Faire passer ssh à travers un relais qui ne permet que HTTP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 mars 2009

https://www.bortzmeyer.org/ssh-a-travers-relais-http.html

Parfois, en voyage, on est coincé sur un réseau qui ne permet que HTTP. Pour se connecter à sa machine distante avec SSH, il « suffit » d'avoir un serveur SSH qui écoute sur le port 443, celui normalement dédié à HTTPS. Mais, si le réseau en question oblige à passer explicitement par un relais, comme cela vient de m'arriver ?

Avant d'aller plus loin, un rappel : les règles techniques sont probablement là pour mettre en œuvre une politique, des conditions d'utilisation, etc. Les violer peut avoir des conséquences pour vous et donc, renseignez-vous avant de tester la technique présentée ici.

Son principe est également d'avoir un serveur SSH qui écoute sur le port 443, ce qui est de toute façon très souvent utile. Ensuite, il faut dire au SSH client de passer par le relais. OpenSSH lui-même ne sait pas parler HTTP mais il sait lancer des commandes arbitraires et il existe des programmes conçus pour relayer des protocoles quelconques au dessus de HTTP. J'utilise corkscrew <http://www.agroman.net/corkscrew/> (« tire-bouchon »). Une fois qu'il est installé, il suffit de configuer le `/.ssh/config` ainsi (je suppose ici que le relais est `proxy.example.com`, port 80) :

```
ProxyCommand corkscrew proxy.example.com  80 %h %p
```

%h et %p seront remplacés par le nom et le port du serveur SSH. corkscrew utilisera la commande HTTP CONNECT (RFC 7231 [1], section 4.3.6) pour se connecter au serveur SSH. Le trafic sur le port 443 étant supposé être chiffré, le relais n'a pas de moyen technique de savoir que ce qui circule est en fait du SSH (mais attention, un relais intelligent pourrait le déduire de certaines caractéristiques du trafic, comme sa relative symétrie).

Le fait qu'il écoute sur le port 443 est important avec certains relais, qui n'acceptent pas de relayer vers un port quelconque et produisent un message comme : " *Proxy could not open connnection to mymachine.example.org : Proxy Error (The specified Secure Sockets Layer (SSL) port is not allowed. ISA Server is not configured to allow SSL requests from this port. Most Web browsers use port 443 for SSL requests.)* ".

Avec certains relais, les connexions SSH coupent au bout d'un moment, car le relais impose une durée maximale aux connexions HTTP. Pas d'autre solution que de se reconnecter.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7231.txt`