



COMPRENDRE ET METTRE EN ŒUVRE DES REGLES DE FIREWALLING

TABLE DES MATIERES

INTRODUCTION.....	1
I- Documentation d'installation	1
A- Configuration de la machine virtuelle	1
B- Installation de pfSense.....	2
II- Documentation de configuration.....	6
A- Configuration de l'interface LAN.....	7
B- Test d'intégration.....	11
Configuration de l'adresse IP sous Windows	12
III- Documentation de paramétrage.....	15
A- Setup pfsense.....	15
B- Paramétrage du Serveur DHCP	19
C- Paramétrage du filtrage "Deny All ».....	20
D- Paramétrage du filtrage internet	23
BONUS : Création d'un alias de filtrage internet.....	25
Test d'intégration	27
E- Mise en place d'un portail Captif sous pfSense.....	28
1. Création du portail captif	28
2. Création d'un utilisateur pour se connecter sur le portail	31
3. Test d'intégration.....	33

INTRODUCTION

Dans le cadre de cette documentation, nous allons procéder à la mise à disposition et service d'un pare-feu sur un réseau en production.

Le pare-feu à mettre en place sera pfSense, logiciel libre permettant de filtrer les connexions réseaux entrant et sortant sur le réseau.

Ainsi, pour mieux comprendre la mise en service de pfSense, nous allons procéder à la documentation d'installation, de configuration et de paramétrage de pfSense sur le réseau.

Ressources nécessaires pour l'installation :

- Une machine virtuelle sous FreeBSD avec pfSense
- Une machine virtuelle cliente sous Windows ou Ubuntu
- Une machine virtuelle Windows Server pour le test d'intégration du pare-feu sur un réseau administré par Windows Server.

I- DOCUMENTATION D'INSTALLATION

A- CONFIGURATION DE LA MACHINE VIRTUELLE

Avant de procéder au démarrage de la machine virtuelle de pfSense, il est important que la machine virtuelle respecte les configurations suivantes :

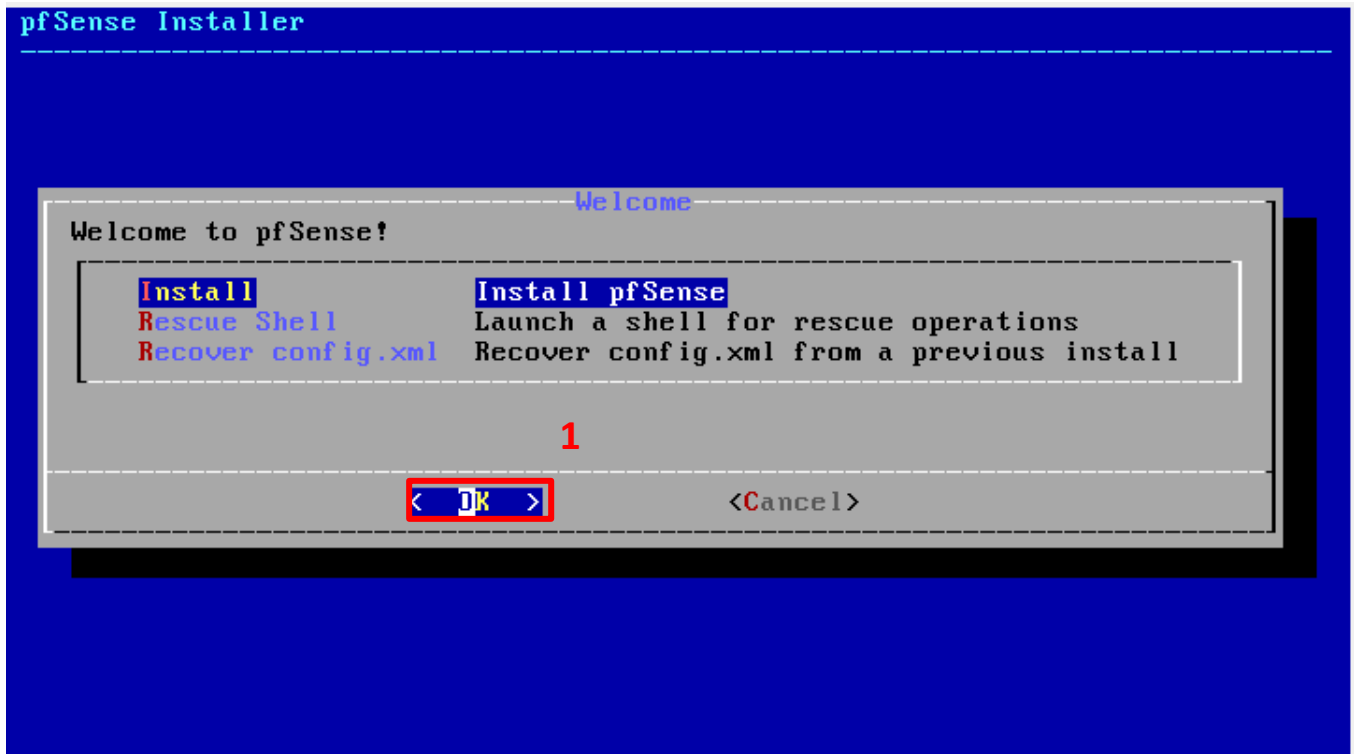
- Noyau du système d'exploitation : FreeBSD
- Système d'exploitation : pfSense téléchargeable sur <https://frafiles.netgate.com/mirror/downloads/pfSense-CE-2.6.0-RELEASE-amd64.iso.gz>
- Cartes réseau : 2 cartes dont 1 pour l'interface WAN qui permettra aux machines clientes derrière pfSense d'accéder à Internet, et 1 pour l'interface LAN pour l'adressage IP des machines clientes.
- Stockage : 16 Go minimum recommandée.
- Mémoire vive : 1 Go minimum recommandée

 System	
Mémoire vive :	1024 Mo
Ordre d'amorçage :	Disquette, Optique, Disque dur
Accélération :	VT-x/AMD-V , Pagination imbriquée
<hr/>	
 Affichage	
Mémoire vidéo :	16 Mo
Contrôleur graphique :	VMSVGA
Serveur de bureau à distance :	Désactivé
Enregistrement :	Désactivé
<hr/>	
 Stockage	
Contrôleur :	IDE
Maître primaire IDE :	pfSense.vmdk (Normal, 16,00 Gio)
Maître secondaire IDE :	[Lecteur optique] Vide
<hr/>	
 Audio	
Pilote hôte :	Windows DirectSound
Contrôleur :	ICH AC97
<hr/>	
 Réseau	
Interface 1 :	Intel PRO/1000 MT Desktop (Interface pont Realtek PCIe GbE Family Controller)
Interface 2 :	Intel PRO/1000 MT Desktop (Réseau interne, 'lnetnet')

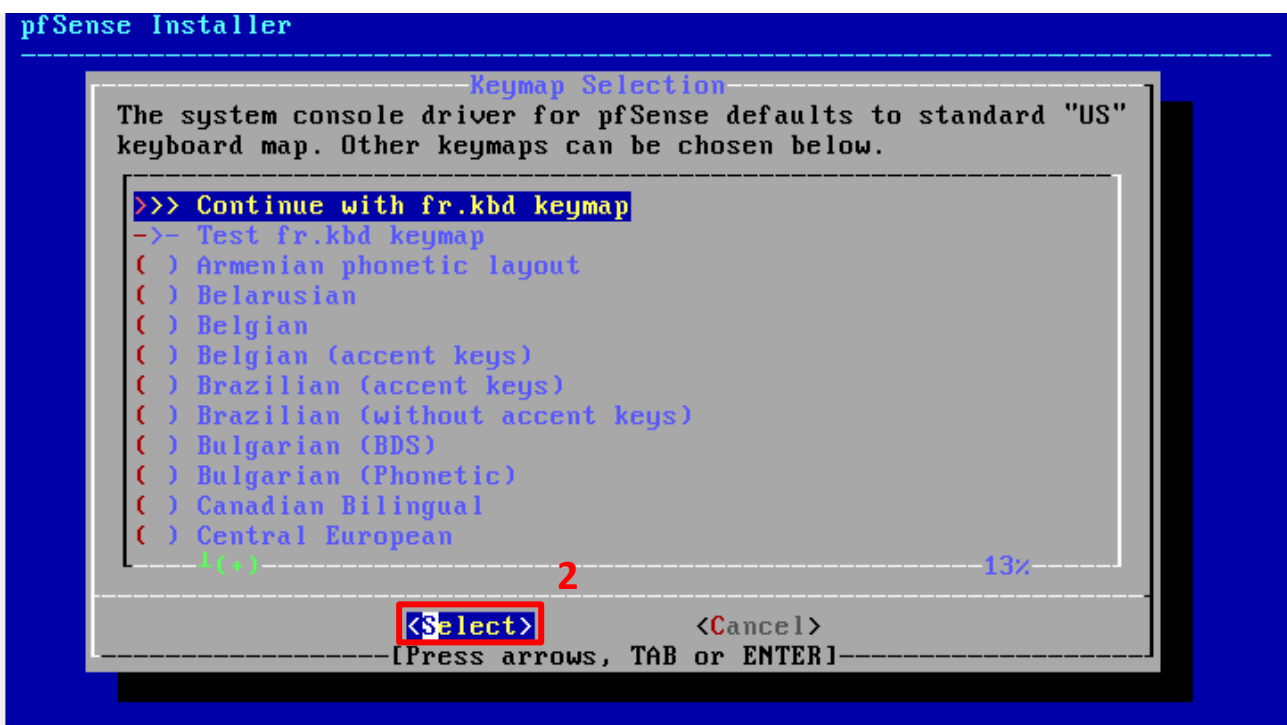
B- INSTALLATION DE pFSense

A présent, nous pouvons démarrer la machine virtuelle pour procéder à l'installation de pfSense. Nous détaillerons les étapes ci-dessous, avec les paramètres à respecter, les cases à cocher pendant l'installation.

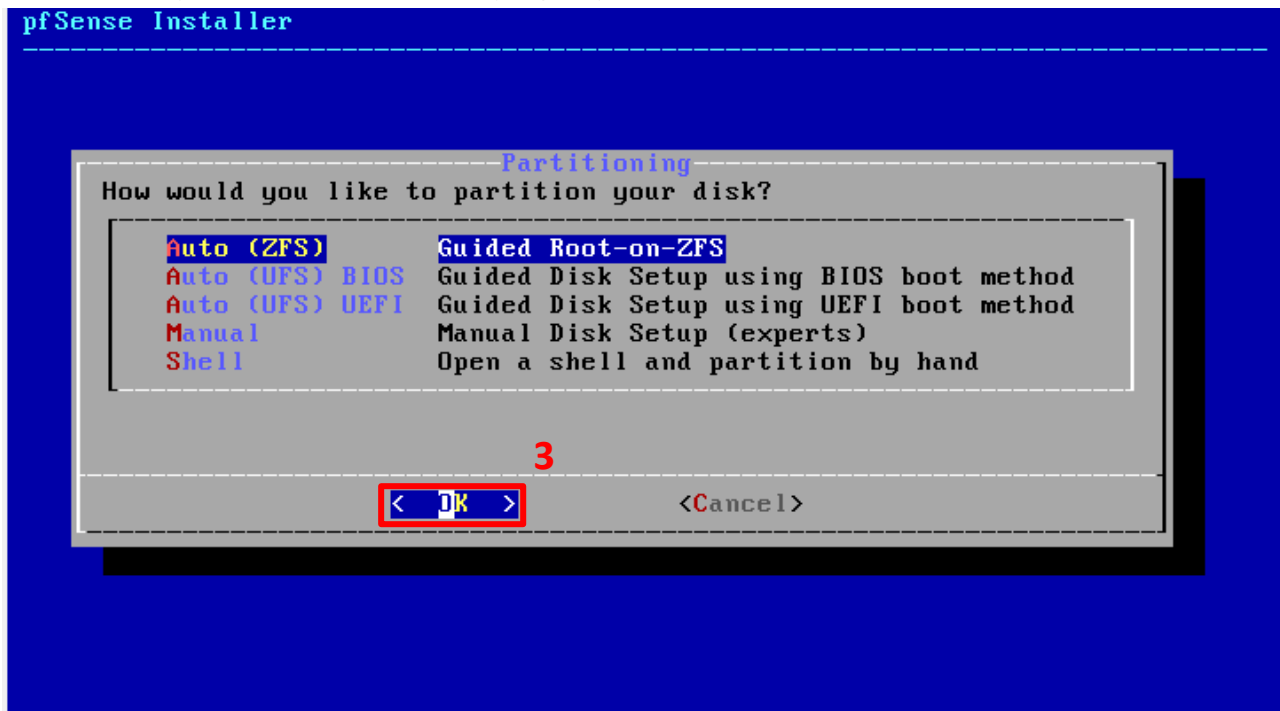
Astuce de manipulation : Touche **Entrée** pour valider et passer à l'étape suivant, touche **Espace** pour cocher.



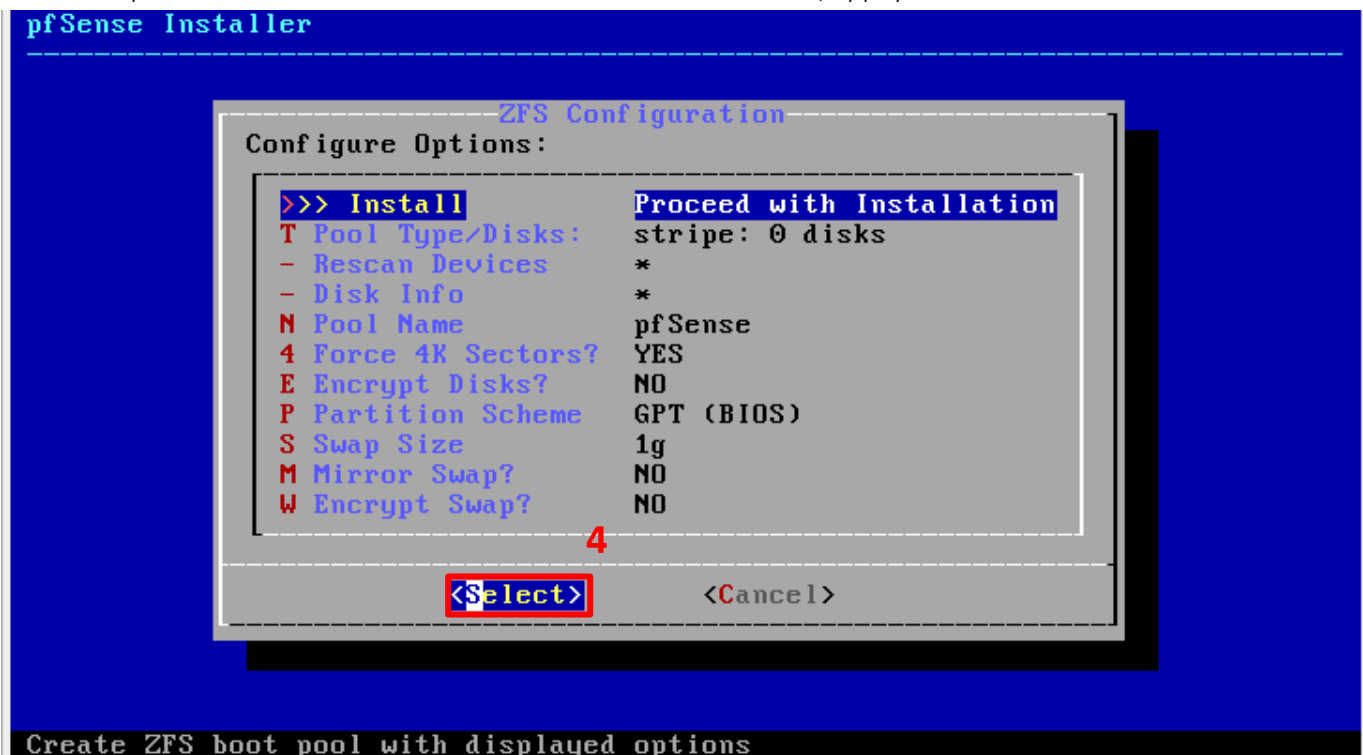
- Sélectionner la langue du clavier (rester sur le clavier FR si vous utilisez AZERTY, ou sélectionner ENG si vous utilisez un clavier sous QWERTY).



- Laisser le partitionnement automatique géré par le ZFS

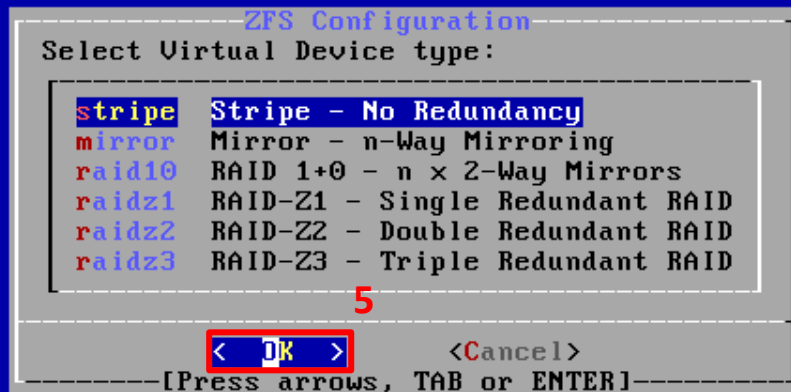


- La prochaine fenêtre vous demandera de valider l'installation, appuyer sur Entrée



- Laisser le paramètre par défaut sur le type de disque pour l'installation. Etant l'unique pare-feu sur le réseau à l'instant, laissez sur le type stripe.

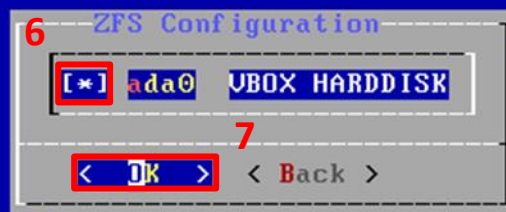
pfSense Installer



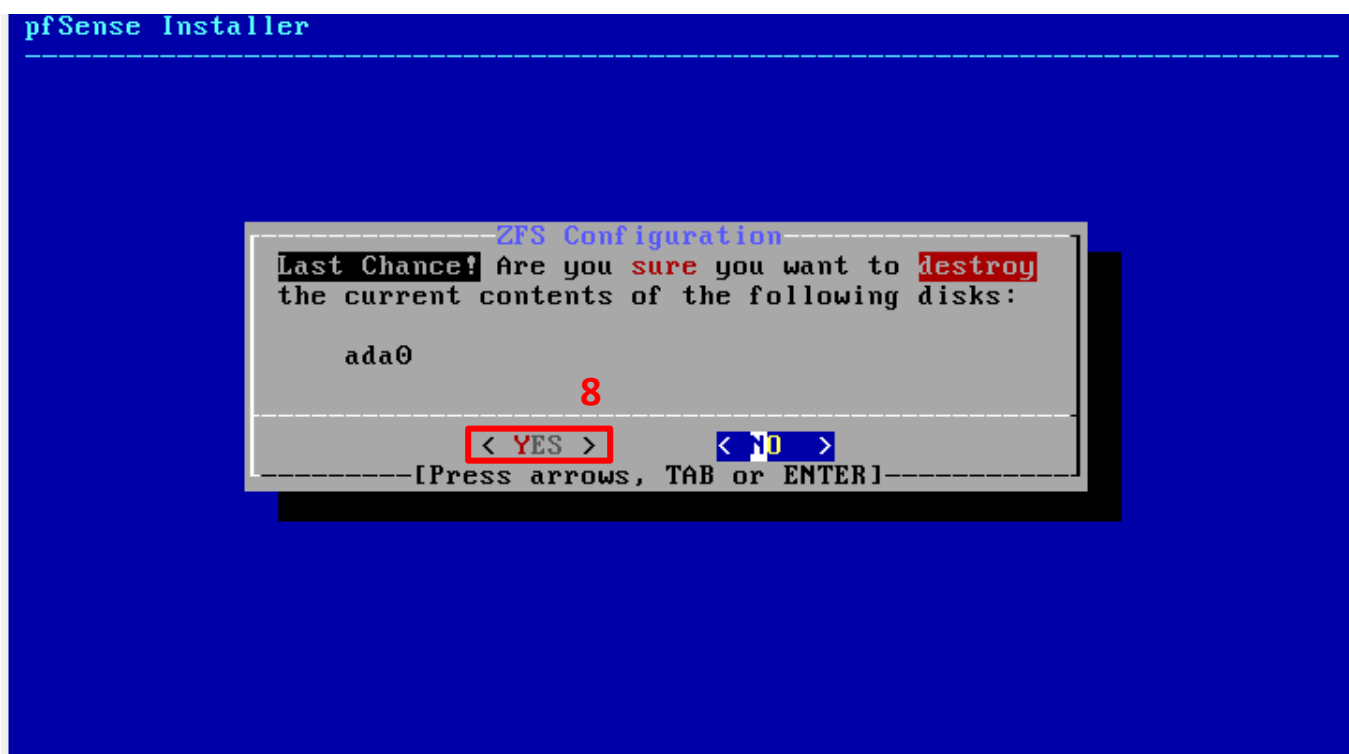
[1+ Disks] Striping provides maximum storage but no redundancy

- Sélectionner le disque pour l'installation. Ici appuyer sur la touche **Espace**, pour cocher le disque puis appuyer sur **Entrée** pour valider.

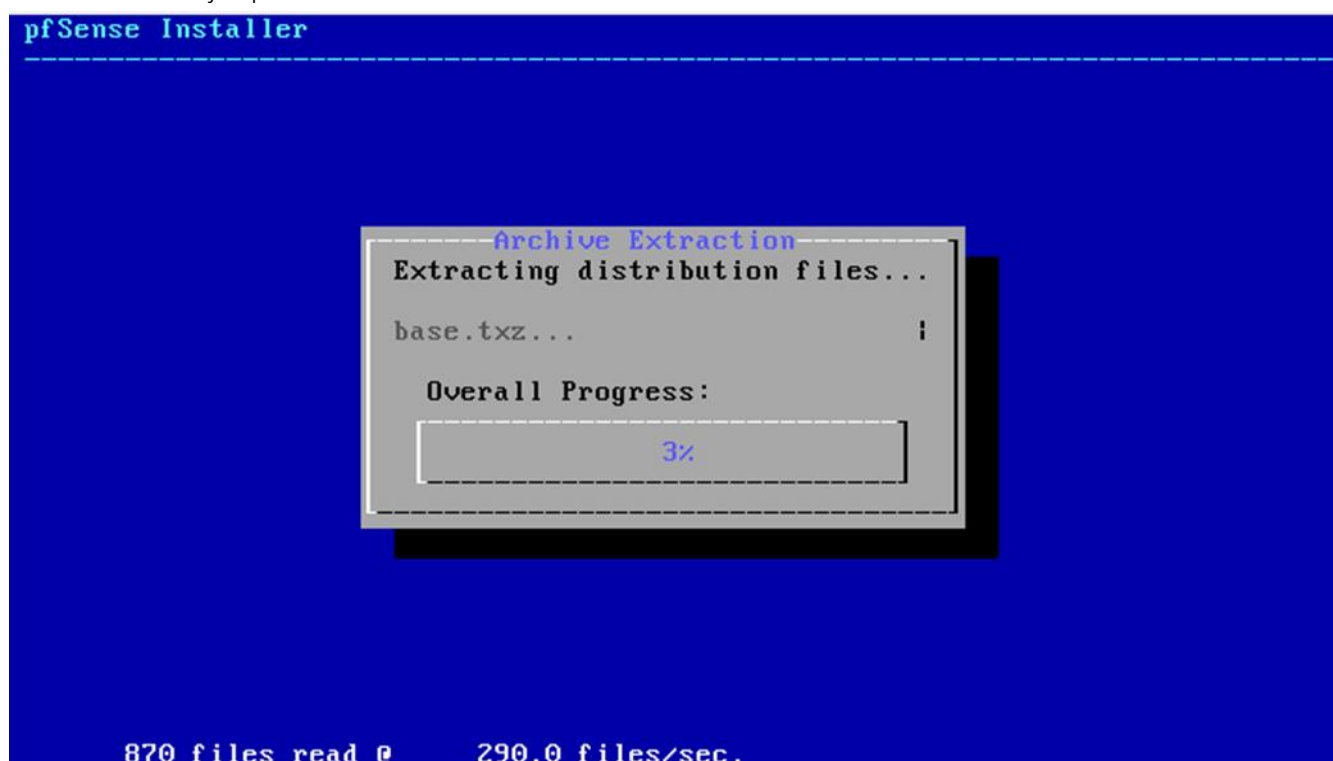
pfSense Installer



- La prochaine étape sera d'accepter le formatage du disque présent, appuyer sur la flèche du gauche puis sur Entrée pour sélectionner YES.

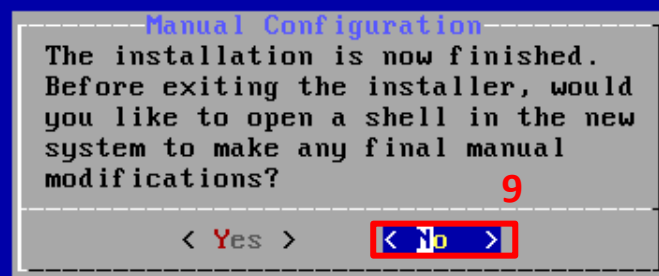


- Patientez jusqu'à la fin de l'installation :



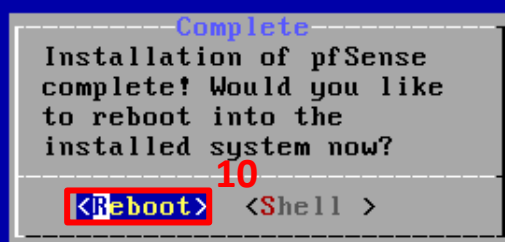
- Ensuite, le programme d'installation nous demandera si nous souhaitant procéder à la configuration actuellement, Sélectionner No. Nous configurerons pfSense plus tard.

pfSense Installer



- Redémarrez ensuite la machine pour finaliser l'installation.

pfSense Installer



II- DOCUMENTATION DE CONFIGURATION

Après redémarrage de pfSense, nous pouvons à présent procéder à la configuration de pfSense. Sur l'écran d'accueil, nous pouvons visualiser les paramètres en cours du réseau de pfSense.


```

VirtualBox Virtual Machine - Netgate Device ID: 9a00f38b0ae2ea9ec024
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 10.77.43.17/24
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:

```

- L'adresse IP WAN est le pont pour pouvoir sortir du réseau et accéder à Internet.
- L'adresse IP LAN sera l'adresse local du réseau, afin de pouvoir isoler les machines en production sur le réseau du réseau externe, créant ainsi une couche de sécurité en plus.

Afin de configurer une option, il suffit de renseigner le numéro auquel l'option est assignée (en exemple 1 pour réassigner les interfaces des cartes réseaux, 2 pour assigner les adresses IP, etc ...)

A- CONFIGURATION DE L'INTERFACE LAN

Etant donné qu'à présent, nous allons surtout agir sur le réseau LAN, nous allons uniquement procéder à la configuration de l'interface LAN. Pour ce faire, sélectionner l'option n°2 en appuyant sur la touche 2, et procéderons comme ci-dessous :

```

VirtualBox Virtual Machine - Netgate Device ID: 9a00f38b0ae2ea9ec024
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.77.43.17/24
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

```

- Sélectionner l'interface LAN en appuyant sur la touche 2.

```

VirtualBox Virtual Machine - Netgate Device ID: 9a00f38b0ae2ea9ec024
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.77.43.17/24
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)
2 - LAN (em1 - static)

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

```

- Renseignez l'adresse IP du pfSense sur le réseau LAN, dont 192.168.100.254. Une norme dans la configuration souhaite que les pare-feux, qui feront office de passerelle ont soit comme adresse, la première adresse du réseau, ou la dernière adresse sur une plage d'adresse, afin de ne pas rentrer en conflit avec un quelconque serveur DHCP sur le réseau.

```

WAN (wan)      -> em0      -> v4/DHCP4: 10.77.43.17/24
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)
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:
> 192.168.100.254

```

- Il faut à présent renseigner le masque de sous-réseau, en notation CIDR. Pour notre cas, ce sera le masque de sous-réseau de 255.255.255.0 équivalent à 24 en CIDR.

```

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)
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:
> 192.168.100.254

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

```

- Ensuite, appuyer sur la touche **Entrée**, comme l'indique l'option car nous configurons actuellement une interface réseau sur le réseau LAN. Et comme nous voulions pas la configuration de l'IPv6 sur le réseau, appuyer également sur la touche **Entrée**, comme il est indiqué.

```

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:
> 192.168.100.254

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

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

```

```

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:
> 192.168.100.254

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

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:
>

```

- Ensuite, nous activerons le DHCP server de pfSense plus tard sur l'interface graphique, ainsi appuyer sur n pour Non, et appuyer sur la touche **Entrée** pour valider.

```

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:
> 192.168.100.254

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

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

```

- Accepter ensuite la configuration par webConfigurator (c'est ce qui nous permettra d'administrer pfSense en interface graphique sur le réseau) et appuyer sur la touche **Entrée**, pour terminer la configuration.

```
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 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) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

The IPv4 LAN address has been set to 192.168.100.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.100.254/





Press <ENTER> to continue.i
```

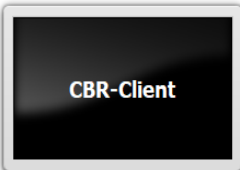
B- TEST D'INTÉGRATION

Pour ce test d'intégration, nous allons démarrer une machine cliente Windows dans le réseau local, et configurer son adresse IP pour faire en sorte qu'il soit sur le réseau de pfSense.

Cette machine cliente aura comme configuration matérielle :

- Système d'exploitation : Windows 10 Pro
- Stockage : 50 Go
- Mémoire vive : 2 Go
- Réseau : en local sur le LAN

Général Nom : CBR-Client Système d'exploitation : Windows 10 (64-bit) Groupes : TP-Cybersécurité	Prévisualisation 
System Mémoire vive : 2048 Mo Ordre d'amorçage : Disquette, Optique, Disque dur Accélération : VT-x/AMD-V, Pagination imbriquée, Paravirtualisation Hyper-V	
Affichage Mémoire vidéo : 256 Mo Contrôleur graphique : VBoxSGA Serveur de bureau à distance : Désactivé Enregistrement : Désactivé	
Stockage Contrôleur : SATA Port SATA 0 : CLIENT.vmdk (Normal, 50,00 Gio) Port SATA 1 : [Lecteur optique] Vide	
Audio Pilote hôte : Windows DirectSound Contrôleur : Intel Audio HD	
Réseau Interface 1: Intel PRO/1000 MT Desktop (Réseau interne, 'intnet')	
USB Contrôleur USB : xHCI Filtres de périphérique : 0 (0 actif)	
Dossiers partagés Aucun	
Description Aucune	

CONFIGURATION DE L'ADRESSE IP SOUS WINDOWS

Pour configurer l'adresse IP nous pouvons passer soit par l'interface graphique en passant par la configuration des cartes réseaux du Panneau de configuration de Windows (accessible en tapant **ncpa.cpl** sur le menu Exécuter de Windows), soit par ligne de commande en utilisant l'utilitaire Networks shell sur l'invite de commande.

INTERFACE GRAPHIQUE

Exécuter

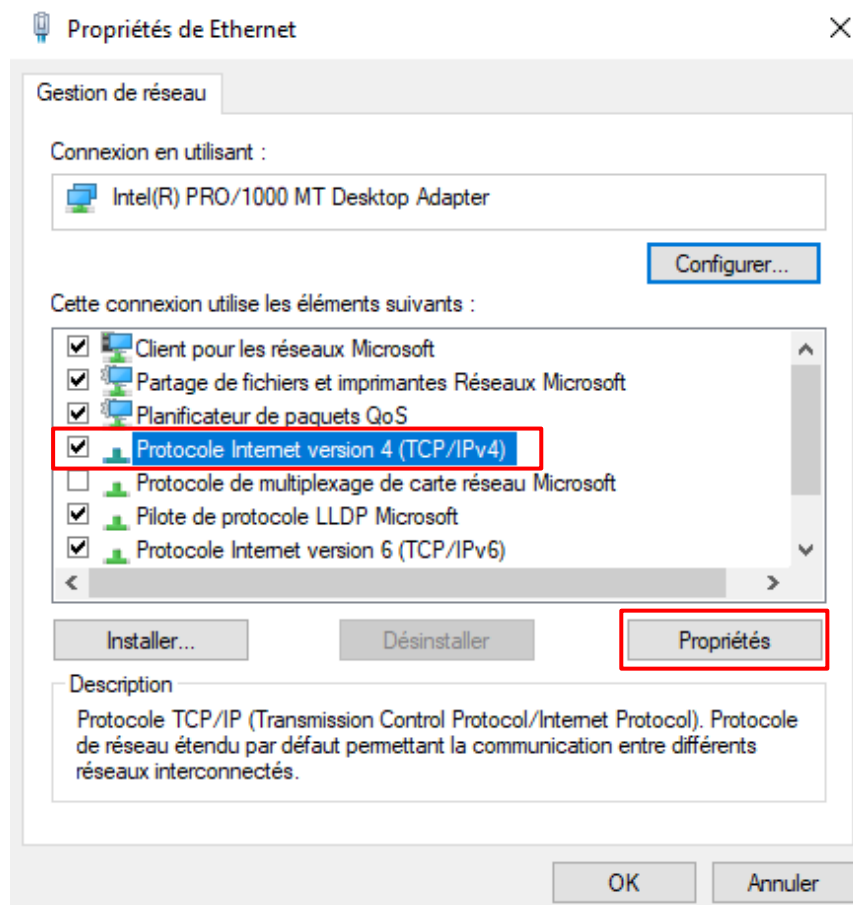
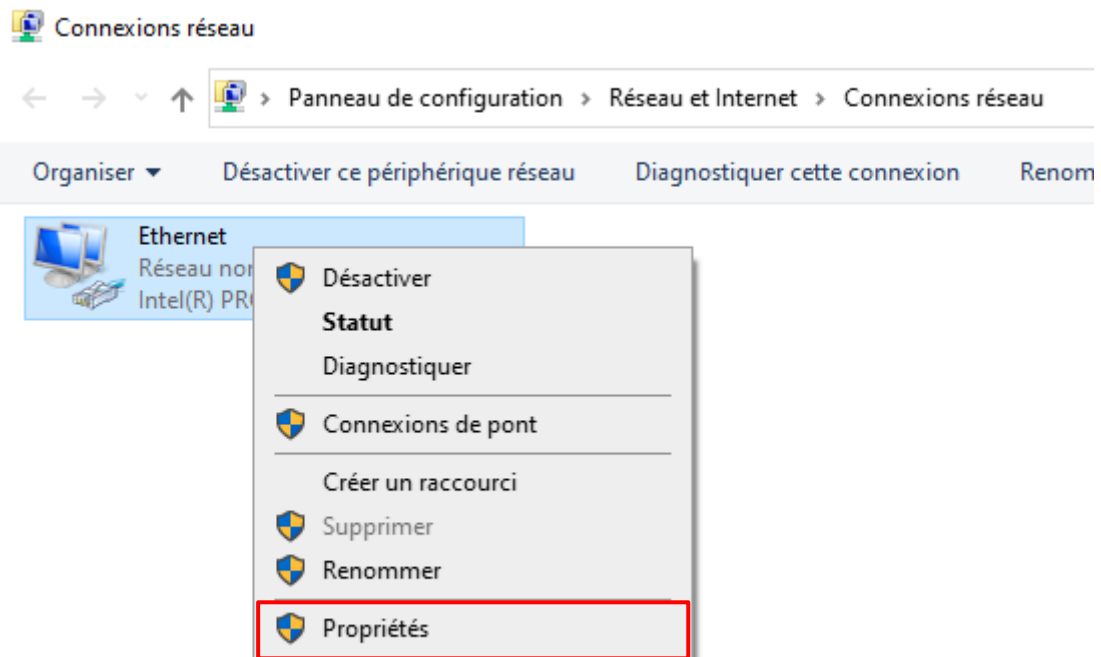
Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.

Ouvrir :

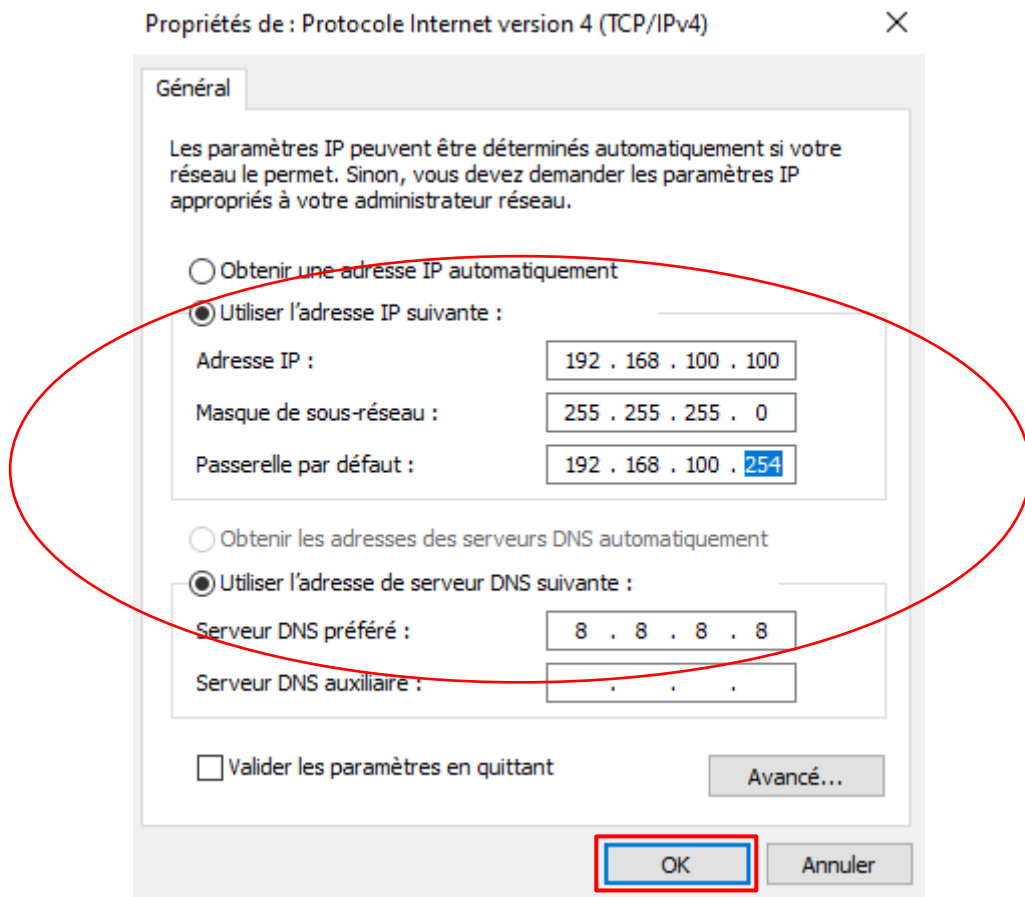
OK

Annuler

Parcourir...



- Renseignez l'adresse IP de la votre machine cliente, sur le réseau 192.168.100.0, comme passerelle par défaut l'adresse IP du pfSense dont 192.168.100.254, et le DNS de google pour permettre la résolution de nom de domaine sur le réseau qui est 8.8.8.8.



A présent votre adresse IP est dans le réseau, procéder à une vérification en effectuant une **ipconfig** sur l'invite de commande.

```
Microsoft Windows [version 10.0.19044.1288]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Client>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::f805:bbba:2fc6:6bdc%12
    Adresse IPv4. . . . . : 192.168.100.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.100.254
```

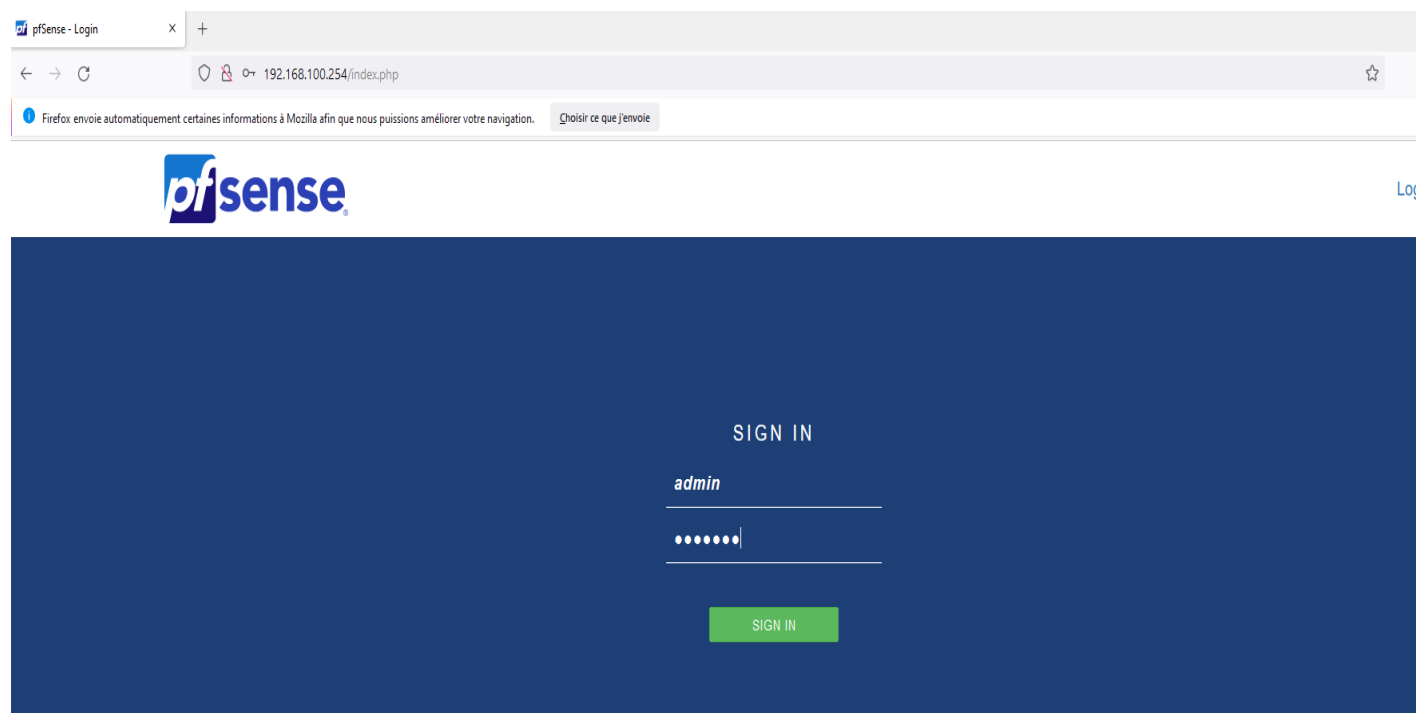
LIGNE DE COMMANDE

La commande pour configurer directement l'adresse IP en ligne de commande en passant par le network shell est :

```
netsh interface ipv4 set address name=Ethernet static 192.168.100.100 255.255.255.0 192.168.100.254
```


CONNEXION AU WEBCONFIGURATOR DE PFSense

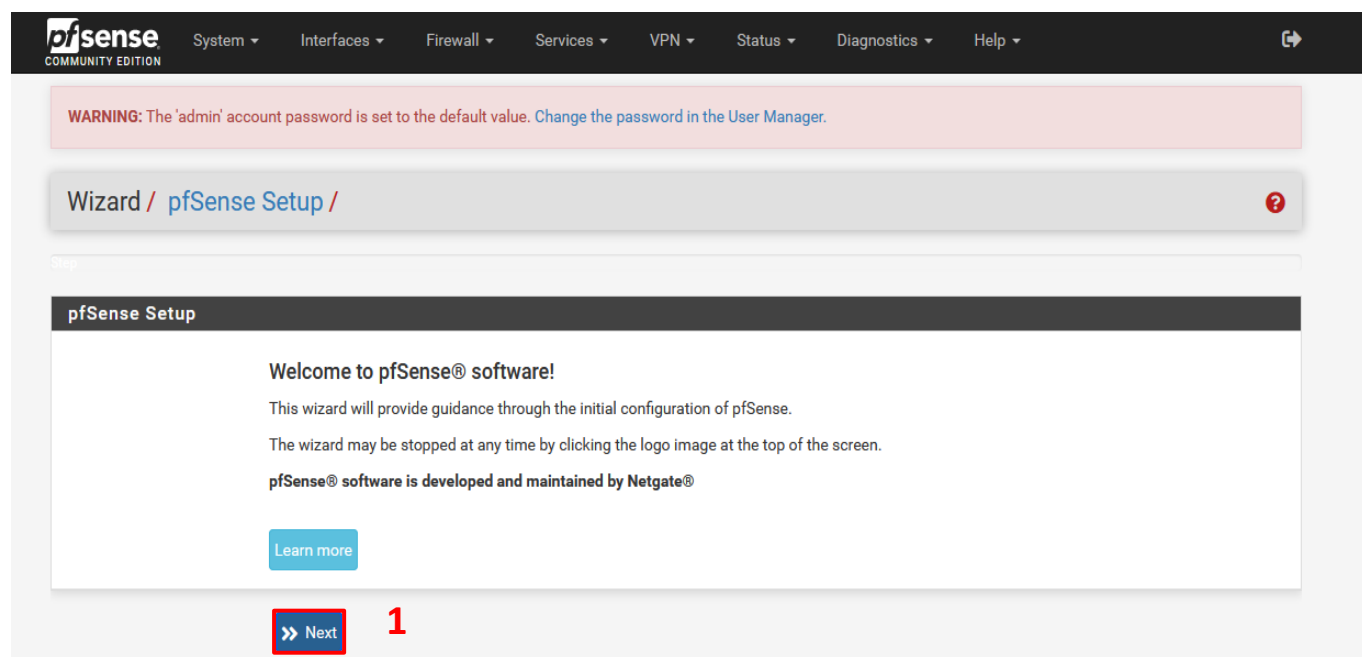
Pour se connecter à l'interface graphique de pfSense, dans un navigateur, renseigner l'adresse IP de pfsense sur le réseau local **192.168.100.254**, et comme login par défaut : Identifiant : admin ; Mot de passe : pfsense



III- DOCUMENTATION DE PARAMETRAGE

Nous allons à présent procéder au paramétrage de pfSense, et pour ce faire, il nous faut se connecter sur l'interface graphique de pfSense, et procéder à l'installation de pfSense (Setup Wizard), et procéder comme ci-dessous :

A- SETUP PFSense



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

Wizard / [pfSense Setup](#) / [Netgate® Global Support is available 24/7](#) ?

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

[» Next](#)

2

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

Wizard / [pfSense Setup](#) / [Netgate® Global Support is available 24/7](#) ?

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

[» Next](#)

3

1. A présent paramétrer le serveur DNS sur pfSense, vous pouvez le laisser par défaut, ou laisser uniquement le DNS de google 8.8.8.8

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

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
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 **4**

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

5

2. Laisser le paramètre de serveur de temps par défaut

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

Wizard / pfSense Setup / Time Server Information ?

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

6

3. Ensuite, on passera à l'étape de la configuration des interfaces de pfSense, (exactement ce que nous avons effectuer en ligne de commande sur la machine dans la partie [II-Documentation de configuration](#)), ainsi appuyez sur **Next**.

RFC1918 Networks

Block RFC1918 Private Networks ☒ Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks ☒ Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

7

4. De même pour l'interface LAN, laisser la configuration telle qu'elle a été configurée.

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

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

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

LAN IP Address

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

8

[» Next](#)

5. Ensuite, renseignez le nouveau mot de passe admin de pfSense afin de ne plus avoir le message d'erreur présent, mais aussi de mieux sécuriser l'accès au pare-feu.

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

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

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

Admin Password

Admin Password AGAIN

9

[» Next](#)

6. Appuyer sur Reload pour recharger pfSense et appliquer les changements effectués.

Wizard / pfSense Setup / Reload configuration

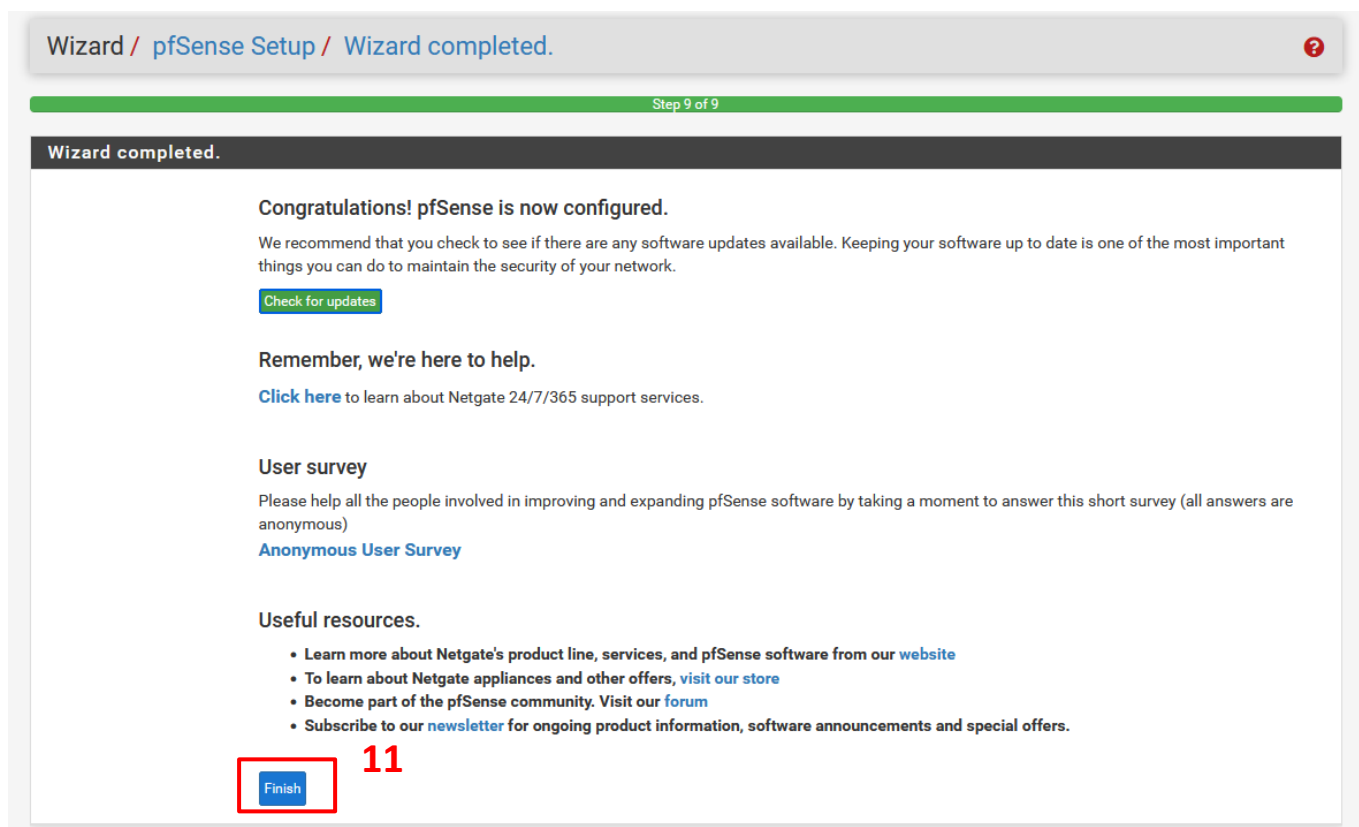
Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

10

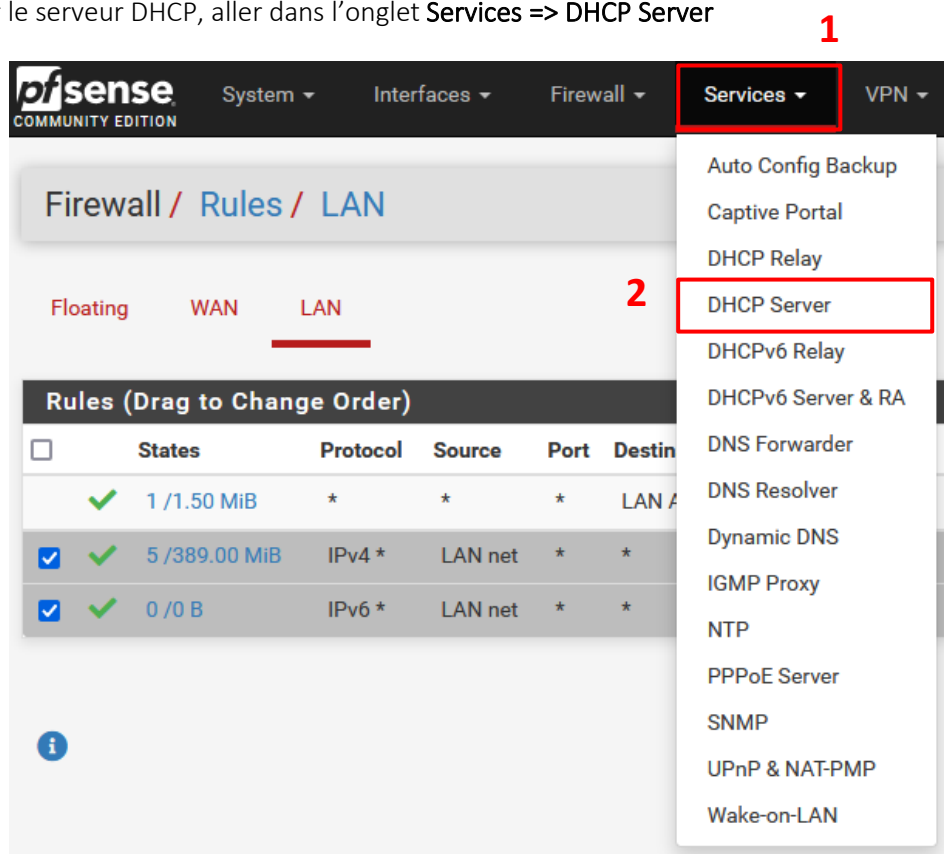
[» Reload](#)



Le setup de pfSense est actuellement terminé, nous allons procéder au paramétrage des filtrages.

B- PARAMETRAGE DU SERVEUR DHCP

Pour paramétrer le serveur DHCP, aller dans l'onglet **Services => DHCP Server**



Services / DHCP Server / LAN

LAN

General Options

Enable ☒ Enable DHCP server on LAN interface **3**

BOOTP ☐ Ignore BOOTP queries

Deny unknown clients **4**

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.
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.
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

Additional BOOTP/DHCP Options [Display Advanced](#)

[Save](#)

DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostnam
------------	-------------	------------	---------

C- PARAMETRAGE DU FILTRAGE «DENY ALL »

Nous allons mettre en place un filtrage « deny all » qui bloquera tous les ports par défaut, incluant ceux de l'internet (que nous débloquerons plus tard dans la partie Paramètre de filtrage internet).

Pour paramétrer les règles de filtrage sur pfSense, allez dans l'onglet **Firewall => Rules**, et sélectionner l'interface LAN, car nous voudrions, au terme de cette procédure, sécuriser le trafic sur le réseau LAN de production.

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ **1** **Firewall ▾** Services ▾ VP

Services / DHCP Server / LAN

The changes have been applied successfully.

2

- Aliases
- NAT
- Rules**
- Schedules
- Traffic Shaper
- Virtual IPs

LAN

Ci-dessous les règles de filtrage par défaut de pfSense :

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1 / 1.74 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 4 / 389.04 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

7. Supprimer les deux règles par défaut et créer une nouvelle règle qui bloquera tous les accès et tous les ports sur le réseau. (Cocher les deux règles, et cliquer sur l'icône de corbeille pour supprimer)

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 1.74 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	✓ 4 / 389.04 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

Firewall / Rules / LAN

Floating WAN LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 1.77 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

8. Cliquer sur la touche **Add** pour ajouter une règle. De principe, pfSense lis les règles de haut vers le bas.

Floating WAN **LAN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 / 1.78 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

6

Add Add Delete Save Separator

9. Mettre l'action sur **Block**, pour bloquer toutes les connexions et ports

Firewall / Rules / Edit

Edit Firewall Rule

Action Block 7
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.

10. Sélectionner **any** pour Source et Destination pour tous bloquer sur le réseau

Source

Source ☐ Invert match any 8 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 any 9

From Custom 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
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 10

D- PARAMÉTRAGE DU FILTRAGE INTERNET

Pour autoriser l'accès internet sur le réseau, nous allons ouvrir les ports suivant sur notre pare-feu : 80 pour le http, 443 pour le https, et 53 pour la résolution de noms (DNS).

Pour cela, encore dans **Firewall => Rules => LAN**, cliquer sur Add, mais pour ce cas-ci le Add vers le haut pour créer la règle tout en haut de la table de filtrage, afin qu'elles aient la priorité sur le filtrage « Deny All ».

Floating **WAN** LAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1 / 933 KIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	*	*	*	none			

↑ Add ↓ Add Delete Save + Separator 1

- Sélectionner l'action Pass pour autoriser le port sur le réseau LAN, sur la famille d'adresse IPv4, et le protocole TCP pour le port 80 et 443, et le protocole UDP pour le port 53 du DNS. Cependant, si deux serveurs DNS communiquent ensemble, notamment par exemple sur un environnement de redondance, il faudra autoriser la règle sur le protocole TCP et le protocole UDP.

Et enfin, Comme nous voudrions maîtriser les connexions sur le réseau LAN, nous allons uniquement prendre en source le LANnet.

Edit Firewall Rule

Action Pass 2

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 3

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 (other) 80 (other) 80 4

From Custom 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 (see the [Status: System Logs: Settings](#) page).

Description Autorisation du port 80 (HTTP)

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the log.

Advanced Options ⚙ Display Advanced

Save 5

12. Et enfin appliquer la table de filtrage en cliquant sur **Apply Changes**.

Firewall / Rules / LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes 6

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 / 1.29 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
✓ 5 / 46 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none		Autorisation du port 53 (DNS)	⬇ ⬆ ⬇ ⬇
✓ 3 / 3.08 MiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		Autorisation du port 443 (HTTPS)	⬇ ⬆ ⬇ ⬇
✓ 5 / 25 KiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		Autorisation du port 80 (HTTP)	⬇ ⬆ ⬇ ⬇
✗ 0 / 43 KiB	IPv4 TCP	LAN net	*	*	*	*	none			⬇ ⬆ ⬇ ⬇

↑ Add
↓ Add
Delete
Save
+ Separator

BONUS : CRÉATION D'UN ALIAS DE FILTRAGE INTERNET

Il est également possible de créer un alias pour le filtrage, regroupant plusieurs règles de filtrage, par exemple l'autorisation des ports 53, 80 et 443 sur une seule règle en alias. Pour cela, naviguer dans **Firewall => Aliases**

Firewall Aliases IP

Name	Values	Description	Actions
------	--------	-------------	---------

1 + Add Import

Renseigner ensuite le nom de l'alias, le type (Port pour l'équivalent de la règle), et sur la case port, afin d'ajouter plusieurs ports, il faut les séparer par des « ; »

Firewall / Aliases / Edit

Properties

Name **2**
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description **3**
A description may be entered here for administrative reference (not parsed).

Type **4**

Port(s)

Hint Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	Protocol	Action
<input type="text" value="80"/>	<input type="text" value="HTTP"/>	Delete
<input type="text" value="443"/>	<input type="text" value="HTTPS"/>	Delete
<input type="text" value="53"/>	<input type="text" value="DNS"/>	Delete

5 Save + Add Port

Firewall / Aliases / Ports

IP **Ports** **URLs** **All**

Firewall Aliases Ports

Name	Values	Description
Internet_access	80, 443, 53	Autorisation port 80,443,53

ALIAS Créé !

13. Ensuite pour l'appliquer, retourner vers **Firewall => Rules**, ajouter une nouvelle règle, et remplissez la nouvelle règle comme ci-dessous. Remplir le port en other et renseigner le nom de l'alias

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/UDP

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

(other)

Internet_access

(other)

Internet_access

From

Custom

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

Access

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

Rule Information

Tracking ID

1655293374

Created

6/15/22 11:42:54 by admin@192.168.100.100 (Local Database)

Updated

6/15/22 11:42:54 by admin@192.168.100.100 (Local Database)

Save

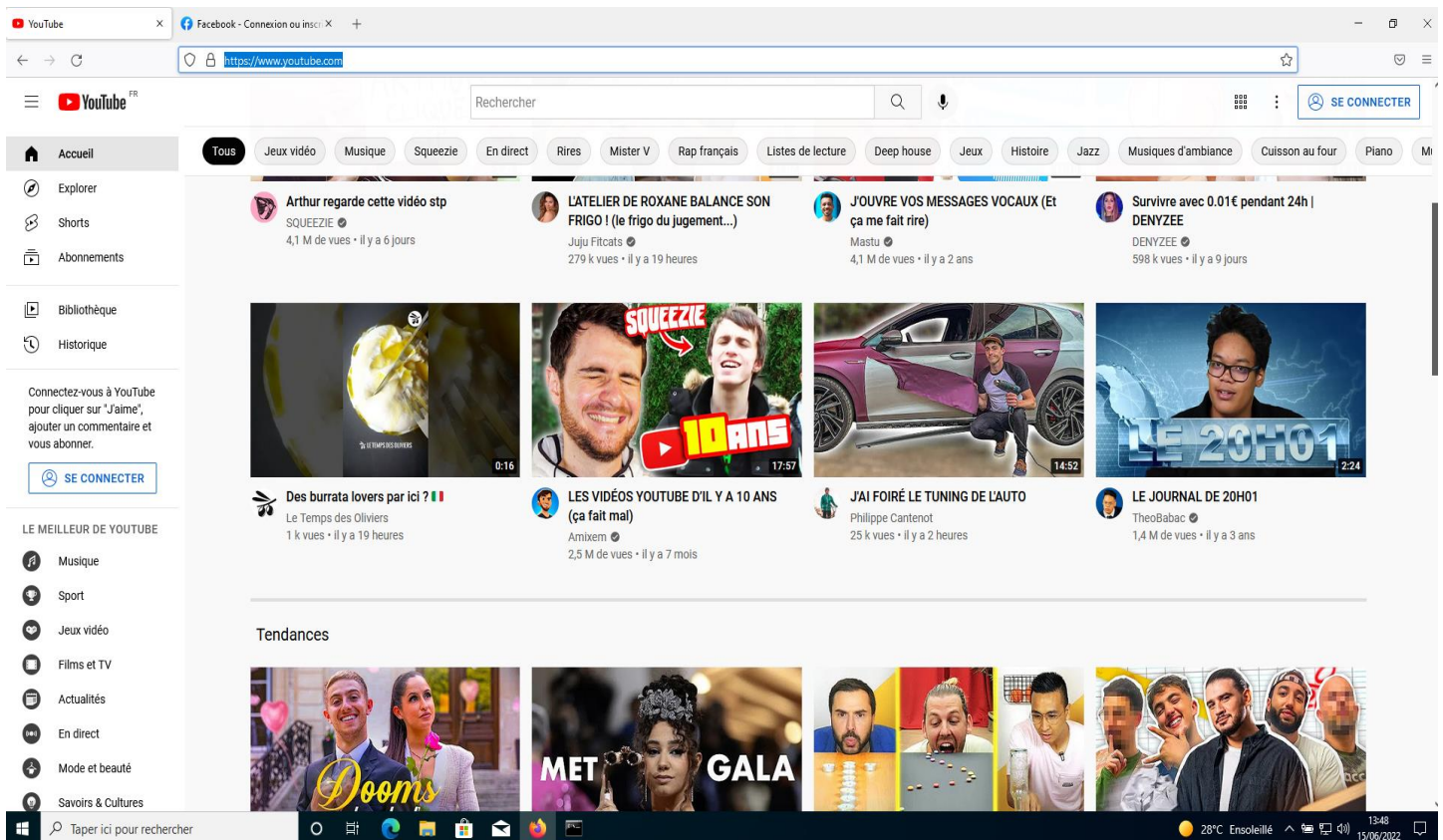
14. La nouvelle table de filtrage sera ainsi que comme ci-dessous :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 3 / 1.47 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓ 14 / 3.16 MiB	IPv4 TCP/UDP	LAN net	*	*	Internet_access	*	none		Acces Internet	🔗✎📄🗑️
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	LAN net	*	*	*	*	none			🔗✎📄🗑️

⬆️ Add
⬆️ Add
🗑️ Delete
💾 Save
⚡ Separator

TEST D'INTÉGRATION

Sur une machine cliente, essayer de se connecter sur Internet en allant sur le navigateur et rentrer sur l'adresse de Youtube.



Internet Ok => Test OK, règle appliqué.

E- MISE EN PLACE D'UN PORTAIL CAPTIF SOUS PFSense

Pour augmenter encore plus l'accès Internet sur le réseau LAN, il est également possible de mettre en place un portail captif sur ce réseau.

1. CREATION DU PORTAIL CAPTIF

Pour ce faire, naviguer dans **Services => Captive Portal**, puis cliquer sur **Add**. Renseignez ensuite le nom du portail, par exemple **CCI_CAMPUS_Portal**.

Activez ensuite le Portail Captif, et configurez comme ci-dessous :

Services / Captive Portal / CCI_CAMPUS_Portal / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Captive Portal Configuration

Enable	<input checked="" type="checkbox"/> Enable Captive Portal 1
Description	<input type="text" value="Portail Captif"/> <small>A description may be entered here for administrative reference (not parsed).</small>
Interfaces	<div><div>WAN</div><div>LAN</div></div> 2 <small>Select the interface(s) to enable for captive portal.</small>
Maximum concurrent connections	<input type="text" value="1"/> <small>Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.</small>
Idle timeout (Minutes)	<input type="text" value="4"/> <small>Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.</small>
Hard timeout (Minutes)	<input type="text"/> <small>Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).</small>
Traffic quota (Megabytes)	<input type="text"/> <small>Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.</small>
Pass-through credits per MAC address.	<input type="text"/>

Waiting period to restore
pass-through credits.
(Hours)

Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.

Reset waiting period

☐ Enable waiting period reset on attempted access

If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.

Logout popup window

☒ Enable logout popup window

3

If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Pre-authentication
redirect URL

Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURL\$ variable in captiveportal's HTML pages.

After authentication
Redirection URL

Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

Blocked MAC address
redirect URL

Blocked MAC addresses will be redirected to this URL when attempting access.

Preserve users database

☐ Preserve connected users across reboot

If enabled, connected users won't be disconnected during a pfSense reboot.

Concurrent user logins

4

Disabled: Do not allow concurrent logins per username or voucher.

Multiple: No restrictions to the number of logins per username or voucher will be applied.

Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected.

First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.

MAC filtering

☒ Disable MAC filtering

If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Pass-through MAC Auto

☐ Enable Pass-through MAC automatic additions

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 ▲

5

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 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

6

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

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
CCI_CAMPUS_Portail	LAN	0	Portail Captif	 

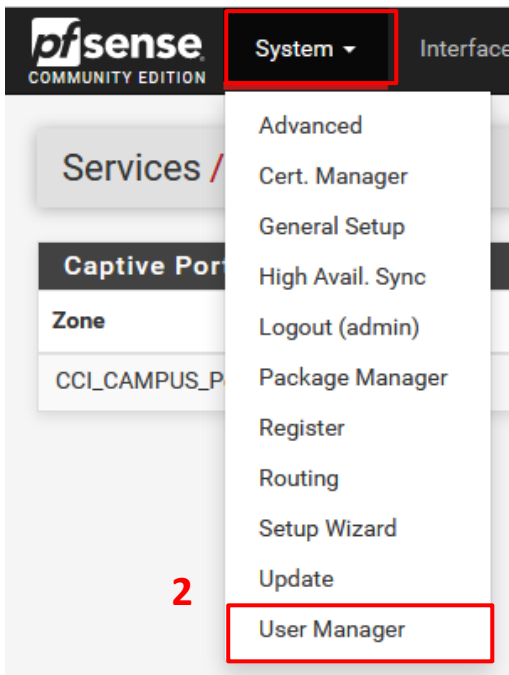
Portail captif créé

 Add

2. CREATION D'UN UTILISATEUR POUR SE CONNECTER SUR LE PORTAIL

Pour créer un utilisateur pouvant se connecter sur le portail captif afin d'accéder à Internet, naviguez dans **System => User Manager** et suivez les instructions ci-dessous


1



2

3

Users Groups Settings Authentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

+ Add **Delete**

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username toto

Password

Full name Toto TOTO
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership admins

Not member of Member of

>> Move to "Member of" list **<< Move to "Not member of" list**

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.

Cependant, actuellement, nous n'avons aucun Certificat d'authentification ainsi nous resterons sur une connexion sur le port http au Portail. A présent nous allons affilier les droits de se connecter et le certificat d'authentification au portail à l'utilisateur.

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input checked="" type="checkbox"/>	toto	Toto TOTO	✓		

+ Add

Delete

GESTION DES DROITS

Pour affilier les droits d'authentification, cliquer sur le bouton **Add** sous Effective Privileges.

Effective Privileges

Inherited from	Name	Description	Action
----------------	------	-------------	--------

+ Add

Sélectionner User-Services : Captive Portal Login pour permettre la connexion à travers le portail Captif.

User toto (Toto TOTO)

Assigned privileges

5

User - Services: Captive Portal login

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

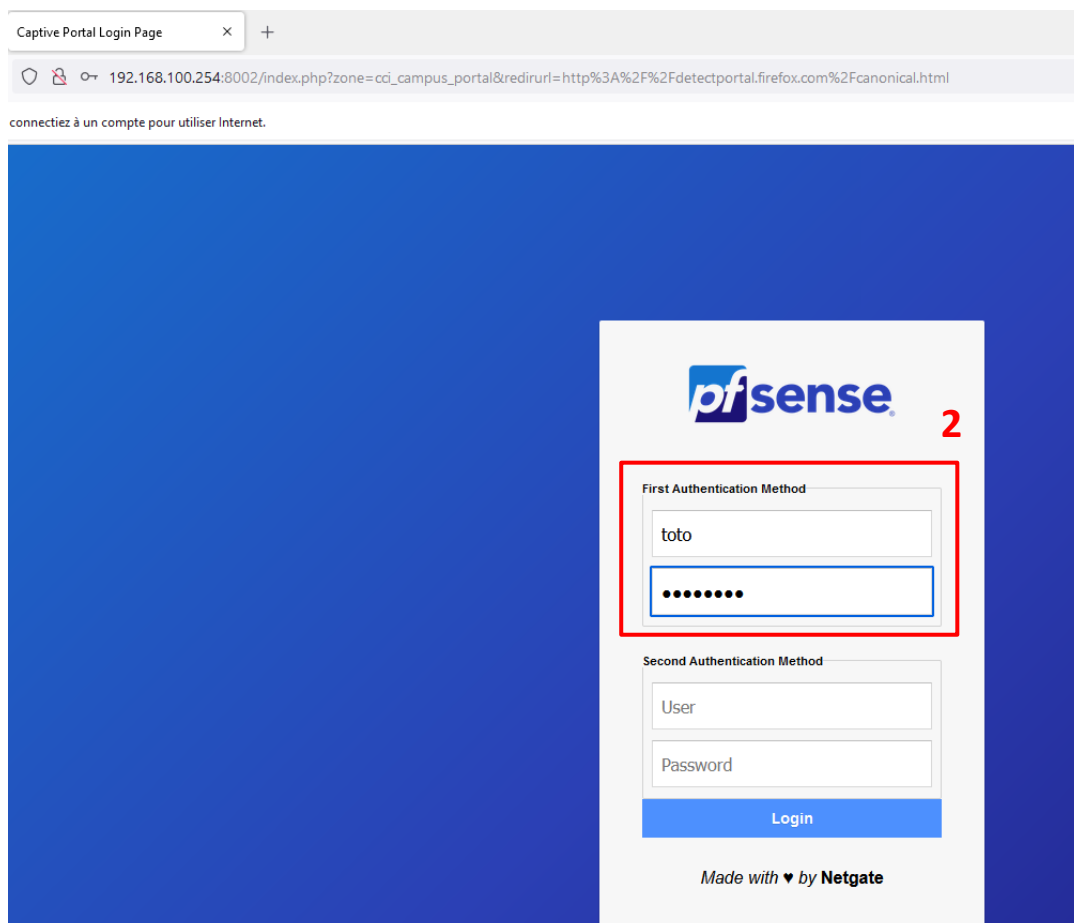
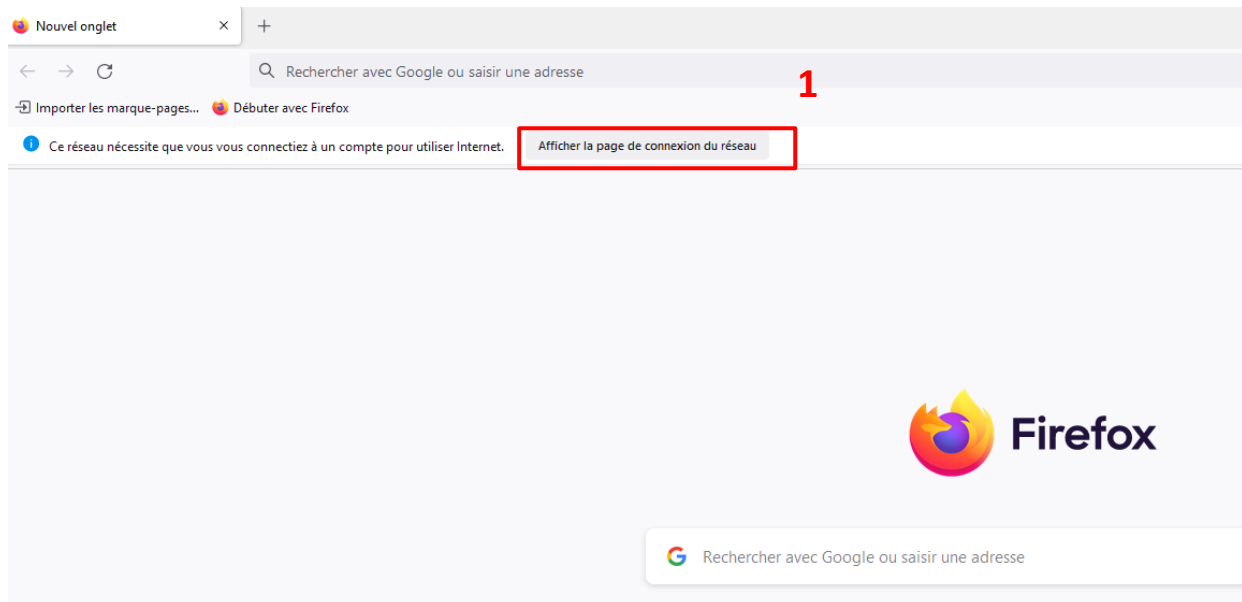
Filter

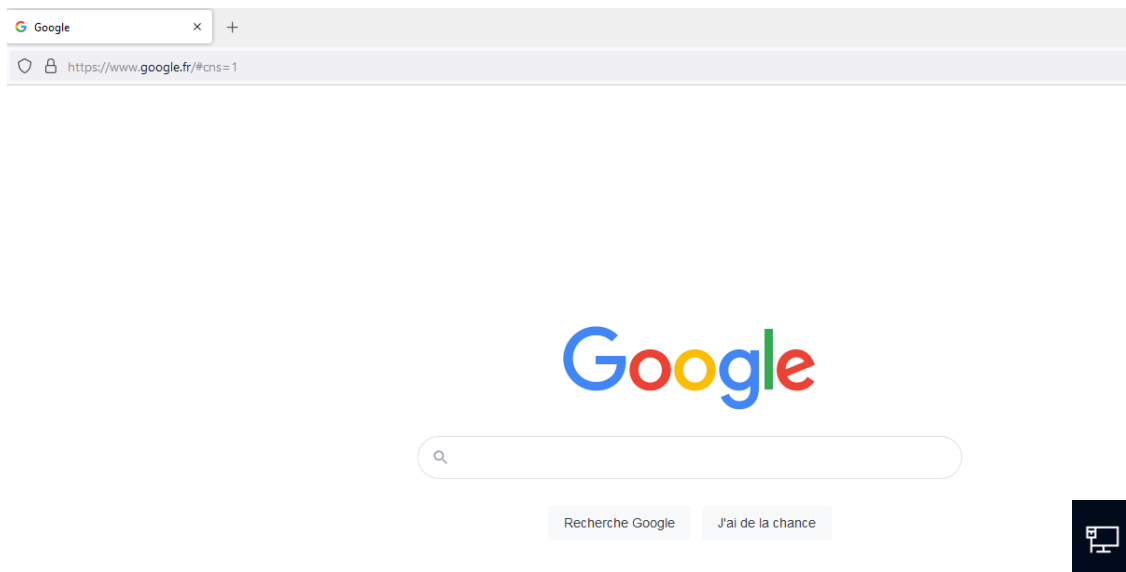
Show only the choices containing this term

3. TEST D'INTÉGRATION

Sur une machine cliente, ouvrir un navigateur web, malgré le fait que la machine n'est pas connectée à Internet. Normalement une fenêtre de sécurité apparaît, et cliquer sur le bouton pour **afficher la page de connexion réseau**.

Si la page d'accueil du navigateur est configurée pour rediriger vers Google, le portail apparaîtra automatiquement par suite du paramétrage effectué. Renseigner le login de l'utilisateur toto créé.





La connexion a été établie. Test OK.