V.P.N. sous LINUX

Table des matières

V.P.N. sous LINUX....1
Introduction aux Réseaux Privés Virtuels....2
Définition d'un VPN (Virtual Private Network) :....2
Quelques explications :....2
Quelles possibilités pour le VPN ?....3
Royaume : « realm »....4
Qui fait une demande de « realm » ?....4
Quels sont les « realms » actifs ?....4
Obtenir un certificat, des droits....4
Rencontrer son correspondant réseau/wifi....5
Délivrance du certificat....5
Droits....5
Les serveurs VPN en usage à l'UFC....5
Configuration du client Linux en mode terminal....6
Les fichiers de configuration importants pour le client Linux :....6
Installation d'IPsec – Openswan....6
Mise en place du certificat....6
Configuration d'Openswan....6
ipsec.conf....6
ipsec.secrets....7
vérification des interfaces et des routes....8
lancement d'openswan....8
Montage du tunnel L2TP....8
Conseil :....10
Rappel : lancement d'uneconnexion....10

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.

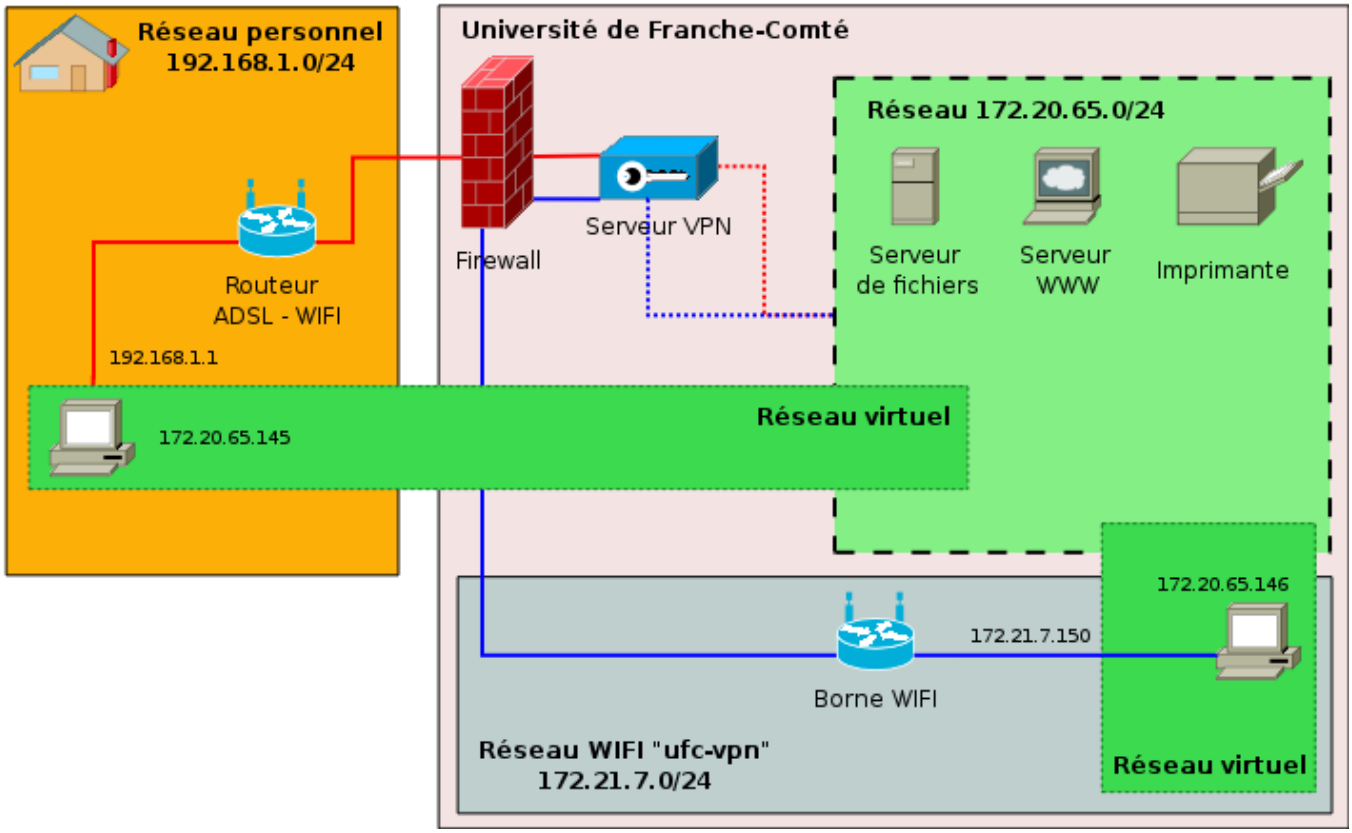
Un réseau privé virtuel est donc l'association de ces trois concepts. Une fois en place, il vous offre la possibilité d'utiliser un réseau public non sécurisé pour créer un réseau privé (données cryptées) et y faire circuler des données.

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 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 test test-vpn 194.57.91.251 actif jusqu'à fin juin 2008
- 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

Configuration du client Linux en mode terminal

Les fichiers de configuration importants pour le client Linux :

/etc :
```
ipsec.conf
ipsec.secrets
```

/etc/ppp :
```
options.l2tpd.client
pap-secrets
```

/etc/xl2tpd :
```
xl2tpd.conf
```

Installation d'IPsec – Openswan

Pour pouvoir créer un tunnel IPSec, nous devons installer le paquet openswan :

pour Debian
```
[root@machine]# apt-get install openswan
```

pour RedHat
```
[root@machine]# yum install openswan
```

Mise en place du certificat

Pour les systèmes d'exploitation Linux, le certificat qui vous sera remis sera composé de trois fichiers, par exemple :
```
monLinux-cert.pem qui correspond au certificat client
monLinux.key      qui est la clé privée du client
cacert.pem        qui est le certificat de l'Autorité de Certification
```

Copier ces fichiers dans les répertoires comme indiqués ci-dessous

1. `monLinux-cert.pem` dans le répertoire `/etc/ipsec.d/certs`
2. `monLinux-key.pem` dans le répertoire `/etc/ipsec.d/private`
3. `cacert.pem` dans le répertoire `/etc/ipsec.d/cacerts`

Configuration d'Openswan

ipsec.conf

A lire : http://linux.die.net/man/5/ipsec.conf

Modifier et compléter le fichier `/etc/ipsec.conf :`

N.B. : pour inscrire l'adresse IP du serveur (right=xxx.xxx.xxx.xx) se référer à la rubrique ci-dessus "Les serveurs VPN en usage à l'UFC".

```
version 2
config setup
    uniqueids=yes             ; connexion avec la clef unique
    nhelpers=0
    nat_traversal=yes         ; IMPORTANT : option à inscrire uniquement si l'on
                              ; est en NAT

conn %default
    authby=rsasig
    leftrsasigkey=%cert       ; clef
    rightrsasigkey=%cert ; clef
    type=tunnel               ; mode tunnel et non transport ou passthrough
                              ; tunnel = host-to-host, host-to-subnet, ou
                              ;          subnet-to-subnet tunnel;
                              ; transport =  host-to-host
    keyingtries=1

conn ufc-vpn            ; notre connexion utile
    rightprotoport=17/1701    ; udp 1701
    leftprotoport=17/1701
    keyexchange=ike
    pfs=no
    #auto=start               ; pas au démarrage
    auto=add            ; mais plutôt en ajout manuel
    #left=192.168.1.1         ; on ne spécifie pas l'interface
    left=%defaultroute        ; mais on utilise la route par defaut
    leftcert="/etc/ipsec.d/certs/monLinux-cert.pem"
    right=194.57.91.250       ; adresse Ip du serveur VPN
    rightca=%same             ; même signature de CA pour le certif du serveur
                              ; que pour le client
    leftnexthop=192.168.1.254 ; IMPORTANT : option à inscrire uniquement si l'on
                              ; est en NAT - adresse IP passerelle par défaut
```

Une petite remarque : si notre système d'exploitation est installé sur une machine virtuelle (VirtualBox ou WMware) l'adresse de la passerelle est bien celle de la machine virtuelle et non celle de la machine hôte. Pour connaître l'adresse de la passerelle, utiliser la commande route -n.

ipsec.secrets

Ajouter au fichier `/etc/ipsec.secrets` :

```
: RSA /etc/ipsec.d/private/monLinux.key "motdepasse"
```

Le « motdepasse » nous a été demandé lors de la création du couple clé/certificat. A défaut, il nous est communiqué par la personne ayant créé le certificat.

Attention : les deux points ainsi que les espaces doivent ne doivent pas être omis.

vérification des interfaces et des routes

Avant de lancer ipsec, il faut vérifier quelques points. Si vous possédez sur la machine plusieurs interfaces réseaux (une filaire et une wifi par exemple), le plus simple sera de couper celle qui ne vous sert pas.

```
[root@machine]# ifdown eth0
```

ou

```
[root@machine]# ifdown eth1
```

En faisant la commande

```
[root@machine]# route -n
```

vous ne devriez voir qu'une seule route du style

```
0.0.0.0 194.57.89.254   0.0.0.0         UG    0      0        0 ethX
```

Veillez à ce que ce type de route soit unique sinon vous aurez un message d'erreur en lancant openswan.

```
ipsec_setup: Stopping Openswan IPsec...
ipsec_setup: Starting Openswan IPsec 2.4.7...
ipsec_setup: multiple default routes, %defaultroute cannot cope!!!
```

lancement d'openswan

Redémarrer `openswan` :

```
[root@machine]# /etc/init.d/ipsec restart
```

Monter la connexion IPSec avec la commande :

```
[root@machine]# ipsec auto --up ufc-vpn
```

Arrêter la connexion IPSec avec la commande :

```
[root@machine]# ipsec auto --down ufc-vpn
```

Montage du tunnel L2TP

La création de connexions L2TP nous impose d'installer le paquet **`xl2tpd.`** Il faut noter que la configuration donnée ci-dessous nécessite au minimum la version 1.1.11 de ce logiciel. A ce jour, de nombreuses distributions Linux ne fournissent pas **`xl2tpd`** mais plutôt **`l2tpd.`**

Pour les utilisateurs de Debian Etch, le paquet **`xl2tpd`** dans une version correcte est disponible sur le site du LIFC.

Il est d'abord nécessaire d'ajouter le dépôt LIFC dans le fichier **`/etc/apt/sources.list`**

```
# deb LIFC
deb http://lifc.univ-fcomte.fr/debian/ etch-lifc main
apt-get update
```

Ajouter ensuite la clé du dépôt du LIFC dans votre trousseau, ceci évite le message d'avertissement vous indiquant que les signatures n'ont pas pu être vérifiées car la clé publique est indisponible.

```
wget http://lifc.univ-fcomte.fr/debian/lifc-apt.key
```

```
apt-key add lifc-apt.key
```

Installer le paquet :

```
[root@machine]# apt-get install xl2tpd
```

Autres distributions

Pour les autres distributions, les utilisateurs devront installer `l2tpd` ou mieux `xl2tpd` dans une version 1.1.11 ou supérieure en se référant à la documentation de leurs éditeurs respectifs ou à partir des sources du logiciel.

Supprimer le contenu du fichier `/etc/xl2tpd/xl2tpd.conf` et ajouter les lignes suivantes :

xl2tpd.conf

```
[global]
port = 1701
access control = no

[lac ma_machine]
lns = 194.57.91.250
redial = yes
redial timeout = 5
max redials = 3
length bit = yes
refuse authentication = yes
refuse chap = yes
require pap = yes
name = ma_machine
ppp debug = no
pppoptfile = /etc/ppp/options.l2tpd.client
```

Créer le fichier `/etc/ppp/options.l2tpd.client` :

options.l2tpd.clients

```
defaultroute            ; prévoir une route par défaut
replacedefaultroute     ; remplacer la route par défaut actuelle
debug
lock
user monNom@ufc         ; le compte à utiliser <=> /etc/ppp/pap-secrets
noipdefault
usepeerdns
noauth
lcp-echo-interval 20
lcp-echo-failure 10
noaccomp
```

Compléter le fichier pap-secrets

```
monNom@ufc  194.57.91.250 "motdepasse"
```

Lorsque le tunnel IPSec est monté, nous pouvons lancer la connexion L2TP avec la commande

avec L2TP : `[root@machine]# echo "c ma_machine" >/var/run/l2tp-control`

avec XL2TP : `[root@machine]# echo "c ma_machine" >/var/run/xl2tpd/l2tp-control`

Une petite remarque : si nous utilisons le logiciel xl2tpd dans une version supérieure ou égale à 1.1.11, le mot de passe n'aura pas à être écrit dans le fichier `/etc/ppp/pap-secrets` d'où une sécurité accrue. En effet, avec ces versions, nous avons la possibilité de passer le mot de passe « à la connexion » en utilisant la ligne de commande :

```
[root@machine]# echo "c ufc passwordfd motdepasse" >/var/run/xl2tpd/l2tp-control
```

Pour démonter le tunnel l2tp :

```
[root@machine]# echo "d ma_machine" >/var/run/xl2tpd/l2tp-control
```

Conseil :

Après plusieurs essais infructueux et diverses modifications, il est conseillé d'arrêter et de relancer

les démons ipsec et xl2tpd avec ces commandes :

```
[root@machine]# /etc/init.d/ipsec stop
[root@machine]# /etc/init.d/xl2tpd stop
[root@machine]# /etc/init.d/ipsec start
[root@machine]# /etc/init.d/xl2tpd start
```

Rappel : lancement d'une connexion

Montage du tunnel IPsec

```
[root@machine]# ipsec auto --up ufc-vpn
```

Lancement PPP à travers L2TP (ou XL2TP)

```
[root@machine]# echo 'c ma_machine' > /var/run/xl2tpd/l2tp-control
```