Corso "Sysadmin Linux" 2019

Lezione #4 - OpenVPN

Matteo F. Vescovi

Free Software Users Group Padova
https://www.fsugpadova.org

27 Novembre 2019
AViLUG - Schio (VI)

Outline

Ora parliamo di...

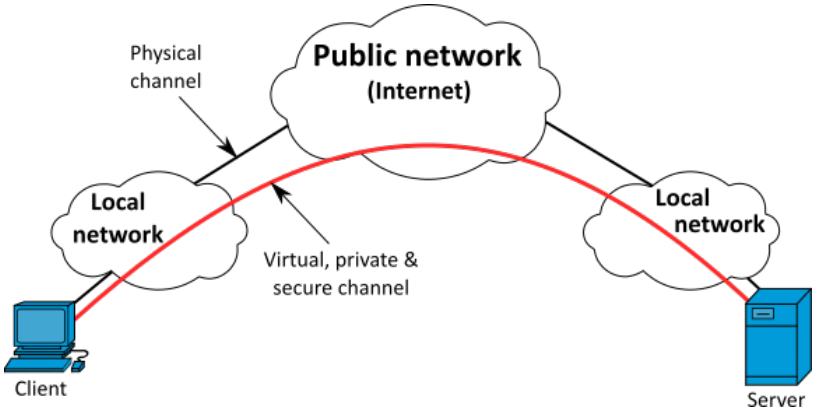
1. Concetti base di una VPN (Virtual Private Network)
2. Come impostare un server OpenVPN in Ubuntu

Come è strutturata una VPN? (a parole)

"È una rete di telecomunicazioni privata instaurata come connessione tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la suite di protocolli internet"

[Fonte: Wikipedia]

Come è strutturata una VPN? (con un'illustrazione)



[Fonte: Wikipedia, ©Michel Bakni]

Ora parliamo di...

1. Concetti base di una VPN (Virtual Private Network)

2. Come impostare un server OpenVPN in Ubuntu

Installazione

In Ubuntu è già pacchettizzato e può essere installato con il semplice comando:

```
$ sudo apt install openvpn
```

Questo va fatto sia lato server che lato client.

Nel caso si utilizzi GNOME come Desktop Environment, si può installare il modulo di Network Manager per la gestione delle connessioni OpenVPN:

```
$ sudo apt install network-manager-openvpn-gnome
```

Configurazione

Un server OpenVPN può autenticare i clients che ad esso si connettono attraverso vari meccanismi:

- user / password
- pre-shared key
- certificati
- etc...

Noi descriveremo il meccanismo basato su certificati.

Certificati TLS (passo 1)

- Sul server OpenVPN installiamo (se non già presente) il pacchetto *easy-rsa* e creiamo la struttura directory per i certificati:

```
$ sudo apt install easy-rsa
$ sudo make-cadir /etc/openvpn/easy-rsa/
```

Certificati TLS (passo 2)

- Modifichiamo il file */etc/openvpn/easy-rsa/vars* aggiungendo in calce le variabili relative alla nostra attività:

```
export KEY_COUNTRY="IT"
export KEY_PROVINCE="VI"
export KEY_CITY="Schio"
export KEY_ORG="AViLUG"
export KEY_EMAIL="info@avilug.it"
```

- Rendiamo queste modifiche operative aggiornando le variabili di ambiente (passando a *root* per eseguire tutte le modifiche):

```
$ sudo su
# cd easy-rsa/
# ln -s openssl-1.0.0.cnf openssl.cnf
# . ./vars
# ./clean-all
```

Certificati TLS (passo 3)

- A questo punto possiamo generare la coppia di certificato+chiave *Certificate Authority*:

```
# ./build-ca
```

che genererà i files *ca.crt* e *ca.key* nella directory */etc/openvpn/easy − rsa/keys/* e firmato con il proprio certificato root.

- Generiamo anche la pre-shared key (PSK) per aumentare il livello di protezione:

```
# openvpn --genkey --secret ../tls-auth.key
```

Certificati TLS (passo 4)

- Generiamo i parametri Diffie-Hellman, necessari lato server per le connessioni SSL/TLS:

```
# ./build-dh
```

- A questo punto possiamo generare i certificati per ogni client che intendiamo connettere al server OpenVPN:

```
# ./build-key <clientname>
```

A questo punto, copieremo ca.crt, <clientname>.crt e <clientname>.key dal server al client nella directory *etc/openvpn/easy-rsa/keys/* o altra posizione utile per il loro utilizzo.

Certificati TLS (passo 5)

Creiamo, ora, la configurazione per il server. Ad esempio:

```
server 10.25.1.0 255.255.255.0
port 1194
proto udp4
dev tun
topology subnet
push "route 192.168.77.0 255.255.255.0"
ifconfig-pool-persist ipp.txt
cipher AES-256-GCM
compress lzo
keepalive 10 120
key-direction 0
persist-key
persist-tun
status log/openvpn-status.log
client-to-client
user nobody
group nogroup
verb 3
explicit-exit-notify 1
tls-auth tls-auth.key 0
ca       easy-rsa/keys/ca.crt
dh       easy-rsa/keys/dh2048.pem
cert     easy-rsa/keys/<server>.crt
key      easy-rsa/keys/<server>.key
```

... e riavviamo il servizio: `$ sudo systemctl restart openvpn@server.service`

Certificati TLS (passo 6)

Creiamo, infine, la configurazione per il client. Ad esempio:

```
client
dev tun
remote avilug.it
port 1194
proto udp
topology subnet
nobind
user nm-openvpn
group nm-openvpn
remote-cert-tls server
auth-nocache
tls-auth /home/utente/.openvpn/tls-auth.key 1
ca       /home/utente/.openvpn/ca.crt
cert     /home/utente/.openvpn/<clientname>.crt
key      /home/utente/.openvpn/<clientname>.key
key-direction 1
cipher AES-256-GCM
compress lz4-v2
persist-key
persist-tun
verb 3
```

Ho concluso...

GRAZIE!