PR05 : SIO SISR - Déploiement de services dans une DMZ





Sommaires

Contexte :	3
Objectifs :	3
Cahier des charges :	3
Solution :	3
Schéma ASI :	3
Prérequis :	4
Configuration du serveur WEB et FTP :	4
Configuration du serveur FTP :	4
Installation de Proftpd :	4
Configuration du Serveur Web :	5
Installation d'Apache2 :	5
Configuration des deux intranets :	5
Configuration des Virtual hosts :	6
Mise en place du protocole HTTPS :	8
Configuration pour la DMZ :	13
Configuration du DNS :	14
Installation de BIND9 :	14
Déclaration et création des zones :	14
Configuration du serveur MariaDB :	19
Installation de MariaDB :	19
Sécurisation de l'installation MariaDB :	19
Création des bases de données :	22
Configuration des connexions distantes :	23
Configuration pour le LAN :	25
Configuration réseau des postes pour le LAN et le WAN :	26
Configuration pour le LAN :	26
Configuration pour le WAN :	26
Configuration du pare-feu PFSENSE :	27
Installation de PFSENSE :	27
Configuration des interfaces réseaux :	35
Connection depuis l'interface WEB depuis un poste du LAN :	37
Mise en place des règles de filtrages :	40
Mise en place du NAT :	40
Règles de filtrage pour le LAN :	42
Règles de filtrage pour la DMZ :	43
Règles de filtrage pour le WAN :	44
Test de Connexion :	44
Conclusion :	50

Contexte :

Dans le cadre de la sécurisation des accès aux serveurs de l'entreprise, il a été décidé de créer un réseau dit DMZ pour contenir tous les services accessibles depuis l'extérieur. La 1^{ère} partie de ce déploiement ne portera que sur le serveur WEB qui sera déplacé du LAN vers cette DMZ

Objectifs :

- Déployer une DMZ intégrant un serveur web.
- Mettre en place un serveur de bases de données MariaDB
- Configurer des règles de filtrages via PFSENSE

Cahier des charges :

NB : pour tester les connexions depuis l'extérieur, on utilisera un poste configuré dans le même réseau que l'interface WAN de votre Firewall.

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

Solution :

Pour répondre à la demande, je vais mettre en place plusieurs VM sous Debian afin d'héberger mon serveur web, mon serveur DNS et mon serveur de base de données. Je vais également mettre en place différentes VM sous Debian afin de tester les connexions depuis la DMZ et le LAN, qui seront sécurisées par un pare-feu.

Schéma ASI :



Prérequis :

Tout d'abord nous allons devoir installer puis paramétrer une machine virtuelle sous Debian qui nous servira de Serveur WEB (Apache2), de serveur DNS (BIND9) et de serveur FTP (Proftpd).

Puis une autre machine virtuelle pour le serveur MariaDB qui sera dans le LAN.

Ensuite on va configurer deux VM sous Debian : une pour le réseau LAN et une autre pour le réseau WAN.

Et enfin nous allons installer et configurer PFSENSE.

Configuration du serveur WEB et FTP :

Configuration du serveur FTP :

Nous devons installer au préalable ProFTPD sur notre VM SERVEUR Debian11

Installation de Proftpd :

- sudo apt-get update
- sudo apt install proftpd

Une fois installé nous pouvons choisir de créer des utilisateurs mais nous allons nous connecter en mode utilisateur pour nos tests.

FTP n'est pas un protocole sécurisé. Pour éviter la transmission d'informations en clair, il est nécessaire de crypter les données en transit. Nous utiliserons donc principalement le protocole SFTP.

Pour cela, nous devrons installer OpenSSH sur les serveurs ainsi que sur les postes clients via la commande :

- sudo apt install openssh-server

```
utilisateur@debianClient:~$ sudo apt-cache policy openssh-server
openssh-server:
    Installé : 1:8.4p1-5+deb11u3
    Candidat : 1:8.4p1-5+deb11u3
    Table de version :
    *** 1:8.4p1-5+deb11u3 500
        500 http://deb.debian.org/debian bullseye/main amd64 Packages
        500 http://security.debian.org/debian-security bullseye-security/main am
d64 Packages
        100 /var/lib/dpkg/status
```

Configuration du Serveur Web :

On va devoir configurer Apache 2 avec nos 2 intranets et mettre en place le protocole HTTPS

Dans un premier temps faire sudo apt-get update afin d'avoir les dernières versions disponibles (il faut le faire avant toutes installations sous Debian)

Installation d'Apache2 :

- sudo apt install Apache2

```
utilisateur@debianServeur:~$ sudo apache2 -v
Server version: Apache/2.4.56 (Debian)
Server built: 2023-04-02T03:06:01
```

On constate donc qu'Apache2 est correctement installé.

Configuration des deux intranets :

On va créer deux dossiers MBWay et DigitalSchool :

Aller dans le dossier cd /var/www/html est créé deux dossiers avec la commande mkdir :

```
utilisateur@debianServeur:~$ cd /var/www/html/
utilisateur@debianServeur:/var/www/html$ ls -l
total 20
drwxr-xr-x 2 root root 4096 15 avril 12:46 digitalschool
-rw-r--r-- 1 root root 10701 7 avril 21:19 index.html
drwxr-xr-x 2 root root 4096 13 avril 18:18 mbway
utilisateur@debianServeur:/var/www/html$
```

Pour chaque dossier nous allons créer un fichier index.html que nous allons ensuite configurer :

```
utilisateur@debianServeur:/var/www/html$ cd mbway
utilisateur@debianServeur:/var/www/html/mbway$ ls -l
total 4
-rw-r--r- 1 root root 123 13 avril 18:18 index.html
utilisateur@debianServeur:/var/www/html/mbway$ cd ..
utilisateur@debianServeur:/var/www/html$ cd digitalschool
utilisateur@debianServeur:/var/www/html$ cd digitalschool
utilisateur@debianServeur:/var/www/html/digitalschool$ ls -l
total 8
-rw-r--r- 1 root root 131 14 avril 11:13 index.html
```

Fichier index.html pour DigitalSchool :

On va créer le même type pour MBWay.

Nous avons donc créé un dossier où nous importerons nos fichiers html, PHP, JavaScript etc... respectifs à chaque site. Ici nous n'avons déposé qu'un « index.html » pour le moment.

Configuration des Virtual hosts :

Grâce à l'étape précédente nous avons créé nos intranets.

De ce fait pour y accéder nous sommes obligés d'écrire : http://AdresseIP/mbway/ pour accéder au site d'MBWay par exemple.

Pour corriger cela nous allons donc configurer des Virtual Host pour accéder à nos sites depuis l'adresse http://www.mbway.lan

On va aller dans le dossier /etc/apache2/sites-available/

On a un fichier 000-default.conf avec une configuration par default que l'on va copier (commande cd) et créé deux fichiers un pour MBWay et un autre pour DigitalSchool.

```
utilisateur@debianServeur:~$ cd /etc/apache2/sites-available/
utilisateur@debianServeur:/etc/apache2/sites-available$ ls -l
total 36
-rw-r--r-- 1 root root 1332 2 avril 2023 000-default.conf
-rw-r--r-- 1 root root 6387 14 avril 19:53 default-ssl.conf
-rw-r--r-- 1 root root 1351 13 avril 15:31 digitalschool.conf
-rw-r--r-- 1 root root 6390 16 avril 09:20 digitalschool-ssl.conf
-rw-r--r-- 1 root root 1636 14 avril 19:38 mbway.conf
-rw-r--r-- 1 root root 6374 16 avril 09:19 mbway-ssl.conf
utilisateur@debianServeur:/etc/apache2/sites-available$
```

On va ensuite les configurer :

```
utilisateur@debianServeur:/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.
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/mbway
```

utilisateur@debianServeur:/etc/apache2/sites-available\$ cat digitalschool.conf
<VirtualHost *:80>
 # The ServerName directive sets the request scheme, hostname and port
 # 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) th:
 # 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

On modifie ServerName par le nom de nos serveurs : <u>www.mbway.lan</u> et <u>www.digitalschool.lan</u>.

On lui indique la route avec DocumentRoot : /var/www/html/mbway et /var/www/html/digitalschool .

On va activer nos sites avec la commande a2ensite + le nom du virtual Host

Maintenant si on ajoute www.mbway.lan en alias à notre serveur dans le fichier /etc/hosts de notre client, vous pouvez voir la page d'accueil de notre site dans notre navigateur.

On vérifie que nos sites fonctionnent :

Bienvenue sur le site de MBWAY

Ceci est la page d'acceuil.

Mise en place du protocole HTTPS :

La connexion à nos sites intranets ne se font de base qu'en HTTP ce qui n'est absolument pas sécurisé. Pour éviter de subir une attaque informatique de type « Man in the middle » nous devons crypter les données qui transitent par le biais du protocole HTTPS.

On a un fichier avec une configuration déjà présente sous Debian :

```
utilisateur@debianServeur:/etc/apache2/sites-available$ ls -l
total 36
-rw-r--r-- 1 root root 1332 2 avril 2023 000-default.conf
-rw-r--r-- 1 root root 6387 14 avril 19:53 default-ssl.conf
-rw-r--r-- 1 root root 1351 13 avril 15:31 digitalschool.conf
-rw-r--r-- 1 root root 6390 16 avril 09:20 digitalschool-ssl.conf
-rw-r--r-- 1 root root 1636 14 avril 19:38 mbway.conf
-rw-r--r-- 1 root root 6374 16 avril 09:19 mbway-ssl.conf
utilisateur@debianServeur:/etc/apache2/sites-available$
```

On va donc copier le fichier default-ssl et créer deux fichiers pour chaque site puis les configurer :

Activités	🔄 Terminal 🔻	16 avril 10:09
Ð		utilisateur@debianServeur: /etc/apache2/sites-availab
<ifmodule< td=""><td>e mod_ssl.c> VirtualHost _defa ServerAdmi</td><td>/etc/apachez/sites-avaitables cat digitatschool-sst.com ult_:443> .n webmaster@localhost e www.digitalschool.lan</td></ifmodule<>	e mod_ssl.c> VirtualHost _defa ServerAdmi	/etc/apachez/sites-avaitables cat digitatschool-sst.com ult_:443> .n webmaster@localhost e www.digitalschool.lan
	DocumentRo	ot /var/www/html/digitalschool
	<pre># Availabl # error, c # It is al # modules, #LogLevel</pre>	e loglevels: trace8,, trace1, debug, info, notice, warn, rit, alert, emerg. so possible to configure the loglevel for particular e.g. info ssl:warn
	ErrorLog \$ CustomLog	{APACHE_LOG_DIR}/error.log \${APACHE_LOG_DIR}/access.log combined
	<pre># For most # enabled # include # followin # after it #Include c</pre>	configuration files from conf-available/, which are or disabled at a global level, it is possible to a line for only one particular virtual host. For example the g line enables the CGI configuration for this host only has been globally disabled with "a2disconf". conf-available/serve-cgi-bin.conf
	# SSL En # Enable SSLEngine	gine Switch: /Disable SSL for this virtual host. on
	<pre># A self # the ss # /usr/s # If bot # SSLCer SSLCertifi SSLCertifi</pre>	-signed (snakeoil) certificate can be created by installing l-cert package. See hare/doc/apache2/README.Debian.gz for more info. h key and certificate are stored in the same file, only the tificateFile directive is needed. .cateFile /etc/ssl/certs/ssl-cert-snakeoil.pem .cateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

Activités	🔈 Terminal 🔻	16 avril 10:10
Ð		utilisateur@debianServeur: /etc/apache2/sites-availab
utilisate <ifmodule <</ifmodule 	e mod_ssl.c> WirtualHost _defau ServerAdmir DocumentRoc ServerName	etc/apache2/sites-available\$ cat mbway-ssl.conf lt_:443> webmaster@localhost t /var/www/html/mbway www.mbway.lan
	<pre># Available # error, cr # It is als # modules, #LogLevel i</pre>	loglevels: trace8,, trace1, debug, info, notice, warn, it, alert, emerg. o possible to configure the loglevel for particular e.g. nfo ssl:warn
	ErrorLog \${ CustomLog \$	APACHE_LOG_DIR}/error.log {APACHE_LOG_DIR}/access.log combined
	<pre># For most # enabled o # include a # following # after it #Include co</pre>	configuration files from conf-available/, which are r disabled at a global level, it is possible to line for only one particular virtual host. For example the line enables the CGI configuration for this host only has been globally disabled with "a2disconf". hf-available/serve-cgi-bin.conf
	# SSL Eng # Enable/ SSLEngine c	ine Switch: Disable SSL for this virtual host. n
	<pre># A self- # the ssl # /usr/sh # If both # SSLCert SSLCertific SSLCertific</pre>	signed (snakeoil) certificate can be created by installing -cert package. See are/doc/apache2/README.Debian.gz for more info. key and certificate are stored in the same file, only the ificateFile directive is needed. ateFile /etc/ssl/certs/ssl-cert-snakeoil.pem ateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

On donne le nom de notre serveur :

ServerName <u>www.mbway.lan</u> et ServerName <u>www.digitalschool.lan</u> ainsi que la route avec DocumentRoot /var/www/html/mbway et /var/www/html/digitalschool .

On va activer a2enmod ssl puis a2ensite default-ssl

On va activer nos sites avec la commande a2ensite + le nom du virtual Host

Puis redemarrer apache2 : service apache2 reload

La recommandation est de créer/acheter un certificat pour chaque site plutôt que d'utiliser la configuration de base d'Apache2.

C'est donc ce que nous allons faire :

Dans un premier temps nous allons verifier que le module SSL est bien activée :

- sudo a2enmod ssl

Nous allons ensuite générer nos clés privées et des CSR(certificate signing request) :

Pour Mbway : openssl req -newkey rsa:2048 -nodes -keyout /etc/ssl/private/mbway.key -out /etc/ssl/certs/mbway.csr

Et pour Digitalschool : openssl req -newkey rsa:2048 -nodes -keyout /etc/ssl/private/digitalschool.key -out /etc/ssl/certs/ digitalschool.csr

Nous devrons répondre à une suite de question :

mult up passe :
root@debianl1:/home/utilisateur# openssl req -newkey rsa:2048 -nodes -keyout /etc/ssl/private/mbway.key -out /etc/ssl/certs/mbway.csr
Generating a RSA private key
.....+++++
writing new private key to '/etc/ssl/private/mbway.key'
.....
You are about to be asked to enter information that will be incorporated
into your certificate request.
You are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:fr
State or Province Name (full name) [Some-State]:paris
Locality Name (eg, city) []:paris
Organization Name (eg, section) []:it
Common Name (e.g. server FQDN or YOUR name) []:thomas
Email Address []:thomas.fr
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:root
An optional company name []:
root@debianl1:/home/utilisateur#

Nous allons enfin passer a la création de nos certificats auto-signés :

Pour Mbway : sudo openssl req x509 -req -days 365 -in /etc/ssl/certs/mbway.csr -signkey /etc/ssl/private/mbway.key -out /etc/ssl/certs/mbway.crt

Et pour digitalschool : sudo openssl req x509 -req -days 365 -in /etc/ssl/certs/digitalschool.csr -signkey /etc/ssl/private/digitalschool.key -out /etc/ssl/certs/digitalschool.crt

Nous devons ensuite modifier les lignes :

- SSLCertificateFile

- SSLCertificateKeyFile

Pour les sites Mbway et Digitaschool dans mbway-ssl.conf et digitalschool-ssl.conf

```
Ð
                                                                                                                 utilisateur@debian11:~
 GNU nano 5.4
                                                                                                                     mbwav-ssl.conf *
 <IfModule mod ssl.c>
           <VirtualHost default :443>
                      ServerAdmin webmaster@localhost
                      ServerName www.mbway.lan
                      DocumentRoot /var/www/html/mbwav
                      # 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
                      # 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
                            SSL Engine Switch:
                            Enable/Disable SSL for this virtual host.
                      SSLEngine on
                            A self-signed (snakeoil) certificate can be created by installing
                            the ssl-cert package. See
/usr/share/doc/apache2/README.Debian.gz for more info.
                      #
                            If both key and certificate are stored in the same file, only the SSLCertificateFile directive is needed.
                      SSLCertificateFile
                                                        /etc/ssl/certs/mbway.crt
                      SSLCertificateKeyFile /etc/ssl/private/mbway_key
                            Server Certificate Chain:
 Ð
                                                                                                            utilisateur@debian11:~
                                                                                                           digitalschool-ssl.conf
GNU nano 5.4
<IfModule mod ssl.c>
          <VirtualHost _default_:443>
                     ServerAdmin webmaster@localhost
                     ServerName www.digitalschool.lan
                     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
                     # robled 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
                          SSL Engine Switch:
Enable/Disable SSL for this virtual host.
                     #
                     SSLEngine on
                          A self-signed (snakeoil) certificate can be created by installing
                          the ssl-cert package. See
/usr/share/doc/apache2/README.Debian.gz for more info
                          If both key and certificate are stored in the same file, only the SSLCertificateFile directive is needed.
                     SSLCertificateFile
                                                    /etc/ssl/certs/digitalschool.crt
                     SSLCertificateKeyFile /etc/ssl/private/digitalschool.key
```

On va activer nos sites avec la commande a2ensite + le nom de notre site

Puis redemarrer apache2 : sudo systemctl restart apache2

Maintenant si on ajoute www.mbway.lan en alias à notre serveur dans le fichier /etc/hosts de notre client, vous pouvez voir la page d'accueil de notre site dans notre navigateur :



Bienvenue sur le site de Mbway !

Nous arrivons donc bien a nous connecter en https !

Configuration pour la DMZ :

On va d'abord aller dans le fichier /etc/network/interfaces afin de paramétrer notre carte réseaux avec la commande sudo nano /etc/network/interfaces.

On redémarrera les interfaces avec la commande sudo systemctl restart networking.service pour que les changements prennent effet.

Il ne faut pas oublier d'activer l'accès par pont.

Pour notre serveur on lui définit comme adresse IP : 192.168.30.10

E	utilisateur@debianServeur: ~ Q = ×
(# 1 # 3	GNU nano 5.4 /etc/network/interfaces This file describes the network interfaces available on your system and how to activate them. For more information, see interfaces(5).
sou	<pre>urce /etc/network/interfaces.d/*</pre>
# 1 au1 ifa	The loopback network interface to lo ace lo inet loopback
au† ifa	to ens33 ace ens33 inet static address 192.168.30.10 netmask 255.255.255.0 gateway 192.168.30.254
^с ^х	<mark>[Lecture de 14 lignes]</mark> Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement Quitter ^R Lire fich.^∖ Remplacer ^U Coller ^J Justifier ^ Aller ligne

Maintenant que l'interface réseau est prête on pourra finir de configurer notre DMZ via PFsense.

Configuration du DNS :

On commence par faire apt-get upgrade

Installation de BIND9 :

On fait ensuite sudo apt install Bind9 puis sudo apt install bind9utils.

Déclaration et création des zones :

On va commencer pas déclarer les zones dans /etc/bind

Ð	utilisateur@debianServeur:/etc/bind Q = ×							×	
utilisateu	r@debia	nServe	eur:~s	\$ C(d /etc,	/bind			
utilisateu	r@debia	nServe	eur:/e	etc,	/bind\$	ls -l			
total 56									
- rw-rr	1 root	root	1991	29	juil.	12:05	bind.keys		
-rw-rr	1 root	root	237	29	juil.	12:05	db.0		
- rw- r r	1 root	root	271	29	juil.	12:05	db.127		
-rw-rr	1 root	root	237	29	juil.	12:05	db.255		
-rw-rr	1 root	bind	362	14	oct.	15:42	db.digitalschool.lan		
- rw-rr	1 root	root	353	29	juil.	12:05	db.empty		
-rw-rr	1 root	root	270	29	juil.	12:05	db.local		
-rw-rr	1 root	bind	337	14	oct.	15:42	db.mbway.lan		
-rw-rr	1 root	bind	463	29	juil.	12:05	named.conf		
-rw-rr	1 root	bind	498	29	juil.	12:05	named.conf.default-zones		
-rw-rr	1 root	bind	318	30	sept.	14:55	named.conf.local		
-rw-rr	1 root	bind	848	7	oct.	16:53	named.conf.options		
- rw- r	1 bind	bind	100	30	sept.	14:15	rndc.key		
- rw- r r	1 root	root	1317	29	juil.	<u>1</u> 2:05	zones.rfc1918		
utilisateu	r@debia	nServe	eur:/e	etc,	/bind\$				

On va aller dans le fichiers named.conf.local et le configurer :

```
utilisateur@debianServeur:/etc/bind$ cat named.conf.local
11
// 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";
};
utilisateur@debianServeur:/etc/bind$
```

On le configure en mode master et ont créé deux zones pour chacun de nos sites et on respecte la convention db.nomDomaine pour le déclarer.

On va ensuite créer nos fichiers de zones :

Thomas Fougeras

GNU na	ano 5.4			db.mb	way.lan					
; BIND c ;	lata file	e for loo	al loopb	ack inter	face					
\$TTL	604800									
0	IN	SOA	debianSe 2 604800 86400 2419200 604800	rver.mbwa ; ; ;) ;	y.lan. roo Serial Refresh Retry Expire Negative	ot.debi Cache	ianServe TTL	r.mb	way.lan.	(
;		NC	de bé e a C e		. 1					
(debience	IN	NS	deblanse	rver.mbwa	/.lan.					
WWW	IN	A	A 192.168.	30.10	9.10					
C Aido	<u>^</u> 0	Écrire	[Le	cture de	14 lignes] ^T E	vécuter	<u>^c</u>	Emplacem	ont

^X	Quitt	er ^	R Lire	fich.^\ F	.nercher Remplacer	^U	Coller	^j .	Executer Justifier	^_	Aller	ligne
(GNU na	ano 5.4			db.digi	ital	.school.la	n				
; ; E ; \$T1	BIND c	lata fi 604800	le for	local loc	opback int	terf	ace					
0		IN	SOA	debiar 60480 8640 241920 60480	Server.di 2 00 00 00 00 00)	igit ; ; ; ;	alschool. Serial Refresh Retry Expire Negative	lan. Cache	root.deb: e TTL	ian	Server	.digit>
0		IN	NS	debiar	Server.di	igit	alschool.	lan.				
deb	bianSe	erver	IN	A	192.168	3.30	0.10					
ww	v	IN	A	192.16	8.30.10							



On lui donne les bons noms et adresse IP : debianRouteur.mbway.lan. et debianRouteur.digitalschool.lan.

On ajoute WWW pour avoir le <u>www.mbway.lan</u> et on voit également que l'on a un enregistrement de type A.

On va également configurer le fichier named.conf.options avec le DNS de Google.

Les forwarders sont d'autres serveurs DNS vers lesquels le serveur DNS local peut envoyer les requêtes qu'il ne peut pas résoudre.

On doit aussi configurer Bind9 pour accepter toutes les requêtes provenant d'adresses privées définies par les standards RFC1918 (qui inclut les réseaux LAN).

Voici les plages d'adresses locales selon RFC1918 :

- 10.0.0/8 : Pour les réseaux de classe A.
- 172.16.0.0/12 : Pour les réseaux de classe B.
- 192.168.0.0/16 : Pour les réseaux de classe C.

Dans notre fichier named.conf.options, remplacez la directive allow-recursion par une liste incluant ces plages avec :

- allow-query: qui contrôle qui peut poser n'importe quelle question DNS (locale ou externe).
- allow-recursion : qui contrôle qui peut poser des questions récursives (requêtes nécessitant que le serveur DNS interroge d'autres serveurs).

Ð	utilisateur@debian11:~ Q = ×
GNU	nano 5.4 named.conf.options
	<pre>// 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</pre>
	<pre>// 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.</pre>
	allow-recursion { localhost; 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16; }; allow-query { l ocalhost; 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16; };
	forwarders {
	//====================================
^G Aid ^X Qui	28 lignes écrites] e ^0 Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement tter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^ Aller ligne

On redémarre Bind9 afin que les modifications prennent effet : sudo systemctl restart bind9

Dans nos machines Debian on va devoir leur indiquer le nouveau DNS dans le fichier

Nano /etc/resolv.conf:

Nameserver: 192.168.30.10

On peut vérifier notre configuration grâce à la commande nslookup :

utilisateur@debianClient2:~\$ nslookup www.mbway.lan
Server: 192.168.30.10
Address: 192.168.30.10#53

Name: www.mbway.lan Address: 192.168.30.10

On peut donc maintenant taper https://www.mbway.lan/

On teste la connexion :

Activ	vités 🛛 🕑 Fir	efox ESR 🔻		18 oc	t. 21	:19		
•	mbway.lan/		× digitalschool.lan/ × +					
\leftarrow	\rightarrow G	O 🔓 http	os://v	vww. mbway.lan				
Bi Ceci	ienven i est la page o	ue su d'acceuil.	ır	le site	de	e MI	BWA	Y
Activ	rités 🛛 🕑 Firefo	x ESR ▼		18 oct. 21:20				?
•	mbway.lan/	×	digit	alschool.lan/	×	+		\sim
\leftarrow	\rightarrow C (🕽 🔒 https://w	/ww. c	ligitalschool.lan			☆	${igsidential}$
Bi Ceci	envenu est la page d'a	le sur acceuil.	le	site de	Di	gital	scho	ol

Configuration du serveur MariaDB :

On va devoir installer et configurer MariaDB puis mettre en place notre base de données.

Dans un premier temps faire sudo apt-get update afin d'avoir les dernières versions disponibles.

Installation de MariaDB :

Utiliser la commande sudo apt-get install mariadb-server mariadb-client

Puis vérifier qu'il se soit bien installé : sudo systemctl status mariadb

```
utilisateur@ServeurMariaDB:~$ sudo systemctl status mariadb
 mariadb.service - MariaDB 10.5.26 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor prese
     Active: active (running) since Sat 2024-11-09 16:41:47 CET; 3min 14s ago
       Docs: man:mariadbd(8)
               https://mariadb.com/kb/en/library/systemd/
    Process: 2843 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var
    Process: 2844 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_ST>
Process: 2846 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && >
Process: 2908 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_S>
    Process: 2910 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/>
   Main PID: 2893 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 9 (limit: 14945)
     Memory: 68.7M
         CPU: 299ms
     CGroup: /system.slice/mariadb.service
               └─2893 /usr/sbin/mariadbd
```

Sécurisation de l'installation MariaDB :

Nous allons utiliser un script afin de sécuriser un minimum notre installation via la commande : sudo mariadb-secure-installation :

utilisateur@ServeurMariaDB:~\$ sudo mariadb-secure-installation NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY! In order to log into MariaDB to secure it, we'll need the current password for the root user. If you've just installed MariaDB, and haven't set the root password yet, you should just press enter here. Enter current password for root (enter for none): OK, successfully used password, moving on... Setting the root password or using the unix socket ensures that nobody can log into the MariaDB root user without the proper authorisation. You already have your root account protected, so you can safely answer 'n'. 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] y New password: Re-enter new password: Sorry, passwords do not match. New password: Re-enter new password: Password updated successfully! Reloading privilege tables.. ... Success! 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] y
... Success!
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] y
- 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] y
... Success!
Cleaning up...
All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.
Thanks for using MariaDB!
utilisateur@ServeurMariaDB:~$
```

Nous avons répondu N à la question Switch to unix_socket authentication. Cela authorisera les connexions sur la base de données MariaDB avec un nom d'utilisateur et un mot de passe.

Puis répondre Y à la question suivante Change the root password ? pour spécifier le mot de passe de l'utilisateur root de MariaDB.

Cet utilisateur root de la base de données aura tous les droits d'accès.

A la question Remove anonymous users ? Répondre Y pour désactiver les connexions anonymes

Pour désactiver les connexions root depuis un serveur autre que le nôtre répondre Y a la question : Disallow root login remotely ?

Répondre Y a : Remove test database and access to it pour supprimer la base de données de test et l'accès.

Et enfin répondre Y a Reload privilege tables now pour recharger les tables de privilèges.

utilisateur@ServeurMariaDB:~\$ sudo mariadb -u root -p Enter password: Welcome to the MariaDB monitor. Commands end with ; or \g. Your MariaDB connection id is 40 Server version: 10.5.26-MariaDB-0+debllu2 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)]>

Maintenant que notre Serveur est installé nous allons pouvoir créer nos bases de données

Création des bases de données :

Connexion a MariaDB :

- Sudo mariadb -u root -p

```
utilisateur@ServeurMariaDB:~$ sudo mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 40
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.
```

Puis création des bases de données pour Mbway et Digitalschool :

- Create database mbway;
- Create database digitalschool;

	MariaDB [(none)]> show databases;
	Database
MariaDB [(none)]> create database mbway; Query OK, 1 row affected (0,001 sec)	digitalschool information_schema mbway mysql performance_schema
MariaDB [(none)]> create database digitalschool; Query OK, 1 row affected (0,000 sec)	++ 5 rows in set (0,000 sec)
MariaDB [(none)]>	MariaDB [(none)]>

Nous allons maintenant configurer notre serveur MariaDB pour autoriser les requêtes SQL provenant du serveur web.

Configuration des connexions distantes :

Tout d'abord, nous devons configurer le serveur de façon qu'il écoute sur une autre adresse IP que "127.0.0.1". On doit modifier le fichier :

- sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf

Puis modifier la ligne :

- bind-address = 192.168.10.20 pour la base de données
- bind-address = 192.168.10.10 pour le poste administrateur
- bind-address = 192.168.30.10 pour le serveur Web

On doit lui indiquer l'adresse IP du poste depuis lequel on pourra interroger MariaDB :

•	utilisateur@debian11: ~	Q ≡	×
GNU nano 5.4	50-server.cnf *		
tmpdir	= /tmp		
lc-messages-dir	= /usr/share/mysql		
lc-messages	= en_US		
skip-external-locking			
# Broken reverse DNS sl # safe to skip if there #skip-name-resolve	ows down connections considerably and name r are no "host by domain name" access grants	esolve is	
<pre># Instead of skip-netwo</pre>	rking the default is now to listen only on		
<pre># localhost which is mo</pre>	re compatible and is not less secure.		- 1
bind-address	= 192.168.10.10		
bind-address	= 192.168.10.20		
bind-address	= 192.168.30.10		
#			- 1
# * Fine Tuning			
#			- 1
#key_buffer_size	= 128M		
^G Aide ^O Écrire ^X Quitter ^R Lire fi	^₩ Chercher <mark>^K</mark> Couper [^] T Exécuter [^] C ch. [^] \ Remplacer [^] U Coller [^] J Justifier [^]	Emplacemer Aller lig	nt ne

Thomas Fougeras

Nous allons devoir maintenant configurer un utilisateur et lui accorder les droits nécessaires à la gestion des bases de données du campus.

Nous allons utiliser la commande :

- GRANT ALL PRIVILEGES ON mbway.* TO 'administrateur'@'192.168.10.10' IDENTIFIED BY 'root' WITH GRANT OPTION;
- su
- GRANT ALL PRIVILEGES ON mbway.* : Donne tous les privilèges (lecture, écriture, modification, suppression, etc.) sur toutes les tables de la base mbway.
- TO 'administrateur'@'192.168.10.10' : Spécifie l'utilisateur administrateur qui se connecte depuis l'adresse IP 192.168.10.10.
- IDENTIFIED BY 'root' : Définit le mot de passe de l'utilisateur administrateur comme root. Lors de la mise en production, nous utiliserons un mot de passe robuste.
- WITH GRANT OPTION : Permet à l'utilisateur administrateur de déléguer (accorder) ces privilèges à d'autres utilisateurs.

Puis, on met à jour les privilèges avant de quitter :

- FLUSH PRIVILEGES;
- EXIT;

```
MariaDB [(none)]> show databases;
+----+
| Database
- - - +
| digitalschool
| information schema |
| mbway
| mysql
| performance_schema |
+----+
5 rows in set (0,003 sec)
MariaDB [(none)]> GRANT ALL PRIVILEGES ON mbway.* TO 'administrateur'@'192.168.1
0.10' IDENTIFIED BY 'root' WITH GRANT OPTION:
Query OK, 0 rows affected (0,001 sec)
MariaDB [(none)]> GRANT ALL PRIVILEGES ON digitalschool.* TO 'administrateur'@'1
92.168.10.10' IDENTIFIED BY 'root' WITH GRANT OPTION;
Query OK, 0 rows affected (0,001 sec)
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,001 sec)
MariaDB [(none)]>
```

Configuration pour le LAN :

On va d'abord aller dans le fichier /etc/network/interfaces afin de paramétrer notre carte réseaux avec la commande sudo nano /etc/network/interfaces.

```
utilisateur@ServeurMariaDB: ~
 Ð
                                                                      Q
                                                                           ≡
                                                                                ×
 GNU nano 5.4
                               /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
auto ens33
iface ens33 inet static
        address 192.168.10.20
        netmask 255.255.255.0
        gateway 192.168.10.254
   Aide
                Écrire
                             Chercher
                                         K Couper
                                                        Exécuter
                                                                    C Emplacement
                                        ^U Coller
                             Remplacer
                                                        Justifier
                                                                      Aller ligne
   Quitter
                Lire fich.
```

On redémarrera les interfaces avec la commande sudo systemctl restart networking.service pour que les changements prennent effet.

Il ne faut pas oublier d'activer l'accès par pont.

Pour notre serveur on lui définit comme adresse IP : 192.168.10.20

Configuration réseau des postes pour le LAN et le WAN :

Configuration pour le LAN :

Pour notre poste administrateur on lui définit comme adresse IP : 192.168.10.10



Configuration pour le WAN :

Pour notre poste situer dans le WAN on sera connecté en DHCP.



Configuration du pare-feu PFSENSE :

Installation de PFSENSE :

Nous allons dans un premier temps réaliser l'installation d'une machine virtuelle sous Pfense :



Choix de l'image ISO



Créations des 3 interfaces réseaux

Début de l'installation :



+0x197de9]

Copyright and distribution notice Copyright and Trademark Notices.
Copyright(c) 2004-2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.
Copyright(c) 2014-2022. Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved.
All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.
"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.
28% <mark>{ficcept></mark>

Nous allons cliquer sur Install pour commencer l'installation de Pfense :



Nous allons sélectionner la langue :





Nous allons sélectionner l'installation Auto (ZFS) :

How would you like t	Partitioning o partition your disk?
Auto (UFS) BIOS Auto (UFS) BIOS Auto (UFS) UEFI Manual Shell	Guided Root-on-ZFS Guided Disk Setup using BIOS boot method Guided Disk Setup using UEFI boot method Manual Disk Setup (experts) Open a shell and partition by hand
K	O <mark>K > <c< mark="">ancel></c<></mark>

ZFS Con Configure Options:	figuration
<pre>>>> Install T Pool Type/Disks: - Rescan Devices - Disk Info N Pool Name 4 Force 4K Sectors? E Encrypt Disks? P Partition Scheme S Swap Size M Mirror Swap? W Encrypt Swap?</pre>	Proceed with Installation stripe: 0 disks * pfSense YES NO GPT (BIOS) 1g NO NO
< <mark>S</mark> elect≻	<cancel></cancel>

Nous allons sélectionner une configuration sans redondance :

pfSense Installe	
_	ZES_Configuration
	Select Virtual Device type:
	stripeStripeNo RedundancyMirrorMirror - n-Way Mirroringraid10RAID 1+0 - n x 2-Way Mirrorsraid21RAID-21 - Single Redundant RAIDraid22RAID-22 - Double Redundant RAIDraid23RAID-23 - Triple Redundant RAID
	Cancel> [Press arrows, TAB or ENTER]

Choix du disque virtuel :

pfSense Installer		
	ZFS Configuration	
	*] <mark>1</mark> a0 UMware, UMware Virtual S	
	COR CRAck >	

Nous autorisont la suppressions de nos données :

pfSense Instal	
	-2FS Configuration Last Chance! Are you sure you want to destroy the current contents of the following disks:
	daØ
	<pre></pre>



Nous allons finir l'installation sans apporter d'autre modifications :

Manual Configuration The installation is now finished. Before exiting the installer, would you like to open a shell in the new system to make any final manual modifications?	
< Yes > < No >	

Nous allons redémarrer notre VM afin de finir l'installation :



L'installation c'est donc dérouler avec succès.

Configuration des interfaces réseaux :

Nous allons maintenant configurer les interfaces réseaux de Pfense :

- Le WAN sera connecté en DHCP
- Le LAN aura une IP statique ici 192.168.10.254
- La DMZ aura une IP statique ici 192.168.30.254

L'interface coté WAN est connecté en DHCP nous n'avons donc pas besoin de la configurer :

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 96460e3499b32302793a
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)
                                               -> v4/DHCP4: 192.168.1.94/24
v6/DHCP6: 2001:861:8c81:26d0:20c:29ff:feae:ceb
                         -> ем0
5/64
                                               -> v4: 192.168.1.1/24
v6/t6: 2001:861:8c81:26d3:20c:29ff:feae:cebf/6
 LAN (lan)
                         -> ем1
                                                         9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restare recent configuration
 0) Logout (SSH only)
 1) Assign Interfaces
2) Set interface(s) IP address
     Reset webConfigurator password
Reset to factory defaults
 3)
 4)
     Reboot system
 5)
                                                          15) Restore recent configuration
16) Restart PHP-FPM
    Halt system
Ping host
Shell
 7)
 8)
Enter an option: 2
```

Nous allons sélectionner 2) dans le menu afin de configurer nos interfaces réseau :

WAN	(wan)	_> ем0	-> V4	4/DHCP4	4: 192.168.1.94/24
			V	6/DHCP6	5: 2001:861:8c81:26d0:20c:29ff:feae:cel
5⁄64 LAN 4	(lan)	-> ем1	-> v4 v6	4: 192. 6∕t6: 2	.168.1.1/24 2001:861:8c81:26d3:20c:29ff:feae:cebf/0
0) 1) 2) 3) 4) 5) 6) 7) 8)	Logout Assign Set int Reset w Reset t Reboot Halt sy Ping ho Shell	(SSH only) Interfaces erface(s) IP addre ebConfigurator pas o factory defaults system stem st	ess sword ;	9) 10) 11) 12) 13) 14) 15) 16)	pfTop Filter Logs Restart webConfigurator PHP shell + pfSense tools Update from console Enable Secure Shell (sshd) Restore recent configuration Restart PHP-FPM
Ente	r an op	tion: 2			
Ava i	lable i	nterfaces:			
1 – 2 –	WAN (em LAN (em	0 - dhcp, dhcp6) 1 - static)			
Ente	r the n	umber of the inter	face yo	ou wish	h to configure:

Nous allons sélectionner l'interface 2 - LAN (em1) :

 Choix de l'adresse IP statique : 192.168.10.254 /24 qui nous servira également de passerelle.

```
Available interfaces:
1 – WAN (ем0 – dhcp, dhcp6)
2
 – LAN (ем1)
3 – ОРТ1 (ем2)
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.254
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
                    = 8
     255.0.0.0
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

Ensuite nous allons sélectionner l'interface 3 – OPT1(em2) qui sera notre DMZ:

 Choix de l'adresse IP statique : 192.168.30.254 /24 qui nous servira également de passerelle.

```
1 - WAN (eM0 - dhcp, dhcp6)
2 - LAN (eM1 - static)
3 - OPT1 (eM2)
Enter the number of the interface you wish to configure: 3
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.30.254
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.08 = 24
    255.255.0.0 = 16
    255.0.0.0 = 8
Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on OPT1? (y/n) n
```

Connection depuis l'interface WEB depuis un poste du LAN :

E	utilisateur@debiantest: ~	Q =	×	
<pre>utilisateur@debiantest:- 1: lo: <loopback,up,lowe t qlen 1000 link/loopback 00:00: inet 127.0.0.1/8 scc valid_lft forever inet6 ::1/128 scope valid_lft forever 2: ens33: <broadcast,mul roup default qlen 1000 link/ether 00:0c:29: altname enp2s1 inet 192.168.10.30/2 valid_lft forever inet6 2a04:cec0:122a ddr valid_lft 3439sec inet6 fe80::20c:29ff valid_lft forever utilisateur@debiantest:-</broadcast,mul </loopback,up,lowe </pre>	<pre>\$ ip a R_UP> mtu 65536 qdisc noqueue state U 00:00:00:00 brd 00:00:00:00:00:00 pe host lo • preferred_lft forever host • preferred_lft forever TICAST,UP,LOWER_UP> mtu 1500 qdisc pf 63:4c:62 brd ff:ff:ff:ff:ff e4 brd 192.168.10.255 scope global ens: • preferred_lft forever 1:7274:20c:29ff:fe63:4c62/64 scope glob : preferred_lft 3439sec *fe63:4c62/64 scope link • preferred_lft forever * ■</pre>	NKNOWN group de ifo_fast state 33 bal dynamic mn <u>c</u>	efaul UP g jtmpa	Nous allons nous connecter à l'interface WEB depuis un poste qui se trouve dans le LAN ici : - 192.168.10.30 Et qui aura comme passerelle : - 192.168.10.254

Connexion avec comme identifiant admin et mot de passe Pfense :

ē	🗾 pfSense - Log	in	×	+												\sim		×
\leftarrow	\rightarrow G	08	https:	//192.10	68.10).25 4/in	nterface	es.php?	?if=opt	:1		ふ	☆		${igardown}$	۲	பி	≡
	of se	n	se,											Lo	ogin to	pfSe	ense	
							S	SIGN										
						adm	nin											
						•••	•				-							
								SIGN	N IN									

Nous allons commencer par renommer OPT1 (em2) par DMZ :

🖬 pfSense	e.home.arpa - Inte ×	+					
$\leftarrow \ \rightarrow$	C	୍ଚ <u>ଛ</u> କ	192.168.10.254	/interfaces.ph	p?if=opt1		
		System -	Interfaces -	Firewall 🗸	Services -	VPN -	Status 🗸 I
	WARNING: The 'a	admin' acco	unt password i	s set to the d	efault value.	Change th	e password i
	Interfaces	/ OPT1	(em2)				
	General Conf	iguration					
	Enal	ble 🔽 E	Enable interface	9			
	Descripti	DN	IZ				
		Ente	er a description	(name) for t	he interface h	ere.	
	IPv4 Configurati Ty	on Sta	tic IPv4				~
	IPv6 Configurati	No No	ne				~

Bootup complete FreeBSD/amd64 (pfSense.home.arpa) (ttyv0) UMware Virtual Machine - Netgate Device ID: e5a16cd19d33c0bb6ccf *** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense *** WAN (wan) -> ем0 -> v4/DHCP4: 192.168.195.135/24 v6/DHCP6: 2a04:cec0:122a:7274:20c:29ff:fed8:37 43/64 -> v4: 192.168.10.254/24 -> v4: 192.168.30.254/24 LAN (lan) -> ем1 DMZ (opt1) -> ем2 0) Logout (SSH only) 1) Assign Interfaces 9) pfTop 10) Filter Logs 11) Restart webConfigurator 2) Set interface(s) IP address Reset webConfigurator password
 Reset to factory defaults 12) PHP shell + pfSense tools 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 7) Ping host 8) Shell 15) Restore recent configuration16) Restart PHP-FPM Enter an option: 📕

Puis nous allons changer le mot de passe administrateur de base :

Système /	Gestio	nnaire d'usag	ers / Utilisateurs / Modifier	
Utilisateurs	Groupes	Paramètres	Serveurs d'authentification	
Propriétés u	ıtilisateur			
[Défini par	SYSTEM		
0	Désactivé	Cet utilisateur r	ne peut pas s'authentifier	
Nom d'u	tilisateur	admin		
Mot	de passe	Password		Confirm Password
Nom	n complet	System Administr	rator	
		Nom complet de l'u	utilisateur, à des fins administratives uniquement	
Date d'e	voiration			

Nous allons ensuite nous rendre sur l'interface WAN afin de désactiver ces deux options car nous allons travailler dans un lab :

Bloquer les réseaux privés et les adresses de loopback	Bloque le trafic depuis des adresses IP qui sont réservées pour les réseaux privés (RFC 1918: 10/8, 172.16/12, 192.168/16) les adresses locales uniques (RFC 4193: fc00::/7) et les adresses de boucle locale (127/8). Cette option doit généralement être activée, sauf si l'interface réseau est également dans un réseau privé.
Bloquer les réseaux invalides	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Nous allons maintenant pouvoir mettre en place nos règles de filtrages afin de contrôler le trafic.

Mise en place des règles de filtrages :

Mise en place du NAT :

Pour la configuration du NAT Outbound (ou NAT sortant) nous allons laisser les règles automatiques de Pfense par défaut (il fonctionnera comme un PAT ici) :

Serveur X For	nation X Post	Administrateur ×	DebianServeur X	RouteurDebian X	Debi X	<>
Activities O Fin		15 dec.	20:46			Č,
proense.no	intelarpa - Paren	Ŧ			· ·	<u></u>
$\leftarrow \ \rightarrow \ G$	🔿 🗛 https://1	92.168.10.254/firev	vall_nat_out.php	80 % 🏠	⊠ പ്	≡
COMMUNITY EDITION	me 🗸 Interfaces 🗸 P	are-feu + Services + V	∕PN → État → Diagno:	stics - Aide -		•
Pare-feu / NA	T / Sortant				6	
Transfert de port 1:1	Sortant NPt					
Mode NAT sortan	it					
Mode	Création automatique de règles NAT sortantes. (IPsec passthrough inclu)	O Création hybride de règles NAT sortantes. (NAT sortant automatique + règles ci-dessous)	O Création manuelle de régles NAT sortantes. (NSA - NAT sortant avancée)	O Désactiver la création de règles NAT sortantes. (Aucune règle NAT sortant)		
Mappages	e Port source Desti	nation Port destination	Adresse NAT Por	t NAT Port statique De	scription Actions	6
			j Ajouter l Aj	outer 🕅 Supprimer 🚫	Toggle 📑 Enregist	rer
Automatic Rules e or press Ctrl+G.			E		(e) e	

- Toutes les machines de mon réseau pourront donc pouvoir accéder à internet à partir d'une seule adresse IP public.

Nous allons ensuite devoir configurer une règle de redirection de ports afin que notre serveur WEB (192.168.30.10) soit accessible depuis le WAN.

Nous devrons aller dans la partie Port Forward (ou Transfert de port en français) pour créer une nouvelle règle :

Serveur X PosteAdministrateur C DebianServeur X DebianServeur X DebianServeur X DebianServeur X DebianServeur X DebianServeur X DebianSer	_ + →
Activites SFirefox ESR	⊙ ▼
● ■ pfSense.home.arpa - Pare× + ×	×
$\leftarrow \rightarrow \mathbb{C}$ ($\bigcirc \mathbb{A}$ https://192.168.10.254/firewall_nat.php 80% \Leftrightarrow	ש ≡
COMMUNITY EDITION	€
Pare-feu / NAT / Transfert de port	0
Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan. Surveiller le rechargement des filtres.	×
Transfert de port 1:1 Sortant NPt	
Règles	
Adresse Ports Adresse de	tions
□ ✓ X WAN TCP * * WAN address 443 192.168.30.10 443 (HTTPS) (HTTPS)	0
🕇 Ajouter 🕽 Ajouter 🛅 Supprimer 🚫 Toggle 🖬 Enregistrer 🕂 Sép	arateur
Légende Autoriser	
X Règle liée	
or press Ctrl+G. 📮 📴 🕫 🛞 🛞 🗷 🖉 🤇	

- Dans interface sélectionner : WAN
- Dans Famille d'adresse sélectionner : IPv4
- Dans Protocole sélectionner : TCP
- Dans Destination sélectionner : WAN address
- Dans Plage de port de destination sélectionner : HTTPS
- Dans IP de redirection cible choisir Hôte unitaire puis rentré son adresse ici celle du serveur web : 192.168.30.10
- Dans Port de redirection cible sélectionner : HTTPS

Nous allons pouvoir maintenant passer à la configuration des règles de filtrage de nos différents réseaux (LAN/DMZ/WAN).

Règles de filtrage pour le LAN :

ense.r	nome											
3		0	🔒 https:/	/192.168	3.10.25	54/firewall_r	rules.p	hp?if=lan			<u>ک</u>	•
pf COMMU		ISE S	Système 🗸	Interface	es •	Pare-feu 🗕	Servic	es 🗸 VPN	✓ État ✓	Diagnostics 🗸 🖌	\ide ▼	C
Pa	are-	-feu /	Règles /	LAN							₽	E 📖 🗏 😧
Flot	tant(e) WAN	LAN D	MZ								
		(- .										
Rè	ègle	s (Faire	glisser po	our cha	nger	l'ordre)			File			
Rè	ègle	s (Faire États	glisser po Protocole	our cha Source	nger Port	l'ordre) Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
Rè	ègle: ✓	s (Faire États 1/309 KiB	glisser po Protocole *	our cha Source *	nger Port *	l'ordre) Destination LAN Address	Port 443 80	Passerelle *	File d'attente *	Ordonnancement	Description Règle anti-blocage	Actions
Rè	ègle: ✓	s (Faire États 1/309 KiB 11/622 KiB	glisser po Protocole * IPv4 *	Source * LAN net	nger Port *	l'ordre) Destination LAN Address	Port 443 80 *	Passerelle * *	File d'attente * aucun	Ordonnancement	Description Règle anti-blocage Default allow LAN to any rule	Actions
	ègle:	s (Faire États 1/309 KiB 11/622 KiB 0/0 B	glisser po Protocole * IPv4* IPv6*	Source * LAN net LAN net	nger Port * *	l'ordre) Destination LAN Address *	Port 443 80 *	Passerelle * *	File d'attente * aucun aucun	Ordonnancement	Description Règle anti-blocage Default allow LAN to any rule Default allow LAN	Actions Com Co

Par défaut, Pfsense autorise toutes les connexions sortantes. Ne souhaitant pas bloquer une connexion en particulier, nous pouvons laisser les règles par défaut.

Nous pouvons aussi autoriser uniquement les connexions voulues :

- Accès au serveur WEB.
- Accès au serveur FTP.
- Accès à Internet.

Flot	tant(e) WA	N LAN I	DMZ								
Ré	ègle	s (Faire	e glisser p	our cha	nger	l'ordre)						
		États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
	~	1/174 KiB	*	*	*	LAN Address	443 80	*	*		Règle anti- blocage	\$
	~	8/21 KiB	IPv4 TCP/UDP	LAN net	*	192.168.30.10	53 (DNS)	*	aucun			ᢤ∥ □ О́面́×
	~	0/10 KiB	IPv4 TCP	LAN net	*	192.168.30.10	443 (HTTPS)	*	aucun			҄ ⊕ ∕ / □ О іі ×
	~	0/10 KiB	IPv4 TCP	LAN net	*	192.168.30.10	22 (SSH)	*	aucun		SFTP	⊕́ ∕∕́ [] О́а́×
	~	1/89 KiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	aucun			҄ ҈⊎∕ О́ Ё ×

Règles de filtrage pour la DMZ :

R	ègle	s (Fair	e glisser	pour change	r l'or	dre)						
0		États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
0	~	0/0 B	IPv4 TCP	192.168.30.10	*	192.168.10.20	3306	*	aucun		autoriser les requetes sql du serveur web vers le serveur mariadb	҈⊎ ∥ □О 直 ×
0	×	0/588 B	IPv4 *	DMZ net	*	LAN net	*	*	aucun			∛ ∕∕ □0 1
	~	0/5 KiB	IPv4 *	DMZ net	*	*	*	*	aucun			Ů∕ □O ■×
0	~	0/0 B	IPv4 ICMP <u>any</u>	*	*	*	×	*	aucun			Ů∕ □Ø ā×
	~	0/0 B	IPv4 TCP	*	×	*	×	×	aucun			Ů ∕ □⁄ ā ×

Nous souhaitons limiter les communications de la DMZ vers le LAN :

- On autorise le serveur web (192.168.30.10) à communiquer avec le serveur MariaDB (192.168.10.20) sur le port 3306.
- On bloque toutes les autres connexions vers le LAN

Puis:

- On autorise toutes les connexions vers les autres réseaux

Nous pouvons aussi autoriser uniquement les connexions voulues :

Flot	ttant(e) W	'AN LAN	DMZ								
Ré	ègle	s (Fai	re glisser	pour change	r l'or	dre)						
		États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
	~	0/0 B	IPv4 TCP	192.168.30.10	*	192.168.10.20	3306	*	aucun		autoriser les requetes sql du serveur web vers le serveur mariadb	∜ ∕∕ □ ○ 面 ×
	~	0/0 B	IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)	*	aucun			҈⊎ ∕∕ □О 直 ×
	~	1/16 KiB	IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	aucun			҈⊎ ∕∕ □О 直 ×
	×	0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	aucun			∜∥ □0 ∎

Règles de filtrage pour le WAN :

•	🗾 pfSe	ense.h	ome	arpa -	Pare×	+									\sim		×
\leftarrow	\rightarrow C			(🔿 🗛 htt	ps:// 192	.168.1	0.254/firewall	_rules.php?i	f=wan				☆	\bigtriangledown	பி	≡
	c			ISE.	Système		faces		Services -	VPN - É	tat 🗕 Dia	agnostics 🗸 Aide 🗸			•		
		Pa	are	-feu /	Règle	s/W	AN							≢ ₩ 🗏 9			
		Flott	ant(e) W	AN LAN	DMZ											
		Rè	gle	s (Fai	re glisse	r pour (chan	ger l'ordre)									
				États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions			
			~	0/0 B	IPv4 TCP	*	*	192.168.30.10	443 (HTTPS)	*	aucun			∜ ∕∕ □ ⊘ ≣×			
			~	0/0 B	IPv4 TCP	*	*	192.168.30.10	443 (HTTPS)	*	aucun		NAT	҈∜ /́ □ О ≣			
			×	0/0 B	IPv4 *	*	*	LAN net	*	*	aucun			҈₩ <i>№</i> © О П			
								1 Ajo	outer 🕽 Ajo	outer <u> </u>	oprimer	Toggle	Enregist	rer 🕂 Séparate	ur		
		6															

- Nous allons autoriser les connexions HTTPS au serveur web (192.168.30.10) pour tous les postes du réseau WAN.
- On peut également voir la régle de redirection de port crééé via le NAT.
- Nous bloquons l'accès au LAN.

Nous allons maintenant pouvoir tester nos règles de filtrage !

Test de Connexion :

- Autoriser les accès au serveur Web depuis Internet (WAN) et depuis le LAN :

Depuis le WAN :



Depuis le LAN :



_

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

sftp://u	tilisateur	@192	2.168.30.10 - Fil	eZilla				×
Fichier Édition Affichage Transfert Serveur Favoris ?								
# · • • • • • • • • • • • • •	Q s)	%					
Hôte : sftp://192.168.30.1 Identifiant : utilisateur Mot de passe	: ••••	•	Port :	Co	onnexion rapide	•		
Statut : Connexion à 192.168.30.10 Statut : Using username "utilisateur". Statut : Connected to 192.168.30.10 Statut : Démarrage du téléchargement de /home/utilisateur/Documents/p Statut : Transfert de fichier réussi, 8 148 octets transférés en 1 seconde	ocedure	pour	H.odt					
Site local : /home/utilisateur/Documents/		•	Site distant :	/home/utilis	isateur/Documents			•
Documents Images			?	local .mozilla				
Nom de fichier 🔨 Taille de fic Type de fichier Dernière modifi			?	.ssh				
			2	Bureau				
procedure pour H.odt 8148 odt-fichier 06/01/202517:			2	Documents				
			Nom de fichier	🔥 Tai	uille de fi Type de fic	Dernière modi	Droits d'acc	Propriétaire
						1		
			📄 procedure p	our	8148 odt-fichier	06/01/2025	rw-rr u	tilisateu
1 fichier. Taille totale : 8148 octets			Sélection de 1	fichier. Taill	lle totale : 8148 octe	ts		
Serveur / Fichier local Directio Fichier distant Tail	e Priori	té T	emps					
sftp://utilisateur@19								
home/utilisateur/D << /home/utilisateur/Docu 814	8 Norm.	06	5/01/2025 17:21:	39				
Fichiers en file d'attente Transferts échoués Transferts réussis (1))					ile d'attente unida		

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

Depuis le LAN :



Depuis la DMZ :



- Interdire tout accès au LAN depuis l'Internet (WAN) ou la DMZ :

Depuis le WAN :

<pre>tivités I Terminal * 4 janv. 20:21</pre>	Serveur	×	FreeBSD version 10 and earlie >	C DebianServeur	×	Windows Server	2019 X	🕞 Debia	n11 2			
<pre>valid_lft forever preferred_lft forever utilisateur@debianClient:~\$ ping 192.168.10.10 PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data. ^C 192.168.10.10 ping statistics 2 packets transmitted, 0 received, 100% packet loss, time 1027ms utilisateur@debianClient:~\$ cat /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 auto ens33 iface ens33 inet dhcp # address 192.108.0.10 # netmask 255.255.0 # gateway 192.108.0.254 utilisateur@debianClient:~\$ su - Mot de passe :</pre>	tivités		🔄 Terminal 🔻	4 janv. 2	0:21				?	())	С	•
<pre>valid_lft forever preferred_lft forever utilisateur@debianClient:~\$ ping 192.168.10.10 PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data. ^C 192.168.10.10 ping statistics 2 packets transmitted, 0 received, 100% packet loss, time 1027ms utilisateur@debianClient:~\$ cat /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 auto ens33 iface ens33 inet dhcp # address 192.108.0.10 # netmask 255.255.0 # gateway 192.108.0.254 utilisateur@debianClient:~\$ su - Mot de passe :</pre>												
<pre>valid_lft forever preferred_lft forever utilisateur@debianClient:-\$ ping 192.168.10.10 PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data. ^C 192.168.10.10 ping statistics 2 packets transmitted, 0 received, 100% packet loss, time 1027ms utilisateur@debianClient:-\$ cat /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 auto ens33 iface ens33 inet dhcp # address 192.108.0.10 # netmask 255.255.0 # gateway 192.108.0.254 utilisateur@debianClient:-\$ su - Mot de passe :</pre>	€			utilisateur@deb	ianCl	ient: ~		٩	Ξ	>	¢	
<pre># 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 auto ens33 iface ens33 inet dhcp # address 192.108.0.10 # netmask 255.255.0 # gateway 192.108.0.254 utilisateur@debianClient:~\$ su - Mot de passe :</pre>	util: PING ^C 2 pac	v isat 192 192. cket	<pre>valid_lft forever pref teur@debianClient:~\$ p 2.168.10.10 (192.168.1 .168.10.10 ping statis ts transmitted, 0 rece teur@debianClient:~\$ c</pre>	erred_lft for ing 192.168.1 0.10) 56(84) tics ived, 100% pa at /etc/netwo	ever 0.10 byte cket rk/i	s of data. loss, time nterfaces	1027ms					
<pre>source /etc/network/interfaces.d/* # The loopback network interface auto lo iface lo inet loopback auto ens33 iface ens33 inet dhcp # address 192.108.0.10 # netmask 255.255.255.0 # gateway 192.108.0.254 utilisateur@debianClient:~\$ su - Mot de passe : ■</pre>	# Th: # and	is f d ho	file describes the net ow to activate them. F	work interfac or more infor	es a mati	vailable on on, see inte	your sys erfaces(5	stem 5).				
<pre># The loopback network interface auto lo iface lo inet loopback auto ens33 iface ens33 inet dhcp # address 192.108.0.10 # netmask 255.255.0 # gateway 192.108.0.254 utilisateur@debianClient:~\$ su - Mot de passe :</pre>	sour	ce /	/etc/network/interface	s.d/*							I	
auto ens33 iface ens33 inet dhcp # address 192.108.0.10 # netmask 255.255.255.0 # gateway 192.108.0.254 utilisateur@debianClient:~\$ su - Mot de passe : ■	# The auto iface	e lo lo e lo	oopback network interf o inet loopback	ace								
	auto ifaco # # util : Mot o	ens e er isat de p	s33 ns33 inet dhcp address 192.108.0.10 netmask 255.255.055.0 gateway 192.108.0.254 teur@debianClient:~\$ s passe : ∎	u -								

Depuis la DMZ :

🕞 Serveur 🛛 🕹	Formation X	PosteAdministrateur	X DebianServe	ur 🗙 🗋 Routeur(Debian X	Debi 🗙	
Activités	Ы Terminal 🔻		15 déc. 19:51			()	り -
		utilis	sateur@debian11: ~		۹ :	= ×	
utilisa PING 8. 64 byte 64 byte cc 8.8 2 packe rtt min utilisa PING 19 64 byte 64 byte 64 byte cc 192 2 packe rtt min utilisa PING 19 cc 192 3 packe utilisa	teur@debian11 8.8.8 (8.8.8. s from 8.8.8. s from 8.8.8. s from 8.8.8. .8.8 ping sta ts transmitte /avg/max/mdev teur@debian11 2.168.10.10 pi ts transmitte /avg/max/mdev teur@debian11 2.168.10.10 pi ts transmitte teur@debian11	<pre>:~\$ ping 8.8.8. 8) 56(84) bytes 8: icmp_seq=1 t 8: icmp_seq=2 t d, 2 received, = 11.120/11.16 :~\$ ping 192.16 192.168.10.10) 8.10.10: icmp_s 8.10.10: icmp_s 8.10.10: icmp_s d, 2 received, = 1.740/2.659/ :~\$ ping 192.16 192.168.10.10) mg statistics - d, 0 received, .:~\$</pre>	8 5 of data. 5 tl=114 time=11 5 tl=114 time=11 0% packet loss 55/11.211/0.045 58.10.10 56(84) bytes o 5eq=1 ttl=63 ti 5eq=2 ttl=63 ti 53.578/0.919 ms 58.10.10 56(84) bytes o 100% packet los	.2 ms .1 ms , time 1001ms ms f data. me=3.58 ms me=1.74 ms , time 1001ms f data. ss, time 2052m	ns		
use pointer insid	le or press Ctrl+G.			🕞 📀 🔄 🐗	1 R! 💾 🕾 🎯 3	$\sim \diamond \diamond$	D,

- autoriser les requêtes SQL du serveur WEB vers le serveur MariaDB :

Afin de pouvoir nous connecter au serveur MariaDB nous devons au préalable installer mariadbclient sur notre serveur web :

Activités 🗵 Terminal 🔻 15 déc. 20:16	t) () 🔻
utilisateur@debian11: ~	Q = ×	
<pre>root@debianl:-# sudo apt-get install mariadb-client Lecture des listes de paquets Fait Construction de l'arbre des dépendances Fait Lecture supplémentaires suivants seront installés : libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libmariadb libterm-readkey-perl mariadb-client-10.5 mariadb-client-core-10.5 mariadb-common mysql-common Paquets suggérés : libmldbm-perl libnet-daemon-perl libsql-statement-perl Les NOUVEAUX paquets suivants seront installés : libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libmariadb libterm-readkey-perl mariadb-client mariadb-client-10.5 mariadb-client-core-10.5 mariadb-client 10.5 mariadb-client-core-10.5 mariadb-client 10.5 mariadb-client-core-10.5 mariadb-common mysql-common 0 mis à jour, 10 nouvellement installés, 0 à enlever et 31 non mis à 11 est nécessaire de prendre 3 526 ko dans les archives. Après cette opération, 39.6 Mo d'espace disque supplémentaires seror Souhaitez-vous continuer ? [0/n] o Réception de :1 http://security.debian.org/debian-security bullseye- n amd64 mariadb-common all 1:10.5.26-0+deb11u2 [37,5 kB] Réception de :2 http://deb.debian.org/debian-security bullseye- n amd64 libmariadb3 amd64 1:10.5.26-0+deb11u2 [177 kB]</pre>	o3 à jour. ht utilisés. -security/mai oconfig-inifi -security/mai	
se pointer inside or press Ctrl+G. 🔤 😋 🖧 🕫 🖆	1 A © A 4 4	D //

Puis connexion au serveur MariaDB :

C RouteurDebiar	X Debian 11 2	X Windows 11 x64	X Windows Server 2019) 🗙 🕞 Se	rveurMariaDB $ imes$		${} \longleftrightarrow$
Activités	🔄 Terminal 🔻	15 d	léc. 20:17		.?. •))	•
Ð		utilisateu	ır@debian11: ~		۹ ≡	×	
2: ens3: roup de lini alti ine dr utilisa Enter p Welcome Your Ma Server v Copyrig Type 'hu MariaDB	<pre>valid_lft foreve 3: <broadcast,ml fault qlen 1000 k/ether 00:0c:29 name enp2s1 t 192.168.10.20, valid_lft foreve t6 2001:861:8c81 valid_lft 863108 t6 fe80::20c:291 valid_lft foreve teur@debian11:-{ assword: to the MariaDB riaDB connection version: 10.5.26 ht (c) 2000, 201 elp;' or '\h' fo [(none)]> GRANT FIED BY 'root';</broadcast,ml </pre>	r preferred lft DITICAST, UP, LOWEF 24 brd 192.168.1 r preferred lft :2640:20c:29ff:1 cec preferred_lft if:fea7:7d1d/64 s r preferred_lft sudo mariadb -u monitor. Commar id is 31 i-MariaDB-0+deb11 8, Oracle, Maria or help. Type '\o FLUSH PRIVILEGES FLUSH PRIVILEGES	forever R_UP> mtu 1500 qdi f:ff:ff:ff:ff:ff 10.255 scope globa forever fea7:7dld/64 scope c 14310sec scope link forever J root -p ads end with ; or Lu2 Debian 11 aDB Corporation Ab c' to clear the cu ON *.* TO 'admini i5;	sc pfifo_f l ens33 global dy \g. and other rrent inpu strateur¶@	ast state U namic mngtm s. t statement '192.168.30	P g pad	
IDENT	iiilb bi ioot ,		-5,				
ouse pointer insid	e or press Ctrl+G.			💽 🔂 🕼 🕸	<u>– no n</u> (<	7 //

Connexion réussie !

Serveur ×	Formation X	osteAdministrateur	X DebianServeur	X RouteurDebian	X 🕞 Debi.	×	\leftarrow
Activités	Ы Terminal 🔻		15 déc. 20:19				•
E		utili	sateur@debian11:~		۹ =	×	
<pre>Paramétrage de libterm-readkey-perl (2.38-1+b2) Paramétrage de libdbi-perl:amd64 (1.643-3+b1) Paramétrage de libdbd-mariadb-perl (1.21-3) Paramétrage de mariadb-client-core-10.5 (1:10.5.26-0+deb11u2) Paramétrage de mariadb-client (1:10.5.26-0+deb11u2) Paramétrage de mariadb-client (1:10.5.26-0+deb11u2) Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) Traitement des actions différées (« triggers ») pour libc-bin (2.31-13+deb11u1) root@debian11:~# mysql -u webuser -p -h 192.168.10.20 Enter password: ERROR 1130 (HY000): Host '192.168.30.10' is not allowed to connect to this Maria DB server root@debian11:~# mysql -u administrateur -p -h 192.168.10.20</pre>							
Enter p Welcome Your Ma Server	essword: to the MariaDB m riaDB connection version: 10.5.26-	onitor. Co id is 30 MariaDB-0+d	mmands end with ebllu2 Debian ll	; or \g.			
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)]>							
nouse pointer insi	de or press Ctrl+G.			🔜 🚱 🔂 🕼 🕫 🕯	∎ ಇ ⊚ ಇ <	< <	J //

Conclusion:

Tous les points du cahier des charges ont été respectés. Le serveur WEB est déployé dans un réseau DMZ, et le serveur de bases de données MariaDB est déployé dans le LAN. Les règles de filtrage ont été configurées via PFSENSE.

- Le serveur web est accessible depuis Internet et le LAN.
- Le serveur MariaDB est installé dans le LAN avec autorisation des requêtes SQL du serveur web.
- Les règles de sécurité permettent les accès FTP et Internet selon les spécifications, tout en interdisant l'accès au LAN depuis Internet et la DMZ.

Ce projet a permis de sécuriser les accès aux serveurs et d'améliorer la gestion des services accessibles depuis l'extérieur. Tous les objectifs ont été atteints avec succès.