Création d’une DMZ

SOMMAIRE

Prérequis :

Machine virtuelle Routeur :

Système d'exploitation : PfSense 3

cartes réseaux :

- Réseau Interne avec le nom « Admin »
- Réseau Interne avec le nom « DMZ »
- Réseau Accès par pont

Machine virtuelle Admin :

Système d'exploitation : Debian Interface graphique 1

cartes réseau :

- Réseau Interne avec le nom « Admin »

Machine virtuelle Web :

Systèmes d'exploitation : Debian Interface graphique 1

cartes réseau :

- Réseau Interne avec le nom « DMZ »

Plan d'adressage :

PLAN D'ADRESSAGE

Routeur PFSense	
WAN	172.31.3.111 /21
LAN	192.168.1.1 / 24 (DHCP)
DMZ	192.168.2.1 / 24

Admin	
LAN	192.168.1.10 / 24

Web	
LAN	192.168.2.2 /24

Interfaces réseaux du routeur PFSense :

WAN : 172.31.3.111 /21

LAN : 192.168.1.1 /24

DMZ : 192.168.2.1 /24

```
Enter an option:
Message from syslogd@pfSense at Apr  9 13:18:27 ...
php-fpm[370]: /index.php: Successful login for user 'admin' from: 192.168.1.10 (
Local Database)
j

KVM Guest - Netgate Device ID: 9209cdf3825e54172001

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

 WAN (wan)       -> em0        -> v4: 172.31.3.111/21
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        -> v4: 192.168.2.1/24

 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:
```

Assignation des Interfaces du routeur :

Taper « 1 » pour assigner nos 3 interfaces :

Puis « n » pour ne pas créer de VLAN :

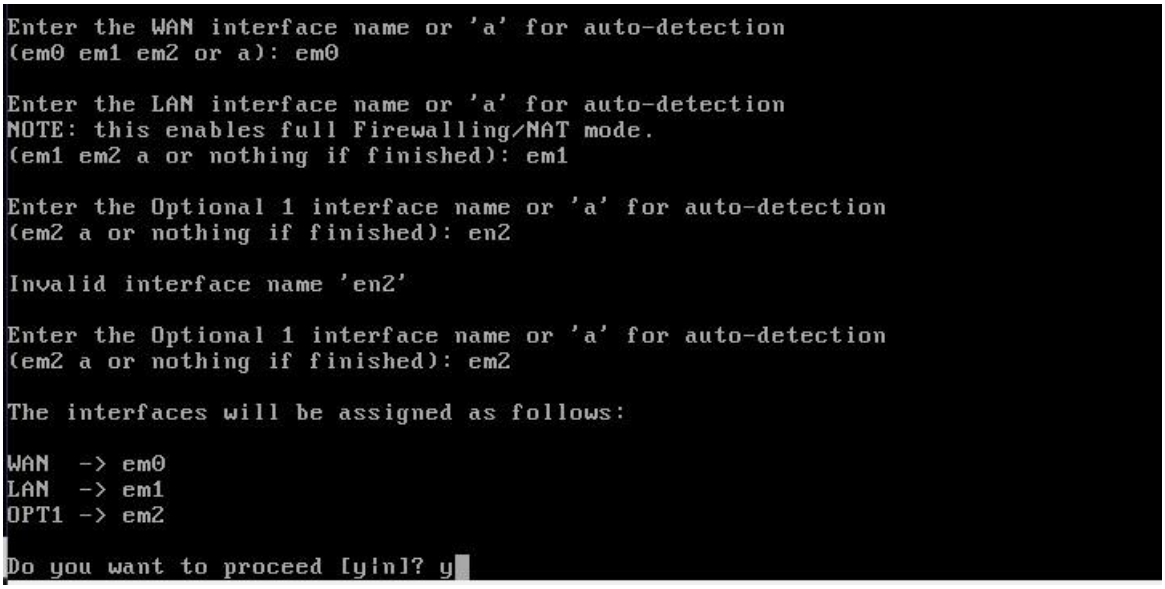
```
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 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: 1


Valid interfaces are:

em0     08:00:27:60:29:6e   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1     08:00:27:46:a5:e0   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2     08:00:27:b7:c3:26   (up) Intel(R) Legacy PRO/1000 MT 82540EM

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
```

Choisir l'interface WAN que l'on veut utiliser dans ce cas-là on choisit « em0 » :

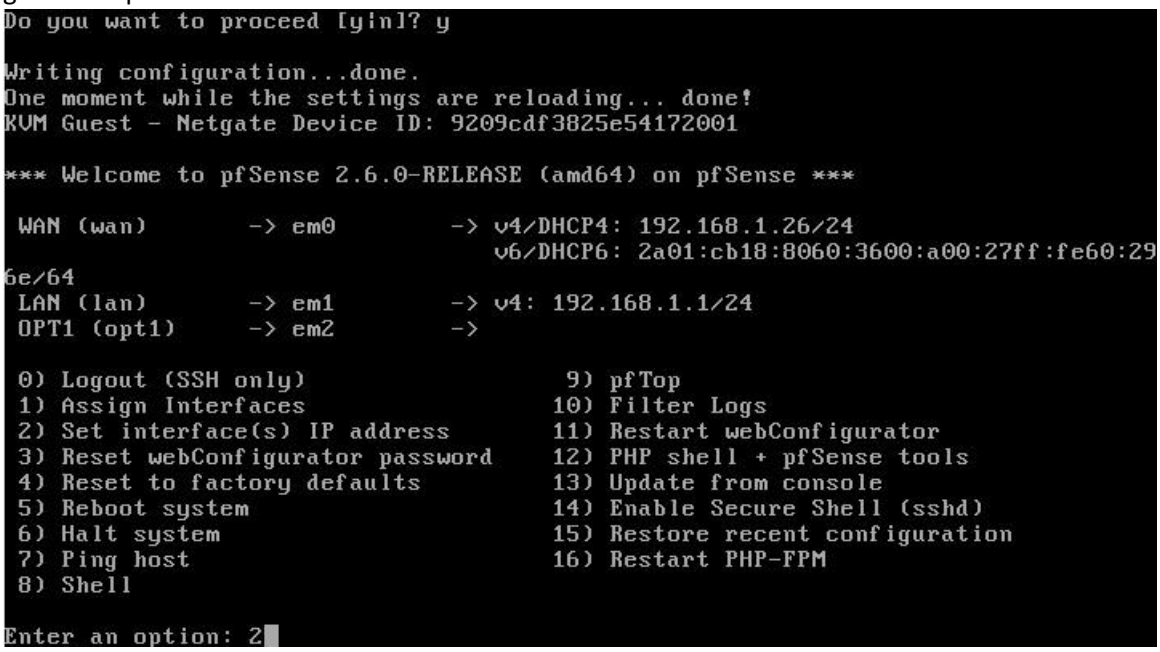
Puis choisir l'interface LAN que l'on veut utiliser dans ce cas-là on choisit « em1 » :

Ensuite choisir l'interface DMZ que l'on veut utiliser dans ce cas-là on choisit « em2 » :

Enfin il faut en dernier temps valider en faisant « y » :

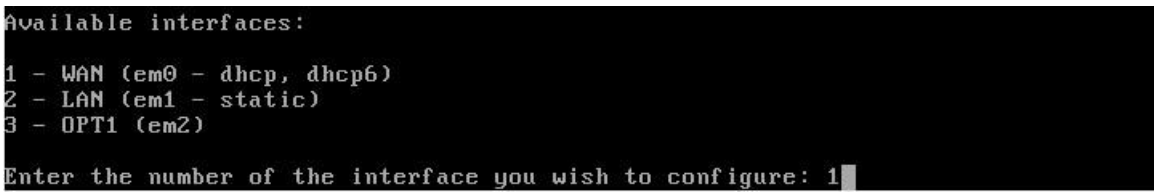


On se retrouve maintenant avec toutes les interfaces assignées il faut maintenant les Paramétrés grâce à l'option « 2 »



Paramétrage WAN :

Choisir le « 1 » :

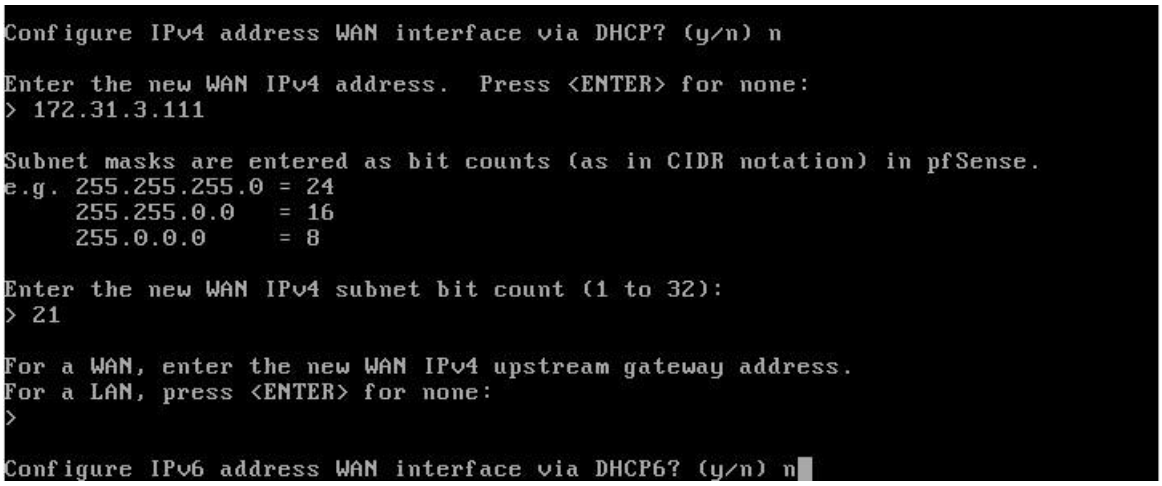


Choisir « n » pour ne pas utiliser le dhcp :

Puis mettre l'adresse IPv4 « 172.31.3.111 » :

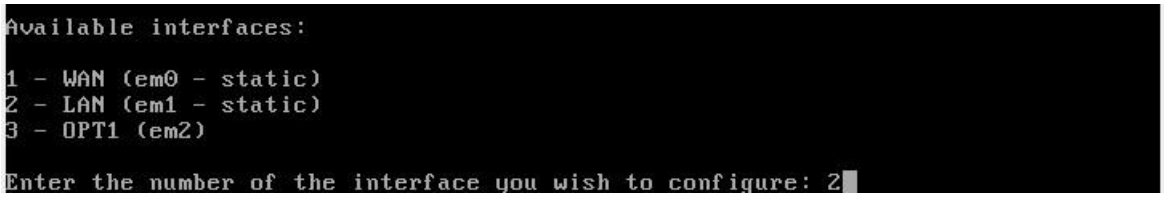
Ensuite mettre le CIDR « 21 » :

Et enfin « n » pour ne pas configurer l'IPv6 :



Paramétrage LAN/DHCP :

Choisir le « 2 » :



Puis mettre l'adresse IPv4 « 192.168.1.1 » :

Ensuite mettre le CIDR « 24 » :

Et enfin « y » pour activer le serveur DHCP :

```
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.1

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:
>

Do you want to enable the DHCP server on LAN? (y/n) y
```

Mettre la première adresse du DHCP « 192.168.1.2 » :

Puis la dernière adresse du DHCP « 192.168.1.10 » :

```
Enter the start address of the IPv4 client address range: 192.168.1.2
Enter the end address of the IPv4 client address range: 192.168.1.10
```

Le routeur nous donne son adresse ip pour accéder sur le web a son interface graphique :

```
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.1.1/

Press <ENTER> to continue.
```

Paramétrage DMZ :

Choisir le « 3 » :

```
Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3
```

Puis mettre l'adresse IPv4 « 192.168.2.1 » :

Ensuite mettre le CIDR « 24 » :

```
Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.2.1

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 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:
>
```

Et enfin « y » pour ne pas activer le serveur DHCP

Configuration web :

Pour commencer la configuration IP de la machine virtuelle web il faut se mettre en « root » avec la commande « su - » puis mettre le mot de passe :

```
sio@web:~$ su -
Mot de passe :
root@web:~#
```

Avec la commande « nano » aller dans « /*etc/*network/interfaces » :

Et modifier le contenu comme ci-dessous :

```
  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

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.2.2
netmask 255.255.255.0
gateway 192.168.2.1
```

Ctrl+o pour enregistrer

Ctrl+x pour quitter

Une fois le fichier modifier il faut relancer le service pour mettre à jour l'ip avec la commande « /*etc*/init.d/networking restart »

Configuration admin :

Cliquer sur l'icône réseau :

Puis sur « Filaire connecté »

Ensuite sur « Paramètre filaire »

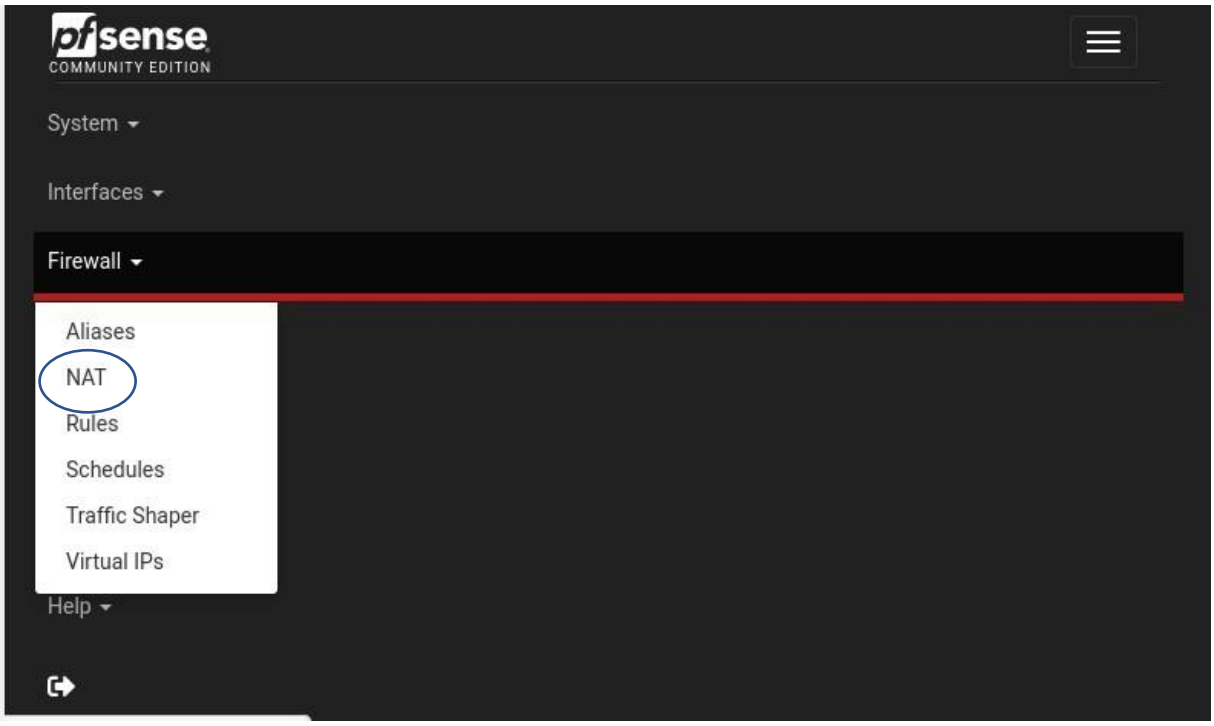
Puis aller sur le petit icone réglage  dans l'onglet « Filaire »

Aller sur IPv4 et se mettre en automatique (DHCP) :

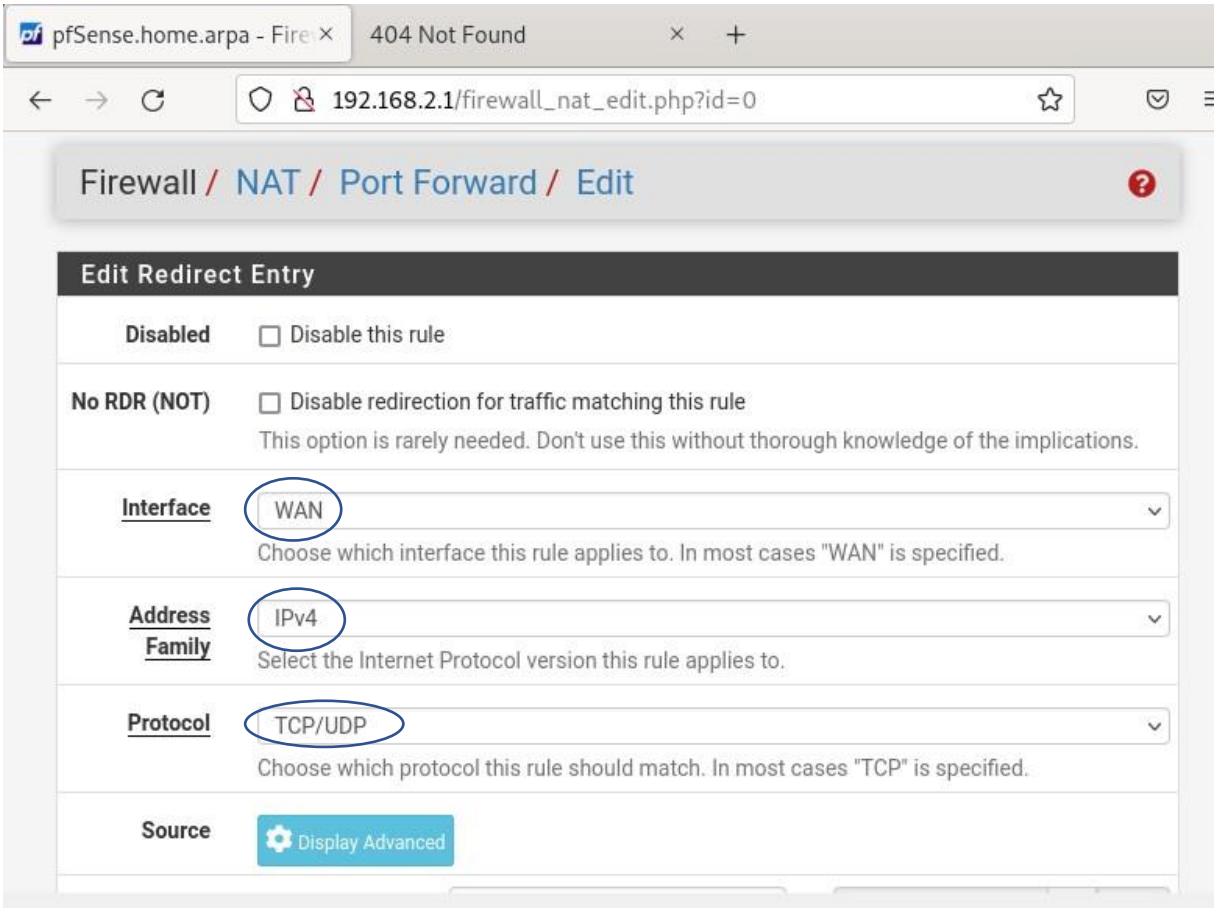
Redirection NAT :

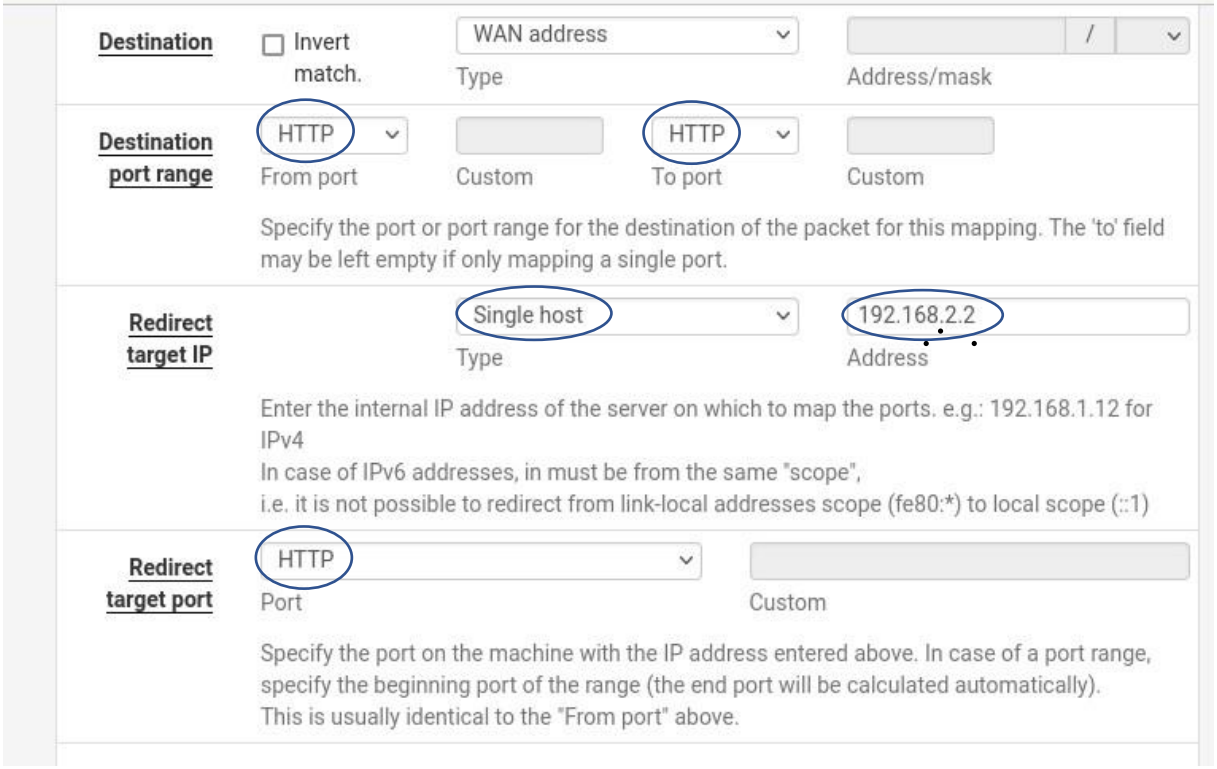
Aller sur le l'interface graphique du routeur avec la machine virtuelle admin avec le navigateur Firefox :

Aller dans l'onglet puis « Firewall » puis « NAT »

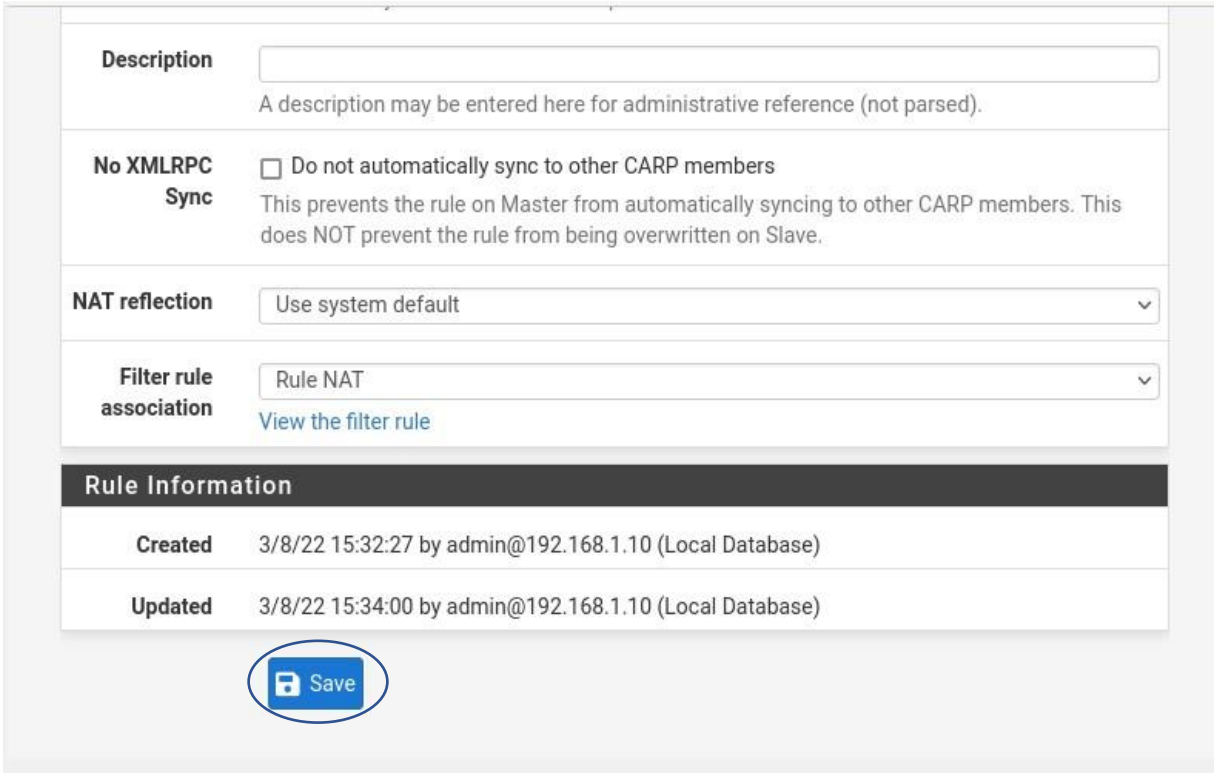


Paramétrer comme ci-dessous :





Et puis on sauvegarde :



Test :

Tester communication depuis le routeur vers machine virtuelle Web	
Tester communication depuis le routeur vers machine virtuelle Admin	
Tester la communication depuis la machine virtuelle Web vers machine virtuelle Admin	
Vérifier l'accès a l'interface graphique du routeur via la machine virtuelle Admin	
Vérifier l'accès au site web de la machine virtuelle Web via la machine virtuelle Admin	

Installation et vérification finis vous avez désormais une infrastructure avec une DMZ.