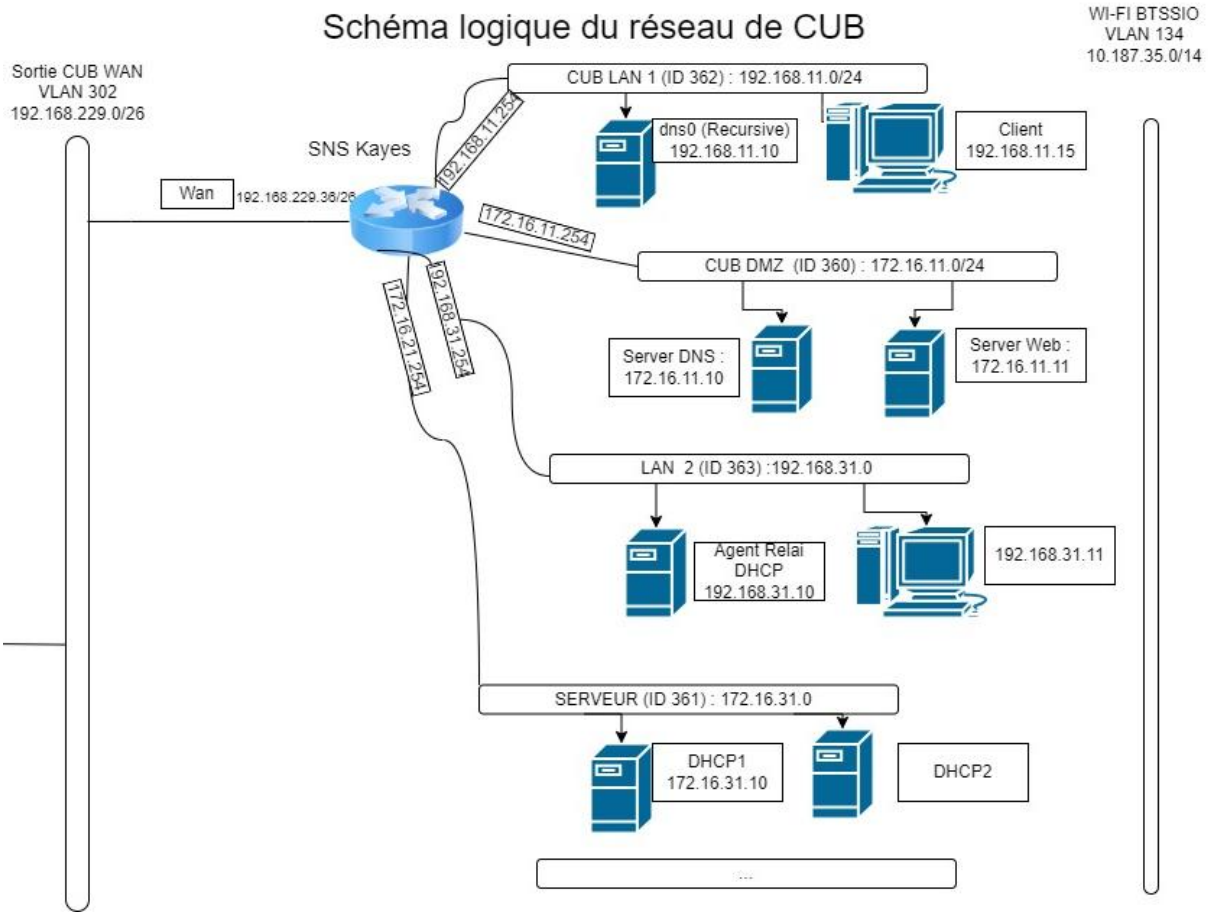
[Date]

Mise en place du serveur DNS (BIND9)

Mamadou CAMARA
[NOM DE LA SOCIETE]

Plan

1. Contexte



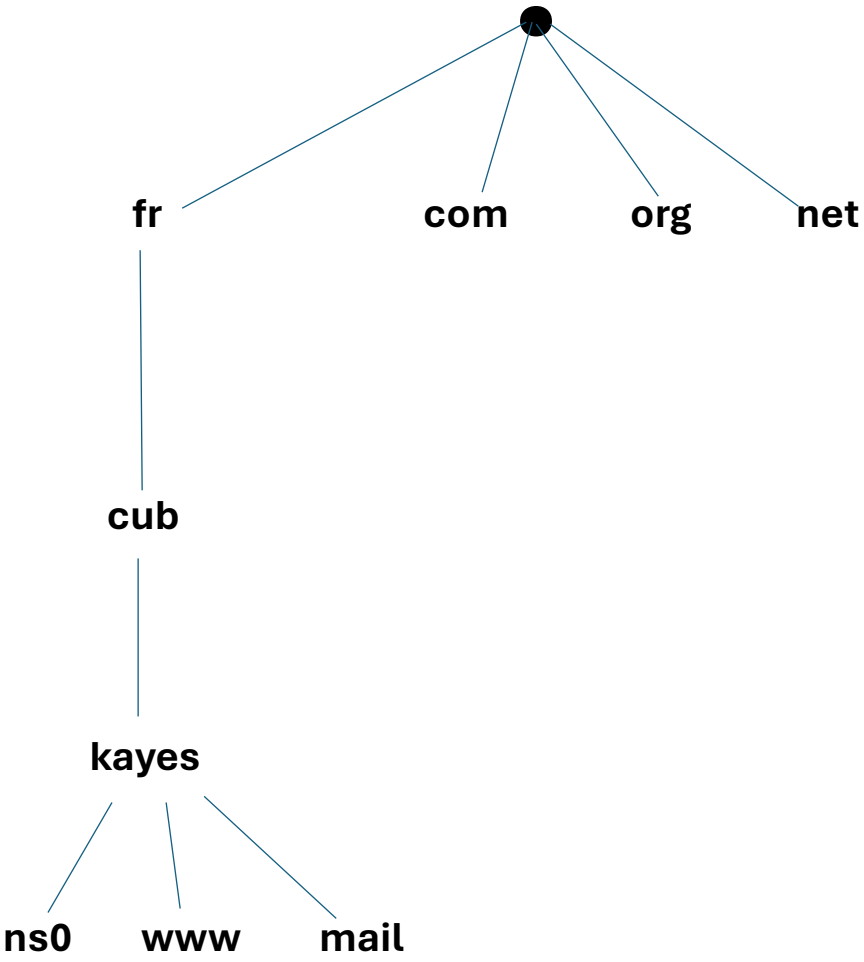
172.16.11.10 : est l'adresse IP de notre serveur DNS qui se trouve dans le VLAN DMZ

ns0.kayes.cub.fr : est le nom de notre serveur DNS

Nous allons installer le serveur DNS ayant autorité sur le domaine **kayes.cub.fr** (non récursif) dans un conteneur Debian appelé ns0 situé dans la DMZ.

192.168.11.10 : est l'adresse IP du DNS récursif (Résolveur)

2. Présentation



Un serveur DNS (Domain Name System) est un serveur de noms qui gère les correspondances entre les noms de domaine et les adresses IP. Ce qui est fort utile pour naviguer sur internet. On peut penser que sans serveur DNS il n'y a plus d'internet.

3. Installation et configuration

a. Installation du service DNS

apt update && apt upgrade

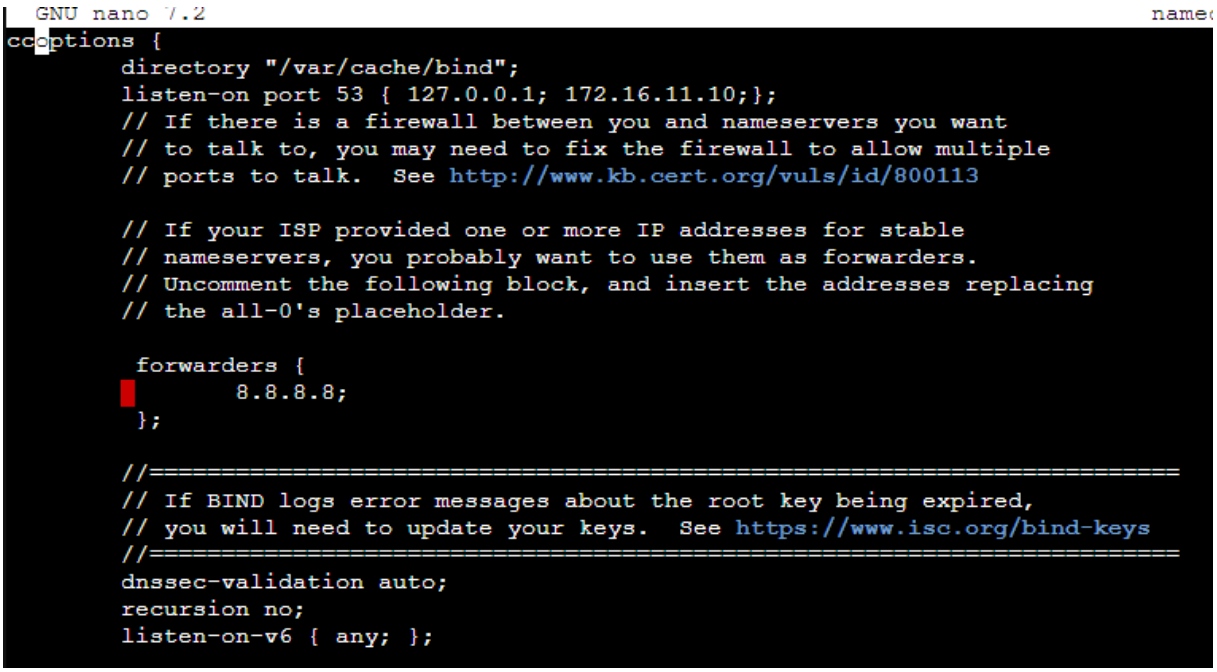
apt -y install bind9 dnsutils

b. Configuration du service

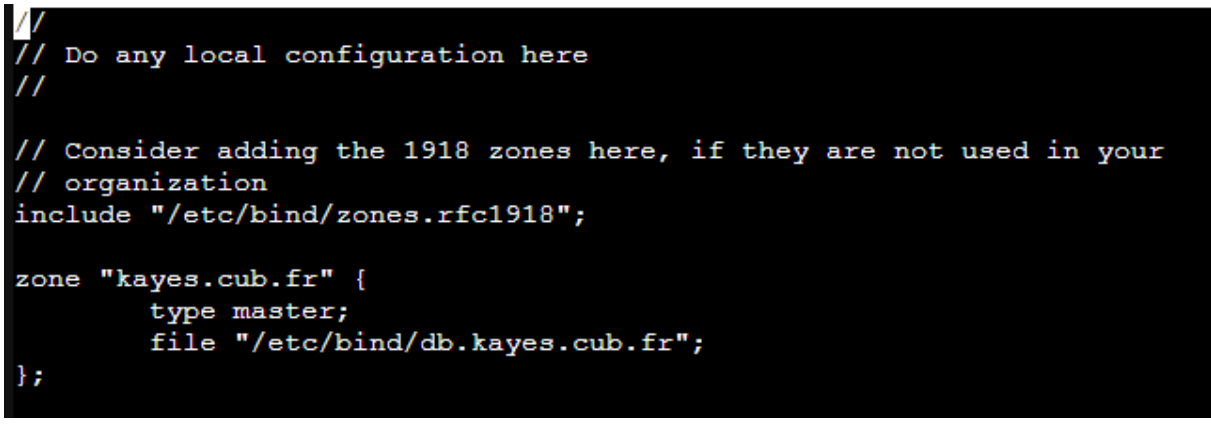
Modification du fichier **/etc/bind/named.conf.options**

Editez le fichier **/etc/bind/named.conf.options** pour :

- désactiver la récursivité,
- indiquer l'interface d'écoute du serveur (127.0.0.1 et 172.16.11.10) :
-



- **Modifiez le fichier de configuration**
  nano /etc/bind/named.conf.local
  On ajoute les information de notre zone :



Voyons la signification de chaque champ :

Option	Commentaires
zone “kayes.cub.fr” {	Le nom de la zone entre guillemets et suivi d’une accolade.
type master;	**Master** indique que vous avez l’autorité sur la zone. D’autres serveurs (esclaves) pourront se synchroniser avec votre serveur.
file “/etc/bind/db.agence.cub.fr”;	Emplacement et nom du fichier de zone. Il sera placé dans /etc/bind/ et s’appellera db.agence.cub.fr
};	L’accolade ferme la définition de la zone.

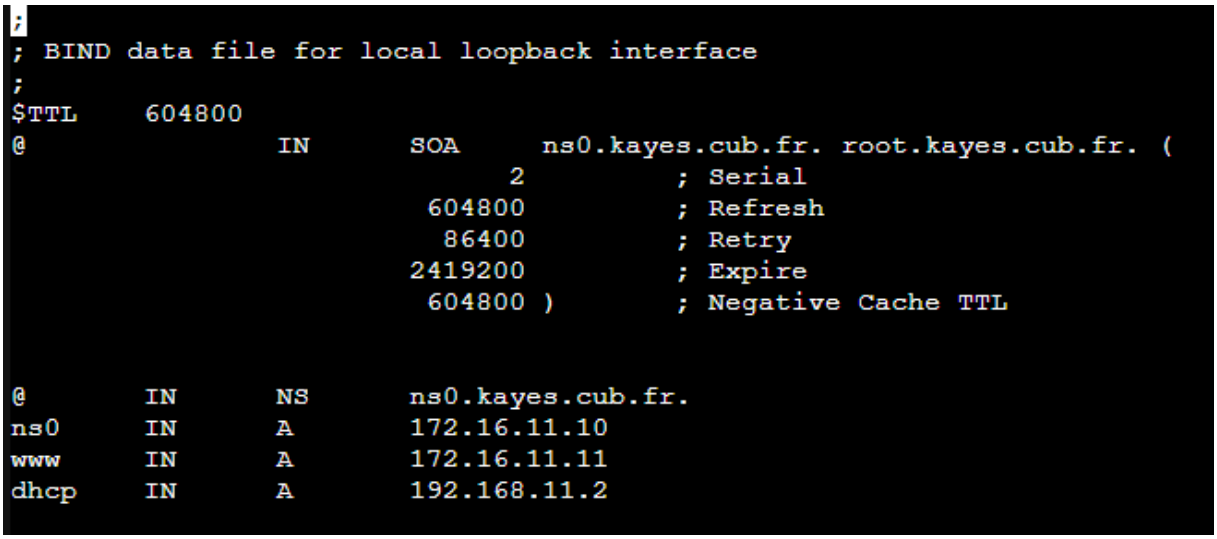
Création du fichier de zone maître

Nous devons maintenant créer les deux fichiers indiqués pour nos zones dans **/etc/bind/named.conf.local**.

On crée des enregistrements pour nos serveurs DHCP , DNS et web.

On crée le fichier **db.kayes.cub.fr** pour la zone **« kayes.cub.fr »**

nano /etc/bind/db.kayes.cub.fr



```
;
; BIND data file for local loopback interface
;
$TTL    604800
@               IN      SOA     ns0.kayes.cub.fr. root.kayes.cub.fr. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL


@       IN      NS      ns0.kayes.cub.fr.
ns0     IN      A       172.16.11.10
www     IN      A       172.16.11.11
dhcp    IN      A       192.168.11.2
```

Chaque ligne (qui ne commence pas par un $) s'appelle un enregistrement DNS.

La première ligne ($TTL 1D) indique la durée de vie des informations transmises par votre serveur DNS. En effet, les machines qui feront appel à notre serveur vont conserver dans un cache les informations découvertes afin de ne pas refaire en permanence les mêmes demandes. Ici, au bout de trois jours (1D = 1 day), les informations doivent être retirées du cache. Comment déterminer ce TTL ? Cela dépend de votre zone. Si elle change souvent, il faut un TTL court.

La deuxième ligne définit le nom du domaine (Notez bien le point à la fin du nom de domaine) et est importante. C'est un enregistrement SOA (Start Of Authority) qui indique que les informations en-dessous sont de votre responsabilité. En effet, vous êtes le serveur maître de la zone kayes.cub.fr.

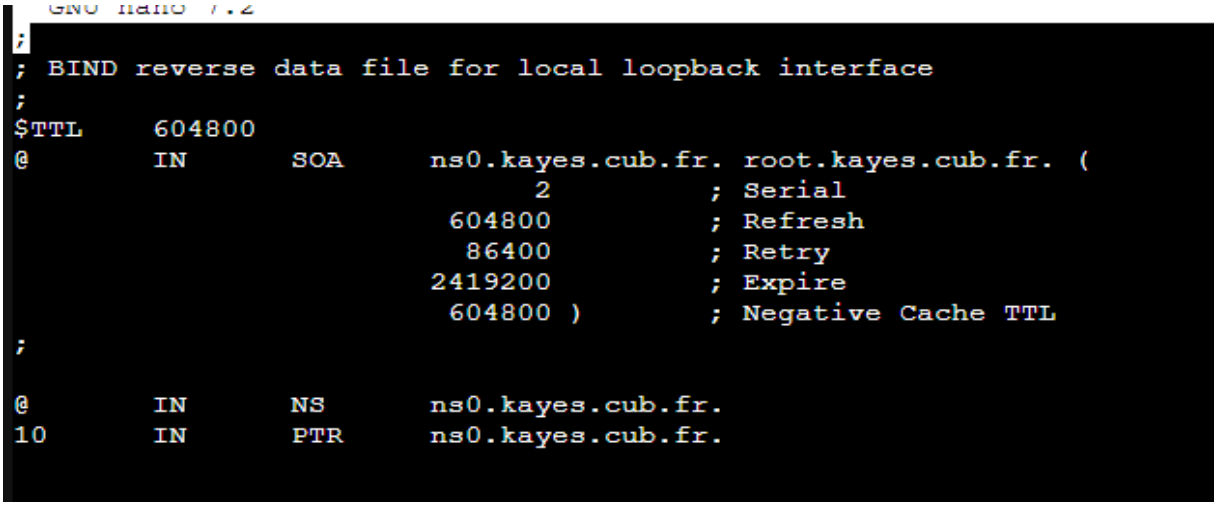
Voici sa structure :

Voici sa structure :

kayes.cub.fr. IN SOA	ns0.kayes.cub.fr.	root.agence.cub.fr .	(
Enregistrement DNS de type Internet (IN) déclarant notre autorité (SOA).	Nom du serveur de nom maître sur la zone kayes.cub.fr	Email (sans @) de l'administrateur de la zone	Une série de valeurs numériques utilisées pour la synchronisation entre le serveur maître et ses esclaves.\\La première parenthèse doit être sur la même ligne que le SOA.

La quatrième ligne est un enregistrement NS (Name Server) qui donne le nom du serveur maître sur la zone (vous). La cinquième ligne est un enregistrement A (Address) qui donne l'IP de la machine dont le nom est indiqué à droite.

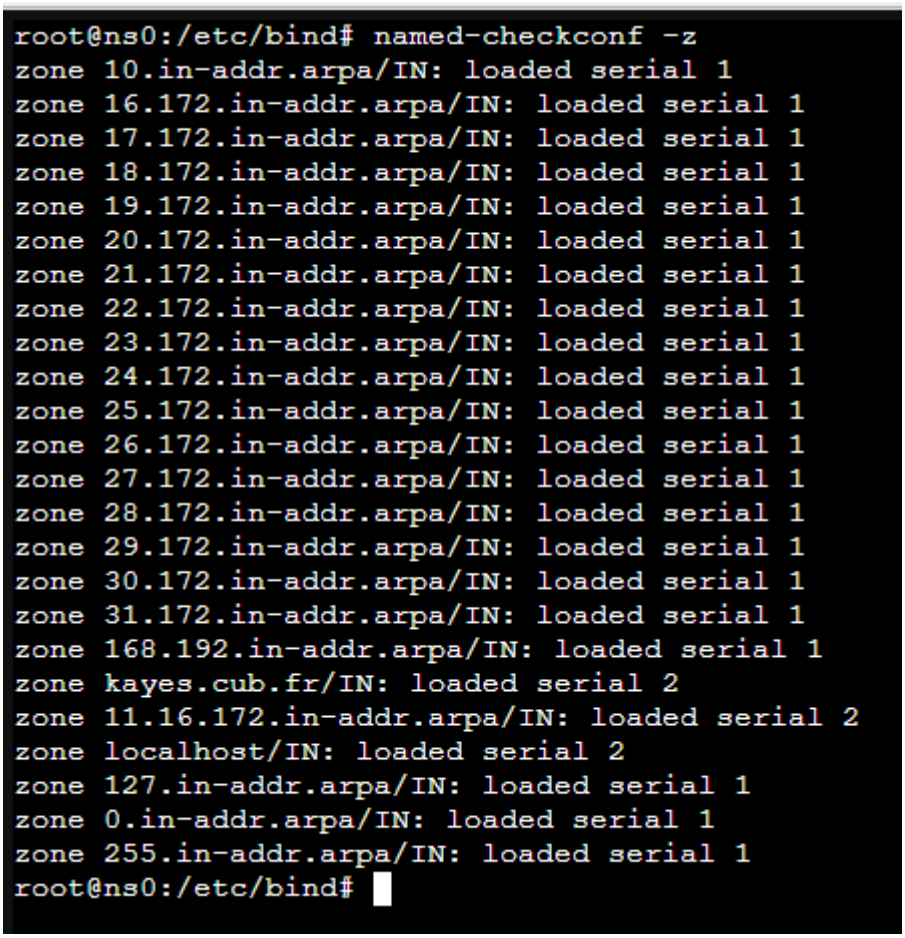
- Création d'un fichier pour la zone inverse : nano /etc/bind/db.172.16.11.rev



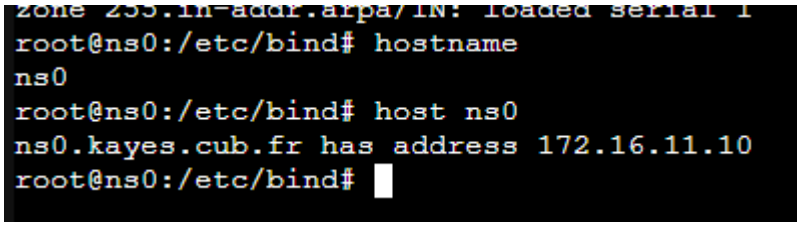
4. Teste interne :

On utilise la commande suivante pour tester notre configuration :

Named-checkconf -z



- On vérifie le nom avec la commande hostname et host « nom de la machine » pour vérifier la résolution :



- On vérifie la résolution avec la commande **dig:**

```
ns0.kayes.cub.fr has address 172.16.11.10
root@ns0:/etc/bind# dig ns0.kayes.cub.fr

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> ns0.kayes.cub.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38817
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ns0.kayes.cub.fr.              IN      A

;; ANSWER SECTION:
ns0.kayes.cub.fr.       82492   IN      A       172.16.11.10

;; Query time: 0 msec
;; SERVER: 192.168.11.10#53(192.168.11.10) (UDP)
;; WHEN: Tue Sep 24 12:30:59 UTC 2024
;; MSG SIZE  rcvd: 61

root@ns0:/etc/bind#
```

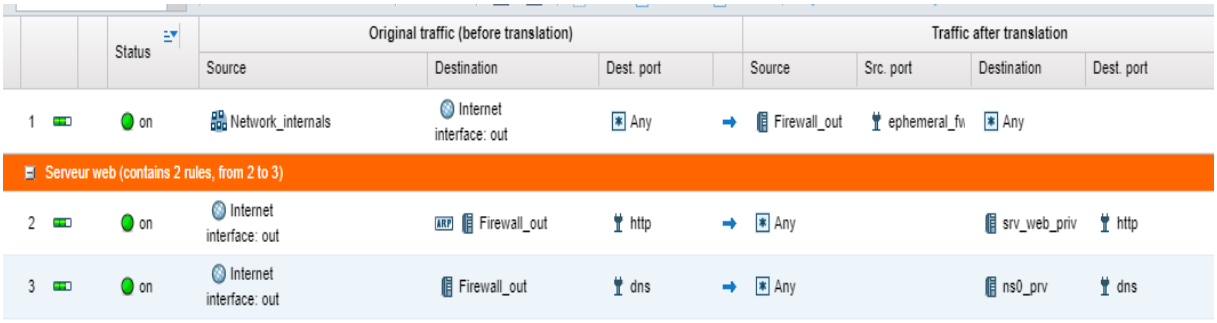
La commande **nslookup** est plus ancienne que la commande **dig**, il est possible de lui passer soit le nom d'une station ou l'adresse d'un serveur pour obtenir les informations fournies par le serveur DNS. Voici ci-dessous un exemple :

```
root@ns0:/etc/bind# nslookup www
Server:         192.168.11.10
Address:        192.168.11.10#53

Non-authoritative answer:
Name:   www.kayes.cub.fr
Address: 172.16.11.11
```

5) Teste depuis le réseau CUB WAN :

Pour tester notre nom de domaine depuis le réseau **CUB WAN**, on publie nos deux serveurs **(web et sn0)** sur le pare-feu Stormshield, via NAT statique :



		Status	Original traffic (before translation)				Traffic after translation			
			Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1		on	Network_internals	Internet interface: out	Any	→	Firewall_out	ephemeral_fw	Any	
Serveur web (contains 2 rules, from 2 to 3)										
2		on	Internet interface: out	ARP Firewall_out	http	→	Any		srv_web_priv	http
3		on	Internet interface: out	Firewall_out	dns	→	Any		ns0_prv	dns

- Ensuite on modifie la passerelle de notre VM CUB WAN par 192.168.229.36 (**l'interface Out** de notre pare-feu)

On teste avec la commande dig www.kayes.cub.fr

```
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> www.kayes.cub.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30076
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6f1278bbe369bc67010000006704d7db0d3c0464c3f96364 (good)
;; QUESTION SECTION:
;www.kayes.cub.fr.              IN      A

;; ANSWER SECTION:
www.kayes.cub.fr.       604800  IN      A       172.16.31.253
www.kayes.cub.fr.       604800  IN      A       192.168.229.36

;; Query time: 0 msec
;; SERVER: 192.168.229.36#53(192.168.229.36) (UDP)
;; WHEN: Tue Oct 08 06:57:31 UTC 2024
;; MSG SIZE  rcvd: 105
```