Mission 2 : Mise en place d'un serveur de noms

0. Pré-requis

Afin de pouvoir réaliser cette mission il faut :

- Un serveur sous PROXMOX
- Un routeur sous Debian 13
- Un ou deux humain(s)

1. Introduction

L'objectif de cette mission est de mettre en place un serveur de noms pour le réseau DMZ.

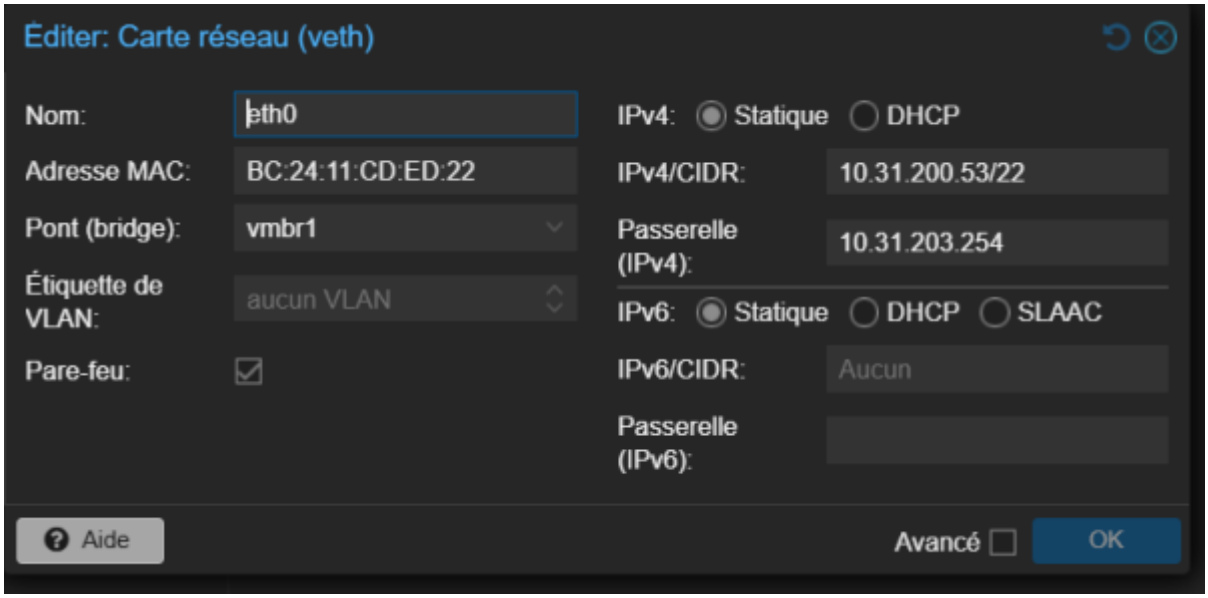
1.1 Rappel DNS

Un DNS (Domain Name System) sert de service de traduction entre les noms de domaine et les adresses IP. En clair : Les ordinateurs communiquent entre eux grâce à des adresses IP (par exemple 142.250.74.14). Pour les humains, retenir des adresses IP n'est pas pratique. On préfère des noms simples comme google.com. Le DNS agit comme un annuaire téléphonique d'Internet : il traduit automatiquement google.com en l'adresse IP correspondante pour que ton ordinateur sache où se connecter. À quoi ça sert concrètement ? Accéder facilement aux sites web sans taper d'adresse IP. Faciliter la gestion du réseau : si l'adresse IP d'un serveur change, on n'a pas besoin de retenir la nouvelle, le DNS fait la mise à jour. Optimiser la performance : certains DNS redirigent vers le serveur le plus proche pour charger un site plus vite. Sécurité : certains services DNS filtrent les sites malveillants ou bloquent la pub. Sans DNS, tu devrais taper quelque chose comme 142.250.74.14 au lieu de google.com.

2. Création et configuration des conteneurs DNS

2.1 Création et configuration réseau

On créé donc un premier conteneur **ns1-europe**, copie du conteneur template qui servira de DNS maître pour le réseau DMZ. Il aura comme IP : **10.31.200.53**
On crée également un deuxième conteneur **ns2-europe**, qui seras aussi une copie du conteneur template, il sera le DNS slave pour le réseau DMZ. Il aura comme IP : **10.31.200.54**
Pour ce faire, on se connecte au serveur PROXMOX à l'aide d'une adresse que l'on tape sur un navigateur : **https://10.31.192.1:8006/** , Voici la configuration réseau du conteneur ns1-europe :



Adresse ip : 10.31.200.53/22 —→ IP du DNS primaire Passerelle : 10.31.203.254 —→ IP du routeur sur le réseau DMZ Pont (bridge) : vmbr1 —→ pont du réseau DMZ

2.2 Configuration du conteneur

Une fois le conteneur ns1-europe crée, on le configure en installant d'abord bind et ses outils :

```
root@ns1-europe:~# apt install bind9 bind9utils dnsutils
root@ns1-europe:~# apt install rsyslog
```

2.3 Declaration des zones DNS

Les zones gérées seront gsb.org et europe.gsb.org, dans le fichier named.conf.local seront déclarées :

```
root@ns1-europe:~# nano /etc/bind/named.conf.local
```

```
//
// Do any local configuration here
//
// Zone directe Europe
zone "europe.gsb.org" IN {
    type master;
    file "/etc/bind/db.europe.gsb.org";
    allow-transfer { 10.31.200.54; };
};

zone "gsb.org" IN {
    type master;
    file "/etc/bind/db.gsb.org";
    allow-transfer { 10.31.200.54; };
};
```

2.4 Configuration des fichiers de zone

On crée ensuite les fichiers de zone pour les domaines déclarés. Ces fichiers contiennent les enregistrements DNS (A, NS, MX, CNAME...).

Fichier de zone pour **gsb.org** :

```
root@ns1-europe:~# nano /etc/bind/db.gsb.org
```

```
$TTL    604800
@       IN      SOA     ns1-europe.gsb.org. admin.gsb.org. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
; Serveurs de noms
@       IN      NS      ns1-europe.gsb.org.
@       IN      NS      ns2-europe.gsb.org.

; Enregistrements A
ns1-europe      IN      A       10.31.200.53
ns2-europe      IN      A       10.31.200.54
```

Fichier de zone pour **europe.gsb.org** :

```
root@ns1-europe:~# nano /etc/bind/db.europe.gsb.org
```

```
$TTL    604800
@       IN      SOA     ns1-europe.gsb.org. admin.gsb.org. (
                              2         ; Serial
```

```
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
; Serveurs de noms
@       IN      NS      ns1-europe.gsb.org.
@       IN      NS      ns2-europe.gsb.org.

; Enregistrements A
ns1-europe      IN      A       10.31.200.53
ns2-europe      IN      A       10.31.200.54
```

2.5 Configuration du DNS secondaire (ns2-europe)

Sur **ns2-europe**, on installe également bind9 et ses outils :

```
root@ns2-europe:~# apt install bind9 bind9utils dnsutils
root@ns2-europe:~# apt install rsyslog
```

On configure ensuite le fichier **named.conf.local** pour déclarer les zones en mode **slave**, en pointant vers le DNS maître (ns1-europe) :

```
root@ns2-europe:~# nano /etc/bind/named.conf.local
```

```
zone "gsb.org" {
    type slave;
    masters { 10.31.200.53; };
    file "/var/cache/bind/db.gsb.org";
};

zone "europe.gsb.org" {
    type slave;
    masters { 10.31.200.53; };
    file "/var/cache/bind/db.europe.gsb.org";
};
```

3. Démarrage et vérification du service BIND

3.1 Démarrage du service

Sur les deux conteneurs (ns1-europe et ns2-europe), on démarre et active le service bind9 au démarrage :

```
root@ns1-europe:~# systemctl enable bind9
root@ns1-europe:~# systemctl start bind9
```

```
root@ns1-europe:~# systemctl status bind9
```

Le statut doit afficher **active (running)**.

3.2 Vérification de la configuration

On vérifie que la configuration de BIND est correcte avec les commandes suivantes :

```
root@ns1-europe:~# named-checkconf
root@ns1-europe:~# named-checkzone gsb.org /etc/bind/db.gsb.org
root@ns1-europe:~# named-checkzone europe.gsb.org
/etc/bind/db.europe.gsb.org
```

Si la configuration est correcte, les commandes retournent **OK**.

3.3 Test de résolution DNS

On teste la résolution DNS depuis un client du réseau DMZ avec la commande **dig** ou **nslookup** :

```
# Test vers le DNS primaire
root@client:~# dig @10.31.200.53 ns1-europe.gsb.org

# Test vers le DNS secondaire
root@client:~# dig @10.31.200.54 ns1-europe.gsb.org

# Vérification de la résolution inverse
root@client:~# nslookup 10.31.200.53 10.31.200.53
```

Une réponse correcte contiendra la section **ANSWER SECTION** avec l'adresse IP attendue.

4. Configuration des clients

4.1 Déclaration des DNS sur les machines du réseau

Pour que les machines du réseau DMZ utilisent les serveurs DNS nouvellement créés, il faut modifier leur fichier **/etc/resolv.conf** :

```
root@machine-cliente:~# nano /etc/resolv.conf
```

```
domain gsb.org
search gsb.org europe.gsb.org
nameserver 10.31.200.53
nameserver 10.31.200.54
```

Ainsi, le DNS primaire (**ns1-europe** - 10.31.200.53) sera interrogé en premier, et le DNS secondaire

(**ns2-europe** - 10.31.200.54) prendra le relais en cas d'indisponibilité du premier.