

## Procédure : Configuration IP interfaces & configuration de routes sur PFSENSE



## **Présentation PFSENSE :**

PFSENSE est un routeur / pare-feu basé sur le système d'exploitation FreeBSD. Il permet de configurer des fonctions de routage, pare-feu et NAT lui permettant d'interconnecter des réseaux.

PFSENSE offre une solution libre & gratuite permettant de remplacer les routeurs professionnels propriétaires.

## **Intérêts pour la M2L :**

- Rendre accessible depuis l'extérieur les deux serveurs WEB présents dans la DMZ (reverse proxy)
- Assurer un périmètre de sécurité avec l'Internet au travers d'une interconnexion entre le réseau interne, la DMZ et Internet grâce aux règles de contrôle d'accès.

## **Dans notre situation :**

On souhaite configurer PFSENSE de la façon suivante :

- L'interface WAN adressé en 172.16.1.209 /24
- L'interface LAN adressé en 10.10.20.2 29
- La route par défaut menant à l'adresse 172.16.1.254
- La route permettant de joindre le réseau 172.16.2.224 /27
- Configurer le NAT pour le réseau 172.16.2.224

## I - Adressage d'une interface

Pour adresser une interface :

Dans le menu de PFSENSE, il faut taper **2** qui est associé à « **Set interface(s) IP address** » :

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to 172.16.1.209/24
Press <ENTER> to continue.
pfSense - Netgate Device ID: e6b95f428338ab4085bf

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> re1      -> v4: 172.16.1.209/24
LAN (lan)      -> re2      -> v4: 192.168.1.1/24

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: 2
```

Choisir le **numéro de l'interface** sur laquelle modifier l'adressage IP :

- Taper **1** pour modifier l'adresse IP de l'interface WAN
- Taper **2** pour modifier l'adresse IP de l'interface LAN

```
DHCPD...

The IPv4 WAN address has been set to 172.16.1.209/24
Press <ENTER> to continue.
pfSense - Netgate Device ID: e6b95f428338ab4085bf

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> re1      -> v4: 172.16.1.209/24
LAN (lan)      -> re2      -> v4: 192.168.1.1/24

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: 2

Available interfaces:
1 - WAN (re1 - static)
2 - LAN (re2 - static)

Enter the number of the interface you wish to configure: 1
```

Après il faut entrer l'**adresse IP** que l'on souhaite attribuer :

```

Press <ENTER> to continue.
pfSense - Netgate Device ID: e6b95f428338ab4085bf

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> re1          -> v4: 172.16.1.209/24
LAN (lan)      -> re2          -> v4: 192.168.1.1/24

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: 2

Available interfaces:

1 - WAN (re1 - static)
2 - LAN (re2 - static)

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.20.2

```

Pour configurer le masque il faut mettre **le nombre de sa notation CIDR** :

```

Enter an option: 2

Available interfaces:

1 - WAN (re1 - static)
2 - LAN (re2 - static)

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.20.2

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 31):
> 29

```

Si on configure une adresse WAN, il faut indiquer la passerelle sinon pour une adresse LAN il ne faut rien mettre :

```

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

```

## II - Crédation des routes

Pour créer une route, il faut d'abord entrer la touche 8 sur le menu PFSENSE :

```

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 10.10.20.2/29
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.10.20.2/

Press <ENTER> to continue.
pfSense - Netgate Device ID: e6b95f428338ab4085bf

*** Welcome to pfSense 2.4.4-RELEASE-p8 (amd64) on pfSense ***

WAN (wan)      -> re1      -> v4: 172.16.1.209/24
LAN (lan)      -> re2      -> v4: 10.10.20.2/29

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 en option: 8

```

Puis pour ajouter la route il faut taper la commande : « route add -net + le réseau de destination + /son cidr + l'adresse IP du routeur de prochain pas pour joindre ce réseau » :

```
[2.4.4-RELEASE][root@pfSense .localdomain]/root: route add -net 172.16.2.224/27 1
0.10.20.1
add net 172.16.2.224: gateway 10.10.20.1
[2.4.4-RELEASE][root@pfSense .localdomain]/root: ]
```

On peut vérifier si la route s'est bien ajoutée en affichant la table de routage à l'aide de la commande : « netstat -nr » :

```
add net 172.16.2.224/27 10.10.20.1
[2.4.4-RELEASE][root@pfSense .localdomain]/root: netstat -nr
[2.4.4-RELEASE][root@pfSense .localdomain]/root: Routing tables

Internet:
Destination     Gateway         Flags     Netif  Expire
default         172.16.1.254    UGS      re0
10.10.20.0/29   link#3        U        re2
10.10.20.2       link#3        UHS     lo0
127.0.0.1        link#5        UH      lo0
172.16.1.0/24   link#1        U       re0
172.16.1.209    link#1        UHS     lo0
172.16.2.224/27 10.10.20.1    UGS      re2

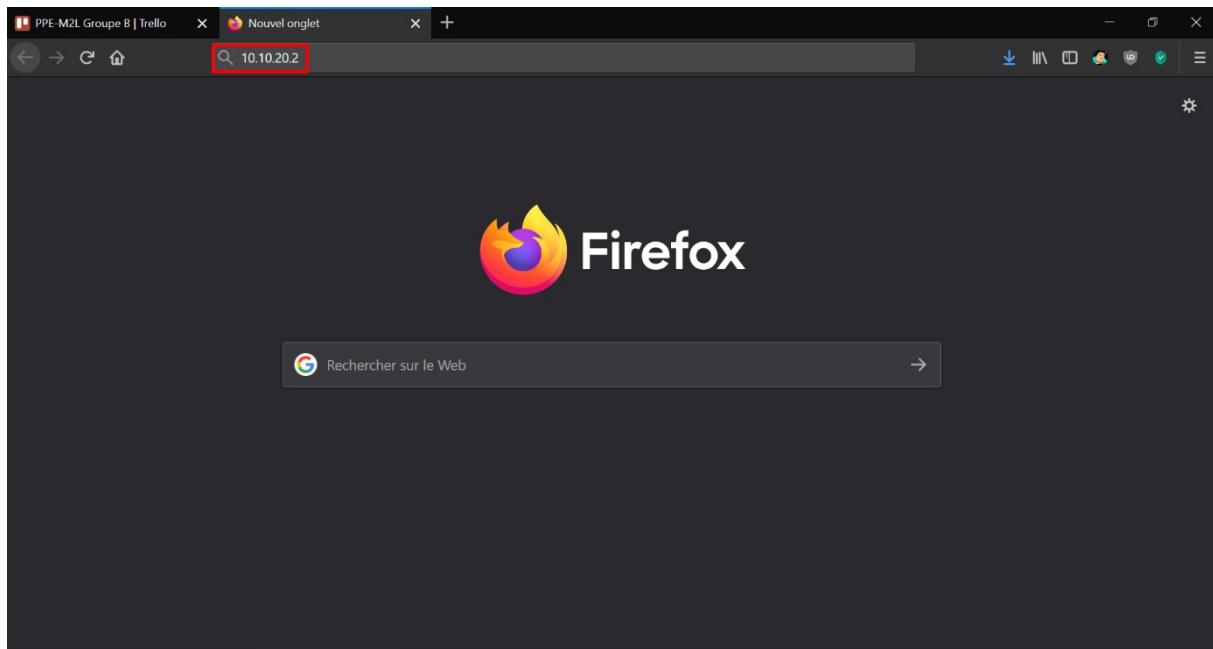
Internet6:
Destination           Gateway           Flags     Net
Expire
::1                  link#5            UH      1
fe80::%re0/64        link#1            U       r
fe80::960c:6dff:fe84:48da%re0  link#1            UHS     1
fe80::%re1/64        link#2            U       r
fe80::960c:6dff:fe84:5827%re1  link#2            UHS     1
fe80::%re2/64        link#3            U       r
fe80::1:1%re2        link#3            UHS     1
fe80::%lo0/64        link#5            U       r
fe80::1%lo0          link#5            UHS     1
[2.4.4-RELEASE][root@pfSense .localdomain]/root: ]
```

### III - Configuration du NAT

Nous devons configurer le NAT pour le réseau 172.16.2.224 /27 pour permettre aux postes de ce réseau la communication avec Internet.

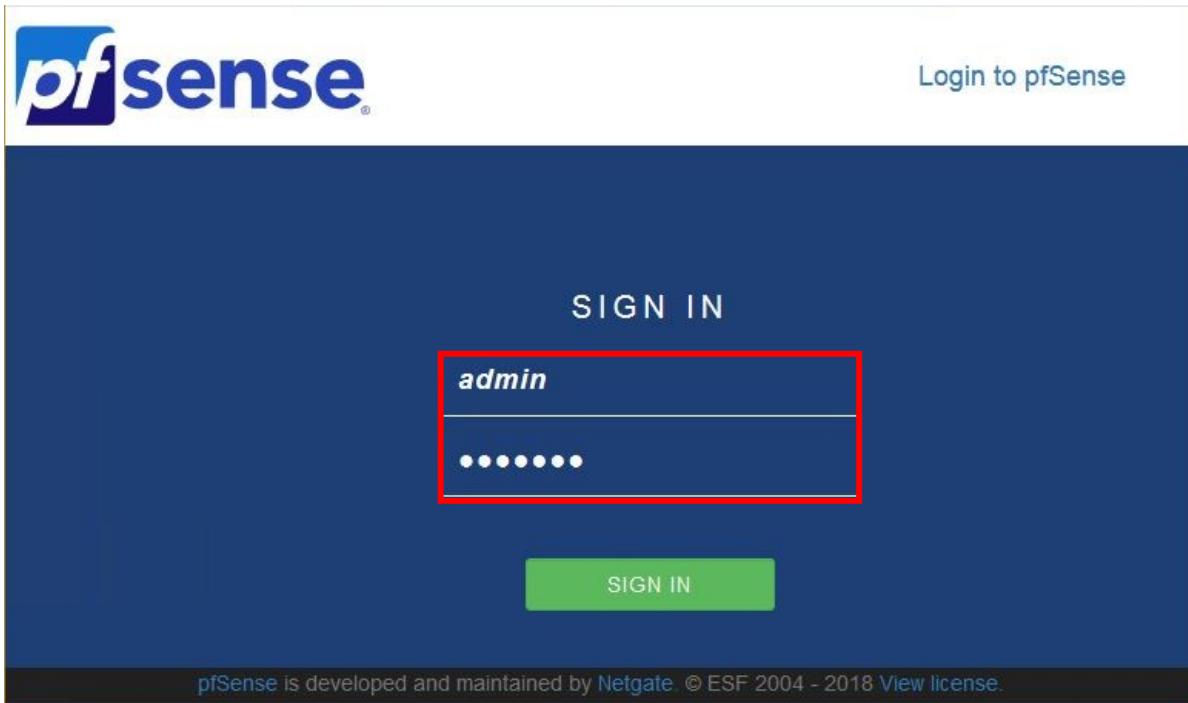
Pour accéder à la configuration du NAT il faut accéder à **l'interface web de configuration du PFSENSE**.

Pour cela il faut taper l'adresse IP de l'interface LAN du PFSENSE dans le navigateur web :



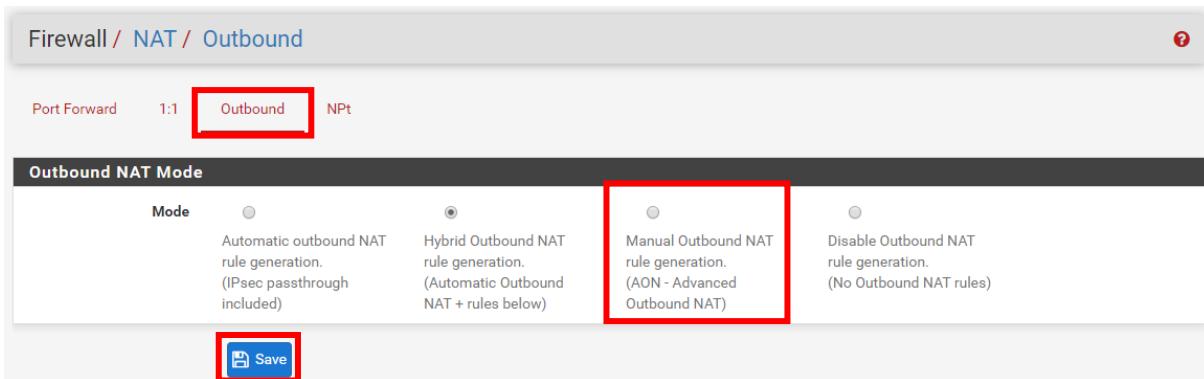
Dans l'interface web de connexion au PFSENSE il faut entrer :

- Nom d'utilisateur : **admin**
- Mot de passe : **PFSENSE**



Une fois dans l'interface, il faut aller dans **Firewall > Nat** :

On souhaite configurer le NAT sur les paquets partants du réseau 172.16.2.224, pour cela il faut cliquer sur « **Outbound** », cliquer sur « **Manual Outbound NAT** » afin de configurer le NAT manuellement et cliquer sur « **Save** » :



Pour ajouter une règle NAT, il faut cliquer sur « **Add** » :

Mappings										
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	WAN	172.16.2.224/27	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	WAN	172.16.2.224/27	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	
<input type="checkbox"/>	WAN	127.0.0.0/8	*	*	*	WAN address	*		Auto created rule - localhost to WAN	
<input type="checkbox"/>	WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	
<input type="checkbox"/>	WAN	::1/128	*	*	*	WAN address	*		Auto created rule - localhost to WAN	
<input type="checkbox"/>	WAN	10.10.20.0/29	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - LAN to WAN	
<input type="checkbox"/>	WAN	10.10.20.0/29	*	*	*	WAN address	*		Auto created rule - LAN to WAN	

Add Add Delete Save

Pour configurer une règle NAT :

Ne pas cocher « **Disabled** » car cela désactiverait la règle et ne pas cocher également « **Do not NAT** » à part si vous souhaitez ajouter une règle pour interdire le NAT :

**Disabled**  Disable this rule

**Do not NAT**  Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules  
In most cases this option is not required.

Dans « **interface** » il faut mettre « **WAN** » car on souhaite configurer la translation d'adresse pour les paquets qui vont vers le WAN :

**Interface** **WAN**

The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Dans « **Address Family** » il faut choisir le protocole IP qui sera utilisé (IPv4, IPv6), dans notre cas c'est « **IPv4** » :

**Address Family** **IPv4**

Select the Internet Protocol version this rule applies to.

Dans « **Protocol** » il faut choisir le protocole pour lequel la règle NAT s'applique, on peut sélectionner « **any** » pour accepter tous les protocoles :

**Protocol** **any**

Choose which protocol this rule should match. In most cases "any" is specified.

Dans « Source » :

- « Type » : « Network »
- « Source network for the outbound NAT mapping » : l'adresse du réseau source + sélectionner le CIDR (dans notre cas 172.16.2.224 /27)

Source

Type

172.16.2.224 / 24

Source network for the outbound NAT mapping.

Port or Range

Dans « Destination » :

- « Type » : « any »

Destination

Type

/ 24

Destination network for the outbound NAT mapping.

Port or Range

Ne pas cocher « Not » :

Not  
Invert the sense of the destination match.

Dans « Address », sélectionner « Interface Address », cela va permettre d'indiquer qu'il faut translater d'adresse sur celle du WAN :

Address

Interface Address

Connections matching this rule will be mapped to the specified Address.  
The Address can be an Interface, a Host-type Alias, or a Virtual IP address.

Dans « Port Range », cocher « Static Port » :

Port or Range

Enter the external source Port or Range used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by ":".  
Leave blank when Static Port is checked.

Static Port

Ne pas cocher « No XMLRPC Sync » :

No XMLRPC Sync

Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

Facultatif : Entrer une description de la règle

Puis cliquer sur « Save » et « Apply Changes » :

A screenshot of the pfSense web interface. The top navigation bar shows 'pfSense COMMUNITY EDITION'. Below it, a warning message in a red box says: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The main title is 'Firewall / NAT / Outbound'. A message box at the bottom left says: 'The NAT configuration has been changed. The changes must be applied for them to take effect.' A green 'Apply Changes' button with a checkmark is on the right. A red box highlights the blue 'Save' button in the top right corner of the configuration area.

## IV - Configuration des règles du pare-feu

Nous devons autoriser les paquets en provenance et en direction du réseau 172.16.2.224 /27.

Toujours dans l'interface web, il faut aller dans **Firewall > Rules** :

A screenshot of the pfSense web interface. The top navigation bar shows 'pfSense COMMUNITY EDITION'. The 'Firewall' menu is open, and 'Rules' is highlighted with a red box. The main title is 'Firewall / NAT / Port Forward'. Below it, there are tabs for 'Port Forward', '1:1', 'Outbound', and 'NPt'. The 'Outbound' tab is selected. The main table header includes columns for 'Interface', 'Protocol', 'Source Address', 'Source Ports', 'Dest. Address', 'Dest. Ports', 'NAT IP', 'NAT Ports', 'Description', and 'Actions'. A red box highlights the 'Rules' tab in the table header.

Pour configurer les règles des paquets qui transiteront vers le WAN, il faut cliquer sur « **WAN** » puis pour ajouter une règle il faut cliquer sur « **Add** » :

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. The 'WAN' tab is selected. A red box highlights the 'Add' button in the bottom right corner of the rule list table.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<b>0 / 0 B</b>	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<b>0 / 0 B</b>	IPv4 *	WAN net	*	*	*	*	none			
<b>0 / 0 B</b>	IPv4 *	*	*	WAN net	*	*	none			
<b>0 / 234 B</b>	IPv4 *	*	*	*	*	*	none			

Pour configurer les règles des paquets qui transiteront vers le LAN, il faut cliquer sur « LAN » puis pour ajouter une règle il faut cliquer sur « Add » :

The screenshot shows the pfSense Firewall Rules configuration page for the LAN interface. The 'LAN' tab is selected. A red box highlights the 'Add' button in the bottom right corner of the rule list table.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<b>0 / 2.38 MiB</b>	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
<b>0 / 0 B</b>	IPv4 ICMP <u>echorep</u>	WAN net	*	*	*	*	none			
<b>0 / 0 B</b>	IPv4 *	WAN net	*	*	*	*	none			
<b>50 / 1.29 MiB</b>	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule	
<b>0 / 0 B</b>	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Exemple de configuration d'une règle de pare-feu vers le LAN :

Dans « Action » choisir « Pass » pour autoriser les paquets, « Reject » ou « Block » pour bloquer les paquets :

The screenshot shows a dropdown menu for the 'Action' field. The option 'Pass' is highlighted with a red box. Below the menu, a tooltip provides information about the differences between 'Block' and 'Reject' actions.

Action: **Pass**

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Dans « **Disable** », ne pas cocher « **Disable this rule** » :

Disabled  Disable this rule  
Set this option to disable this rule without removing it from the list.

Dans « **Interface** » mettre « **WAN** » pour filtrer les paquets venant du WAN vers le LAN :

Interface **WAN**  
Choose the interface from which packets must come to match this rule.

Dans « **Address Family** », choisir le protocole IP (IPv4, IPv6) sur lequel la règle s'applique :

Address Family **IPv4**  
Select the Internet Protocol version this rule applies to.

Dans « **Protocol** », choisir le protocole sur lequel la règle s'applique. Choisir « **any** » pour sélectionner tous les protocoles :

Protocol **Any**  
Choose which IP protocol this rule should match.

Dans « **Source** » :

- Ne pas cocher « **Invert Match** »
- Sélectionner « **WAN net** »

Source  Invert match **WAN net** Source Address /

Dans « **Destination** » :

- Ne pas cocher « **Invert Match** »
- Sélectionner « **any** »

Destination  Invert match **any** Destination Address /

Dans « **Log** », ne pas cocher « **Log packets that are handled by this rule** » :

Log  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Facultatif : insérer une description pour la règle

Pour finir cliquer sur « Save » puis « Apply Changes » :

The screenshot shows the pfSense configuration interface. At the top, there is a 'Description' field with a note: 'A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.' Below it is an 'Advanced Options' section with a 'Display Advanced' button. In the center, there is a large blue 'Save' button. At the bottom, there is a message box with a red background containing the text: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the navigation bar shows 'Firewall / Rules / WAN'. A yellow message box at the bottom states: 'The firewall rule configuration has been changed. The changes must be applied for them to take effect.' To the right of this message is a green 'Apply Changes' button with a checkmark icon.

## V - Haute Disponibilité

La haute disponibilité permet au routeur PfSense de rediriger les requêtes http/https vers un ou plusieurs serveurs.

Cela permet d'éviter une surcharge d'un serveur Web ou d'éviter une indisponibilité en cas de panne d'un des serveurs Web.

Pour configurer la haute disponibilité il faut se rendre dans « Load Balancer » :

The screenshot shows the pfSense dashboard. At the top, there is a 'Status / Dashboard' section with a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this is a 'System Information' table. In the 'Services' menu on the left, the 'Load Balancer' option is highlighted with a red box. To the right, there is a 'Netgate Services And Support' section with a 'Community Support' contract type. At the bottom, there is a 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' section with links to upgrade support, community resources, and global support FAQ.

On va commencer par ajouter le pool de serveurs qui contiendra nos 2 serveurs Web :

- Dans « **Mode** » : Mettre « **Load Balancer** »
- Dans « **Port** » : mettre le port de destination des requêtes au serveur, dans notre cas ce sera 80 et 443 puisqu'il s'agit de serveurs Web
- Dans « **Retry** » : Mettre le nombre de requêtes sans réponses après lequel le serveur sera considéré comme indisponible
- Dans « **Monitor** » : Mettre le protocole concerné
- Puis ajouter les adresses IP des serveurs concernés par la haute disponibilité

Members	Disabled	Enabled (Default)

**Add/Edit Load Balancer - Pool Entry**

Name	serveur_webHTTPS
Mode	Load Balance
Description	
Port	443
This is the port the servers are listening on. A port alias listed in Firewall -> Aliases may also be specified here.	
Retry	3
Optionally specify how many times to retry checking a server before declaring it down.	

**Add Item to the Pool**

Monitor	HTTPS
Server IP Address	IP Address
<b>+ Add to pool</b>	

**Current Pool Members**

Members	
192.168.0.3	Enabled (Default)
192.168.0.2	Disabled

**Actions:**

- Remove**
- Move to enabled list**
- Move to disabled list**

Ensuite il faut se rendre sur « Virtual Servers » :

**WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.**

Services / Load Balancer / Virtual Servers

Pools **Virtual Servers** Monitors Settings

**Virtual Servers**

Name	Protocol	IP Address	Port	Pool	Fallback pool	Description	Actions
No virtual servers have been configured.							

**Add**

- Dans « **IP Address** » : Mettre l'adresse IP d'une des interfaces de Pfsense qui écoutera les requêtes pour la haute disponibilité.

Note : Plusieurs interfaces de Pfsense peuvent écouter pour la haute disponibilité, on peut imaginer que l'on souhaite que Pfsense redirige les requêtes http/https pour les requêtes provenant du WAN comme du LAN.

- Dans « **Port** » : Le port de destination du serveur concerné par la haute disponibilité
- Dans « **Relay Protocol** » : Le protocole de transport utilisé

Exemple de configuration pour les requêtes http/https provenant du WAN (172.16.1.209 étant l'adresse de l'interface WAN de notre Pfsense) :

Services / Load Balancer / Virtual Servers / Edit

Edit Load Balancer - Virtual Server Entry

Name	serveur_web_wan
Description	
IP Address	172.16.1.209
This is normally the WAN IP address for the server to listen on. All connections to this IP and port will be forwarded to the pool cluster. A host alias listed in Firewall -> Aliases may also be specified here.	
Port	80
Port that the clients will connect to. All connections to this port will be forwarded to the pool cluster. If left blank listening ports from the pool will be used. A port alias listed in Firewall -> Aliases may also be specified here.	
Virtual Server Pool	serveurs_web
Fall-back Pool	None
Relay Protocol	TCP

Save

Don't forget to add a firewall rule for the virtual server/pool after finished setting it up.

Services / Load Balancer / Virtual Servers / Edit

Edit Load Balancer - Virtual Server Entry

Name	serveurs_web_wan
Description	
IP Address	172.16.1.209
This is normally the WAN IP address for the server to listen on. All connections to this IP and port will be forwarded to the pool cluster. A host alias listed in Firewall -> Aliases may also be specified here.	
Port	443
Port that the clients will connect to. All connections to this port will be forwarded to the pool cluster. If left blank listening ports from the pool will be used. A port alias listed in Firewall -> Aliases may also be specified here.	
Virtual Server Pool	serveur_webHTTPS
Fall-back Pool	None
Relay Protocol	TCP

Save

Don't forget to add a firewall rule for the virtual server/pool after finished setting it up.

Exemple de configuration pour les requêtes http/https provenant du LAN (10.10.20.2 étant l'adresse de l'interface LAN du PfSense) :

Services / Load Balancer / Virtual Servers / Edit

**Edit Load Balancer - Virtual Server Entry**

Name	serveur_web_lan
Description	
IP Address	10.10.20.2
This is normally the WAN IP address for the server to listen on. All connections to this IP and port will be forwarded to the pool cluster. A host alias listed in Firewall -> Aliases may also be specified here.	
Port	80
Port that the clients will connect to. All connections to this port will be forwarded to the pool cluster. If left blank listening ports from the pool will be used. A port alias listed in Firewall -> Aliases may also be specified here.	
Virtual Server Pool	serveurs_web
Fall-back Pool	None
Relay Protocol	TCP
<b>Save</b>	

Don't forget to add a firewall rule for the virtual server/pool after finished setting it up.

**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Load Balancer / Virtual Servers / Edit

**Edit Load Balancer - Virtual Server Entry**

Name	https_web_lan
Description	
IP Address	10.10.20.2
This is normally the WAN IP address for the server to listen on. All connections to this IP and port will be forwarded to the pool cluster. A host alias listed in Firewall -> Aliases may also be specified here.	
Port	443
Port that the clients will connect to. All connections to this port will be forwarded to the pool cluster. If left blank listening ports from the pool will be used. A port alias listed in Firewall -> Aliases may also be specified here.	
Virtual Server Pool	serveur_webHTTPS
Fall-back Pool	None
Relay Protocol	TCP
<b>Save</b>	

On modifie ensuite notre serveur DNS afin que les noms de domaines de nos différentes pages Web pointent sur l'adresse IP du Pfsense, puisque c'est lui désormais qui décide sur quel serveur Web la requête http/https va aller :

