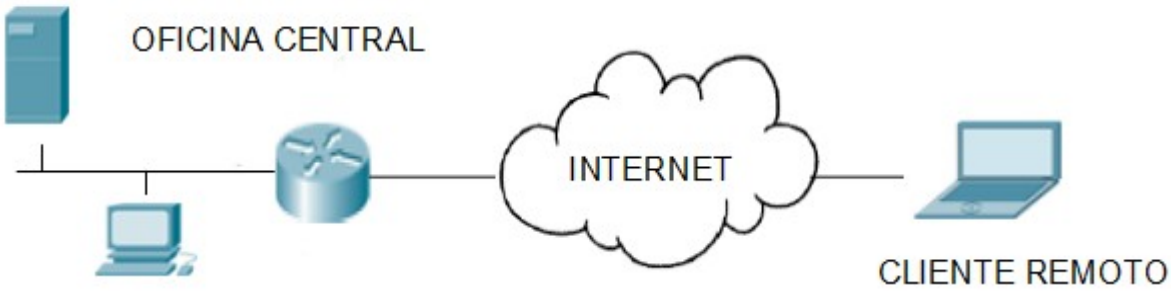
OpenVPN: Una solución VPN basada en SSL/TLS

Escenario 1: Acceso remoto



En este primer escenario vamos a establecer una VPN de acceso remoto. La autenticación será con TLS utilizando certificados X.509 y la asignación de direcciones dinámica.

Direcciones del servidor OpenVPN:

- Eth0: IP Pública, 80.80.80.1/24
- Eth1: Red Local interna, 192.168.1.1/24
- Dirección virtual: 10.0.0.1/24

Direcciones del cliente remoto:

- IP Pública: 80.80.80.2/24
- Dirección virtual: una de la red 10.0.0.0/24 que le asignará el servidor OpenVPN

Fichero de configuración del servidor: /etc/openvpn/office.com

```
#Dispositivo de túnel
dev tun

#Direcciones IP virtuales
server 10.0.0.0 255.255.255.0

#subred local
push “route 192.168.1.0
255.255.255.0”

# Rol de servidor
tls-server

#Parámetros Diffie-Hellman
dh /etc/openvpn/dh1024.pem

#Certificado de la CA
ca /etc/openvpn/ca.crt
```

```
#Certificado local
cert /etc/openvpn/server.crt

#Clave privada local
key /etc/openvpn/server.key

#Activar la compresión LZO
comp-lzo

#Detectar caídas de la conexión
keepalive 10 60

#Archivo de log
log /var/log/office.log

#Nivel de información
verb 3
```

OpenVPN: Una solución VPN basada en SSL/TLS

En el servidor OpenVPN hay que activar el enrutamiento y copiar en el directorio /etc/openvpn los archivos dh1024.pem, ca.crt, server.crt y server.key

En los clientes que quieran conectarse por acceso remoto a la VPN habrá que copiar el certificado digital y la clave privada del usuario, así como el certificado de la CA a su propio directorio /etc/openvpn.

Configuración del cliente: /etc/openvpn/user1.conf

```
#Dispositivo de túnel
dev tun

#Direcciones remota
remote 80.80.80.1

#Aceptar directivas del extremo
remoto
pull

# Rol de cliente
tls-client

#Certificado de la CA
ca /etc/openvpn/ca.crt

#Certificado local
cert /etc/openvpn/client1.crt

 #Clave privada local
 key /etc/openvpn/client1.key

 #Activar la compresión LZO
 comp-lzo

 #Detectar caídas de la conexión
 keepalive 10 60

 #Nivel de información
 verb 3
```

OpenVPN: Una solución VPN basada en SSL/TLS

Escenario 2: Site-to-Site

En este segundo escenario se va a establecer una VPN de sitio a sitio. La autenticación será basada en TLS utilizando certificados X.509.Las direcciones del servidor OpenVPN de la oficina central son:

- Eth0: IP Pública, 80.80.80.1/24
- Eth1: Red Local interna, 192.168.1.1/24
- Dirección virtual: 10.0.0.1/24

Las direcciones del servidor OpenVPN de la oficina remota son:

- Eth0: IP Pública, 80.80.80.2/24
- Eth1: Red Local interna, 192.168.2.1/24
- Dirección virtual: 10.0.0.2/24

Configuración del router de la oficina central, /etc/openvpn/office1.conf :

```
#Dispositivo de túnel                #Certificado local
dev tun                              cert /etc/openvpn/server.crt

#Direcciones IP virtuales             #Clave privada local
ifconfig 10.0.0.1 10.0.0.2           key /etc/openvpn/server.key

#subred remota                       #Activar la compresión LZO
route 192.168.2.0 255.255.255.0      comp-lzo

# Rol de servidor                    #Detectar caídas de la conexión
tls-server                           keepalive 10 60

#Parámetros Diffie-Hellman           #Archivo de log
dh /etc/openvpn/dh1024.pem           log /var/log/office1.log

#Certificado de la CA                #Nivel de información
ca /etc/openvpn/ca.crt               verb 3
```

Configuración del router de la oficina remota, /etc/openvpn/office2.conf :

```
#Dispositivo de túnel
dev tun

#Direcciones IP virtuales
ifconfig 10.0.0.2 10.0.0.1

#Dirección IP remota
remote 80.0.0.1

#Subred remota
route 192.168.1.0 255.255.255.0

# Rol de cliente (iniciará la conexión)
tls-client

#Certificado de la CA
ca /etc/openvpn/ca.crt

#Certificado local
 cert /etc/openvpn/client1.crt

#Clave privada local
key /etc/openvpn/client1.key

#Activar la compresión LZO
comp-lzo

#Detectar caídas de la conexión
keepalive 10 60

#Archivo de log
log /var/log/office2.log

#Nivel de información
verb 3
```

En este caso hay que activar el servicio de enrutamiento en ambos servidores y copiar el fichero de Diffie-Hellman, la clave privada y el certificado digital de cada servidor, así como el certificado de la CA, al directorio /etc/openvpn de cada equipo.