

OpenVPN e tunnelling IPv6

Introduzione a OpenVPN ed al routing di
una subnet IPv6 attraverso una
connessione sicura

Linux Day 05 – 20051126

Cherubini Enrico - kevin@bestkevin.com
InfoSysNet Snc

OpenVPN: cos'è una VPN

- VPN: Virtual Private Network
 - Virtuale perché è una rete inesistente, basata su reti pubbliche
 - Privata perché criptata
 - Sicura perché utilizza cifrature forti
-
-

OpenVPN: perché non altri ?

- Software libero, quindi il codice è verificabile
 - Varie tipologie di autenticazione: shared key e certificati
 - Multipiattaforma: client e server sia per linux che per altri sistemi operativi proprietari
 - Maturo e solido
-
-

IPv6: cos'è ?

- Il futuro di IPv4, ma già presente
- Spazi di indirizzamento a 128 bit virtualmente infinito (16^{32} indirizzi IP)
- Include al suo interno IPv4
- IP in formato esadecimale:

2001:0DB8:0000:0000:0000:0000:1428:57ab/64

o più brevemente:

2001:0DB8::1428:57ab/64

IPv6: perché ?

- Perché è nuovo
- Perché è bello provare
- Perché no ?



OpenVPN: Il server

- Per avere Ipv6 deve essere di tipo 'tap'
 - Per essere multicient si deve configurare con uso dei certificati, quindi niente shared key
 - Per gestire i certificati dobbiamo iniziare con la CA
 - Ricordarsi di aprire il firewall per la porta UDP 1194
-
-

OpenVPN: la CA

Per gestire i certificati dei client, uno per ogni client, dobbiamo iniziare installando una Certification Authority. Fortunatamente OpenVPN ci da già gli strumenti

OpenVPN: la CA

```
cd /etc/openvpn/easy-rsa
```

- modificare vars
- impostare KEY_CONFIG
- impostare KEY_DIR
- eseguire ./vars per impostare i valori delle variabili
- eseguire ./clean-all

Ricordare che i file .key sono segreti, mentre i file .crt e .csr non sono critici.

OpenVPN: la CA

Costruiamo la CA:

- `./build.ca`

nella directory `KEY_DIR` avremo ora
l'accoppiata `ca.crt` e `ca.key`

- `./build-dh`



OpenVPN: la CA

Generiamo ora i certificati per il client.

```
./build-req client
```

I campi possono essere impostati come si vuole, con l'accortezza che il common name dev'essere univoco tra tutti, di solito il nome del client.

Il certificato dev'essere ora firmato dall'autorità:

```
./sign-req client
```

In KEY_DIR si troveranno le chiavi appena create, client.crt e client.key

Per semplificare il tutto: ./build-key client

OpenVPN: la CA

Copiare i file necessari dal server al client:
ca.crt e client.crt non sono sensibili
client.key deve essere copiato usando un
canale sicuro

OpenVPN: server.conf

```
port 1194
proto udp
dev tap

ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server.crt
key /etc/openvpn/easy-rsa/keys/server.key # This
file should be kept secret
dh /etc/openvpn/easy-rsa/keys/dh1024.pem
server 10.0.0.0 255.255.255.0
client-config-dir ccd
route 10.0.0.0 255.255.255.252
```

OpenVPN: server.conf

```
client-to-client
keepalive 10 120
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
log      openvpn.log
log-append openvpn.log
verb 3
route-gateway 10.0.0.1
```

OpenVPN: ccd/client

Questo file contiene i comandi da dare quando si collega il client...normalmente per l'attribuzione di un IP statico.

```
ifconfig-push 10.0.0.11 255.255.255.0
```

OpenVPN: avvio del server

```
/etc/init.d/openvpn start
```

Controllare `openvpn.log` per eventuali errori. Se tutto risulta corretto, dovrete avere un'interfaccia `tap1` con l'ip del server:

```
tap1    Link encap:Ethernet HWaddr 1A:8D:57:BF:3C:71  
        inet addr:10.0.0.1 Bcast:10.0.0.255 Mask:255.255.255.0  
        inet6 addr: fe80::188d:57ff:febf:3c71/64 Scope:Link
```

OpenVPN: client.conf

```
client
dev tap
proto udp
remote jenny.bestkevin.com 1194
  resolv-retry infinite
  nobind
  user nobody
  group nogroup
  persist-key
  persist-tun
  ca /etc/openvpn/ca.crt
  cert /etc/openvpn/client1.crt
  key /etc/openvpn/client1.key
  comp-lzo
  verb 3
```

OpenVPN: avvio del client

```
/etc/init.d/openvpn start
```

come prima controlliamo i log, anche lato server, e controlliamo se abbiamo il device:

```
tap0    Link encap:Ethernet HWaddr AE:4B:18:E9:20:A6  
        inet addr:10.0.0.11 Bcast:10.0.0.255 Mask:255.255.255.0  
        inet6 addr: fe80::ac4b:18ff:fee9:20a6/64 Scope:Link
```

```
        PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.  
        64 bytes from 10.0.0.1: icmp_seq=93 ttl=64 time=80.3 ms
```

OpenVPN: aggiungere IPv6

Il server ha una classe /64:

```
sixxs Link encap:IPv6-in-IPv4
```

```
inet6 addr: 2001:1418:100:e::2/64 Scope:Global
```

```
inet6 addr: fe80::3e5e:908c/64 Scope:Link
```

```
inet6 addr: fe80::c0a8:45/64 Scope:Link
```

più una subnet /48 che viene ruotata ad esso,
2001:1418:13c::1/48 che possiamo spezzare in 65536
/64 del tipo 2001:1418:13c:XXXX:Y/64 Dobbiamo
attribuire un IPv6 della classe /64 all'interfaccia tap
del server ed uno alla tap del client.

OpenVPN: IPv6 lato server

Eseguire il seguente script:

```
#!/bin/bash
```

```
tap=`ifconfig | grep tap | awk {'print $1'}`
```

```
echo $tap
```

```
ip -6 addr add fe80::201:2ff:fede:c1ac/64 dev $tap scope link
```

```
ip -6 addr add 2001:1418:13c:0001::1/64 dev $tap
```

```
ip -6 route add 2001:1418:13c:0001::2/64 dev $tap
```

OpenVPN: IPv6 lato client

Eseguire il seguente script:

```
#!/bin/bash
# IPv6
ip -6 route del fe80::/64 dev eth0
ip -6 route del ff00::/8 dev eth0
ip -6 addr add 2001:1418:13c:0001::2/64 dev tap0
ip -6 addr add fe80::20e:a6ff:fe1f:26e2 dev tap0 scope link
ip -6 route add 2001:1418:13c:0001::1/64 dev tap0
ip -6 route add default via 2001:1418:13c:0001::1 dev tap0
```

OpenVPN: IPv6 - verifica

Dal server:

```
ping6 2001:1418:13c:1::2
```

```
PING 2001:1418:13c:1::2(2001:1418:13c:1::2) 56 data bytes  
64 bytes from 2001:1418:13c:1::2: icmp_seq=1 ttl=64 time=181  
ms
```

Dal client:

```
ping6 2001:1418:13c:1::1
```

```
PING 2001:1418:13c:1::1(2001:1418:13c:1::1) 56 data bytes  
64 bytes from 2001:1418:13c:1::1: icmp_seq=1 ttl=64 time=77.6  
ms
```

Si può testare con un browser andando su www.ipv6.org

You are using IPv6 from 2001:1418:13c:1::2

OpenVPN: The end

Qualcuno afferma che ci sono VPN più sicure: OpenVPN è libero, di facile installazione e manutenzione ed estremamente resistente agli attacchi.

Qualcuno afferma che IPv6 non prenderà mai piede: meglio intanto iniziare a familiarizzare e a giocarci, nonchè è sempre utile avere migliaia di indirizzi a disposizione. E poichè con IPv6 non esiste il concetto di NAT, sono indirizzi pubblici.

Saluti e domande

Author: kevin@bestkevin.com

Homepage: www.bestkevin.com (anche su
Ipv6)

Queste slides sono rilasciate sotto licenza
Creative Commons – Attribution –
Sharealike 2.5
