

Utilisation d'un tunnel ICMP

Table des matières

Utilisation d'un tunnel ICMP	1
Introduction.....	2
Configuration du réseau.....	2
Installation de ptunnel	2
Lancer le tunnel.....	2
Coté client	2
Test SSH.....	3
Coté client :.....	4
Coté serveur :	4
Proxy SOCKS	4
Coté client :.....	4
Coté serveur :	5

Introduction

Dans cette documentation nous allons voir comment créer un tunnel ICMP entre deux hôtes pour notamment 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 inoffensif 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 Sébastien Raveau, <sebastien.raveau@epita.fr>
[inf]: Forwarding incoming ping packets over TCP.
[inf]: Ping proxy is listening in privileged mode.
```

Côté client

```
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`

```
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.
```

Test SSH

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

J'ai pu me connecter avec succès

```
root@grogu:~# ssh -p 2222 root@localhost
The authenticity of host '[localhost]:2222 ([127.0.0.1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:DQGY9IF6G8kXUWfR7ylYN4qk0R003cr227yPe1xGKc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts.
root@localhost's password:
Permission denied, please try again.
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 04:54:16 2025 from 86.195.60.74
root@smtp:~#
```

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 Sébastien 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 Sébastien Raveau, <sebastien.raveau@epita.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

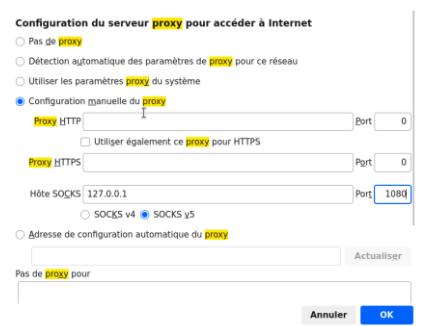
Proxy SOCKS

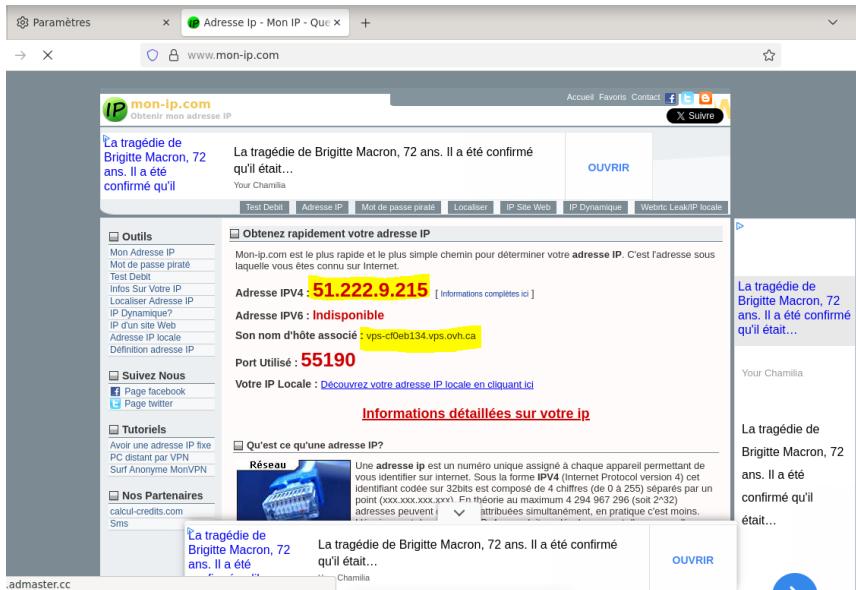
Coté client :

```
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:~#
```





The screenshot shows a web browser window for the website www.mon-ip.com. The main content area displays the IP address **51.222.9.215** in red, with a note that it is **Indisponible** (Unreachable). Below the IP address, there is a link to a news article titled "La tragédie de Brigitte Macron, 72 ans. Il a été confirmé qu'il était...". The sidebar on the left contains various links for tools like "Obtenez rapidement votre adresse IP", "Port Utilisé : 55190", and "Votre IP Locale : Découvrez votre adresse IP locale en cliquant ici". The sidebar also includes a "Tutoriels" section with links to "Réseau" and "La tragédie de Brigitte Macron, 72 ans. Il a été confirmé qu'il était...". The footer of the page includes links to "Paramètres", "Adresse IP - Mon IP - Que", and "Suivre".

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

Coté serveur :

```
Session statistics:  
[inf]: I/0: 0.00/ 0.00 mb ICMP I/O/R: 187/ 22/ 0 Loss: 0.0%  
[inf]:  
[inf]: Incoming tunnel request from 86.195.60.74.  
[inf]: Starting new session to 127.0.0.1:22 with ID 58734  
[err]: Dropping duplicate proxy session request.
```