Table des matières :

Présentation 1

Prérequis 2

Configuration du service DHCP 4

Configuration du service DNS 8

Présentation

La redondance croisée est une approche efficace pour assurer la disponibilité des services réseau en entreprise. Elle permet de répartir les rôles entre plusieurs serveurs afin d'éviter un point unique de défaillance.

Dans cette configuration, deux solutions open-source sont utilisées :

- ISC-DHCP-Server : Un serveur DHCP robuste permettant d'attribuer automatiquement des adresses IP aux clients du réseau.
- BIND9 : Un serveur DNS performant et largement utilisé pour la résolution de noms de domaine.

Le serveur DHCP principal est configuré comme DNS secondaire, tandis que le DNS principal joue également le rôle de serveur DHCP secondaire. Cette architecture garantit une continuité de service en cas de panne, renforçant la résilience et la stabilité du réseau.

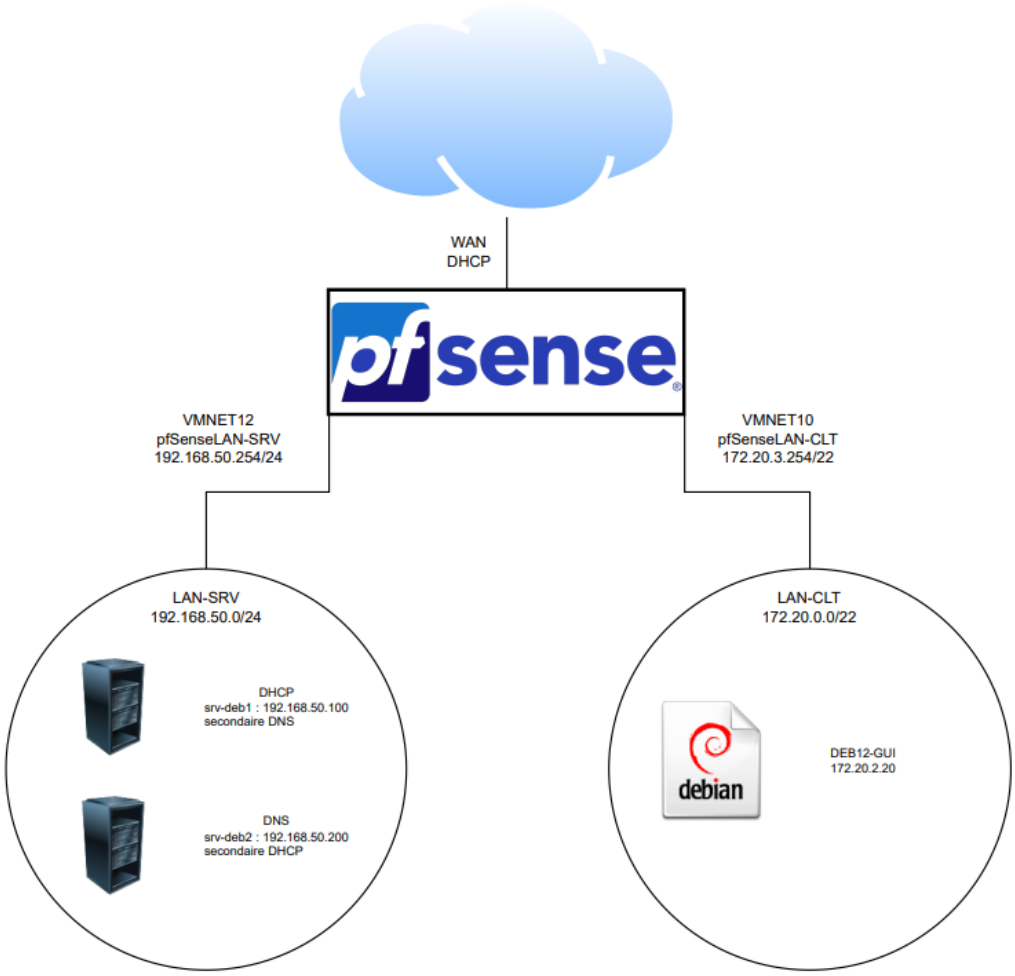
Prérequis :

Nous aurons besoin d'un routeur pF SENSE, de deux serveurs linux non-graphiques et d'un client Debian pour les tests.

Nous utilisons seulement deux serveurs non-graphiques afin de minimiser les coûts matériels.

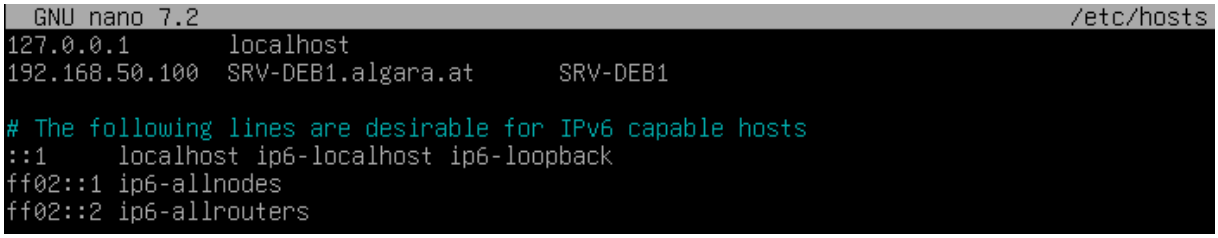
Ces deux serveurs devront avoir les packages **isc-dhcp-server** ainsi que **bind9** de préinstallés.

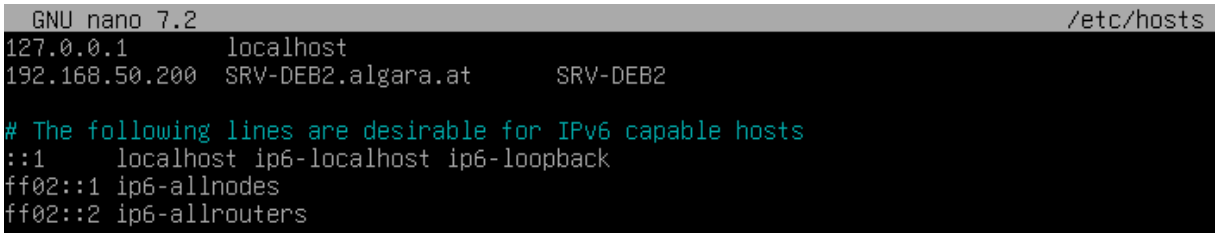
Le routeur pfSENSE devra être configuré selon le schéma réseau suivant :



Premièrement nous configurons le fichiers **/etc/hosts** de nos deux serveurs :

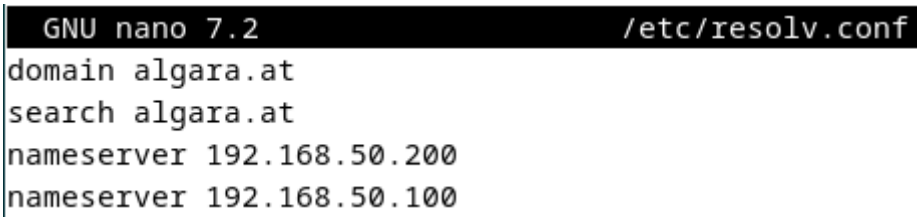
```
sudo nano /etc/hosts
```





Puis le fichier **/etc/resolv.conf** de notre client Debian :

```
sudo nano /etc/resolv.conf
```



Configuration du service DHCP :

Voici la configuration du serveur principal dhcp via le fichier de configuration **/etc/dhcp/dhpd.conf**

Nous y indiquons quel est le serveur principal et quel est le secondaire, puis nous lui donnons une plage d'adresses à distribuer, enfin nous faisons une réservation d'adresse pour notre client.

```
sudo nano /etc/dhcp/dhcpd.conf
```

```
  GNU nano 7.2                                                  /etc/dhcp/dhcpd.conf
option domain-name "algara.at";
option domain-name-servers 192.168.50.100, 192.168.50.200;

default-lease-time 21966;
max-lease-time 42000;

ddns-update-style interim;

authoritative;

log-facility local7;

subnet 192.168.50.0 netmask 255.255.255.0 {
}

failover peer "lancli-failover" {
        primary;
        address 192.168.50.100;
        port 647;

        peer address 192.168.50.200;
        peer port 647;

        max-response-delay 60;
        max-unacked-updates 10;
        load balance max seconds 3;
        mclt 3600;
        split 128;
}

subnet 172.20.0.0 netmask 255.255.252.0 {
        option routers 172.20.3.254;
        pool {
                failover peer "lancli-failover";
                range 172.20.3.1 172.20.3.253;
                host DEB12-GUI {
                        hardware ethernet 00:0c:29:f9:50:07;
                        fixed-address 172.20.2.20;
                        }
        }
}
```

Voici la configuration du serveur dhcp secondaire, via le fichier **/etc/dhcp/dhcpd.conf**

```
sudo nano /etc/dhcp/dhcpd.conf
```

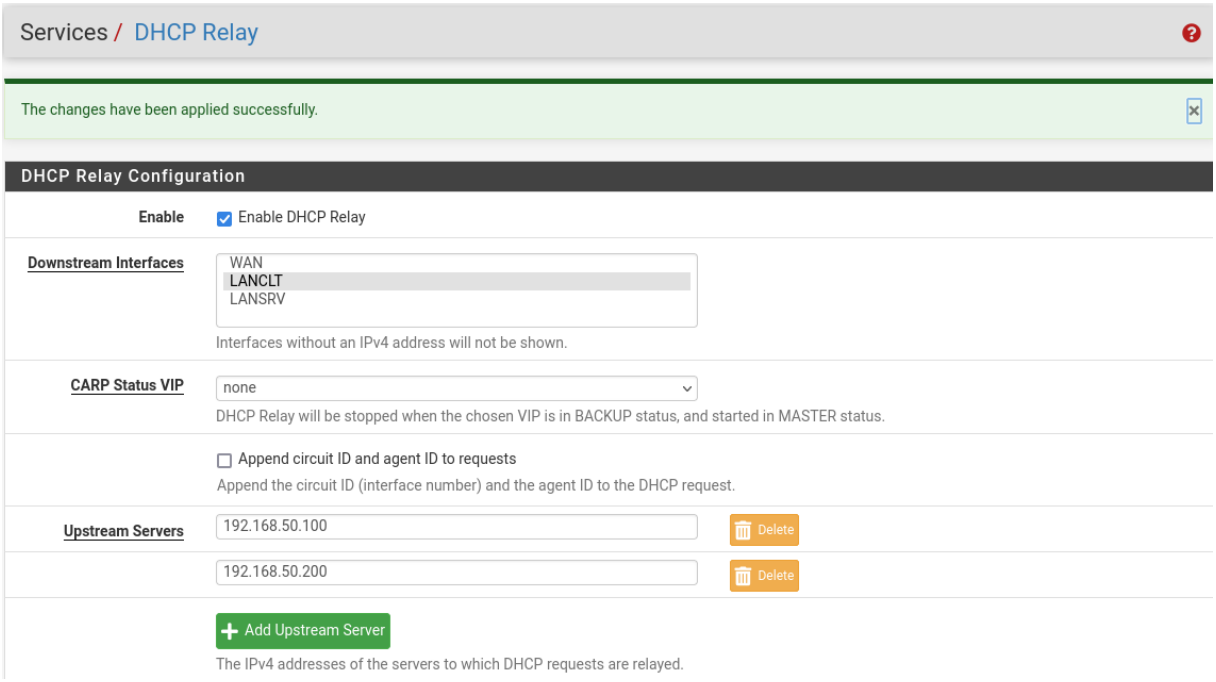
```
  GNU nano 7.2                                                  /etc/dhcp/dhcpd.conf
option domain-name "algara.at";
option domain-name-servers 192.168.50.100, 192.168.50.200;

default-lease-time 21966;
max-lease-time 42000;

ddns-update-style interim;

#authoritative;

log-facility local7;

subnet 192.168.50.0 netmask 255.255.255.0 {
}

failover peer "lancli-failover" {
        secondary;
        address 192.168.50.200;
        port 647;

        peer address 192.168.50.100;
        peer port 647;

        max-response-delay 60;
        max-unacked-updates 10;
        load balance max seconds 3;
}

subnet 172.20.0.0 netmask 255.255.252.0 {
        option routers 172.20.3.254;
        pool {
                failover peer "lancli-failover";
                range 172.20.3.1 172.20.3.253;
                host DEB12-GUI {
                        hardware ethernet 00:0c:29:f9:50:07;
                        fixed-address 172.20.2.20;
                        }
        }
}
```

Une fois le fichier dhcpd.conf configuré, il est nécessaire de configurer la ou les interfaces sur lesquelles le service doit être à l'écoute, via le fichier **/etc/default/isc-dhcp-server**, sur les deux serveurs dhcp :

```
sudo nano /etc/default/isc-dhcp-server
```

```
  GNU nano 7.2                                          /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""
```

Enfin, nous devons activer le relay DHCP sur notre router pfSENSE :



Vérifions que notre client possède la bonne adresse ip, en faisant un release renew à la linux :

```
sudo nano /etc/default/isc-dhcp-server
```

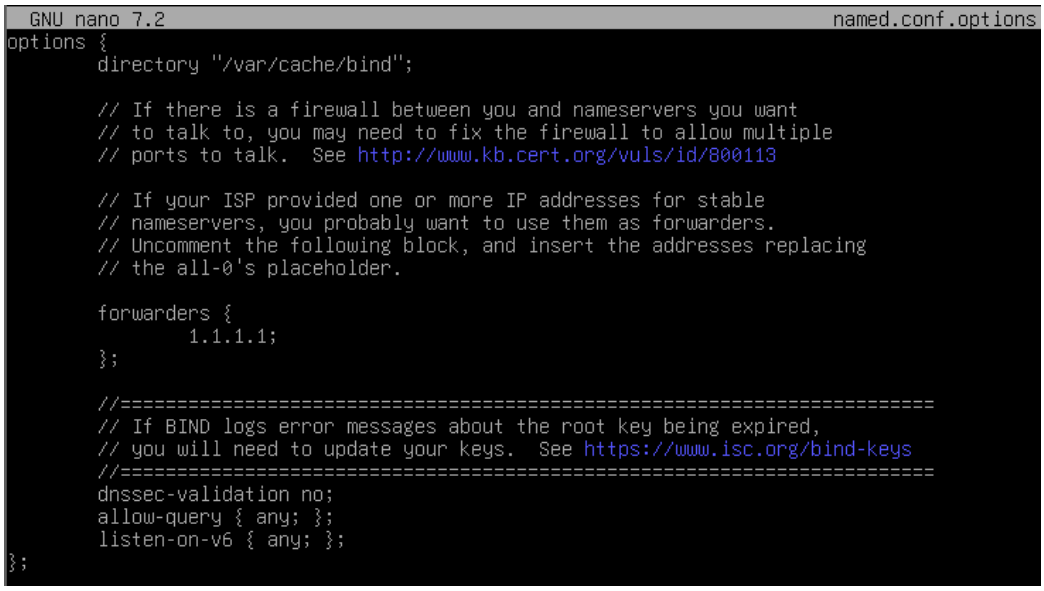
```
root@DEB12-GUI:~# dhclient -r
Killed old client process
root@DEB12-GUI:~# dhclient
root@DEB12-GUI:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f9:50:07 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.20.2.20/22 brd 172.20.3.255 scope global dynamic ens33
       valid_lft 18760sec preferred_lft 18760sec
```

Configuration du service DNS :

Nous allons maintenant configurer le service DNS tel que le srv-deb2 soit le serveur DNS principal.

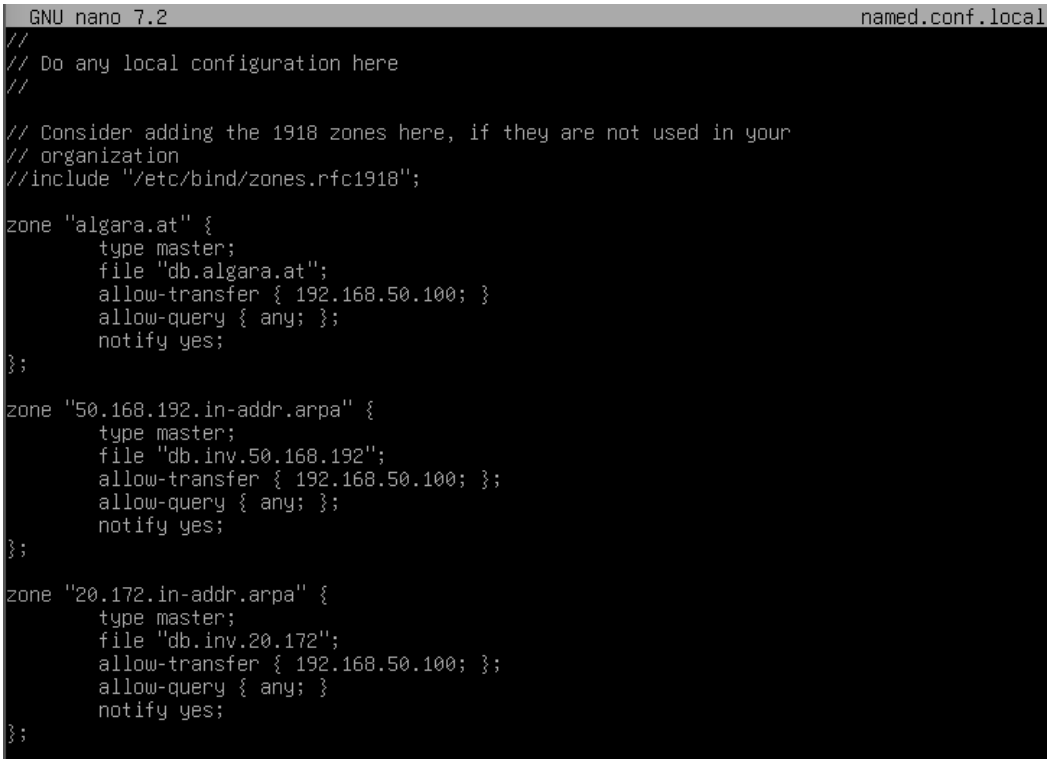
Premièrement, nous allons créer une redirection non-conditionnelle afin de rediriger de façon permanente le trafic d'un nom de domaine vers un autre grâce au fichier :
/etc/bind/named.conf.options

```
sudo nano /etc/bind/named.conf.options
```



Voici la configuration du fichier **/etc/bind/named.conf.local** du serveur principal. Ce fichier permet d'indiquer quelles sont nos zones directes et inverses, et d'autoriser le transfert de ces zones à notre serveur secondaire :

```
sudo nano  /etc/bind/named.conf.local
```



Nous allons maintenant créer et configurer les fichiers de configuration de nos zones. Pour cela nous avons à disposition des exemples de ces fichiers dans le dossier **/etc/bind**, à copier dans le dossier **/var/cache/bind/** afin de récupérer les en-têtes SOA et NS :

```
cp db.local /var/cache/bind/db.algara.at
```

```
root@SRV-DEB2:/etc/bind# ls
bind.keys  db.0  db.127  db.255  db.empty  db.local  named.conf  namec
root@SRV-DEB2:/etc/bind# cat db.local
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
root@SRV-DEB2:/etc/bind# cp db.local /var/cache/bind/db.algara.at
```

De même pour nos zones inverses :

```
cp db.local /var/cache/bind/db.inv.50.168.192

cp db.local /var/cache/bind/db.inv.20.172
```

Configurons notre fichier de zone directe **/var/cache/bind/db.algara.at** :

```
sudo nano  /var/cache/bind/db.algara.at
```

```
  GNU nano 7.2                                                  db.algara.at
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     srv-deb2.algara.at. root.srv-deb2.algara.at. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      srv-deb2.algara.at.
@       IN      A       192.168.50.200
@       IN      NS      srv-deb1.algara.at.
@       IN      A       192.168.50.100
@       IN      AAAA    ::1
srv-deb2        IN      A       192.168.50.200
srv-deb1        IN      A       192.168.50.100
WAN     IN      A       192.168.255.234
LANSRV  IN      A       192.168.50.254
LANCLT  IN      A       172.20.3.254
```

Puis nos zones inverses :

/var/cache/bind/db.inv.50.168.192 :

```
sudo nano  /var/cache/bind/db.inv.50.168.192
```

```
  GNU nano 7.2                                              db.inv.50.168.192
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     srv-deb2.algara.at. root.algara.at. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      srv-deb2.algara.at.
@       IN      NS      srv-deb1.algara.at.
200     IN      PTR     srv-deb2.algara.at.
100     IN      PTR     srv-deb1.algara.at.
254     IN      PTR     lansrv.algara.at._
@       IN      AAAA    ::1
```

/var/cache/bind/db.inv.20.172 :

```
sudo nano  /var/cache/bind/db.inv.20.172
```

```
 GNU nano 7.2                                                /var/cache/bind/db.inv.20.172
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     srv-deb2.algara.at. root.algara.at. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      srv-deb2.algara.at.
@       IN      NS      srv-deb1.algara.at.
srv-deb2        IN      A       192.168.50.200
srv-deb1        IN      A       192.168.50.100
lanclt  IN      A       172.20.3.254
254.3   IN      PTR     lanclt.algara.at.
20.2    IN      PTR     deb12-gui
```

Chargeons les changements de configurations grâce à la commande : **rndc reload** puis testons nos fichiers grâce aux commandes : **named-checkconf -z** et **named-checkzone algara.at /var/cache/bind/db.algara.at** :

```
rndc reload

named-checkconf -z

named-checkzone algara.at /var/cache/bind/db.algara.at
```

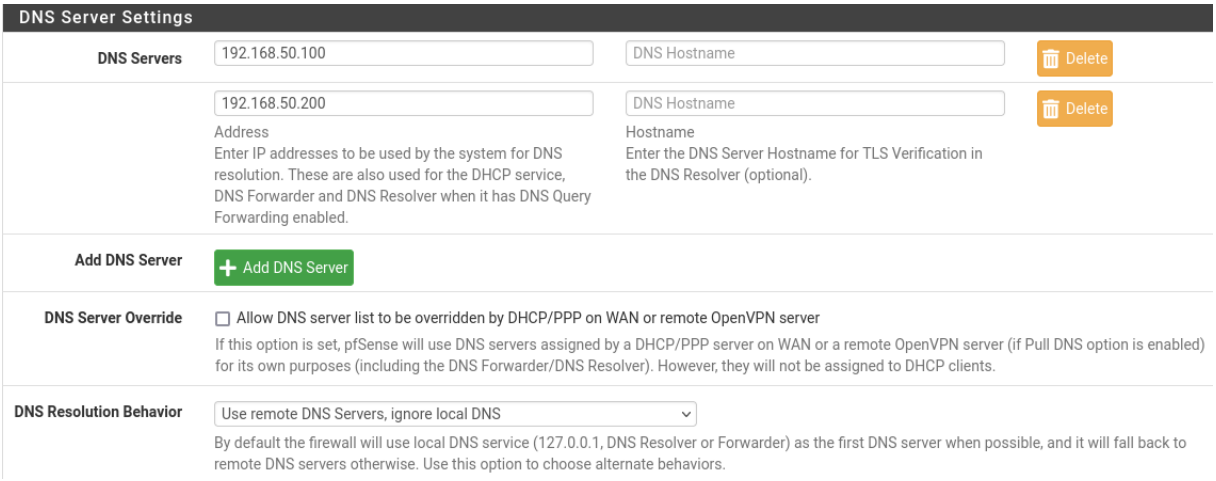
```
root@SRV-DEB2:/var/cache/bind# rndc reload
server reload successful
root@SRV-DEB2:/var/cache/bind# named-checkconf -z
zone algara.at/IN: loaded serial 2
zone 50.168.192.in-addr.arpa/IN: loaded serial 2
zone 20.172.in-addr.arpa/IN: 2.20.20.172.in-addr.arpa/NS 'deb12-gui.20.172.in-addr.arpa' has no address records (A or AA
zone 20.172.in-addr.arpa/IN: loaded serial 2
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
root@SRV-DEB2:/var/cache/bind# named-checkzone algara.at /var/cache/bind/db.algara.at
zone algara.at/IN: loaded serial 2
OK
```

Configurons maintenant notre serveur DNS secondaire srv-deb1 via le fichier **/etc/bind/named.conf.local** :

```
sudo nano  /etc/bind/named.conf.local
```

```
  GNU nano 7.2                                                /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 "algara.at" {
        type slave;
        masters { 192.168.50.200; };
        file "db.algara.at";
        allow-query { any; };
};

zone "50.168.192.in-addr.arpa" {
        type slave;
        masters { 192.168.50.200; };
        file "db.inv.50.168.192";
        allow-query { any; };
};

zone "20.172.in-addr.arpa" {
        type slave;
        masters { 192.168.50.200; };
        file "db.inv.20.172";
        allow-query { any; };
};
```

Ne pas oublier de renseigner nos deux serveurs DNS dans les paramètres généraux de notre pfSENSE :



La configuration étant terminée, nous pouvons tester la résolution de nos différent appareils réseaux sur notre client Debian grâce à la commande nslookup :

```
root@DEB12-GUI:~# nslookup srv-deb1
Server:         192.168.50.200
Address:        192.168.50.200#53

Name:   srv-deb1.algara.at
Address: 192.168.50.100

root@DEB12-GUI:~# nslookup srv-deb2
Server:         192.168.50.200
Address:        192.168.50.200#53

Name:   srv-deb2.algara.at
Address: 192.168.50.200

root@DEB12-GUI:~# nslookup 192.168.50.100
100.50.168.192.in-addr.arpa     name = srv-deb1.algara.at.

root@DEB12-GUI:~# nslookup 192.168.50.200
200.50.168.192.in-addr.arpa     name = srv-deb2.algara.at.
```

```
root@DEB12-GUI:~# nslookup lansrv
Server:         192.168.50.200
Address:        192.168.50.200#53

Name:   LANSRV.algara.at
Address: 192.168.50.254

root@DEB12-GUI:~# nslookup lanclt
Server:         192.168.50.200
Address:        192.168.50.200#53

Name:   LANCLT.algara.at
Address: 172.20.3.254

root@DEB12-GUI:~# nslookup 192.168.50.254
254.50.168.192.in-addr.arpa     name = lansrv.algara.at.

root@DEB12-GUI:~# nslookup 172.20.3.254
254.3.20.172.in-addr.arpa       name = lanclt.algara.at.
```