

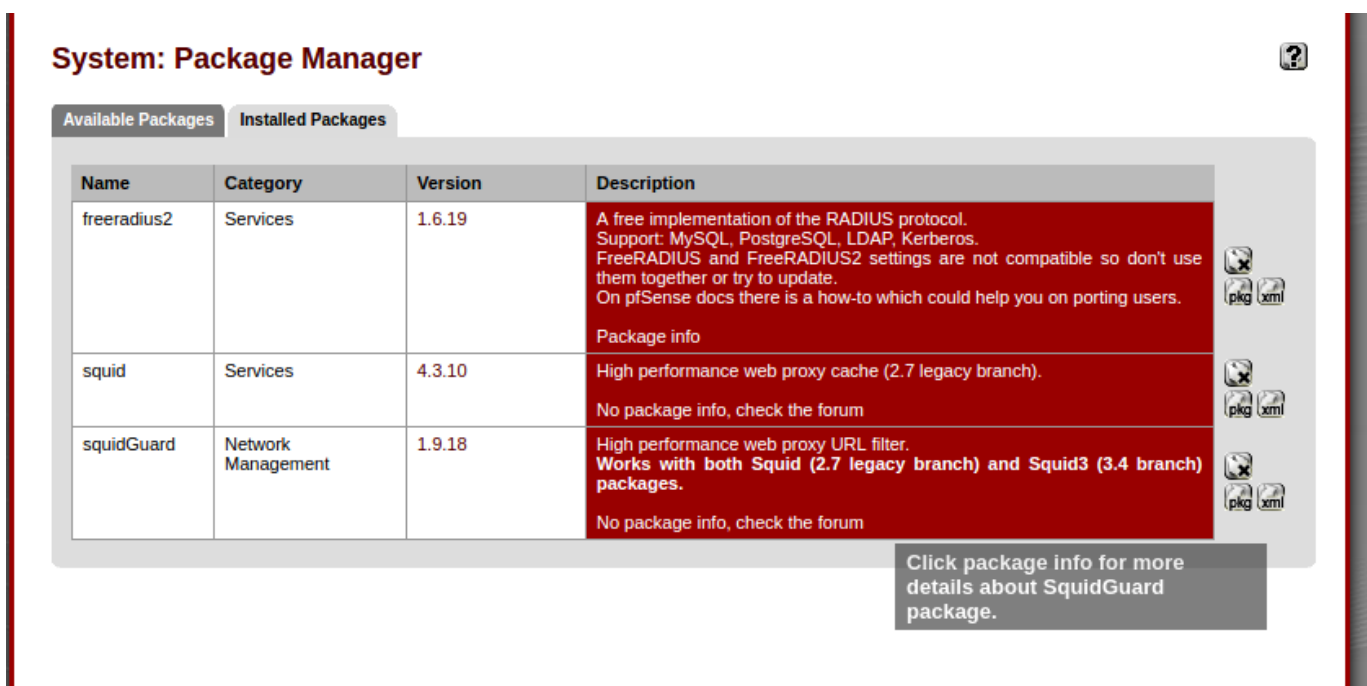
Mise en place d'un portail captif PfSense

I- Installation des paquets

Pour faire du filtrage web ainsi qu'un portail captif, il faudra installer les paquets suivant :

```
squid  
squidguard  
freeradius
```

Pour cela il faut se rendre dans "Systeme", "Packages" :



II- Configuration du filtrage avec Squid & Squidguard

Une fois les paquets installer, il faut se rendre dans :

```
"Service"  
"Squidguard Proxy"
```

Commencer par renseigner l'URL de notre blacklist, l'université de Toulouse a mis en ligne une blacklist ([Blacklist Université de Toulouse](https://www.univ-toulouse.fr/blacklist))

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.

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

Ensuite se rendre dans l'onglet "Blacklist" pour telecharger la blacklist :

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

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.
For saving configuration YOU need click button 'Save' on bottom of page
After changing configuration squidGuard you must **apply all changes**

Apply

SquidGuard service state: **STARTED**

Proxy filter SquidGuard: Blacklist page



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

Blacklist Update 0 %

Download **Cancel** **Restore default**

Enter FTP or HTTP path to the blacklist archive here.

Enfin se rendre dans "Comon ACL" pour selection ce que l'on souhaite bloquer dans "Target rules List" :

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

Target Categories

[fb]	access	deny ▼
[blk_BL_adv]	access	allow ▼
[blk_BL_aggressive]	access	deny ▼
[blk_BL_alcohol]	access	deny ▼
[blk_BL_anonvpn]	access	deny ▼
[blk_BL_automobile_bikes]	access	allow ▼
[blk_BL_automobile_boats]	access	allow ▼
[blk_BL_automobile_cars]	access	allow ▼
[blk_BL_automobile_planes]	access	allow ▼
[blk_BL_chat]	access	allow ▼
[blk_BL_cotraps]	access	allow ▼
[blk_BL_dating]	access	allow ▼
[blk_BL_downloads]	access	allow ▼
[blk_BL_drugs]	access	deny ▼
[blk_BL_dynamic]	access	allow ▼
[blk_BL_education_schools]	access	allow ▼
[blk_BL_finance_banking]	access	allow ▼
[blk_BL_finance_insurance]	access	allow ▼
[blk_BL_finance_moneylending]	access	allow ▼
[blk_BL_finance_other]	access	allow ▼
[blk_BL_finance_realestate]	access	allow ▼
[blk_BL_finance_trading]	access	allow ▼
[blk_BL_fortunetelling]	access	allow ▼
[blk_BL_forum]	access	allow ▼
[blk_BL_gamble]	access	allow ▼
[blk_BL_government]	access	allow ▼
[blk_BL_hacking]	access	deny ▼
[blk_BL_hobby_cooking]	access	allow ▼
[blk_BL_hobby_games-misc]	access	allow ▼
[blk_BL_hobby_games-online]	access	allow ▼
[blk_BL_hobby_gardening]	access	allow ▼
[blk_BL_hobby_pets]	access	allow ▼
[blk_BL_homestyle]	access	allow ▼
[blk_BL_hospitals]	access	allow ▼
[blk_BL_imagehosting]	access	allow ▼

Ne jamais oublier de cliquer sur "Save" et "Apply" a chaque modification :

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

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.
 For saving configuration YOU need click button 'Save' on bottom of page
 After changing configuration squidGuard you must **apply all changes**

SquidGuard service state: **STARTED**

III- Configuration du Portail Captif lié à un LDAP

Pour configurer le portail captif, il faut se rendre dans "Service" et "Captive Portal" :
Sélectionner l'interface :

Services: Captive portal: Wifi



Captive portal(s) | **MAC** | **Allowed IP addresses** | **Allowed Hostnames** | **Vouchers** | **File Manager**

Enable captive portal

Interfaces WAN
WANPRIVATEWIFI
PUBLICWIFI
Select the interface(s) to enable for captive portal.

Maximum concurrent connections per client IP address (0 = no limit)
This setting 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 users can load the portal page or authenticate at the same time! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100 connections.

Idle timeout minutes
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout minutes
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).

Pass-through credits allowed per MAC address per client MAC address (0 or blank = none)
This setting 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.

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

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

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

Des liens e redirection si besoin :

Astuce : pour que la pages d'authentification apparaisse tout le temps, renseignez une "Pre-authentication redirect URL"

Pre-authentication redirect URL
Use this field to set \$PORTAL_REDIRURL\$ variable which can be accessed using your custom captive portal index.php page or error pages.

After authentication Redirection URL
If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.

Blocked MAC address redirect URL
If you provide a URL here, MAC addresses set to be blocked will be redirect to that URL when attempt to access anything.

Concurrent user logins **Disable concurrent logins**
If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.

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

Pass-through MAC Auto Entry **Enable Pass-through MAC automatic additions**
If this option is set, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry you either have to log in and remove it manually from the MAC tab or send a POST from another system to remove it. If this is enabled, RADIUS MAC authentication cannot be used. Also, the logout window will not be shown.

Enable Pass-through MAC automatic addition with username
If this option is set, with the automatically MAC passthrough entry created the username, used during authentication, will be saved. To remove the passthrough MAC entry you either have to log in and remove it manually from the MAC tab or send a POST from another system to remove it.

Configuration du radius :

Primary Authentication Source

Primary RADIUS server

IP address
Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Port
Leave this field blank to use the default port (1812).

Shared secret
Leave this field blank to not use a RADIUS shared secret (not recommended).

Secondary RADIUS server

IP address
If you have a second RADIUS server, you can activate it by entering its IP address here.

Port

Shared secret

(il est possible de configurer sa page d'authentification)

Pour la liaison a son "ActiveDirectory", on se rend sur "Service", et "FreeRadius" puis dans l'onglet "NAS/Clients" :

FreeRADIUS: Clients



Users | MACs | **NAS / Clients** | Interfaces | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
127.0.0.1	ipaddr	captif.wifi	udp	other	no	16	

Important: mettre le meme "shared secret" que l'on a mit précédemment dans la configuration du portail captif:

General Configuration	
Client IP Address	<input type="text" value="127.0.0.1"/> Enter the IP address of the RADIUS client. This is the IP of the NAS (switch, access point, firewall, router, etc.).
Client IP Version	<input type="text" value="IPv4"/>
Client Shortname	<input type="text" value="captif.wifi"/> Enter a short name for the client. This is generally the hostname of the NAS.
Client Shared Secret	<input type="password" value="....."/> Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch or accesspoint) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret.

Miscellaneous Configuration	
Client Protocol	<input type="text" value="UDP"/> Enter the protocol the client uses. (Default: UDP)
Client Type	<input type="text" value="other"/> Enter the NAS type of the client. This is used by checkrad.pl for simultaneous use checks. (Default: other)
Require Message Authenticator	<input type="text" value="No"/> RFC5080 requires Message-Authenticator in Access-Request. But older NAS (switches or accesspoints) do not include that. (Default: no)
Max Connections	<input type="text" value="16"/> Takes only effect if you use TCP as protocol. This is the mirror of "Max Requests Server" from "Settings" tab. (Default 16)
NAS Login	<input type="text"/> If your NAS supports it you can use SNMP or finger for simultaneous-use checks instead of (s)radutmp file and accounting. Leave empty to choose (s)radutmp. (Default: empty)
NAS Password	<input type="text"/> If your NAS supports it you can use SNMP or finger for simultaneous-use checks instead of (s)radutmp file and accounting. Leave empty to choose (s)radutmp. (Default: empty)
Description	<input type="text"/> Enter any description you like for this client.

Se rendre ensuite dans l'onglet Interface :

FreeRADIUS: Interfaces: Edit



Users | MACs | NAS / Clients | **Interfaces** | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

General Configuration

Interface IP Address
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)

Port
Enter the port number of the listening interface. Different interface types need different ports.
You could use this as an example:
Authentication = 1812
Accounting = 1813
Status = 1816
IMPORTANT: For every interface type listening on the same IP address you need different ports.

Interface Type
Enter the type of the listening interface. (Default: auth)

IP Version
Enter the IP version of the listening interface. (Default: IPv4)

Description
Optionally enter a description here for your reference.

Se rendre dans l'onglet LDAP, bien cocher les deux case

FreeRADIUS: LDAP



Users | MACs | NAS / Clients | Interfaces | Settings | EAP | SQL | Certificates | **LDAP** | View config | XMLRPC Sync

ENABLE LDAP SUPPORT - SERVER 1

Enable LDAP For Authorization
This enables LDAP in authorize section. The ldap module will set Auth-Type to LDAP if it has not already been set. (Default: unchecked)

Enable LDAP For Authentication
This enables LDAP in authenticate section. Note that this means "check plain-text password against the ldap database", which means that EAP won't work, as it does not supply a plain-text password.

Configurer la liaison LDAP avec le Serveur AD :

General Configuration - SERVER 1	
Server	<input type="text" value="192.168.2.201"/> <small>No description. (Default: ldap.your.domain)</small>
Port	<input type="text" value="389"/> <small>No description. (Default: 389)</small>
Identity	<input type="text" value="cn=administrateur,cn=Users,dc=klyuch,dc=lan"/> <small>No description. (Default: cn=admin,o=My Org,c=UA)</small>
Password	<input type="password" value="*****"/> <small>No description. (Default: mypass)</small>
Basedn	<input type="text" value="ou=Wifi,ou=Utilisateurs,dc=klyuch,dc=lan"/> <small>No description (Default: o=My Org,c=UA)</small>
Filter	<input type="text" value="(samaccountname=%{User-Name})"/> <small>No description. (Default: (uid=%{%{Stripped-User-Name}}-){User-Name}))</small>
Base Filter	<input type="text" value="(objectclass=radiusprofile)"/> <small>No description. (Default: (objectclass=radiusprofile))</small>
LDAP Connections Number	<input type="text" value="5"/> <small>How many connections to keep open to the LDAP server. This saves time over opening a new LDAP socket for every authentication request. (Default: 5)</small>
Timeout	<input type="text" value="4"/> <small>Seconds to wait for LDAP query to finish. (Default: 4)</small>
Timelimit	<input type="text" value="3"/> <small>Seconds the LDAP server has to process the query (server-side time limit). (Default: 3)</small>
Net Timeout	<input type="text" value="1"/> <small>Seconds to wait for response of the server because of network failures. (Default: 1)</small>

Astuce : En cas de redémarrage du PfSense, il faudra revenir sur "Free Radius" et ré enseigner le mot de passe administrateur du LDAP, ainsi que re-télécharger la "blacklist" dans "Squidguard".

IV- Test

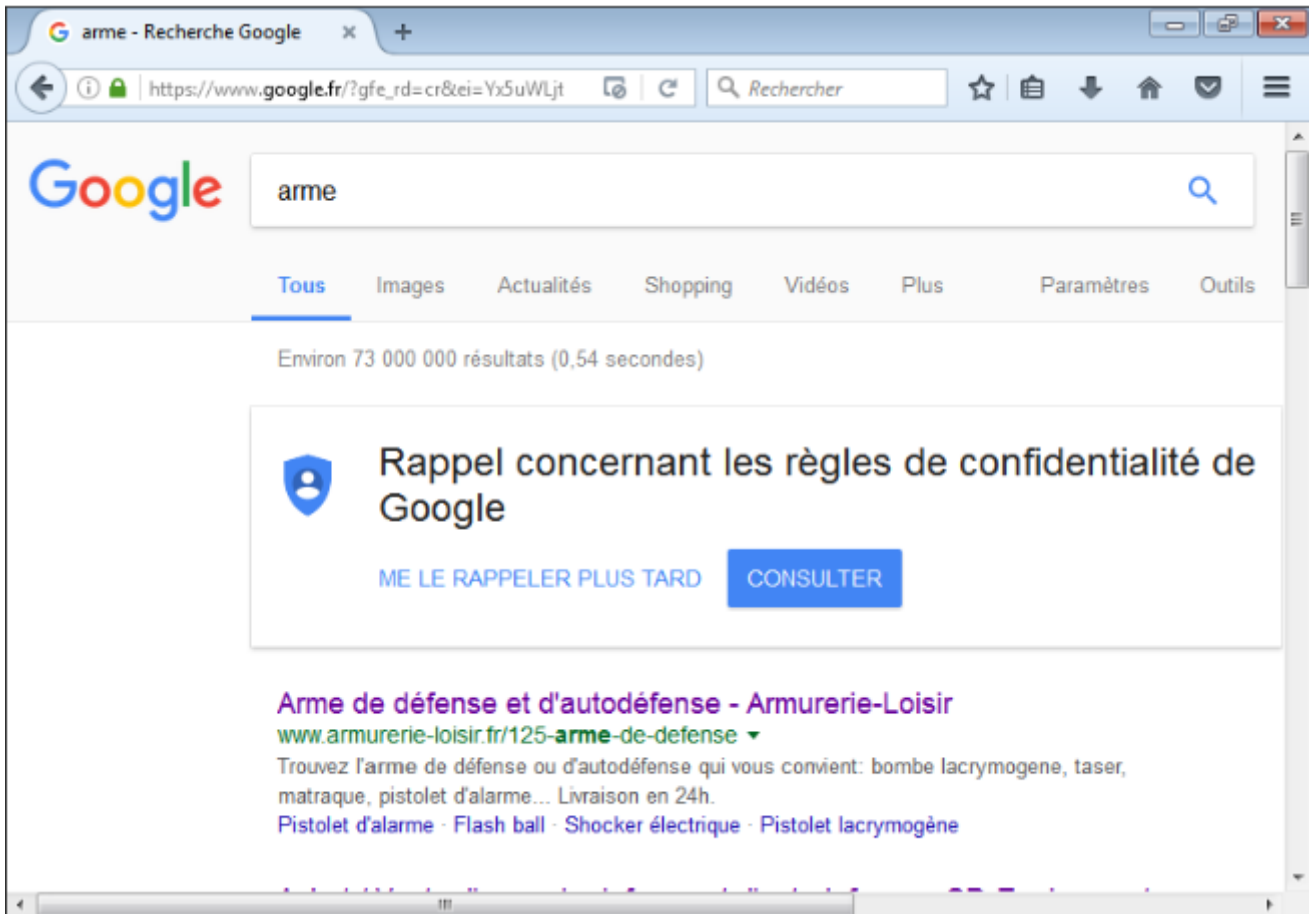
Pour tester on va se rendre sur un machine client et lancer internet, je suis automatiquement rediriger vers ma page d'authentification :



Après authentification je suis bien rediriger vers le site de redirection :



Ensuite je vais essayer d'accéder a un site de vente d'arme :



Je suis bien bloquer par "Squidguard"



From:

<https://wiki.virtit.fr/> - VirtIT

Permanent link:

https://wiki.virtit.fr/doku.php/kb:linux:pfSense:mise_en_place_d_un_portail_captif_pfsense

Last update: **2018/04/04 00:22**