PRÉSENTÉ PAR DRUELLE NICOLAS

TP-IPTABLES

TP1 - DÉCOUVERTE

CAHIER DES CHARGES

-Ajout de la seconde interface

-Réalisation des règles client

-Accès au serveur WEB uniquement en http

-Interdire le ping vers le serveur

-Autoriser les connexion établies

-Réalisation des règles serveur

-Autoriser le serveur à répondre qu'au requête http

-Empêcher le ping vers le poste client

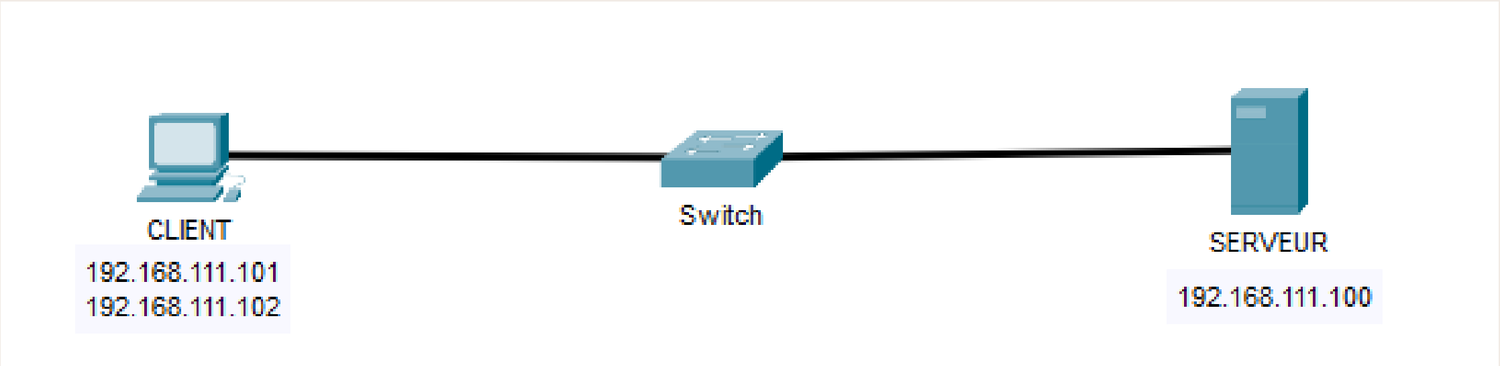
-Refuser les connections en telnet

-Bloquer l'accès au serveur à partir de la 2ème adresse ip du client

-Autoriser les connexion établies

-Réalisation des tests

TOPOLOGIE


CLIENT
192.168.111.101
192.168.111.102
Switch
SERVEUR
192.168.111.100

AJOUT DE LA SECONDE INTERFACE

AJOUT DE L'INTERFACE

```
allow-hotplug ens18
iface ens18 inet static
address 192.168.111.101/24
gateway 192.168.111.254

auto ens18:0
iface ens18:0 inet static
address 192.168.111.102/24
```

```
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:95:05:82 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.111.102/24 brd 192.168.111.255 scope global ens18:0
       valid_lft forever preferred_lft forever
    inet 192.168.111.101/24 brd 192.168.111.255 scope global secondary ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe95:582/64 scope link
       valid_lft forever preferred_lft forever
```

Sur la machine qui fera office de client on ajoute une sous interface dans le fichier “/etc/network/interfaces”

MISE EN PLACE DES RÈGLES CLIENTS

CONFIGURATION RÈGLES DU CLIENT

```
Vider les règles existantes
iptables -F
iptables -X
iptables -Z

Politique par défaut blocage intégrale
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

Autoriser le trafic sortant en http vers le serveur (port 80)
iptables -A OUTPUT -p tcp --dport 80 -d 192.168.111.100 -j ACCEPT
iptables -A INPUT -p tcp --sport 80 -s 192.168.111.100 -j ACCEPT

Interdire le ping vers de le serveur
iptables -A OUTPUT -p icmp --icmp-type echo-request -d 192.168.111.100 -j DROP

Empêcher le ping
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

Autoriser les connexions établies
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Vérification des règles
iptables -L -v -n
```

En suivant les demandes du cahier des charges, la topologie mise en place et les annexes.
J'ai mit en place les règles suivantes pour le poste client.

MISE EN PLACE DES RÈGLES SERVEUR

CONFIGURATION RÈGLES DU SERVEUR

```
Vider les règles existantes
iptables -F
iptables -X
iptables -Z

Politique par défaut tout bloquer
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

Autoriser le serveur à répondre qu'au requête HTTP
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

Bloquer l'accès du serveur à partir de la 2ème adresse du client
iptables -A INPUT -s 192.168.111.102 -j DROP

Bloquer le telnet (port 23)
iptables -A INPUT -p tcp --dport 23 -j DROP
iptables -A OUTPUT -p tcp --sport 23 -j DROP

Empêcher le ping serveur > client
iptables -A OUTPUT -p icmp --icmp-type echo-request -d 192.168.111.101 -j DROP

Autoriser les connexions établies
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Comme pour le poste client j'ai réalisé les règles en suivant le cahier des charges et la topologie en m'aidant des annexes.

RÉALISATION DES TESTS

PING

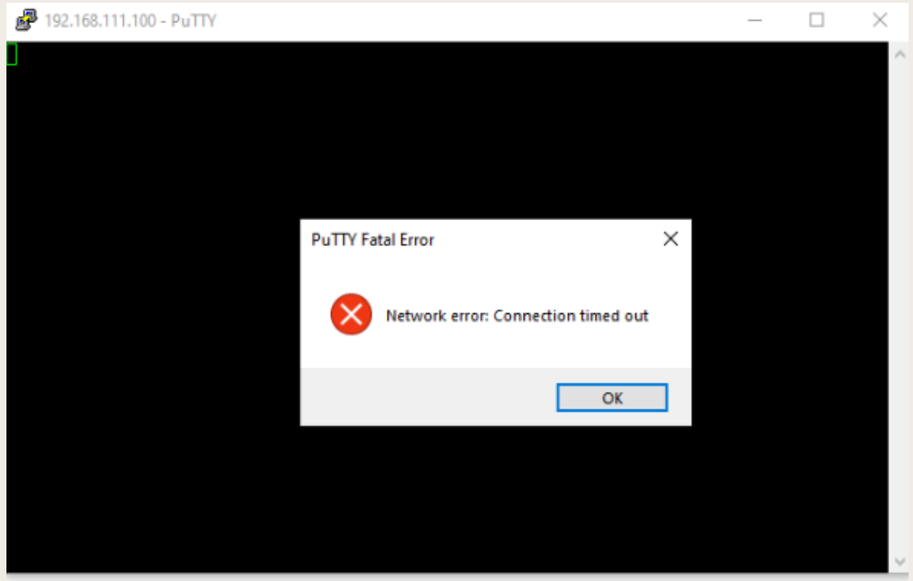
```
root@debian:~# ping -c 4 192.168.111.100
PING 192.168.111.100 (192.168.111.100) 56(84) bytes of data.
^C
--- 192.168.111.100 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3065ms
```

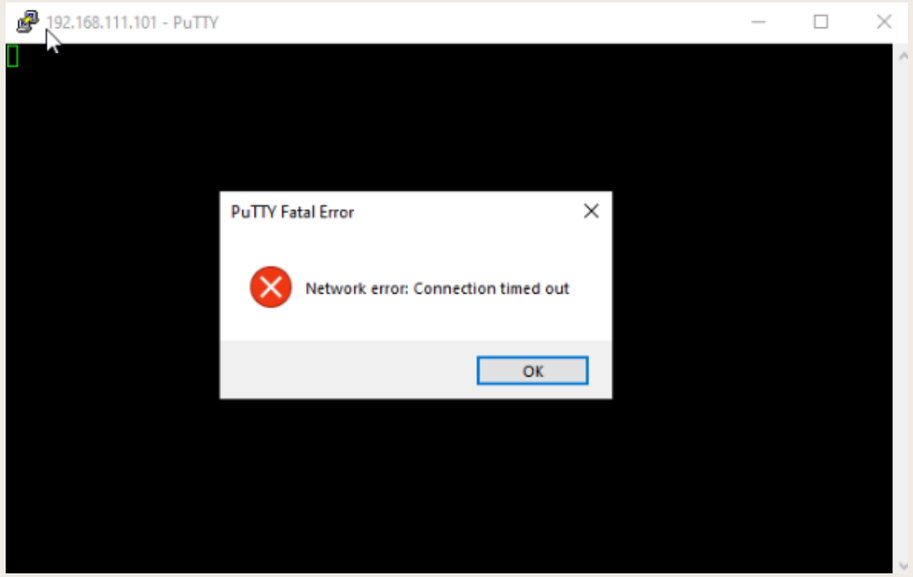
Client vers serveur

```
root@debian:~# ping -c 4 192.168.111.101
PING 192.168.111.101 (192.168.111.101) 56(84) bytes of data.
^C
--- 192.168.111.101 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3052ms
```

Serveur vers client

TELNET





On peut ici voir que la connexion en telnet vers le serveur ne fonctionne pas

TP2 - IPTABLES

CAHIER DES CHARGES

-Mise en place des règles

-Mise en place du trafic par défaut

-Autoriser les connexions établies

-Autoriser l’accès et le ping du LAN vers la DMZ

-Autoriser le LAN à ping l’interface LAN du routeur

-Autoriser le SSH du LAN vers la DMZ

-Autoriser tout le trafic vers la DMZ

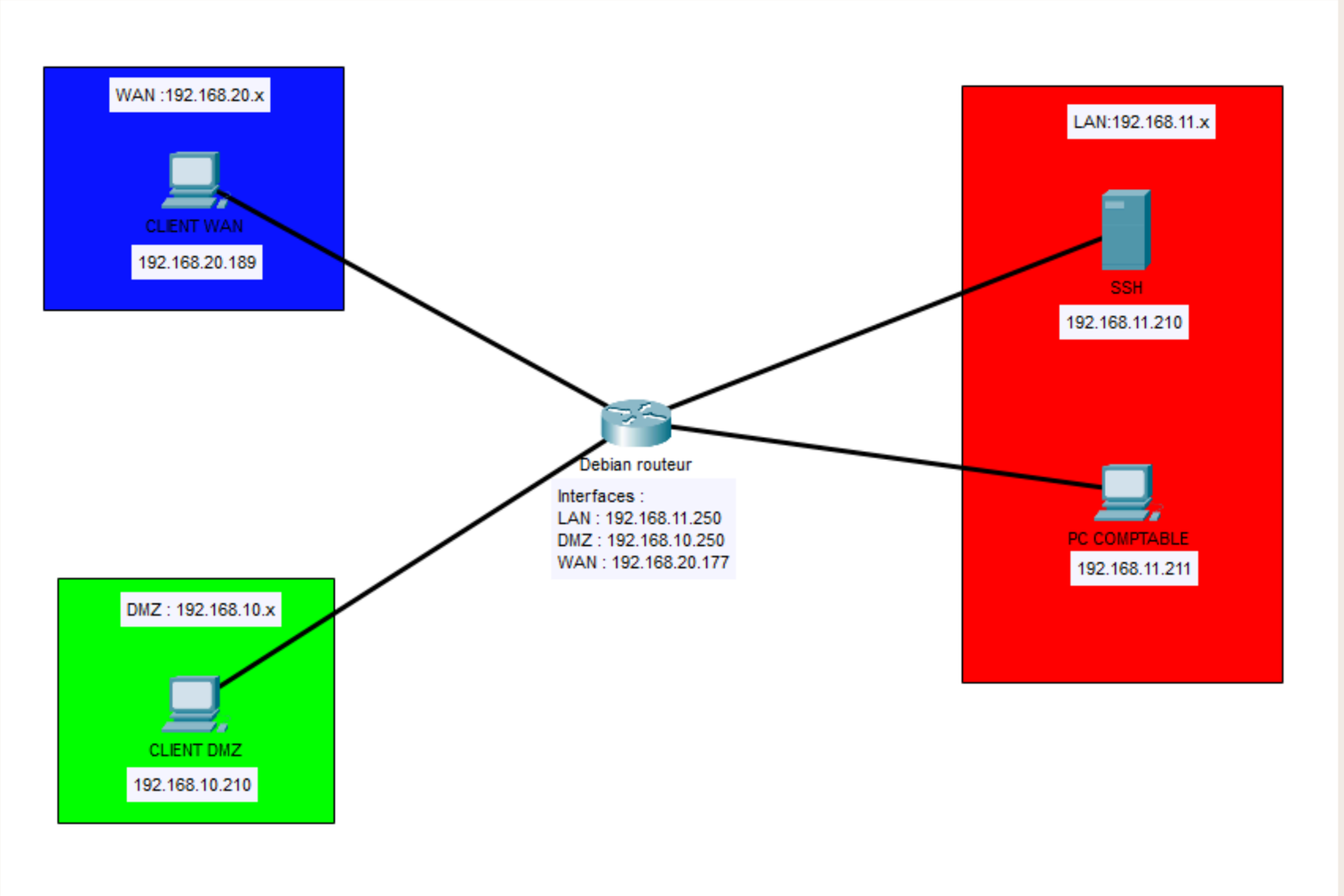
-Bloquer le ping du WAN vers la DMZ

-Configuration du NAT pour permettre un accès à internet

-Bloquer l’accès du poste comptable sur internet en utilisant l’adresse mac du poste

-Vérification

TOPOLOGIE


WAN :192.168.20.x
CLIENT WAN
192.168.20.189
LAN:192.168.11.x
SSH
192.168.11.210
Debian routeur
Interfaces :
LAN : 192.168.11.250
DMZ : 192.168.10.250
WAN : 192.168.20.177
PC COMPTABLE
192.168.11.211
DMZ : 192.168.10.x
CLIENT DMZ
192.168.10.210

MISE EN PLACE DES RÈGLES

RÈGLES

En suivant les annexes, le cahier des charges et la topologie je mets en place les règles suivante :

1.Réinitialisation des règles existantes

iptables -F

iptables -X

iptables -t nat -F

iptables -t nat -X

iptables -t mangle -F

iptables -t mangle -X

Supprime toutes les règles existantes pour partir d'une configuration propre.

2.Définition des politiques par défaut

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

INPUT DROP : Bloque tout le trafic entrant sauf règles explicites.

FORWARD DROP : Bloque le routage sauf règles autorisées.

OUTPUT ACCEPT : Autorise tout le trafic sortant.

3.Autoriser les connexions établies

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

Permet le retour des connexions initiées par des machines du LAN ou de la DMZ.

4.Règles spécifiques au LAN

Autoriser le LAN à accéder à la DMZ

iptables -A FORWARD -s 192.168.11.0/24 -d 192.168.10.0/24 -j ACCEPT

Autoriser le ping depuis le LAN vers la DMZ

iptables -A FORWARD -s 192.168.11.0/24 -d 192.168.10.0/24 -p icmp --icmp-type echo-request -j ACCEPT

Autoriser les postes du LAN à ping l'interface LAN du pare-feu

iptables -A INPUT -s 192.168.11.0/24 -d 192.168.11.250 -p icmp --icmp-type echo-request -j ACCEPT

Autoriser le serveur SSH du LAN à accéder aux machines de la DMZ

iptables -A FORWARD -s 192.168.11.210 -d 192.168.10.0/24 -j ACCEPT

5.Règles spécifiques à la DMZ

Autoriser tout le trafic vers la DMZ

iptables -A FORWARD -d 192.168.10.0/24 -j ACCEPT

Bloquer le ping WAN depuis la DMZ

iptables -A FORWARD -s 192.168.10.0/24 -d 192.168.20.0/24 -p icmp --icmp-type echo-request -j DROP

6.Configuration NAT pour l'accès Internet

Masquer les IPs du LAN pour aller sur Internet

iptables -t nat -A POSTROUTING -s 192.168.11.0/24 -o ens18 -j MASQUERADE

Assure que les machines du LAN peuvent sortir sur Internet via la WAN (ens18).

7.Bloquer l'accès Internet du poste comptable

Bloquer tout trafic du poste comptable

iptables -I FORWARD 1 -m mac --mac-source BC:24:11:A6:45:F0 -j DROP

Placée en première position pour s'assurer qu'aucune autre règle ne l'autorise avant.

8.Journalisation des paquets rejetés

iptables -A INPUT -j LOG --log-prefix "IPTables-Reject: " --log-level 4

iptables -A FORWARD -j LOG --log-prefix "IPTables-Reject: " --log-level 4

VÉRIFICATION

PING DMZ

```
root@debian:~# ping 192.168.10.210
PING 192.168.10.210 (192.168.10.210) 56(84) bytes of data.
64 bytes from 192.168.10.210: icmp_seq=1 ttl=63 time=2.68 ms
64 bytes from 192.168.10.210: icmp_seq=2 ttl=63 time=0.810 ms
64 bytes from 192.168.10.210: icmp_seq=3 ttl=63 time=0.805 ms
```

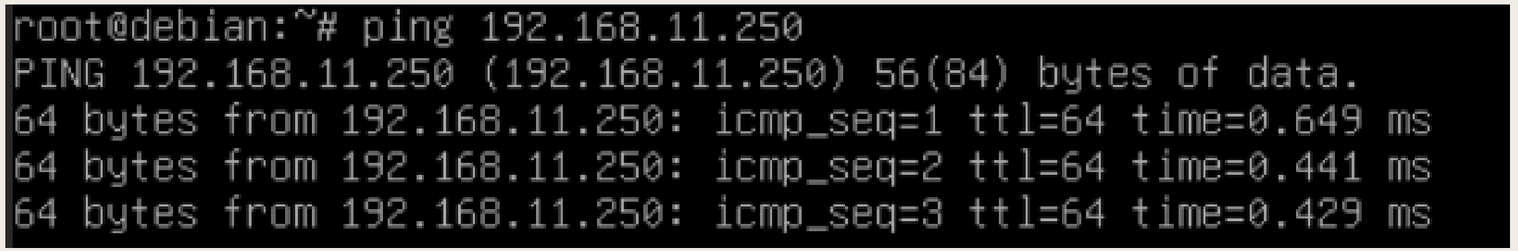
Le ping du LAN vers la DMZ est fonctionnel

TEST DDOS

```
root@debian:~# ping 192.168.20.177
PING 192.168.20.177 (192.168.20.177) 56(84) bytes of data.
```

On peut voir ici que le LAN ne peut pas ping vers l’extérieur

PING LAN -> ROUTEUR



Le ping vers l'interface LAN du routeur fonctionne et fait office de passerelle

TEST LAN SSH -> DMZ

```
root@debian:~# ping 192.168.10.210
PING 192.168.10.210 (192.168.10.210) 56(84) bytes of data.
64 bytes from 192.168.10.210: icmp_seq=1 ttl=63 time=4.36 ms
64 bytes from 192.168.10.210: icmp_seq=2 ttl=63 time=0.801 ms
64 bytes from 192.168.10.210: icmp_seq=3 ttl=63 time=0.870 ms
64 bytes from 192.168.10.210: icmp_seq=4 ttl=63 time=0.831 ms
64 bytes from 192.168.10.210: icmp_seq=5 ttl=63 time=0.811 ms
```

Le ping entre le serveur SSH et le poste de la DMZ est fonctionnel

On peut aussi se connecter en SSH sur celui-ci

```
root@debian:~# ssh user@192.168.10.210
user@192.168.10.210's password:
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar 23 00:22:42 2025 from 192.168.11.210
user@debian:~$
```

TEST ACCÈS INTERNET

```
root@debian:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=6.45 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=6.28 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=6.35 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=6.27 ms
```

On peut voir que le serveur SSH a accès à internet

Mais que le poste comptable lui n'y a pas accès

```
C:\Windows\system32>ping 8.8.8.8

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

TEST CONNEXION ÉTABLIS

```
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:24:11:56:aa:14 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.20.189/24 brd 192.168.20.255 scope global dynamic ens18
       valid_lft 7108sec preferred_lft 7108sec
    inet6 fe80::be24:11ff:fe56:aa14/64 scope link
       valid_lft forever preferred_lft forever
root@debian:~# ssh user@192.168.11.210
```

Pour vérifier les connexions établis j’essaie depuis l’extérieur de me connecter en SSH sur un poste du LAN. On peut ici voir que cela ne fonctionne pas

TEST WIRESHARK

```
root@debian:~# ping 192.168.20.82
PING 192.168.20.82 (192.168.20.82) 56(84) bytes of data.
```

629	161.035941	192.168.20.177	192.168.20.82	ICMP
633	162.059773	192.168.20.177	192.168.20.82	ICMP
638	163.083935	192.168.20.177	192.168.20.82	ICMP
653	164.107695	192.168.20.177	192.168.20.82	ICMP
659	165.132264	192.168.20.177	192.168.20.82	ICMP
661	166.155900	192.168.20.177	192.168.20.82	ICMP
664	167.180055	192.168.20.177	192.168.20.82	ICMP
669	168.203986	192.168.20.177	192.168.20.82	ICMP
672	169.227994	192.168.20.177	192.168.20.82	ICMP
674	170.252052	192.168.20.177	192.168.20.82	ICMP
679	171.275963	192.168.20.177	192.168.20.82	ICMP

On peut voir ici que lors que je capture une trame d’un ping du LAN vers le poste du WAN que la source prend l’adresse IP de la passerelle qui est l’interface WAN du routeur grâce à la règles NAT établis précédemment.

ANNEXES

Réinitialisation des règles existantes

iptables -F

iptables -X

iptables -t nat -F

iptables -t nat -X

iptables -t mangle -F

iptables -t mangle -X

Explication :

-F : Vide toutes les règles actuelles.

-X : Supprime toutes les chaînes personnalisées.

Les options -t nat et -t mangle signifient qu'on applique cela aux tables nat (pour le NAT) et mangle (pour modifications spécifiques des paquets).

Définition des politiques par défaut

iptables -P INPUT DROP/ACCEPT

iptables -P FORWARD DROP/ACCEPT

iptables -P OUTPUT DROP/ACCEPT

Explication :

INPUT DROP/ACCEPT : Bloque ou autorise tout trafic entrant par défaut.

FORWARD DROP/ACCEPT : Bloque ou autorise tout trafic routé par défaut.

OUTPUT DROP/ACCEPT : Bloque ou autorise tout trafic sortant.

Autoriser les connexions établies

iptables -A (INPUT/FORWARD/OUTPUT) -m state --state ESTABLISHED,RELATED -j ACCEPT

Explication :

ESTABLISHED : Connexion déjà établie (par exemple, une réponse à une requête qu'on a envoyée).

RELATED : Connexions liées (ex. : une session FTP active).

Autorisation spécifique :

-Autoriser un réseau (Lan par exemple) à accéder à un autre (exemple : DMZ ou Internet)

iptables -A FORWARD -s 192.168.1.0/24 -d 10.0.0.0/24 -j ACCEPT

Explication :

Source (-s) : Réseau local = 192.168.1.0/24

Destination (-d) : Autre réseau (par exemple, DMZ) = 10.0.0.0/24

Autorise les machines du LAN à communiquer avec l'autre réseau.

-Autoriser le ping (ICMP) depuis le LAN vers un autre réseau

iptables -A FORWARD -s 192.168.1.0/24 -d 10.0.0.0/24 -p icmp --icmp-type echo-request -j ACCEPT

Explication :

Permet aux machines du LAN de tester la connectivité (via ping) vers un autre réseau grâce au « -p » suivi du protocole ici icmp et du type d'icmp

-Autoriser les machines du LAN à ping le pare-feu lui-même

iptables -A INPUT -s 192.168.1.0/24 -p icmp --icmp-type echo-request -j ACCEPT

Autoriser un serveur du LAN à accéder à un service spécifique

iptables -A FORWARD -s 192.168.1.100 -d 10.0.0.50 -p tcp --dport 22 -j ACCEPT

Explication :

Autorise le serveur 192.168.1.100 à accéder au port SSH (22) d'une machine distante avec l'utilisation du « -p tcp » et du « --dport 22 » qui permet de renseigner le port.

Autoriser tout le trafic vers un réseau

iptables -A FORWARD -d 10.0.0.0/24 -j ACCEPT

Configuration NAT pour donner un accès Internet

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

Explication :

Source : Réseau LAN 192.168.1.0/24

Interface WAN : eth0/ens en fonction de l'interface utiliser

Le pare-feu remplace l'IP source par sa propre IP publique.

Bloquer un poste spécifique par IP ou mac

iptables -A FORWARD -s 192.168.1.50 -j DROP

Explication :
Bloque tout le trafic provenant de l'IP 192.168.1.50.

iptables -A FORWARD -m mac --mac-source AA:BB:CC:DD:EE:FF -j DROP

Explication :
Bloque une machine spécifique identifiée par son adresse MAC.