TP 3 - SERPOLLET - VALETTE

Created	@6 mai 2022 08:20
Class	NE372
Type	TP
Materials	

Mise en œuvre de la solution pour le client1 :

On configure R2_home :

- On ajoute l'@ du routeur sur la gateway du client1.
- On ajoute le port 0 du FAI comme gateway de R2
- On fait le postrouting :

```
nft add table nat
nft 'add chain nat postrouting { type nat hook postrouting priority 100 ; }'
nft add rule nat postrouting ip saddr 192.168.130.11 oif eth0 masquerade
```

- Puis, on fait le filtrage :

```
nft add table ip filter
nft 'add chain ip filter forward {type filter hook forward priority 0 ; policy drop ;}';
nft 'insert rule ip filter forward ct state established counter accept'
nft 'add rule ip filter forward ip saddr 192.168.130.11 oif eth0 tcp dport { 80 } accept' #accepter HTTP
nft 'add rule ip filter forward ip saddr 192.168.130.11 oif eth0 udp dport { 53 } accept' #accepter DNS
```

Configuration du serveur DNS :

On configure la zone titi.fr :

/var/cache/bind/titi.fr :

```
$TTL    3600
@       IN      SOA     titi.fr. titi.mail.com. (
                     1          ; Serial
                          3600           ; Refresh [1h]
                           600           ; Retry   [10m]
                         86400           ; Expire  [1d]
                           600 )         ; Negative Cache TTL [1h]
;
@       IN      NS      titi.fr.

@       IN      A       193.23.23.2 ; adresse publique du routeur 1
```

⚠️ L'ordre des records compte !!

/etc/bind/named.conf.local

```
zone "titi.fr" {
  type master;
  file "/var/cache/bind/titi.fr";
};
```

Sur le client, **/etc/resolv.conf :**

```
nameserver 193.23.23.2
```

On utilise l'adresse IP publique du routeur R1. Et non, cela ne fonctionne pas en l'état. Il faut configurer R1 afin qu'il laisse le serveur DNS communiquer avec le reste du "monde".

Mise en œuvre de la solution pour l'accès aux serveurs :

On configure R1 pour faire du prerouting :

```
nft add table nat
nft 'add chain nat prerouting { type nat hook prerouting priority 100 ; }'
nft 'add rule nat prerouting iif eth0 udp dport { 53 } dnat to 192.168.100.1' #DNS
nft 'add rule nat prerouting iif eth0 tcp dport { 80 } dnat to 192.168.100.2' #HTTP
```

Les ports à rediriger sont 53 udp et 80 tcp.

On allume le serveur HTTP et le DNS :

```
systemctl start lighttpd
systemctl start bind9
```

On utilise curl et wget pour essayer d'atteindre le serveur HTTP et dig pour atteindre le serveur DNS.

Après moultes problèmes, ça fonctionne.

Mise en œuvre de la solution pour le client2 :

Question : Doit-il y avoir une translation d'adresse pour client2 ?

Non, car c'est le proxy qui communique avec le "monde". Lui, se fait translater.

Question : Quelle doit être la route par défaut de client2 ?

Ça ne change pas, c'est toujours le routeur 4.

On effectue la translation d'adresse du proxy :

```
nft add table nat
nft 'add chain nat postrouting { type nat hook postrouting priority 100 ; }'
nft add rule nat postrouting ip saddr 192.168.0.2 oif eth0 masquerade
```

Question : Le client2 a-t-il besoin d'un résolveur DNS ? Le flux DNS doit-il être autorisé pour client2 ?

S'il ne fait que des requêtes HTPP, il n'en a pas besoin. En effet, le proxy se chargera d'envoyer les requêtes, donc lui a besoin d'un résolveur. Le flux DNS n'a donc pas besoin d'être autorisé pour le client.

Question : Sur quel port TCP écoute le proxy HTTP ? Quel est le fichier de configuration de ce proxy ?

Le proxy écoute sur le port 8888, le fichier de configuration du proxy est /etc/tinyproxy.conf.

Autorisations flux :

Source	Protocole	Autorisation
client2	HTTP	NON
	DNS	NON
proxy	HTTP	OUI
	DNS	OUI

On configure le client pour qu'il passe par le proxy :

Dans le fichier /etc/wgetrc

```
http_proxy = http://192.168.0.2:8888
use_proxy = on
```

On configure le proxy pour que le client puisse passer par lui.

Dans /etc/tinyproxy.conf

```
Allow 192.168.0.10
```

Puis

```
systemctl restart tinyproxy
```

Les avantages sont que l'on peut avoir un cache et que l'on peut filtrer les requêtes.

Les inconvénients sont que c'est plus long (un intermédiaire en plus).