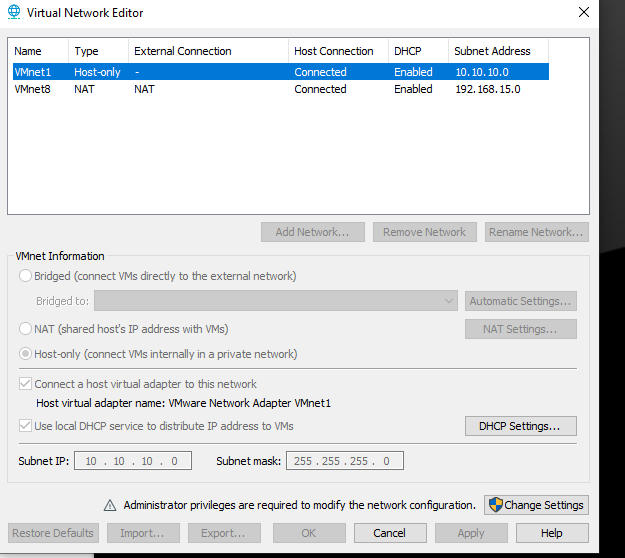
iptables -I FORWARD -p tcp -m multiport --dports 80,443 -j ACCEPT

1. Write a set of ip tables rules to log packets directed to port 3389 (RDP)

iptables -A INPUT -p tcp --dport 3389 -j LOG --log-prefix "RDP traffic" --log-level 4



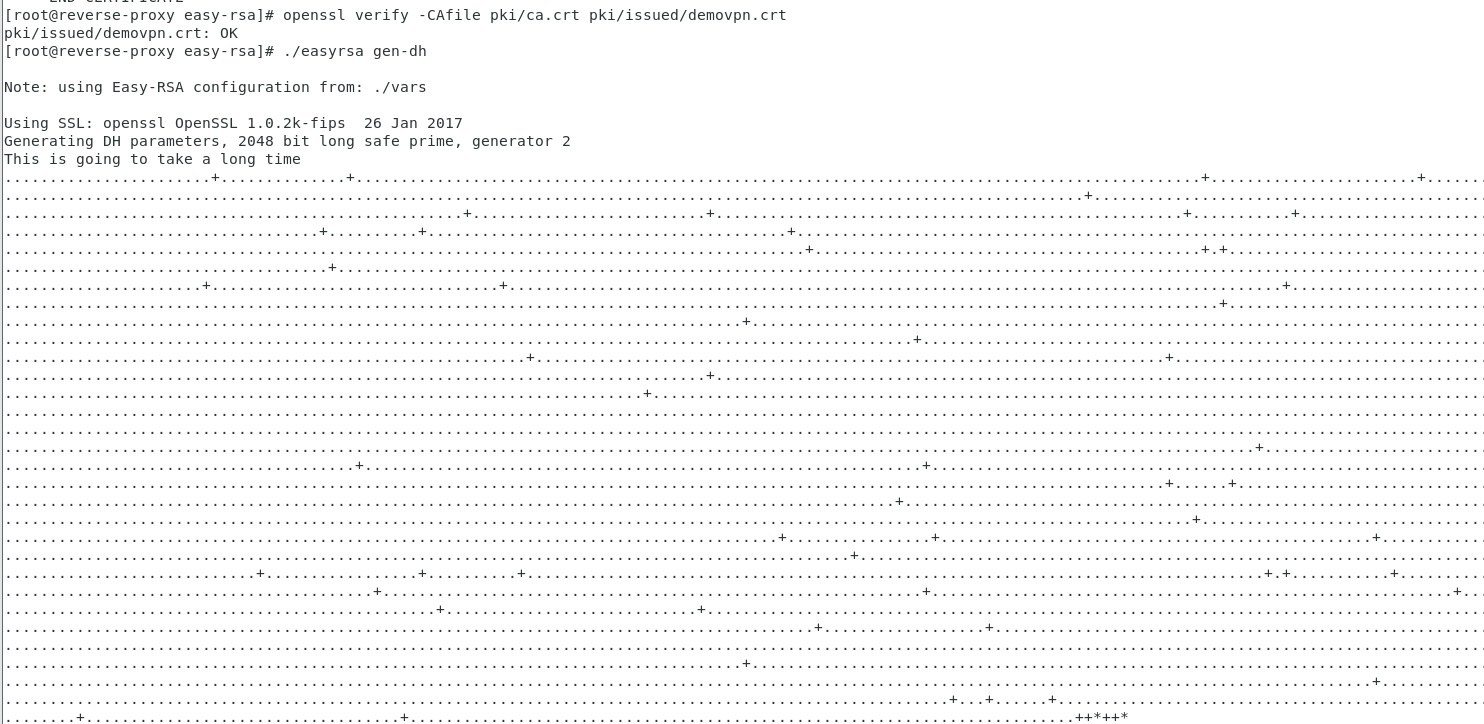
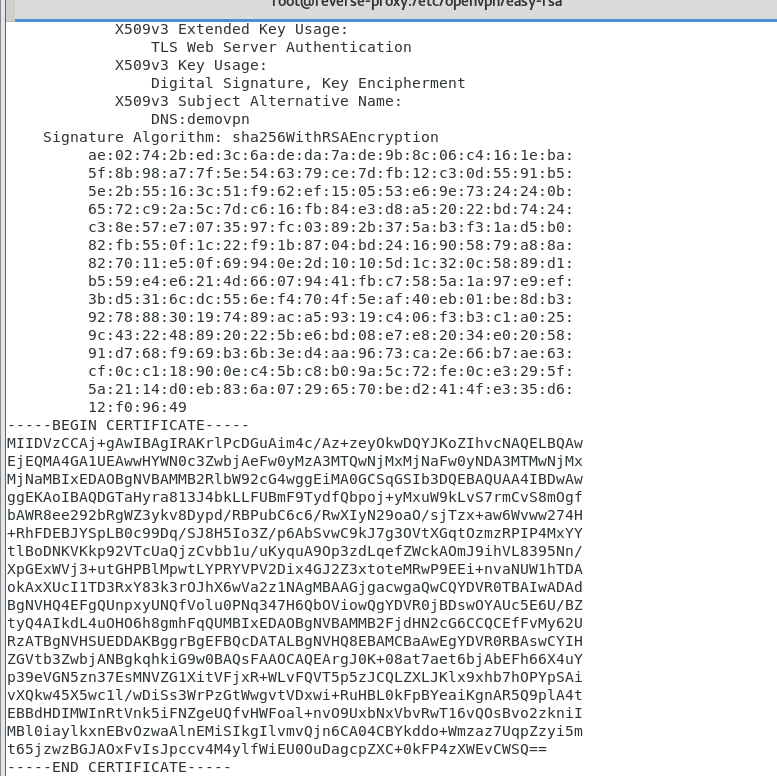
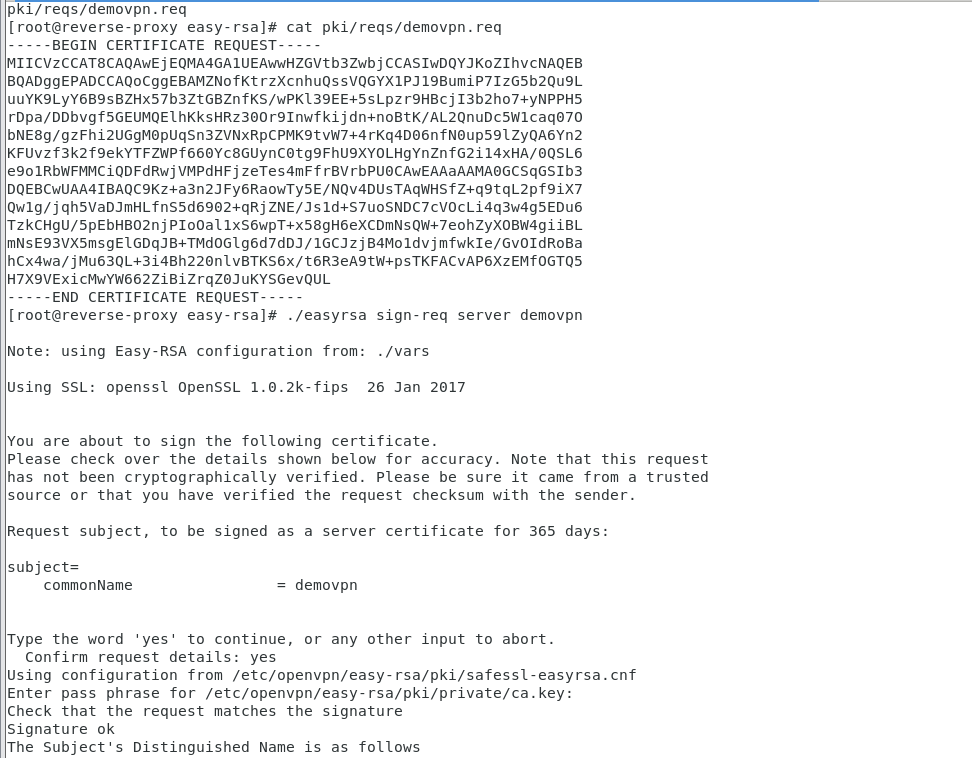
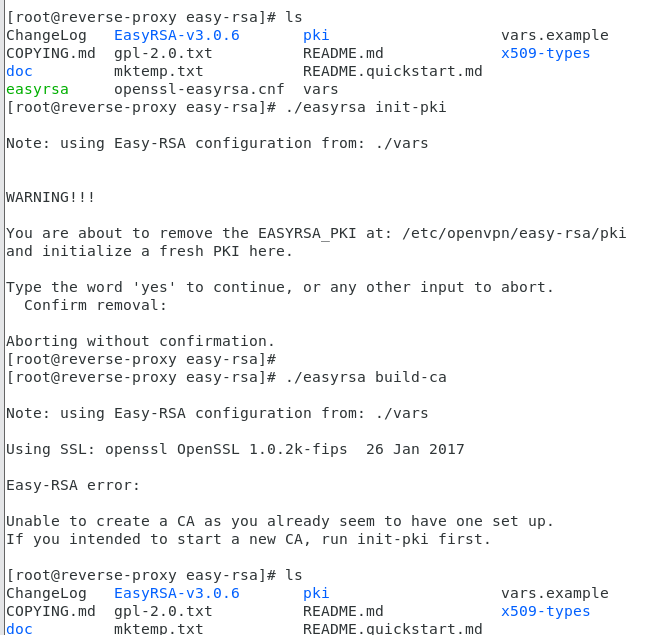
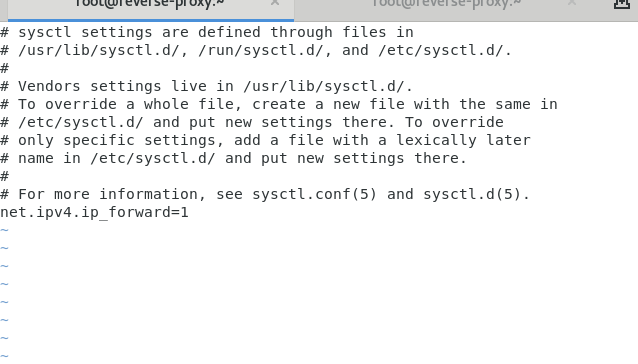
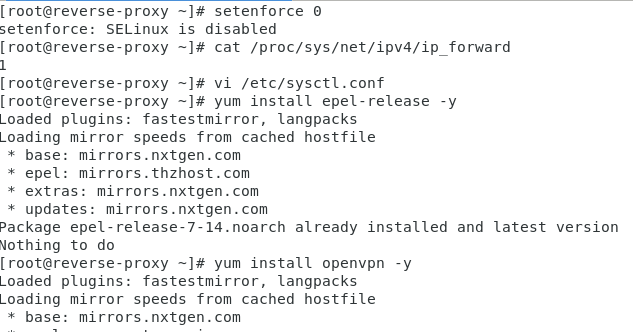
**Configuring the public IP 196.1.113.45**



2) configuring Two Linux Machine

Open vpn 🡪 NAT and host only

Client 🡪 host only



setenforce 0

cat /proc/sys/net/ipv4/ip\_forward

vi /etc/sysctl.conf

cat /proc/sys/net/ipv4/ip\_forward

yum install openvpn -y

cd /etc/openvpn/

wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz

ls

tar -xvzf EasyRSA-unix-v3.0.6.tgz

mv EasyRSA-v3.0.6 easy-rsa

ls

cd easy-rsa/

vim vars

ls

./easyrsa init-pki

./easyrsa init-pki

./easyrsa build-ca

ls pki

ls pki/private/

./easyrsa gen-req hpcsa1 nopass

ls pki/reqs/hpcsa1.req

cat pki/reqs/hpcsa1.req

./easyrsa sign-req server demovpn

./easyrsa sign-req server hpcsa1

cat pki/issued/hpcsa1.crt

./easyrsa gen-dh

cp pki/ca.crt /etc/openvpn/server/

cp pki/dh.pem /etc/openvpn/server/

cp pki/private/hpcsa1.key /etc/openvpn/server/

cp pki/issued/hpcsa1.crt /etc/openvpn/server/

./easyrsa gen-req client nopass

./easyrsa sign-req client client

./easyrsa gen-req jerry nopass

cp pki/ca.crt /etc/openvpn/client/

ls /etc/openvpn/client/

cp pki/issued/client.crt /etc/openvpn/client/

cp pki/private/client.key /etc/openvpn/client/

ls /etc/openvpn/client/

vi /etc/openvpn/server/server.conf

systemctl start openvpn-server@reverse-proxy

vi /etc/openvpn/server/server.conf

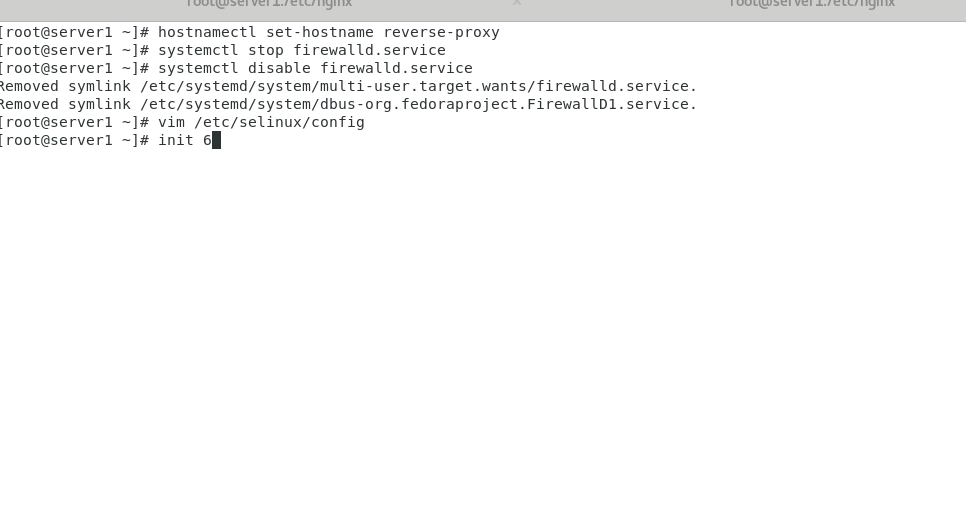
systemctl start openvpn-server@server

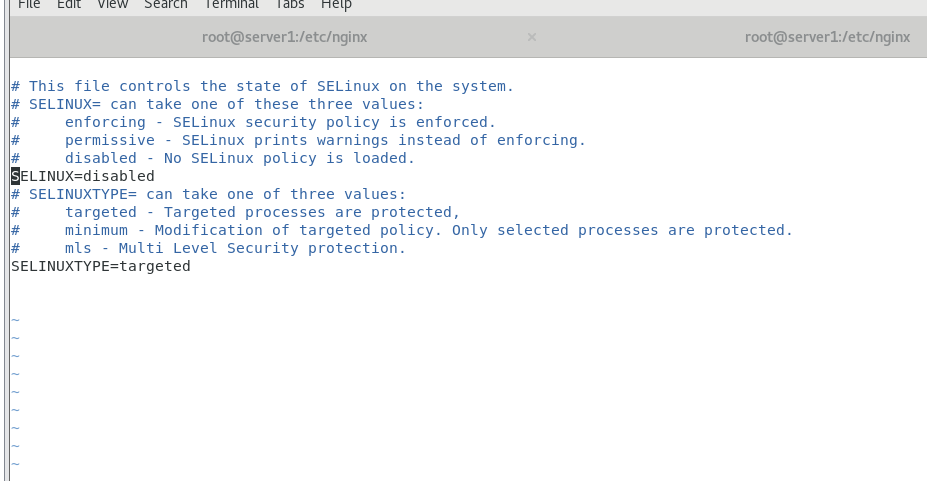
4) We take three Machine

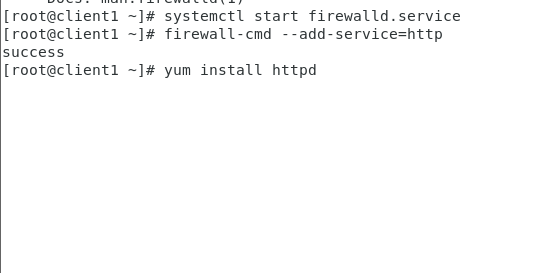
Reverse Proxy 🡪 Nat and Host only NAT ip – 196.1.113.128

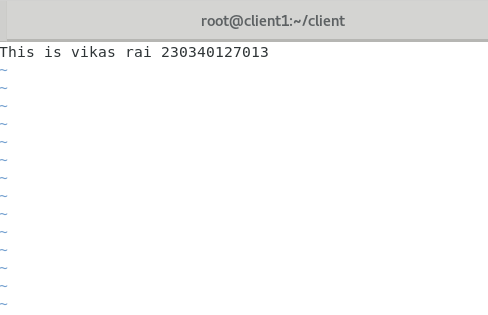
Client 🡪 host Only 10.10.10.137

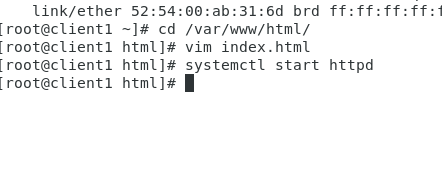
Window 🡪 host only 10.10.10.133 install iis manager 🡪 go to c drive inetpub 🡪 [www.root](http://www.root) 🡪 create html file (index.html)

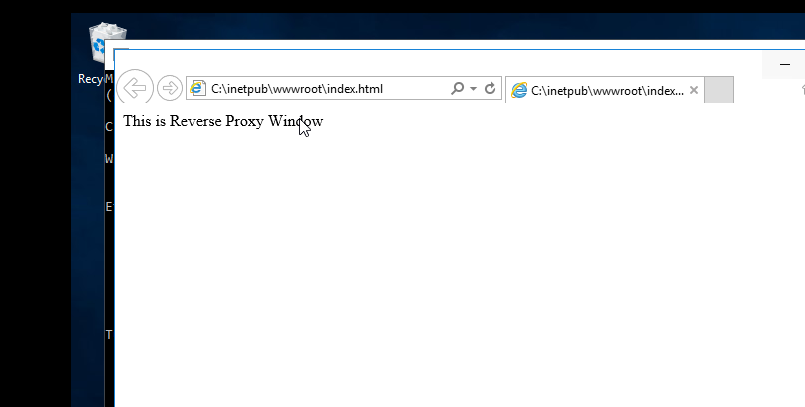


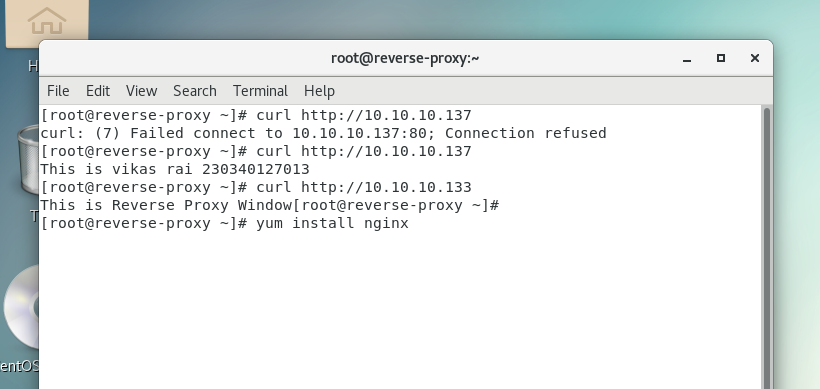




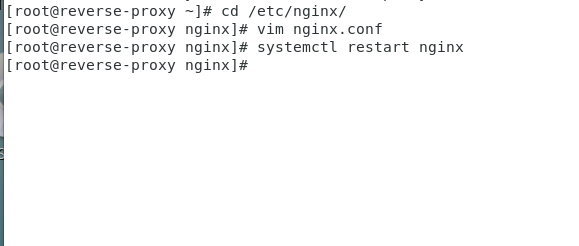






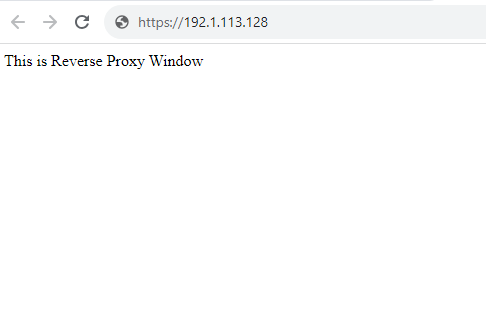
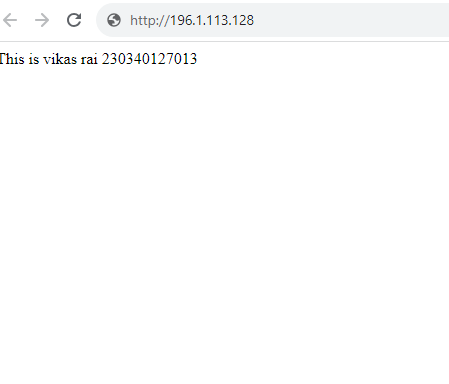






#systemctl restart nginx

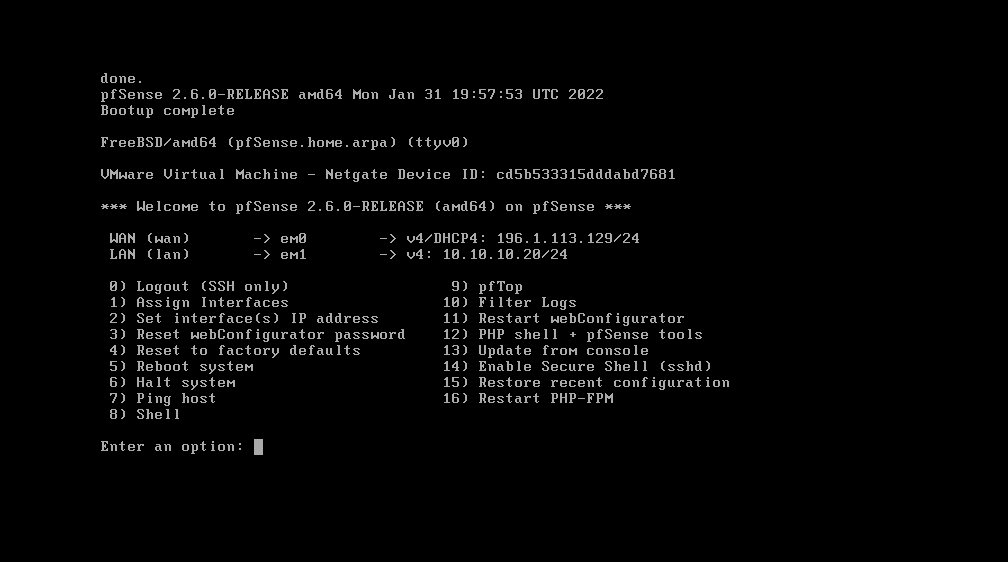
Output -



3)

Pfsense machine 🡪 NAT and host only

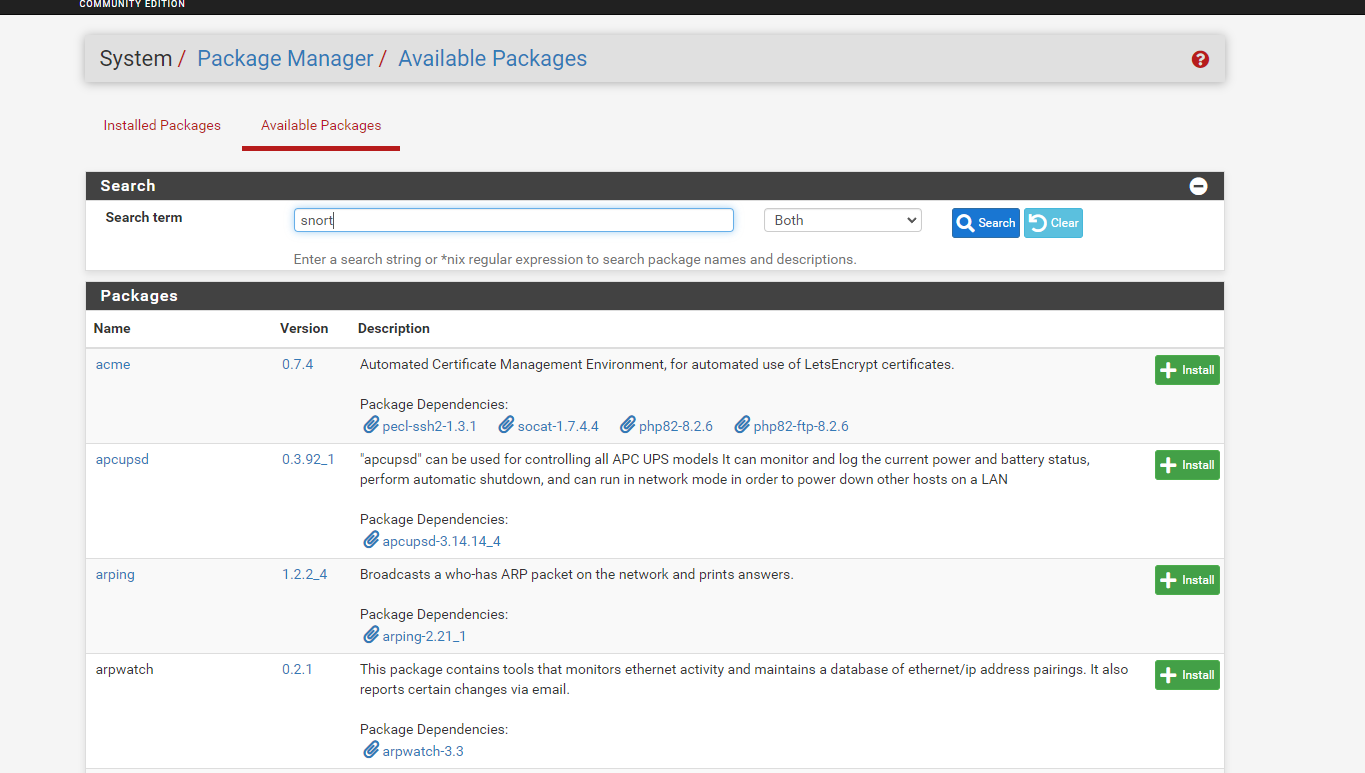
Centos machine 🡪 Bridge



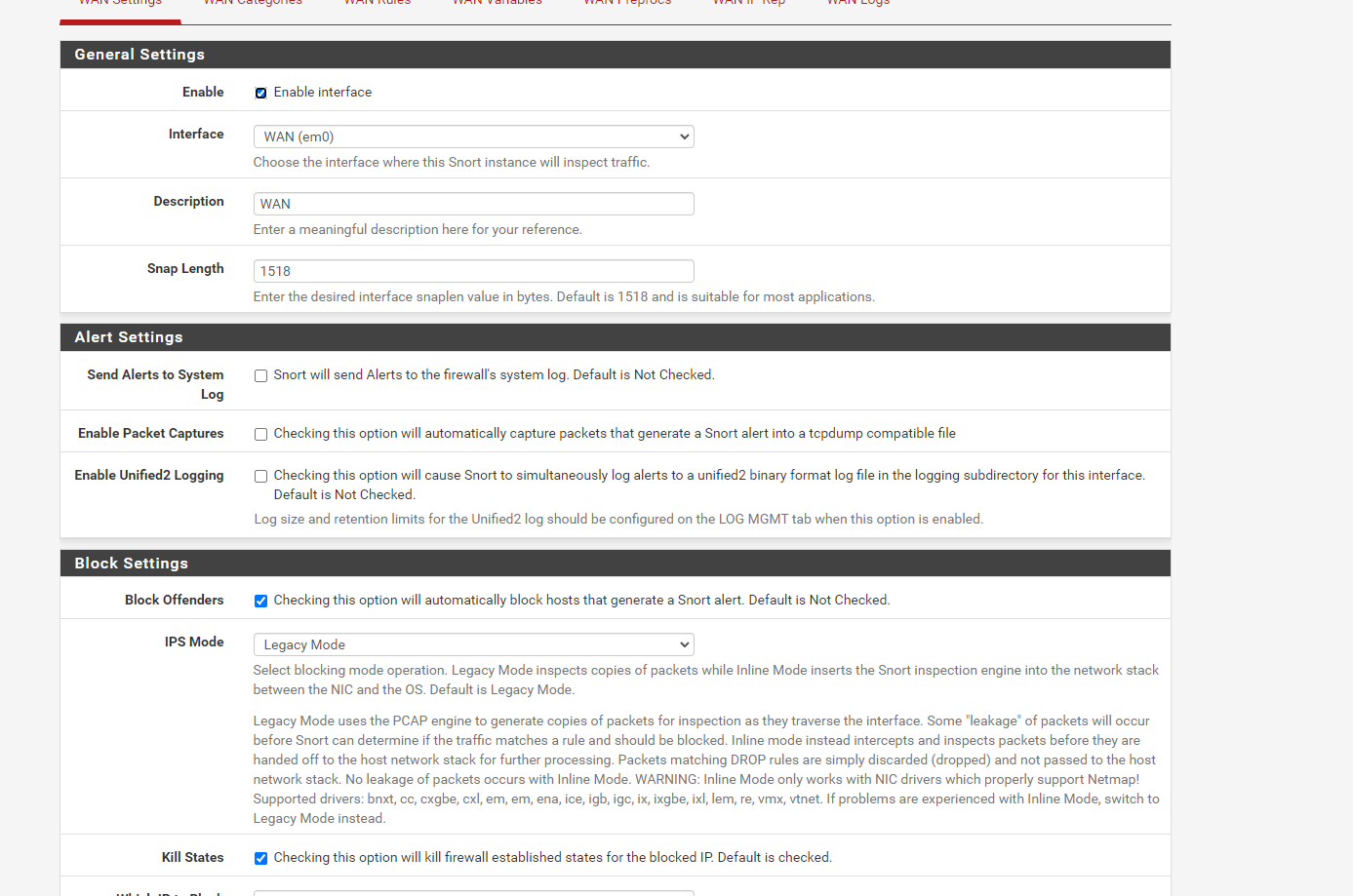
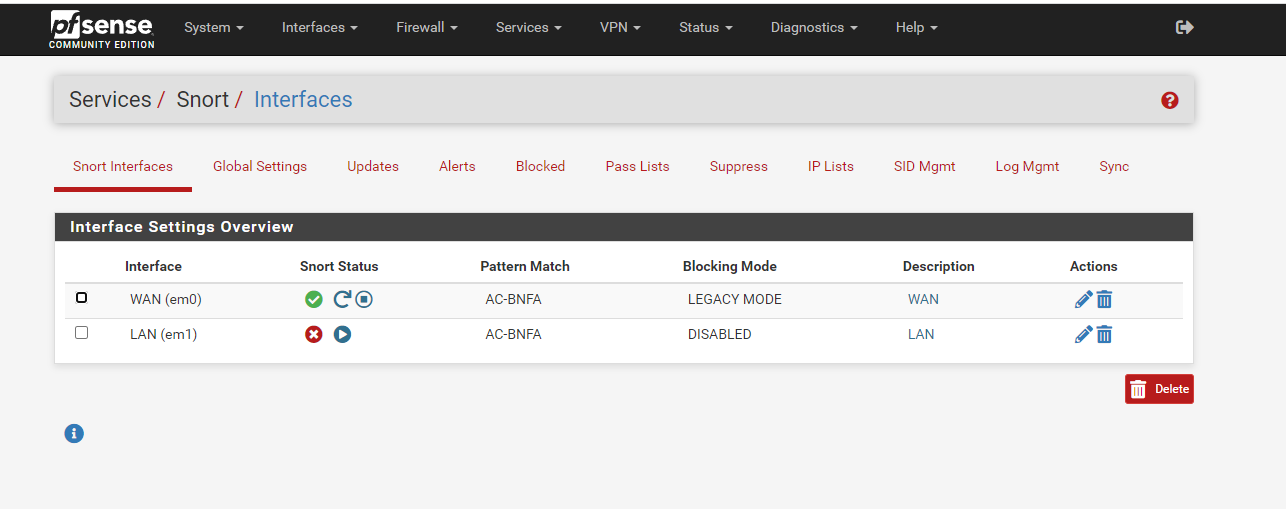
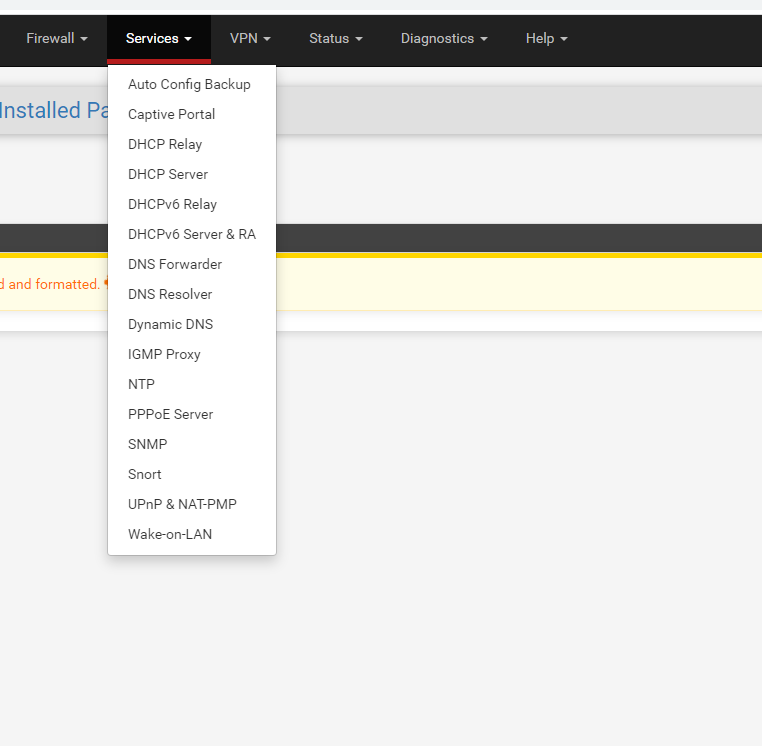
Login 🡪



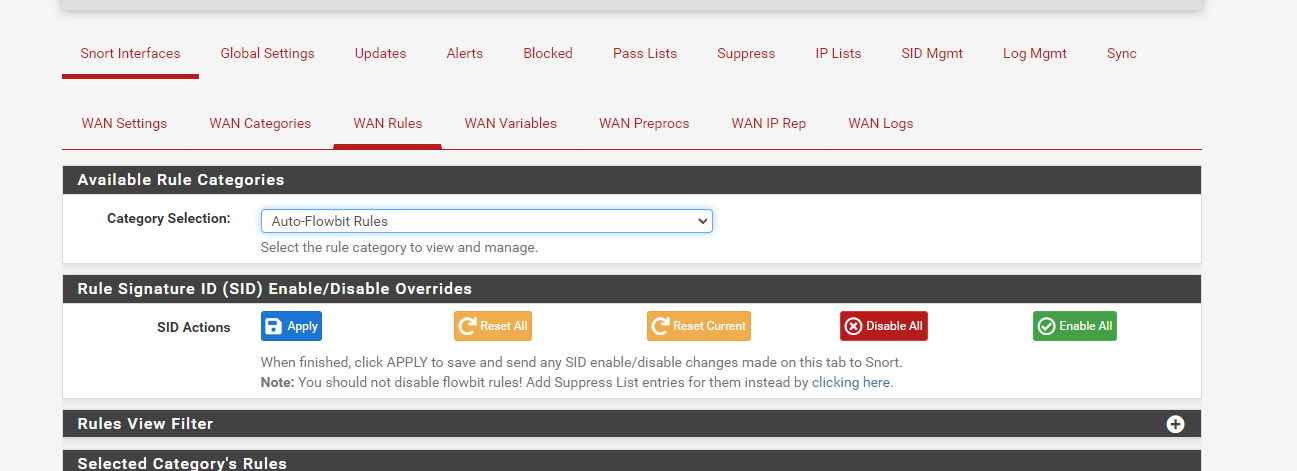
Install the Snort Packages



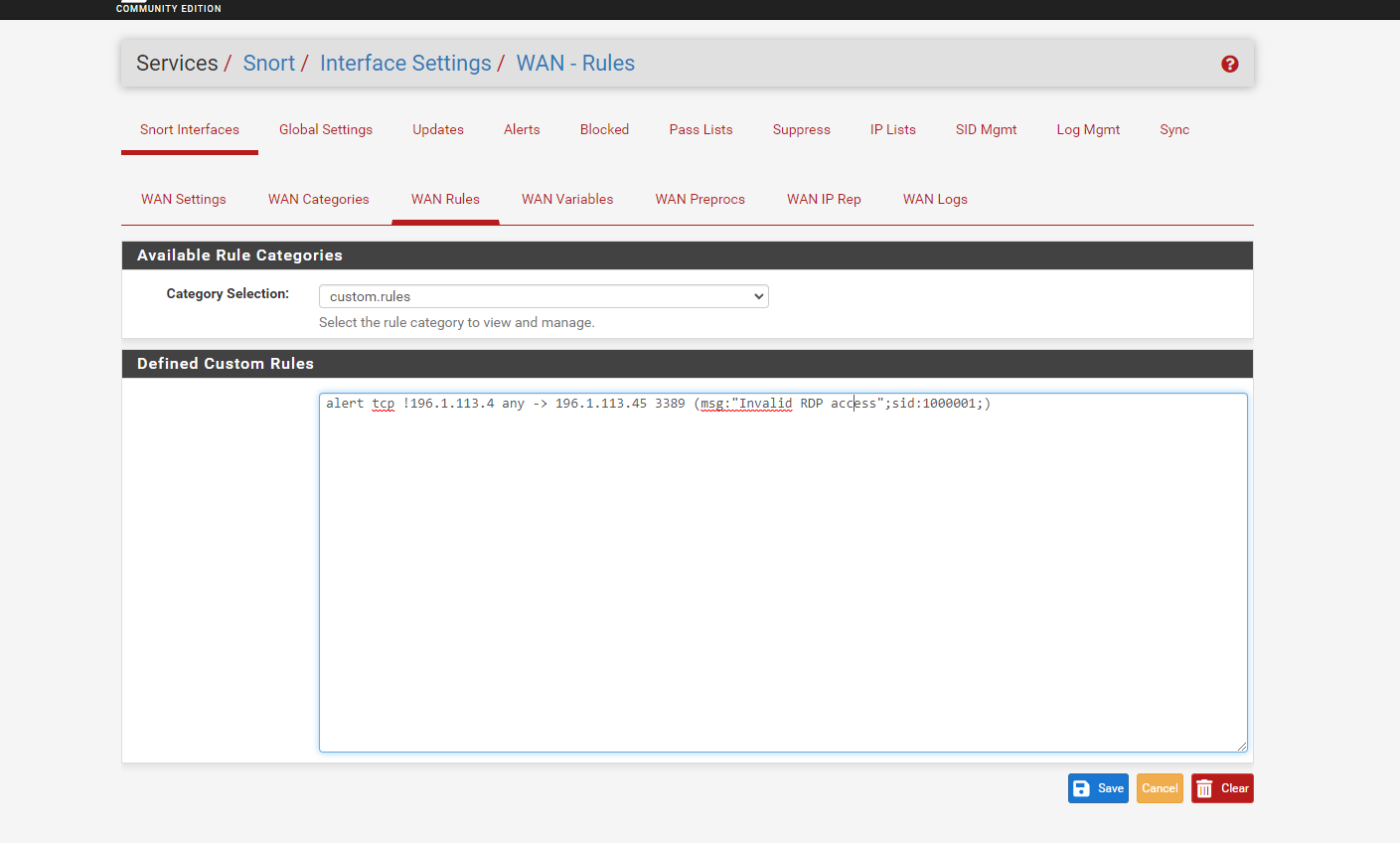
Go to the Services and then go to snort



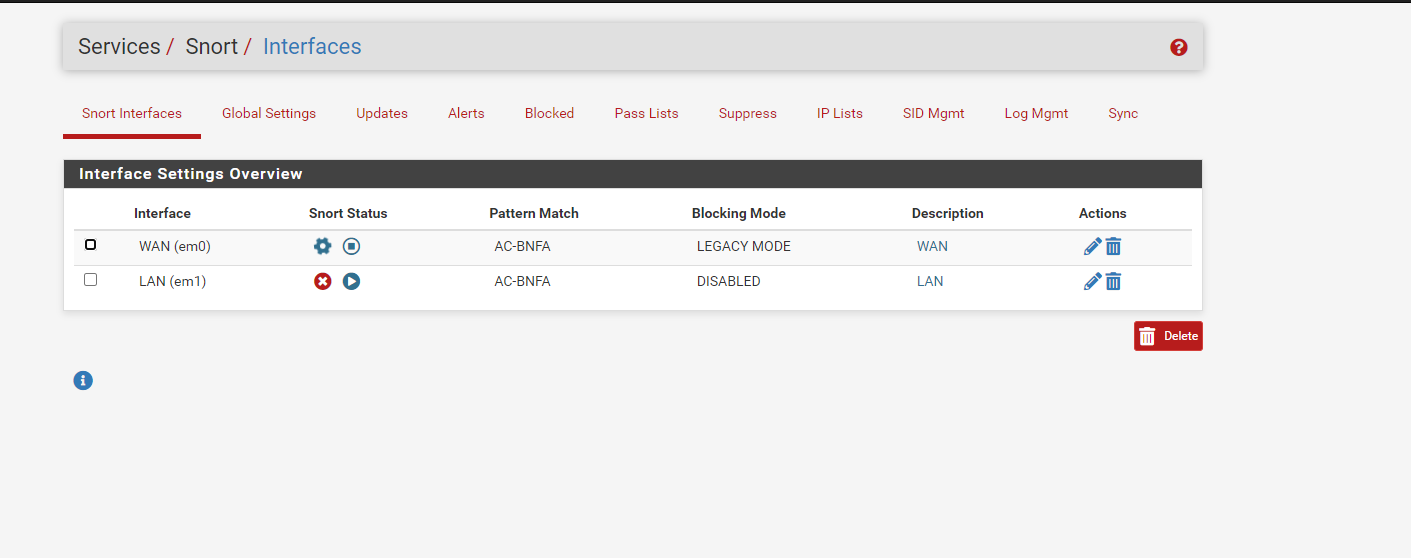
Category selection 🡪 custom rules



In Custom rules write the Rules



Now go to Snort interface and restart the snort status



Now go to alert msg and check

