

Nous utiliserons PfSense 2.3.2 qui est la dernière version. Nous lui allouons une capacité d'image de 700 Mb minimum afin de lui permettre de bien fonctionner pour son interface.

**Afin de réaliser le portail captif il nous faudra une configuration des cartes réseaux de la sorte :**

**Réseau 1 WAN :**            **Pour pouvoir avoir internet**

Activer la carte réseau  
Mode d'accès réseau : Accès par pont ▼

**Réseau 2 LAN :**            **Pour utiliser notre machine physique**

Activer la carte réseau  
Mode d'accès réseau : Réseau privé hôte ▼

**Réseau 3 OPT1 :**            **Pour l'assigner au portail captif**

Activer la carte réseau  
Mode d'accès réseau : Réseau interne ▼

Par la suite il faudra configurer la carte réseau **WAN** qui obtiendra une adresse IP via le DHCP du réseau internet, pour la carte réseau **LAN** nous lui assignerons une adresse IP puis la configurons sur un DHCP, enfin **OPT1** nous pourrons la configurer via le terminal *PFSENSE* ou sur son interface graphique, en allant dans la machine administrateur puis sur l'adresse IP de **LAN**. Elle assignera une adresse IP via le DHCP.

Une fois les adresse IP configurer nous devrions obtenir (selon votre configuration) ceci :

```
WAN (wan)      -> em0          -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2          -> v4: 192.168.10.1/24
```

Afin de vérifier votre connexion internet nous pourrons tenter un PING vers Google en appuyant sur la touche **7** puis en entrant l'adresse **8.8.8.8** ou **8.8.4.4**.

```
Enter an option: 7
Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=45 time=80.767 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=45 time=94.874 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=45 time=71.507 ms
```

## Paramétrage Active Directory

Nous utiliserons Pfsense avec authentification Active Directory, afin de créer directement des user dans la base de données Windows Server 2008 R2. Pfsense récupèrera les user dans la forêt créée sur Windows Server.

### Sur Pfsense :

Il faudra pour activer la connexion sous AD, nous devons aller dans **Service/System/CaptivPortal** il faudra cocher la case **Authentification RADIUS** puis dans **protocole RADIUS** il faudra sélectionner **MSCHAPv2**.

Ensuite dans **Primary Authentication Sourcer** puis remplir dans **Serveur RADIUS primaire** l'adresse IP de la machine **Windows Server**, puis à coter il faudra entre le mot de passe entré dans la création de l'AD (register secret).

Authentification				
Méthode d'authentification	<input type="radio"/> Pas d'authentification	<input type="radio"/> Local User Manager / Coupons	<input checked="" type="radio"/> authentification RADIUS	
protocole RADIUS	<input type="radio"/> BOUILLIE	<input type="radio"/> CHAP-MD5	<input type="radio"/> MSCHAPv1	<input checked="" type="radio"/> MSCHAPv2
Primary Authentication Source				
serveur RADIUS primaire	<input type="text" value="192.168.1.2"/>	<input type="text"/>	<input type="text" value="you"/>	
serveur RADIUS secondaire	<input type="text"/>	<input type="text"/>	<input type="text"/>	
	adresse IP du serveur RADIUS pour authentifier contre.	Port RADIUS. Laissez vide par défaut (1812)	RADIUS secret partagé. Laissez vide pour ne pas utiliser un secret partagé (non recommandé)	

Par la suite nous devons remplir dans **System/Package/FreeRADIUS : LDAP/LDAP**, il faudra cocher les deux premières cases ensuite rentré l'adresse IP du serveur dans la case **Server**, puis rentrer le mot de passe que nous avons configuré dans **Password** puis enfin, dans la case **Filter** il faudra supprimer **uid** et remplacer par **samAccount**.

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="192.168.1.2"/> No description. (Default: ldap.your.domain)
Port	<input type="text" value="389"/> No description. (Default: 389)
Identity	<input type="text" value="cn=admin,o=My Org,c=UA"/> No description. (Default: cn=admin,o=My Org,c=UA)
Password	<input type="text" value="....."/> No description. (Default: mypass)
Basedn	<input type="text" value="o=My Org,c=UA"/> No description (Default: o=My Org,c=UA)
Filter	<input type="text" value="(samAccount=%{%Stripped-User-Name}-%{User-Name})"/> No description. (Default: (uid=%{%Stripped-User-Name}-%{User-Name}))

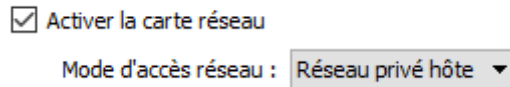
Maintenant dans **Service/FreeRADIUS : Client/Edit/Nas/Clients** nous devons configurer l'adresse IP du client soit l'adresse IP du PfSense. Puis dans **Client Shortname** le nom de l'Active Directory rentré dans Windows Server soit **youad** pour moi.

General Configuration	
<b>Client IP Address</b>	<input type="text" value="192.168.1.1"/> Enter the IP address of the RADIUS client. This is the IP of the NAS (switch, access po
<b>Client IP Version</b>	<input type="text" value="IPv4"/>
<b>Client Shortname</b>	<input type="text" value="youad"/> Enter a short name for the client. This is generally the hostname of the NAS.
<b>Client Shared Secret</b>	<input type="text" value="..."/> Enter the shared secret of the RADIUS client here. This is the shared secret (password with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret.

## Configuration Windows Server 2008 R2 :

La machine devra disposer de cette configuration :

**Réseau 1 LAN :** *Comme nous utilisons notre machine PfSense sur machine physique nous mettrons cette configuration afin que la connexion fonctionne.*



Il faudra configurer l'adresse IP de la machine afin qu'elle soit sur le même réseau que le portail PfSense.

Connexion au réseau local 192.168.1.2, Compatible IPv6  
2 :

Ensuite il faudra créer une **Forêt Active Directory**. Une fois créer nous devrions pouvoir voir notre domaine créer dans le **Répertoire Tacher de Configuration Initiales**.

Domaine : pfsense.you

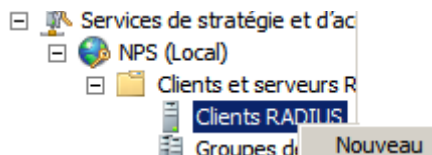
Il faudra ensuite créer un nouveau rôle puis dans **Rôles de serveurs**, nous sélectionnerons  **Services de stratégie et d'accès réseau**.

Maintenant il faudra cliquer sur suivant pour continuer puis dans **Services de rôle**, sélectionner  **Serveur NPS (Network Policy Server)** puis cliquer sur Suivant et enfin sur **Installer**.

Arriver à ce stade :



Nous pourrons quitter et puis aller dans **Services de stratégie**, double cliquer sur : **NPS (local)**, **Clients et serveurs Radius** et puis cliquer Droit sur **Client RADIUS** et cliquer sur nouveau.



Après avoir cliqué sur **Nouveau** il faudra remplir les champs libres. Le nom convivial sera le nom du répertoire ou les user seront répertoriés. Ensuite remplir l'adresse IP sur **PareFeu PfSense**. Et enfin remplir le **Secret partagé** que nous rentrerons dans les réglages **RADIUS** du portail captif.

**Nouveau client RADIUS**

Paramètres | Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :  
youad

Adresse (IP ou DNS) :  
192.168.1.1

Secret partagé

Sélectionnez un modèle de secrets partagés existant :  
Aucun

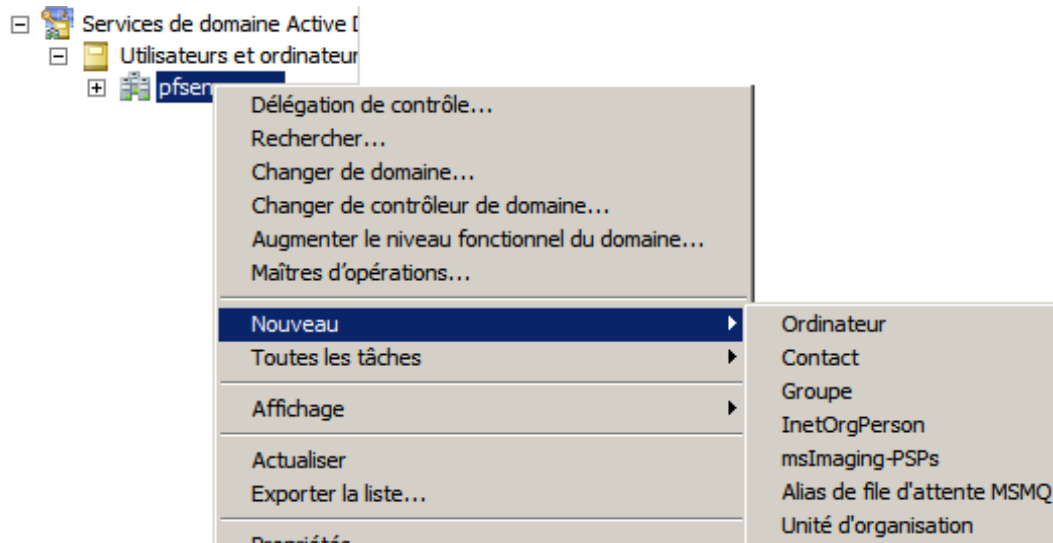
Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel  Générer

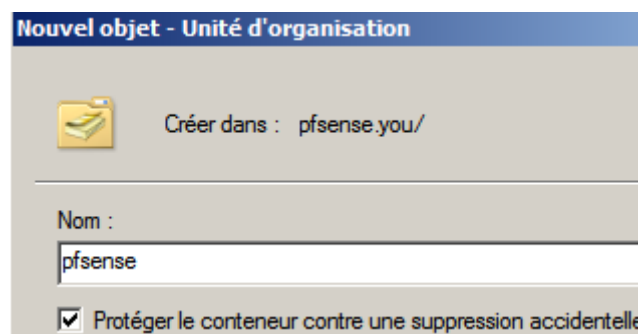
Secret partagé :  
●●●

Confirmez le secret partagé :  
●●●

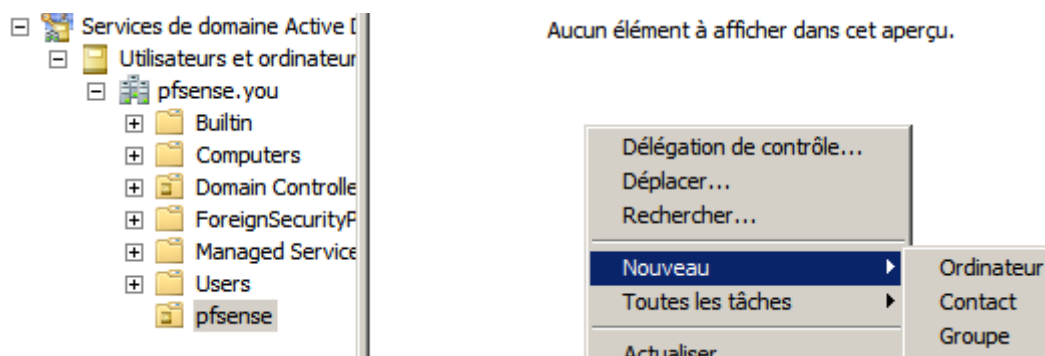
Maintenant il faudra aller sur **Services de domaine Active Directory** puis **utilisateurs et ordinateurs** ensuite le **nom** de notre **domaine** il faudra **cliquer Droit** dessus ensuite sélectionner **Unité d'organisation**.



Ensuite nous rentrerons le **nom** de l'Unité organisationnelle.



Dorénavant nous devons aller dans **Services de domaine Active Directory** puis **utilisateurs et ordinateurs** ensuite double cliquer sur le nom de notre **Forêt** ensuite cliquer sur notre nom de **domaine** et enfin dans le vide blanc **Cliquer Droit** et faire **Nouveau > Groupe**.



Configuré votre nom de groupe avec les cases sélectionnées tel quelle :

Nom du groupe :  
yougrp

Nom de groupe (antérieur à Windows 2000) :  
yougrp

Étendue du groupe

- Domaine local
- Globale
- Universelle

Type de groupe

- Sécurité
- Distribution

Nous cliquerons sur suivant ensuite il faudra sélectionner le **groupe à partager** en **vérifiant** les noms et appuyer sur **Ok**.

Sélectionnez des groupes

Sélectionnez le type de cet objet :  
des groupes ou Entités de sécurité intégrées

À partir de cet emplacement :  
pfsense.you

Entrez les noms des objets à sélectionner (exemples) :  
yougrp

Avancé... OK Annuler

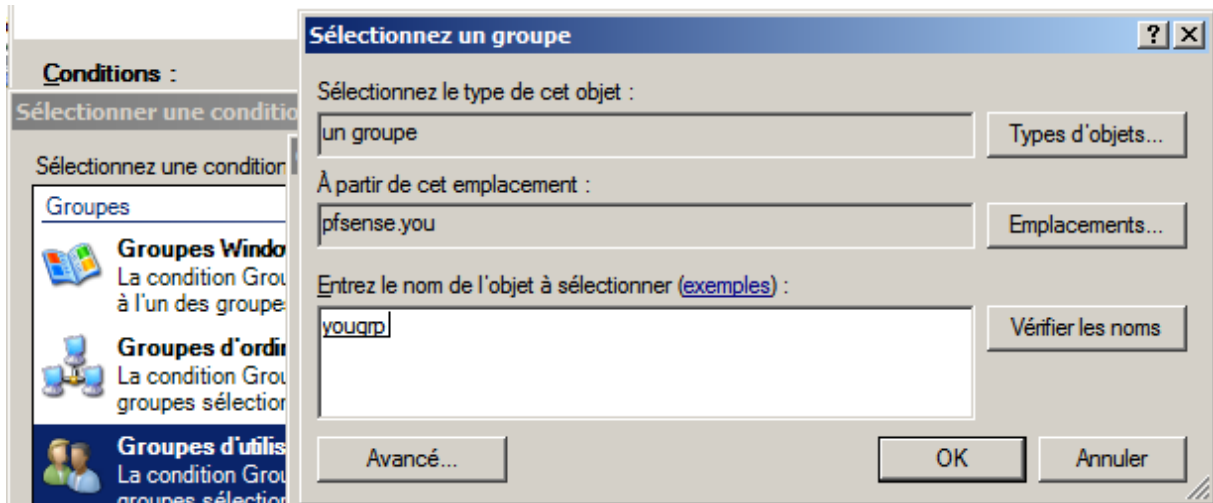
### Stratégie Réseau

Nous entrerons ensuite le nom de la stratégie pour le portail captif :

Nom de la stratégie :  
youad

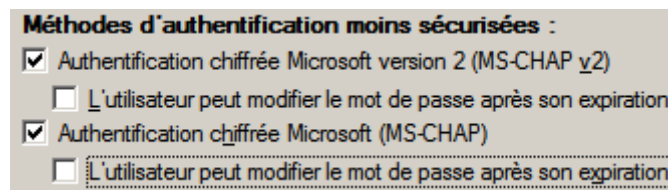
**NTPS > Stratégie Réseau > Nouveau**

Maintenant il faudra sélectionner un groupe d'utilisateur à partir de la forêt.



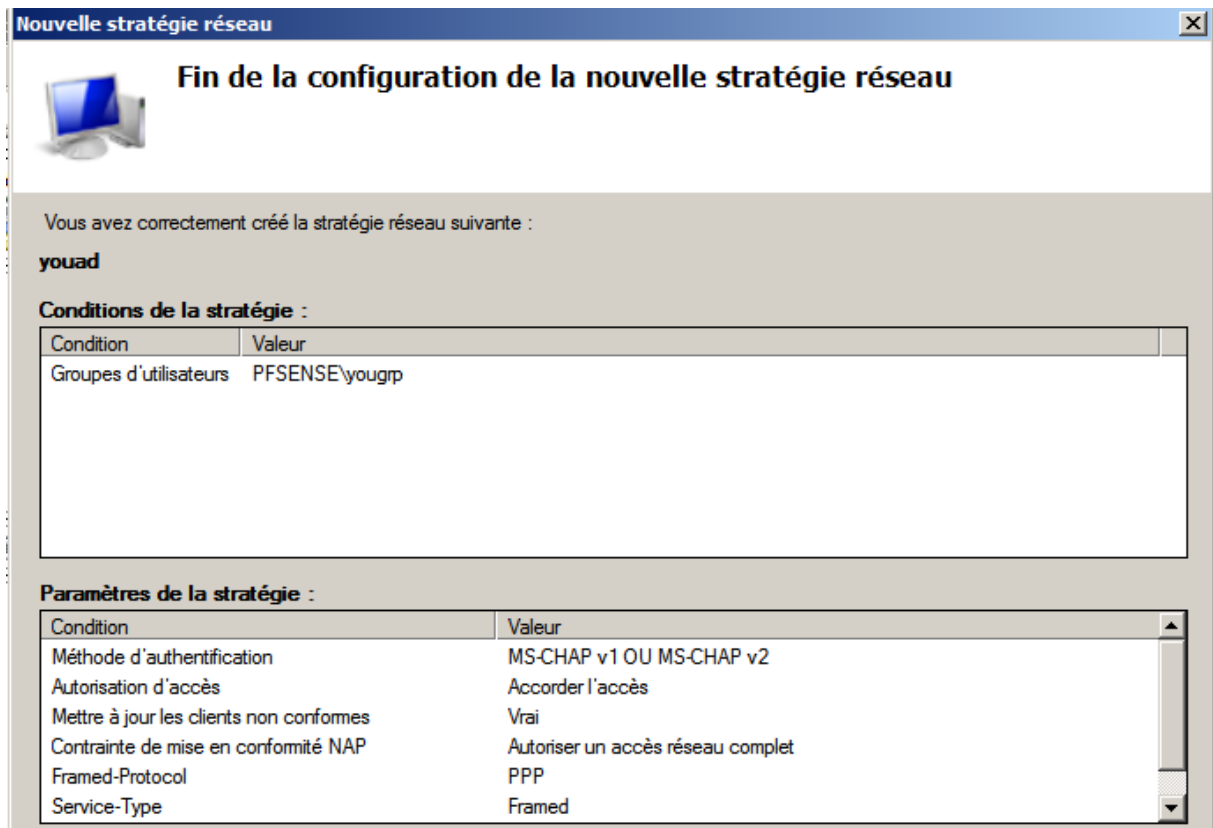
Il faudra sélectionner  Accès accordé et puis poursuivre.

Maintenant il faudra désélectionner les deux sous cases. Pour que l'utilisateur soit limité niveau droit.





Nous devrions au final obtenir cette page :



**Nouvelle stratégie réseau**

### Fin de la configuration de la nouvelle stratégie réseau

Vous avez correctement créé la stratégie réseau suivante :

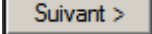
**youad**

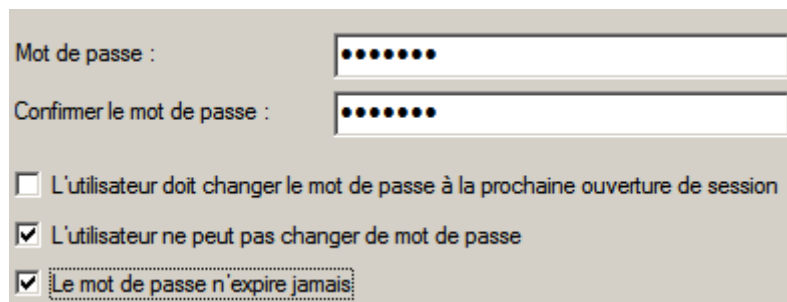
**Conditions de la stratégie :**

Condition	Valeur
Groupes d'utilisateurs	PFSENSE\yougrp

**Paramètres de la stratégie :**

Condition	Valeur
Méthode d'authentification	MS-CHAP v1 OU MS-CHAP v2
Autorisation d'accès	Accorder l'accès
Mettre à jour les clients non conformes	Vrai
Contrainte de mise en conformité NAP	Autoriser un accès réseau complet
Framed-Protocol	PPP
Service-Type	Framed

Ensuite nous créerons un user et cliquerons sur  et puis configurerons les mots de passe.



Mot de passe :

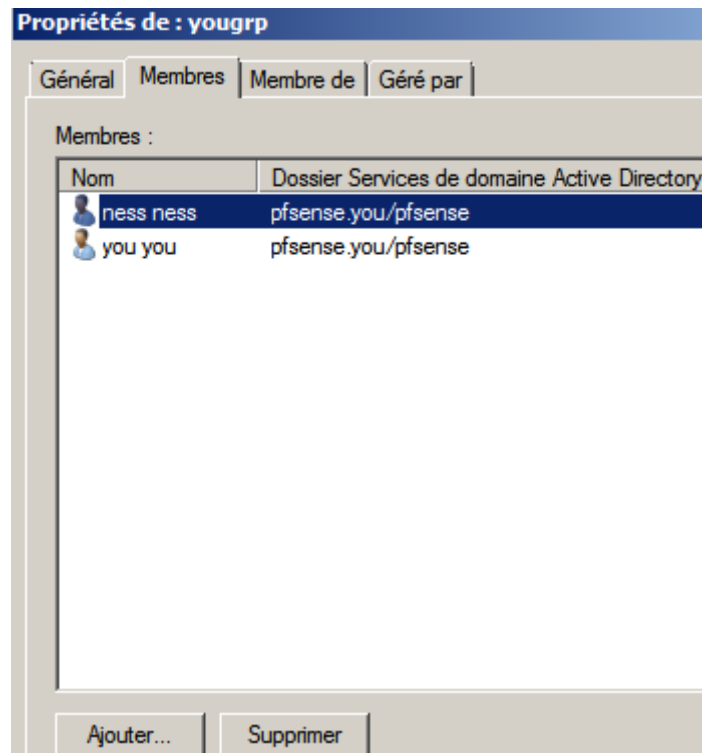
Confirmer le mot de passe :

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

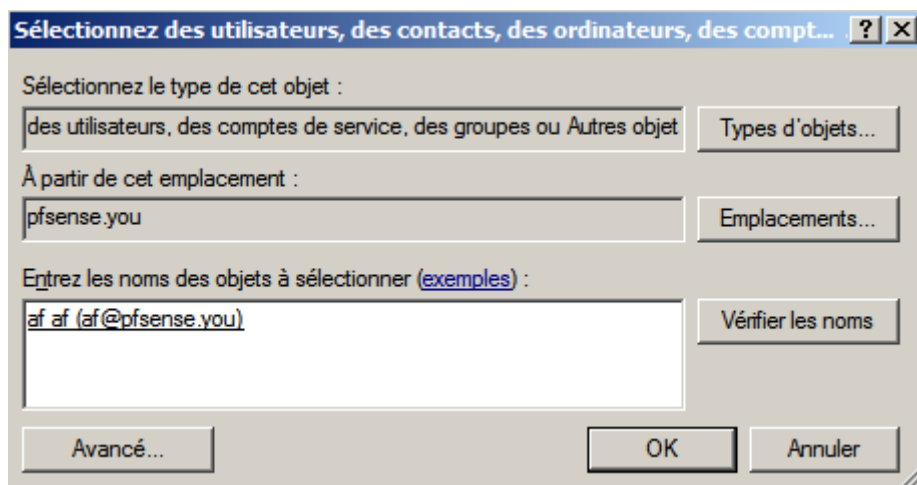
L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Nous devons assigner cette user au groupe partagé pour qu'un client puisse utiliser l'utilisateur pour se connecter. Pour cela il faut double-cliquer sur le groupe ensuite aller dans l'onglet **Membre** et cliquer sur ajouter.



Il faudra rentrer le nom et vérifier les noms et puis cliquer sur Ok puis **Appliquer** et enfin **Ok** :



Et enfin il faudra démarrer le Services système pour activer la connexion avec la machine via le RADIUS. Et puis faire le test.

