2024-2025

SIOSISR

COURS-FIREWALL-IPTABLES

Axel Hespel

DÉCOUVERTE

Table	Description
filter	table permettant le passage ou non des paquets selon les regles mise en place.
nat	Permet de venir faire le routage entre les différente carte
mangle	Table qu viens modifier le paquet lui meme et y ajouter différent marquer pour un traitement ultérieur.

DÉCOUVERTE

Chaine	Table	Description
PREROUTING	NAT MANGLE	S’applique aprés l’input en préambule du routage
INPUT	Filter	S’applique a l’entrer du paquet
FORWARD	Filter	S’applique pendant un passage vers une autre carte réseau
OUTPUT	Filter	S’applique en sortant d’une pate réseau
POSTROUTING	NAT MANGLE	S’applique aprés le routage

DÉCOUVERTE

Cible	Description
ACCEPT	Laisse le paquet passer vers les prochaines regle
DROP	Refuse le paquet
REJECT	Refuse le paquet et préviens de son rejet a l'émetteur
LOG	Enregistre les règles le passant dans les logs
MASQUERADE	Masque l'ip source des connexions sortantes
SNAT	change l'ip source du paquet sortant avec une IP statique
DNAT	Modifie l'adresse de destination
RETURN	Fais un revenir a une regle X le paquet

2024-2025

SIOSISR

TP- DÉCOUVERTE IPTABLES

Axel Hespel

DÉCOUVERTE

CRÉATION DE LA CHAINE

iptables -N machaine

AJOUTER AU LOGS PLUS & DROP CE QUI VIENS DE : 127.0.0.1

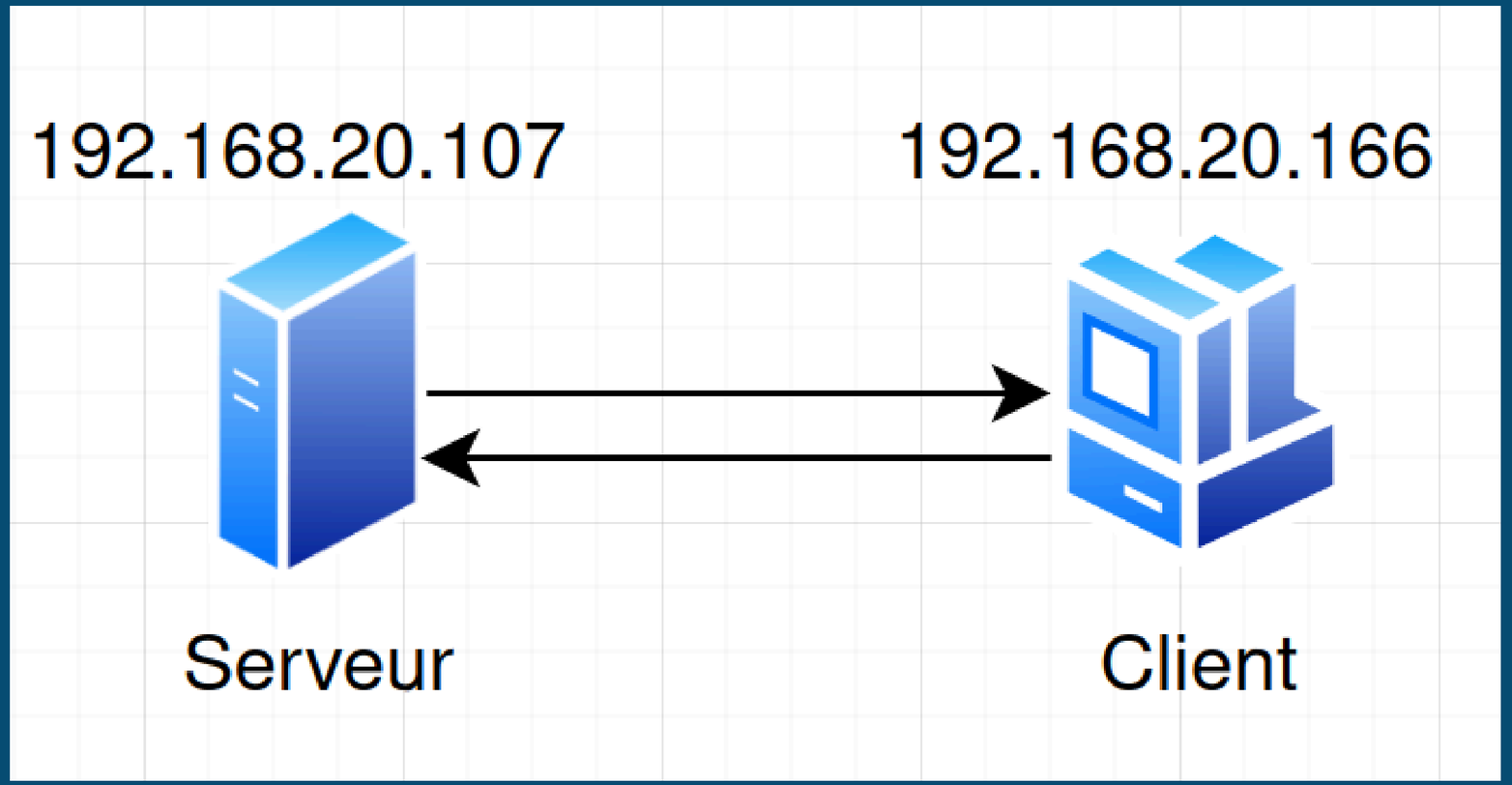
```
iptables -A chaine -j LOG
```

```
iptables -A chaine -j DROP
```

```
root@Apache-1:~# iptables -A INPUT -p icmp -s 127.0.0.1 -j chaine
```

On ajoute une regle de filtrage a l'entré, mais aucune regle autorise de passer donc il est se voir rejeter

MON INFRA



3.

Nous vollons donc empecher les pings de serveur > client

Avant :

```
root@Apache-1:~# ping 192.168.20.166
PING 192.168.20.166 (192.168.20.166) 56(84) bytes of data.
64 bytes from 192.168.20.166: icmp_seq=1 ttl=64 time=0.354 ms
64 bytes from 192.168.20.166: icmp_seq=2 ttl=64 time=0.222 ms
^C
--- 192.168.20.166 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1062ms
rtt min/avg/max/mdev = 0.222/0.288/0.354/0.066 ms
root@Apache-1:~#
```

```
iptables -N ping_client
iptables -A ping_client -j LOG
iptables -A ping_client -j DROP
iptables -A OUTPUT -p icmp -s 192.168.20.166 -j ping_client
```

Apres :

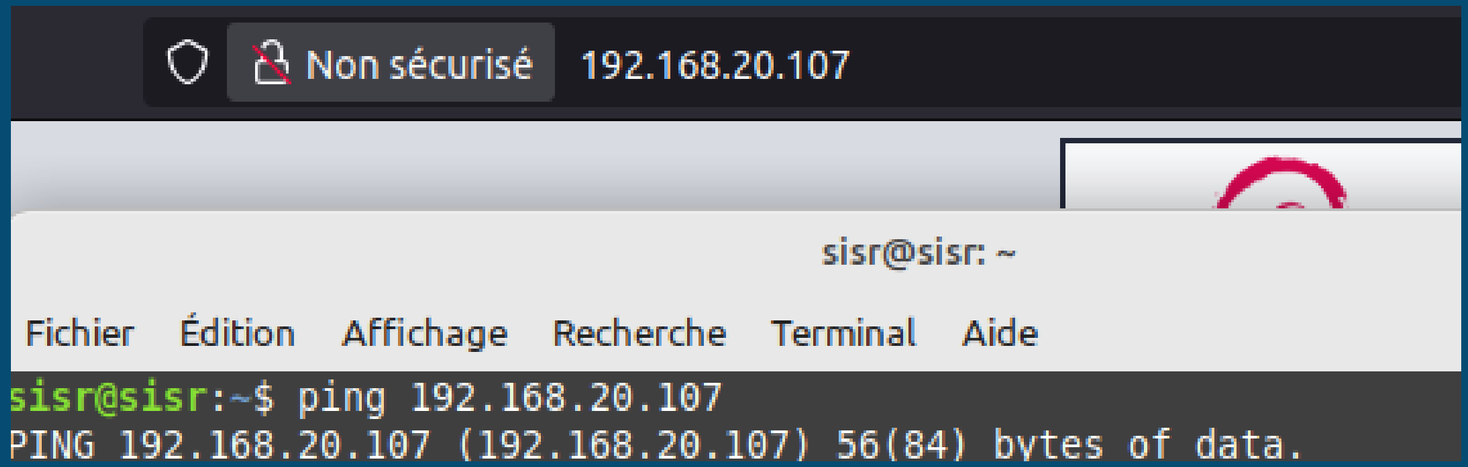
```
root@Apache-1:~# ping 192.168.20.166
PING 192.168.20.166 (192.168.20.166) 56(84) bytes of data.
^C
--- 192.168.20.166 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1027ms
```

3.

Pour accéder au serveur en http et uniquement https, on autorise uniquement le port 80 avec !

```
root@Apache-1:~# iptables -A INPUT -p tcp ! --dport 80 -j web_rules
```

ici je bloque toute les entrés qui ne sont pas sur le port 80



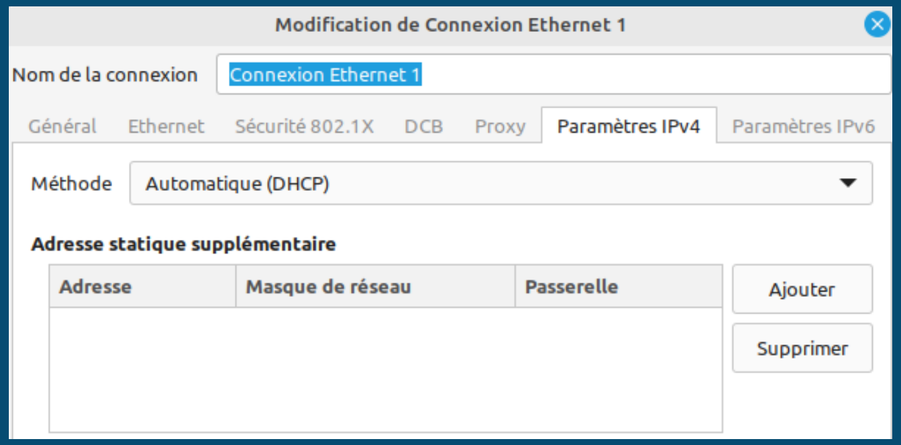
Je vérifie, le ping ne passe pas mais j’accède au serveur WEB

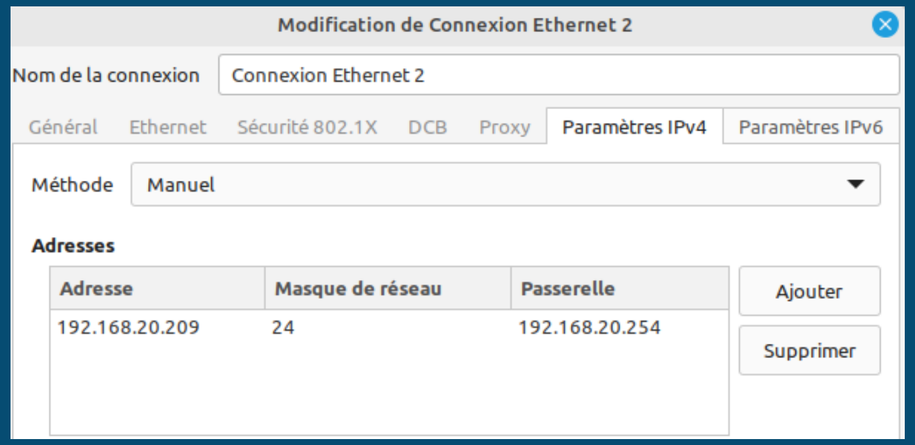
3. DIFFÉRENTES CONFIG : CLIENT

Interdisez votre serveur web à cette seconde adresse.

La regle précédente, viens bloquer tous SAUF http, donc telnet avec

```
root@Apache-1:~# iptables -A INPUT -p tcp ! --dport 80 -j web_rules
```

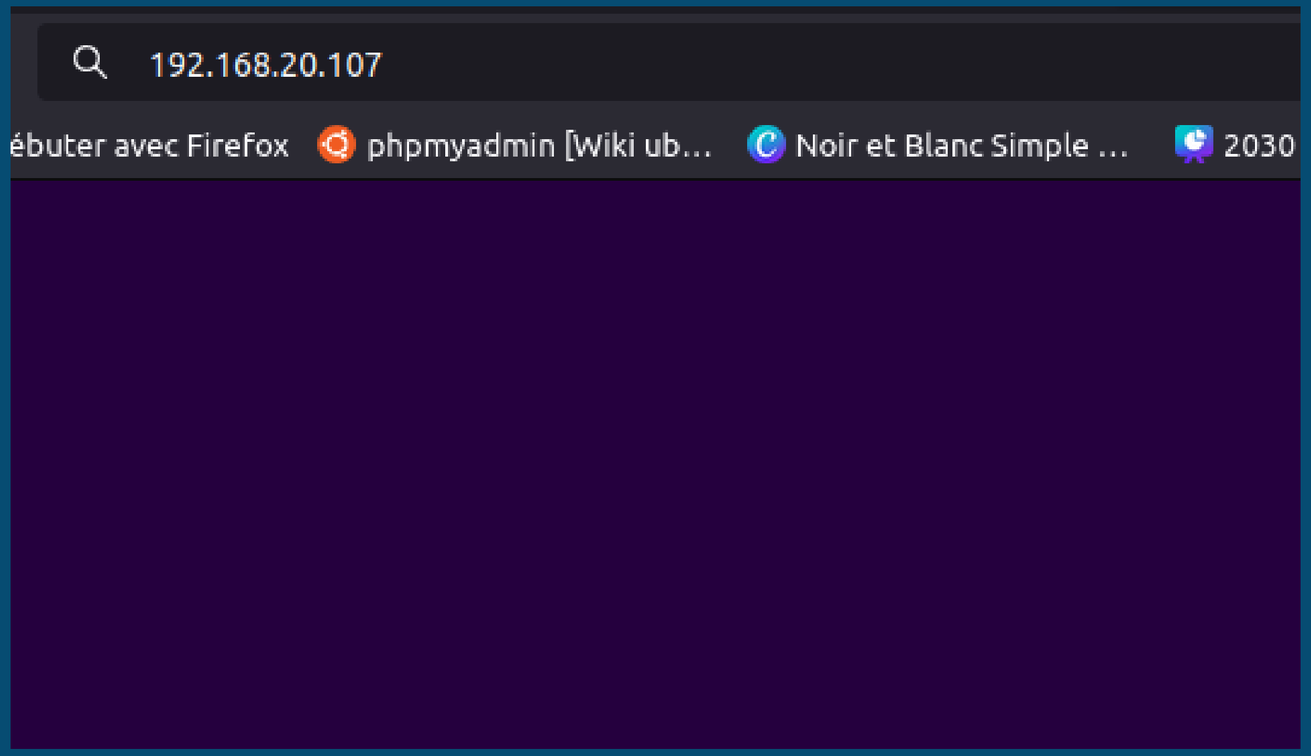




3.

```
iptables -A INPUT -s 192.168.20.209 -p tcp --dport 80 -j web_rules
```

Je bloque la source en 209 (deuxième IP)



Je n’ai plus accés avec cette IP

3.

ÉCRIRE LES RÈGLES QUI RÉPONDENT AUX DEMANDES SUIVANTES

```
root@sisr:~# iptables -A client_rules -m state --state ESTABLISHED,RELATED -j ACCEPT
root@sisr:~# iptables -A OUTPUT -p tcp -d 192.168.20.209 --dport 80 -j client_rules
root@sisr:~# iptables -A OUTPUT -p tcp -j client_rules
root@sisr:~# iptables -A OUTPUT -p icmp -d 192.168.20.107 -j client_rules
root@sisr:~# iptables -A INPUT -p icmp -j client_rules
```

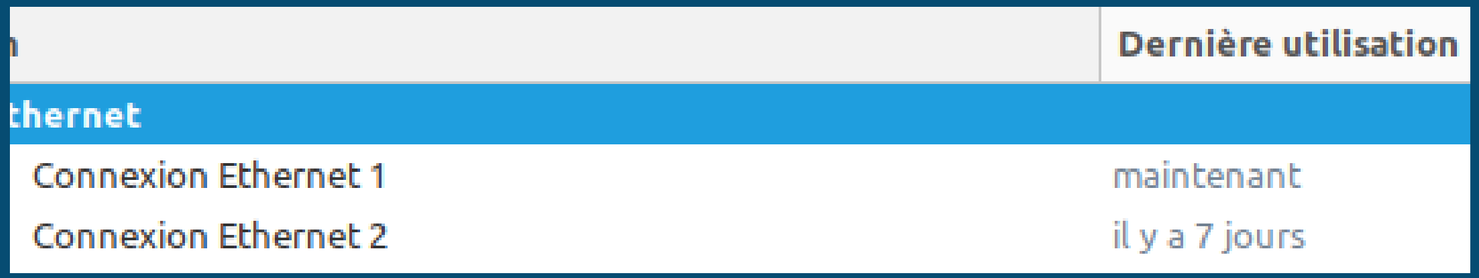
VOTRE SERVEUR WEB EST UNIQUEMENT SERVEUR WEB

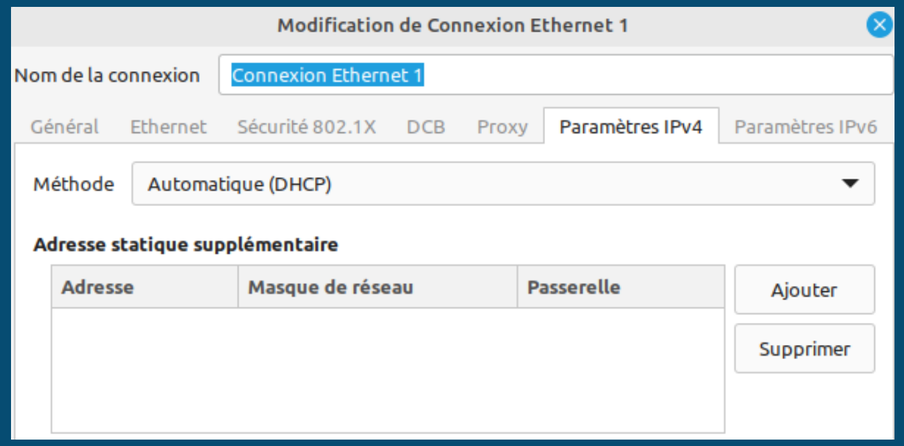
```
root@Apache-1:~# iptables -A INPUT -p tcp ! --dport 80 -j web_rules
```

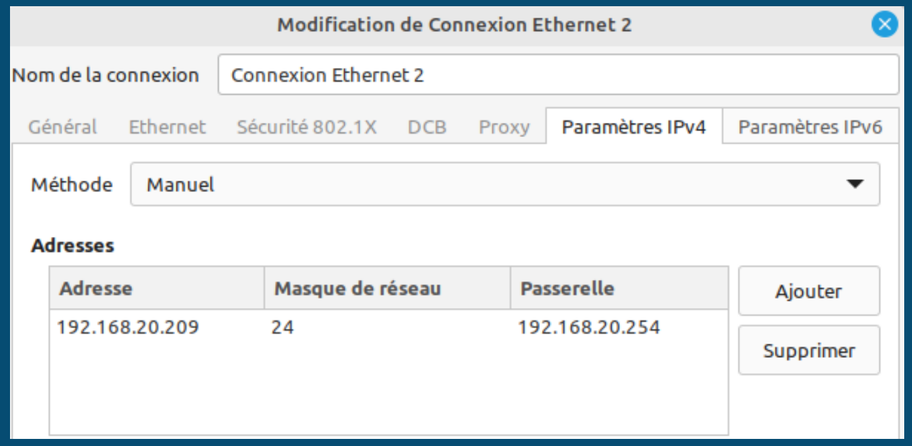
LE POSTE CLIENT NE PEUT PAS ÊTRE PINGUÉ

```
iptables -A INPUT -p icmp -d 192.168.20.166 -j DROP
```

3. CLIENT CONFIG







Une seule regle présente:

```
iptables -A INPUT -p icmp -d 192.168.20.166 -j DROP
```

3. SERVEUR CONFIG

```
  GNU nano 7.2
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

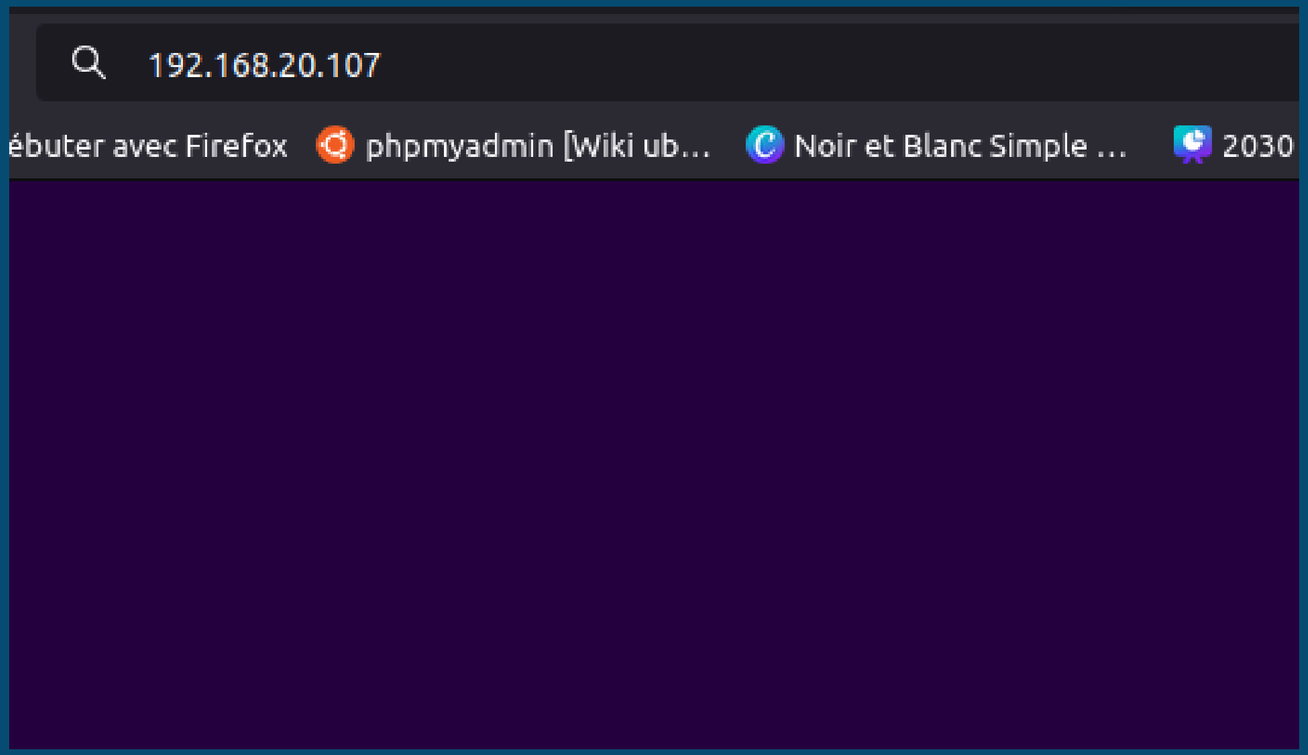
```
root@Apache-1:~# iptables -L                                    Disconnecting... (Detecting m
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
chaine     icmp --  localhost            anywhere
chaine     icmp --  localhost            anywhere
web_rules  tcp  --  anywhere             anywhere             tcp dpt:!http
web_rules  tcp  --  192.168.20.209       anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ping_client  icmp --  192.168.20.166       anywhere
ping_client  icmp --  anywhere             192.168.20.166

Chain chaine (2 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warn
DROP       all  --  anywhere             anywhere

Chain ping_client (2 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warn
DROP       all  --  anywhere             anywhere

Chain web_rules (2 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             LOG level warn
DROP       all  --  anywhere             anywhere
```

3. TEST

PING Serveur > Client

```
root@Apache-1:~# ping 192.168.20.166
PING 192.168.20.166 (192.168.20.166) 56(84) bytes of data.
^C
--- 192.168.20.166 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1027ms
```

Accés WEB avec deuxieme IP

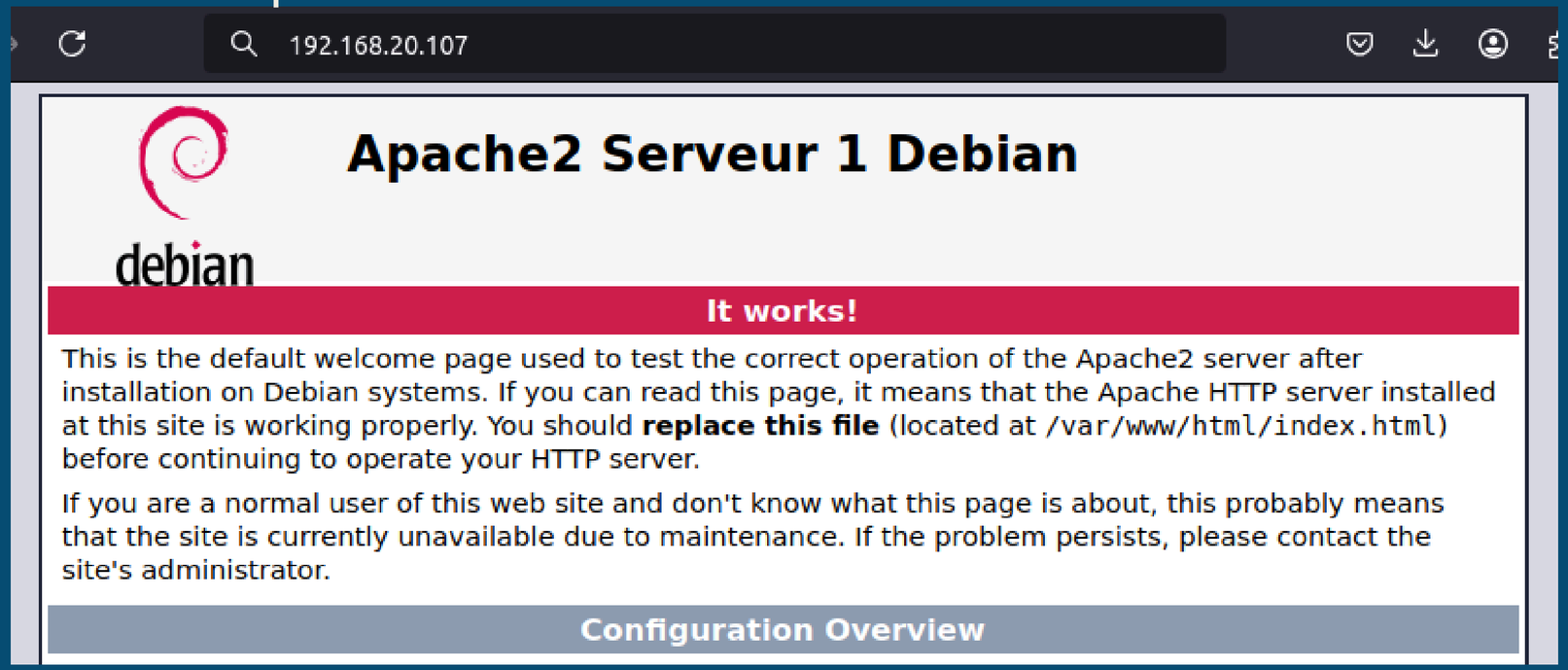


3. TEST

PING Client > Serveur

```
root@sisr:~# ping 192.168.20.107
PING 192.168.20.107 (192.168.20.107) 56(84) bytes of data.
^C
--- 192.168.20.107 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3075ms

root@sisr:~#
```

Avec ma premiere IP



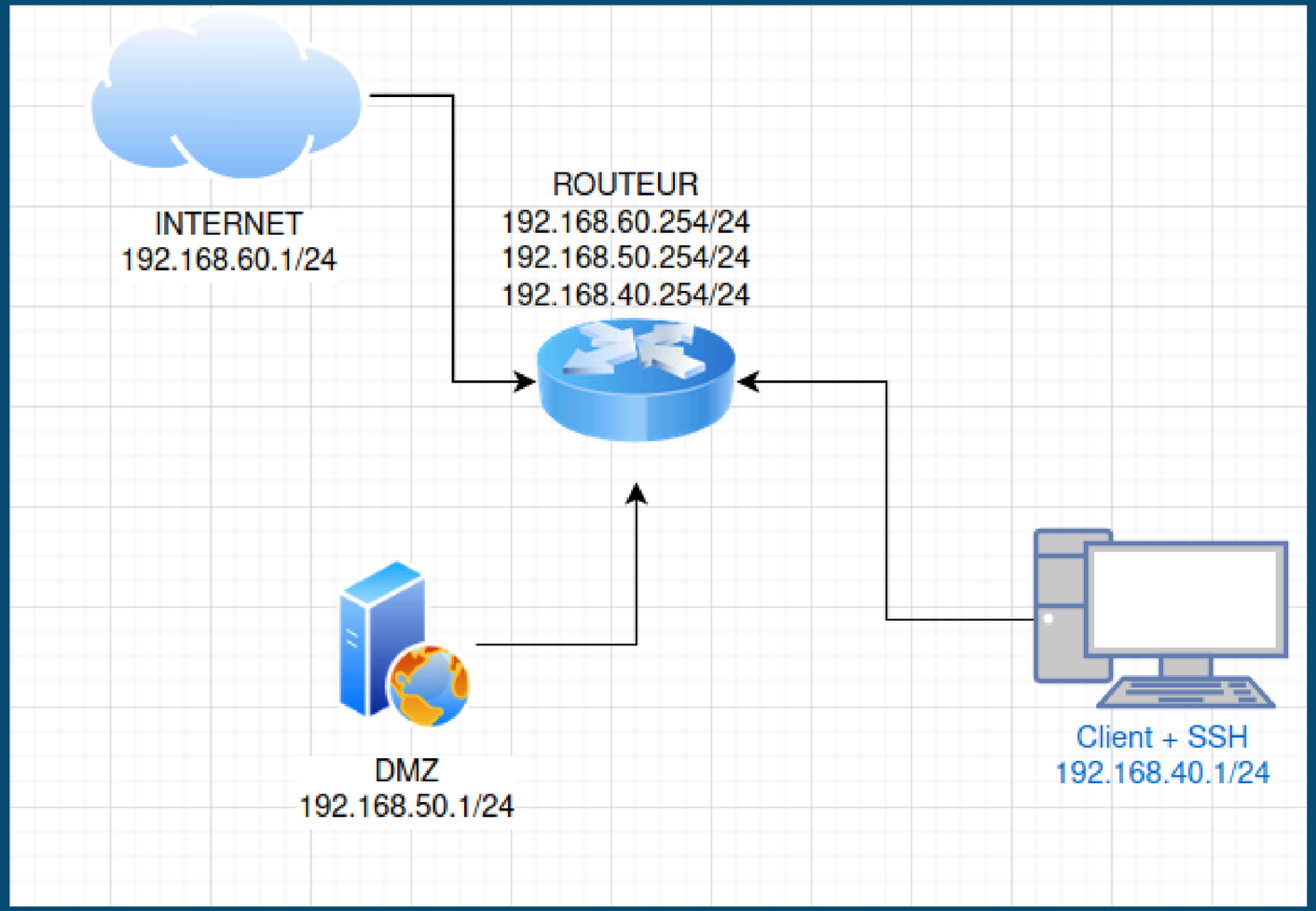
2024-2025

SIOSISR

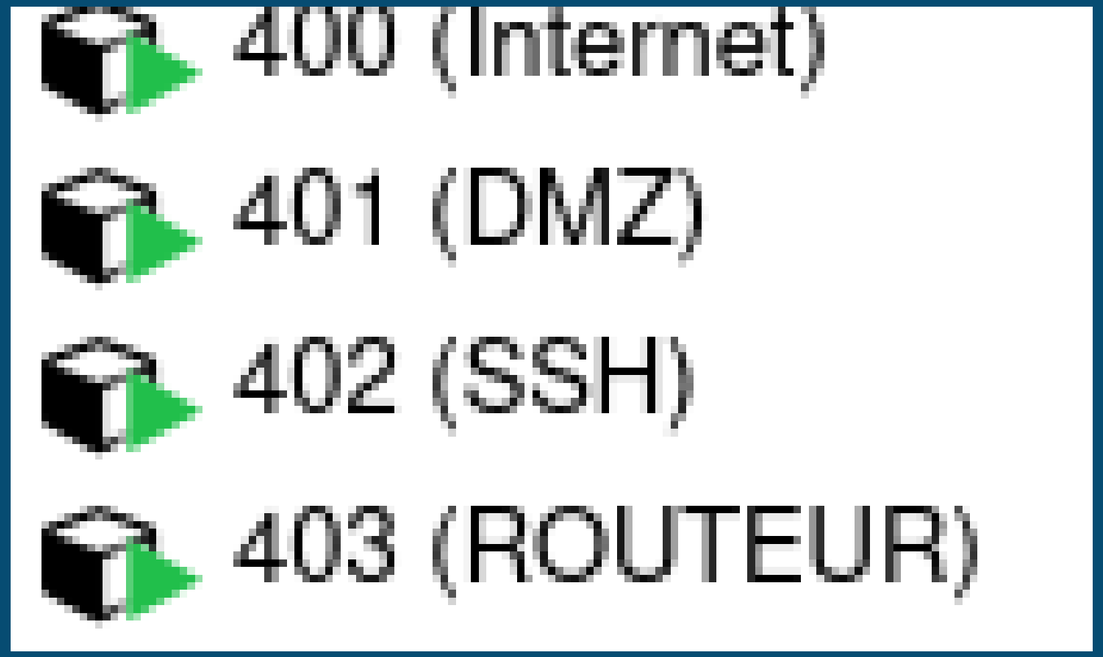
TP2- IPTABLES

Axel Hespel

2. INFRASTRUCUTRE



2. TP2- IPTABLES



(Routeur)

net0	eth0	Temp	Yes	BC:24:11:08:...	192.168.40.254/24
net1	eth1	Temp	Yes	BC:24:11:52:...	192.168.50.254/24
net2	eth2	Temp	Yes	BC:24:11:BA...	192.168.60.254/24

2. TP2- IPTABLES

Activer le routing entre les adresses dans /etc/sysctl.conf

```
NET.IPV4.IP_FORWARD=1
```

Rendre accessible la DMZ au LAN et WAN

```
root@ROUTEUR:~# iptables -A FORWARD -s 192.168.60.0/24 -d 192.168.50.0/24 -j ACCEPT
root@ROUTEUR:~# iptables -A FORWARD -s 192.168.50.0/24 -d 192.168.60.0/24 -j ACCEPT
root@ROUTEUR:~# iptables -A FORWARD -s 192.168.60.0/24 -d 192.168.40.0/24 -j ACCEPT
root@ROUTEUR:~# iptables -A FORWARD -s 192.168.40.0/24 -d 192.168.60.0/24 -j ACCEPT
```

On bloque le reste

```
iptables -A FORWARD -j REJECT
```

2. GESTION DE LA DMZ

```
root@ROUTEUR:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  192.168.50.0/24      192.168.40.0/24
ACCEPT     icmp --  192.168.40.0/24      192.168.50.0/24
REJECT     icmp --  anywhere             anywhere             reject-with icmp-port-unreachable
ACCEPT     all  --  192.168.60.0/24      192.168.50.0/24
ACCEPT     all  --  192.168.50.0/24      192.168.60.0/24
ACCEPT     all  --  192.168.50.0/24      192.168.40.0/24
ACCEPT     all  --  192.168.40.0/24      192.168.50.0/24
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ROUTEUR:~#
```

2 + 3

1 + 4

On ne demande pas de bloquer les demandes SSH depuis le WAN, mais si jamais :
IPTABLES -A INPUT -p tcp --dport 22 -j DROP

2. GESTION DES POSTES DU LAN

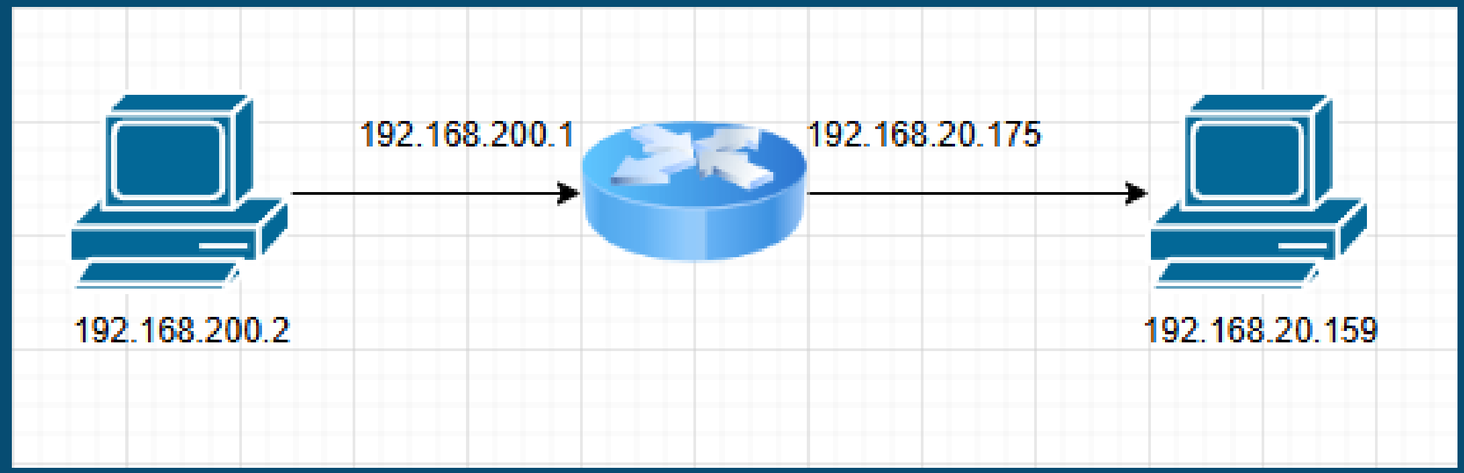
```
root@ROUTEUR:~# iptables-save
# Generated by iptables-save v1.8.9 (nf_tables) on Thu Mar 13 10:27:02 2025
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT ]5
-A FORWARD -s 192.168.50.0/24 -d 192.168.40.0/24 -p icmp -j ACCEPT
-A FORWARD -s 192.168.40.0/24 -d 192.168.50.0/24 -p icmp -j ACCEPT ]1
-A FORWARD -p icmp -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -s 192.168.40.0/24 -d 192.168.60.0/24 -j ACCEPT
-A FORWARD -s 192.168.60.0/24 -d 192.168.50.0/24 -j ACCEPT
-A FORWARD -s 192.168.50.0/24 -d 192.168.60.0/24 -j ACCEPT
-A FORWARD -s 192.168.50.0/24 -d 192.168.40.0/24 -j ACCEPT
-A FORWARD -s 192.168.40.0/24 -d 192.168.50.0/24 -j ACCEPT ]2
-A FORWARD -j LOG --log-prefix "PAQUET REJETÉ FORWARD : "
-A FORWARD -j REJECT --reject-with icmp-port-unreachable ]6
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT ]5
COMMIT
# Completed on Thu Mar 13 10:27:02 2025
# Generated by iptables-save v1.8.9 (nf_tables) on Thu Mar 13 10:27:02 2025
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 192.168.40.0/24 -o eth2 -j MASQUERADE ] 3
COMMIT
# Completed on Thu Mar 13 10:27:02 2025
```

4. Interdiction pose contable

IPTABLES -A FORWARD -M MAC --MAC-SOURCE LAMAC -O ETH2 -J REJECT

2. VÉRIFICATION AVEC WIRESHARK

Mon infra pour le test



2. VÉRIFICATION AVEC WIRESHARK

Résultat

	Time	Source	Destination
265	12.073570316	192.168.20.159	192.168.20.166
269	12.292635762	192.168.20.159	192.168.20.166
298	13.772972431	192.168.20.175	192.168.20.166
303	13.773322659	192.168.20.166	192.168.20.175
326	14.822391693	192.168.20.175	192.168.20.166
327	14.822427300	192.168.20.166	192.168.20.175

Je ping avec 192.168.200.2

et avec mon client, je trouve 192.168.20.175 (le routeur) qui ping 192.168.20.166 (mon client Wireshark