Enzo

LEFORT

BTS SIO 2

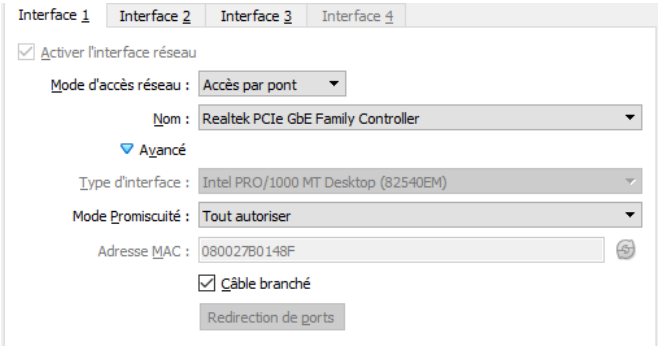
TP PfSense

I- Installation PfSense sur Virtual Box

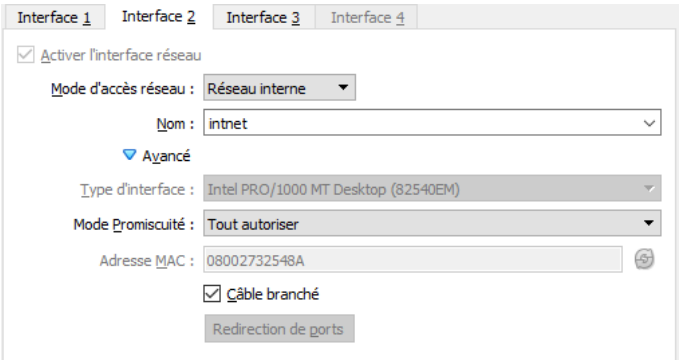
Configuration de la VM PfSense sur virtual box :

- Ajouter un disque
- 512go de RAM est suffisant
- Ajout de 3 interfaces réseaux :

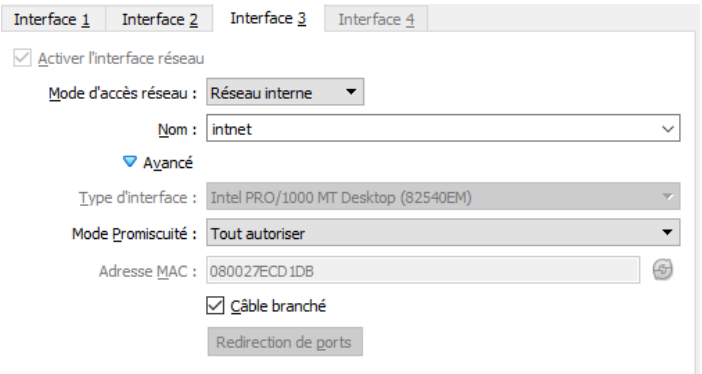
Pour le WAN (accés par pont et tout autoriser dand Mode Promoscuité)



Pour le LAN (réseau interne et tout autoriser dand Mode Promoscuité)

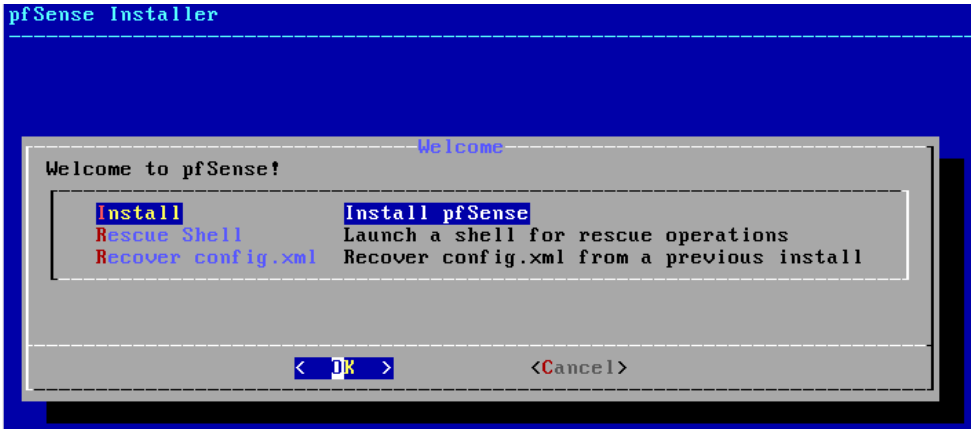


Pour la DMZ (réseau interne et tout autoriser dand Mode Promoscuité)

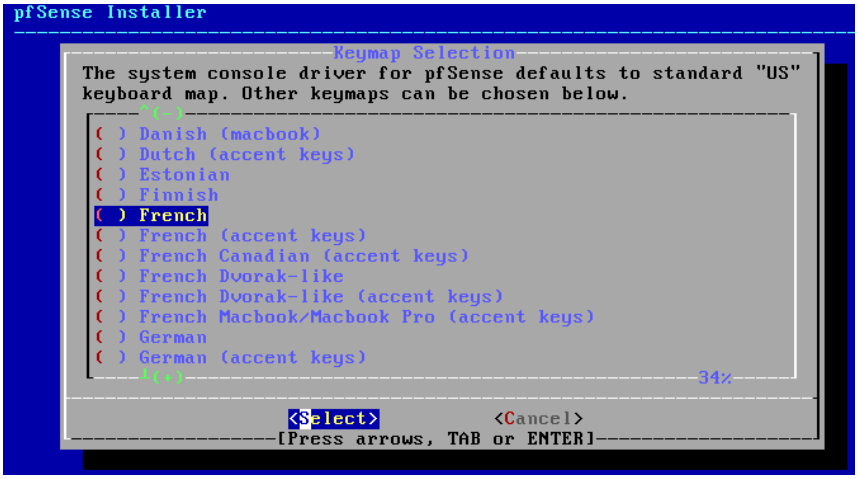


- Démarrage sur l'ISO de PfSense :

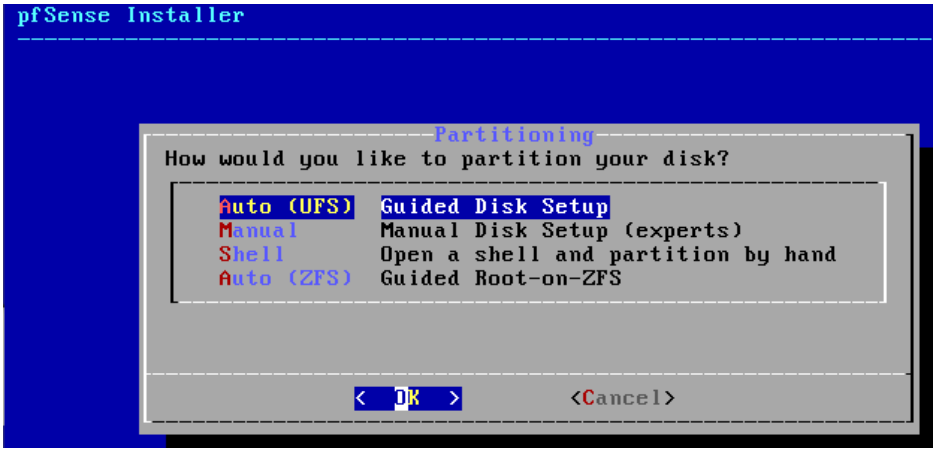
Appuyez sur Entrée :



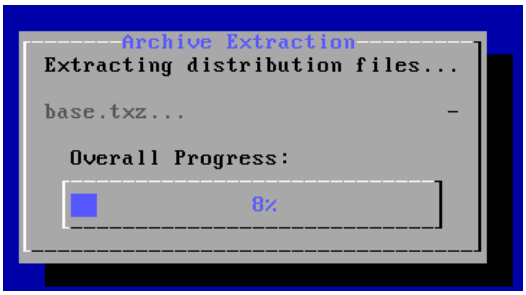
Choix de la langue :



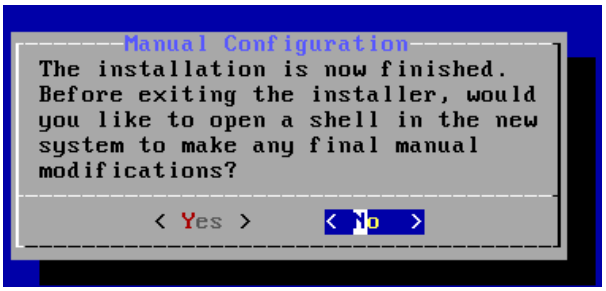
Auto (UFS) :



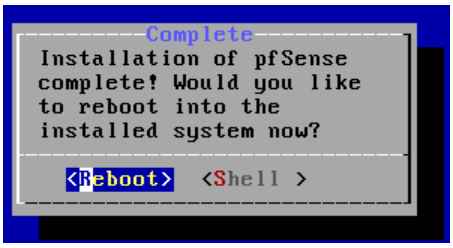
Installation :



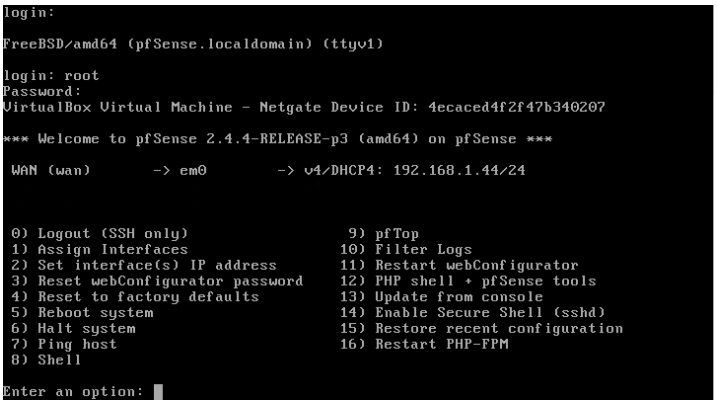
No :



Redémarrage du système :



Après redémarrage :



II- Mise en place d'un serveur Web

- Installation serveur web (serveur LAMP) :

  Mise à jour du système : apt update && apt upgrade

  Installation Apache 2 : apt install apache2

  Installation php 7 : apt install php

  Installation Mysql : apt install mysql-server

  Sécuriser mysql : mysql_secure_installation

  Creation d'un utilisateur administrateur : mysql –p

  CREATE USER sio@localhost IDENTIFIED BY 'sio2018';

  GRANT ALL PRIVILEGES ON *.* TO sio@localhost WITH GRANT OPTION ;

  QUIT

  Installation phpMyAdmin : apt install phpmyadmin

- Création d'une page simple
  On place le fichier nommé index1.html dans le répertoire /var/www/html

```
 GNU nano 2.7.4                Fichier : index1.html

<!DOCTYPE html>
<html>
  <head>
    <title>Coucou</title>
  </head>
  <body>
  Cette page est une page toute simple
  </body>
<a href="/var/www/html/index2.html" target="_blank"> <input type="button" value$
</html>
```

III- Configuration de PfSense

On assigne les interfaces aux cartes réseau :

Pour cela on selectionne 1

Should Vlans be set up nwow : n

On indique les cartes réseau à chaque interface : em0 pour le WAN, em1 pour le LAN et em2 pour la DMZ.

```
em0     08:00:27:5c:52:7f   (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1     08:00:27:6c:a7:8f   (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em2     08:00:27:b3:e5:e6   (up) 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

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
(em0 em1 em2 or a): em0

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

Optional interface 1 description found: DMZ
Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2
```

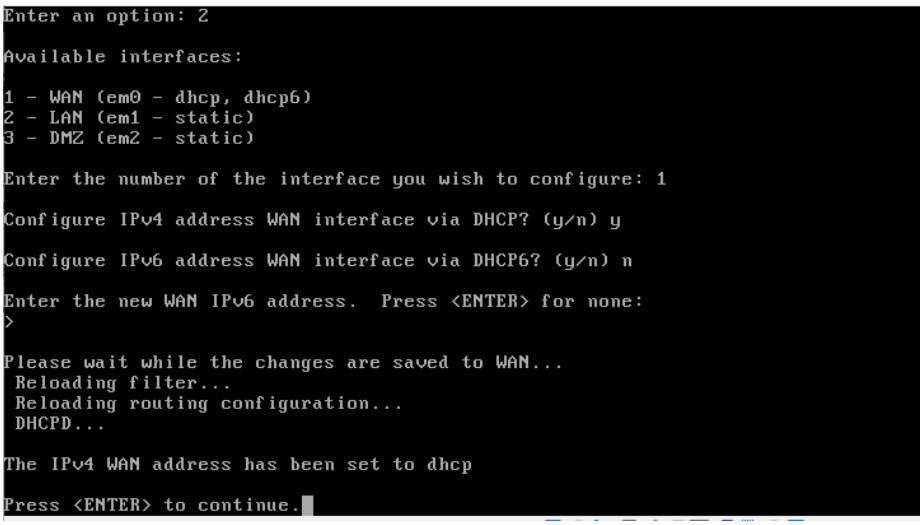
Do you want to proceed : y

On indique l'adresse IP de chaque interface :

Pour cela on selectionne 2

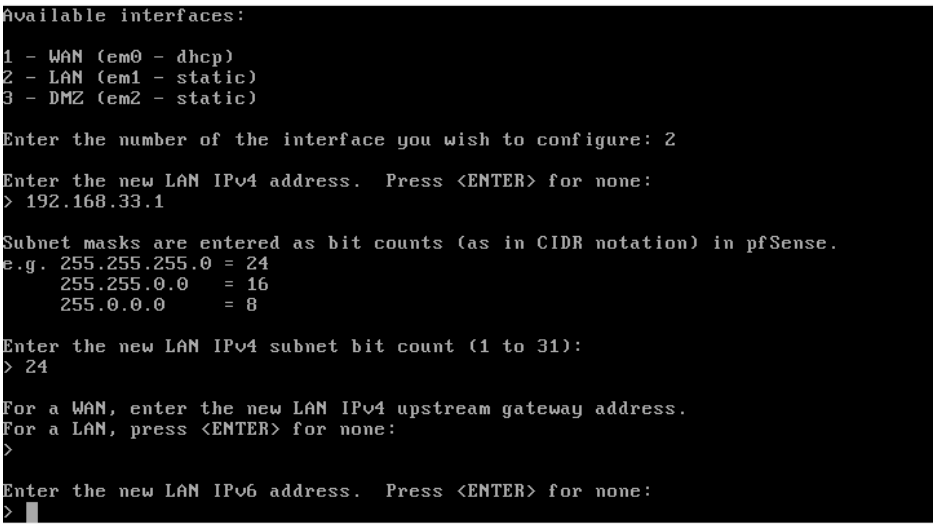
Pour le WAN:

Configuration de l'adresse IPv4 du WAN via le DHCP, on ne configure par d'adresse IPv6



Pour le LAN :

Adresse IP du LAN 192.168.33.1 /24, on ne configure pas d'adresse IPv6. On ne configure pas le DHCP sur cette interface. L'interface WEB sera accessible depuis cette adresse.



Pour la DMZ :

Adresse IP de la DMZ 10.0.0.1/ /8, on ne configure pas d'adresse IPv6. On ne configure pas le DHCP sur cette interface.

```
Available interfaces:

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

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

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 10.0.0.1

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 31):
> 8

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

Please wait while the changes are saved to OPT1...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT1 address has been set to 10.0.0.1/8

Press <ENTER> to continue.
```

Une fois finie l'interface de PfSense devrait ressembler à cela :

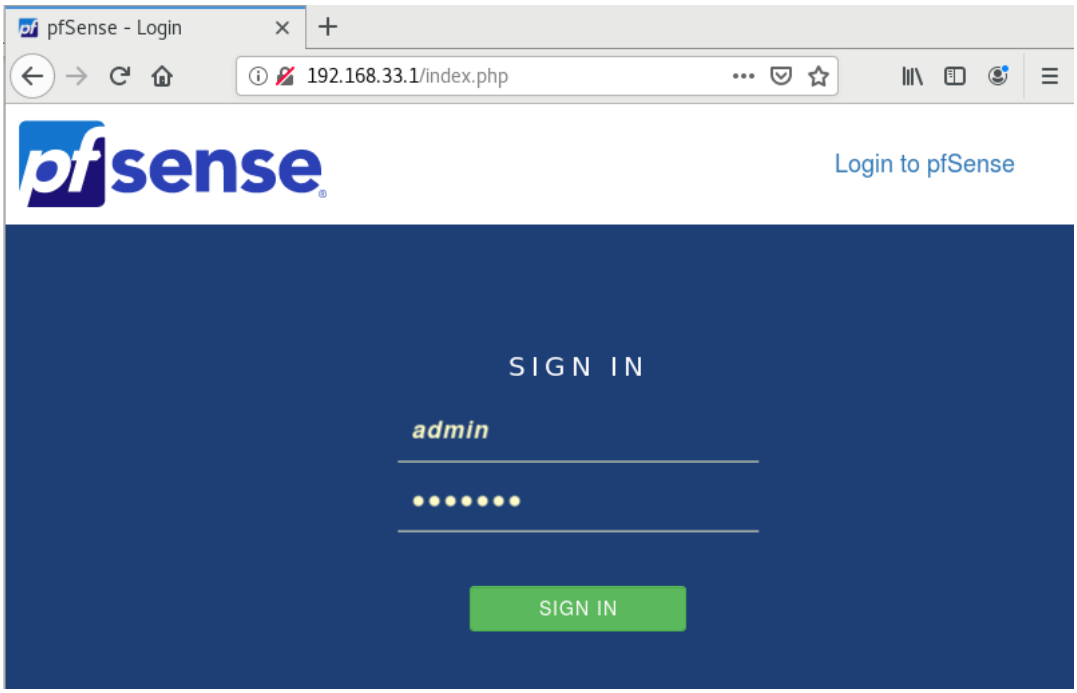
```
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT1 address has been set to 10.0.0.1/8

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 6b4cbbfebb3050d8f154

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

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.92/24
 LAN (lan)       -> em1        -> v4: 192.168.33.1/24
 DMZ (opt1)      -> em2        -> v4: 10.0.0.1/8

 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:
```

Accès à l'interface WEB :

Adresse IP du PC connecté sur le LAN : 192.168.33.3 /24

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:f4:2c:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.33.3/24 brd 192.168.33.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef4:2c92/64 scope link
       valid_lft forever preferred_lft forever
```

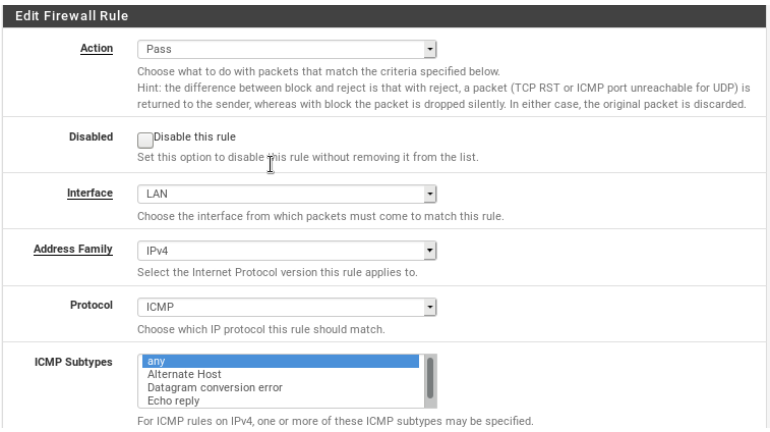
On recherche l'adresse IP du LAN sur un navigateur :

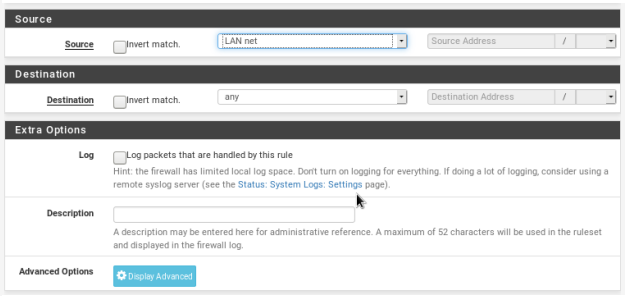


Créaion des regles pour le LAN :

Firewall > Rules > LAN > Add

Première règle : Autoriser toute les requêtes pings en provenance du LAN





Action = PASS ; signifie que c'est une règle qui va ouvrir des ports pour pouvoir laisser passer des paquets.

Interface = LAN ; L'interface auquel la règle s'applique.

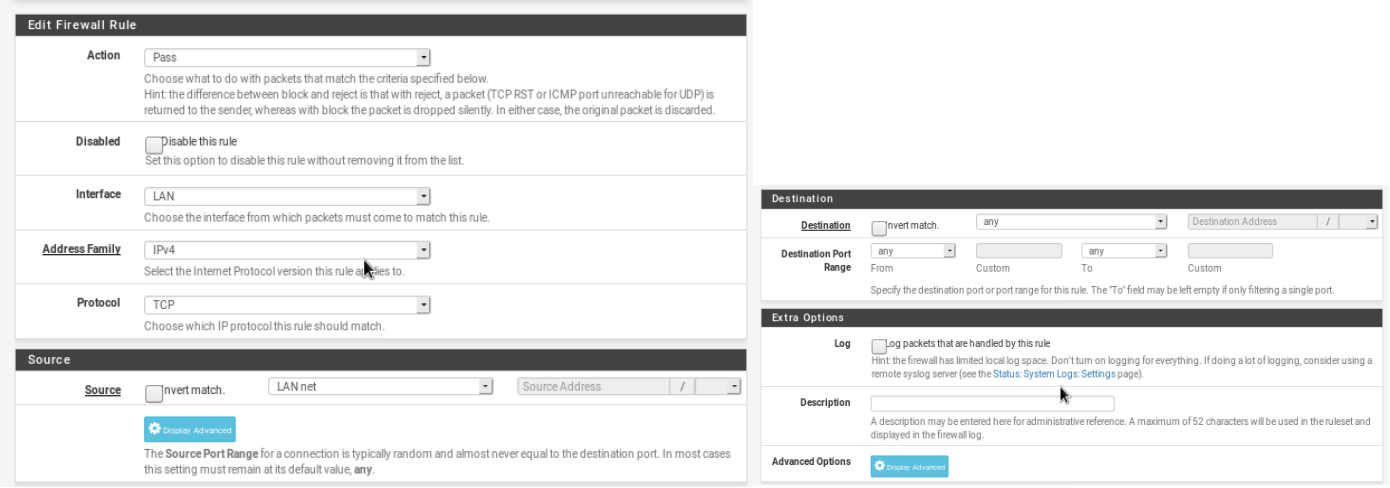
TCP/IP Version = IPv4 ; cette règle s'applique aux machines possédants une adresse IPv4.

Protocol=ICMP ; cette règle va s'appliquer au protocole ICMP.

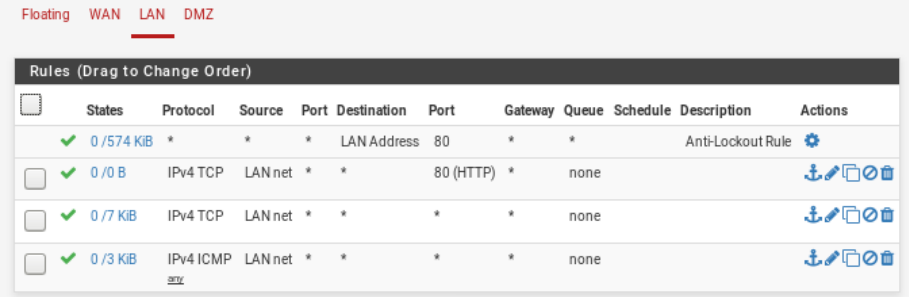
Source = LAN net ; on autorise ce qui provient du réseau LAN.

Destination=any ; ping n'importe qui.

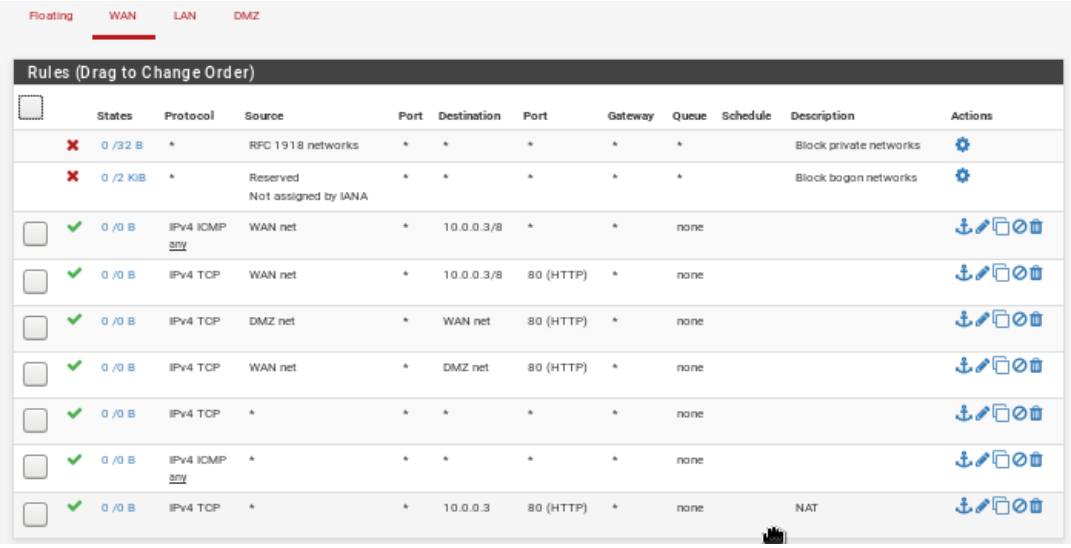
Deuxième règle :



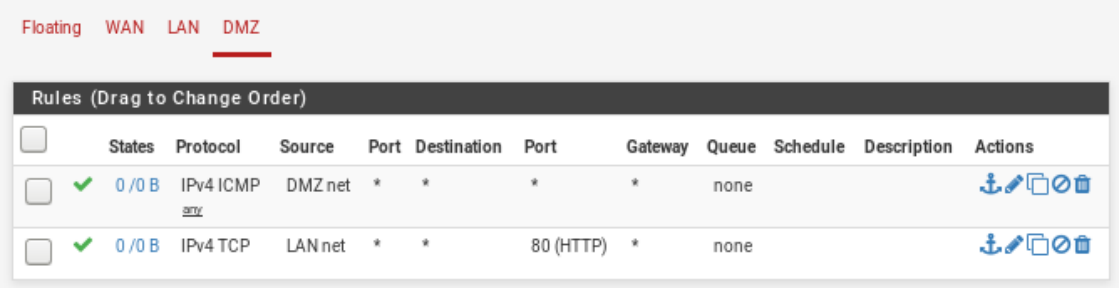
Toutes les régles pour le LAN :



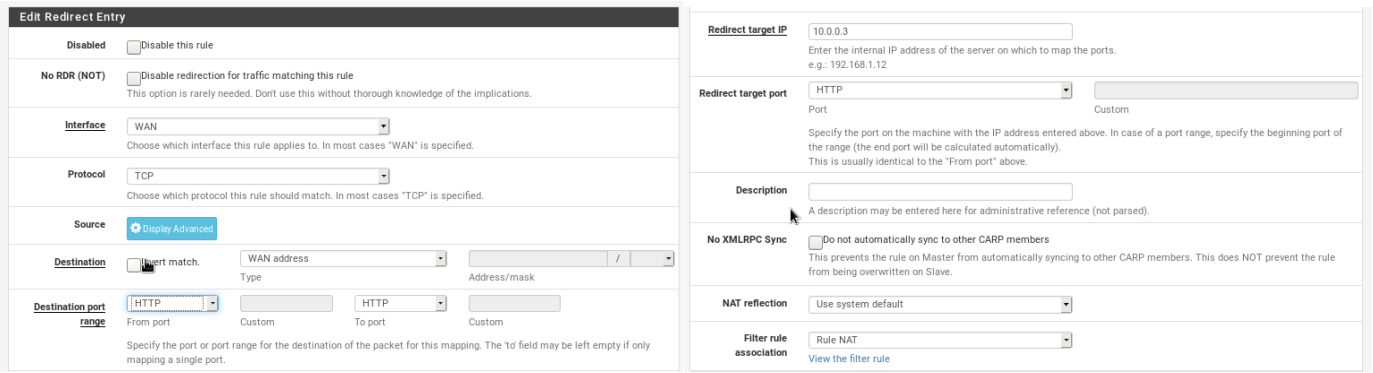
Toutes les régles pour le WAN :



Toutes les régles pour la DMZ :



Redirection de port :



Interface=WAN ; Spécifie que cette règle se situe sur l'interface WAN du PfSENSE

Protocol=TCP ;

Destination=WAN ; On redirige vers le WAN

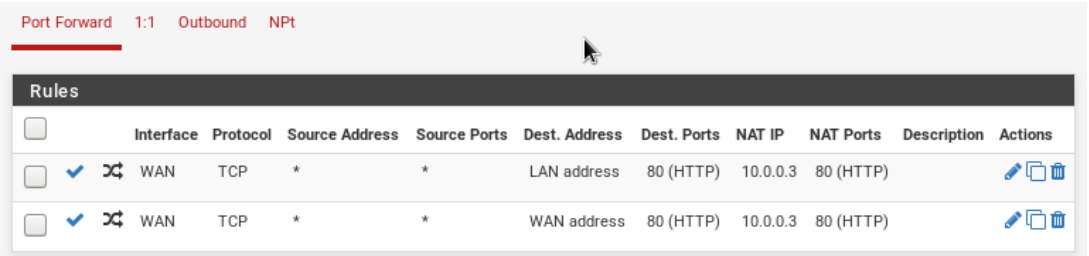
Destination port range=HTTP ; spécifie le(s) port utilisés pour rediriger le serveur WEB

Redirect target IP= 10.0.0.3

Redirect target port=HTTP ; spécifie avec quel(s) port(s) on accède à la machine

On refait la même règle, mais cette fois si pour rediriger vers le LAN.

Toutes les redirections de ports :



Test du service mis en place :

Depuis une machine connecté sur le LAN en 192.168.33.3 /24, on essaie d'accéder au serveur WEB connecté sur la DMZ en 10.0.0.3 /8 :

On accède bien au serveur WEB.

Test de ping :

PC LAN vers WAN :

```
root@debian:/home/sio# ping 192.168.1.92
PING 192.168.1.92 (192.168.1.92) 56(84) bytes of data.
64 bytes from 192.168.1.92: icmp_seq=1 ttl=64 time=0.267 ms
64 bytes from 192.168.1.92: icmp_seq=2 ttl=64 time=0.539 ms
```

PC LAN vers LAN :

```
root@debian:/home/sio# ping 192.168.33.1
PING 192.168.33.1 (192.168.33.1) 56(84) bytes of data.
64 bytes from 192.168.33.1: icmp_seq=1 ttl=64 time=0.276 ms
64 bytes from 192.168.33.1: icmp_seq=2 ttl=64 time=0.798 ms
```

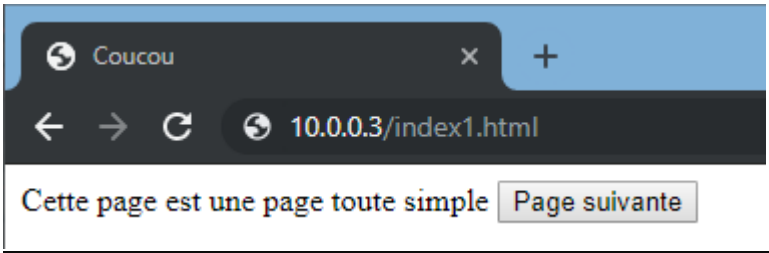
PC LAN vers DMZ :

```
root@debian:/home/sio# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.542 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.805 ms
```

PC LAN vers Serveur WEB (sur la DMZ) :

```
root@debian:/home/sio# ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=63 time=0.755 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=63 time=1.53 ms
```

Test depuis un PC connecté sur le WAN :




```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : lan
   Adresse IPv6 de liaison locale. . . . .: fe80::caa:3808:33d1:fe8f%7
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.9
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.1.254
```