

Projet Infra – B2 Ynov Info 2021

CHAMASS Ali & LECCHI Louis

Table des matières

- I. Groupe & Consignes
- II. Présentation
- III. Installation & Configuration de PfSense
- IV. Mise en place des règles du Firewall
- V. Mise en place du DNS
- VI. Création serveur DHCP
- VII. Mise en place d'un portail captif
- VIII. Configuration de SquidGuard
- IX. Configuration de Snort
- X. Conclusion

I. Consignes

2eme PROJET : Architecture réseau et sécurité

Mise en place d'une architecture réseau avec des fonctionnalités avancées

- De préférence Open Source
- Fonctionnalités possibles :
 - firewall
 - portail captif
 - DMZ
 - Honeypot
 - VLAN
 - Redondance réseau
 - Sauvegarde de la configuration réseau
- Gestion de zones réseau
 - Sécurisé/non sécurisé, connecté à internet/isolé
 - Où sont les PCs clients ? Les serveurs ? quid de la robustesse ?

II. Présentation

PfSense est un routeur/pare-feu open source basée sur FreeBSD. Il peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (packet filter), comme iptables sur GNU/Linux, il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN.

Fonctionnalités :

- Firewall,
- NAT (Network Address Translation)
- Load Balancer
- Proxy et Proxy inverse
- VPN
- DNS dynamique

III. Installation et configuration de PfSense

Nous allons commencer par créer une VM pour le pfSense, pour cela, suivre les étapes suivantes comme indiqué sur l'image ci-dessous (nous allons utiliser la version 16 de Workstation).

Création de la VM

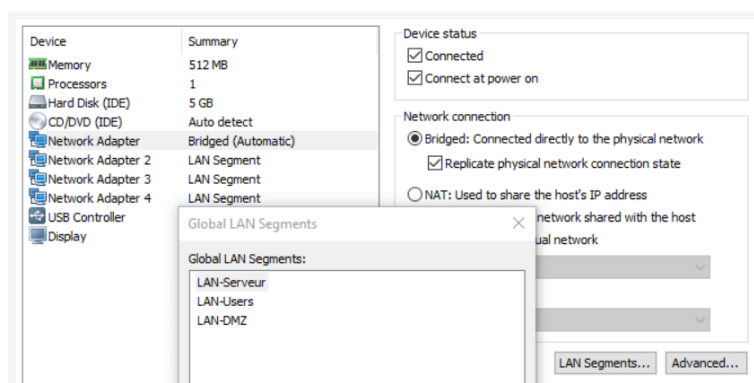
Préparez le fichier ISO de pfSense et lancez **VMware Workstation Pro**.

- « **Create a New Virtual Machine** »
 - « **Custom (Advanced)** »
 - Hardware Compatibility : « **Workstation 11.x ou Workstation 12.x** »
 - Install From : « **I will install the operating system later** »
 - Select a Guest Operating System : « **Other à FreeBSD 64-bit** »
 - Virtual Machine Name : « **pfSense** »
 - Processors :
 - Number of Processors : « **1** »
 - Number of Cores per Processor : « **1** »
 - Memory for this Virtual Machine : « **512 MB** »
 - Network Connection : « **Use Bridged Networking** »
 - SCSI Controller : « **LSI Logic (Recommended)** »
 - Virtual Disk Type : « **IDE ou SCSI** »
 - **Create a New Virtual Disk**
 - Max Disk Size : « **5 GB** » « **Store Virtual Disk as a single file** »

Ensuite, nous allons ajouter 3 cartes réseaux à la VM :

Ajout des interfaces LAN-Segments

Éditez les paramètres de la machine virtuelle pfSense. En bas, cliquez sur le bouton « **Add** » sélectionnez « **Network Adapter** » et valider. Répétez l'opération 3 fois.



NetWork Adapter	= Bridged	= 192.168.1.41/24	= Le réseau de ma machine hôte
NetWork Adapter 2	= LAN_Serveurs	= 172.16.1.1/18	= Le réseau LAN pour les serveurs
NetWork Adapter 3	= LAN_Users	= 172.16.64.1/18	= Le réseau LAN pour les Utilisateurs
NetWork Adapter 4	= LAN_DMZ	= 172.16.128.1/18	= Le réseau de la DMZ

Utiliser ces adresses IP comme sur l'image ci-dessus.

Redémarrer la VM pour prendre en compte les nouvelles cartes réseaux

Nous allons maintenant configurer ces sous réseaux sous pfSense.

```
*** Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.41/24
LAN (lan)      -> em1      ->

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: █
```

Tapez « 1 » pour « Assign Interfaces » puis choisir les options suivantes :

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

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(em1 em2 em3 em4 a or nothing if finished): em1
```

Sur votre PC (machine hôte), lancez une invite de commande (CMD) et tapez « ipconfig /all ». Il faut donc identifier l'adresse IP de votre PC et la passerelle. Vous ne pouvez pas utiliser cette adresse pour l'interface WAN de pfSense car votre PC l'utilise déjà. Il faut donc choisir une autre adresse. Nous avons choisi : 192.168.1.41
Le masque et la passerelle ne change pas.

Retourner sur la console pfSense puis tapez « 2 » pour « Set interface(s) IP address » puis appliquez les paramètres suivants pour configurer le WAN

```
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.41
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
255.255.255.0 = 24
255.255.0.0   = 16
255.0.0.0     = 8
Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.254
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
> <ENTÉE>
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

L'interface WAN est prête, vous pouvez même faire un test avec la commande PING.

- Tapez « 7 » pour « Ping host »
- Tapez en minuscule : google.fr ou : 8.8.8.8

Retourner sur la console pfSense puis tapez « 2 » pour « Set interface(s) IP address » puis appliquez les paramètres suivants pour configurer le LAN

```

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.1.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
255.0.0.0 = 8
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 18
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> <ENTER>
Enter the new LAN IPv6 address. Press <ENTER> for none:
> <ENTER>
Do you want to enable DHCP server on LAN? (y/n) n
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

```

C'est bon pour le réseau LAN (LAN-Serveurs). L'interface web de pfSense est accessible à l'adresse <http://172.16.1.1/> avec les ID par défaut suivant : admin – pfsense

Nous devons obtenir un résultat final qui ressemble à ceci :

```

WAN (wan)      -> em0      -> v4: 192.168.1.41/24
SERVEURS (lan) -> em1      -> v4: 172.16.1.1/18
USERS (opt1)   -> em2      -> v4: 172.16.64.1/18
DMZ (opt2)     -> em3      -> v4: 172.16.128.1/18

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
4) Reset to factory defaults  12) PHP shell + pfSense tools
5) Reboot system              13) Update from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                   15) Restore recent configuration
8) Shell                       16) Restart PHP-FPM

Enter an option: █

```

- WAN (réseau de ma machine hôte)
- LAN-Serveurs (réseau pour les serveurs) (portail pfsense)
- Lan-Users (réseau pour les utilisateurs)
- Lan-DMZ (réseau de la DMZ) : zone démilitarisée, réseau isolé séparant le LAN du WAN, hébergeant les machines du réseaux interne qui ont besoin d'être accessibles depuis l'extérieur (serveur web, ftp, proxy), donc les serveurs du lan ne sont jamais directement exposé à internet. La DMZ augmente la sécurité.

Installons maintenant une VM Windows server 2019 pour accéder à PfSense via l'interface web.

- « **Create a New Virtual Machine** »
 - « **Custom (Advanced)** »
 - Hardware Compatibility : « **Workstation 11.x ou Workstation 12.x** »
 - Install From : « **I will install the operating system later** »
 - Select a Guest Operating System : « **Microsoft Windows > Windows Server 2012** »
 - Virtual Machine Name : « **AD-SERVER12** »
 - **Processors :**
 - Number of Processors : « **2** »
 - Number of Cores per Processor : « **1** »
 - Memory for this Virtual Machine : « **2024 MB** »
 - Network Connection : « **Use Bridged Networking** »
 - SCSI Controller : « **LSI Logic (Recommended)** »
 - Virtual Disk Type : « **IDE ou SCSI** »
 - **Create a New Virtual Disk**
 - Max Disk Size : « **60 GB** » « **Store Virtual Disk as a single file** »

Après l'installation de la VM nous allons configurer le réseau du serveur :

- Effectuez un clic droit sur le Centre Réseau et partage présent dans la zone de notification
- Cliquez sur Ouvrir le Centre Réseau et partage.
- Sur la colonne de gauche, cliquez sur Modifier les paramètres de la carte.
- Clic droit sur la carte réseau, puis sur Propriété
- Double clic sur Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 1 . 2

Masque de sous-réseau : 255 . 255 . 192 . 0

Passerelle par défaut : 172 . 16 . 1 . 1

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 8 . 8 . 8 . 8

Serveur DNS auxiliaire : 8 . 8 . 4 . 4

☐ Valider les paramètres en quittant

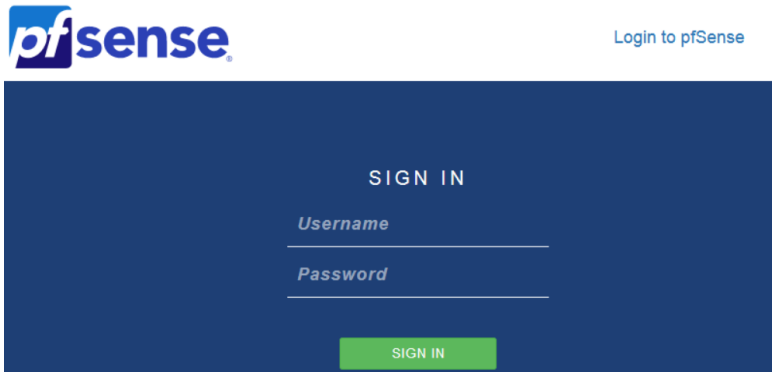
Avancé...

OK Annuler

IV. Mise en place des règles du Firewall

Se connecter à l'interface pfSense à l'adresse suivante :

- `http://172.16.1.1`
- User : admin
- Password : pfsense



Normalement, sur PfSense les règles du firewall sont configurées de base.

Une fois connecté, cliquez sur « Next » pour procéder à une configuration initiale. C'est facultatif, vous pouvez aussi cliquer sur le logo pfSense pour atteindre le tableau de bord.

À l'étape 3/9, « Time Server Information », sélectionnez Europe/Paris dans « Timezone » laissez le reste par défaut.

À l'étape 6/9, mettez un mot de passe pour le compte admin <Next>. C'est terminé.

On peut installer les VM-Tools via le menu « Système / Gestionnaire de paquets / Paquets disponibles » :

- CTRL+F et chercher « Open-VM-Tools »
- Cliquez sur « install » puis confirmer et patientez.



V. Mise en place du DHCP

Dans Services > DHCP Server dans la partie LAN :

On coche la case « Activer le serveur DHCP sur l'interface SERVEURS » et on définit la plage de l'adresse IP :

WAN **SERVEURS** USERS DMZ

Options générales

Activer ☒ Activer le serveur DHCP sur l'interface SERVEURS

BOOTP ☐ Ignorer les requêtes BOOTP

Rejeter les clients inconnus ☐ Seuls les clients définis ci-dessous obtiendront des bails DHCP de ce serveur.

Ignorer les clients inconnus ☐ Les clients refusés seront ignorés plutôt que rejetés
Cette option n'est pas compatible avec le failover et ne peut pas être activée lorsqu'une adresse Failover Peer IP est configurée.

Ignorer les identifiants clients ☐ Si un client inclue un identifiant unique dans sa requête DHCP, cet UID ne sera pas enregistré dans son bail.
Cette option peut être utile lorsqu'un client peut dual boot en utilisant différents identifiants client, mais avec la même adresse matérielle (MAC).
Notez que ce comportement du serveur est contraire aux spécifications officielles de DHCP.

Sous-réseau 172.16.0.0

Masque de sous-réseau 255.255.192.0

Plage disponible 172.16.0.1 - 172.16.63.254

Plage De 172.16.0.1 À 172.16.63.245

V. Mise en place du DNS

Dans Services > DNS Resolver Server dans la partie LAN :

On coche la case « Enable DNS Resolver » :

General DNS Resolver Options

Enable ☒ Enable DNS resolver

On active le DNSSEC :

DNSSEC ☒ Enable DNSSEC Support

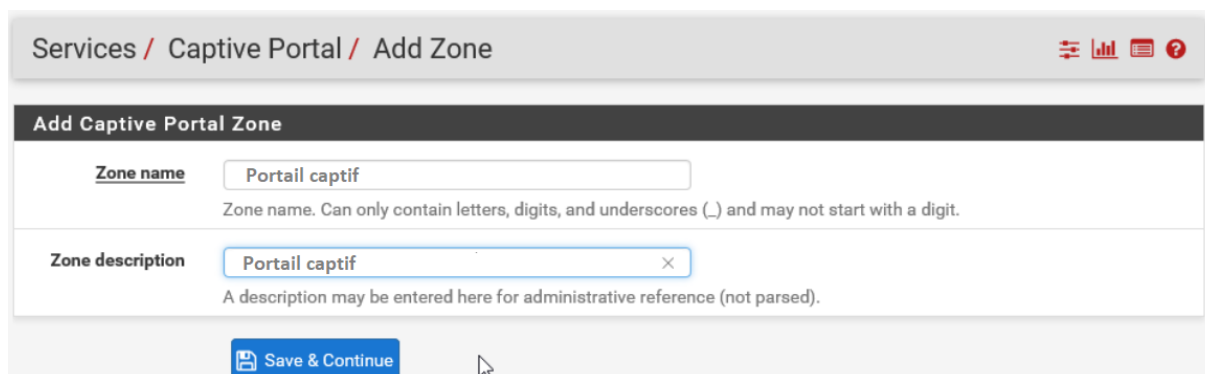
Pour plus de sécurité on active les extensions de sécurité du système des noms de domaine (DNSSEC) :

DNS Query Forwarding ☐ Enable Forwarding Mode

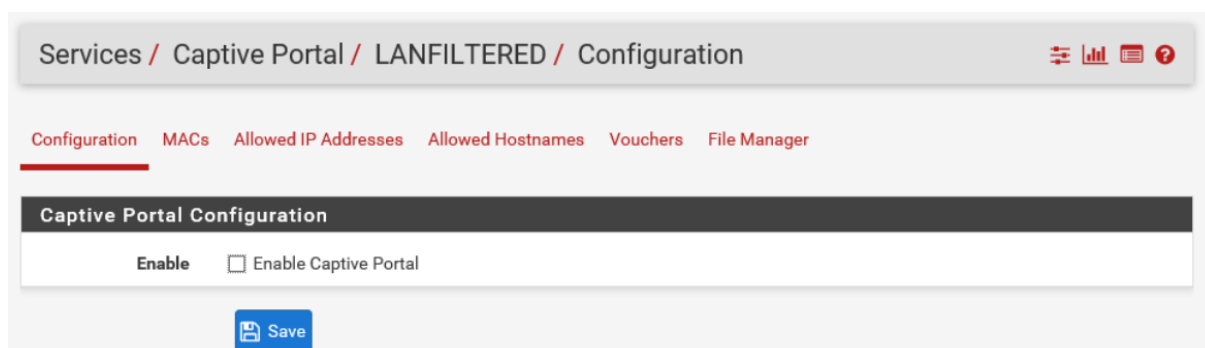
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via DHCP/PPP on WAN (if DNS Server Override is enabled there).

V. Mise en place d'un portail captif

Dans l'interface principale de pfSense, cliquez sur le menu « Services », puis sur l'option « Captive portal ». Cliquez sur le bouton « Add ». Donner un nom et une description à cette zone :



Cliquez sur le bouton « Save & continue » pour passer à la suite de la configuration – c'est à partir de cet instant que ça devient plus intéressant mais aussi plus complexe. Pour accéder aux paramètres du portail captif, il vous faut activer ce portail, en cochant la case à côté de « Enable captive portal » – n'oubliez pas de cliquer sur le bouton « Save » pour activer les paramètres.



Ainsi, tous les paramètres de configuration du portail captif vont s'afficher.

Dans l'ordre des options importantes et quasi obligatoires :

- Interfaces : il s'agit là de quelle interface sur laquelle le portail captif sera exploité – il faut cliquer sur l'interface correspondant à votre LAN (ici, LAN)
- Maximum concurrent connections : limite le nombre de connexion en même temps sur le portail captif ; si cette limite est dépassée, le portail captif ne sera pas accessible par les autres clients, jusqu'à temps qu'une place se libère. Laissez vide si vous ne souhaitez pas de limites

- Idle timeout : délai en minutes à laquelle les clients seront déconnectés s'ils n'ont pas eu / effectué d'activité. Laissez vide si vous ne souhaitez pas de limites
- Hard timeout : délai en minutes pour forcer la déconnexion des utilisateurs, qu'importe leur activité

Captive Portal Configuration	
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Interfaces	<div> <div>WAN</div> <div>LAN</div> </div> <p>Select the interface(s) to enable for captive portal.</p>
Maximum concurrent connections	<input type="text" value="3"/> <p>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.</p>
Idle timeout (Minutes)	<input type="text" value="15"/> <p>Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.</p>
Hard timeout (Minutes)	<input type="text" value="900"/> <p>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).</p>
Pass-through credits per MAC address.	<input type="text"/> <p>Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.</p>

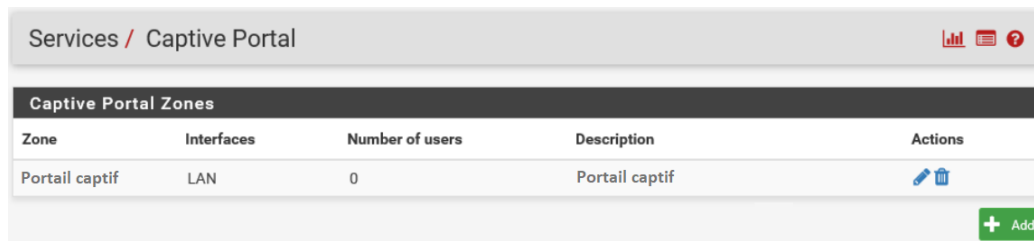
La mise en place de quota de débits (entrants / sortants) est importante – vous vous assurez ainsi une qualité de service (QoS) fiable. Il faut pour cette option cocher la case « Per-user bandwidth restriction » et saisir juste après les débits max autorisés, en Kbits/s.



Per-user bandwidth restriction	<input checked="" type="checkbox"/> Enable per-user bandwidth restriction
Default download (Kbit/s)	<input type="text" value="10000"/>
Default upload (Kbit/s)	<input type="text" value="2000"/> <p>If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty for no limit.</p>

Ensuite, cliquez sur la case « Local user manager / vouchers » et n'oubliez pas de cocher la case « Allow only users/groups with », « Captive portal login » « privilege set ».

Authentication method	<input type="radio"/> No Authentication <input checked="" type="radio"/> Local User Manager / Vouchers <input type="radio"/> RADIUS Authentication
<input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set	

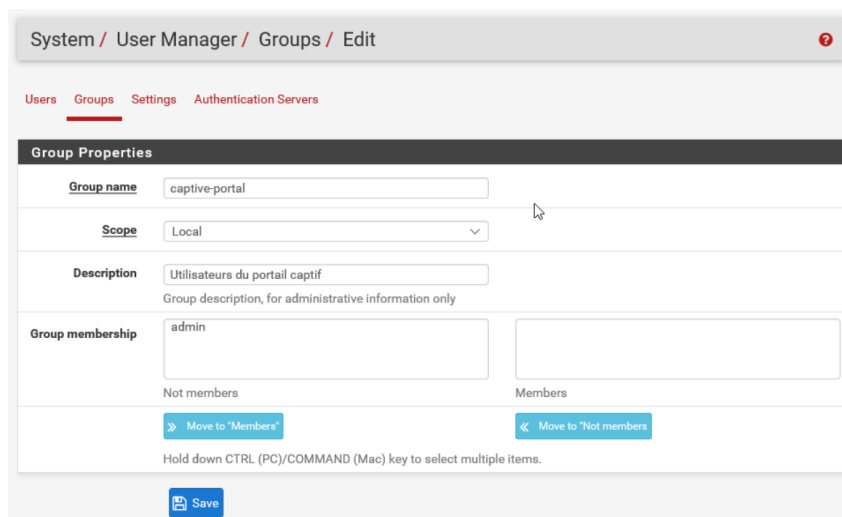
Enregistrer les modifications puis retourner à la page d'accueil du service en affichant les portails captifs disponibles :



Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
Portail captif	LAN	0	Portail captif	 

[+ Add](#)

Dirigez-vous dans la partie « System », puis dans « User manager ». Vous récupérerez une liste de tous les utilisateurs de votre pfSense. Dans la page « User Manager », cliquez sur l'option « Groups ». La liste de tous les groupes d'utilisateurs de pfSense va s'afficher – nous allons donc créer un nouveau groupe, via le bouton vert « Add ».



System / User Manager / Groups / Edit

Users Groups Settings Authentication Servers

Group Properties

Group name: captive-portal

Scope: Local

Description: Utilisateurs du portail captif
Group description, for administrative information only

Group membership

Not members: admin

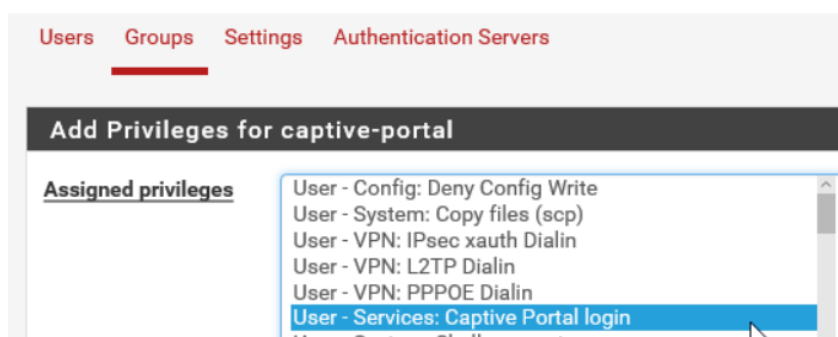
Members:

[Move to 'Members'](#) [Move to 'Not members'](#)

[Save](#)

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

Lorsque les modifications sont effectuées, enregistrez-les en cliquant sur le bouton « save ». Il va falloir de nouveau modifier le groupe précédemment créé. En effet, nous devons ajouter à notre nouveau groupe les droits pour utiliser le portail captif. Dans la rubrique « add privilèges for [nom du groupe] », sélectionnez « User – services : captive portal login » :



Users Groups Settings Authentication Servers

Add Privileges for captive-portal

Assigned privileges

- User - Config: Deny Config Write
- User - System: Copy files (scp)
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPOE Dialin
- User - Services: Captive Portal login**
- User - System: Shell account access

Pour valider les changements, cliquez une nouvelle fois sur « Save ».

Créons un compte utilisateur, retournez dans le menu « System », puis sur « User manager ». Cliquez sur le bouton vert « Add » :

The screenshot shows the 'System / User Manager / Users / Edit' page. The breadcrumb trail is 'System / User Manager / Users / Edit'. Below the breadcrumb, there are tabs: 'Users' (selected), 'Groups', 'Settings', and 'Authentication Servers'. The main section is titled 'User Properties'. It contains the following fields:

- Defined by:** USER
- Disabled:** ☐ This user cannot login
- Username:** user2
- Password:** Two password input fields, both showing masked characters (dots).
- Full name:** Compte utilisateur test. Below it, a note: 'User's full name, for administrative information only'.
- Expiration date:** A date input field. Below it, a note: '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:** Two lists. The left list is titled 'Not member of' and contains 'admins'. The right list is titled 'Member of' and contains 'captive-portal'. A mouse cursor is pointing at 'captive-portal'.

At the bottom, there are two buttons: 'Move to "Member of" list' (with a right arrow) and 'Move to "Not member of" list' (with a left arrow).

Dans le « Group membership », il faut que le groupe précédemment créé (« captive-portal » dans l'exemple de cet article) soit bien dans « Member of ». Faites bien attention à ce que le groupe « admins » soit bien dans la case « Not member of ».

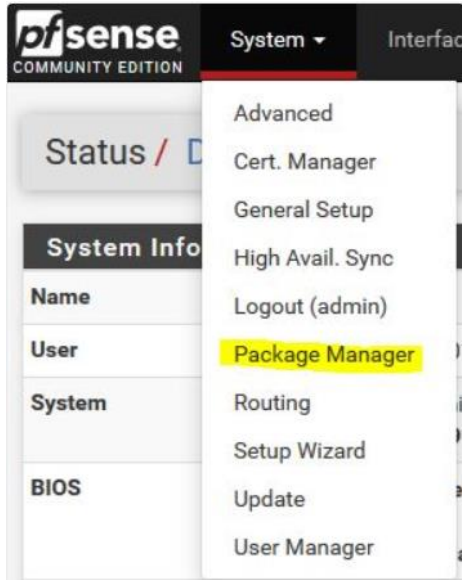
Pour tester si tout fonctionne bien, ouvrez une autre VM dans le même LAN que pfSense, ouvrez votre navigateur et tentez d'accéder à une page web. Vous devriez avoir quelque chose de ce genre :

The screenshot shows the 'pfSense captive portal' login page. It has a red header bar with the text 'pfSense captive portal'. The main content area is white and contains the following elements:

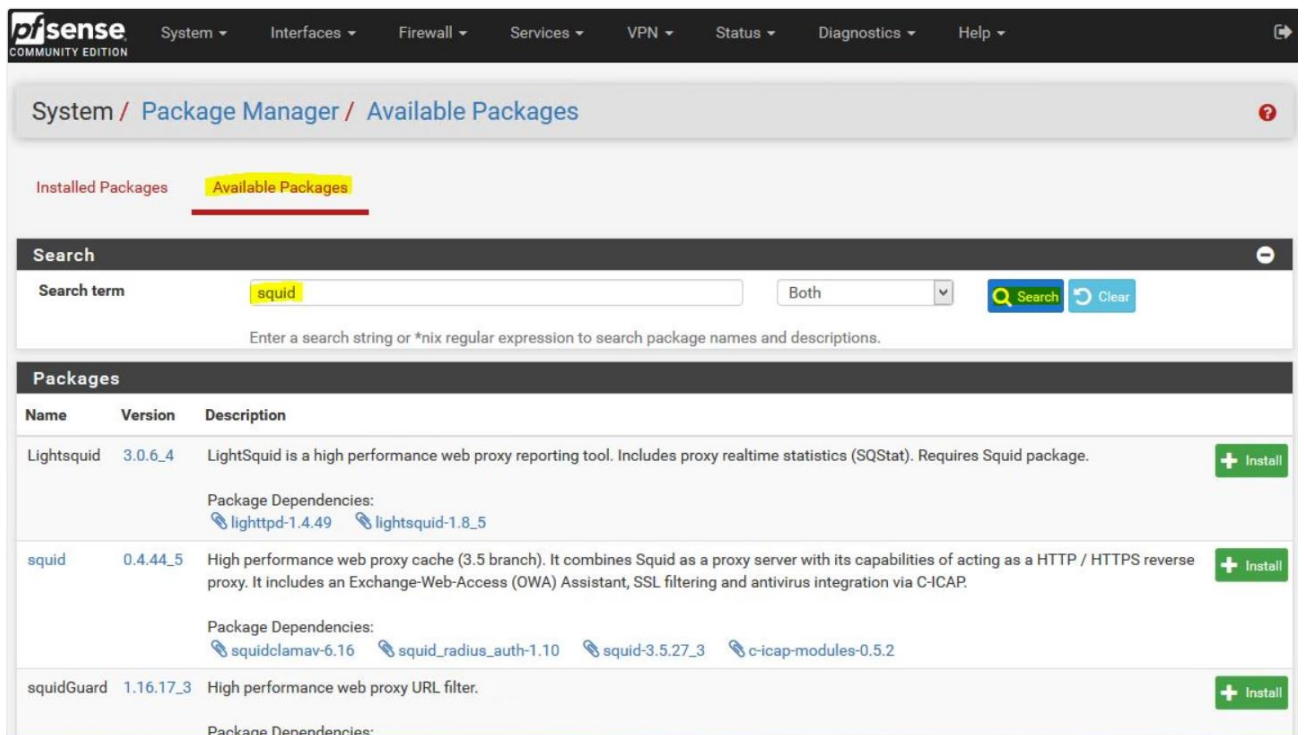
- A welcome message: 'Welcome to the pfSense Captive Portal!'.
- Two input fields: 'Username:' and 'Password:'. Both fields are empty and have dashed borders.
- A 'Continue' button located below the password field.
- A mouse cursor pointing at the 'Continue' button.

VI. Configuration de SquidGuard

Sélectionner : System, Package Manager



Sélectionner “Available Packages”, dans la recherche taper “squid” puis cliquez sur “Search”. Installer les 3 packages un par un : Squid, SquidGuard, LightSquid.



Création du Certificat pour le filtrage en HTTPS, Sélectionner : System, Cert. Manager, cliquer sur "Add". Ensuite donner un nom et laisser le reste par défaut.

System / Certificate Manager / CAs / Edit

CAs

Certificates

Certificate Revocation

Create / Edit CA

Descriptive name

SquiGuard

Method

Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits)

2048

Digest Algorithm

sha256

Lifetime (days)

3650

Common Name

internal-ca

The following certificate authority subject components are optional and may be left blank.

Country Code

None

State or Province

e.g. Texas

City

e.g. Austin

Organization

e.g. My Company Inc

Organizational Unit

e.g. My Department Name (optional)

Save

Le Certificat est créé

System / Certificate Manager / CAs

CAs

Certificates

Certificate Revocation

Search

Search term





Both

Search

Clear

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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
DemoCA	✓	self-signed	0	CN=internal-ca Valid From: Mon, 20 Jul 2020 17:27:46 +0200 Valid Until: Thu, 18 Jul 2030 17:27:46 +0200		   

Add

Configurons Squid maintenant, sélectionner “Services” et “Squid Proxy Server” :

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', and 'VPN'. The 'Services' menu is open, displaying a list of services. 'Squid Proxy Server' is highlighted in yellow. On the left, the 'System Information' section is visible, showing details about the system, BIOS, and version.

System Information	
Name	pfSense.localdomain
User	admin@192.168.2.101 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: 391ed73786ee43989c09
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Wed May 23 2012
Version	2.4.4-RELEASE (amd64) built on Thu Sep 20 09:03:12 EDT 2018 FreeBSD 11.2-RELEASE-p3 The system is on the latest version. Version information updated at Mon Oct 1 12:00:00 EDT 2018
CPU Type	Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	01 Hour 32 Minutes 59 Seconds

- 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

Sélectionner “Local Cache” et paramétrer :

- “Hard Disk Cache Size” : 500 Mo, mais 3000 Mo est préférable en production
- “Memory Cache Size” : 50% de la RAM installée > 1000 MB
- Cliquer sur “Save”

The screenshot shows the 'Squid Cache General Settings' page in the pfSense web interface. The page has tabs for 'General', 'Remote Cache', 'Local Cache', 'Antivirus', 'ACLs', 'Traffic Mgmt', 'Authentication', 'Users', 'Real Time', and 'Sync'. The 'Local Cache' tab is selected. The settings include 'Cache Replacement Policy' set to 'Heap LFUDA', 'Low-Water Mark in %' set to '90', and 'High-Water Mark in %' set to '95'. Each setting has a description and an information icon.

Package / Proxy Server: Cache Management / Local Cache

General Remote Cache **Local Cache** Antivirus ACLs Traffic Mgmt Authentication Users Real Time Sync

Squid Cache General Settings

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

Low-Water Mark in %: 90
The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.

High-Water Mark in %: 95
The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.

Squid Hard Disk Cache Settings

Hard Disk Cache Size

500

Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System

ufs

This specifies the kind of storage system to use.

Clear Disk Cache NOW

Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.

If you wish to clear cache **immediately**, click this button **once**:

Clear Disk Cache NOW

Level 1 Directories

16

Specifies the number of Level 1 directories for the hard disk cache.

Hard Disk Cache Location

/var/squid/cache

This is the directory where the cache will be stored. Default: /var/squid/cache

Minimum Object Size

0

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

Maximum Object Size

4

Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

Squid Memory Cache Settings

Memory Cache Size

64

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)

Maximum Object Size in RAM

256

Objects greater than this size (in kilobytes) will not be attempted to kept in the memory cache. Default: 256 (KB)

Memory Replacement Policy

Heap GDSF

The memory replacement policy determines which objects are purged from memory when space is needed. Default: heap GDSF

Dynamic and Update Content

Cache Dynamic Content

☐ Select to enable caching of dynamic content.

With dynamic cache enabled, you can also apply refresh_patterns to sites like Windows Updates.

Custom refresh_patterns

Enter custom refresh_patterns for better dynamic cache usage.

Note: These refresh_patterns will only be included if 'Cache Dynamic Content' is enabled.

Save

Dans l'onglet « General » : Activer "Enable Squid Proxy", sélectionner l'interface réseau « LAN » et « Resolve DNS IPv4 First ».

Package / Proxy Server: General Settings / General

General

Remote Cache

Local Cache

Antivirus

ACLs

Traffic Mgmt

Authentication

Users

Real Time

Sync

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.

Proxy Interface(s)

LAN

WAN

loopback

The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Proxy Port

3128

This is the port the proxy server will listen on. Default: 3128

ICP Port

This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

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 (;)

Activer “Transparent HTTP Proxy” et sélectionner l'interface réseau “LAN”

- “Bypass Proxy for These Source IPs” : Autoriser des postes du réseau local par leurs IP, Nom d'Hôte, Alias... Entrées séparées par des points-virgules (;)
- “Bypass Proxy for These Destination IPs” : Autoriser IP extérieure (Web)

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. <i>Transparent proxy mode works without any additional configuration being necessary on clients.</i> 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)	<div> <div>WAN</div> <div>LAN</div> </div> <p>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</p>
Bypass Proxy for Private Address Destination	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.
Bypass Proxy for These Source IPs	<input type="text" value="192.168.2.10;192.168.2.55;10-2004;MON-ORDINATEUR"/> Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)
Bypass Proxy for These Destination IPs	<input type="text"/> Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)

Activer “HTTPS/SSL Interception SSL filtering”, sélectionner “Splice All“, l'interface “LAN” et le Certificat précédemment créé “DemoCA”

SSL Man In the Middle Filtering	
HTTPS/SSL Interception	<input checked="" type="checkbox"/> Enable SSL filtering.
SSL/MITM Mode	<div>Splice All</div> <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.</p>
SSL Intercept Interface(s)	<div> <div>10.10.10.1 (pF DNSBL - DO NOT EDIT)</div> <div>WAN</div> <div>LAN</div> </div> <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"/> This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129
SSL Proxy Compatibility Mode	<div>Modern</div> <p>The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details.</p>
DHParams Key Size	<div>2048 (default)</div> <p>DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.</p>
CA	<div>DemoCA</div> <p>Select Certificate Authority to use when SSL interception is enabled.</p>
SSL Certificate Daemon Children	<input type="text" value="5"/> This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

Activer “Enable Access Logging” et définir combien de jours les logs seront conservés : 365 (un an)

Logging Settings	
Enable Access Logging	<input checked="" type="checkbox"/> This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	<input type="text" value="/var/squid/logs"/> 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	<input type="text" value="365"/> Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Log Pages Denied by SquidGuard	<input type="checkbox"/> Makes it possible for SquidGuard denied log to be included on Squid logs. Click Info for detailed instructions.

Sélectionner “fr” pour “Error language” et Activer “Suppress Squid Version”
Puis Cliquer sur “Save” pour enregistrer toutes les modifications effectuées dans Squid

Headers Handling, Language and Other Customizations	
Visible Hostname	<input type="text" value="localhost"/> This is the hostname to be displayed in proxy server error messages.
Administrator's Email	<input type="text" value="admin@localhost"/> This is the email address displayed in error messages to the users.
Error Language	<input type="text" value="fr"/> Select the language in which the proxy server will display error messages to users.
X-Forwarded Header Mode	<input type="text" value="(on)"/> Choose how to handle X-Forwarded-For headers. Default: on
Disable VIA Header	<input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616.
URI Whitespace Characters Handling	<input type="text" value="strip"/> Choose how to handle whitespace characters in URL. Default: strip
Suppress Squid Version	<input checked="" type="checkbox"/> Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Save Show Advanced Options

Configuration de SquidGuard

Sélectionner “Services” et “SquidGuard Proxy Filter”

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ **Services ▾** VPN ▾

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.2.101 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: 391ed73786ee43989c09
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Wed May 23 2012
Version	2.4.4-RELEASE (amd64) built on Thu Sep 20 09:03:12 EDT 2018 FreeBSD 11.2-RELEASE-p3 The system is on the latest version. Version information updated at Mon Oct 1 15:00:00 UTC 2018
CPU Type	Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	03 Hours 01 Minute 26 Second

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


Activer SquidGuard “Enable”

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

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**

Activer “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.

Miscellaneous

Clean Advertising ☐ Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

Activer “Enable Blacklist” et inserer dans Blacklist URL : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Puis cliquez sur “Save”

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).

 Save

Onglet “Blacklist” : Cliquer sur “Download” pour télécharger les listes de filtrage




Package / SquidGuard / Blacklists

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

Blacklist Update

Blacklist DB rebuild progress

1 %

 Download  Cancel  Restore Default

Enter FTP or HTTP path to the blacklist archive here.

Onglet “Common ACL”, Cliquez, dans “Target Rules List” sur le “ + ”
Sélectionner les catégories a bloquer (ou a autoriser), Sélectionner ”Allow” pour
“Default access [all]”

[URL_BLACKLISTS_WAREZ]	access	—
[blk_blacklists_webmail]	access	—
Default access [all]	access	allow

Cocher “Do not allow IP addresses in URL” et “Use SafeSearch engine”
Puis cliquer “Save”

Do not allow IP-Addresses in URL	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
Proxy Denied Error	<input type="text"/> <small>The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$g[product_name] proxy"</small>
Redirect mode	<input type="text" value="int error page (enter error message)"/> <small>Select redirect mode here. Note: If you use 'transparent proxy', then 'int' redirect mode will not be accessible. Options: ext url err page, ext url redirect, ext url as 'move', ext url as 'found'.</small>
Redirect info	<input type="text"/> <small>Enter external redirection URL, error message or size (bytes) here.</small>
Use SafeSearch engine	<input checked="" type="checkbox"/> Enable the protected mode of search engines to limit access to mature content. <small>At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. Note: This option overrides 'Rewrite' setting.</small>
Rewrite	<input type="text" value="none (rewrite not defined)"/> <small>Enter the rewrite condition name for this rule or leave it blank.</small>
Log	<input type="checkbox"/> Check this option to enable logging for this ACL.
<input type="button" value="Save"/>	

Pour valider les paramétrages, retournez sur l’onglet “General settings” et cliquez sur
“Apply”

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

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.**

SquidGuard service state: **STARTED**

Configurons LightSquid, sélectionner “Status” et “Squid Proxy Reports”
Décocher “LightSquid Web SSL” pour une connexion Web en HTTP et définir le mot de passe admin

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Package / Squid Proxy Reports: Settings

Instructions

Perform these steps after install **IMPORTANT:** Click Info and follow the instructions below if this is initial install! [i](#)

Web Service Settings

Lightsquid Web Port 7445
Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)

Lightsquid Web SSL ☐ Use SSL for Lightsquid Web Access
This option configures the Lightsquid web server to use SSL and uses the WebGUI HTTPS certificate.

Lightsquid Web User admin
Username used to access lighttpd. (Default: admin)

Lightsquid Web Password *****
Password used to access lighttpd. (Default: pfsense)

Links [Open Lightsquid](#) [Open sqstat](#)

Sélectionner la langue “French”

Report Template Settings

Language French
Select report language.

Report Template Base
Select report template.

Bar Color Orange
Select bar color.

Sélectionner “SquidAuth” pour “IP Resolve Method” et “60min” pour “Refresh Scheduler”

Puis cliquez “Save” et “Refresh Full”

Reporting Settings and Scheduler

IP Resolve Method Squidauth
Select which method(s) should be attempted (in the order listed below) to resolve IPs to hostnames.
Click Info for details. (Default: DNS) [i](#)

Skip URL(s)

If you want to omit some sites from statistics (e.g., a local webserver), specify the URL(s) here.
Separate multiple entries by | character. **Example:** example.com|192.168.1.|example.net

Refresh Scheduler 60min (+)
Select data refresh period. The reporting task will be executed every XX minutes/hours.
Legend: (!)(*) Use only with fast hardware (+) Recommended values

Manual Refresh Use these buttons to start a background refresh of the Lightsquid reports.

[Refresh](#) Will (re)parse today's entries only in Squid's current access.log.

[Refresh Full](#) Will (re)parse all entries in all Squid's access logs, including the rotated ones. This may take a long time to finish!

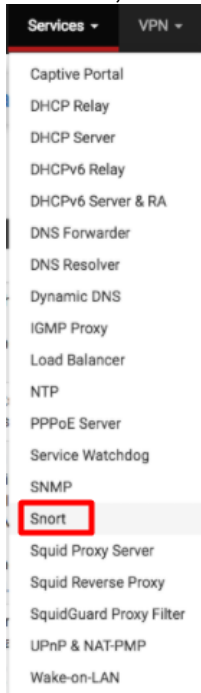
[Save](#)

Pour accéder à la Console Web LightSquid, Tapez http://192.168.2.1:7445 dans la barre d'adresse du navigateur et renseigner le login et mot de passe.

VII. Configuration de Snort

Sélectionner “Available Packages”, dans la recherche taper “Snort” puis cliquez sur “Search”. Installer le premier package.

Ensuite, accédez à Services -> Snort dans le menu de l'interface Web pfSense.



Cliquez sur l'onglet « Global settings » et activez les téléchargements de l'ensemble de règles à utiliser :

A screenshot of the 'Services / Snort / Global Settings' page in pfSense. The page has a breadcrumb trail at the top: 'Services / Snort / Global Settings'. Below this is a horizontal tab bar with 'Snort Interfaces', 'Global Settings' (selected), 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The main content area is divided into several sections:

- Snort Vulnerability Research Team (VRT) Rules**: Includes a checkbox for 'Enable Snort VRT' (checked), a link to 'Click to enable download of Snort VRT free Registered User or paid Subscriber rules', and a text input field for 'Snort Oinkmaster Code' containing 'my_oinkcode'. Below the input field is a note: 'Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL)'.
- Snort GPLv2 Community Rules**: Includes a checkbox for 'Enable Snort GPLv2' (unchecked) and a link to 'Click to enable download of Snort GPLv2 Community rules'. Below is a paragraph: 'The Snort Community Ruleset is a GPLv2 VRT certified ruleset that is distributed free of charge without any VRT License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.'
- Emerging Threats (ET) Rules**: Includes a checkbox for 'Enable ET Open' (checked) and a link to 'Click to enable download of Emerging Threats Open rules'. Below is a paragraph: 'ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.' It also includes a checkbox for 'Enable ET Pro' (unchecked) and a link to 'Click to enable download of Emerging Threats Pro rules'. Below that is a link to 'Sign Up for an ETPro Account' and a paragraph: 'ETPro for Snort offers daily updates and extensive coverage of current malware threats.'
- Sourcefire OpenAppID Detectors**: Includes a checkbox for 'Enable OpenAppID' (unchecked) and a link to 'Click to enable download of Sourcefire OpenAppID Detectors'. Below is a paragraph: 'The OpenAppID package contains the application signatures required by the AppID preprocessor.' and a label for 'OpenAppID Version'.

Une fois que les ensembles de règles souhaités sont activés, définissez ensuite l'intervalle pour que Snort vérifie les mises à jour des packages de règles activées.

Rules Update Settings

Update Interval
Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time
Enter the rule update start time in 24-hour format (HH:MM). Default is 00:05. Rules will update at the interval chosen above starting at the time specified here. For example, using the default start time of 00:05 and choosing 12 Hours for the interval, the rules will update at 00:05 and 12:05 each day.

Hide Deprecated Rules Categories ☐ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification ☐ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

Cliquez sur le bouton Mettre à jour les règles pour télécharger les dernières mises à jour du package de règles.

Services / Snort / **Update Rules**

Snort Interfaces Global Settings **Updates** Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort VRT Rules	b9df3daf94e9505fb8183c6875be19a5	Tuesday, 25-Jul-17 19:51:23 CEST
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Emerging Threats Open Rules	7069111b1e5d46f1fbdcd5190be1543d	Tuesday, 25-Jul-17 19:51:24 CEST
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort OpenAppID RULES Detectors	Not Enabled	Not Enabled

Update Your Rule Set

Last Update Jul-25 2017 19:51 Result: **Success**

Update Rules [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

[View Log](#) [Clear Log](#)

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size 34 KiB

Cliquez sur l'onglet Snort Interfaces, puis sur « Add » pour ajouter une nouvelle interface Snort. Ensuite configurer comme sur l'image ci-dessous :

Services / Snort / Edit Interface / **None**

Snort Interfaces **Global Settings** Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

None Settings **None Categories** None Rules None Variables None Preprocs None Barnyard2 None IP Rep None Logs

General Settings

Enable ☒ Enable interface

Interface
Choose the interface where this Snort instance will inspect traffic.

Description
Enter a meaningful description here for your reference.

Alert Settings

Send Alerts to System Logs ☐ Snort will send Alerts to the firewall's system logs

Block Offenders ☐ Checking this option will automatically block hosts that generate a Snort alert

Detection Performance Settings

Search Method
Choose a fast pattern matcher algorithm. Default is AC-BNFA.

Split ANY-ANY ☐ Enable splitting of ANY-ANY port group

Search Optimize ☐ Enable search optimization

Stream Inserts ☐ Do not evaluate stream inserted packets against the detection engine

Checksum Check Disable ☐ Disable checksum checking within Snort to improve performance

Sauvegarder les modifications.

Ensuite dans les paramètres de l'interface, dans WAN, cocher « USE IPS Policy et sélectionner Connectivity ».

Snort VRT IPS Policy Selection

Use IPS Policy ☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort VRT rules. Default is Not Checked.

Selecting this option disables manual selection of Snort VRT categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection Connectivity

Snort IPS policies are: Connectivity, Balanced or Security.

Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file.

Cocher ensuite les règles comme suit :

Snort VRT IPS Policy Selection

Use IPS Policy ☐ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort VRT rules. Default is Not Checked.

Selecting this option disables manual selection of Snort VRT categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection Connectivity

Snort IPS policies are: Connectivity, Balanced or Security.

Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file.

Select the rulesets (Categories) Snort will load at startup

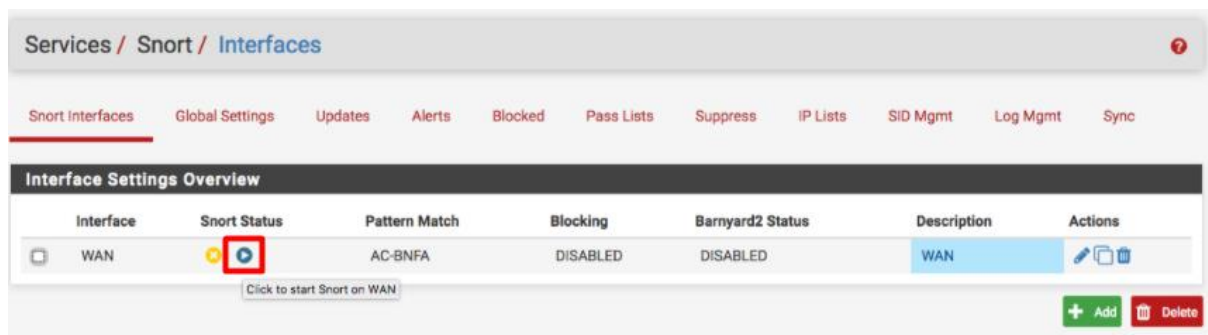
● - Category is auto-enabled by SID Mgmt conf files
● - Category is auto-disabled by SID Mgmt conf files

[Select All](#)
[Unselect All](#)
[Save](#)

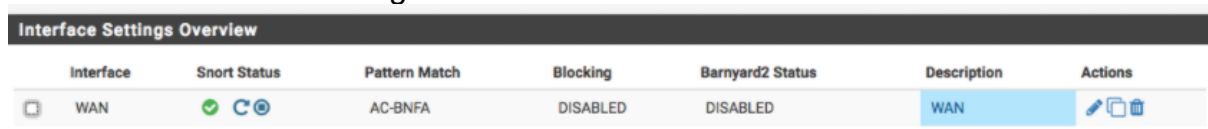
Enabled	Ruleset: ET Open Rules	Enabled	Ruleset: Snort Text Rules	Enabled	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	
<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_browser-other.so.rules	
<input type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_browser-plugins.so.rules	
<input type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	
<input checked="" type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_file-executable.so.rules	
<input type="checkbox"/>	emerging-ciarmy.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-flash.so.rules	
<input type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_file-image.so.rules	
<input type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_file-java.so.rules	
<input type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_browser-ie.rules	<input type="checkbox"/>	snort_file-multimedia.so.rules	
<input checked="" type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_browser-other.rules	<input type="checkbox"/>	snort_file-office.so.rules	
<input type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_browser-plugins.rules	<input type="checkbox"/>	snort_file-other.so.rules	
<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_browser-webkit.rules	<input type="checkbox"/>	snort_file-pdf.so.rules	
<input type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_chat.rules	<input type="checkbox"/>	snort_indicator-shellcode.so.rules	
<input type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_malware-cnc.so.rules	
<input type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_ddos.rules	<input type="checkbox"/>	snort_malware-other.so.rules	

Enregistrer les modifications avant de quitter.

Démarrons l'interface Snort en appuyons sur l'icone encadré en rouge sur l'image :



Une fois lancé l'icône changera :



Créons une liste de pass, dans « Pass Lists », cliquez sur « Add ». Laisser tout cocher comme par défaut et ajouter un alias :

The screenshot shows the 'Services / Snort / Pass List Edit' page. It has several sections: 'General Information' with fields for 'Name' (passlist_62260) and 'Description' (Pass list of IP's never to block); 'Auto-Generated IP Addresses' with checkboxes for Local Networks, WAN Gateways, WAN DNS Servers, Virtual IP Addresses, and VPN Addresses, all of which are checked; 'Custom IP Address from Configured Alias' with a field for 'Assigned Alias' (Friendly_ext_hosts); and 'Choose the Networks Snort Should Inspect and Whitelist' with dropdowns for 'Home Net' (default) and 'External Net' (passlist_62260). There are 'Save' and 'Cancel' buttons at the bottom of the first section, and 'View List' buttons next to the network dropdowns.

Enregistrer les modifications.

FIN