Léo DI BATTISTA 2024/2025

PR05 : MISE EN PLACE D'UNE DMZ AVEC PFSENSE

ESICAD

SIO 2nde année option SISR

Table des matières

Cahier des charges 3
Configuration de PfSense.....3
Configuration du Serveur Web & FTP 4
Configuration du Serveur MariaDB 9
Configuration des règles de filtrage.....11
Test des règles de filtrage 13

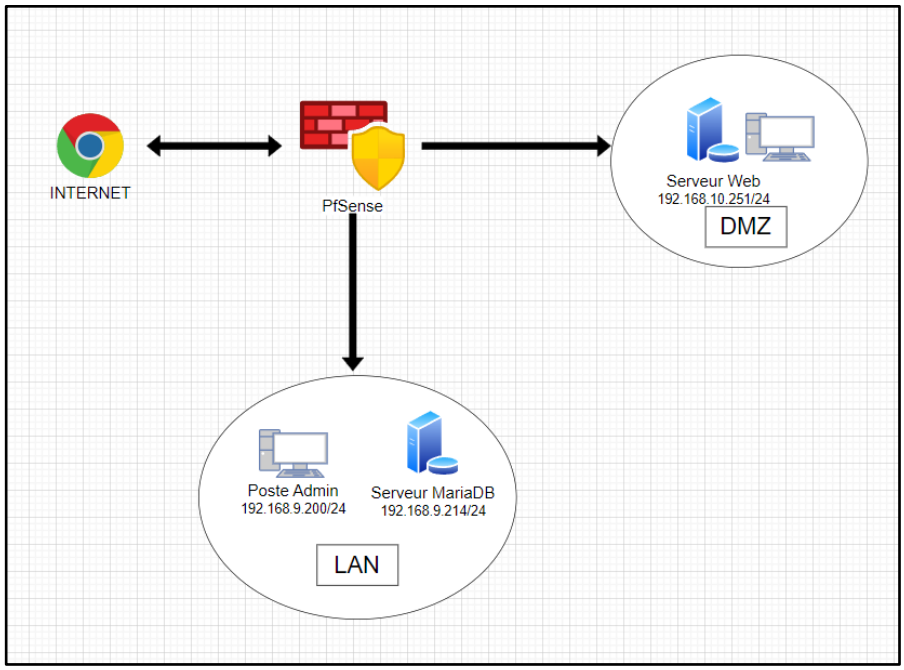
Cahier des charges

Phase 1

- Autoriser les accès au serveur Web depuis Internet et depuis le LAN.
- Autoriser les accès FTP sur le serveur de la DMZ depuis le LAN.
- Autoriser les accès Internet depuis le LAN et la DMZ en passant par le Firewall.
- Interdire tout accès au LAN depuis l'Internet ou la DMZ.

Phase 2 :

- On considère que le site web migré la DMZ est associé à une de BDD dans le LAN.
- Installer un serveur de base de données MariaDB dans le LAN et, autoriser les requêtes SQL du serveur WEB vers le serveur MariaDB.



Configuration Réseau

Configuration du Projet :

1 VM PfSense, 1 VM Serveur Web/FTP, 1 VM Serveur MariaDB, 1 machine client

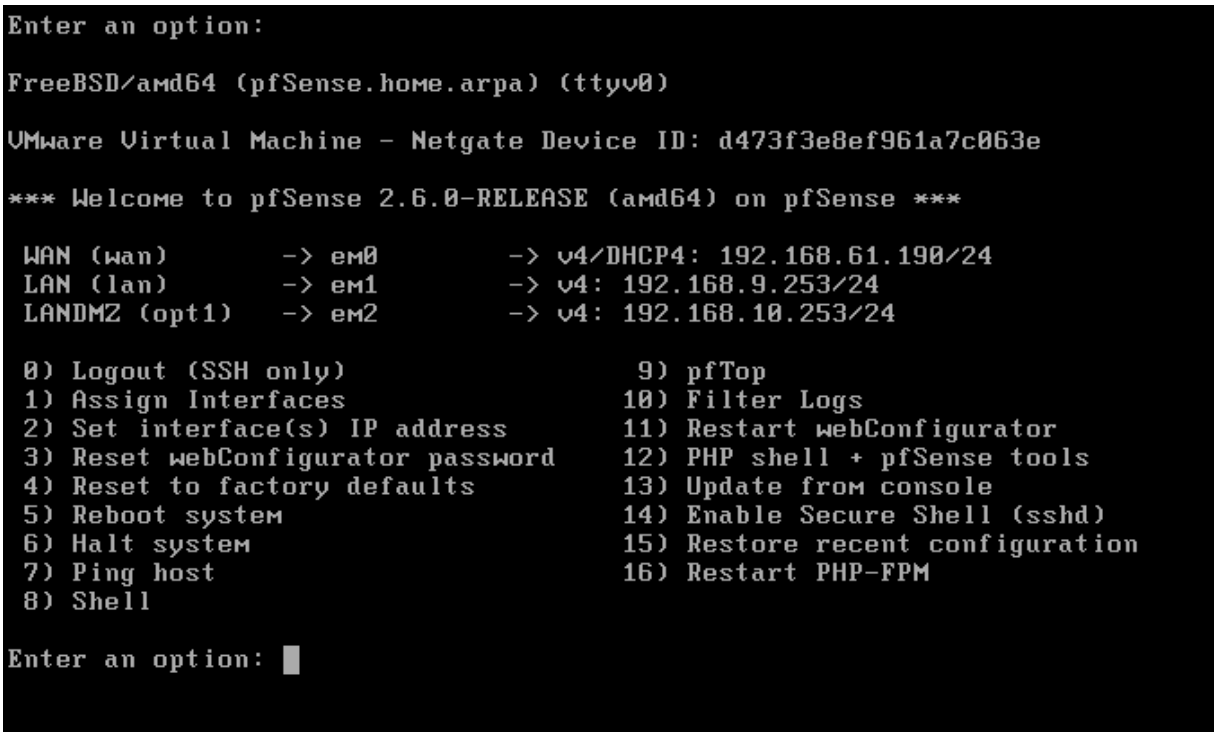
Logiciels/services/applications/OS : Debian11, Apache2, MariaDB, ProFTPD, Bind9,PfSense

Configuration de PfSense

Pfsense qu'est que c'est ?

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

Nous passons la création de la machine virtuelle pour arriver directement sur la configuration de PfSense.



C'est une configuration avec 3 cartes réseaux :

- Une en DHCP (afin d'accéder à internet)
- Une en LAN (ServeurMariaDB & Poste Admin)
- Une DMZ (Serveur Web)

Nous reviendrons sur PfSense pour la configuration des règles de filtrage.

Configuration du Serveur Web & FTP

Pour la bonne configuration d'un Serveur Web il faut Apache2 et Bind9.

```
serveur@debian:~$ sudo apt install apache2
```

```
serveur@debian:~$ sudo apt install bind9
```

Une fois l'installation faite, il faut créer des fichiers index (le contenu de la page web)

```
-rw-r--r-- 1 root root 130 30 sept. 11:54 index.html
root@debian:/var/www/html/digitalschool# cat index.html
<!DOCTYPE html>
<html>
<body>
        <h1>Bienvenue sur le site de Digitalschool</h1>
        <p>Ceci est la page d'accueil</p>
</body>
</html>
```

fichiers index de chaque site

```
root@debian:/var/www/html/mbway# cat index.html
<!DOCTYPE html>
<html>
<body>
        <h1>Bienvenye sur le site de Mbway</h1>
        <p>Ceci est la page d'accueil.</p>
</body>
</html>
```

Puis un fichier de configuration pour chaque site web (ici mbway & digitalschool)

```
root@debian:/etc/apache2/sites-available# cat digitalschool.conf
<VirtualHost *: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.digitalschool.lan

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/digitalschool

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
root@debian:/etc/apache2/sites-available# cat mbway.conf
<VirtualHost *: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.mbway.lan

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/mbway

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Il faut maintenant démarrer les sites à l'aide d'une commande

```
root@debian:~# a2ensite mbway.conf
```

```
root@debian:~# a2ensite digitalschool.conf
```

Les sites sont démarrés, on peut maintenant y accèder en tapant l'adresse IP du serveur suivit du nom du fichier

page d'accueil de nos 2 sites

La première partie est terminée, il faut maintenant mettre en place un DNS et le certificat HTTPS.

Pour le certificat HTTPS, nous utiliserons le certificat dèjà fournit par apache2.
Il suffit de reprendre la configuration des sites mais d'avoir en Virtual Host le port 443.

```
root@debian:/etc/apache2/sites-available# cat mbway-ssl.conf
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html/mbway
                ServerName www.mbway.lan

                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
```

configuration des sites

```
root@debian:/etc/apache2/sites-available# cat digitalschool-ssl.conf
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html/digitalschool
                ServerName www.digitalschool.lan
                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
```

Nos 2 sites ont leurs virutals hosts de configurer, on peut maintenant les réactiver avec la même commande précedemment utilisée.

```
root@debian:~# a2ensite mbway-ssl.conf
```

```
root@debian:~# a2ensite digitalschool-ssl.conf
```

Il faut maintenant créer nos zones et les déclarer.

```
root@debian:/etc/bind# cat db.digitalschool.lan
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian.digitalschool.lan. root.debian.digitalschool.lan. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian.digitalschool.lan.
debian          IN      A       192.168.10.251
www     IN      A       192.168.10.251
```

Fichier de zones des deux sites

```
root@debian:/etc/bind# cat db.mbway.lan
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian.mbway.lan. root.debian.mbway.lan. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian.mbway.lan.
debian          IN      A       192.168.10.251
www     IN      A       192.168.10.251
```

Une fois créer il faut les déclarer

```
root@debian:/etc/bind# cat 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";
zone "mbway.lan" {
        type master;
        file "/etc/bind/db.mbway.lan";
};

zone "digitalschool.lan" {
        type master;
        file "/etc/bind/db.digitalschool.lan";
};
```

Fichier de déclaration de zone : « named.conf.local

Une fois chose faite, il ne faut pas oublier de rajouter en tant que DNS, l'adresse ip du serveur dans le fichier /etc/resolv.conf

```
nameserver 192.168.10.251
```

Une fois toutes ces étapes terminées, on peut accèder à nos sites en utilisant respectivement www.mbway.lan et www.digitalschool.lan.

Le serveur Web ainsi que les sites sont correctements configurés.

Installation de ProFTP :

```
serveur@debian:~$ sudo apt install proftpd
```

Configuration du Serveur MariaDB

MariaDB qu'est que c'est ?

MariaDB est un système de gestion de base de données relationnelle (SGBDR) open source qui constitue une solution de remplacement compatible avec la technologie très répandue des bases de données MySQL.

Il faut déjà commencer par installer MariaDB

```
serveur@debian:~$ sudo apt install mariadb-server -y
```

Nous suivons les étapes d'installation.

```
root@debian:~# sudo apt install mariadb-server mariadb-client -y
```

```
Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
 ... skipping.

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n]
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.
```

Et on fait la secure_installation.

On suit les étapes et nous pouvons maintenant utiliser mariaDB et s'y connecter

```
Thanks for using MariaDB!
```

```
Thanks for using MariaDB!
root@debian:~# sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.5.26-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Il faut maintenant faire en sorte de permettre les connexions distantes.

```
 GNU nano 5.4          /etc/mysql/mariadb.conf.d/50-server.cnf
lc-messages             = en_US
skip-external-locking

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
```

Il faut mettre bind-address = 0.0.0.0 pour autoriser toute les ip de s'y connecter.

Il faut maintenant rajouter un utilisateur permettant la connexion distante.

```
MariaDB [(none)]> SELECT user, host FROM mysql.user;
+-------------+-----------+
| User        | Host      |
+-------------+-----------+
| root        | %         |
| webuser     | %         |
| mariadb.sys | localhost |
| mysql       | localhost |
| root        | localhost |
+-------------+-----------+
5 rows in set (0,001 sec)
```

Nous pouvons maintenant nous connecter.

Configuration des règles de filtrage

Règle NAT :

Firewall / NAT / Port Forward

Port Forward | 1:1 | Outbound | NPt

Rules

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	✓	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.10.251	443 (HTTPS)	redirection WEB	

Règles WAN :

Firewall / Rules / WAN

Floating | WAN | LAN | DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓ 0 /0 B	IPv4 TCP	*	*	DMZ address	443 (HTTPS)	*	none			
☐	✗ 0 /0 B	IPv4 TCP	*	*	LAN net	*	*	none			
☐	✓ 0 /15 KiB	IPv4 TCP	*	*	192.168.10.251	443 (HTTPS)	*	none		NAT redirection WEB	

Règles LAN :

Firewall / Rules / LAN

Floating | WAN | LAN | DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓ 1 /1.63 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	✓ 22 /3.60 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
☐	✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Règles DMZ :

Firewall / Rules / DMZ

Floating | WAN | LAN | DMZ

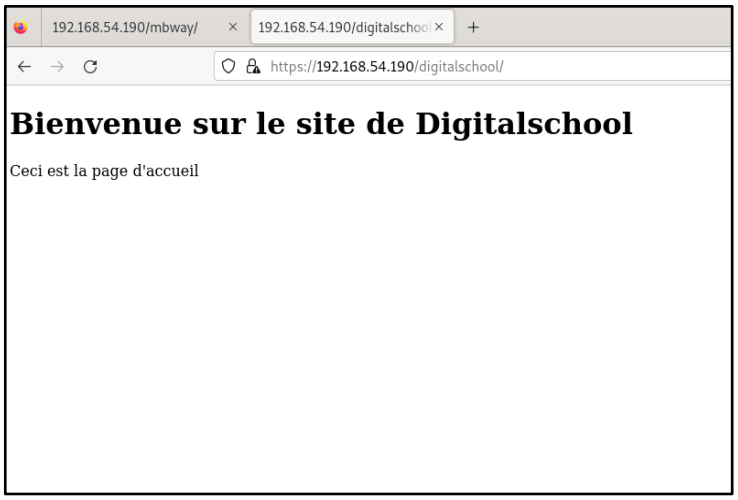
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓ 2 /2 KiB	IPv4 TCP	DMZ net	*	192.168.9.214	3306	*	none			
☐	✓ 0 /769 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none			
☐	✗ 0 /0 B	IPv4 *	DMZ net	*	LAN net	*	*	none			
☐	✓ 0 /3 KiB	IPv4 ICMP any	*	*	*	*	*	none			

Test des règles de filtrage

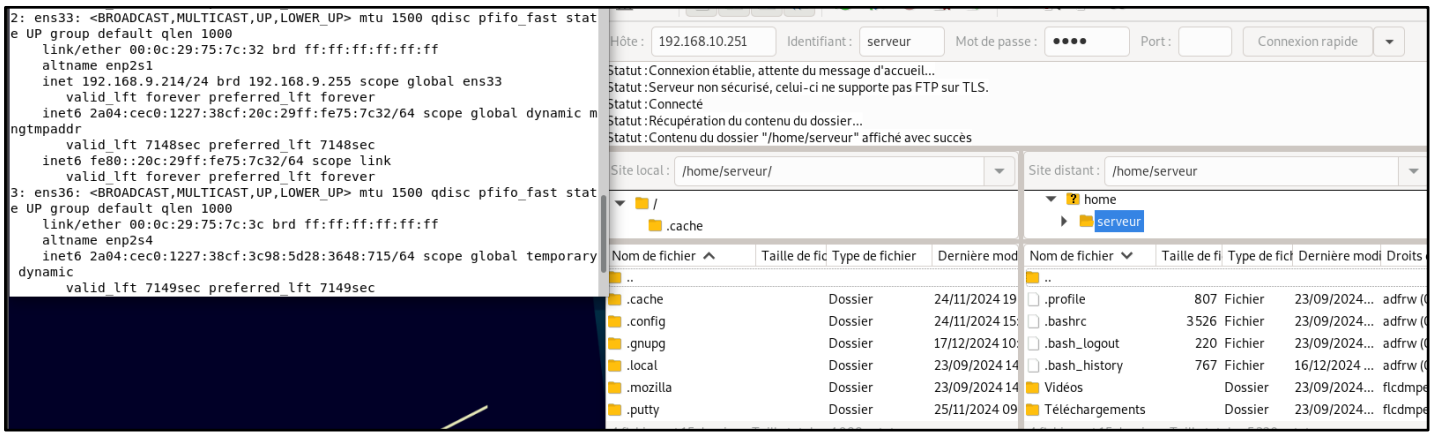
Objectif :

Autoriser les accès au serveur Web depuis Internet et depuis le LAN.



Les connexions sont opérationnelles.

Autoriser les accès FTP sur le serveur de la DMZ depuis le LAN.



Autoriser les accès Internet depuis le LAN et la DMZ en passant par le Firewall.

```
serveur@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=33.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=39.4 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 33.430/36.403/39.376/2.973 ms
serveur@debian:~$ ping google.com
PING google.com(fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e)) 56 data bytes
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=1 ttl=107 time=46.8 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=2 ttl=107 time=40.9 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 40.947/43.885/46.824/2.938 ms
serveur@debian:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f2:62:aa brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.251/24 brd 192.168.10.255 scope global ens33
```

Serveur WEB/FTP

```
serveur@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=30.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=59.8 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 30.700/45.255/59.810/14.555 ms
serveur@debian:~$ ping google.com
PING google.com(fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e)) 56 data bytes
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=1 ttl=106 time=46.8 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=2 ttl=106 time=41.6 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 41.609/44.222/46.835/2.613 ms
serveur@debian:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:75:7c:32 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.9.214/24 brd 192.168.9.255 scope global ens33
```

Serveur MariaDB

Interdire tout accès au LAN depuis l'Internet ou la DMZ.

```
serveur@debian:~$ ping 192.168.9.214
PING 192.168.9.214 (192.168.9.214) 56(84) bytes of data.
^C
--- 192.168.9.214 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2045ms

serveur@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gro
t 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast s
roup default qlen 1000
    link/ether 00:0c:29:f2:62:aa brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.251/24 brd 192.168.10.255 scope global ens33
```

Serveur WEB/FTP

```
root@debian:~# ping 192.168.9.214
PING 192.168.9.214 (192.168.9.214) 56(84) bytes of data.
^C
--- 192.168.9.214 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6070ms

root@debian:~# 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
 1000
    link/ether 00:0c:29:b8:a5:75 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.161/24 brd 192.168.10.255 scope global dynamic ens33
       valid_lft 546sec preferred_lft 546sec
    inet6 2a04:cec0:120b:1d7d:20c:29ff:feb8:a575/64 scope global dynamic mngtmpaddr
       valid_lft 6761sec preferred_lft 6761sec
    inet6 2a04:cec0:1227:38cf:20c:29ff:feb8:a575/64 scope global dynamic mngtmpaddr
       valid_lft 3593sec preferred_lft 3593sec
```

Client WAN

Connexion distante à MySQL

```
root@debian:~# mysql -h 192.168.9.214 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.5.26-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Nous pouvons bien nous connecter même avec les règles de filtrage.

La configuration de cette infrastructure est désormais complète et opérationnelle. Elle peut même évoluer en fonction des demandes de sécurité ou en cas d'une infrastructure plus importante.