Chapitre 8 – Routage filtrant (pare-feu IPtables) – Partie 2

1. Modification sur US3.

Modification de l'adresse du serveur DNS

```
root@US3:~# ls /etc/netplan
00-installer-config.yaml
root@US3:~# _
```

```
  GNU nano 6.2                    /etc/netplan/00-installer-config.yaml *
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [172.17.101.204/24]
      dhcp4: no
      gateway4: 172.17.250.3
      nameservers:
        addresses: [8.8.8.8]
    enp0s8:
      addresses: [192.168.2.254/24]
      dhcp4: no
    enp0s9:
      addresses: [192.168.3.254/24]
      dhcp4: no
  version: 2
```

```
root@US3:~# netplan apply

** (generate:1007): WARNING **: 14:29:39.249: `gateway4` has been deprecated, use default routes ins
tead.
See the 'Default routes' section of the documentation for more details.
WARNING:root:Cannot call Open vSwitch: ovsdb-server.service is not running.

** (process:1005): WARNING **: 14:29:40.002: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.

** (process:1005): WARNING **: 14:29:40.264: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.

** (process:1005): WARNING **: 14:29:40.265: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.
root@US3:~#
```

Vérification de la bonne configuration de l’ip

```
root@US3:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
    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 fq_codel state UP gr
0
    link/ether 08:00:27:fd:c6:4b brd ff:ff:ff:ff:ff:ff
    inet 172.17.101.204/24 brd 172.17.101.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fefd:c64b/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
0
    link/ether 08:00:27:c6:2d:fe brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.254/24 brd 192.168.2.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec6:2dfe/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
0
    link/ether 08:00:27:df:b7:40 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.254/24 brd 192.168.3.255 scope global enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fedf:b740/64 scope link
       valid_lft forever preferred_lft forever
root@US3:~#
```

Vérification de la bonne attribution du DNS

```
  GNU nano 6.2                        /run/systemd/resolve/resolv.conf
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 8.8.8.8
search .
```

2. Modifications sur DS2.

Désactivation de l'interface Enp0s3

```
root@DS2: ~#ifdown enp0s3
root@DS2: ~#_
```

Modifcation de sa configuration IP ainsi que celle de son alias :

```
  GNU nano 8.4                                                  /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 192.168.2.1
netmask 255.255.255.0
network 192.168.2.0
broadcast 192.168.2.255
gateway 192.168.2.254
dns-search sio-exupery.fr
dns-domain sio-exupery.fr
dns-nameservers 192.168.2.1

auto enp0s3:0
iface enp0s3:0 inet static
address 192.168.2.9
netmask 255.255.255.0
network 192.168.2.0
broadcast 192.168.2.255
```

Réactivation de la carte et vérification de la prise en compte des modifications de enp0s3

```
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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ab:c6:47 brd ff:ff:ff:ff:ff:ff
    altname enx080027abc647
    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:feab:c647/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Modification des fichiers d'hôte virtuels :

```
<VirtualHost 192.168.2.9:80>
        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>
```

Rechargement de la configuration d'apache2

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

Modification du fichier contenant les zones de recherche DNS

```
  GNU nano 8.4                                        /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; };
};
```

Modification du fichier pour la zone de recherche directe :

```
 GNU nano 8.4                                                /var/cache/bind/db.sio-exupery.fr

; fichier pour la résolution directe
$TTL 86400
@       IN SOA DS2.sio-exupery.fr root.sio-exupery.fr. (
              2026030501
              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
```

Modification de la zone de recherche inverser

```
 GNU nano 8.4                                                /var/cache/bind/rev.sio-exupery.fr

; Fichier pour la résolution inverse
$TTL 86400
@       IN SOA DS2.sio-exupery.fr. root.sio-exupery.fr. (
               2026030501
               1w
               1d
               4w
               1w )
@                       IN NS   DS2.sio-exupery.fr.
1                       IN PTR  DS2.sio-exupery.fr.
```

Modification le fichier /etc/bind/named.conf.options (directives allow-query et allow-recursion) et relance du service DNS :

```
 GNU nano 8.4                                                  /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";
        forward only;
        forwarders { 8.8.8.8; };
        dnssec-validation no;
        listen-on-v6 { any; };
        allow-query { any; };
        allow-recursion { 192.168.2.0/24;192.168.3.0/24; };
};
```

```
root@DS2: ~#systemctl restart bind9
root@DS2: ~#
```

3. Modifications sur DS1.

Modification du mode d'accès réseau pour la carte 1 (enp0s3) : Réseau interne (LAN2).

Modification de la configuration IP de l'interface réseau enp0s3 avec un ifdown de la carte :

```
  GNU nano 8.4                                                  /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
auto 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


allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.4.254
netmask 255.255.255.0
network 192.168.4.0
broadcast 192.168.4.255
dns-search intra.sio-exupery.fr
dns-domain intra.sio-exupery.fr
dns-nameservers 192.168.4.254
```

Ifup de la carte :

```
root@DS1: ~#ifup enp0s3
dhcpcd-10.1.0 starting
DUID 00:01:00:01:30:82:86:88:08:00:27:2c:4f:c5
enp0s3: waiting for carrier
enp0s3: carrier acquired
enp0s3: IAID 27:2c:4f:c5
enp0s3: adding address fe80::47ae:20a7:77af:2a58
enp0s3: soliciting a DHCP lease
enp0s3: soliciting an IPv6 router
enp0s3: probing for an IPv4LL address
enp0s3: using IPv4LL address 169.254.218.141
enp0s3: adding route to 169.254.0.0/16
enp0s3: adding default route
root@DS1: ~#
```

Modification du fichier /etc/bind/named.conf.options. La directive forwarders doit renvoyer vers la nouvelle adresse IP de DS2 pour les résolutions hors zone intra.sio-exupery.fr :

```
options {
        directory "/var/cache/bind";
        forward only;
        forwarders { 192.168.2.1; };
        allow-recursion { localnets; };
        allow-query { any; };
        auth-nxdomain no;
        listen-on-v6 { any; };
};
```

Relance des services DNS

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

4. Tests depuis DD1/UD1

Test des deux résolutions DNS figurant ci-dessous :

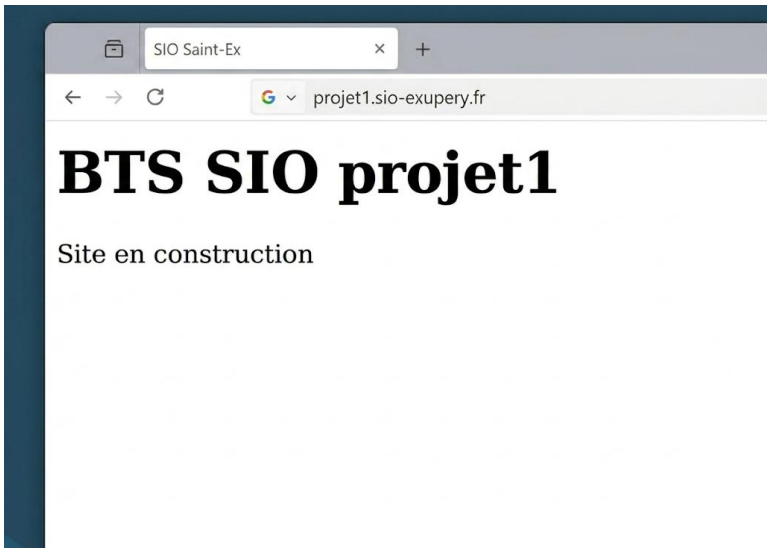
```
sio@DD1:~$ dig SOA intra.sio-exupery.fr

; <<>> DiG 9.20.11-4-Debian <<>> SOA intra.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57091
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ca7cc94501afd5390100000069f35e8e033220cdd0bcde8f (good)
;; QUESTION SECTION:
;intra.sio-exupery.fr.          IN      SOA

;; ANSWER SECTION:
intra.sio-exupery.fr.   86400   IN      SOA     DS1.intra.sio-exupery.fr.intra
io-exupery.fr. root.intra.sio-exupery.fr. 2026030501 604800 86400 2419200 6048

;; Query time: 4 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Thu Apr 30 15:52:13 CEST 2026
;; MSG SIZE  rcvd: 143

sio@DD1:~$
```

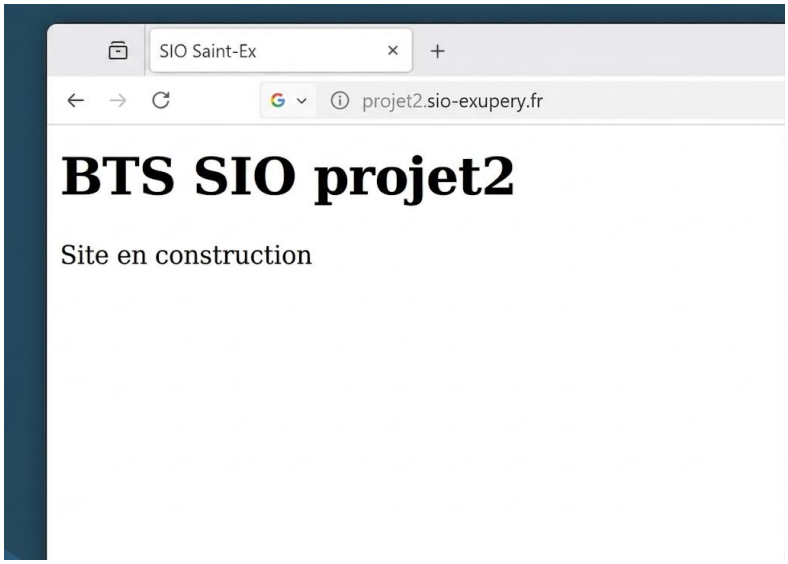
```
sio@DD1:~$ dig SOA sio-exupery.fr

; <<>> DiG 9.20.11-4-Debian <<>> SOA sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44523
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 08ceff0bbe4dfb100100000069f4b7cceff4317cc652281b (good)
;; QUESTION SECTION:
;sio-exupery.fr.                        IN      SOA

;; ANSWER SECTION:
sio-exupery.fr.         86400   IN      SOA     DS2.sio-exupery.fr.sio-exupery
r. root.sio-exupery.fr. 2026030501 604800 86400 2419200 604800

;; Query time: 4 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Fri May 01 16:25:16 CEST 2026
;; MSG SIZE  rcvd: 131
```

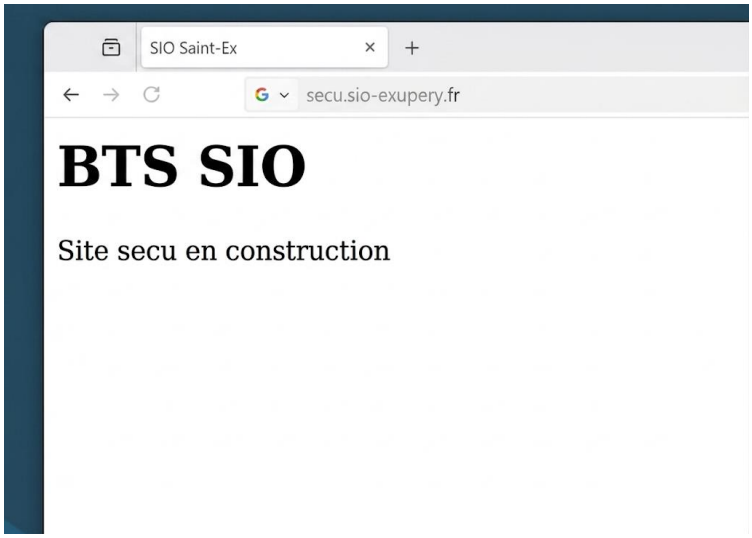
Vérification de la résolution hors zones intra.sio-exupery.fr et sio-exupery.fr

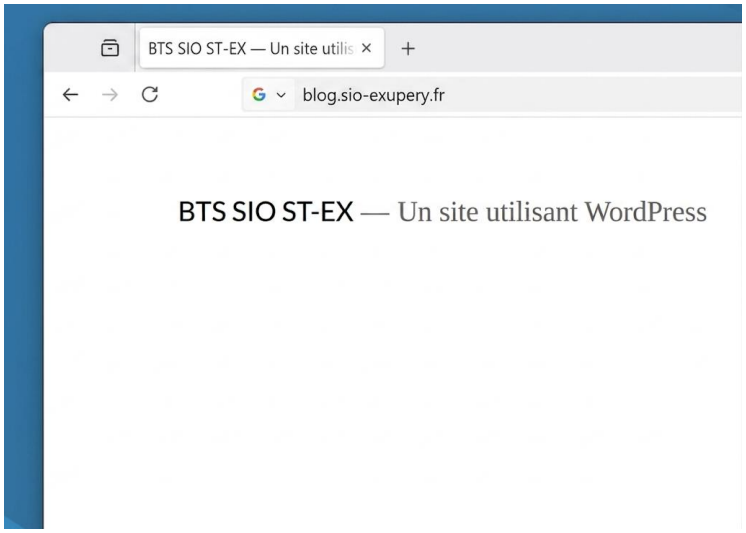
```
sio@DD1:~$ dig www.ac-nice.fr

; <<>> DiG 9.20.11-4-Debian <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1499
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d76a6ad5a39783da0100000069f4b7f23024b74b6f01d3d2 (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                        IN      A

;; ANSWER SECTION:
www.ac-nice.fr.         3600    IN      CNAME   www.ac-nice.fr.cdn.cloudflare
t.
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.105
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.106
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.107
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.104

;; Query time: 204 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Fri May 01 16:25:55 CEST 2026
;; MSG SIZE  rcvd: 182
```

Connexion au site :


SIO Saint-Ex
projet1.sio-exupery.fr
BTS SIO projet1
Site en construction


SIO Saint-Ex
projet2.sio-exupery.fr
BTS SIO projet2
Site en construction


SIO Saint-Ex
secu.sio-exupery.fr
BTS SIO
Site secu en construction


BTS SIO ST-EX — Un site utilis
blog.sio-exupery.fr
BTS SIO ST-EX — Un site utilisant WordPress

5. Test du pare-feu.

Test de la connectivité à internet

```
sio@DD1:~$ ping www.google.fr
PING www.google.fr (172.217.16.227) 56(84) bytes of data.
64 bytes from pnpara-ae-in-f3.1e100.net (172.217.16.227): icmp_seq=1 ttl=116 t
e=24.4 ms
64 bytes from pnpara-ae-in-f3.1e100.net (172.217.16.227): icmp_seq=2 ttl=116 t
e=25.6 ms
64 bytes from pnpara-ae-in-f3.1e100.net (172.217.16.227): icmp_seq=3 ttl=116 t
e=24.4 ms
^C
--- www.google.fr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 24.383/24.797/25.616/0.579 ms
sio@DD1:~$
```