VPN Exercises

OpenVPN is a fully-featured, open-source Secure Socket Layer (SSL) VPN solution.

Log into the AWS Management Console.
Launch an EC2 instance.
Create a keyfile(.pem) and download the key file.
Go to windows terminal
Change into the downloads folder
Type $ chmod 400 VPNopdracht.pem #changing permissions to read,write and execute the file.
Connect to ec2 instance using

$ ssh -i "VPNopdracht.pem" 52.29.235.84

change into root directory

Step 1: **Install OpenVPN**

Type $ yum update -y #Updates repositories and packages.

#OpenVPN is available in the Extra Packages for Enterprise Linux (EPEL) repository. To enable the EPEL repository, run the command:

$ yum install epel-release -y
$ sudo amazon-linux-extras epel-release

```
Installed:
  epel-release.noarch 0:7-11
```

$ yum update -y #update repositories again

$ yum install -y openvpn #Installs OpenVPN

```
Installed:
  openvpn.x86_64 0:2.4.11-1.el7

Dependency Installed:
  lzo.x86_64 0:2.06-8.amzn2.0.4                    pkcs11-helper.x86_64 0:1.11-3.el7

Complete!
[root@ip-172-31-40-188 ec2-user]#
```

Step2: **Install Easy RSA**

Install **easy RSA**, a CLI utility for creating and managing a PKI Certificate Authority (CA).
Easy RSA helps you set up an internal certificate authority (CA) and generate SSL key pairs to secure the VPN connections

1)$yum install -y wget # install **wget** command,used to download easy RSA package.

2)$wget https://github.com/OpenVPN/easy-rsa/archive/v3.0.8.tar.gz #new version of CLI utility

```
Complete!
[root@ip-172-31-40-188 ec2-user]# yum install -y wget
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                               | 3.7 kB  00:00:00
208 packages excluded due to repository priority protections
Package wget-1.14-18.amzn2.1.x86_64 already installed and latest version
Nothing to do
[root@ip-172-31-40-188 ec2-user]# wget https://github.com/OpenVPN/easy-rsa/archive/v3.0.8.tar.gz
--2021-11-19 20:23:43--  https://github.com/OpenVPN/easy-rsa/archive/v3.0.8.tar.gz
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/OpenVPN/easy-rsa/tar.gz/v3.0.8 [following]
--2021-11-19 20:23:43--  https://codeload.github.com/OpenVPN/easy-rsa/tar.gz/v3.0.8
Resolving codeload.github.com (codeload.github.com)... 140.82.121.10
Connecting to codeload.github.com (codeload.github.com)|140.82.121.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3864366 (3.7M) [application/x-gzip]
Saving to: ‘v3.0.8.tar.gz’

100%[===================================================================>] 3,864,366   --.-K/s   in 0.1s

2021-11-19 20:23:43 (38.8 MB/s) - ‘v3.0.8.tar.gz’ saved [3864366/3864366]
```

3) $ tar -xf v3.0.8.tar.gz #Extract the downloaded archive.

4) $ cd /etc/openvpn #Change into the openvpn directory

5) $ mkdir /etc/openvpn/easy-rsa #Make a new directory

6) $ mv /root/easy-rsa-3.0.8 /etc/openvpn/easy-rsa
We list the content in easy-rsa.

```
[root@ip-172-31-5-43 ~]# cd /etc/openvpn/
[root@ip-172-31-5-43 openvpn]# mkdir /etc/openvpn/easy-rsa
[root@ip-172-31-5-43 openvpn]# mv /root/easy-rsa-3.0.8 /etc/openvpn/easy-rsa
[root@ip-172-31-5-43 openvpn]# cd /etc/openvpn/easy-rsa
[root@ip-172-31-5-43 easy-rsa]# ls
easy-rsa-3.0.8
[root@ip-172-31-5-43 easy-rsa]# cd easy-rsa-3.0.8
[root@ip-172-31-5-43 easy-rsa-3.0.8]# ls
build      COPYING.md  doc       KNOWN_ISSUES  op_test.orig  README.md             release-keys  wop_test.sh
ChangeLog  distro      easyrsa3  Licensing     op_test.sh    README.quickstart.md  wop_test.bat
```

Step 3: Configure OpenVPN

1)$ cp /usr/share/doc/openvpn-2.4.11/sample/sample-config-files/server.conf /etc/openvpn #Copy a sample file from openvpn documentation directory

2)$ find /-name server.conf #displays the openvpn version

3)$ vi /etc/openvpn/server.conf #opens this server.conf and make changes

```
ec2-user@ip-172-31-40-188:~
#                                                     #
# OpenVPN also supports                               #
# single-machine <-> single-machine                   #
# configurations (See the Examples page               #
# on the web site for more info).                     #
#                                                     #
# This config should work on Windows                  #
# or Linux/BSD systems.  Remember on                  #
# Windows to quote pathnames and use                  #
# double backslashes, e.g.:                           #
# "C:\\Program Files\\OpenVPN\\config\\foo.key"       #
#                                                     #
# Comments are preceded with '#' or ';'               #
#######################################################

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp
-- INSERT --
```

Locate the following lines and edit by removing '#' and adding ';' before the following lines

- `topology subnet` (makes the OpenVPN installation function as a subnetwork)
- `push "redirect-gateway def1 bypass-dhcp"` (instructs the client to redirect traffic through the OpenVPN server)
- `push "dhcp-option DNS 208.67.222.222"` (uses an OpenDNS resolver to connect to OpenVPN)
- `push "dhcp-option DNS 208.67.220.220"` (uses an OpenDNS resolver to connect to OpenVPN)

- `user nobody` (runs OpenVPN with no privileges)
- `group nobody` (runs OpenVPN with no privileges)

4);tls-auth ta.key 0 # locate the line **tls-auth ta.key 0** and comment it by adding **;** infront of the line

tls-crypt myvpn.tlsauth #add this command at a new line.

```
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret
tls-crypt myvpn.tlsauth
```

5)Save and exit server.conf

#Generate a static encryption key to enable TLS authentication.

6)$ openvpn –genkey –secret /etc/openvpn/myvpn.tlsauth

Step 4: Generate keys and certificates.

1)$ cd /etc/openvpn/easy-rsa/easyrsa3 #change directory to easyrsa3

2)$ cp vars.example vars #copy .example to vars and ls

3)$ ls

```
[root@ip-172-31-5-43 ~]# cd /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3
[root@ip-172-31-5-43 easyrsa3]# cp vars.example vars
[root@ip-172-31-5-43 easyrsa3]# ls
easyrsa  openssl-easyrsa.cnf  vars  vars.example  x509-types
[root@ip-172-31-5-43 easyrsa3]# vi vars
```

4)$ vi vars # open this vars file and remove # from this following lines.
and add the following Key lines

set_var EASYRSA_REQ_COUNTRY “NL”
set_var EASYRSA_REQ_PROVINCE “FLEVOLAND”
set_var EASYRSA_REQ_CITY “ALMERE”
set_var EASYRSA_REQ_ORG “TECHGROUNDS CERTIFICATE CO”
set_var EASYRSA_REQ_EMAIL “me@example.net”
set_var EASYRSA_REQ_OU “TECHGROUNDS UNIT”
export KEY_NAME=”server”
export KEY_CN=openvpn.yourdomain.com

5)# save and close the vars file.

6)$./easyrsa clean-all #clean up any previous keys and generate the certificate authority

```
[root@ip-172-31-5-43 easyrsa3]# ./easyrsa clean-all

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/pki
```

7) $./easyrsa build-ca #set a CA key passphrase and common name for CA

```
[root@ip-172-31-5-43 easyrsa3]# ./easyrsa build-ca

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/vars
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus
.........................+++
.................+++
e is 65537 (0x10001)
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) [Easy-RSA CA]:Marieke
```

8) $ ./easyrsa build-server-full server #create a key and certificate for the server

```
[root@ip-172-31-5-43 easyrsa3]# ./easyrsa build-server-full server

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/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/easy-rsa-3.0.8/easyrsa3/pki/easy-rsa-4924.pcC104/tmp.Jh1rp9'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/pki/easy-rsa-4924.pcC104/tmp.gFjBlO
Enter pass phrase for /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Feb 23 19:35:28 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated
```

9) $./easyrsa gen-dh # generate Diffie-Hellman key exchange file

```
[root@ip-172-31-5-43 easyrsa3]# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/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
...............................+.........................+.........................+.....
```

10)$./easyrsa build-client-full client1

```
[root@ip-172-31-5-43 easyrsa3]# ./easyrsa build-client-full client1

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/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/easy-rsa-3.0.8/easyrsa3/pki/easy-rsa-1543.40Dn8N/tmp.qOusUu'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/pki/easy-rsa-1543.40Dn8N/tmp.fqkkHr
Enter pass phrase for /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'client1'
Certificate is to be certified until Feb 23 19:39:13 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated
```

11) cd /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/pki #navigate to pki directory

Copy 4 files(keys and certificates files)

- ca.crt
- dh.pem
- ca.key
- server.key

```
[root@ip-172-31-5-43 easyrsa3]# cd
[root@ip-172-31-5-43 ~]# cd /etc/openvpn/easy-rsa/easy-rsa-3.0.8/easyrsa3/pki
[root@ip-172-31-5-43 pki]# ls
ca.crt          dh.pem     index.txt.attr      index.txt.old  openssl-easyrsa.cnf  renewed  revoked              serial
certs_by_serial  index.txt  index.txt.attr.old  issued         private              reqs     safessl-easyrsa.cnf  serial.old
[root@ip-172-31-5-43 pki]# cp ca.crt dh.pem /etc/openvpn
[root@ip-172-31-5-43 pki]# cd private
[root@ip-172-31-5-43 private]# cp ca.key server.key /etc/openvpn
```

12) cp ca.crt dh.pem /etc/openvpn

13) cd private

14) cp ca.key server.key /etc/openvpn

Step 5: Firewall and Routing Configuration
$cd / #back to root directory

$ yum install firewalld #Install firewalld

$systemctl enable firewalld # enable firewalld

$sudo systemctl status firewalld # checking status firewalld

```
[root@ip-172-31-5-43 ~]# yum install firewalld
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
208 packages excluded due to repository priority protections
Resolving Dependencies
--> Running transaction check
```

$ firewalld-cmd –get-active-zones #check active firewalld zone

```
[root@localhost ~]# firewall-cmd --get-active-zone
public
  interfaces: enp0s3
```

$ firewall-cmd --zone=public –add-service openvpn #add openvpn to the list of services firewalld allows within the zone(public)

$firewall-cmd –zone=public –add-service openvpn permanent #openvpn is made permanent

$firewall-cmd –list-services --zone=public #check whether openvpn was added

```
[root@localhost ~]# firewall-cmd --zone=public --add-service openvpn
success
[root@localhost ~]# firewall-cmd --zone=public --add-service openvpn --permanent
success
[root@localhost ~]# firewall-cmd --list-services --zone=public
dhcpv6-client openvpn ssh
```

$firewall-cmd –add-masquerade #add masquerade to runtime instance

$firewall-cmd –add-masquerade –permanent #make masquerade permanent

$firewall-cmd –query-masquerade#verify the masquerade added

```
ssh dhcpv6-client openvpn
[root@ip-172-31-5-43 ~]# firewall-cmd --add-masquerade
success
[root@ip-172-31-5-43 ~]# firewall-cmd --add-masquerade --permanent
success
[root@ip-172-31-5-43 ~]# firewall-cmd --query-masquerade
yes
```

Routing the Configuration

1)Create a variable that represents the primary network primary interface used by the server.

VAR=$(ip route get 208.67.222.222 | awk ‘NR==1 {print $(NF-2)}’)

2) Permanently add the routing rule using the variable created.

$firewall-cmd --permanent –direct –passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o $VAR -j MASQUERADE

3) Reload firewalld for the changes

$firewall-cmd –reload

```
[root@ip-172-31-5-43 ~]# VAR=$(ip route get 208.67.222.222 | awk 'NR==1 {print $(NF-2)}')
[root@ip-172-31-5-43 ~]# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o $VAR -j MASQUERADE
success
[root@ip-172-31-5-43 ~]# firewall-cmd --reload
success
[root@ip-172-31-5-43 ~]# vi /etc/sysctl.conf
```

4) vi /etc/sysctl.conf #open sysctl.conf file. Routing all webtraffic from the client to server’s IP address by enabling IP forwarding

5)Add the following line at the top of /etc/sysctl.conf file
net.ipv4.ip_forward = 1

6) Restart the service
$systemctl restart network.service

```
[root@ip-172-31-5-43 ~]# firewall-cmd --reload
success
[root@ip-172-31-5-43 ~]# vi /etc/sysctl.conf
[root@ip-172-31-5-43 ~]# systemctl restart network.service
```

Step 6: Start OpenVPN

1) $ systemctl -f start openvpn@server.service #Start OpenVPN service

```
[root@ip-172-31-5-43 ~]# systemctl -f start openvpn@server.service
Job for openvpn@server.service failed because the control process exited with error code. See "systemctl status openvpn@server.service" and
[root@ip-172-31-5-43 ~]# sysctl -f start openvpn@server.service
sysctl: cannot open "start": No such file or directory
sysctl: cannot open "openvpn@server.service": No such file or directory
[root@ip-172-31-5-43 ~]# sudo systemctl -f start openvpn@server.service
Job for openvpn@server.service failed because the control process exited with error code. See "systemctl status openvpn@server.service" and
```

The openvpn server failed. No idea how to fix this error.