

Paquetage VPN

Version 4.0.0-trunk-x86-r60803

Frank Meyer L'équipe fli4l
courriel: frank@fli4l.de courriel: team@fli4l.de

28 décembre 2022

Table des matières

1	Documentation du paquetage VPN	3
1.1	VPN - Réseau privé virtuel	3
1.1.1	PPTP-Tunnel	3
	Table des figures	9
	Liste des tableaux	10
	Index	11

1 Documentation du paquetage VPN

1.1 VPN - Réseau privé virtuel

Ce paquetage permet d'établir une connexion sécurisée entre réseau privé à travers le réseau public qui n'est pas sécurisé.

1.1.1 PPTP-Tunnel

Le PPTP¹ permet, d'établir un canal privé sur un réseau public. Un tunnel sera construit et exploité en utilisant le protocole TCP/IP spécial pour les règles de contrôle. Les paquets PPP de l'utilisateur sont encapsulés avec le protocole GRE².

En Autriche (et dans d'autres pays européens) le protocole PPTP est également utilisé entre le routeur et le modem DSL. Contrairement aux protocoles PPPoE et PPPoA, il travaille en dessous de la couche IP (avec une couche de liaison "Link Layer"), le PPTP décrit ci-dessus, utilise donc deux flux pour les données. Ainsi, il faut pour une connexion DSL via le protocole PPTP réserver une adresse IP pour le PPTP sur la carte Ethernet, contrairement à d'autres méthodes d'accès DSL. Selon le fournisseur vous devez configurer soit une adresse fixe ou via le DHCPv4. Vous trouverez plus d'informations dans la description de la variable CIRC_x_PPP_PPTP_PEER.

Si vous avez besoin d'une connexion DSL ou d'une connexion distante par VPN avec le PPTP, il est déconseillé d'utiliser le PPTP pour une solution VPN. Car le cryptage du protocole PPTP se crack facilement³ et vous ne devez pas envoyer de données sensibles via un tunnel PPTP. Il vaut mieux utiliser OpenVPN pour envoyer vos données via un tunnel, c'est certainement le meilleur choix.

Connexion PPTP sortante

Généralement une connexion PPTP sortante se configure comme un circuit PPP (voir Circuit de type "ppp" (Page ??)), c'est à dire, vous devez avoir :

```
CIRC_x_TYPE='ppp'
```

En outre, la variable OPT_PPP_PPTP doit être activé :

OPT_PPP_PPTP Cette variable vous permet de supporter le protocole PPTP. C'est en fait une connexion PPTP que vous allez utiliser, avec un circuit PPP du type "pptp", donc vous devez également configurer

```
CIRC_x_TYPE='ppp'  
CIRC_x_PPP_TYPE='pptp'
```

1. "Point-to-Point Tunneling Protocol" protocole de tunnel point-à-point voir RFC 2637
2. "Generic Routing Encapsulation" cette trame sera ensuite transférée sur le réseau IP à travers un tunnel, voir RFC 2784
3. voir <http://heise.de/-1701365>

(le "x" est l'indexation de la variable des circuits).

Paramètre par défaut : OPT_PPP_PPTP='no'

Exemple : OPT_PPP_PPTP='yes'

CIRC_x_PPP_PPTP_TYPE cette variable sert à configurer l'encapsulage des paquets de données PPP dans le protocole GRE, ensuite cette trame sera envoyée sur le canal. Pour cela le programme (**pptp**) ou le kernel peut être utilisé. la variable **CIRC_x_PPP_PPTP_TYPE** est utilisée pour générer les paquets GRE voir le tableau 1.1.

Valeur	Description
kernel	Les paquets PPP sont transmis directement au noyau Linux, les paquets GRE seront créés. Cela élimine la communication avec un second processus, donc une quantité de copie et une gestion du temps améliorée et qui à son tour conduit à réduire la charge du processeur.
daemon	Les paquets sont générés par le démon pptp , la communication entre pppd et pptp est asynchrone. Cela signifie que le flux de données ont des marqueurs de début et de fin, ainsi le démon pptp peut distinguer les paquets individuellement. En raison du second processus et du marquages supplémentaires, cette méthode est plus complexe que la méthode "kernel".

TABLE 1.1 – (Manière de générer les paquets GRE)

Actuellement, "daemon" est la seule méthode supportée (et donc par défaut, si le type n'est pas spécifié). Une extension du paquetage pour bénéficier du module **kernel** PPTP est envisageable.

Paramètre par défaut : CIRC_x_PPP_PPTP_TYPE='daemon'

CIRC_x_PPP_PPTP_PEER Dans cette variable vous indiquez l'adresse IP du serveur PPTP.

Si vous utilisez PPTP pour un accès Internet à haute débit, l'adresse IP de la carte Ethernet du routeur fli4l pour l'accès au PPTP doit être choisie en conséquence. Dans le tableau 1.2 vous avez une liste connue des options de configuration.

Fournisseur	Adresse IP local (IP_NET_2)	Adresse IP distant (CIRC_x_PPP_PPTP_PEER)
Telekom Austria (Autriche)	10.0.0.140/29	10.0.0.138
mxstream (Pays-Bas, Danemark)	10.0.0.140/29	10.0.0.138
Inode xDSL (Autriche)	via DHCPv4	10.0.0.138

TABLE 1.2 – Réglages des fournisseurs qui utilisent le PPTP

Si vous utilisez le DHCP pour configurer la carte de réseau local, vous devez installer le paquetage **dhcp_client** et configurer le circuit DHCPv4 correspondant à la carte ethernet (généralement eth1). Vous pouvez voir à la fin de la documentation un exemple pour une connexion avec Inode xDSL.

CIRC_x_PPP_PPTP_REORDER_TIMEOUT Si le client PPTP a besoin d'une mémoire tampon pour les paquets vous pouvez l'indiquer dans cette variable. Normalement un paquet attend 0,3 secondes avant le traitement de celui-ci. Vous pouvez varier le délai entre 0.00 (pas de tampon) et 10.00 (max. attend 10 secondes) dans cette variable. Le temps doit toujours être indiqué avec un point et deux décimales.

Paramètre par défaut : `CIRC_x_PPP_PPTP_REORDER_TIMEOUT='0.30'`

Exemple : `CIRC_1_PPP_PPTP_REORDER_TIMEOUT='1.00'`

CIRC_x_PPP_PPTP_LOGLEVEL Vous pouvez indiquer dans cette variable un nombre pour les informations du fichier journal. Les nombres possibles sont, 0 (faible), 1 (milieu) et 2 (beaucoup).

Paramètre par défaut : `CIRC_x_PPP_PPTP_LOGLEVEL='1'`

Exemple : `CIRC_1_PPP_PPTP_LOGLEVEL='2'`

Connexion PPTP entrante

fl4l peut également être configuré pour *accepter* les connexions PPTP entrantes, il agira comme un serveur. Ces connexions PPTP sont également configurés comme un circuit PPP. (Voir Circuits du type "ppp" (Page ??)), c'est à dire, vous devez avoir :

`CIRC_x_TYPE='ppp'`

En outre, la variable `OPT_PPP_PPTP_SERVER` doit être activé :

OPT_PPP_PPTP_SERVER Cette variable vous permet d'activer une connexion PPTP entrante. C'est en fait une connexion PPTP que vous allez utiliser, avec un circuit PPP du type "pptp-server", donc vous devez également configurer

`CIRC_x_TYPE='ppp'`

`CIRC_x_PPP_TYPE='pptp-server'`

(le "x" est l'indexation de la variable circuit).

Paramètre par défaut : `OPT_PPP_PPTP_SERVER='no'`

Exemple : `OPT_PPP_PPTP_SERVER='yes'`

Les variables du circuit général sont les suivantes pour le circuit PPP du type "pptp-server", des variables spécifiques ont également été ajoutées :

CIRC_x_PPP_PPTP_SERVER_LISTEN Dans cette variable, vous indiquez l'adresse IPv4 sur laquelle écoute le serveur PPTP. Si vous n'indiquez rien dans cette variable le serveur PPTP écoutera sur *toutes* les interfaces du routeur.⁴

Exemple : `CIRC_1_PPP_PPTP_SERVER_LISTEN='IP_NET_1_ADDR'`

CIRC_x_PPP_PPTP_SERVER_ALLOW_FROM_y Dans ces variables vous configurez la liste des adresses de réseau IPv4 qui accéderont au serveur PPTP et qui seront autorisées par le pare-feu. Avec les adresses configurées ici et avec les variables `PF_INPUT_ACCEPT_DEF='yes'` (Page ??) et `PF_OUTPUT_ACCEPT_DEF='yes'` (Page ??) le pare-feu ouvre les chaînes INPUT et OUTPUT pour le contrôle du protocole PPTP sur le port TCP 1723 et pour les paquets GRE. Si cet ensemble de variables, le pare-feu ainsi que le contrôle et les paquets de données sont configurés tous sera acceptés *de partout* sur le serveur.

Exemple :

4. Cela correspond à l'adresse IPv4 0.0.0.0.

```
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_N='3'
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_1='IP_NET_1'
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_2='10.1.2.0/24'
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_3='{Labor}'
```

CIRC_x_PPP_PPTP_SERVER_SESSIONS Avec cette variable vous pouvez indiquer le nombre de connexions que peut gérer le serveur PPTP simultanément. 255 tunnels peuvent être pris en charge.⁵

Paramètre par défaut : CIRC_x_PPP_PPTP_SERVER_SESSIONS='100'

Exemple : CIRC_1_PPP_PPTP_SERVER_SESSIONS='200'

Exemples

Exemple 1 (Accès à Internet via le PPTP avec une adresse locale fixe) :

```
IP_NET_N='2' # (Au moins) deux réseaux (LAN + PPTP)
IP_NET_1='192.168.6.0/24' # Réseau local, configuration nécessaire
IP_NET_1_DEV='eth0' # Réseau local qui dépend de la première carte
IP_NET_2='10.0.0.140/29' # Votre adresse pour le réseau PPTP
IP_NET_2_DEV='eth1' # Modem Internet accroché à la deuxième carte
#
OPT_PPP='yes' # Circuits PPP activé
OPT_PPP_PPTP='yes' # Client du circuits PPTP activé
#
CIRC_N='1'
CIRC_1_NAME='DSL-mxstream' # Arbitraire, mais c'est évident
CIRC_1_TYPE='ppp' # C'est un circuit PPP
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='0.0.0.0/0' # Route par défaut pour Internet
CIRC_1_CLASS_N='1'
CIRC_1_CLASS_1='internet' # Classe pour la connexion Internet
CIRC_1_UP='yes' # Activer au moment du boot
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_USEPEERDNS='yes' # Utiliser les serveurs DNS du fournisseur
CIRC_1_PPP_TYPE='pptp' # Client PPTP
CIRC_1_PPP_USERID='anonymer' # Authentification de l'utilisateur
CIRC_1_PPP_PASSWORD='surfer' # Authentification par mot de passe
CIRC_1_PPP_PPTP_PEER='10.0.0.138' # Adresse du modem Internet dans le réseau PPTP
#
CIRC_CLASS_N='1'
CIRC_CLASS_1='internet' # Classe de tous les circuits Internet
```

Exemple 2 (Accès à Internet via le PPTP avec une adresse locale dynamique) :

```
IP_NET_N='2' # (Au moins) deux réseaux (LAN + PPTP)
IP_NET_1='192.168.6.0/24' # Réseau local, configuration nécessaire
IP_NET_1_DEV='eth0' # Réseau local qui dépend de la première carte
```

5. Cette limitation résulte que le démon PPTP utilise une plage d'adresses autorisées en utilisant uniquement un seul composant de l'adresse IPv4, par exemple "192.168.222.0-254". Puisqu'un composant peut accepter seulement les valeurs 0-255 et si la valeur 255 est réservé pour l'adresse Broadcast (ou de diffusion), cela se traduit par la valeur indiqué ci-dessus.

1 Documentation du paquetage VPN

```
IP_NET_2='{DHCP-Inode}'          # Réseau PPTP configuré via le DHCP
IP_NET_2_DEV='eth1'              # Modem Internet accroché à la deuxième carte
#
OPT_DHCP_CLIENT='yes'            # Circuits DHCP activé
OPT_PPP='yes'                    # Client du circuits PPP activé
OPT_PPP_PPTP='yes'              # Client du circuits PPTP activé
#
CIRC_N='2'                       # Deux circuits: DHCP et PPTP
#
CIRC_1_NAME='DHCP-Inode'         # Arbitraire, mais évident
CIRC_1_TYPE='dhcp'              # C'est un circuit DHCP
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'          # Ici nombre de station distante PPTP
CIRC_1_NETS_IPV4_1='10.0.0.138/32' # (= Modem Internet) pour être accessible
CIRC_1_DHCP_DEV='IP_NET_2_DEV'  # Carte Ethernet PPTP
CIRC_1_UP='yes'                 # Activer au moment du boot
#
CIRC_2_NAME='PPTP-Inode'         # Arbitraire, mais évident
CIRC_2_TYPE='ppp'               # C'est un circuit PPP
CIRC_2_ENABLED='yes'
CIRC_2_PPP_TYPE='pptp'          # Client PPTP
CIRC_2_PPP_USER='anonymer'      # Authentification de l'utilisateur
CIRC_2_PPP_PASS='surfer'        # Authentification par mot de passe
CIRC_2_PPP_FILTER='yes'         # Activer le filtrage du trafic
CIRC_2_PPP_PPTP_PEER='10.0.0.138' # Adresse du modem Internet dans le réseau PPTP
CIRC_2_NETS_IPV4_N='1'
CIRC_2_NETS_IPV4_1='0.0.0.0/0'  # Route par défaut pour Internet
CIRC_2_USEPEERDNS='yes'         # Utiliser les serveurs DNS du fournisseur
CIRC_2_HUP_TIMEOUT='600'        # Couper après 10 minutes d'inactivité
CIRC_2_UP='yes'                 # Activer au moment du démarrage
CIRC_2_DEPS='DHCP-Inode'        # PPTP nécessite une configuration DHCP
```

Exemple 3 (Client VPN) :

```
IP_NET_N='1'                    # (Au moins) un réseau (local)
IP_NET_1='192.168.6.0/24'       # Réseau local, configuration nécessaire
IP_NET_1_DEV='eth0'             # Réseau local qui dépend de la première carte
#
OPT_PPP='yes'                   # Circuit PPP activé
OPT_PPP_ETHERNET='yes'          # Client du circuit PPPoE activé (DSL)
OPT_PPP_PPTP='yes'              # Client du circuit PPTP activé (VPN)
#
CIRC_N='2'                       # Deux circuits: PPPoE (Internet) et PPTP
#
CIRC_1_NAME='DSL-Telekom'        # Arbitraire, mais évident
CIRC_1_TYPE='ppp'               # C'est un circuit PPP
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='0.0.0.0/0'  # Route par défaut pour Internet
CIRC_1_CLASS_N='1'
CIRC_1_CLASS_1='internet'       # Classe pour la connexion Internet
CIRC_1_UP='yes'                 # Activer au moment du boot
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
```

1 Documentation du paquetage VPN

```
CIRC_1_USEPEERDNS='yes'           # Utiliser les serveurs DNS du fournisseur
CIRC_1_PPP_TYPE='ethernet'        # Client PPPoE
CIRC_1_PPP_USERID='anonymer'      # Authentification de l'utilisateur
CIRC_1_PPP_PASSWORD='surfer'      # Authentification par mot de passe
CIRC_1_PPP_ETHERNET_TYPE='kernel' # Kernel pour compacter les paquets PPPoE
CIRC_1_PPP_ETHERNET_DEV='eth1'    # Modem DSL accroché à la deuxième carte
#
CIRC_2_NAME='VPN-Firma'           # Arbitraire, mais évident
CIRC_2_TYPE='ppp'                 # C'est un circuit PPP
CIRC_2_ENABLED='yes'
CIRC_2_NETS_IPV4_N='1'
CIRC_2_NETS_IPV4_1='10.11.12.0/24' # Réseau de la société
CIRC_2_DEPS='internet/ipv4'       # Connexion Internet IPv4 si besoin
                                   # pour la société
CIRC_2_UP='yes'                   # Activer au moment du boot
CIRC_2_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_2_PPP_TYPE='pptp'            # Client PPTP
CIRC_2_PPP_USERID='mustermann'    # Authentification de l'utilisateur
CIRC_2_PPP_PASSWORD='geheim'      # Authentification par mot de passe
CIRC_2_PPP_PPTP_PEER='192.0.2.1'  # Adresse du serveur PPTP de la société
#
CIRC_CLASS_N='1'
CIRC_CLASS_1='internet'           # Classe pour la connexion Internet
```

Exemple 4 (Serveur VPN) :

```
OPT_PPP='yes'                     # Circuit PPP activé
OPT_PPP_PPTP_SERVER='yes'        # Circuit du serveur PPTP activé
OPT_PPP_PEERS='yes'              # Pour stocker les informations d'identification
PPP_PEER_N='1'                   # 1x nombre de donnée d'enregistrement
PPP_PEER_1_USERID='user'         # Nom d'utilisateur du client
PPP_PEER_1_PASSWORD='pass'       # Mot de passe du client
PPP_PEER_1_CIRCUITS='pptp-eth1'  # Enregistrement du circuit PPTP valide
#
CIRC_N='1'
CIRC_1_NAME='pptp-eth1'           # Arbitraire, mais évident
CIRC_1_TYPE='ppp'                 # C'est un circuit PPP
CIRC_1_ENABLED='yes'
CIRC_1_UP='yes'                   # Activer au moment du boot
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_PROTOCOLS='ipv4'          # Exécuter IPv4 sur la connexion
CIRC_1_PPP_TYPE='pptp-server'    # Serveur PPTP
CIRC_1_PPP_PEER_AUTH='yes'       # Authentification du client obligatoire
CIRC_1_PPP_COMP_MPPE='yes'       # Utiliser le cryptage
CIRC_1_PPP_LOCALIP='192.168.222.1' # Adresse IP du serveur
CIRC_1_PPP_REMOTEIP='192.168.222.2' # Adresse IP de départ des clients
CIRC_1_PPP_PPTP_SERVER_SESSIONS='10' # max. 10 tunnels
```


Table des figures

Liste des tableaux

1.1	(Manière de générer les paquets GRE	4
1.2	Réglages des fournisseurs qui utilisent le PPTP	4

Index

CIRC_x_PPP_PPTP_LOGLEVEL, [5](#)
CIRC_x_PPP_PPTP_PEER, [4](#)
CIRC_x_PPP_PPTP_REORDER_TIMEOUT,
[4](#)
CIRC_x_PPP_PPTP_SERVER_ALLOW_-
FROM_N, [5](#)
CIRC_x_PPP_PPTP_SERVER_ALLOW_-
FROM_y, [5](#)
CIRC_x_PPP_PPTP_SERVER_LISTEN,
[5](#)
CIRC_x_PPP_PPTP_SERVER_SESSIONS,
[6](#)
CIRC_x_PPP_PPTP_TYPE, [4](#)

OPT_PPP_PPTP, [3](#)
OPT_PPP_PPTP_SERVER, [5](#)