DM Filtrage

ROCHER
ALEXANDRE
SIO2

Plan adressage des machines : mot de passe routeur : root:root

Machine	Interface	Adresse ip	VLAN
CtlWin(Ext)	/	192.168.1.138	2
ArSrvWeb (DMZ)	/	192.168.38.10	38
CltWin7(Lan)	/	192.168.32.11	32
RouteurAlexandre	ens224	192.168.45.252	45
RouteurAlexandre	ens192	192.168.32.253	32
RouteurAlexandre	ens256	192.168.38.253	38

01.

Communication actuelle des machines.

Sens de communication : vertical à horizontale (bleu à vert)

Communication	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	✔	✔	✔
RouteurAlexandre	✔	✔	✔	✔	✔
ArSrvWeb (DMZ)	✔	✔	✔	✔	✔
CltWin7(Lan)	✔	✔	✔	✔	✔
Internet (Wan)	✔	✔	x	x	x

Internet ne peut pas communiquer avec certaines machines car il n'y pas de "PAT" vers toutes mes machines sur le routeur du BTS.

02. La question ne précisant pas de "Chaîne", j'ai donc définie la politique de "liste blanche" sur chaque chaîne (FORWARD,INPUT et OUTPUT)

a. iptables -P FORWARD DROP
b. iptables -P INPUT DROP
c. iptables -P OUTPUT DROP
    i. Avant d'exécuter ces commandes, je vais créer **2 règles** afin de toujours pouvoir configurer ma machine en SSH malgré la politique de liste blanche. (règles en à la question 3)

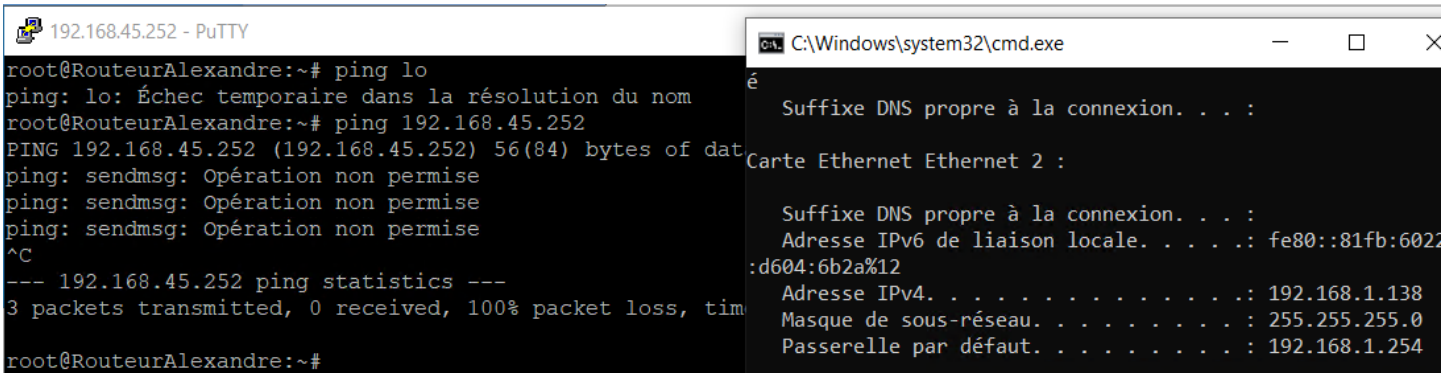
03.

En cas de perte de mon routeur sur le SSH, la seule solution est d'administrer mon routeur depuis **Vsphere** (interface de l'esx).

a. Pour résoudre le problème, il faudrait créer une règle pour **autoriser l'accès ssh sur une machine précise.**
b. **Règles** pour que la machine ("CtlWin(Ext)") qui me sert à configurer le routeur garde un accès ssh sur le routeur :
   i. iptables -I INPUT -s 192.168.1.138/32 -p tcp --dport 22 -j ACCEPT
   ii. iptables -I OUTPUT -d 192.168.1.138/32 -p tcp --sport 22 -j ACCEPT
      1. Je laisse "-I", sans argument, car de base cela insert en numéro 1 dans la table de filtrage, cela évite qu'une autre règle puisse bloquer cette règle.
c. Teste de la règles :

Sens de communication : vertical à horizontale (bleu à vert)

Communication SSH	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	x	x	✔	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	x	x
CltWin7(Lan)	x	x	x	x	x
Internet (Wan)	x	x	x	x	x



04.

Sauvegarde : iptables-save > /etc/filtrages.save
Restauration : iptables-restore < /etc/filtrages.save
Vérification de la validité : cat /etc/filtrages.save

05.

Objectif : le **réseau local** puisse accéder au **serveur web**

a. Réseau local : 192.168.32.0/24
b. Serveur web : 192.168.38.10/32

Règle du réseau local au serveur web avec explication :

- iptables : *base de la commande*
- -A : append : *ajouter à la table*
- -FORWARD : *affecte ce qui passe à travers le routeur*
- -s 192.168.32.0/24 : *Source du paquet*
- -d 192.168.38.10/32 : *Destination du paquet*
- -p tcp : *précise le protocole de couche 4*
- -m multiport : *permet d'autoriser plusieurs ports*
- --dport 80,443 : Règles qui concerne les ports web (http et https)
- -m state --state : NEW,RELATED,ESTABLISHED : Précise l'état tcp
- -j ACCEPT : *Fait accepter c'est paquets*

Règles brute :

- iptables -A FORWARD -s 192.168.32.0/24 -d 192.168.38.10/32 -p tcp -m multiport --dport 80,443 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

Il n'y a pas besoin de mettre le port dns car le serveur DNS ne sera dans le même réseau (du serveur web)

Etat tcp :

J'ai mis New, related et established car le réseau local à besoin d'accéder au serveur web (lancer la conversation et de continuer la conversation tcp avec le serveur web).

Règles du serveur web au réseau local :

- iptables -A FORWARD -s 192.168.38.10/32 -d 192.168.32.0/24 -p tcp -m multiport --sport 80,443 -m state --state RELATED,ESTABLISHED -j ACCEPT

Etat tcp :

Le serveur web n'a pas besoin d'avoir un accès au réseau local, je lui donne donc uniquement le droit de répondre au requête web du réseau local à l'aide de cette règle.

Table de filtrage actuelle : (“iptables -L”)

```
root@RouteurAlexandre:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.138        anywhere             tcp dpt:ssh

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.32.0/24      192.168.38.10        multiport dports
http,https state NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.38.10        192.168.32.0/24      multiport sports
http,https state RELATED,ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.1.138        tcp spt:ssh
```

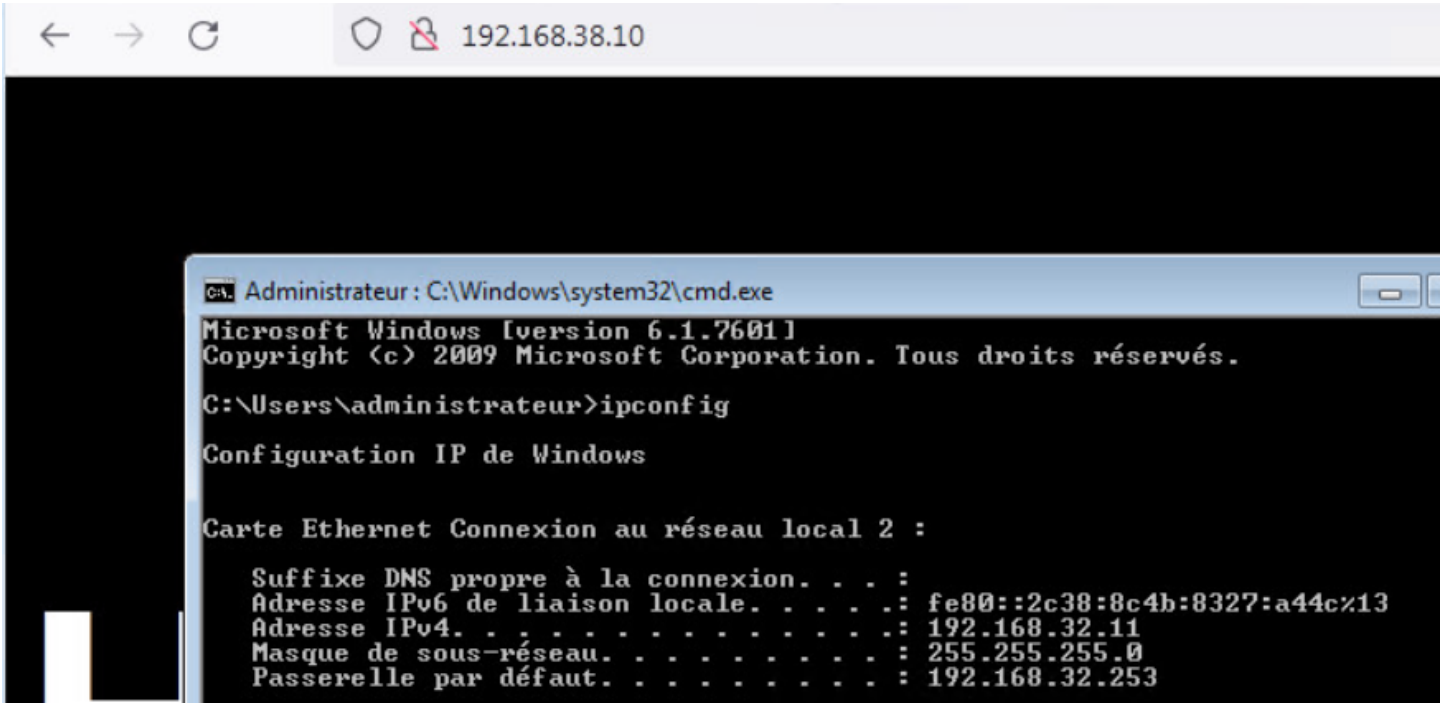
Tests :

Pour les tests, j’ai installé wampserver sur “CltWin7(Lan)” et mises en ligne le serveur (accès au page web wamp de l'extérieur).

Sens de communication : vertical à horizontale (bleu à vert)

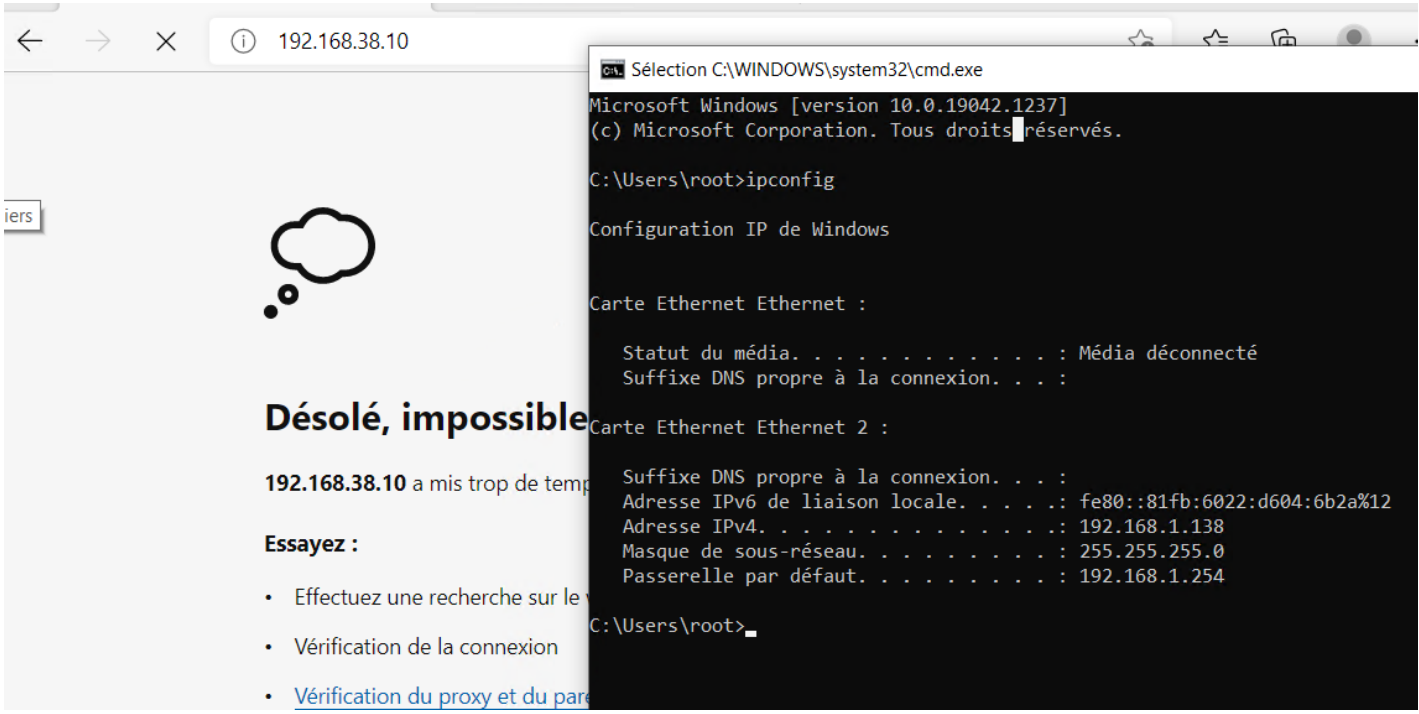
Accès page web.	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	x	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	✔	x
CltWin7(Lan)	x	x	x	✔	✔
Internet (Wan)	✔	x	x	x	x

De “CltWin7(Lan)” au serveur web



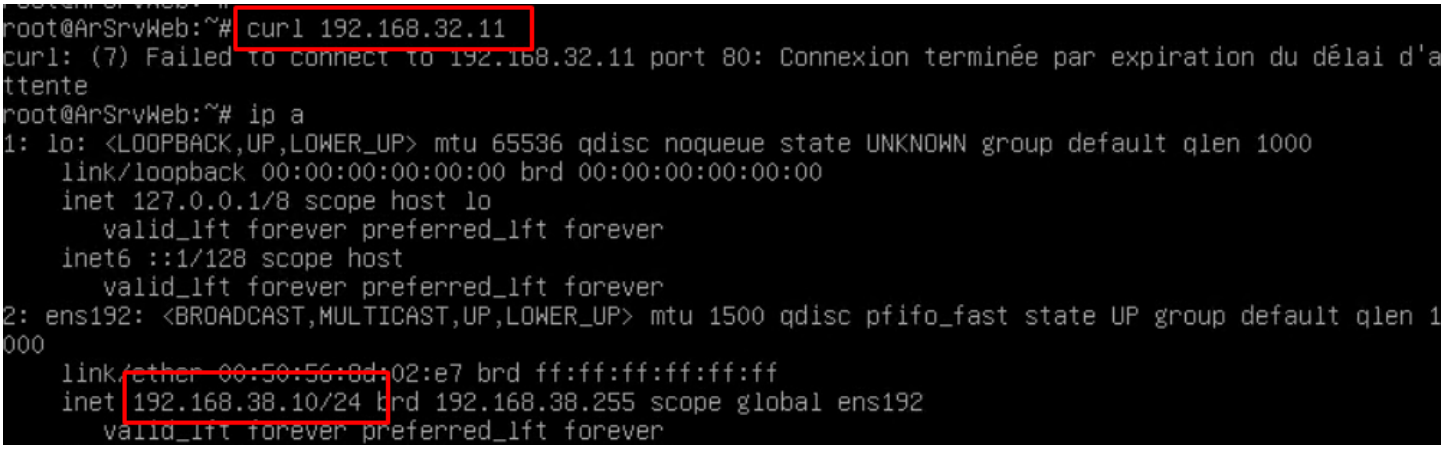
Le LAN à bien accès à la page web.

De “CtlWin(Ext)” au serveur web :



Comment prévu l'extérieure n’a pas accès à la page web

De ArSrvWeb(serveur web) à CltWin7(Lan) :



Comme prévu il n'y a que le réseau local qui peut à un accès .

Tests de non-régression :

Sens de communication : vertical à horizontale (bleu à vert)

Communication SSH	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	x	x	✔	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	x	x
CltWin7(Lan)	x	x	x	x	x
Internet (Wan)	x	x	x	x	x

06.

Objectif : que le **réseau local** puisse accéder à internet.

a. réseau local : 192.168.32.0/24
b. Internet : 0.0.0.0/0

Règles du réseau local à internet

- iptables -A FORWARD -s 192.168.32.0/24 -d 0.0.0.0/0 -p tcp -m multiport --sport 80,443 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 192.168.32.0/24 -d 0.0.0.0/0 -p udp --dport 53 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
    - Le protocole dns utilise “udp” et “tcp”

Règles d’internet au réseau local

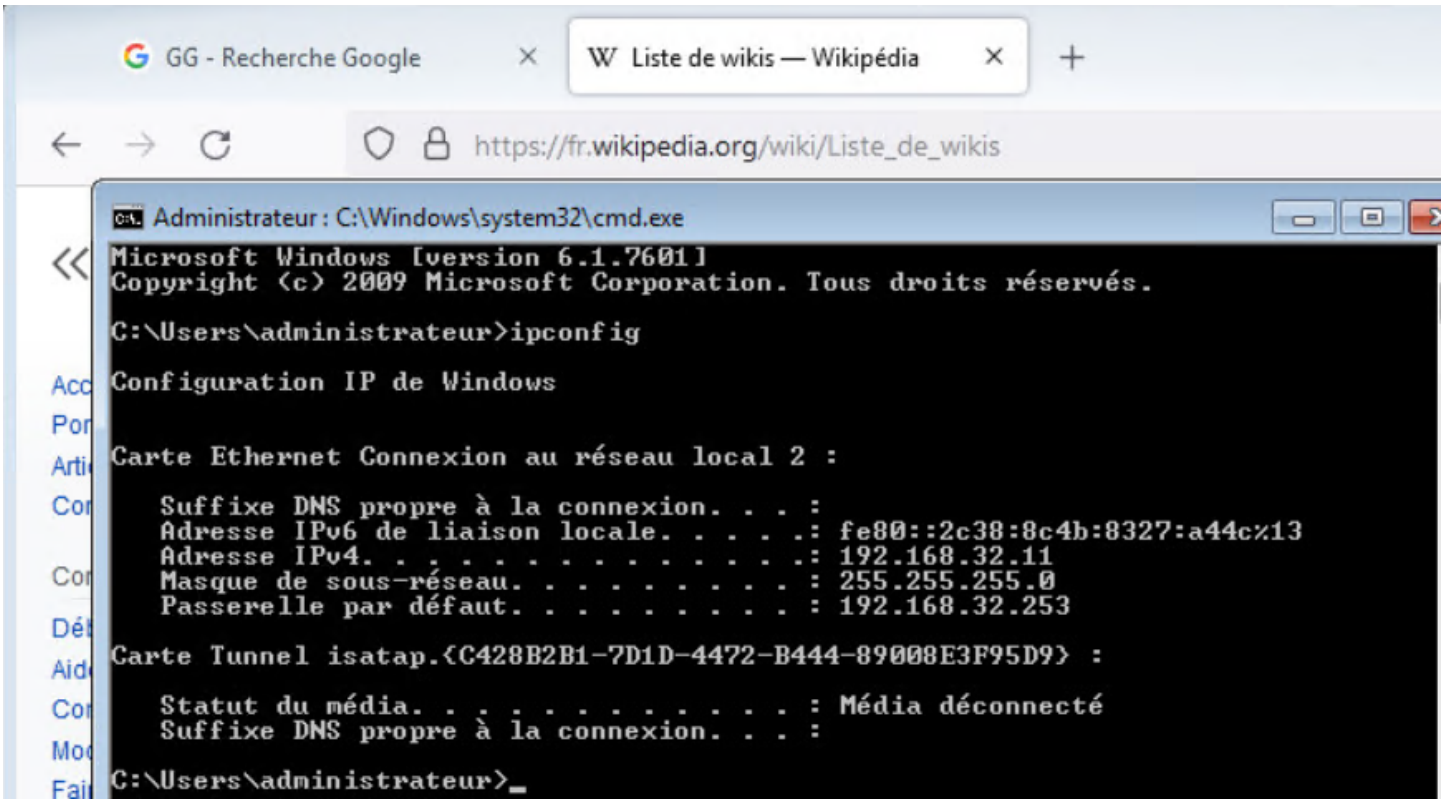
- iptables -A FORWARD -s 0.0.0.0/0 -d 192.168.32.0/24 -p tcp -m multiport --sport 80,443 -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 0.0.0.0/0 -d 192.168.32.0/24 -p udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT

Tests

Sens de communication : vertical à horizontale (bleu à vert)

Accès web	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	x	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	✔	x
CltWin7(Lan)	✔	x	x	✔	✔
Internet (Wan)	✔	x	x	x	x

Réseau local à internet :



Le réseau local à bien un accès à internet.

Réseau extérieur au réseau local :

Comme prévu, la communication n’est possible que d’un sens.

Tests de non-régression :

Sens de communication : vertical à horizontale (bleu à vert)

Communication SSH	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	x	x	✔	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	x	x
CltWin7(Lan)	x	x	x	x	x
Internet (Wan)	x	x	x	x	x

Sens de communication : vertical à horizontale (bleu à vert)

Accès web	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	x	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	✔	x
CltWin7(Lan)	✔	x	x	✔	✔
Internet (Wan)	✔	x	x	x	x

Iptables actuelle (iptables -L) :

```
root@RouteurAlexandre:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.138        anywhere             tcp dpt:ssh

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.32.0/24      192.168.38.10        multiport dports http,https state NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.38.10        192.168.32.0/24      multiport sports http,https state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             192.168.32.0/24      multiport sports domain,http,https state RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.32.0/24      anywhere             multiport dports domain,http,https state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  192.168.32.0/24      anywhere             multiport dports domain state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             192.168.32.0/24      multiport sports domain state RELATED,ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.1.138        tcp spt:ssh
```

07. Rendre accessible le **serveur web** depuis **l'extérieur**.

Afin de rendre accessible le serveur web depuis l'extérieur, j'ai dû laisser passer tous les paquets entre 0.0.0.0/0 et 192.168.38.10/32 sur les port web (80 et 443)

Pour plus de sécurité seul internet peut commencer la communication, le serveur web ne peux que y répondre.

Information machine :

Réseau extérieur : 0.0.0.0/0
Serveur web : 192.168.38.10/32

Règles brute :

- iptables -A FORWARD -s 0.0.0.0/0 -d 192.168.38.10/32 -p tcp -m multiport --dport 80,443 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 192.168.38.10/32 -d 0.0.0.0/0 -p tcp -m multiport --sport 80,42 -m state --state RELATED,ESTABLISHED -j ACCEPT

La règle que je viens de créer rend une autre règle inutile, donc je la supprime.

Tables de filtrage routeurAlexandre (FORWARD) :

Policy : DROP

N'	Action	Ip source	Port source	Ip destination	Port destination	Protocole	Etat TCP	Description
	A	192.168.32.0/24	*	192.168.38.10/32	80,443	tcp	NEW,RELATED, ESTABLISHED	Q5
	A	192.168.38.10/32	80,443	192.168.32.0/24	*	tcp	RELATED,ESTABLISHED	Q5
	A	192.168.32.0/24	*	0.0.0.0/0	80,443,53	tcp	NEW,RELATED, ESTABLISHED	Q6
	A	0.0.0.0/0	80,443,53	192.168.32.0/24	*	tcp	RELATED,ESTABLISHED	Q6
	A	192.168.32.0/24	*	0.0.0.0/0	53	udp	NEW,RELATED, ESTABLISHED	Q6
	A	0.0.0.0/0	53	192.168.32.0/24	*	udp	RELATED,ESTABLISHED	Q6
	A	0.0.0.0/0	*	192.168.38.10/32	80,443	tcp	NEW,RELATED,ESTABLISHED	Q7
	A	192.168.38.10/32	80,443	0.0.0.0/0	*	tcp	RELATED,ESTABLISHED	Q7

- iptables -L --line-numbers
- iptables -D FORWARD 1

Table de filtrage actuelle (iptables -L):

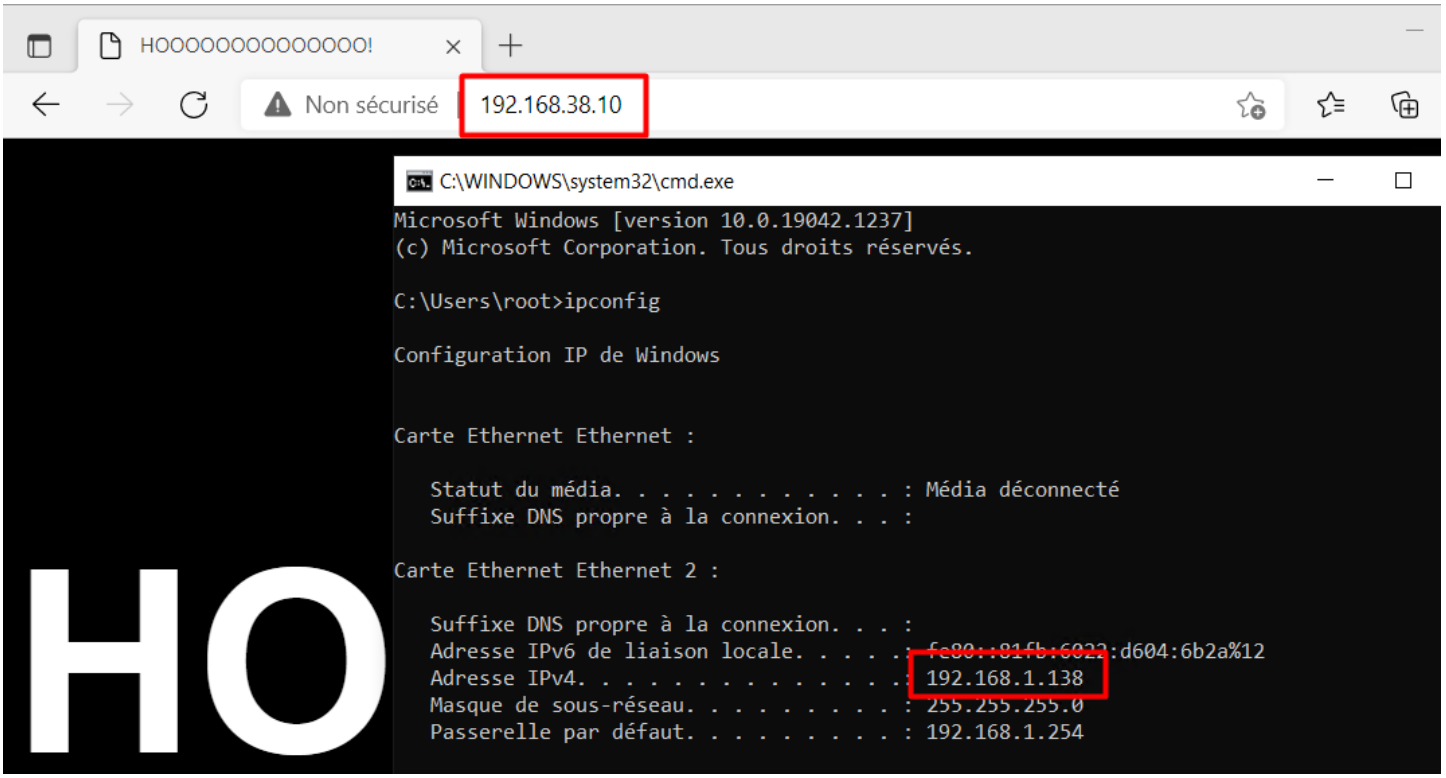
```
root@RouteurAlexandre:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.138        anywhere             tcp dpt:ssh

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.32.0/24      multiport sports domain,http,https state RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.32.0/24      anywhere             multiport dports domain,http,https state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  192.168.32.0/24      anywhere             multiport dports domain state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             192.168.32.0/24      multiport sports domain state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             192.168.38.10        multiport dports http,https state NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.38.10        anywhere             multiport sports http,nameserver state RELATED,ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.1.138        tcp spt:ssh
```

Tests :

Sens de communication : vertical à horizontale (bleu à vert)

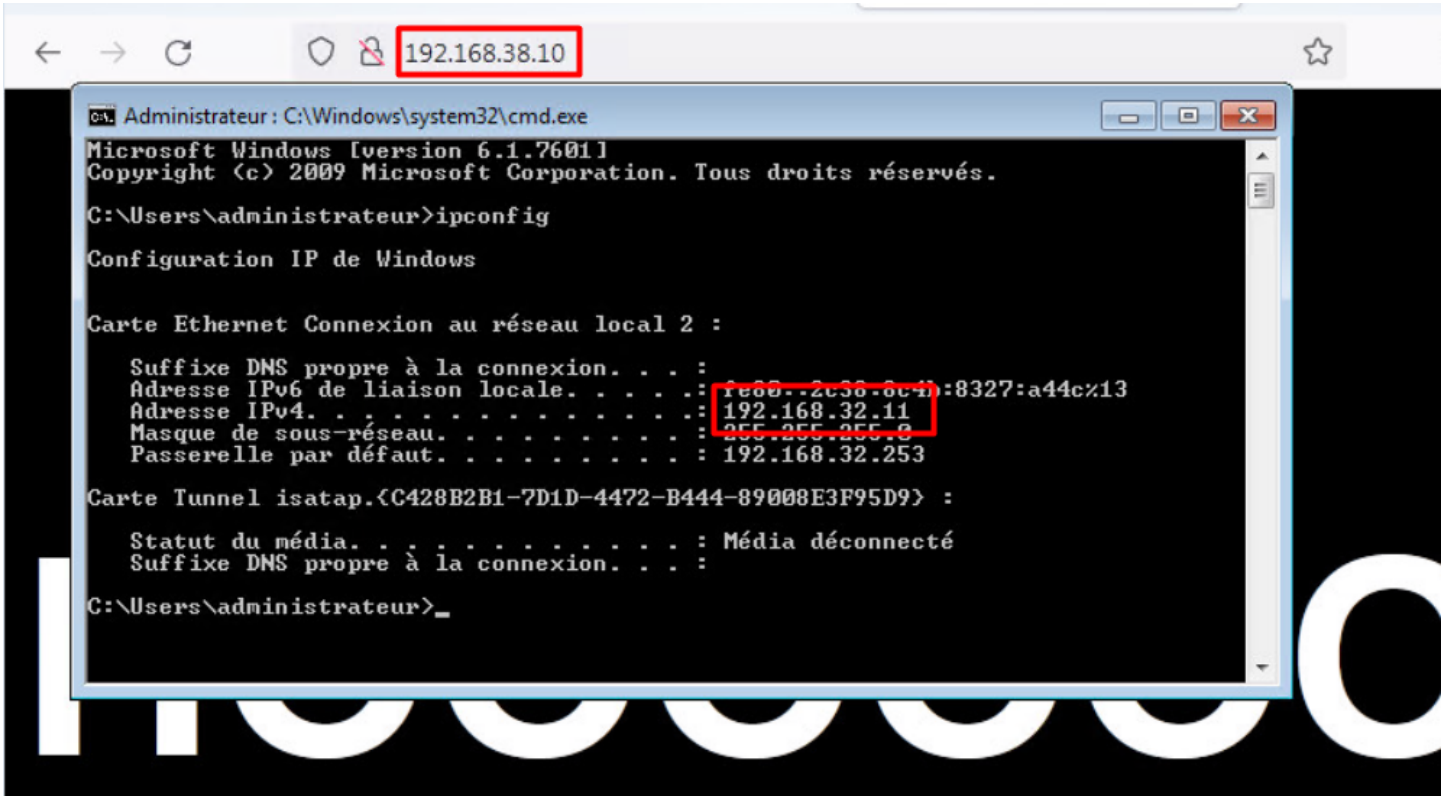
Accès web	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	x	✔	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	✔	x
CltWin7(Lan)	✔	x	x	✔	✔
Internet (Wan)	✔	x	x	x	x

Accès web du CltWin(Ext) au ArSrvWeb



Le réseau extérieur à bien accès au serveur web.

Accès web de CltWin7(Lan) au ArSrvWeb



Le réseau lan toujours bien accès au serveur web.

Tests de non-régression :

Sens de communication : vertical à horizontale (bleu à vert)

Communication SSH	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	x	x	✔	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	x	x
CltWin7(Lan)	x	x	x	x	x
Internet (Wan)	x	x	x	x	x

Sens de communication : vertical à horizontale (bleu à vert)

Accès web	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	x	✔	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	✔	x
CltWin7(Lan)	✔	x	x	✔	✔
Internet (Wan)	✔	x	x	x	x

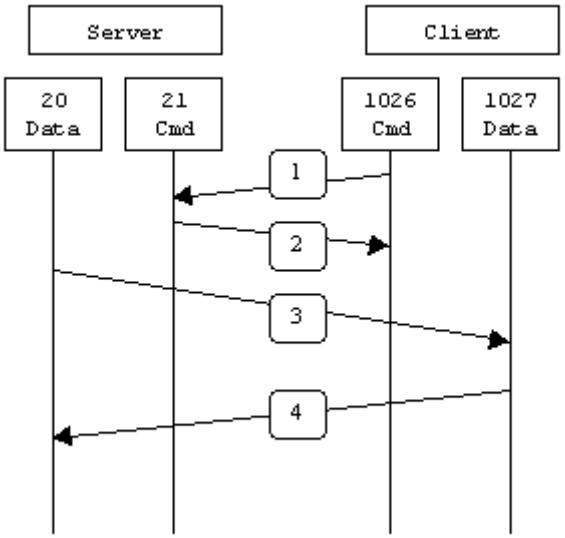
08. Accès **FTP** sur "**ArSrvWeb (DMZ)**" depuis réseau **lan** et un poste **exterieure**.

- machine ArSrvWeb : 192.168.38.10/32
- réseau lan : 192.168.32.0/24
- réseau extérieur : 192.168.1.0/24
    - machine extérieur : 192.168.1.138/32

J'ai installé proFTPD sur le serveur web pour avoir un accès ftp à distance.

Port à autoriser :

Le schéma de fonctionnement du ftp me fait comprendre qu'il faut les port 20,21 en source/destination



Le port 21 permet la connexion et l'envoi de commande.

Le port 20 data-ftp n'utilise pas d'authentification sur son port, il utilise celui du port 21. Le "--state NEW,RELATED,ESTABLISHED" n'est donc pas possible sur le port 20.

Règle brute :

Machine extérieure :

Machine extérieure au Serveur Web :

- iptables -A FORWARD -s 192.168.1.138/32 -d 192.168.38.10/32 -p tcp -m multiport --dport 21 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 192.168.1.138/32 -d 192.168.38.10/32 -p tcp -m multiport --dport 20 -j ACCEPT

Serveur Web à la Machine extérieure :

- iptables -A FORWARD -s 192.168.38.10/32 -d 192.168.1.138/32 -p tcp -m multiport --sport 21 -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 192.168.38.10/32 -d 192.168.1.138/32 -p tcp -m multiport --sport 20 -j ACCEPT

Réseau lan :

Machine extérieure au Serveur Web :

- iptables -A FORWARD -s 192.168.32.0/24 -d 192.168.38.10/32 -p tcp -m multiport --dport 21 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 192.168.32.0/24 -d 192.168.38.10/32 -p tcp -m multiport --dport 20 -j ACCEPT

Serveur Web à la Machine extérieure :

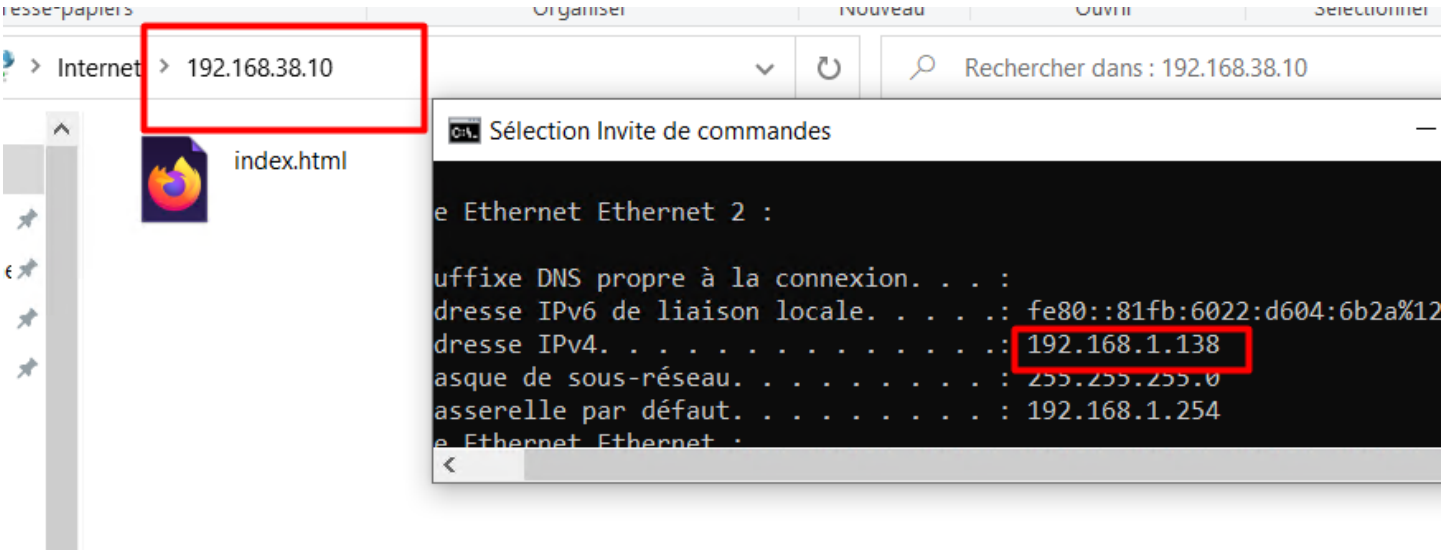
- iptables -A FORWARD -s 192.168.38.10/32 -d 192.168.32.0/24 -p tcp -m multiport --sport 21 -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 192.168.38.10/32 -d 192.168.32.0/24 -p tcp -m multiport --sport 20 -j ACCEPT

Tests :

Sens de communication : vertical à horizontale (bleu à vert)

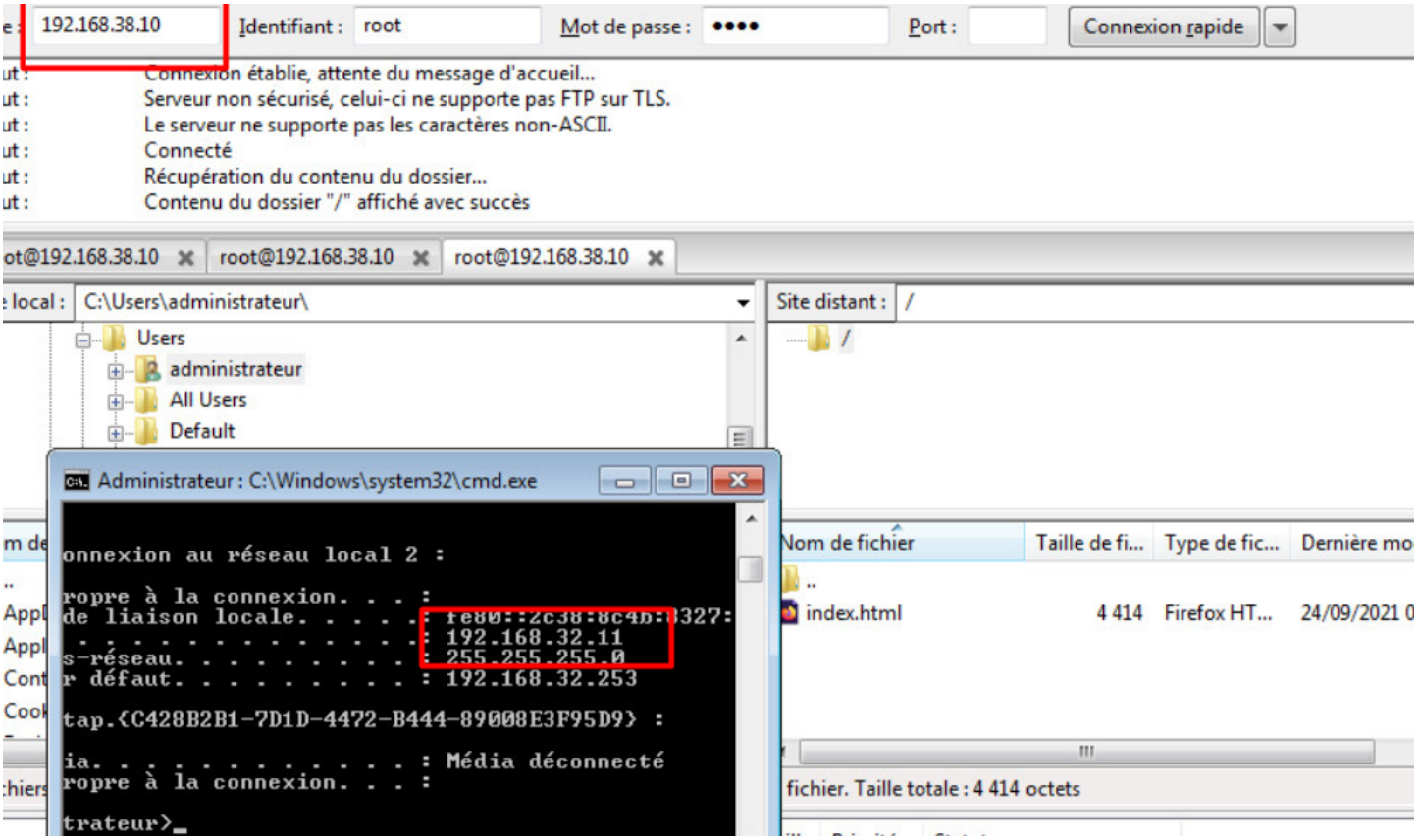
Accès FTP	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	x	x	x	✔	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	x	x
CltWin7(Lan)	x	x	x	✔	x
Internet (Wan)	x	x	x	x	x

Connexion FTP de CtlWin(Ext) à ArSrvWeb :



La connexion FTP entre la machine extérieure et le serveur Web est opérationnelle.

Connexion FTP de CltWin7(Lan) à ArSrvWeb :



La connexion FTP entre la machine locale Windows 7 et le serveur Web est opérationnelle.

Tests de non-régression :

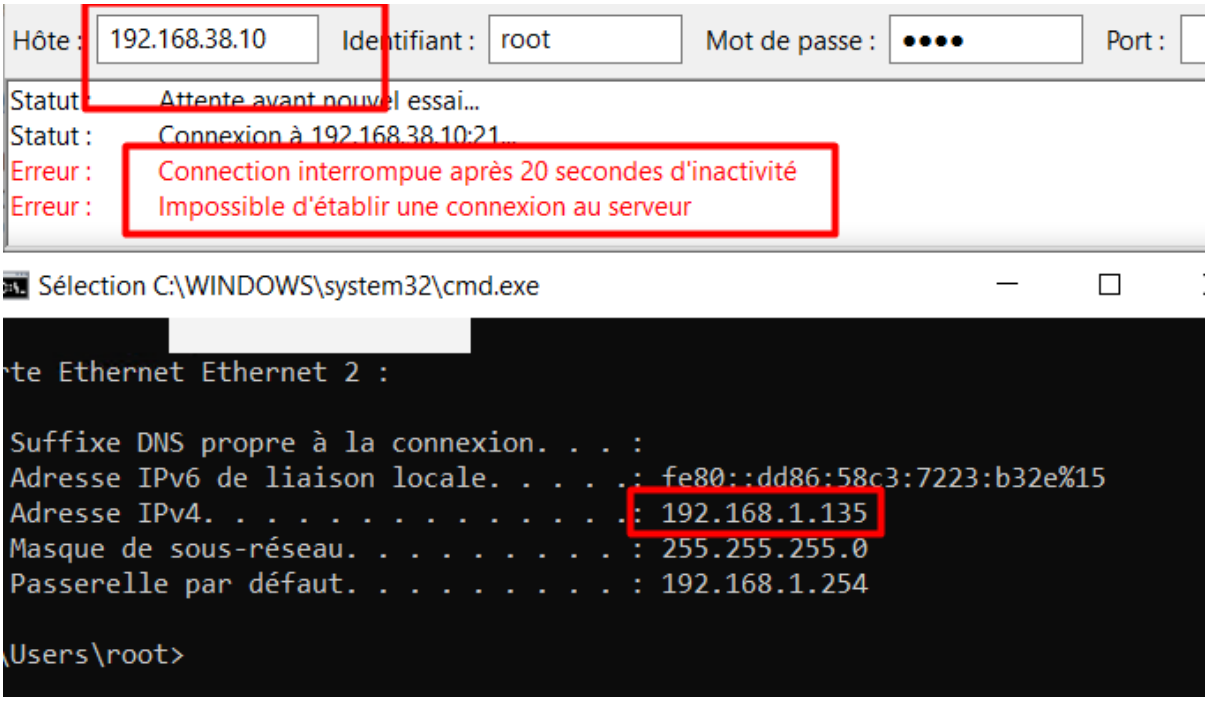
Sens de communication : vertical à horizontale (bleu à vert)

Communication SSH	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	x	x	✔	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	x	x
CltWin7(Lan)	x	x	x	x	x
Internet (Wan)	x	x	x	x	x

Sens de communication : vertical à horizontale (bleu à vert)

Accès web	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	x	✔	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	✔	x
CltWin7(Lan)	✔	x	x	✔	✔
Internet (Wan)	✔	x	x	x	x

Connexion FTP d'un client extérieure au ArSrvWeb :

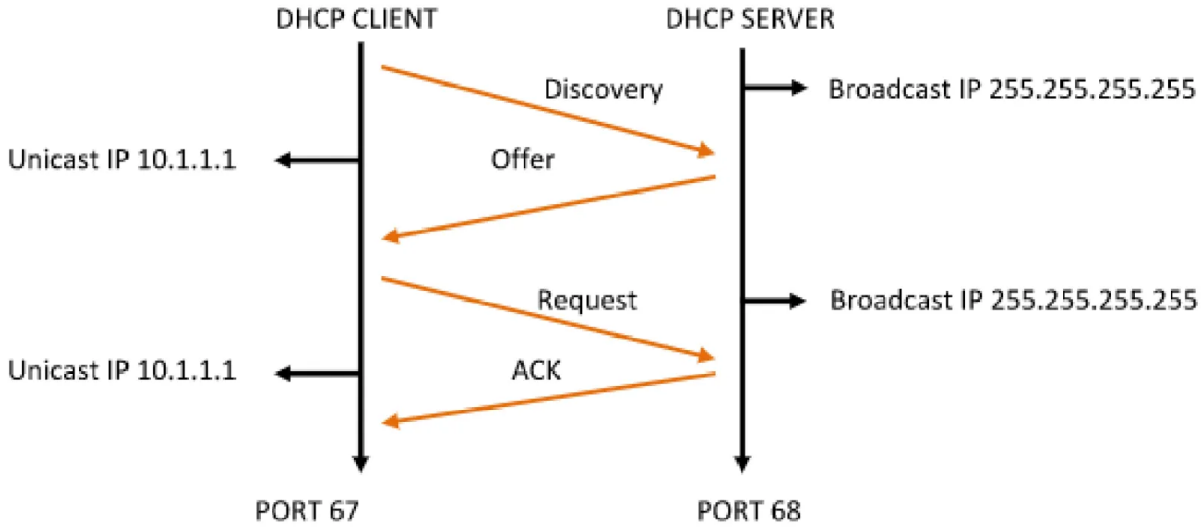


La connexion FTP entre la machine extérieure et le serveur Web n'est pas possible car la seule machine extérieure avec accès FTP est : 192.168.1.138.

09. Objectif : Mise en place d'un agent relais qui fonctionne avec le filtrage.

- Serveur DHCP : 192.168.44.10/32
- Réseau lan : 192.168.32.0/24

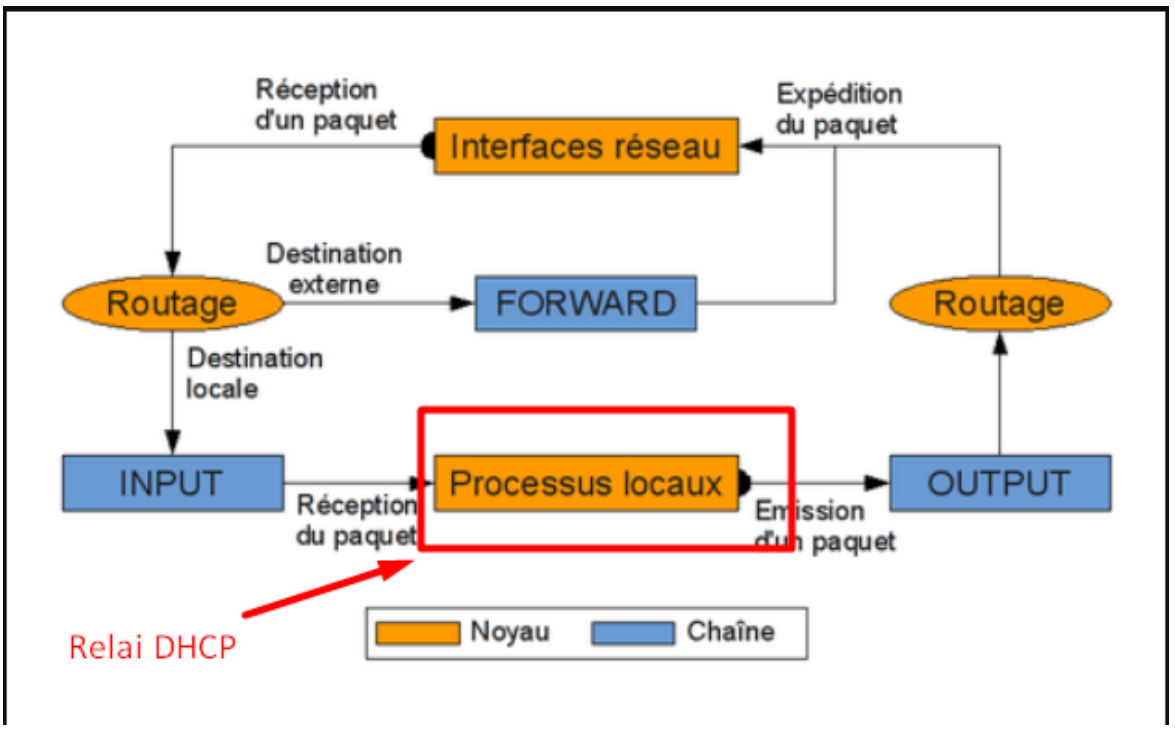
Fonctionnement du DHCP :



Port DHCP :

Client : 68
Serveur : 67

J'ai ouvert les ports "INPUT" et "OUTPUT", car le relay DHCP est dans le routeur (Processus local).



Règles bute :

- iptables -A INPUT -i ens192 -p udp -m multiport --dport 67,68 -j ACCEPT
- iptables -A OUTPUT -o ens192 -p udp -m multiport --dport 67,68 -j ACCEPT
- iptables -A INPUT -i ens224 -p udp -m multiport --dport 67,68 -j ACCEPT
- iptables -A OUTPUT -o ens224 -p udp -m multiport --dport 67,68 -j ACCEPT

Tests :

DCHP Sur la Machine de test “Debian2”, mise sur le Vlan32 :

```
root@debian:~# dhclient -r
Killed old client process
^[[Aroot@debian:~# dhclient
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
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 00:50:56:8d:67:5e brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.21/24 brd 192.168.32.255 scope global dynamic ens192
       valid_lft 86399sec preferred_lft 86399sec
    inet6 fe80::250:56ff:fe8d:675e/64 scope link
       valid_lft forever preferred_lft forever
```

```
# The primary network interface
allow-hotplug ens192
iface ens192 inet dhcp
```

Ouvrir les ports à bien permis à faire passer les paquets du DHCP sur le vlan 32 car la règle autorise l’interface ens192

DCHP Sur la Machine de test “Debian2”, mise sur le Vlan38 :

```
       valid_lft forever preferred_lft forever
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
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 00:50:56:8d:67:5e brd ff:ff:ff:ff:ff:ff
    inet6 fe80::250:56ff:fe8d:675e/64 scope link
       valid_lft forever preferred_lft forever
root@debian:~# dhclient
```

Ouvrir les ports n’a pas permis de faire passer les paquets du DHCP sur le vlan 38 car la règle n’autorise pas l’interface ens256 (interface mise sur le vlan38)

Tests	Fonctionnement DCHP de 192.168.44.10
Internet (Wan)	x
CtlWin(Ext)	x
RouteurAlexandre	x
ArSrvWeb (DMZ)	x
CltWin7(Lan)	x
Debian2(Vlan38)	x
Debian2(Vlan32)	✔

Tests de non-régression :

Sens de communication : vertical à horizontale (bleu à vert)

Communication SSH	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	x	x	✔	x	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	x	x
CltWin7(Lan)	x	x	x	x	x
Internet (Wan)	x	x	x	x	x

Sens de communication : vertical à horizontale (bleu à vert)

Accès web	Internet (Wan)	CtlWin(Ext)	RouteurAlexandre	ArSrvWeb (DMZ)	CltWin7(Lan)
CtlWin(Ext)	✔	✔	x	✔	x
RouteurAlexandre	x	x	x	x	x
ArSrvWeb (DMZ)	x	x	x	✔	x
CltWin7(Lan)	✔	x	x	✔	✔
Internet (Wan)	✔	x	x	x	x

Tables de filtrage actuelle : “Iptables -L” :

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.138        anywhere             tcp dpt:ssh
ACCEPT     udp  --  anywhere             anywhere             multiport dports b
ootps,bootpc
ACCEPT     tcp  --  192.168.44.10        anywhere             tcp dpt:68
ACCEPT     udp  --  anywhere             anywhere             multiport dports b
ootps,bootpc
ACCEPT     udp  --  anywhere             anywhere             multiport dports b
ootps,bootpc

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.32.0/24      multiport sports d
omain,http,https state RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.32.0/24      anywhere             multiport dports d
omain,http,https state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  192.168.32.0/24      anywhere             multiport dports d
omain state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             192.168.32.0/24      multiport sports d
omain state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             192.168.38.10        multiport dports h
ttp,https state NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.38.10        anywhere             multiport sports h
ttp,nameserver state RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.1.138        192.168.38.10        multiport dports f
tp state NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.1.138        192.168.38.10        multiport dports f
tp-data
ACCEPT     tcp  --  192.168.38.10        192.168.1.138        multiport sports f
tp state RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.38.10        192.168.1.138        multiport sports f
tp-data
ACCEPT     tcp  --  192.168.32.0/24      192.168.38.10        multiport dports f
tp state NEW,RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.32.0/24      192.168.38.10        multiport dports f
tp-data
ACCEPT     tcp  --  192.168.38.10        192.168.32.0/24      multiport sports f
tp state RELATED,ESTABLISHED
```

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.138        anywhere             tcp dpt:ssh
ACCEPT     udp  --  anywhere             anywhere             multiport dports b
ootps,bootpc
ACCEPT     tcp  --  192.168.44.10        anywhere             tcp dpt:68
ACCEPT     udp  --  anywhere             anywhere             multiport dports b
ootps,bootpc
ACCEPT     udp  --  anywhere             anywhere             multiport dports b
ootps,bootpc
```

10. Comment supprime-ton des règles ?

iptables -D OUTPUT 5

“OUTPUT” est la chaîne

“5” est le numéro de la règle que l'on veut supprimer

Le serveur web peut-il faire les mises à jour de son OS ?

Le serveur web n’a pas d’accès à internet, il ne peut donc pas faire les mise à jours de l’OS

Est-il possible de pinger le routeur ?

Non il n’est pas possible de pinger le routeur à cause de la politique de “liste blanche”.

Quels outils vous permettent de faciliter la tâche de gestion des règles de filtrage ?

Une interface web me permet de faciliter la tâche sur la gestion des règles de filtrage, par exemple “pfsense” pourrait faciliter la tâche de gestion.

Tables de filtrage routeurAlexandre (FORWARD) :

Policy : DROP

N’	Action	Ip source	Port source	Ip destination	Port destination	Protocole	Etat TCP	Description
	A	192.168.32.0/24	*	0.0.0.0/0	80,443,53	tcp	NEW,RELATED, ESTABLISHED	Q6
	A	0.0.0.0/0	80,443,53	192.168.32.0/24	*	tcp	RELATED,ESTABLISHED	Q6
	A	192.168.32.0/24	*	0.0.0.0/0	53	udp	NEW,RELATED, ESTABLISHED	Q6
	A	0.0.0.0/0	53	192.168.32.0/24	*	udp	RELATED,ESTABLISHED	Q6
	A	0.0.0.0/0	*	192.168.38.10/32	80,443	tcp	NEW,RELATED,ESTABLISHED	Q5 et Q7
	A	192.168.38.10/32	80,443	0.0.0.0/0	*	tcp	RELATED,ESTABLISHED	Q5 et Q7
	A	192.168.1.138/32	*	192.168.38.10/32	21	tcp	NEW,RELATED,ESTABLISHED	Q8
	A	192.168.38.10/32	21	192.168.1.138/32	*	tcp	RELATED,ESTABLISHED	Q8
	A	192.168.1.138/32	*	192.168.38.10/32	20	tcp		Q8
	A	192.168.38.10/32	20	192.168.1.138/32	*	tcp		Q8
	A	192.168.32.0/24	*	192.168.38.10/32	21	tcp	NEW,RELATED,ESTABLISHED	Q8
	A	192.168.38.10/32	21	192.168.32.0/24	*	tcp	RELATED,ESTABLISHED	Q8
	A	192.168.32.0/24	*	192.168.38.10/32	20	tcp		Q8
	A	192.168.38.10/32	20	192.168.32.0/24	*	tcp		Q8

Tables de filtrage routeurAlexandre (OUTPUT) :

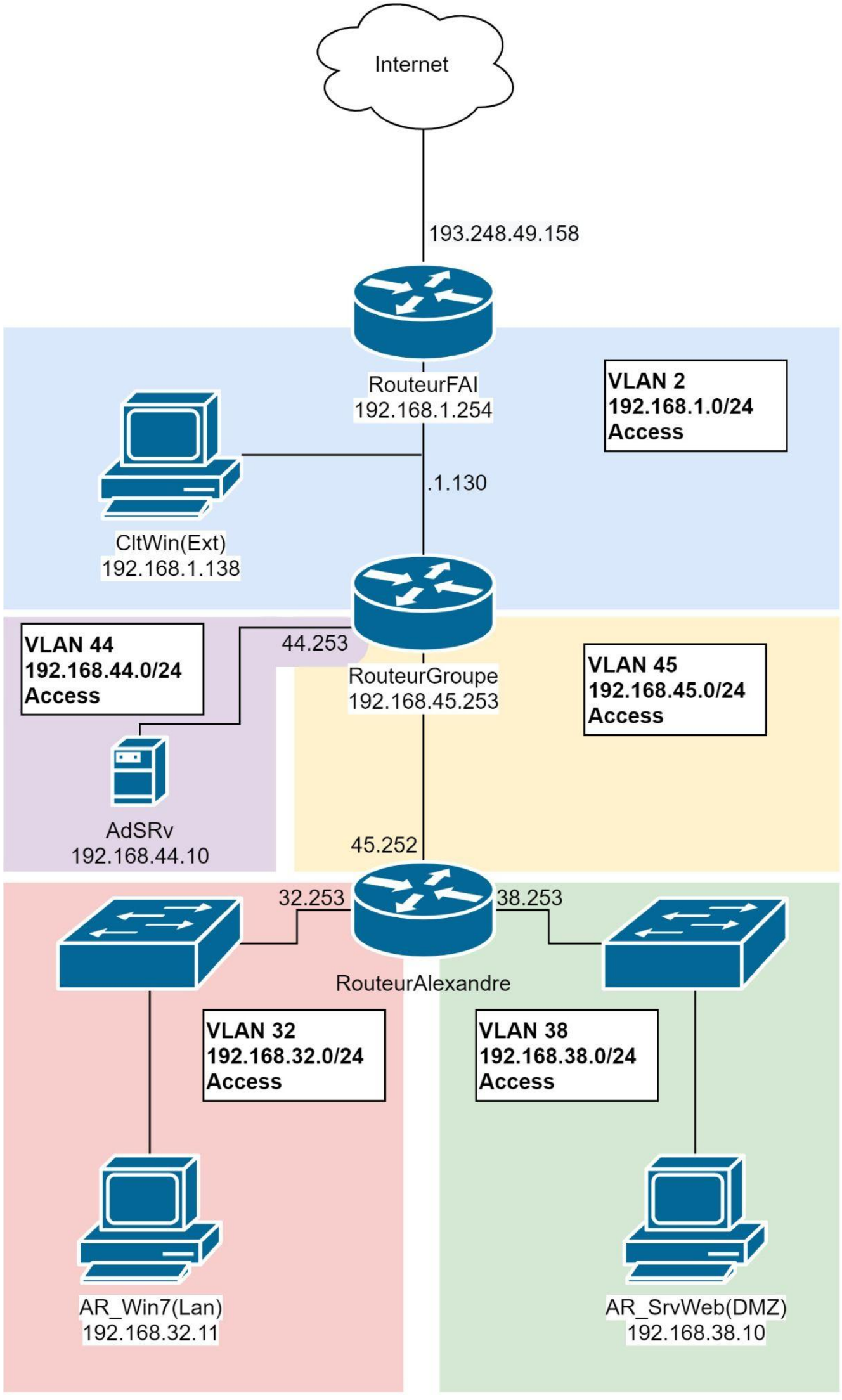
Policy : DROP

N’	Action	Ip source	Port source	Ip destination/inter	Port destination	Protocole	Etat TCP	Description
1	A	*	22	192.168.1.138/32	*	tcp		
2	A	*	*	ens192	67,68	udp		Q9
3	A	*	*	ens224	67,68	udp		Q9

Tables de filtrage routeurAlexandre (INPUT) :

Policy : DROP

N’	Action	Ip source/interfaces	Port source	Ip destination	Port destination	Protocole	Etat TCP	Description
1	A	192.168.1.138/32	*	*	22	tcp		
2	A	ens192	*	*	67,68	udp		Q9
3	A	ens224	*	*	67,68	udp		Q9


Internet
193.248.49.158
RouteurFAI
192.168.1.254
VLAN 2
192.168.1.0/24
Access
.1.130
CltWin(Ext)
192.168.1.138
VLAN 44
192.168.44.0/24
Access
44.253
RouteurGroupe
192.168.45.253
VLAN 45
192.168.45.0/24
Access
AdSRv
192.168.44.10
45.252
32.253
38.253
RouteurAlexandre
VLAN 32
192.168.32.0/24
Access
VLAN 38
192.168.38.0/24
Access
AR_Win7(Lan)
192.168.32.11
AR_SrvWeb(DMZ)
192.168.38.10