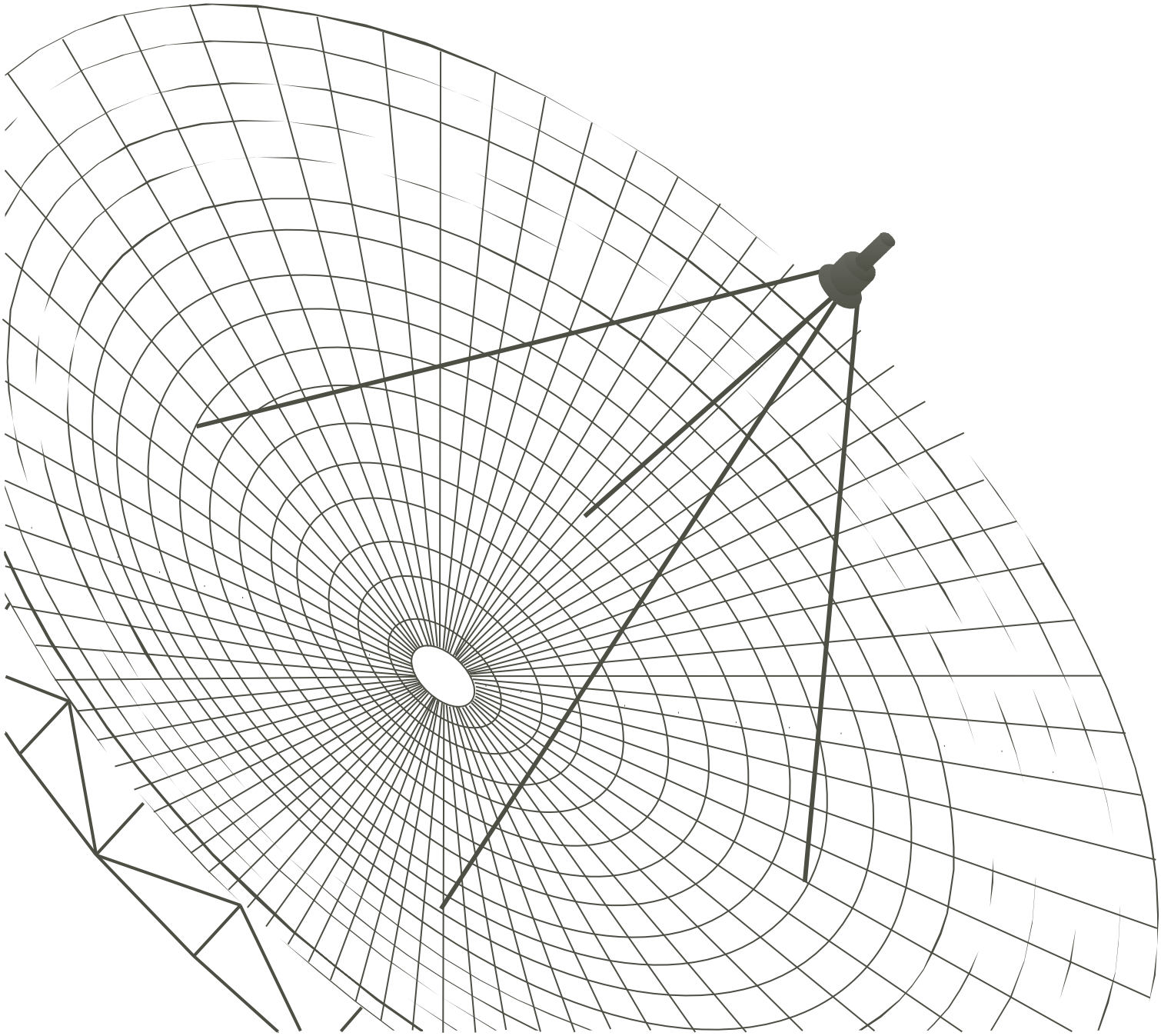
Les réseaux des EPLEFPA

Guide « Clients Mercure Ubuntu & Mac »



Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	1/14

Table des matières

Contexte de Mercure

Le Ministère de l'Alimentation, de l'Agriculture, de la Pêche, de la Ruralité et de l'Aménagement du Territoire (MAAPRAT) a mis en place le service Mercure VPN (en remplacement de prisme3 et Cisco VPN) permettant l'accès aux ressources du réseau MAAPRAT depuis Internet.

L'accès aux ressources par Mercure VPN, nécessite d'installer le client Mercure VPN et de posséder un certificat numérique délivré par l'IGC du MAAPRAT installé sur le poste de utilisateur. Le client Mercure VPN permet de réaliser un Tunnel VPN (Virtual Private Network, ou réseau privé virtuel et chiffré) entre le client et le MAAPRAT. L'utilisateur est authentifié par son certificat numérique sur un portail d'accueil. Ce certificat lui permet d'accéder aux ressources et applications du MAAPRAT pour lesquelles une autorisation lui a été délivrée.

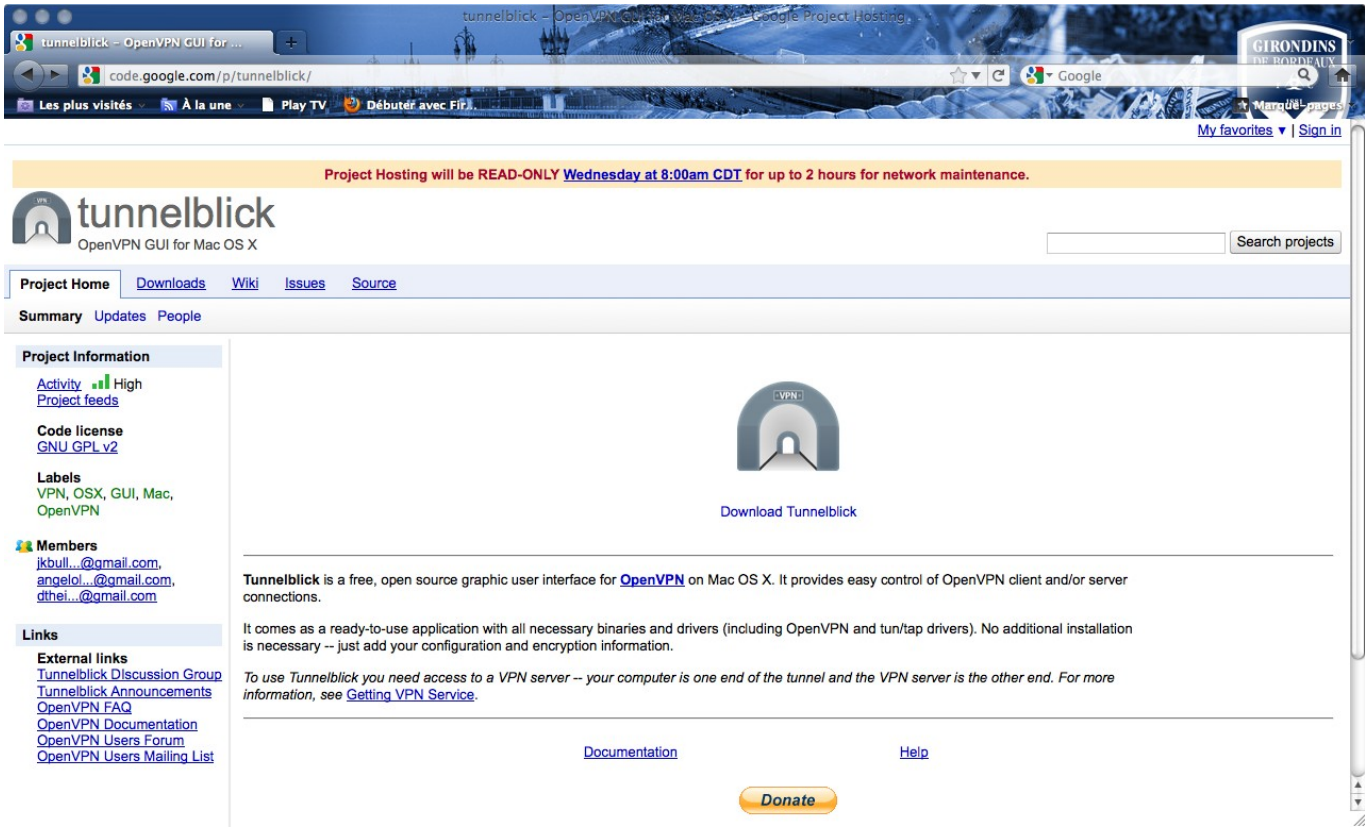
Mercure est opérationnel depuis le 01/07/2011.
Toute la documentation, ainsi que les logiciels d'installation de Mercure se trouvent sur le site du pôle de sécurité sur le réseau intranet du MAAPRAT : http://securite.rmap.auzeville.agri/ sous les rubriques « Extranet » puis « MercureVPN ».

Toutefois, les services en charge de ce projet ne produisent et ne maintiennent que les versions pour les systèmes d'exploitations de la famille « Microsoft Windows ». Cependant l'équipement des établissements et des enseignants comporte un nombre important d'autres systèmes. Ce guide concerne les deux principaux : Mac OsX Léopard et supérieur ainsi que Ubuntu 11.04 et suivant.

Installation du client OpenVPN

Mac OsX

Téléchargez le client TunnelBlick sur la forge de Google :



Procédez à l'installation du fichier en double cliquant sur le fichier .dmg :

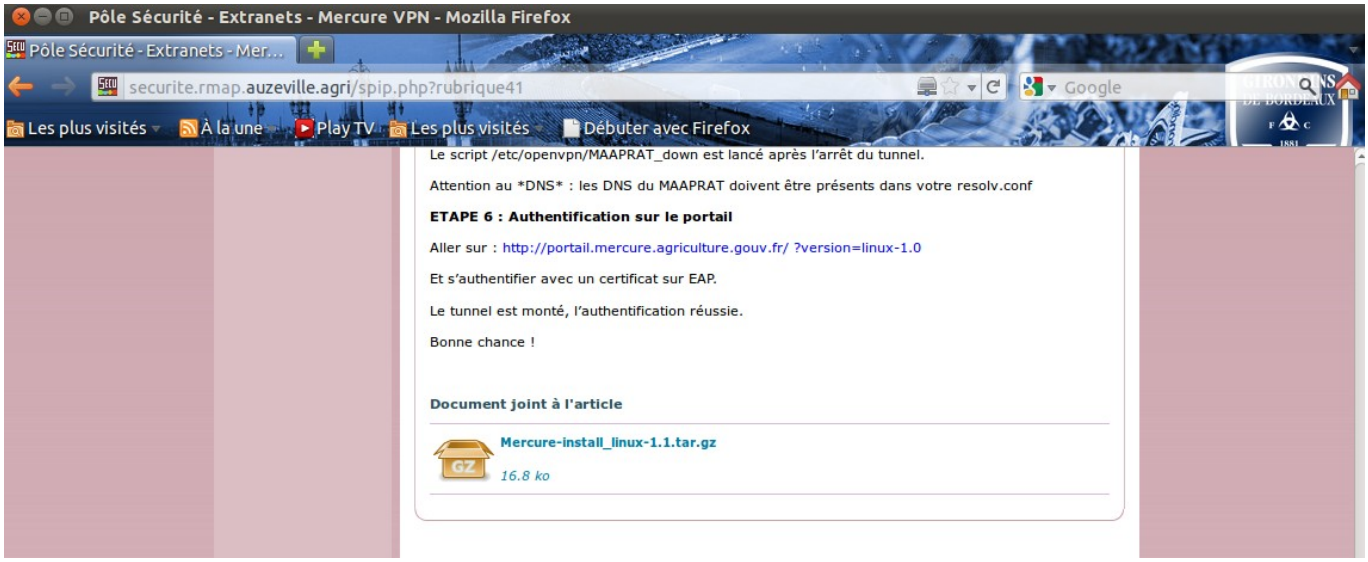
Ubuntu

Téléchargez et installez le client OpenVpn depuis la Logithèque Ubuntu.

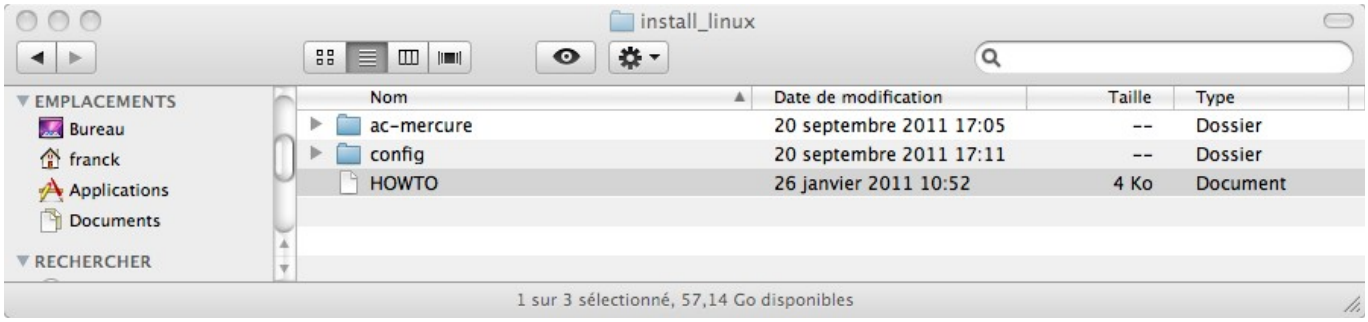
Téléchargement de la configuration mercure

Depuis un poste connecté au réseau du MAAPRAT, accédez au portail de sécurité du Ministère

Téléchargez l'archive compressée pour Linux en bas de la rubrique « Extranet/Mercure »

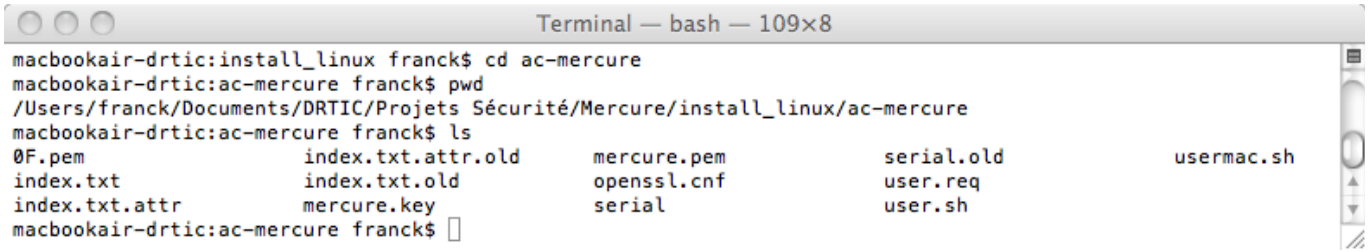


Enregistrez et décompressez ce fichier dans un répertoire personnel. Vous obtenez les répertoires :



Générer le certificat utilisateur

Pour les deux OS, ouvrez une console et placez vous dans votre dossier install_linux/ac-mercure.



Adaptation du script pour Mac OsX

Le script user.sh fourni nécessite une modification de la commande date pour s'exécuter sous Mac OsX.

usermac.sh

```
#!/bin/bash

if [ -z $1 ]; then

echo "ERREUR"
echo " le parametre mail est manquant"
echo " USAGE : sudo ./user.sh jean.dupont@ministere.gouv.fr"

else

echo "GÈnÈration du certificat de connexion..."

openssl genrsa -out ../config/user.key 2048

openssl req -subj "/C=FR/O=MAAPRAT/OU=Mercure VPN/CN=$1" -new -key ../config/user.key -out user.req

startdate=`date -v -1d +%y%m%d000000Z`

openssl ca -batch -startdate $startdate -in user.req -out ../config/user.pem -config openssl.cnf

fi
```

Génération de la clef

Vérifiez que vous êtes dans le bon répertoire « install_linux/ac-mercure ».
Exécutez la commande suivante en spécifiant votre propre adresse mail agriculture.gouv.fr ou educagri.fr

sudo ./user.sh jean.dupont@ministere.gouv.fr

Votre certificat user.pem et votre clef user.key sont alors générés et copiés dans le répertoire ../config

franck › Documents › Travail

Nom	Taille	Type	Date de modification
install_linux	3 éléments	dossier	mer. 26 janv. 2011 10:52:38 CET
config	8 éléments	dossier	mer. 28 sept. 2011 17:59:10 CEST
MAAPRAT.conf	565 octets	document texte brut	mer. 28 sept. 2011 17:59:10 CEST
user.pem	4,4 Kio	certificat X.509 codé DER/PEM/Netscape	jeu. 22 sept. 2011 09:30:14 CEST
user.key	1,6 Kio	document texte brut	jeu. 22 sept. 2011 09:30:14 CEST
update-resolv-conf	1,3 Kio	script shell	mer. 26 janv. 2011 10:27:04 CET
MAAPRAT_up.sh	353 octets	script shell	mer. 26 janv. 2011 10:27:04 CET
MAAPRAT_down.sh	7 octets	script shell	mer. 26 janv. 2011 10:27:04 CET
hmac.key	636 octets	document texte brut	mer. 26 janv. 2011 10:27:04 CET
ca.crt	12,6 Kio	certificat X.509 codé DER/PEM/Netscape	mer. 26 janv. 2011 10:27:04 CET
ac-mercure	12 éléments	dossier	jeu. 22 sept. 2011 09:30:14 CEST
HOWTO	2,6 Kio	différences entre fichiers	mer. 26 janv. 2011 10:52:38 CET

« install_linux » sélectionné (contenant 3 éléments), Espace libre : 9,2 Gio

Adaptation du fichier de configuration MAAPRAT.conf

Mac OsX

MAAPRAT-Mac.conf

```
client

resolv-retry infinite
<connection>
remote vpn.mercure.agriculture.gouv.fr 443 udp
</connection>

<connection>
remote vpn.mercure.agriculture.gouv.fr 443 tcp
</connection>

dev tun
ca ca.crt
cert user.pem
key user.key

tls-auth hmac.key 1 # This file is secret

ns-cert-type server
comp-lzo
verb 2
```

Ubuntu

MAAPRAT.conf [Lecture seule] (/etc/openvpn) - gedit

Ouvrir | Enregistrer | Annuler

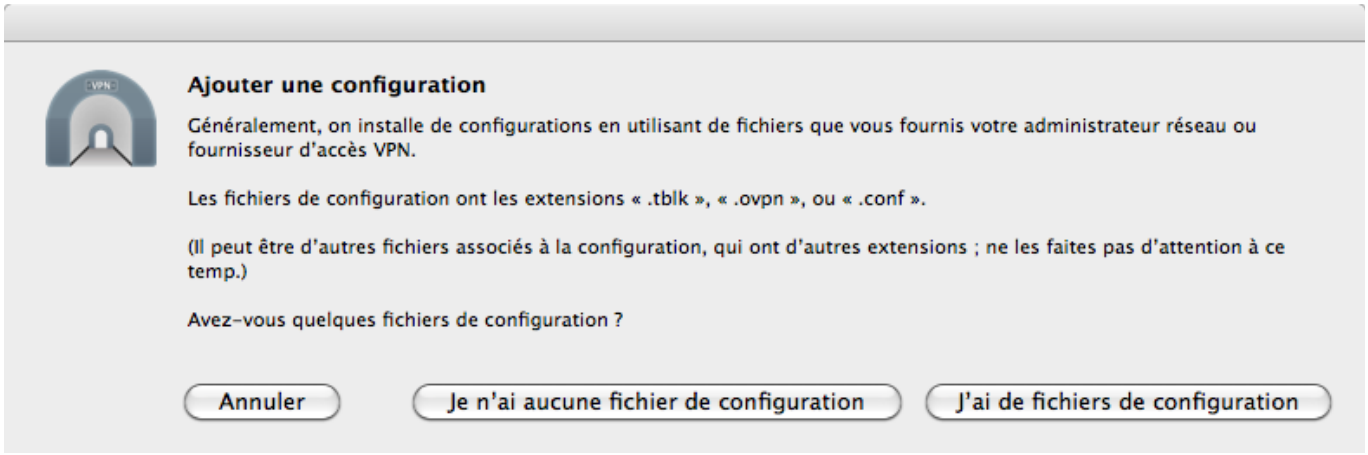
MAAPRAT.conf

```
client

resolv-retry infinite
<connection>
remote vpn.mercure.agriculture.gouv.fr 443 udp
</connection>

<connection>
remote vpn.mercure.agriculture.gouv.fr 443 tcp
</connection>

dev tun
ca ca.crt
cert user.pem
key user.key

tls-auth hmac.key 1 # This file is secret

ns-cert-type server
comp-lzo
verb 3

script-security 4

up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf

#up   '/bin/sh -x /etc/openvpn/MAAPRAT_up.sh'
#down '/bin/sh -x /etc/openvpn/MAAPRAT_down.sh'

log-append /tmp/openvpn-MAAPRAT.log
```

Mise en place de la configuration

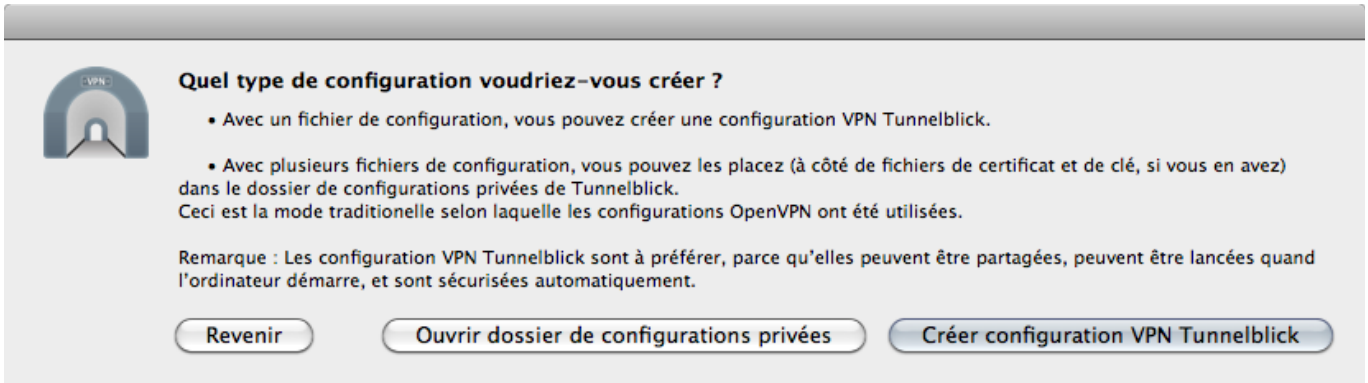
TunnelBlick sous Mac OsX

Exécutez l'application tunnelBlick précédemment installée puis ajoutez une configuration en choisissant « j'ai des fichiers de configuration » :



Choisissez ensuite « Configuration(s) OpenVPN :

Choisissez ensuite « Ouvrir dossier de configurations privées » :



Une fenêtre s'ouvre alors sur le dossier qui contient les configurations de Tunnelblick.
Vous devez alors y déposer les fichiers du répertoire install_linux/config suivants :

```
MAAPRAT.conf      # Fichier de configuration du Tunnel
ca.crt            # Certificat de l'AC Mercure
hmac.key          # Fichier secret pour établir la connection TLS
user.key          # Clef privée de l'utilisateur
user.pem          # Certificat de l'utilisateur
```

TunnelBlick est alors prêt à l'emploi.

Ubuntu

Copier l'ensemble des fichiers de configuration du répertoire install_linux/config dans le répertoire de configuration OpenVPN :

```
sudo cp ./config/.* /etc/openvpn/
```

Dans le répertoire /etc/openvpn, il faut trouver les fichiers suivants :

```
MAAPRAT.conf      # Fichier de configuration du Tunnel
ca.crt            # Certificat de l'AC Mercure
hmac.key          # Fichier secret pour établir la connection TLS
user.key          # Clef privée de l'utilisateur
user.pem          # Certificat de l'utilisateur
update-resolv-conf  # Script de configuration du DNS
```

Le Vpn est alors prêt à l'emploi.

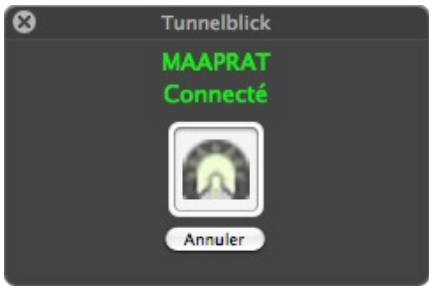
Etablir la connexion VPN

Mac OsX

TunnelBlick est représenté par une icône grisée en forme de tunnel dans la barre supérieure

Cliquez sur ce tunnel et choisissez « connecter MAAPRAT »

l'icône clignote et des fenêtres d'état se succèdent jusqu'à :

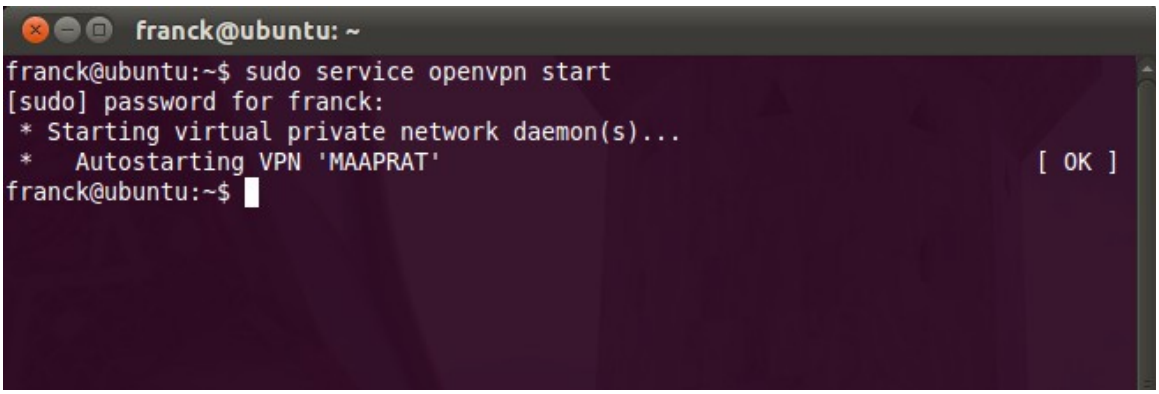


l'icône se fige sur un tunnel ouvert et vous êtes connecté :

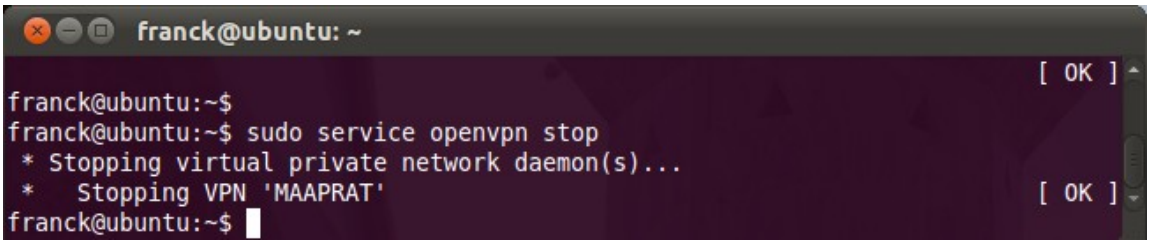
Vous devez alors vous authentifiez sur le **portail mercure depuis Firefox**.

La déconnection s'effectue en cliquant sur l'icône du tunnel ouvert et choix « deconnecter MAAPRAT »

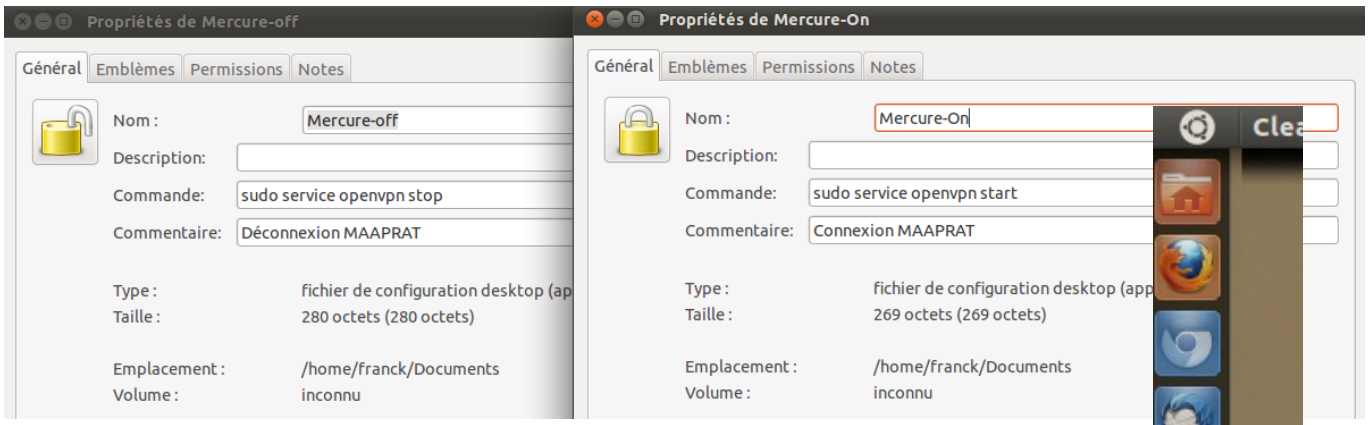
Il est possible d'établir le tunnel VPN à l'aide de commandes depuis une console :



et de le stopper par :



Vous pouvez également créer deux lanceurs de type « Application dans un terminal » (sur le bureau click droit/nouveau lanceur) :

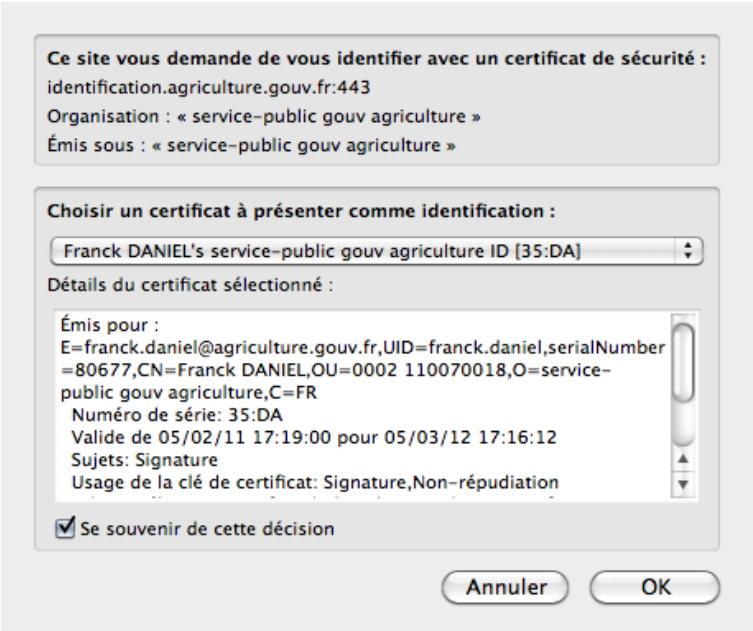


Vous pouvez laisser ces lanceurs on et off sur votre bureau ou les copier dans un répertoire de travail avant de les intégrer à votre barre Unity.

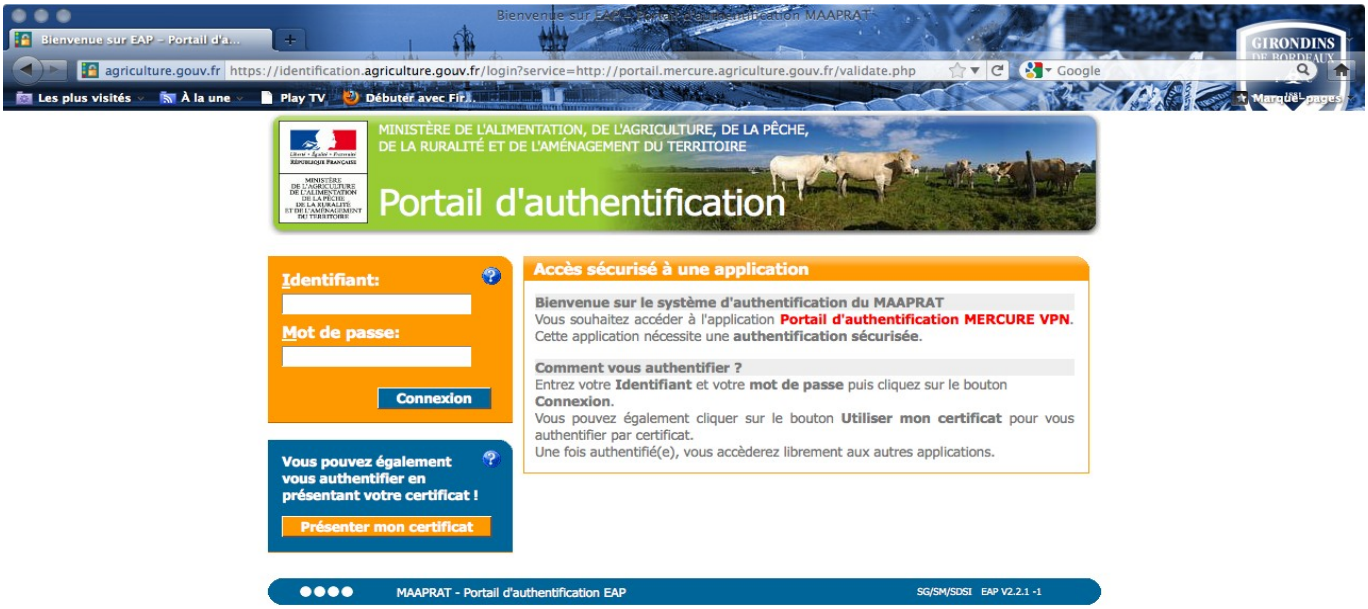
S'authentifier grâce à son certificat

Pour accéder au réseau du MAAPRAT le tunnel VPN ne suffit pas, il faut s'authentifier sur le portail mercure avec son certificat Agricoll depuis le navigateur Firefox qui le contient :

Cliquez sur « s'authentifier avec mon certificat » puis delectionner le bon certificat :



Vous arrivez alors sur le portail d'authentification du MAAPRAT.
Cliquez sur « Présenter mon certificat » :



Victoire :

Post Scriptum

Dysfonctionnement DNS

Des dysfonctionnements dans la résolution des noms (DNS) peuvent se produire si votre configuration de base comporte déjà plusieurs DNS.

La solution consiste à ne laisser qu'un DNS par défaut sur un poste utilisant Mercure.

Assistance

Ce guide est réalisé à l'aide des configurations que j'ai mises en œuvre sur mes deux postes de travail sous ubuntu 11.04 et Mac OsX Snow Léopard. Elles sont opérationnelles.

Ce document est réalisé pour vous aider en vous évitant de trop chercher.

Vous comprendrez aisément que je ne suis pas en mesure d'assurer l'assistance technique.

BON COURAGE