

## 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:**

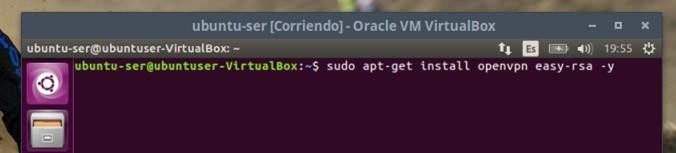
Wilber Alexander Palacios Mármol Juan Gabriel Soto Aldana

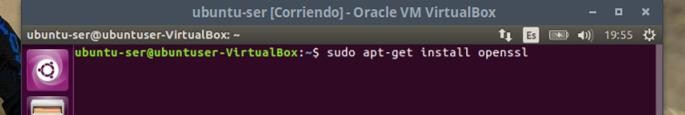
Ivan Steven Funes Ventura Yesica Yaneth najarro Moreira

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

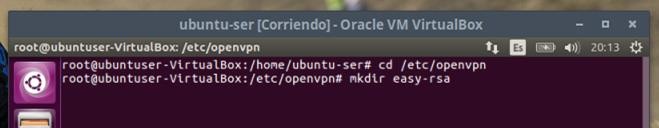
# Instalar OpenVPN

Vamos a instalar los paquetes



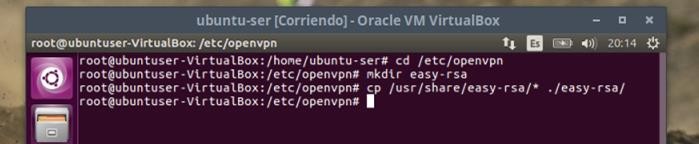


en la máquina que va a actuar de servidor «Server», una vez instalado creamos un directorio que se llamara **easy-rsa** como se muestra en la imagen:

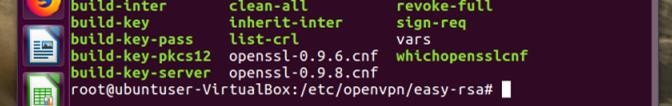


OpenVPN nos ofrece una serie de scripts para la creación de certificados auto firmados para identificar a nuestro servidor tanto como a los clientes, la ubicación de estos scripts es el directorio.

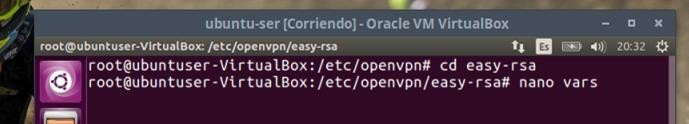
ahora copiaremos las series de scripts al directorio de la siguiente manera:



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.**



Se proceder a modificarlo con el siguiente comando :



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

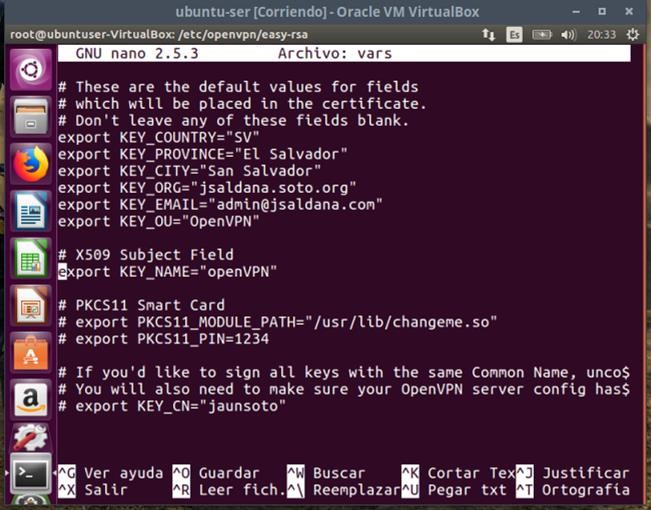
export KEY\_SIZE=2048 export CA\_EXPIRE=365 export KEY\_EXPIRE=365

export KEY\_COUNTRY="SV"

export KEY\_PROVINCE="El Savador" export KEY\_CITY="San Salvador" export KEY\_ORG="jsaldana.soto.org"

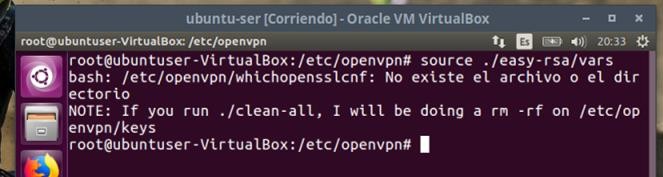
export KEY\_EMAIL="[admin@jsaldana.com](mailto:admin@jsaldana.com)" export KEY\_OU="OpenVPN"

export KEY\_NAME=openVPN export KEY\_CN=JuanluRamirez

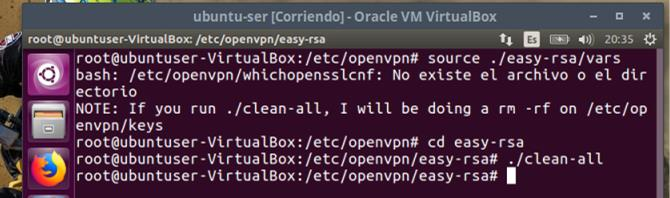


Luego de haber hecho las modificaciones en el archivo se guarda con Ctrl+o y Ctrl+x para salir

Ejecutamos el script modificado



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



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 autentificada). 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.

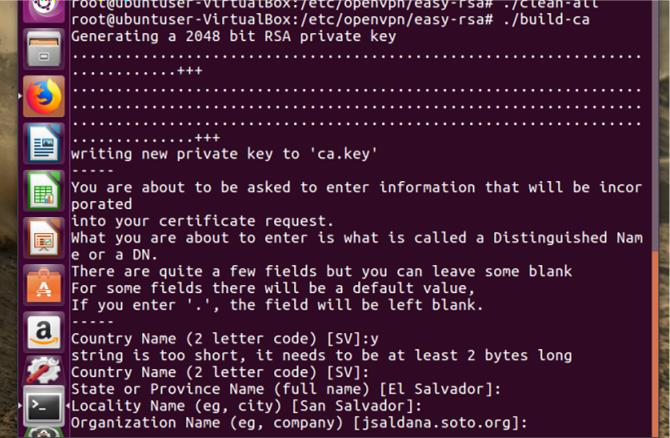
Para ello ejecutamos el script

## build-dh



**Creación certificado Autoridad certificadora**

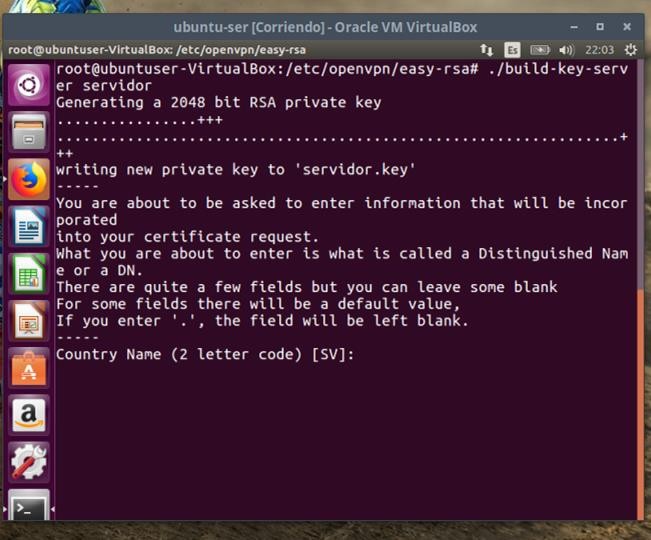
A continuación, lo que vamos a realizar la creación del certificado y se realiza ejecutando el siguiente fichero.

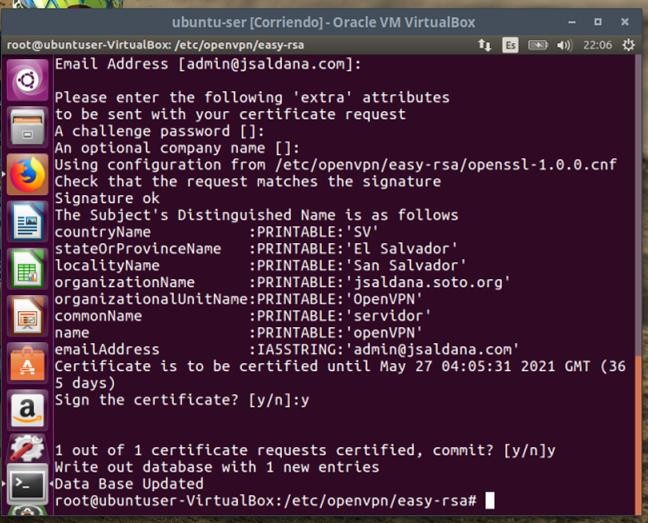


Solo damos enter según sea necesario.

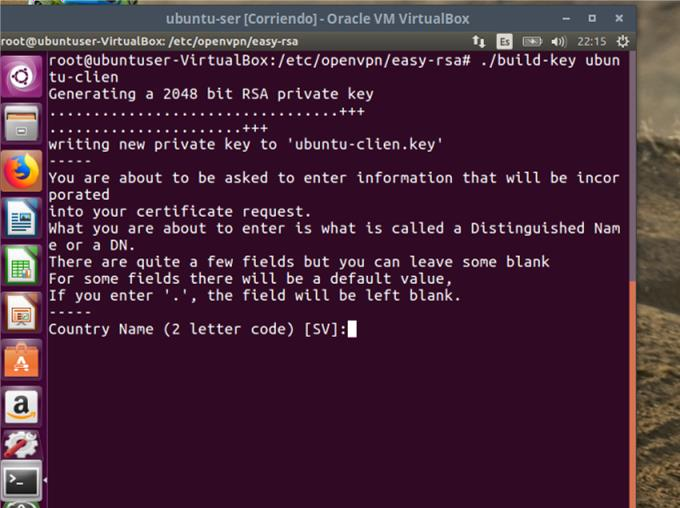
## Creación de Clave y Certificado raíz

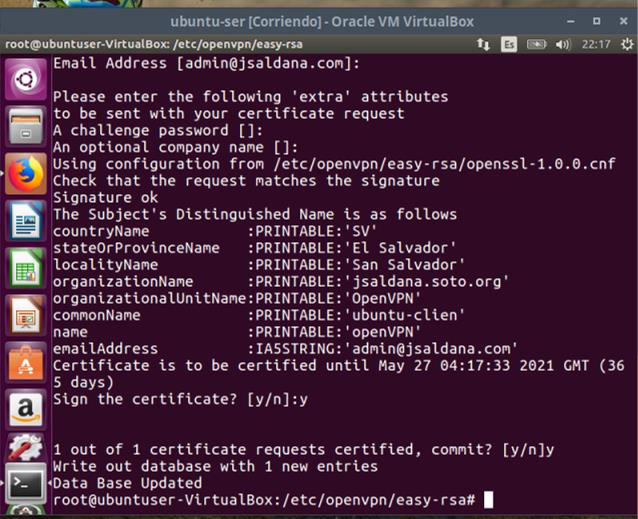
Para que OpenVPN pueda funcionar correctamente tendremos que crear un certificado y una key en el servidor para que así se pueda realizar la conexión correctamente, para ello vamos a ejecutar el siguiente fichero, seguido del nombre del servidor que en nuestro caso vamos a poner servidor.





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.

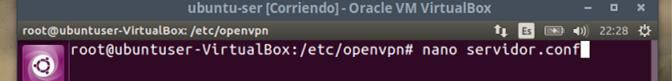


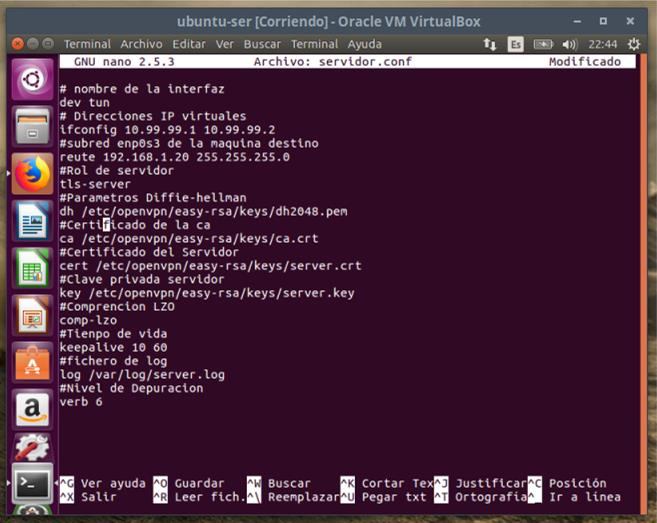


Ya tendremos todas las claves y certificados en el directorio.

Configuración túnel en las dos maquinas

vamos a crear un fichero que se llamara servidor.conf



con el contenido siguiente:

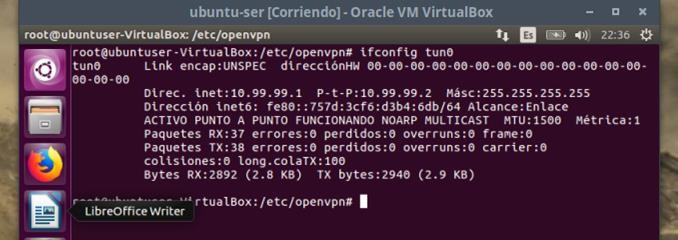
## Una vez creado y guardado el fichero reiniciamos el servicio

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

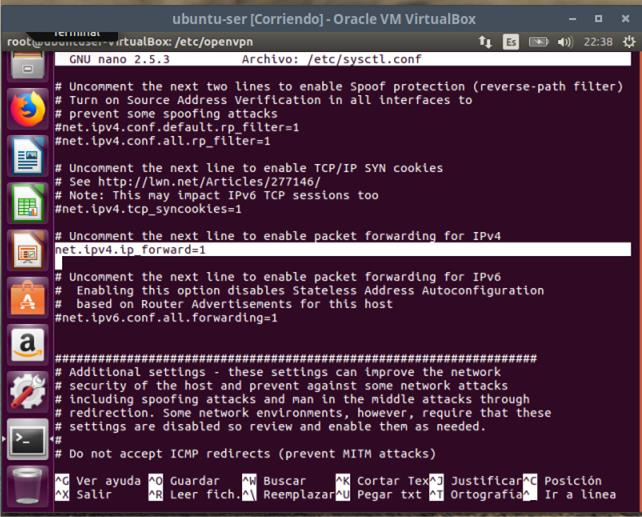
, al volver a arrancar la maquina realizamos un

## 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**



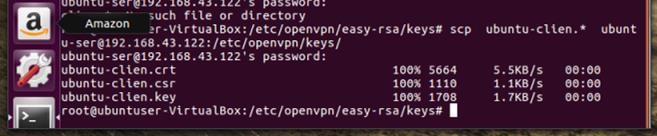
## Ubuntu-clien

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**

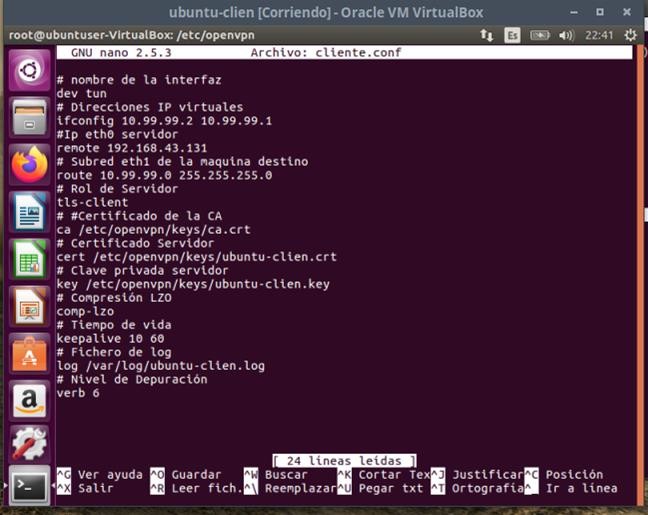
una vez instalado, vamos a adquirir los certificados creados en nuestro servidor, para ello vamos a utilizar el comando



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

## nano cliente.conf

Dentro del archivo se escribirá lo siguiente:

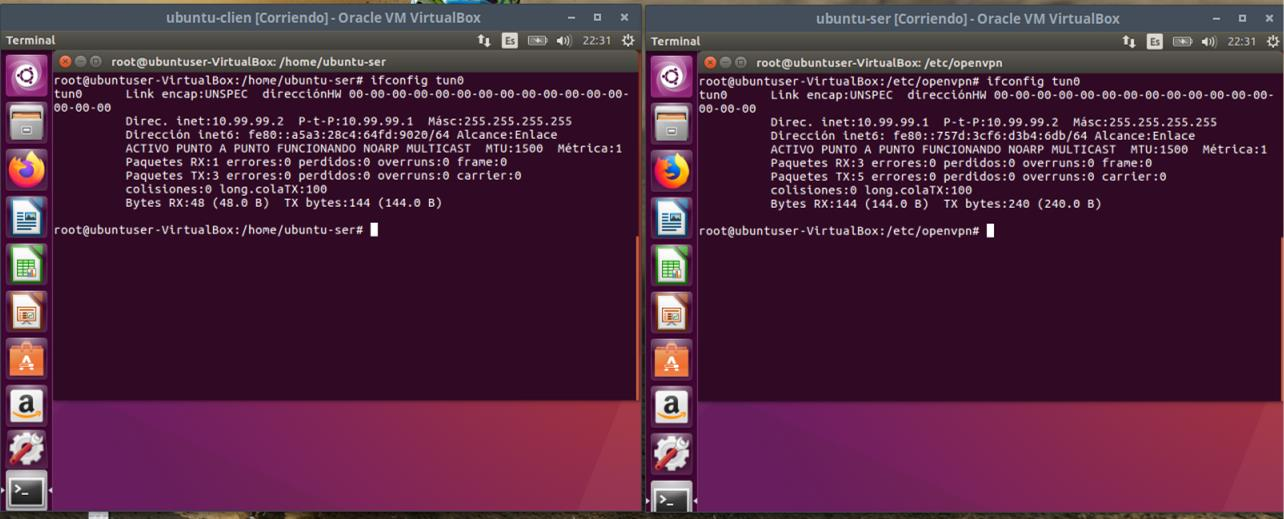


Guardamos la configuración Ctrl + O y Ctrl + X para salir, reiniciamos el servicio y reiniciamos la maquina como super usuario con el siguiente comando:

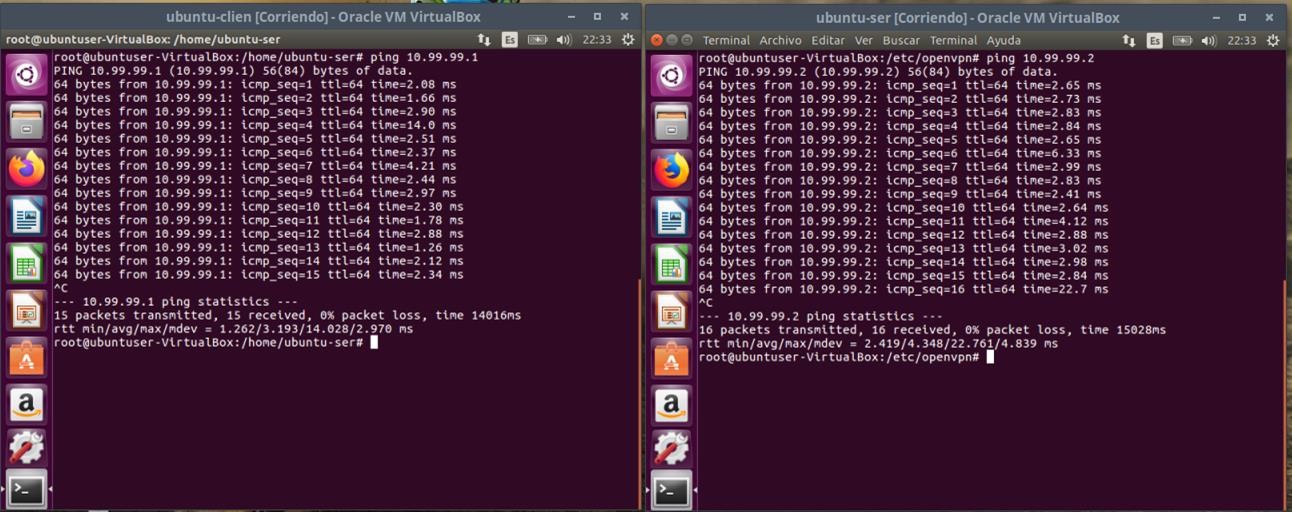
## /etc/init.d/openvpn restart

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.