A dark blue vertical bar on the left side of the page. A blue arrow points to the right from this bar, containing the date.

15/06/2022

# Pfsense

Cybersécurité

- Comprendre et mettre en œuvre des règles de firewalling
- Documentation : installation, la configuration et le paramétrage
- Filtrage : « deny all »
- Filtrage : internet
- Portail captif

## Table des matières

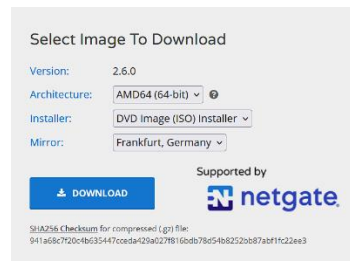
Chercher l'ISO de pfsense .....	2
VirtualBox .....	2
Configuration de la vm pfsense .....	3
Cartes réseaux .....	3
IPs (et si on veut le modifier).....	3
Configuration de la VM Client W10 .....	4
Accès à pfsense web configuration .....	4
Accès par internet.....	4
Accès à la création d'Alias .....	5
Création de l'alias pour autoriser le port 80,443 et 53. ....	6
Alias créé .....	6
Mise en place des règles.....	7
Règles mises en place sur pfsense .....	7
Test d'intégration .....	8
Le portail captif.....	9

## Chercher l'ISO de pfsense

L'ISO de pfsense est trouvable sur le site

<https://www.pfsense.org/download/>

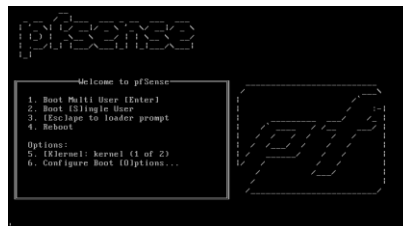
Ici on télécharge FreeBSD



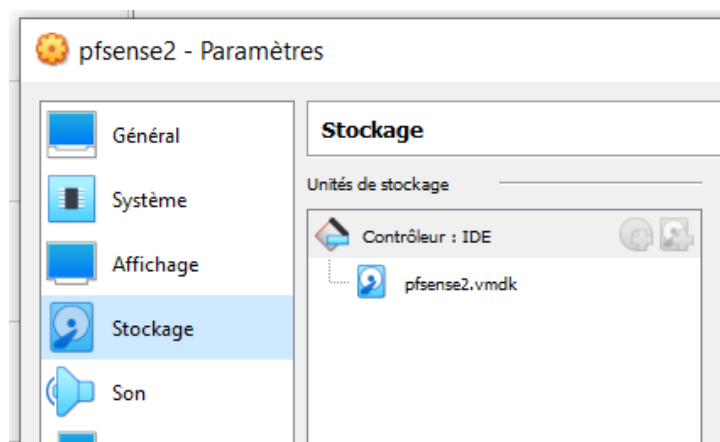
## VirtualBox

Ensuite on va créer une VM pour accueillir FreeBSD, une classique.

Lancer l'installation classique et on n'oublie pas d'activer le disque en appuyant sur espace pour cocher ada0 avec \* lors du paramétrage. Laisser l'installation se terminer.



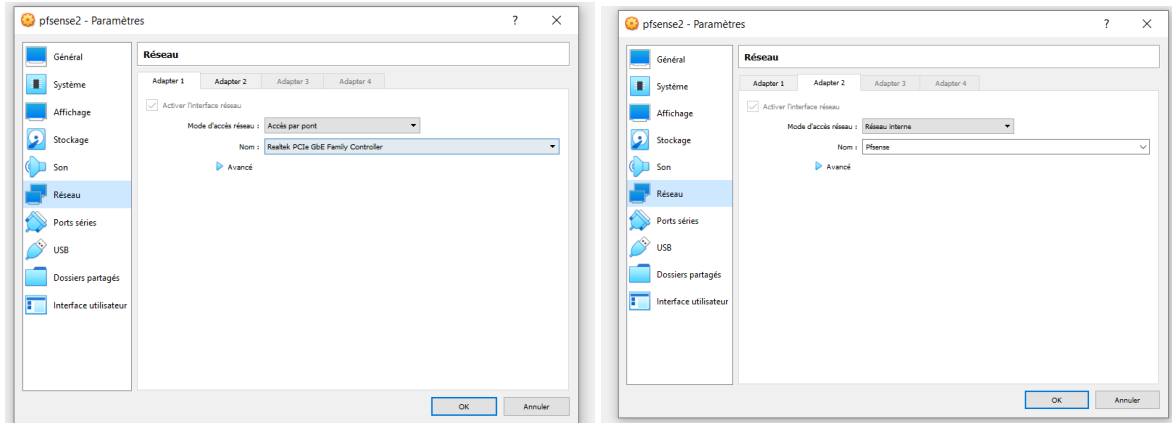
Ensuite redémarrer comme demandé. Cependant, il ne peut pas redémarrer, il faut éjecter l'ISO de pfsense qui se trouve dans l'espace vide ici et le supprimer. Il ne doit rester que la vm, ici pfsense2.vmdk.



Ensuite redémarrer et l'interface apparaît.

## Configuration de la vm pfsense

### Cartes réseaux



Ici je vais créer un d'abord

- Un accès par pont avec ma carte réseau actuelle
- Un réseau interne nommé PfSense

### IPs (et si on veut le modifier)

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.77.43.22/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
```

Si on aurait voulu modifier l'adresse on peut y accéder en appuyant sur 1 ou 2

1 pour configurer les interfaces (LAN ou WAN) et 2 pour paramétrer les adresse IP des cartes.

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.77.43.22/24
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
4) Reset to factory defaults  12) PHP shell + pfSense tools
5) Reboot system             13) Update from console
6) Halt system               14) Enable Secure Shell (sshd)
7) Ping host                 15) Restore recent configuration
8) Shell                     16) Restart PHP-FPM
```

On peut y voir les interfaces valides

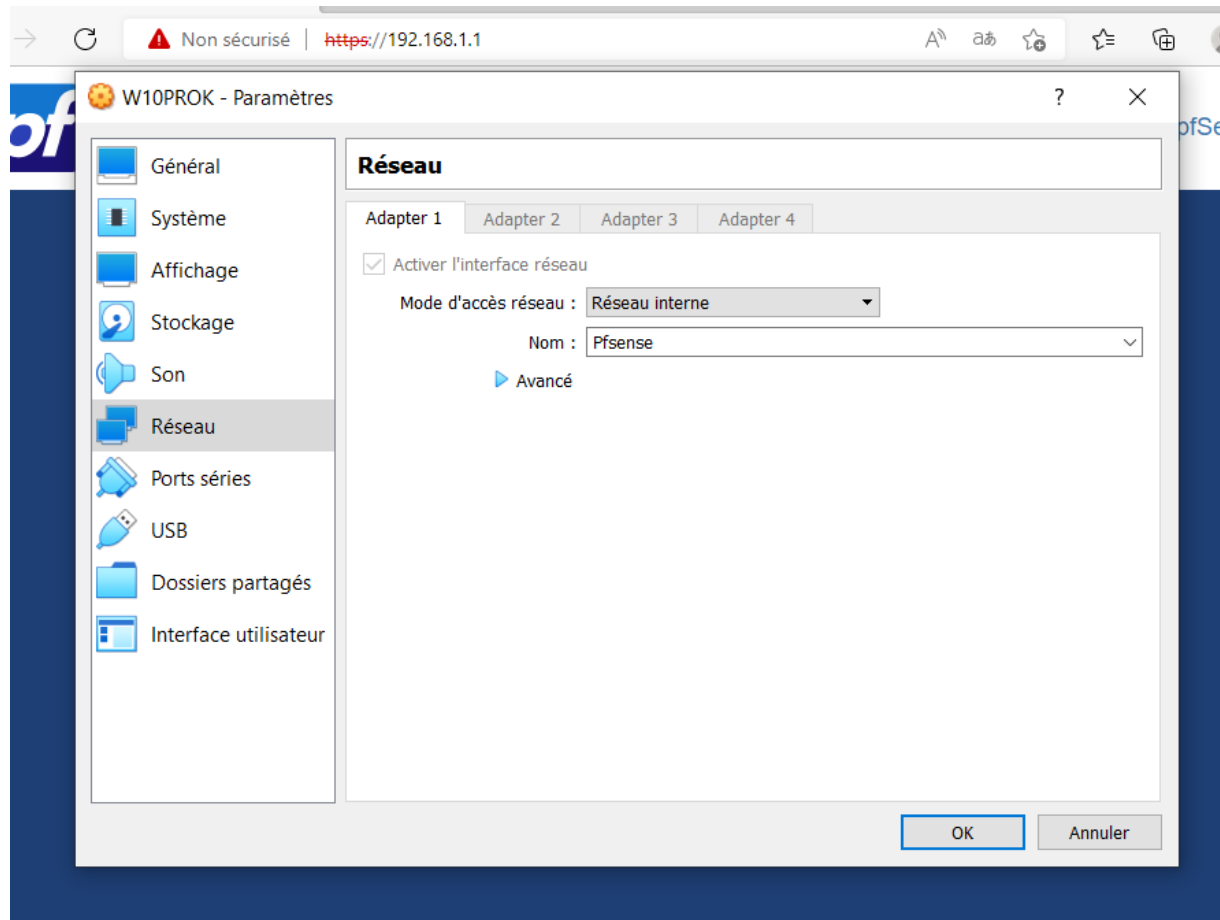
```
Valid interfaces are:

em0      08:00:27:68:41:a7  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:14:31:c7  (up) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
```

Dans notre cas l'adresse de em0 et em1 ont été préconfigurées

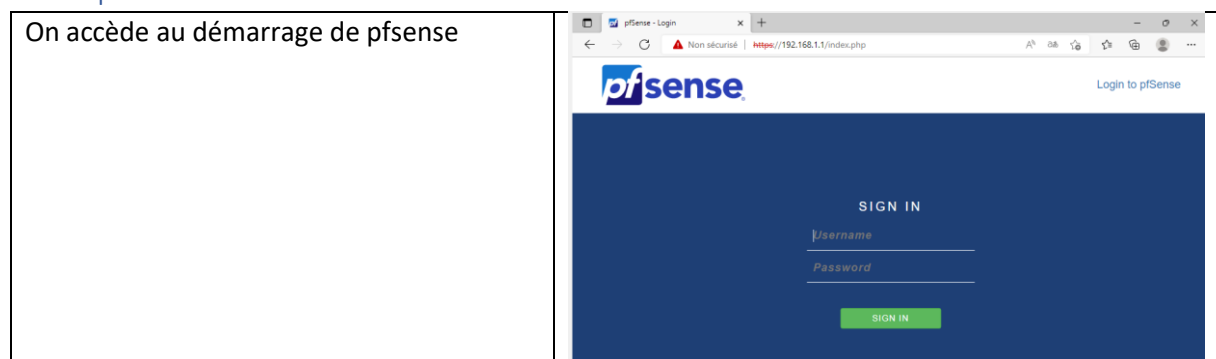
## Configuration de la VM Client W10



Je suis en réseau interne (nommé Pfsense)

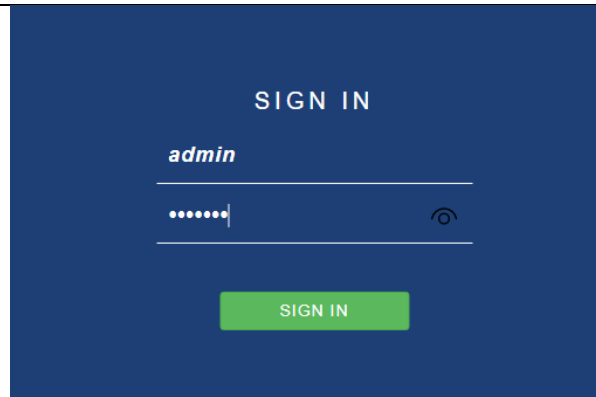
## Accès à pfsense web configuration

### Accès par internet



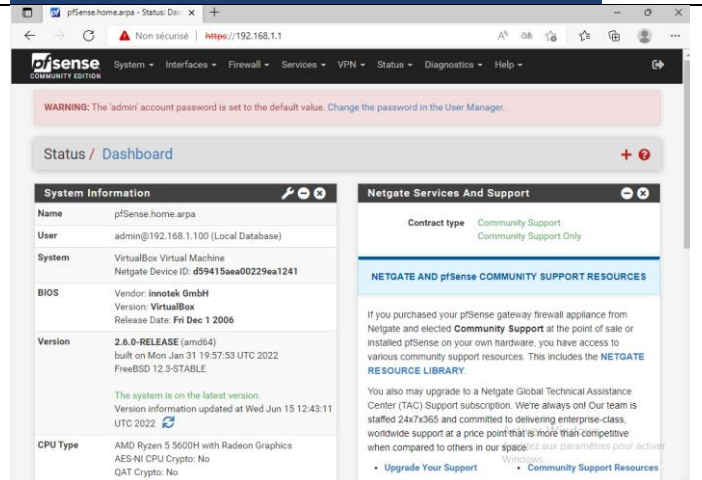
Les identifiants sont par défaut

Login : admin  
Mdp : pfsense



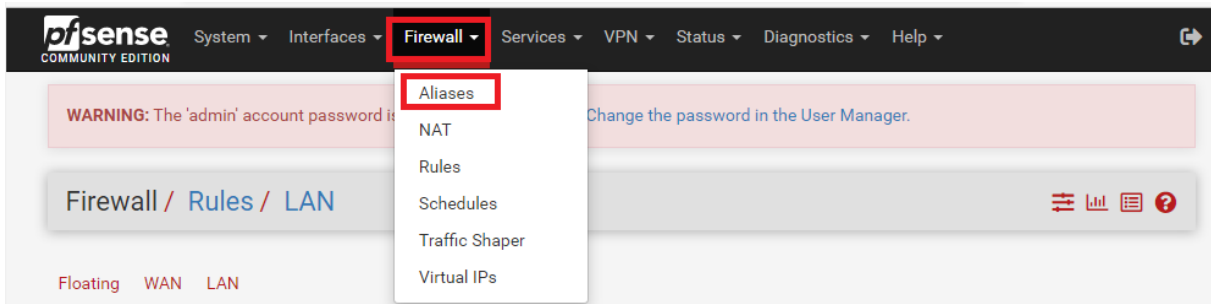
Après une série de configurations, on arrive au dashboard, le tableau de bord, de pfsense.

On y trouve l'user, le nom utilisé, les données systèmes, etc.

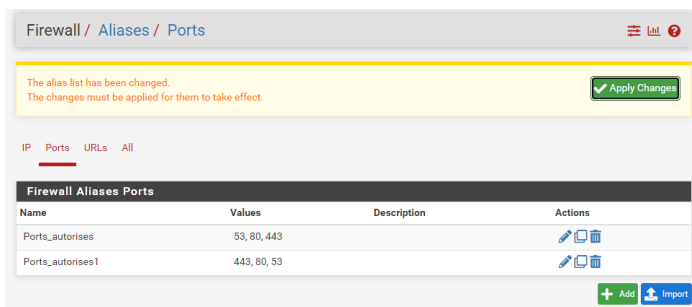


Désormais, on va commencer à élaborer les règles que va utiliser le pare-feu. Nous ferons tout en local sur la machine client. D'abord grâce aux alias, nous allons pouvoir regrouper plusieurs règles en une seule, si on veut mettre plusieurs infos en une fois (ports/ip)

## Accès à la création d'Alias



On peut choisir entre plusieurs alias, ici nous avons besoin de la catégorie Ports



Création de l'alias pour autoriser le port 80,443 et 53.

**Properties**

**Name**   
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)**

**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	Entry added	Action
<input type="text" value="443"/>	Wed, 15 Jun 2022 11:33:55 +0001	
<input type="text" value="80"/>	Wed, 15 Jun 2022 11:33:55 +0001	
<input type="text" value="53"/>	Wed, 15 Jun 2022 11:33:55 +0001	

Save Export to file Add Port

Activer Windows

Ici nous pouvons choisir le nom donné à l'alias, et mettre une description si besoin, choisir le type, et on peut y ajouter les ports voulus, ici le 443, 80 et le 53.

## Alias créé

Firewall / Aliases / Ports

The alias list has been changed.  
The changes must be applied for them to take effect.

IP Ports URLs All

Name	Values	Description	Actions
Ports_autorises	53, 80, 443		
Ports_autorises1	443, 80, 53		

Add Import

Les ports qu'on choisit son en fait ceux d'internet ou des protocoles qu'on souhaite garder, ici

- Le port 80 relatif au TCP/http
- Le port 443 relatif au http sécurisé : https
- Le port 53 relatif au TCP UDP DNS

## Mise en place des règles

Nous allons nous intéresser à la catégorie LAN car c'est là que nous travaillons. Ici nous allons pouvoir choisir l'ordre des règles, les informations sur le protocole, l'état actuel (si des données transitent par la règle), mettre à jour les ports, une description, une passerelle...

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	6 / 17.42 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0 / 0 B	IPv4 ICMP any	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	6 / 40.90 MiB	IPv4 TCP/UDP	LAN net	*	*	Ports_ autorises1	*	none		Ports autorisés	
<input type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	*	none		Activator Windows	

Si la règle bloque, passe ou rejette.

Le protocole utilisé

le groupe de protocole

description

## Règles mises en place sur pfSense

Floating

WAN

LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 / 14.05 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0 / 0 B	IPv4 ICMP any	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	LAN net	*	*	Ports_ autorises1	*	none		Ports autorisés	
<input type="checkbox"/>	0 / 6 KiB	IPv4 *	LAN net	*	*	*	*	none			

Add

Add

Delete

Save

Separator

On retrouve dans postes autorisés1

L'ordre expliqué, de bas en haut :

- La première règle est bloquée, elle est liée à tous les ports existants (tout internet est bloqué)
- La deuxième règle ouvre les ports 53, 443 et 80, ils sont autorisés



- La troisième et quatrième règle sont des règles d'origine. Ils sont là pour autoriser ou bloquer l'accès à internet pour toutes les règles.
- La dernière règle est celle qui nous permet d'aller sur la pfsense grâce au protocole 443/80, on doit le laisser.

## Test d'intégration

On va vérifier si tout est ok au niveau des règles de pfsense.

Ping de google pour voir si tout est ok

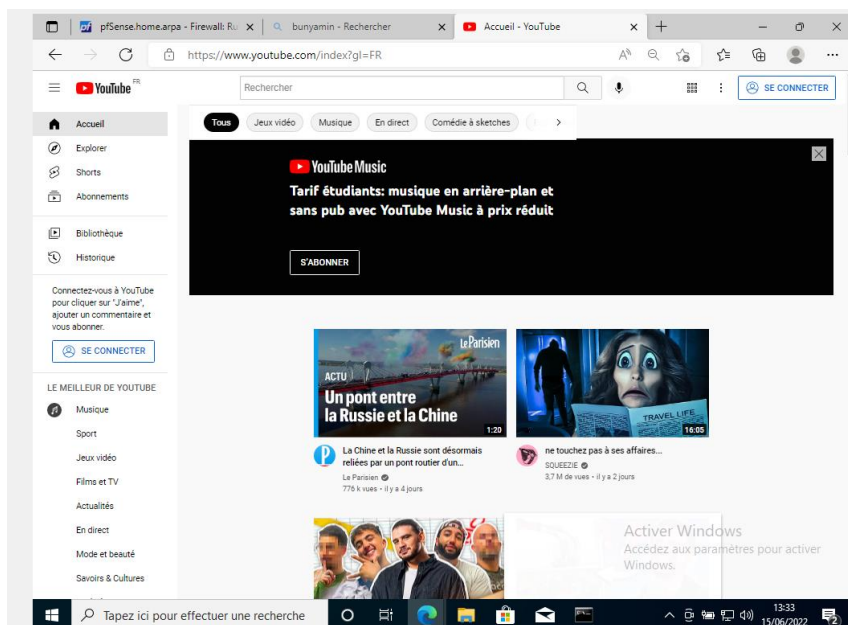
```
C:\Users\W10TEST>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=118
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=118
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=118
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=118

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 9ms, Maximum = 9ms, Moyenne = 9ms



C:\Users\W10TEST>
```



Test aussi sur youtube




## Le portail captif

Nous allons configurer une partie du portail captif

Services / Captive Portal  

Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
captive_portail	LAN	0	portail captif	 

 Add

Je n'ai pas fait beaucoup de modifications mis à part l'interface ou j'ai choisi LAN et après je n'ai rien modifié d'autre.