Paquetage OPENVPN
Version 3.10.18

Claas Hilbrecht
courriel: babel (+at+) fli4l dot de

L'équipe fli4l
courriel: team@fli4l.de

15 septembre 2019

Table des matières

1. Documentation du paquetage OPENVPN **3**
1.1. OpenVPN - Supporte le VPN . . . 3
1.1.1. OpenVPN - Introduction et exemple . . . 3
1.1.2. OpenVPN - Configuration . . . 5
1.1.3. OpenVPN - Configuration du bridge . . . 7
1.1.4. OpenVPN - Configuration du tunnel . . . 8
1.1.5. Paramètres experts . . . 11
1.1.6. OpenVPN - WebGUI . . . 19
1.1.7. OpenVPN - Aide pour différentes versions OpenVPN . . . 22
1.1.8. OpenVPN - Exemples . . . 23
1.1.9. Liens sur le thème OpenVPN . . . 26

A. Annexe du paquetage OPENVPN **28**

Table des figures **29**

Liste des tableaux **30**

Index **31**

1. Documentation du paquetage OPENVPN

1.1. OpenVPN - Supporte le VPN

Depuis la version 2.1.5, le paquetage OpenVPN fait partie intégrante de fli4l.

Important: *Avec l'utilisation du paquetage VPN vous pouvez installer un tunnel VPN sur Internet, il est nécessaire d'avoir soit, un forfait d'accès Internet illimité soit un forfait avec un volume heure important ! Le routeur fli4l reste allumé en permanence, la connexion ne peut pas être coupée, étant donné que les données sont transférées en permanence sur le tunnel (même si c'est quelques octets pendant quelques secondes), les frais de communications seront élevés si vous utilisez un forfait avec un volume d'heures liminés, il en va de même si vous Choisissez une connexion ISDN.*

Il y a dans la base de données OPT sur le site http://www.fli4l.de/fr/telechargement/paquetage-annexe/, en plus du tunnel OpenVPN le paquetage OPT_PoPToP pour la création de tunnel.

Le fait d'opter pour une solution VPN, dépend en premier lieu de la sécurité et des fonctionnalités l'installation. Voici Des rapports sur la sécurité et des solutions pour des réseaux privés virtuels, l'équipe fli4l n'est pas concerné sur ces rapport, voici des pages Web sur ces rapports :

Magazin Linux numéro janvier 2004

http://diswww.mit.edu/bloom-picayune/crypto/14238

http://sites.inka.de/bigred/archive/cipe-l/2003-09/msg00263.html

L'équipe fli4l a une position claire sur la fonctionnalité d'OpenVPN. Sur ce point, OpenVPN est le gagnant, le meilleur par rapport à Poptop. OpenVPN supporte avec le tunnel le module Bridge et une compression des données, contrairement à Poptop, en plus il est stable sur le routeur fli4l. il existe également une version OpenVPN pour Windows, qui peut être utilisé à partir de Windows 2000. Les seuls inconvénients d'OpenVPN par rapport à Poptop est la taille de l'archive opt et la version 2.0.x de fli4l qui n'est pas supportée par OpenVPN.

1.1.1. OpenVPN - Introduction et exemple

Pour entrer plus facilement dans la configuration, vous pouvez voir dans l'exemple ci-dessous. Deux réseaux qui utilise chacun un routeur fli4l connecté à Internet. Avec l'installation d'OpenVPN (tunnel codé) sur les routeurs fli4l, les ordinateurs des deux réseaux pourront communiquer entre eux par Internet dans des villes différentes. Et aussi les variables de configuration dans la figure 1.1.

local net, remote net La figure représente deux réseaux reliés entre eux par un tunnel. Les deux réseaux reliés doivent avoir un TCP/IP différent et ne doivent pas non plus s'entrecroiser avec leurs masques de sous-réseau. Le réglage respectif `IP_NET_x` (Page **??**) dans le fichier de configuration base.txt ne doivent pas être le même que le tunnel VPN.

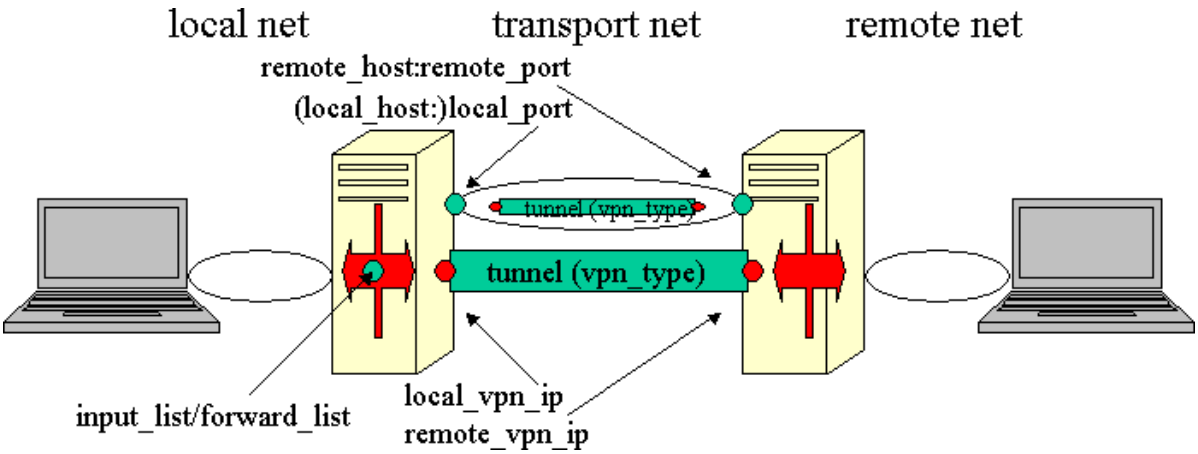

FIGURE 1.1. – Exemple de configuration VPN — Tunnel entre deux routeurs

Si les deux réseaux utilisent la même adresse IP 192.168.6.0/24 ils ne peuvent pas être liés par un tunnel VPN.

transport net Le réseau de transport se compose de deux éléments :

— La connexion entre les deux démons OpenVPN, sont décritent dans *remote_host : remote_port* et *local_host : local_port*. Cela correspond aux paramètres de configuration OpenVPN : `OPENVPN_x_REMOTE_HOST`, `OPENVPN_x_REMOTE_PORT`, `OPENVPN_x_LOCAL_HOST` et `OPENVPN_x_LOCAL_PORT`.

— Le tunnel, sur lequel la liaison entre les démons OpenVPN est établie, sont décritent dans *local_vpn_ip/remote_vpn_ip*. Cela correspond alors à : `OPENVPN_x_LOCAL_VPN_IP` et `OPENVPN_x_REMOTE_VPN_IP`. Les deux adresses IP sont uniquement utilisé pour le VPN et se trouvent dans les deux routeurs du réseau connus.

Les variables [input_list et forward_list] servent à filtrer les paquets qui circulent dans le tunnel. Le seule filtre autorisé que l'on peut utiliser et qui permet à tester le tunnel par des messages standards est ICMP (exemple le ping). Dans tout les autres cas, on doit d'abord autoriser les paquets explicitement, voici le cas le plus simple :

```
OPENVPN_x_PF_INPUT_POLICY='ACCEPT'
OPENVPN_x_PF_FORWARD_POLICY='ACCEPT'
```

N'oubliez pas que si vous «ouvrez» complètement les liaisons VPN, cela pourrais être dangereux pour la sécurité. Utilisez plutôt le tmpl : fichier de syntaxe pour le filtrage de paquets, afin d'ouvrir uniquement les services que vous avez besoin.

Il n'est pas nécessaire de paramétrer d'avantage de variables pour un simple tunnel VPN. Toutes les autres possibilités de réglage traitent des fonctionnalités avancées, ils sont disponibles pour des applications spéciales. Avec un minimum de réglage le tunnel VPN peut fonctionner, si vous paramétrez les variables avancées celles-ci doivent d'être compatibles pour un bon fonctionnement.

1.1.2. OpenVPN - Configuration

Puisqu'OpenVPN est assez complexe, nous commencerons par les variables obligatoires, nécessaires pour une liaison VPN. Ce n'est que lorsque le routeur fli4l sera connecté avec ces paramètres, que vous pourrez vous lancer à configurer les autres variables pour une utilisation étendues d'OpenVPN.

OPT_OPENVPN Par défaut : `OPT_OPENVPN='no'`

Avec `'yes'` vous activez le paquetage OpenVPN. Avec `'no'` vous désactivez complétement le paquetage OpenVPN.

OPENVPN_N Par défaut : `OPENVPN_N='0'`

Dans cette variable vous indiquez le nombre de configuration OpenVPN à activer.

OPENVPN_x_REMOTE_HOST Par défaut : `OPENVPN_x_REMOTE_HOST="`

Vous indiquez ici l'adresse IP ou l'adresse DNS du poste OpenVPN distant. Dans le cas d'un Roadwarrior (Page 25) (on peut dire "commerciaux nomade informatisés") vous devez laisser cette variable vide. Si le paramètre est omis, OpenVPN attendra une connexion, il ne tentera pas de se connexion.

OPENVPN_x_REMOTE_HOST_N Par défaut : `OPENVPN_x_REMOTE_HOST_N='0'`

Lorsque l'on utilise un service DNS dynamique, ce service n'est malheureusement pas fiable à 100%. C'est pourquoi il est plus simple dans n'installer deux, voire plusieurs services DynDNS différent et d'enregistrer en même temps une seul adresse IP pour tous ces services. Ainsi OpenVPN vérifira tout les noms DynDNS, dans cette variable on enregistre le nombre de nom de DNS *supplémentaire*. dans la variable `OPENVPN_x_REMOTE_HOST` on enregistrera la liste des adresses, OpenVPN essaira de contacter cette liste dans un ordre aléatoire. La variable `OPENVPN_x_REMOTE_HOST` doit donc continuer d'exister !

OPENVPN_x_REMOTE_HOST_x Par défaut : `OPENVPN_x_REMOTE_HOST_x="`

Il s'agit de la même description que la variable `OPENVPN_x_REMOTE_HOST` (Page 5) on place ici l'adresse DynDNS ou l'adresse IP statique.

OPENVPN_x_REMOTE_PORT Par défaut : `OPENVPN_x_REMOTE_PORT="`

Lorsque OpenVPN est connecté, on a besoin sur le routeur fli4l un Port qui n'est pas encore utilisé. Il est recommandé d'utiliser les ports au delà de 10000, car ces ports ne sont généralement pas utilisés. Lorsque vous voulez déployer une liaison vers un poste distant, si ce poste a une adresse IP dynamique et s'il n'a pas d'adresse DynDNS, vous pouvez laisser cette variable vide exactement comme la variable `OPENVPN_x_REMOTE_HOST`.

OPENVPN_x_LOCAL_HOST Par défaut : `OPENVPN_x_LOCAL_HOST="`

On indique ici l'adresse IP qui doit être connecté à l'OpenVPN. Cette entrée doit rester vide ou complètement omise lors de connexion Internet. Si une adresse IP est indiqué ici, OpenVPN écoute les demandes de connexion entrante uniquement sur cet adresse IP. Si vous voulez assurer une connexion WLAN, vous devez enregistrer ici l'adresse IP de la carte WLAN qui est sur le routeur fli4l.

OPENVPN_x_LOCAL_PORT Par défaut : `OPENVPN_x_LOCAL_PORT="`

On indique ici le numéro du Port, sur lequel le démon OpenVPN écoute. Pour chaque configuration d'OpenVPN vous aurez besoin de réserver le port, c.-à-d. que ce port ne peut être utilisé que par la liaison OpenVPN et ne peut être utilisé par aucun autre programme sur le routeur fli4l. Les paramètres des variables `OPENVPN_x_REMOTE_PORT` et

OPENVPN_x_LOCAL_PORT doivent être installé pour une liaison OpenVPN ! Si vous paramétrez la variable OPENVPN_x_REMOTE_PORT='10111' d'un côté du tunnel, on *doit* impérativement placer de l'autre côté du tunnel dans la variable OPENVPN_x_LOCAL_PORT='10111' le même port.

Encore une fois : il est très important d'ajuster ces réglages sur les deux côtés respectifs de l'OpenVPN, autrement la liaison entre les partenaires OpenVPN ne sera pas possible.

Afin qu'OpenVPN puisse écouter les connexions entrantes, OpenVPN ouvre indépendamment les ports qui sont indiqués dans la variable OPENVPN_x_LOCAL_PORT pour le filtrage de paquets. Si vous ne le souhaité pas, vous pouvez ajuster les ports dans la variable OPENVPN_DEFAULT_OPEN_OVPNPORT (Page 12). Il n'est pas nécessaire d'activer la variable OPENVPN_DEFAULT_OPEN_OVPNPORT='yes' puisque c'est le paramètre par défaut !

Il n'est pas possible pour OpenVPN d'écouter des ports en dessous de 1025. Si vous voulez configurer un port en dessous comme par ex. si vous voulez configurer OpenVPN comme serveur tcp sur le port 443 (port https), vous devez transmettre par le port 443 les paquets filtrés vers un port supérieur à 1024. Par ex votre OpenVPN écoute sur le port 5555 il transmettra les paquets vers le port 443, cela doit être enregistré dans la variable PF_PREROUTING comme ceci.

```
PF_PREROUTING_5='tmpl:https dynamic REDIRECT:5555'
```

OPENVPN_x_SECRET Par défaut : OPENVPN_x_SECRET="

OpenVPN a besoin pour crypter une connexion OpenVPN d'un soi-disant fichier clé. Ce fichier clé peut être produit directement avec OpenVPN sous Windows ou Linux. Pour les débutants, vous avez soit le logiciel OpenVPN sous Windows ou soit le WebGUI, interface graphique pour OpenVPN. Si vous ne voulez pas utiliser OpenVPN sous Windows, mais créer seulement le ou les fichiers clés pour OpenVPN, il suffit, d'installer ces quelques fichiers *OpenVPN User-Space Components*, *OpenSSL DDLs*, *OpenSSL Utilities*, *Add OpenVPN to PATH* et *Add Shortcuts to OpenVPN*. Au démarrage d'OpenVPN vous avez dans le menu la commande *Generate a static OpenVPN key*, qui est nécessaire pour produire le fichier clé. Après avoir activé cette commande dans le menu, un message apparais «Randomly generated 2048 bit key written to C:/Programme/OpenVPN/config/key.txt». Le fichier key.txt sera créé il est essenciel pour l'utilisation de ce fichier, de copier celui-ci dans le répertoire <config>/etc/openvpn et de renommer le fichier key.txt de façon à ce que le nom du fichier soit significatif pour être placé dans cette variable.
Vous pouvez aussi produire le fichier clé automatiquement au démarrage du routeur fli4l, pour cela, vous devez mettre la variable OPENVPN_CREATE_SECRET sur 'yes'. Si vous configurez pour la première fois OpenVPN, vous devez enregistrer toutes les données du fichier config et placer la variable OPENVPN_DEFAULT_CREATE_SECRET (Page 11) sur 'yes', vous pouvez produire plusieurs fichiers clés pour plusieurs liaisons OpenVPN ou produire qu'un seul fichier clé pour une liaison OpenVPN, pour cela vous devez placer la variable OPENVPN_x_CREATE_SECRET sur 'yes'. Après le démarrage du routeur fli4l, le ou les fichiers clé(s) seront alors produits automatiquement et placés ces fichiers dans le dossier /etc/openvpn avec leur nom respectif, voir ci-dessous. Le ou les fichiers clé(s) peuvent alors être transféré avec le SCP ou copié sur le support de boot. Vous devez replacer la variable de création de fichier clé sur 'no'. Ne laissez pas la variable de création de clé sur 'yes' car à chaque redémarrage du routeur fli4l de nouveaux fichiers clés seront produits par le démon OpenVPN. Il sera alors impossible de déployer le tunnel VPN.

Si vous voulez utiliser l'interface Web pour produire le ou les fichiers clé(s), vous devez mettre la variable `OPENVPN_x_CREATE_SECRET` sur `'webgui'`. Vous devez vous connecter sur l'interface Web, dans la fenêtre générale sélectionner gestion clé. Pour plus de précision vous pouvez aller voir le paragraphe 1.1.6.
Astuce : avec la commande

```
openvpn --genkey --secret <dateiname>
```

vous pouvez produire par ligne de command un fichier clé sur la console du routeur fli4l. Les fichiers clés doivent être copiés dans le dossier `<config>/etc/openvpn` comme indiqué dans l'illustration ci-dessous. Le nom du ou des fichiers clés doivent ensuite être placé dans la variable `OPENVPN_x_SECRET`. Alors, les fichiers clés seront compactés et intégrés dans le fichier opt-Archives.

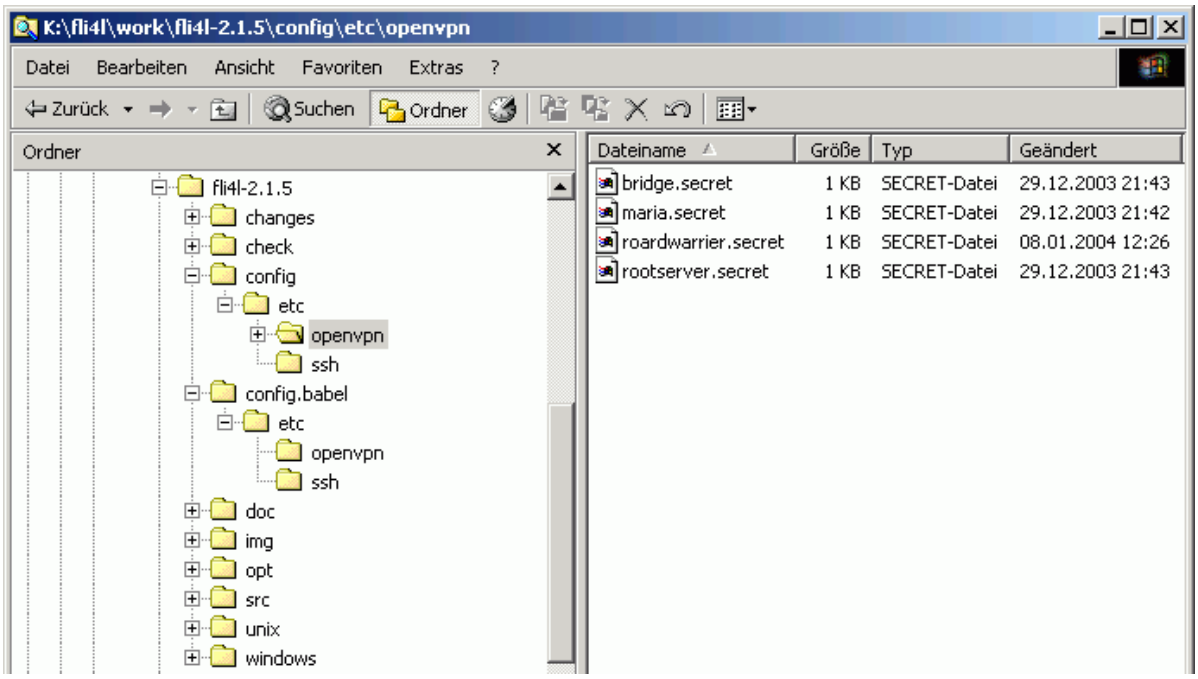

FIGURE 1.2. – fli4l répertoire OpenVPN avec les fichiers *.secret

OPENVPN_x_TYPE Par défaut : `OPENVPN_x_TYPE="`
On peut utiliser une liaison OpenVPN soit par tunnel, soit par Bridge. OpenVPN par tunnel utilise exclusivement le trafic IP routé. OpenVPN par bridge, le transfère se fait non seulement en trafic IP et aussi en frames Ethernet, par ex. avec le protocole IPX ou NetBEUI. Si vous utilisez OpenVPN avec le transport frames Ethernet, dans tous les cas le paquetage advanced_networking est nécessaire. Veuillez considérer que l'utilisation du Bridging avec une connexion DSL peut être lente !

1.1.3. OpenVPN - Configuration du bridge

Si vous utilisez OpenVPN par Bridge, vous pouvez paramétrer les entrées suivantes, N'oubliez pas, que lors de l'utilisation d'un Bridge sur Internet, avec le trafic Broadcast on a besoin d'une

bande passante relativement élevée.

Considérer que les réglages suivants ne sont valables que si la variable OPENVPN_x_TYPE (Page 7) a été paramétrée sur 'bridge' pour une liaison OpenVPN ! En outre, la configuration du bridge dans le paquetage advanced_networking est nécessaire, auquel cas la liaison VPN se bloque.

OPENVPN_x_BRIDGE Par défaut : OPENVPN_x_BRIDGE=""

On indique ici, le nom du Bridge, avec lequel la liaison OpenVPN doit se faire. Donc si dans la variable BRIDGE_DEV_x_NAME='cuj-br' du paquetage advanced_networking le nom est 'cuj-br', vous devez indiquer également le même nom ici pour avoir une liaison OpenVPN par Bridge valide.

OPENVPN_x_BRIDGE_COST Par défaut : OPENVPN_x_BRIDGE_COST=""

Si vous utilisez STP (voir http://de.wikipedia.org/wiki/Spanning_Tree ou la documentation dans le paquetage advanced_networking) vous pouvez indiquer ici le coût de la connexion.

OPENVPN_x_BRIDGE_PRIORITY Par défaut : OPENVPN_x_BRIDGE_PRIORITY=""

Si vous utilisez STP (voir http://de.wikipedia.org/wiki/Spanning_Tree ou la documentation dans le paquetage advanced_networking) vous pouvez indiquer ici la priorité de la connexion.

1.1.4. OpenVPN - Configuration du tunnel

OPENVPN_x_REMOTE_VPN_IP Par défaut : OPENVPN_x_REMOTE_VPN_IP=""

Considérer que les réglages suivants ne sont valables que si la variable OPENVPN_x_TYPE (Page 7) a été paramétrée sur 'tunnel' pour une liaison OpenVPN !

Adresse IP VPN du poste éloigné pour une liaison OpenVPN. Les adresses IP VPN sont nécessaires et peuvent être choisies presque librement. Ci-dessous les restrictions pour le choix d'une adresse IP VPN sont les suivantes :

- L'adresse IP ne peut pas être utilisée dans le réseau local. Elle ne peut pas non plus se trouver dans le sous-réseau du routeur fli4l.
- L'adresse IP ne peut pas être utilisé pour la restauration système par le réseau.
- L'adresse IP ne peut pas faire partie d'un réseau IP_ROUTE_x.
- L'adresse IP ne peut pas faire partie d'un réseau ISDN_CIRC_ROUTE_x.
- L'adresse IP ne peut pas faire partie d'un réseau CIPE_ROUTE_x.
- L'adresse IP ne peut pas faire partie d'un réseau OPENVPN_ROUTE_x.
- Il est entendu que l'adresse IP ne doit pas appartenir à un réseau fli4l ou à un réseau du routeur fli4l.

Comme vous le voyez, l'adresse IP ne peut être utilisée nulle part ailleurs. Avant que vous commenciez la configuration d'OpenVPN, vous devez chercher une adresse IP qui n'est pas utilisée par de réseau, avec laquelle vous pouvez installer une liaison VPN. L'adresse IP du réseau devrait aussi absolument faire partie d'un réseau privé (voir http://ftp.univie.ac.at/netinfo/rfc/rfc1597.txt).

OPENVPN_x_LOCAL_VPN_IP Par défaut : OPENVPN_x_LOCAL_VPN_IP=""

Ce réglage est valable, que si la variable OPENVPN_x_TYPE (Page 7) est paramétrée sur 'tunnel' pour pouvoir régler une liaison OpenVPN.

On indique ici l'adresse IP de l'OpenVPN local périphérique tunX. Le choix de l'adresse IP est soumis à la même restriction que la variable OPENVPN_x_REMOTE_VPN_IP (Page 8).

Il est d'ailleurs possible d'utiliser pour toutes les liaisons OpenVPN locale, la même adresse IP qui est dans la variable OPENVPN_x_LOCAL_VPN_IP. Ainsi, il est plus facilement pour un hôte utilisé la même adresse IP dans le VPN. Cela simplifie énormément les règles de filtrage de paquets.

OPENVPN_x_IPV6 Par défaut : OPENVPN_x_IPV6='no'

Avec cette variable vous pouvez activez le support IPv6 natif pour OpenVPN. Cette programmation est assez nouvelle et peut être qualifiée d'expérimentale. pour cela vous devez activer le paquetage OPT_IPV6 et le configurer. Si vous indiquez OPENVPN_x_IPV6='no' et/ou OPT_IPV6='no' ces variables sont en relations, elle sera ignorer.

Attention ! Actuellement, il n'existe pas de contrôle si les informations se chevauchent avec d'autres parties de la configuration ! Ceci s'applique aux variables OPENVPN_x_LOCAL_VPN_IPV6, OPENVPN_x_REMOTE_VPN_IPV6 et OPENVPN_x_ROUTE_x.

OPENVPN_x_REMOTE_VPN_IPV6 Par défaut : OPENVPN_x_REMOTE_VPN_IPV6="

La variable IPv6 est égal à celle-ci OPENVPN_x_REMOTE_VPN_IP (Page 8).

```
OPENVPN_X_REMOTE_IPV6='FD00::1'
```

OPENVPN_x_LOCAL_VPN_IPV6 Par défaut : OPENVPN_x_LOCAL_VPN_IPV6="

La variable IPv6 est la même que la variable OPENVPN_x_LOCAL_VPN_IP (Page 8). si vous n'indiquez pas de sous-réseau, /64 sera automatiquement utilisé comme sous-réseau.

```
OPENVPN_X_LOCAL_IPV6='FD00::2/112'
```

OPENVPN_x_ROUTE_N Par défaut : OPENVPN_x_ROUTE_N="

Ce réglage n'est valable, que si la variable OPENVPN_x_TYPE (Page 7) est paramétrée sur 'tunnel' pour pouvoir régler une liaison OpenVPN.

Les routes (ou les destinations) données seront lu automatiquement, aussitôt qu'OpenVPN est démarré. On indique ici le nombre de route, on peut mettre jusqu'à 50 réseaux pour une liaison OpenVPN. Il faudra tout de même pour chaque réseau indiquer une adresse IP dans une variable différente OPENVPN_x_ROUTE_x pour le routeur.

Veuillez noter que vous devez paramétrer des règles de filtrage pour les paquets dans les variables OPENVPN_PF_FORWARD_x OPENVPN_PF_INPUT_x ou varOPENVPN_PF6_FORWARD_x OPENVPN_PF6_INPUT_x. OpenVPN permet uniquement l'envoi ICMP sur une liaison VPN tout autre fluxde données est interdit. Vous trouverez plus de détails dans OPENVPN_x_PF_INPUT_N (Page 17) et OPENVPN_x_PF_FORWARD_N (Page 18) ou sous OPENVPN_x_PF6_INPUT_N (Page 18) et OPENVPN_x_PF6_FORWARD_N (Page 19)

OPENVPN_x_ROUTE_x Par défaut : OPENVPN_x_ROUTE_x="

Vous devez indiquer ici les adresses IP des réseaux, qui seront accessibles par le biais du poste éloigné de la liaison VPN. Par ex. les postes éloignés du tunnel OpenVPN veulent atteindre les réseaux 192.168.33.0/24 et 172.18.0.0/16, vous devez respectivement enregistrer ces deux réseaux dans OPENVPN_x_ROUTE_x. Vous pouvez également enregistrer un hôte à router avec la valeur (/32).

Si une route par défaut doit être paramétrée via un tunnel OpenVPN, entrez s.v.p. 0.0.0.0/0 ou : :/0 et un flag (ou option) optionnel pour la route. Encore une fois, vous devez activer OPT_IPv6 pour les routes IPv6, l'adresse IPv6 locale et distante du tunnel doivent être établies et la variable OpenVPN_x_IPV6 être sur yes. OpenVPN reconnaît les différentes possibilités de route par défaut mise en place, pour lesquels, vous pourrez choisir un flag. Chaque méthode qui définie une route par défaut, a ces avantages et ces inconvénients. Pour le moment, OpenVPN prend en charge les flags suivantes :

local Vous devez utiliser le flag *local*, si avec openVPN se trouve un serveur à l'intérieur d'un sous-réseau qui soit directement accessible du routeur fli4l. Ce cas est fréquent, par exemple pour l'installation d'une route par défaut sur OpenVPN avec un serveur WLAN.

def1 Avec ce flag on peut enregistrer dans OpenVPN une route d'un hôte supplémentaire, par exemple 0.0.0.0/1 et 128.0.0.0/1 deux nouvelles routes. Ces deux routes fonctionnent comme une seule route par défaut et sur ces routes OpenVPN pourra transférer par le tunnel le trafic complètement (crypté) avec (en plus une route pour un hôte accessible).

Ces flags sont facultatives, pour l'installation de chacune des méthodes avec une route par défaut sur OpenVPN. Le choix de la méthode se fera sur la version actuelle OpenVPN, l'option *local* est utilisé pour une installation standard.

```
OPENVPN_1_ROUTE_N='3'
OPENVPN_1_ROUTE_1='192.168.33.0/24'
OPENVPN_1_ROUTE_2='172.18.0.0/16'
OPENVPN_1_ROUTE_3='2001:db8:/32'
```

OpenVPN - Délégation de DNS et DNS inversé

OPENVPN_x_DOMAIN Par défaut : `OPENVPN_x_DOMAIN=""`

Vous indiquez dans cette variable un domaine distant. Cette variable peut contenir plusieurs noms de domaine, vous devez les séparer par un espace. Si cette variable est uniquement paramétrée (sans indiquer de serveur DNS supplémentaire), alors, on suppose que l'ordinateur opposé dans le tunnel écoute l'adresse IP du serveur DNS, (voir `OPENVPN_x_REMOTE_VPN_IP` (Page 8)). Bien sûr, pour cela, il faut que sur le routeur distant les requêtes DNS entrantes soit acceptés, (par exemple via la variable `OPENVPN_x_INPUT_y='tmpl:dns ACCEPT'`).

OPENVPN_x_ROUTE_x_DOMAIN Par défaut : `OPENVPN_x_ROUTE_x_DOMAIN=""`

Dans cette variable différents sous-réseaux peuvent également être associés à différents domaines. Avec la variable `OPENVPN_x_ROUTE_y` vous pouvez configurer d'autre serveur de domaine. Si la variable `OPENVPN_x_ROUTE_y_DNSIP` est paramétrée et si le serveur existe il sera utilisé, dans le cas contraire, c'est le serveur de la variable `OPENVPN_x_DNSIP` qui est utilisé. L'action est la même que la variable `OPENVPN_x_DOMAIN` de la documentation, cette méthode convient également.

OPENVPN_x_DNSIP Par défaut : `OPENVPN_x_DNSIP=""`

Si le point de terminaison du tunnel n'a pas de serveur DNS, l'adresse IP du serveur DNS compétent peut être spécifiée ici. Si vous n'indiquez rien dans cette variable, c'est la variable `OPENVPN_x_REMOTE_VPN_IP` (Page 8) qui sera utilisé.

OPENVPN_x_ROUTE_x_DNSIP Par défaut : `OPENVPN_x_ROUTE_x_DNSIP="`

Dans cette variable, vous pouvez router différents sous-réseaux, pour desservir différents serveurs DNS - Vous pouvez définir dans la variable `OPENVPN_x_ROUTE_x` (Page 9) votre propre serveur compétent.

1.1.5. Paramètres experts

Dans ce chapitre tout les paramètres des variables sont facultatifs et ne doivent être modifiés que si la liaison OpenVPN fonctionne correctement avec les paramètres essentiels, vous pouvez alors utiliser les paramètres optimisés, (par exemple pour avoir d'autres algorithmes de cryptages).

Tous les paramètres des variables `OPENVPN_DEFAULT_` décrits ci-dessous sont optionnels et agissent sur toutes les configurations OpenVPN, c.-à-d. que ces options n'ont pas besoin d'être rajoutées dans le fichier configuration openvpn.txt. Si l'entrée correspondante n'est pas dans le fichier openvpn.txt, lors du script de démarrage les valeurs par défaut sont quand même utilisées par OpenVPN. Si vous ne prévoyez pas de modifier les valeurs standard, ne rien écrire de plus dans le fichier de configuration openvpn.txt !

Paramètres généraux

OPENVPN_DEFAULT_CIPHER Par défaut : `OPENVPN_DEFAULT_CIPHER='BF-CBC'`

Méthodes de codage disponibles. L'algorithme de chiffrage `'BF-CBC'` est utilisé par toutes les versions OpenVPN (aussi par les versions spécifiques de fli4l) c'est le réglage standard.

OPENVPN_DEFAULT_COMPRESS Par défaut : `OPENVPN_DEFAULT_COMPRESS='yes'`

OpenVPN utilise la compression de données LZO adaptative, pour augmenter le débit d'une connexion. Adaptatif cela signifie qu'OpenVPN reconnaît indépendamment, si c'est un paquet déjà compressé qui est envoyé sur la liaison OpenVPN par ex. un fichier ZIP. Dans ce cas, la compression de données est mise hors circuit, et sera à nouveau réactivée pour les données qui ont besoin d'une compression avant d'être transférées. Il y a aucune raison pour désactiver la compression de données, car le débit sera augmenté quasi gratuitement. Le seul désavantage de la compression de données est une faible augmentation du temps de latence elle est de quelques millisecondes. Les Online Games qui joue par l'intermédiaire du VPN, le temps de réaction ("meilleur" ping) est crucial, dans ce cas il est judicieux de mettre hors circuit la compression de données.

OPENVPN_DEFAULT_CREATE_SECRET Par défaut : `OPENVPN_DEFAULT_CREATE_SECRET='no'`

Avec cette variable, OpenVPN produit automatiquement une clés au démarrage du routeur fli4l. Toutefois, la connexion entre OpenVPN n'est pas commencée. Pour plus de détails, veuillez lire le point suivant `OPENVPN_x_SECRET` (Page 6).

OPENVPN_DEFAULT_DIGEST Par défaut : `OPENVPN_DEFAULT_DIGEST='SHA1'`

On paramètre ici, l'algorithme de hachage disponible. OpenVPN utilise la méthode d'algorithme de hachage `'SHA1'` comme réglage standard.

OPENVPN_DEFAULT_FLOAT Par défaut : `OPENVPN_DEFAULT_FLOAT='yes'`

Si le poste distant sur une liaison OpenVPN utilise une adresse DynDNS, il est possible qu'à tout moment l'adresse IP du poste distant change sur OpenVPN. Pour qu'OpenVPN accepte l'adresse IP modifiée, on doit paramétrer la variable `OPENVPN_DEFAULT_FLOAT` sur

'yes'. Avec le paramètre 'no' la modification d'adresse IP n'est pas permise. Il est généralement judicieux de placer 'no' avec une liaison WLAN ou avec un poste distant qui a une adresse IP statique sur une liaison OpenVPN (par ex. pour soumettre différents serveurs root soumissionnaires). Vous pouvez modifier ce paramètre et tous les autres paramètres OPENVPN_DEFAULT_ pour définir une liaison OpenVPN.

OPENVPN_DEFAULT_KEYSIZE Par défaut : OPENVPN_DEFAULT_KEYSIZE="

La longueur de code (=KEYSIZE) dépend de la méthode de codage utilisée. Modifiez ce réglage, si vous devez travailler en collaboration avec un poste distant d'OpenVPN, qui ne respectent pas les valeurs par défaut utilisées ou que vous ne pouvez pas agir sur ces paramètres. Alors, vous pouvez déterminer vous-mêmes la longueur clé, cette valeur devrait toujours rester vide. OpenVPN applique une longueur de code optimale pour chaque méthode de codage.

OPENVPN_DEFAULT_OPEN_OVPNPORT Par défaut : OPENVPN_DEFAULT_OPEN_OVPNPORT='yes'

Afin qu'un poste distant puisse prendre contact avec vous par OpenVPN, vous devez régler le filtrage de paquets conformément à votre routeur fli4l. Vous devez généralement paramétrer les protocoles TCP ou UDP dans la variable OPENVPN_x_PROTOCOL, ainsi OpenVPN écoutera les adresses que vous avez réglées dans PF_INPUT_x (Page **??**) du fichier base.txt. Avec le paramètre 'yes' les règles de filtrage de paquets seront produites automatiquement. Pour certaines liaisons VPN, vous pouvez placer la variable sur 'no' et de définir soi-même les règles du filtrage de paquets correspondants.

OPENVPN_DEFAULT_ALLOW_ICMPPING Par défaut : OPENVPN_DEFAULT_ALLOW_ICMPPING='yes'

Si l'on paramètre 'yes' dans cette variable, cela permet aux paquets de traverser le filtrage, pour tester la configuration d'une liaison, de sorte que le ping puisse passer le filtrage de paquets. Si vous n'avez pas de raison importante, le Ping ICMP devrait toujours être autorisé. Ce réglage n'a *rien* à voir avec l'option Ping d'OpenVPN !

OPENVPN_DEFAULT_PF_INPUT_LOG Par défaut : OPENVPN_DEFAULT_PF_INPUT_LOG='BASE'

Avec 'yes' ou 'no' on enregistre ou pas dans un fichier log le détaille du filtrage de paquets INPUT (ou entrant), si le paquet de données est refusé sur une liaison VPN et si vous avez placé 'BASE' le paramètre de la variable 'PF_INPUT_LOG=' du fichier base.txt est pris en charge.

OPENVPN_DEFAULT_PF_INPUT_POLICY Par défaut : OPENVPN_DEFAULT_PF_INPUT_POLICY='REJECT'

Ce paramètre correspond à la variable 'PF_INPUT_POLICY=' (Page **??**) du fichier base.txt. Si vous paramétrez 'BASE' le paramètre de la variable 'PF_INPUT_POLICY=' du fichier base.txt est pris en charge.

OPENVPN_DEFAULT_PF_FORWARD_LOG Par défaut : OPENVPN_DEFAULT_PF_FORWARD_LOG='BASE'

Avec 'yes' ou 'no' on enregistre dans un fichier log le détaille du filtrage de paquets FORWARD pour une liaison VPN, si vous paramétrez 'BASE' le paramètres de la variable 'PF_FORWARD_LOG=' du fichier base.txt est pris en charge.

OPENVPN_DEFAULT_PF_FORWARD_POLICY Par défaut : OPENVPN_DEFAULT_PF_FORWARD_POLICY='REJECT'

Ce paramètre correspond à la variable 'PF_FORWARD_POLICY=' (Page **??**) du fichier base.txt. Si vous paramétrez 'BASE' le paramètre de la variable 'PF_FORWARD_POLICY=' du fichier base.txt est pris en charge.

OPENVPN_DEFAULT_PING Par défaut : OPENVPN_DEFAULT_PING='60'

Une fois le tunnel OpenVPN installé et reconnu, Pour savoir si le poste éloigné est toujours joignable, pour tenir la liaison ouvert, on envoie par intervalle régulier indiqué en secondes un ping cryptographié c'est plus sûr. Avec le paramètre 'off' aucun ping n'est envoyé sur la liaison OpenVPN, les données seront uniquement transférées sur le tunnel VPN.

OPENVPN_DEFAULT_RENEG_SEC Par défaut : OPENVPN_DEFAULT_RENEG_SEC='3600'

Dans cette variable vous pouvez paramétrer le RENEG-SEC pour OpenVPN, lorsque vous avez une connexion DSL (ou ISDN) un peu lente, vous n'aurez pas de délai d'attente avant l'arrêt de la connexion.

OPENVPN_DEFAULT_PING_RESTART Par défaut : OPENVPN_DEFAULT_PING_RESTART='180'

On indique ici l'intervalle en secondes. S'il n'y a pas de ping ou si aucune donnée n'est transmise avec succès sur la liaison OpenVPN, la liaison OpenVPN correspondante redémarrera. La valeur de la variable OPENVPN_DEFAULT_PING_RESTART doit être plus grande que la valeur de la variable OPENVPN_DEFAULT_PING. Le paramètre 'off' empêche le redémarrage automatique de la liaison OpenVPN.

OPENVPN_DEFAULT_RESOLV_RETRY Par défaut : OPENVPN_DEFAULT_RESOLV_RETRY='infinite'

Dans la variable OPENVPN_x_REMOTE_HOST ou OPENVPN_x_LOCAL_HOST si le nom du DNS est mis à la place d'adresse IP, au démarrage de la liaison OpenVPN le nom sera transformé en une adresse IP. Si la résolution a échoué, OpenVPN essaiera dans la période indiquée en seconde de résoudre à nouveau l'adresse DNS. Finalement s'il ne réussit pas dans le temps alloué, aucune liaison OpenVPN ne sera réalise. Avec le paramètre 'infinite' (= à l'infini) dans la variable, OpenVPN essaiera infiniment de résoudre le DNS. Ce réglage ne devrait pas être modifié ou uniquement dans des cas particulier !

OPENVPN_DEFAULT_RESTART Par défaut : OPENVPN_DEFAULT_RESTART='ip-up'

Après une déconnexion de la liaison, il est logique que le tunnel OpenVPN correspondant redémarre immédiatement, afin que l'interruption du tunnel soit si possible la plus courte possible. Pour toutes les liaisons OpenVPN, qui disposent d'une connexion ADSL ou ISDN, il convient de paramétrer ici 'ip-up'. En revanche pour une liaison OpenVPN via une connexion WLAN (ou sans fil), vous devez paramétrer ici 'never'. Dans ce cas, la connexion ne sera pas redémarrée après une déconnexion, car une connexion WLAN est une connexion indépendante. Si le tunnel OpenVPN est sur une connexion ISDN et si la variable est sur ISDN_CIRC_x_TYPE='raw', vous devez alors enregistrer ici 'raw-up'.

OPENVPN_DEFAULT_PROTOCOL Par défaut : OPENVPN_DEFAULT_PROTOCOL='udp'

Avec cette Variable, on règle le protocole par défaut qui doit être utilisée. Le protocole UDP est normalement un très bon choix, toutefois il est possible de travailler avec le protocole TCP. Mais avec celui-ci vous avez une surcharge considérable. Les réglages possibles sont 'udp' ou 'udp6', 'tcp-server' ou 'tcp-server6', 'tcp-client' ou 'tcp-client6'. Les paramètres 'tcp-server' ou 'tcp-client' sont, en règle générale utilisés lorsqu'un tunnel VPN est configuré pour d'autres filtrages de paquets ou pour d'autres tunnels spécifiques, Si vous n'envisagez pas d'utiliser un tunnel spécifique, vous devez *toujours* utiliser la valeur standard 'udp'. Si vous ajoutez '6' le tunnel IPv6 pourra passer par un (WAN) et pourra être accessible via Internet IPv6.

OPENVPN_DEFAULT_START Par défaut : `OPENVPN_DEFAULT_START='always'`

Une liaison OpenVPN peut être soit toujours en fonctionnement (`='always'`) ou soit avec un démarrage manuelle (`='on-demand'`). Si vous avez besoin d'arrêter ou démarrer une liaison OpenVPN vous pouvez le faire par l'intermédiaire du WebGUI (voir 1.1.6). Vous pouvez aussi contrôler le démarrage sur la console du routeur fli4l. Pour cela vous devez écrire les commandes suivantes directement sur la console fli4l et les exporter :

```
cd /etc/openvpn
openvpn --config name.conf --daemon openvpn-name
```

De cette façon, le tunnel OpenVPN sera démarré et fonctionnera à présent en arrière-plan. Naturellement a la place du fichier `name.conf` vous devez mettre le nom de votre fichier de configuration qui est dans le répertoire `/etc/openvpn`.

OPENVPN_DEFAULT_VERBOSE Par défaut : `OPENVPN_DEFAULT_VERBOSE='2'`

Avec cette variable on indique comment OpenVPN doit communiquer. Si la liaison VPN fonctionne parfaitement, il est possible de mettre cette valeur sur `'0'` pour empêcher les messages de débogages. Pour les premiers essais, il est logique de mettre la valeur sur `'3'`. Plus la valeur augmente plus vous avez de messages de débogages et aident parfois à trouver les erreurs. La valeur maximale est de `'11'`.

OPENVPN_DEFAULT_MANAGEMENT_LOG_CACHE Par défaut : `OPENVPN_DEFAULT_MANAGEMENT_LOG_CACHE='100'`

Cette variable indique le nombre lignes à stocker dans le fichier Log. Ce fichier Log peut alors être consulté dans le WebGUI (Page 19).

OPENVPN_DEFAULT_MUTE_REPLAY_WARNINGS Par défaut : `OPENVPN_DEFAULT_MUTE_REPLAY_WARNINGS='no'`

Avec cette variable on règle, lors de la réception d'un double paquets une alerte est envoyé dans le fichier Log, car cela, référence peut être à un problème de sécurité dans le réseau. En particulier avec une connexion fragile par WLAN, souvent, il arrive que les paquets soient envoyés deux fois. Il faut afficher judicieusement les avertissements, afin que ceux-ci ne remplissent pas le fichier Log. Le réglage de cette variable n'a *pas* d'influence sur la sécurité d'une liaison OpenVPN.

OPENVPN_DEFAULT_MSSFIX Par défaut : `OPENVPN_DEFAULT_MSSFIX="`

Dans la variable MSSFIX on paramètre la taille du paquet TCP pour une liaison VPN. Cette option sera désactivée si la variable est sur `OPENVPN_DEFAULT_MSSFIX='0'`. Si les options FRAGMENT et MSSFIX sont laissés vides, la taille de la fragmentation sera utilisée automatiquement. Ce réglage fonctionne que si la variable est paramétrée sur `OPENVPN_x_PROTOCOL='udp'`.

OPENVPN_DEFAULT_FRAGMENT Par défaut : `OPENVPN_DEFAULT_FRAGMENT='1300'`

Active la fragmentation interne de la taille des paquets en x octets sur OpenVPN. Ce réglage fonctionne que si la variable est sur `OPENVPN_x_PROTOCOL='udp'`. Avec le paramètre `OPENVPN_DEFAULT_FRAGMENT='0'`, la fragmentation est totalement désactivé.

OPENVPN_DEFAULT_TUN_MTU Par défaut : `OPENVPN_DEFAULT_TUN_MTU='1500'`

Réglage du MTU en x octets pour l'adaptateur OpenVPN virtuel. Si vous savez ce que vous faite cette option peut être modifiée. Il est plus logique de travailler principalement et seulement avec les options FRAGMENT ou MSSFIX.

OPENVPN_DEFAULT_TUN_MTU_EXTRA Par défaut : `OPENVPN_DEFAULT_TUN_MTU_EXTRA=""`

Si vous avez paramétrer la variable sur `OPENVPN_x_PROTOCOL='bridge'`, 32 octets de mémoires supplémentaires sont réservés sur le routeur pour l'administration de l'amortissement du débit. Avec le paramètre `OPENVPN_x_PROTOCOL='tunnel'` aucune mémoire supplémentaire n'est réservée. Ce réglage ne se répercute que sur le besoin de mémoire dans le routeur et n'a pas d'influence sur le volume de données envoyées sur le tunnel.

OPENVPN_DEFAULT_LINK_MTU Par défaut : `OPENVPN_DEFAULT_LINK_MTU=""`

Réglage du MTU en x octets pour une liaison OpenVPN. Si vous savez ce que vous faites, cette option peut être modifiée. Il est plus logique de travailler principalement et seulement avec les options FRAGMENT ou MSSFIX.

OPENVPN_DEFAULT_SHAPER Par défaut : `OPENVPN_DEFAULT_SHAPER=""`

Vous pouvez ici limiter le débit *sortant* du tunnel en octet par seconde, les valeurs possibles sont de 100 octets par seconde à 100000000 octets. Avec une valeur de 1000 octets par seconde, vous devriez réduire le MTU de la liaison VPN et le délaie du ping augmentera fortement. Si vous voulez limiter le débit dans les deux sens du tunnel, vous devez ajuster le réglage sur les deux postes de chaque côté du tunnel VPN.

Dans la version OpenVPN actuel, le Shaping ne fonctionne pas correctement, c'est à dire que la vitesse de transfert dans un tunnel configuré au moyen du Shaping oscille, il peut-être extrêmement instable ou le débit peut tomber totalement. Le problème peut produire des comportements complètements différents selon le matériel employé. Actuellement, la fonction Shaping doit être utilisé avec prudence, dans le doute, lors de chaque changement, la liaison doit être testée intensivement.

OPENVPN_EXPERT Par défaut : `OPENVPN_EXPERT='no'`

Le mode expert vous permet d'utiliser les fichiers natif de configuration d'OpenVPN. Ils sont placés dans les sous répertoires etc/openvpn et etc/openvpn/scripts. Tous les fichiers se trouvant dans ce répertoire seront transférés au routeur.

Le mode expert ignore le reste des variables de configuration. Il faut donc régler la variable sur `OPENVPN_N='0'`.

Avec le mode expert, des règles du Firewall ne sont pas établies. Vous devez les entrer manuellement dans le fichier base.txt.

Connexion des paramètres spécifiques

Les options OpenVPN suivantes, s'appliquent uniquement pour les liaisons OpenVPN respectives. Ici aussi Il y a peux de définitions impératives. La plupart des options peuvent simplement être omises. On peut considérer, que toutes valeurs par défaut indiquées dans les variables `OPENVPN_DEFAULT_x` sont équivalentes aux variables suivantes. Donc si vous modifiez la valeur de la variable `OPENVPN_DEFAULT_` correspondante, cette valeur par défaut vaut pour tous les liaisons OpenVPN, en général il ne faut pas écraser la valeur par défaut.

OPENVPN_x_NAME Par défaut : `OPENVPN_x_NAME=""`

On indique ici le nom de la liaison OpenVPN, la longueur du nom ne doit pas dépasser 16 caractères. Ce nom peut contenir des lettres, des chiffres et le signe '-'. Ce nom de fichier de configuration sera enregistré dans le répertoire /etc/openvpn (avec l'extension .conf). En outre, le nom apparaîtra dans le syslog. Par exemple si vous enregistrez le

nom 'peter', l'entrée dans le syslog sera indiqué, 'openvpn-peter'. De cette façon, vous pouvez mieux distinguer les différentes liaisons OpenVPN.

OPENVPN_x_ACTIV Par défaut : OPENVPN_x_ACTIV='yes'

Dans cette variable si vous paramétrez 'no' vous désactivez la liaison OpenVPN, mais vous ne supprimez pas la configuration, Les données de configuration sont alors incluses dans le fichier rc.cfg, mais vous ne pouvez pas produire de liaison OpenVPN.

OPENVPN_x_CHECK_CONFIG Par défaut : OPENVPN_x_CHECK_CONFIG='yes'

Dans certaine circonstance, les contrôles étendus d'OpenVPN sont trop stricts. Par exemple si vous faites un Backup d'une connexion ISDN et si les entrées de routage utilisé sont les mêmes que la liaison vpn via Internet, le contrôle étendu de ces connexions produit un message d'erreur important. Dans ce cas, le Backup de la connexion ISDN sera désactivé. Pour remédier à ce problème, vous devez mettre la variable sur OPENVPN_x_CHECK_CONFIG='no' pour passer le contrôle de cette liaison.

OPENVPN_x_CIPHER Par défaut voir : OPENVPN_DEFAULT_CIPHER

Voir OPENVPN_DEFAULT_CIPHER (Page 11). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_COMPRESS Par défaut voir : OPENVPN_DEFAULT_COMPRESS

Voir OPENVPN_DEFAULT_COMPRESS (Page 11). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_CREATE_SECRET Par défaut voir : OPENVPN_DEFAULT_CREATE_SECRET='no'

Voir OPENVPN_x_SECRET (Page 6). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_DIGEST Par défaut voir : OPENVPN_DEFAULT_DIGEST

Voir OPENVPN_DEFAULT_DIGEST (Page 11). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_FLOAT Par défaut voir : OPENVPN_DEFAULT_FLOAT

Voir OPENVPN_DEFAULT_FLOAT (Page 11). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_KEYSIZE Par défaut voir : OPENVPN_DEFAULT_KEYSIZE

Voir OPENVPN_DEFAULT_KEYSIZE (Page 12). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_ISDN_CIRC_NAME Par défaut : OPENVPN_x_ISDN_CIRC_NAME=”

On indique ici, le circuit ISDN sur lequel la liaison OpenVPN doit être installée. Le nom du circuit ISDN correspondant est enregistré dans la variable jumpISDNCIRCx-NAMEISDN_CIRC_x_NAME=" du fichier isdn.txt. Le circuit ISDN doit être du type 'raw'.

OPENVPN_x_PING Par défaut voir : OPENVPN_DEFAULT_PING

Voir OPENVPN_DEFAULT_PING (Page 13). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_PROTOCOL Par défaut : OPENVPN_x_PROTOCOL='udp'

On indique ici le protocole qui doit être utilisé pour un tunnel OpenVPN. Les réglages possibles sont 'udp', 'tcp-server' ou 'tcp-client'. Les paramètres 'tcp-server' ou 'tcp-client' sont, en règle généralement utilisé lorsqu'un tunnel VPN doit être développé pour d'autres filtrages de paquets ou pour d'autres tunnels. Si vous n'envisagez *pas* d'utiliser des tunnels spécifiques, vous devez toujours utiliser la valeur standard 'udp'.

OPENVPN_x_RESOLV_RETRY Par défaut voir : OPENVPN_DEFAULT_RESOLV_RETRY

Voir OPENVPN_DEFAULT_RESOLV_RETRY (Page 13). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_PING_RESTART Par défaut voir : OPENVPN_DEFAULT_PING_RESTART

Voir OPENVPN_DEFAULT_PING_RESTART (Page 13). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_START Par défaut voir : OPENVPN_DEFAULT_START

Voir OPENVPN_DEFAULT_START (Page 14). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_VERBOSE Par défaut voir : OPENVPN_DEFAULT_VERBOSE

Voir OPENVPN_DEFAULT_VERBOSE (Page 14). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_MANAGEMENT_LOG_CACHE Par défaut voir : OPENVPN_DEFAULT_MANAGEMENT_LOG_CACHE

Voir OPENVPN_DEFAULT_MANAGEMENT_LOG_CACHE (Page 14). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_MUTE_REPLAY_WARNINGS Par défaut voir : OPENVPN_DEFAULT_MUTE_REPLAY_WARNINGS

Voir OPENVPN_DEFAULT_MUTE_REPLAY_WARNINGS (Page 14). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_RESTART Par défaut voir : OPENVPN_DEFAULT_RESTART

Voir OPENVPN_DEFAULT_RESTART (Page 13). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_ALLOW_ICMPPING Par défaut voir : OPENVPN_DEFAULT_ALLOW_ICMPPING

Voir OPENVPN_DEFAULT_ALLOW_ICMPPING (Page 12). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_OPEN_OVPNPORT Par défaut voir : OPENVPN_DEFAULT_OPEN_OVPNPORT

Voir OPENVPN_DEFAULT_OPEN_OVPNPORT (Page 12). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_PF_INPUT_LOG Par défaut voir : OPENVPN_DEFAULT_PF_INPUT_LOG

Voir OPENVPN_DEFAULT_PF_INPUT_LOG (Page 12). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_PF_INPUT_POLICY Par défaut voir : OPENVPN_DEFAULT_PF_INPUT_POLICY

Voir OPENVPN_DEFAULT_PF_INPUT_POLICY (Page 12). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_PF_INPUT_N Par défaut : OPENVPN_x_PF_INPUT_N='0'

Dans cette variable OPENVPN_x_PF_INPUT_x= vous indiquez le nombre de variables pour le filtrage de paquets.

OPENVPN_x_PF_INPUT_x Par défaut : OPENVPN_x_PF_INPUT_x="

Ici les informations sur le filtrage de paquets sont les même que le paquetage base. On utilise précisément les même syntaxes que dans le fichier base.txt. Il est possible d'utiliser tmpl : et Host_alias. En plus, on a aussi la possibilité d'utiliser quelques noms symboliques spéciaux. Les noms symboliques suivants serons supportés :

VPNDEV Correspond au périphérique actuel de la liaison OpenVPN respectif.

LOCAL-VPN-IP Définit l'adresse IP de la variable `OPENVPN_x_LOCAL_VPN_IP`.

REMOTE-VPN-IP Définit l'adresse IP de la variable `OPENVPN_x_REMOTE_VPN_IP`.

REMOTE-NET Définit l'adresse IP de la variable `OPENVPN_x_REMOTE_VPN_IP` et en plus tous les réseaux qui ont été indiqués dans la variable `OPENVPN_x_ROUTE_x`.

OPENVPN_x_PF_FORWARD_LOG Par défaut voir : `OPENVPN_DEFAULT_PF_FORWARD_LOG`

Voir `OPENVPN_DEFAULT_PF_FORWARD_LOG` (Page 12). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_PF_FORWARD_POLICY Par défaut voir : `OPENVPN_DEFAULT_PF_FORWARD_POLICY`

Voir `OPENVPN_DEFAULT_PF_FORWARD_POLICY` (Page 12). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_PF_FORWARD_N Par défaut : `OPENVPN_x_PF_FORWARD_N='0'`

Dans cette variable `OPENVPN_x_PF_FORWARD_x=` vous indiquez le nombre de variables pour le filtrage de paquets.

OPENVPN_x_PF_FORWARD_x Par défaut : `OPENVPN_x_PF_FORWARD_x="`

Voir `OPENVPN_x_PF_INPUT_x` (Page 17).

OPENVPN_x_PF_PREROUTING_N Par défaut : `OPENVPN_x_PF_PREROUTING_N='0'`

Dans cette variable `OPENVPN_x_PF_PREROUTING_x=` vous indiquez le nombre de variables pour le filtrage de paquets.

OPENVPN_x_PF_PREROUTING_x Par défaut : `OPENVPN_x_PF_PREROUTING_x="`

Voir `OPENVPN_x_PF_INPUT_x` (Page 17).

OPENVPN_x_PF_POSTROUTING_N Par défaut : `OPENVPN_x_PF_POSTROUTING_N='0'`

Dans cette variable `OPENVPN_x_PF_POSTROUTING_x=` vous indiquez le nombre de variables pour le filtrage de paquets.

OPENVPN_x_PF_POSTROUTING_x Par défaut : `OPENVPN_x_PF_POSTROUTING_x="`

Un changement de paramètrage est sortie pour cette variable avec la version 3.5.0 de fli4l (ou la version 3.5.0-rev18133 du tarball). Auparavant on pouvais paramétrer cette variable sous cette forme

`OPENVPN_1_PF_POSTROUTING_1='MASQUERADE'`

Désormais nous devons spécifier une adresse source et une adresse destination. Cela est devenu nécessaire, car les règles POSTROUTING ne pouvaient pas être utilisé pleinement. Dans la plupart des cas, il suffit simplement de compléter la variable avec ces règles `IP_NET_x` (Page **??**) et REMOTE-NET.

Voir `OPENVPN_x_PF_INPUT_x` (Page 17).

OPENVPN_x_PF6_INPUT_N Par défaut : `OPENVPN_x_PF6_INPUT_N='0'`

Le numéro indiquez dans `OPENVPN_x_PF6_INPUT_x=` donne le nombre d'enregistrement de variable.

OPENVPN_x_PF6_INPUT_x Par défaut : `OPENVPN_x_PF6_INPUT_x="`

Comme dans le paquetage IPv6 voici les instructions pour le filtre de paquets. Les syntaxes utilisées sont exactement les mêmes que dans ipv6.txt. Il est possible d'indiquer le tmpl : et les alias des Hôtes. En outre, il est possible d'utiliser des noms symboliques spéciaux. Voir `OPENVPN_x_PF_INPUT_x` (Page 17)

OPENVPN_x_PF6_FORWARD_N Par défaut : `OPENVPN_x_PF6_FORWARD_N='0'`

Le numéro indiquez dans `OPENVPN_x_PF6_FORWARD_x=` donne le nombre d'enregistrement de variable.

OPENVPN_x_PF6_FORWARD_x Par défaut : `OPENVPN_x_PF6_FORWARD_x="`

Voir `OPENVPN_x_PF6_INPUT_x` (Page 18).

OPENVPN_x_MSSFIX Par défaut voir : `OPENVPN_DEFAULT_MSSFIX`

Voir `OPENVPN_DEFAULT_MSSFIX` (Page 14). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_FRAGMENT Par défaut voir : `OPENVPN_DEFAULT_FRAGMENT`

Voir `OPENVPN_DEFAULT_FRAGMENT` (Page 14). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_TUN_MTU Par défaut voir : `OPENVPN_DEFAULT_TUN_MTU`

Voir `OPENVPN_DEFAULT_TUN_MTU` (Page 14). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_TUN_MTU_EXTRA Par défaut voir : `OPENVPN_DEFAULT_TUN_MTU_EXTRA`

Voir `OPENVPN_DEFAULT_TUN_MTU_EXTRA` (Page 15). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_LINK_MTU Par défaut voir : `OPENVPN_DEFAULT_LINK_MTU`

Voir `OPENVPN_DEFAULT_LINK_MTU` (Page 15). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

OPENVPN_x_SHAPER Par défaut voir : `OPENVPN_DEFAULT_SHAPER="`

Voir `OPENVPN_DEFAULT_SHAPER` (Page 15). Contrairement à la variable par défaut, ce réglage n'agit que sur cette liaison OpenVPN.

1.1.6. OpenVPN - WebGUI

Depuis la version 2.1.10, il est possible, de configurer, de démarrer, d'arrêter, d'exporter et d'utiliser d'autres fonctions fondamentales sur le WebGUI pour une liaison OpenVPN. Le paquetage mini_httpd est nécessaire à l'installation. En outre, la variable `OPENVPN_WEBGUI` doit être placée sur 'yes' dans openvpn.txt. Le menu OpenVPN sera alors ajouté sur la page Web de fli4l. Si vous choisissiez ce menu, un aperçu de la configuration des liaisons OpenVPN apparaît, avec le statut et les actions pour chacune des liaisons respectives disponibles (voir l'illustration 1.3).

OpenVPN - WebGUI - Aperçut des connexions

Statut : Le statut d'une liaison est symbolisé par un signal pour piéton. Lorsque le piéton est rouge cela signifie que le processus OpenVPN ne fonctionne pas, le piéton jaune que le processus ne fonctionne pas (encore) avec le poste éloigné, mais que la liaison peut être activée à tout moment et le piéton vert que la liaison est «établie». Des informations plus précises sont indiquées en dessous des icônes piétons. Cela peut être instructif en particulier, pour le statut du piéton «jaune».

Nom : Dans cette colonne, les noms des liaisons OpenVPN sont indiqués comme dans la configuration. En cliquant sur le nom, cela vous conduit dans une vue d'ensemble, dans laquelle est indiquée des informations plus précises de la liaison.

FIGURE 1.3. – Aperçut des connexions

Action : Ici, les actions sont symbolisées par des icônes. Que signifie chaque icône ? Voici ci-dessous un tableau récapitulatif :

Symbole	Explication
	Démarrer le processus OpenVPN et tente de se connecter.
	Arrête le processus OpenVPN.
	Réinitialise la connexion.
	stoppe la connexion, elle est en attente. Plus aucune donnée ne circule sur la liaison.
	Relance la connexion. Les données peuvent à nouveau circuler sur la liaison.

TABLE 1.1. – Commande du Webgui OpenVPN

OpenVPN - WebGUI - Vue détaillée d'une connexion

FIGURE 1.4. – Vue détaillée d'une connexion (gestion de clé)

Statistique : on peut voir sur cet onglet, les statistiques intéressantes de la liaison. Les statistiques ne peuvent être visibles que si la liaison est démarrée et non arrêtée.

Log : On peut voir sur cet onglet, les 20 dernières lignes de la connexion. Si vous voulez voir plus de lignes, vous pouvez indiquer le nombre et cliquer sur "afficher". Si vous indiquez "all" vous pouvez voir la totalité du fichier log. Cet onglet est visible que si la liaison est démarrée.

Debug-Log : on peut voir sur cet onglet le processus de démarrage. On voit le démarrage de la liaison OpenVPN et ces sorties. C'est utile lorsque que l'on veut démarrer la liaison avec l'icône démarrée et que la connexion ne veut pas s'activer, en plus dans le fichier log normal il n'y a rien d'indiqué sur le démarrage.

Filtrage de paquets : on peut voir sur cet onglet le filtrage de paquets valide pour une liaison. Le filtrage de paquets est configuré que si la liaison est démarrée et que le tunnel est installé.

Bridge : on peut voir sur cet onglet la configuration du Bridge sur le routeur. Cet onglet est visible que si la liaison avec Bridge est installée.

Configuration : on peut voir sur cet onglet, la configuration de la liaison générée par le boot.

Gestion de clé : sur cet onglet, on peut produire une clé pour une liaison et peut également être téléchargés, (voir l'illustration 1.4). Aucune clé n'existe (au premier démarrage) du VPN, vous devez la produire automatiquement. Il peut être transféré directement avec le Symbole Download ou être copier/coller dans un fichier texte. Cliquez sur l'icône disquette pour enregistrer la clé qui a été nouvellement produite sur le routeur, ce processus peut-être annulé, par un clic sur l'icône restauration.

Support informations : sont indiquées dans cet onglet, toutes les informations qui pourraient être pertinentes, si vous avez un problème. Vous pouvez transmettre ces renseignements, par exemple pour un article dans des Newsgroups en faisant un copier/coller.

1.1.7. OpenVPN - Aide pour différentes versions OpenVPN

Avec les versions différentes d'OpenVPN, vous devez veiller à l'utilisation les paramètres, car les valeurs standards diffèrent pour chaque liaison VPN. Cela concerne en particulier les réglages, MTU, FRAGMENT et MSSFIX. Si les valeurs correspondent ne sont pas «adaptées» aux config OpenVPN ou si la connexion fonctionne avec la commande ping, mais se bloque par exemple lors de l'utilisation ssh, alors ces valeurs ne sont peut être pas ajustées correctement. Voici les messages d'erreurs typiques, pour de tels cas :

```
FRAG_IN error flags=0xfa2a187b: FRAG_TEST not implemented
FRAG_IN error flags=0xfa287f34: spurrious FRAG_WHOLE flags
```

Les paramètres cruciaux, pour la réalisation d'une liaison sont les suivants :

OPENVPN_x_TUN_MTU La valeur MTU du périphérique TUN est pour la version OpenVPN 1.x à 1300. La valeur à partir de la version OpenVPN 2.0 est de 1500, valeur standard.

OPENVPN_x_LINK_MTU Taille en octet de la liaison des deux démons OpenVPN. Cette valeur par défaut est fonction de l'utilisation de la version OpenVPN et du système d'exploitation.

OPENVPN_x_FRAGMENT Les paquets (peu importe que ce soit UDP ou TCP) dont la taille est au-dessus du seuil de fragmentation, ces paquets de données seront fragmentés, et ne seront pas supérieures à celles indiquées dans la variable `OPENVPN_x_FRAGMENT` en octet.

OPENVPN_x_MSSFIX Afin d'échangent les paquets de données TCP sur une liaison VPN, sans que ces paquets soit si possible fragmentés, vous pouvez indiquer ici la dimension maximale souhaitée des paquets donnés TCP. Les systèmes d'exploitation actuels analysent mieux les normes de fragmentation, ainsi la fragmentation des paquets de données n'est plus nécessaire.

Les différentes versions OpenVPN utilisent les valeurs suivantes en tant que valeurs par défaut. Vous devez faire attention à ces valeurs, si vous voulez connecter ces versions OpenVPN qui ne fonctionnent pas sur le routeur fli4l. Les valeurs par défaut spécifiées sur le routeur fli4l sont dans le deuxième tableau.

En raison de ces différents paramètres, vous devez déterminer les valeurs par défaut à installer dans votre réseau et écrire alors explicitement ceux-ci dans le fichier config/openvpn.txt. Les valeurs sont dans la plupart des cas, des valeurs satisfaisantes pour des premiers tests.

Option/version OpenVPN	1.xx	2.00
OPENVPN_x_TUN_MTU	1300	1500
OPENVPN_x_TUN_MTU_EXTRA	inconnu	32
OPENVPN_x_FRAGMENT	inconnu	non configuré
OPENVPN_x_MSSFIX	non configuré	1450

TABLE 1.2. – Paramètre MTU des différentes versions OpenVPN.

Option/version fli4l	jusqu'à 2.1.8	à partir 2.1.9
OPENVPN_x_TUN_MTU	1300	1500
OPENVPN_x_TUN_MTU_EXTRA	64	32
OPENVPN_x_FRAGMENT	non configuré	1300
OPENVPN_x_MSSFIX	non configuré	1300

TABLE 1.3. – Paramètre MTU des différentes versions pour le routeur fli4l.

```
OPENVPN_DEFAULT_TUN_MTU='1500'
OPENVPN_DEFAULT_MSSFIX='1300'
OPENVPN_DEFAULT_FRAGMENT='1300'
```

Malheureusement, il n'est pas possible pour les versions fli4l antérieures à 2.1.9 de paramétrer directement le «tun-mtu». Toutefois, on peut influencer indirectement sur ce paramètre avec la variable `OPENVPN_x_LINK_MTU`. La valeur tun-mtu est d'environ 45 octets inférieurs à la valeur spécifiée dans `OPENVPN_x_LINK_MTU`. Pour déterminer la valeur précise, vous devez faire des essais.

1.1.8. OpenVPN - Exemples

Quelques exemples illustrent la configuration du paquetage OpenVPN.

Exemple - Joindre deux réseaux par le routeur fli4l

Dans le premier exemple, nous allons effectuer une liaison OpenVPN sur deux routeurs fli4l. Il s'agit d'accéder au réseau derrière le routeur fli4l du poste distant. Dans cet exemple, Peter et Maria veulent relier leurs réseaux par leur routeur fli4l. Peter utilise l'adresse 192.168.145.0/24 pour le réseau privés et l'adresses peter.eisfair.net pour DynDNS. Maria, utilise de façon semblable l'adresse 10.23.17.0/24 pour le réseau et l'adresse maria.eisfair.net pour DynDNS. Les deux se font confiance mutuellement et pourrons avoir accès à l'ensemble de leurs réseaux.

Exemple - deux réseaux reliés par un Bridge (ou pont)

Dans l'exemple suivant, un Bridge est développé par l'intermédiaire une connexion sans fil. Avec un Bridge, le filtrage de paquets ne peut pas être configuré judicieusement, puisque seuls les frames Ethernet sont transmises, absolument pas les paquets IP. Merci de ne pas oublier, qu'un réseau commun doit être utiliser dans une configuration de bridge. En plus, il ne faut pas que l'adresse IP soit attribuée deux fois.

Naturellement En plus des paramètres d'OpenVPN, vous devez configurer le Bridge dans advanced_networking et aussi de configurer base.txt, de telle sorte que le Bridge soit utilisé en tant que périphérique réseau et non pas eth0 pour le réseau interne. Ci-dessous nous avons adapté la configuration de advanced_networking et de base.

Option OpenVPN	Peter	Maria
OPENVPN_1_NAME=	'maria'	'peter'
OPENVPN_1_REMOTE_HOST=	'maria.eisfair.net'	'peter.eisfair.net'
OPENVPN_1_REMOTE_PORT=	'10000'	'10001'
OPENVPN_1_LOCAL_PORT=	'10001'	'10000'
OPENVPN_1_SECRET=	'pema.secret'	'pema.secret'
OPENVPN_1_TYPE=	'tunnel'	'tunnel'
OPENVPN_1_REMOTE_VPN_IP=	'192.168.200.202'	'192.168.200.193'
OPENVPN_1_LOCAL_VPN_IP=	'192.168.200.193'	'192.168.200.202'
OPENVPN_1_ROUTE_N=	'1'	'1'
OPENVPN_1_ROUTE_1=	'10.23.17.0/24'	'192.168.145.0/24'
OPENVPN_1_PF_INPUT_N=	'1'	'1'
OPENVPN_1_PF_INPUT_1=	'ACCEPT'	'ACCEPT'
OPENVPN_1_PF_FORWARD_N=	'1'	'1'
OPENVPN_1_PF_FORWARD_1=	'ACCEPT'	'ACCEPT'

Table 1.4. – Configuration d'OpenVPN avec 2 routeurs fli4l

Option OpenVPN	Peter	Maria
OPENVPN_2_NAME	'bridge'	'bridge'
OPENVPN_2_REMOTE_HOST	'10.1.0.1'	'10.2.0.1'
OPENVPN_2_REMOTE_PORT	'10005'	'10006'
OPENVPN_2_LOCAL_HOST	'10.2.0.1'	'10.1.0.1'
OPENVPN_2_LOCAL_PORT	'10006'	'10005'
OPENVPN_2_FLOAT	'no'	'no'
OPENVPN_2_RESTART	'never'	'never'
OPENVPN_2_SECRET	'bridge.secret'	'bridge.secret'
OPENVPN_2_TYPE	'bridge'	'bridge'
OPENVPN_2_BRIDGE	'pema-br'	'pema-br'

Table 1.5. – Configuration d'OpenVPN avec 2 routeurs fli4l leurs réseaux ont une connexion sans fil et utilise un Bridge

Option advanced_networking	Peter	Maria
OPT_BRIDGE_DEV	'yes'	'yes'
BRIDGE_DEV_BOOTDELAY	'no'	'no'
BRIDGE_DEV_N	'1'	'1'
BRIDGE_DEV_1_NAME	'pema-br'	'pema-br'
BRIDGE_DEV_1_DEVNAME	'br0'	'br0'
BRIDGE_DEV_1_DEV_N	'1'	'1'
BRIDGE_DEV_1_DEV_1_DEV	'eth0'	'eth0'

Table 1.6. – Configuration d'OpenVPN avec 2 routeurs fli4l leurs réseaux ont une connexion sans fil et utilise un Bridge, configuration dans advanced_networking.

Option base	Peter	Maria
IP_NET_N	'1'	'1'
IP_NET_1	'192.168.193.254/24'	'192.168.193.1/24'
IP_NET_1_DEV	'br0'	'br0'

Table 1.7. – Configuration d'OpenVPN avec 2 routeurs fli4l leurs réseaux ont une connexion sans fil et utilise un Bridge, configuration dans (base.txt).

Exemple - Configuration pour un accès Road warrior (ou Guerre commerciale informatisée)

Pour cet exemple (Road warrior), un portable sous Windows XP est permis et un accès GPRS pour accéder au RÉSEAU LOCAL derrière le routeur fli4l. Sur le portable est installé un OpenVPN pour Windows XP, le fichier *.ovpn correspondant doit être adapté. Malheureusement, les pilotes tun/tap sous Windows ne sont pas aussi souples que son homologue Unix. C'est pourquoi avec le Point-to-Point pour VPN les adresses IP doivent se trouver dans le réseau 255.255.255.252 (ou /30). Si Road Warrior doit seulement accéder aux services du LAN derrière le routeur fli4l, il ne sera pas nécessaire d'indiquer un itinéraire sur la page fli4l, comme cela il ne réagira pas. Avec Road warrior si nécessaire on peut utiliser une adresse IP virtuels dans (`OPENVPN_3_REMOTE_VPN_IP`). Si Road warrior dispose d'une adresse IP statique, on pourra également enregistrer une route pour un hôte, par ex. si Road warrior a une adresse IP 192.168.33.33 statique, vous pouvez insérer dans le fichier de configuration openvpn.txt de fli4l :

```
OPENVPN_3_ROUTE_N='1'
OPENVPN_3_ROUTE_1='192.168.33.33/32'
```

Au sujet de la configuration de filtrage de paquets ci-dessous, il vous permet une communication complète dans les deux sens. Road warrior ne peut pas interroger directement le routeur fli4l. Mais si c'est nécessaire, il est possible d'utilise le serveur DNS du routeur fli4l.

```
OPENVPN_3_PF_FORWARD_N='1'
OPENVPN_3_PF_FORWARD_1='ACCEPT'
```

Si Road warrior est autorisé pour accéder au serveur DNS interne du routeur fli4l, il faut ajouter dans la configuration de fli4l les paramètres suivant :

```
OPENVPN_3_PF_INPUT_N='1'
OPENVPN_3_PF_INPUT_1='if:VPNDEV:any tmpl:dns ACCEPT'
```

Exemple - Liaison WLAN sécurisé

Dans cet exemple, on passe par un WLAN (ou sans fil) pour accéder à la liaison OpenVPN. On part du principe que le WLAN est installé sur le routeur fli4l , une carte Ethernet pour le réseau local et une carte WLAN, dont le point d'accès est activé. L'objectif doit être, un Client WLAN sans liaison VPN a seulement accès au VPN par le port du routeur fli4l. Ce n'est qu'après la connexion réussite avec OpenVPN, que l'échange sans restriction avec le réseau local du poste distant peut être possible. Pour cela des modifications du serveur DNSMASQ DHCP doivent être réalisées. En outre, le paquetage advanced_networking est nécessaire à l'installation. Il faut aussi paramétrer `IP_NET_1` pour le LAN (réseau local) et `IP_NET_2` pour le WLAN (réseau sans fil) dans le fichier base.txt.

```
IP_NET_N='2'
IP_NET_1='192.168.3.254/24'
IP_NET_1_DEV='br0'
IP_NET_2='192.168.4.254/24'
IP_NET_2_DEV='eth2'
```

Option OpenVPN routeur fli4l	roadwarrior
OPENVPN_3_NAME='roadwarrior'	remote peter.eisfair.net
OPENVPN_3_LOCAL_PORT='10011'	rport 10011
OPENVPN_3_SECRET='roadwarrior.secret'	secret roadwarrior.secret
OPENVPN_3_TYPE='tunnel'	dev tun
OPENVPN_3_REMOTE_VPN_IP='192.168.200.238'	
OPENVPN_3_LOCAL_VPN_IP='192.168.200.237'	ifconfig 192.168.200.238 192.168.200.237
OPENVPN_3_ROUTE_N='0'	
OPENVPN_3_PF_FORWARD_N='1'	
OPENVPN_3_PF_FORWARD_1='ACCEPT'	
	route 192.168.145.0 255.255.255.0
	comp-lzo
	persist-tun
	persist-key
	ping-timer-rem
	ping-restart 60
	proto udp
	tun-mtu 1500
	fragment 1300
	mssfix

TABLE 1.8. – Configuration d'OpenVPN pour un ordinateur Windows avec GPRS

La plage DHCP doit être réglé selon vos besoins. Pour la variable `IP_NET_2` vous devez absolument ajouter les paramètres suivants :

```
DNSDHCP_RANGE_2_DNS_SERVER1='none'
DNSDHCP_RANGE_2_NTP_SERVER='none'
DNSDHCP_RANGE_2_GATEWAY='none'
```

Paramètre advanced_networking.txt :

```
OPT_BRIDGE_DEV='yes'
BRIDGE_DEV_BOOTDELAY='yes'
BRIDGE_DEV_N='1'
BRIDGE_DEV_1_NAME='br'
BRIDGE_DEV_1_DEVNAME='br0'
BRIDGE_DEV_1_DEV_N='1'
BRIDGE_DEV_1_DEV_1_DEV='eth0'
```

1.1.9. Liens sur le thème OpenVPN

Pour terminer, encore quelques liens qui traitent de la configuration OpenVPN :

http://openvpn.net
http://de.wikipedia.org/wiki/OpenVPN
http://openvpn.se/
http://arnowelzel.de/wiki/en/fli4l/openvpn
http://wiki.freifunk.net/OpenVPN
http://w3.linux-magazine.com/issue/24/Charly.pdf
http://w3.linux-magazine.com/issue/25/WirelessLAN_Intro.pdf
http://w3.linux-magazine.com/issue/25/OpenVPN.pdf

Option OpenVPN routeur	Client WLAN
OPENVPN_4_NAME='wlan1'	
OPENVPN_4_LOCAL_HOST='192.168.4.254'	remote 192.168.4.254
OPENVPN_4_LOCAL_PORT='20001'	rport 20001
OPENVPN_4_SECRET='wlan1.secret'	secret wlan1.secret
OPENVPN_4_TYPE='bridge'	dev tap
OPENVPN_4_BRIDGE='br'	
OPENVPN_4_RESTART='never'	
OPENVPN_4_MUTE_REPLAY_WARNINGS='yes'	
	comp-lzo
	persist-tun
	persist-key
	ping-timer-rem
	ping-restart 60
	proto udp
	tun-mtu 1500
	fragment 1300
	mssfix

TABLE 1.9. – OpenVPN sécurisé dans un WLAN

A. Annexe du paquetage OPENVPN

Table des figures

1.1. Exemple de configuration VPN — Tunnel entre deux routeurs 4
1.2. fli4l répertoire OpenVPN avec les fichiers *.secret 7
1.3. Aperçut des connexions 20
1.4. Vue détaillée d'une connexion (gestion de clé) 21

Liste des tableaux

1.1. Commande du Webgui OpenVPN 20
1.2. Paramètre MTU des différentes versions OpenVPN. 23
1.3. Paramètre MTU des différentes versions pour le routeur fli4l. 23
1.4. Configuration d'OpenVPN avec 2 routeurs fli4l 24
1.5. Configuration d'OpenVPN avec 2 routeurs fli4l leurs réseaux ont une connexion sans fil et utilise un Bridge 24
1.6. Configuration d'OpenVPN avec 2 routeurs fli4l leurs réseaux ont une connexion sans fil et utilise un Bridge, configuration dans advanced_networking. 24
1.7. Configuration d'OpenVPN avec 2 routeurs fli4l leurs réseaux ont une connexion sans fil et utilise un Bridge, configuration dans (base.txt). 24
1.8. Configuration d'OpenVPN pour un ordinateur Windows avec GPRS 26
1.9. OpenVPN sécurisé dans un WLAN 27

Index

OPENVPN_DEFAULT_ALLOW_-ICMPPING, 12
OPENVPN_DEFAULT_CIPHER, 11
OPENVPN_DEFAULT_COMPRESS, 11
OPENVPN_DEFAULT_CREATE_-SECRET, 11
OPENVPN_DEFAULT_DIGEST, 11
OPENVPN_DEFAULT_FLOAT, 11
OPENVPN_DEFAULT_FRAGMENT, 14
OPENVPN_DEFAULT_KEYSIZE, 12
OPENVPN_DEFAULT_LINK_MTU, 15
OPENVPN_DEFAULT_-MANAGEMENT_LOG_-CACHE, 14
OPENVPN_DEFAULT_MSSFIX, 14
OPENVPN_DEFAULT_MUTE_-REPLAY_WARNINGS, 14
OPENVPN_DEFAULT_OPEN_-OVPNPORT, 12
OPENVPN_DEFAULT_PF_-FORWARD_LOG, 12
OPENVPN_DEFAULT_PF_-FORWARD_POLICY, 12
OPENVPN_DEFAULT_PF_INPUT_-LOG, 12
OPENVPN_DEFAULT_PF_INPUT_-POLICY, 12
OPENVPN_DEFAULT_PING, 13
OPENVPN_DEFAULT_PING_-RESTART, 13
OPENVPN_DEFAULT_PROTOCOL, 13
OPENVPN_DEFAULT_RENEG_SEC, 13
OPENVPN_DEFAULT_RESOLV_-RETRY, 13
OPENVPN_DEFAULT_RESTART, 13
OPENVPN_DEFAULT_SHAPER, 15
OPENVPN_DEFAULT_START, 13
OPENVPN_DEFAULT_TUN_MTU, 14
OPENVPN_DEFAULT_TUN_MTU_-EXTRA, 14
OPENVPN_DEFAULT_VERBOSE, 14
OPENVPN_EXPERT, 15
OPENVPN_N, 5
OPENVPN_WEBGUI, 19
OPENVPN_x_ACTIV, 16
OPENVPN_x_ALLOW_ICMPPING, 17
OPENVPN_x_BRIDGE, 8
OPENVPN_x_BRIDGE_COST, 8
OPENVPN_x_BRIDGE_PRIORITY, 8
OPENVPN_x_CHECK_CONFIG, 16
OPENVPN_x_CIPHER, 16
OPENVPN_x_COMPRESS, 16
OPENVPN_x_CREATE_SECRET, 16
OPENVPN_x_DIGEST, 16
OPENVPN_x_DNSIP, 10
OPENVPN_x_DOMAIN, 10
OPENVPN_x_FLOAT, 16
OPENVPN_x_FRAGMENT, 19
OPENVPN_x_IPV6, 9
OPENVPN_x_ISDN_CIRC_NAME, 16
OPENVPN_x_KEYSIZE, 16
OPENVPN_x_LINK_MTU, 19
OPENVPN_x_LOCAL_HOST, 5
OPENVPN_x_LOCAL_PORT, 5
OPENVPN_x_LOCAL_VPN_IP, 8
OPENVPN_x_LOCAL_VPN_IPV6, 9
OPENVPN_x_MANAGEMENT_LOG_-CACHE, 17
OPENVPN_x_MSSFIX, 19
OPENVPN_x_MUTE_REPLAY_-WARNINGS, 17
OPENVPN_x_NAME, 15
OPENVPN_x_OPEN_OVPNPORT, 17
OPENVPN_x_PF6_FORWARD_N, 18
OPENVPN_x_PF6_FORWARD_x, 19

OPENVPN_x_PF6_INPUT_N, 18
OPENVPN_x_PF6_INPUT_x, 18
OPENVPN_x_PF_FORWARD_LOG, 18
OPENVPN_x_PF_FORWARD_N, 18
OPENVPN_x_PF_FORWARD_POLICY, 18
OPENVPN_x_PF_FORWARD_x, 18
OPENVPN_x_PF_INPUT_LOG, 17
OPENVPN_x_PF_INPUT_N, 17
OPENVPN_x_PF_INPUT_POLICY, 17
OPENVPN_x_PF_INPUT_x, 17
OPENVPN_x_PF_POSTROUTING_N, 18
OPENVPN_x_PF_POSTROUTING_x, 18
OPENVPN_x_PF_PREROUTING_N, 18
OPENVPN_x_PF_PREROUTING_x, 18
OPENVPN_x_PING, 16
OPENVPN_x_PING_RESTART, 17
OPENVPN_x_PROTOCOL, 16
OPENVPN_x_REMOTE_HOST, 5
OPENVPN_x_REMOTE_HOST_N, 5
OPENVPN_x_REMOTE_HOST_x, 5
OPENVPN_x_REMOTE_PORT, 5
OPENVPN_x_REMOTE_VPN_IP, 8
OPENVPN_x_REMOTE_VPN_IPV6, 9
OPENVPN_x_RESOLV_RETRY, 16
OPENVPN_x_RESTART, 17
OPENVPN_x_ROUTE_N, 9
OPENVPN_x_ROUTE_x, 9
OPENVPN_x_ROUTE_x_DNSIP, 10
OPENVPN_x_ROUTE_x_DOMAIN, 10
OPENVPN_x_SECRET, 6
OPENVPN_x_SHAPER, 19
OPENVPN_x_START, 17
OPENVPN_x_TUN_MTU, 19
OPENVPN_x_TUN_MTU_EXTRA, 19
OPENVPN_x_TYPE, 7
OPENVPN_x_VERBOSE, 17
OPT_OPENVPN, 5