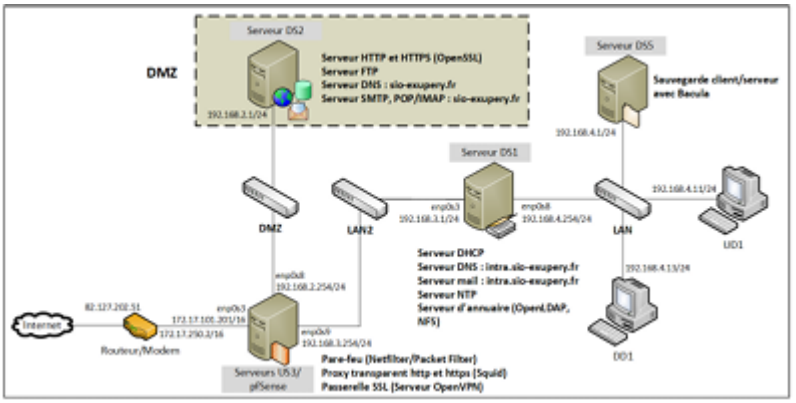
Chapitre 8 – Routage filtrant (pare-feu IPtables) – Partie 2



1. Modification sur US3.

▪ Nous modifions l'adresse du serveur DNS :

```
#MAISON
network:
  version: 2
  renderer: networkd
  ethernets:
      enp0s3:
          addresses: [192.168.1.241/24]
          dhcp4: no
          routes:
            - to: default
              via: 192.168.1.1
          nameservers:
              addresses: [80.10.246.2]
      enp0s8:
          addresses: [192.168.2.254/24]
          dhcp4: no
      enp0s9:
          addresses: [192.168.3.254/24]
          dhcp4: no
```

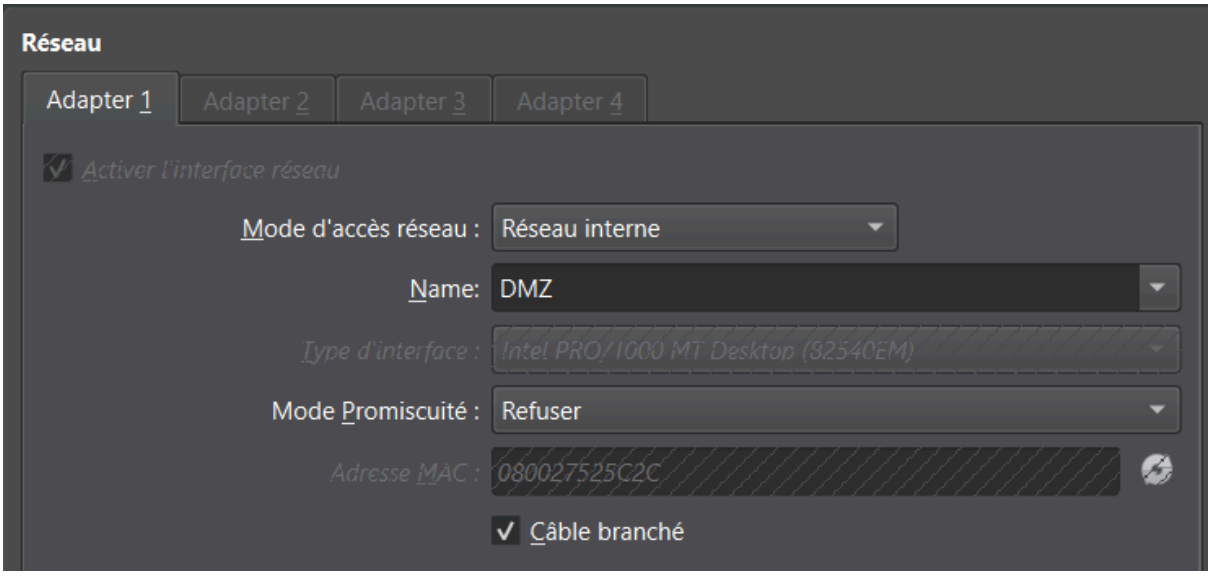
```
root@us3:/etc/netplan# netplan apply
root@us3:/etc/netplan#
```

▪ Affichage du fichier /run/systemd/resolve/resolv.conf afin de vérifier l'adresse du serveur DNS.

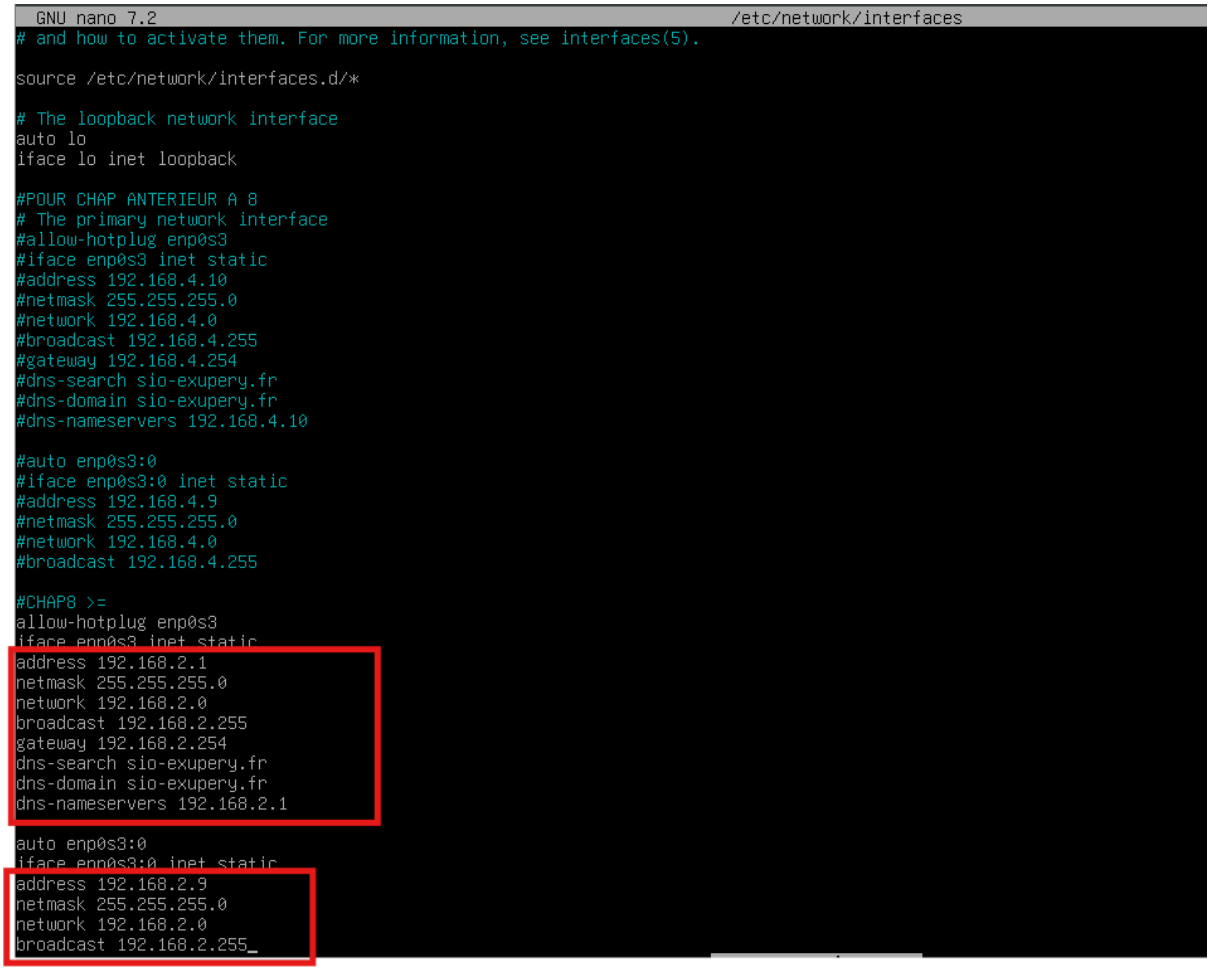
```
root@us3:~# cat /run/systemd/resolve/resolv.conf
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This 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 80.10.246.2
nameserver 2a02:842a:83c7:b001:ce19:a8ff:fecf:70df
search .
root@us3:~#
```

2. Modifications sur DS2.

▪ Nous modifions le mode d'accès réseau pour la carte 1 (enp0s3) : Réseau interne (DMZ).



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



▪ 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 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 08:00:27:52:5c:2c 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:fe52:5c2c/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 7.2                                  /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>
```

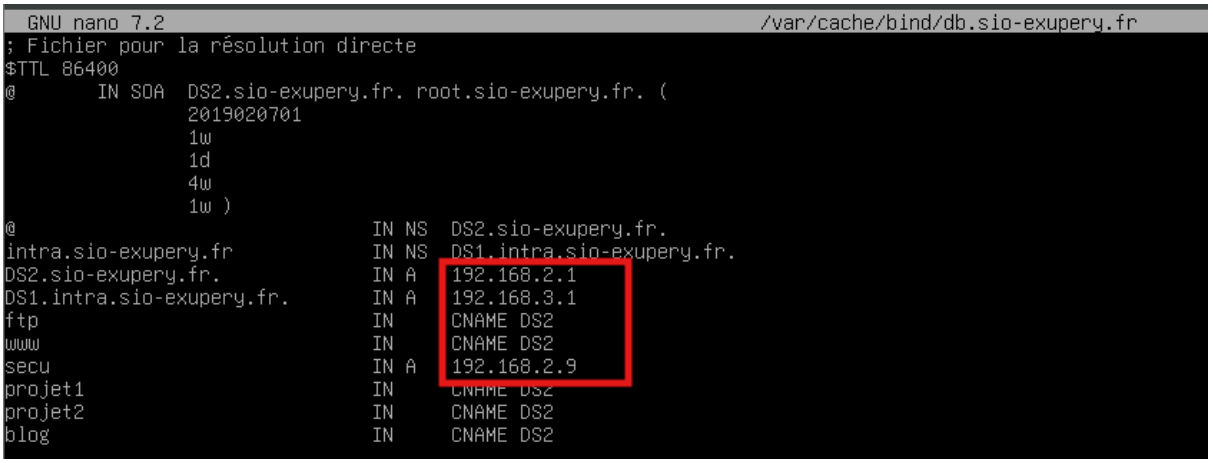
▪ Rechargement de la configuration d'apache2 :

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

▪ Nous modifions le fichier /etc/bind/named.conf.local contenant les noms des zones de recherche DNS :

```
 GNU nano 7.2                                          /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; };
};
```

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



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

▪ Nous modifionsle fichier /etc/bind/named.conf.options (directives allow-query et allow-recursion) :

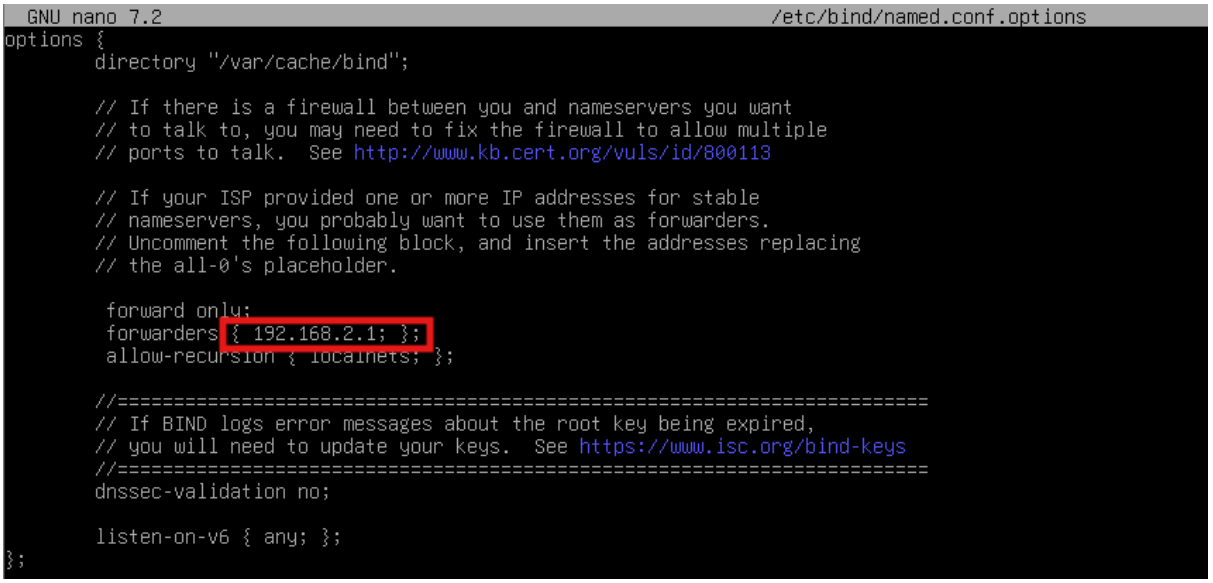
```
 GNU nano 7.2                                          /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";
        forward only;

        // 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.

        forwarders { 80.10.246.2; };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation no;

        listen-on-v6 { any; };
        allow-query { any; };
        allow-recursion { 192.168.2.0/24;192.168.3.0/24; };
};
```

▪ Relancement du service DNS :

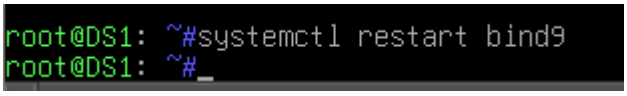
```
root@DS2: ~#systemctl restart bind9
root@DS2: ~#
```

3. Modifications sur 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 :



▪ Relancement du service DNS sur DS1 :



4. Tests depuis UD1.

▪ Test des deux résolutions DNS figurant ci-dessous :

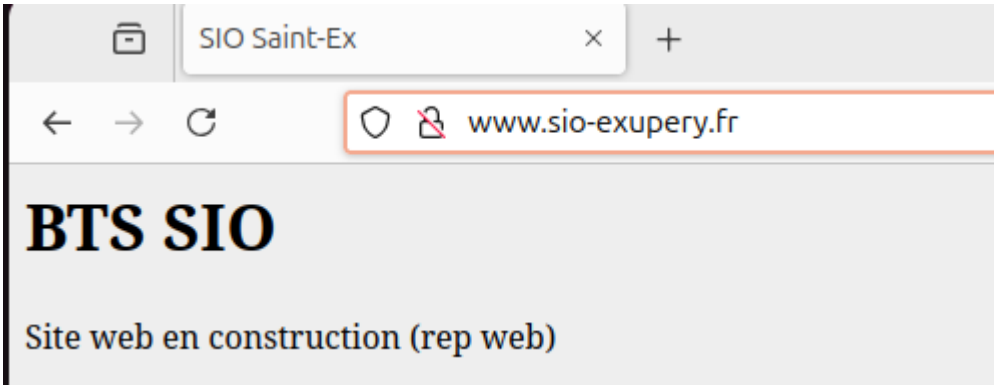
```
nicolasmtru@UD1:~$ dig SOA sio-exupery.fr

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> SOA sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58474
;; 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. 2019020701 604800 86400 2419200 604800

;; Query time: 2 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Apr 11 19:17:48 CEST 2025
;; MSG SIZE  rcvd: 88
```

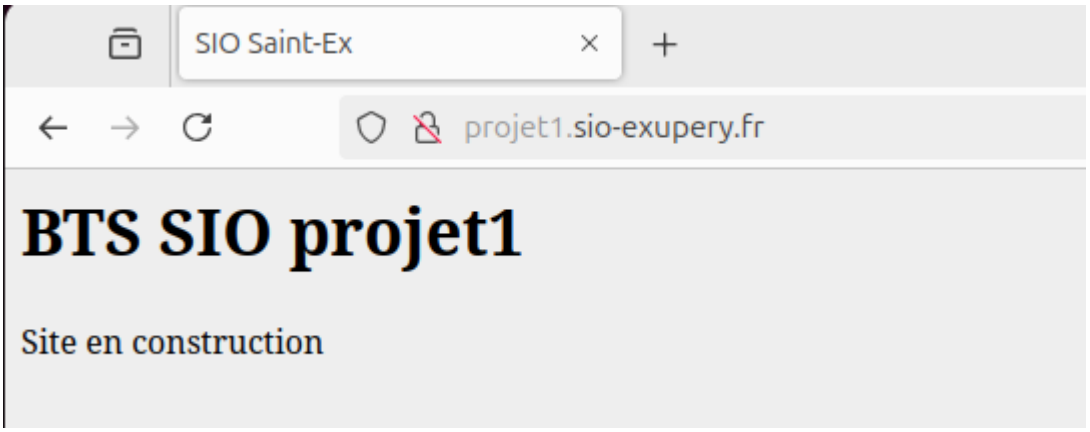
```
nicolasmtru@UD1:~$ dig SOA intra.sio-exupery.fr

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> SOA intra.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3785
;; 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. 2024032101 604800 86400 2419200 604800

;; Query time: 2 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Apr 11 19:18:28 CEST 2025
;; MSG SIZE  rcvd: 94
```

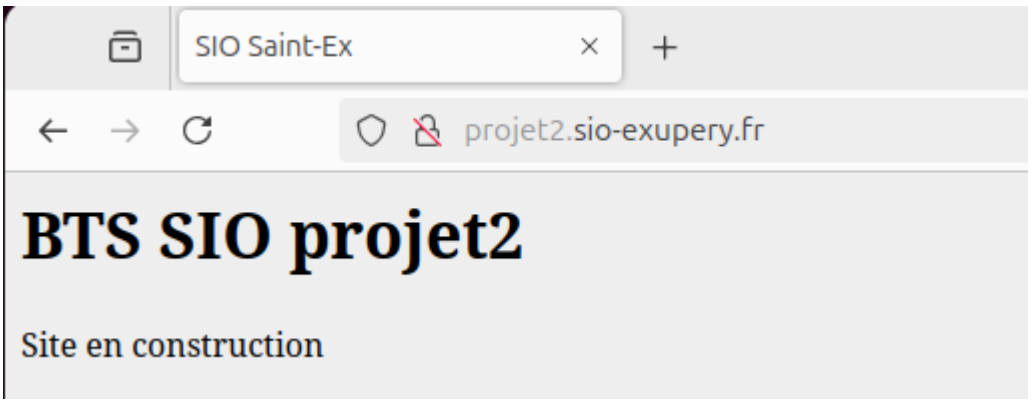
▪ Vérification de la résolution hors zones intra.sio-exupery.fr et sio-exupery.fr :

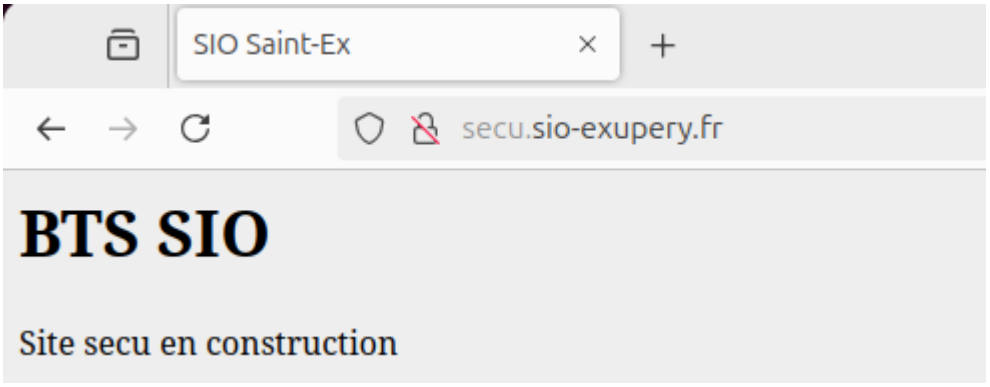
```
nicolasmtru@UD1:~$ dig www.ac-nice.fr

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42342
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, 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.         10809   IN      CNAME   www.ac-nice.fr.cdn.cloudflare.n
t.
www.ac-nice.fr.cdn.cloudflare.net. 263 IN A     141.101.90.104
www.ac-nice.fr.cdn.cloudflare.net. 263 IN A     141.101.90.106
www.ac-nice.fr.cdn.cloudflare.net. 263 IN A     141.101.90.105
www.ac-nice.fr.cdn.cloudflare.net. 263 IN A     141.101.90.107

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Apr 11 20:03:05 CEST 2025
;; MSG SIZE  rcvd: 154
```

▪ Vérification de l'accessibilité aux différents sites hébergés sur DS2 situé maintenant dans la DMZ :






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

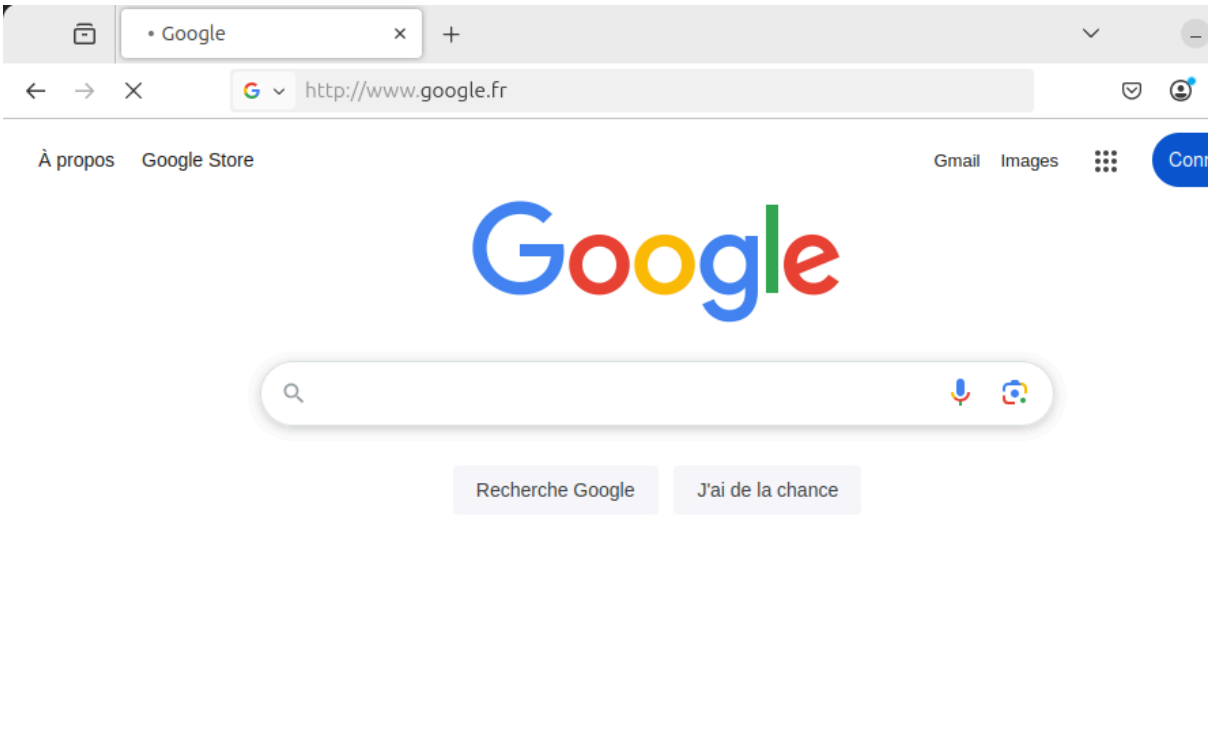

SIO Saint-Ex
secu.sio-exupery.fr
BTS SIO
Site secu en construction

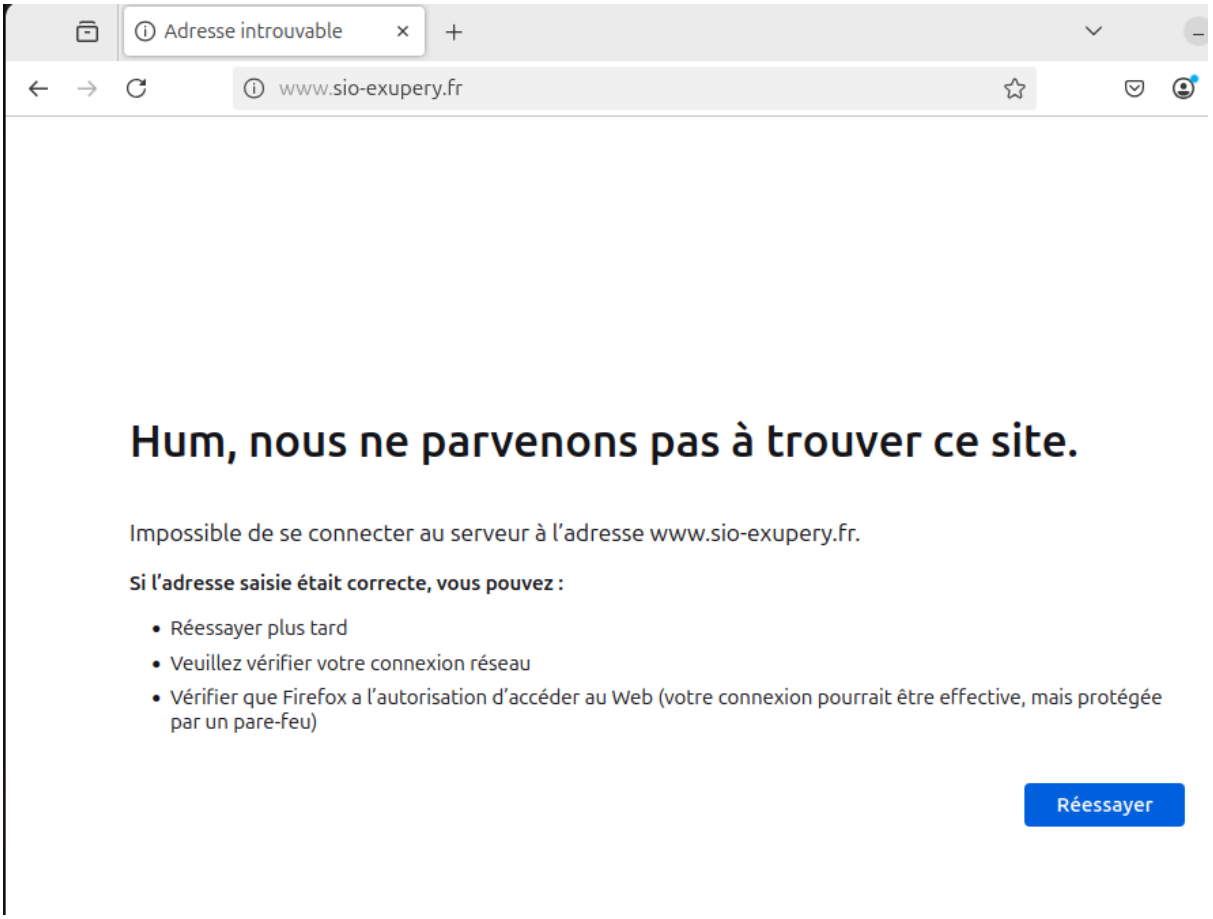

BTS SIO ST-EX
blog.sio-exupery.fr
BTS SIO ST-EX
Page d'exer
Blog
Bonjour tout le monde !
Bienvenue sur WordPress. Ceci est votre premier article. Modifiez-le ou supprimez-le, puis commencez à écrire !
15 mars 2025

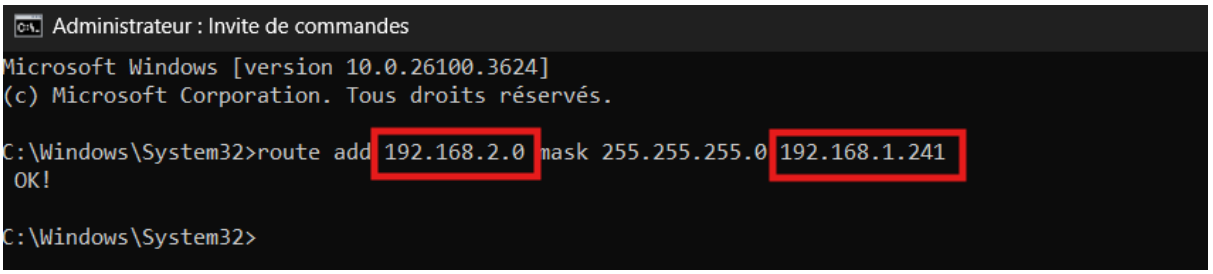
5. Test du pare-feu.

▪ Après avoir activé le pare-feu, test depuis UD1 les communications Internet ainsi que l'accès aux sites Web hébergés sur DS2

```
root@us3:~# ./parefeu.sh
Script pour le pare-feu
--> Initialisation des variables :
 OK.
--> Vidage des règles existantes et vérouillage :
--> Voulez-vous continuer le script (o/n) ?
o
iptables: Bad policy name. Run `dmesg' for more information.
 Pare-feu en fonctionnemen, blocage maximum.
 Communications locales, internes et externes OK.
root@us3:~#
```




Adresse introuvable
www.sio-exupery.fr
Hum, nous ne parvenons pas à trouver ce site.
Impossible de se connecter au serveur à l'adresse www.sio-exupery.fr.
Si l'adresse saisie était correcte, vous pouvez :
Réessayer plus tard
Veuillez vérifier votre connexion réseau
Vérifier que Firefox a l'autorisation d'accéder au Web (votre connexion pourrait être effective, mais protégée par un pare-feu)
Réessayer


Administrateur : Invite de commandes
Microsoft Windows [version 10.0.26100.3624]
(c) Microsoft Corporation. Tous droits réservés.
C:\Windows\System32>route add 192.168.2.0 mask 255.255.255.0 192.168.1.241
OK!
C:\Windows\System32>

▪ Je met comme serveur DNS principal, 192.168.2.1