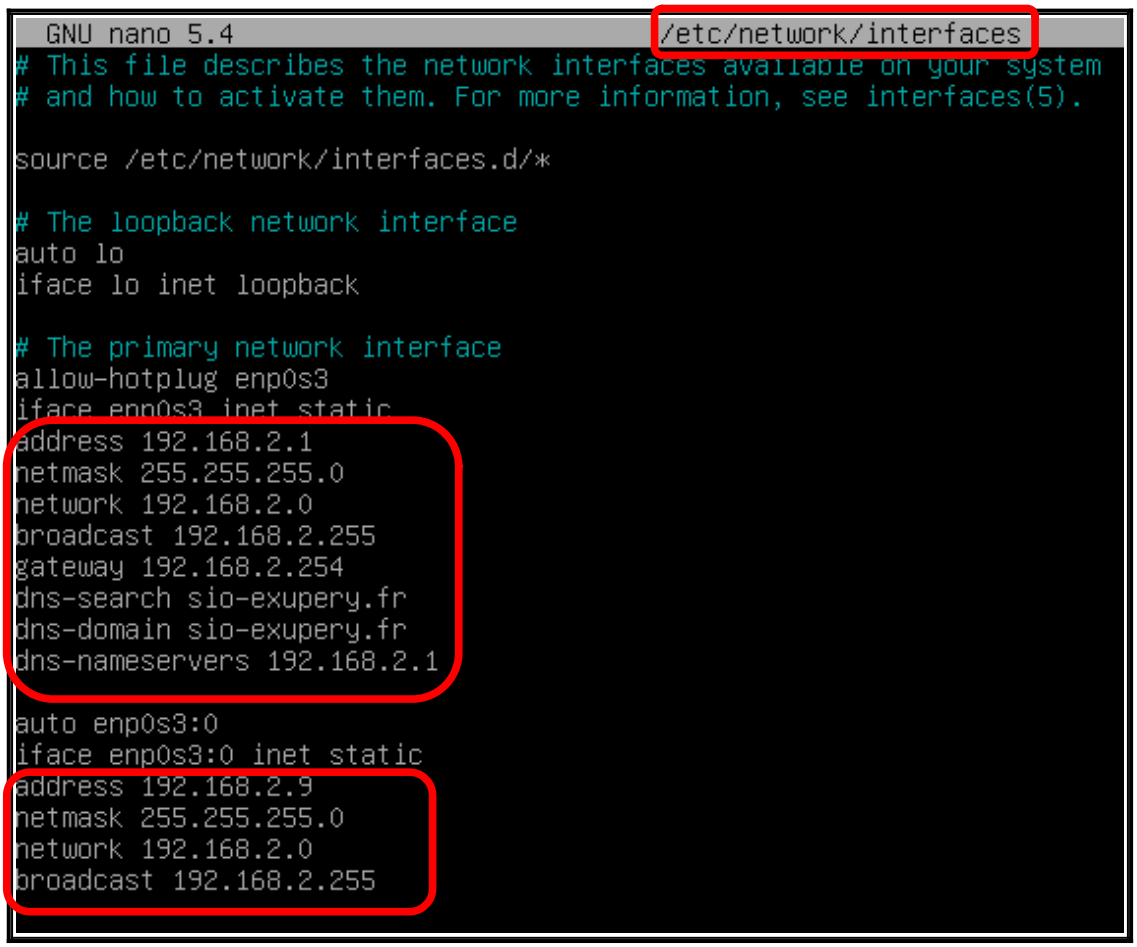
Chapitre 8 – Routage filtrant (pare-feu Iptables)

Sommaire :

2. Modifications sur DS2.



1ère étape : Nous modifions la **configuration IP** de l'interface réseau **enp0s3** ainsi que **enp0s3:0**.

```
root@DS2: ~#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:eb:10:db brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/24 brd 192.168.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.2.9/24 brd 192.168.2.255 scope global secondary enp0s3:0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feeb:10db/64 scope link
       valid_lft forever preferred_lft forever
```

2ème étape : Nous vérifions la bonne prise des **modifications**.

```
 GNU nano 5.4                  /etc/apache2/sites-available/sites-sio.conf *
<VirtualHost 192.168.2.9:80>
        ServerName secu.sio-exupery.fr:443
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/secu
        ErrorLog /var/www/html/web/logs/error.log
        CustomLog /var/www/html/web/logs/access.log combined
        SSLEngine on
        LogLevel info
</VirtualHost>

<VirtualHost 192.168.2.1:80>
        ServerName www.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/web
        ErrorLog /var/www/html/web/logs/error.log
        CustomLog /var/www/html/web/logs/access.log combined
</VirtualHost>

<VirtualHost 192.168.2.1:80>
        ServerName projet1.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/projet1/repweb
        ErrorLog /var/www/html/projet1/repweb/logs/error.log
        CustomLog /var/www/html/projet1/repweb/logs/access.log combined
</VirtualHost>

<VirtualHost 192.168.2.1:80>
        ServerName projet2.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/projet2/repweb
        ErrorLog /var/www/html/projet2/repweb/logs/error.log
        CustomLog /var/www/html/projet2/repweb/logs/access.log combined
</VirtualHost>
```

```
<VirtualHost 192.168.2.1:80>
        ServerName blog.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/sitewordpress/wordpress
        ErrorLog /var/www/html/sitewordpress/wordpress/logs/error.log
        CustomLog /var/www/html/sitewordpress/wordpress/logs/access.log combined
</VirtualHost>
```

3ème étape : Nous modifions l'intégralité des **adresses IP** dans le fichier des **hôtes virtuels**.

```
root@DS2: ~#systemctl reload apache2
```

4ème étape : Nous relançons la configuration **d'apache2**.

```
  GNU nano 5.4                          /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";
//les zones
zone "sio-exupery.fr" IN {
        type master;
        file "db.sio-exupery.fr";
        allow-update { none; };
};

zone "2.168.192.in-addr.arpa" IN {
        type master;
        file "rev.sio-exupery.fr";
        allow-update { none; };
};
```

5ème étape : Nous modifions le fichier ci-dessus contenant les noms de **zones de recherche DNS**.

```
 GNU nano 5.4                          /var/cache/bind/db.sio-exupery.fr *

; Fichier pour la résolution directe
$TTL 86400
@       IN SOA DS2.sio-exupery.fr. root.sio-exupery.fr. (
               2019020701
               1w
               1d
               4w
               1w )
@                               IN NS   DS2.sio-exupery.fr.
intra.sio-exupery.fr            IN NS   DS1.intra.sio-exupery.fr.
DS2.sio-exupery.fr.             IN A    192.168.2.1
DS1.intra.sio-exupery.fr.       IN A    192.168.3.1
ftp                             IN      CNAME DS2
www                             IN      CNAME DS2
secu                            IN A    192.168.2.9
projet1                         IN      CNAME DS2
projet2                         IN      CNAME DS2
blog                            IN      CNAME DS2
```

6ème étape : Cette fois-ci nous modifions le fichier concernant la **zone de recherche directe**.

```
 GNU nano 5.4                          /var/cache/bind/rev.sio-exupery.fr *

; Fichier pour la résolution inverse
$TTL 86400
@       IN SOA  DS2.sio-exupery.fr. root.sio-exupery.fr. (
                2019020701
                1w
                1d
                4w
                1w )
@                       IN NS   DS2.sio-exupery.fr.
1                       IN PTR  DS2.sio-exupery.fr.
```

7ème étape : Même manipulation mais cette fois pour la **zone de recherche inverse.**

```
 GNU nano 5.4                          /etc/bind/named.conf.options

options {
        directory "/var/cache/bind";
        forward only;
        forwarders { 172.17.254.1; };
        auth-nxdomain no;     # conform to RFC1035
        listen-on-v6 { any; };
        allow-query { any; };
        allow-recursion { 192.168.2.0/24;192.168.3.0/24; };_
};
```

8ème étape : Nous modifions le fichier indiqué afin de lui indiquer les **directives allow-query et allow-recursion** .

3. Modifications sur DS1.

```
 GNU nano 5.4                          /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.3.1
netmask 255.255.255.0
network 192.168.3.0
broadcast 192.168.3.255
gateway 192.168.3.254
```

1ère étape : Nous modifions la configuration IP de l'interface **enp0s3** sur DS1.

```
root@DS1: ~#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:e2:22:7f brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.1/24 brd 192.168.3.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee2:227f/64 scope link tentative
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:67:29:55 brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.254/24 brd 192.168.4.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe67:2955/64 scope link
       valid_lft forever preferred_lft forever
```

2ème étape : Nous vérifions la bonne prise en compte de la modification.

```
root@DS1: ~#ping  -c2 172.17.250.2
PING 172.17.250.2 (172.17.250.2) 56(84) bytes of data.
64 bytes from 172.17.250.2: icmp_seq=1 ttl=254 time=0.682 ms
64 bytes from 172.17.250.2: icmp_seq=2 ttl=254 time=0.839 ms

--- 172.17.250.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.682/0.760/0.839/0.078 ms
```

3ème étape : Nous effectuons un **ping** vers la box du Lycée.

```
 GNU nano 5.4                          /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.

        forward only;
        forwarders { 192.168.2.1; };
        allow-recursion { localnets; };
        auth-nxdomain no;
        listen-on-v6 { any; };
};
```

4ème étape : Nous modifions ce fichier ici présent , en ajoutant la directive **forwarders** qui doit renvoyer vers la nouvelle **adresse IP de DS2**.

```
root@DS1: ~#systemctl restart bind9
```

5ème étape : Nous relançons par la suite le **service DNS**.

4. Tests depuis UD1.

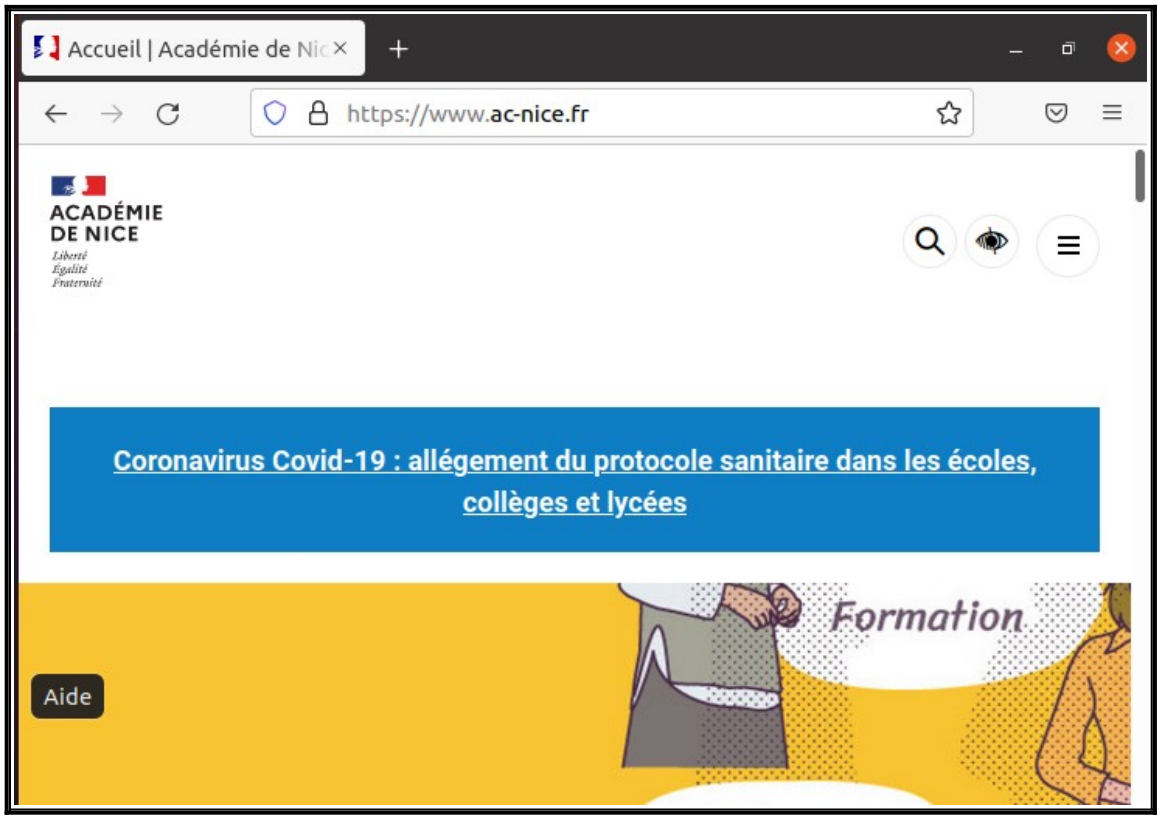
```
root@UD1:~# dig SOA sio-exupery.fr

; <<>> DiG 9.16.1-Ubuntu <<>> SOA sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60155
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sio-exupery.fr.                        IN      SOA

;; ANSWER SECTION:
sio-exupery.fr.         86400   IN      SOA     DS2.sio-exupery.fr. root.sio-ex
upery.fr. 2019020701 604800 86400 2419200 604800

;; Query time: 56 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: jeu. avril 28 15:50:48 CEST 2022
;; MSG SIZE  rcvd: 88
```

```
sio@UD1:~$ dig SOA intra.sio-exupery.fr

; <<>> DiG 9.16.1-Ubuntu <<>> SOA intra.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48903
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;intra.sio-exupery.fr.          IN      SOA

;; ANSWER SECTION:
intra.sio-exupery.fr.   86400   IN      SOA     DS1.intra.sio-exupery.fr. root.
intra.sio-exupery.fr. 2019020705 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: mer. avril 27 17:11:50 CEST 2022
;; MSG SIZE  rcvd: 94
```

1ère étape : Nous testons les deux résolutions **DNS** **interne**.

```
root@UD1:~# dig www.ac-nice.fr

; <<>> DiG 9.16.1-Ubuntu <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57451
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.ac-nice.fr.                        IN      A

;; ANSWER SECTION:
www.ac-nice.fr.         20896   IN      CNAME   cs234.wpc.alphacdn.net.
cs234.wpc.alphacdn.net. 3590    IN      A       93.184.221.161

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: jeu. avril 28 15:51:47 CEST 2022
;; MSG SIZE  rcvd: 95
```

2ème étape : Nous vérifions la résolution cette fois-ci **extérieur**.



3ème étape : Nous vérifions vérifions l'accès aux différents **sites hébergés sur DS2 depuis UD1**.