TheGreenBow VPN Certified 2013

Guide de Déploiement

Site Web : http://www.thegreenbow.com
Contact : support@thegreenbow.com

Table des matières

1 Introduction

Le Client VPN TheGreenBow est un Client VPN logiciel utilisable sur toute plate-forme Windows.

Le Client VPN TheGreenBow est conçu pour être facilement déployable et administrable.
A ce titre, le logiciel intègre de nombreuses fonctions qui permettent à l'administrateur réseau de préconfigurer l'installation avant un déploiement, d'installer ou de mettre à jour le logiciel à distance, ou encore d'administrer le logiciel et les politiques de sécurité VPN de façon centralisée.

Ce document décrit les options d'administration et de configuration du Client VPN TheGreenBow.
Il propose aussi un ensemble d'exemples de mise en œuvre de ces options, qui illustrent la façon de gérer le logiciel.

1.1 Méthode de déploiement ou d'installation

Le Client VPN TheGreenBow est spécialement étudié pour permettre les installations et les déploiements depuis différents supports, et suivants différents modes :
1/ Installation en mode silencieux
2/ Installation depuis un lecteur réseau
3/ Installation depuis un CD-ROM ou un support amovible type USB, préconfiguré

1.2 Options d'installation

Les options d'installation sont appliquées durant le processus d'installation du Client VPN TheGreenBow :

- Numéro de licence
- Mode de démarrage du Client VPN
- Masquage de l'interface du logiciel
- Options de gestion de PKI
- etc...

1.3 Options de mise en oeuvre

Les options de mise en oeuvre sont appliquées au lancement (parfois au premier lancement) du Client VPN TheGreenBow :

- Importation d'une la politique de sécurité VPN
- Démarrage du logiciel
- Ouverture d'un tunnel
- etc...

Toutes les options et fonctions décrites dans ce document sont applicables au Client VPN TheGreenBow à partir de la version 4.2 et supérieures. Pour des versions du logiciel antérieures, se reporter aux documents disponibles sur le site web TheGreenBow : http://www.thegreenbow.com/vpn_doc.html

1.4 Documentation

Ce document fait référence aux deux guides complémentaires, disponibles sur le site web TheGreenBow :

Intitulé	Référence
Guide Utilisateur du Client VPN TheGreenBow	tgbvpn_ug_fr.pdf
Guide de Déploiement Options PKI	tgbvpn_ug_deployment_pki_fr.pdf

2 Considérations de sécurité

2.1 Configuration du poste hôte

La machine sur laquelle est installé et exécuté le logiciel Client VPN IPsec TheGreenBow doit être saine et correctement administrée. En particulier :
1/ Elle dispose d'un anti-virus dont la base de données est régulièrement mise à jour,
2/ Elle est protégée par un pare-feu qui permet de maîtriser les communications entrantes et sortantes du poste qui ne passent pas par le Client VPN,
3/ Son système d'exploitation est à jour des différents correctifs
4/ Sa configuration permet d'éviter les attaques menées localement (analyse de la mémoire, patch ou corruption de binaire).

Note à destination de l'administrateur : Une vulnérabilité affectant l'installeur du logiciel a été identifiée. Pour éviter cette vulnérabilité, il est requis de veiller à installer le logiciel dans un répertoire vierge.

Des recommandations de configuration pour durcir le poste de travail sont disponibles sur le site de l'ANSSI, par exemple (sans que cette liste ne soit exhaustive) :

- Guide d'hygiène informatique
- Guide de configuration
- Mises à jour de sécurité
- Mot de passe

Pour une installation sur poste Windows 7, le guide Microsoft suivant peut aussi être consulté :
Common Criteria Security Target, Windows 7 and Windows Server 2008 R2

2.2 Droits d'exécution

Le Client VPN TheGreenBow est conçu pour pouvoir être installé avec les droits "administrateur", et être ensuite complètement utilisable avec des droits "utilisateur" stricts, ceci quelle que soit la plate-forme Windows utilisée.

Dans la mesure où certaines opérations sont interdites en mode "utilisateur" (par exemple la désinstallation du logiciel), il est fortement recommandé de déployer le logiciel en respectant cette utilisation des droits :
1/ Installation en mode "administrateur"
2/ Utilisation en mode "Utilisateur"

2.3 Configuration pour l'utilisateur final

Le Client VPN TheGreenBow est conçu pour pouvoir être utilisé, simultanément et de façon cloisonnée, par un administrateur (installation, configuration initiale personnalisation) et par l'utilisateur final.

Toute l'interface du logiciel peut être paramétrée pour ne laisser à l'utilisateur final qu'un nombre restreint d'opérations disponibles (ouvrir ou fermer un tunnel VPN).

De même, le logiciel peut être intégralement configuré, dès son installation ou son déploiement, pour réserver strictement l'accès aux politiques de sécurité VPN à l'administrateur seul (masquage des fonctions, mot de passe de contrôle d'accès, etc…)

Les options de configuration du logiciel décrites dans la suite de ce document permettent précisément de mettre en place ce cloisonnement, afin de mettre œuvre le Client VPN dans les meilleures conditions de sécurité et de fiabilité possibles.

2.4 Gestion multi-utilisateurs

Le Client VPN TheGreenBow présente la même configuration VPN (politique de sécurité) à tous les utilisateurs d'un poste multi-utilisateurs. Il est donc recommandé de mettre en œuvre le logiciel sur un poste dédié (en conservant par exemple un compte administrateur et un compte utilisateur, comme indiqué précédemment).

2.5 Gestion des politiques de sécurité VPN

Le Client VPN TheGreenBow offre en standard un ensemble d'options de ligne de commande permettant l'importation, l'exportation, le remplacement ou l'application de nouvelles politiques de sécurité VPN.

Ces options sont destinées à être utilisées pour des scripts de déploiement du logiciel, pour des opérations de mises à jour ou de maintenance à distance, pour la réalisation d'automatisations diverses telles que les ouvertures et fermetures automatiques de tunnel VPN.

Ce document décrit la façon d'utiliser ces différentes options de ligne de commande, pour ne pas mettre en péril l'intégrité ou la confidentialité des politiques de sécurité VPN.

2.6 Authentification de l'utilisateur

Comme détaillé dans le "Guide Utilisateur du Client VPN TheGreenBow" (tgbvpn_ug_fr.pdf), il est recommandé de privilégier l'utilisation de certificat, si possible stocké sur token ou sur carte à puce, pour assurer l'authentification forte de l'utilisateur lors de l'ouverture du tunnel VPN.

Les options de configuration du logiciel concernant la mise en œuvre de cette fonction sont détaillées dans un document dédié : le "Guide de Déploiement Options PKI" (tgbvpn_ug_deployment_pki_fr.pdf)

2.7 Protection des données sensibles

Comme détaillé dans le "Guide Utilisateur du Client VPN TheGreenBow" (tgbvpn_ug_fr.pdf), il est recommandé de ne mémoriser aucune donnée sensible dans le fichier de configuration VPN : login / mot de passe X-Auth, pre-shared key ou certificat.

2.8 Réinitialisation

L'environnement Windows permet de désinstaller puis de ré-installer le logiciel.
Au cours d'une désinstallation, la politique de sécurité est supprimée. Cette procédure permet de réinitialiser le logiciel dans sa configuration initiale.

3 Déploiement du Client VPN

Le déploiement du logiciel s'appuie principalement sur sa capacité à être installé de façon silencieuse, c'est-à-dire, sans sollicitation (question ou alerte) de l'utilisateur.

Ainsi, toutes les options de configuration du logiciel peuvent être transmises à l'installation, via des fichiers d'initialisation, ou via le jeu d'options de ligne de commande.

3.1 Installation silencieuse

Une installation "silencieuse" est une installation qui s'effectue sans sollicitation de l'utilisateur : aucune question ni aucune alerte. L'installation est exécutée intégralement de façon transparente.

Les paramètres de l'installation sont dans ce cas configurés via le jeu d'options de ligne de commande, ou via le fichier d'initialisation "VpnSetup.ini" qui accompagne l'installation.

Note : Suivant la politique de sécurité mise en place sur le poste cible, une notification Windows de lancement du programme peut être affichée. Contacter le support TheGreenBow pour éviter l'affichage de cette fenêtre.

3.1.1 Créer une installation silencieuse

L'installation du Client VPN TheGreenBow s'exécute en mode "silencieux" lorsque l'option "/S" est ajoutée à la ligne d'exécution du programme d'installation :

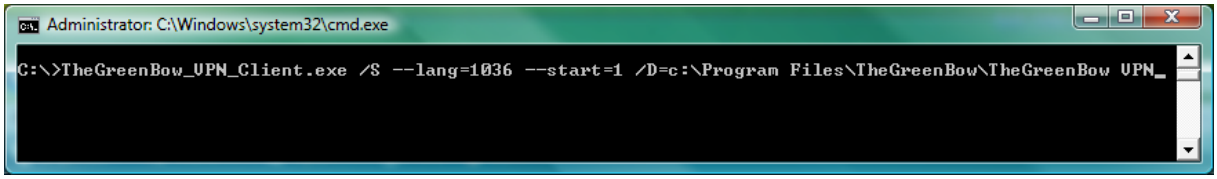
```
TheGreenBow_VPN_Client.exe /S (options supplémentaires)
```

3.1.2 Exemple

Installation en ligne de commande depuis la fenêtre de commande Windows
1/ Télécharger le Client VPN TheGreenBow depuis http://www.thegreenbow.com/vpn
2/ Ouvrir la fenêtre de commande Windows
3/ Entrer la ligne de commande suivante :

```
[rép_téléchargement]\TheGreenBow_VPN_Client.exe /S --lang=1036 /D=[rép_installation]
```

[rép_téléchargement] est le répertoire où le fichier TheGreenBow_VPN_Client.exe a été téléchargé
[rép_installation] est le répertoire où le logiciel doit être installé (le logiciel est installé par défaut sous le répertoire "C:\Program Files\TheGreenBow\TheGreenBow VPN")
L'option "`/D`" doit être utilisée en fin de ligne de commande, et sans espace entre l'option, le signe "=" et la valeur.
L'option "`--lang`" est détaillée dans les chapitres suivants.



Note : Se reporter au chapitre 7.1 pour les différentes règles de syntaxe des options.

3.2 Déploiement depuis un script

1/ Créer un fichier texte appelé "vpn_setup.bat"
2/ Editer ce fichier (clic droit et sélectionner "Modifier")
3/ Entrer les lignes de commandes à exécuter
4/ Déployer ce fichier batch avec l'exécutable TheGreenBow_VPN_Client.exe

Exemple :

```
cd .\setup
TheGreenBow_VPN_Client.exe /S --lang=1036
cd ..
copy myvpnconfig.tgb C:\Program Files\TheGreenBow\TheGreenBow VPN
cd C:\Program Files\TheGreenBow\TheGreenBow VPN
vpnconf.exe /importonce:myvpnconfig.tgb
```

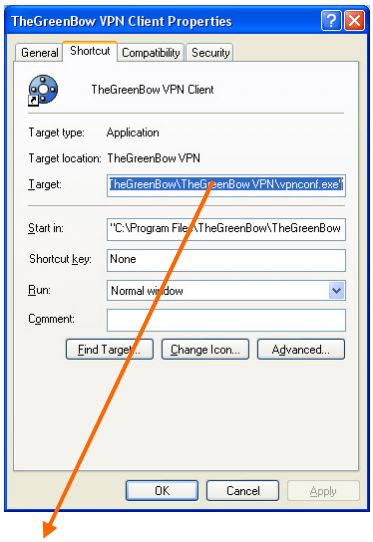
Dans cet exemple :
- Le répertoire contenant l'installeur du logiciel s'appelle "setup" et est situé dans le répertoire contenant le fichier batch
- Cette installation se termine par l'importation de la politique de sécurité "myvpnconfig.tgb"

Note : Se reporter au chapitre 7.1 pour les différentes règles de syntaxe des options.

3.3 Déploiement depuis un lecteur réseau ou un raccourci

1/ Télécharger le Client VPN TheGreenBow
2/ Clic-droit sur l'exécutable "TheGreenBow_VPN_Client.exe"
3/ Sélectionner "Créer un raccourci"
4/ Clic-droit sur le raccourci qui vient d'être créé
5/ Sélectionner "Propriétés"
6/ Dans l'onglet "**Raccourci**", dans le champ "**Cible :**", ajouter les options désirées à la ligne de commandes, en veillant à conserver des espaces entre les différentes options.
7/ Copier le raccourci à l'endroit où l'utilisateur peut l'exécuter (par exemple sur son bureau Windows)

Exemple :



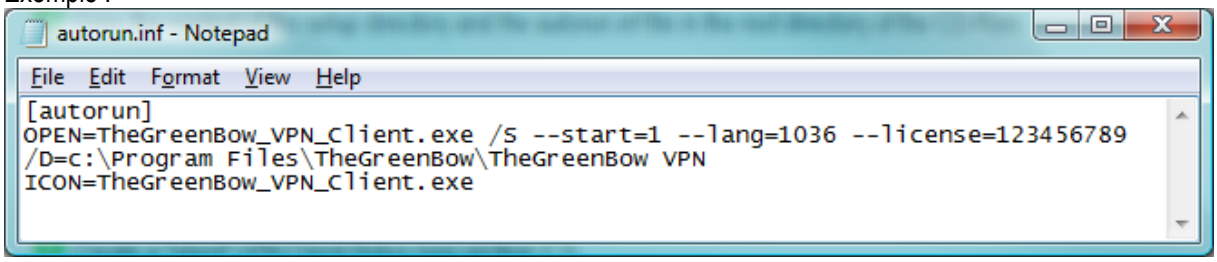

```
"F:\TheGreenBow_VPN_Client.exe /S --start=1 --lang=1036 /D=C:\Program Files\TheGreenBow\TheGreenBow VPN"
```

3.4 Déploiement depuis un CD-ROM

1/ Créer un fichier texte appelé "autorun.inf" dont le contenu est le suivant :

```
[autorun]
OPEN=TheGreenBow_VPN_Client.exe /S /D=c:\Program Files\TheGreenBow\TheGreenBow VPN
(+ options supplémentaires, Cf. chapitre 7.1)
ICON=TheGreenBow_VPN_Client.exe
```

Exemple :



2/ Copier à la racine du CD-ROM
- Le fichier "autorun.inf"
- Le fichier "TheGreenBow_VPN_Client.exe"

Dès son insertion dans le poste cible, l'installation sera exécutée automatiquement et de façon silencieuse.

Note : Se reporter au chapitre 7.1 pour les différentes règles de syntaxe des options.

Note : voir aussi 'Enabling and Disabling AutoRun' pour certaines versions de Windows (i.e. http://msdn.microsoft.com/en-us/library/windows/desktop/cc144204%28v=vs.85%29.aspx#floppy).

3.5 Déploiement d'une mise à jour

Le déploiement d'une mise à jour du Client VPN TheGreenBow s'exécute exactement comme le déploiement d'une nouvelle installation.

Dans le cadre d'une mise à jour silencieuse, tout le processus de mise à jour est silencieux : backup de la politique de sécurité VPN de la précédente version, installation de la nouvelle version, restauration de la politique de sécurité VPN de l'ancienne version.

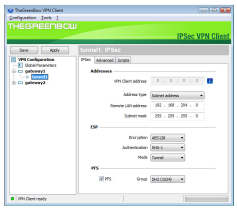
Restriction : Si la version du Client VPN installé est inférieure à 4.2, la mise à jour du logiciel nécessite une désinstallation de ce logiciel qui, en standard, n'est pas silencieuse. Pour rendre cette désinstallation silencieuse, contacter le support TheGreenBow.

4 Paramétrage du Client VPN pour l'utilisateur final

4.1 Interface du logiciel

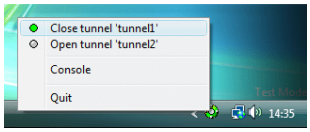
Le Client VPN TheGreenBow est utilisable via 3 interfaces :

1/ Le Panneau de Configuration
Cette interface est utilisée pour configurer la politique de sécurité VPN.
Elle permet toutes les opérations de gestion de la politique de sécurité VPN : création, modification, sauvegarde, exportation, importation.



2/ Le Panneau des Connexions
Cette interface permet d'ouvrir et de fermer les tunnels VPN, et d'informer l'utilisateur sur les éventuels incidents VPN

3/ Le menu en barre des tâches
Cette interface est utilisée pour ouvrir et fermer les tunnels VPN, et pour ouvrir les différentes interfaces.



Le Panneau de Configuration donne accès à la politique de sécurité VPN : Il permet de modifier, de sauvegarder, d'importer, d'exporter et d'appliquer toute nouvelle politique de sécurité VPN.
Il est donc fortement recommandé de restreindre son accès, voire son affichage, à l'administrateur seul.

Le Panneau des Connexions ainsi que le menu en barre des tâches peuvent aussi être limités, pour ne présenter à l'utilisateur final qu'un jeu réduit d'opérations autorisées : Il est ainsi possible de configurer l'installation du Client VPN TheGreenBow pour que l'utilisateur final ne puisse qu'ouvrir et fermer un tunnel VPN, aucune autre fonction ne lui étant laissée accessible.

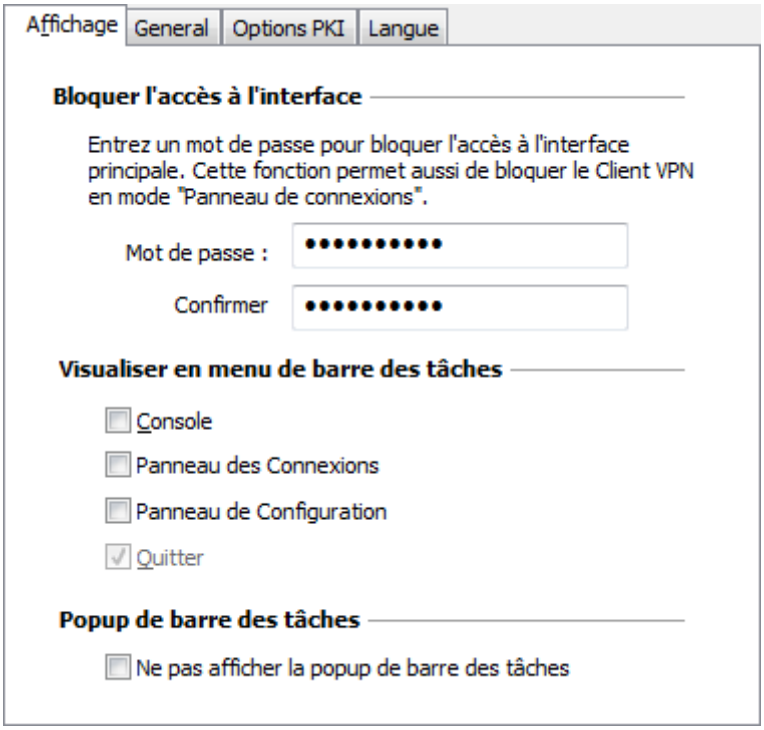
Ces limitations et restrictions d'accès peuvent toutes être configurées au cours de l'installation du logiciel. Les différentes options de configuration font l'objet du chapitre présent.

4.2 Limitation de l'interface utilisateur

4.2.1 Via le Panneau de Configuration du Client VPN

Le Panneau de Configuration peut être masqué ou protégé par mot de passe, les items du menu en barre des tâches peuvent être limités. Ces limitations sont configurables via le Panneau de Configuration du logiciel, comme décrit dans le "Guide Utilisateur du Client VPN TheGreenBow" (référence : tgbvpn_ug_fr)

Exemple :
Dans le Panneau de Configuration, ouvrir le menu "Outils > Options", sélectionner l'onglet "Affichage"
Entrer un mot de passe et confirmer
Décocher toutes les options "Console", "Panneau des Connexions" et "Panneau de Configuration"
Valider puis fermer l'interface du logiciel (bouton "Fermer" en haut à droite du Panneau de Configuration)



Le Client VPN n'est plus accessible que de deux façons :
1/ Soit par le menu en barre des tâches, qui ne donne plus la possibilité que d'ouvrir ou fermer les tunnels VPN
2/ Soit par clic gauche sur l'icône en barre des tâches, qui ouvre la fenêtre de demande du mot de passe pour accéder au Panneau de Configuration, désormais protégé.

Dans ce mode, plus aucune opération sur la politique de sécurité VPN n'est possible ni autorisée à l'utilisateur final.

4.2.2 Via les options d'installation

L'option d'installation "**`--guidefs=user`** " permet de configurer le Client VPN pour qu'il affiche le Panneau des Connexions à son démarrage (plutôt que le Panneau de Configuration)

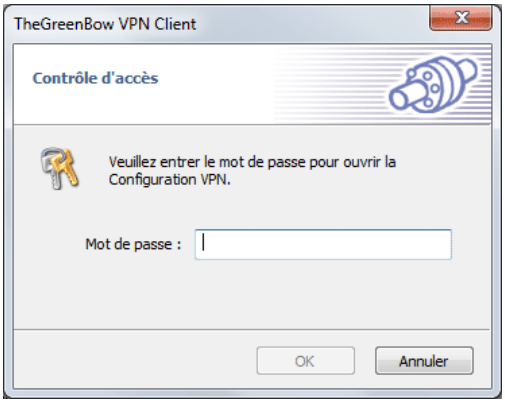
```
TheGreenBow_VPN_Client.exe --guidefs=user
```

L'option d'installation "**`--guidefs=hidden`** " permet de configurer le Client VPN pour qu'il n'affiche ni le Panneau de Configuration ni le Panneau des Connexions à son démarrage. Son affichage est réduit à l'icône en barre des tâches.

```
TheGreenBow_VPN_Client.exe --guidefs=hidden
```

L'option d'installation "**--password=*mypassword*** " permet de protéger l'accès au panneau de Configuration par un mot de passe

```
TheGreenBow_VPN_Client.exe --guidefs=hidden --password=Adm1#
```



Dans cette configuration, l'utilisateur ne peut pas ouvrir le Panneau des Connexions, et l'accès au Panneau de Configuration est protégé par mot de passe. Aucune opération sur la politique de sécurité VPN ne lui est autorisée. L'utilisateur peut uniquement ouvrir un tunnel VPN via le menu en barre des tâches (clic-droit sur l'icône en barre des tâches).

Cette configuration est recommandée dans la mesure où elle sécurise complètement l'accès à la politique de sécurité VPN.

4.2.3 Via le paramétrage de la base de registre

Le Client VPN TheGreenBow offre, en standard, un mode dit "mode USB", qui permet de stocker une politique de sécurité sur clé USB, et de monter le tunnel VPN associé à cette politique automatiquement sur insertion de cette clé USB.
Ce mode peut être désactivé en positionnant la clé suivante en base de registre :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\TgbIke.exe
NoUSBMode = 1 (binary)
```

5 Déploiement des politiques de sécurité VPN

5.1 Embarquer une politique de sécurité VPN dans l'installation

Une politique de sécurité VPN (configuration VPN) préconfigurée peut être embarquée avec l'installation du Client VPN TheGreenBow.
Cette politique de sécurité sera automatiquement importée et appliquée au cours de l'installation du logiciel.
Elle sera ainsi immédiatement opérationnelle pour l'utilisateur final, dès le premier lancement du Client VPN.

5.1.1 Procédure

1/ Créer la politique de sécurité VPN (Configuration VPN) à destination du poste à équiper

2/ Exporter cette politique de sécurité VPN (menu "Configuration > Export", Cf. Guide Utilisateur du Client VPN TheGreenBow) sans la protéger par mot de passe.

3/ Copier la politique de sécurité VPN dans le répertoire dans lequel se trouve le setup du Client VPN (fichier TheGreenBow_VPN_Client.exe)

4/ Transférer ce package (setup + politique de sécurité VPN) sur le poste à équiper

5/ Exécuter l'installation du Client VPN : A la fin de l'installation, le Client VPN est installé avec la politique de sécurité VPN importée et appliquée.

Du point de vue de la sécurité du déploiement, cette méthode exploite la fonction de contrôle d'intégrité des politiques de sécurité VPN (fonction standard du Client VPN). Cette fonction garantit que la politique de sécurité importée au moment de l'installation n'a pas été corrompue.
Pour un déploiement mettant aussi en œuvre la fonction de confidentialité de la politique de sécurité VPN, voir la procédure ci-dessous.

5.2 Déployer une nouvelle politique de sécurité VPN

5.2.1 Procédure

1/ Créer la politique de sécurité VPN (Configuration VPN) à destination du poste à équiper

2/ Exporter cette politique de sécurité (menu "Configuration > Export", Cf. Guide Utilisateur du Client VPN TheGreenBow). Elle peut être chiffrée par un mot de passe.

3/ Transférer cette politique de sécurité VPN sur le poste à mettre à jour (mail, partage de fichier, etc...)

4/ Sur le poste cible, ouvrir (double-clic sur le fichier ".tgb") la politique de sécurité VPN : le mot de passe de protection est automatiquement demandé. Une fois correctement renseigné, la politique de sécurité VPN est importée et appliquée.

Remarque : Dans la version "Client VPN Certifié 2013", l'ouverture directe d'un fichier ".tgb" n'est pas autorisée.
L'importation d'une nouvelle politique de sécurité reste néanmoins possible :
1/ via le menu "Configuration > Import" du Panneau de Configuration
2/ ou par ligne de commande, en spécifiant le cas échéant le mot de passe utilisé pour protéger la configuration exportée (Cf. options /import et /pwd détaillées au chapitre 7.2)

5.3 Protéger une politique de sécurité VPN avant déploiement

Comme vu précédemment, le Client VPN vérifie en standard l'intégrité des politiques de sécurité importées et exportées. Il est de plus possible d'assurer leur confidentialité en spécifiant un mot de passe de protection au moment de l'exportation. Ce mot de passe est demandé à leur importation.

5.3.1 Intégrité d'une politique de sécurité VPN exportée

La protection de l'intégrité d'une politique de sécurité VPN lorsqu'elle est exportée est une fonction activable par la clé en base de registre :

- Windows XP :
  `HKEY_LOCAL_MACHINE\SOFTWARE\TheGreenBow\TheGreenBow VPN\SignFile = 1 (binary)`
- Windows x64 :
  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TheGreenBow\TheGreenBow VPN\SignFile = 1 (binary)`

5.3.2 Procédure

1/ Créer la politique de sécurité VPN (Configuration VPN) à destination du poste à équiper

2/ Exporter cette politique de sécurité (menu "Configuration > Export", Cf. Guide Utilisateur du Client VPN TheGreenBow) en la protégeant par un mot de passe.

3/ Exécuter l'installation du Client VPN sur le poste cible

4/ Une fois le logiciel installé, transférer la politique de sécurité VPN sur le poste à installer

5/ Importer cette politique de sécurité VPN: soit par ouverture directe du fichier ".tgb", soit par ligne de commande (Cf. options /import et /pwd détaillées au chapitre 7.2), soit par le menu "Configuration > Import" du Panneau de Configuration : le mot de passe de protection est demandé.

Remarque : Dans la version "Client VPN Certifié 2013", l'ouverture directe d'un fichier ".tgb" n'est pas autorisée.
L'importation d'une nouvelle politique de sécurité reste néanmoins possible :
1/ via le menu "Configuration > Import" du Panneau de Configuration
2/ ou par ligne de commande, en spécifiant le cas échéant le mot de passe utilisé pour protéger la configuration exportée (Cf. options /import et /pwd détaillées au chapitre 7.2)

6 Automatisations du logiciel Client VPN

6.1 Créer un batch/script qui ouvre ou ferme un tunnel automatiquement

Depuis la version 4.1, le logiciel Client VPN permet d'ouvrir et de fermer un tunnel par les lignes de commande suivantes, utilisables dans un script :

```
vpnconf.exe /open:[NomPhase1-NomPhase2]
vpnconf.exe /close:[NomPhase1-NomPhase2]
```

Pour toutes les versions du logiciel Client VPN, il est aussi possible d'ouvrir et de fermer un tunnel par script, via la procédure suivante :

1/ Créer une politique de sécurité VPN (Configuration VPN) avec l'option "Ouvrir automatiquement ce tunnel lorsque le Client VPN démarre" sélectionnée.

2/ Exporter la politique de sécurité VPN (Configuration VPN) dans un fichier (p.ex.: "MonTunnel.tgb")

3/ Créer le script avec la ligne de commande suivante : `vpnconf.exe /import:MyTunnel.tgb`

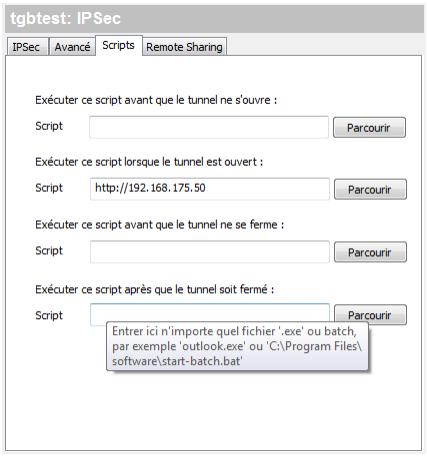
Ce script démarrera le logiciel Client VPN en important la politique de sécurité VPN (Configuration VPN) "MonTunnel.tgb", et ouvrira automatiquement le tunnel VPN.
Pour fermer le tunnel, il est possible d'utiliser la ligne de commande : `vpnconf.exe /stop`
Qui fermera le tunnel VPN ouvert, avant de quitter le logiciel.

6.2 Ouvrir automatiquement une page web lorsque le tunnel VPN est ouvert

1/ Créer une politique de sécurité VPN (Configuration VPN)

2/ Ouvrir l'onglet "Scripts" de la Phase 2 du tunnel VPN concerné

3/ Dans le champ "Exécuter ce script lorsque le tunnel est ouvert :", entrer l'url de la page web à ouvrir (page web internet ou sur l'intranet de l'entreprise)



4/ Sauver la Configuration VPN et ouvrir le tunnel VPN : la page web est automatiquement ouverte dès que le tunnel VPN est ouvert.

6.3 Ouvrir un tunnel VPN par double-clic sur un icône du bureau Windows

Le Client VPN TheGreenBow permet d'ouvrir un tunnel VPN par double-clic sur un icône du bureau Windows.

1/ Créer une politique de sécurité VPN (Configuration VPN) avec l'option "Ouvrir automatiquement ce tunnel lorsque le Client VPN démarre" sélectionnée.

2/ Exporter cette Configuration VPN dans un fichier (p.ex.: "MonTunnel.tgb")

3/ Déplacer ce fichier, ou faire un raccourci sur ce fichier, sur le bureau Windows

Un double-clic sur l'icône ainsi créé sur le bureau Windows ouvrira le logiciel Client VPN, qui importera automatiquement la Configuration VPN "MonTunnel.tgb" et ouvrira automatiquement le tunnel VPN.

A noter : Cette fonction n'est pas proposée dans la version "Client VPN Certifié 2013".

6.4 Options d'importation "/import", "/importonce", "/add" et "/replace"

L'option de ligne de commande "`/import`" permet d'importer une politique de sécurité VPN (Configuration VPN) en démarrant en même temps le logiciel Client VPN, s'il n'est pas déjà démarré.

L'option "`/importonce`" permet d'importer une politique de sécurité VPN (Configuration VPN) sans démarrer le logiciel Client VPN.

Lorsque le logiciel Client VPN est démarré, ces deux options importent simplement la politique de sécurité VPN.

Lorsque la politique de sécurité VPN courante (avant importation) du Client VPN n'est pas vide, ces deux options demandent à l'utilisateur s'il veut "Ajouter ou remplacer" la nouvelle politique de sécurité VPN.
Les options "`/add`" et "`/replace`" permettent d'éviter cette demande à l'utilisateur : L'option "`/add`" ajoute systématiquement la politique de sécurité VPN, l'option "`/replace`" la remplace systématiquement.

Option	Demande à l'utilisateur "Ajouter ou remplacer"	Lance le Client VPN s'il n'est pas démarré
/import	oui	oui
/importonce	oui	non
/add	non : ajoute la politique de sécurité VPN	non
/replace	non : remplace la politique de sécurité VPN	non

Remarque : Lorsque la politique de sécurité VPN est vide, les options "`/import`" et "`/importonce`" ne demandent rien à l'utilisateur et "ajoutent" la politique de sécurité VPN.

6.4.1 Protection de la politique de sécurité VPN

Il est possible et recommandé de conditionner l'utilisation de cette option de ligne de commande à l'utilisation du mot de passe administrateur :

Lorsque l'accès au Panneau de Configuration (interface principale du logiciel) est protégée par mot de passe (appelé "mot de passe administrateur"), il est obligatoire d'ajouter ce mot de passe, en ligne de commande via l'option "/pwd", à toutes les commandes d'importation ou d'exportation : "`/import`", "`/importonce`", "`/add`", "`/replace`"

Si le mot de passe "administrateur" n'est pas spécifié dans la ligne de commande, l'opération d'importation ou d'exportation est refusée.

Note : Cette fonction de sécurité implique que, lorsque l'accès au Panneau de Configuration est protégé par mot de passe, l'importation ou l'exportation d'une politique de sécurité chiffrée par mot de passe (autre que le mot de passe administrateur) n'est pas possible en ligne de commande. Elle reste possible en utilisant les menus du Panneau de Configuration.

D'un point de vue sécurité, il est recommandé de privilégier les options "/importonce", "/add" et "/replace" pour des opérations de maintenance (versus l'option "/import"), puisque le logiciel est quitté immédiatement après leur exécution.

6.5 Options d'exportation "/export", "/exportonce"

L'option de ligne de commande "`/export`" permet d'exporter une politique de sécurité VPN (Configuration VPN) en démarrant en même temps le logiciel Client VPN, s'il n'est pas déjà démarré.

L'option "`/exportonce`" permet d'exporter une politique de sécurité VPN (Configuration VPN) sans démarrer le logiciel Client VPN.

Lorsque le logiciel Client VPN est démarré, ces deux options exportent simplement la politique de sécurité VPN.

6.5.1 Protection de la politique de sécurité VPN

Il est possible et recommandé de conditionner l'utilisation de cette option de ligne de commande à l'utilisation du mot de passe administrateur :

Lorsque l'accès au Panneau de Configuration (interface principale du logiciel) est protégée par mot de passe (appelé "mot de passe administrateur"), il est obligatoire d'ajouter ce mot de passe, en ligne de commande via l'option "/pwd", à toutes les commandes d'exportation : "/export", "/exportonce".

D'un point de vue sécurité, il est recommandé de privilégier l'option "/exportonce" à l'option "/export pour des opérations de maintenance, puisque le logiciel est quitté immédiatement après son exécution.

7 Manuel de référence

7.1 Options de ligne de commande de l'Installation du Client VPN

L'installeur (setup) du Client VPN TheGreenBow peut être configuré grâce à un jeu d'options de ligne de commande.

Règle de syntaxe

1/ Les options qui requièrent une valeur doivent être spécifiées sans espace entre l'option et sa valeur.

2/ Les valeurs qui contiennent des espaces (par exemple des répertoires) doivent être encadrées par des guillements

7.1.1 /S

Syntaxe : `/S` (S doit être en majuscule)
Usage : Configure l'installation en mode silencieux (aucun question ni alerte à l'utilisateur)
Exemple : `TheGreenBow_VPN_Client.exe /S`

7.1.2 /D

Syntaxe : `/D=[rep install]` (D doit être en majuscule)
Usage : `[rep install]` est le répertoire où le logiciel Client VPN doit être installé.
Exemple : `TheGreenBow_VPN_Client.exe /S /D=C:\mon repertoire\vpn`

Attention : [rep install] ne nécessite pas d'être encadré par des guillemets, même si le répertoire contient des espaces. En revanche, il est obligatoire que cette option soit la dernière de la ligne de commande.

Note : Le répertoire doit être indiqué en entier. Cette option ne prend pas en compte les répertoires relatifs (du type "`../../myrep`")

Par défaut, le répertoire d'installation du Client VPN est "C:\Program Files\TheGreenBow\TheGreenBow VPN".

7.1.3 --license

Syntaxe : `--license=[license_number]` ("license" est précédé de 2 tirets)
Usage : Permet de configurer le numéro de licence utilisé pour l'activation du logiciel. (Cf. "Guide Utilisateur du Client VPN TheGreenBow" pour les caractéristiques de ce numéro de licence).
Exemple : `TheGreenBow_VPN_Client.exe --license=1234567890ABCDEF12345678`

7.1.4 --activmail

Syntaxe : `--activmail=[activation_email]` ("activmail" est précédé de 2 tirets)
Usage : Permet de configurer l'adresse email utilisée pour l'activation du logiciel. (Cf. "Guide Utilisateur du Client VPN TheGreenBow" pour les caractéristiques de cette adresse email).
Exemple : `TheGreenBow_VPN_Client.exe --activmail=sales@company.com`

7.1.5 --autoactiv

Syntaxe : `--autoactiv=1` ("autoactiv" est précédé de 2 tirets)

Usage : Dans le cas d'une mise à jour (i-e : le numéro de licence et l'adresse email d'activation ont déjà été saisies au cours d'une précédente installation), le paramètre "`--autoactiv=1`" permet de configurer le logiciel pour s'activer automatiquement.

Exemple : `TheGreenBow_VPN_Client.exe --autoactiv=1`

7.1.6 --noactiv

Syntaxe : `--noactiv=1` ("noactiv" est précédé de 2 tirets)

Usage : Permet de ne pas afficher la fenêtre d'activation.
Cette option est typiquement associée à l'option "`--autoactiv=1`"

Exemple : `TheGreenBow_VPN_Client.exe --noactiv=1 --autoactiv=1`

7.1.7 --start

Syntaxe : `--start=[1|2]` ("start" est précédé de 2 tirets)

Usage : Permet de configurer le mode de démarrage du logiciel Client VPN :
1 : automatique après le logon Windows (enmême temps que l'ouverture de la session Windows)
2 : manuellement (p.ex. par double-clic sur l'icône de l'application)

Par défaut, le logiciel Client VPN démarre automatiquement à l'ouverture de la session Windows (mode 1)

Exemple : `TheGreenBow_VPN_Client.exe --start=2`

7.1.8 --reboot

Syntaxe : `--reboot=1` ("reboot" est précédé de 2 tirets)

Usage : Force le poste à redémarrer à la suite d'une l'installation silencieuse.
Lorsque cette option n'est pas spécifiée, l'installation silencieuse ne se termine pas par un redémarrage (reboot) du poste.

A noter : Cette option est particulièrement destinée aux postes Windows XP, pour lesquels l'installation du logiciel Client VPN nécessite un reboot. Elle n'est pas nécessaire pour les postes Windows Vista ou Windows 7 et OS supérieurs.

Exemple : `TheGreenBow_VPN_Client.exe --reboot=1`

7.1.9 --password

Syntaxe : `--password=[password]` ("password" est précédé de 2 tirets)

Usage : Permet de protéger par un mot de passe l'accès au Panneau de Configuration, et donc à la politique de sécurité VPN. Le mot de passe sera demandé lorsque l'utilisateur clique sur l'icône en barre des tâches, ou lorsqu'il passe du Panneau des Connexions au Panneau de Configuration.

Le mot de passe ne doit pas contenir d'espace.
La longueur maximale du mot de passe est de 14 caractères.

Exemple : `TheGreenBow_VPN_Client.exe --password=adm253q`

7.1.10 --guidefs

Syntaxe : `--guidefs=[full|user|hidden]` ("guidefs" est précédé de 2 tirets)

Usage : Permet de définir l'apparence du logiciel Client VPN lorsqu'il démarre.
"`full`" : Au démarrage, le Panneau de Configuration est affiché
"`user`" : Au démarrage, le Panneau des Connexions est affiché
"`hidden`" : Au démarrage, aucune Panneau n'est affiché, et le menu en barre des tâches est réduit aux deux items "Quitter" et "Console".

Par défaut, le Panneau de Configuration est affiché.

Exemple : `TheGreenBow_VPN_Client.exe --guidefs=hidden`

7.1.11 --menuitem

Syntaxe : `--menuitem=[0..31]` ("menuitem" est précédé de 2 tirets)
Usage : Permet de définir les items du menu en barre des tâches.
La valeur de menuitem est un champ de bit, chaque bit représente un item du menu en barre des tâches :
1 (1st bit) = Quitter,
2 (2nd bit) = Panneau des Connexions,
4 (3rd bit) = Console,
8 (4th bit) = Sauver et Appliquer (*obsolète à partir de la version 5*)
16 (5th bit) = Panneau de Configuration.

Par défaut, tous les items sont affichés : valeur = 31 (1F hexa).

Exemple : "`TheGreenBow_VPN_Client.exe --menuitem=3`" affichera seulement les items "Quitter" et "Panneau des Connexions".

Note 1 : Les tunnels VPN sont toujours affichés dans le menu en barre des tâches. Ils peuvent toujours être ouverts ou fermés depuis ce menu.

Note 2 : L'option "`--menuitem`" est prioritaire sur l'option "`--guidefs=hidden`".
L'option "`--guidefs=hidden` " réduit les items du menu en barre des tâches à "Quitter" et "Console".
Mais l'option "`--menuitem` " est prioritaire sur l'option "`--guidefs` ".
Ainsi, les deux options "`"--guidefs=hidden --menuitem=1`" auront pour effet de réduire le menu en barre des tâches à l'item "Quitter" uniquement.

7.1.12 --pkicheck

Voir le "Guide de Déploiement Options PKI" (tgbvpn_ug_deployment_pki_fr.pdf)

7.1.13 -- smartcardroaming

Voir le "Guide de Déploiement Options PKI" (tgbvpn_ug_deployment_pki_fr.pdf)

7.1.14 --lang

Syntaxe : `--lang=[language code]` ("lang" est précédé de 2 tirets)
Usage : Cette option spécifie la langue d'installation et d'utilisation du logiciel Client VPN.
Les langues disponibles sont énumérées ci-dessous.
Exemple : `TheGreenBow_VPN_Client.exe --lang=1040` démarrera le logiciel en italien.

Code	Langue	Nom français	Code ISO 639-2

1033 (default)	English	Anglais	EN
1036	Français	Français	FR
1034	Español	Espagnol	ES
2070	Português	Portugais	PT
1031	Deutsch	Allemand	DE
1043	Nederlands	Hollandais	NL
1040	Italiano	Italien	IT
2052	简化字	Chinois simplifié	ZH
1060	Slovenscina	Slovène	SL
1055	Türkçe	Turc	TR
1045	Polski	Polonais	PL
1032	ελληνικά	Grec	EL
1049	Русский	Russe	RU
1041	日本語	Japonais	JA
1035	Suomi	Finois	FI
2074	српски језик	Serbe	SR
1054	ภาษาไทย	Thai	TH
1025	عـربي	Arabe	AR
1081	हिन्दी	Hindi	HI
1030	Danske	Danois	DK
1029	Český	Tchèque	CZ
1038	Magyar nyelv	Hongrois	HU
1044	Bokmål	Norvégien	NO
1065	ىفـارس	Persan	FA
1042	한국어	Coréen	KO

7.2 Options de ligne de commande du logiciel Client VPN

Le Client VPN TheGreenBow offre en standard un jeu d'options de ligne de commande, utilisables dans des scripts ou dans des fichiers batch. Ces options permettent d'effectuer diverses opérations comme : ouvrir ou fermer un tunnel VPN, importer ou exporter une politique de sécurité VPN, etc…

La syntaxe des options de ligne de commande est toujours la même :

```
[répertoire]\vpnconf.exe [/option[:valeur]]
```

"répertoire" est le répertoire dans lequel se trouve l'exécutable "vpnconf.exe" (typiquement le répertoire d'installation du logiciel Client VPN)

Si la valeur contient des espaces (par exemple un répertoire), elle doit être encadrée par des guillemets.

7.2.1 /import

Syntaxe : `/import:[ConfigFileName]`
Usage : Permet d'importer une politique de sécurité VPN en démarrant le Client VPN.
[ConfigFileName] est le chemin complet du fichier à importer.

Il doit être encadré de guillemets s'il contient des espaces.

"`/import`" peut être utilisée avec "`/pwd`" pour importer une politique de sécurité VPN protégée par un mot de passe (voir "`/pwd`" ci-dessous et chapitre 6.4.1 concernant la protection de la politique de sécurité VPN)

Voir au chapitre 6.4 les différences avec les options "`/importonce`", "`/add`" et "`/replace`"

Exemple : `vpnconf.exe /import:"c:\my documents\myvpnconf.tgb"`
`vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd:gq1a`

7.2.2 /importonce

Syntaxe : `/importonce:[ConfigFileName]`
Usage : Permet d'importer une politique de sécurité VPN sans démarrer le Client VPN.
[ConfigFileName] est le chemin complet du fichier à importer.
Il doit être encadré de guillemets s'il contient des espaces.

"`/importonce`" peut être utilisée avec "`/pwd`" pour importer une politique de sécurité VPN protégée par un mot de passe (voir "`/pwd`" ci-dessous et chapitre 6.4.1 concernant la protection de la politique de sécurité VPN)

Voir au chapitre 6.4 les différences avec les options "`/import`", "`/add`" et "`/replace`"

Exemple : `vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb"`
`vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb" /pwd:gq1a`

7.2.3 /add

Syntaxe : `/add:[ConfigFileName]`
Usage : Permet d'ajouter une politique de sécurité VPN.
[ConfigFileName] est le chemin complet du fichier à importer.
Il doit être encadré de guillemets s'il contient des espaces.

"`/add`" peut être utilisée avec "`/pwd`" pour importer une politique de sécurité VPN protégée par un mot de passe (voir "`/pwd`" ci-dessous et chapitre 6.4.1 concernant la protection de la politique de sécurité VPN)

Voir au chapitre 6.4 les différences avec les options "`/import`", "`/importonce`" et "`/replace`"

Exemple : `vpnconf.exe /add:"c:\my documents\myvpnconf.tgb"`
`vpnconf.exe /add:"c:\my documents\myvpnconf.tgb" /pwd:gq1a`

7.2.4 /replace

Syntaxe : `/replace:[ConfigFileName]`
Usage : Permet de remplacer une politique de sécurité VPN.
[ConfigFileName] est le chemin complet du fichier à importer.
Il doit être encadré de guillemets s'il contient des espaces.

"/replace" peut être utilisée avec "/pwd" pour importer une politique de sécurité VPN protégée par un mot de passe (voir "/pwd" ci-dessous et chapitre 6.4.1 concernant la protection de la politique de sécurité VPN)

Voir au chapitre 6.4 les différences avec les options "/import", "/importonce" et "/add"

Exemple : `vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb"`
`vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb" /pwd:gq1a`

7.2.5 /export

Syntaxe : `/export:[ConfigFileName]`
Usage : Permet d'exporter une politique de sécurité VPN, en démarrant le logiciel Client VPN.
[ConfigFileName] est le chemin complet du fichier à importer.
Il doit être encadré de guillemets s'il contient des espaces.

"/export" peut être utilisée avec "/pwd" pour exporter une politique de sécurité VPN en la protégeant par un mot de passe (voir "/pwd" ci-dessous et chapitre 6.5.1 concernant la protection de la politique de sécurité VPN)

Voir ci-dessous la différence avec l'option "/exportonce"

Exemple : `vpnconf.exe /export:"c:\my documents\myvpnconf.tgb"`
`vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" /pwd:gq1a`

7.2.6 /exportonce

Syntaxe : `/exportonce:[ConfigFileName]`
Usage : Permet d'exporter une politique de sécurité VPN, sans démarrer le logiciel Client VPN.
[ConfigFileName] est le chemin complet du fichier à importer.
Il doit être encadré de guillemets s'il contient des espaces.

"/exportonce" peut être utilisée avec "/pwd" pour exporter une politique de sécurité VPN en la protégeant par un mot de passe (voir "/pwd" ci-dessous et chapitre 6.4.1 concernant la protection de la politique de sécurité VPN)

Voir ci-dessus la différence avec l'option "/export"

Exemple : `vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb"`
`vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb" /pwd:gq1a`

7.2.7 /pwd

Syntaxe : `/pwd:[Password]`
Usage : Permet de spécifier un mot de passe pour les opérations d'importation et d'exportation des politiques de sécurité VPN.
Cette option peut être utilisée avec les options : "/import", "/importonce", "/add", "/replace", "/export", "/exportonce".

voir chapitre 6.4.1 concernant la protection de la politique de sécurité VPN

Dans la ligne de commande, l'option "/pwd" doit être positionnée après les options d'importation ou d'exportation.

Exemple : `vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd:gq1a`

7.2.8 /stop

Syntaxe : `/stop`
Usage : Ferme tous les utnnels VPN ouverts, et arrête le logiciel Client VPN.
Exemple : `vpnconf.exe /stop`

7.2.9 /open

Syntaxe : `/open:[NomPhase1-NomPhase2]`
Usage : Permet d'ouvrir un tunnel VPN en ligne de commande.
Exemple : `vpnconf.exe /open:Corporate-gateway1`

7.2.10 /close

Syntaxe : `/close:[NomPhase1-NomPhase2]`
Usage : Permet de fermer, par ligne de commande, un tunnel VPN ouvert.
Exemple : `vpnconf.exe /close:"Home gateway-cnx1"` (les guillemets sont requis puisque le nom du tunnel contient des espaces).

8 Support

Informations et mises à jour sur le site web TheGreenBow : http://www.thegreenbow.com

Support technique par email à : support@thegreenbow.com
ou sur le site web TheGreenBow : http://www.thegreenbow.com/support.html

Contact commercial par email à : sales@thegreenbow.com

Secure, Strong, Simple.

TheGreenBow Security Software