Sadek Adel, 19/12/2025
Etudiant à l'université Sorbonne Paris 1

Utilisation d'un tunnel ICMP

Table des matières

Sadek Adel, 19/12/2025
Etudiant à l'université Sorbonne Paris 1

Introduction

Dans cette documentation nous allons voir comment créer un tunnel ICMP entre deux hôtes pour notamments relier le port 22 d'une machine distante à une autre via un tunnel ICMP et pouvoir utiliser un proxy ssh SOCKS

Ceci est un laboratoire expérimentale en sécurité informatique pour voir à quel point le protocole ICMP n'est pas innofensif et qu'il faut le surveiller et filtrer pour éviter des fuites

Configuration du réseau

Client : 192.168.0.33

Serveur : 51.222.9.215

Installation de ptunnel

Sur les deux machines il faut installer ptunnel

Apt-get install ptunnel

Lancer le tunnel

```
ptunnel -x monpass
```

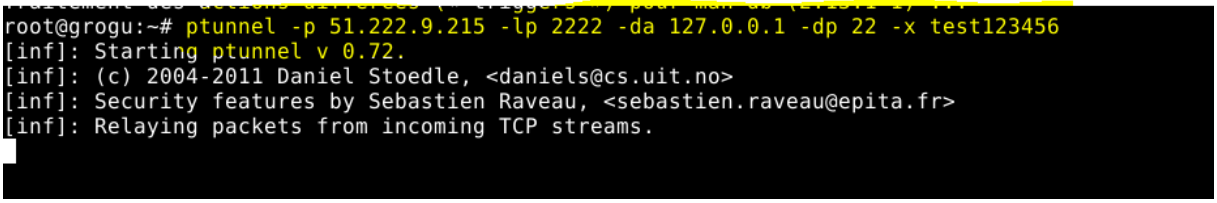
```
root@smtp:~# ptunnel -x test123456
[inf]: Starting ptunnel v 0.72.
[inf]: (c) 2004-2011 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@ep
ita.fr>
[inf]: Forwarding incoming ping packets over TCP.
[inf]: Ping proxy is listening in privileged mode.
```

Coté client

Sadek Adel, 19/12/2025
Etudiant à l'université Sorbonne Paris 1

ptunnel -p IP_SERVEUR -lp 2222 -da 127.0.0.1 -dp 22 -x monpass

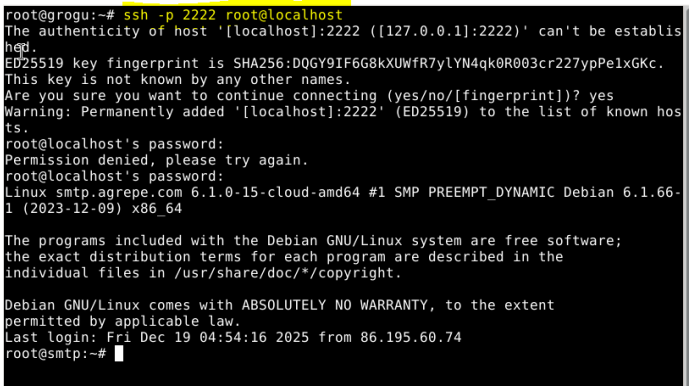
- `-p IP_SERVEUR` : IP publique du serveur ptunnel.
- `-lp 2222` : port local pour rejoindre le SSH du serveur.
- `-da 127.0.0.1 -dp 22` : côté serveur, ptunnel se connecte à `localhost:22`



Test SSH

D'abord nous allons essayer de joindre le port 22 de la amchine distante via notre port 2222 local

J'ai pu me connecter avec succès



Sadek Adel, 19/12/2025
Etudiant à l'université Sorbonne Paris 1

Coté client :

```
root@grogu:~# ptunnel -p 51.222.9.215 -lp 2222 -da 127.0.0.1 -dp 22 -x test123456
[inf]: Starting ptunnel v 0.72.
[inf]: (c) 2004-2011 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@epita.fr>
[inf]: Relaying packets from incoming TCP streams.
[inf]: Incoming connection.
[evt]: No running proxy thread - starting it.
[inf]: Ping proxy is listening in privileged mode.
```

Coté serveur :

```
root@smtp:~# ptunnel -x test123456
[inf]: Starting ptunnel v 0.72.
[inf]: (c) 2004-2011 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@ep
ita.fr>
[inf]: Forwarding incoming ping packets over TCP.
[inf]: Ping proxy is listening in privileged mode.
[inf]: Incoming tunnel request from 86.195.60.74.
[inf]: Starting new session to 127.0.0.1:22 with ID 52014
[err]: Dropping duplicate proxy session request.
```

Nous voyons ici une nouvelle connexion entrante

Proxy SOCKS

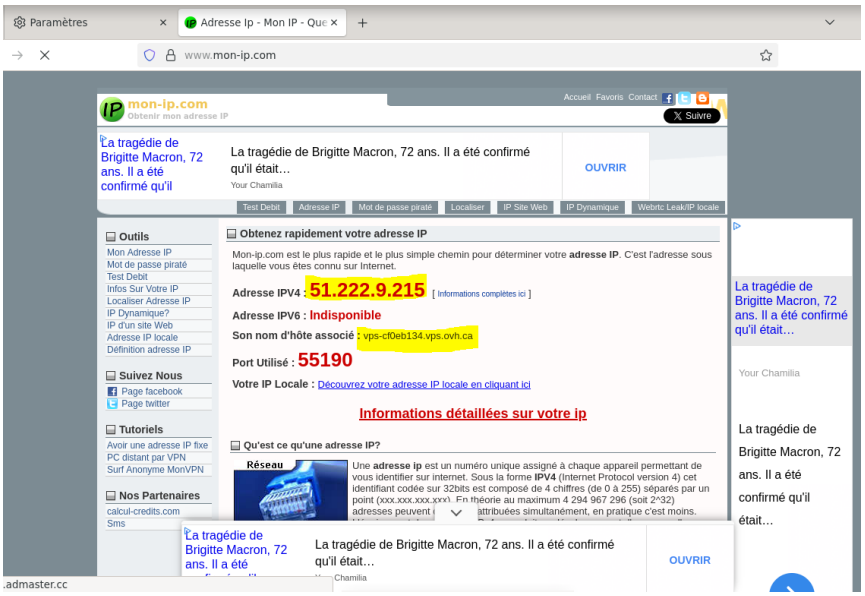
Coté client :

```
root@grogu:~# ssh -p 2222 -D 1080 root@localhost
root@localhost's password:
Linux smtp.agrepe.com 6.1.0-15-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.66-
1 (2023-12-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Dec 19 04:56:29 2025 from 127.0.0.1
root@smtp:~#
```

Sadek Adel, 19/12/2025
Etudiant à l'université Sorbonne Paris 1



On voit bien que mon IP a changé pour le vps chez ovh

Coté serveur :