

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

HIDAOUÏ Mohamed-Amine — BTS SIO SLAM

BTS SIO — Option SLAM

2025 – 2026

## Chapitre 8

### Routage filtrant (pare-feu IPtables)

*Partie 2*

**HIDAOUÏ Mohamed-Amine**

BTS SIO SLAM 1 — Lycée Saint-Exupéry

## Sommaire

1. Modification sur US3.
2. Modifications sur DS2.
3. Modifications sur DS1.
4. Tests depuis DD1/UD1.
5. Test du pare-feu.

## 1. Modification sur US3.

Listage du contenu du répertoire `/etc/netplan` (présence du fichier `00-installer-config.yaml`)

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

Mise à jour du fichier `/etc/netplan/00-installer-config.yaml` (ajout du DNS Orange `80.10.246.2`, conservation de `gateway4`)

```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [172.17.101.203/16]
      dhcp4: no
      gateway4: 172.17.250.3
      nameservers:
        addresses: [80.10.246.2]
    enp0s8:
      addresses: [192.168.2.254/24]
      dhcp4: no
    enp0s9:
      addresses: [192.168.3.254/24]
      dhcp4: no
  version: 2
```

Application de la configuration réseau via `netplan apply`

```
root@US3:/etc/netplan# netplan apply
WARNING:root:Cannot call Open vSwitch: ovssdb-server.service is not running.
root@US3:/etc/netplan# _
```

## 2. Modifications sur DS2.

Mise à jour du fichier `/etc/network/interfaces` sur DS2 (nouvelle adresse `192.168.2.1/24` sur `enp0s3`, alias `enp0s3:0` à `192.168.2.9`, passerelle `192.168.2.254`, DNS `192.168.2.1`)

```
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
```

Vérification de la configuration IP de DS2 après modification (`ip a`) — présence de `192.168.2.1/24` et `192.168.2.9/24` sur `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 00:00:27:85:94:3e brd ff:ff:ff:ff:ff:ff
    altname enx00002785943e
    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:fe85:943e/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
root@DS2: ~#
```

Mise à jour du fichier `/etc/apache2/sites-available/sites-sio.conf` (remplacement des adresses `192.168.4.x` par `192.168.2.x` dans tous les VirtualHost)

```
GNU nano 8.4 /etc/apache2/sites-available/sites-sio.conf
<VirtualHost 192.168.2.9:80>
    ServerName secu.sio-exupery.fr
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/secu
    ErrorLog /var/www/html/secu/logs/error.log
    CustomLog /var/www/html/secu/logs/access.log combined
</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>
```

Redémarrage du service Apache2 sur DS2

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

Mise à jour du fichier `/etc/bind/named.conf.local` (zone inverse mise à jour en [2.168.192.in-addr.arpa](#))

```
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; };
};
```

Mise à jour du fichier `/var/cache/bind/db.sio-exupery.fr` (nouvelles adresses IP : [DS2.sio-exupery.fr](#) → 192.168.2.1, [DS1.intra.sio-exupery.fr](#) → 192.168.3.1, [secu](#) → 192.168.2.9)

```
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. (
        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
```

Mise à jour du fichier `/var/cache/bind/rev.sio-exupery.fr` (zone inverse inchangée, PTR sur `DS2.sio-exupery.fr`)

```
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. (
                2019020201
                1w
                1d
                4w
                1w )
@      IN NS  DS2.sio-exupery.fr.
1      IN PTR DS2.sio-exupery.fr.
```

Mise à jour du fichier `/etc/bind/named.conf.options` sur DS2 (ajout des directives `allow-query { any; }` et `allow-recursion { 192.168.2.0/24;192.168.3.0/24; }`, `forwarders` → `80.10.246.2`)

```
GNU nano 8.4 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
    forward only;
    forwarders { 80.10.246.2; };
    dnssec-validation no;
    listen-on-v6 { any; };
    allow-query { any; };
    allow-recursion { 192.168.2.0/24;192.168.3.0/24; };
};
```

Redémarrage du service BIND9 sur DS2

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

### 3. Modifications sur DS1.

Mise à jour du fichier `/etc/bind/named.conf.options` sur DS1 (forwarders → nouvelle IP de DS2 : 192.168.2.1)

```
GNU nano 8.4 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
    forward only;
    forwarders { 192.168.2.1; };
    allow-recursion { localnets; };
    allow-query { any; };
    dnssec-validation no;
    listen-on-v6 { any; };
};
```

Mise à jour du fichier `/etc/network/interfaces` sur DS1 (interface `enp0s3` commentée en DHCP, adresse 192.168.3.1/24 sur `enp0s3`, `enp0s8` conservé à 192.168.4.254)

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

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
```

Redémarrage du service BIND9 sur DS1

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

## 4. Tests depuis DD1/UD1.

Résolution SOA de [sio-exupery.fr](https://sio-exupery.fr) depuis DD1 → [DS2.sio-exupery.fr](https://DS2.sio-exupery.fr) (serveur 192.168.4.254)

```
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: 5011
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: call15ebff87575c70100000069d7c6026b1505dce085da69 (good)
;; QUESTION SECTION:
;sio-exupery.fr.                IN      SOA

;; ANSWER SECTION:
sio-exupery.fr.                84058  IN      SOA      DS2.sio-exupery.fr. root.sio-exu
pery.fr. 2019020701 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Thu Apr 09 17:30:10 CEST 2026
;; MSG SIZE rcvd: 116
```

Résolution SOA d'[intra.sio-exupery.fr](https://intra.sio-exupery.fr) depuis DD1 → [DS1.intra.sio-exupery.fr](https://DS1.intra.sio-exupery.fr)

```
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: 46619
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 74831657130369320100000069d7c6126c12bcb061fa7895 (good)
;; QUESTION SECTION:
;intra.sio-exupery.fr.         IN      SOA

;; ANSWER SECTION:
intra.sio-exupery.fr.         86400  IN      SOA      DS1.intra.sio-exupery.fr. root.:
ntra.sio-exupery.fr. 2019020701 604800 86400 2419200 604800

;; Query time: 4 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Thu Apr 09 17:30:26 CEST 2026
;; MSG SIZE rcvd: 122
```

Résolution externe de [www.ac-nice.fr](http://www.ac-nice.fr) depuis DD1 (chaîne DS1 → DS2 → DNS Orange 80.10.246.2)

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

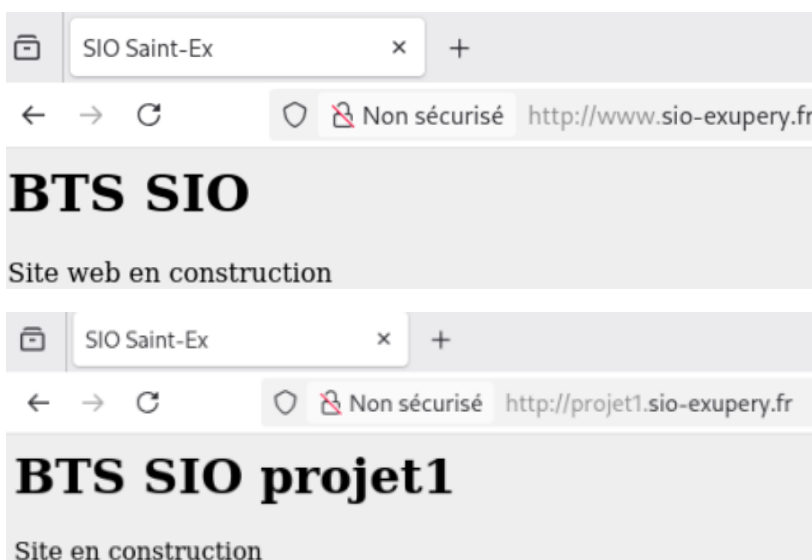
; <<>> DiG 9.20.11-4-Debian <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23804
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

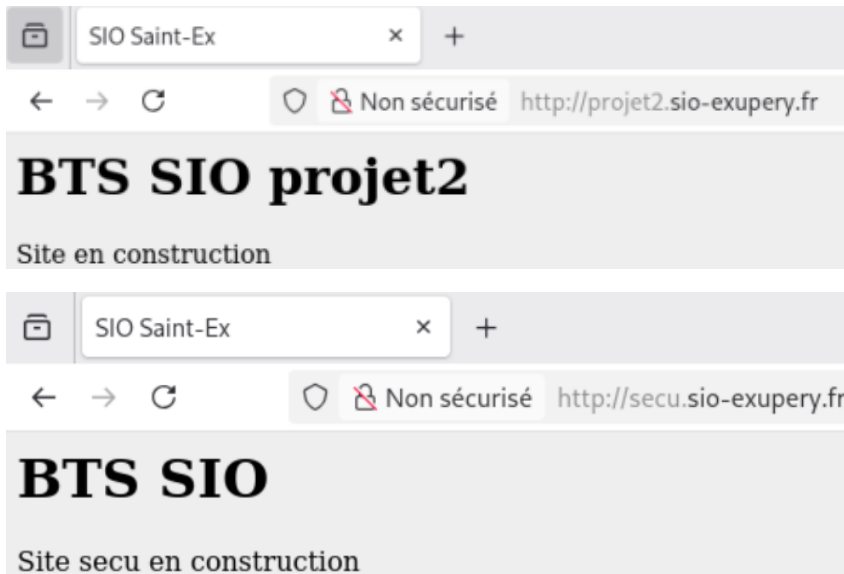
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2781b940adf484e20100000069d7c6246a8c83910a91c920 (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                IN      A

;; ANSWER SECTION:
www.ac-nice.fr.                2059    IN      CNAME   www.ac-nice.fr.cdn.cloudflare.net.
www.ac-nice.fr.cdn.cloudflare.net. 300    IN      A       141.101.90.104
www.ac-nice.fr.cdn.cloudflare.net. 300    IN      A       141.101.90.107
www.ac-nice.fr.cdn.cloudflare.net. 300    IN      A       141.101.90.106
www.ac-nice.fr.cdn.cloudflare.net. 300    IN      A       141.101.90.105

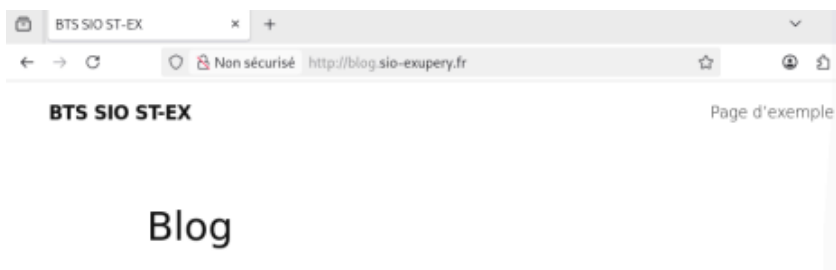
;; Query time: 140 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Thu Apr 09 17:30:44 CEST 2026
;; MSG SIZE rcvd: 182
```

Vérification de l'accessibilité des sites hébergés sur DS2 (maintenant en DMZ) depuis le navigateur de DD1 — accès confirmé à <http://www.sio-exupery.fr>, <http://projet1.sio-exupery.fr>, <http://projet2.sio-exupery.fr> et <http://secu.sio-exupery.fr>



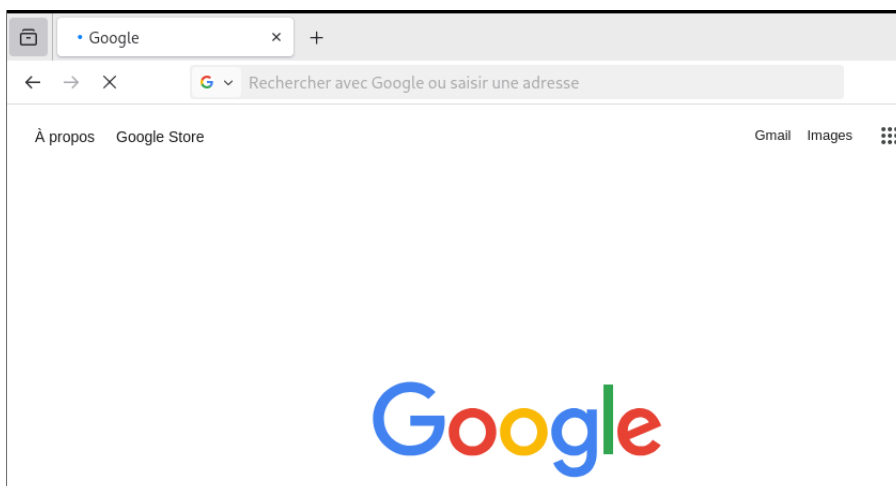


Vérification de l'accessibilité de <http://blog.sio-exupery.fr> (WordPress) depuis DD1



## 5. Test du pare-feu.

Vérification de l'accès Internet depuis DD1 (navigation sur [www.google.fr](http://www.google.fr) fonctionnelle)



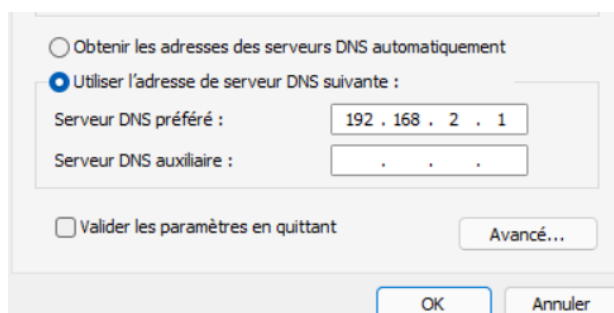
Ajout de la route statique vers 192.168.2.0/24 via 192.168.1.101 sur la machine hôte Windows

```
C:\Windows\System32>route add 192.168.2.0 mask 255.255.255.0 192.168.1.101
OK!
```

Vérification de la présence de la route 192.168.2.0 dans la table de routage IPv4 de la machine hôte (passerelle 192.168.1.101)

```
IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau      Masque réseau  Adr. passerelle  Adr. interface  Métrique
0.0.0.0                0.0.0.0       172.17.250.3    172.17.1.47     35
127.0.0.0              255.0.0.0     On-link         127.0.0.1       331
127.0.0.1              255.255.255.255  On-link         127.0.0.1       331
127.255.255.255       255.255.255.255  On-link         127.0.0.1       331
172.17.0.0             255.255.0.0   On-link         172.17.1.47     291
172.17.1.47           255.255.255.255  On-link         172.17.1.47     291
172.17.255.255       255.255.255.255  On-link         172.17.1.47     291
192.168.2.0           255.255.255.0   192.168.1.101   172.17.1.47     36
```

Configuration du serveur DNS préféré à 192.168.2.1 dans les propriétés TCP/IPv4 de la machine hôte



Accès au site <http://www.sio-exupery.fr> depuis le navigateur de la machine hôte — résolution DNS via DS2 en DMZ fonctionnelle (page « BTS SIO — Site en construction »)

