

# TP Iptables

FLORENTIN BRACQ- -FLABAT BTS 2 SIO

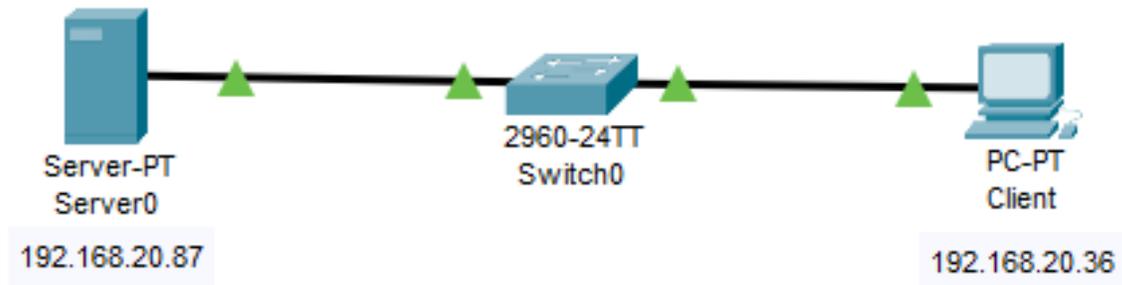
# Iptables avantages et inconvénients

---

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, taper 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-contrack3 libnfnetlink0
Paquets suggérés :
  firewalld
Les NOUVEAUX paquets suivants seront installés :
  iptables libip6tc2 libnetfilter-contrack3 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**

```
root@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
florentin  icmp -- localhost            anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain florentin (1 references)
target     prot opt source                destination
LOG        all  -- anywhere             anywhere             LOG level warn
DROP      all  -- anywhere             anywhere
```

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

```
root@debian:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14328ms
root@debian:~# _
```

# 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 2<sup>ème</sup> IP sur la carte réseau du client, taper la commande **nano /etc/network/interfaces** pour modifier le fichier de configuration

```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens18
iface ens18 inet static
    address 192.168.20.36/24

allow-hotplug ens18
iface ens18 inet static
    address 192.168.20.1/24
```

Test avec la commande **ip a**

```
root@debian:~# systemctl restart networking.service
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:af:a2:ec brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.20.36/24 brd 192.168.20.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet 192.168.20.1/24 brd 192.168.20.255 scope global secondary ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:feaf:a2ec/64 scope link
        valid_lft forever preferred_lft forever
```

# Bloquer le protocole telnet

---

Pour bloquer le 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
```

```
root@debian:~# iptables -t filter -A INPUT -p tcp --dport 23 -j DROP
root@debian:~# iptables -t filter -A OUTPUT -p tcp --dport 23 -j DROP
root@debian:~#
```

# Bloquer une adresse IP sur une page web

---

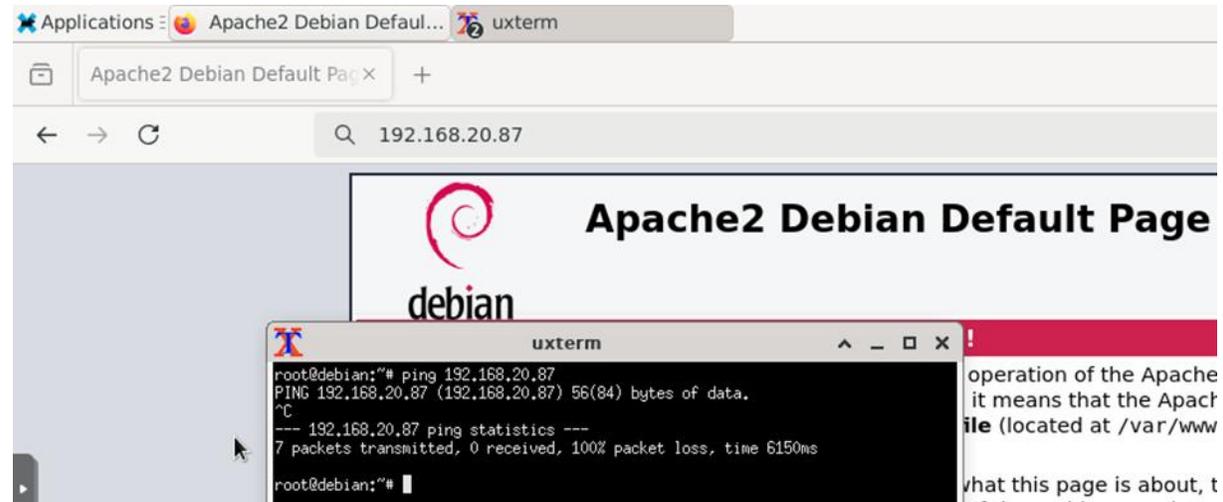
Pour bloquer une adresse IP sur une page web, utiliser les commandes suivantes :

```
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 :

```
root@debian:~# ping 192.168.20.36
PING 192.168.20.36 (192.168.20.36) 56(84) bytes of data.
^C
--- 192.168.20.36 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3067ms
root@debian:~#
```