

Installation d'un routeur avec pfSense

PfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise un pare-feu, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il s'administre à distance depuis une interface web ce qui rend la prise en main plus agréable.

Dans ce tutoriel, nous allons voir comment installer le routeur et le configurer (NAT, relais DHCP, redirection de port). Le routeur ainsi que les sous-réseaux sont virtuels et il y a 5 interfaces dont l'interface « Pédagogique » qui sert d'interface WAN.

Configuration requise :

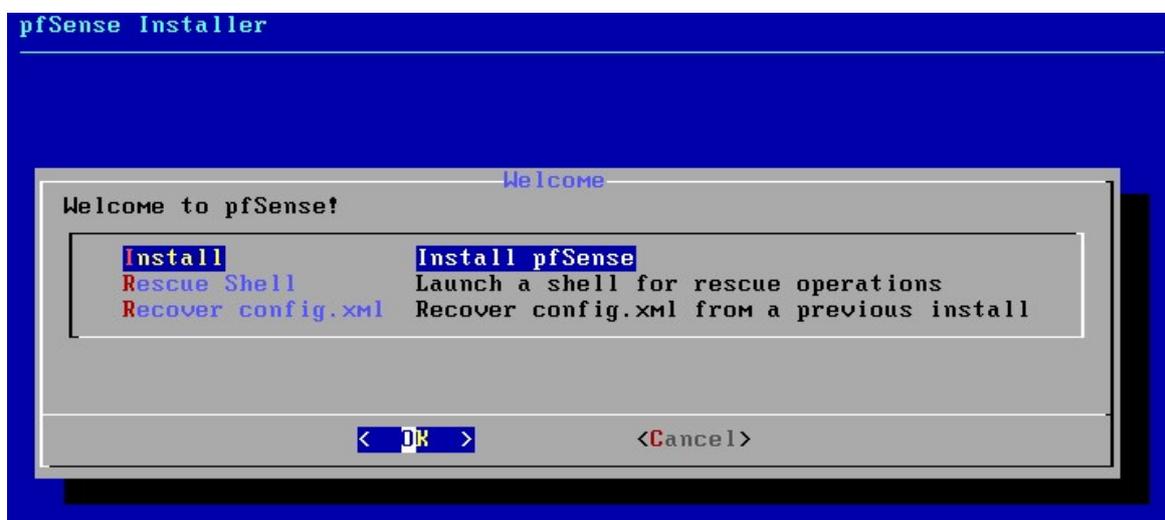
	Minimale	Recommandée
Processeur	500 MHz	1 GHz
Mémoire vive	256 Mo	1 Go
Stockage	> 1 Go	

Tout d'abord, il faut créer une nouvelle machine virtuelle avec :

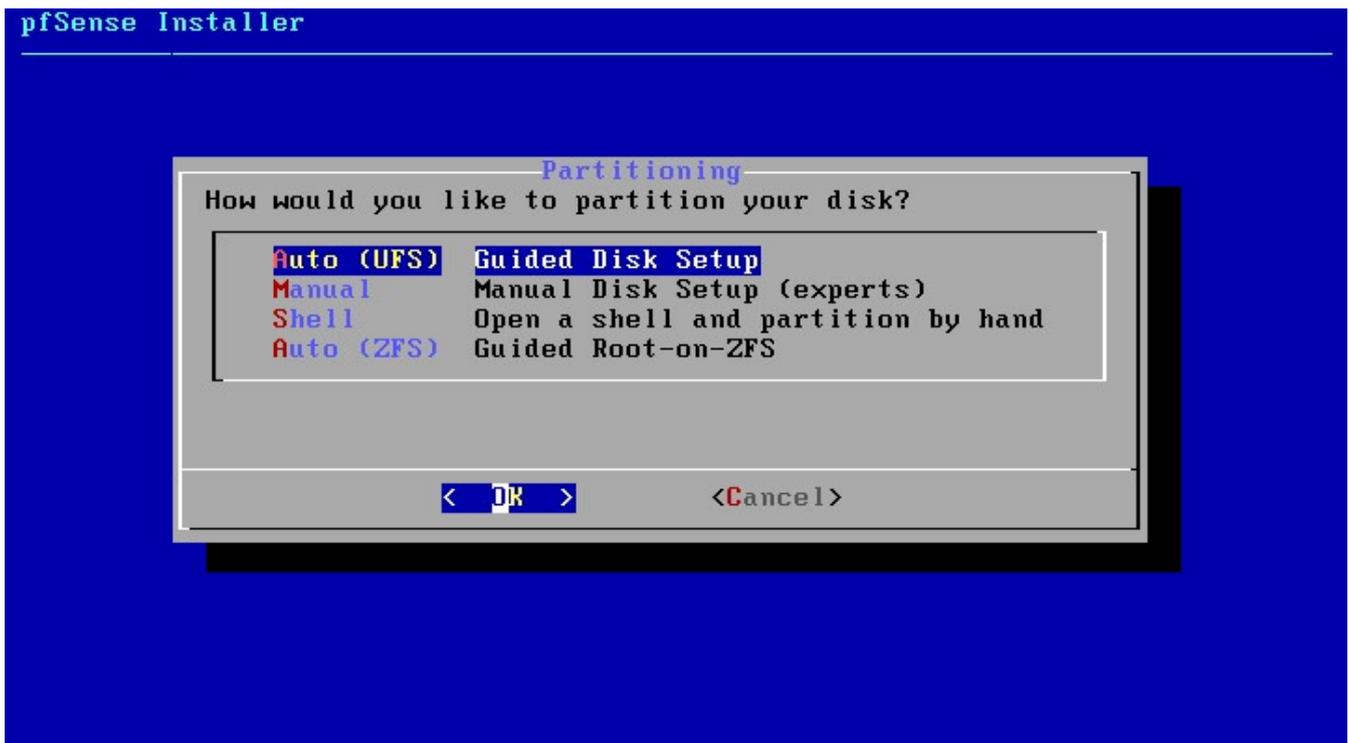
- l'image ISO de pfSense téléchargeable depuis le [site officiel](#)
- au moins 2 cartes réseau
- 1 Go de RAM
- 8 Go d'espace de stockage

Installation :

Démarrer la machine et l'installation va commencer :



Choisir le partitionnement du disque automatique :



On peut maintenant redémarrer le système :



On peut maintenant assigner les interfaces de notre machine virtuelle aux interfaces du routeur en tapant "1":

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE amd64 Thu Sep 20 09:03:12 EDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 2cdc19884432240deef2

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

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      ->

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: █
```

Voulez vous configurer des interfaces VLAN ? Non, nous n'avons pas besoin de VLAN :

```
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: 1

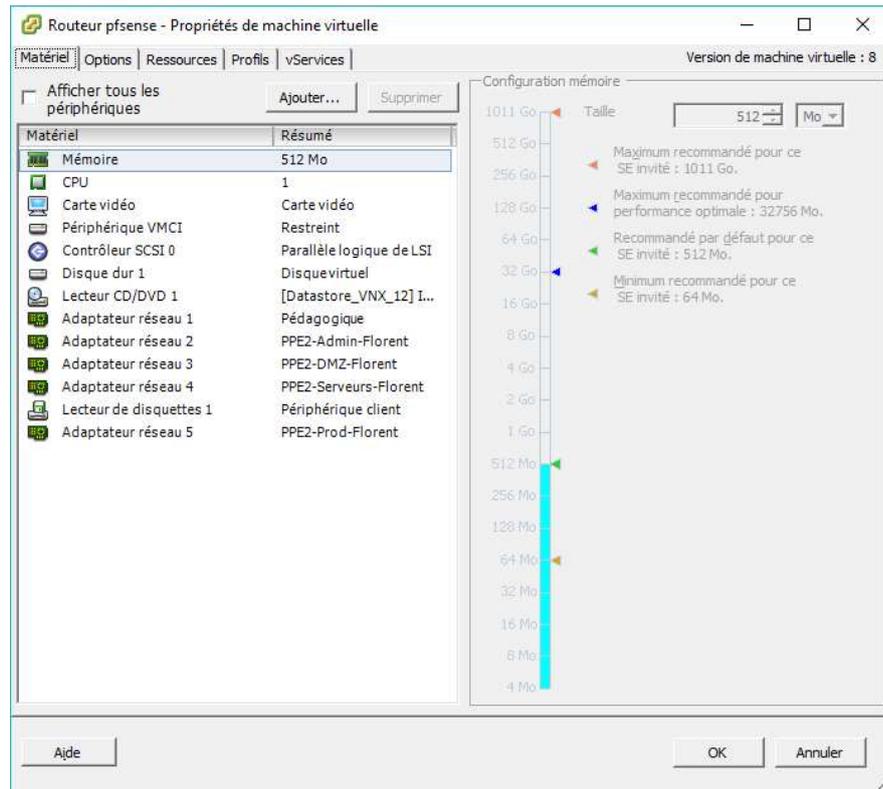
Valid interfaces are:

em0      00:0c:29:a2:5a:b1   (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1      00:0c:29:a2:5a:d9   (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em2      00:0c:29:a2:5a:c5 (down) Intel(R) PRO/1000 Legacy Network Connection 1.
em3      00:0c:29:a2:5a:cf (down) Intel(R) PRO/1000 Legacy Network Connection 1.
em4      00:0c:29:a2:5a:bb (down) Intel(R) PRO/1000 Legacy Network Connection 1.

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█
```

Entrer le nom des interfaces correspondant au WAN, au LAN et les interfaces restantes aux options en fonction des réseaux attribués dans les paramètres de la machine virtuelle, puis valider :



```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 a or nothing if finished): em4

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4

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

Appuyer ensuite sur "2" pour configurer les adresses IP sur chaque interfaces, puis sur "1" pour choisir l'interface WAN :

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)

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

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.16.20.108

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 WAN IPv4 subnet bit count (1 to 31):
> 17

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.16.127.254

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 WAN address has been set to 172.16.20.108/17

Press <ENTER> to continue. █
```

Recommencer ensuite pour chaque interfaces pour obtenir ceci :

```
The IPv4 OPT3 address has been set to 10.0.0.30/27

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 49b344910cd909f2f6b0

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

WAN (wan)      -> em0      -> v4: 172.16.20.108/17
LAN (lan)      -> em1      -> v4: 10.0.0.62/27
OPT1 (opt1)    -> em2      -> v4: 10.0.0.94/28
OPT2 (opt2)    -> em3      -> v4: 10.0.0.78/28
OPT3 (opt3)    -> em4      -> v4: 10.0.0.30/27

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

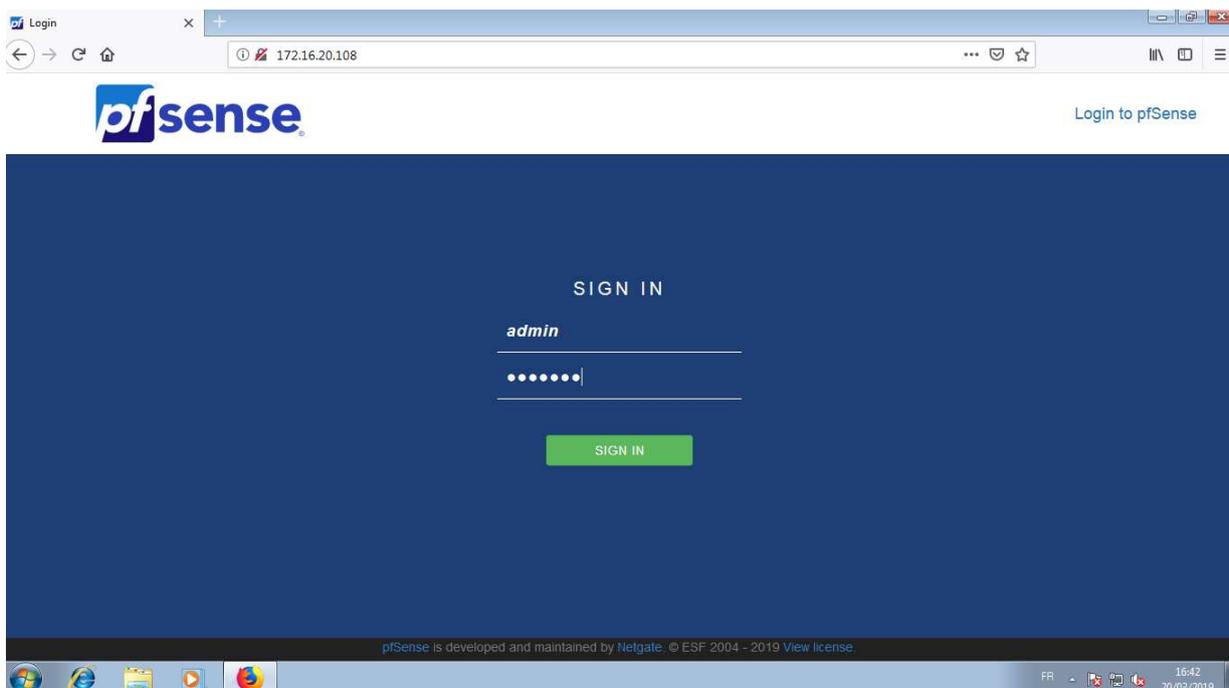
Enter an option: █
```

Vous pouvez ensuite redémarrer le routeur ("5"), pour être sur que tout les paramètres indiqués soient bien pris en compte.

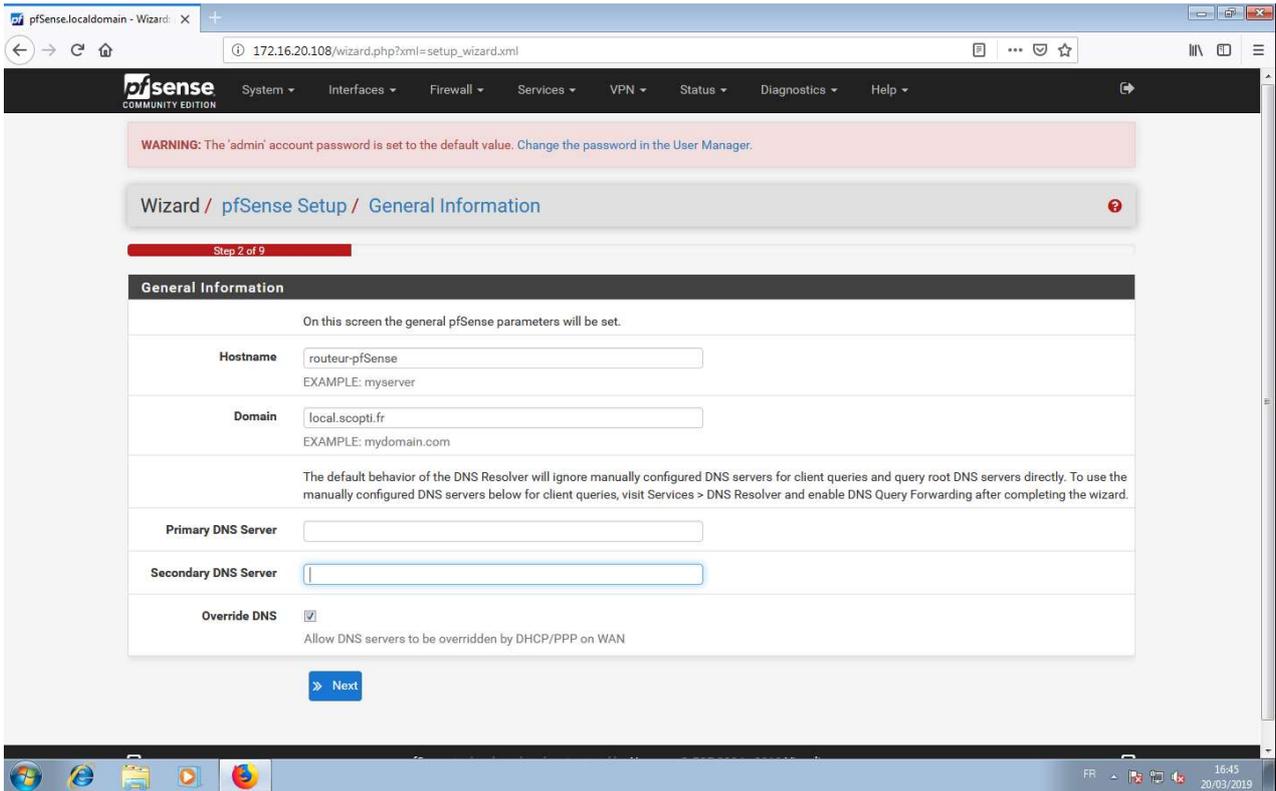
Configuration avec l'interface Web :

Il faut maintenant à partir d'un sous réseau crée précédemment (Admin, DMZ, Serveur, Prod) créer une nouvelle machine virtuelle possédant une interface graphique. Dans votre navigateur web préféré, entrer l'adresse ip correspondant à l'interface WAN pour arriver sur la page de configuration.

Par défaut : login – admin mot de passe – pfsense

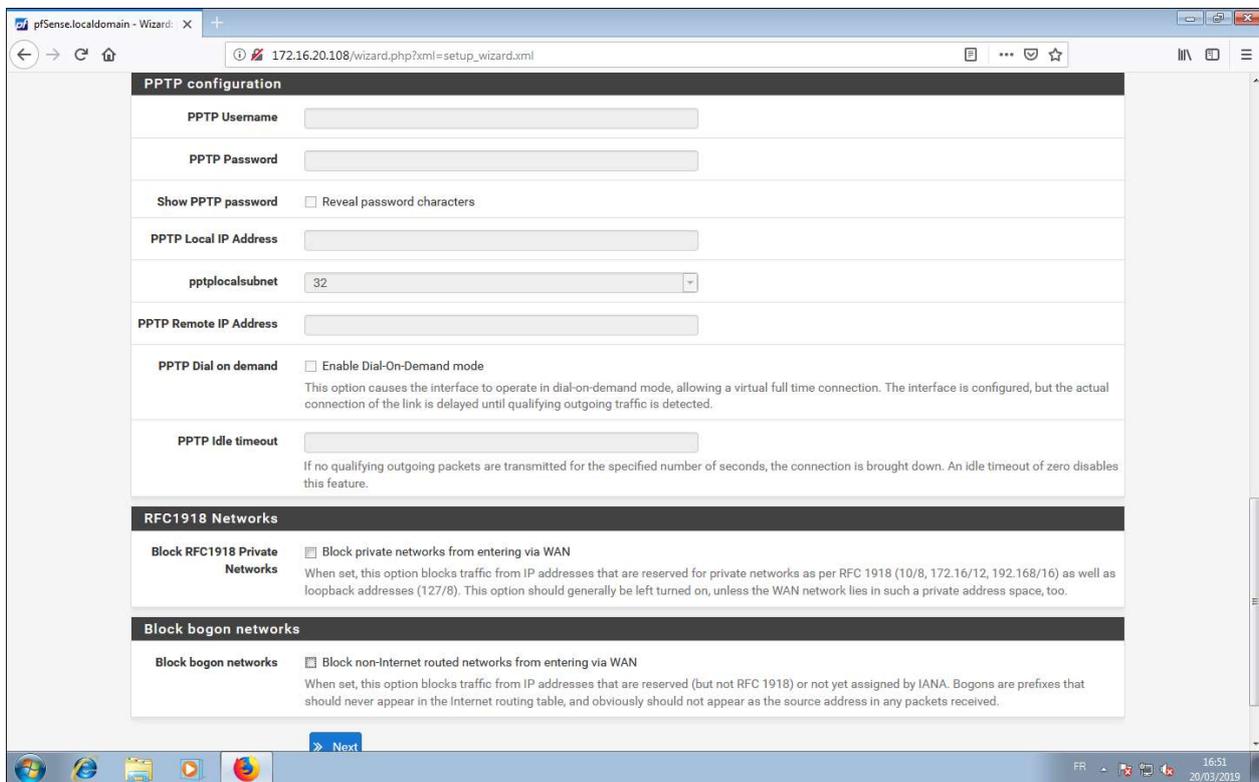


Entrer le nom du routeur ainsi que le nom de domaine. On peut aussi renseigner les adresses des serveurs DNS si vous en avez. (Possible de le faire plus tard)



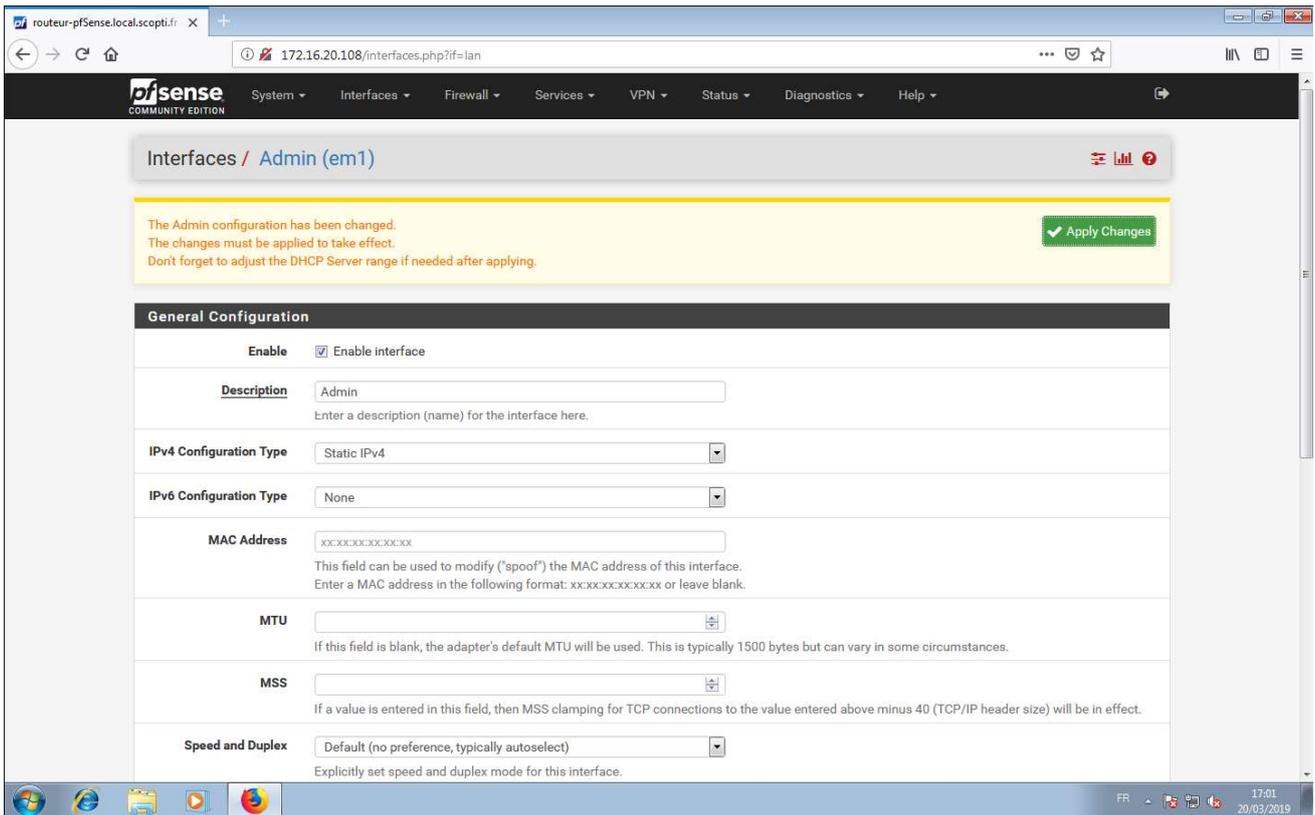
On peut ensuite configurer l'interface WAN. (qui est déjà fait normalement)

Tout en bas, il faut décocher les 2 cases si vous voulez que les adresses IP privée puissent se connecter par l'interface WAN :

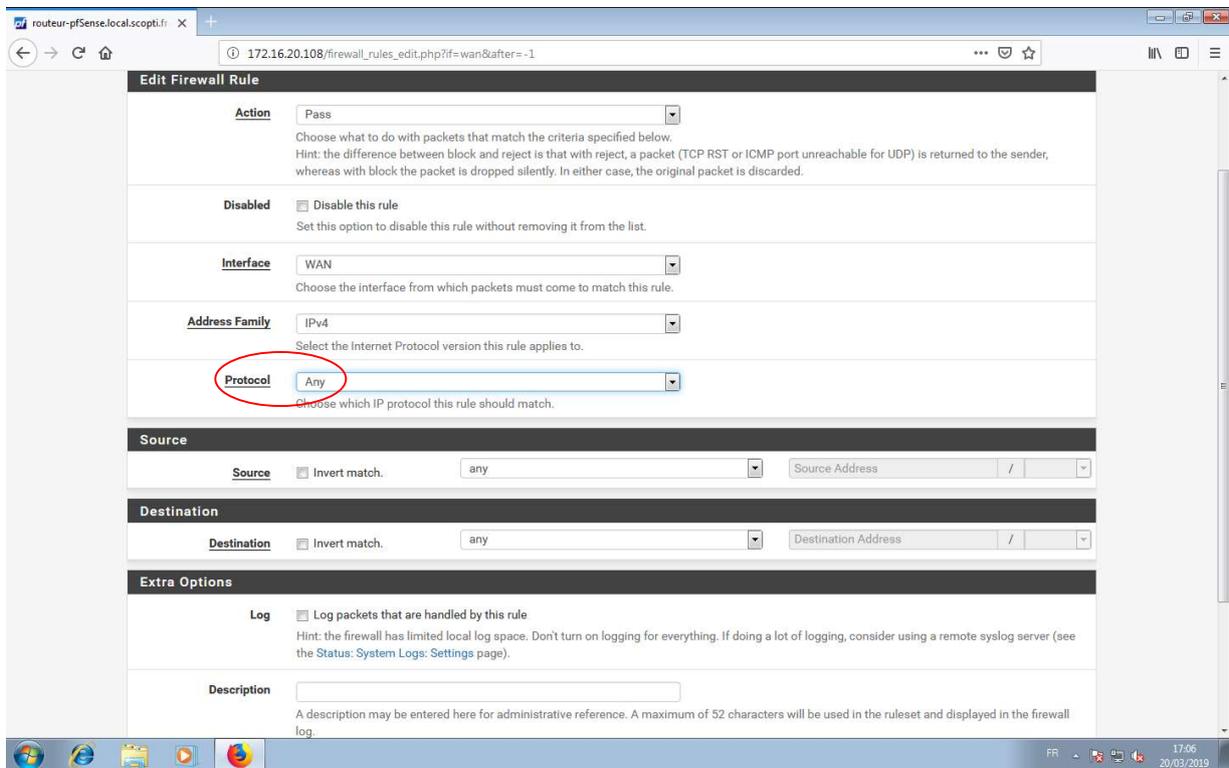


Continuer ensuite l'installation jusqu'au redémarrage.

On peut ensuite renommer les interfaces pour plus de facilité dans le menu « Interfaces » :



Dans le menu « Firewall » -> « Rules », créer une nouvelle règle qui autorise tout et supprimer les règles existantes pour plus de facilité au début :



Recommencer pour toutes les interfaces.

Configuration du NAT :

Aller maintenant dans « Firewall » -> « NAT »-> « Outbound » puis sélectionner « Manuel » et supprimer toutes les règles existantes :

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPT

Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions		
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8	*	*	500	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN			
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN			
<input checked="" type="checkbox"/>	WAN	::1/128	*	*	500	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN			
<input checked="" type="checkbox"/>	WAN	::1/128	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.32/27	*	*	500	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - ADMIN to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.32/27	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - ADMIN to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.80/28	*	*	500	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - DMZ to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.80/28	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - DMZ to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.64/28	*	*	500	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - SERVEUR to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.64/28	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - SERVEUR to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.0/27	*	*	500	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - PROD to WAN			
<input checked="" type="checkbox"/>	WAN	10.0.0.0/27	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - PROD to WAN			

Delete selected maps

Add Add Delete Save

Créer une nouvelle règle en autorisant tout les protocoles et tout les sous réseaux :

routeur-pfSense.local.scopti.fr

172.16.20.108/firewall_nat_out_edit.php?id=0

System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

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.

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.

Address Family IPv4+IPv6
Select the Internet Protocol version this rule applies to.

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

Source Any / 24
Type Source network for the outbound NAT mapping. Port or Range

Destination Any / 24
Type Destination network for the outbound NAT mapping. Port or Range

Not
Invert the sense of the destination match.

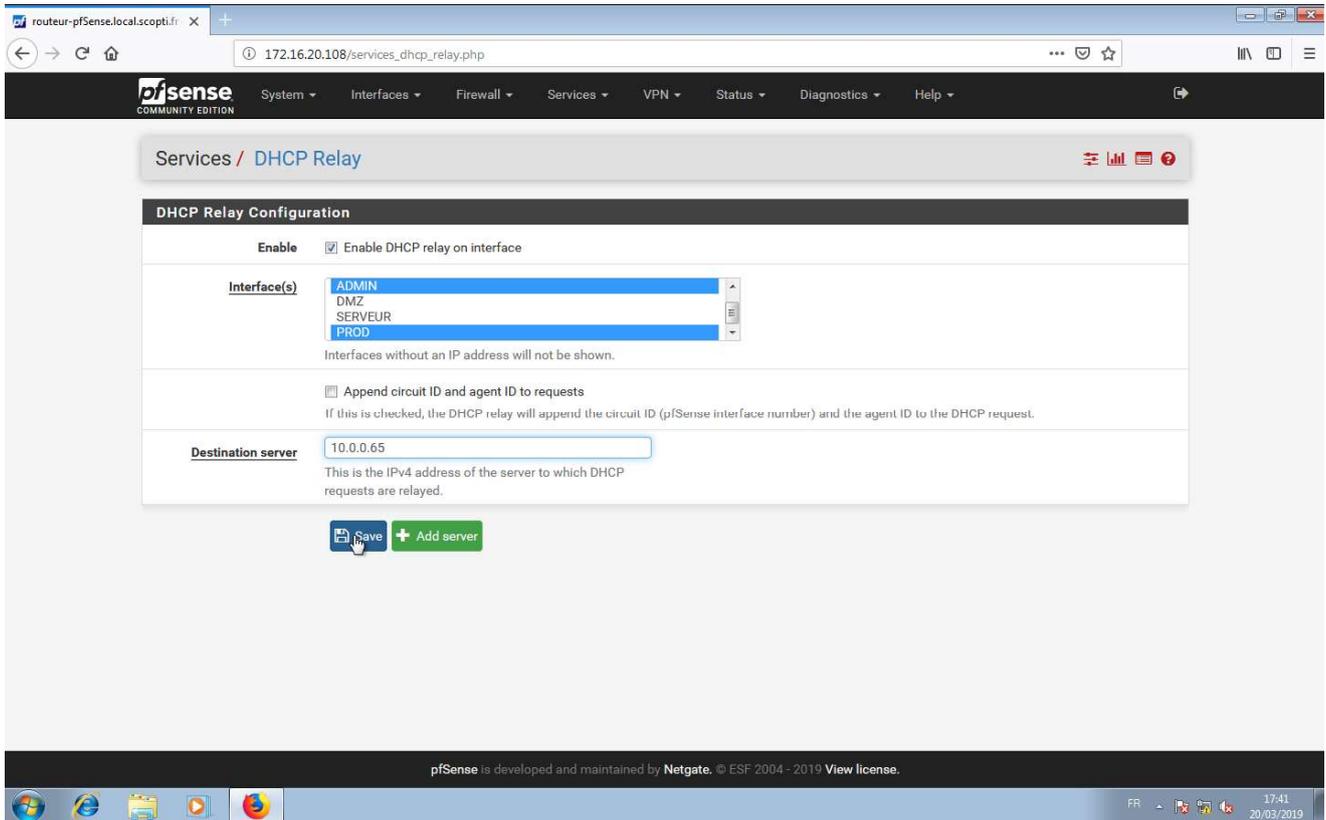
Translation

Address Interface Address
Connections matching this rule will be mapped to the specified Address.

FR 17:36 20/03/2019

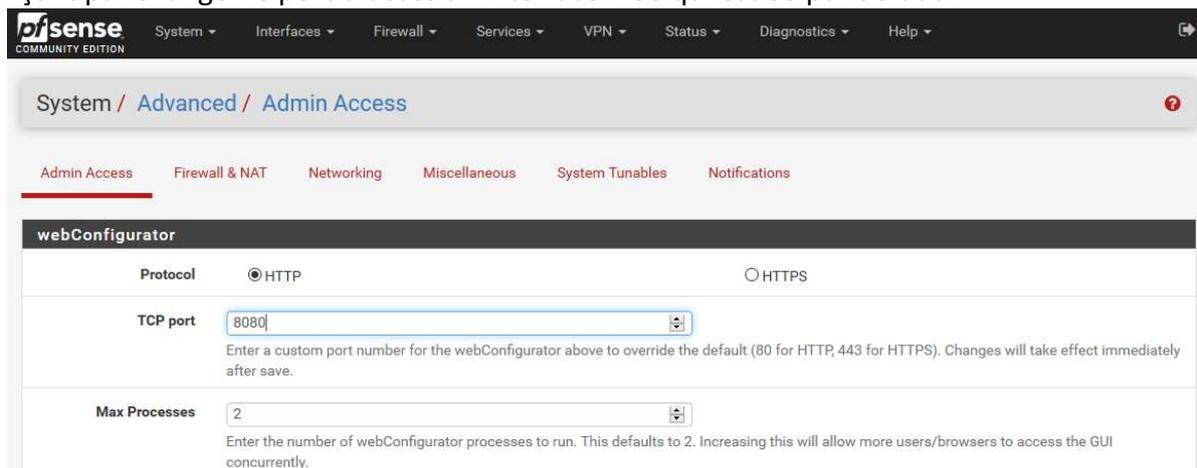
Configuration du relais DHCP :

Configurer maintenant le relais DHCP dans le menu « Services »-> « DHCP Relay » en sélectionnant les sous réseaux voulu et l'adresse IP du serveur DHCP :



Configuration de la redirection de port :

On va ensuite faire une redirection de port car il y a un site Web dans le sous-réseaux DMZ en commençant par changer le port d'accès à l'interface web qui est 80 par défaut :



On va maintenant faire en sorte que tout ce qui vient par l'interface WAN sur le port 80 soit rediriger vers le site web dans la DMZ :

The screenshot shows the 'Edit Redirect Entry' configuration page in the pfSense web interface. The breadcrumb trail is 'Firewall / NAT / Port Forward / Edit'. The page contains several sections for configuring the redirect rule:

- Disabled:** A checkbox labeled 'Disable this rule' is currently unchecked.
- No RDR (NOT):** A checkbox labeled 'Disable redirection for traffic matching this rule' is unchecked. A note below states: 'This option is rarely needed. Don't use this without thorough knowledge of the implications.'
- Interface:** A dropdown menu is set to 'WAN'. A note below says: 'Choose which interface this rule applies to. In most cases "WAN" is specified.'
- Protocol:** A dropdown menu is set to 'TCP'. A note below says: 'Choose which protocol this rule should match. In most cases "TCP" is specified.'
- Source:** A button labeled 'Display Advanced' is visible.
- Destination:** A checkbox 'Invert match.' is unchecked. A dropdown menu is set to 'WAN address'. To its right is an input field for 'Address/mask' with a slash separator. A note below says: 'Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a single port.'
- Destination port range:** Two dropdown menus are both set to 'HTTP'. Below them are input fields for 'From port' and 'To port', both set to 'Custom'. A note below says: 'Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a single port.'
- Redirect target IP:** An input field contains '10.0.0.81'. A note below says: 'Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12'
- Redirect target port:** A dropdown menu is set to 'HTTP'. To its right is an input field for 'Custom'. A note below says: 'Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.'
- Description:** An empty input field. A note below says: 'A description may be entered here for administrative reference (not parsed).'