

Mise en place d'un portail captif sécurisé avec pfSense et authentification RADIUS

À quoi ça sert :

- Sécuriser un réseau invité ou public en obligeant les utilisateurs à **s'authentifier** via une page de portail captif.
- Contrôler l'accès à Internet à travers des **droits d'accès** définis dans le serveur RADIUS.
- Mettre en place une **traçabilité** des connexions (logs).
- Créer une **infrastructure modulaire et sécurisée** pour l'accueil de visiteurs ou d'utilisateurs externes.

pfSense :

Routeur/firewall qui servira à isoler le réseau invité, activer le portail captif, attribuer les adresses IP via DHCP et rediriger les utilisateurs non authentifiés vers une page de connexion. Il jouera aussi le rôle de passerelle vers Internet.

Serveur RADIUS (FreeRADIUS sur Debian) :

Serveur d'authentification centralisée qui validera les identifiants des utilisateurs se connectant au portail captif. Il permettra également de gérer les droits d'accès au réseau.

Client Windows (poste de test utilisateur) :

Ordinateur client connecté au réseau invité, utilisé pour tester le comportement du portail captif et vérifier la connexion Internet après authentification.

- ```
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
```

Notre routeur virtuel est prêt.

Nous pouvons désormais nous rendre sur le web config de pfsense pour y configurer le portail captif.

Nous allons activer le portail captif afin de contrôler l'accès au réseau invité. Nous devons ensuite rédiger une description pour faciliter l'identification de cette configuration dans l'interface pfSense. Nous pouvons ainsi associer ce portail à une interface réseau spécifique pour y appliquer notre politique d'authentification RADIUS.

**Captive Portal Configuration**

**Enable**  Enable Captive Portal

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

**Interfaces**

Nous devons associer le portail captif à l'interface LAN pour filtrer les connexions sortantes. Nous configurons une limite d'une connexion par IP, ainsi qu'un délai d'inactivité de 5 minutes pour libérer les sessions inutilisées. Nous pouvons également définir des règles supplémentaires comme un quota de trafic ou un temps de connexion maximal si nécessaire.

**Enable**  Enable Captive Portal

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

**Interfaces**   
Select the interface(s) to enable for captive portal.

**Maximum concurrent connections**   
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.

**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).

**Traffic quota (Megabytes)**   
Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.

**Pass-through credits per MAC address.**   
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**  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.

Nous devons sélectionner "Authentication backend" puis choisir notre serveur RADIUS comme source d'authentification. Cela permet de forcer l'identification des utilisateurs via une base centralisée. Nous pouvons également activer la réauthentification périodique si nous souhaitons vérifier régulièrement la validité des sessions en cours.

**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.

---

**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.

Nous pouvons visualiser ici la zone de portail captif créée, associée à l'interface LAN. Nous avons nommé cette zone "invites\_zone" afin d'identifier clairement son usage. Nous devons nous assurer qu'elle est bien active et correctement configurée pour gérer l'accès des utilisateurs invités via RADIUS.

| Captive Portal Zones |            |                 |                                                                   |                                                                                                                                                                             |
|----------------------|------------|-----------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zone                 | Interfaces | Number of users | Description                                                       | Actions                                                                                                                                                                     |
| invites_zone         | LAN        | 0               | Portail captif pour le réseau invité avec authentification RADIUS |   |

On passe sur la machine Ubuntu qui servira à accueillir FreeRadius

Nous commençons par installer FreeRadius avec cette commande : `sudo apt install freeradius -y`

Nous devons nous assurer que le service FreeRADIUS est bien actif sur notre serveur Ubuntu. Ici, nous pouvons constater que le service est en cours d'exécution et prêt à traiter les requêtes d'authentification.

```
radius@radius-VirtualBox:~$ systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
 Loaded: loaded (/usr/lib/systemd/system/freeradius.service; enabled; preset: enabled)
 Active: active (running) since Mon 2025-04-07 05:17:48 CEST; 1min 26s ago
 Docs: man:radiusd(8)
 man:radiusd.conf(5)
 http://wiki.freeradius.org/
 http://networkradius.com/doc/
 Process: 1450 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited, status=0/SUCCESS)
 Main PID: 1460 (freeradius)
 Status: "Processing requests"
 Tasks: 6 (limit: 4609)
 Memory: 47.9M (max: 2.0G available: 1.9G peak: 48.2M)
 CPU: 137ms
 CGroup: /system.slice/freeradius.service
 └─1460 /usr/sbin/freeradius -f
```

Nous nous rendons ici

```
/etc/freeradius/3.0/clients.conf *
```

Nous devons déclarer l'adresse IP de pfSense comme client autorisé dans le fichier de configuration de FreeRADIUS. Nous y associons un secret partagé, nécessaire pour sécuriser les échanges d'authentification entre le serveur et pfSense.

```
#}
client pfsense {
 ipaddr = 192.168.1.1
 secret = xxxxxxxx
 shortname = pfSense
}
```

Nous devons ajouter manuellement les utilisateurs autorisés dans le fichier users de FreeRADIUS. Ici, nous créons l'utilisateur "ilyes" avec un mot de passe en clair "changeme", ce qui permet au portail captif de pfSense de valider les identifiants transmis par l'utilisateur.

```
Note that there is NO 'Fall-Through' attribute, so the user will not
be given any additional resources.

#lameuser Auth-Type := Reject
Reply-Message = "Your account has been disabled."

Deny access for a group of users.

Note that there is NO 'Fall-Through' attribute, so the user will not
be given any additional resources.
ilyes Cleartext-Password := "changeme"

#DEFAULT Group == "disabled", Auth-Type := Reject
Reply-Message = "Your account has been disabled."

This is a complete entry for "steve". Note that there is no Fall-Through
entry so that no DEFAULT entry will be used, and the user will NOT
get any attributes in addition to the ones listed here.

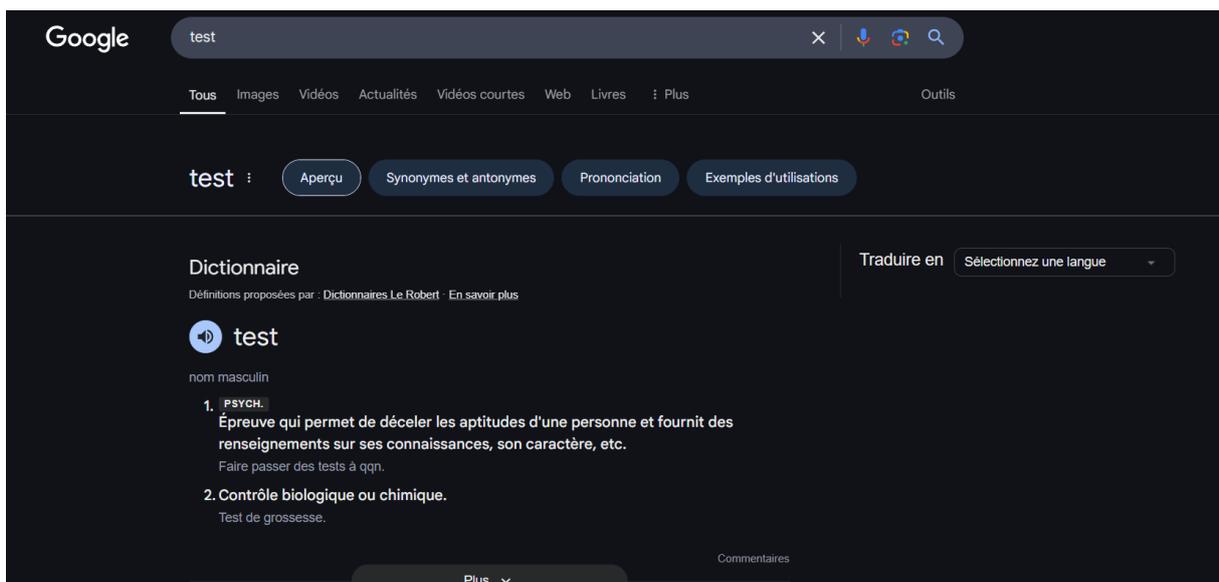
#steve Cleartext-Password := "testing"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 172.16.3.33,
Framed-IP-Netmask = 255.255.255.0,
Framed-Routing = Broadcast-Listen,
Framed-Filter-Id = "std.ppp",
Framed-MTU = 1500,
Framed-Compression = Van-Jacobson-TCP-IP
#
```

Nous allons maintenant nous rendre sur notre machine client et tenter de se connecter à un internet, cette machine tourne sous windows 10 et est présente dans le réseau de mon pfsense.

Nous pouvons maintenant accéder au portail captif depuis un poste client. Nous devons saisir un nom d'utilisateur et un mot de passe, qui seront vérifiés par le serveur FreeRADIUS.



Une fois l'utilisateur authentifié via le portail captif, nous pouvons accéder librement à Internet. Cette étape valide le bon fonctionnement du portail avec l'authentification RADIUS et confirme que la politique d'accès est bien appliquée sur le réseau invité.



Grâce à la mise en place d'un portail captif avec pfSense et une authentification centralisée via RADIUS, nous avons sécurisé l'accès au réseau invité. Cette solution permet de contrôler les connexions et de garantir que seuls les utilisateurs autorisés peuvent naviguer sur Internet. Nous avons validé l'ensemble du fonctionnement par des tests d'authentification et de connectivité, assurant ainsi une maîtrise complète de l'accès au réseau.