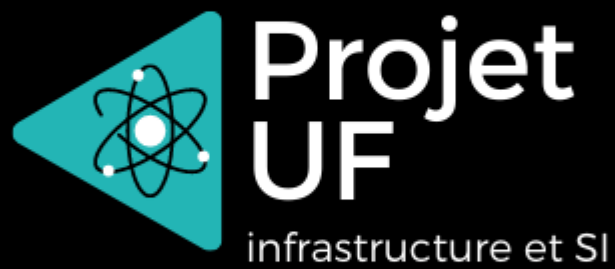


# Compte rendus projet UF



RODRIGUES Cyril

MOUNIER Matthieu

LANDO Anthony

Bachelor 1 Informatique

# SOMMAIRE

I-	Contexte du projet .....	Page 3
II-	Documents attendus .....	Page 3-4
III-	L'architecture réseau proposer .....	Page 4-7
IV-	Documentation Pfsense .....	Page 7-24
V-	Documentation Serveur web .....	Page 24-27
VI-	Documentation back-up .....	Page 27-31
VII-	Annexe .....	Page 31

## I- Contexte du projet

L'objectif de ce projet est de répondre à la demande d'un client possédant une petite entreprise (TPE), qui souhaite mettre en place une architecture réseau pour son entreprise avec certaines contraintes de communication entre les machines mais aussi une liste de machines imposées dont l'entreprise dispose.

Le client souhaite une architecture qui comprend :

- Un client Linux
- Un client Windows
- Un serveur Web
- Un serveur de Back-up du serveur Web
- Un pare-feu (à choisir)

Les contraintes de communications entre les machines :

- L'accès au serveur Web doit être possible depuis le réseau local (intérieur) mais aussi le réseau internet (extérieur).
- L'accès au serveur de back-up doit se faire uniquement depuis le réseau LAN.

## II- Documents attendus

Schéma de l'architecture

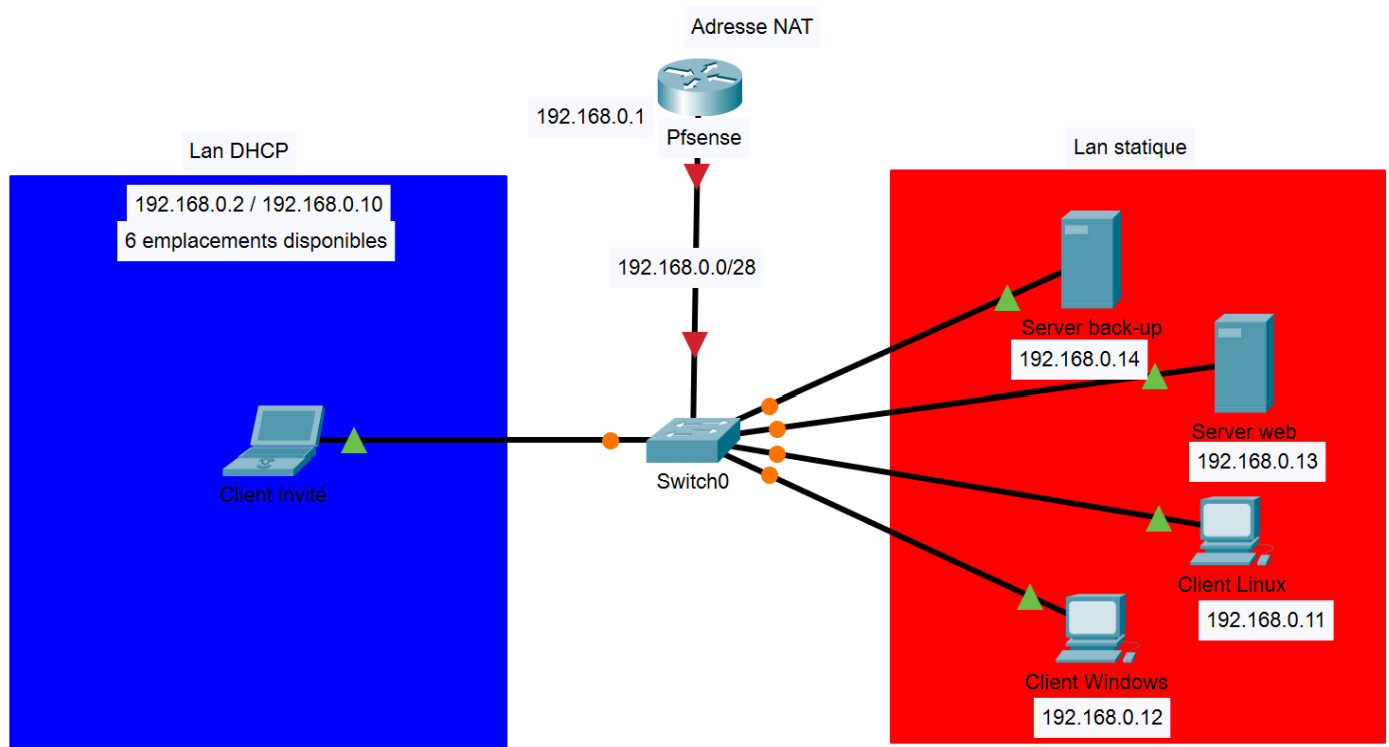


Table d'adressage

Périphérique	Adresse IP	CIDR	Masque réseau	Passerelles
Pfsense (LAN)	192.168.0.1	/28	255.255.255.240	///
Client Linux	192.168.0.11	/28	255.255.255.240	192.168.0.1
Client Windows	192.168.0.12	/28	255.255.255.240	
Serveur web	192.168.0.13	/28	255.255.255.240	
Serveur back-up	192.168.0.14	/28	255.255.255.240	
Serveur DHCP	192.168.0.2 / 192.168.0.10	/28	255.255.255.240	
IP Broadcaste	192.168.0.15	/28	255.255.255.240	///

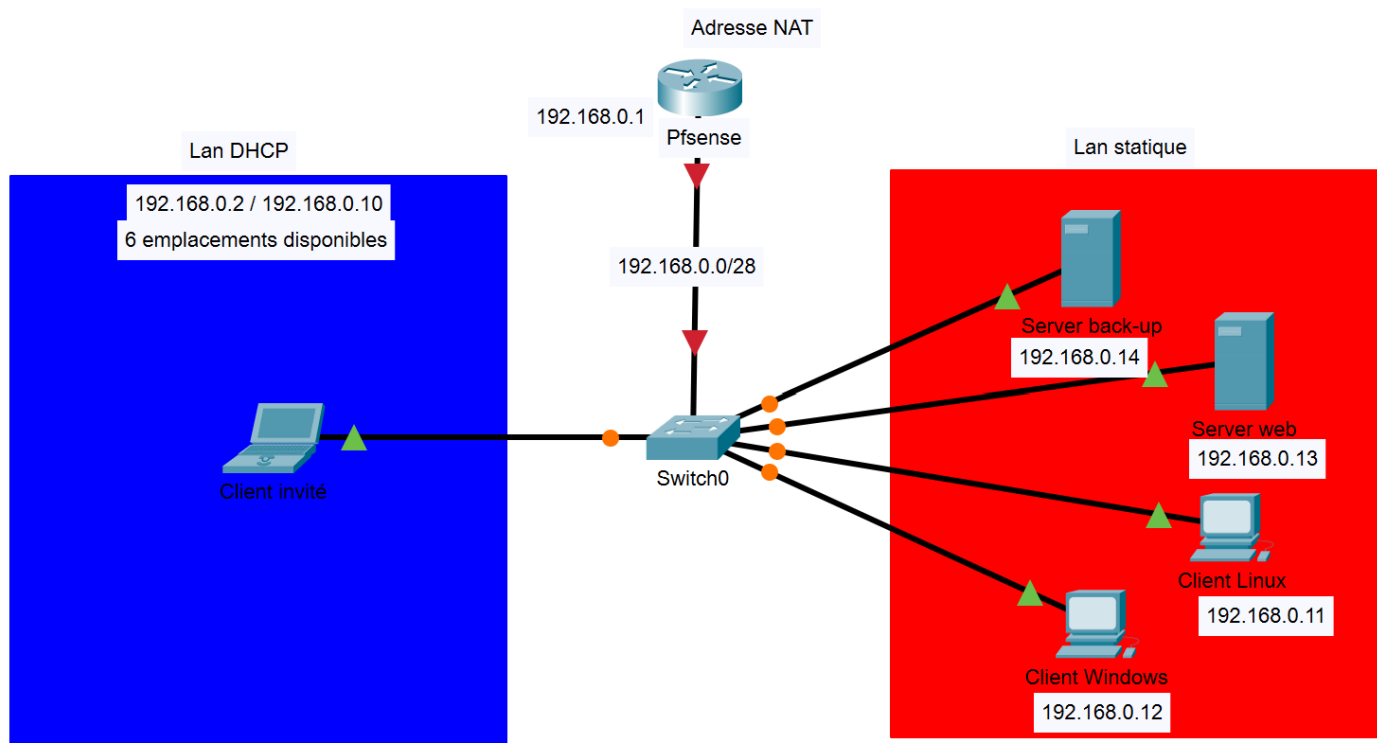
Table de filtrage

Action	Protocole	IP source	Port d'origine	IP destination	Port destination
LAN					
Pass	UDP	LAN net	*	*	53
Pass	TCP/UDP	LAN net	*	*	80
Pass	TCP/UDP	LAN net	*	*	443
Block	*	*	*	*	*
WAN					
Pass	TCP	WAN adresse	85	192.168.0.13	80
Block	*	*	*	*	*

### III- L'architecture réseau proposer

Pour arriver à cette issue nous avons premièrement tiré quelques contraintes à partir du sujet. Comme le commanditaire est un professionnel il faut que la solution que nous lui apportons respect plusieurs notions importantes : **fiabilité, flexibilité, évolutivité** mais aussi également **faible coût** puisque c'est une petite entreprise. Ces quatre notions ont été notre fil rouge pour développer la solution que nous avons retenue.

Nous avons choisi de mettre en place **une architecture complètement virtualisée** pour répondre à la question du **faible coût** mais cependant la configuration peut être mise sur des machines physiques de la même manier, mais cela s'accompagne de coût supplémentaire et quelques petits changements (mise en place d'un réseau local filaire). Nous avons divisé en **deux sous-réseaux** le LAN (local). **Un réseau avec un serveur DHCP** qui s'occupe dynamiquement d'attribuer à l'utilisateur une adresse IP, la passerelle, le serveur DNS.... ce qui illustre la **notion flexibilité**. Puis **un réseau statique** composé des machines du client qui sont présents sur le lieu de l'entreprise ces machines procède des adresses IP statiques unique à chaque machine qui sont configurés manuellement sur chaque poste. Pour **contrôler le flux des connexions et router les connexions** dans l'objectif de sécuriser l'architecture réseau de l'entreprise nous avons choisi **d'utiliser le router / pare-feu** qui se nomme **Pfsense** qui sera le de liaison entre le WAN (internet) et le LAN (réseau local).



Comme nous pouvons le voir le réseau est séparé en deux partis : **en bleu le LAN DHCP** ainsi qu'en **rouge le LAN statique**. Le LAN statique est mis en place **respectant les bonnes pratiques** : renommer les machines, des IP fixes, activations des pare-feu des machines, changement de navigateur web pour Firefox... ce qui permet de rendre **le réseau statique le plus fiable possible**.

Pour le réseau local de l'entreprise nous avons choisi l'adresse **IP réseau suivante 192.168.0.0 avec un CIDR de 28** à fin de réduire le nombre d'adresses IP disponibles, tout en gardant une certaine marge d'adresses disponible pour laisser la possibilité à l'entreprise de continuer son expansion et sa croissance sans impacter les intervenants de l'entreprise. Un CIDR de 28 nous permet d'acquérir 14 adresses IP pour notre réseau local qui sont réparti entre les machines, plus de détails dans la table d'adressage ci-dessous :

Périphérique	Adresse IP	CIDR	Masque réseau	Passerelles
Pfsense (LAN)	192.168.0.1	/28	255.255.255.240	///
Client Linux	192.168.0.11	/28	255.255.255.240	192.168.0.1
Client Windows	192.168.0.12	/28	255.255.255.240	
Serveur web	192.168.0.13	/28	255.255.255.240	
Serveur back-up	192.168.0.14	/28	255.255.255.240	
Serveur DHCP	192.168.0.2 / 192.168.0.10	/28	255.255.255.240	
IP Broadcaste	192.168.0.15	/28	255.255.255.240	///

Le serveur DHCP peut attribuer 9 adresses IP de façon automatiquement aux machines qui viendraient se rajouter au réseau local, pour un délai interminé ou bien provisoire. Avec une plage d'IP allant de 192.168.0.2 jusqu'à 192.168.0.10.

Pfsense est configuré de manier à servir de pare-feu mais également de router, par conséquent il est paramétré avec **deux cartes réseaux** : une première carte pour le **LAN placer en mode LAN-segment** (comparable à un réseau filaire en RJ45) puis enfin seconde carte pour le **WAN placer en mode NAT** qui récupère l'adresse IP de la machine pour s'attribuer une adresse.

Le pare-feu est configuré pour **autoriser seulement les intervenants de l'entreprise** connecter sur le réseau à utiliser uniquement le protocole TCP/UDP sur le port http (80) ou bien https (443) à destination du LAN et WAN soit uniquement **à surf sur internet mais également à utiliser des serveurs DNS** avec le port DNS (53). Pour des raisons de sécurité nous avons désactivé tous les autres flux pour la partie LAN. En ce qui concerne la partie WAN nous avons uniquement autorisé le flux qui provient depuis l'IP WAN de pfsense (WAN adresse) sur le port 85 à destination de l'adresse IP du serveur WEB (192.168.0.13) sur le port 80. Voici la table de filtrage qui résume toutes les règles d'action configure sur le pare-feu :

Action	Protocole	IP source	Port d'origine	IP destination	Port destination
LAN					
Pass	UDP	LAN net	*	*	DNS (53)
Pass	TCP/UDP	LAN net	*	*	HTTP (80)
Pass	TCP/UDP	LAN net	*	*	HTTPS (443)
Block	*	*	*	*	*
WAN					
Pass	TCP	WAN adresse	85	192.168.0.13	HTTP (80)
Block	*	*	*	*	*

Par la suite **pour rendre notre serveur WEB accessible depuis le LAN mais également le WAN** nous configuré une règle de redirection de port (NAT) qui redirige le flux grâce au port source, **on effectue ce que l'on nomme une translation de port**. Pour cela nous avons redirigé le flux vers l'IP 192.168.0.13 (serveur WEB) sur le port HTTP lorsque nous pointons sur l'adresse IP WAN de pfsense sur le port 85, ce qui rend le serveur WEB accessible depuis le WAN.

**Pour des raisons de sécurité très importante le mot de passe par défaut du compte admin doit être changé.**

Toute les configurations citées ci-dessus sont toutes détailler dans la partie « Documentation PFSense » qui montre comment mettre en place chacune de ces configurations.

**Pour le serveur** on s'est tournée sur **apache** car il tourne sur linux et est facile à configurer. Il nous permet de mettre en place un site web http. Apache est open source, c'est à dire que c'est gratuit donc en raccord avec le fais que ce soit **flexible et à faible coût**. On fait tourner apache sur une machine virtuelle qui tourne sous Linux .

**Apache** est fait pour fournir **un serveur sécuriser, efficace et extensible** qui fournit des services HTTP avec les normes HTTP actuel. Pour tout ce qui est technique est installation se référer à la partie « **Documentation Serveur web** ».

Pour ce qui est de **la back-up on utilise** différente technologie tel que **rsync, crontab et ssh**.

Pourquoi avoir choisi toute c'est technologie ?

**Premièrement le faible coût car rsync est aussi en open source.**

Deuxièmement le fais que se soit pas très compliquer d'utilisation pour que **le client puisse faire ces back-up toute simplicité et autonomie avec la documentation de restauration fournie**, ou il y a juste à suivre les étapes pour effectuer une restauration du serveur.

Pour automatiser la back-up, on utilise **crontab** de la machine linux qui va **effectuer la back-up tous les jours à 00h**, ce qui se passe c'est que **crontab** **enregistre les fichiers importants du site web** comme ça s'il y a un souci on a la restauration possible.

Le protocole **ssh** nous permet de **nous connecter à la machine virtuelle qui sert de serveur** pour pouvoir remettre les fichiers de la back up **mais aussi de pouvoir redémarrer le serveur apache en cas de soucis**, il nous sert de plus à transférer les fichiers du site web

Tous les liens pour télécharger les fichier iso ou autres se situe dans la partie « Annexe » !









## IV- Documentation PFSENSE

Pour commencer un petit rappelle sur Pfsense, c'est un routeur / pare-feu open source qui est basé sur un freeBSD. Un routeur à pour rôle de gérer la communication entre deux réseaux par exemple entre le WAN (internet) puis le LAN (réseau local). Quant au pare-feu aussi très souvent nommé firewall à pour rôle de contrôler le flux des connexions entrent mais également sortent grâce à des règles d'action pour le flux de communication qui bloque ou bien autorise.

### 1- Installation de pfsense sur une machine virtuel

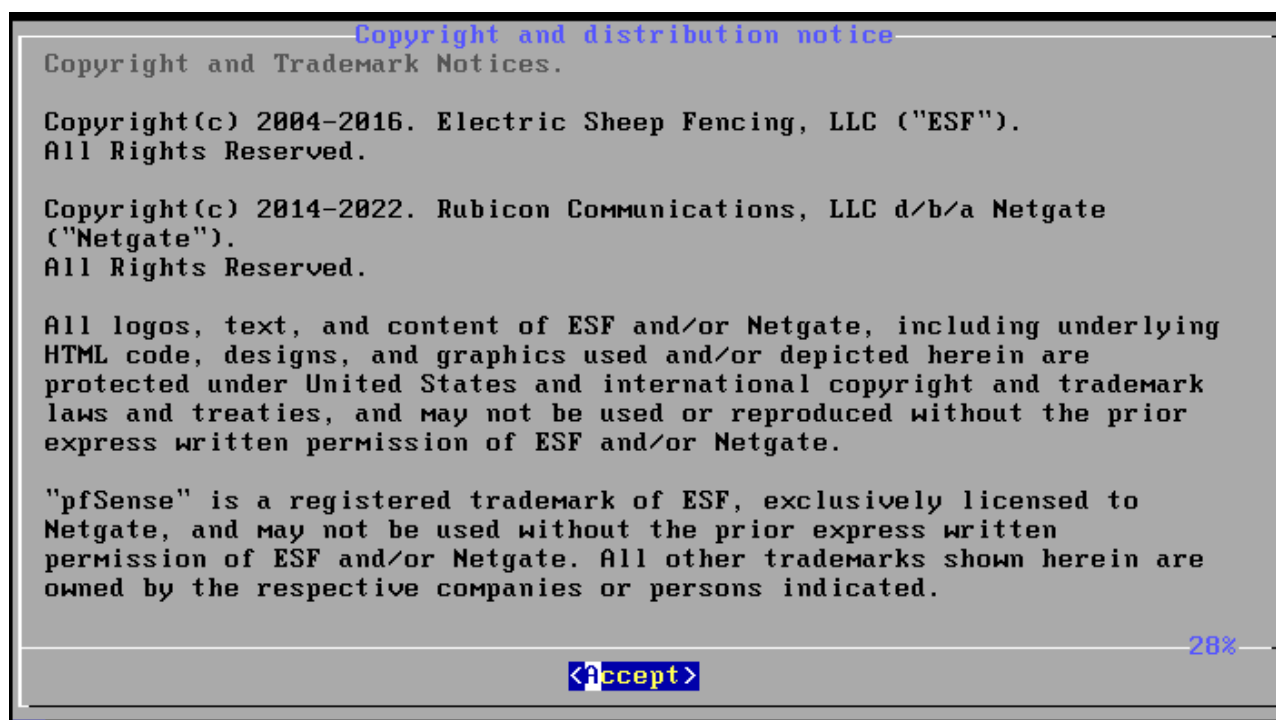
Configuration de la machine virtuelle, il faut lui passer **deux cartes réseaux** : Une carte réseau qui effectue du NAT donc qui récupère l'adresse IP... de notre machine qui représentera l'interface WAN, puis une autre carte reglée en LAN segment qui représentera l'interface LAN. Puis enfin il faut lui passer **le fichier ISO de Pfsense**, voici un exemple de **configuration optimale pour une machine Pfsense** :

Virtual Machine Settings

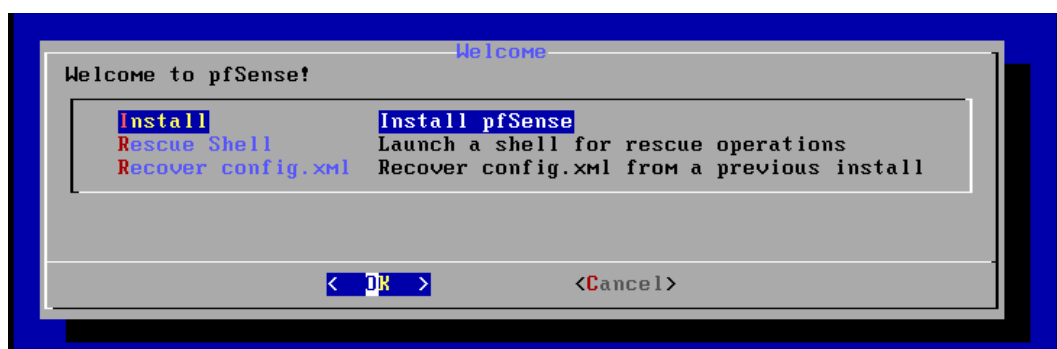
Hardware Options	
Device	Summary
 Memory	1 GB
 Processors	1
 Hard Disk (IDE)	8 GB
 CD/DVD (IDE)	Using file C:\Users\Cyril\Docum...
 Network Adapter	NAT
 Network Adapter 2	LAN Segment
 Sound Card	Auto detect
 Display	Auto detect

Une fois votre machine virtuelle préparée puis configurée comme indiqué ci-dessus, vous pouvez commencer l'installation de Pfsense. Comme nous utilisons Pfsense comme un **routeur il nous faut dès à présent identifier nos deux différentes cartes** : la carte WAN et la carte LAN **grâce à leur adresse MAC** pour pouvoir configurer notre réseau durant l'installation !

Vous pouvez démarrer votre machine, puis patienter pendant le chargement ! Jusqu'à arriver aux conditions générales... maintenant la configuration se fait uniquement via le clavier ! Appuyer sur « entrée » pour passer à l'étape suivante.

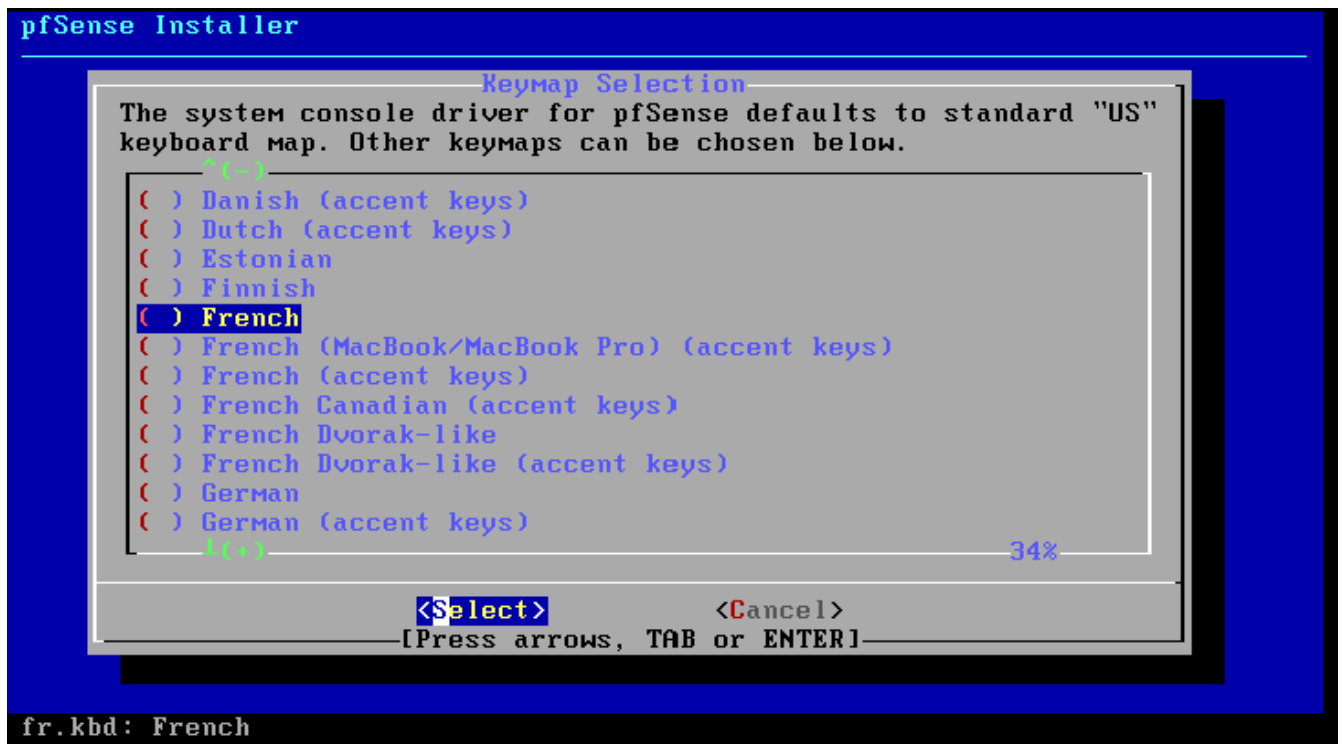


Maintenant sélectionner **Install** grâce aux flèches directionnelles, puis appuyer sur « entrée ».

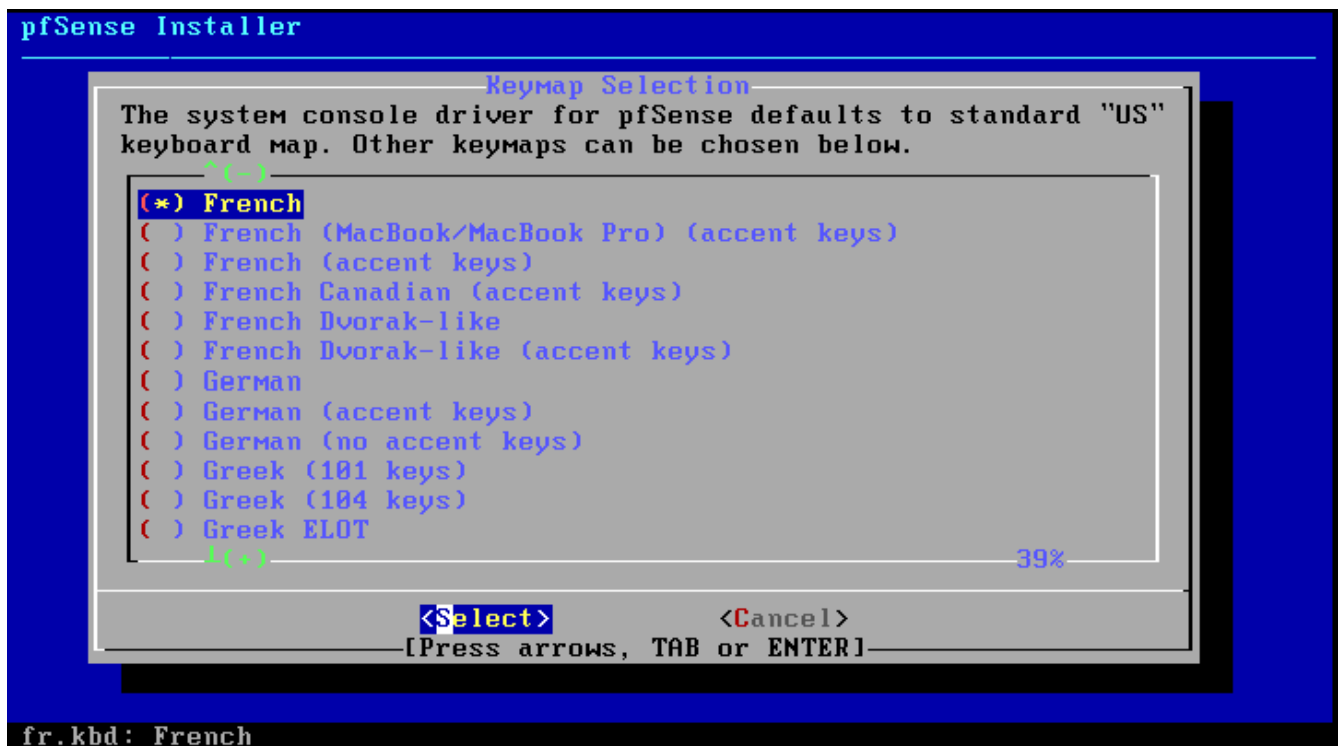




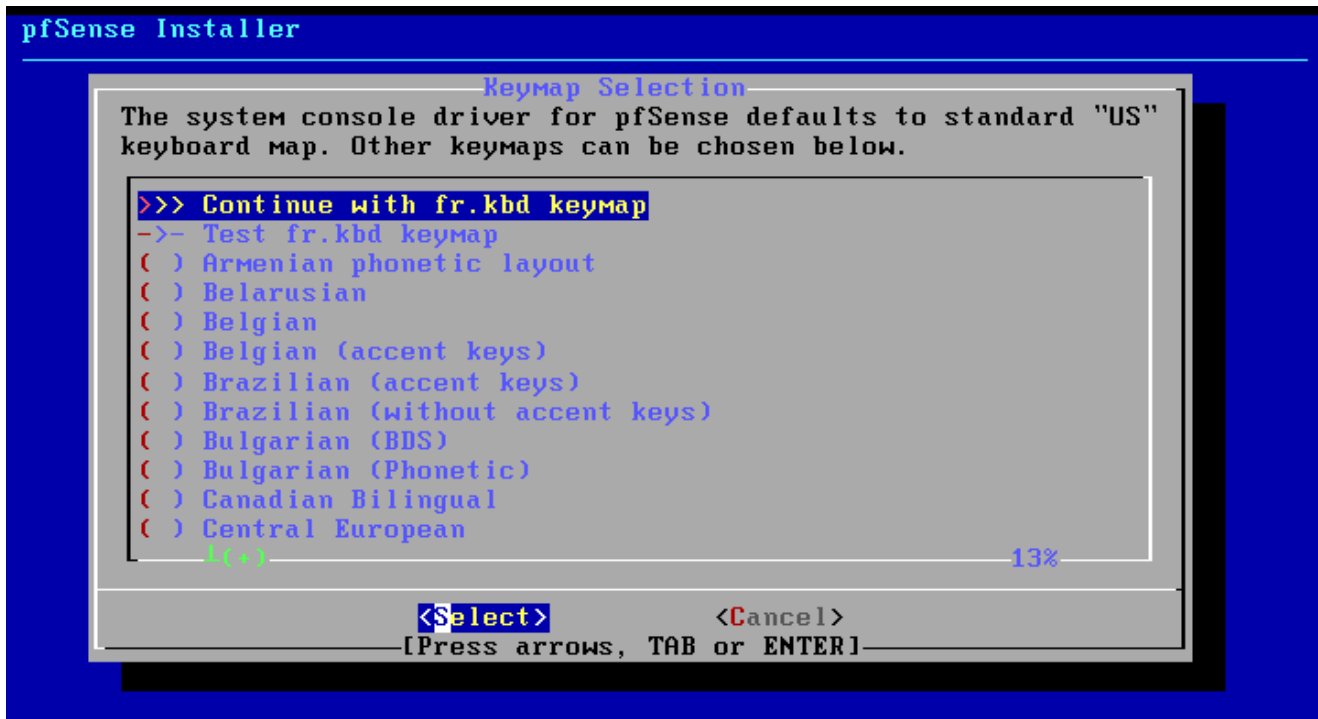
Pour cette étape, il faut configurer notre clavier en AZERTY, [trouver le clavier French](#) grâce aux flèches directionnelles puis [appuyer sur « entrée »](#).



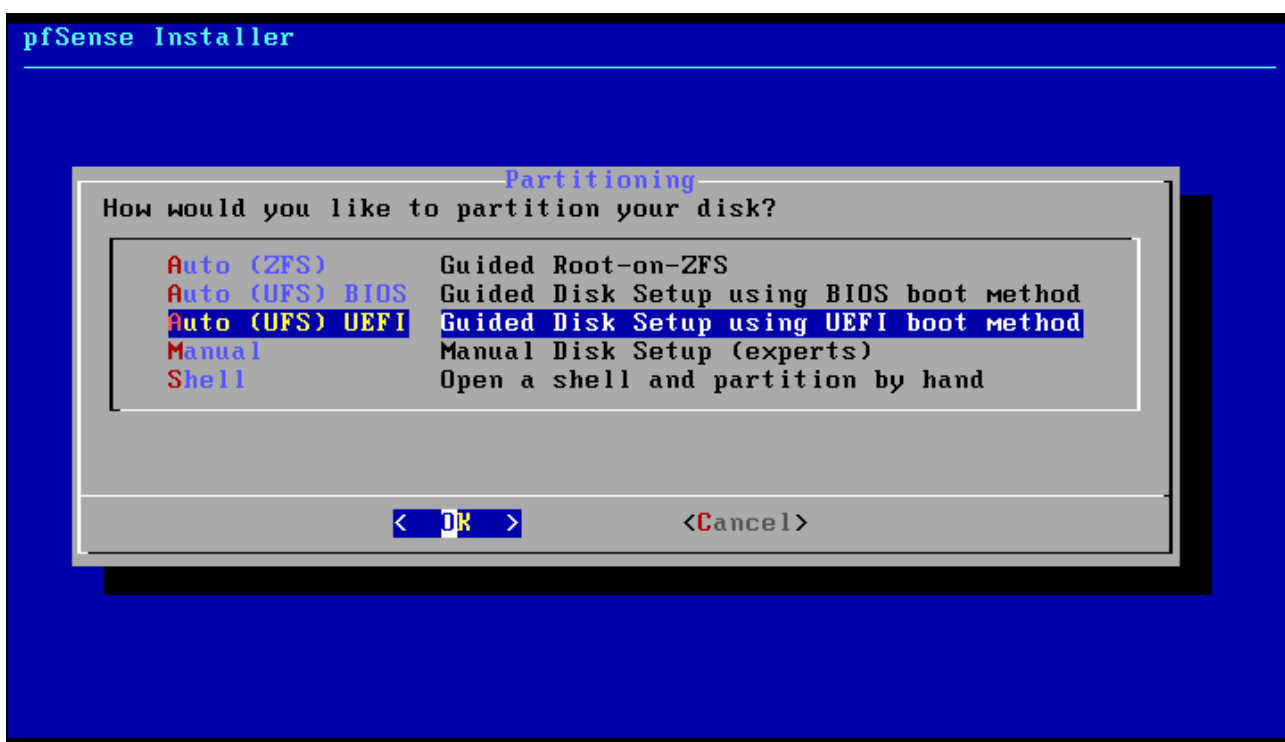
Recommencer encore une fois la même opération.



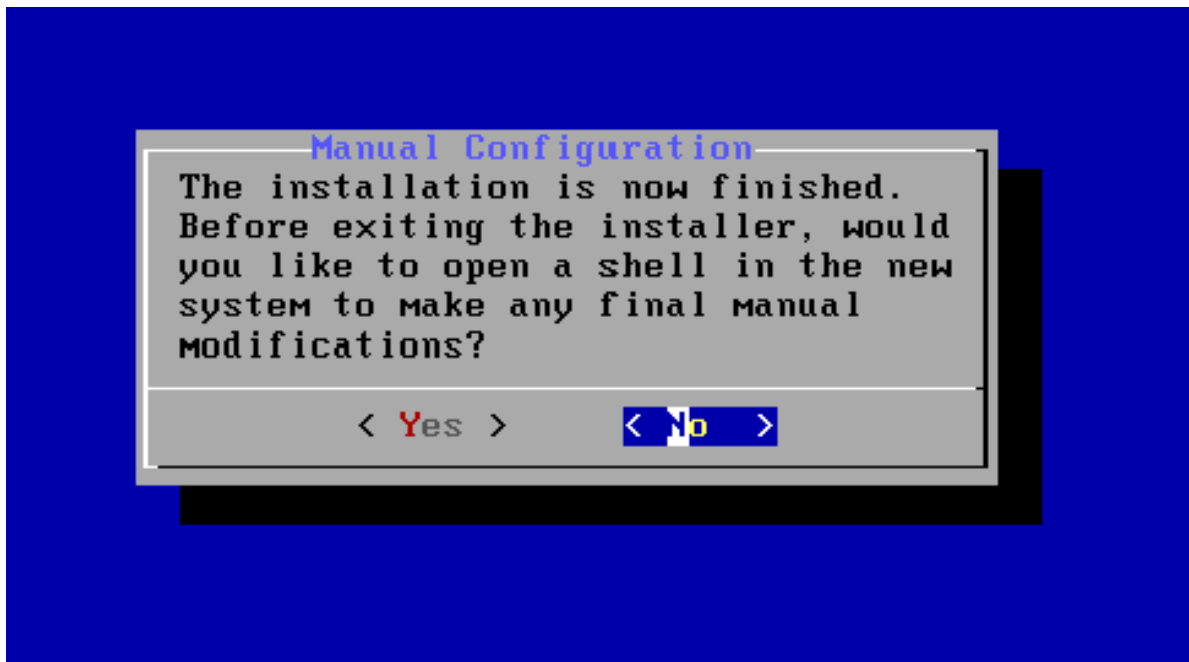
Maintenant [sélectionner « continu with fr.kdb... »](#) pour valider votre choix de clavier puis [appuyer « entrée »](#).



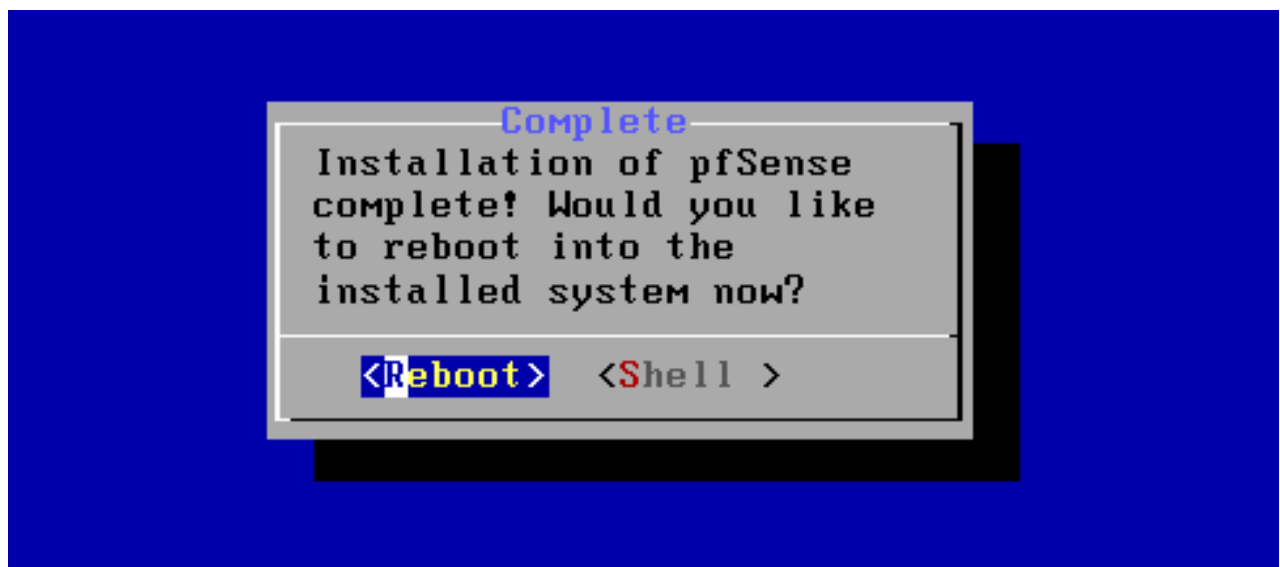
Maintenant sélectionner la façon de partitionner le disque de la machine (dans mon cas je prends BIOS) puis appuyer « entrée ».



Une fois le chargement il va vous proposer d'ouvrir un shell pour apporter des modifications sélectionner « No » puis appuyer « entrée ».



Pour terminer l'installation de pfsense maintenant **sélectionner « Reboot »** puis **appuyer deux fois sur « entrée »**.



Voilà pfsense est installé sur votre machine ! passons à la configuration de base de pfsense...

## **2- Configuration de base de pfsense**

Bravo à vous avez terminé la première étape puisque vous êtes ici !! Pour commencer Pfsense vous demande si vous voulez configure un VLANs dans notre cas non donc **appuyer sur « n » puis « entrée »**.

```

Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration...done.

Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are:

le0      00:0c:29:d3:2d:57 (down) AMD PCnet-PCI
le1      00:0c:29:d3:2d:61 (down) AMD PCnet-PCI

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.

Should VLANs be set up now [y;n]? n

```

Maintenant il demande de configurer l'interface WAN soit de lui indiquer la carte réseau qui gère l'interface WAN soit celle placée précédemment en NAT. Comme demandé au début du tuto vous avez identifié vos deux cartes grâce à leur adresse MAC respective ! Donc vous avez juste à **écrire le nom de la carte puis appuyer sur « entrée »**, dans mon cas c'est la le1.

```

Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration...done.

Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are: adresse MAC des cartes réseaux
le0      00:0c:29:d3:2d:57 (down) AMD PCnet-PCI
le1      00:0c:29:d3:2d:61 (down) AMD PCnet-PCI

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.

Should VLANs be set up now [y;n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): le1

```

Maintenant c'est la même manipulation sauf que c'est pour l'interface LAN ! dans mon cas c'est la le0.

```

le1      00:0c:29:d3:2d:61 (down) AMD PCnet-PCI

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.

Should VLANs be set up now [y!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): le1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le0 a or nothing if finished): le0

```

Il vous demande de confirmer votre sélection donc **appuyer sur « y » puis « entrée »** pour confirmer.

```

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le0 a or nothing if finished): le0

The interfaces will be assigned as follows:

WAN   -> le1
LAN   -> le0

Do you want to proceed [y!n]? y

```

Voilà maintenant il faut lui assigner une adresse IP, pour cela il faut sélectionner l'option « Assigne interfaces » **appuyer sur « 2 » suivit de « entrée »**.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 9c04c2dc0a101da20e28

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

WAN (wan)      -> le0      -> v4/DHCP4: 192.168.242.135/24
LAN (lan)      -> le1      -> 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:

```

Maintenant encore une fois sur **« 2 » suivit « d'entrée »** pour configurer l'interface LAN de pfsense.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 9c04c2dc0a101da20e28

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

WAN (wan)          -> le0          -> v4/DHCP4: 192.168.242.135/24
LAN (lan)          -> le1          -> 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

```

Indiquer lui son adresse IP pour l'interface LAN (dans mon cas c'est 192.168.0.1 ) puis le CIDR de l'adresse IP (dans mon cas /28 ).

```

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 (le1 - dhcp, dhcp6)
2 - LAN (le0 - static)

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1

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):
> 28

```

Maintenant appuyer deux fois sur « entrée » pour éviter de configurer IPv6 et la gateway (passerelle). Puis sélectionner « n » pour configurer le serveur DHCP nous le verrons plus tard ! puis encore une fois n suivi de « entrée ».

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1

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):
> 28

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
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Voici la configuration des interfaces est termin  **appuyer sur « entr e »** !

```
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
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

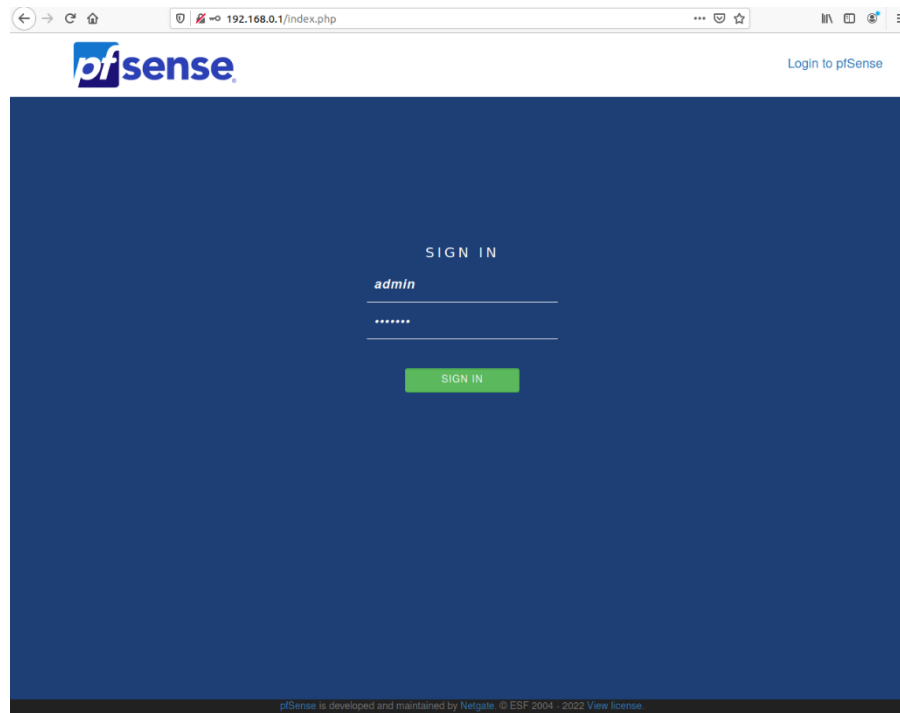
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

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

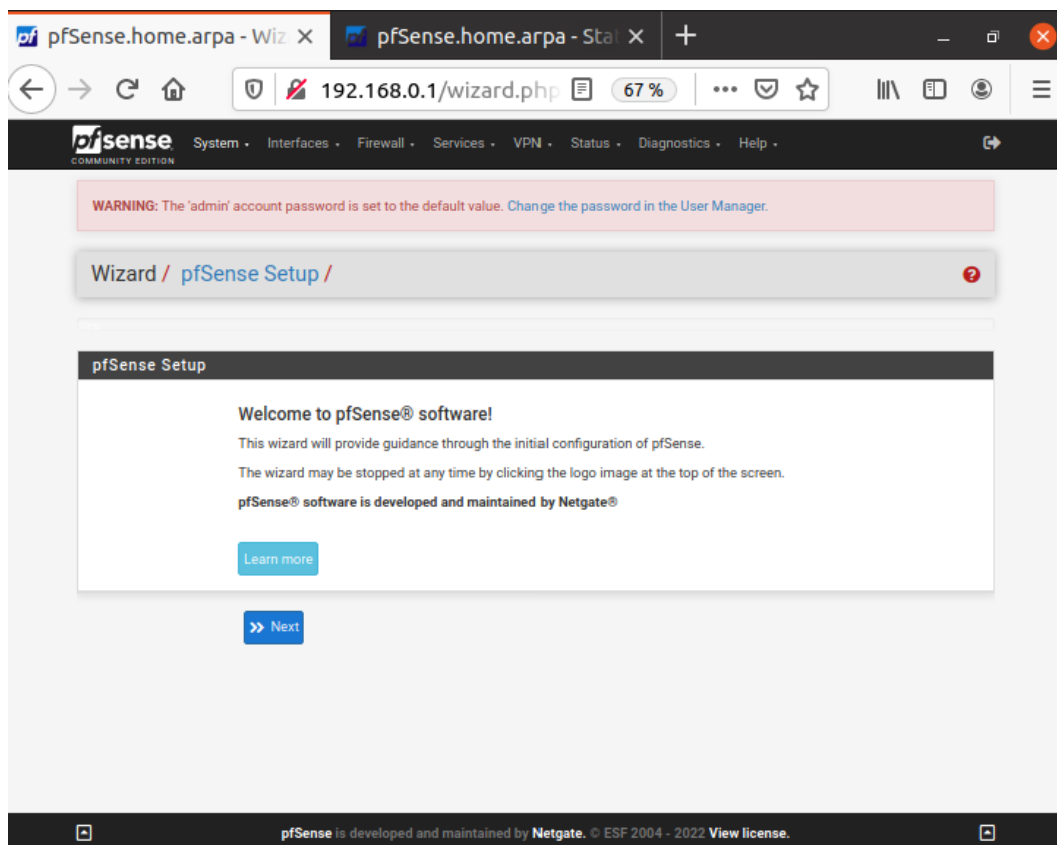
The IPv4 LAN address has been set to 192.168.0.1/28
You can now access the webConfigurator by opening the following URL in your web
browser:
https://192.168.0.1/

Press <ENTER> to continue.
```

Maintenant **ouvrez un navigateur sur une machine placée sur le réseau LAN puis accédez à l'interface web de pfSense** (c'est l'adresse IP LAN le lien) pour continuer la configuration ! les identifiants de connexion par défaut : **user : admin / mot de pass : pfsense**



Une fois connecté **aller dans System > Steup Wizard** puis commencer la configuration (hostname, domaine, WAN, LAN, mot de passe administrateur...). **Appuyer sur « next »**.





Maintenant remplissez les champs Hostname et Domain puis **appuyer encore une nouvelle fois sur « Next »**.

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

[Next](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

**Appuyer directement sur « Next »** puisque l'interface WAN à été configuré via la console de pfsense. Mais penser tout de même à vérifier les information !

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:   
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: xxxxxxxxxxxxxx or leave blank.

MTU:   
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:   
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.

**Static IP Configuration**

IP Address:

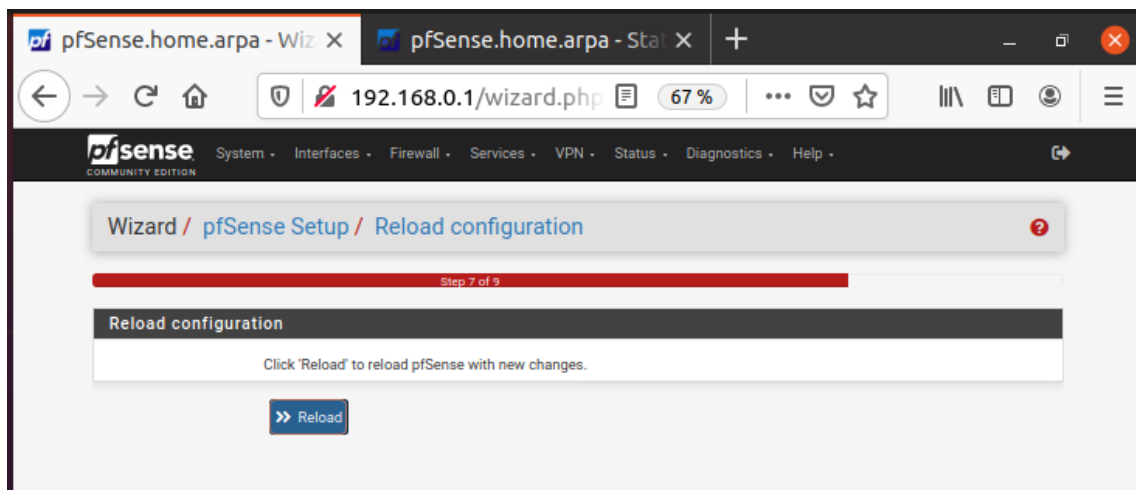
Faite de même pour l'interface LAN !

The screenshot shows the pfSense WebGUI Wizard at Step 5 of 9, titled "Configure LAN Interface". The breadcrumb trail is "Wizard / pfSense Setup / Configure LAN Interface". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area has the heading "Configure LAN Interface" and a sub-heading "On this screen the Local Area Network information will be configured." Below this, there are two input fields: "LAN IP Address" with the value "192.168.0.1" and a checkbox "Type dhcp if this interface uses DHCP to obtain its IP address." which is unchecked. The "Subnet Mask" is set to "28" in a dropdown menu. At the bottom, there is a blue button labeled "» Next".

Maintenant configurer le nouveau mot de passe pour le compte admin, penser à noter le mot de passe sur un bout de papier ! **Puis appuyer sur « entrée »** (vous pouvez réinitialiser le mot de passe du compte par défaut via la console avec l'option 3 ).

The screenshot shows the pfSense WebGUI Wizard at Step 6 of 9, titled "Set Admin WebGUI Password". The breadcrumb trail is "Wizard / pfSense Setup / Set Admin WebGUI Password". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area has the heading "Set Admin WebGUI Password" and a sub-heading "On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled." Below this, there are two input fields for the "Admin Password": the first is labeled "Admin Password" and the second is labeled "Admin Password AGAIN". Both fields contain masked characters (dots). At the bottom, there is a blue button labeled "» Next".

Appuyer sur « Reload » pour ajouter les changements ! puis appuyer sur « Finish » pour valider.

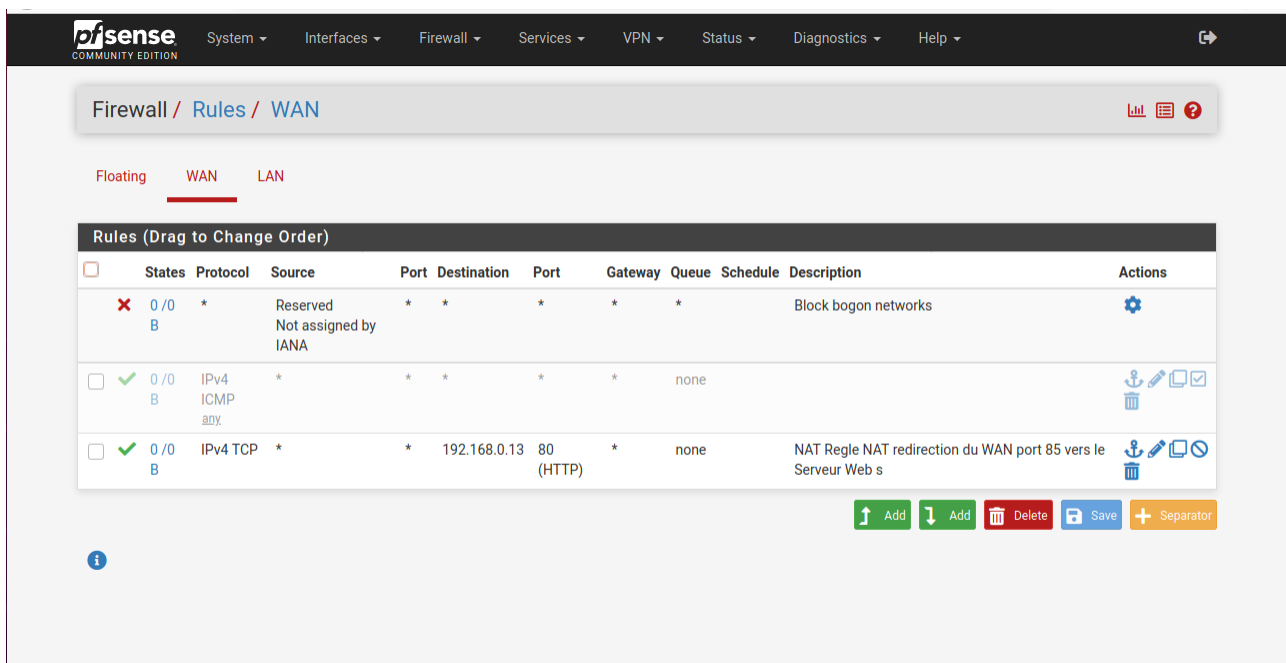


Bravo à vous ! vous avez fini la configuration de base de Pfsense !

### 3- Mettre en place une règle d'action (flirter le flux des connexions)

Une règle d'action à pour simple rôle de **contrôler le flux entrant et sortant pour sécuriser** nos machines, **pour éviter toute action malveillante** venant de l'intérieur par exemple un logiciel infecter installer mais aussi de l'extérieur causer par un accès à un site web malveillant ! **Les règles d'action sont mises en application par le pare-feu** qui à pour rôle de bouclier pour le réseau local. Il vérifie si la connexion (selon l'ip, le protocole, le port, ...) correspond à une des règles d'actions pour **autoriser le flux ou bien bloquer le flux**.

Pour mettre en place une règle d'action **il faut aller dans FierWall>Ruler**. Nous pouvons voir différents onglets : Wan, Lan, puis floating. Nous allons nous intéresser au LAN. Pour ajouter une



règle à la [liste il faut cliquer sur « add »](#) : deux options possibles ajouter au début ou bien à la fin de la liste.

Voilà l'interface de mise en place de règle d'action. La règle que l'on souhaite mettre en place pour l'exemple est une règle d'action « Pass » donc qui autorise le Protocol TCP depuis les adresses ip LAN sur n'importe quel port à destination du LAN/WAN sur le port 80. [Regarder l'exemple ci-dessous de la page remplie](#) :

**Firewall / Rules / Edit**

### Edit Firewall Rule

**Action** Pass  
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** TCP  
Choose which IP protocol this rule should match.

### Source

**Source** ☐ Invert match LAN net Source Address /

[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 any Destination Address /

**Destination Port Range** HTTP (80) From Custom HTTP (80) 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.

### Extra Options

**Log** ☒ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** Autorisation du LAN à utiliser le WAN avec le port HTTP (80)  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

[Save](#)

Une fois la page compléter [appuyer sur « save »](#) suivit de [« apply changes »](#) en haut à gauche pour valider la nouvelle configuration !

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor](#) the filter reload progress.

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 743 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	LAN net	*	*	*	*	none			
LAN autoeiser à utiliser les ports HTTP-HTTPS											
<input type="checkbox"/>	✓ 1 / 5.15 MiB	IPv4 TCP/UDP	LAN net	*	*	80 - 443	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		Autorisation du LAN à utiliser le WAN avec le port HTTP (443)	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		Autorisation du LAN à utiliser le WAN avec le port HTTP (80)	
Bloque les autres flux											
<input type="checkbox"/>	✗ 0 / 269 KiB	IPv4 *	*	*	*	*	*	none		Bloque le flux	

Add Add Delete Save Separator

Voilà maintenant votre règle est en place et fonctionne maintenant ! bravo à vous...

#### 4- Mise en place d'une règle de redirection de port (NAT)

Une règle de redirection de port aussi appelé «port forwarding » permet de rediriger un flux qui pointe vers une IP et un port précis dans la direction d'une autre ip de destination avec un port précis également. L'utilité d'une règle de redirection de port s'illustre par exemple dans le cas où l'on désire rediriger une connexion à notre IP public de notre routeur vers notre serveur web placé sur le réseau local.

Pour mettre en place une règle de redirection de port il faut aller « Firewall > NAT » puis appuyer sur « add » pour ajouter une règle.

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>										

Add Add Delete Save Separator

Pour cet exemple nous souhaitons mettre en place une redirection vers notre serveur web local lorsque nous pointons notre l'IP WAN de pfsense (l'IP WAN de pfsense = WAN adresse) sur le port 85 vers le serveur web (l'IP du serveur web = 192.168.0.13) sur le port 80. [Regarder l'exemple ci-dessous de la page remplie](#) :

Firewall / NAT / Port Forward / Edit ?

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN  
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol TCP  
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source Display Advanced

Destination ☐ Invert match. WAN address  
Type Address/mask

Destination port range Other 85 Other 85  
From port Custom To port Custom  
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Single host 192.168.0.13  
Type Address  
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope",  
i.e. it is not possible to redirect from link-local addresses scope (fe80:\*) to local scope (::1)

Redirect target port HTTP   
Port Custom  
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).  
This is usually identical to the "From port" above.

Description Regle NAT redirection du WAN port 85 vers le Serveur Web sur le port 80  
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other CARP members  
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Regle NAT redirection du WAN port 85 vers le Serveur Web sur le port 80  
[View the filter rule](#)

Rule Information

Created 5/1/22 19:41:53 by admin@192.168.0.11 (Local Database)

Updated 5/1/22 19:41:53 by admin@192.168.0.11 (Local Database)

Save

Remarque lorsque l'on pointe l'IP WAN de pfsense il faut éviter le port 80 (HTTP) vos mieux utiliser un port comme 85 ou bien 8080 .

Une fois la page compléter **appuyer sur « save » suivit de « apply changement »** en haut à gauche pour valider la nouvelle configuration !

Firewall / NAT / Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor](#) the filter reload progress.

Port Forward 1:1 Outbound NPt

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	85	192.168.0.13	80 (HTTP)	Regle NAT redirection du WAN port 85 vers le Serveur Web sur le port HTTP (80)

Legend  
 Pass  
 Linked rule

↑ Add ↓ Add Delete Save + Separator

Voilà vous avez réussie à mettre en place une redirection de port ! bravo à vous votre site web est dorénavant accessible depuis le Wan !

## 5- Mise en place d'un serveur DHCP

Petit rappelle **un serveur DHCP** permet de **fournir à l'hôte automatiquement une configuration réseau** qui contient une adresse IP unique, le masque de sous-réseau, ou encore la passerelle... ce qui permet d'éviter une intervention humaine sur la machine pour remplir la configuration puisque sans configuration réseau la machine ne peut pas accéder à internet !

Pour mettre en place un serveur DHCP avec pfSense il faut aller dans Services > DHCP Server puis il faut remplir les champs « range » qui tout simplement la plage d'adresse IP que l'on souhaite rendre dynamique ! dans notre exemple c'est de 192.168.0.2 jusqu'à 192.168.0.10

The screenshot shows the Pfsense web interface for configuring the DHCP server on the LAN interface. The breadcrumb trail is 'Services / DHCP Server / LAN'. The 'LAN' tab is selected. The 'General Options' section contains the following settings:

- Enable:** ☒ Enable DHCP server on LAN interface
- BOOTP:** ☐ Ignore BOOTP queries
- Deny unknown clients:** ☐ Allow all clients. A dropdown menu is set to 'Allow all clients'. A detailed explanation follows: 'When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.'
- Ignore denied clients:** ☐ Denied clients will be ignored rather than rejected. A note states: 'This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.'
- Ignore client identifiers:** ☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. A note states: 'This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.'
- Subnet:** 192.168.0.0
- Subnet mask:** 255.255.255.240
- Available range:** 192.168.0.1 - 192.168.0.14
- Range:** Two input fields are shown: 'From' (192.168.0.2) and 'To' (192.168.0.14).

Below the 'General Options' section is the 'Additional Pools' section, which is currently empty.

Puis enfin **il faut appuyer sur « save »** suivit de **« apply changes »** pour confirmer et voilà le serveur DHCP en route.

## V- Documentation Serveur web

**Apache HTTP Serveur** vise à **développer et à maintenir un serveur HTTP** open source pour les systèmes d'exploitation modernes, notamment UNIX et Windows. L'objectif de ce projet est de fournir un serveur sécurisé, efficace et extensible qui fournit des services HTTP en synchronisation avec les normes HTTP actuelles.

### 1- Installation du serveur APCHE

On va le crée sur une machine virtuelle qui tourne sous linux, après avoir installé la machine on ouvre un terminal et on va procéder à l'installation d'apache. **D'abord on commence par faire la commande « sudo apt install apache2 »**

```
matthieu@matthieu-virtual-machine:~$ sudo apt install apache2
```

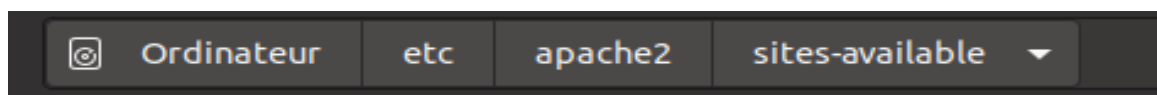


Après avoir installé apache on peut accéder à son dossier pour effectuer des changements de configurations. [Le dossier se situe dans le chemin /etc/apache2](#). C'est le répertoire de configuration Apache, tous les fichiers de configuration Apache se trouvent à l'intérieur.

## 2- Création d'un hôte virtuel

On commence par une petite définition d'un [hôte virtuel](#). Lorsque vous utilisez le serveur web Apache, vous pouvez utiliser des *hôtes virtuels* [pour encapsuler les détails de la configuration et héberger plusieurs domaines à partir d'un seul serveur](#). Les fichiers d'hôte virtuel sont les fichiers qui spécifient la configuration réelle de nos hôtes virtuels et dictent comment le serveur web Apache répondra aux diverses requêtes de domaine.

Le chemin pour créer un hôte virtuel en passant par les fichiers celui-ci :



Et en passant par le terminal le chemin est : « [ordinateur/etc/apache2/sites-available](#) »

```
matthieu@matthieu-virtual-machine:/etc/apache2$
```

Maintenant on va créer un nouvel hôte virtuel, Pour créer le fichier [on fait la commande](#) « [sudo touch nomdufichier.conf](#) »



Après avoir créé le fichier on va l'éditer [avec la commande suivante](#) « [vi nomdufichier.conf](#) ».

```
matthieu@matthieu-virtual-machine:/etc/apache2$ vi nomdufichier.conf
```

Après avoir fait cette commande on peut éditer le fichier de configuration via une interface.

```

1 VirtualHost *:80>
2
3     ServerAdmin webmaster@localhost
4
5     ServerName http://www.projet.com
6
7     DocumentRoot /var/www/html/bienvenue/
8
9     ErrorLog /var/log/apache2/bienvenue.log
10
11     CustomLog /var/log/apache2/access.log combined
12
13 </VirtualHost>

```

Explication du contenu du fichier de configuration :

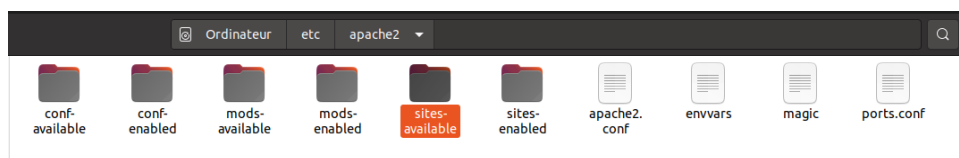
**VirtualHost \*:80** : signifie que le serveur va écouter le port 80

**ServerAdmin webmaster@localhost** : c'est une e-mail auquel l'administrateur du site peut accéder.

**ServerName** : établit le domaine de base qui doit correspondre à cette définition d'hôte virtuel.

Nous avons mis à jour le DocumentRoot dans notre nouveau répertoire.

Une fois modifier le fichier de configuration éditer nous allons **modifier le fichier « port.conf »**.



Pareil on utilise la commande vi sur le fichier suivant **« port.conf »**.

```

/etc/apache2
1 # If you just change the port or add more ports here, you will likely also
2 # have to change the VirtualHost statement in
3 # /etc/apache2/sites-enabled/test.conf
4
5 Listen 80
6
7 <IfModule ssl_module>
8     Listen 443
9 </IfModule>
10
11 <IfModule mod_gnutls.c>
12     Listen 443
13 </IfModule>
14
15 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet

```

Ici on peut modifier le port d'écoute du serveur (dans l'image si dessus il écoute sur le port 80 mais on aurait pu mettre n'importe quel ports)

Petite explication du fichiers port.conf :

**/etc/apache2/ports.conf** : ce fichier **spécifie les ports sur lesquels Apache écoutera**. Par défaut, Apache écoute sur le port 80 et sur le port 443 en plus lorsqu'un module fournissant des capacités SSL est activé.

Voilà le serveur est fonctionnel en local ! Pour l'ouvrir depuis le WAN il faudra utiliser un routeur comme pfsense avec une règle NAT.

## VI- Documentation back-up

On commence par quelques petites définitions importante.

Définition de rsync : **rsync est un logiciel de synchronisation libre de droit**. La **synchronisation est unidirectionnelle**, c'est-à-dire qu'elle copie les fichiers de la source en direction de la destination. **rsync est donc utilisé pour réaliser des sauvegardes incrémentielles ou différentielles ou pour diffuser le contenu d'un répertoire de référence**.

Définition de cron : **cron est un programme qui permet aux utilisateurs des systèmes unix D'exécuter automatiquement des scripts, des commandes ou des logiciels** à une date et une heure spécifiée à l'avance, ou selon un cycle défini à l'avance.

Définition de ssh : **Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé**. Le protocole de connexion impose un échange de clé de chiffrement en début de connexion.

### 1- installer openssh

Pour avoir accès au ssh il faut d'abord l'installer avec **la commande « apt install openssh-server »**.

```
matthieu@matthieu-virtual-machine:~$ apt install openssh-server
```

On peut vérifier si ssh fonctionne bien **en faisant la commande « systemctl status ssh »**.

```
matthieu@matthieu-virtual-machine:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e
   Active: active (running) since Mon 2022-05-02 15:13:55 CEST; 52s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 2564 (sshd)
     Tasks: 1 (limit: 2246)
    Memory: 1.0M
    CGroup: /system.slice/ssh.service
            └─2564 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
```

Ensuite on se connecte en ssh à la machine virtuelle qui contient notre back up pour envoyer le dossier de back up.

Voici un Exemple de connexion en ssh sur une autre machine virtuelle en local

```
matthieu@matthieu-virtual-machine:~/home$ ssh user@debian
```

Et voici avec une IP fix.

```
matthieu@matthieu-virtual-machine:~$ ssh user@192.168.0.15
```

Pour voir l'IP on peut faire la commande « ip ad »

```
matthieu@matthieu-virtual-machine:~$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ae:d3:72 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.5.130/24 brd 192.168.5.255 scope global dynamic noprefixroute ens33
        valid_lft 1353sec preferred_lft 1353sec
    inet6 fe80::55e6:a3af:9591:bd0e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
matthieu@matthieu-virtual-machine:~$
```

Une fois qu'on connecte en ssh on peut se déconnecter, c'était pour vérifier que ça fonctionnait bien

## 2- le transfert de fichier/dossier

Pour envoyer le dossier d'une machine virtuelle à l'autre on va utiliser rsync . Voici une commande rsync pour envoyer un fichier ou bien dossier à une autre machine, on voit bien que les dossier jour/mois ... sont transférés sur le bureau d'utilisateur

```
matthieu@matthieu-virtual-machine:~/home$ sudo rsync -av ./sauvegarde/ user@debian:~
[sudo] Mot de passe de matthieu :
user@debian's password:
sending incremental file list
./
.bash_logout
.bashrc
.profile
jour/
jour/current/
mois/
semaine/

sent 2,757 bytes  received 150 bytes  646.00 bytes/sec
```

Voici une petite liste d'option à ajouter à la commande précédente :

**-a** : archive

**-r** : récursive, cela indique a rsync de copier les répertoires de façons récursive

**-b** : backup

**-exclude/include** : pour exclure ou inclure différent type de fichiers

**-v** : verbose, cette option augmente la quantité d'information qui vous sont fournies lors du transfère

**-q** : est l'inverse de **-v**, il réduit les informations lors du transfère

**-u, --update** : cela oblige rsync à ignorer tous les fichiers qui existent sur la destination et dont l'heure modifiée est plus récente que le fichier source

**-p, --perm** : cette option amené le rsync récepteur à définir les autorisations de destination pour qu'elles soient identiques aux autorisation source

**Les commande rsync marche toujours de la même façon c'est à dire :**

On fait " ~: **rsync -avp** ./dossier qui envoie nom de l'hôte@ip de l'hôte:~/nom du dossier receteur"

Le dossier qui envoie est toujours avant le récepteur.

### **3- le script avec cron**

On a mis en place une commande cron pour automatiser les sauvegardes tout le jour à la même heure. La commande pour éditer la table est la suivante :



```
matthieu@matthieu-virtual-machine:~$ crontab -e
```

Une la table prete à êtres éditer il faut ajouter la ligne suivante : « **0 0 \* \* \* /bin/sh sauvegarde.sh** », Pour effectuer une sauvegarde de la base de données à minuit, et fonctionner une fois par jour. Voici la nouvelle table !

```

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
27 18 * * * touch ~/timesync-status.csv
0 0 * * * /bin/sh sauvegarde.sh

```

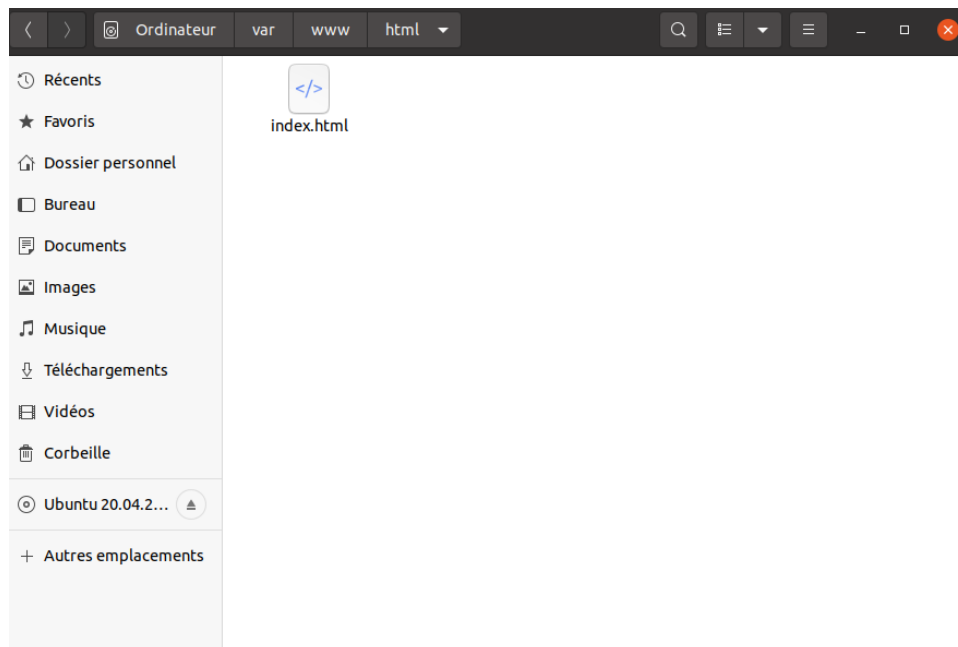
#### 4- Mettre en place les fichier html/css

Pour se faire vous avez deux possibilités la première consiste à faire un dossier ou vous voulez et de changer la route utiliser pour le document root dans le « fichier.conf »

Ici vous pouvez mettre le chemin que vous voulez (là ou se situe dans votre dossier avec vos page web)

```
DocumentRoot /var/www/html/bienvenue/
```

Sinon on mais directement les fichiers dans le dossier de base indiquer dans le « fichier.conf ». Ici vous pouvez déposer vos fichiers html/css ...



Voilà le serveur est fonctionnel en local ! Pour l'ouvrir depuis le WAN il faudra utiliser un routeur comme pfsense avec une règle NAT.

## VII- Annexe

ISO PFSENSE :

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

ISO Ubuntu (LINUX) :

<https://www.ubuntu-fr.org/download/>

ISO Windows 10 :

<https://tb.rg-adguard.net/public.php>

Logiciel VMware Pro :

<https://www.vmware.com/go/getworkstation-win>

Licence VMware Pro :

<https://gist.github.com/williamgh2019/cc2ad94cc18cb930a0aab42ed8d39e6f>