

1)

- a) 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
```

- b) 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
```

- c) 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
```

```
[root@reverse-proxy ~]# yum install iptables* -y
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
epel/x86_64/metalink | 5.9 kB 00:00:00
 * base: mirrors.nextgen.com
 * epel: mirrors.thzhost.com
 * extras: mirrors.nextgen.com
 * updates: mirrors.nextgen.com
base | 3.6 kB 00:00:00
epel | 4.7 kB 00:00:00
extras | 2.9 kB 00:00:00
updates | 2.9 kB 00:00:00
epel/x86_64/primary.db FAILED 0% [- ] 0.0 B/s | 64 kB --:--:-- ETA
https://mirror.yer.az/fedora-epel/7/x86_64/repodata/c48897bb68bdb7e715878bede95d2deb7a67f57f702dc076234bcc41da00c116-primary.sqlite.bz2: [Errno 14] HTTP Error 404 - Not Found --:--:-- ETA
Trying other mirror.
To address this issue please refer to the below wiki article
https://wiki.centos.org/yum-errors
If above article doesn't help to resolve this issue please use https://bugs.centos.org/.
(1/2): epel/x86_64/primary.db | 7.0 MB 00:00:02
(2/2): epel/x86_64/updateinfo | 786 kB/s | 7.4 MB 00:00:00 ETA
```

```

Transaction test succeeded
Running transaction
  Installing : iptables-devel-1.4.21-35.el7.x86_64
  Verifying  : iptables-devel-1.4.21-35.el7.x86_64

Installed:
  iptables-devel.x86_64 0:1.4.21-35.el7

Complete!
[root@reverse-proxy ~]# iptables -I FORWARD -p tcp -m tcp --dport 3389 -s 196.1.113.4 -j ACCEPT
[root@reverse-proxy ~]# iptables -I FORWARD -p tcp -m multiport --dports 80,443 -j ACCEPT
[root@reverse-proxy ~]# iptables -A INPUT -p tcp --dport 3389 -j LOG --log-prefix "RDP traffic" --log-level 4
[root@reverse-proxy ~]# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           udp dpt:domain
ACCEPT     udp  --  anywhere              anywhere              tcp dpt:domain
ACCEPT     tcp  --  anywhere              anywhere              udp dpt:bootps
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:bootps
ACCEPT     all  --  anywhere              anywhere              state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              anywhere              state NEW tcp dpt:ssh
REJECT     all  --  anywhere              anywhere              reject-with icmp-host-prohibited
LOG        tcp  --  anywhere              anywhere              tcp dpt:ms-wbt-server LOG level warning prefix "RDP traffic"

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination           multiport dports http,https
ACCEPT     tcp  --  196.1.113.4           anywhere              tcp dpt:ms-wbt-server
ACCEPT     all  --  anywhere              192.168.122.0/24     ctstate RELATED,ESTABLISHED
ACCEPT     all  --  192.168.122.0/24      anywhere
ACCEPT     all  --  anywhere              anywhere
REJECT     all  --  anywhere              anywhere              reject-with icmp-port-unreachable
REJECT     all  --  anywhere              anywhere              reject-with icmp-port-unreachable
REJECT     all  --  anywhere              anywhere              reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination           udp dpt:bootpc
ACCEPT     udp  --  anywhere              anywhere
[root@reverse-proxy ~]#

```

## Configuring the public IP 196.1.113.45

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	10.10.10.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.15.0

Add Network...

Remove Network

Rename Network...

## VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to:

Automatic Settings...

☐ NAT (shared host's IP address with VMs)

NAT Settings...

☒ Host-only (connect VMs internally in a private network)☒ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☒ Use local DHCP service to distribute IP address to VMs

DHCP Settings...

Subnet IP: 10 . 10 . 10 . 0

Subnet mask: 255 . 255 . 255 . 0

⚠ Administrator privileges are required to modify the network configuration.

Change Settings

Restore Defaults

Import...

Export...

OK

Cancel

Apply

Help

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	10.10.10.0
VMnet8	NAT	NAT	Connected	Enabled	196.1.113.45

Add Network...Remove NetworkRename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)  
Bridged to: AutomaticAutomatic Settings...

☒ NAT (shared host's IP address with VMs)  
NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet8

☒ Use local DHCP service to distribute IP address to VMsDHCP Settings...

Subnet IP: 196 . 1 . 113 . 45

Subnet mask: 255 . 255 . 255 . 0

Restore DefaultsImport...Export...OKCancelApplyHelp

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	10.10.10.0
VMnet8	NAT	NAT	Connected	Enabled	196.1.113.0

Add Network...
Remove Network
Rename Network...

### VMnet Information

☐ Bridged (connect VMs directly to the external network)  
Bridged to: Automatic Automatic Settings...

☒ NAT (shared host's IP address with VMs) NAT Settings...

☐ Host-only (connect VMs internally in a private network)

---

☒ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet8

☒ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: 196 . 1 . 113 . 0 Subnet mask: 255 . 255 . 255 . 0

Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help

```

[root@reverse-proxy ~]# systemctl start NetworkManager
[root@reverse-proxy ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:47:ec:f7 brd ff:ff:ff:ff:ff:ff
    inet 196.1.113.128/24 brd 196.1.113.255 scope global noprefixroute dynamic ens33
        valid_lft 1574sec preferred_lft 1574sec
    inet6 fe80::c4e6:ed22:6b40:e0f3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:47:ec:01 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.136/24 brd 10.10.10.255 scope global noprefixroute dynamic ens37
        valid_lft 1710sec preferred_lft 1710sec
    inet6 fe80::1e9f:478d:f09b:15a1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::2b6b:1dd8:24ff:5a28/64 scope link flags 800
        valid_lft forever preferred_lft forever

```

## 2) configuring Two Linux Machine

Open vpn → NAT and host only

Client → host only

```
[root@reverse-proxy ~]# setenforce 0
setenforce: SELinux is disabled
[root@reverse-proxy ~]# cat /proc/sys/net/ipv4/ip_forward
1
[root@reverse-proxy ~]# vi /etc/sysctl.conf
[root@reverse-proxy ~]# yum install epel-release -y
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.nxtgen.com
 * epel: mirrors.thzhost.com
 * extras: mirrors.nxtgen.com
 * updates: mirrors.nxtgen.com
Package epel-release-7-14.noarch already installed and latest version
Nothing to do
[root@reverse-proxy ~]# yum install openvpn -y
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.nxtgen.com
```

```
root@reverse-proxy ~
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward=1
~
~
~
~
~
~
~
```

```
[root@reverse-proxy ~]# cd /etc/openvpn/
[root@reverse-proxy openvpn]# wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz
--2023-07-14 11:51:14-- https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/4519663/8d46db80-266e-11e9-85e3-7de4dbee40d9?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230714%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230714T062935Z&X-Amz-Expires=300&X-Amz-Signature=9b5bfb1cee32435a387c01678a16898d0125bedd1fca88cda0c15ea205e300946X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=4519663&response-content-disposition=attachment%3B%20filename%3DEasyRSA-unix-v3.0.6.tgz&response-content-type=application%2Foctet-stream [
lowing]
--2023-07-14 11:51:14-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/4519663/8d46db80-266e-11e9-85e3-7de4dbee40d9?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
dential=AKIAIWNJYAX4CSVEH53A%2F20230714%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230714T062935Z&X-Amz-Expires=300&X-Amz-Signature=9b5bfb1cee32435a387c01678a16898d0125bedd1fca88cda0c1
205e300946X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=4519663&response-content-disposition=attachment%3B%20filename%3DEasyRSA-unix-v3.0.6.tgz&response-content-type=application%
tet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.108.133, 185.199.111.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 40840 (40K) [application/octet-stream]
Saving to: 'EasyRSA-unix-v3.0.6.tgz.1'

100%[=====>] 40,840 --.-K/s in 0.008s

2023-07-14 11:51:15 (5.02 MB/s) - 'EasyRSA-unix-v3.0.6.tgz.1' saved [40840/40840]

[root@reverse-proxy openvpn]# ls
client EasyRSA-unix-v3.0.6.tgz server
easy-rsa EasyRSA-unix-v3.0.6.tgz.1 server.conf
[root@reverse-proxy openvpn]# tar -xvzf EasyRSA-unix-v3.0.6.tgz
EasyRSA-v3.0.6/
EasyRSA-v3.0.6/easyrsa
EasyRSA-v3.0.6/openssl-easyrsa.cnf
EasyRSA-v3.0.6/vars.example
EasyRSA-v3.0.6/x509-types/
EasyRSA-v3.0.6/gpl-2.0.txt
EasyRSA-v3.0.6/mktemp.txt
EasyRSA-v3.0.6/COPYING.md
EasyRSA-v3.0.6/Changelog
EasyRSA-v3.0.6/README.md
EasyRSA-v3.0.6/README.quickstart.md
EasyRSA-v3.0.6/doc/
EasyRSA-v3.0.6/doc/EasyRSA-Advanced.md
```

```
[root@reverse-proxy easy-rsa]# ls
ChangeLog      EasyRSA-v3.0.6      pki              vars.example
COPYING.md     gpl-2.0.txt         README.md        x509-types
doc            mktemp.txt          README.quickstart.md
easyrsa        openssl-easyrsa.cnf  vars
[root@reverse-proxy easy-rsa]# ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars

WARNING!!!

You are about to remove the EASYRSA_PKI at: /etc/openvpn/easy-rsa/pki
and initialize a fresh PKI here.

Type the word 'yes' to continue, or any other input to abort.
Confirm removal:

Aborting without confirmation.
[root@reverse-proxy easy-rsa]#
[root@reverse-proxy easy-rsa]# ./easyrsa build-ca

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017

Easy-RSA error:

Unable to create a CA as you already seem to have one set up.
If you intended to start a new CA, run init-pki first.

[root@reverse-proxy easy-rsa]# ls
ChangeLog      EasyRSA-v3.0.6      pki              vars.example
COPYING.md     gpl-2.0.txt         README.md        x509-types
doc            mktemp.txt          README.quickstart.md
```



Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017  
Generating a 2048 bit RSA private key

.....+++  
.....+++

writing new private key to '/etc/openvpn/easy-rsa/pki/private/demovpn.key.YjbydLeIlk  
-----

You are about to be asked to enter information that will be incorporated  
into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Common Name (eg: your user, host, or server name) [demovpn]:

Keypair and certificate request completed. Your files are:

req: /etc/openvpn/easy-rsa/pki/reqs/demovpn.req

key: /etc/openvpn/easy-rsa/pki/private/demovpn.key

[root@reverse-proxy easy-rsa]# ls pki/reqs/demovpn.req

pki/reqs/demovpn.req

[root@reverse-proxy easy-rsa]# cat pki/reqs/demovpn.req

-----BEGIN CERTIFICATE REQUEST-----

MIICVzCCAT8CAQAwEjEQMA4GA1UEAwHZGVtb3ZwbjCCASIwDQYJKoZIhvcNAQEB  
BQADggEPADCCAQoCggEBAMZNofKtrzXcnhuQssVQGYX1PJ19BumiP7IzG5b2Qu9L  
uuYK9LyY6B9sBZHx57b3ZtGBZnfKS/wPKl39EE+5sLpZr9HBcjI3b2ho7+yNPPH5  
rDpa/DDbvgf5GEUMQElhKksHRz300r9InwfkiJdn+noBtK/AL2QnuDc5Wlcaq070  
bNE8g/gzFhi2UGgM0pUqSn3ZVNxRpCPMK9tvW7+4rKq4D06nfN0up59LZyQA6Yn2  
KFUvzf3k2f9ekYTFZWPf660Yc8GUynC0tg9FhU9XYOLHgYnZnfG2i14xHA/0QSL6  
e9o1RbWFMmCiQDFdRwjVMPdHFjzeTes4mFfrBVrbPU0CAwEAaAAMA0GCSqGSIb3  
DQEBcwUAA4IBAQC9Kz+a3n2JFy6RaowTy5E/NQv4DUstAqWHSfZ+q9tqL2pf9iX7  
Qwlg/jqh5VaDJmHLfnS5d6902+qRjZNE/Js1d+S7uoSNDC7cV0cLi4q3w4g5EDu6  
TzkCHgU/5pEbHB02njPIoallxS6wpT+x58gH6eXCDmNsQW+7eohZyX0BW4giiBL  
mNsE93VX5msgElGDqJB+TMd0Gl6d7dDJ/1GCJzjB4Mo1dvjmfwkIe/Gv0IdRoBa  
hCx4wa/jMu63QL+3i4Bh220nlvBTKS6x/t6R3eA9tW+psTKFACvAP6XzEMf0GTQ5  
H7X9VExcMwYW662ZiBiZrqZ0JuKYSgeVQUL

-----END CERTIFICATE REQUEST-----

[root@reverse-proxy easy-rsa]# █

```
pki/reqs/demovpn.req
[root@reverse-proxy easy-rsa]# cat pki/reqs/demovpn.req
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwHZGVtb3ZwbjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMZNoKtrZXcnhuQssVQGYX1PJ19BumiP7IzG5b2Qu9L
uuYK9Ly6B9sBZHx57b3ZtGBZnfKS/wPKl39EE+5sLpZr9HBcjI3b2ho7+yNPPH5
rDpa/DDbvfgf5GEUMQELhKksHRz300r9InwfkiJdn+noBtK/AL2QnuDc5W1caq070
bNE8g/gzFhi2UGgM0pUqSn3ZVNxRpCPMK9tvW7+4rKq4D06nfN0up59lZyQA6Yn2
KFUvzf3k2f9ekYTFZWPF660Yc8GUynC0tg9FhU9XYOLHgYnZnfG2i14xHA/0QSL6
e9o1RbWFMmCiQDFdRwjVMPdHFjzeTes4mFfrBVrbPU0CAwEAAaAAMA0GCSqGSIb3
DQEBCCUAA4IBAQC9Kz+a3n2JFy6RaowTy5E/NQv4DUstAQWHSfZ+q9tqL2pf9iX7
Qw1g/jqh5VaDJmHLfnS5d6902+qRjZNE/Js1d+S7uoSNDc7cV0cLi4q3w4g5EDu6
TzkCHgU/5pEbHB02njPIo0allxS6wpT+x58gH6eXCDmNsQW+7eohZyX0BW4giiBL
mNsE93VX5msgElGDqJB+TMd0GLg6d7dDJ/1GCJzjB4Mo1dvjmfwkIe/Gv0IdRoBa
hCx4wa/jMu63QL+3i4Bh220nlvBTKS6x/t6R3eA9tW+psTKFACvAP6XzEMf0GTQ5
H7X9VEx1cMwYW662ZiBiZrQZ0JuKYSgeVQUL
-----END CERTIFICATE REQUEST-----
[root@reverse-proxy easy-rsa]# ./easyrsa sign-req server demovpn
```

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017

You are about to sign the following certificate.

Please check over the details shown below for accuracy. Note that this request has not been cryptographically verified. Please be sure it came from a trusted source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 365 days:

```
subject=
  commonName              = demovpn
```

Type the word 'yes' to continue, or any other input to abort.

Confirm request details: yes

Using configuration from /etc/openssl/easy-rsa/pki/safessl-easyrsa.cnf

Enter pass phrase for /etc/openssl/easy-rsa/pki/private/ca.key:

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

X509v3 Extended Key Usage:  
TLS Web Server Authentication  
X509v3 Key Usage:  
Digital Signature, Key Encipherment  
X509v3 Subject Alternative Name:  
DNS:demovpn

Signature Algorithm: sha256WithRSAEncryption

ae:02:74:2b:ed:3c:6a:de:da:7a:de:9b:8c:06:c4:16:1e:ba:  
5f:8b:98:a7:7f:5e:54:63:79:ce:7d:fb:12:c3:0d:55:91:b5:  
5e:2b:55:16:3c:51:f9:62:ef:15:05:53:e6:9e:73:24:24:0b:  
65:72:c9:2a:5c:7d:c6:16:fb:84:e3:d8:a5:20:22:bd:74:24:  
c3:8e:57:e7:07:35:97:fc:03:89:2b:37:5a:b3:f3:1a:d5:b0:  
82:fb:55:0f:1c:22:f9:1b:87:04:bd:24:16:90:58:79:a8:8a:  
82:70:11:e5:0f:69:94:0e:2d:10:10:5d:1c:32:0c:58:89:d1:  
b5:59:e4:e6:21:4d:66:07:94:41:fb:c7:58:5a:1a:97:e9:ef:  
3b:d5:31:6c:dc:55:6e:f4:70:4f:5e:af:40:eb:01:be:8d:b3:  
92:78:88:30:19:74:89:ac:a5:93:19:c4:06:f3:b3:c1:a0:25:  
9c:43:22:48:89:20:22:5b:e6:bd:08:e7:e8:20:34:e0:20:58:  
91:d7:68:f9:69:b3:6b:3e:d4:aa:96:73:ca:2e:66:b7:ae:63:  
cf:0c:c1:18:90:0e:c4:5b:c8:b0:9a:5c:72:fe:0c:e3:29:5f:  
5a:21:14:d0:eb:83:6a:07:29:65:70:be:d2:41:4f:e3:35:d6:  
12:f0:96:49

-----BEGIN CERTIFICATE-----

MIIDVzCCAj+gAwIBAgIRAKrLPcDGuAim4c/Az+zey0kwDQYJKoZIhvcNAQELBQAw  
EjEQMA4GA1UEAwHYWN0c3ZwbjAeFw0yMzA3MTQwNjMxMjNaFw0yNDA3MTMwNjMx  
MjNaMBIxEDAOBgNVBAMMB2RlbW92cG4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw  
ggEKAoIBAQDGTaHyra813J4bkLLFUBmF9TydfQbpoj+yMxuW9kLvS7rmCvS8mOgf  
bAWR8ee292bRGWZ3ykv8Dypd/RBpubC6c6/RwXIyN29oa0/sjTzx+aw6WvwW274H  
+RhFDEBJYSplB0c99Dq/SJ8H5Io3Z/p6AbSvwC9kJ7g30VtXGqt0zmzRPIP4MxYY  
tlBoDNKVKkp92VTcUaQjzCvbb1u/uKyquA90p3zdLqefZWckA0mJ9ihVL8395Nn/  
XpGExWVj3+utGHPBlMpwtLYPRYVPV2Dix4GJ2Z3xtoteMRwP9EEi+nvaNUW1hTDA  
okAxXUcI1TD3RxY83k3r0JhX6wVa2z1NagMBAAGjgacwgaQwCQYDVR0TBAlwADAd  
BgNVHQ4EFgQUunpxyUNQfVolu0PNq347H6Qb0VlowQgYDVR0jBDswOYAuc5E6U/BZ  
tyQ4AIkdL4u0H06h8gmhFqQUMBIXEDAOBgNVBAMMB2FjdHN2cG6CCQCEfFvMy62U  
RzATBgNVHSUEDDAKBggrBgEFBQcDATAALBgNVHQ8EBAMCBaAwEgYDVR0RBAswCYIH  
ZGVtb3ZwbjANBgkqhkiG9w0BAQsFAA0CAQEArgJ0K+08at7aet6bjAbEFh66X4uY  
p39eVGN5zn37EsMNVZG1XitVFjxR+WLvFQVT5p5zJCQLZXLJKlx9xhb7h0PYpSAi  
vXQkw45X5wc1l/wDiSs3WrPzGtWwgvVDxwi+RuHBL0kFpBYeaiKgnAR5Q9plA4t  
EBBdHDIMWInRtVnk5iFNZgeUQfvHWFoal+nv09UxbNxBvRwT16vQ0sBvo2zkniI  
MB10iaylkxneBv0zwaAlnEMiSIkgIlvmvQjn6CA04CBYkddo+Wmzaz7UqpZzyi5m  
t65jzwzBGJA0xFvIsJpccv4M4ylfWiEU00uDagcpZXC+0kFP4zXWEvCWSQ==

-----END CERTIFICATE-----

```
[root@reverse-proxy easy-rsa]# openssl verify -CAfile pki/ca.crt pki/issued/demovpn.crt
pki/issued/demovpn.crt: OK
[root@reverse-proxy easy-rsa]# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
```

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
```

Is

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

mv EasyRSA-v3.0.6 easy-rsa

Is

```
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/openssl/server/

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

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

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

./easyrsa gen-req client nopass

./easyrsa sign-req client client

./easyrsa gen-req jerry nopass

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

ls /etc/openssl/client/

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

cp pki/private/client.key /etc/openssl/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)

```
root@server1:~# hostnamectl set-hostname reverse-proxy
[root@server1 ~]# systemctl stop firewalld.service
[root@server1 ~]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
[root@server1 ~]# vim /etc/selinux/config
[root@server1 ~]# init 6
```

```
File Edit View Search Terminal Tabs Help
root@server1:/etc/nginx x root@server1:/etc/nginx

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

~
~
~
~
~
~
~
~
```

```
root@client1 ~]# systemctl start firewalld.service
[root@client1 ~]# firewall-cmd --add-service=http
success
[root@client1 ~]# yum install httpd
```

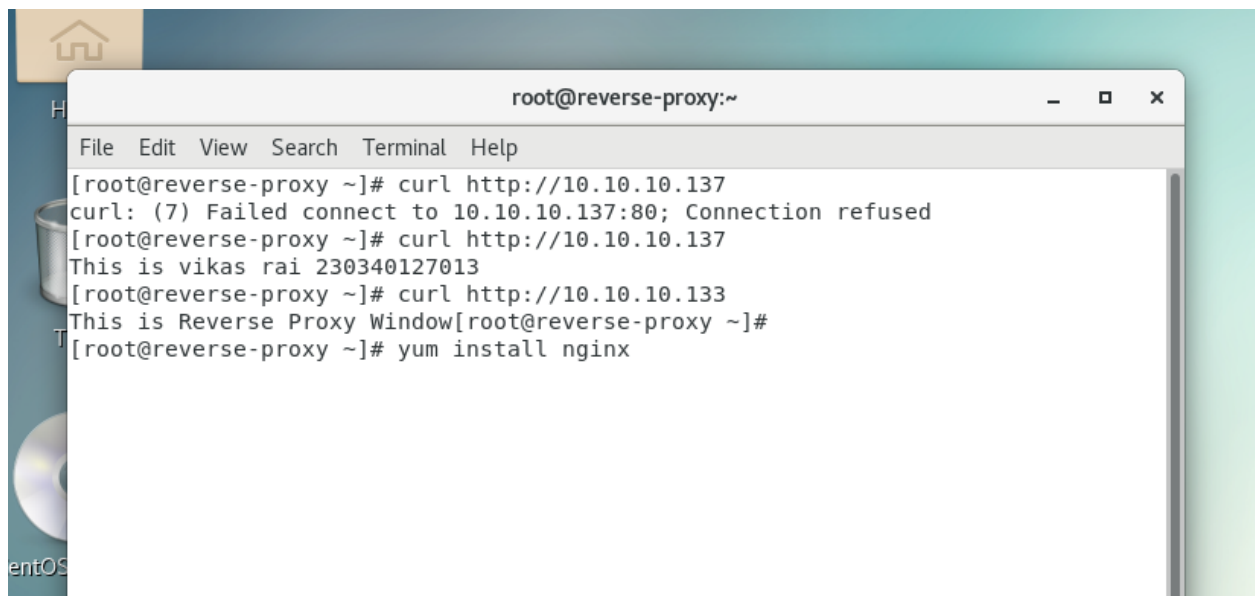
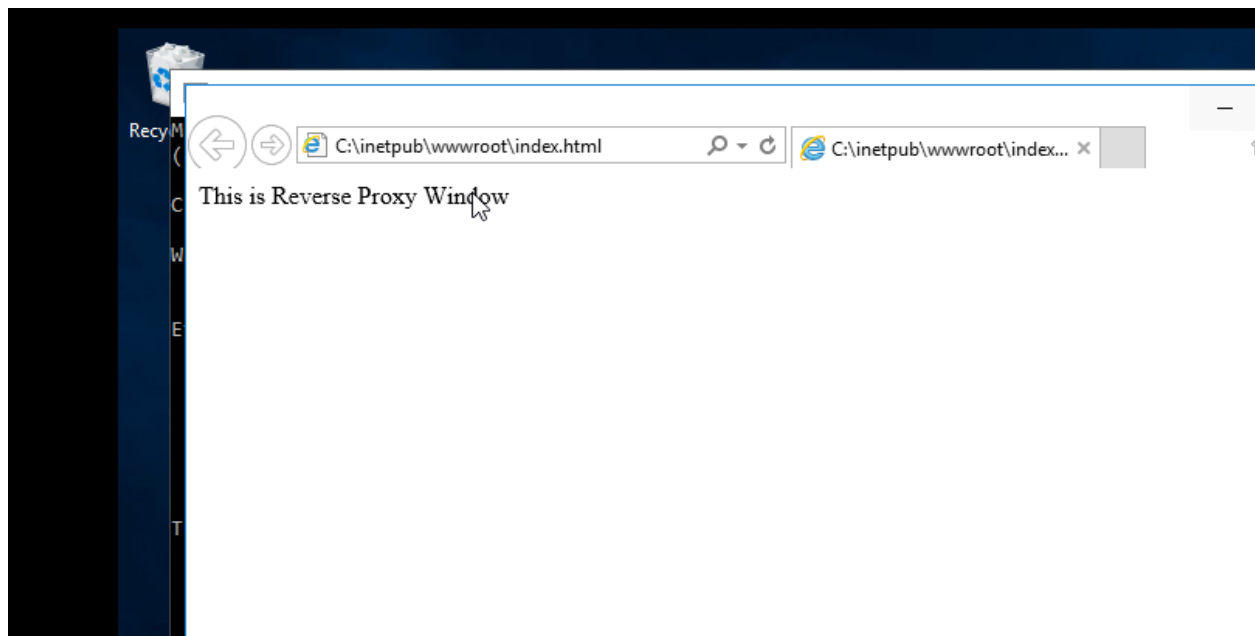


```
root@client1:~/client
```

This is vikas rai 230340127013

[illegible]

```
link/ether 52:54:00:ab:31:6d brd ff:ff:ff:ff:ff:ff
[root@client1 ~]# cd /var/www/html/
[root@client1 html]# vim index.html
[root@client1 html]# systemctl start httpd
[root@client1 html]#
```



```

sendfile            on;
tcp_nopush          on;
tcp_nodelay         on;
keepalive_timeout   65;
types_hash_max_size 4096;

include             /etc/nginx/mime.types;
default_type        application/octet-stream;

# Load modular configuration files from the /etc/nginx/conf.d directory.
# See http://nginx.org/en/docs/nginx_core_module.html#include
# for more information.
include /etc/nginx/conf.d/*.conf;
    upstream hpcsa {
        server 10.10.10.137 weight=3;
        server 10.10.10.133;

server {
    listen      80;
    listen      [::]:80;
    server_name _;
    root        /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;
    location /{
        proxy_pass http://hpcsa/;

```

```

[root@reverse-proxy ~]# cd /etc/nginx/
[root@reverse-proxy nginx]# vim nginx.conf
[root@reverse-proxy nginx]# systemctl restart nginx
[root@reverse-proxy nginx]#

```

#systemctl restart nginx

Output -

← → ↻  http://196.1.113.128

This is vikas rai 230340127013

← → ↻  https://192.1.113.128

This is Reverse Proxy Window

3)

Pfsense machine → NAT and host only

Centos machine → Bridge

```
done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: cd5b533315dddabd7681

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

WAN (wan)      -> em0      -> v4/DHCP4: 196.1.113.129/24
LAN (lan)      -> em1      -> v4: 10.10.10.20/24

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: █
```

Login →

## SIGN IN

*admin*

••••|

SIGN IN

Install the Snort Packages

COMMUNITY EDITION

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term

snort

Both

Search

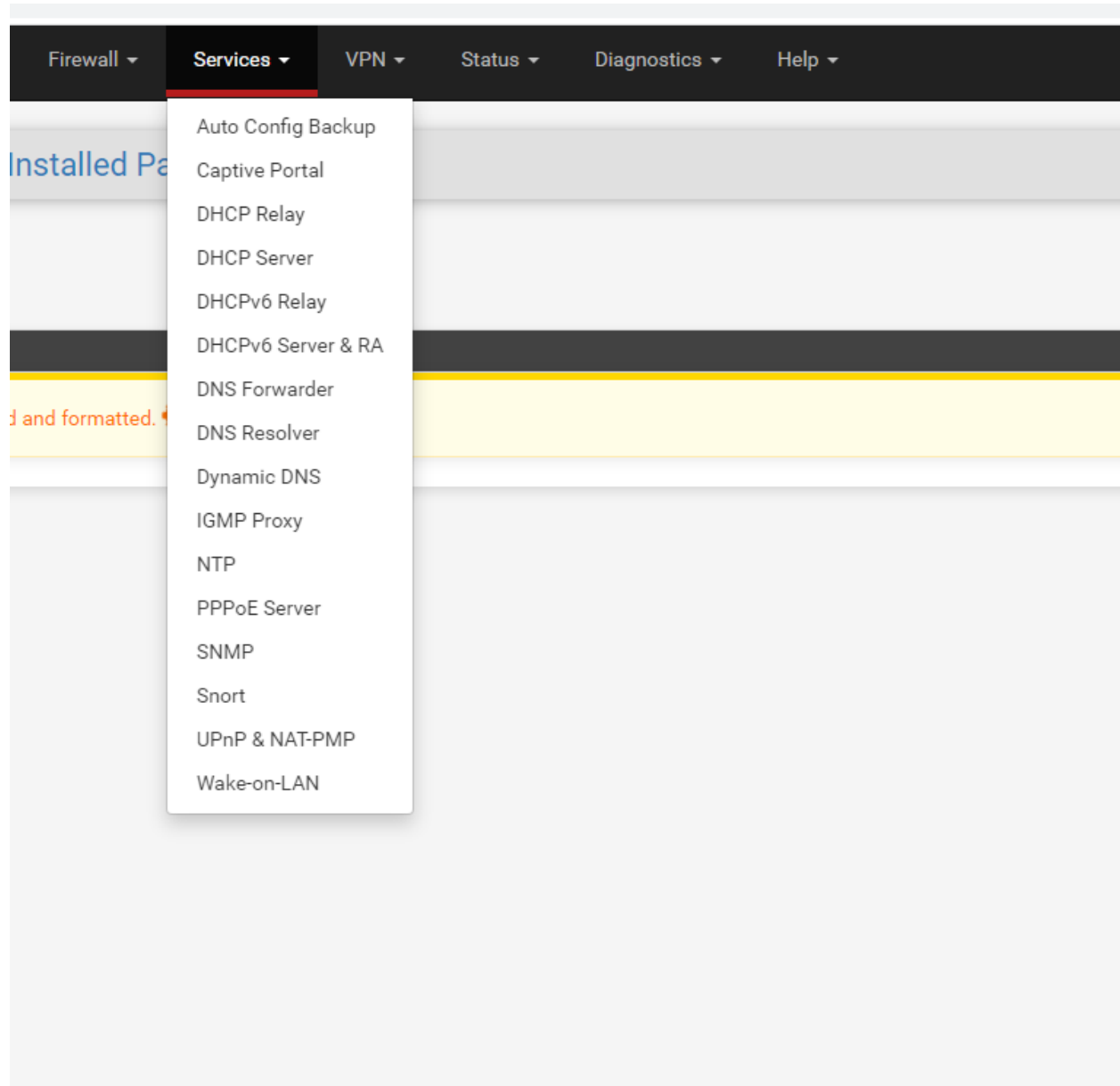
Clear

Enter a search string or \*nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
acme	0.7.4	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.  Package Dependencies: <a href="#">pecl-ssh2-1.3.1</a> <a href="#">socat-1.7.4.4</a> <a href="#">php82-8.2.6</a> <a href="#">php82-ftp-8.2.6</a>	+ Install
apcupsd	0.3.92_1	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN  Package Dependencies: <a href="#">apcupsd-3.14.14_4</a>	+ Install
arping	1.2.2_4	Broadcasts a who-has ARP packet on the network and prints answers.  Package Dependencies: <a href="#">arping-2.21_1</a>	+ Install
arpwatch	0.2.1	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.  Package Dependencies: <a href="#">arpwatch-3.3</a>	+ Install

Go to the Services and then go to snort



- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server & RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- NTP
- PPPoE Server
- SNMP
- Snort
- UPnP & NAT-PMP
- Wake-on-LAN



pi

sense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

Services / Snort / Interfaces

?

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input checked="" type="checkbox"/> WAN (em0)	<div><div></div><div></div><div></div></div>	AC-BNFA	LEGACY MODE	<a href="#">WAN</a>	<div><div></div><div></div></div>
<input type="checkbox"/> LAN (em1)	<div><div></div><div></div><div></div></div>	AC-BNFA	DISABLED	<a href="#">LAN</a>	<div><div></div><div></div></div>

Delete

i

Snort Settings

Snort Categories

Snort Rules

Snort Variables

Snort Profiles

Snort Help

Snort Logs

General Settings

Enable

☒ Enable interface

Interface

WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description

WAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Enable Packet Captures

☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Enable Unified2 Logging

☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.

Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

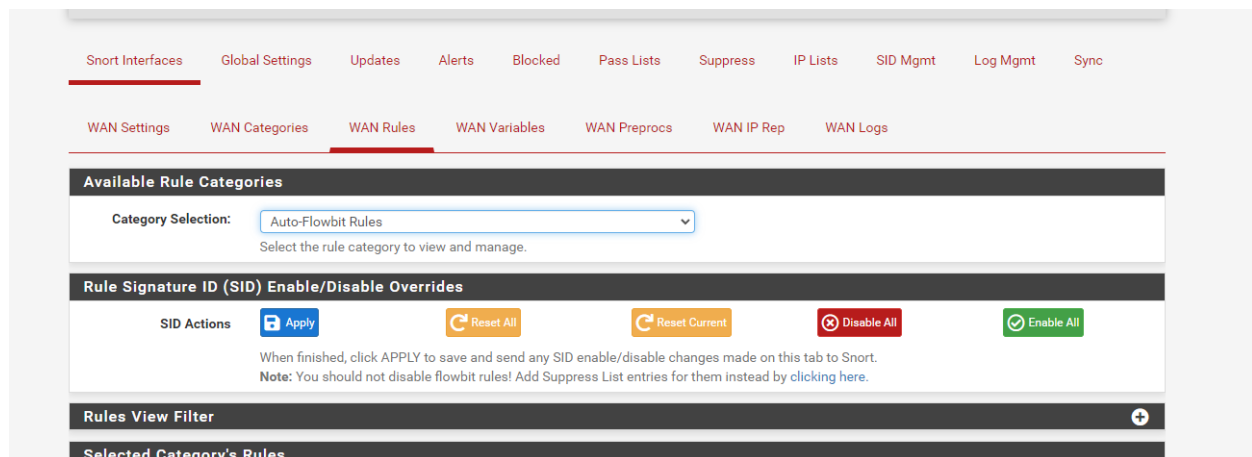
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

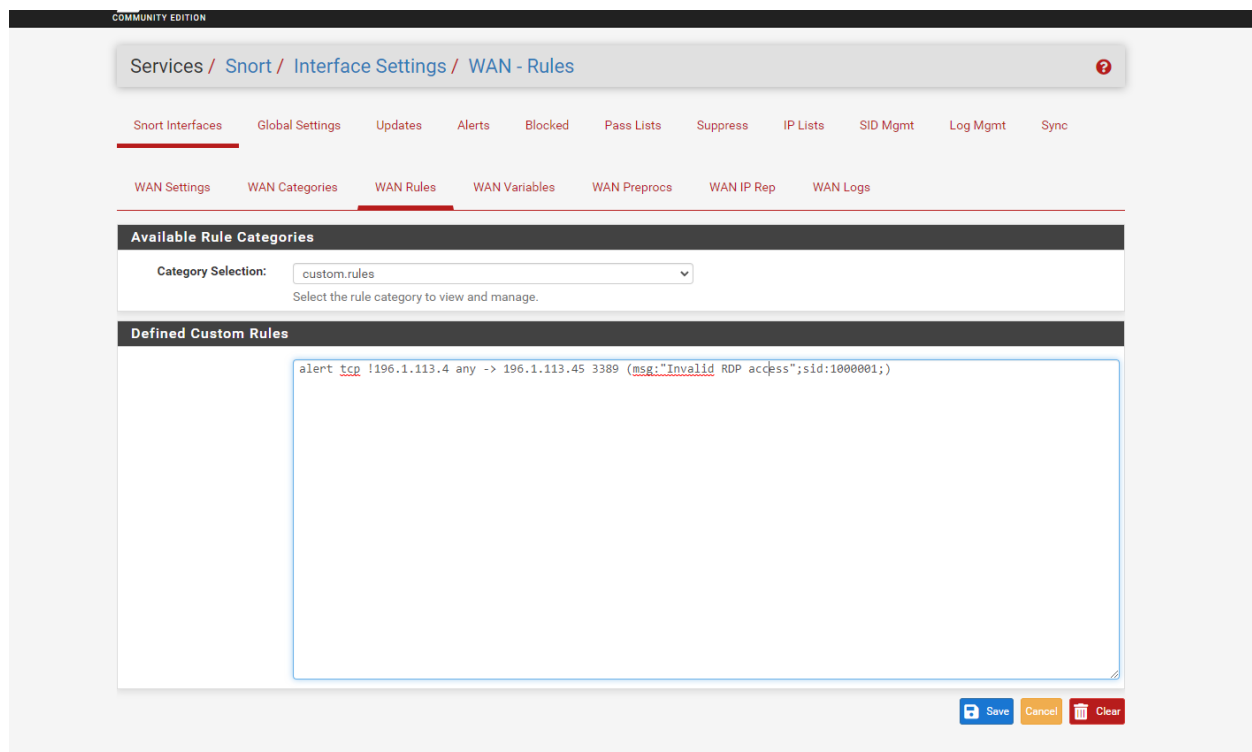
Kill States

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Category selection → custom rules



In Custom rules write the Rules



Now go to Snort interface and restart the snort status

Services / Snort / Interfaces

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input checked="" type="checkbox"/>	WAN (em0)		AC-BNFA	LEGACY MODE	WAN	
<input type="checkbox"/>	LAN (em1)		AC-BNFA	DISABLED	LAN	

Delete

Now go to alert msg and check

Services / Snort / Alerts

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-07-14		3	TCP	Deny-HTTP-Req	192.168.15.106	49474	52.24.221.24	443	1073.1	(...)