

Projet Personnel Encadré : Portail Captif

21/10/2016

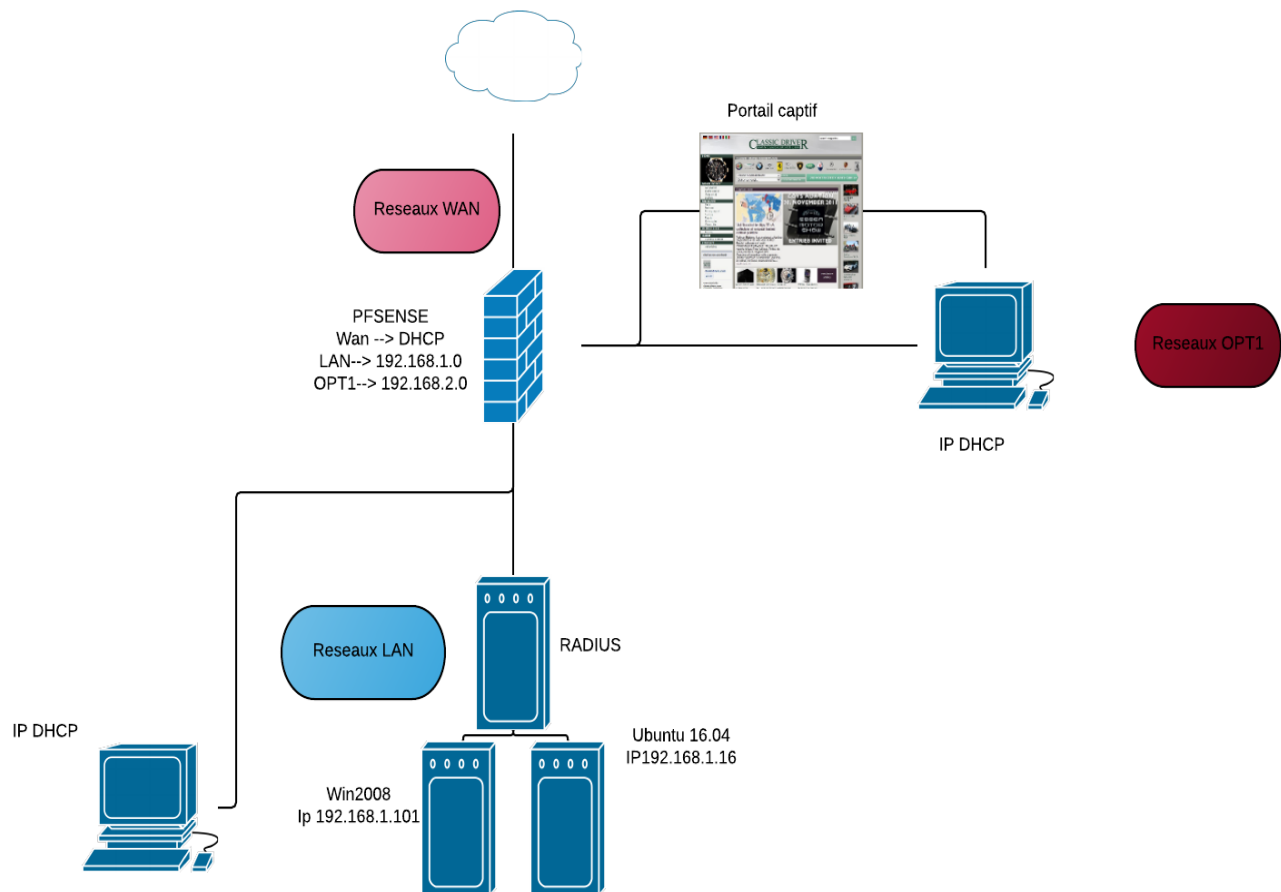
PPE : Portail Captif

Sommaire

| | |
|--|----|
| Schéma réseaux | 3 |
| Contexte..... | 4 |
| 1.1. Introduction | 4 |
| 1.2. Définition | 4 |
| Prérequis..... | 5 |
| Paramétrage de la carte OPT1 | 6 |
| Paramétrage du DHCP sur l'interface OPT1..... | 7 |
| L'ajout de la règle du pare feu | 8 |
| Portail captive sans authentification user et mots de passe | 9 |
| Portail captive avec authentification user et mots de passe local..... | 11 |
| Portail captif avec Authentification Active Directory..... | 14 |
| Portail captif avec Authentification OPENLDAP | 23 |

PPE : Portail Captif

Schéma réseaux



PPE : Portail Captif

Contexte

1.1. Introduction

Dans ce compte rendu, nous allons procéder à la mise en place d'un portail captive via l'outil PfSense

Plusieurs types de portail captif existe, dans notre présentation nous allons vous montrer ces différents types de portail

- Authentification LDAP
- Authentification AD
- Authentification avec un User ID local
- Authentification simple sans contrôle accès

1.2. Définition

Le portail captif est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement.

Au-delà de l'authentification, les portails captifs permettent d'offrir différentes classes de services et tarifications associées pour l'accès Internet. Par exemple, Wi-Fi gratuit, filaire payant, 1 heure gratuite...

Cette technique est généralement mise en œuvre pour les accès Wi-Fi mais peut aussi être utilisée pour l'accès à des réseaux filaires (ex. : hôtels, campus, etc.)/

PPE : Portail Captif

Prérequis

Les Prérequis nécessaire afin de mettre en place un portail captif il faut :

- 1 Serveur Pfsense :
 - 3 Carte réseaux :
 - Wan → NAT → *Nom* : « WAN » → DHCP
 - LAN → Réseaux inet → *Nom* : « LAN » → DHCP → interface LAN : 192.168.1.1
 - OPT1 → Réseaux inet → *Nom* : « OPT1 » → DHCP → Interface OPT1 : 192.168.2.1
- 1 Serveur Windows 2008 R2
 - 1 Carte réseaux
 - LAN → Réseaux Inet → *Nom* : « LAN » → STATIC → Interface LAN : 192.168.1.101
 - Active directory → Groupe + User
- 2 Windows 7
 - 1 carte
 - 1 Windows 7 LAN
 - LAN → réseaux inet → *Nom* : « LAN » → DHCP
 - 2 Windows 7 OPT1
 - OPT1 → Réseaux inet → *Nom* : « OPT1 » → DHCP
- 1 Serveur Ubuntu 16.04 LTS
 - 1 Carte réseaux
 - LAN → Réseaux Inet → *Nom* : « LAN » → STATIC → Interface LAN : 192.168.1.16
 - Openldap → User + group

PPE : Portail Captif

Paramétrage de la carte OPT1

Pour activer la carte OPT1 cliquer sur « Interfaces ».

| Interfaces | | | |
|------------|---|-------------------------|-------------|
| WAN | ↑ | 1000baseT <full-duplex> | 10.0.2.15 |
| LAN | ↑ | 1000baseT <full-duplex> | 192.168.1.1 |

Puis cliquer sur « réglage » :



Actuellement l'interface OPT1 est pas disponible, pour l'activer il suffit de cliquer sur l'icône « Add » :

| Interface | Network port |
|--------------------------|---|
| WAN | em0 (08:00:27:23:a3:cc) |
| LAN | em1 (08:00:27:6e:3b:61) Delete |
| Available network ports: | em2 (08:00:27:76:b4:c4) + Add |

Save

Carte OPT1 et ajouter cliquer save pour enregistrer la carte.

| Interface | Network port |
|-----------|---|
| WAN | em0 (08:00:27:23:a3:cc) |
| LAN | em1 (08:00:27:6e:3b:61) Delete |
| OPT1 | em2 (08:00:27:76:b4:c4) Delete |

Save

Nous allons ensuite définir une adresse réseau sur cette carte cliquer sur OPT1

Information :

Description : **OPT1**

IPV4 configuration type : **Static IPv4**

IPV4 Address : **192.168.2.1**

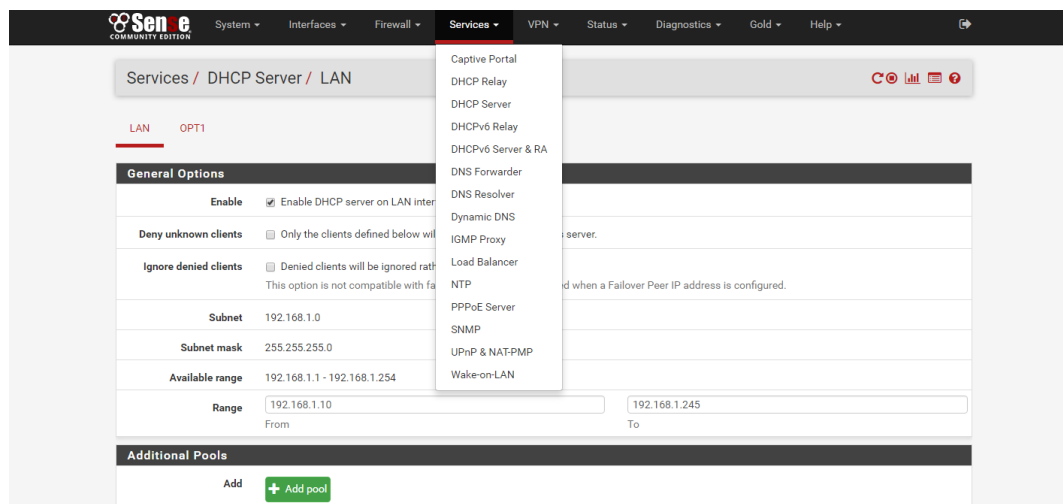
Les 3 interfaces sont activées :

| Interfaces | | | |
|------------|---|-------------------------|-------------|
| WAN | ↑ | 1000baseT <full-duplex> | 10.0.2.15 |
| LAN | ↑ | 1000baseT <full-duplex> | 192.168.1.1 |
| OPT1 | ↑ | 1000baseT <full-duplex> | 192.168.2.1 |

PPE : Portail Captif

Paramétrage du DHCP sur l'interface OPT1

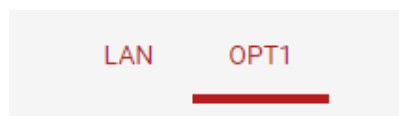
Pour paramétrer le serveur DHCP sur l'interface OPT1 il faut aller sur « service » -- « DHCP Server »



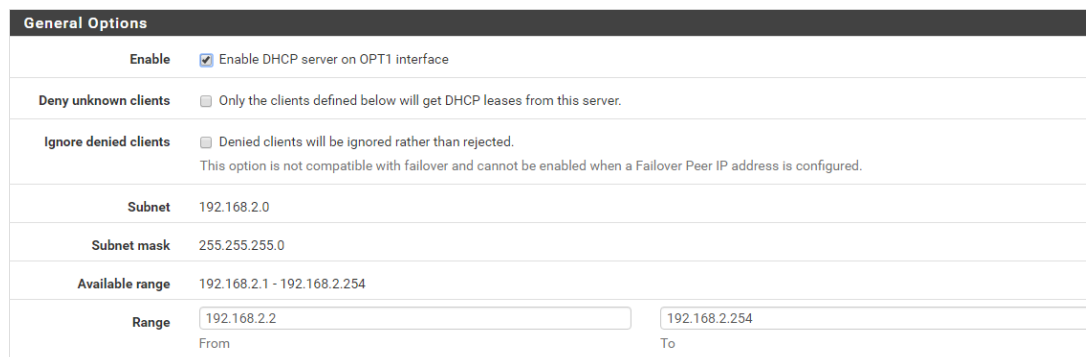
The screenshot shows the Mikrotik WinBox interface for configuring the DHCP Server on the LAN interface. The 'Services' menu is open, highlighting 'DHCP Server'. The configuration page shows the following settings:

- General Options:**
 - Enable: Enable DHCP server on LAN interface
 - Deny unknown clients: Only the clients defined below will get DHCP leases from this server.
 - Ignore denied clients: Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
 - Subnet: 192.168.1.0
 - Subnet mask: 255.255.255.0
 - Available range: 192.168.1.1 - 192.168.1.254
 - Range: From 192.168.1.10 To 192.168.1.245
- Additional Pools:** Add

Choisir l'interface OPT1 :



Activer le DHCP – et ajouter le range début de ip puis la fin de l'adresse ip puis sauvegarder



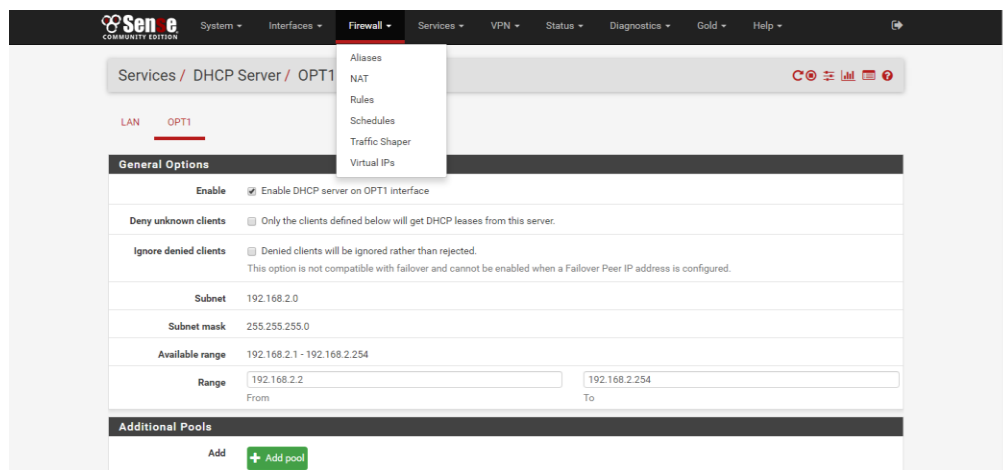
The screenshot shows the Mikrotik WinBox interface for configuring the DHCP Server on the OPT1 interface. The configuration page shows the following settings:

- General Options:**
 - Enable: Enable DHCP server on OPT1 interface
 - Deny unknown clients: Only the clients defined below will get DHCP leases from this server.
 - Ignore denied clients: Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
 - Subnet: 192.168.2.0
 - Subnet mask: 255.255.255.0
 - Available range: 192.168.2.1 - 192.168.2.254
 - Range: From 192.168.2.2 To 192.168.2.254

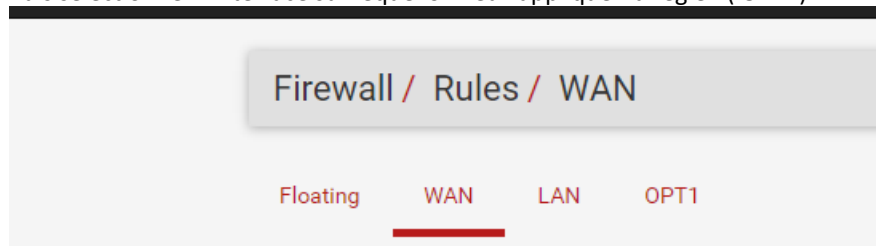
PPE : Portail Captif

L'ajout de la règle du pare feu

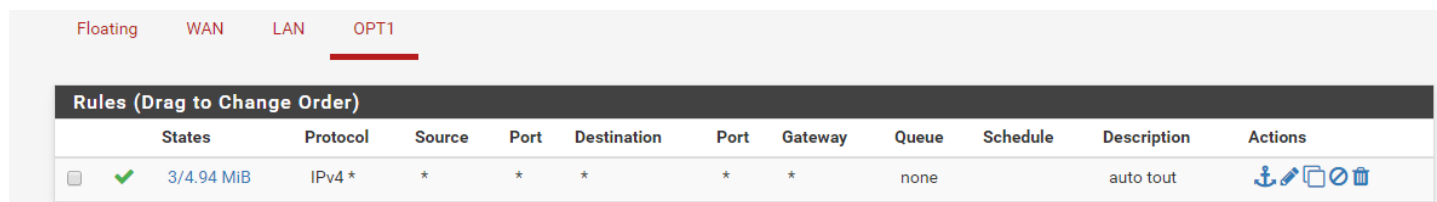
Pour ajouter la règle sur le pare feu il faut aller dans « Firewall » puis « Rules »



Puis sélectionner l'interface sur lequel on veut appliquer la règle : (OPT1)



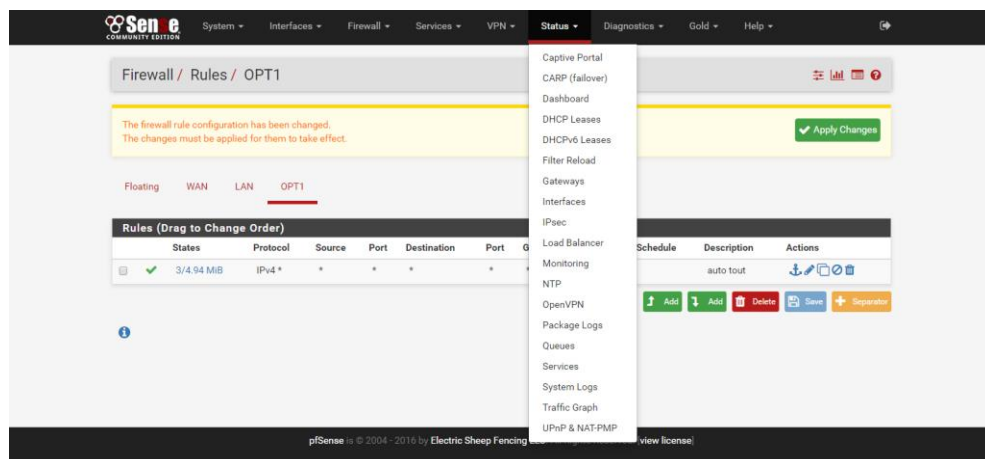
On va ajouter la règle qui va permettre de pouvoir se connecter a interface grâce à cette interface



PPE : Portail Captif

Portail captif sans authentification user et mots de passe

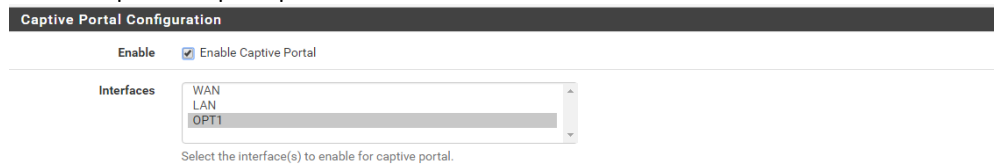
Pour ajouter un portail captif il faut aller dans « status » -- « Captive portail »



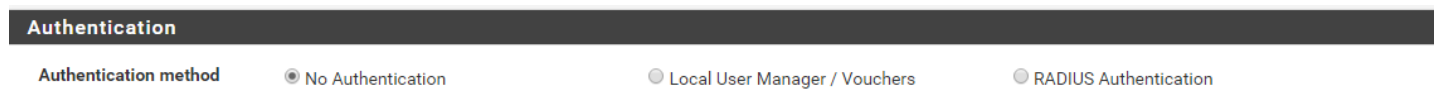
Puis réglage puis ajouter :



Activer le portail captif puis sélectionner l'interface :



Sélectionner la méthode d'authentification dans cette situation nous allons choisir no Authentification :



PPE : Portail Captif

Nous allons insérer une fonction en .php qui va permettre seulement de d'avoir un commentaire et valider sur le bouton

HTML Page Contents

Portal page contents

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL_ACTIONS\$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL_REDIRURL\$". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail.

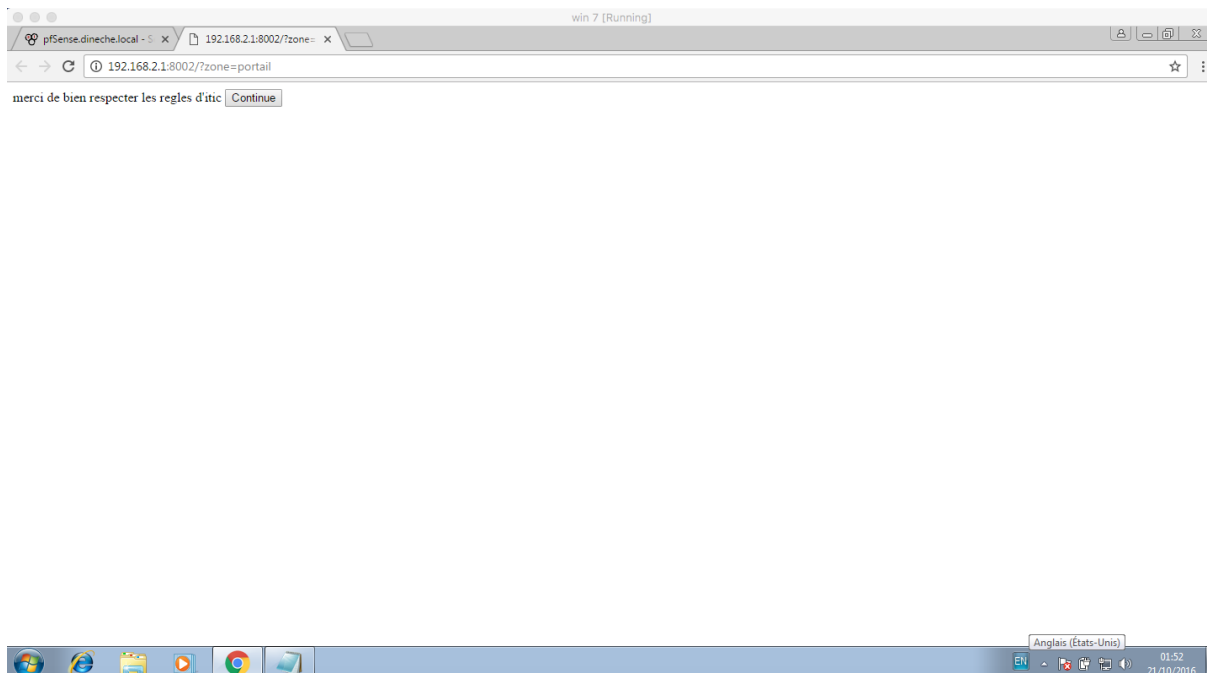
Example code for the form:

```
<form method="post" action="$PORTAL_ACTIONS$">
<input name="auth_user" type="text">
<input name="auth_pass" type="password">
<input name="auth_voucher" type="text">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="zone" type="hidden" value="$PORTAL_ZONE$">
<input name="accept" type="submit" value="Continue">
</form>
```

code qui sera mis en php

```
<form method="post" action="$PORTAL_ACTIONS$">
merci de bien respecter les regles d'itic
<input name="auth_user" type="hidden" values="captif">
<input name="auth_pass" type="hidden" values="captif">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="zone" type="hidden" value="$PORTAL_ZONE$">
<input name="accept" type="submit" value="Continue">
</form>
```

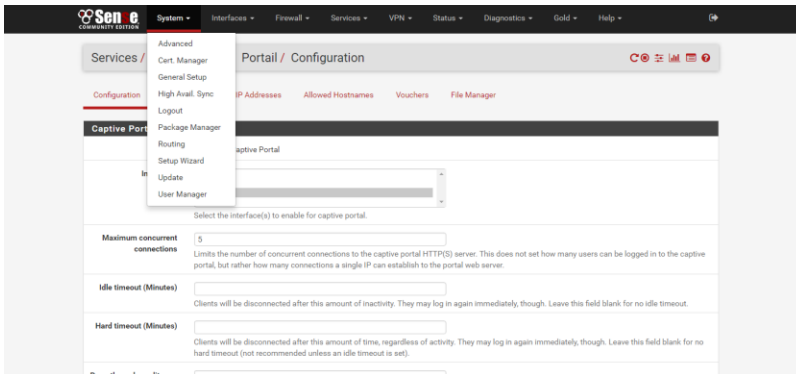
Le rendu final :



PPE : Portail Captif

Portail captif avec authentification user et mots de passe local

Ajouter un user pour le portail captif : « System » -- « User Manager »

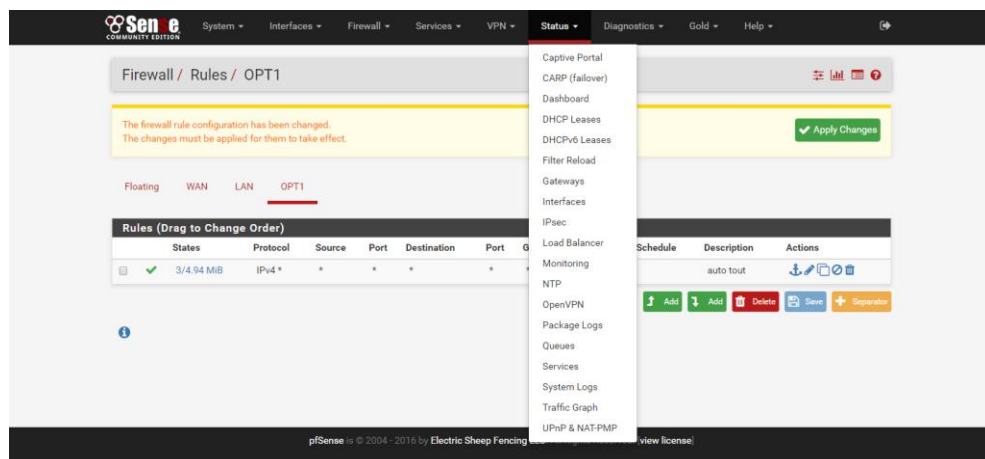


Nom – mots de passe – ajouter des droits admin si nécessaire (dans notre situation le compte serre seulement d’authentification sur le portail pour les droit admin ne sont pas nécessaire)

| User Properties | |
|------------------|--|
| Defined by | USER |
| Disabled | <input checked="" type="checkbox"/> This user cannot login |
| Username | <input type="text"/> |
| Password | <input type="password"/> Password <input type="password"/> Confirm Password |
| Full name | <input type="text"/> User's full name, for administrative information only |
| Expiration date | <input type="text"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date |
| Custom Settings | <input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user. |
| Group membership | <input type="text"/> admins <input type="text"/> Not member of Member of |

PPE : Portail Captif

Puis retourner dans :



Puis choisir le portail captif OPT1 puis éditer

| Captive Portal Zones | | | | |
|----------------------|------------|-----------------|-------------|---|
| Zone | Interfaces | Number of users | Description | Actions |
| Portail | OPT1 | 1 | OPT1 |   |

Verifier que le portail captif sélectionne de l'interface et bien OPT1:

Captive Portal Configuration

Enable Enable Captive Portal

Interfaces

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

Sélectionner la méthode d'authentification dans cette situation nous allons choisir no Authentification :

Authentication

Authentication method No Authentication Local User Manager / Vouchers RADIUS Authentication

PPE : Portail Captif

Nous allons insérer une fonction en .PHP qui va permettre seulement de d'avoir un id et mots de passe

HTML Page Contents

Portal page contents Choisissez un fichier Aucun fichier choisi

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL_ACTIONS") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL_REDIRURL\$". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail.

Example code for the form:

```
<form method="post" action="$PORTAL_ACTIONS">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="zone" type="hidden" value="$PORTAL_ZONES$">
  <input name="accept" type="submit" value="Continue">
</form>
```

Code qui sera mis en PHP

```
<form method="post" action="$PORTAL_ACTIONS">
  nom user <input name="auth_user" type="text">
  password <input name="auth_pass" type="password">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="zone" type="hidden" value="$PORTAL_ZONES$">
  <input name="accept" type="submit" value="continue">
</form>
```

Le rendu final :



The screenshot shows a web browser window with the address bar displaying "192.168.2.1:8002/?zone=portail". The page content includes a form with the following elements:

- A text input field labeled "nom user".
- A password input field labeled "password".
- A "Continue" submit button.

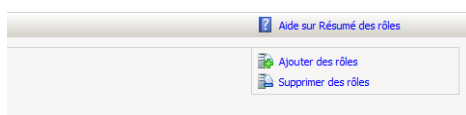
PPE : Portail Captif

Portail captif avec Authentification Active Directory

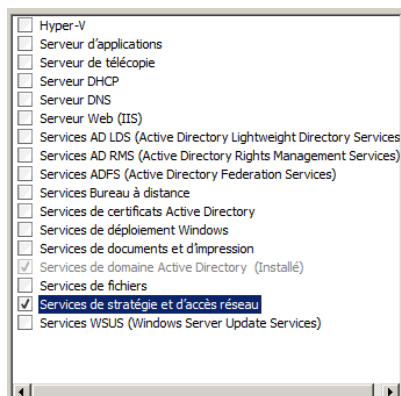
Il faut d'abord installer un serveur Radius afin que le serveur et pfSense puis faire une liaison entre les deux :

Pour cela :

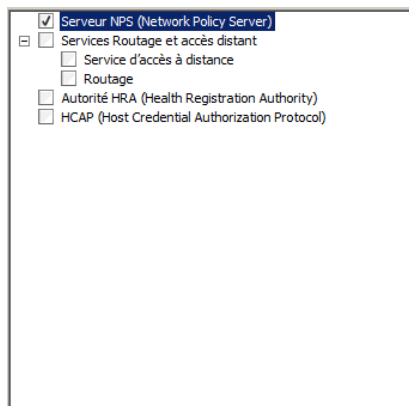
Ajouter un nouveau rôle :



Cocher « Services de stratégies et d'accès réseau »

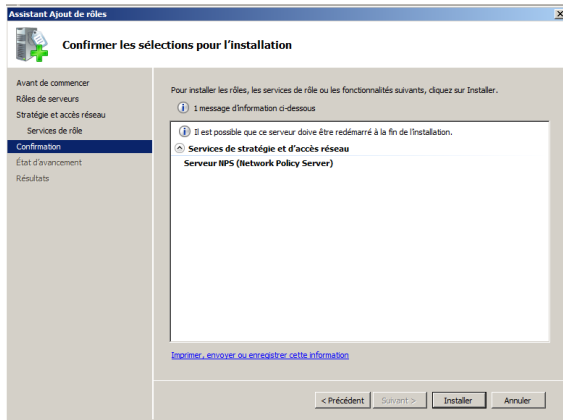


Sélectionner le service de rôles : « Serveur NPS (Network Policy Server) il permet de créer et d'appliquer des stratégies d'accès réseau à l'échelle de l'entreprise pour l'intégrité des clients, l'authentification et l'autorisation de la demande de connexion.

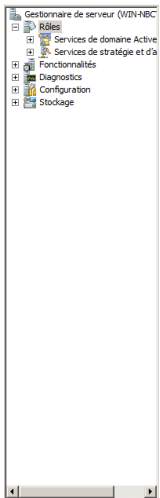


PPE : Portail Captif

Puis installer :

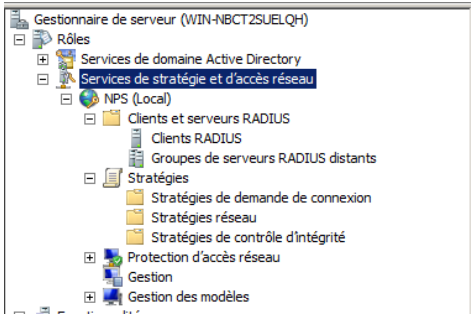


Une fois installer dans → rôles → service de stratégie et d'accès au réseaux

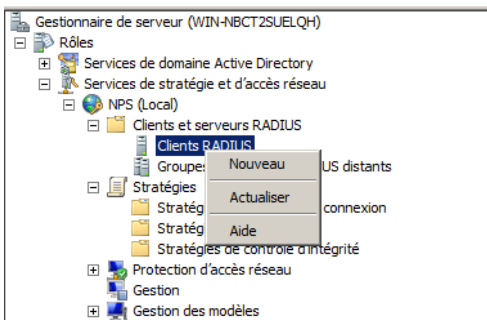


PPE : Portail Captif

Tout d'abord nous allons paramétrer le serveur radius afin qu'il puisse communiquer avec le serveur pfsense :



Clique droit puis crée un nouveau client :



PPE : Portail Captif

Ajouter les informations nécessaires :

Nom convivial → pfsense

Adresse ip sur serveur pfsense → 192.168.1.10

Secret partager (c'est le mots de passe qui va permettre au serveur pfsense de se connecter au serveur) → *****

Puis cliquer sur vérifier IP

Nouveau client RADIUS

Paramètres | Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial : Pfsense

Adresse (IP ou DNS) : 192.168.1.1 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant : Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel Générer

Secret partagé : *****

Confirmez le secret partagé : *****

OK Annuler

Résoudre ip afin qu'il puisse vérifier

Vérifier l'adresse

Adresse : 192.168.1.1 Résoudre

Pour identifier le client à l'aide d'une adresse IP, sélectionnez-la dans la liste suivante.

Adresse IP :

OK Annuler

Vérifier l'adresse

Adresse : 192.168.1.1 Résoudre

Pour identifier le client à l'aide d'une adresse IP, sélectionnez-la dans la liste suivante.

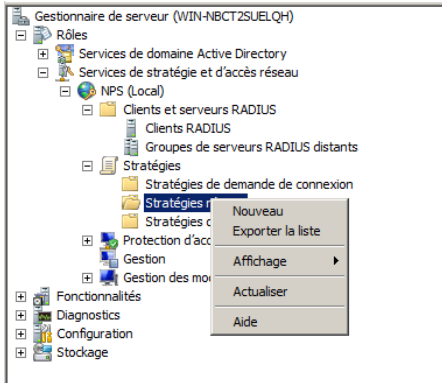
Adresse IP : 192.168.1.1

OK Annuler

Puis valider → radius et enfin paramettre

PPE : Portail Captif

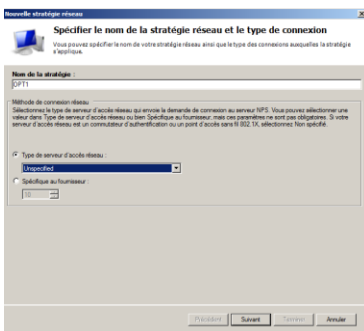
Nous allons aussi cree une nouvelle strategie → clique droit → nouveau



Nom de la strategie → OPT1

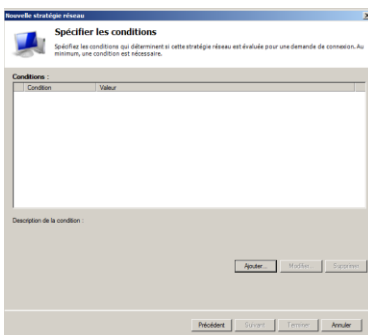
Type de reseaux acces → Unspecified

Puis suivant



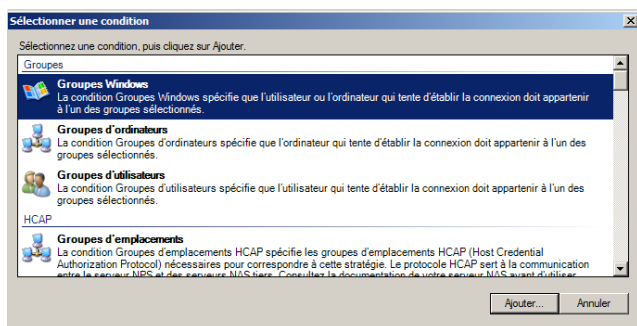
Puis nous allons autoriser les accès elle va permettre d 'autoriser les compte ad a se connecter au portail captif

▪ Ajouter

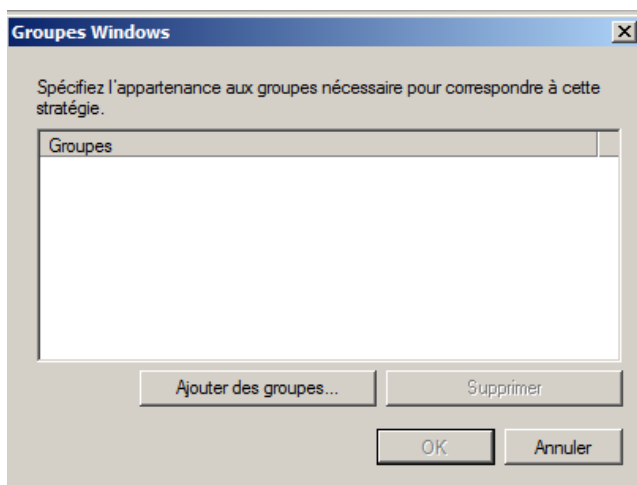


PPE : Portail Captif

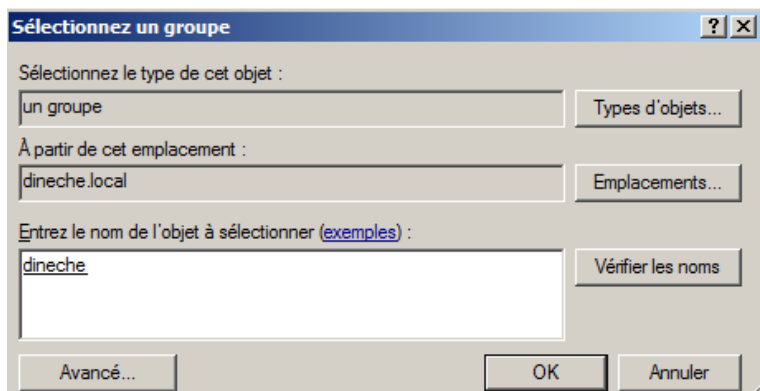
Sélectionner groupe Windows puis ajouter :



Ajouter des groupe (attention bien crée au préalable un groupe et rajouter le user dans le groupe pour exemple mon groupe s'appelle « dineche » → le compte « Itic »

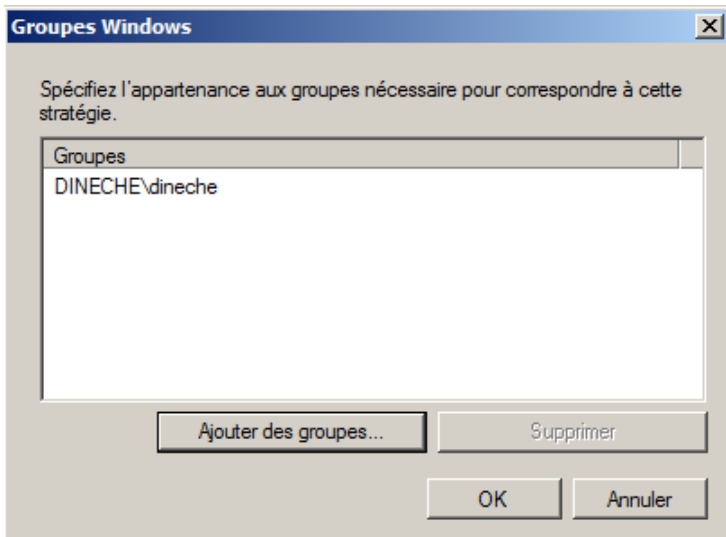


Écrire le nom puis vérifier afin qu'il puisse ajouter sans erreur

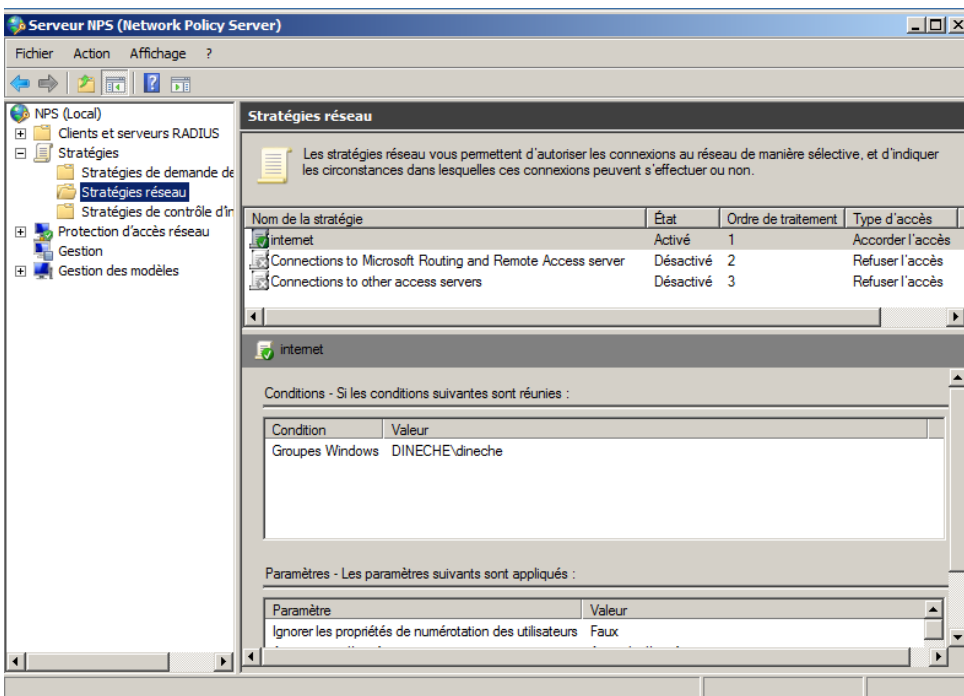


PPE : Portail Captif

Puis valider enfin la stratégie sera opérationnelle :



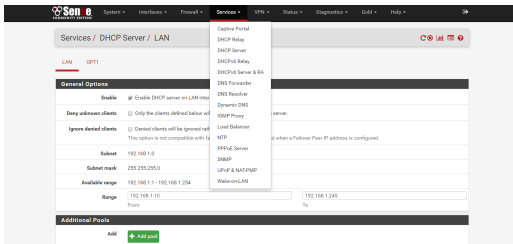
Petit résumer




PPE : Portail Captif

Paramétrage cote Serveur pfsense :

- Service
 - CAPTIVE PORTAIL



Editer l'ancien portail captif ou bien crée un nouveau

| Captive Portal Zones | | | | |
|----------------------|------------|-----------------|-------------|--|
| Zone | Interfaces | Number of users | Description | Actions |
| Portail | OPT1 | 1 | OPT1 |   |

Authentification :

- Radius Authentication
- MSCHAPv2 (c'est le Protocol qui nous avons choisie lors de l'installation du radius)

Primary Authentication Source :

IP serveur Win2008 : 192.168.1.101

Port : 1812 par default

Mots de passe secret : dineche

| Authentication | | | |
|--|--|---|--|
| Authentication method | <input type="radio"/> No Authentication | <input type="radio"/> Local User Manager / Vouchers | <input checked="" type="radio"/> RADIUS Authentication |
| RADIUS protocol | <input type="radio"/> PAP | <input type="radio"/> CHAP-MD5 | <input checked="" type="radio"/> MSCHAPv1 |
| Primary Authentication Source | | | |
| Primary RADIUS server | <input type="text" value="192.168.1.101"/> | <input type="text" value="1812"/> | <input type="text" value="dineche"/> |
| Secondary RADIUS server | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| | IP address of the RADIUS server to authenticate against. | RADIUS port. Leave blank for default (1812) | RADIUS shared secret. Leave blank to not use a shared secret (not recommended) |
| Secondary Authentication Source | | | |

PPE : Portail Captif

Puis modifier le RADIUS NAS IP Attribute en choisant le OPT1

**RADIUS NAS IP
Attribute**

OPT1 - 192.168.2.1 ▼

Choose the IP to use for calling station attribute.

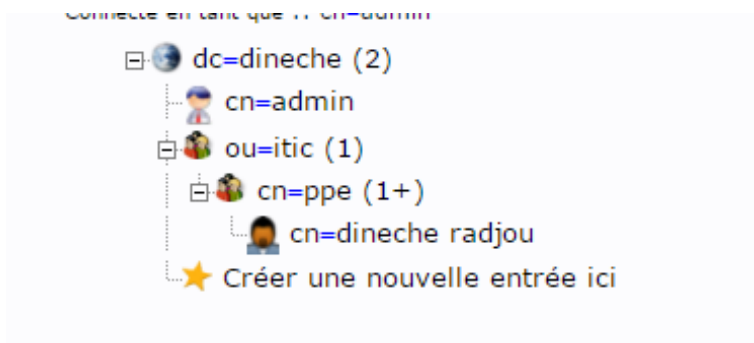
Voilà les configurations sont terminer afin que le portail captif puis se connecter au serveur 2008 via le serveur radius.

PPE : Portail Captif

Portail captif avec Authentification OPENLDAP

Se connecter sur PHPLDAPADMIN

Crée un user et un groupe



Vérifier sous ligne de commande que le compte a bien été créé ça va aussi nous aider pour les étapes qui suivront après :

`ldapsearch -x -h localhost -b « dc=dineche »`

```
searchdb: No such file or directory
root@dineche:~# ldapsearch -D "cn=admin" -w dineche -p 389 -h 127.0.0.1 -f searchdb
searchdb: No such file or directory
root@dineche:~# ldapsearch -D "cn=admin" -w dineche -p 389 -h 127.0.0.1 -f searchdb
searchdb: No such file or directory
root@dineche:~# ldapsearch -D "cn=admin" -w dineche -p 389 -h 127.0.0.1 -f searchdb
searchdb: No such file or directory
root@dineche:~# ldapsearch -D "cn=admin" -w dineche -p 389 -h 127.0.0.1 -f searchdb
searchdb: No such file or directory
root@dineche:~# ldapsearch -x -h localhost -b "dc=dineche"
# extended LDIF
#
# LDAPv3
# base <dc=dineche> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# dineche
dn: dc=dineche
objectClass: domain
dc: dineche

# example, dineche
dn: uid=example,dc=dineche
cn: Example user
sn: Example user
uid: example
uidNumber: 9999
gidNumber: 9999
loginShell: /bin/sh
homeDirectory: /home/example
objectClass: posixAccount
objectClass: person

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
root@dineche:~#
```

PPE : Portail Captif

Paramétrer l'interface user :

System / User Manager / Users

Puis choisir :

Authentication Servers

Renseigner les champs grâce à la commande que nous avons effectuée sur le serveur ubuntu 16.04

Description : LDAP

Ip serveur : 192.168.1.18

Port : 389

Search scope : One Level

Cn=toto (user LDAP) dn=dineche (domaine)

The screenshot shows the 'LDAP Server Settings' configuration page. The 'Descriptive name' is 'LDAP' and the 'Type' is 'LDAP'. Under 'LDAP Server Settings', the 'Hostname or IP address' is '192.168.1.16', 'Port value' is '389', and 'Transport' is 'TCP - Standard'. The 'Peer Certificate Authority' section shows 'No Certificate Authorities defined'. The 'Protocol version' is '3', 'Server Timeout' is '25', and 'Search scope' is 'One Level'. The 'Base DN' is 'cn=toto, dn=dineche'.

| Server Settings | |
|----------------------------|--|
| Descriptive name | LDAP |
| Type | LDAP |
| LDAP Server Settings | |
| Hostname or IP address | 192.168.1.16 <small>NOTE: When using SSL, this hostname MUST match the Common Name (CN) of the LDAP server's SSL Certificate.</small> |
| Port value | 389 |
| Transport | TCP - Standard |
| Peer Certificate Authority | No Certificate Authorities defined. Create one under System > Cert. Manager. |
| Protocol version | 3 |
| Server Timeout | 25 <small>Timeout for LDAP operations (seconds)</small> |
| Search scope | Level One Level |
| Base DN | cn=toto, dn=dineche |

PPE : Portail Captif

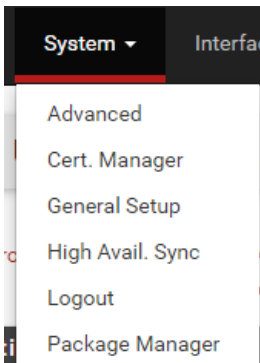
Authentication containers : CN= admin (user) DC=dineche (domaine)

Group Object Class : manager (groupe LDAP)

| | | |
|----------------------------------|---|---|
| Authentication containers | <input type="text" value="CN=toto;DC=dineche"/> | <input type="button" value="Select a container"/> |
| | <small>Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff,OU=Freelancers</small> | |
| Extended query | <input type="checkbox"/> Enable extended query | |
| Bind anonymous | <input checked="" type="checkbox"/> Use anonymous binds to resolve distinguished names | |
| User naming attribute | <input type="text" value="cn"/> | |
| Group naming attribute | <input type="text" value="cn"/> | |
| Group member attribute | <input type="text" value="member"/> | |
| RFC 2307 Groups | <input type="checkbox"/> LDAP Server uses RFC 2307 style group membership <small>RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).</small> | |
| Group Object Class | <input type="text" value="manager"/> <small>Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".</small> | |
| UTF8 Encode | <input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server. <small>Required to support international characters, but may not be supported by every LDAP server.</small> | |

Installation Freeraduis sur le pfsense :

- System
- Package Manager



PPE : Portail Captif

Verification des Packer disponible :

Available Packages

Recherche de freeradius2 :

freeradius2 net 1.7.3.2 A free implementation of the RADIUS protocol.
Support: MySQL, PostgreSQL, LDAP, Kerberos.
FreeRADIUS and FreeRADIUS2 settings are not compatible so don't use them together or try to update.
On pfSense docs there is a how-to which could help you on porting users.

Package Dependencies:
[bash-4.3.46_1](#) [freeradius2-2.2.9](#)

Puis installer

+ Install

Puis paramétrage du freeradius :

Services ▾ VPN ▾ St

Captive Portal

DHCP Relay

DHCP Server

DHCPv6 Relay

DHCPv6 Server & RA

DNS Forwarder

DNS Resolver

Dynamic DNS

FreeRADIUS

PPE : Portail Captif

2 paramétrage a effectuer LDAP puis NAS/client :

[NAS / Clients](#) [Interfaces](#) [Settings](#) [EAP](#) [SQL](#) [Certificates](#) [LDAP](#)

1. LDAP

- Activer le ldap
- Ip du serveur LDAP
- Identity : cn : « compte administrateur LDAP » dc « domaine »
- Password : *****
- Basedn : dc= « domaine »

| ENABLE LDAP SUPPORT - SERVER 1 | |
|------------------------------------|---|
| LDAP Authorization Support | <input checked="" type="checkbox"/> Enable LDAP For Authorization (Default: unchecked) Enables LDAP in the authorize section. The ldap module will set Auth-Type to LDAP if it has not already been set. |
| LDAP Authentication Support | <input checked="" type="checkbox"/> Enable LDAP For Authentication Enables LDAP in the authenticate section. Note that this means "check plain-text password against the ldap database", which means that EAP won't work, as it does not supply a plain-text password. |
| General Configuration - SERVER 1 | |
| Server | <input type="text" value="192.168.1.18"/> No description. (Default: ldap.your.domain) |
| Port | <input type="text" value="389"/> No description. (Default: 389) |
| Identity | <input type="text" value="cn=admin,dc=dineche"/> No description. (Default: cn=admin,o=My Org,c=UA) |
| Password | <input type="password" value="....."/> No description. (Default: mypass) |
| Basedn | <input type="text" value="dc=dineche"/> No description (Default: o=My Org,c=UA) |
| Filter | <input type="text" value="(uid=%(Stripped-User-Name)-%(User-Name))"/> No description. (Default: (uid=%(Stripped-User-Name)-%(User-Name))) |

2. NAS/Client

- Client IP address : ipseveur radius
- Client IP version IPV4
 - Information doit être similaire au serveur radius Ubuntu
- Client Shortname : « nom qui sera en liaison entre le serveur radius »
- Client Shared secret : « mots de passe qui sera mis sur le serveur freeradius »

| General Configuration | |
|-----------------------------|--|
| Client IP Address | <input type="text" value="192.168.1.18"/> Enter the IP address of the RADIUS client. This is the IP of the NAS (switch, access point, firewall, router, etc.). |
| Client IP Version | <input type="text" value="IPv4"/> |
| Client Shortname | <input type="text" value="admin"/> Enter a short name for the client. This is generally the hostname of the NAS. |
| Client Shared Secret | <input type="password" value="....."/> Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch or accesspoint) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret. |

PPE : Portail Captif

Installation Freeradius sur l'Ubuntu 16.0.4

En ligne de commande :

```
apt-get install freeradius freeradius-ldap
```

Puis paramètre le serveur freeradius il y aura plusieurs configurations à faire :

1. Modifier le client.conf

```
root@dineche:/etc/freeradius# nano /etc/freeradius/clients.conf
```

il y aura l'IP du serveur à ajouter (Pfsense)

```
client 192.168.1.1 {
    secret          = dineche
    shortname       = admin
}
```

2. Modifier la conf du ldap

```
root@dineche:/etc/freeradius# nano /etc/freeradius/modules/ldap
```

Pour modifier la configuration il faut décocher les commentaires puis rentrer les informations du serveur :

```
ldap {
    #
    # Note that this needs to match the name in the LDAP
    # server certificate, if you're using ldaps.
    server = "192.168.1.18"
    identity = "cn=admin,dc=dineche"
    password = dineche
    basedn = "dc=dineche"
    filter = "(uid=%{Stripped-User-Name}:-%{User-Name})"
    #base_filter = "(objectclass=radiusprofile)"
}
```

Puis on va commenter la ligne où c'est écrit files

Pour commenté il faut rajouter le dièse devant le mot

```
# files
```

Et on va décommenter Auth-type LDAP pour qu'il puisse communiquer :

```
Auth-Type LDAP {
    ldap
}
```

PPE : Portail Captif

3. Modifier le fichier Inner-tunnel

```
root@dineche:/etc/freeradius/modules# nano /etc/freeradius/sites-available/inner-tunnel
```

puis faire la meme manipulation que l'etape precedente

Puis on va commenter la ligne ou c'est ecrie files

Pour commenté ou des commenté il faut rajouter le dièse devant le mot

```
# files
```

Et on va des commenté Auth-type LDAP pour qu'il puisse communiquer :

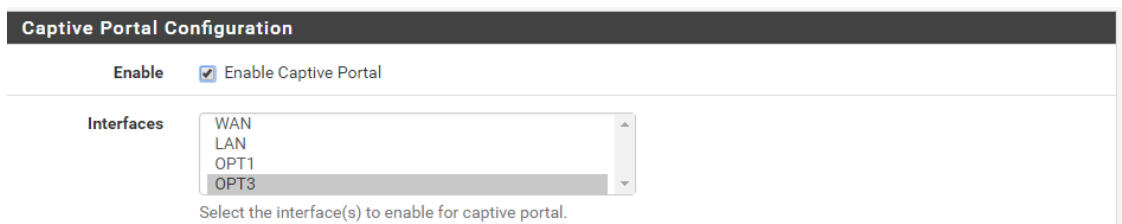
```
Auth-Type LDAP {  
    ldap  
}
```

Puis faire un restart du Freeradius afin que les configurations soient bien prises :

```
service freeradius resrtart
```

Puis crée un portail captif :

- Activer le portail
- Choisir l'interface du réseau



Captive Portal Configuration

Enable Enable Captive Portal

Interfaces
WAN
LAN
OPT1
OPT3

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

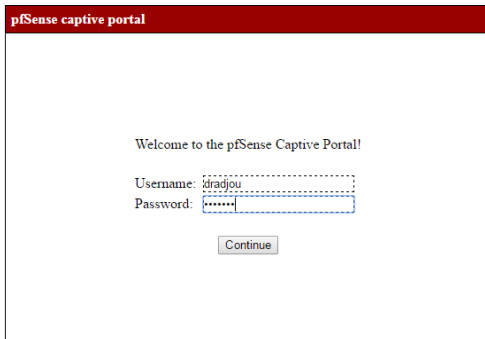
PPE : Portail Captif

On rentre les informations nécessaires :


- Authentication method : RADIUS Authentication
- RADIUS protocol : PAP (
- Primary RADIUS : (address du serveur freeradius linux)
- Port par default
- Mots de passe secret du Raduis : *****

| Authentication | | | |
|-------------------------------|---|--|---|
| Authentication method | <input type="radio"/> No Authentication | <input type="radio"/> Local User Manager / Vouchers | <input checked="" type="radio"/> RADIUS Authentication |
| RADIUS protocol | <input checked="" type="radio"/> PAP | <input type="radio"/> CHAP-MD5 | <input type="radio"/> MSCHAPv1 <input type="radio"/> MSCHAPv2 |
| Primary Authentication Source | | | |
| Primary RADIUS server | <input type="text" value="192.168.1.18"/> | <input type="text"/> | <input type="text" value="dineche"/> |
| Secondary RADIUS server | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| | <small>IP address of the RADIUS server to authenticate against.</small> | <small>RADIUS port. Leave blank for default (1812)</small> | <small>RADIUS shared secret. Leave blank to not use a shared secret (not recommended)</small> |

Puis effectuer un test :



Et vérifier sur Pfsense les historiques des user afin de vérifier que le login soit correct et visible par pfsense :

| Users Logged In (1) | | | | | |
|---------------------|-------------------|----------|---------------------|---------------------|---|
| IP address | MAC address | Username | Session start | Last activity | Actions |
| 192.168.3.3 | 08:00:27:fe:48:43 | dradjou | 11/03/2016 14:56:10 | 11/03/2016 14:56:13 |  |