

Epreuve E4

Intitule de la mission:

L'école INSTA m'a fait part de leur souhait de mettre en place un portail captif pour ses utilisateurs d'ici la rentrée de septembre pour l'année 2023-2024, en me donnant la solution pfSense.

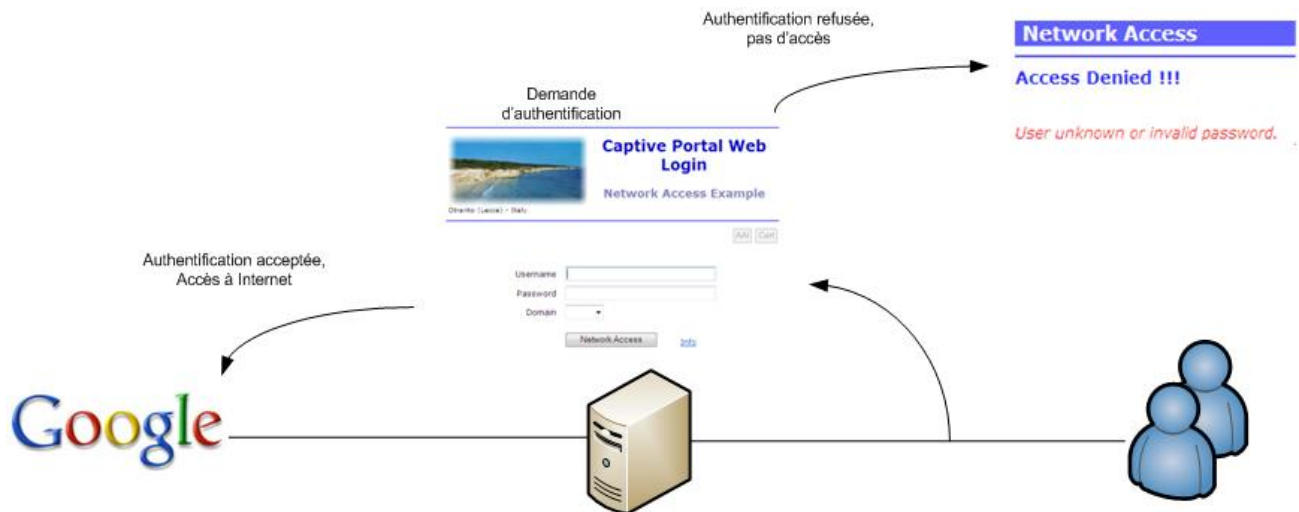
Prérequis sous VMWare Workstation Pro :

1. pfSense
2. 1 PC

Présentation :

La distribution pfSense est une solution ayant pour but la mise en place de routeur/pare-feu basée sur l'OS FreeBSD. Sa souplesse de configuration et d'utilisation facilite son intégration dans tous les systèmes d'information, tout en respectant les exigences de la politique de sécurité en vigueur.

Elle nous propose la configuration d'un portail captif sur ses interfaces. Un portail captif est une page web d'authentification qui s'affichera sur le navigateur des clients qui souhaitent aller sur Internet.



Le portail captif offre donc un contrôle et une restriction de l'utilisation de l'accès Internet.

Début de la mission :

1. Installation et création de la VM pfSense

Création d'une machine virtuelle sur VMWare workstation en respectant les paramètres suivants :

OS: pfSense

RAM: 2Go

SSD: 20 Go

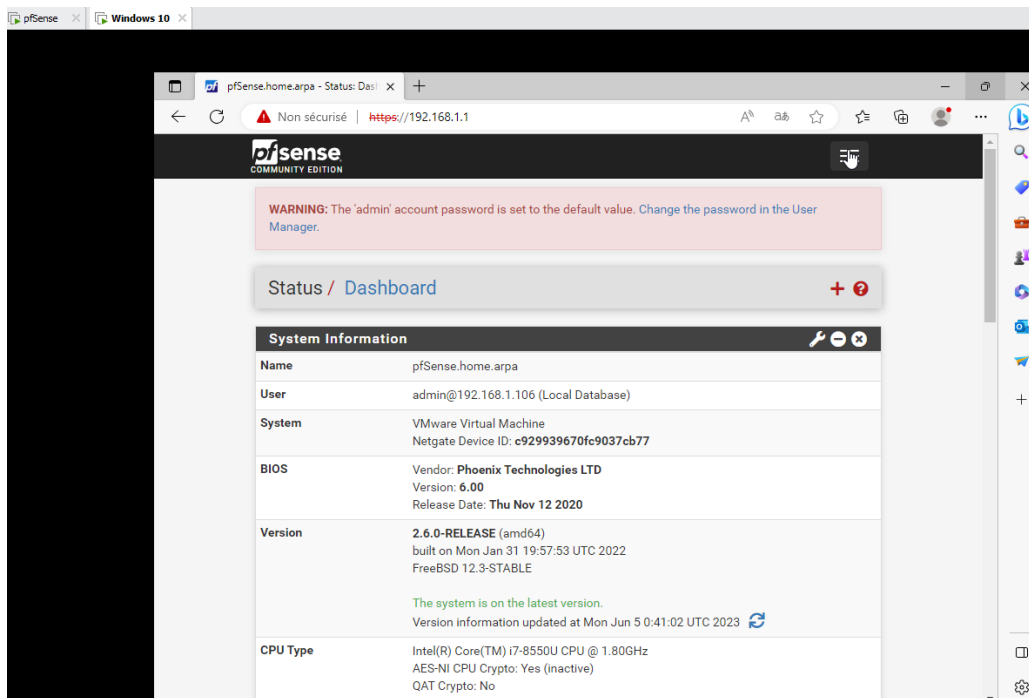
Notre pfSense est équipé de 2 cartes réseaux, la première en NAT pour qu'elle récupère le réseau dans notre PC physique pour avoir accès à internet. Et la deuxième carte sera en LAN Segment pour que notre pfSense soit connecté à notre réseau local, où se trouve notre machine cliente pour nos tests.

2. Création d'une VM cliente pour réaliser nos tests

La machine cliente s'agit d'un poste client équipé d'un Windows 10

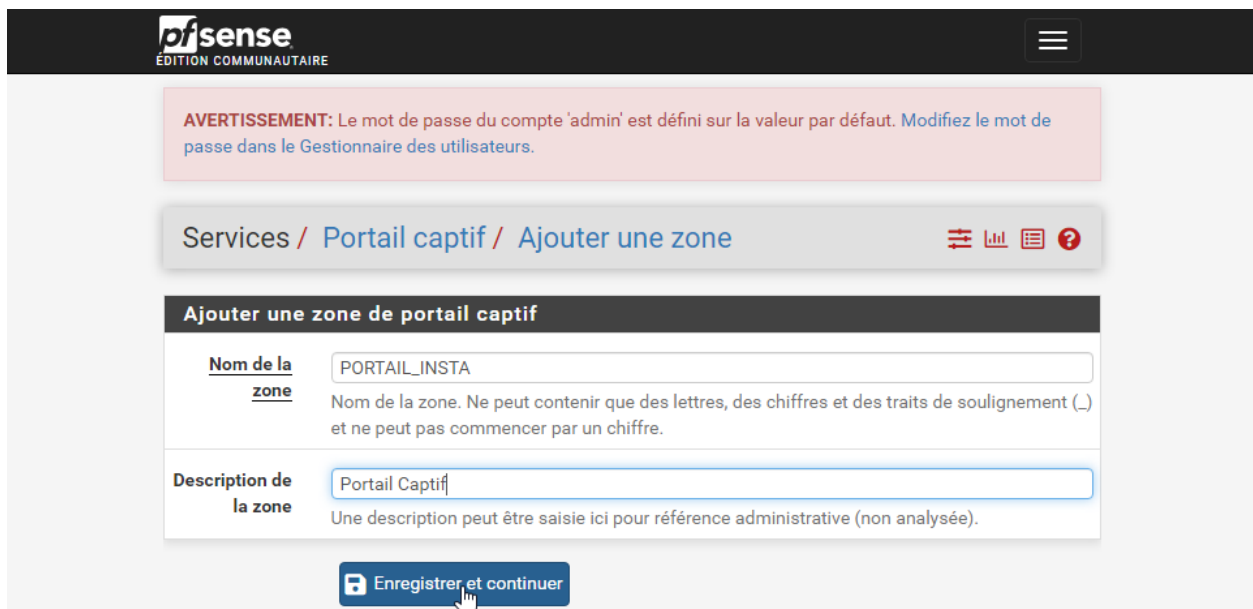
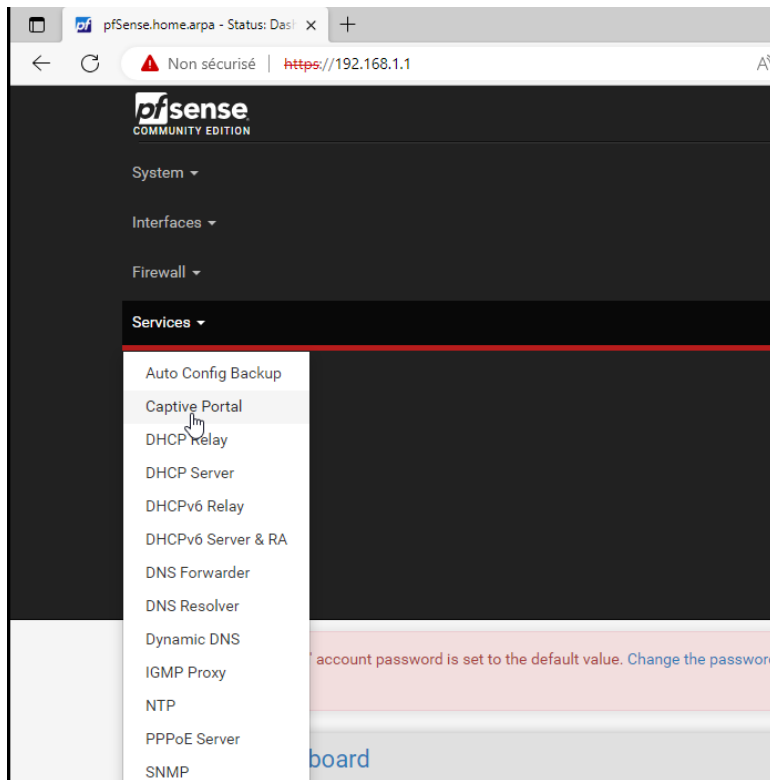
3. Installation du service

A partir de notre machine cliente, on va dans le navigateur pour accéder à l'interface graphique de notre pfSense.



MAFUTA MUKENDI HONORE
BTS SIO option SISR promo 234

Allez dans l'onglet Portail Captif pour le configurer



Configuration du portail captif	
Activer	<input checked="" type="checkbox"/> Activer le portail captif
Description	<input type="text" value="Portail Captif"/> Une description peut être saisie ici pour référence administrative (non analysée).
Interfaces	<div style="border: 1px solid #ccc; padding: 2px;"><input type="text" value="WAN"/> <input checked="" type="checkbox"/> LAN</div> Sélectionnez la ou les interfaces à activer pour le portail captif.
Nombre maximal de connexions simultanées	<input type="text" value="1"/> Limite le nombre de connexions simultanées au serveur HTTP(S) du portail captif. Cela ne définit pas le nombre d'utilisateurs pouvant être connectés au portail captif, mais plutôt le nombre de connexions qu'une seule adresse IP peut établir au serveur Web du portail.
Délai d'inactivité (minutes)	<input type="text" value="5"/> Les clients seront déconnectés après cette période d'inactivité. Cependant, ils peuvent se reconnecter immédiatement. Laissez ce champ vide sans délai d'inactivité.
Délai d'attente difficile (minutes)	<input type="text" value="300"/> Les clients seront déconnectés après ce laps de temps, quelle que soit leur activité. Cependant, ils peuvent se reconnecter immédiatement. Laissez ce champ vide sans délai d'expiration (non recommandé sauf si un délai d'inactivité est défini).
Fenêtre contextuelle de déconnexion	<input checked="" type="checkbox"/> Activer la fenêtre contextuelle de déconnexion Si cette option est activée, une fenêtre contextuelle apparaîtra lorsque les clients seront autorisés à passer par le portail captif. Cela permet aux clients de se déconnecter explicitement avant que le délai d'inactivité ou d'expiration difficile ne se produise.
URL de redirection de pré-authentification	<input type="text" value="https://www.google.fr"/> Définissez une URL de redirection par défaut. Les visiteurs seront redirigés vers cette URL après authentification uniquement si le portail captif ne sait pas où les rediriger. Ce champ sera accessible via la variable \$PORTAL_REDURL\$ dans les pages HTML de captiveportal.
Après l'authentification URL de redirection	<input type="text" value="https://www.insta.fr"/> Définissez une URL de redirection forcée. Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont initialement essayé d'accéder après s'être authentifiés.
URL de redirection d'adresse MAC bloquée	<input type="text"/> Les adresses MAC bloquées seront redirigées vers cette URL lors de la tentative d'accès.
Conserver la base de données des utilisateurs	<input type="checkbox"/> Préserver les utilisateurs connectés lors du redémarrage Si cette option est activée, les utilisateurs connectés ne seront pas déconnectés lors d'un redémarrage pfSense.
Connexions utilisateur simultanées	<input type="text" value="Handicapé"/> Désactivé : N'autorisez pas les connexions simultanées par nom d'utilisateur ou bon. Multiple : Aucune restriction quant au nombre de connexions par nom d'utilisateur ou bon ne sera appliquée. Dernière connexion : Seule la connexion la plus récente par nom d'utilisateur ou bon sera accordée. Les connexions précédentes seront déconnectées.

Filtrage MAC Désactiver le filtrage MAC

Si cette option est activée, aucune tentative ne sera faite pour s'assurer que l'adresse MAC des clients reste la même lorsqu'ils sont connectés. Ceci est nécessaire lorsque l'adresse MAC du client ne peut pas être déterminée (généralement parce qu'il existe des routeurs entre pfSense et les clients). Si cette option est activée, l'authentification RADIUS MAC ne peut pas être utilisée.

Page de connexion au portail captif

Afficher une image de logo personnalisée Activer l'utilisation d'un logo téléchargé personnalisé

Logo Image insta.jpg

Ajoutez un logo à utiliser dans l'écran de connexion au portail par défaut. Le fichier sera renommé captiveportal-logo.* L'image sera redimensionnée pour tenir dans la zone donnée, il peut être de n'importe quel type d'image: .png, .jpg, .svg **Cette image ne sera pas stockée dans la configuration.** Le logo par défaut sera utilisé si aucune image personnalisée n'est présente.

Afficher une image d'arrière-plan personnalisée Activer l'utilisation d'une image d'arrière-plan téléchargée personnalisée

Image d'arrière-plan R.jfif

Ajoutez une image d'arrière-plan à utiliser dans l'écran de connexion au portail par défaut. Le fichier sera renommé captiveportal-background.* L'image d'arrière-plan remplira l'écran. **Cette image ne sera pas stockée dans la configuration.** L'image d'arrière-plan par défaut sera utilisée si aucun arrière-plan personnalisé n'est présent.

Authentification

Méthode d'authentification

Sélectionnez une méthode d'authentification à utiliser pour cette zone. Une méthode doit être sélectionnée.

- « Authentication backend » forcera l'affichage de la page de connexion et authentifiera les utilisateurs à l'aide de leur identifiant et de leur mot de passe, ou à l'aide de bons.
- La méthode « Aucun » forcera l'affichage de la page de connexion mais acceptera tout visiteur qui clique sur le bouton « soumettre ».
- La méthode « RADIUS MAC Authentication » tentera d'authentifier automatiquement les appareils avec leur adresse MAC sans afficher de page de connexion.

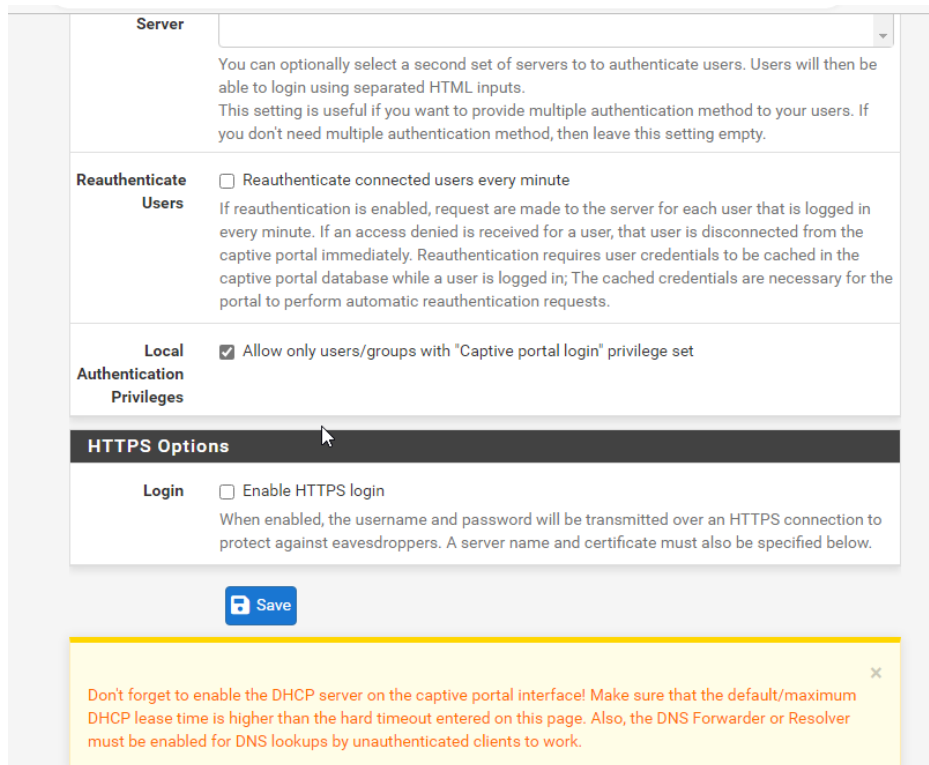
Serveur d'authentification

Vous pouvez ajouter un serveur d'authentification distant dans le [Gestionnaire des utilisateurs](#). Les bons peuvent également être utilisés, veuillez vous rendre sur la [page des bons](#) pour les activer.

Serveur d'authentification secondaire

Vous pouvez éventuellement sélectionner un deuxième ensemble de serveurs pour authentifier les utilisateurs. Les utilisateurs pourront alors se connecter à l'aide d'entrées HTML séparées.

Ce paramètre est utile si vous souhaitez fournir plusieurs méthodes d'authentification à vos utilisateurs. Si vous n'avez pas besoin de plusieurs méthodes d'authentification, laissez ce paramètre vide.



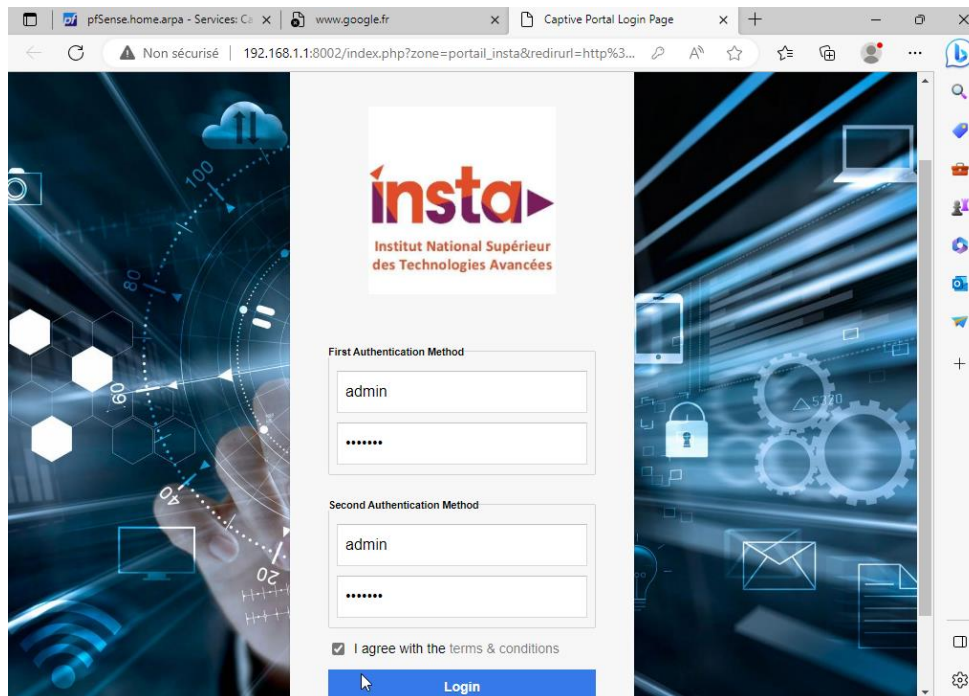
The screenshot shows the configuration interface for a captive portal. It includes several sections:

- Server:** A dropdown menu and explanatory text: "You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty."
- Reauthenticate Users:** A checkbox for "Reauthenticate connected users every minute" (unchecked). Text below: "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."
- Local Authentication Privileges:** A checked checkbox for "Allow only users/groups with 'Captive portal login' privilege set".
- HTTPS Options:** A section header.
- Login:** A checkbox for "Enable HTTPS login" (unchecked). Text below: "When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below."

A blue "Save" button is located below the configuration options. At the bottom, a yellow warning box contains the text: "Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work."

Et nous aurons accès à notre portail captif après les configurations ci-dessus.

Voici l'extrait:



The screenshot shows a web browser displaying the captive portal login page. The page features the logo for "insta Institut National Supérieur des Technologies Avancées". The login form includes:

- First Authentication Method:** Username field with "admin" and a password field with "*****".
- Second Authentication Method:** Username field with "admin" and a password field with "*****".
- A checked checkbox for "I agree with the terms & conditions".
- A blue "Login" button.

The browser's address bar shows the URL: "192.168.1.1:8002/index.php?zone=portail_insta&redirurl=http%3...". The page is marked as "Non sécurisé" (Not secure).