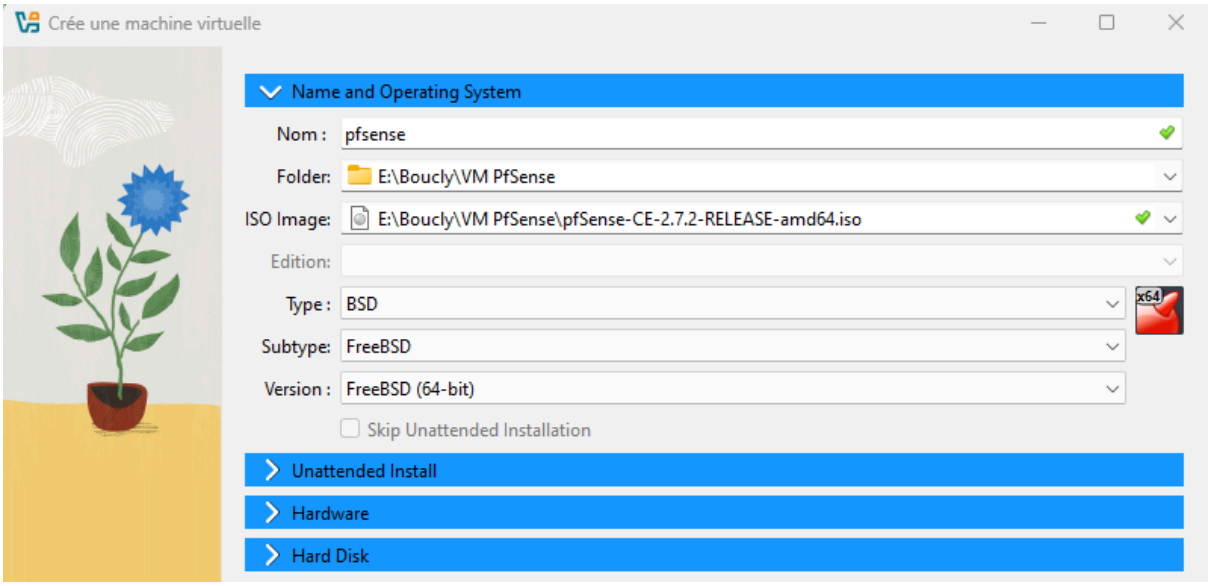
Chapitre 12 – Nouvelle passerelle de sécurité PfSense

1. Création de la VM PfSense.

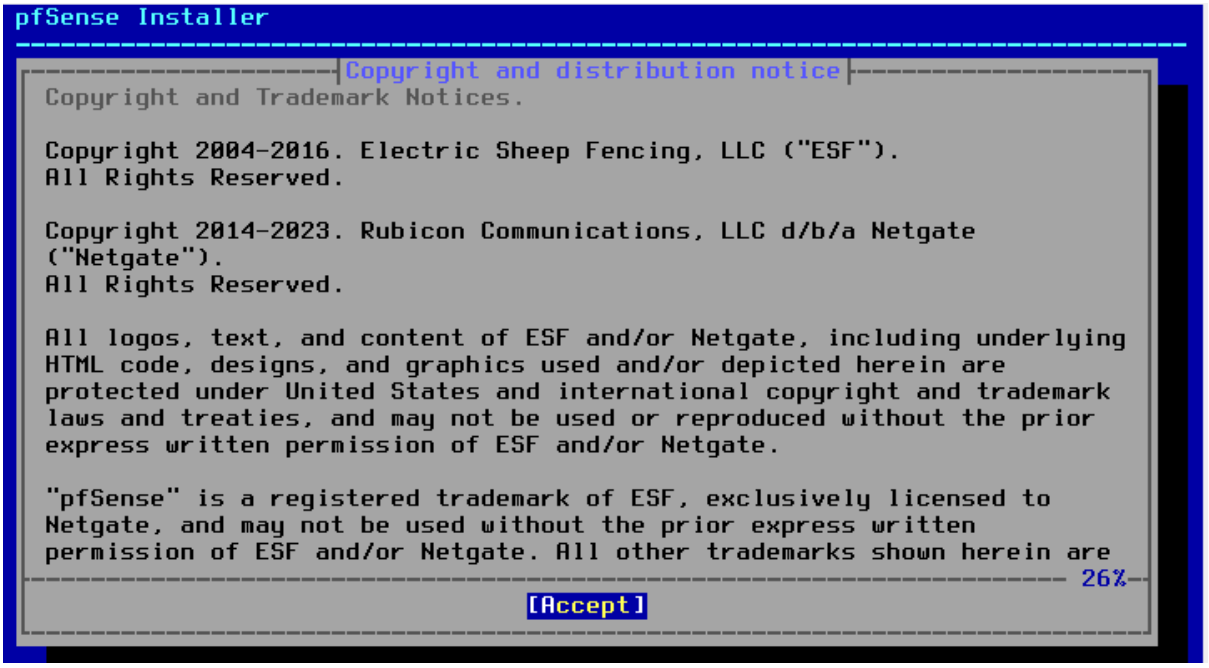
• RAM : 2 Go ; HD : 32 Go
• Iso : pfSense-CE-2.7.2-RELEASE-amd64

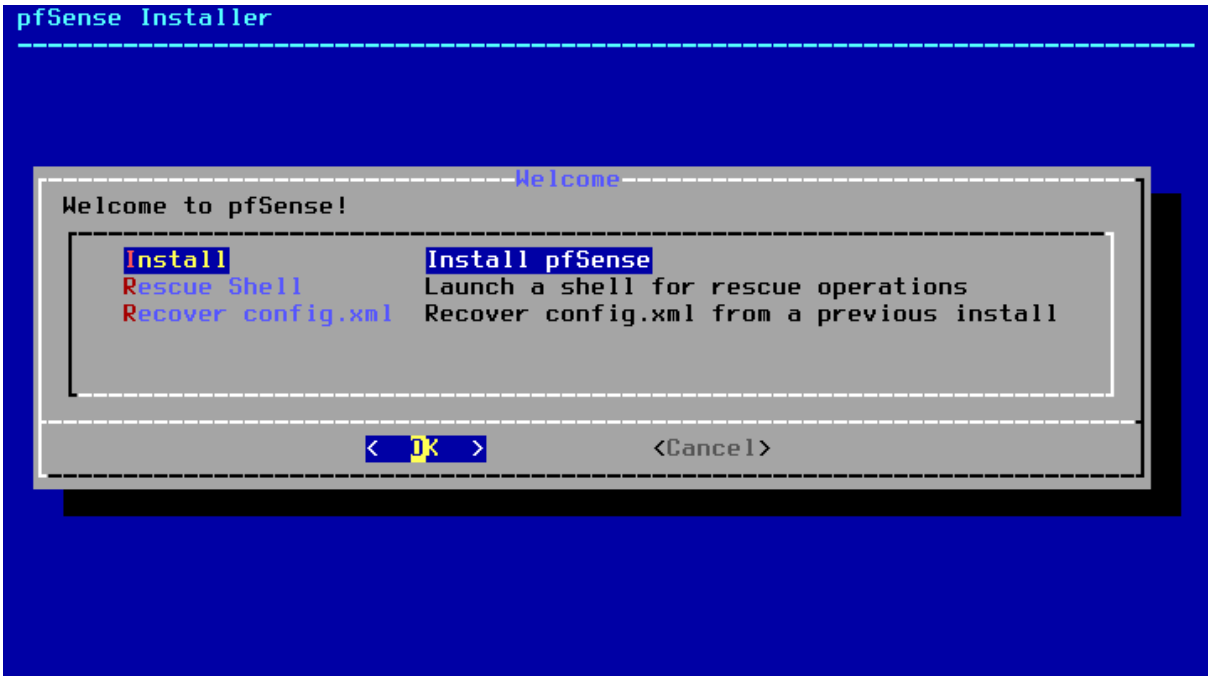
https://provya.net/?d=2024/05/28/10/37/02-installer-pfsense#telecharger-pfsense
https://repo.ialab.dsu.edu/pfsense/)

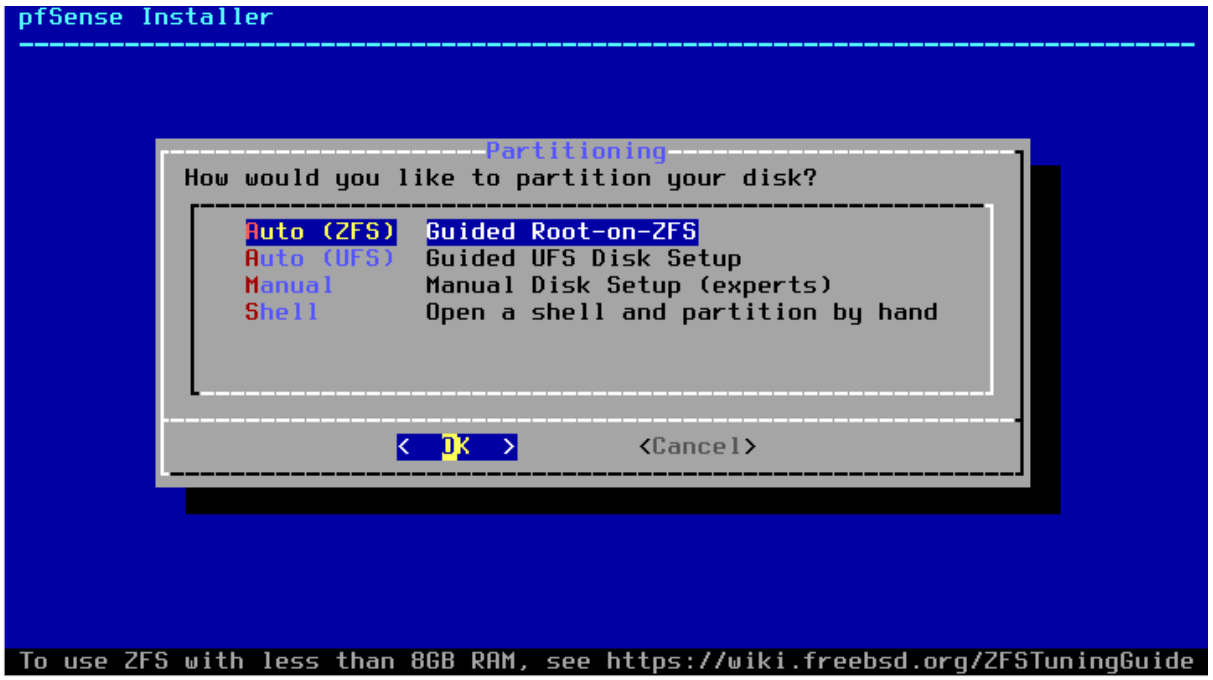
• 3 NIC à l'instar de la machine US3 :
- em0 : accès pont
- em1 : réseau interne (DMZ)
- em2 : réseau interne (LAN)

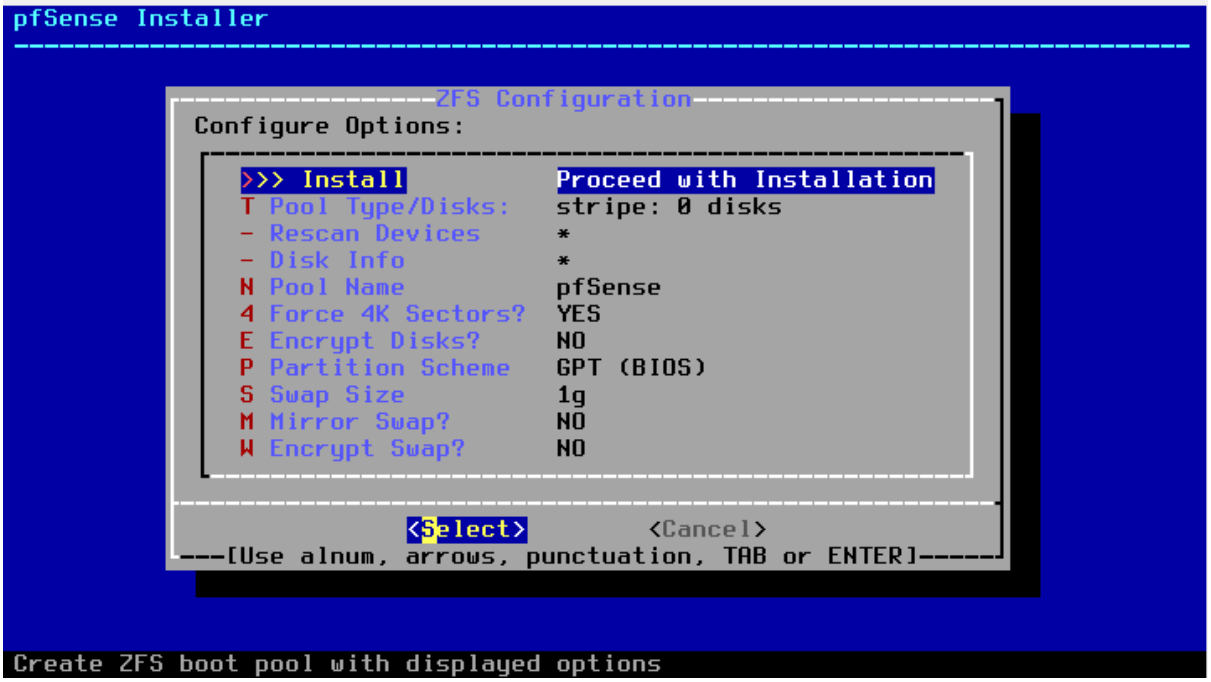


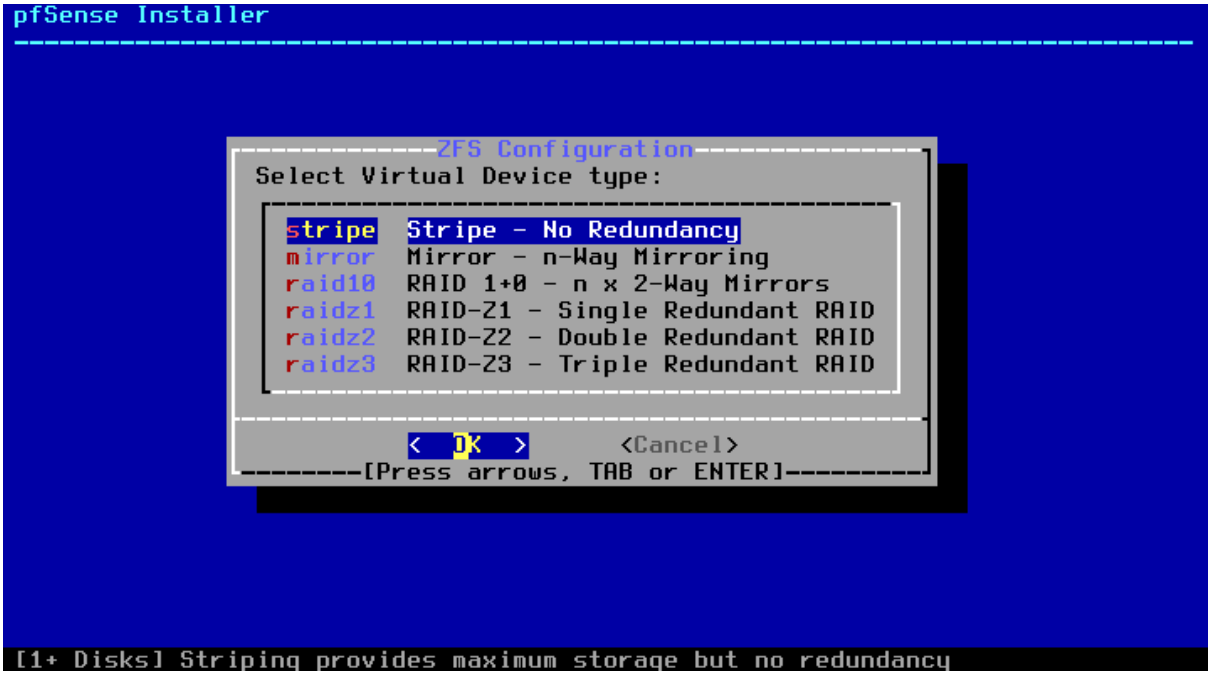
2. Installation du serveur PfSense.

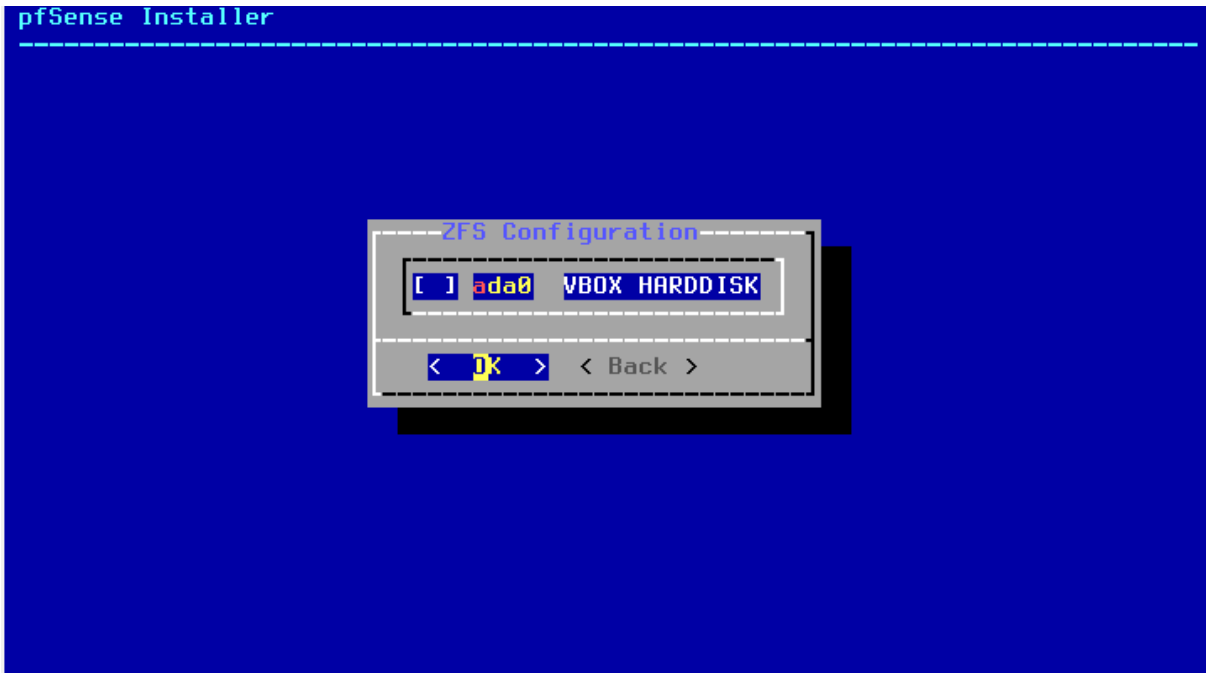


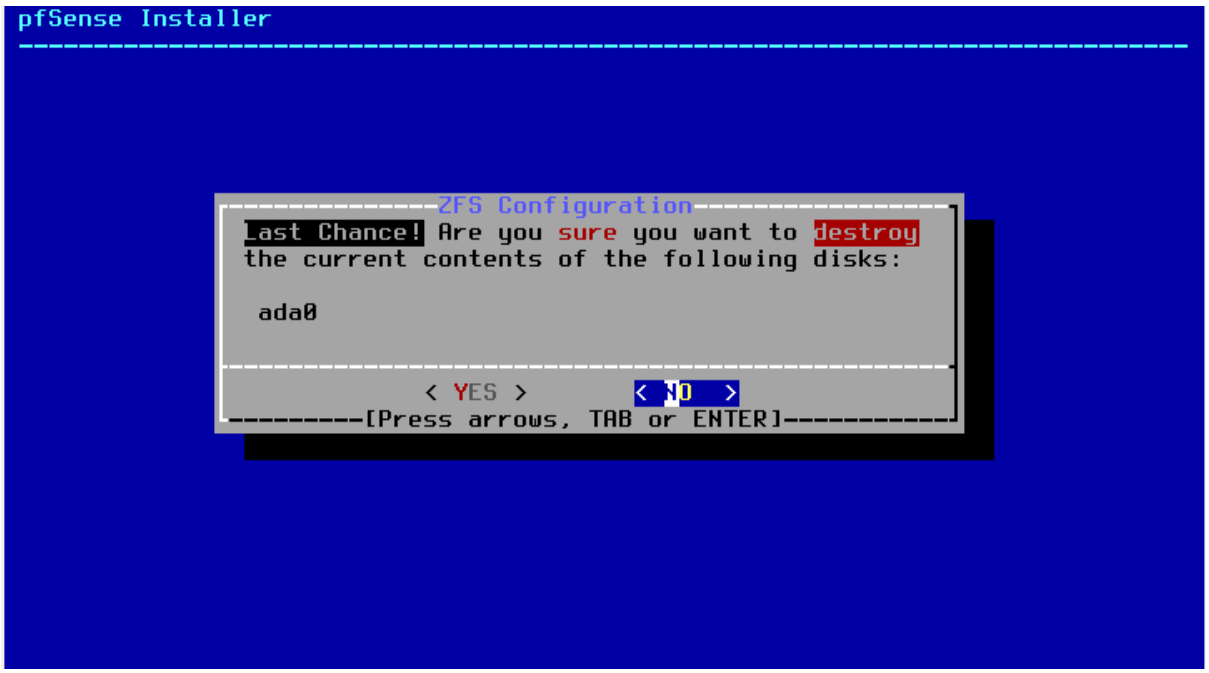


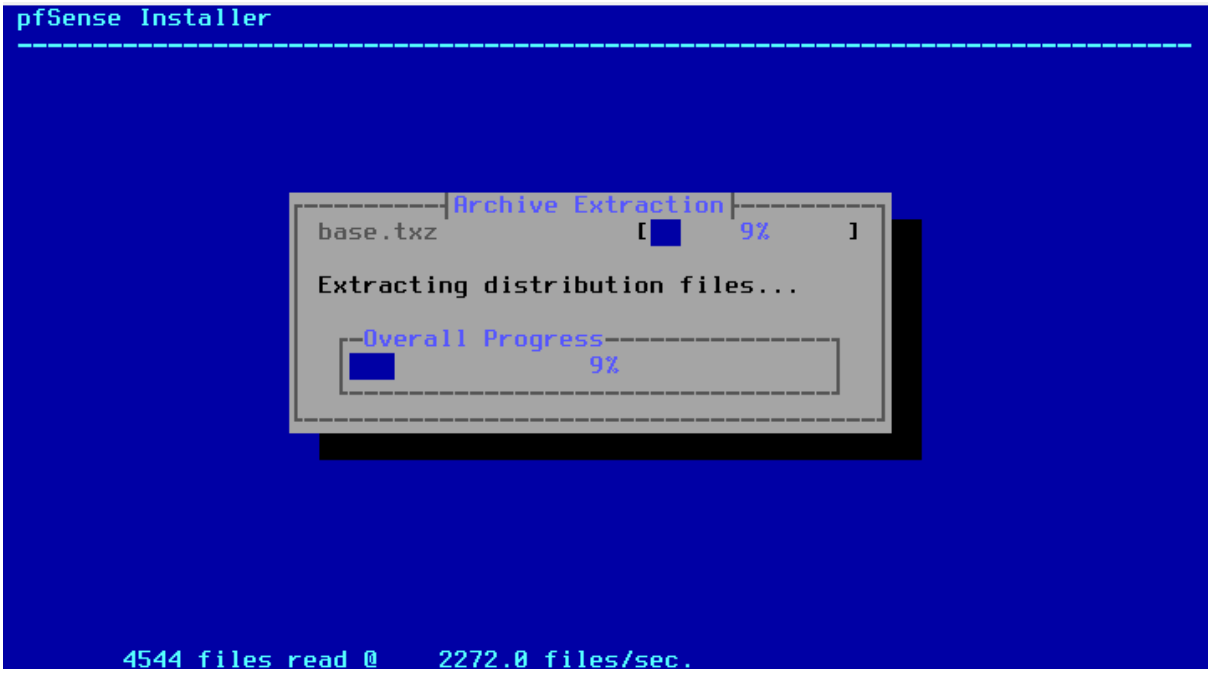

pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) Guided UFS Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuide

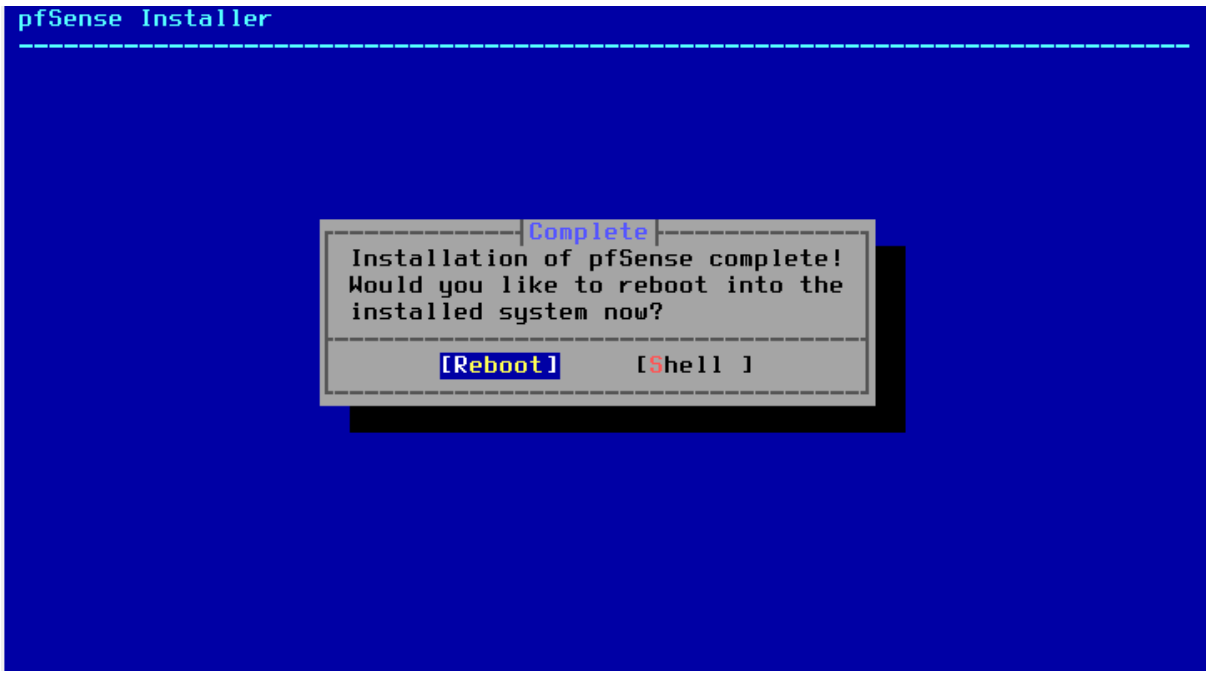

pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options


pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK >
<Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy


pfSense Installer
ZFS Configuration
[ ] ada0 VBOX HARDDISK
< OK >
< Back >


pfSense Installer
ZFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
ada0
< YES >
< NO >
[Press arrows, TAB or ENTER]


pfSense Installer
Archive Extraction
base.txz
9%
Extracting distribution files...
Overall Progress
9%
4544 files read @ 2272.0 files/sec.




```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.17.5.9/16
 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:
```

3. Configuration des cartes réseau.

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.17.5.9/16
 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: 1
```

```
Valid interfaces are:

em0     08:00:27:e3:39:18   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1     08:00:27:e4:e0:cf   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2     08:00:27:65:71:6d (down) 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
```

```
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): em2

Enter the Optional 1 interface name or 'a' for auto-detection
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em2
OPT1 -> em1

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

```
OPT1 -> em1

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.17.5.9/16
 LAN (lan)       -> em2        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> 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: 2
```

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1)

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

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.3.254

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:
>

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

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

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

```
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) n
```

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

The IPv4 LAN address has been set to 192.168.3.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.3.254/

Press <ENTER> to continue.
```

```
The IPv4 LAN address has been set to 192.168.3.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.3.254/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.17.5.9/16
 LAN (lan)       -> em2        -> v4: 192.168.3.254/24
 OPT1 (opt1)     -> 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: 2
```

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1)

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

```
Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.2.254

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 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:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

```
The IPv4 OPT1 address has been set to 192.168.2.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.2.254/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.17.5.9/16
 LAN (lan)       -> em2        -> v4: 192.168.3.254/24
 OPT1 (opt1)     -> em1        -> v4: 192.168.2.254/24

 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: 2
```

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1 - static)

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

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

Réseau SIO : 172.17.0.0/16 ; GW : 172.17.250.2

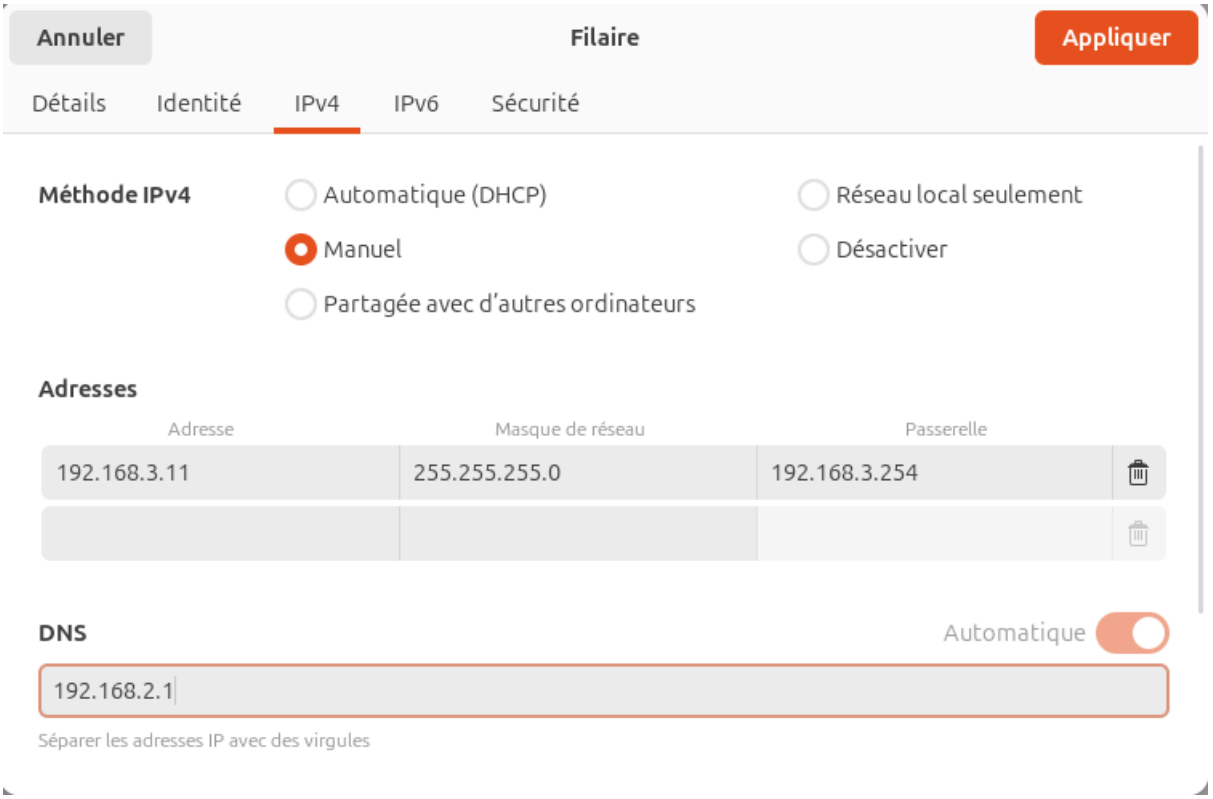
```
Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 172.17.101.1

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 WAN IPv4 subnet bit count (1 to 32):
> 16

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.17.250.2

Should this gateway be set as the default gateway? (y/n) y
```

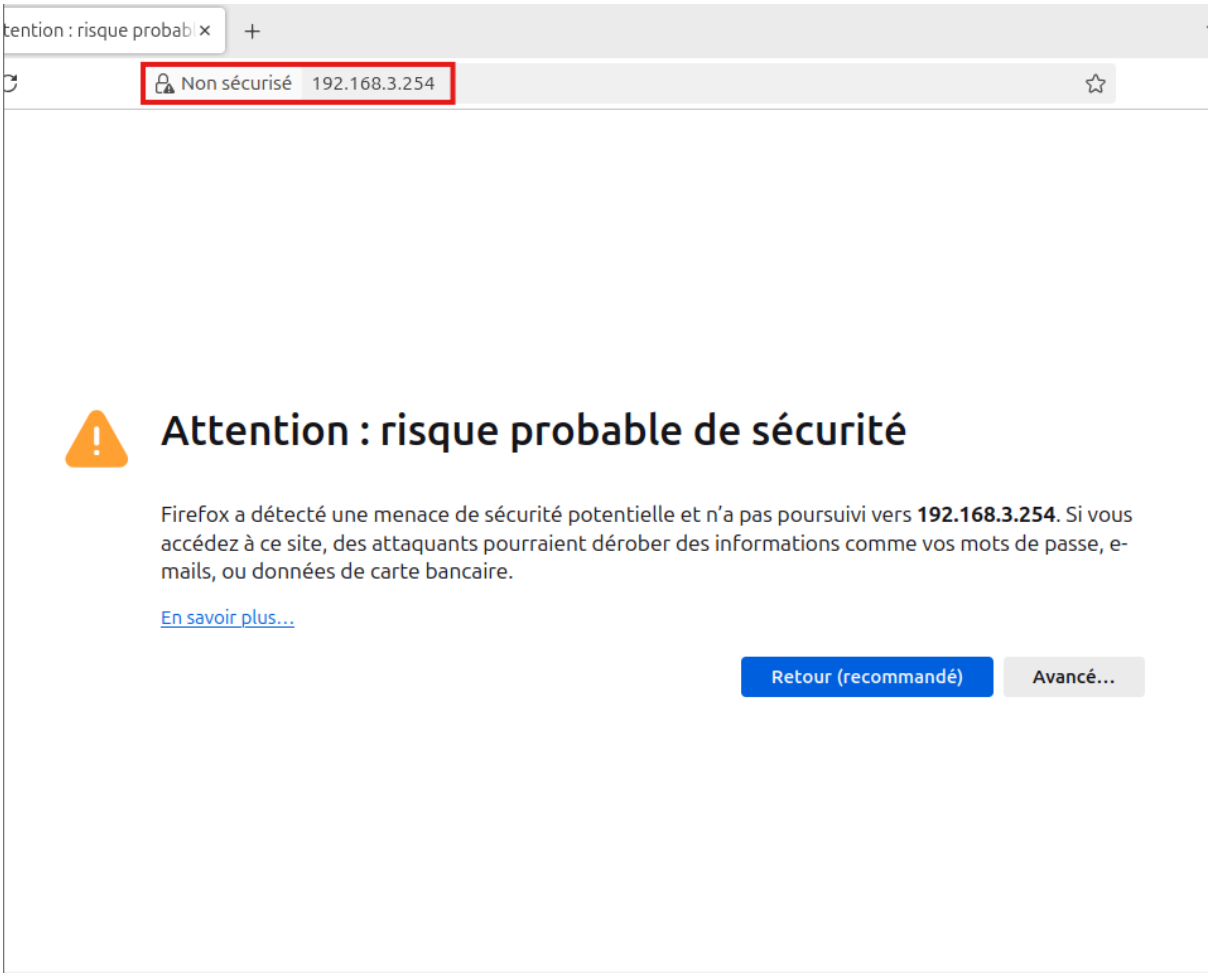
```
Configure IPv6 address WAN interface via DHCP6? (y/n) n

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

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

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

```
The IPv4 WAN address has been set to 172.17.101.1/16

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 172.17.101.1/16
 LAN (lan)       -> em2        -> v4: 192.168.3.254/24
 OPT1 (opt1)     -> em1        -> v4: 192.168.2.254/24
```

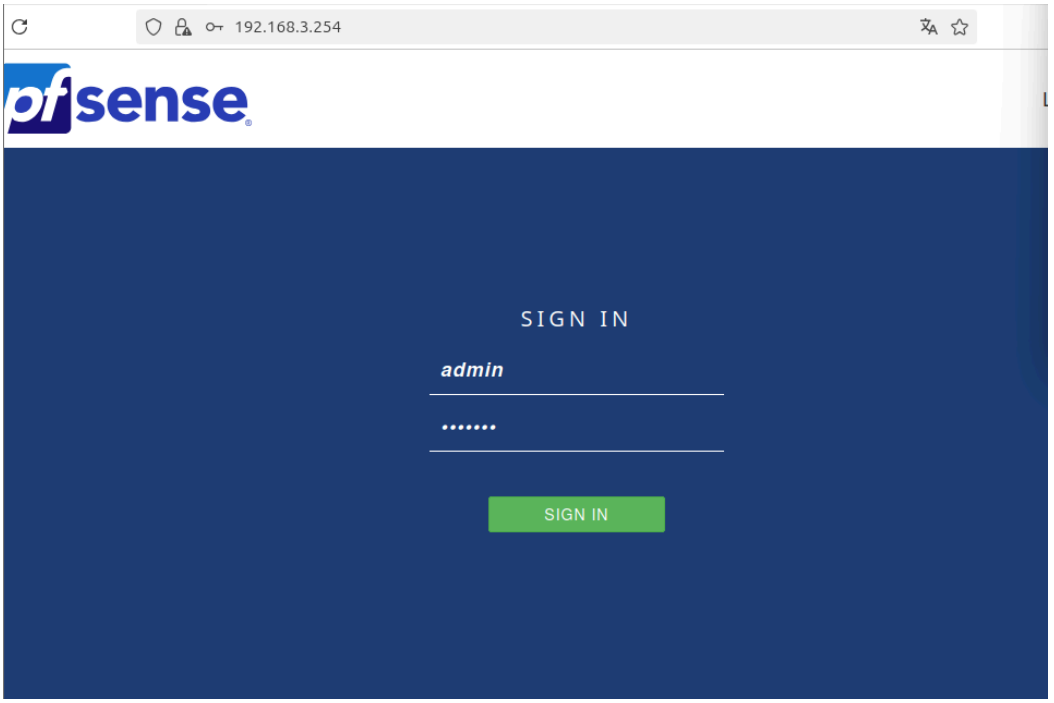
4. Configuration générale depuis la Web GUI.

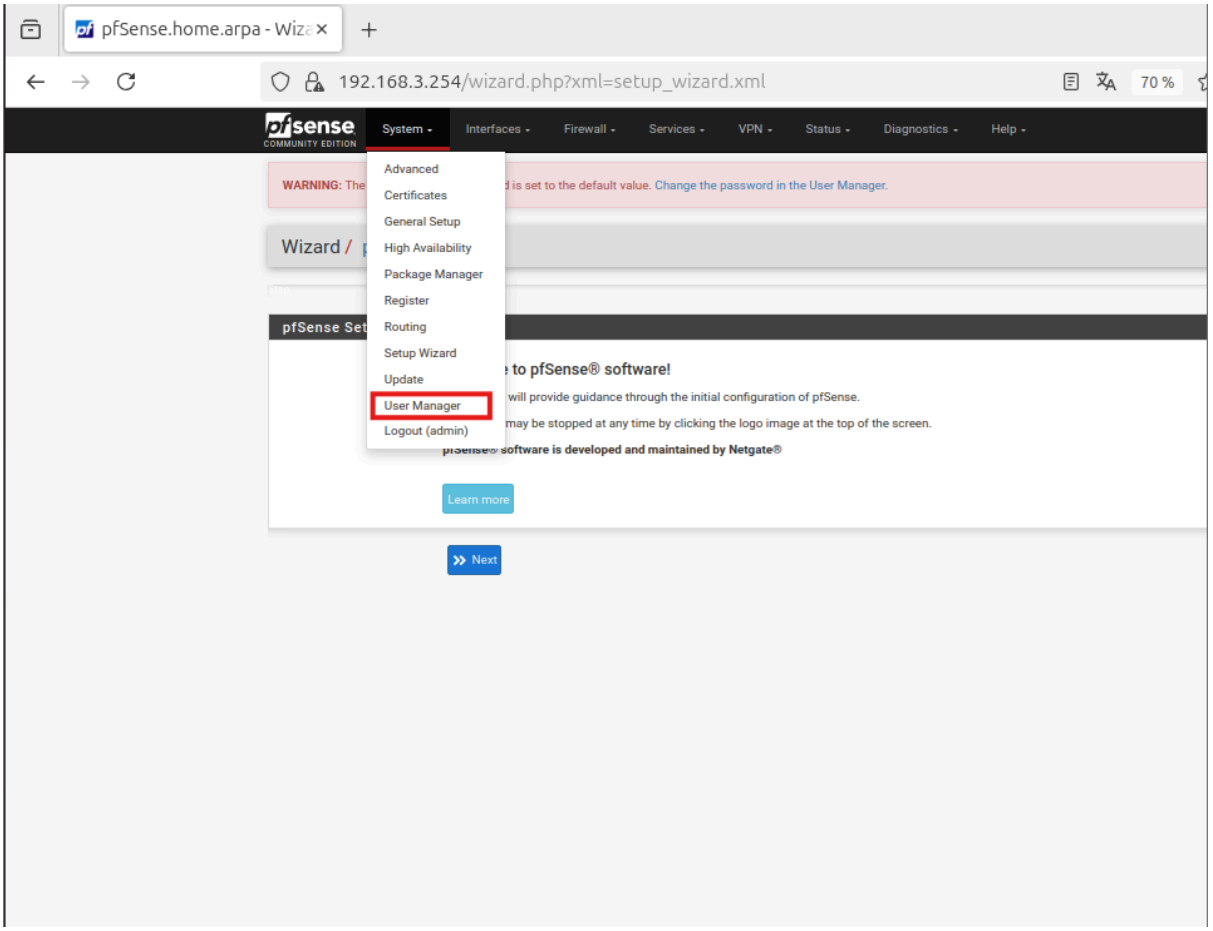
Nous accédons à l'interface Web de PfSense depuis le LAN avec UD1. Nous accédons également à l'interface Web de PfSense depuis le LAN avec UD1 :

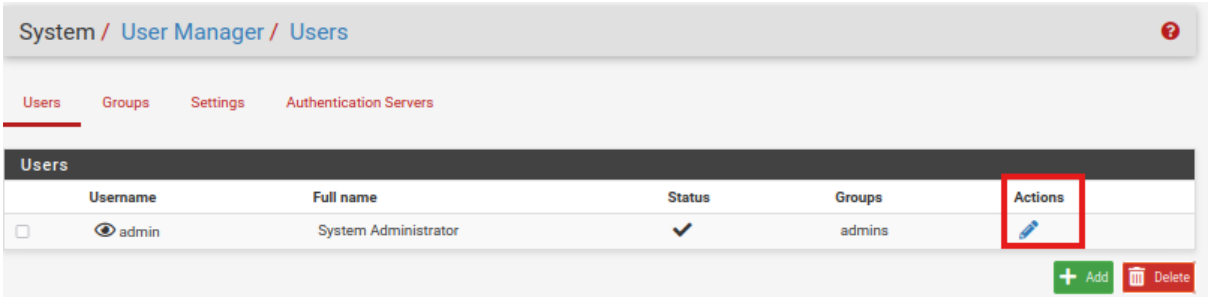




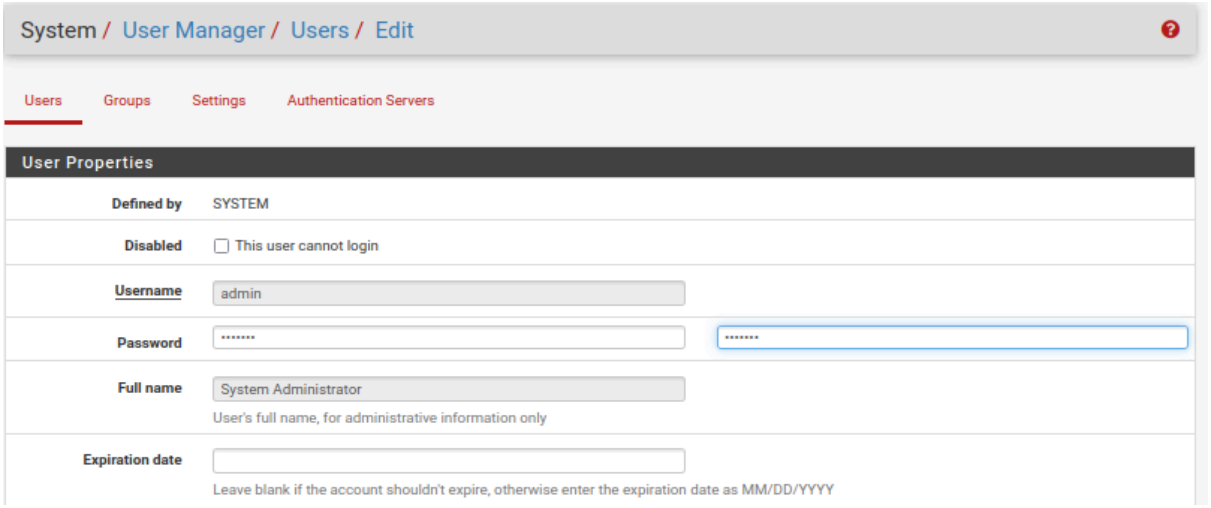
Login : admin ; mot de passe : pfsense

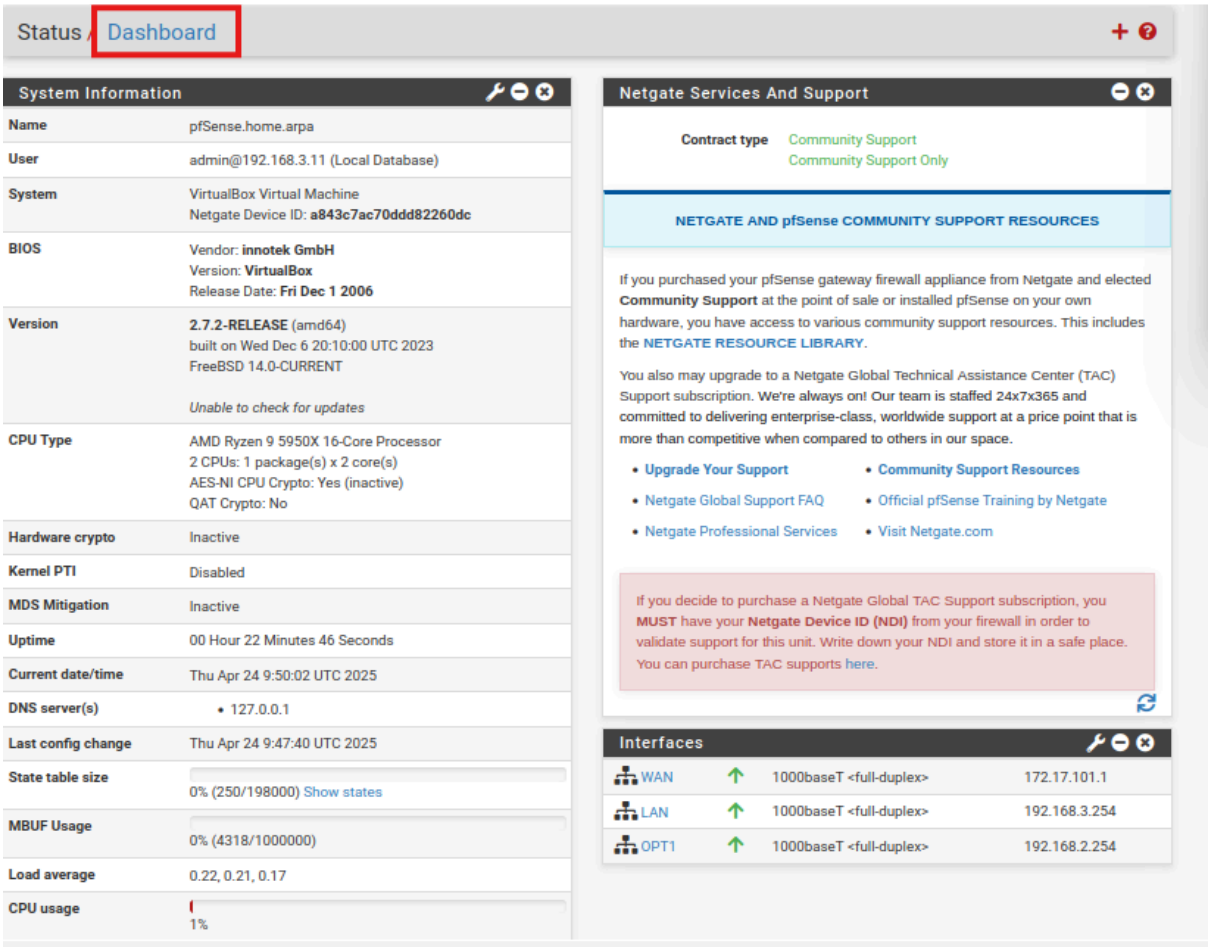


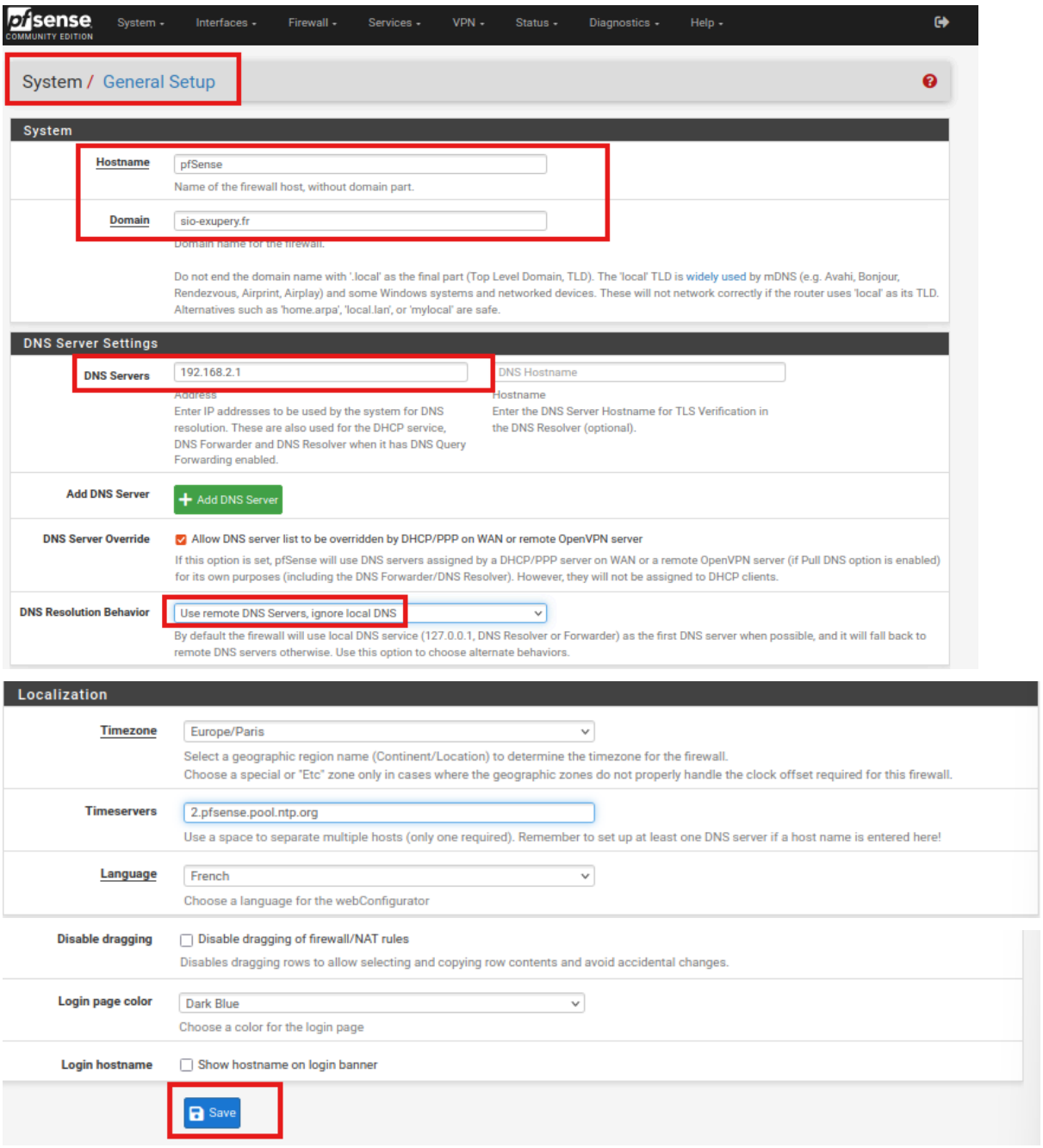

pfSense.home.arpa - Wiz
192.168.3.254/wizard.php?xml=setup_wizard.xml
70 %
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Advanced
Certificates
General Setup
High Availability
Package Manager
Register
Routing
Setup Wizard
Update
User Manager
Logout (admin)
WARNING: The
is set to the default value. Change the password in the User Manager.
Wizard /
pfSense Set
to pfSense® software!
will provide guidance through the initial configuration of pfSense.
may be stopped at any time by clicking the logo image at the top of the screen.
software is developed and maintained by Netgate®
Learn more
Next

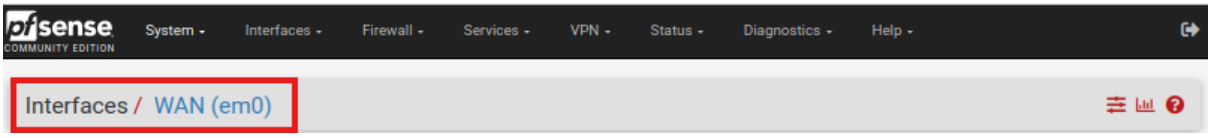

System / User Manager / Users
Users
Groups
Settings
Authentication Servers
Users
Username
Full name
Status
Groups
Actions
admin
System Administrator
admins
Add
Delete

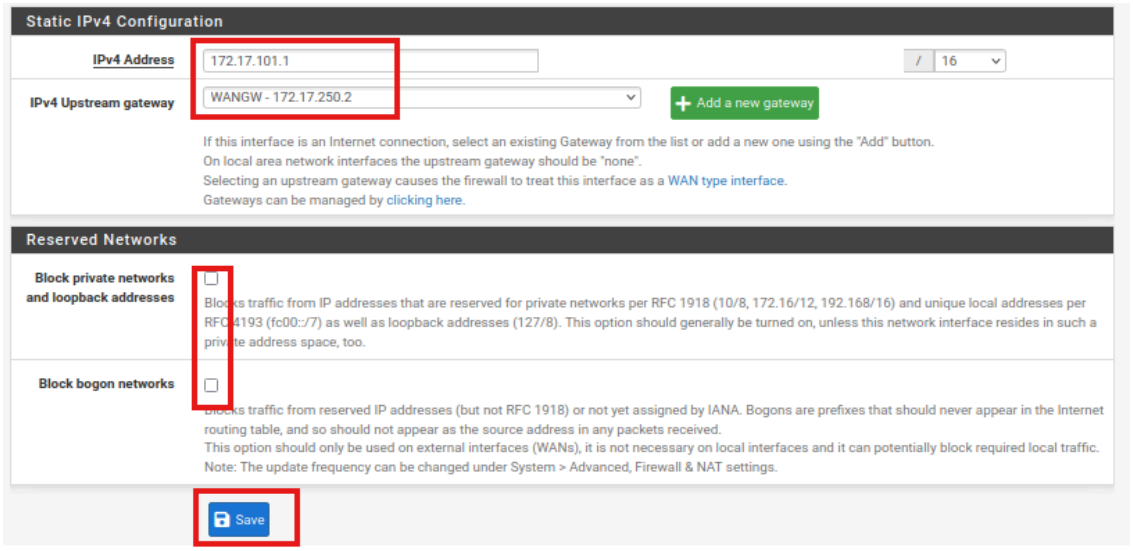
Nous modifions le mot de passe du compte admin : Azerty0 (pas de capture mais le mdp a été sauvegardé

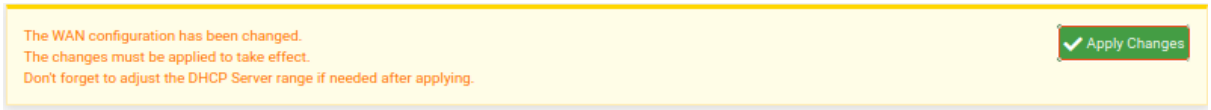




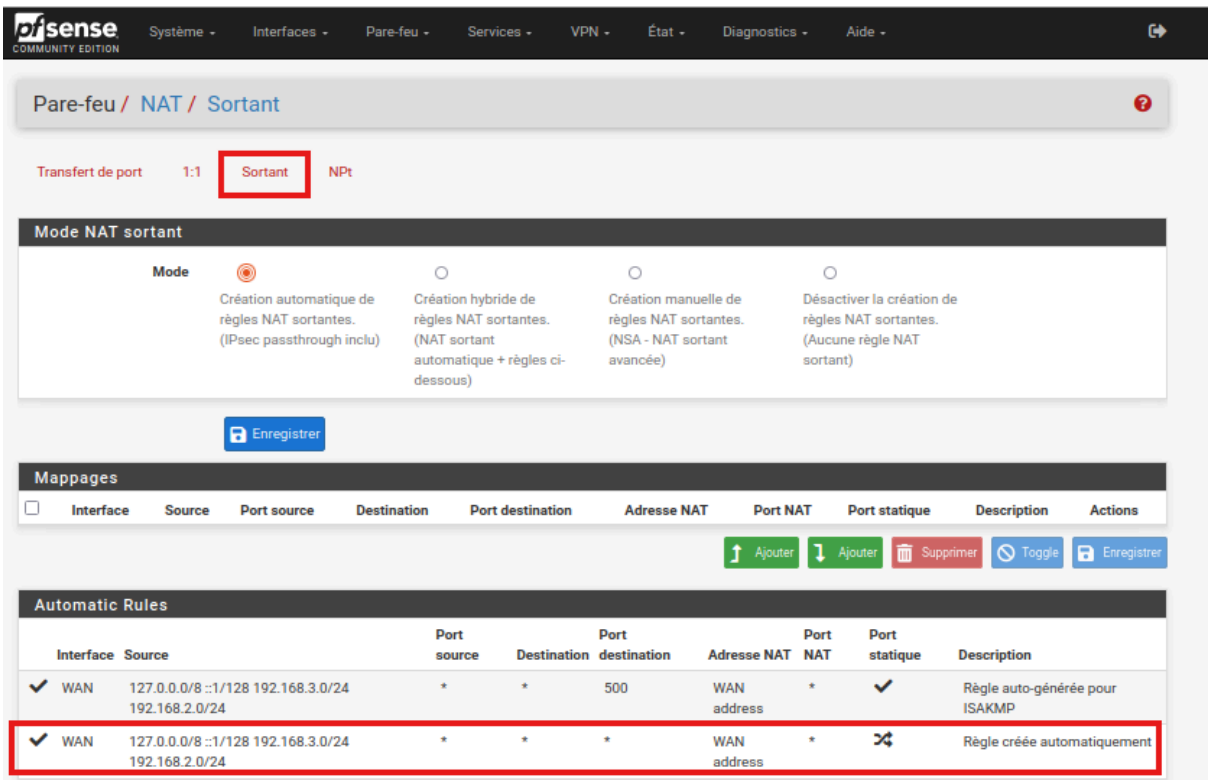

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
System / General Setup
System
Hostname
pfSense
Name of the firewall host, without domain part.
Domain
sio-exupery.fr
Domain name for the firewall.
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
DNS Server Settings
DNS Servers
192.168.2.1
Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.
DNS Hostname
Hostname
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).
Add DNS Server
Add DNS Server
DNS Server Override
Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.
DNS Resolution Behavior
Use remote DNS Servers, ignore local DNS
By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.
Localization
Timezone
Europe/Paris
Select a geographic region name (Continent/Location) to determine the timezone for the firewall.
Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.
Timeservers
2.pfsense.pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!
Language
French
Choose a language for the webConfigurator
Disable dragging
Disable dragging of firewall/NAT rules
Disables dragging rows to allow selecting and copying row contents and avoid accidental changes.
Login page color
Dark Blue
Choose a color for the login page
Login hostname
Show hostname on login banner
Save


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / WAN (em0)



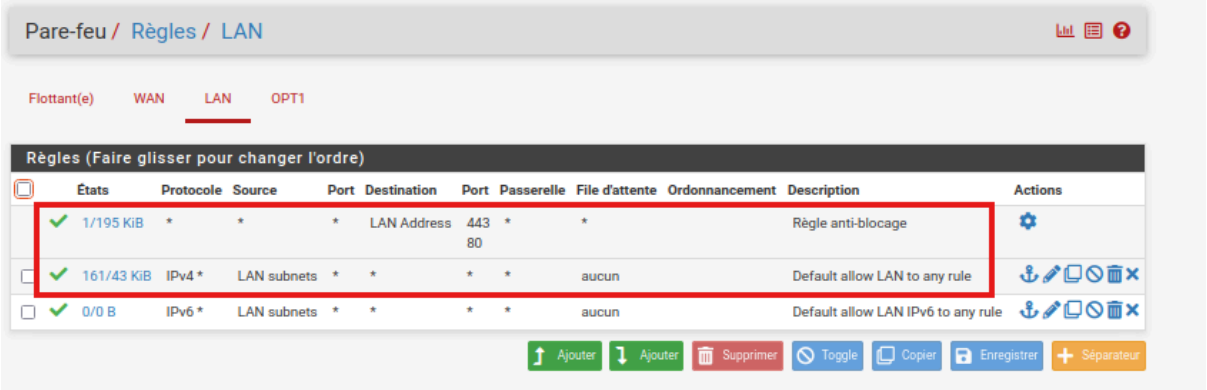


Visualisation de la règle de translation existante. Que permet-elle ?



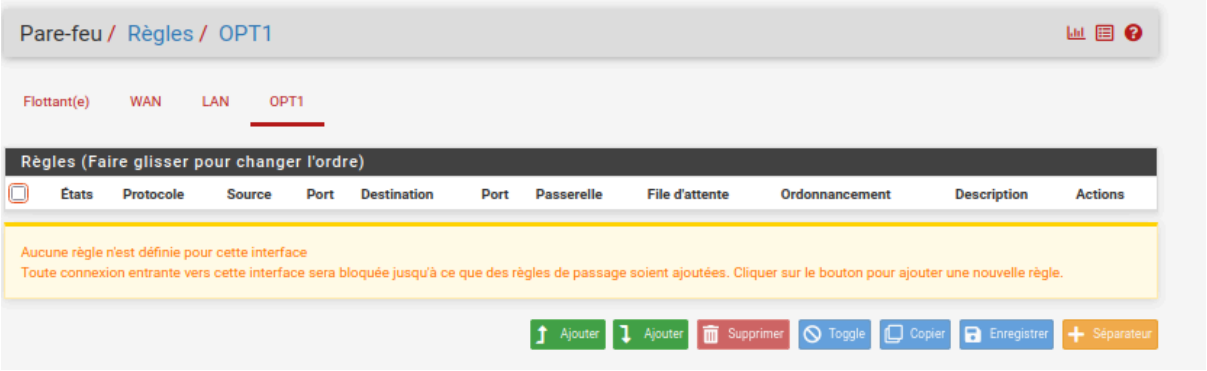
Cette règle NAT permet aux machines des réseaux 192.168.2.0/24,192.168.3.0/24, d'accéder à Internet, en traduisant leur adresse IP source vers l'adresse IP publique du routeur sur l'interface WAN.

Visualisez les règles de pare-feu existantes concernant l'interface LAN. Que permettent-elles ?



Elle permet à tous les appareils du réseau LAN de communiquer librement avec n'importe quelle destination, interne ou externe provenant des ports : 443 (HTTPS) et 80 (HTTP).

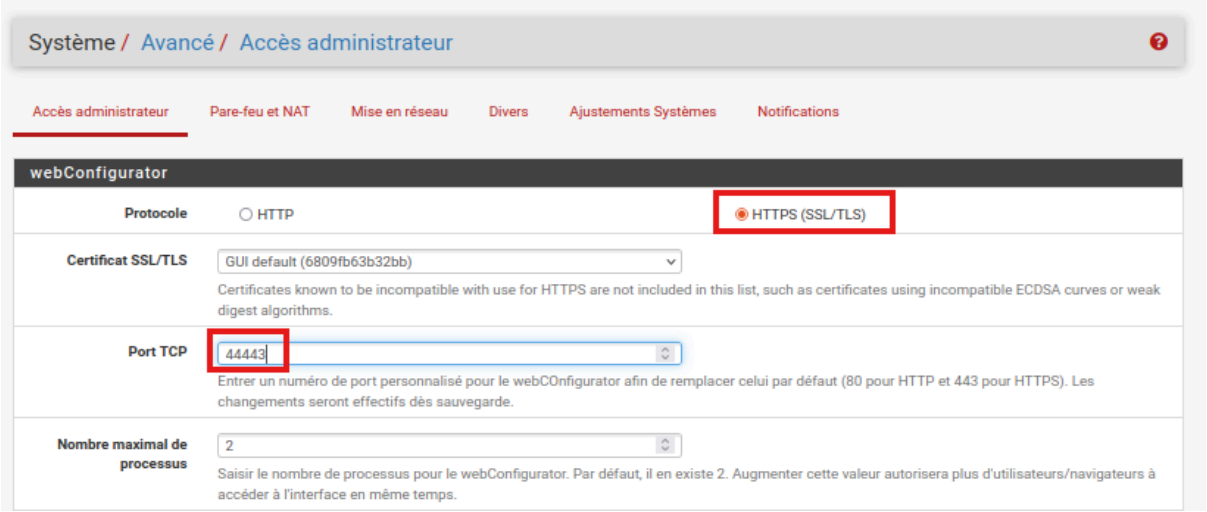
Consultez les règles pour les interfaces OPT1 et WAN. Qu'en déduisez-vous ?



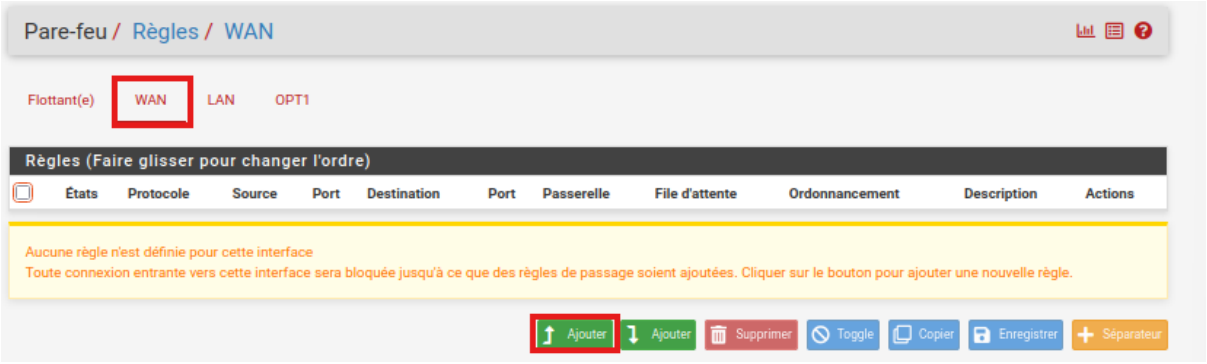
Nous allons appliquer des règles plus tard pour permettre un filtrage

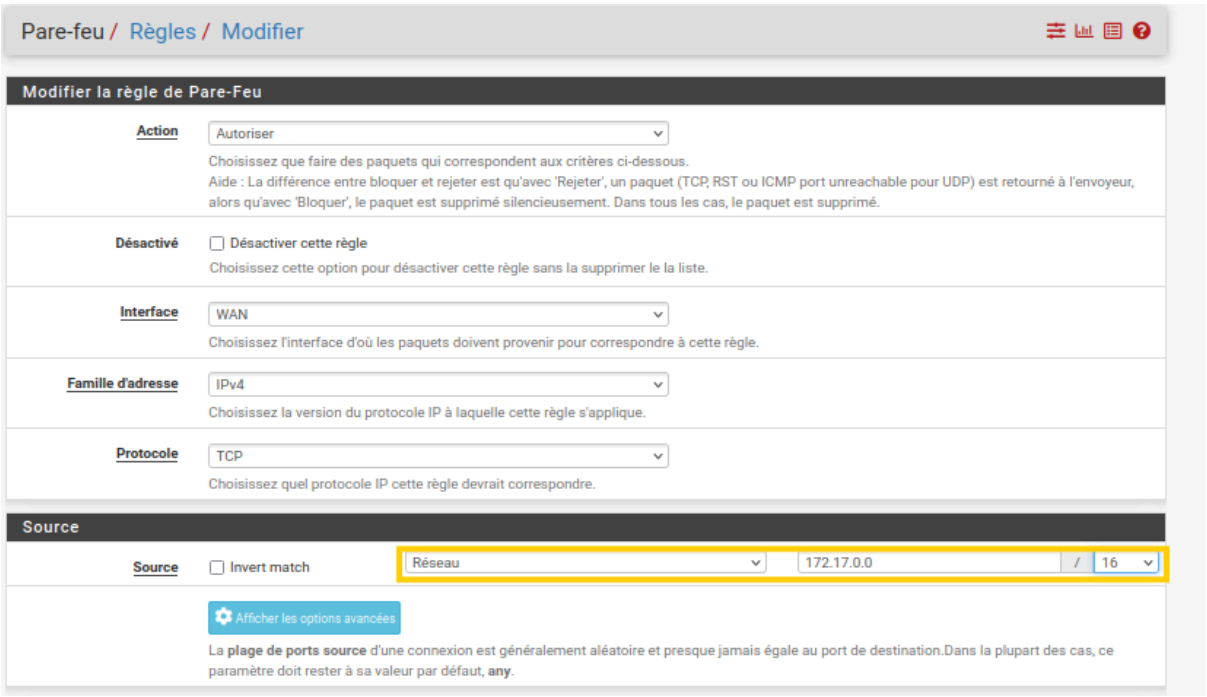
5. Accès à la Web GUI depuis l'interface WAN.

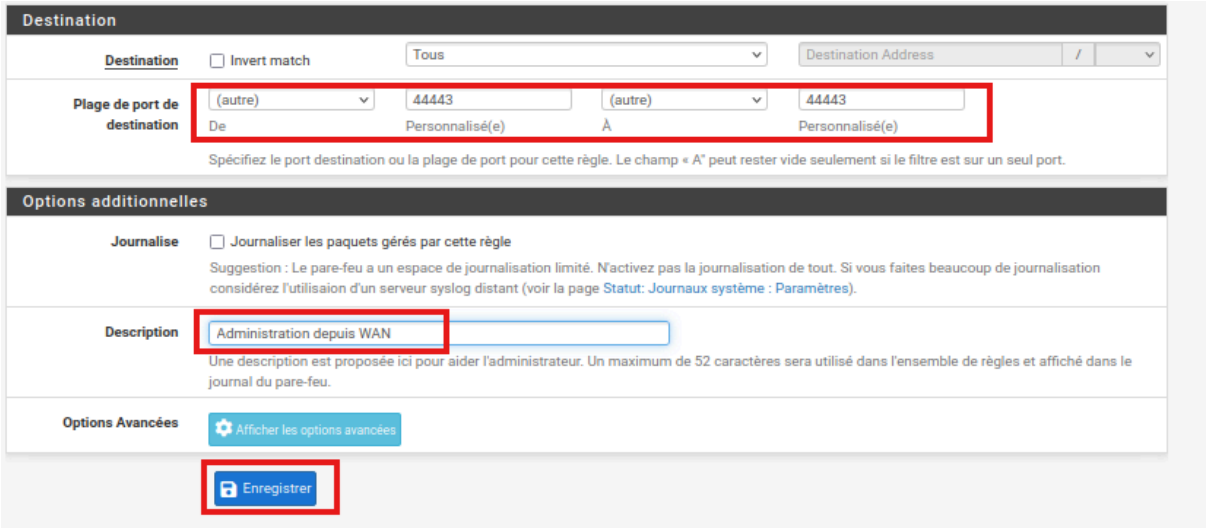
Modification du port de l'interface Web d'administration de Pfsense.

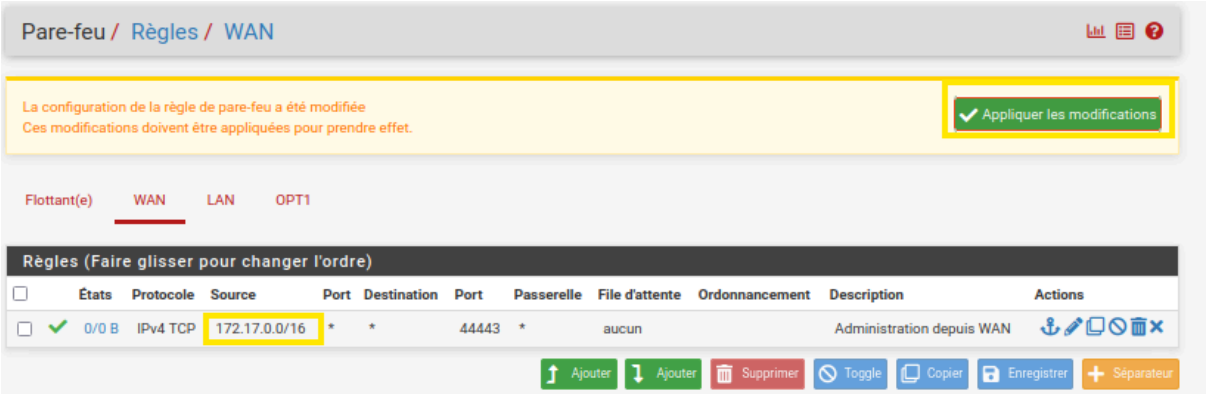


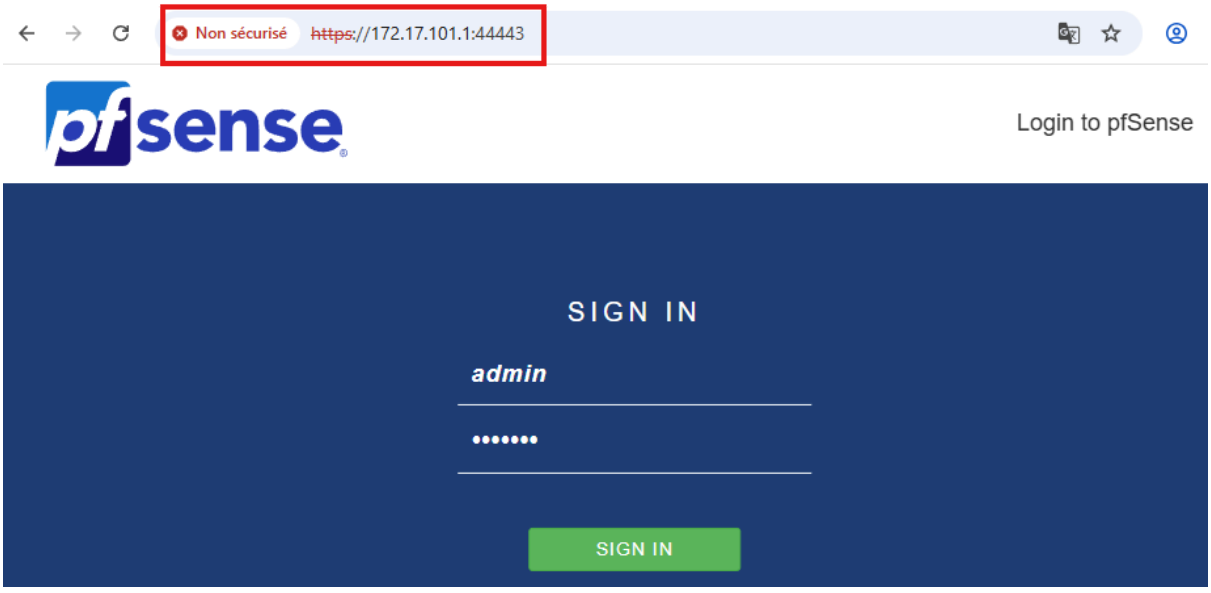
Activation de l'accès à l'interface web depuis WAN (réseau 172.17.0.0/16).





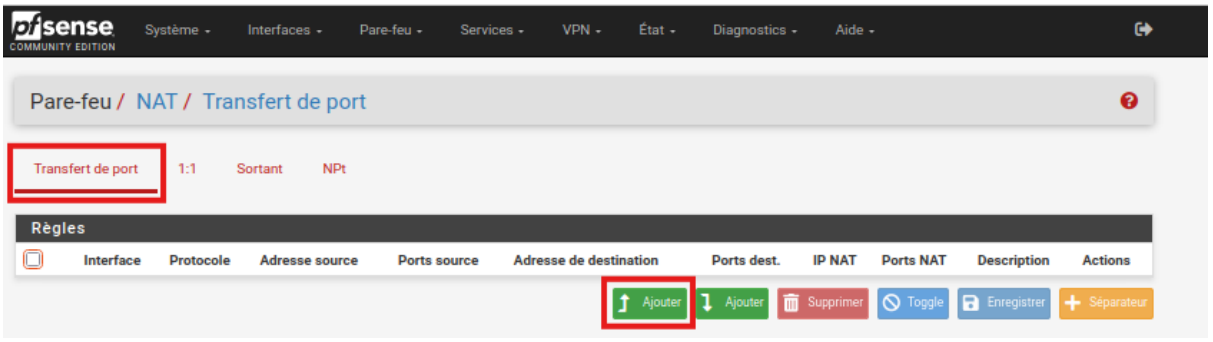

Destination
Destination
Invert match
Tous
Destination Address
Plage de port de destination
(autre)
44443
(autre)
44443
De
Personnalisé(e)
À
Personnalisé(e)
Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A" peut rester vide seulement si le filtre est sur un seul port.
Options 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
Administration depuis WAN
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
Enregistrer

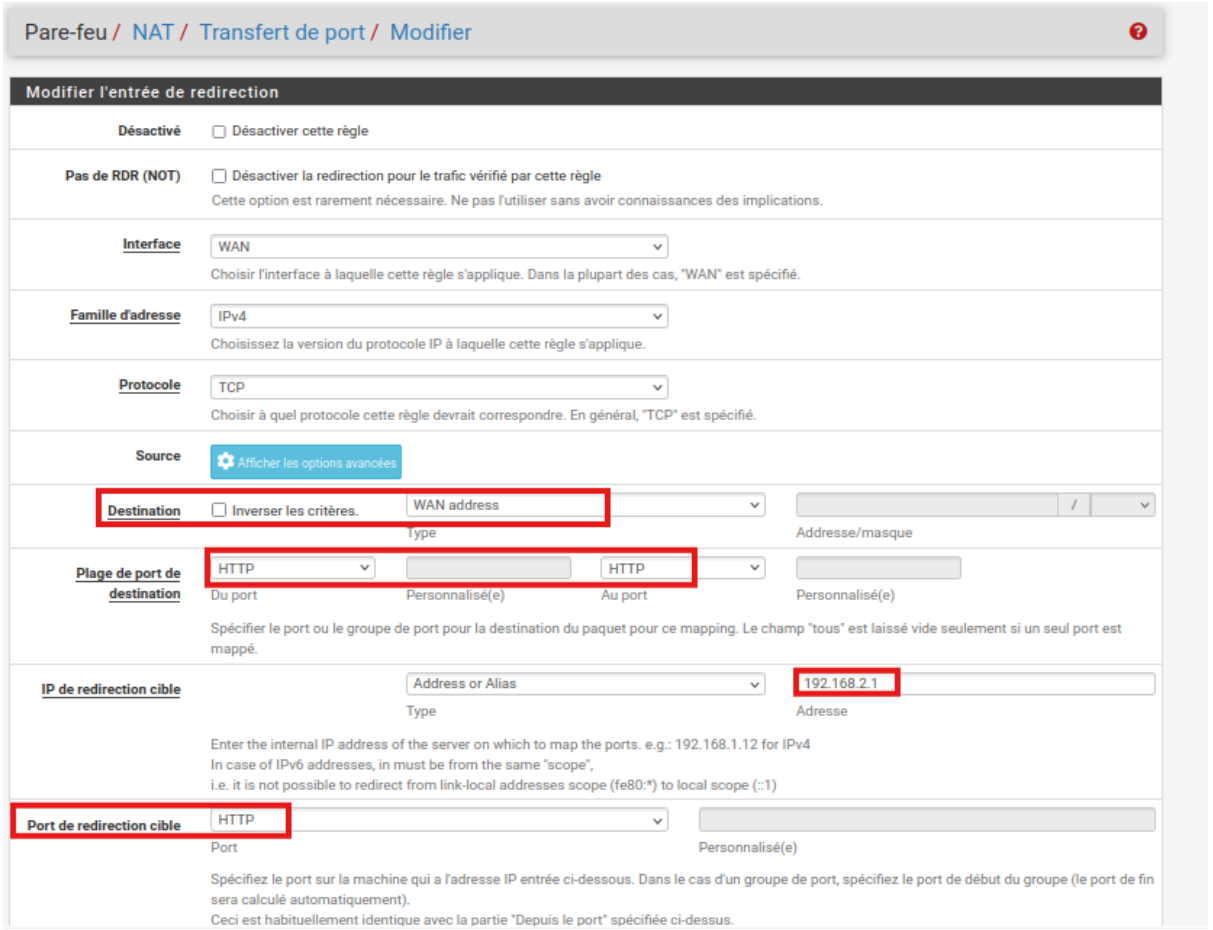

Pare-feu / Règles / WAN
La configuration de la règle de pare-feu a été modifiée
Ces modifications doivent être appliquées pour prendre effet.
Appliquer les modifications
Flottant(e)
WAN
LAN
OPT1
Règles (Faire glisser pour changer l'ordre)
États
Protocole
Source
Port
Destination
Port
Passerelle
File d'attente
Ordonnancement
Description
Actions
0/0 B
IPv4 TCP
172.17.0.0/16
*
*
44443
*
aucun
Administration depuis WAN
Ajouter
Ajouter
Supprimer
Toggle
Copier
Enregistrer
Séparateur

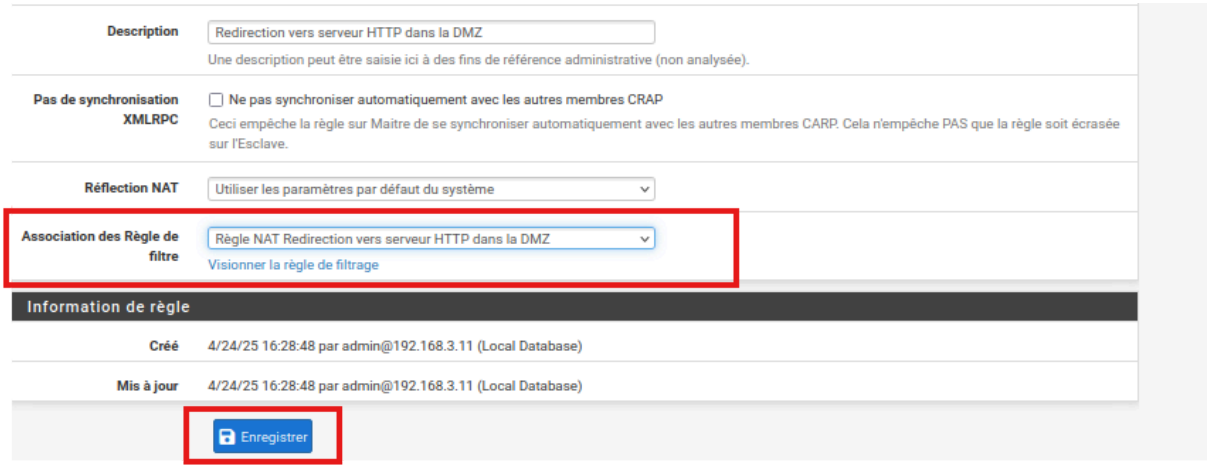

Non sécurisé
https://172.17.101.1:44443
pfsense
Login to pfSense
SIGN IN
admin
SIGN IN

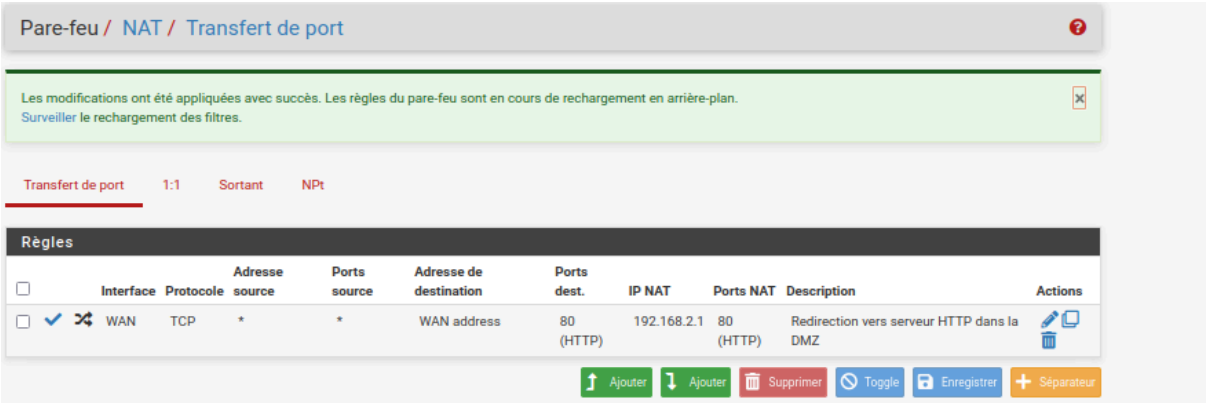
6. Port forwarding.

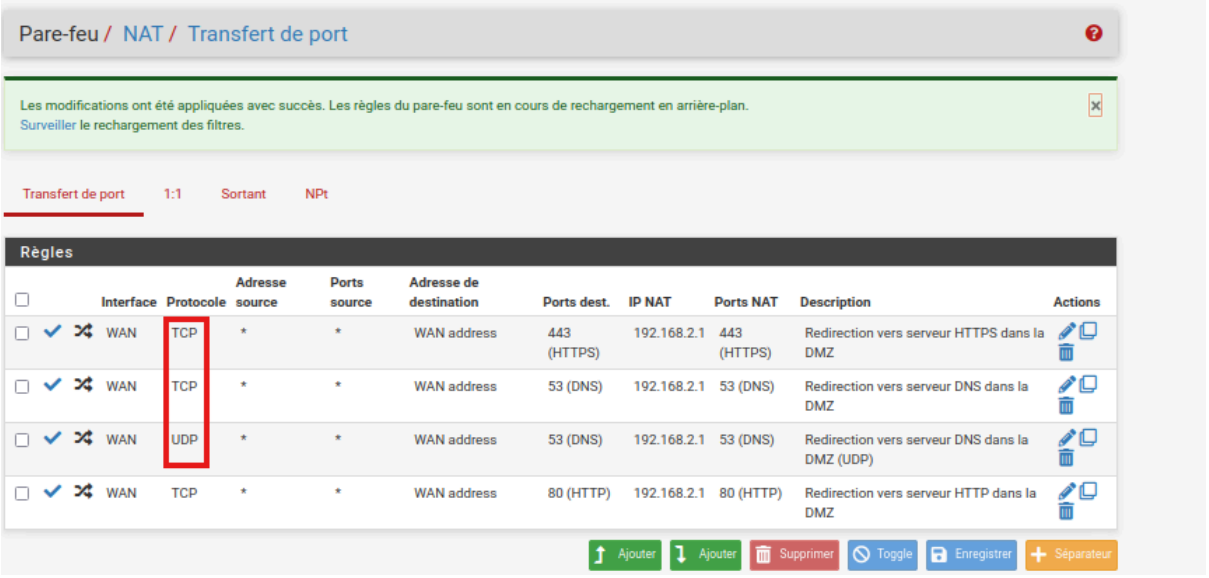
Port forwarding : on souhaite que les flux arrivant sur l'interface WAN à destination des ports 80, 443 et 53 soient redirigés vers le serveur web DS2 figurant dans la DMZ.

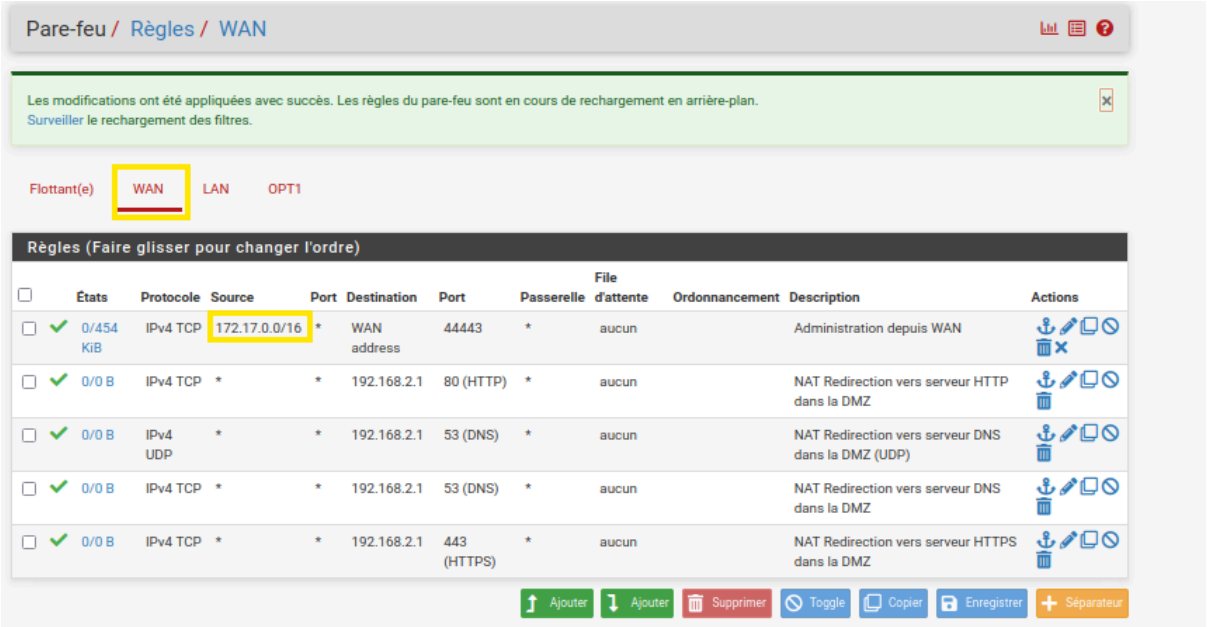





Description
Redirection vers serveur HTTP dans la DMZ
Une description peut être saisie ici à des fins de référence administrative (non analysée).
Pas de synchronisation XMLRPC
Ne pas synchroniser automatiquement avec les autres membres CRAP
Ceci empêche la règle sur Maitre de se synchroniser automatiquement avec les autres membres CARP. Cela n'empêche PAS que la règle soit écrasée sur l'Esclave.
Réflection NAT
Utiliser les paramètres par défaut du système
Association des Règle de filtre
Règle NAT Redirection vers serveur HTTP dans la DMZ
Visionner la règle de filtrage
Information de règle
Créé
4/24/25 16:28:48 par admin@192.168.3.11 (Local Database)
Mis à jour
4/24/25 16:28:48 par admin@192.168.3.11 (Local Database)
Enregistrer

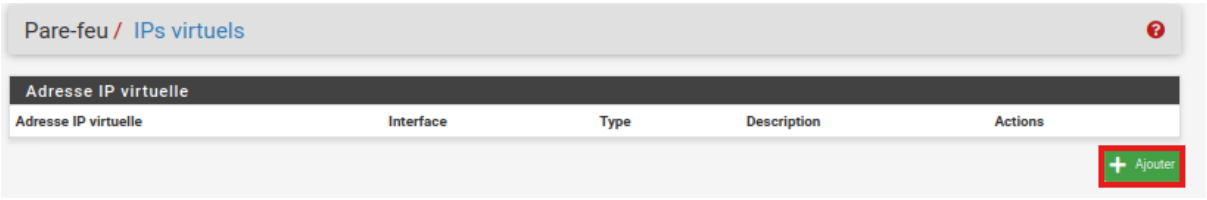

Pare-feu / NAT / Transfert de port
Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan.
Surveiller le rechargement des filtres.
Transfert de port
1:1
Sortant
NPt
Règles
Interface
Protocole
Adresse source
Ports source
Adresse de destination
Ports dest.
IP NAT
Ports NAT
Description
Actions
WAN
TCP
*
*
WAN address
80 (HTTP)
192.168.2.1
80 (HTTP)
Redirection vers serveur HTTP dans la DMZ
Ajouter
Ajouter
Supprimer
Toggle
Enregistrer
Séparateur

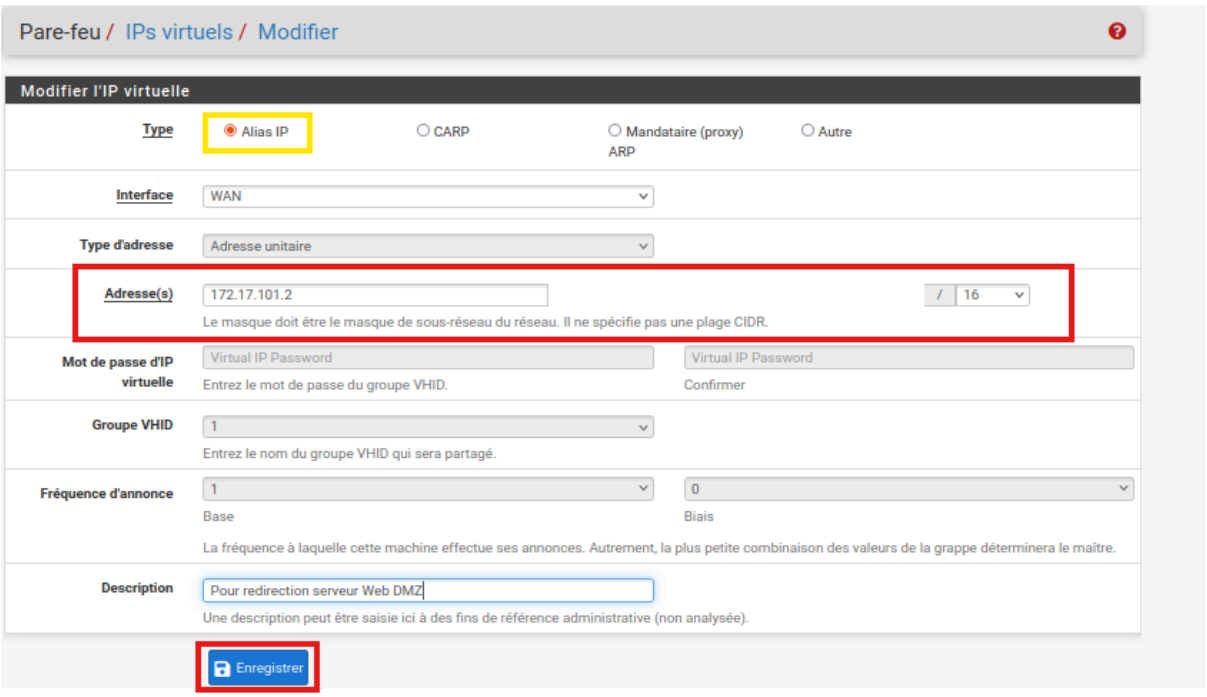

Pare-feu / NAT / Transfert de port
Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan.
Surveiller le rechargement des filtres.
Transfert de port
1:1
Sortant
NPt
Règles
Interface
Protocole
Adresse source
Ports source
Adresse de destination
Ports dest.
IP NAT
Ports NAT
Description
Actions
WAN
TCP
*
*
WAN address
443 (HTTPS)
192.168.2.1
443 (HTTPS)
Redirection vers serveur HTTPS dans la DMZ
WAN
TCP
*
*
WAN address
53 (DNS)
192.168.2.1
53 (DNS)
Redirection vers serveur DNS dans la DMZ
WAN
UDP
*
*
WAN address
53 (DNS)
192.168.2.1
53 (DNS)
Redirection vers serveur DNS dans la DMZ (UDP)
WAN
TCP
*
*
WAN address
80 (HTTP)
192.168.2.1
80 (HTTP)
Redirection vers serveur HTTP dans la DMZ
Ajouter
Ajouter
Supprimer
Toggle
Enregistrer
Séparateur

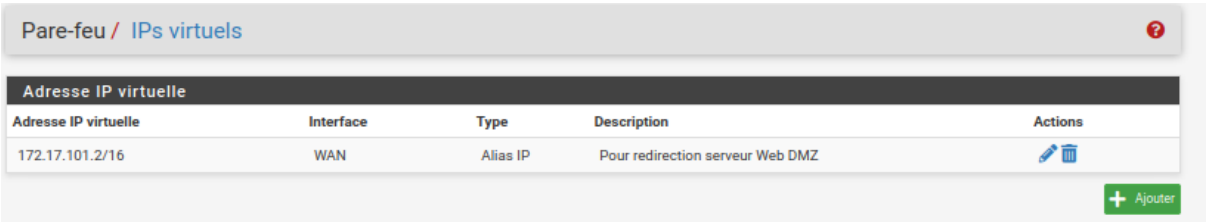


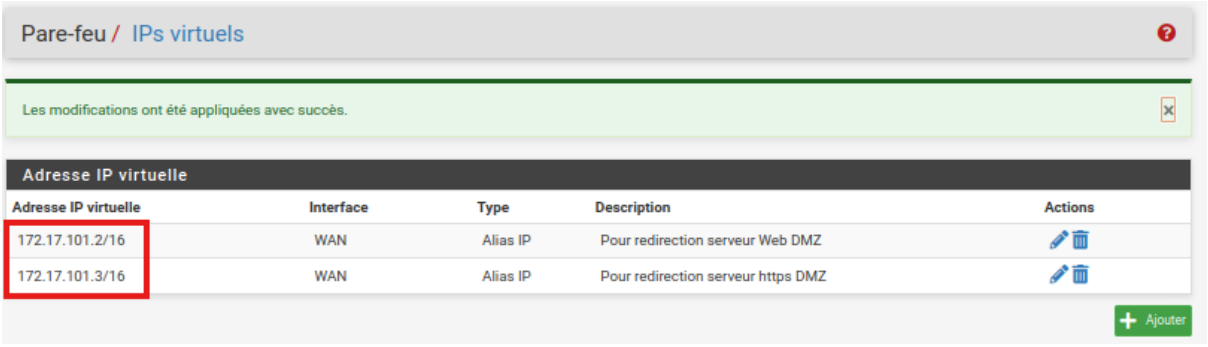
(J'ai modifié la première en conséquence que j'avais oublié en destination "WAN address").

Création de deux IP virtuels pour les redirections http et https.

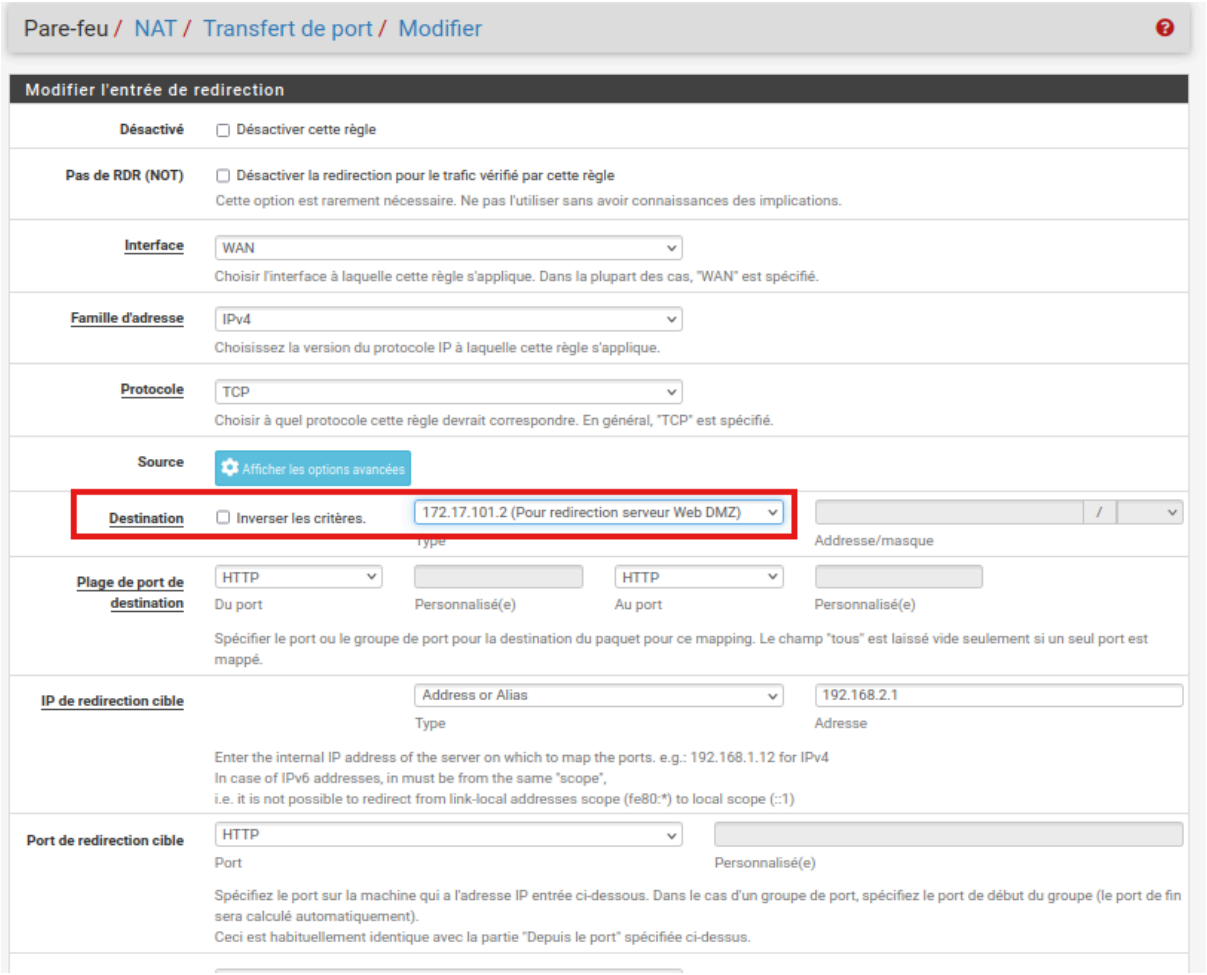


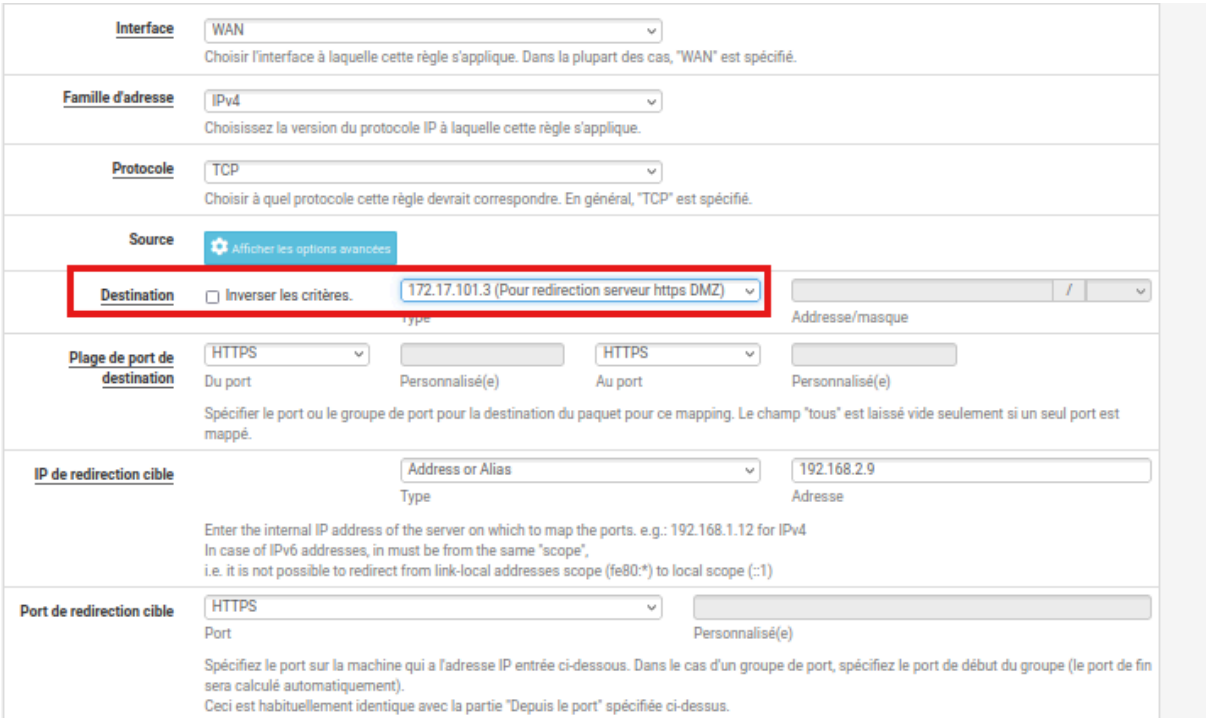


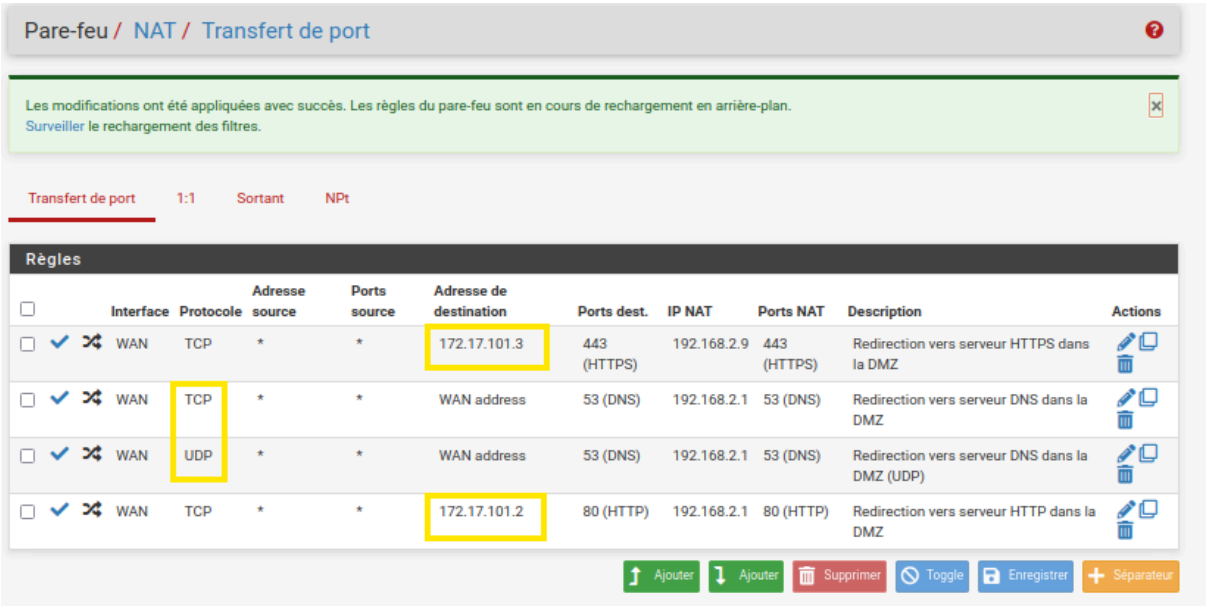




Modification des règles de redirection.

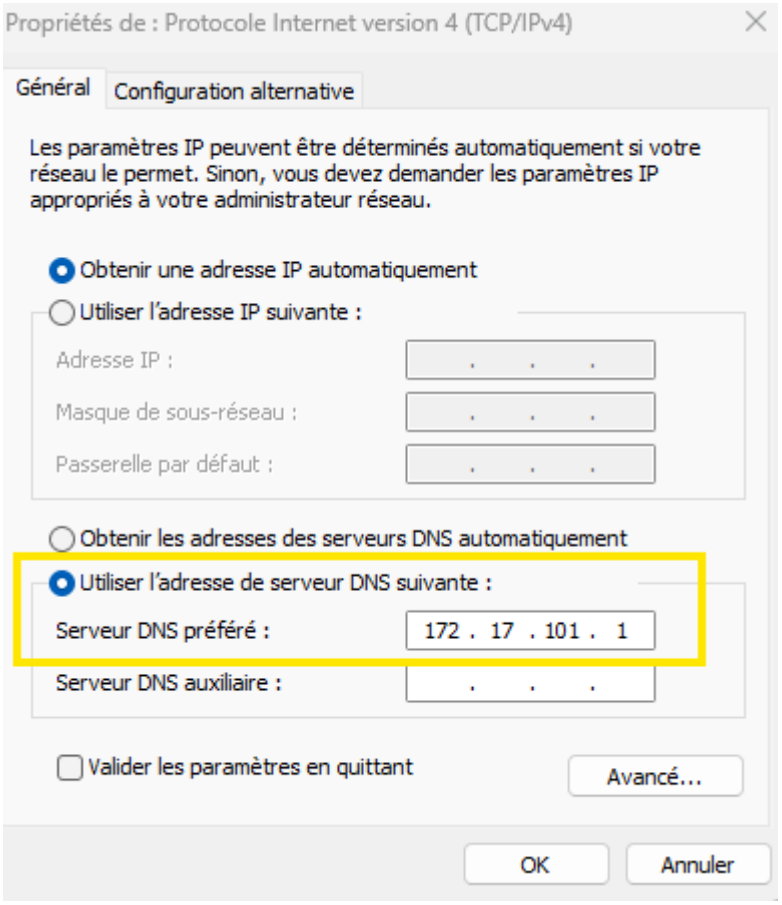






(J'ai également modifier la règle avec https d'où j'avais fais une erreur sur l'IP NAT qui était de 192.168.2.9)

Modification de l’adresse du serveur DNS de notre machine physique.



7. Mise en place du split DNS.

Le serveur DNS DS2.sio-exupery.fr, situé dans la DMZ, doit indiquer une adresse IP du serveur Web différente en fonction de la source de la requête qui lui est adressée : celle-ci proviendra soit de l'extérieur soit du réseau LAN. Vous allez utiliser pour cela la notion de vue.

```
  GNU nano 7.2                                                    /etc/bind/na
// Fichier de configuration générale pour le DNS avec vues.

acl lans {
        192.168.2.0/24;
        192.168.3.0/24;
};

options {
        forward only;
        forwarders { 80.10.246.2;_};
        auth-nxdomain no;
};

//Zones de la vue interne

view "interne" {
        match-clients { lans; };
        allow-recursion {lans; };
```

```
root@DS2: ~#cat /etc/bind/named.conf.default-zones >> /etc/bind/named.conf
```

```
// prime the server with knowledge of the root servers
//zone "." {
//      type hint;
//      file "/usr/share/dns/root.hints";
//};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

```
//notre zone vue de l'intérieur

        zone "sio-exupery.fr" IN {
                type master;
                file "/var/cache/bind/internals/db.sio-exupery.fr";
                allow-update { none; };
        };

        zone "2.168.192.in-addr.arpa" IN {
                type master;
                file "/var/cache/bind/internals/rev.sio-exupery.fr";
                allow-update { none; };
        };
};
```

```
// zones de la vue externe

        zone "sio-exupery.fr" IN {
                type master;
                file "/var/cache/bind/externals/db.sio-exupery.fr";
                allow-update { none; };
        };

        zone "2.168.192.in-addr.arpa" IN {
                type master;
                file "/var/cache/bind/externals/rev.sio-exupery.fr";
                allow-update { none; };
        };
};
```

Création des deux répertoires externals et internals dans /var/cache/bind/.

```
root@DS2: ~#mkdir /var/cache/bind/externals/
root@DS2: ~#mkdir /var/cache/bind/internals/
root@DS2: ~#cd /var/cache/bind
root@DS2: /var/cache/bind#ls -l
total 24
-rw-rw-r-- 1 root bind  554 11 avril 19:04 db.sio-exupery.fr
drwxr-xr-x 2 root root 4096 24 avril 17:38 externals
drwxr-xr-x 2 root root 4096 24 avril 17:38 internals
-rw-rw-r-- 1 bind bind  221 25 mars  17:44 managed-keys.bind
-rw-rw-r-- 1 bind bind 2438 25 mars  17:43 managed-keys.bind.jnl
-rw-rw-r-- 1 root bind  201 11 avril 19:06 rev.sio-exupery.fr
root@DS2: /var/cache/bind#
```

Copie des fichiers db.sio-exupery.fr et rev.sio-exupery.fr existants.

```
root@DS2: ~#cp /var/cache/bind/db.sio-exupery.fr /var/cache/bind/internals/
root@DS2: ~#cp /var/cache/bind/db.sio-exupery.fr /var/cache/bind/externals/
root@DS2: ~#cp /var/cache/bind/rev.sio-exupery.fr /var/cache/bind/internals/
root@DS2: ~#cp /var/cache/bind/rev.sio-exupery.fr /var/cache/bind/externals/
root@DS2: ~#
```

Attribution de ces fichiers de zone au groupe bind afin de les rendre accessibles au démon.

```
root@DS2: ~#chgrp bind /var/cache/bind/*
root@DS2: ~#chmod 664 /var/cache/bind/*
root@DS2: ~#chmod 664 /var/cache/bind/internals/*
root@DS2: ~#chmod 664 /var/cache/bind/externals/*
root@DS2: ~#
```

Nous Testons www.sio-exupery.fr, projet1.sio-exupery.fr et secu.sio-exupery.fr depuis notre machine hôte puis depuis depuis UD1/DD1 ou WIN11.