

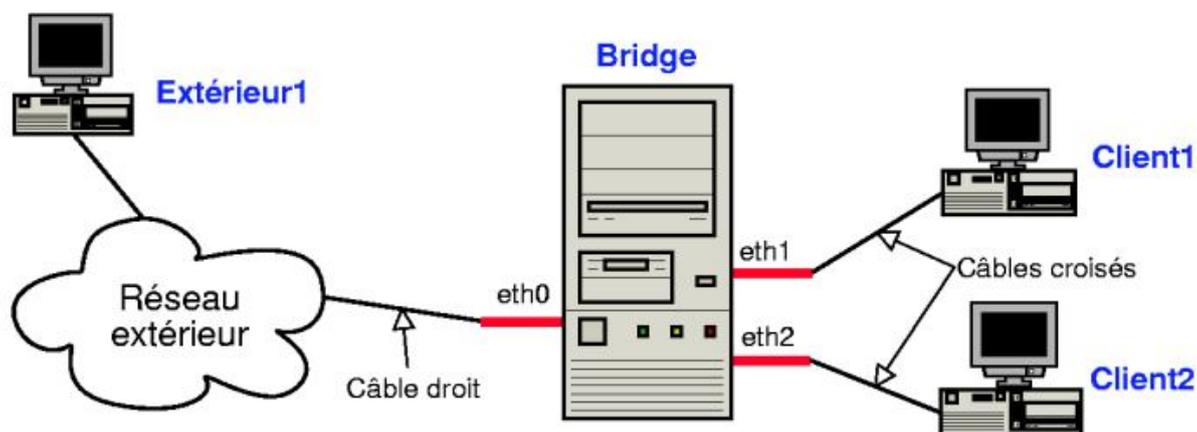
Mise en place d'une solution de pare-feu pfsense

Documentation :

1. Qu'est-ce qu'un Linux bridge ?

L'idée est d'ajouter à votre ordinateur sous Linux la fonction de switch Ethernet aussi appelée bridge ;

Pour ajouter à votre ordinateur sous Linux cette fonction de bridge, il lui faut au minimum deux cartes réseau. Chaque carte réseau devient alors l'équivalent d'un port du switch. Le bridge fonctionnera comme un switch Ethernet classique : il apprend tout seul les adresses MAC qui sont derrière ses interfaces réseau et aiguille les paquets Ethernet comme un switch. Par contre, contrairement à un switch classique, il ne croise pas la connexion réseau : il faudra donc relier le bridge aux autres ordinateurs par des câbles croisés, et aux autres switchs par des câbles droits (les câbles "normaux" sont des câbles droits).



2. Qu'elle est sa fonction ici ?

3. Définissez la fonction d'un pare-feu.

Un pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données.

4. Sur quel système d'exploitation est basé pfsense ?

pfSense est une distribution de type « routeur / pare-feu », sous FreeBSD. C'est un système d'exploitation à part entière dont les maîtres mots sont fiabilité, rapidité, robustesse.

5. Relevez les services essentiels fournis par cette solution.

pfSense permet :

Filtrage par IP source et destination, port du protocole, IP source et destination pour le trafic TCP et UDP

Capable de limiter les connexions simultanées sur une base de règle

pfSense utilise p0f, un utilitaire permettant de filtrer le trafic en fonction du système d'exploitation qui initie la connexion.

Possibilité d'enregistrer ou de ne pas enregistrer le trafic correspondant à chaque règle.

Politique très souple de routage possible en sélectionnant une passerelle sur une base par règle (pour l'équilibrage de charge, basculement, connexions WAN multiples, etc).

Utilisation d'alias permettant le regroupement et la désignation des adresses IP, des réseaux et des ports, rendant ainsi votre jeu de règles de pare-feu propre et facile à comprendre, surtout dans des environnements avec plusieurs adresses IP publiques et de nombreux serveurs.

Filtrage transparent au niveau de la Couche 2, le pare-feu est capable d'agir en pont filtrant.

La normalisation des paquets est utilisée, il n'y a donc aucune ambiguïté dans l'interprétation de la destination finale du paquet. La directive « scrub » réassemble aussi des paquets fragmentés, protège les systèmes d'exploitation de certaines formes d'attaque, et laisse les paquets TCP contenant des combinaisons de Flags invalides.

Activé dans pfSense par défaut Vous pouvez le désactiver si nécessaire. Cette option provoque des problèmes pour certaines implémentations NFS, mais elle est sûre et devrait être laissée activée sur la plupart des installations. Désactiver le filtre - vous pouvez désactiver entièrement le filtre de pare-feu si vous souhaitez configurer pfSense comme un routeur pur.

Network address translation (NAT)

Rediriger les ports y compris les rangs et l'utilisation de plusieurs adresses IP publiques NAT pour les adresses IP individuelles ou des sous-réseaux entiers.

Redirection NAT Par défaut, le NAT redirige tout le trafic sortant vers l'adresse IP WAN.

Dans le cas de connexions WAN multiples, le NAT redirige le trafic sortant vers l'adresse IP de l'interface WAN utilisée.

NAT réflexion : dans certaines configurations, NAT réflexion est possible si les services sont accessibles par IP publique à partir de réseaux internes.

Basculement base sur CARP et pfsync

Common Address Redundancy Protocol ou CARP est un protocole permettant à un groupe d'hôtes sur un même segment réseau de partager une adresse IP.

Le nom CARP est en fait un sigle qui signifie « Common Address Redundancy Protocol » (Protocole Commun De Redondance D'Adresse), à ne pas confondre avec « Cache Array Routing Protocol » utilisé pour faire de la répartition de charge de mandataires caches web. Il a été créé pour contourner des brevets.

Ce protocole peut être utilisé pour faire de la redondance et de la répartition de charge. Il supporte IPv4 et IPv6, et à le numéro de protocole 112. Il est supporté par pfSense.

pfsync assure la table d'état du pare-feu qui est répliquée sur tous les pare-feu configurés de basculement.

Cela signifie que vos connexions existantes seront maintenues dans le cas d'échec, ce qui est important pour prévenir les perturbations du réseau.

Load Balancing/ Répartition de charge :

La répartition de charge du trafic sortant est utilisée avec plusieurs connexions WAN pour assurer la répartition de charge et des capacités de basculement.

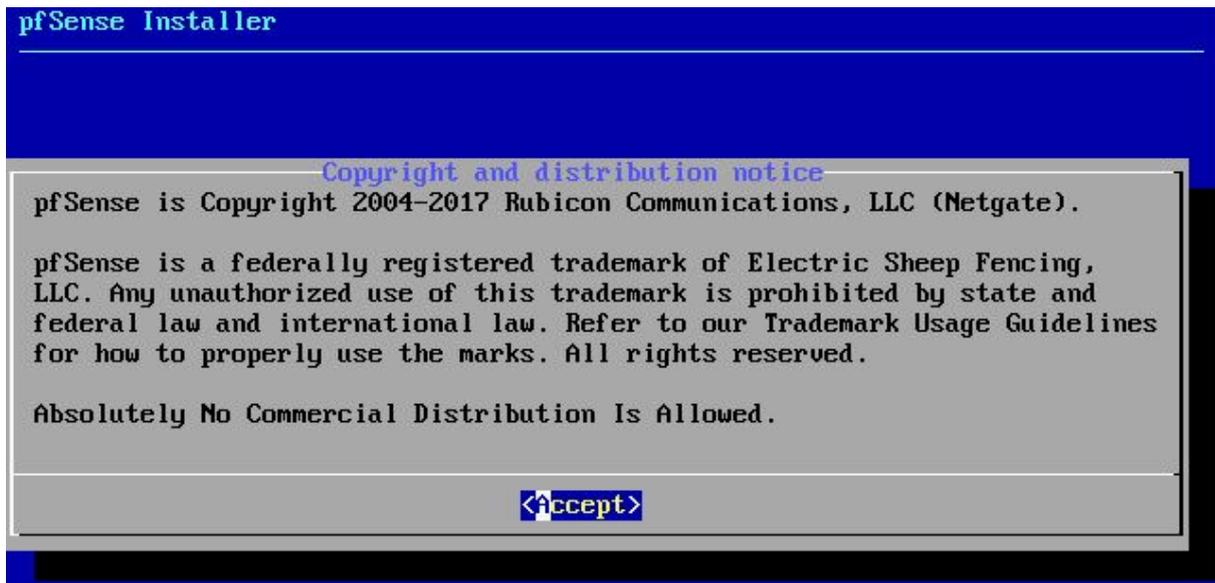
Le trafic est dirigé vers la passerelle souhaitée ou le groupe d'équilibrage local.

6. Relevez les services nécessaires à la navigation internet

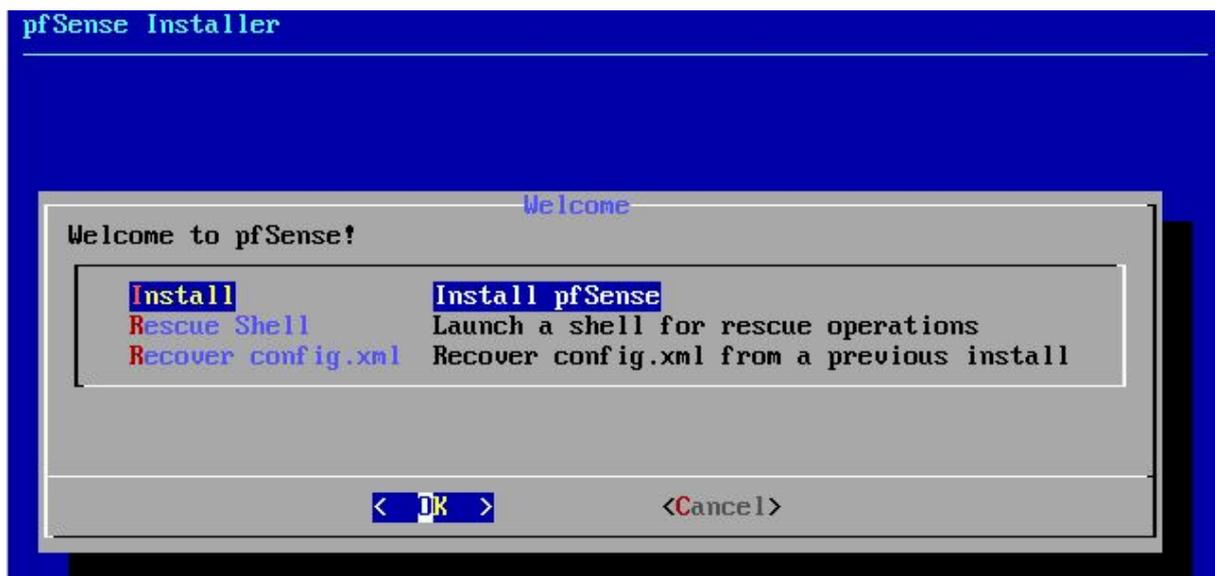
Http/https port 80/443 et DNS

Installation pfSense

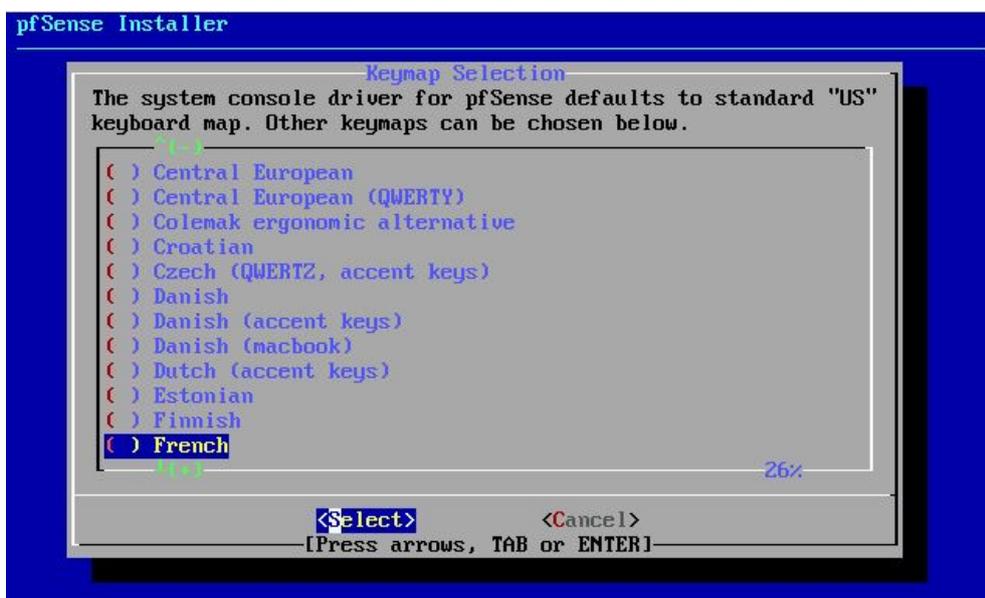
Accepter la licence.



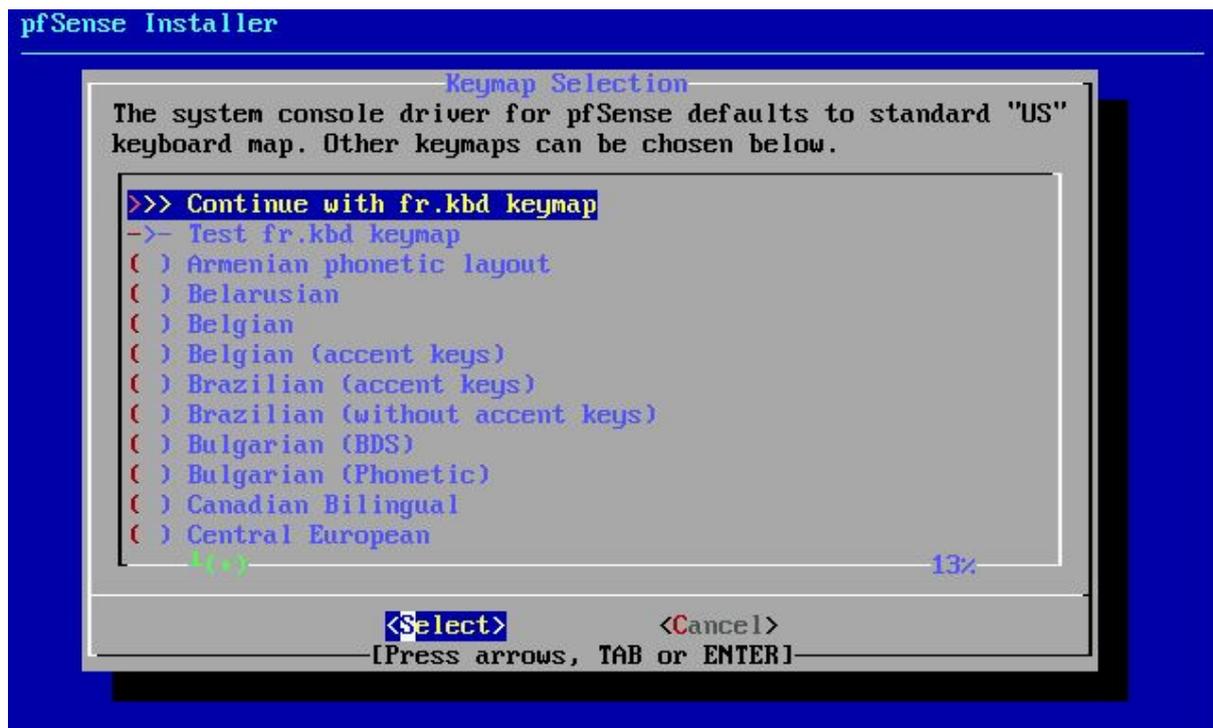
Installez pfSense : OK



Sélectionnez la langue « French »

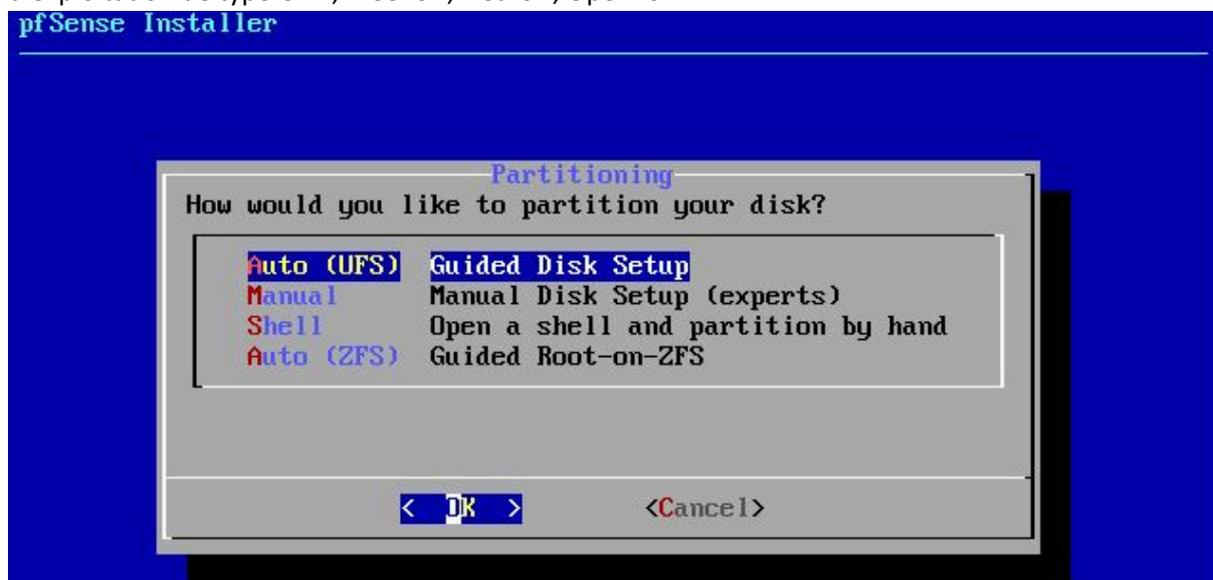


Sélectionnez : Continue With fr.kbd Keymap

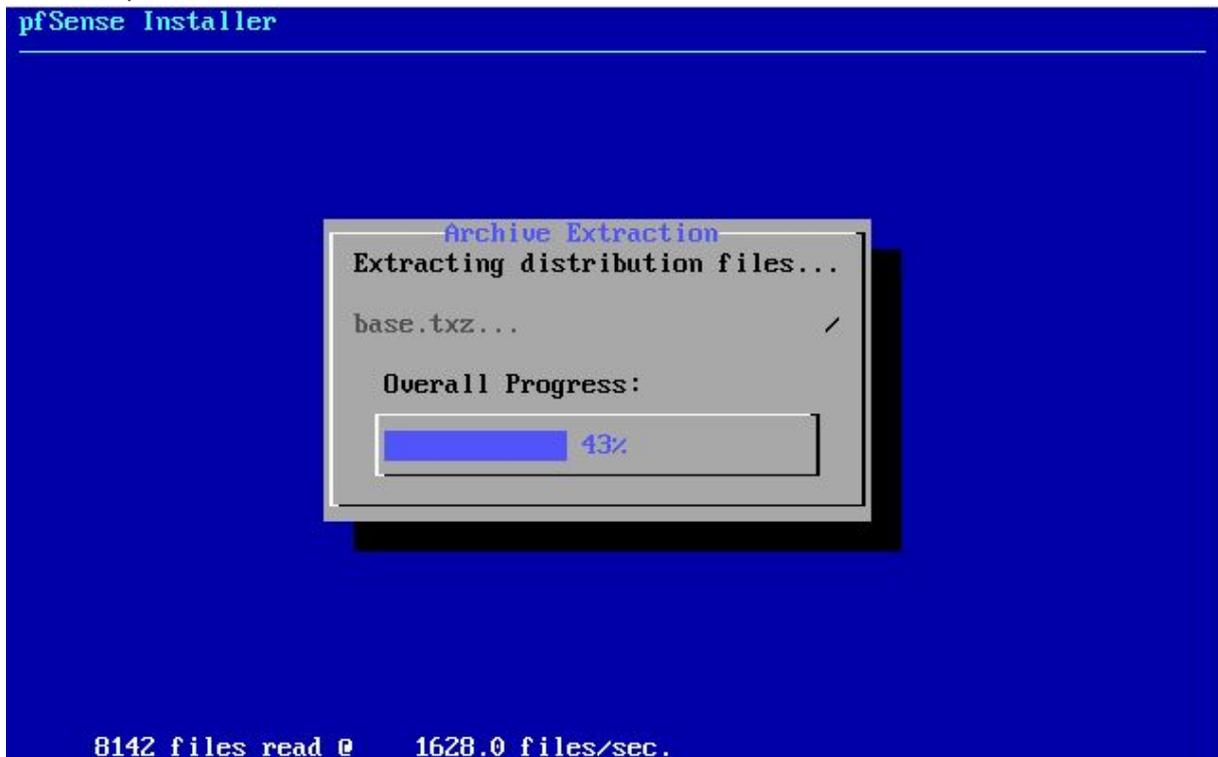


Sélectionnez Auto (UFS) (la configuration de disque guidée) qui veut dire fixer automatiquement les partitions disque et utilise le système de fichiers UFS.

UFS, abréviation de Unix File System, est un système de fichiers utilisé par de nombreux systèmes d'exploitation de type Unix, FreeBSD, NetBSD, OpenBSD.

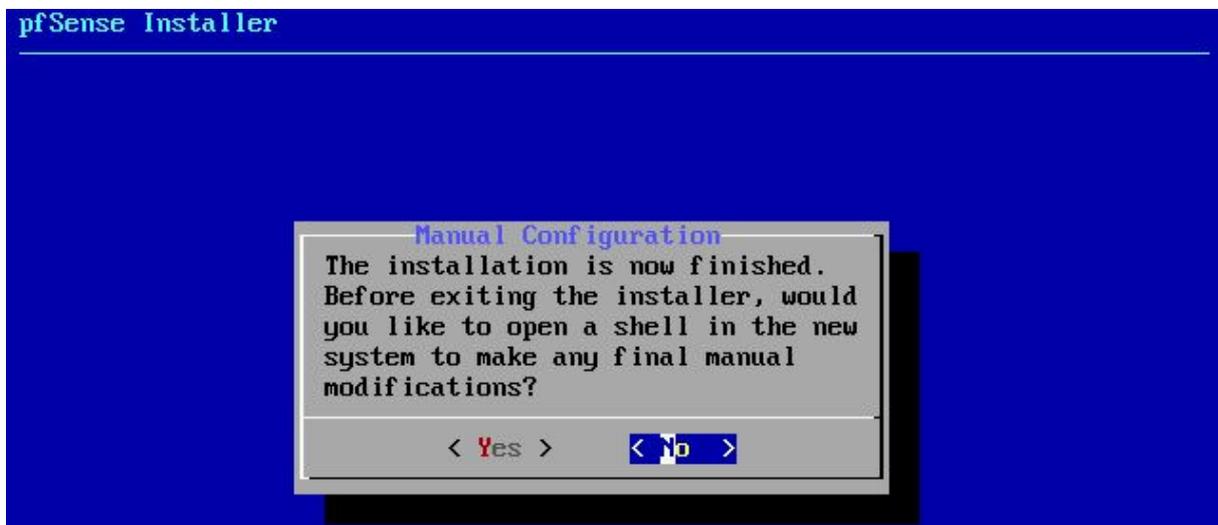


Patientez pendant l'installation.



Avant de quitter le programme d'installation, souhaitez-vous ouvrir un shell dans le nouveau système pour effectuer les dernières modifications manuelles ?

Faites oui ou non. Dans notre cas on fait non.



Sélectionnez Reboot (ne pas oublier d'éjecter le cd si vous ne voulez pas que l'installation se relance)



Saisissez "n" si vous voulez faire des VLAN sinon sélectionner "no".

```
AMD Features2=0x21<LAHF,ABM>
Structured Extended Features=0x2bb9<FSGSBASE,BMI1,HLE,AUX2,SMEP,BMI2,ERMS,RTM,
NFPUSG>
XSAVE Features=0x1<XSAVEOPT>
Hypervisor: Origin = "Microsoft Hv"
Done.
..... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

hn0      00:15:5d:64:04:3f (down) Hyper-V Network Interface
hn1      00:15:5d:64:04:40 (down) Hyper-V Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n
```

Sélectionnez la carte réseau internet Wan hno (sélectionnez votre carte réseau).

```
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

hn0      00:15:5d:64:04:3f (down) Hyper-V Network Interface
hn1      00:15:5d:64:04:40 (down) Hyper-V Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

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

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

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): hn0
```

Sélectionnez la carte réseau local LAN hn1

```
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

hn0      00:15:5d:64:04:3f (down) Hyper-V Network Interface
hn1      00:15:5d:64:04:40 (down) Hyper-V Network Interface

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 [yn]? n

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

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn1 a or nothing if finished): hn1
```

Appliquez les changements : "y" pour "yes".

```
The interfaces will be assigned as follows:
```

```
WAN -> hn0
LAN -> hn1
```

```
Do you want to proceed [yn]? y
```

Et nous voici au Menu.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE amd64 Thu Sep 20 09:03:12 EDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyu0)
Hyper-V Virtual Machine - Netgate Device ID: 391ed73786ee43989c09

*** Welcome to pfSense 2.4.4-RELEASE (amd64) on pfSense ***

WAN (wan)      -> hn0      -> v4/DHCP4: 192.168.100.150/24
LAN (lan)      -> hn1      -> 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: 
```

Configuration de l'adresse IP de la carte réseau local LAN hn1

Sélectionnez : 2 (Set interface IP address)

Sélectionnez la carte réseau local LAN : 2

```
Available interfaces:
1 - WAN (hn0 - dhcp, dhcp6)
2 - LAN (hn1 - static)
Enter the number of the interface you wish to configure: 2
```

Saisissez l'adresse IP souhaitée :

Saisissez le masque sous réseau au format CIDR : 24

Laissez vide pour ne pas définir la passerelle : Tapez ENTREE.

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

Laissez vide pour ne pas définir d'adresse IPV6 : Tapez ENTREE.

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

Activez le Serveur DHCP : "y" pour "yes".

```
Do you want to enable the DHCP server on LAN? (y/n) y
```

Définir la plage d'adressage IP du DHCP (exemple : 192.168.200.10 jusqu'à 192.168.200.30)

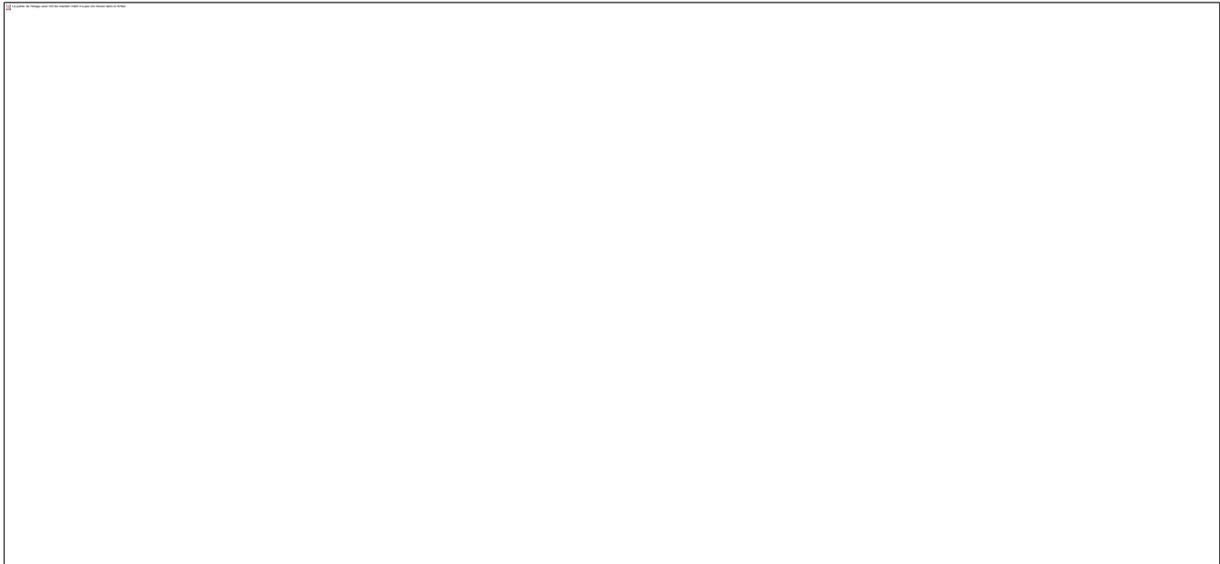
Ne pas activer le retour http car il ne sera pas sécurisé, faites non.

Ce qui nous permet de nous connecter en https.

Configuration terminée.

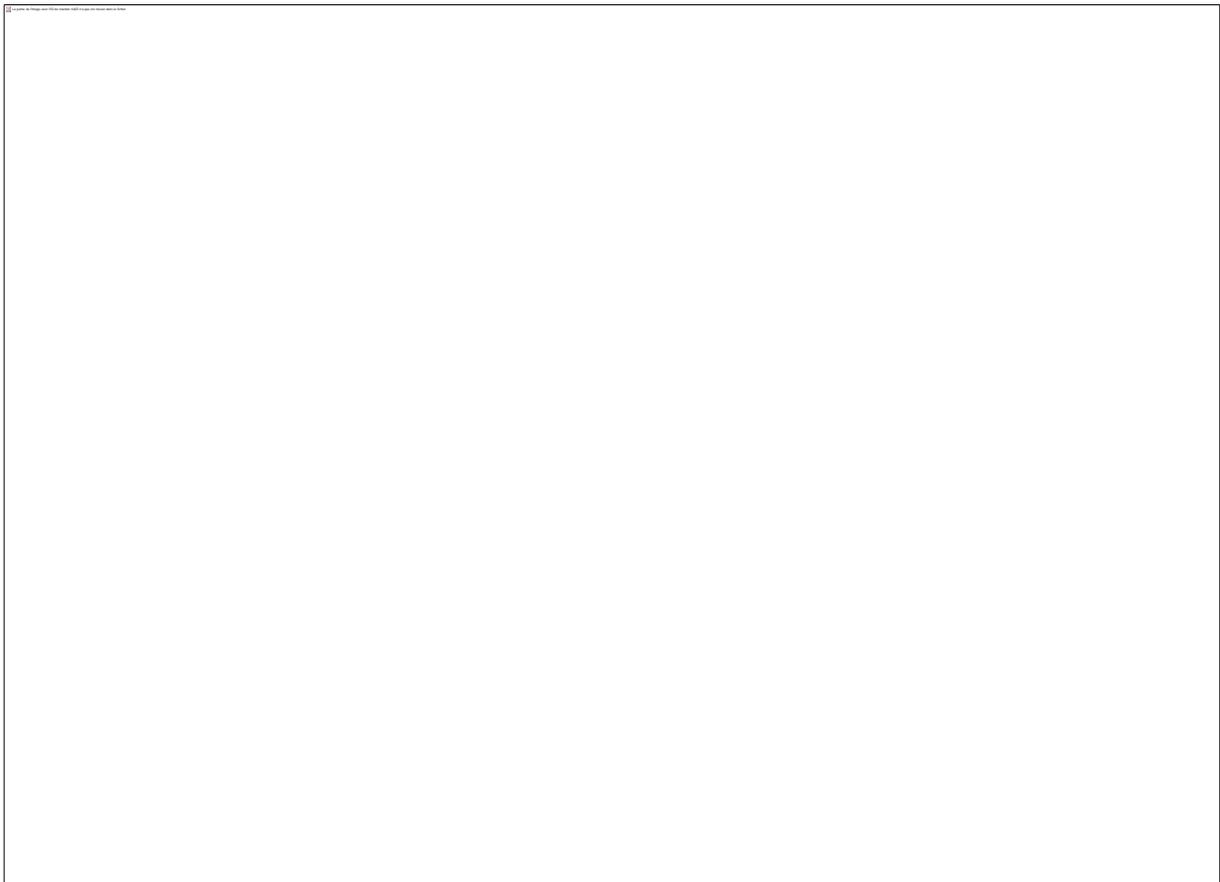
Retour au Menu. L'adresse IP de pfSense est notée dans la partie LAN : 192.168.200.254

On se connecte au portail pfSense avec l'IP du LAN.



Dans system information vous pouvez trouver toutes les informations de votre machine, le CPU, ID de pfSense, BIOS, Version, combien de temps la machine est allumée, la date, les DNS (si vous en avez plusieurs), combien de RAM est utilisé et la quantité de disk utilisé.

Vous pouvez ajouter une représentation graphique du trafic LAN / WAN.

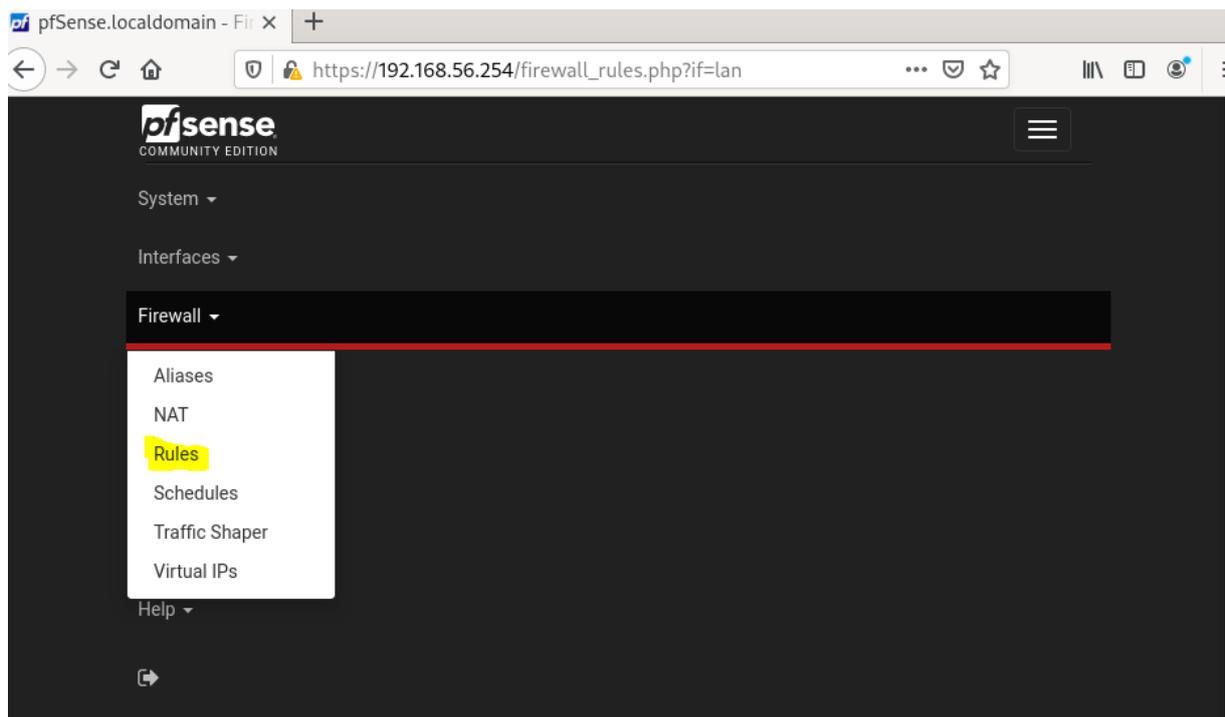


Pour se faire, remontez tout en haut de la page, suivez la ligne Status / Dashboard, au bout de cette ligne vous trouverait un +, cliquez et ajoutez les fonctionnalités qu'il vous convient.



Création de règle de filtrage.

Il faut se rendre dans Firewall, Rules et on choisit l'interface LAN.



Firewall / Rules / WAN

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"/> | 0/0 B | * | Reserved Not assigned by IANA | * | * | * | * | * | | Block bogon networks | |

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.

Add Add Delete Save Separator

Nous voulons restreindre les protocoles réseaux pour effectuer un premier filtrage.

Sur cette image tout est autorisé donc nous allons les désactiver (ne pas supprimer ça pourrait vous servir à des tests si cela ne fonctionne pas). Pour les désactiver cliquer sur l'icône en jaune.

Firewall / Rules / LAN

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

Floating WAN LAN

Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------------------------------|-------------------|----------|------------|------|----------------|-----------|---------|-------|----------|---|---------|
| <input checked="" type="checkbox"/> | 0 /2.64 MiB | * | * | * | LAN Address | 443 80 | * | * | | Anti- Lockout Rule | |
| <input type="checkbox"/> | 0/0 B | 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

Il ne faut pas oublier d'appliquer les changements après chaque modification.

Firewall / Rules / LAN 🔍 📊 📄 ?

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

✔ Apply Changes

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 /2.66 MiB | * | * | * | LAN Address | 443 80 | * | * | | Anti- Lockout Rule | ⚙️ |
| <input type="checkbox"/> | 17 /38 KiB | 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

📘

Mise en place des règles.

Créer un séparateur pour ordonner les règles, nommer le Pass http/https

Firewall / Rules / LAN 🔍 📊 📄 ?

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress. ✕

Floating WAN LAN

Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------------------------------|-------------------|----------|------------|------|----------------|-----------|---------|-------|----------|---|------------------|
| <input checked="" type="checkbox"/> | 1 /2.67 MiB | * | * | * | LAN Address | 443 80 | * | * | | Anti- Lockout Rule | ⚙️ |
| <input type="checkbox"/> | 4 / 40 KiB | 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

Puis cliquez sur Add pour ajouter une règle juste en dessous de votre séparateur.

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

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

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source Invert match LAN net Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Logiquement les champs sont préinscrits :

Action Pass c'est pour autoriser / interdire

L'interface ou les paquets vont passer par rapport à la règle.

Sélectionnez le protocole IP que vous avez en fonction de votre réseau.

Le Protocole = le protocole que vous voulez autoriser.

La Source = la destination. C'est-à-dire d'où vient la requête, c'est le client qui demande s'il peut passer.

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 HTTPS (443) Custom **To** HTTPS (443) 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

La destination c'est d'où va le paquet et sur quelle interface dans mon cas je mets any vers tous les interfaces.

Le port de destination, dont du HTTPS sur le port 443

Une description de la règle.

Ce qui devrait ressembler à ceci :

Floating WAN LAN

Rules (Drag to Change Order)

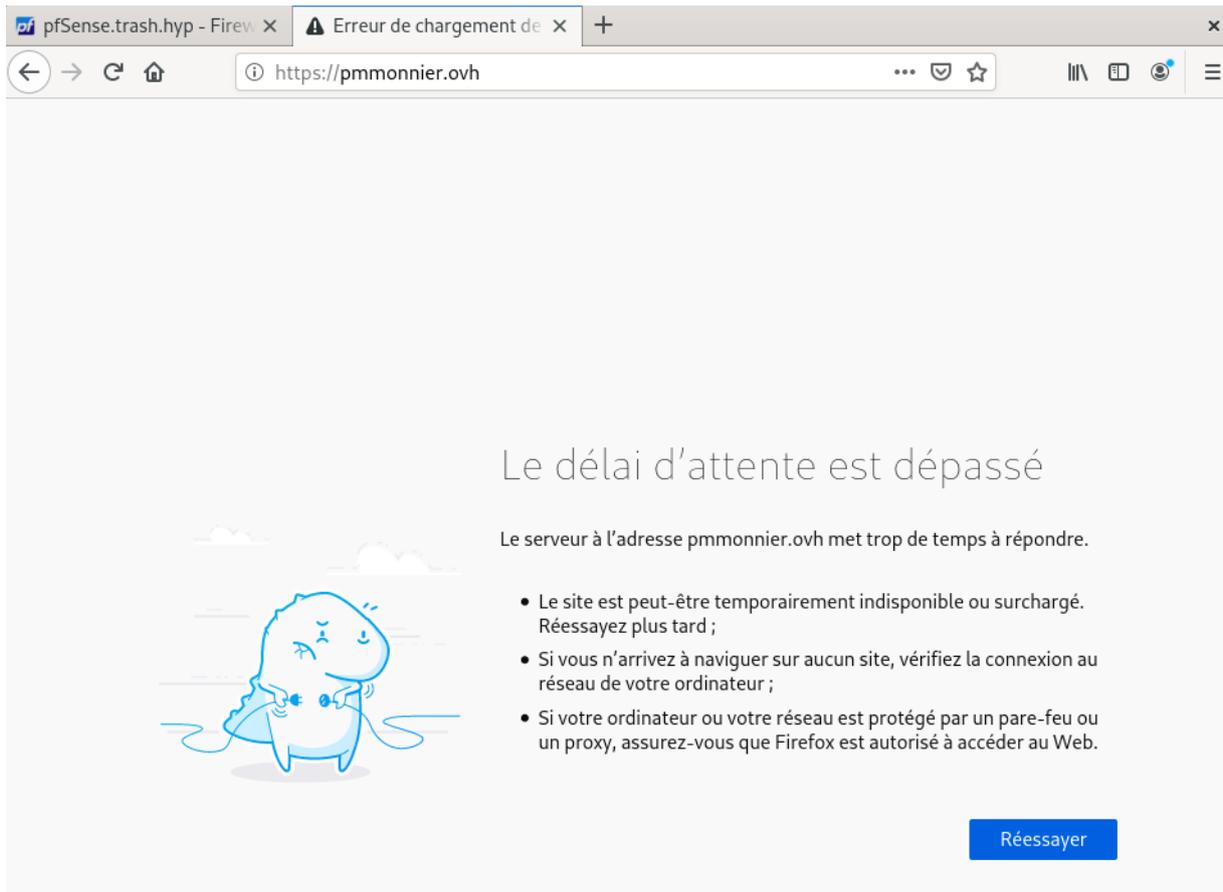
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------------------------------|-------------|--------------|---------|------|-------------|-------------|---------|-------|----------|------------------------------------|--------------|
| <input checked="" type="checkbox"/> | 0 /2.83 MiB | * | * | * | LAN Address | 443 80 | * | * | | Anti-Lockout Rule | |
| <input type="checkbox"/> | 0 /0 B | 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 | |
| Pass http/https | | | | | | | | | | | |
| <input type="checkbox"/> | 0 /0 B | IPv4 TCP | LAN net | * | * | 443 (HTTPS) | * | none | | Pass HTTPS | |
| <input type="checkbox"/> | 0 /0 B | IPv4 TCP | LAN net | * | * | 80 (HTTP) | * | none | | Pass HTTP | |
| <input type="checkbox"/> | 0 /0 B | IPv4 TCP/UDP | LAN net | * | * | 53 (DNS) | * | none | | Pass DNS | |

Si nous désactivons le DNS.

Floating WAN LAN

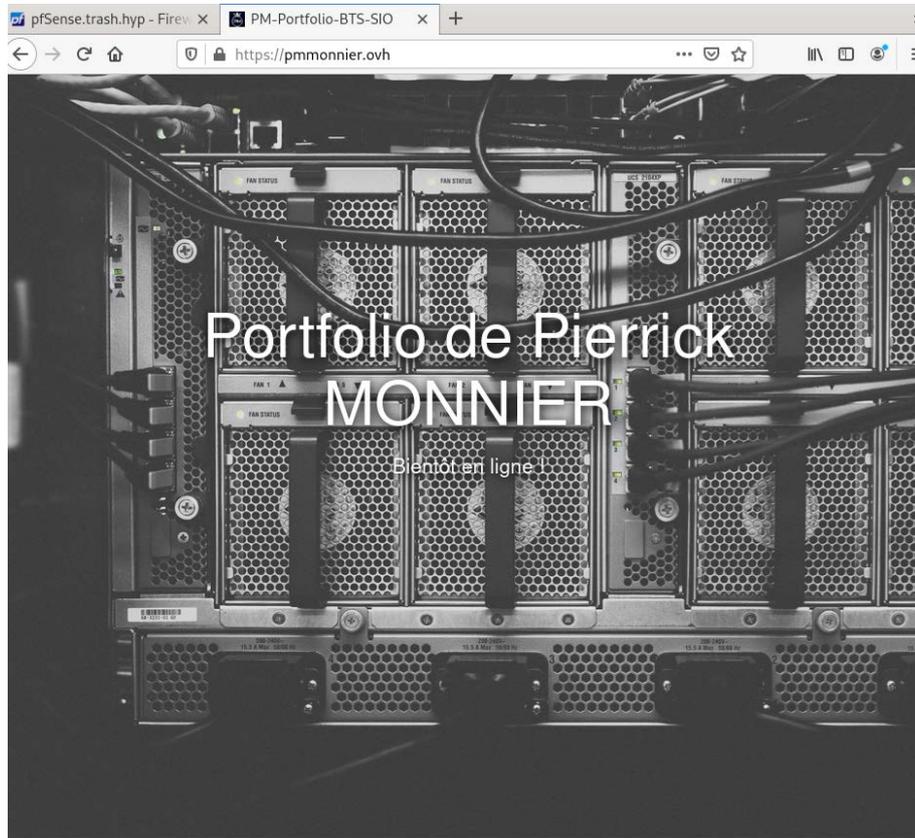
Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------------------------------|-------------|--------------|---------|------|-------------|-------------|---------|-------|----------|------------------------------------|--------------|
| <input checked="" type="checkbox"/> | 0 /1.18 MiB | * | * | * | LAN Address | 443 80 | * | * | | Anti-Lockout Rule | |
| <input type="checkbox"/> | 0 /0 B | 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 | |
| Pass http/https | | | | | | | | | | | |
| <input type="checkbox"/> | 0 /590 KiB | IPv4 TCP | LAN net | * | * | 443 (HTTPS) | * | none | | Pass HTTPS | |
| <input type="checkbox"/> | 0 /0 B | IPv4 TCP | LAN net | * | * | 80 (HTTP) | * | none | | Pass HTTP | |
| <input type="checkbox"/> | 0 /80 KiB | IPv4 TCP/UDP | LAN net | * | * | 53 (DNS) | * | none | | Pass DNS | |



Test de recherche, nous pouvons voir que nous arrivons pas à afficher la page.

Sinon réactivons les règles nous pouvons accéder aux sites internet rechercher.



2 Documentation

1. Qu'est-ce qu'un serveur mandataire ?

Un serveur mandataire il filtre les sites internet que nous consultons, le navigateur envoi une requête pour recevoir la ou les pages à afficher.

2. Explicitez le fonctionnement d'un serveur mandataire. Quelques éléments à considérer :

- Modèle.
- Ports utilisés est le port du protocole utiliser exemple https 443
- Cache est utiliser pour enregistrer les pages web les plus visités, quand un client visite une page assez souvent, elle est enregistrée, elle est plus rapide à recevoir car elle est en cache.
- Filtrage c'est une constitution d'activité les logs qui enregistre toutes les requêtes des utilisateurs lorsqu'il se connecte à internet.
- Sécurité c'est le fiewall qui assure la sécurité.

3. Quelles peuvent être ses fonctions dans un réseau ?

Ses fonctions dans un réseau sont de filtrer les connections, bloquer des sites ou des services.

4. Expliquer les avantages et inconvénients d'un fonctionnement en mode "normal".

Les avantages c'est qu'on peut faire ce qu'on veut, voir n'importe quel site web. Les inconvénients c'est qu'on peut rencontrer des sites web malicieux ou réduire la bande passante.

5. Expliquer les avantages et inconvénients d'un fonctionnement en mode "transparent".

Le mode "transparent" permet de bloquer des sites ou des services. L'utilisateur en revanche ne le voit pas d'où le nom transparent. L'inconvénient c'est que si l'utilisateur veut visiter un site web bloqué il sera averti qu'il n'a pas le droit de voir cette page web.

Installation du proxy :

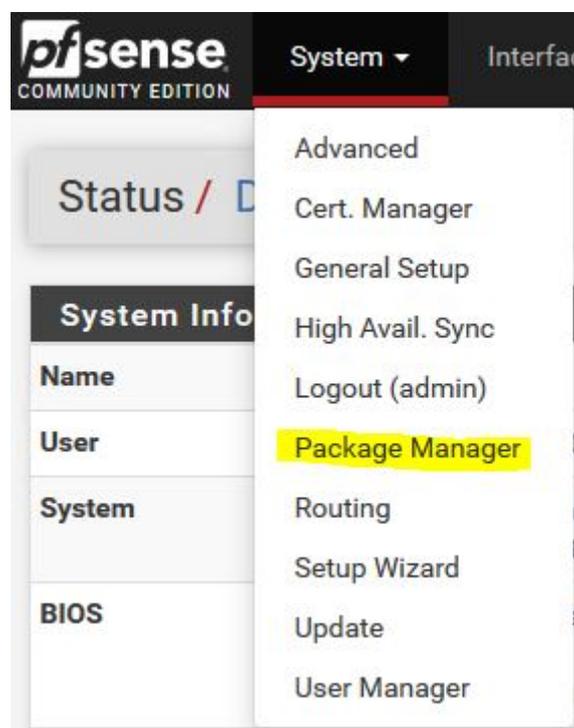
Proxy Transparent Filtrage Web URL Squid SquidGuard

Mise en place d'un proxy transparent Squid avec filtrage d'URL SquidGuard permettant de filtrer les accès à Internet de l'ensemble des utilisateurs connectés au réseau interne, de bloquer l'accès aux sites à caractères indésirables ou offensant.

Rapport de connexion LightSquid. Il s'agit d'un analyseur de logs qui affiche sous forme de pages Web, l'utilisation du Proxy.

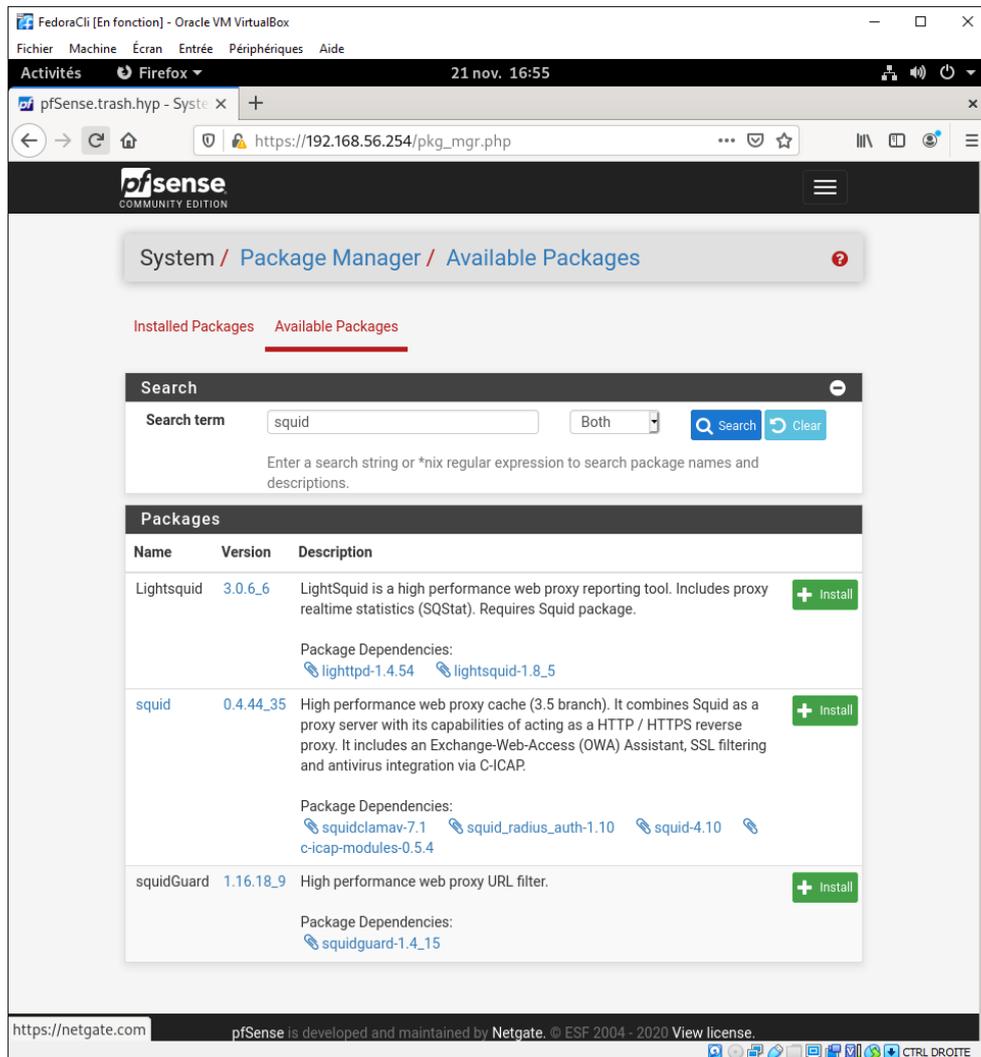
Installation des packages Squid SquidGuard et LightSquid

System, Package Manager



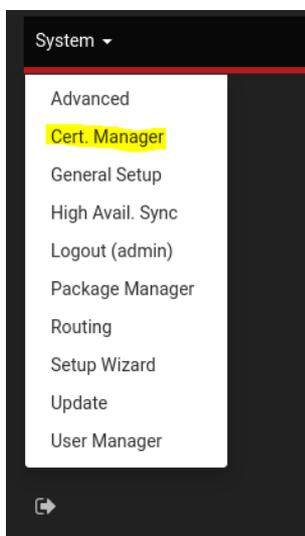
Allez dans “Available Packages”, dans la recherche taper “squid” puis cliquez sur “Search”.

Installez les 3 packages un par un : Squid, SquidGuard, LightSquid.



Création du Certificat pour le filtrage en HTTPS :

Sélectionnez : System, Cert. Manager



Cliquez sur Add :

Donnez un "Nom", sans espace. Exemple : "CertHTTPS", remplissez les informations du certificat et cliquez sur "Save".

CA's Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

| Name | Internal | Issuer | Certificates | Distinguished Name | In Use | Actions |
|-----------|-------------------------------------|-------------|--------------|--|--------|---------|
| CertHTTPS | <input checked="" type="checkbox"/> | self-signed | 0 | ST=France, OU=Informatique, O=BTS, L=Desertines, CN=internal-ca Valid From: Sat, 21 Nov 2020 17:02:44 +0100 Valid Until: Tue, 19 Nov 2030 17:02:44 +0100 | | |

Configuration de Squid :

Sélectionnez "Services" et "Squid Proxy Server"

Services ▾

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server & RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- Load Balancer
- NTP
- PPPoE Server
- SNMP
- Squid Proxy Server
- Squid Reverse Proxy**
- SquidGuard Proxy Filter
- UPnP & NAT-PMP
- Wake-on-LAN

board

pfSense.trash.hyp

admin@192.168.56.16 (Local Database)

VirtualBox Virtual Machine
Netgate Device ID: 8f8807db4af0464b44c8

Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006

2.4.5-RELEASE-p1 (amd64)
built on Tue Jun 02 17:51:17 EDT 2020
FreeBSD 11.3-STABLE

The system is on the latest version.

Sélectionnez : "Local Cache" et paramétrez le "Hard Disk Cache Size" à 500 Mo puis cliquer sur "Save"

Pour avoir plus d'objets (les pages web qui sont souvent rechercher par l'utilisateur) mis en cache.

Package / Proxy Server: Cache Management / Local Cache ?

General Remote Cache **Local Cache** Antivirus ACLs Traffic Mgmt Authentication Users

Real Time Status Sync

Squid Cache General Settings

| | |
|---------------------------------|---|
| Disable Caching | <input type="checkbox"/> Disable caching completely. This may be required if Squid is only used as a proxy to audit website access. |
| Cache Replacement Policy | Heap LFUDA The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default: heap LFUDA i |
| Low-Water Mark in % | 90 The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm. i |
| High-Water Mark in % | 95 The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm. i |
| Do Not Cache | <div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div> <p>Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.</p> |
| Enable Offline | <input type="checkbox"/> Enable this option and the proxy server will never try to validate cached objects. |

Squid Hard Disk Cache Settings

Hard Disk Cache Size
Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System
This specifies the kind of storage system to use. [i](#)

Clear Disk Cache NOW Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. [i](#)
If you wish to clear cache **immediately**, click this button **once**:

Level 1 Directories
Specifies the number of Level 1 directories for the hard disk cache. [i](#)

Hard Disk Cache Location
This is the directory where the cache will be stored. Default: /var/squid/cache [i](#)

Minimum Object Size
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

Maximum Object Size
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) [i](#)

Squid Memory Cache Settings

Memory Cache Size
Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-Cached objects.
Minimum value: 1 (MB). Default: 64 (MB) [i](#)

Onglet "General" : Activez "Enable Squid Proxy", sélectionnez l'interface réseau "LAN" et "Resolve DNS IPv4 First"

Squid General Settings

Enable Squid Proxy Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall /upgrade.

Listen IP Version
Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen

| | |
|---|--|
| Allow Users on Interface | <input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets. |
| Patch Captive Portal | This feature was removed - see Bug #5594 for details! |
| Resolve DNS IPv4 First | <input checked="" type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites. |
| Disable ICMP | <input type="checkbox"/> Check this to disable Squid ICMP pinger helper. |
| Use Alternate DNS Servers for the Proxy Server | <input type="text"/> To use DNS servers other than those configured in System > General Setup , enter the IP(s) here. Separate entries by semi-colons (;) |
| Transparent Proxy Settings | |
| Transparent HTTP Proxy | <input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server.  Transparent proxy mode works without any additional configuration being necessary on clients. Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below. Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections , configure WPAD/PAC options on your DNS/DHCP servers. |
| Transparent Proxy Interface(s) | <input type="text" value="WAN"/> <input checked="" type="text" value="LAN"/> The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces . |

Activez "Transparent HTTP Proxy" et sélectionnez l'interface réseau "LAN".

| | |
|--|--|
| HTTPS/SSL Interception | <input checked="" type="checkbox"/> Enable SSL filtering. |
| SSL/MITM Mode | <input type="text" value="Splice All"/> <p>The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. Click Info for details. i</p> |
| SSL Intercept Interface(s) | <input type="text" value="WAN"/> <input checked="" type="text" value="LAN"/> <p>The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.</p> |
| SSL Proxy Port | <input type="text" value="3129"/> <p>This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129</p> |
| SSL Proxy Compatibility Mode | <input type="text" value="Modern"/> <p>The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details. i</p> |
| DHParams Key Size | <input type="text" value="2048 (default)"/> <p>DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.</p> |
| CA | <input type="text" value="CertHTTPS"/> <p>Select Certificate Authority to use when SSL interception is enabled. i</p> |
| SSL Certificate Daemon Children | <input type="text" value="5"/> <p>This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5</p> |
| Remote Cert Checks | <input type="text" value="Accept remote server certificate with errors"/> <input type="text" value="Do not verify remote certificate"/> <p>Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.</p> |

Activez "HTTPS/SSL Interception SSL filtering", sélectionner "Splice All", l'interface "LAN" et le Certificat précédemment créé "CertHTTPS"

Le mode « Splice ALL » permet à pfSense de capturer à la volée et d'effectuer le contrôle sur le flux sans devoir faire une quelconque manipulation sur les machines clientes ; De plus, il permet de bloquer les sites web interdits via la rubrique « ACL » de Squid.

Activez "Enable Access Logging" et définir combien de jours les logs seront conservés : 365 (un an)

Logging Settings

Enable Access Logging This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory
The directory where the logs will be stored; also used for logs other than the Access Log above. **Default:** /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard Makes it possible for SquidGuard denied log to be included on Squid logs.
[Click Info for detailed instructions.](#) 

Headers Handling, Language and Other Customizations

Visible Hostname
This is the hostname to be displayed in proxy server error messages.

Administrator's Email
This is the email address displayed in error messages to the users.

Error Language
Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode
Choose how to handle X-Forwarded-For headers. **Default:** on 

Disable VIA Header If not set, Squid will include a Via header in requests and replies as required by RFC2616.

URI Whitespace Characters Handling
Choose how to handle whitespace characters in URL. **Default:** strip 

Suppress Squid Version Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Sélectionnez "fr" pour "Error language" et Activez "Suppress Squid Version"

Puis Cliquez sur "Save" pour enregistrer toutes les modifications effectuées dans Squid.

Configuration de SquidGuard :

Sélectionnez “Services” et “SquidGuard Proxy Filter”.

Activez SquidGuard “Enable”.

General Options

Enable Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked.**

Apply

SquidGuard service state: **STOPPED**

Activez “Enable Log” et “Enable log rotation”.

Logging options

Enable GUI log Check this option to log the access to the Proxy Filter GUI.

Enable log Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

Enable log rotation Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Blacklist options

Blacklist Check this option to enable blacklist
Do NOT enable this on NanoBSD installs!

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Activez “Enable Blacklist” et insérez dans Blacklist URL :

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Puis cliquez sur “Save”.

Onglet "Blacklist" : Cliquer sur "Download" pour télécharger les listes de filtrages.

General settings Common ACL Groups ACL Target categories Times Rewrites **Blacklist** Log

XMLRPC Sync

Blacklist Update

Blacklist download progress

100 %

 Download  Cancel  Restore Default

Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

```
Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download
/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 62 items.
Start rebuild DB.
Copy DB to workdir.
```

Onglet "Common ACL", Cliquez, dans "Target Rules List" sur le "+".

Target Rules List + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

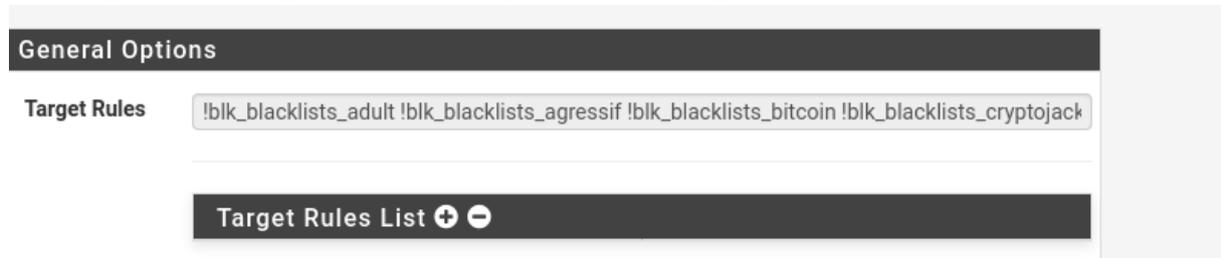
| Target Categories | | |
|---|--------|---------------------|
| [blk_blacklists_adult] | access | deny ▼ |
| [blk_blacklists_agressif] | access | deny ▼ |
| [blk_blacklists_arjel] | access | ---- ▼ |
| [blk_blacklists_associations_religieuses] | access | ---- ▼ |
| [blk_blacklists_astrology] | access | ---- ▼ |
| [blk_blacklists_audio-video] | access | ---- ▼ |
| [blk_blacklists_bank] | access | ---- ▼ |
| [blk_blacklists_bitcoin] | access | deny ▼ |
| [blk_blacklists_blog] | access | ---- ▼ |
| [blk_blacklists_celebrity] | access | ---- ▼ |
| [blk_blacklists_chat] | access | ---- ▼ |
| [blk_blacklists_child] | access | ---- ▼ |
| [blk_blacklists_cleaning] | access | ---- ▼ |
| [blk_blacklists_cooking] | access | ---- ▼ |
| [blk_blacklists_cryptojacking] | access | deny ▼ |
| [blk_blacklists_dangerous_material] | access | deny ▼ |
| [blk_blacklists_dating] | access | ---- ▼ |
| [blk_blacklists_ddos] | access | ---- ▼ |
| [blk_blacklists_dialer] | access | ---- ▼ |
| [blk_blacklists_doh] | access | ---- ▼ |
| [blk_blacklists_download] | access | ---- ▼ |
| [blk_blacklists_droque] | access | deny ▼ |

Default access [all] access allow ▼

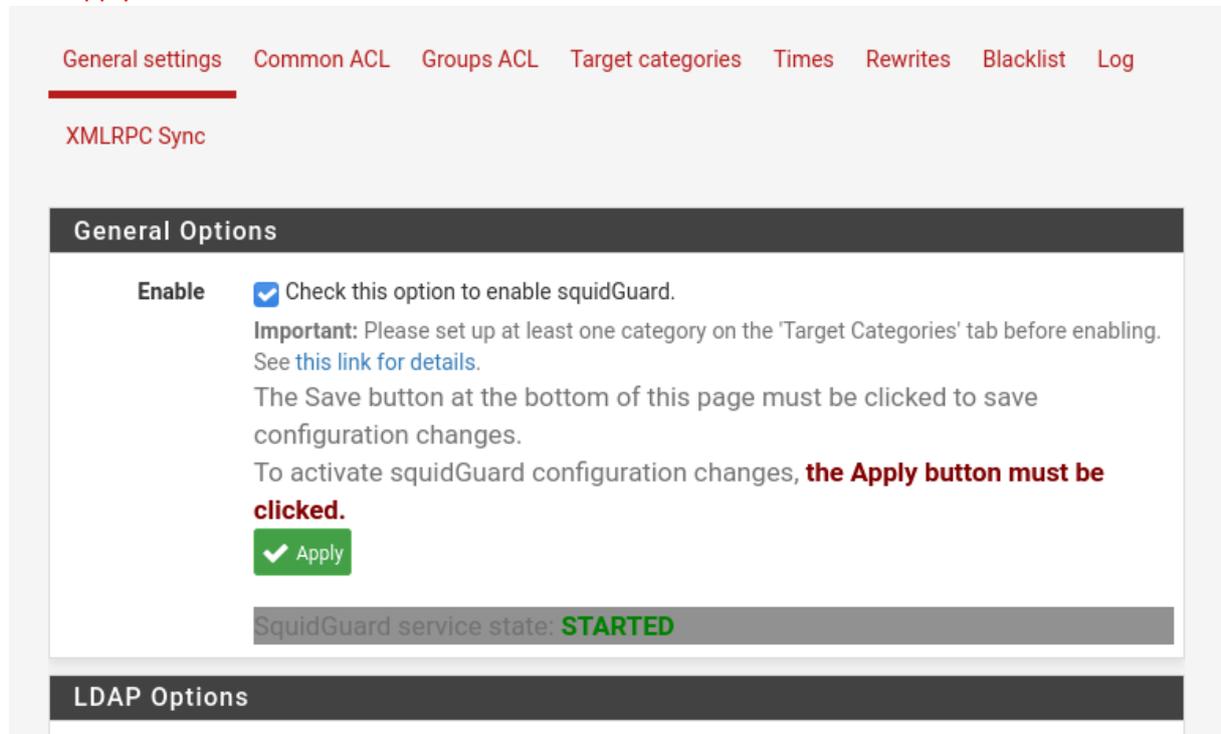
Cochez “Do not allow IP addresses in URL” et “Use SafeSearch engine”

Ceci est pour éviter le contournement d’URL en utilisant simplement les adresses IP au lieu du FQND. Activez le mode protégé des moteurs de recherche pour limiter l'accès au contenu mature. Pour le moment, il est pris en charge par Google, Yandex, Yahoo, MSN, Live Search et Bing. Assurez-vous que les moteurs de recherche sont accessibles. Il est recommandé d'interdire l'accès à d'autres.

Les catégories de filtrages sont bien enregistrées dans “Target Rules” .



TRES IMPORTANT : Pour valider les paramètres, retournez sur l’onglet “General settings” et cliquez sur “Apply”



Il est indispensable de cliquer sur “Apply” après chaque modification de la configuration sinon les paramètres ne seront pas pris en compte (et vous chercherez longtemps pour trouver d’où vient le problème.)

Test de connection sur un site :

Nous pouvons remarquer que le site est bien bloqué.



Documentation

1. Quelle est la fonction d'un portail captif dans un réseau ?

Le portail captif est de forcer l'utilisateur à se connecter au réseau.

2. Comment fonctionne le portail captif ?

Le fonctionnement du portail captif est simple, l'utilisateur voudra se connecter au réseau, une page web lui envoie un formulaire de connections avec identifiant et mot de passe. Si ce dernier n'est pas renseigné alors il ne pourra pas s'authentifier pour accéder a du contenu WEB et réseau.

pfSense : Portail Captif avec Authentification Utilisateur

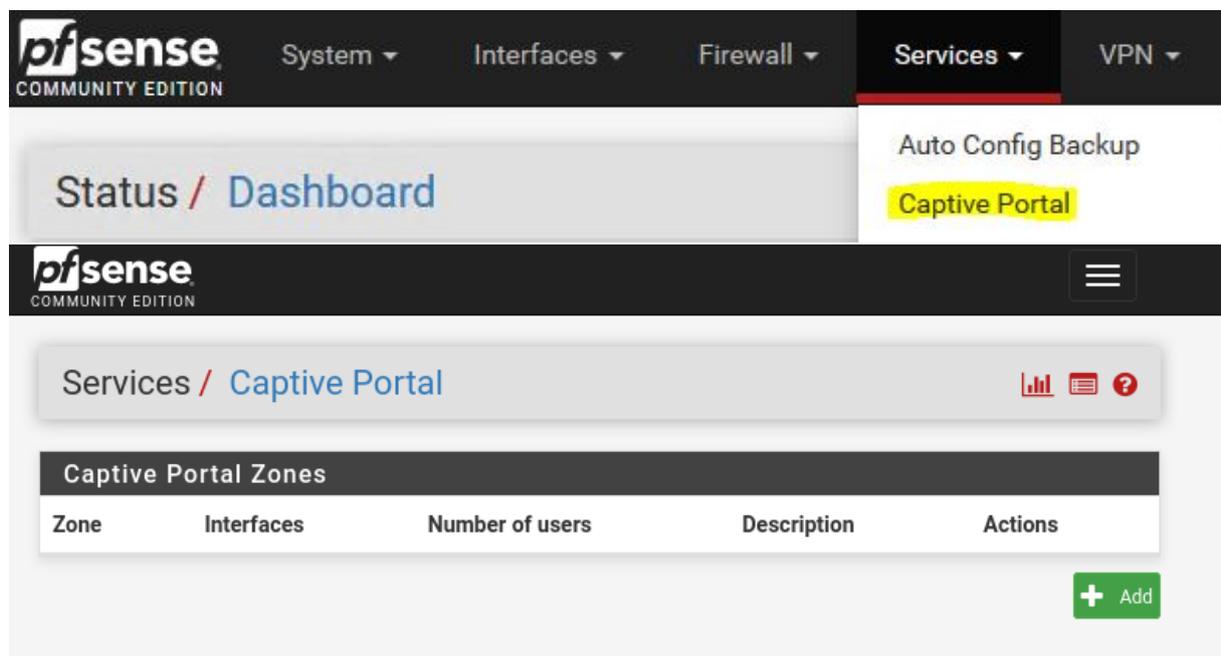
pfSense dispose d'un portail captif. Le portail captif force les clients d'un réseau à afficher une page Web d'authentification avant de pouvoir se connecter à Internet.

Dans notre contexte nous avons un Serveur de DNS sur Debian en utilisant Bind9 en Interne, ce qui veut dire qu'il faut le configurer avec l'IP passerelle dans son fichier de Forwarder et dans le named.conf. Si nous ne faisons pas cette manipulation la page du portail captif ne s'affichera pas.

Ajoutez dans le DNS le nom de votre pfSense, dans mon cas ça sera pfSense.trash.hyp

Configuration du Portail Captif

Sélectionnez : Services – Captive Portal



The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services (highlighted), and VPN. Below the navigation bar, there is a breadcrumb trail: Status / Dashboard. The main content area shows the Services / Captive Portal configuration page. It features a table titled "Captive Portal Zones" with columns: Zone, Interfaces, Number of users, Description, and Actions. There is a green "+ Add" button at the bottom right of the table.

Renseignez le Nom du Portail Captif et sa description. Pour l'exemple : "PortailCaptife "

Activez "Enable Captive Portal" et sélectionnez l'interface "LAN"

Maximum concurrent connections : 1 (Limite le nombre de connexions simultanées d'un même utilisateur).

Idle timeout (Minutes) : Choisir entre 1 à 5 (Les clients seront déconnectés après cette période d'inactivité).

Activez "Enable logout popup window" (une fenêtre popup permet aux clients de se déconnecter).

Définir "Pre-authentication Redirect URL" (URL de redirection par défaut. Les visiteurs ne seront redirigés vers cette URL après authentification que si le portail captif ne sait pas où les rediriger).

Note : Avec "http://....." devant le domaine : Exemple : http://www.google.fr

Définir "After authentication Redirection URL" (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).

Note : Avec "http://....." devant le domaine : Exemple : http://www.google.fr

Activez "Disable Concurrent user logins" (seule la connexion la plus récente par nom d'utilisateur sera active)

Activez "Disable MAC filtering" (nécessaire lorsque l'adresse MAC du client ne peut pas être déterminée)

The screenshot shows the 'Authentication' configuration page. It is divided into several sections:

- Authentication Method:** A dropdown menu is set to 'Use an Authentication backend'. Below it, instructions state: 'Select an Authentication Method to use for this zone. One method must be selected.' and list three options: 'Authentication backend', 'None', and 'RADIUS MAC Authentication'.
- Authentication Server:** A dropdown menu is set to 'Local Database'. Below it, instructions state: '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:** A dropdown menu is set to 'Local Database'. Below it, instructions state: 'You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.'
- Reauthenticate Users:** A checkbox labeled 'Reauthenticate connected users every minute' is unchecked. Below it, instructions state: '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:** A checkbox labeled 'Allow only users/groups with "Captive portal login" privilege set' is checked.

Sélectionnez "Use an Authentication backend".

Sélectionnez "Local Database" pour "Authentication Server" **vérifier qu'il soit bien sélectionné.**

Attention : Ne pas sélectionner "Local Database" pour "Secondary Authentication Server".

Activez "Local Authentication Privileges" (Autoriser uniquement les utilisateurs avec les droits de "Connexion au portail captif").

Puis cliquez "Save".

Authentication

Authentication Method Use an Authentication backend

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

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

Authentication Server Local Database

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

Secondary authentication Server Local Database

You can optionally select a second set of servers to 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

Services / **Captive Portal** 📊 📄 ?

Captive Portal Zones

| Zone | Interfaces | Number of users | Description | Actions |
|---------------|------------|-----------------|---------------|---|
| PortailCaptif | LAN | 0 | PortailCaptif |   |

+ Add

Configuration du Groupe et Utilisateur pour délégation du Portail Captif.

Création d'un groupe et d'un utilisateur qui aura pour fonction de créer des Utilisateurs autorisés à se connecter au Portail Captif. Ce groupe d'utilisateurs associés auront seulement le droit de créer des Utilisateurs du Portail Captif.

Sélectionnez : System – User Manager

Onglet "Groups", cliquez sur "+ Add".

System / User Manager / Groups ?

Users Groups Settings Authentication Servers

| Groups | | | |
|------------|-----------------------|--------------|---------|
| Group name | Description | Member Count | Actions |
| all | All Users | 1 | |
| admins | System Administrators | 1 | |

Add

Cliquez sur Add, Renseigner le Nom du Groupe "Agent" et sa description "Delegation Creation Utilisateurs Portail". Cliquez "Save".

Users Groups Settings Authentication Servers

Group Properties

Group name

Scope

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

Group description, for administrative information only

Group membership

admin

Not members

Members

>> Move to "Members"
<< Move to "Not members"

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

Save

Dans le menu “Actions”, modifiez le groupe créé en cliquant sur le stylo.

| Groups | | | |
|------------|---|--------------|---|
| Group name | Description | Member Count | Actions |
| Agent | Délégation Creation Utilisateur Portail | 0 |   |
| admins | System Administrators | 1 |  |
| all | All Users | 1 |  |



Cliquez sur “+ Add” rubrique “Assigned Privileges”.

Sélectionnez dans la liste “WebCfg – System : User Manager” (Accès à la page de gestion des utilisateurs “User Manager”).

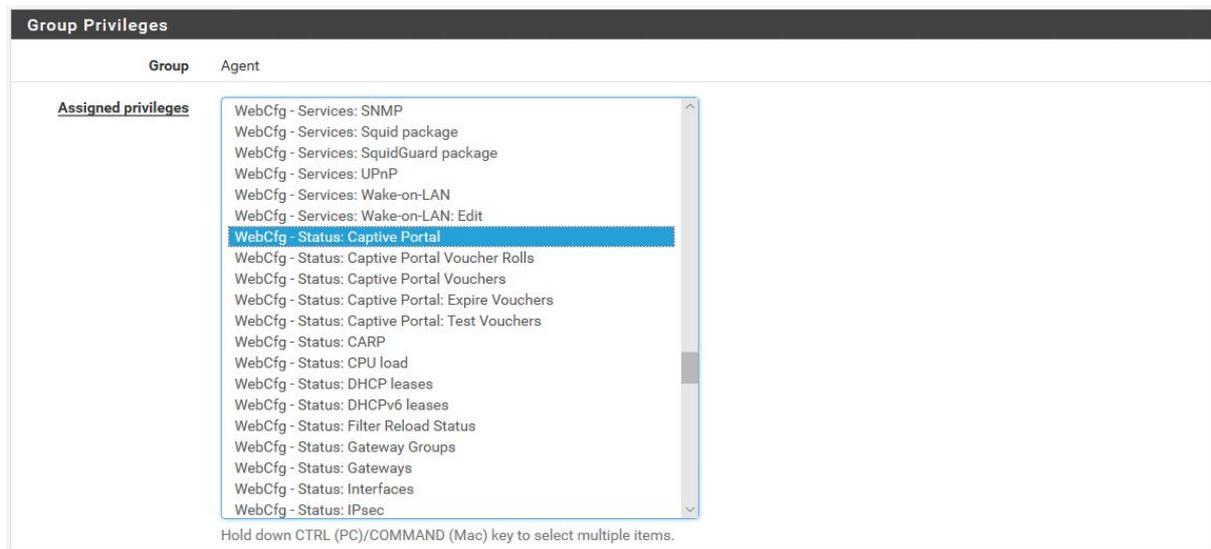
| Group Privileges | |
|----------------------------|---|
| Group | Agent |
| <u>Assigned privileges</u> | <ul style="list-style-type: none">WebCfg - System: Group ManagerWebCfg - System: Group Manager: Add PrivilegesWebCfg - System: High Availability SyncWebCfg - System: Login / Logout / DashboardWebCfg - System: Package ManagerWebCfg - System: Package Manager: Install PackageWebCfg - System: Package Manager: InstalledWebCfg - System: Static RoutesWebCfg - System: Static Routes: Edit routeWebCfg - System: Update: SettingsWebCfg - System: User ManagerWebCfg - System: User Manager: Add PrivilegesWebCfg - System: User Manager: SettingsWebCfg - System: User Password ManagerWebCfg - System: User SettingsWebCfg - VPN: IPsecWebCfg - VPN: IPsec: Edit Phase 1WebCfg - VPN: IPsec: Edit Phase 2WebCfg - VPN: IPsec: Edit Pre-Shared KeysWebCfg - VPN: IPsec: Mobile |

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

Puis cliquez sur “Save”.

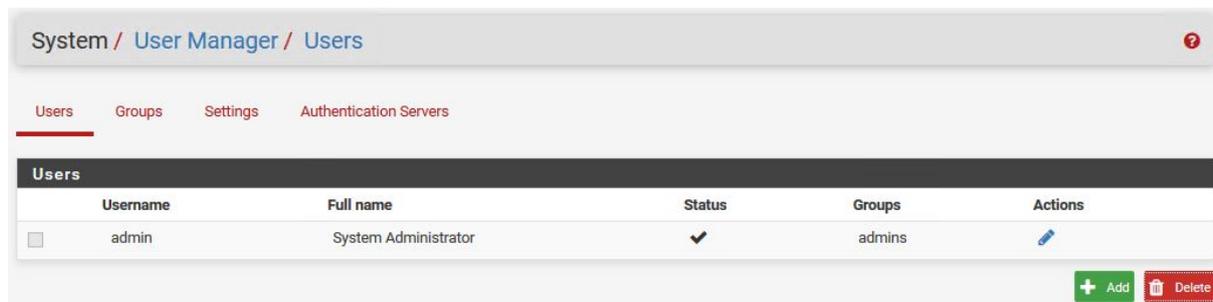
Revenir à la rubrique “Assigned Privileges” en cliquant sur “+ Add”.

Sélectionnez dans la liste “WebCfg – Status: Captive Portal” (Voir le Statut des utilisateurs connectés”).



Vérifiez les droits, puis cliquez sur “Save”.

Onglet “Users”, cliquez sur “+ Add”.



Entrez un Nom d’Utilisateur “agent”, son mot de passe et sa description (Agent autorisé à créer des utilisateurs du Portail Captif).

Sélectionnez dans “Group membership” le groupe “Agent” précédemment créé. Cliquez sur “Move to Member of list” puis “Save”.

User Properties

Defined by USER

Disabled This user cannot login

Username

Password

Full name
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

Not member of

[» Move to "Member of" list](#)

Member of

[« Move to "Not member of" list](#)

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

Certificate Click to create a user certificate

La délégation pour l'utilisateur "Agent" est autorisé à créer des utilisateurs pour connexion au Portail Captif.

Users Groups Settings Authentication Servers

Users

| | Username | Full name | Status | Groups | Actions |
|--------------------------|----------|---|--------|--------|---------|
| <input type="checkbox"/> | admin | System Administrator | ✓ | admins | |
| <input type="checkbox"/> | agent | Agent autorisé a créer des utilisateurs du Portail Captif | ✓ | Agent | |

+ Add
 - Delete

Configuration du Groupe et Utilisateurs autorisés à se connecter au Portail Captif.

Ce groupe est utilisateurs associés auront seulement le droit d'utiliser le Portail Captif.

Onglet "Groups", cliquez sur "+ Add"

The screenshot shows the 'System / User Manager / Groups' page. At the top, there are navigation tabs: 'Users', 'Groups' (which is selected and underlined), 'Settings', and 'Authentication Servers'. Below the tabs is a table titled 'Groups' with the following data:

| Group name | Description | Member Count | Actions |
|------------|---|--------------|---|
| Agent | Délégation Creation Utilisateur Portail | 1 |   |
| admins | System Administrators | 1 |  |
| all | All Users | 2 |  |

At the bottom right of the table area, there is a green '+ Add' button.

Renseignez le Nom du Groupe "Portail" et sa description "Utilisateurs du Portail". Cliquez "Save"

Dans le menu "Actions", modifier le groupe créé en cliquant sur le stylo.

The screenshot shows the 'Group Properties' configuration page. At the top, there are navigation tabs: 'Users', 'Groups' (selected), 'Settings', and 'Authentication Servers'. The page is divided into two main sections: 'Group Properties' and 'Assigned Privileges'.

Group Properties:

- Group name:** Portail
- Scope:** Local (dropdown menu)
- Warning:** Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.
- Description:** Utilisateur du Portail
- Group description:** Group description, for administrative information only
- Group membership:** Two lists are shown: 'Not members' (containing 'admin', 'agent') and 'Members' (empty).
- Buttons:** 'Move to "Members"' and 'Move to "Not members"'. A note below says: 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.'

Assigned Privileges:

| Name | Description | Action |
|------|-------------|--------|
|------|-------------|--------|

At the bottom right of the 'Assigned Privileges' section, there is a green '+ Add' button. At the bottom center of the page, there is a blue 'Save' button.

Sélectionnez dans la liste “User – Services : Captive Portal login” (Autorisé seulement à se connecter au Portail Captif).

Users **Groups** Settings Authentication Servers

Group Properties

Group name Portail

Scope Local
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description Utilisateur du Portail
Group description, for administrative information only

Group membership

admin
agent

Not members

Members

» Move to "Members" « Move to "Not members"

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

Assigned Privileges

| Name | Description | Action |
|---------------------------------------|--|--------|
| User - Services: Captive Portal login | Indicates whether the user is able to login on the captive portal. | |

+ Add

Save

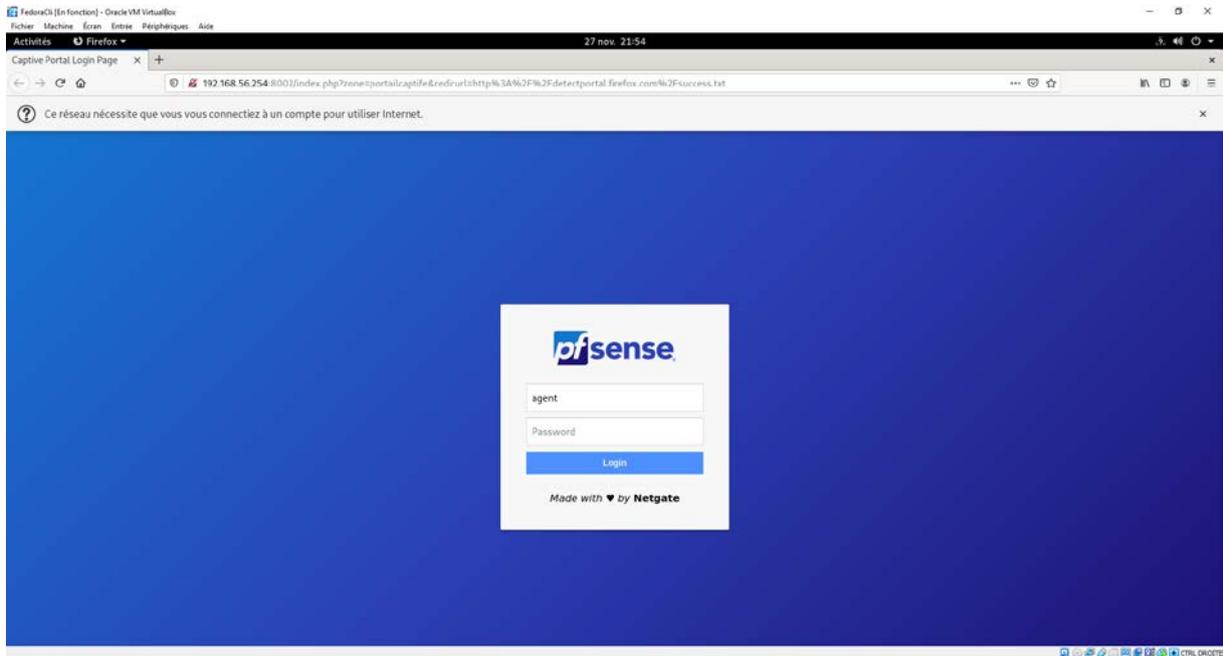
Onglet “Users“, cliquez sur “+ Add”.

Entrer un Nom d’Utilisateur “test”, son mot de passe et sa description “Un Utilisateur du Portail”.

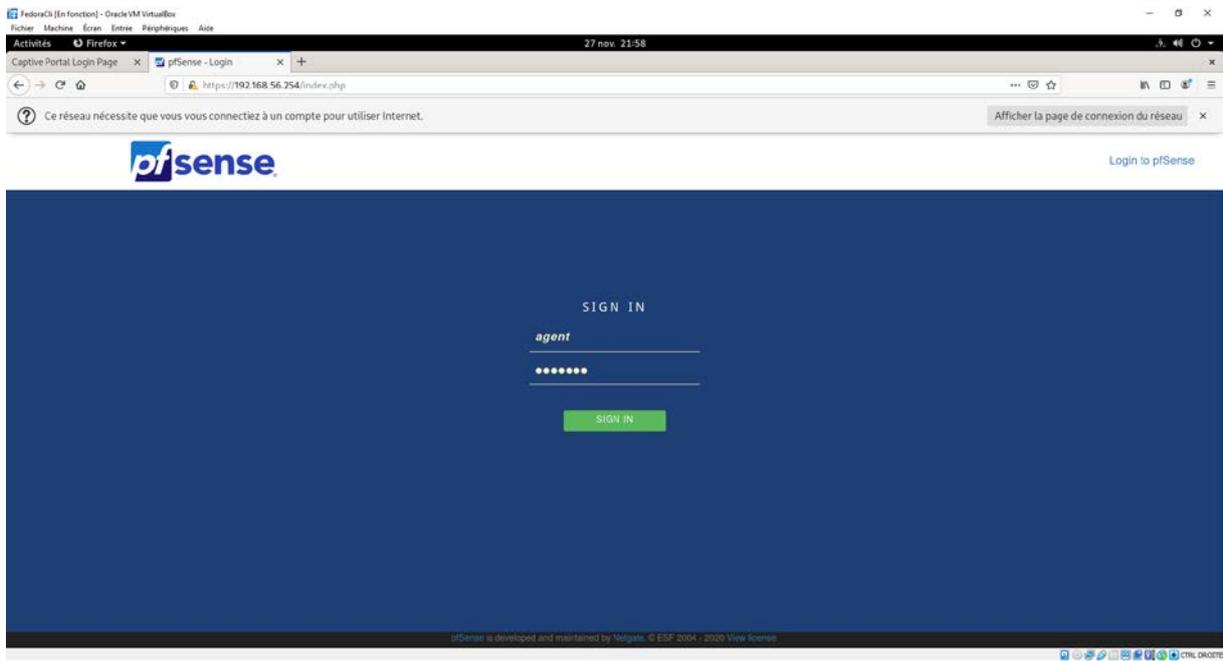
Sélectionner dans “Group membership” le groupe “Portail” précédemment créé. Cliquez sur “Move to Member of list” puis “Save”.

L’utilisateur “test” est autorisé à se connecter au Portail Captif.

Connexion avec le Compte "agent".

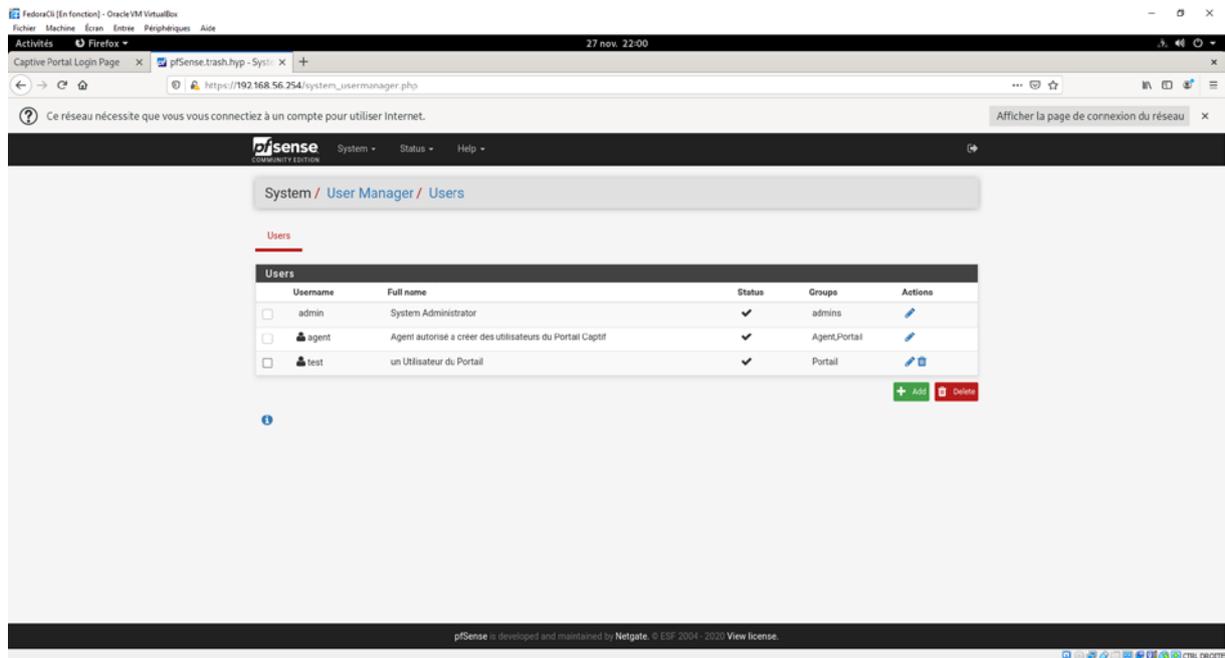


Comme nous pouvons le voir, il nous indique que ce réseau nécessite que nous nous connectons pour utiliser Internet. Testons avec le compte Agent.

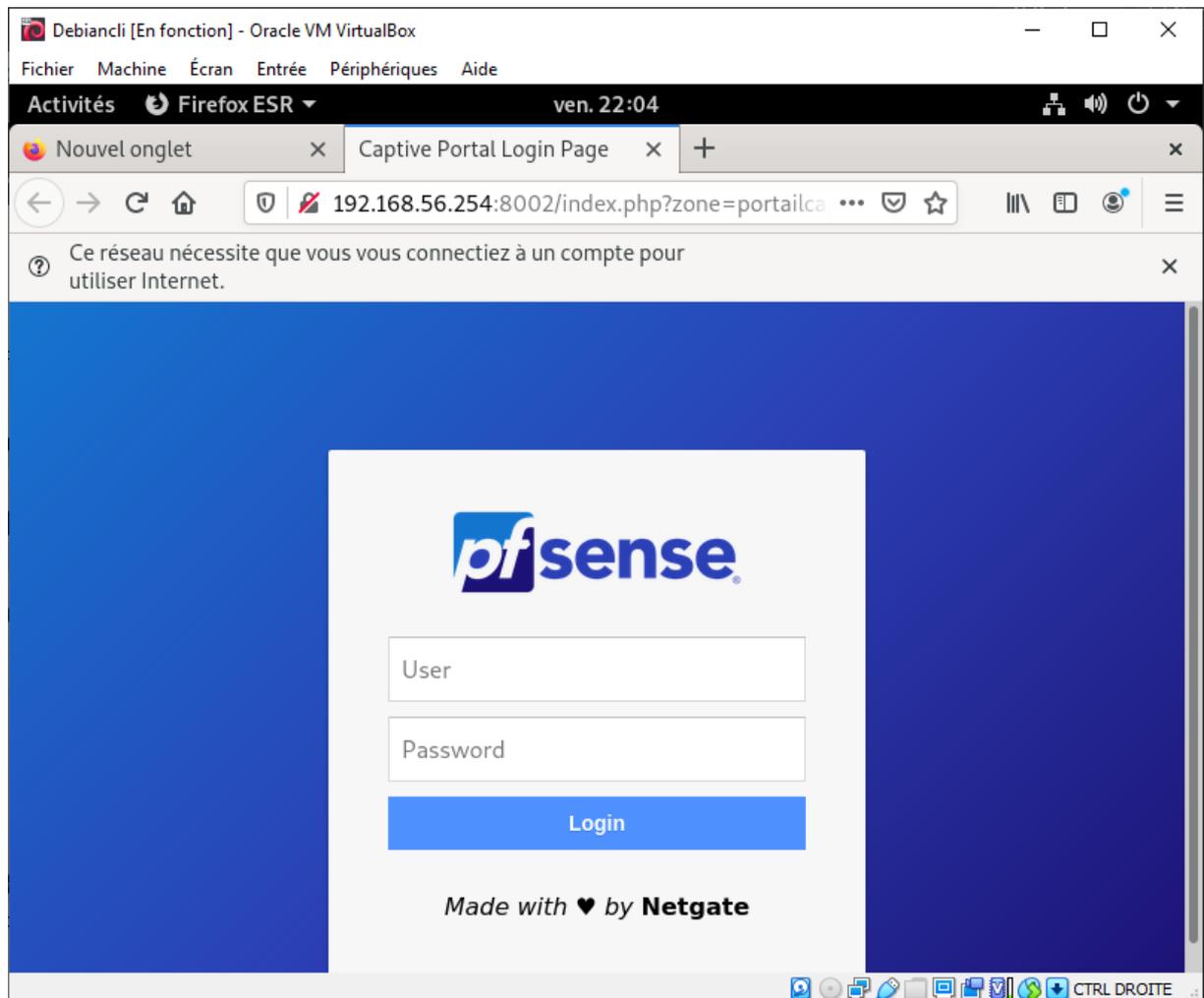


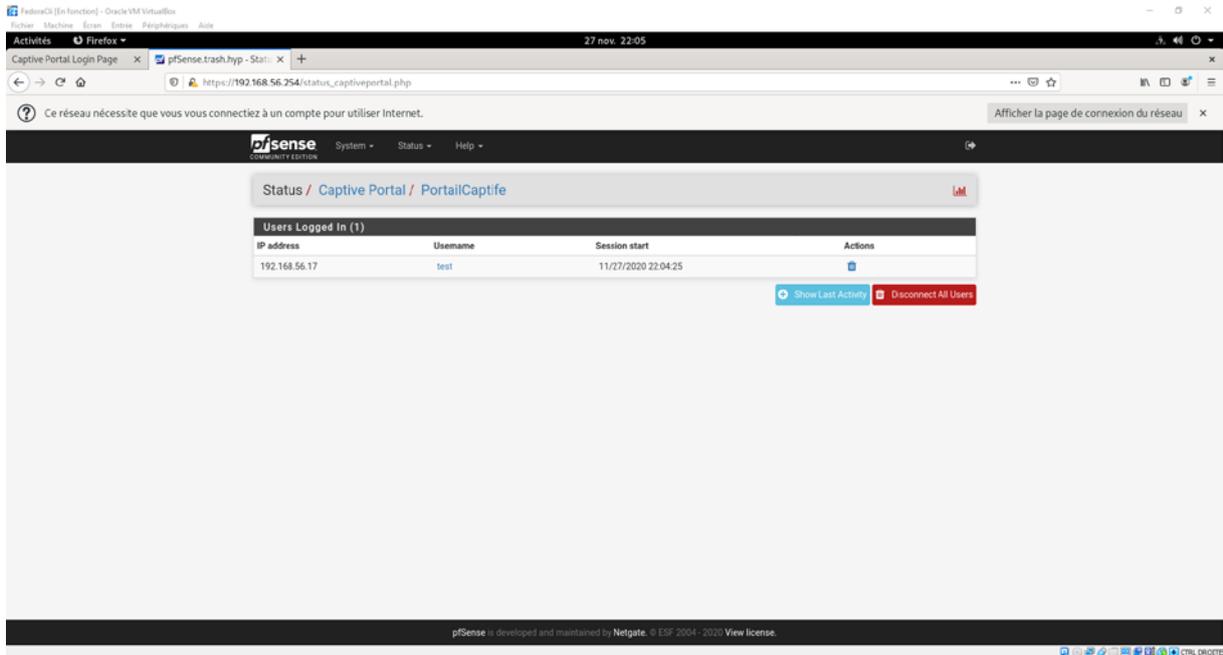
Utilisez la page de connections pfSense d'administration.

Cet utilisateur a seulement le droit de créer des Utilisateurs du Portail Captif par délégation et de voir le Statut des utilisateurs connectés.



Dans l'onglet Status nous pouvons voir les utilisateurs qui sont connecter au portail captif. testons cela avec un client avec l'identifiant test.





Comme nous pouvons le voir le client s'est connecter et peut faire des recherches internet.

