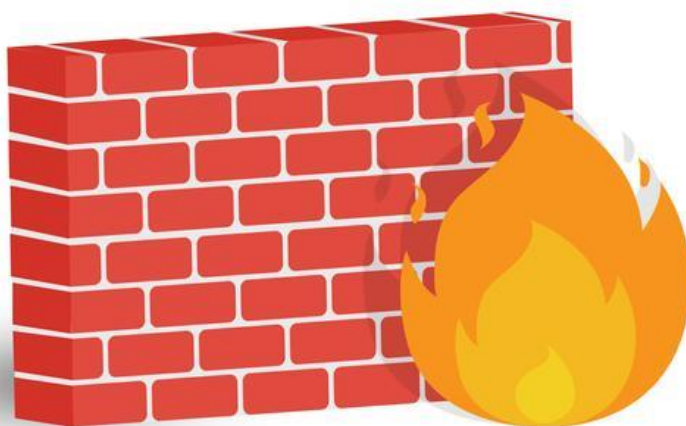


Installation d'un Pare-feu



 **Sense FIREWALL**

SOMMAIRE

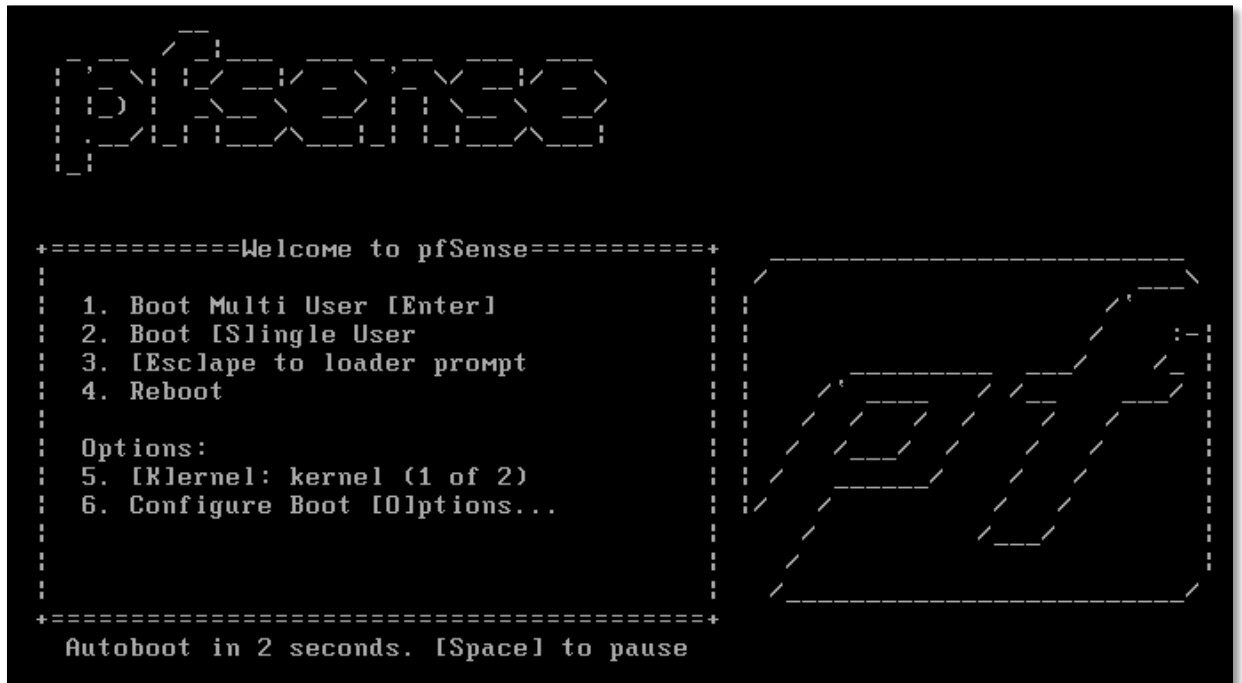
1) Introduction.....	1
2) Installation de Pfsense.....	2
3) Configuration de Pfsense.....	7
4) Configuration de l'interface web.....	11
5) Création de règle.....	18
6) Lexique	20

1) Introduction

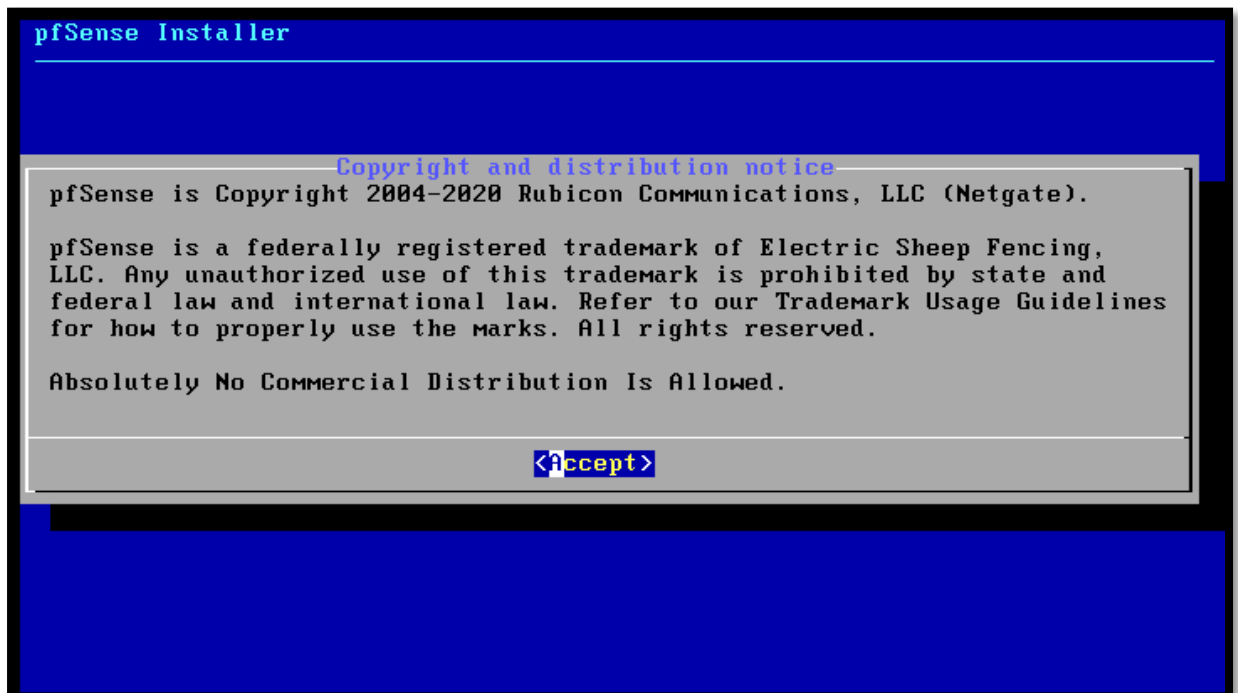
Les pare-feux sécurisent les connexions à Internet. Des protections de pare-feu sont installées sur chaque Mac, PC Windows et routeur. Dans les entreprises, un pare-feu logiciel équipe tous les ordinateurs des employés ainsi que leur réseau dans son ensemble afin de protéger les communications de l'entreprise.

2) Installation de PfSense

Commençons l'installation de pfsense. Après avoir insérer l'ISO et lancé votre VM
L'installation va démarrer automatiquement quelques secondes après.

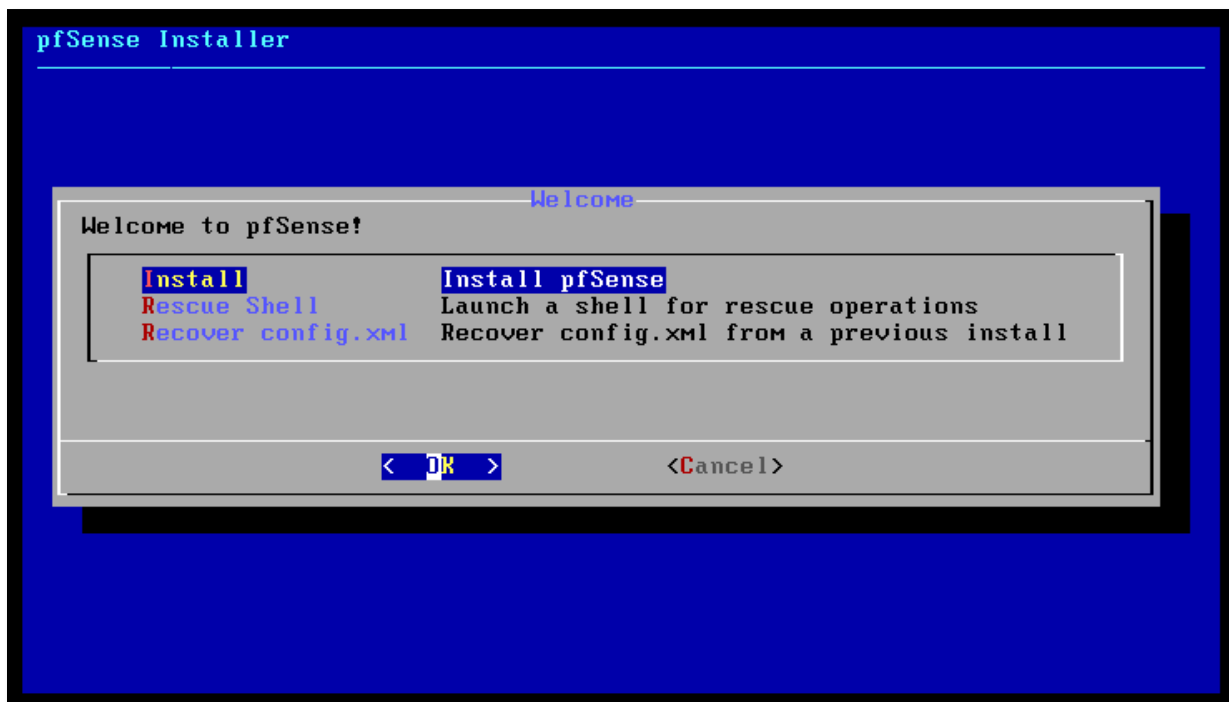


L'installation se fera uniquement au clavier.

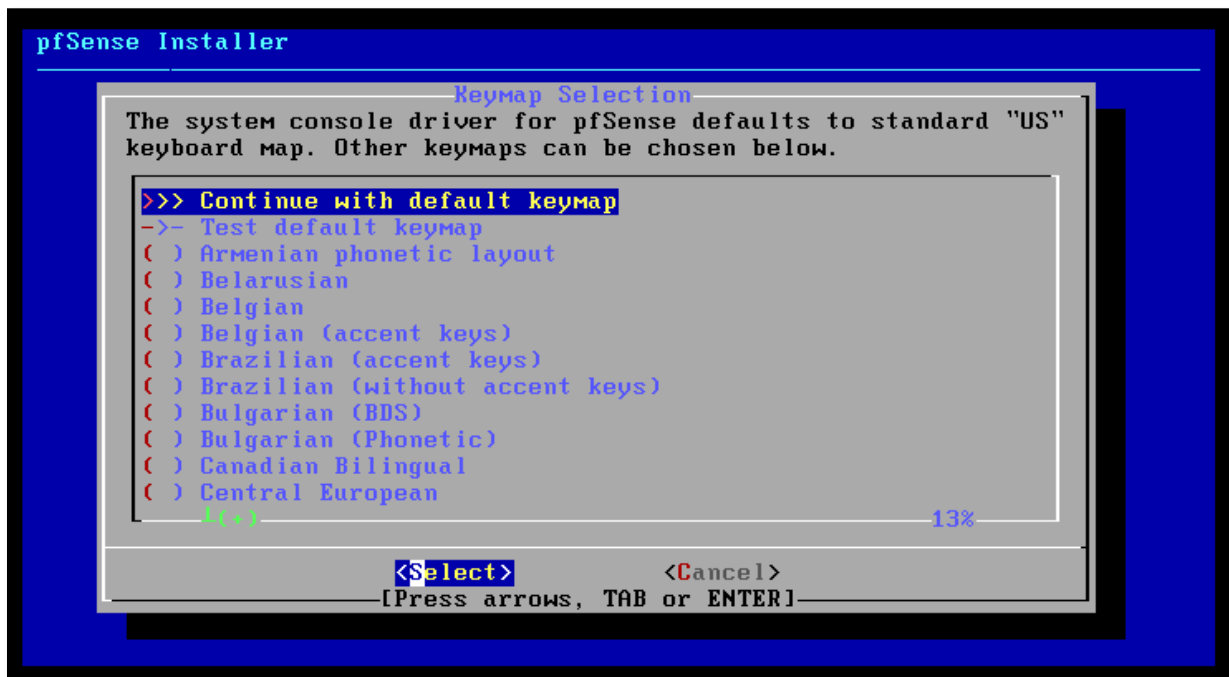


Appuyez sur la touche Entrée pour Accepter.

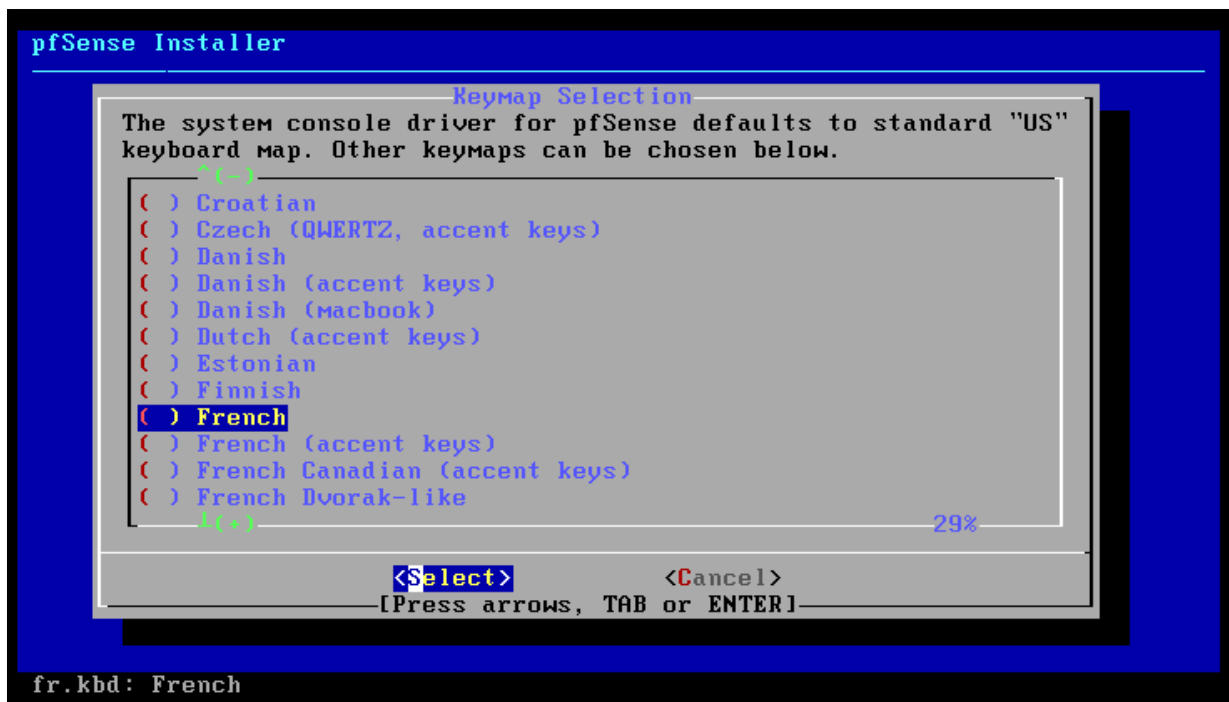
Vérifiez que vous êtes bien sur « Install » et appuyez sur Entrée pour faire OK.



Il faut sélectionner votre langue afin d'avoir la bonne disposition selon votre clavier



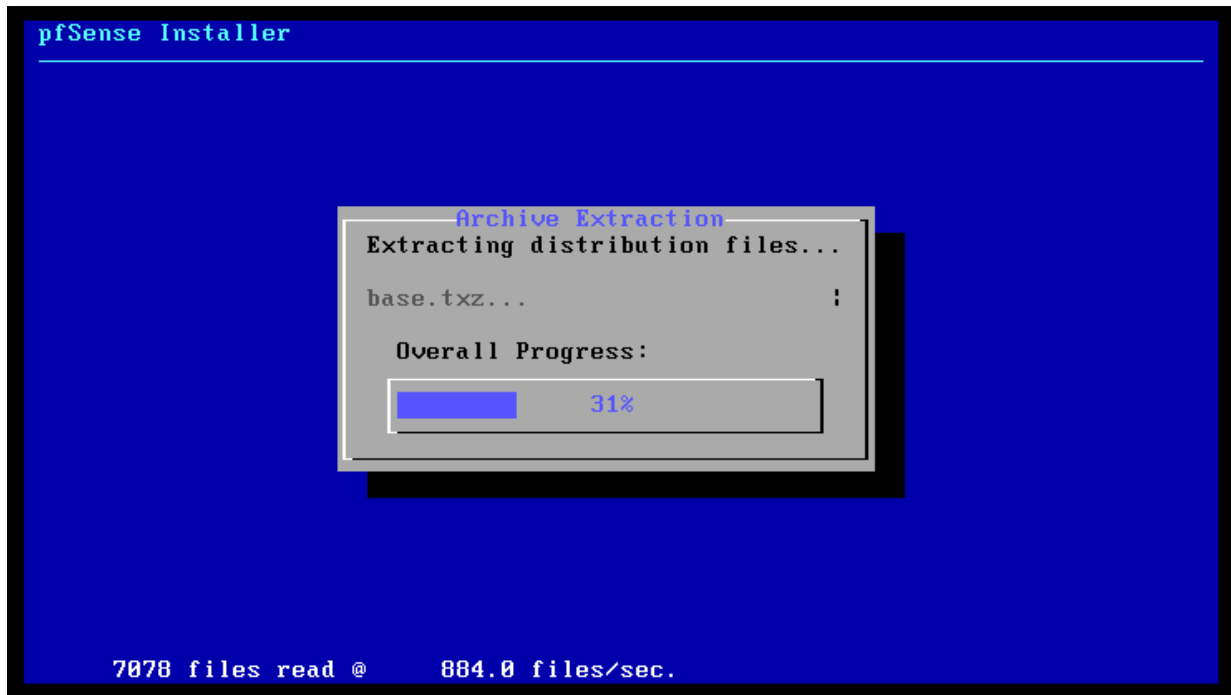
Descendez avec les flèches jusqu'à « French » et appuyez sur Entrée.



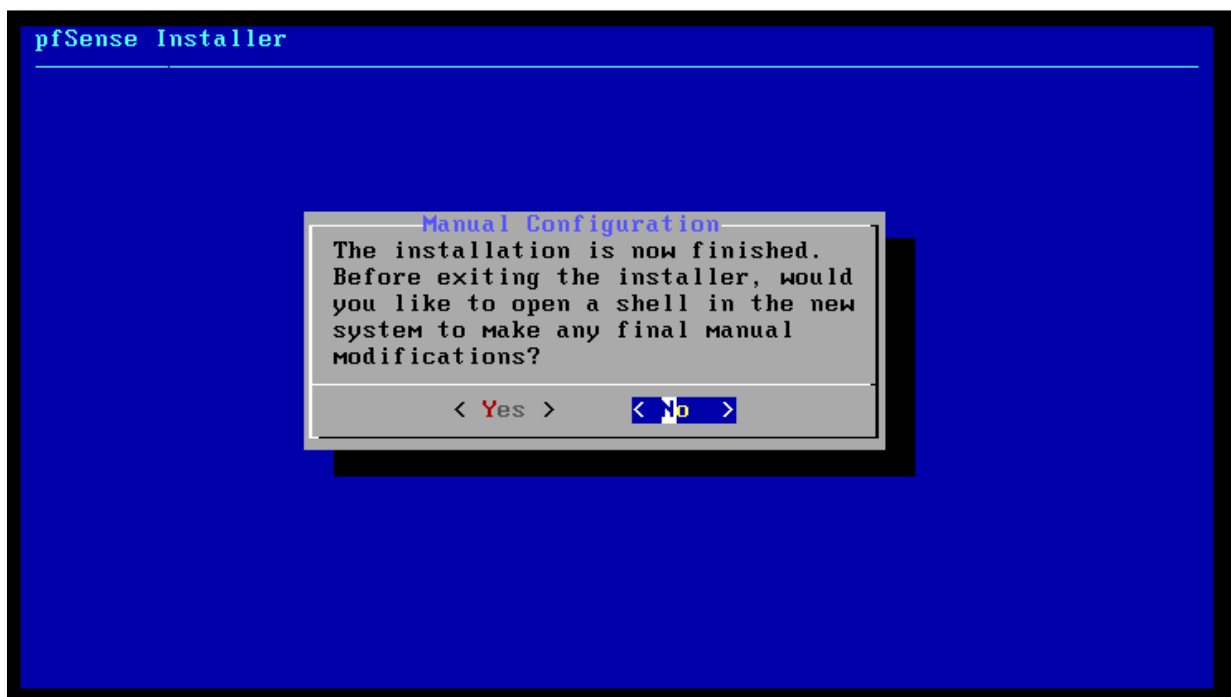
L'installateur va vous demander si vous voulez partitionner le disque dur. Nous allons rester, sur « Auto (UFS) » et appuyez sur Entrée.



L'installation se fera automatiquement pendant quelque seconde

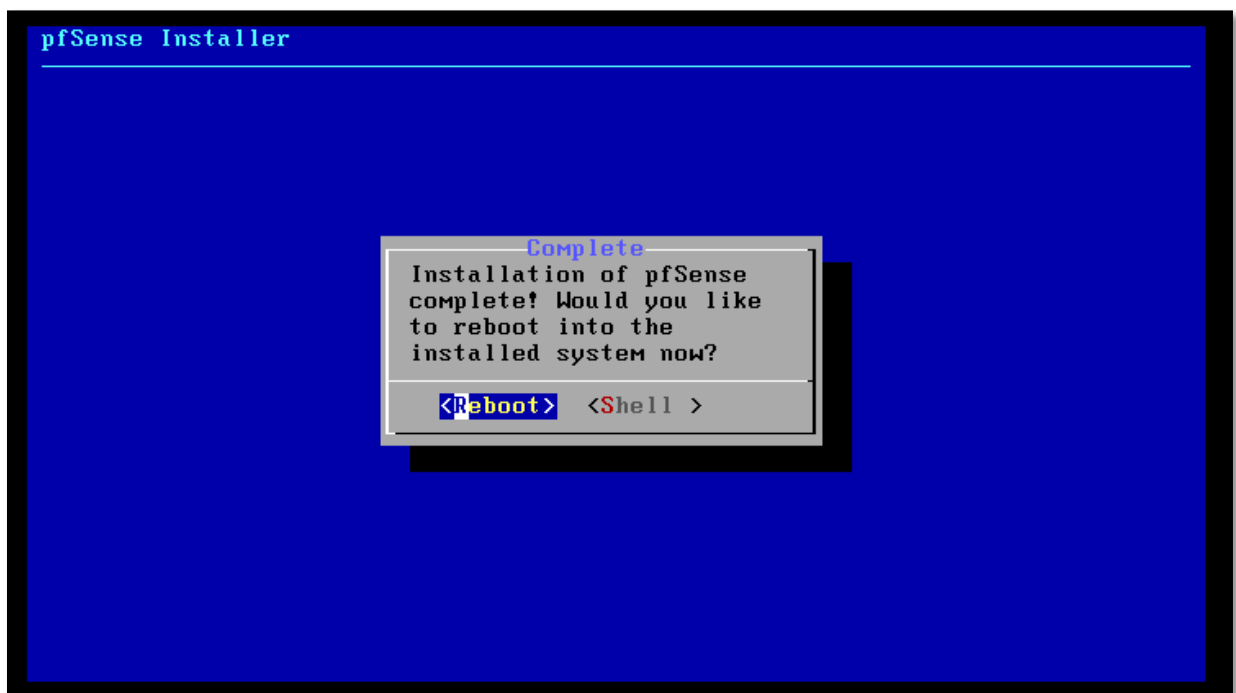


Il vous sera ensuite proposer d'ouvrir un terminal si vous souhaitez apporter des modifications. Passez sur la case « No » et appuyez sur Entrée.



Et pour terminer cette installation du système, appuyez une dernière fois sur Entrée pour reboot.

Attention, vérifiez que vous avez bien enlever l'ISO sinon vous allez devoir reprocéder a l'installation



3) Configuration de PfSense

```
Updating configuration.....done.
Checking config backups consistency...done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...lo0: link state changed to UP
done.
Starting syslog...done.
Starting Secure Shell Services...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Creating wireless clone interfaces...done.
Configuring LAGG interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring IPsec VTI interfaces...done.
Configuring WAN interface...done.
Configuring LAN interface...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Setting up static routes...done.
Setting up DNSs...
Starting DNS Resolver...█
```

Une fois l'initialisation de PfSense terminée cette interface va apparaître.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 20bc68d50f788aeb75b4

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.200.131/24
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: █
```

On voit bien nos deux interfaces réseaux (WAN et LAN).

Vous avez 16 options qui vont permettre de faire différentes actions et configurations. Pour les utiliser, il faut saisir leur numéro et appuyez sur Entrée.

Testons ensemble avec le menu ping. Saisissez au clavier le chiffre 7 puis la touche Entrée.

```
Enter an option: 7

Enter a host name or IP address: █
```

Lançons un ping vers google.fr pour tester l'accès à internet et le bon fonctionnement de la résolution de nom.

```
Enter a host name or IP address: google.fr

PING google.fr (172.217.18.195): 56 data bytes
64 bytes from 172.217.18.195: icmp_seq=0 ttl=128 time=45.646 ms
64 bytes from 172.217.18.195: icmp_seq=1 ttl=128 time=45.635 ms
^C
```

Vous pouvez arrêter le ping en appuyant simultanément sur les touches Ctrl et C. On voit que le ping passe sans problème, l'interface WAN est donc fonctionnelle.

Il faut attribuer une adresse IP à l'interface LAN, celle qui correspond à notre réseau local.

Pour cela, au choix des menus, tapez 2 puis Entrée.

```
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

Enter an option: 2█
```

On me demande quelle interface je veux modifier. L'interface LAN est ici la 2, donc je tape 2 et j'appuie sur Entrée.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
```

Ensuite saisissez l'adresse IP que vous voulez donner au réseau LAN .

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.3.1
```

Définissez le masque de sous-réseau du réseau local, donc 24 dans notre cas.

```
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 31):
> 24
```

Pfsense demande ensuite si le réseau dispose d'une passerelle vers laquelle renvoyer les flux. Ce n'est pas le cas pour moi donc on appuie sur Entrée pour passer

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Je ne souhaite pas configurer d'adresse en IPv6.

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

Je ne souhaite pas non plus activer le service DHCP pour le réseau local donc je saisis « n » pour répondre « no » et Entrée.

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

Et enfin, la dernière question concerne le protocole utilisé pour aller sur l'interface web. Par défaut, il est en HTTPS donc sécurisé. Vous pouvez choisir de le passer en HTTP si vous le souhaitez en répondant « y » pour « Yes ».

```
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) █
```

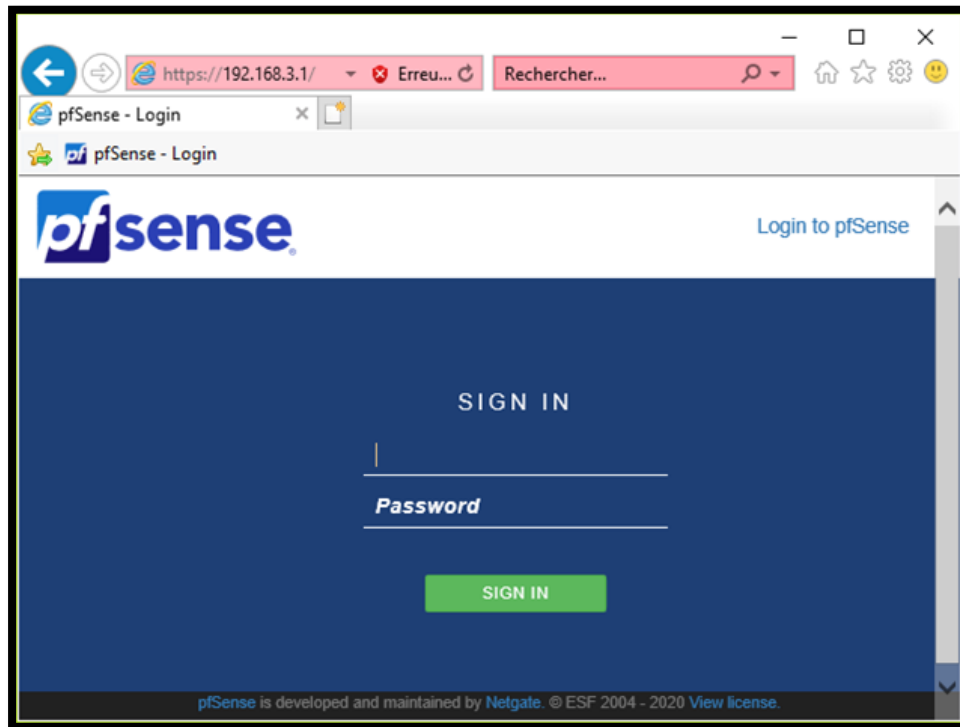
La configuration de l'interface LAN est terminée, on nous donne ici « https://192.168.3.1/ » . Il s'agit de l'url permettant d'accéder a l'interface web.

```
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
  
The IPv4 LAN address has been set to 192.168.3.1/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
                https://192.168.3.1/  
  
Press <ENTER> to continue. █
```

La configuration de pfsense est maintenant terminée, passons sur l'interface web.

4) Configuration de l'interface web

Depuis un PC sur le réseau local, ouvrez un navigateur internet et accédez à votre pfsense.

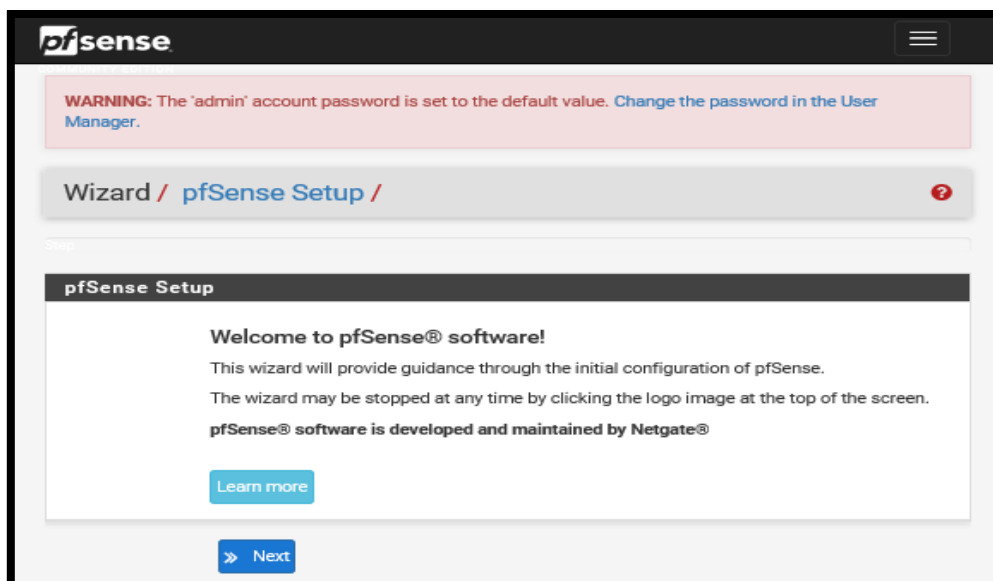


Les identifiants par défaut de pfsense sont les suivants :

Login : admin

Mot de passe : pfsense

Vous arrivez ensuite sur cette page qui va nous permettre de finaliser l'installation de notre firewall. Cliquez sur le bouton « Next ».



Cliquez de nouveau sur Next.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Netgate® Global Support is available 24/7 ?

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise — on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

» Next

Au niveau de la partie des informations générales, vous pouvez modifier le nom du pare-feu et déclarer votre nom de domaine si vous en avez un dans votre réseau. Vous pouvez également déclarer un serveur DNS local.

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

Choisissez « Europe/Paris » dans « Timezone » et continuez.

The screenshot shows the 'Time Server Information' step of the pfSense Setup Wizard. The breadcrumb trail at the top reads 'Wizard / pfSense Setup / Time Server Information'. A progress bar indicates 'Step 3 of 9'. The section title is 'Time Server Information'. Below the title, a message says 'Please enter the time, date and time zone.' There are two input fields: 'Time server hostname' with the value '2.pfsense.pool.ntp.org' and a description 'Enter the hostname (FQDN) of the time server.', and 'Timezone' with a dropdown menu showing 'Europe/Paris'.

Ensuite nous arrivons à la configuration de l'interface WAN qui est configurée automatiquement par DHCP

The screenshot shows the 'Configure WAN Interface' step of the pfSense Setup Wizard. The breadcrumb trail at the top reads 'Wizard / pfSense Setup / Configure WAN Interface'. A progress bar indicates 'Step 4 of 9'. The section title is 'Configure WAN Interface'. Below the title, a message says 'On this screen the Wide Area Network information will be configured.' There is a 'SelectedType' dropdown menu set to 'DHCP'. Below this is a section titled 'General configuration' with three fields: 'MAC Address' (with a description about spoofing), 'MTU' (with a description about setting the MTU), and 'MSS' (with a description about MSS clamping).

Si vous avez besoin d'attribuer une adresse IP statique à cette interface, celle-ci sera définie dans cette partie.

Static IP Configuration	
IP Address	
Subnet Mask	32 v
Upstream Gateway	

DHCP client configuration	
DHCP Hostname	
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).	

La partie « PPPoE configuration » sert en général à mettre les identifiants fournis par votre FAI. Ce sont ces identifiants qui sont définis dans votre box internet actuellement. Si vous souhaitez placer un pare-feu à la place de la box, il sera nécessaire de remplir cette partie.

PPPoE configuration	
PPPoE Username	
PPPoE Password	
Show PPPoE password	☐ Reveal password characters
PPPoE Service name	 Hint: this field can usually be left empty
PPPoE Dial on demand	☐ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPPoE Idle timeout	 If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

La partie suivante « PPTP configuration » servira plutôt au montage d'un VPN point à point

PPTP configuration	
PPTP Username	
PPTP Password	
Show PPTP password	☐ Reveal password characters
PPTP Local IP Address	
pptplocalsubnet	32 v
PPTP Remote IP Address	
PPTP Dial on demand	☐ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout	 If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

Les deux dernières options de cette page définissent tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué.

RFC1918 Networks	
Block RFC1918 Private Networks	☐ Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks	
Block bogon networks	☐ Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

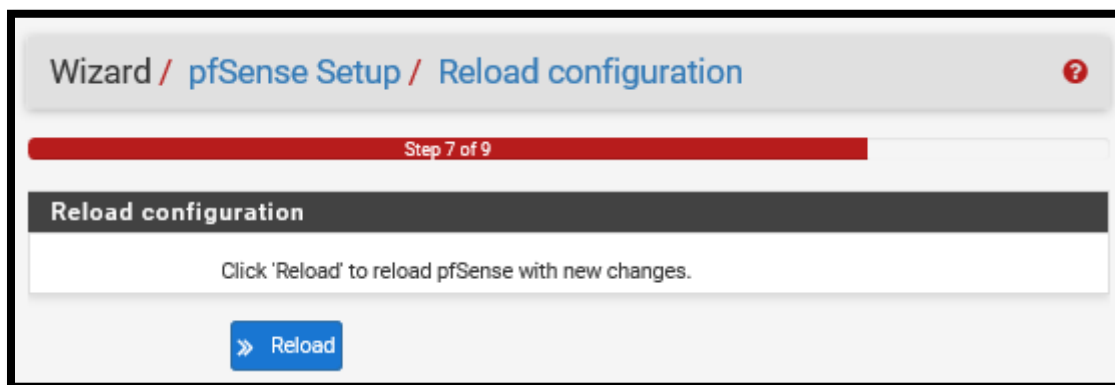
On passe maintenant du côté LAN. Vous pouvez changer ici l'adresse IP de l'interface LAN de pfSense

The screenshot shows the 'Configure LAN Interface' step of the pfSense setup wizard. The breadcrumb trail at the top reads 'Wizard / pfSense Setup / Configure LAN Interface'. A progress bar indicates 'Step 5 of 9'. The title bar says 'Configure LAN Interface'. Below this, a message states: 'On this screen the Local Area Network information will be configured.' There are two input fields: 'LAN IP Address' with the value '192.168.3.1' and a subtext 'Type dhcp if this interface uses DHCP to obtain its IP address.', and 'Subnet Mask' with the value '24' and a dropdown arrow. At the bottom is a blue button labeled '» Next'.

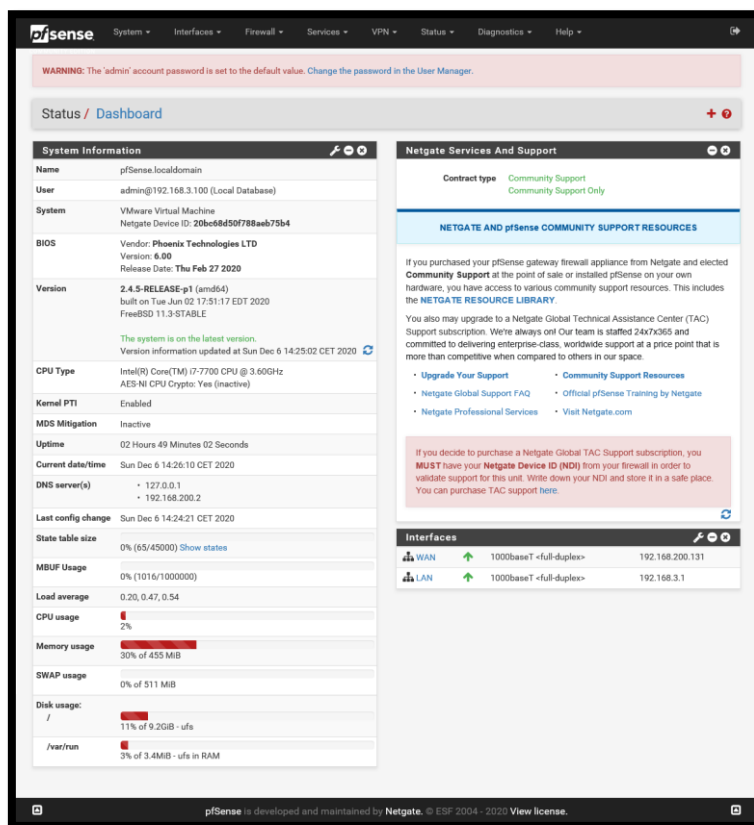
Durant la phase de configuration, il est également nécessaire de changer les identifiants par défaut du compte admin de pfsense.

The screenshot shows the 'Set Admin WebGUI Password' step of the pfSense setup wizard. The breadcrumb trail at the top reads 'Wizard / pfSense Setup / Set Admin WebGUI Password'. A progress bar indicates 'Step 6 of 9'. The title bar says 'Set Admin WebGUI Password'. Below this, a message states: 'On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.' There are two password input fields: 'Admin Password' and 'Admin Password AGAIN', both masked with dots. At the bottom is a blue button labeled '» Next'.

La phase finale de l'installation de » pfSense » est terminée. Cliquez sur « Reload » puis « Finish ».

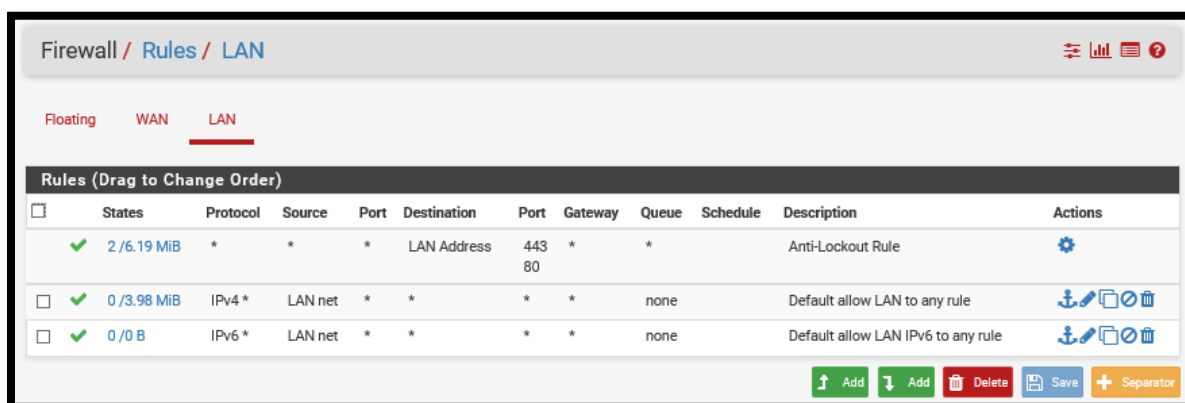


Vous arrivez donc sur le tableau de bord de votre pfSense. Vous retrouvez ici des informations nécessaires.



5) Création de règle

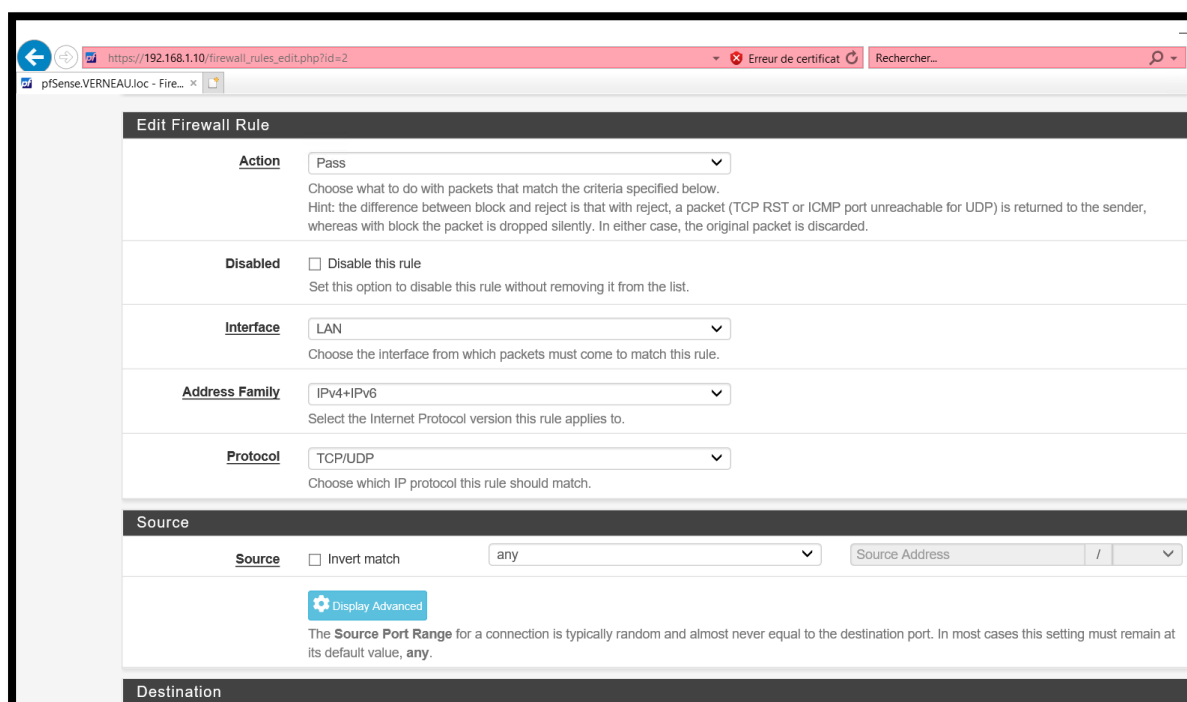
Par défaut lors de son installation, tout est ouvert. On peut voir ceci dans le menu « Firewall », sous-menu « Rules » et partie « LAN ».



Les règles présentes ici définissent que tout le trafic IPv4 et IPv6, tout protocole confondu, venant sur réseau local (LAN Net) sur n'importe quel port et vers n'importe quelle destination est autorisé.

Nous allons remplacer les règles pour accéder à internet et avoir un pare-feu qui est utiliser correctement.

Pour commencer aller l'onglet Firewall et sélectionner « Rules », puis nous allons créer une règle qui autorise la communication avec les sites en HTTPS.



Pour ce faire reproduisez l'image ci-dessus.

Sélectionner votre destination dans notre cas sélectionner HTTPS dans « From et dans To », dans la description vous pouvez renseigner un nom pour votre règle.

The screenshot shows the pfSense Firewall Rule configuration page. The 'Destination' section is expanded, showing 'Destination Port Range' set to 'HTTPS (443)' for both 'From' and 'To' ports. The 'Description' field contains 'HTTPS'. The 'Log' checkbox is unchecked. The 'Advanced Options' section is also visible.

Pour finir cliquez sur « Save », il suffit de faire la même règle pour les sites non sécurisée « http ».

The screenshot shows the pfSense Firewall Rule configuration page. The 'Destination Port Range' section is expanded, showing 'Destination Port Range' set to 'HTTPS (443)' for both 'From' and 'To' ports. The 'Description' field contains 'HTTPS'. The 'Log' checkbox is unchecked. The 'Advanced Options' section is also visible. At the bottom, there is a 'Save' button.

Voilà, vous savez à présent crée une règle de pare-feu.

6) Lexique

FAI = fournisseur d'accès à Internet

WAN = WAN (Wide Area Network, ou réseau étendu)

LAN = LAN ou Local Area Network est un réseau informatique physique et/ou virtuel

PPTP = Protocole de tunnel point-à-point

PPPoE = Point-to-Point Protocol over Ethernet