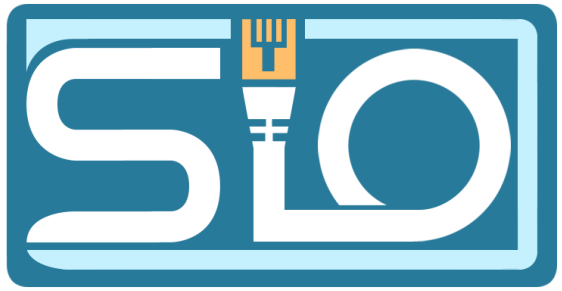


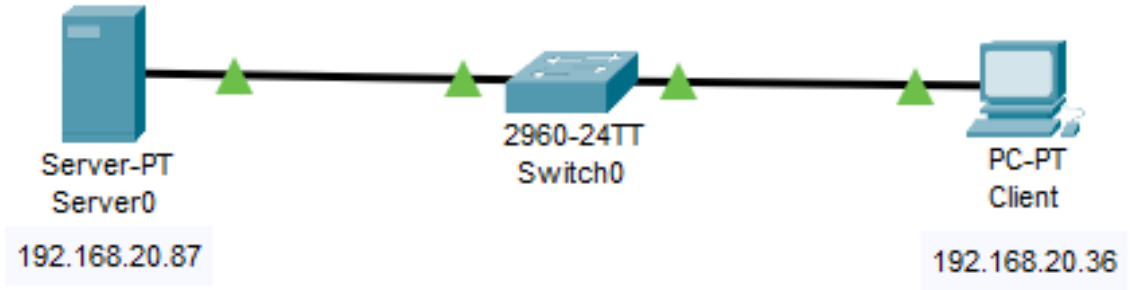
TP Iptables

FLORENTIN BRACQ- -FLABAT BTS 2 SIO

Iptables avantages et inconvénients

Avantages	Inconvénients
Libre Open source Gratuit Inclus dans Linux	Syntaxe compliquée Gestion difficile

Schéma réseau



Installation de iptables sur Debian

Pour installer iptables sur debian, tapper la commande **apt install iptables**

```
root@debian:~# apt install iptables
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  linux-image-6.1.0-22-amd64
Veuillez utiliser « apt autoremove » pour le supprimer.
Les paquets supplémentaires suivants seront installés :
  libip6tc2 libnetfilter-conntrack3 libnfnetlink0
Paquets suggérés :
  firewalld
Les NOUVEAUX paquets suivants seront installés :
  iptables libip6tc2 libnetfilter-conntrack3 libnfnetlink0
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 435 ko dans les archives.
Après cette opération, 2 728 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] _
```

Empêcher le ping sur l'adresse de loopback

Créer une chaîne personnelle :

Iptables –N florentin

Prise en compte de la chaîne dans les logs :

Iptables –A florentin –j LOG

Prise en compte de l'action :

Iptables –A florentin –j DROP

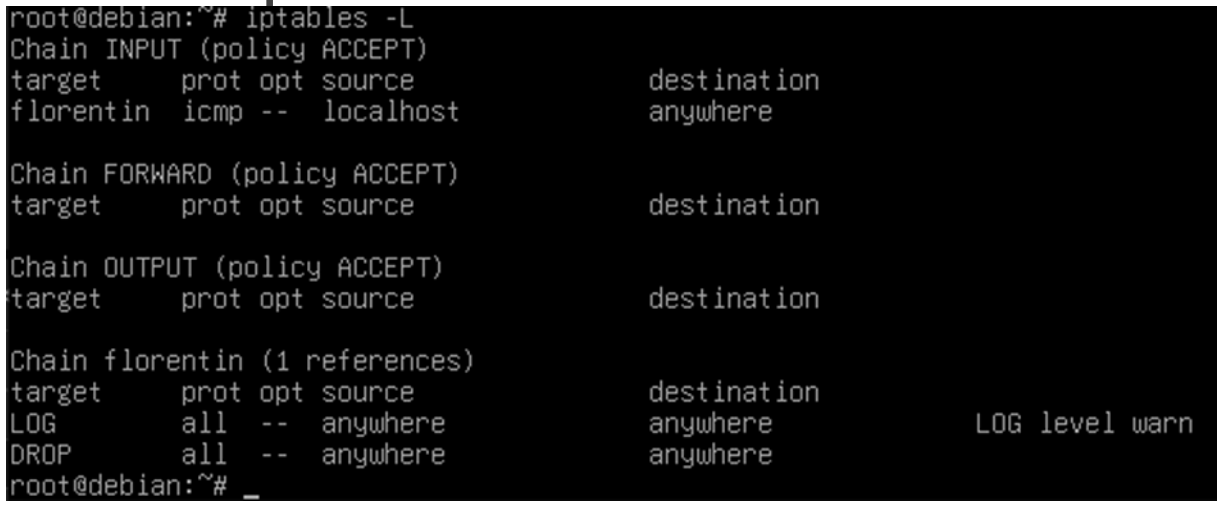
```
root@debian:~# iptables -N florentin
root@debian:~# iptables -A florentin -j LOG
root@debian:~# iptables -A florentin -j DROP
root@debian:~# iptables -A INPUT -p icmp -s 127.0.0.1 -j florentin
```

Écriture de la chaîne :

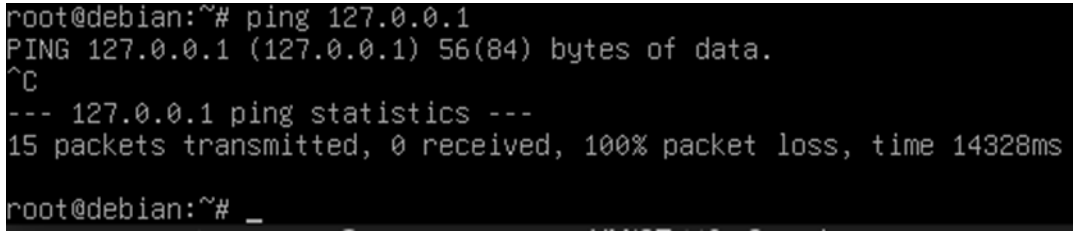
Iptables –A INPUT –p icmp –s 127.0.0.1 –j florentin

Vérification

Vérification avec la commande **iptables –L**



Vérification qu'il n'est plus possible de ping 127.0.0.1



Empêcher le client de ping le serveur

Pour bloquer le ping du client vers le serveur, utiliser la commande suivante :

```
root@debian:~# iptables -A INPUT -p icmp -s 192.168.20.36 -j florentin_
```

L'adresse IP correspond à la machine cliente.

Test du ping à partir du client vers le serveur :

```
root@debian:~# ping 192.168.20.87
PING 192.168.20.87 (192.168.20.87) 56(84) bytes of data.
^C
--- 192.168.20.87 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5105ms

root@debian:~#
```

Accéder au serveur web uniquement en http

Pour accéder au serveur web uniquement en http, utiliser les commandes suivantes :

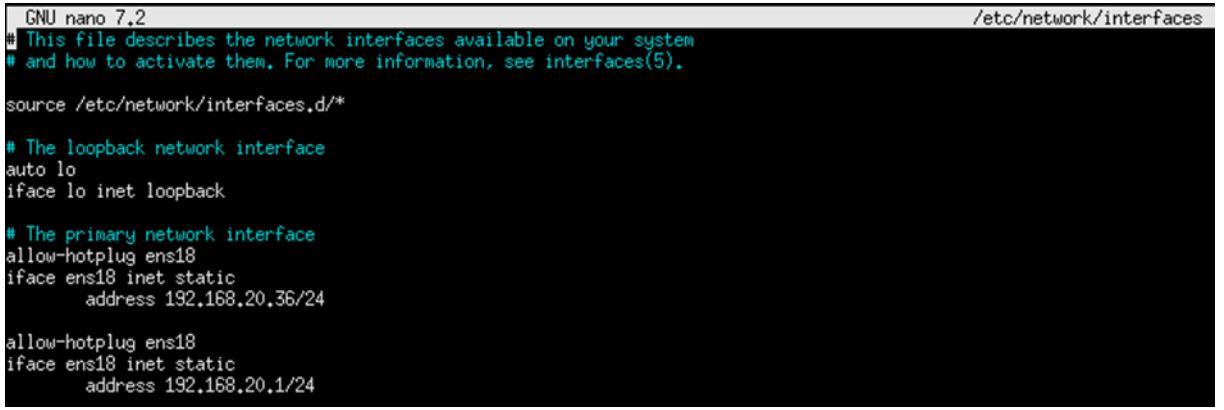
iptables -A INPUT -m tcp -p tcp --dport 443 -j DROP

iptables -A OUTPUT -m tcp -p tcp --dport 443 -j DROP

```
root@debian:~# iptables -A INPUT -m tcp -p tcp --dport 443 -j DROP
root@debian:~# iptables -A OUTPUT -m tcp -p tcp --dport 443 -j DROP
root@debian:~# _
```

Affecter une double IP sur le client

Pour mettre une 2ème IP sur la carte réseau du client, taper la commande **nano /etc/network/interfaces** pour modifier le fichier de configuration



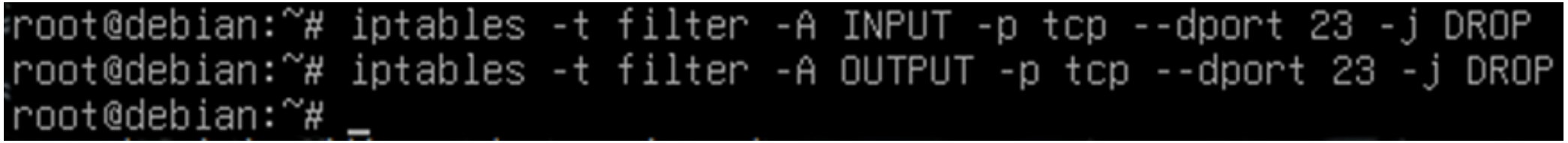
Test avec la commande **ip a**

Bloquer le protocole telnet

Pour bloquer les protocole telnet, utiliser les commandes suivantes :

iptables -t filter -A INPUT -p tcp --dport 23 -j DROP

iptables -t filter -A OUTPUT -p tcp --dport 23 -j DROP



Bloquer une adresse IP sur une page web

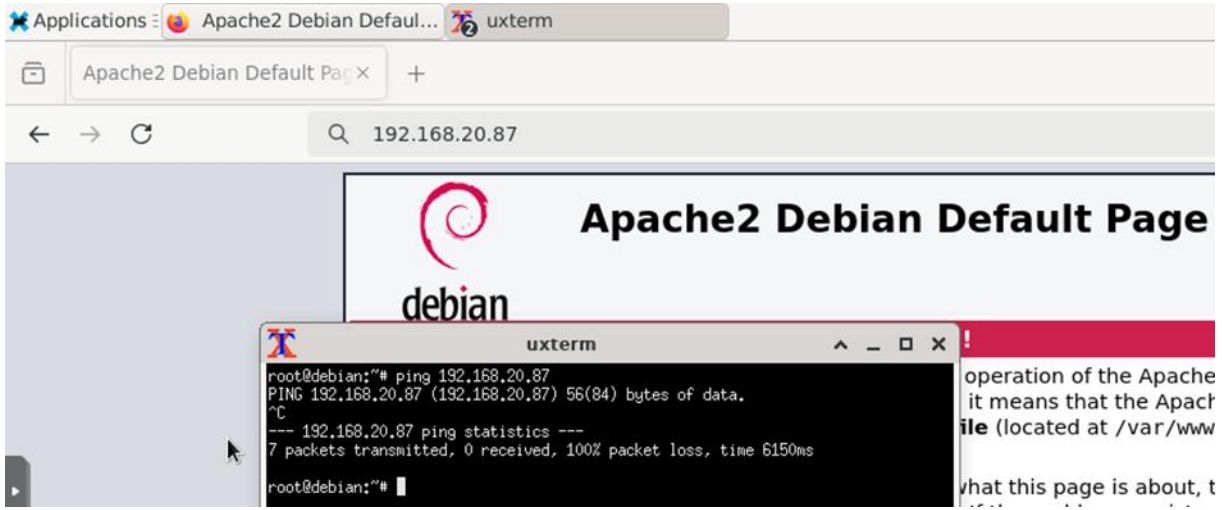
Pour bloquer une adresse IP sur une page web, utiliser les commandes suivantes :

iptables -A INPUT -s <ADRESSE_IP> -p tcp --dport 80 -j DROP

iptables -A INPUT -s <ADRESSE_IP> -p tcp --dport 443 -j DROP

Tests

Depuis le client :



Depuis le serveur :