Ayoub Belbachir

Cours : BLOC 1
Professeur : M. VERSCUEREN
Date : 18/05/2021

Compte rendu Portail captif

Sommaire

Ayoub Belbachir

Mise en Contexte

Pfsense est un pare-feu (pare-feu) open source basée sur le système d'exploitation FreeBSD, Mise en place du firewall pour une protection optimale contre les malwares ou d'autres appareils qui partagent la même connexion et peuvent contaminer le réseau, nous permet de configurer l'accès réseaux, dans ce contexte nous mettrons en place un portail captif qui vas nous permettre de forcer les clients HTTP du réseau OPT1 à afficher une page web spécifique qui permettra ou non l'accès à internet

Prérequis :

Un ordinateur performant (sous Windows de préférence) avec 100GO de place disponible, 6 Go de RAM ou plus, un processeur cadencer à 3,5 GHz ou plus.

L'ISO officielle de Pfsense (architecture amd64, on cherche à l'émuler pas à l'installer sur une Appliance netgate) ainsi que l'iso officielle de Windows 10 (x64 bits)

Virtual Box, ainsi que les VM suivante :

Windows 10 (machine cliente OPT1)

- Une RAM de 2 Go ou plus
- Un espace disque disponible de 40 Go
- 1 gigahertz (GHz) ou plus rapide

Ubuntu Server 20.04 LTS (LDAP) :

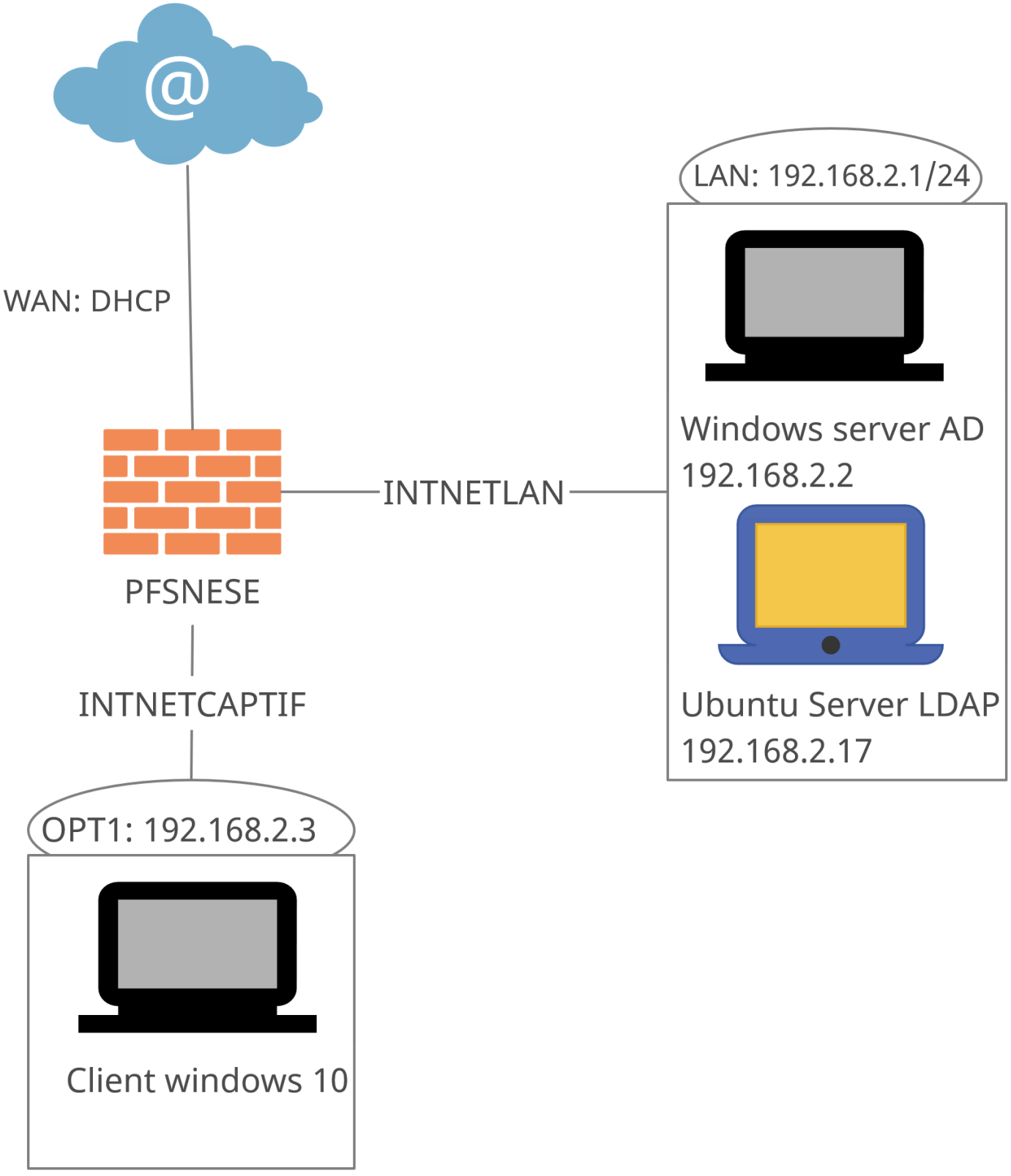
- 1 GHz processeur ou plus
- 10 Go d'espace libre sur le disque dur
- 1.5 Go de mémoire RAM
- LDAP DN=dc=ultrasamo,dc=com

Windows server (Active directory)

- Une RAM de 2 Go ou plus
- Un espace disque disponible de 40 Go
- 1,5 gigahertz (GHz) ou plus rapide
- Domain=samodigi.lan
- NetBIOS=samo

Ayoub Belbachir

Diagramme



Ayoub Belbachir

Installation de pfsense et de Windows server

Tutorial:

Dans VirtualBox Création du nouvel environnement ; attribution du nom “Pfsense”, type “BSD[1]”, Version FreeBSD (64-bits). (Cette étape serre à renseigner à Virtual box le type de noyaux et l’architecture de notre OS, afin de crée un environnement fonctionnel à notre os)

Allouer de la mémoire vive à la machine virtuelle (1,5go selon vos préférences), création d’un disque dur virtuel (8go) en VDI (le VDI est le format natif de VirtualBox dans ce contexte nous n’avons pas besoin d’utiliser cette VM avec d’autres logiciel de verticalisation.)

Insertion de l’ISO de Pfsense ; aller dans configuration > Stockage > Pfsense > clique sur “vide ” > > “Choose a disk file ”> puis sélectionner l’iso Pfsense télécharger précédemment.

Configurer une 2éme carte réseau ; aller dans configuration > Réseau > Adapter 2 > cocher la case “Activer l’interface réseau”, mode d’accès réseau en réseau interne à nom écrive intnetlan, cliquer sur avancer mode de promiscuité en “Allow VMs” et configurer la premier carte réseau en mode d’accès réseau en réseau “NAT” (Cette étape nous permet de permettre au V.M de communiquer entre elle).

Configurer une 3éme carte réseau(opt1) : aller dans configuration > Réseau > Adapter 3 > cocher la case “Activer l’interface réseau”, mode d’accès réseau en réseau interne à nom écrive intnetcaptif, cliquer sur avancer sélectionner un type d’interface diffèrent de celui d’adaptateur 2 si possible, mode de promiscuité en “Allow VMs”

Création d’un nouvel environnement ; attribution du nom “Windows Server” Virtual Box vas lui-même assigner automatiquement un type “Microsoft Windows” ainsi que la version “Windows 2016 (64-bit)” dans le cas contraire faite le vous-même Allouer de la mémoire vive à la machine virtuelle (3go selon vos préférences et votre matériel), création d’un disque dur virtuel (50go) en VDI. Configurer la 1e carte réseau en mode d’accès réseau en réseau interne et changer le nom en “intnetlan”,

Lancer la V.M Pfsense, la navigation de l’installation se fait à l’aide des flèches du clavier, de la touche tabulation, d’espace pour cocher/décocher et entrer pour valider.

Accepter des droits d’auteur, sélectionner Install, sélectionner votre type de clavier, type de partition UFS (ce type de partition et propre à Unix sa particularité est qu’il crée plusieurs parties dont une pour grub (la partions boot d’amorçage). Ne redémarrer pas ouvrer Shell et taper la commande “Init 0” pour éteindre proprement votre machine, retiré ensuite l’iso (dans configuration > stockage) afin que votre machine ne s’amorce pas sur le CD indéfiniment.

Lacer la V.M Windows 10 faite une installation personnaliser en sélection la partions cliquer sur nouveau et suivent une fois l’installation terminer retirer le cd.

[2] Berkeley Software Distribution dérivé d’Unix

Ayoub Belbachir

Démarrer la V.M Windows 10, Lors du premier démarrage nous allons renseigner notre pays, notre type de clavier (qwerty pour moi), un nom d'utilisateur et nous connecter au wifi nous allons ensuite mettre ajours les driver pour une meilleur stabilité et optimisation de la machine. Une foi terminer la machine est prêt à l'utilisation. (Windows nous oblige à renseigner ou créé une adresse Outlook pour le bypass il suffit de désactiver le wifi et de passer l'étape).

On sait que l'interface n°1 sera WAN celle qui est connectée au wifi. L'interface n°2 sera la LAN en réseau interne et qui l'administrateur de mon Pfsense Windows 10 ainsi que OPT1 pour l'interface qui servira de portail captif. Lacer la V.M Pfsense

Premier démarrage de la VM Pfsense, Paramétrage de la vlan laisser par défaut taper "n" pour la WAN taper " em0" pour le LAN taper "le0" et pour opt1 taper em2 ensuite taper "y" Pfsense va démarrer différent service dons le pare-feu un DNS et un service DHCP, paramétrage de l'adresse IP du LAN entré l'option "2" puis l'option "2"

Entrer l'adresse ip de votre choix (192.168.2.1) entrer ensuite le sous réseau qui lui correspond le CIDR (24) appuyer ensuite 2 fois sur entrer pour passer les étapes activer le DHCP, définir la plage d'adressage IP du DHCP (192.168.2.10 à 192.168.2.110), activer ensuite le protocole de configuration web

Paramétrage de l'adresse IP de opt1 entré l'option "2" puis l'option "3"

Entrer l'adresse ip de votre choix (192.168.4.1) entrer ensuite le sous réseau qui lui correspond le CIDR (24) appuyer ensuite 2 fois sur entrer pour passer les étapes activer le DHCP, définir la plage d'adressage IP du DHCP (192.168.4.5 à 192.168.4.45), activer ensuite le protocole de configuration web

Rendez-vous sur votre V.M Windows server ouvrir le cmd taper les commandes suivantes ; "ipconfig /revise" puis" ipconfig /renew" Ouvre un navigateur (Firefox de préférence) entrer l'adresse ip que vous avez attribuer à votre Lan (192.168.2.1) connecter vous a l'interface web de Pfsense (utilisateur : admin, mot de passe : pfsense) saisir le DNS public de google 8.8.8.8 et 8.8.4.4, sélectionner le fuseau horaire (Europe paris), changer le mot de passe par défaut. Vérifier les maj. Ajouter le widget trafic graphe pour voir si pfsense détecte la fluctuation de donner entrant et sortant de notre V.M Windows, dans Dashboard appuyer sur l'Icon + et cliquer sur "trafic graphe".

Lancer un test de connexion sur Nperf on peut observer que la courbe de débit montant et descendent fluctue

Enfin ajouter un outil de gestion de disque de VM à Pfsense aller dans "System" > "Package Manager" > " Available Package" puis chercher "Open-VM-Tools" cliquer sur l'icône 

Dernière vérification sur le cmd de votre V.M pinger google.com pour vérifier notre connexion internet ; "ping goole.com"

Ayoub Belbachir

Mise en place du portail captif sans authentification

Sur notre navigateur dans le WebUI de Pfsense

Firewall>Rules> opt1 add

Action > pass

Interface OPT1

Protocol any source opt1 net cliquez sur Save,

Cette règle nous permet de donner l'accès internet à opt1

Allez dans service puis cliquer sur portail captif

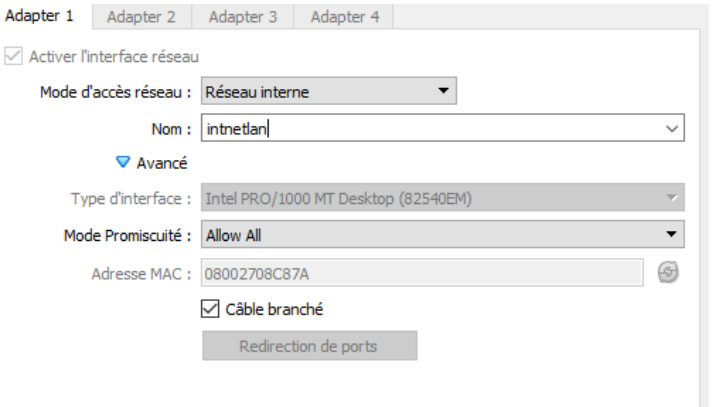
Cliquez ensuite sur add remplir les champs en saisissent le nom de notre portail captif ainsi que la description de celui-ci,

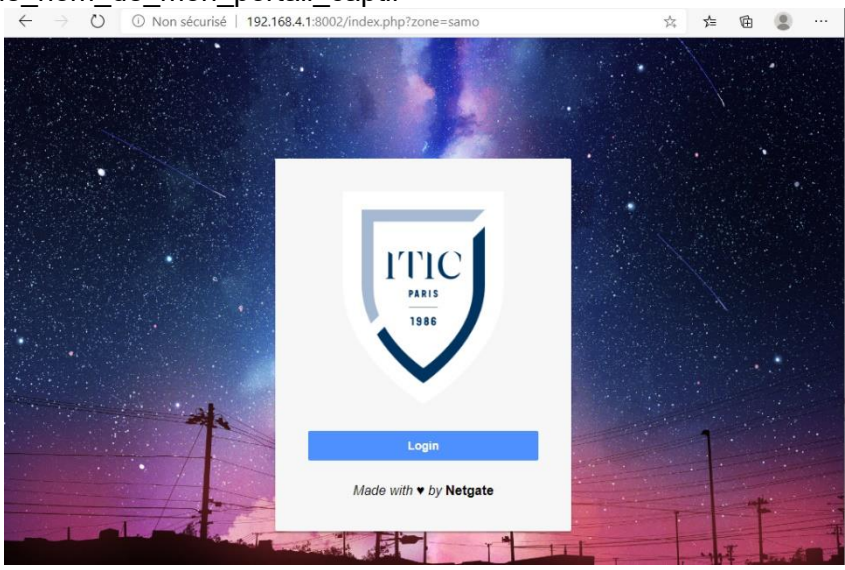
Cliquer sur Save puis nous cocherons la case "Enable Captive Portal", afin d'activer le portail puis sélectionnerons OPT1 pour assigner le portail captif à OPT1.

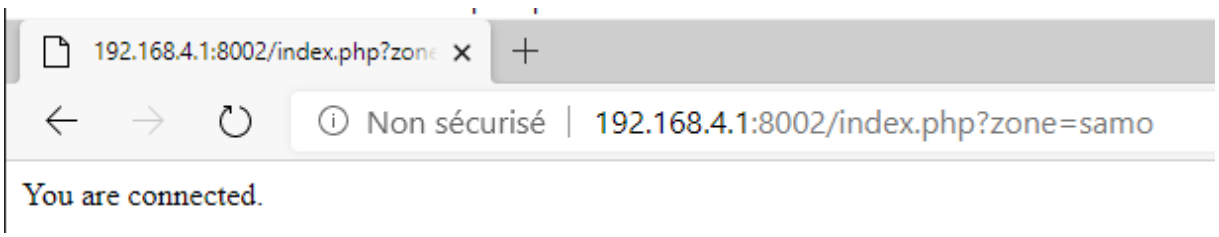
Nous pouvons choisir l'adresse de redirection apes avoir était authentifier par le portail captif celui-ci nous enverra vers l'adresse de redirection inscrite par exemple https://www.google.com/

Rendez-vous ensuite sur votre VM client (Windows 10) accéder à votre navigateur, normalement une page du portail captif s'ouvre d'elle-même sinon accéder au lien

http://192.168.4.1:8002/index.php?zone= "le_nom_de_mon_portail_captif "



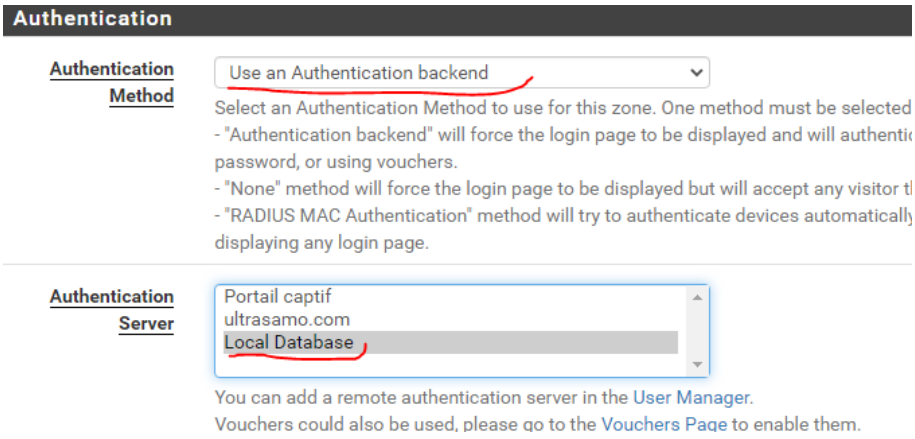




Ayoub Belbachir

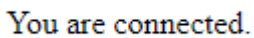
Mise en place du portail captif avec authentification

Cette foi ci rendez-vous dans la configuration de votre portail captif dans l'onglet authentification activer l'authentification backend ensuit sélection " Local Database " cliquer sur Save



Nous allons créer et configurer un Groupe et des Utilisateurs pour la délégation du Portail Captif :

1. System – User Manager
2. Onglet "Groups", cliquez sur "+ Add"
3. Renseigner le Nom du Groupe "Agents" et sa description " délégation du Portail Captif ".
4. Dans l'onglet " Assigned Privileges " cliquez sur add
5. Sélectionnez dans la liste "WebCfg – System : User Manager" Accès à la page de gestion des utilisateurs "User Manager, "WebCfg – Status : Captive Portal "Autoriser l'accès à la page "Status : Portail captif', "User – Services : Captive Portal " Indique si l'utilisateur peut se connecter sur le portail captif et "User – Services: Captive Portal login" (Autorisé seulement à se connecter au Portail Captif)
6. Cliquez "Save"
7. Onglet "Users", cliquez sur "+ Add"
8. Entrer un Nom d'Utilisateur "samo", son mot de passe et sa description
9. Sélectionner dans "Group membership" le groupe "Agents" précédemment créé. Cliquez sur "Move to Member of list" puis "Save"



Ayoub Belbachir

Mise en place du portail captif avec Active directory

Nous allons nous authentifier sur notre portail captif(opt1) à l'aide d'utilisateur crée au préalable sur notre Windows server qui se situe sur le LAN de notre Pfsense.

Avant de créer un domaine et de promouvoir notre serveur en contrôleur de domaine, il faut installer le rôle "ADDS", c'est ce que nous allons faire :

- Ouvrez le gestionnaire de serveur, puis cliquez sur "Gérer" puis "Ajouter des rôles et fonctionnalités".
- On passe l'étape "Avant de commencer" et on poursuit ensuite en laissant le type d'installation sur le choix de base.
- On installe l'ADDS uniquement sur ce serveur, on laisse là encore le choix par défaut et on continue.
- L'étape cruciale de l'installation du rôle est ici, puisqu'il va falloir dans la liste cocher "Services AD DS", "Services de stratégie et d'accès réseau" et validez aussi quand l'assistant vous propose d'installer les outils de gestion. Qui dit outils de gestion, dit console d'administration comme "Utilisateurs et ordinateurs Active Directory" mais aussi le module PowerShell pour Active Directory.
- Nous n'installons pas de fonctionnalités en plus, donc poursuivez sans rien sélectionner.
- Cliquer sur suivant puis installer

Enfin depuis Windows Server 2012, un message dans le gestionnaire de serveur qui permet de promouvoir le serveur en tant que contrôleur de domaine est apparue on choisit cliquer dessus, ensuite "Ajouter une nouvelle forêt" et on indique le nom de domaine Enfin, indiquez un mot de passe, Indiquez un nom NETBIOS pour le domaine, à savoir un nom court et qui ne s'appuie pas sur DNS pour être résolu. Cliquez 2 fois sur suivant puis sur installer.

Nous allons créer un nouveau group et de nouveaux utilisateurs pour s'identifier via le portail captif

- Ouvrez ensuite l'outil "Utilisateur et ordinateur Active directory"
- Clic droit sur votre domaine : samodigi.lan, nouveau "Unité d'organisation" attribuer lui un nom "Pfsense" entrer dans le répertoire que l'on vient de crée
- Clic Droit et faire Nouveau > Group donner lui un nom "samogrp"
- Clic droit Nouveau > Utilisateur nommer le "client" attribuer lui un mot de passe clic droit sur l'utilisateur "client" > propriété dans l'onglet "membre de" cliquer sur ajouter et ajouter le group précédemment crée "samogrp"

Une fois l'installation du rôle terminé, lancez la console d'administration du serveur NPS, Nous allons commencer par mettre en place un nouveau client RADIUS.

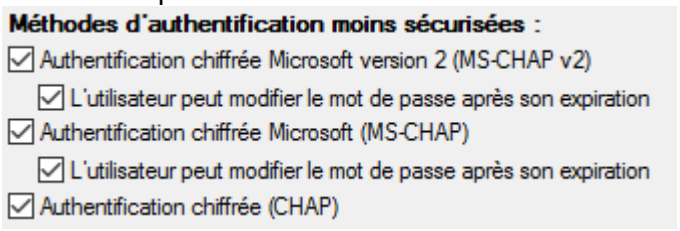
Ouvrir le gestionnaire de serveur et aller dans le menu Outil > Serveur NPS (Network Policy Server), Effectuer un clic-droit sur NPS (Local)

- Cliquez sur Inscrire un serveur dans Active Directory
- Allez dans Client et serveurs RADIUS (sous NPS (Local))

- Effectuer un clic-droit sur Client RADIUS > Nouveau Nom convivial : samo
- Adresse IP : 192.168.2.1 (IP de l'interface LAN de Pfsense)
- Ajouter un secret partagé à retenir, cliquer ensuite sur ok

Nous allons maintenant donner l'autorisation aux utilisateurs. Dans notre cas, il faut donc ajouter le groupe de sécurité portail et tous les utilisateurs appartenant à ce groupe auront l'autorisation :

- Allez dans Stratégies
- Effectuer un clic-droit sur Stratégies réseau > Nouveau
- Nom de la stratégie : portail captif
- Cliquez sur suivant
- Cliquez sur Ajouter…
- Sélectionnez Groupes d'utilisateur et cliquez sur Ajouter…
- Cliquez sur Ajouter des groupes…
- Tapez le nom de votre groupe : samogrp et cliquez sur Vérifier les noms
- Cliquez sur Ok
- Cliquez ensuite sur Suivant
- Laissez par défaut : Accès accordé et cliquez sur Suivant
- Cocher les cases suivantes :



- Laissez tout le reste par défaut et cliquez sur suivant jusqu'à la fin.
- Cliquez sur Terminer.
- Effectuer un double clic sur le nom de la stratégie qu'on vient de créer (portail captif)
- Allez dans l'onglet Paramètres
- Allez dans Chiffrement
- Décochez la case : Aucun chiffrement
- On désactive les 2 autre stratégie car elles ne sont pas utile pour notre portail captif

Connectez-vous à la WebUI de votre Pfsense avec un compte administrateur. Nous allons configurer un serveur d'authentification Radius :

- Allez dans le menu : Système > User Manager > Serveurs d'authentification
- Cliquez sur Ajouter

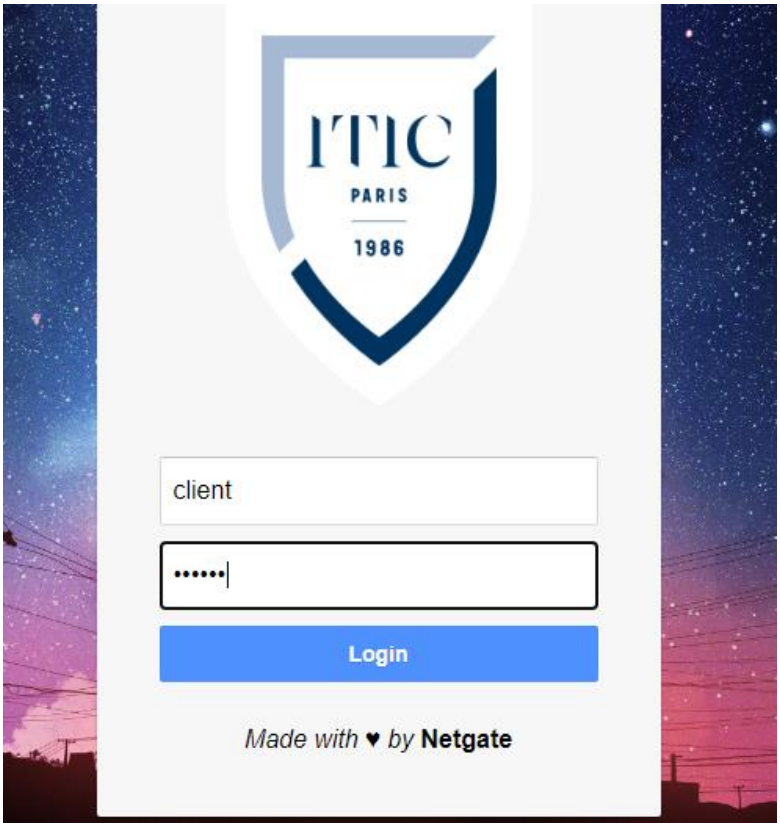
- ✓ Nom descriptif : portail captif
- ✓ Type : RADIUS
- ✓ Protocole : MS-CHAPv2
- ✓ Nom d'hôte ou adresse IP : 192.168.2.5 (Adresse du serveur RADIUS)
- ✓ Secret partagé : ce que vous avez mis lors de l'activation du client RADIUS sous Windows
- ✓ Services offered: Authentification and Accounting
- ✓ Port d'authentification: 1812

Ayoub Belbachir

- ✓ Port de comptabilité : 1813
- ✓ Délai d'expiration de l'authentification : 5
- ✓ RADIUS NAS IP : LAN – 192.168.2.1

- Cliquez sur Save

Cette foi ci rendez-vous dans la configuration de votre portail captif dans l'onglet authentification activer l'authentification backend ensuit sélection " Portal captif " cliquer sur Save



You are connected.

Ayoub Belbachir

Mise en place du portail captif avec LDAP

Installer et configurer le serveur OpenLDAP :

Nous allons commencer par l'installation d'OpenLDAP sur Ubuntu 18.04 LTS. Définissez le nom d'hôte de votre système et ajoutez-le au fichier /etc/hosts :

- sudo hostnamectl set-hostname ultrasamo.com
- sudo nano /etc/hosts
  - 192.168.18.50 ultrasamo.com
- sudo reboot

Tout d'abord, vous devrez installer Slapd et d'autres utilitaires LDAP sur votre serveur. Vous pouvez les installer en exécutant la commande suivante :

- sudo apt update
- sudo apt-get install slapd ldap-utils

Lors de l'installation, il vous sera demandé de configurer un mot de passe administrateur

Fournissez votre mot de passe sécurisé et appuyez sur Entrée pour continuer. Une fois l'installation terminée, vous devrez reconfigurer le package SLAPD pour définir les informations de votre domaine :

- sudo dpkg-reconfigure slapd

Il vous sera demandé d'omettre la configuration du serveur OpenLDAP Sélectionnez Non et appuyez sur Entrée pour continuer. Il vous sera demandé de fournir un nom de domaine DNS

Entrer un nom de domaine DNS (ultrasamo.com)

Fournissez votre nom de domaine et appuyez sur Entrée pour continuer, Il vous sera demandé de fournir le nom de l'organisation comme indiqué ci-dessous :

Entrer le nom de l'organisation (ultrasamo.com)

Fournissez votre mot de passe administrateur et appuyez sur **Entrée** pour continuer. Il vous sera demandé de supprimer la base de données sélectionner YES puis entrer.

Vérifier si notre installation à était pris en compte avec la commande :

- sudo slapcat

À la ligne "dn:" les informations que vous avez précédemment saisies devraient s'affiché :

  - dn: dc=ultrasamo,dc=com

Ouvrir le fichier de configuration de phpldapadmin :

≥ sudo nano /etc/phpldapadmin/config.php

Et modifier les ligne suivante selon vous et selon votre “dn:” ou votre adresse ip

- config->custom->appearance['timezone'] = 'Europe/Paris';
- $servers->setValue('server','name','mon ldap');
- $servers->setValue('server','base', array('dc=ultrasamo,dc=com'));
- $config->custom->appearance['hide_template_warning'] = true;
- $servers->setValue('login','bind_id','cn=admin,dc=ultrasamo,dc=com');
- $servers->setValue('server','host','192.168.2.17');

Ensuite, désactivez le fichier de configuration d'hôte virtuel Apache par défaut et redémarrez le service Apache pour appliquer les modifications :

≥ a2dissite 000-default.conf
≥ systemctl restart apache2

Accéder au WebUI de notre serveur phpmyldap (remplacer l’adresse ip par celle de votre server LDAP) : http://192.168.2.17/phpldapadmin

- Cliquer sur “login” entrée votre “dn”, puis le mot de passe
- Création des Utilisateurs et d’un groupe :
- Cliquer sur le “+” situer à gauche de votre “dc”
- Cliquer ensuite sur “Create new entry here” sélectionner “generic: organisation Unit” donner lui un nom “samog” cliquer ensuite sur “comit”
- Puis sélectionner l’unité crée, créer une sous entrée, sélectionner “generic: Posix Group” donner lui un nom “samogroup”
- Puis sélectionner le group crée, créer une sous entrée, sélectionner “genericUser Account” remplir les cases suivantes celons vos préférences :

  - Common Name : client
  - First name : client
  - GDI Number : samogroup (par défaut)
  - Home Directory:/home/user/cclient (par défaut)
  - Last name : client
  - Login Shell : /bin/sh (correspond au bash de Ubuntu server)
  - Password : (attribuer un mot de passe pour cette utilisateur)
  - Cliquer sur “ Create Object” puis comit
  - Cliquer en suite sur l’utilisateur que nous venons de crée et renommer le en “client” (par défaut son devrait être “client client”, par ce que le “Last Name” si est mêlé

Ensuite nous allons configure nous rendre sur le WebUI de Pfsense :

- Allez dans le menu : Système > User Manager > Serveurs d’authentification
- Cliquez sur Ajouter

✓ Nom descriptif : ulrasamo.com
✓ Type : LDAP
✓ Hostname or IP : 192.168.1.17 (l’adresse ip de notre serveur LDAP)

Ayoub Belbachir

- ✓ Protocol value : 389 (par défaut)
- ✓ Transport : Standard TCP
- ✓ Peer Certificate Authority: Global Root VA List
- ✓ Protocol version: 3 (par default)
- ✓ Server Timeout: 25 (par default)
- ✓ Search scope level: Entire Subtree
- ✓ Base DN: dc=ultrasamo,dc=com

- Authentification containers: ou=ultrasamogroup,cn=admin,dc=ultrasamo,dc=com (coller notre dn puis cliquer sur “select container” Pfsense devrai alors notre base donner qu’on a paramétré , sélectionner la)

- ✓ Cocher la case “Use anonymous binds to resolve distinguished names”
- ✓ Group Object Class: posixGroup

- Laisser les autre valeur par défaut et cocher la case “Allow unauthenticate”

- Cliquer sur Save

Cette foi ci rendez-vous dans la configuration de votre portail captif dans l’onglet authentification activer l’authentification backend ensuit sélection “ultrasamo.com” cliquer sur Save

Rendez-vous sur le Windows 10