

TP Wifi/Portail Captif

Sommaire:

Sommaire.....	1
Bloc Compétence Analysé.....	2
Analyse.....	3
Première borne Wifi.....	3-6
-Description Borne.....	3
- Trouver et Installation ISO (Fail).....	3-6
Deuxième Borne.....	6-8
-Description.....	6
- interface Graphique.....	6-8
Pfsense.....	8-16
-Installation.....	8-13
-Configuration.....	14-16
Portail Captif.....	17-20
Partie Juridique.....	20-21

Bloc compétence analysé:

Activité 1.1. Gestion du patrimoine informatique

- Mise en place et vérification des niveaux d'habilitation associées à un service ;
- Vérification du respect des règles d'utilisation des ressources numériques.

Activité 1.4. Travail en mode projet

- Analyse des objectifs et des modalités d'organisation d'un projet ;
- Évaluation des indicateurs de suivi d'un projet et analyse des écarts.

Activité 1.5. Mise à disposition des utilisateurs d'un service informatique

- Test d'intégration et d'acceptation d'un service ;
- Déploiement d'un service ;

Activité 2.1. Conception d'une solution d'infrastructure

- Analyse d'un besoin exprimé et de son contexte juridique ;
- Élaboration d'un dossier de choix d'une solution d'infrastructure et rédaction des spécifications techniques ;
- Choix des éléments nécessaires pour assurer la qualité et la disponibilité d'un service ;
- Maquettage d'une solution d'infrastructure permettant d'atteindre la qualité de service attendue.

Activité 2.2. Installation, test et déploiement d'une solution d'infrastructure réseau

- Installation et configuration d'éléments d'infrastructure ;
- Instal. et config. des éléments nécessaires pour assurer la QoS ; (travail complémentaire)
- Déploiement d'une solution d'infrastructure.

Activité 3.1. Protection des données à caractère personnel

- Application de la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel.

Activité 3.3. Sécurisation des équipements et des usages des utilisateurs

- Gestion des accès et des privilèges appropriés.

Activité 3.4. Garantie de la disponibilité, de l'intégrité et de la confidentialité des services informatiques et

des données de l'organisation face à des cyberattaques

- Caractérisation des risques liés à l'utilisation malveillante d'un service informatique ;
- Application des procédures garantissant le respect des obligations légales.

Activité 3.5. Cybersécurisation d'une infrastructure réseau, d'un système, d'un service

- Vérification des éléments contribuant à la sûreté d'une infrastructure informatique ;
- Prise en compte de la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure.

Analyse:

Ce TP consiste à mettre en place une borne Wifi avec un portail captif. Pour cela nous avons à disposition un VLAN, 2 poste Windows, une connexion à Internet et une borne

Description Borne 1:

Borne Cisco utilisée :

Ref: AIR-SAP1602I-E-k9

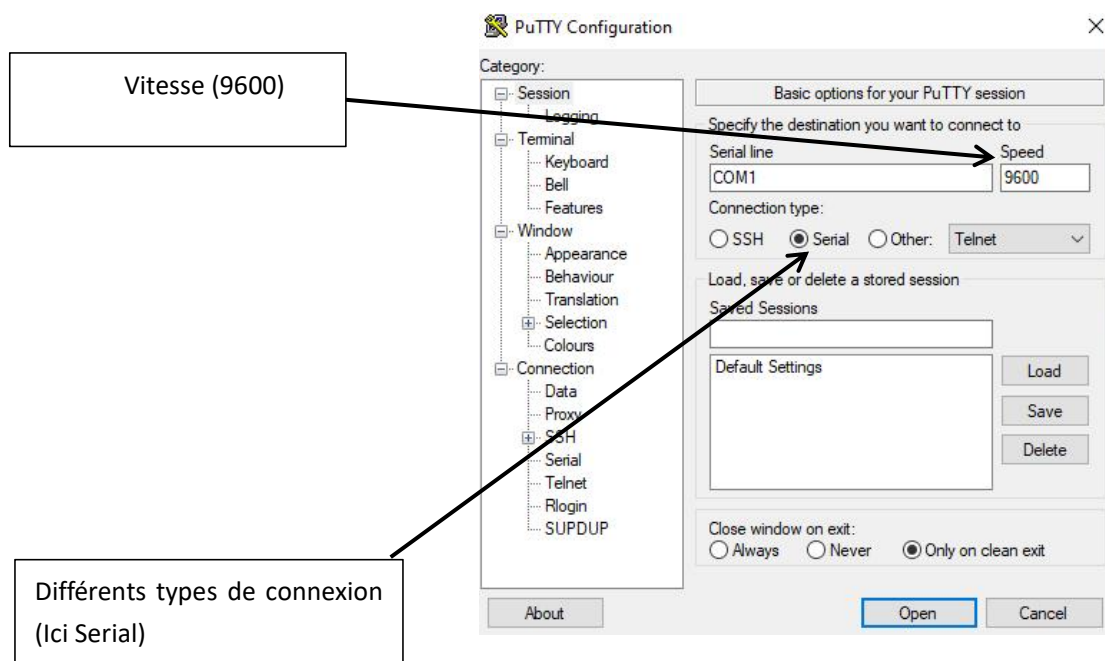


Manuel:

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1600/quick/guide/ap1600getstart.pdf

Trouver et Installation ISO (Fail)

Au début du TP, nous devons réinstaller le système d'exploitation de la borne Cisco. Pour cela nous avons utilisé un Vlan (créé par notre chère camarade Baptiste) pour nous connecter à celle-ci. On a donc utilisé Putty (PuTTY est un émulateur de terminal pour Windows permettant la connexion à une machine distante par protocole SSH)



Une fois connecter a celle-ci, on a voulu la réinitialiser afin de «boot» sur le nouvelle OS (Cette OS, que nous avons trouver sur le site de Cisco mais qui, malgré tout, n'as pas fonctionner). Pour effectuer cette réinitialisation, on a du aller voir le document d'utilisation de la borne afin de savoir combien de temps il fallait rester appuyer sur le bouton «RESET». Une fois trouvé, on a suivi la documentation

Au préalable, nous avons utiliser «Tftpd64» qui est une application IPv6 gratuite, légère et open source qui comprend des serveurs DHCP, TFTP, DNS, SNTP et Syslog ainsi qu'un client TFTP. Cette application nous a permit de mettre notre nouvelle ISO sur la borne lors de sa réinitialisation

Lors de la réinitialisation de la borne, on peut voir, sur Putty, ce qui se passe

```
Boot from flash

IOS Bootloader - Starting system.
FLASH CHIP: Spansion S25FL256
Xmodem file system is available.
flashfs[0]: 226 files, 8 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 31936000
flashfs[0]: Bytes used: 12450816
flashfs[0]: Bytes available: 19485184
flashfs[0]: flashfs fsck took 10 seconds.
Reading cookie from SEEPROM
Base Ethernet MAC address: a0:ec:f9:31:8c:38
***** loopback_mode = 0

Boot from flash

IOS Bootloader - Starting system.
FLASH CHIP: Spansion S25FL256
Xmodem file system is available.
flashfs[0]: 226 files, 8 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 31936000
flashfs[0]: Bytes used: 12450816
flashfs[0]: Bytes available: 19485184
flashfs[0]: flashfs fsck took 10 seconds.
Reading cookie from SEEPROM
Base Ethernet MAC address: a0:ec:f9:31:8c:38
***** loopback_mode = 0
button is pressed, wait for button to be released...
button pressed for 32 seconds
process_config_recovery: set IP address and config to default 10.0.0.1
process_config_recovery: image recovery
image_recovery: Download default IOS tar image tftp://255.255.255.255/aplg2-k9w7-tar.default
```

Bouton pressé pour réinitialiser

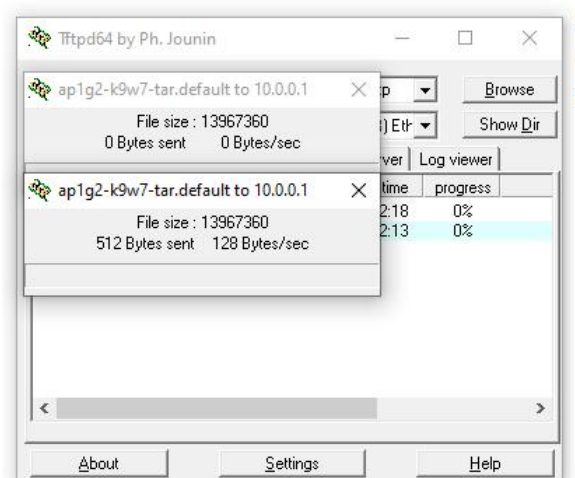
Le bouton a été pressé pendant 32 seconde (20 secondes pour réinitialiser)

Une fois réinitialiser, la borne redémarre

```
COM1 - PuTTY
button is pressed, wait for button to be released...
button pressed for 36 seconds
process_config recovery: set IP address and config to default 10.0.0.1
process_config recovery: image recovery
image_recovery: Download default IOS tar image tftp://255.255.255.255/aplg2-k9w7
-tar.default

examining image...
extracting info (291 bytes)
Image info:
  Version Suffix: k9w8-.153-3.JF15
  Image Name: aplg2-k9w8-mx.153-3.JF15
  Version Directory: aplg2-k9w8-mx.153-3.JF15
  Ios Image Size: 13292032
  Total Image Size: 13947392
  Image Feature: WIRELESS LAN|LWAPP
  Image Family: AP1G2
  Wireless Switch Management Version: 8.5.182.0
Extracting files...
aplg2-k9w8-mx.153-3.JF15/ (directory) 0 (bytes)
aplg2-k9w8-mx.153-3.JF15/html/ (directory) 0 (bytes)
aplg2-k9w8-mx.153-3.JF15/html/level/ (directory) 0 (bytes)
aplg2-k9w8-mx.153-3.JF15/html/level/15/ (directory) 0 (bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/officeExtendapEvent.shtml.gz (
988 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/officeExtendapBanner.htm (7514
bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/easyApManagementSummary.shtml.
gz (3371 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/easyApManagementConfig.shtml.g
z (4999 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/officeExtendapConfig.shtml.gz
(3147 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/easyApManagement.html (967 byt
es)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/officeExtendapMain.shtml.gz (3
350 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/officeExtendapHelp.htm (5721 b
ytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/15/officeExtendapSummary.htm (985
bytes)
aplg2-k9w8-mx.153-3.JF15/html/level/1/ (directory) 0 (bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/jquery-1.11.3.min.js (95957 byt
es)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/ap_home.shtml.gz (1540 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/officeExtendap.css (41801 bytes
)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/back.shtml (512 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/sitewide.js (17290 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/config.js (29225 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/appui.js (563 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/forms.js (20442 bytes)
aplg2-k9w8-mx.153-3.JF15/html/level/1/images/ (directory) 0 (bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/images/login_homeap.gif (19671
bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/images/background_web41.jpg (73
2 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/images/info.gif (399 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/html/level/1/images/cisco-logo-2007.gif (164
8 bytes)
extracting aplg2-k9w8-mx.153-3.JF15/8005.img (1181564 bytes)
.....
```

Et on peut voir que le transfert est entrain de se faire
(Auparavant ,sur Tftpd, j'ai saisi le répertoire ou se trouvait le nouvel ISO)



Cependant, après l'installation de celui-ci, il était impossible d'accéder a l'interface de la borne et nous avons du changer d'ISO. Malgré nos changement d'ISO

(5 au total), l'ensemble de la classe n'arrivait pas à trouver un ISO convenable, nous avons du changer de borne afin d'éviter de perdre plus de temps.

Deuxième Borne (Description):

Borne Cisco utilisé :

Modèle: WG602 v4

Documentation:

<https://www.netgear.fr/support/product/wg602v4#docs>



Interface Graphique:

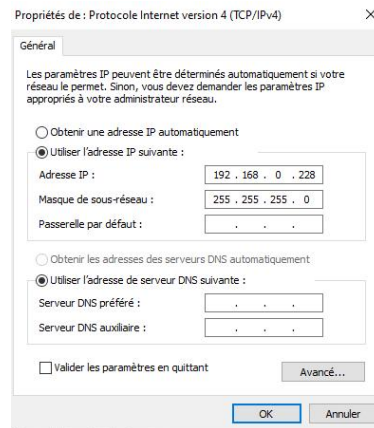
Sur cette 2eme borne, pas besoin de réinstaller un nouvel ISO. Donc nous avons directement chercher à accéder à l'interface graphique. Pour cela, nous l'avons directement réinitialiser, elle a donc repris sa configuration de base:



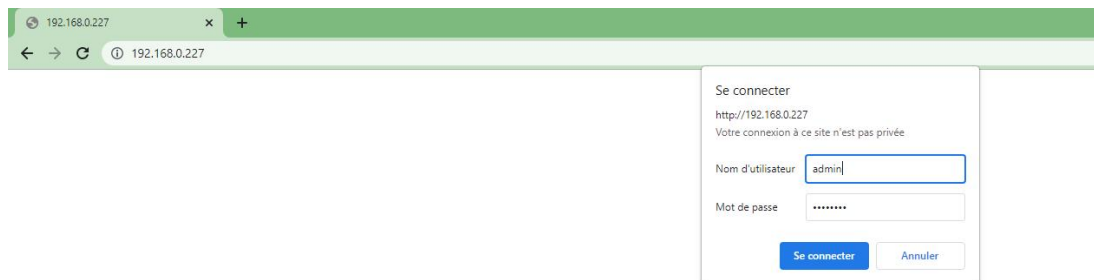
Ensuite, pour se connecter à celle-ci, nous avons dû nous mettre dans la même plage d'adresse que l'adresse de la borne:

Adresse Borne: 192.168.0.227

Adresse du PC:



Et désormais, nous pouvons accéder à l'interface de la borne et nous nous sommes connectés avec les identifiants de base

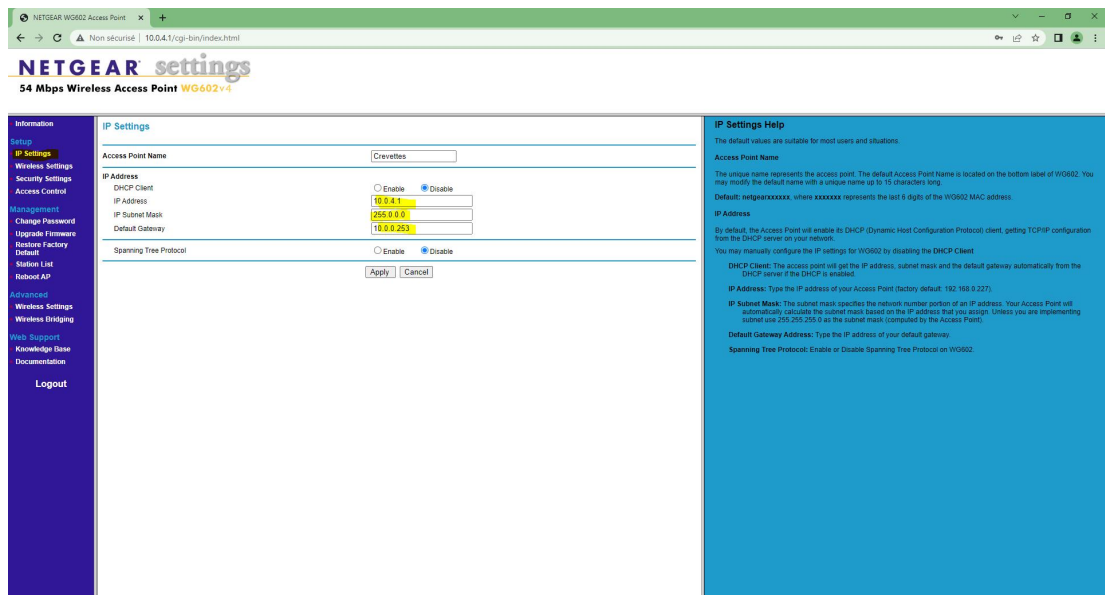


Directement après, j'ai changé l'adresse de la borne comme demandé :

IP: 10.0.4.1 (4 car on est le binôme 4)

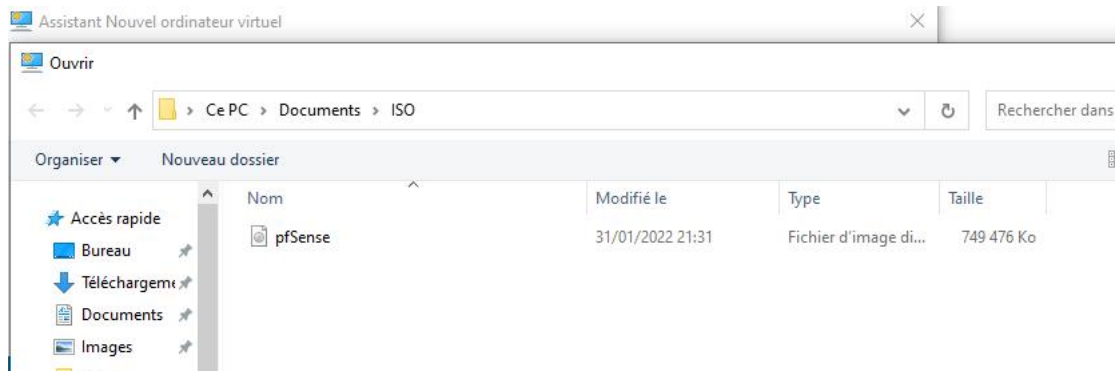
Le masque: Par défaut donc /8 (255.0.0.0)

Et la passerelle par défaut: 10.0.0.253



Pfsense Installation:

Par la suite, pour mon portail captif j'ai utilisé un OS open source, Pfsense
Pfsense est un système d'exploitation open source ayant pour but la mise en place d'un pare-feu (Portail captif)
Pour commencer, je suis allé chercher l'ISO de Pfsense sur le Web mais après plusieurs recherche et test, je n'ai pas réussi à le récupérer. Cependant nos camarades on réussi à l'avoir et nous l'on gentiment donner.



Ensuite, j'ai créé une VM pour faire fonctionner Pfsense, avec comme virtualisation «Hyper-V» (Car je préfère Hyper-V qu'au autres du style vmware ou virtualbox)

Assistant Nouvel ordinateur virtuel

Spécifier le nom et l'emplacement

Avant de commencer

Spécifier le nom et l'emplacement

Spécifier la génération

Affecter la mémoire

Configurer la mise en réseau

Connecter un disque dur virtuel

Options d'installation

Résumé

Choisissez un nom et un emplacement pour cet ordinateur virtuel.


Le nom est affiché dans le Gestionnaire Hyper-V. Nous vous recommandons d'utiliser un nom qui vous permettra d'identifier facilement cet ordinateur virtuel, tel que le nom de la charge de travail ou du système d'exploitation invité.

Nom :

Vous pouvez créer un dossier ou utiliser un dossier existant pour stocker l'ordinateur virtuel. Si vous ne sélectionnez pas de dossier, l'ordinateur virtuel est stocké dans le dossier par défaut configuré pour ce serveur.

☐ Stocker l'ordinateur virtuel à un autre emplacement

Emplacement :

 Si vous envisagez de créer des points de contrôle de cet ordinateur virtuel, choisissez un emplacement avec un espace libre suffisant. Les points de contrôle induent les données des ordinateurs virtuels et peuvent nécessiter un espace considérable.

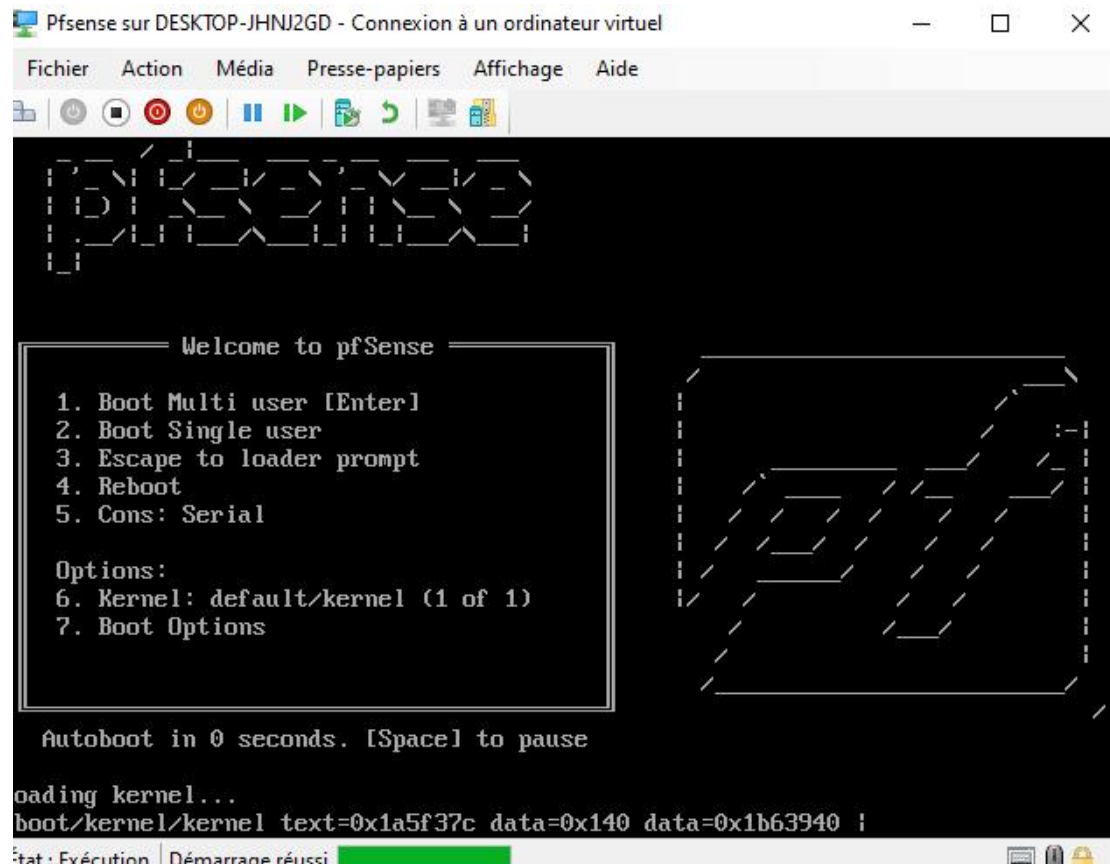
< Précédent

Suivant >

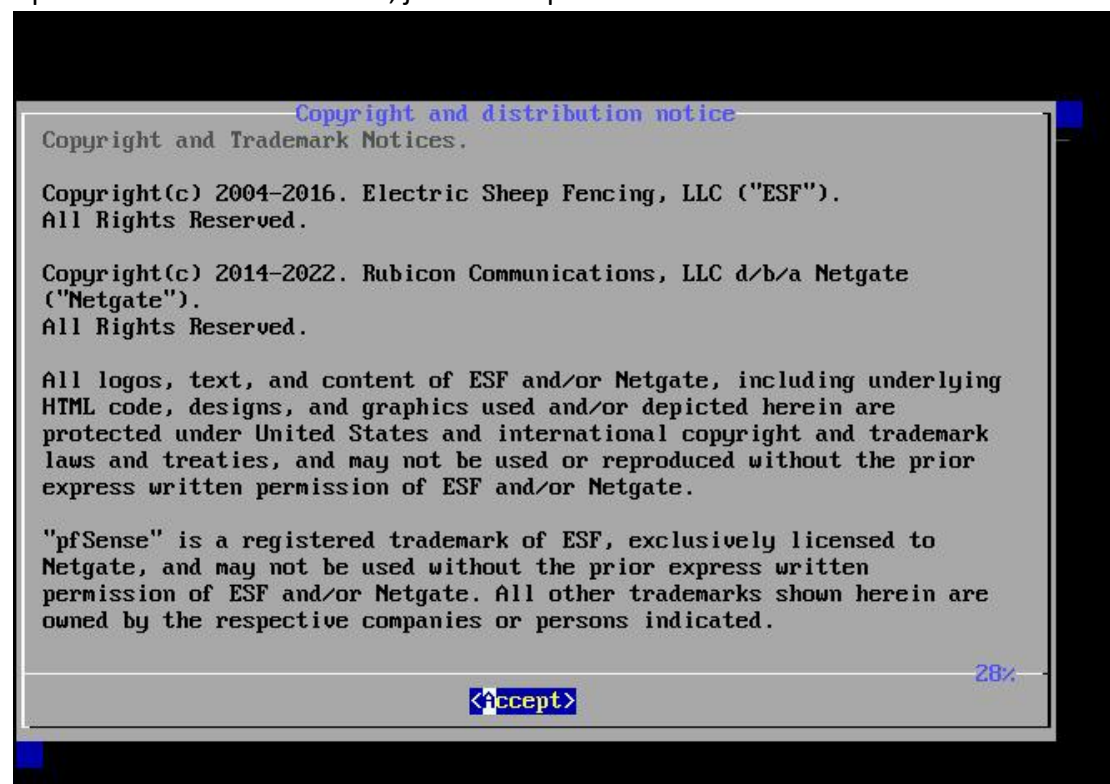
Terminer

Annuler

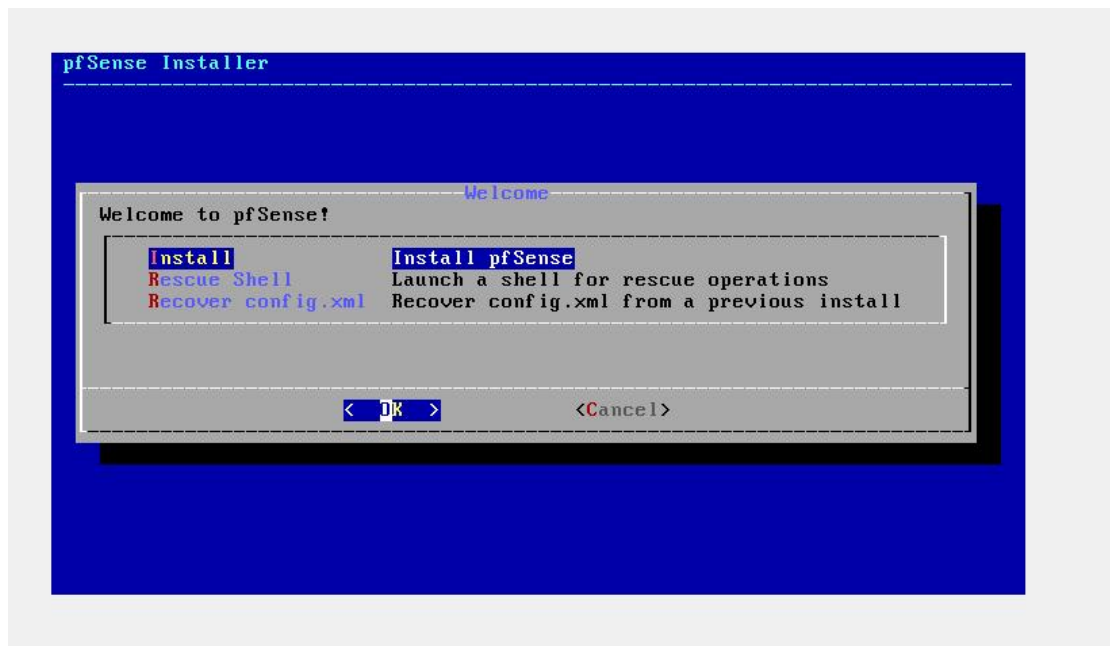
J'ai ensuite sélectionné l'ISO de Pfsense et j'ai démarré ma VM:
La machine démarre:



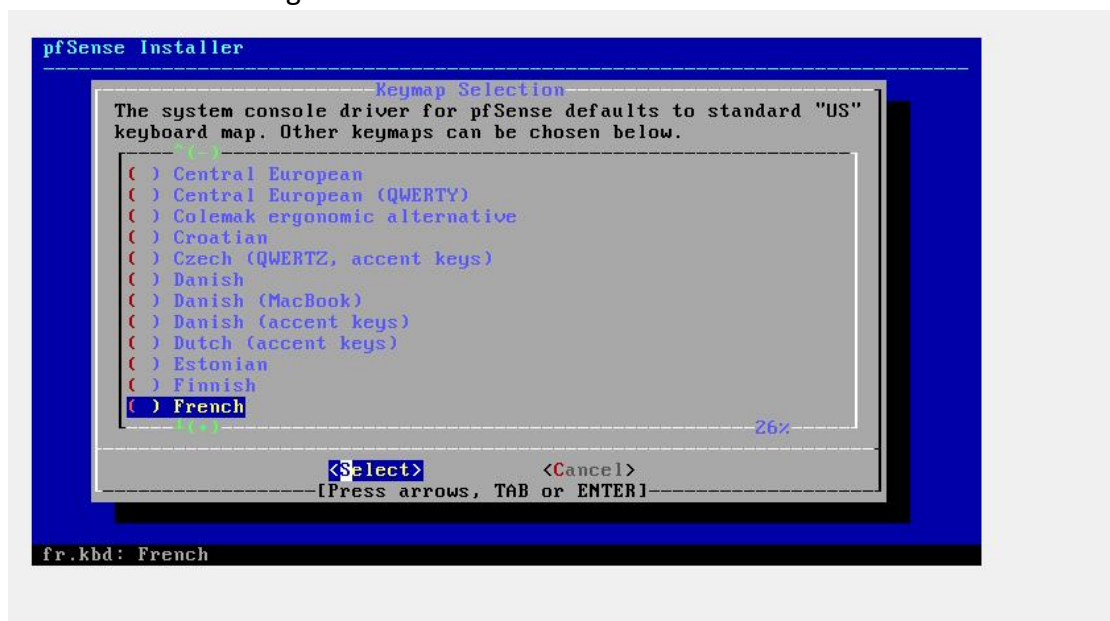
Après l'avoir laissé démarrer, j'ai du accepter le conditions de Pfsense



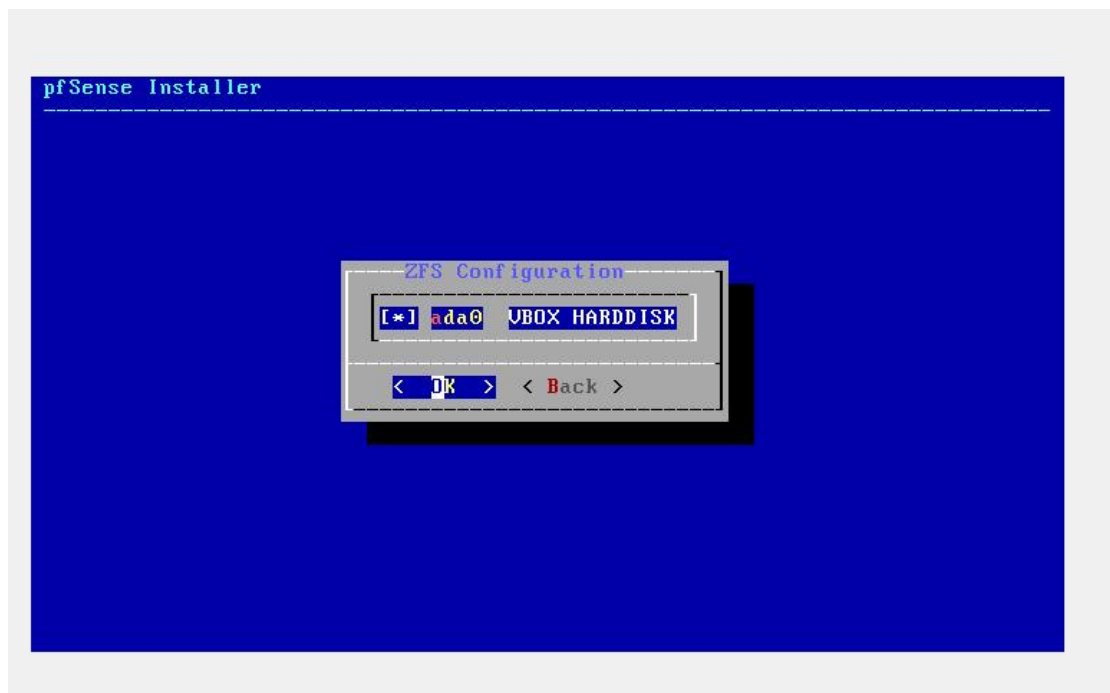
Une fois ces conditions accepté, j'ai sélectionné «Install Pfsense» car je veux l'installé



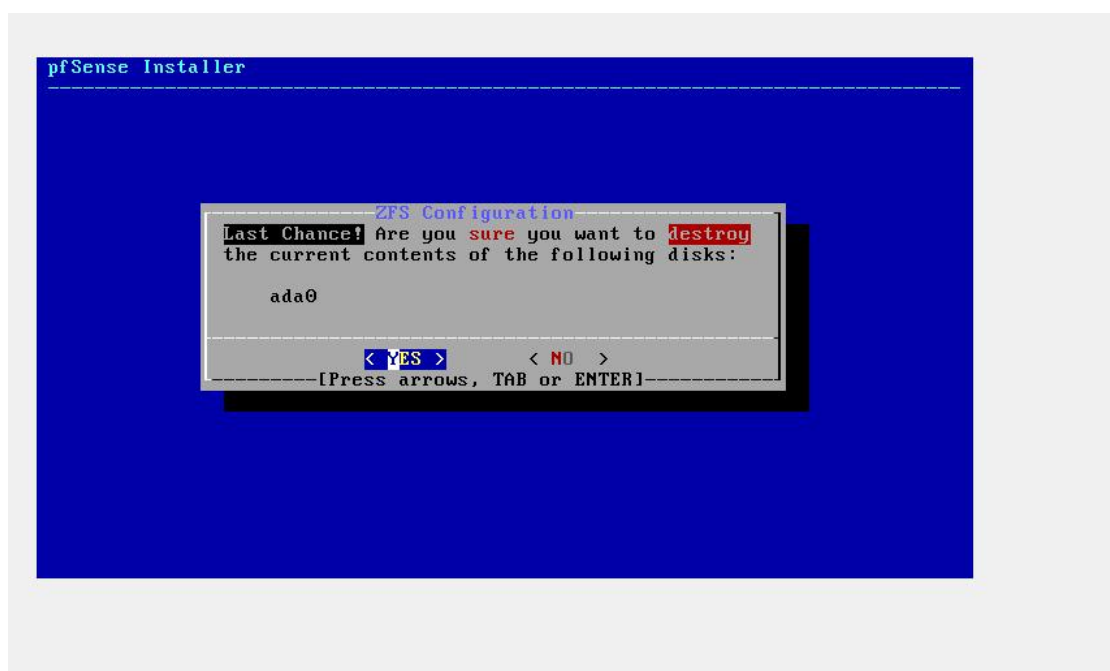
Je selectionne ma langue «Francais»



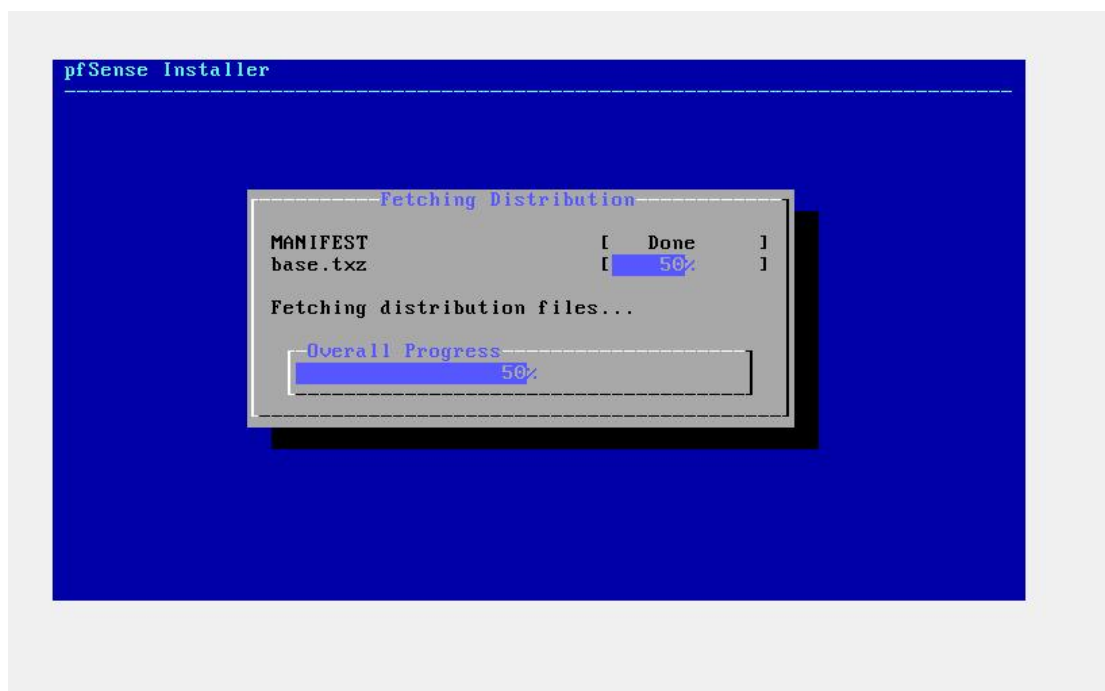
Je selectionne mon disque en appuyant sur «Espace» (Nous avons ramer sur cette étape, avec l'habitude d'appuyer sur la touche «entrée» pour selectionné, nous somme resté pendant plus de 1h30 min a comprendre cette étape)



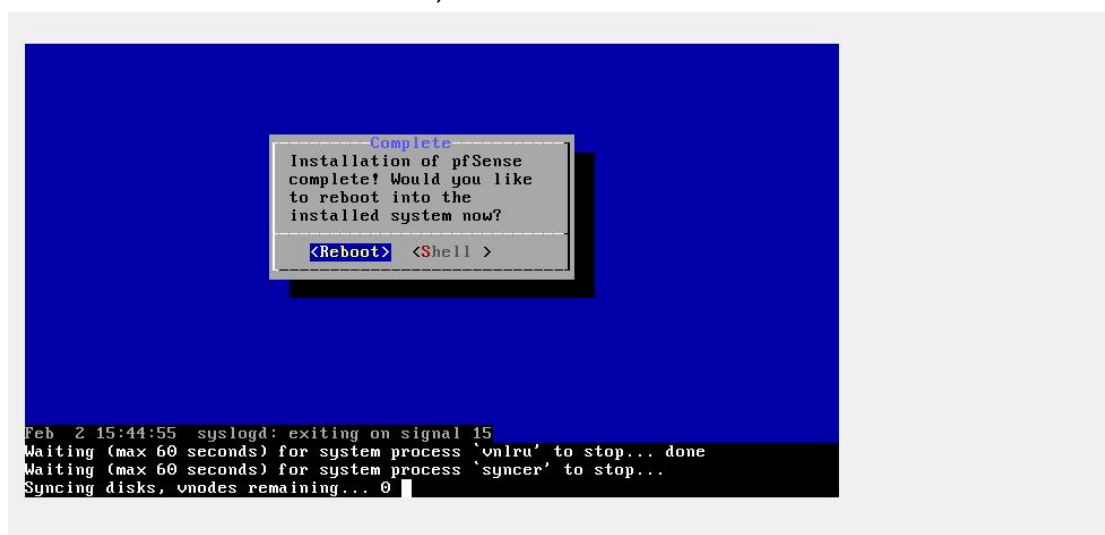
Une fois le disque sélectionner, il va tout supprimer sur ce disque. (Ici, j'ai créé un disque virtuel donc je risque rien)



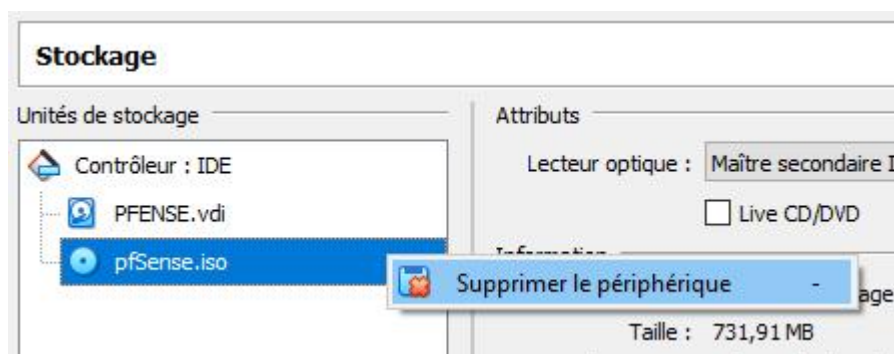
Il s'installe



Et une fois l'installation terminée, il va redémarrer



Ensuite, dès qu'il redémarre, j'ai éteint directement la VM pour retirer l'ISO sinon celui-ci va redémarrer sur l'ISO et va reproceder a l'installation. Évidement c'est ce que nous voulons pas donc on va proceder a l'éjection de l'ISO



Pfsense Configuration:

Une fois l'ISO supprimer, on redémarre la VM et on accède a l'interface 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.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 07a83821e8dfee0a966c

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

WAN (wan)      -> em0      -> v4/DHCP4: 172.20.32.176/20
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: 
```

Une fois cela fait, on va définir l'IP de l'interface. Pour cela on va appuyer sur 2 et entre l'adresse IP

```
WAN (wan)      -> em0      -> v4/DHCP4: 172.20.32.176/20
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: 2

Available interfaces:

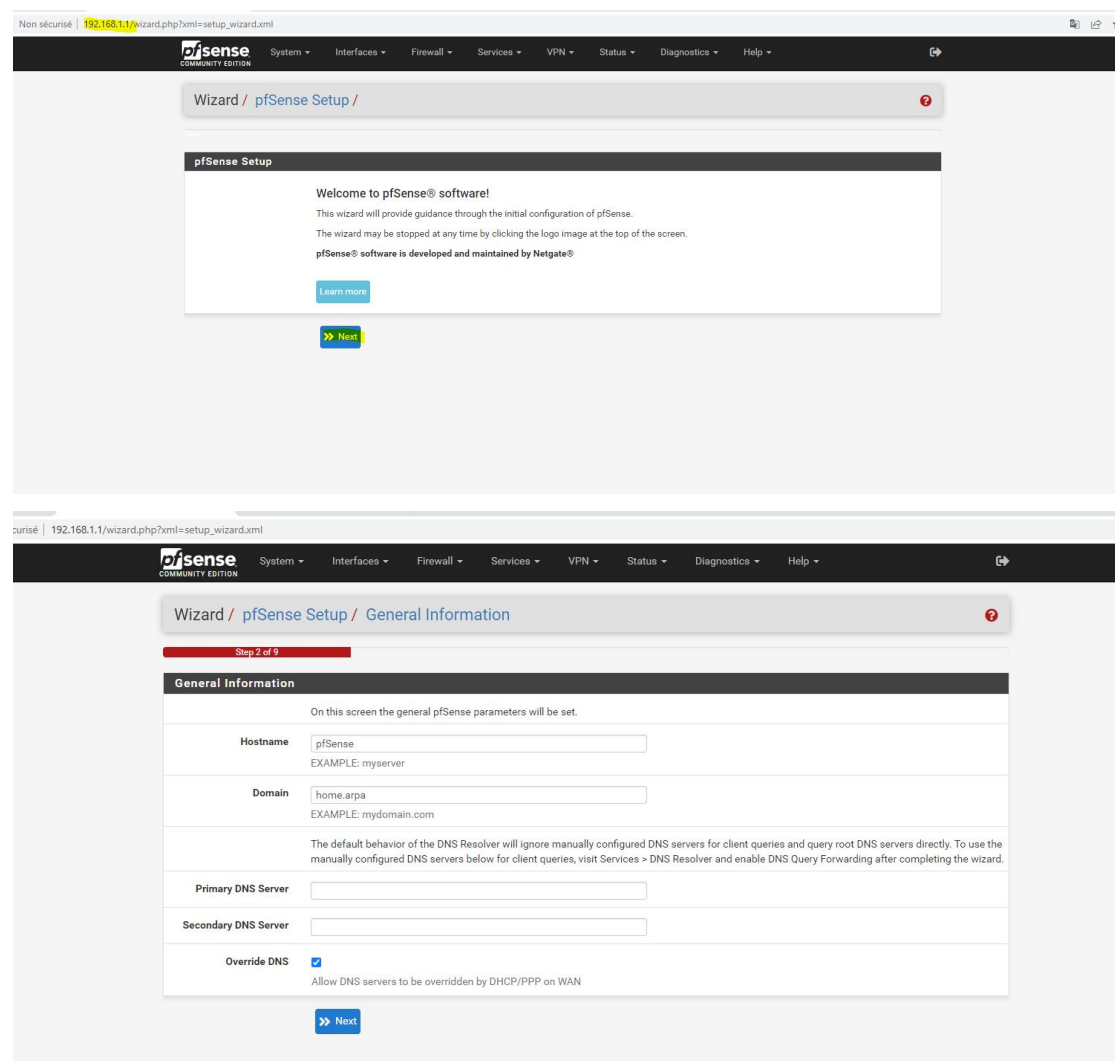
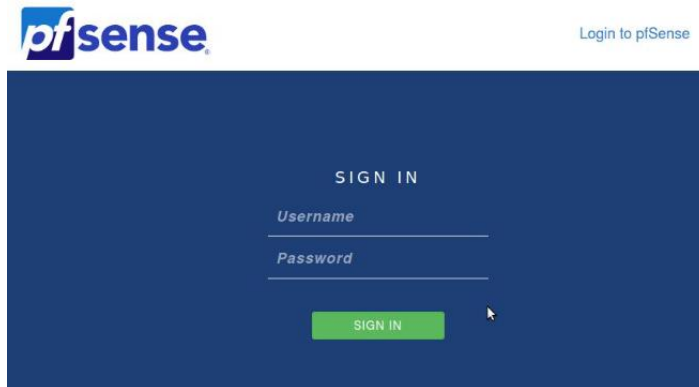
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

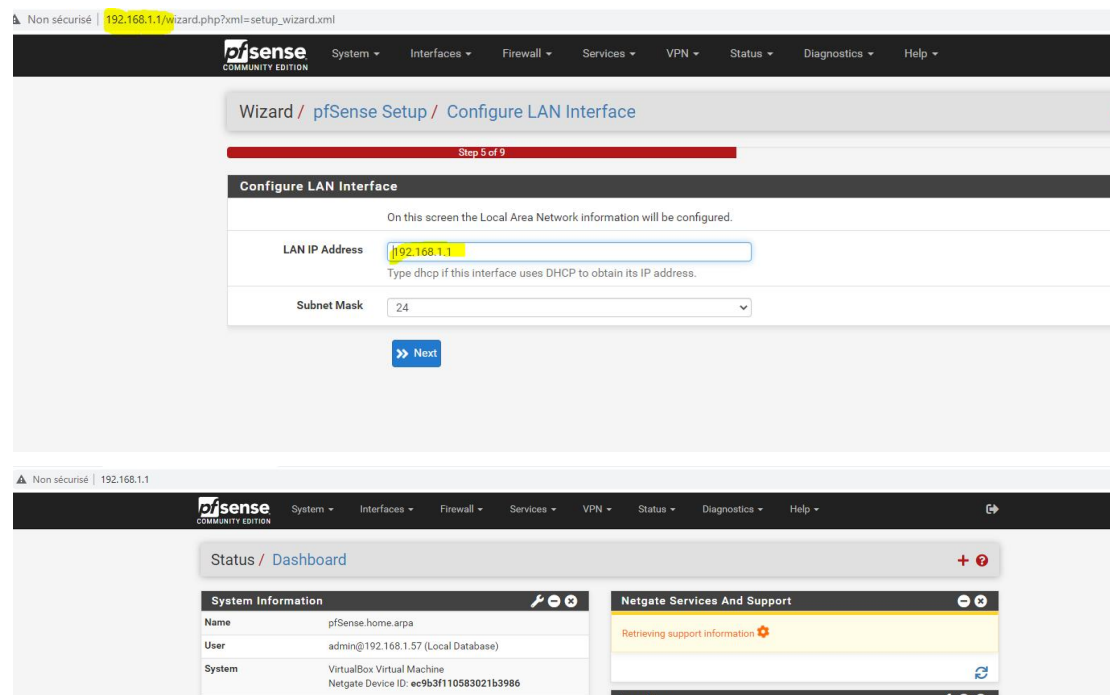
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.4.254
```

Pour configurer le portail captif, nous nous sommes connectés en web à notre VM PFSENSE, pour ce faire, il suffit de se rendre sur un navigateur de recherche et de rentrer l'IP de la VM.

Par défaut, l'identifiant est admin et le mot de passe est pfsense.



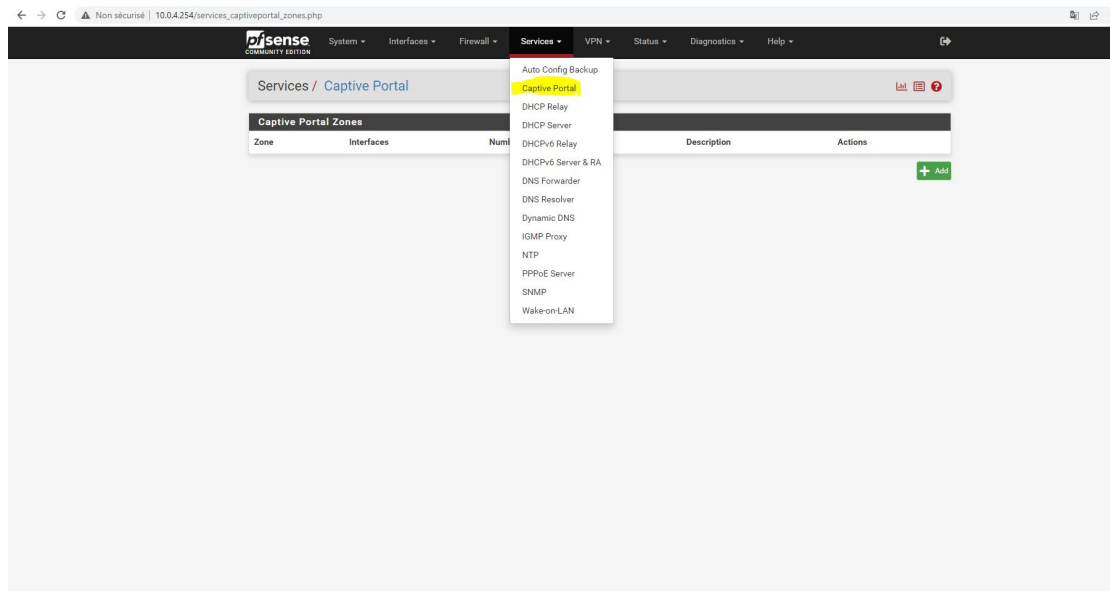
Nous donnons une adresse IP a notre LAN



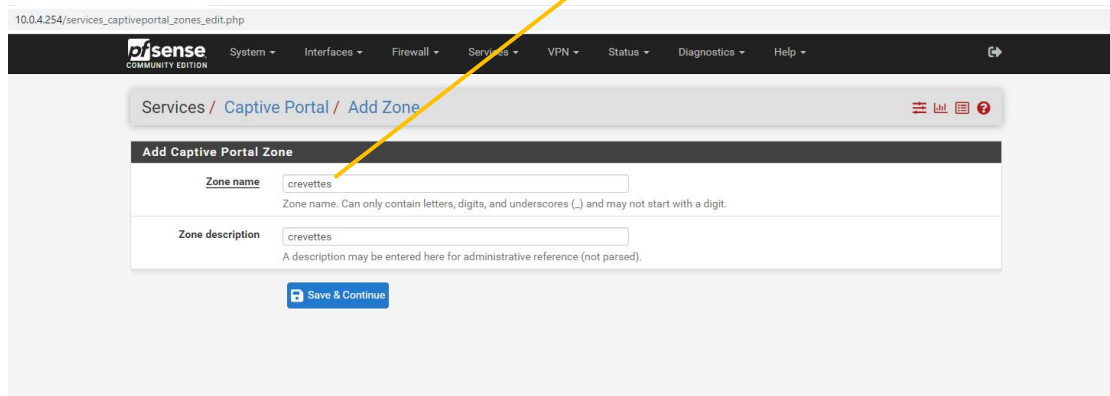
Depuis ce Dashboard nous pouvons par exemple modifier les interfaces en allant dans l'onglet « Interfaces ».

Portail Captif:

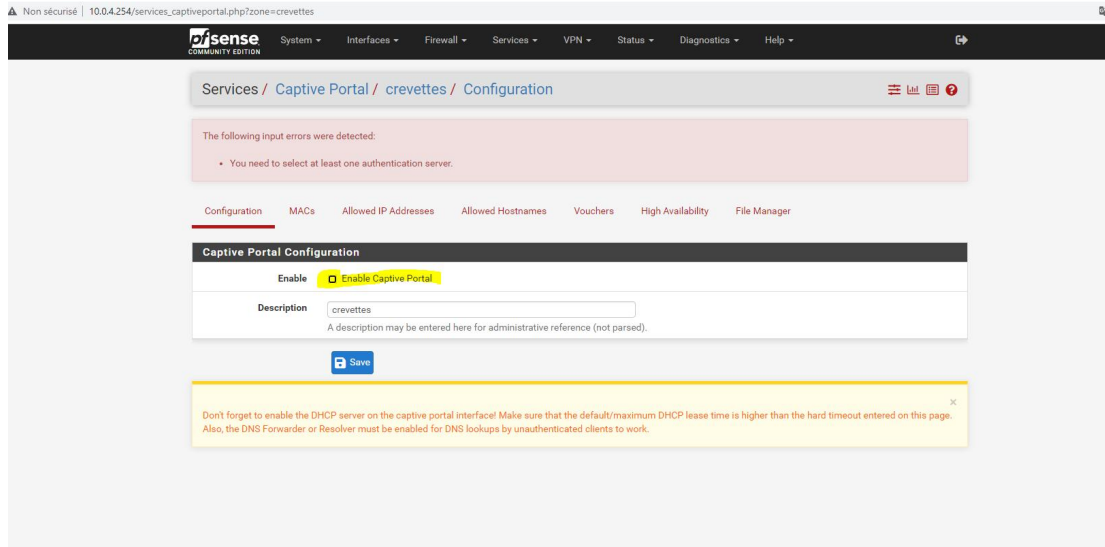
Ensuite, une fois que j'accède a Pfsense, je vais directement créer mon portail captif pour cela je me rend *service/ Captive Portal* et puis add



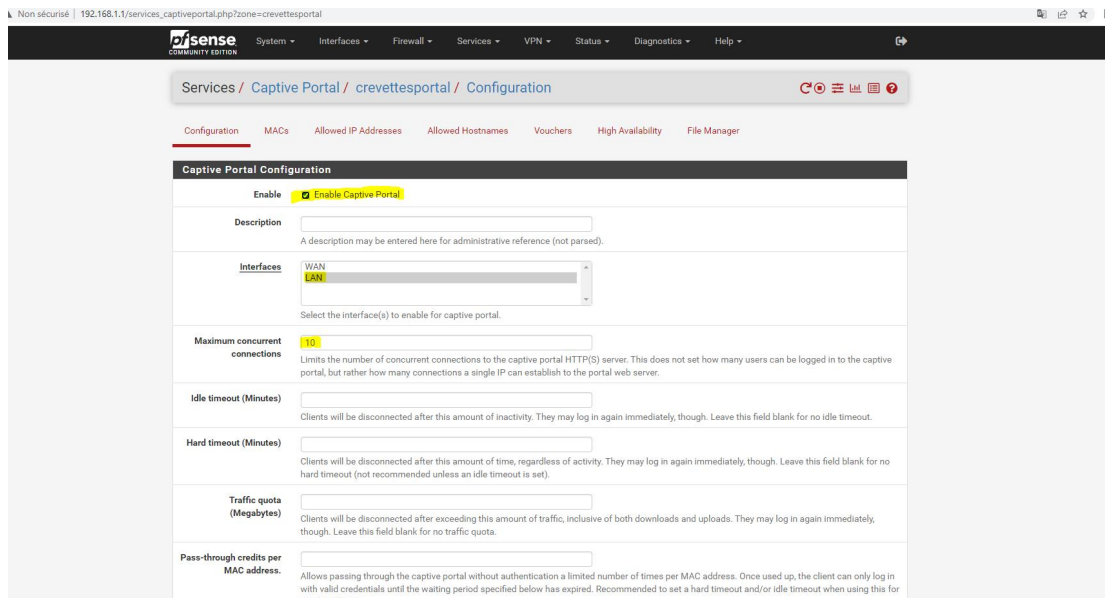
Je vais tombé sur cette ou je vais renseigné le nom et la description de mon portail captif



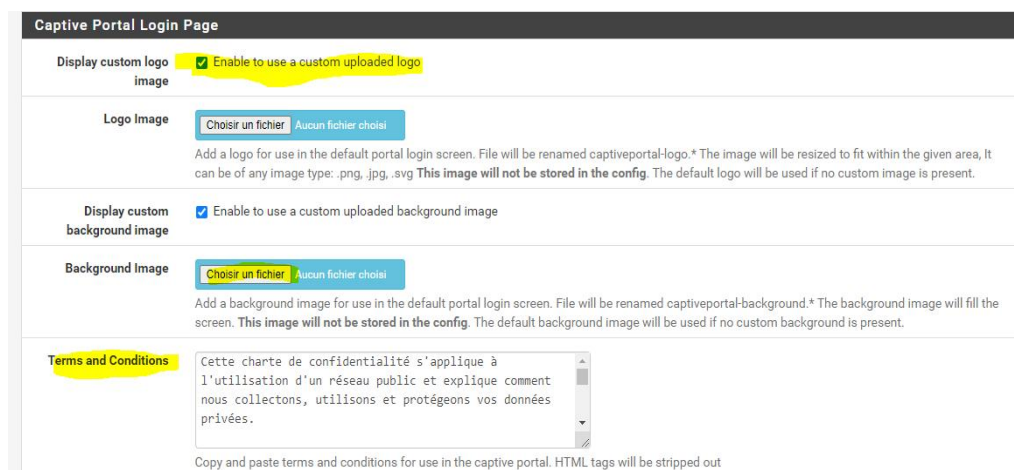
Une fois le nom de ma borne trouver «crevettes», je vais sauvegarde et activer le portail captif



Une fois activé, j'ai limité le nombre de connexion a 10 et j'ai mis sur l'interface LAN que j'ai crée auparavant



Une fois cela fait, j'ai mis mon image de fond et un logo. J'ai aussi mis la charte de confidentialité de notre réseau (Partie Juridique)



Authentication

Authentication Method Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server Local Database

You can add a remote authentication server in the [User Manager](#).
Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

Secondary authentication Server Local Database

You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs.
This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

Reauthenticate Users ☐ Reauthenticate connected users every minute

If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in. The cached credentials are necessary for the portal to perform automatic reauthentication requests.

Local Authentication Privileges ☒ Allow only users/groups with "Captive portal login" privilege set

HTTPS Options

Login ☐ Enable HTTPS login

When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

[Save](#)

Par la suite, nous avons accéder au portail. Pour cela j'ai mis dans la barre de recherche :

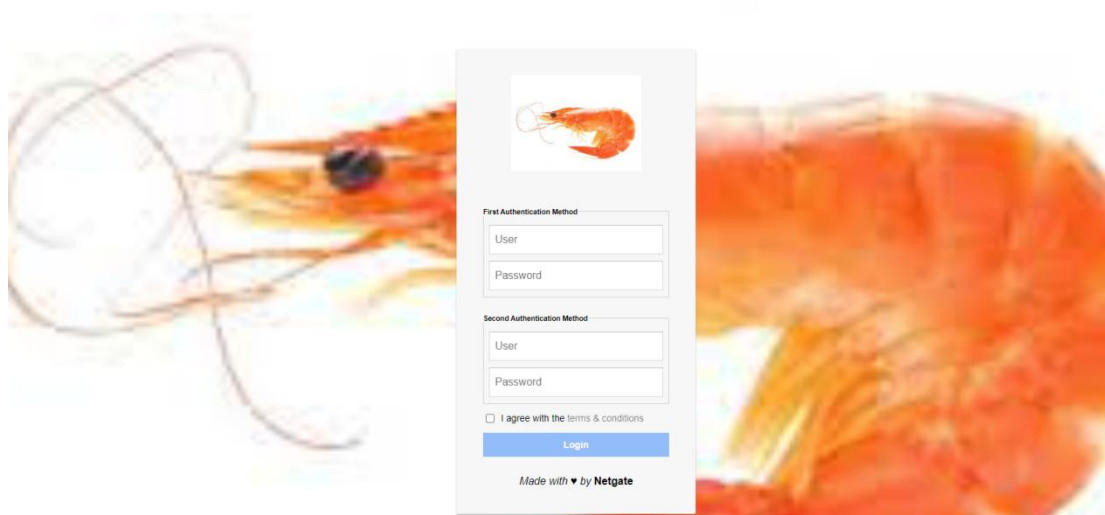
192.168.1.1 (L'adresse de notre Pfsense)


:8002 (Le port de notre portail Captif)

/?zone=crevettesportal (Le nom de notre portail)

Merci a notre chère camarade Baptiste pour cette solution

Non sécurisé | 192.168.1.1:8002/?zone=crevettesportal





First Authentication Method

User

Password


Second Authentication Method

User

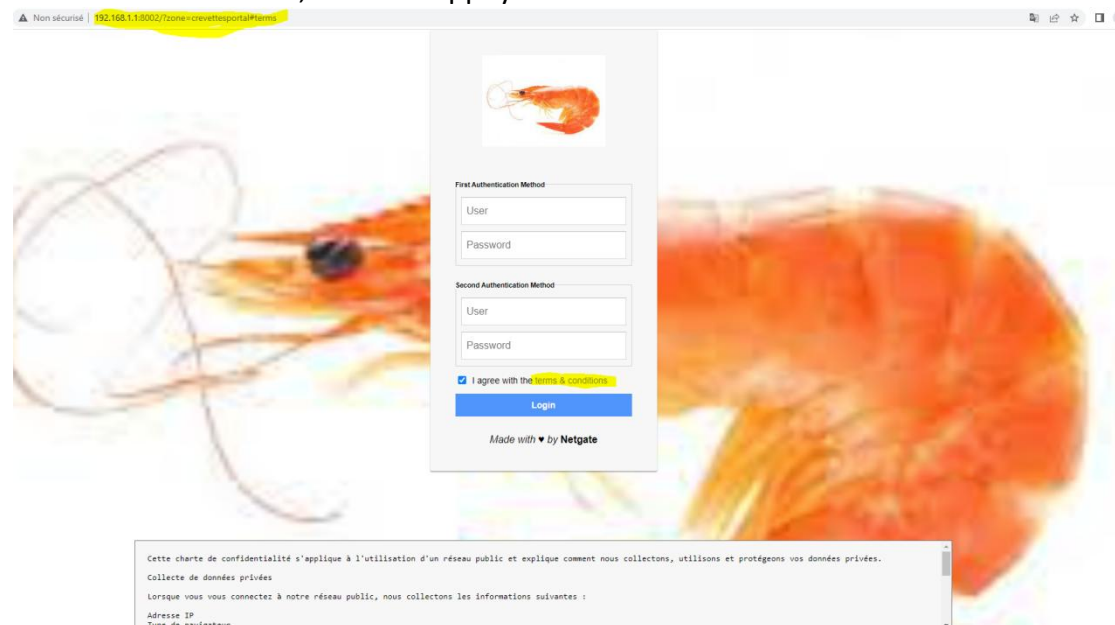
Password

☐ I agree with the terms & conditions

[Login](#)

Made with  by Netgate

Pour voir notre charte, il suffit d'appuyer sur «terms et conditions»



Non sécurisé | 192.168.1.1:8002/zone=crochetportalPfense

First Authentication Method

User

Password

Second Authentication Method

User

Password

☒ I agree with the terms & conditions

Login

Made with by Netgate

Cette charte de confidentialité s'applique à l'utilisation d'un réseau public et explique comment nous collectons, utilisons et protégeons vos données privées.

Collecte de données privées

Lorsque vous vous connectez à notre réseau public, nous collectons les informations suivantes :

Adresse IP

Type de navigateur

On peut voir notre charte de confidentialité

Partie Juridique:

Cette charte de confidentialité s'applique à l'utilisation d'un réseau public et explique comment nous collectons, utilisons et protégeons vos données privées.

1- Collecte de données privées :

Lorsque vous vous connectez à notre réseau public, nous collectons des informations comme votre adresse IP, le type de navigateur, cela permet d'être utilisé pour améliorer la qualité de notre réseau public et pour assurer la sécurité de nos utilisateurs.

2- Utilisation des données privées

Nous n'utilisons pas vos données privées à des fins commerciales. Nous ne partageons pas vos données avec des tiers sans votre consentement explicite. Nous ne vendons pas vos données à des annonceurs. Vous avez le droit de savoir quelles données nous collectons à votre sujet. Vous pouvez demander à accéder à ces données et à les modifier si elles sont inexacts. Vous pouvez également demander à ce que vos données soient supprimées.

3- En créant un compte sur ce réseau Pfense, vous acceptez donc toutes ces conditions d'utilisation et vous vous engagez à les respecter

Si vous avez des questions sur notre charte de confidentialité ou sur la collecte de vos données privées, veuillez nous contacter à l'Administrateur