24/09/2024

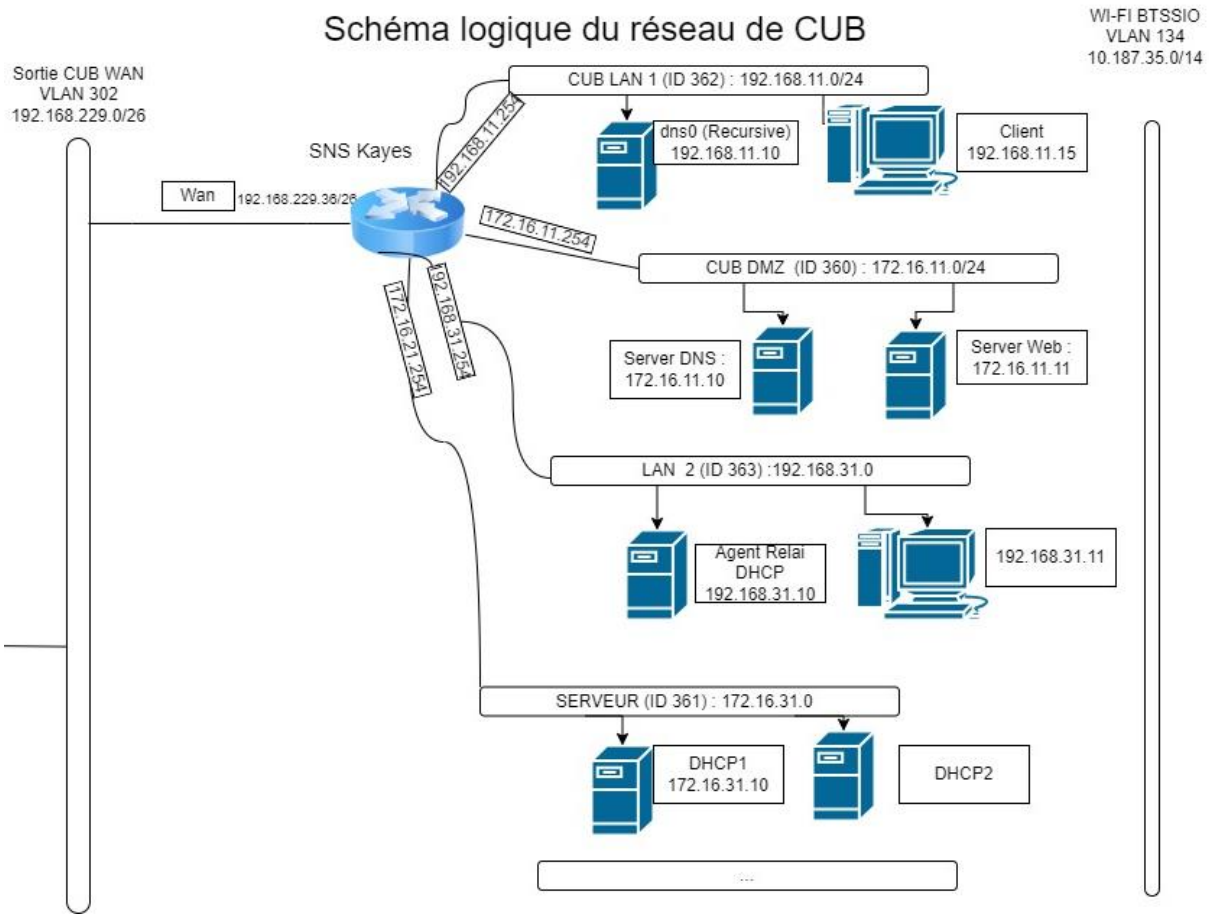
Mise en place du serveur DNS récursif (Unbound)

Mamadou CAMARA
BTS SIO

Sommaire :

1. Contexte
2. Présentation
3. Installation de UnBound
4. Configuration
5. Test

1. Contexte :



- **Kayes.cub.fr : est notre (sous) zone autoritaire**
- **Cub.fr : est la siège**
- **172.16.11.10 : est l'adresse IP du serveur DNS autoritaire kayes.cub.fr**
- **192.168.11.10 : est l'adresse IP du résolveur**

2. Présentation :

Le paquet logiciel Unbound permet de configurer un serveur récursif avec Debian. Ce logiciel ne fera que des requêtes DNS de type récursif sans héberger de zone DNS.

Pour le contexte CUB, le domaine cub.fr est un domaine fictif. Le résolveur ne doit pas utiliser son principe de fonctionnement classique qui consiste à solliciter les serveurs racines sur Internet quand une résolution de nom concerne le domaine cub.fr.
Notre configuration doit indiquer que lorsque le serveur récursif est interrogé pour le nom de domaine cub.fr, il doit rediriger la requête vers le serveur DNS présent dans la DMZ du siège (cub.fr) :

- Nous utiliserons la notion de **stub-zone** et non de **forward-zone** pour rediriger la requête vers un serveur faisant autorité.
- Nous utiliserons la notion de **forward-zone** dans Unbound pour la redirection vers le serveur récursif 8.8.8.8 (ou 1.1.1.1, 9.9.9.9 par exemple) pour tous les autres domaines sur Internet.

3. Installation de Unbound :

a. **Première étape :**
Création d'une VM (conteneur LXC) appellé dns0 dans notre Lan 1 (utilisateur) avec l'adresse IP **192.168.11.10**
NB : Cette VM ne gére pas de zone mais uniquement le processus récursif de résolution de nom.

b. **Installation des paquets unbound**

- Mise à jour de la VM
  Apt update && apt upgrade
- Installation de Unbound

Apt install unbound dnsutils

4. Configuration :

Le fichier de configuration de unbound se trouve dans **/etc/unbound/unbound.conf**

On ouvre le fichier avec la commande :

nano /etc/unbound/unbound.conf

```
# See the unbound.conf(5) man page.
#
# See /usr/share/doc/unbound/examples/unbound.conf for a commented
# reference config file.
#
# The following line includes additional configuration files from the
# /etc/unbound/unbound.conf.d directory.
#include-toplevel: "/etc/unbound/unbound.conf.d/*.conf"
server:

interface: 192.168.11.10
interface: 127.0.0.1

access-control: 172.16.11.0/24 allow
access-control: 192.168.11.0/24 allow
access-control: 172.16.31.0/24 allow
access-control: 192.168.31.0/24 allow
access-control: 127.0.0.0/8 allow
access-control: 0.0.0.0/0 refuse

hide-version: yes
hide-identity: yes

do-ip4: yes

logfile: /var/log/unbound/unbound.log
verbosity: 2

private-domain: cub.fr.

# interroger le serveur DNS du siege cub.fr
stub-zone:
name: "cub.fr."
stub-addr: 192.168.229.1

# r  cursivite pour les domaines sur Internet
forward-zone:
name: "."
forward-addr: 8.8.8.8
forward-addr: 8.8.4.4

# interroger le serveur DNS ns0.kayes.cub.fr de l'agence
```

Explication :

- **Les interfaces d’écoutes** :

  interface: 192.168.11.10

  interface: 127.0.0.1

  Le serveur DNS écoutera sur ces deux adresses IP : une IP locale (127.0.0.1) et une IP spécifique à notre réseau interne (192.168.11.10)

- **Règles de contrôles d’accès :**

  access-control: 172.16.11.0/24 allow

  access-control: 192.168.11.0/24 allow

  access-control: 172.16.31.0/24 allow

  access-control: 192.168.31.0/24 allow

  access-control: 127.0.0.0/8 allow

  access-control: 0.0.0.0/0 refuse

  Seuls les réseaux définis (ici les réseaux internes) sont autorisés à interroger le serveur DNS, et toute autre demande venant d'ailleurs sera refusée (0.0.0.0/0 refuse).
  NB : Ces règles de contrôle d’accès permettent nos réseaux internes d’accéder à internet

- Sécurité et confidentialité :

  hide-version: yes

  hide-identity: yes

  Ces options masquent la version du serveur et l'identité d'Unbound, renforçant ainsi la sécurité.

- **Adresse des journaux et niveau de verbosité** :

  logfile: /var/log/unbound/unbound.log

  verbosity: 2

Les logs sont stockés dans /var/log/unbound/unbound.log avec un niveau de verbosité modéré (2).

- **Zone privée et stub-zone** :

  private-domain: cub.fr.
  stub-zone:
  name: "cub.fr."
  stub-addr: 192.168.229.1

  Nous configurons une zone **stub** pour le domaine **cub.fr** qui redirige les requêtes pour ce domaine vers le serveur DNS **192.168.229.1.**

- Récursivité pour le domain externes :

  forward-zone:
  name: "."
  forward-addr: 8.8.8.8
  forward-addr: 8.8.4.4

  Cette partie définit l'utilisation des serveurs DNS de Google pour résoudre toutes les autres requêtes de domaine.

- **Résolution pour le domaine DNS kayes.cub.fr de notre agence**

  Une stub-zone supplémentaire doit être créée pour gérer la résolution de nom pour notre domaine DNS d'agence.
  On ajoute dans le fichier **/etc/unbound/unbound.conf** les lignes suivantes en indiquant l'adresse IP de notre serveur DNS dans notre **VLAN DMZ**

  # interroger le serveur DNS ns0.kayes.cub.fr de l'agence

  stub-zone:

name: "kayes.cub.fr."
stub-addr: 172.16.11.10

kayes.cub.fr : est notre sous domaine autoritaire avec l'adresse IP 172.16.11.10

Cette directive permet au serveur Unbound de déléguer la résolution des requêtes pour le domaine kayes.cub.fr au serveur DNS ns0.kayes.cub.fr, situé à l'adresse IP 172.16.11.10.

Lancement du serveur :

On crée un dossier unbound dans /var.log

mkdir /var/log/unbound

touch /var/log/unbound/unbound.log

On donne le droit

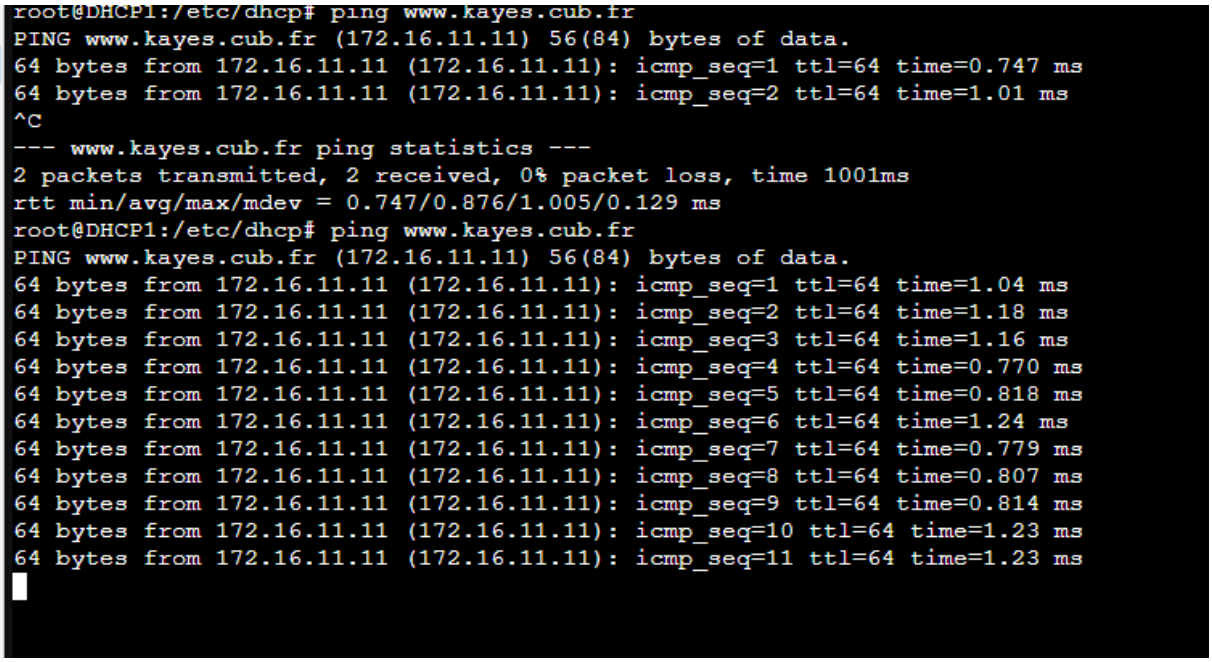
chown -R unbound:unbound /var/log/unbound

On redemarre le service :

systemctl restart unbound

5. Teste :

- Modification de la configuration de tous les clients de notre agence
  Dans le fichier **/etc/resolv.conf :**
  Domain kayes.cub.fr
  Search kayes.cub.fr
  Nameserver 192.168.11.10


root@DHCP1:/etc/dhcp# ping www.kayes.cub.fr
PING www.kayes.cub.fr (172.16.11.11) 56(84) bytes of data.
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=1 ttl=64 time=0.747 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=2 ttl=64 time=1.01 ms
^C
--- www.kayes.cub.fr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.747/0.876/1.005/0.129 ms
root@DHCP1:/etc/dhcp# ping www.kayes.cub.fr
PING www.kayes.cub.fr (172.16.11.11) 56(84) bytes of data.
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=1 ttl=64 time=1.04 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=2 ttl=64 time=1.18 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=3 ttl=64 time=1.16 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=4 ttl=64 time=0.770 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=5 ttl=64 time=0.818 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=6 ttl=64 time=1.24 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=7 ttl=64 time=0.779 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=8 ttl=64 time=0.807 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=9 ttl=64 time=0.814 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=10 ttl=64 time=1.23 ms
64 bytes from 172.16.11.11 (172.16.11.11): icmp_seq=11 ttl=64 time=1.23 ms