



| | | |
|---|--|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

1. Objet du document



PfSense est un système d'exploitation open source ayant pour but la mise en place de firewall basé sur le système d'exploitation FreeBSD.

Sur cette documentation, vous sera proposé les instructions pour installer une VM pfSense, configurer et paramétrer, et ensuite d'ajouter des filtrages.

2. Historique


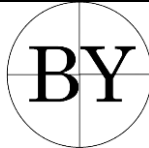
| Utilisateur | Document | Date |
|-----------------|--------------------------------|------------|
| YILMAZ Bünyamin | Mise en place de la VM pfSense | 01/06/2022 |
| YILMAZ Bünyamin | Mise à disposition du document | 15/06/2022 |
| | | |



| | | |
|---|--|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

3. Sommaire

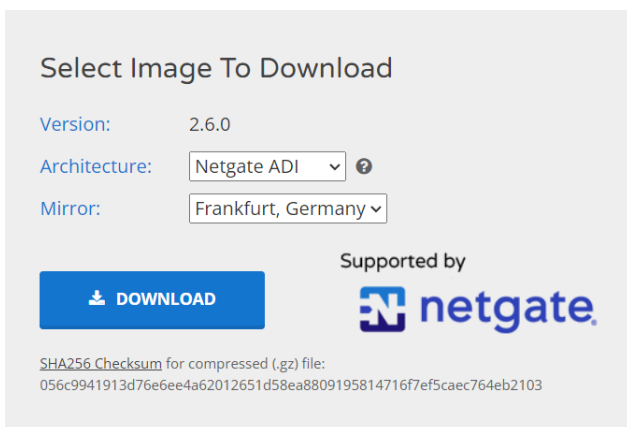
1. *Objet du document*
2. *Historique*
3. *Sommaire*
4. Installation de la Machine Virtuel
5. Configuration de PfSense
6. Paramétrage Web
7. Ajout de filtrage « deny all »
8. Ajout de filtrage internet

| | | |
|---|--|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

4. Installation de la Machine Virtuel

Tout d'abord, pour commencer l'installation de pfSense, il faut se procurer l'image sur le site officiel de pfSense : www.pfsense.org/download/

Les paramètres suivants seront requis pour avoir l'image ISO adapté à notre VM.



Select Image To Download

Version: 2.6.0

Architecture: Netgate ADI

Mirror: Frankfurt, Germany

Supported by 



[SHA256 Checksum](#) for compressed (.gz) file:
056c9941913d76e6ee4a62012651d58ea8809195814716f7ef5caec764eb2103

PS : L'installation va se faire entièrement grâce au clavier. La touche **Entrée** signifie *Accepter*, et la **Barre espace** sert à *Valider un choix*.

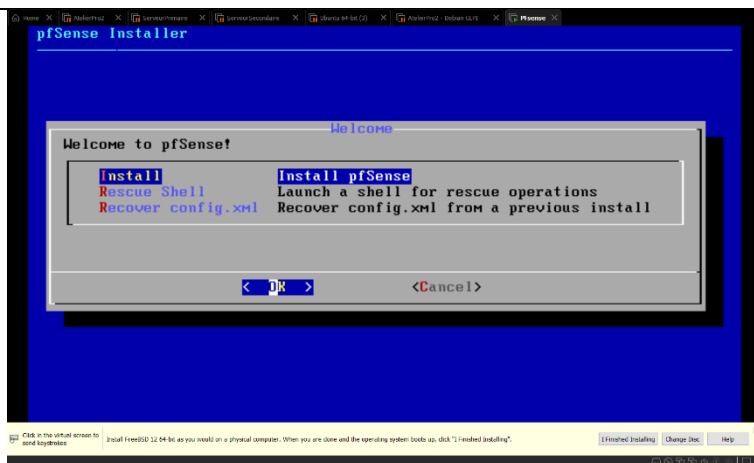
Avant de lancer votre VM, il faut impérativement avoir 2 cartes réseaux avec les configurations suivantes :

| Name | Type | External Connection | Host Connection | DHCP | Subnet Address |
|--------|-----------|---------------------|-----------------|---------|----------------|
| VMnet0 | NAT | NAT | Connected | Enabled | 192.168.91.0 |
| VMnet1 | Custom | - | - | - | 192.168.15.0 |
| VMnet2 | Host-only | - | Connected | - | 192.168.60.0 |

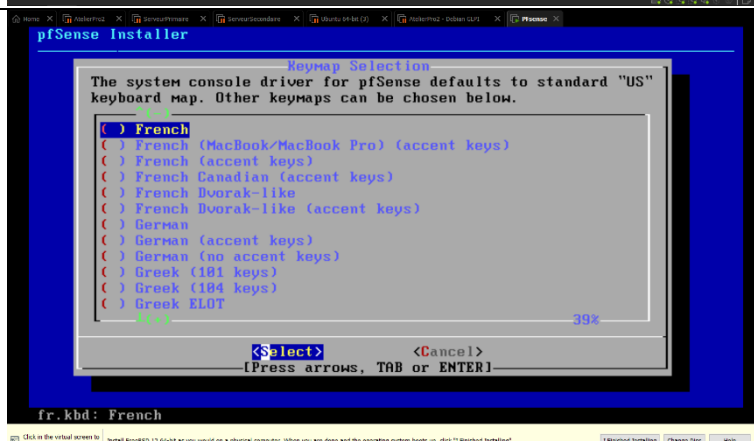
La première carte *VMnet0* va correspondre à l'interface WAN de pfSense, elle a été positionnée en NAT, et la seconde *VMnet1* sera l'interface LAN, elle a été positionnée dans un réseau privé (custom).

| | | |
|---|---|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

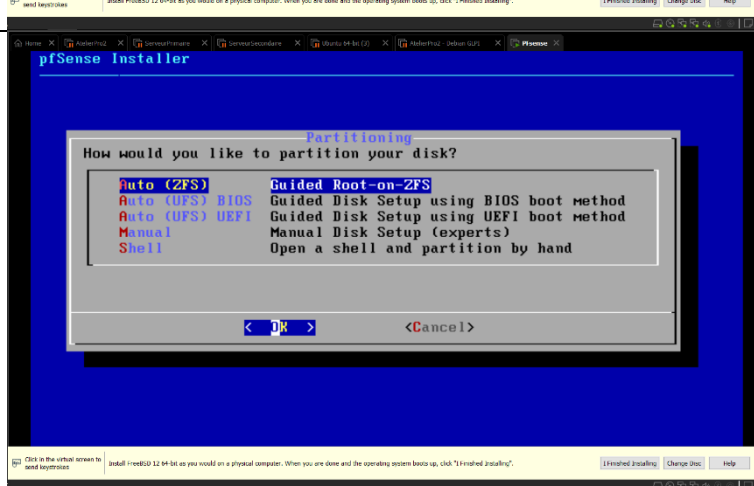
L'installation peut maintenant débuter validant l'option Install pfSense.





On choisit ensuite la langue du clavier (French), puis **Entrée**.



Une interface qui demande de partitionner le disque se propose. Restez sur le choix «Auto (2FS)» et appuyez sur **Entrée**.



| | | |
|---|---|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

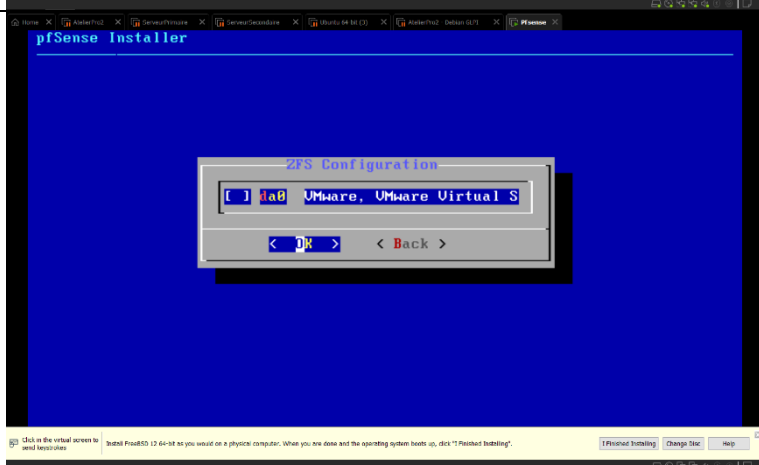
La configuration du partitionnement du disque va être demandé, voici le paramétrage.





Il faut bien s'assurer à valider le choix :

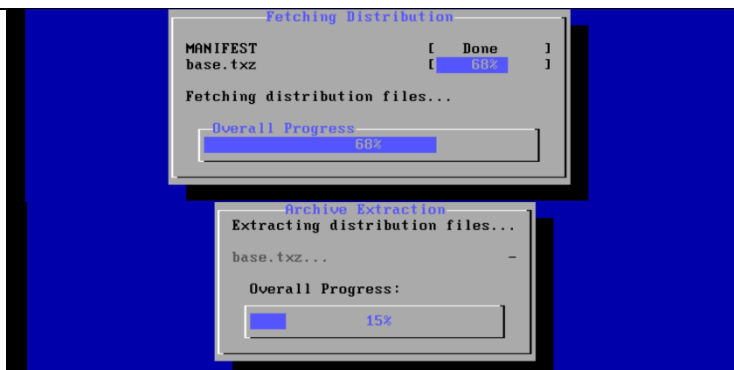
" da0 VMware, VMware Virtual S "

avec **Espace**, puis appuyez sur **Entrée**.

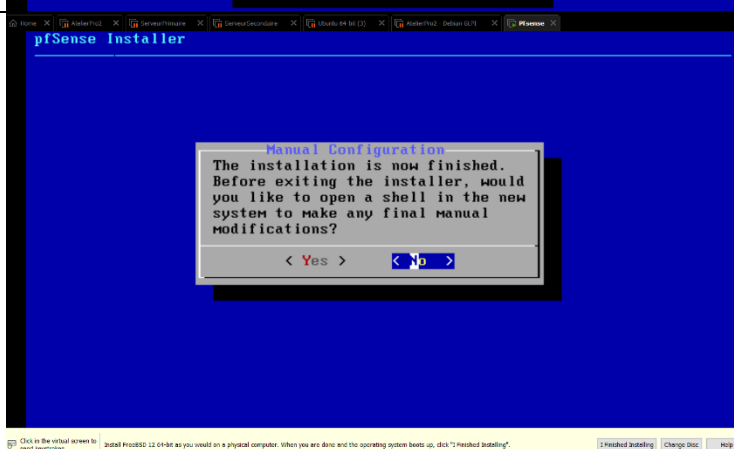


| | | |
|---|--|--|
|  | <p>CCI-SIO – U6 – Cybersécurité des Services Informatiques</p> |  |
| <p>Bünyamin YILMAZ</p> | <p>Manipulation d'une VM PfSense</p> | <p>Version A</p> |

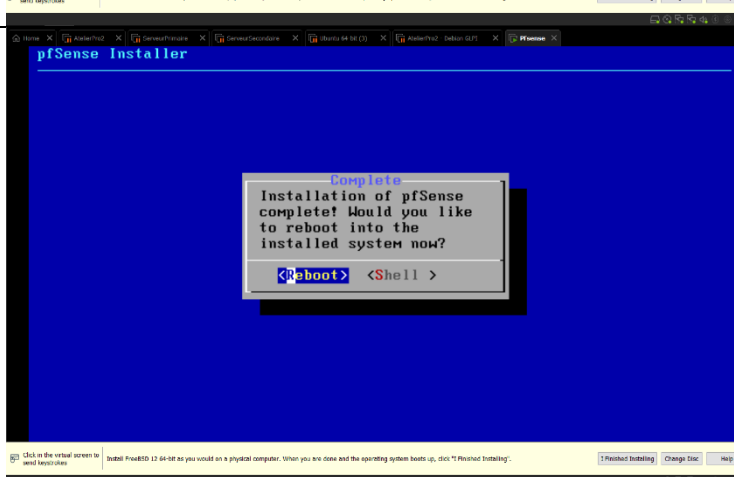
Le partitionnement du disque, puis l'installation de pfSense va alors se lancer.


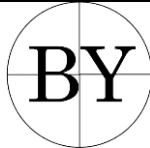


Une interface qui demande d'ouvrir un shell (terminal) se propose. Restez sur le choix « No » et appuyez sur Entrée.

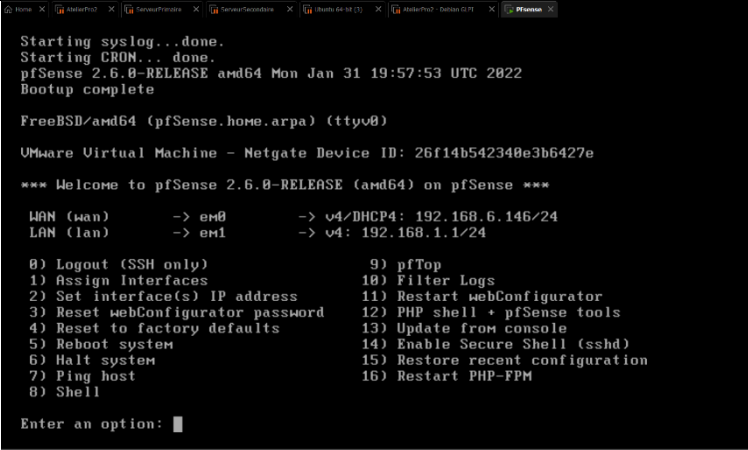
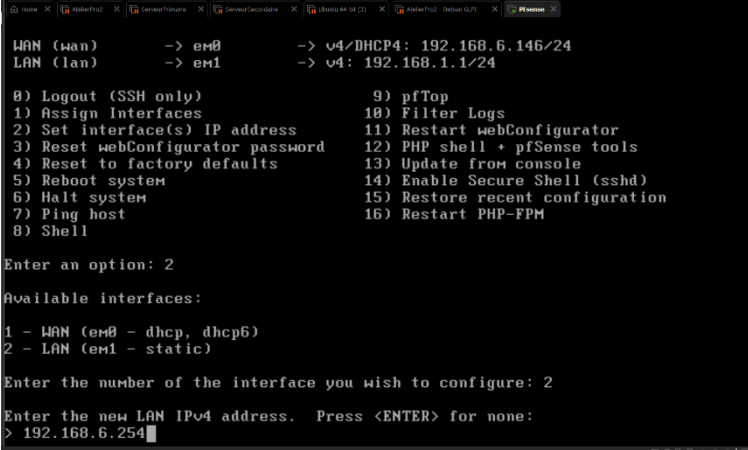
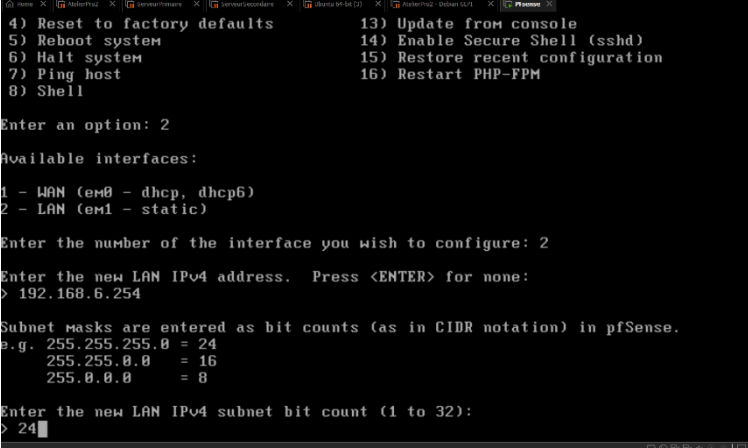




L'installation est à présent terminée. Dernièrement, appuyez sur Entrée pour reboot la machine et lancer pfSense.

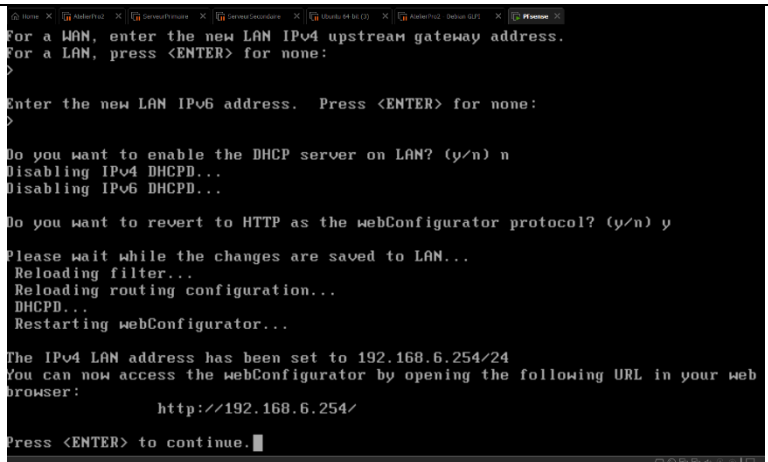


| | | |
|---|---|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |


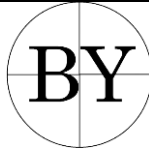
5. Configuration de PfSense

| | |
|---|---|
| <p>L'interface suivante sera proposée une fois la machine démarrée.</p> <p>A partir de ce menu, nous pouvons taper un numéro de 0 à 16 selon le besoin pour configurer la machine.</p> |  <pre> 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) VMware Virtual Machine - Netgate Device ID: 26f14b542340e3b6427e *** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense *** WAN (wan) -> em0 -> v4/DHCP4: 192.168.6.146/24 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: █ </pre> |
| <p>Avant de se lancer sur pfSense, il faut d'abord assigner une adresse IP à l'interface LAN.</p> <p>Tapez "2 " puis Entrée.</p> <p>Il va alors proposer de choisir entre WAN ou LAN</p> <p>Tapez "2 " puis configurer l'IP.</p> |  <pre> WAN (wan) -> em0 -> v4/DHCP4: 192.168.6.146/24 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: 2 Enter the new LAN IPv4 address. Press <ENTER> for none: > 192.168.6.254 </pre> |
| <p>Définissez le masque de sous-réseau du réseau local, tapez 24</p> |  <pre> 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: > 192.168.6.254 Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8 Enter the new LAN IPv4 subnet bit count (1 to 32): > 24 </pre> |

| | | |
|---|---|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

| | |
|--|---|
| <p>pfSense demande si le réseau possède une passerelle pour renvoyer les flux. Ne rien taper puis Entrée. pfSense demande de configurer d'adresse en IPv6. Ne rien taper puis Entrée. Saisir « n » puis Entrée pour désactiver le service DHCP. Saisir « y » puis Entrée pour activer le service HTTPS pour pouvoir aller sur l'interface web.</p> |  <pre> 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) y Please wait while the changes are saved to LAN... Reloading filter... Reloading routing configuration... DHCPD... Restarting webConfigurator... The IPv4 LAN address has been set to 192.168.6.254/24 You can now access the webConfigurator by opening the following URL in your web browser: http://192.168.6.254/ Press <ENTER> to continue. </pre> |
|--|---|

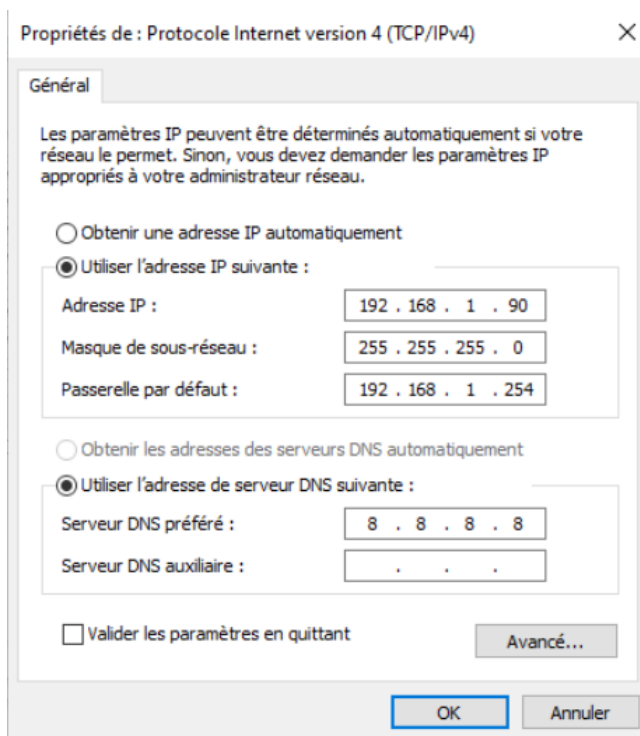
La configuration de pfSense est terminée.

| | | |
|---|---|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

6. Paramétrage Web

PfSense s'utilise via une interface web, il faut donc disposer d'un poste client avec un navigateur web et ayant une adresse IP dans le même réseau local que lui.

- Sur le poste client (Windows), aller sur Systèmes / Réseaux et Internet / Etat / Modifier les options d'adaptateur
- Sélectionner Ethernet1 et aller dans propriétés / Protocole IPv4
- Appliquer les configurations suivantes selon l'IP du LAN sur serveur pfSense





Ensuite, taper l'adresse IP LAN du serveur pfSense, nous aurons alors accès à pfSense via Web

Les identifiants par défaut sont les suivants :

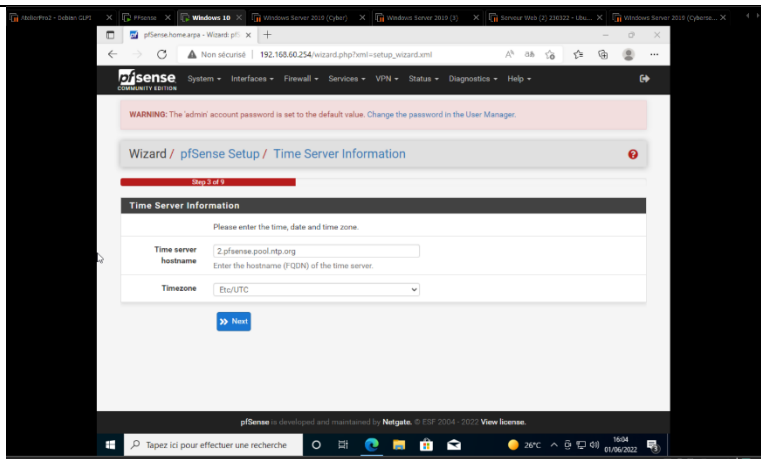
login : **admin**
mot de passe : **pfsense**

Cliquez sur l'interface pfSense Setup pour commencer la configuration du firewall.

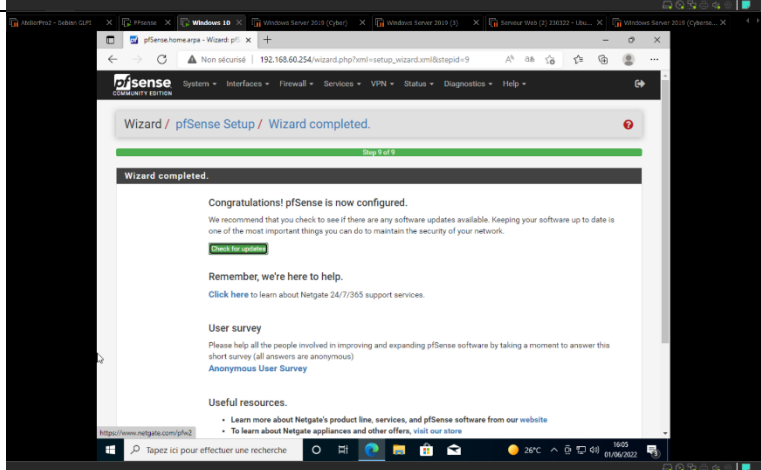
| | | |
|---|--|--|
|  | <h1>CCI-SIO – U6 – Cybersécurité des Services Informatiques</h1> |  |
| Bünyamin YILMAZ | <h2>Manipulation d'une VM PfSense</h2> | Version A |



pfSense est configuré automatiquement. Cliquez sur **Next** en vérifiant les paramètres :

*General Information,
 Time Server Information
 Configure WAN Interface
 Configure LAN Interface
 Set Admin WebGUI Password
 Reload Configuration*



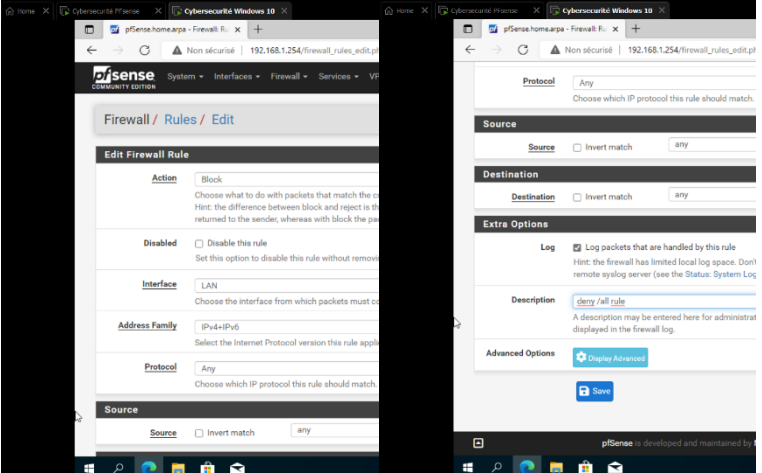
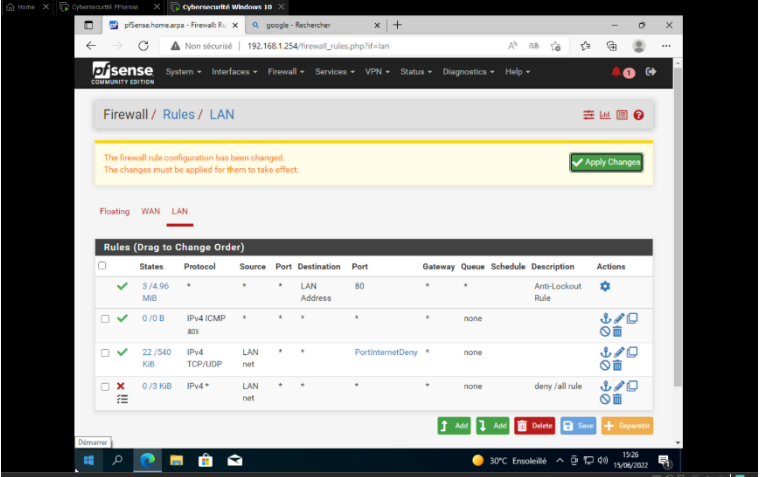
La phase finale de l'installation de pfSense est terminée. Cliquez sur **Reload** puis **Finish**.




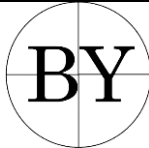
| | | |
|---|---|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

7. Ajout de filtrage « deny all »

Les filtrages permettent de mettre des restrictions sur des protocoles, Port, adresse IP.

| | |
|---|--|
| <p>Pour cela, nous devons aller dans Firewall / Rules, puis dans les paramètres de l'interface LAN, et commencer à configurer selon le besoin</p> |  |
| <p>Une fois que vous avez sauvegardé les filtrages, appliquez les modifications en cliquant sur <i>Apply Changes</i></p> |  |

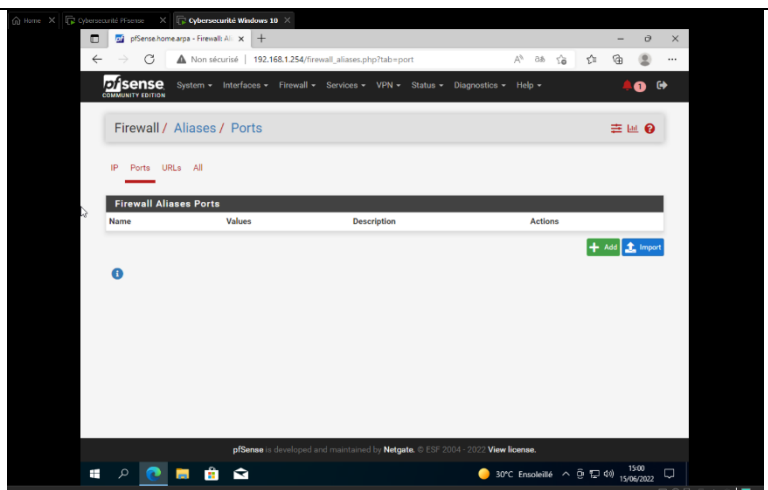
Lorsque les filtrages seront appliqués, il faudra tester le fonctionnement de celles-ci en se rendant sur une page Web

| | | |
|---|---|--|
|  | CCI-SIO – U6 – Cybersécurité des Services Informatiques |  |
| Bünyamin YILMAZ | Manipulation d'une VM PfSense | Version A |

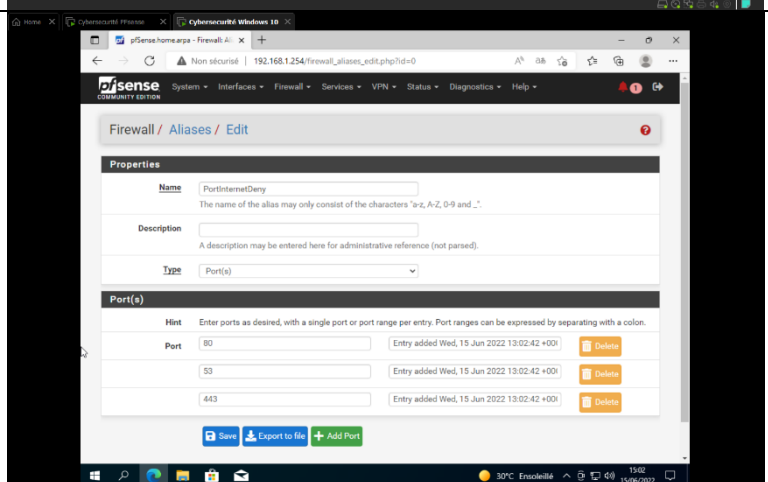
8. Ajout de filtrage internet

Les filtrages internet vont servir à débloquer certains ports pour avoir l'autorisation de faire des recherches sur le Web

Pour cela, nous devons aller dans Firewall / Aliases / Port, commencer à répertorier les ports souhaités selon le besoin.



Pour notre cas, les ports 80, 53 et 443 vont être ajoutés



Finalement, il faudra faire une recherche internet (Youtube) et vérifier son bon fonctionnement.