



PPE N°3 PfSense - CrowdSec

DOCUMENTATION TECHNIQUE



Nolian Botelho
PROMEO

UIMM

PROMEO

LA FABRIQUE
DE L'AVENIR

SOMMAIRE

- I. Présentation du projet
- 1.1 Introduction

- II. Contexte
- 2.1. Scénario
- 2.2 Cahier des charges
- 2.3 Besoin logiciels
- 2.4 Schéma réseaux

- III. Déroulement de l'installation et des configurations

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.

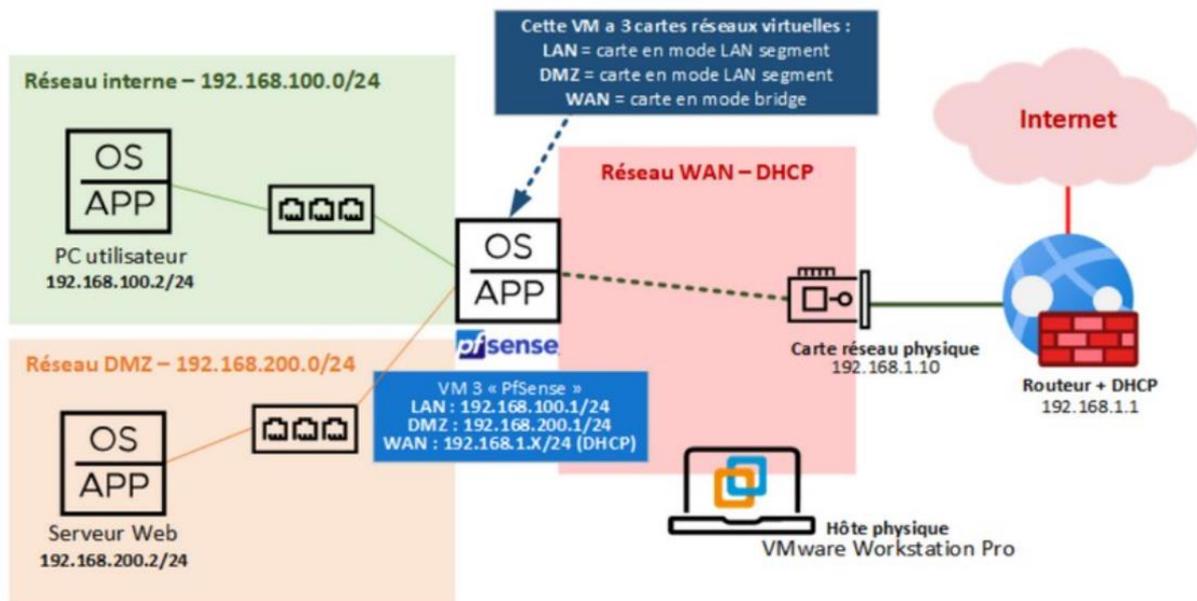
Test d'intrusion :

- 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

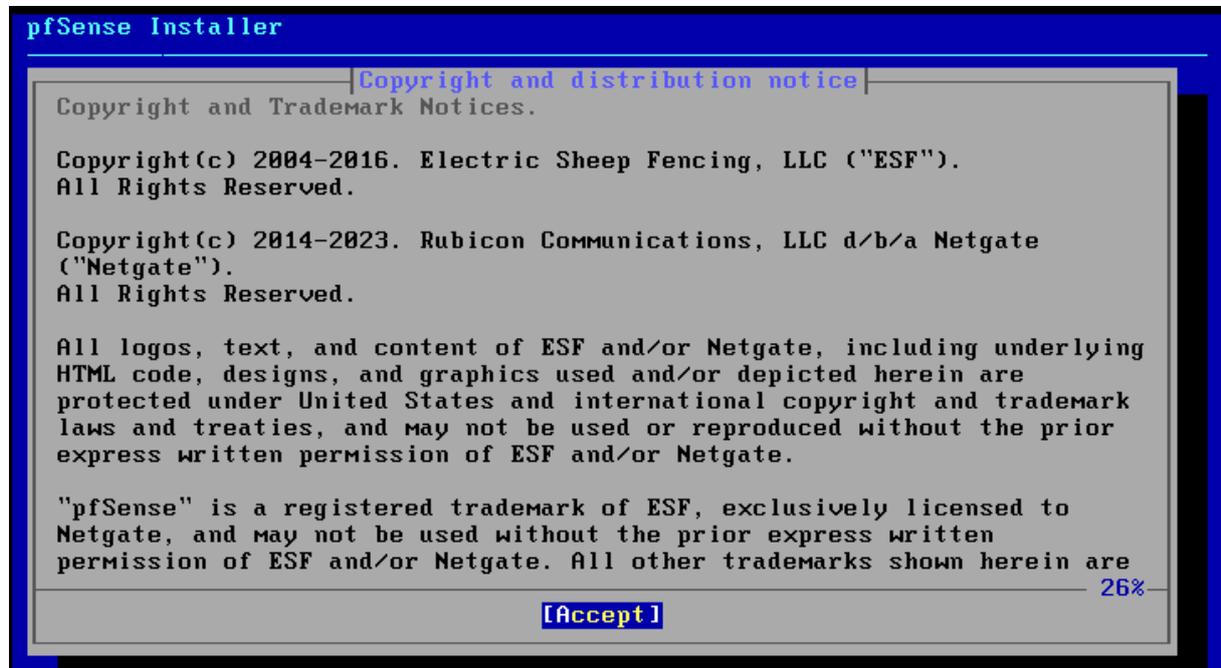


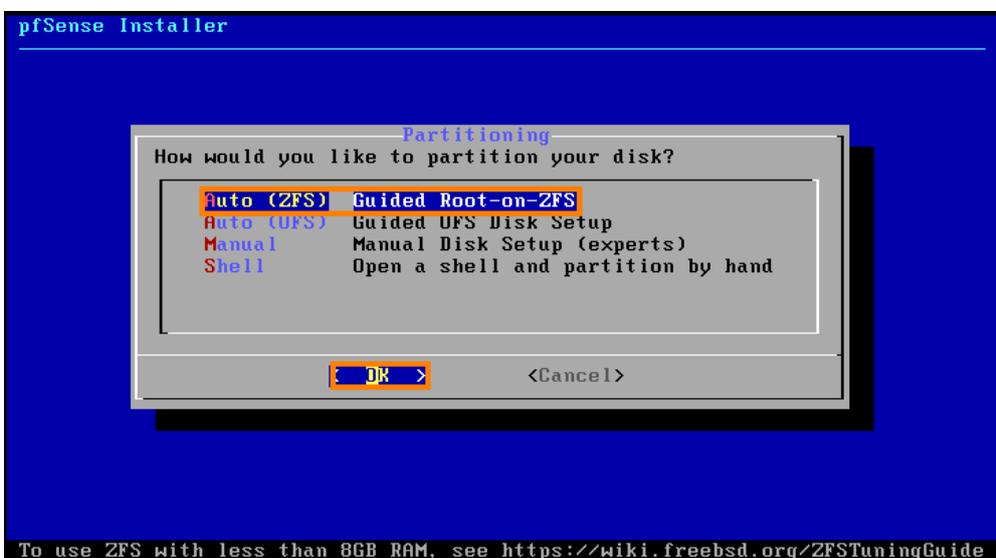
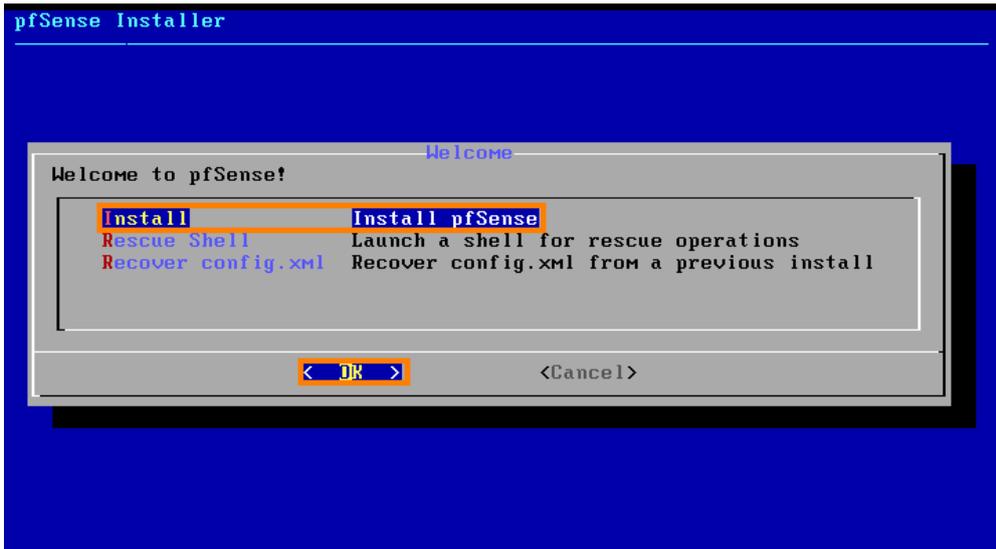
III. Déroulement de l'Installation de PFSense

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

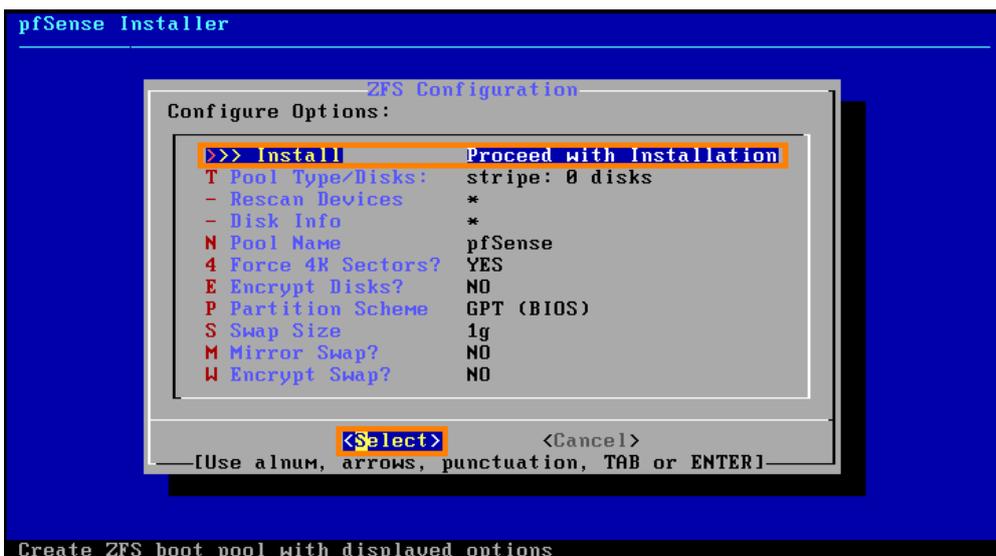
```
pci0: <ACPI PCI-PCI bridge> at device 24.1 on pci0
pci0: <ACPI PCI-PCI bridge> at device 24.2 on pci0
pci0: <ACPI PCI-PCI bridge> at device 24.3 on pci0
pci0: <ACPI PCI-PCI bridge> at device 24.4 on pci0
pci0: <ACPI PCI-PCI bridge> at device 24.5 on pci0
pci0: <ACPI PCI-PCI bridge> at device 24.6 on pci0
pci0: <ACPI PCI-PCI bridge> at device 24.7 on pci0
acpi0: <AC Adapter> on acpi0
atkbdc0: <Keyboard controller (i8042)> port 0x60,0x64 irq 1 on acpi0
atkbdc0: <AT Keyboard> irq 1 on atkbdc0
kbd0 at atkbdc0
atkbdc0: [GIANT-LOCKED]
psm0: <PS/2 Mouse> irq 12 on atkbdc0
psm0: [GIANT-LOCKED]
WARNING: Device "psm" is Giant locked and may be deleted before FreeBSD 14.0.
psm0: model IntelliMouse, device ID 3
acpi_syscontainer0: <System Container> on acpi0
orm0: <ISA Option ROMs> at iomem 0xc0000-0xc7fff,0xc8000-0xc9fff,0xca000-0xcafff
,0xcb000-0xcbfff,0xcc000-0xccfff,0xcd000-0xdffff,0xe0000-0xe7fff npnid ORM0000 o
n isa0
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff npnid PNP0900
on isa0
Timecounter "TSC-low" frequency 1896440000 Hz quality 1000
Timecounters tick every 10.000 msec
█
```

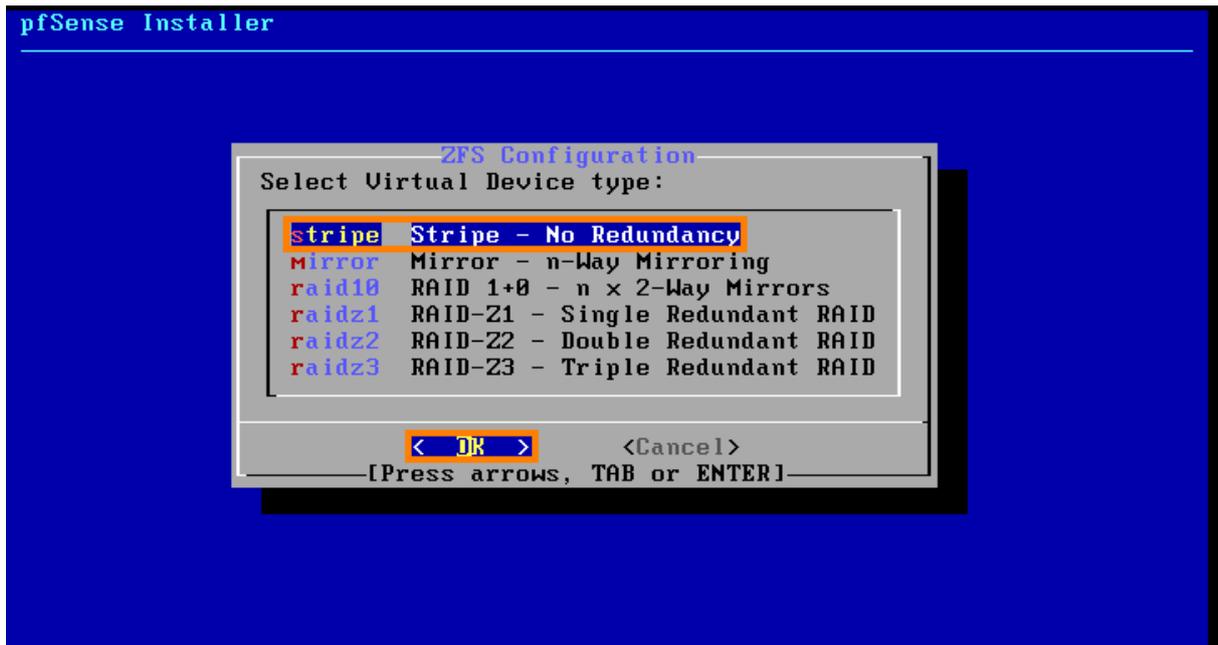
Une fois fait appuyé sur entrée :



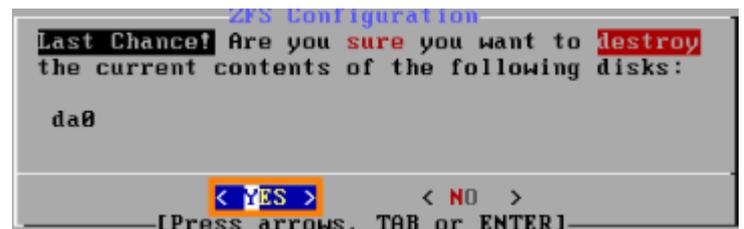
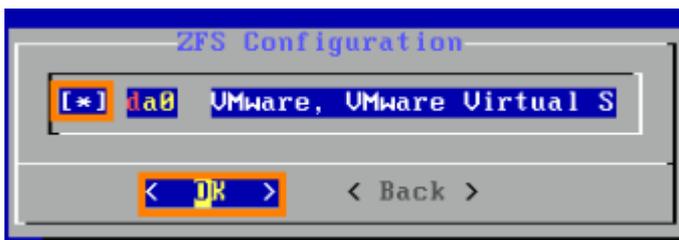


Veillez donc suivre les encadrement.



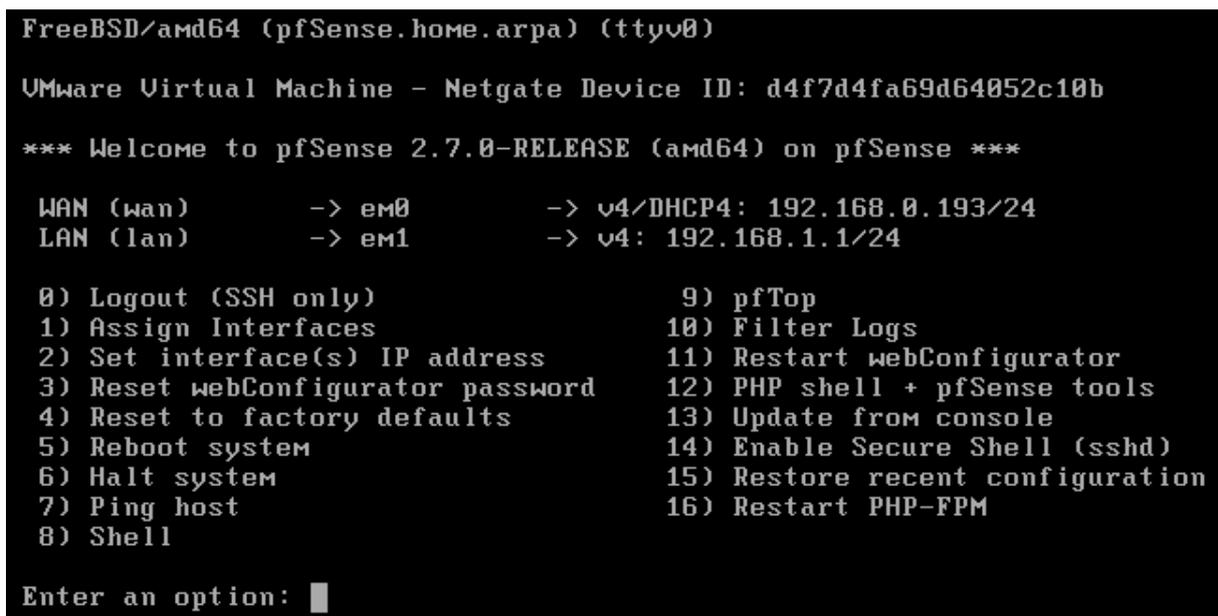


Ici, il faut sélectionner le disque virtuel, on appuie donc sur Espace puis Entrée.



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

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



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

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.193/24
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: 2
```

```
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
```

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

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.1

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 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
```

Il faut désormais se connecter à l'interface web de PfSense grâce à l'ip <https://192.168.100.1>

Les identifiants sont :

Id : admin

Mdp : pfsense

IV. Installation de Crowdsec

Execute Shell Command

Command

Execute Clear

Secure Shell

Secure Shell Server Enable Secure Shell

SSHd Key Only Password or Public Key

When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and a password. The default *Password or Public Key* setting allows either a valid password or a valid authorized key.

Allow Agent Forwarding Enables ssh-agent forwarding support.

SSH port 9922

Note: Leave this blank for the default of 22.

```
ssh admin@192.168.100.1 -p 9922
```

```
Windows PowerShell
PS C:\> ssh admin@192.168.100.1 -p 9922
The authenticity of host '[192.168.100.1]:9922 ([192.168.100.1]:9922)' can't be established.
ED25519 key fingerprint is SHA256:NyJF3X1psKbziThEGAsGF7BUYFZGX1QH66R2hw7KHdU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.100.1]:9922' (ED25519) to the list of known hosts.
(admin@192.168.100.1) Password for admin@pfSense.home.arpa:
VMware Virtual Machine - Netgate Device ID: d78dc7fa6e70ecde9511

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.60/24
LAN (lan)     -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)    -> em2      -> v4: 192.168.200.1/24

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

Enter an option: 8
```

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
```

```
Windows PowerShell
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: setenv IGNORE_OVERSION yes
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root:
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: pkg add -f https://github.com/crowdsecurity/pfsense-pkg-crowdsec/releases/download/v0.1.3/absell-20230126.3.pkg

Fetching absell-20230126.3.pkg: 100% 1 MiB 1.0MB/s 00:01
Installing absell-20230126.3...
Extracting absell-20230126.3: 100%
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: pkg add -f https://github.com/crowdsecurity/pfsense-pkg-crowdsec/releases/download/v0.1.3/rv2-20231101.pkg
Fetching rv2-20231101.pkg: 100% 296 KiB 303.3KB/s 00:01
Installing rv2-20231101...
Extracting rv2-20231101: 100%
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: pkg add -f https://github.com/crowdsecurity/pfsense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-1.6.0.pkg
Fetching crowdsec-1.6.0.pkg: 100% 42 MiB 22.2MB/s 00:02
Installing crowdsec-1.6.0...
Extracting crowdsec-1.6.0: 100%
#####
Package from crowdsec-1.6.0:
```

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

The screenshot shows the pfSense web interface. At the top, the navigation menu includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', and 'Diagnostic'. The 'Services' menu is open, and 'CrowdSec' is highlighted with an orange box. Below the menu, the 'Services: CrowdSec' configuration page is displayed. It features a 'Documentation' section with an 'IMPORTANT' note, a 'Remediation component (firewall bouncer)' section with an 'Enable' checkbox checked, and a 'Log processor (CrowdSec agent)' section with an 'Enable' checkbox checked. The page also includes a warning: 'Advanced Users Only. The capabilities offered here can be dangerous. No support is available.'

Veillez rentrez donc cette configuration :

Local API

Enable

Enable a local API on the pfSense box. Used by log processor and remediation components.
Recommended unless:

- you have a pre-existing main installation, maybe running on linux
- you want more control over the configuration, backup/restore, need a bigger machine or a postgres database
- you want more control over the running versions or want to run them on docker, k8s

If disabled, use a remote LAPI on an external machine.

LAPI host
Host name or IP. Change this to expose the LAPI to the LAN. For example you can have other servers running only the report to the LAPI in this pfSense machine. Otherwise, leave the default value (127.0.0.1).

LAPI port
Port number for the LAPI endpoint. Change in case of conflict with other services.

CrowdSec rules settings

 Rules will be hidden in the pfSense UI. If you have special needs, you can disable the rules here and provide your own.

Apply to all interfaces

Direction

Log

Tag

The actual rules may be slightly different according to the above options. Check /var/log/system.log

Enable CrowdSec IPv4 blocklist rule block drop (direction) {log} quick on (interfaces) inet from crowdsec_blacklists to any label "CrowdSec IPv4" tag (tag)

Enable CrowdSec IPv6 blocklist rule block drop (direction) {log} quick on (interfaces) inet6 from crowdsec6_blacklists to any label "CrowdSec IPv6" tag (tag)

CrowdSec rules settings

Rules will be hidden in the pfSense UI. If you have special needs, you can disable the rules here and provide your own.

Apply to all interfaces

Direction

Log

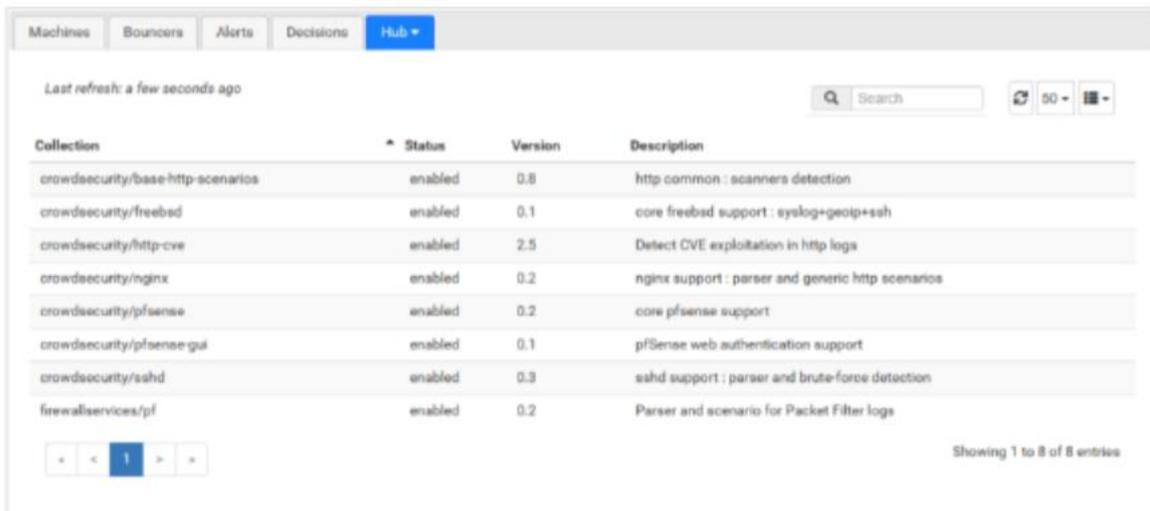
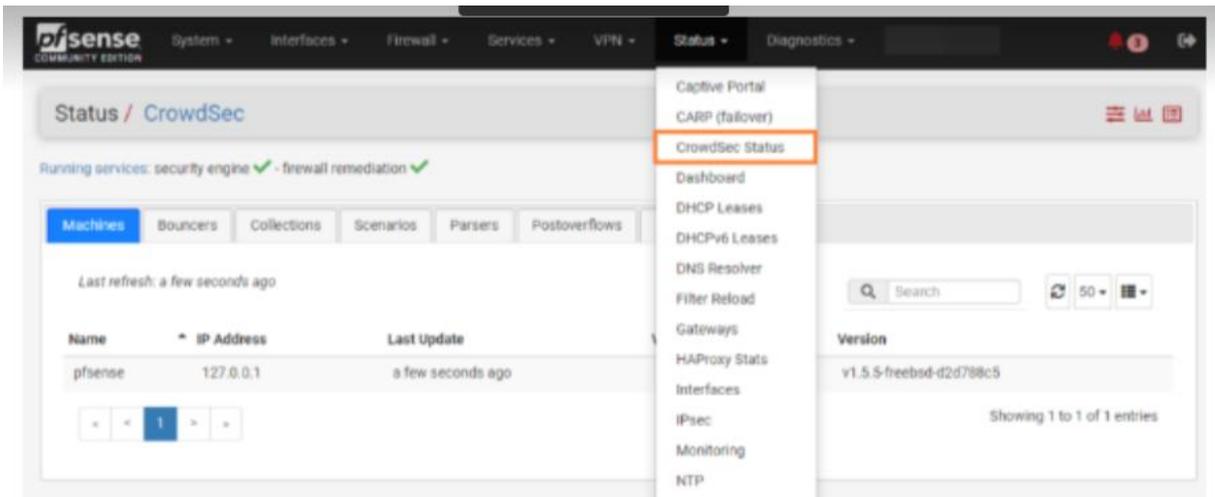
Tag

The actual rules may be slightly different according to the above options. Check /var/log/system.log

Enable CrowdSec IPv4 blocklist rule block drop (direction) {log} quick on (interfaces) inet from crowdsec_blacklists to any label "CrowdSec IPv4" tag (tag)

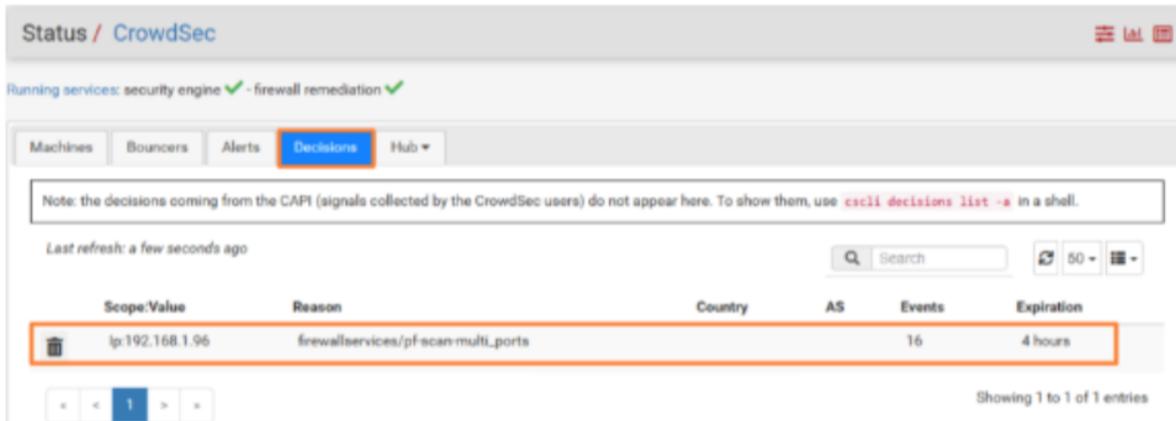
Enable CrowdSec IPv6 blocklist rule block drop (direction) {log} quick on (interfaces) inet6 from crowdsec6_blacklists to any label "CrowdSec IPv6" tag (tag)

  Saving settings, please wait..



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 été bannie en consultant la liste des décisions :

```
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	A5	Events	expiration	Alert ID
15001	crowdsec	Ip:192.168.1.96	firewallservices/pf-scan-multi_ports	ban			16	3h52m22.16200364s	2

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