***Open VPN***

**Required Machines**

1. VPN server (centos7) : NAT = 192.168.44.150

Host-Only = 10.10.10.132

1. VPN client (centos7) : NAT = 192.168.44.139
2. Windows : Host-Only = 10.10.10.133

**IN Windows Machine**

Create one **index.html** page in **C:/inetpub/wwwroot/** folder

**IN VPN server Machine**

# vi /etc/selinux/config ------------SELINUX=disabled

# echo 1 > /proc/sys/net/ipv4/ip-forward

# vi /etc/sysctl.conf ---------------add this line at last (net.ipv4.ip\_forwad=1)

# yum install epel-release

# yum install openvpn

# cd /etc/openvpn/

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

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

# mv EasyRSA-v3.0.6 easy-rsa

# cd easy-rsa/

# vi vars

set\_var EASYRSA "$PWD"

set\_var EASYRSA\_PKI "$EASYRSA/pki"

set\_var EASYRSA\_DN "cn\_only"

set\_var EASYRSA\_REQ\_COUNTRY "INDIA"

set\_var EASYRSA\_REQ\_PROVINCE "Maharashtra"

set\_var EASYRSA\_REQ\_CITY "Pune"

set\_var EASYRSA\_REQ\_ORG "ACTS CDAC"

set\_var EASYRSA\_REQ\_EMAIL "admin@demo.lab"

set\_var EASYRSA\_REQ\_OU "ACTS"

set\_var EASYRSA\_KEY\_SIZE 2048

set\_var EASYRSA\_ALGO rsa

set\_var EASYRSA\_CA\_EXPIRE 7500

set\_var EASYRSA\_CERT\_EXPIRE 365

set\_var EASYRSA\_NS\_SUPPORT "no"

set\_var EASYRSA\_NS\_COMMENT "ACTS CDAC"

set\_var EASYRSA\_EXT\_DIR "$EASYRSA/x509-types"

set\_var EASYRSA\_SSL\_CONF "$EASYRSA/openssl-easyrsa.cnf"

set\_var EASYRSA\_DIGEST "sha256"

# ./easyrsa init-pki

# ./easyrsa build-ca

Set password = **hpcsa**

Set Common name = **open-vpn-server**

# ./easyrsa gen-req demovpn nopass

# ./easyrsa sign-req server demovpn

Confirm request = **yes**

Password = **hpcsa**

# openssl verify -CAfile pki/ca.crt pki/issued/demovpn.crt

# ./easyrsa gen-dh

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

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

# cp pki/private/demovpn.key /etc/openvpn/server/

# cp pki/issued/demovpn.crt /etc/openvpn/server/

# ./easyrsa gen-req client nopass

# ./easyrsa sign-req client client

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

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

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

# vi /etc/openvpn/server/server.conf

port 1194

proto udp

dev tun

ca /etc/openvpn/server/ca.crt

cert /etc/openvpn/server/demovpn.crt

key /etc/openvpn/server/demovpn.key

dh /etc/openvpn/server/dh.pem

server 10.8.0.0 255.255.255.0

#push "redirect-gateway def1"

#push "dhcp-option DNS 208.67.222.222"

#push "dhcp-option DNS 208.67.220.220"

duplicate-cn

cipher AES-256-CBC

tls-version-min 1.2

tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256

auth SHA512

auth-nocache

keepalive 20 60

persist-key

persist-tun

compress lz4

daemon

user nobody

group nobody

log-append /var/log/openvpn.log

verb 3

# systemctl start openvpn-server@server

# systemctl enable openvpn-server@server

# systemctl start firewalld.service

# systemctl enable firewalld.service

# firewall-cmd --permanent --add-service=openvpn

# firewall-cmd --permanent --zone=trusted --add-service=openvpn

# firewall-cmd --permanent --zone=trusted --add-interface=tun0

# firewall-cmd --add-masquerade

# firewall-cmd --permanent --add-masquerade

# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o ens33 -j MASQUERADE

# firewall-cmd --reload

# vi /etc/openvpn/client/client.ovpn

cient

dev tun

proto udp

remote 192.168.44.150 1194

ca ca.crt

cert client.crt

key client.key

cipher AES-256-CBC

auth SHA512

auth-nocache

tls-version-min 1.2

tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256

resolv-retry infinite

compress lz4

nobind

persist-key

persist-tun

mute-replay-warnings

verb 3

# scp -r /etc/openvpn/client root@192.168.44.139:/root

**IN VPN Client Machine**

# yum install epel-release.noarch

# yum install openvpn

Now change network setting to manual and give ip address same as previous 192.168.44.139 & subnet mask 255.255.255.0

Don’t give DNS & Gateway

# cd /root/client

# openvpn --config client.ovpn

Now open the new terminal & run command **#ip a**

**‘tun0’** adapter is added now

Now press ‘ctrl c’

**IN VPN server Machine**

# vi /etc/openvpn/server/server.conf

Add this line ----🡪 push "route 10.10.10.0 255.255.255.0"

# systemctl restart open-server@server.service

**IN VPN Client Machine**

# openvpn --config client.ovpn

Now go to browser and put windows machine ip address in web browser.

**Index.html** will get host and you will able to see content in that file