



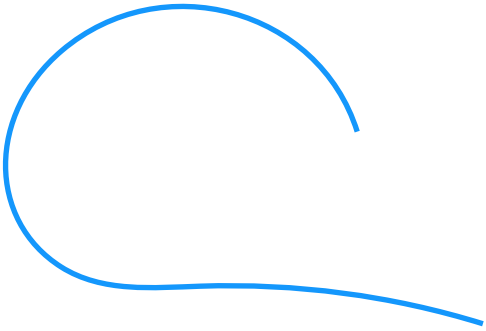
Connexions refusées

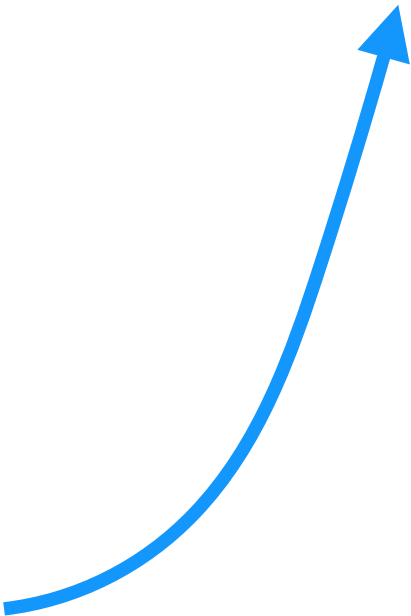
Connexions refusées

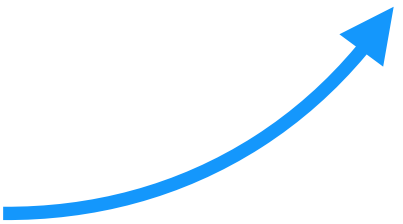
Connexions  
refusées



Connexions filtrées











Tunnel SSH

Connexions sortant  
du tunnel SSH







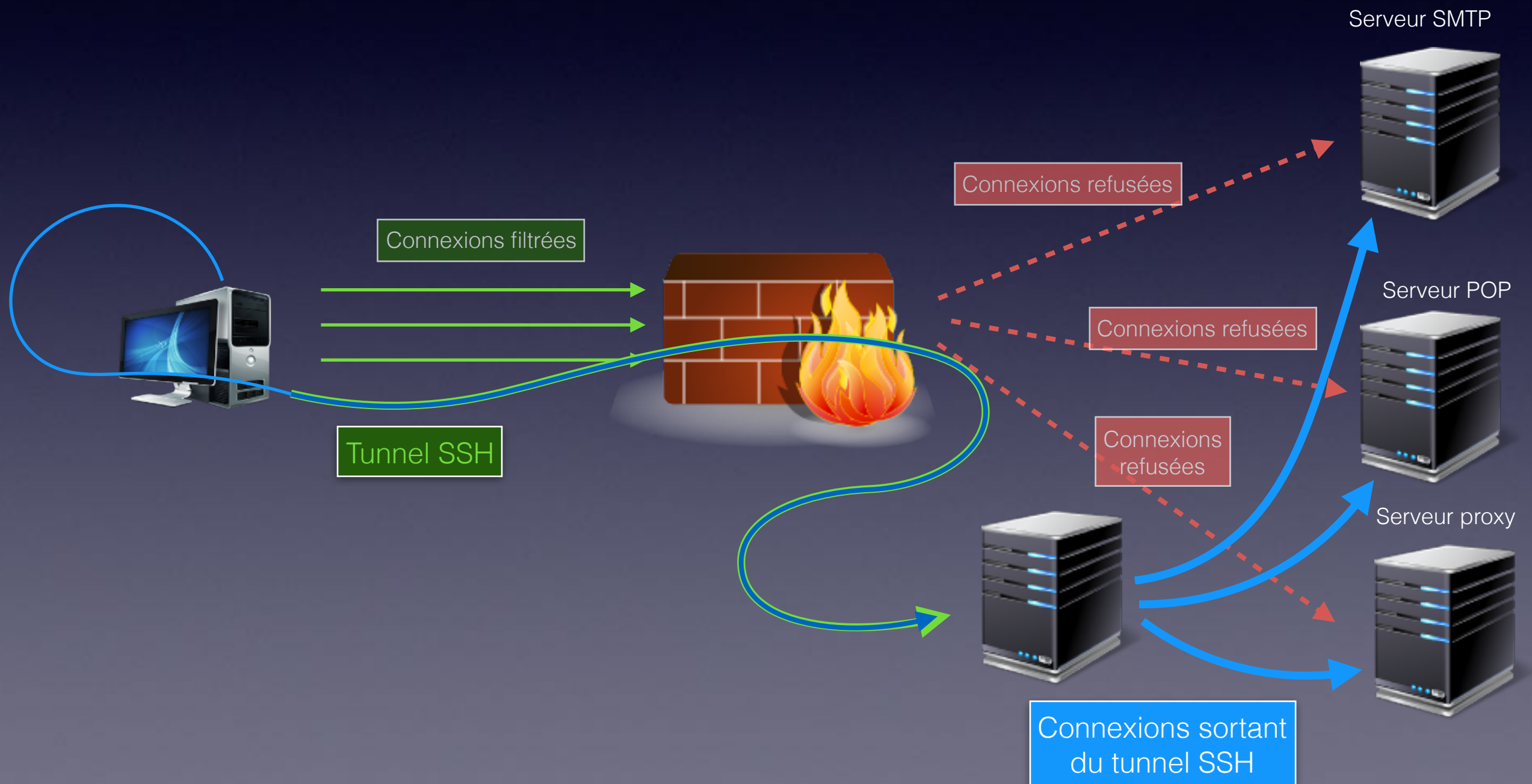






# Exploitation

## Contournement de pare-feu - Rebonds



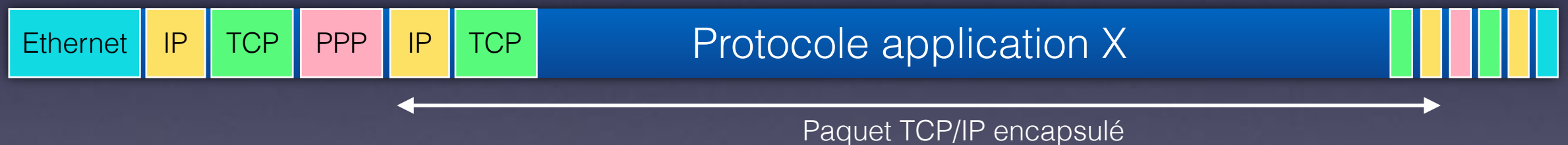
# Exploitation

## Contournement de pare-feu

### Tunneling

- Tunnel

- Encapsulation d'un protocole (payload) dans un autre protocole réseau dit « de délivrance ».
- le tunnel diffère d'une pile réseau classique car le protocole encapsulé est de niveau inférieur ou égal au protocole de délivrance.
  - Ex : IP -> GRE -> IP -> TCP
  - Ex : IP -> IPSEC -> IP -> TCP



- Principaux protocoles de tunneling :

- GRE
- L2TP
- IPSec
- PPPoE
- ...

<http://www.cert.ssi.gouv.fr/site/CERTA-2001-INF-003/>