



Guide d'installation & configuration

www.pfsense.org

Par Laura Giannico

1. Introduction & Contexte :

Dans cette documentation nous allons voir comment installer et configurer pas a pas, une VM afin d'accueillir un outil : **PfSense**.

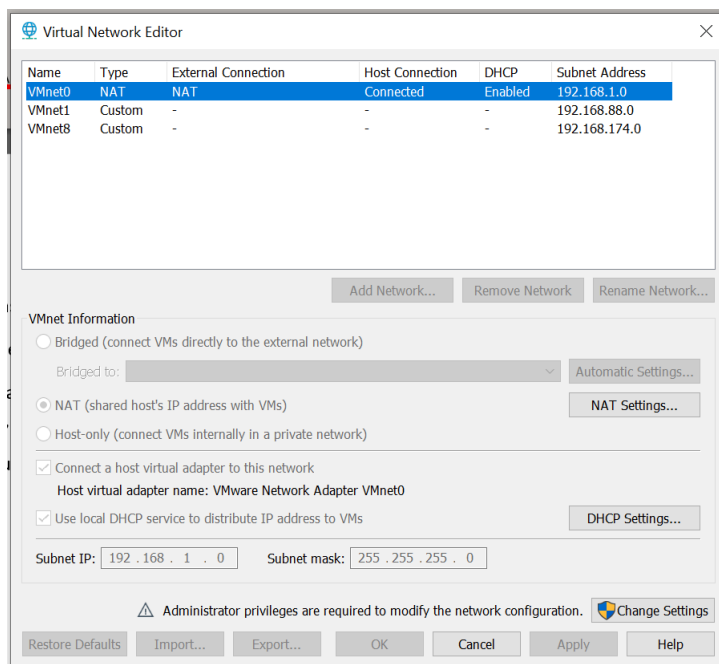
PfSense est un pare-feu base sous FreeBSD, qui a des fonctionnalités de routeur également. Nous verrons comment accéder à la version gratuite (open-source) Community Edition. FreeBSD est un OS sous Linux.

2. Configurer une VM :

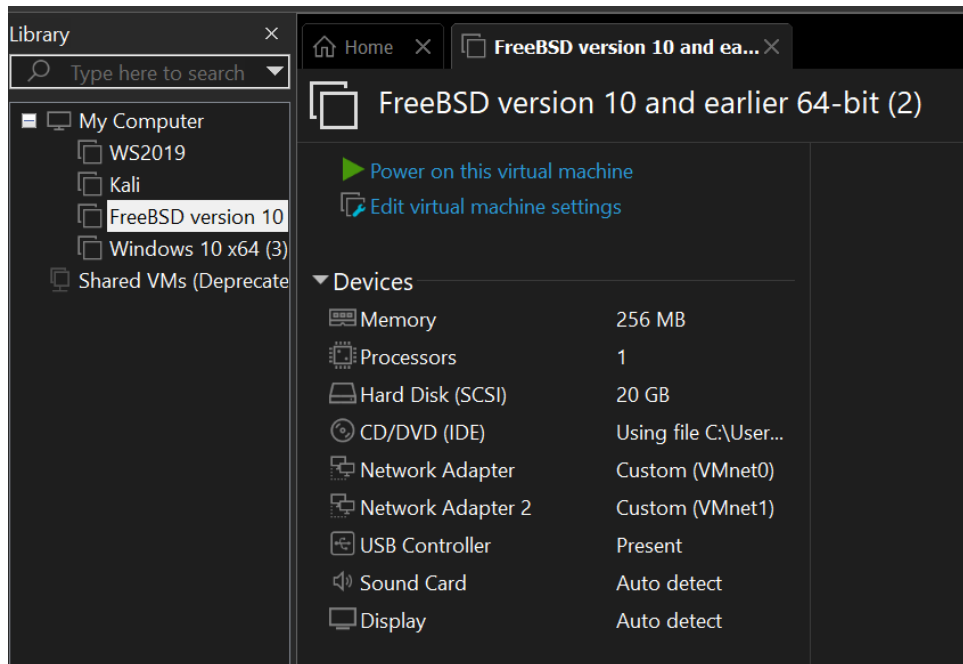
Télécharger l'ISO de **Pfsense** à l'adresse suivante : <https://www.pfsense.org/download/>

Une fois fait, ouvrez VMware, et créer une nouvelle VM en intégrant l'ISO dessus. Avant de lancer votre VM, il faudra la configurer. Pour commencer, aller sur *Edit > Virtual Network Editor*.

Il vous faudra le VMnet1 en Custom, et pour le VMnet0, il le faut en NAT et configurer de manière suivante :

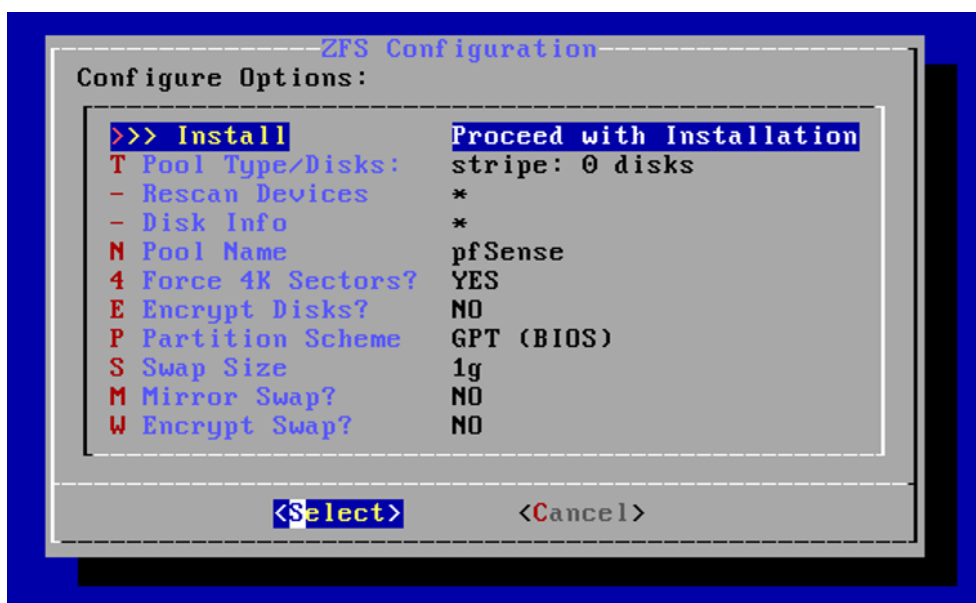
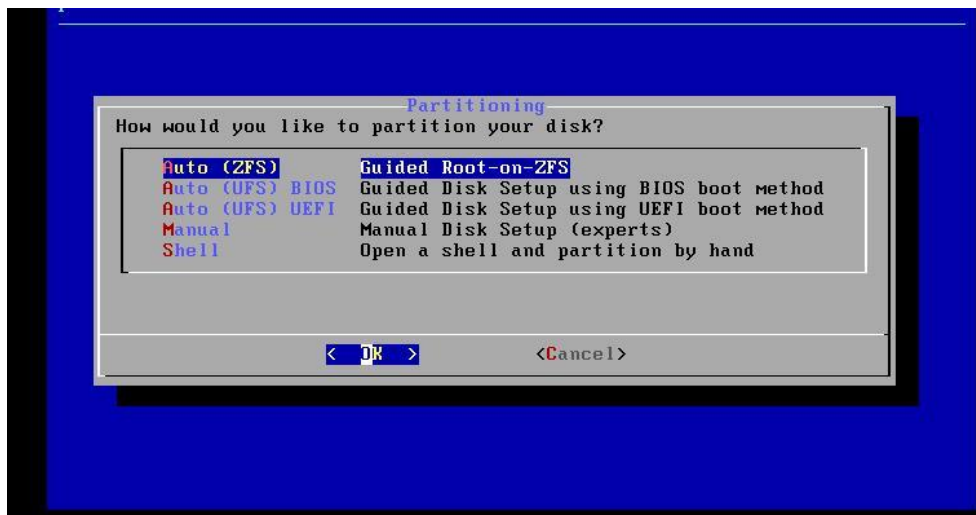
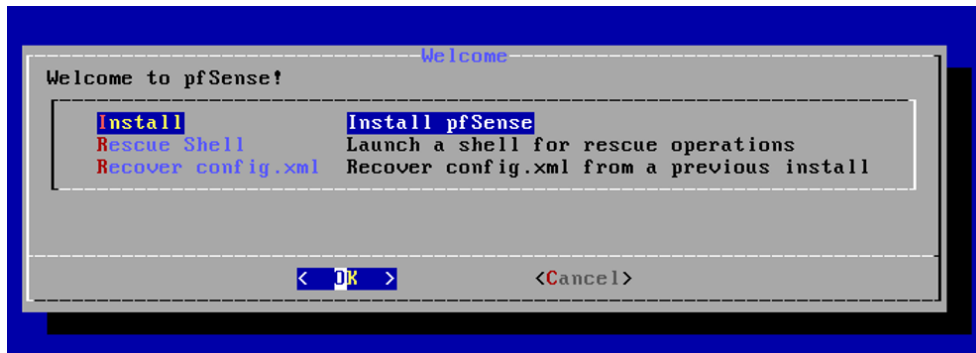


Puis, il faut ensuite modifier les paramètres de la VM en question. Sélectionner, 2 Network Adapter, en Custom, un pour VMnet0 et l'autre pour VMnet1.



3. Installer PfSense :

Allumez votre VM, l'installateur de **PfSense** va alors vous guider. Globalement, il y a juste à faire suivant sans modifier quoi que ce soit, mais juste au cas où, voici le guide complet :

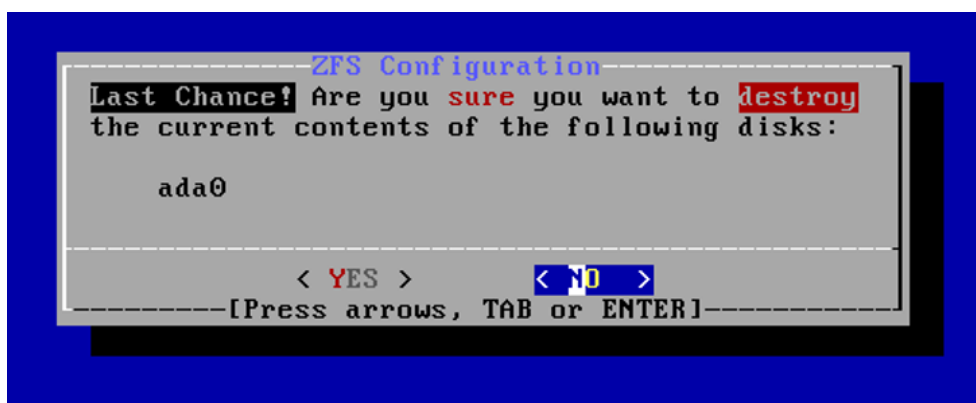


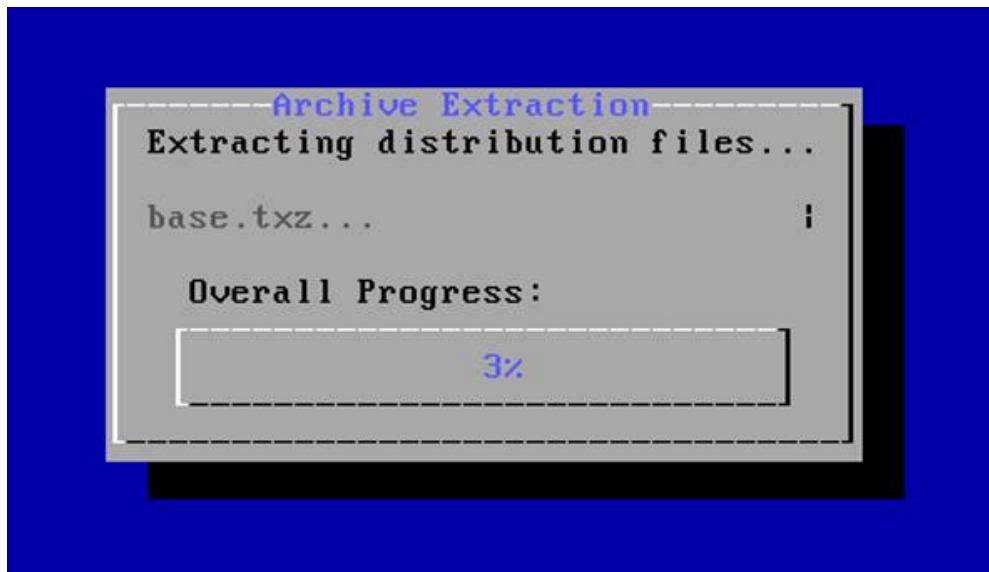


Sur le menu suivant, faite « espace » pour cocher :

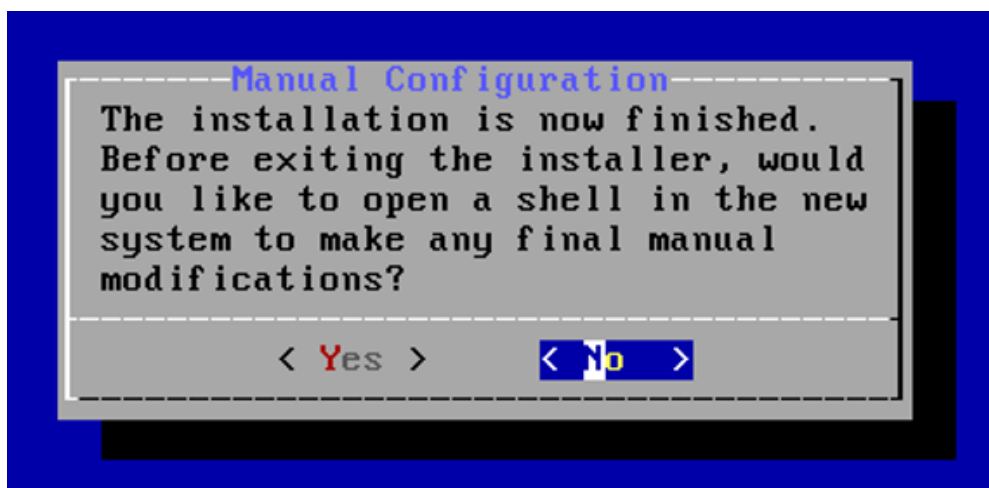


Sur le menu suivant, il faut dire « yes », vous n'avez pas le choix :

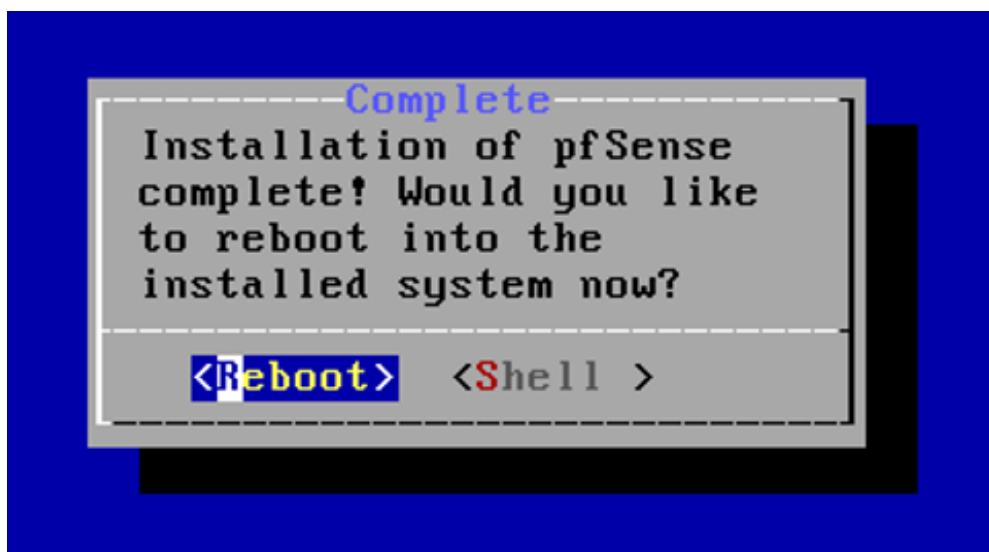




Dans le menu suivant, vous pouvez dire « non » :



Terminez l'installation en redémarrant votre VM :



4. Configurer Pfsense :

Lorsque votre VM redémarre, il faudra faire quelques modifications finales avant de pouvoir accéder à l'interface de Pfsense. De plus, ici tout se fera sous ligne de commande. Voici le menu que vous devriez voir apparaître si votre installation s'est bien passée :

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 05c9f0fc1b1bc5d9b4ca
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.14.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.254/24

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:
```

Sélectionner l'option 2, puis encore 2 (pour modifier l'IP du LAN) et entrez une adresse IPv4 statique :

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
```

L'interface va vous poser les questions suivantes, il faudra répondre par :

```
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:
>

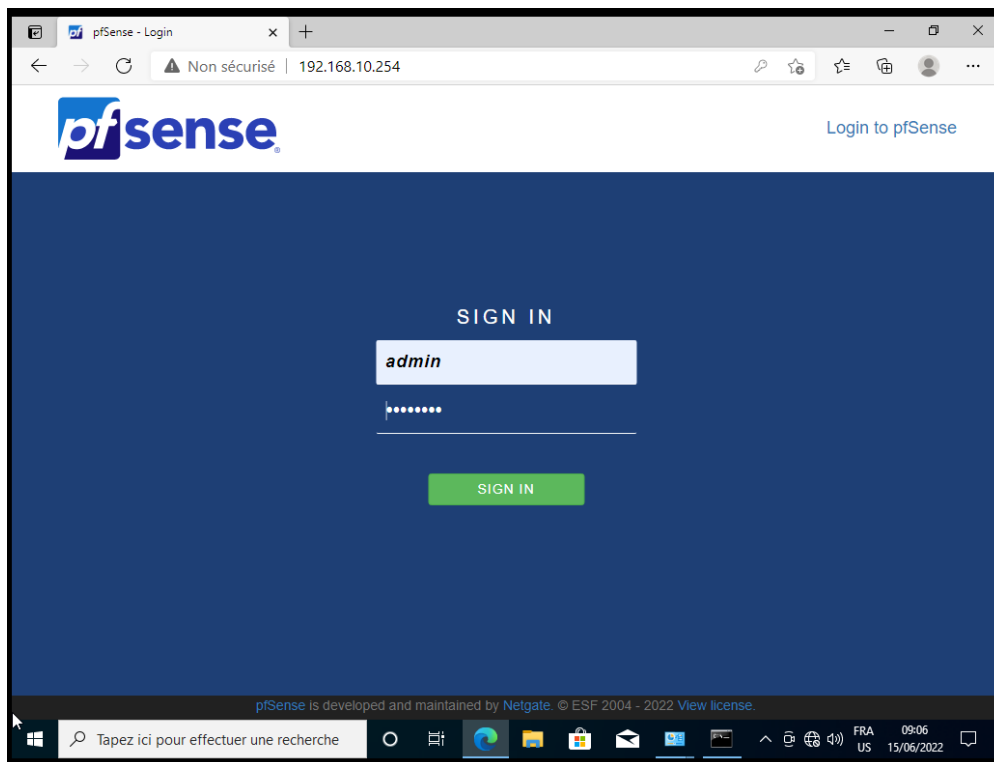
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
```

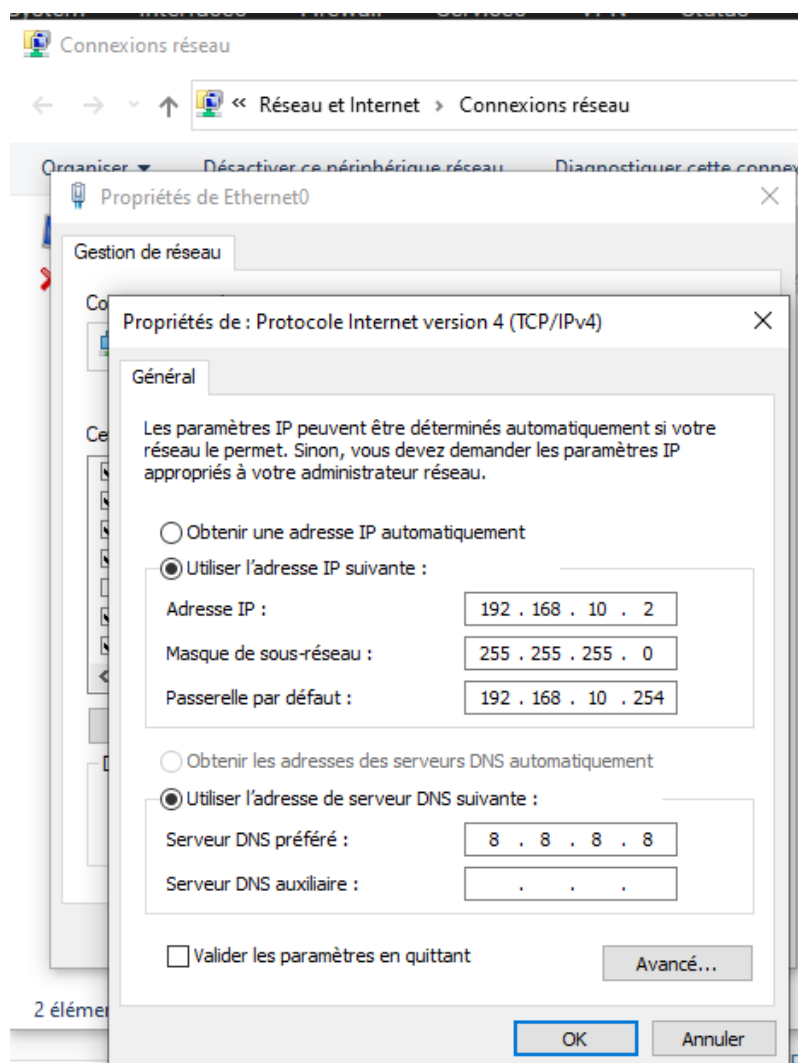

La configuration devrait être terminée. Hors de votre VM, sur votre ordinateur hôte, ouvrez votre navigateur et entrez l'adresse IP du LAN de votre VM :

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.14.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Restart webConfigurator     12) WebUI Shell
4) Reboot                     13) Shell
```



Dans le cas où cela ne fonctionnerait pas, il faut changer les configurations IPv4 de votre machine. Cependant, ne le faites pas, et préférez l'utilisation d'une VM sous Windows 10. Les configurations réseaux pour cette nouvelle VM sont les suivantes :



Ouvrez ensuite le navigateur sur la VM de Windows 10 et accédez à l'interface de **PfSense** grâce à l'adresse IP du LAN. Les identifiants par défaut pour se connecter à l'interface sont :

Username : *admin*

Mot de passe : *pfsense*

Bienvenue sur le dashboard de **Pfsense**, vous pouvez commencer à travailler !

The screenshot displays the pfSense Community Edition dashboard in a web browser. The browser's address bar shows the URL `pfSense.home.arpa` and the IP address `192.168.10.254`. The dashboard is titled "Status / Dashboard" and features two main panels.

System Information

Name	pfSense.home.arpa
User	admin@192.168.10.2 (Local Database)
System	VMware Virtual Machine Netgate Device ID: cf4a9a10e9b21abfb943
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Wed Jul 22 2020
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE The system is on the latest version. Version information updated at Wed Jun 15 7:04:09 UTC 2022
CPU Type	Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Disabled

Netgate Services And Support

Contract type: **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

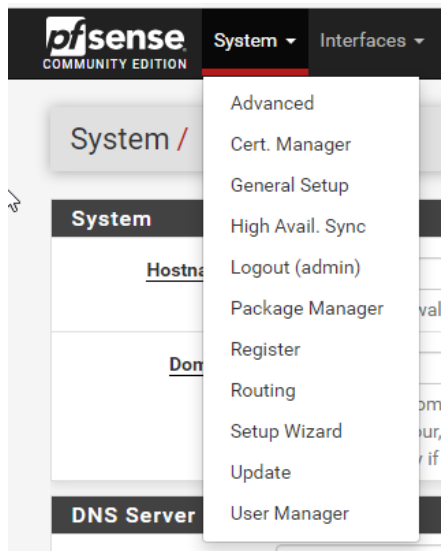
- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional](#)
- [Visit Netgate.com](#)

The Windows taskbar at the bottom shows the search bar with the text "Tapez ici pour effectuer une recherche", the system clock at 09:12 on 15/06/2022, and the location FRA US.

5. Appréhendez l'interface de Pfsense :

a. Configurations générales :

La première chose à faire est d'aller dans [System > General Setup](#) :

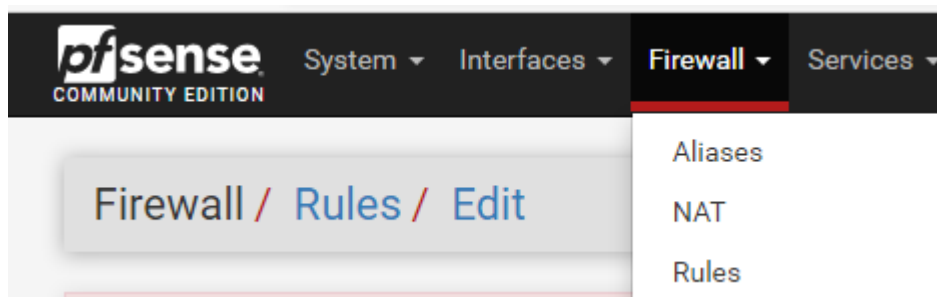


Laissez tout par défaut, sauf l'adresse du DNS Server : j'ai personnellement mis 8.8.8.8

Cliquez sur [\[Save\]](#), on vous demandera d'autres configurations, dont le mot de passe. Changez-le ou remettez celui par défaut.

b. Filtrage « deny all » :

Nous allons performer un filtrage qui bloque tout connexion internet. Pour faire un filtrage grâce a Pfsense, il faut se rendre ici : [Firewall > Rules](#)



Ajouter une nouvelle règle en cliquant sur [\[Add\]](#).

Puis configurer votre règle comme ceci :

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

La source et la destination devront être configurées a « *any* » pour se laisser aucune connexion entrante ni sortante. Enregistrez votre règle. Votre pare-feu bloque désormais toute tentative d'entrées et de sorties de n'importe quels protocoles.

c. Filtrage internet :

L'exercice précédent n'est pas très pratique : plus rien ne peut entrer ou sortir sur votre réseau. Cette fois-ci, nous allons configurer une règle pour faire en sorte qu'uniquement le trafic internet puisse passer.

Retournez sur l'interface, vérifiez que votre règle précédente est toujours active, car nous allons en rajouter une nouvelle par-dessus pour autoriser internet. Allez dans [Firewall > Aliases](#) pour vous créer un alias qui contiendra les plages de Ports a autorisé. Vous devrez mettre les Ports 80, 53 et 443.

Firewall / Aliases / Edit

Properties

Name

MyCuteAlias

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Port(s)

Port(s)

Hint

Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	443	Entry added Wed, 15 Jun 2022 11:21:27 +0000	Delete
	80	Entry added Wed, 15 Jun 2022 11:21:27 +0000	Delete
	53	Entry added Wed, 15 Jun 2022 11:21:27 +0000	Delete

Save

Export to file

Add Port

Page 14 | 17

Validez votre alias. Puis retourner dans [Firewall > Rules](#), ou il faudra autoriser l'accès à ces Ports (il faudra mettre en Destination votre Alias). Voici les screenshots de la configuration de la règle :

Firewall / Rules / Edit

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match /

Destination Port Range
From Custom To Custom

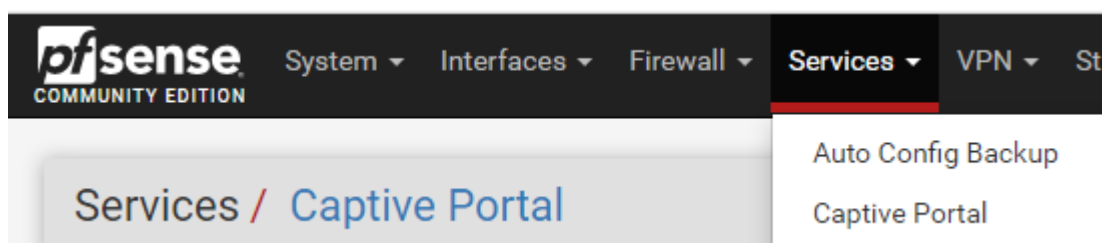
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Sauvegardez votre configuration, et normalement, tout le trafic est bloqué, à l'exception d'internet.

d. Portail captif :

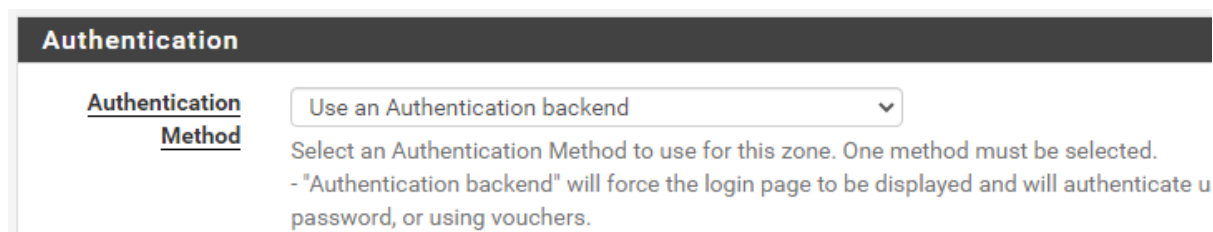
Un portail captif est une interface web qui s'affiche sur le navigateur vous demandant des identifiants afin d'accéder au réseau. Exemple, vous vous connectez sur le réseau Wi-Fi d'un hôtel, et l'interface vous demande des identifiants pour savoir si vous avez bien payé la connexion ou non. Vous ne serez pas autorisé à naviguer sur internet si les codes d'accès ne sont pas renseignés.

Nous allons mettre en place cette solution grâce à **Pfsense**, un portail captif avec authentification interne. C'est-à-dire que vous ne pourrez qu'accéder à Internet si vous avez des identifiants (créer sous **Pfsense**). Il faut aller dans *Services > Captive Portal*.



Puis cliquez sur [Add]. Donnez un nom et une description puis cliquez sur [Save]. Cochez la case « *Enable Captive Portal* », et d'autres options vont apparaître.

Sélectionnez LAN dans le champ « Interfaces » et laissez tout le reste par défaut. Aller ensuite dans la section « Authentification » et sélectionnez :



Sauvegardez votre règle.

Puis allez dans *System > User Manager > Groups*. Créer un groupe :

Group Properties

Group name

Scope

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

Group description, for administrative information only

Group membership

admin

Not members

Members

» Move to "Members"

« Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Ensuite, sauvegardez le groupe et rééditez-le. De nouvelles configurations sont disponibles. Sélectionnez les suivantes :

Group Privileges

Group LauraGroup

Assigned privileges

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted sc
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPoE Dialin
- WebCfg - AJAX: Get Queue Stats
- WebCfg - AJAX: Get Service Providers
- WebCfg - AJAX: Get Stats
- WebCfg - All pages
- WebCfg - Crash reporter
- WebCfg - Dashboard (all)
- WebCfg - Dashboard widgets (direct access).
- WebCfg - Diagnostics: ARP Table

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Sauvegardez votre groupe. Et voilà le travail ! Il faudra par la suite créer vos utilisateurs, et les assigner au groupe que vous venez de créer. Ils auront alors l'obligation de passer par votre portail captif pour se connecter, avec les identifiants que vous leur avez créés.