

GUIDA ALLA CREAZIONE DI UN TUNNEL SSH INVERSO ("Reverse" ssh tunnel)

La procedura che a breve verrà illustrata consente di accedere ad un host che sta dietro un firewall di cui non avete il controllo e che non consenta accessi dall'esterno, in particolare verrà illustrato come rendere il vostro demone ssh locale accessibile attraverso suddetto firewall.

Per prima cosa occorre che sugli host interessati ci siano server e client di ssh installati e funzionanti, se non lo fossero provvedete in tal senso.

Facciamo un esempio pratico: supponete che dal vostro pc a casa vogliate eseguire dei comandi via ssh sul vostro pc aziendale che sta dentro la rete aziendale protetta da un firewall (ad es. NAT) che blocca le connessioni ssh in ingresso.

NOTA: quello che segue è solo un esempio, se volete realmente applicarlo assicuratevi che tale operazione non sia contraria alla politica adottata dalla vostra azienda, l'autore declina ogni responsabilità derivante da un uso improprio o non consentito, da leggi o regolamenti, della tecnica illustrata in questa guida.

NOTA: tale tecnica è stata utilizzata con successo per accedere ad un pc con accesso ad internet fornito dall'ISP Fastweb

Dal vostro pc aziendale date il seguente comando:

sintassi :

```
ssh -R porta_non_in_uso_sul_vostro_pc_di_casa:localhost:22 -p 22 -l nome_di_utente_abilitato_a_ricevere_connessioni_via_ssh_sul_vostro_pc_di_casa indirizzo_del_vostro_pc_a_casa -f -N
```

esempio:

```
ssh -R 9000:127.0.0.1:22 -p 22 -l sempronio ip_del_pc_di_casa -f -N
```

vediamo cosa significa il comando di cui sopra:

- ssh -R specifica che la porta indicata (ad esempio la 9000) sull'host remoto (il pc che avete a casa) deve essere forwardata sulla porta (il server ssh di default sta in ascolto sulla porta 22) indicata sull'host locale (pc aziendale)
- -p 22 serve a specificare su che porta sta in ascolto il server ssh sull'host remoto (il pc a casa) se sta in ascolto sulla porta di default questo parametro può essere omesso
- -l sempronio serve a specificare il nome dell'utente sull'host remoto (il pc a casa)
- -f manda ssh in background dopo l'autenticazione, alcuni preferiscono non usare questo parametro

- -N riporto testualmente quanto detto in `man ssh`: Do not execute a remote command. This is useful for just forwarding ports (protocol version 2 only).

una volta lanciato il comando sopra indicato vi verrà chiesta la password per accedere sul pc di casa con le credenziali dell'utente che avete indicato (sempronio).

Una volta che avete fatto questo per connettervi al server ssh in esecuzione sul pc aziendale non vi resta che dare il seguente comando:

sintassi:

```
ssh -p numero_della_porta_che_avete_prima_scelto_per_forwardare_sul_pc_di_casa_il_vostro_server_ssh_sul_pc_aziendale -l nome_dell'utente_sul_pc_aziendale 127.0.0.1
```

esempio:

```
ssh -p 9000 -l ciccio 127.0.0.1
```

la stessa procedura la si può utilizzare anche per accedere ad altri servizi in esecuzione sul pc aziendale

facciamo un esempio: accediamo ad un server VNC (di default in ascolto sulla porta 5900) anziché al server ssh

```
ssh -R 9000:127.0.0.1:5900 -p 22 -l sempronio ip_del_pc_di_casa -f -N
```

sul pc di casa dovrete semplicemente puntare il client VNC su 127.0.0.1:9000

This document is a free handbook; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This document is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA