

TP8P2– Routage filtrant

SAOU Rayan

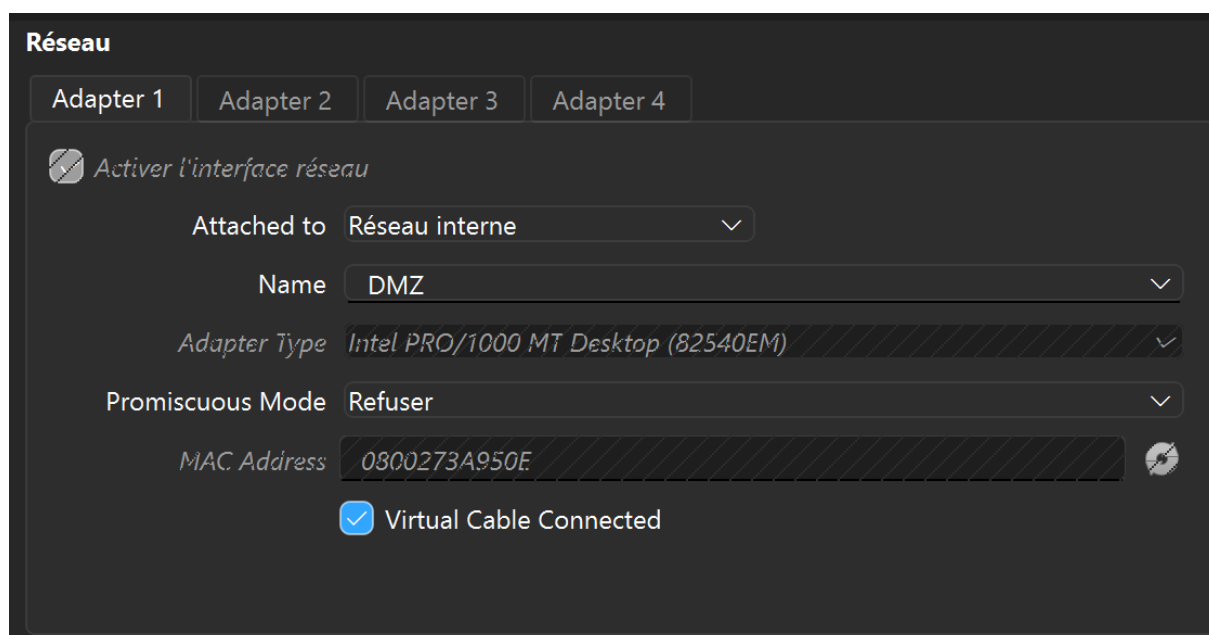
Table des matières

Table des matières	1
1. Modification sur DS2	2
2. Modification sur DS1	6
3. Tests depuis DD1	7
4. Test du pare-feu	9

1. Modification sur DS2

Puisque nous avons bâtis notre propre US3, nous n'avons pas besoin de modifier sa configuration IP.

Nous modifions le mode d'accès réseau de DS2 pour la mettre dans la DMZ.



Nous désactivons l'interface enp0s3 et modifions sa configuration IP :

```

# 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

# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto

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

iface enp0s8 inet dhcp

```

Nous réactivons la carte et vérifions la prise ne compte des modifications à l'aide de la commande ip a :

```

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 08:00:27:3a:95:0e brd ff:ff:ff:ff:ff:ff
    altname enx0800273a950e
    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::a90:27ff:fe3a:950e/64 scope link proto kernel_l1
        valid_lft forever preferred_lft forever
root@DS2: ~#

```

Nous modifions donc le fichier des hôtes virtuels en conséquence :

```

GNU nano 8.4 /etc/apache2/sites-ava
<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 192.168.2.10:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com
    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 192.168.2.10:80>
    ServerName projet1.sio-exupery.fr
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/projet1/repweb
    ErrorLog /var/www/html/web/logs/error.log
    CustomLog /var/www/html/projet1/repweb/logs/access.log combined
</VirtualHost>

<VirtualHost 192.168.2.10:80>
    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_10:80>
    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

```

Nous redémarrons le service Apache :

```

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

```

Nous modifions le fichier named.conf.local contenant les noms des zones recherche DNS :

```

GNU nano 8.4 /etc/bind/named.conf.local
//
// Do any local configuration here
//
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; };
};

```

Nous modifions le fichier pour la zone de recherche directe :

```

GNU nano 8.4 /var/cache/bind/db.sio-exupery.fr *
$TTL 86400
@      IN SOA  DS2.sio-exupery.fr. root.sio-exupery.fr. (
        20260305
        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

```

Idem pour la zone de recherche inverse :

```

GNU nano 8.4 /var/cache/bind/rev.sio-exupery.fr *
$TTL 86400
@      IN SOA  DS2.sio-exupery.fr. root.sio-exupery.fr. (
        20260305
        1w
        1d
        4w
        1w )
@      IN NS   DS2.sio-exupery.fr.
1      IN PTR  DS2.sio-exupery.fr.

```

Nous modifions le fichier named.conf.options :

```

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; };
};

```

Nous relançons le service DNS :

```

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

```

2. Modification sur DS1

Nous modifions la directive du fichier named.conf.optiouns :

```

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;
};

```

Nous relançons le service DNS :

```

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

```

3. Tests depuis DDI

Nous testons les deux résolutions DNS suivantes :

```
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: 63067
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 98cad0336745830f0100000069d4b6daae88d890a358be71 (good)
;; QUESTION SECTION:
; sio-exupery.fr.                IN      SOA

;; ANSWER SECTION:
sio-exupery.fr. 86400 IN      SOA      DS2.sio-exupery.fr. root.sio-
oery.fr. 20260305 604800 86400 2419200 604800

;; Query time: 23 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Tue Apr 07 09:48:42 CEST 2026
;; MSG SIZE rcvd: 128
```

```
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: 50643
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: b149d6f4051e550d0100000069d4b6ed3c9cb385b14991d7 (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. 20260332 604800 86400 2419200 604800

;; Query time: 7 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Tue Apr 07 09:49:01 CEST 2026
;; MSG SIZE rcvd: 122
```

Ainsi que résolution hors zone :

```

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: 20065
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

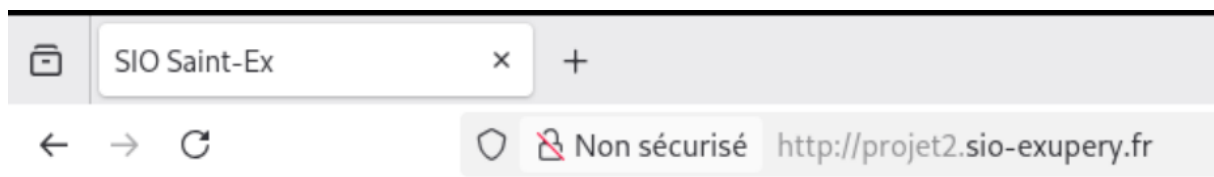
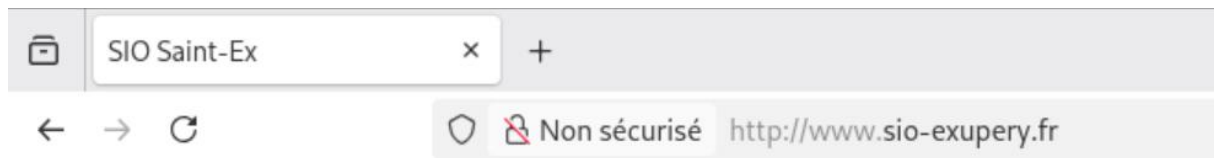
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2f59245f6a74f7660100000069d4bb29d788e01dae5d2432 (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                IN      A

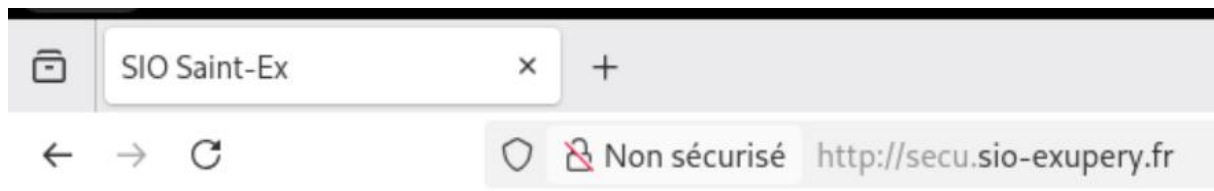
;; ANSWER SECTION:
www.ac-nice.fr.                3575    IN      CNAME   www.ac-nice.fr.cdn.cloudflare.net.
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.105
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.104
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.107
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.106

;; Query time: 59 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Tue Apr 07 10:07:05 CEST 2026
;; MSG SIZE rcvd: 182

```

Nous vérifions l'accès aux différents sites hébergés :





BTS SIO1

Site secu en construction



BTS SIO1

Site en construction

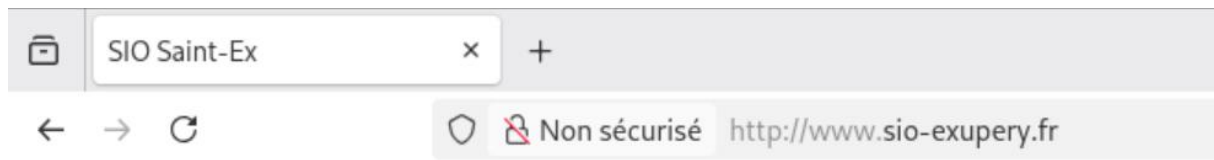
4. Test du pare-feu

Le pare-feu étant activé, nous testons d'aller sur Internet ainsi que sur les sites hébergés :

```

root@US3:~# ./parefeu.sh
Script pour le pare-feu
Initialisation des variables :
OK.
Vidage des règles existantes et verouillage :
Voulez vous continuer le script ? (o/n) :
o
Communication locales, internes et externes OK.
Pare-feu en fonctionnement, blocage maximum.
root@US3:~# _

```



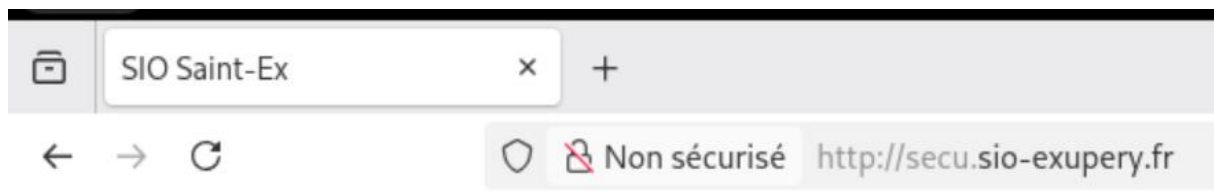
BTS SIO1

Site en construction



BTS SIO1

Site en construction



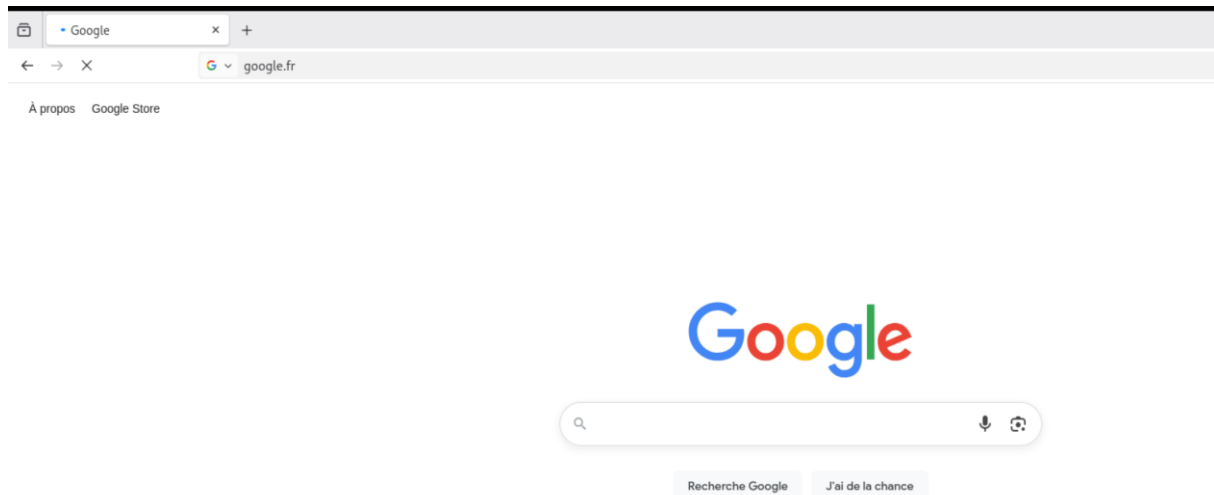
BTS SIO1

Site secu en construction



BTS SIO1

Site en construction



Nous vérifions que le serveur DNS et Web DS2 soit accessible depuis l'extérieur, nous ajoutons une route statique depuis notre système hôte :

```
C:\Windows\System32>route add 192.168.2.0 mask 255.255.255.0 172.17.110.220
OK!
C:\Windows\System32>
```

Nous modifions le serveur DNS en mettant 192.168.2.1 :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) ✕

Général **Configuration alternative**

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

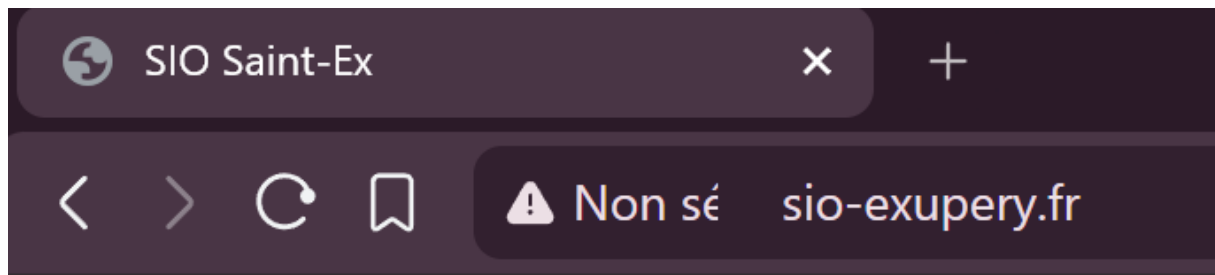
Adresse IP :	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Masque de sous-réseau :	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Passerelle par défaut :	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :	<input type="text" value="192"/> <input type="text" value="."/> <input type="text" value="168"/> <input type="text" value="."/> <input type="text" value="2"/> <input type="text" value="."/> <input type="text" value="1"/>
Serveur DNS auxiliaire :	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>

Valider les paramètres en quittant Avancé...



BTS SIO1

Site en construction