

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
```

Configuration machine Ubuntu LDAP :

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

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

Nous configurerons maintenant les adresses IP de la machine afin d'y mettre une adresse IP en statique et configurer un DHCP.

```
GNU nano 2.5.3      Fichier : /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s8
iface enp0s8 inet static
address 192.168.1.3
netmask 255.255.255.0

auto enp0s3
iface enp0s3 inet dhcp
```

Nous devons configurer maintenant les adresse IP DHCP de la machine dans le menu **nano /etc/dhcpd.conf**.

```
GNU nano 2.5.3      Fichier : /etc/dhcpd.conf
network 192.168.2.1
netmask 255.255.255.0
gateway 192.168.2.1_
```

Ensuite nous irons dans le répertoire **/etc/ldap/ldap.conf** afin de le configurer pour pouvoir atteindre la page de connexion **LDAP**, modifier dans la ligne **BASE** supprimer les **#** et ensuite pour permettre la connexion entrer (**ldap://xxx.xxx.xxx.xxx:389/phpldapadmin**).

```
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE      dc=you,dc=ness
URI       ldap://192.168.1.3:389

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT     /etc/ssl/certs/ca-certificates.crt
```

Maintenant nous devons aller dans le répertoire du LDAP dans le `/etc/phpldapadmin/config.php` puis, changer certaines lignes par celles-ci :

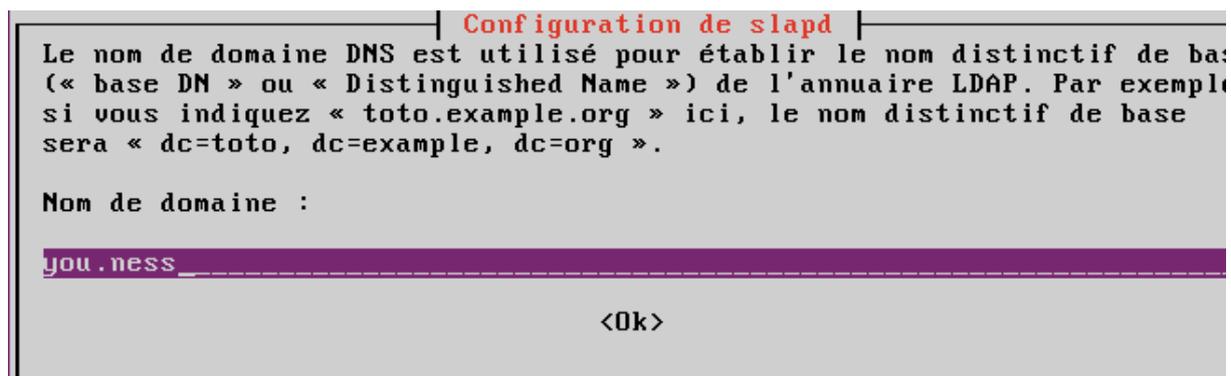
La première est pour permettre la **connexion au post (host)**.

La deuxième et quatrième pour les **identifiants de connexion(login)**.

La troisième est pour la **connexion server**.

```
GNU nano 2.5.3      Fichier : /etc/phpldapadmin/config.php
$servers->setValue('server','host','192.168.1.3');
$servers->setValue('login','bind_id','cn=admin,dc=you,dc=ness');
$servers->setValue('server','base',array('dc=you,dc=ness'));
$servers->setValue('login','bind_id','cn=admin,dc=you,dc=ness');
// $config->custom->appearance['hide_template_warning'] = true;
```

Il faudra ensuite taper `sudo dkpg-reconfigure slapd` puis, dedans nous taperons le nom de notre domaine pour permettre la connexion. Nous devons ensuite lancer la configuration sélectionner le **HBD**, ne pas supprimer les données et appliquer les modifications.



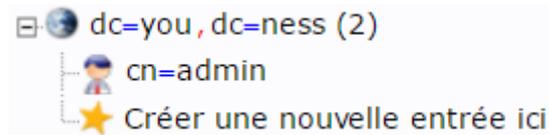
Ensuite il faudra configurer les **mots de passe**, nous devons ensuite lancer la configuration sélectionner le **HBD**, ne pas **supprimer la base de données** et **appliquer les modifications sur l'ancienne base de données** puis enfin, **autoriser le protocole LDAP v2**.

Nous devrions maintenant pouvoir obtenir cette page d'authentification :

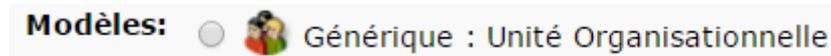


Création User :

Afin de créer un user nous devons aller dans le compte **Admin** puis dans **Créer une nouvelle entrée ici**.



Ensuite nous sélectionnerons dans **Modèles** cette icone :



Puis il faudra entrer le nom puis valider et nous devrions obtenir ceci comme résultat :

Attribut	Nouvelle valeur	Passer
ou=YouOrgaa,dc=you,dc=ness		
objectClass	organizationalUnit	<input type="checkbox"/>
Organisational Unit	YouOrgaa	<input type="checkbox"/>

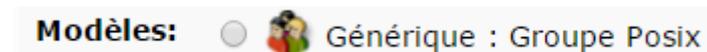
Maintenant nous cliquerons sur pour confirmer la création.

Ceci nous permettra de créer un groupe qui ensuite dedans recréerons un **Groupe Posix** afin de créer des User.

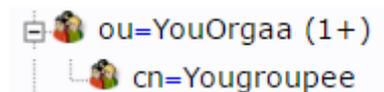
Une fois réalisé il faudra aller sur le nom du **Générique** créée puis sur :

★ [Créer une sous-entrée](#)

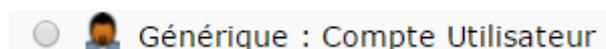
Et enfin sélectionner Groupe Posix, ensuite créer le nom de groupe qui nous permettra ensuite d'y créer un utilisateur à l'intérieur.



Une fois créée il faudra cliquer sur le  du **Générique** puis cliquer sur le nom du **Groupe** et enfin sur **créer une sous-entrée**.



Afin de créer l'utilisateur il faudra maintenant cliquer sur **Générique : Compte utilisateur**.



Une fois dedans il faudra remplir les cases vides (Les cases avec une * doivent être obligatoirement rempli) une fois fini valider sur [Créer un objet](#) .

Nom Commun	alias, requis, rdn
<input type="text" value="Ness Af"/>	*
Prénom	alias
<input type="text" value="Ness"/>	
GID	alias, requis, astuce
<input type="text" value="Yougroupee"/>	*
Répertoire personnel	alias, requis
<input type="text" value="/home/users/naf"/>	*
Nom de famille	alias, requis
<input type="text" value="Af"/>	*
Login shell	alias
<input type="text" value="/bin/sh"/>	
Mot de passe	alias, astuce
<input type="password" value="....."/> <input type="text" value="md5"/>	
<input type="password" value="....."/> (confirmer)	
Vérifier le mot de passe...	
UID	alias, requis, astuce, ro
<input type="text" value="1000"/>	
ID utilisateur	alias, requis
<input type="text" value="naf"/>	*

GID est le groupe dans lequel nous voulons créer l'utilisateur.

Répertoire Personnel est le répertoire des utilisateurs.

UID est le numéro d'ID de l'utilisateur.

Paramétrage LDAP :

Dans l'invite de commande nous devons installer **FreeRadius** en tapant **apt-get install freeradius freeradius-ldap**.

Il faudra retourner sur la machine Ubuntu puis taper **nano /etc/freeradius/sites-available/default**, pour faciliter les choses appuyer sur **CTRL 8** puis saisir la ligne 170 et il faudra y rajouter un #.

```
# files
```

Ensuite à la ligne **188** il faudra supprimer le # pour décommenter le **LDAP**.

```
_ ldap
```

Puis à la ligne **304** il faudra décommenté encore une fois les 3 lignes

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

Maintenant il nous faudra taper **nano /etc/freeradius/modules/ldap** puis dedans nous devons décommenté et puis rentrer nos informations selon votre configuration. Afin de permettre la connexion.

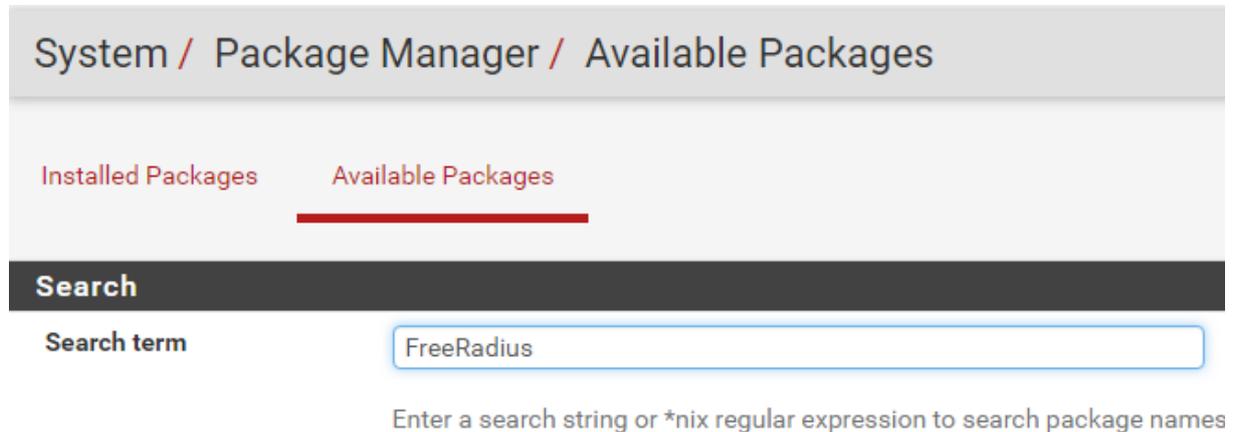
```
ldap {
    #
    # Note that this needs to match the name in the LDAP
    # server certificate, if you're using ldaps.
    server = "192.168.1.3"
    identity = "cn=admin,dc=you,dc=ness"
    password = you
    basedn = "dc=you,dc=ness"
    filter = "(uid=%{{Stripped-User-Name}}:-{{User-Name}})"
    #base filter = "(objectclass=radiusprofile)"
}
```

Dans le fichier **nano /etc/freeradius/client.conf** nous ajouterons l'adresse IP cliente du pfsense avec le **secret** et **shortname** à retenir pour le **PfSense**.

```
client 192.168.1.1 {
    secret = you
    shortname = pfsense
}
```

Activer portail captif avec authentification LDAP :

Dans le portail captif il nous faudra aller dans **System/PackageManager/AvailablePackages** puis dans **Available Packages** ensuite dans Search term taper **FreeRADIUS** et enfin cliquer sur .



System / Package Manager / Available Packages

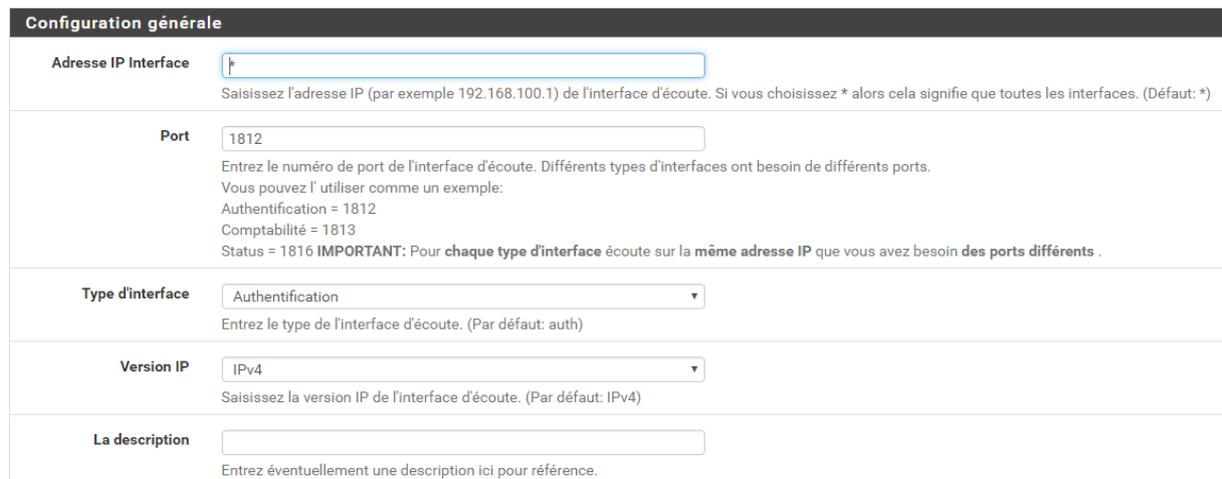
Installed Packages Available Packages

Search

Search term

Enter a search string or *nix regular expression to search package names

Ensuite dans le portail captif il faudra accéder à l'interface dans les onglets **Service/FreeRADIUS/Interfaces**, il ne faudra toucher à rien, laisser par défaut et simplement cliquer sur .



Configuration générale

Adresse IP Interface

Saisissez l'adresse IP (par exemple 192.168.100.1) de l'interface d'écoute. Si vous choisissez * alors cela signifie que toutes les interfaces. (Défaut: *)

Port

Entrez le numéro de port de l'interface d'écoute. Différents types d'interfaces ont besoin de différents ports. Vous pouvez l'utiliser comme un exemple:
Authentification = 1812
Comptabilité = 1813
Status = 1816 **IMPORTANT:** Pour chaque type d'interface écoute sur la même adresse IP que vous avez besoin des ports différents .

Type d'interface

Entrez le type de l'interface d'écoute. (Par défaut: auth)

Version IP

Saisissez la version IP de l'interface d'écoute. (Par défaut: IPv4)

La description

Entrez éventuellement une description ici pour référence.

Une fois réalisé il faudra ensuite aller dans la rubrique **LDAP** et puis sélectionner les 2 cases et puis rentrer l'adresse IP du serveur.

Activer le support LDAP - SERVEUR 1	
Soutien LDAP Autorisation	<input checked="" type="checkbox"/> Activer LDAP pour l'autorisation (par défaut: décochée) Active LDAP dans la section autorisent. Le module ldap établira Auth-Type à LDAP si elle n'a pas déjà été défini.
Soutien d'authentification LDAP	<input checked="" type="checkbox"/> Activer LDAP pour l'authentification Active LDAP dans la section authenticate. Notez que cela signifie "vérifier le mot de passe en texte clair contre la base de données ldap", ce qui signifie que le PAE ne fonctionnera pas, car il ne fournit pas un mot de passe en texte clair.
Configuration générale - SERVEUR 1	
Serveur	<input type="text" value="192.168.1.3"/> Pas de description. (Par défaut: ldap.your.domain)
Port	<input type="text" value="389"/> Pas de description. (Par défaut: 389)
Identité	<input type="text" value="cn=admin,dc=you,dc=ness"/> Pas de description. (Par défaut: cn = admin, o = Ma Org, c = UA)
Mot de passe	<input type="text" value="..."/> Pas de description. (Par défaut: mypass)
baseDN	<input type="text" value="dc=you,dc=ness"/>

Maintenant dans **Service/CaptivePortal** il nous faudra activer le mode **RADIUS Authentification** puis et RADIUS Protocol cocher PAP afin de permettre la connexion entre eux. Ensuite il faudra rentrer l'adresse IP du server et rentrer le mot de passe dans **secret**.

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="192.168.1.3"/>	<input type="text"/>	<input type="text" value="you"/>
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)

Il ne nous restera plus qu'à tester la connexion.

