

KAPALA Paul-Alexis

MASSEI Liam

LIGNIERE Timothée

BTS SIO2

Date de création 21/03/23

Date de maj 15/04/23

DMZ

Sommaire

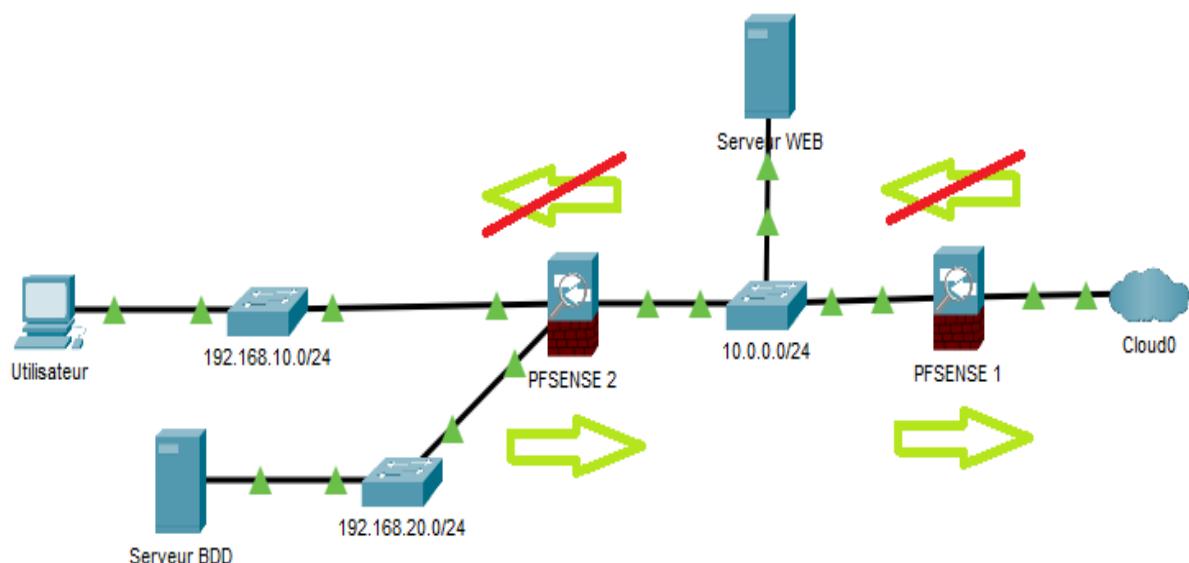
1 - Problématique.....	2
2 - Schéma logique de la solution.....	2
3 - Notice d'installation.....	3
3.1.1 - Installation de Pfsense.....	3
3.1.1 – Configuration basique du Pfsense 1.....	7
3.1.1.1 – Configuration passerelle.....	7
3.2 – Configuration basique du Pfsense 2.....	9
3.3 – Connecter les machines aux Pfsenses.....	11
3.4.1 – Configuration poussée du Pfsense 1.....	12
3.4.1.1 – Mise en place du proxy.....	13
3.4.1.2 – Routage statique du web à la BDD.....	18
3.4.2 – Configuration poussée du Pfsense 2.....	20
3.5 – Installer les services sur les serveurs.....	21
3.5.1 – Installation du serveur WEB.....	21
3.5.2 – Installation de la BDD.....	22
4 – Résolution de potentiels problèmes.....	23
4.1 – Problème de communications entre machines.....	23
4.2 – Problème d'Internet sur les clients.....	23
4.3 – Problème de connexion à la page web des Pfsenses.....	23
4.4 – Aucune des vérifications n'apportent de résultat.....	24
5 - Annexes.....	25

1 - Problématique

Il peut être nécessaire de sécuriser un réseau des menaces extérieures tout en laissant un accès volontaire à un site web et en conservant pour autant la connexion à Internet pour les machines des utilisateurs du réseau. Une solution a été recommandé par l'ANSSI afin de résoudre cette problématique, la DMZ (ou Zone démilitarisée).

Une DMZ a pour but de sécuriser un réseau interne tout en permettant aux machines des utilisateurs d'accéder à Internet, la connexion des utilisateurs passant par deux pare-feu avec des règles légèrement différentes avant de pouvoir être reçus.

2 - Schéma logique de la solution



Le Pfsense 1 refuse toutes les connexions entrantes mis à part celles à destinations du serveur WEB à l'aide d'un reverse proxy ; le Pfsense2 bloque lui aussi toutes les connexions entrantes, mais sans exception.

L'utilisateur et le serveur BDD peuvent donc accéder à Internet, au Serveur Web et communiquer entre eux .

Le Serveur WEB ne peut qu'accéder à Internet.

3 - Notice d'installation

L'installation présentée après se déroule sous Oracle VM.

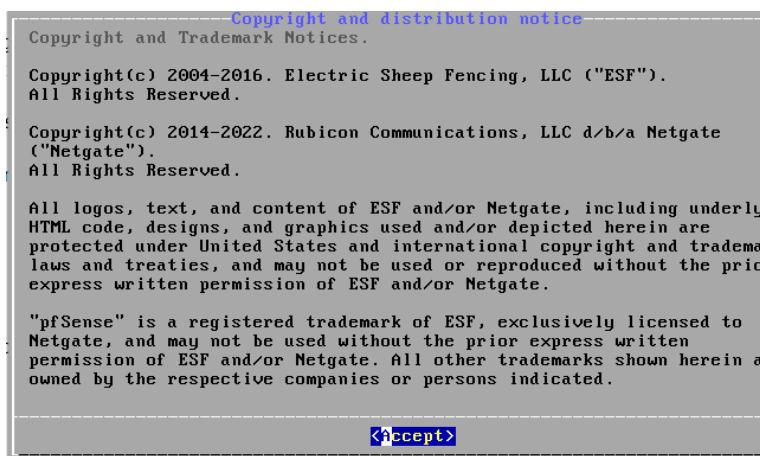
3.1.1 - Installation de Pfsense

L'installation est la même pour les 2 Pfsenses, seul la configuration diffère légèrement.

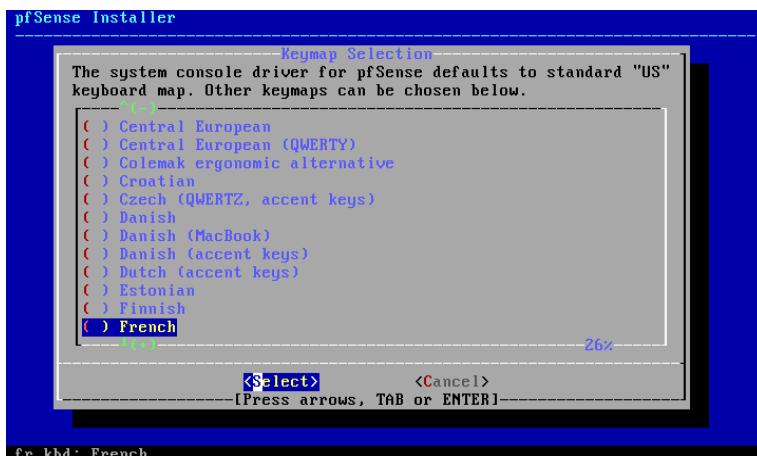
Pfsense n'est pas un logiciel à installer sur une machine déjà existante, il est sa propre machine. Crée donc une machine avec minimum 1 Go de RAM et 1 Go de stockage pour son bon fonctionnement, cela n'est pas un problème si vous lui donnez plus.

Insérez ensuite l'image iso lors de la mise en route de votre machine, il se peut que l'iso de votre pfsense soit incorrect selon votre architecture de processeur

Peu de temps après le lancement, vous aurez cet écran :



Acceptez ceci puis validez l'installation de Pfsense. Vous pourrez ensuite choisir la langue de votre clavier.

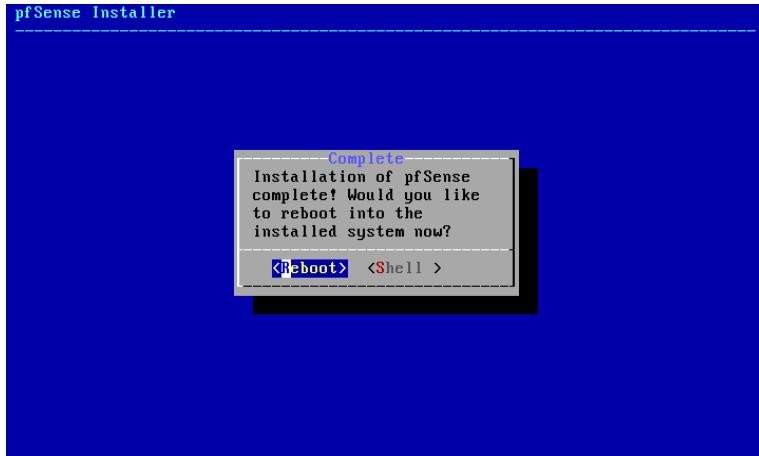


Sélectionnez-la avec les flèches puis validez. Puis continué à valider jusqu'à l'écran suivant :



Pour choisir votre disque utilisé la barre espace puis valider. L'installation devrait se lancer après la confirmation de la suppression des données du disque choisi.

Poursuivez jusqu'à cet écran.



Lorsque vous arriverez à cet écran, éjecter de force l'image iso de pfsense afin d'éviter que lors du redémarrage, l'image relance l'installation.

Après cela, redémarrer votre machine. Si tout s'est installé correctement, vous aurez cet écran à la fin du démarrage.

```
AMD Features=0x28100800<SYSCALL,MX,RDTSCP,LMB>
AMD Features2=0x121<LAHF,ABM,Prefetch>
Structured Extended Features=0x842421<FSGSBASE,AUX2,INUPCID,NPFUSG,RDSEED,CLFL
USHOPT>
Structured Extended Features3=0x10000400<MD_CLEAR,L1DFL>
TSC: P-state invariant
Done.
.... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration...done.

Default interfaces not found -- Running interface assignment option.
pcn0: link state changed to UP

Valid interfaces are:
pcn0    08:00:27:a8:ab:4a (down) AMD PCnet/PCI 10/100BaseTX

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? █
```

Pfsense va donc vous demander ses premiers paramètres.

Nous n'avons pas besoin des vlans, vous pouvez donc refuser, puis sélectionnez vos interfaces (L'une de vos interfaces doit être de préférence en accès par pont et la deuxième en réseau interne).

Le menu de base de Pfsense apparaîtra suite à cela :

```
WAN -> pcn0
LAN -> pcn1

Do you want to proceed [y\?n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: 23fa89eb5b25670dda70

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> pcn0      -> v4/DHCP4: 172.16.130.28/24
LAN (lan)      -> pcn1      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: █
```

Pfsense est donc désormais installé, la configuration de ce dernier pour initialiser la DMZ se trouve dans la partie suivante . (Vous pouvez cloner cette première machine pour le Pfsense 2 si vous êtes sur une plateforme de virtualisation).

3.1.1 – Configuration basique du Pfsense 1

3.1.1.1 – Configuration passerelle

Pour rajouter une adresse IP à la passerelle du côté du LAN, retourner sur votre Pfsense et entrer l'option 2 :

```
VirtualBox Virtual Machine - Netgate Device ID: 23fa89eb5b25670dda70
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> pcn0      -> v4/DHCP4: 172.16.130.28/24
LAN (lan)      -> pcn1      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (pcn0 - dhcp)
2 - LAN (pcn1)

Enter the number of the interface you wish to configure: 2
```

Dans le cas présent, le WAN est déjà géré par le DHCP de notre réseau (Ce n'est pas le cas si vous configurez le pcn0 du Pfsense2). Nous allons donc configurer le LAN et lui assigner l'adresse 10.0.0.254 avec un CIDR de 24 :

```
Available interfaces:
1 - WAN (pcn0 - dhcp)
2 - LAN (pcn1)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.254

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
     255.0.0.0 = 8

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:
> 
```

Vous pouvez activer le DHCP si vous le voulez, vous n'aurez qu'à remplir l'adresse de début de plage et celle de fin, vous pouvez refuser le reste.

Une fois cette configuration terminer, vous obtiendrez à peu près cela :

```
The IPv4 LAN address has been set to 10.0.0.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.0.0.254/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 23fa89eb5b25670dda70

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> pcn0      -> v4/DHCP4: 172.16.130.28/24
LAN (lan)      -> pcn1      -> v4: 10.0.0.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: [
```

Votre Pfsense est désormais prêt à gérer les machines qui seront connectées sur le LAN, afin de ne pas perdre le fil, nous allons désormais configurer le Pfsense2.

3.2 – Configuration basique du Pfsense 2

Vous pouvez démarrer votre pfsense 2 pour mettre en place les adresses sur chaque passerelle et le pfsense 1 pour vérifier la communication avec l'extérieur.

La configuration des passerelles est la même que pour le [Pfsense 1](#), cependant si votre machine a été clonée depuis la première, il peut être nécessaire de lui assigner une nouvelle interface.

Pour cela rentrer l'option 1 puis dites les différents noms de passerelles avec chacune leurs utilités (pcn0=WAN, pcn1=LAN, pcn2=OPT1)

```
Enter an option: 1

Valid interfaces are:
pcn0  08:00:27:0d:ce:48  (up) AMD PCnet/PCI 10/100BaseTX
pcn1  08:00:27:84:b1:2f  (up) AMD PCnet/PCI 10/100BaseTX
pcn2  08:00:27:26:24:39 (down) AMD PCnet/PCI 10/100BaseTX

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\?n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(pcn0 pcn1 pcn2 or a): pcn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/MAT mode.
(pcn1 pcn2 a or nothing if finished): pcn1

Enter the Optional 1 interface name or 'a' for auto-detection
(pcn2 a or nothing if finished): pcn2

The interfaces will be assigned as follows:
WAN -> pcn0
LAN -> pcn1
OPT1 -> pcn2

Do you want to proceed [y\?n]? n
```

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\?n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(pcn0 pcn1 pcn2 or a): pcn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/MAT mode.
(pcn1 pcn2 a or nothing if finished): pcn1

Enter the Optional 1 interface name or 'a' for auto-detection
(pcn2 a or nothing if finished): pcn2

The interfaces will be assigned as follows:
WAN -> pcn0
LAN -> pcn1
OPT1 -> pcn2

Do you want to proceed [y\?n]? n
```

Vous retournerez ensuite sur le menu principal avec cet affichage :

```

Writing configuration...done.
One moment while the settings are reloading... done!
route: writing to routing socket: Network is unreachable
route: writing to routing socket: Network is unreachable
route: writing to routing socket: Network is unreachable
VirtualBox Virtual Machine - Netgate Device ID: adb549a47b174f640814

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> pcn0      ->
LAN (lan)      -> pcn1      -> v4: 10.0.0.254/24
OPT1 (opt1)    -> pcn2      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■

```

Aucune des adresses n'est donc correcte, pour notre infrastructure pcn0 doit avoir comme adresse 10.0.0.253, pcn1 192.168.10.254 et pcn2 192.168.20.254 tous en CIDR 24 et comme passerelle sur pcn0 10.0.0.254. Pour rappel, ceci est similaire au [Pfsense 1.](#)

Vous aurez donc à la fin de votre configuration ceci :

```

FreeBSD/amd64 (pfSense.home.arp) (ttyv7)

login: admin
Password:
VirtualBox Virtual Machine - Netgate Device ID: adb549a47b174f640814

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> pcn0      -> v4: 10.0.0.253/24
LAN (lan)      -> pcn1      -> v4: 192.168.10.254/24
OPT1 (opt1)    -> pcn2      -> v4: 192.168.20.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■

```

La configuration basique du Pfsense 2 est terminé.

3.3 – Connecter les machines aux Pfenses

Si vous n'avez pas activé le DHCP de votre Pfense1, mettez les paramètres suivants pour l'adresse réseau :

Détails	Identité	IPv4	IPv6	Sécurité
Vitesse de la connexion 1000 Mb/s Adresse IPv4 10.0.0.1 Adresse IPv6 fe80::a00:27ff:fe51:6d0b Adresse matérielle 08:00:27:51:6D:0B Route par défaut 10.0.0.254 DNS 8.8.8.8 <input checked="" type="checkbox"/> Connexion automatique <input checked="" type="checkbox"/> Rendre accessible aux autres utilisateurs <input type="checkbox"/> Connexion avec quota : limite les données ou peut engendrer des frais <small>Les mises à jour logicielles et autres téléchargements importants ne seront pas démarrés automatiquement.</small>				Supprimer le profil de la connexion

La machine cliente a elle comme configuration ceci :

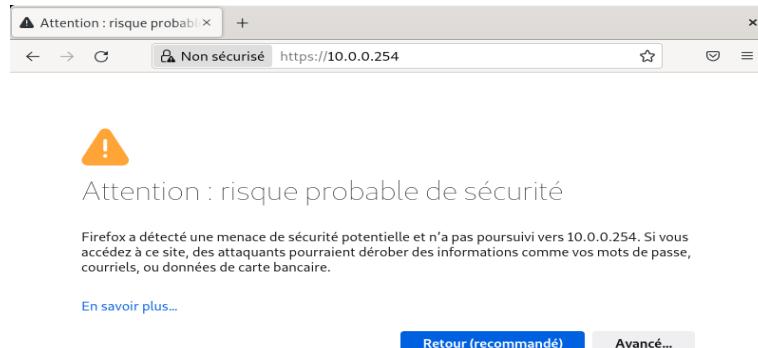
Détails	Identité	IPv4	IPv6	Sécurité
Vitesse de la connexion 1000 Mb/s Adresse IPv4 192.168.10.1 Adresse IPv6 fe80::a00:27ff:fec7:a066 Adresse matérielle 08:00:27:C7:A0:66 Route par défaut 192.168.10.1 DNS 8.8.8.8 <input checked="" type="checkbox"/> Connexion automatique <input checked="" type="checkbox"/> Rendre accessible aux autres utilisateurs <input type="checkbox"/> Connexion avec quota : limite les données ou peut engendrer des frais <small>Les mises à jour logicielles et autres téléchargements importants ne seront pas démarrés automatiquement.</small>				Supprimer le profil de la connexion

La machine gérant le serveur BDD a pour configuration :

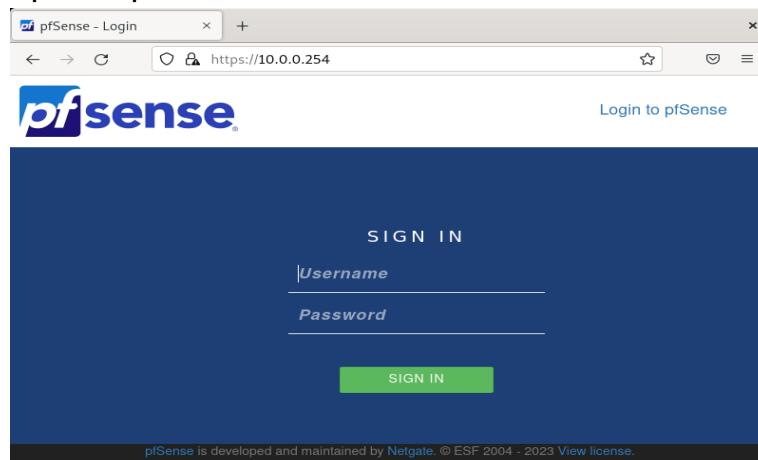
Détails	Identité	IPv4	IPv6	Sécurité
Vitesse de la connexion 1000 Mb/s Adresse IPv4 192.168.20.1 Adresse IPv6 fe80::a00:27ff:fec7:a066 Adresse matérielle 08:00:27:C7:A0:66 Route par défaut 192.168.20.1 DNS 8.8.8.8 <input checked="" type="checkbox"/> Connexion automatique <input checked="" type="checkbox"/> Rendre accessible aux autres utilisateurs <input type="checkbox"/> Connexion avec quota : limite les données ou peut engendrer des frais <small>Les mises à jour logicielles et autres téléchargements importants ne seront pas démarrés automatiquement.</small>				Supprimer le profil de la connexion

3.4.1 - Configuration poussée du PfSense 1

Connectez-vous à votre serveur Web puis dans votre navigateur, entrer l'adresse de votre PfSense 1 du côté de son LAN :



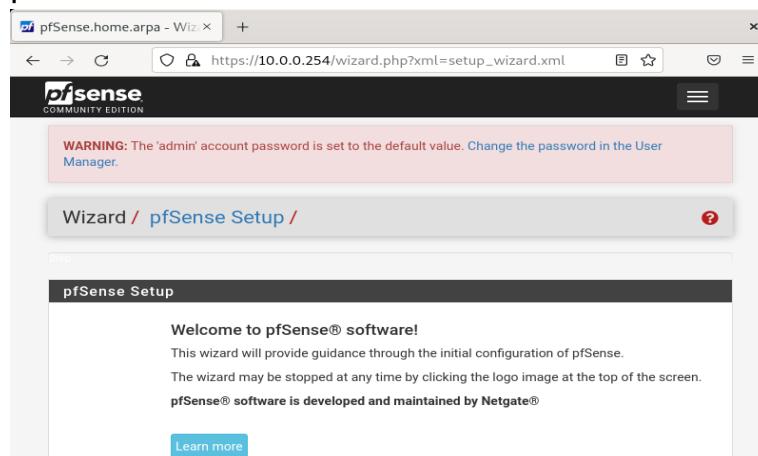
Il est possible que votre navigateur vous mettes en garde comme dans l'image précédente, mais ce n'est rien de grave, cliqué sur « Avancé... » puis « Accepter le risque et poursuivre »



Vous voilà donc sur la page de connexion de votre PfSense1, le nom d'utilisateur et le mot de passe sont toujours les mêmes lors de la première connexion :

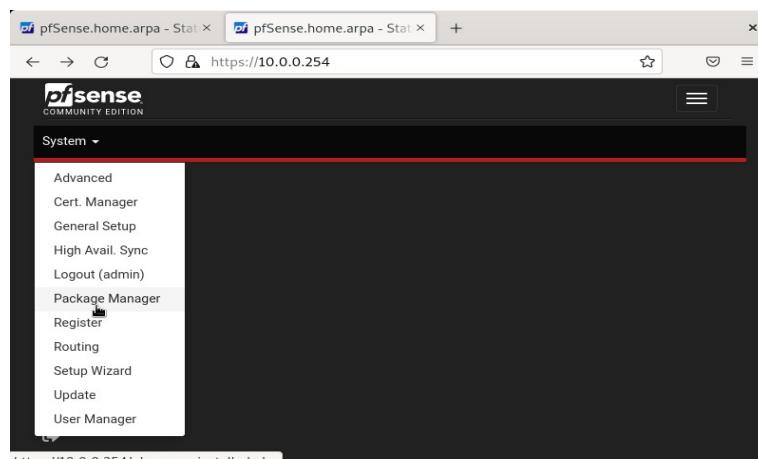
Username = admin

Password = pfSense



3.4.1.1 – Mise en place du proxy

Pour que le serveur Web soit accessible depuis l'extérieur du pare-feu, nous avons besoin de mettre en place un proxy sur le pfSense 1, pour cela, allez dans « System » puis « Package manager »



Puis sélectionné « Available Packages » en recherchant « haproxy »

Installez-le et confirmer l'installation

Puis allez dans « Services », « haproxy » et enfin « Backend »:

Puis dans « Backend », appuyer sur « add » pour rajouter un serveur web géré par le proxy, remplissez le alors avec les paramètres suivants :

Mode	Name	Forwardto	Address	Port	
<input type="checkbox"/>	active	WEB-server	Address+Port: <input type="button" value="▼"/>	10.0.0.100	80

Bien évidemment, remplissez « Address » par celle de votre machine Web. Puis sauvegarder en bas de la page. Appliquer les modifications.

Ensuite, allez dans « Frontend » :

The screenshot shows the pfSense web interface with the following details:

- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Page Title:** Services / HAProxy / Frontend
- Sub-Menu:** Settings, **Frontend**, Backend, Files, Stats, Stats FS, Templates. The "Frontend" tab is selected.
- Table Header:** Frontends, Primary, Shared, On, Advanced, Name, Description, Address, Type, Backend, Actions.
- Buttons:** Add (green), Delete (red), Save (blue).

Appuyer sur « Add » pour rajouter une règle :

The screenshot shows the pfSense web interface with the following details:

- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Page Title:** Services / HAProxy / Frontend / Edit
- Sub-Menu:** Settings, **Frontend**, Backend, Files, Stats, Stats FS, Templates. The "Frontend" tab is selected.
- Form Fields:** Name (Frontend-haproxy), Description, Status (Active).
- Section:** External address, Define what ip:port combinations to listen on for incoming connections.
- Table:** Listen address, Custom address, Port, SSL Offloading, Advanced.
- Row:** WAN address (IPv4) dropdown, Port 80.
- Buttons:** Activer Windows, Accédez aux paramètres pour activer.

Dans « default backend », nous allons rajouter une règle pour définir qui pourra utiliser le haproxy pour se connecter au serveur WEB :

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Name	Expression	CS	Not	Value	Action
ACL1	Path matches:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10.0.0.100

« Value » doit correspondre à votre adresse de serveur Web dans le cas de « Path matches ».

Puis encore une autre règle dans « Actions » tout en définissant le Backend par default pour renvoyer vers le serveur Web :

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Action	Parameters	Condition acl names	Actions
Use Backend	See below	ACL1	
backend:	Backend-haproxy-server-web		

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAcl

Default Backend Backend-haproxy-server-web

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

Vous avez terminé la configuration de Haproxy. Sauvegarder puis appliquer les changements.

Il faut néanmoins encore créer une règle pour le pare-feu pour autoriser le passage des utilisateurs extérieurs sur le serveur WEB, pour cela, dirigez-vous vers « Firewall » « Rules ».

Créé ensuite une règle avec les paramètres suivants :

```
Action = Pass  
Interface = WAN  
Address Family = IPv4  
Protocol = TCP  
Source = any  
Destination = single host 10.0.0.100 (L'adresse de votre machine WEB)  
Destination Port Range = 80 to 80 (Nous n'avons que le HTTP dans cette configuration)
```

Vous pouvez sauvegarder et essayer de, vous connectez à votre serveur WEB depuis l'extérieur (Attention, il faut que votre machine extérieure ait en passerelle l'adresse WAN du pfSense 1), cependant, nous n'avons pas encore installé le service permettant d'avoir une page web sur la machine en question.

3.4.1.2 – Routage statique du web à la BDD

Pour rappel, le serveur web doit pouvoir accéder à notre BDD sans que les utilisateurs externes au Pfsense1 puissent y accéder (la BDD).

Il faut donc mettre une route statique pour rediriger les requêtes à direction de la BDD.

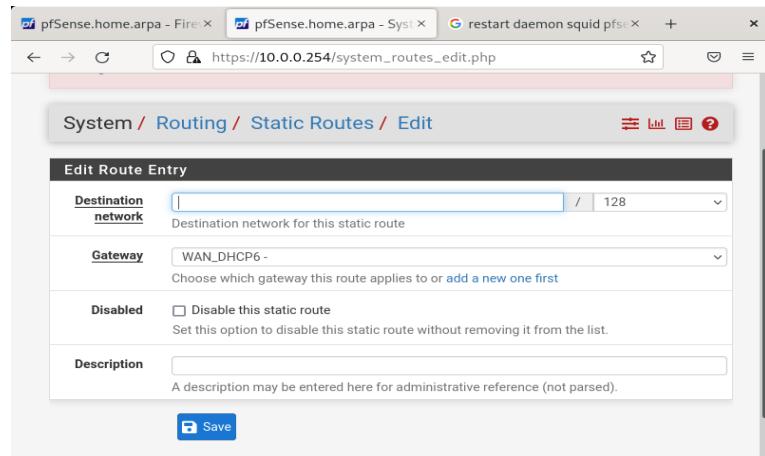
Pour cela, dirigez-vous vers « System », « Routing » et « Gateways »

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
WAN_DHCP6		WAN			Interface WAN_DHCP6 Gateway	
WAN_DHCP		WAN	172.16.130.254	172.16.130.254	Interface WAN_DHCP Gateway	

Descendez pour accéder au bouton « Add » puis crée la passerelle suivante puis sauvegarder

Disabled	<input type="checkbox"/> Disable this gateway
Set this option to disable this gateway without removing it from the list.	
Interface	LAN
Choose which interface this gateway applies to.	
Address Family	IPv4
Choose the Internet Protocol this gateway uses.	
Name	BDD_ACCESS
Gateway name	
Gateway	10.0.0.253
Gateway IP address	
Gateway Monitoring	<input type="checkbox"/> Disable Gateway Monitoring
This will consider this gateway as always being up.	
Gateway Action	<input type="checkbox"/> Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.	

Après cela, allez dans « Static Routes » afin de créer la route statique expliquer précédemment, en appuyant sur « Add »



Nos paramètres de route sont donc :

Destination Network = 192.168.20.0 /24

Gateway = BDD_ACCESS

Votre pfSense1 est donc terminé en termes de configurations, mis à part si vous désirez y rajouter encore des paramètres, libre à vous.

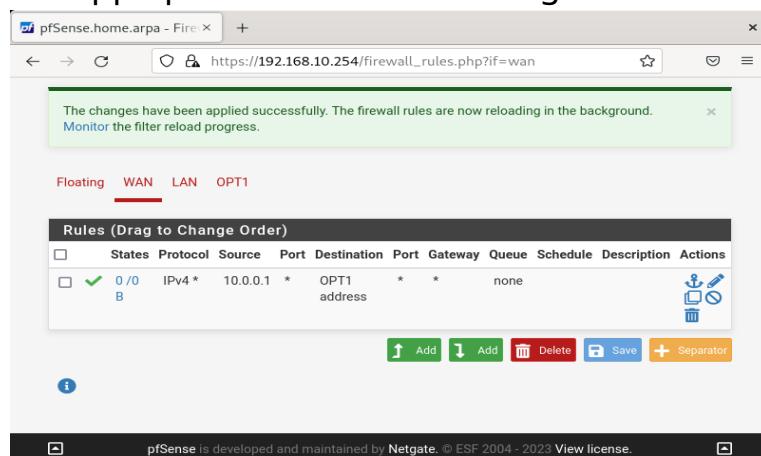
3.4.2 – Configuration poussée du PfSense 2

Par défaut, la passerelle du PfSense 2 gérant le LAN où se trouvera notre BDD n'a aucune règle permettant le passage de paquets nécessaires. Hors, les utilisateurs de notre infrastructure et le serveur Web doivent pouvoir y accéder, nous allons donc rajouter une règle.

Allez ensuite dans les règles du WAN puis rajouter une règle avec les paramètres suivants pour que le serveur Web puisse accéder à votre BDD suite au routage précédent :

```
Action = Pass  
Interface = WAN  
Address Family = IPv4  
Source = Single host or alias , <Adresse de votre serveur Web>  
Destination = OPT1 address
```

Sauvegarder et appliquer les nouveaux changements.



The screenshot shows a web browser window titled "pfSense.home.arpa - Firewall" with the URL "https://192.168.10.254/firewall_rules.php?if=wan". A green message bar at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, there is a navigation bar with tabs: Floating, WAN (selected), LAN, and OPT1. Under the WAN tab, there is a table titled "Rules (Drag to Change Order)". The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. One rule is listed: "0 /0 IPv4 * 10.0.0.1 * OPT1 * * none". At the bottom of the table are buttons for "Add", "Delete", "Save", and "Separator". The pfSense footer at the bottom of the page reads: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license."

3.5 – Installer les services sur les serveurs

Au total, nous avons donc dans notre infrastructure, un serveur web et un serveur mariadb.

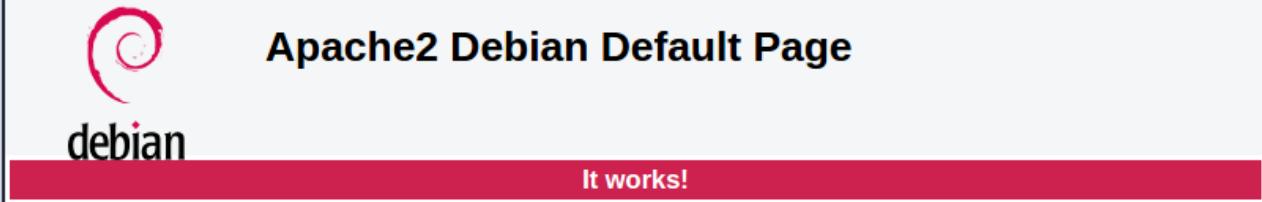
Je considère dans ce tuto que vous avez déjà des machines Linux prêtes à recevoir les différents services.

3.5.1 – Installation du serveur WEB

Sur votre machine de serveur Web, positionnez-vous dans le terminal puis faites la commande suivante

```
sudo apt install apache2
```

Si votre machine est correctement connectée à Internet l'installation devrait se lancer, une fois terminer, rentrez l'adresse IP de la machine dans son navigateur, vous permettant d'accéder à cette page.



The screenshot shows the Apache2 Debian Default Page. It features the Debian logo (a red spiral icon) and the word "debian" below it. The main title is "Apache2 Debian Default Page". A red banner at the top right contains the text "It works!". The page content explains that this is the default welcome page for testing the Apache server. It mentions that if the page is readable, the server is working properly. It advises replacing the index.html file before continuing. It also notes that if the site is unavailable, it might be due to maintenance and suggests contacting the administrator. A "Configuration Overview" section provides information about the configuration files used by Apache2 on Debian systems, mentioning the /etc/apache2 directory and its subfolders like apache2.conf, mods-enabled, conf-enabled, and sites-enabled, each containing various configuration files.

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

L'installation de votre serveur Web est terminé

Lorsque vous essaierez de vous connecter à cette machine pour sa page, n'oubliez pas de changer la passerelle de la machine extérieure à l'adresse de WAN du pfSense 1.

3.5.2 – Installation de la BDD

Sur votre machine BDD, allez sur votre terminal et rentrez la commande suivante :

```
Sudo apt install mariadb-server
```

L'installation devrait se lancer puis se terminer, pour vérifier la bonne installation, lancez la commande suivante

```
mysql_secure_installation
```

Si votre machine vous renvoie un message comme quoi, elle n'existe pas, l'installation est ratée, dans le cas contraire, vous avez terminé. (Nous n'allons pas chercher à configurer mariadb dans ce tuto, juste à s'assurer de sa bonne installation).

4 – Résolution de potentiels problèmes

Il se peut que lors de l'installation de l'infrastructure, différents problèmes peuvent survenir, voici donc une liste des premières choses à vérifier dans ces cas-là.

4.1 – Problème de communications entre machines

1, Essayer de ping la machine en question par son adresse IP (si c'est le serveur WEB, essayez de, vous y connectez par son adresse IP sur le navigateur)

2, Vérifier que le pfsense que vous essayez de contacter est bien allumé

3, Vérifier que les machines sont sur les bons réseaux internes (En cas de VM)

4, Vérifier les interfaces des machines (Est-ce qu'elles ont les bonnes adresses de passerelle à leurs pfsenses respectifs ?)

5, Vérifier les règles de pare-feu, il se peut que vos règles ne concernent soit pas les bons protocoles ou les bons réseaux, aussi, s'il n'y a aucune règle de passage, toutes les requêtes sont arrêtées

6, Vérifier s'il n'y a pas un conflit d'interfaces sur le Pfsense connecté de manière direct à votre machine

4.2 – Problème d'Internet sur les clients

1, Vérifier les problèmes évoqués précédemment

2, Mettez en DNS l'adresse 8.8.8.8

4.3 – Problème de connexion à la page web des Pfsenses

1, Vérifier les problèmes évoqués précédemment

2, Redémarrer le configIBUTEUR web avec l'option 11 sur le pfsense en question

3, Réinitialiser le mot de passe du configIBUTEUR web (remets le mot de passe à « Pfsense »)

4.4 – Aucune des vérifications n'apportent de résultat

1, Refaites les règles des pfSense, les règles initiales des LAN de pfSense ont parfois tendance à ne pas fonctionner correctement pour aucune raison apparente.

2, Changez vos noms de réseaux internes, les noms en majuscule ont l'air de ne pas fonctionner correctement parfois.

3, Réinstaller la machine défectueuse.

5 - Annexes

Fiche de recette

Vérification de l'opérationnalité de la solution mise en œuvre : Titre

Description du test :

1. Test d'accès du client au serveur base de données
2. Test d'accès du client au serveur Web
3. Test d'Accès du client à internet
4. Test d'accès du serveur Web au serveur base de données
5. Test d'accès du serveur Web à internet
6. Test de communication du serveur Web avec le client
7. Test d'accès du serveur base de données vers internet
8. Test d'accès du serveur base de données vers au client
9. Test de fonctionnement du reverse proxy

Résultats Attendus :

1. Le client peut accéder au serveur base de données
2. Le client peut accéder au serveur Web
3. Le client peut accéder à internet
4. Le serveur Web peut accéder au serveur base de données
5. Le serveur Web peut accéder à internet
6. Le serveur Web ne peut pas communiquer vers le client
7. Le serveur base de données ne peut pas accéder à internet
8. Le serveur base de données ne peut pas accéder au client
9. Le reverse proxy renvoie sur le serveur Web

Réception Globale : DMZ Timothée Lignière, Paul-Alexis Kappala, Masseï Liam	Date: 11/04/2023 Auteurs:
Reçu : <input type="checkbox"/>	
Reçu avec réserve : <input type="checkbox"/>
Refusé : <input type="checkbox"/>
Commentaire :	

Recette étape par étape *	* (pour chaque étape, vous devez élaborer dans un fichier distinct un scénario détaillé à faire appliquer au « client » venant valider votre solution)
----------------------------------	--

Réception Etape 1: Accès par MySQLsh du client vers le serveur base de données	
Reçu : <input type="checkbox"/>	
Reçu avec réserve : <input type="checkbox"/>
Refusé : <input type="checkbox"/>
Commentaire :	

Réception Etape 2 : Le client peut ouvrir la page Web du serveur Web en y accédant par explorateur web en 10.0.0.100	
Reçu : <input type="checkbox"/>	
Reçu avec réserve : <input type="checkbox"/>
Refusé : <input type="checkbox"/>
Commentaire :	

Réception Etape 3 : Ouverture de plusieurs page Web par le clientReçu : Reçu avec réserve : Refusé :

Commentaire :

Réception Etape 4 : Accès via MySQLsh du serveur Web vers le serveur base de donnéesReçu : Reçu avec réserve : Refusé :

Commentaire :

Réception Etape 5 : Ping vers 8.8.8.8 depuis le serveur WebReçu : Reçu avec réserve : Refusé :

Commentaire :

Réception Etape 6 : Ping du serveur Web vers le ClientReçu : Reçu avec réserve : Refusé :

Commentaire :

Réception Etape 7 : Ping vers 8.8.8.8 depuis le serveur base de donnéesReçu : Reçu avec réserve : Refusé :

Commentaire :

Réception Etape 8 : Ping vers le client depuis le serveur base de donnéesReçu : Reçu avec réserve : Refusé :

Commentaire :

Réception Etape 9 : Connexion par IP avec un explorateur depuis une machine exterieur	
Reçu :	<input type="checkbox"/>
Reçu avec réserve :	<input type="checkbox"/>
Refusé :	<input type="checkbox"/>
Commentaire :	