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:

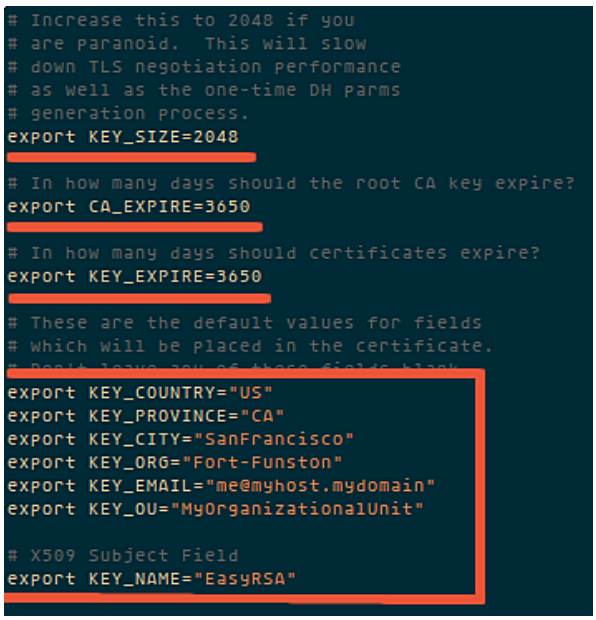
- Autoridade de certificação (ca)
- Chave do servidor e certificado
- Chave Diffie-Hellman.
- Cliente Chave e Certificado

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
```



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

```
# source ./vars
```

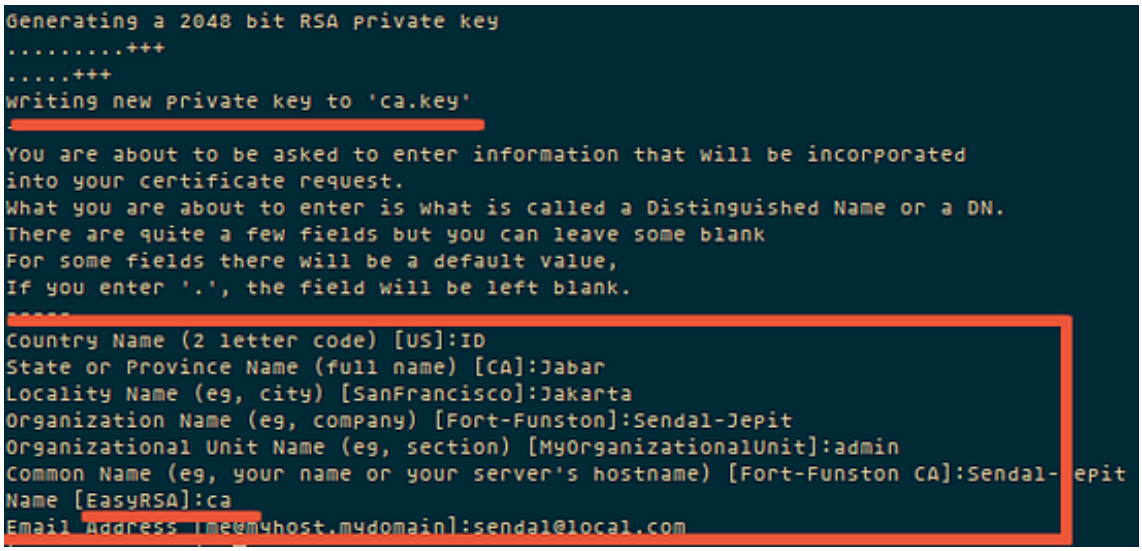
Em seguida, execute *clean-all* para garantir que temos uma configuração de certificado limpa.

```
# ./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/.

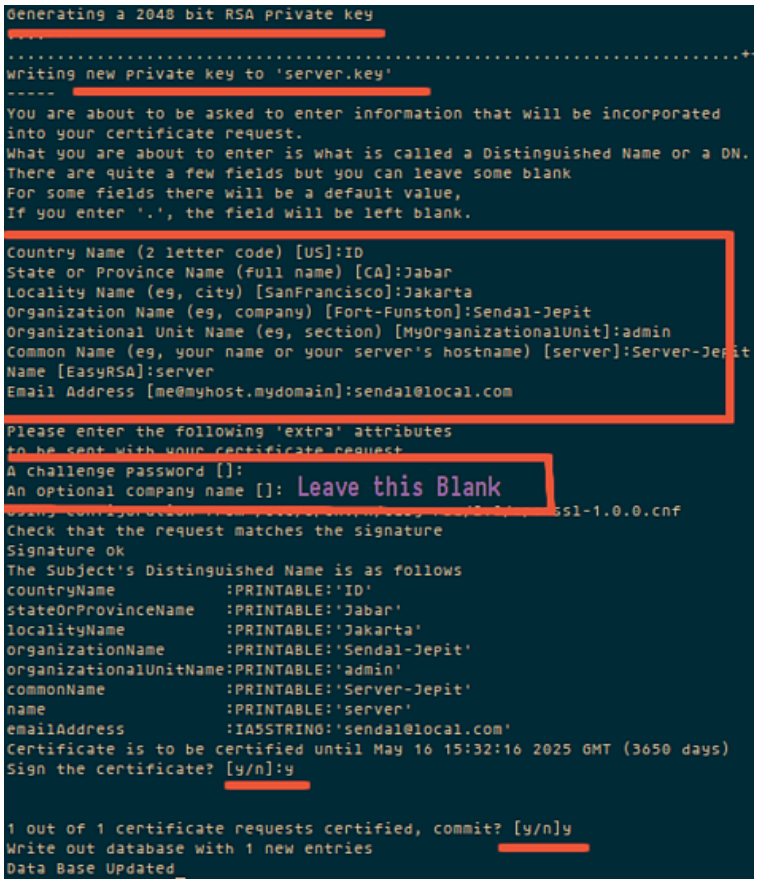
```
# ./build-ca
```



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

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

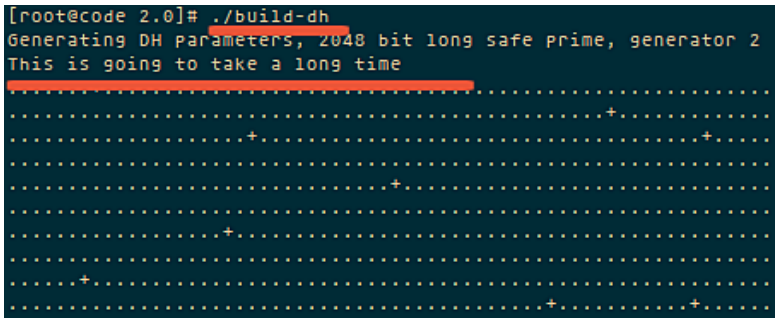
```
# ./build-key-server server
```



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

Execute o comando build-dh:

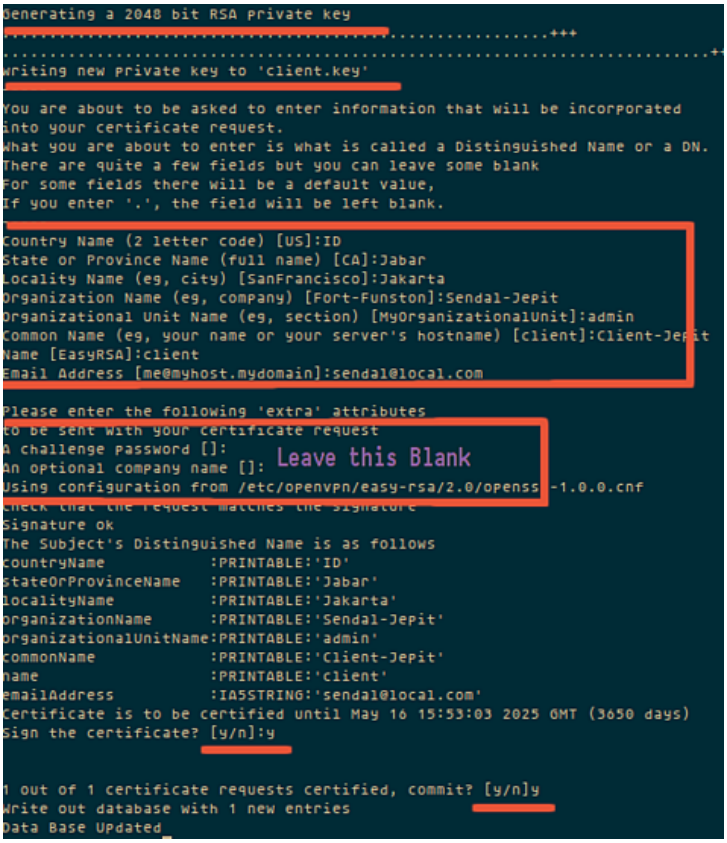
```
# ./build-dh
```



Aguarde, será necessário algum tempo para gerar os arquivos.

Etapa 4 - Gerar chave do cliente e certificado.

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



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 goolge 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):

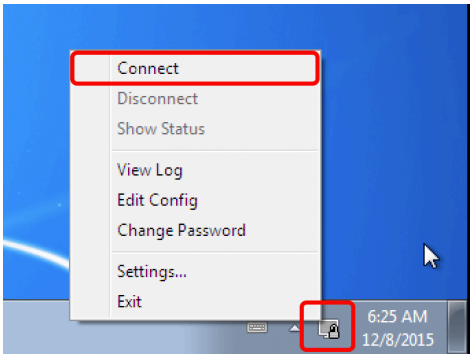
```
client
dev tun
proto udp

#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 partilhada 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 publica.