V1.0

DOCUMENTATION PFSENSE

Installation et configuration

15 JUIN 2022

CCI CAMPUS STRASBOURG
BTS SIO SISR

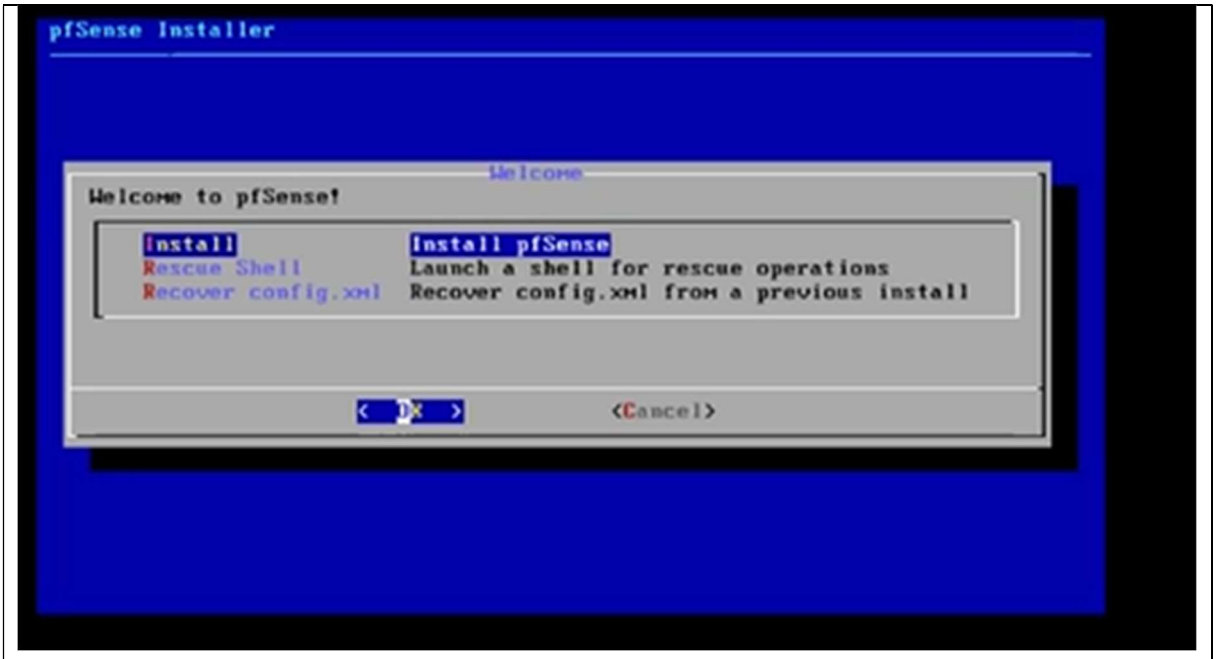
Table des matières

Prérequis

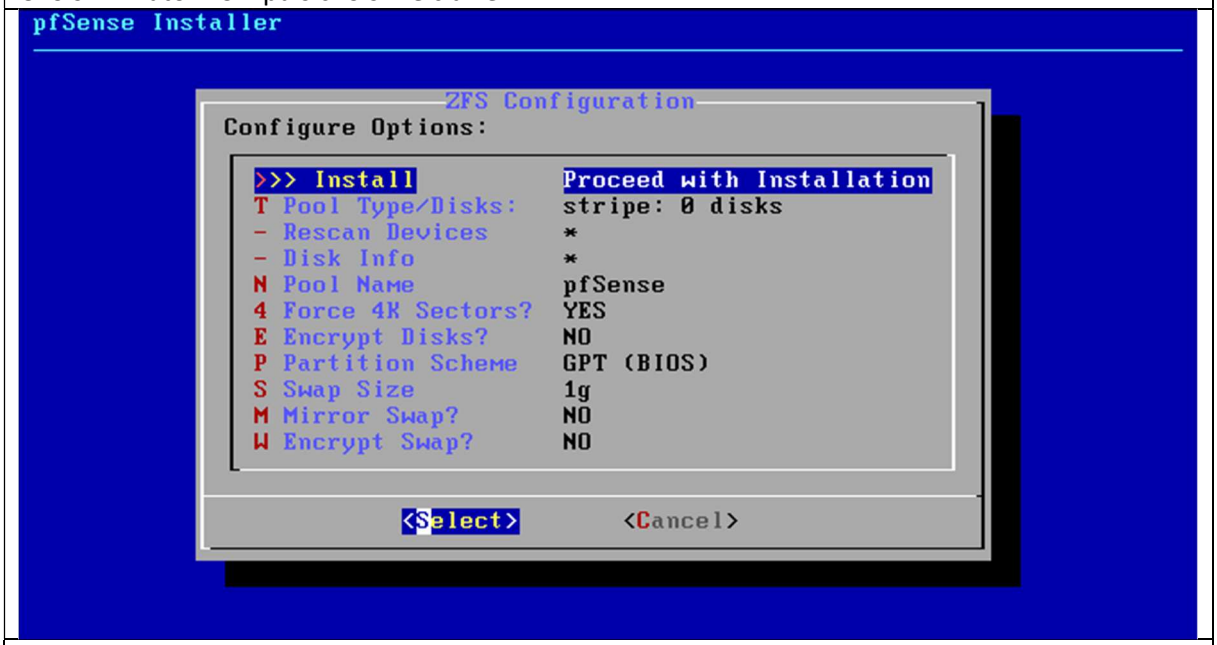
- Une vm Pfsense FreeBSD sur VMware avec 2 carte réseaux, une pour le WAN et une pour le LAN.

- Un client Windows 10 (ici c'est un PRO)

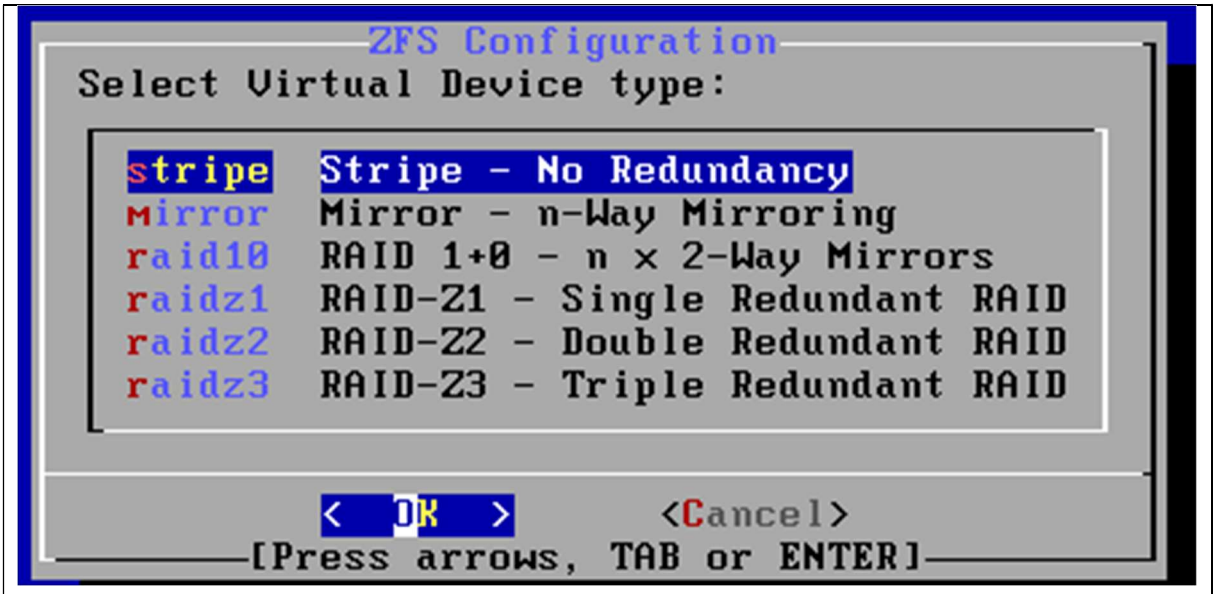
1.Installation de pfsense freeBSD

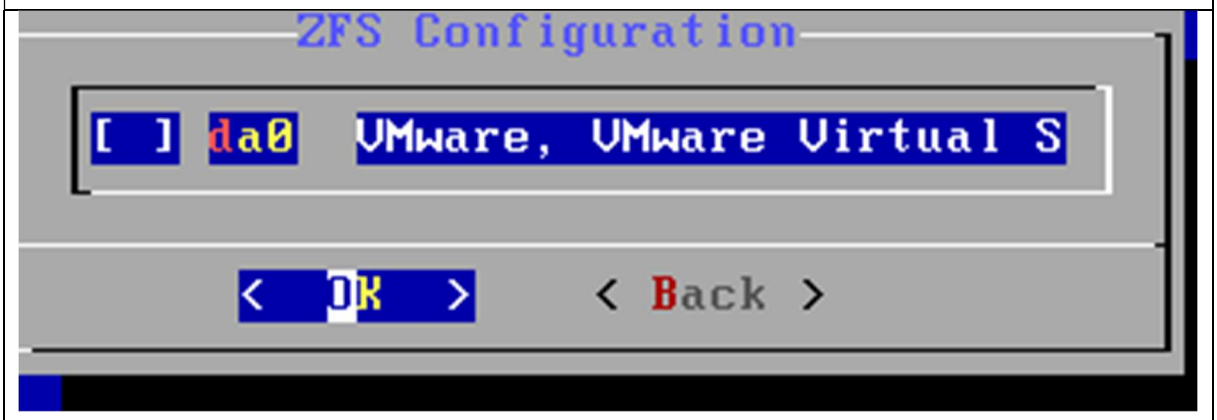


Choisir « Auto ZFS » puis choisir le clavier

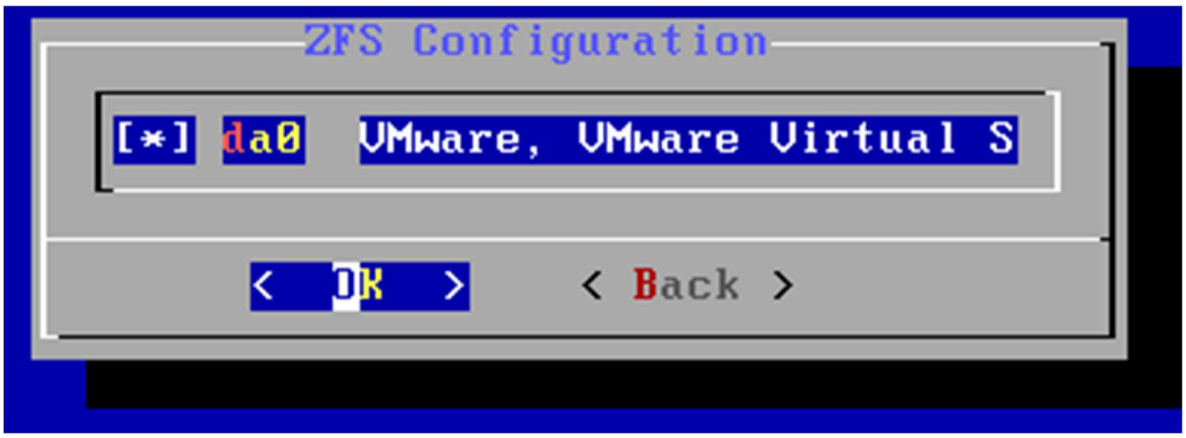


Sélectionnez « **pool Type/Disks** » et choisir « **No Redundancy** » parce qu'on a pas besoin de mettre en place de redondance dans ce tp.



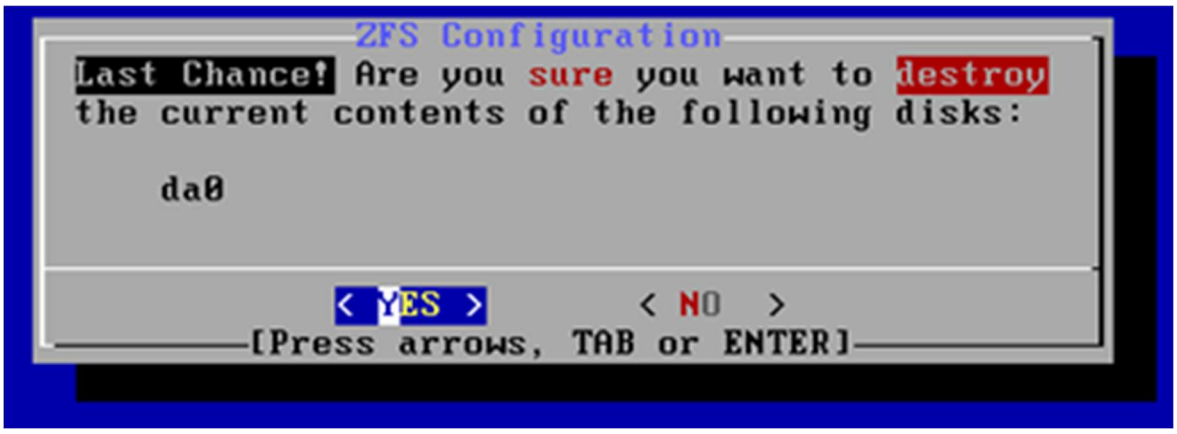


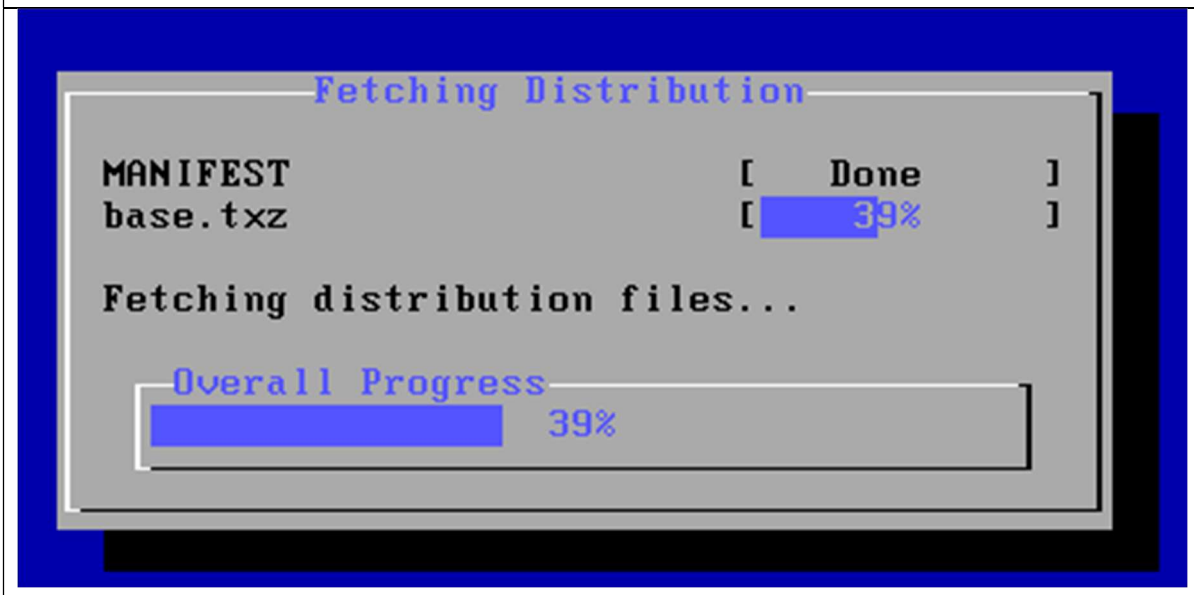
Cocher la case avec la touche « espace »

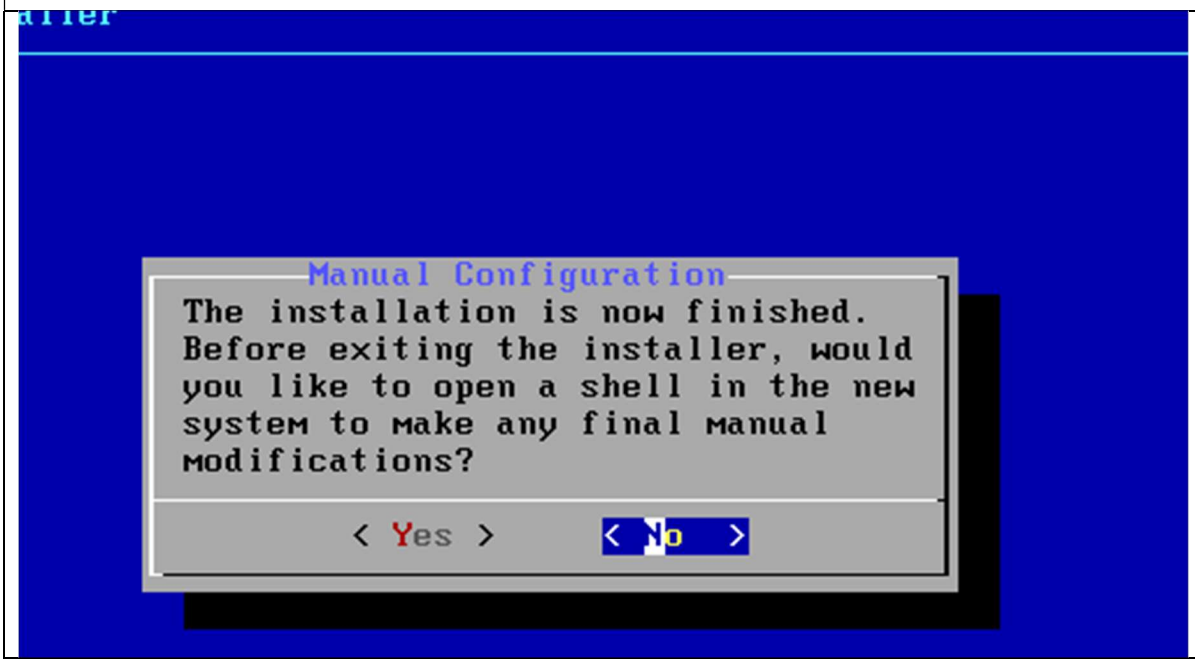


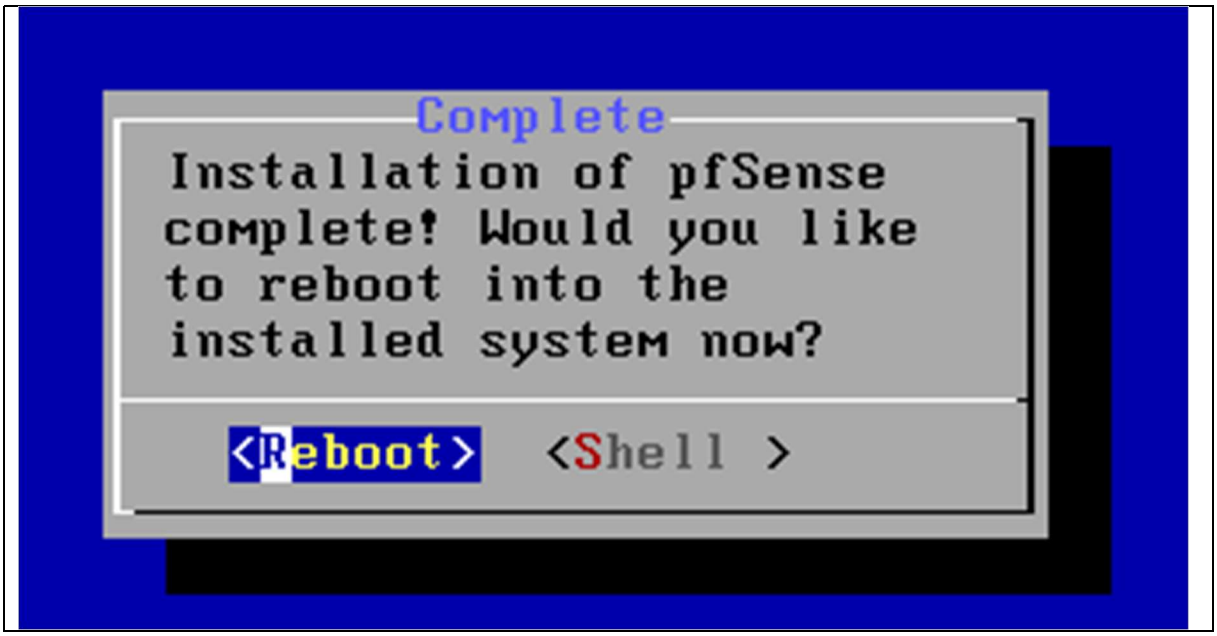
Puis « ok »

Validez


ZFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
da0
< YES >
< NO >
[Press arrows, TAB or ENTER]


Fetching Distribution
MANIFEST [Done]
base.txz [39%]
Fetching distribution files...
Overall Progress
39%


Manual Configuration
The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?
< Yes >
< No >



2.Configuration sur pfsense

On va configurer l'adresse ip de la carte réseau « LAN »

```
VMware Virtual Machine - Netgate Device ID: 7c7fb77f9313d79e20a5

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

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.71.128/24
 LAN (lan)       -> em1        -> v4: 192.168.1.254/24

 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:
```

Choix « 2 »

```
VMware Virtual Machine - Netgate Device ID: 7c7fb77f9313d79e20a5

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

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.71.128/24
 LAN (lan)       -> em1        -> 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
```

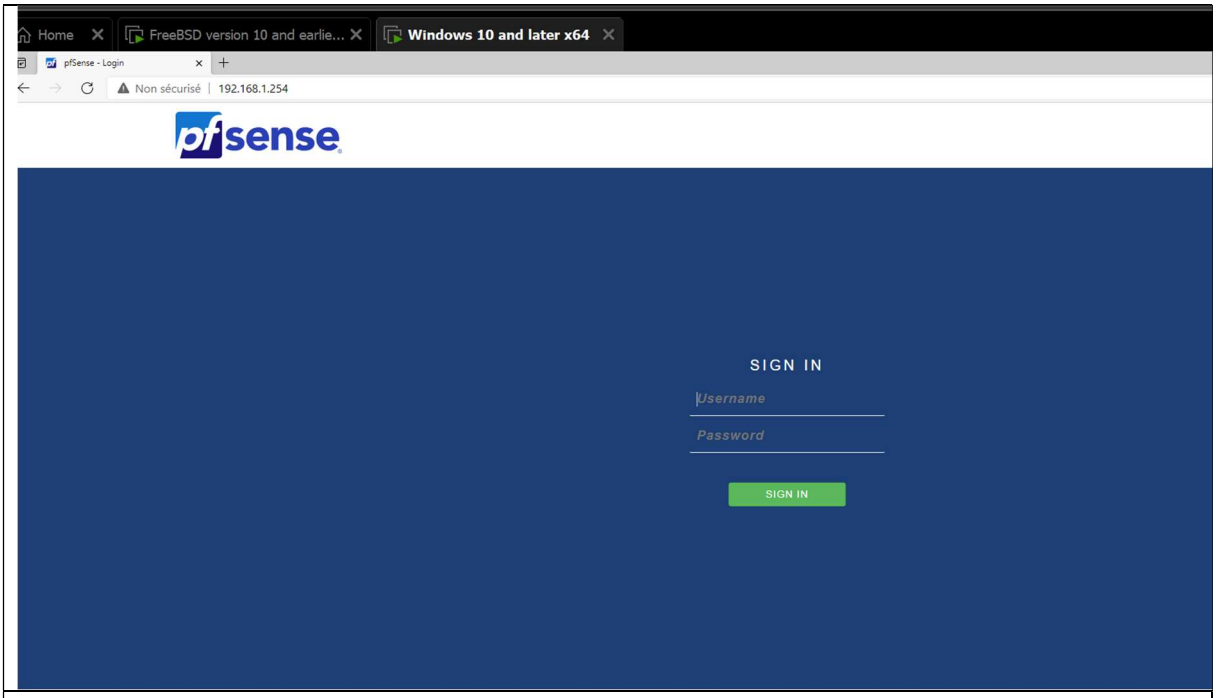
Choisir l'interface « LAN » choix « 2 » puis renseignez les réglages de l'adresse ip suivant
Ip : 192.168.1.254
Subnet bit count : 24
DHCP : n

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.254

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:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

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

The IPv4 LAN address has been set to 192.168.1.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.1.254/

Press <ENTER> to continue.
```

L'adresse ip est configurée.

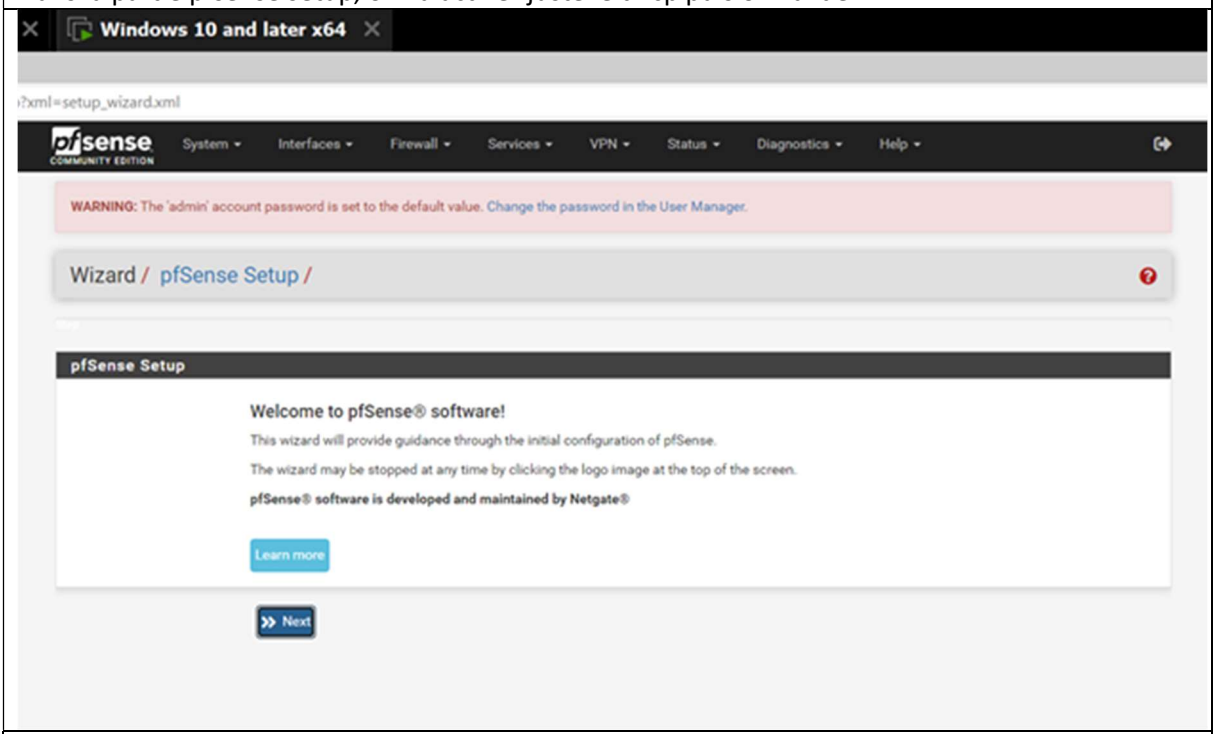
3.Configuration depuis client Windows 10 Pro

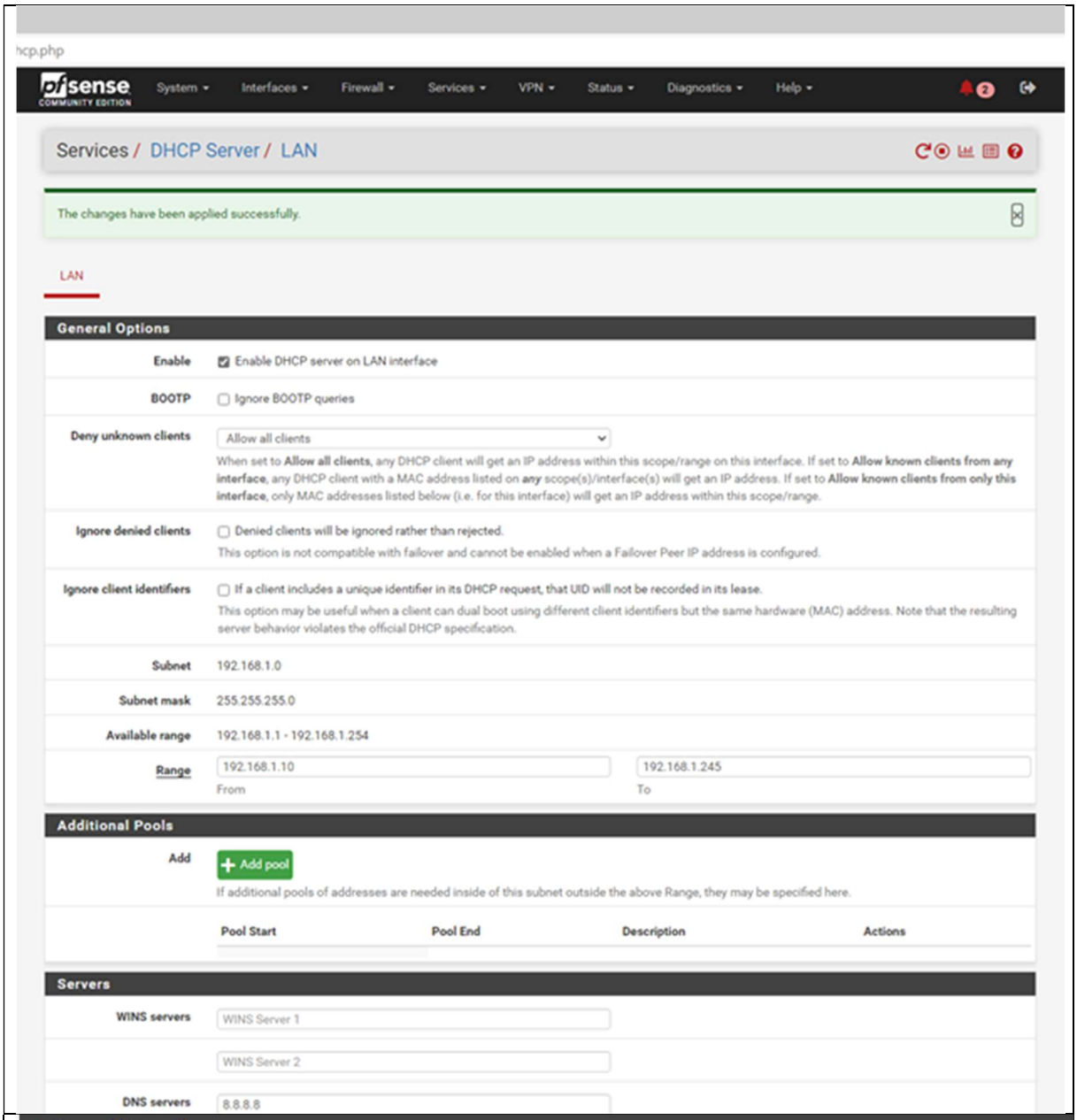
Configuration de base = carte réseau avec l'ip sur le même réseau que pfsense et mettre l'ip de pfsense en passerelle (8.8.8.8 en dns pour internet).

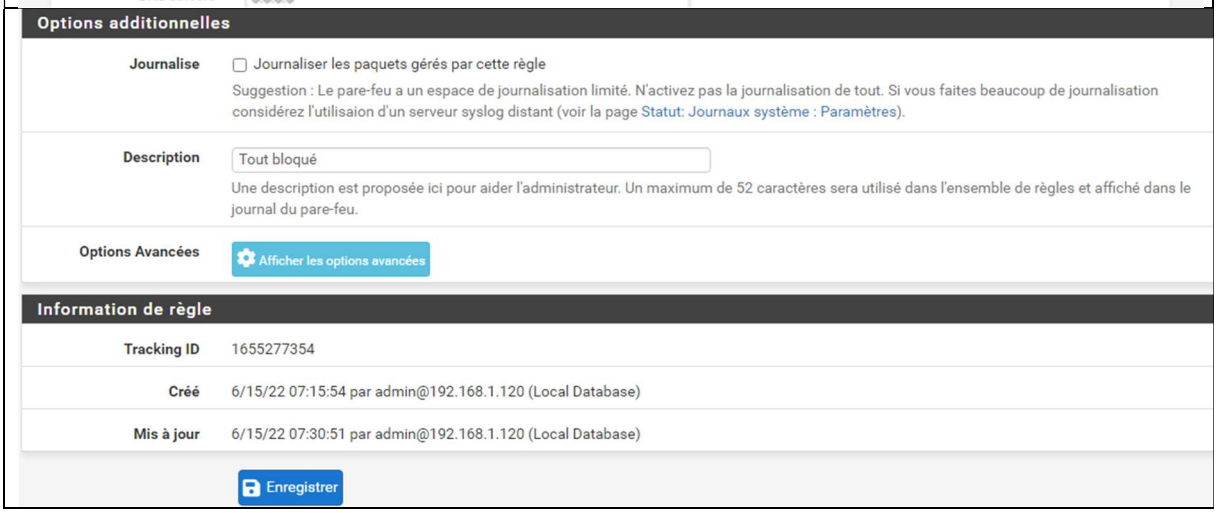


Par défaut le login est : admin et le MDP est : pfsense

Dans la partie pfsense setup, on va activer juste le dhcp puis on valide.

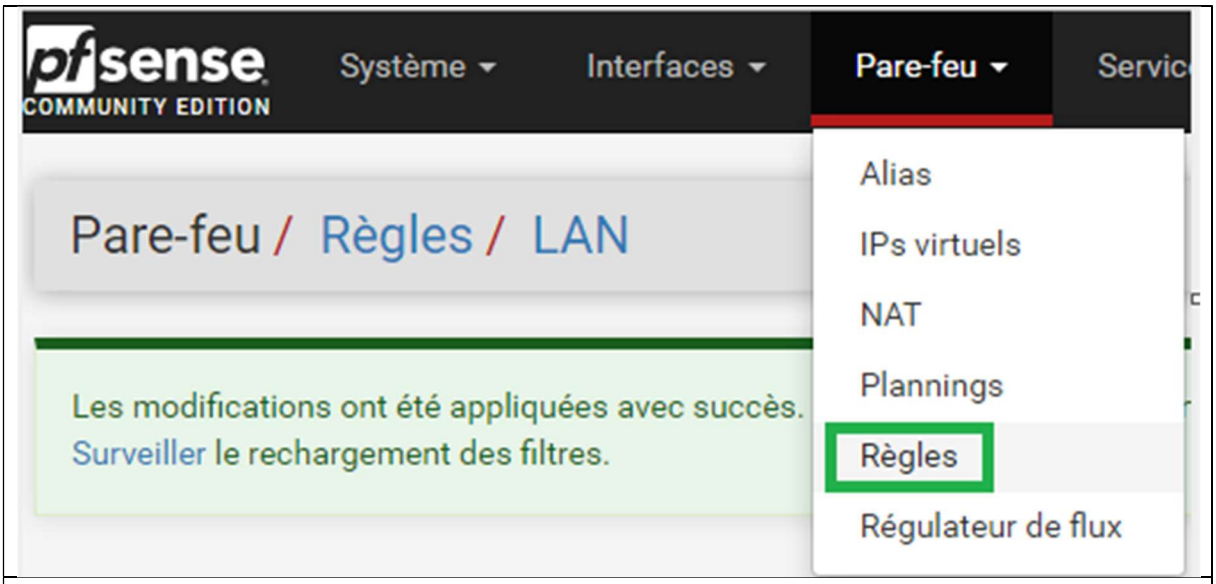



hcp.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / DHCP Server / LAN
The changes have been applied successfully.
LAN
General Options
Enable
Enable DHCP server on LAN interface
BOOTP
Ignore BOOTP queries
Deny unknown clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
Ignore denied clients
Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers
If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet
192.168.1.0
Subnet mask
255.255.255.0
Available range
192.168.1.1 - 192.168.1.254
Range
192.168.1.10
From
192.168.1.245
To
Additional Pools
Add
Add pool
If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.
Pool Start
Pool End
Description
Actions
Servers
WINS servers
WINS Server 1
WINS Server 2
DNS servers
8.8.8.8

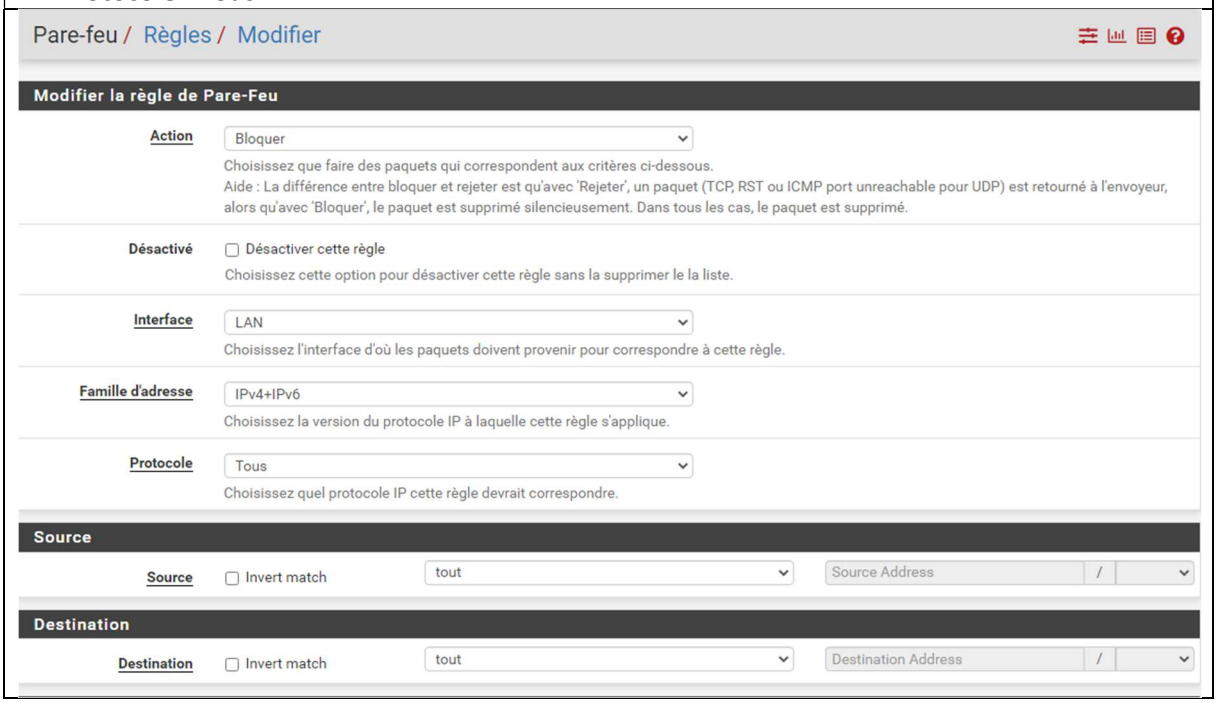

Options additionnelles
Journalise
Journaliser les paquets gérés par cette règle
Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisaion d'un serveur syslog distant (voir la page Statut: Journaux système : Paramètres).
Description
Tout bloqué
Une description est proposée ici pour aider l'administrateur. Un maximum de 52 caractères sera utilisé dans l'ensemble de règles et affiché dans le journal du pare-feu.
Options Avancées
Afficher les options avancées
Information de règle
Tracking ID
1655277354
Créé
6/15/22 07:15:54 par admin@192.168.1.120 (Local Database)
Mis à jour
6/15/22 07:30:51 par admin@192.168.1.120 (Local Database)
Enregistrer

4.Création règle « deny all »

Onglet « Pare-feu » choisir « règles »



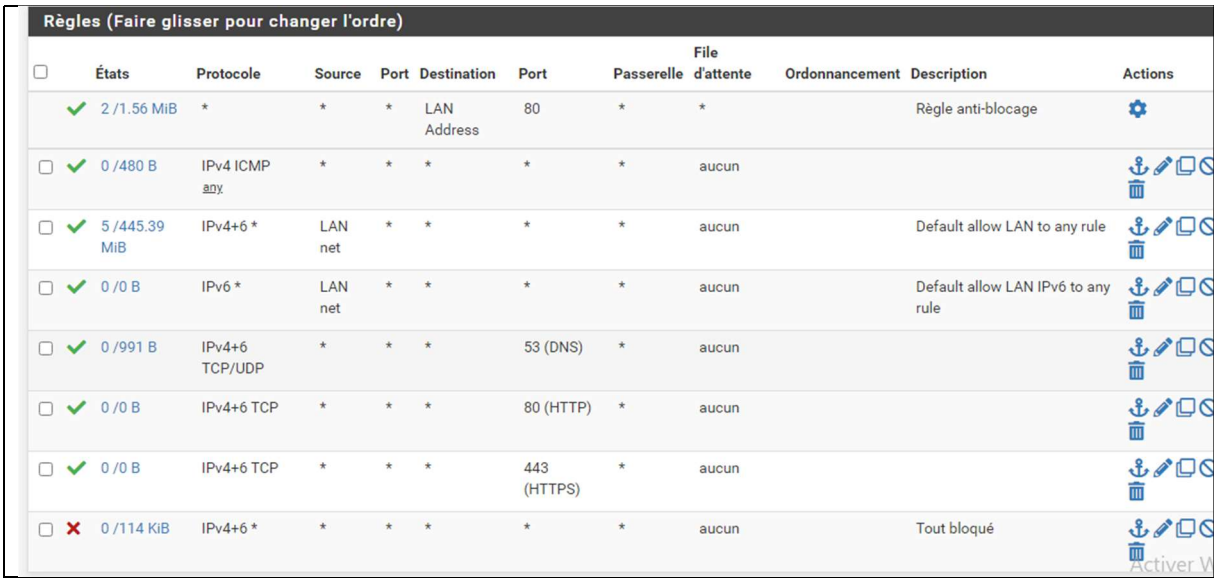
Choisir action : bloquer
Interface : LAN
Famille d'ad : IPv4+IPv6
Protocole : Tous



5. Autoriser accès internet

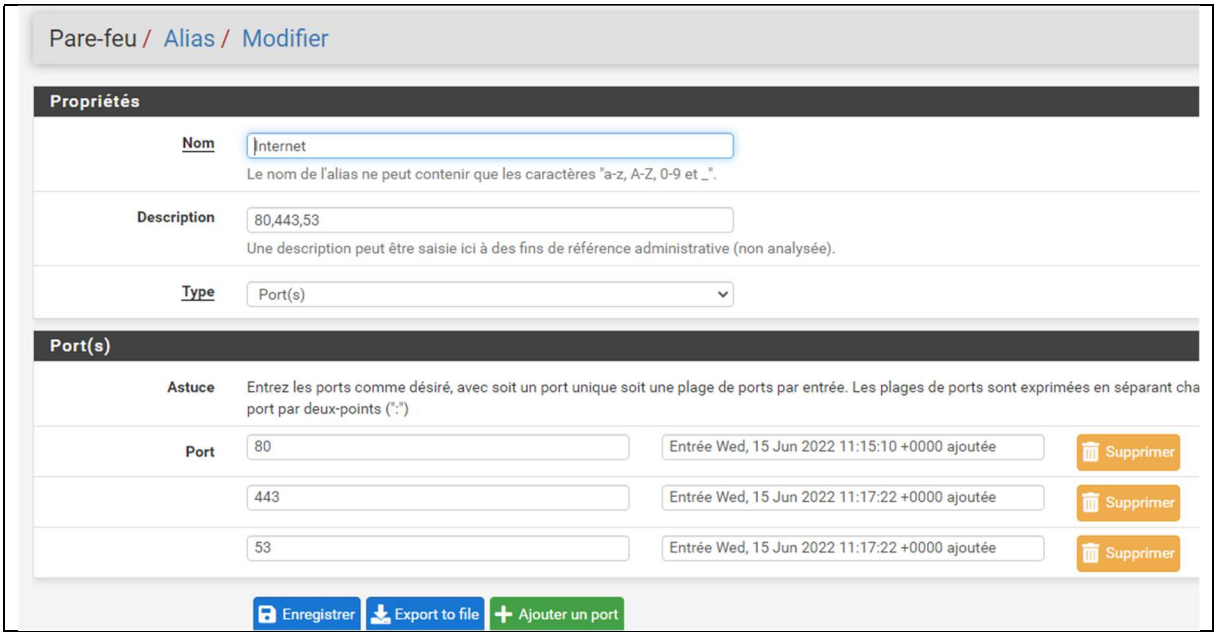
Il s'agit de créer 3 règles pour autoriser les port 80 (http) Protocol TCP, 443(http/s) Protocole TCP et 53(dns) protocole TCP/UDP puis une dernière pour autoriser le Protocole ICMP(ping).

On va également créer une règle avec le protocole ICMP pour autoriser le ping.

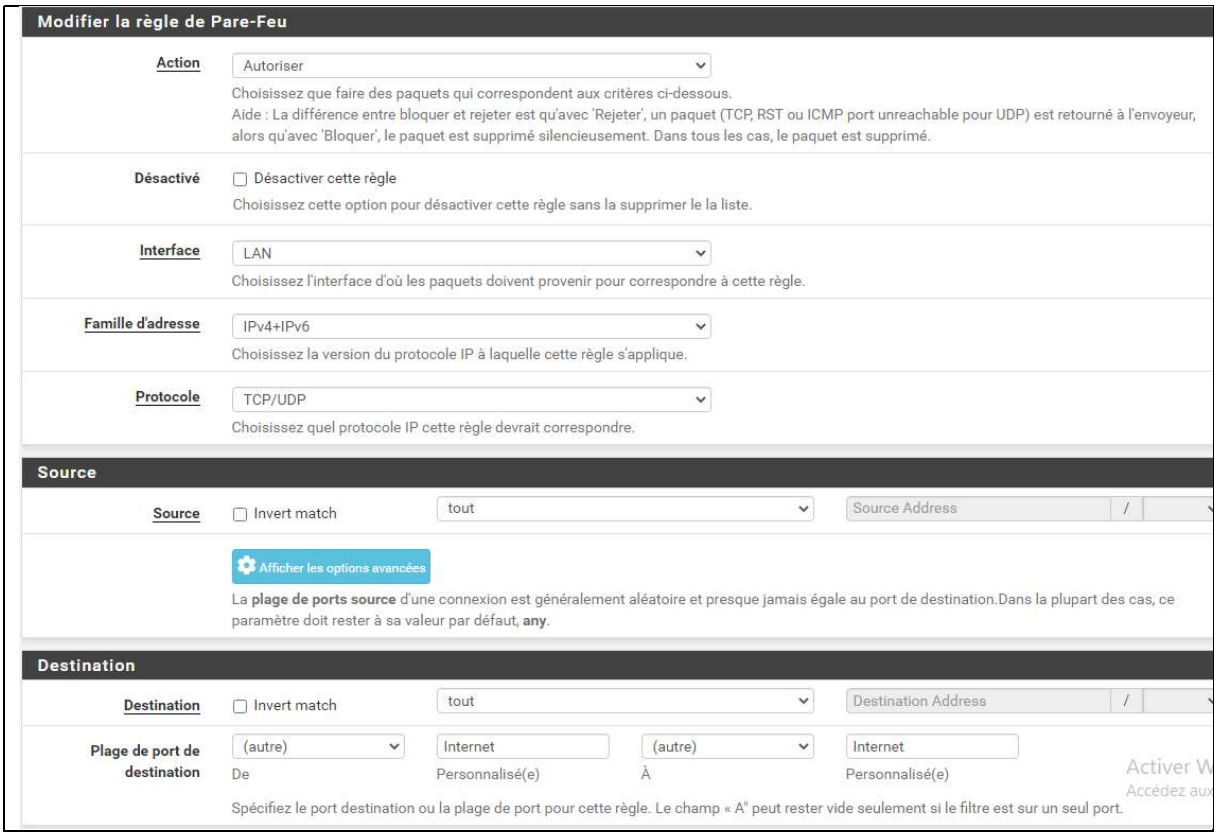


6.Alias

Il existe une autre façon de faire, plutôt que de créer 3 règles, on peut regrouper les ports sous un alias. Ex : les ports 80 , 443, 53 sous l'allias « internet » qu'on peut créer dans l'onglet « Pare-feu » puis « Alias » et sélectionner « Ports » puis « ajouter »



Puis ajouter une règle dans « règles »


Modifier la règle de Pare-Feu
Action
Autoriser
Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'envoyeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.
Désactivé
Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer le la liste.
Interface
LAN
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.
Famille d'adresse
IPv4+IPv6
Choisissez la version du protocole IP à laquelle cette règle s'applique.
Protocole
TCP/UDP
Choisissez quel protocole IP cette règle devrait correspondre.
Source
Source
Invert match
tout
Source Address
/
Afficher les options avancées
La plage de ports source d'une connexion est généralement aléatoire et presque jamais égale au port de destination.Dans la plupart des cas, ce paramètre doit rester à sa valeur par défaut, any.
Destination
Destination
Invert match
tout
Destination Address
/
Plage de port de destination
(autre)
Internet
(autre)
Internet
De
Personnalisé(e)
À
Personnalisé(e)
Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A" peut rester vide seulement si le filtre est sur un seul port.