THEGREENBOW

TheGreenBow VPN Certified

Guide Utilisateur

Table des Matières

1 Présentation

1.1 Le Client VPN TheGreenBow VPN Certified

TheGreenBow VPN Certified est le premier logiciel Client VPN IPsec certifié Critères Communs au niveau EAL3+, et qualifié au niveau standard.

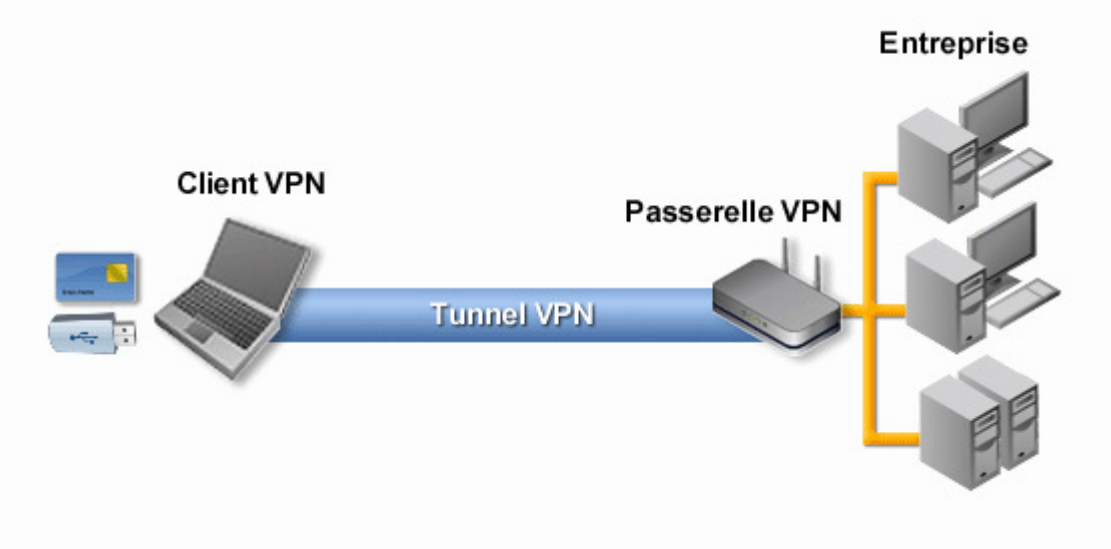
La Certification de cette version du Client VPN TheGreenBow apporte à l'utilisateur la garantie d'un produit hautement sécurisé, à la fiabilité éprouvée et à la qualité de production validée.

Le Client TheGreenBow VPN Certified apporte un haut niveau de sécurité dans l'établissement des tunnels VPN, dans la gestion des politiques de sécurité VPN, dans leur utilisation et leur exploitation : importation, exportation et déploiement.

1.2 Le Client VPN universel

Le Client VPN TheGreenBow est un logiciel Client VPN conçu pour tout poste de travail sous Windows, fixe ou nomade. Il permet d'établir une connexion sécurisée avec le Système d'Information de l'entreprise depuis n'importe quel endroit et en utilisant n'importe quel moyen de communication (Wi-Fi, 3G/4G, satellite, etc.).

Le Client VPN TheGreenBow permet d'ouvrir des connexions VPN avec toutes les passerelles VPN du marché.
La liste des passerelles qualifiées avec le Client VPN TheGreenBow est disponible sur le site TheGreenBow : http://www.thegreenbow.fr/vpn_gateway.html. Chaque passerelle est accompagnée de son guide de configuration.



Le Client VPN TheGreenBow est multi-protocoles VPN. Il permet d'ouvrir simultanément des connexions VPN IPsec en IKEv1, IKEv2 et des connexions VPN SSL. Toutes les connexions VPN peuvent être établies sur IPv4 ou IPv6.
Voir les recommandations de mise en œuvre pour le choix des protocoles à privilégier dans le cadre de l'utilisation du Client VPN Certified.

1.3 Utilisateurs du logiciel Client VPN TheGreenBow

Le logiciel Client VPN TheGreenBow est conçu pour être utilisé par deux types d'utilisateurs :

1.3.1 Utilisateur

L'utilisateur accède principalement à la seule fonction d'ouverture et de fermeture du tunnel.
Suivant le paramétrage du logiciel, il peut effectuer cette opération via le panneau de connexion ou via le menu contextuel associé à l'icône en barre des tâches.
Réciproquement, il est averti de l'état du tunnel VPN par l'apparence de l'icône VPN en barre des tâches.

Le paramétrage recommandé du Client VPN Certified consiste à limiter l'interface du logiciel accessible à l'utilisateur aux stricts menus dont il a besoin (Cf. recommandations des chapitres 23.1 et 23.2)

1.3.2 Administrateur

Comme décrit dans la Cible de sécurité du Client VPN Certified, le rôle de l'Administrateur regroupe les deux rôles d'Administrateur de sécurité et d'administrateur système et réseau.

Ainsi, l'Administrateur assume toutes les opérations de gestion du logiciel lui-même (installation, paramétrage du logiciel, mise à jour, désinstallation), et toutes les opérations de gestion de la politique de sécurité VPN (création, export, import, modification, diffusion). Toutes ces opérations sont regroupées dans le "Panneau de Configuration" du logiciel, dont l'accès en mode certifié doit être restreint à l'Administrateur (Cf. chapitre 25 "Recommandations de sécurité").

Le logiciel Client VPN Certified offre tous les moyens de paramétrage et de gestion de configuration décrits plus avant dans ce guide. Toutes ces opérations peuvent être restreintes à l'administrateur seul, et par la même être inaccessibles à l'utilisateur. (Cf. recommandations des chapitres 23.1 et 23.2).

1.4 Compatibilité totale avec les IGC / PKI

Fonctionnant sur tout type d'équipement Windows (ordinateur, tablette), Windows 10 inclus, et permettant d'établir une connexion sécurisée au travers de tout type de réseau, le Client VPN TheGreenBow s'intègre totalement dans toute IGC (Infrastructure de Gestion de Clés). Il apporte une souplesse inégalée dans la prise en compte des certificats et des cartes à puces ou tokens de toute nature.
TheGreenBow met à disposition sur son site la liste des tokens et cartes à puce qualifiés.

Le Client VPN TheGreenBow implémente en particulier :

- La détection automatique des cartes à puce et des tokens (en PKCS11 ou en CSP) ou du support de stockage des éléments de sécurité (fichier, magasin de certificats Windows)
- La configuration de tokens ou de lecteurs de cartes à la volée
- La prise en compte de certificats multi-formats (PKCS12, X509, PEM, etc.)
- La configuration multi-critères des certificats à utiliser (sujet, key usage, etc.)

Le Client VPN TheGreenBow apporte des fonctions de sécurité supplémentaires sur la gestion des PKI comme l'ouverture et la fermeture automatique du tunnel sur insertion et extraction de la carte à puce, ou encore la possibilité de configurer l'interface PKI et Carte à puce dans l'installeur du logiciel de façon à automatiser le déploiement.

En version "VPN Certified", l'utilisation de certificats issus d'une IGC de confiance, comme l'utilisation de supports de confiance pour ces certificats (token ou carte à puce), est recommandé. Cf. chapitre 25 "Recommandations de sécurité".

1.5 Sécurité des politiques VPN

Le Client VPN TheGreenBow apporte un haut niveau de sécurité dans la gestion et dans la prise en compte des politiques de sécurité VPN.

Le logiciel peut être configuré, dès son installation, pour restreindre totalement l'accès aux politiques de sécurité VPN à l'administrateur seul.

Le logiciel permet aussi de sécuriser au maximum l'utilisation des politiques de sécurité VPN, en conditionnant l'ouverture d'un tunnel aux divers mécanismes d'authentification disponibles : X-Auth, certificats, etc.

A noter : Le Client VPN TheGreenBow n'est pas conçu pour gérer des configurations multi-utilisateurs Windows simultanés. Pour des raisons de sécurité, ce cloisonnement des fonctions VPN entre plusieurs utilisateurs d'un même poste est renforcé dans la version certifiée (il est impossible de partager un tunnel entre plusieurs utilisateurs simultanés d'un même poste).

1.6 Fonctions inédites

Pour améliorer l'expérience utilisateur et pour faciliter son intégration et son déploiement, le Client VPN TheGreenBow implémente de nombreuses fonctions inédites :

- Interface utilisateur customisable (jusqu'à pouvoir être invisible)
- Mode USB permettant de conditionner l'ouverture du tunnel à l'insertion d'une clé USB VPN
- Pré-configuration exhaustive du logiciel avant son déploiement
- Ensemble d'options permettant le pilotage du logiciel en ligne de commande (par script)
- Sécurisation et automatisation de connexion RDP (remote sharing desktop)
- Possibilité d'associer des scripts à l'ouverture et à la fermeture du tunnel
- Mécanismes de stabilisation du tunnel VPN sur réseau instable

Note : Toutes ces fonctions sont proposées dans le logiciel VPN Certified à l'exception de la fonction "Mode USB".

1.7 Caractéristiques techniques

Le Client VPN TheGreenBow implémente la totalité des caractéristiques requises pour assurer la sécurisation fiable et maximale des connexions :

- Tunnel VPN sur tout type de média : Ethernet, Wi-Fi, 3G/4G, satellite, etc.
- Automatisme d'ouverture du tunnel (détection de trafic, automatique, etc.)
- Mode GINA (ouverture tunnel avant logon Windows)
- DPD et gestion de passerelle redondante (bascule automatique)
- Etablissement de tunnel VPN en mode point à passerelle ou point à point
- Mode "Bloquer les flux non chiffrés"
- Tunnels imbriqués
- IKEv1, IKEv2
- IPsec ou SSL
- IPV4 ou IPV6 pour le tunnel et le transport
- X-Auth, ConfigMode / Mode CP
- Pre-shared Key, Certificats X509 ou PKCS12
- Gestion des tokens et cartes à puce en PKCS11 ou CSP

Voir en annexe le détail des caractéristiques techniques du Client VPN TheGreenBow.

En version "VPN Certified", les algorithmes mis en œuvre doivent être conformes aux recommandations du RGS 2.0.
A ce titre, les protocoles et algorithmes suivants doivent être mis en œuvre :
- IKE V2 / IPsec
- Authentification par certificat
- Chiffrement IKE/IPsec : AES CBC 128/192/256 avec PRF et HMAC SHA2 256/384/512
- Groupes DH 15, 16, 17, 18 (supérieurs à DH14)
- Le mode "bloquer les flux non chiffrés" doit être sélectionné
- Le mode "tout le trafic dans le tunnel" doit être configuré

Ces recommandations sont détaillées au chapitre 25 "Recommandations de sécurité".

1.8 Conditions de mise en œuvre de TheGreenBow VPN Certified

Le Client TheGreenBow VPN Certified est certifié sur les plates-formes Windows 7 32/64bit et Windows 10 32/64bit.

Le logiciel installeur (ainsi que tous les binaires constitutifs) du Client TheGreenBow VPN Certified est signé par le certificat TheGreenBow. Ceci permet à l'installateur ou à l'utilisateur de vérifier à tout moment l'intégrité du programme d'installation.

Si le logiciel est corrompu, un message Windows d'alerte est affiché.
A tout moment, la conformité du logiciel peut être vérifiée en visualisant les propriétés du programme (clic droit sur le fichier exécutable), et en sélectionnant l'onglet "Signatures numériques".

A ce titre, la version du Client TheGreenBow VPN Certified objet de ce guide utilisateur est la version **6.52.006**.
Cette version peut être vérifiée par l'utilisateur dans la fenêtre "A propos..." du logiciel, Cf. chapitre 11.

Par ailleurs, un utilisateur du Client TheGreenBow VPN Certified peut être averti des vulnérabilités identifiées dans le logiciel dès lors qu'il s'inscrit à la newsletter TheGreenBow (sur le site web TheGreenBow).
Cette inscription est automatique pour les clients du logiciel, à savoir une personne ayant fourni son adresse email lors de l'achat du logiciel.

Important : Voir aussi les recommandations de mise en œuvre du Client VPN TheGreenBow.

2 Installation

2.1 Installation

L'installation du Client VPN TheGreenBow s'effectue en exécutant le programme téléchargeable sur le site web TheGreenBow :

TheGreenBow_VPN_Client.exe

L'installation est une procédure standard qui ne requiert aucune saisie de l'utilisateur.

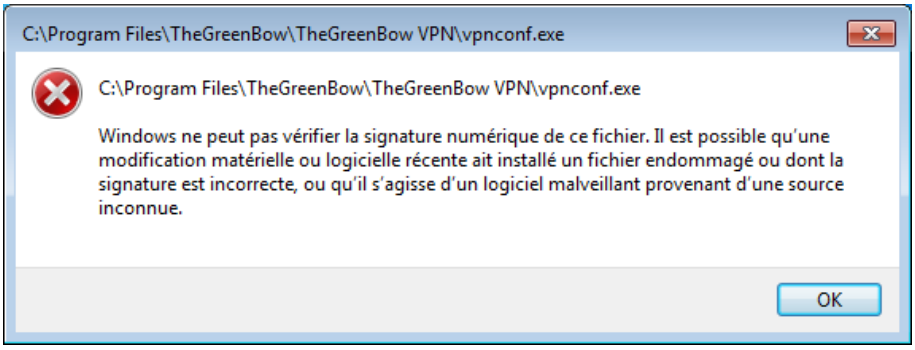
L'installation du logiciel est configurable, via un ensemble d'options de ligne de commande et de fichiers de configuration. Ces options et possibilités sont détaillées dans le document "Guide de Déploiement du Client VPN TheGreenBow" (tgbvpn_ug_deployment_fr.pdf) disponible sur le site TheGreenBow.

Note de sécurité : par défaut, le logiciel est installé protégé par le mot de passe administrateur : "admin". Il est fortement recommandé de modifier ce mot de passe dès l'installation terminée. Cf. chapitre 22 "Contrôle d'accès à la politique VPN".

2.1.1 Conditions d'installation

Le Client VPN TheGreenBow fonctionne sur différentes versions Windows. Les versions supportées sont détaillées dans les caractéristiques techniques du Client VPN TheGreenBow.
L'installation du logiciel sur Windows Vista, 7, 8 et 10 requiert d'être en mode administrateur.
Un avertissement est affiché à l'utilisateur si ce n'est pas le cas.

Le Client TheGreenBow VPN Certified implémente une vérification de son intégrité. Si le programme est corrompu, le logiciel ne s'exécute pas et l'utilisateur est averti par la fenêtre suivante :

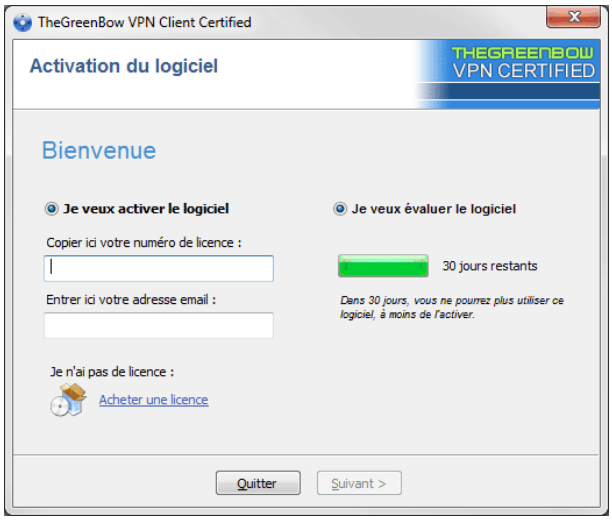


Note : La mise à jour ou l'installation d'un Client VPN Certifié en remplacement d'un Client VPN "Standard" ou "Premium" nécessite que ces Clients VPN soient désinstallés avant d'effectuer la mise à jour. Si la configuration VPN doit être conservée d'une version à l'autre, contacter le support TheGreenBow.

2.2 Période d'évaluation

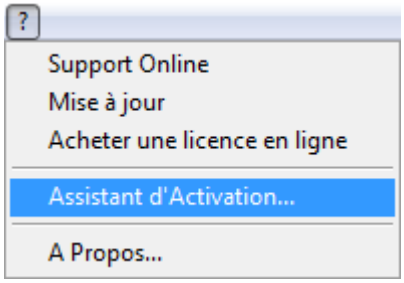
A la première installation sur un poste, le Client VPN est en période d'évaluation de 30 jours. Pendant cette période d'évaluation, le Client VPN est complètement opérationnel : toutes les fonctions sont disponibles.

Pendant la période d'évaluation, la fenêtre d'activation est affichée à chaque démarrage du logiciel. Elle indique le nombre de jours d'évaluation restants.



Sélectionner "Je veux évaluer le logiciel" puis cliquer sur "Suivant >" pour lancer le logiciel.
Pendant la période d'évaluation, la fenêtre "A propos…" affiche le nombre de jours d'évaluation restants.

Pendant la période d'évaluation, il est toujours possible d'accéder à la fenêtre d'activation depuis le logiciel, via le menu "? > Assistant d'activation" de l'interface principale (panneau de configuration).



3 Activation

Le Client VPN doit être activé pour fonctionner en dehors de la période d'évaluation.
La procédure d'activation est accessible soit à chaque lancement du logiciel, soit via le menu "? > Assistant d'activation" de l'interface principale.

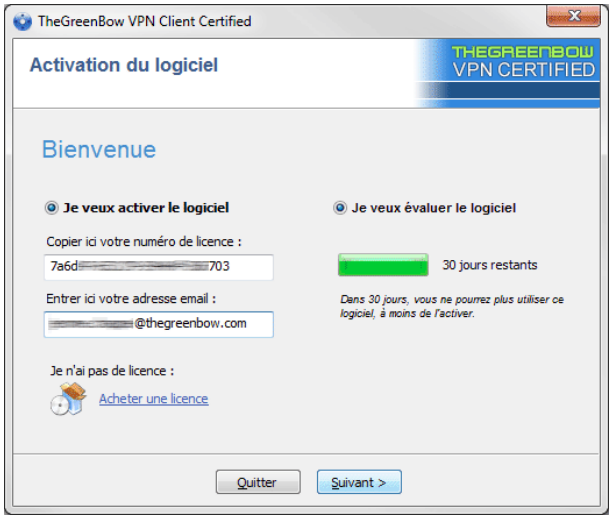
3.1 Etape 1

Entrer dans le champ "Copier ici votre numéro de licence :" le numéro de licence reçu par email.

Pour recevoir le numéro de licence, cliquer sur "Acheter une licence".

Le numéro de licence peut être copié-collé depuis l'email de confirmation d'achat directement dans le champ.
Le numéro de licence est uniquement composé de caractères [0…9] et [A..F], éventuellement regroupés par 6 et séparés par des tirets.

Entrer dans le champ "Entrer ici votre adresse email :" l'adresse email permettant d'identifier votre activation. Cette information permet de retrouver, en cas de perte, les informations sur votre activation.



3.2 Etape 2

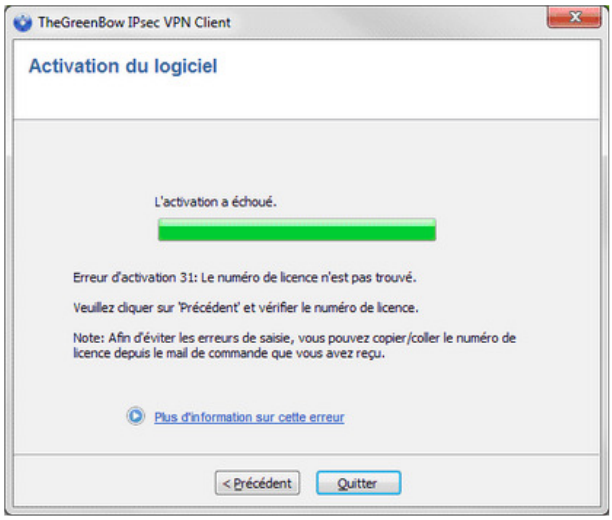
Cliquer sur "Suivant >", le processus d'activation en ligne s'exécute automatiquement.

Lorsque l'activation aboutit, cliquer sur "Démarrer" pour lancer le logiciel.

A noter : L'activation du logiciel est liée au poste sur lequel le logiciel est installé. Ainsi, un numéro de licence qui ne permet qu'une seule activation ne peut, une fois activé, être réutilisé sur un autre poste.
Réciproquement, l'activation de ce numéro de licence peut-être annulée en désinstallant le logiciel.

3.3 Erreur d'activation

L'activation du logiciel peut ne pas aboutir pour différentes raisons. Chaque erreur est indiquée sur la fenêtre d'activation. Elle est accompagnée le cas échéant par un lien qui permet d'obtenir des informations complémentaires, ou qui propose une opération permettant de résoudre le problème.



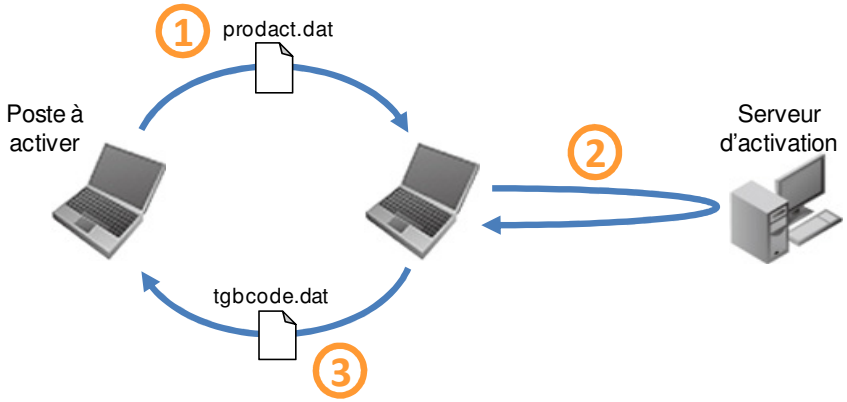
TheGreenBow indique sur son site web toutes les erreurs d'activation ainsi que les procédures de résolution des problèmes d'activation.

Les erreurs d'activation les plus courantes sont les suivantes :

N°	Signification	Résolution
31	Le numéro de licence n'est pas correct	Vérifier le numéro de licence
33	Le numéro de licence est déjà activé sur un autre poste	Désinstaller le poste sur lequel a été activée la licence, ou contacter l'équipe commerciale TheGreenBow
53 54	La communication avec le serveur d'activation est impossible	Vérifier que le poste est bien connecté à Internet Vérifier que la communication n'est pas filtrée par un firewall pour par un proxy. Le cas échéant, configurer le firewall pour laisser passer la communication, ou le proxy pour la rediriger correctement.

3.4 Activation manuelle

Lorsque l'activation échoue à cause d'un problème de communication avec le serveur d'activation, il est toujours possible d'activer manuellement le logiciel sur le site web TheGreenBow. La procédure est la suivante :



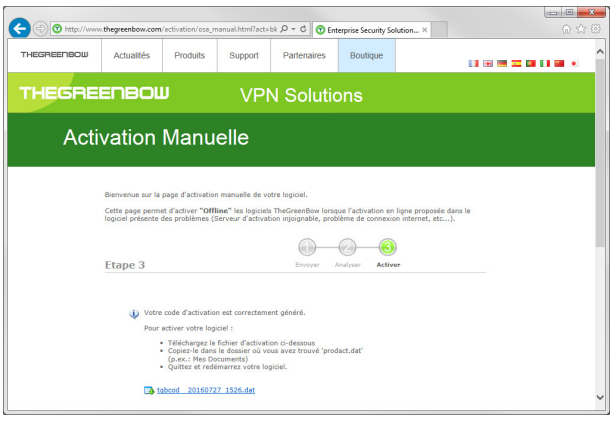
1	Fichier "prodact.dat"	Sur le poste à activer, récupérer le fichier "prodact.dat" situé dans le répertoire Windows "Mes Documents". (1)
2	Activation	Sur un poste connecté au serveur d'activation (2), ouvrir la page d'activation manuelle (3), y poster le fichier prodact.dat et récupérer le fichier tgbcode créé automatiquement par le serveur.
3	Fichier "tgbcode"	Copier ce fichier "tgbcode" dans le répertoire Windows "Mes documents" du poste à activer. Lancer le logiciel : il est activé.

(1) Le fichier "prodact.dat" est un fichier texte qui contient les éléments du poste utilisés pour l'activation. Si ce fichier n'existe pas dans le répertoire "Mes documents", effectuer sur le poste une activation : même si elle échoue, elle a pour effet de créer ce fichier.
(2) Le serveur d'activation est le serveur TheGreenBow, accessible sur Internet.
(3) Cf. procédure détaillée ci-dessous

3.4.1 Activation manuelle sur le serveur d'activation TheGreenBow

Sur un poste ayant une connexion au site web TheGreenBow ouvrir la page web suivante :
http://www.thegreenbow.com/activation/osa_manual.html?lang=fr

Cliquer sur le bouton "Parcourir" et ouvrir le fichier "prodact.dat" créé sur le poste à activer.
Cliquer sur "Envoyer". Le serveur d'activation vérifie la validité des informations du fichier prodact.dat.
Cliquer sur "Effectuer".
Le serveur d'activation présente en téléchargement le fichier contenant le code d'activation destiné au poste à activer.

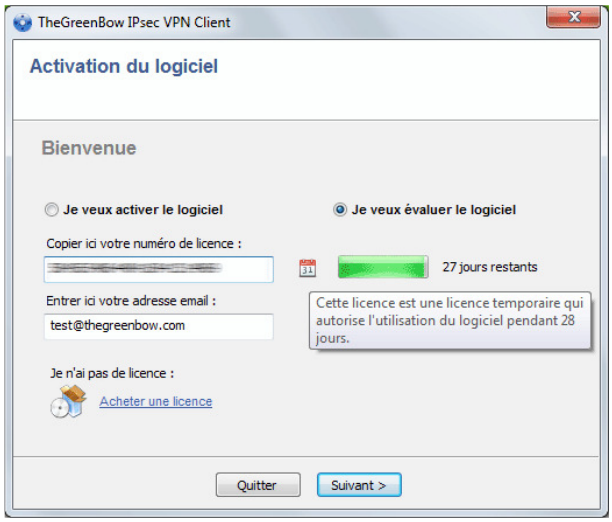


Ce fichier a un nom de la forme : tgbcod_*[date]*_*[code]*.dat (par exemple : tgbcod__20120625_1029.dat)

3.5 Licence temporaire

Il est possible d'acquérir auprès de TheGreenBow des licences d'évaluation, dites licences temporaires, par exemple pour poursuivre des sessions de tests au-delà de la période d'évaluation standard.
Pour obtenir une licence temporaire, contacter le service commercial par mail : sales@thegreenbow.com

Pendant l'utilisation d'une licence temporaire, la fenêtre d'activation est toujours affichée au démarrage du logiciel. Un icône identifie que la licence est temporaire, et le nombre de jours restants est affiché.



Pour lancer le logiciel, cliquer sur "Suivant >"

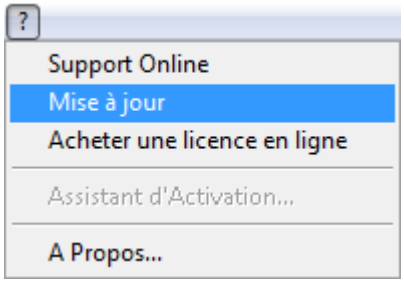
A la fin de la période de validité de la licence temporaire, le logiciel doit être activé par une licence définitive pour fonctionner.

3.6 Licence et logiciel activé

Lorsque le logiciel est activé, la licence et l'email utilisés pour l'activation sont consultables dans la fenêtre "A propos…" du logiciel. Cf. chapitre Fenêtre "A propos…"

4 Mise à jour

Le logiciel permet de vérifier à tout moment si une mise à jour est disponible, via le menu de l'interface principale : " ? > Mise à jour "



Ce menu ouvre la page web de vérification de mise à jour, qui indique si une mise à jour est disponible et activable, suivant le type de licence achetée, et suivant le type de maintenance ou d'abonnement souscrit.

Exemple :

4.1 Comment obtenir une mise à jour

L'obtention d'une mise à jour du logiciel suit les règles suivantes :

En cours de période de maintenance (1)	Je peux installer toute mise à jour
Hors période de maintenance, ou sans maintenance	Je peux installer les mises à jour mineures (2)
En cours d'abonnement (3)	Je peux installer toute mise à jour

(1) La période de maintenance démarre à la première activation du logiciel.
(2) Les versions mineures (ou mises à jour de maintenance) sont identifiées par le dernier chiffre de la version : par exemple le "2" de "6.12".
(3) Pour les versions VPN premium ou VPN Certifié

Exemple :
J'ai activé le logiciel en version 6.12. Ma période de maintenance a expiré.

Sont autorisées toutes les mises à jour des versions 6.13 à 6.19.
Sont refusées les mises à jour des versions 6.20 et supérieures.

4.2 Mise à jour de la politique de sécurité VPN

Au cours d'une mise à jour, la politique de sécurité VPN (configuration VPN) est automatiquement sauvegardée et restaurée.

A noter : Si l'accès à la politique de sécurité VPN est verrouillé par mot de passe, ce mot de passe est demandé au cours de la mise à jour, pour autoriser la restauration de la configuration.

4.3 Automatisation

L'exécution d'une mise à jour est configurable, en utilisant une liste d'options de ligne de commande, ou en utilisant un fichier d'initialisation. Ces options sont décrites dans le document "Guide de Déploiement" (tgbvpn_ug_deployment_fr.pdf).

5 Désinstallation

Pour désinstaller le Client VPN TheGreenBow :
1/ ouvrir le panneau de contrôle Windows
2/ sélectionner "Ajout/Suppression de programmes"

Ou

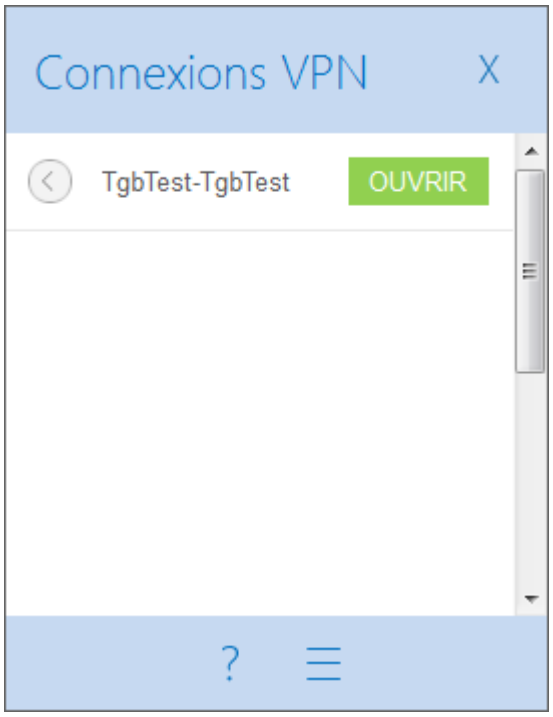
1/ Ouvrir le menu Windows "Démarrer"
2/ Sélectionner "Programmes > TheGreenBow > TheGreenBow VPN > Désinstaller le Client VPN"

6 Utilisation rapide

6.1 Ouvrir un tunnel VPN

Le Client VPN TheGreenBow est fourni en standard avec une politique de sécurité VPN contenant un tunnel VPN de test : TgbTest IKEv2/IPv4.

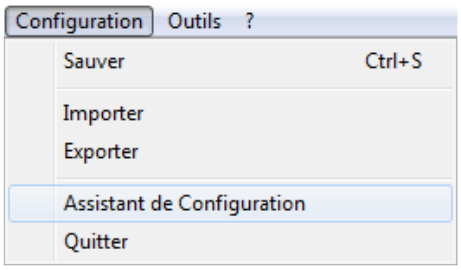
Lancer le Client VPN.
Dans le panneau des connexions, cliquer sur le bouton "OUVRIR" du premier tunnel "TgbTest"
Ou dans le panneau de configuration, double-cliquer sur le tunnel "TgbTest" dans l'arborescence



Le tunnel s'ouvre et le site web de test TheGreenBow est affiché automatiquement.

6.2 Configurer un tunnel VPN

Dans l'interface principale, ouvrir l'assistant de configuration VPN : "Configuration > Assistant de Configuration"



Utiliser l'assistant comme décrit au chapitre Assistant de Configuration ci-dessous.

Pour parfaire ou affiner la configuration VPN, vous trouverez sur le site web TheGreenBow un grand nombre de guides de configuration disponibles pour la plupart des passerelles VPN : http://www.thegreenbow.com/vpn/vpn_gateway.html

6.3 Automatiser l'ouverture du tunnel VPN

Le Client VPN TheGreenBow permet d'automatiser l'ouverture d'un tunnel VPN de différentes façons :

1/ Un tunnel VPN peut s'ouvrir automatiquement sur détection de trafic à destination du réseau distant. Cf. chapitre "IPsec Avancé"

2/ Un tunnel peut s'ouvrir automatiquement sur ouverture (double-clic) d'une politique de sécurité VPN (fichier .tgb). Cf. chapitre "IPsec Avancé"

3/ Un tunnel VPN peut s'ouvrir automatiquement sur insertion d'une clé USB contenant la politique de sécurité VPN adéquate. Cf. chapitre "Mode USB"

4/ Un tunnel VPN peut s'ouvrir automatiquement sur insertion de la Carte à Puce (ou du Token) contenant le certificat utilisé pour ce tunnel. Cf. chapitre "Utiliser un tunnel VPN avec un Certificat sur Carte à puce"

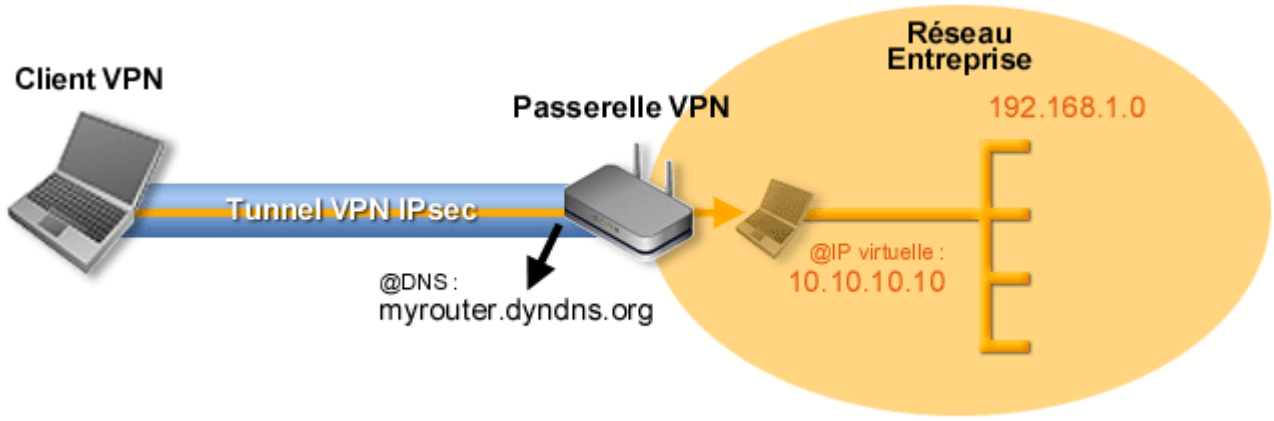
Note : Dans la version "VPN Certified" les modes 2/ et 3/ sont désactivés.

7 Assistant de configuration

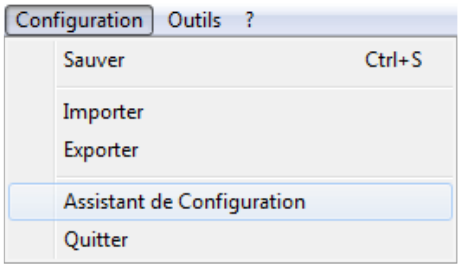
L'assistant de configuration du Client VPN TheGreenBow permet de configurer un tunnel VPN en 3 étapes simples.

L'utilisation de l'assistant de configuration est illustrée par l'exemple suivant :

- Le tunnel est ouvert entre un poste et une passerelle VPN dont l'adresse DNS est "myrouter.dyndns.org"
- Le réseau local de l'entreprise est 192.168.1.0 (il contient par exemple des machines dont l'adresse IP est 192.168.1.3, 192.168.1.4, etc.)
- Une fois le tunnel ouvert, le poste distant aura comme adresse IP dans le réseau de l'entreprise : 10.10.10.10

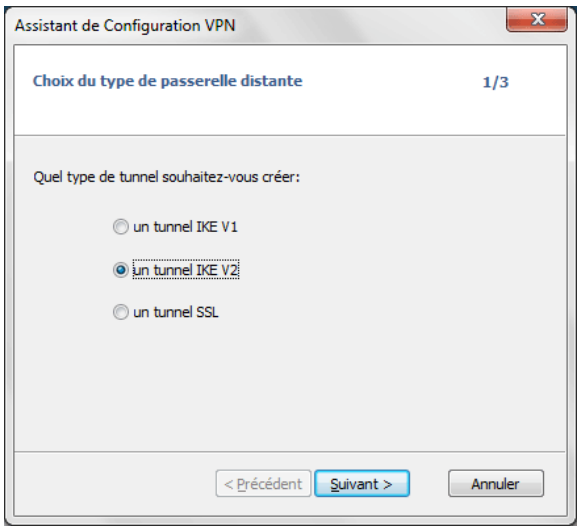


Dans l'interface principale, ouvrir l'assistant de configuration VPN : "Configuration > Assistant de Configuration"



Etape 1 :

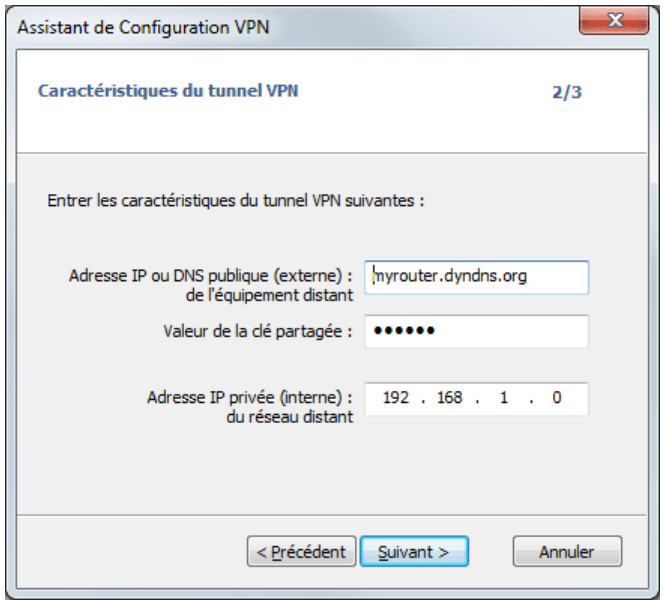
Choisir le protocole VPN à utiliser pour le tunnel : IKEv1, IKEv2 ou SSL.



Etape 2 pour un tunnel VPN IKEv1 :

Entrer les valeurs suivantes :

- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (exemple : myrouter.dyndns.org)
- Une clé partagée ("pre-shared key") qui doit être configurée de façon identique sur la passerelle.
- L'adresse IP du réseau de l'entreprise (exemple : 192.168.1.0). (1)

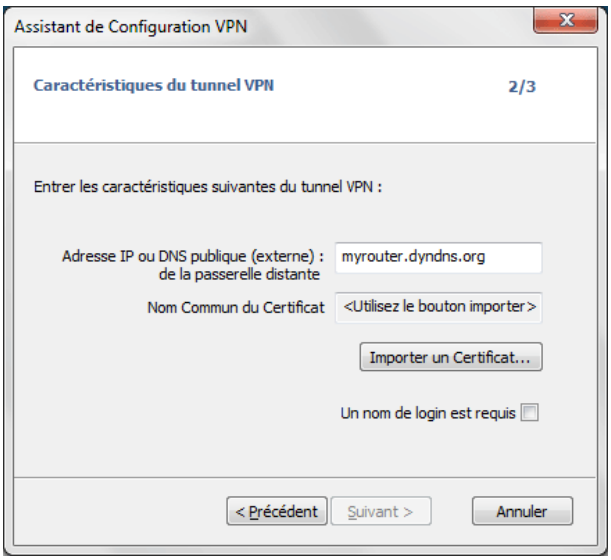


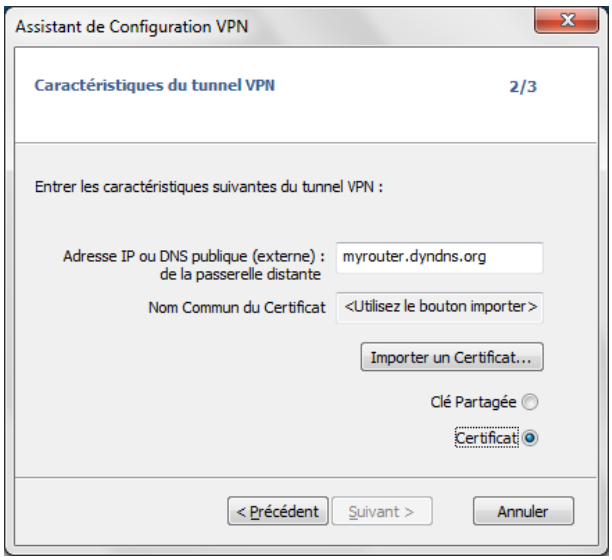
(1) Par défaut, l'adresse du réseau distant est exploitée avec une longueur de préfixe de 24. Cette valeur peut être modifiée ultérieurement.

Etape 2 pour un tunnel VPN IKEv2 :

Entrer les valeurs suivantes :

- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (exemple : myrouter.dyndns.org)
- Une clé partagée ("pre-shared key") qui doit être configurée de façon identique sur la passerelle
- OU Un certificat qui doit être importé grâce au bouton "Importer un Certificat…" (voir chapitre "Importer un certificat")

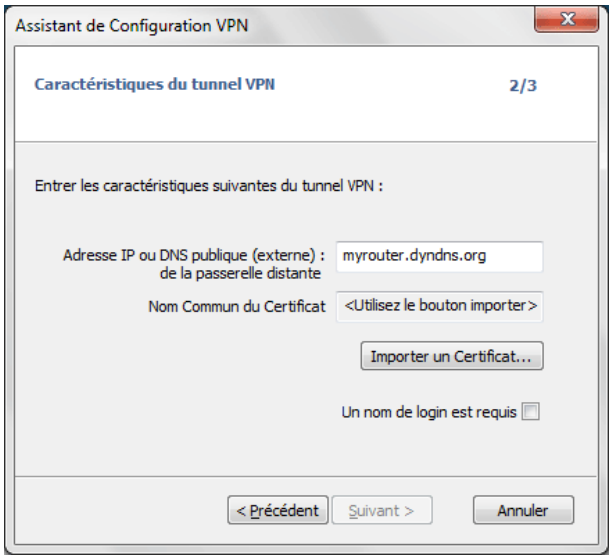




Etape 2 pour un tunnel SSL (OpenVPN) :

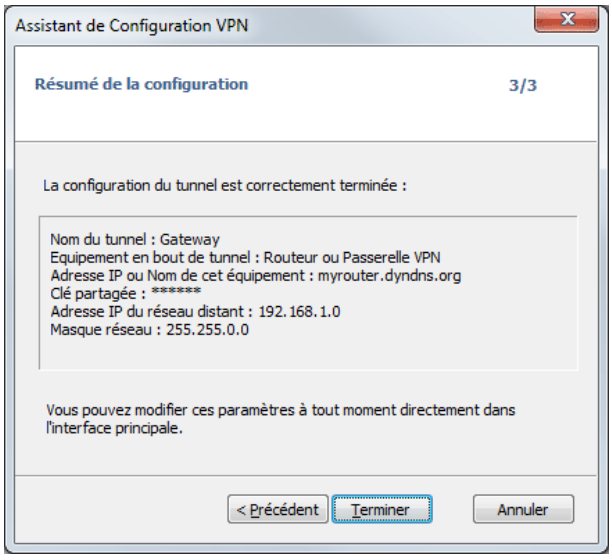
Entrer les valeurs suivantes :

- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (exemple : myrouter.dyndns.org)
- Un certificat qui doit être importé grâce au bouton "Importer un Certificat..." (voir chapitre "Importer un certificat")



Etape 3 :

Vérifier dans la fenêtre de résumé que la configuration est correcte et cliquer sur "Terminer".



Le tunnel qui vient d'être configuré apparaît dans l'arborescence des tunnels de l'interface principale.
Double-cliquer sur le tunnel pour l'ouvrir, ou affiner la configuration via les onglets de l'interface principale.

Pour toute configuration plus complexe, ou pour tout complément d'information concernant la configuration des passerelles VPN, consulter notre site : http://www.thegreenbow.com/vpn

Recommandation de sécurité : Dans le cadre d'une utilisation du Client VPN en mode certifié, il est recommandé de configurer des tunnels IKEv2 avec certificat. Cf. chapitre "Recommandations de sécurité"

8 Interface utilisateur

8.1 Interface utilisateur

L'interface utilisateur du Client VPN permet :
1/ de configurer le logiciel lui-même (mode de démarrage, langue, contrôle d'accès, etc.),
2/ de gérer les politiques de sécurité VPN (configuration des tunnels VPN, gestion des certificats, importation, exportation, etc.)
3/ d'utiliser les tunnels VPN (ouverture, fermeture, identification des incidents, etc.)

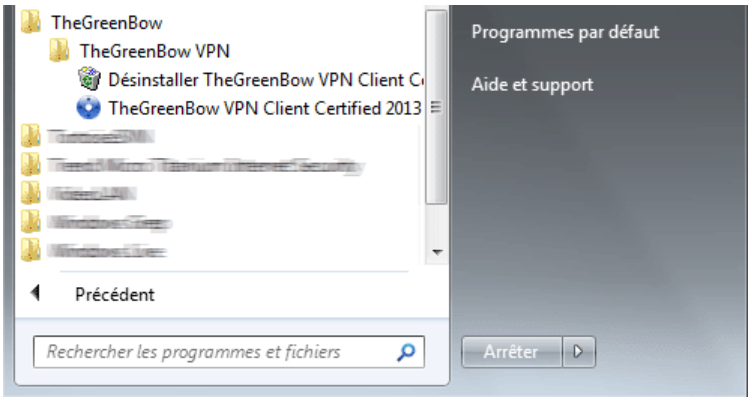
L'interface utilisateur se répartit en :
- Les éléments du logiciel disponibles sur le bureau Windows (icônes sur le bureau, menu démarrer)
- Un icône en barre des tâches et son menu associé
- Le Panneau des Connexions (liste des tunnels VPN à ouvrir)
- Le Panneau de Configuration (configuration de la politique de sécurité VPN et du logiciel)

Le Panneau de Configuration est composé des éléments suivants :
- Un ensemble de menus de gestion du logiciel et des politiques de sécurité VPN
- L'arborescence des tunnels VPN
- Des onglets de configuration des tunnels VPN
- Une barre d'état

8.2 Bureau Windows

8.2.1 Menu Démarrer

A l'issue de l'installation, le Client VPN peut être lancé depuis le menu démarrer Windows.
Deux liens sont créés dans le répertoire TheGreenBow / TheGreenBow VPN du menu démarrer :
1/ Lancement du Client VPN TheGreenBow
2/ Désinstallation du Client VPN TheGreenBow



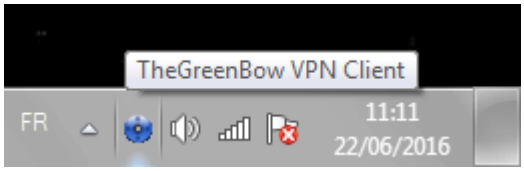
8.2.2 Bureau

Au cours de l'installation du logiciel, l'icône de l'application est créé sur le bureau Windows.
Le Client VPN peut être lancé directement en double-cliquant sur cet icône.

8.3 Barre des tâches

8.3.1 Icône

En utilisation courante, le Client VPN TheGreenBow est identifié par un icône situé en barre des tâches.



L'icône change de couleur si un tunnel VPN est ouvert :

Icône bleu : aucun tunnel VPN n'est ouvert

Icône vert : au moins un tunnel VPN est ouvert

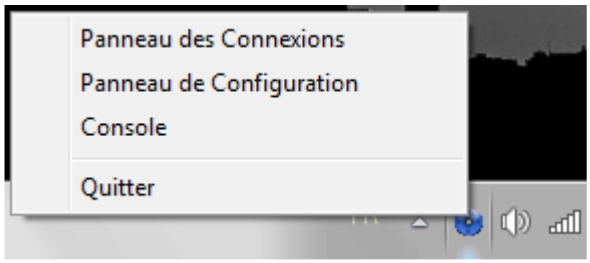
Le "tooltip" de l'icône du Client VPN indique à tout moment l'état du logiciel :
- "VPN Tunnel ouvert" si un ou plusieurs tunnels sont ouverts.
- "Attente VPN prêt..." pendant le temps de lancement du moteur VPN IKE.
- "TheGreenBow VPN Client Certified" lorsque le Client VPN est lancé, sans tunnel ouvert.

Un clic gauche sur l'icône ouvre le panneau des connexions.

Un clic droit sur l'icône affiche le menu contextuel associé à l'icône.

8.3.2 Menu

Un clic droit sur l'icône du Client VPN en barre des tâches affiche le menu contextuel associé à l'icône :

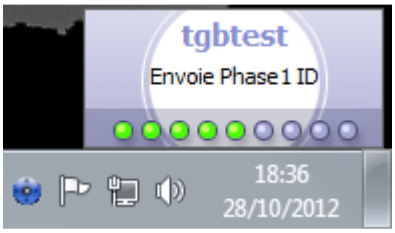


Les items du menu contextuel sont les suivants :
1/ Panneau des Connexions : ouvre le Panneau des Connexions
2/ Panneau de Configuration : ouvre le Panneau de Configuration
3/ Console : ouvre la fenêtre des traces VPN
4/ Quitter : Ferme les tunnels VPN ouverts et quitte le logiciel.

8.3.3 Popup glissante

Au moment de l'ouverture ou de la fermeture d'un tunnel VPN, une fenêtre glissante apparaît au dessus de l'icône du Client VPN en barre des tâches. Cette fenêtre identifie l'état du tunnel au cours de son ouverture ou de sa fermeture, et disparaît automatiquement, à moins que la souris ne soit dessus :

Tunnel en cours d'ouverture



Tunnel ouvert

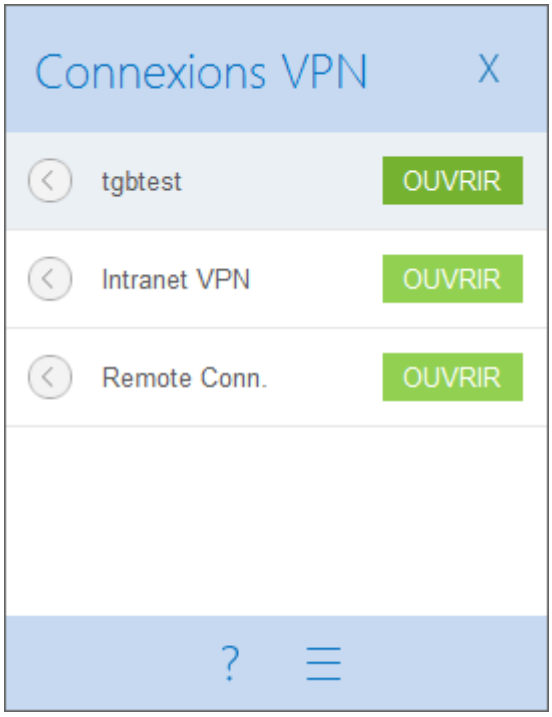
Tunnel fermé

Incident d'ouverture du tunnel : la fenêtre affiche l'explication succincte de l'incident, et un lien cliquable vers plus d'informations sur cet incident.

Note : L'affichage de la fenêtre glissante peut être désactivé, dans le menu "Outils > Options", onglet "Affichage", option "Ne pas afficher la popup de barre des tâches".

9 Panneau des Connexions

Le Panneau des Connexions permet d'ouvrir et de fermer simplement les connexions VPN configurées :



Nouveau : Depuis la version 6.4, le panneau de connexions est configurable : Il est possible de choisir les connexions VPN qui doivent y apparaître. Il est possible de renommer ces connexions VPN et de les ordonner.
Voir le chapitre "Gestion du panneau des connexions".

Pour ouvrir une connexion VPN, cliquer sur le bouton "OUVRIR" associé.
L'icône à gauche de la connexion indique les différents états de cette connexion :

- Connexion fermée. Un clic sur cet icône ouvre la configuration de la connexion dans le panneau de configuration.
- Connexion en cours d'ouverture ou de fermeture
- Connexion ouverte. Le trafic dans la connexion est représenté par une variation de l'intensité lumineuse du disque central.
- Connexion ayant eu un incident d'ouverture ou de fermeture. Un clic sur l'icône d'alerte ouvre une fenêtre popup qui fournit des informations détaillées ou complémentaires sur le problème rencontré.

Les boutons du panneau de connexion permettent respectivement de :

- Ouvrir la fenêtre "A propos…".
- Ouvrir le panneau de configuration (Note : L'accès au Panneau de Configuration peut être protégé par un mot de passe. Voir le chapitre "Contrôle d'accès à la politique de sécurité VPN")
- Fermer le panneau des connexions

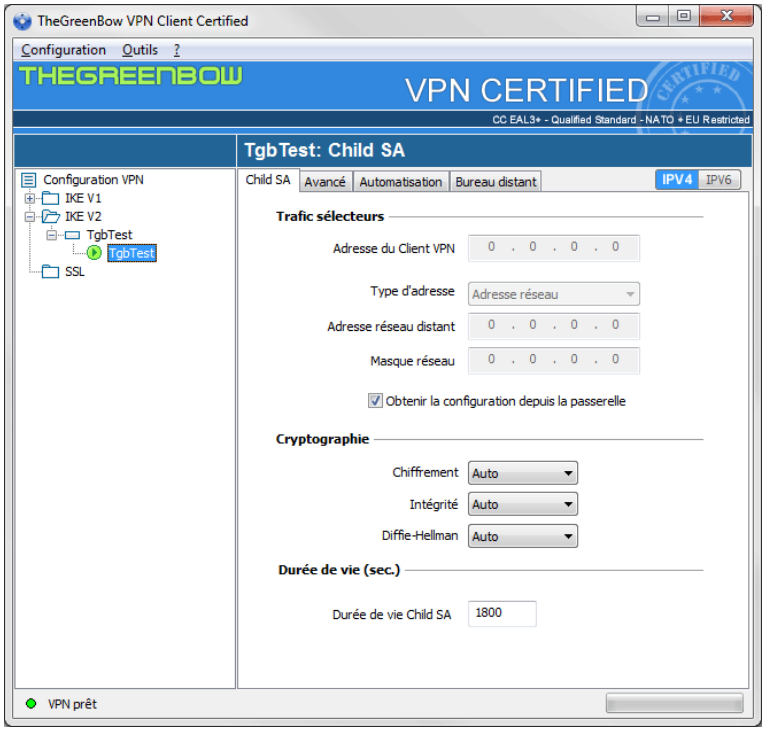
Sur le panneau des connexions, les raccourcis claviers suivants sont disponibles :

- ESC (ou ALT+F4) ferme la fenêtre
- CTRL+ENTER ouvre le panneau de configuration (interface principale)
- CTRL+O ouvre la connexion VPN sélectionnée
- CTRL+W ferme la connexion VPN sélectionnée
- Les flèches haut / bas permettent de se déplacer parmi les connexions VPN

10 Panneau de Configuration

Le panneau de Configuration est l'interface principale du Client VPN TheGreenBow.

Il est composé des éléments suivants :
- Un ensemble de menus permettant la gestion du logiciel et des politiques de sécurité VPN
- L'arborescence des tunnels VPN
- Des onglets de configuration des tunnels VPN
- Une barre d'état



10.1 Menus

Les menus du panneau de configuration sont les suivants :

- Configuration
  - Importer : Importation d'une politique de sécurité VPN (Configuration VPN)
  - Exporter : Exportation d'une politique de sécurité VPN (Configuration VPN)
  - Assistant de Configuration
  - Quitter : Fermer les tunnels VPN ouverts et quitter le logiciel

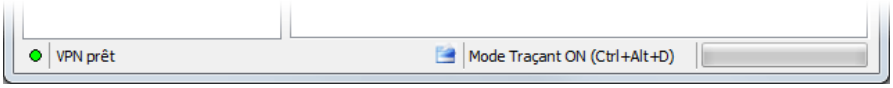
- Outils
  - Panneau des Connexions
  - Gestion du panneau des connexions
  - Console : Fenêtre de traces des connexions IKE
  - Reset IKE : Redémarrage du service IKE
  - Options : Options de protection, d'affichage, de démarrage, gestion de la langue, gestion des options IGC/PKI

- ?
  - Support Online : Accès au support en ligne
  - Mise à jour : Vérification de la disponibilité d'une mise à jour

- Acheter une licence en ligne : Accès à la boutique en ligne
- Assistant d'activation
- A propos…

10.2 Barre d'état

La barre d'état en bas de l'interface principale fournit plusieurs informations :



- La "led" à l'extrémité gauche est verte lorsque tous les services du logiciel sont opérationnels (service IKE)
- Le texte à gauche indique l'état du logiciel ("VPN prêt", "Sauve configuration", "Applique Configuration", etc.)
- Lorsqu'il est activé, le mode traçant est identifié au milieu de la barre d'état.
  L'icône à sa gauche est un icône cliquable qui ouvre le dossier contenant les fichiers de logs générés par le mode traçant.
- La barre de progression à droite de la barre d'état identifie la progression de la sauvegarde d'une Configuration.

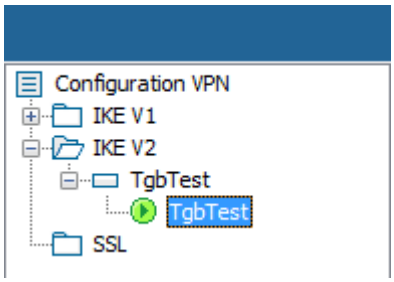
10.3 Raccourcis

CTRL+S	Sauvegarde de la configuration VPN
CTRL+ENTER	Permet de basculer sur le Panneau des Connexions
CTRL+D	Ouvre la fenêtre "Console" de traces VPN
CTRL+ALT+R	Redémarrage du service IKE
CTRL+ALT+T	Activation du mode traçant (génération de logs)

10.4 Arborescence des tunnels VPN

10.4.1 Utilisation

La partie gauche du Panneau de Configuration est la représentation sous forme d'arborescence de la politique de sécurité VPN. L'arborescence peut contenir un nombre illimité de tunnels.



Sous la racine "Configuration VPN", 3 niveaux permettent de créer respectivement

- Des tunnels IPsec IKEv1, caractérisés par une Phase 1 et une Phase 2, chaque phase1 pouvant contenir plusieurs phases 2.
- Des tunnels IPsec IKEv2, caractérisés par une IKE Authentication et une ChildSA, chaque IKE Authentication pouvant contenir plusieurs Child SA
- Des tunnels SSL/ TLS

Un clic sur une phase1, phase2, IKE Auth, Child SA ou TLS ouvre dans la partie droite du panneau de configuration les onglets de configuration associés. Voir dans les chapitres suivants :

1. Tunnel VPN IPsec IKEv1
   Configure IPsec IKEv1: Authentication
   Configure IPsec IKEv1: IPsec

2. Tunnel VPN IPsec IKEv2
   Configure IPsec IKev2: IKE Authentication
   Configure IPsec IKEv2: Child SA

3. Tunnel VPN SSL
   Configure SSL: TLS connection

Un icône est associé à chaque tunnel (Phase2, ChildSA ou TLS). Cet icône identifie le statut du tunnel VPN :

- Tunnel fermé
- Tunnel configuré pour s'ouvrir automatiquement sur détection de trafic
- Tunnel en cours d'ouverture
- Tunnel ouvert
- Incident d'ouverture ou de fermeture du tunnel

En cliquant successivement deux fois – sans faire de double-clic - sur un item de l'arborescence, il est possible d'éditer et de modifier le nom de cet item.

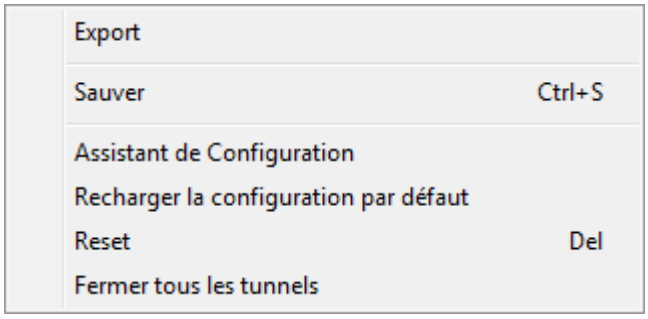
A noter : Deux items de l'arborescence ne peuvent avoir le même nom. Si l'utilisateur saisit un nom déjà attribué, le logiciel l'en avertit.

Toute modification non sauvegardée de la Configuration VPN est identifiée par le passage en caractères gras de l'item modifié. L'arborescence repasse en caractères normaux dès qu'elle est sauvegardée.

10.4.2 Menus contextuels

1. Configuration VPN

Un clic droit sur la Configuration VPN (racine de l'arborescence) affiche le menu contextuel suivant :



Export	Permet d'exporter la politique de sécurité VPN complète.

Sauver	Permet de sauvegarder la politique de sécurité VPN.
Assistant de Configuration	Ouvre l'Assistant de Configuration VPN
Recharger la configuration par défaut	Le Client VPN TheGreenBow est installé avec une Configuration par défaut qui permet de tester l'ouverture d'un tunnel VPN. Ce menu permet de la recharger à tout moment.
Reset	Remise à zéro, moyennant confirmation de l'utilisateur, de la politique de sécurité VPN.
Fermer tous les tunnels	Fermeture de tous les tunnels ouverts.

2. IKEv1, IKEv2, SSL

Un clic droit sur les items IKEv1, IKEv2 ou SSL affiche le menu contextuel suivant, qui permet d'exporter, de sauvegarder, de créer ou de coller une Phase1/IKE Auth/SSL :

Menu IKEv1

Menu IKEv2

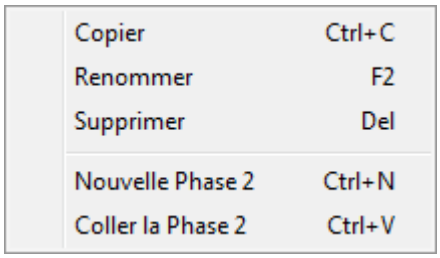
Menu SSL

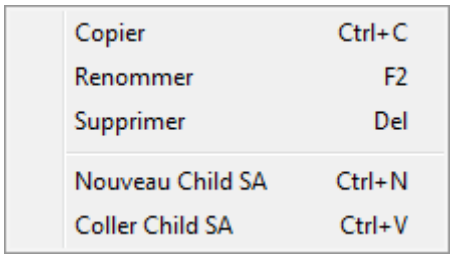
Export	Permet d'exporter tous les tunnels IKEv1 (resp. tous les tunnels IKEv2)
Sauver	Permet de sauvegarder tous les tunnels IKEv1 (resp. tous les tunnels IKEv2)
Nouvelle Phase 1 Nouvelle IKE AUth Nouveau TLS	Permet de créer une nouvelle Phase 1 / IKE Auth / TLS. Les paramètres de cette nouvelle Phase1/ IKE AUth / TLS sont renseignés avec des valeurs par défaut.
Coller la Phase1 Coller IKE Auth Coller TLS	Ajoute une Phase1 / IKE Auth / TLS copiée précédemment dans le clipboard.

(1) Ce choix apparaît lorsqu'une Phase1 / IKE Auth / TLS a été copiée dans le clipboard via le menu contextuel associé à cette Phase1/ IKE Auth / TLS (Cf ci-après).

3. Phase1 ou IKE Auth

Un clic droit sur une Phase1 ou IKE Auth affiche le menu contextuel suivant :





Copier	Copie la Phase1 ou la IKE Auth sélectionnée dans le "clipboard".
Renommer (1)	Permet de renommer la Phase1 / IKE Auth.
Supprimer (1)	Supprime, moyennant confirmation de l'utilisateur, la Phase1 ou IKE Auth, incluant toutes les Phases2 (respectivement toutes les ChildSA) associées.
Nouvelle Phase2 Nouvelle Child SA	Ajoute une nouvelle Phase 2 / ChildSA à la Phase1 / IKE Auth sélectionnée.
Coller la Phase2 (2) Coller Child SA	A joute à la Phase1 / IKE Auth la Phase2 / ChildSA copiée dans le clipboard.

(1) Ce menu est désactivé tant qu'un des tunnels de la Phase1/IKE Auth concernée est ouvert.
(2) Ce choix apparaît lorsqu'une Phase2 / ChildSA a été copiée dans le clipboard via le menu contextuel associé à la Phase2 / ChildSA concernée (Cf ci-après)

3. Phase2, ChildSA ou TLS

Un clic droit sur une Phase2, une Child SA ou une TLS affiche le menu contextuel suivant :

Menu tunnel fermé

Menu tunnel ouvert

Ouvre Tunnel	Affiché si le tunnel VPN est fermé, permet d'ouvrir le tunnel (Phase2, ChildSA ou TLS) sélectionné
Fermer le tunnel	Affiché si le tunnel VPN est ouvert, permet de fermer le tunnel (Phase2, ChildSA ou TLS) sélectionné
Export (1)	Permet d'exporter la Phase2 / ChildSA / TLS sélectionnée
Copier	Permet de copier la Phase2 / ChildSA / TLS sélectionnée
Renommer (2)	Permet de renommer la Phase2 / ChildSA /TLS sélectionnée
Supprimer (2)	Permet de supprimer, moyennant confirmation de l'utilisateur, la Phase2 / ChildSA / TLS sélectionnée

(1) Cette fonction permet d'exporter le tunnel complet, c'est-à-dire, la Phase 2 et sa Phase 1 associée (ou la ChildSA et sa IKE Auth associée, ou la TLS), et de créer ainsi une politique de sécurité VPN mono-tunnel complètement opérationnelle (qui peut par exemple être importée en étant immédiatement fonctionnelle).
(2) Ce menu est désactivé tant que le tunnel est ouvert

10.4.3 Raccourcis

Pour la gestion de l'arborescence, les raccourcis suivants sont disponibles :

F2	Permet d'éditer le nom de la Phase sélectionnée
DEL	Si une phase est sélectionnée, la supprime après confirmation de l'utilisateur. Si la Configuration est sélectionnée (racine de l'arborescence), propose l'effacement (reset) de la configuration complète.
CTRL+O	Si une Phase2/ChildSA/TLS est sélectionnée, ouvre le tunnel VPN correspondant.
CTRL+W	Si une Phase2/ChildSA/TLS est sélectionnée, ferme le tunnel VPN correspondant.
CTRL+C	Copie la phase sélectionnée dans le "clipboard".
CTRL+V	Colle (ajoute) la phase copiée dans le "clipboard".
CTRL+N	Crée une nouvelle Phase 1/IKE Auth, si la Configuration VPN est sélectionnée, ou crée une nouvelle Phase 2 /ChildSA / TLS pour la Phase 1 / IKE Auth sélectionnée.
CTRL+S	Sauvegarde la politique de sécurité VPN.

11 Fenêtre "A propos…"

La fenêtre "A propos…" est accessible :
- par le menu " ? > A propos…" du Panneau de Configuration,
- par le menu système du Panneau de Configuration,
- ou par le bouton [?] du Panneau des Connexions.

La fenêtre "A propos…" donne les informations suivantes :
- Le nom et la version du logiciel.
- Lien internet sur le site web TheGreenBow.
- Lorsque le logiciel est activé, le numéro de licence et l'email utilisés pour l'activation.
- Lorsque le logiciel est en période d'évaluation, le nombre de jours restants pour l'évaluation.
- Les versions de tous les composants du logiciel (1).

(1) Il est possible de sélectionner tout le contenu de la liste des versions (clic droit dans la liste et choisir "Tout sélectionner"), puis de le copier, par exemple pour transmettre l'information à des fins d'analyse.

12 Importer, exporter la politique VPN

12.1 Importer une politique de sécurité VPN

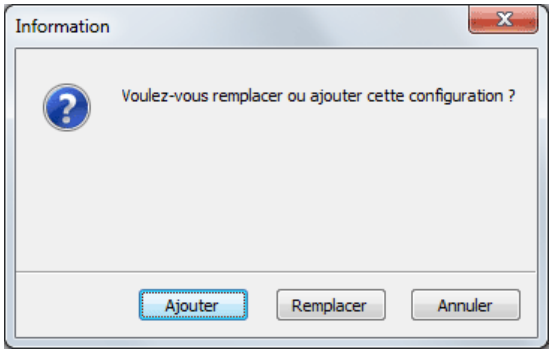
Le Client VPN TheGreenBow permet d'importer une politique de sécurité VPN de différentes façons :
- Par le menu "Configuration > Importer" du Panneau de Configuration (interface principale)
- Par "Glisser-déposer" d'un fichier de Configuration VPN (fichier ".tgb") sur le Panneau de Configuration (interface principale)
- Par double-clic sur un fichier de Configuration VPN (fichier ".tgb") (1)
- Par ligne de commande en utilisant l'option " /import " (2)

(1) Dans le cadre du renforcement de la sécurité du logiciel, la fonction d'import d'une configuration par double-clic sur le fichier de configuration n'est pas disponible dans la version TheGreenBow VPN Certified.

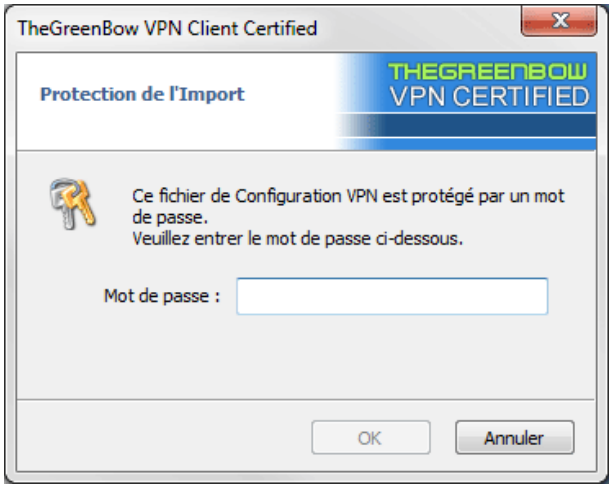
(2) L'utilisation des options de ligne de commande du logiciel est détaillée dans le document "Guide de Déploiement". Y sont en particulier détaillées toutes les options disponibles pour l'importation d'une politique de sécurité VPN : " /import ", " /add", " /replace " ou " /importonce ".

A noter : Les fichiers de configurations VPN importées portent par défaut l'extension ".tgb".

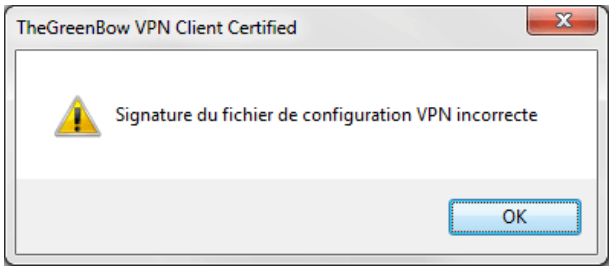
A l'importation d'une Configuration VPN, il est demandé à l'utilisateur s'il veut ajouter la nouvelle Configuration VPN à la Configuration courante, ou s'il veut remplacer (écraser) la Configuration courante par la nouvelle Configuration VPN :



Si la politique de sécurité VPN importée a été exportée protégée par un mot de passe (Cf. "Exporter une politique de sécurité VPN" ci-dessous), le mot de passe est demandé à l'utilisateur



Si la politique de sécurité VPN a été exportée avec contrôle d'intégrité (Cf. "Exporter une politique de sécurité VPN" ci-dessous) et qu'elle a été corrompue, un message alerte l'utilisateur, et le logiciel n'importe pas la Configuration.



Note : Si des tunnels VPN ajoutés ont le même nom que des tunnels VPN de la configuration courante, ils sont automatiquement renommés au cours de l'importation (ajout d'un incrément entre parenthèse).

Importation des Paramètres Généraux (IKEv1 seul)

Si à l'importation, l'utilisateur choisit "Remplacer", ou si la Configuration courante est vide, les Paramètres Généraux de la configuration VPN importée remplacent les Paramètres Généraux de la configuration courante.
Si à l'importation, l'utilisateur choisit "Ajouter", les Paramètres Généraux de la configuration VPN courante sont conservés.

Choix utilisateur à l'importation	Configuration courante vide	Configuration courante non vide
Ajouter	Paramètres Généraux remplacés par les nouveaux	Paramètres Généraux conservés
Remplacer	Paramètres Généraux remplacés par les nouveaux	Paramètres Généraux remplacés par les nouveaux

12.2 Exporter une politique de sécurité VPN

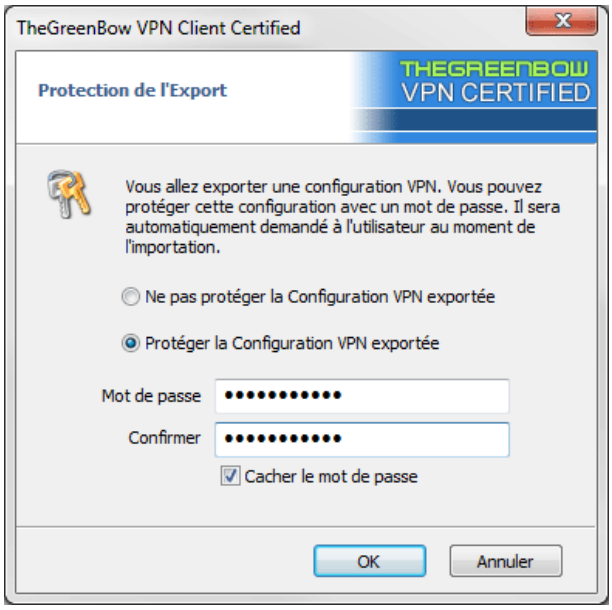
Le Client VPN TheGreenBow permet d'exporter une politique de sécurité VPN de différentes façons :

1/ Menu "Configuration > Exporter : La politique de sécurité VPN entière est exportée
2/ Menu contextuel associé à la racine de l'arborescence VPN > Export : La politique de sécurité VPN entière est exportée
3/ Menu contextuel associé à une Phase1 (IKEv1) ou à IKE Auth (IKEv2) > Export : Toute la Phase1 / IKE Auth (incluant les Phases2 / Child SA qu'elle contient) est exportée
4/ Menu contextuel associé à une Phase2 (IKEv1) ou Child SA (IKEv2) > Export : La Phase2 / Child SA est exportée, avec la Phase1/IKE Auth à laquelle elle est associée
5/ Menu Contextuel associé à une TLS > Export : La TLS est exportée
6/ Par ligne de commande en utilisant l'option " /export " (1)

(1) L'utilisation des options de ligne de commande du logiciel est détaillée dans le document "Guide de Déploiement " (tgbvpn_ug_deployment_fr.pdf). Y sont en particulier détaillées toutes les options disponibles pour l'exportation d'une politique de sécurité VPN : " /export " ou " /exportonce ".

A noter : Les fichiers de configurations VPN exportées portent par défaut l'extension ".tgb".

Quelle que soit la méthode employée, l'opération d'exportation débute par le choix de la protection pour la politique de sécurité VPN exportée : Elle peut-être exportée protégée (chiffrée) par un mot de passe, ou exportée "en clair". Quand il est configuré, le mot de passe est demandé à l'utilisateur au moment de l'importation.



A noter : qu'elle soit exportée chiffrée ou "en clair", la configuration exportée peut être protégée en intégrité.
La protection en intégrité de la politique de sécurité VPN exportée est une fonction activable via une clé en Base de Registre. Cette fonction est détaillée dans le "Guide de Déploiement" (tgbvpn_ug_deployment_fr.pdf)

Note : Dans la version TheGreenBow VPN Certified, toute configuration exportée est par défaut protégée en intégrité.

Il est recommandé de toujours exporter la politique de sécurité VPN protégée par un mot de passe (chiffrée).

Lorsqu'une politique de sécurité VPN exportée est protégée en intégrité, et par la suite corrompue, un message d'alerte prévient l'utilisateur au moment de l'importation, et le logiciel n'importe pas cette configuration (Cf. chapitre "Importer une politique de sécurité VPN" ci-dessus).

12.3 Fusionner des politiques de sécurité VPN

Il est possible de fusionner plusieurs politiques de sécurité VPN en une seule, en important successivement les Configurations VPN, et en choisissant "Ajouter" à chaque importation (Cf. chapitre "Importer une politique de sécurité VPN" ci-dessus).

12.4 Diviser une politique de sécurité VPN

En utilisant les différentes options d'exportation (exportation d'une phase 1/IKE Auth/TLS avec toutes les Phases 2 / ChildSA / TLS associées, ou exportation d'un tunnel simple), il est possible de diviser une politique de sécurité VPN en autant de "sous-Configurations" que désiré. (Cf. "Exporter une politique de sécurité VPN" ci-dessus).

Cette technique peut être utilisée pour déployer les politiques de sécurité VPN d'un parc informatique : dériver d'une politique VPN commune les politiques VPN associées chacune à un poste, avant de les diffuser à chaque utilisateur pour importation.

13 Configurer un tunnel VPN

13.1 VPN SSL, IPsec IKEv1 ou IPsec IKEv2

Le Client VPN TheGreenBow permet de créer et de configurer plusieurs types de tunnels VPN.
Il permet aussi, le cas échéant, de les ouvrir simultanément.

Le Client VPN TheGreenBow permet de configurer des tunnels
- IPsec IKEv1
- IPsec IKEv2
- SSL

La méthode pour créer un nouveau tunnel VPN est décrite dans les chapitres précédents : "Assistant de Configuration" et "Arborescence des tunnels VPN > Menus contextuels"

Recommandation de sécurité : Dans le cadre de la mise en œuvre et de l'utilisation du client TheGreenBow VPN Certified, il est recommandé de configurer des tunnels IKEv2 avec certificats. Cf. "Recommandations de sécurité"

13.2 Modification et sauvegarde de la configuration VPN

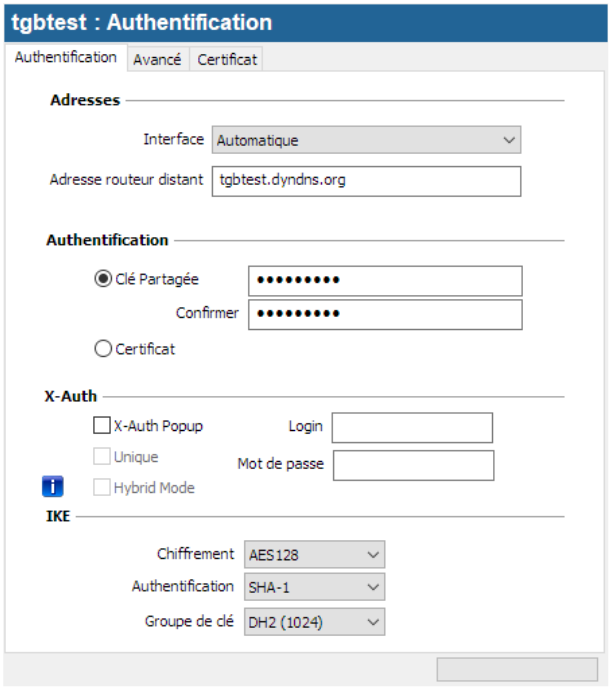
Le Client VPN TheGreenBow permet d'effectuer des modifications dans les tunnels VPN, et de tester "à la volée" ces modifications, ceci sans avoir besoin de sauvegarder la configuration.
Toute modification dans la configuration VPN est illustrée dans l'arborescence par le passage en caractères gras du nom de l'item modifié.

A tout moment, la configuration peut être sauvegardée :
- Par CTRL+S
- Via le menu "Configuration > Sauver"

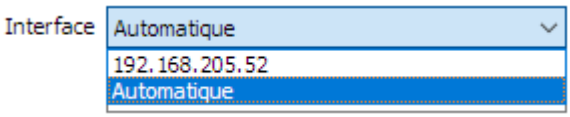
Si une configuration est modifiée et que l'utilisateur quitte l'application sans l'avoir sauvegardée, il est alerté.

13.3 Configurer un tunnel IPsec IKEv1

13.3.1 Phase1 : Authentification



Adresses

Interface	Adresse IP de l'interface réseau sur laquelle la connexion VPN est ouverte. Il est possible de laisser au logiciel le soin de déterminer cette interface, en sélectionnant "Automatique".  Privilégier ce choix lorsque le tunnel en cours de configuration est destiné à être déployé sur un autre poste par exemple.
Adresse routeur distant	Adresse IP (IPv4 ou IPv6) ou adresse DNS de la Passerelle VPN distante. Ce champ doit être obligatoirement renseigné.

Authentification

Clé partagée	Mot de passe ou clé partagée par la Passerelle distante. A noter : La clé partagée (preshared key) est un moyen simple de configurer un tunnel VPN. Il apporte toutefois moins de souplesse dans la gestion de la sécurité que l'utilisation de certificats. Cf. "Recommandations de sécurité"

Certificat	Utilisation de Certificat pour l'authentification de la connexion VPN. A noter : L'utilisation de Certificat apporte une plus grande sécurité dans la gestion des connexions VPN (authentification mutuelle, vérification des durées de vie, révocation, etc.). Cf. "Recommandations de sécurité" Se reporter au chapitre dédié : "Gestion des Certificats"

X-Auth

Voir la section "Gestion X-Auth" ci-dessous.

IKE

Chiffrement	Algorithme de chiffrement négocié au cours de la Phase d'Authentification : Auto (1), DES, 3DES, AES-128, AES-192, AES-256. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Authentification	Algorithme d'authentification négocié au cours de la Phase d'Authentification : Auto (1), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Groupe de clé	Longueur de la clé Diffie-Hellman : Auto (1), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) Cf. "Recommandations de sécurité" pour le choix de l'algorithme.

(1) Auto signifie que le Client VPN s'adapte automatiquement aux paramètres de la gateway. Lorsque "Auto" est sélectionné, les algorithmes suivants (et leurs diverses combinaisons) sont supportés :
- Chiffrement : DES, 3DES, AES-128, AES-192, AES-256
- Authentification : MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512
- Groupe de clé : DH1, DH2, DH5, DH14, DH15, DH16, DH17, DH18

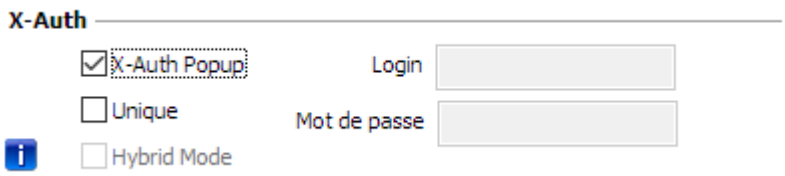
Si la passerelle est configurée avec un algorithme différent, alors le mode "Auto" ne peut être utilisé. L'algorithme doit être explicitement configuré dans le Client VPN.

Gestion X-Auth

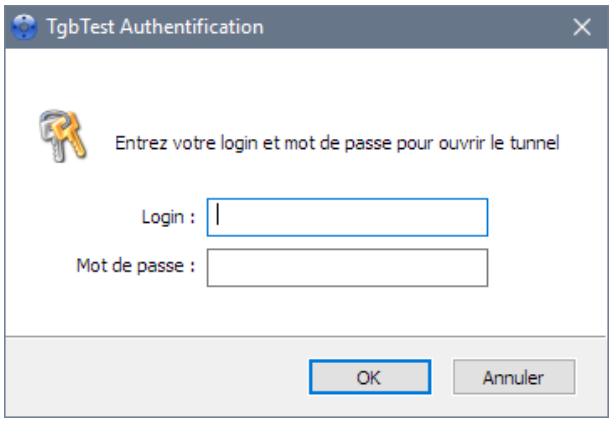
X-Auth est une extension du protocole IKE (Internet Key Exchange).

La fonction X-Auth est utilisée pour conditionner l'ouverture du tunnel VPN à la présentation, par l'utilisateur, d'un login et d'un mot de passe.

A noter : Cette fonction nécessite une configuration équivalente sur la Passerelle VPN.

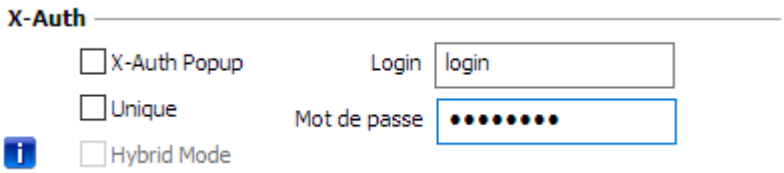


Lorsque la case "X-Auth Popup" est cochée, une fenêtre demande à chaque ouverture de tunnel VPN, le login et le mot de passe d'authentification de l'utilisateur (la fenêtre de demande de login et de mot de passe a pour titre le nom du tunnel, pour éviter les confusions).



Sur expiration du temps d'attente de cette fenêtre (configurable dans les paramètres généraux), un message d'alerte avertit l'utilisateur qu'il doit ré-ouvrir le tunnel.

Le Client VPN permet de mémoriser les login et mot de passe X-Auth dans la politique de sécurité VPN. Ces login et mot de passe sont alors automatiquement présentés à la Passerelle VPN au cours de l'ouverture du tunnel.



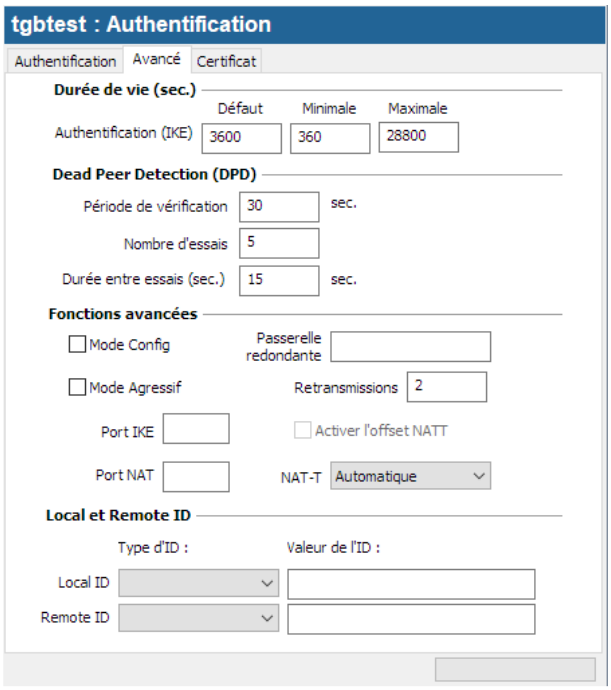
Cette possibilité facilite l'utilisation et le déploiement du logiciel. Elle reste néanmoins moins sécurisée que la présentation dynamique de la fenêtre de saisie du login / mot de passe X-Auth.

Cocher l'option "Unique" pour ne pas avoir de nouvelle demande de saisie du mot de passe lors d'une renégociation de Phase1.

Le Mode Hybride est un mode qui réunit deux types d'authentification : l'authentification de la Passerelle VPN classique et l'authentification X-Auth pour le Client VPN.
Pour activer le Mode Hybride, il est nécessaire que le tunnel soit associé à un certificat (Cf. Gestion des Certificats), et que la fonction X-Auth soit configurée

Il est recommandé de consulter le chapitre "Recommandations de sécurité" pour évaluer la pertinence de la mise en œuvre de cette fonction.

13.3.2 Phase1 : Avancé



Durée de vie

Durée de vie (sec.)	Les durées de vie sont négociées lors de la montée du tunnel. Chaque extrémité transmet la durée de vie par défaut, et vérifie que la durée de vie de l'autre extrémité se trouve dans la plage attendue (entre la valeur minimale et la valeur maximale) (1) A échéance de la durée de vie, la phase 1 est renégociée. Les durées de vie sont exprimées en secondes. Les valeurs par défaut sont :

	Défaut	Min	Max
Authentification (IKE)	7200 (2h)	360 (6min)	28800 (8h)

(1) Les durées de vie sont destinées à être négociées entre le Client VPN et la Gateway VPN. Toutefois, certaines Gateways se limitent à retourner la valeur par défaut de la durée de vie proposée par le Client VPN. Quelle que soit la méthode, le Client VPN applique toujours la durée de vie envoyée par la Gateway VPN.

Dead Peer Detection (DPD)

DPD	La fonction de DPD (Dead Peer Detection) permet au Client VPN de détecter que la Passerelle VPN devient inaccessible ou inactive. (1)

Période de vérification	Période entre deux messages de vérification DPD envoyés, exprimée en secondes.
Nombre d'essais	Nombre d'essais infructueux consécutifs avant de

	déclarer que la Passerelle VPN est inaccessible.
Durée entre essais	Intervalle entre les messages DPD quand aucune réponse n'est reçue de la Passerelle VPN, exprimée en secondes.

(1) La fonction de DPD est active une fois le tunnel ouvert (phase 1 montée). Associé à une Passerelle redondante, le DPD permet au Client VPN de basculer automatiquement d'une Passerelle à l'autre sur indisponibilité de l'une ou l'autre.

Fonctions avancées

Mode Config	Le Mode Config, une fois activé, permet au Client VPN de récupérer depuis la Passerelle VPN des éléments de configuration nécessaires à l'ouverture du tunnel VPN. Voir le paragraphe ci-dessous : Gestion du Mode Config.
Passerelle redondante	Définit l'adresse d'une Passerelle VPN de secours sur laquelle le Client VPN bascule lorsque la Passerelle VPN initiale est indisponible ou inaccessible. L'adresse de la Passerelle VPN redondante peut être une adresse IP ou DNS. Voir le chapitre Passerelle redondante
Mode agressif	Le Client VPN utilise le mode agressif pour se connecter à la Passerelle VPN. Voir le chapitre "Recommandations de sécurité" concernant l'usage du mode agressif versus l'usage du Main Mode.
Retransmissions	Nombre de retransmissions de messages protocolaires IKE avant échec.
Port IKE	Les échanges IKE Phase 1 (Authentification) s'effectuent sur le protocole UDP, en utilisant par défaut le port 500. Le paramétrage du port IKE permet de passer les équipements réseau (Firewall, routeurs) qui filtrent ce port 500. A noter : La Passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Phase 1 sur un port différent de 500.
Port NAT	Les échanges IKE Phase 2 (IPsec) s'effectuent sur le protocole UDP, en utilisant par défaut le port 4500. Le paramétrage du port NAT permet de passer les équipements réseau (Firewall, routeurs) qui filtrent ce port 4500. A noter : La Passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Phase 2 sur un port différent de 4500.
Activer l'offset NAT-T	Lorsque le port IKE est différent de 500, il peut être nécessaire de cocher cette option pour que la passerelle accepte la connexion.
NAT-T	Mode "NAT-Traversal". Le Client VPN permet de gérer 3types de modes NAT-T :

Désactivé	Empêche le Client VPN et la Passerelle VPN de passer en mode NAT-Traversal
Automatique	Laisse le Client VPN et la Passerelle VPN négocier le mode NAT-Traversal
Forcé	Le Client VPN force le mode NAT-T par l'encapsulation systématique des paquets IPsec dans des trames UDP. Ceci permet de résoudre les problèmes de NAT-Traversal au travers de certains routeurs intermédiaires.

Local et Remote ID

Local ID	Le "Local ID" est l'identifiant de la Phase d'Authentification (Phase1) que le Client VPN envoie à la Passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : - une adresse IP (type = Adresse IP), p.ex. 195.100.205.101 - un nom de domaine (type = FQDN), p.ex. gw.mydomain.net - une adresse email (type = USER FQDN), p.ex. support@thegreenbow.com - une chaîne de caractères (type = KEY ID), p.ex. 123456 - le sujet d'un certificat (type = Sujet X509 (alias DER ASN1 DN)), c'est le cas lorsque le tunnel est associé à un certificat utilisateur (Cf. Gestion des Certificats) Quand ce paramètre n'est pas renseigné, c'est l'adresse IP du Client VPN qui est utilisée par défaut.
Remote ID	Le "Remote ID" est l'identifiant que le Client VPN s'attend à recevoir de la Passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : - une adresse IP (type = Adresse IP), par exemple : 80.2.3.4 - un nom de domaine (type = FQDN), par exemple : routeur.mondomaine.com - une adresse email (type = USER FQDN), par exemple : admin@mydomain.com - une chaîne de caractères (type = KEY ID), par exemple : 123456 - le sujet d'un certificat (type = DER ASN1 DN) Quand ce paramètre n'est pas renseigné, le Client VPN accepte sans vérification tout identifiant envoyé par la passerelle. ⚠ Point de Sécurité : Voir le chapitre "Recommandations de sécurité" pour la gestion du Remote ID lorsque le Client VPN est configuré pour vérifier le certificat de la gateway.

Gestion du Mode Config

Le Mode Config, une fois activé, permet au Client VPN de récupérer depuis la Passerelle VPN des éléments de configuration nécessaires à l'ouverture du tunnel VPN :
- Adresse IP virtuelle du Client VPN
- Adresse d'un serveur DNS (optionnel)
- Adresse d'un serveur WINS (optionnel)

Important : Pour que le Mode Config soit opérationnel, il est nécessaire que la Passerelle VPN le supporte aussi.

Lorsque le Mode Config n'est pas activé, les 3 informations "Adresse du Client VPN", "Serveur DNS" et "Serveur WINS" sont configurables manuellement dans le Client VPN (Cf. "Phase 2, avancé")

Réciproquement, lorsque le Mode Config est activé, les champs de Phase 2 : "Adresse du Client VPN", "Serveur DNS" et "Serveur WINS" sont renseignés automatiquement au cours de l'ouverture du tunnel VPN. Ils sont donc interdits à la saisie (grisés).

13.3.3 Phase1 : Certificat

Voir le chapitre Gestion des Certificats.

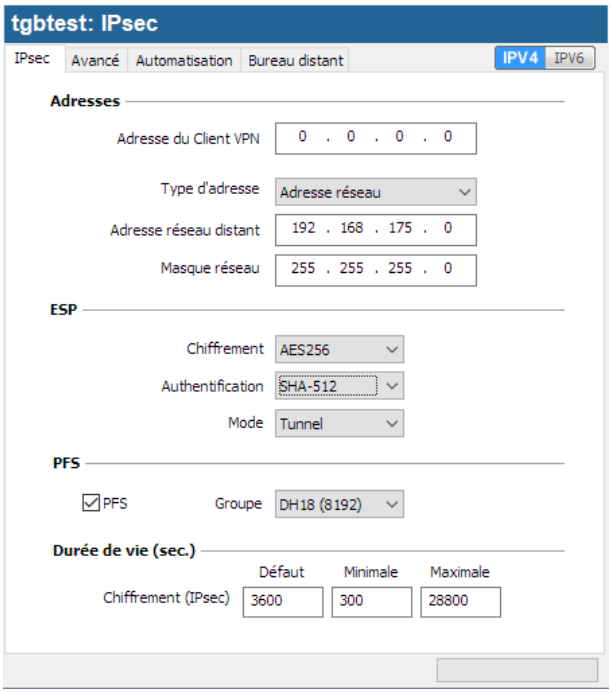
13.3.4 Phase2

La Phase 2 d'un tunnel VPN est la phase IPsec. Cette Phase sert à la négociation des paramètres de sécurité qui seront appliqués aux données transmises dans le tunnel VPN.

Pour configurer les paramètres de Phase 2, sélectionner cette Phase 2 dans l'arborescence du Panneau de Configuration. Les paramètres se configurent dans les onglets de la partie droite du Panneau de Configuration.

Après modification, le tunnel concerné passe en caractères gras dans l'arborescence VPN. Il n'est pas nécessaire de sauvegarder la configuration pour que celle-ci soit prise en compte : le tunnel peut-être testé immédiatement avec la configuration modifiée.

13.3.5 Phase2 : IPsec



Adresses

Adresse du Client VPN	Adresse IP "virtuelle" du poste, tel qu'il sera "vu" sur le réseau distant. Techniquement, c'est l'adresse IP source des paquets IP transportés dans le tunnel IPsec. Quand le champ est à "0.0.0.0", le logiciel prend automatiquement l'adresse IP physique du poste comme adresse IP virtuelle fournie à la passerelle. A noter : Si le Mode Config est activé, ce champ est grisé (non disponible à la saisie). Il est en effet automatiquement renseigné au cours de l'ouverture du tunnel, avec la valeur envoyée par la Passerelle VPN dans l'échange Mode Config.
Type d'adresse	L'extrémité du tunnel peut être un réseau ou un poste distant. Voir le paragraphe ci-dessous pour la **configuration du Type d'adresse**

ESP

Chiffrement	Algorithme de chiffrement négocié au cours de la Phase IPsec : Auto (1), DES, 3DES, AES-128, AES-192, AES-256. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Authentification	Algorithme d'authentification négocié au cours de la Phase IPsec : Auto (1), MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Mode	Mode d'encapsulation IPsec : Tunnel ou Transport Cf. "Recommandations de sécurité" pour le choix de l'algorithme.

(1) Auto signifie que le Client VPN s'adapte automatiquement aux paramètres de la gateway. Quand "Auto" est sélectionné, les algorithmes suivants (et leurs diverses combinaisons) sont supportés :
- Chiffrement : DES, 3DES, AES-128, AES-192
- Authentification : MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512

Si la gateway est configurée avec un algorithme différent, alors le mode "Auto" ne peut être utilisé. L'algorithme doit être explicitement spécifié dans le Client VPN.

PFS

PFS - Groupe	Activable ou pas : Longueur de la clé Diffie-Hellman : DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048)), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) Note : IKEv1 ne propose pas de mode automatique pour le Groupe DH. Il est requis de le connaître a priori. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.

Durée de vie

Durée de vie (sec.)

Les durées de vie sont négociées lors de la montée du tunnel.
Chaque extrémité transmet la durée de vie par défaut, et vérifie que la durée de vie de l'autre extrémité se trouve dans la plage attendue (entre la valeur minimale et la valeur maximale) (1)
A échéance de la durée de vie, la phase 2 est renégociée.

Les durées de vie sont exprimées en secondes. Les valeurs par défaut sont :

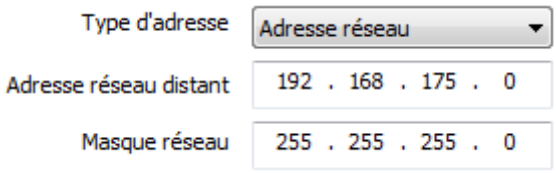
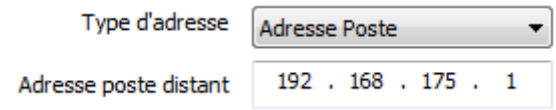
	Défaut	Min	Max
Chiffrement (IPsec)	2700 (45 min)	300 (5 min)	28800 (8 h)

(1) Les durées de vie sont échangées entre le Client VPN et la Gateway VPN. Toutefois, certaines Gateways se limitent à retourner la valeur de la durée de vie proposée par le Client VPN. Quelle que soit la méthode, le Client VPN applique toujours la durée de vie envoyée par la Gateway VPN.

IPv4 / IPv6

IPv4-IPv6	Voir le chapitre "IPv4 et IPv6".

Configuration du Type d'adresse

Si l'extrémité du tunnel est un réseau, choisir le type "Adresse réseau" puis définir l'adresse et le masque du réseau distant :	
Ou choisir "Plage d'adresses" et définir l'adresse de début et l'adresse de fin :	
Si l'extrémité du tunnel est un poste, choisir "Adresse Poste" et définir l'adresse du Poste distant :	

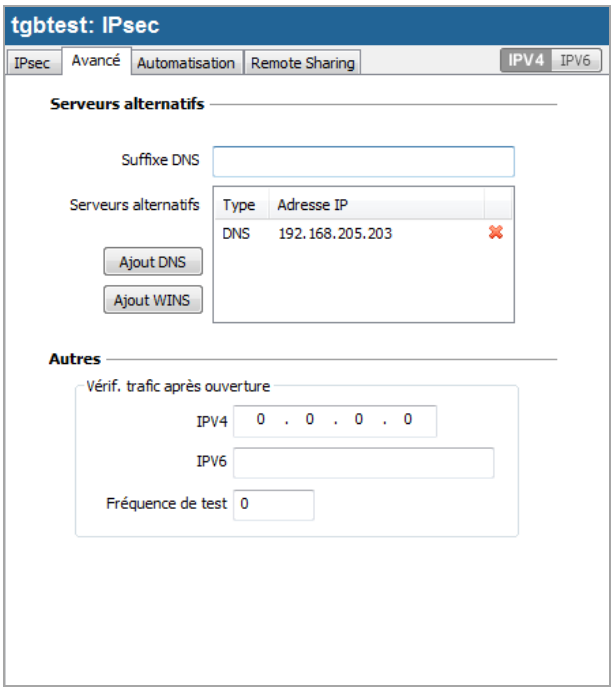
A noter : La fonction "Ouverture automatiquement sur détection de trafic" permet d'ouvrir automatiquement un tunnel sur détection de trafic vers l'une des adresses de la plage d'adresses spécifiée (moyennant le fait que cette plage d'adresses soit aussi autorisée dans la configuration de la Passerelle VPN).

A noter : Si l'adresse IP du poste Client VPN fait partie du plan d'adressage du réseau distant (p.ex. @IP poste = 192.168.10.2 et @réseau distant = 192.168.10.x), l'ouverture du tunnel empêche le poste de communiquer avec son réseau local. En effet, toutes les communications sont orientées dans le tunnel VPN.

Configuration "tout le trafic dans le tunnel VPN"
Il est possible de configurer le Client VPN pour que l'intégralité du trafic sortant du poste passe dans le tunnel VPN. Pour réaliser cette fonction, sélectionner le type d'adresse "Adresse réseau" et indiquer comme adresse et masque réseau "0.0.0.0".

Rappel : De nombreux guides de configuration du Client VPN avec différentes Passerelles VPN sont disponibles sur le site web TheGreenBow : http://www.thegreenbow.com/vpn/vpn_gateway.html

13.3.6 Phase2 : Avancé



Serveurs alternatifs

Suffixe DNS	Suffixe de domaine à ajouter à chaque nom de machine, par exemple : "mozart.dev.thegreenbow". Ce paramètre est optionnel : Lorsqu'il est spécifié, le Client VPN essaye de traduire l'adresse de la machine sans ajouter le suffixe DNS. Puis, si la traduction échoue, il ajoute le suffixe DNS et essaye à nouveau de traduire l'adresse.
Serveurs alternatifs	Table des adresses IP des serveurs DNS (2 maximum) et WINS (2 maximum) accessibles sur le réseau distant. Les adresses IP seront des adresses IPv4 ou IPv6 suivant le type de réseau choisi dans l'onglet "IPsec". A noter : Si le Mode Config est activé, ces champs sont grisés (non disponibles à la saisie). Ils sont en effet automatiquement renseignés au cours de l'ouverture du tunnel, avec les valeurs envoyées par la Passerelle VPN dans l'échange Mode Config.

Autres

Vérification trafic après ouverture	Il est possible de configurer le Client VPN pour vérifier régulièrement la connectivité au réseau distant. Si la connectivité est perdue, le Client VPN ferme puis tente de ré-ouvrir le tunnel automatiquement. Le champ IPV4/IPV6 est l'adresse d'une machine située sur le réseau distant, censée répondre aux "ping" envoyés par le Client VPN. S'il n'y a pas de réponse au "ping", la connectivité est considérée comme perdue. Note : Si le tunnel est configuré en IPv4 (bouton en haut à droite de l'onglet), c'est le

	champ IPv4 qui est présenté. Si le tunnel est configuré en IPv6, c'est le champ IPv6 qui est présenté. Le champ "Fréquence de test" indique la période, exprimée en secondes, entre chaque "ping" émis par le Client VPN à destination de la machine dont l'adresse IP est spécifiée au dessus.

13.3.7 Phase2 : Automatisation

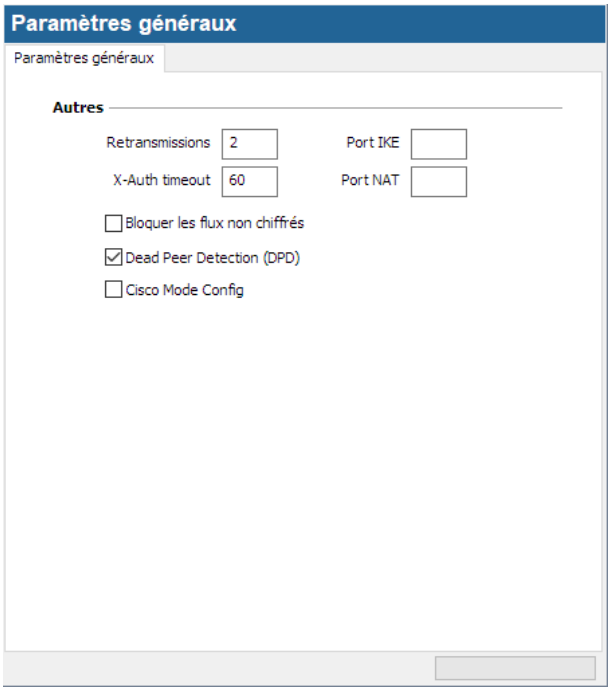
Voir le chapitre Automatisation

13.3.8 Phase2 : Remote Sharing

Voir le chapitre Partage de bureau distant

13.3.9 Paramètres généraux

Les paramètres généraux sont les paramètres communs à tous les tunnels IKEv1 (toutes les Phases 1 et toutes les Phases 2).



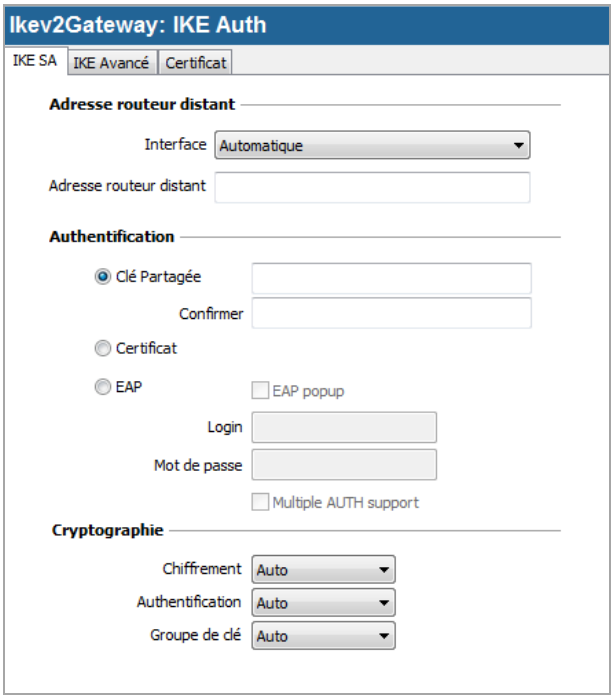
Autres

Retransmissions	Nombre de retransmissions de messages protocolaires IKE avant échec.
X-Auth timeout	Temps pour saisir le login / mot de passe X-Auth
Port IKE	Ce champ permet de configurer le Port IKE pour tous les tunnels IKEv1. Note : Le Port IKE configurable dans chaque tunnel est prioritaire par rapport à ce paramètre.
Port NAT	Ce champ permet de configurer le Port NAT pour tous les tunnels IKEv1. Note : Le Port NAT configurable dans chaque tunnel est prioritaire par rapport à ce paramètre.
Bloquer les flux non chiffrés	Lorsque cette option est cochée, seul le trafic passant dans le tunnel est autorisé. Voir la note (1) ci-dessous
Dead Peer Detection (DPD)	La fonction DPD peut être activée ou désactivée pour tous les tunnels IKEv1.
Cisco Mode Config	Cette case doit être cochée pour assurer la compatibilité avec les passerelles de type Cisco ASA.

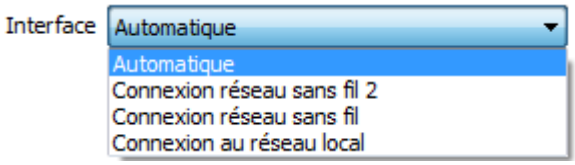
(1) L'option de configuration "Bloquer les flux non chiffrés" accroît "l'étanchéité" du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction permet d'éviter les risques de flux entrants qui pourraient transiter hors du tunnel VPN. Associée à la configuration "Passer tout le trafic dans le tunnel" (voir le chapitre Phase2 : IPsec), cette option permet de garantir une étanchéité totale du poste, dès lors que le tunnel VPN est ouvert

13.4 Configurer un tunnel IPsec IKEv2

13.4.1 IKE Auth : IKE SA



Adresses

Interface	Nom de l'interface réseau sur laquelle la connexion VPN est ouverte. Il est possible de laisser au logiciel le soin de déterminer cette interface, en sélectionnant "Automatique".  Privilégier ce choix lorsque le tunnel en cours de configuration est destiné à être déployé sur un autre poste par exemple.
Adresse routeur distant	Adresse IP (IPv6 ou IPv4) ou adresse DNS de la Passerelle VPN distante. Ce champ doit être obligatoirement renseigné.

Authentification

Clé partagée	Mot de passe ou clé partagée par la Passerelle distante. A noter : La clé partagée (preshared key) est un moyen simple de configurer un tunnel VPN. Il apporte toutefois moins de souplesse dans la gestion de la sécurité que

	l'utilisation de certificats. Cf. "Recommandations de sécurité"
Certificat	Utilisation de Certificat pour l'authentification de la connexion VPN. A noter : L'utilisation de Certificat apporte une plus grande sécurité dans la gestion des connexions VPN (authentification mutuelle, vérification des durées de vie, révocation, etc.). Cf. "Recommandations de sécurité" Se reporter au chapitre dédié : "Gestion des Certificats"
EAP	Le mode EAP (Extended Authentication Protocol) permet d'authentifier l'utilisateur grâce à un couple login/mot de passe. Quand le mode EAP est sélectionné, une fenêtre demande à l'utilisateur de saisir son login/mot de passe à chaque ouverture du tunnel. Lorsque le mode EAP est sélectionné, il est possible de choisir entre le fait que le login/mot de passe EAP soient demandés à chaque ouverture de tunnel (via la case "EAP popup"), ou qu'ils soient mémorisés dans la configuration VPN en les configurant dans les champs Login et Mot de passe. Ce dernier mode n'est pas recommandé dans le cadre de l'utilisation du logiciel en mode certifié. Cf. "Recommandations de sécurité"
Multiple Auth Support	Active la combinaison des deux authentifications par certificat puis par EAP. (1)

(1) Le Client VPN supporte la double authentification "certificat puis EAP".
Le Client VPN ne supporte pas la double authentification "EAP puis certificat".

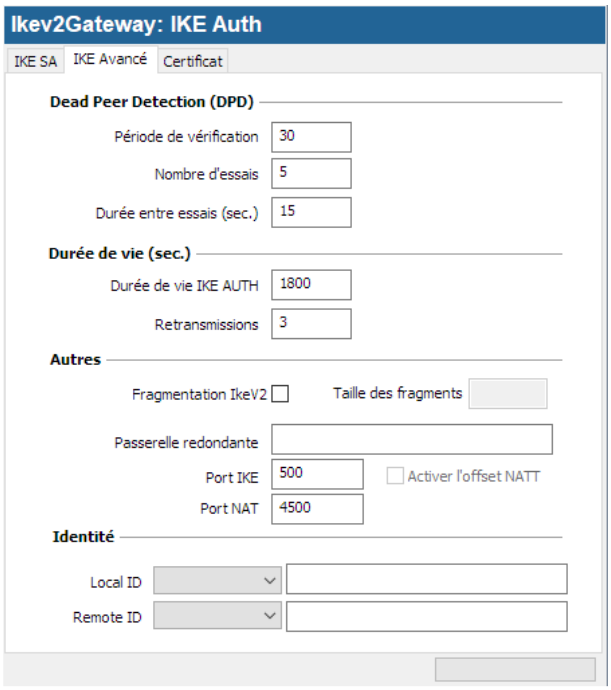
Cryptographie

Chiffrement	Algorithme de chiffrement négocié au cours de la Phase d'Authentification : Auto (1), DES, 3DES, AES-128, AES-192, AES-256. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Authentification	Algorithme d'authentification négocié au cours de la Phase d'Authentification : Auto (1), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Groupe de clé	Longueur de la clé Diffie-Hellman : Auto (1), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) Cf. "Recommandations de sécurité" pour le choix de l'algorithme.

(1) Auto signifie que le Client VPN s'adapte automatiquement aux paramètres de la gateway. Lorsque "Auto" est sélectionné, les algorithmes suivants (et leurs diverses combinaisons) sont supportés :
- Chiffrement : DES, 3DES, AES-128, AES-192, AES-256
- Authentification : MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512
- Groupe de clé : DH1, DH2, DH5, DH14, DH15, DH16, DH17, DH18

Si la gateway est configurée avec un algorithme différent, alors le mode "Auto" ne peut être utilisé. L'algorithme doit être explicitement configuré dans le Client VPN.

13.4.2 IKE Auth : IKE Avancé



Dead Peer Detection (DPD)

Période de vérification	La fonction DPD (Dead Peer Detection) permet au Client VPN de détecter que la passerelle VPN devient inaccessible ou inactive. (1) La période de vérification est la période entre deux envois de messages de vérification DPD, exprimée en secondes.
Nombre d'essais	Nombre d'essais infructueux consécutifs avant de déclarer que la passerelle VPN est injoignable.
Durée entre essais	Intervalle entre les messages DPD lorsqu'aucune réponse n'est reçue de la passerelle VPN, exprimé en secondes.

(1) La fonction de DPD est active à l'ouverture du tunnel (après la phase d'authentification). Associé à une Passerelle redondante, le DPD permet au Client VPN de basculer automatiquement d'une Passerelle à l'autre sur indisponibilité de l'une ou l'autre.

Durée de vie

Durée de vie IKE AUTH	Durée de vie de la phase IKE Authentication. La durée de vie est exprimée en secondes. Sa valeur par défaut est de 1800 secondes.
Retransmissions	Nombre de retransmissions de messages protocolaires IKE avant échec.

Autres

Fragmentation IKEv2	Active la fragmentation des paquets IKEv2 conformément à la RFC 7383. Cette fonction permet d'éviter que les paquets IKEv2 ne soient fragmentés par le réseau IP traversé. A ce titre, la valeur du champ "taille des fragments" doit être au maximum égale à la taille des fragments du réseau (typiquement 1500).
Passerelle redondante	Permet de définir l'adresse d'une Passerelle VPN de secours sur laquelle le Client VPN bascule lorsque la Passerelle VPN initiale est indisponible ou inaccessible. L'adresse de la Passerelle VPN redondante peut être une adresse IP ou DNS. Voir le chapitre Passerelle redondante
Port IKE	Les échanges IKE Auth (Authentification) s'effectuent sur le protocole UDP, en utilisant par défaut le port 500. Le paramétrage du port IKE permet de passer les équipements réseau (Firewall, routeurs) qui filtrent ce port 500. A noter : La Passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Auth sur un port différent de 500.
Port NAT	Les échanges IKE Child SA (IPsec) s'effectuent sur le protocole UDP, en utilisant par défaut le port 4500. Le paramétrage du port NAT permet de passer les équipements réseau (Firewall, routeurs) qui filtrent ce port 4500. A noter : La Passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Child SA sur un port différent de 4500.
Activer l'offset NAT-T	Lorsque le port IKE est différent de 500, il peut être nécessaire de cocher cette option pour que la passerelle accepte la connexion.

Identité

Local ID	Le "Local ID" est l'identifiant de la Phase d'Authentification que le Client VPN envoie à la Passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : - une adresse IP (type = Adresse IP), p.ex. 195.100.205.101 - un nom de domaine (type = FQDN), p.ex. gw.mydomain.net - une adresse email (type = USER FQDN), p.ex. support@thegreenbow.com - une chaîne de caractères (type = KEY ID), p.ex. 123456 - le sujet d'un certificat (type = DER ASN1 DN), c'est le cas lorsque le tunnel est associé à un certificat utilisateur (Cf. Gestion des Certificats) Quand ce paramètre n'est pas renseigné, c'est l'adresse IP du Client VPN qui est utilisée par défaut.
Remote ID	Le "Remote ID" est l'identifiant que le Client VPN s'attend à recevoir de la Passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : - une adresse IP (type = Adresse IP), par exemple : 80.2.3.4 - un nom de domaine (type = FQDN), par exemple : routeur.mondomaine.com

- une adresse email (type = USER FQDN), par exemple : admin@mydomain.com
- une chaîne de caractères (type = KEY ID), par exemple : 123456
- le sujet d'un certificat (type = DER ASN1 DN)

Quand ce paramètre n'est pas renseigné, le Client VPN accepte sans vérification tout identifiant envoyé par la passerelle.

⚠ Point de Sécurité : Voir le chapitre "Recommandations de sécurité" pour la gestion du Remote ID lorsque le Client VPN est configuré pour vérifier le certificat de la gateway.

13.4.3 IKE Auth : Certificat

Voir le chapitre : Gestion des Certficats

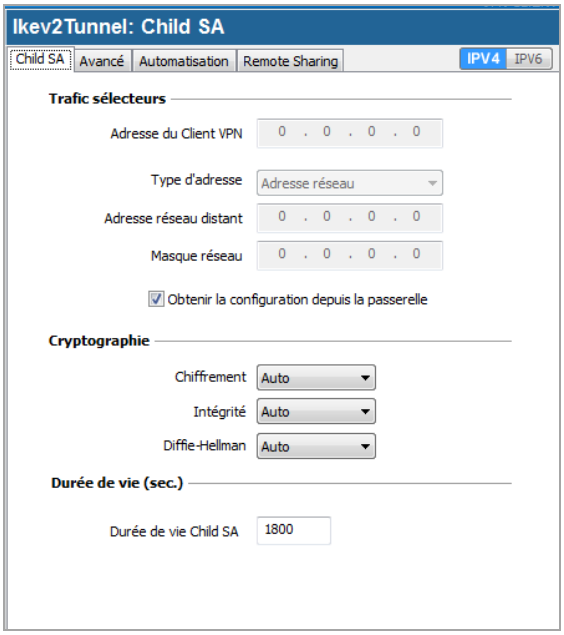
13.4.4 Child SA : Généralités

La "Child SA" d'un tunnel VPN est la phase IPsec. Cette Phase sert à la négociation des paramètres de sécurité qui seront appliqués aux données transmises dans le tunnel VPN.

Pour configurer les paramètres d'une Child SA, sélectionner cette Child SA dans l'arborescence du Panneau de Configuration. Les paramètres se configurent dans les onglets de la partie droite du Panneau de Configuration.

Après modification, le tunnel concerné passe en caractères gras dans l'arborescence VPN. Il n'est pas nécessaire de sauvegarder la configuration pour que celle-ci soit prise en compte : le tunnel peut-être testé immédiatement avec la configuration modifiée.

13.4.5 Child SA : Child SA



Trafic sélecteurs

Adresse du Client VPN	Adresse IP "virtuelle" du poste, tel qu'il sera "vu" sur le réseau distant. Techniquement, c'est l'adresse IP source des paquets IP transportés dans le tunnel IPsec.
Type d'adresse	L'extrémité du tunnel peut être un réseau ou un poste distant. Voir le paragraphe ci-dessous pour la **configuration du Type d'adresse**
Obtenir la configuration depuis la passerelle	Cette option (aussi appelée "Configuration Payload" ou encore "Mode CP") permet au Client VPN de récupérer depuis la passerelle VPN toutes les informations utiles à la connexion VPN : Adresses Client VPN, adresse réseau distant, subnet mask et adresses DNS. Lorsque cette option est cochée, tous ces champs sont grisés (désactivés). Ils sont renseignés dynamiquement au cours de l'ouverture du tunnel, avec les valeurs envoyées par la Passerelle VPN dans l'échange ModeCP.

Cryptographie

Chiffrement	Algorithme de chiffrement négocié au cours de la Phase IPsec : Auto (1), DES, 3DES, AES-128, AES-192, AES-256. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Intégrité	Algorithme d'authentification négocié au cours de la Phase IPsec : Auto (1), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. Cf. "Recommandations de sécurité" pour le choix de l'algorithme.
Diffie-Hellman	Longueur de la clé Diffie-Hellman : Auto (1), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192), No Diffie-Hellman Cf. "Recommandations de sécurité" pour le choix de l'algorithme.

(1) Auto signifie que le Client VPN s'adapte automatiquement aux paramètres de la gateway. Lorsque "Auto" est sélectionné, les algorithmes suivants (et leurs diverses combinaisons) sont supportés :
- Chiffrement : DES, 3DES, AES-128, AES-192, AES-256
- Authentification : MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512
- Groupe de clé : DH1, DH2, DH5, DH14, DH15, DH16, DH17, DH18

Si la gateway est configurée avec un algorithme différent, alors le mode "Auto" ne peut être utilisé. L'algorithme doit être explicitement configuré dans le Client VPN.

Durée de vie

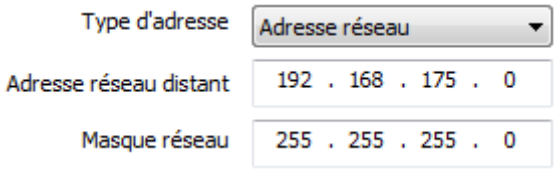
Durée de vie Child SA	Durée en secondes entre deux renégociations. Note : Contrairement à IKEv1, les durées de vie ne sont pas négociées en IKEv2 entre le Client VPN et la passerelle. Ainsi, les durées de vie appliquées au tunnel seront bien celles configurées sur le Client VPN.

IPv4 / IPv6

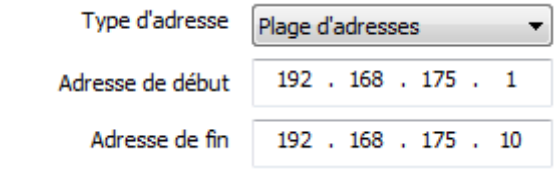
Voire le chapitre "IPv4 et IPv6"

Configuration du Type d'adresse

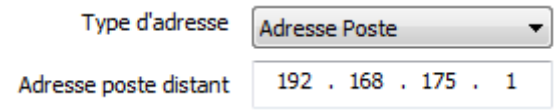
Si l'extrémité du tunnel est un réseau, choisir le type "Adresse réseau" puis définir l'adresse et le masque du réseau distant :



Ou choisir "Plage d'adresses" et définir l'adresse de début et l'adresse de fin :



Si l'extrémité du tunnel est un poste, choisir "Adresse Poste" et définir l'adresse du Poste distant :



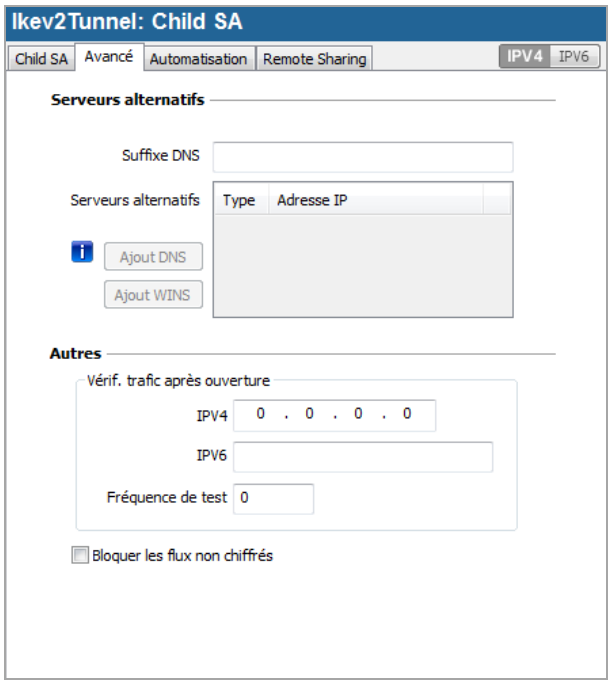
A noter : La fonction "Ouverture automatiquement sur détection de trafic" permet d'ouvrir automatiquement un tunnel sur détection de trafic vers l'une des adresses de la plage d'adresses spécifiée (moyennant le fait que cette plage d'adresses soit aussi autorisée dans la configuration de la Passerelle VPN).

A noter : Si l'adresse IP du poste Client VPN fait partie du plan d'adressage du réseau distant (p.ex. @IP poste = 192.168.10.2 et @réseau distant = 192.168.10.x), l'ouverture du tunnel empêche le poste de communiquer avec son réseau local. En effet, toutes les communications sont orientées dans le tunnel VPN.

Configuration "tout le trafic dans le tunnel VPN"
Il est possible de configurer le Client VPN pour que l'intégralité du trafic sortant du poste passe dans le tunnel VPN. Pour réaliser cette fonction, sélectionner le type d'adresse "Adresse réseau" et indiquer comme adresse et masque réseau "0.0.0.0".

Rappel : De nombreux guides de configuration du Client VPN avec différentes Passerelles VPN sont disponibles sur le site web TheGreenBow : http://www.thegreenbow.com/vpn/vpn_gateway.html

13.4.6 Child SA : Avancé



Serveurs alternatifs

Suffixe DNS	Suffixe de domaine à ajouter à chaque nom de machine, par exemple : "mozart.dev.thegreenbow". Ce paramètre est optionnel : Lorsqu'il est spécifié, le Client VPN essaye de traduire l'adresse de la machine sans ajouter le suffixe DNS. Puis, si la traduction échoue, il ajoute le suffixe DNS et essaye à nouveau de traduire l'adresse.
Serveurs alternatifs	Table des adresses IP des serveurs DNS (2 maximum) et WINS (2 maximum) accessibles sur le réseau distant. Les adresses IP seront des adresses IPv4 ou IPv6 suivant le type de réseau choisi dans l'onglet "Child SA". A noter : Si le Mode CP est activé (voir le paramètre "obtenir la configuration depuis la passerelle" dans l'onglet "Child SA"), ces champs sont grisés (non disponibles à la saisie). Ils sont en effet automatiquement renseignés au cours de l'ouverture du tunnel, avec les valeurs envoyées par la Passerelle VPN dans l'échange Mode CP.

Autres

Vérification trafic après ouverture	Il est possible de configurer le Client VPN pour vérifier régulièrement la connectivité au réseau distant. Si la connectivité est perdue, le Client VPN ferme automatiquement le tunnel puis tente de le ré-ouvrir. Le champ IPV4/IPV6 est l'adresse d'une machine située sur le réseau distant, censée répondre aux "ping" envoyés par le Client VPN. S'il n'y a pas de réponse au "ping", la connectivité est considérée comme perdue.

	Note : Si le tunnel est configuré en IPv4 (bouton en haut à droite de l'onglet), c'est le champ IPv4 qui est présenté. Si le tunnel est configuré en IPv6, c'est le champ IPv6 qui est présenté. Le champ "Fréquence de test" indique la période, exprimée en secondes, entre chaque "ping" émis par le Client VPN à destination de la machine dont l'adresse IP est spécifiée au dessus.
Bloquer les flux non chiffrés	Lorsque cette option est cochée, seul le trafic passant dans le tunnel est autorisé. Voir la note (1) ci-dessous

(1) L'option de configuration "Bloquer les flux non chiffrés" accroît "l'étanchéité" du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction permet d'éviter les risques de flux entrants qui pourraient transiter hors du tunnel VPN. Associée à la configuration "Passer tout le trafic dans le tunnel" (voir le chapitre IPsec), cette option permet de garantir une étanchéité totale du poste, dès lors que le tunnel VPN est ouvert.
Ce mode est recommandé pour la version "VPN Certified"

13.4.7 Child SA : Automatisation

Voir le chapitre "Automatisation"

13.4.8 Child SA : Remote Sharing

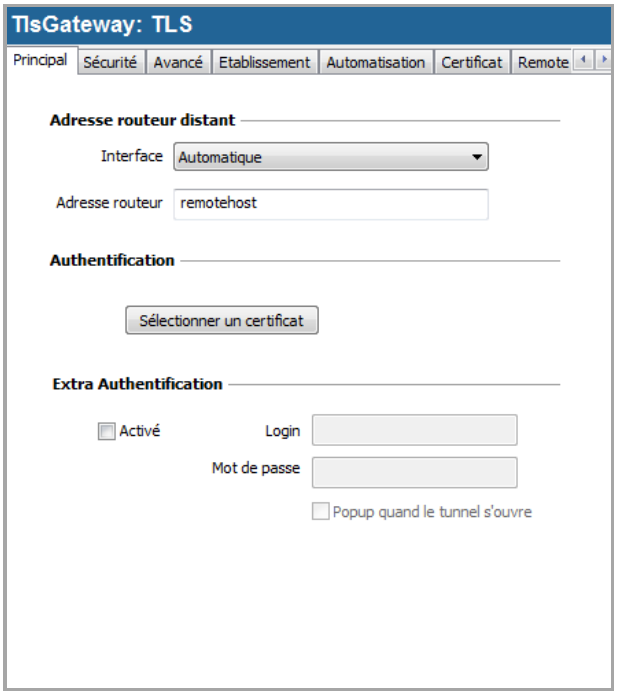
Voir le chapitre "Partage de bureau distant"

13.5 Configurer un tunnel VPN SSL

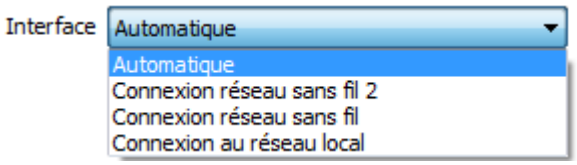
13.5.1 Introduction

Le Client VPN TheGreenBow permet depuis la version 6 d'ouvrir des tunnels VPN SSL.
Les tunnels VPN SSL du Client VPN TheGreenBow sont compatibles OpenVPN et permettent d'établir des connexions sécurisées avec toutes les passerelles qui implémentent ce protocole.

13.5.2 Principal



Adresse routeur distant

Interface	Nom de l'interface réseau sur laquelle la connexion VPN est ouverte. Il est possible de laisser au logiciel le soin de déterminer cette interface, en sélectionnant "Automatique".  Privilégier ce choix lorsque le tunnel en cours de configuration est destiné à être déployé sur un autre poste par exemple.
Adresse routeur distant	Adresse IP (IPv6 ou IPv4) ou adresse DNS de la Passerelle VPN distante. Ce champ doit être obligatoirement renseigné.

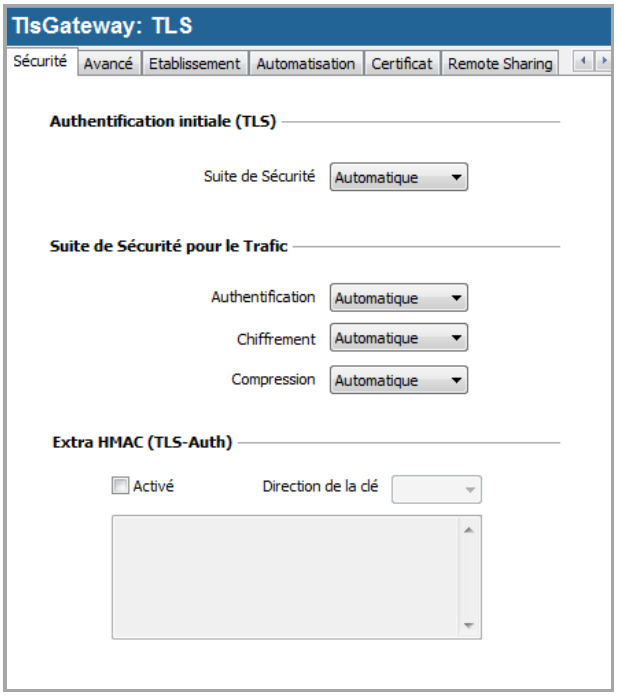
Authentification

Sélectionner un certificat	Sélection du Certificat pour l'authentification de la connexion VPN. Se reporter au chapitre dédié : "Gestion des Certificats"

Extra Authentification

Extra authentification	Cette option apporte un niveau de sécurité supplémentaire en demandant à l'utilisateur la saisie d'un login / mot de passe à chaque ouverture du tunnel. Le login / mot de passe peuvent être saisis de façon statique ou demandés dynamiquement à l'utilisateur à chaque ouverture du tunnel, lorsque la case "Popup quand le tunnel s'ouvre" est cochée.

13.5.3 Sécurité



Authentification initiale (TLS)

Suite de Sécurité	Ce paramètre est utilisé pour configurer le niveau de sécurité de la phase d'authentification dans l'échange SSL. - Automatique : toutes les suites cryptographiques (sauf nulle) sont proposées à la passerelle qui décide de la meilleure suite à utiliser - Basse : seules les suites cryptographiques faibles sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement de 64 ou 56 bits.

	- Normale : seules les suites cryptographiques "moyennes" sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement de 128 bits - Haute : seules les suites cryptographiques fortes sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement supérieurs ou égaux à 128 bits Pour plus d'informations : https://www.openssl.org/docs/apps/ciphers.html

Suite de Sécurité pour le Trafic

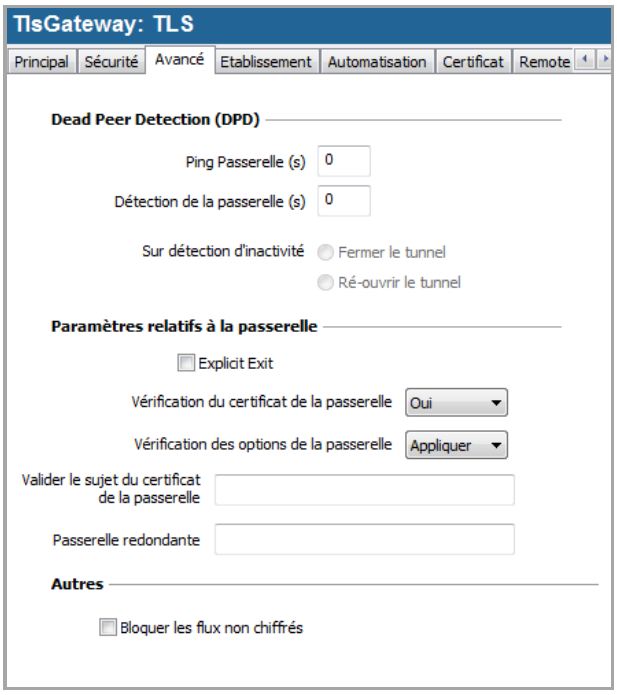
Authentification	Algorithme d'authentification négocié pour le trafic : Automatique (1), MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512. Note : Si l'option "Extra HMAC" est activée (Cf ci-dessous), l'algorithme d'authentification ne peut être "Automatique". Il doit être configuré explicitement, et doit être identique à celui choisi côté passerelle.
Chiffrement	Algorithme de chiffrement du trafic : Automatique (1), BF-CBC-128, AES128-CBC, AES192-CBC, AES256-CBC.
Compression	Compression du trafic : Automatique (1), activée (oui) ou désactivée (non).

(1) Automatique signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.

Extra HMAC (TLS-Auth)

Extra HMAC	Cette option ajoute un niveau d'authentification aux paquets échangés entre le Client et la Passerelle VPN. Pour être opérationnelle, cette option doit aussi être configurée sur la passerelle (sur une passerelle, cette option est souvent appelée "TLS-Auth") Quand cette option est sélectionnée, une clé doit être saisie dans le champ situé en dessous de la case cochée. Cette clé doit être saisie à l'identique sur la passerelle. C'est une suite de caractères hexadécimaux, dont le format est : -----BEGIN Static key----- 362722d4fbff4075853fbe6991689c36 b371f99aa7df0852ec70352122aee7be ... 515354236503e382937d1b59618e5a4a cb488b5dd8ce9733055a3bdc17fb3d2d -----END Static key----- La "Direction de la clé" doit être choisie : - BiDir : La clé spécifiée est utilisée dans les deux sens (mode par défaut) - Client : La direction de la clé à configurer sur la passerelle doit être "Serveur" - Serveur : La direction de la clé à configurer sur la passerelle doit être "Client"

13.5.4 Avancé



Dead Peer Detection (DPD)

La fonction DPD (Dead Peer Detection) permet aux deux extrémités du tunnel de vérifier mutuellement leur présence. (1)

Ping passerelle	Période exprimée en seconde d'envoi par le Client VPN d'un "ping" vers la passerelle. Cet envoi permet à la passerelle de déterminer que le Client VPN est toujours présent.
Détection de la passerelle	Durée en secondes à l'issue de laquelle, si aucun "ping" n'a été reçu de la passerelle, celle-ci est considérée comme indisponible.
Détection d'inactivité	Lorsque la passerelle est détectée comme indisponible (c'est-à-dire à la fin de la durée "Détection de la passerelle"), le tunnel peut-être fermé ou le Client VPN peut tenter de le ré-ouvrir.

(1) La fonction de DPD est active une fois le tunnel ouvert. Associé à une Passerelle redondante, le DPD permet au Client VPN de basculer automatiquement d'une Passerelle à l'autre sur indisponibilité de l'une ou l'autre.

Paramètres relatifs à la passerelle

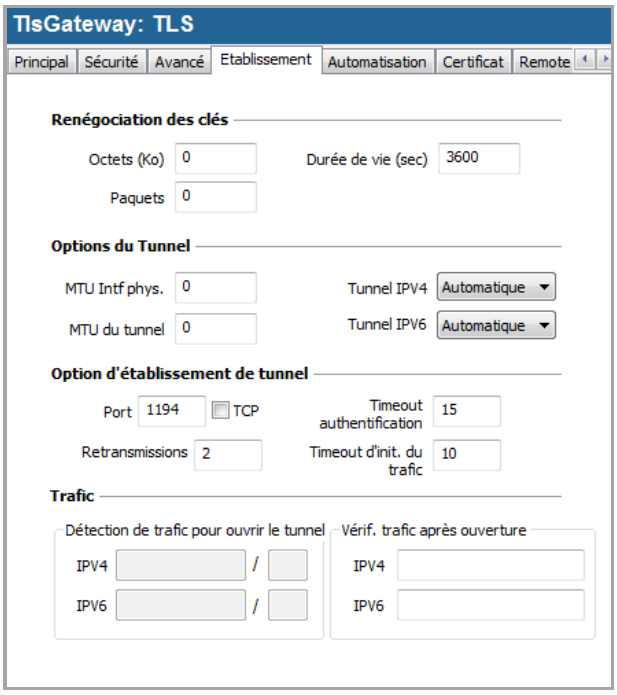
Explicit exit	Ce paramètre configure le Client VPN pour envoyer une trame spécifique de clôture du tunnel VPN à la passerelle, quand on ferme le tunnel. Si cette option n'est pas cochée, la passerelle utilise le DPD pour fermer le tunnel de son côté, ce qui est moins performant.
Vérification du certificat de la passerelle	Spécifie le niveau de contrôle du certificat de la passerelle. Dans la version actuelle, deux niveaux sont disponibles : - Oui (la validité du certificat est vérifiée)

	- Non (la validité du certificat n'est pas vérifiée). Le choix "simple" est réservé pour usage futur et, dans la version actuelle revient à "oui".
Vérification des options de la passerelle	Permet de définir le niveau de cohérence entre les paramètres du tunnel VPN et ceux de la passerelle (algorithmes de chiffrement, compression, etc.). - Oui : La cohérence est vérifiée sur l'ensemble des paramètres VPN. Le tunnel VPN ne peut s'ouvrir si un paramètre diffère. - Non : La cohérence n'est pas vérifiée avant ouverture du tunnel. Le tunnel VPN tente de s'ouvrir, quitte à ce qu'aucun trafic ne puisse passer parce que certains paramètres sont incohérents. - Simple : La cohérence entre le Client VPN et la passerelle n'est vérifiée que sur les paramètres essentiels. - Appliquer : Les paramètres de la passerelle sont appliqués.
Valider le sujet du certificat de la passerelle	Si ce champ est rempli, le Client VPN vérifie que le sujet du certificat reçu de la passerelle est bien celui spécifié.
Passerelle redondante	Définit l'adresse d'une Passerelle VPN de secours sur laquelle le Client VPN bascule lorsque la Passerelle VPN initiale est indisponible ou inaccessible. L'adresse de la Passerelle VPN redondante peut être une adresse IP ou DNS. Voir le chapitre Passerelle redondante

Autres

Bloquer les flux non chiffrés	Lorsque cette option est cochée, seul le trafic passant dans le tunnel est autorisé. L'option de configuration "Bloquer les flux non chiffrés" accroît "l'étanchéité" du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction permet d'éviter les risques de flux entrants qui pourraient transiter hors du tunnel VPN.

13.5.5 Etablissement



Renégociation des clés

Octets, Paquets, durée de vie	Les clés peuvent être renégociées sur échéance de 3 critères (qui peuvent être combinés) : - Quantité de trafic, exprimée en Ko - Quantité de paquets, exprimée en nombre de paquets - Durée de vie, exprimée en seconde Si plusieurs critères sont configurés, les clés sont renégociées sur échéance du premier critère vérifié

Options du tunnel

MTU interface physique	Taille maximale des paquets OpenVPN. Permet de spécifier une taille de paquet de façon à ce que les trames OpenVPN ne soient pas fragmentées au niveau réseau. Par défaut, la MTU spécifiée est à 0, ce qui signifie que le logiciel prend la valeur de la MTU de l'interface physique.
MTU du tunnel	MTU de l'interface virtuelle. Lorsqu'elles sont renseignées, il est recommandé de configurer une valeur pour la MTU du tunnel inférieure à celle de la MTU de l'interface physique. Par défaut, la MTU spécifiée est à 0, ce qui signifie que le logiciel prend la valeur de la MTU de l'interface physique moins un delta fixe.
Tunnel IPv4	Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv4 :

	- Automatique : Accepte ce qui est envoyé par la passerelle - Oui : Vérifie que ce qui est envoyé par la passerelle correspond au comportement configuré. Si ce n'est pas le cas, un message d'alerte est affiché dans la console et le tunnel ne se monte pas - Non : Ignore Note : Vérifier que les deux choix "Tunnel IPv4" et "Tunnel IPv6" ne sont pas tous deux à "Non".
Tunnel IPv6	Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv6 : - Automatique : Accepte ce qui est envoyé par la passerelle - Oui : Vérifie que ce qui est envoyé par la passerelle correspond au comportement configuré. Si ce n'est pas le cas, un message d'alerte est affiché dans la console et le tunnel ne se monte pas. - Non : Ignore Note : Vérifier que les deux choix "Tunnel IPv4" et "Tunnel IPv6" ne sont pas tous deux à "Non".

Option d'établissement du tunnel

Port / TCP	Numéro du port utilisé pour l'établissement du tunnel. Par défaut, le port est configuré à 1194. Par défaut, le tunnel utilise UDP. L'option "TCP" permet de transporter le tunnel sur TCP.
Timeout authentification	Délai d'établissement de la phase d'authentification au bout duquel on considère que le tunnel ne s'ouvrira pas. A échéance de ce timeout, le tunnel est fermé.
Retransmissions	Nombre de retransmission d'un message protocolaire. Sur absence de réponse au bout de ce nombre de retransmission du message, le tunnel est fermé.
Timeout d'init. du trafic	Phase d'établissement du tunnel : délai au bout duquel, si toutes les étapes n'ont pas été établies, le tunnel est fermé.

Trafic

Détection de trafic pour Ouvrir le tunnel	Les caractéristiques du réseau distant ne sont pas configurées en OpenVPN (elles sont récupérées automatiquement dans l'échange d'ouverture du tunnel avec la passerelle). Pour mettre en œuvre la fonction de détection de trafic en OpenVPN, il est donc nécessaire de spécifier explicitement ces caractéristiques du réseau distant. C'est l'objet des champs IPv4 et IPv6. Il n'est pas obligatoire de renseigner les deux champs. Le champ IP est une adresse de sous réseau, configurée sous forme d'une adresse IP et d'une longueur de préfixe. Exemple : IP = 192.168.1.0 / 24 : les 24 premiers bits de l'adresse IP sont pris en compte, soit le réseau : 192.168.1.x Note : Ces paramètres sont liés à la fonction de détection de trafic. Pour que les

	champs IPv4 et IPv6 soient activés, la case "Ouvrir automatiquement sur détection de trafic" de l'onglet "Automatisation" doit être cochée.
Test de trafic dans le tunnel	Si ces champs sont renseignés, le Client VPN tente de faire un "ping" sur ces adresses après ouverture du tunnel VPN. L'état de la connexion (réponse au ping ou absence de réponse au ping) est affiché dans la console. Il n'est pas obligatoire de renseigner les deux champs. Note : Aucune action particulière n'est faite s'il n'y a pas de réponse au "ping".

13.5.6 Automatisation

Voir le chapitre Automatisation

13.5.7 Certificat

Voir le chapitre Gestion des Certficats

13.5.8 Remote Sharing

Voir le chapitre Partage de bureau distant

14 Passerelle redondante

Le Client VPN TheGreenBow permet la gestion d'une passerelle VPN redondante.

Associée au paramétrage du DPD (Dead Peer Detection), cette fonction permet au Client VPN de basculer automatiquement sur la passerelle redondante dès que la passerelle principale est détectée comme étant injoignable ou indisponible.

En effet, sur perte des DPD, si une passerelle redondante est configurée, le tunnel tente de se ré-ouvrir automatiquement. Il est possible de configurer une passerelle redondante identique à la passerelle principale pour profiter de ce mode de réouverture automatique sans avoir réellement 2 passerelles.

L'algorithme de prise en compte de la Passerelle redondante est le suivant :

Le Client VPN contacte la Passerelle initiale pour ouvrir le tunnel VPN.
Si le tunnel ne peut être ouvert au bout de N tentatives
Le Client VPN contacte la Passerelle redondante.

Le même algorithme s'applique à la Passerelle redondante :

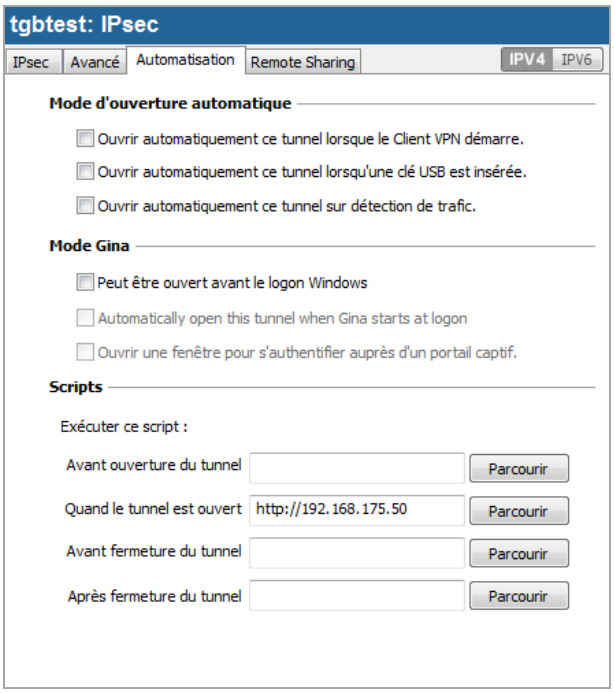
Si la Passerelle redondante est indisponible,
le Client VPN tente d'ouvrir le tunnel VPN avec la Passerelle initiale.

A noter : Le Client VPN n'essaye pas de contacter la Passerelle redondante si la Passerelle initiale est accessible mais qu'il y a des incidents d'ouverture du tunnel.

15 Automatisation

Le Client VPN TheGreenBow permet d'associer des automatismes à chaque tunnel VPN : ouverture automatique du tunnel suivant différents critères, exécution de batches ou de scripts à différentes étapes de l'ouverture ou de la fermeture du tunnel, etc.

Pour chaque type de tunnel, le paramétrage des automatisations s'effectue dans l'onglet "Automatisation" du tunnel : Phase2 (IKEv1), Child SA (IKEv2) ou TLS (SSL).



Mode d'ouverture automatique

Lorsque le Client VPN démarre	Le tunnel s'ouvre automatiquement au démarrage du Client VPN (1)
Lorsqu'une clé USB est insérée	Le tunnel fait partie d'une configuration sur clé USB (voir le chapitre "Mode USB"), et il est ouvert automatiquement sur insertion de cette clé USB (2)
Sur détection de trafic	Le tunnel s'ouvre automatiquement sur détection de trafic à destination d'une adresse IP faisant partie du réseau distant.

(1) Cette option permet de configurer l'ouverture automatique d'un tunnel sur double-clic sur le fichier ".tgb" qui le contient : Sélectionner l'option "Ouvrir automatiquement ce tunnel lorsque le Client VPN démarre", exporter la configuration dans un fichier "tunnel_auto.tgb", quitter le Client VPN. En double-cliquant sur le fichier "tunnel_auto.tgb", le Client VPN démarre et le tunnel s'ouvre automatiquement.
Note : la fonction d'ouverture automatique d'un tunnel sur double-clic sur le fichier ".tgb" qui le contient n'est pas disponible dans la version TheGreenBow VPN Certified.

(2) Par extension, cette option est aussi utilisée pour caractériser un tunnel à ouvrir automatiquement sur insertion d'une Carte à puce ou d'un Token contenant le certificat utilisé par le Tunnel VPN.

Mode GINA

Peut être ouvert avant le logon Windows	Cette option indique que la connexion VPN peut être ouverte avant le logon Windows : Elle apparaît dans la fenêtre des connexions GINA (voir le chapitre ci-dessous "Mode GINA")
Ouvrir automatiquement le tunnel par la GINA au logon	Quand cette option est cochée, le tunnel s'ouvre automatiquement avant le logon Windows. Cette option est active si l'option "Peut être ouvert avant le logon windows" est sélectionnée.
Ouvrir une fenêtre pour s'authentifier auprès d'un portail captif	L'utilisation de réseaux Wi-Fi requiert parfois une authentification locale auprès d'un portail dédié. Pour les utilisateurs du Mode GINA, le Client VPN implémente une nouvelle fenêtre de navigation qui s'ouvre automatiquement avant l'ouverture du tunnel, et qui permet l'authentification sur le portail Wi-Fi captif. ⚠ Point de sécurité : pour des raisons de sécurité, cette fonction n'est pas proposée dans le logiciel TheGreenBow VPN Certified. Nous contacter si cette fonction est nécessaire à votre utilisation du logiciel.

Scripts

Avant ouverture du tunnel	La ligne de commande spécifiée est exécutée avant que le tunnel ne s'ouvre
Après ouverture du tunnel	La ligne de commande spécifiée est exécutée dès que le tunnel est ouvert
Avant fermeture du tunnel	La ligne de commande spécifiée est exécutée avant que le tunnel ne se ferme
Après fermeture du tunnel	La ligne de commande est exécutée dès que le tunnel est fermé

Les lignes de commande peuvent être :

- l'appel à un fichier "batch", par exemple : `"C:\vpn\batch\script.bat"`
- l'exécution d'un programme, par exemple : `"C:\Windows\notepad.exe"`
- l'ouverture d'une page web, par exemple : `"http://192.168.175.50"`
- etc.

Les applications sont nombreuses :

- Création d'un fichier sémaphore lorsque le tunnel est ouvert, de façon à ce qu'une application tierce puisse détecter le moment où le tunnel est ouvert,
- Ouverture automatique d'un serveur intranet de l'entreprise, une fois le tunnel ouvert,
- Nettoyage ou vérification d'une configuration avant l'ouverture du tunnel,
- Vérification du poste (anti-virus mis à jour, versions correctes des applications, etc.) avant l'ouverture du tunnel,
- Nettoyage automatique (suppression des fichiers) d'une zone de travail sur le poste avant fermeture du tunnel,
- Application de comptabilisation des ouvertures, fermetures et durées des tunnels VPN,
- Modification de la configuration réseau, une fois le tunnel ouvert, puis restauration de la configuration réseau initiale après fermeture du tunnel,
- etc.

Note : Les scripts ne sont pas configurables pour un tunnel configuré en mode GINA. Les champs de saisie sont désactivés.

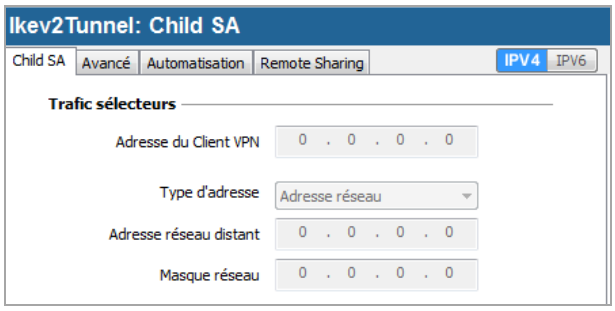
16 IPv4 et IPv6

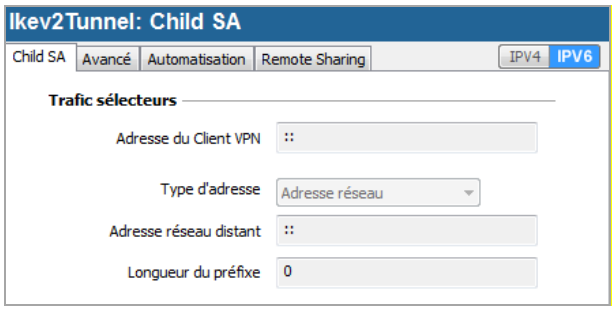
Le Client VPN TheGreenBow supporte les protocoles IPv4 et IPv6, que ce soit pour la communication avec la passerelle ou pour la communication sur le réseau distant. Le Client VPN permet de combiner l'utilisation d'IPv4 et IPv6, par exemple pour établir une connexion IPv4 sécurisée dans un tunnel VPN transporté sur IPv6.

Le choix IPv4/IPv6 se fait soit d'après l'adresse IP si elle est numérique, soit d'après la résolution DNS. Dans ce dernier cas, la résolution du nom de la gateway fournit soit une adresse IP soit IPv4, soit IPv6, soit les 2. Si les 2 adresses sont fournies, l'adresse IPv4 est privilégiée.

Pour les tunnels VPN IKEv1 et IKEv2, la configuration du protocole IPv4 ou IPv6 est accessible en haut à droite de l'onglet IPsec (pour les Phases 2 d'un tunnel IKEv1) ou Child SA (pour les Child SA d'un tunnel IKEv2).

Le protocole IP configuré par le bouton IPv4/IPv6 est exactement le protocole utilisé sur le réseau distant.





Note : Le choix IPv4 ou IPv6 a un impact sur les paramètres des autres onglets de configuration du tunnel. Ainsi, pour ces autres onglets, le bouton de choix IPv4/IPv6 est rappelé en haut à droite mais est désactivé.

Pour les tunnels SSL, la détection de la configuration protocolaire est automatique. Aucun paramétrage n'est requis. De plus, un tunnel SSL peut supporter du trafic IPv4 et IPv6 simultanément dans un même tunnel : il n'est pas nécessaire de configurer deux tunnels distincts comme pour IKEv1 ou IKEv2.

17 Gestion des Certificats

Le Client VPN TheGreenBow est le logiciel de connexion VPN pour lequel les innovations en matière d'intégration avec les PKI/IGC sont les plus avancées. Le Client VPN TheGreenBow est ainsi intégrable avec tout type de PKI/IGC, de façon souple, évolutive, automatisable et particulièrement configurable.

Le Client VPN TheGreenBow offre un ensemble inégalé de fonctions permettant l'exploitation de certificats de toute nature, issus de PKI de tout type et stockés sur des supports de toute nature : token, carte à puce, magasin de certificat, etc.

Le Client VPN TheGreenBow implémente en particulier les fonctions et facilités suivantes :

- Exploitation de tout type de support de certificat : token, carte à puce, magasin de certificat, fichier, politique de sécurité VPN, clé USB
- Caractérisation du support de certificat à utiliser : sélection automatique parmi plusieurs supports concurrents
- Accès aux cartes à puce et aux tokens en PKCS11 et en CSP
- Prise en compte des formats de certificats PKCS12, X509, PEM, PFX
- Configuration multicritères des certificats à utiliser : sujet, key usage, etc.
- Gestion des certificats côté utilisateur (côté Client VPN) comme les certificats de la passerelle VPN, incluant la gestion des dates de validité, des chaînes de certification, des certificats racines et des CRL
- Validation des certificats Client et Passerelle : authentification mutuelle, avec autorité de certification identiques ou différentes (importation de CA spécifiques)
- Exploitation de clés privées aux formats PKCS1 et PKCS8
- Possibilité de préconfigurer tous les paramètres PKI pour une prise en compte automatique lors de l'installation

Le Client VPN TheGreenBow apporte des fonctions de sécurité supplémentaires sur la gestion des PKI comme l'ouverture et la fermeture automatique du tunnel sur insertion et extraction de la carte à puce, ou encore la possibilité de configurer l'interface PKI et Carte à puce dans l'installeur du logiciel de façon à automatiser le déploiement.

La liste des lecteurs de Cartes à puces et des Tokens compatibles avec le Client VPN TheGreenBow est disponible sur le site TheGreenBow à l'adresse : http://www.thegreenbow.com/vpn_token.html

La configuration et la caractérisation des certificats à utiliser se répartissent en trois étapes :
1/ L'onglet "Certificat" du tunnel concerné : Phase1 (IKEv1) ou IKE Auth (IKEv2) ou TLS (SSL).
2/ L'onglet "Options PKI" de la fenêtre " Outils > Options " du Panneau de Configuration
3/ Un fichier de configuration initiale optionnel : vpnconf.ini

17.1 Configuration

17.1.1 Sélectionner un certificat (onglet "Certificat")

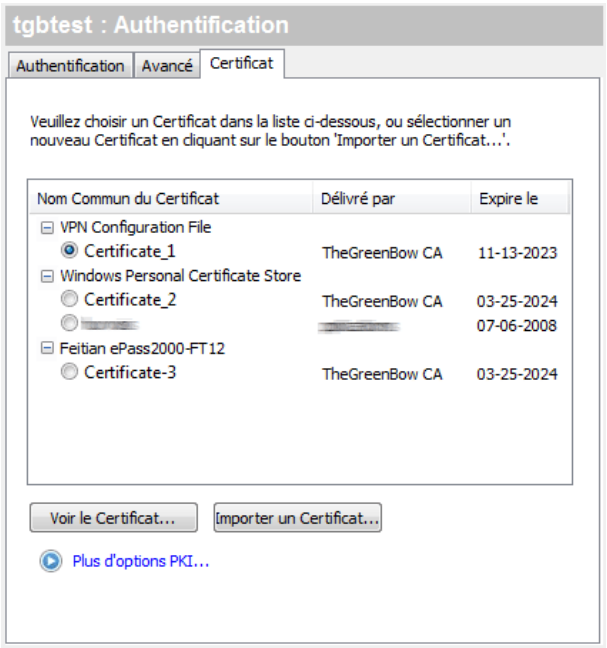
Le Client VPN permet d'affecter un certificat utilisateur à un tunnel VPN.
Il ne peut y avoir qu'un seul certificat par tunnel, mais chaque tunnel peut avoir son propre certificat.

Le Client VPN permet de choisir un certificat stocké :
- Dans le fichier de Configuration VPN (voir ci-dessous "Importer un Certificat")
- Dans le magasin de certificats Windows (voir ci-dessous "Magasin de Certificat Windows")
- Sur une Carte à puce ou dans un Token (voir ci-dessous "Configurer une carte à puce ou un Token")

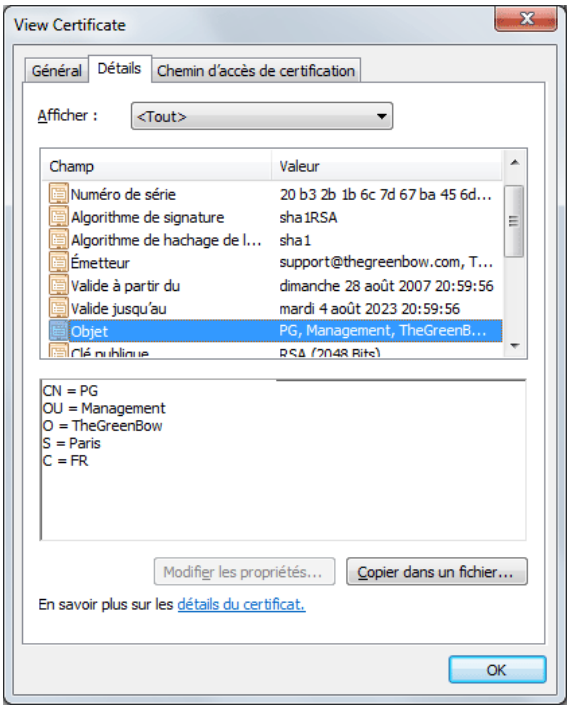
L'onglet "Certificat" du tunnel concerné énumère tous les supports accessibles sur le poste, qui contiennent des certificats.
Si un support ne contient pas de certificat, il n'est pas affiché dans la liste (p.ex. si le fichier de Configuration VPN ne contient pas de certificat, il n'apparaît pas dans la liste).

En cliquant sur le support désiré, la liste des certificats qu'il contient est affichée.

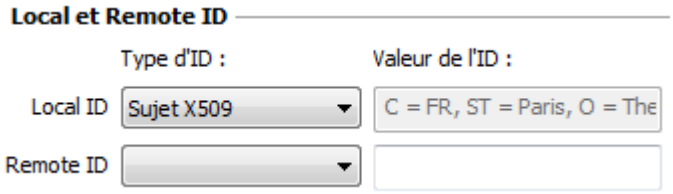
Cliquer sur le certificat souhaité pour l'affecter au tunnel VPN.



Une fois le certificat sélectionné, le bouton "Voir le certificat" permet d'afficher le détail du certificat.



Remarque : Une fois le certificat sélectionné, le type de Local ID du tunnel passe automatiquement à "Sujet X509" (alias DER ASN1 DN), et le sujet du certificat est utilisé par défaut comme valeur de ce "Local ID".

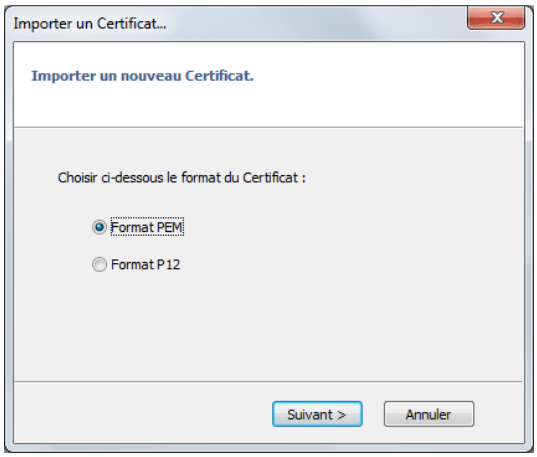


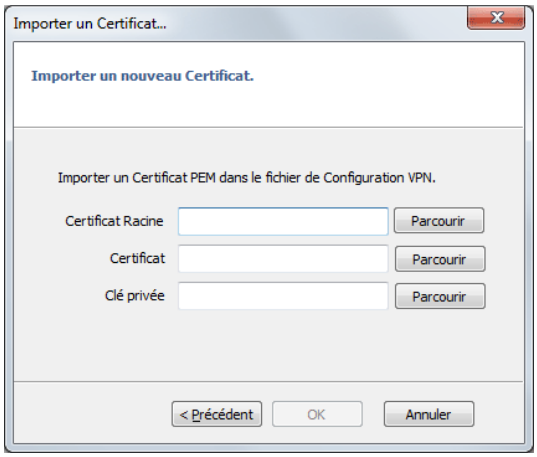
17.2 Importer un certificat

Le Client VPN TheGreenBow permet d'importer dans la politique de sécurité VPN des certificats au format PEM ou PKCS12. L'intérêt de cette solution, moins sécurisée que l'utilisation du Magasin de Certificats Windows ou d'une Carte à puce, est de faciliter le transport des certificats.

Importer un certificat au format PEM

1/ Dans l'onglet Certificat d'une Phase 2, cliquer sur "Importer un Certificat..."
2/ Choisir "Format PEM"
3/ Sélectionner ("Parcourir") les certificats Racine, Utilisateur et clé privée à importer
Note : Le fichier avec la clé privée ne doit pas être chiffré.
4/ Valider

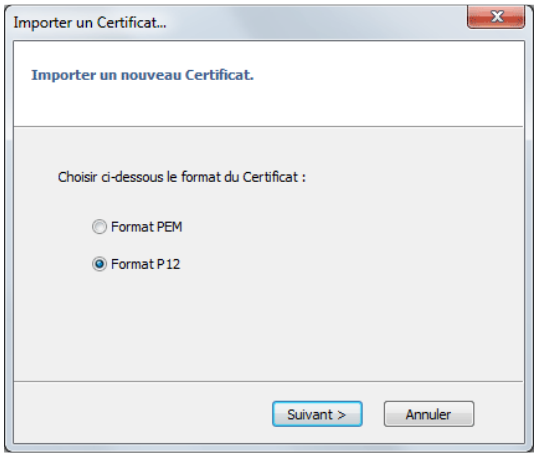


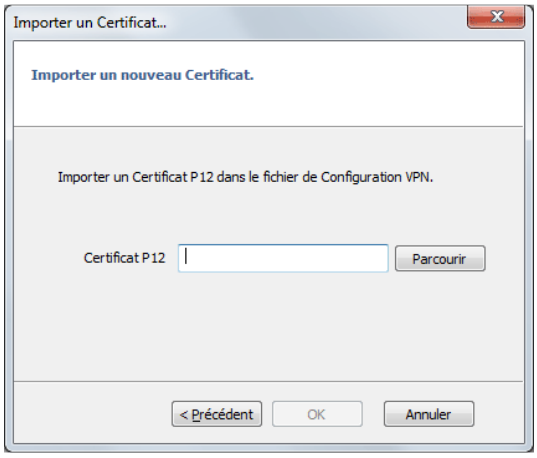


Le certificat apparaît et est sélectionné dans la liste des certificats de l'onglet "Certificat".
Sauvegarder la politique VPN : Le certificat est sauvegardé dans la politique de sécurité VPN.

Importer un certificat au format PKCS12

1/ Dans l'onglet Certificat d'une Phase 2, cliquer sur "Importer un Certificat..."
2/ Choisir "Format P12"
3/ Sélectionner ("Parcourir") le certificat PKCS12 à importer
4/ S'il est protégé par mot de passe, saisir le mot de passe et valider





Le certificat apparaît et est sélectionné dans la liste des certificats de l'onglet "Certificat".
Sauvegarder la politique VPN : Le certificat est sauvegardé dans la politique de sécurité VPN.

17.3 Magasin de Certificats Windows

Pour qu'un certificat du Magasin de Certificats Windows soit identifié par le Client VPN, il doit respecter les caractéristiques suivantes :

- Le Certificat doit être certifié par une autorité de certification (ce qui exclut les certificats auto-signés)
- Le Certificat doit être situé dans le magasin de Certificats "Personnel" (Il représente l'identité personnelle de l'utilisateur qui veut ouvrir un tunnel VPN vers son réseau d'entreprise).

A noter : Pour gérer les certificats dans le Magasin de Certificats Windows, Microsoft propose en standard l'outil de gestion "certmgr.msc". Pour exécuter cet outil, aller dans le menu Windows "Démarrer", puis dans le champ "Rechercher les programmes et fichiers", entrer "certmgr.msc".

17.4 Options PKI : Caractériser le certificat et son support

Le Client VPN TheGreenBow offre plusieurs possibilités pour caractériser le Certificat à utiliser, ainsi que les cartes à puces ou Tokens : automatismes pour retrouver le token à utiliser, critères de sélection du certificat à utiliser, options de déploiement ou de caractérisation de nouveaux tokens, etc.

Cette fonctionnalité est disponible uniquement dans les versions VPN Premium et VPN Certified via le lien "Plus d'options PKI" en bas de l'onglet "Certificat", et dans l'onglet "Options PKI" de la fenêtre de configuration des Options.

Cette fonctionnalité est décrite dans le document "Guide utilisateur Token et Carte à puce" (tgbvpn_ug_pki_smartcard_fr) disponible sur la page web : http://www.thegreenbow.fr/vpn_token.html.

Note : La mise en œuvre de l'authentification de la passerelle est décrite au chapitre 3.2 "Options PKI" du guide "Gestion des PKI, certificats, tokens et carte à puce" : tgbvpn_ug_pki_smartcard_fr, disponible sur le site TheGreenBow.

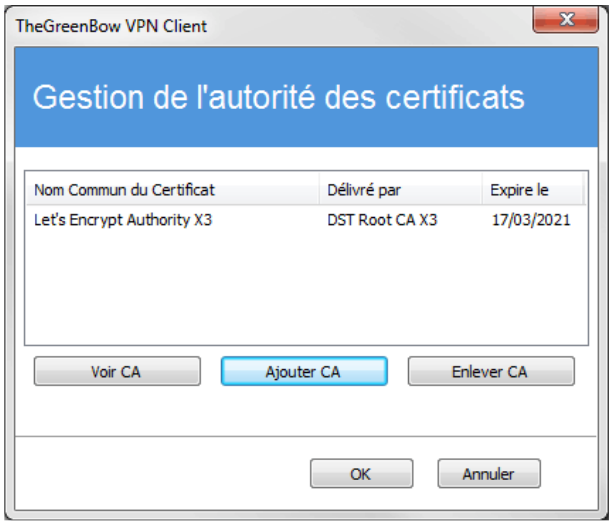
17.5 Gestion des CA (Autorités de Certification)

Lorsque le Client VPN TheGreenBow est configuré pour vérifier les certificats Client et Gateway, il peut être nécessaire d'importer des Autorités de Certification (CA), en complément des certificats exploités.
C'est le cas à chaque fois que le logiciel ne peut trouver localement le CA du certificat de la Gateway, c'est-à-dire dans les cas suivants :

1/ Le CA du certificat de la Gateway est différent de celui du Client, et ce CA Gateway n'est pas présent/accessible sur le poste (typiquement il est absent du magasin de certificat Windows)

2/ Le CA du certificat de la Gateway est le même que celui du Client mais le CA du Client est stocké sur un token ou une carte à puce : dans ce cas, il est inaccessible au logiciel.

3/ Le mode EAP est sélectionné (ce mode ne requiert pas certificat Client), et le CA du certificat de la Gateway n'est pas présent/accessible sur le poste.



1/ Dans la fenêtre "Gestion des CAs", cliquer sur "Ajouter CA"
2/ Choisir le format de CA souhaité (PEM ou DER)
3/ Sélectionner ("Parcourir") le CA à importer

17.6 Utiliser un tunnel VPN avec un Certificat sur Carte à puce

Lorsqu'un tunnel VPN est configuré pour exploiter un certificat stocké sur Carte à puce ou sur Token, le PIN code d'accès à cette Carte à puce est demandé à l'utilisateur à chaque ouverture du tunnel

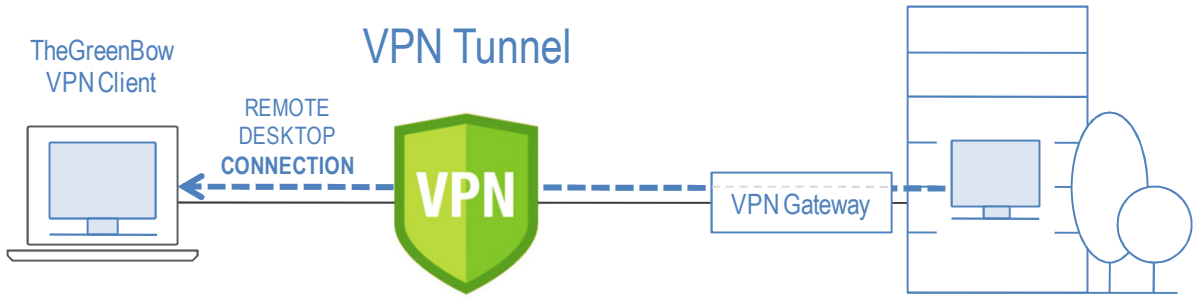
Si la Carte à puce n'est pas insérée, ou si le Token n'est pas accessible, le tunnel ne s'ouvre pas.
Si le certificat trouvé ne remplit pas les conditions configurées (Cf. "'Options PKI" ci-dessus), le tunnel ne s'ouvre pas.
Si le PIN code présenté est erroné, le Client VPN avertit l'utilisateur qui a 3 essais consécutifs avant blocage de la Carte à puce.

Le Client VPN implémente un mécanisme de détection automatique de l'insertion d'une Carte à puce.
Ainsi, les tunnels associés au certificat contenu sur la Carte à puce sont montés automatiquement à l'insertion de cette Carte à puce. Réciproquement, l'extraction de la Carte à puce ferme automatiquement tous les tunnels associés.
Pour mettre en œuvre cette fonction , cocher : "Ouvrir ce tunnel automatiquement lorsqu'une clé USB est insérée" (Cf. chapitre Automatisation)

18 Partage de bureau distant

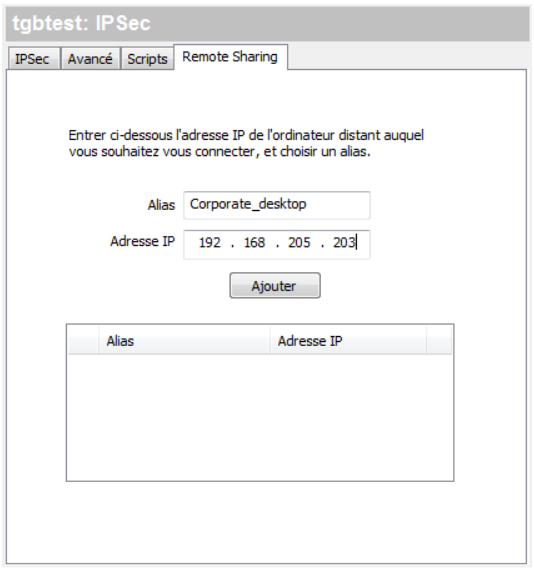
L'ouverture d'une session "Remote Desktop" (partage de bureau distant) au travers d'internet sur un ordinateur Windows distant nécessite habituellement l'établissement d'une connexion sécurisée, ainsi que la saisie des paramètres de connexions (adresse de l'ordinateur distant, etc.).

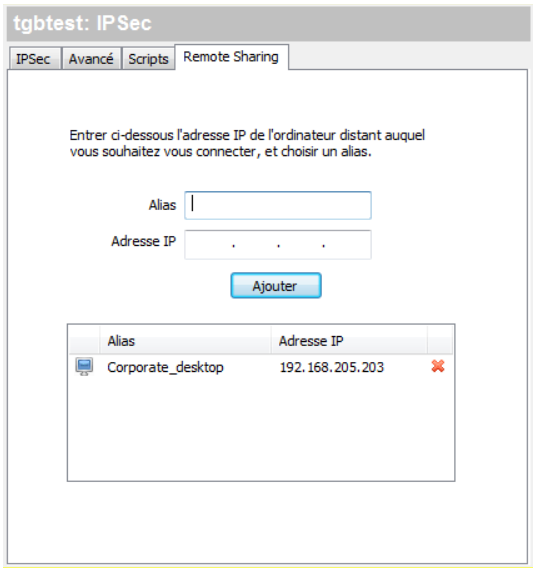
Le Client VPN TheGreenBow permet de simplifier et de sécuriser automatiquement l'ouverture d'une session "Remote Desktop" : En un seul clic, la connexion VPN s'établit avec le poste distant et la session RDP (Remote Desktop Protocol) est automatiquement ouverte sur ce poste distant.



18.1 Configuration du partage de bureau distant

1/ Sélectionner le tunnel VPN (Phase 2, Child SA ou TLS) dans lequel sera ouverte la session "Remote Desktop".
2/ Sélectionner l'onglet " Remote Sharing ".
3/ Entrer un alias pour la connexion (ce nom est utilisé pour identifier la connexion dans les différents menus du logiciel), et entrer l'adresse IP ou le nom Windows du poste distant.
4/ Cliquer sur "Ajouter" : La session de partage Remote Desktop est ajoutée à la liste des sessions.

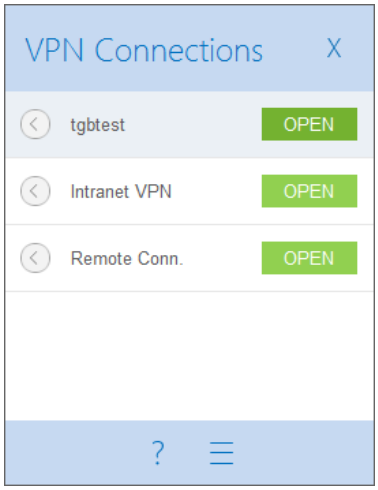




Pour ouvrir cette connexion RDP en un seul clic, il est recommandé de la faire apparaître spécifiquement dans le panneau des connexions, en utilisant la fonction de "Configuration du panneau des connexions" détaillée ci-après.

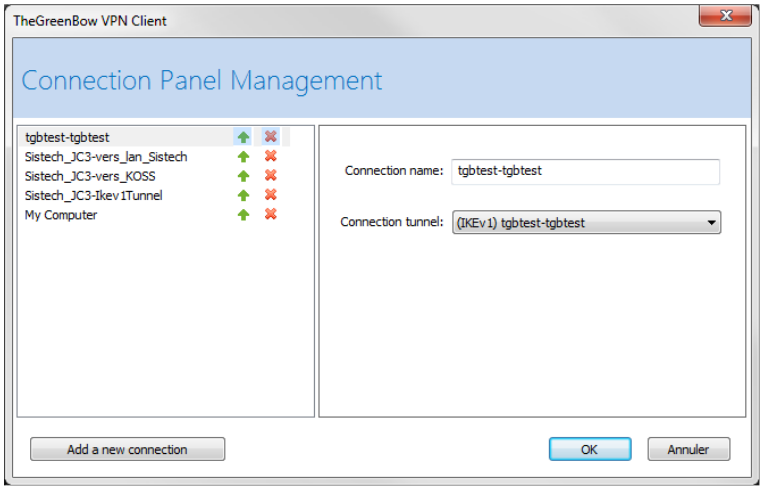
19 Configuration du panneau des connexions

A partir de la version 6.4, le panneau des connexions du Client VPN est entièrement configurable.



Une connexion VPN est soit un tunnel VPN, soit une connexion "Remote Desktop", c'est-à-dire un tunnel VPN dont la fonction "Remote Sharing" est renseignée.

Une nouvelle fenêtre, accessible dans le menu " Outils > Configuration du panneau des connexions " permet la gestion des connexions VPN dans le panneau des connexions : création, nommage, ordonnancement.



La nouvelle fenêtre de configuration du panneau des connexions permet de :

- choisir les connexions VPN qui apparaissent ou pas dans le panneau des connexions
- créer et ordonner les connexions VPN
- renommer les connexions VPN

La partie gauche de la fenêtre illustre la liste des connexions telles qu'elles apparaissent dans le panneau des connexions, la partie droite indique les paramètres de chaque connexion : son nom, le tunnel VPN associé et l'éventuelle connexion RDP (remote sharing) configurée.

Pour créer une nouvelle connexion VPN, cliquer sur le bouton "Ajouter une connexion", choisir un nom, choisir le tunnel VPN associé. Si une connexion Remote Sharing est configurée, la possibilité de la choisir apparaît automatiquement en dessous du tunnel choisi. Une fois validées, les modifications faites dans la fenêtre de gestion du panneau de connexions apparaissent immédiatement dans le panneau des connexions VPN.

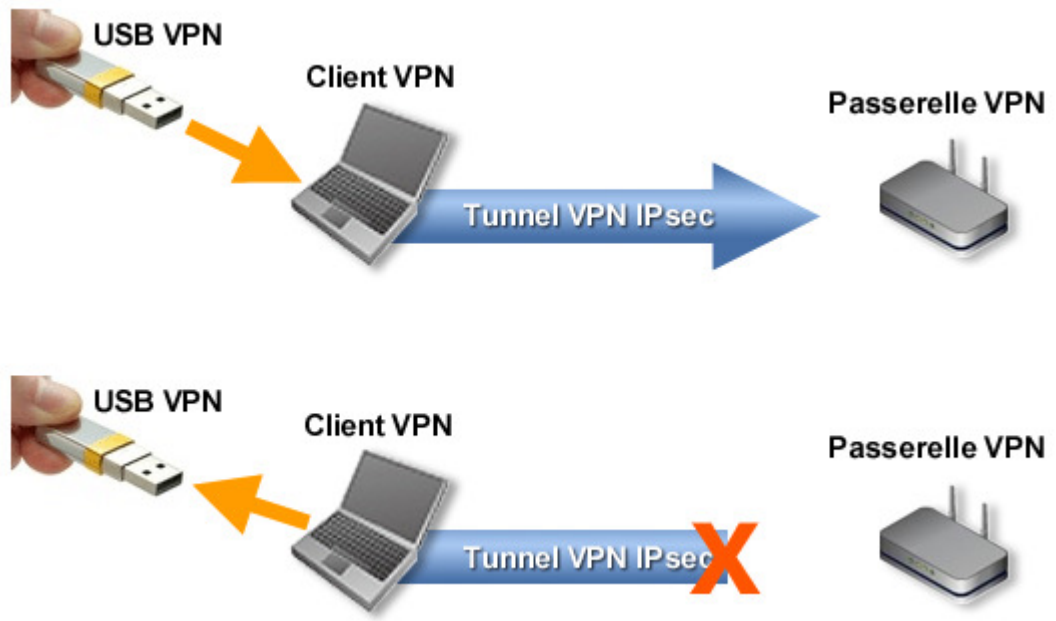
20 Mode USB

20.1 Le Mode USB VPN

Le Client VPN TheGreenBow offre un mode de gestion d'une connexion VPN inédit : le Mode VPN USB.

Ce mode VPN USB n'est pas disponible dans la version TheGreenBow VPN Certified.

Dans ce mode, la politique de sécurité VPN est mémorisée de façon sécurisée sur support amovible (clé USB), le poste à partir duquel la connexion VPN est ouverte est vierge de tout élément de sécurité VPN, la connexion VPN s'établit automatiquement dès insertion de la clé USB et se ferme dès extraction de la clé USB.

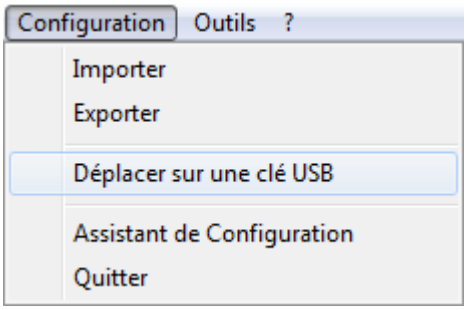


Dans le mode VPN USB :
- Aucun élément de sécurité n'est mémorisé sur le poste à partir duquel la connexion VPN est ouverte : le poste est vierge de toute politique de sécurité VPN.
- Les éléments de sécurité sont transportés de façon sécurisée sur le support amovible (clé USB).
- Le support amovible peut être une clé USB standard.
- Les éléments de sécurité sont mémorisés sur la clé USB chiffrés et protégés par mot de passe.
- La connexion VPN s'ouvre automatiquement sur insertion de la clé USB.
- La connexion VPN se ferme automatiquement sur extraction de la clé USB.

Dans la suite du document, la clé USB contenant la politique de sécurité VPN est appelée "Clé USB VPN".

20.2 Configurer le Mode USB

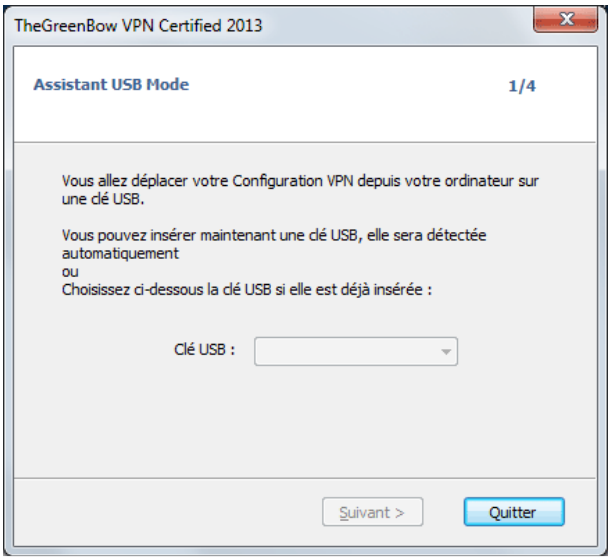
La configuration du Mode VPN USB s'effectue via l'assistant de configuration accessible par le menu "Configuration > Déplacer sur une clé USB" du panneau de configuration



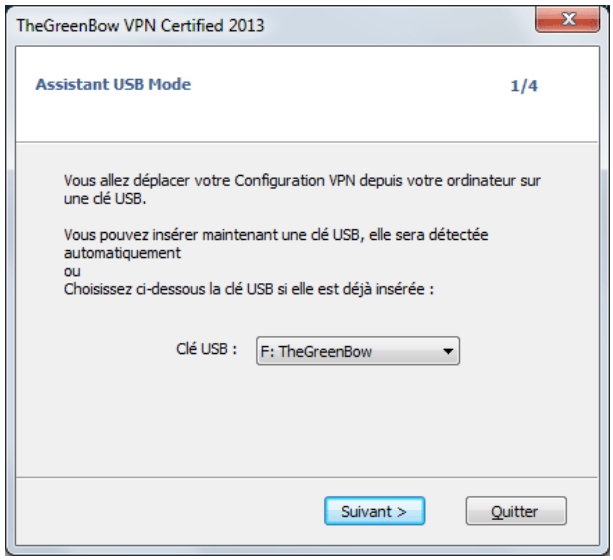
Etape 1 : Choix de la clé USB

L'écran 1 permet de choisir le support amovible (clé USB) sur lequel protéger la politique de sécurité VPN.
Si une clé est déjà insérée, elle est automatiquement présentée dans la liste des clés USB disponibles.
Sinon, il suffit d'insérer à cette étape la clé USB choisie, qui sera détectée automatiquement à l'insertion.

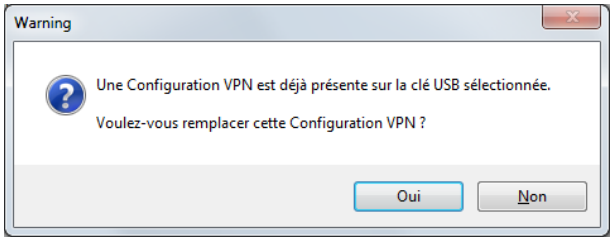
Pas de clé USB insérée



Clé USB déjà insérée



A noter : Le mode USB n'autorise la protection que d'une seule Configuration VPN sur une clé USB. Si une Configuration VPN est déjà présente sur la clé USB insérée, le message d'alerte suivant est affiché :



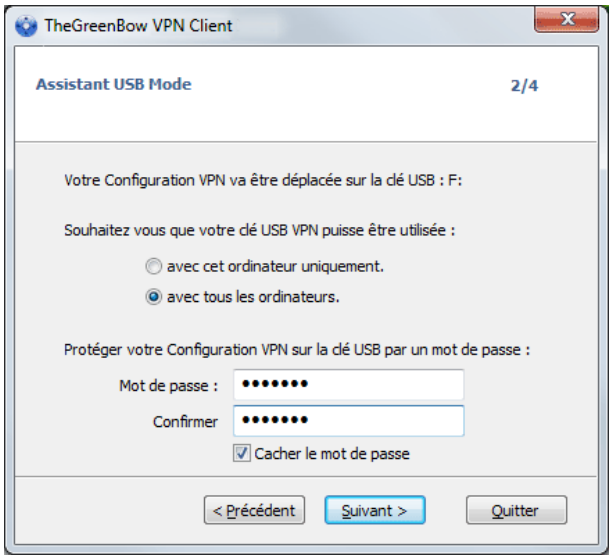
A noter : Lorsqu'une clé USB vierge est insérée et qu'elle est la seule à être insérée sur le poste, l'assistant passe automatiquement à l'étape 2.

Etape 2 : Protection de la politique de sécurité VPN USB

Deux protections sont proposées :

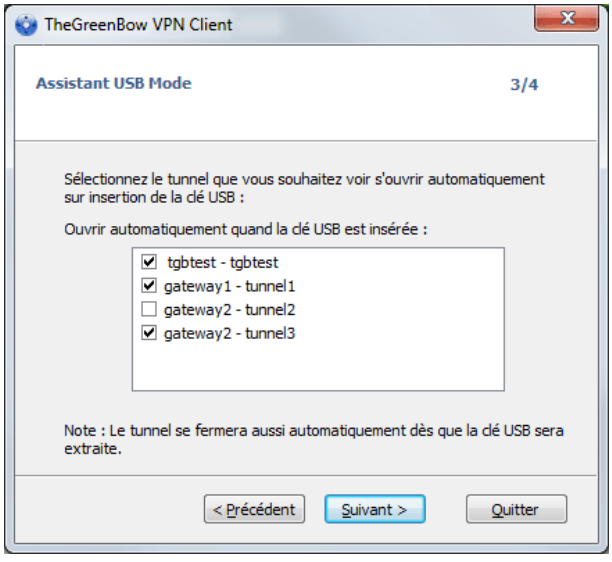
1/ Affiliation au poste de l'utilisateur :
La politique VPN USB peut être associée de façon unique au poste duquel elle est issue.
Dans ce cas, la clé USB VPN ne pourra être utilisée que sur ce poste.
Dans le cas contraire (la clé USB n'est pas associée à un poste en particulier), la clé USB VPN pourra être utilisée sur n'importe quel poste, équipé du Client VPN.

2/ Protection par mot de passe :
La politique de sécurité VPN USB peut être protégée par mot de passe.
Dans ce cas, le mot de passe est demandé à chaque insertion de la clé USB VPN.



Etape 3 : Ouverture automatique du tunnel

L'assistant permet de configurer les connexions VPN qui seront automatiquement ouvertes à chaque insertion de la clé USB VPN.



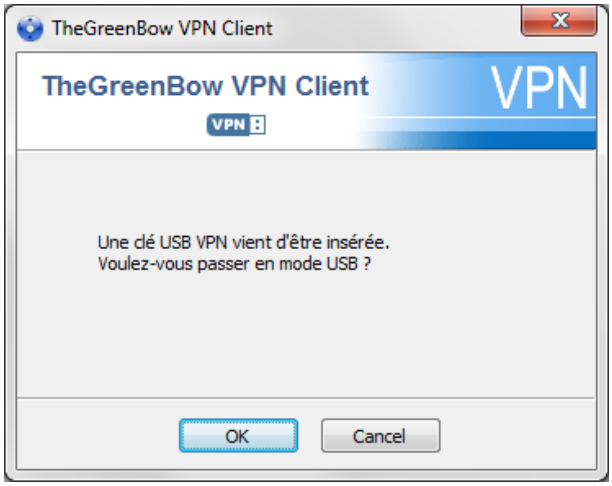
Etape 4 : Résumé

Le résumé permet de valider le bon paramétrage de la Clé USB VPN.

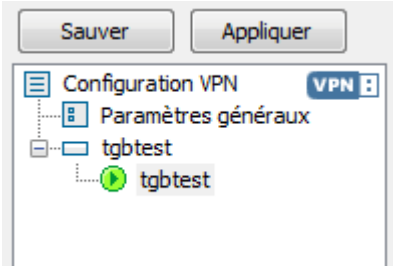
Sur validation de cette dernière étape, la politique de sécurité VPN du poste est transférée sur la Clé USB.
Elle reste active tant que la Clé USB reste insérée. Sur extraction de la Clé USB VPN, le Client VPN revient à une Configuration VPN vide.

20.3 Utiliser le Mode USB

Lorsque le Client VPN TheGreenBow est lancé, avec une politique de sécurité VPN chargée ou pas, insérer la Clé USB VPN. La fenêtre d'information suivante est automatiquement affichée :



Sur validation, la politique VPN USB est automatiquement chargée, et, le cas échéant, le(s) tunnel(s) automatiquement ouvert(s). Le mode USB est identifié dans le Panneau de Configuration, par un icône "Mode USB VPN" en haut à droite de l'arborescence :



Sur extraction de la Clé USB VPN, les connexions VPN USB sont fermées. La politique de sécurité VPN transportée par la clé USB est extraite du poste. (Si une politique de sécurité VPN était présente sur le poste avant insertion de la clé USB, elle est restaurée dans le logiciel).

Remarque : Le Client VPN ne prend en compte qu'une seule clé USB VPN à la fois. Tant qu'une clé USB VPN est insérée, l'insertion d'autres clés USB VPN n'est pas prise en compte.

A noter : La fonction d'importation est désactivée en Mode USB VPN.

En Mode USB VPN, la politique de sécurité VPN USB peut être modifiée. Les modifications apportées à la politique VPN sont sauvegardées sur la Clé USB VPN.

A noter : Le Client VPN ne propose pas d'option directe pour modifier le mot de passe et l'affiliation ou non à un poste.
Pour les modifier, suivre la procédure suivante :
1/ Insérer la clé USB VPN

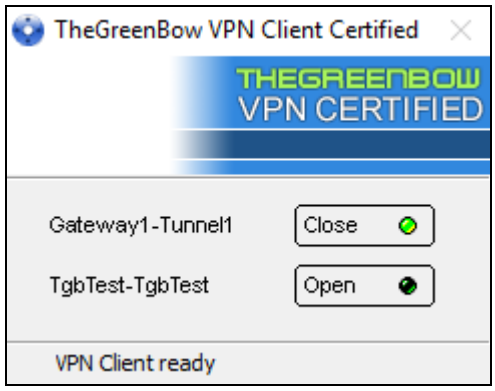
2/ Exporter la Configuration VPN
3/ Extraire la clé USB VPN
4/ Importer la configuration VPN exportée à l'étape 2
5/ Relancer l'assistant mode USB avec cette configuration et les nouveaux paramètres souhaités.

21 Mode GINA

21.1 Le Mode GINA

Le mode GINA permet d'ouvrir des connexions VPN avant le logon Windows.
Cette fonction permet par exemple d'établir une connexion sécurisée vers un serveur de gestion des droits d'accès de façon à obtenir les droits d'accès au poste utilisateur avant l'ouverture de la session utilisateur.

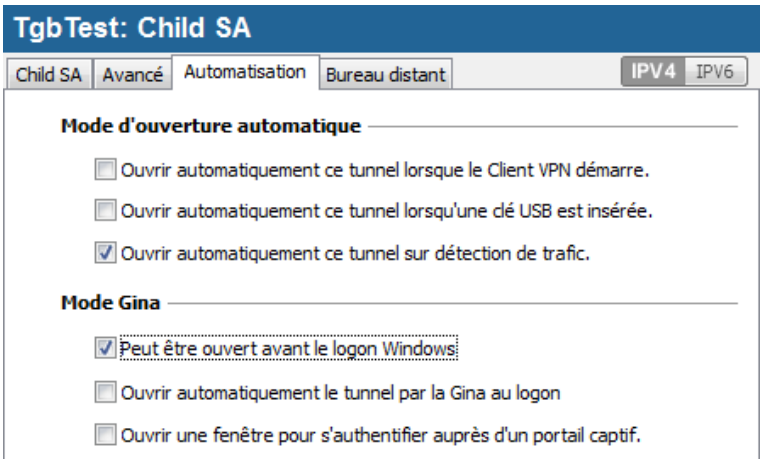
Lorsqu'un tunnel est configuré "en mode GINA", une fenêtre d'ouverture de tunnel similaire au Panneau des Connexions est affichée sur l'écran de logon Windows. Elle permet d'ouvrir manuellement le tunnel VPN.



Comme le panneau des connexions VPN, cette fenêtre permet d'ouvrir manuellement un tunnel.
Un tunnel VPN peut aussi être ouvert automatiquement avant le logon Windows.
Enfin, pour les utilisateurs de connexion Wi-Fi requérant une authentification sur un portail dédié, le Client VPN implémente une fenêtre de navigation automatique permettant l'authentification sur ce portail Wi-Fi captif.

21.2 Configurer le Mode GINA

La configuration d'une connexion VPN en mode GINA s'effectue dans l'onglet "Automatisation" du tunnel concerné. Voir le chapitre "Automatisation"



21.3 Utiliser le Mode GINA

Lorsque le tunnel VPN est configuré en mode GINA, la fenêtre d'ouverture des tunnels GINA est affichée sur l'écran de logon Windows. Le tunnel VPN s'ouvre automatiquement s'il est configuré dans ce sens.

Un tunnel VPN en mode GINA peut parfaitement mettre en œuvre une authentification X-Auth (l'utilisateur doit alors entrer son login / mot de passe), ou une authentification par certificat (L'utilisateur doit alors entrer le PIN code d'accès à la carte à puce).

Avertissement : Si deux tunnels sont configurés en mode GINA, et l'un d'eux en ouverture automatique, il se peut que les deux tunnels s'ouvrent automatiquement.

Remarque : Pour que l'option "Ouvrir automatiquement sur détection de trafic" soit opérationnelle après ouverture de la session Windows, l'option "Peut-être ouvert avant le logon Windows" ne doit pas être cochée.

Limitation : Les scripts, le Mode Config ainsi que le mode USB ne sont pas disponibles pour les tunnels VPN en mode GINA..
De même, un tunnel VPN configuré avec un certificat mémorisé dans le Magasin de Certificats Windows ne fonctionne pas en mode GINA. En effet, le mode GINA est exécuté avant qu'un utilisateur Windows ne soit identifié (hors de toute session utilisateur). Le logiciel ne peut donc pas identifier, dans le Magasin de Certificats Windows, le magasin utilisateur qui doit être utilisé.

Considération de sécurité

Un tunnel configuré en mode Gina peut être ouvert avant le logon Windows, donc par n'importe quel utilisateur du poste. Il est donc fortement recommandé de configurer une authentification, si possible forte, pour un tunnel en mode Gina, par exemple une authentification X-Auth, ou de préférence une authentification par Certificat, si possible sur support amovible. Voir le chapitre Configurer la Phase 1 : Authentification.

⚠ Point de sécurité : la fonction d'ouverture d'une fenêtre pour l'authentification auprès d'un portail captif est susceptible d'être vulnérable à certaines attaques (Cf. vulnérabilité 2018_7300). Pour des raisons de sécurité, cette fonction n'est pas proposée dans la version TheGreenBow VPN Certified. Veuillez Nous contacter si elle est nécessaire à votre utilisation du logiciel.

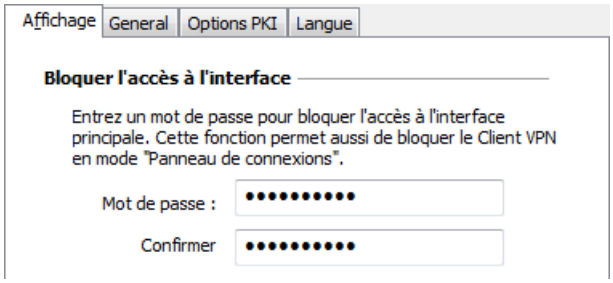
22 Contrôle d'accès à la politique VPN

Tout accès à la politique de sécurité VPN (lecture, modification, application, importation, exportation) est protégé par un mot de passe. Cette protection vaut aussi pour les opérations réalisées via la ligne de commande.

Afin de garantir l'intégrité et la confidentialité de la politique de sécurité VPN, l'accès à cette politique est systématiquement protégé par mot de passe dans le logiciel TheGreenBow VPN Certified. A la fin d'une installation par défaut, ce mot de passe vaut "admin". Il est fortement recommandé de le modifier.

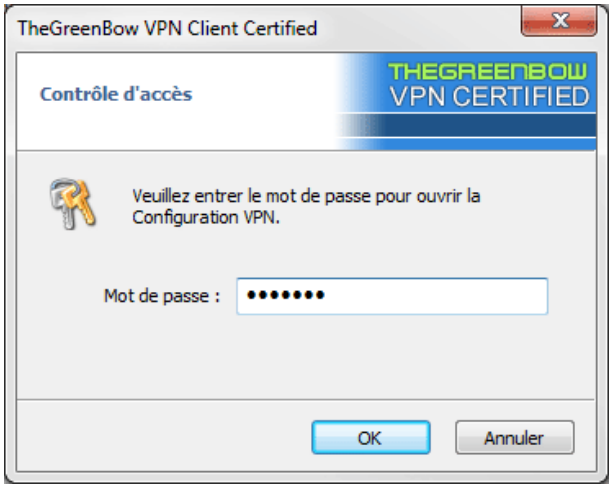
Il est fortement recommandé de configurer un mot de passe suffisamment fort, et pour ce faire, de respecter les règles de constitution du mot de passe indiquée le document ANSSI "Recommandations de sécurité relatives aux mots de passe". Il est par exemple recommandé de choisir un mot de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

La protection de la politique de sécurité VPN est configurée via le menu " Outils > Options ", onglet "Affichage".



Dès qu'un mot de passe est configuré, l'ouverture du Panneau de Configuration et l'accès à la politique de sécurité VPN (importation, remplacement, ajout) sont toujours conditionnés par la saisie de ce mot de passe :

- quand l'utilisateur clique sur l'icône en barre des tâches
- quand l'utilisateur sélectionne le menu "Panneau de Configuration" du menu de l'icône en barre des tâches
- quand l'utilisateur clique sur le bouton "Panneau de Configuration" du Panneau des Connexions
- lors de l'importation via la ligne de commande d'une nouvelle politique de sécurité VPN
- au cours d'une mise à jour du logiciel



En associant cette option aux autres options de limitation de l'affichage du logiciel, l'administrateur peut configurer le logiciel en mode quasi-invisible et non-modifiable. Voir le chapitre sur les options d'affichage.

Pour supprimer la protection par mot de passe, vider les deux champs "Mot de passe" et "Confirmer" puis valider (cette possibilité n'est pas disponible dans la version TheGreenBow VPN Certified, où le mot de passe est systématiquement configuré. Dans cette version, vider les deux champs ramène le mot de passe à sa valeur par défaut "admin").

Note à destination de l'administrateur : La protection de la politique de sécurité VPN peut aussi être configurée en ligne de commande de l'installation. Cette option est décrite dans le "Guide de Déploiement VPN" (tgbvpn_ug_deployment_fr).

23 Options

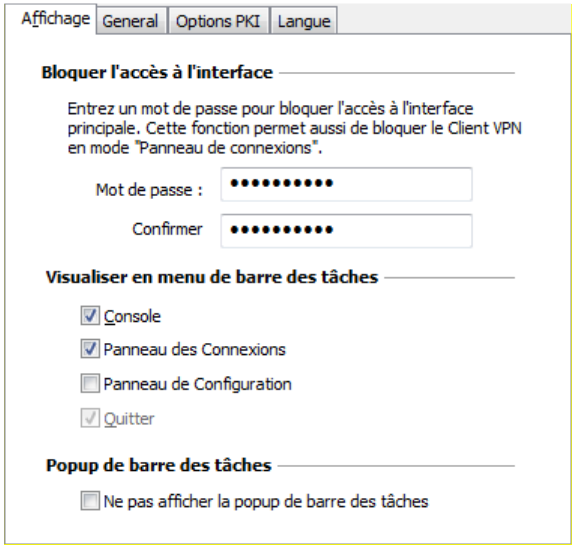
23.1 Contrôle d'accès

Voir le chapitre "Contrôle d'accès à la politique de sécurité VPN".

23.2 Affichage de l'interface (masquage)

Les options de l'onglet "Affichage" de la fenêtre "Options" permettent de masquer toutes les interfaces du logiciel, en enlevant du menu en barre des tâches les items "Console", "Panneau de Configuration" et "Panneau des Connexions". Le menu en barre des tâches peut ainsi se réduire à l'item "Quitter".

La fenêtre popup d'ouverture et de fermeture du tunnel peut aussi être masquée (Popup de barre des tâches)



Note à destination de l'administrateur : Dans le cadre du déploiement du logiciel, toutes ces options peuvent être préconfigurées au cours de l'installation du logiciel Client VPN TheGreenBow. Ces options sont décrites dans le document "Guide de Déploiement" (tgbvpn_ug_deployment_fr.pdf)

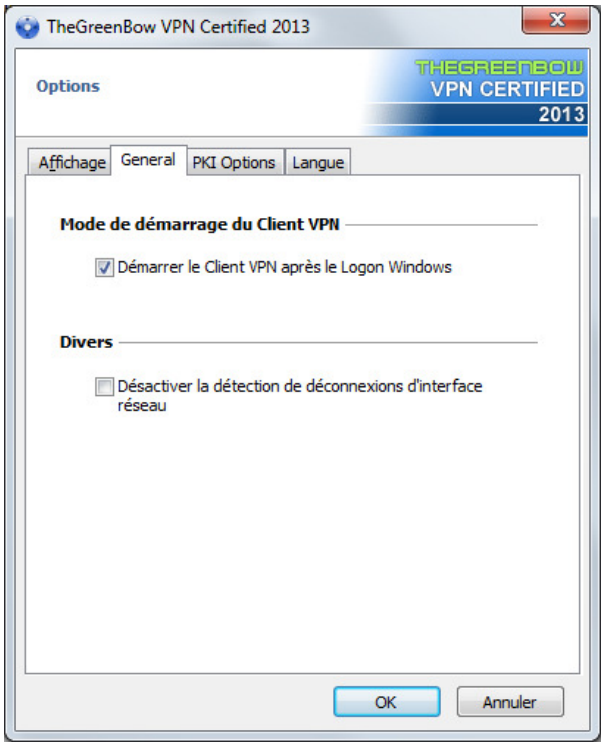
L'item "Quitter" du menu en barre des tâches ne peut être supprimé via le logiciel. Il peut toutefois être supprimé en utilisant les options d'installation (Cf. Guide de Déploiement)

23.3 Général

23.3.1 Mode de démarrage du Client VPN

Lorsque l'option "Démarrer le Client VPN après le logon Windows" est cochée, le Client VPN démarre automatiquement à l'ouverture de la session utilisateur.

Si l'option est décochée, l'utilisateur doit lancer manuellement le Client VPN, soit par double-clic sur l'icône du bureau, soit en sélectionnant le menu de lancement du logiciel dans le menu "Démarrer" Windows.
Cf. chapitre "Bureau Windows".



23.3.2 Désactiver la détection de déconnexion

Dans son comportement standard, le Client VPN ferme le tunnel VPN (de son côté), dès lors qu'il constate un problème de communication avec la passerelle VPN distante.

Pour des réseaux physiques peu fiables, sujets à des micro-déconnexions fréquentes, cette fonction peut présenter des inconvénients (qui peuvent aller jusqu'à l'impossibilité d'ouvrir un tunnel VPN).

En cochant la case "Désactiver la détection de déconnexion", le Client VPN évite de fermer les tunnels dès qu'une déconnexion est constatée. Cela permet de garantir une excellente stabilité du tunnel VPN, y compris sur des réseaux physiques peu fiables, typiquement les réseaux wireless de type Wi-Fi, 3G, 4G, ou satellite.

23.4 Options IGC / PKI

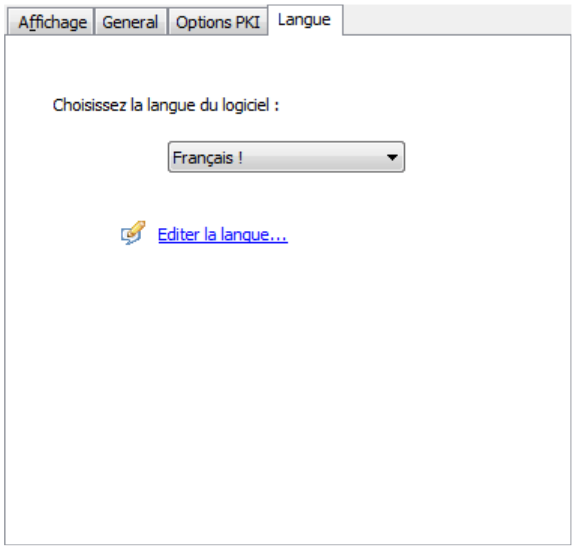
Cf. chapitre 17.4 "Options PKI : Caractériser le certificat et son support".

23.5 Gestion des langues

23.5.1 Choix d'une langue

Le Client VPN TheGreenBow peut être exécuté en plusieurs langues.
Il est possible de changer de langue en cours d'exécution du logiciel.

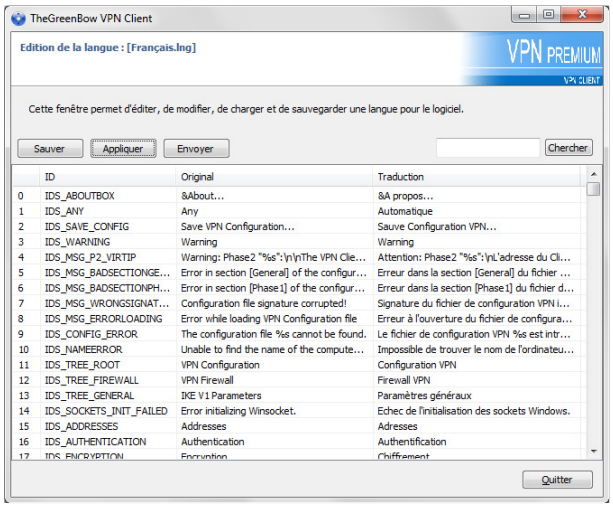
Pour choisir une autre langue, ouvrir le menu " Outils > Options " et sélectionner l'onglet "Langue".
Choisir la langue souhaitée dans la liste déroulante proposée :



La liste des langues disponibles en standard dans le logiciel est donnée en annexe au chapitre "Liste des langues disponibles"

23.5.2 Modification ou création d'une langue

Le Client VPN TheGreenBow permet aussi de créer une nouvelle traduction ou d'effectuer des modifications sur la langue utilisée, puis de tester ces modifications dynamiquement, via un outil de traduction intégré.
Dans l'onglet "Langue", cliquer sur le lien "Editer la langue…", la fenêtre de traduction est affichée :



La fenêtre de traduction est partagée en 4 colonnes qui indiquent respectivement le numéro de la chaîne de caractère, son identifiant, sa traduction dans la langue d'origine, et sa traduction dans la langue choisie.

La fenêtre de traduction permet :
1/ De traduire chaque chaîne de caractère en cliquant sur la ligne correspondante
2/ De rechercher une chaîne de caractère donnée dans n'importe quelle colonne du tableau (champ de saisie "Chercher", puis utiliser la touche "F3" pour parcourir toutes les occurrences de la chaîne de caractères recherchée)
2/ De sauvegarder les modifications (bouton "Sauver").
Toute langue modifiée ou créée est sauvegardée dans un fichier ".lng".
3/ D'appliquer immédiatement une modification au logiciel : cette fonction permet de valider en temps réel la pertinence d'une chaîne de caractère ainsi que son bon affichage (bouton "Appliquer").
4/ D'envoyer à TheGreenBow une nouvelle traduction (bouton "Envoyer").

Le nom du fichier de langue en cours d'édition est rappelé dans l'entête de la fenêtre de traduction.

A noter : Toute traduction envoyée à TheGreenBow est publiée, après vérification, sur le site TheGreenBow, puis intégrée dans le logiciel, en général dans la version officielle publiée, suivant la réception de la traduction.

Remarque :
Les caractères ou suites de caractères suivantes ne doivent pas être modifiées au cours de la traduction :

"%s"	sera remplacé par le logiciel par une chaîne de caractères
"%d"	sera remplacé par le logiciel par un nombre
"\n"	indique un retour chariot
"&"	indique que le caractère suivant doit être souligné
"%m-%d-%Y"	indique un format de date (ici le format américain : mois-jour-année). Ne modifier ce champ qu'en connaissance du format dans la langue traduite.

La chaîne "IDS_SC_P11_3" doit être reprise sans modification.

24 Mode traçant et Console

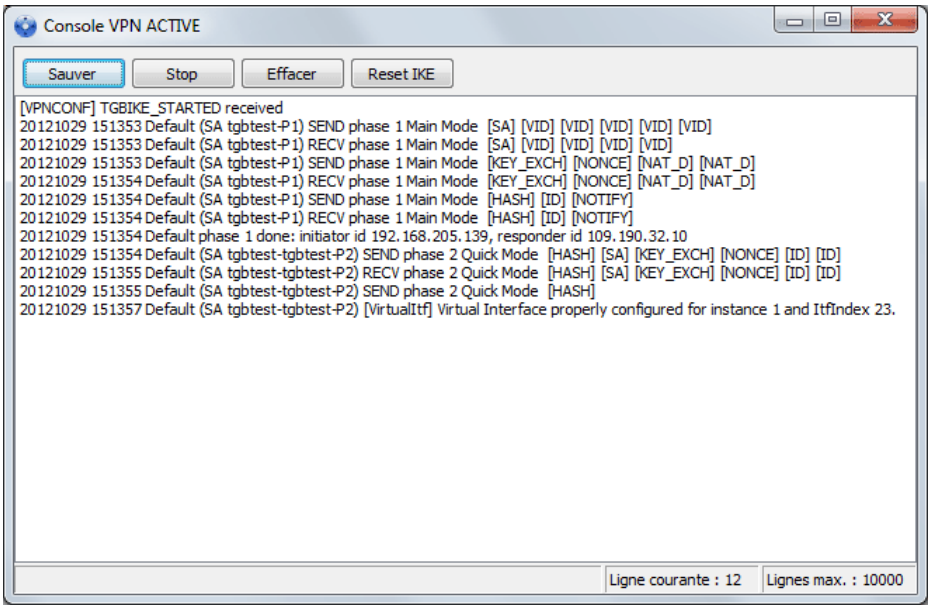
Le Client VPN TheGreenBow propose deux outils de génération de traces :

1/ La "Console" détaille les informations et les étapes des ouvertures et fermeture des tunnels (messages IKE pour la plupart)

2/ Le mode "traçant" fait produire par chaque composant du logiciel le log de son activité.
Ces deux outils ont pour but d'aider l'administrateur réseau à diagnostiquer un incident dans l'ouverture des tunnels, ou le support TheGreenBow dans l'identification d'incidents du logiciel.

24.1 Console

La Console peut être affichée par les moyens suivants :
- Menu "Outils > Console" du Panneau de Configuration (interface principale)
- Raccourci CTRL+D lorsque le Panneau de Configuration est ouvert
- Dans le menu du logiciel en barre des tâches, sélectionner "Console"



Les fonctions de la Console sont les suivantes :
- Sauver : Sauvegarde dans un fichier la totalité des traces affichées dans la fenêtre
- Start / Stop : Démarre / arrête la capture des traces
- Effacer : Efface le contenu de la fenêtre
- Reset IKE : Redémarre le service IKE

24.2 Mode traçant

Le mode traçant est activé par le raccourci : CTRL+ALT+T

Le passage en mode traçant ne nécessite pas de redémarrer le logiciel.

Lorsque le mode traçant est activé, chaque composant du Client VPN TheGreenBow génère les logs de son activité. Les logs générés sont mémorisés dans un dossier accessible en cliquant sur l'icône "Dossier" bleu dans la barre d'état du Panneau de Configuration (interface principale).

Note à destination de l'administrateur : L'activation des logs ne peut se faire que depuis le panneau de configuration, dont l'accès peut être strictement réservé à l'administrateur.
Même si les logs ne contiennent pas d'information sensible, il est recommandé que, lorsqu'ils sont activés par l'administrateur, celui-ci veille à ce qu'ils soient désactivés, et si possible supprimés, lorsqu'il quitte le logiciel.

25 Recommandations de sécurité

25.1 Certification

Le Client VPN **TheGreenBow VPN Certified** est le premier Client VPN IPsec TheGreenBow certifié selon les Critères Communs au niveau EAL3+, et qualifié au niveau standard.

Le Client VPN **TheGreenBow VPN Certified** est certifié sur les plates-formes Windows 7 32/64bit et Windows 10 32/64bit.

La version du Client VPN **TheGreenBow VPN Certified** objet de ce guide utilisateur est la version 6.52.006. Cette version peut être vérifiée dans la fenêtre "A propos..." du logiciel, Cf. chapitre 11.

25.2 Recommandations

Les recommandations suivantes s'adressent à l'Administrateur du logiciel.

25.2.1 Recommandations générales

Afin de garantir un niveau de sécurité approprié, les conditions de mise en œuvre et d'utilisation suivantes doivent être respectées :

- L'administrateur système et l'administrateur sécurité chargés respectivement de l'installation du logiciel et de la définition des politiques de sécurité VPN sont considérés de confiance.
- L'utilisateur du logiciel est une personne formée à son utilisation. En particulier, elle ne doit pas divulguer les informations utilisées pour son authentification auprès du système de chiffrement.
- La passerelle VPN à laquelle se connecte le Client VPN permet de tracer l'activité VPN et permet de remonter le cas échéant les dysfonctionnements ou les violations des politiques de sécurité.
- Le poste de l'utilisateur est sain et correctement administré. Il dispose d'un anti-virus à jour et est protégé par un pare-feu.
- Les bi-clés et les certificats utilisés pour ouvrir le tunnel VPN, sont générés par une autorité de certification de confiance.

25.2.2 Précaution de mise en œuvre

La machine sur laquelle est installé et exécuté le logiciel Client VPN 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 (cloisonner ou filtrer) 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).

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

En particulier, il est recommandé de mettre en place une politique de filtrage des flux entrants sur le poste sur lequel est installé le Client VPN, de manière à interdire les accès distants au logiciel.

25.2.3 Administration du Client VPN

Il est vivement recommandé de protéger l'accès à la politique de sécurité VPN par un mot de passe, et de limiter la visibilité du logiciel à l'utilisateur final, comme détaillé au chapitre "Contrôle d'accès à la politique VPN".
A noter que dans la version TheGreenBow VPN Certified, la protection de l'accès à la politique de sécurité VPN est systématique et non débrayable.

Il est fortement recommandé de configurer un mot de passe suffisamment fort, et pour ce faire, de respecter les règles de constitution du mot de passe indiquée le document ANSSI "Recommandations de sécurité relatives aux mots de passe". Il est par exemple recommandé de choisir un mot de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Il est aussi recommandé de définir cette protection au moment de l'installation, via les options d'installation décrites dans le document "Guide de Déploiement" (tgbvpn_ug_deployment_fr.pdf)

Il est recommandé de veiller à ce que les utilisateurs utilisent le Client VPN dans un environnement "utilisateur", et d'essayer autant que possible, de limiter l'utilisation du système d'exploitation avec des droits administrateur.

Il est recommandé de conserver le mode "Démarrage du Client VPN avec la session Windows" (après le logon Windows), qui est le mode d'installation par défaut.

Enfin, il est à noter que 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).

25.2.4 Configuration de la politique de sécurité VPN

Données sensibles dans la politique de sécurité VPN

Il est recommandé de ne mémoriser aucune donnée sensible dans le fichier de configuration VPN.

A ce titre, il est recommandé de ne pas utiliser les facilités suivantes offertes par le logiciel :

1/ Ne pas mémoriser le login / mot de passe EAP dans la configuration (fonction décrite au chapitre "IKE Auth : IKE SA", section "Authentification")

2/ Ne pas importer de certificat dans la configuration (fonction décrite au chapitre "Importer un certificat"), et privilégier l'utilisation de certificats stockés sur support amovible (token) ou dans le Magasin de Certificats Windows.

3/ Ne pas utiliser le mode "Clé partagée" (fonction décrite au chapitre "IKE Auth : IKE SA") et privilégier le mode "Certificat" avec des certificats stockés sur support amovible (token) ou dans le magasin de certificat Windows.

4/ Ne pas exporter la politique de sécurité VPN en clair, c'est-à-dire non protégée par un mot de passe (fonction décrite au chapitre "Exporter une politique de sécurité VPN")

Authentification de l'Utilisateur

Les fonctions d'authentification de l'utilisateur proposées par le Client VPN sont décrites ci-dessous, de la plus faible à la plus forte.

En particulier, il est à noter qu'une authentification par clé partagée (pre-shared key), si elle est facile à mettre en œuvre, permet néanmoins à tout utilisateur ayant accès au poste, de monter un tunnel, sans vérification d'authentification.

Type d'authentification de l'utilisateur	Force
Clé partagée	faible
X-Auth statique	
X-Auth dynamique	
Certificat mémorisé dans la politique de sécurité VPN	
Certificat dans le Magasin de Certificat Windows	
Certificat sur Carte à puce ou sur Token	forte

Authentification de la Passerelle VPN

Il est recommandé de mettre en œuvre la vérification du certificat de la Passerelle VPN, tel que décrit au chapitre 3.2 "Options PKI" du document "Gestion des PKI, certficats, token et cartes à puce" (tgbvpn_ug_pki_smartcard_fr).

⚠ Dans cette configuration, pour éviter toute exploitation de la vulnérabilité 2018_7293, le logiciel impose de renseigner le champ "Remote ID" du tunnel VPN concerné avec le sujet du certificat de la Passerelle VPN.

Protocole IKE

La certification du logiciel TheGreenBow VPN Certified porte sur le protocole IKEv2 exclusivement.
Il est recommandé de ne configurer que des tunnels IKEv2.

Mode "tout dans le tunnel" et "split tunneling"

Il est recommandé de configurer le tunnel VPN en mode "tout le trafic dans le tunnel" avec le mode "bloquer les flux non chiffrés" (split tunneling) activé.
Cf. chapitre 13.4.5 "Child SA : Child SA" et 13.4.6 "Child SA : Avancé".

Mode Gina

Il est recommandé d'associer une authentification forte à tout tunnel en mode Gina.

Algorithmes cryptographiques et longueur de clés

Dans le cadre de l'utilisation du Client TheGreenBow VPN Certified, et pour utiliser le logiciel conformément à l'annexe B-1 du RGS 2.0, il est recommandé de choisir les algorithmes suivants :

IKEv2	Chiffrement	AES128 minimum, AES192 ou AES256
	Authentification	SHA2 256 minimum, ou SHA2 384 ou SHA2 512
	Groupe de clé	DH15 (3072) minimum, ou DH16 (4096), DH17 (6144), DH18 (8192)
ESP	Chiffrement	AES128 minimum, AES192 ou AES256
	Intégrité	SHA2 256 minimum, ou SHA2 384 ou SHA2 512
	Diffie-Hellman	DH15 (3072) minimum, ou DH16 (4096), DH17 (6144), DH18 (8192)

Certificat

Le logiciel TheGreenBow VPN Certified permet l'utilisation de certificats, et en vérifie la validité, mais il ne permet pas leur génération. La génération des certificats, et en particulier la qualité et la conformité de ces certificats aux recommandations de l'ANSSI (RGS 2.0) est du ressort du Gestionnaire de l'IGC/PKI de l'entreprise concernée.
En particulier, il est recommandé que la durée de vie du certificat soit inférieure à 5 ans et que l'algorithme de signature du certificat soit d'une qualité suffisante.

Les certificats manipulés par le Client VPN doivent posséder des dates de validité au format UTCTime.

Recommandations de configuration IPsec de l'ANSSI

Les recommandations décrites ci-dessus peuvent être complétées par le document de configuration IPsec rédigé par l'ANSSI : Recommandations de sécurité relatives à IPsec pour la protection des flux réseau.

26 FAQ, troubleshooting

Ce chapitre présente la liste des problèmes fréquemment rencontrés, ainsi que leur résolution.
Consulter le site : http://www.thegreenbow.fr/vpn_faq.html pour avoir la dernière version de cette liste.

26.1 Client VPN TheGreenBow

26.1.1 Quelles versions de Windows sont supportées par le Client VPN TheGreenBow ?

- Windows 7 32/64-bit
- Windows 8 32/64-bit
- Windows 8.1 32/64-bit
- Windows 10 32/64-bit
- Windows Server 2008 32/64-bit
- Windows Server 2012 32/64-bit

Anciennes versions de Windows

Télécharger ici les versions du Client VPN disponibles pour les anciennes versions de windows :

Windows XP /Server 2003	VPN Client 5.55
Windows 2000 Server	VPN Client 4.51
Windows 98	VPN Client 3.11

26.1.2 Langues disponibles pour le Client VPN TheGreenBow

Le Client VPN TheGreenBow est disponible en plusieurs langues (Allemand, Anglais, Espagnol, Français, Portugais, etc.).
La langue est choisie durant l'installation du Client VPN TheGreenBow.

Vous pouvez aussi contribuer aux traductions du logiciel via la page de traduction du logiciel VPN.

26.1.3 Quels sont les passerelles/routeurs VPN compatibles ?

Le client de TheGreenBow IPsec VPN est compatible avec tous les routeurs IPsec conformes aux normes IKE et IPsec.
Visitez la liste des routeurs VPN qualifiés, qui augmente chaque jour, pour trouver votre routeur VPN.

Si l'équipement que vous recherchez n'est pas contenu dans cette liste, contactez notre support technique et nous travaillerons avec vous pour le qualifier.

26.1.4 Comment connecter le Client VPN à un Routeur VPN Linksys ?

Nous fournissons des Guides de Configuration VPN pour la plupart des passerelles et routeurs que nous avons qualifiés.
Ces guides de configuration VPN sont rédigés par notre équipe de qualification ou par nos partenaires.

Les routeurs Linksys en font partie: les modèles Linksys RV082, BEFVP41 et Linksys WRV54G sont supportés. Vous pouvez aussi consulter notre faq Linksys WRV54G.

26.1.5 Comment configurer le Client VPN pour un Routeur VPN Cisco ?

Nous fournissons des Guides de Configuration VPN pour la plupart des passerelles et routeurs que nous avons qualifiés. Ces guides de configuration VPN sont rédigés par notre équipe de qualification ou par nos partenaires.

Les routeurs Cisco en font partie: Les routeurs Cisco PIX501, Cisco ASA 5510, Cisco PIX 506-E, Cisco 871 et Cisco 1721 sont supportés.

26.1.6 Le NAT Traversal est il supporté par le Client VPN ?

Oui. Le Client VPN TheGreenBow supporte NAT Traversal Draft 1 (enhanced), Draft 2 and 3 (full implementation). IP address emulation.

- Incluant le support NAT_OA
- Incluant NAT keepalive
- Incluant NAT-T mode agressif

26.1.7 Le Client VPN TheGreenBow supporte-t il DNS/WINS discovering ?

Le Client VPN TheGreenBow supporte le Mode-Config. Le "Mode Config" est une extension de Internet Key Exchange (IKE) qui permet de récupérer certains paramètres réseau comme les adresses IP des serveurs DNS/WINS depuis la gateway distante et de les utiliser dans la configuration VPN du Client VPN. Si le "Mode Config" n'est pas supporté par la gateway distante, le Client VPN permet aussi la configuration manuelle des serveurs DNS/WINS de l'entreprise.

26.1.8 Le Client VPN est-il compatible avec le routeur Wi-Fi Linksys WRV54G ?

Le Client VPN TheGreenBow est qualifié avec le routeur Linksys WRV54G firmware 2.37 et suivants. N'hésitez à télécharger le Guide de Configuration VPN du routeur Linksys WRV54G.

Le Firmware 2.25.2 du routeur Linksys WRV54G n'accepte pas les connexions IPsec d'un Client VPN avec des adresses IP dynamiques. Cependant, il y a un contournement possible. Vous devez configurer l'adresse IP du client VPN dans la configuration du Linksys WRV54G. Linksys a produit un firmware plus récent depuis, que vous pourrez télécharger ici.

Le Client VPN TheGreenBow est aussi qualifié avec les routeurs Linksys RV082 et Linksys BEFVP41 (voir aussi la Liste de Routeurs VPN qualifiés ou télécharger les Guides de Configuration VPN).

26.1.9 Quel ports sont utilisés par le Client VPN TheGreenBow ?

Les ports UDP 500 et UDP 4500 doivent être ouverts et le protocole ESP (protocol number 50) doit être autorisé.

Voir aussi nos autres FAQs :
Comment configurer les connexions VPN et les ports VPN pour les utilisateurs dans des hôtels ou de bornes wifi ?
Impossible d'ouvrir le tunnel sous Vista, problème avec le Firewall Vista ?
Peut on modifer le port IKE ?

26.1.10 Le Client VPN TheGreenBow et Microsoft ISA Server 2000 & 2004 ?

D'aprés le support technique de Microsoft, dans la plupart des cas, le trafic VPN IPsec ne traverse pas le serveur ISA 2000.

Pour plus de détails au sujet du serveur 2004 d'ISA, vous pouvez consulter la page suivante: Q838379 dans la base de connaissance Microsoft.

26.1.11 Que doit-on remplir dans le champ "Adresse Client VPN" en Phase 2 ?

Ce champ est l'adresse IP virtuelle que le Client VPN aura à l'intérieur du réseau distant. Paradoxalement, avec la plupart des routeurs VPN, cette adresse ne doit pas appartenir au réseau distant.
Par exemple, si vous utilisez un routeur VPN avec un réseau 192.168.0.0/255.255.255.0, vous devrez la plupart du temps, spécifier une adresse virtuelle du type 192.168.100.1 ou 10.10.10.1 dans le champ "Adresse Client VPN".

En effet, si vous choisissez une adresse IP appartenant au réseau distant, par exemple 192.168.0.200, le Client VPN essaiera de communiquer avec une machine cible du "même" réseau, par exemple 192.168.0.53. Cette machine cible, en tentant de lui répondre, enverra avant tout une requête ARP afin d'obtenir l'adresse MAC (physique) du Client VPN. Or, le Client VPN n'étant pas physiquement connecté au réseau, il n'a pas d'adresse MAC déclarée sur le réseau. Donc la machine cible ne pourra pas répondre au Client VPN. A l'inverse, si le Client VPN a une adresse IP virtuelle n'appartenant pas au réseau distant, la machine cible cherchera (et trouvera) l'adresse MAC d'un routeur capable de sortir du réseau (vraisemblablement le routeur VPN concerné).

Ainsi, il n'est possible de spécifier une adresse IP virtuelle appartenant au réseau distant que si le routeur VPN utilisé sait gérer les requêtes ARP émises dans le contexte décrit ci-dessus.

Pour plus d'information, télécharger le Guide Utilisateur du Client VPN TheGreenBow.

26.1.12 Peut on rendre l'interface utilisateur invisible ?

Il est possible de rendre invisible le Client VPN . Vous devez télécharger la procédure décrite dans le document : VPN Deployment Guide

26.1.13 Le Client VPN est-il compatible avec les Linksys WRVS4400N / WRV200 ?

Oui, le Client VPN TheGreenBow est certifié avec les routeurs Linksys WRVS4400N ou WRV200 (voir aussi Liste Routeurs VPN Certifiés ou télécharger les Guides de Configuration).

26.1.14 Est il possible de définir une gateway de secours ?

Oui. Il est possible de définir une gateway de secours ou Redundant Gateway. La fonctionnalité de Redundant Gateway permet d'offrir aux utilisateurs mobiles un access au réseau d'entreprise plus disponible et plus simple utilisation. Le Client VPN TheGreenBow peut ouvrir un tunnel VPN IPsec avec la gateway de secours dans le cas ou la gateway principale est inaccessible ou non opérationnelle. L'indisponibilité est détectée par la fonction "Dead Peer Detection" ou DPD.

26.1.15 Peut on modifer le port IKE ?

Oui. Un port IKE spécifique peut être défini. Pour ce faire, allez dans le menu 'Paramètres' globaux dans le panneau de configuration et entrer le port dans le champ 'Port IKE'.

Voir aussi nos autres FAQs :
Comment configurer les connexions VPN et les ports VPN pour les utilisateurs dans des hôtels ou de bornes wifi ?
Impossible d'ouvrir le tunnel sous Vista, problème avec le Firewall Vista ?

26.1.16 A quoi correspondent les exécutables TgbStarter.exe et Tgblke.exe ?

TgbStarter.exe et Tgblke.exe sont des composants du Client VPN TheGreenBow.

- TgbStarter.exe est le composant "daemon" du logiciel. Il est exécuté en tant que service.
- Tgblke.exe est le composant IKE/IPsec du logiciel.

L'activation du logiciel a échoué.
Lorsque j'essaye d'activer le logiciel, j'obtiens une erreur d'activation.

Veuillez vous reporter à notre guide complet concernant l'activation sur notre guide d'activation en ligne.

Vous pouvez aussi activer votre logiciel à tout moment, en suivant la procédure d'activation manuelle décrite sur ce lien : Activation manuelle.

26.1.17 Existe-t il une configuration VPN à utiliser pour tester le Client VPN ?

Une configuration VPN a été conçue par l'équipe technique de TheGreenBow pour se connecter à nos passerelles VPN IPsec en ligne et aux serveurs. Accessible en permanence, vous pouvez l'utiliser pour tester votre environnement réseaux à tout moment. Cette configuration de test est intégrée dans le Client VPN TheGreenBow. Consultez l'aide en ligne ou téléchargez le fichier de configuration ci-dessous.

Configuration VPN pour VPN Client IKEv1 (tgbvpn_demo.tgb)

Configuration VPN pour VPN Client IKEv2 (standard, Premium ou Certifié) (tgbvpn_demo_IKEv2.tgb)

26.1.18 Est-il possible d'avoir des licences temporaires pour test ?

TheGreenBow peut fournir des licences temporaires permettant de poursuivre les tests du logiciel au delà de la période d'évaluation de 30 jours. Ces licences temporaires peuvent durer plusieurs semaines. Pour plus de détails, contacter notre équipe commerciale.

26.1.19 Est-il possible d'ouvrir automatiquement mon CRM quand le tunnel est ouvert ?

Le Client VPN TheGreenBow permet de configurer l'exécution automatique de scripts dès que le tunnel est ouvert, ou lorsqu'il vient de se fermer. Il suffit de choisir l'application à lancer avant ou aprè l'ouverture ou la fermeture du tunnel et de la configurer dans l'onglet "scripts" du tunnel concerné.

Exemple de scripts pouvant être configurés :

- Accès à l'intranet de l'entreprise
- Ouverture automatique de l'outil CRM dès que le tunnel est ouvert
- Vérification de l'état du poste avant ouverture du tunnel
- Transmission automatique dans le tunnel de l'état du poste au système de gestion de la sécurité de l'entreprise (SIEM)
- Mémorisation de paramètres avant ouverture du tunnel, et restauration de ces paramètres après la fermeture
- etc.

26.1.20 Le Client VPN est-il compatible avec les moyens d'authentification à deux facteurs ?

Oui. Le Client VPN TheGreenBow est compatible avec les fonctions d'authentification à deux facteurs et bidirectionnelle pour stocker les utilisateurs, les qualifications personnelles telles que des clefs privées, des mots de passe et des certificats numériques. Veuillez vous référer à la liste des Tokens qualifiés.

26.1.21 Connexion VPN à un domaine Windows avant le Logon Windows ?

Le Client VPN TheGreenBow permet d'établir une connexion VPN avant le logon Windows, par exemple pour ouvrir une connexion sécurisée vers un domaine Windows. Tout tunnel VPN peut être configuré pour pouvoir être ouvert avant le logon Windows, dans l'onglet "Automatisation" du tunnel, en cochant la case : "Peut être ouvert avant le logon Windows". Cette fonction est décrite dans le Guide Utilisateur du Client VPN au chapitre "Mode GINA".

26.1.22 Comment configurer une connexion VPN dans un hôtel ou vers une borne wifi ?

Pour plus d'informations sur la négociation de NAT Transversal dans IKE, voir IETF RFC 3948 (UDP Encapsulation of IPsec Packets), IETF RFC 3947 (Negotiation of NAT-Traversal in the IKE) ou le mémo "draft-ietf-ipsec-nat-t-ike-08". Regarder aussi la liste des ports TCP et UDP.

La table ci-dessous décrit les phases de négociation dans la connexion VPN et les ports VPN par défaut quand le client VPN est derrière un routeur :

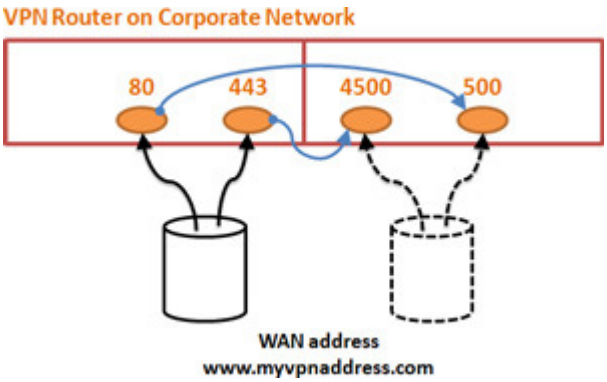
Phase	Port par défaut	Où modifier les ports ?
Phase 1	UDP Port 500	Paramètres généraux > Port IKE
Phase 2	UDP Port 4500	Paramètres généraux > Port NAT
Trafic IPsec	Reste sur le dernier port défini	

Dans certains hôtels, points wifi ou aéroports, les ports UDP 500 et 4500 pour le trafic sortant peuvent être bloqués, pour empêcher toute connexion étrangère à votre réseau. Il est donc nécessaire de configuer les ports IKE ET NAT-T en conséquence.

Voici un exemple de port VPN alternatif dans le panneau de configuration (Rappelez vous que cela affecte uniquement le protocole UDP):

Port IKE	Port NAT-T
80	443

Si vous décidez d'utiliser d'autres ports VPN que ceux par défaut (UDP 500 et UDP 4500), le routeur de destination (celui en entrée de votre réseau d'entreprise) doit être configuré pour rediriger le trafic entrant associé aux nouveaux ports VPN sélectionnés sur les ports par défaut UDP 500 et UDP 4500 pour qu'ils acheminent correctement jusqu'au service IPsec. Voir le diagramme ci-dessus, par exemple, sachant que certains modèles de routeur ne fournissent pas la capacité de rediriger les ports vers eux-mêmes et deux routeurs peuvent être nécessaires :



Voici un fichier de configuration de Parefeu Linux lorsque votre routeur ne permet pas de rediriger les ports vers lui-même et que vous voulez ajouter un front-end firewall :

firewall-reroute-port.sh

26.1.23 Est-il possible d'utiliser des certificats utilisateurs depuis le magasin Windows ?

Est-il possible d'utiliser les certificats du Windows Certificate Store là où notre logiciel PKI place les certificats des utilisateurs ?
Oui. En paramétrant un nouveau tunnel VPN :

- Aller sur 'Phase1' > onglet 'Certificat'.
- Tous les certificats du Windows Certificate Store (Personal Store) apparaissent ici.
- Sélectionner le Certificat dont vous avez besoin, cliquer sur 'Ok', cliquer sur 'Sauver'.

Vous pouvez télécharger notre Guide d'utilisateur du Client VPN.

26.1.24 Le Client VPN supporte-t-il SHA-2 ?

Le Client VPN TheGreenBow supporte SHA-1 et SHA-2 256 bit. Le Client VPN support aussi MD5.
Voir les spécifications du Client VPN.

26.1.25 Comment visualiser les connexions VPN ?

Il y a plusieurs façon de visualiser les connexions VPN ouvertes :

- Clic droit sur l'icone systray du Client VPN. La lumière verte signifie que le tunnel VPN est ouvert.
- Clic sur l'icone systray du Client VPN pour ouvrir le Panneau de configuration. Appuyer sur Ctrl+Entrée pour aller sur le Panneau de connexion, idem pour revenir sur le Panneau de configuration.
- Une fois le Panneau de configuration apparut, cliquer sur le bouton 'Connexions'.

26.1.26 Comment forcer tout le trafic Internet dans le tunnel VPN ?

Il est possible de forcer tout le trafic Internet dans le tunnel VPN. Ce faisant, tout le trafic Internet sera acheminé à partir de la passerelle distante au lieu du réseau local des utilisateurs distants, et l'adresse IP du réseau de l'utilisateur distant sera virtuellement cachée sur les sites visités car elle est remplacée par l'adresse IP de la passerelle distante. De plus, le réseau d'entreprise peut appliquer un niveau d'analyse supplémentaire sur une partie du trafic pour accroître la sécurité puisque tout le trafic passe par l'entreprise.

La configuration VPN est simple et nécessite 3 étapes :

- Dans le 'Panneau de Configuration' > 'Paramètres généraux' > sélectionner 'Bloquer les flux non chiffrés' afin d'interdire le trafic non chiffré d'être routé directement vers Internet.
- Dans le 'Panneau de Configuration' > 'Phase2' > sélectionner 'Adresse réseau' comme 'Type d'adresse' et définir 'Adresse réseau distant' et 'Masque réseau' à '0.0.0.0', de sorte que tout le trafic (vers n'importe quelle adresse IP) soit routé dans le tunnel VPN. Noter que '0.0.0.0' signifie que tout le trafic y compris le trafic du réseau local sera routé dans le tunnel VPN.
- Sur la passerelle distante, configurer le tunnel VPN de la même manière car les deux configurations doivent être symétriques avec un sous-réseau local de 0.0.0.0/0.

Remarque: Certains passerelles/Routeurs VPN ne supportent pas cette fonctionnalité (i.e. hub&spoke: '0.0.0.0/0'). Si supportée, il sera nécessaire de créer une règle pour autoriser le trafic WAN vers WAN.

26.1.27 Le Client VPN TheGreenBow est-il compatible avec WWAN ?

Oui. WWAN signifie Wireless Wide Area Network. WWAN est maintenant compatible avec plusieurs modem/adaptateurs 3G/4G de différents fabricants. WWAN utilise des technologies de télécommunication de réseau mobile telles que WiMAX, UMTS, GPRS, CDMA2000, GSM, HSDPA ou 3G/4G pour transférer des données. La connectivité WWAN permet à un utilisateur d'un ordinateur portable muni d'une carte WWAN de surfer sur internet, de vérifier les emails ou de se connecter à un réseau privé virtuel (VPN) à partir de n'importe où dans les limites régionales du réseau mobile.

Microsoft a introduit le pilote miniport WWAN pour supporter cette spécification. L'adaptateur miniport WWAN est utilisé pour gérer l'installation, la configuration, la transmission des paquets, la réception de paquets et la déconnexion des données NDIS.

Tous les fabricants doivent prendre en compte les pilotes "Mobile Broadband Driver Model Specification" pour Windows 7 basées sur le modèle du pilote miniport NDIS6.20.
Consulter la liste des modems/adaptateurs 3G/4G.

26.1.28 Comment améliorer les performances du trafic VPN en changeant la MTU ?

La taille de MTU a un impact sur la performance du trafic VPN. Il est possible de changer la taille MTU pour tout le trafic passant par un tunnel VPN. La Maximum Transmission Unit (MTU) est la taille du plus gros paquet envoyés sur TCP/IP. Les messages plus grand que la MTU doivent être divisés en petits paquets qui diminue la performance.

Voici comment modifier la MTU pour le trafic VPN par l'ajout d'une entrée dans la registry :
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TgbIpSec\Parameters] "MTUSize"=dword:000004b0

Valeurs limites : #4b0 < MTUSize < #ffff (ou 1200 < MTUSize < 65535)

Remarques :
1/ Cette modification ne fonctionne pas sur Vista et Seven avec les versions 5.x du logiciel.
2/ Pour la version 5.1 du logiciel (sur Windows Vista et Seven), la possibilité de modifier la taille de la MTU n'est plus nécessaire. La taille de la MTU du client VPN est réglée automatiquement sur celle de l'interface réseau Windows lors de l'ouverture d'un tunnel.

26.1.29 Comment partager son bureau à distance dans un tunnel VPN en un seul clic ?

Le Client VPN TheGreenBow implémente le partage de bureau à distance (Remote Desktop Sharing) sécurisé :

- Cette fonctionnalité permet à un utilisateur de partager sa machine sur le réseau d'entreprise à partir d'un emplacement à distance comme à la maison.
- Lorsque l'utilisateur clique sur un alias de la session de partage de bureau, le tunnel VPN associé s'ouvre automatiquement, et une session Remote Desktop Protocol est lancé pour atteindre la machine distante.
- Cette fonctionalité est détaillée sur le lien : Partage de bureau à distance sécurisé

Voici un exemple de logiciel tiers ayant utilisé cette fonctionnalité via les options en ligne de commande :

- **Devolutions.net**: Remote Desktop Manager est une application qui permet de gérer toutes ses connexions distantes et machines virtuelles. Il est possible d'ajouter, éditer, remplacer et trouver rapidement les connexions distantes. Devolution a developé un plugin pour ouvrir et fermer les tunnels avant d'ouvrir automatiquement une session RDP et importer un fichier de configuration VPN. Voir le tutoriel vidéo

26.1.30 Comment désactiver la Gina ?

Le mode Gina du Client VPN est disponible sur Windows Vista, seven, 8 et 10.
Parfois, lorsque Windows sort du mode de veille ou hibernation, il est impossible d'ouvrir un tunnel. Pour corriger cela, il est possible de désactiver le mode de Gina.

- Télécharger ces fichiers pour désactiver Gina sur Windows Vista/Seven 32-bit ou Gina sur Windows Vista/Seven 64-bit

- Télécharger ces fichiers pour activer Gina sur Windows Vista/Seven 32-bit ou Gina sur Windows Vista/Seven 64-bit

Une fois téléchargé, double-cliquer sur le fichier pour l'exécuter, cliquer sur 'OK' pour confirmer.

26.1.31 Gestion des configurations multi-utilisateurs

Le Client VPN TheGreenBow n'est pas conçu pour être utilisé par plusieurs utilisateurs d'un même poste Windows simultanément.
Si toutefois vous souhaitez mettre en œuvre une telle configuration, contactez-nous : support@thegreenbow.com.

26.2 Client VPN TheGreenBow IPV6

26.2.1 Une configuration VPN de test pour IPv6 est-elle disponible ?

Oui. Un test (ou une démo) de configuration VPN conçu par l'équipe Techsupport de TheGreenBow permet de se connecter à nos serveurs et gateway en ligne.

Ils sont toujours en ligne et vous pouvez les utiliser pour tester votre environnement réseau à tout moment. Cette configuration VPN de test est spécifique au Client VPN IPsec 6.0 et aux versions supérieure.

tgbvpn_demo_ipv6.tgb

26.2.2 À propos du support de Windows XP ?

À partir de la version 6.0, le Client VPN TheGreenBow ne supporte plus Windows XP.
Pour retrouver les versions du logiciel compatibles avec toute version de Windows, veuillez vous reporter à la page : Téléchargement du Client VPN

26.2.3 Est-il possible d'avoir la même adresse IP virtuelle sur de multiple réseaux distants ?

Oui. Gérer une adresse IP virtuelle unique pour chaque utilisateur distant, utilisable simultanément sur des réseaux distants multiples, facilite la tâche des responsables informatiques puisque cela diminue le nombre d'adresses IP virtuelles à gérer. Cela est possible en créant plusieurs tunnels VPN avec la même Phase1 et plusieurs Phase2, puis en ajoutant les paramètres suivants :

- Phase1 > 'Avancé' > 'Mode-Config'
- Phase2 > Entrer la même adresse IP dans 'Adresse du Client VPN' pour toutes les Phases 2

26.2.4 Quels sont les liens ou les outils sur IPv4/IPv6 ?

- IPv6 ready :
  https://ipv6test.google.com,
  http://test-ipv6.com
- IPv6 littérature :
  http://www.worldipv6launch.org,
  http://en.wikipedia.org/wiki/IPv6,
  https://www.ipv6ready.org,
  https://www.ipv6ready.org/db/index.php/public
- IPv6 infographie :
  http://www.worldipv6launch.org/infographic/,
  http://www.google.com/ipv6/index.html

- IPv6 adoption :
  http://www.google.com/intl/en/ipv6/statistics.html

26.2.5 Configurer le client VPN quand le réseau local et distant ont le même sous-réseau ?

Si le réseau domestique (maison de l'utilisateur) et le réseau d'entreprise ont le même sous-réseau et que l'utilisateur à la maison veut imprimer sur une imprimante locale, le client VPN doit être configuré pour éviter d'envoyer du trafic vers le réseau d'entreprise lorsque la destination est locale.

La fonction à utiliser est la restriction de trafic basée sur une plage d'adresses IP.

Dans le cas d'utilisation ci-dessus en supposant que LAN1 (192.168.133.x), et LAN2 (192.168.133.y), nous allons limiter le LAN1 aux plages suivantes (x->1-20) et LAN2 (y->30-50). Ce faisant, tout le trafic en dehors des plages définies est acheminé vers le réseau local (LAN1).

Voici la configuration du client VPN et la passerelle VPN :

1) Configuration du Client VPN :

- Phase1 > 'Interface' sélectionner 'Automatique'
- Phase2 > 'Adresse du Client VPN' entrer une adresse IP et pour 'Type d'adresse' sélectionner 'Plage d'adresse' avec début/fin comme suit : 192.168.133.30/192.168.133.50

2) Configuration de la passerelle VPN :

- Phase2 > address type=Adresse réseau avec réseau distant/masque=192.168.133.0/255.255.255.0

Note: Merci de contacter notre support si vous voulez configurer votre Client VPN de cette manière.

26.2.6 Forcer tout le trafic dans le tunnel VPN à l'exception du trafic du réseau local ?

Pour forcer tout le trafic dans un tunnel VPN à l'exception du trafic du réseau local, le Client VPN doit être configuré pour forcer l'envoi du trafic vers le réseau d'entreprise lorsque la destination n'est pas locale.

La fonctionnalité à utiliser est la restriction de trafic basée sur la plage d'adresse.

Ci-dessous la configuration du Client VPN :

1) Configuration du Client VPN :

- Phase2 > 'Type d'adresse' sélectionner 'Adresse réseau' avec réseau distant/masque=0.0.0.0/0.0.0.0

2) Configuration du Client VPN :

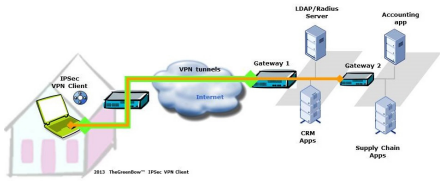
- Phase2 > 'Type d'adresse' sélectionner 'Adresse réseau' avec réseau distant/masque=0.0.0.0/0.0.0.0

Note: Merci de contacter notre support si vous voulez configurer votre Client VPN de cette manière.

26.2.7 Est-il possible d'ouvrir un tunnel VPN dans un autre tunnel VPN ?

Oui. Cette fonction permet de gérer un réseau sécurisé avec une application sensible au sein du réseau d'entreprise. Les utilisateurs ont besoin d'ouvrir un tunnel VPN pour l'accès au réseau d'entreprise, puis ouvrir un autre tunnel VPN pour accéder au second réseau.

Dans ce cas d'utilisation, en supposant que LAN1 (192.168.133.x) est le réseau d'entreprise avec une Passerelle VPN 1, et LAN2 (192.168.10.y) est l'autre réseau sécurisé dans le réseau d'entreprise, avec une Passerelle VPN 2 (WAN:192.168.133.1, LAN: 192.168.10.1).



Zoom
Tunnels VPN imbriqués

Voici la configuration du Client VPN :

1) Tunnel VPN#1:

- Phase1 > 'Adresse routeur distant' entrer l'adresse WAN de la Passerelle VPN 1
- Phase2 > 'Addresse du Client VPN' entrer une adresse IP, 'Type d'adresse' sélectionner 'Adresse réseau' avec réseau distant/masque= 192.168.133.1/255.255.255.0

2) Tunnel VPN#2:

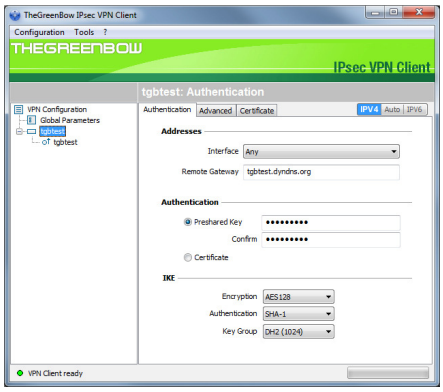
- Phase1 > 'Adresse routeur distant' entrer l'adresse WAN de la Passerelle VPN 2 (i.e. 192.168.133.1)
- Phase2 > 'Addresse du Client VPN' entrer une adresse IP, 'Type d'adresse' sélectionner 'Adresse réseau' avec réseau distant/masque= 192.168.10.1/255.255.255.0

26.2.8 Comment configurer le Client VPN IPsec dans un réseau hétérogène IPv6 - IPv4 ?

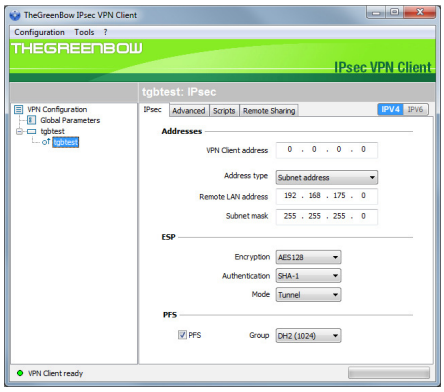
Le Client VPN IPsec prend en charge les réseaux hétérogènes IPv4 et IPv6 côté LAN et côté WAN, que ce soit sur les réseaux distants ou d'entreprise. Une fois activée, la fonction 'Auto' (pour IPv4/IPv6) permet de supporter les environnements complexes.

En fonction de la configuration de votre réseau IPv4 et IPv6, vous pouvez utiliser l'une des configurations citées ci-dessous : Vous n'avez pas besoin du Client VPN 6.0 pour une configuration réseau IPv4 seulement (local et distant). Toutes les versions antérieures du Client VPN fonctionneront parfaitement.

- Phase1-Authentication: sélectionnez toujours le mode 'Auto' pour IPv4/IPv6. Si la passerelle VPN de l'entreprise restreint à IPv4 du côté WAN alors sélectionnez 'IPv4' dans le Client VPN IPsec Phase 1.
- Phase2-IPsec: sélectionnez 'IPv4' si votre réseau d'entreprise est en IPv4, et sélectionnez 'IPv6' si votre réseau d'entreprise est en IPv6.



Zoom
VPN Phase 1



Zoom
VPN Phase 2

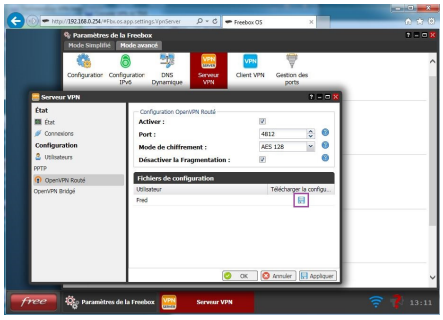
26.3 Client VPN TheGreenBow SSL

26.3.1 Est-il possible de configurer en même temps un tunnel VPN IPsec et SSL ?

À partir de la version 6.1, le Client VPN TheGreenBow permet de configurer des tunnels IPsec (IKEv1 ou IKEv2) et aussi des tunnels SSL.

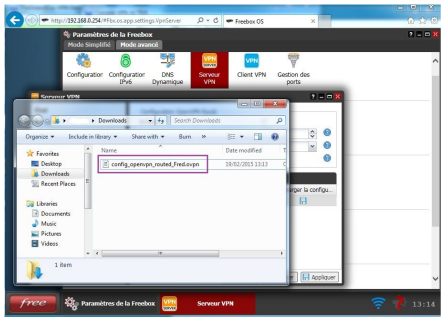
26.3.2 Comment installer un tunnel OpenVPN avec la FreeBox ?

FreeboxConfig1
Activer le mode OpenVPN Routé comme sur l'exemple (important: cocher "Désactiver la fragmentation") et ajouter un utilisateur ("Fred" dans l'exemple), un nouveau mot de passe vous sera demandé pour l'utilisateur créé. Cliquer sur la disquette pour récupérer la configuration du client.



Zoom

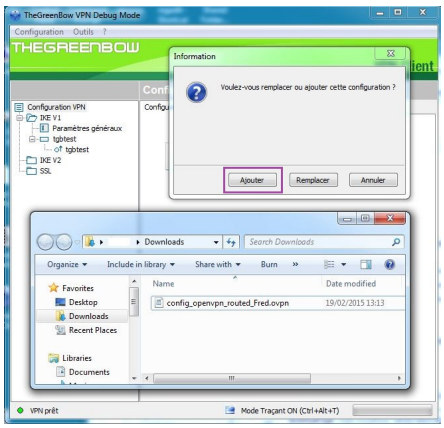
FreeboxConfig2
Un fichier de configuration .ovpn est téléchargé, le récupérer et le mettre sur le poste cible où est installé le client VPN TheGreenBow. Il s'agit du poste qui va se connecter à distance sur la passerelle VPN de la Freebox.



Zoom

FreeboxConfig3

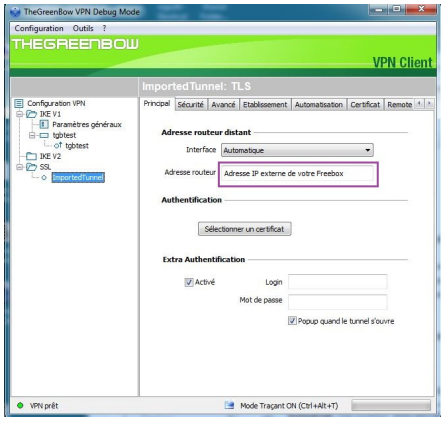
Sur le poste où est installé le client VPN TheGreenBow importer le fichier .ovpn, soit par un Drag & Drop du fichier soit en utilisant le menu Configuration/Importer. Cliquer sur ajouter pour conserver les tunnels existants.



Zoom

FreeboxConfig4

Après l'importation, vous pouvez constater que l'adresse IP externe de votre Freebox est bien renseignée dans le champ "Adresse routeur".

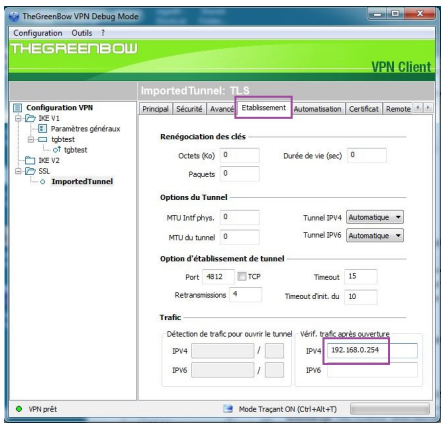


Zoom

FreeboxConfig5

Cliquez sur l'onglet "Etablissement", puis, comme sur l'exemple, dans le champ "Vérif. trafic après ouverture" entrez l'adresse IP 192.168.0.254. C'est un cas par défaut en supposant que vous n'avez pas modifié l'adresse IP de votre réseau local. Si votre sous-réseau n'est pas 192.168.0.0, alors vous avez à adapter ce champ. Par défaut 192.168.0.254 est

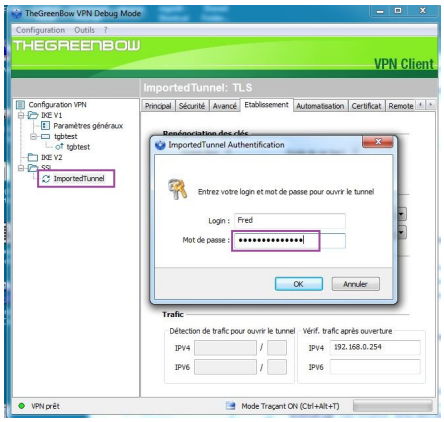
l'adresse local du Freebox Server, vous pouvez mettre tout autre machine de votre réseau local si vous connaissez son adresse IP. Faites CTRL-S (ou menu Configuration/Sauver) pour sauver la configuration.



Zoom

FreeboxConfig6

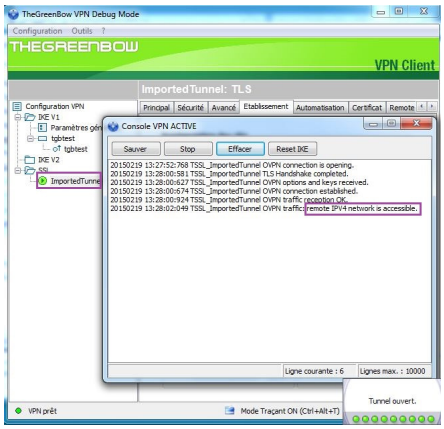
Double cliquez (ou clic-droit/"Ouvre Tunnel...") sur ImportedTunnel (vous pouvez modifier le nom) pour ouvrir le tunnel. Une popup va s'ouvrir et vous avez à entrer le nom d'utilisateur et son mot de passe (configurés sur la Freebox lors de l'étape 1).



Zoom

FreeboxConfig7

Le tunnel doit passer en vert et dans la console (Menu Outils/Console) vous devriez voir que vous avez accès à votre réseau local de manière distante à travers le tunnel.



Zoom

26.4 Troubleshootings

"J'ai le message XXXXX dans la console". Qu'est ce que cela veut dire ?

Nous rendons disponible pour téléchargement le guide plus complet des messages Console du Client VPN TheGreenBow avec explications et astuces pour résolutions. Si le document ne suffit pas, envoyez nous tous les échanges avec les lignes RECV et SEND . Réglez les filtres de Log à "0" et cliquez sur "Save File" (i.e. "sauver fichier").
Vous trouverez le fichier de Log dans C:\Program Files\TheGreenBow\TheGreenBow VPN.

No response from the VPN server

Les traces suivantes indiquent que le routeur VPN distant ne répond pas aux requêtes IKE du Client VPN.

115317 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115319 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115321 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115323 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]

Regardez les traces du routeur VPN distant et vérifiez si des requêtes du Client sont reçues. Si vous ne trouvez aucune trace, des requêtes IKE doivent avoir été perdues quelque part, ou filtrées par un logiciel ou un équipement de type firewall.Vérifiez les règles des Firewalls (incluant le Firewall éventuellement installé sur la machine) qui peuvent être situés entre le Client VPN et le routeur VPN. En particulier, sur Vista, se reporter à la faq suivante.

Tunnel VPN ouvert mais le ping ne fonctionne pas ?

Si vous avez les traces suivantes, le tunnel VPN IPsec est établi. Vous devriez pouvoir faire un ping sur n'importe quel adresse du réseau LAN. La configuration du Client VPN TheGreenBow est correct dans ce cas.

121902 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
121905 Default (SA Cnx-Cnx-P2) RECV phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
121905 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [HASH]

Si vous ne pouvez toujours pas "pinger" le réseau LAN distant, voici quelques directives :

- Vérifiez la configuration Phase 2 : Adresse Client VPN et adresse réseau distant. Normalement, l'Adresse Client VPN ne devrait pas appartenir au subnet du LAN distant (Lire également comment remplir le champ "Adresse Client VPN" ?)

- Une fois le tunnel ouvert, des paquets sont envoyés avec le protocole ESP. Ce protocole peut être bloqué par un Firewall. Vérifiez que chaque élément entre le client et le serveur VPN accepte ESP
- Vérifiez vos traces de serveur VPN. Des paquets peuvent être éliminés par une des règles du Firewall.
- Verifiez que votre FAI support ESP. Les principaux le supporte.
- Si vous ne pouvez toujours pas faire de ping, suivez le trafic ICMP sur l'interface LAN du serveur VPN et sur l'interface LAN de l'ordinateur (avec Ethereal par exemple). Vous aurez une indication que le chiffrement fonctionne.
- Vérifiez le routeur "par défaut" dans la configuration LAN du serveur VPN. Une cible sur votre LAN distant peut recevoir des ping mais ne répond pas parce qu'il n'y a pas de routeur "par défaut" configuré.
- Vous ne pouvez pas accéder aux ordinateurs par leur nom dans le LAN. Vous devez indiqué leur adresses IP à l'intérieur du LAN.

Pour des traces plus complètes et des conseils de résolution, veuillez aussi consulter notre document Troubleshooting.

Ordinateurs portables DELL ou HP avec des chipsets Broadcom

TheGreenBow recommande aux clients utilisant un chipset Broadcom intégré avec certains ordinateurs portables DELL ou HP de mettre à jour le pilote bcmwl5.sys avec la version la plus récente. Ce pilote provoque des écrans bleus de temps en temps, même si notre Client VPN n'est pas installé.

Adaptateur Intel Switching Utility

L'adaptateur Intel Switching Utility provoque des écrans bleus lorsque le Client VPN est installé.
Si vous possédez un processeur Intel Pro/Wireless 2100 or 2200, suivez ces étapes dans l'ordre :

- Allez sur Démarrer/Panneau de configuration/Ajout\Suppression de programmes. Retirez la section Intel PROSet.
- Allez sur Démarrer/Panneau de configuration Systeme :
  - Sélectionnez l'onglet Matériel, puis appuyez sur le bouton Gestionnaire de périphériques.
  - Dans le Gestionnaire de périphériques, cliquez sur le signe plus pour afficher la section Adaptateurs réseaux.
  - Sélectionnez adaptateur Intel PRO/Wireless LAN 2200 (ou 2100) et faites un clic droit.
  - Sélectionnez Désinstaller dans le menu pop-up.
- Redémarrez l'ordinateur.

Apres le redémarrage, l'ordinateur portable détectera de nouveau la carte sans-fil et installera les pilotes correspondants. Il n'installera pas les pilotes Intel PROset. La carte sans-fil devrait encore fonctionner, mais les fonctionnalités ajoutées à l'adaptateur Switching ne seront pas disponibles. Windows va alors gérer les profils sans-fil au lieu de l'utilitaire Intel PROSet .

Pour plus de détails, consultez Intel technical advisory

Je n'arrive pas à désinstaller le Client VPN

Problème : Je n'arrive pas à désinstaller le Client VPN, il demande toujours de désinstaller la version précédente d'abord.
Solution : Vous pouvez utiliser our tool pour nettoyer les composants restants du Client VPN .

Problèmes avec les pilotes TheGreenBow sur Windows Vista

Nous recommandons vivement aux utilisateurs de Windows Vista de mettre à jour leurs pilotes de carte réseau avec Windows Update. Cette action peut empêcher qu'un pilote se plante dans certaines configurations de réseau. Aussi, le pack Windows Vista correction de bug KB938194 doit être installé. Plus de détails et téléchargement sont disponibles sur http://support.microsoft.com/?kbid=938194.

Impossible d'ouvrir le tunnel sous Vista, problème avec le Firewall Vista ?

A la suite de l'installation du Client VPN TheGreenBow sur Vista, il peut être impossible d'ouvrir un tunnel. L'ouverture du tunnel reste bloquée sur le message :

115317 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115319 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]

Ce cas de figure peut arriver sur Windows Vista parce que le Firewall Vista interdit les communi-cations IPsec.

TheGreenBow VPN IPsec 4.2 (et supérieures): Le logiciel crée automatiquement des nouvelles règles dans le pare-feu Windows Vista au cours de l'installation autorisant ainsi tout trafic VPN IPsec (voir la section "Pare-feu Windows" dans le Guide de l'utilisateur).

Note: Dans windows Seven (Wind 7), votre profil 'Privé' et 'Domaine' dans les règles existantes du pare-feu Windows pour le Client VPN TheGreenBow peut ne pas être paramétré en conséquence. S'il vous plait vérifiez les règles de pare-feu Windows et vérifiez que votre profil 'Privée' et 'Domaine' est sélectionné (voir l'étape 6 ci-dessous).

TheGreenBow VPN IPsec 4.1(et antérieures) : Afin de permettre les communications IPsec (ou de vérifier qu'ils sont autorisés ou restreinte), procéder comme suit :

- Etape 1 : Aller au bouton "Démarrer" de Windows et entrer "Pare-feu Windows avec sécurité avancée" dans le champs "Rechercher". Sinon, taper "cmd" et dans la fenêtre de ligne de commande entrer "wf".

- Etape 2 : Sélectionner dans la colonne de gauche "Règles de trafic entrant", puis dans la colonne de droite "Nouvelle règle...".

- Etape 3 : Sélectionner "Port" puis cliquer sur "Suivant".

- Etape 4 : Sélectionner "UDP" et dans le champ "Ports locaux", puis entrer les deux valeurs 500 et 4500 séparées par une virgule ("500,4500").
  Cliquer sur "Suivant".

- Etape 5 : Vérifier que le champ "Autoriser la connexion" est sélectionné.
  Cliquer sur "Suivant".

- Etape 6 : Vérifier que les champs Domaine, Privées et Publiques sont tous cochés.
  Cliquer sur "Suivant".

- Etape 7 : Affecter un nom à cette nouvelle règle. Cliquer sur "Terminer".

- Etape 8 : La nouvelle règle est créée.

- Etape 9 : Sélectionner dans la colonne de gauche "Règles de trafic sortant" et dans la colonne de droite "Nouvelle règle...", et configurer exactement la même règle (UDP, ports 500 et 4500, VPN sortant).

Purge du pilote sous Windows Visa et Windows Seven

(IPsec VPN Client 4.* et 5.0)

Dans certains cas, le driver TheGreenBow NDIS peut pas être mis à jour avec une installation de nouveaux logiciels. Pour y parvenir, suivez les étapes suivantes:

- Exécuter 'cmd.exe' en tant qu'administrateur
- Type 'pnputil.exe-e' et cliquez sur 'Entrée'

La réponse devrait ressembler à ceci:

```
Published name : oem68.inf
Driver package provider : Atheros Communications Inc.
Class : Network adapters
Driver version and date : 01/13/2009 7.6.1.204
Signer name : microsoft windows hardware compatibility publisher

Published name : oem86.inf
Driver package provider : TheGreenBow
Class : Network Service
Driver version and date : 05/19/2009 1.0.1.20
Signer name : thegreenbow

Published name : oem95.inf
Driver package provider : Microsoft
Class : Mobile devices
Driver version and date : 10/06/2004 4.0.4232.0
Signer name : microsoft windows hardware compatibility publisher

Published name : oem69.inf
Driver package provider : Acer
Class : Monitors
Driver version and date : 12/11/2006 1.00
Signer name : microsoft windows hardware compatibility publisher

Published name : oem78.inf
Driver package provider : Microsoft
Class : Network Service
Driver version and date : 01/24/2007 2.6.553.0
Signer name : microsoft windows hardware compatibility publisher
```

- find a "Driver package provider" line with "TheGreenBow" and note the INF file associated with. In our example, it is oem86.inf.
- type "pnputil.exe -d oem86.inf"

Le driver devrait être entièrement supprimé.

Comment installer manuellement les pilotes du Client VPN ?

(IPsec VPN Client 4.* et 5.0)

Microsoft Windows module d'installation du pilote peut ne pas installer les pilotes troisième partie régulièrement (par exemple IPsec TheGreenBow VPN pilotes ndistgb.inf Client), surtout quand Windows est chargé avec des tâches multiples. Parfois, les paramètres de Registre ne sont pas effectuées correctement, parfois, pas du tout.

Il ya une procédure manuelle simple pour vous permettre de démarrer. Les pilotes nécessaires sont encore dans le système, donc aucun téléchargement supplémentaire ne devrait être nécessaire. Voici les étapes:

- Ouvrir Windows 'Configuation Panel' > 'Network and Sharing Center' > 'Manage Network Connections' > clique droit sur une 'Network connection' > cliquez sur 'Properties'.

- Cliquez sur 'Installer...'

- Selectionnez 'Service' et cliquez sur 'Ajouter...'.

- Cliquez sur 'Have Disk ...' pour trouver les pilotes.

- Cliquez sur "Parcourir..." pour trouver les pilotes.

- Allez dans C:\Program Files\Common Files\temp\{389b11eb-c24e-4a3d-8032-f44daa4cde4d} et selectionnez le fichier 'ndistgb.inf' (i.e. setup information), et cliquez sur 'Ouvrir'.

- Recommencer à nouveau avec tous les autres "Connexions réseau" avec lequel que vous souhaitez utiliser le Client VPN .

Le tunnel VPN peut ne pas s'ouvrir après une mise à jour Windows 10

Le tunnel VPN peut ne pas s'ouvrir après une mise à jour Windows 10. Vérifiez si le message suivant s'affiche dans la console log du Client VPN :

20150806 14:12:55:088 TSocket No socket for IPV4 address 192.168.0.20:500
20150806 14:12:55:088 TSocket message data type IKE (0) could not be sent

Si c'est le cas, le service Windows IKEEXT doit être désactivé.

Solution#1: Effectuez les étapes suivantes :

- Allez sur 'Panneau de configuration' > 'Outils d'administration' > 'Services'.
- Initialisez 'Type de démarrage' du service IKEEXT à 'Désactivé'.

- Redémarrez le Client VPN.

Solution#2: Re-installez le Client VPN (même numéro de version si vous n'avez pas 'd'option de mise à jour').

Sur Windows 10, le tunnel VPN s'ouvre mais aucun trafic ne passe (driver VPN et fonction secureboot)

Ce problème est aussi identifié comme un problème "Windows 10 secureboot" : certains ordinateurs Windows 10 sont configurés avec la fonction **BIOS secureboot** activée. Cette fonction peut causer un dysfonctionnement des drivers VPN de la version 6.41 du logiciel. Nous fournirons très bientôt un setup intégrant la correction de ce problème. En attendant, nous fournisson une mise à jour des drivers, téléchargeable ci-dessous, qui corrige le problème.

1/ Quels sont les symptômes du problème ?

- Sur Windows 10, le tunnel VPN s'ouvre correctement mais aucun trafic ne passe
- La console VPN montre les messages d'erreur suivants :

20170414 10:36:12:628 [VPNCONF] TGBIKE_STOPPED received 20170414 10:36:13:159 [VPNCONF] IKE could not be started because driver was not loaded.
puis, après que le tunnel soit ouvert :
20170414 10:36:25:645 Default ConfigureVirtualItf: IM_NewInstance failed with errors 4 - 3.

2/ Comment vérifier que la fonction secureboot est activée sur mon ordinateur ?

- Cliquer sur le bouton démarrer de Windows
- Entrer "msinfo32.exe" dans la barre de recherche
- Vérifier que la ligne "Etat du démarrage sécurisé activé" est affichée ou pas comme illustré par la saisie d'écran ci-contre.

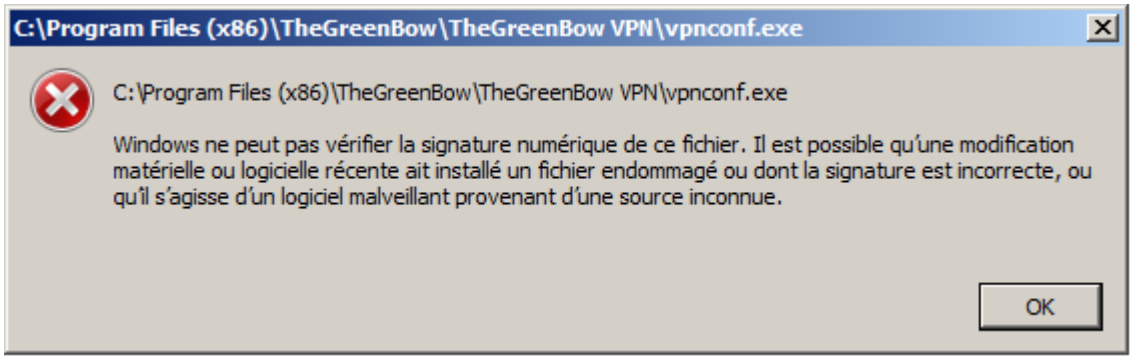
3/ Comment corriger le problème ?

- Télécharger et installer la mise à jour des drivers VPN suivante (disponible pour Windows 10, sur une version 6.4x du logiciel VPN)

  Mise à jour des drivers 6.4x

Sous Windows 7: Erreur de vérification de signature.

Si au lancement de VPNConf vous obtenez l'erreur suivante:



alors, il est nécessaire d'installer le KB3033929:

- 32 bits: https://www.microsoft.com/en-us/download/details.aspx?id=46078
- 64 bits: https://www.microsoft.com/en-us/download/details.aspx?id=46148

27 Contact

27.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur les sites :
Anglais : www.thegreenbow.com
Français : www.thegreenbow.fr

27.2 Commercial

Contact téléphonique : +33.1.43.12.39.30
Contact mail : sales@thegreenbow.com

27.3 Support

Les sites TheGreenBow proposent plusieurs pages concernant le support technique des logiciels :

Support

Anglais : http://www.thegreenbow.com/support.html
Français : http://www.thegreenbow.fr/support.html

Aide en ligne

Anglais : http://www.thegreenbow.com/support_flow.html?product=vpn&lang=en
Français : http://www.thegreenbow.com/support_flow.html?product=vpn&lang=fr

FAQ

Anglais : http://www.thegreenbow.com/vpn_faq.html
Français : http://www.thegreenbow.fr/vpn_faq.html

Contact

Le support technique est accessible via les formulaires disponibles sur le site TheGreenBow ou directement par email à l'adresse : support@thegreenbow.com

28 Annexes

28.1 Raccourcis

Panneau des Connexions

- ESC ferme la fenêtre
- CTRL+ENTER ouvre le Panneau de Configuration (interface principale)
- Flèches les flèches haut et bas permettent de sélectionner une connexion VPN
- CTRL+O ouvre la connexion VPN sélectionnée
- CTRL+W ferme la connexion VPN sélectionnée

Arborescence du Panneau de Configuration :

- F2 Permet d'éditer le nom de la Phase sélectionnée
- DEL Si une phase est sélectionnée, la supprime après confirmation de l'utilisateur.
  Si la Configuration est sélectionnée (racine de l'arborescence), propose l'effacement (reset) de la configuration complète.
- CTRL+O Si une phase 2 est sélectionnée, ouvre le tunnel VPN correspondant.
- CTRL+W Si une phase 2 est sélectionnée, ferme le tunnel VPN correspondant.
- CTRL+C Copie la phase sélectionnée dans le "clipboard".
- CTRL+V Colle (ajoute) la phase copiée dans le "clipboard".
- CTRL+N Crée une nouvelle phase 1, si la Configuration VPN est sélectionnée, ou crée une nouvelle phase 2 pour la phase 1 sélectionnée.
- CTRL+S Sauvegarde la politique de sécurité VPN.

Panneau de Configuration

- CTRL+ENTER Permet de basculer au Panneau des Connexions
- CTRL+D Ouvre la fenêtre "Console" de traces VPN
- CTRL+ALT+R Redémarrage du service IKE
- CTRL+ALT+T Activation du mode traçant (génération de logs)
- CTRL+S Sauvegarde la politique de sécurité VPN.

28.2 Langues

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

28.3 Caractéristiques techniques du Client VPN TheGreenBow

Général

Version Windows	Windows Server 2008 32/64bit Windows Server 2012 R2 64bit Windows Vista 32/64bit Windows 7 32/64bit Windows 8 32/64bit Windows 10 32/64bit
Langues	Allemand, Anglais, Arabe, Chinois (simplifie), Coréen, Espagnol, Danois, Persan, Finnois, Français, Grec, Hindi, Hongrois, Italien, Japonais, Néerlandais, Norvégien, Polonais, Portugais, Russe, Serbe, Slovène, Tchèque, Thaï, Turc

Mode d'utilisation

Mode invisible	Ouverture automatique du tunnel sur détection de trafic Contrôle d'accès aux politiques de sécurité VPN Possibilité de masquer tout ou partie des interfaces

Mode USB	Plus aucune politique de sécurité VPN sur le poste Ouverture du tunnel sur insertion d'une clé USB configurée VPN Fermeture automatique du tunnel sur extraction de la clé USB configurée VPN
Gina	Ouverture d'un tunnel avant le logon Windows par : Gina / XP Credential providers sur Windows Vista et Windows 7 et supérieur
Scripts	Exécution de scripts configurable sur ouverture et fermeture du tunnel VPN
Remote Desktop Sharing	Ouverture en un seul clic d'un ordinateur distant (remote desktop) via le tunnel VPN

Connexion / Tunnel

Mode de connexion	Peer-to-peer (point à point entre deux postes équipés du Client VPN) Peer-to-Gateway (voir la liste des gateways qualifiées et leurs guides de configuration)
Media	Ethernet, Dial up, DSL, Cable, GSM/GPRS, Wi-Fi Wireless LAN : 3G, 4G, satellite
Tunneling Protocol	IPsec : support complet IKEv1 ou IKEv2 (IKE basé sur OpenBSD 3.1 (ISAKMPD)) SSL : support complet Diffie-Hellmann DH groupe 1 à 18
Tunnel mode	Main mode et Aggressive mode
Mode-Config	Récupération automatique des paramètres réseaux depuis la passerelle VPN

Cryptographie

Chiffrement	Symétrique : DES, 3DES, AES 128/192/256bit Asymétrique : RSA Diffie-Hellmann: DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) Hash: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512
Authentification	Administrateur : Protection de l'accès aux politiques de sécurité VPN Utilisateur : - X-Auth statique ou dynamique (demande à chaque ouverture du tunnel) - Hybrid Authentication - Pre-shared key - EAP (MSCHAP-V2) - Multiple Auth
IGC / PKI	- Support des certificats au format X509, PKCS12, PEM - Multi-support : Magasin de certificats Windows, carte à puce, Token - Critères certificats : expiration, révocation, CRL, sujet, key usage - Possibilité de caractériser l'interface Token / carte à puce (voir la liste des Token / carte à puce qualifiés) - Détection automatique du Token / carte à puce - Accès aux Token / carte à puce en PKCS11 ou CSP - Vérification des certificats "Client" et "Passerelle"

Divers

NAT / NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 et RFC 3947, IP address emulation, inclut le support de : NAT_OA, NAT keepalive, NAT-T mode agressif, NAT-T en mode forcé, automatique ou désactivé
DPD	RFC3706. Détection des extrémités IKE non actives.
Redundant Gateway	Gestion d'une passerelle de secours (redundant gateway), automatiquement sélectionnée sur déclenchement du DPD (passerelle inactive)

Administration

Déploiement	Options pour le déploiement des politiques VPN (options de ligne de commande de l'installeur, fichiers d'initialisation configurables, etc.) Installation silencieuse
Gestion des politiques VPN	Options d'importation et d'exportation des politiques VPN Sécurisation des importations / exportations par mot de passe, chiffrement et contrôle d'intégrité
Automatisation	Possibilité d'ouvrir, fermer et superviser un tunnel en ligne de commande (batch et scripts) Possibilité de démarrer et arrêter le logiciel par batch
Log et traces	Console de logs IKE/IPsec et SSL et mode traçant activable
Live update	Vérification des mises à jour depuis le logiciel
Licence et activation	Modularité des licences (standard, temporaires, à durée limitée, abonnement), de l'activation du logiciel (WAN, LAN), et des options de déploiement (déploiement des logiciels activés, activation silencieuse, etc.)

28.4 Licence et Crédits

Crédits et references de licence.

```
/*
 * Copyright (c) 1998, 1999 Niels Provos.  All rights reserved.
 * Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>.  All rights reserved.
 * Copyright (c) 1998, 1999, 2000, 2001 Niklas Hallqvist.  All rights reserved.
 * Copyright (c) 1999, 2000, 2001, 2002, 2004 Håkan Olsson.  All rights reserved.
 * Copyright (c) 1999, 2000, 2001 Angelos D. Keromytis.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 */

/* ====================================================================
 * Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
```

```
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software