SSH tunneling

Internet è una rete progettata ormai 30 anni or sono da un gruppo di studenti di Berkeley, che all'epoca si preoccupavano principalmente di una cosa: progettare entro breve una rete funzionante, stabile, veloce e basata su uno stack di rete all'epoca estremamente snello e innovativo, quale il TCP/IP, sviluppato da loro stessi. All'epoca la sicurezza della rete era un aspetto che passava in secondo piano, anche visto l'hardware dell'epoca. La priorità era progettare entro breve una rete alla portata di tutto l'hardware dell'epoca. Questo approccio ha portato i suoi frutti, portando al boom di internet in tutte le applicazioni e su tutti i dispositivi, ma ha una grossa pecca: quella della sicurezza dei dati. I progettisti dell'epoca pur di avere una rete prestante non hanno pensato ad un layer dedicato alla cifratura dei dati inviati da un capo all'altro della rete, e questa mancanza si è fatta sentire fortemente soprattutto negli ultimi 10 anni, in cui il boom di internet ha portato anche ad un aumento esponenziale delle transazioni online e in generale del traffico di dati sensibili attraverso la rete. Si doveva quindi trovare un modo per costruire una sovrastruttura sicura alla struttura già esistente del TCP/IP su cui si basava l'intera internet, senza portare rivoluzioni che avrebbero sconvolto l'intera struttura dei protocolli internet, che si erano dimostrati affidabile e robusti per oltre 20 anni. La soluzione arrivata proprio per questo sembra un po' arrangiata, ma si è dimostrata decisamente affidabile: quella di introdurre al livello applicativo dello stack TCP/IP un layer sicuro per i protocolli non affidabili. E così l'HTTP passa su SSL (Secure Socket Layer), in modo da proteggere le transazioni dei dati sensibili, diventando HTTPS. Un metodo più generale invece è quello di inoltrare le connessioni che sfruttano protocolli non cifrati su un canale sicuro. Sotto questo punto di vista, attualmente SSH è uno dei protocolli applicativi che offrono una maggiore affidabilità, e consente di fare il tunneling con pochi sforzi. Ecco come è strutturata la nostra rete:

Fondamentalmente ho un client che vuole connettersi al server destinatario usando però un canale sicuro. I motivi possono essere in genere due:

- Necessità di costruire un canale sicuro su un protocollo che non è cifrato
- Necessità di collegarsi al server dietro un firewall che blocca le connessioni su quella porta, mentre si può sfruttare il tunneling su un server SSH

Per fare una cosa del genere SSH dà tutto quello che ci serve. Basta dare sul server questo comando:

```
ssh -L porta_locale:server_dest:porta_dest user@server_ssh
```

Quello che faccio in questo modo è collegarmi al server SSH con l'utente user, che mi forwarda verso server_dest sulla sua porta porta_dest. Le connessioni in ingresso arriveranno su porta_locale. Esempio:

```
ssh -L 8080:www.google.it:80 user@mio_server_ssh
```

In questo modo creo un socket sicuro forwardato su SSH con Google che passerà attraverso il mio server SSH, al quale mi loggherò tranquillamente con l'utente in questione. I dati ricevuti dal server destinatario arriveranno sulla porta 8080 locale, quindi, se ad esempio vorrò inoltrare una richiesta a Google, basterà un

```
perl -e 'print "GET / HTTP/1.1\r\nHost: www.google.it\r\n\r\n"' | nc
localhost 8080
```