OpenVPN

OpenVPN es un programa open source de gestión de redes virtuales privadas (VPN, *Virtual Private Network*). Apoyándose en SSL, permite crear un canal de comunicación seguro a través de una red IP.

1. Los principios de OpenVPN

OpenVPN ofrece servicios de autenticación y de confidencialidad. Permite conectar hosts con redes, dándoles un canal seguro (túnel) a través de redes IP.

a. Autentificación

Los extremos del túnel seguro, es decir los dos sistemas que aseguran el cifrado de los flujos salientes y el descifrado de los flujos entrantes, tienen que autenticarse mutuamente.

OpenVPN administra diferentes modos de autentificación, los dos más usados son la autenticación por clave compartida y la autentificación por certificados digitales X.509. La primera técnica es más simple de implementar, pero menos segura.

b. Confidencialidad

La confidencialidad de las comunicaciones la asegura la biblioteca OpenSSL. El cifrado de los intercambios utiliza por defecto el algoritmo Blowfish, pero acepta también algoritmos simétricos (AES especialmente).

c. Tipos de funcionamiento de red

OpenVPN propone diferentes tipos de conexión entre sistemas y redes:

- El modo punto a punto: la VPN conecta solamente dos máquinas.
- El modo sitio a sitio: la VPN se usa para conectar dos redes entre ellas. Dos servidores OpenVPN aseguran la implementación del túnel, pero los extremos de

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema

tráfico son las dos redes conectadas. Los servidores OpenVPN tienen una función de enrutamiento seguro entre las dos redes.

- El modo acceso remoto: la VPN permite conectar una máquina a una red.
- El modo *bridge*: la VPN conecta dos redes remotas a nivel físico.

2. Creación de un túnel punto a punto

El túnel punto a punto permite conectar dos máquinas a través de una red.

a. Autentificación por clave compartida

El archivo de clave puede ser generado por el comando `openvpn`. Tiene que estar presente en el servidor y en el cliente, por lo tanto hay que copiarlo en la otra máquina después de haberlo generado, usando un medio seguro (pendrive USB, `scp` o `sftp`).

Sintaxis

```
openvpn --genkey --secret RutaArchivoClave
```

Ejemplo

Creación del archivo de clave:

```
openvpn --genkey --secret secret.key
cat secret.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
1a0cf1144f1e99f9976cbb1609c917d3
44d4a7b8e9da0b0ec6a9a728a24ad545
0027ba5552bf1195ba4108beecb62b5a
b0cfe83e41007d250ce95e5f493312e9
7586f78da40b437138970b0246f9f4cf
```

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema

```
296f95b5e477bc23bfd79ccc38bf12d9
51587df33fce4f3986ce930445887e47
9826d8276d5f5b9e1c6cde1c8e285e19
7ae80be18a3d4122cafdc8e6e49ec259
c3d810e2457b23c1bb58029b516feefa
8a4d503c556b06bbd5f32348f2082259
67e5a24bd7ff64e2a6c16e2e2b1a8fe2
24efb6061a53b8cc37bee3b4fa39ed37
2b883890046b1640de4b8c3887d17f1c
c0f07c9908808f859044df8a07d2d891
de44880fce62153b2ae3083bd7861183
-----END OpenVPN Static key V1-----
```

b. Archivos de configuración

Los archivos de configuración se encuentran por defecto en `/etc/openvpn/client` y `/etc/openvpn/server`. Son necesarios un archivo, con extension `.conf`, para el cliente y otro para servidor.

Archivo de configuración OpenVPN

```
remote idServidor
dev tun
ifconfig IP_local IP_remota
secret RutaArchivoclave
route idRedRemota Máscara
```

Donde:

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema

`remote idServidor`	En el cliente: nombre o dirección del servidor OpenVPN.
`dev tun`	Modo de funcionamiento de red (`tun` = túnel).
`ifconfig IP_local IP_remota`	Dirección IP local y remota. Estarán asociadas, por OpenVPN, a una tarjeta de interfaz virtual punto a punto.
`secret RutaArchivoClave`	Camino de acceso al archivo de clave.
`route idRedRemota MÆscara`	En el cliente: identificador y máscara de red accesible a partir del servidor OpenVPN.

Ejemplo

Archivo de configuración en el servidor:

```
vi /etc/openvpn/server/server.conf
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret secret.key
```

Archivo de configuración en el cliente:

```
vi /etc/openvpn/client/client.conf
remote centos8
dev tun
ifconfig 10.8.0.2 10.8.0.1
secret secret.key
route 192.168.1.0 255.255.255.0
```

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema

c. Implementación del túnel VPN

Una vez hechos los archivos de configuración y las claves instaladas en el servidor y en el cliente, hay que iniciar en cada uno de ellos el servicio OpenVPN, usando su script de inicio `init System V` o a través de `systemd`.

OpenVPN establece el túnel usando UDP, en el puerto 1194.

Ejemplo

Ejecución del servicio en el cliente y en el servidor.

Lista de las tarjetas de interfaz de red del sistema cliente:

```
ip -br link
lo               UNKNOWN        00:00:00:00:00:00 <LOOPBACK,UP,LOWER_UP>
enp0s10          UP             00:1b:24:6a:78:14 <BROADCAST,MULTICAST,UP,LOWER_UP>
```

Se inicia el servicio OpenVPN:

```
openvpn --config /etc/openvpn/client/client.conf
 Thu Jun 18 19:15:28 2020 disabling NCP mode (--ncp-disable) because not in P2MP client
or server mode
Thu Jun 18 19:15:28 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
[EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20 2019
Thu Jun 18 19:15:28 2020 library versions: OpenSSL 1.1.1d  10 Sep 2019, LZO 2.10
Thu Jun 18 19:15:28 2020 WARNING: INSECURE cipher with block size less than 128 bit
(64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher with a
larger block size (e.g. AES-256-CBC).
Thu Jun 18 19:15:28 2020 WARNING: INSECURE cipher with block size less than 128 bit
(64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher with a
larger block size (e.g. AES-256-CBC).
Thu Jun 18 19:15:28 2020 TUN/TAP device tun0 opened
Thu Jun 18 19:15:28 2020 /sbin/ip link set dev tun0 up mtu 1500
Thu Jun 18 19:15:28 2020 /sbin/ip addr add dev tun0 local 10.8.0.2 peer 10.8.0.1
Thu Jun 18 19:15:28 2020 TCP/UDP: Preserving recently used remote address:
[AF_INET]192.168.0.60:1194
Thu Jun 18 19:15:28 2020 UDP link local (bound): [AF_INET][undef]:1194
```

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema

```
Thu Jun 18 19:15:28 2020 UDP link remote: [AF_INET]192.168.0.60:1194
beta:~# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=0.864 ms
```

Mostramos la lista de las tarjetas de interfaz de red:

```
ip -br a
lo               UNKNOWN        127.0.0.1/8::1/128
enp0s10          UP             192.168.0.70/24
2a01:e35:2439:1510:21b:24ff:fe6a:7814/64 fe80::21b:24ff:fe6a:7814/64
tun0             UNKNOWN        10.8.0.2 peer 10.8.0.1/32 fe80::6877:a3e:f2a:1d50/64
```

El servidor OpenVPN ha creado una tarjeta de interfaz virtual `tun0`.

En el lado del servidor, se ejecuta también el servicio.

Después de haber copiado el archivo de clave, configuramos `OpenVPN` como servidor:

```
openvpn --config /etc/openvpn/server/server.conf
Thu Jun 18 19:56:17 2020 disabling NCP mode (--ncp-disable) because not in P2MP client
or server mode
Thu Jun 18 19:56:17 2020 OpenVPN 2.4.9 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO]
[LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 24 2020
Thu Jun 18 19:56:17 2020 library versions: OpenSSL 1.1.1c FIPS  28 May 2019, LZO 2.08
Thu Jun 18 19:56:17 2020 WARNING: INSECURE cipher with block size less than 128 bit
(64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher with a
larger block size (e.g. AES-256-CBC).
Thu Jun 18 19:56:17 2020 WARNING: INSECURE cipher with block size less than 128 bit
(64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher with a
larger block size (e.g. AES-256-CBC).
Thu Jun 18 19:56:17 2020 TUN/TAP device tun0 opened
Thu Jun 18 19:56:17 2020 /sbin/ip link set dev tun0 up mtu 1500
Thu Jun 18 19:56:17 2020 /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
Thu Jun 18 19:56:17 2020 Could not determine IPv4/IPv6 protocol. Using AF_INET
Thu Jun 18 19:56:17 2020 UDPv4 link local (bound): [AF_INET][undef]:1194
```

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema

```
Thu Jun 18 19:56:17 2020 UDPv4 link remote: [AF_UNSPEC]
```

Mostramos la lista de las tarjetas de interfaces de red:

```
ip -br a
lo               UNKNOWN        127.0.0.1/8::1/128
enp38s0          UP             192.168.0.60/24
2a01:e35:2439:1510:e611:5bff:fe50:1332/64 fe80::e611:5bff:fe50:1332/64
wlo1             DOWN
tun0             UNKNOWN        10.8.0.1 peer 10.8.0.2/32
fe80::87be:dc8d:2826:79c6/64
```

El servidor OpenVPN también ha creado una tarjeta de interfaz virtual `tun0`.

Los dos sistemas pueden comunicarse entre ellos, con el comando `ping` por ejemplo.

Desde el sistema cliente `debian10` :

```
ping -c 1 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=0.953 ms

--- 10.8.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.953/0.953/0.953/0.000 ms
```

Desde el sistema servidor `centos8` :

```
ping -c 1 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=64 time=0.975 ms

--- 10.8.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.975/0.975/0.975/0.000 ms
```

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema

Usamos el túnel para conectarnos, desde la máquina `centos8`, al servidor HTTP de la máquina `debian10`:

```
wget -O - 10.8.0.2 | more
--2020-06-18 20:12:43--  http://10.8.0.2/
Conectando con 10.8.0.2:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 10701 (10K) [text/html]
Grabando a: « STDOUT »

-           100%[=============================>]  10,45K  --.-KB/s    ds 0,001s

2020-06-18 20:12:43 (8,96 MB/s) — escritos a stdout [10701/10701]


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>Apache2 Debian Default Page: It works</title>
  <style type="text/css" media="screen">
[...]
```

El túnel está operativo.

© Éditions ENI - Todos los derechos reservados - Copia personal de Diego Armando Simbaña Quisilema