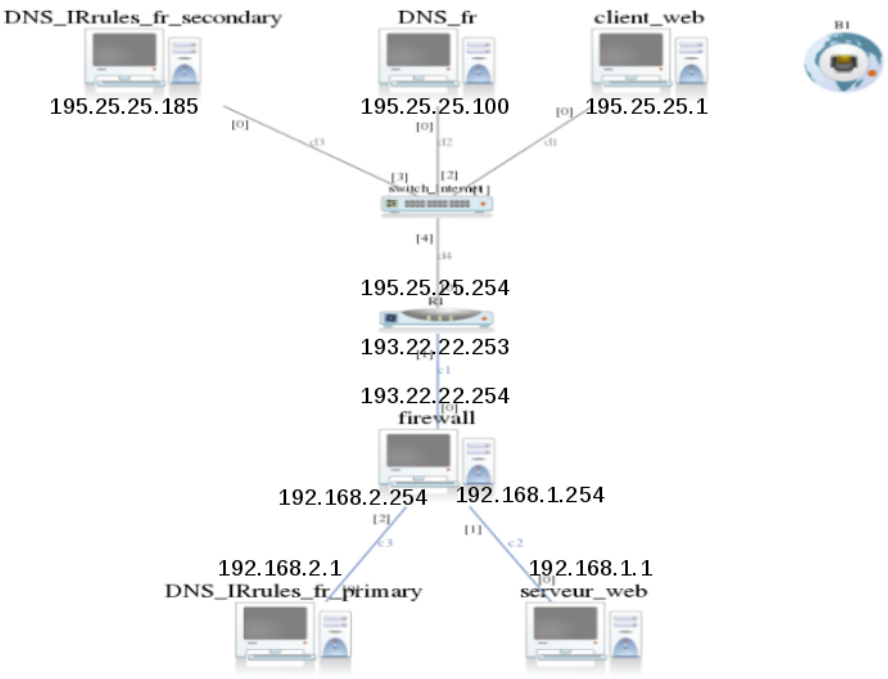
TP NE372 - DNS

Etape 1 : Routage, NAT et filtrage des flux

1. Routage



-On active le routage sur le firewall, on fait en sorte que cette modification soit effectuée à chaque reboot en modifiant /etc/sysctl.conf :

- On ajoute la ligne ***net.ipv4.ip_forward =1***
- On redémarre avec *sysctl -p*

-Pour attribuer les routes par défaut on tape :

- *Route add default gw 192.168.1.254* (pour le serveur web)
- *Route add default gw 192.168.2.254* (pour le DNS primaire)
- *Route add default gw 195.25.25.254* (pour le DNS secondaire, DNS_fr et client_web)
- *Route add default gw 193.22.22.253* (pour le firewall)

Les stations internes peuvent se pinger entre elles. Elles ne peuvent pas pinguer le routeur : en effet le routeur est dans le domaine public et le NAT n'est pas encore activé, il n'est donc pas possible de le pinguer car les réseaux internes ne sont pas routables sur internet.

Les stations dans les réseaux 192.168.x.0 peuvent se pinger entre elles car le forwarding est activé sur le firewall. Leur « portée » s'arrête à l'interface eth0 du firewall, elles ne peuvent pas atteindre le routeur, ce qui est tout à fait normal car la pool IP est privée.

Les stations dans le reseau 195.25.25.x peuvent se pinger entre elles car elles sont sur le même réseau.

TP NE372 - DNS

Les stations externes ne peuvent pas pinger les stations internes car leurs IP ne sont pas routables et le NAT n'est pas encore actif, c'est donc normal.

2. NAT

-On veut que le serveur DNS_IRrules_fr soit accessible depuis internet avec l'adresse IP publique 193.22.22.2:

- *Iptables -t nat -I PREROUTING -d 193.22.22.2 -j DNAT –to-destination 192.168.2.1*

-On veut que le serveur web soit accessible depuis internet avec l'adresse IP publique 193.22.22.1 :

- *Iptables -t nat -I PREROUTING -d 193.22.22.1 -j DNAT –to-destination 192.168.1.1*

-Il faut activer le proxy arp : echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy_arp et on ajoute la route :

- *route add 193.22.22.2 dev eth1*
- *route add 193.22.22.1 dev eth1*

3. Filtrage

-On commence par tout interdire :

- *Iptables -F FORWARD*
- *Iptables -P FORWARD DROP*

-On ajoute, pour pouvoir voir dans les logs tout ce qui est interdit par le firewall, en fin de table : iptables – A FORWARD -j LOG

-On ajoute ensuite les règles d'autorisation des flux une à une conformément à la table donnée dans le sujet :

- **Pour HTTP:**
  iptables -I FORWARD -d 192.168.1.1 -p tcp --dport 80 -j ACCEPT
- **Pour HTTPS :**
  iptables -I FORWARD -d 192.168.1.1 -p tcp --dport 443 -j ACCEPT
- **Pour ICMP:**
  iptables -I FORWARD -p icmp -j ACCEPT
- **Pour DNS (sync) :**
  iptables -I FORWARD -s 195.25.25.185 -d 192.168.2.1 -p tcp --dport 53 -j ACCEPT
- **Pour DNS (requête) :**
  iptables -I FORWARD -d 192.168.2.1 -p tcp --dport 53 -j ACCEPT
  iptables -I FORWARD -d 192.168.2.1 -p udp --dport 53 -j ACCEPT
- **On rajoute une règle en plus (pour ne pas casser les connexions déjà établies) :**
  Iptables -I FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

TP NE372 - DNS

Etape 2 : configuration du client et du serveur DNS_fr

On modifie le fichier /etc/bind/named.conf.local pour configurer une zone fr. en master :

```
Zone « fr. » {
type master ;
file « /var/cache/bind/db.fr » ;
} ;
```

On créer le fichier de zone de .fr dans /var/cache/bind/db.fr :

```
$TTL 3600
@   IN    SOA     ns1.fr.     root.fr. (
              200701001 ; Serial
              3600 ; Refresh
              600 ; Retry
              86400 ; Expire
              600 ) ; Negative Cache TTL
;
@     IN    NS    ns1.fr.
ns1   IN    A      195.25.25.100
```

- La commande named-checkconf ne retourne rien. (si la configuration est bonne => cette commande ne retourne rien).

- La commande named-checkzone fr /var/cache/bind/db.fr retourne :
  zone fr/IN : loaded serial 200701001
  OK

- Un ping depuis « client » vers « ns1.fr » marche mais prend beaucoup de temps car on n'a pas encore configuré le reverse DNS. Alors que le ping depuis « client » vers « 195.25.25.100 » fonctionne rapidement car le reverse DNS n'entre pas en jeu.
  NB : l'option ping avec l'option -n permet de pinguer sans faire le reverse DNS.

Pour configurer le reverse DNS :
On modifie le fichier /etc/bind/named.conf.local :

```
Zone « 25.25.195.in-addr.arpa » {
type master ;
file « /var/cache/bind/db.25.25.195.in-addr.arpa  » ;
} ;
```

```
Zone « 22.22.193.in-addr.arpa » {
type master ;
file « /var/cache/bind/db.22.22.193.in-addr.arpa  » ;
} ;
```

TP NE372 - DNS

On crée le fichier /var/cache/bind/db.25.25.195.in-addr.arpa :

```
$TTL 3600
$ORIGIN 25.25.195.in-addr.arpa.
@   IN      SOA     ns1.fr.     root.fr. (
            200701001 ; Serial
            3600 ; Refresh
            600 ; Retry
            86400 ; Expire
            600 ) ; Negative Cache TTL
;
@       IN      NS      ns1.fr.
100     IN     PTR    ns1.fr.
1       IN     PTR    client.fr.
185     IN     PTR    ns2IR.fr.
```

On crée le fichier /var/cache/bind/db.22.22.193.in-addr.arpa :

```
$TTL 3600
$ORIGIN 22.22.193.in-addr.arpa.
@   IN      SOA     ns1.fr.     root.fr. (
            200701001 ; Serial
            3600 ; Refresh
            600 ; Retry
            86400 ; Expire
            600 ) ; Negative Cache TTL
;
@       IN     NS     ns1.fr.
1       IN     PTR    server.fr.
2       IN     PTR    ns1IR.fr.
```

Etape 3 : Délégation de la zone IRrules.fr

On ajoute à la fin du fichier /etc/bind/db.fr sur DNS_fr :

$ORIGIN IRrules.fr.

@ IN NS ns1.IRrules.fr.

@ IN NS ns2.IRrules.fr.

ns1 IN A 193.22.22.2

ns2 IN A 195.25.25.185

Cela permet d'indiquer à DNS_fr que le sous-domaine IRrules est gérer par 193.22.22.2 et 195.25.25.185

On ajoute dans /etc/bind/named.conf.local sur DNS_IRrules_fr :

Zone « IRrules.fr. » {
type master ;
file « /var/cache/bind/db.IRrules.fr » ;
} ;

On modifie le fichier /var/cache/bind/db.IRrules.fr :

$TTL 10800

$ORIGIN IRrules.fr.

@ IN SOA ns1.IRrules.fr. root.IRrules.fr. (

20160512;

20;

10;

30;

10);

@ IN NS ns1.IRrules.fr.

ns1 IN A 193.22.22.2

www IN A 193.22.22.1

La commande named-checkconf ne retourne rien. La commande named-checkzone fr « /var/cache/bind/db.fr » renvoie :

zone fr/IN: IRrules.fr/NS 'ns1.IRrules.fr' (out of zone) has no addresses records (A or AAAA)

zone fr/IN: loaded serial 20160500

OK

La commande renvoie une erreur car le NS de la zone IRrules.fr n'est pas déclaré dans la zone .fr, ce qui est normal car il n'en fais pas partie.

Le client peut pinger "www.IRrules.fr".

Un « glue record » est l'adresse IP d'un serveur de nom.
Les « glue records » sont nécessaires lorsque le NS fait référence au nom de domaine lors de la déclaration dans le fichier de zone.

Etape 4 : Redondance de IRrules.fr

On ajoute dans /etc/bind/named.conf.local sur DNS_IRrules_fr_secondary :

```
zone "IRrules.fr" {
    type slave;
    file"/var/cache/bind/db.IRrules.fr";
    masters {193.22.22.2;};
};
```

On modifie /etc/bind/named.conf.local sur DNS_IRrules_fr_primary :

```
zone "IRrules.fr" IN{
    type master;
    file"/var/cache/bind/db.IRrules.fr";
    allow-transfer {195.25.25.185;};
    notify yes;
    also-notify {195.25.25.185;};
};
```

TP NE372 - DNS

On modifie /var/cache/bind/db.fr sur DNS_fr et /var/cache/bind/db.IRrules.fr sur DNS_IRrules_fr_primary :

$ORIGIN IRrules.fr.

@ IN NS ns1.IRrules.fr.

@ IN NS ns2.IRrules.fr.

ns1 IN A 193.22.22.2

ns2 IN A 195.25.25.185

On ajoute le NS secondaire ainsi que sont glue record pour la zone.

La commande « dig in NS Irrules.fr » depuis client retourne les NS de la zone Irrules :

;; ANSWER SECTION:

IRrules.fr. 10794 IN NS ns2.IRrules.fr.

IRrules.fr. 10794 IN NS ns1.IRrules.fr.