OpenVPN: Redes Privadas Virtuales sencillas

Jesús Espino García
jespinog@gmail.com

Jornadas de Otoño 2009

16 de marzo de 2012

Índice

¿Qué es una VPN?

- Red Privada Virtual.
- Redes privadas sobre redes publicas.
- Trasferencia de datos cifrada.

¿Que es OpenVPN?

- Software para construir VPNs.
- GPL.
- Multi Plataforma.
- Cifrado sobre OpenSSL.

¿Por qué OpenVPN?

- Libre.
- Portable.
- SSL.
- Fácil de configurar.
- Escalable.
- Es un programa en espacio de usuario.
- Puede conectar a través de proxy HTTP.

Índice

Routing

- Eficiente y escalable.
- Usa modo "Tun"del driver tun/tap.
- Modifica reglas de firewall y rutado.
- Funciona con IPv4 y en algunos casos con IPv6.
- No propaga el trafico broadcast.

Bridge

- Bridge Ethernet.
- Usa modo "Tap"del driver tun/tap.
- Usa las bridge tools.
- Une dos redes.
- Soporta otros protocolos a parte de IPv4 (IPX, AppleTalk...).
- Menos eficiente y escalable que el routing.

Índice

Clave compartida

- Usar una clave que comparten cliente y servidor.
- Poco seguro.
- Poco escalable.

Certificados X509

- Usar Certificados para autenticar ambos extremos.
- Utiliza una Autoridad certificador para dar validez a los certificados.
- Las altas se hacen mediante generación y firma de certificados por parte de la CA.
- Las bajas se hacen como revocaciones de un certificado.
- Muy seguro.
- Muy escalable.

Índice

Clave compartida con Routing

Configuración con clave estática y compartida.

- Creamos una clave:
  `openvpn --genkey --secret static.key`
- Copiamos esta clave en los dos equipos a conectar.
- Configuramos el servidor para que acepte esta clave.
- Configuramos el cliente para que conecte al servidor y use esta clave.

Clave compartida con Routing

- Cliente:

```
dev tun0
ifconfig 10.8.0.1 10.8.0.2
secret static.key
```

- Servidor:

```
remote myserver.com
dev tun0
ifconfig 10.8.0.2 10.8.0.1
secret static.key
```

Índice

X509 con Bridging

Configuración con certificados X509.

- Creamos una autoridad certificadora.
- Creamos un certificado y su clave para el servidor.
- Creamos un certificado y su clave para el cliente.
- Firmamos los certificados del servidor y cliente con la autoridad certificadora.
- Configuramos el servidor para usar esa CA, su certificado y su clave.
- Configuramos el cliente para usar esa CA, su certificado y su clave.

X509 con Bridging

- Cliente:

```
client
dev tap1
proto tcp
port 1196
ca keys/ca.crt
cert keys/client.crt
key keys/client.key
dh keys/dh1024.pem
remote 127.0.0.1 1195
```

X509 con Bridging

- Servidor:

```
dev tap0
proto tcp
lport 1195
ca keys/ca.crt
cert keys/server.crt
key keys/server.key
dh keys/dh1024.pem
server-bridge 192.168.0.2 255.255.255.0 192.168.0.128 1
```

Índice

Referencias

- www.openvpn.net: Pagina oficial de OpenVPN.
- gul@gul.uc3m.es: Lista de correo del GUL.

Índice

Dudas

...