

## **RAPPORT DEPLOIEMENT D'UN PORTAIL CAPTIF EN UTILISANT PFSense**

**EKRA EPHRAÏM MELCHISEDEK**

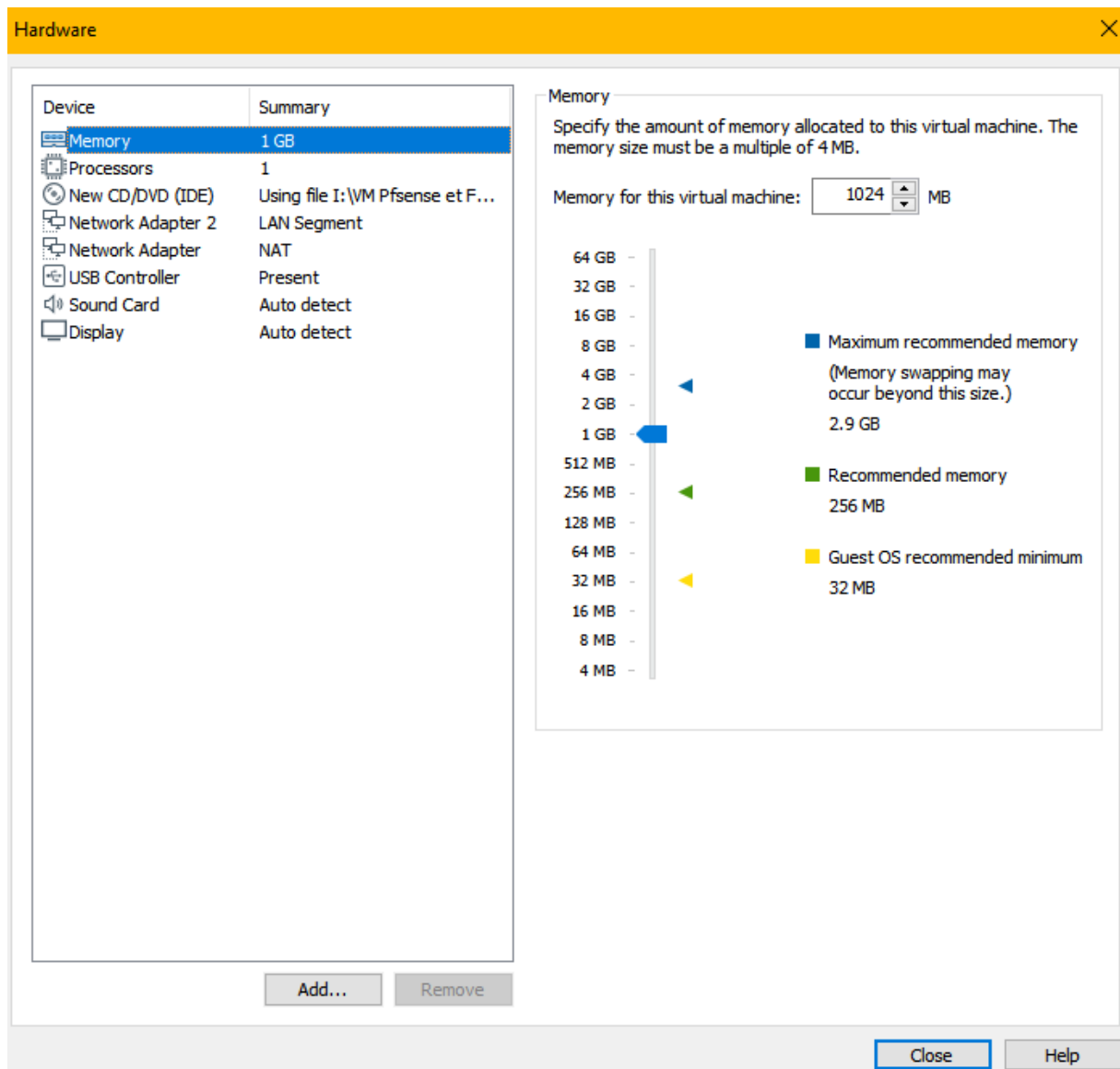
**TAH JOEL GUELASSE NEHEMIE**

**SOW ABDOULAYE**

**KOUAKOU YAO FRANCK**

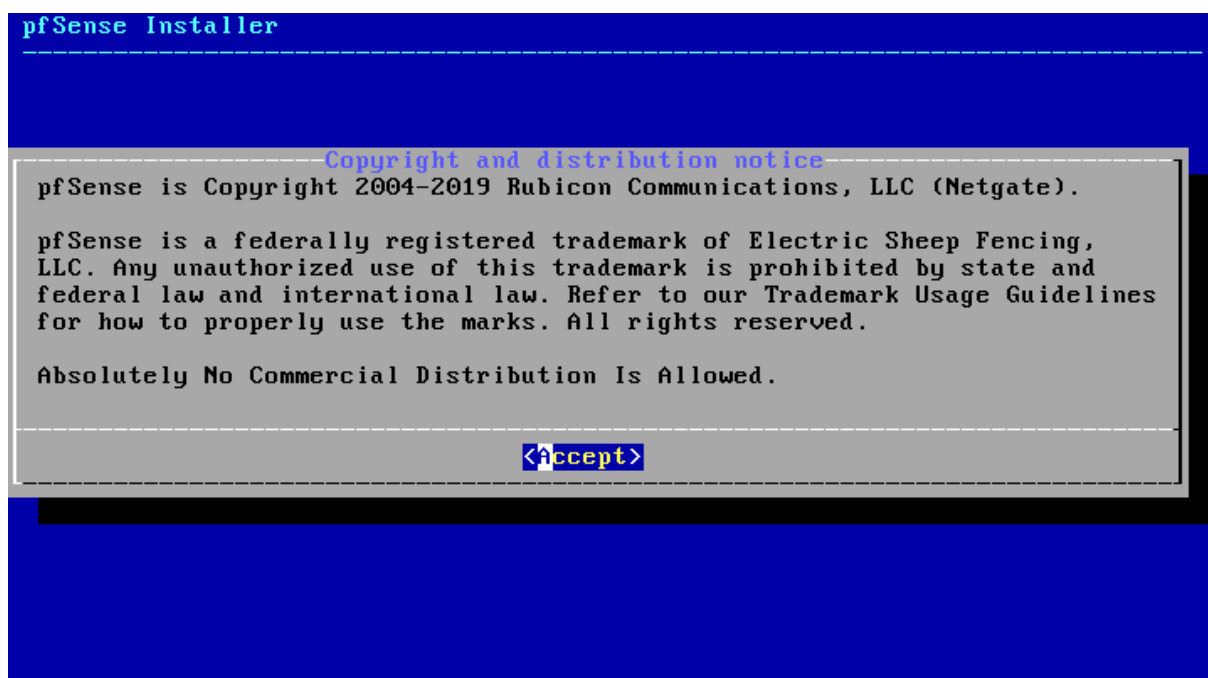
Pour ce travail, nous allons utiliser le logiciel de virtualisation VMWare. Nous allons avant tout créer la machine virtuelle, celle du pare-feu pfsense. Pour ce qui est des caractéristiques de la machine, nous donnons :

- 1 GB à la RAM
- 1 Processeur
- 30 GB de mémoire de stockage
- 2 cartes réseau dont une carte réseau connecté en NAT et la seconde carte réseau en LAN SEGMENT.



Une fois toutes ces configurations effectuées, on lance la machine virtuelle et on procède à l'installation du pare-feu.

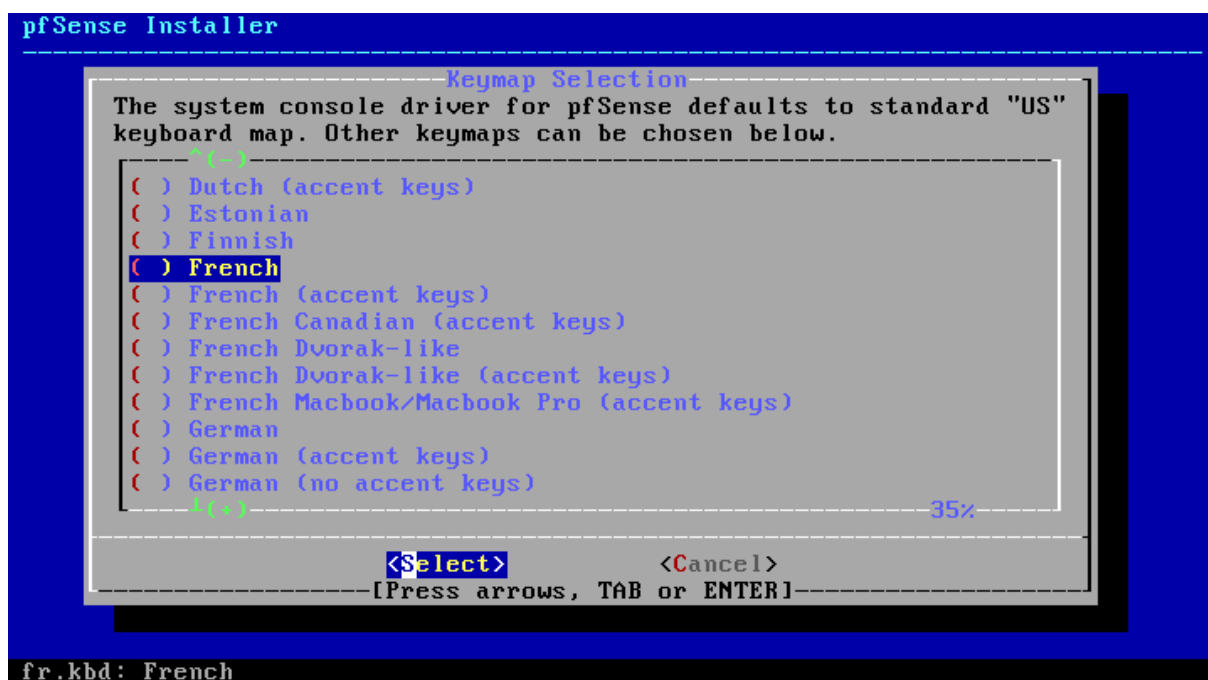
Avant tout, il faut d'abord accepter la licence. A ce niveau là, nous n'avons pas accès à la souris, nous allons donc principalement utiliser le clavier. Nous allons donc cliquer sur la touche **Entrer** afin d'accepter la licence.



Ensuite, nous allons lancer l'installation de pfsense de manière proprement dite. Nous allons donc cliquer sur la touche **Entrer** encore une fois.

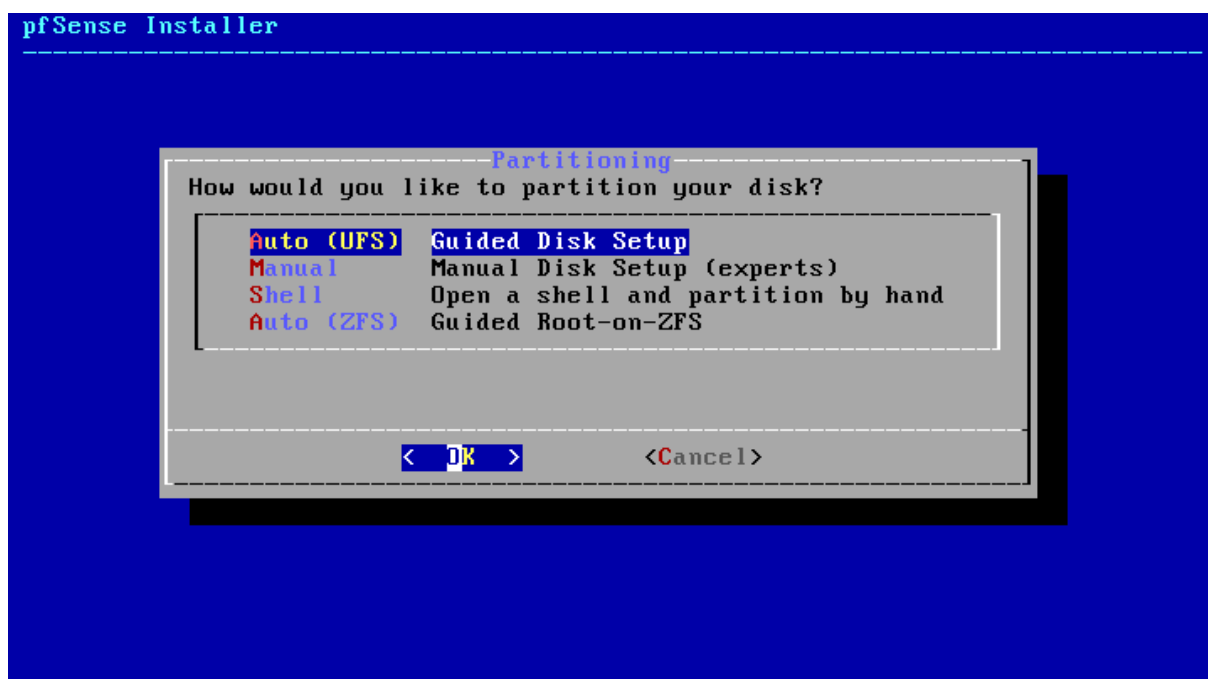


Ensuite, il va falloir choisir la langue du clavier. Dans notre cas, nous allons prendre **French**. Pour choisir French, nous allons descendre jusqu'à atteindre les langues commençant par F. Puis nous allons cliquer sur la touche **Entrer**.

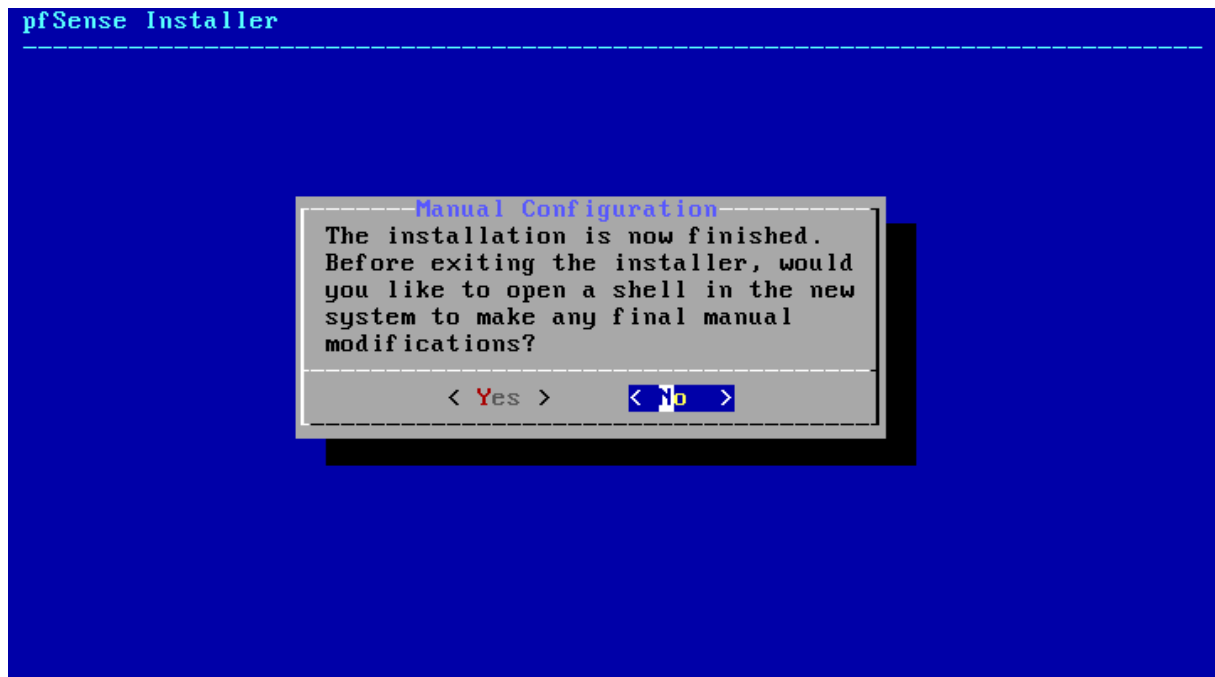


Une fois la langue sélectionnée, nous allons remonter tout en haut puis appuyer sur la touche entrer lorsque nous serons sur la première option.

Nous tombons par la suite sur le cas des partitions du disque, nous choisirons la première option. Nous allons donc cliquer sur la touche **Entrer**, cela lancera donc l'installation de pfsense.

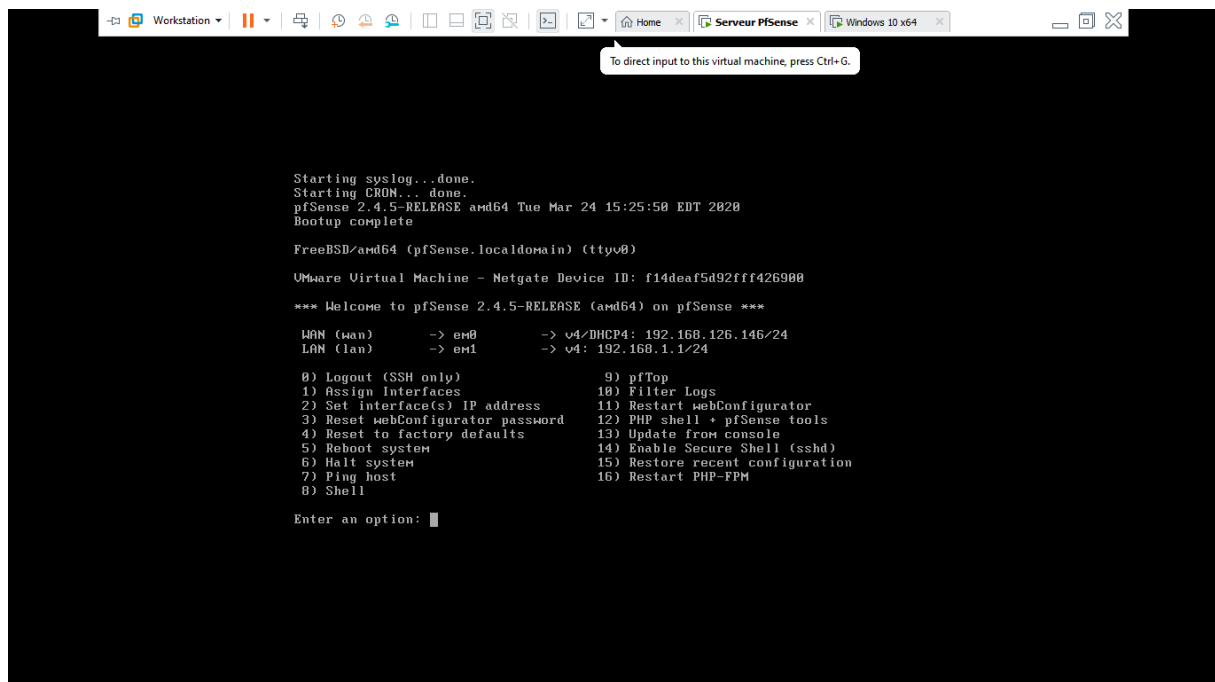


L'installation terminée, nous allons choisir l'option **No** afin de nous permettre de pouvoir redémarrer la machine pour commencer à l'utiliser.

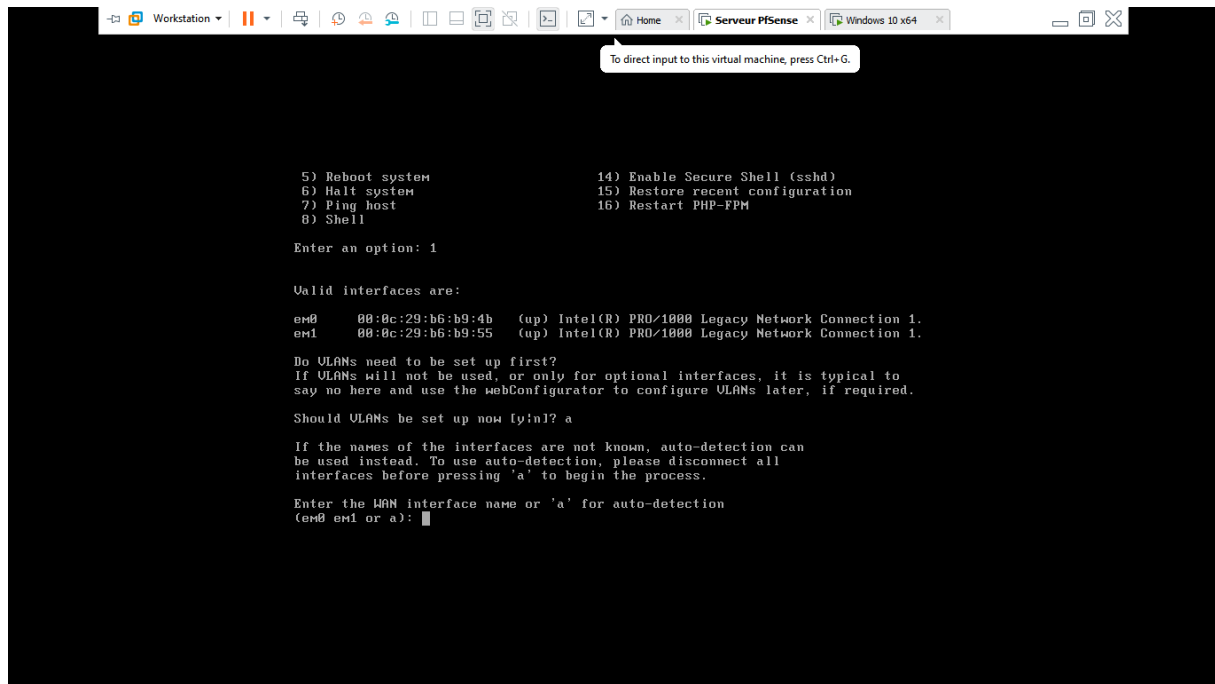


Nous allons enfin choisir l'option **Reboot** afin de redémarrer la machine pour qu'elle soit à présent utilisable.

Nous arrivons à présent sur l'interface de pfsense



Pour débiter nous allons cliquer sur l'option 1 afin d'assigner une interface au LAN et une interface au WAN.



```
5) Reboot system
6) Halt system
7) Ping host
8) Shell
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: 1

Valid interfaces are:

em0  00:0c:29:b6:b9:4b  (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1  00:0c:29:b6:b9:55  (up) Intel(R) PRO/1000 Legacy Network Connection 1.

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.

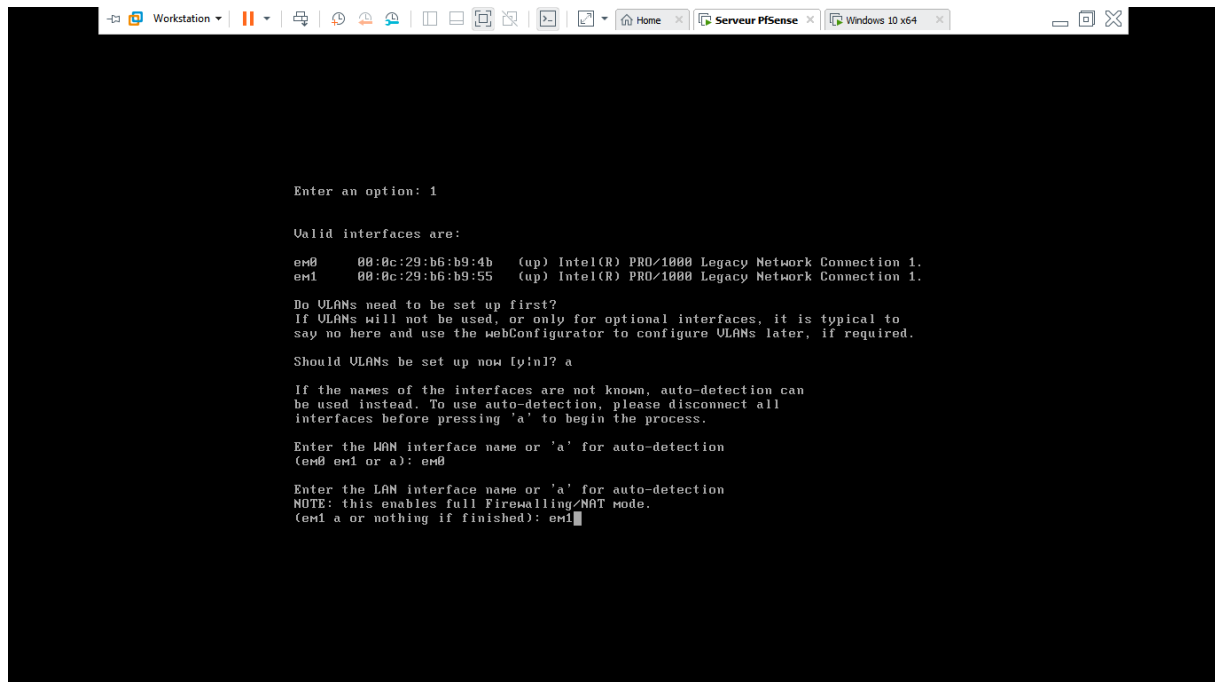
Should VLANs be set up now [y:n]? a

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
(em0 em1 or a):
```

L'option "a" est valable dans le cas où on n'a plus d'une interface car par défaut, les interfaces à partir de la 3eme sont éteinte. L'option "a" permet donc d'effectuer une auto-détection des interfaces.

L'assignation des interfaces commence par le WAN, dans notre cas, nous choisirons "em0" puis cliquerons sur la touche **Entrer**.



```
Enter an option: 1

Valid interfaces are:

em0  00:0c:29:b6:b9:4b  (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1  00:0c:29:b6:b9:55  (up) Intel(R) PRO/1000 Legacy Network Connection 1.

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.

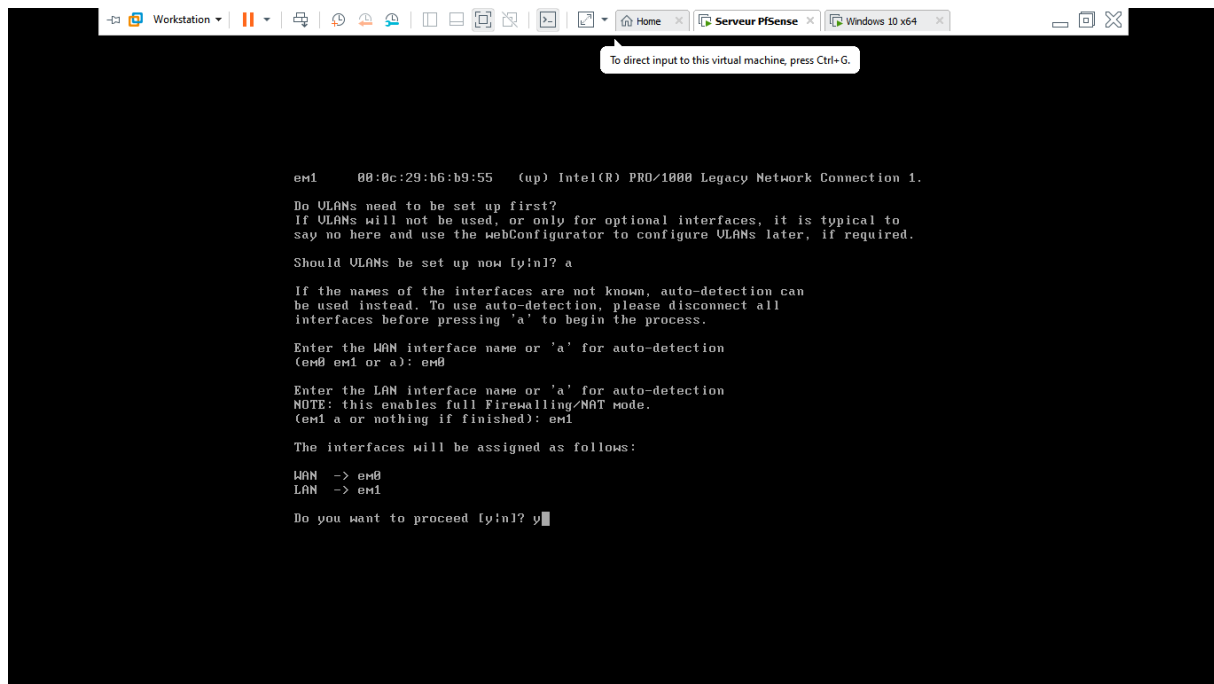
Should VLANs be set up now [y:n]? a

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
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full firewalling/NAT mode.
(em1 a or nothing if finished): em1
```

Ensuite, pour ce qui est du LAN, nous choisirons l'interface "em1".



```
em0  00:0c:29:b6:b9:55  (up) Intel(R) PRO/1000 Legacy Network Connection 1.

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]? a

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
(em0 em1 or a): em0

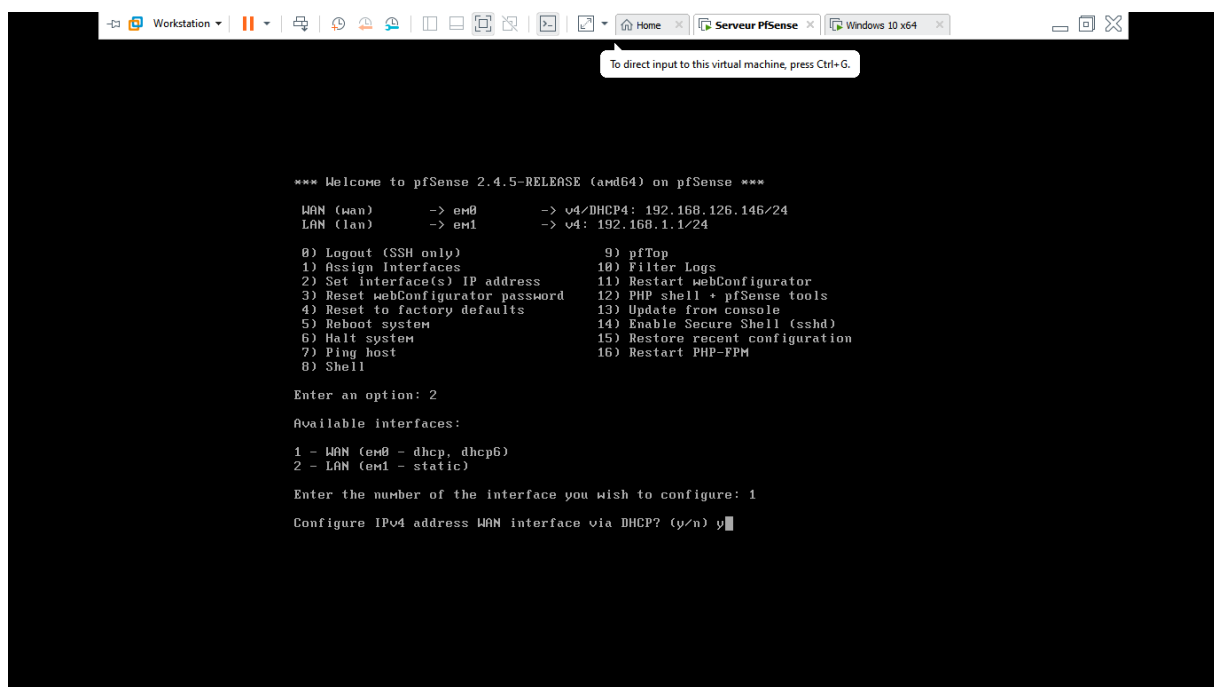
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y/n]? y
```

Nous allons ensuite appuyer la touche **Entrer** afin d’attester nos choix.



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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.126.146/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

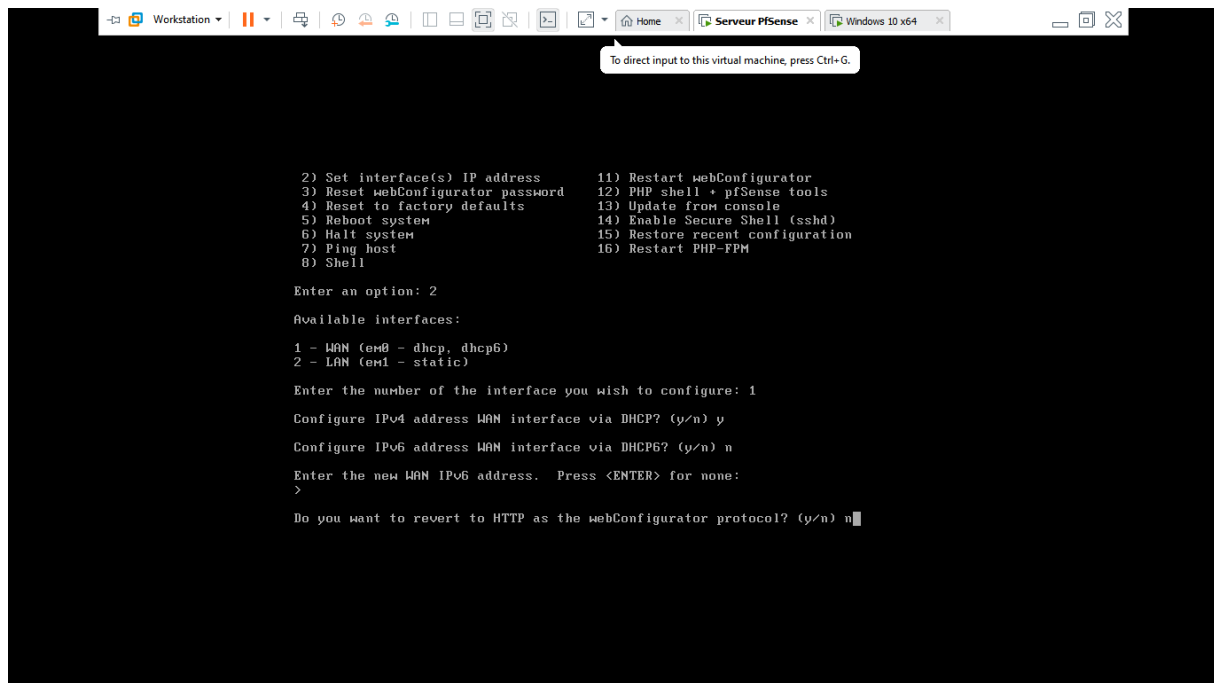
Available interfaces:

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

Enter the number of the interface you wish to configure: 1

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

Une fois les interfaces assignées, nous allons à présent assigner les adresses IP aux différentes interfaces afin de permettre les communications dans le réseau. Nous allons donc choisir l’option “2” qui permet d’assigner les adresses ou le mode d’adressage. Nous allons par la suite choisir l’option “1” afin d’assigner l’interface WAN. Le pare-feu nous demande si on veut configurer l’adressage IPv4 via le service DHCP. Dans notre cas, vu que nous avons choisi le paramètre NAT pour la première carte réseau, nous allons donc choisir l’option “y” qui nous permettra des recevoir les adresses par DHCP (nous avons choisi NAT afin d’avoir accès à internet, on aurait pu choisir BRIDGE, là, nous aurions dû chercher l’adresse du réseau local et fixer dynamiquement l’adresse sur l’interface WAN).



```
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 (ssh)
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)

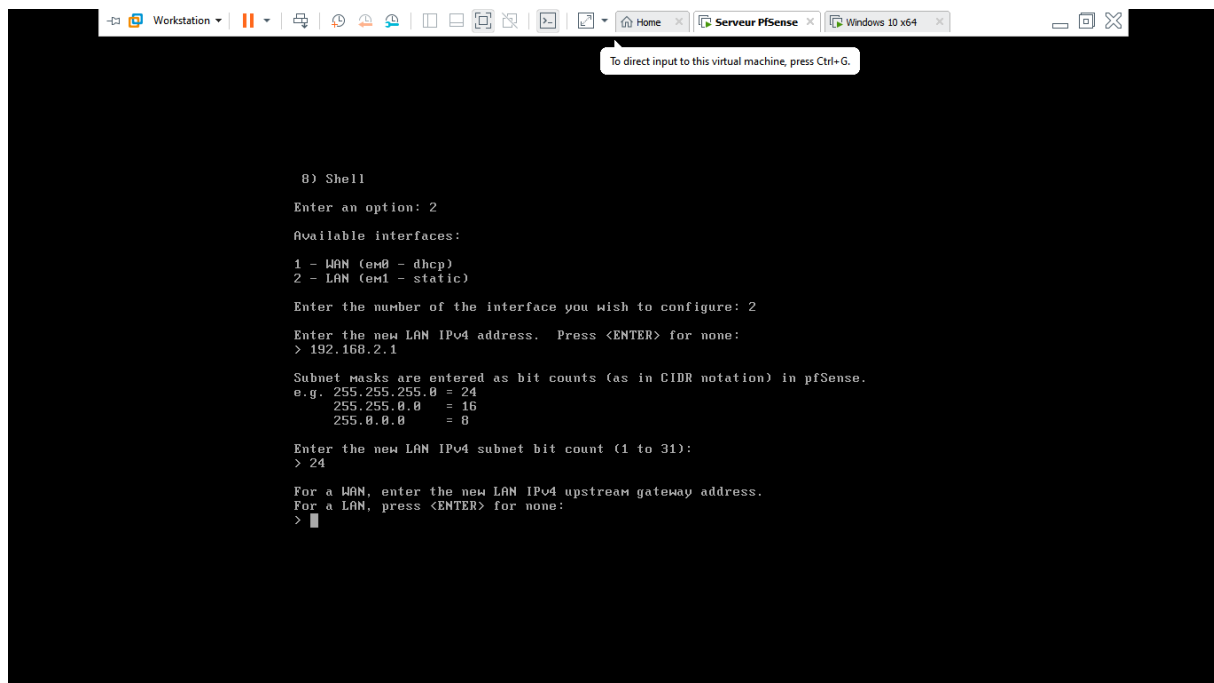
Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>

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

Ensuite, il nous est demandé si nous voulons configurer l’adressage IPv6 via le service DHCP. Dans notre cas, nous choisirons l’option ‘n’. Ensuite, on nous demande l’adresse IPv6, nous cliquerons directement sur **Entrer**.

Par la suite, il nous est demandé si nous voulons permettre la configuration du pare-feu pfsense au travail du protocole http sur l’interface WAN. Nous allons choisir l’option ‘n’.



```
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp)
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:
> 192.168.2.1

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

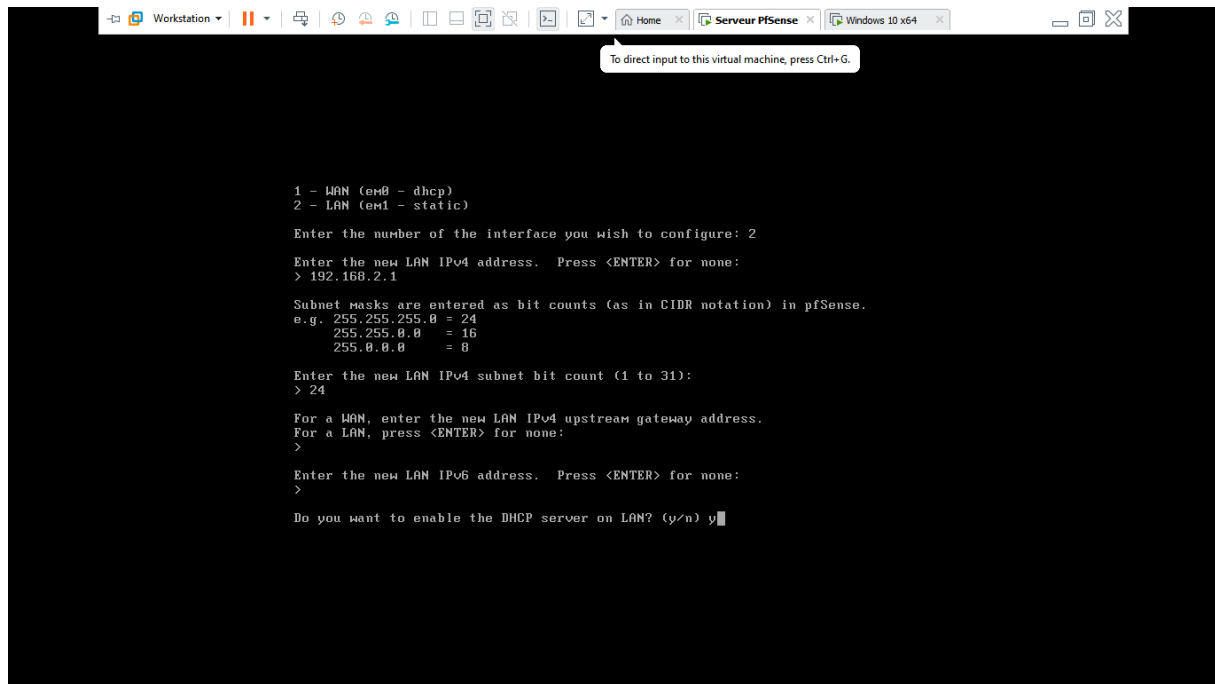
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

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

L’interface WAN configurée, nous allons à présent configurer l’interface LAN. Nous allons donc choisir l’option ‘2’ puis l’option ‘2’ afin de souligner le choix pour la configuration du LAN. Pour le LAN, nous allons assigner statiquement l’adresse. Nous allons d’abord entrer l’adresse IPv4 : **192.168.2.1**. Ensuite nous allons entrer le préfixe pour le masque :



24. Nous n'entrerons pas de passerelle par défaut donc nous cliquerons directement sur Entrer.



```
Workstation | [Icons] | Home | Serveur PfSense | Windows 10 x64
To direct input to this virtual machine, press Ctrl+G.

1 - WAN (em0 - dhcp)
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:
> 192.168.2.1

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

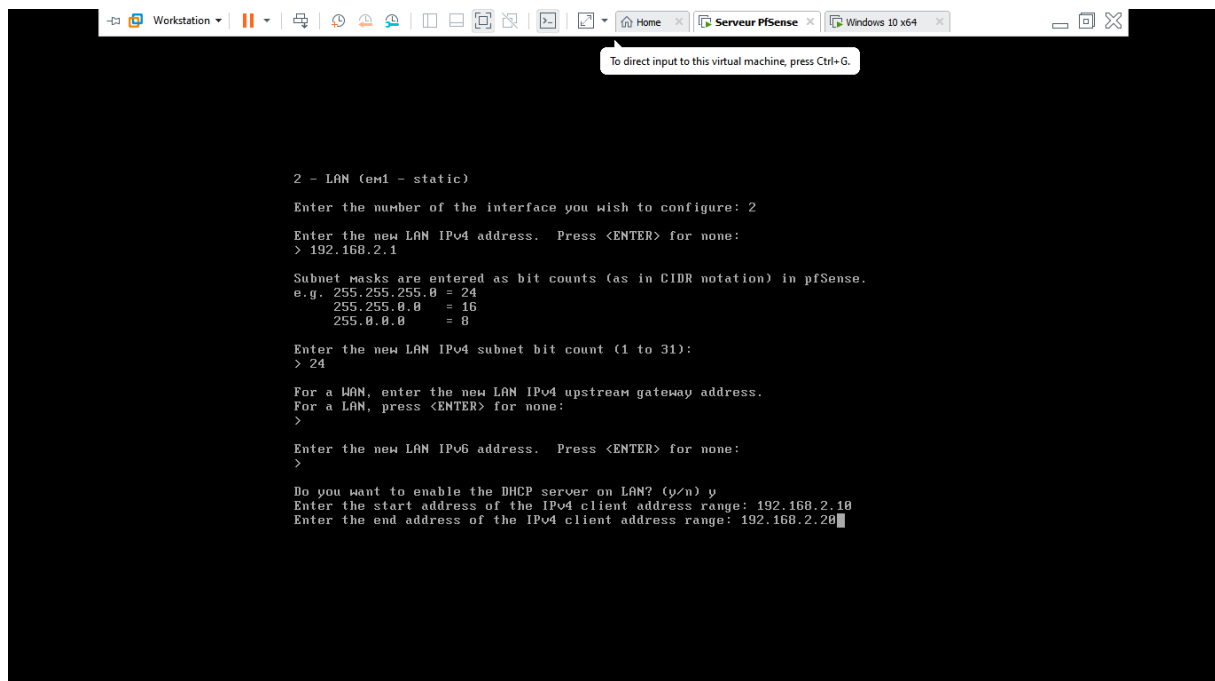
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

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) y
```

Ensuite, il nous est demandé si nous voulons activer le service DHCP sur l'interface LAN afin que les machines reçoivent dynamiquement les adresses IP. Nous choisirons l'option "y" (dans notre cas, il n'y a pas de serveur DHCP autre que celui que nous allons déployer grâce au pare-feu).



```
Workstation | [Icons] | Home | Serveur PfSense | Windows 10 x64
To direct input to this virtual machine, press Ctrl+G.

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:
> 192.168.2.1

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 31):
> 24

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) y
Enter the start address of the IPv4 client address range: 192.168.2.10
Enter the end address of the IPv4 client address range: 192.168.2.20
```

Nous allons ensuite entrer la plage d'adresse. Nous débuterons par l'adresse : **192.168.2.10** et finirons par l'adresse **192.168.2.20**

```
Workstation | Server PfSense | Windows 10 x64
To direct input to this virtual machine, press Ctrl+G.

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.1

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 31):
> 24

For a LAN, 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) y
Enter the start address of the IPv4 client address range: 192.168.2.10
Enter the end address of the IPv4 client address range: 192.168.2.20
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Ensuite, il nous est demandé si nous voulons permettre la configuration de pfsense via le protocole http sur l'interface LAN. Nous choisirons l'option 'y', puis nous cliquerons sur **Entrer**.

```
Workstation | Server PfSense | Windows 10 x64
To direct input to this virtual machine, press Ctrl+G.

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: 7

Enter a host name or IP address: 8.8.8.8

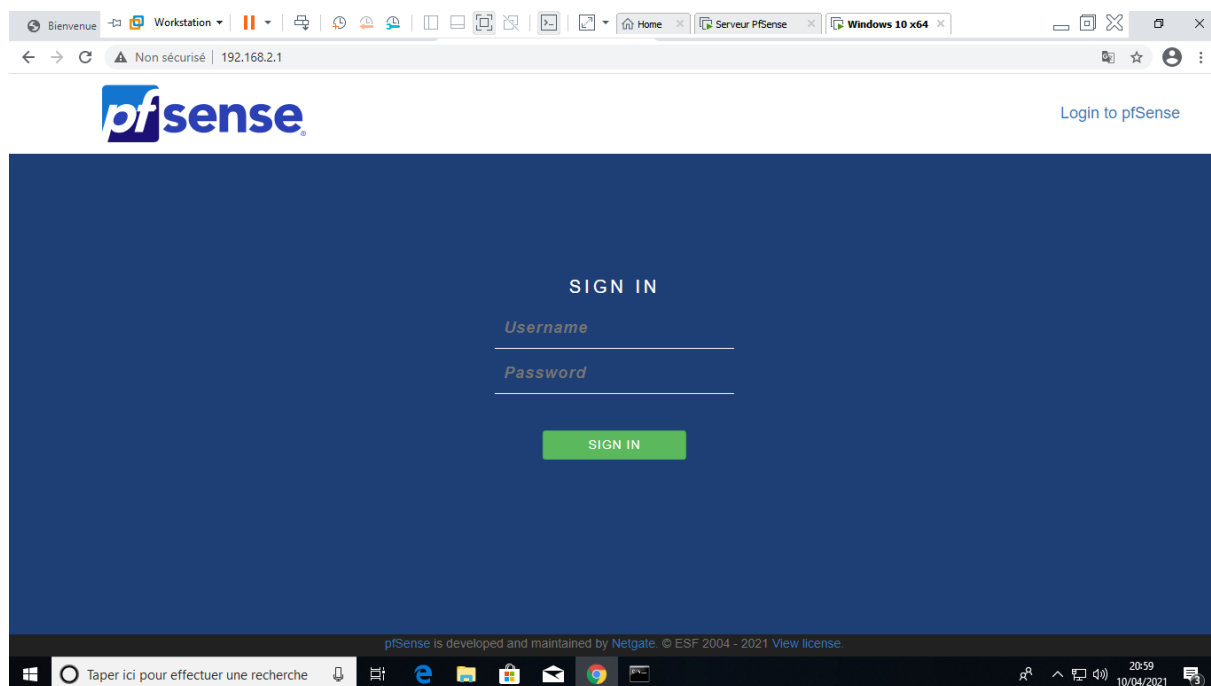
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=124.076 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=122.194 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=136.987 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 122.194/127.726/136.987/6.537 ms

Press ENTER to continue.
```

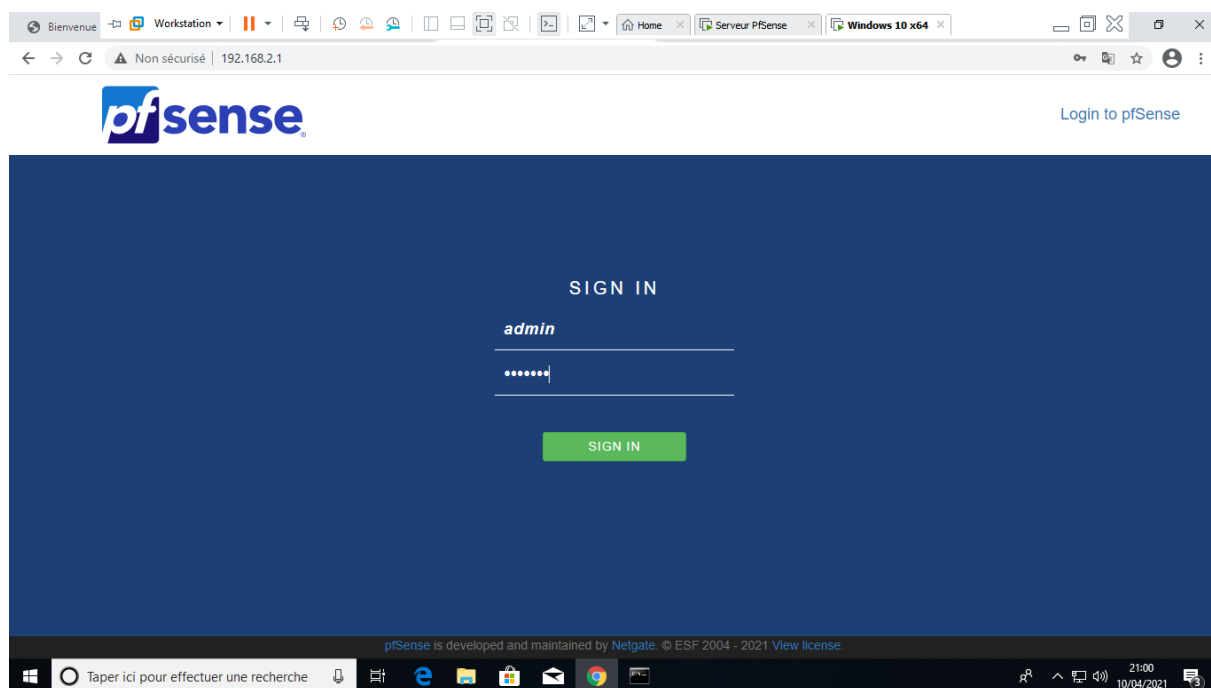
Nous allons à présent vérifier si nous avons accès la connexion Internet sur le pare-feu. Nous lançons donc des pings sur l'adresse **8.8.8.8**. Le résultat nous montre que nous avons bien accès à la connexion Internet.

Sur la machine hôte, nous allons définir la carte réseau en mode LAN SEGMENT, puis nous allons allumer la machine. Nous ouvrirons le navigateur puis entrerons dans la barre de recherche l'adresse **192.168.2.1**. Nous tomberons donc sur l'interface d'authentification pour la configuration du pare-feu pfsense.



Nous allons donc nous authentifier avec les identifiants suivant :

- **Username : admin**
- **Password : pfsense**



Par la suite, il faudra terminer avec les configurations. Ici nous rentrerons le nom d'hôte de l'appareil **"serveurpfense"** dans notre cas avec **"upb.ci"** comme domaine. Pour ce qui est du DNS, on prend le **192.168.126.146** qui dans notre cas est l'adresse IP de l'interface WAN comme Serveur DNS primaire et le **192.168.2.1** comme serveur DNS secondaire, puis on valide.

The screenshot shows the 'Configuration de pfSense / Informations générales' screen. It is Step 2 of 9. The form contains the following fields:

- Nom d'hôte:** serveurpfense (EXAMPLE: myserver)
- Domaine:** upb.ci (EXAMPLE: mydomain.com)
- Serveur DNS primaire:** 192.168.126.146
- Serveur DNS secondaire:** 192.168.2.1
- Remplacer DNS:** ☒ (Autoriser le remplacement des serveurs DNS par DHCP / PPP sur le WAN)

A 'Suivant' button is at the bottom.

Nous allons ensuite définir le mot de passe administrateur WebGUI. Nous utiliserons le mot de passe **"azerty"**, puis nous validerons.

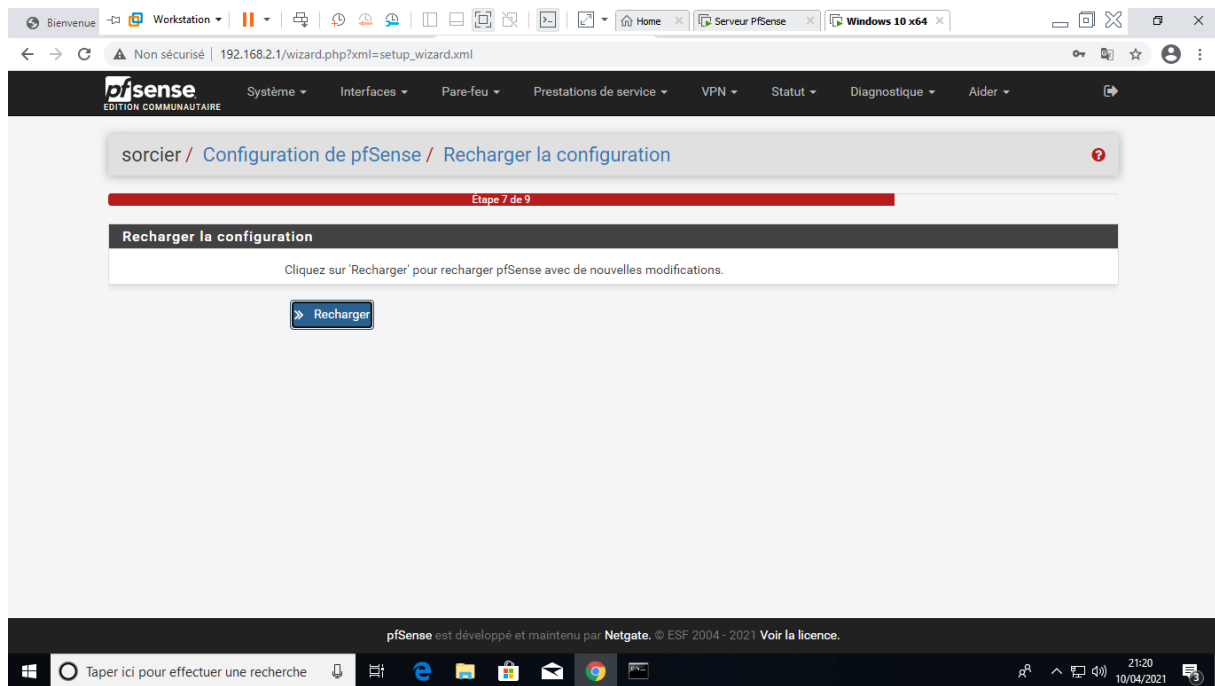
The screenshot shows the 'Configuration de pfSense / Définir le mot de passe Admin WebGUI' screen. It is Step 6 of 9. The form contains the following fields:

- Mot de passe d'administrateur:** (masked with dots)
- Mot de passe administrateur ENCORE:** (masked with dots)

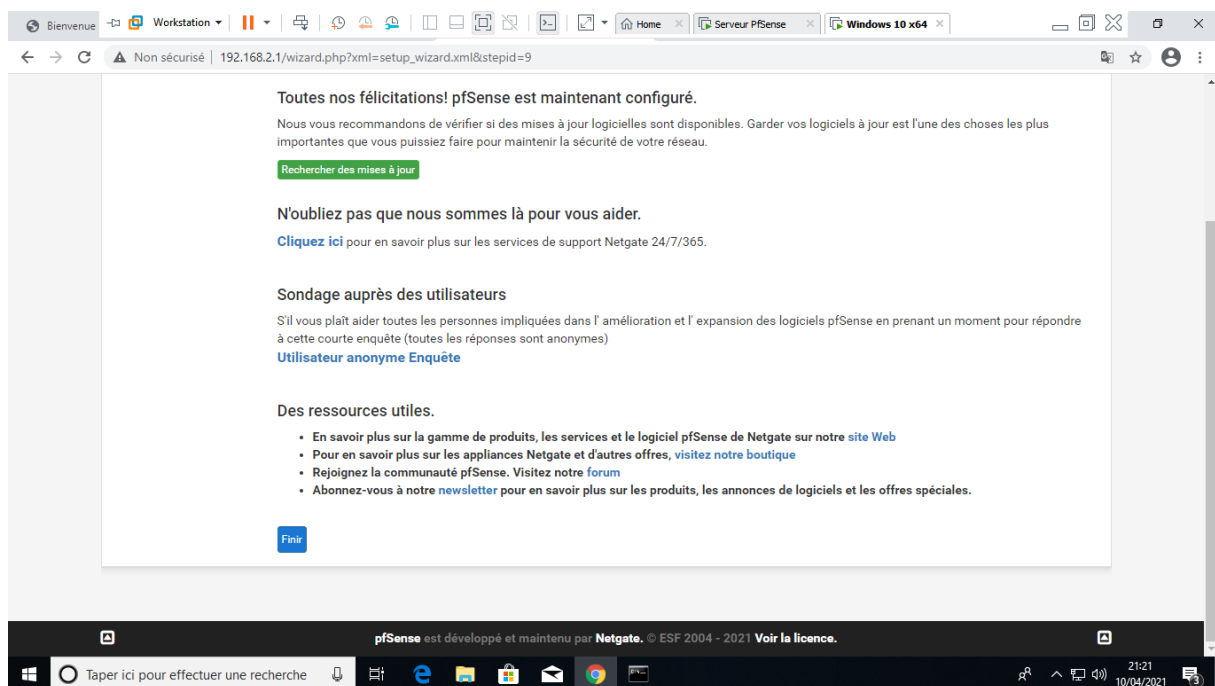
A 'Suivant' button is at the bottom.

At the top, there is a warning: 'AVERTISSEMENT: le mot de passe du compte «admin» est défini sur la valeur par défaut. Modifiez le mot de passe dans le Gestionnaire des utilisateurs.'

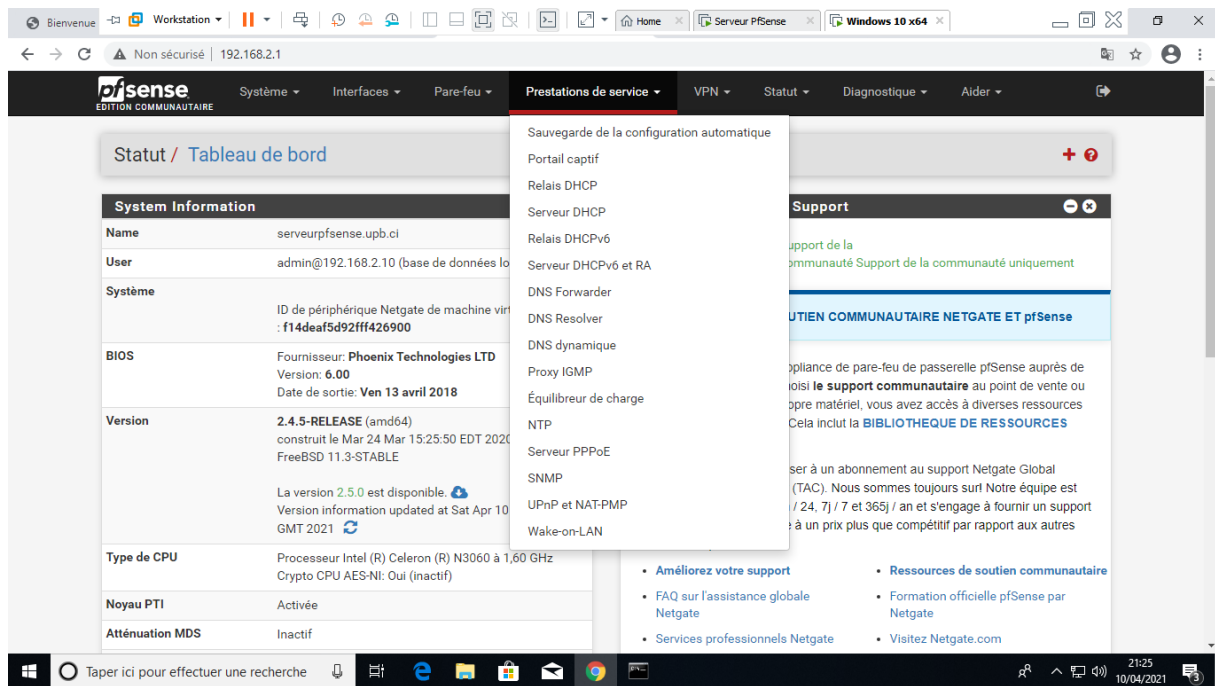
The footer of the pfSense interface reads: 'pfSense est développé et maintenu par Netgate. © ESF 2004 - 2021 Voir la licence.'



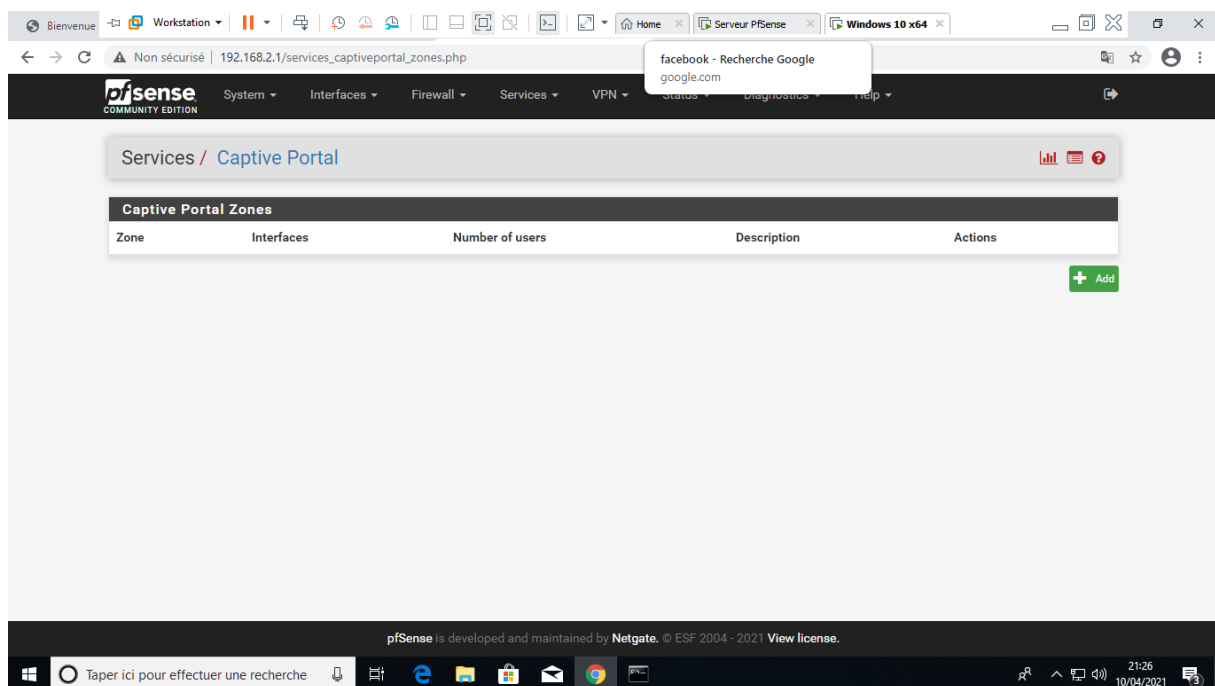
Nous devons ensuite relancer la page afin que celle-ci prenne en compte les informations entrées.



Voilà, nous pouvons donc à présent configurer le portail captif.



Pour configurer le portail captif, nous allons donc cliquer sur l’option “**Prestation de service**” et sur le service “**Portail captif**”



Ensuite nous allons cliquer sur “add”

The screenshot shows the pfSense web interface in a browser window. The address bar displays '192.168.2.1/services\_captiveportal\_zones\_edit.php'. The breadcrumb trail is 'Prestations de service / Portail captif / Ajouter une zone'. The form 'Ajouter une zone de portail captif' contains two input fields: 'Nom de zone' with the value 'upb' and 'Description de la zone' with the value 'Le portail captif de l'université Polytechnique de Bingerville'. A blue button labeled 'Enregistrer continuer' is at the bottom of the form. The footer of the interface indicates 'pfsense est développé et maintenu par Netgate. © ESF 2004 - 2021 Voir la licence.'

Ensuite on entre le nom de la zone. Dans notre cas c'est **"upb"**. La description est facultative. On valide par la suite.

The screenshot shows the 'Configuration du portail captif' page in the pfSense web interface. The breadcrumb trail is 'Prestations de service / Portail captif / upb / Configuration'. The 'Configuration du portail captif' section includes several settings: 'Activer' is checked with 'Activer le portail captif'; 'La description' is 'Le portail captif de l'université Polytechnique de Bingerville'; 'Interfaces' shows 'BLÈME' and 'LAN' selected in a list; 'Nombre maximal de connexions simultanées' is set to '5'; and 'Délai d'inactivité (minutes)' is set to '10'. The footer of the interface shows the time '21:38' and date '10/04/2021'.

Nous rentrons à présent dans le vif du sujet. D'abord, nous allons activer le portail captif en cochant sur la première case. Nous pouvons en second lieu apporter une description. Ensuite nous choisirons l'interface sur laquelle elle doit s'appliquer. Dans notre cas c'est sur le LAN.

Ensuite, nous allons définir le nombre de connexion possible pour un utilisateur au portail captif. Dans notre cas, nous avons pris **"5"**.

Ensuite, nous définirons le délai d'inactivité en d'autres termes la durée qui une fois atteinte dans le cas où l'utilisateur n'utilise pas la machine, déconnectera l'utilisateur de sa session.

Bienvenue | Workstation | Non sécurisé | 192.168.2.1/services\_captiveportal.php?zone=upb

|  |                                     |  |
|--|-------------------------------------|--|
| <b>Délai d'attente difficile (minutes)</b>                                     | <input type="text"/>                | Les clients seront déconnectés après ce laps de temps, quelle que soit l'activité. Cependant, ils peuvent se reconnecter immédiatement. Laissez ce champ vide pour aucun délai d'attente fixe (non recommandé sauf si un délai d'inactivité est défini).   |
| <b>Quota de trafic (mégaoctets)</b>  | <input type="text" value="1024"/>   | Les clients seront déconnectés après avoir dépassé cette quantité de trafic, y compris les téléchargements et les téléchargements. Cependant, ils peuvent se reconnecter immédiatement. Laissez ce champ vide pour aucun quota de trafic.  |
| <b>Crédits directs par adresse MAC</b>   | <input type="text"/>                | Permet de passer par le portail captif sans authentification un nombre limité de fois par adresse MAC. Une fois épuisé, le client ne peut se connecter qu'avec des informations d'identification valides jusqu'à ce que la période d'attente spécifiée ci-dessous soit expirée. Il est recommandé de définir un délai d'attente fixe et / ou un délai d'inactivité lors de son utilisation pour qu'il soit efficace. |
| <b>Période d'attente pour restaurer les crédits pass-through. (Les heures)</b> | <input type="text"/>                | Les clients verront leurs crédits relais disponibles rétablis au décompte d'origine après ce laps de temps écoulé depuis l'utilisation du premier. Cela doit être supérieur à 0 heure si les crédits pass-through sont activés.  |
| <b>Réinitialiser la période d'attente</b>                                      | <input type="checkbox"/>            | Activer la réinitialisation de la période d'attente lors d'une tentative d'accès<br>Si cette option est activée, la période d'attente est réinitialisée à sa durée d'origine si l'accès est tenté alors que tous les crédits d'intercommunication ont déjà été épuisés.  |
| <b>Fenêtre contextuelle de déconnexion</b>                                     | <input checked="" type="checkbox"/> | Activer la fenêtre contextuelle de déconnexion<br>Si cette option est activée, une fenêtre contextuelle apparaîtra lorsque les clients sont autorisés à traverser le portail captif. Cela permet aux clients de se déconnecter explicitement avant que le délai d'inactivité ou d'expiration matérielle ne se produise.  |
| <b>URL de redirection de</b>   | <input type="text"/>                |  |

logo upb.jpg | npp.7.9.1.Installer.exe | Tout afficher

Taper ici pour effectuer une recherche

Nous allons ensuite définir le **Quota de trafic (Mo) : 1024**

Puis nous allons cocher la case de **“Activer la fenêtre contextuelle de déconnexion”**. Celle-ci permettra aux utilisateurs de se déconnecter de manière autonome.

Bienvenue | Workstation | Non sécurisé | 192.168.2.1/services\_captiveportal.php?zone=upb

|   |                                     |  |
|---|-------------------------------------|--|
| <b>Après authentification URL de redirection</b>        | <input type="text"/>                | Définissez une URL de redirection forcée. Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont initialement tenté d'accéder après s'être authentifiés.  |
| <b>URL de redirection d'adresse MAC bloquée</b>         | <input type="text"/>                | Les adresses MAC bloquées seront redirigées vers cette URL lors de la tentative d'accès.   |
| <b>Connexions utilisateur simultanées</b>               | <input checked="" type="checkbox"/> | Désactiver les connexions utilisateur simultanées<br>Si cette option est activée, seule la connexion la plus récente par nom d'utilisateur sera active. Les connexions ultérieures entraîneront la déconnexion des machines précédemment connectées avec le même nom d'utilisateur.  |
| <b>Filtrage MAC</b>                                     | <input type="checkbox"/>            | Désactiver le filtrage MAC<br>Si cette option est activée, aucune tentative ne sera faite pour garantir que l'adresse MAC des clients reste la même lorsqu'ils sont connectés. Ceci est nécessaire lorsque l'adresse MAC du client ne peut pas être déterminée (généralement parce qu'il y a des routeurs entre pfSense et les clients). Si cette option est activée, l'authentification RADIUS MAC ne peut pas être utilisée.   |
| <b>Entrée automatique MAC Pass-through</b>              | <input type="checkbox"/>            | Activer les ajouts automatiques de MAC d'intercommunication<br>Lorsqu'elle est activée, une entrée de relais MAC est automatiquement ajoutée une fois que l'utilisateur s'est authentifié avec succès. Les utilisateurs de cette adresse MAC n'auront plus jamais à s'authentifier. Pour supprimer l'entrée MAC relais, connectez-vous et supprimez-la manuellement de l'onglet MAC ou envoyez un POST depuis un autre système. Si cette option est activée, la fenêtre de déconnexion ne sera pas affichée. |
| <b>Restriction de bande passante par utilisateur</b>    | <input type="checkbox"/>            | Activer la restriction de bande passante par utilisateur   |
| <b>Utiliser la page de portail captif personnalisée</b> | <input checked="" type="checkbox"/> | Activer pour utiliser une page de connexion au portail captif personnalisé<br>Si défini, une page portal.html doit être créée et téléchargée. Si elle n'est pas cochée, le modèle par défaut sera utilisé  |

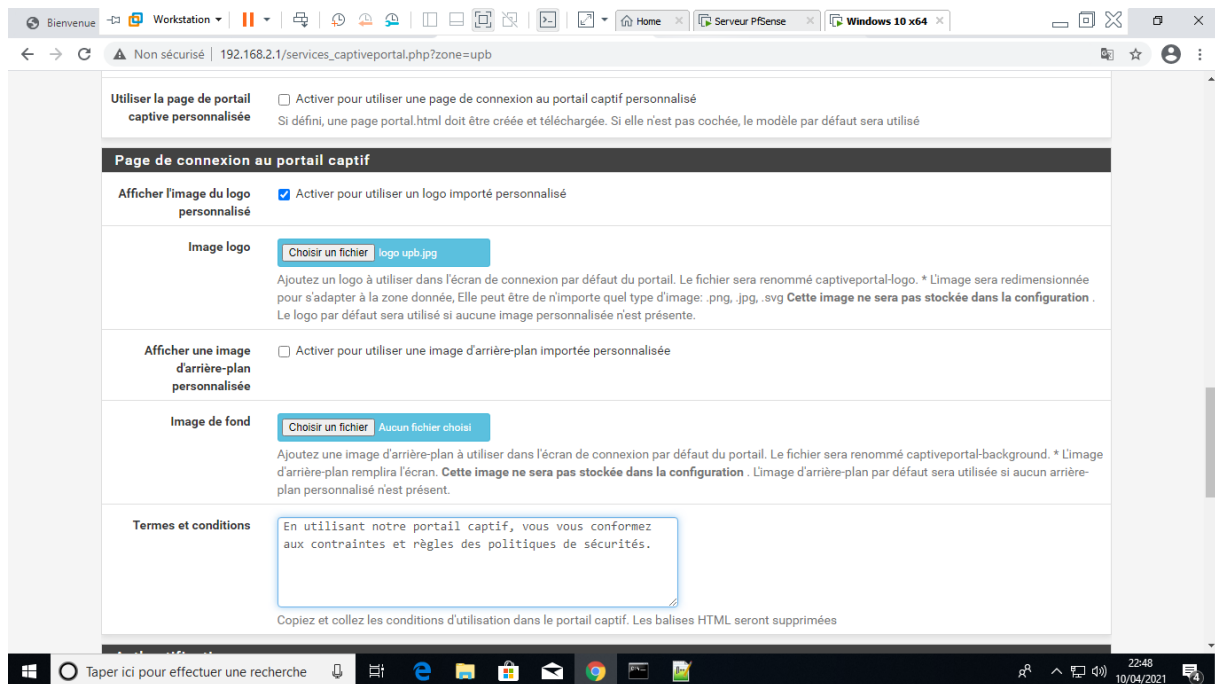
logo upb.jpg | npp.7.9.1.Installer.exe | Tout afficher

Taper ici pour effectuer une recherche

Nous allons donc cocher la case de **“connexion utilisateur simultanées”** afin de désactiver les connexions utilisateurs simultanées.

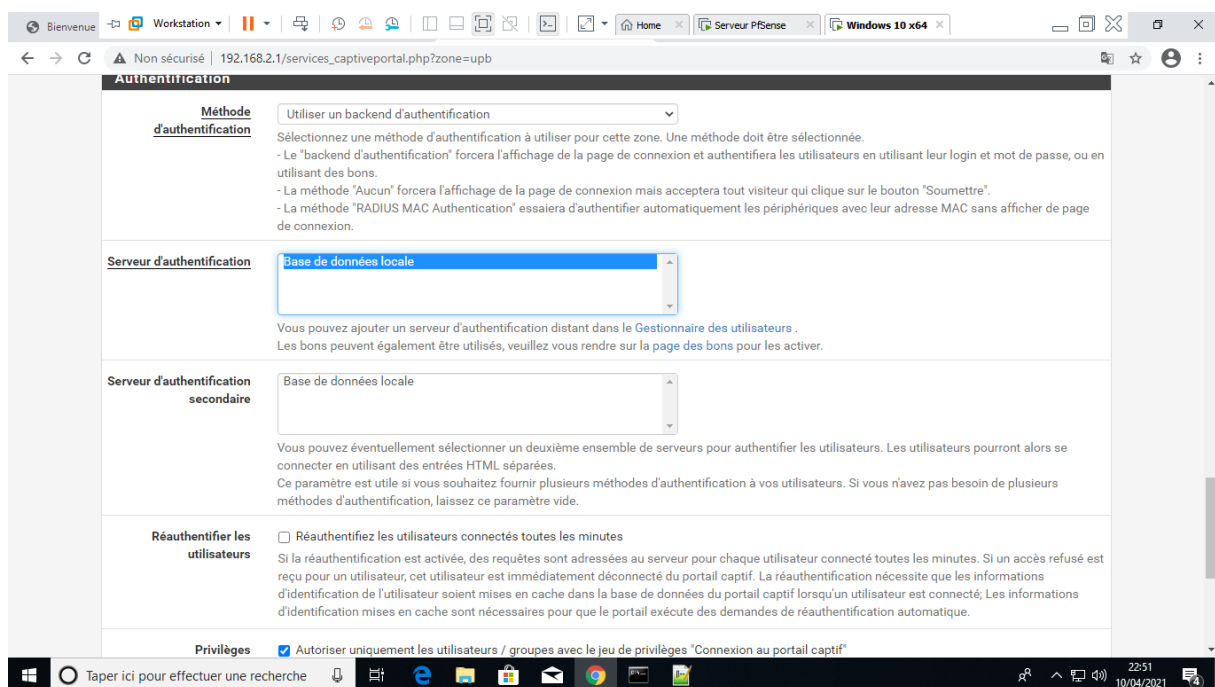
**Toutefois, nous ne cocherons pas la case de “Utiliser la page de portail captif personnalisé”**



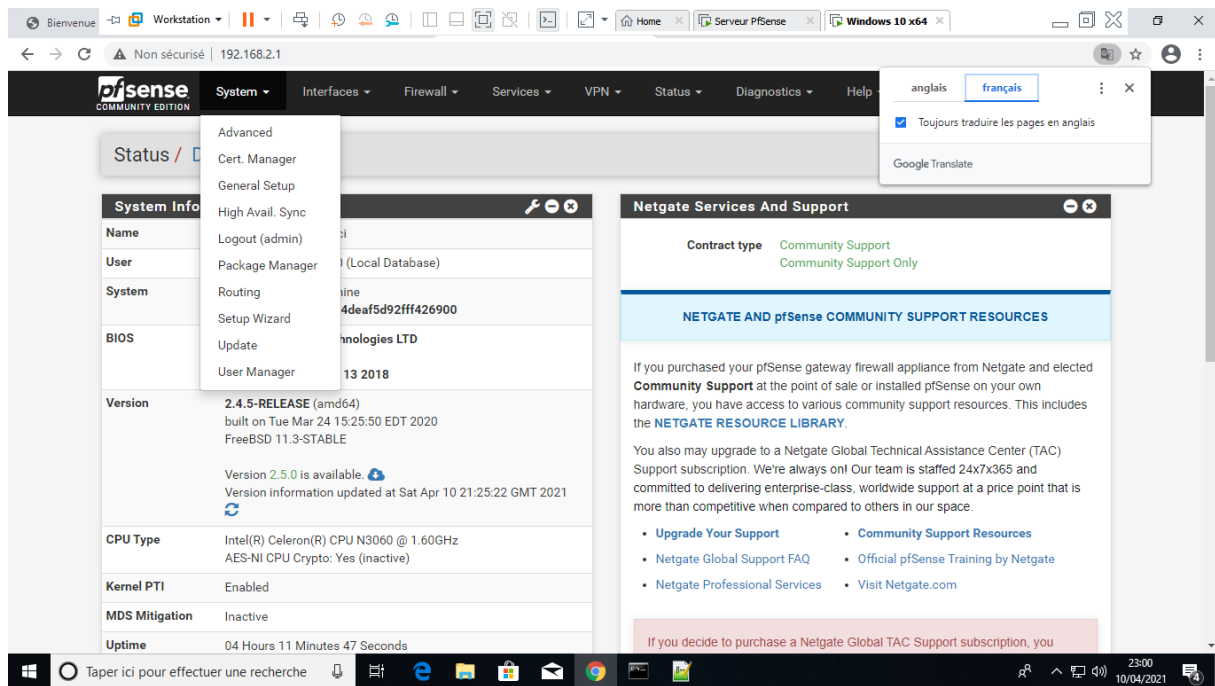


Nous allons donc cocher la case de “**Afficher l’image du logo personnalisé**” afin d’activer l’utilisation d’un logo importé. Nous téléchargerons ensuite le logo grâce au champs juste en dessous.

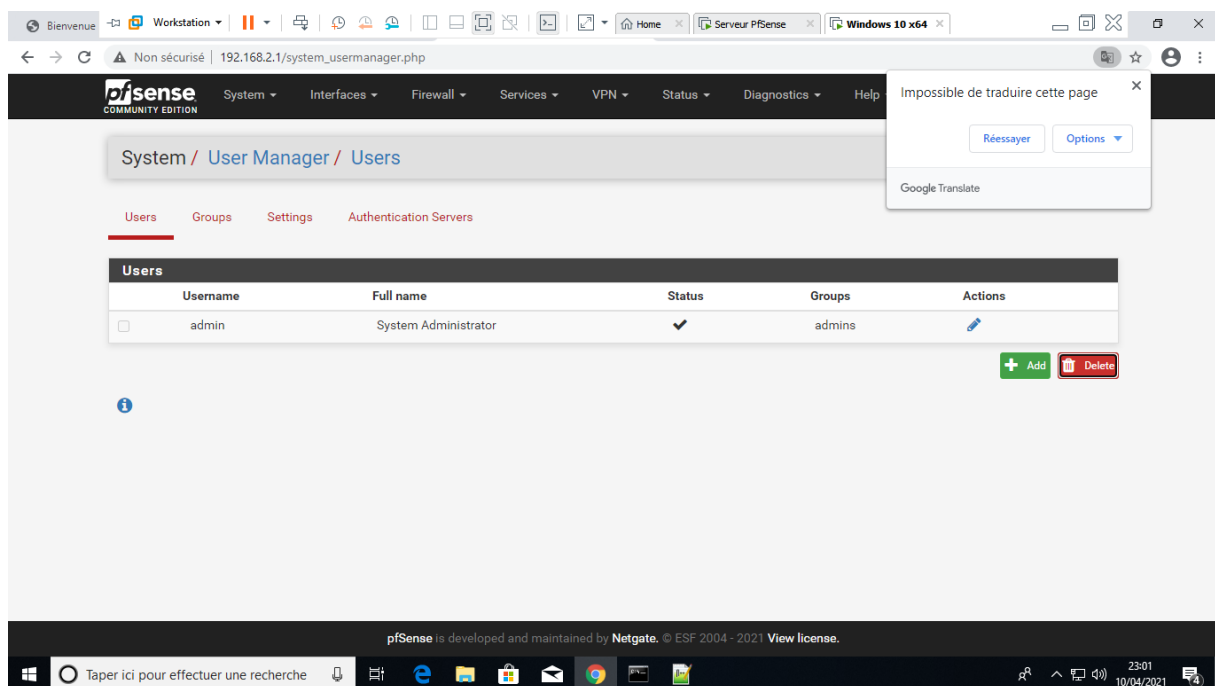
Ensuite nous pouvons entrer du texte dans les **Termes et conditions**.



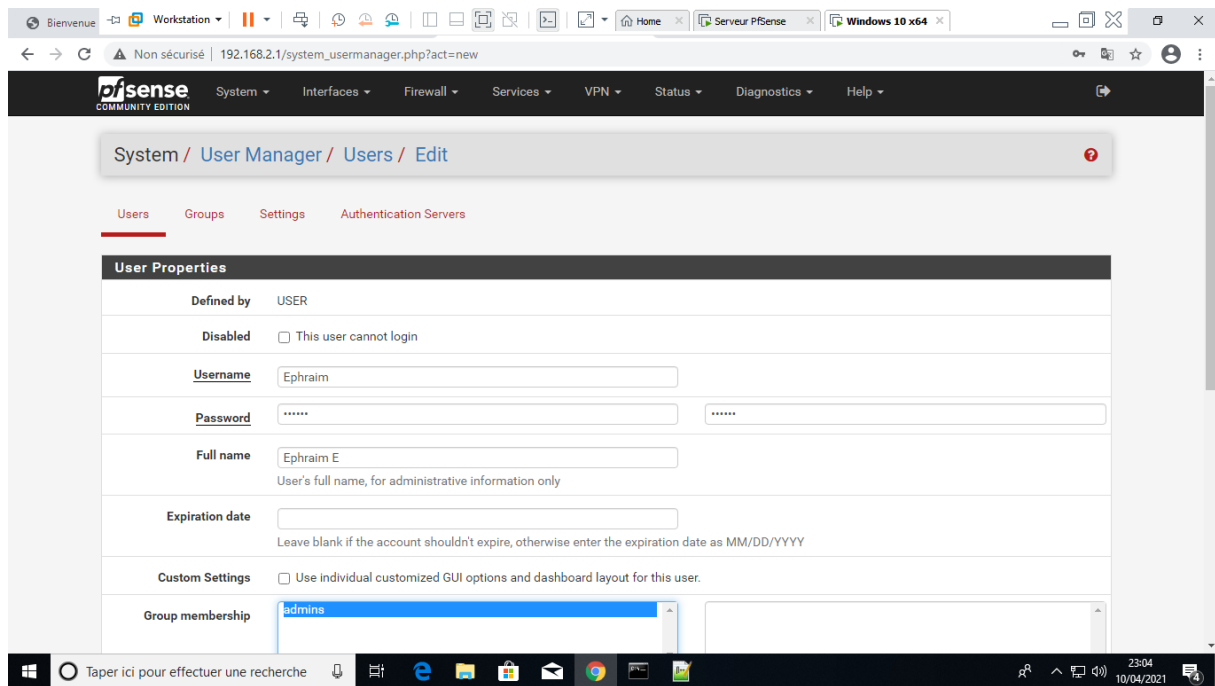
Nous allons à présent choisir le serveur d’authentification en cliquant sur “**base de données locale**”



Nous allons par la suite créer les utilisateurs et leur attribuer les privilèges. Nous allons d'abord choisir l'option **Système** puis le service "User Manager" ou "Gestion des utilisateur".

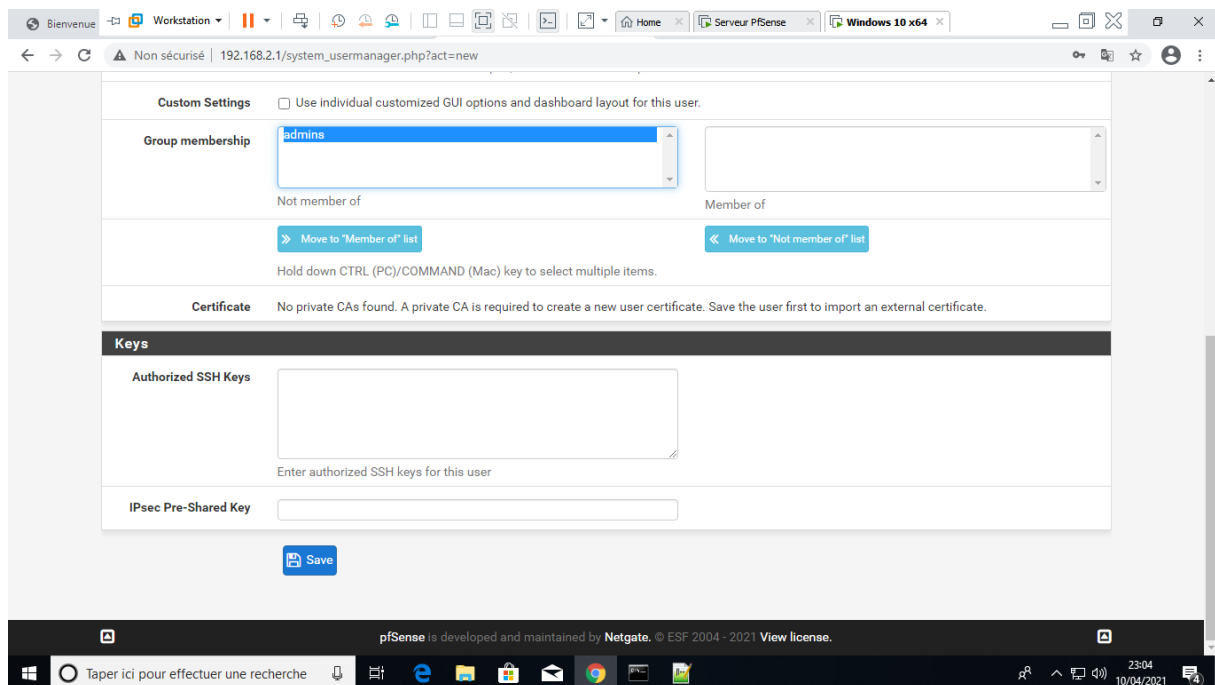


Nous cliquerons sur le bouton "add" afin d'ajouter les utilisateurs.

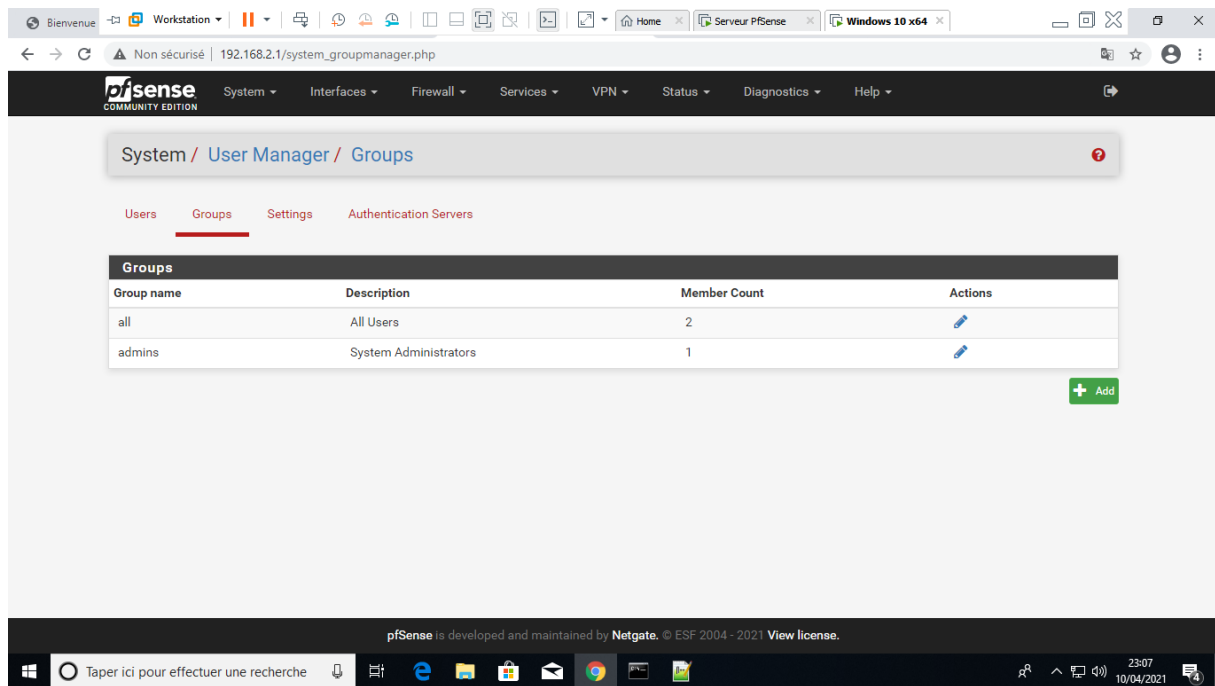


Nous allons donc créer un utilisateur avec pour

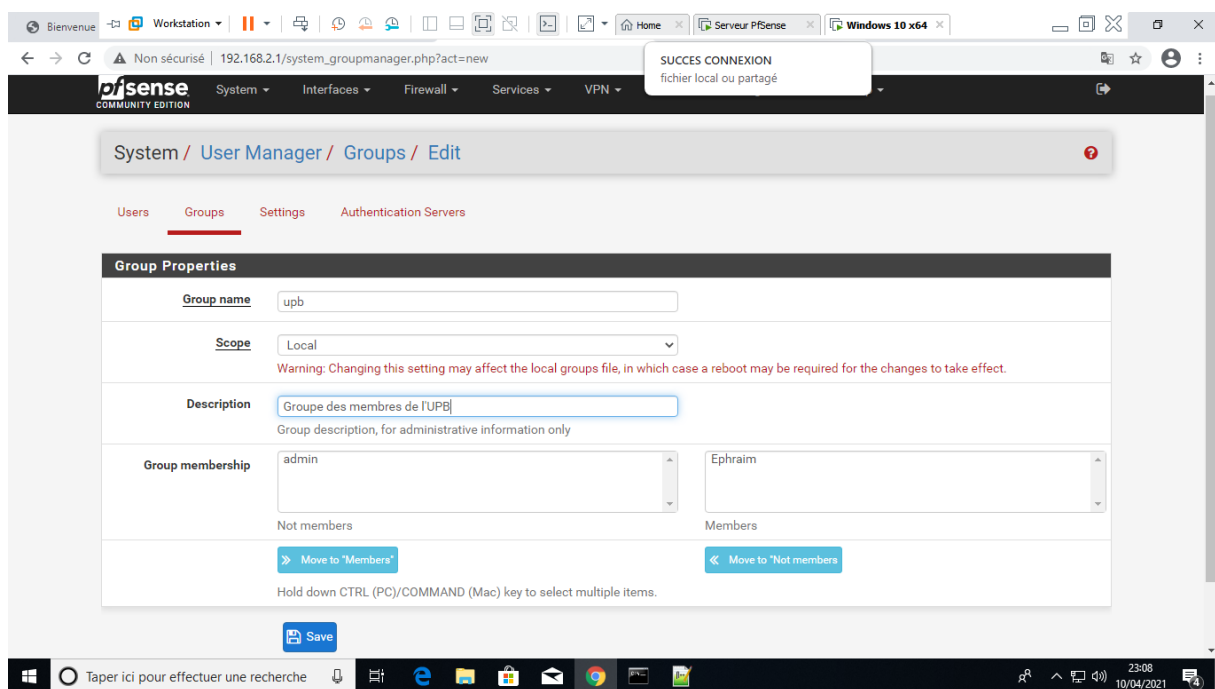
- **Nom d'utilisateur : Ephraim**
- **Mot de passe : azerty**
- **Nom complet : Ephraim E**



Nous allons ensuite enregistrer. Puis nous allons créer un groupe afin d'y insérer notre utilisateur.



Nous cliquerons donc sur le bouton ‘add’

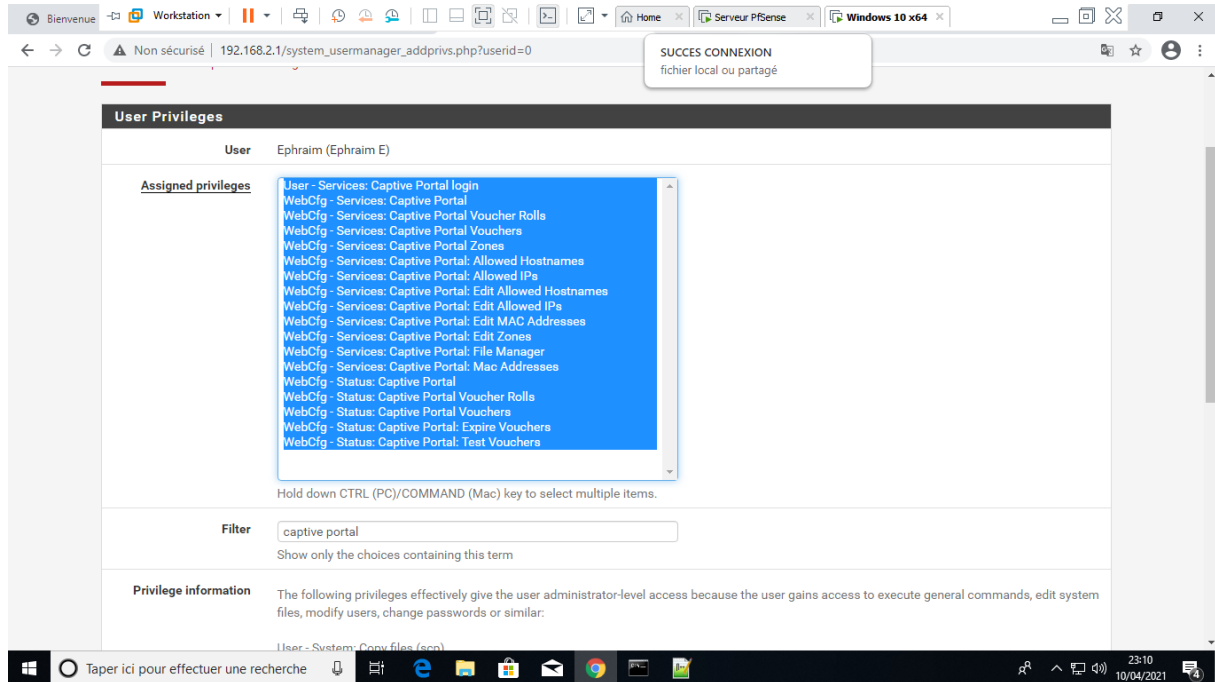


Nous lui donnerons les informations suivantes :

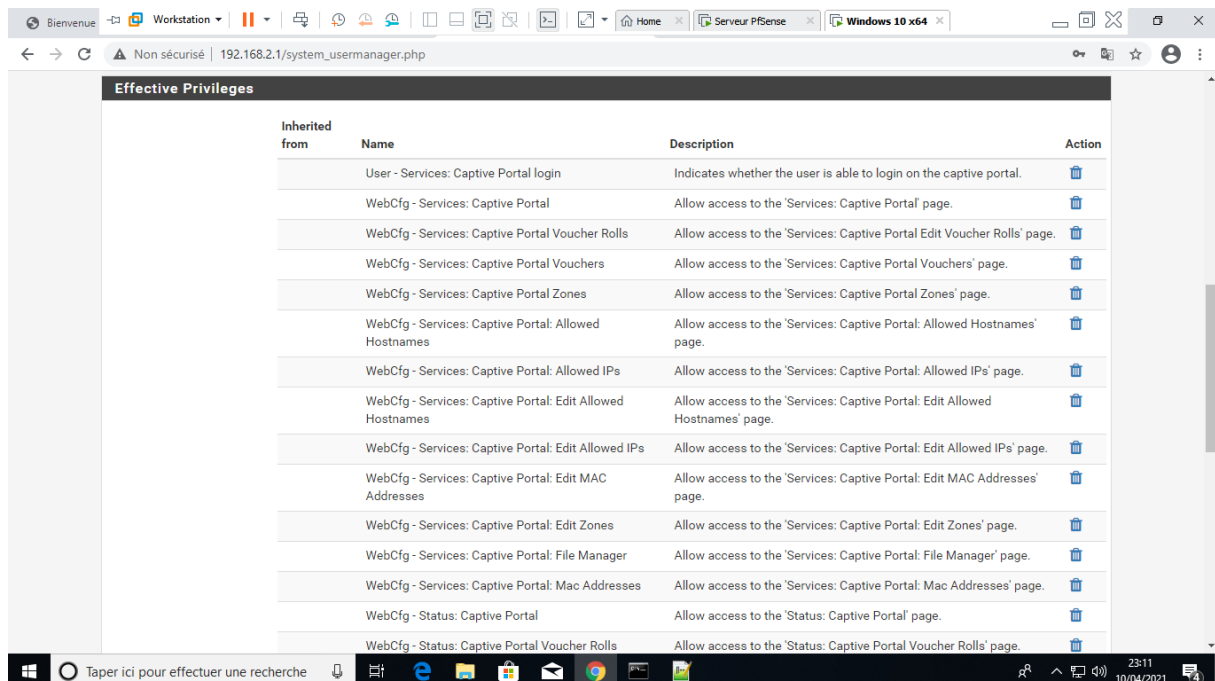
- **Nom de groupe : upb**
- **Etendu : Local**

Une description facultative. Puis nous allons y insérer notre utilisateur en cliquant sur lui en dessous d'admin et en cliquant sur le bouton de **Move to member** ou **Déplacer vers les membres**. Puis nous validerons.

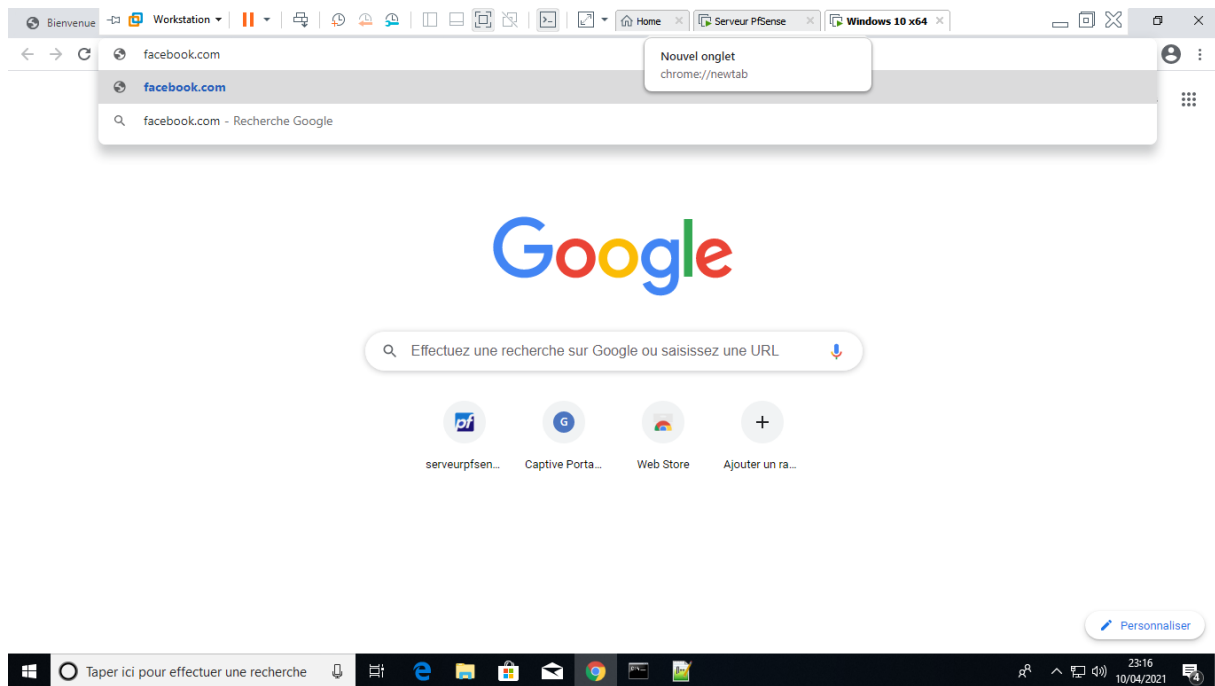
Ensuite nous retournerons vers les utilisateurs, nous ferons une double clique sur notre utilisateur ou nous cliquerons sur l'icone de crayon à droite, puis nous descendrons jusqu'au privilèges d'utilisateur. Une fois ce niveau atteint, nous cliquerons sur le bouton **“add”** et là ou c'est inscrit **Filter**, nous entrer **“captive portal”** puis **Entrer**. Il va filtrer et afficher les privilèges en relation avec le portail captif. Nous allons tous les cocher puis nous descendrons tout en bas afin de valider le choix.



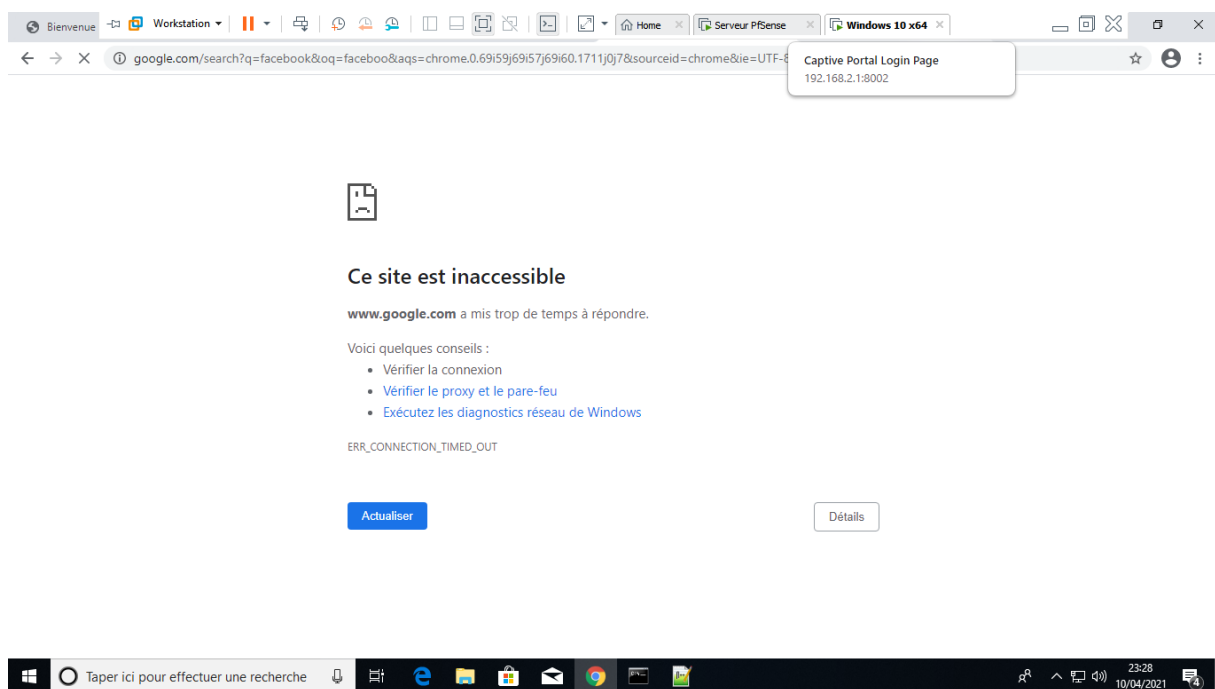
Et de là, nous retombons sur la page de configuration de l'utilisateur. Là encore, nous descendrons jusqu'en bas afin de valider les configurations.



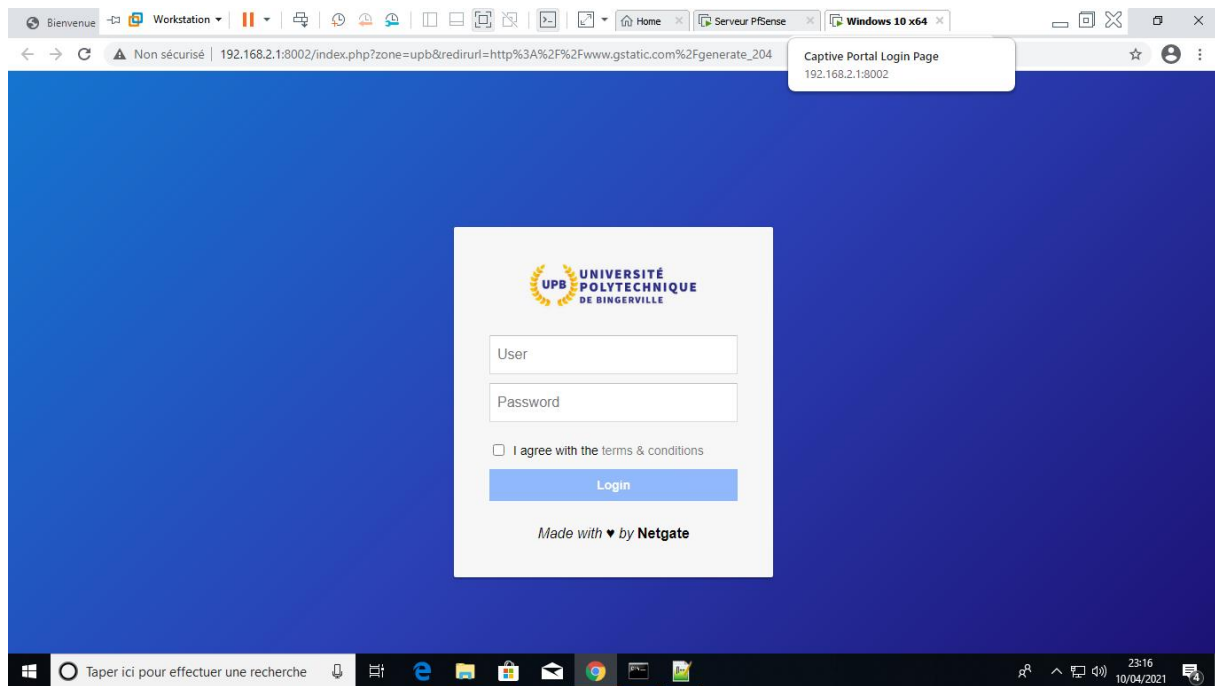
Nous allons à présent tester. Pour le test nous allons taper **“facebook.com”** afin de voir si nous arrivons à accéder librement à Internet.



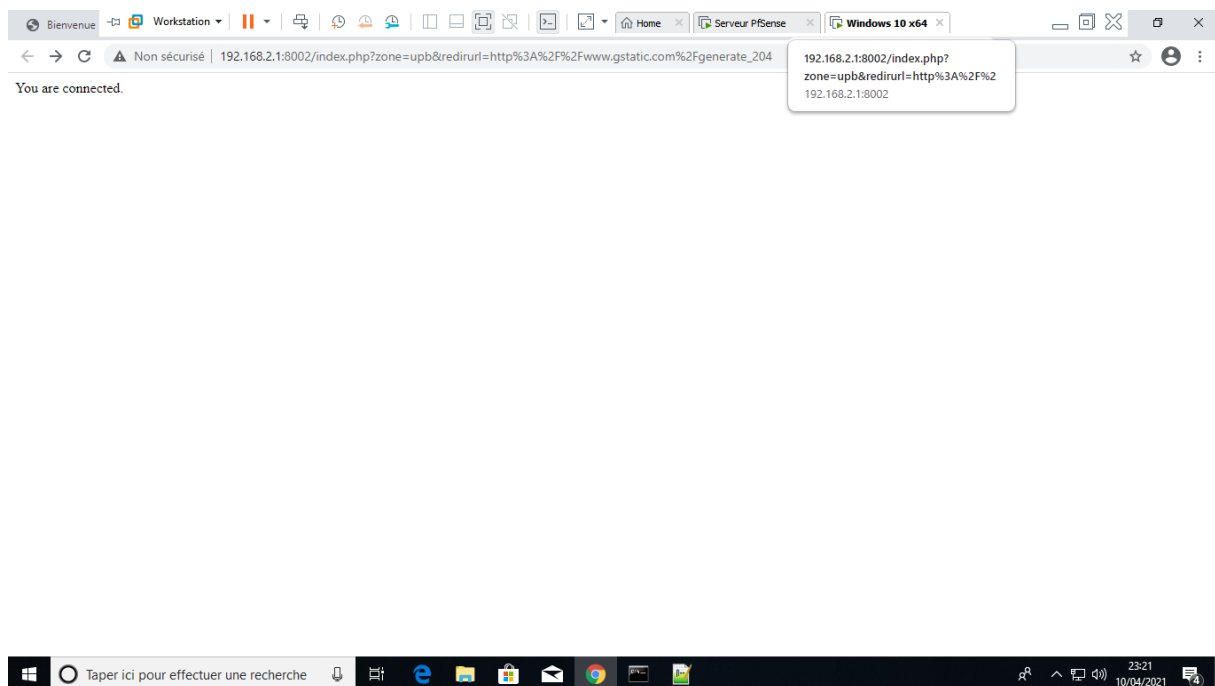
Nous voyons donc que nous n'arrivons pas à accéder à Internet.

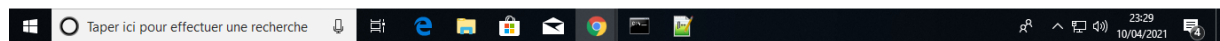
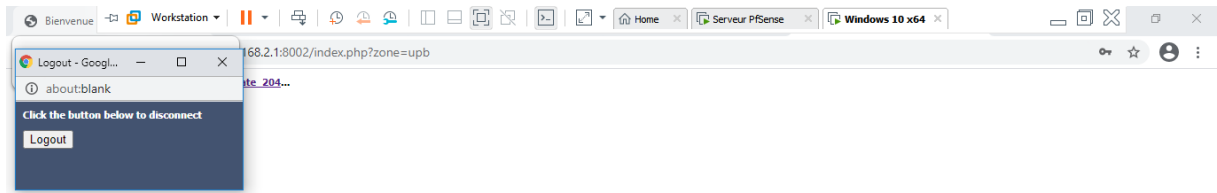


Voici donc la page de connexion qui apparaît. Nous devons donc renseigner ici les informations de l'utilisateur afin que celui-ci arrive à se connecter et utiliser Internet.

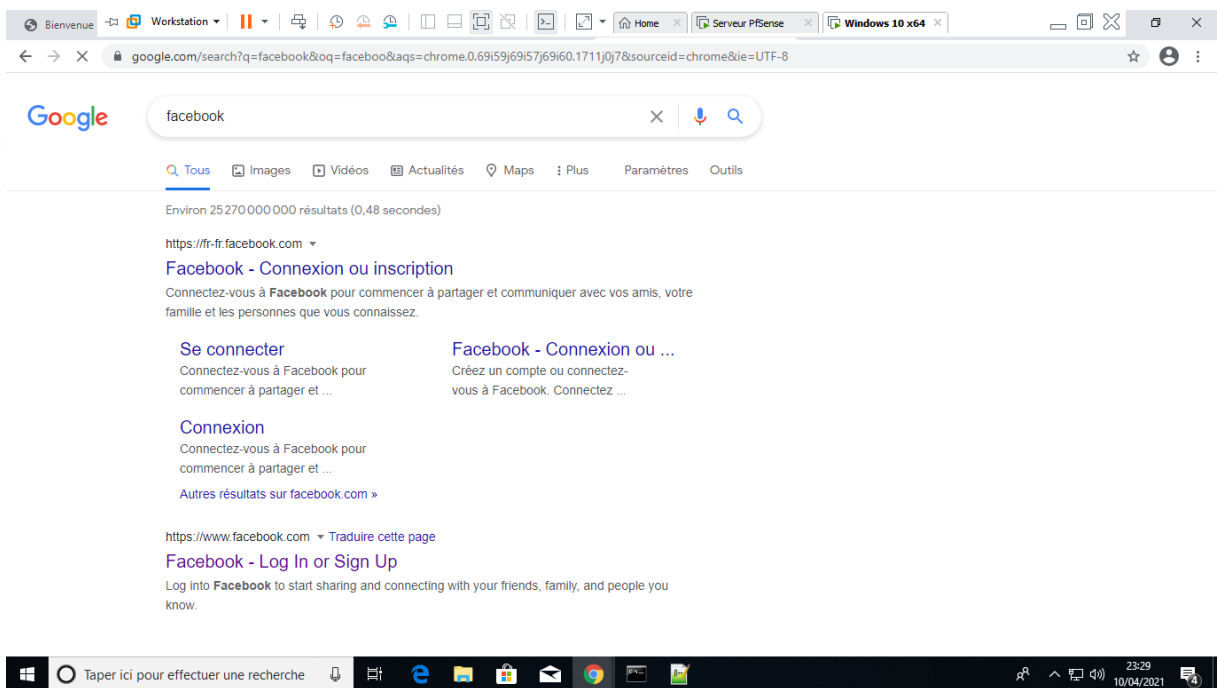


Nous voyons que l'utilisateur a pu se connecter grâce à l'expression **“You are connected.”**





Nous avons ici la fenêtre qui permet aux utilisateurs de se connecter de manière autonome.



Nous voyons donc à présent que nous avons accès à Internet.