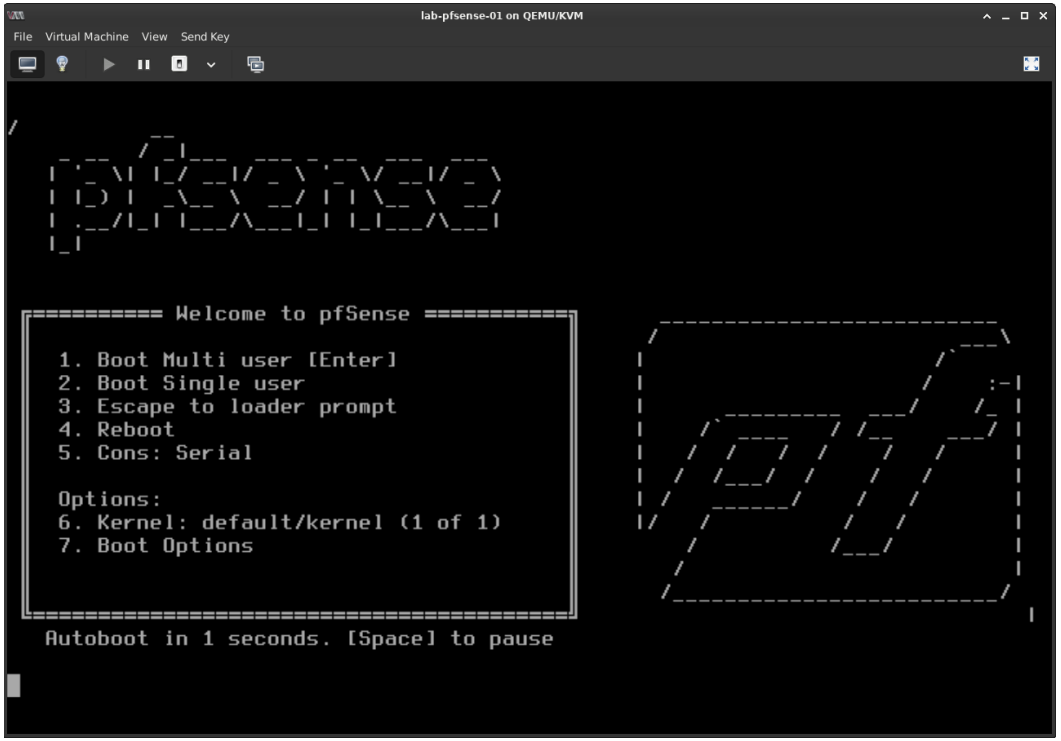
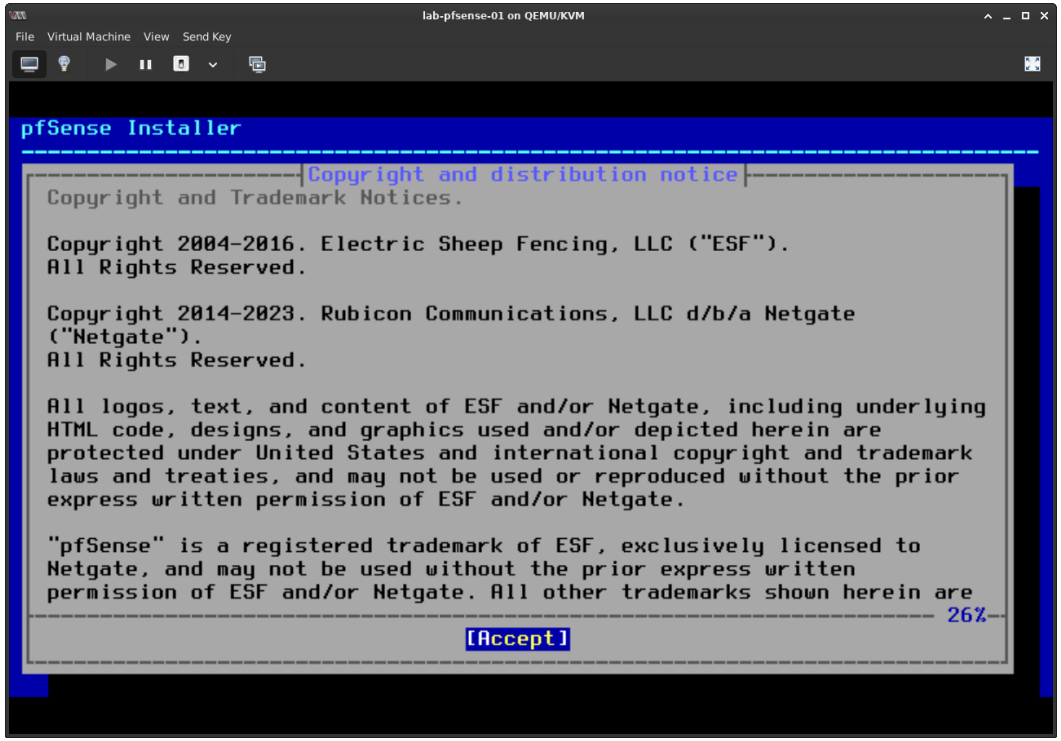
SOP - PfSense CE-2.7.2

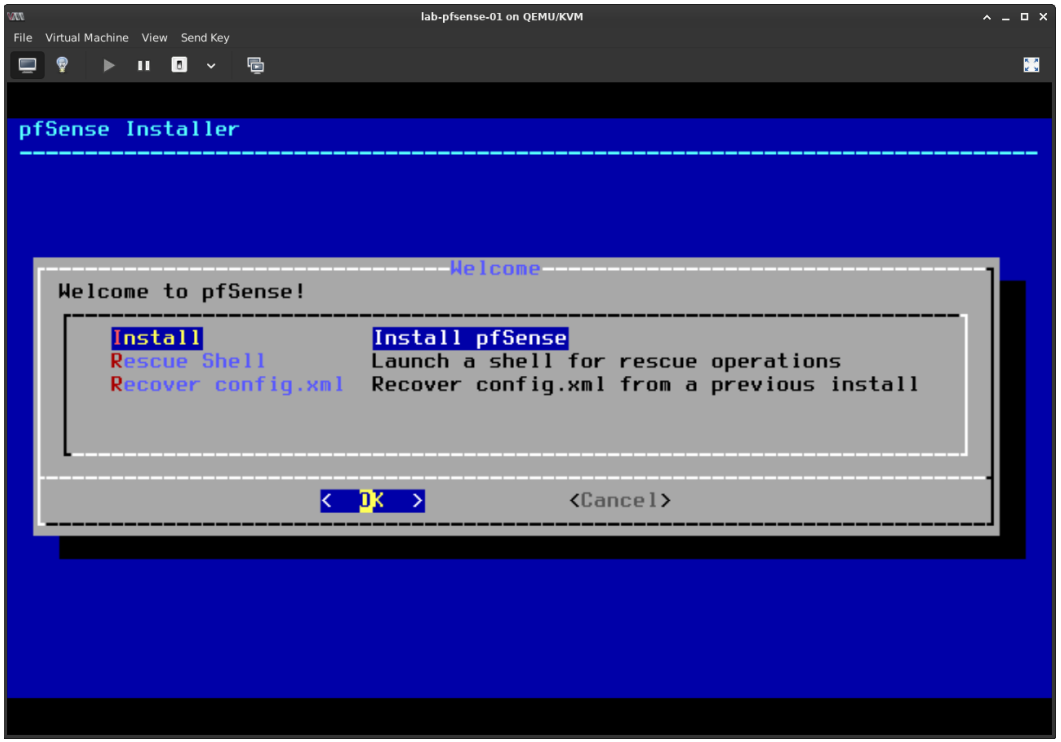
Initialisation de l'environnement

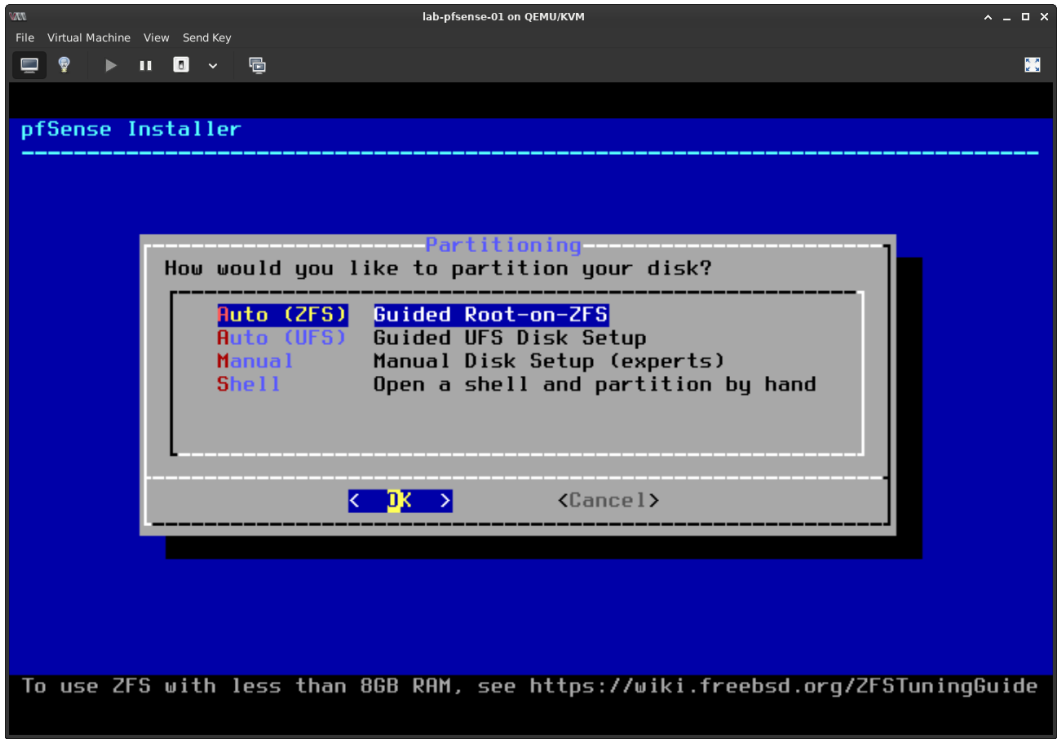




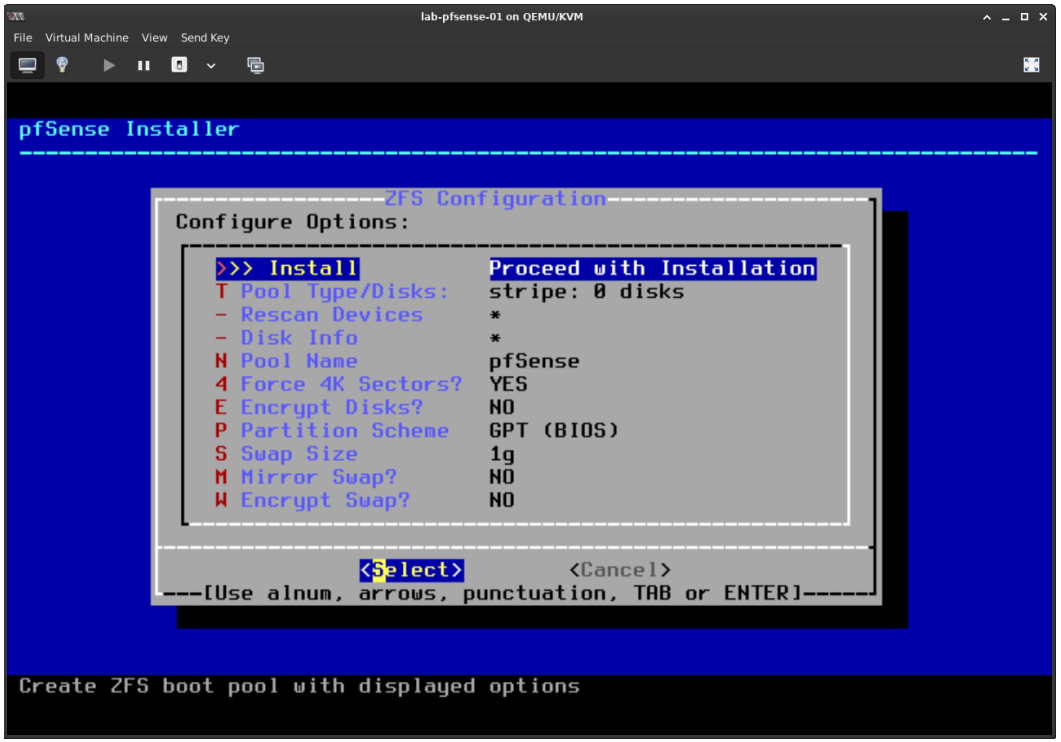
Acceptation de la EULA (End User License Agreement).

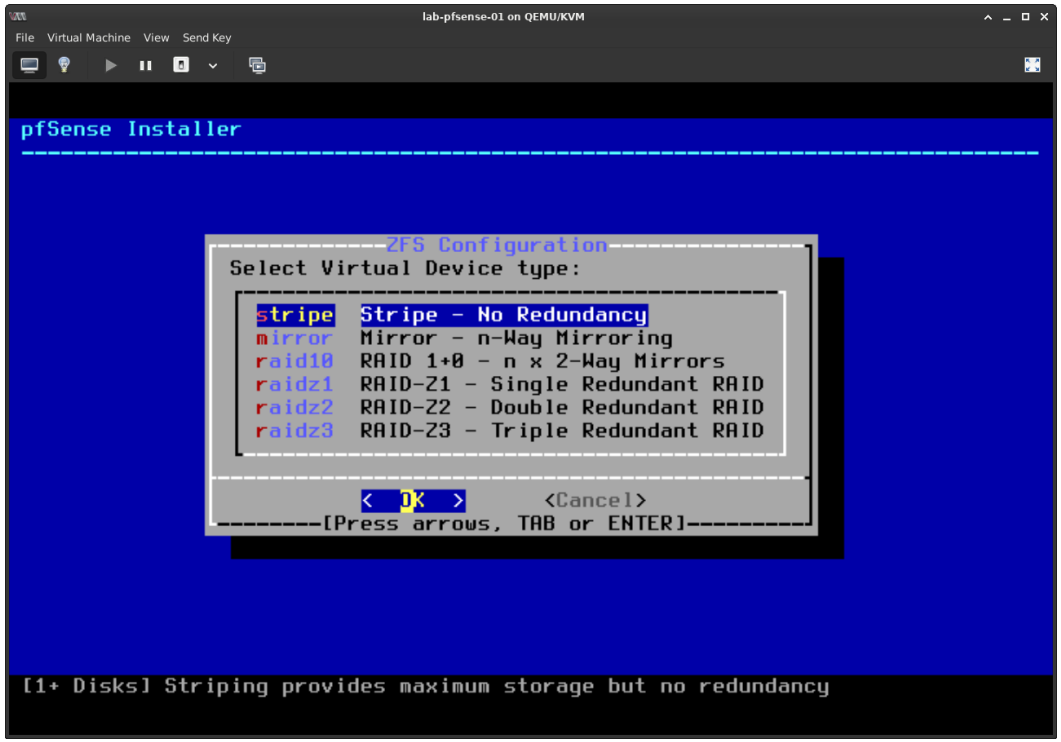
"On accepte les conditions sans lire, comme tout le monde."



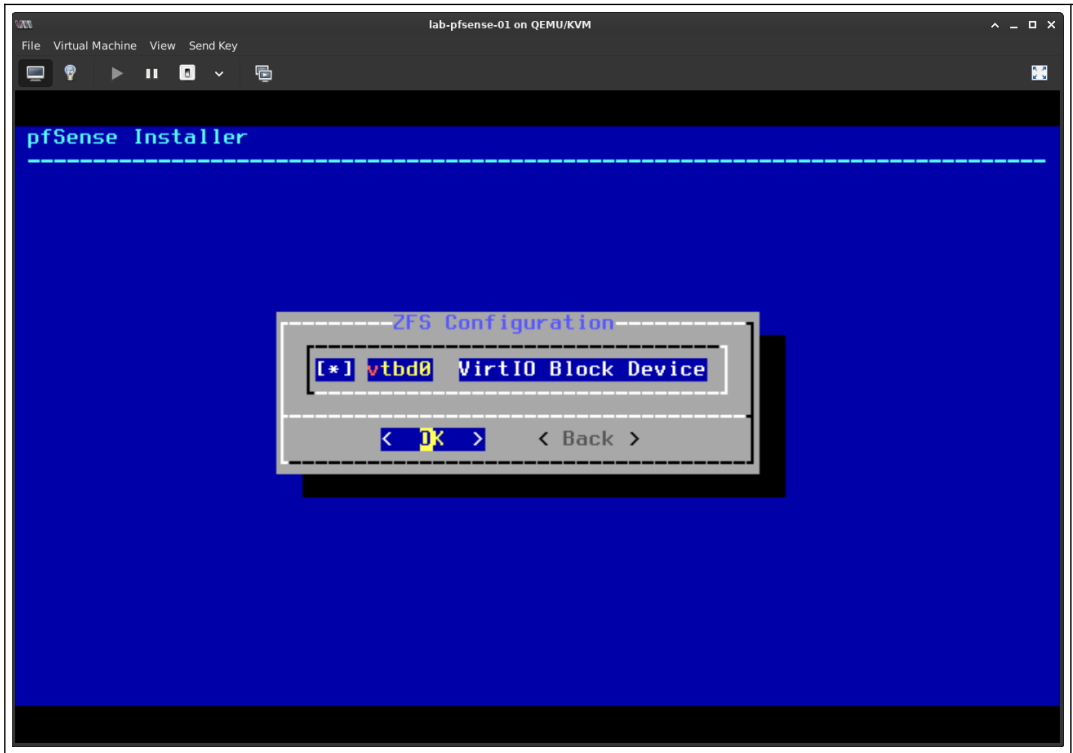
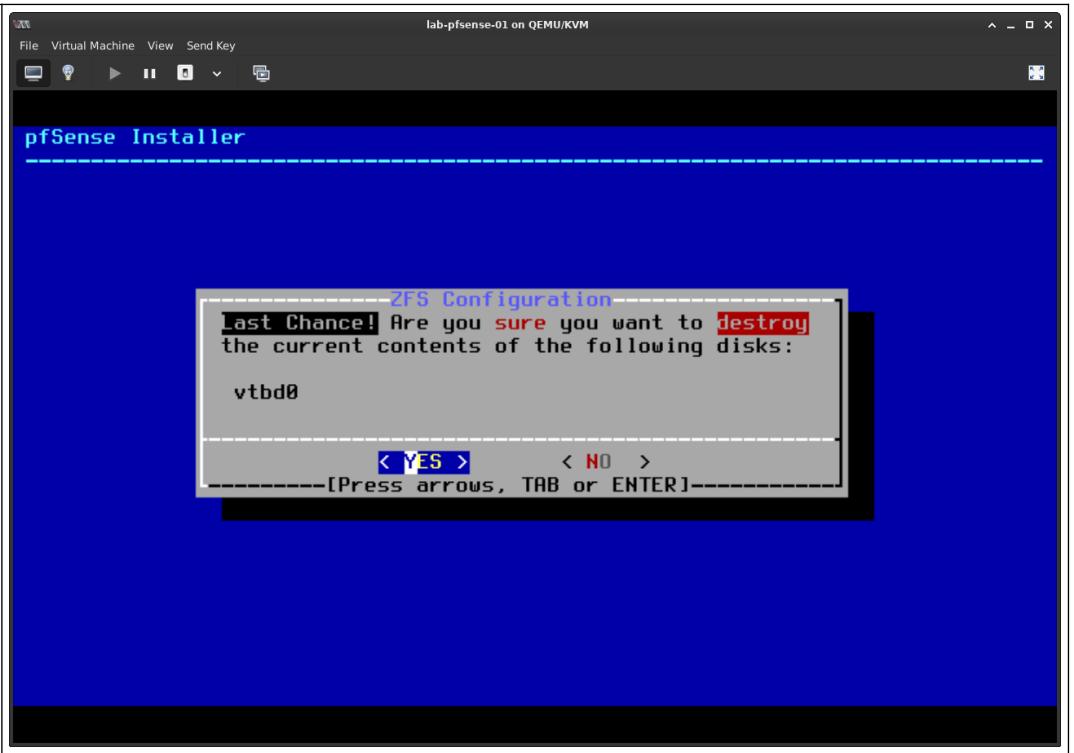


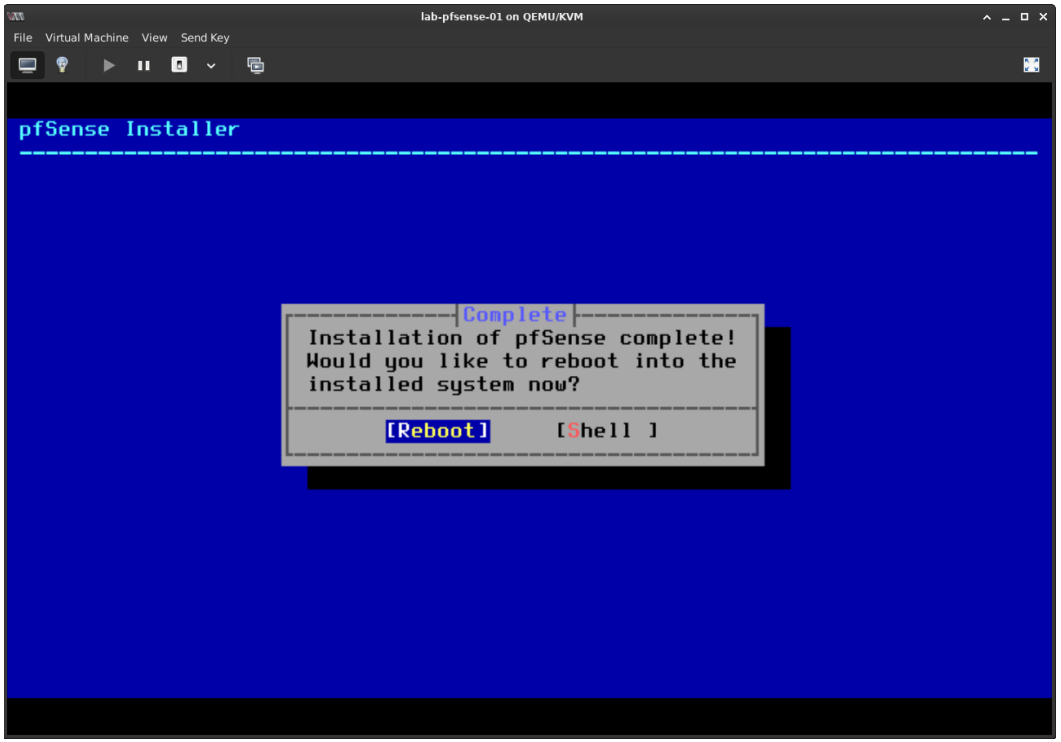
Le choix du système de fichiers **ZFS** (Zettabyte File System) est privilégié par rapport à UFS (Unix File System) pour sa résilience. ZFS intègre nativement la gestion de volumes logiques et des snapshots, essentiel pour les retours arrière (Rollback) en cas de mise à jour ratée.





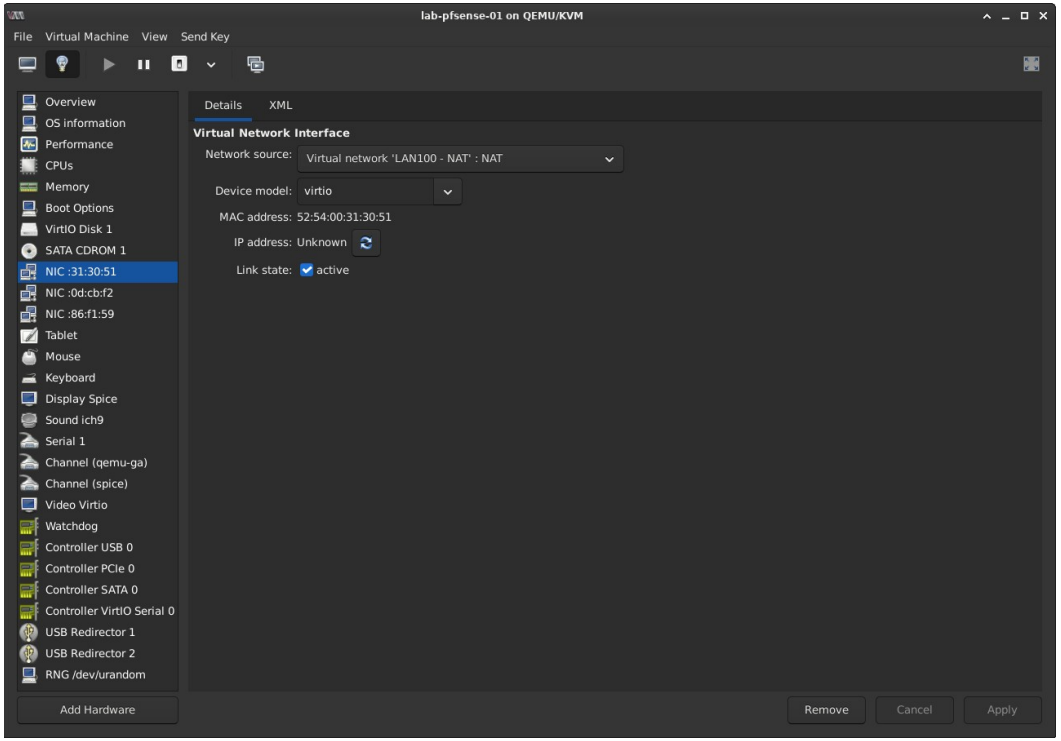
Dans un environnement virtualisé (Lab), nous sélectionnons la topologie **Stripe** (0 redondance) car la redondance disque est gérée par l'hyperviseur sous-jacent (RAID matériel ou stockage Ceph du cluster). En production physique, un Mirror (RAID 1) serait a privilègier.

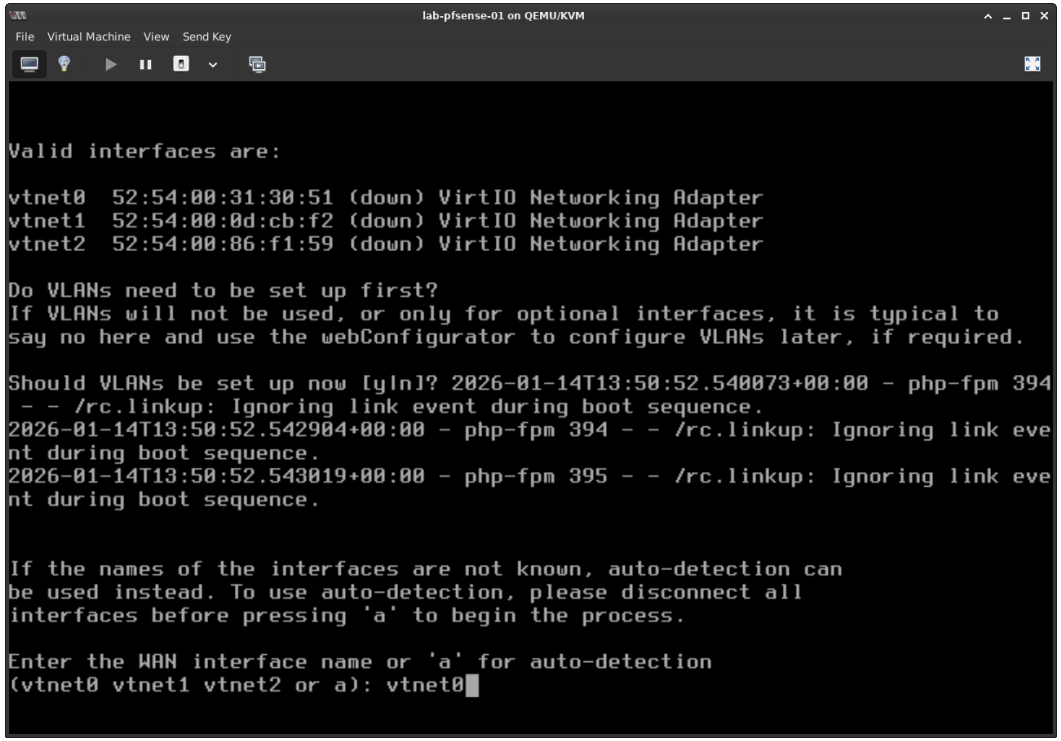
	
Faire espace pour valider l'utilisation du disque vtbd0	Passer sur YES et entrer ! Cette étape formate le disque virtuel vtbd0. Toutes les données précédentes seront déclarées *Excommunicado*. Destruction totale.



Retirer l'ISO du lecteur virtuel pour éviter une boucle de boot (si ce n’est pas fait automatiquement).

Gestion des interfaces réseaux

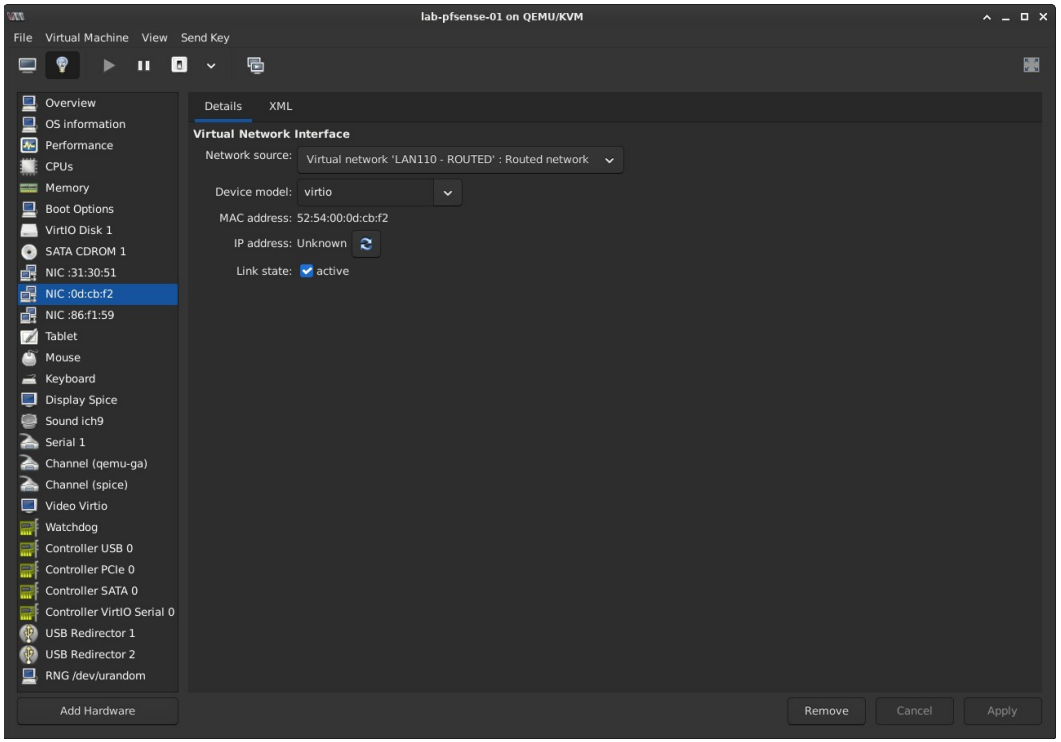


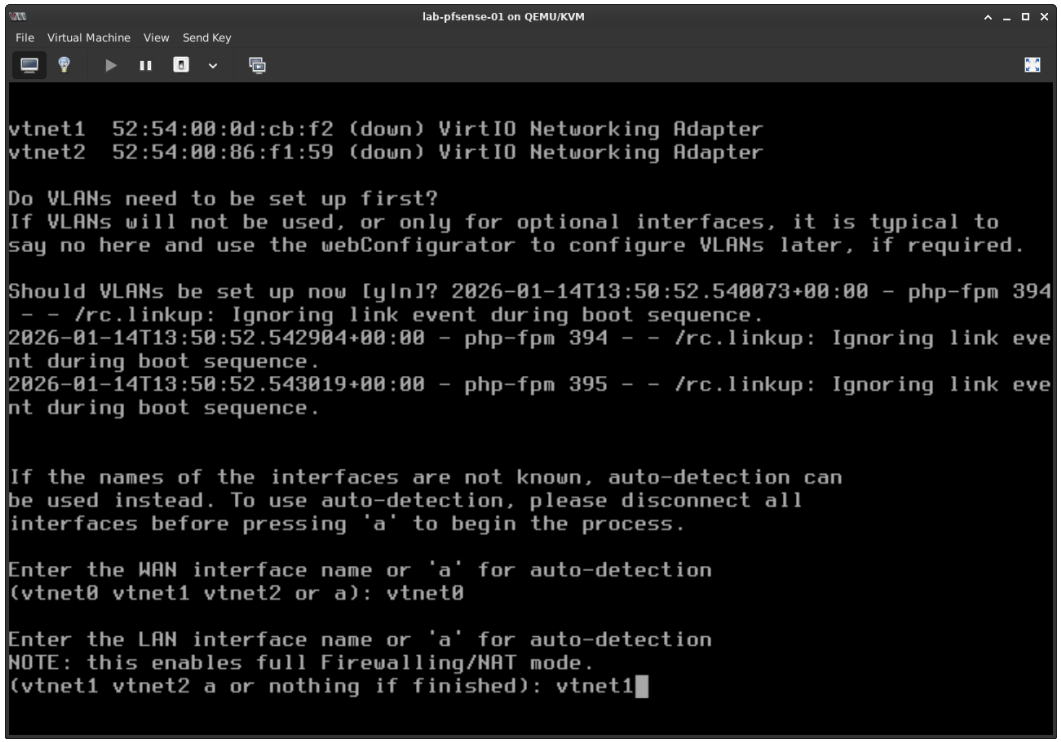


Identifier les adresses MAC affichées si nécessaire pour distinguer les cartes.

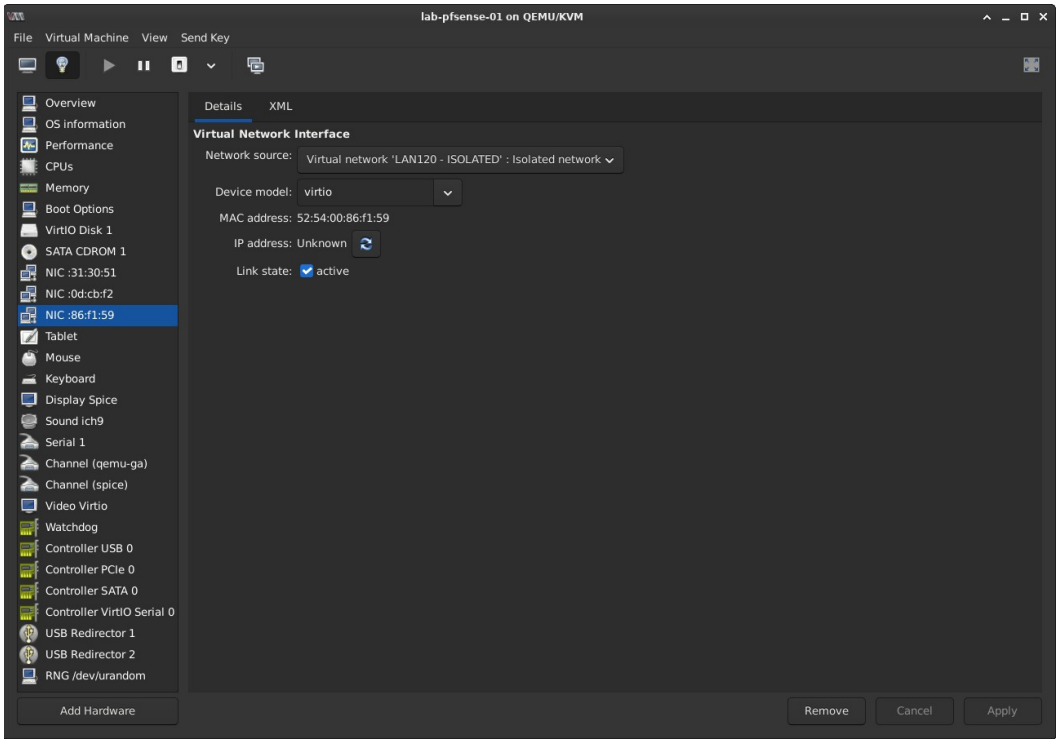
WAN : Interface de sortie, connectée au routeur FAI ou au réseau externe.

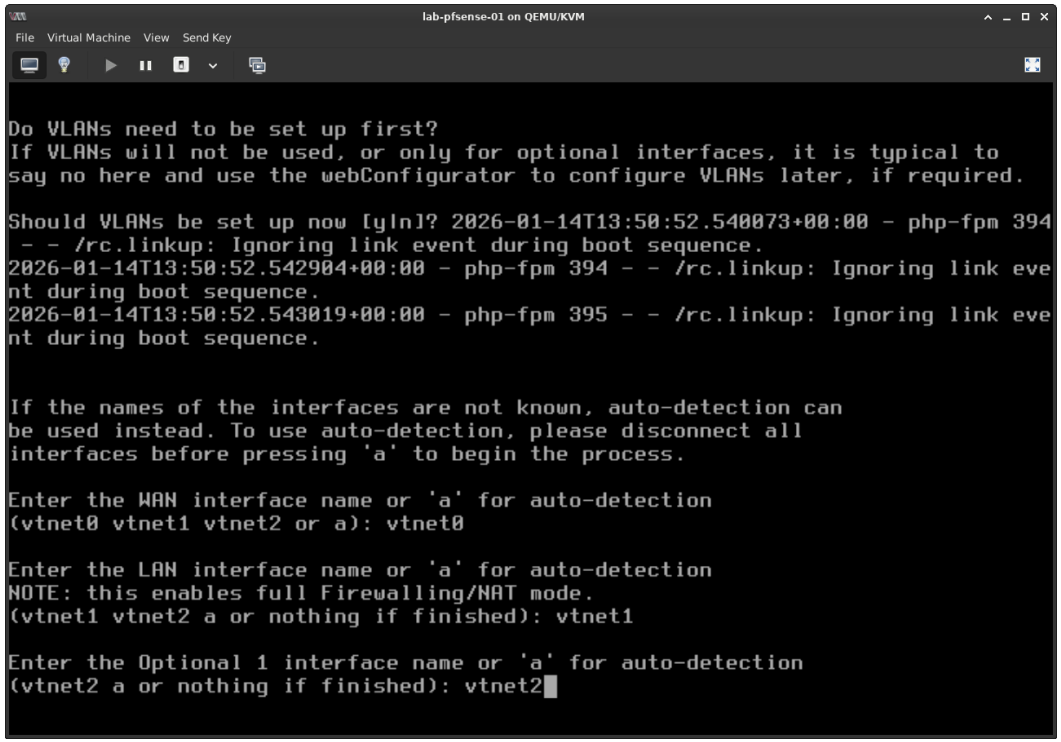
> "Le préfixe **vtnet** indique l'utilisation de drivers para-virtuels **VirtIO** (environnement KVM/Proxmox). Sur VMware, vous verriez vmxnet3. Sur du matériel physique Intel, ce serait igb ou ix."



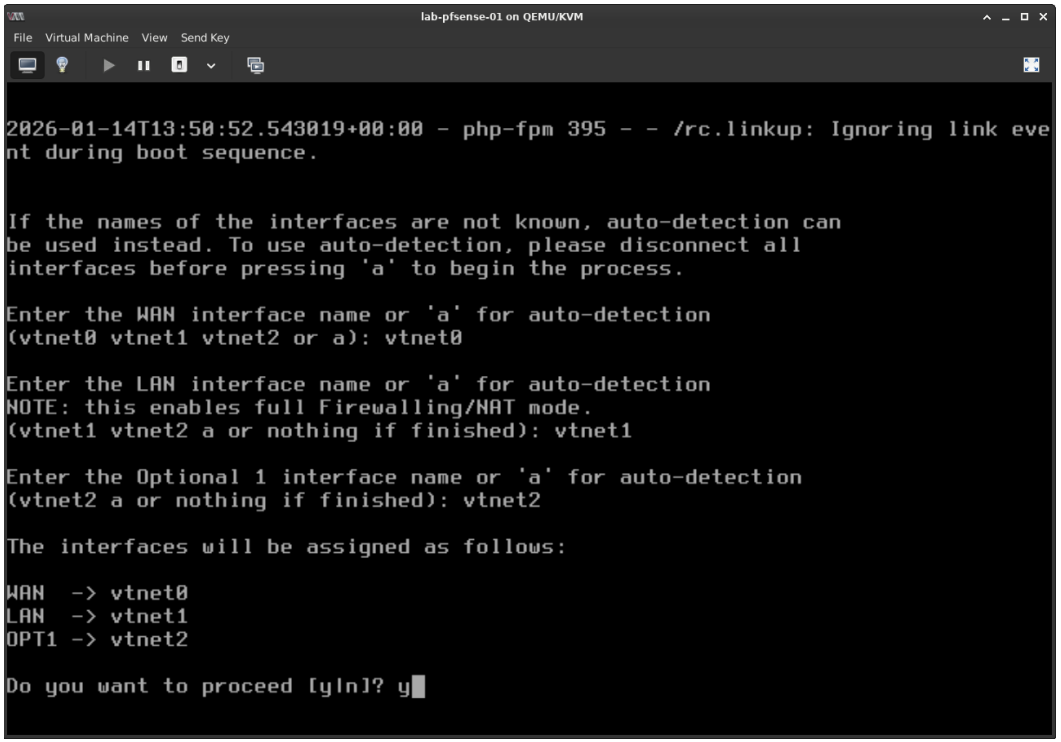


LAN : Réseau de confiance (Trust), gestion native du pare-feu.

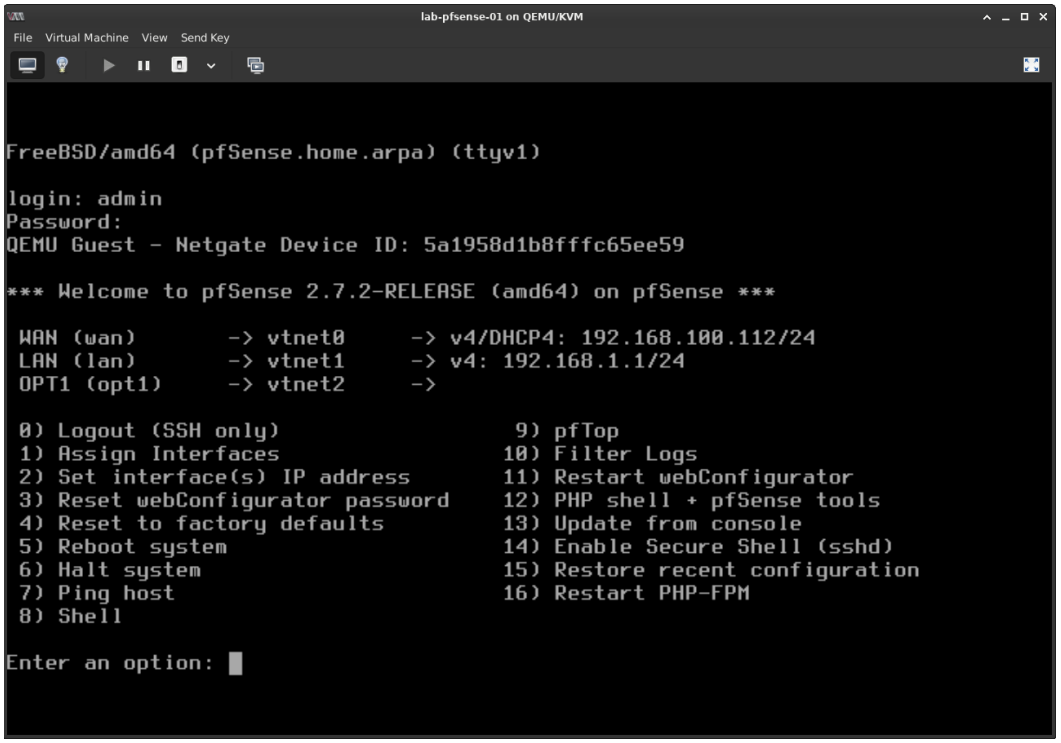


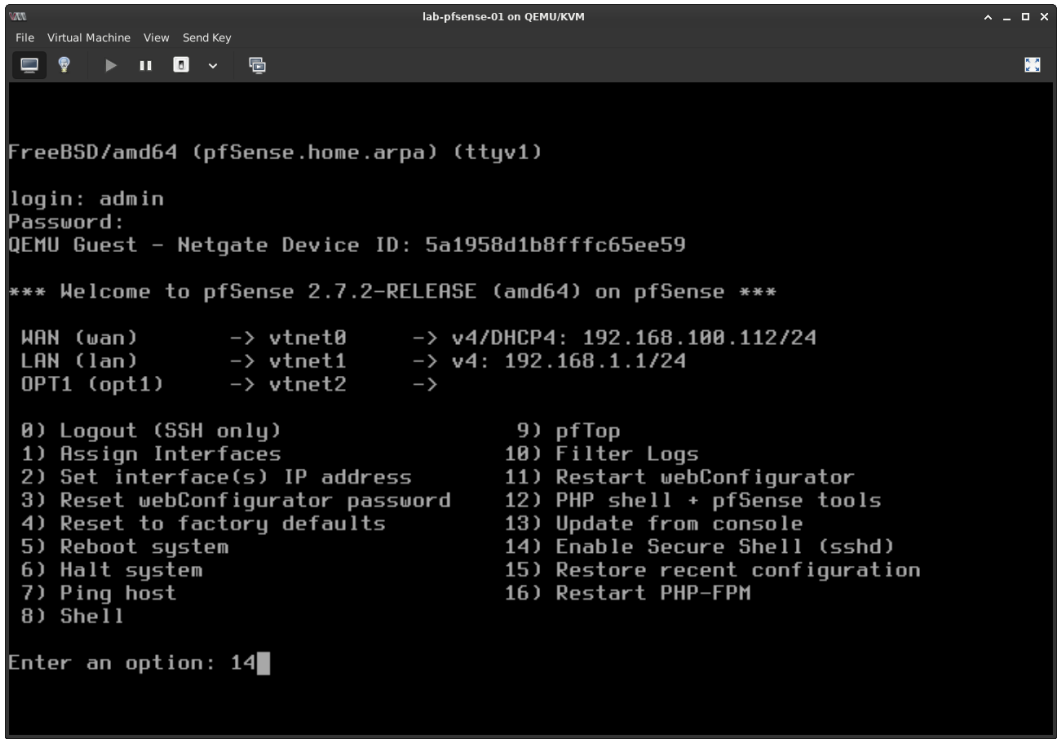


OPT1 : Zone démilitarisée (DMZ) ou réseau isolé.

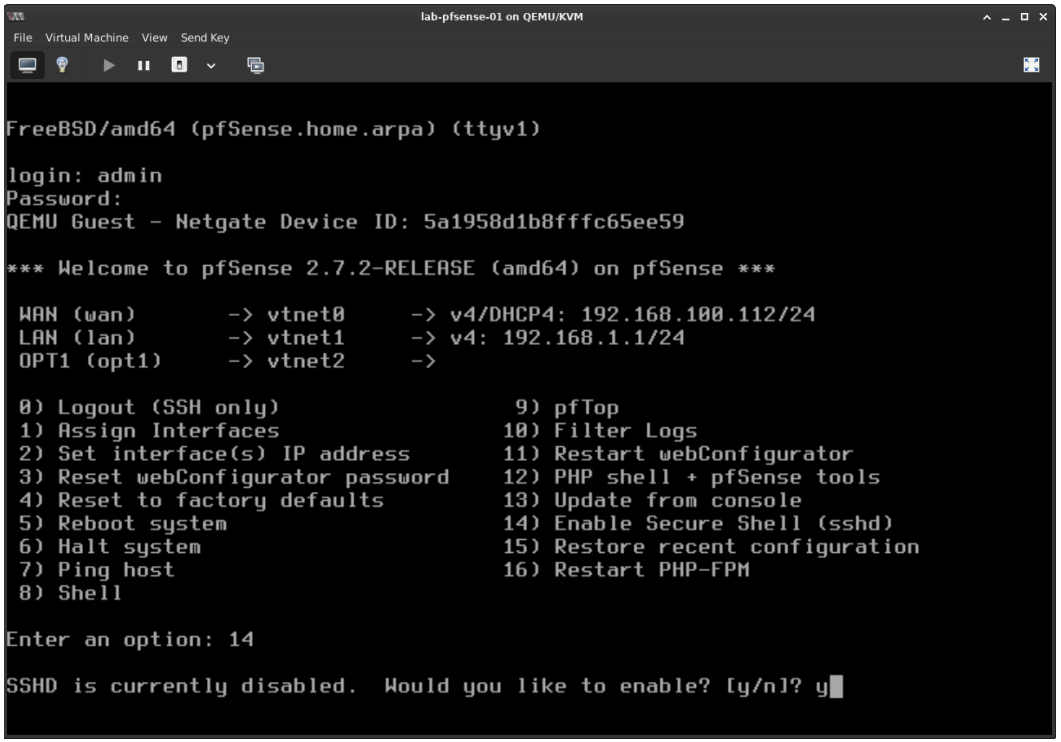


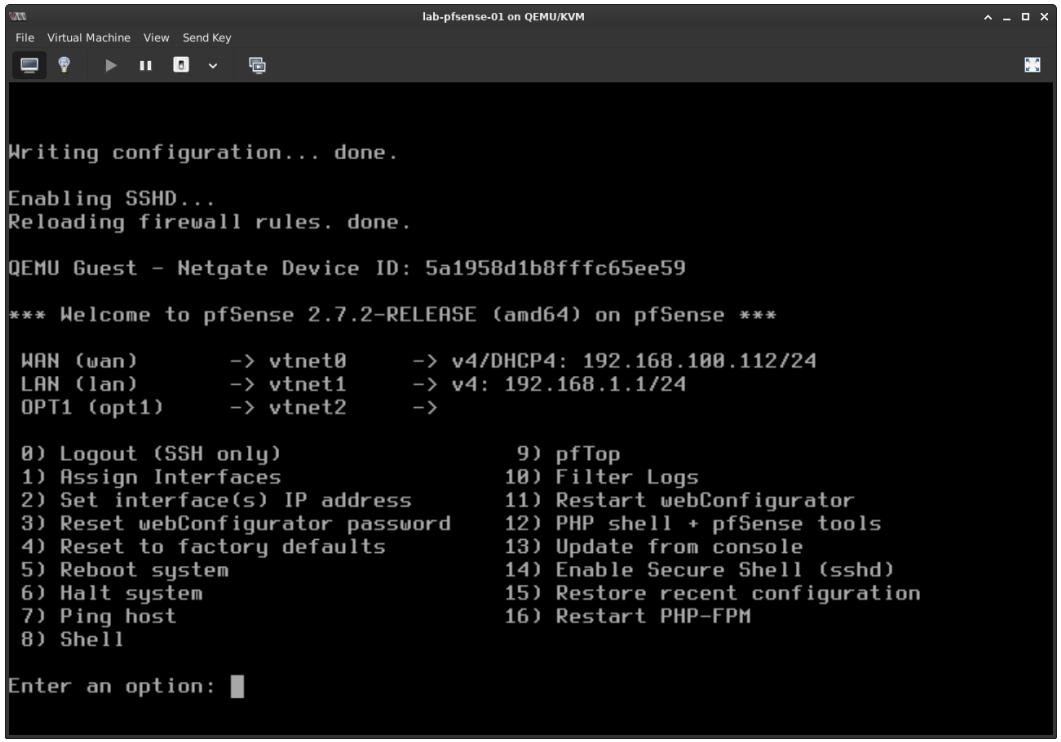
Activation de SSH





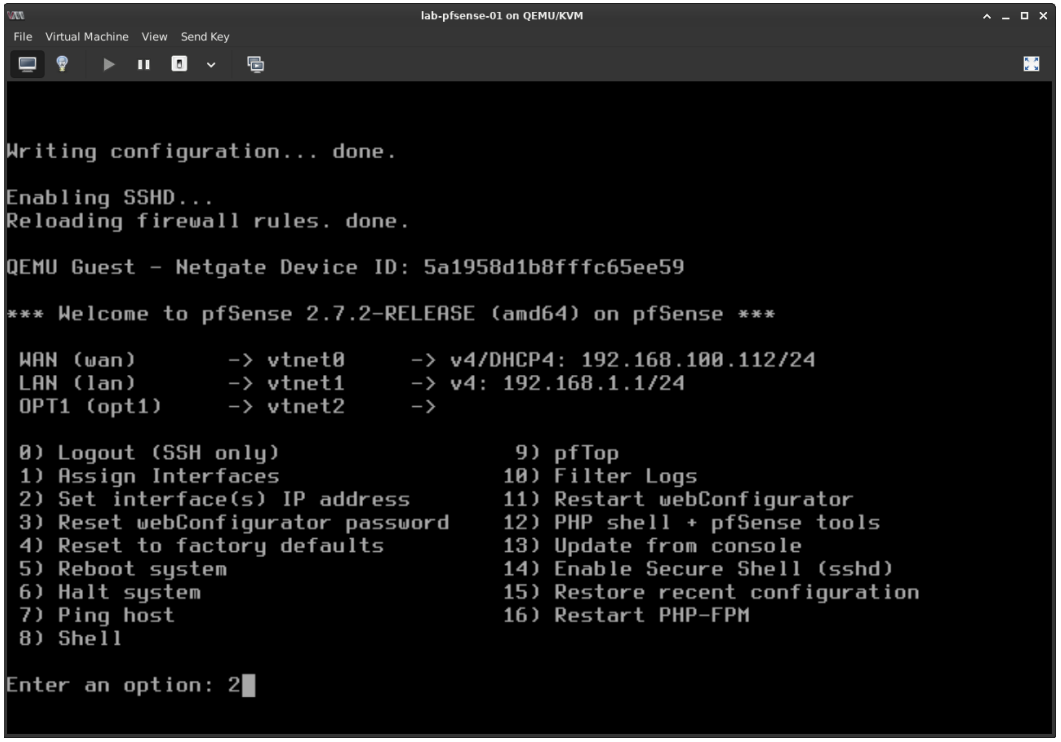
Par défaut, pfSense garde ses portes fermées. Pour administrer confortablement, il faut activer le démon SSH.

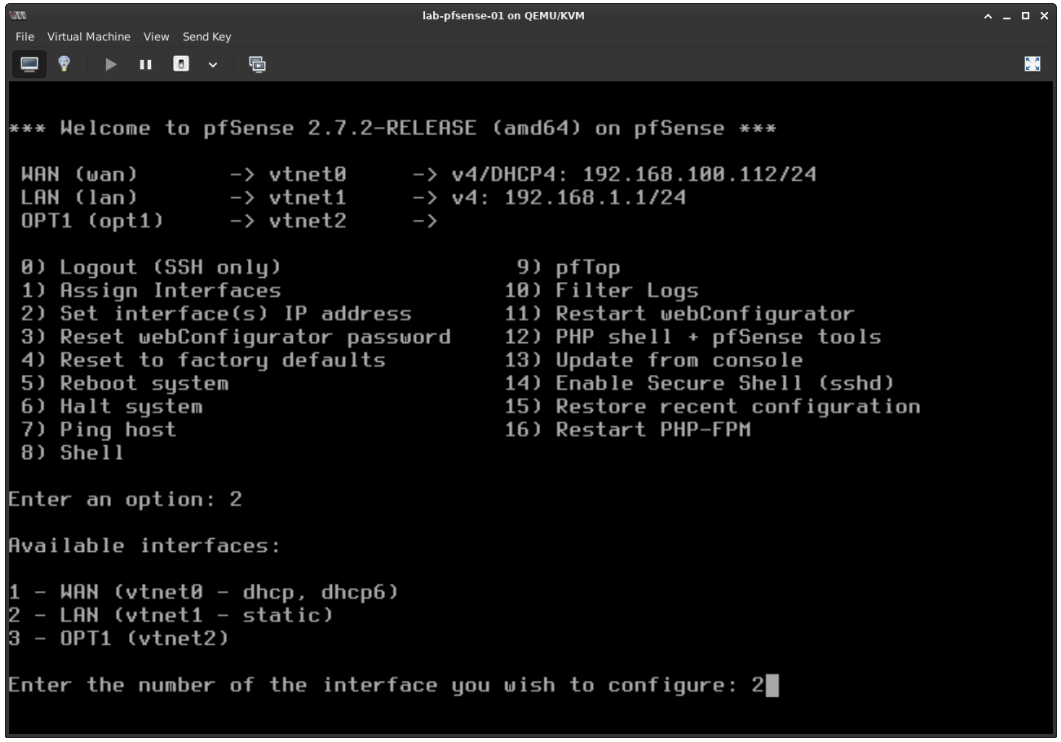




"On active le SSH (Secure Shell). Sans quoi, vous êtes condamné à taper vos commandes dans une console VNC lente et pixelisée. Un admin système sans SSH est un admin qui souffre inutilement."

Conguration de l’interface LAN

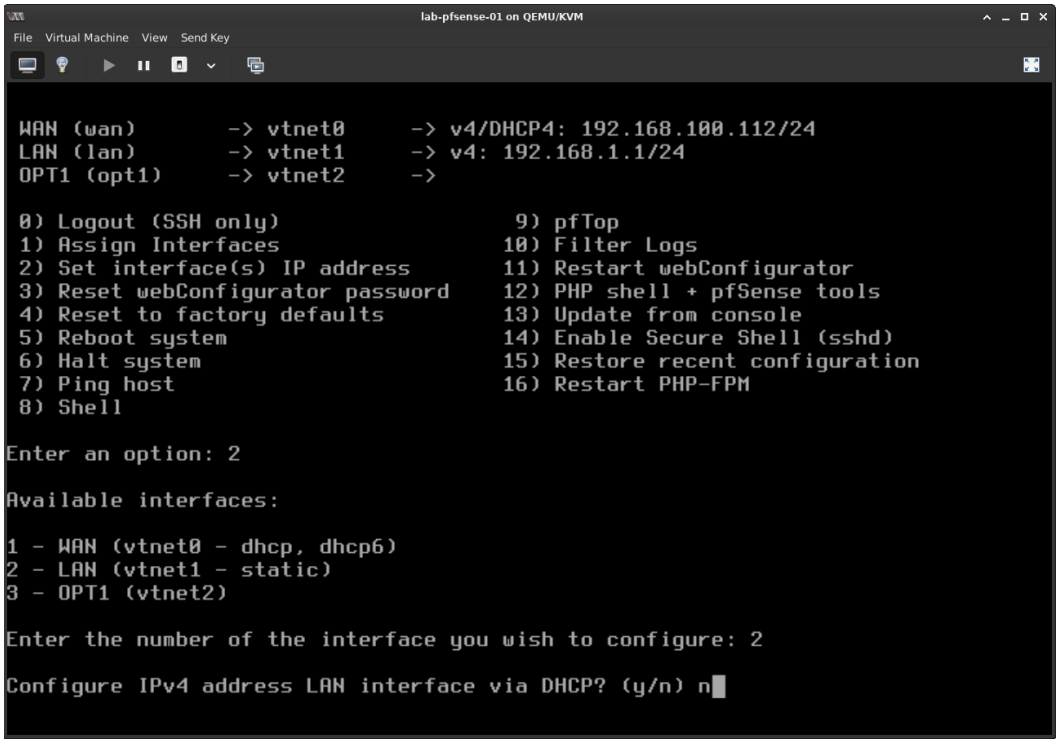


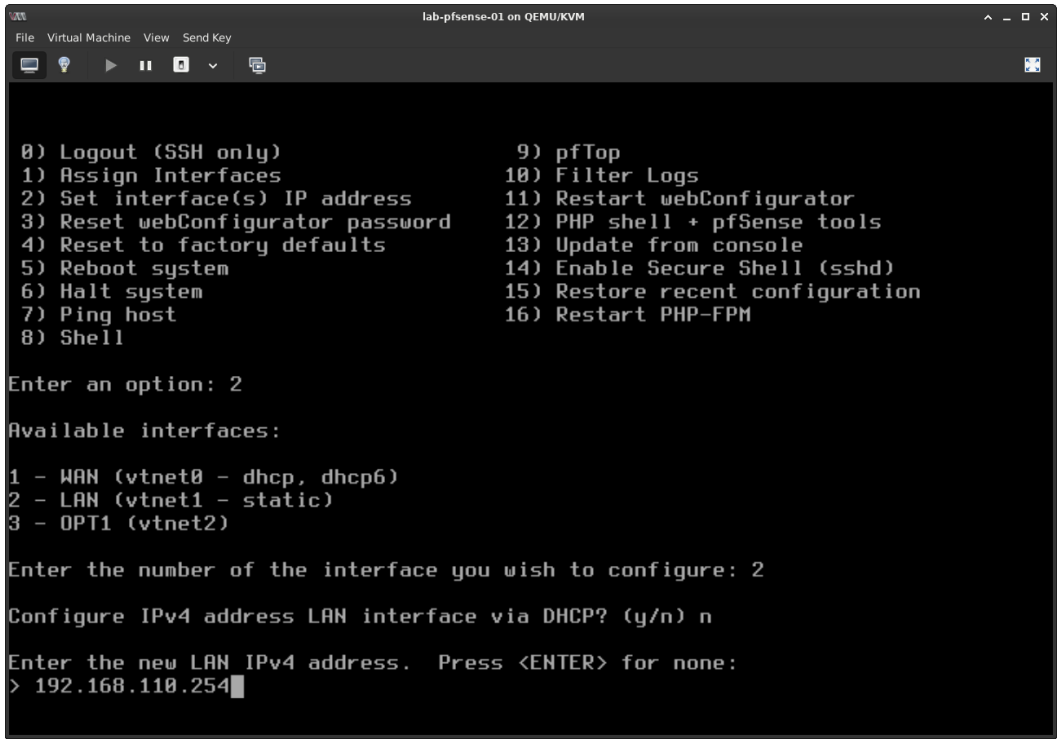


2 : (Set interface(s) IP address).

On fixe l'adresse IP de la passerelle (le pfSense lui-même) pour le réseau interne.

2 (LAN).

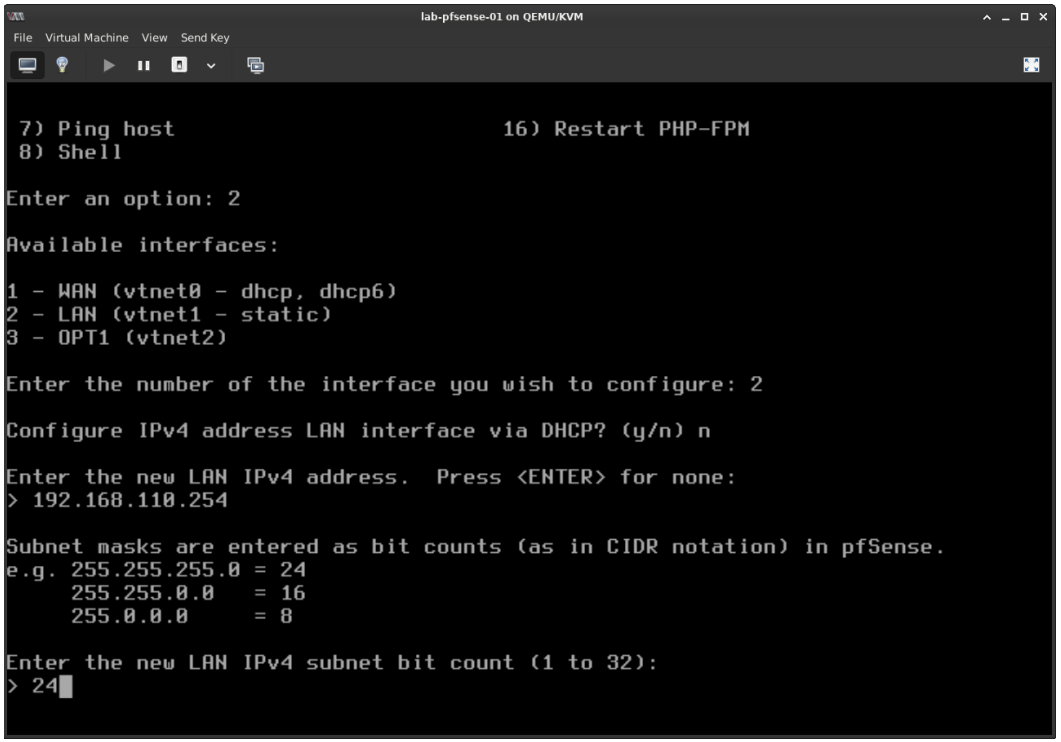


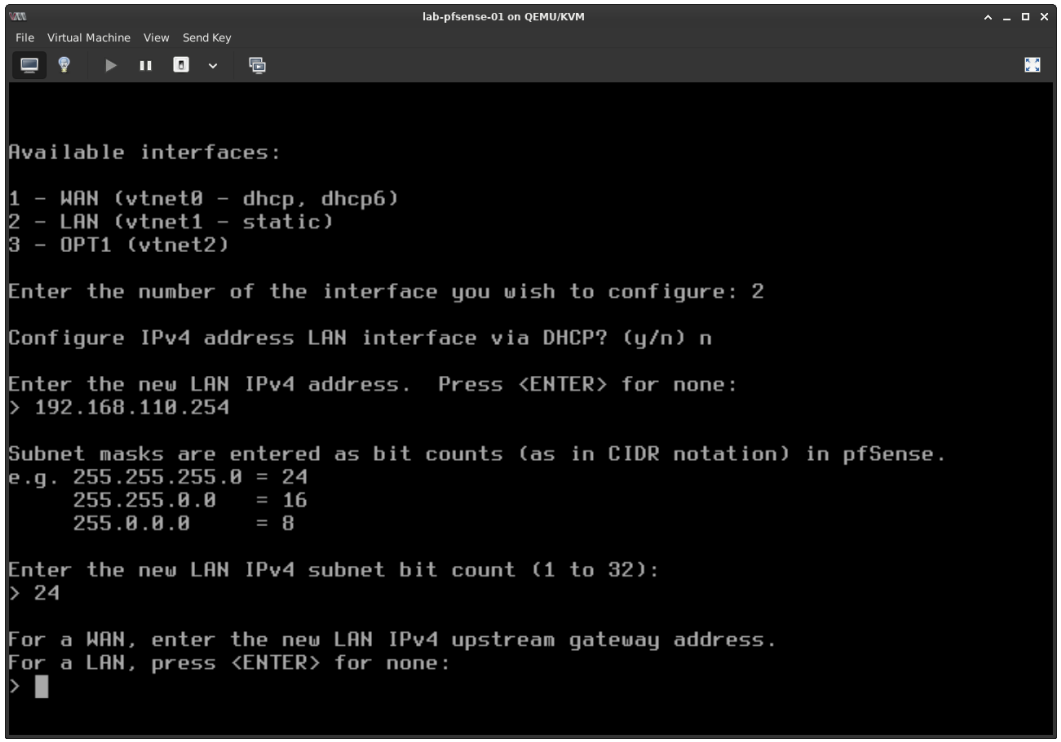


n : on veut une IP fixe, c'est un serveur (qui plus est une passerelle) !

192.168.110.254

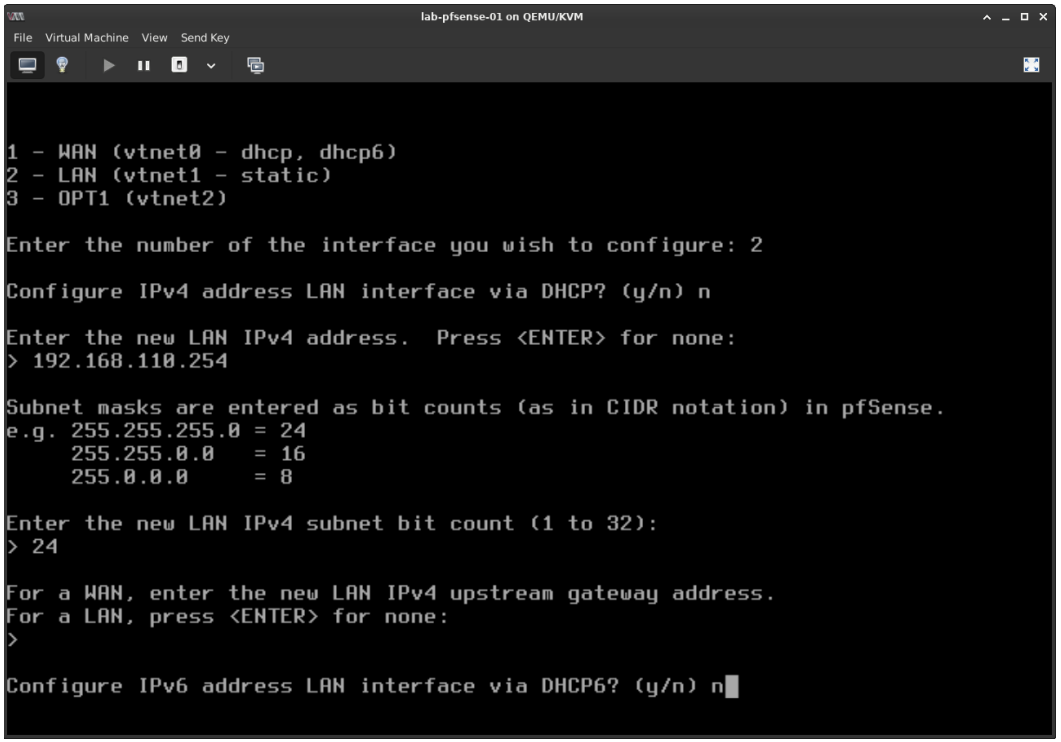
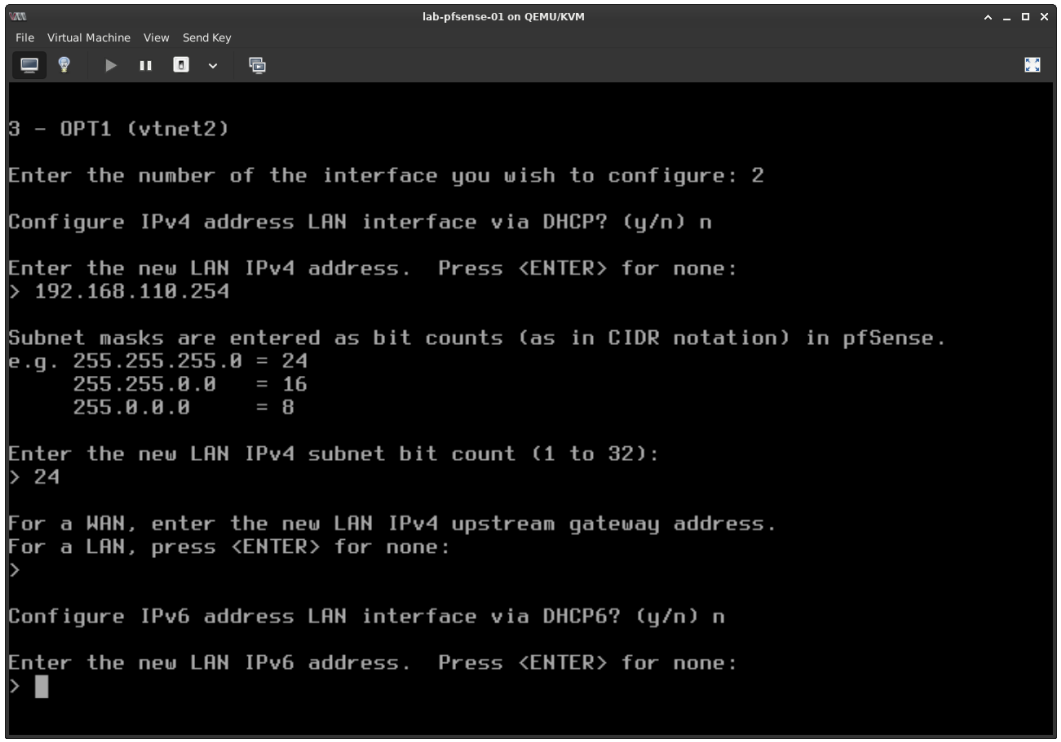
Note : L'usage du .254 (la dernière IP utilisable) est une convention courante pour les passerelles.

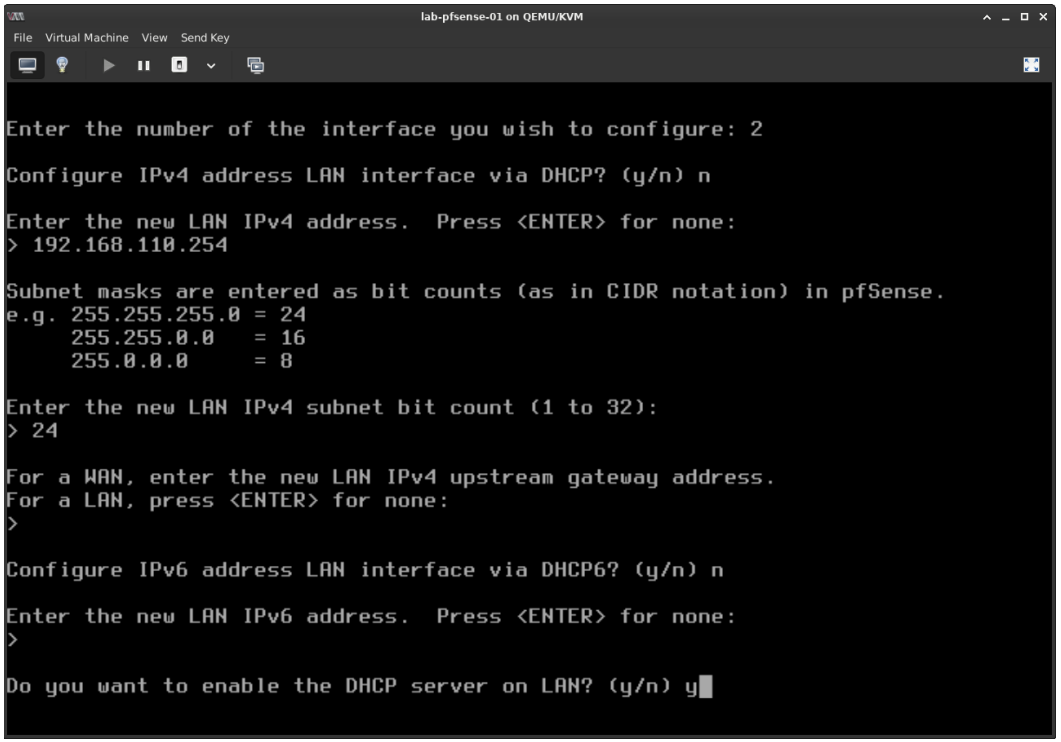


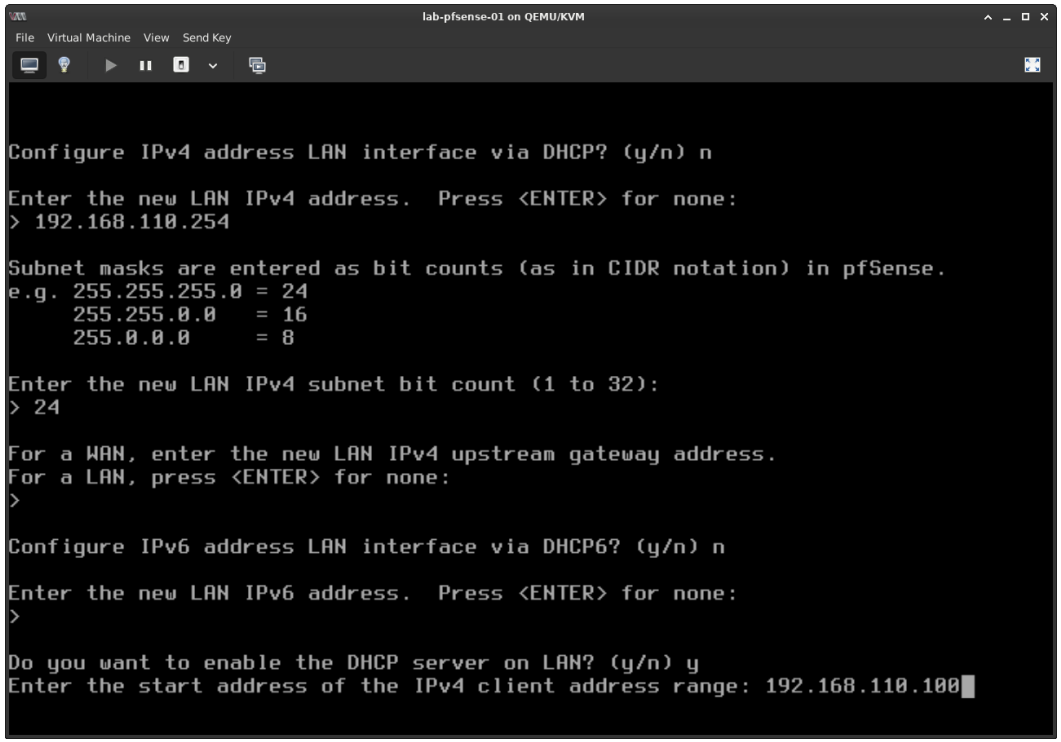


24 : (soit 255.255.255.0).

On réfléchie pas, **Entrée**. Il est la gateway …

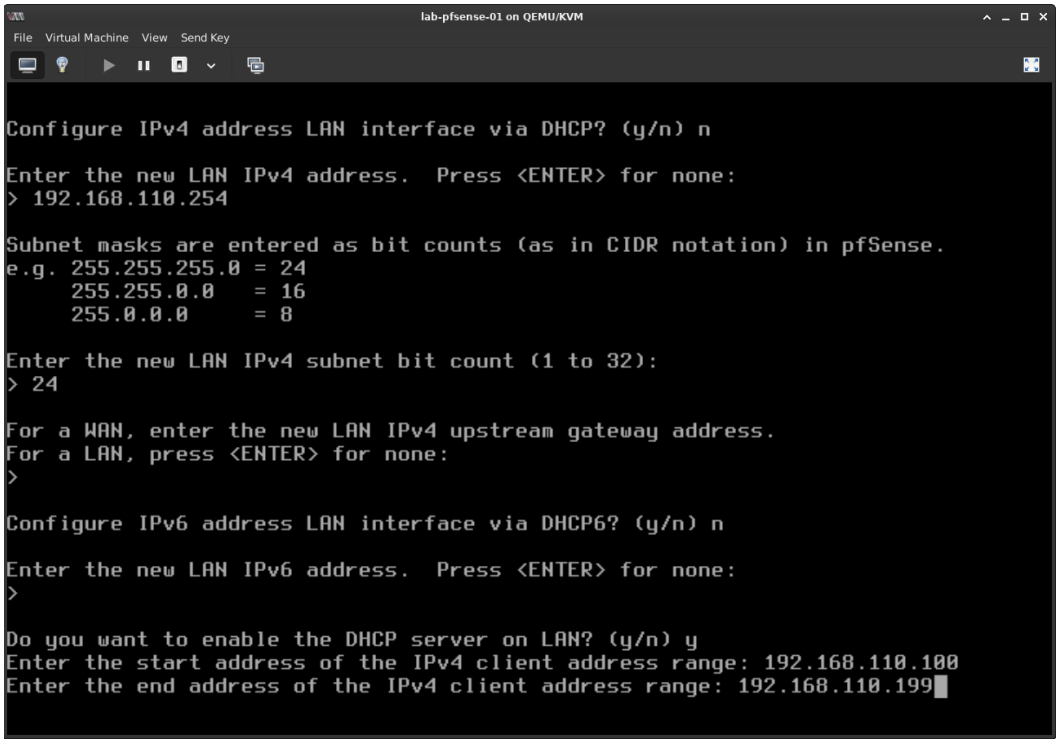
<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>n : (Sauf si vous êtes masochiste ou chez un FAI full IPv6).</td>
<td>Entrée</td>
</tr>
</table>

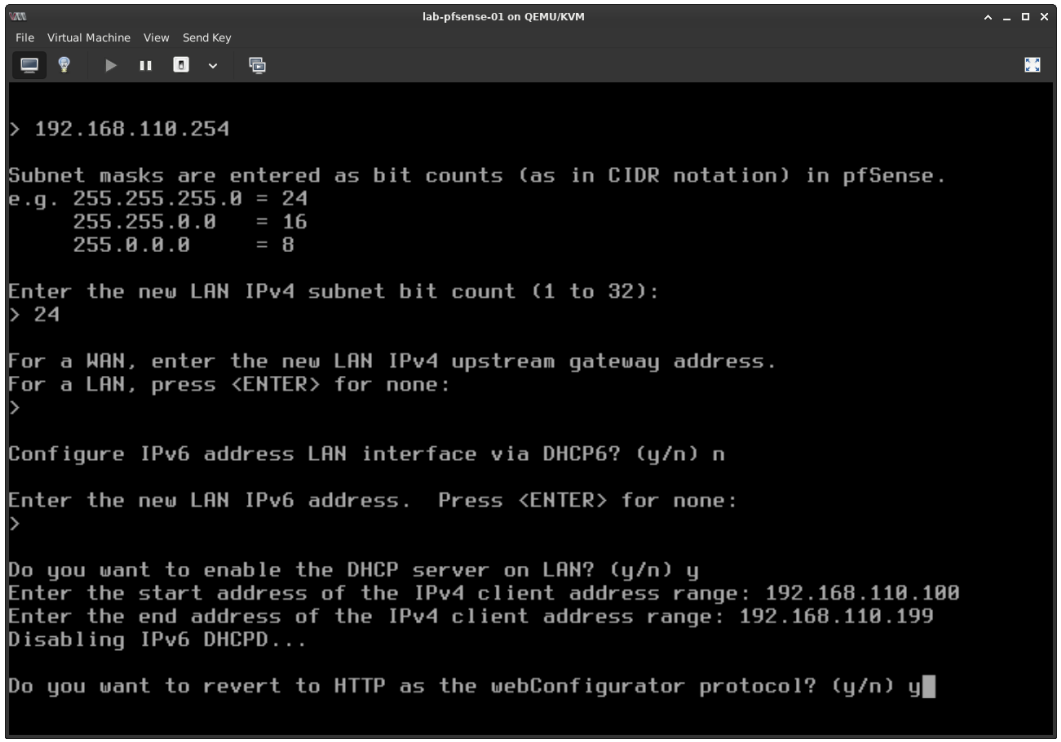




y : (Oui, pour distribuer des IP aux clients).

Plage DHCP : De **192.168.110.100**

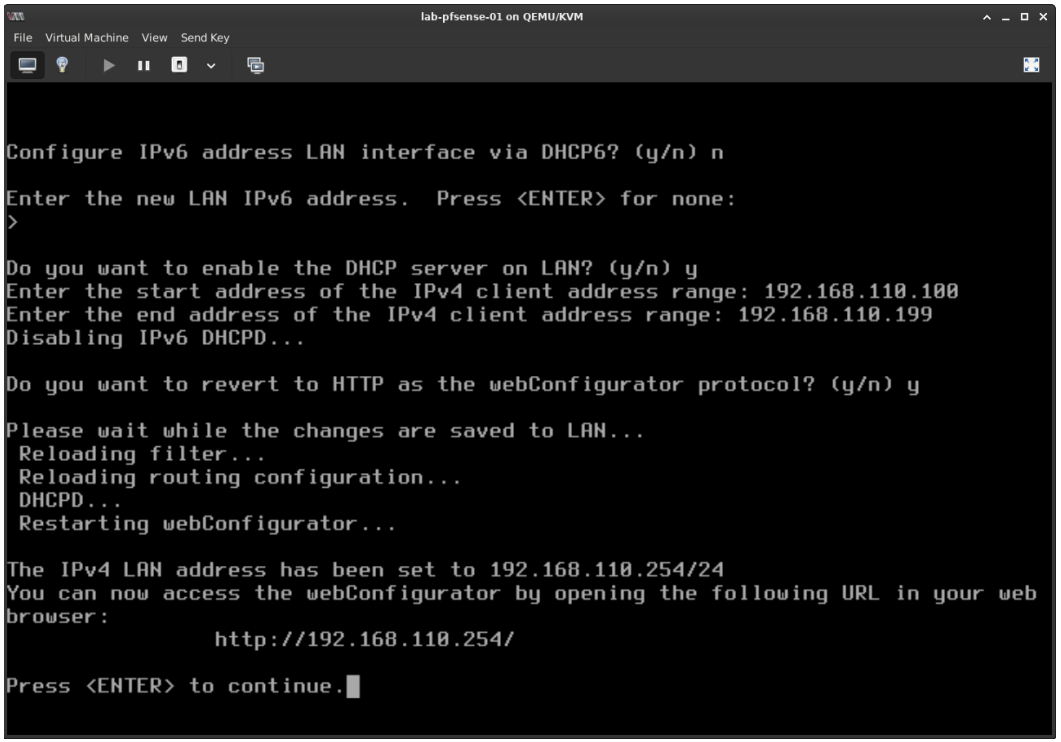
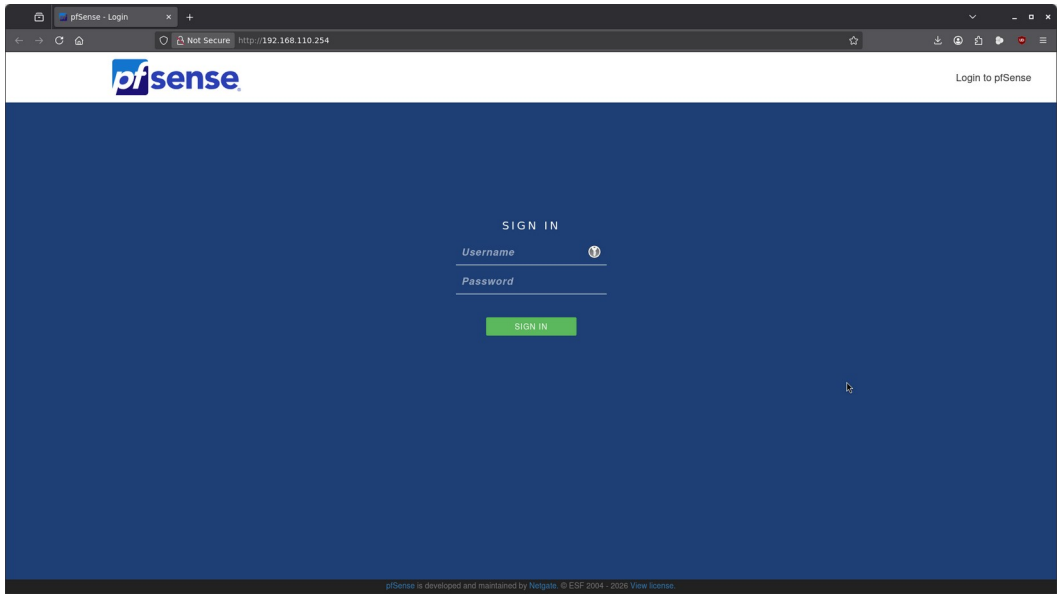




Plage DHCP : à **192.168.110.199**

y

Note : Dans un environnement Lab sans certificats valides, le HTTPS génère des alertes de sécurité pénibles. On passe en HTTP pour l'initialisation.

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Entrée</td>
<td>LOGIN : admin --> pfsense</td>
</tr>
</table>

Connexion en SSH

```
jesus@legion:~$ ssh admin@192.168.110.254
The authenticity of host '192.168.110.254 (192.168.110.254)' can't be established.
ED25519 key fingerprint is SHA256:xBPuXiLa9ERffcX7K6jwnnEMny5+7hzSrcjly4i8Q5U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes           <-- On accepte le fingerprint
Warning: Permanently added '192.168.110.254' (ED25519) to the list of known hosts.
(admin@192.168.110.254) Password for admin@pfSense.home.arpa:            <-- On rentre le mot de passe
```

```
QEMU Guest - Netgate Device ID: 5a1958d1b8fffc65ee59

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.100.112/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.110.254/24
 OPT1 (opt1)     -> vtnet2     ->

 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) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Parametrage de l’interface OPT1 (en SSH)

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.100.112/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.110.254/24
 OPT1 (opt1)     -> vtnet2     ->

 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) Disable 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 (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2)

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

```
Configure IPv4 address OPT1 interface via DHCP? (y/n) n
```

```
Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.120.254
```

```
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
```

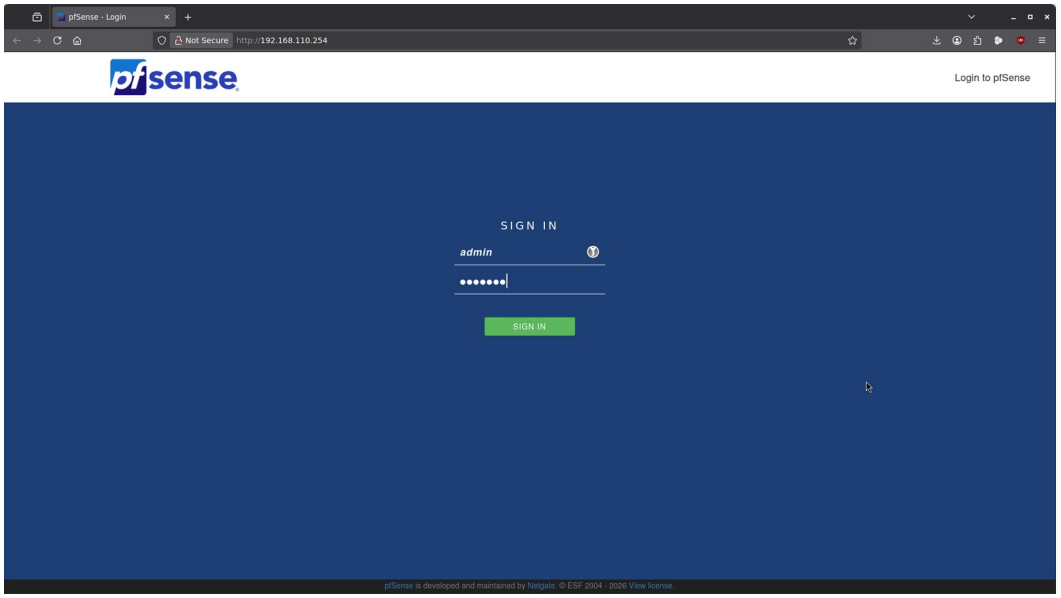
```
Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>
```

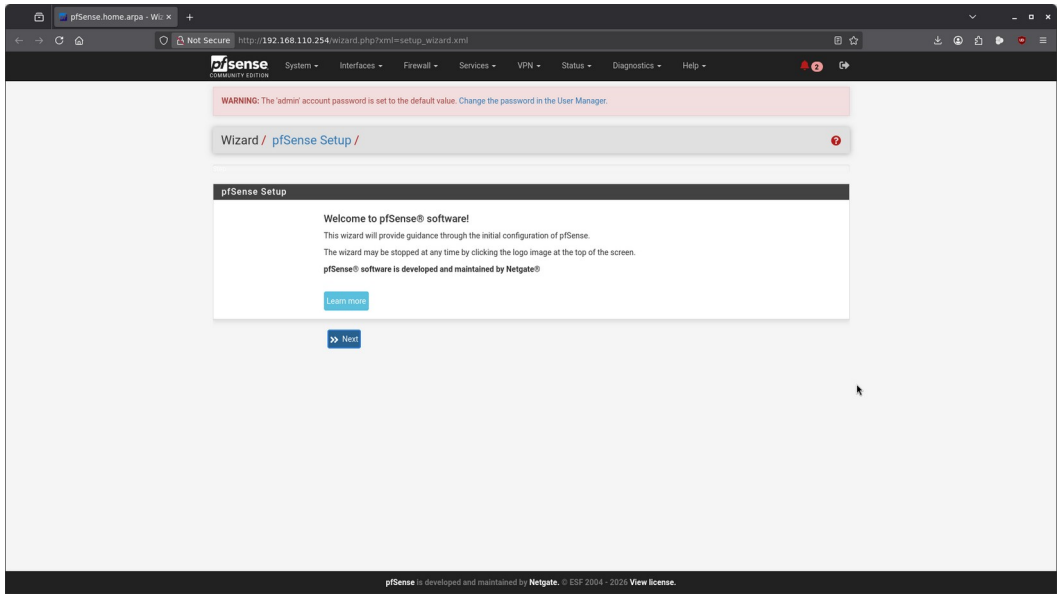
```
Do you want to enable the DHCP server on OPT1? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.120.100
Enter the end address of the IPv4 client address range: 192.168.120.199
Disabling IPv6 DHCPD...
```

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

The IPv4 OPT1 address has been set to 192.168.120.254/24
You can now access the webConfigurator by opening the following URL in your web browser:
              http://192.168.120.254/

Press <ENTER> to continue.
```

"Voilà. La bête a une adresse, elle parle le SSH, et elle distribue des IP comme des bonbons. Prochaine étape : L'interface Web."

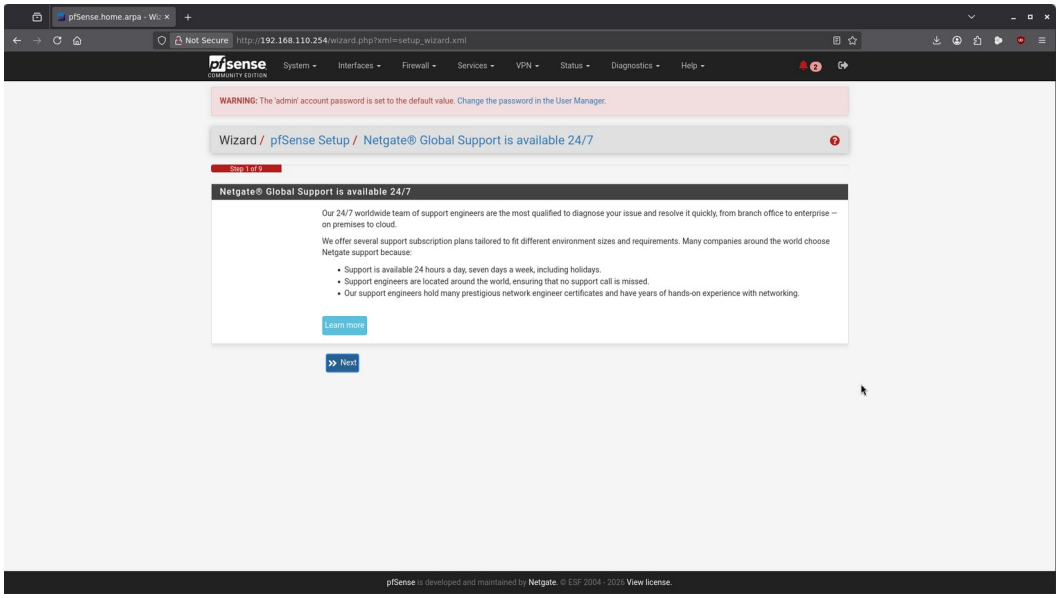
Premiere connexion a l'interface web



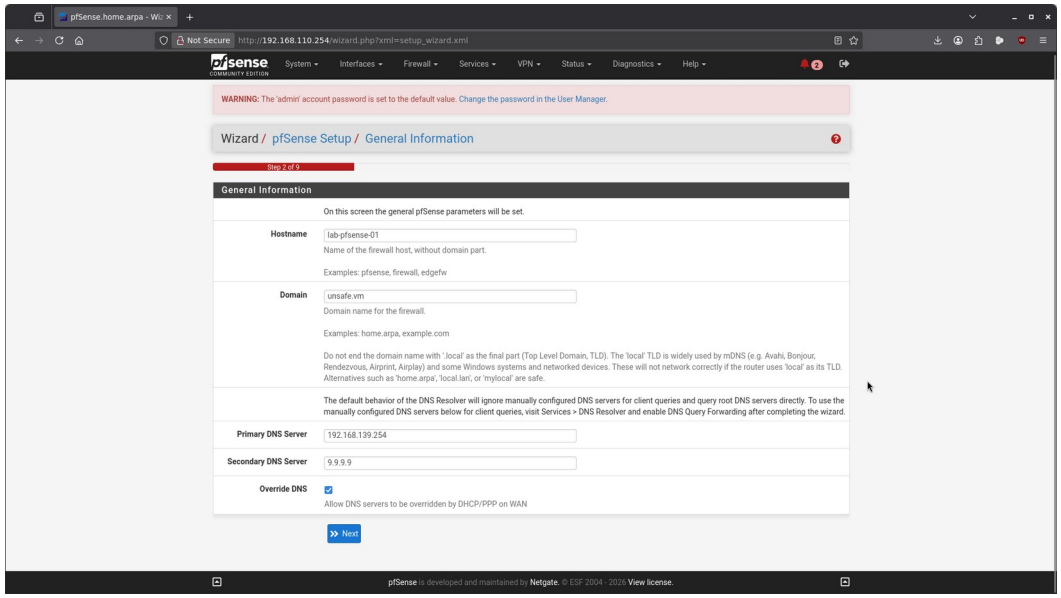


admin --> pfsense

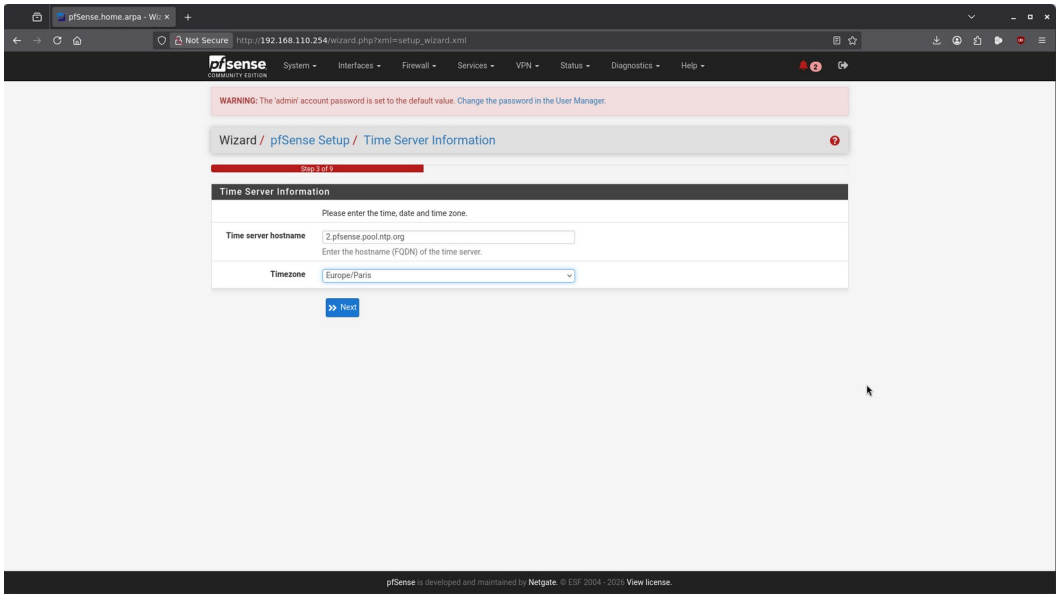
```
Message from syslogd@pfSense at Jan 14 14:16:58 ...
php-fpm[394]: /index.php: Successful login for user 'admin' from:
192.168.110.1 (Local Database)
```



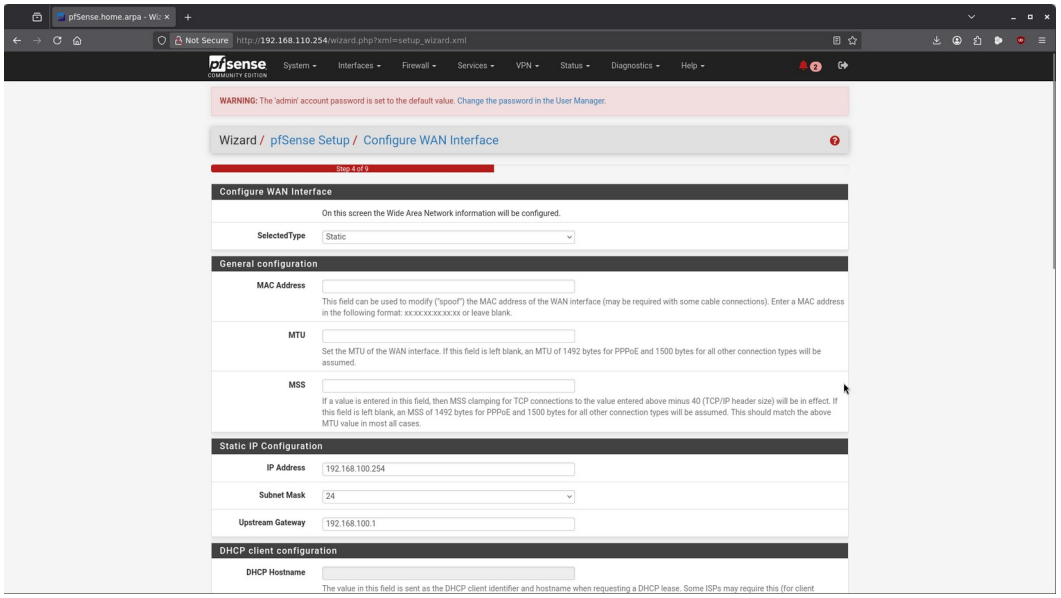
L'assistant "pfSense Setup" démarre automatiquement. Cliquez sur **Next**.

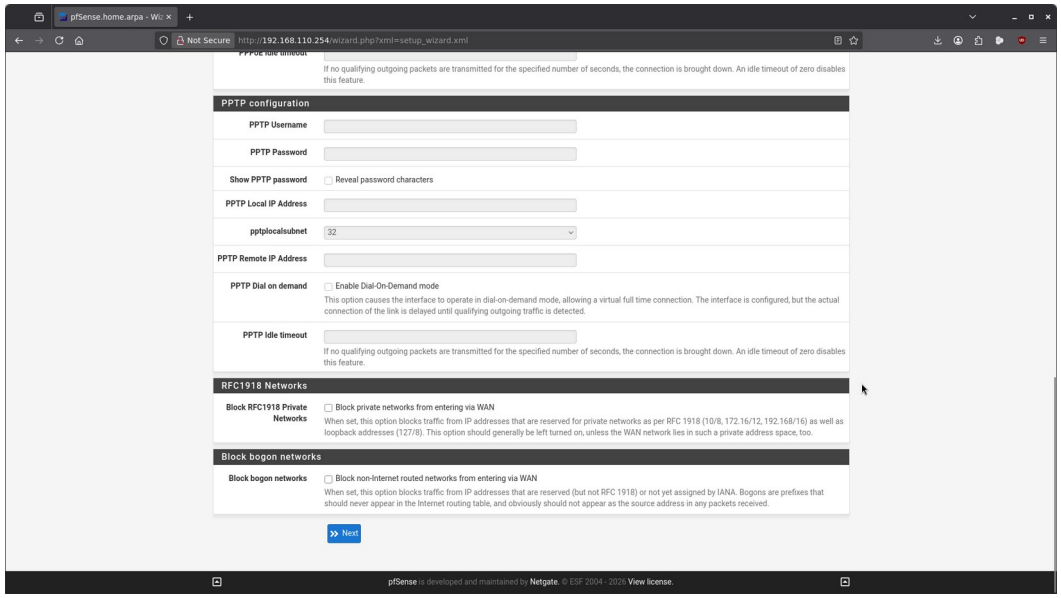


- **Hostname :** pfSense (ou le nom de votre choix, ex: fw-main).
- **Domain :** home.arpa (ou votre domaine lab).
- **Primary DNS Server :** Laisser vide pour utiliser ceux du WAN (DHCP) ou mettre 9.9.9.9 (ou encore 1.1.1.1 / 8.8.8.8 pour ceux qui aime bigbrother).

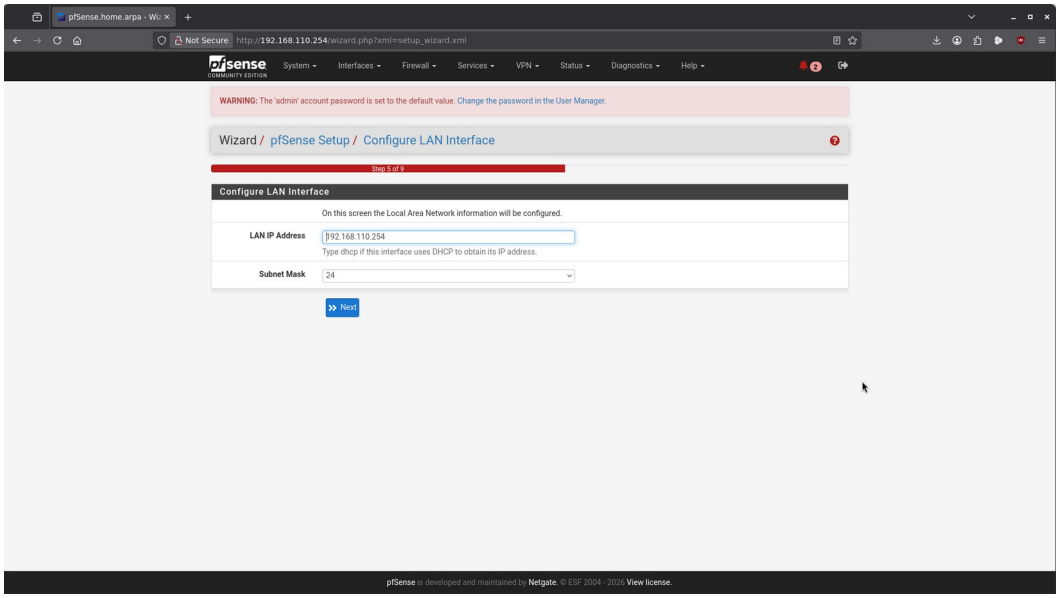


Sélectionner **Europe/Paris** (ou votre zone locale).

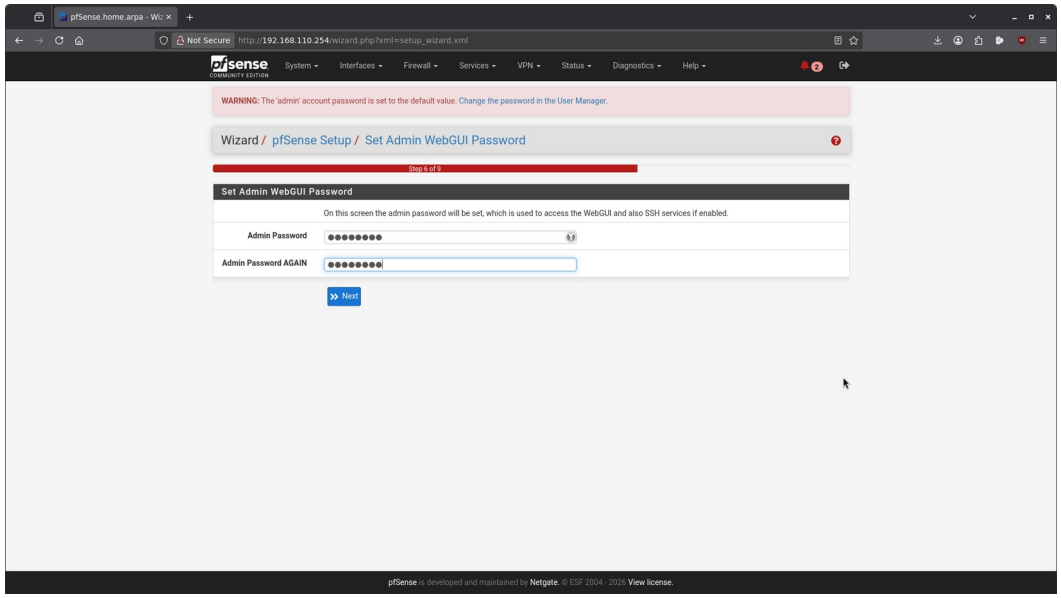




Décocher "Block private networks" (RFC1918) si votre WAN est derrière une Box FAI (double NAT), sinon vous bloquerez internet.

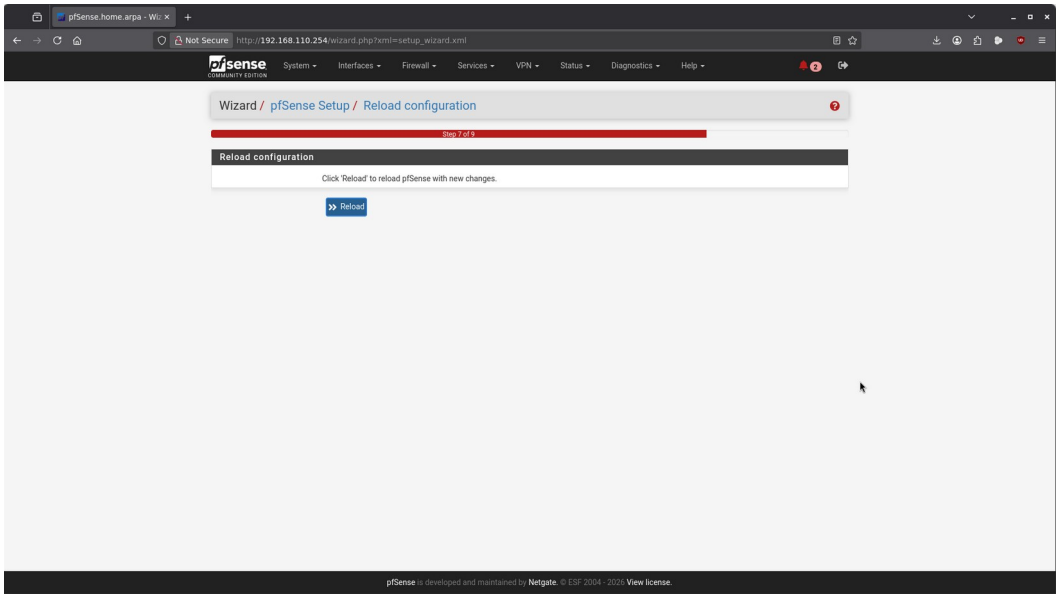
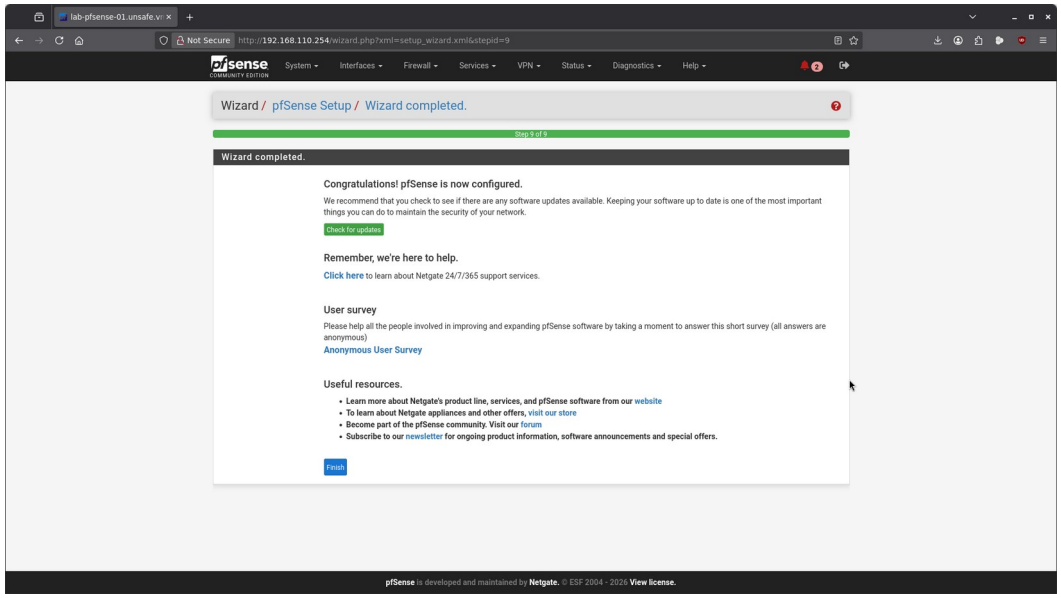


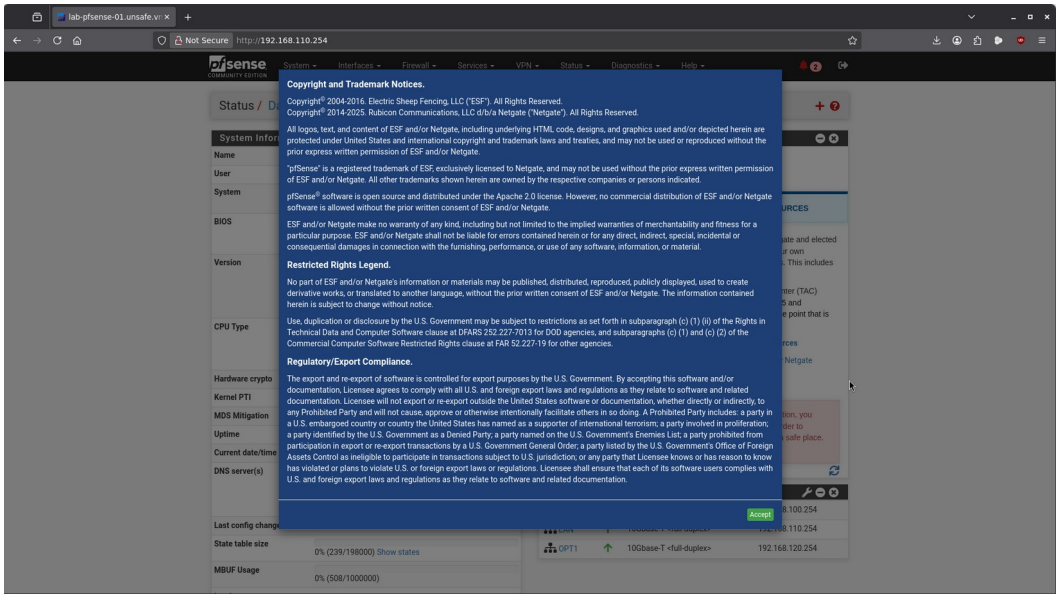
Vérifier l'IP : 192.168.110.254 / Mask /24. Normalement, c'est déjà pré-rempli (car nous l'avons déjà fait en ligne de commande)



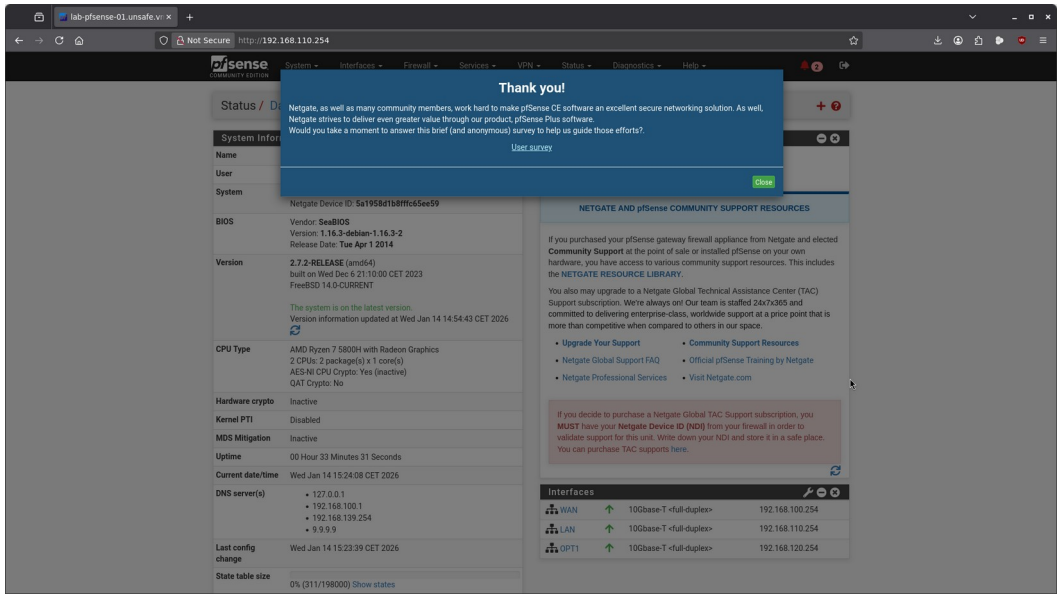
Action Critique : Définir un nouveau mot de passe complexe.

> "Pas de 123456. Pas de password. Soyez créatifs. Si vous oubliez ce mot de passe, il faudra revenir en console physique. C'est la punition pour avoir une mémoire de poisson rouge."

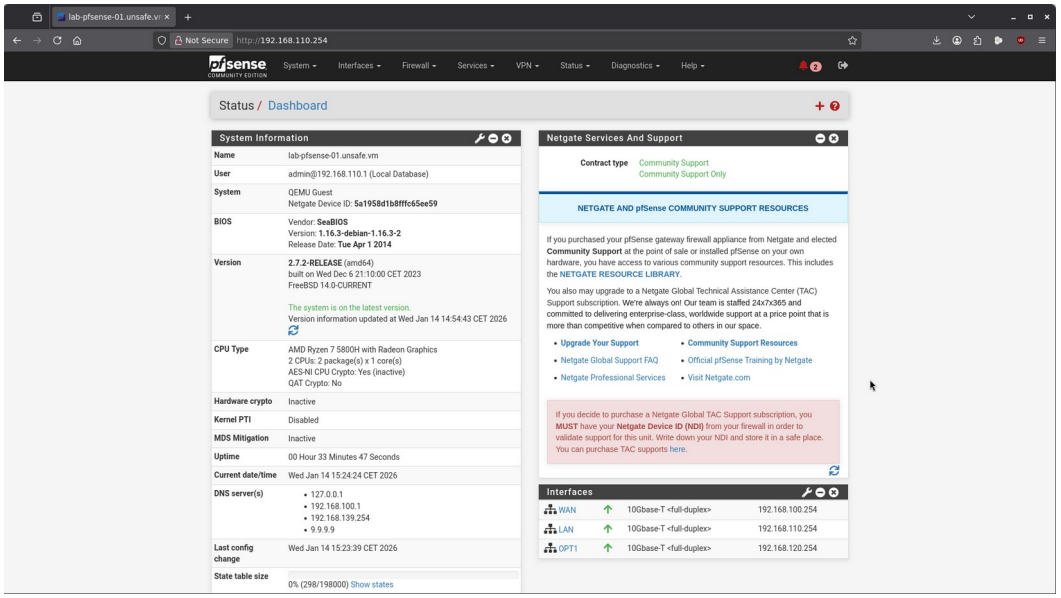
	
Cliquer sur le bouton **Reload**. PfSense applique toutes les modifications, redémarre les services et régénère les règles de filtrage.	"Congratulations! pfSense is now configured.".



On valide le blabla !



Again ...



Le Dashboard (Tableau de Bord)