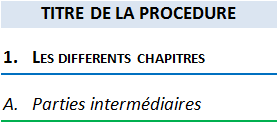
|  |  |
| --- | --- |
| **Installation et configuration d'un pare-feu avec pfSense** | |
| Cette procédure décrit l'installation et la configuration de pfSense en tant que pare-feu ainsi que l'implémentation de SquidGuard pour le filtrage de contenu Web. | |
|  |  |
| Auteur : Zakaria sow | Date de publication : 05/03/2025 |

|  |  |
| --- | --- |
| Objectif | L'objectif de cette procédure est de mettre en place un pare-feu fonctionnel afin de contrôler l'accès à Internet en appliquant des règles de filtrage des contenus web pour l’entreprise belletable |
| Ressources | Virtuelle compatible avec pfSense LINUX |
| Outils | Interface Web de pfSense ,Squid (proxy) et SquidGuard (filtrage de contenu) |
| URL | [Installation de Pfsense | pfSense | IT-Connect](https://www.it-connect.fr/installation-de-pfsense%ef%bb%bf/) |
| Autres |  |

**Convention**

Par convention, les informations particulières seront mises en avant tout au long de cette procédure en respectant les règles et mise en page ci-dessous :



Ce paragraphe apporte à l‘utilisateur une information qui pourra l’aider ou lui rappeler un ou plusieurs points précis et utiles pour sa réalisation.

Ce paragraphe apporte à l’utilisateur une information importante sur un ou plusieurs points précis.  
Celle-ci est indispensable pour la bonne réalisation de la procédure.

Table des matières

[TITRE PROCÉDURE 3](#_Toc764249688)

[1. Installation et configuration de Pfsense 4](#_Toc934677598)

[2. Configuration de pfsense 7](#_Toc1435201792)

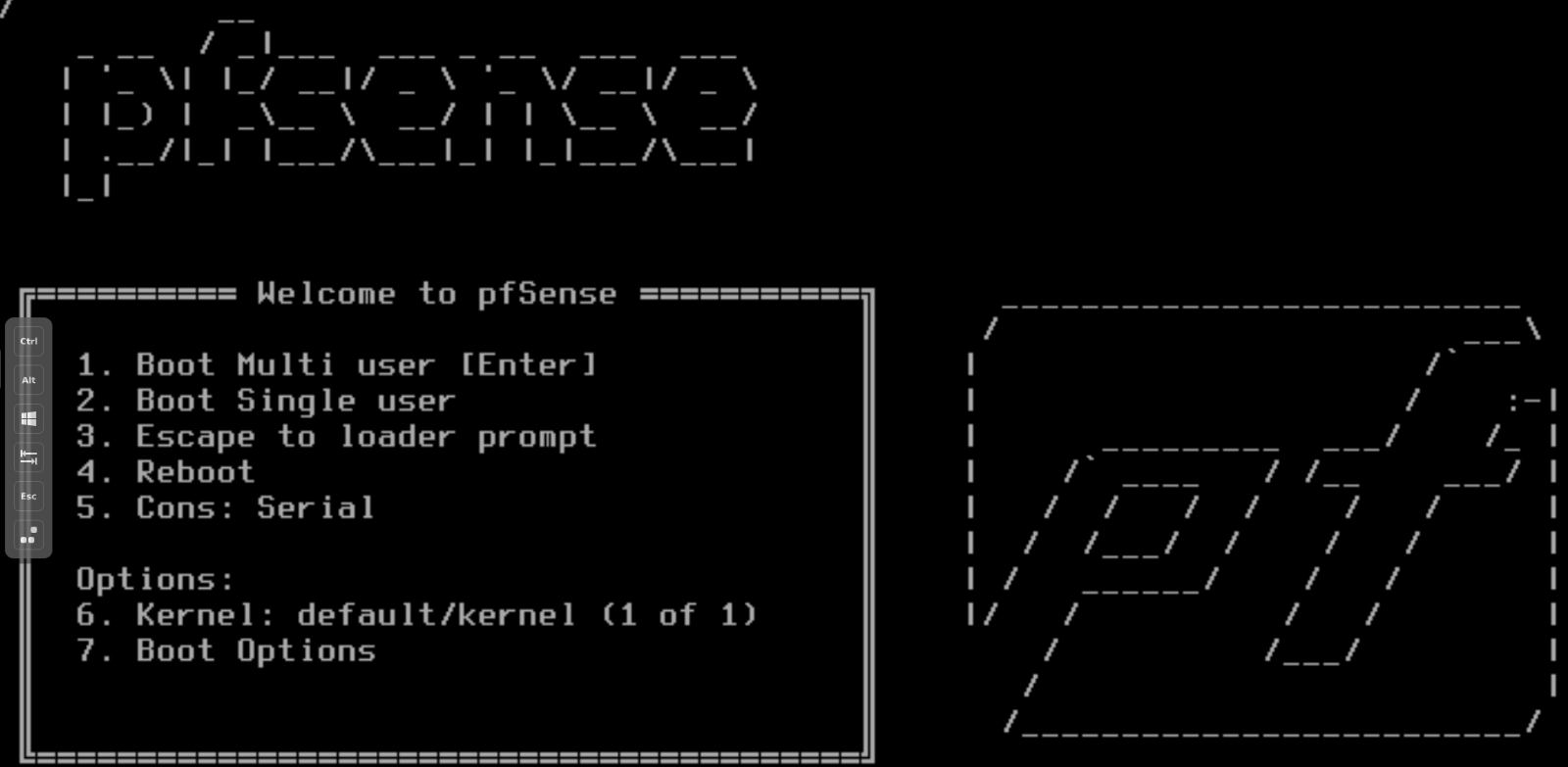
[A. Configuration de base 8](#_Toc1118863808)

[B. Installation et configuration de package squidguard 10](#_Toc690101868)

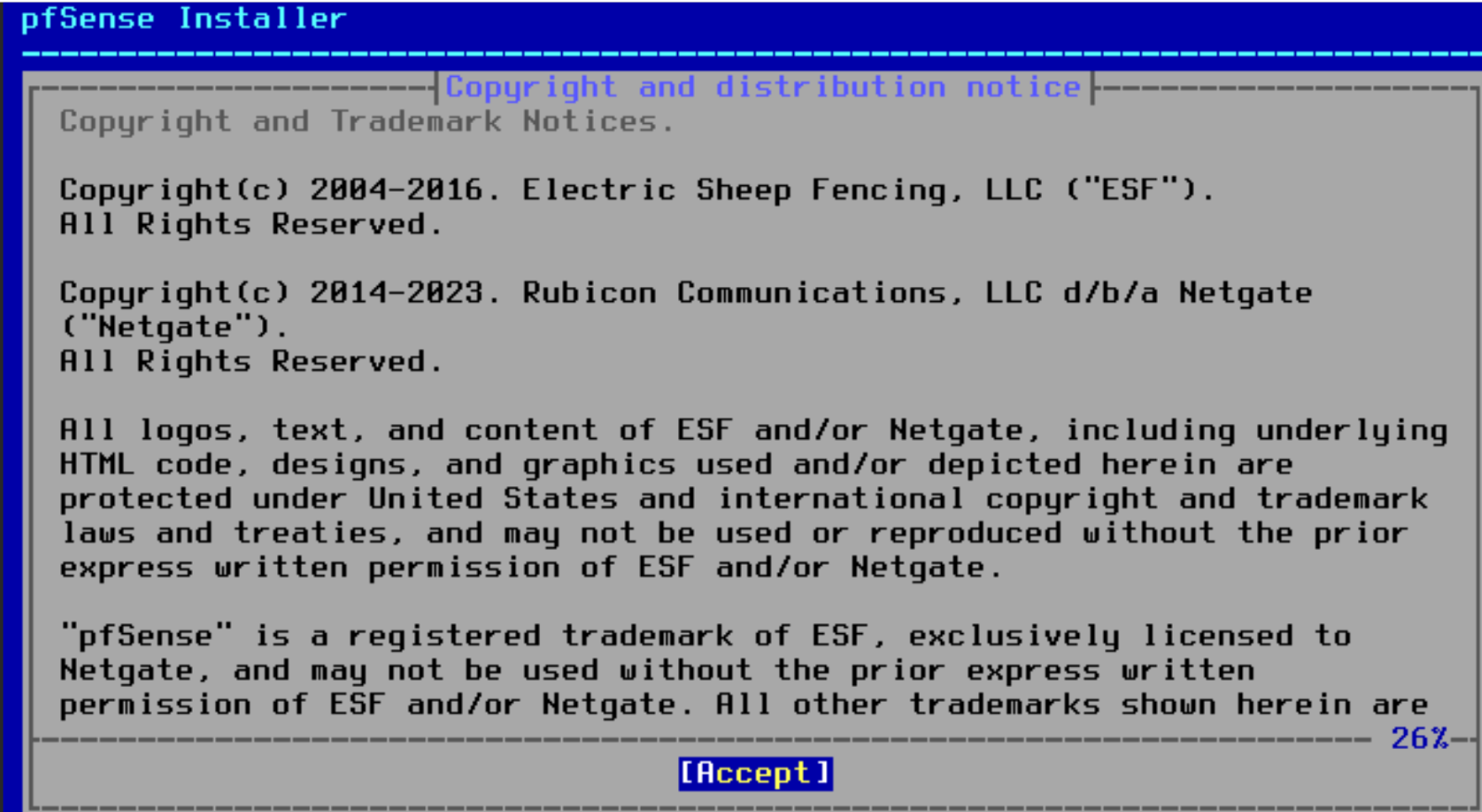
# TITRE PROCÉDURE

## Installation et configuration de Pfsense

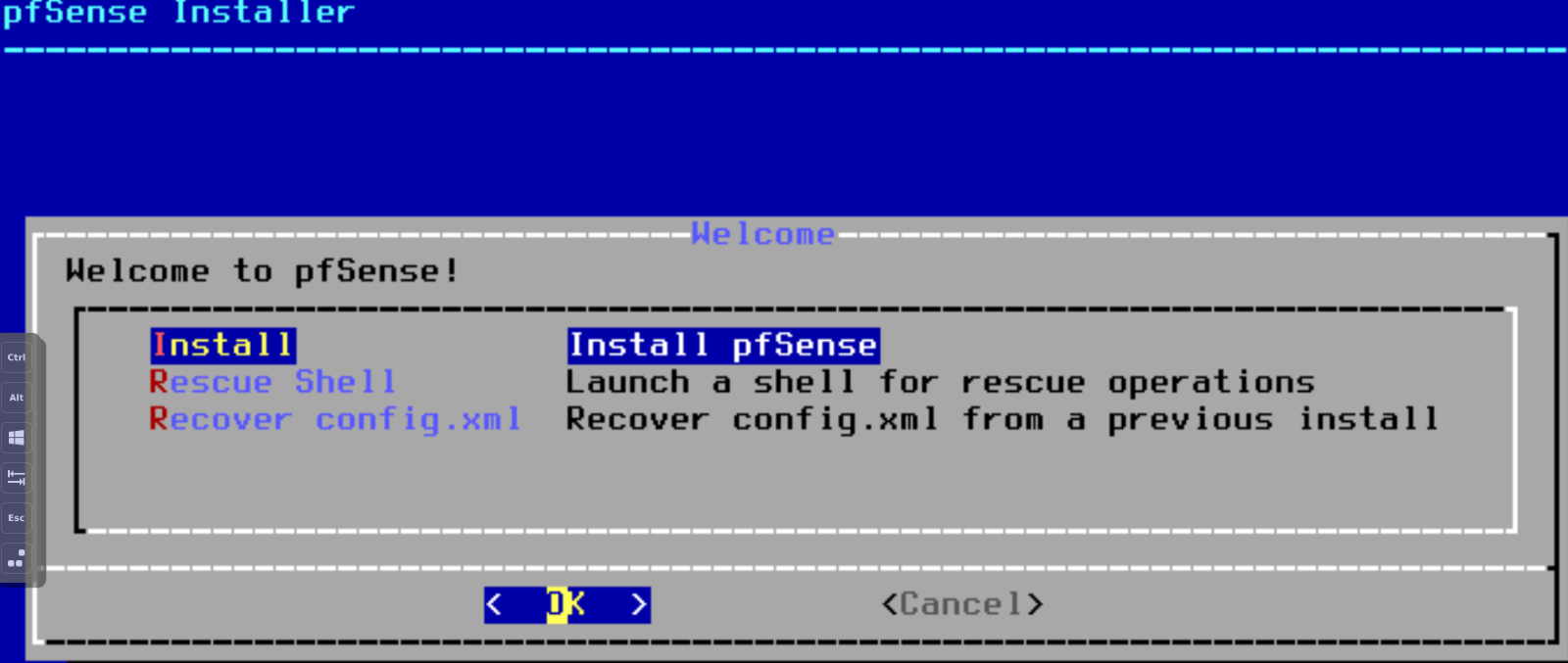
Appuyez sur "Entrée" pour booter avec les options par défaut.



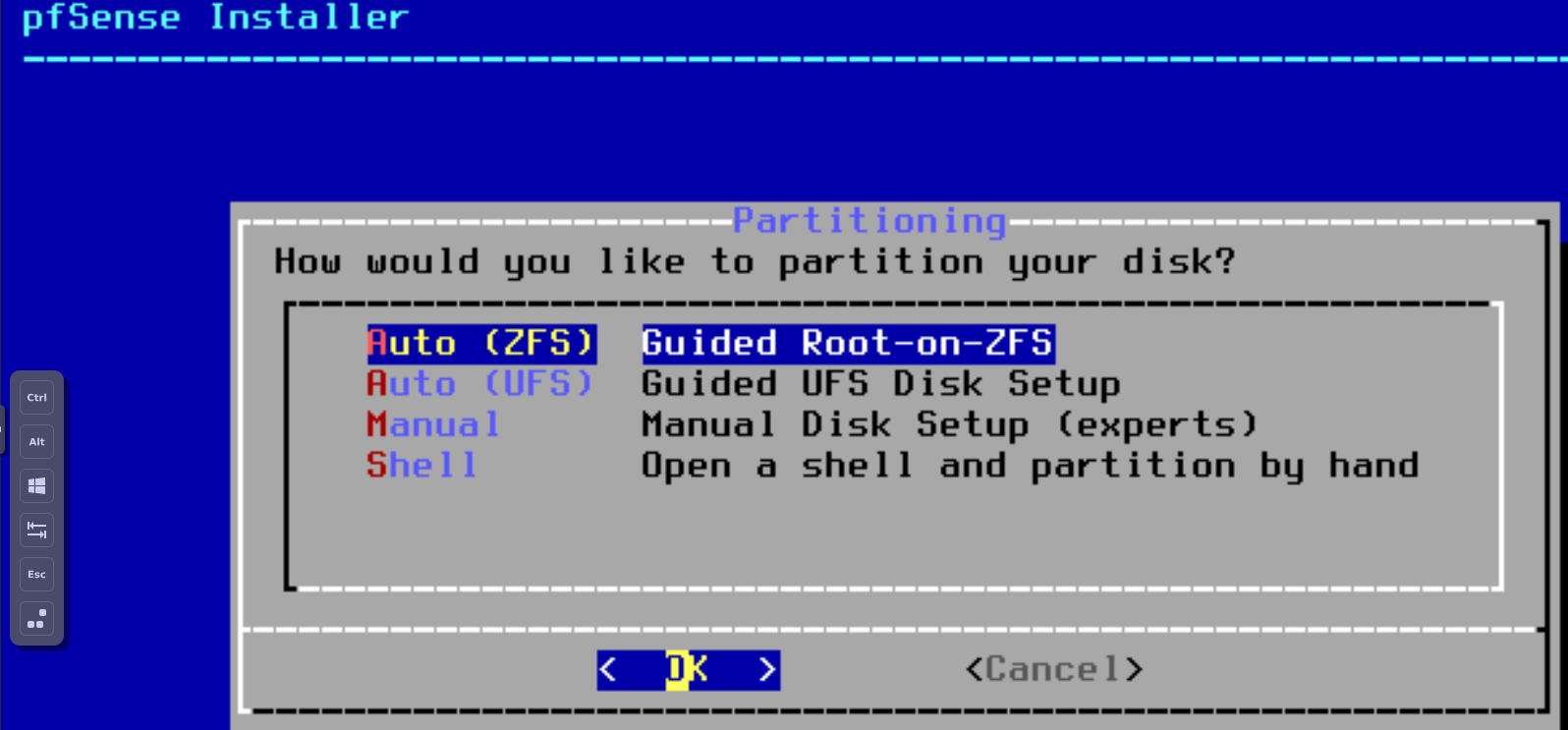
Cliquer sur “Accept”



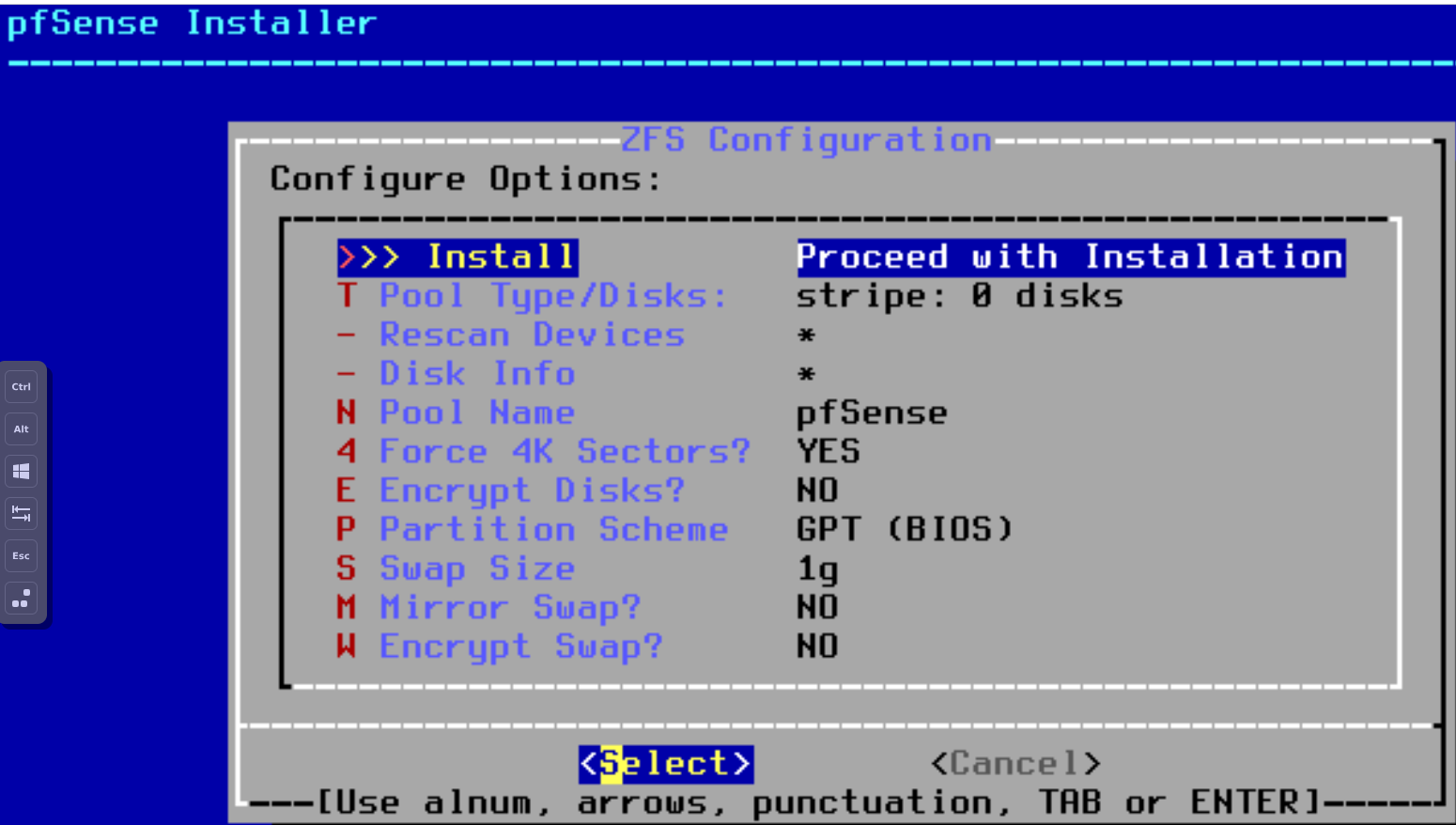
Sélectionne “Install” puis ok

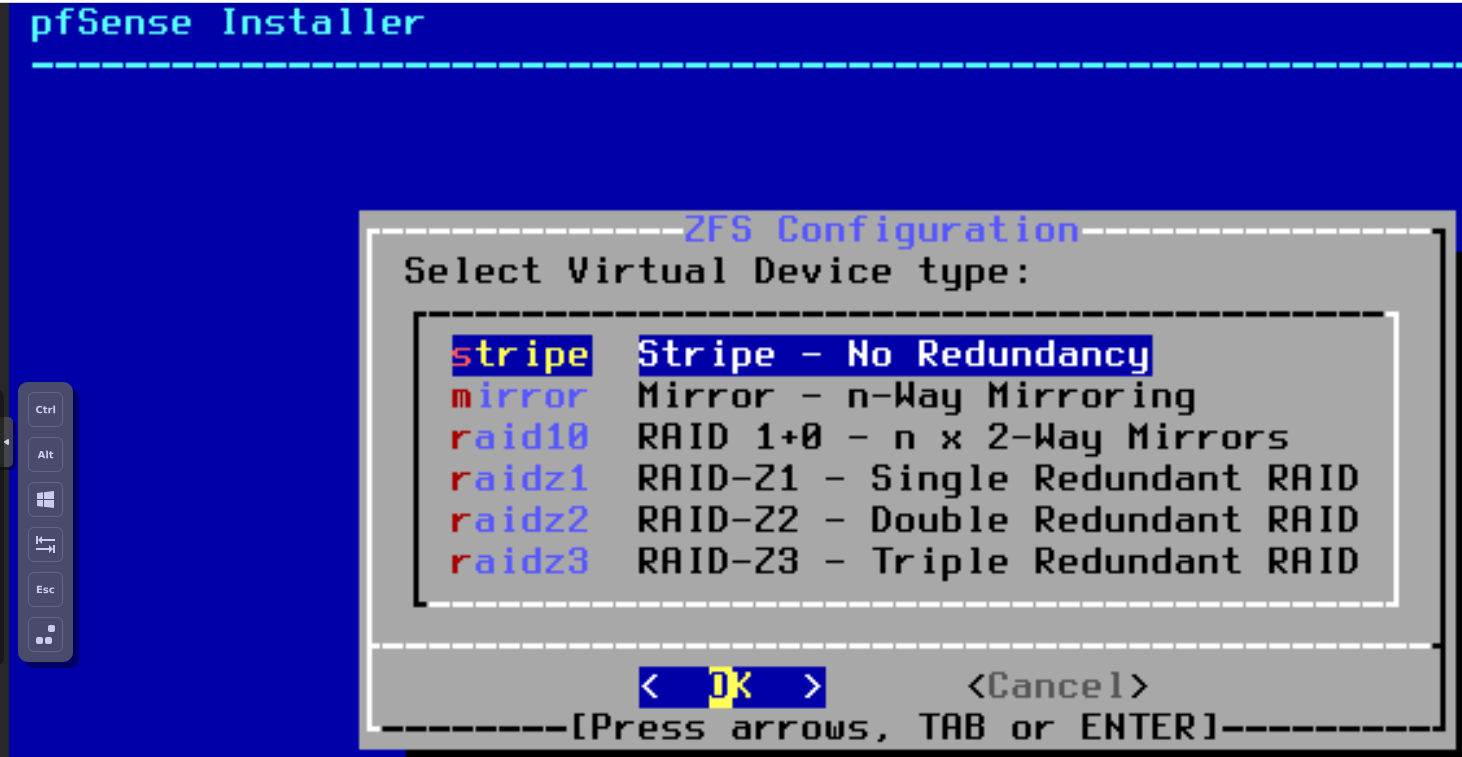


Sélectionne “Auto guided” puis ok



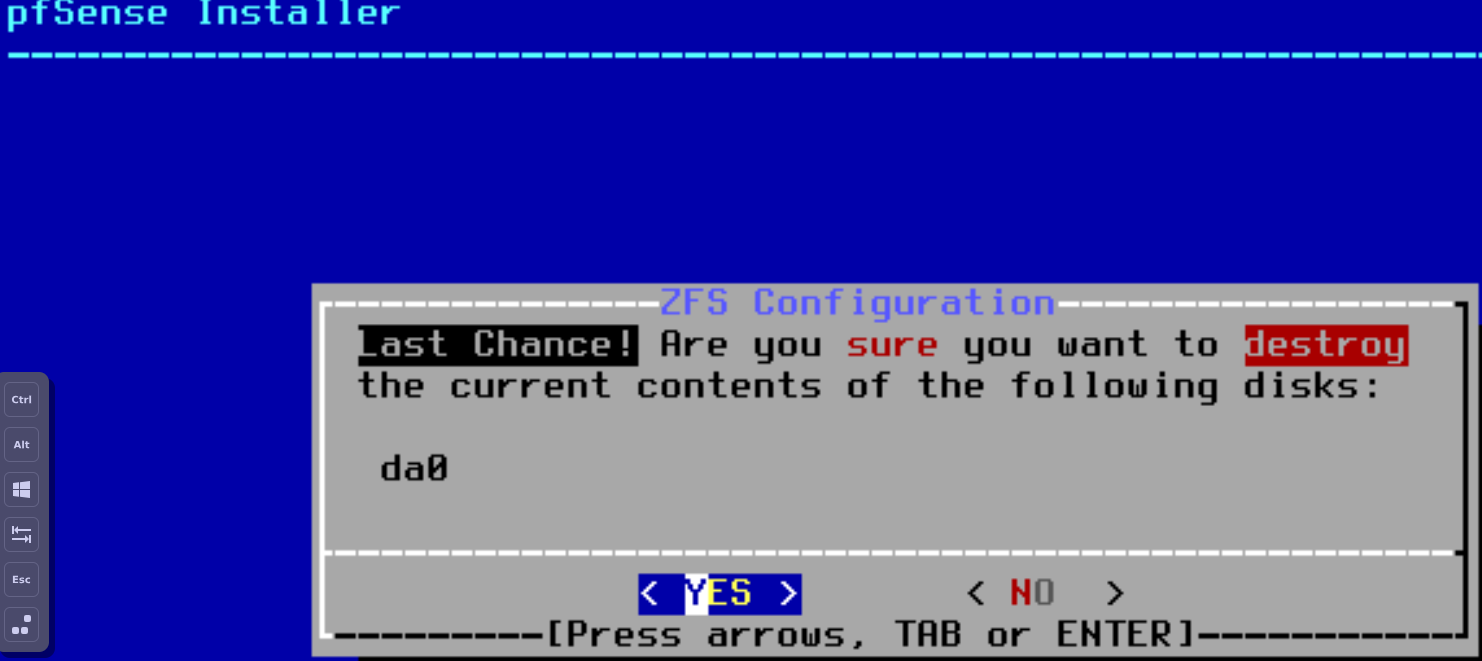
Sélectionner « Install » puis « Stripe »

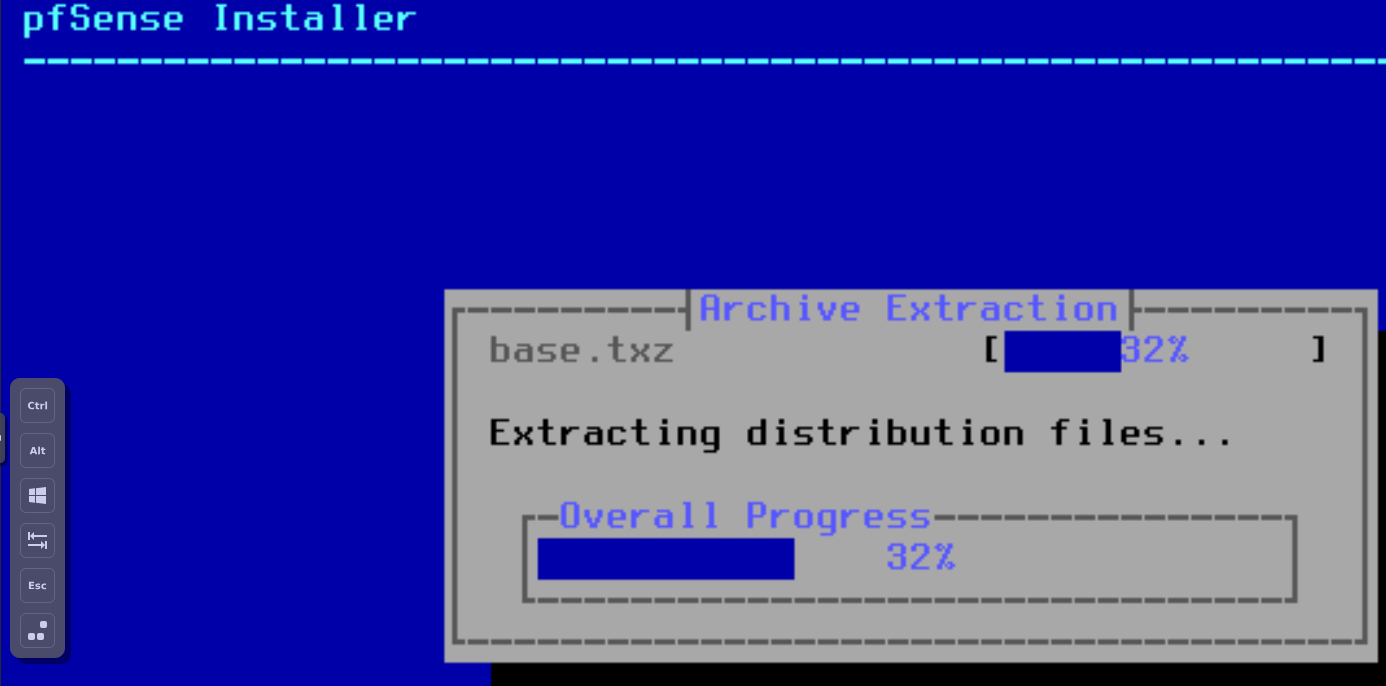


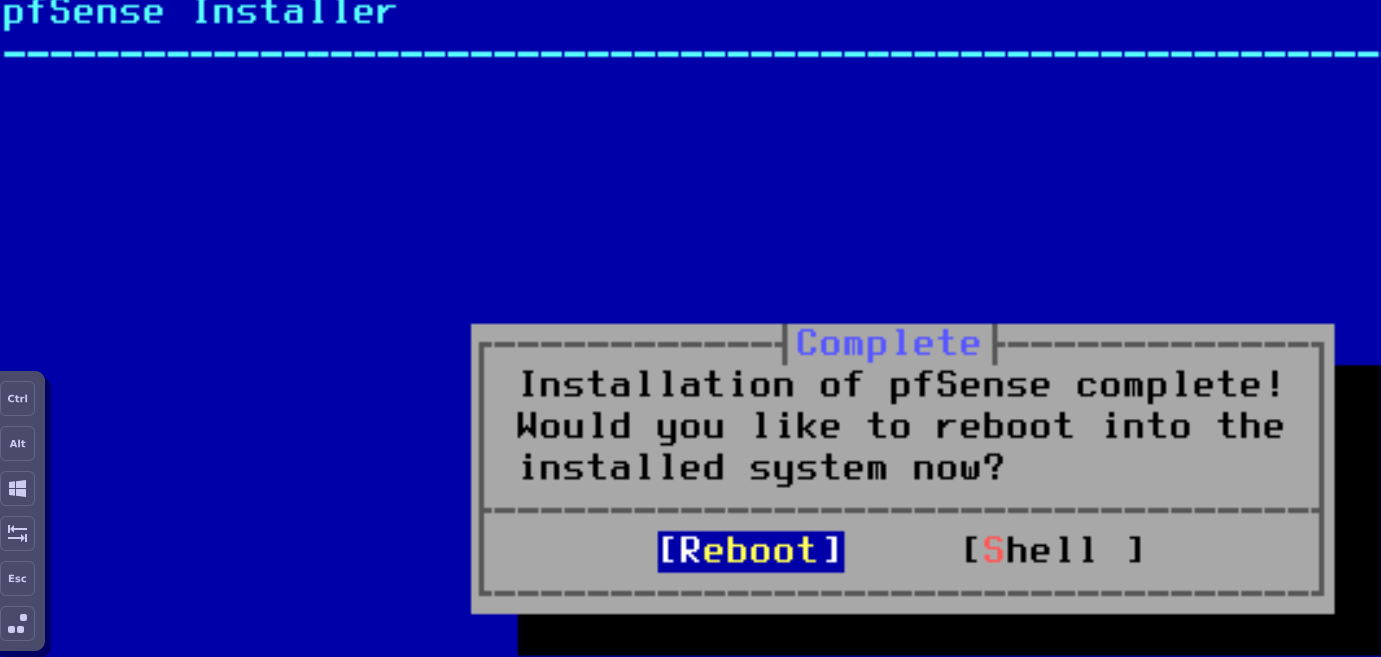


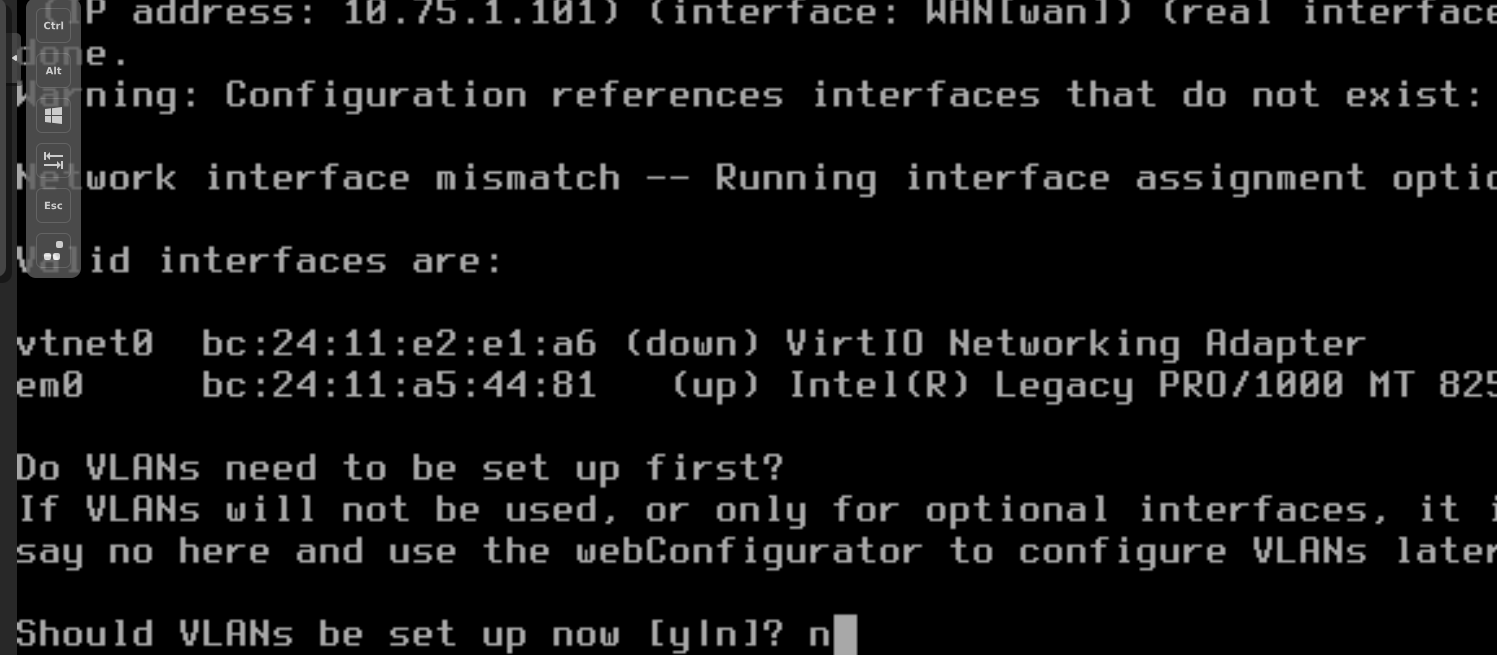
Sélectionner avec la touche « Espace » le disque et sélectionner « YES »



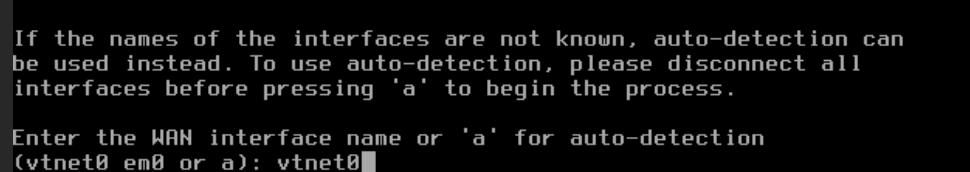
  
  
Patientez pendant l’installation

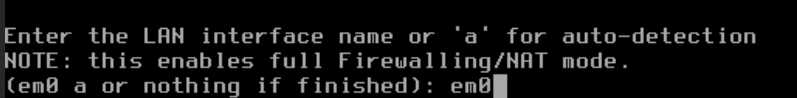
  
  
Sélectionner : Reboot

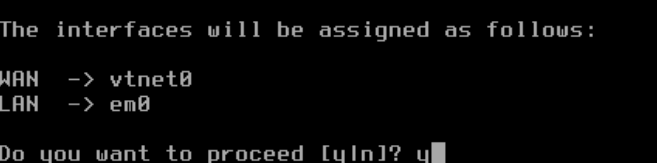
  
  
Saisissez “n” pour “no” pour la création de VLAN



Sélectionner la carte réseau internet WAN : vtnet0

  
Sélectionner la carte réseau local LAN : vtnet1

  
Appliquer les changements : “y” pour “yes”

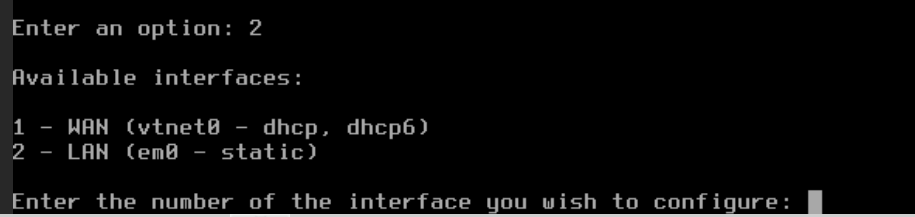
  
  
Retour au Menu



Configuration de l’adresse IP de la carte réseau local LAN hn1

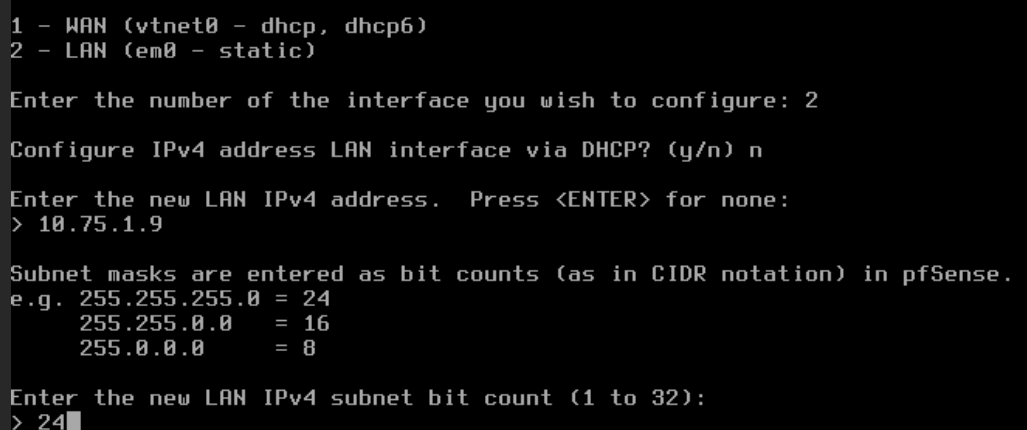
Sélectionner : 2 (Set interface IP address)

Sélectionner la carte réseau local LAN : 2

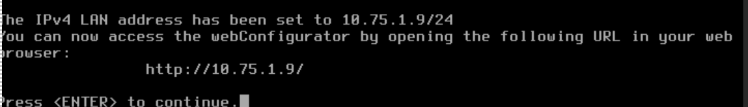


Saisissez l’adresse IP souhaitée : 10.75.1.9 (pour notre exemple)

Saisissez le masque sous réseau au format CIDR : 24

  
  
Activez le retour a http en tant que protocole de configuration Web. Entrez : « y” pour “yes”

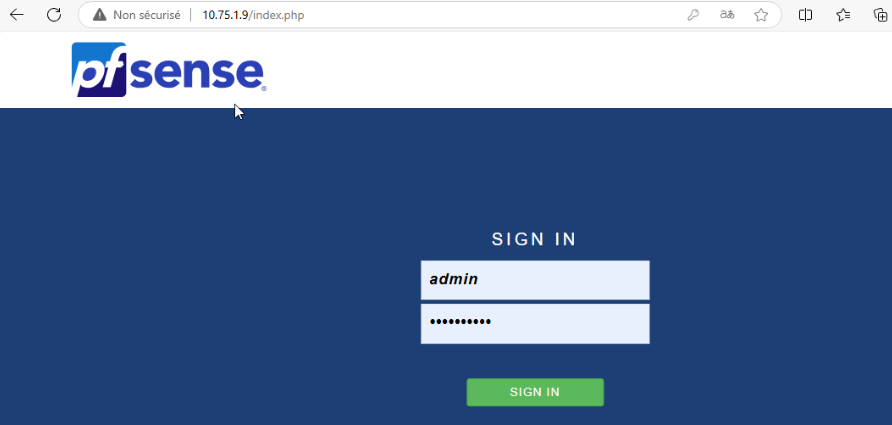


Configuration terminée. Cliquez : ENTREE

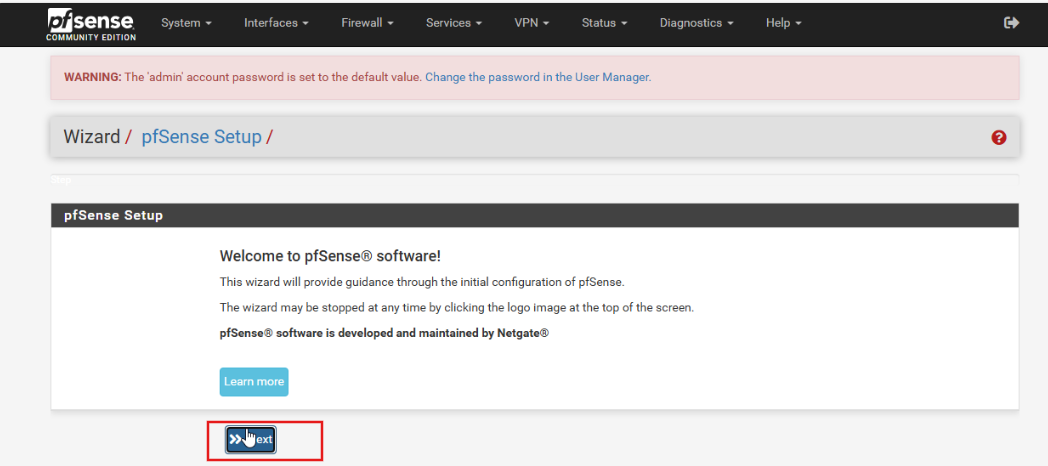
## Configuration de pfsense

### Configuration de base

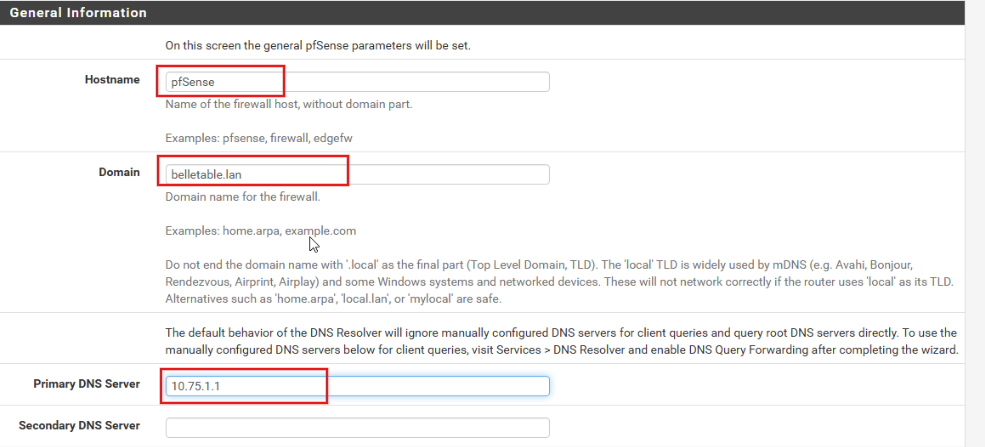
Tapez L’adresse IP dans le navigateur : 10.75.1.9 – Username : admin – Password : pfsense



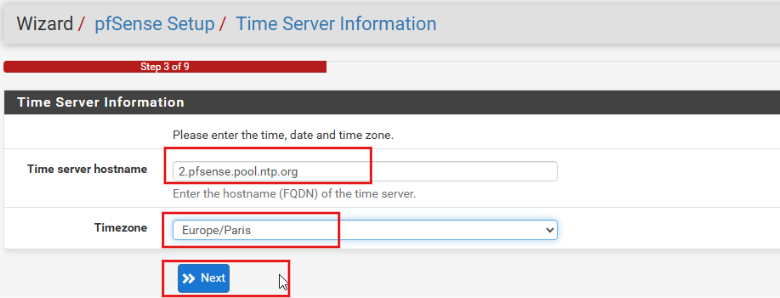
Cliquer sur Next

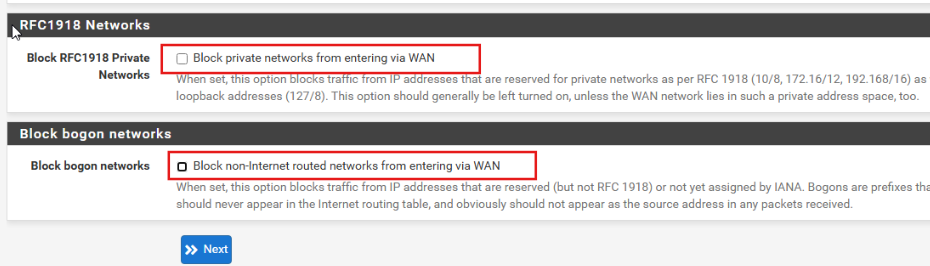


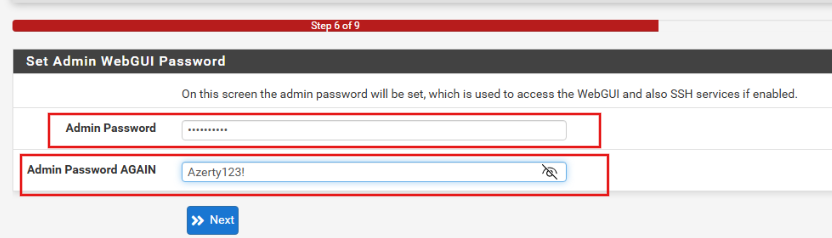
Renseigner : Hostname, Domain belletable.lan, Primary DNS 10.75.1.1

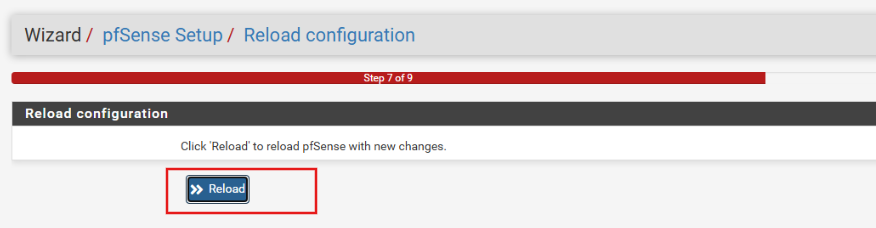


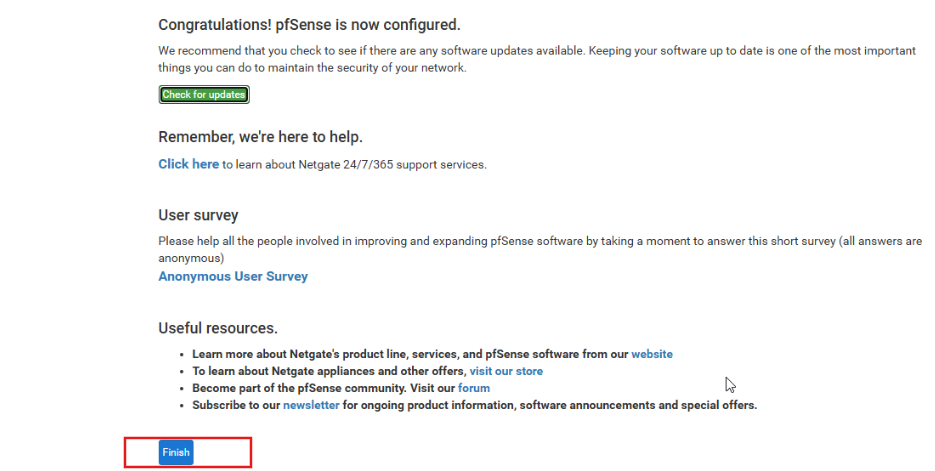
Sélectionner la Timezone Europe



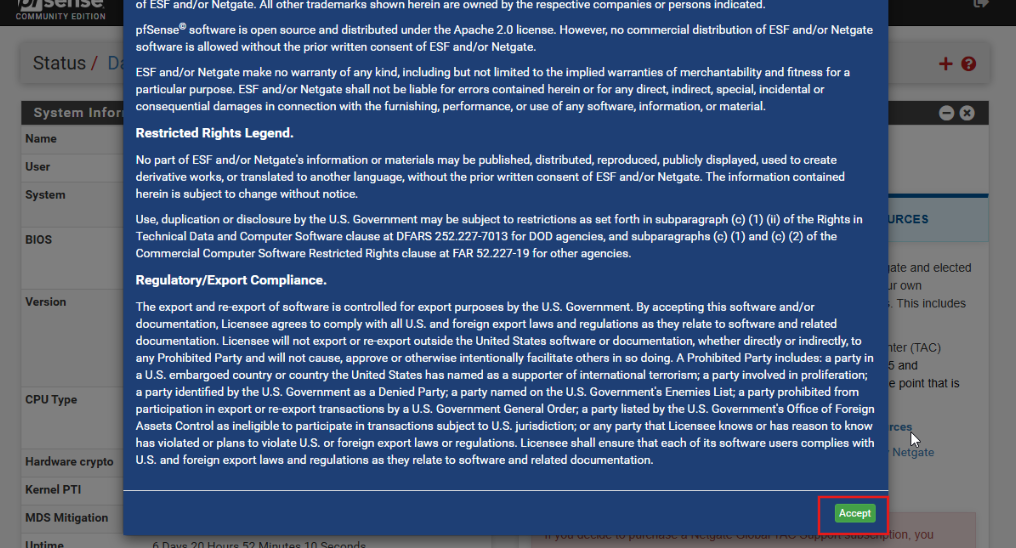
  
Modifier le mot de passe admin

  
Cliquer sur : Reload

  
Sélectionner : Finish

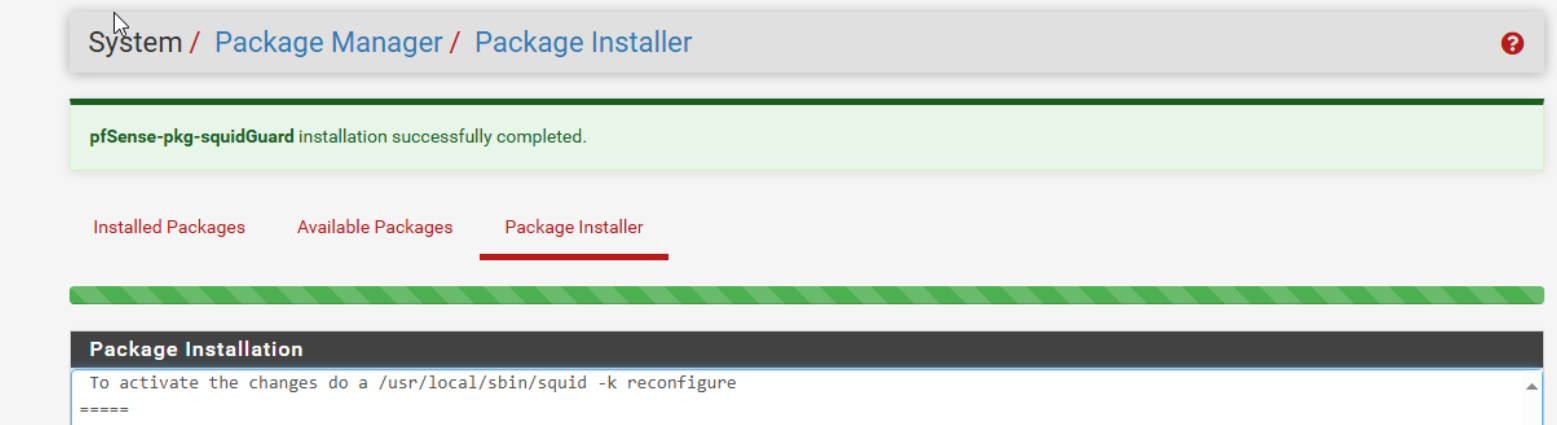


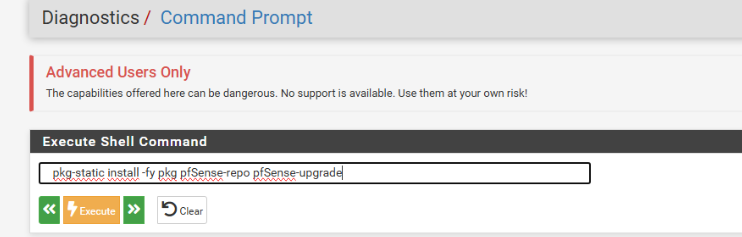
Accepter la licence



### Installation et configuration de package squid guard

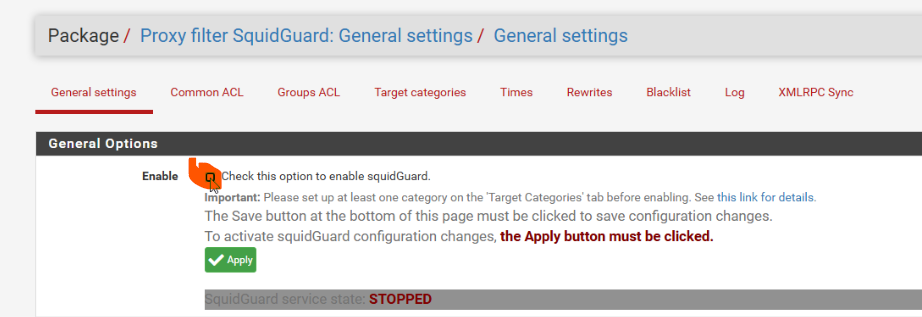
"System", puis "Package manager". Dans la section "Available Packages", recherchez "squid" et vous devriez voir le paquet Squid Guard apparaître. Il ne reste plus qu'à cliquer sur le bouton "Install".

  
Si les packages n’apparaît pas tape cette ligne de commande dans ”Diagnostic/ commande prompt

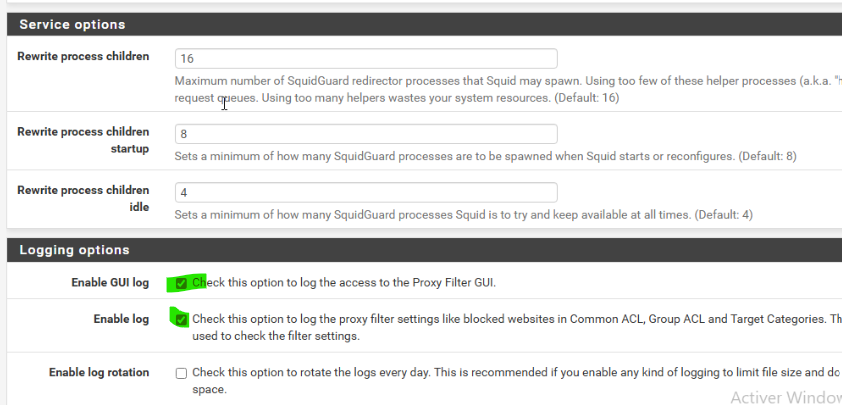


Une fois que c'est fait, nous pouvons passer à la configuration via le menu "Services" où se trouve une entrée "SquidGuard Proxy Filter".

ne cochez pas l'option "Check this option to enable SquidGuard" pour le moment, car il faut le préconfigurer avant de l'activer.

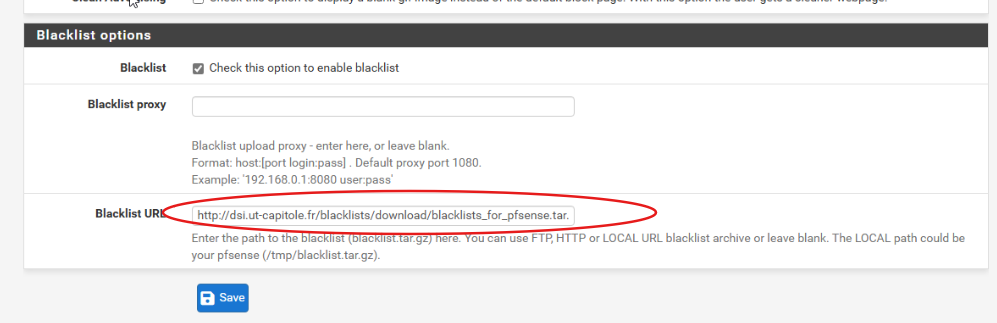


Cochez les deux options suivantes pour activer les logs : "Enable GUI Log" et "Enable log".

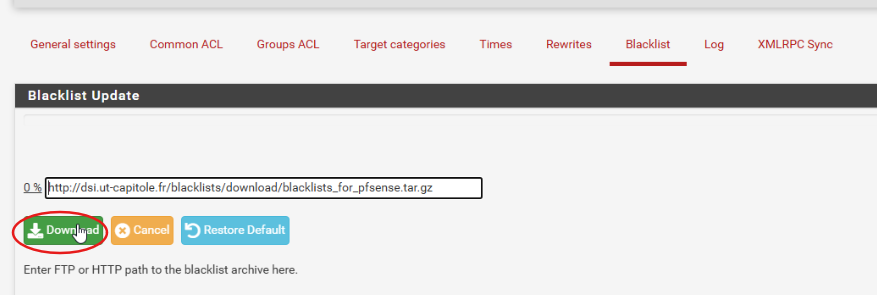


Ensuite, renseignez l'option "Blacklist URL" avec l'URL suivante :Enfin, cliquez sur le bouton "Save".

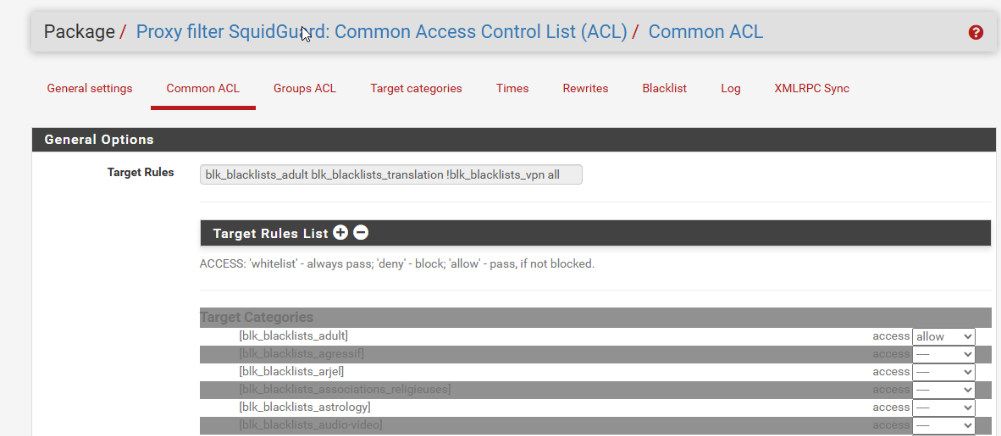
http://dsi.ut-capitole.fr/blacklists/download/blacklists\_for\_pfsense.tar.gz http://dsi.ut-capitole.fr/blacklists/download/blacklists\_for\_pfsense.tar.gz http://dsi.ut-capitole.fr/blacklists/download/blacklists\_for\_pfsense.tar.gz http://dsi.ut-capitole.fr/blacklists/download/blacklists\_for\_pfsense.tar.gz



Maintenant, basculez sur l'onglet "Blacklist" de SquidGuard. Cliquez sur le bouton "Download" pour télécharger la dernière version de la liste noire que nous avons renseignée dans les paramètres de SquidGuard.



Au sein du champ "Target Rules List", vous avez la liste de toutes les catégories récupérées à partir de la blacklist.

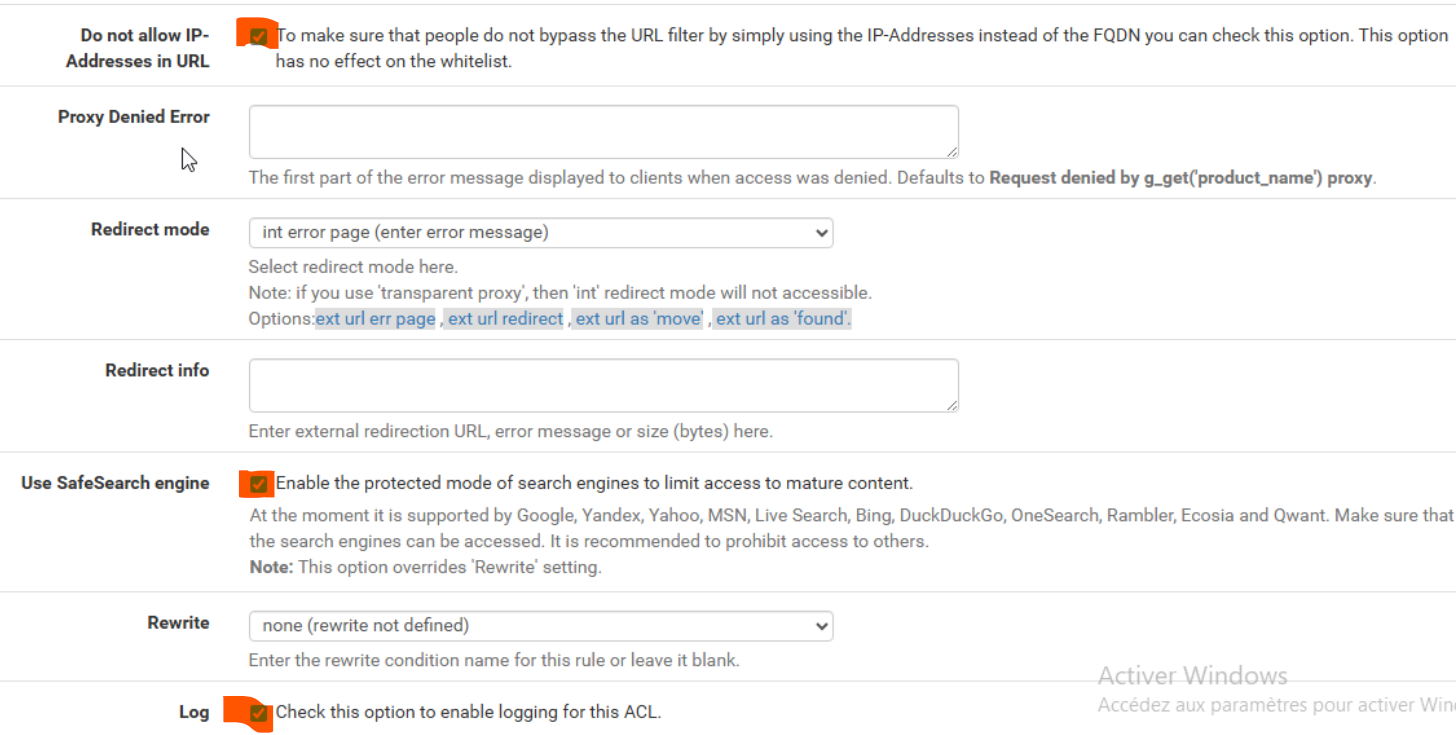


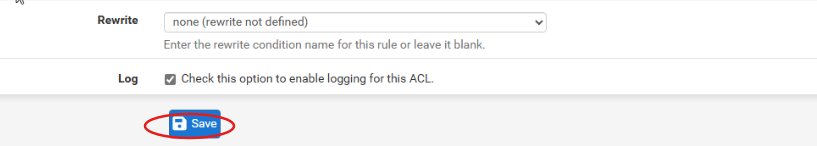
Pour blacklist il faut donc modifier la valeur du champ "access" pour préciser "deny"

Pour autoriser “ allow”



Pour ne pas utiliser l'adresse IP du serveur distant à la place du nom de domaine, cochez l'option "Do not allow IP-Addresses in URL"

  
Enfin, activez les logs pour cette règle en cochant l'option "Log" tout en bas, puis cliquez sur "Save".



La configuration étant prête, retournez dans "General Settings", cochez l'option "Check this option to enable SquidGuard" et cliquez sur "Apply".

