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

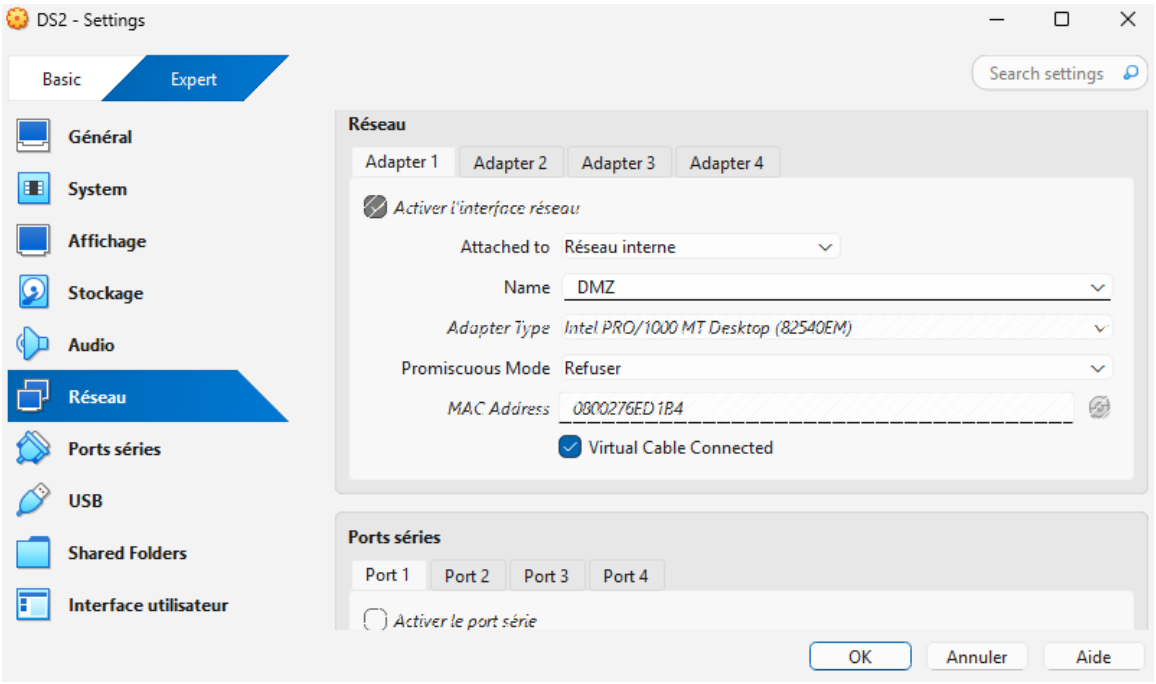
Sommaires

1. Modification sur US3

Déjà fait

2. Modifications sur DS2

On modifie le mode d'accès réseau pour la carte 1 (enp0s3) en Réseau interne (DMZ).



On désactive l'interface réseau enp0s3 et on modifie sa configuration IP ainsi que celle de l'alias IP

```
  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
# 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
```

On réactive la carte et on vérifie 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 08:00:27:6e:d1:b4 brd ff:ff:ff:ff:ff:ff
    altname enx0800276ed1b4
    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:fe6e:d1b4/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
root@DS2: ~#
```

On modifie en conséquence le fichier des hôtes virtuels /etc/apache2/sites-available/sites-sio.conf

```
 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>
```

On recharge la configuration d’apache2

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

On modifie le fichier /etc/bind/named.conf.local contenant les noms des 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; };
};
```

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

```
  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. (
                2026031201
                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
```

On modifie le fichier pour la zone de recherche inverse /var/cache/bind/rev.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. (
                2026031201
                1w
                1d
                4w
                1w )
@                       IN NS   DS2.sio-exupery.fr.
1                       IN PTR  DS2.sio-exupery.fr.
```

On modifie le fichier /etc/bind/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; };
};
```

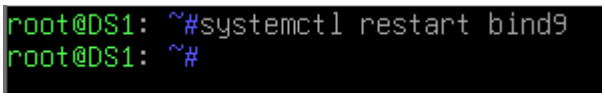
On relance le service DNS

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

3. Modifications sur DS1

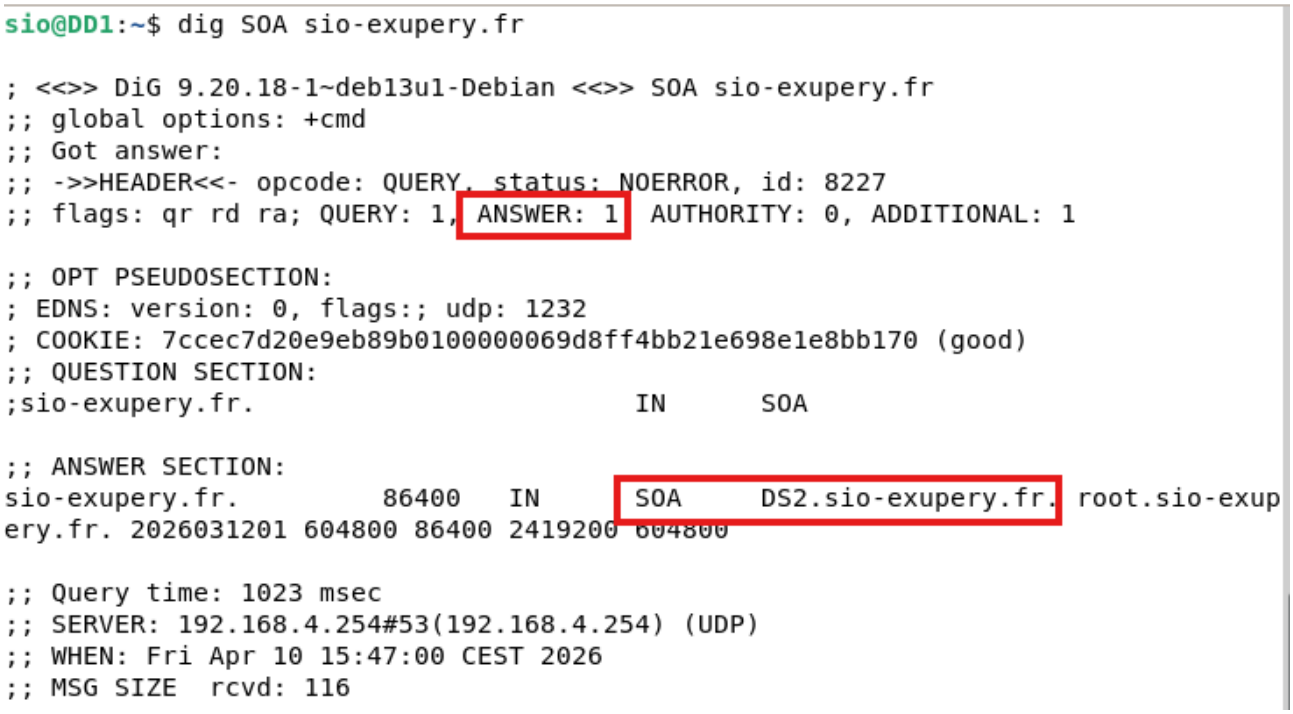
On modifie le fichier /etc/bind/named.conf.options. La directive forwarders doit renvoyer vers la nouvelle adresse IP de DS2 pour les résolutions hors zone intra.sio-exupery.fr

On relance le service DNS sur DS1



4. Tests depuis DD1

On test les deux résolutions DNS figurant ci-dessous

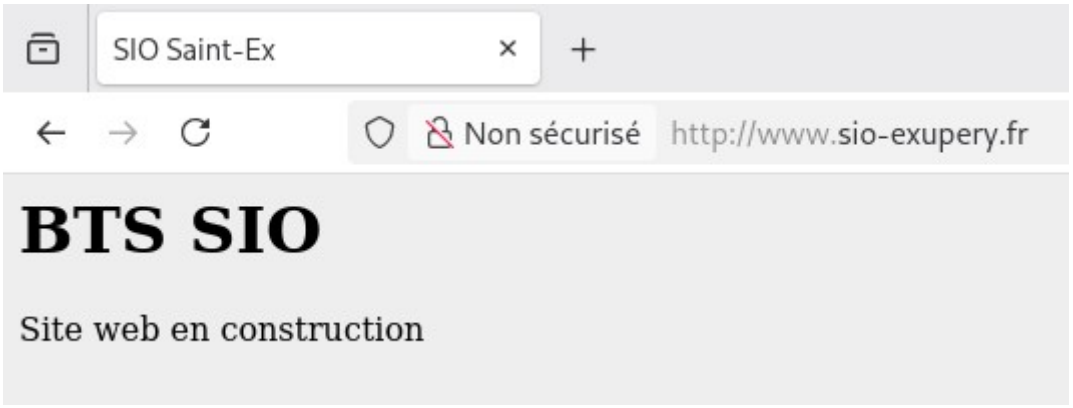


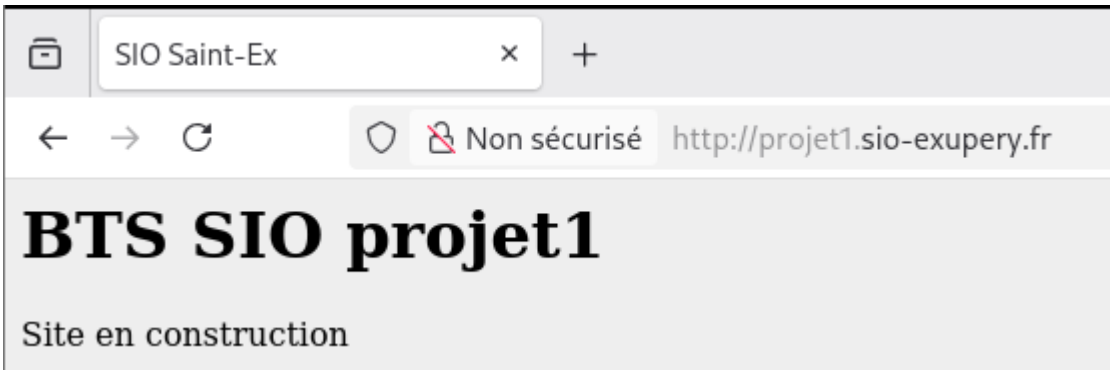
```
sio@DD1:~$ dig SOA intra.sio-exupery.fr

; <<>> DiG 9.20.18-1~deb13u1-Debian <<>> SOA intra.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30517
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b90903519e2916490100000069d8ffb8131f8fd91449dedc (good)
;; QUESTION SECTION:
;intra.sio-exupery.fr.          IN      SOA

;; ANSWER SECTION:
intra.sio-exupery.fr.   86400   IN      SOA     DS1.intra.sio-exupery.fr. root.in
tra.sio-exupery.fr. 2026031214 604800 86400 2419200 604800

;; Query time: 3 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Fri Apr 10 15:48:49 CEST 2026
;; MSG SIZE  rcvd: 122
```

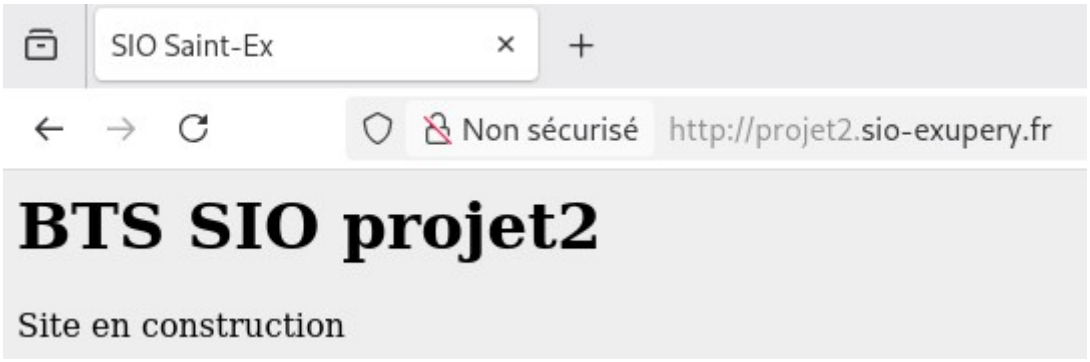
On vérifie la résolution hors zones intra.sio-exupery.fr et sio-exupery.fr

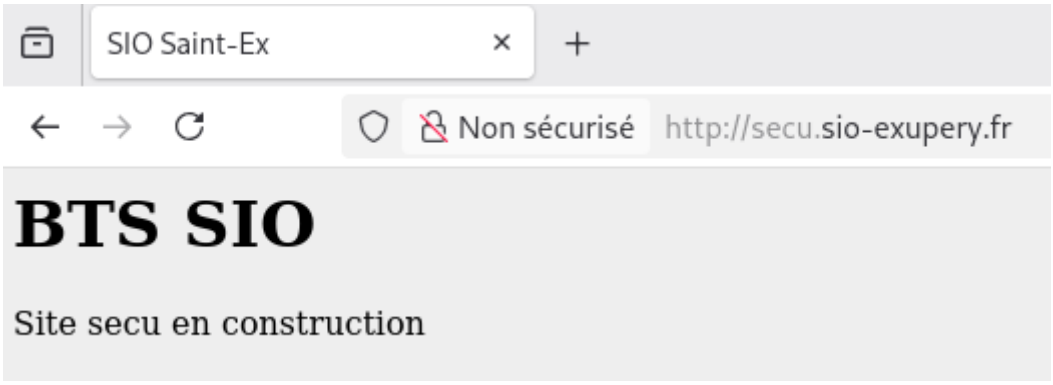
```
sio@DD1:~$ dig www.ac-nice.fr

; <<>> DiG 9.20.18-1~deb13u1-Debian <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62486
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f7cc35d37920a7090100000069d8fff0f26ff14dc692db5e (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                        IN      A

;; ANSWER SECTION:
www.ac-nice.fr.         3152    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     141.101.90.106
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.105
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.107
```

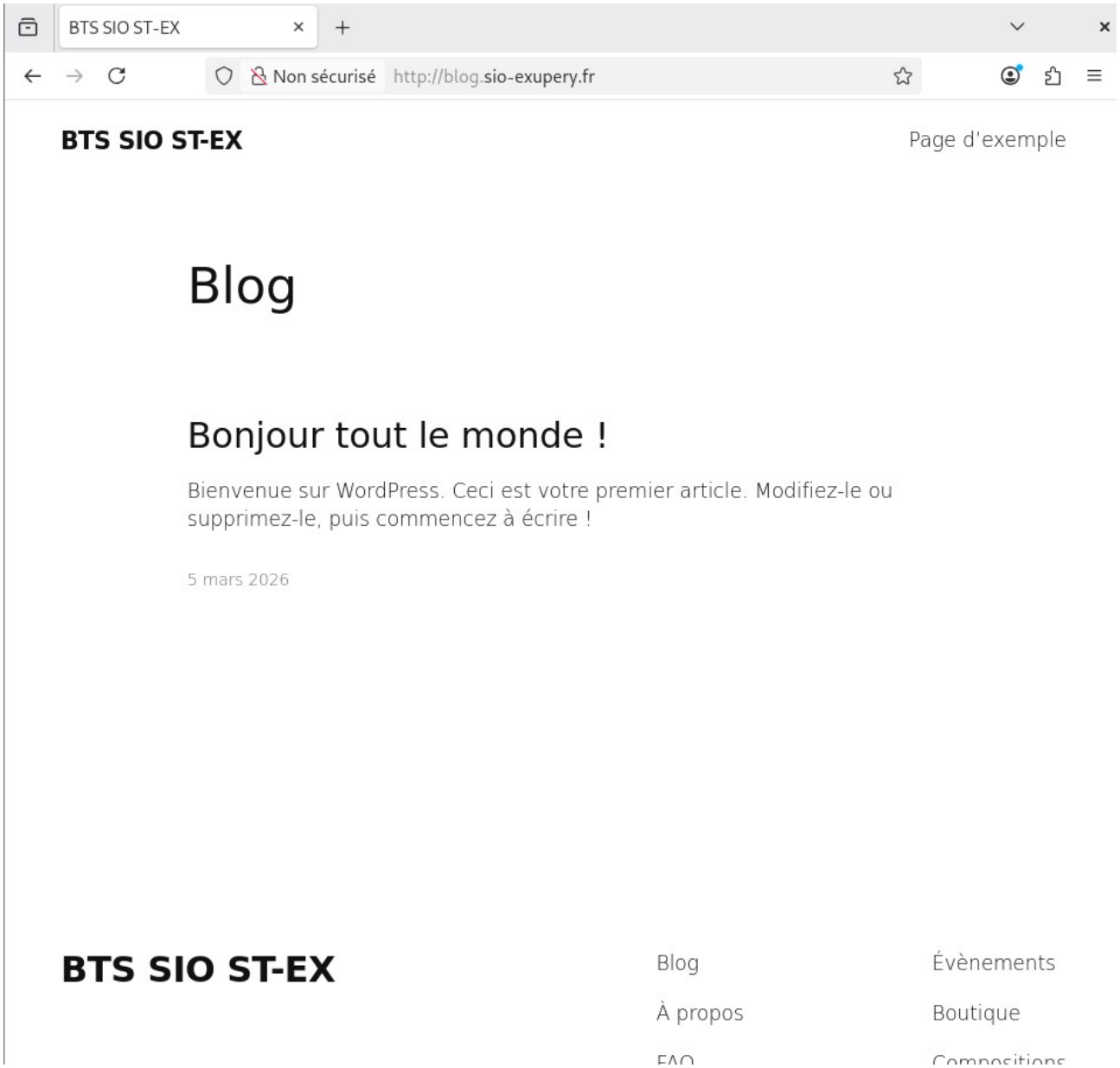
On vérifie l’accessibilité aux différents sites hébergés sur DS2 situé maintenant dans la DMZ





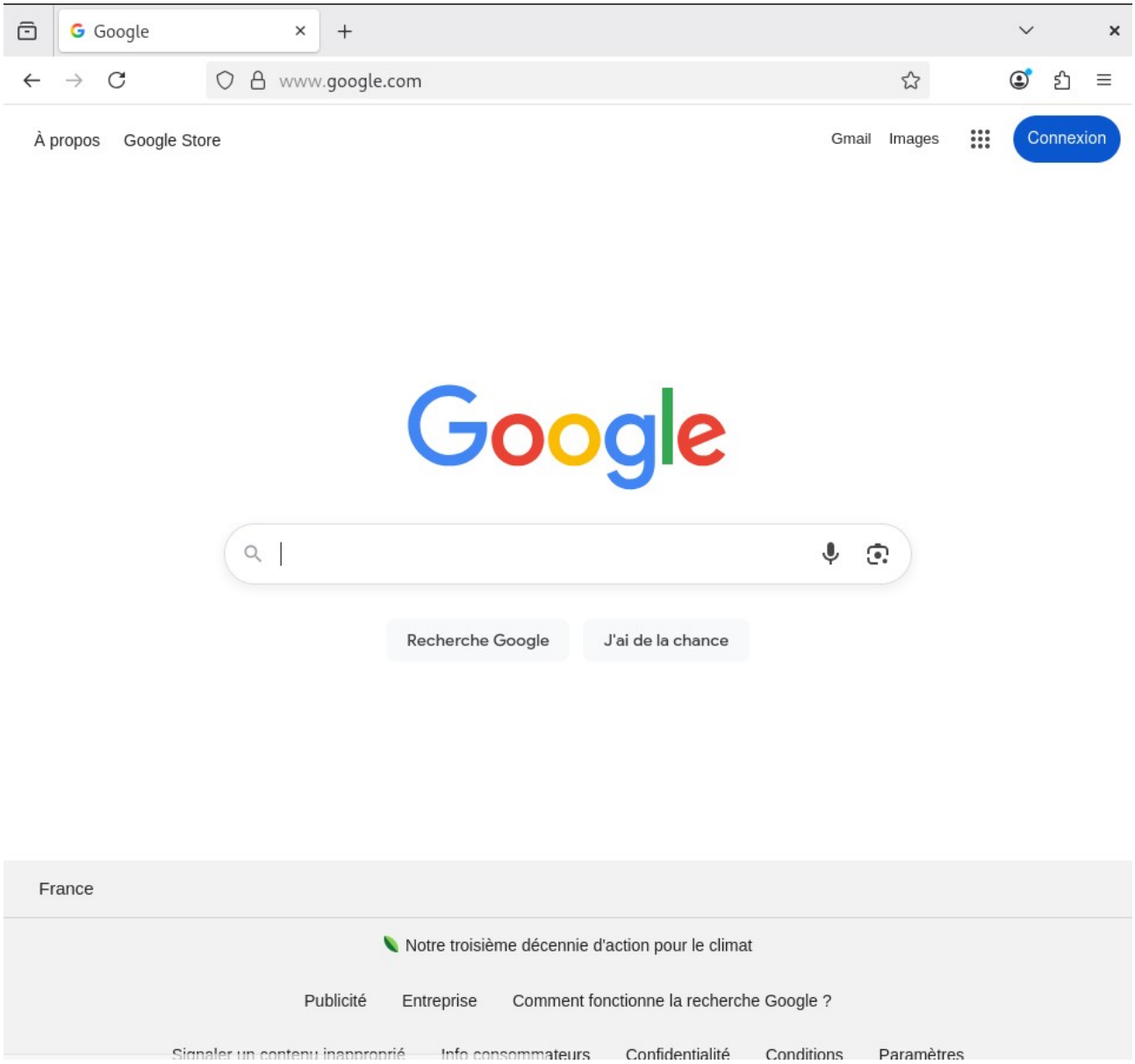


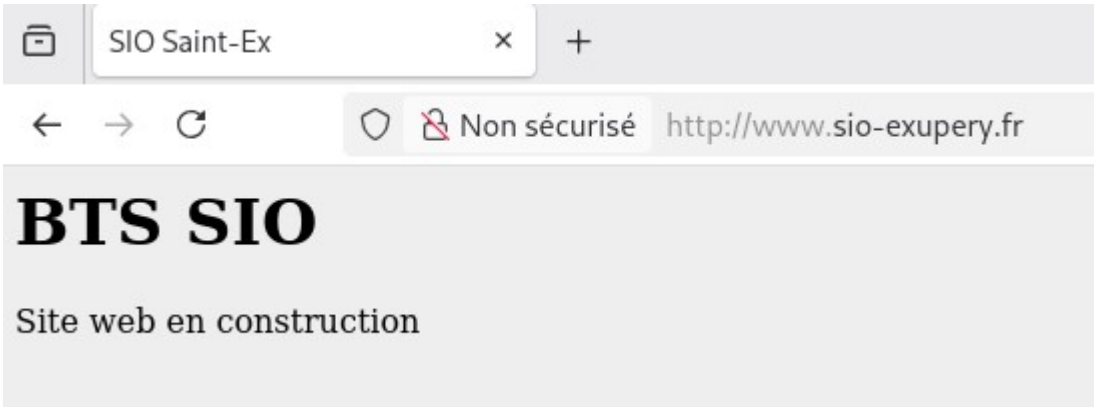




5. Test du pare-feu

On testez depuis DD1 les communications Internet ainsi que l'accès aux sites Web hébergés sur DS2 avec le pare-feu activé


Google
www.google.com
À propos
Google Store
Gmail
Images
Connexion
Google
Recherche Google
J'ai de la chance
France
Notre troisième décennie d'action pour le climat
Publicité
Entreprise
Comment fonctionne la recherche Google ?
Signaler un contenu inapproprié
Info consommateurs
Confidentialité
Conditions
Paramètres


SIO Saint-Ex
Non sécurisé
http://www.sio-exupery.fr
BTS SIO
Site web en construction

On vérifie que le serveur DNS et Web DS2 soit accessible depuis l'extérieur on ajoute donc une route statique sur le système hôte vers le réseau 192.168.2.0 en lui indiquant de passer par l'interface enp0s3 du serveur US3 ayant pour adresse IP 172.17.101.219

```
Microsoft Windows [version 10.0.26200.8037]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>route add 192.168.2.0 mask 255.255.255.0 172.17.101.219
 OK!

C:\Windows\System32>
```

Afin d'utiliser l'adresse http://www.sio-exupery.fr à la place de l'adresse IP, on met comme serveur DNS principal, toujours sur le système hôte, 192.168.2.1 dans les propriétés de votre connexion au réseau local. La page index.html doit apparaître dans votre navigateur