

CREAR VPN EN GOOGLE CLOUD

Creación de máquina virtual

Aprovechando la capa gratuita de Google, creamos una máquina virtual que nos servirá para configurarla como vpn

Google Cloud Platform My First Project

Buscar productos y recursos

Crear una instancia

Para crear una instancia de VM, selecciona una de las opciones:

- Nueva instancia de VM**
Crea una instancia de VM desde cero
- Nueva instancia de VM a partir de una plantilla**
Crea una instancia de VM a partir de una plantilla disponible
- Nueva instancia de VM a partir de una imagen de máquina**
Crea una instancia de VM a partir de una imagen de máquina disponible
- Marketplace**
Despliega una solución lista para usarse en una instancia de VM

Nombre ⓘ
El nombre es permanente.
instance-1

Etiquetas ⓘ (Optional)
+ Añadir etiqueta

Región ⓘ
La región es permanente.
us-central1 (Iowa)

Zona ⓘ
La zona es permanente.
us-central1-a

Configuración de la máquina

Familia de máquinas
Uso general ⓘ Optimizada para la computación
Con memoria optimizada
Tipo de máquinas para cargas de trabajo habituales, optimizadas en cuanto al costo y a la flexibilidad

Serie
E2
La plataforma de CPU se elige según las que haya disponibles

Tipo de máquina
e2-medium (2 vCPU, 4 GB de memoria)

vCPU Memoria GPUs
1 núcleo compartido 4 GB -

Plataforma de CPU y GPU

Servicio de VM confidencial ⓘ
☐ Habilitar el servicio de computación confidencial en esta instancia de VM.

Contenedor ⓘ
☐ Desplegar una imagen de contenedor en esta instancia de VM. [Más información](#)

Disco de arranque ⓘ
Nuevo disco persistente estándar de 10 GB
Imagen
Debian GNU/Linux 10 (buster) [Cambiar](#)

Te quedan 264,768165 \$ de crédito de la versión de prueba gratuita.
Precio mensual estimado: 24,86 \$
Eso significa 0,034 \$ por hora
Paga por lo que uses: facturación por segundos, sin gastos por adelantado.
[Detalles](#)

Seleccionamos una instancia de Ubuntu 18.04

Crear una instancia

vCPU Memoria GPUs
1 núcleo compartido 4 GB -

Plataforma de CPU y GPU

Servicio de VM confidencial ⓘ
☐ Habilitar el servicio de computación confidencial en esta instancia de VM.

Contenedor ⓘ
☐ Desplegar una imagen de contenedor en esta instancia de VM. [Más información](#)

Disco de arranque ⓘ
Nuevo disco persistente estándar de 10 GB
Imagen
Debian GNU/Linux 10 (buster) [Cambiar](#)

Identidad y acceso de API ⓘ

Cuenta de servicio ⓘ
Compute Engine default service account

Alcance del acceso ⓘ
☒ Permitir el acceso predeterminado
☐ Permitir el acceso completo a todas las API de Cloud
☐ Definir acceso para cada API

Configuración ⓘ
Añade reglas de configuración y etiquetas para permitir tráfico de red concreto de Internet
☐ Permitir el tráfico HTTP
☐ Permitir el tráfico HTTPS

Administración, seguridad, discos, redes, único propietario

Se utilizará tu crédito de la versión de prueba gratuita para esta instancia de VM.
Nivel gratuito de GCP ⓘ

[Crear](#) [Cancelar](#)

REST o línea de comandos equivalentes

Crear reglas de Firewall

Google Cloud Platform My First Project

Buscar productos y recursos

Red de VPC

Redes de VPC

Direcciones IP externas

Cortafuegos

Rutas

Emparejamiento entre redes ...

VPC compartida

Acceso a VPC sin servidor

Replicación de paquetes

Crear regla de cortafuegos

Actualizar

Configurar registros

Eliminar

Las reglas de cortafuegos controlan el tráfico entrante o saliente de una instancia. De forma predeterminada, se bloquea el tráfico entrante que sea ajeno a tu red. [Más información](#)

Nota: Los cortafuegos de App Engine se administran en [esta página](#).

Filtrar tabla

Nombre	Tipo	Destinos	Filtros	Protocolos y puertos	Acción	Prioridad	Red	Registros	Número de coincidencias	Última coincidencia	Estadísticas
default-allow-http	Entrada	http-server	Intervalos de	tcp:80	Permitir	1000	default	Desactivado	—	—	▼
default-allow-https	Entrada	https-server	Intervalos de	tcp:443	Permitir	1000	default	Desactivado	—	—	▼
default-allow-ssh	Entrada	Aplicar a todos	Intervalos de	all	Permitir	1000	default	Desactivado	—	—	▼
default-allow-icmp	Entrada	Aplicar a todos	Intervalos de	icmp	Permitir	65534	default	Desactivado	—	—	▼
default-allow-internal	Entrada	Aplicar a todos	Intervalos de	tcp:0-65535 udp:0-65535 icmp	Permitir	65534	default	Desactivado	—	—	▼
default-allow-rdp	Entrada	Aplicar a todos	Intervalos de	tcp:3389	Permitir	65534	default	Desactivado	—	—	▼
default-allow-ssh	Entrada	Aplicar a todos	Intervalos de	tcp:22	Permitir	65534	default	Desactivado	—	—	▼
salida	Salida	Aplicar a todos	Intervalos de	all	Permitir	1000	default	Desactivado	—	—	▼
vpnopensalida	Salida	Aplicar a todos	Intervalos de	udp:1194	Permitir	1000	default	Desactivado	—	—	▼

Regla de entrada y salida

Permite la entrada en cualquier rango de ip y en el puerto udp 1194

Google Cloud Platform My First Project

Buscar productos y recursos

Red de VPC

Redes de VPC

Direcciones IP externas

Cortafuegos

Rutas

Emparejamiento entre redes ...

VPC compartida

Acceso a VPC sin servidor

Replicación de paquetes

Detalles de regla de cortafuegos

Editar

Eliminar

default-allow-http

Registros

Desactivar

Ver

Red

default

Prioridad

1000

Dirección

Entrada

Acción tras coincidencia

Permitir

Filtros de origen

Intervalos de IP

0.0.0.0/0

Protocolos y puertos

udp:1194

Aplicación obligatoria

Habilitado

Estadísticas

Ninguna

Supervisión de número de aciertos

—

Se aplica a las instancias

En la siguiente tabla solo se muestran las instancias de VM que tienes permiso para ver. Es posible que la red "default" contenga otras instancias que no figuran en la tabla.

Descargamos <https://openvpn.net/community-downloads/> para conectar hacia la vpn

Corremos los siguientes comandos:

- Copiamos el archivo de las configuraciones de la vpn a la virtual y las ejecutamos

- Se definen las siguientes configuraciones

- Comienza a configurarse la virtual como una vpn

```
root@vpn-ubuntu:/home/yamir84cuba
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/openvpn/easy-rsa/pki/private/client.key.knIpYwIaQ'
-----
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Can't load /etc/openvpn/easy-rsa/pki/.rnd into RNG
139823727624640:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:
88:Filename=/etc/openvpn/easy-rsa/pki/.rnd
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'client'
Certificate is to be certified until Oct  2 15:27:35 2030 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

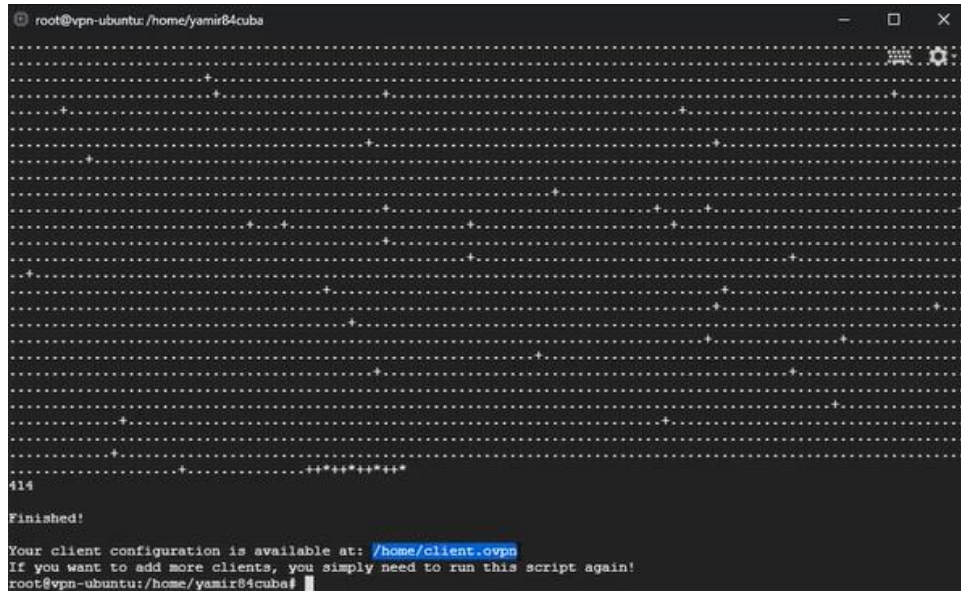
Using SSL: openssl OpenSSL 1.1.1 11 Sep 2018
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Can't load /etc/openvpn/easy-rsa/pki/.rnd into RNG
139928318529984:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:
88:Filename=/etc/openvpn/easy-rsa/pki/.rnd

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

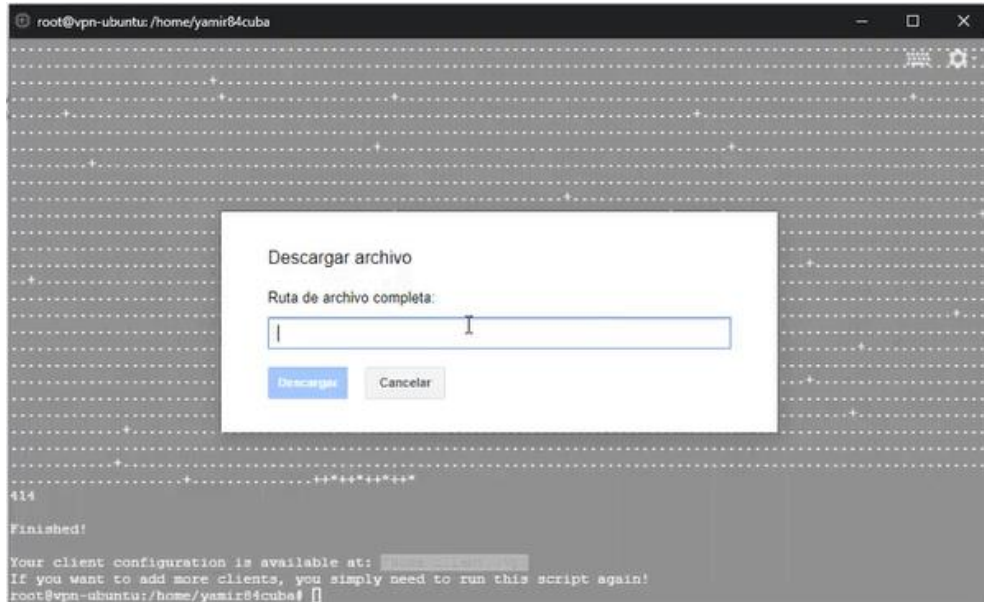
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.
.....+.
.....+.
.....+.
.....+.
.....+
```

Descargar el archivo del cliente nuevo

Al terminar la instalación nos muestra la ubicación del archivo de conexión del cliente, lo seleccionamos y lo copiamos



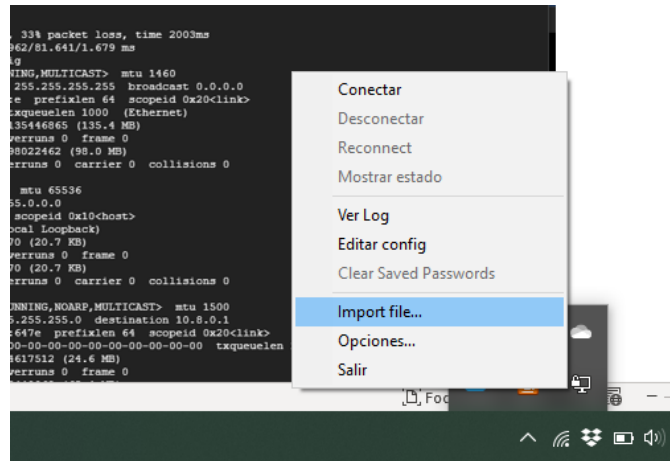
Nos vamos a las configuraciones que nos provee la conexión SSH de Google cloud en la esquina superior derecha de la pantalla y seleccionamos descargar archivo



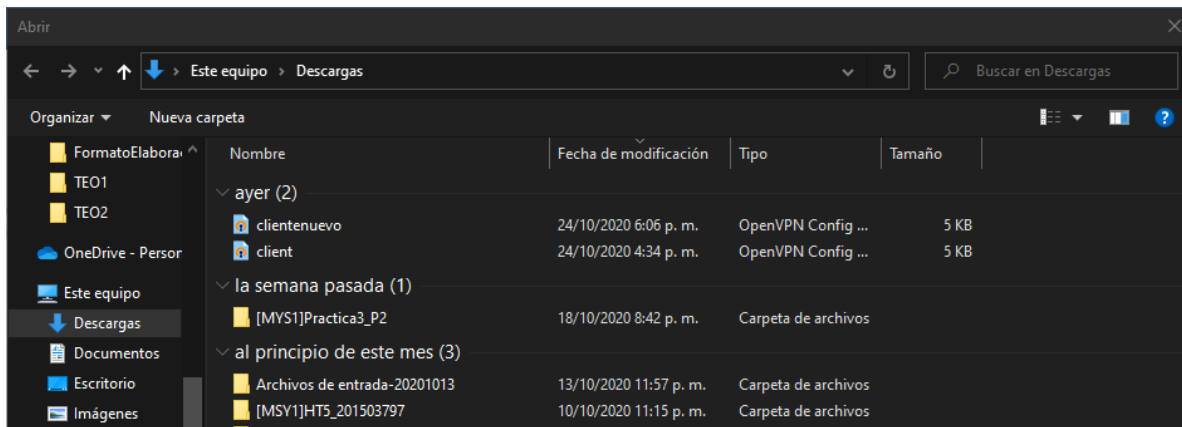
Ingresamos el path que copiamos y le damos Descargar

Conectarse a la VPN

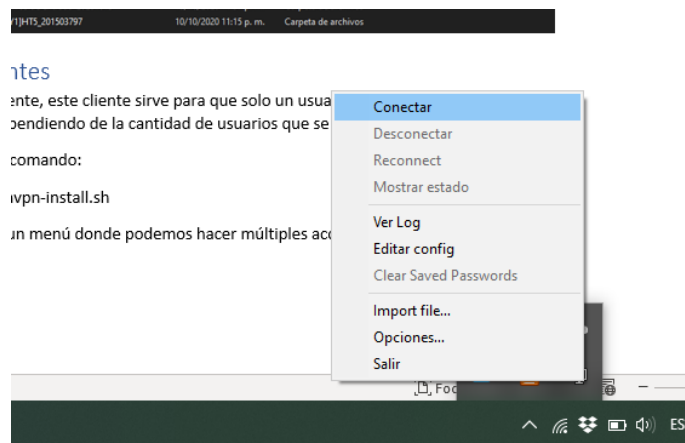
Con el programa `openvpn` instalado, nos vamos a la esquina superior izquierda y le damos click derecho al ícono de la aplicación y seleccionamos



Y nos vamos a la ubicación donde se descargó el cliente y lo cargamos.



Ahora la aplicación openvpn nos habilita una nueva opción que es “Conectar”



Nos conecta a la vpn y nos asigna una dirección ip dentro de la red de la vpn de manera dinámica

```
C:\WINDOWS\system32\cmd.exe

Adaptador desconocido OpenVPN TAP-Windows6:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::a466:80f6:cfb0:98bf%41
    Dirección IPv4. . . . . : 10.8.0.2
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

Adaptador desconocido OpenVPN Wintun:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::985c:72b7:205f:1c7d%4
    Dirección IPv4. . . . . : 192.168.1.4
    Máscara de subred. . . . . : 255.255.255.0
```

Utilizando una página web (<https://www.myip.com>) podemos ver que tenemos la misma ip pública que la máquina virtual

My First Project

Buscar productos y recursos

Instanc... de VM

CREAR INSTANCIA

IMPORTAR VM

ACTUALIZAR

INICIAR/REANUDAR

GESTIONAR ACCESO

Nombre	Zona	Recomendación	Usada por	IP interna	IP externa	Conectar
vpn-ubuntu	us-central1-a			10.128.0.14 (nic0)	34.71.50.210	SSH

Acciones relacionadas

- Ver informe de facturación: Ver y gestionar la facturación de Compute Engine
- Monitorizar VMs: Consulta los valores atípicos de las VM en métricas como la CPU y la red
- Consultar registros de VM: Consulta, busca, analiza y descarga registros de instancias de VM
- Configurar reglas de cortafuegos: Controlar el tráfico que entra y sale de las instancias de VM

Probar conexión

Vamos a la máquina virtual y escribimos el comando para ver la ip:

- Ifconfig

```

amontufarc97@vpn-ubuntu: ~ - Opera
ssh.cloud.google.com/projects/velvety-study-291323/zones/us-central1-a/instances/vpn-ubuntu

amontufarc97@vpn-ubuntu:~$ ping 10.8.0.2
PING 10.8.0.2 (10.8.0.2) 56(84) bytes of data.
64 bytes from 10.8.0.2: icmp_seq=1 ttl=128 time=81.6 ms
64 bytes from 10.8.0.2: icmp_seq=2 ttl=128 time=78.2 ms
^C
--- 10.8.0.2 ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 2003ms
rtt min/avg/max/mdev = 78.283/79.962/81.641/1.679 ms
amontufarc97@vpn-ubuntu:~$ ifconfig
ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460
    inet 10.128.0.14 netmask 255.255.255.255 broadcast 0.0.0.0
    inet6 fe80::4001:aff:fe80:e prefixlen 64 scopeid 0x20<link>
    ether 42:01:0a:80:00:0e txqueuelen 1000 (Ethernet)
    RX packets 174476 bytes 135446865 (135.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 165642 bytes 98022462 (98.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 200 bytes 20770 (20.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 200 bytes 20770 (20.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.8.0.1 netmask 255.255.255.0 destination 10.8.0.1
    inet6 fe80::1ef5:5c44:30c:647e prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
    RX packets 65209 bytes 24617512 (24.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 87655 bytes 65440068 (65.4 MB)
    TX errors 0 dropped 354 overruns 0 carrier 0 collisions 0

amontufarc97@vpn-ubuntu:~$
de subred . . . . . : 255.255.255.0

```

Hacemos ping a la ip de la red interna de la máquina virtual y a la ip de la vpn

```

C:\WINDOWS\system32\cmd.exe

C:\Users\andre>ping 10.8.0.1

Haciendo ping a 10.8.0.1 con 32 bytes de datos:
Respuesta desde 10.8.0.1: bytes=32 tiempo=80ms TTL=64
Respuesta desde 10.8.0.1: bytes=32 tiempo=82ms TTL=64
Respuesta desde 10.8.0.1: bytes=32 tiempo=93ms TTL=64
Respuesta desde 10.8.0.1: bytes=32 tiempo=81ms TTL=64

Estadísticas de ping para 10.8.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 80ms, Máximo = 93ms, Media = 84ms

C:\Users\andre>ping 10.128.0.14

Haciendo ping a 10.128.0.14 con 32 bytes de datos:
Respuesta desde 10.128.0.14: bytes=32 tiempo=102ms TTL=64
Respuesta desde 10.128.0.14: bytes=32 tiempo=80ms TTL=64
Respuesta desde 10.128.0.14: bytes=32 tiempo=80ms TTL=64
Respuesta desde 10.128.0.14: bytes=32 tiempo=81ms TTL=64

Estadísticas de ping para 10.128.0.14:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 80ms, Máximo = 102ms, Media = 85ms

C:\Users\andre>

```


Creación de clientes

Al inicio creamos un cliente, este cliente sirve para que solo un usuario ingrese, entonces debemos crear varios clientes dependiendo de la cantidad de usuarios que se van a conectar a la vpn

Volvemos a ejecutar el comando:

- `sudo bash openvpn-install.sh`

Y nos aparecerá ahora un menú donde podemos hacer múltiples acciones, seleccionamos un nuevo usuario y agregamos un nuevo nombre para el cliente y esto generará un nuevo archivo

```
amontufarc97@vpn-ubuntu: ~ - Opera
ssh.cloud.google.com/projects/velvety-study-291323/zones/us-central1-a/instances/vpn-ubuntu
Parece que OpenVPN ya está instalado.
Qué quieres hacer?
1) Agregar nuevo usuario
2) Eliminar usuario existente
3) Desinstalar OpenVPN
4) Salir
Selecciona una opción [1-4]: 2
Selecciona el certificado de cliente existente que desea remover:
1) client
2) clientel
3) cliente
4) clientenuevo
Selecciona un cliente [1-4]: 3
Realmente esta seguro de eliminar el cliente cliente? [y/N]: y
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Can't load /etc/openvpn/easy-rsa/pki/.rnd into RNG
140288485097920:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:
88:Filename=/etc/openvpn/easy-rsa/pki/.rnd
Revoking Certificate 7F16747CE4E5ECS7314C310C8AA6559.
Data Base Updated
Using SSL: openssl OpenSSL 1.1.1 11 Sep 2018
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Can't load /etc/openvpn/easy-rsa/pki/.rnd into RNG
139826874253760:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:
88:Filename=/etc/openvpn/easy-rsa/pki/.rnd
An updated CRL has been created.
CRL file: /etc/openvpn/easy-rsa/pki/crl.pem
Certificado para el cliente cliente eliminado!
amontufarc97@vpn-ubuntu:~$ ping 10.8.0.2
PING 10.8.0.2 (10.8.0.2) 56(84) bytes of data.
```

Prueba de conexión en distintas máquinas físicas

Con la ayuda de un compañero hicimos esta prueba, el se conectó desde su ubicación a la vpn con el último cliente creado, asignándole una ip distinta a la mia

```
Configuración IP de Windows

Adaptador desconocido OpenVPN TAP-Windows6:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::3898:77e2:66bf:566%81
Dirección IPv4. . . . . : 10.8.0.3
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
```

Hicimos una prueba de ping entre nuestras máquinas sin importar la ubicación donde estuviéramos y logramos conectarnos entre nosotros sin ningún problema

C:\WINDOWS\system32\cmd.exe - ping -t 10.8.0.2

C:\Users\Junior>ping -t 10.8.0.2

Haciendo ping a 10.8.0.2 con 32 bytes de datos:

Respuesta desde 10.8.0.2: bytes=32 tiempo=152ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=149ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=155ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=151ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=161ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=152ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=160ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=154ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=152ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=239ms TTL=127

Respuesta desde 10.8.0.2: bytes=32 tiempo=179ms TTL=127