**OPEN VPN (DIAL UP VPN)**

**THREE MACHINE REQUIRED AS GIVEN BELOW**

**OPEN VPN-SERVER (CENTOS7) => NAT (192.168.15.161) & HOST ONLY (10.10.10.134)**

**OPEN VPN-CLIENT (CENTOS7) => NAT (192.168.15.151)**

**WINDOW ON VM => HOST ONLY (10.10.10.133)**

**IN VPN SERVER MACHINE**

[root@server ~]# setenforce 0

setenforce: SELinux is disabled

[root@server ~]# vi /etc/selinux/config

­­ [root@server ~]# cat /proc/sys/net/ipv4/ip\_forward

1

[root@server ~]# vi /etc/sysctl.conf

*# 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@server ~]# cat /proc/sys/net/ipv4/ip\_forward

1

[root@server ~]# yum install epel-release -y

Loaded plugins: fastestmirror, langpacks

Loading mirror speeds from cached hostfile

\* base: bd.mirror.vanehost.com

\* epel: epel.excellmedia.net

\* extras: bd.mirror.vanehost.com

\* updates: bd.mirror.vanehost.com

Resolving Dependencies

--> Running transaction check

---> Package epel-release.noarch 0:7-11 will be updated

---> Package epel-release.noarch 0:7-14 will be an update

--> Finished Dependency Resolution

Dependencies Resolved

================================================================================

Package Arch Version Repository Size

================================================================================

Updating:

epel-release noarch 7-14 epel 15 k

Transaction Summary

================================================================================

Upgrade 1 Package

Total download size: 15 k

Downloading packages:

epel/x86\_64/prestodelta | 641 B 00:00

epel-release-7-14.noarch.rpm | 15 kB 00:00

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Updating : epel-release-7-14.noarch 1/2

Cleanup : epel-release-7-11.noarch 2/2

Verifying : epel-release-7-14.noarch 1/2

Verifying : epel-release-7-11.noarch 2/2

Updated:

epel-release.noarch 0:7-14

Complete!

[root@server ~]# yum install openvpn -y

Loaded plugins: fastestmirror, langpacks

Loading mirror speeds from cached hostfile

\* base: bd.mirror.vanehost.com

\* epel: epel.excellmedia.net

\* extras: bd.mirror.vanehost.com

\* updates: bd.mirror.vanehost.com

Package openvpn-2.4.12-1.el7.x86\_64 already installed and latest version

Nothing to do

[root@server ~]# cd /etc/openvpn/

[root@server openvpn]# wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz

--2023-07-03 16:13:29-- 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%2F20230703%2Fus-east-1%2Fs3%2Faws4\_request&X-Amz-Date=20230703T105155Z&X-Amz-Expires=300&X-Amz-Signature=ad17479e3484ee025c4fdca805763eeb9da42f11eaf7b05523b739cfe579bf6a&X-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 [following]

--2023-07-03 16:13:29-- 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%2F20230703%2Fus-east-1%2Fs3%2Faws4\_request&X-Amz-Date=20230703T105155Z&X-Amz-Expires=300&X-Amz-Signature=ad17479e3484ee025c4fdca805763eeb9da42f11eaf7b05523b739cfe579bf6a&X-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

Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.108.133, 185.199.109.133, ...

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’

100%[======================================>] 40,840 --.-K/s in 0s

2023-07-03 16:13:30 (131 MB/s) - ‘EasyRSA-unix-v3.0.6.tgz’ saved [40840/40840]

[root@server openvpn]# ls

client EasyRSA-unix-v3.0.6.tgz server

[root@server 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

EasyRSA-v3.0.6/doc/EasyRSA-Readme.md

EasyRSA-v3.0.6/doc/EasyRSA-Upgrade-Notes.md

EasyRSA-v3.0.6/doc/Hacking.md

EasyRSA-v3.0.6/doc/Intro-To-PKI.md

EasyRSA-v3.0.6/x509-types/COMMON

EasyRSA-v3.0.6/x509-types/ca

EasyRSA-v3.0.6/x509-types/client

EasyRSA-v3.0.6/x509-types/code-signing

EasyRSA-v3.0.6/x509-types/server

EasyRSA-v3.0.6/x509-types/serverClient

[root@server openvpn]# mv EasyRSA-v3.0.6 easy-rsa

[root@server openvpn]# ls

client easy-rsa EasyRSA-unix-v3.0.6.tgz server

[root@server openvpn]# cd easy-rsa/

[root@server easy-rsa]# vim 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"

[root@server easy-rsa]# ls

ChangeLog easyrsa openssl-easyrsa.cnf vars

COPYING.md gpl-2.0.txt README.md vars.example

doc mktemp.txt README.quickstart.md x509-types

[root@server easy-rsa]# ./easyrsa init-pki

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

init-pki complete; you may now create a CA or requests.

Your newly created PKI dir is: /etc/openvpn/easy-rsa/pki

[root@server easy-rsa]# ./easyrsa build-ca

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

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

Enter New CA Key Passphrase:

Re-Enter New CA Key Passphrase:

Easy-RSA error:

Passphrases do not match.

[root@server easy-rsa]# ./easyrsa build-ca

Note: using Easy-RSA configuration from: ./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]:**actsvpn**

CA creation complete and you may now import and sign cert requests.

Your new CA certificate file for publishing is at:

/etc/openvpn/easy-rsa/pki/ca.crt

[root@server easy-rsa]# ls pki

ca.crt index.txt private reqs safessl-easyrsa.cnf

certs\_by\_serial issued renewed revoked serial

[root@server easy-rsa]# ls pki/private/

ca.key

[root@server easy-rsa]# ./easyrsa gen-req hpcsa1 nopass

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/hpcsa1.key.jjIS5M0QG2'

-----

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) [hpcsa1]:hpcsa1

Keypair and certificate request completed. Your files are:

req: /etc/openvpn/easy-rsa/pki/reqs/hpcsa1.req

key: /etc/openvpn/easy-rsa/pki/private/hpcsa1.key

[root@server easy-rsa]# ls pki/reqs/hpcsa1.req

pki/reqs/hpcsa1.req

[root@server easy-rsa]# cat pki/reqs/hpcsa1.req

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

MIICVjCCAT4CAQAwETEPMA0GA1UEAwwGaHBjc2ExMIIBIjANBgkqhkiG9w0BAQEF

AAOCAQ8AMIIBCgKCAQEA6uOktQFcPFv4nDrSh1zZKunvRvzn+/SLG+AxD+XgP1Vl

VTi3D8hD9ewdzQhMxV6447/tfoYX14oKKXthQW52IQsQxG+yUWvNy5DHGrkw8Nbt

XEA5N1w1kw2XJP+BZerDPtApA1K1bGLVioaI+dHYHTv4WKmHPD9fevIWhdBBelpF

3eimoqD8eC4LRD2du0u8OfNJ4QSE1/WjUk/haRHZJXoDHhKbrf9XO1OzeX8clcIu

/5UeXWXzyC9DlVUrUrvNf8b5CiMDm/nbqQRMRdTqVOjVYjQs+2KxjKfKd8ttkhE6

9YV87bf1FQNzg03nUlspa74JH4yVB4DFSrYNFXHHhwIDAQABoAAwDQYJKoZIhvcN

AQELBQADggEBADoNuv+0+fjhYNoV6MKjPHFNRd8bqnxR33YRcjkJJQghC+WPHxuR

j7JFztdF9s5nOyUaX+1Da2q0BwzEwsPjI/+LueHMGuWiGIT6oabgNg3/HJPQ2uWE

wHc5zTj5XwPAXGw8AN2m1PG2SAktHcWD/ICQfAUaTimW1OcLEmnKiRyouSrjJrQd

e13r5s9mPo0336foGZZ2KN+9Kut/NRsVZNDLRXPplPxYq01pSV4nqfcKHfYeZN4m

VYJBDwwHebjQYye0Tj3XA8+W6isY77bmkZzglc9OMILd1L/EOyue9z5EMC/S00bg

dAdIusmGcElCNCYWWvPgeNOMMzRsZqwwEWo=

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

[root@server 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

Easy-RSA error:

No request found for the input: 'demovpn'

Expected to find the request at: /etc/openvpn/easy-rsa/pki/reqs/demovpn.req

[root@server easy-rsa]# ./easyrsa sign-req server hpcsa1

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 = hpcsa1

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

Confirm request details: yes

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

Enter pass phrase for /etc/openvpn/easy-rsa/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:'hpcsa1'

Certificate is to be certified until Jul 2 10:52:44 2024 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/hpcsa1.crt

[root@server easy-rsa]# cat pki/issued/hpcsa1.crt

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

d3:39:1a:13:85:0c:db:a8:db:59:1d:e6:27:d6:1f:59

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=actsvpn

Validity

Not Before: Jul 3 10:52:44 2023 GMT

Not After : Jul 2 10:52:44 2024 GMT

Subject: CN=hpcsa1

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:ea:e3:a4:b5:01:5c:3c:5b:f8:9c:3a:d2:87:5c:

d9:2a:e9:ef:46:fc:e7:fb:f4:8b:1b:e0:31:0f:e5:

e0:3f:55:65:55:38:b7:0f:c8:43:f5:ec:1d:cd:08:

4c:c5:5e:b8:e3:bf:ed:7e:86:17:d7:8a:0a:29:7b:

61:41:6e:76:21:0b:10:c4:6f:b2:51:6b:cd:cb:90:

c7:1a:b9:30:f0:d6:ed:5c:40:39:37:5c:35:93:0d:

97:24:ff:81:65:ea:c3:3e:d0:29:03:52:b5:6c:62:

d5:8a:86:88:f9:d1:d8:1d:3b:f8:58:a9:87:3c:3f:

5f:7a:f2:16:85:d0:41:7a:5a:45:dd:e8:a6:a2:a0:

fc:78:2e:0b:44:3d:9d:bb:4b:bc:39:f3:49:e1:04:

84:d7:f5:a3:52:4f:e1:69:11:d9:25:7a:03:1e:12:

9b:ad:ff:57:3b:53:b3:79:7f:1c:95:c2:2e:ff:95:

1e:5d:65:f3:c8:2f:43:95:55:2b:52:bb:cd:7f:c6:

f9:0a:23:03:9b:f9:db:a9:04:4c:45:d4:ea:54:e8:

d5:62:34:2c:fb:62:b1:8c:a7:ca:77:cb:6d:92:11:

3a:f5:85:7c:ed:b7:f5:15:03:73:83:4d:e7:52:5b:

29:6b:be:09:1f:8c:95:07:80:c5:4a:b6:0d:15:71:

c7:87

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Subject Key Identifier:

51:CE:C7:1D:78:CC:31:FD:5C:14:E0:0A:F7:8B:97:92:1E:64:73:CA

X509v3 Authority Key Identifier:

keyid:9A:F1:72:05:78:0D:46:40:63:BD:D9:5F:AF:89:95:2E:C8:15:4A:93

DirName:/CN=actsvpn

serial:DD:C5:99:3E:3B:EB:13:33

X509v3 Extended Key Usage:

TLS Web Server Authentication

X509v3 Key Usage:

Digital Signature, Key Encipherment

X509v3 Subject Alternative Name:

DNS:hpcsa1

Signature Algorithm: sha256WithRSAEncryption

a8:5c:df:1b:b6:47:6b:25:db:31:c6:55:cc:bb:a5:4b:cc:99:

08:ee:4b:40:9a:28:32:b0:98:20:28:79:df:a3:69:b5:f8:f6:

98:bc:2e:65:e2:4a:3b:84:84:28:5a:b1:6e:29:fc:e4:ae:f4:

e8:b8:63:44:a6:f9:85:2a:e4:02:da:e3:37:13:b2:b9:4e:02:

ee:07:fa:ac:69:f5:aa:16:60:f3:39:2f:b3:58:29:82:b0:db:

3f:6b:61:94:0f:81:35:d7:dc:57:08:05:d1:2c:f9:ba:0f:6f:

c5:21:a7:6c:44:aa:c5:80:36:8e:22:d9:51:0a:dd:49:09:98:

78:97:d3:8e:7b:7f:d2:b4:b2:cf:57:e7:f3:ed:7e:b2:d8:99:

7f:37:83:92:d9:db:bd:0c:e8:08:4d:77:36:10:ad:04:d5:08:

b7:ed:1e:ef:d5:59:aa:51:b1:d4:68:f9:29:6b:7e:19:14:0e:

7d:5b:c5:17:52:34:d3:8d:54:81:bb:6a:cc:54:e4:1e:9a:0c:

8a:10:26:1a:e1:f5:c9:2a:69:4a:97:ef:43:58:84:1c:a5:8f:

d3:9b:f6:d1:74:ee:2b:5e:82:00:57:d2:ca:07:24:c0:0e:39:

aa:34:2a:67:6f:68:16:91:bf:48:5b:7c:86:d4:20:ad:37:10:

7d:ef:09:47

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

MIIDVTCCAj2gAwIBAgIRANM5GhOFDNuo21kd5ifWH1kwDQYJKoZIhvcNAQELBQAw

EjEQMA4GA1UEAwwHYWN0c3ZwbjAeFw0yMzA3MDMxMDUyNDRaFw0yNDA3MDIxMDUy

NDRaMBExDzANBgNVBAMMBmhwY3NhMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC

AQoCggEBAOrjpLUBXDxb+Jw60odc2Srp70b85/v0ixvgMQ/l4D9VZVU4tw/IQ/Xs

Hc0ITMVeuOO/7X6GF9eKCil7YUFudiELEMRvslFrzcuQxxq5MPDW7VxAOTdcNZMN

lyT/gWXqwz7QKQNStWxi1YqGiPnR2B07+Fiphzw/X3ryFoXQQXpaRd3opqKg/Hgu

C0Q9nbtLvDnzSeEEhNf1o1JP4WkR2SV6Ax4Sm63/VztTs3l/HJXCLv+VHl1l88gv

Q5VVK1K7zX/G+QojA5v526kETEXU6lTo1WI0LPtisYynynfLbZIROvWFfO239RUD

c4NN51JbKWu+CR+MlQeAxUq2DRVxx4cCAwEAAaOBpjCBozAJBgNVHRMEAjAAMB0G

A1UdDgQWBBRRzscdeMwx/VwU4Ar3i5eSHmRzyjBCBgNVHSMEOzA5gBSa8XIFeA1G

QGO92V+viZUuyBVKk6EWpBQwEjEQMA4GA1UEAwwHYWN0c3ZwboIJAN3FmT476xMz

MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIFoDARBgNVHREECjAIggZo

cGNzYTEwDQYJKoZIhvcNAQELBQADggEBAKhc3xu2R2sl2zHGVcy7pUvMmQjuS0Ca

KDKwmCAoed+jabX49pi8LmXiSjuEhChasW4p/OSu9Oi4Y0Sm+YUq5ALa4zcTsrlO

Au4H+qxp9aoWYPM5L7NYKYKw2z9rYZQPgTXX3FcIBdEs+boPb8Uhp2xEqsWANo4i

2VEK3UkJmHiX0457f9K0ss9X5/PtfrLYmX83g5LZ270M6AhNdzYQrQTVCLftHu/V

WapRsdRo+SlrfhkUDn1bxRdSNNONVIG7asxU5B6aDIoQJhrh9ckqaUqX70NYhByl

j9Ob9tF07iteggBX0soHJMAOOao0KmdvaBaRv0hbfIbUIK03EH3vCUc=

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

[root@client easy-rsa]# openssl verify -CAfile pki/ca.crt pki/issued/hpcsa1.crt

pki/issued/hpcsa1.crt: OK

[root@server 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

....................................................................................................................................................................................................................+....................................................................................................+.......................................................................................................................................................+.........................................................................................................................................................................................................++\*++\*

DH parameters of size 2048 created at /etc/openvpn/easy-rsa/pki/dh.pem

[root@server easy-rsa]# cp pki/ca.crt /etc/openvpn/server/

[root@server easy-rsa]# cp pki/dh.pem /etc/openvpn/server/

[root@server easy-rsa]# cp pki/private/hpcsa1.key /etc/openvpn/server/

[root@server easy-rsa]# cp pki/issued/hpcsa1.crt /etc/openvpn/server/

[root@server easy-rsa]# ./easyrsa gen-req client nopass

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/client.key.nYw41xF1Xo'

-----

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) [client]:client

Keypair and certificate request completed. Your files are:

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

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

[root@server easy-rsa]# ./easyrsa sign-req client client

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 client certificate for 365 days:

subject=

commonName = client

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

Confirm request details: yes

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

Enter pass phrase for /etc/openvpn/easy-rsa/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:'client'

Certificate is to be certified until Jul 2 11:30:11 2024 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/client.crt

[root@server easy-rsa]# ./easyrsa gen-req jerry nopass

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/jerry.key.two2G7VOsY'

-----

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) [jerry]:jerry

Keypair and certificate request completed. Your files are:

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

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

[root@server easy-rsa]# cp pki/ca.crt /etc/openvpn/client/

[root@server easy-rsa]# ls /etc/openvpn/client/

ca.crt

[root@server easy-rsa]# cp pki/issued/client.crt /etc/openvpn/client/

[root@server easy-rsa]# cp pki/private/client.key /etc/openvpn/client/

[root@server easy-rsa]# ls /etc/openvpn/client/

ca.crt client.crt client.key

[root@server easy-rsa]# vi /etc/openvpn/server/server.conf

port 1194

proto udp

dev tun

ca /etc/openvpn/server/ca.crt

cert /etc/openvpn/server/hpcsa1.crt

key /etc/openvpn/server/hpcsa1.key

dh /etc/openvpn/server/dh.pem

server 10.8.0.0 255.255.255.0

push "route 10.10.10.0 255.255.255.0"

#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

[root@server easy-rsa]# systemctl start openvpn-server@server

[root@server easy-rsa]# systemctl enable openvpn-server@server

Created symlink from /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service to /usr/lib/systemd/system/openvpn-server@.service.

[root@server easy-rsa]# systemctl status openvpn-server@server

● openvpn-server@server.service - OpenVPN service for server

Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; vendor preset: disabled)

Active: active (running) since Mon 2023-07-03 17:06:06 IST; 25s ago

Docs: man:openvpn(8)

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

https://community.openvpn.net/openvpn/wiki/HOWTO

Main PID: 13030 (openvpn)

Status: "Initialization Sequence Completed"

CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service

└─13030 /usr/sbin/openvpn --status /run/openvpn-server/status-serv...

Jul 03 17:06:06 client systemd[1]: Starting OpenVPN service for server...

Jul 03 17:06:06 client systemd[1]: Started OpenVPN service for server.

[root@server easy-rsa]# systemctl start firewalld.service

[root@server easy-rsa]# systemctl enable firewalld.service

[root@server easy-rsa]# firewall-cmd --permanent --add-service=openvpn

success

[root@server easy-rsa]# firewall-cmd --permanent --zone=trusted --add-service=openvpn

success

[root@server easy-rsa]# firewall-cmd --permanent --zone=trusted --add-interface=tun0

success

[root@server easy-rsa]# firewall-cmd --add-masquerade

success

[root@server easy-rsa]# firewall-cmd --permanent --add-masquerade

success

[root@server easy-rsa]# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24 -o ens33 -j MASQUERADE

success

[root@server easy-rsa]# firewall-cmd --reload

success

[root@server easy-rsa]# vim /etc/openvpn/client/client.ovpn

[root@server easy-rsa]# cat /etc/openvpn/client/client.ovpn

client

dev tun

proto udp

remote 192.168.15.161 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

[root@server easy-rsa]# scp -r /etc/openvpn/client/ root@192.168.15.151:/root

The authenticity of host '192.168.15.151 (192.168.15.151)' can't be established.

ECDSA key fingerprint is SHA256:idQrcsHLX9HtMVnUqB2hqBWFnWyj2wXVvye26WSXTIY.

ECDSA key fingerprint is MD5:88:41:f4:ab:26:f2:91:47:d3:d9:ed:a7:08:6a:96:9f.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.15.151' (ECDSA) to the list of known hosts.

root@192.168.15.151's password:

ca.crt 100% 1155 1.5MB/s 00:00

client.crt 100% 4412 5.7MB/s 00:00

client.key 100% 1704 3.6MB/s 00:00

client.ovpn 100% 406 945.6KB/s 00:00

[root@server easy-rsa]# cd /etc/openvpn/server/

[root@server server]# vi server.conf

[root@server server]# cat server.conf

port 1194

proto udp

dev tun

ca /etc/openvpn/server/ca.crt

cert /etc/openvpn/server/hpcsa1.crt

key /etc/openvpn/server/hpcsa1.key

dh /etc/openvpn/server/dh.pem

server 10.8.0.0 255.255.255.0

push "route 10.10.10.0 255.255.255.0"

#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

[root@server server]# systemctl restart openvpn-server@server

[root@server server]# systemctl status openvpn-server@server

● openvpn-server@server.service - OpenVPN service for server

Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; vendor preset: disabled)

Active: active (running) since Mon 2023-07-03 17:15:08 IST; 8s ago

Docs: man:openvpn(8)

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

https://community.openvpn.net/openvpn/wiki/HOWTO

Main PID: 13329 (openvpn)

Status: "Initialization Sequence Completed"

CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service

└─13329 /usr/sbin/openvpn --status /run/openvpn-server/status-serv...

Jul 03 17:15:08 client systemd[1]: Stopped OpenVPN service for server.

Jul 03 17:15:08 client systemd[1]: Starting OpenVPN service for server...

Jul 03 17:15:08 client systemd[1]: Started OpenVPN service for server.

**ON CLIENT MACHINE**

[root@master ~]# 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:29:69:cb:51 brd ff:ff:ff:ff:ff:ff

inet 192.168.15.151/24 brd 192.168.15.255 scope global noprefixroute dynamic ens33

valid\_lft 1561sec preferred\_lft 1561sec

inet6 fe80::3d22:895a:a56a:4b06/64 scope link noprefixroute

valid\_lft forever preferred\_lft forever

3: 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::cd7f:48bd:4cb2:b9b5/64 scope link flags 800

valid\_lft forever preferred\_lft forever

4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000

link/ether 52:54:00:16:df:82 brd ff:ff:ff:ff:ff:ff

inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0

valid\_lft forever preferred\_lft forever

5: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo\_fast master virbr0 state DOWN group default qlen 1000

link/ether 52:54:00:16:df:82 brd ff:ff:ff:ff:ff:ff

[root@master ~]# yum install epel-release

[root@master ~]# yum install openvpn –y

[root@master ~]# ping 10.10.10.133

PING 10.10.10.133 (10.10.10.133) 56(84) bytes of data.

64 bytes from 10.10.10.133: icmp\_seq=1 ttl=128 time=0.904 ms

64 bytes from 10.10.10.133: icmp\_seq=2 ttl=128 time=1.86 ms

64 bytes from 10.10.10.133: icmp\_seq=3 ttl=128 time=0.787 ms

^C

--- 10.10.10.133 ping statistics ---

3 packets transmitted, 3 received, 0% packet loss, time 2005ms

rtt min/avg/max/mdev = 0.787/1.183/1.860/0.482 ms

[root@master ~]# ping 10.10.10.133

connect: Network is unreachable

[root@master ~]# cd client/

[root@master client]# ll

total 20

-rw------- 1 root root 1155 Jul 3 17:12 ca.crt

-rw------- 1 root root 4412 Jul 3 17:12 client.crt

-rw------- 1 root root 1704 Jul 3 17:12 client.key

-rw-r--r-- 1 root root 406 Jul 3 17:12 client.ovpn

[root@master client]# openvpn --config client.ovpn

Mon Jul 3 17:19:03 2023 OpenVPN 2.4.12 x86\_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar 17 2022

Mon Jul 3 17:19:03 2023 library versions: OpenSSL 1.0.2k-fips 26 Jan 2017, LZO 2.06

Mon Jul 3 17:19:03 2023 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.

Mon Jul 3 17:19:03 2023 TCP/UDP: Preserving recently used remote address: [AF\_INET]192.168.15.161:1194

Mon Jul 3 17:19:03 2023 Socket Buffers: R=[212992->212992] S=[212992->212992]

Mon Jul 3 17:19:03 2023 UDP link local: (not bound)

Mon Jul 3 17:19:03 2023 UDP link remote: [AF\_INET]192.168.15.161:1194

Mon Jul 3 17:19:03 2023 TLS: Initial packet from [AF\_INET]192.168.15.161:1194, sid=1a00049c 13c500f8

Mon Jul 3 17:19:03 2023 VERIFY OK: depth=1, CN=actsvpn

Mon Jul 3 17:19:03 2023 VERIFY OK: depth=0, CN=hpcsa1

Mon Jul 3 17:19:03 2023 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA

Mon Jul 3 17:19:03 2023 [hpcsa1] Peer Connection Initiated with [AF\_INET]192.168.15.161:1194

Mon Jul 3 17:19:05 2023 SENT CONTROL [hpcsa1]: 'PUSH\_REQUEST' (status=1)

Mon Jul 3 17:19:05 2023 PUSH: Received control message: 'PUSH\_REPLY,route 10.10.10.0 255.255.255.0,route 10.8.0.1,topology net30,ping 20,ping-restart 60,ifconfig 10.8.0.6 10.8.0.5,peer-id 0,cipher AES-256-GCM'

Mon Jul 3 17:19:05 2023 OPTIONS IMPORT: timers and/or timeouts modified

Mon Jul 3 17:19:05 2023 OPTIONS IMPORT: --ifconfig/up options modified

Mon Jul 3 17:19:05 2023 OPTIONS IMPORT: route options modified

Mon Jul 3 17:19:05 2023 OPTIONS IMPORT: peer-id set

Mon Jul 3 17:19:05 2023 OPTIONS IMPORT: adjusting link\_mtu to 1625

Mon Jul 3 17:19:05 2023 OPTIONS IMPORT: data channel crypto options modified

Mon Jul 3 17:19:05 2023 Data Channel: using negotiated cipher 'AES-256-GCM'

Mon Jul 3 17:19:05 2023 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key

Mon Jul 3 17:19:05 2023 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key

Mon Jul 3 17:19:05 2023 ROUTE: default\_gateway=UNDEF

Mon Jul 3 17:19:05 2023 TUN/TAP device tun1 opened

Mon Jul 3 17:19:05 2023 TUN/TAP TX queue length set to 100

Mon Jul 3 17:19:05 2023 /sbin/ip link set dev tun1 up mtu 1500

Mon Jul 3 17:19:05 2023 /sbin/ip addr add dev tun1 local 10.8.0.6 peer 10.8.0.5

Mon Jul 3 17:19:05 2023 /sbin/ip route add 10.10.10.0/24 via 10.8.0.5

Mon Jul 3 17:19:05 2023 /sbin/ip route add 10.8.0.1/32 via 10.8.0.5

Mon Jul 3 17:19:05 2023 Initialization Sequence Completed

Mon Jul 3 18:19:03 2023 VERIFY OK: depth=1, CN=actsvpn

Mon Jul 3 18:19:03 2023 VERIFY OK: depth=0, CN=hpcsa1

Mon Jul 3 18:19:03 2023 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key

Mon Jul 3 18:19:03 2023 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key

Mon Jul 3 18:19:03 2023 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA