

**UNIVERSIDAD LUTERANA SALVADOREÑA  
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA  
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN**



**Facultad: Ciencias del Hombre y La Naturaleza**

**Asignatura: Administración de sistemas informáticos, Sábado de 7:00 am – 9:30 am**

**Ciclo: I 2020**

**Docente: Licda. Ana Lissette Girón de Bermúdez**

**TAREA: Configuración de openVPN basada en  
SSL/TLS de sitio a sitio**

**Integrantes:**

Wilber Alexander Palacios Mármol

Juan Gabriel Soto Aldana

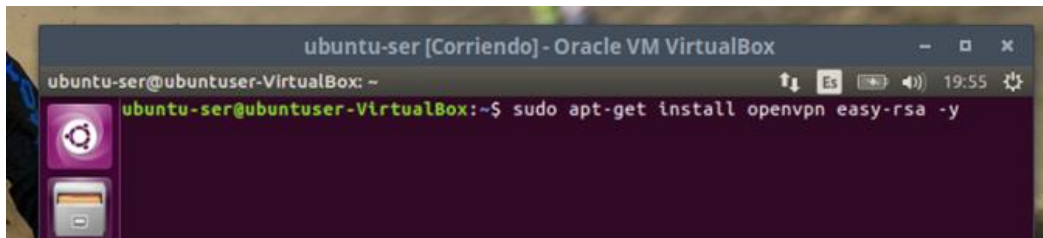
Ivan Steven Funes Ventura

Yesica Yaneth najarro Moreira

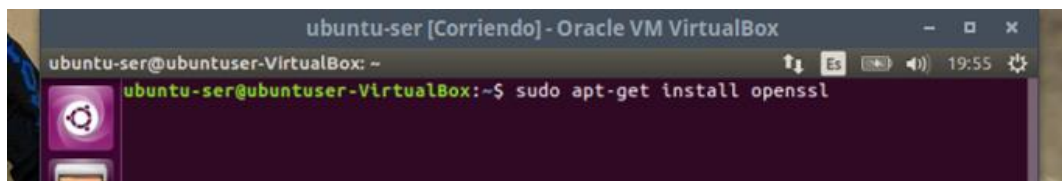
# Configuración de openVPN basada en SSL/TLS de sitio a sitio

Instalar OpenVPN

Vamos a instalar los paquetes

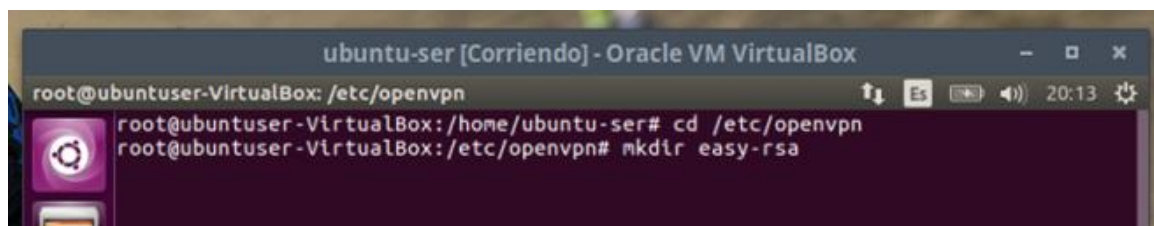


```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
ubuntu-ser@ubuntu-ser-VirtualBox: ~
ubuntu-ser@ubuntu-ser-VirtualBox:~$ sudo apt-get install openvpn easy-rsa -y
```



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
ubuntu-ser@ubuntu-ser-VirtualBox: ~
ubuntu-ser@ubuntu-ser-VirtualBox:~$ sudo apt-get install openssl
```

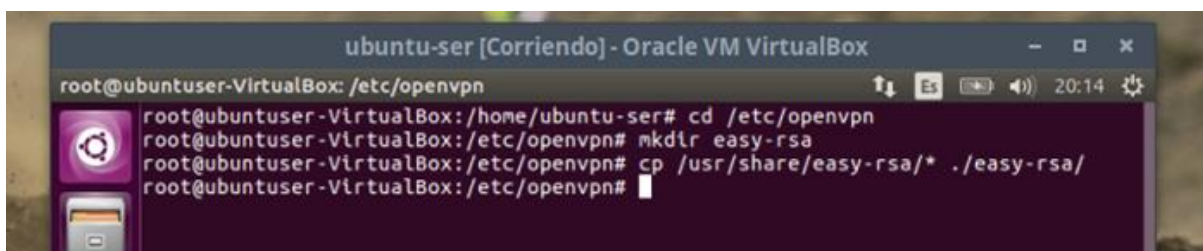
en la máquina que va a actuar de servidor «Server», una vez instalado creamos un directorio que se llamara **easy-rsa** como se muestra en la imagen:



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntu-ser-VirtualBox: /etc/openvpn
root@ubuntu-ser-VirtualBox:/home/ubuntu-ser# cd /etc/openvpn
root@ubuntu-ser-VirtualBox:/etc/openvpn# mkdir easy-rsa
```

OpenVPN nos ofrece una serie de scripts para la creación de certificados auto firmados para identificar a nuestro servidor tanto como a los clientes, la ubicación de estos scripts es el directorio.

ahora copiaremos las series de scripts al directorio de la siguiente manera:



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntu-ser-VirtualBox: /etc/openvpn
root@ubuntu-ser-VirtualBox:/home/ubuntu-ser# cd /etc/openvpn
root@ubuntu-ser-VirtualBox:/etc/openvpn# mkdir easy-rsa
root@ubuntu-ser-VirtualBox:/etc/openvpn# cp /usr/share/easy-rsa/* ./easy-rsa/
root@ubuntu-ser-VirtualBox:/etc/openvpn#
```

Para la creación de los certificados es necesario exportar una serie de variables para definir los datos en la creación de los certificados que vamos a crear. Esto lo realizamos editando el fichero **vars**, que se encuentra en los archivos que copiamos a la carpeta que creamos anterior mente.

```
build-inter      clean-all      revoke-full
build-key         inherit-inter   sign-req
build-key-pass    list-crl        vars
build-key-pkcs12  openssl-0.9.6.cnf whichopensslcnf
build-key-server  openssl-0.9.8.cnf
root@ubuntuser-VirtualBox:/etc/openvpn/easy-rsa#
```

Se proceder a modificarlo con el siguiente comando :

```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa
root@ubuntuser-VirtualBox:/etc/openvpn# cd easy-rsa
root@ubuntuser-VirtualBox:/etc/openvpn/easy-rsa# nano vars
```

y dentro del directorio **vars** se aran ciertas modificaciones quedando de la siguiente manera:

```
export EASY_RSA="`pwd`"
```

```
export OPENSSL="openssl"
```

```
export PKCS11TOOL="pkcs11-tool"
```

```
export GREP="grep"
```

```
export KEY_CONFIG=`$EASY_RSA/whichopensslcnf $EASY_RSA`
```

```
export KEY_DIR="$EASY_RSA/keys"
```

```
echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY_DIR
```

```
export PKCS11_MODULE_PATH="/usr/lib/changeme.so"
```

```
export PKCS11_PIN=usuario
```

```
export KEY_SIZE=2048
```

```
export CA_EXPIRE=365
```

```
export KEY_EXPIRE=365
```

```
export KEY_COUNTRY="SV"
```

```
export KEY_PROVINCE="El Savador"
```

```
export KEY_CITY="San Salvador"
```

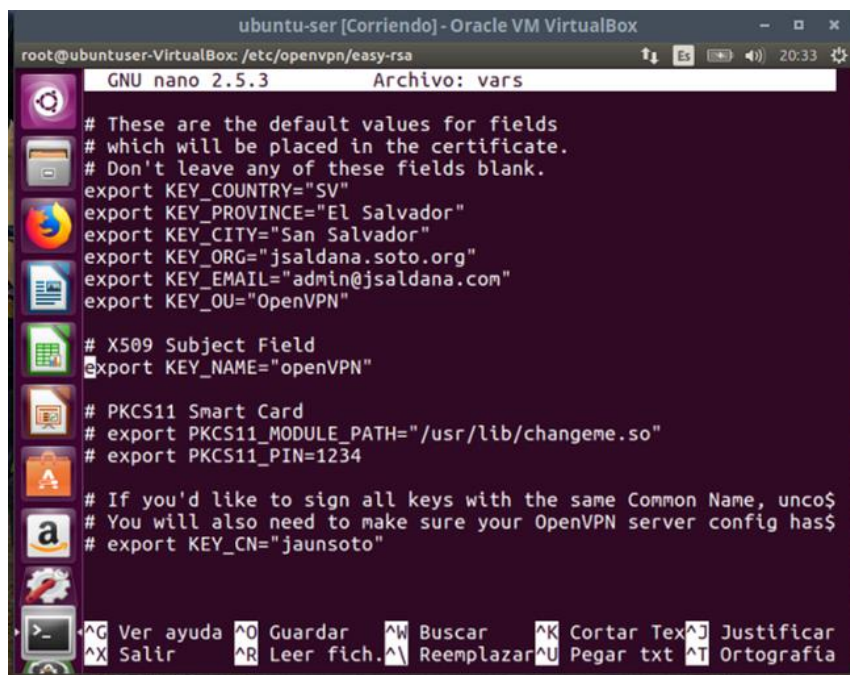
```
export KEY_ORG="jsaldana.soto.org"
```

```
export KEY_EMAIL="admin@jsaldana.com"
```

```
export KEY_OU="OpenVPN"
```

```
export KEY_NAME=openVPN
```

```
export KEY_CN=JuanluRamirez
```



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa
GNU nano 2.5.3 Archivo: vars
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="SV"
export KEY_PROVINCE="El Salvador"
export KEY_CITY="San Salvador"
export KEY_ORG="jsaldana.soto.org"
export KEY_EMAIL="admin@jsaldana.com"
export KEY_OU="OpenVPN"

# X509 Subject Field
export KEY_NAME="openVPN"

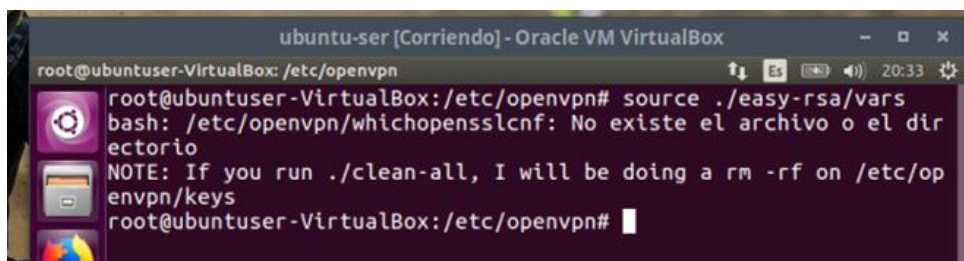
# PKCS11 Smart Card
# export PKCS11_MODULE_PATH="/usr/lib/changetime.so"
# export PKCS11_PIN=1234

# If you'd like to sign all keys with the same Common Name, unco$
# You will also need to make sure your OpenVPN server config has$
# export KEY_CN="jaunsoto"

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar
^X Salir ^R Leer fich. ^L Reemplazar ^U Pegar txt ^T Ortografia
```

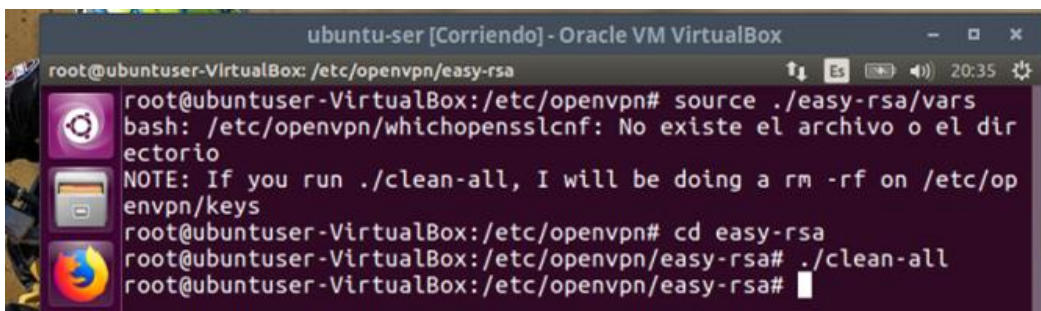
Luego de haber hecho las modificaciones en el archivo se guarda con Ctrl+o y Ctrl+x para salir

Ejecutamos el script modificado



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn
root@ubuntuser-VirtualBox:/etc/openvpn# source ./easy-rsa/vars
bash: /etc/openvpn/whichopensslcnf: No existe el archivo o el directorio
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/keys
root@ubuntuser-VirtualBox:/etc/openvpn#
```

Una de las líneas que podemos observar en el script es la que podemos ver anteriormente, es decir, nos solicitará la ejecución del script para eliminar posibles claves:



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa
root@ubuntuser-VirtualBox:/etc/openvpn# source ./easy-rsa/vars
bash: /etc/openvpn/whichopensslcnf: No existe el archivo o el directorio
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/keys
root@ubuntuser-VirtualBox:/etc/openvpn# cd easy-rsa
root@ubuntuser-VirtualBox:/etc/openvpn/easy-rsa# ./clean-all
root@ubuntuser-VirtualBox:/etc/openvpn/easy-rsa#
```

Con esto tenemos todas las configuraciones previas a la creación de certificados.

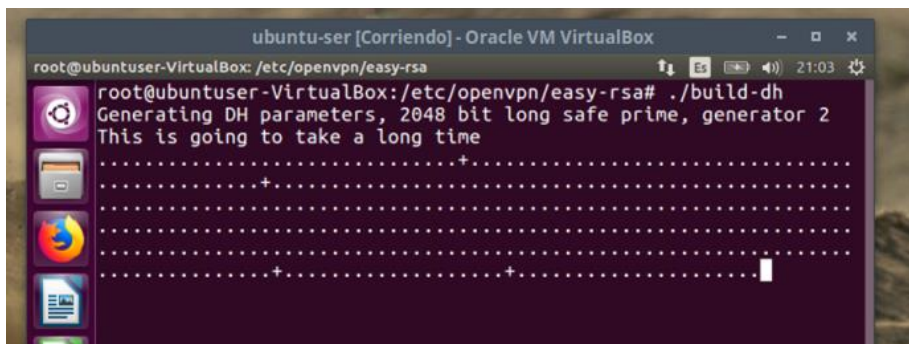


## Creación llave diffies hellman

Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión (establecer clave de sesión). Siendo no autenticado, sin embargo, provee las bases para varios protocolos autenticados.

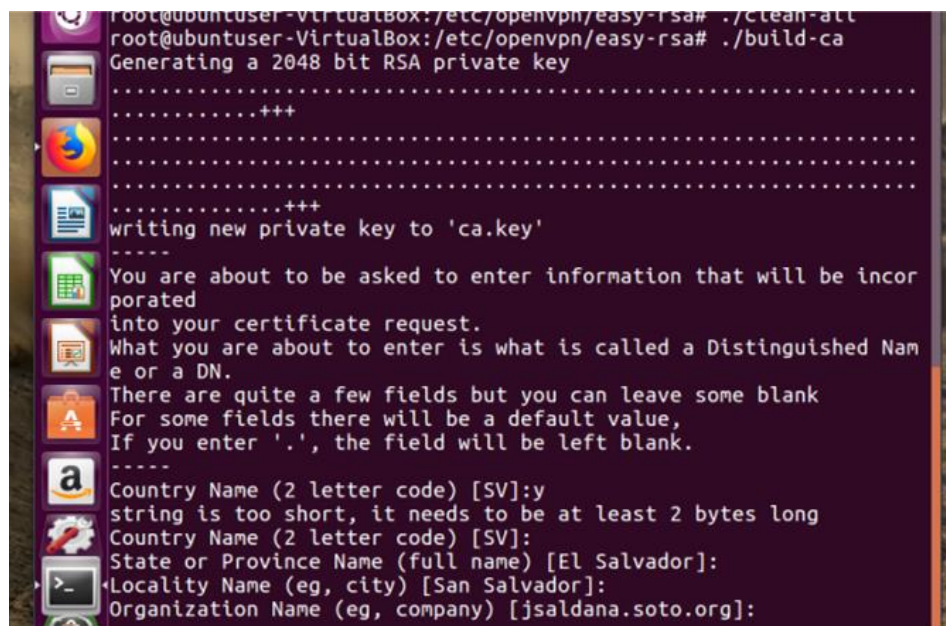
Para ello ejecutamos el script

## build-dh



## Creación certificado Autoridad certificadora

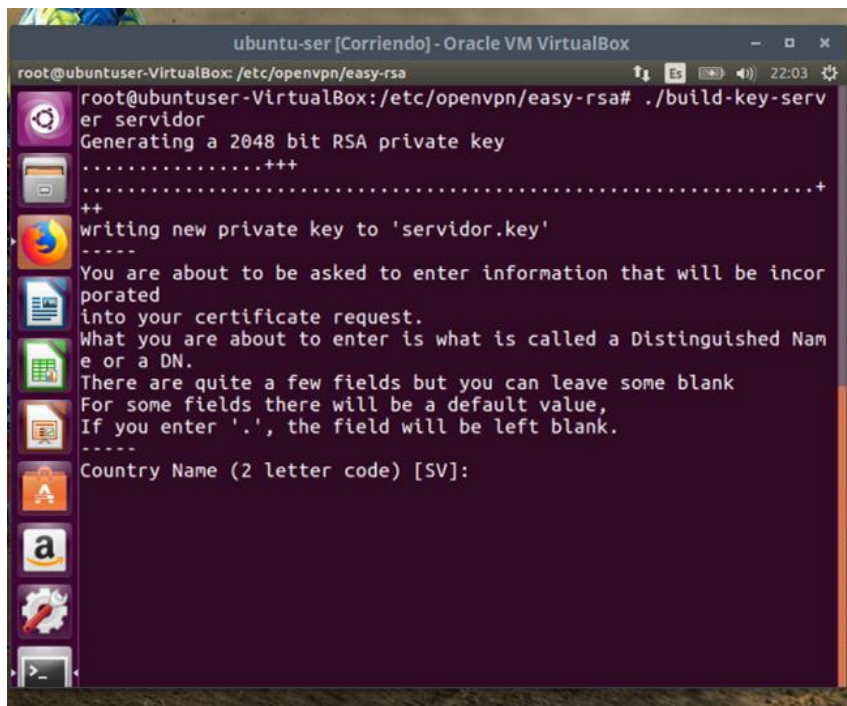
A continuación, lo que vamos a realizar la creación del certificado y se realiza ejecutando el siguiente fichero.



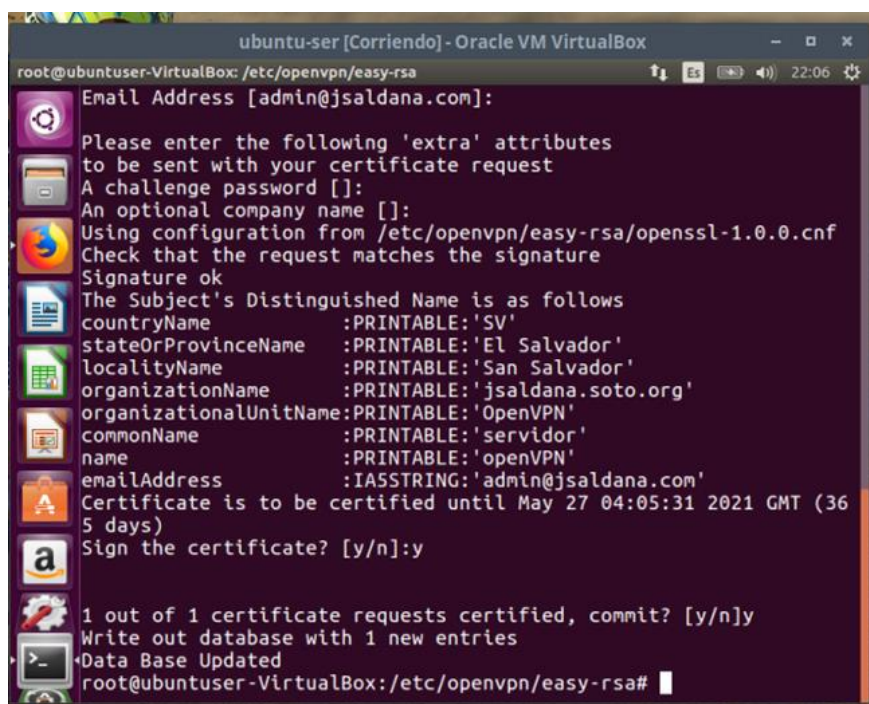
Solo damos enter según sea necesario.

## Creación de Clave y Certificado raíz

Para que OpenVPN pueda funcionar correctamente tendremos que crear un certificado y una key en el servidor para que así se pueda realizar la conexión correctamente, para ello vamos a ejecutar el siguiente fichero, seguido del nombre del servidor que en nuestro caso vamos a poner servidor.



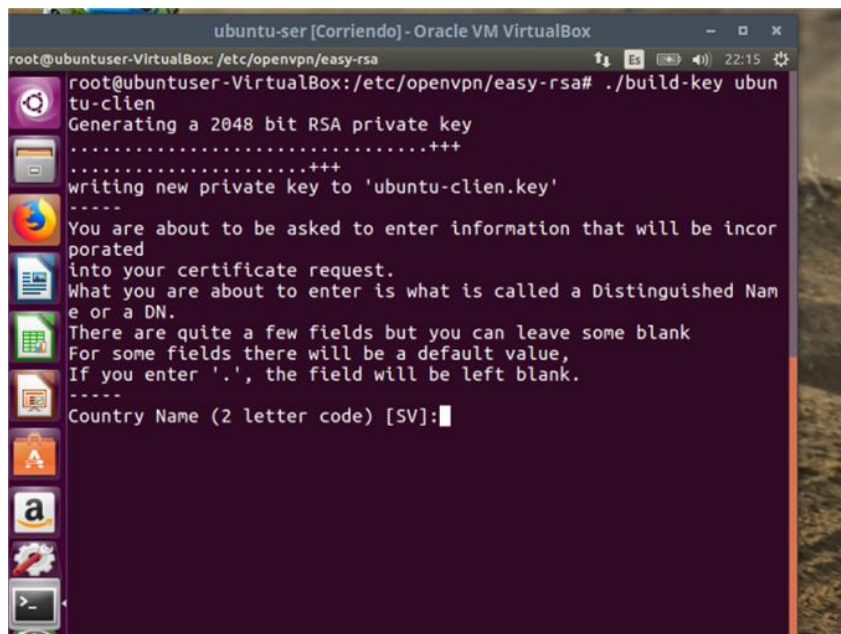
```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa# ./build-key-server servidor
Generating a 2048 bit RSA private key
.....+++
++++
writing new private key to 'servidor.key'
-----
You are about to be asked to enter information that will be incorporated
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) [SV]:
```



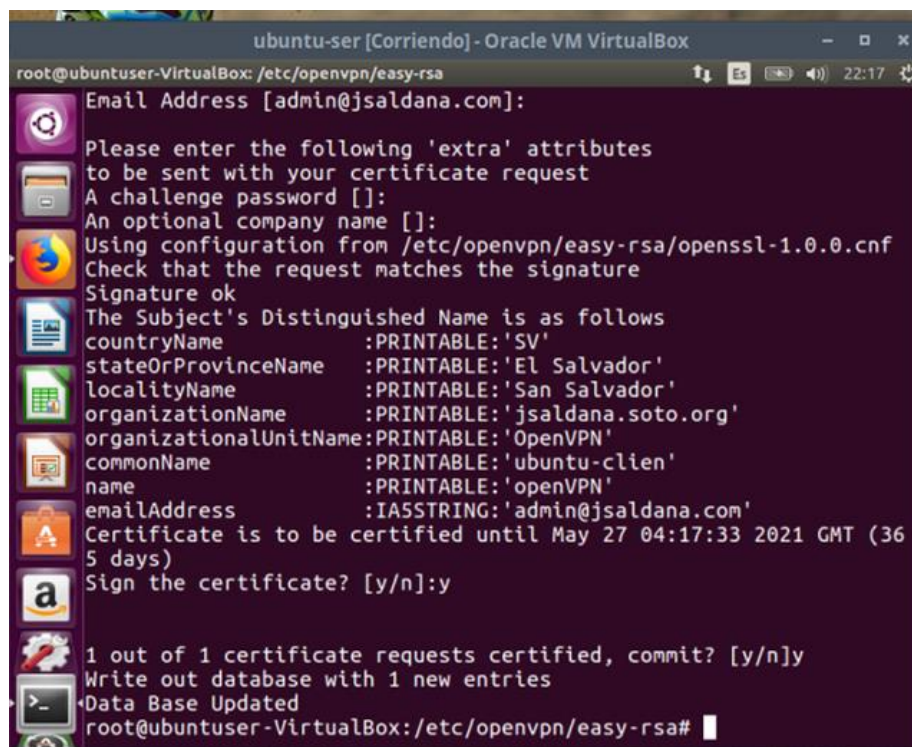
```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa#
Email Address [admin@jsaldana.com]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'SV'
stateOrProvinceName     :PRINTABLE:'El Salvador'
localityName             :PRINTABLE:'San Salvador'
organizationName         :PRINTABLE:'jsaldana.soto.org'
organizationalUnitName   :PRINTABLE:'OpenVPN'
commonName               :PRINTABLE:'servidor'
name                     :PRINTABLE:'openVPN'
emailAddress             :IASSTRING:'admin@jsaldana.com'
Certificate is to be certified until May 27 04:05:31 2021 GMT (36
5 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
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa#
```

Acto seguido vamos realizar la creación del certificado de la segunda máquina que permitirá la conexión remota para ello vamos a ejecutar el fichero denominado build-key, seguido del nombre del equipo que en nuestro caso se denomina ubuntu-clien.



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openssl/easy-rsa
root@ubuntuser-VirtualBox: /etc/openssl/easy-rsa# ./build-key ubuntu-clien
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ubuntu-clien.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) [SV]:
```



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openssl/easy-rsa
root@ubuntuser-VirtualBox: /etc/openssl/easy-rsa# Email Address [admin@jsaldana.com]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openssl/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'SV'
stateOrProvinceName     :PRINTABLE:'El Salvador'
localityName            :PRINTABLE:'San Salvador'
organizationName        :PRINTABLE:'jsaldana.soto.org'
organizationalUnitName  :PRINTABLE:'OpenVPN'
commonName              :PRINTABLE:'ubuntu-clien'
name                   :PRINTABLE:'openVPN'
emailAddress            :IA5STRING:'admin@jsaldana.com'
Certificate is to be certified until May 27 04:17:33 2021 GMT (365 days)
Sign the certificate? [y/n]:y

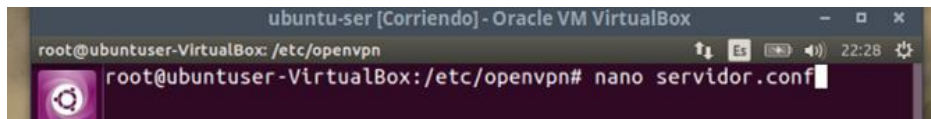
1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
root@ubuntuser-VirtualBox: /etc/openssl/easy-rsa#
```

Ya tendremos todas las claves y certificados en el directorio.

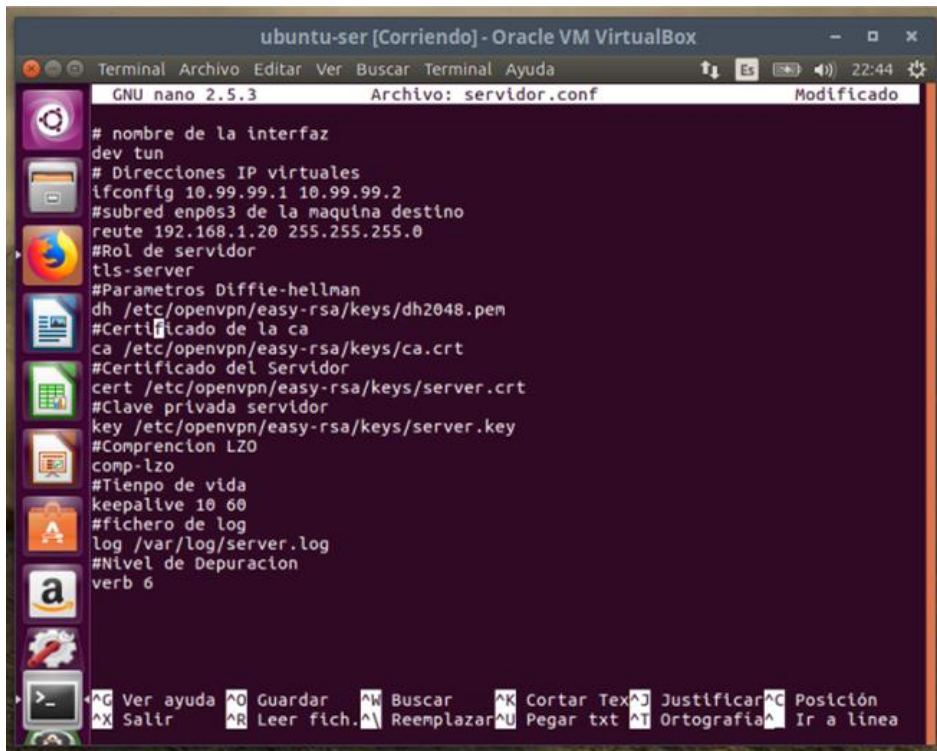


Configuración túnel en las dos maquinas

vamos a crear un fichero que se llamara servidor.conf



con el contenido siguiente:



Una vez creado y guardado el fichero reiniciamos el servicio

**/etc/init.d/openvpn restart && reboot**

, al volver a arrancar la maquina realizamos un

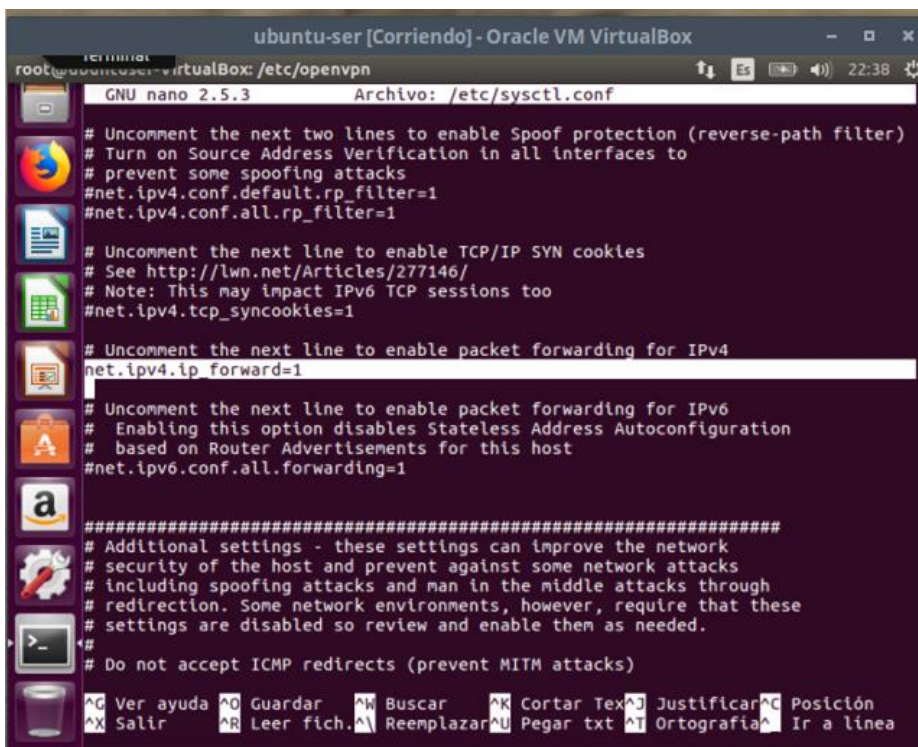
**ip a**

y observamos ya tenemos nuestro tunel:





El último paso en el servidor es permitir el enrutamiento para ello modificamos la siguiente línea en **/etc/sysctl.conf**



```
root@ubuntu-ser-VirtualBox: /etc/openvpn
GNU nano 2.5.3 Archivo: /etc/sysctl.conf

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#
```

## Ubuntu-clien

Esta máquina actuara como cliente y de igual manera se instalaran los paquete de openvpn, ssh, y openssl .

**apt-get instal openvpn**

**apt-get instal ssh**

**apt-get instal openssl**

una vez instalado, vamos a adquirir los certificados creados en nuestro servidor, para ello vamos a utilizar el comando

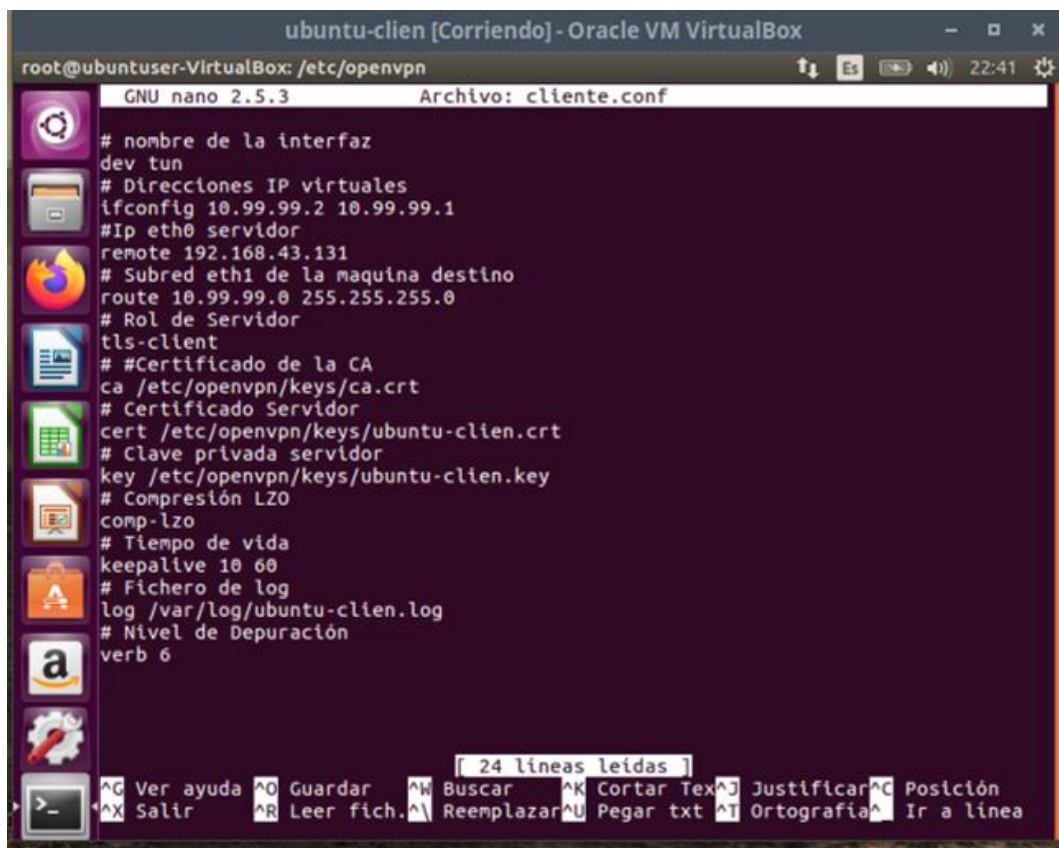


```
ubuntu-ser@192.168.43.122's password:
Amazon such file or directory
ar-VirtualBox:/etc/openvpn/easy-rsa/keys# scp ubuntu-clien.* ubuntu
u-ser@192.168.43.122:/etc/openvpn/keys/
ubuntu-ser@192.168.43.122's password:
ubuntu-clien.crt          100% 5664    5.5KB/s   00:00
ubuntu-clien.csr         100% 1110    1.1KB/s   00:00
ubuntu-clien.key         100% 1708    1.7KB/s   00:00
root@ubuntu-ser-VirtualBox:/etc/openvpn/easy-rsa/keys#
```

Creamos fichero cliente.conf dentro del archivo openvpn como super usuario

### **nano cliente.conf**

Dentro del archivo se escribirá lo siguiente:



```
ubuntu-clien [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn
GNU nano 2.5.3 Archivo: cliente.conf

# nombre de la interfaz
dev tun
# Direcciones IP virtuales
ifconfig 10.99.99.2 10.99.99.1
# Ip eth0 servidor
remote 192.168.43.131
# Subred eth1 de la maquina destino
route 10.99.99.0 255.255.255.0
# Rol de Servidor
tls-client
# #Certificado de la CA
ca /etc/openvpn/keys/ca.crt
# Certificado Servidor
cert /etc/openvpn/keys/ubuntu-clien.crt
# Clave privada servidor
key /etc/openvpn/keys/ubuntu-clien.key
# Compresión LZ0
comp-lzo
# Tiempo de vida
keepalive 10 60
# Fichero de log
log /var/log/ubuntu-clien.log
# Nivel de Depuración
verb 6

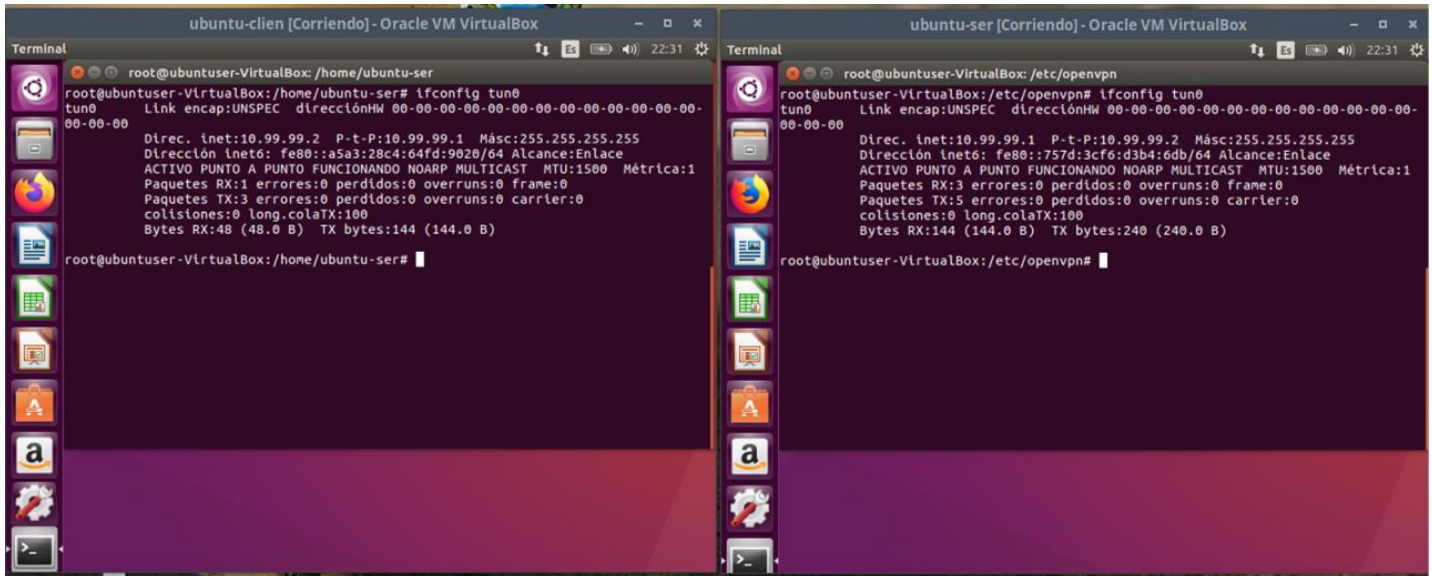
[ 24 lineas leidas ]
^G Ver ayuda ^O Guardar ^K Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografia ^_ Ir a linea
```

Guardamos la configuración Ctrl + O y Ctrl + X para salir, reiniciamos el servicio y reiniciamos la maquina como super usuario con el siguiente comando:

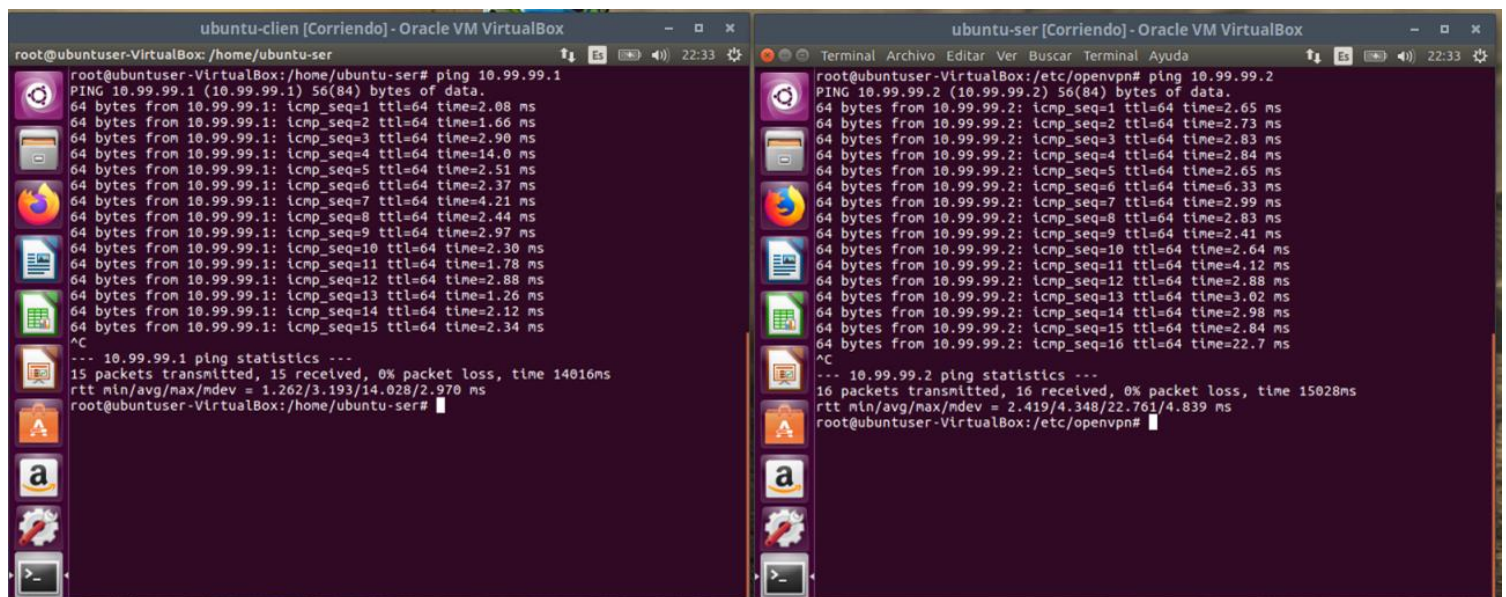
### **/etc/init.d/openvpn restart**

Luego se reinician las máquinas.

## Comprobaciones tunel



Como vemos las dos máquinas tienen el acceso a túnel ahora comprobaremos si existe comunicación entre las dos máquinas, asiendo ping, de la siguiente manera:



como vemos ambas maquinas se encuentran comunicadas entre ellas de esta manera podemos comprobar que la configuración túnel de sitio a sitio fue correcta.