

- [Accueil](#)
- Missions 1 à 5
 - [Mission 1 : Configuration réseau](#)
 - [Mission 2 : GPG](#)
 - [Mission 3 : Clonezilla](#)
 - [Mission 4 : BackupPC](#)
 - [Mission 5 : MariaDB](#)
- Missions 6 à 10
 - [Mission 6 : DHCP](#)
 - [Mission 7 : Failover](#)
 - [Mission 8 : DNS](#)
 - [Mission 9 : Nginx](#)
 - [Mission 10 : FTP](#)
- [Mission 11 : SSL/TLS](#)
- [Mission 12 : OPNsense](#)
- [Mission 13 : Zabbix](#)

OPNsense

I) Pare-feu et OPNsense

A) Qu'est-ce qu'un pare-feu ?

Un pare-feu, également connu sous le nom de firewall en anglais, est un dispositif de sécurité informatique conçu pour surveiller, filtrer et contrôler le trafic réseau, en fonction de règles prédéfinies. L'objectif principal d'un pare-feu est de protéger un réseau informatique, comme celui d'une entreprise ou d'un particulier, en empêchant l'accès non autorisé ou en bloquant les communications indésirables.

Il existe deux types principaux de pare-feu :

Pare-feu matériel : Il s'agit d'un dispositif physique dédié, généralement installé entre le réseau local et l'Internet. Les pare-feu matériels sont autonomes et agissent comme une barrière entre le réseau interne et les menaces externes. Ils peuvent offrir une protection robuste en filtrant le trafic en fonction d'adresses IP, de ports et de protocoles.

Pare-feu logiciel : Il s'agit d'un programme logiciel installé sur un ordinateur ou un serveur. Les pare-feu logiciels peuvent être configurés pour contrôler le trafic entrant et sortant de cet appareil particulier. Ils sont souvent utilisés pour protéger les ordinateurs individuels et peuvent être intégrés dans des solutions de sécurité plus larges.

Les pare-feu peuvent être configurés pour autoriser ou bloquer différents types de trafic en fonction de règles spécifiques définies par l'administrateur réseau. Ces règles peuvent être basées sur des adresses IP, des ports, des protocoles ou d'autres critères. Les pare-feu sont un élément essentiel de la sécurité informatique, contribuant à protéger les réseaux contre les attaques malveillantes telles que les tentatives d'intrusion, les virus, les vers et autres menaces en ligne.

B) OPNsense

OPNsense est une distribution open-source de pare-feu et de routeur basée sur le système d'exploitation FreeBSD. Elle est conçue pour fournir des fonctionnalités avancées de sécurité réseau, de gestion du trafic et d'administration système. OPNsense offre une interface utilisateur basée sur le web pour simplifier la configuration et la gestion des fonctionnalités du pare-feu.

Voici quelques caractéristiques importantes d'OPNsense :

Pare-feu avancé : OPNsense propose un ensemble complet de fonctionnalités de pare-feu, y compris la prise en charge de la prévention d'intrusion (IPS), de la détection de logiciels malveillants, du filtrage de contenu, de la gestion des règles de pare-feu et plus encore.

VPN (Virtual Private Network) : Il offre la possibilité de mettre en place des connexions VPN, permettant ainsi de sécuriser les communications réseau à travers Internet.

Proxy : OPNsense peut être configuré pour agir en tant que serveur proxy, offrant ainsi des fonctionnalités telles que le filtrage web et la mise en cache.

OPNsense fait donc office de pare-feu logiciel.

II) IPtables

Afin de configurer notre pare-feu, nous créons un script IPtables. Ce script servira de base à la création de notre pare-feu avec OPNsense :

```
#!/bin/bash

iptables -F
iptables -X

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#-----
#- - - - - STATEFULL
#- - - - -
#-----

iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

```
#-----  
-----  
#--                               SSH  
--  
#-----  
-----  
  
#reseau beaup vers notre reseau  
iptables -A FORWARD -p tcp -s 10.187.20.0/24 -d 10.31.176.0/20 --dport  
22 -j ACCEPT  
  
#autoriser les connexion ssh entre lan et dmz  
iptables -A FORWARD -p tcp -s 10.31.176.0/20 -d 10.31.176.0/20 --dport  
22 -j ACCEPT  
  
#reseau beaup vers routeur  
iptables -A INPUT -p tcp -s 10.187.20.0/24 --dport 22 -j ACCEPT  
  
#-----  
-----  
#--                               ICMP  
--  
#-----  
-----  
  
# autoriser uniquement les echo reply et request  
iptables -A FORWARD -p icmp --icmp-type 0 -s 10.31.176.0/20 -j ACCEPT  
iptables -A FORWARD -p icmp --icmp-type 8 -s 10.31.176.0/20 -j ACCEPT  
  
#autoriser les pings du reseau de beaup vers notre reseau  
iptables -A FORWARD -p icmp --icmp-type 0 -s 10.187.20.0/24 -d  
10.31.176.0/20 -j ACCEPT  
iptables -A FORWARD -p icmp --icmp-type 8 -s 10.31.176.0/20 -d  
10.187.20.0/24 -j ACCEPT  
  
#autoriser les pings de Backuppc vers la DMZ  
iptables -A FORWARD -p icmp --icmp-type 0 -s 10.31.177.73/22 -d  
10.31.185.0/22 -j ACCEPT  
iptables -A FORWARD -p icmp --icmp-type 8 -s 10.31.185.0/22 -d  
10.31.177.73/22 -j ACCEPT  
iptables -A FORWARD -p icmp --icmp-type 0 -s 10.31.177.73/22 -d  
10.31.186.0/22 -j ACCEPT  
iptables -A FORWARD -p icmp --icmp-type 8 -s 10.31.186.0/22 -d  
10.31.177.73/22 -j ACCEPT  
  
#autoriser les pings vers notre routeur  
iptables -A INPUT -p icmp --icmp-type 0 -d 10.187.20.0/24 -j ACCEPT  
iptables -A INPUT -p icmp --icmp-type 8 -s 10.31.179.254/22 -j ACCEPT  
iptables -A INPUT -p icmp --icmp-type 8 -s 10.31.187.254/22 -j ACCEPT  
iptables -A INPUT -p icmp --icmp-type 8 -s 172.31.176.254/22 -j ACCEPT
```

```
#autoriser notre routeur a ping le réseau 10.31.80.0/20
iptables -A INPUT -p icmp --icmp-type 0 -s 10.31.179.254/22 -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 0 -s 10.31.187.254/22 -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 0 -s 172.31.176.254/22 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 8 -d 10.31.176.0/20 -j ACCEPT

#-----
#-----
#--                               DNS
--
#-----
#-----

#autoriser contact reseau beaup vers dns 1 et 2
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d
10.31.185.53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d
10.31.185.54 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d
10.31.186.53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d
10.31.186.54 -j ACCEPT

# DNS Marius
iptables -A FORWARD -p udp --dport 53 -s 10.31.185.53 -d 8.8.8.8 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.185.53 -d 8.8.4.4 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.185.54 -d 8.8.8.8 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.185.54 -d 8.8.4.4 -j
ACCEPT

# DNS Lucie
iptables -A FORWARD -p udp --dport 53 -s 10.31.186.53 -d 8.8.8.8 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.186.53 -d 8.8.4.4 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.186.54 -d 8.8.8.8 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.186.54 -d 8.8.4.4 -j
ACCEPT

#autoriser le routeur a faire des request vers les dns
iptables -A OUTPUT -p udp --dport 53 -d 10.31.185.53 -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -d 10.31.185.54 -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -d 10.31.186.53 -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -d 10.31.186.54 -j ACCEPT
#autoriser LAN a faire de request DNS
```

```
iptables -A FORWARD -p udp --dport 53 -s 10.31.176.0/22 -d
10.31.185.53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.176.0/22 -d
10.31.185.54 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.176.0/22 -d
10.31.186.53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.176.0/22 -d
10.31.186.54 -j ACCEPT
```

```
#-----
```

```
#-- HTTP
--
```

```
#-----
```

```
-----
```

```
#autoriser les request http vers nos serveur web
```

```
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d
10.31.185.80 -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d
10.31.177.80 -j ACCEPT
```

```
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d
10.31.186.80 -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d
10.31.178.80 -j ACCEPT
```

```
# backuppc
```

```
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d
10.31.177.73 -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d
10.31.178.73 -j ACCEPT
```

```
#autoriser nos serveur web a avoir internet
```

```
iptables -A FORWARD -p tcp --dport 80 -s 10.31.184.0/22 ! -d
10.31.176.0/22 -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -s 10.31.176.0/22 ! -d
10.31.184.0/22 -j ACCEPT
```

```
#accès internet sur notre réseau
```

```
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
```

```
#-----
```

```
-----
```

```
#-- HTTPS
--
```

```
#-----
```

```
-----
```

```
#autoriser les request http vers nos serveur web
```

```
iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/24 -d
10.31.185.80 -j ACCEPT
```

```
iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/24 -d
10.31.177.80 -j ACCEPT

iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/24 -d
10.31.186.80 -j ACCEPT
iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/24 -d
10.31.178.80 -j ACCEPT

#autoriser nos serveur web a avoir internet
iptables -A FORWARD -p tcp --dport 443 -s 10.31.184.0/22 ! -d
10.31.176.0/22 -j ACCEPT
iptables -A FORWARD -p tcp --dport 443 -s 10.31.176.0/22 ! -d
10.31.184.0/22 -j ACCEPT

# backuppc
iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/24 -d
10.31.177.73 -j ACCEPT
iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/24 -d
10.31.178.73 -j ACCEPT

#accès internet sur notre routeur
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT

#-----
#--
--
#-----
-----

iptables -A FORWARD -p tcp --dport 8006 -s 10.187.20.0/24 -d
10.31.176.1 -j ACCEPT

#-----
#--
--
#-----
-----

#autoriser les transfert ftp
# Marius
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d
10.31.185.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 20 -d 10.187.20.0/24 -s
10.31.185.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d
10.31.185.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 20 -d 10.187.20.0/24 -s
10.31.185.15 -j ACCEPT
```

```
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d
10.31.185.16 -j ACCEPT
iptables -A FORWARD -p tcp --dport 20 -d 10.187.20.0/24 -s
10.31.185.16 -j ACCEPT

# Lucie
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d
10.31.186.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 20 -d 10.187.20.0/24 -s
10.31.186.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d
10.31.186.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 20 -d 10.187.20.0/24 -s
10.31.186.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d
10.31.186.16 -j ACCEPT
iptables -A FORWARD -p tcp --dport 20 -d 10.187.20.0/24 -s
10.31.186.16 -j ACCEPT

#autoriser les transfert ftps
# Marius
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d
10.31.185.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 989 -d 10.187.20.0/24 -s
10.31.185.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d
10.31.185.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 989 -d 10.187.20.0/24 -s
10.31.185.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d
10.31.185.16 -j ACCEPT
iptables -A FORWARD -p tcp --dport 989 -d 10.187.20.0/24 -s
10.31.185.16 -j ACCEPT
# Lucie
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d
10.31.186.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 989 -d 10.187.20.0/24 -s
10.31.186.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d
10.31.186.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 989 -d 10.187.20.0/24 -s
10.31.186.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d
10.31.186.16 -j ACCEPT
iptables -A FORWARD -p tcp --dport 989 -d 10.187.20.0/24 -s
10.31.186.16 -j ACCEPT

#gère le mode passif de ftp/ftps
# Marius
iptables -A FORWARD -p tcp --dport 55000:60000 -s 10.187.20.0/24 -d
10.31.185.20 -j ACCEPT
```

```
iptables -A FORWARD -p tcp --dport 55000:60000 -s 10.187.20.0/24 -d 10.31.185.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 55000:60000 -s 10.187.20.0/24 -d 10.31.185.16 -j ACCEPT
```

Lucie

```
iptables -A FORWARD -p tcp --dport 55000:60000 -s 10.187.20.0/24 -d 10.31.186.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 55000:60000 -s 10.187.20.0/24 -d 10.31.186.15 -j ACCEPT
iptables -A FORWARD -p tcp --dport 55000:60000 -s 10.187.20.0/24 -d 10.31.186.16 -j ACCEPT
```

```
#-----
-----
```

```
#--                                SAMBA
--
```

```
#-----
-----
```

```
iptables -A FORWARD -p tcp --dport 445 -s 10.187.20.0/24 -d 10.31.177.13 -j ACCEPT
iptables -A FORWARD -p tcp --dport 445 -s 10.187.20.0/24 -d 10.31.178.13 -j ACCEPT
```

```
#-----
-----
```

```
#--                                DB
--
```

```
#-----
-----
```

```
iptables -A FORWARD -p tcp --dport 3306 -s 10.31.185.80 -d 10.31.177.33 -j ACCEPT
iptables -A FORWARD -p tcp --dport 3306 -s 10.31.186.80 -d 10.31.178.33 -j ACCEPT
```

Nous pouvons exécuter le script et vérifier que toutes les communications puissent aboutir une à une.

III) OPNsense

A) Mise en place du pare-feu OPNsense

Dans un premier temps, nous commençons par créer une clé bootable à l'aide du logiciel Rufus. Nous téléchargeons l'image sur le site suivant : <https://opnsense.org/download/>

Avant de reconfigurer notre routeur, nous notons les correspondances entre nos interfaces réseaux, nos adresses MAC et nos adresses IP afin de pouvoir les reconfigurer plus tard lors de

l'installation du pare feu :

- enp2s0 (WAN) : 172.31.176.254/16 | fc:aa:14:52:b3:24
- enp4s0 (LAN) : 10.31.179.254/22 | 64:ee:b7:23:b1:87
- enp5s0 (DMZ) : 10.31.187.254/22 | 64:ee:b7:23:b1:59

Nous pouvons commencer à faire l'installation d'OPNsense sur notre routeur à l'aide de notre clé bootable. Nous lançons OPNsense. Par défaut, le compte utilisateur est root/opnsense. Nous nous connectons sur le terminal et choisissons l'option "Shell" (8). Nous pouvons installer OPNsense en entrant la commande ci-dessous :

```
opnsense-install
```

Plusieurs étapes sont à compléter :

1. Sélection du clavier :
2. Choix du système de fichiers (ZFS)
3. Partitionnement
4. Sélection du disque
5. Suppression des anciennes données du disque
6. Autoriser/Refuser le swap
7. Changement du mot de passe
8. Finalisation de l'installation

Nous pouvons maintenant configurer nos interfaces en sélectionnant l'option "Assign interfaces" (1). Nous commençons par assigner les interfaces à leurs nom en faisant la correspondance avec leur nom et leur adresse MAC. Ainsi :

```
re0 = WAN  
re1 = LAN  
opt1 = DMZ
```

Il est possible durant l'assignation des interfaces d'en rajouter une nouvelle étant donné que seulement deux interfaces (re0 et re1) sont disponibles au début de la configuration.

Nous devons maintenant assigner nos adresses IP à nos interfaces. Pour ce faire, nous choisissons l'option "Set interface(s) IP address" (2). Nous assignons à chaque interface son adresse IP ainsi que son masque, et ajoutons à l'interface WAN sa passerelle par défaut (172.31.0.1/16).

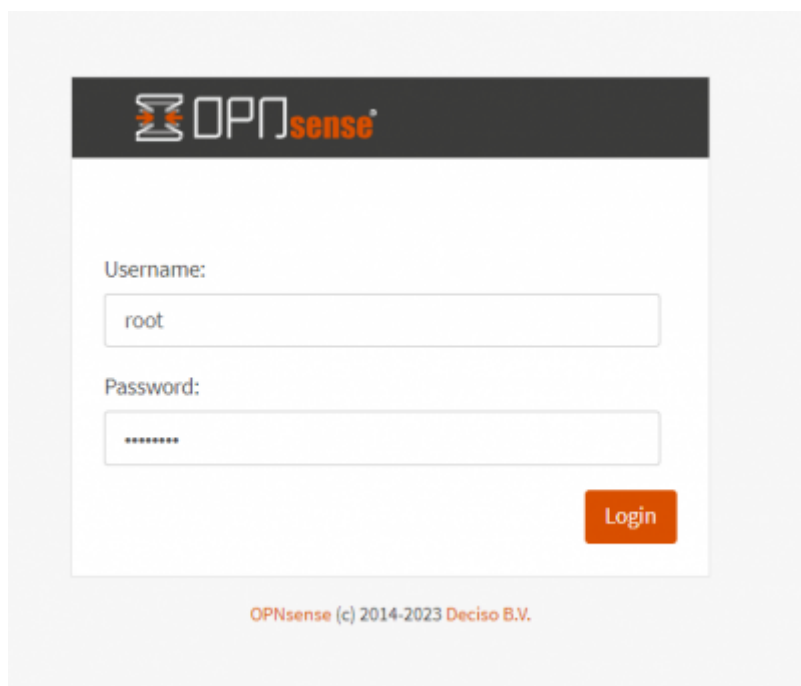
Par défaut, le pare-feu est activé et bloque tous les flux. Pour accéder à l'interface web, nous devons momentanément désactiver le pare-feu :

```
pfctl -d
```

La commande pour réactiver le pare-feu est “pfctl -e”.

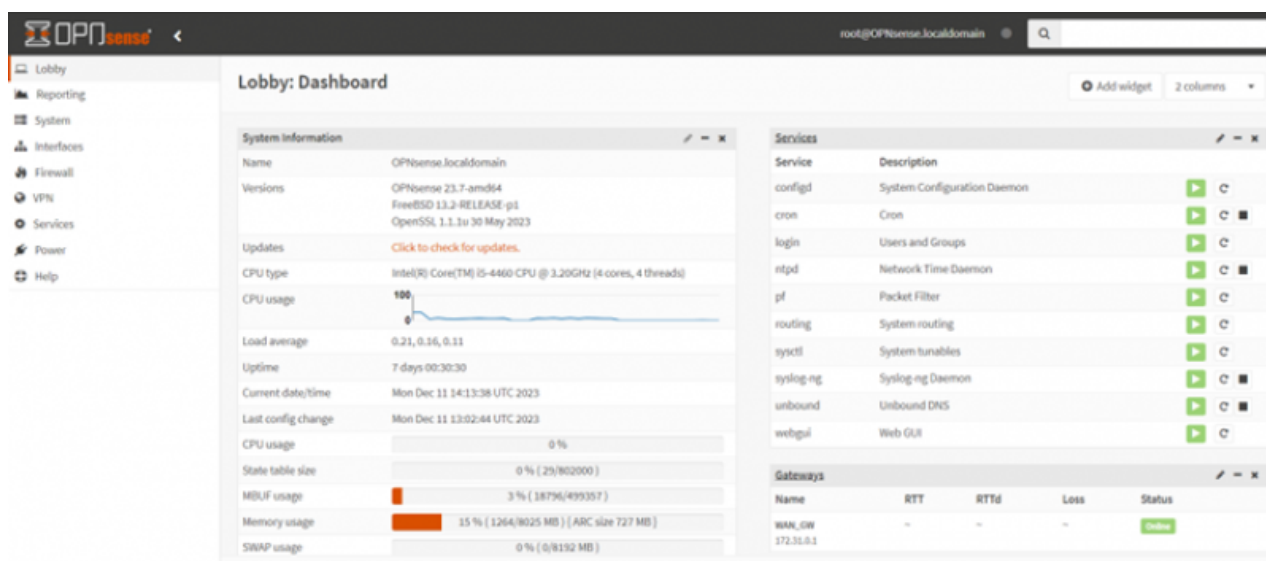
B) Configuration d'OPNsense

Une fois l'installation terminée, nous pouvons accéder à l'interface web d'OPNsense à l'adresse suivante : <https://10.31.179.254> :



The image shows the OPNsense login interface. At the top is the OPNsense logo. Below it, there are two input fields: 'Username:' with 'root' entered, and 'Password:' with '*****' entered. A green 'Login' button is positioned to the right of the password field. At the bottom, it says 'OPNsense (c) 2014-2023 Deciso B.V.'.

Les identifiants sont ceux que nous avons changé lors de l'installation du pare-feu, donc root/opnsense. Voici l'interface de gestion du Pare-feu :



The image shows the OPNsense 'Lobby: Dashboard'. On the left is a sidebar with navigation links: Lobby, Reporting, System, Interfaces, Firewall, VPN, Services, Power, and Help. The main content area is divided into several sections:

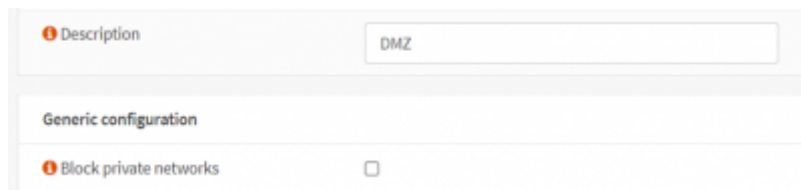
- System Information:** A table showing system details like Name (OPNsense.localdomain), Versions (OPNsense 23.7-amd64, FreeBSD 13.2-RELEASE-p1, OpenSSL 1.1.1u 30 May 2023), Updates (Click to check for updates), CPU type (Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz (4 cores, 4 thread)), CPU usage (100%), Load average (0.21, 0.16, 0.11), Uptime (7 days 00:30:30), Current date/time (Mon Dec 11 14:13:38 UTC 2023), Last config change (Mon Dec 11 13:02:44 UTC 2023), CPU usage (0%), State table size (0% (25/802000)), MBUF usage (3% (18796/499357)), Memory usage (15% (1264/8025 MB) (ARC size 727 MB)), and SWAP usage (0% (0/8192 MB)).
- Services:** A table listing system services and their status.
- Gateways:** A table showing gateway status.

Service	Description	Status
configd	System Configuration Daemon	Running
cron	Cron	Running
login	Users and Groups	Running
ntpd	Network Time Daemon	Running
pf	Packet Filter	Running
routing	System routing	Running
systd	System tunables	Running
syslog-ng	Syslog-ng Daemon	Running
unbound	Unbound DNS	Running
webgui	Web GUI	Running

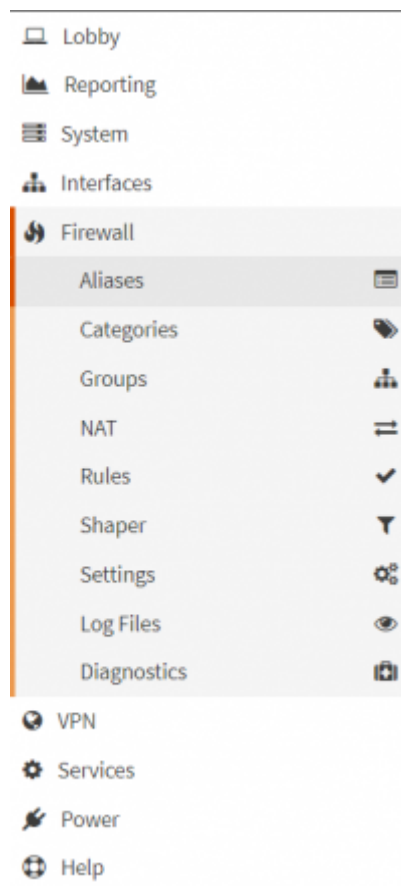
Gateway	RTT	RTTd	Loss	Status
WAN_0W	--	--	--	Online

Dans un premier temps, nous devons changer le nom de l'interface reliée au réseau DMZ. Pour cela, nous sélectionnons “Interfaces”, puis l'option “[NOM DE L'INTERFACE]”. Nous en

changeons la descriptions et nous décochons la case "Block private networks". Cela nous permettra de pouvoir autoriser les communications entre nos réseaux ayant des adresses privées. Nous devons décocher cette case pour toutes les interfaces.



Nous créons ensuite de nouveaux alias qui permettront de sélectionner plusieurs machines pour une seule et même règle. Pour ce faire, nous sélectionnons "Firewall", puis l'option "Aliases" :



Nous créerons de nouveaux alias qui regrouperont certaines machines afin d'optimiser nos règles :

- Beaupeyrat : 10.187.20.0/24
- FTP : 10.31.185.20, 10.31.185.15, 10.31.185.16, 10.31.186.20, 10.31.186.15, 10.31.186.16
- Web : 10.31.177.80, 10.31.178.80, 10.31.185.80, 10.31.186.80
- Samba : 10.31.177.13, 10.31.178.13
- Backuppc : 10.31.177.73, 10.31.178.73
- DNS : 10.31.185.53, 10.31.185.54, 10.31.186.53, 10.31.186.54

Edit Alias

full help

Enabled

☒

Name

Type

Network(s)

Categories

Content

Clear All

Copy

Paste

Statistics

☒

Description

Cancel

Save

Aliases

GeoIP settings























Q

Search

Filter type

Categories

7

<input type="checkbox"/> Enabled	Name	Type	Description	Content	Loaded#	Last updated	Commands
<input type="checkbox"/> <input checked="" type="checkbox"/>	Beaupeyrat	Network(s)		10.187.20.0/24	1	2023-12-05 13:56:04	  
<input type="checkbox"/> <input checked="" type="checkbox"/>	FTP	Host(s)	srv-ftp	10.31.185.20,10.31.1...	6	2023-12-11 14:58:00	  
<input type="checkbox"/> <input checked="" type="checkbox"/>	Web	Host(s)	Serveurs web	10.31.177.80,10.31.1...	4	2023-12-11 14:56:24	  
<input type="checkbox"/> <input checked="" type="checkbox"/>	Samiba	Host(s)	Samiba	10.31.177.13,10.31.1...	2	2023-12-11 15:00:00	  
<input type="checkbox"/> <input checked="" type="checkbox"/>	Backuppc	Host(s)	Serveurs Backuppc	10.31.177.73,10.31.1...	2	2023-12-11 15:00:00	  
<input type="checkbox"/> <input checked="" type="checkbox"/>	DNS	Host(s)	Serveurs DNS	10.31.185.53,10.31.1...	4	2023-12-11 15:00:00	  
<input type="checkbox"/> <input checked="" type="checkbox"/>	bogons	External (advanced)	bogon networks (int...		10		 
							 

«

<

1

2

>

»

Showing 1 to 7 of 14 entries

Nous pouvons maintenant écrire nos règles de pare-feu. Toujours dans l'onglet "Firewall", nous sélectionnons l'option "Rules". L'option "Floating" correspond aux règles pouvant être affectées à plusieurs interfaces à la fois. Il existe une option pour chaque interface. Nous sélectionnons l'option "Floating". Nous pouvons créer une nouvelle règle. La règle que nous allons créer sera celle autorisant le réseau de Beaupeyrat (interface WAN) à communiquer avec les DNS (interface DMZ). Nous devons ainsi :

- Activer l'option "Quick" permettant d'exécuter une action lorsque cette règle est utilisée
- Sélectionner l'Interface concernée (WAN)
- Sélectionner la direction (IN)
- Sélectionner le protocole (UDP)
- Sélectionner une source (l'alias "Beaupeyrat")
- Sélectionner une destination (l'alias "DNS")
- Sélectionner une plage de port (DNS)
- Renseigner une catégorie (Allow DNS)
- Renseigner une description (Allow DNS from Beaupeyrat)

Un message apparait alors nous informant de la modification de règles. Nous cliquons sur le bouton "Apply changes" :

The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

Nous pouvons ainsi créer toutes nos règles pour chaque interface :

Floating :

Firewall: Rules: Floating										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules											
	IPv4 UDP	Beaupeyrat	*	DNS	53 (DNS)	*	*	1	Allow DNS from Beaupeyrat		
	IPv4 TCP	*	*	This Firewall	80 (HTTP)	*	*	1	Allow HTTP in firewall		
	IPv4 TCP	*	*	This Firewall	443 (HTTPS)	*	*	1	Allow HTTPS in firewall		
	IPv4 ICMP	Beaupeyrat	*	LAN net	*	*	*	1	Allow ping (Request) LAN		
	IPv4 ICMP	Beaupeyrat	*	LAN net	*	*	*	1	Allow ping (Reply) LAN		
	IPv4 ICMP	Beaupeyrat	*	DMZ net	*	*	*	1	Allow ping (Request) DMZ		
	IPv4 ICMP	Beaupeyrat	*	DMZ net	*	*	*	1	Allow ping (Reply) DMZ		
	IPv4 TCP/UDP	*	*	*	22 (SSH)	*	*	3	Allow SSH everywhere		

DMZ :

Firewall: Rules: DMZ										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules											
Floating rules											
	IPv4 TCP	DMZ net	*	LAN net	80 (HTTP)	*	*		Deny HTTP DMZ to LAN		
	IPv4 TCP	DMZ net	*	LAN net	443 (HTTPS)	*	*		Deny HTTPS DMZ to LAN		
	IPv4 UDP	10.31.185.67	67 - 68	10.31.177.67	67 - 68	*	*		Allow Acces DHCP		
	IPv4 UDP	10.31.186.67	67 - 68	10.31.178.67	67 - 68	*	*		Allow Acces DHCP		
	IPv4 UDP	10.31.185.67	67 - 68	10.31.177.68	67 - 68	*	*		Allow Acces DHCP		
	IPv4 UDP	10.31.186.67	67 - 68	10.31.178.68	67 - 68	*	*		Allow Acces DHCP		
	IPv4 TCP	10.31.185.80	*	10.31.177.33	3306	*	*		Allow BDD to Web-Pub-Marius		
	IPv4 TCP	10.31.186.80	*	10.31.178.33	3306	*	*		Allow BDD to Web-Pub-Lucie		
	IPv4 TCP	DMZ net	*	*	80 (HTTP)	*	*		Allow Internet		
	IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	*		Allow Internet		
	IPv4 UDP	DNS	*	*	53 (DNS)	*	*		Allow DNS to everywhere		

LAN :

Firewall: Rules: LAN

Select category

Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
Floating rules									
<input type="checkbox"/>	IPv4 TCP	LAN net	*	DMZ net	80 (HTTP)	*	*	Deny HTTP LAN to DMZ	
<input type="checkbox"/>	IPv4 TCP	LAN net	*	DMZ net	443 (HTTPS)	*	*	Deny HTTPS LAN to DMZ	
<input type="checkbox"/>	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	*	Allow Internet	
<input type="checkbox"/>	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	*	Allow Internet	
<input type="checkbox"/>	IPv4 ICMP	10.31.177.73	*	DMZ net	*	*	*	Allow ping backuppc	
<input type="checkbox"/>	IPv4 ICMP	10.31.177.73	*	DMZ net	*	*	*	Allow ping backuppc	
<input type="checkbox"/>	IPv4 UDP	LAN net	*	DNS	53 (DNS)	*	*	Allow DNS to DMZ	

WAN :

Firewall: Rules: WAN

Select category

Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
Floating rules									
<input type="checkbox"/>	IPv4 TCP/UDP	Beaupeyrat	*	10.31.176.1/22	8006	*	*	Access Promox	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	Backuppc	80 (HTTP)	*	*	Allow Access Backuppc (80)	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	Web	80 (HTTP)	*	*	Allow Access Websites (80)	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	Web	443 (HTTPS)	*	*	Allow Access Website (443)	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	Samba	445 (MS DS)	*	*	Allow Samba from Beaupeyrat	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	FTP	20 - 21	*	*	Allow Access FTP from Beaupeyrat	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	FTP	55000 - 60000	*	*	Allow Access FTPS from Beaupeyrat (passive mod)	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	FTP	989 - 990	*	*	Allow Access FTPS from Beaupeyrat	
<input type="checkbox"/>	IPv4 TCP	Beaupeyrat	*	10.31.176.252	80 (HTTP)	*	*	Allow Access Website OCS	

IV) Test

HTTP

La DMZ doit avoir accès à Internet :

```
root@srv-web2-1:~# apt update && apt upgrade
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Réception de :2 http://security.debian.org/debian-security bookworm-security InRelease [40,0 kB]
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [52,1 kB]
Réception de :4 http://security.debian.org/debian-security bookworm-security/main Sources [62,4 kB]
Réception de :5 http://security.debian.org/debian-security bookworm-security/non-free-firmware Sources [796 B]
Réception de :6 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [186 kB]
Réception de :7 http://security.debian.org/debian-security bookworm-security/main Translation-en [64,1 kB]
Réception de :8 http://security.debian.org/debian-security bookworm-security/non-free-firmware amd64 Packages [688 B]
334 ko réceptionnés en 8s (571 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
2 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
```

La LAN doit avoir accès à Internet :

```
root@srv-web2-2:~# apt update && apt upgrade
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Réception de :2 http://security.debian.org/debian-security bookworm-security InRelease [40,0 kB]
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [52,1 kB]
Réception de :4 http://security.debian.org/debian-security bookworm-security/main Sources [62,4 kB]
Réception de :5 http://security.debian.org/debian-security bookworm-security/non-free-firmware Sources [796 B]
Réception de :6 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [186 kB]
Réception de :7 http://security.debian.org/debian-security bookworm-security/main Translation-en [64,1 kB]
Réception de :8 http://security.debian.org/debian-security bookworm-security/non-free-firmware amd64 Packages [688 B]
334 ko réceptionnés en 8s (569 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
3 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
```

La LAN ne doit pas avoir accès aux machines de la DMZ en utilisant le protocole HTTP. Voici à quoi ressemble une requête CURL de la LAN vers la DMZ lorsque les flux ne sont pas filtrés :

```
root@srv-web2-2:~# curl http://www.gsb.org
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>
```

Voici les résultats de la requête CURL de la LAN vers la DMZ une fois que les flux sont filtrés :

```
root@srv-web2-2:~# curl http://www.gsb.org
curl: (28) Failed to connect to www.gsb.org port 80 after 130507 ms: Couldn't connect to server
```

La DMZ ne doit pas avoir accès aux machines de la LAN en utilisant le protocole HTTP. Voici à quoi ressemble une requête CURL de la DMZ vers la LAN lorsque les flux ne sont pas filtrés :

```
root@srv-web2-1:~# curl http://intranet.asie.gsb.org
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>
```

Voici les résultats de la requête CURL de la DMZ vers la LAN une fois que les flux sont filtrés :

```
root@srv-web2-1:~# curl http://intranet.asie.gsb.org
curl: (28) Failed to connect to intranet.asie.gsb.org port 80 after 129620 ms: Couldn't connect to server
```

HTTPS

La LAN ne doit pas avoir accès aux machines de la DMZ en utilisant le protocole HTTPS. Voici à quoi ressemble une requête CURL de la LAN vers la DMZ lorsque les flux ne sont pas filtrés :

```
root@srv-web2-2:~# curl https://www.gsb.org
curl: (60) SSL certificate problem: self-signed certificate
More details here: https://curl.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

Voici les résultats de la requête CURL de la LAN vers la DMZ une fois que les flux sont filtrés :

```
root@srv-web2-2:~# curl https://www.gsb.org
curl: (28) Failed to connect to www.gsb.org port 443 after 130984 ms: Couldn't connect to server
```

La DMZ ne doit pas avoir accès aux machines de la LAN en utilisant le protocole HTTPS. Voici à quoi ressemble une requête CURL de la DMZ vers la LAN lorsque les flux ne sont pas filtrés :


```
root@srv-web2-1:~# curl https://intranet.asie.gsb.org
curl: (60) SSL certificate problem: self-signed certificate
More details here: https://curl.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

Voici les résultats de la requête CURL de la DMZ vers la LAN une fois que les flux sont filtrés :

```
root@srv-web2-1:~# curl https://intranet.asie.gsb.org
curl: (28) Failed to connect to intranet.asie.gsb.org port 443 after 129781 ms: Couldn't connect to server
```

PING

Les requêtes ICMP request et reply doivent permettre depuis le réseau Beaupeyrat de ping la LAN :

```
PS C:\Users\Lucie> ping 10.31.178.80

Envoi d'une requête 'Ping' 10.31.178.80 avec 32 octets de données :
Réponse de 10.31.178.80 : octets=32 temps=3 ms TTL=62

Statistiques Ping pour 10.31.178.80:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 3ms, Maximum = 3ms, Moyenne = 3ms
```

Les requêtes ICMP request et reply doivent permettre depuis le réseau Beaupeyrat de ping la DMZ :

```
PS C:\Users\Lucie> ping 10.31.186.80

Envoi d'une requête 'Ping' 10.31.186.80 avec 32 octets de données :
Réponse de 10.31.186.80 : octets=32 temps=2 ms TTL=62

Statistiques Ping pour 10.31.186.80:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms
```

Les requêtes ICMP request et reply doivent permettre à la machine Backuppc de contacter la DMZ :

```
root@backup-01:~# ping 10.31.186.80
PING 10.31.186.80 (10.31.186.80): 56 data bytes
64 bytes from 10.31.186.80: icmp_seq=0 ttl=63 time=0,440 ms
^C--- 10.31.186.80 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0,440/0,440/0,440/0,000 ms
```

SSH

Le réseau LAN doit avoir accès au réseau DMZ :

```
root@backup-01:~# ssh std@10.31.186.53
std@10.31.186.53's password:
Linux ns2-1-pub 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec 11 14:39:00 2023 from 10.31.177.73
std@ns2-1-pub:~$
```


Le réseau DMZ doit avoir accès au réseau LAN :

```
root@ns2-1-pub:~# ssh std@10.31.177.73
std@10.31.177.73's password:
Linux backup-01 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec 11 14:13:12 2023 from 10.31.177.68
std@backup-01:~$ |
```

Le réseau de Beaupeyrat doit avoir accès au réseau DMZ :

```
root@ns2-1-pub:~# ssh std@10.31.177.73
std@10.31.177.73's password:
Linux backup-01 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec 11 14:13:12 2023 from 10.31.177.68
std@backup-01:~$ |
```

Le réseau de Beaupeyrat doit avoir accès au réseau LAN :

```
root@ns2-1-pub:~# ssh std@10.31.177.73
std@10.31.177.73's password:
Linux backup-01 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec 11 14:13:12 2023 from 10.31.177.68
std@backup-01:~$ |
```

DNS

Les DNS doivent pouvoir être joignables depuis le réseau de Beaupeyrat :

```
PS C:\Users\Lucie> nslookup documentation.asie.gsb.org
Serveur : UnKnown
Address: 10.31.186.53

Nom : documentation.asie.gsb.org
Address: 10.31.178.80
```

```
PS C:\Users\Lucie> nslookup documentation.asie.gsb.org
Serveur : UnKnown
Address: 10.31.185.53

Nom : documentation.asie.gsb.org
Address: 10.31.177.80
```

Les DNS doivent pouvoir être joignables depuis la LAN :

```
root@priv-db1:~# dig google.com

;<<>> DiG 9.18.19-1-deb12u1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 49282
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 89d28100c84dcb38010000006576ffb8301810bfeccfd9ec (good)
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                235     IN      A      142.251.37.46

;; Query time: 32 msec
;; SERVER: 10.31.185.53#53(10.31.185.53) (UDP)
;; WHEN: Mon Dec 11 13:25:28 CET 2023
;; MSG SIZE rcvd: 83
```

```
root@priv-db2:~# dig google.com

;<<>> DiG 9.18.19-1-deb12u1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 29434
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: d7b8926126beb3b101000000657701b3d78e929a76de37a1 (good)
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                300     IN      A      142.251.37.46

;; Query time: 52 msec
;; SERVER: 10.31.186.53#53(10.31.186.53) (UDP)
;; WHEN: Mon Dec 11 13:33:56 CET 2023
;; MSG SIZE rcvd: 83
```

DHCP

La DMZ a besoin de contacter le DHCP situé sur la LAN :

```
root@srv-web2-1:~# dhclient -r && dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

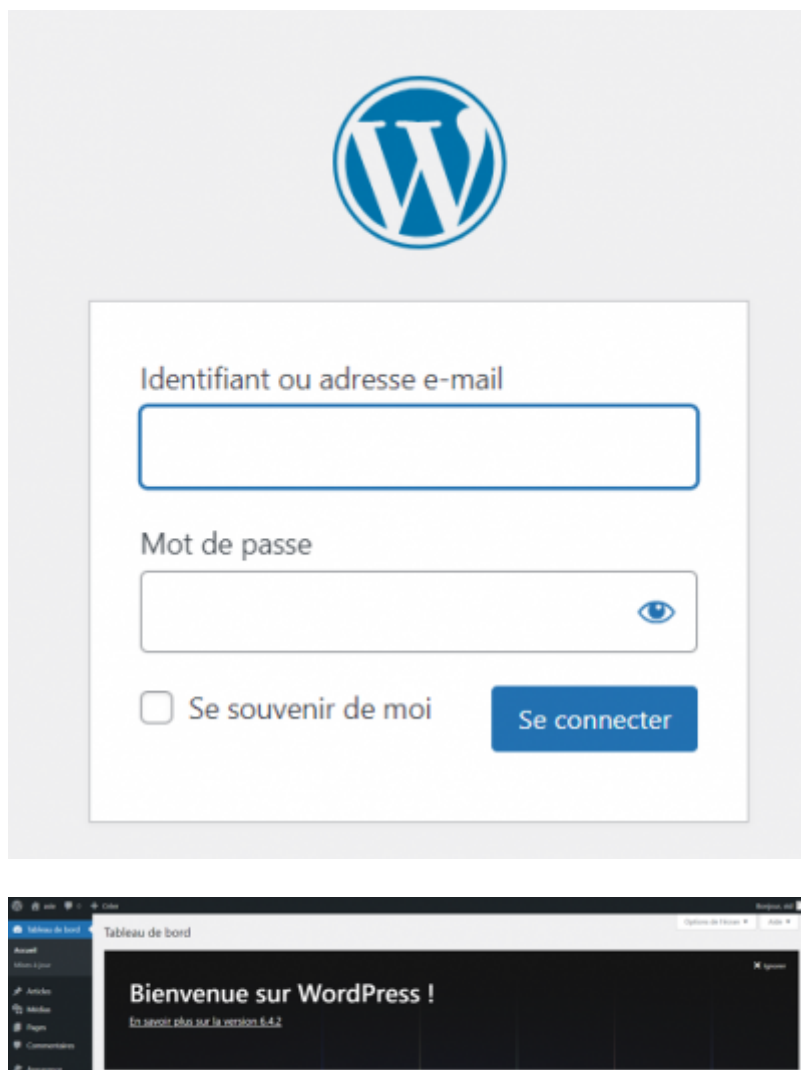
Listening on LPF/ens18/86:8e:ac:0f:5b:96
Sending on LPF/ens18/86:8e:ac:0f:5b:96
Sending on Socket/fallback
DHCPDISCOVER on ens18 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 10.31.186.80 from 10.31.185.67
DHCPREQUEST for 10.31.186.80 on ens18 to 255.255.255.255 port 67
DHCPACK of 10.31.186.80 from 10.31.185.67
bound to 10.31.186.80 -- renewal in 36053 seconds.
```

```
root@srv-web1-1:~# dhclient -r && dhclient -v
Killed old client process
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens18/12:67:12:99:53:b4
Sending on   LPF/ens18/12:67:12:99:53:b4
Sending on   Socket/fallback
DHCPDISCOVER on ens18 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 10.31.185.80 from 10.31.185.67
DHCPREQUEST for 10.31.185.80 on ens18 to 255.255.255.255 port 67
DHCPACK of 10.31.185.80 from 10.31.185.67
bound to 10.31.185.80 -- renewal in 36947 seconds.
```

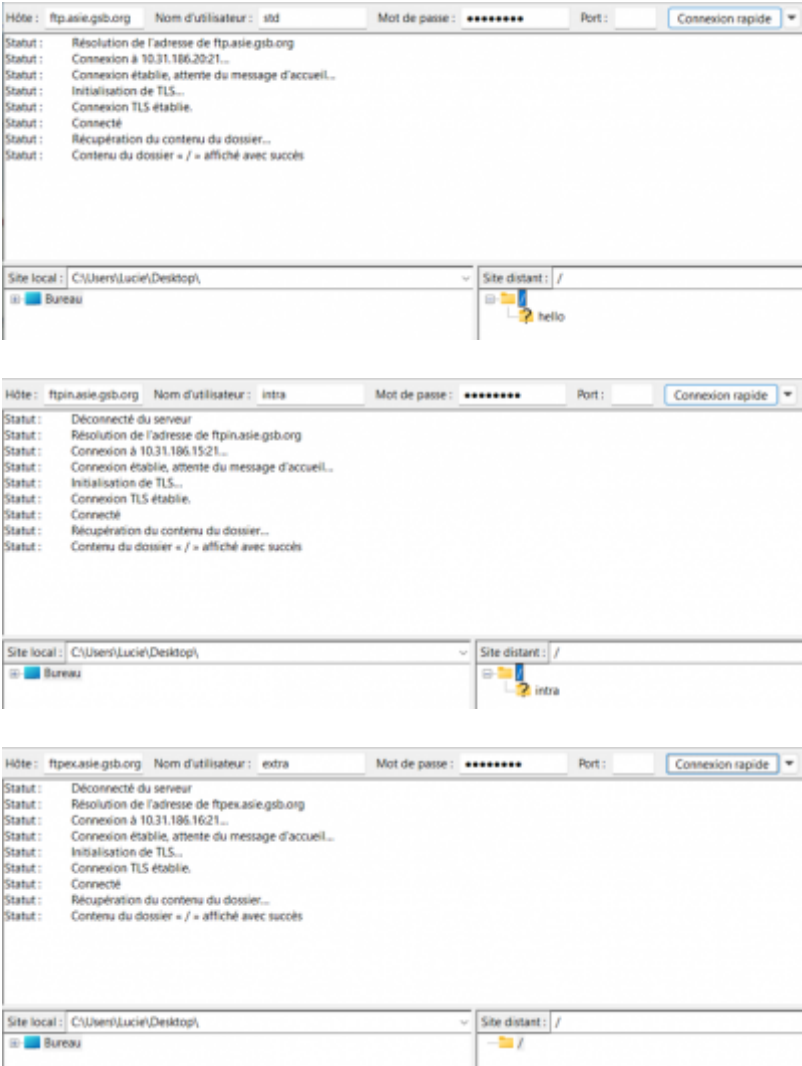
BDD

Le serveur web de la DMZ doit pouvoir contacter la base de données. Pour vérifier la règle, nous pouvons nous rendre dans l'interface d'administration de WordPress via le lien suivant : <https://www.asie.gsb.org/wp-admin>. Les identifiants du site sont std et password (pour les sites du serveur 10.31.186.80) :



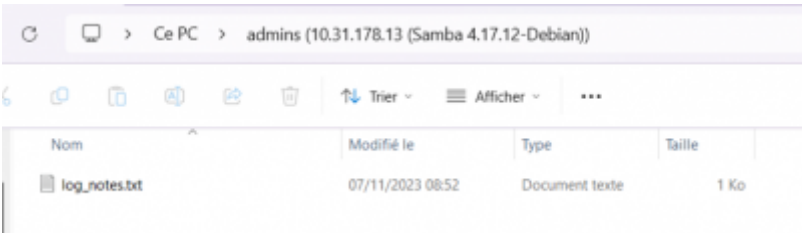
FTPS

Le réseau de Beaupeyrat doit avoir accès au serveur de fichiers FTP :



SAMBA

Le serveur de fichiers Samba doit être accessible depuis le réseau de Beaupeyrat :



From:
<https://sir2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:
<https://sir2.beaupeyrat.com/doku.php?id=sir2-asie:mission12>

Last update: 2024/04/02 18:08

