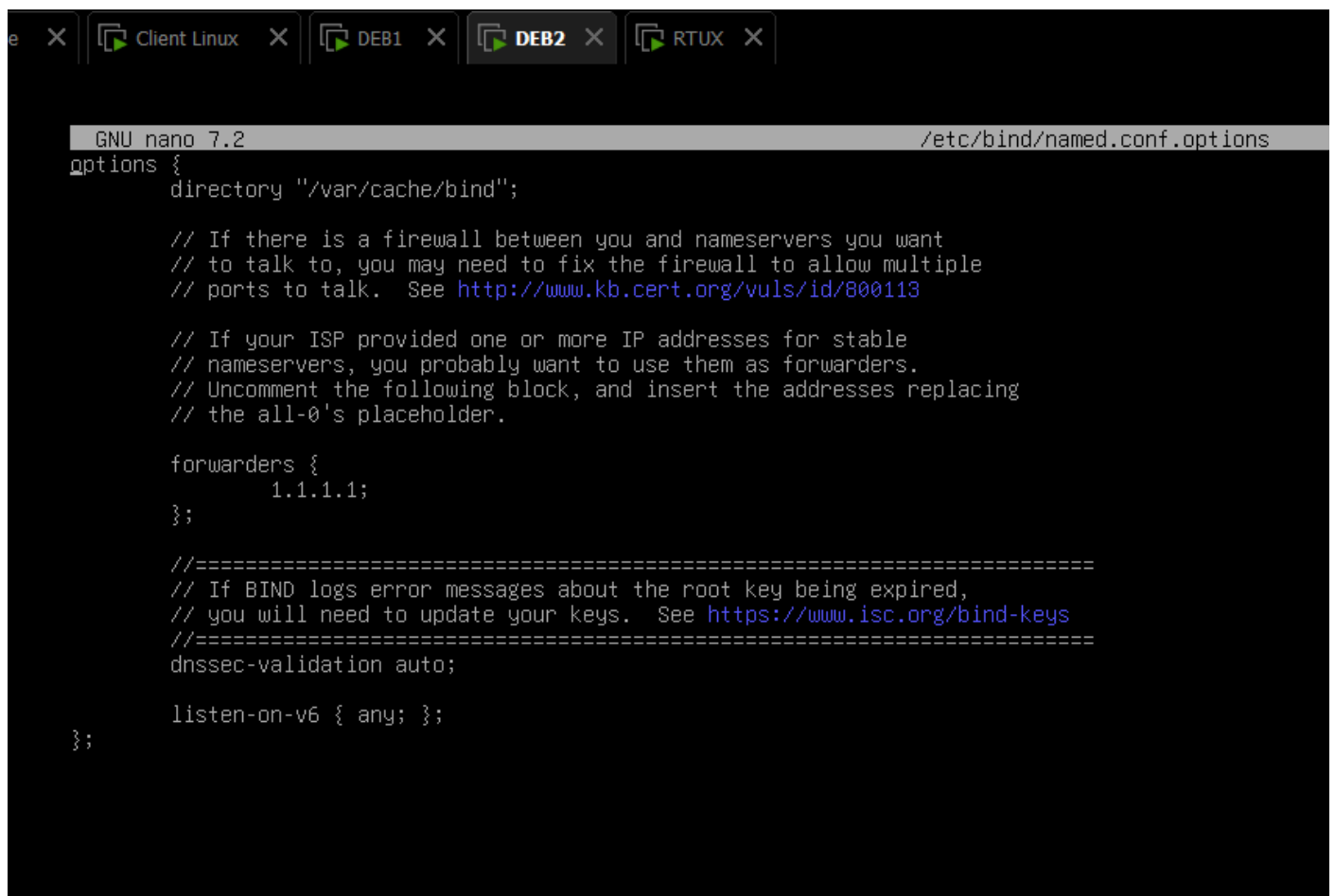


Mise en place d'un service DNS sous Linux avec des clients sur des réseaux différents

Configuration de SRV-DEB2

1. Configuration des redirecteurs



```
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // 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 {
        1.1.1.1;
    };

    //=====
    // 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;

    listen-on-v6 { any; };
};
```

2.

3. Creation de la zone DNS + enregistrements pour serveurs et interfaces RTUX de la LAN

```
GNU nano 7.2 /etc/bind/db.radouane.yn *
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      srv-deb2.radouane.yn.  admin.radouane.yn. (
                        2      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
; Zone
@         IN      NS       srv-deb2.radouane.yn.

; Serveurs
srv-deb1  IN      A        172.20.30.1
srv-deb2  IN      A        172.20.30.2

; Interfaces RTUX
rtux-clients IN      A        172.18.127.254
rtux-pfsense IN      A        172.20.20.6
rtux-servers IN      A        172.20.30.14

; Interface LAN PfSense
pfsense   IN      A        172.20.20.2

; Alias pour srv-deb1
www        IN      CNAME    srv-deb1_

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler  M-A Marq
^X Quitter   ^R Lire fich. ^_ Remplacer ^U Coller    ^J Justifier ^_ Aller ligne M-E Refaire  M-6 Copi
```

4. Modification du service DHCP pour qu'il fournisse le DNS du SRV-DEB2

```
DEB1 - VMware Workstation
File Edit View VM Tabs Help
GNU nano 7.2 /etc/dhcp/dhcpd.conf *
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "radouane.yn";
option domain-name-servers 172.20.30.2, 1.1.1.1;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
```

Configuration de PfSense

Non sécurisé http://172.20.20.2/system.php 110 %

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / **General Setup**

System

Hostname
Name of the firewall host, without domain part.

Domain
Domain name for the firewall.

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is **widely used** by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

DNS Server Settings

DNS Servers	<input type="text" value="172.20.30.2"/>	<input type="text" value="1.1.1.1"/>	<input type="text" value="none"/>
Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it	Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).	Gateway Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.	

Test de la résolution (depuis le client)

```
root@debian:/home/youss# sudo systemctl restart networking
root@debian:/home/youss# cat /etc/resolv.conf
domain radouane.yr
search radouane.yr
nameserver 172.20.30.2
nameserver 1.1.1.1
root@debian:/home/youss#
```

Tester depuis les clients

1. DIG radouane.yr SOA

```
root@debian:/home/youss# dig radouane.yr SOA

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> radouane.yr SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17545
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c3f5f94259bee6b70100000068ecf766d7ab943a0b794f41 (good)
;; QUESTION SECTION:
;radouane.yr.                IN      SOA

;; ANSWER SECTION:
radouane.yr.                604800  IN      SOA      srv-deb2.radouane.yr. admin.radouane.yr. 2 604800 86400 2419200 604800

;; Query time: 3 msec
;; SERVER: 172.20.30.2#53(172.20.30.2) (UDP)
;; WHEN: Mon Oct 13 14:58:14 CEST 2025
;; MSG SIZE rcvd: 119

root@debian:/home/youss#
```

2. DIG radouane.yr SA

```
root@debian:/home/youss# dig radouane.yr NS

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> radouane.yr NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21535
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 93d8fa512af12e870100000068ecf78c932ce870b87c7803 (good)
;; QUESTION SECTION:
;radouane.yr.                IN      NS

;; ANSWER SECTION:
radouane.yr.                604800  IN      NS      srv-deb2.radouane.yr.

;; ADDITIONAL SECTION:
srv-deb2.radouane.yr.      604800  IN      A      172.20.30.2

;; Query time: 3 msec
;; SERVER: 172.20.30.2#53(172.20.30.2) (UDP)
;; WHEN: Mon Oct 13 14:58:52 CEST 2025
;; MSG SIZE rcvd: 107
```

Dans la section ANSWER SECTION, on a bien radouane.yr avec le bon serveur « srv-deb2.radouane.yr » donc tout est bon.

Test des différents enregistrements

Sur le test nslookup j'ai eu cette erreur :

```
root@debian:/home/youss# nslookup srv-deb1.radouane.yr.
;; Got recursion not available from 172.20.30.2, trying next server
Server:          1.1.1.1
Address:         1.1.1.1#53

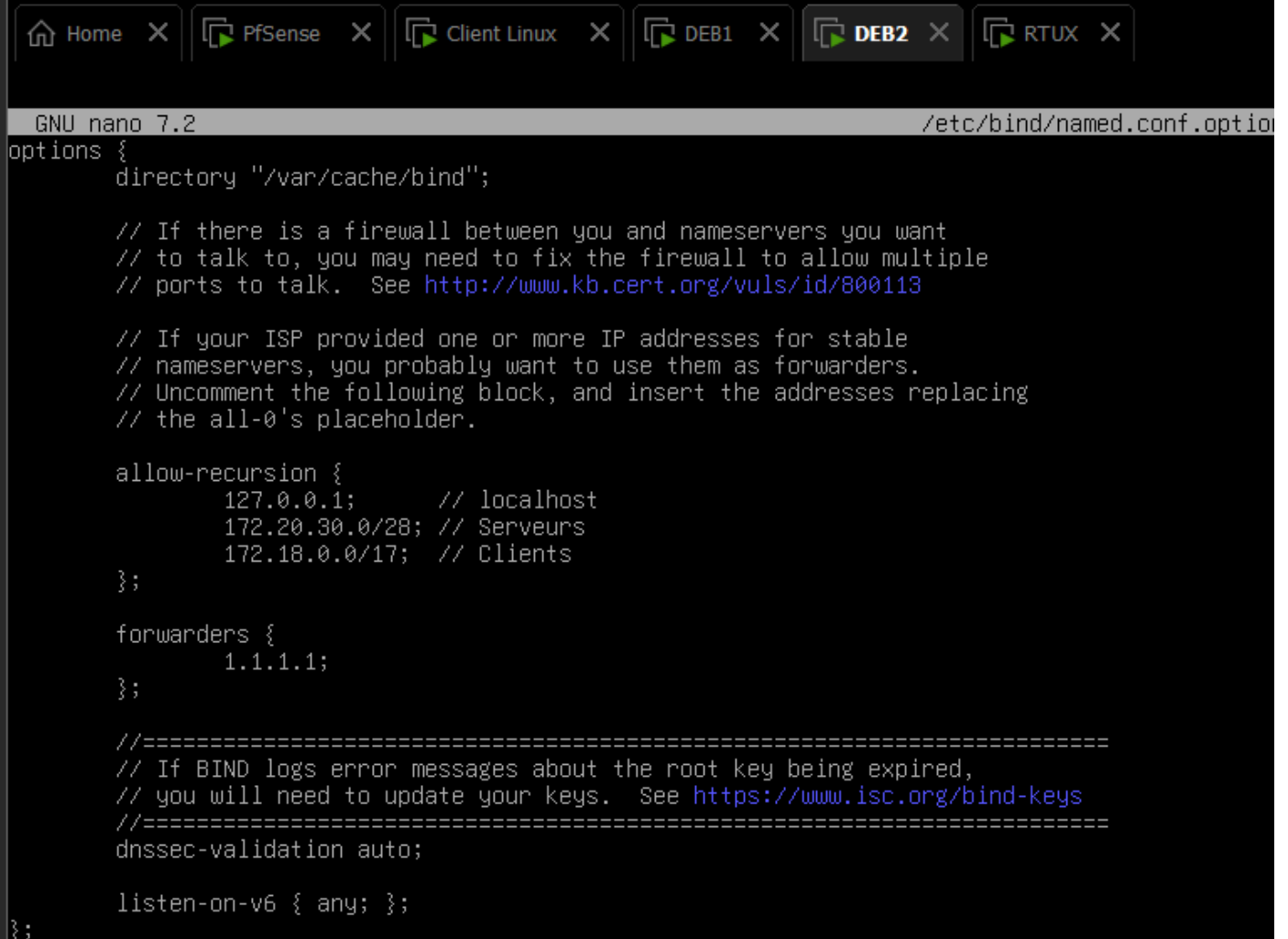
** server can't find srv-deb1.radouane.yr: NXDOMAIN

root@debian:/home/youss# nslookup srv-deb2.radouane.yr.
;; Got recursion not available from 172.20.30.2, trying next server
Server:          1.1.1.1
Address:         1.1.1.1#53

** server can't find srv-deb2.radouane.yr: NXDOMAIN

root@debian:/home/youss#
```

J'ai donc rajouté ça sur le fichier named.conf.options dans DEB2 le fichier /etc/bind/named.conf.options et rajouté le bloc allow-recursion



```
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // 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.

    allow-recursion {
        127.0.0.1;          // localhost
        172.20.30.0/28;    // Serveurs
        172.18.0.0/17;     // Clients
    };

    forwarders {
        1.1.1.1;
    };

    //=====
    // 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;

    listen-on-v6 { any; };
};
```

Les NSLOOKUP fonctionnent désormais

```
root@debian:/home/youss# nslookup srv-deb2.radouane.yr.
Server:          172.20.30.2
Address:         172.20.30.2#53

Name:   srv-deb2.radouane.yr
Address: 172.20.30.2

root@debian:/home/youss# nslookup srv-deb1.radouane.yr.
Server:          172.20.30.2
Address:         172.20.30.2#53

Name:   srv-deb1.radouane.yr
Address: 172.20.30.1
```

Et les DIG donnent la bonne réponse dans ANSWER SECTION

```
root@debian:/home/youss# dig www.radouane.yr

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> www.radouane.yr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15891
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0352788185b820fb0100000068ecfcd2d533a02410e4ff54 (good)
;; QUESTION SECTION:
;www.radouane.yr.                IN      A

;; ANSWER SECTION:
www.radouane.yr.        604800  IN      CNAME   srv-deb1.radouane.yr.
srv-deb1.radouane.yr.  604800  IN      A       172.20.30.1

;; Query time: 0 msec
;; SERVER: 172.20.30.2#53(172.20.30.2) (UDP)
;; WHEN: Mon Oct 13 15:21:22 CEST 2025
;; MSG SIZE rcvd: 111
```

```

root@debian:/home/youss# dig pfsense.radouane.yr

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> pfsense.radouane.yr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46567
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e3ba0499787d0d870100000068ecfcc82ae0ae55f930cc21 (good)
;; QUESTION SECTION:
;pfsense.radouane.yr.          IN      A

;; ANSWER SECTION:
pfsense.radouane.yr.        604800  IN      A      172.20.20.2

;; Query time: 0 msec
;; SERVER: 172.20.30.2#53(172.20.30.2) (UDP)
;; WHEN: Mon Oct 13 15:21:12 CEST 2025
;; MSG SIZE rcvd: 92

```

Test de connectivité

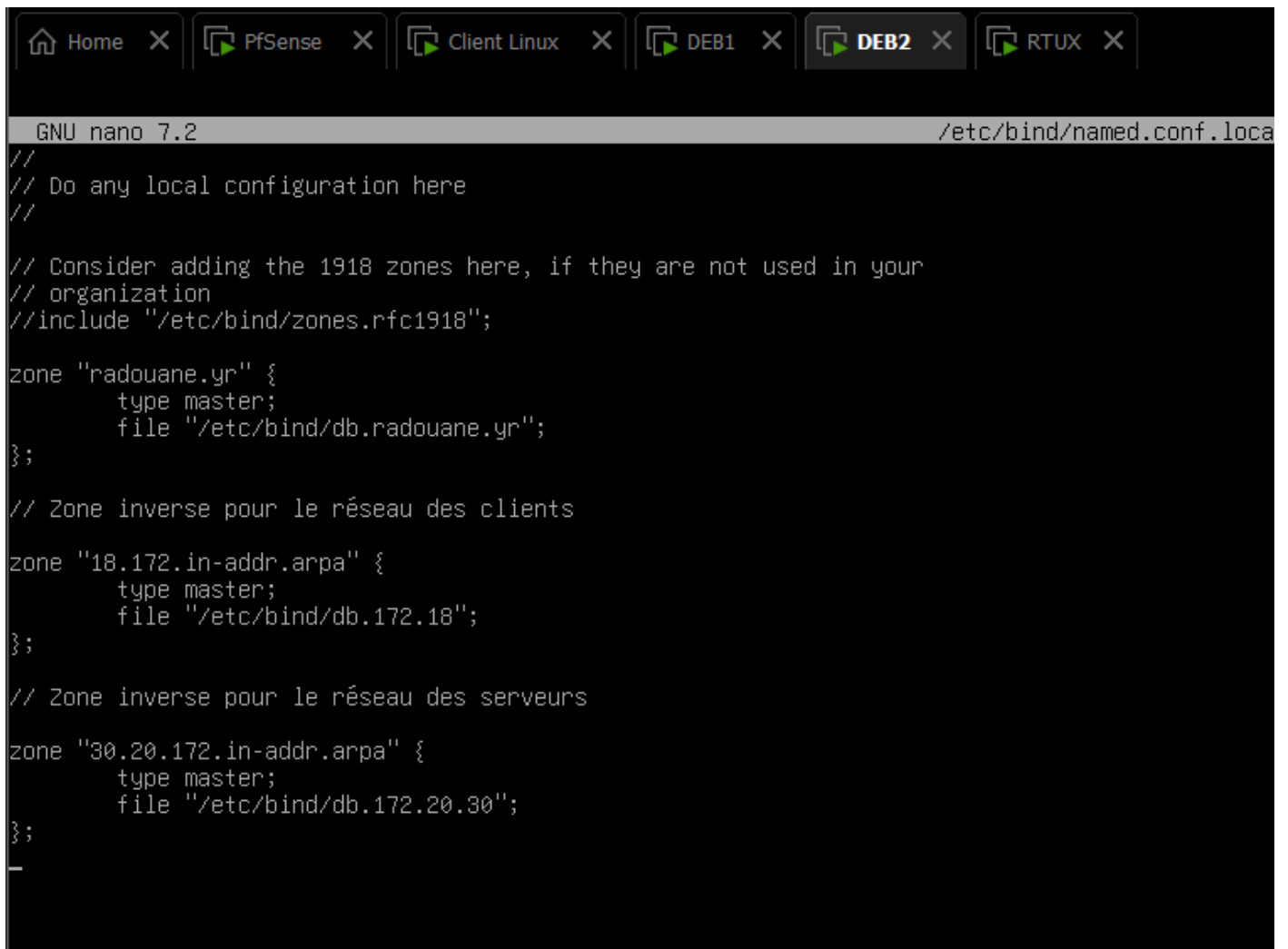
```

root@debian:/home/youss# ping srv-deb1.radouane.yr
PING srv-deb1.radouane.yr (172.20.30.1) 56(84) bytes of data.
64 bytes from 172.20.30.1 (172.20.30.1): icmp_seq=1 ttl=63 time=0.492 ms
64 bytes from 172.20.30.1 (172.20.30.1): icmp_seq=2 ttl=63 time=0.791 ms
64 bytes from 172.20.30.1 (172.20.30.1): icmp_seq=3 ttl=63 time=0.747 ms
^C
--- srv-deb1.radouane.yr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.492/0.676/0.791/0.131 ms
root@debian:/home/youss# ping srv-deb2
PING srv-deb2.radouane.yr (172.20.30.2) 56(84) bytes of data.
64 bytes from 172.20.30.2 (172.20.30.2): icmp_seq=1 ttl=63 time=2.80 ms
64 bytes from 172.20.30.2 (172.20.30.2): icmp_seq=2 ttl=63 time=0.740 ms
64 bytes from 172.20.30.2 (172.20.30.2): icmp_seq=3 ttl=63 time=0.822 ms
^C
--- srv-deb2.radouane.yr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.740/1.454/2.802/0.953 ms
root@debian:/home/youss#

```

Configuration des zones inverses

1. Modification du fichier de configuration



```
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 "radouane.yr" {
    type master;
    file "/etc/bind/db.radouane.yr";
};

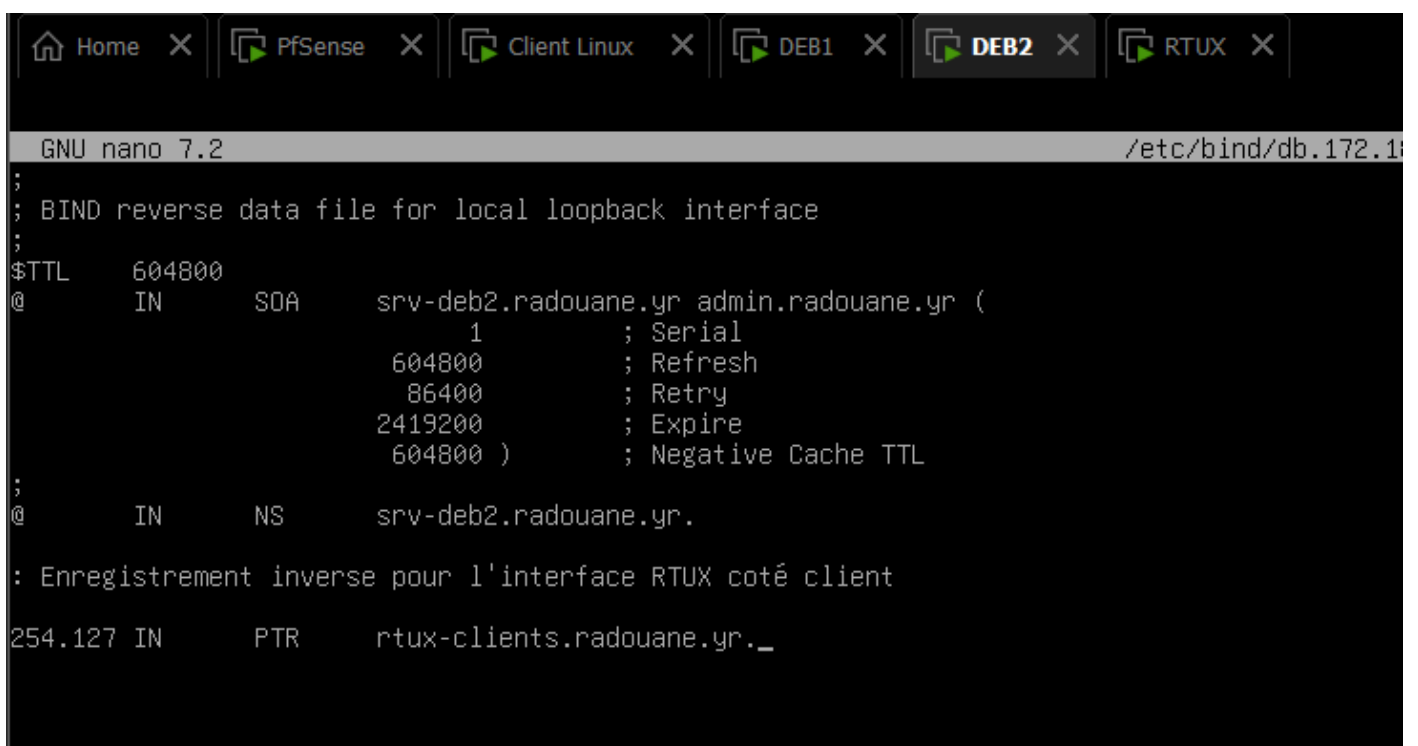
// Zone inverse pour le réseau des clients

zone "18.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.18";
};

// Zone inverse pour le réseau des serveurs

zone "30.20.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.20.30";
};
```

2. Creation des fichiers de zones inverses



```
GNU nano 7.2 /etc/bind/db.172.18
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@        IN      SOA      srv-deb2.radouane.yr admin.radouane.yr (
                        1      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@        IN      NS       srv-deb2.radouane.yr.

: Enregistrement inverse pour l'interface RTUX coté client
254.127 IN      PTR      rtux-clients.radouane.yr._
```



```
GNU nano 7.2 /etc/bind/db.172.20.30
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      srv-deb2.radouane.yr. admin.radouane.yr. (
                        1      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       srv-deb2.radouane.yr.

; Enregistrements PTR pour le LAN Serveurs
1         IN      PTR      srv-deb1.radouane.yr.
2         IN      PTR      srv-deb2.radouane.yr.
14        IN      PTR      rtux-servers.radouane.yr.
```

Tests

```
Home X | PFSense X | Client Linux X | DEB1 X | DEB2 X | RTUX X
root@debian:~# sudo named-checkconf
root@debian:~# sudo named-checkzone 18.172.in-addr.arpa /etc/bind/db.172.18
zone 18.172.in-addr.arpa/IN: loaded serial 1
OK
root@debian:~# sudo named-checkzone 30.20.172.in-addr.arpa /etc/bind/db.172.20.30
zone 30.20.172.in-addr.arpa/IN: loaded serial 1
OK
root@debian:~#
```

Test de résolution depuis le client

```
Home X PfSense X Client Linux X DEB1 X DEB2 X RTUX X
root@debian:/home/youss# dig -x 172.20.30.1

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> -x 172.20.30.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48599
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 023accd6e4bc26050100000068ed0310251d4003fc7b7c56 (good)
;; QUESTION SECTION:
;1.30.20.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.30.20.172.in-addr.arpa. 604800 IN      PTR      srv-deb1.radouane.yr.

;; Query time: 0 msec
;; SERVER: 172.20.30.2#53(172.20.30.2) (UDP)
;; WHEN: Mon Oct 13 15:48:00 CEST 2025
;; MSG SIZE rcvd: 115

root@debian:/home/youss# nslookup 172.20.30.14
14.30.20.172.in-addr.arpa      name = rtux-servers.radouane.yr.

root@debian:/home/youss#
```