

Compte-rendu

Contexte :

La société Amine nous a sollicité afin de mettre à disposition un portail captif pour contrôler et gérer l'accès aux utilisateurs. Nous pourrons le configurer afin d'avoir plusieurs manières de s'authentifier et de simplifier cela pour les salariés.

Sommaire:

- 1 - Paramétrage de Pfsense
- 2 - Paramétrage des cartes réseaux
- 3 - Paramétrage du portail captifs
- 4 - Installation et paramétrage des services pour l'authentification RADIUS sur le portail avec l'Active Directory

Prérequis :

- Un routeur Pfsense
- Serveur Windows 2019
- Station Windows 10 Pro

Explication :

Tout d'abord, nous allons paramétrer le routeur Pfsense.

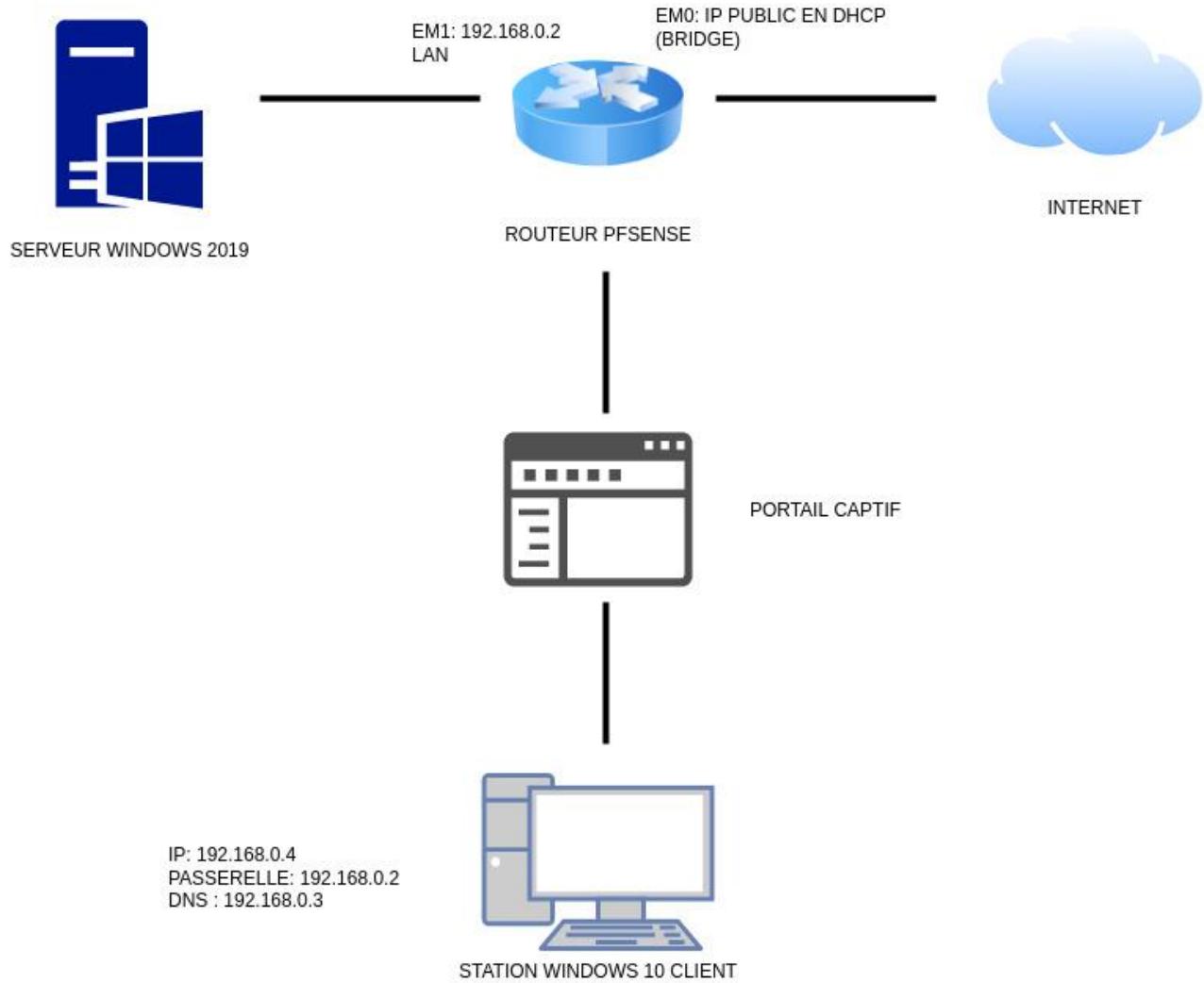
Ensuite, nous allons paramétrer les cartes réseaux de la station Windows 10 et du serveur Windows 2019.

Puis, on installera le service Active Directory et le service de stratégie et d'accès réseaux afin de pouvoir s'authentifier avec un compte de l'AD DS.

Enfin, nous allons mettre en place les différents moyens de s'authentifier sur le portail.

Schéma de la mission :

IP: 192.168.0.3
PASSERELLE: 192.168.0.2
DNS : 192.168.0.3



Tutoriel :

1- Paramétrage de Pfsense

On configure le routeur Pfsense avec deux interfaces réseaux, une interface sera en LAN et une autre en WAN.

Celle en LAN aura un seul sous réseau avec le serveur et la station WIndows puis le WAN permettra d'aller de se rediriger sur internet une fois que l'utilisateur à réussi à s'authentifier.

```
The IPv6 WAN address has been set to dhcp6

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 9a4bf9ee5fce6f350a39

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.107/24
                           v6/DHCP6: 2a04:cec2:29:5e73:20c:29ff:fef1:7415
/64
LAN (lan)      -> em1          -> v4: 192.168.0.2/24

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

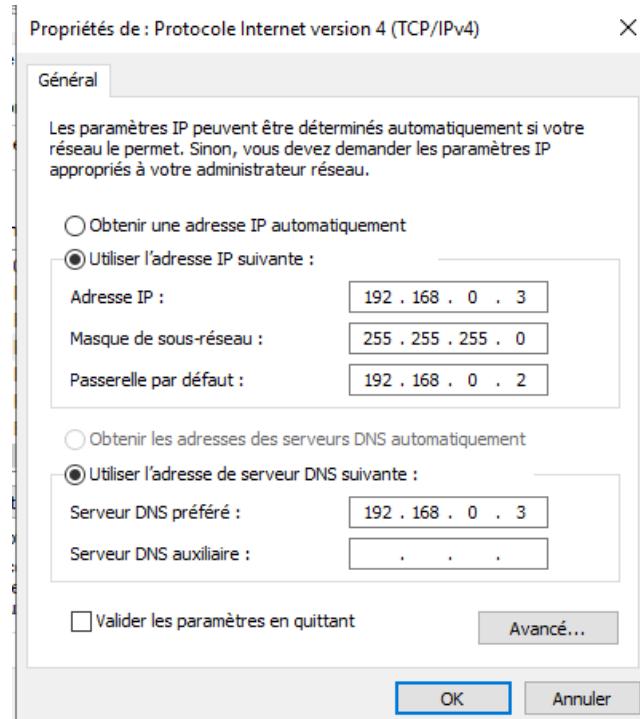
Enter an option: ■
```

Configuration des interfaces sur PFsense

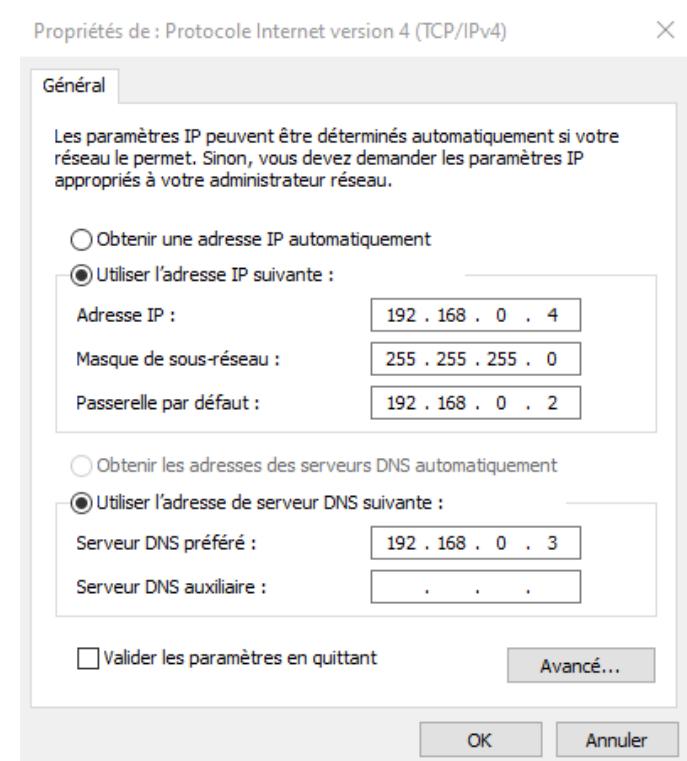
2- Paramétrage des cartes réseaux

On change l'ip du WIndows 10 et du Serveur Windows 10 pour les mettre dans le même sous réseau.

Configuration de l'interface réseau du serveur windows 10



Configuration de l'interface réseau du Poste client



The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

Alias IPv4 address / 32

The value in this field is used as a fixed alias IPv4 address by the DHCP client.

Reject leases from

To have the DHCP client reject offers from specific DHCP servers, enter their IP addresses here (separate multiple entries with a comma). This is useful for rejecting leases from cable modems that offer private IP addresses when they lose upstream sync.

Reserved Networks

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

On laisse passer le trafic allant du WAN vers notre LAN pour avoir internet pour nos utilisateurs lorsqu'ils ont réussi à s'authentifier sur le portail captif.

Protégez votre ordinateur avec le Pare-feu Windows Defender

Le Pare-feu Windows Defender a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.

Mettre à jour les paramètres du pare-feu

Le Pare-feu Windows Defender n'utilise pas les paramètres recommandés pour protéger votre ordinateur.

[Quels sont les paramètres recommandés ?](#)

 Utiliser les paramètres recommandés

 Réseaux avec domaine	Non connecté 
 Réseaux privés	Connecté 
Réseaux à domicile ou sur un lieu de travail, où vous faites confiance aux personnes et aux périphériques présents sur le réseau	
État du Pare-feu Windows Defender :	Désactivé
Connexions entrantes :	Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées
Réseaux privés actifs :	 Réseau 2
État de notification :	Ne pas m'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application
 Réseaux publics ou invités	Non connecté 

Désactiver le pare feu pour la station Windows 10 et le serveur windows 10

3- Paramétrage du portail captif

Le portail captif est un portail sécurisé qui consiste à demander à l'utilisateur ses identifiants pour pouvoir être reconnu et avoir accès au réseau.

On configure le portail sur Pfsense en l'activant sur l'interface Lan.

High Availability File Manager

Captive Portal Configuration

Enable

Enable Captive Portal

Description

Portail Captif

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

Interfaces

WAN

LAN

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

Maximum concurrent connections

1

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)

5

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

On personnalise une image et un logo pour le portail donc on active l'utilisation d'images.

Captive Portal Login Page

Display custom logo image Enable to use a custom uploaded logo image

Logo Image [Choisir un fichier](#) Apple-logo.png
Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, it can be of any image type: .png, .jpg, .svg **This image will not be stored in the config.** The default logo will be used if no custom image is present.

Display custom background image Enable to use a custom uploaded background image

Background Image [Choisir un fichier](#) d9iqgnm-13d1...21c3e674f.png
Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. **This image will not be stored in the config.** The default background image will be used if no custom background is present.

Terms and Conditions
Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out

Puis, on crée un utilisateur avec le droit d'accès à ce portail.

System / User Manager / Users

Users Groups Settings Authentication Servers

Users				
Username	Full name	Status	Groups	Actions
<input type="checkbox"/> Amine	• Amine	✓		
<input type="checkbox"/> admin	System Administrator	✓	admins	

Add **Delete**

Utilisateur “Amine” créé

Not member of Member of
[» Move to ‘Member of’ list](#) [« Move to ‘Not member of’ list](#)

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

Effective Privileges

Inherited from	Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.		
WebCfg - System: User Manager	Allow access to the ‘System: User Manager’ page. (admin privilege)		
WebCfg - Status: Captive Portal	Allow access to the ‘Status: Captive Portal’ page.		

Security notice: This user effectively has administrator-level access

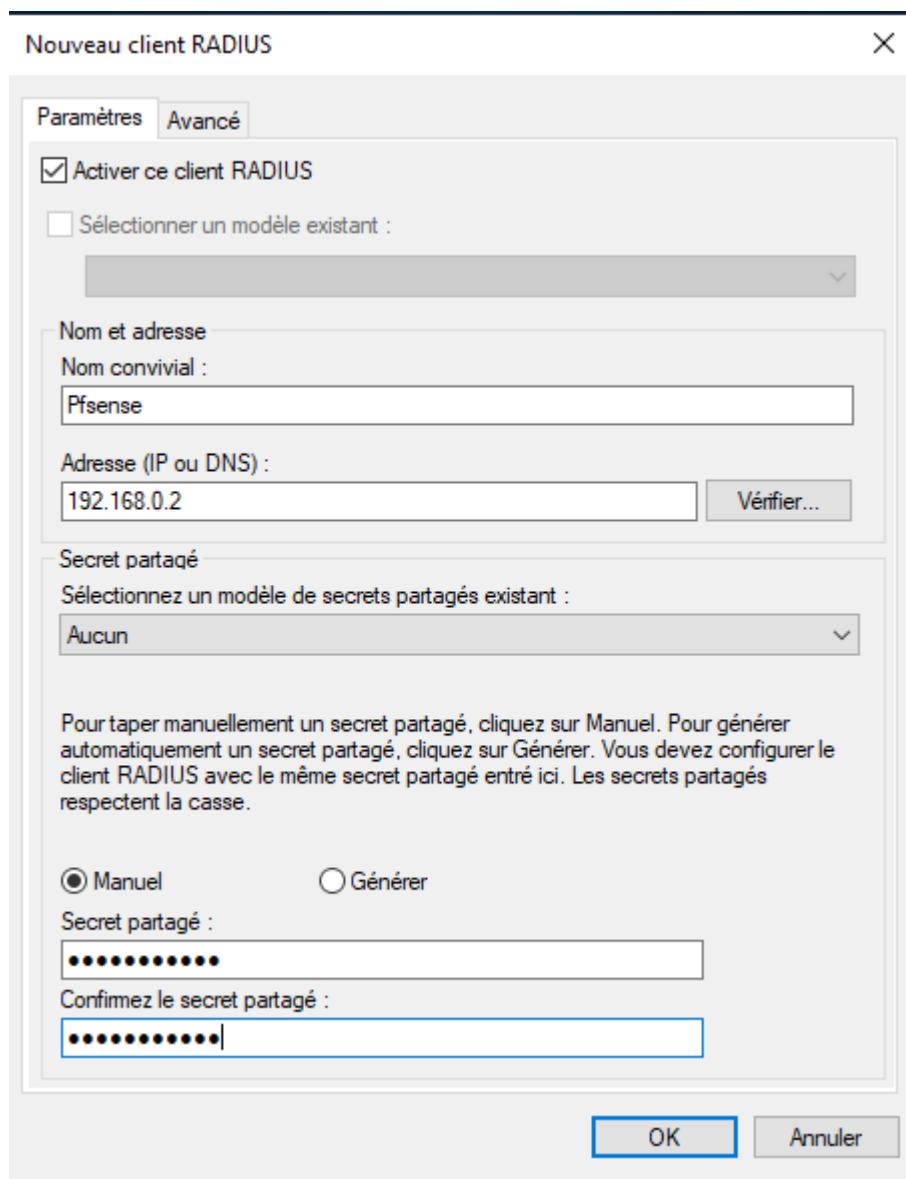
Add

Privilège accordé à Amine (voir membre connecté, gestion des utilisateurs et accès autorisé aux portail)

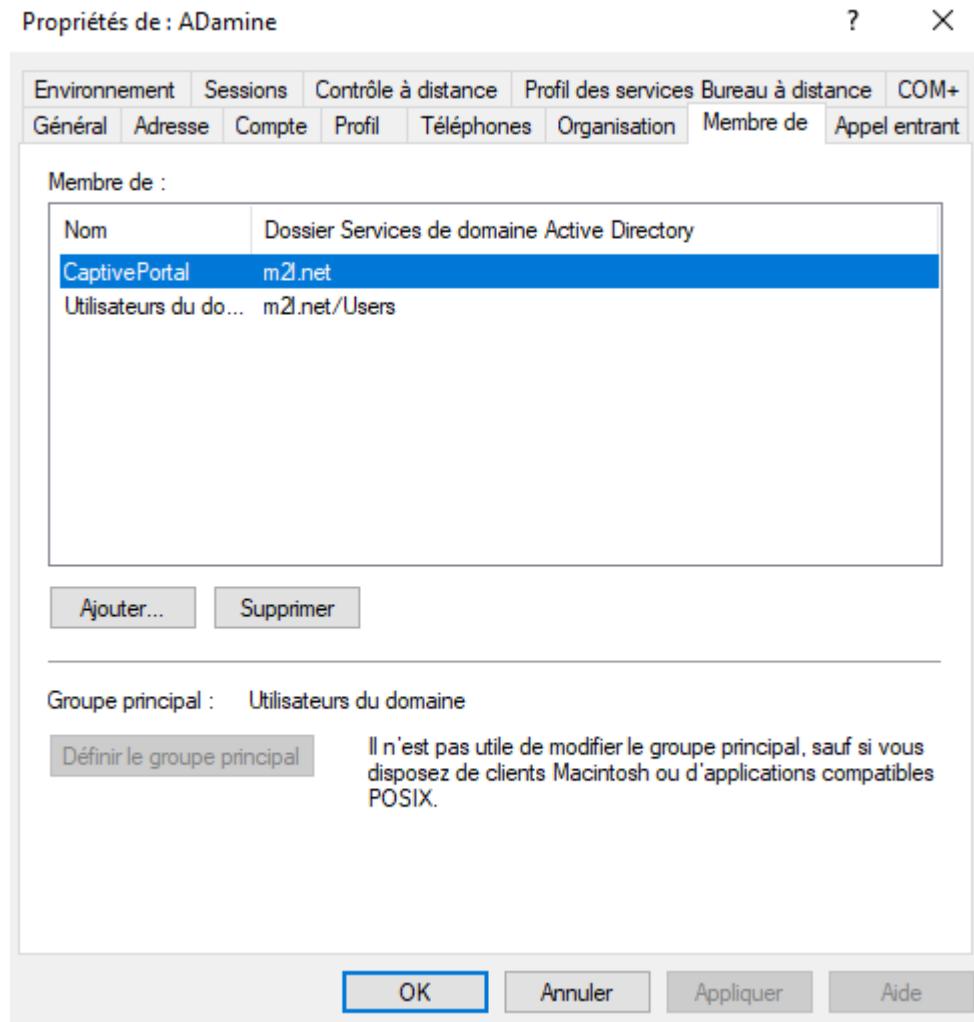
4- Installation et paramétrage des services pour l'authentification RADIUS sur le portail avec l'Active Directory

On installe les services Active Directory et service de stratégie et d'accès réseaux.

Le service stratégie et d'accès réseaux installera le protocole RADIUS qui permet de s'authentifier sur le portail captif grâce à une liaison avec le serveur Active Directory.



Paramétrage de RADIUS



Créé le groupe “CaptivePortal” avec l’utilisateur ADamine intégré

Propriétés de CaptivePortal

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur NPS utilise cette stratégie pour autoriser la connexion. Si la demande de connexion ne répond pas aux conditions, le serveur NPS ignore cette stratégie et enverra une autre stratégie supplémentaire si d'autres stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes d'utilisateurs	M2L\CaptivePortal

Description de la condition :

Condition d'authentification avec le groupe “CaptivePortal”

System / User Manager / Authentication Servers

Users Groups Settings Authentication Servers

Authentication Servers

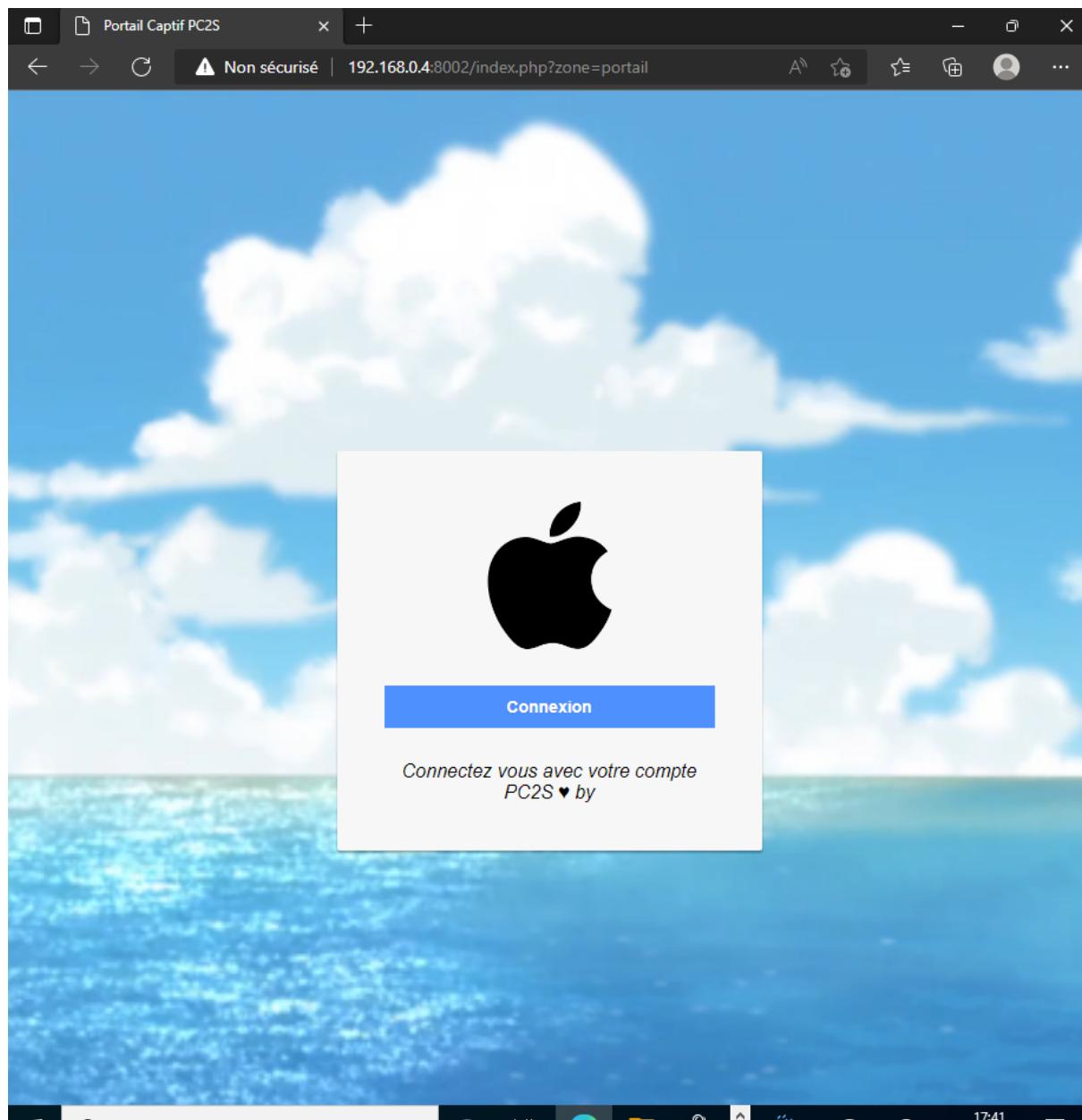
Server Name	Type	Host Name	Actions
CaptivePortal	RADIUS	192.168.0.3	
Local Database		pfSense	

Add

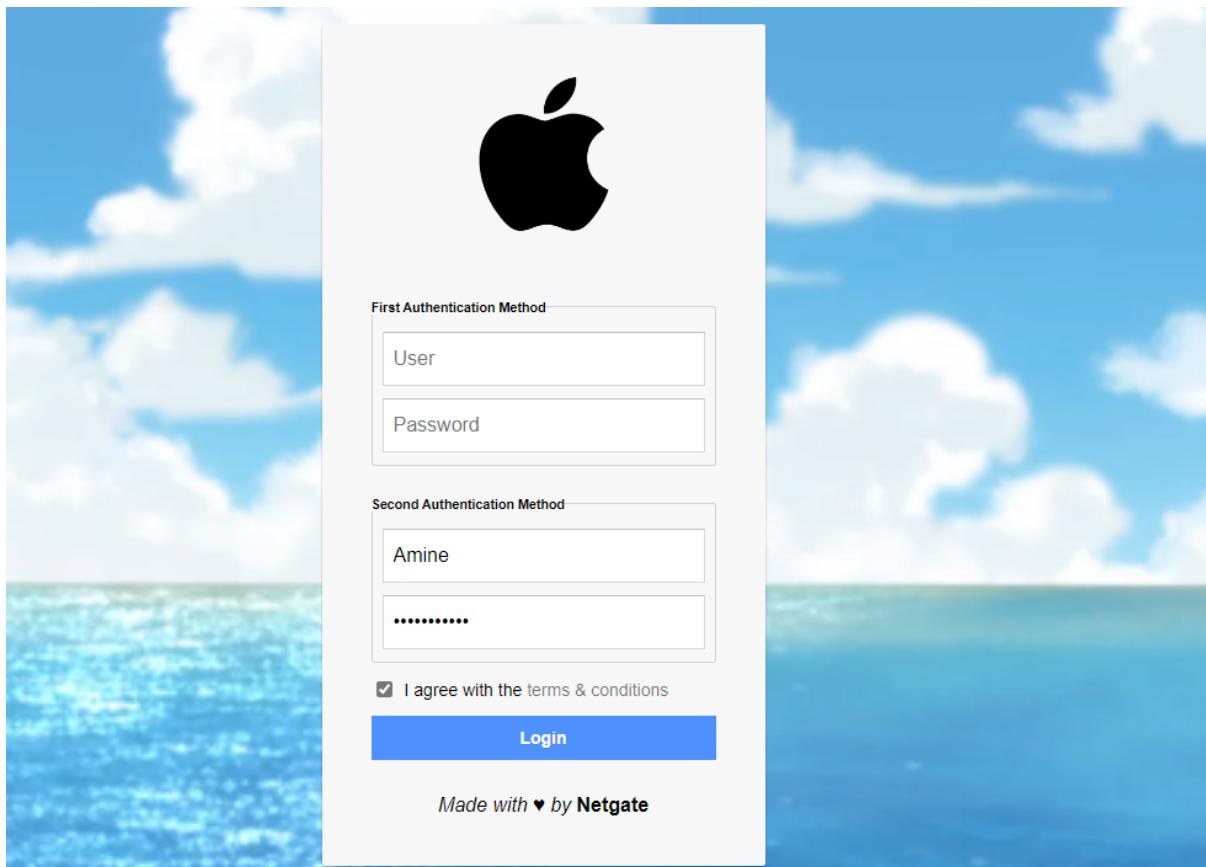
Faire une authentification Radius avec un lien entre PFsense et le serveur AD

Conclusion

On essaye de se connecter avec les trois modes d'authentifications (bouton connecter sans mot de passe, avec le mot de passe et avec authentification à l'aide de l'active directory)



Interface avec le bouton connexion



Interface avec le nom d'utilisateur et le mot de passe (en local)

Status / Captive Portal / CaptivePortal

Users Logged In (1)				
IP address	Username	Authentication method	Session start	Actions
192.168.0.4	Amine	Local Auth	09/09/2022 01:08:17	

[Show Last Activity](#) [Disconnect All Users](#)

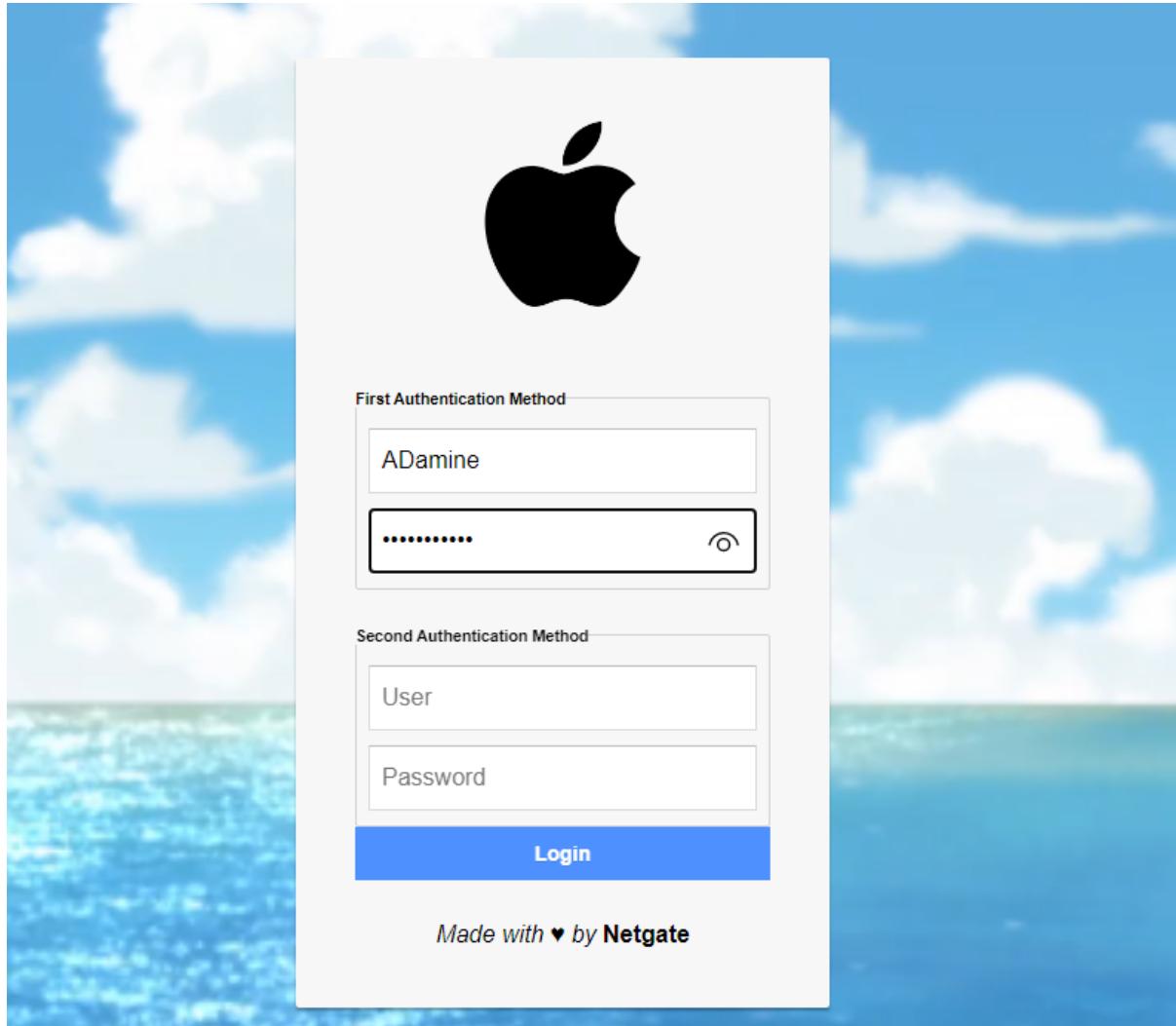
Utilisateur connecté avec le compte “Amine” en local

The screenshot shows the pfSense User Manager interface. At the top, there are tabs for 'System' (selected), 'Status', and 'Help'. Below the tabs, there are links for 'Logout (Amine)', 'User Manager', and 'Users'. The main area is titled 'Users' and contains a table with two rows. The columns are 'Username', 'Full name', 'Status', 'Groups', and 'Actions'. The first row has a checkbox, a user icon, 'Amine', 'Amine', a checkmark in the status column, and an empty 'Groups' column. The second row has a checkbox, an administrator icon, 'admin', 'System Administrator', a checkmark in the status column, and 'admins' in the 'Groups' column. At the bottom right of the table are 'Add' and 'Delete' buttons.

Test de l'utilisateur “Amine” avec ses privilèges

The screenshot shows the pfSense Diagnostics / Authentication test page. At the top, it says 'Diagnostics / Authentication'. Below that, a message states 'User ADamine authenticated successfully. This user is a member of groups:'. The main section is titled 'Authentication Test'. It has fields for 'Authentication Server' (set to 'CaptivePortal'), 'Username' (set to 'ADamine'), and 'Password' (represented by a series of dots). A 'Test' button is at the bottom. The entire page has a light green background.

Authentification Radius réussi avec l'utilisateur “ADamine”



Authentification Radius réussi avec l'utilisateur “ADamine”

The screenshot shows a web-based application for managing user sessions. At the top, there are navigation links: "Status / Captive Portal / CaptivePortal" and several icons for refresh, search, and help. Below this is a header bar with the text "Users Logged In (1)". A table follows, displaying a single row of data:

IP address	Username	Authentication method	Session start	Actions
192.168.0.4	ADamine	radius	09/09/2022 00:53:39	

At the bottom of the table are two buttons: "Show Last Activity" and "Disconnect All Users".

On remarque que l'utilisateur ADamine de l'active Directory est bien connecté.

Les trois manières de s'authentifier de façon sécurisée permettent bien à l'utilisateur de pouvoir se connecter et de se rediriger vers une autre page selon la configuration.