

Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

Situation 2 : Mise en place des serveurs et des services

Le **document 1** présente le fonctionnement du service DNS.

Le **document 2** détaille la configuration du résolveur DNS récursif de l'agence Galway.

Le **document 3** rappelle la configuration du service DNS bind9 et donne la configuration du serveur DNS ayant autorité sur la zone galway.cub.fr.

Le **document 4** décrit la configuration du serveur DNS ayant autorité sur la zone cub.fr. Ce serveur a été installé au préalable par le professeur et est opérationnel.

Pour chaque agence, il est nécessaire d'installer et configurer :

- le serveur DNS ayant autorité sur le domaine **<agence>.cub.fr (non récursif)** ;
- le serveur DNS ayant autorité sur la zone **lan.<agence>.cub.fr (non récursif)** ;
- le résolveur récursif.
- Un serveur Web dans la DMZ (*vous pouvez migrer un de vos serveurs actuellement en place*).

Vous devez :

1. Mettre en place les serveurs et services de votre agence.
2. Procéder aux ajouts nécessaires sur le pare-feu pour le cas particulier du réseau Wan-CUB (document 5) pour permettre notamment l'accessibilité des serveurs DNS et Web (protocole HTTP et HTTPS).



Si l'administration s'effectue via l'interface OUT, l'ajout de la règle de redirection vers le protocole HTTPS fait perdre de facto l'accès à l'interface. En effet, les flux d'administration HTTPS seront redirigés vers le serveur Web. Une solution consiste à ne rediriger que le protocole HTTP mais l'accès au site Web de l'extérieur en HTTPS ne sera alors pas possible. C'est l'occasion de rappeler qu'une telle situation ne peut se produire en production car l'administration du pare-feu ne doit jamais être possible via l'interface OUT.

3. Vérifier le fonctionnement des services DNS et Web. *Vous utiliserez le modèle de fiche recette.*

Attention, lors des tests, il est nécessaire de vider le cache DNS et le cache de votre navigateur pour les tests sur le serveur Web (ou réaliser les tests en navigation privée).

Par exemple :

À partir du résolveur (pour le domaine et le sous domaine) :

```
root@resolvDNSgalway:~# unbound-control flush_zone galway.cub.fr
ok removed 4 rrsets, 4 messages and 0 key entries
root@resolvDNSgalway:~# unbound-control flush_zone cub.fr
ok removed 0 rrsets, 1 messages and 0 key entries
```

ou

```
root@resolvDNSgalway:~# unbound-control reload
```

À partir de n'importe quel Debian ou Ubuntu :

```
systemd-resolve --flush-caches
```



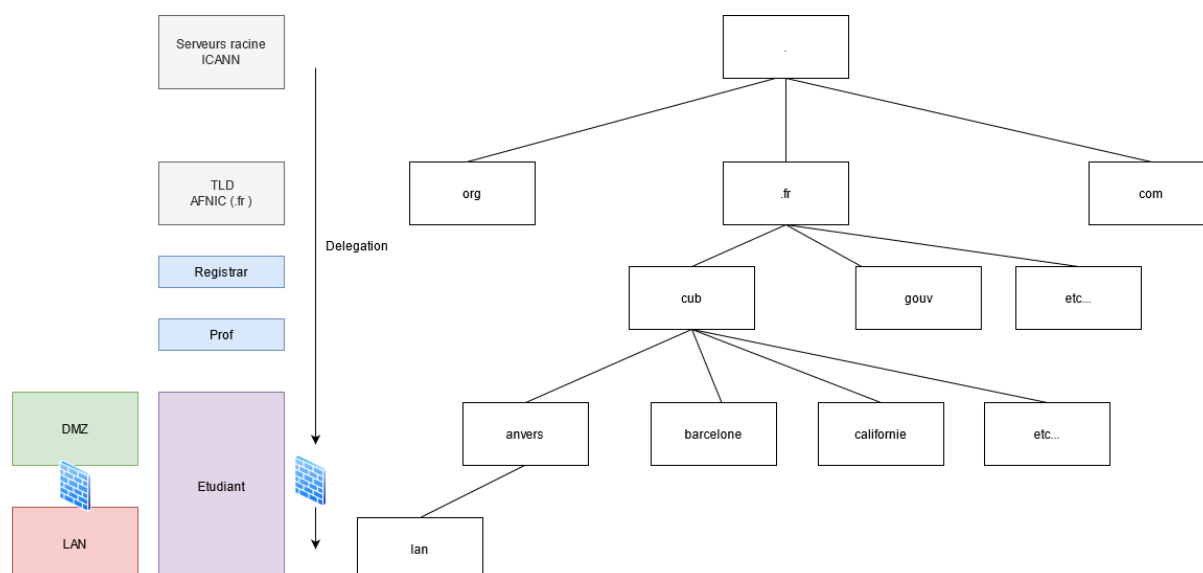
La commande « dig » est plus verbeuse pour dépanner le service DNS que la commande « nslookup ».

4. Documenter l'infrastructure.

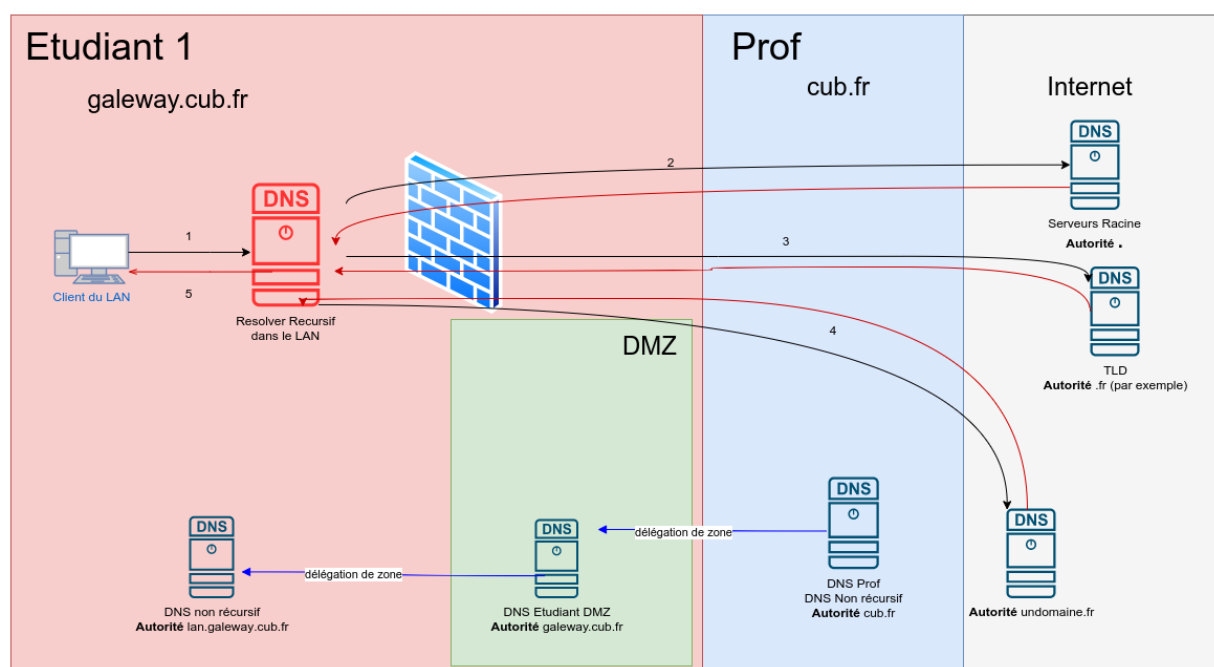
Documents

Document 1 : Présentation du fonctionnement du service DNS au sein de l'entreprise CUB

A) Arborescence DNS



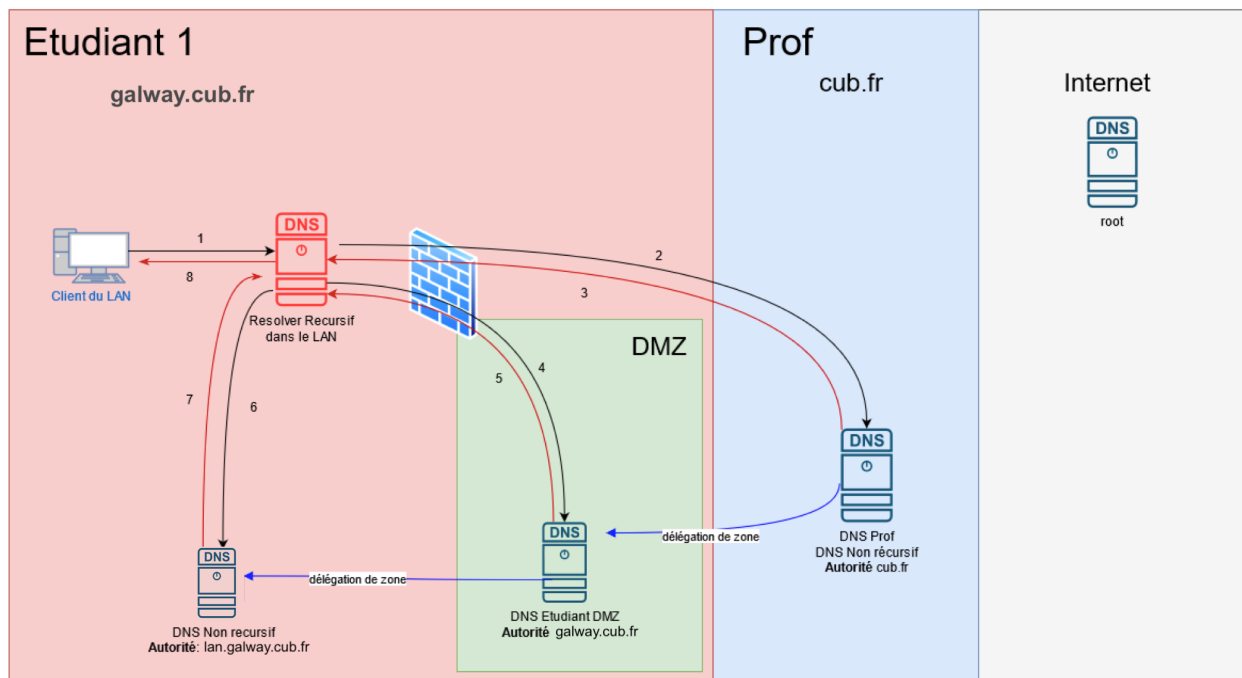
B) Fonctionnement global de la résolution DNS



1. Le client du LAN souhaite obtenir l'adresse IP correspondant au nom de domaine FQDN `www.undomaine.fr` (`www.undomaine.fr. IN A?`). Pour cela, il sollicite le serveur DNS récursif défini dans ses paramètres réseaux.
2. Le serveur récursif vérifie s'il a déjà la réponse dans son cache, ce qui n'est pas le cas. Il décide donc de solliciter le serveur racine le plus proche. Le serveur racine lui indique qu'il ne dispose pas de l'information recherchée mais qu'il connaît les serveurs faisant autorité sur le TLD `.fr`.

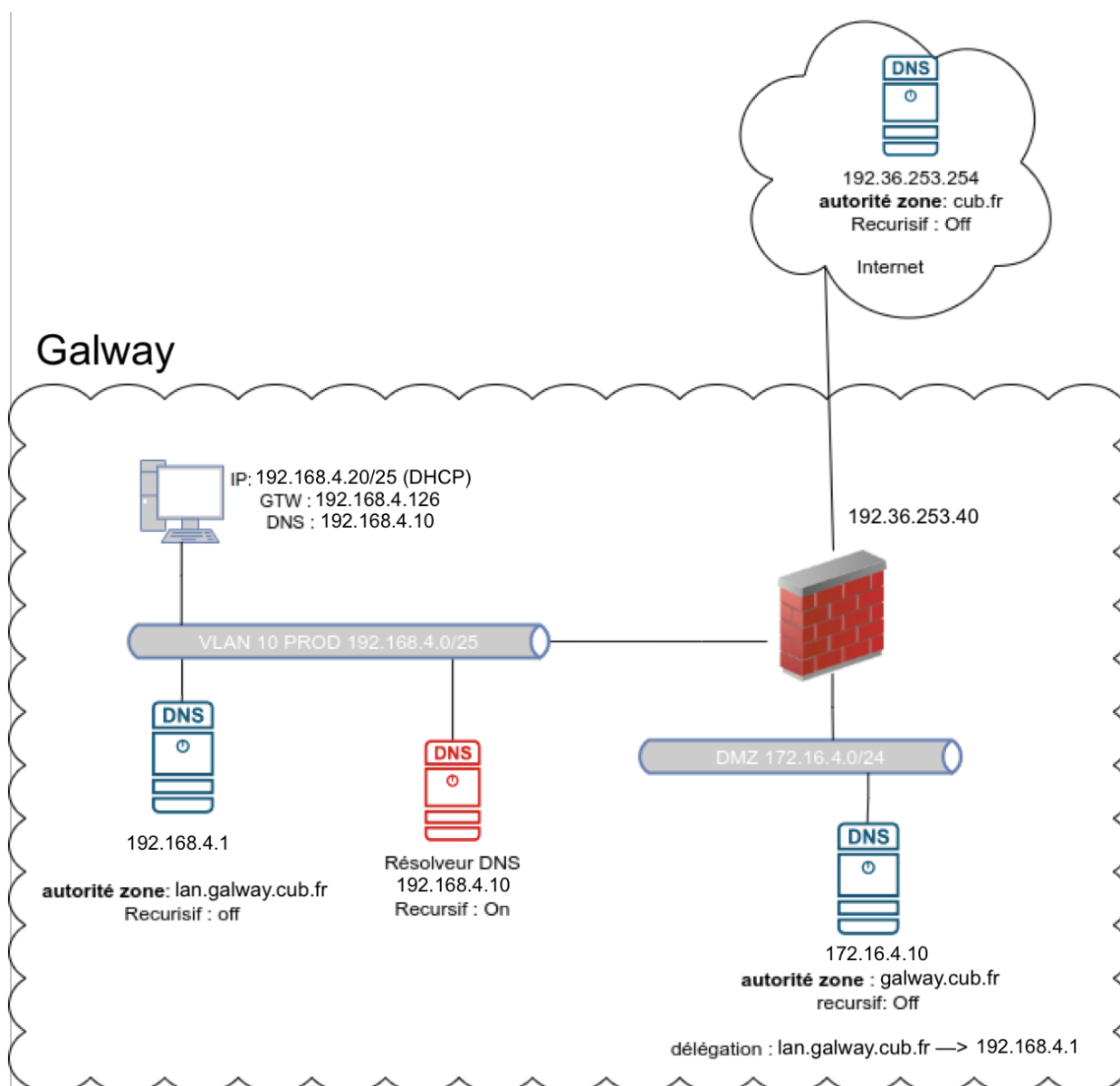
3. Le serveur récursif sollicite maintenant l'un des serveurs faisant autorité sur le TLD .fr. Ce dernier lui indique qu'il n'a pas l'information recherchée mais qu'il connaît le ou les serveurs faisant autorité sur le sous-domaine undomaine.fr.
4. Le serveur récursif contacte ensuite le serveur faisant autorité sur le domaine undomaine.fr. Ce dernier dispose de l'information recherchée dans son fichier de zone sous la forme d'un enregistrement. Il l'a fourni au serveur récursif.
5. Ce dernier stocke l'information dans son cache et la transmet enfin au client.

C) Fonctionnement de la résolution DNS pour le domaine cub.fr



1. Le client souhaite obtenir l'adresse IP correspondant au nom de domaine FQDN dc0.lan.galway.cub.fr (dc0.lan.galway.cub.fr. IN A?) auprès du serveur récursif défini dans ses paramètres réseaux.
2. Le serveur récursif vérifie s'il a déjà la réponse dans son cache, ce qui n'est pas le cas. Il décide donc de solliciter le serveur faisant autorité sur le domaine cub.fr. Attention ! Ce fonctionnement n'est pas le fonctionnement normal d'un serveur récursif qui commencera par contacter l'un des serveurs racines en premier lieu. Dans le cas présent, le domaine cub.fr étant un domaine fictif, nous avons paramétré le serveur récursif pour qu'il sollicite directement le serveur faisant autorité sur ce domaine via les directives « private-zone » et « stub-zone ».
3. Le serveur faisant autorité sur le domaine cub.fr répond au serveur récursif qu'il ne détient pas l'information souhaitée mais qu'il connaît (grâce à la délégation de zone) les serveurs faisant autorité sur galway.cub.fr.
4. Le serveur récursif interroge donc l'un des serveurs faisant autorité sur galway.cub.fr situé dans la DMZ de l'agence.
5. Le serveur faisant autorité sur galway.cub.fr répond au serveur récursif qu'il ne détient pas l'information mais qu'il connaît le ou les serveurs faisant autorité sur le sous-domaine lan.galway.cub.fr.
6. Le serveur récursif interroge ensuite le serveur DNS faisant autorité sur lan.galway.cub.fr.
7. Ce dernier dispose de l'enregistrement (RR) recherché et fournit la réponse au serveur récursif.
8. Le serveur récursif stocke la réponse dans son cache et la transmet au client.

D) Topologie DNS d'une agence



Remarque : la configuration IP des serveurs de la DMZ fait référence à un serveur DNS externe récursif (9.9.9.9). En effet, les serveurs de la DMZ n'ont pas la légitimité à accéder à des serveurs internes.

Document 2 : Création du serveur récursif de l'agence de galway avec Unbound

Il existe une particularité concernant la configuration de ce serveur récursif. En effet, le domaine cub.fr utilisé dans ce contexte étant un domaine fictif, le résolveur ne doit pas utiliser son principe de fonctionnement classique qui consiste à solliciter les serveurs racines.

Nous indiquons donc dans sa configuration que lorsqu'il est interrogé concernant le nom de domaine cub.fr, il doit rediriger la requête vers le serveur DNS présent dans sur le siège.

Nous utilisons la notion de stub-zone et non de forward-zone, car nous souhaitons rediriger la requête vers un serveur faisant autorité. L'utilisation de la notion de forward dans Unbound implique la redirection vers un autre serveur récursif (8.8.8.8, 1.1.1.1, 9.9.9.9 par exemple).

Il n'y a pas de nécessité à réaliser la même opération concernant le domaine lan.galway.cub.fr, car la résolution se fera naturellement par le biais de la délégation de zone.

```
adminleve@dns0:~$ sudo apt update && sudo apt upgrade
adminleve@dns0:~$ sudo apt install unbound dnsutils
```

```
adminleve@dns0:~$ sudoedit /etc/unbound/unbound.conf
```

```
# Unbound configuration file for Debian.
#
# 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: "/etc/unbound/unbound.conf.d/*.conf"
```

```
server:
```

```
interface: 192.168.4.10
interface: 127.0.0.1
```

```
access-control: 192.168.4.0/24 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
# La ligne suivante est à ajouter si le domaine est local et qu'il ne passe pas réellement par la racine
domain-insecure: cub.fr
```

```
stub-zone:
name: "cub.fr."
stub-addr: 192.36.253.254
```

```
adminleve@dns0:~$ sudo mkdir /var/log/unbound
adminleve@dns0:~$ sudo touch /var/log/unbound/unbound.log
adminleve@dns0:~$ sudo chown -R unbound:unbound /var/unbound
adminleve@dns0:~$ sudo systemctl restart unbound
```

Document 3 : Création du serveur faisant autorité sur le domaine galway.cub.fr avec Bind9

```
adminелеve@ns0:~$ sudo apt update && sudo apt upgrade
```

```
adminелеve@ns0:~$ sudo apt install bind9 dnsutils
```

```
adminелеve@ns0:~$ sudoedit /etc/bind/named.conf.options
```

```
options {
    directory "/var/cache/bind";
    listen-on port 53 { 127.0.0.1; 172.16.4.10; };
    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;
    recursion no;
    version none;
};
```

```
adminелеve@ns0:~$ sudoedit /etc/bind/named.conf.local
```

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

```
zone "galway.cub.fr" {
    type master;
    file "/var/cache/bind/db.galway.cub.fr";
};
```

```
adminелеve@ns0:~$ sudoedit /var/cache/bind/db.galway.cub.fr
```

```
$TTL 43200 ; 12 heures
```

```
galway.cub.fr. IN SOA ns0.galway.cub.fr. postmaster.galway.cub.fr. (
    2021040102 ; Serial
    1D ; Refresh
    1H ; Retry
    1W ; Expire
    3H ) ; Negative Cache TTL
```

```
galway.cub.fr.    IN  NS  ns0.galway.cub.fr.
ns0               IN  A   192.36.253.40
www               IN  A   192.36.253.40

lan.galway.cub.fr. IN  NS  ns0.lan.galway.cub.fr.
ns0.lan           IN  A   192.168.4.1
```

Pour que les serveurs DNS et Web puissent être accessibles en dehors du réseau local, il est nécessaire qu'ils aient une adresse IP publique → Les règles de redirection qui seront mises en place sur le pare-feu permettront d'atteindre les serveurs via leur adresse IP privée.

```
adminелеve@ns0:~$ sudo named-checkconf -z
```

```
zone galway.cub.fr/IN: loaded serial 2021040102
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
```

```
adminleve@ns0:~$ sudo systemctl restart bind9
```

Document 4 : Configuration du serveur faisant autorité sur le domaine cub.fr avec Bind9 (réalisé par le professeur)

Concernant le concept de délégation de zone, il existe deux enregistrements importants :

- L'enregistrement correspondant à la délégation (galway.cub.fr. IN NS ns0.galway.cub.fr.) ;
- L'enregistrement de type glue (appelé glue record) qui est indispensable afin de préciser l'adresse IP correspondante au nom de domaine ns0.galway.cub.fr. Cet enregistrement est obligatoire car ns0.galway.cub.fr fait partie du domaine cub.fr. Si nous utilisons comme serveur faisant autorité un serveur correspondant à un autre domaine, il ne serait pas nécessaire de le créer (ex : ns6.gandi.net).

```
adminprof@ns0:~$ sudo apt update && sudo apt upgrade
adminprof@ns0:~$ sudo apt install bind9 dnsutils
```

```
adminprof@ns0:~$ sudoedit /etc/bind/named.conf.options
```

```
options {
    directory "/var/cache/bind";
    listen-on port 53 { 127.0.0.1; 172.16.250.10; };
    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;
    recursion no;
    version none;
};
```

```
adminprof@ns0:~$ sudoedit /etc/bind/named.conf.local
```

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "cub.fr" {
    type master;
```

```

    file "/var/cache/bind/db.cub.fr";
};

adminелеve@ns0:~$ sudo nano /var/cache/bind/db.cub.fr

$TTL 43200; 12 heures

cub.fr. IN SOA ns0.cub.fr. postmaster.cub.fr. (
    2021040101 ; Serial
    1D ; Refresh
    1H ; Retry
    1W ; Expire
    3H ); Negative Cache TTL

cub.fr.      IN  NS  ns0.cub.fr.
ns0          IN  A   192.36.253.254
www          IN  A   192.36.253.254

anvers.cub.fr.  IN  NS  ns0.anvers.cub.fr.
ns0.anvers     IN  A   192.36.253.10

barcelone.cub.fr. IN  NS  ns0.barcelone.cub.fr.
ns0.barcelone  IN  A   192.36.253.20

californie.cub.fr. IN  NS  ns0.californie.cub.fr.
ns0.californie IN  A   192.36.253.30

galway.cub.fr.  IN  NS  ns0.galway.cub.fr.
ns0.galway     IN  A   192.36.253.40

edimbourg.cub.fr. IN  NS  ns0.edimbourg.cub.fr.
ns0.edimbourg  IN  A   192.36.253.50

frankfurt.cub.fr. IN  NS  ns0.frankfurt.cub.fr.
ns0.frankfurt  IN  A   192.36.253.60

dortmund.cub.fr. IN  NS  ns0.dortmund.cub.fr.
ns0.dortmund   IN  A   192.36.253.70

hong-kong.cub.fr. IN  NS  ns0.hong-kong.cub.fr.
ns0.hong-kong  IN  A   192.36.253.80

adminprof@ns0:~$ sudo named-checkconf -z
zone cub.fr/IN: loaded serial 2021040101
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1

adminprof@ns0:~$ sudo systemctl restart bind9 restart

```


Document 5 : Le cas particulier du réseau Wan-CUB

Plutôt que d'utiliser des vues afin de fournir un fichier de zone pour le réseau public et un fichier de zone pour le réseau privé avec des enregistrements différents. Nous avons fait le choix de créer un sous-domaine spécifique pour le réseau privé et l'utilisation d'adresses IP privées non routables sur Internet.¹

Un serveur DNS doit être configuré afin qu'il fasse autorité sur le domaine lan.galway.cub.fr. La récursivité sera désactivée afin que ce dernier respecte les bonnes pratiques en matière de service DNS.²

Pour que la résolution d'adresses IP privées n'entraîne pas une alarme et un blocage au niveau de l'IPS du pare-feu. Il sera nécessaire d'inclure notre nom de domaine dans une liste blanche spécifique.

The screenshot displays the EVA1 FW_GALEWAY configuration interface. The left sidebar shows the navigation menu with 'Protocoles' selected. The main area shows the 'PROTECTION APPLICATIVE / PROTOCOLES' section with 'DNS' selected. The right pane shows the 'IPS' configuration for 'dns_00', including a 'Liste blanche de domaines DNS (DNS rebinding)' with 'galeway.cub.fr' and 'cub.fr' added, and a table of 'Types d'enregistrements DNS'.

Type	Code	Action
A	1	Analyser
A6	38	Analyser

Il est nécessaire également de réaliser une **règle de redirection de ports NAPT** permettant de rediriger toutes les requêtes DNS émises depuis le serveur DNS récursif du réseau local (ex : VLAN Production galway) à destination de l'adresse externe du pare-feu (out – 192.36.253.40 pour galway) sur le port 53 vers le serveur DNS faisant autorité hébergé en DMZ toujours sur le port 53.

En effet, c'est bien l'adresse IP publique du pare-feu que nous avons déclarée comme enregistrement dans le fichier de zone du serveur DNS parent cub.fr :

```
galway.cub.fr.    IN  NS  ns0.galway.cub.fr.
ns0.galway       IN  A   192.36.253.40
```

Pour atteindre le serveur de la DMZ, le serveur récursif envoie donc une requête DNS sur cette adresse IP.



De même, pour atteindre le service Web de galway, installé en DMZ, depuis l'intérieur et l'extérieur, le nom DNS (www.galway.cub.fr) pointe vers 192.36.253.40 : une règle NAPT est là aussi indispensable.

1 <https://www.bortzmeyer.org/pas-de-tld-interne.html>

2 <https://www.bortzmeyer.org/separer-resolveur-autorite.html>