

Como instalar o OpenVPN Server e Client no Ubuntu

OpenVPN é uma aplicação de código aberto que permite que você crie uma rede privada através da Internet pública. OpenVPN encaminha sua conexão de rede com segurança através da internet. Este tutorial descreve as etapas para configurar um servidor e um cliente OpenVPN no Ubuntu.

Instale o OpenVPN e o *easy-rsa*

```
# apt-get update  
# sudo apt-get install openvpn easy-rsa
```

Configurando o *easy-rsa*

Nesta fase, você irá gerar alguma chave e certificado:

- Autoridade de certificação (ca)
- Chave do servidor e certificado
- Chave Diffie-Hellman.
- Cliente Chave e Certificado

Passo 1 - copie os scripts do *easy-rsa* para o diretório do OpenVPN

```
# cp -r /usr/share/easy-rsa/ /etc/openvpn/
```

Em seguida, vá para o diretório ***easy-rsa*** e edite o arquivo de ***vars***.

```
# cd /etc/openvpn/easy-rsa/  
nano vars
```

```
# Increase this to 2048 if you  
# are paranoid. This will slow  
# down TLS negotiation performance  
# as well as the one-time DH parms  
# generation process.  
export KEY_SIZE=2048  
  
# In how many days should the root CA key expire?  
export CA_EXPIRE=3650  
  
# In how many days should certificates expire?  
export KEY_EXPIRE=3650  
  
# These are the default values for fields  
# which will be placed in the certificate.  
# Don't touch any of these fields unless  
export KEY_COUNTRY="US"  
export KEY_PROVINCE="CA"  
export KEY_CITY="SanFrancisco"  
export KEY_ORG="Fort-Funston"  
export KEY_EMAIL="me@myhost.mydomain"  
export KEY_OU="MyOrganizationalUnit"  
  
# X509 Subject Field  
export KEY_NAME="EasyRSA"
```

Agora é hora de gerar novas chaves e certificado para a nossa instalação.

```
# source ./vars
```

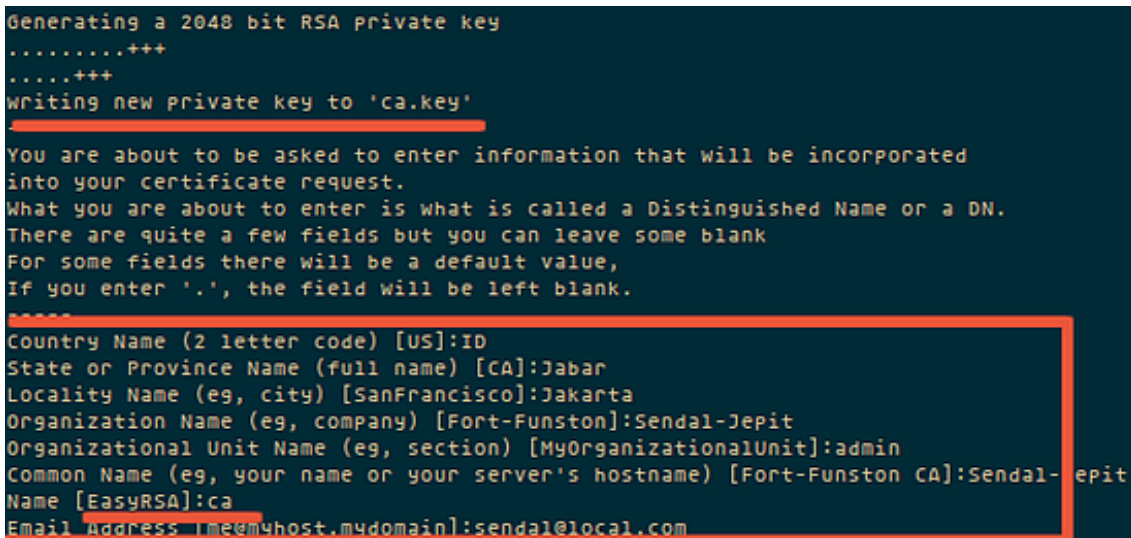
Em seguida, execute *clean-all* para garantir que temos uma configuração de certificado limpa.

```
# ./clean-all
```

Agora gerar uma *autoridade de certificação (CA)*, você será questionado sobre *dados do servidor*. Veja a imagem abaixo para meus valores.

Este comando irá criar um arquivo *ca.crt* e *ca.key* em no diretório */etc/openvpn/easy-rsa/keys/*.

```
# ./build-ca
```

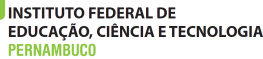


```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few 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.
-----
Country Name (2 letter code) [US]:ID
State or Province Name (full name) [CA]:Jabar
Locality Name (eg, city) [SanFrancisco]:Jakarta
Organization Name (eg, company) [Fort-Funston]:Sendal-Jepit
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:admin
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:Sendal-Jepit
Name [EasyRSA]:ca
Email Address [me@myhost.mydomain]:sendal@local.com
```

Etapas 2 - Agora gere uma chave de servidor e um certificado.

Execute o comando "*build-key-server server*" no diretório atual:

```
# ./build-key-server server
```



Campus: Palmares

Curso: Redes de Computadores

Disciplina: Segurança em Redes de Computadores

```

Generating a 2048 bit RSA Private Key
-----
writing new private key to 'server.key'
-----
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.

Country Name (2 letter code) [US]:ID
State or Province Name (full name) [CA]:Jabar
Locality Name (eg, city) [SanFrancisco]:Jakarta
Organization Name (eg, company) [Fort-Flunston]:Sendal-Jepit
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:admin
Common Name (eg, your name or your server's hostname) [server]:Server-Jepit
Name [EasyRSA]:server
Email Address [me@myhost.mydomain]:sendal@local.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []: Leave this Blank

Generating a RSA Certificate
-----
Check that the request matches the signature
Signature OK
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'ID'
stateOrProvinceName :PRINTABLE:'Jabar'
localityName      :PRINTABLE:'Jakarta'
organizationName   :PRINTABLE:'Sendal-Jepit'
organizationalUnitName:PRINTABLE:'admin'
commonName        :PRINTABLE:'Server-Jepit'
name              :PRINTABLE:'server'
emailAddress       :IA5STRING:'sendal@local.com'
Certificate is to be certified until May 16 15:32:16 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

```

Passo 3 - Criar uma troca de chaves Diffie-Hellman.

Execute o comando build-dh:

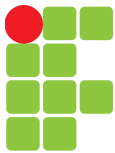
```
# ./build-dh
```

[illegible]

Aguarde, será necessário algum tempo para gerar os arquivos.

Etapa 4 - Gerar chave do cliente e certificado.

```
# ./build-key client
```



```
Generating a 2048 bit RSA private key
.....+++
.....
Writing new private key to 'client.key'

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.

Country Name (2 letter code) [US]:ID
State or Province Name (full name) [CA]:Jabar
Locality Name (eg, city) [SanFrancisco]:Jakarta
Organization Name (eg, company) [Fort-Flunston]:Sendal-Jepit
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:admin
Common Name (eg, your name or your server's hostname) [client]:Client-Jepit
Name [EasyRSA]:client
Email Address [me@myhost.mydomain]:sendal@local.com

Please enter the following 'extra' attributes
to be sent with your certificate request
a challenge password []:
an optional company name []: Leave this Blank
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'ID'
stateOrProvinceName     :PRINTABLE:'Jabar'
localityName            :PRINTABLE:'Jakarta'
organizationName        :PRINTABLE:'Sendal-Jepit'
organizationalUnitName  :PRINTABLE:'admin'
commonName              :PRINTABLE:'Client-Jepit'
name                   :PRINTABLE:'client'
emailAddress             :IA5STRING:'sendal@local.com'
Certificate is to be certified until May 16 15:53:03 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
```

Etapa 5 - Mover ou copiar o diretório *keys* para */etc/openvpn*

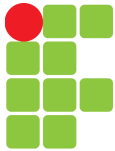
```
# cd /etc/openvpn/easy-rsa/
# cp -r keys/ /etc/openvpn/
```

Configurar o OpenVPN

Crie um arquivo de configuração para o servidor:

```
# cd /etc/openvpn/
# nano server.conf
```

Colar configuração abaixo dentro do arquivo acima:



```
#change with your port
port 8080

#You can use udp or tcp
proto udp

# "dev tun" will create a routed IP tunnel.
dev tun

#Certificate Configuration

#ca certificate
ca /etc/openvpn/keys/ca.crt

#Server Certificate
cert /etc/openvpn/keys/server.crt

#Server Key and keep this is secret
key /etc/openvpn/keys/server.key

#See the size a dh key in /etc/openvpn/keys/
dh /etc/openvpn/keys/dh2048.pem

#Internal IP will get when already connect
server 192.168.200.0 255.255.255.0

#this line will redirect all traffic through our OpenVPN
push "redirect-gateway def1"

#Provide DNS servers to the client, you can use google DNS
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"

#Enable multiple client to connect with same key
duplicate-cn

keepalive 20 60
comp-lzo
persist-key
persist-tun
daemon

#enable log
log-append /var/log/myvpn/openvpn.log

#Log Level
verb 3
```

Crie uma pasta para o arquivo de log.

```
# mkdir -p /var/log/myvpn/  
# touch /var/log/myvpn/openvpn.log
```

Etapa 3 - Ativar o encaminhamento de porta.

```
# nano /etc/sysctl.conf
```

Adicione ao final da linha:

```
net.ipv4.ip_forward = 1
```

Etapa 4 – Inicie o Servidor OpenVPN

```
# openvpn --config client.ovpn
```

Configuração do cliente

Faça o download do aplicativo cliente para openvpn e instale-o no computador cliente (provavelmente o Desktop):

Usuário do Windows

https://swupdate.openvpn.org/community/releases/openvpn-install-2.3.13-I601-x86_64.exe

Para se conectar ao servidor Openvpn, o cliente requer uma chave e um certificado que já criou, faça o download dos 3 arquivos do seu servidor usando *SFTP* ou *SCP*:

- *ca.crt*
- *client.crt*
- *client.key*

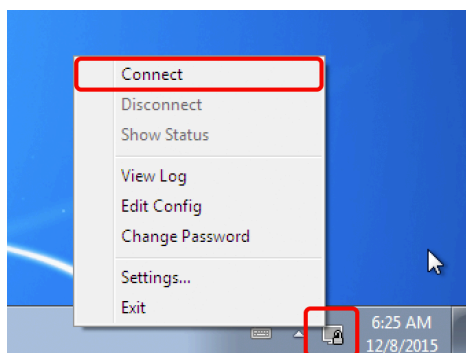
Salve os arquivos acima em **C:\Program Files\OpenVPN\config**

Se você usar um cliente Windows, então você pode usar [WinSCP](#) para copiar os arquivos. Depois crie um novo arquivo chamado *client.ovpn* salve-o na pasta acima (substituindo o IP em vermelho pelo IP do seu servidor):

```
client  
dev tun  
proto udp  
  
#Server IP and Port
```

```
remote 192.168.1.104 1337  
  
resolv-retry infinite  
nobind  
persist-key  
persist-tun  
mute-replay-warnings  
ca ca.crt  
cert client.crt  
key client.key  
ns-cert-type server  
comp-lzo
```

Inicie o cliente OpenVPN no Windows e solicite conexão.



Conclusão

OpenVPN é um software de código aberto para construir uma rede privada compartilhada que é fácil de instalar e configurar no servidor. É uma solução para aqueles que precisam de uma conexão de rede segura através da Internet pública.