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) :

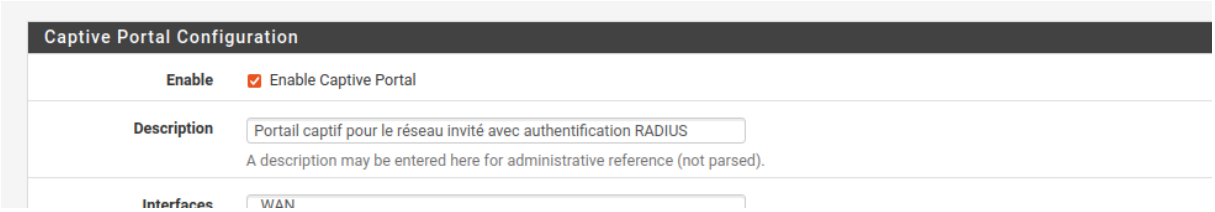
Ordinateur client connecté au réseau invité, utilisé pour tester le comportement du portail captif et vérifier la connexion Internet après authentification.

```
0) Logout (SSH only)                  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
```

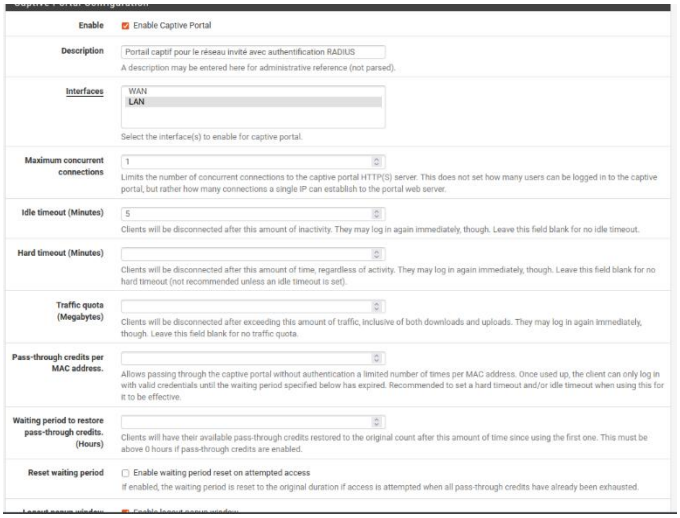
Notre routeur virtuel est prêt.

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

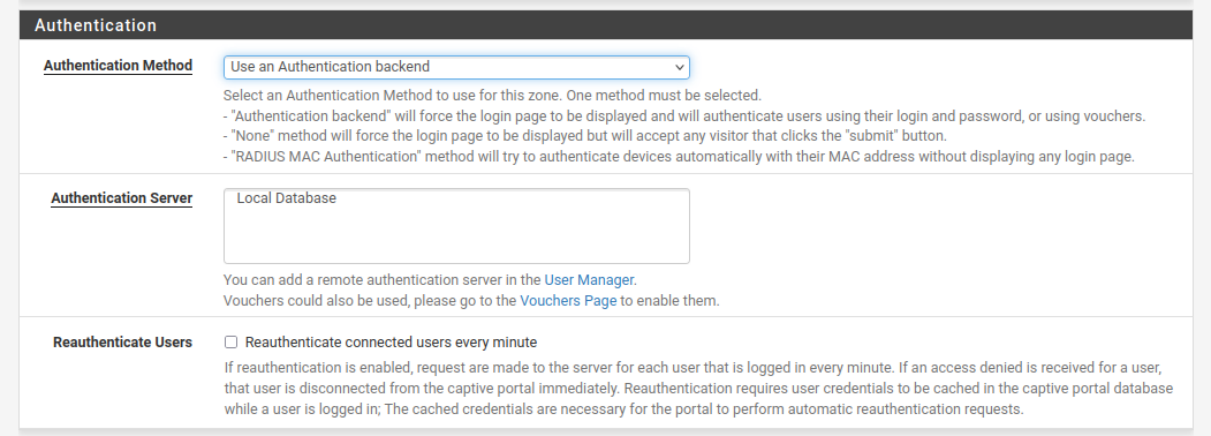
Nous allons activer le portail captif afin de contrôler l'accès au réseau invité. Nous devons ensuite rédiger une description pour faciliter l'identification de cette configuration dans l'interface pfSense. Nous pouvons ainsi associer ce portail à une interface réseau spécifique pour y appliquer notre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



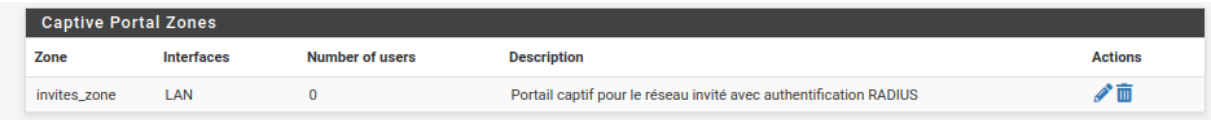
Nous devons associer le portail captif à l'interface LAN pour filtrer les connexions sortantes. Nous configurons une limite d'une connexion par IP, ainsi qu'un délai d'inactivité de 5 minutes pour libérer les sessions inutilisées. Nous pouvons également définir des règles supplémentaires comme un quota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



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.



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.



On passe sur la machine Unbuntu 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 *
on.
```

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 = xxxxxxxxx
    shortname = pfSense
}
```

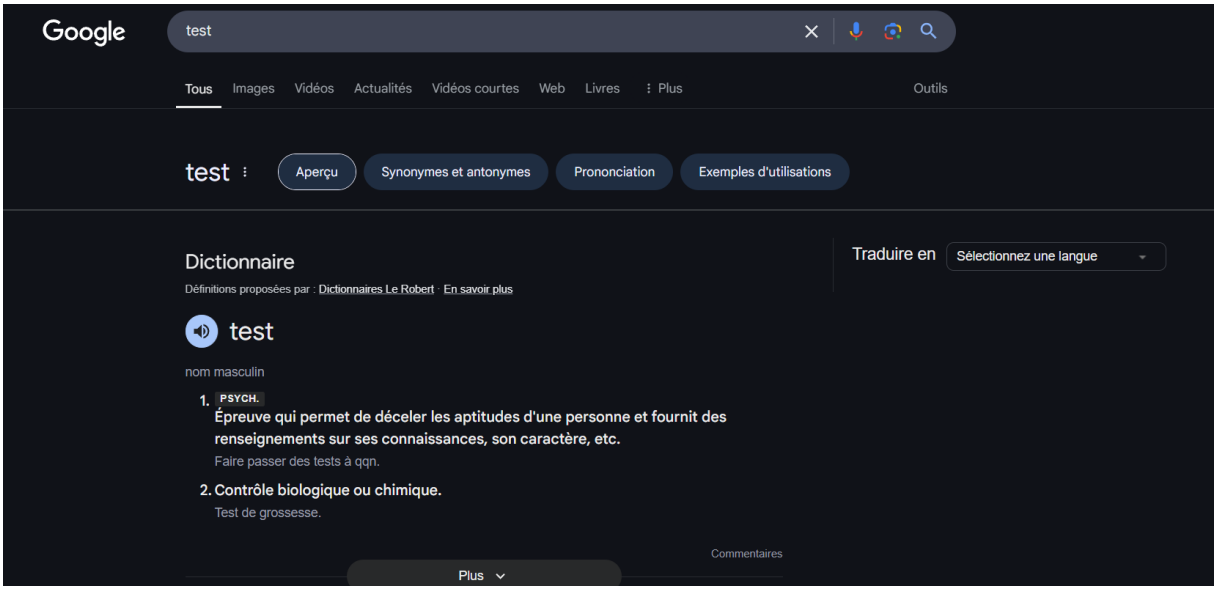
Nous devons ajouter manuellement les utilisateurs autorisés dans le fichier users de FreeRADIUS. Ici, nous créons l'utilisateur "ilyes" avec un mot de passe en clair "changeme", ce qui permet au portail captif de pfSense de valider les identifiants transmis par l'utilisateur.

```
# 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 := "[redacted]"
#
#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-Jacobsen-TCP-IP

#
```

Nous allons maintenant nous rendre sur notre machine client et tenter de se connecter a 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.