Installation du client VPN pour Ubuntu Debian 18.04

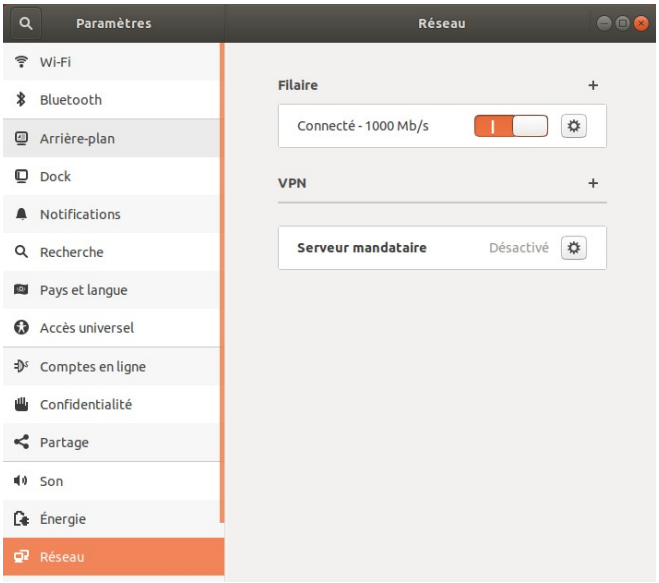
Cette documentation fournit la procédure de mise en œuvre d'une connexion VPN vers le réseau de l'Université de Franche-Comté. Elle concerne la distribution Ubuntu 18.04.

Importance de la MTU

Une valeur incorrecte de la MTU va générer des erreurs qui rendront la session VPN inutilisable. Il est donc important de fixer une valeur acceptable avant de poursuivre. La MTU doit être définie pour chaque interface réseau[1] pouvant être utilisée pour une session VPN. La valeur maximale ne doit pas excéder `1380` ou mieux `1300`.

Modification de la MTU de l'interface filaire

1. affichez le panneau « Paramètres - Réseau »
2. cliquez sur le bouton paramètres de la carte à modifier
3. sélectionnez l'onglet « Identité » et définissez la valeur de la MTU à `1300`



Modification de la MTU de l'interface WIFI

Sur Ubuntu 18.04, il n'est pas possible de modifier la valeur de la MTU depuis l'interface graphique. En effet, la zone de saisie a disparu alors qu'elle était présente sur la version précédente (Ubuntu 16.04).

1 Carte réseau filaire ou WIFI

Vous devez intervenir manuellement sur le contenu du fichier `01-ifupdown`[2] en modifiant la section concernant les connexions VPN. Le résultat devrait ressembler à celui-ci :

```
# If we have a VPN connection ignore the underlying IP address(es)
if [ "$2" = "vpn-up" ] || [ "$2" = "vpn-down" ]; then
    ADDRESS_FAMILIES=""
    ip link set dev "$1" mtu 1300
fi
```

Cas particulier des station d'accueil DELL

Le problème a été repéré par M. Giersch sur une station d'accueil Dell WD19DCS. Une fois le portable connecté à sa station d'accueil, la connexion VPN monte, mais la connexion n'est pas utilisable, et cela malgré le changement à 1300 de la MTU.

Ce problème intervient du fait que la connexion à la station d'accueil utilise une autre voie que l'interface considérée habituellement pour le VPN (et donc là où est réglée la MTU).

Une solution qui semble fonctionner (pour les flux TCP comme http, https, ...) est de modifier à la volée la valeur de MSS (taille maximale de la partie utile d'un paquet TCP).

Cela peut se faire avec l'instruction suivante :

```
iptables -t mangle -A POSTROUTING -m policy --pol ipsec --dir out \
      -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
```

Une variante si la ligne ci-dessus ne fonctionne pas :

```
iptables -t mangle -A POSTROUTING -m policy --pol ipsec --dir out \
      -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1361:1536 \
      -j TCPMSS --set-mss 1360
```

Cette modification peut être rendu permanente en ajoutant le fichier `00-local` dans `/etc/NetworkManager/dispatcher.d/`

ce qui nous donne `/etc/NetworkManager/dispatcher.d/00-local`

```
#!/bin/sh
set -e
DEV=$1
ACTION=$2
# Usage: mss_rule [-A|-C|-D]
mss_rule() {
    iptables -t mangle "$1" POSTROUTING -o "$DEV"  \
             -m policy --pol ipsec --dir out       \
             -p tcp -m tcp --tcp-flags SYN,RST SYN \
             -j TCPMSS --clamp-mss-to-pmtu
#            -m tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360
}
case "$ACTION" in
vpn-up)
    mss_rule -C > /dev/null 2>&1 || mss_rule -A
    ;;
vpn-down)
    mss_rule -D
    ;;
esac
```

2 Le nom complet du fichier est : `/etc/NetworkManager/dispatcher.d/01-ifupdown`

Modification du gestionnaire de noms DNS sur Ubuntu < 24

Attention, cette section ne concerne pas Ubuntu 24 et les suivante

En général, lorsqu'une connexion VPN est ouverte, les serveurs de noms DNS de l'uFC/uMLP sont bien pris en compte au niveau de votre système d'exploitation. Néanmoins, l'ordre d'interrogation des serveurs de noms a son importance. En effet, les serveurs DNS de l'uFC/uMLP ne fourniront pas forcément de réponse à toutes les requêtes concernant le domaine `univ-fcomte.fr` si l'émetteur de la requête n'est pas situé dans un réseau de l'uFC/uMLP.

Ce cas se présentera à vous si le premier DNS interrogé par votre système est celui de la box de votre FAI (Orange, Bouygues, SFR, etc). Votre box est située dans un réseau public appartenant à votre FAI. Malgré l'ouverture d'une session VPN, c'est la box qui sera l'émetteur des requêtes DNS d'où l'impossibilité de résoudre certains noms de machines universitaires.

Vous allez donc modifier la configuration de votre machine afin que toutes les requêtes destinées à résoudre des noms en `*.univ-fcomte.fr` soient dirigées directement vers les serveurs DNS de l'uFC/uMLP sans passer par le service DNS de votre box.

Pour pouvoir atteindre cet objectif, nous allons changer le service DNS utilisé par défaut par votre système. Nous allons donc utiliser `dnsmasq` à la place de `systemd-resolved` [3].

Vous désactivez le service `systemd-resolved` :

```
sudo systemctl stop systemd-resolved
sudo systemctl disable systemd-resolved
```

Dans le fichier `/etc/NetworkManager/NetworkManager.conf`, vous ajoutez/remplacez la ligne `dns=` dans la section `[main]` par :

```
dns=dnsmasq
```

Vous créez les fichiers suivant

- `/etc/NetworkManager/dnsmasq.d/dns-uFC/uMLP.conf` avec le contenu ci-dessous :

```
server=/univ-fcomte.fr/194.57.91.200
server=/univ-fcomte.fr/194.57.91.201
```

- `/etc/NetworkManager/dnsmasq.d/00-use-dns-google.conf` avec le contenu ci-dessous :

```
server=8.8.8.8
server=8.8.4.4
```

Vous supprimez le fichier `/etc/resolv.conf` :

```
sudo rm -f /etc/resolv.conf
```

Vous relancez le service `Network-Manager` :

```
sudo systemctl restart NetworkManager
```

3 Actuellement, `systemd-resolved` ne permet pas de choisir les serveurs DNS à utiliser en fonction du domaine.

Vous devriez pouvoir observer la prise en compte des modifications en allant regarder dans le fichier de logs `/var/log/syslog` :

sudo tail -100f `/var/log/syslog` :

```
Mar 27 20:25:28 jm-VirtualBox systemd[1]: Reloaded Network Manager.
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: configuration des serveurs amonts à partir de DBus
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: using nameserver 194.57.91.201#53 for domaine univ-fcomte.fr
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: using nameserver 194.57.91.200#53 for domaine univ-fcomte.fr
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: using nameserver 194.57.91.200#53 for domaine 138.252.20.172.in-addr.arpa
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: using nameserver 194.57.91.201#53 for domaine 138.252.20.172.in-addr.arpa
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: utilise le serveur de nom 194.57.91.200#53 (via enp0s3)
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: utilise le serveur de nom 194.57.91.201#53 (via enp0s3)
Mar 27 20:25:28 jm-VirtualBox dnsmasq[3564]: utilise le serveur de nom 192.168.1.1#53 (via enp0s3)
```

Comme indiqué dans les logs, `dnsmasq` va résoudre les noms `*.univ-fcomte.fr` en utilisant les serveurs de noms de l'uFC/uMLP.

Les requêtes DNS emprunteront les tunnels IPsec montés par la connexion VPN pour atteindre les DNS `194.57.91.200` et `194.57.91.201`. et les résultats seront corrects.

Les autres résolutions de noms utiliseront le service DNS de la box.

Modification concernant les serveurs de noms DNS sur Ubuntu 24[4]

Avec cette version d'Ubuntu, il n'y a normalement rien à faire pour que le fonctionnement du DNS passe en priorité sur les DNS de l'uFC/uMLP pour les domaines de l'uFC/uMLP.

Si vous avez effectué la section précédente, vous pouvez simplement retaper :

```
sudo systemctl enable systemd-resolved
sudo systemctl start systemd-resolved
sudo systemctl restart NetworkManager
```

4 Merci à l'usager Mehmet Ates qui nous a signaler ce point.

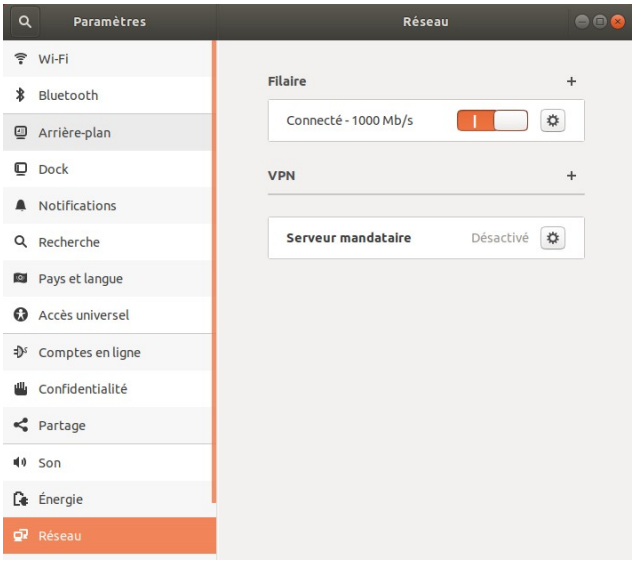
Installation des paquets du client VPN

Ouvrez un terminal et exécutez les commandes suivantes :

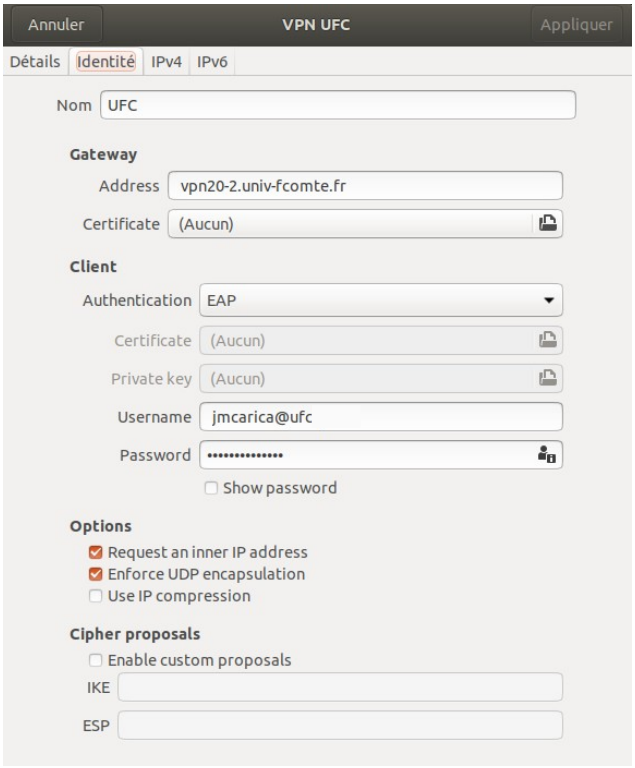
```
$ sudo apt-get update
$ sudo apt-get install -y network-manager-strongswan \
libstrongswan-extra-plugins libcharon-extra-plugins
```

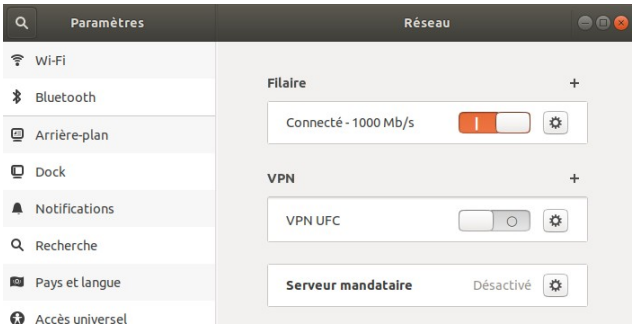
Création d’une connexion VPN

1. affichez le panneau « Paramètres - Réseau »
2. cliquez sur le signe + à la hauteur de VPN
3. cliquez sur « Ipsec/IKEv2(strongswan) »
4. renseignez les champs avec les valeurs indiquées. Les champs « Username » et « Password » sont à adapter [5]
5. Cliquez sur « Ajoutez »



5 Remarque : il ne faut pas modifier la valeur de la zone « Certificate ». Si par erreur vous avez sélectionné une option dans la liste, il est nécessaire de supprimer la connexion et d’en créer une nouvelle.





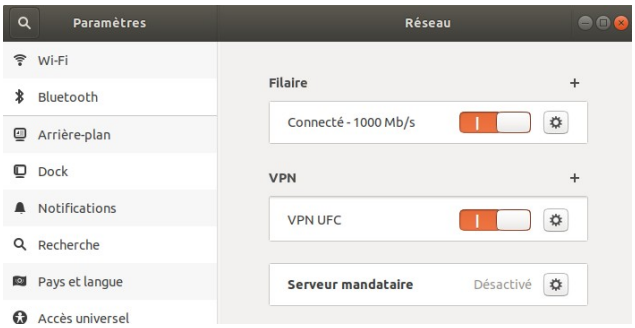
Il est important de vérifier que les options

- « `Request an inner IP address` »
- « `Enforce UDP encapsulation` »

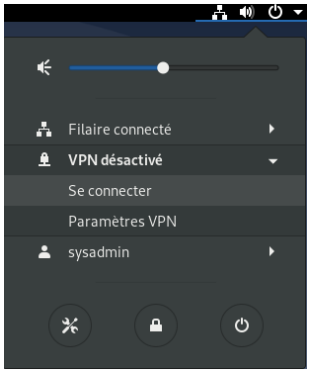
sont bien cochées.

La création de la connexion VPN est terminée. Vous pouvez ouvrir une session VPN depuis le panneau « Paramètres - Réseau » ou depuis l'outil « Connexions réseaux » situé dans le menu du Bureau.

Depuis le panneau « Réseau » :



Depuis le Bureau :



Lorsque la session VPN est active, une indication apparaît sur le menu du Bureau :