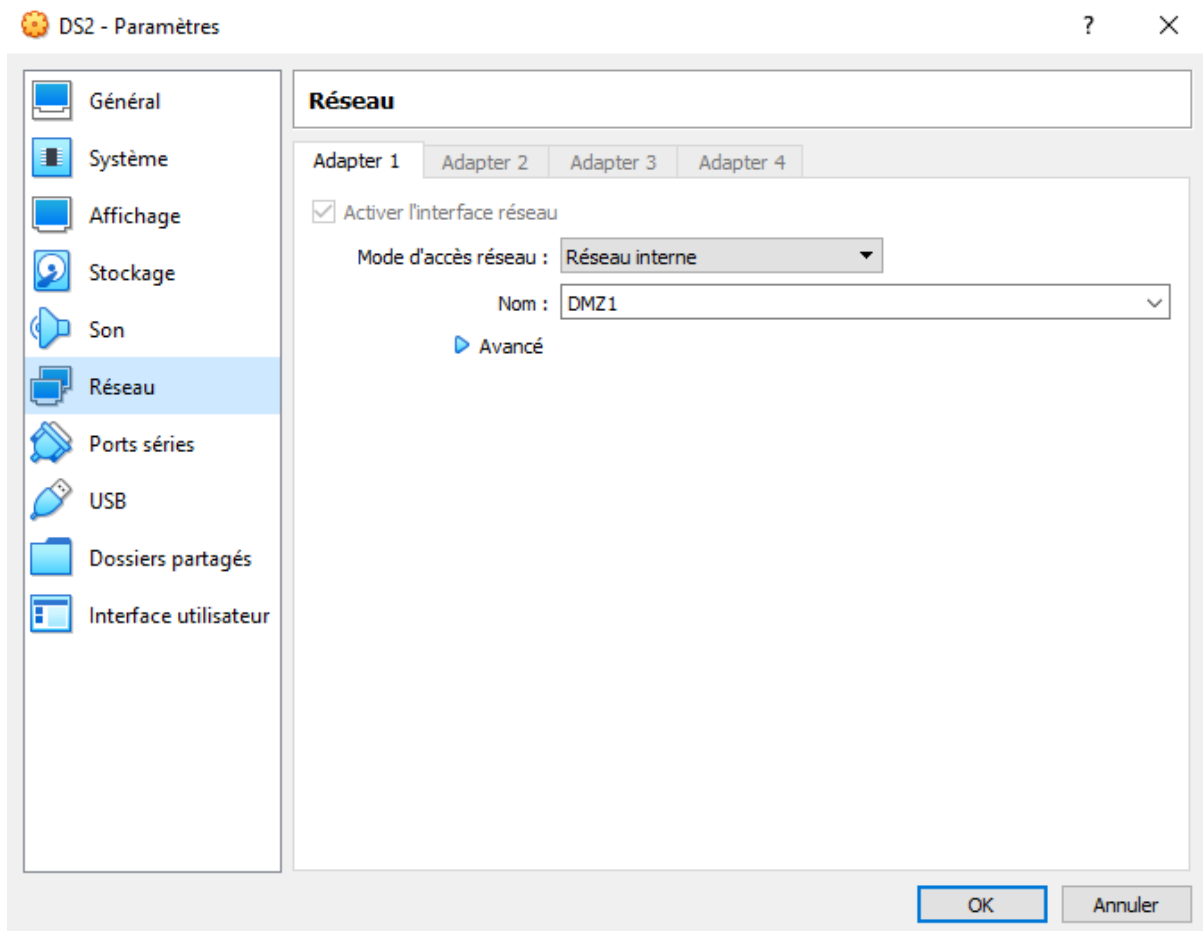


# TP Chapitre 8 – Routage filtrant (pare-feu IPtables)

## 2. Modifications sur DS2 (SLAM et SISR).

- Modifiez le mode d'accès réseau pour la carte 1 (enp0s3) : Réseau interne (DMZ1).



- Désactivez l'interface réseau enp0s3 et modifiez sa configuration IP ainsi que celle de l'alias IP :

```

GNU nano 3.2 /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

```

- Réactivez la carte et vérifiez la prise en 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
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:cb:45:a9 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
    inet6 fe80::a00:27ff:feeb:45a9/64 scope link
        valid_lft forever preferred_lft forever
root@DS2: ~#

```

- ▪ Modifiez en conséquence le fichier des hôtes virtuels /etc/apache2/sites-available/sites-sio.conf (cf. page 6 Chapitre 7) :

```

GNU nano 3.2 /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>

```

- Rechargez la configuration d'apache2 :

```

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

```

- Modifiez le fichier /etc/bind/named.conf.local contenant les noms des zones de recherche DNS :

```

GNU nano 3.2 /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";
//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; };
};

```

- Modifiez le fichier pour la zone de recherche directe  
/var/cache/bind/db.sio-exupery.fr :

```
GNU nano 3.2 /var/cache/bind/db.sio-exupery.fr
; Fichier pour la résolution directe
$TTL 86400
@      IN SOA  DS2.sio-exupery.fr. root.sio-exupery.fr. (
        2021040901
        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
```

- Modifiez le fichier pour la zone de recherche inverse  
/var/cache/bind/rev.sio-exupery.fr :

```
GNU nano 3.2 /var/cache/bind/rev.sio-exupery.fr
; Fichier pour la résolution inverse
$TTL 86400
@      IN SOA  DS2.sio-exupery.fr. root.sio-exupery.fr. (
        2021040901
        1w
        1d
        4w
        1w )
@      IN NS   DS2.sio-exupery.fr.
1      IN PTR  DS2.sio-exupery.fr.
```

- Modifiez le fichier /etc/bind/named.conf.options (directives allow-query et allow-recursion) :

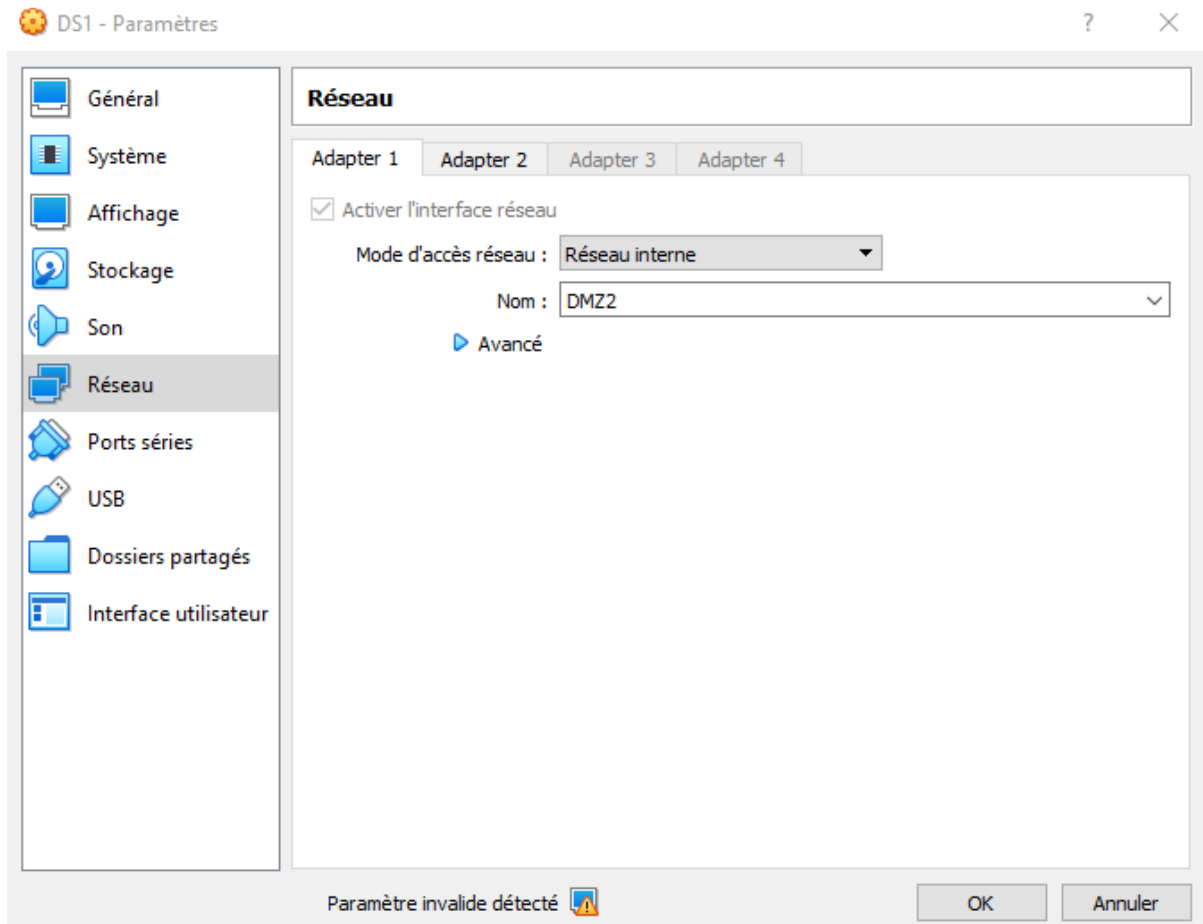
```
GNU nano 3.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
    forward only;
    forwarders { 192.168.1.1; };
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
    allow-query { any; };
    allow-recursion { 192.168.2.0/24;192.168.3.0/24; };
};
```

- Relancez le service DNS :

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

### 3. Modifications sur DS1 (SLAM et SISR).

- Modifiez le mode d'accès réseau pour la carte 1 (enp0s3) : Réseau interne (DMZ2).



- Modifiez la configuration IP de l'interface réseau enp0s3 (enp0s8 reste dans le réseau 192.168.4.0/24) :

```
GNU nano 3.2 /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
```

- Vérifiez la configuration IP avec la commande ip a :

```

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 1000
    link/ether 08:00:27:71:86:85 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:fe71:8685/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:f6:88:48 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:fef6:8848/64 scope link
        valid_lft forever preferred_lft forever
root@DS1: ~#

```

- Vérifiez la connectivité avec la box :

```

root@DS1: ~#ping -c2 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=7.92 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=8.12 ms

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 7.917/8.018/8.119/0.101 ms
root@DS1: ~#

```

- Modifiez le 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` :

```

GNU nano 3.2 /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.

    forward only;
    forwarders { 192.168.2.1; };
    allow-recursion { localnets; }; # conform to RFC1035
    listen-on-v6 { any; };
};

```

- Relancez le service DNS sur DS1 :

```

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

```

## 4. Tests depuis UD1 (SLAM et SISR).

- Testez les deux résolutions DNS figurant ci-dessous :

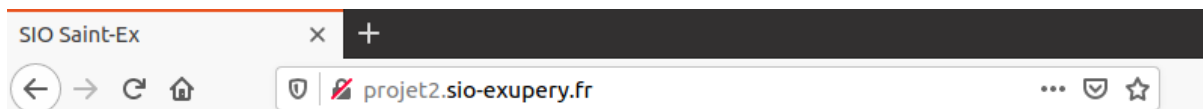
```
sio@ud1: ~  
sio@ud1:~$ dig SOA sio-exupery.fr  
  
; <<>> DiG 9.16.1-Ubuntu <<>> SOA sio-exupery.fr  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27423  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; 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-exu  
pery.fr. 2021040901 604800 86400 2419200 604800  
  
;; Query time: 3 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: lun. avril 19 10:24:20 CEST 2021  
;; MSG SIZE rcvd: 88  
  
sio@ud1:~$  
  
sio@ud1: ~  
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: 43760  
;; 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.i  
ntra.sio-exupery.fr. 2021040917 604800 86400 2419200 604800  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: lun. avril 19 10:25:20 CEST 2021  
;; MSG SIZE rcvd: 94  
  
sio@ud1:~$
```

- Vérifiez la résolution hors zones intra.sio-exupery.fr et sio-exupery.fr :

```
sio@ud1: ~  
sio@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: 41634  
;; 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.                20601   IN      CNAME   cs234.wpc.alphacdn.net.  
cs234.wpc.alphacdn.net. 2631    IN      A       93.184.221.161  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: lun. avril 19 10:26:31 CEST 2021  
;; MSG SIZE rcvd: 95  
  
sio@ud1:~$
```

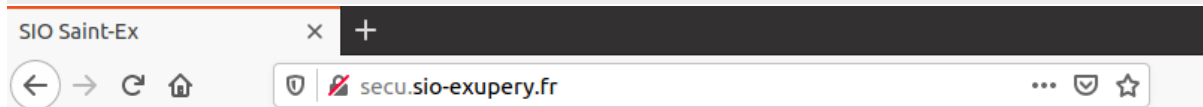
- Vérifiez l'accessibilité aux différents sites hébergés sur DS2 situé maintenant dans la DMZ :





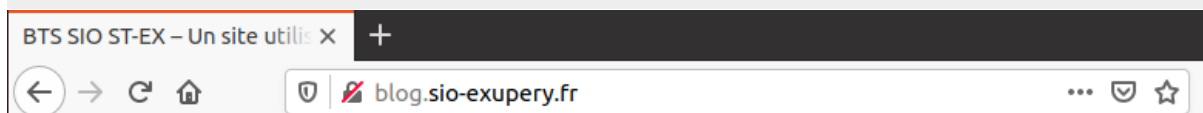
# BTS SIO projet2

Site en construction



# BTS SIO

Site secu en construction



[Aller au contenu](#)

# BTS SIO ST-EX

Un site utilisant WordPress

**[Bonjour tout le monde !](#)**

Bienvenue sur WordPress. Ceci est votre premier article. Modifiez-le ou supprimez-le, puis con