OpenVPN

IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León
Alberto Molina Coballes

Redes de Área Local

Junio 2009

Introducción

El proyecto OpenVPN desarrolla una implementación de VPNs basadas SSL/TLS

Las razones de su desarrollo son las limitaciones y problemas de IPSec y el rápido desarrollo de SSL

Se trata de un producto de software libre liberado bajo los términos de la GPL que fue creado por James Johan en el año 2001

Características principales

- El componente principal es el driver *tun/tap* utilizado para simular interfaces de red, que se encarga de levantar el túnel y encapsular los paquetes a través del enlace virtual
- Encriptación y autenticación con OpenSSL
- Utiliza un único puerto TCP o UDP → fácil para firewalls
- Multiplataforma → misma herramienta funcionando sobre distintos SO vs implementaciones diferentes de un mismo estándar en distintas arquitecturas
- Compresión de datos LZO

Algunos problemas

- No es compatible con IPSec, el estándar para soluciones VPN
- Comunidad no muy amplia
- Faltan dispositivos con clientes OpenVPN integrados

COMPARATIVA: OpenVPN - IPSec

Modos de funcionamiento

- Modo túnel

  Emplea el driver *tun* y es utilizado para crear túneles virtuales operando con el protocolo IP

- Modo puente

  Utiliza el driver *tap* y es empleado para túneles que encapsulan directamente paquetes Ethernet. Se recomienda en las siguientes situaciones:

  - La VPN necesita encapsular protocolos no-IP
  - Se ejecutan aplicaciones que necesitan network broadcasts
  - No se cuenta con un servidor Samba y se necesita que los usuarios puedan navegar por los ficheros compartidos

Autenticación

La autenticación de los extremos remotos de una conexión SSL/TLS está basada en el modelo de claves asimétricas RSA

Los participantes intercambian sus claves públicas a través de certificados digitales X.509, que han sido firmados previamente por una Autoridad de Certificación en la que se confía

Instalación

Muy sencilla; puede hacerse desde los repositorios o descargando el tarball

- Descomprimimos el fichero:

```
tar xvzf openvpn-[version].tar.gz
```

- Nos movemos al directorio openvpn y compilamos e instalamos:

```
./configure
make
make install
```

Creación CA y certificados

Para implementar una infraestructura OpenVPN es necesario configurar una PKI (public key infrastructure):

- Un certicado para la autoridad de certificación (CA) y una clave privada con los que firmar cada certificado de servidores y clientes
- Un certificado (clave pública) y una clave privada para cada servidor y cliente

HOWTO

Creación de los ficheros de configuración

La aplicación OpenVPN (de GNU/Linux) utiliza un único fichero de configuración donde se especifican los parámetros de túnel VPN SSL que se quiere establecer, y puede tener cualquier nombre

Ejemplos de ficheros

Parámetros comunes:

- **auth *alg***
- **cipher *alg***
- **comp-lzo**
- **dev *device***
- **route *ip mask***
- **key *key_file***
- **log *log_file***
- **remote *IP***
- **ca *cert_file***
- **tls-client**
- **proto *protocol***
- **port *port***
- **server *ip mask***
- **verb *level***
- **tls-server**

Establecer la VPN

- Para arrancar el servidor:

  `openvpn [server config file]`

  ¡OJO! Hay que tener en cuenta varias cuestiones importantes:

  - Hay que abrir el puerto 1194 UDP (o el que se haya configurado) en el firewall y redirigir la petición a la máquina donde corra OpenVPN
  - En la máquina OpenVPN hay que permitir las peticiones entrantes a la interfaz *tun/tap*

- Para arrancar los clientes:

  `openvpn [client config file]`

Establecer la VPN

Si se instaló OpenVPN desde repositorio el instalador crea un script de inicio. Cuando se ejecuta, el script buscará ficheros **`.conf`** en el directorio **`/etc/openvpn`** e iniciará un demonio diferente de OpenVPN para cada fichero encontrado