V.P.N. sous MacOs

Table des matières

Introduction aux Réseaux Privés Virtuels

L'objectif d'un VPN est simple. Il s'agit de sécuriser des échanges de données en utilisant comme support un réseau non sécurisé comme par exemple le réseau Internet. Un VPN est également un bon candidat pour la sécurisation de flux informatiques à travers un réseau WIFI.

Définition d'un VPN (Virtual Private Network) :

Décomposons l'expression VPN.

Network : un réseau est constitué de plusieurs machines qui peuvent communiquer entre elles d'une façon ou d'une autre. Ces machines peuvent être dans un même endroit physiquement ou dispersées, et les méthodes de communication sont diverses.

Private : privé veut dire que les communications entre deux ou plusieurs machines sont secrètes et donc inaccessibles pour une machine ne participant pas à la communication privée.

Virtual : dans le concept de virtuel, nous retiendrons l'émulation d'une fonction d'un objet qui n'est pas vraiment là. Un réseau virtuel n'est pas un réseau physique, mais émuler pour faire croire à un réseau physique.

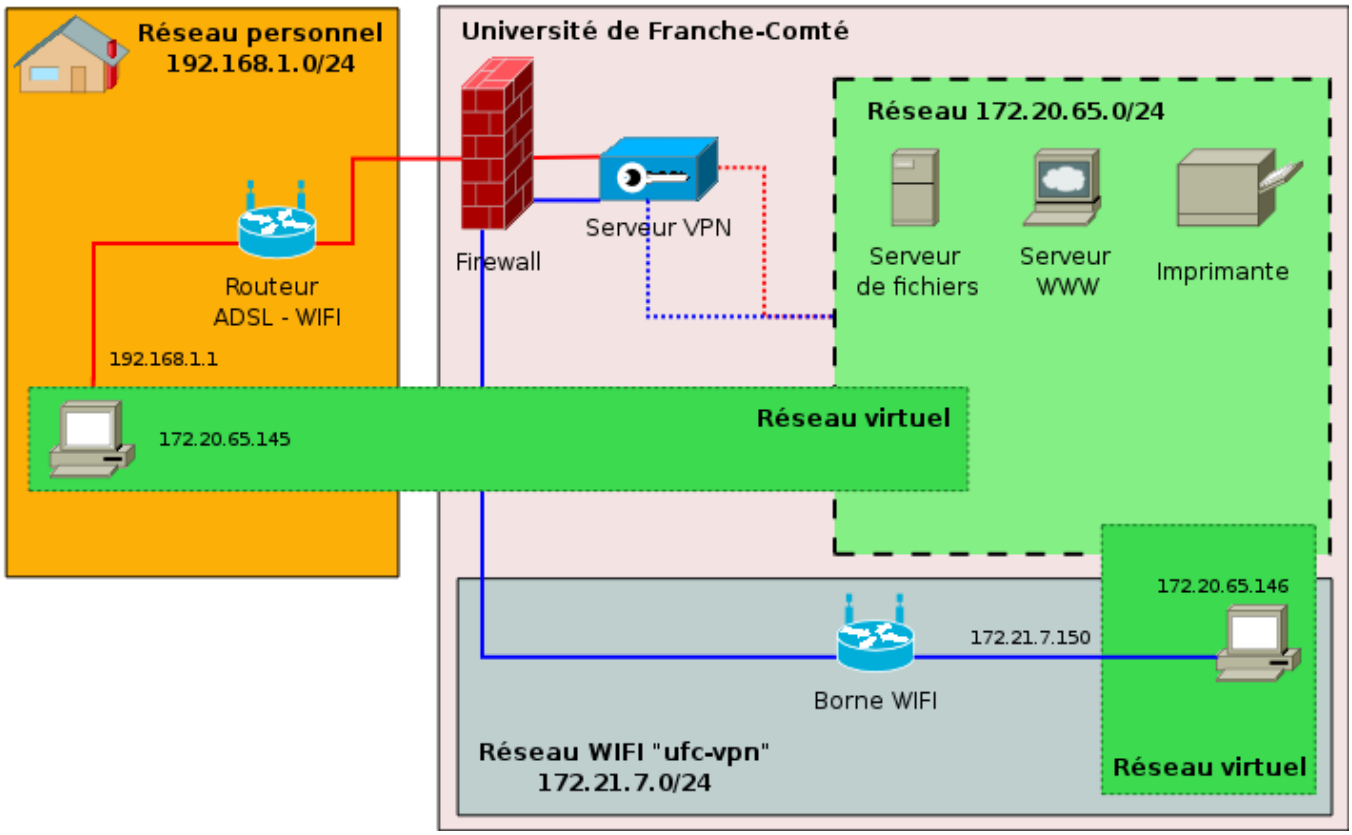
Un réseau privé virtuel est donc l'association de ces trois concepts. Une fois en place, il vous offre la possibilité d'utiliser un réseau public non sécurisé pour créer un réseau privé (données cryptées) et y faire circuler des données.

Quelques explications :

En général, les RPV permettent à des utilisateurs de se servir de leur connexion Internet de type ADSL pour accéder à leur réseau professionnel de manière transparente. Un fois connecté, l'utilisateur peut atteindre les ressources (espaces disques, imprimantes, etc) fournies par ce réseau.

Dans le schéma ci-dessous, nous voyons un utilisateur travaillant depuis son ordinateur personnel. Il emprunte donc son accès Internet personnel pour se connecter à travers un VPN à son réseau universitaire. Les traits rouges montrent les liens physiques réels. La zone « Réseau virtuel » montre le réseau virtuel mis en place entre son domicile et le réseau interne après l'établissement de la connexion.

Une autre connexion est établie entre un poste utilisant le réseau WIFI universitaire. L'utilisation du réseau WIFI "ufc-vpn" permet de créer un réseau virtuel entre ce poste nomade et un réseau interne. Tout comme le premier exemple, le poste fait partie du réseau interne et peut user de toutes les ressources mises à sa disposition.



Quelles possibilités pour le VPN ?

Concrètement, que pourra faire l'utilisateur accédant au réseau de l'UFC en utilisant le VPN ?

Tout simplement, exactement ce qu'il peut faire sur son PC lorsque celui-ci est branché physiquement au réseau lorsqu'il est au bureau, par exemple récupérer ses courriers électroniques sur le serveur de messagerie, consulter des sites Intranet (ceux qui ne sont pas accessibles depuis l'extérieur de l'UFC), accéder à ses fichiers sur les serveurs de fichiers, etc. Tout ceci via Internet et de façon

sécurisée.

La sécurité du VPN mise en place à l'UFC dépend de trois éléments :

- l’authentification machine ;
- le cryptage des données ;
- l'authentification de l'utilisateur.

L’authentification machine : les deux machines s’assurent mutuellement qu’elles ont les droits pour communiquer entre elles (vérification du certificat).

Le cryptage des données s'effectue par l'échange de clefs.

L'authentification de l'utilisateur est faite à travers l'annuaire LDAP de l'UFC ou d'un serveur d'authentification cascadé (laboratoires, UFR ...).

Parmi les termes fréquemment employés, nous retrouverons « realm », « certificat ».

Royaume : « realm »

Un « royaume » (« realm » dans le monde de Radius) est, d'une manière plus restrictive pour le projet VPN de l'UFC, l'association d'un nom vis à vis d'un réseau de l'UFC.

Lors d'une connexion VPN, vous indiquerez le « realm » auquel vous voulez rattacher votre session VPN.

Par exemple, si je crée une session VPN avec l'identifiant « monNom@lifc-edu » et que je suis autorisé à me connecter sur le « realm » « @lifc-edu », ma machine obtiendra une adresse IP du réseau « lifc-edu », c'est-à-dire, une adresse dans le réseau 172.20.128.0/24.

Qui fait une demande de « realm » ?

Les demandes de « realms » seront effectuées par les correspondants réseaux de l'UFC. Le CRI étudiera avec eux les besoins et créera si nécessaire le « realm » proposé.

La création d'un « realm » est une opération lourde et ne se justifie que pour des besoins importants.

Quels sont les « realms » actifs ?

Pour l'ensemble des personnels et étudiants de l'Université de Franche-Comté, il existe un « realm » par défaut « @ufc » qui donne accès à un réseau interne de l'UFC, comme le faisait le service du PPP.

Pour les laboratoires, des royaumes spécifiques sont créés, en voici quelques exemples :

à Besançon :

« @lifc-edu »	sur le réseau 172.20.128.0/24 (vlan 7)
« @lifc-lab »	sur le réseau 172.20.65.0/24 (vlan 9)
« @femto-st »	sur le réseau 172.20.208.64/26 (vlan 44)

à Montbéliard et Belfort :

« @iutbm»

Obtenir un certificat, des droits

L'utilisation du VPN n'est pas anonyme, ni anodine. Ce service vous permet de vous connecter dans l'un des réseaux de l'Université de Franche-Comté depuis n'importe quel réseau extérieur ayant la possibilité de créer un VPN IPSEC (protocole ESP).

Cette connexion doit s'établir sans problème depuis chez vous ou depuis un accès WiFi (SSID ufc-vpn) de l'UFC.

Vos droits s'acquièrent en deux phases :

1) récupérer un certificat pour accéder à la machine VPN ;
2) obtenir des droits sur un « realm ».

Rencontrer son correspondant réseau/wifi

Il est impératif que votre demande de certificat passe par le correspondant informatique de votre laboratoire ou de votre UFR, car il nous faut des renseignements sur votre identité et la machine pour laquelle le certificat sera délivré (PC windows/linux, MacOs).

Délivrance du certificat

Le certificat est généré par le CRI qui le fournira directement à l'utilisateur ou au correspondant réseau. Ce certificat de machine permet ensuite à la machine sur lequel il est installé, de se connecter et surtout d'être reconnu par le serveur VPN comme une machine valide.

Vous pouvez installer un même certificat sur plusieurs machines, mais une seule à la fois pourra effectuer une connexion sur le serveur VPN. Si vous avez des besoins multiples, il faudra demander plusieurs certificats.

Droits

Les droits sont attribués par le correspondant réseau qui est en charge des « realms » qui lui sont confiés. Le CRI pourra aussi vous attribuer des droits, mais ne le fera que sur le « realm » générique « @ufc ».

Les serveurs VPN en usage à l'UFC

• le serveur de Besançon	vpn1	194.57.91.250	actif début juin 2008
• le serveur de Montbéliard	vpn2	194.57.89.97	actif début juin 2008
• le serveur de Belfort	vpn3	194.57.89.105	actif début juin 2008

Création de la connexion réseau V.P.N. sous MacOs Tiger

Attention, pour que votre connexion fonctionne, **il faut impérativement que vous ayez reçu votre certificat**.

Pour cela, veuillez suivre la procédure de remise des certificats comme indiquée page précédente et le chapitre page pour sa mise en place.

Les tests de connexions ont été réalisés avec succès en utilisant les versions 10.4 (aucune mise à jour installée) et 10.4.11 (toutes les mises installées à la date des tests).

Importation du certificat P12

La première étape consiste à importer le certificat machine fourni par le CRI. Ce certificat devra être importé en étant identifié comme l'utilisateur `root`. Nous ouvrons donc un terminal **Applications - Utilitaires - Terminal** puis nous appelons l'application **Keychain Access** :

```
# sudo "/Applications/Utilities/Keychain Access.app/Contents/MacOS/Keychain Access"
```

Nous donnons notre mot de passe et la boîte **Trousseau d'accès** s'affiche. Nous commençons l'importation en passant par le menu **Fichier - Importer**. Le trousseau à sélectionner est **Système**. Le certificat que nous allons importer s'appelle `tiger.p12` :

Une boîte d'authentification s'affiche et attend un mot de passe que nous devrions avoir en notre possession. Ce mot de passe est nécessaire pour pouvoir utiliser le certificat. Si nous ne l'avons pas, nous devons en faire la demande à l'émetteur du certificat :

Après avoir correctement renseigné la boîte, nous revenons au trousseau d'accès :

Plusieurs fichiers apparaissent maintenant dans notre trousseau **Système**. Avec un cliqué-glissé, nous déplaçons le fichier `LIFC Root CA` dans le trousseau **X509Anchors**.

Si nous constatons une différence entre l'affichage que nous obtenons et l'image ci-dessus en ce qui concerne la validité du certificat, nous devrons indiquer à notre système de toujours approuver le certificat. Pour réaliser cette opération, nous

double-cliquons sur le fichier `tiger` puis nous développons l'option **Réglages de confiance** :

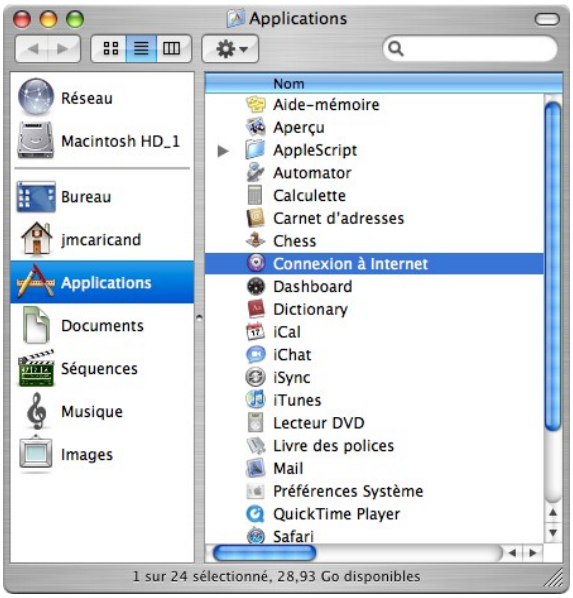
Dans la liste **Lors de l'utilisation de ce certificat** nous sélectionnons l'option **Toujours approuver**. Nous refermons cette boîte.

Nous sélectionnons le trousseau **X509Anchors**. Nous nous double-cliquons sur le fichier `LIFC Root CA` et nous effectuons les mêmes opérations que précédemment.

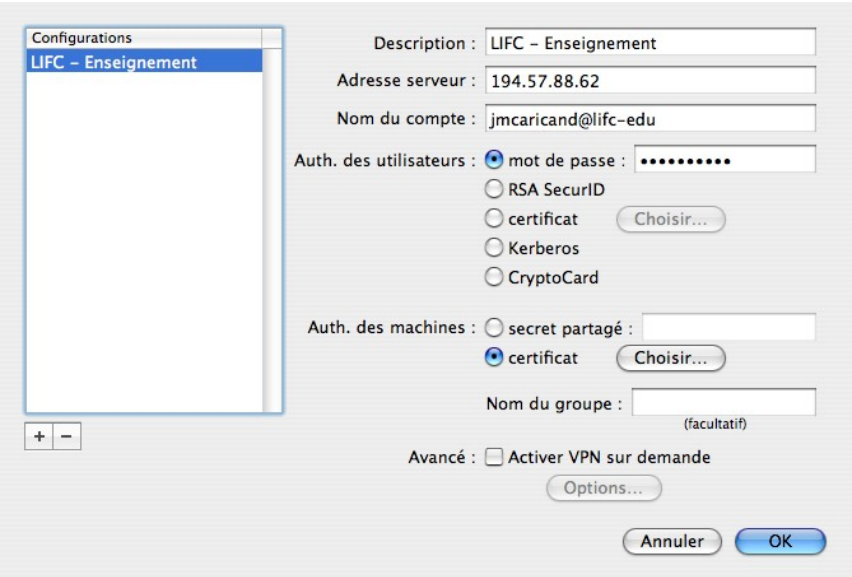
Nous avons dû redémarrer la machine pour que les modifications soient réellement prises en compte au niveau de la validité des certificats.

Création d'une connexion VPN

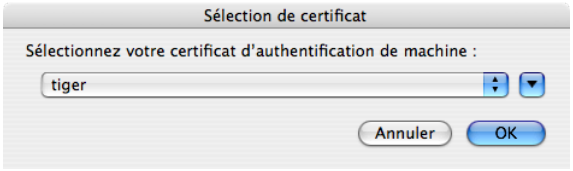
Nous allons créer maintenant une connexion VPN en utilisant IPSec/L2TP pour pouvoir accéder au réseau enseignement du Laboratoire Informatique de l'Université de Franche-Comté. L'utilisateur voulant établir la connexion doit bien évidemment posséder les droits suffisants pour accéder à ce réseau. Nous ouvrons l'application **Connexion à Internet** :



Nous renseignons la boîte comme ci-dessous. Les informations présentes seront sont bien sûr à adapter (pour choisir l'adresse IP du serveur, nous nous référons à la rubrique ci-dessus " Les serveurs VPN en usage à l'UFC") :



Nous devons utiliser un certificat pour pouvoir établir notre connexion. En cliquant sur l'option **certificat** dans le groupe **Auth. des machines**, nous obtenons la boîte ci-dessous. Nous sélectionnons le certificat que nous avons importer dans la première étape. Nous validons la boîte de sélection du certificat puis la boîte de configuration de la connexion :



Lancer une connexion VPN

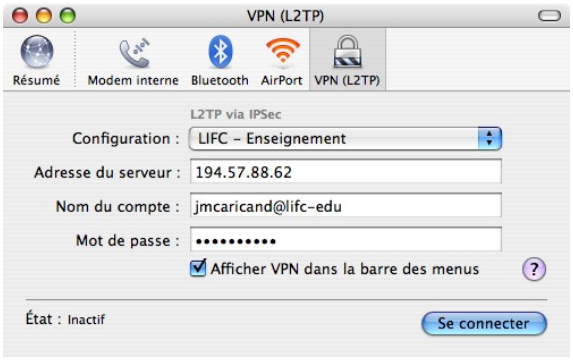
La boîte de connexion au VPN est maintenant affichée. Il nous suffit de cliquer sur **Se connecter** pour établir une connexion VPN avec le réseau distant.

N.B. : Le **Nom d'utilisateur** correspondant à votre login__ldap@votre_realm

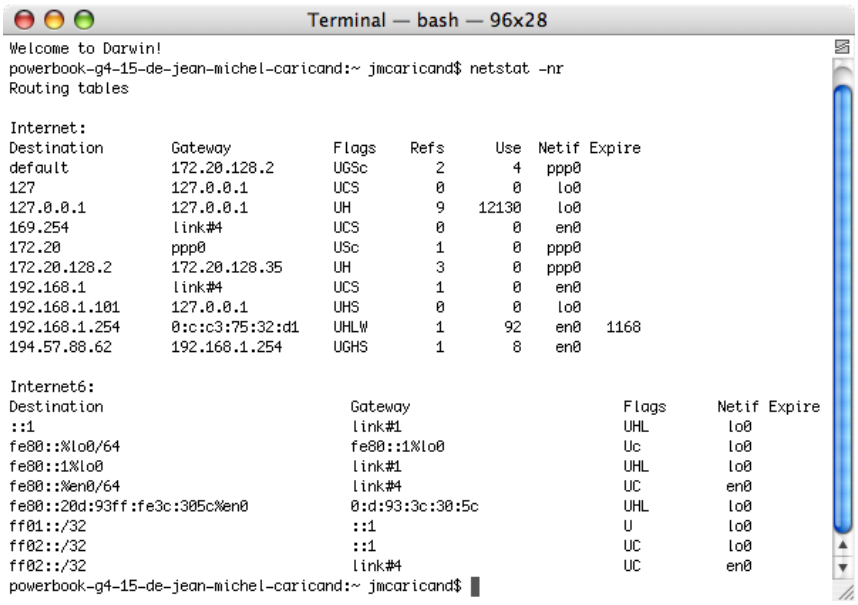
Exemple : jdupont@ufc pour J. Dupont qui souhaite se connecter sur le realm générique de l'université.

Le **Mot de passe** est celui stocké dans LDAP, que vous utilisez pour l'ENT ou votre messagerie.

Afin d'obtenir un raccourci vers cette boîte dans la barre des menus, nous cochons l'option **Afficher VPN dans la barre des menus** :



La connexion établie, nous pouvons "pinguer" les machines situées sur le réseau distant. L'affichage de la table de routage montre une route par défaut établie sur l'interface `ppp0` et dirigée vers la passerelle `172.20.128.2`. Ces valeurs seront certainement différentes dans d'autres cas :



Pour pouvoir naviguer sur Internet, il nous restera à définir le serveur mandataire à utiliser.

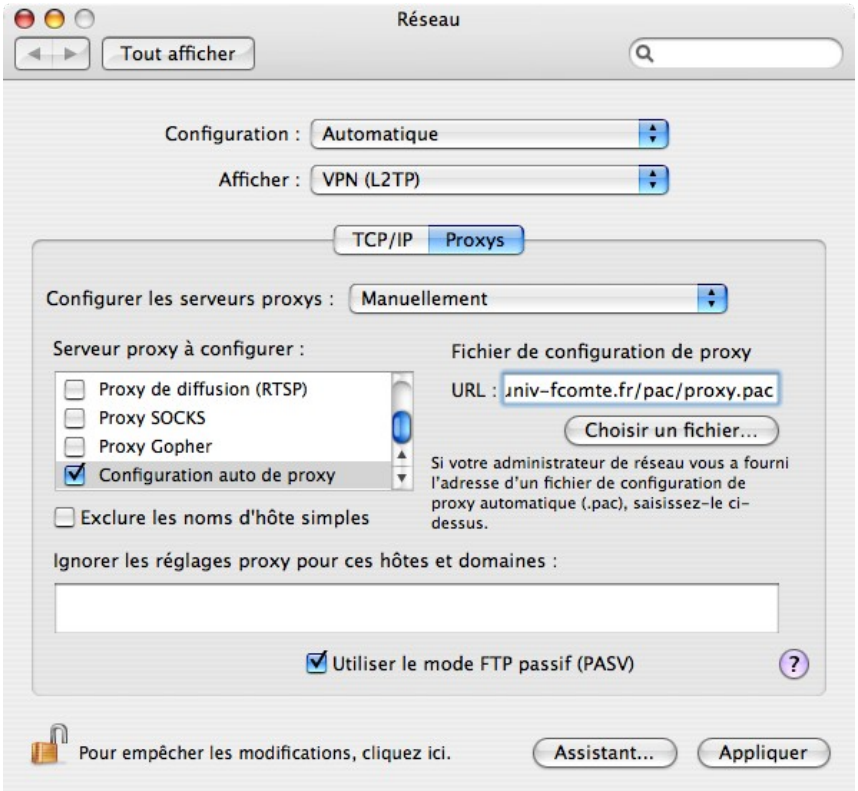
Nous accédons à la boîte de gestion des proxies en passant par le menu **Pomme - Configuration réseau - Préférences Réseau...**.

Dans la boîte **Réseau** nous cliquons sur **Configurer...**.

Dans la liste **Afficher** nous sélectionnons l'option **VPN (L2TP)** puis l'onglet **Proxies**.

Dans la liste **Serveur proxy à configurer :** nous cochons l'option **Configuration auto de proxy**.

Dans la zone de saisie **URL** nous entrons le texte `http://wifi.univ-fcomte.fr/pac/proxy.pac` :



Nous validons la boîte. Désormais, nous devrions pouvoir naviguer sur Internet.

Création de la connexion réseau V.P.N. sous MacOs Léopard

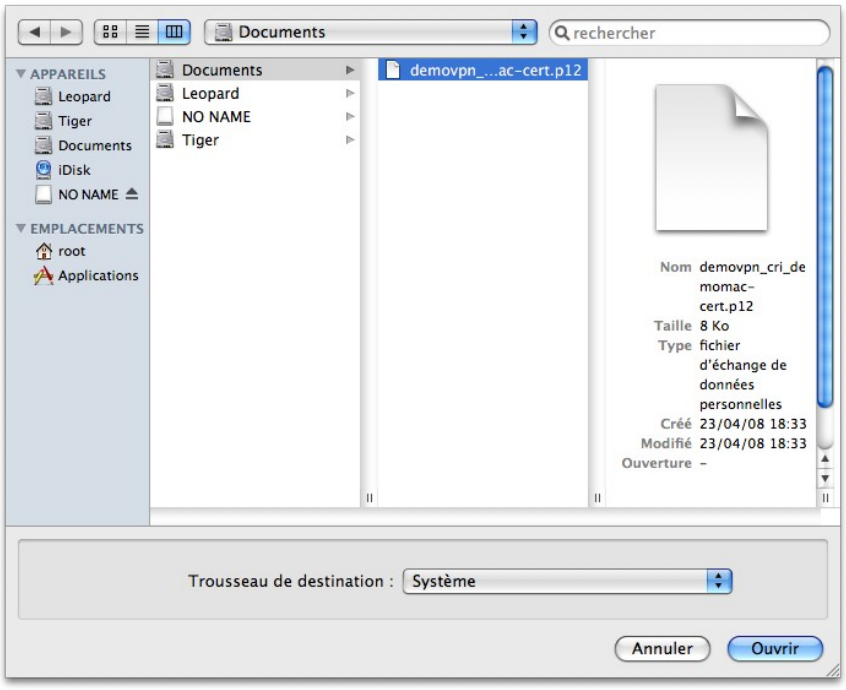
Les tests de connexions ont été réalisés avec succès en utilisant la version 10.5.1 du système d'exploitation Mac OS X.

Importation du certificat P12

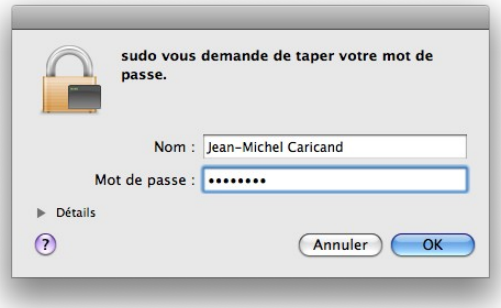
La première étape consiste à importer le certificat machine fourni par le CRI. Ce certificat devra être importé en étant identifié comme l'utilisateur `root`. Nous ouvrons donc un terminal **Applications - Utilitaires - Terminal** puis nous appelons l'application **Keychain Access** :

```
# sudo "/Applications/Utilities/Keychain Access.app/Contents/MacOS/Keychain Access"
```

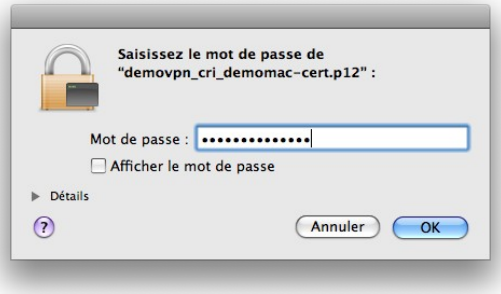
Nous donnons notre mot de passe et la boîte **Trousseau d'accès** s'affiche. Nous commençons l'importation en passant par le menu **Fichier - Importer des éléments**. Le trousseau à sélectionner est **Système**. Le certificat que nous allons importer s'appelle `demovpn_cri_demomac-cert.p12` :



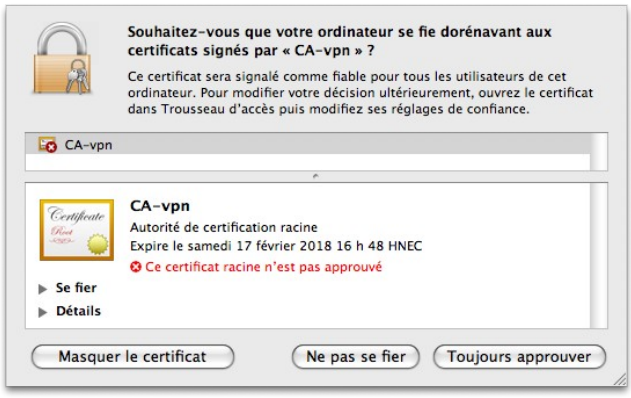
Une boîte de dialogue vous demande de fournir votre mot de passe :



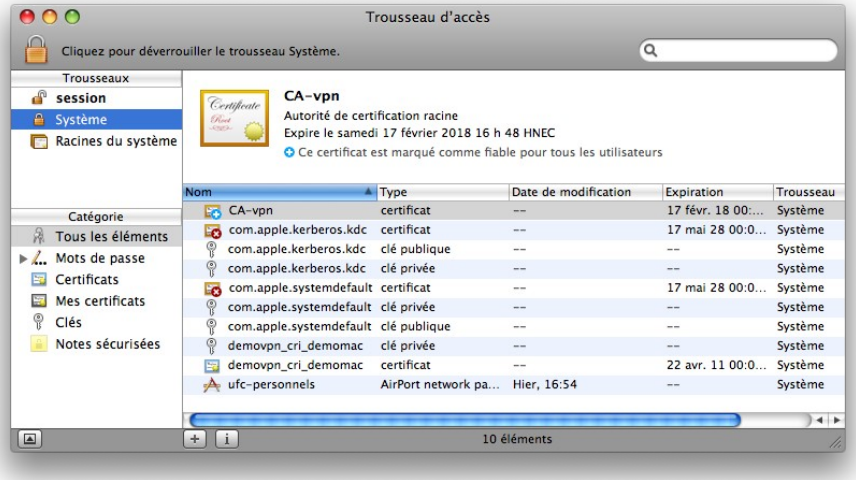
Une boîte d'authentification s'affiche et attend un mot de passe que nous devrions avoir en notre possession. Ce mot de passe est nécessaire pour pouvoir utiliser le certificat. Si nous ne l'avons pas, nous devons en faire la demande à l'émetteur du certificat c'est à dire le CRI :



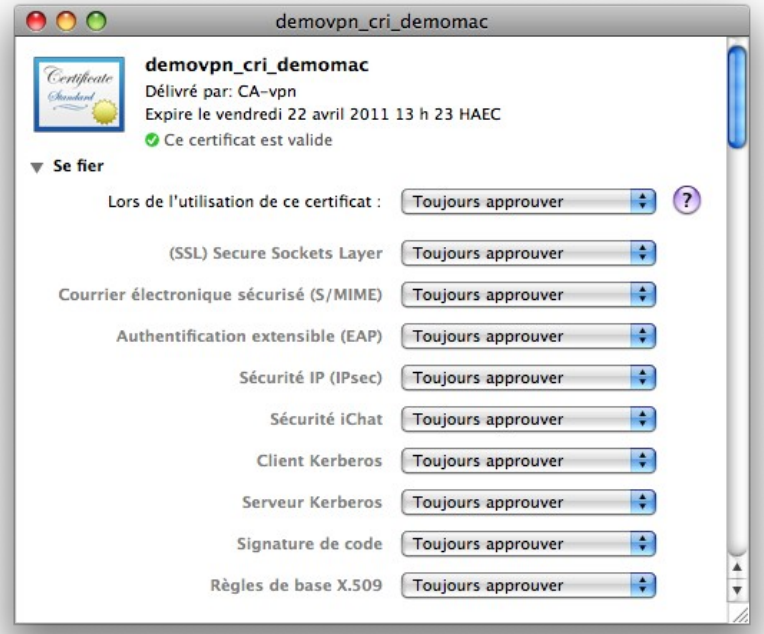
Une boîte de confirmation nous demande si nous pouvons avoir confiance dans l'autorité de certification. Nous cliquons sur **Toujours approuver** :



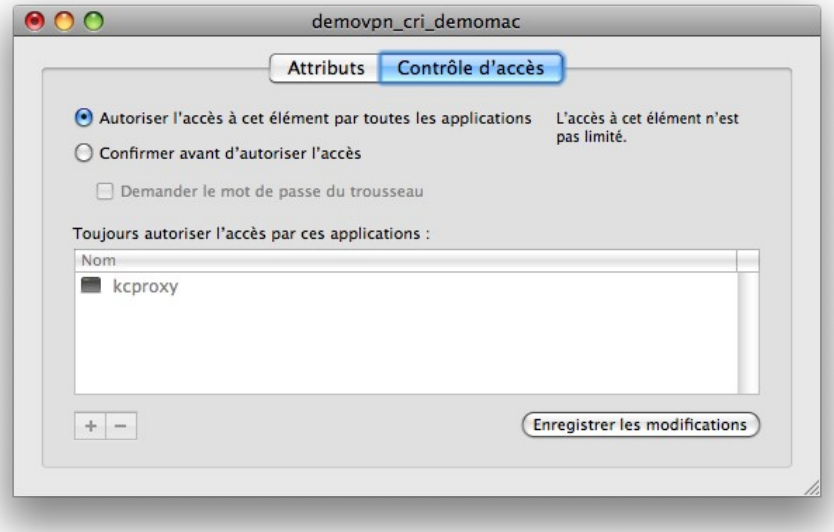
Après avoir correctement renseigné la boîte, nous revenons au trousseau d'accès :



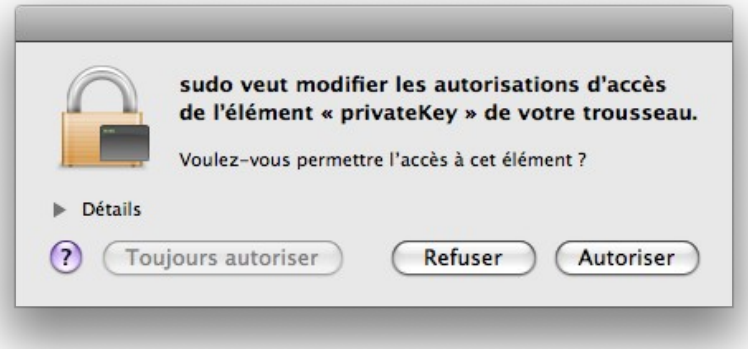
Plusieurs fichiers apparaissent maintenant dans notre trousseau **Système**. Nous double-cliquons sur le certificat `demovpn_cri_demomac`. Nous ouvrons la branche **Se fier** puis nous sélectionnons l'option **Toujours approuver** dans la liste **Lors de l'utilisation de ce certificat**.



Nous double-cliquons sur la clé privée `demovpn_cri_demomac`. Nous sélectionnons l'onglet **Contrôle d'accès** (nous devons fournir notre mot de passe) et nous cochons l'option **Autoriser l'accès à cet élément par toutes les applications** et nous enregistrons les modifications :



A l'affichage de la boîte ci-dessous, nous cliquons sur **Autoriser** :

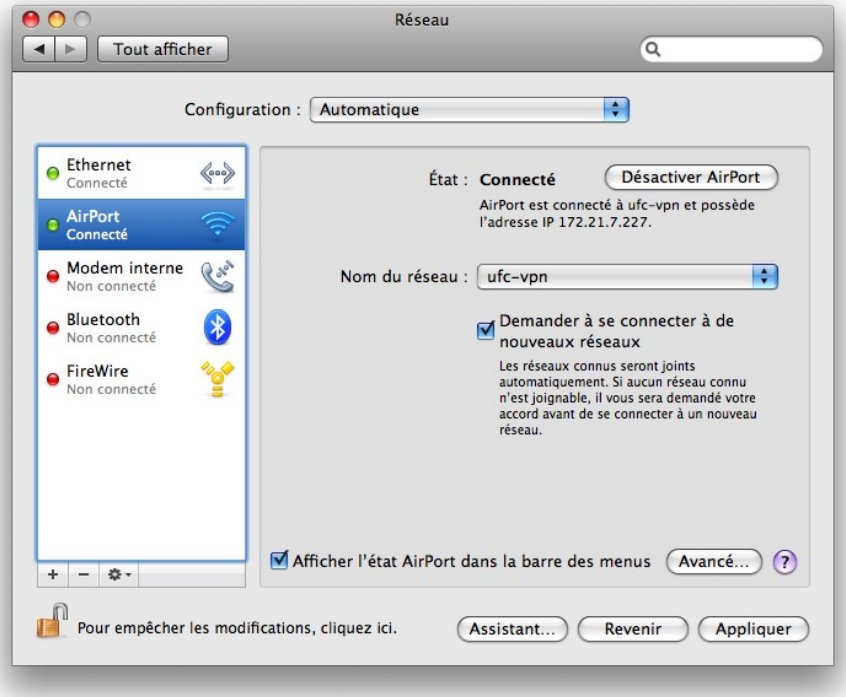


Nous pouvons refermer le **Trousseau d'accès**.

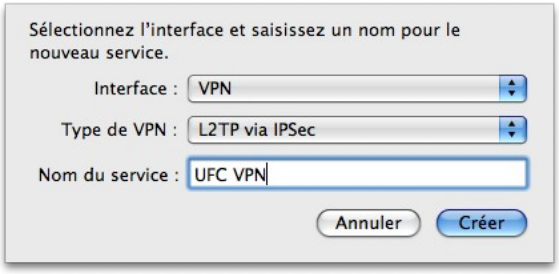
Création d'une connexion VPN

Nous allons créer maintenant une connexion VPN en utilisant IPSec/L2TP pour pouvoir accéder au réseau du Laboratoire Informatique de l'Université de Franche-Comté. L'utilisateur voulant établir la connexion doit bien évidemment posséder les droits suffisants pour accéder à ce réseau :

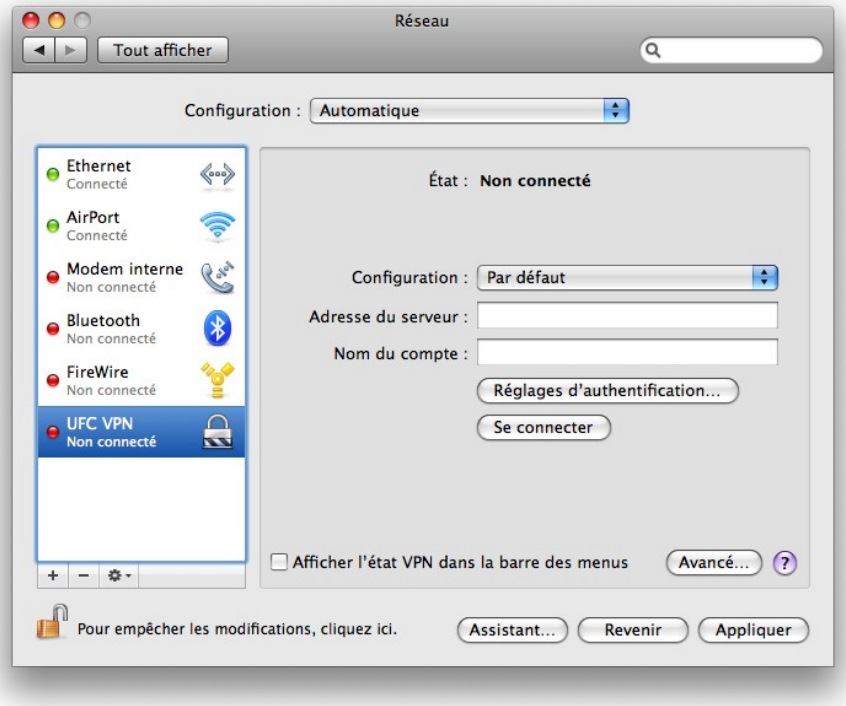
Par le menu : **Pomme - Préférences Systèmes... - Réseaux**. Pour l'exemple, nous utilisons une connexion WIFI disponible (SSID "ufc-vpn") :



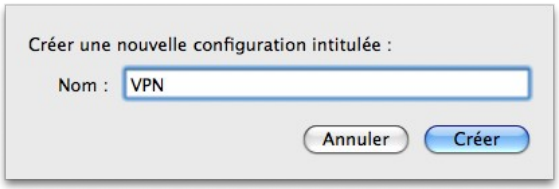
Nous ajoutons un nouveau type de connexion en cliquant sur le signe + en bas à gauche de la boîte. Nous sélectionnons **VPN** pour la zone **Interface Type de VPN** doit rester sur l'option **L2TP via IPSec** :



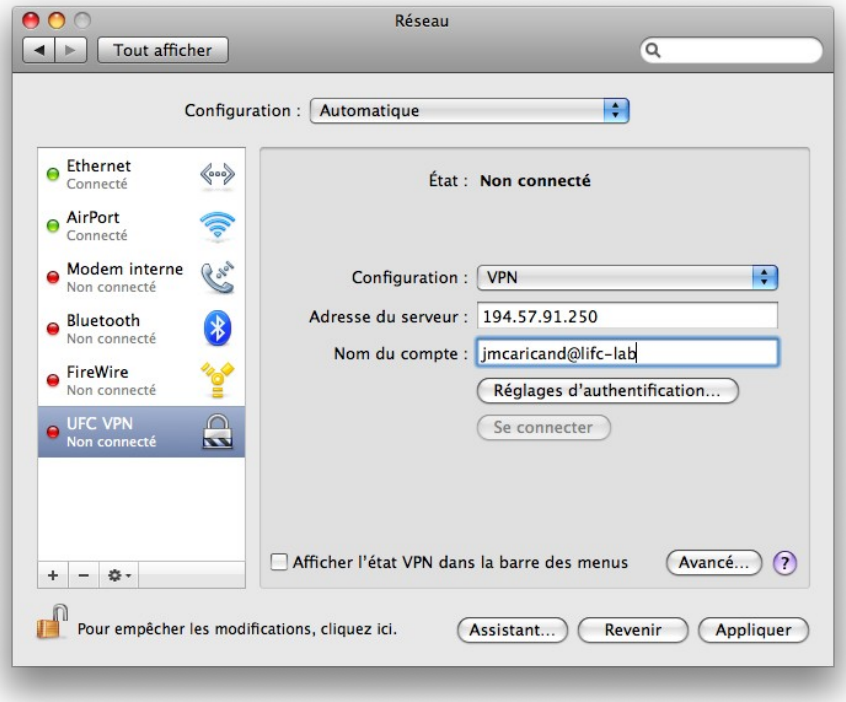
La nouvelle connexion doit apparaître dans la liste :



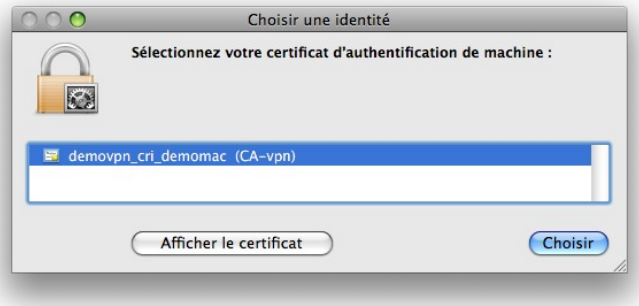
Nous ajoutons une nouvelle configuration que nous appelons **VPN** :



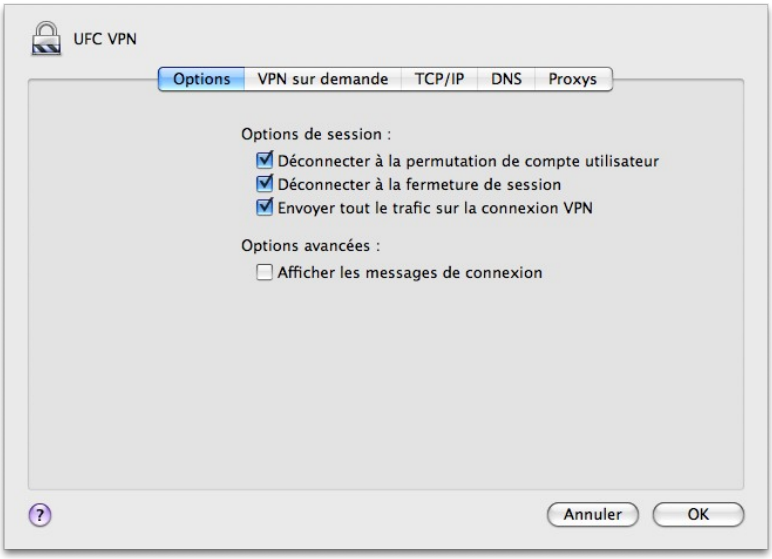
Nous renseignons la boîte puis nous cliquons sur **Réglages d'authentification...**



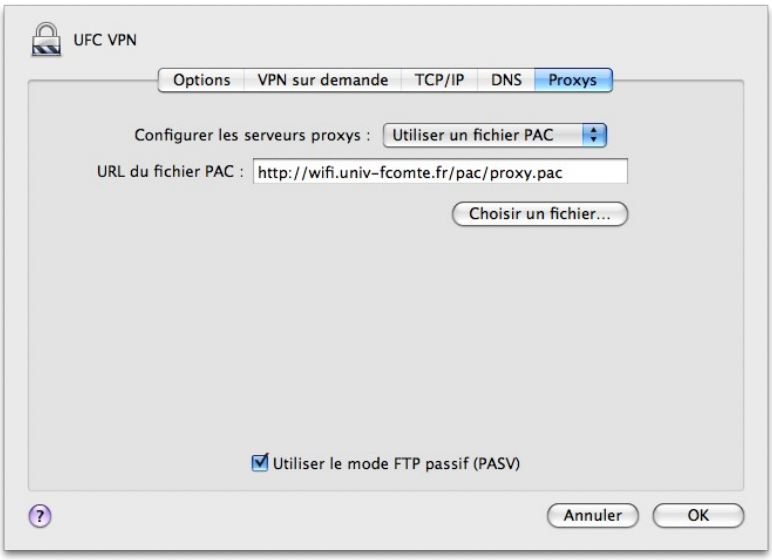
Nous sélectionnons et renseignons la zone **Mot de passe** puis nous cochons **Certificat** et nous cliquons sur **Choisir...**. Nous choisissons le certificat proposé et validons :



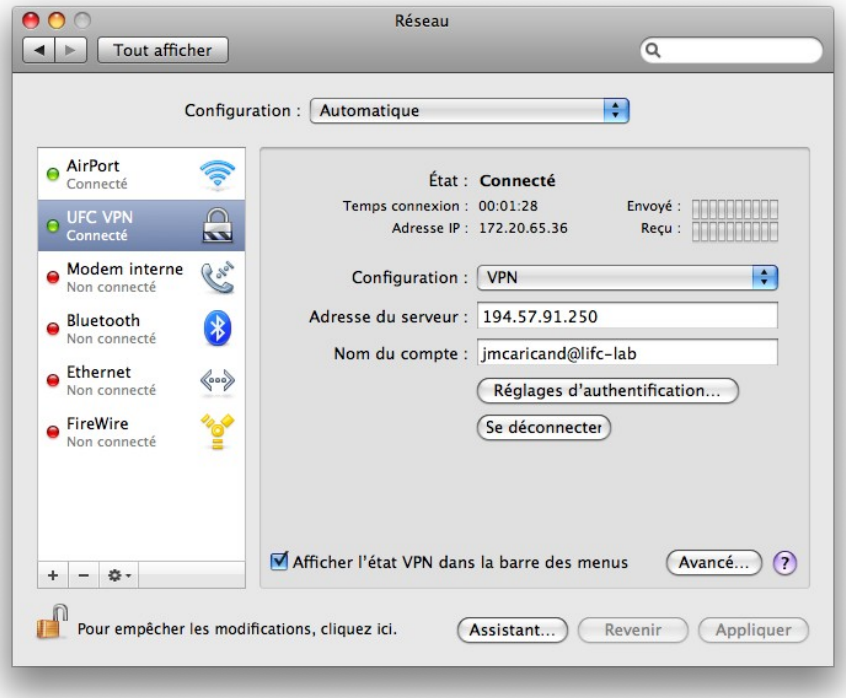
Nous cochons l'option **Afficher l'état VPN dans la barre des menus** et cliquons sur le bouton **Avancé...**. Nous sélectionnons l'onglet **Options** puis cochons **Envoyer tout le trafic sur la connexion VPN** :



Nous sélectionnons l'onglet **Proxys** et nous renseignons la boîte :

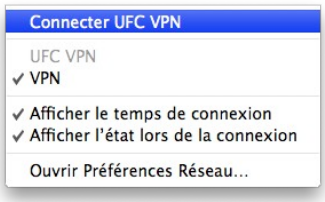


Nous appliquons les modifications. La création est terminée.



Lancer une connexion VPN

Le fait d'avoir coché l'option **Afficher l'état VPN dans la barre des menus** au cours de l'étape de création de la connexion, nous permet d'avoir un raccourci dans la barre des menus en haut à droite de l'écran.



N.B. : Le **Nom d'utilisateur** correspondant à votre login__ldap@votre_realm

Exemple : jdupont@ufc pour J. Dupont qui souhaite se connecter sur le realm générique de l'université.

Le **Mot de passe** est celui stocké dans LDAP, que vous utilisez pour l'ENT ou votre messagerie.