

OpenVPN routing mini howto

- [Introduzione](#)
- [Bridging - Routing](#)
- [Installazione del server](#)
- [Installazione del client](#)
- [Configurazione del server](#)
- [Configurazione del client \(linux\)](#)
- [Configurazione e installazione del client \(windows\)](#)
- [Test della VPN](#)
- [Note per Slackware](#)
- [Note per l'utilizzo di server con firewall](#)
- [Link Utili](#)
- [Ringraziamenti](#)

Introduzione

Una VPN (Virtual Private Network) si usa quando si ha la necessita di creare un collegamento tra 2 o piu reti private attraverso una rete pubblica (come internet). Una volta stabilita la connessione tra le 2 reti private, gli utenti vedranno la rete opposta in modo del tutto trasparente come se fossero collegate fisicamente tra di loro. Bisogna tenere pero conto che la velocita di connessione massima tra le 2 reti è definita dalla rete pubblica: se usassimo una connessione adsl normale con banda in upload di 256kbs ad esempio, la velocita massima di trasferimento dei file sarà circa 32kbyte al secondo, e non i classici 10/100mbit della LAN. Altra cosa molto importante dell'uso di OpenVPN è quello di creare un sistema di comunicazione protetto: potete stare quindi tranquilli anche nel caso dobbiate trasferire dati confidenziali e riservati.

Questa guida vuole solo essere una sorta di QuickStart per configurare velocemente una VPN in modalita routing.

La guida si basa sulla configurazione di OpenVPN 2.X su una macchina slackware (kernel 2.6) con installazione da sorgenti, e non sostituisce assolutamente la documentazione ufficiale che è molto esauriente e ben scritta ([la trovate qui](#)).

Quali sono le differenze tra modalita bridging e routing?

Bridging e routing sono 2 sistemi per collegare sistemi con VPN.

Vantaggi Bridging

- I Broadcasts viaggiano sulla VPN -- Questo permette ai software che fanno uso di broadcast di funzionare, come ad esempio la condivisione dei file di windows o i giochi in lan, di funzionare.
- Non sono necessarie configurazioni di routing.
- Funziona con tutti i protocolli che viaggiano su ethernet incluso IPv4, IPv6, Netware IPX, AppleTalk, etc.
- Relativamente facile da configurare per soluzioni roadwarriors (moleplici sedi distaccate, utenti che si collegano da posti diversi)

Svantaggi Bridging

- Meno efficiente rispetto la modalita routing, e poca scalabilita.

Vantaggi Routing

- Efficienza e scalabilita
- Permette un miglior runing dell MTU per una maggiore efficienza.

Svantaggi Routing

- I client devono usare un WINS server (come samba) per poter usare la condivisione di file su VPN.
- Ogni instradamento deve essere configurato in modo da collegarsi alla subnet.
- I software che dipendono dai broadcast non vedono le altre macchine in lan sulla VPN.
- Funziona solo con IPv4, e IPv6 nel caso che i dispositivi che entrambi le parti lo supportino.

Primo passo. Installazione di openvpn.

Requisiti per OpenVPN: libreria LZO, pacchetto iproute2 moduli tap/tun compilati nel kernel.

Installazione di LZO

```
# wget http://www.oberhumer.com/opensource/lzo/download/lzo-1.08.tar.gz
# tar xvzf lzo-1.08.tar.gz
# cd lzo-1.08
# ./configure --prefix=/usr --sysconfdir=/etc
# make && make install
```

Installazione del pacchetto iproute2:

```
# wget ftp://ftp.slackware.at/slackware-current/slackware/n/iproute2-2.6.9_ss040831-i486-1.tgz
# installpkg iproute2-2.6.9_ss040831-i486-1.tgz
```

Andiamo a scaricare i sorgenti di OpenVPN ed effettuiamo l'installazione. Verificate che sul vostro sistema abbiate il modulo tun compilato nel kernel (se il comando **# modprobe tun** non da errori è correttamente installato)

```
# wget http://openvpn.net/release/openvpn-2.0_rc21.tar.gz
# tar xvzf openvpn-2.0_rc21.tar.gz
# cd openvpn-2.0_rc21
# mkdir /etc/openvpn
# mkdir /etc/openvpn/keys
# ./configure --prefix=/usr --sysconfdir=/etc/openvpn --enable-iproute2
# make && make install
```

A questo punto ci servono gli script di esempio che andremo a modificare e gli script per la creazione dei certificati. Copiamo il contenuto delle dir easy-rsa e sample-config-files in /etc/openvpn/

```
# cd easy-rsa/
# cp -R */etc/openvpn/
# cd ..
# cd sample-config-files/
# cp -R */etc/openvpn/
```

Ora siamo pronti per creare i certificati e modificare i file di configurazione.

```
# cd /etc/openvpn/
```

editiamo il file vars in modo che la riga che esporta la variabile D sia cosi scritta cosi: **export D=/etc/openvpn**

Configurazione del server

Creiamo i certificati e modifichiamo i file di configurazione:

```
# cd /etc/openvpn/
# . ./vars
# ./clean-all
# ./build-ca
```

A questo punto vi verrà chiesto di inserire le informazioni della VPN per la creazione dei certificati.

L'unico parametro che va per forza esplicitato è Common Name (eg. your name or your server's hostname) []: in cui dovete inserire l'identificativo della vostra VPN (ad esempio VPN-test).

E' il momento adesso di creare i certificati e le chiavi:

```
# ./build-key-server server
```

Vi verranno chieste nuovamente i parametri. In questo caso al punto Common Name: dovete scrivere server e confermare con y le richieste successive.

La configurazione dei certificati per il server è adesso completa. Bisogna pero creare i certificati per i client che si dovranno collegare al server:

```
# ./build-key client1
```

e cosi via per tutti i client che dovete collegare al server.

Fate attenzione quando inserite il Common Name per i vari client, che ogni client abbia un nome univoco! Se volete proteggere le chiavi con una password potete usare lo script **build-key-pass**.

Generiamo ora i parametri Diffie Hellman

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

La configurazione dei certificati per server e client è terminata.

Per sapere quali file servono sul server e quali sul client è molto utile fare riferimento alla seguente tabella:

Filename	Necessario per	Utilizzo	Secret
ca.crt	server + tutti i clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh {n}.pem	solo server	Diffie Hellman paramters	NO
server.crt	solo server	Server Certificate	NO
server.key	solo server	Server Key	YES
client1.crt	solo client1	Client1 Certificate	NO
client1.key	solo client1	Client1 Key	YES

Nel nostro caso i file che saranno necessari sul client1 sono: ca.crt client1.crt client1.key
Per mettere questi file sul client, usate un canale sicuro!

La configurazione del server si trova nel file server.conf

Se non modificate nulla, verrà creata una VPN usando come device virtuale TUN (usato nel caso di routing) che stara in ascolto per i client sualla porta 1194 UDP e verranno assegnati ai client degli ip con subnet **10.8.0.0/24**.

Per una soluzione di easy setup, queste impostazioni sono sufficienti. Per una configurazione ad hoc invece, vi rimando alla documentazione ufficiale.

Per quello che ho potuto constatare, la configurazione cosi comè, funziona solo se si lancia openvpn dalla directory in cui sono presenti i certificati cioe da /etc/openvpn/keys .Questo accade perche nel file di configurazione, i certificati hanno il percorso (relativo e non assoluto. Per fare in modo che openvpn sia avviabile anche da altre directory, è necessario inserire i percorsi assoluti nel file server.conf) modificando in questo modo le righe relative:

```
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
dh /etc/openvpn/keys/dh1024.pem
```

Nota: per caricare il dispositivo virtuale di routing per la VPN con kernel 2.6 è necessario caricare il modulo tun:

```
# modprobe tun
```

a questo punto possiamo effettivamente lanciare il server:

```
# openvpn /etc/openvpn/server.conf
```

Se tutto andrà correttamente vedrete una cosa del tipo:

```
Wed Apr 13 15:49:02 2005 OpenVPN 2.0_rc21 i686-pc-linux [SSL] [LZO] built on Apr 13 2005
Wed Apr 13 15:49:02 2005 Diffie-Hellman initialized with 1024 bit key
Wed Apr 13 15:49:02 2005 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed Apr 13 15:49:02 2005 TUN/TAP device tun0 opened
Wed Apr 13 15:49:02 2005 /sbin/ip link set dev tun0 up mtu 1500
Wed Apr 13 15:49:02 2005 /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
Wed Apr 13 15:49:02 2005 /sbin/ip route add 10.8.0.0/24 via 10.8.0.2
Wed Apr 13 15:49:02 2005 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:23 ET:0 EL:0 AF:3/1 ]
Wed Apr 13 15:49:02 2005 CID set to nobody
Wed Apr 13 15:49:02 2005 UDP set to nobody
Wed Apr 13 15:49:02 2005 UDPv4 link local (bound): [undef]:1194
Wed Apr 13 15:49:02 2005 UDPv4 link remote: [undef]
Wed Apr 13 15:49:02 2005 MULTI: multi init called, r=256 v=256
Wed Apr 13 15:49:02 2005 IFCONFIG POOL: base=10.8.0.4 size=62
Wed Apr 13 15:49:02 2005 IFCONFIG POOL LIST
Wed Apr 13 15:49:02 2005 Initialization Sequence Completed
```

Significa che il dispositivo è stato inizializzato correttamente.

Installazione del client.

La procedura di installazione del client è esattamente la stessa di quella del server,ma in questo caso non vanno create le chiavi.

Configurazione del client (Linux)

La riga da editare per stabilire la connessione con il server è quella del tipo:

```
remote my-server-1 1194
```

in cui dovreste sostituire l' ip o l'host name del server su cui gira openvpn.

Se ad esempio create una vpn all'interno di una lan, la riga sarà una cosa del tipo:

```
remote 192.168.0.1 1194
```

(192.168.0.1 è l'ip del mio server ma potrebbe anche essere un host name di un server accessibile da internet)

Copiamo i file necessari dal server al client: ca.crt client1.crt client1.key in /etc/openvpn/keys (del pc client)

Anche in questo caso andiamo a inserire i percorsi assoluti dei certificati per fare in modo che openvpn possa essere lanciato da qualsiasi dir.

Editiamo il file client.conf :

```
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/client.crt
key /etc/openvpn/keys/client.key
```

Faccio notare che quando mettiamo i certificati creati sul server, sul pc client, il loro nome sarà del tipo client1.key e client1.crt. Percio sarà necessario rinominare tali file per farli combaciare con la sintassi del file client.conf (o rinominiamo i file oppure modifichiamo il loro nome all'interno del file client.conf)

A questo punto (dopo aver caricato il modulo tun anche sul client) possiamo instaurare la connessione, impartendo sul client il comando:

```
# openvpn /etc/openvpn/client.conf
```

Se tutto è corretto vedrete una cosa del tipo:

```
Wed Apr 13 16:03:05 2005 OpenVPN 2.0_rc21 i686-pc-linux [SSL] [LZO] built on Apr 12 2005
Wed Apr 13 16:03:05 2005 IMPORTANT: OpenVPN's default port number is now 1194, based on an official port number assignment by IANA. OpenVPN 2.0-beta16 and earlier used 5000 as the default port.
Wed Apr 13 16:03:05 2005 LZO compression initialized
Wed Apr 13 16:03:05 2005 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed Apr 13 16:03:05 2005 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:23 ET:0 EL:0 AF:3/1 ]
Wed Apr 13 16:03:05 2005 Local Options hash (VER=V4): '41690919'
Wed Apr 13 16:03:05 2005 Expected Remote Options hash (VER=V4): '530fdded'
---
---
Wed Apr 13 16:03:06 2005 OPTIONS IMPORT: timers and/or timeouts modified
Wed Apr 13 16:03:06 2005 OPTIONS IMPORT: --ifconfig/up options modified
Wed Apr 13 16:03:06 2005 OPTIONS IMPORT: route options modified
Wed Apr 13 16:03:06 2005 TUN/TAP device tun0 opened
Wed Apr 13 16:03:06 2005 /sbin/ip link set dev tun0 up mtu 1500
Wed Apr 13 16:03:06 2005 /sbin/ip addr add dev tun0 local 10.8.0.10 peer 10.8.0.9
Wed Apr 13 16:03:06 2005 /sbin/ip route add 10.8.0.1/32 via 10.8.0.9
Wed Apr 13 16:03:06 2005 CID set to nobody
Wed Apr 13 16:03:06 2005 UID set to nobody
Wed Apr 13 16:03:06 2005 Initialization Sequence Completed
```

Cio significa che al client è stato assegnato l'ip 10.8.0.10.

Configurazione e installazione del client (Windows XP)

Scarichiamo il pacchetto binario per windows e lo installiamo seguendo il wizard. Verrà chiesto di installare un driver non certificato, clicchiamo per continuare l'installazione.

Una volta installato, troveremo i file di configurazione sotto C:\Programmi\OpenVPN\sample-config Andiamo a editare il file C:\Programmi\OpenVPN\vars.bat come segue:

```
set KEY_DIR=C:\Programmi\OpenVPN\easy-rsa\keys
```

Creiamo una directory in C:\Programmi\OpenVPN\easy-rsa\ di nome keys.

Copiamo i certificati creati ca.crt client2.crt client2.key nella directory keys andando a rinominare i file in modo che combacino con le direttive del file client.ovpn

cioe avremo una cosa del tipo:

```
ca C:\Programmi\OpenVPN\keys\ca.crt
cert C:\Programmi\OpenVPN\keys\client.crt
key C:\Programmi\OpenVPN\keys\client.key
```

da notare le \ per indicare che il percorso è assoluto.

Editiamo il file client.ovpn andando ad inserire la riga che contiene l'ip del server:

```
remote 192.168.0.1 1194
```

salviamo e chiudiamo l' editor.

A questo punto è sufficiente cliccare con il destro sul file appena editato e cliccare su:

```
Start openvpn on this config file
```

In questo modo sarà instaurata la connessione con il server.

Si aprirà anche una console contenente i log della connessione, in modo da capire se è tutto funzionante.

Verificare il funzionamento:

testiamo la connessione dal client con un semplice ping al server che ha ip 10.8.0.1

```
$ ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data:
 64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=3.08 ms
 64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=3.01 ms
```

che come vedete risponde correttamente.

Proviamo anche ora dal lato server al client:

```
$ ping 10.8.0.10
PING 10.8.0.10 (10.8.0.10) 56(84) bytes of data.
 64 bytes from 10.8.0.10: icmp_seq=1 ttl=64 time=4.83 ms
 64 bytes from 10.8.0.10: icmp_seq=2 ttl=64 time=4.41 ms
```

Anche in questo caso è tutto corretto.

Note per l'automatizzazione su slackware

Se vogliamo che sia il server che il client vpn siano inizializzati al boot, è sufficiente aggiungere a /etc/rc.d/rc.local una riga del tipo:

```
openvpn /etc/openvpn/client.conf
```

(per il client)

oppure

```
openvpn /etc/openvpn/server.conf
```

(per il server)

e aggiungere la riga

```
/sbin/modprobe tun
```

in /etc/rc.d/rc.modules.

In entrambi i casi sia server che client saranno lanciati con user e group di default cioe nobody.

Note per l'utilizzo di server con firewall

Se state cercando di collegare un client ad un server attraverso internet, dovete ricordarvi di aprire la porta 1194 UDP del firewall, e se state usando anche un router, dovete ricordarvi di ridirigere la porta 1194 verso l'ip del server su cui gira il servizio openvpn.

Link Utili

<http://openskills.info/in/foebox.php?ID=595>
<http://www.sistemistiindipendenti.org/modules/news/article.php?storyid=66>

Ringraziamenti

Grazie a matrig che mi ha aiutato nella realizzazione della sezione dedicata a OpenVPN per windows.
Grazie a darkpand per i chiarimenti sul networking.

Autore: scomodo
www.scomodo.com