

The logo for Simplon, featuring a dark blue vertical bar on the left and a blue arrow pointing right with the word "Simplon" inside.

Simplon

# Pfsense

Brief

## Table des matières

Contexte du projet .....	3
1. Définitions.....	5
Le nat : .....	5
Le wan : .....	5
Le lan : .....	6
Le firewall :.....	6
2. schéma de l'infrastructure mise en place. ....	7
3. l'installation et la configuration du firewall pfsense. ....	8
Installation.....	8
Configuration.....	11
4. les tests de validation.....	15

# Contexte du projet

Dans La Société D'eau Raillée, spécialisée dans le développement de logiciels, le département informatique a récemment investi dans une infrastructure basée sur des machines virtuelles pour héberger ses applications et services internes. L'entreprise a connu quelques problèmes de sécurité et de confidentialité des données ces derniers temps, ce qui a incité le département informatique à renforcer la sécurité de son réseau.

Le responsable de la sécurité informatique, en collaboration avec l'équipe des opérations informatiques, a décidé de mettre en place un pare-feu logiciel pour sécuriser l'infrastructure. Le choix s'est porté sur l'installation d'un pare-feu logiciel sur une VM dédiée.

Tâches du technicien :

**Sélection de la VM :** Le technicien doit sélectionner une VM adaptée pour héberger le pare-feu logiciel. Cette VM doit avoir des ressources suffisantes pour exécuter le logiciel de pare-feu tout en garantissant des performances optimales.

**Installation du système d'exploitation :** Avant d'installer le pare-feu, le technicien doit installer un système d'exploitation sur la VM. Un système d'exploitation minimaliste et sécurisé est souvent recommandé pour réduire les vulnérabilités. (peu être fusionner avec l'étape suivante)

**Installation du pare-feu logiciel :** Une fois le système d'exploitation installé, le technicien installe le pare-feu logiciel choisi. Il configure les règles de pare-feu pour filtrer le trafic réseau entrant et sortant, en fonction des besoins de l'entreprise. Par exemple, il peut bloquer les connexions non autorisées, limiter l'accès à certains services, ouvrir uniquement certains ports, etc.

**Configuration avancée :** En fonction des besoins spécifiques de l'entreprise, le technicien peut devoir configurer des fonctionnalités avancées du pare-feu, telles que la surveillance du trafic, la détection des intrusions, la prévention des fuites de données, etc.

Tests et validation : Une fois la configuration terminée, le technicien effectue des tests pour s'assurer que le pare-feu fonctionne correctement. Il teste différentes situations, comme le blocage de connexions non autorisées, la redirection de trafic, la gestion des performances, etc.

Documentation : Enfin, le technicien documente toutes les étapes de mise en place du pare-feu, y compris les configurations réalisées, les règles de pare-feu, les tests effectués, etc. Cette documentation est essentielle pour assurer la maintenance future du pare-feu et pour former d'autres membres de l'équipe.

Conclusion :

En mettant en place un pare-feu logiciel sur une VM, l'entreprise renforce la sécurité de son infrastructure informatique. Le technicien joue un rôle crucial dans ce processus, en sélectionnant les bons outils, en les configurant correctement et en s'assurant de leur bon fonctionnement. Ce pare-feu contribue à protéger les données sensibles de l'entreprise et à garantir la disponibilité et l'intégrité de ses services.

# 1. Définitions.

## **Le nat :**

Le mécanisme de translation d'adresses (aussi appelé Network Address Translation ou NAT) a été conçu pour répondre à la pénurie d'adresses IP utilisées avec le protocole IPv4.

Le fonctionnement du NAT consiste à utiliser une seule adresse IP routable (ou un nombre limité d'adresses IP), afin de connecter l'ensemble des machines du réseau. Ceci permet de réaliser une translation au niveau de la passerelle de connexion à Internet entre l'adresse interne de la machine souhaitant se connecter (qui est non routable) et l'adresse IP de la passerelle.

Ce processus permet de sécuriser le réseau interne, puisqu'il masque totalement l'adressage interne. Vu d'un observateur extérieur au réseau, toutes les requêtes semblent provenir de la même adresse IP.

## **Le wan :**

le WAN, ou réseau étendu, est un réseau informatique qui connecte des réseaux plus petits. Étant donné que les WAN ne sont pas liés à un emplacement spécifique, ils permettent aux réseaux localisés de communiquer entre eux sur de grandes distances. Ils facilitent également la communication et le partage d'informations entre les dispositifs, partout dans le monde.

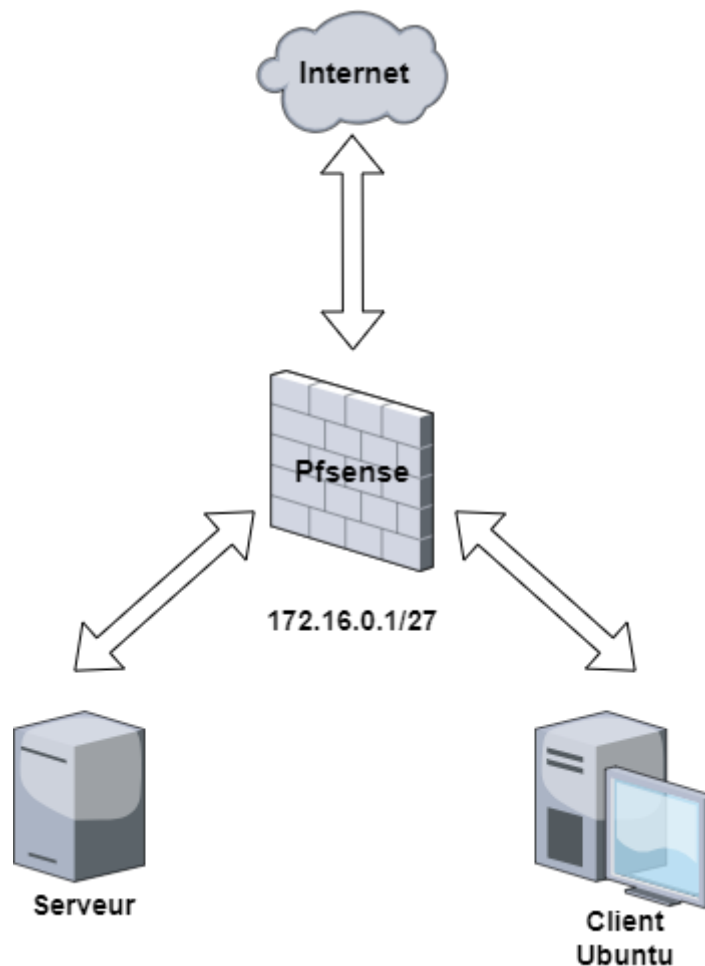
## **Le lan :**

Acronyme de Local Area Network, le terme LAN désigne un réseau informatique local. Il est constitué d'un ensemble d'ordinateurs et de périphériques reliés entre eux.

## **Le firewall :**

Un firewall est un appareil de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de données en se basant sur un ensemble de règles de sécurité. Il est chargé de dresser une barrière entre votre réseau interne et le trafic entrant provenant de sources externes (comme Internet) afin de bloquer le trafic malveillant.

## 2. schéma de l'infrastructure mise en place.



Masque réseau: 255.255.255.224

Adresse réseau: 172.16.0.0

Adresse du premier hôte: 172.16.0.1

Adresse du dernier hôte: 172.16.0.30

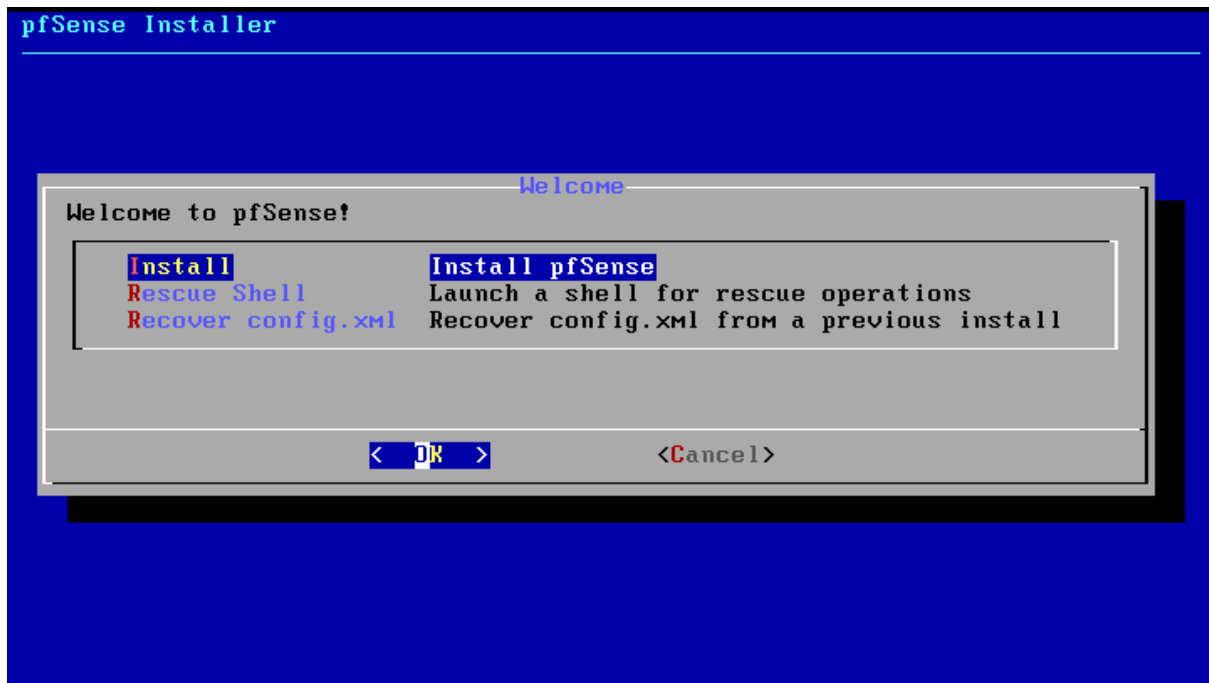
Adresse de diffusion: 172.16.0.31

Nombre maximal d'hôtes: 30

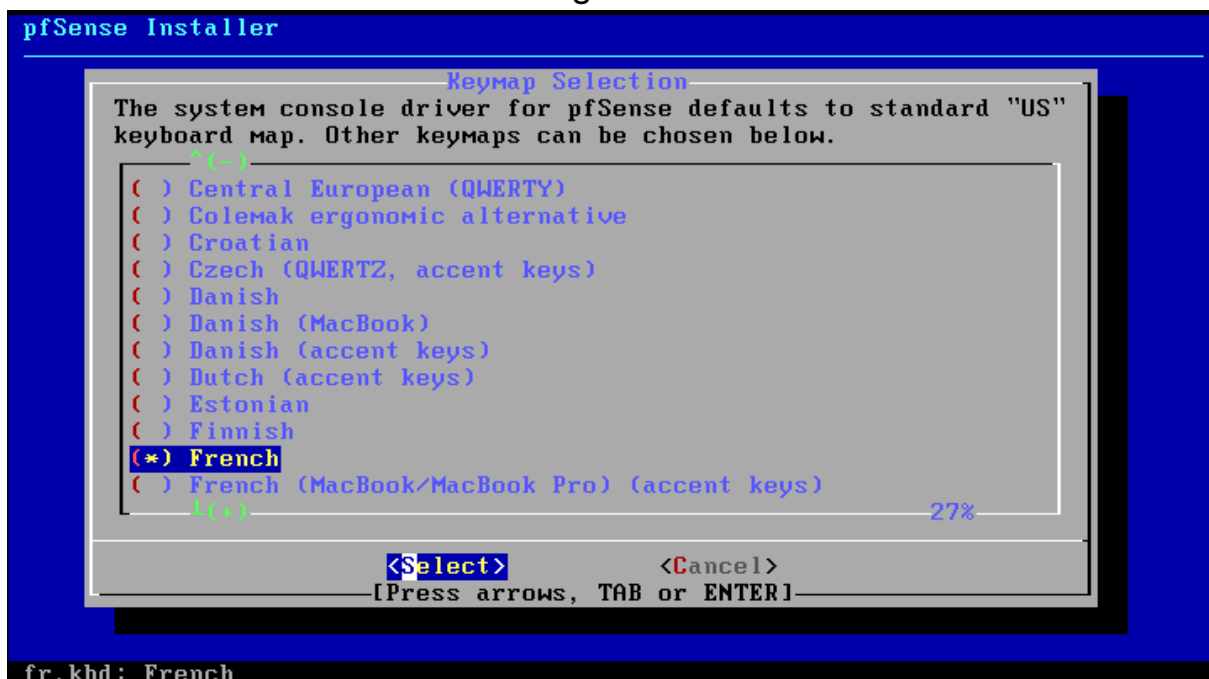
### 3. l'installation et la configuration du firewall pfsense.

#### Installation

Lors du lancement de l'iso pfsense, on va pouvoir choisir de l'installer sur la machine

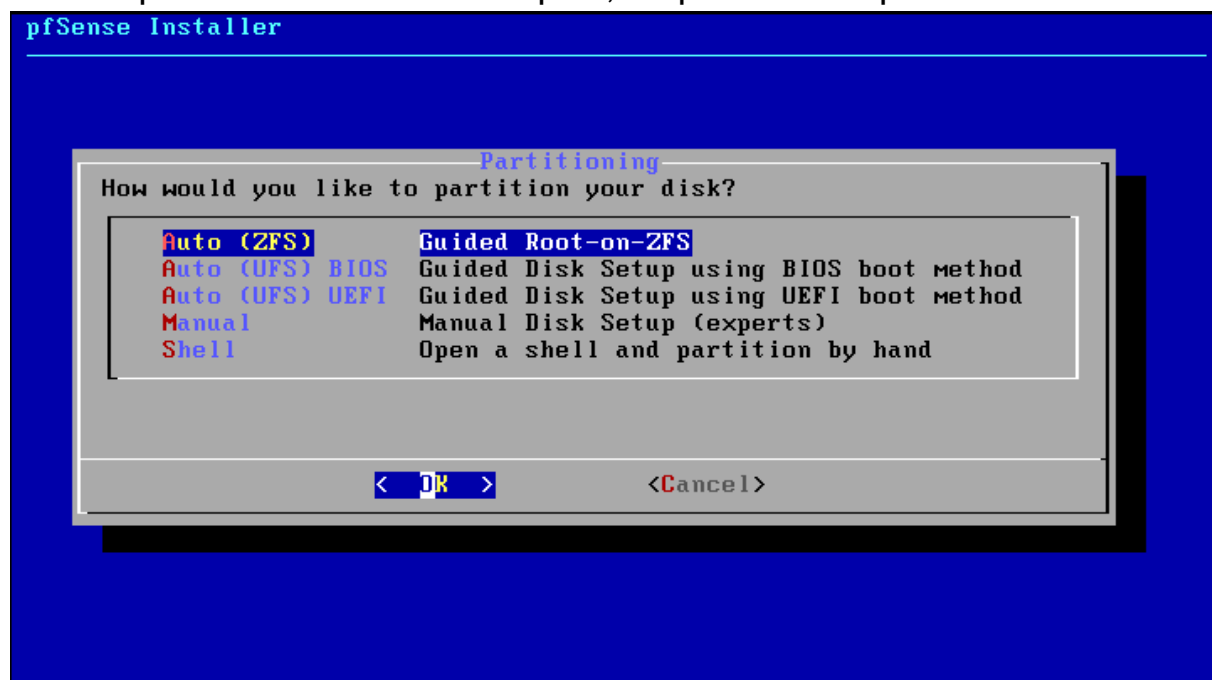


Ensuite il faut sélectionner la configuration du clavier

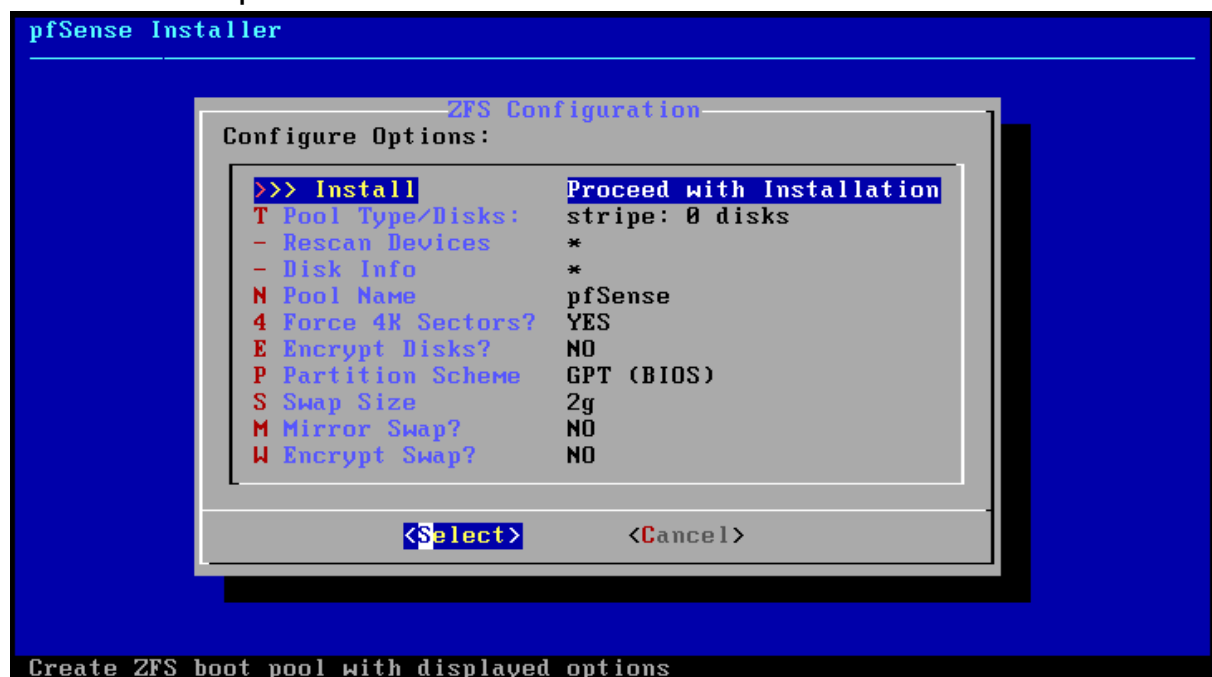




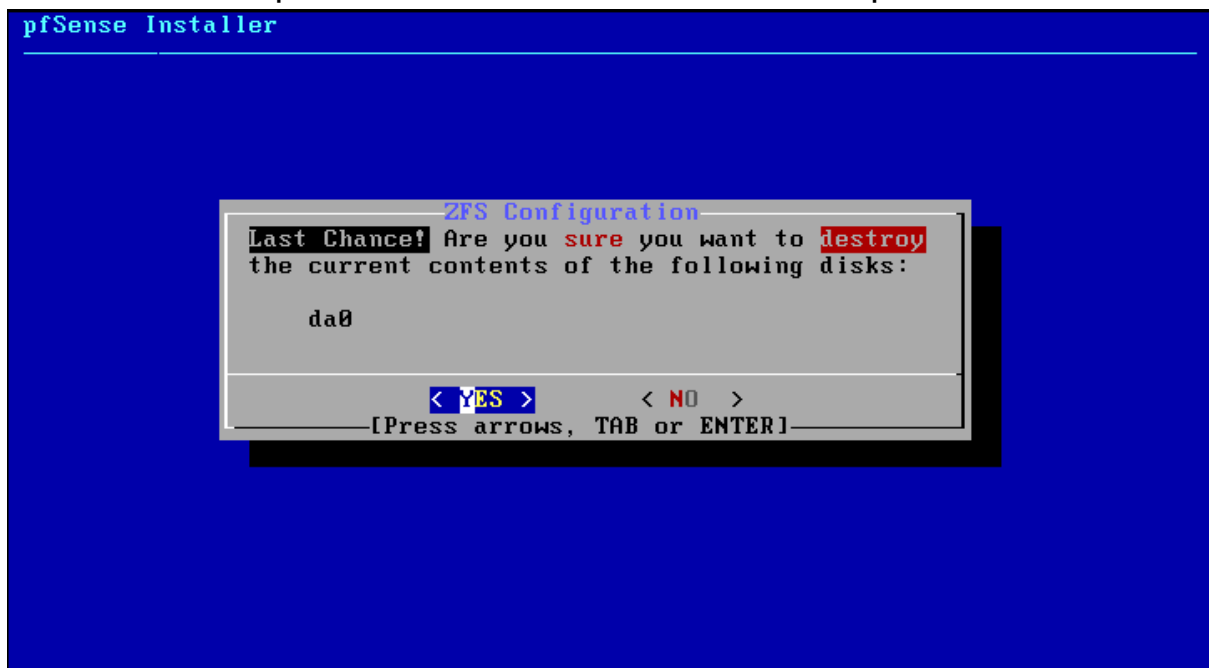
Pour le partitionnement des disques, on peut laisser par default



Et ensuite on procede à l'installation



On nous demande de choisir un disque, dans notre cas nous en avons un seul disponible, ensuite un message nous avertis que cela entraînera la perte des données de ce même disque.



L'installation se finalise, il est ensuite demandé de reboot la machine.



## Configuration

Tout d'abord, on va vérifier si nos LAN et WAN sont configuré sur les bonnes carte réseau, pour ce faire on va choisir l'option 1

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.195.142/24
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

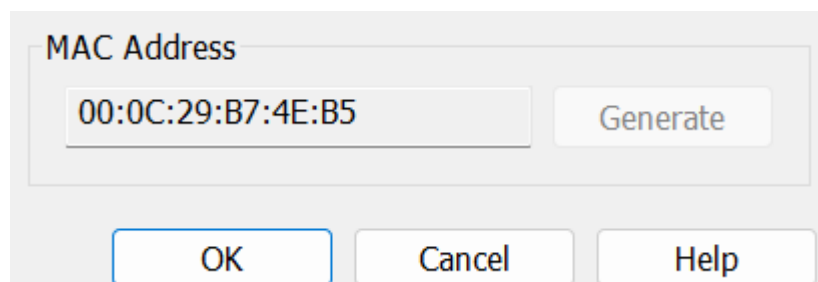
Enter an option: █
```

Ce qui nous donne

```
Valid interfaces are:

em0      00:0c:29:b7:4e:b5   (up) Intel(R) PRO/1000 Network Connection
em1      00:0c:29:b7:4e:bf   (up) Intel(R) PRO/1000 Network Connection
```

Em0 correspond au WAN, on va ensuite vérifier l'adresse mac de notre carte réseau WAN sur vmware



Les deux adresses correspondent, donc c'est bien configuré.

Ensuite on va configurer l'adresse ip de notre lan

```
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 (em1 - static)
```

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

Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 172.16.0.1

Enter the new LAN IPv4 subnet bit count (1 to 31):  
> 27

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)

Là, on nous demande de configurer le DHCP sur le LAN, il nous a demandé de créer une plage de 15 adresses avec le dhcp.

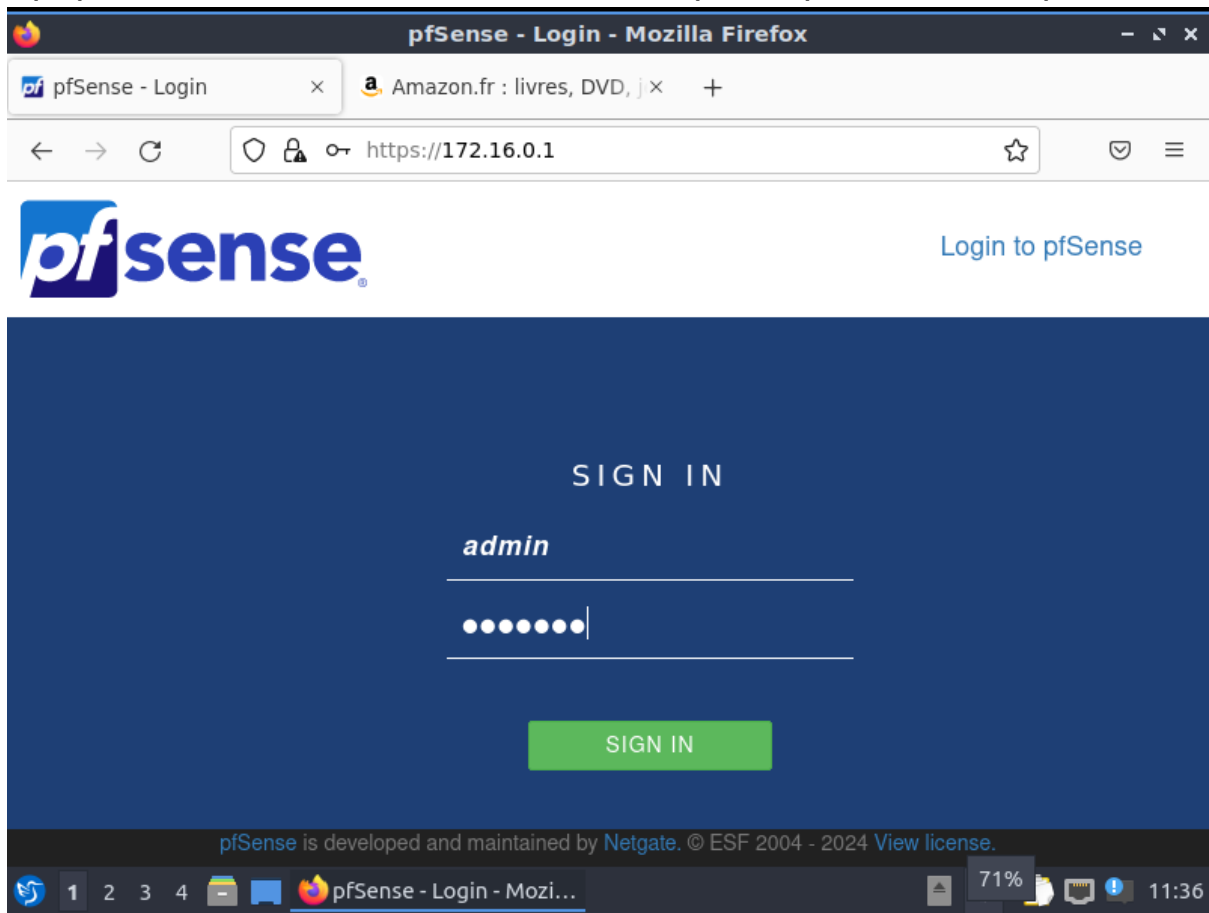
```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.0.2
Enter the end address of the IPv4 client address range: 172.16.0.16
Disabling IPv6 DHCPD...

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

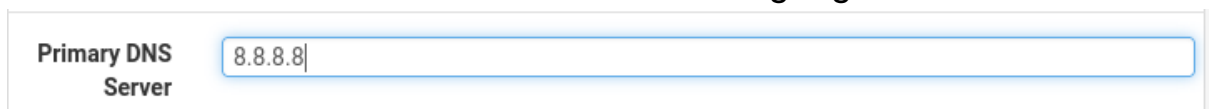
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 172.16.0.1/27
You can now access the webConfigurator by opening the following URL in your web browser:
    https://172.16.0.1/
```

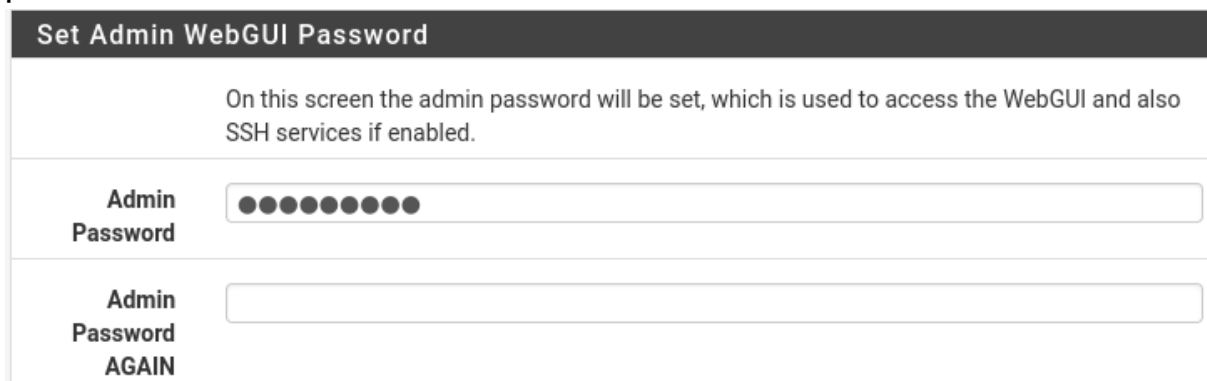
Depuis la machine ubuntu, il est maintenant possible de gérer le pfsense depuis une interface graphique en ouvrant un navigateur et en utilisant l'ip que l'on a defini sur le LAN, le mot de passe par défaut est pfsense



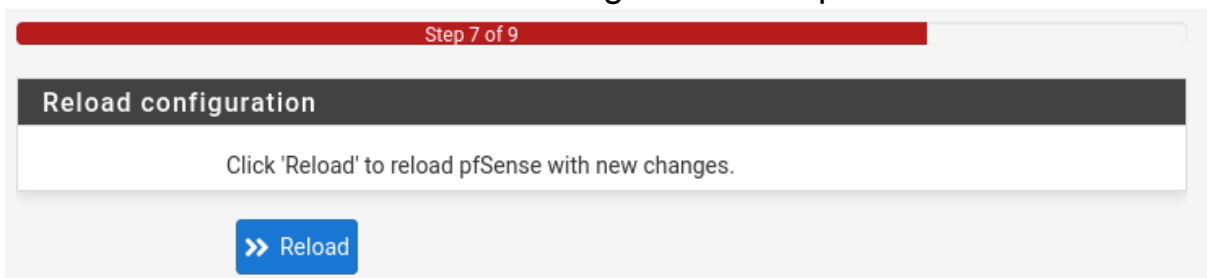
Une fois log, une page nous accueil, cliquez sur >>next  
Ensuite on nous demande d'indiquer notre DNS, nous n'en avons pas dans notre réseau donc on va utiliser celui de google.



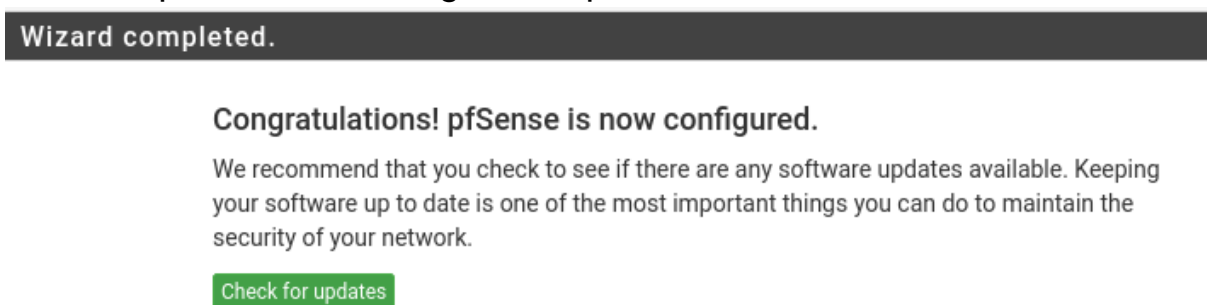
La page suivante nous demande de régler la timezone, ensuite faite next jusqu'à arriver a la page de modification du mot de passe Admin du pfsense



Pour des raison de sécurité on change le mot de passe et on reload



Et voilà ! pfsense est configuré et opérationnel.



## 4. les tests de validation.

Pfsense ping les 2 VMs Linux.

```
Enter a host name or IP address: 172.16.0.2

PING 172.16.0.2 (172.16.0.2): 56 data bytes
64 bytes from 172.16.0.2: icmp_seq=0 ttl=64 time=1.390 ms
64 bytes from 172.16.0.2: icmp_seq=1 ttl=64 time=1.272 ms
64 bytes from 172.16.0.2: icmp_seq=2 ttl=64 time=1.563 ms

--- 172.16.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.272/1.408/1.563/0.119 ms
```

```
Enter a host name or IP address: 172.16.0.10

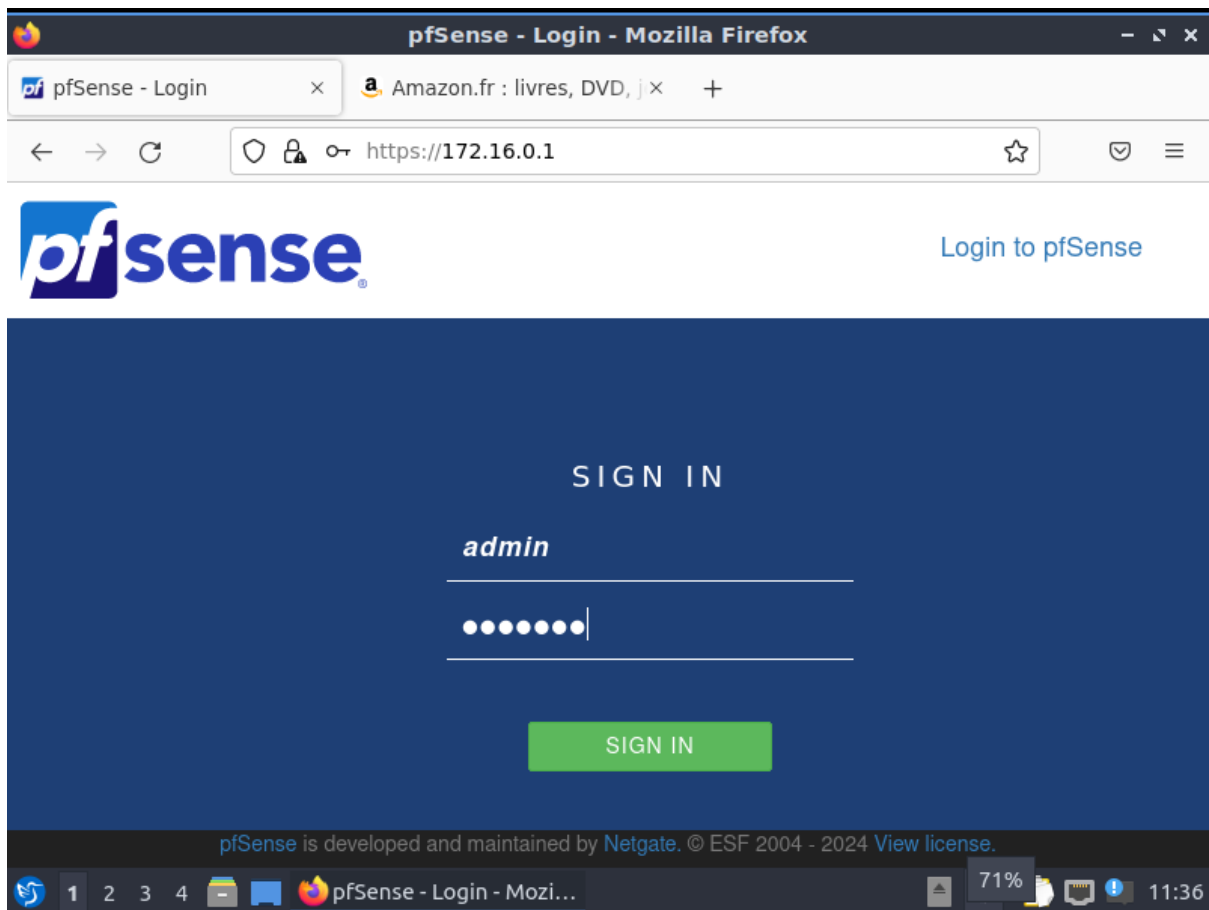
PING 172.16.0.10 (172.16.0.10): 56 data bytes
64 bytes from 172.16.0.10: icmp_seq=0 ttl=64 time=2.115 ms
64 bytes from 172.16.0.10: icmp_seq=1 ttl=64 time=1.574 ms
64 bytes from 172.16.0.10: icmp_seq=2 ttl=64 time=0.743 ms
```

Les 2 machines Linux ping l'adresse du LAN de Pfsense.

```
florient@ubuntu:~$ ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 172.16.0.1: icmp_seq=4 ttl=64 time=0.916 ms
64 bytes from 172.16.0.1: icmp_seq=5 ttl=64 time=2.18 ms

PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=1.36 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=1.57 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=64 time=1.47 ms
^C
--- 172.16.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.360/1.468/1.572/0.086 ms
```

La machine cliente a accès à l'interface Web de Pfsense.



Les 2 machines ont accès à internet.

```
florient@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=158 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=79.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=203 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=533 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 79.061/243.169/532.585/172.888 ms
florient@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=127 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=457 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=480 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=607 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4002ms
rtt min/avg/max/mdev = 126.664/417.548/606.739/177.364 ms
```