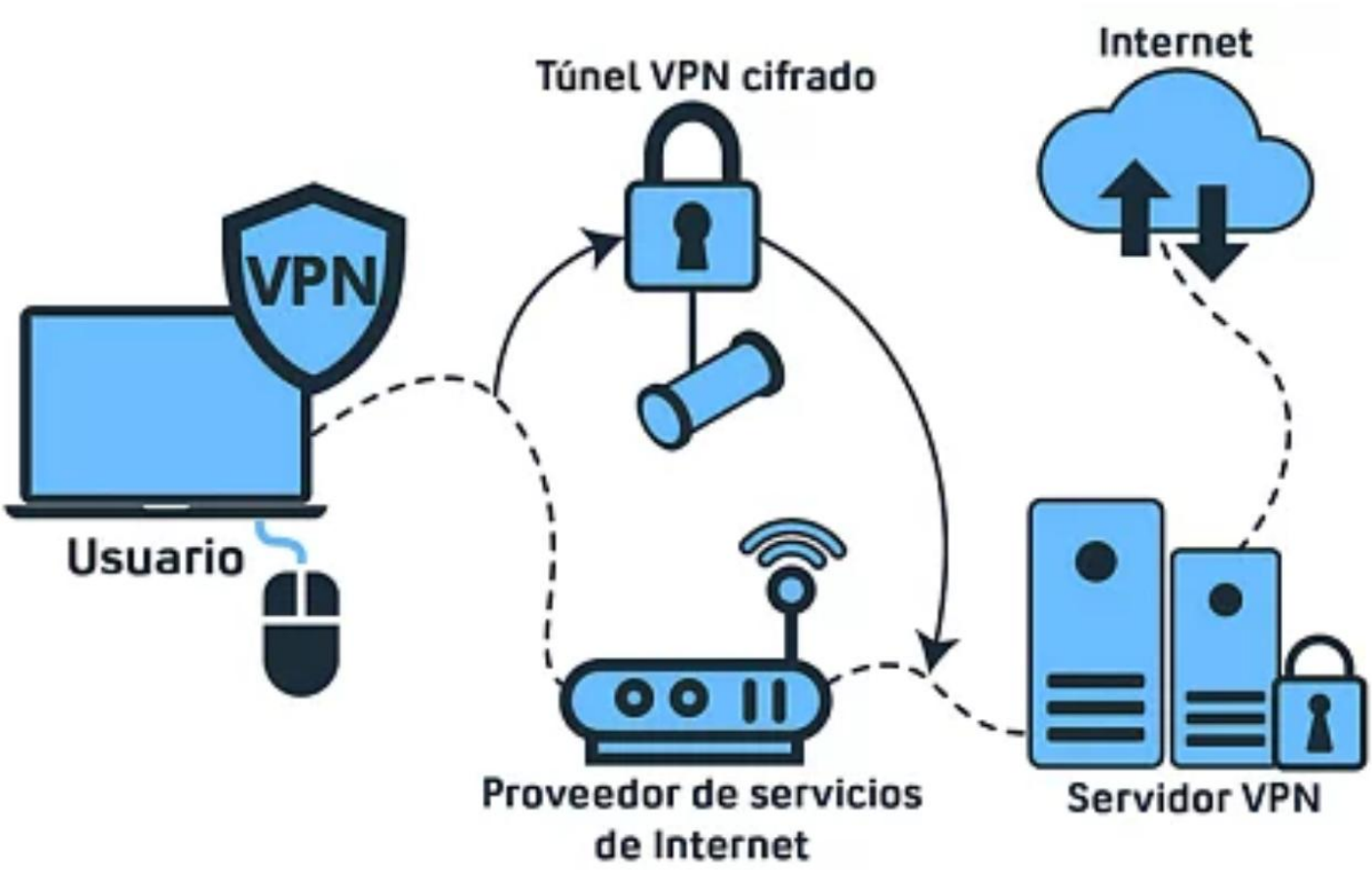


Ivana Sánchez Pérez

GUÍA RÁPIDA DE COMANDOS Y CONTENIDO DE ARCHIVOS PARA LA CONFIGURACIÓN DE VPN.

1. **Actualizar el sistema:**

   apt update

   apt upgrade

2. **Instalar OpenVPN y Easy-RSA:**

   apt install openvpn

   apt install easy-rsa

3. **Configurar Easy-RSA:**

   cp -r /usr/share/easy-rsa /etc/

   cd /etc/easy-rsa

   ./easyrsa init-pki

   ./easyrsa build-ca

   ./easyrsa gen-dh

   ./easyrsa build-server-full server nopass

   openvpn --genkey secret /etc/easy-rsa/pki/ta.key

   ./easyrsa gen-crl

4. **Copiar archivos de configuración y certificados:**

   cp -rp /etc/easy-rsa/pki/{ca.crt,dh.pem,ta.key,crl.pem,issued,private} /etc/openvpn/server/

5. **Crear certificado para el cliente:**

   ./easyrsa build-client-full clientname nopass

   mkdir -p /etc/openvpn/client/clientname

   cp -rp /etc/easy-rsa/pki/{ca.crt,issued/clientname.crt,private/clientname.key} /etc/openvpn/client/clientname/

6. **Configurar el servidor OpenVPN:**

   cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn/server/

   cp /etc/openvpn/server/server.conf /etc/openvpn/server/server.conf.bak

   Contenido del archivo server.conf : nano /etc/openvpn/server/server.conf

   port 1194

   proto udp

   dev tun

   ca ca.crt

   cert issued/server.crt

   key private/server.key

   dh dh.pem

   topology subnet

   server 172.16.0.0 255.255.0.0

   push "redirect-gateway def1 bypass-dhcp"

   push "dhcp-option DNS 208.67.222.222"

   push "dhcp-option DNS 208.67.220.220"

   client-to-client

   keepalive 10 120

   tls-auth ta.key 0

   cipher AES-256-CBC

   persist-key

   persist-tun

   status /var/log/openvpn/openvpn-status.log

   log-append /var/log/openvpn/openvpn.log

   verb 3

   explicit-exit-notify 1

   auth SHA512

7. **Habilitar el reenvío de IP:**

   sed -i 's/#net.ipv4.ip_forward=1/net.ipv4.ip_forward=1/' /etc/sysctl.conf

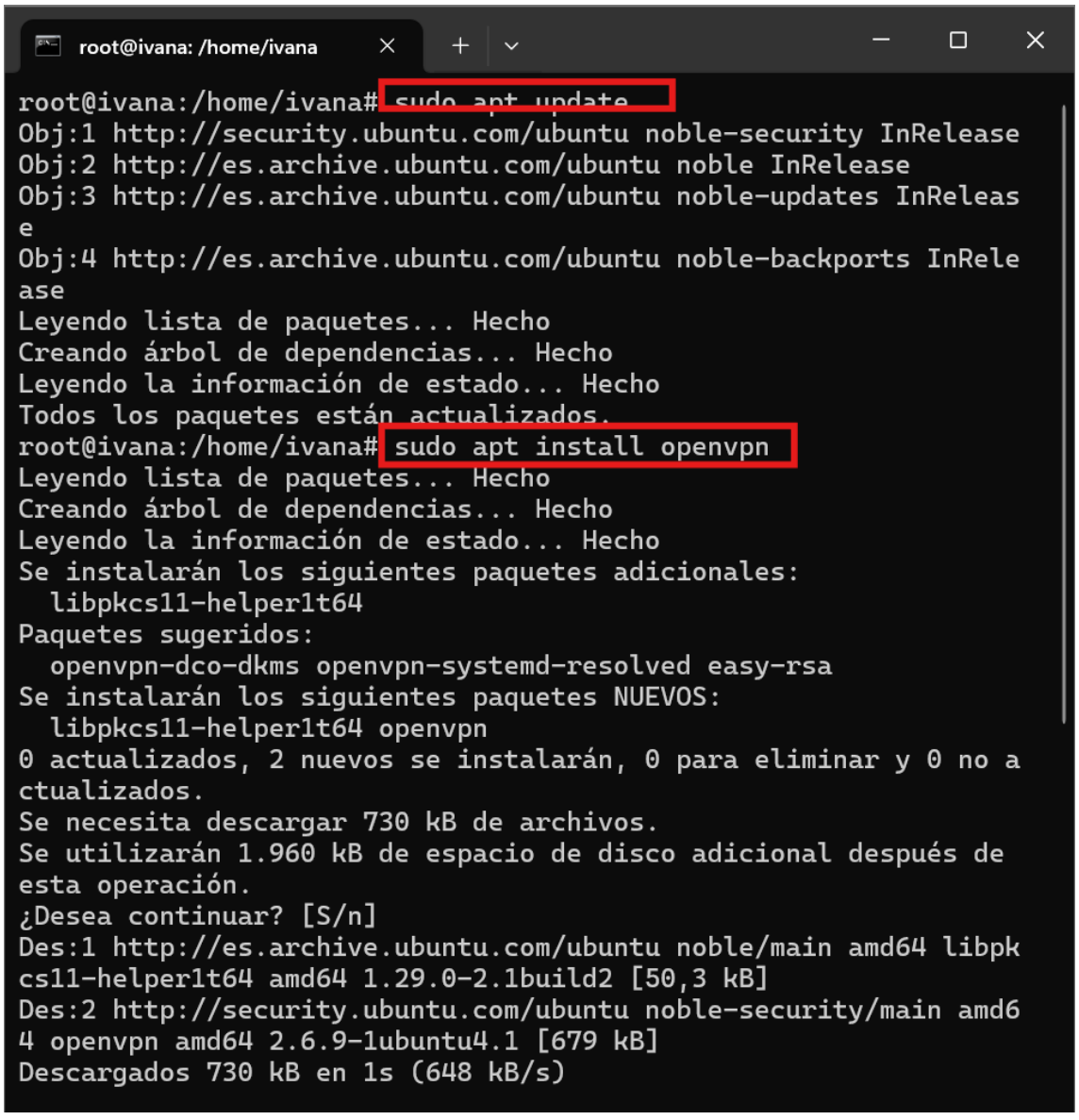
   sysctl --system

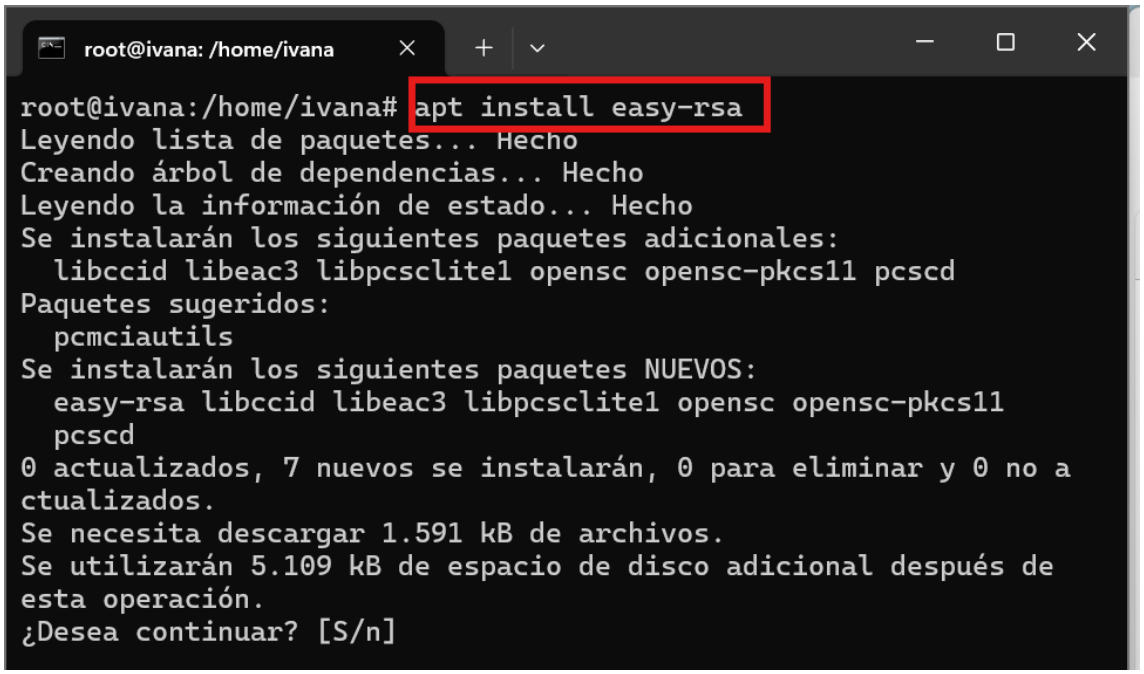
8. **Verificar la ruta de red:**

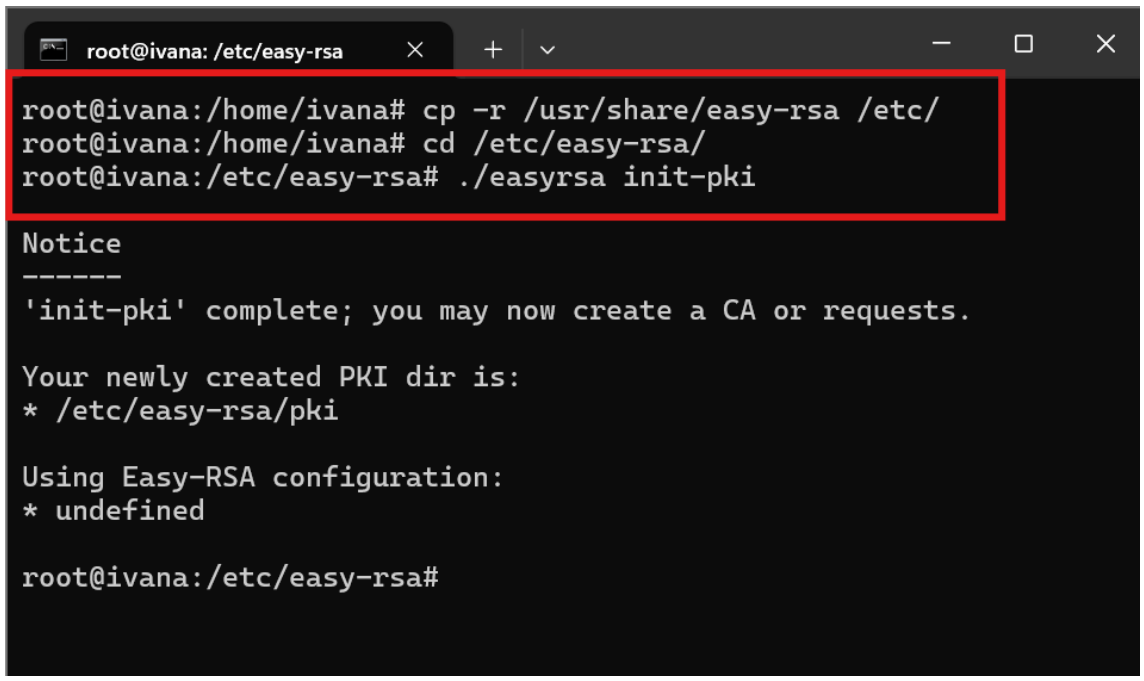
   ip route get 8.8.8.8

9. **Habilitar e iniciar el servicio OpenVPN:**

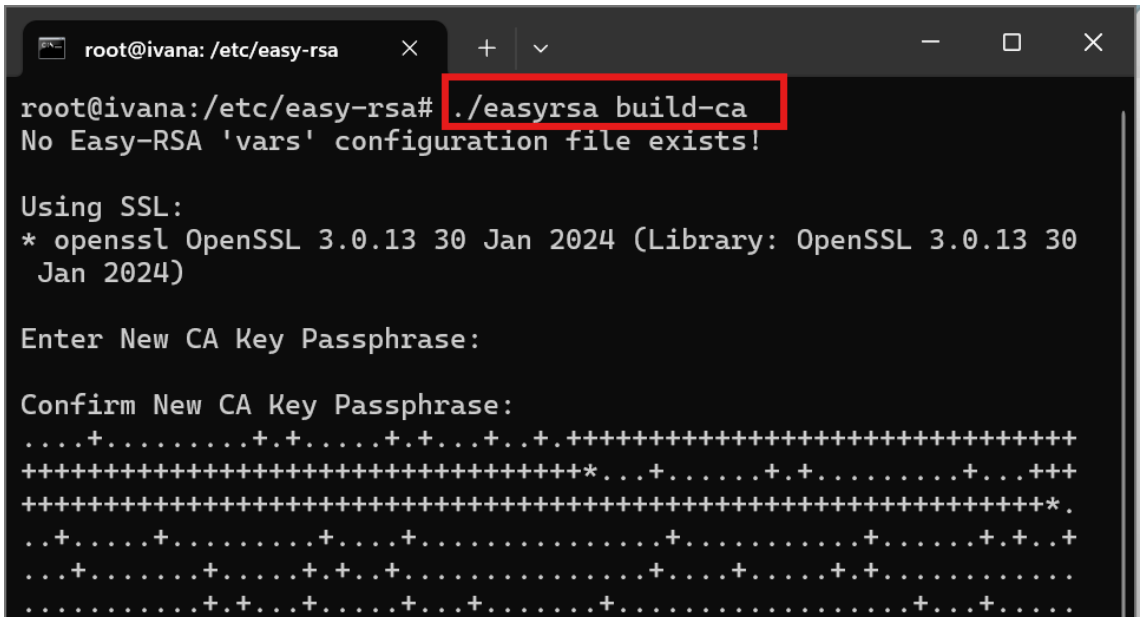
   systemctl enable --now openvpn-server@server

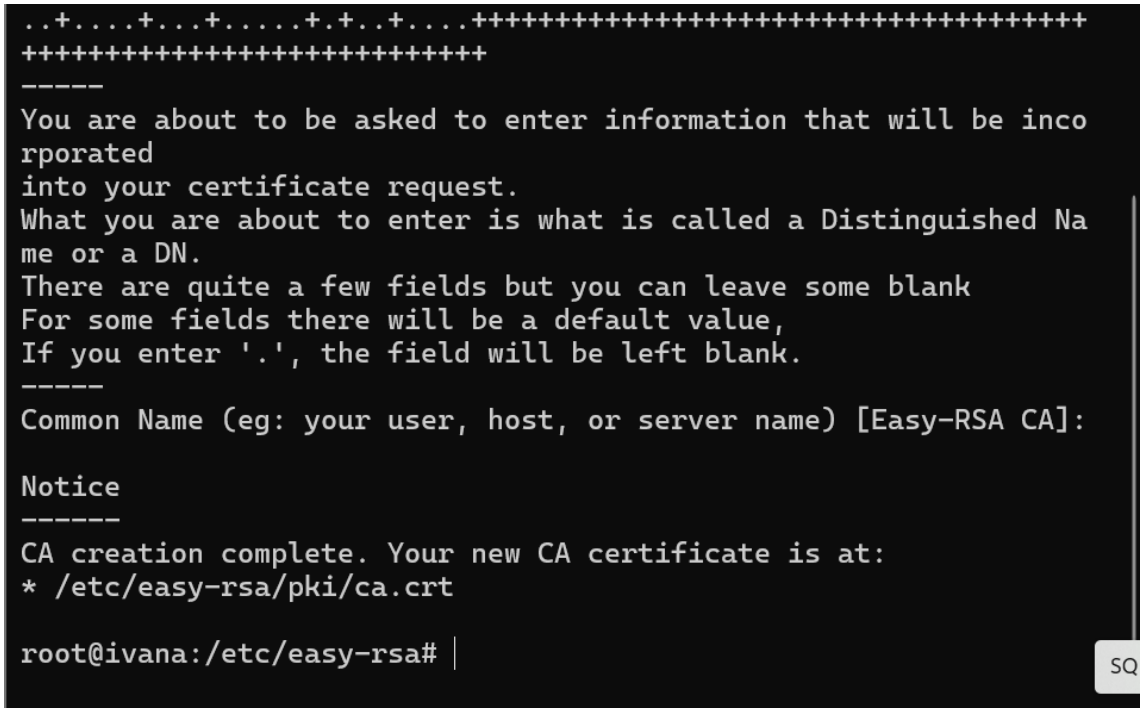



root@ivana: /home/ivana
root@ivana:/home/ivana# apt install easy-rsa
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
libccid libeac3 libpcsclite1 opensc opensc-pkcs11 pcscd
Paquetes sugeridos:
pcmciautils
Se instalarán los siguientes paquetes NUEVOS:
easy-rsa libccid libeac3 libpcsclite1 opensc opensc-pkcs11
pcscd
0 actualizados, 7 nuevos se instalarán, 0 para eliminar y 0 no a
ctualizados.
Se necesita descargar 1.591 kB de archivos.
Se utilizarán 5.109 kB de espacio de disco adicional después de
esta operación.
¿Desea continuar? [S/n]


root@ivana: /etc/easy-rsa
root@ivana:/home/ivana# cp -r /usr/share/easy-rsa /etc/
root@ivana:/home/ivana# cd /etc/easy-rsa/
root@ivana:/etc/easy-rsa# ./easyrsa init-pki
Notice

'init-pki' complete; you may now create a CA or requests.
Your newly created PKI dir is:
* /etc/easy-rsa/pki
Using Easy-RSA configuration:
* undefined
root@ivana:/etc/easy-rsa#

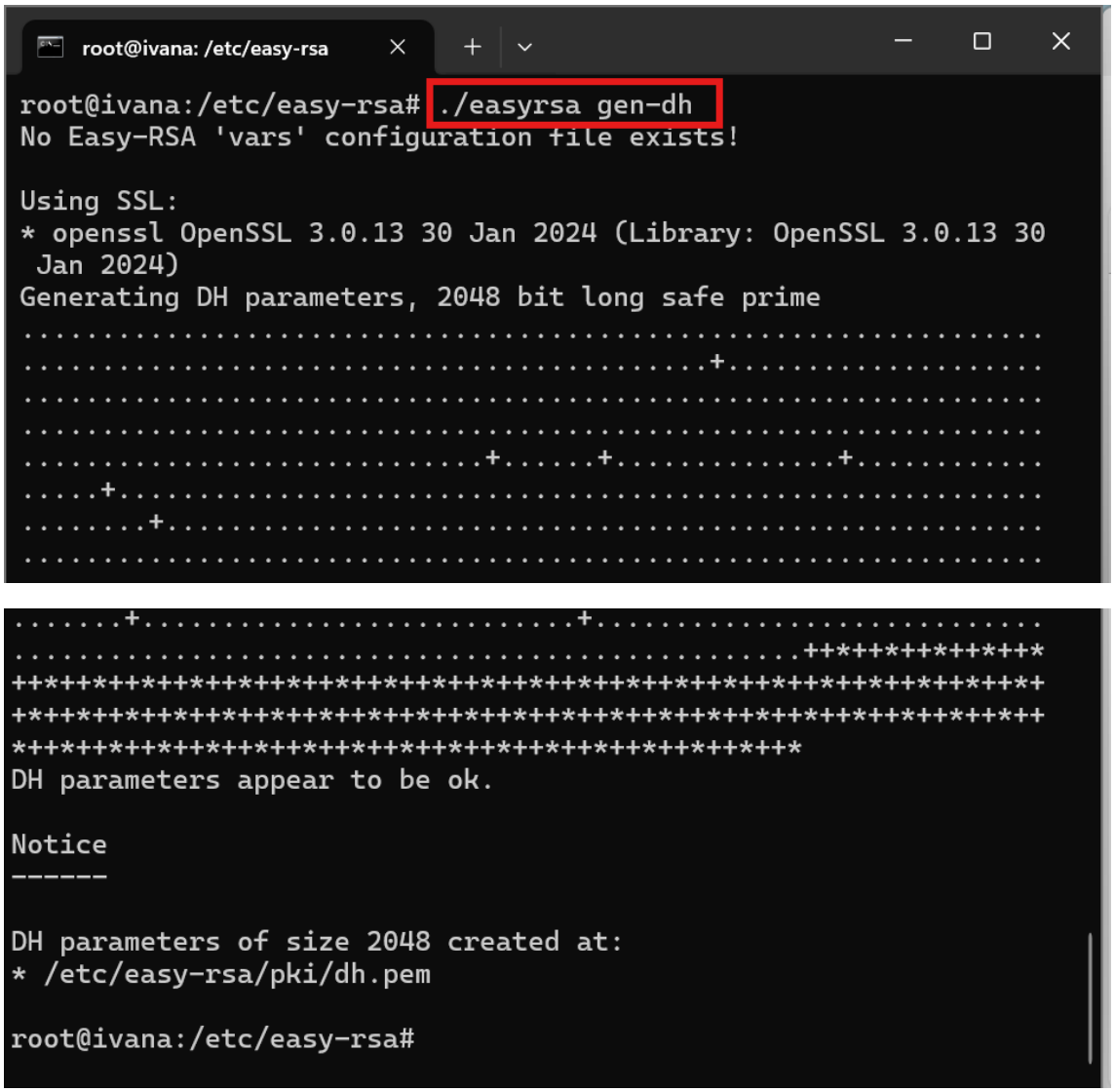

root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# ./easyrsa build-ca
No Easy-RSA 'vars' configuration file exists!
Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
Enter New CA Key Passphrase:
Confirm New CA Key Passphrase:

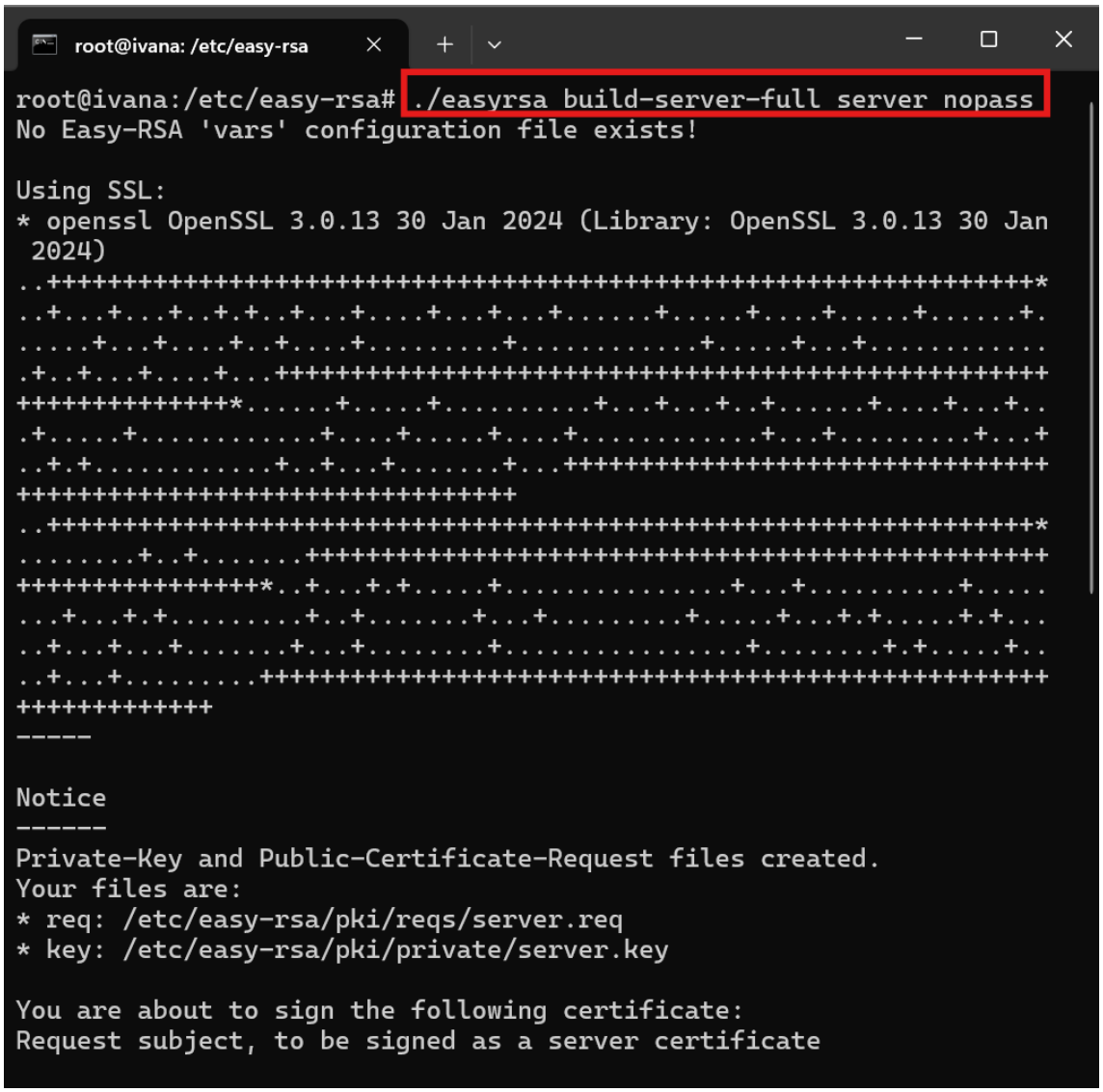


You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Common Name (eg: your user, host, or server name) [Easy-RSA CA]:
Notice

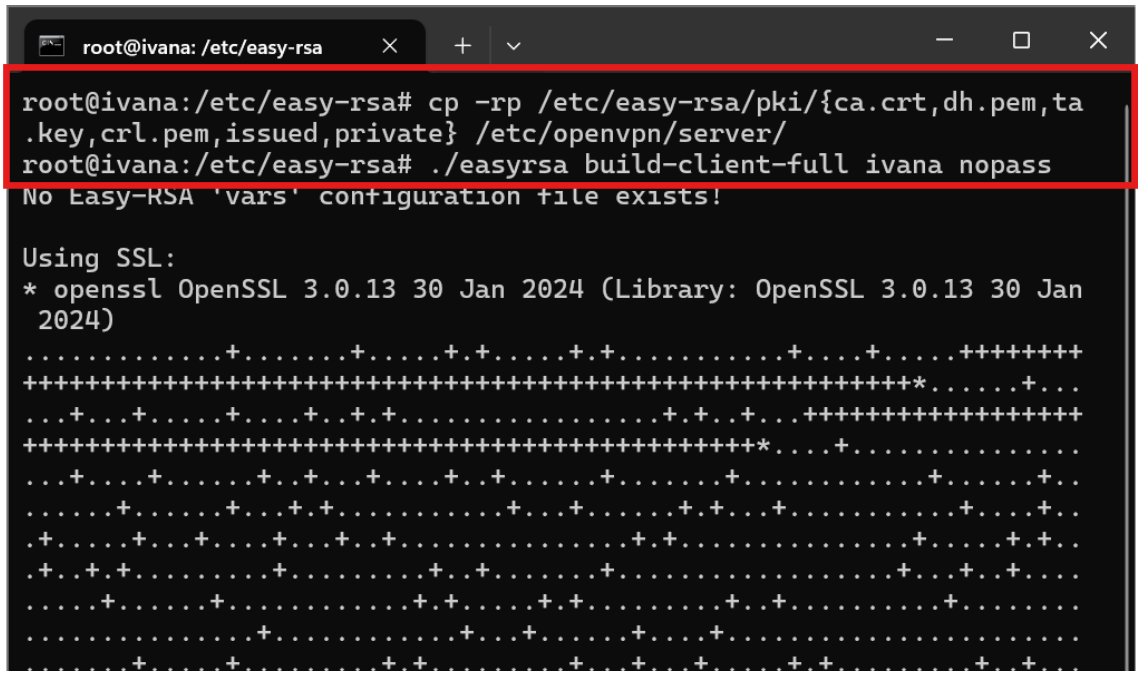
CA creation complete. Your new CA certificate is at:
* /etc/easy-rsa/pki/ca.crt
root@ivana:/etc/easy-rsa#

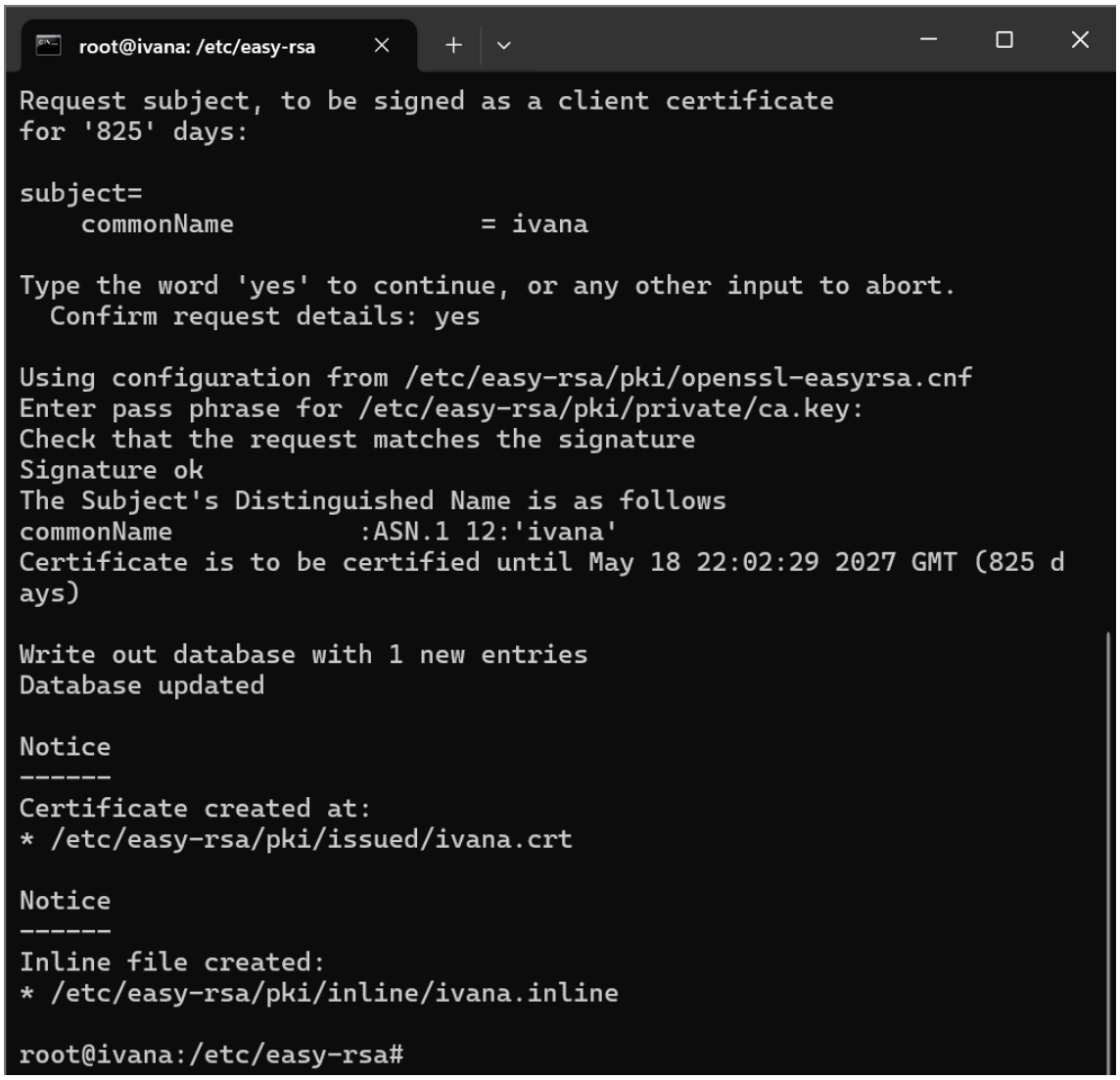

root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# ./easyrsa gen-dh
No Easy-RSA 'vars' configuration file exists!
Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
Generating DH parameters, 2048 bit long safe prime
DH parameters appear to be ok.
Notice
DH parameters of size 2048 created at:
* /etc/easy-rsa/pki/dh.pem
root@ivana:/etc/easy-rsa#

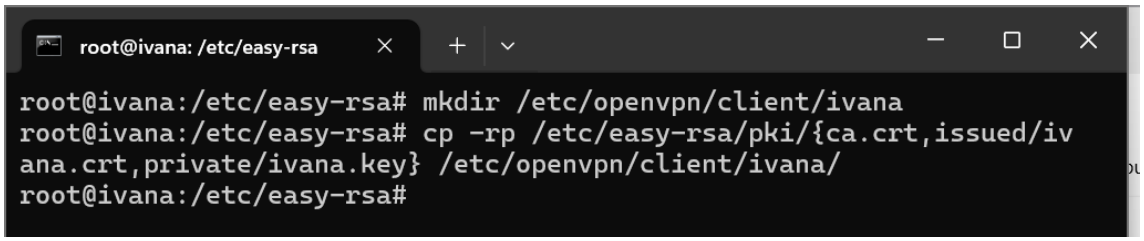

root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# ./easyrsa build-server-full server nopass
No Easy-RSA 'vars' configuration file exists!
Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
Notice
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /etc/easy-rsa/pki/reqs/server.req
* key: /etc/easy-rsa/pki/private/server.key
You are about to sign the following certificate:
Request subject, to be signed as a server certificate

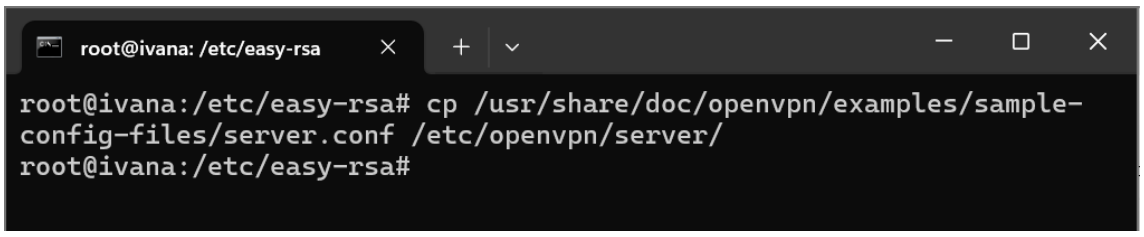
```
You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:

subject=
    commonName                = server
                           yes
Type the word 'yes' to continue, or any other input to abort.
Using configuration from /etc/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/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:'server'
Certificate is to be certified until May 18 21:54:37 2027 GMT (825 d
ays)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* /etc/easy-rsa/pki/issued/server.crt

Notice
------
Inline file created:
* /etc/easy-rsa/pki/inline/server.inline

root@ivana:/etc/easy-rsa#
```

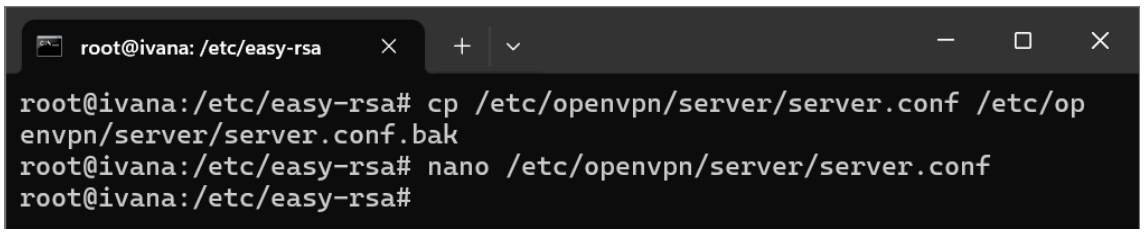
```
root@ivana: /etc/easy-rsa

root@ivana:/etc/easy-rsa# openvpn --genkey secret /etc/easy-rsa/pki/
ta.key
root@ivana:/etc/easy-rsa# ./easyrsa gen-crl
No Easy-RSA 'vars' configuration file exists!

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan
 2024)
Using configuration from /etc/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/easy-rsa/pki/private/ca.key:

Notice
------
An updated CRL has been created:
* /etc/easy-rsa/pki/crl.pem

root@ivana:/etc/easy-rsa#
```

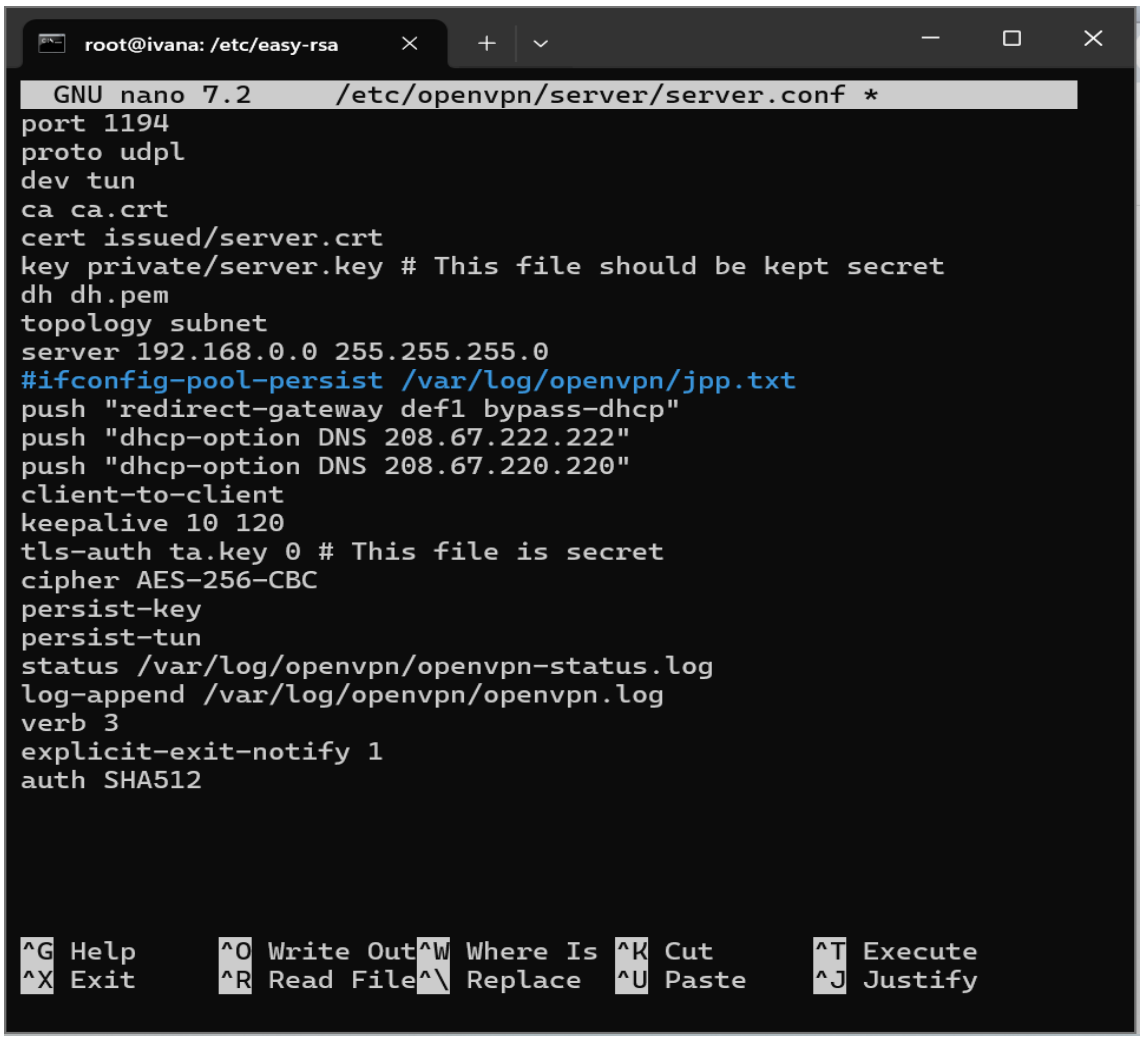

root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# cp -rp /etc/easy-rsa/pki/{ca.crt,dh.pem,ta
.key,crl.pem,issued,private} /etc/openvpn/server/
root@ivana:/etc/easy-rsa# ./easyrsa build-client-full ivana nopass
No Easy-RSA 'vars' configuration file exists!
Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan
2024)


root@ivana: /etc/easy-rsa
Request subject, to be signed as a client certificate
for '825' days:
subject=
commonName = ivana
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /etc/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/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:'ivana'
Certificate is to be certified until May 18 22:02:29 2027 GMT (825 d
ays)
Write out database with 1 new entries
Database updated
Notice
Certificate created at:
* /etc/easy-rsa/pki/issued/ivana.crt
Notice
Inline file created:
* /etc/easy-rsa/pki/inline/ivana.inline
root@ivana:/etc/easy-rsa#


root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# mkdir /etc/openvpn/client/ivana
root@ivana:/etc/easy-rsa# cp -rp /etc/easy-rsa/pki/{ca.crt,issued/iv
ana.crt,private/ivana.key} /etc/openvpn/client/ivana/
root@ivana:/etc/easy-rsa#


root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# cp /usr/share/doc/openvpn/examples/sample-
config-files/server.conf /etc/openvpn/server/
root@ivana:/etc/easy-rsa#

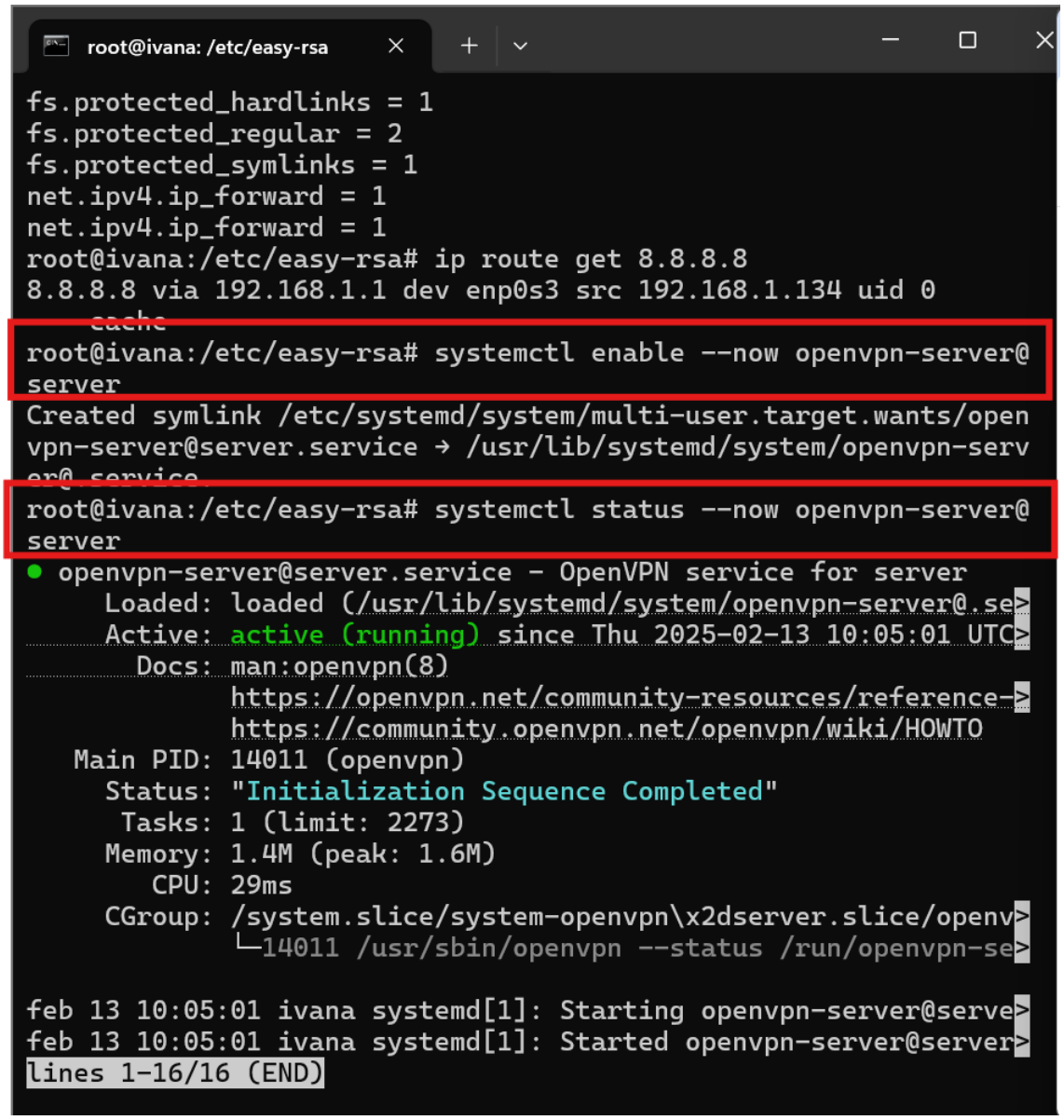

root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# cp /etc/openvpn/server/server.conf /etc/op
envpn/server/server.conf.bak
root@ivana:/etc/easy-rsa# nano /etc/openvpn/server/server.conf
root@ivana:/etc/easy-rsa#


root@ivana: /etc/easy-rsa
GNU nano 7.2 /etc/openvpn/server/server.conf *
port 1194
proto udpl
dev tun
ca ca.crt
cert issued/server.crt
key private/server.key # This file should be kept secret
dh dh.pem
topology subnet
server 192.168.0.0 255.255.255.0
#ifconfig-pool-persist /var/log/openvpn/jpp.txt
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"
client-to-client
keepalive 10 120
tls-auth ta.key 0 # This file is secret
cipher AES-256-CBC
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
verb 3
explicit-exit-notify 1
auth SHA512
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

```
root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# sed -i 's/#net.ipv4.ip_forward=1/net.ipv4.
ip_forward=1/' /etc/sysctl.conf
root@ivana:/etc/easy-rsa#
```

```
root@ivana: /etc/easy-rsa
ip_forward=1/' /etc/sysctl.conf
root@ivana:/etc/easy-rsa# sysctl --system
* Applying /usr/lib/sysctl.d/10-apparmor.conf ...
* Applying /etc/sysctl.d/10-console-messages.conf ...
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
* Applying /etc/sysctl.d/10-map-count.conf ...
* Applying /etc/sysctl.d/10-network-security.conf ...
* Applying /etc/sysctl.d/10-ptrace.conf ...
* Applying /etc/sysctl.d/10-zeropage.conf ...
* Applying /usr/lib/sysctl.d/50-pid-max.conf ...
* Applying /usr/lib/sysctl.d/99-protect-links.conf ...
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.conf ...
kernel.apparmor_restrict_unprivileged_userns = 1
kernel.printk = 4 4 1 7
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
kernel.kptr_restrict = 1
kernel.sysrq = 176
vm.max_map_count = 1048576
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.all.rp_filter = 2
kernel.yama.ptrace_scope = 1
vm.mmap_min_addr = 65536
kernel.pid_max = 4194304
fs.protected_fifos = 1
fs.protected_hardlinks = 1
fs.protected_regular = 2
fs.protected_symlinks = 1
net.ipv4.ip_forward = 1
```

```
root@ivana: /etc/easy-rsa
root@ivana:/etc/easy-rsa# ip route get 8.8.8.8
8.8.8.8 via 192.168.0.1 dev enp0s3 src 192.168.0.32 uid 0
    cache
root@ivana:/etc/easy-rsa#
```


root@ivana: /etc/easy-rsa
fs.protected_hardlinks = 1
fs.protected_regular = 2
fs.protected_symlinks = 1
net.ipv4.ip_forward = 1
net.ipv4.ip_forward = 1
root@ivana:/etc/easy-rsa# ip route get 8.8.8.8
8.8.8.8 via 192.168.1.1 dev enp0s3 src 192.168.1.134 uid 0
cache
root@ivana:/etc/easy-rsa# systemctl enable --now openvpn-server@server
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service → /usr/lib/systemd/system/openvpn-server@.service.
root@ivana:/etc/easy-rsa# systemctl status --now openvpn-server@server
● openvpn-server@server.service - OpenVPN service for server
Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.se>
Active: active (running) since Thu 2025-02-13 10:05:01 UTC>
Docs: man:openvpn(8)
https://openvpn.net/community-resources/reference->
https://community.openvpn.net/openvpn/wiki/HOWTO
Main PID: 14011 (openvpn)
Status: "Initialization Sequence Completed"
Tasks: 1 (limit: 2273)
Memory: 1.4M (peak: 1.6M)
CPU: 29ms
CGroup: /system.slice/system-openvpn\x2dserver.slice/openv>
└─14011 /usr/sbin/openvpn --status /run/openvpn-se>
feb 13 10:05:01 ivana systemd[1]: Starting openvpn-server@serve>
feb 13 10:05:01 ivana systemd[1]: Started openvpn-server@server>
lines 1-16/16 (END)

- ***CA.CRT***

```
root@ivana:/etc/easy-rsa# cat /etc/easy-rsa/pki/ca.crt
-----BEGIN CERTIFICATE-----
MIIDSzCCAjOgAwIBAgIUNxnWP8u/92caPpIofioPFgTwF2YwDQYJKoZIhvcNAQEL
BQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjUwMjIwMjMyNzA2WhcNMzUw
MjE4MjMyNzA2WjAWMRQwEgYDVQQDDAtFYXN5LVJTQSBDQTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALN+2Ux0Uwb2PMF/VcQmoj0JBTVM4fsK/em1qJpH
Yu+UBx26x3uXX129UjKiJsDPkGUnsllWzfyd5ZhXsJ8LiF3riPWts4yENsQTKX+k
a0dJBLHscohJrerjyEh1l/XSZoITCpugXwdK8+IPCK0mm0SePHNX6brSWfKqCLB4
H7RF99N7/opwuCC3uOojklMg7iOQTDUFqKN9jqHfrGjgP+tneiq5y/3xiN62SKZU
KPn7PVokygfUl+mE8t1/dgVb+viYypTMuajuxHAlCTlwS4QyHlNUWQZeBUiCRmwl
jwUKSWVUD7ZJKG/g4jbVjh62EfMNeixxOSOGhzaSsxLM8DECAwEAAaOBkDCBjTAd
BgNVHQ4EFgQUIaa7SQpyz+tFV0ORjJ2iDBqWbHowUQYDVR0jBEowSIAUIaa7SQpy
z+tFV0ORjJ2iDBqWbHqhGqQYMBYxFDASBgNVBAMMC0Vhc3ktUlNBIENBghQ3GdY/
y7/3Zxo+kih+Kg8WBPAXZjAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjANBgkq
hkiG9w0BAQsFAAOCAQEAgiuL6xiMMYUj8ivpWXdUdJjp0V2N4UYye2ka70hZLR1d
6qppAG175zJcx6RJkvw+ZCWbmahHuIPOSZVuOpve2pj8sJqKLaGHx/UVsctcREtd
SmmcDDp8CZIoYNVP3modp1BCLZDj/XAeJOvOW+72xEBnCZejy34e3ydFDqMbERuN
AHxwZ+u6Tq01X7lMcyQYtwaoTruN26Tj54ks1hbLMcTSL2RtYpZ6/tMWlnqCY5rr
UXpyTl8hMg12lh2qb8hl35AQnmL2ymjSPIEPuE2UIo0bruLiwXyqTr+3h1HntNoe
f1VDT2RbGpX/9AIxrHF7i40/BlR3+LwHv+12/r56Xw==
-----END CERTIFICATE-----
root@ivana:/etc/easy-rsa#
```

- ***CLIENTE1.CRT***

```
root@ivana:/etc/easy-rsa# cat /etc/easy-rsa/pki/issued/clientnam
e.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            82:a0:a5:3c:76:ce:d1:15:ad:f9:53:8b:98:2a:00:0b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Easy-RSA CA
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

82:a0:a5:3c:76:ce:d1:15:ad:f9:53:8b:98:2a:00:0b

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Easy-RSA CA

Validity

Not Before: Feb 20 23:35:26 2025 GMT

Not After : May 26 23:35:26 2027 GMT

Subject: CN=clientname

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:b8:dc:b0:0f:9b:80:d2:24:0e:e4:f3:59:3f:85:

44:ce:2e:eb:ab:43:1e:b6:14:49:e0:7b:e4:bd:42:

6c:97:c7:2f:71:46:94:25:0f:10:57:3a:42:68:49:

1b:78:bb:29:71:39:25:38:f9:67:be:74:9d:aa:7f:

02:a6:86:df:b3:0e:17:22:f7:aa:9d:03:cc:aa:9d:

5d:cf:fe:9f:9d:f9:e9:20:ef:90:15:c2:e9:c9:cc:

fc:30:c8:7f:0a:da:2b:8b:0a:bb:53:71:2e:96:3d:

9f:d7:1c:66:d4:46:4b:41:56:5a:f0:94:b7:33:1a:

6d:a1:5e:2c:98:58:e3:a3:70:f4:6b:55:8f:d8:f0:

a8:7a:af:28:6f:cf:73:54:76:b1:1e:ce:f3:af:05:

8b:44:94:3f:77:e3:5a:e9:7c:ee:c5:9a:67:91:33:

2a:b2:2b:92:f6:30:01:c8:f2:6b:a9:6b:23:c1:a9:

b9:a7:d4:41:d8:59:d5:a5:49:3c:e8:31:6b:09:72:

ea:3f:15:53:c3:6c:68:ae:cd:61:90:87:96:36:b4:

85:04:b8:1b:ad:77:49:1d:ac:10:4f:e6:3f:3c:0a:

ba:4e:9b:de:10:4c:eb:c3:32:16:81:46:49:2c:69:

22:fd:20:98:45:dc:19:f9:ce:b9:2b:de:09:ab:5a:

ab:95

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Subject Key Identifier:

39:4A:CB:A9:F8:FB:8A:C5:E5:16:0E:9E:A4:E2:A4:25:8A:07:E9:2F

X509v3 Authority Key Identifier:

keyid:21:A6:BB:49:0A:72:CF:EB:45:57:43:91:8C:9D:A2:0C:1A:96:6C:7A

DirName:/CN=Easy-RSA CA

serial:37:19:D6:3F:CB:BF:F7:67:1A:3E:92:28:7E:2A:0F:16:04:F0:17:66

X509v3 Extended Key Usage:

TLS Web Client Authentication

X509v3 Key Usage:

Digital Signature

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

7b:1e:48:d4:64:53:8a:e6:4a:70:c9:19:cf:8e:30:a5:4f:98:

43:13:a2:4d:91:de:35:52:77:90:cb:4a:17:a4:bd:4c:72:97:

35:fb:b6:64:a8:88:af:c1:f6:0a:3b:4e:26:58:96:96:05:42:

77:20:73:a1:19:fc:53:5c:7e:8b:7e:5b:1b:5a:26:24:21:38:

ae:2d:c3:ad:80:89:e6:35:a9:1c:0a:d7:cc:4c:9e:f9:06:42:

3c:b0:ae:ba:cb:b9:36:db:2a:9b:e5:c1:ad:52:70:d7:b9:55:

2b:cb:e2:cd:7c:ca:e5:a9:07:3e:b3:16:cb:30:69:50:3d:90:

6b:88:1a:c9:87:09:29:ad:4d:ff:52:f4:53:e2:4b:fd:0f:f4:

62:5b:d5:0f:21:3f:0f:40:43:60:d4:ec:3f:51:56:ef:fe:23:

26:f3:34:1d:9c:b9:d1:b8:92:1c:55:d2:a1:b7:7a:94:d6:e8:

08:38:15:63:b4:72:e6:2f:b9:94:6c:5b:bf:f8:8f:af:3d:13:

bf:bc:02:2f:e8:0d:f5:84:1c:68:a8:56:fe:29:ab:b3:31:fc:

d7:44:71:ff:70:3d:bb:08:df:fc:a8:d6:7c:08:a7:9c:dd:88:

d3:80:83:26:1d:a8:bd:ef:97:05:3e:c1:91:28:51:39:11:87:

55:85:c1:13

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

MIIDWTCCAkGgAwIBAgIRAIKgpTx2ztEVrflTi5gqAAswDQYJKoZIhvcNAQELBQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjUwMjIwMjMzNTI2WhcNMjcwNTI2MjMzNTI2WjAVMRMwEQYDVQQDDApjbGllbnRuYW1lMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuNywD5uA0iQO5PNZP4VEzi7rq0MethRJ4HvkvUJsl8cvcUaUJQ8QVzpCaEkbeLspcTklOPlnvnSdqn8Cpobfsw4XIveqnQPMqp1dz/6fnfnpIO+QFcLpycz8MMh/Ctoriwq7U3Eulj2f1xxm1EZLQVZa8JS3MxptoV4smFjjo3D0a1WP2PCoeq8ob89zVHaxHs7zrwWLRJQ/d+Na6XzuxZpnkTMqsiuS9jAByPJrqWsjwam5p9RB2FnVpUk86DFrCXLqPxVTw2xors1hkIeWNrSFBLgbrXdJHawQT+Y/PAq6TpveEEzrwzIWgUZJLGki/SCYRdwZ+c65K94Jq1qrlQIDAQABo4GiMIGfMAkGA1UdEwQCMAAwHQYDVR0OBBYEFDlKy6n4+4rF5RYOnqTipCWKB+kvMFEGA1UdIwRKMEiAFCGmu0kKcs/rRVdDkYydogwalmx6oRqkGDAWMRQwEgYDVQQDDAtFYXN5LVJTQSBDQYIUNxnWP8u/92caPpIofioPFgTwF2YwEwYDVR0lBAwwCgYIKwYBBQUHAwIwCwYDVR0PBAQDAgeAMA0GCSqGSIb3DQEBCwUAA4IBAQB7HkjUZFOK5kpwyRnPjjClT5hDE6JNkd41UneQy0oXpL1Mcpc1+7ZkqIivwfYKO04mWJaWBUJ3IHOhGfxTXH6LflsbWiYkITiuLcOtgInmNakcCtfMTJ75Bkl8sK66y7k22yqb5cGtUnDXuVUry+LNfMrlqQc+sxbLMGlQPZBriBrJhwkprU3/UvRT4kv9D/RiW9UPIT8PQENg1Ow/UVbv/iMm8zQdnLnRuJIcVdKht3qU1ugIOBVjtHLmL7mUbFu/+I+vPRO/vAIv6A31hBxoqFb+KauzMfzXRHH/cD27CN/8qNZ8CKec3YjTgIMmHai975cFPsGRKFE5EYdVhcET

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

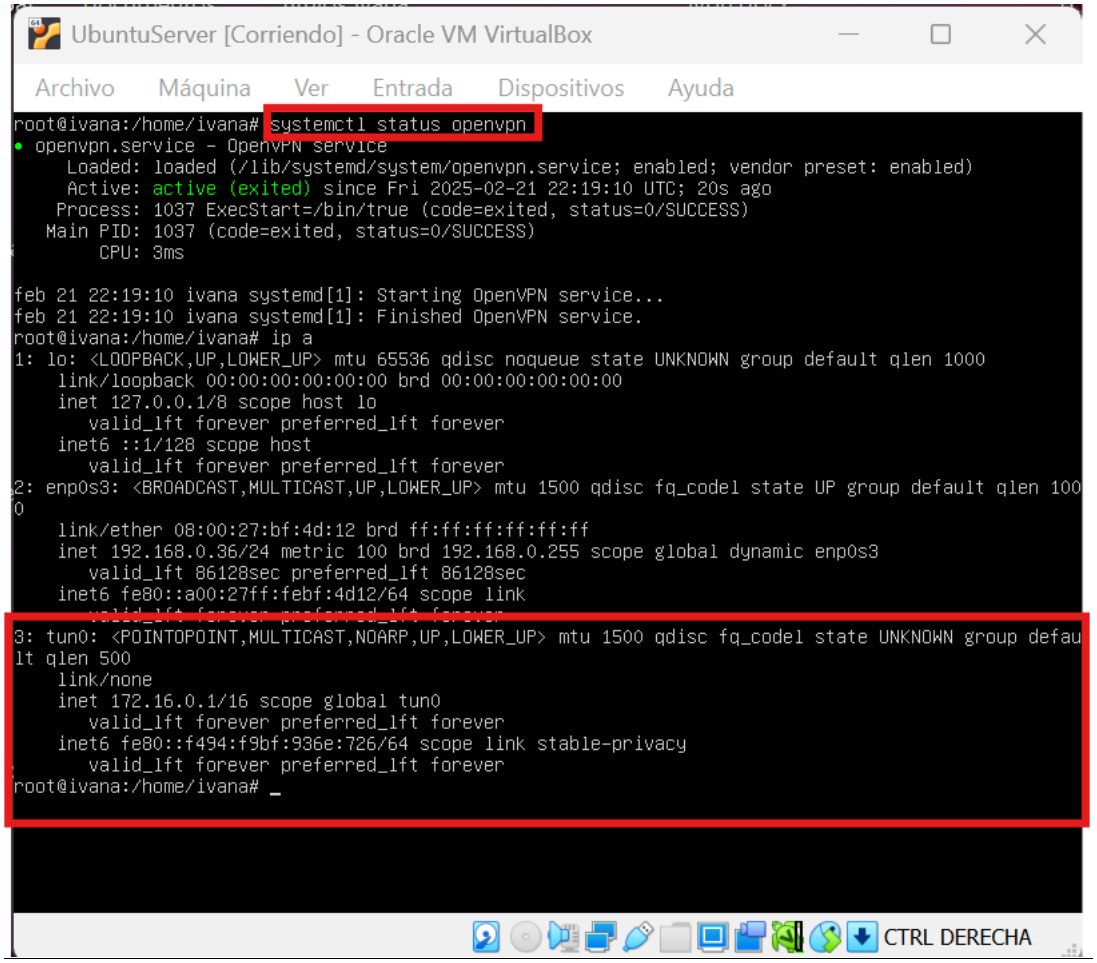
- ***CLIENTE1.KEY***

```
root@ivana:/etc/easy-rsa# cat /etc/easy-rsa/pki/private/clientna
me.key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC43LAPm4DSJA7k
81k/hUTOLuurQx62FEnge+S9QmyXxy9xRpQlDxBXOkJoSRt4uylxOSU4+We+dJ2q
fwKmht+zDhci96qdA8yqnV3P/p+d+ekg75AVwunJzPwwyH8K2iuLCrtTcS6WPZ/X
HGbURktBVlrwlLczGm2hXiyYWOOjcPRrVY/Y8Kh6ryhvz3NUdrEezvOvBYtElD93
41rpfO7FmmeRMyqyK5L2MAHI8mupayPBqbmn1EHYWdWlSTzoMWsJcuo/FVPDbGiu
zWGQh5Y2tIUEuButd0kdrBBP5j88CrpOm94QTOvDMhaBRkksaSL9IJhF3Bn5zrkr
3gmrWquVAgMBAAECggEAOYXqfyDLSBiSTenvRpXIoEP3b3ZWUyAjEOhceAv4UI5Z
k+z7YkC6u/nT+jFti/bpYWL/0yfAgYI2IXyeLYVgjI4A4w+gFnW9NQX80CESOA0w
3t/MvQjGyNWxT9jDt3PGAuEXA1L/xR5t43jiAoHRHwapC52rGArMPF9ajxlx1ERj
8amov0nnbNj3+je89yQFwLAV/CW1GSyvKkNTAmAI/o+K3Ylukwvxi/Db1Hezte3n
RX+PZhnBt4o5CoxqPImM6Z3wS+jcL6zEka48qFNy4p5BZc0NHhVYgROgDMUzNBkg
/AYOhb2dHK48mPrtwXlk7Im8GUtbBUmrAgu3quAbDQKBgQD7HNPzA+ow08gVvxo9
ZMlgtElE8CI5z4dztPRUteFmR58J4why/RnZ+LSScnBDc75jB6LbOfUMMAAL0iw9
tYsEX8hly+ro8OdAz93EGIgqqYUnuBYmEp0GRf8yfYkX3fHSlmQRJ8H/xhzBMXrG
A92Hm+fjpGnhwRfY6RnthPrjqwKBgQC8dcP6F2lg7v3PLRb8ey6qOerxHLcj084j
VYmwutGiJMVudpB/o1zPJfLyCgB0L+FJNsV3ol4zi4ECnmie7U7foxcKv0y2Nf5H
nNHvTzK12pMTSMK2SMK0JL0PBpuRumkIMXHnJbnSqjOvBxEi62VtYp6Eg2zrDFRn
bRL/qLFtvwKBgQDlpdyT722aj+P5N1bo9KZSIS6stCuo0QkgIUodumRTZIamxRFy
D9Q3ioKhN7VBirV/3XjroppfNfqk1OYO3VsweeRMbGv98mqa1D8M2h6VXYjf5TOk
R/uAxDz50OKyiBBitZT4N3Ls1iJv8C9GrjxHi6ZLgo4unqePgMZseOP1lwKBgHQK
SzZVbgRKg6sqR0oFCxGzgc8ecEG2K+ojxBk2nteorow6ovSEgSPnaPTRZcAkryHm
gKYOKtSwJCqZoS+iTPt0rz5l1fUnv78Wd0lTyZSh1gd8uK+Gk6RaLrLuzaFoVz29
PDYoS4fEVviBcHLA4H3+yD4tskX0HJBmX9ldZIp/AoGAGqPryaiyKOzlepVJNP42
h/VaaC6MvwupX+D1RKpTIcC+2ZLx+OiEEKtsxLj1PXsFqEOKKJrVV9GBJ1fmXPyE
/fJmqWQLlR6CMjPZMjXzjikAqWCbYnr1RKirvopbZ5VQzkMDpHvizRtAdLRWzZLw
peIpIpUz3CXTyyTPSmiGszM=
-----END PRIVATE KEY-----
root@ivana:/etc/easy-rsa#
```

- ***TA.KEY***

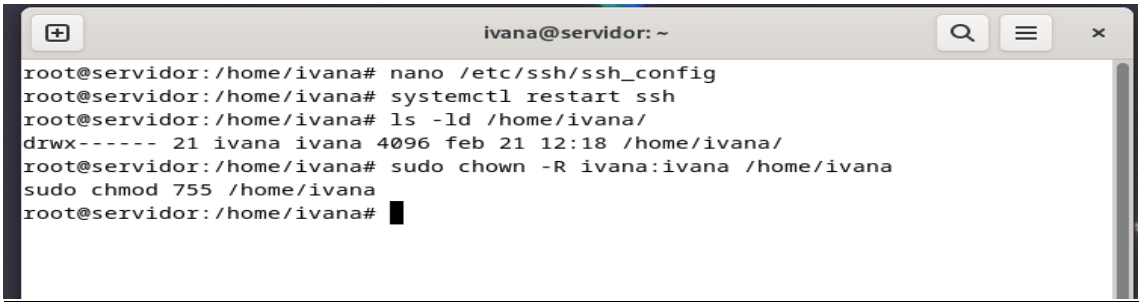
```
root@ivana:/etc/easy-rsa# cat /etc/easy-rsa/pki/ta.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
f2551e653c5f61eeafc462e6af448677
a56fe7df62aa1d9dffca5ba419c93b3e
d0a65a206d8bf2f2d32b5fdc8a3173c9
65b2f60e0243258e4db5d9f63d768521
e9acf2d44bad75c431ffbdea1f2098ea
e208c0a4bfbc263e81890df7c55ee503
8d6cf9a02bece6c2d396a877db5e99da
8c0695751cd7119f29b3e6f10628657e
3616be36e22589b5fec372bef9121463
d685abc755fedbe310ae83e6434e56fc
aa9197475ea56d306be6ee316003c217
0cc21eb6f0b583b309331fce3d673ccf
7c4dd3c196e24748a3b30e8f90a025a9
eb4137173f7c0cb2d1515c1f4420c370
fa69ccdc353cef8be0c9071a055c2733
0a794403ef02699936e2e59d69891db9
-----END OpenVPN Static key V1-----
root@ivana:/etc/easy-rsa#
```

COMPROBACIÓN DEL ESTADO Y DE LA RED E IP

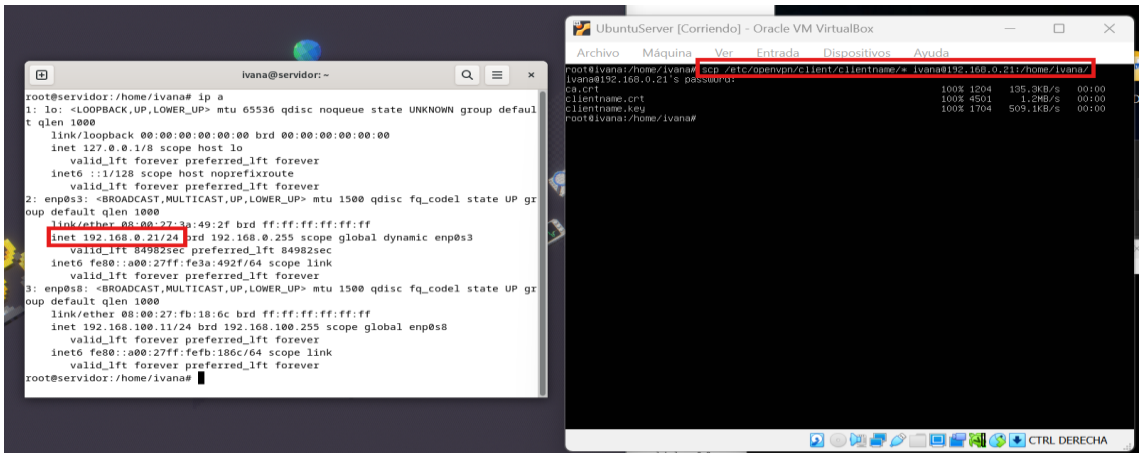


RESOLUCIÓN DE LA ACTIVIDAD

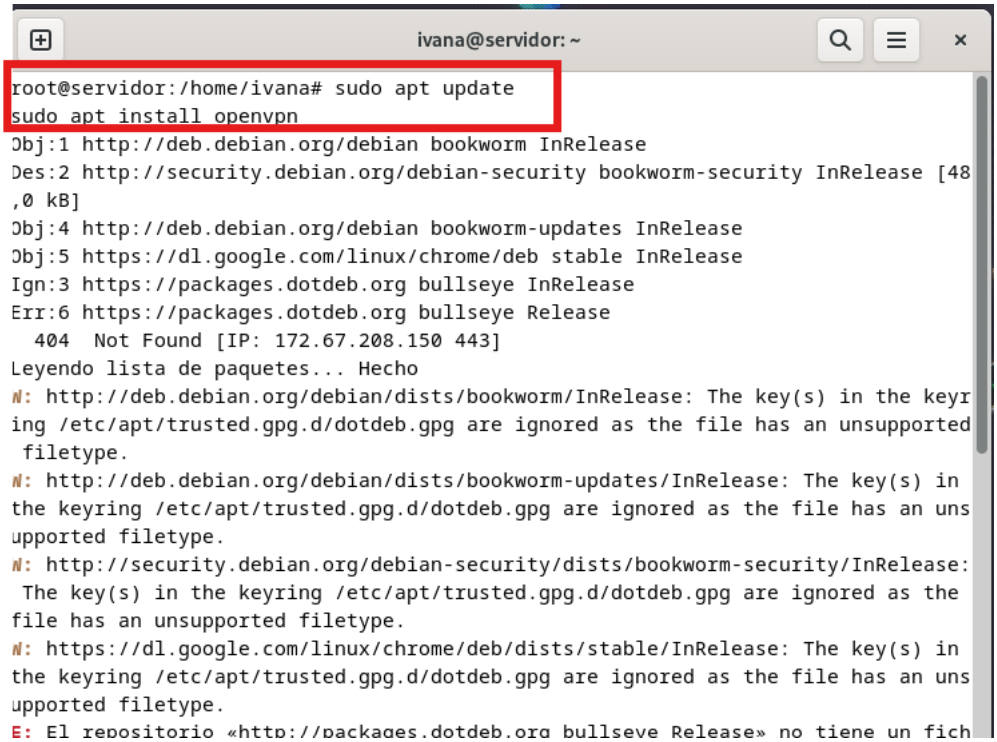
Le doy los permisos necesarios al cliente.



Y procedemos a enviarle los archivos necesarios desde el servidor.

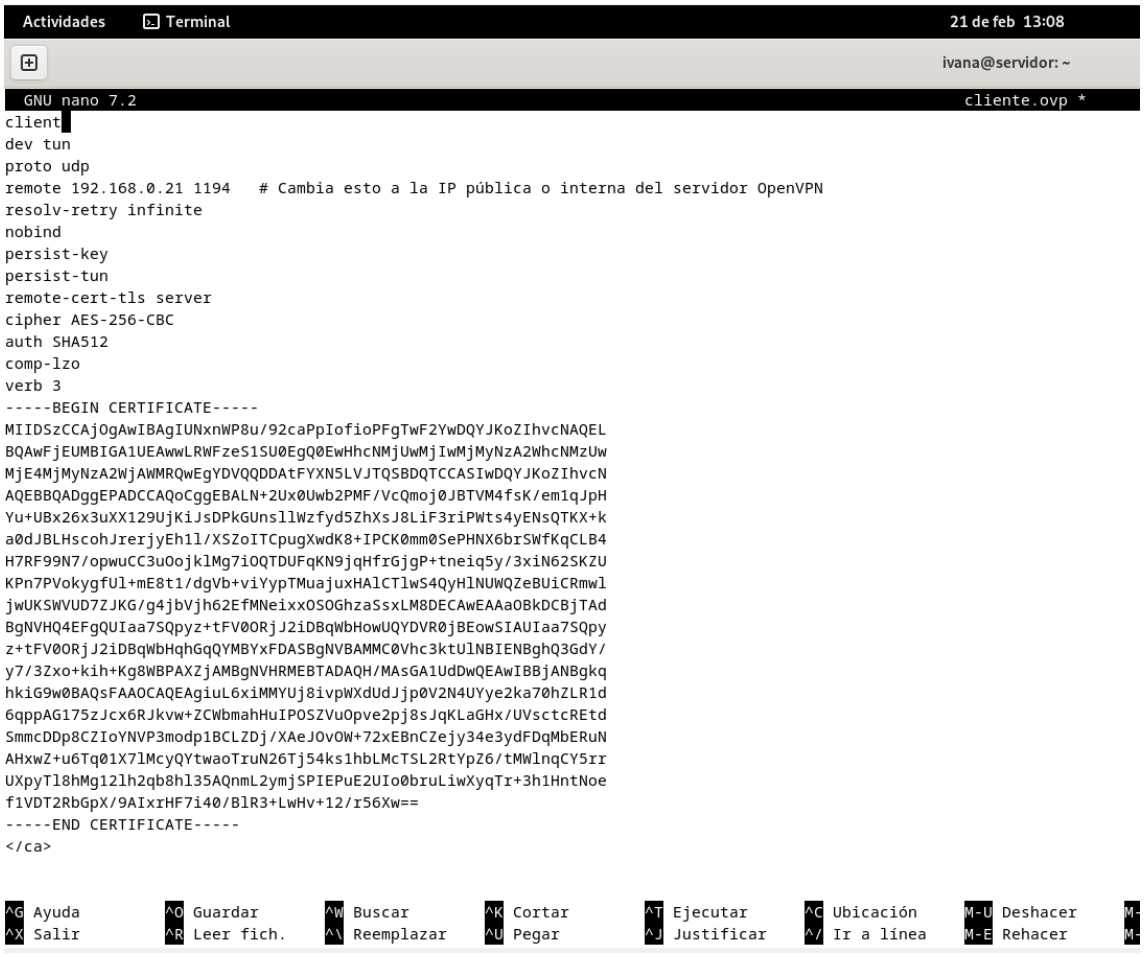


Instalamos openvpn en el cliente



Creamos el archivo clientname.ovpn con las claves que generamos y enviamos al cliente.


ivana@servidor: ~
GNU nano 7.2 /etc/openvpn/clientname.ovpn *
client
dev tun
proto udp
remote 192.168.0.36 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
auth SHA512
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIDSzCCAjOgAwIBAgIUNxnWP8u/92caPpIofioPFgTwF2YwDQYJKoZIhvcNAQEL
BQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjUwMjIwMjMyNzA2WhcNMzUw
MjE4MjMyNzA2WjAWMRQwEgYDVQQDDAtFYXN5LVJTQSBDQTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALN+2Ux0Uwb2PMF/VcQmoj0JBTVM4fsK/em1qJpH
Yu+UBx26x3uXX129UjKiJsDPkGUnsllWzfyd5ZhXsJ8LiF3riPWts4yENsQTKX+k
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^/ Ir a línea


Actividades
Terminal
21 de feb 13:08
ivana@servidor: ~
GNU nano 7.2 cliente.ovp *
client
dev tun
proto udp
remote 192.168.0.21 1194 # Cambia esto a la IP pública o interna del servidor OpenVPN
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
auth SHA512
comp-lzo
verb 3
-----BEGIN CERTIFICATE-----
MIIDSzCCAjOgAwIBAgIUNxnWP8u/92caPpIofioPFgTwF2YwDQYJKoZIhvcNAQEL
BQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjUwMjIwMjMyNzA2WhcNMzUw
MjE4MjMyNzA2WjAWMRQwEgYDVQQDDAtFYXN5LVJTQSBDQTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALN+2Ux0Uwb2PMF/VcQmoj0JBTVM4fsK/em1qJpH
Yu+UBx26x3uXX129UjKiJsDPkGUnsllWzfyd5ZhXsJ8LiF3riPWts4yENsQTKX+k
a0dJBLHscohJrerjyEh1l/XSZoITCpugXwdK8+IPCK0mm0SePHNX6brSWfKqCLB4
H7RF99N7/opwuCC3uOojklMg7iOQTDUFqKN9jqHfrGjgP+tneiq5y/3xiN62SKZU
KPn7PVokygfUl+mE8t1/dgVb+viYypTMuajuxHAlCTlwS4QyHlNUWQZeBUiCRmwl
jwUKSWVUD7ZJKG/g4jbVjh62EfMNeixxOSOGhzaSsxLM8DECAwEAAaOBkDCBjTAd
BgNVHQ4EFgQUIaa7SQpyz+tFV0ORjJ2iDBqWbHowUQYDVR0jBEowSIAUIaa7SQpy
z+tFV0ORjJ2iDBqWbHqhGqQYMBYxFDASBgNVBAMMC0Vhc3ktUlNBIENBghQ3GdY/
y7/3Zxo+kih+Kg8WBPAXZjAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjANBgkq
hkiG9w0BAQsFAAOCAQEAgiuL6xiMMYUj8ivpWXdUdJjp0V2N4UYye2ka70hZLR1d
6qppAG175zJcx6RJkvw+ZCWbmahHuIPOSZVuOpve2pj8sJqKLaGHx/UVsctcREtd
SmmcDDp8CZIoYNVP3modp1BCLZDj/XAeJOvOW+72xEBnCZejy34e3ydFDqMbERuN
AHxwZ+u6Tq01X7lMcyQYtwaoTruN26Tj54ks1hbLMcTSL2RtYpZ6/tMWlnqCY5rr
UXpyTl8hMg12lh2qb8hl35AQnmL2ymjSPIEPuE2UIo0bruLiwXyqTr+3h1HntNoe
f1VDT2RbGpX/9AIxrHF7i40/BlR3+LwHv+12/r56Xw==
-----END CERTIFICATE-----
</ca>
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer M-
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^/ Ir a línea M-E Rehacer M-

```
 GNU nano 7.2
<cert>
-----BEGIN CERTIFICATE-----
MIIDWTCCAkGgAwIBAgIRAIKgpTx2ztEVrflTi5gqAAswDQYJKoZIhvcNAQELBQAw
FjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjUwMjIwMjMzNTI2WhcNMjcwNTI2
MjMzNTI2WjAVMRMwEQYDVQQDDApjbGllbnRuYW1lMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAuNywD5uA0iQO5PNZP4VEzi7rq0MethRJ4HvkvUJsl8cv
cUaUJQ8QVzpCaEkbeLspcTklOPlnvnSdqn8Cpobfsw4XIveqnQPMqp1dz/6fnfnp
IO+QFcLpycz8MMh/Ctoriwq7U3Eulj2f1xxm1EZLQVZa8JS3MxptoV4smFjjo3D0
a1WP2PCoeq8ob89zVHaxHs7zrwWLRJQ/d+Na6XzuxZpnkTMqsiuS9jABByPJrqWsj
wam5p9RB2FnVpUk86DFrCXLqPxVTw2xors1hkIeWNrSFBLgbrXdJHawQT+Y/PAq6
TpveEEzrwzIWgUZJLGki/SCYRdwZ+c65K94Jq1qrlQIDAQABo4GiMIGfMAkGA1Ud
EwQCMAAwHQYDVR0OBBYEFDlKy6n4+4rF5RYOnqTipCWKB+kvMFEGA1UdIwRKMEiA
FCGmu0kKcs/rRVdDkYydogwalmx6oRqkGDAWMRQwEgYDVQQDDAtFYXN5LVJTQSBD
QYIUNxnWP8u/92caPpIofioPFgTwF2YwEwYDVR0lBAwwCgYIKwYBBQUHAwIwCwYD
VR0PBAQDAgeAMA0GCSqGSIb3DQEBCwUAA4IBAQB7HkjUZFOK5kpwyRnPjjClT5hD
E6JNkd41UneQy0oXpL1Mcpc1+7ZkqIivwfYKO04mWJaWBUJ3IHOhGfxTXH6Lflsb
WiYkITiuLcOtgInmNakcCtfMTJ75BkI8sK66y7k22yqb5cGtUnDXuVUry+LNfMrl
qQc+sxbLMGlQPZBriBrJhwkprU3/UvRT4kv9D/RiW9UPIT8PQENg1Ow/UVbv/iMm
8zQdnLnRuJIcVdKht3qU1ugIOBVjtHLmL7mUbFu/+I+vPRO/vAIv6A31hBxoqFb+
KauzMfzXRHH/cD27CN/8qNZ8CKec3YjTgIMmHai975cFPsGRKFE5EYdVhcET
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC43LAPm4DSJA7k
81k/hUTOLuurQx62FEnge+S9QmyXxy9xRpQlDxBXOkJoSRt4uylxOSU4+We+dJ2q
fwKmht+zDhci96qdA8yqnV3P/p+d+ekg75AVwunJzPwwyH8K2iuLCrtTcS6WPZ/X
HGbURktBVlrwlLczGm2hXiyYWOOjcPRrVY/Y8Kh6ryhvz3NUdrEezvOvBYtElD93
41rpfO7FmmeRMyqyK5L2MAHI8mupayPBqbmn1EHYWdWlSTzoMWsJcuo/FVPDbGiu
zWGQh5Y2tIUEuButd0kdrBBP5j88CrpOm94QTOvDMhaBRkksaSL9IJhF3Bn5zrkr
3gmrWquVAgMBAAECggEAOYXqfyDLSBiSTenvRpXIoEP3b3ZWUyAjEOhceAv4UI5Z
k+z7YkC6u/nT+jFti/bpYWL/0yfAgYI2IXyeLYVgjI4A4w+gFnW9NQX80CESOA0w
3t/MvQjGyNWxT9jDt3PGAuEXA1L/xR5t43jiAoHRHwapC52rGArMPF9ajxlx1ERj
8amov0nnbNj3+je89yQFwLAV/CW1GSyvKkNTAmAI/o+K3Ylukwvxi/Db1Hezte3n
RX+PZhnBt4o5CoxqPImM6Z3wS+jcL6zEka48qFNy4p5BZc0NHhVYgROgDMUzNBkg
/AYOhb2dHK48mPrtwXlk7Im8GUtbBUmrAgu3quAbDQKBgQD7HNPzA+ow08gVvxo9
ZMlgtElE8CI5z4dztPRUteFmR58J4why/RnZ+LSScnBDc75jB6LbOfUMMAAL0iw9
tYsEX8hly+ro8OdAz93EGIgqqYUnuBYmEp0GRf8yfYkX3fHSlmQRJ8H/xhzBMXrG
A92Hm+fjpGnhwRfY6RnthPrjqwKBgQC8dcP6F2lg7v3PLRb8ey6qOerxHLcj084j
VYmwutGiJMVudpB/o1zPJfLyCgB0L+FJNsV3ol4zi4ECnmie7U7foxcKv0y2Nf5H
```

```
/fJmqWQLlR6CMjPZMjXzjikAqWCbYnr1RKirvopbZ5VQzkMDpHvizRtAdLRWzZLw
peIpIpUz3CXTyyTPSmiGszM=
-----END PRIVATE KEY-----
</key>

<tls-auth>
-----BEGIN OpenVPN Static key V1-----
f2551e653c5f61eeafc462e6af448677
a56fe7df62aa1d9dffca5ba419c93b3e
d0a65a206d8bf2f2d32b5fdc8a3173c9
65b2f60e0243258e4db5d9f63d768521
e9acf2d44bad75c431ffbdea1f2098ea
e208c0a4bfbc263e81890df7c55ee503
8d6cf9a02bece6c2d396a877db5e99da
8c0695751cd7119f29b3e6f10628657e
3616be36e22589b5fec372bef9121463
d685abc755fedbe310ae83e6434e56fc
aa9197475ea56d306be6ee316003c217
0cc21eb6f0b583b309331fce3d673ccf
7c4dd3c196e24748a3b30e8f90a025a9
eb4137173f7c0cb2d1515c1f4420c370
fa69ccdc353cef8be0c9071a055c2733
0a794403ef02699936e2e59d69891db9
-----END OpenVPN Static key V1-----
</tls-auth>
key-direction 1
```

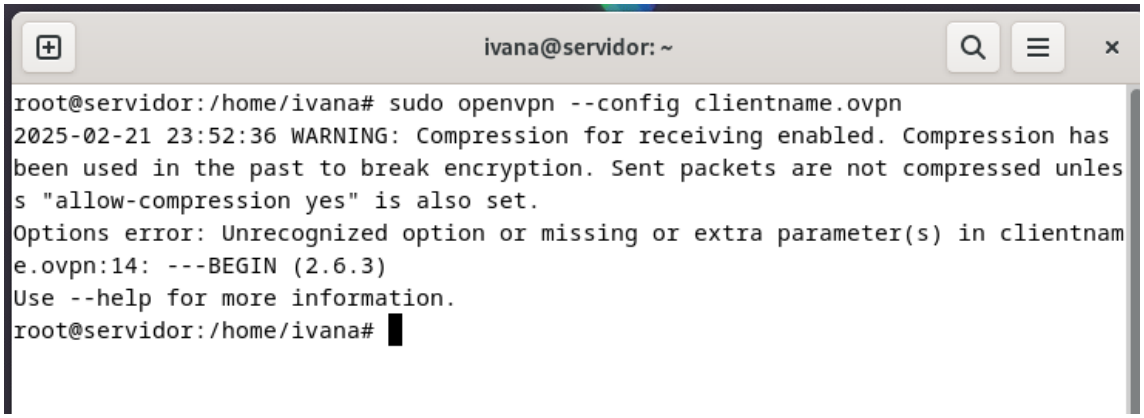
Y ya tenemos todo lo necesario

Colocamos el archivo clientname.ovp en el directorio adecuado

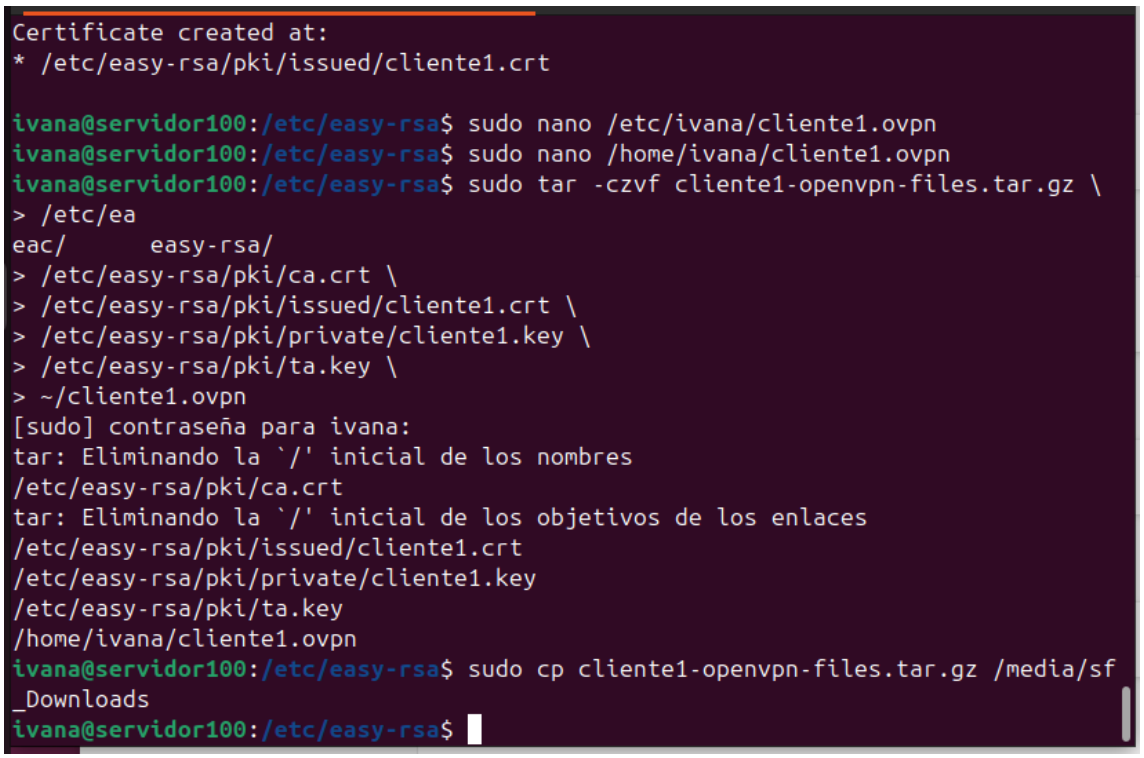
sudo cp clientname.ovpn /etc/openvpn/

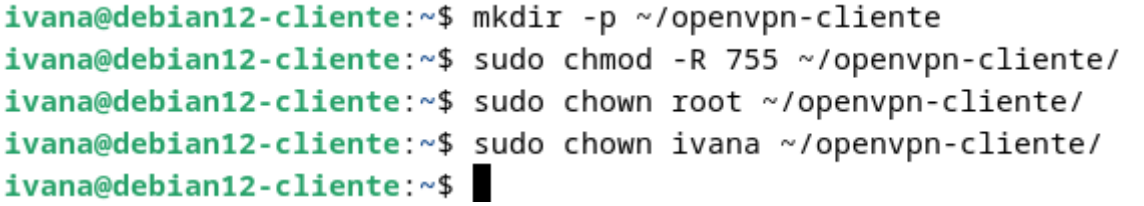
```
root@servidor:/home/ivana# sudo cp clientname.ovpn /etc/openvpn/
root@servidor:/home/ivana#
```

Procedemos a conectarnos con openvpn –config clientname.ovpn. Nos da error .



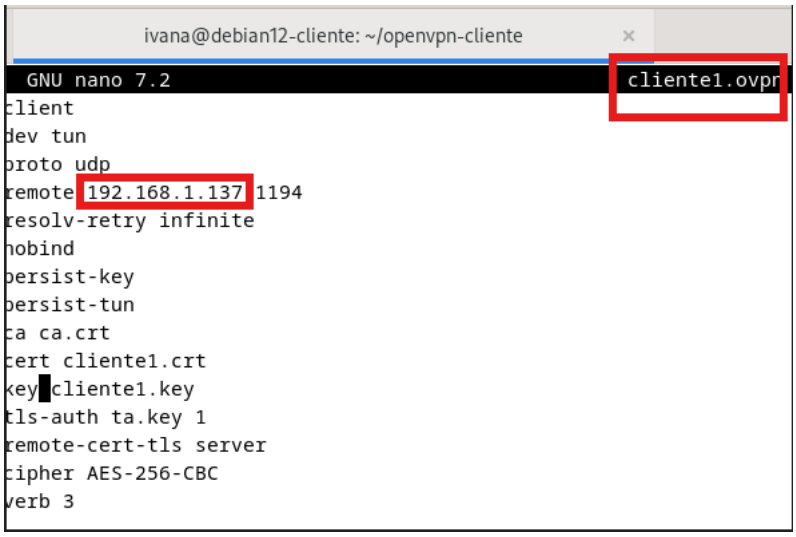
Después de intentar averiguar el error y no conseguirlo, vuelvo a crear las dos máquina e iniciar la tarea. Los cambios que procedo a hacer (también he cambiado de lugar, por lo que las IPs son distintas).





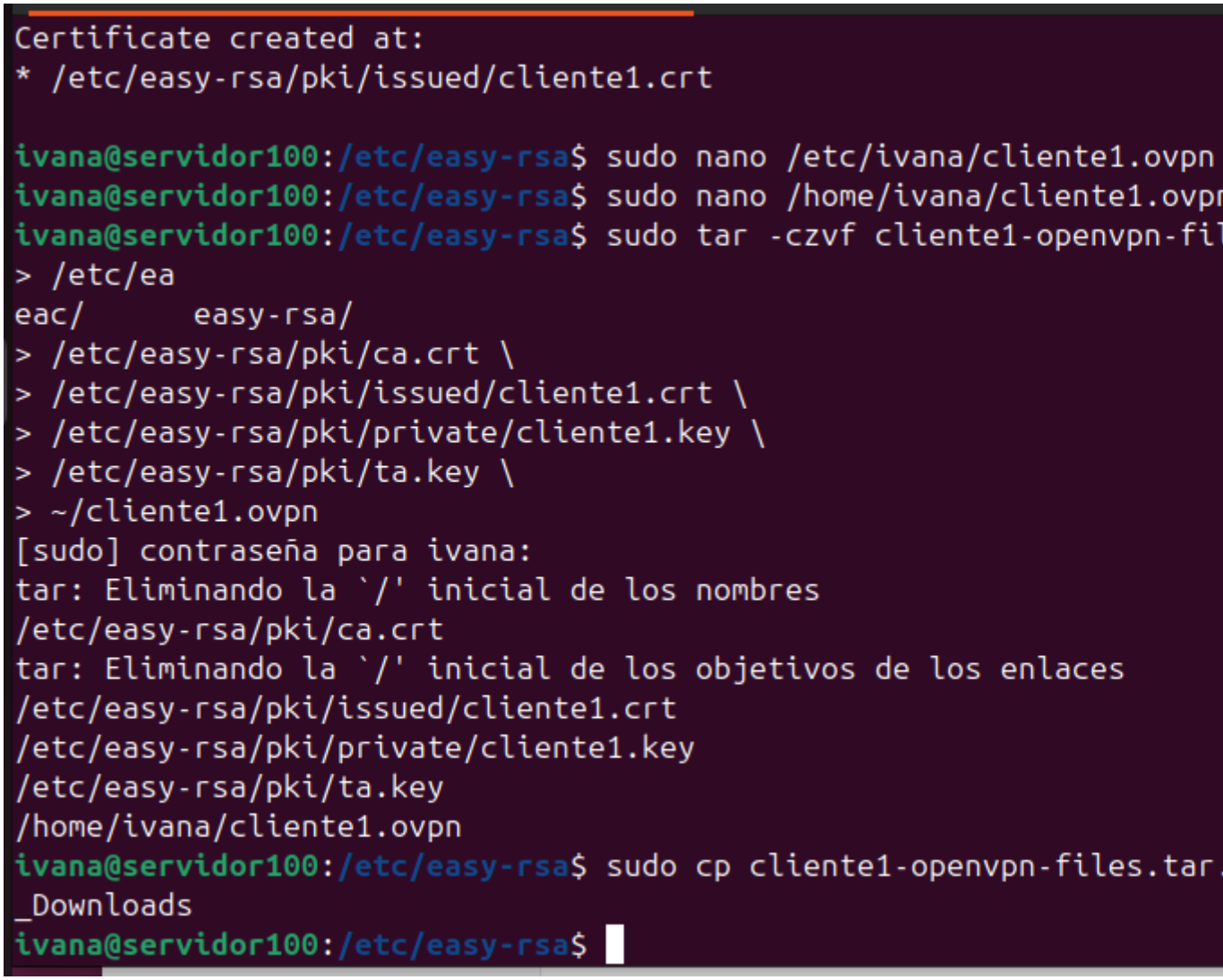
```
ivana@debian12-cliente:~/openvpn-cliente$ ls
ca.crt        cliente1.key                    cliente1.ovpn
cliente1.crt  cliente1-openvpn-files.tar.gz   ta.key
ivana@debian12-cliente:~/openvpn-cliente$
```

```
ivana@debian12-cliente:~$ sudo mv ~/Descargas/cliente1-openvpn-files.tar.gz
 ~/openvpn-cliente/
ivana@debian12-cliente:~$ cd ~/openvpn-cliente/
ivana@debian12-cliente:~/openvpn-cliente$ sudo tar -xzvf cliente1-openvpn-f
iles.tar.gz
etc/easy-rsa/pki/ca.crt
etc/easy-rsa/pki/issued/cliente1.crt
etc/easy-rsa/pki/private/cliente1.key
etc/easy-rsa/pki/ta.key
home/carmona/cliente1.ovpn
ivana@debian12-cliente:~/openvpn-cliente$
```



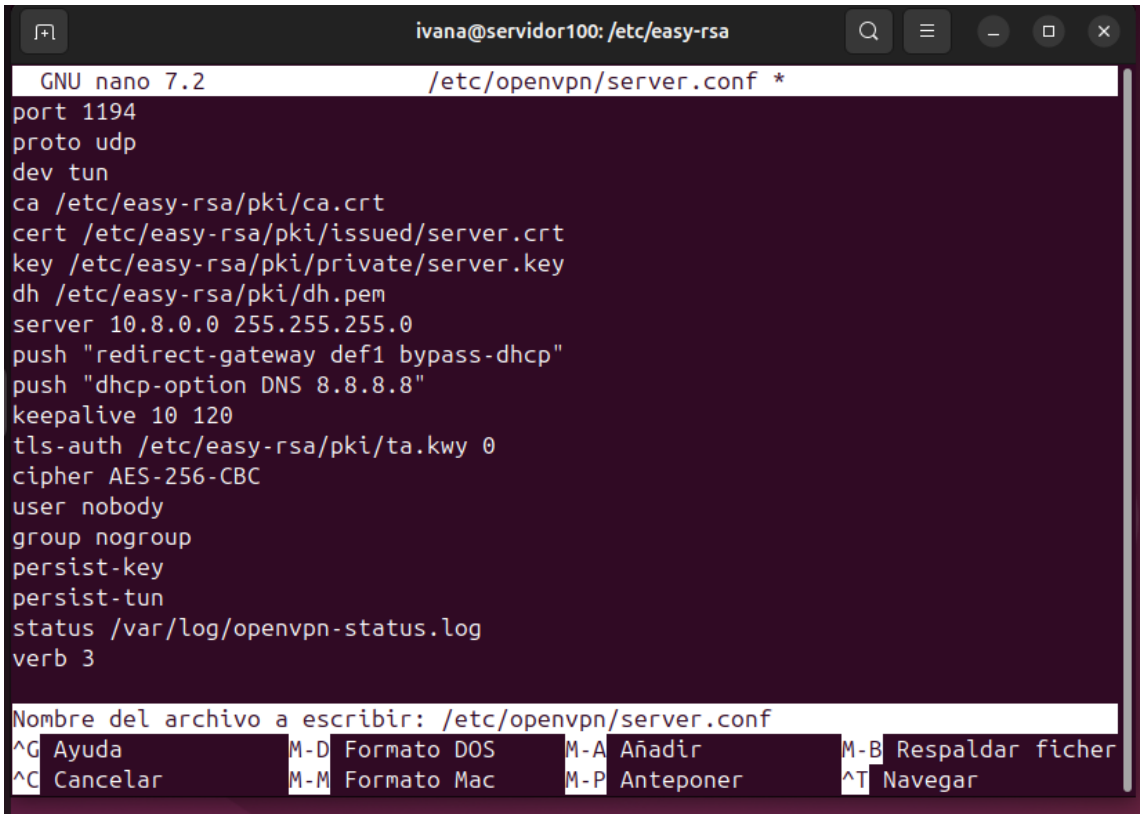
PRUEBAS FINALES

Desde el servidor



```
ivana@servidor100:~$ $ scp /etc/easy-rsa/cliente1-openvpn-files.tar.gz
ivana@192.168.1.136:/home/ivana/Descargas/
$: no se encontró la orden
ivana@servidor100:~$ sudo scp /etc/easy-rsa/cliente1-openvpn-files.tar.g
z  ivana@192.168.1.136:/home/ivana/Descargas/
[sudo] contraseña para ivana:
The authenticity of host '192.168.1.136 (192.168.1.136)' can't be establ
ished.
ED25519 key fingerprint is SHA256:MB2J94kZvJo9JNOPJMEINJmAq4/tQSsp/LDymp
O8wzg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.136' (ED25519) to the list of know
n hosts.
ivana@192.168.1.136's password:
cliente1-openvpn-files.tar.gz         100% 5217   953.9KB/s   00:00
ivana@servidor100:~$
```

```
ivana@servidor100:/etc/easy-rsa$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:47:4a:74 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::f447:7fff:7755:6f5e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:79:fb:5c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.135/24 brd 192.168.1.255 scope global dynamic noprefixroute e
np0s3
       valid_lft 38312sec preferred_lft 38312sec
    inet6 fe80::f568:4910:bca5:c957/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
 UNKNOWN group default qlen 500
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::9167:361:b836:c8ed/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
ivana@servidor100:/etc/easy-rsa$
```



Desde el cliente

```
ivana@debian12-cliente:~/openvpn-cliente$ sudo openvpn --config ~/openvpn-cliente/cliente1.ovpn
2025-02-23 01:46:42 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:A
ES-128-GCM:CHACHA20-POLY1305). OpenVPN ignores --cipher for cipher negotiations.
2025-02-23 01:46:42 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2025-02-23 01:46:42 WARNING: file 'cliente1.key' is group or others accessible
2025-02-23 01:46:42 OpenVPN 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [
AEAD] [DCO]
2025-02-23 01:46:42 library versions: OpenSSL 3.0.15 3 Sep 2024, LZO 2.10
2025-02-23 01:46:42 DCO version: N/A
2025-02-23 01:46:42 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.137:1194
2025-02-23 01:46:42 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-02-23 01:46:42 UDPv4 link local: (not bound)
2025-02-23 01:46:42 UDPv4 link remote: [AF_INET]192.168.1.137:1194
2025-02-23 01:46:42 TLS: Initial packet from [AF_INET]192.168.1.137:1194, sid=d4426ab3 b1dfeaae
2025-02-23 01:46:42 VERIFY OK: depth=1, CN=server-ivana
2025-02-23 01:46:42 VERIFY KU OK
2025-02-23 01:46:42 Validating certificate extended key usage
2025-02-23 01:46:42 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentica
tion
2025-02-23 01:46:42 VERIFY EKU OK
2025-02-23 01:46:42 VERIFY OK: depth=0, CN=server-ivana
2025-02-23 01:46:42 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit R
SA, signature: RSA-SHA256
2025-02-23 01:46:42 [server-ivana] Peer Connection Initiated with [AF_INET]192.168.1.137:1194
2025-02-23 01:46:42 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-02-23 01:46:42 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-02-23 01:46:42 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS
 8.8.8.8,route 10.8.0.1,topology net30,ping 10,ping-restart 120,ifconfig 10.8.0.6 10.8.0.5,peer-id 0,cipher AES-2
56-GCM,protocol-flags cc-exit tls-ekm dyn-tls-crypt,tun-mtu 1500'
2025-02-23 01:46:42 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-23 01:46:42 OPTIONS IMPORT: route options modified
2025-02-23 01:46:42 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
2025-02-23 01:46:42 OPTIONS IMPORT: tun-mtu set to 1500
2025-02-23 01:46:42 net_route_v4_best_gw query: dst 0.0.0.0
2025-02-23 01:46:42 net_route_v4_best_gw result: via 192.168.1.1 dev enp0s3
2025-02-23 01:46:42 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=enp0s3 HWADDR=08:00:27:34:0f:81
```

```
ivana@debian12-cliente:~/openvpn-cliente$ ping -c 4 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=7.01 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=1.66 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=2.93 ms
64 bytes from 10.8.0.1: icmp_seq=4 ttl=64 time=11.9 ms

--- 10.8.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.661/5.868/11.877/3.992 ms
ivana@debian12-cliente:~/openvpn-cliente$
```

```
ivana@debian12-cliente:~$ ping -c 4 192.168.1.135
PING 192.168.1.135 (192.168.1.135) 56(84) bytes of data.
64 bytes from 192.168.1.135: icmp_seq=1 ttl=64 time=1.92 ms
64 bytes from 192.168.1.135: icmp_seq=2 ttl=64 time=0.603 ms
64 bytes from 192.168.1.135: icmp_seq=3 ttl=64 time=0.408 ms
64 bytes from 192.168.1.135: icmp_seq=4 ttl=64 time=0.601 ms

--- 192.168.1.135 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 0.408/0.882/1.916/0.602 ms
ivana@debian12-cliente:~$
```