THEGREENBOW

Client VPN
Linux 2.0
CentOS/RedHat

Guide Utilisateur

Dernière mise à jour : 28 avril 2021

Table des matières

1 Présentation

1.1 Introduction

Merci d'avoir téléchargé le logiciel Client VPN Linux 2.0 pour CentOS et RedHat.

Le Client VPN Linux a été spécialement pensé pour répondre aux besoins des grands comptes, OIV/OSE et administrations civiles et gouvernementales. Procurant un niveau élevé de sécurisation des communications, il est facile à déployer, à intégrer et simple à utiliser.

Le Client VPN Linux bénéficie en outre d'un support personnalisé qui va d'un suivi dédié à la prise en compte d'évolutions spécifiques.

Il ne nécessite pas de remise en cause de l'infrastructure de gestion de clés (IGC) existante, et il est conçu pour s'intégrer de façon transparente avec les passerelles IKEv2 mises en place.

Le Client VPN Linux est commercialisé sous forme d'abonnement annuel. Cet abonnement inclut un support dédié et la maintenance du logiciel.

1.2 Sécurité

Conçu pour équiper les postes nomades, le Client VPN Linux est un logiciel client VPN IPsec IKEv2 pour postes de travail Linux, qui permet d'établir des connexions avec le système d'information de l'entreprise via internet, de façon parfaitement sécurisée. Il implémente une large variété d'algorithmes de chiffrement et de hachage, ainsi que différentes méthodes d'authentification forte.

1.3 Ergonomie

Facile à installer, facile à configurer et à déployer, parfaitement transparent pour l'utilisateur, le Client VPN Linux est aujourd'hui reconnu pour son ergonomie inégalée.

1.4 Simplicité

Nos guides de configuration facilitent les opérations d'intégrations et de déploiement en accélérant la mise en place d'une solution VPN de bout en bout.

1.5 Universalité

Le Client VPN Linux fonctionne sous CentOS 8 et RedHat 8. Le logiciel est compatible avec de très nombreuses passerelles IPsec du marché. La liste, en constante évolution, des passerelles testées dans notre laboratoire est disponible sur le site TheGreenBow.

1.6 Fonctionnalités

- Pilote réseau IPsec et module IKE développés par TheGreenBow
- Module IPsec intégré en mode noyau
- Prise en charge du protocole IKEv2
- Interopérable avec tous les routeurs VPN compatibles IKEv2
- Cryptographie : AES CBC, AES CTR, AES GCM 128/192/256
- Hachage : SHA2 256/384/512
- Groupes de clés : DH 14-21
- Gestion des certificats X.509 : PEM, PFX, PKCS #12
- Authentification : clé partagée, certificats, EAP, double authentification (certificat + EAP)
- Authentification des certificats par :
    - méthode 1 : RSA Digital Signature [RFC7296]
    - méthode 9 : ECDSA avec SHA-256 [RFC4754]
    - méthode 14 : Digital Signature Authentication RSA [RFC7427]
- Fragmentation IP
- Mode « tout le trafic dans le tunnel »
- Dead Peer Detection (DPD)
- Passerelle redondante
- Mode CP
- Négociation automatique des algorithmes avec la passerelle
- Fragmentation IKE
- Mode NAT-Traversal automatique
- Remote ID, Local ID
- Importation de configuration VPN générées par les clients VPN Windows et macOS TheGreenBow
- Pilotage en ligne de commande
- Activation par licence logicielle
- Prise en charge du format et du protocole de journaux d'évènements syslog
- Compilé pour CentOS version 8 et RedHat version 8, 64 bits

2 Téléchargement et vérification du logiciel

2.1 Introduction

Le Client VPN Linux est disponible en téléchargement à partir du site web TheGreenBow : https://www.thegreenbow.fr/vpn_linux.html. Vous pourrez télécharger le paquet logiciel après avoir renseigné un formulaire qui s'affiche lorsque vous cliquez sur le lien **Télécharger** correspondant à la distribution dans l'onglet **Téléchargement**.

Avant de procéder à l'installation du Client VPN Linux, il est important de vérifier l'authenticité du paquet logiciel téléchargé, afin de confirmer qu'il a bien été signé par TheGreenBow et qu'il n'a subi aucune altération.

2.2 Procédure de vérification

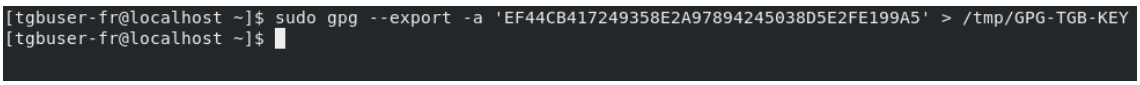
Pour vérifier l'authenticité du paquet, suivez les étapes ci-dessous :

1. Ouvrez une fenêtre de terminal.
2. Exécutez la commande suivante pour télécharger la clé publique :

```
sudo gpg --keyserver keys.gnupg.net --recv-keys
EF44CB417249358E2A97894245038D5E2FE199A5
```

3. Exécutez la commande suivante pour exporter la clé vers un fichier temporaire :

```
sudo gpg --export -a
'EF44CB417249358E2A97894245038D5E2FE199A5' > /tmp/GPG-TGB-KEY
```

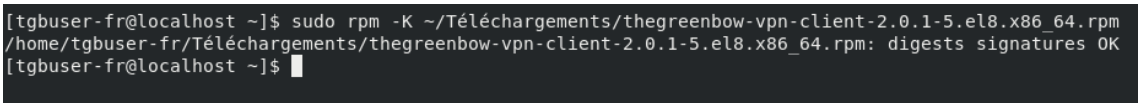


4. Exécutez la commande suivante pour importer la clé :

```
sudo rpm --import /tmp/GPG-TGB-KEY
```

5. Vérifiez le paquet logiciel en exécutant la commande suivante dans le répertoire où se trouve le paquet (ici `Téléchargements`, où `x` est le numéro de révision) :

```
sudo rpm -K ~/Téléchargements/thegreenbow-vpn-client-2.0.1-x.el8.x86_64.rpm
```



6. Vérifiez que les informations en sortie sont bien les suivantes :

```
/home/[nom_utilisateur]/Téléchargements/thegreenbow-vpn-client-2.0.1-x.el8.x86_64.rpm: digests signatures OK
```

Si ce n'est pas le cas, contactez le support client : https://www.thegreenbow.com/form.html?lang=fr.

2.3 Informations techniques

Le paquet CentOS/RedHat est signé avec une clé RSA de 4096 bits. La clé publique correspondante est disponible sous ce lien : http://keys.gnupg.net/pks/lookup?op=get&search=0x45038D5E2FE199A5.

Identifiant de la clé : `EF44 CB41 7249 358E 2A97 8942 4503 8D5E 2FE1 99A5`.

Empreinte de la clé : `2FE199A5`.

Pour supprimer la clé publique de la base de données RPM, suivez les étapes décrites ci-dessous :

1. Exécutez la commande suivante pour récupérer l'identifiant complet de la clé :

```
rpm -q gpg-pubkey --qf '%{NAME}-%{VERSION}-%{RELEASE}\t%{SUMMARY}\n'
```

   Les informations en sortie doivent indiquer le nom de la clé avec ses numéros de version et de révision comme suit :

```
gpg-pubkey-2fe199a5-[numéro_révision] gpg(TGB Linux product manager <linux@thegreenbow.com>)
```

2. Exécutez la commande suivante pour supprimer la clé en remplaçant le numéro de révision avec les résultats obtenus à l'étape précédente :

```
sudo rpm --erase gpg-pubkey-2fe199a5-[numéro_révision]
```

3 Installation

3.1 Introduction

Après avoir téléchargé le Client VPN Linux à partir du site web TheGreenBow et vérifié son authenticité (voir chapitre 2 Téléchargement et vérification du logiciel), l'installation peut s'effectuer en double-cliquant sur l'icône du paquet logiciel téléchargé, avant de poursuivre avec la ligne de commande.

Il est également possible d'installer le produit uniquement en ligne de commande, ce qui vous permettra de créer des scripts automatisant ce processus.

3.2 Conditions d'installation

Pour installer le Client VPN Linux vous devez disposer des privilèges de super-utilisateur (ou *root*) sur la machine.

Par ailleurs, vous devrez créer un fichier de configuration à utiliser sur le poste Linux à l'aide du client VPN Windows ou macOS.

3.3 Dépendances

Lors de l'installation du Client VPN Linux, les dépendances suivantes doivent également installées :

- epel

3.4 Contenu du paquet

Lors de l'installation du Client VPN Linux, les répertoires et fichiers suivants seront ajoutés sur le poste :

- `/usr/bin/tgbctl` : commande permettant de piloter le Client VPN Linux en ligne de commande
- `/usr/sbin/tgbiked` : daemon du Client VPN Linux qui tourne en tâche de fond
- `/lib/systemd/system/tgbiked.service` : fichier de configuration du daemon
- `/etc/tgb/conf.tgb` : fichier de configuration de la police de sécurité VPN, incluant un tunnel de test TheGreenBow
- `/usr/share/doc/thegreenbow/CLUF_VPN_TheGreenBow_vFR3.51.pdf` : document contenant le Contrat de Licence Utilisateur Final TheGreenBow
- `/usr/src/tgbtun-1.0` : dossier contenant les sources pour la gestion dynamique des modules noyau (DKMS)

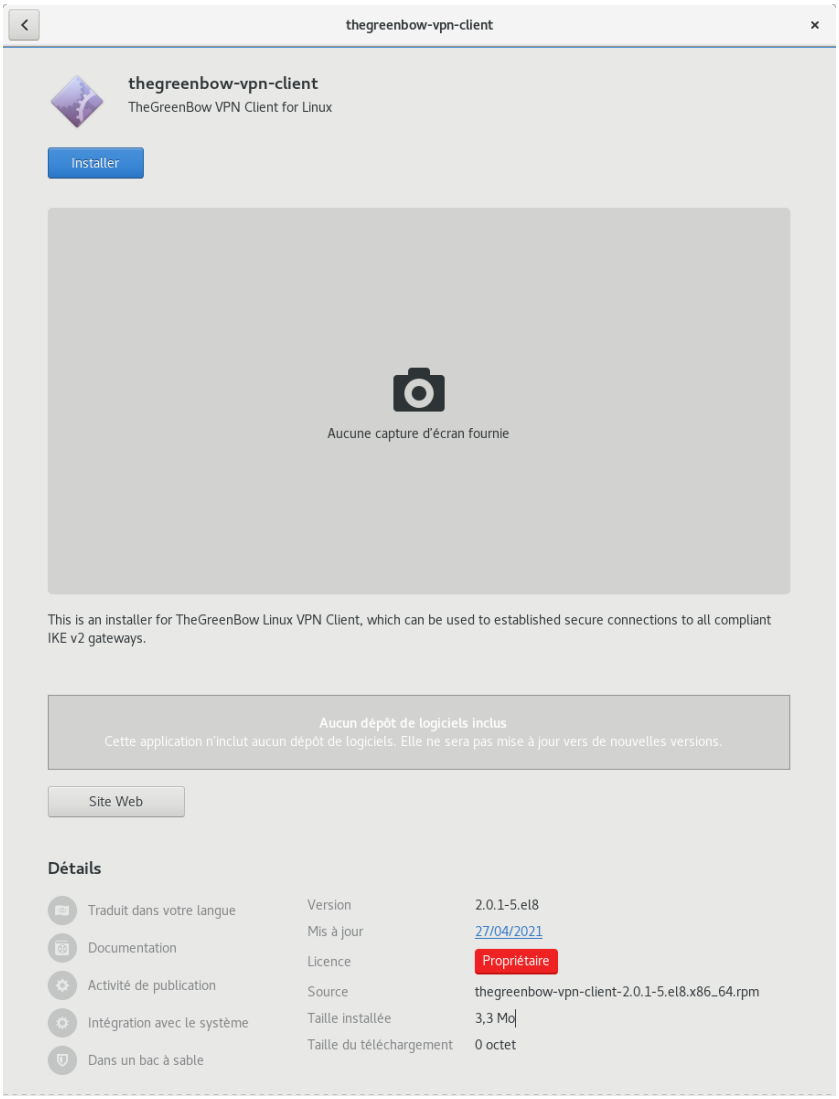
3.5 Installation interactive

Pour installer le Client VPN Linux, procédez de la manière suivante :

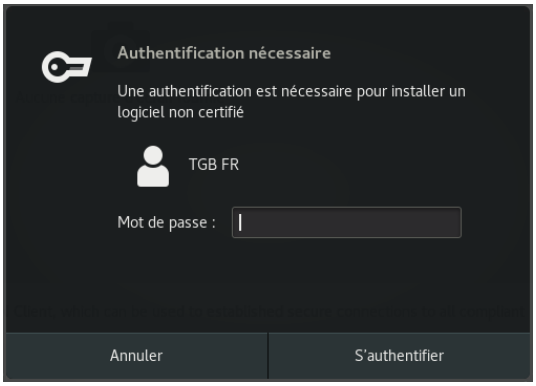
1. Si vous avez téléchargé le paquet logiciel à partir d'une autre machine que celle sur laquelle le Client VPN Linux doit être installé, copiez-le vers la machine de destination.

2. Double-cliquez sur l'icône du paquet :

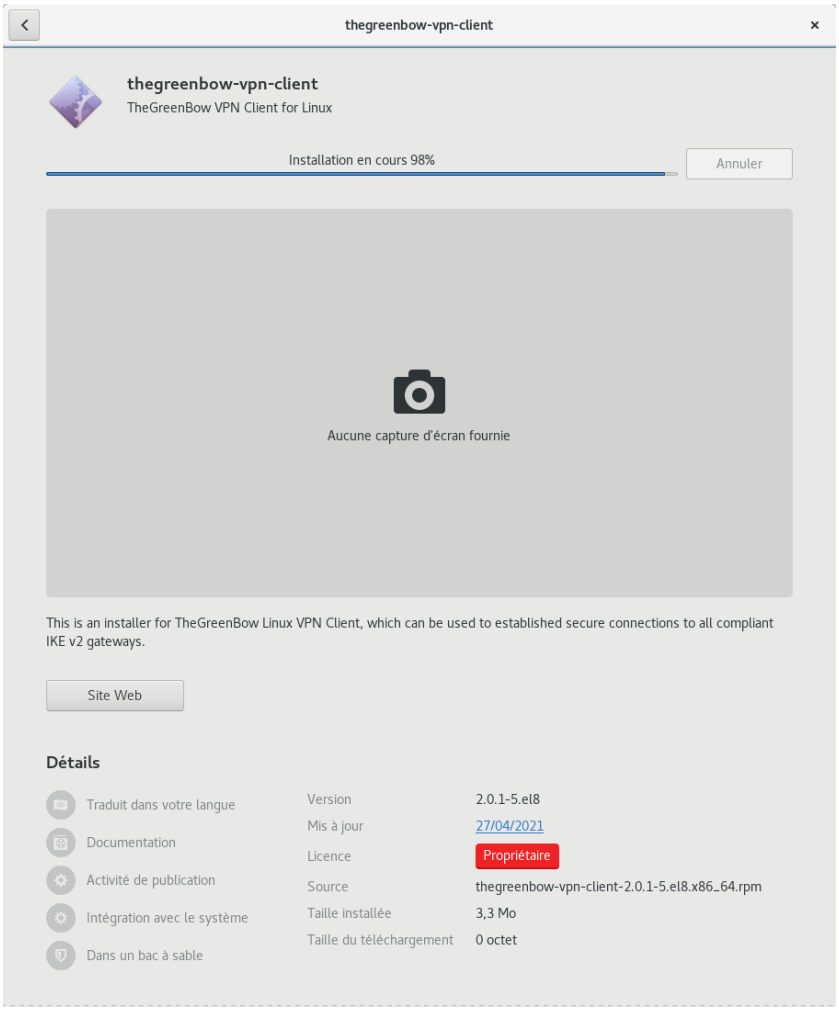
3. L'installation du programme se lance et la fenêtre suivante s'affiche :



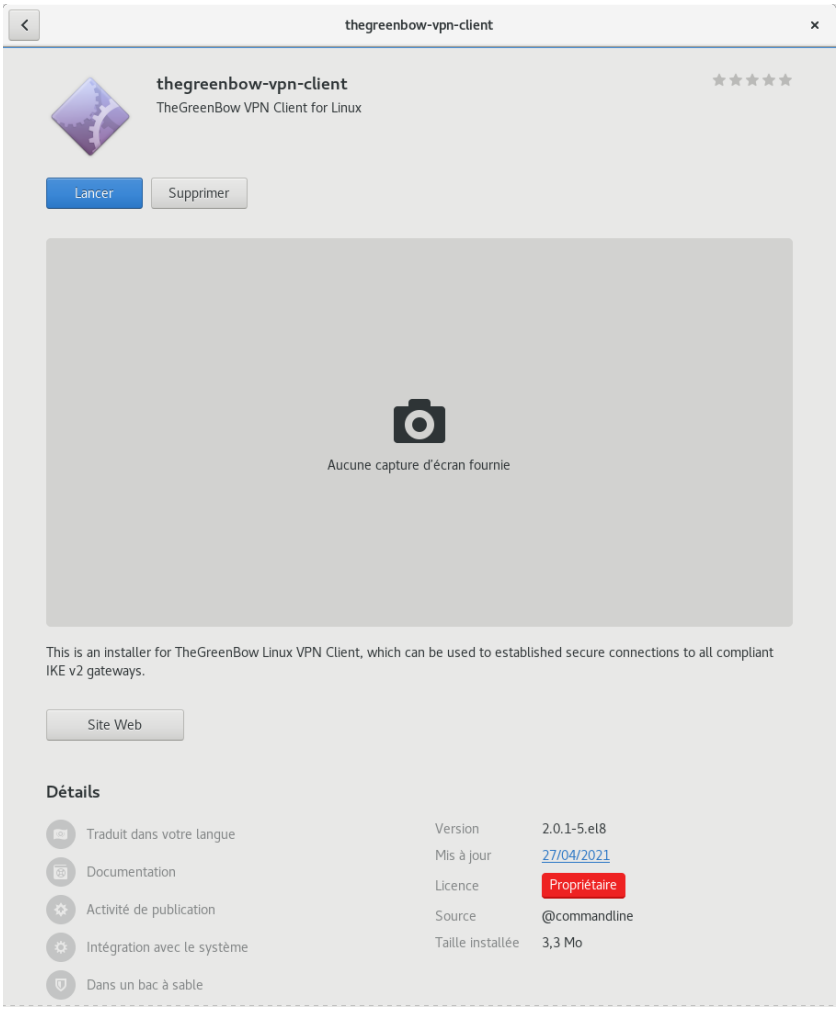
4. Cliquez sur **Installer**. Le programme d'installation vous demande de vous authentifier :



5. Entrez le mot de passe pour vous authentifier. L'installation proprement dite du logiciel commence :

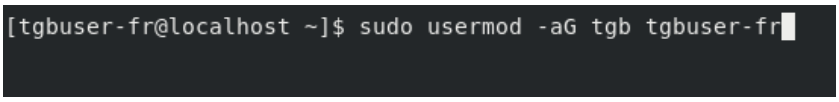


6. Si l'installation a réussi, l'écran suivant s'affiche :

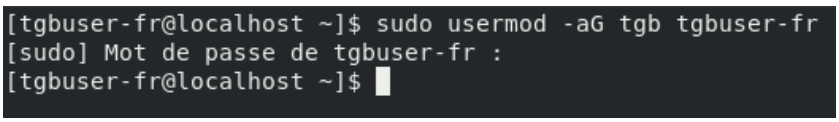


7. Ouvrez une fenêtre de terminal.
8. Ajoutez les utilisateurs du VPN au groupe `tgb` en exécutant la commande suivante :

```
sudo usermod -aG tgb [nom_utilisateur]
```



9. Saisissez le mot de passe du compte administrateur et appuyez sur Entrée.



10. Activez le produit (voir chapitre 4 Activation).

3.6 Installation en ligne de commande

Le Client VPN Linux peut être installé en ligne de commande. Pour cela, procédez de la manière suivante :

1. Si vous avez téléchargé le paquet logiciel à partir d'une autre machine que celle sur laquelle le Client VPN Linux doit être installé, copiez-le vers la machine de destination.
2. Ouvrez une fenêtre de terminal.
3. Accédez au dossier contenant le paquet `thegreenbow-vpn-client-2.0.1-x.el8.x86_64.rpm` (où le premier `x` est le numéro de révision du logiciel)
4. Exécutez la commande pour mettre à jour les dépôts de paquets :

```
sudo yum makecache
```

```
[tgbuser-fr@localhost ~]$ sudo yum makecache
[sudo] Mot de passe de tgbuser-fr :
CentOS Linux 8 - AppStream                      282  B/s | 4.3 kB     00:15
CentOS Linux 8 - BaseOS                         390  B/s | 3.9 kB     00:10
CentOS Linux 8 - Extras                         152  B/s | 1.5 kB     00:10
Extra Packages for Enterprise Linux Modular 8 - 6.4 kB/s |  36 kB     00:05
Extra Packages for Enterprise Linux 8 - x86_64  4.1 kB/s |  24 kB     00:05
Cache des métadonnées créé.
[tgbuser-fr@localhost ~]$
```

5. Exécutez la commande suivante pour installer le paquet complémentaire pour Linux Enterprise :

```
sudo yum install -y
https://dl.fedoraproject.org/pub/epel/epel-release-latest-
8.noarch.rpm
```

```
[tgbuser-fr@localhost ~]$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
Last metadata expiration check: 0:03:57 ago on Tue 27 Apr 2021 01:07:25 AM CEST.
epel-release-latest-8.noarch.rpm                                3.9 kB/s |  22 kB     00:05
Dependencies resolved.
================================================================================
 Package          Architecture     Version          Repository             Size
================================================================================
Installing:
 epel-release     noarch           8-10.el8         @commandline           22 k

Transaction Summary
================================================================================
Install  1 Package

Total size: 22 k
Installed size: 32 k
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : epel-release-8-10.el8.noarch                           1/1
  Running scriptlet: epel-release-8-10.el8.noarch                           1/1
  Verifying        : epel-release-8-10.el8.noarch                           1/1
Installed products updated.

Installed:
  epel-release-8-10.el8.noarch

Complete!
[tgbuser-fr@localhost ~]$
```

6. Exécutez la commande suivante pour installer le logiciel Client VPN Linux :

```
sudo yum install -y ~/Téléchargements/thegreenbow-vpn-client-
2.0.1-x.el8.x86_64.rpm
```

```
[tgbuser-fr@localhost ~]$ sudo yum install -y ~/Téléchargements/thegreenbow-vpn-client-2.0.1-6.el8.x86_64.rpm
Dernière vérification de l'expiration des métadonnées effectuée il y a 0:02:31 le mar. 27 avril 2021 15:01:42
CEST.
Dépendances résolues.
================================================================================================================
 Paquet                          Architecture       Version                Dépôt                   Taille
================================================================================================================
Installation:
 thegreenbow-vpn-client          x86_64             2.0.1-6.el8            @commandline            3.1 M

Résumé de la transaction
================================================================================================================
Installer  1 Paquet
```

7. Ajoutez les utilisateurs du VPN au groupe `tgb` en exécutant la commande suivante :

```
sudo usermod -aG tgb [nom_utilisateur]
```

8. Saisissez le mot de passe du compte administrateur et appuyez sur Entrée.

```
[tgbuser-fr@localhost ~]$ sudo usermod -aG tgb tgbuser-fr
[sudo] Mot de passe de tgbuser-fr :
[tgbuser-fr@localhost ~]$
```

9. Activez le produit (voir chapitre 4 Activation).

4 Activation

4.1 Introduction

Le Client VPN Linux doit être activé avant de pouvoir l'utiliser.

Les licences sont disponibles sous forme d'abonnement. Consultez la page du Client VPN Linux sur le site TheGreenBow pour en connaître tous les détails : https://www.thegreenbow.fr/vpn_linux.html.

Si vous souhaitez tester le logiciel avant de l'acheter, vous pouvez bénéficier d'une version d'essai. Téléchargez le logiciel à partir du site TheGreenBow, installez-le et suivez la procédure d'activation de la licence d'essai décrite ci-dessous à la section 4.4 Période d'essai.

Pour activer le Client VPN Linux, vous devez disposer des privilèges de super-utilisateur (*root*) sur la machine. Vous devez également créer un fichier de licence nommé `vpnsetup.ini` comme décrit ci-dessous.

4.2 Format et contenu du fichier vpnsetup.ini

Les informations d'activation du Client VPN Linux doivent être saisies dans un fichier `vpnsetup.ini` au format ASCII.

Pour cela, renseignez le numéro de licence qui vous a été fourni et l'adresse e-mail de l'utilisateur dans une section Activation comme suit :

```
[Activation]
License=123456-789012-345678-901234
Email=utilisateur@domaine.com
```

4.3 Procédure d'activation

4.3.1 Étapes d'activation

Pour activer le Client VPN Linux, suivez les étapes décrites ci-dessous :

10. Déposez le fichier `vpnsetup.ini` dans le dossier `/etc/tgb`.
11. Exécutez la commande suivante pour redémarrer le service :

```
sudo systemctl restart tgbiked.service
```

12. Exécutez la commande suivante pour générer un journal :

```
journalctl -r -t tgbiked
```

13. Vérifiez que le message suivant est présent dans le journal « Activation succeeded with license number 123456-789012-345678-901234. ». Pour savoir comment afficher le journal, reportez-vous au chapitre 9 Journaux.

4.3.2 Erreurs d'activation

Si le journal contient le message « Activation failed: no activation parameters » et/ou « Cancel starting UI Thread, product not activated », l'activation a échoué. Le Client VPN Linux s'arrête immédiatement.

```
Apr 20 12:14:35 localhost.localdomain tgbiked[99681]: Activation failed : no activation parameters
Apr 20 12:14:35 localhost.localdomain tgbiked[99681]: Cancel starting UI thread, product not activated
Apr 20 12:14:35 localhost.localdomain tgbiked[99681]: stopping ...
```

4.4 Période d'essai

Vous pouvez utiliser le Client VPN Linux gratuitement avec toutes ses fonctionnalités pendant une période d'essai de 30 jours.

Pour cela, installez le logiciel normalement et fabriquez un fichier de licence `vpnsetup.ini` comme décrit ci-dessus (voir section 4.2 Format et contenu du fichier vpnsetup.ini) en insérant 000000-000000-000000-000000 (24 zéros) à la place du numéro de licence.

À l'issue de la période d'essai de 30 jours, la licence est expirée et vous ne pourrez plus utiliser le logiciel. Si vous souhaitez continuer à l'utiliser, nous vous invitons à acquérir une licence.

Notre serveur d'activation enregistre l'identifiant de votre machine. Vous ne pourrez bénéficier d'une licence d'essai qu'une seule fois.

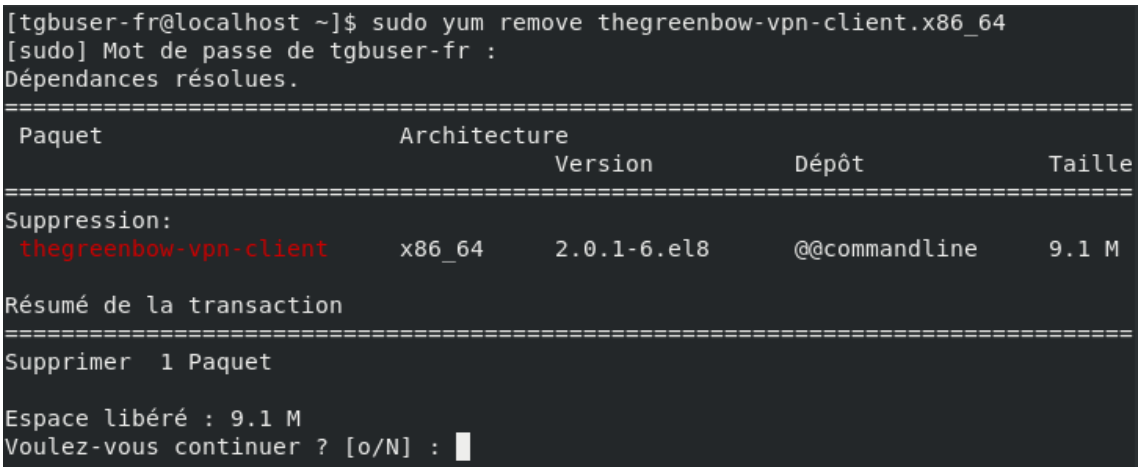
5 Désinstallation

Lorsque vous ne souhaitez plus utiliser le Client VPN Linux, vous pouvez le désinstaller en ligne de commande de la manière suivante :

1. Ouvrez une fenêtre de terminal.
2. Exécutez la commande suivante :

```
sudo yum remove thegreenbow-vpn-client.x86_64
```

Cette commande supprime les fichiers et les paquets dépendants ajoutés lors de l'installation et qui ne sont plus utilisés. Les fichiers de configuration ajoutés par la suite, p. ex. `config.tgb` ne sont pas supprimés.



Le Client VPN Linux a été désinstallé.

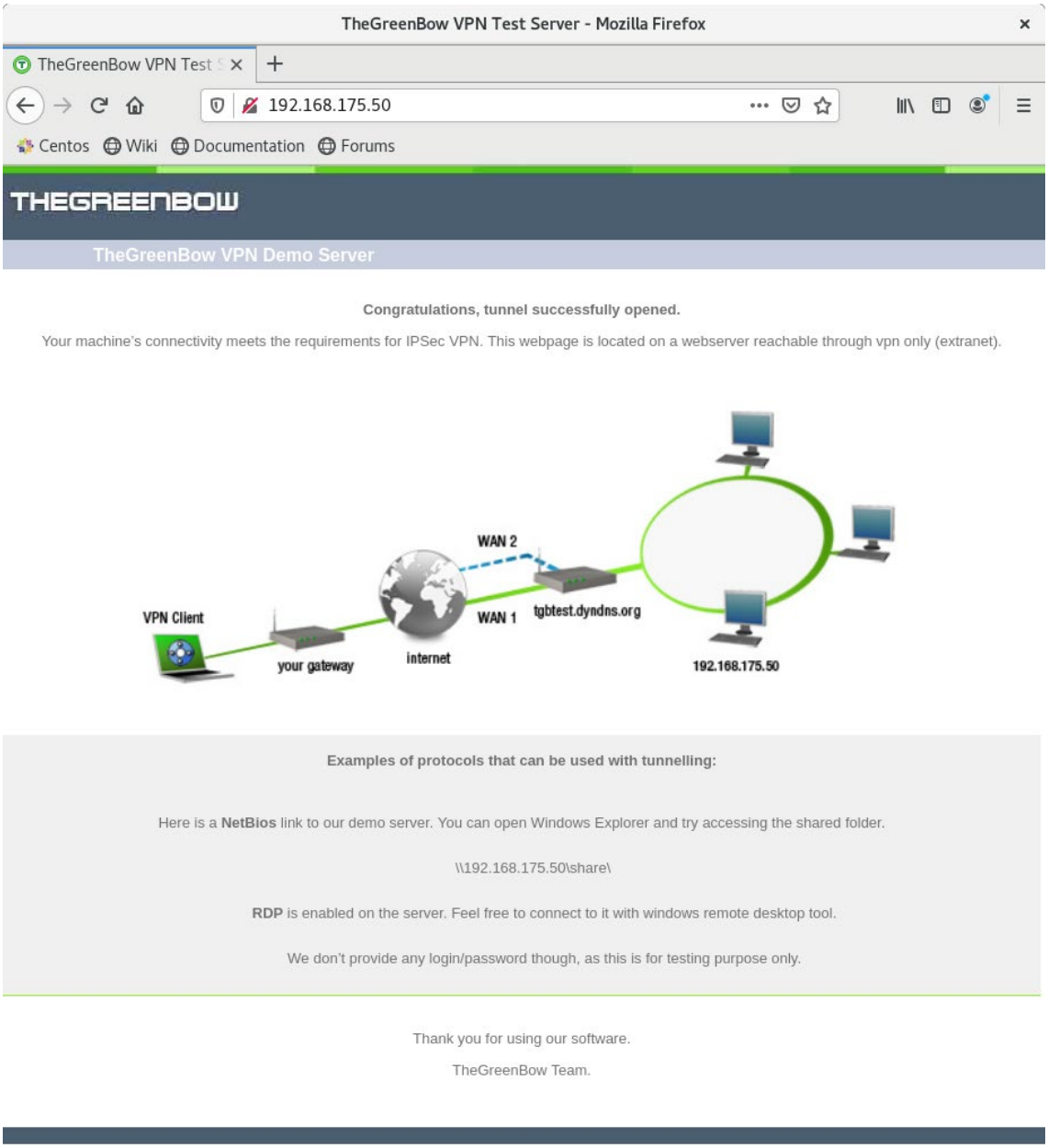
6 Utilisation du tunnel de test

Une politique de sécurité VPN contenant un tunnel VPN de test appelé « TgbTest » est fournie dans le fichier `conf.tgb` qui se trouve dans le répertoire `/etc/tgb/`.

Elle est importée par défaut et vous permet de tester le Client VPN Linux en vous connectant à une passerelle de test.

Cette configuration de test peut être utilisée pour vérifier que le Client VPN Linux est opérationnel.

Une fois le tunnel ouvert, vous devriez pouvoir envoyer une requête ping à l'adresse IP 192.168.175.50 ou visiter la page Web http://192.168.175.50/ dans votre navigateur Web.



7 Ligne de commande

7.1 Introduction

Le Client VPN Linux propose une interface en ligne de commande permettant de réaliser les opérations suivantes :

- Afficher l'aide
- Lister les tunnels configurés
- Ouvrir un tunnel
- Fermer un tunnel
- Afficher l'état du tunnel

7.2 Afficher l'aide

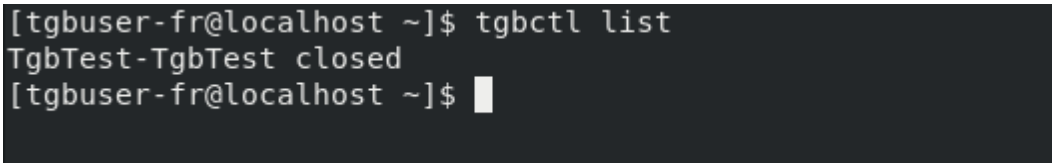
Pour afficher l'aide, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
tgbctl help
```

7.3 Lister les tunnels configurés

Pour lister les tunnels configurés, ouvrir une fenêtre de terminal et exécuter la commande suivante :

```
tgbctl list
```



7.4 Ouvrir un tunnel

Pour ouvrir un tunnel, ouvrir une fenêtre de terminal et exécuter la commande suivante :

```
tgbctl up [nom_tunnel]
```

```
[tgbuser-fr@localhost ~]$ tgbctl up TgbTest-TgbTest
opening TgbTest-TgbTest....opened
[tgbuser-fr@localhost ~]$
```

7.5 Fermer un tunnel

Pour fermer un tunnel, ouvrir une fenêtre de terminal et exécuter la commande suivante :

```
tgbctl down [nom_tunnel]
```

```
[tgbuser-fr@localhost ~]$ tgbctl down TgbTest-TgbTest
closing TgbTest-TgbTest....closed
[tgbuser-fr@localhost ~]$
```

7.6 Afficher l'état du tunnel

Pour afficher l'état du tunnel, ouvrir une fenêtre de terminal et exécuter la commande suivante :

```
tgbctl status [nom_tunnel]
```

```
[tgbuser-fr@localhost ~]$ tgbctl status TgbTest-TgbTest
open
[tgbuser-fr@localhost ~]$
```

8 Configuration des tunnels VPN

8.1 Introduction

Les clients VPN TheGreenBow s'appuient sur une politique de sécurité VPN qui définit la liste des tunnels mis à disposition par l'administrateur pour l'utilisateur du poste. Ce fichier s'appelle aussi fichier de configuration et son extension est `.conf`.

Le Client VPN Linux ne propose pas d'IHM permettant de fabriquer ou modifier la configuration VPN.

Cette fonctionnalité est assurée par les produits Client VPN Windows ou macOS (voir le guide de déploiement correspondant, vous trouverez les liens vers ces documents au chapitre 12 Documents connexes à consulter).

Si vous êtes administrateur, vous devez utiliser l'un de ces produits pour générer une politique de sécurité VPN comme indiqué dans la section 8.3 Mise à jour de la politique de sécurité VPN.

8.2 Protection de la politique de sécurité VPN

Le Client VPN Linux s'appuie sur le système d'exploitation Linux pour protéger la configuration. Le fichier de configuration est uniquement accessible aux utilisateurs bénéficiant des privilèges de super-administrateur.

Aucun autre utilisateur ne peut modifier le fichier de configuration ou en injecter un nouveau, ce qui en garantit l'authenticité et l'intégrité.

Le fichier de configuration VPN est stocké dans le fichier `conf.tgb` sous le répertoire `/etc/tgb/`.

Les droits sur ce fichier sont `-rw-------, owner root`. Un utilisateur standard ne peut donc pas accéder à la configuration VPN que ce soit en lecture ou en écriture.

8.3 Mise à jour de la politique de sécurité VPN

Afin de modifier la configuration de votre Client VPN Linux, procédez de la manière suivante :

1. Générez la configuration sous Windows ou macOS.
2. Exportez la configuration au format TGB, sans la protéger par mot de passe, sous le nom `conf.tgb`.
3. Remplacez le fichier `conf.tgb` dans le répertoire `/etc/tgb/` sur la machine sur laquelle vous souhaitez importer la configuration.

9 Journaux

9.1 Introduction

Les journaux du daemon IKE sont stockés à l'aide de la gestion des journaux `systemd`.

Pour accéder aux journaux du daemon IKE, exécutez la commande suivante dans une fenêtre de terminal :

```
journalctl -t tgbiked
```

9.2 Export au format texte

Pour exporter le contenu du journal au format texte, exécutez la commande suivante dans une fenêtre de terminal :

```
journalctl -t tgbiked > [mon_fichier_de_log.log]
```

Ce fichier sert de base pour le support client.

Dans le cas où il vous est demandé, afin que l'équipe support dispose de l'ensemble des informations dont elle a besoin, il convient également de lui communiquer les éléments suivants :

- version du paquet binaire utilisé,
- version de la distribution Linux,
- version du noyau Linux (*kernel*),
- version de la bibliothèque GNU C (glibc).

Pour obtenir les informations concernant la distribution et le noyau, exécutez la commande suivante dans une fenêtre de terminal :

```
uname -a
```

Pour obtenir les informations concernant la bibliothèque `glibc`, exécutez la commande suivante dans une fenêtre de terminal :

```
ldd --version
```

10 Limitations actuelles

La version actuelle du Client VPN Linux comporte des limitations suivantes :

- Il n'est pas possible d'importer une configuration chiffrée.
- Il n'est pas possible d'utiliser de carte à puce ou de token.
- Une seule connexion VPN peut être ouverte à la fois.
- Le groupe de clés DH 21 n'est pas encore disponible.

11 Gestion des erreurs

11.1 L'utilisateur doit appartenir au groupe « tgb »

Si vous n'avez pas ajouté l'utilisateur courant au groupe d'utilisateurs `tgb`, le message d'erreur suivant s'affiche lorsque vous exécutez des commandes :

```
ERROR: User must belong to "tgb" group
```

Pour ajouter l'utilisateur au groupe `tgb`, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
sudo usermod -aG tgb [nom_utilisateur]
```

Il est nécessaire de fermer/rouvrir la session, voire redémarrer le système, pour que cette commande soit prise en compte par CentOS/RedHat. Nous vous recommandons de faire un redémarrage du système dans tous les cas.

11.2 Impossible de récupérer la liste des tunnels

Lorsque vous exécutez la commande `tgbctl up [nom-tunnel]`, l'erreur suivante peut s'afficher :

```
Error : Can't get tunnel list, check if tgbiked
service is started
can't be open: check status
```

Pour vérifier que l'utilisateur a bien été ajouté au groupe `tgb`, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
id
```

Si le groupe `tgb` ne figure pas dans la liste, redémarrez la machine pour que l'ajout soit pris en compte.

11.3 Échec d'ouverture du tunnel

Lorsque le Client VPN Linux n'arrive pas à ouvrir un tunnel, le message d'erreur suivant s'affiche :

```
Opening [nom_tunnel] ..... failed
```

Lorsque l'ouverture du tunnel a échoué, ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
journalctl -r -t tgbiked
```

Vous pouvez analyser le journal vous-même (voir chapitre 9 Journaux) ou contacter l'équipe support : https://www.thegreenbow.com/form.html?subject=vpn&lang=fr.

11.4 Les utilisateurs standard ne doivent pas avoir accès au fichier de configuration

Lorsque le Client VPN Linux n'arrive pas à ouvrir un tunnel après avoir remplacé le fichier `/etc/tgb/conf.tgb` par une nouvelle configuration, consultez le journal pour voir s'il contient le message suivant : « Non-root users must not be able have access to file /etc/tgb/conf.tgb ». En effet, le fichier de configuration ne doit pas être accessible en lecture aux utilisateurs autres que les super-utilisateurs (*root*).

Si c'est le cas, exécutez la commande suivante :

```
sudo chmod 600 /etc/tgb/conf.tgb
```

11.5 Vérification des pilotes

Pour vérifier que le pilote (ou *driver*) est chargé, exécutez la commande suivante :

```
lsmod | grep tgb
```

La commande doit retourner le message suivant :

```
tgbtun       [identifiant] 0
```

Si ce n'est pas le cas, veuillez contacter l'équipe support pour comprendre ce qui s'est passé : https://www.thegreenbow.com/form.html?subject=vpn&lang=fr.

11.6 Blocage du daemon IKE

Si jamais le daemon IKE ne répond pas, ce qui peut arriver après un changement d'interface réseau, ou après avoir débranché et rebranché le câble réseau, lancez la commande suivante pour le redémarrer :

```
sudo kill -9 $(pidof tgbiked)
```

12 Documents connexes à consulter

Pour savoir comment générer le fichier de configuration à utiliser avec le Client VPN Linux, nous vous invitons à consulter les guides utilisateur suivant :

- Client VPN Windows Enterprise,
- Client VPN TheGreenBow macOS.

Retrouvez la liste des routeurs VPN compatibles et les guides de configuration correspondants sur le site TheGreenBow : https://www.thegreenbow.fr/vpn_gateway.html.

Vous pouvez télécharger une configuration de démonstration et ouvrir un tunnel de test en suivant les indications sur le site TheGreenBow : https://www.thegreenbow.com/support_flow.html?page=122&product=vpn&lang=fr.

Vous trouverez plus d'informations sur les produits TheGreenBow sur notre site internet : https://www.thegreenbow.fr.

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software