

Installation de Pfsense

PfSense est un *pare-feu open source faisant également fonction de routeur* appartenant à Rubicon Communications et Netgate. Il est basé sur le système d'exploitation **FreeBSD** issu de la famille d'Unix (*Unix, qui n'est PAS Linux, ne pas confondre ^^*).

La version utilisée dans ce tuto (*et dans la vidéo*) est la **2.7.0**. Vous pouvez vous procurer la dernière version de l'ISO au lien suivant : [pfSense official download](#)



Pour rappel, **un routeur est chargé de faire communiquer différents réseaux entre eux**, comme par exemple, votre réseau local, chez vous, avec le reste du monde, c'est à dire le réseau **Internet**.

Un pare-feu, aussi nommé firewall, est un système de sécurité (*matériel ou logiciel*) qui va **définir et contrôler les flux de données qui sont autorisés à entrer et sortir de votre réseau**. Votre modem fournit par votre fournisseur d'accès à internet est un firewall matériel par exemple. Avec peu de fonction certes, mais c'est tout de même un firewall.

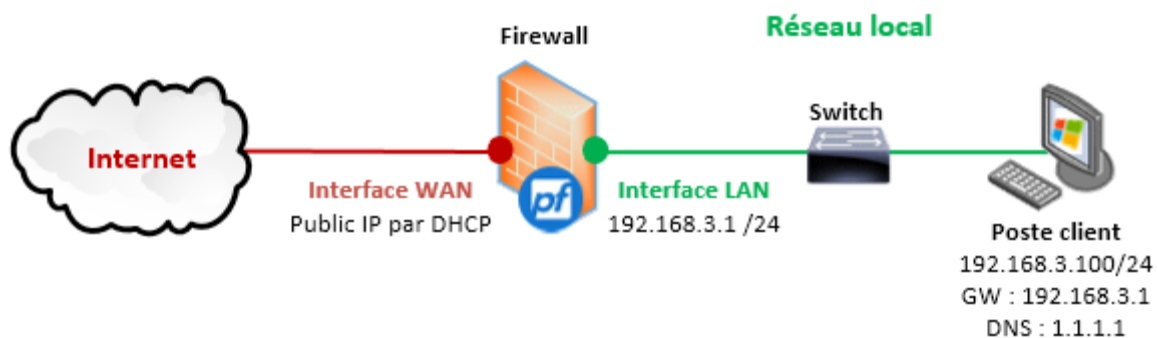
On dit globalement d'un firewall qu'il « **applique la politique de sécurité de l'entreprise** » grâce à des **règles d'actions pour le trafic réseau**. Pour simplifier, il va en fait accepter seulement les types de communications définies dans des règles et rejeter tout ce qui n'est pas explicitement autorisé.



Par exemple, on peut **autoriser aux machines du réseau local les requêtes web sécurisées (HTTPS)**. Si nous n'incluons pas aussi le trafic web non sécurisé (*HTTP*), le firewall va interdire tout ce qui sort en HTTP.

Autre exemple pour rentrer dans le réseau local cette fois-ci : on peut **autoriser les connexions entrantes avec le protocole sécurisé SSH** à destination d'une machine du réseau local, **mais pas les connexions en Telnet** qui lui n'est pas sécurisé.

Voilà pour ces courtes explications sur les firewalls ! Comme toujours avant de commencer, petit topo sur l'infrastructure virtuelle utilisée dans ce tuto ! Voici un **schéma de l'infrastructure que l'on va faire** :



Pfsense s'utilise via une interface web, il faut donc disposer d'un poste client avec un navigateur web et ayant une **adresse IP dans le même réseau local que lui**. J'ai donc une VM cliente sous Windows 10 avec une installation classique pour pouvoir accéder à pfsense par la suite et une seconde VM qui sera mon firewall.

Au niveau de la configuration de la VM pfsense, elle est assez légère (*réalisé sous VMWare Workstation*) :

▼ Devices	
Memory	1 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file E:\ISO\...
Network Adapter	NAT
Network Adapter 2	Custom (VMnet3)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

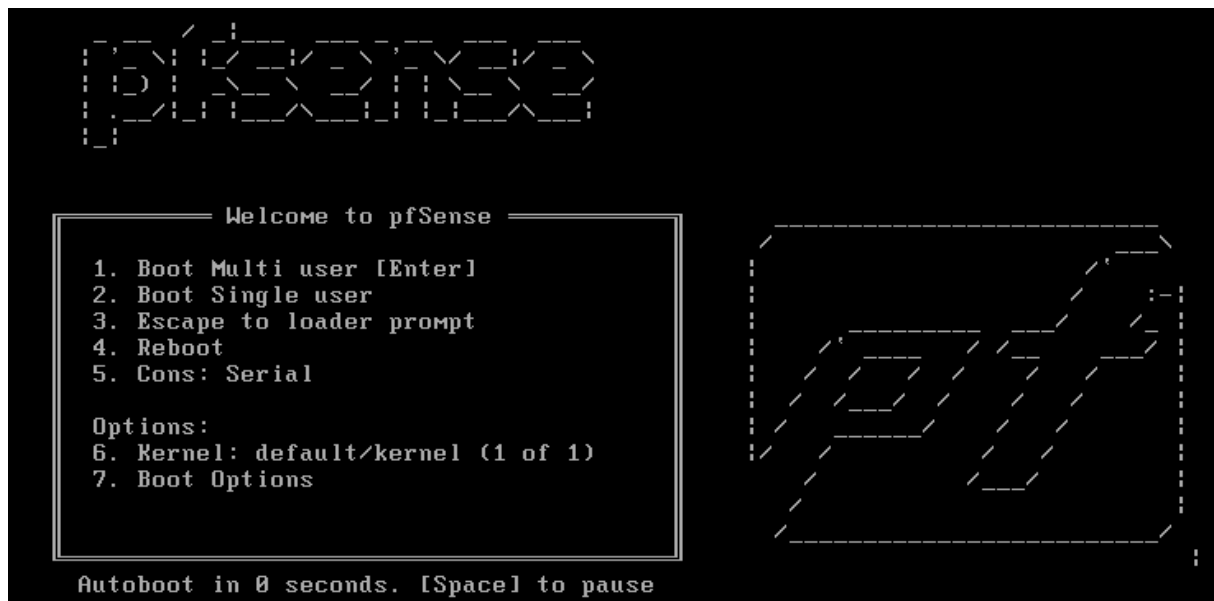
Info + : Pas besoin d'une grosse configuration matérielle, ce qui est recommandé officiellement est d'ailleurs très léger, vous pouvez donc mettre le minimum requis : [Minimum Hardware Requirements](#)

En revanche, pfsense agissant comme un routeur, **il est impératif d'avoir au moins 2 cartes réseaux, sur 2 réseaux différents** : le réseau WAN (*Internet*) et le réseau LAN (*local*). La première carte va correspondre à l'interface WAN de pfsense, **elle a été positionnée en NAT** et la seconde sera l'interface LAN, elle est ici positionnée dans un **réseau privé (vmnet3)**.

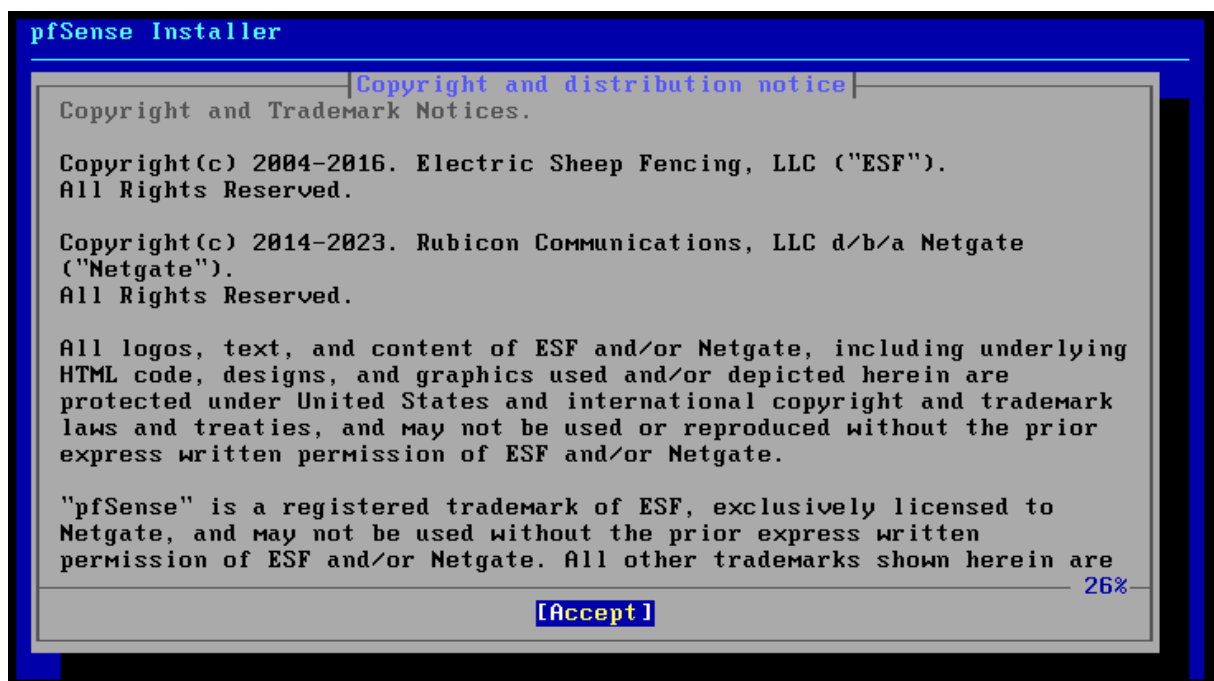
Une fois vos 2 machines virtuelles prêtes, vous pouvez vous lancer dans ce tuto ! 🙌

Info ++ : La version de pfsense utilisée dans ce tuto est la 2.7.0. Il sera peut être nécessaire de s'adapter selon la version utilisée.

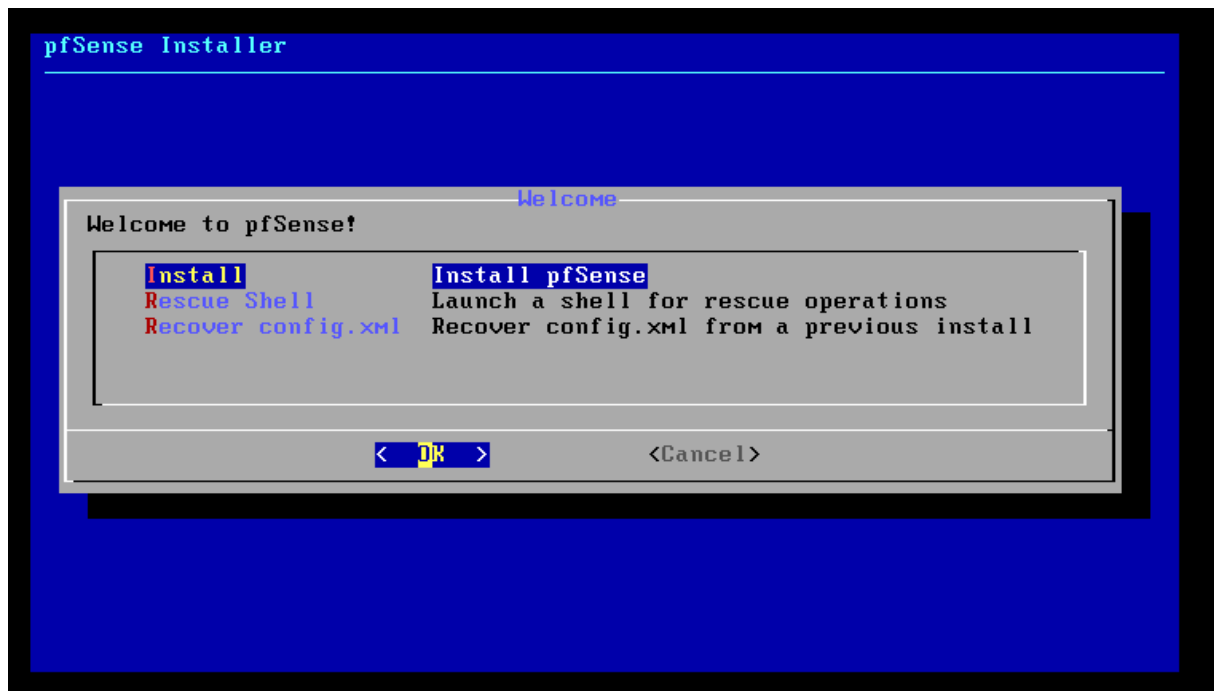
Commençons tout de suite par **installer pfsense**. Après avoir insérer l'ISO de pfsense dans VM dédiée, vous pouvez démarrer la machine. Le setup va démarrer automatiquement après quelques secondes .



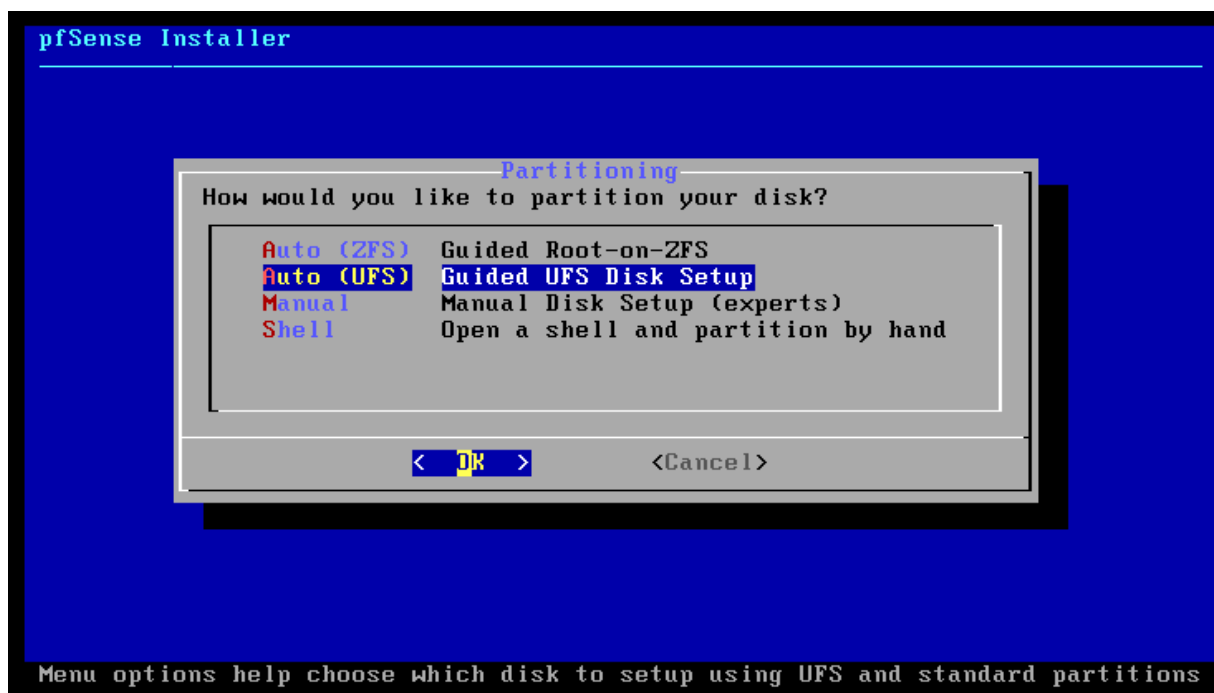
L'installation va s'effectuer au clavier. Appuyez sur la touche Entrée pour Accepter.



Vérifiez que vous êtes bien sur « Install » (doit être sélectionné en bleu foncé comme dans l'image ci-dessous, sinon déplacez vous avec les flèches de votre clavier) et appuyez sur Entrée pour faire OK.



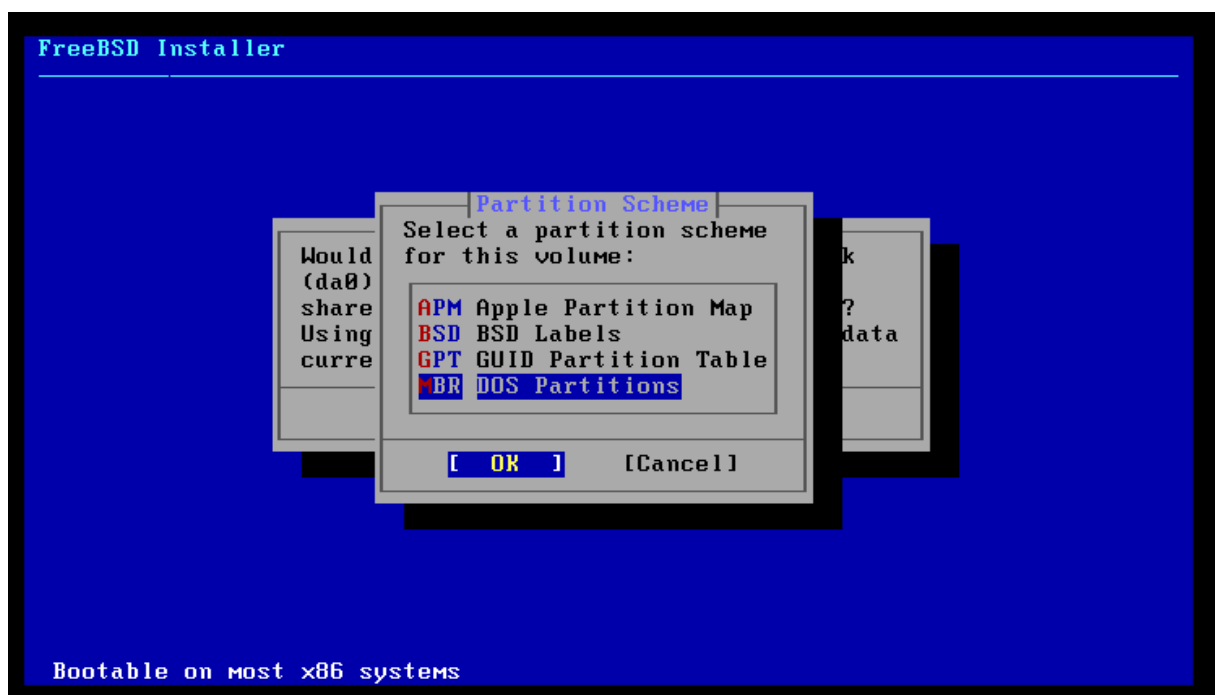
Le setup va vous demander de **partitionner le disque** de stockage de la machine. Avec les touches fléchées de votre clavier, allez sur « **Auto (UFS)** » et appuyez sur Entrée.



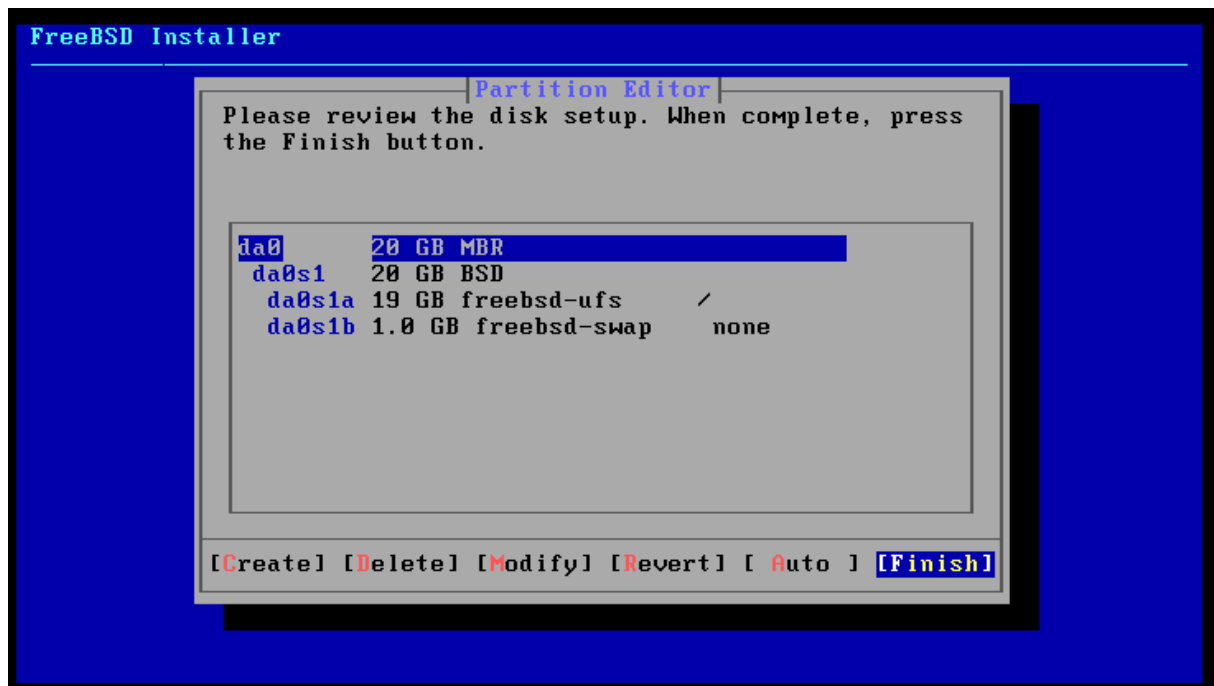
Vous pouvez confirmer que vous voulez utiliser le disque entier pour installer le système d'exploitation, pour cela, placez vous sur « **Entire Disk** » et appuyez sur Entrée.



Selon vos besoins (*nécessite des connaissances pouvez en partitionnement !*), sélectionnez le type de partition. Ici je reste simplement sur « **MBR DOS Partitions** » et appuyez sur Entrée pour valider.



L'installer propose un découpage sur le disque 0 (*nommé ici da0*), je n'ai pas besoin de modifier la proposition faites, placez vous sur « **Finish** » et appuyez sur Entrée.



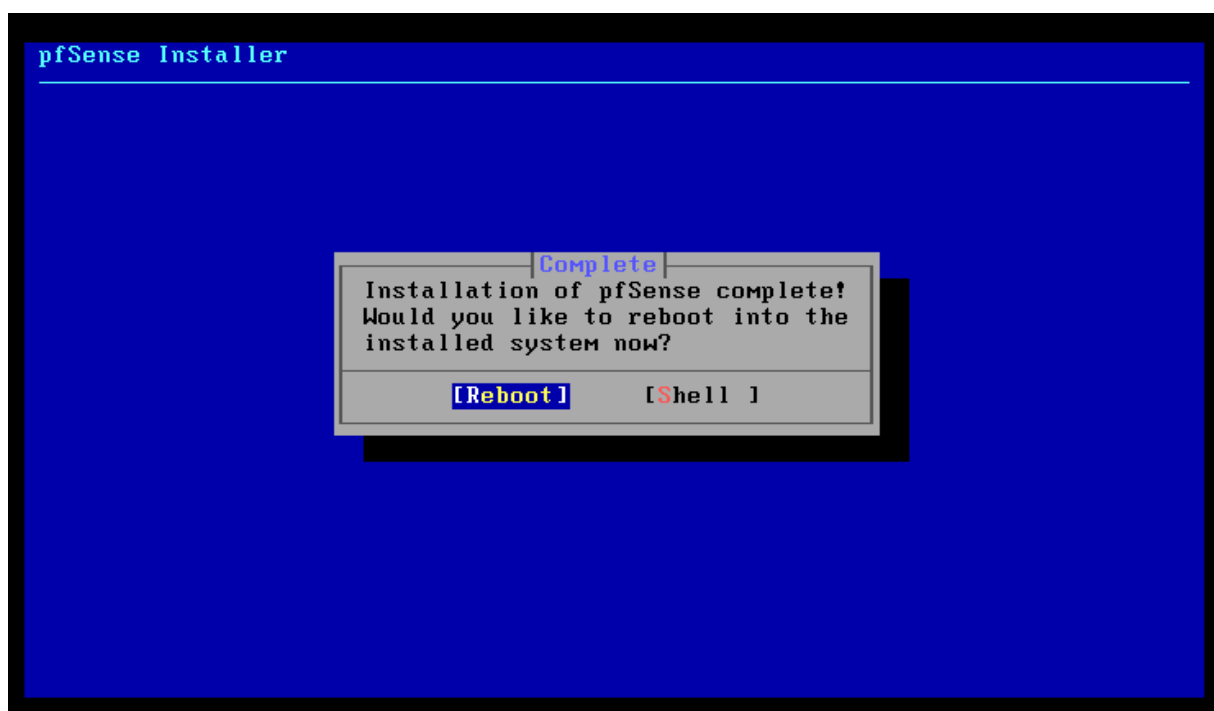
Un ultime avertissement sur le fait que le disque sera effacé pour faire face au système d'exploitation de pfsense. Placez vous sur « **Commit** » et appuyez sur Entrée.



L'installation est désormais lancée. **Patiencez quelques secondes**, c'est très rapide.



Il vous sera ensuite proposer d'ouvrir un shell (*terminal*) si vous souhaitez apporter des modifications. Sinon, placez vous directement sur « **Reboot** » et appuyez sur Entrée.



Au démarrage, **pfSense va se lancer, tester et configurer les services dont il a besoin**. Par exemples dans l'image ci-dessous, on peut voir que pfSense a testé la présence de l'interface WAN (*ligne Configuring WAN interface...done.*) et l'a configuré, idem pour l'interface LAN. Il a également lancé le service DNS pour la résolution de nom de domaine (*ligne Configuring DNS Resolver...*).

```

Starting device manager (devd)...2023-08-14T16:36:43.739744+00:00 - php-fpm 372
- - /rc.linkup: DHCP Client not running on wan (em0), reconfiguring dhclient.
2023-08-14T16:36:43.768898+00:00 - php-fpm 371 - - /rc.linkup: Ignoring link eve
nt during boot sequence.
done.
Loading configuration....done.
Updating configuration.....Migrating System Memory RRD file to new format
.done.
Checking config backups consistency...done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting syslog...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Configuring LAN interface...done.
Configuring WAN 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 que le démarrage est finalisé, vous aurez la vue suivante sur la machine :

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: a86f287011fe9e1cd7a2

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.128.0.1/8
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). On voit également que **l'interface WAN a bien récupéré une adresse IP automatiquement depuis un DHCP** (ce qui peut correspondre à l'IP publique par exemple). Concernant le LAN, il attribue une adresse statique par défaut qui est 192.168.1.1 mais que nous allons changer.

Vous avez **16 menus** 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: google.fr
```

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

Info ++ : Attention, le clavier est par défaut en qwerty ! Pour saisir le point, il faut appuyez sur la touche « / ».

```
PING google.fr (142.250.179.99): 56 data bytes
64 bytes from 142.250.179.99: icmp_seq=0 ttl=128 time=8.129 ms
64 bytes from 142.250.179.99: icmp_seq=1 ttl=128 time=9.790 ms
64 bytes from 142.250.179.99: icmp_seq=2 ttl=128 time=8.825 ms

--- google.fr ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 8.129/8.915/9.790/0.681 ms

Press ENTER to continue.
```

On voit que le ping passe sans problème, l'interface WAN est donc fonctionnelle.

Nous avons une dernière petite chose à faire avant de passer sur l'interface web de pfsense pour la configuration finale. Il faut **assigner la bonne adresse IP à l'interface LAN**, c'est-à-dire celle qui correspond à notre réseau local (*pour moi dans le cadre de ce tuto, 192.168.3.1*).

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
```

La 1ère question posée concernant l'attribution d'une IP à l'interface LAN via un DHCP. Je veux l'attribuer manuellement, saisissez « n » **pour répondre Non** et appuyez sur Entrée.

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
```

Ensuite saisissez l'adresse IP que vous donnez à cette interface qui sera je le rappelle la **passerelle de sortie de votre réseau local**. Quand vous avez saisi l'adresse IP, appuyez sur Entrée pour passer à la suite.

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

Définissez le masque de sous-réseau du réseau local **en notation CIDR uniquement**, donc 24 pour moi.

```
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
```

Pfsense demande ensuite si le réseau dispose d'une passerelle vers laquelle renvoyer les flux. Ce n'est pas le cas pour moi, l'interface WAN fait déjà le job et je n'ai pas d'autre routeur dans mon réseau donc j'appuie simplement sur **Entrée pour laisser vide**.

```
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, je réponds donc « n » c'est à dire **non** pour la question concernant le DHCP et j'appuie **ensuite sur Entrée** quand il demande de définir une IPv6 **pour ignorer cette partie**.

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n  
  
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 encore une fois Non et Entrée**.

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

Info + : le service DHCP peut être activé et configuré plus simplement par la suite via l'interface web.

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 ». Personnellement je vais répondre « n ».

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

La configuration de l'interface LAN est terminée. Je vois à l'écran l'**URL à utiliser pour aller sur pfsense qui est donc ici https://192.168.3.1/**, soit son adresse IP.

```
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

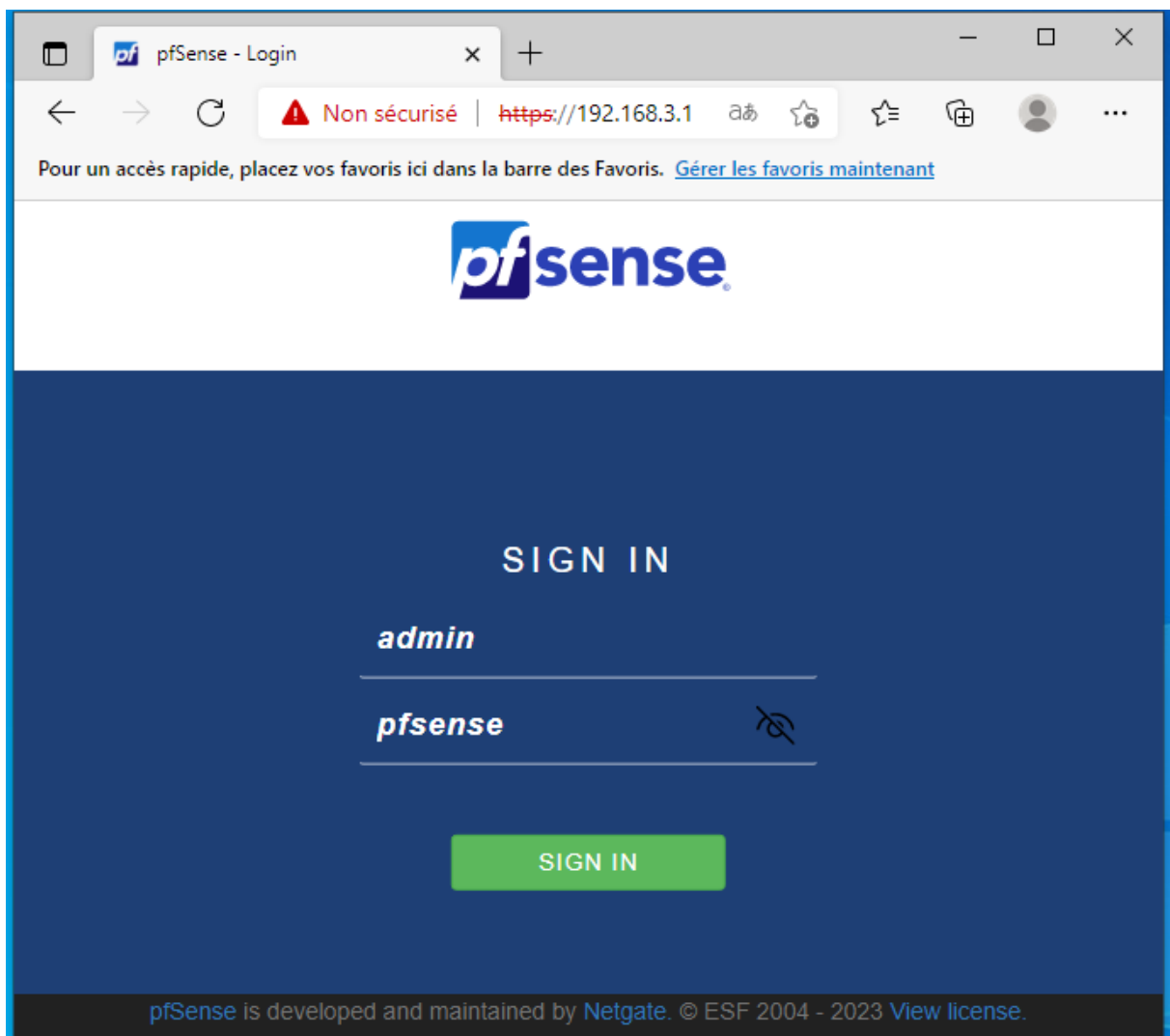
The IPv4 LAN address has been set to 192.168.3.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:

        https://192.168.3.1/

Press <ENTER> to continue. █
```

La configuration de pfsense en **lignes de commande** est maintenant terminée, passons sur l'interface web.

Depuis un PC sur le réseau local disposant d'une adresse IP fixe si le DHCP n'est pas actif, **ouvrez un navigateur internet et accédez à votre pfsense.**

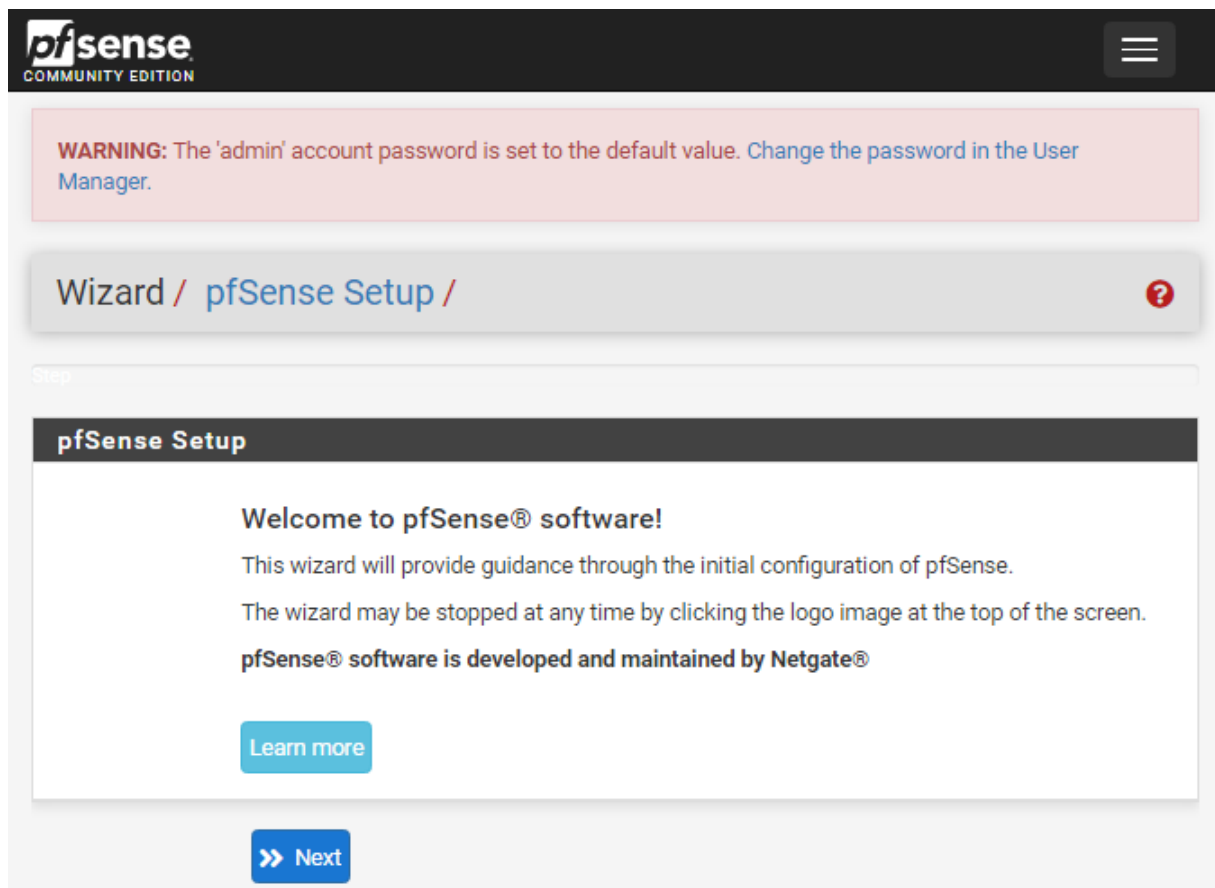


***Info ++ :** Si vous avez laissé le protocole HTTPS, vous aurez une erreur de certificat qui est tout à fait normal. Le navigateur va vous prévenir qu'il y a un problème mais rien ne vous empêche de poursuivre votre navigation (méthode variable navigateur) pour accéder à pfsense.*

Les **identifiants par défaut de pfsense** sont les suivants :

- - **Login** : admin
 - **Mot de passe** : pfsense

Vous arrivez sur l'**assistant de configuration** de pfsense qui va nous permettre de finaliser l'installation de notre firewall. Cliquez sur le bouton « **Next** ».



L'assistant nous informe qu'il est possible d'avoir un **support technique sous condition de souscrire un contrat** (un peu de pub pour la solution payante au passage 🗿). 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 firewall** et déclarer votre **nom de domaine si vous en avez un** dans votre réseau. Ici également vous pouvez **déclarer un serveur DNS local** (*ce n'est pas mon cas, j'utilise le DNS public de CloudFlare pour ce tuto*). Je ne modifie ici aucun champ.

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

Wizard / pfSense Setup / General Information



Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

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

>> Next

Choisissez « **Europe/Paris** » dans la **Timezone** et poursuivez.

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

Wizard / [pfSense Setup](#) / [Time Server Information](#)



Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server
hostname

Enter the hostname (FQDN) of the time server.

Timezone



» Next

Ensuite nous arrivons à la configuration de l'**interface WAN**. Elle est **configurée automatiquement par DHCP** donc **je ne vais rien toucher** dans la partie supérieure de cette page.

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

Wizard / [pfSense Setup](#) / [Configure WAN Interface](#)

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

General configuration

MAC Address	<input type="text"/>
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.	
MTU	<input type="text"/>
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.	
MSS	<input type="text"/>
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.	

Si vous avez besoin d'attribuer une IP fixe à cette interface WAN, c'est dans cette partie que ça se définit, sinon, continuez simplement.

Static IP Configuration

IP Address

Subnet Mask

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 firewall à la place de la box, il sera nécessaire de remplir cette partie.

PPPoE configuration	
PPPoE Username	<input type="text"/>
PPPoE Password	<input type="password"/>
Show PPPoE password	<input type="checkbox"/> Reveal password characters
PPPoE Service name	<input type="text"/> Hint: this field can usually be left empty
PPPoE Dial on demand	<input type="checkbox"/> 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	<input type="text"/> 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** (*Protocole de tunnel point-à-point, à éviter car peu sécurisé, plutôt privilégier son petit frère IPSEC*).

PPTP configuration	
PPTP Username	<input type="text"/>
PPTP Password	<input type="password"/>
Show PPTP password	<input type="checkbox"/> Reveal password characters
PPTP Local IP Address	<input type="text"/>
pptplocalsubnet	<input type="text" value="32"/> ▼
PPTP Remote IP Address	<input type="text"/>
PPTP Dial on demand	<input type="checkbox"/> 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	<input type="text"/> 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 que tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué. **Comme mon infra est ici virtuelle, je vais obligatoirement faire communiquer des réseaux privés, je n'utilise pas réellement une adresse publique.** Il est donc **nécessaire dans le cadre d'un labo de décocher ces 2 cases** sinon vous pourriez avoir des petits couacs.

RFC1918 Networks	
Block RFC1918 Private Networks	<input type="checkbox"/> 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	<input type="checkbox"/> 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.

» Next

Nous n'avons donc rien modifier de spécial sur notre interface WAN ici, vous pouvez poursuivre.

L'assistant de pfsense passe donc cette fois-ci à l'**interface côté LAN**. Vous pouvez changer ici l'adresse IP de l'interface LAN de pfSense (*nous l'avons déjà fait en amont*).

The screenshot shows the pfSense Community Edition web interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb navigation reads "Wizard / pfSense Setup / Configure LAN Interface". A progress bar indicates "Step 5 of 9". The main section is titled "Configure LAN Interface" and contains the instruction: "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". A blue "Next" button is at the bottom.

pfSense
COMMUNITY EDITION

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

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface


On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.3.1
Type dhcp if this interface uses DHCP to obtain its IP address.


Subnet Mask: 24

Next


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



COMMUNITY EDITION



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

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password


On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password


Admin Password AGAIN


>> Next

La phase finale de l'installation de pfsense est terminée. Cliquez sur Reload pour recharger pfsense.



COMMUNITY EDITION



Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

Patientez quelques secondes, la page va se recharger d'elle même.

Wizard / pfSense Setup / Reload in progress



Step 8 of 9

Reload in progress

A reload is now in progress. Please wait.

The wizard will redirect to the next step once the reload is completed.

A la fenêtre suivante, cliquez sur le bouton **Finish**.

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Cliquez sur le bouton **Accept** pour valider les points législatifs divers (*que personne ne lit jamais...*).

Regulatory/Export Compliance.

The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Accept

Dernière petite fenêtre de la part de Netgate qui vous invite à répondre à un sondage sur ses produits. Cliquez sur le bouton **Close** pour passer.

Thank you!

Netgate, as well as many community members, work hard to make pfSense CE software an excellent secure networking solution. As well, Netgate strives to deliver even greater value through our product, pfSense Plus software.

Would you take a moment to answer this brief (and anonymous) survey to help us guide those efforts?.

[User survey](#)

Close

Vous arrivez donc sur le **tableau de bord de votre pfsense**. Vous retrouvez ici des **infos sur l'utilisation des ressources de la machine** elle-même, ses **différentes adresses IP**, sa **version** et ses **mise à jour** si nécessaire etc...

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.3.100 (Local Database)
System	VMware Virtual Machine Netgate Device ID: a86f287011fe9e1cd7a2
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Mon Aug 14 16:37:26 CEST 2023
CPU Type	13th Gen Intel(R) Core(TM) i5-13400 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 20 Minutes 57 Seconds
Current date/time	Mon Aug 14 16:57:26 CEST 2023
DNS server(s)	<ul style="list-style-type: none"> 127.0.0.1 10.0.0.2
Last config change	Mon Aug 14 16:54:36 CEST 2023
State table size	0% (12/96000) Show states
MBUF Usage	0% (3556/1000000)
Load average	0.19, 0.24, 0.23
CPU usage	1%
Memory usage	27% of 960 MiB
SWAP usage	0% of 1023 MiB

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 Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

Interfaces

WAN	↑	1000baseT <full-duplex>	10.128.0.1
LAN	↑	1000baseT <full-duplex>	192.168.3.1

Disks

Mount	Used	Size	Usage
> /	1.3G	18G	8% of 18G (ufs)

Cette **vue est personnalisable** est cliquant sur le **petit + en haut à droite** dans la barre de titre.

Status / Dashboard

Available Widgets

+ Captive Portal Status

+ Interface Statistics

+ OpenVPN

+ Services Status

+ Wake-on-Lan

+ CARP Status

+ Gateways

+ Interfaces

+ Picture

+ System Information

+ Dynamic DNS Status

+ GEOM Mirror Status

+ IPsec

+ RSS

+ Thermal Sensors

+ Firewall Logs

+ Installed Packages

+ NTP Status

+ S.M.A.R.T. Status

+ Traffic Graphs

Other dashboard settings are available from the [General Setup](#) page.

Vous pouvez ajouter des graphiques, des infos sur les load balancer, le trafic, les logs, les VPN etc...

Les **différents menus** vont vous permettre de faire toutes sortes de choses sur votre firewall.

- - Mettre en place des VPN (*IPSEC, OpenVPN...*)
 - Activer des services (*DHCP, DNS, NLB, NTP, WOL...*)
 - Faire du NAT et du port forwarding
 - Ajouter des routes
 - Définir des règles pour le trafic entrant/sortant
 - Surveiller précisément ce même trafic
 - Ajouter des plugins qui vont apporter d'autres fonctionnalités (*filtrage Squidguard ou monitoring réseau avec Ntopng par exemples*)
- ...

Info + : Pour modifier la langue de pfsense, allez dans le menu System et General Setup.

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

Firewall / Rules / LAN

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"/>	1/1.55 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1/31.57 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

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.**

D'ailleurs si vous avez correctement suivi ce tuto et que depuis le PC client vous faites un ping vers google.fr, le ping va bien aboutir, preuve en est que le trafic peut sortir sans intervention de votre part.

Il est plus que conseillé de brider ce trafic pour n'autoriser que les protocoles/port nécessaires. Le but d'un firewall étant de sécuriser ce qui entre et sort de son réseau, si c'est porte ouverte, il n'y a pas vraiment d'intérêt...