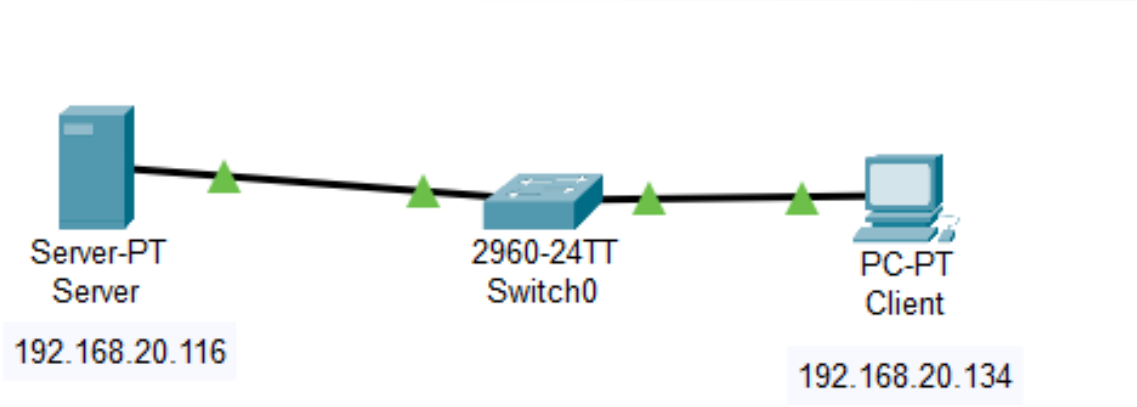
TP Iptables

Banse Viny

Présentation

- **Iptables** est un outil sous Linux permettant de filtrer le trafic réseau en définissant des règles. Il utilise des **chaînes** comme **INPUT** (trafic entrant), **FORWARD** (trafic redirigé) et **OUTPUT** (trafic sortant) pour décider si un paquet est accepté, rejeté ou bloqué. Il permet aussi la gestion du NAT et la modification des paquets, offrant un contrôle efficace sur la sécurité du réseau.

Schéma


Server-PT
Server
192.168.20.116
2960-24TT
Switch0
PC-PT
Client
192.168.20.134

Empêcher le ping du poste serveur sur le poste client

- iptables -A OUTPUT -d 192.168.20.116 -p icmp --icmp-type echo-request -j DROP
  - Cette commande iptables empêche la machine d'envoyer des requêtes ping vers l'adresse 192.168.20.116. Elle ajoute une règle à la chaîne OUTPUT (trafic sortant) pour bloquer les paquets ICMP echo-request, qui sont utilisés pour tester la connectivité avec la commande ping.

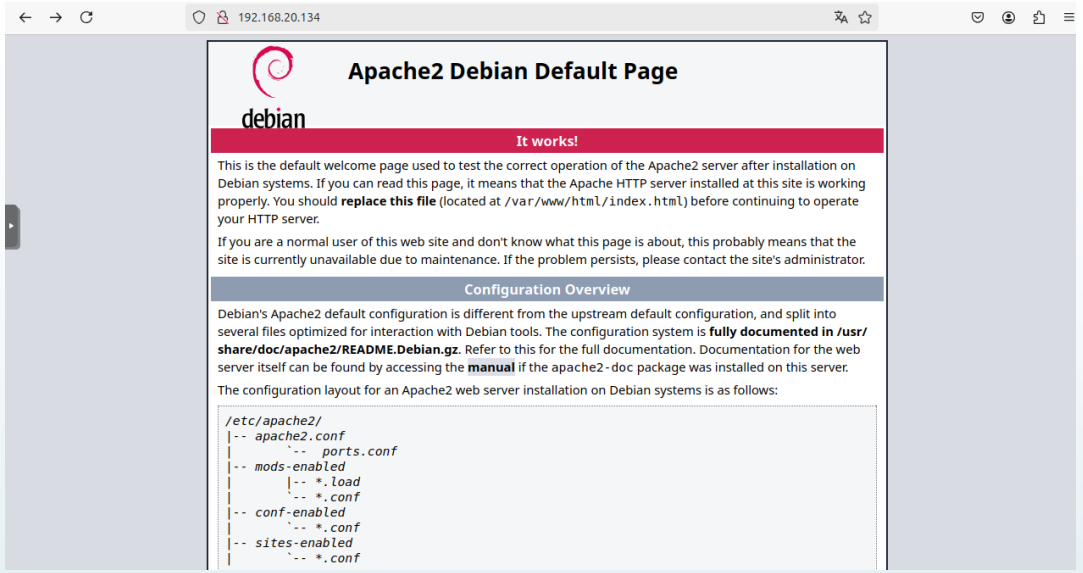
```
root@debian:~# ping 192.168.20.116
PING 192.168.20.116 (192.168.20.116) 56(84) bytes of data.
64 bytes from 192.168.20.116: icmp_seq=1 ttl=64 time=0.633 ms
64 bytes from 192.168.20.116: icmp_seq=2 ttl=64 time=0.738 ms
^C
--- 192.168.20.116 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.633/0.685/0.738/0.052 ms
root@debian:~# iptables -A OUTPUT -d 192.168.20.116 -p icmp --icmp-type echo-request -j DROP
root@debian:~# ping 192.168.20.116
PING 192.168.20.116 (192.168.20.116) 56(84) bytes of data.
^C
--- 192.168.20.116 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4080ms
```

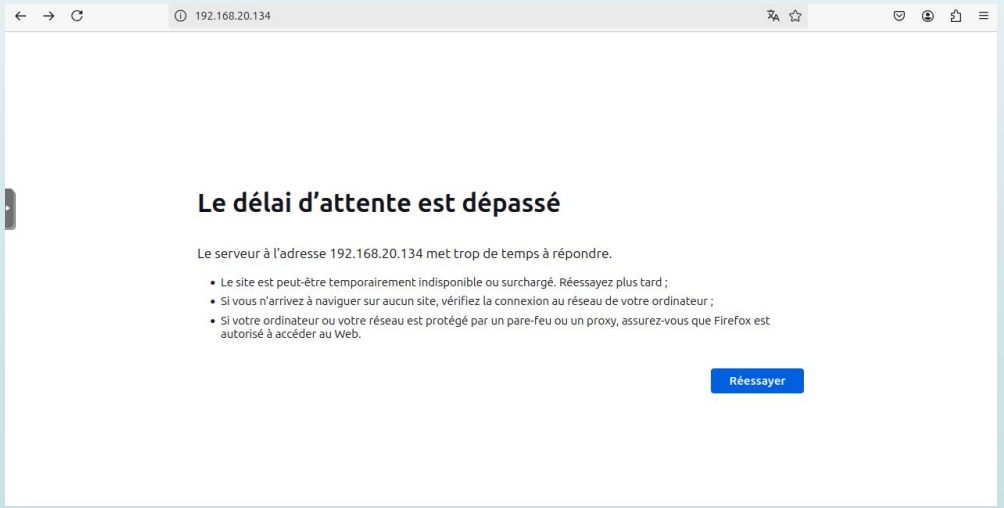
Empêcher l'accès à votre serveur web en http uniquement

- iptables -A INPUT -p tcp --dport 80 -j ACCEPT # Autoriser HTTP
- iptables -A INPUT -p tcp --dport 443 -j DROP # Bloquer HTTPS

Interdire l'accès à une addresse

- iptables -A INPUT -p tcp --dport 80 -s 192.168.20.116 -j DROP
  - Cette commande iptables bloque les connexions entrantes depuis l'adresse 192.168.20.116 vers le port 80 (HTTP). Elle ajoute une règle à la chaîne INPUT (trafic entrant) pour refuser les paquets TCP provenant de cette IP et destinés au port utilisé par les serveurs web.
- On voit ici que l'accès a bien été bloqué





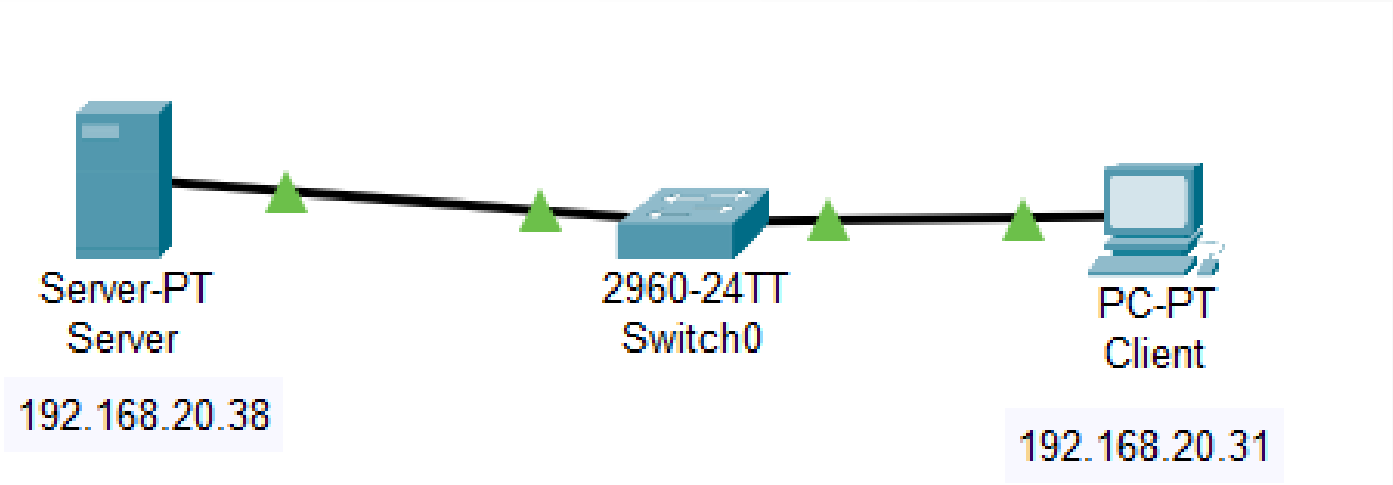
Refuser connexion telnet

- iptables -A INPUT -p tcp --dport 23 -j DROP
  - Cette commande iptables bloque toute connexion entrante sur le port 23, utilisé par le protocole Telnet. Elle ajoute une règle à la chaîne INPUT (trafic entrant) pour refuser les paquets TCP destinés à ce port. Cela empêche ainsi toute tentative de connexion Telnet vers la machine

```
sio@sio-Standard-PC-i440FX-PIIX-1996:~$ telnet 192.168.20.134
Trying 192.168.20.134...
telnet: Unable to connect to remote host: Connexion refusée
```

Ecrire les règles qui répondent aux demandes suivantes

- Il va ici falloir écrire des règles qui répondent aux demandes suivantes
  - Votre poste client ne peut que consulter votre serveur web
  - Le poste client de ne peut pas pinguer votre serveur
  - Le poste client ne peut pas être pingué
  - Votre serveur web est uniquement serveur web
  - Seules les connexions établies sont acceptées

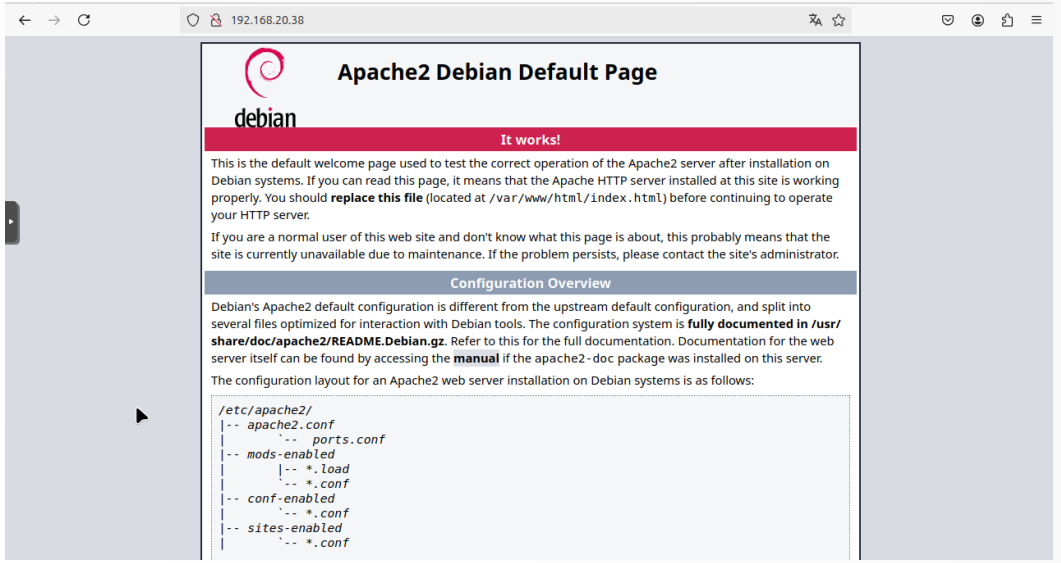


Ecrire les règles qui répondent aux demandes suivantes

- Votre poste client ne peut que consulter votre serveur web
  - iptables -A INPUT -p tcp --dport 80 -s 192.168.20.31 -j ACCEPT
  - iptables -A INPUT -s 192.168.20.31 -j DROP
    - La première règle autorise uniquement l'adresse 192.168.20.31 à accéder au port 80 (HTTP) du serveur.
    - La seconde règle bloque tout autre type de communication venant de 192.168.20.31.
- Le poste client de ne peut pas pinguer votre serveur
  - iptables -A INPUT -p icmp --icmp-type echo-request -s 192.168.20.31 -j DROP
    - Cette règle bloque les paquets ICMP echo-request (les requêtes de ping) provenant de 192.168.20.31.
- Le poste client ne peut pas être pingué
  - iptables -A OUTPUT -p icmp --icmp-type echo-reply -d 192.168.20.31 -j DROP
    - Cette règle empêche le serveur d'envoyer des réponses aux pings (echo-reply) vers 192.168.20.31.
- Votre serveur web est uniquement serveur web
  - iptables -P INPUT DROP
  - iptables -A INPUT -p tcp --dport 80 -j ACCEPT
  - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
    - La première règle bloque par défaut tout le trafic entrant (DROP).
    - La deuxième règle autorise uniquement le trafic web (HTTP, port 80).
    - La troisième règle permet les connexions déjà établies ou liées (exemple : les réponses aux requêtes HTTP).
- Seules les connexions établies sont acceptées
  - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
    - Cette règle autorise uniquement les connexions déjà établies ou liées à une connexion existante.

TEST

- On voit donc ici que le serveur web est accessible
- Le poste client ne peux pas pinguer le serveur
- Le poste client ne peux pas être pingué
- On voit ici avec le test de connexion ssh que le serveur est uniquement serveur web (le service ssh est installé sur le serveur)



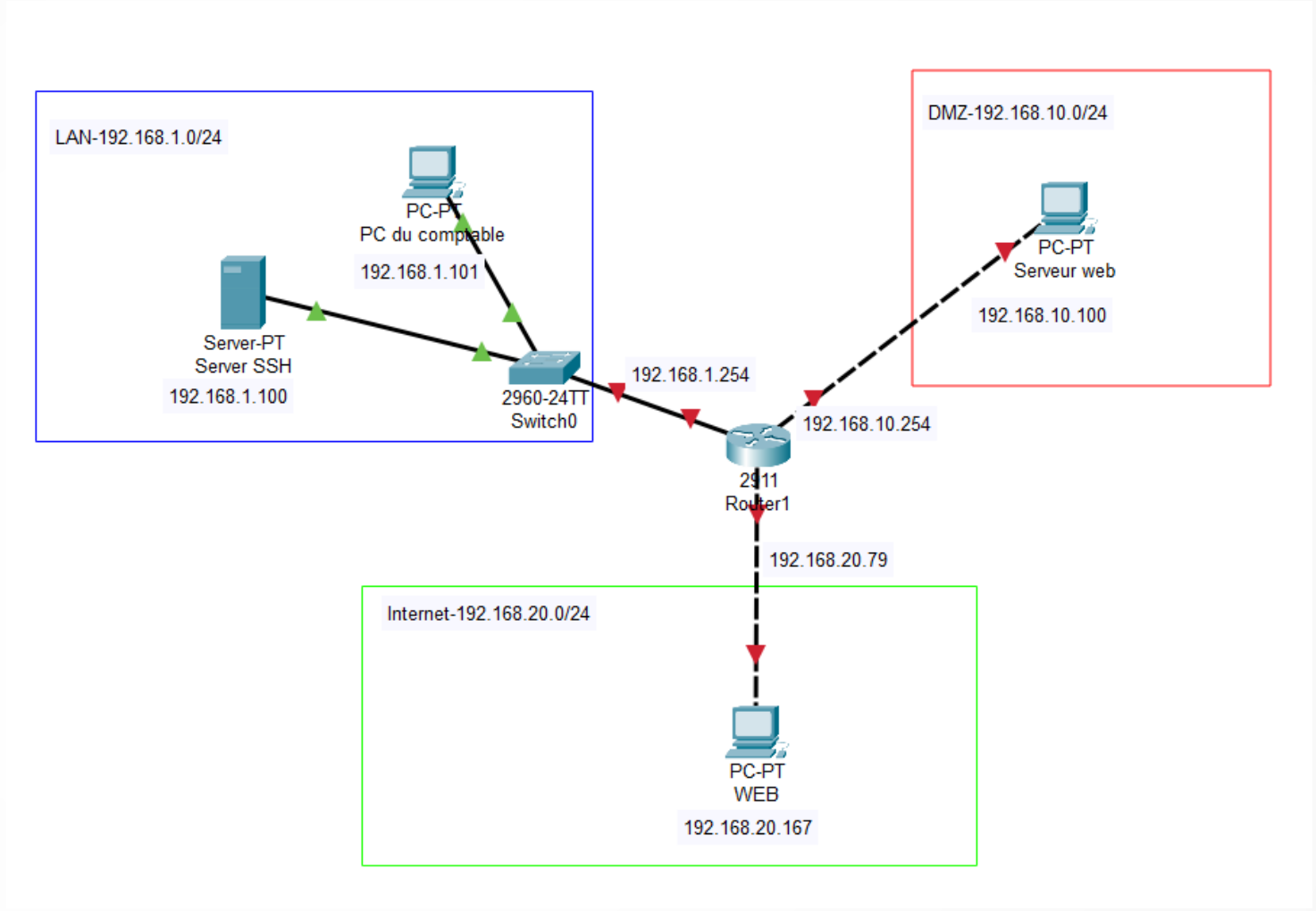

```
sio@sio-Standard-PC-i440FX-PIIX-1996:~$ ping 192.168.20.38
PING 192.168.20.38 (192.168.20.38) 56(84) bytes of data.
^C
--- 192.168.20.38 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4125ms
```

```
root@debian:~# ping 192.168.20.31
PING 192.168.20.31 (192.168.20.31) 56(84) bytes of data.
^C
--- 192.168.20.31 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2033ms
```

```
sio@sio-Standard-PC-i440FX-PIIX-1996:~$ ssh root@192.168.20.38
The authenticity of host '192.168.20.38 (192.168.20.38)' can't be established.
ED25519 key fingerprint is SHA256:zulgS/NUdlB12j7uyuWKN/1ZJQJNj3MGG5PEyihHkug.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? ^C
sio@sio-Standard-PC-i440FX-PIIX-1996:~$ ssh root@192.168.20.38
ssh: connect to host 192.168.20.38 port 22: Connection timed out
```

TP iptables partie 2

- Il va ici falloir configurer une mini infrastructures afin de mettre en place des restrictions pour la DMZ
  - Notre DMZ est accessible de partout donc d'internet et de notre réseau local
  - Pour éviter que nos serveurs soient victimes d'une attaque de DDOS le ping n'est pas autorisé depuis l'extérieur
  - Par contre pour vérifier la connectivité le ping depuis le LAN reste possible
  - Le serveur SSH peut se connecter aux postes de la DMZ

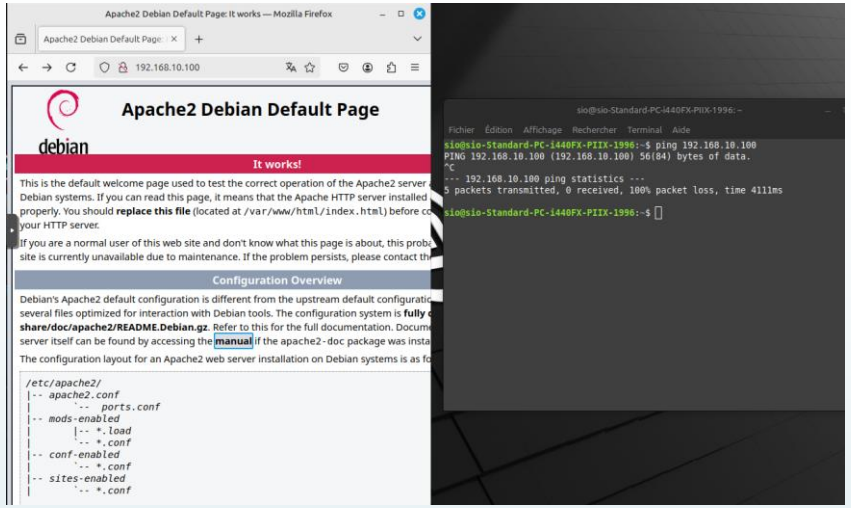


Gestion de la dmz

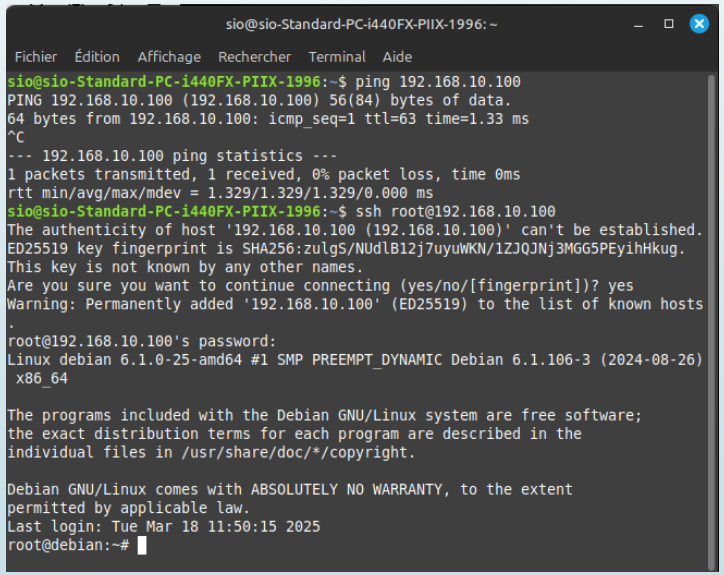
- Afin de répondre aux restrictions donné précédemment il va falloir utilizer les commandes suivantes
  - iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.10.0/24 -j ACCEPT
  - iptables -A FORWARD -s 192.168.10.0/24 -d 192.168.1.0/24 -j ACCEPT
  - iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.20.0/24 -j ACCEPT
  - iptables -A FORWARD -s 192.168.10.0/24 -d 192.168.20.0/24 -j ACCEPT
    - Ces commandes permettent au LAN de communiquer vers la DMZ et inversement et permettent au LAN et à la DMZ de communiquer jusqu'à internet mais pas inversement
- iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.10.0/24 -p tcp --dport 80 -j ACCEPT
- iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.10.0/24 -p tcp --dport 443 -j ACCEPT
    - Ces commandes permettent de d'autoiser uniquement l'accès web de la DMZ

Gestion de la DMZ

- Test depuis le web
  - On voit ici que depuis le web nous pouvons accéder au site web mais le ping est impossible



- Test depuis le LAN
  - On peux voir ici que le ping et la connexion ssh est possible



Gestion des postes du LAN

- Pour mettre en place la gestion du LAN il va falloir mettre en place des règles tel qu'ici
  - Autorisez le ping de tous les postes du réseau privé sur l'interface LAN du routeur
  - Autorisez le routage des paquets provenant du réseau privé vers la DMZ
  - camoufler les adresses Ip des postes du réseau privé qui vont sur internet (voir masquerade)
  - le poste du comptable ne peut pas aller sur internet : on travaillera avec l'@ MAC
  - on n'acceptera que les connexions établies
  - Les paquets rejetés seront enregistrés dans le journal /var/log/syslog/rejeter

Gestion des postes du LAN

- Autorisez le ping de tous les postes du réseau privé sur l'interface LAN du routeur
  - Par défaut le ping de tous les postes du LAN vers l'interface LAN du routeur est activé
- Autorisez le routage des paquets provenant du réseau privé vers la DMZ
  - iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.10.0/24 -j ACCEPT
- camoufler les adresses Ip des postes du réseau privé qui vont sur internet (voir masquerade)
  - iptables -t nat -A POSTROUTING -s 192.168.1.0/24 –o ens18 -j MASQUERADE
    - On voit sur le screen ici que sur la première partie l'ip du lan est visible et ensuite une fois la commande effectuée on ne voit que l'ip de la gateway

No.	Time	Source	Destination	Protocol
14	2.474755	192.168.1.100	192.168.20.230	ICMP
15	2.474987	192.168.20.230	192.168.1.100	ICMP
19	3.492667	192.168.1.100	192.168.20.230	ICMP
20	3.492948	192.168.20.230	192.168.1.100	ICMP
22	4.516759	192.168.1.100	192.168.20.230	ICMP
23	4.517025	192.168.20.230	192.168.1.100	ICMP
1288	331.845177	192.168.20.79	192.168.20.230	ICMP
1289	331.845449	192.168.20.230	192.168.20.79	ICMP
1295	332.869040	192.168.20.79	192.168.20.230	ICMP
1296	332.869325	192.168.20.230	192.168.20.79	ICMP

Gestion dus postes du LAN

- le poste du comptable ne peut pas aller sur internet : on travaillera avec l'@ MAC
  - iptables -A FORWARD -m mac --mac-source BC:24:11:36:CD:5E -d 192.168.20.79 -j DROP
- on n'acceptera que les connexions établies
  - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
- Les paquets rejetés seront enregistrés dans le journal /var/log/syslog/rejeter
  - iptables -A INPUT -j LOG --log-prefix "REJETER : " --log-level 4
  - iptables -A INPUT -j DROP