PPE N°3 PfSense - CrowdSec

DOCUMENTATION TECHNIQUE

Nolian Botelho
PROMEO

SOMMAIRE

I. Présentation du Projet

3.1 Introduction

Dans un monde où la cybercriminalité est en constante évolution, la sécurisation des réseaux informatiques est devenue une préoccupation majeure pour les entreprises.

Afin de protéger efficacement les données sensibles et d'assurer la continuité des opérations, il est essentiel de mettre en place des solutions de sécurité robustes et adaptées aux besoins spécifiques de chaque organisation. Dans ce contexte, la mise en œuvre d'un pare-feu performant tel que pfSense, associé à des outils de filtrage web comme Squid et à des mécanismes de détection d'intrusion tels que CrowdSec, représente une stratégie essentielle pour renforcer la sécurité du réseau.

2.1 Scénario

SecureNet Solutions spécialisée dans les services informatiques et la sécurité des réseaux. Forte de son expertise, l'entreprise s'est vu confier la mission de concevoir et de déployer une infrastructure réseau sécurisée pour un client stratégique, une grande entreprise internationale opérant dans le secteur financier.

Pour répondre aux besoins spécifiques de ce client, SecureNet Solutions a décidé de mettre en place une architecture réseau comprenant un pare-feu pfSense configuré avec plusieurs zones distinctes, notamment un LAN (Local Area Network), un WAN (Wide Area Network) et une DMZ (Zone Démilitarisée). Cette architecture permettra de segmenter le réseau et de limiter l'exposition aux menaces potentielles.

De plus, afin de renforcer la sécurité du réseau, SecureNet Solutions prévoit d'installer Squid, un proxy/cache web, pour filtrer le trafic web et limiter l'accès à certains sites jugés non sécurisés ou non conformes aux politiques de l'entreprise. Parallèlement, l'entreprise envisage d'intégrer CrowdSec, un système de détection d'intrusion collaboratif, pour détecter et bloquer automatiquement les comportements malveillants sur le réseau.

2.2 Cahier des Charges

Configuration du réseau :

● Installation d'un pare-feu pfSense pour assurer la sécurité du réseau.

● Configuration d'un réseau local (LAN) pour les utilisateurs internes de TechCorp.

● Configuration d'un réseau étendu (WAN) pour la connexion à Internet.

● Mise en place d'une zone démilitarisée (DMZ) pour héberger les serveurs accessibles depuis l'extérieur tout en isolant le réseau interne.

Sécurité du réseau :

● Mise en œuvre de règles de pare-feu strictes pour contrôler le trafic entrant et sortant.

● Configuration de listes de contrôle d'accès (ACL) pour restreindre l'accès aux ressources sensibles.

● Utilisation de VLANs pour segmenter le réseau et limiter la propagation des menaces potentielles.

Filtrage web :

● Installation et configuration de Squid comme proxy pour le filtrage du contenu web.

● Paramétrage de règles de filtrage pour bloquer l'accès à des sites web malveillants ou non autorisés.

● Mise en place de rapports de journalisation pour suivre l'activité web des utilisateurs et détecter les comportements suspects.

Protection contre les menaces :

● Intégration de CrowdSec pour détecter et bloquer automatiquement les tentatives d'attaques sur le réseau.

● Configuration de règles de détection pour identifier les comportements anormaux et les activités malveillantes.

● Mise en place de mécanismes de réponse automatisée pour neutraliser les attaques et protéger l'intégrité du réseau.

Test d'intrusion :

● Configuration d'une machine Kali Linux pour simuler une attaque depuis l'extérieur du réseau.

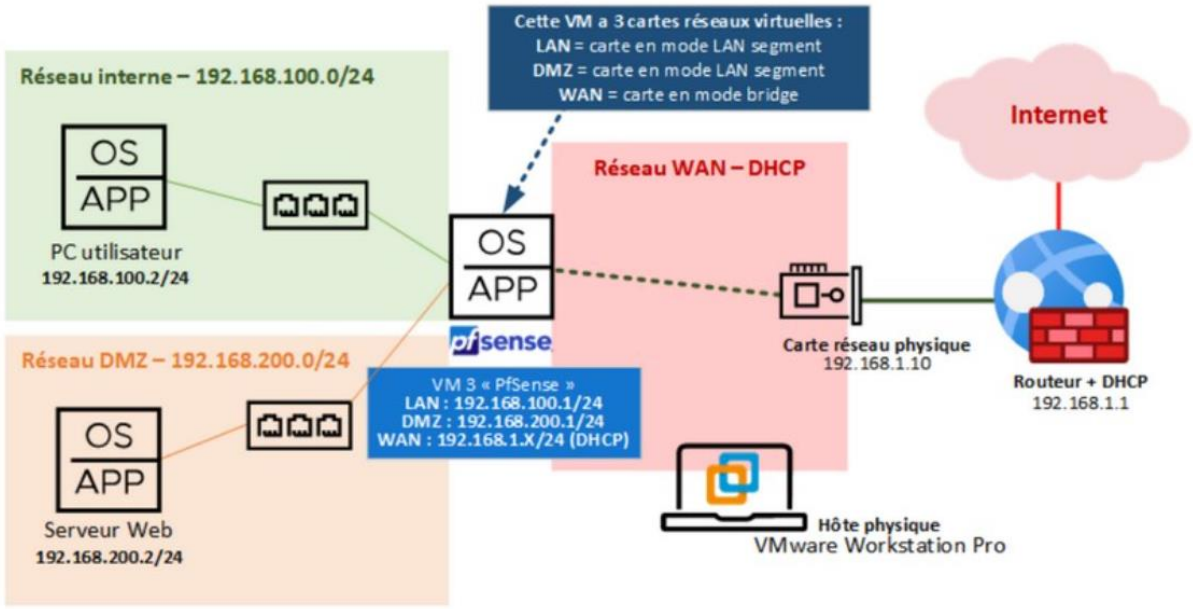
● Réalisation de tests d'intrusion réguliers pour évaluer l'efficacité des mesures de sécurité mises en place.

● Analyse des résultats des tests d'intrusion pour identifier les failles potentielles et renforcer la sécurité du réseau.

2.3 Besoins Logiciels

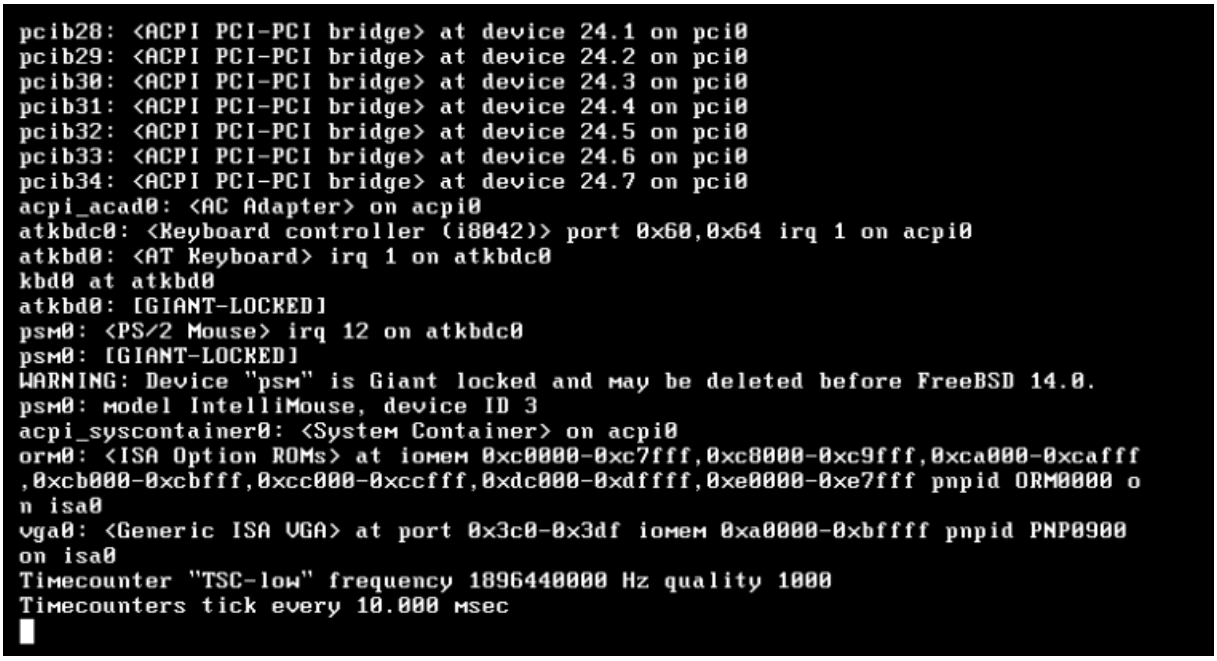
- Machine Kali Linux
- Serveur Active Directory
- Serveur Contrôleur de domaine
- Serveur WEB
- Machine PfSense
- 1 client Windows 10
- 1 client Windows 10

2.4 Schéma Reseaux

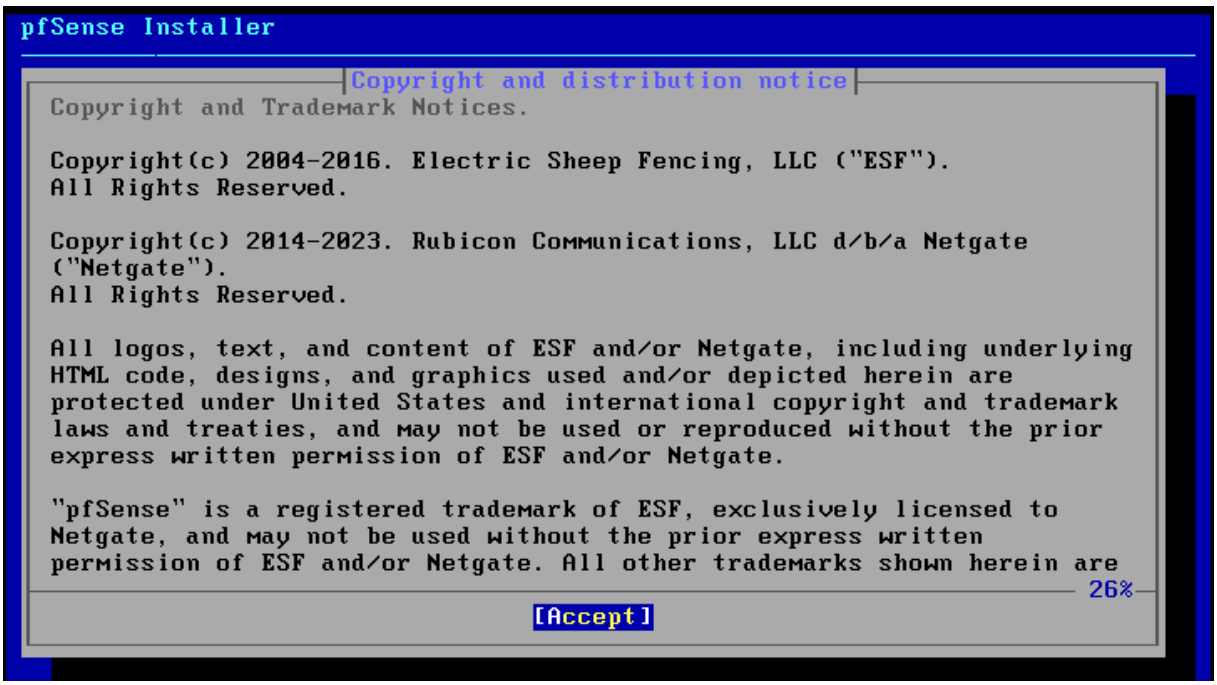


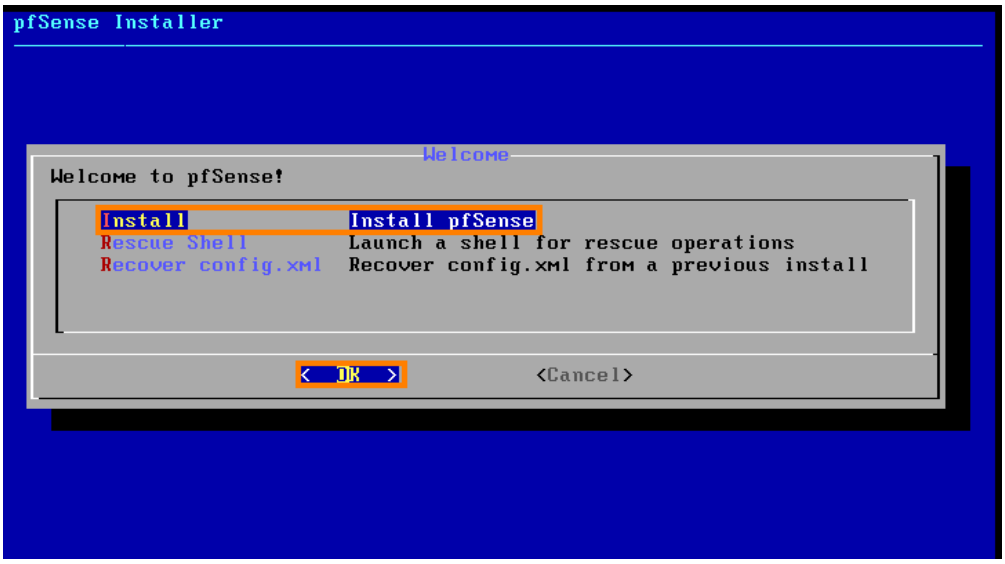
III. Déroulement de l'Installation de PFSENSE

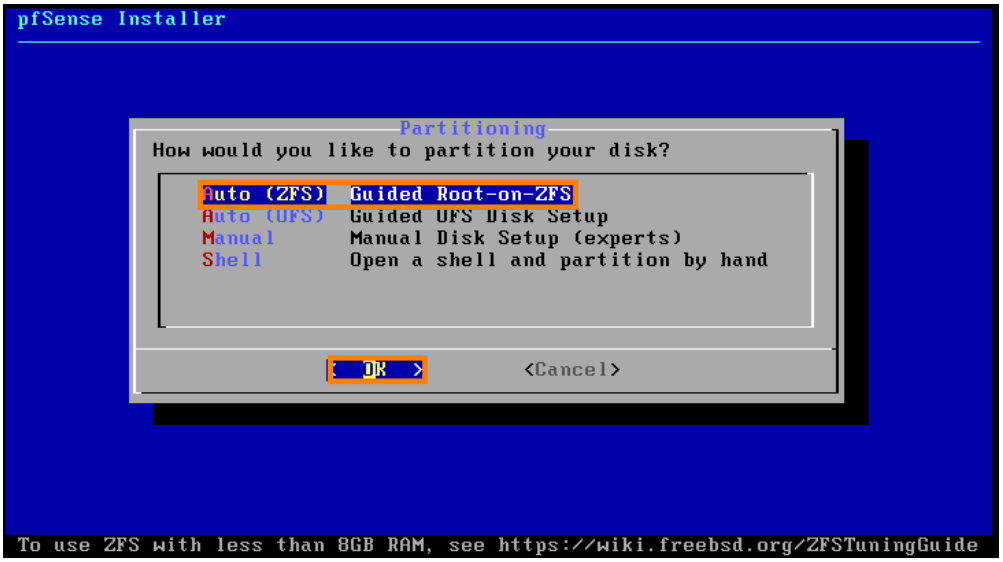
Pour commencer nous allons commencer par l'installation de PfSense. Lancer la VM précédemment télécharger sur le site de PfSense.



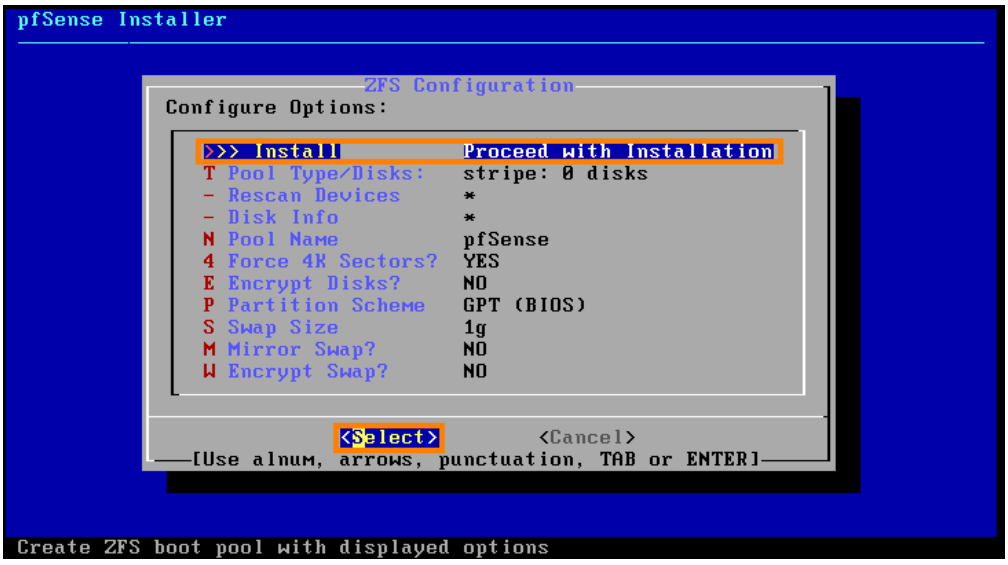
Une fois fait appuyé sur entrée :

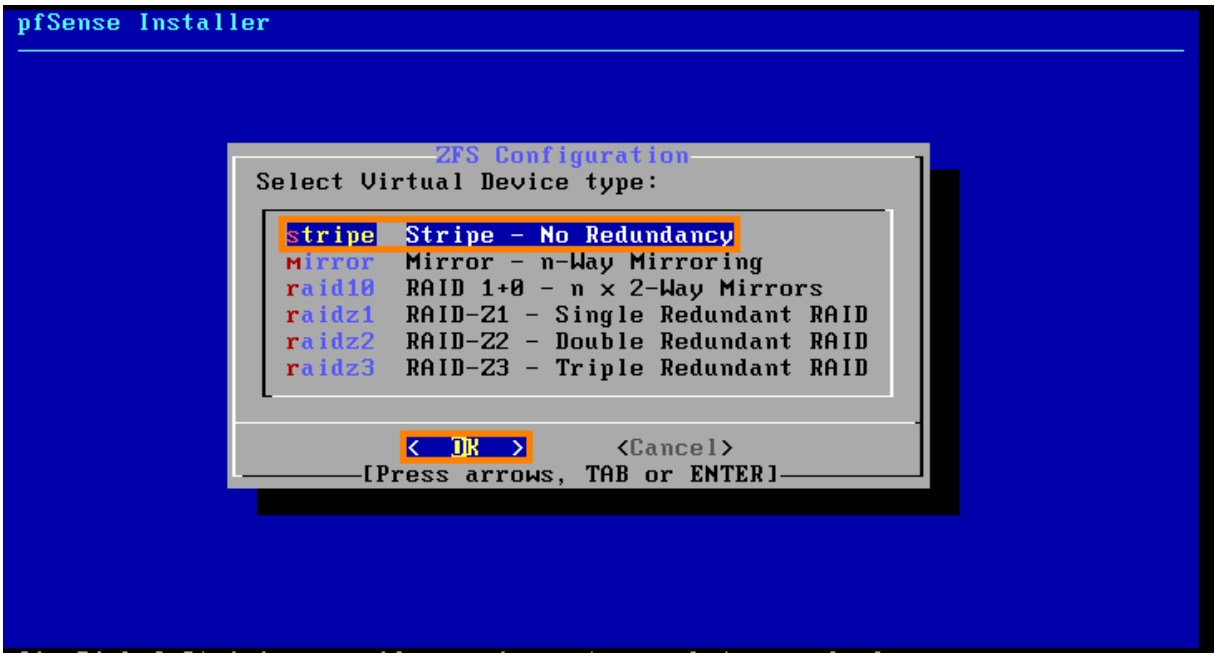




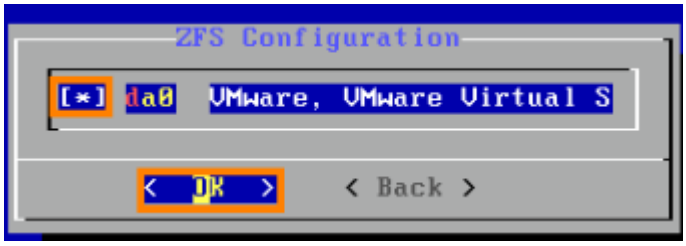


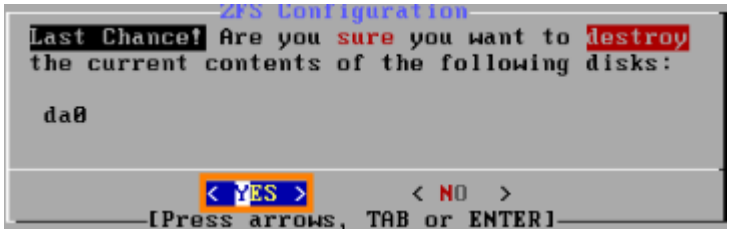
Veuillez donc suivre les encadrement.





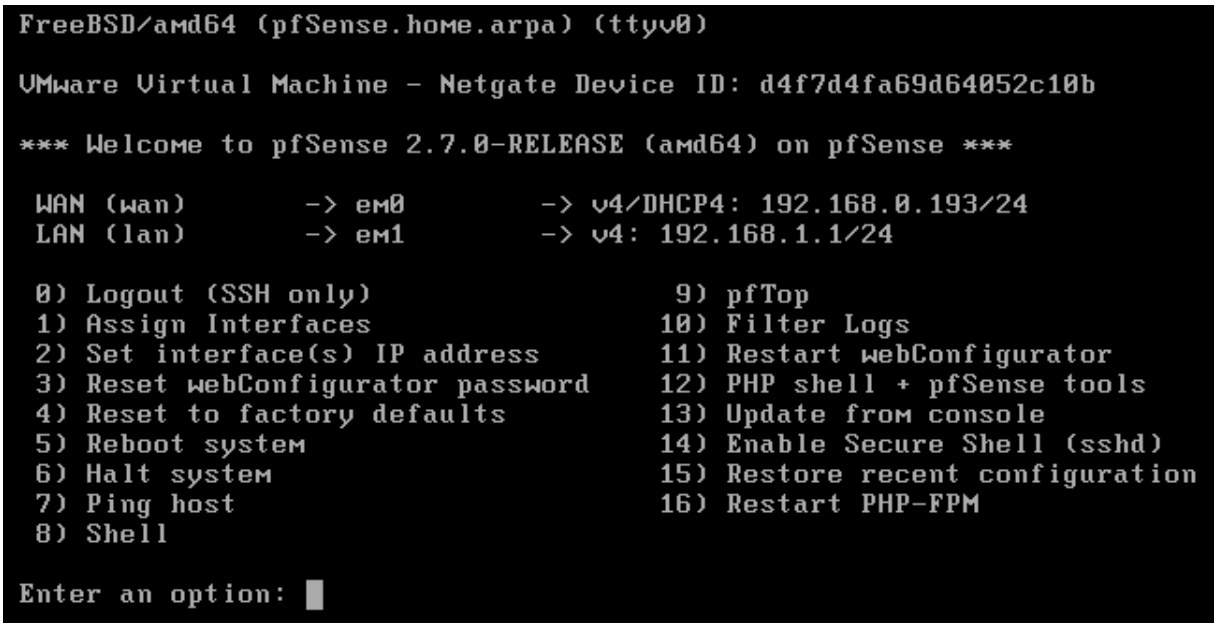
Ici, il faut séléctionner le disque virtuel, on appuye donc sur Espace puis Entrée.



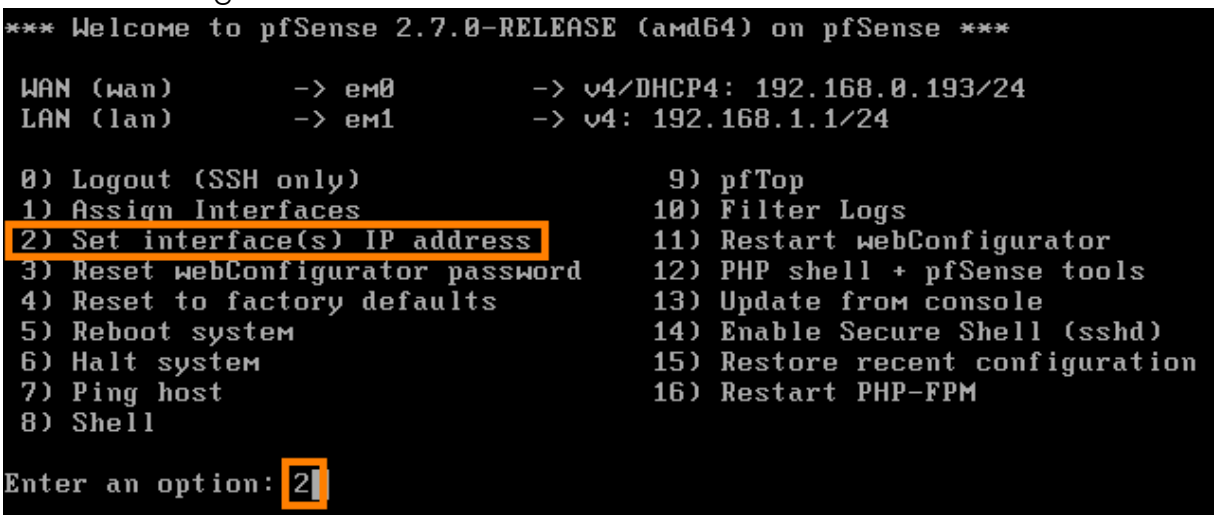


Une fois l'installation terminer relancer le système et l'installation est terminer.

Une fois PfSense lancer on se retrouvre donc sur cette page.

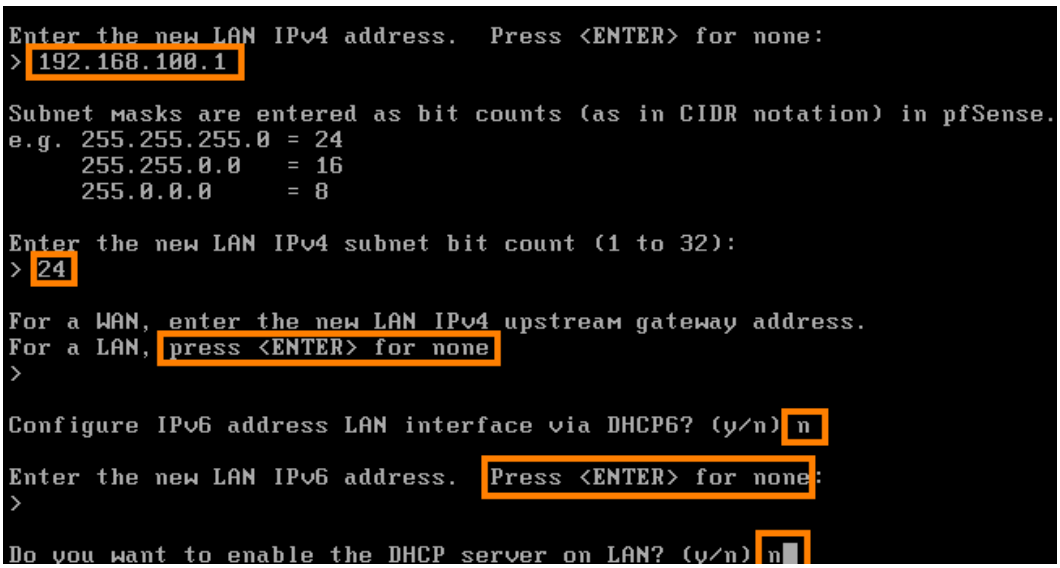


Nous allons configurer l'IP WAN de notre PfSense, pour ce faire nous suivons les encadrés orange.



Détails de notre configuration :

Adresse IP LAN : 192.168.100.1
Masque de sous-réseau : 24 = 255.255.255.0
Pas de passerelle
Pas de configuration IPv6
Pas de server DHCP

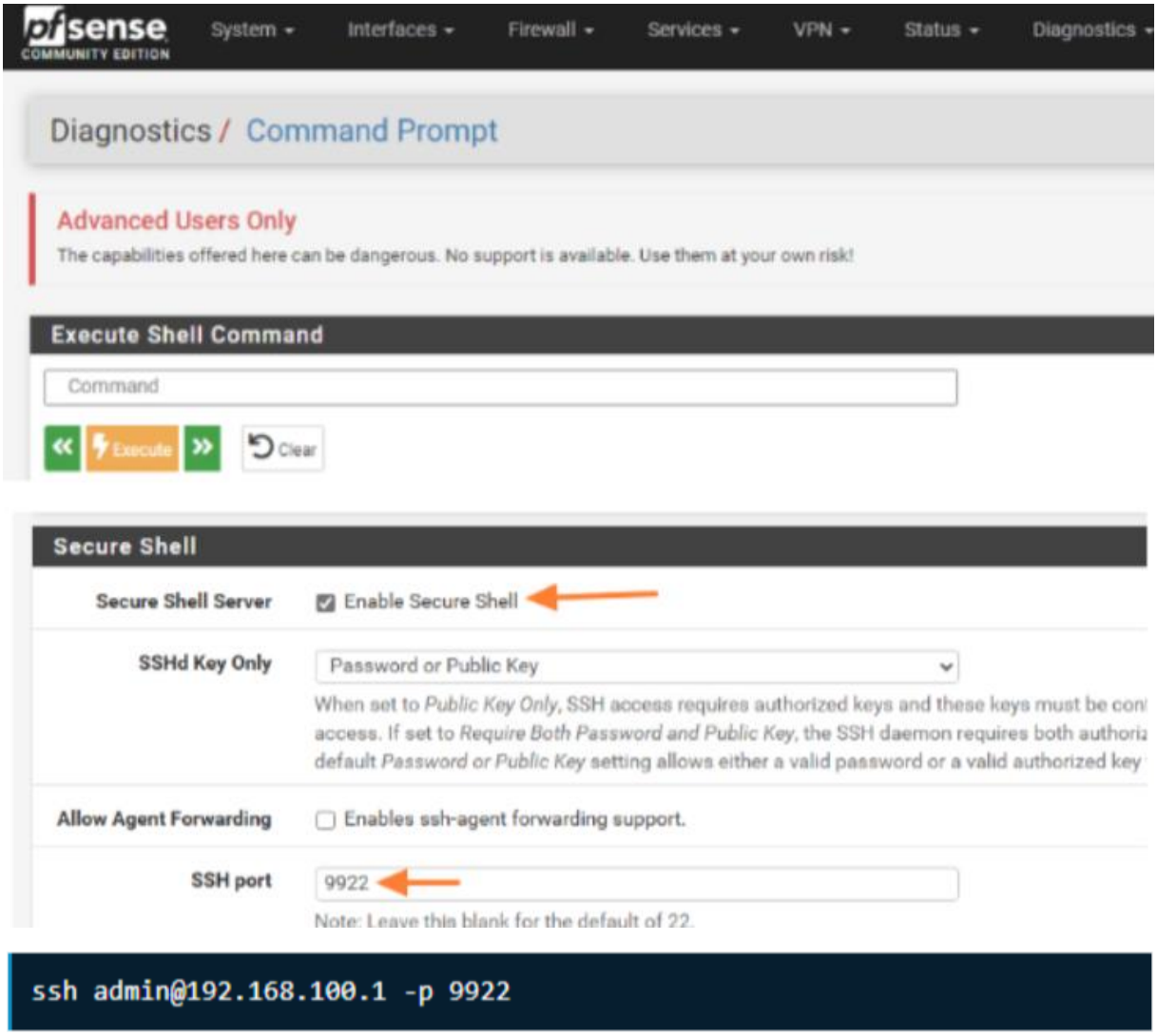


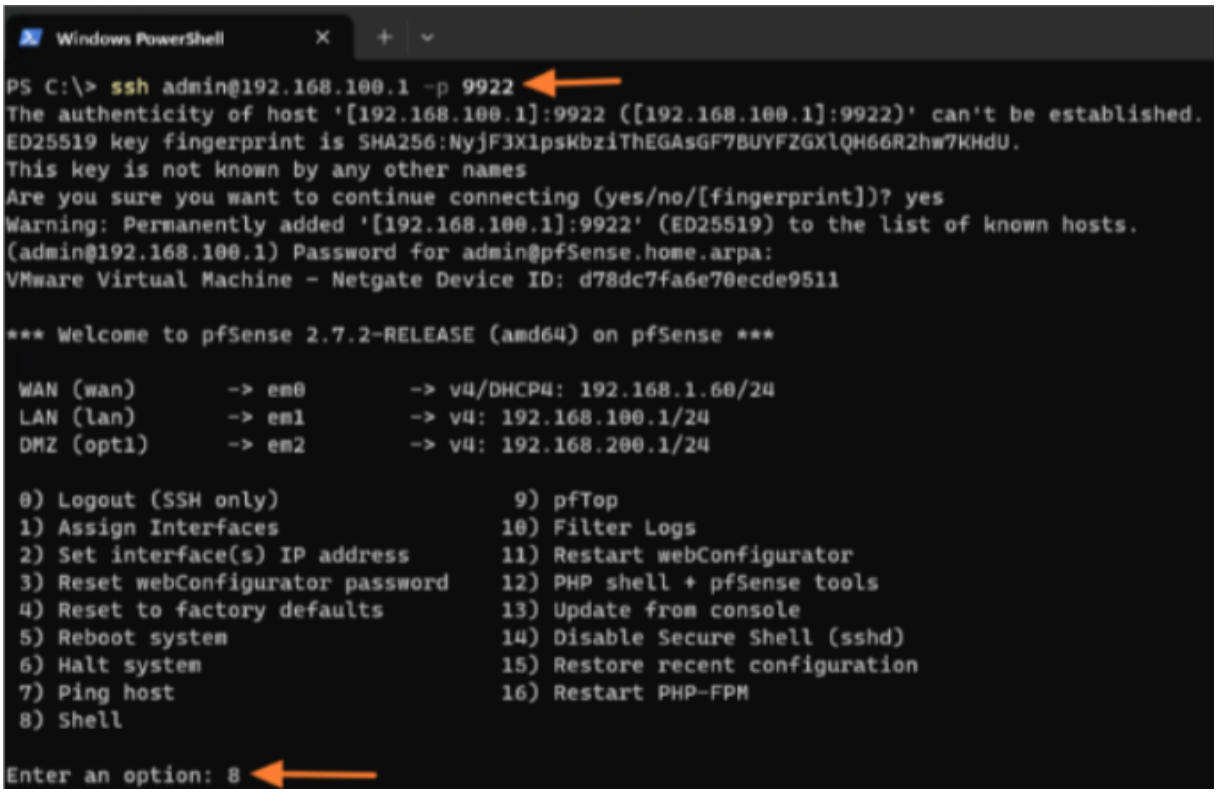
Il faut désormais se conecter a l'interface web de PfSense grace a l'ip https://192.168.100.1

Les identifiants sont :

Id : admin
Mdp : pfsense

IV. Installation de Crowdsec



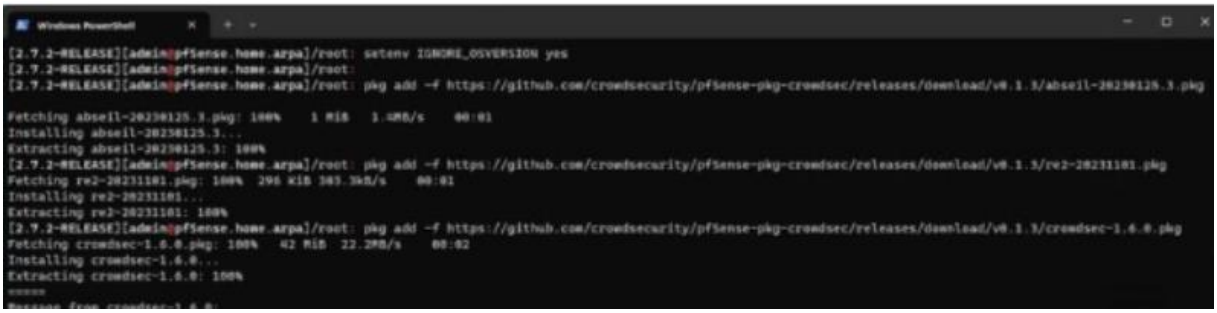


Ensuite nous rentrons cette commande :

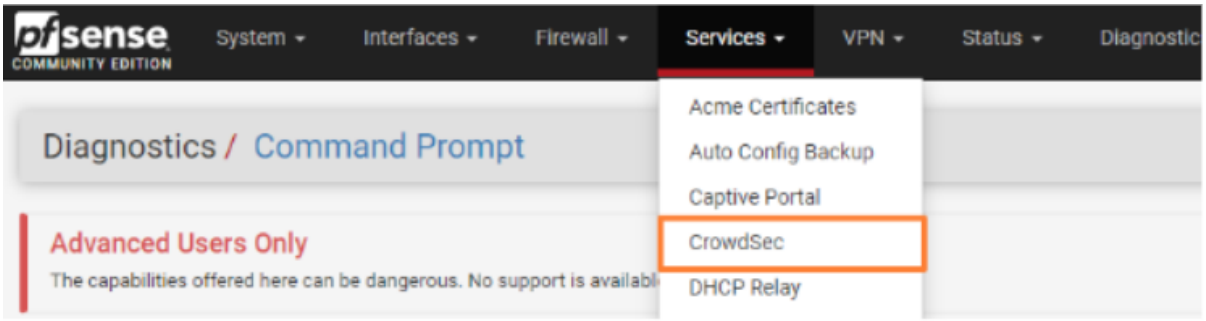
```
setenv IGNORE_OSVERSION yes
```

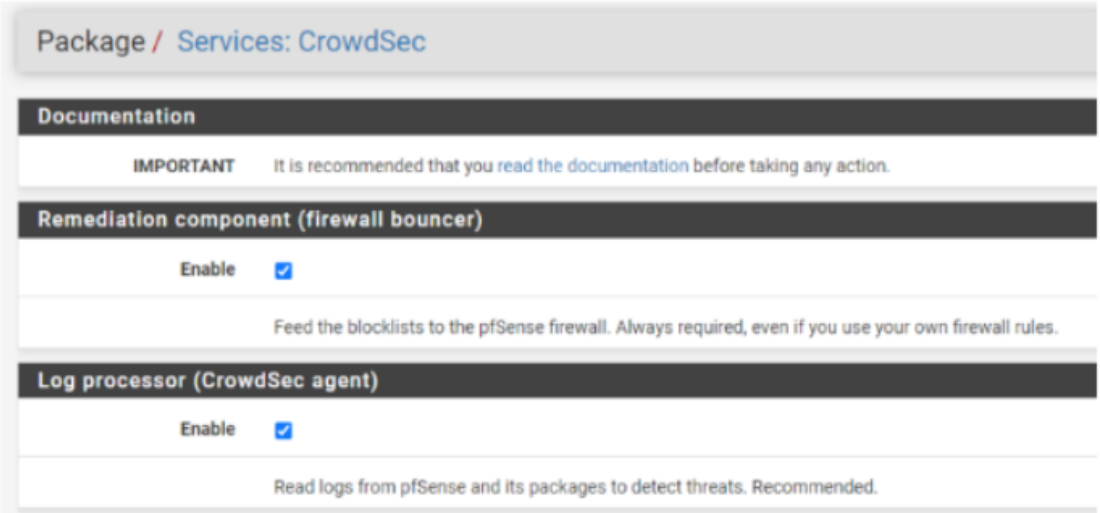
Puis :

```
pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/abseil-20230125.3.pkg
pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/re2-20231101.pkg
pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-1.6.0.pkg
pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-firewall-bouncer-0.0.28_3.pkg
pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/pfSense-pkg-crowdsec-0.1.3.pkg
```

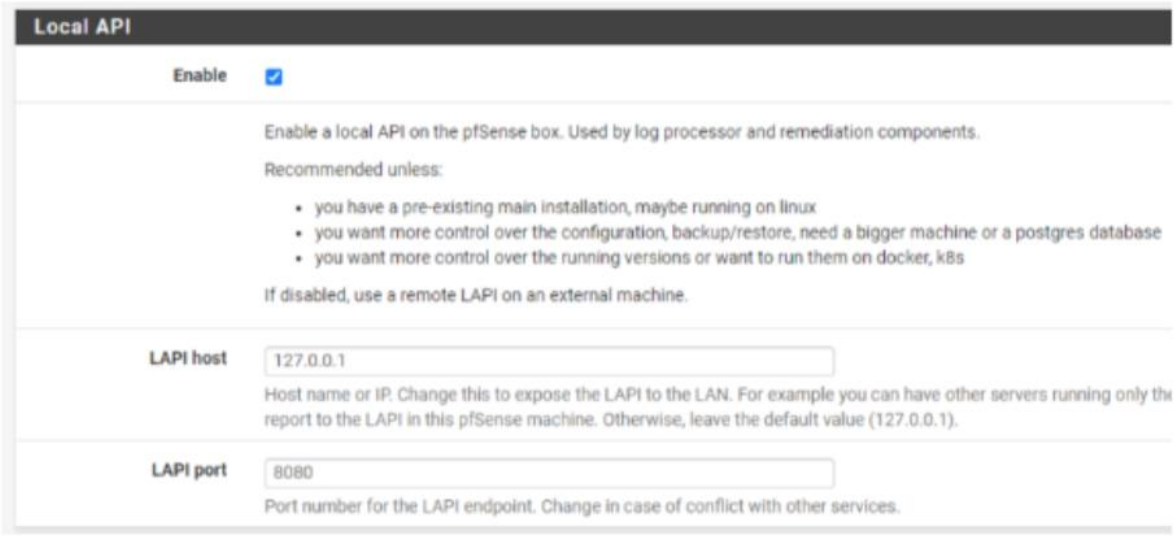


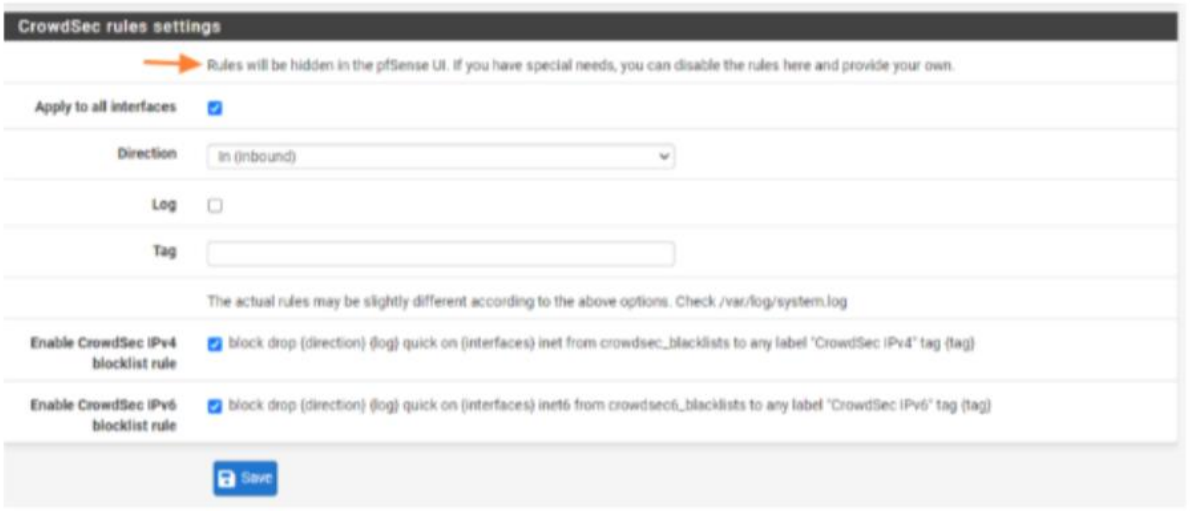
Ensuite nous retournons sur notre interface PfSense et dans « Services » -> CrowdSec

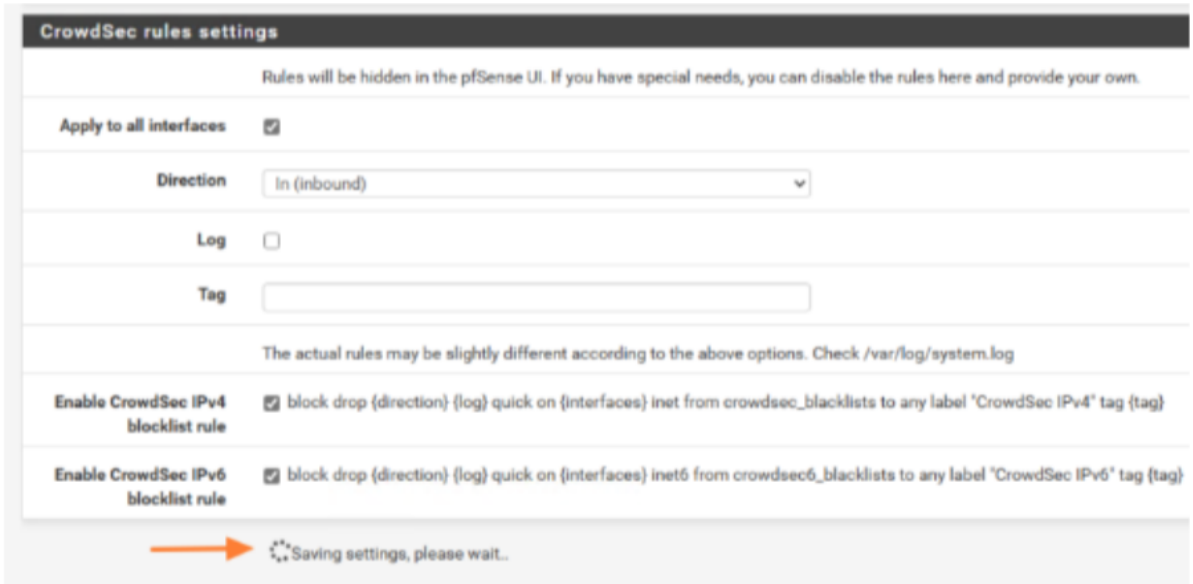


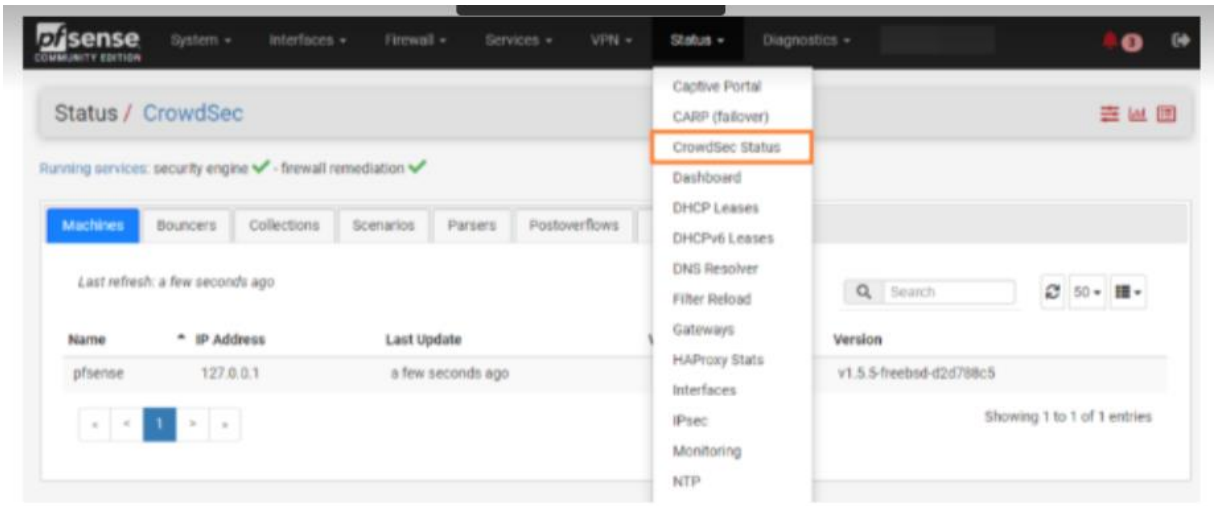


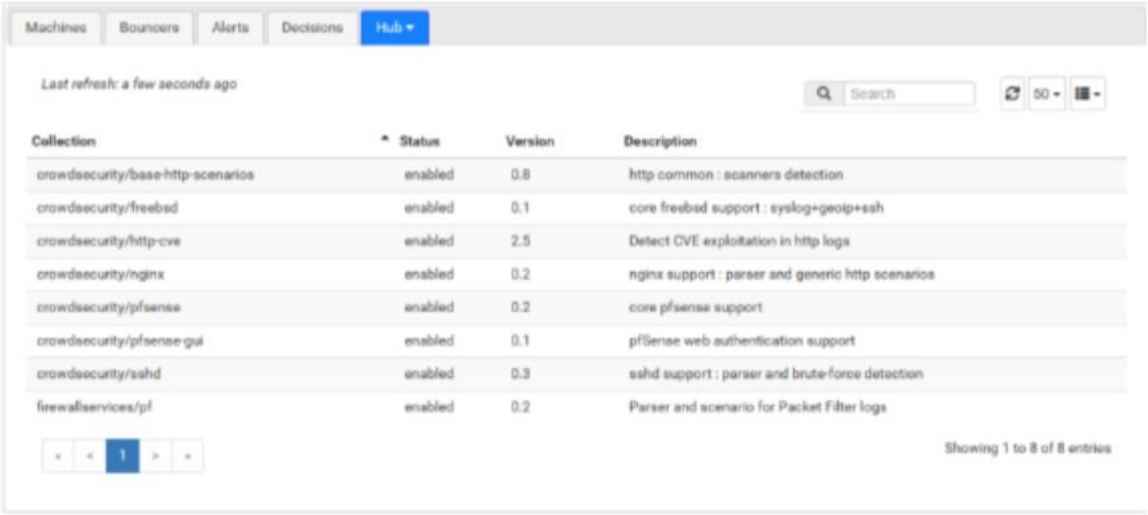
Veuillez rentrez donc cette configuration :





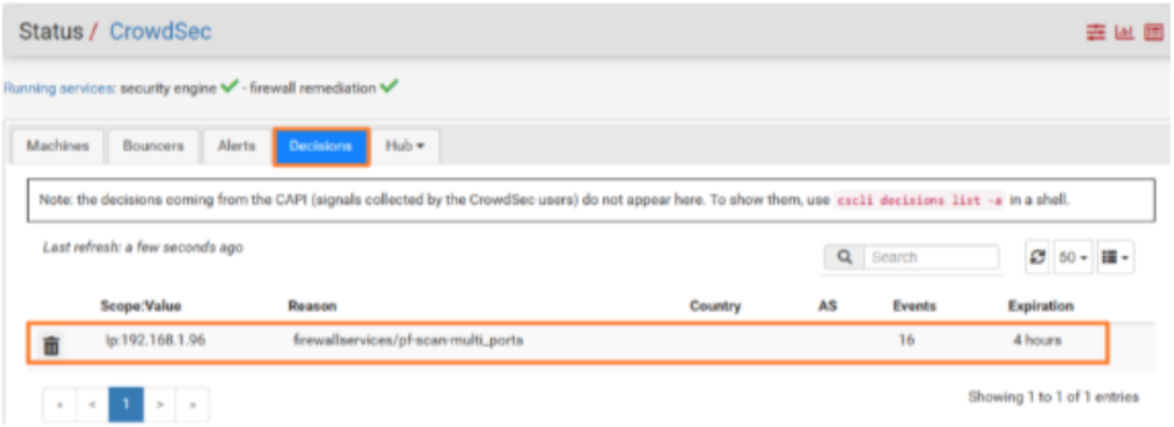






Une fois ceci fait, nous pouvons lancer un nmap comme ceci :

```
nmap -sV 192.168.1.60
```



Par la suite nous vérifions si l'ip a bien était bannie en consultant la liste des décision :

```
cscli decisions list
```

On peut constater que l'ip a bien été banni.

```
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions list
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
15001	crowdsec	Ip:192.168.1.96	firewallservices/pf-scan-multi_ports	ban			16	3h52m22.15208364s	2

```
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root:
```