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" :

vailable Packag	es Installed Package	\$		
Name	Category	Version	Description	
freeradius2	Services	1.6.19	A free implementation of the RADIUS protocol. Support: MySQL, PostgreSQL, LDAP, Kerberos. FreeRADIUS and FreeRADIUS2 settings are not compatible so don't use them together or try to update. On pfSense docs there is a how-to which could help you on porting users.	
			Package info	
squid	Services	4.3.10	High performance web proxy cache (2.7 legacy branch).	
			No package info, check the forum	pkg (x
squidGuard	Network Management	1.9.18	High performance web proxy URL filter. Works with both Squid (2.7 legacy branch) and Squid3 (3.4 branch) packages.	
			No package info, check the forum	(1999) (20
			Click package info for more details about SquidGuard package.	

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)

Logging opti	ions
Enable GUI log	Check this option to log the access to the Proxy Filter GUI.
Enable log	Image: Second
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.
Miscellaneou	IS
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 opt	ions
Blacklist	Check this option to enable blacklist. Do NOT enable this on NanoBSD installs!
Blacklist proxy	N Blacklist unload 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	Nttp://www.shallalist.de/Downloads/shallalist.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 Squ	idGuard: Blacklist page	?
General settings Comm	non ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync	
Blacklist Update	O % http://www.shallalist.de/Downloads/shallalist.tar.gz 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: 'whitelis	" - always pass;	deny - block;	'allow' - pass,	if not blocked.
-------------------	------------------	---------------	-----------------	-----------------

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

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 Apply 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 :

D R C I O I R

Services: Captive portal: Wifi

Captive portal(s) MAC Allowe	ed IP addresses Allowed Hostnames Vouchers File Manager
	Enable captive portal
Interfaces	WAN WANPRIVATEWIFI PUBLICWIFI
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 "Preauthentication redirect URL"

Pre-authentication redirect URL	https://www.google.fr 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	https://duckduckgo.com/ 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	Solution of the second
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 RADIUS s	erver
IP address	N 127.0.0.1 Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against
Port	No. 1812 Leave this field blank to use the default port (1812).
Shared secret	PISENSE Leave this field blank to not use a RADIUS shared secret (not recommended).
Secondary RADIUS	5 server
IP address	If you have a second RADIUS server, you can activate it by entering its IP address here.
Port	

(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 Settin	gs EAP SQ	L Certific	ates 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		e 🔉
Save								

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

2025/05/21 05:01	

General Configuration	
Client IP Address	No. 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	IPv4 T
Client Shortname	Scaptif.wifi Enter a short name for the client. This is generally the hostname of the NAS.
Client Shared Secret	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	UDP ▼ Enter the protocol the client uses. (Default: UDP)	
Client Type	other T Enter the NAS type of the client. This is used by checkrad.pl for simultaneous use checks. (Default: other)	
Require Message Authenticator	No ▼ RFC5080 requires Message-Authenticator in Access-Request. But older NAS (switches or accesspoints) do not include that. (Default: no)	
Max Connections	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	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	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	Enter any description you like for this client.	

Se rendre ensuite dans l'onglet Interface :

2

FreeRADIUS: Interfaces: Edit

eneral Configuration	
nterface IP Address	No. 127.0.0.1 Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)
Port	1812 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	Authentication T Enter the type of the listening interface. (Default: auth)
P Version	IPv4 ▼ 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: L	DAP	?	
Users MACs NAS /	Clients Interfaces Settings EAP SQL Certificates LDAP View config XMLRPC Sync		
ENABLE LDAP SUP	PORT - SERVER 1		
Enable LDAP For Authorization	✓ This enables LDAP in authorize section. The Idap module will set Auth-Type to LDAP if it has not already been set. (Default: und	checked)	
Enable LDAP For Authentication	✓ This enables LDAP in authenticate section. Note that this means "check plain-text password against the Idap database", which is a section of the section.	means that EAP v	won't

Configurer la liaison LDAP avec le Serveur AD :

General Configuratio	General Configuration - SERVER 1		
Server	No description. (Default: Idap.your.domain)		
Port	No description. (Default: 389)		
Identity	Scn=administrateur,cn=Users,dc=klyuch,dc=lan No description. (Default: cn=admin,o=My Org,c=UA)		
Password	No description. (Default: mypass)		
Basedn	No description (Default: o=My Org,c=UA)		
Filter	No description. (Default: (uid=%{%{Stripped-User-Name}:-%{User-Name}}))		
Base Filter	No description. (Default: (objectclass=radiusprofile))		
LDAP Connections Number	5 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)		
Timeout	Seconds to wait for LDAP query to finish. (Default: 4)		
Timelimit	Seconds the LDAP server has to process the query (server-side time limit). (Default: 3)		
Net Timeout	N 1 Seconds to wait for response of the server because of network failures. (Default: 1)		

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'acceder a un site de vente d'arme :

10/11

2025/05/21 05:01



Je suis bien bloquer par "Squidguard"

偷

☆自

 \equiv



G C

Q. Rechercher

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: 2018/04/03 22:22



←

ERREUR : L'URL demandée n'a ... 🛛 🗶

ERREUR

) (i) www.armurerie-loisir.fr/125-arme-de-defense

+

L'URL demandée n'a pu être chargée