

TheGreenBow
VPN Client

Guide Utilisateur

Table des Matières

| | | |
|------|--|----|
| 1 | Présentation..... | 4 |
| 1.1 | Le Client VPN TheGreenBow..... | 4 |
| 1.2 | Le Client VPN universel | 5 |
| 1.3 | Fonctions inédites | 6 |
| 1.4 | Caractéristiques techniques..... | 7 |
| 1.5 | Conditions de mise en œuvre du Client VPN TheGreenBow..... | 7 |
| 2 | Installation..... | 8 |
| 2.1 | Installation..... | 8 |
| 2.2 | Période d'évaluation..... | 9 |
| 3 | Activation | 10 |
| 3.1 | Etape 1..... | 10 |
| 3.2 | Etape 2..... | 10 |
| 3.3 | Erreur d'activation | 11 |
| 3.4 | Activation manuelle..... | 12 |
| 3.5 | Licence temporaire..... | 13 |
| 3.6 | Licence et logiciel activé | 13 |
| 4 | Mise à jour | 14 |
| 4.1 | Comment obtenir une mise à jour | 14 |
| 4.2 | Mise à jour de la politique de sécurité VPN..... | 15 |
| 4.3 | Automatisation | 15 |
| 5 | Désinstallation | 16 |
| 6 | Utilisation rapide | 17 |
| 6.1 | Ouvrir un tunnel VPN | 17 |
| 6.2 | Configurer un tunnel VPN | 17 |
| 6.3 | Automatiser l'ouverture du tunnel VPN | 18 |
| 7 | Assistant de configuration..... | 19 |
| 8 | Interface utilisateur | 22 |
| 8.1 | Interface utilisateur..... | 22 |
| 8.2 | Bureau Windows | 22 |
| 8.3 | Barre des tâches | 23 |
| 9 | Panneau des Connexions..... | 25 |
| 10 | Panneau de Configuration | 26 |
| 10.1 | Menus | 26 |
| 10.2 | Barre d'état..... | 27 |
| 10.3 | Raccourcis | 27 |
| 10.4 | Arborescence des tunnels VPN | 27 |
| 11 | Fenêtre "A propos..." | 32 |
| 12 | Importer, exporter la politique VPN..... | 33 |
| 12.1 | Importer une politique de sécurité VPN..... | 33 |
| 12.2 | Exporter une politique de sécurité VPN | 34 |
| 12.3 | Fusionner des politiques de sécurité VPN | 35 |
| 12.4 | Diviser une politique de sécurité VPN | 35 |
| 13 | Configurer un tunnel VPN..... | 36 |
| 13.1 | VPN SSL, IPsec IKEv1 ou IPsec IKEv2..... | 36 |
| 13.2 | Modification et sauvegarde de la configuration VPN..... | 36 |
| 13.3 | Configurer un tunnel IPsec IKEv1 | 37 |
| 13.4 | Configurer un tunnel IPsec IKEv2 | 49 |
| 13.5 | Configurer un tunnel VPN SSL..... | 58 |
| 14 | Passerelle redondante..... | 65 |

| | | |
|------|---|-----|
| 15 | Automatisation..... | 66 |
| 16 | VPN Tunnel Fallback..... | 68 |
| 17 | IPv4 et IPv6..... | 69 |
| 18 | Gestion des Certificats..... | 70 |
| 18.1 | Configuration..... | 71 |
| 18.2 | Importer un certificat..... | 72 |
| 18.3 | Magasin de Certificats Windows..... | 73 |
| 18.4 | Options PKI : Caractériser le certificat et son support..... | 74 |
| 18.5 | Gestion des CA (Autorités de Certification)..... | 74 |
| 18.6 | Utiliser un tunnel VPN avec un Certificat sur Carte à puce..... | 75 |
| 19 | Partage de bureau distant..... | 76 |
| 19.1 | Configuration du partage de bureau distant..... | 76 |
| 20 | Gestion du panneau des connexions..... | 77 |
| 21 | Mode USB..... | 78 |
| 21.1 | Le Mode USB VPN..... | 78 |
| 21.2 | Configurer le Mode USB..... | 78 |
| 21.3 | Utiliser le Mode USB..... | 81 |
| 22 | Mode GINA..... | 82 |
| 22.1 | Le Mode GINA..... | 82 |
| 22.2 | Configurer le Mode GINA..... | 82 |
| 22.3 | Utiliser le Mode GINA..... | 82 |
| 23 | Contrôle d'accès à la politique VPN..... | 84 |
| 24 | Options..... | 85 |
| 24.1 | Contrôle d'accès..... | 85 |
| 24.2 | Affichage de l'interface (masquage)..... | 85 |
| 24.3 | Général..... | 86 |
| 24.4 | Gestion des logs..... | 87 |
| 24.5 | Options PKI..... | 87 |
| 24.6 | Gestion des langues..... | 87 |
| 25 | Logs administrateur, console et traces..... | 89 |
| 25.1 | Logs administrateur..... | 89 |
| 25.2 | Console..... | 90 |
| 25.3 | Mode traçant..... | 91 |
| 25.4 | Note à destination de l'administrateur..... | 91 |
| 26 | Recommandations de sécurité..... | 92 |
| 26.1 | Certification..... | 92 |
| 26.2 | Recommandations..... | 92 |
| 27 | Contact..... | 95 |
| 27.1 | Information..... | 95 |
| 27.2 | Commercial..... | 95 |
| 27.3 | Support..... | 95 |
| 28 | Annexes..... | 96 |
| 28.1 | Raccourcis..... | 96 |
| 28.2 | Langues..... | 96 |
| 28.3 | Logs administrateur..... | 98 |
| 28.4 | Caractéristiques techniques du Client VPN TheGreenBow..... | 99 |
| 28.5 | Licence et Crédits..... | 101 |

1 Présentation

1.1 Le Client VPN TheGreenBow

Le Client VPN TheGreenBow est le premier logiciel VPN de sécurisation des connexions distantes au Système d'Information de l'entreprise.

Disponible en 25 langues, utilisé par plus d'1,7 millions de connexions à travers le monde, il permet d'établir des connexions sécurisées (tunnel VPN) avec n'importe quelle gateway VPN.

Le Client VPN TheGreenBow est disponible sur toute plateforme : Windows, Linux, Android, iOS et macOS.

Le Client VPN TheGreenBow pour Windows est disponible en trois versions : VPN Standard, VPN Premium et VPN Certifié. Le tableau ci-dessous résume les principales caractéristiques de ces 3 versions.

| | VPN Standard | VPN Premium | VPN Certifié |
|---|---|--|--|
| Type d'utilisateurs | TPE / PME, quelques collaborateurs distants | PME ou entité de plusieurs dizaine/centaines de collaborateurs. Cf. (1) et (2) | Grand compte, administration, OIV pour gestion de données sensibles (agrément Diffusion Restreint, OTAN et UE) |
| Général | | | |
| Langues | 25 | 25 | 25 |
| Fiabilité sur tout réseau 3G, 4G, WiFi, Satellite, etc. | ✓ | ✓ | ✓ |
| Algorithmes et protocoles | | | |
| IPsec / IKEv1 | ✓ | ✓ | ✓ |
| IPsec / IKEv2 | ✓ | ✓ | ✓ |
| SSL | ✓ | ✓ | ✓ |
| Intégration et déploiement | | | |
| Intégration PKI | | ✓ (1) | ✓ (1) |
| Aide au déploiement | | ✓ (2) | ✓ (2) |
| Qualité et suivi | | | |
| Support | Support standard | Support personnalisé (3) | Support personnalisé (3) |
| Audit | | | Logiciel audité et certifié |
| Cryptographie | | | Cryptographie auditée et certifiée |
| Sécurité | | | Mécanismes anti-hack renforcés |

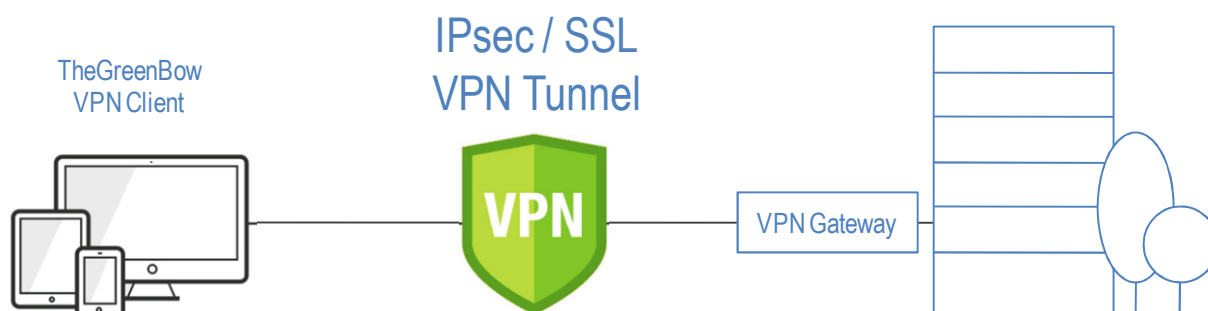
(1) Fonctions avancées d'intégration dans les PKI existantes et prise en compte modulaire de tous certificats et de tous supports de certificat (token carte à puce, certstore, etc.)

(2) Fonctions avancées d'aide au déploiement du logiciel, des mises à jour et des configurations VPN

(3) Le Client VPN PREMIUM et le Client VPN Certifié bénéficient d'un support personnalisé qui va d'un suivi dédié permettant une gestion prioritaire rapide et efficace des besoins des clients, jusqu'à la prise en compte d'évolutions spécifiques.

1.2 Le Client VPN universel

Le Client VPN TheGreenBow est le premier logiciel VPN universel de sécurisation des connexions distantes au Système d'Information de l'entreprise.



VPN disponible pour tout équipement

Le Client VPN TheGreenBow est disponible sur toute plateforme : Windows, Linux, Android, iOS et macOS. Toutes les versions du Client VPN TheGreenBow sont disponibles en téléchargement pour évaluation gratuite sur le site www.thegreenbow.fr.

Ce Guide Utilisateur concerne la version du Client VPN TheGreenBow pour Windows.

Compatible toute gateway VPN

Le Client VPN TheGreenBow permet d'établir des connexions sécurisées (tunnel VPN) avec toutes les passerelles VPN du marché. TheGreenBow évalue régulièrement la compatibilité des nouvelles passerelles VPN avec le logiciel Client VPN et met à disposition de ses utilisateurs la liste des passerelles évaluées, accompagnées de leur guide configuration : www.thegreenbow.fr/vpn_gateway.html

VPN sur tout type de réseau

Le Client VPN TheGreenBow permet de sécuriser et de maintenir les communications sur tout type de réseau : 3G, 4G, WiFi, Ethernet, ADSL, Satellite, etc. Il est spécifiquement conçu et renforcé pour être performant sur les réseaux les moins fiables.

VPN IPsec et SSL

Le Client VPN TheGreenBow implémente plusieurs protocoles VPN : il permet d'ouvrir simultanément des connexions VPN IPsec IKEv1 et IKEv2 et des connexions VPN SSL. Toutes les connexions VPN peuvent être établies sur IPv4 ou IPv6. Depuis la version 6.6, la fonction de "tunnel fallback" bascule automatiquement d'un protocole à l'autre sur échec du premier.

VPN compatible avec toute IGC / PKI

Le Client VPN TheGreenBow peut exploiter des certificats issus de toute PKI. Il implémente un jeu étendu de paramètres permettant de caractériser les certificats ainsi que leurs medias de stockage : token, carte à puce ou magasin de certificat.

Ces paramètres avancés sont disponibles dans les versions Premium et Certifiée du Client VPN TheGreenBow. Ils sont détaillés dans le Guide "[Gestion des PKI, certificats, tokens et cartes à puces](#)" disponible sur le site TheGreenBow.

TheGreenBow évalue régulièrement la compatibilité de nouveaux tokens avec le logiciel Client VPN et met à disposition des ses utilisateurs la liste des tokens et cartes à puce évalués : www.thegreenbow.fr/vpn_token.html.

VPN intégrable dans toute infrastructure

Le Client VPN TheGreenBow est spécifiquement conçu pour s'intégrer dans toute infrastructure existante. Il implémente d'une part un jeu étendu de facilités de déploiement, tant du logiciel lui-même (logiciel et mises à jour), que des configurations VPN (politiques de sécurité VPN) : options d'installation scriptables, customisation de l'installation, etc. Il implémente d'autre part une large gamme de logs exploitable par tout système de gestion d'évènements et de logs (SIEM).

Ces paramètres avancés sont disponibles dans les versions Premium et Certifiée du Client VPN TheGreenBow. Ils sont détaillés dans le "[Guide de déploiement du Client VPN TheGreenBow](#)" disponible sur le site TheGreenBow.

VPN en 25 langues

Utilisé partout dans le monde, le Client VPN TheGreenBow est disponible en 25 langues et intègre en standard un outil de traduction de son interface.

Se reporter au lien suivant pour plus d'information sur les traductions du logiciel : www.thegreenbow.fr/vpn_local.html

1.3 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
- Génération de logs administrateur

1.4 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, satellite, etc.
- Automatisation 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"
- Mode "tout dans le tunnel"
- Fonction de "tunnel fallback"
- 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](#).

1.5 Conditions de mise en œuvre du Client VPN TheGreenBow

Le logiciel installeur (ainsi que tous les binaires constitutifs) du Client VPN TheGreenBow 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".

La version du Client VPN TheGreenBow peut être vérifiée par l'utilisateur dans la fenêtre "A propos..." du logiciel, Cf. chapitre 11.

Par ailleurs, un utilisateur du Client VPN TheGreenBow 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 :

VPN Standard

[vpn_client.html](#)

VPN Premium

[vpn_premium.html](#)

VPN Certifié

[vpn_client_certified.html](#)

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

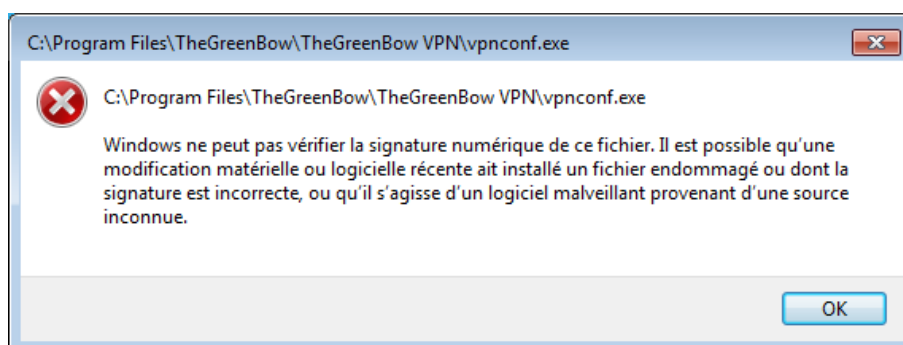
L'installation du logiciel est configurable, via un ensemble d'options de ligne de commande et de fichiers de configuration. Ces options et possibilités sont détaillées dans le document "Guide de Déploiement du Client VPN TheGreenBow" (tgbvpn_ug_deployment_fr.pdf) disponible sur le site TheGreenBow.

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.

En version certifiée, le Client VPN TheGreenBow 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 :

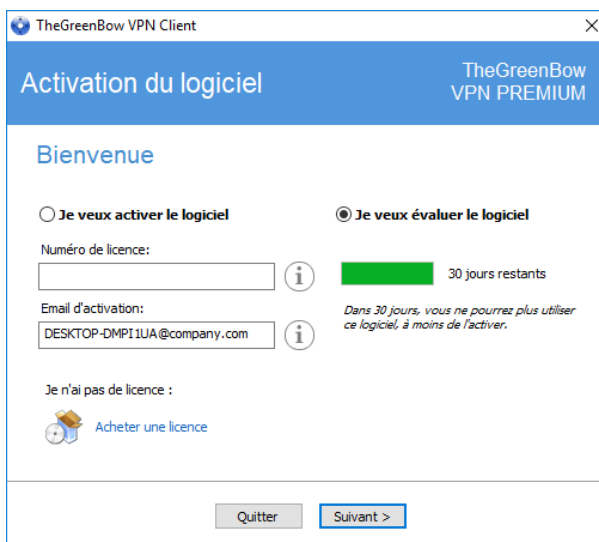


Note : La mise à jour ou l'installation d'une version donnée d'un Client VPN en remplacement d'une autre version (par exemple l'installation d'un Client VPN Premium en remplacement d'un Client VPN Standard) nécessite que le Client VPN soit désinstallé avant d'effectuer la mise à jour. Si la configuration 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.

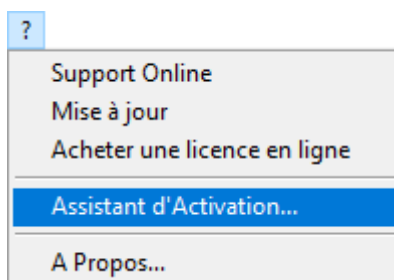
Pendant la période d'évaluation, la fenêtre d'activation est affichée à chaque démarrage du logiciel. Elle indique le nombre de jours d'évaluation restants.



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 via le menu "? > Assistant d'activation" de l'interface principale (panneau de configuration).



3 Activation

Le Client VPN TheGreenBow 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

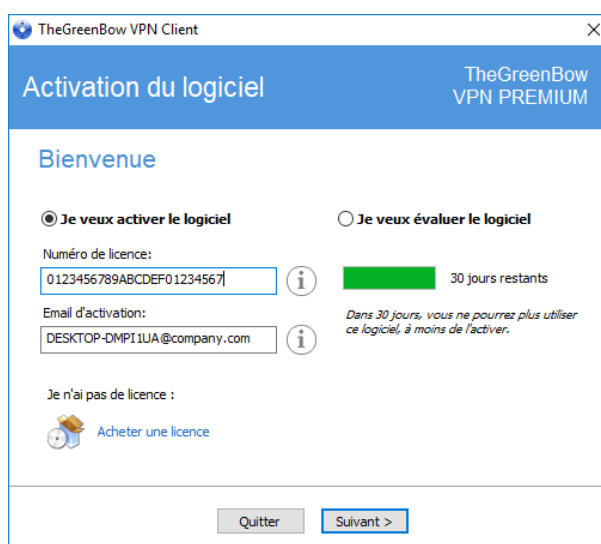
Entrer dans le champ "Copier ici votre numéro de licence.:" le numéro de licence reçu par email.

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.



Note pour l'administrateur : En version VPN PREMIUM, le champ "email d'activation" est rempli par défaut avec le "username" du poste sur lequel le logiciel est installé (sous la forme "username@company.com"). Ce mécanisme propose à l'administrateur qui gère une licence logicielle "master" une façon d'identifier unitairement chaque poste activé. Cela lui permet de gérer les activations et désactivations logicielles de façon déterministe.

3.2 Etape 2

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

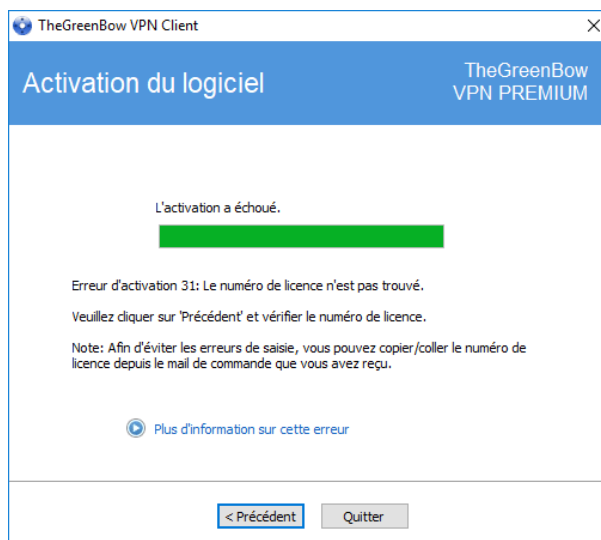
Lorsque l'activation aboutit, cliquer sur "Démarrer" pour lancer le logiciel.

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.



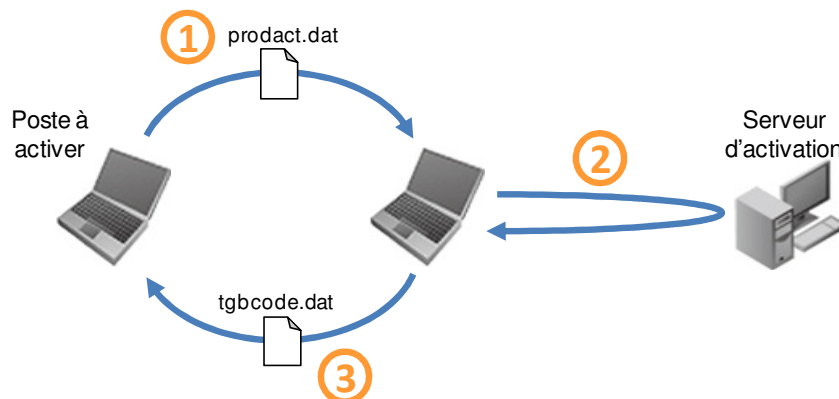
TheGreenBow indique sur son site web toutes les erreurs d'activation ainsi que [les procédures de résolution des problèmes d'activation](#).

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 "product.dat" Sur le poste à activer, récupérer le fichier "product.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 product.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 "product.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 "product.dat" créé sur le poste à activer. Cliquer sur "Envoyer". Le serveur d'activation vérifie la validité des informations du fichier product.dat.

Cliquer sur "Effectuer".

Le serveur d'activation présente en téléchargement le fichier contenant le code d'activation destiné au poste à activer.



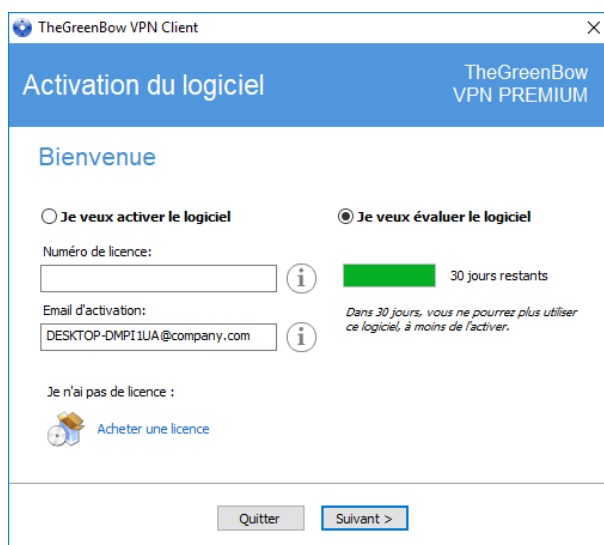
Ce fichier a un nom de la forme : tgbcod_[date]_[code].dat (par exemple : tgbcod__20120625_1029.dat)

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 >"

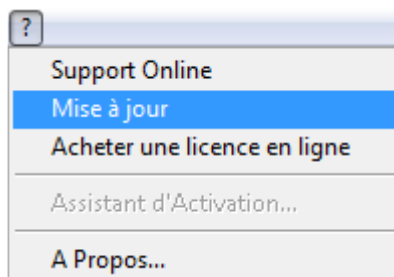
A la fin de la période de validité de la licence temporaire, le logiciel doit être activé par une licence définitive pour fonctionner.

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 :

Dernière version disponible

Cette page fournit des informations sur la version du logiciel que vous pouvez installer, en fonction de vos options d'achat.

| Votre Produit | | | |
|---|---|-----------------------|-------------------------|
| Produit: IPsec VPN Client Certified | La version de votre logiciel est 6.50.005 | | |
|  | Durée de abonnement : 1 (année(s)) | Commence : 06/06/2020 | Se termine : 06/06/2021 |
|  | Activations faites/autorisées: 14/25 | | |

| Versions du logiciel disponibles | | | | |
|---|------------|--|---|---|
|  5.2 | 02/06/2014 | 5.22.005 Release Note |  | Télécharger le logiciel |

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

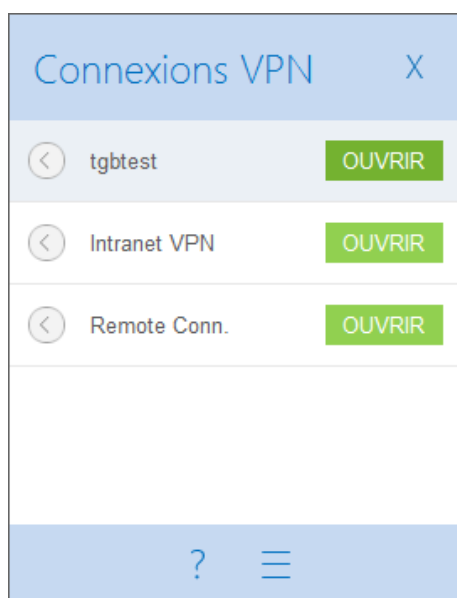
6.1 Ouvrir un tunnel VPN

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"

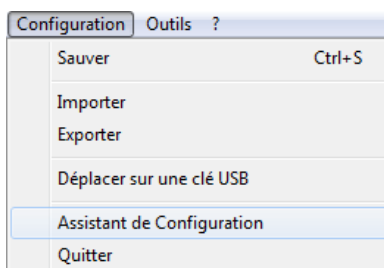
Ou dans le panneau de configuration, double-cliquer sur le tunnel "TgbTest" dans l'arborescence



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

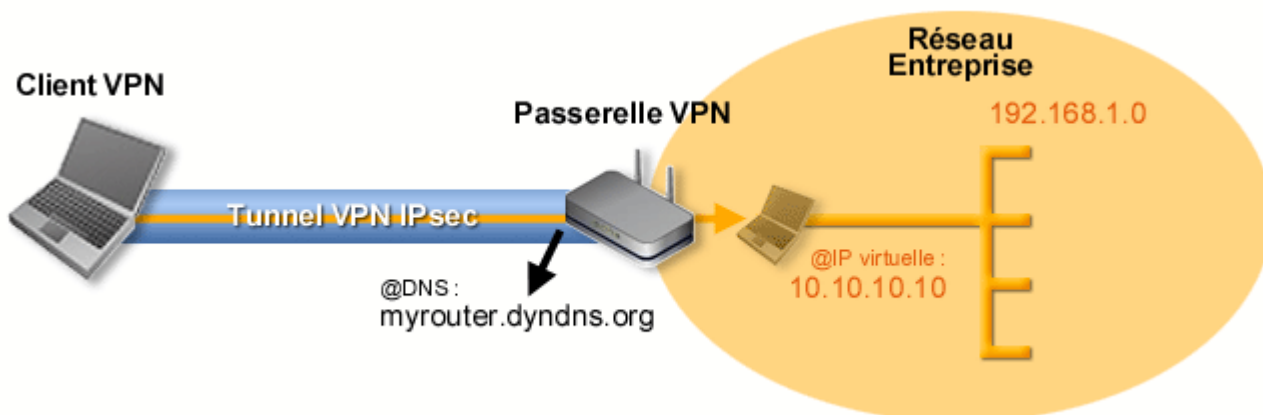
Note : Dans la version "TheGreenBow VPN Certified" les modes 2/ et 3/ sont désactivés.

7 Assistant de configuration

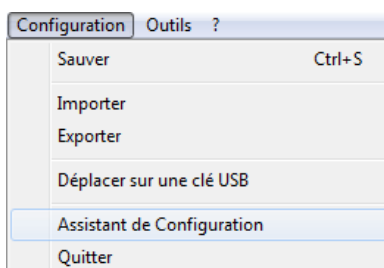
L'assistant de configuration du Client VPN TheGreenBow permet de configurer un tunnel VPN en 3 étapes simples.

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

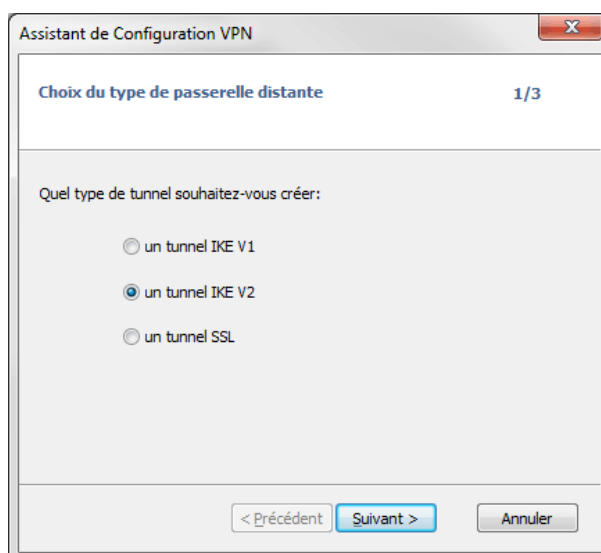


Dans l'interface principale, ouvrir l'assistant de configuration VPN : "Configuration > Assistant de Configuration"



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)

The screenshot shows a window titled "Assistant de Configuration VPN" with a close button in the top right corner. The main title is "Caractéristiques du tunnel VPN" and the progress indicator is "2/3". Below the title, it says "Entrer les caractéristiques du tunnel VPN suivantes :". There are three input fields: "Adresse IP ou DNS publique (externe) : de l'équipement distant" with the value "myrouter.dyndns.org", "Valeur de la clé partagée :" with a masked value of "*****", and "Adresse IP privée (interne) : du réseau distant" with the value "192 . 168 . 1 . 0". At the bottom, there are three buttons: "< Précédent", "Suivant >", and "Annuler".

(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 :

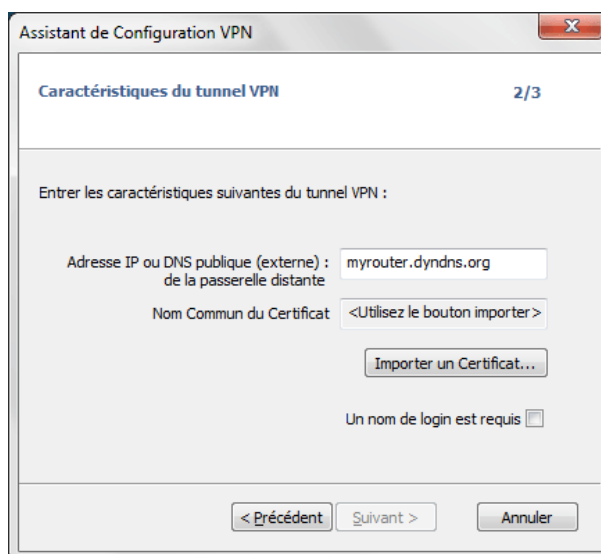
- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (exemple : myrouter.dyndns.org)
- Une clé partagée ("pre-shared key") qui doit être configurée de façon identique sur la passerelle
- OU Un certificat qui doit être importé grâce au bouton "Importer un Certificat..." (voir chapitre "Importer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

The screenshot shows a window titled "Assistant de Configuration VPN" with a close button in the top right corner. The main title is "Caractéristiques du tunnel VPN" and the progress indicator is "2/3". Below the title, it says "Entrer les caractéristiques suivantes du tunnel VPN :". There are two input fields: "Adresse IP ou DNS publique (externe) : de la passerelle distante" with the value "myrouter.dyndns.org" and "Nom Commun du Certificat" with the value "<Utilisez le bouton importer >". Below these fields is a button labeled "Importer un Certificat...". At the bottom, there are two radio buttons: "Clé Partagée" (unselected) and "Certificat" (selected). At the very bottom, there are three buttons: "< Précédent", "Suivant >", and "Annuler".

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")



Assistant de Configuration VPN

Caractéristiques du tunnel VPN 2/3

Entrer les caractéristiques suivantes du tunnel VPN :

Adresse IP ou DNS publique (externe) : myrouter.dyndns.org
de la passerelle distante

Nom Commun du Certificat <Utilisez le bouton importer >

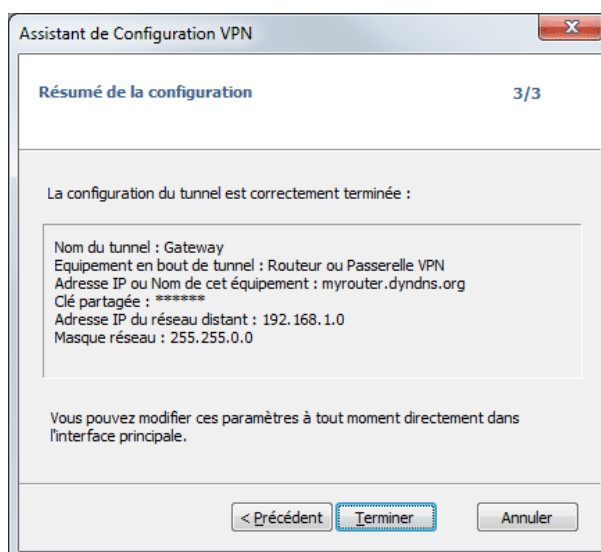
Importer un Certificat...

Un nom de login est requis

< Précédent Suivant > Annuler

Etape 3 :

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



Assistant de Configuration VPN

Résumé de la configuration 3/3

La configuration du tunnel est correctement terminée :

Nom du tunnel : Gateway
Equipement en bout de tunnel : Routeur ou Passerelle VPN
Adresse IP ou Nom de cet équipement : myrouter.dyndns.org
Clé partagée : *****
Adresse IP du réseau distant : 192.168.1.0
Masque réseau : 255.255.0.0

Vous pouvez modifier ces paramètres à tout moment directement dans l'interface principale.

< Précédent Terminer Annuler

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](#)

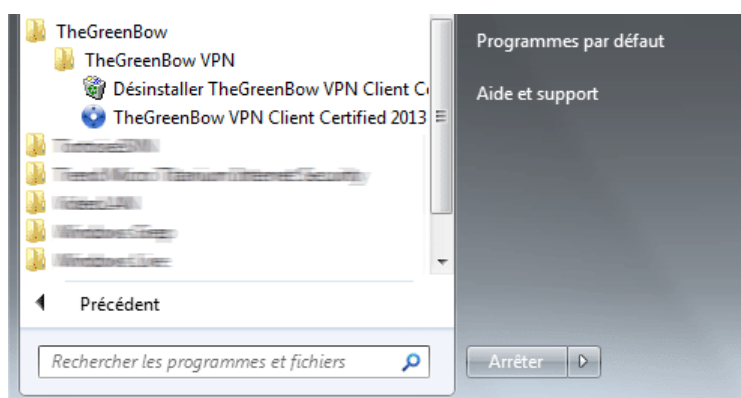
8.2 Bureau Windows

8.2.1 Menu Démarrer

À 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.

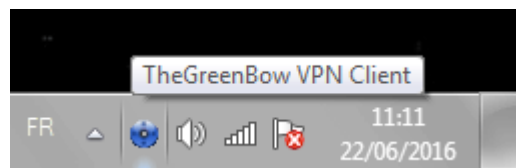
Le Client VPN peut être lancé directement en double-cliquant sur cet icône.



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 :

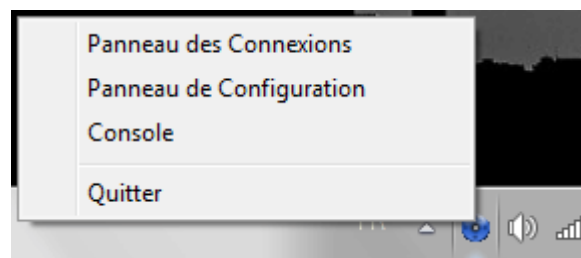
- "Tunnel <NomDuTunnel>" si un ou plusieurs tunnels sont ouverts.
- "Attente VPN prêt..." pendant le temps de lancement du moteur VPN IKE.
- "TheGreenBow VPN Client Certified" lorsque le Client VPN est lancé, sans tunnel ouvert.

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 :



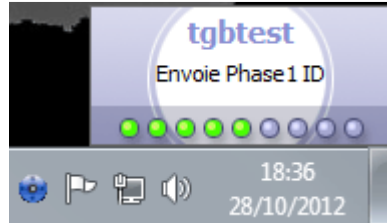
Les items du menu contextuel sont les suivants :

- 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



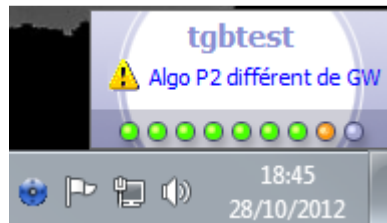
Tunnel ouvert



Tunnel fermé



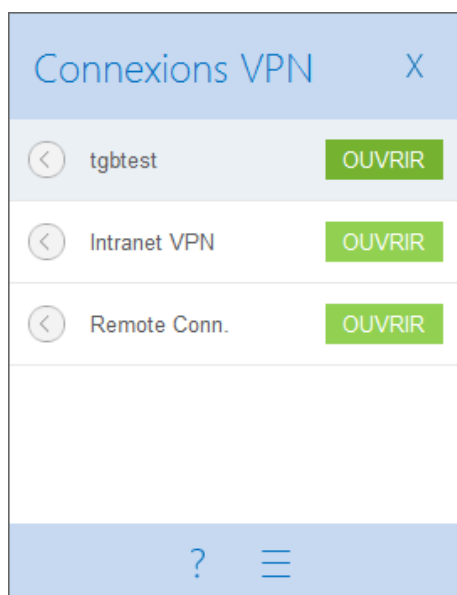
Incident d'ouverture du tunnel : la fenêtre affiche l'explication succincte de l'incident, et un lien cliquable vers plus d'informations sur cet incident.



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 VPN](#)")
-  Fermer le panneau des connexions

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

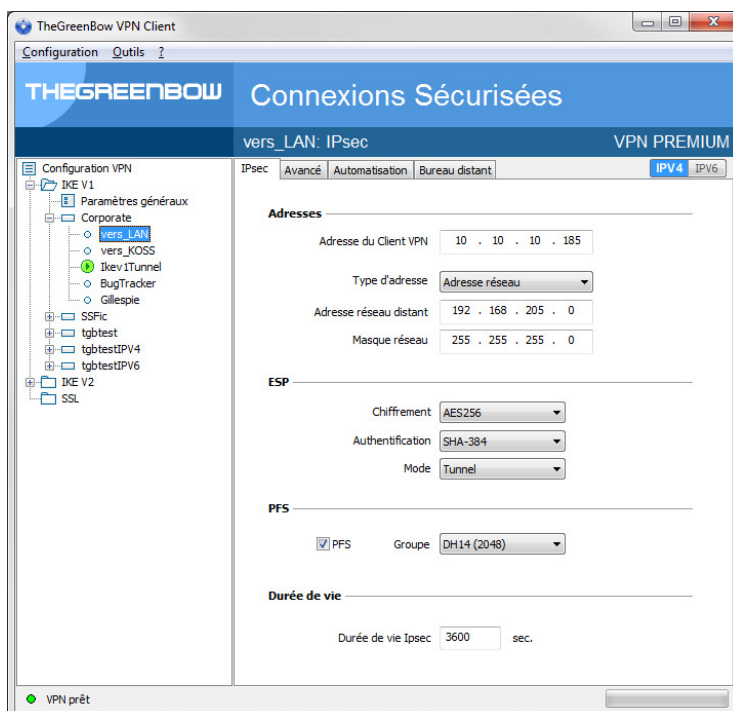
- ESC (ou ALT+F4) ferme la fenêtre
- CTRL+ENTER ouvre le panneau de configuration (interface principale)
- CTRL+O ouvre la connexion VPN sélectionnée
- CTRL+W ferme la connexion VPN sélectionnée
- Les flèches haut / bas permettent de se déplacer parmi les connexions VPN

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

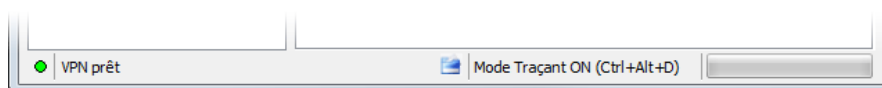
Les menus du panneau de configuration sont les suivants :


- Configuration
 - Sauver
 - Importer : Importation d'une politique de sécurité VPN (Configuration VPN)
 - Exporter : Exportation d'une politique de sécurité VPN (Configuration VPN)
 - Déplacer sur une clé USB : Mode USB
 - [Assistant de Configuration](#)
 - Quitter : Fermer les tunnels VPN ouverts et quitter le logiciel
- Outils
 - [Panneau des Connexions](#)
 - [Configuration 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.

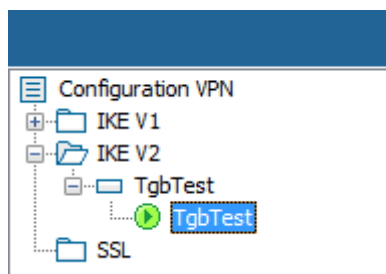
10.3 Raccourcis

| | |
|------------|--|
| 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
[IKEv1 \(Phase1\) : Authentification](#)
[IKEv1 \(Phase2\) : IPsec](#)
2. Tunnel VPN IPsec IKEv2
[IKEv2 \(IKE Auth\) : Authentification](#)
[IKEv2 \(Child SA\) : IPsec](#)
3. Tunnel VPN SSL
[SSL : TLS](#)

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 | |
| Déplacer sur la clé USB... | |
| Sauver | Ctrl+S |
| Assistant de Configuration | |
| Recharger la configuration par défaut | |
| Reset | Del |
| Fermer tous les tunnels | |

| | |
|---------------------------------------|--|
| Export | Permet d' exporter la politique de sécurité VPN complète. |
| Déplacer sur la clé USB... | Déplacer la politique de sécurité VPN sur une clé USB et initier le Mode USB |
| 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 :

| | | | | | |
|-------------------|--------|-----------------|--------|-------------|--------|
| Export | | Export | | Export | |
| Sauver | Ctrl+S | Sauver | Ctrl+S | Sauver | Ctrl+S |
| Nouvelle Phase 1 | Ctrl+N | Nouvel IKE Auth | Ctrl+N | Nouveau TLS | Ctrl+N |
| Coller la Phase 1 | Ctrl+V | Coller IKE Auth | Ctrl+V | Coller TLS | Ctrl+V |
| 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 | Ctrl+C | Copier | Ctrl+C |
| Renommer | F2 | Renommer | F2 |
| Supprimer | Del | Supprimer | Del |
| Nouvelle Phase 2 | Ctrl+N | Nouveau Child SA | Ctrl+N |
| Coller la Phase 2 | Ctrl+V | Coller Child SA | Ctrl+V |

| | |
|---|--|
| 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 ajoute 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 :

| | |
|-----------------|--------|
| Ouvre Tunnel... | Ctrl+O |
| Export | |
| Copier | Ctrl+C |
| Renommer | F2 |
| Supprimer | Del |

Menu tunnel fermé

| | |
|------------------|--------|
| Fermer le tunnel | Ctrl+W |
| Export | |
| Copier | Ctrl+C |
| Renommer | F2 |
| Supprimer | Del |

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

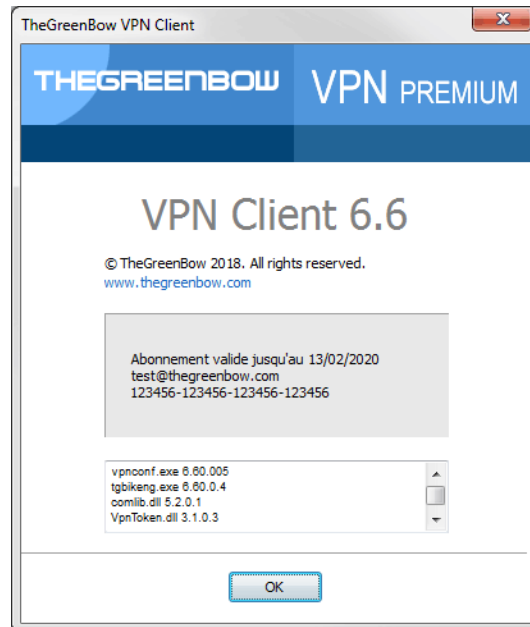
Pour la gestion de l'arborescence, les raccourcis suivants sont disponibles :

- | | |
|--------|--|
| 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 :

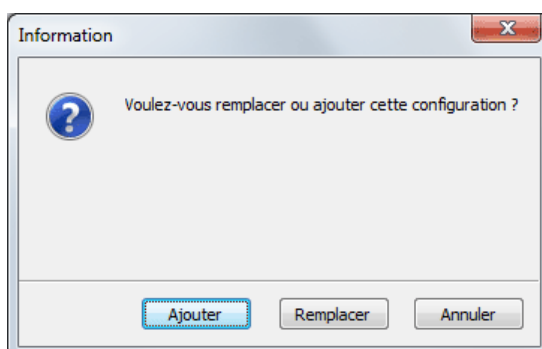
- Par le menu "Configuration > Importer" du Panneau de Configuration (interface principale)
- Par "Glisser-déposer" d'un fichier de Configuration VPN (fichier ".tgb") sur le Panneau de Configuration (interface principale)
- Par double-clic sur un fichier de Configuration VPN (fichier ".tgb") (1)
- Par ligne de commande en utilisant l'option "/import " (2)

(1) Note : 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".

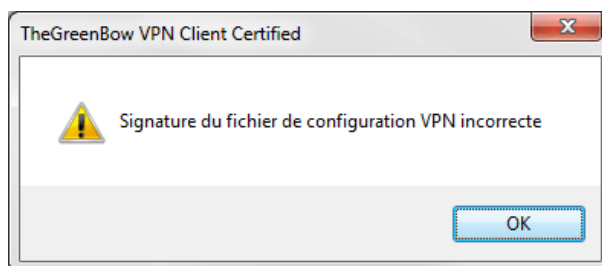
A l'importation d'une Configuration VPN, il est demandé à l'utilisateur s'il veut ajouter la nouvelle Configuration VPN à la Configuration courante, ou s'il veut remplacer (écraser) la Configuration courante par la nouvelle Configuration VPN :



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

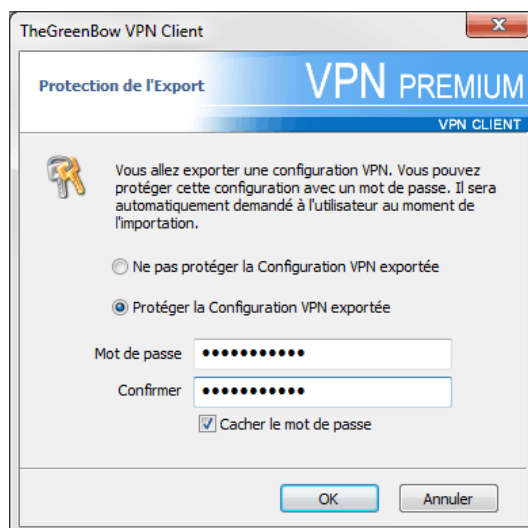
Le Client VPN TheGreenBow permet d'exporter une politique de sécurité VPN de différentes façons :

- 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 : Authentication

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

Cryptographie

| | |
|------------------|---|
| Chiffrement | Algorithme de chiffrement négocié au cours de la Phase d'Authentification (1) : Auto (2), DES, 3DES, AES-128, AES-192, AES-256. |
| Authentification | Algorithme d'authentification négocié au cours de la Phase d'Authentification (1) : Auto (2), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. |
| Groupe de clé | Longueur de la clé Diffie-Hellman (1) : Auto (2), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) |

(1) Cf. "[Recommandations de sécurité](#)" pour le choix de l'algorithme

(2) 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.

X-Auth

Activé X-Auth Popup

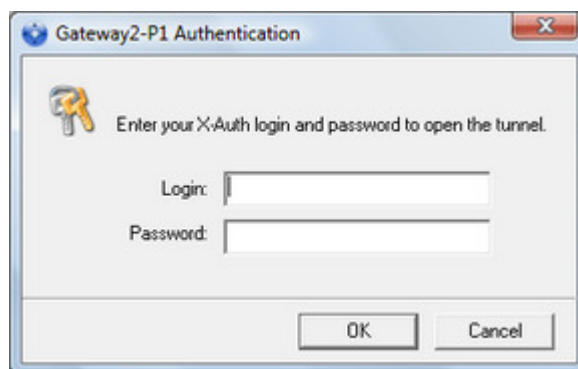
Login

Mot de passe

Unique

Hybrid Mode

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.

X-Auth

Activé X-Auth Popup

Login Unique

Mot de passe Hybrid Mode

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.

X-Auth

Activé X-Auth Popup

Login

Mot de passe

Unique Hybrid Mode

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 : Protocole

The screenshot shows a configuration window with tabs for 'Authentification', 'Protocole', 'Passerelle', and 'Certificat'. The 'Protocole' tab is active. Under the 'Identité' section, there are fields for 'Local ID' (set to 'Sujet X509') and 'Remote ID'. A dropdown menu shows 'C = FR, ST = Paris, O = TheGreenBow'. The 'Fonctions avancées' section includes checkboxes for 'Fragmentation', 'Mode Config', and 'Mode Agressif'. There are also input fields for 'Port IKE', 'Port NAT', and 'Taille des fragments'. A 'NAT-T' dropdown is set to 'Automatique'.

Identité

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.

Fonctions avancées

| | | | | | | | |
|---|---|-----------|--|-------------|--|-------|--|
| Fragmentation / Taille des fragments | Cette option active la fragmentation IKE qui évite que des paquets soient fragmentés (et potentiellement bloqués) au niveau IP. En général, il convient de spécifier une taille de fragment inférieure à la MTU de l'interface physique, par exemple 1400 octets dans le cas d'une MTU classique de 1500. | | | | | | |
| 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. <u>A noter</u> : 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. <u>A noter</u> : 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 | Lorsque le port IKE est différent de 500, il peut être nécessaire de cocher cette option pour que la passerelle accepte la connexion. | | | | | | |
| 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. | | | | | | |
| 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. | | | | | | |
| NAT-T | Mode "NAT-Traversal". Le Client VPN permet de gérer 3types de modes NAT-T : <table border="1" data-bbox="517 1391 1457 1693"> <tr> <td>Désactivé</td> <td>Empêche le Client VPN et la Passerelle VPN de passer en mode NAT-Traversal</td> </tr> <tr> <td>Automatique</td> <td>Laisse le Client VPN et la Passerelle VPN négocier le mode NAT-Traversal</td> </tr> <tr> <td>Forcé</td> <td>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.</td> </tr> </table> | 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. |
| 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. | | | | | | |

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. "[Phase2 : 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 : Passerelle

Dead Peer Detection (DPD)

Dead Peer Detection

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.

Durée de vie

Durée de vie

Les durées de vie sont échangées lors de la montée du tunnel (1).
A échéance de la durée de vie, la phase1 est renégociée.
La valeur par défaut de la durée de vie de la Phase1 est de 2700 sec (45 min.)

(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.

Paramètres relatifs à la passerelle

| | |
|-----------------------|---|
| 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 |
| Retransmissions | Nombre de retransmissions de messages protocolaires IKE sur non-réponse de la passerelle. A l'issue de ces retransmissions, le tunnel est déclaré en échec. |

13.3.4 Phase1 : Certificat

Voir le chapitre [Gestion des Certificats](#).

13.3.5 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.

13.3.6 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 (1) : Auto (2), DES, 3DES, AES-128, AES-192, AES-256. |
| Authentification | Algorithme d'authentification négocié au cours de la Phase IPsec (1) : Auto (2), MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512. |
| Mode | Mode d'encapsulation IPsec : Tunnel ou Transport (1) |

(1) Cf. "[Recommandations de sécurité](#)" pour le choix de l'algorithme

(2) 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) |
| | <u>Note</u> : 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 | Les durées de vie sont échangées lors de la montée du tunnel. (1) A échéance de la durée de vie, la phase 2 est renégociée. La valeur par défaut de la durée de vie de la Phase2 est de 1800 sec. (30 min.) |
|--------------|---|

(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 :

| | |
|------------------------|--|
| Type d'adresse | <input type="text" value="Adresse réseau"/> |
| Adresse réseau distant | <input type="text" value="192 . 168 . 175 . 0"/> |
| Masque réseau | <input type="text" value="255 . 255 . 255 . 0"/> |

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

| | |
|------------------|----------------------|
| Type d'adresse | Plage d'adresses |
| Adresse de début | 192 . 168 . 175 . 1 |
| Adresse de fin | 192 . 168 . 175 . 10 |

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

| | |
|-----------------------|---------------------|
| Type d'adresse | Adresse Poste |
| Adresse poste distant | 192 . 168 . 175 . 1 |

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_gateway.html

13.3.7 Phase2 : Avancé

IPsec Avancé Automatisation Bureau distant IPv4 IPv6

Serveurs alternatifs

Suffixe DNS dev.corporate

| Type | Adresse IP | |
|------|-----------------|---|
| DNS | 192.168.205.203 | ✘ |
| WINS | 192.168.205.203 | ✘ |

Ajout DNS

Ajout WINS

Test de trafic dans le tunnel

Periodicité et adresse IP de la machine distante à pinger:

Adresse IPv4 0 . 0 . 0 . 0

Fréquence de test 0 sec.

Serveurs alternatifs

| | |
|----------------------|---|
| Suffixe DNS | <p>Suffixe de domaine à ajouter à chaque nom de machine, par exemple : "mozart.dev.corporate".</p> <p>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.</p> |
| Serveurs alternatifs | <p>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".</p> <p><u>A noter</u> : 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.</p> |

Test de trafic dans le tunnel

| | |
|-------------------|---|
| Adresse IP | <p>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.</p> <p>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.</p> <p>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.</p> |
| Fréquence de test | <p>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.</p> |

13.3.8 Phase2 : Automatisation

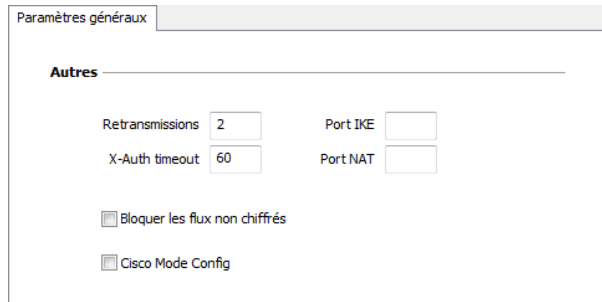
Voir le chapitre [Automatisation](#)

13.3.9 Phase2 : Bureau distant

Voir le chapitre [Partage de bureau distant](#)

13.3.10 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 : Les Port IKE configurables dans chaque tunnel sont prioritaires par rapport à ce paramètre. |
| Port NAT | Ce champ permet de configurer le Port NAT pour tous les tunnels IKEv1. Note : Les Port NAT configurables dans chaque tunnel sont prioritaires 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 |
| Cisco Mode Config | Cette case doit être cochée pour assurer la compatibilité avec les passerelles de type Cisco ASA (version Premium et Certifiée seulement) |

(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". |
| | |
| 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. <u>A noter</u> : 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 | <p>Le mode EAP (Extensible 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.</p> <p>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.</p> <p>Ce dernier mode n'est pas recommandé dans le cadre de l'utilisation du logiciel en mode certifié. Cf. "Recommandations de sécurité"</p> |
|-----|--|

| | |
|-----------------------|---|
| 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 (1) : Auto (2), DES, 3DES, AES-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256). |
| Authentification | Algorithme d'authentification négocié au cours de la Phase d'Authentification (1) : Auto (2), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. |
| Groupe de clé | Longueur de la clé Diffie-Hellman (1) : Auto (2), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192), DH19 (ECP256), DH20 (ECP384), DH21 (ECP521), No Diffie-Hellman. |

- (1) Cf. "[Recommandations de sécurité](#)" pour le choix de l'algorithme.
- (2) 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-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256)
 - Authentification : MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512
 - Groupe de clé : DH1, DH2, DH5, DH14, DH15, DH16, DH17, DH18, DH19, DH20, DH21
- 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 : Protocole

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 = 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.

Fonctions avancées

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). |
| Port IKE | <p>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.</p> <p><u>A noter</u> : La Passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Auth sur un port différent de 500.</p> |
| Port NAT | <p>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.</p> <p><u>A noter</u> : La Passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Child SA sur un port différent de 4500.</p> |
| Activer l'offset NATT | Lorsque le port IKE est différent de 500, il peut être nécessaire de cocher cette option pour que la passerelle accepte la connexion. |

13.4.3 IKE Auth : Passerelle

The screenshot shows a configuration window with four tabs: 'Authentification', 'Protocole', 'Passerelle', and 'Certificat'. The 'Passerelle' tab is active. It contains three sections:

- Dead Peer Detection (DPD)**:
 - Période de vérification: 30 sec.
 - Nombre d'essais: 5
 - Durée entre essais (sec.): 15 sec.
- Durée de vie**:
 - Durée de vie: 1800 sec.
- Paramètres relatifs à la passerelle**:
 - Passerelle redondante: (empty text box)
 - Retransmissions: 3
 - Délai passerelle: 5 sec.

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 | Durée de vie de la phase IKE Authentication. La durée de vie est exprimée en secondes. Sa valeur par défaut est de 1800 secondes. |
|--------------|---|

Paramètres relatifs à la passerelle

| | |
|-----------------------|---|
| 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 |
| Retransmissions | Nombre de retransmissions de messages protocolaires IKE avant échec. |
| Délai passerelle | Délai entre chaque retransmission |

13.4.4 IKE Auth : Certificat

Voir le chapitre : [Gestion des Certificats](#)

13.4.5 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.

13.4.6 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 <u>configuration du Type d'adresse</u> |
| 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 (1) : Auto (2), DES, 3DES, AES-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256). |
| Intégrité | Algorithme d'authentification négocié au cours de la Phase IPsec (1) : Auto (2), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. |
| Diffie-Hellman | Longueur de la clé Diffie-Hellman (1) : Auto (2), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192), DH19 (ECP256), DH20 (ECP384), DH21 (ECP521), No Diffie-Hellman. |

(1) Cf. "[Recommandations de sécurité](#)" pour le choix de l'algorithme.

(2) 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-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256)
- Authentification : MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512
- Groupe de clé : , DH2, DH5, DH14, DH15, DH16, DH17, DH18, DH19, DH20, DH21

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

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 :

| | |
|------------------------|---------------------|
| Type d'adresse | Adresse réseau ▼ |
| Adresse réseau distant | 192 . 168 . 175 . 0 |
| Masque réseau | 255 . 255 . 255 . 0 |

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

| | |
|------------------|----------------------|
| Type d'adresse | Plage d'adresses ▼ |
| Adresse de début | 192 . 168 . 175 . 1 |
| Adresse de fin | 192 . 168 . 175 . 10 |

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

| | |
|-----------------------|---------------------|
| Type d'adresse | Adresse Poste ▼ |
| Adresse poste distant | 192 . 168 . 175 . 1 |

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_gateway.html

13.4.7 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.

Test de trafic dans le tunnel

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.

Fréquence de test

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.

Autres

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"

13.4.8 Child SA : Automatisation

Voir le chapitre "[Automatisation](#)"

13.4.9 Child SA : Bureau distant

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](#)"

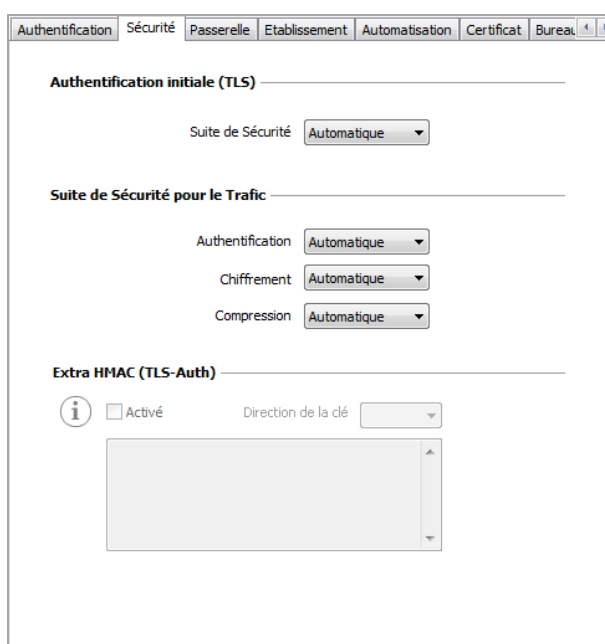
Extra Authentication

Extra authentication

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 "Pop up 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. <u>Note</u> : 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 | <p>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")</p> <p>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 :</p> <pre>-----BEGIN Static key----- 362722d4fbff4075853fbe6991689c36 b371f99aa7df0852ec70352122aee7be ... 515354236503e382937d1b59618e5a4a cb488b5dd8ce9733055a3bdc17fb3d2d -----END Static key-----</pre> <p>La "Direction de la clé" doit être choisie :</p> <ul style="list-style-type: none">- 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 Passerelle

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, il revient à "Oui" dans cette version. |
| 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 | <p>Les clés peuvent être renégociées sur échéance de 3 critères (qui peuvent être combinés) :</p> <ul style="list-style-type: none"> - Quantité de trafic, exprimée en Ko - Quantité de paquets, exprimée en nombre de paquets - Durée de vie, exprimée en seconde <p>Si plusieurs critères sont configurés, les clés sont renégociées sur échéance du premier critère vérifié</p> |
|-------------------------------|---|

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 : <ul style="list-style-type: none"> - 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 <p><u>Note</u> : Vérifier que les deux choix "Tunnel IPv4" et "Tunnel IPv6" ne sont pas tous deux à "Non".</p> |
| Tunnel IPv6 | Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv6 : <ul style="list-style-type: none"> - 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 <p><u>Note</u> : Vérifier que les deux choix "Tunnel IPv4" et "Tunnel IPv6" ne sont pas tous deux à "Non".</p> |

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 Certificats](#)

13.5.8 Bureau distant

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 : bascule vers un tunnel de repli (tunnel fallback), 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.

Ces automatismes sont disponibles pour tout type de tunnel : IKEv1, IKEv2 et SSL.

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).

Tunnel de repli (fallback)

Cf. chapitre 16 "[VPN Tunnel Fallback](#)"

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 plus proposée dans le logiciel à partir de la version 6.62. 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.

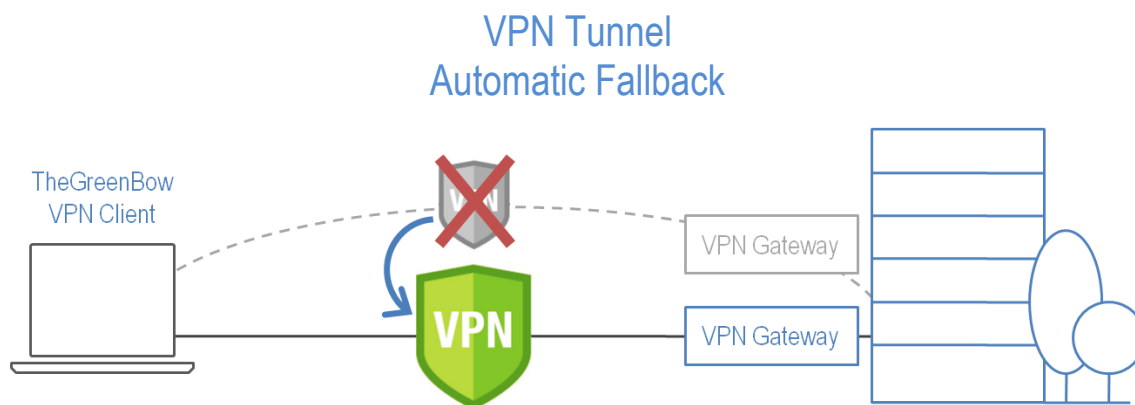
Les applications sont nombreuses :

- 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 VPN Tunnel Fallback

Le Client VPN TheGreenBow implémente une fonction de tunnel de repli (tunnel fallback) qui permet de tenter automatiquement l'ouverture d'un tunnel alternatif lorsque l'ouverture du premier tunnel échoue.



Cette fonction se configure dans l'onglet "Automatisation" de chaque tunnel (IKEv1, IKEv2 ou SSL).

Tunnel de repli

Repli vers le tunnel: (IKEv2) TgbTest-TgbTest

Message à afficher: Attention : tunnel fallback.

Nombre d'essais: 1

Autoriser l'utilisateur à refuser le repli

| | |
|--|---|
| Repli vers le tunnel | Le champ présente la liste des tunnels vers lequel le logiciel peut basculer automatiquement si le tunnel en cours d'édition est indisponible. |
| Message à afficher | Comme cette fonction peut passer automatiquement d'un tunnel à un autre, le second étant par exemple moins sécurisé que le premier, il est possible de saisir un message d'avertissement à l'utilisateur, qui lui sera délivré à chaque bascule vers le tunnel de fallback. |
| Nombre d'essais | Le nombre d'essais de fallback est enregistré de façon à éviter les boucles de bascules sans fin (un tunnel 1 qui se replie sur un tunnel 2 qui se replie sur un tunnel 1). |
| Autoriser l'utilisateur à refuser ce repli | Permet de configurer la fonction de repli de façon à ce que ce soit l'utilisateur qui décide de passer d'un tunnel à l'autre. |

17 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 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.

The image shows two side-by-side screenshots of the 'Child SA' configuration window in TheGreenBow VPN Client. Both windows have tabs for 'Avancé', 'Automatisation', and 'Bureau distant'. The left window has the 'IPv4' button selected, and the right window has the 'IPv6' button selected. Both windows have a 'Trafic sélecteurs' section with the following fields:

| Field | IPv4 Configuration | IPv6 Configuration |
|------------------------|--------------------|------------------------|
| Adresse du Client VPN | 0 . 0 . 0 . 0 | :: |
| Type d'adresse | Adresse réseau | Adresse réseau |
| Adresse réseau distant | 0 . 0 . 0 . 0 | :: |
| Masque réseau | 0 . 0 . 0 . 0 | Longueur du préfixe: 0 |

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.

18 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'installateur 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

18.1 Configuration

18.1.1 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.

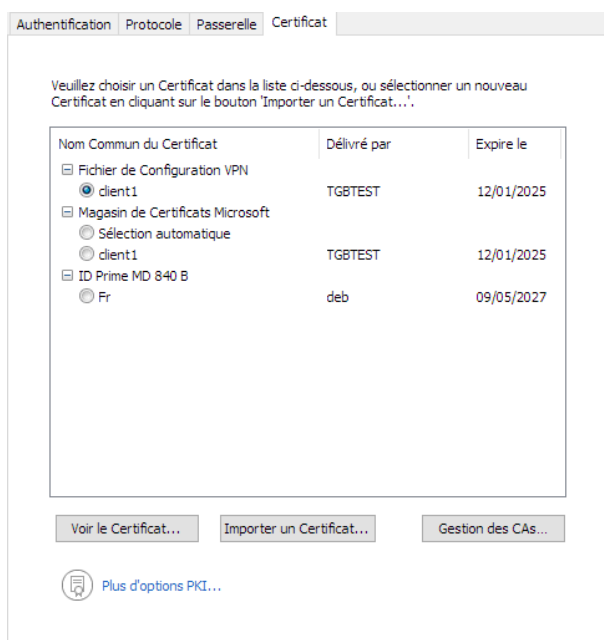
Le Client VPN permet de choisir un certificat stocké :

- 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](#)")

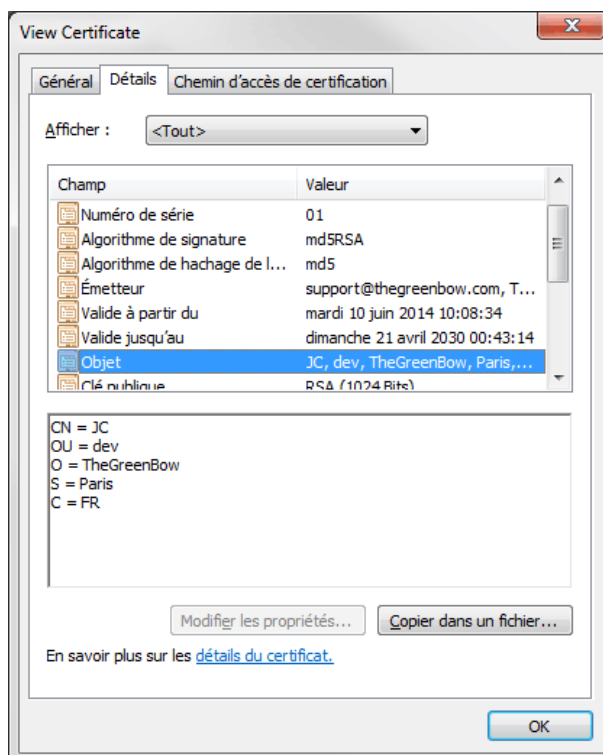
L'onglet "Certificat" du tunnel concerné énumère tous les supports accessibles sur le poste, qui contiennent des certificats. Si un support ne contient pas de certificat, il n'est pas affiché dans la liste (p.ex. si le fichier de Configuration VPN ne contient pas de certificat, il n'apparaît pas dans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

Identité

Local ID C = FR, ST = Paris, O = TheGreenBow

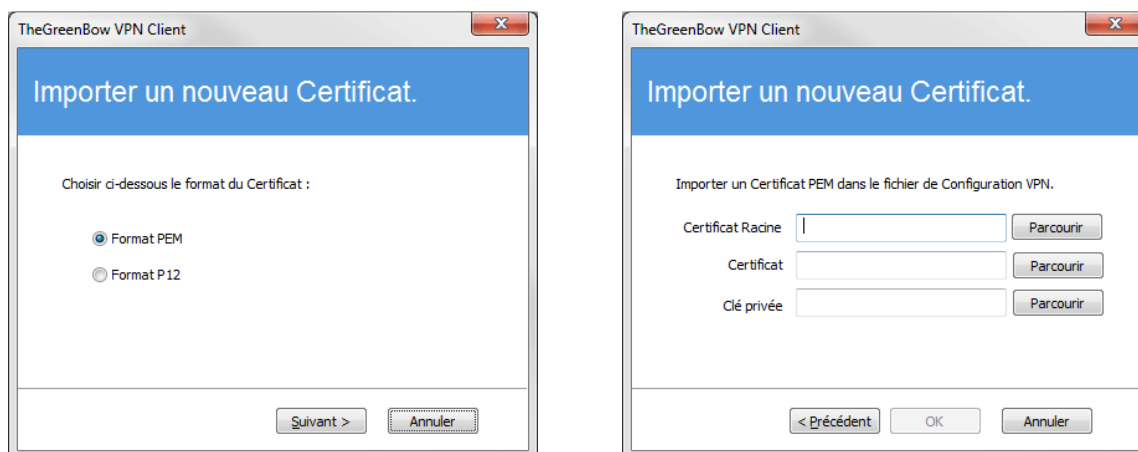
Remote ID

18.2 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

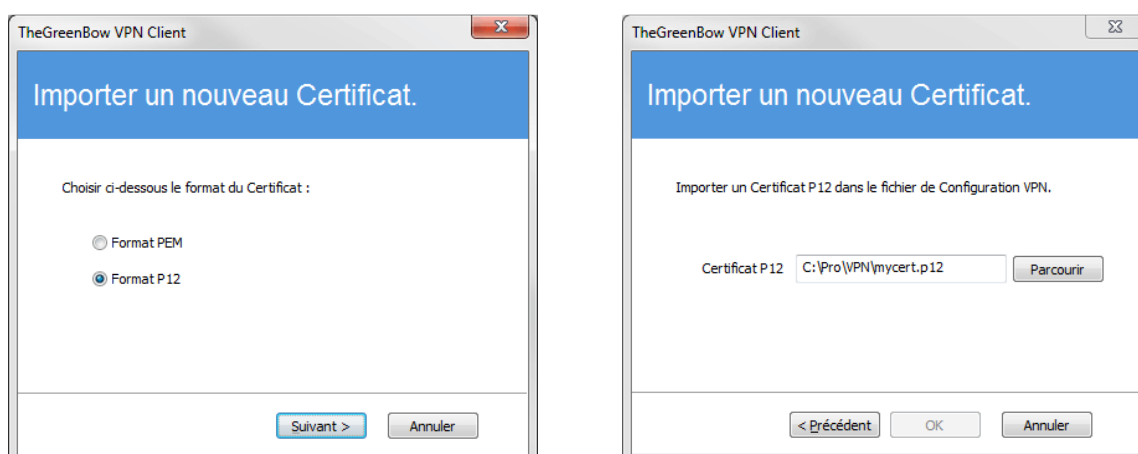
- 1/ Dans l'onglet Certificat d'une Phase 2, cliquer sur "Importer un Certificat..."
 - 2/ Choisir "Format PEM"
 - 3/ Sélectionner ("Parcourir") les certificats Racine, Utilisateur et clé privée à importer
- Note** : Le fichier avec la clé privée ne doit pas être chiffré.
- 4/ Valider



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.

18.3 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".

18.4 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.

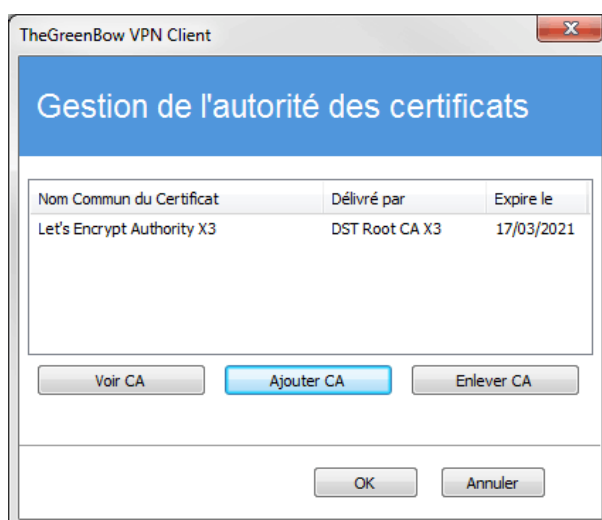
Cette fonctionnalité est décrite dans le document "Guide utilisateur Token et Carte à puce" (tgbvpn_ug_pki_smartcard_fr) disponible sur la page web : http://www.thegreenbow.fr/vpn_token.html.

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.

18.5 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

18.6 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.

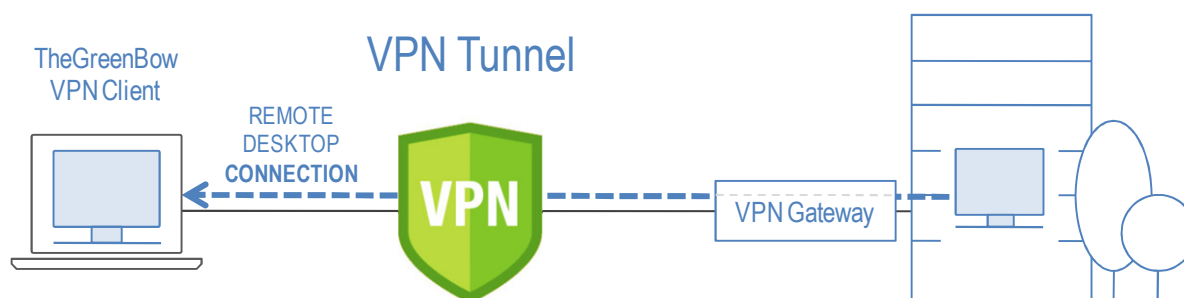
Ainsi, les tunnels associés au certificat contenu sur la Carte à puce sont montés automatiquement à l'insertion de cette Carte à puce. Réciproquement, l'extraction de la Carte à puce ferme automatiquement tous les tunnels associés.

Pour mettre en œuvre cette fonction, cocher : "Ouvrir ce tunnel automatiquement lorsqu'une clé USB est insérée" (Cf. chapitre [Automatisation](#))

19 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.



19.1 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 " Bureau distant ".
- 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.

Child SA | Avancé | Automatisation | Bureau distant | IPV4 | IPV6

Entrer ci-dessous l'adresse IP de l'ordinateur distant auquel vous souhaitez vous connecter, et choisir un alias.

Alias

Nom de l'ordinateur ou adresse IP

| Alias | Nom ou adresse IP |
|-------|-------------------|
| | |

Child SA | Avancé | Automatisation | Bureau distant | IPV4 | IPV6

Entrer ci-dessous l'adresse IP de l'ordinateur distant auquel vous souhaitez vous connecter, et choisir un alias.

Alias

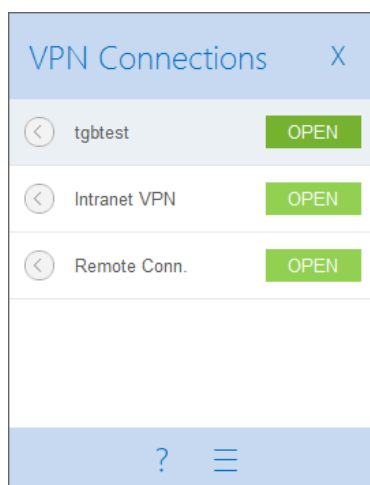
Nom de l'ordinateur ou adresse IP

| Alias | Nom ou adresse IP | |
|-------------------|-------------------|--|
| Corporate_desktop | 192.168.205.203 | |

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 "[Gestion du panneau des connexions](#)" détaillée ci-après.

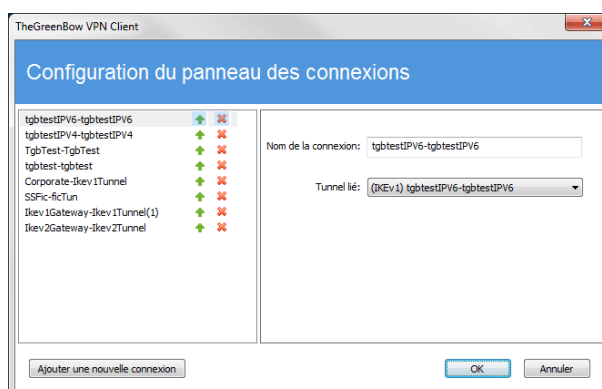
20 Gestion du panneau des connexions

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 "Bureau distant", c'est-à-dire un tunnel VPN dont la fonction "Bureau distant" 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.

Note pour l'administrateur : La configuration du panneau des connexions est mémorisée dans le fichier de configuration VPN. Elle peut donc être exportée dans les fichiers .tgb, ce qui est utile pour déployer un panneau de connexion identique sur tous les postes.

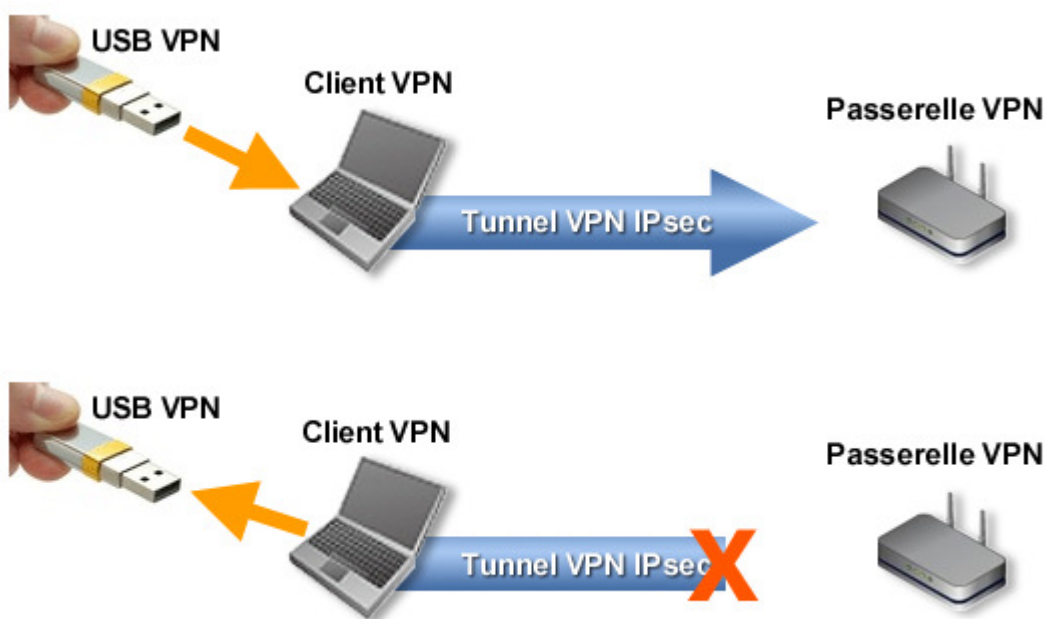
21 Mode USB

21.1 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.



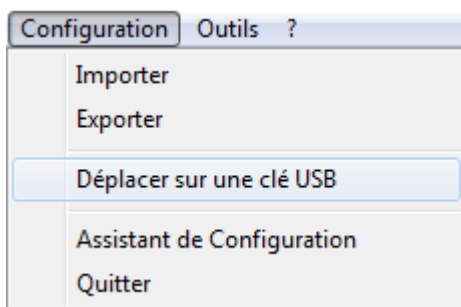
Dans le mode VPN USB :

- 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".

21.2 Configurer le Mode USB

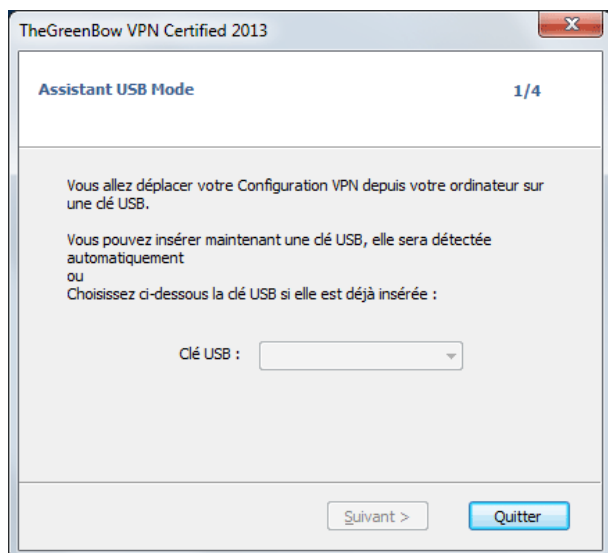
La configuration du Mode VPN USB s'effectue via l'assistant de configuration accessible par le menu "Configuration > Déplacer sur une clé USB" du panneau de configuration



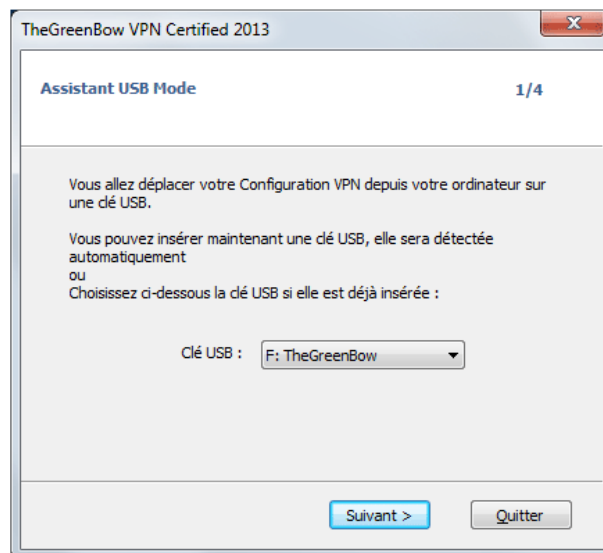
Etape 1 : Choix de la clé USB

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.

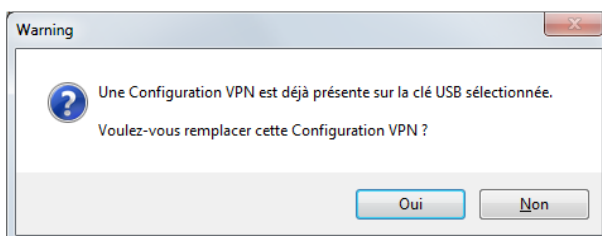
Pas de clé USB insérée



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.

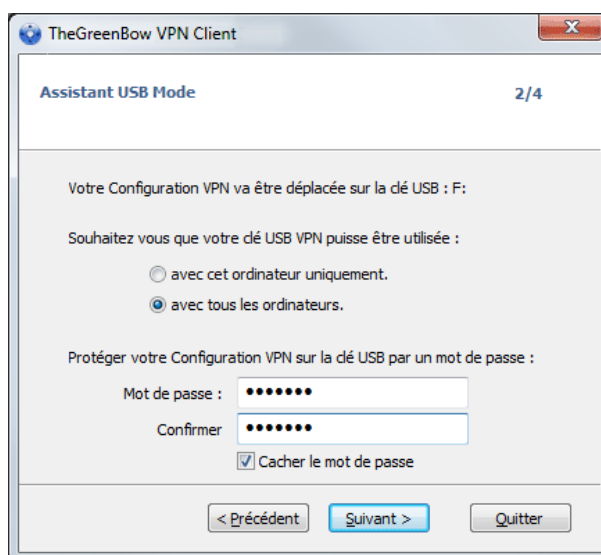
Dans ce cas, la clé USB VPN ne pourra être utilisée que sur ce poste.

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 :

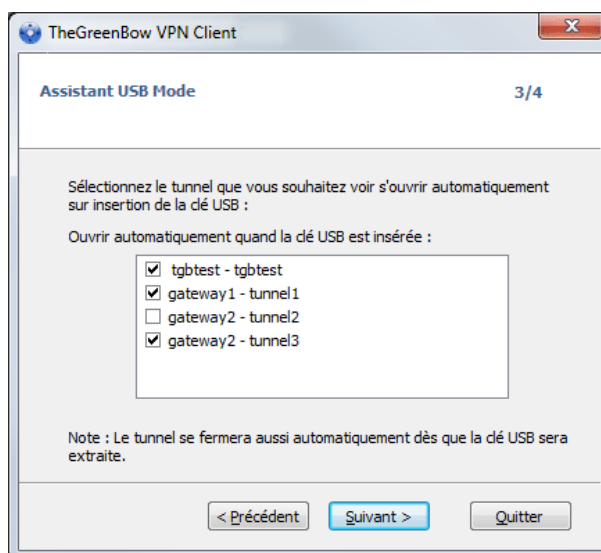
La politique de sécurité VPN USB peut être protégée par mot de passe.

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

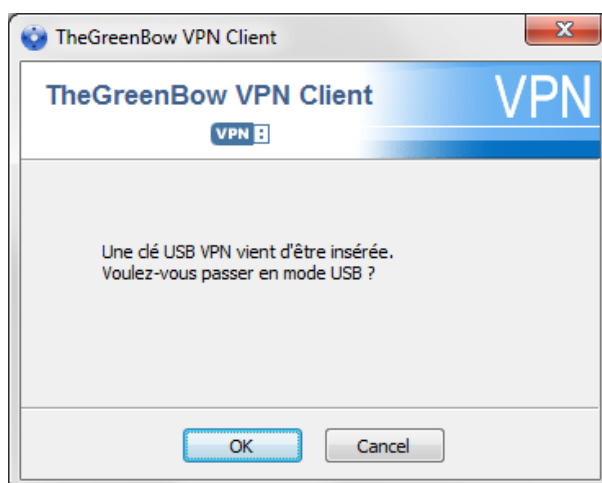
Le résumé permet de valider le bon paramétrage de la Clé USB VPN.

Sur validation de cette dernière étape, la politique de sécurité VPN du poste est transférée sur la Clé USB.

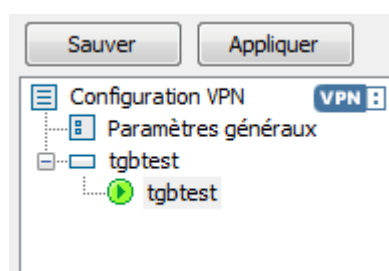
Elle reste active tant que la Clé USB reste insérée. Sur extraction de la Clé USB VPN, le Client VPN revient à une Configuration VPN vide.

21.3 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 :

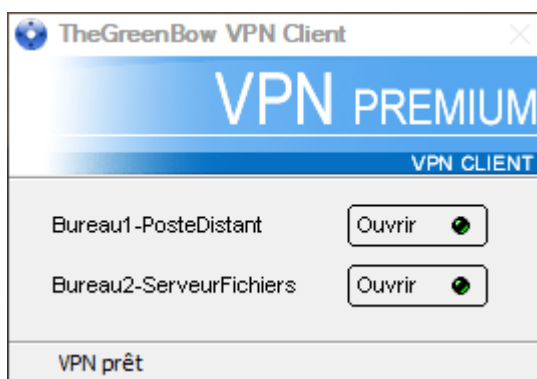
- 1/ Insérer la clé USB VPN
- 2/ Exporter la Configuration VPN
- 3/ Extraire la clé USB VPN
- 4/ Importer la configuration VPN exportée à l'étape 2
- 5/ Relancer l'assistant mode USB avec cette configuration et les nouveaux paramètres souhaités.

22 Mode GINA

22.1 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.

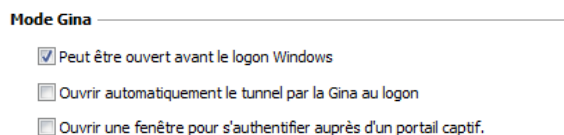
Lorsqu'un tunnel est configuré "en mode GINA", une fenêtre d'ouverture de tunnel similaire au Panneau des Connexions est affichée sur l'écran de logon Windows. Elle permet d'ouvrir manuellement le tunnel VPN.



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.

22.2 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](#)".



22.3 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](#).



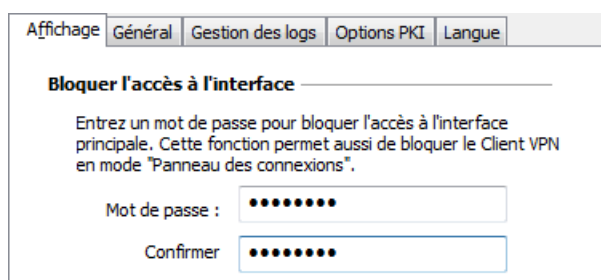
Point de sécurité : la fonction d'ouverture d'une fenêtre pour l'authentification auprès d'un portail captif est susceptible d'être vulnérable à certaines attaques (Cf. vulnérabilité [2018_7300](#)). Il est recommandé de ne mettre en œuvre cette option qu'en cas de stricte nécessité.

23 Contrôle d'accès à la politique VPN

Tout accès à la politique de sécurité VPN (lecture, modification, application, importation, exportation) peut être 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, il est recommandé de mettre en œuvre cette protection. Dans la version TheGreenBow VPN Certified, cette protection est du reste systématiquement activée : dans cette version, lorsque le mot de passe n'est pas configuré par l'administrateur, il a pour valeur par défaut "admin".

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 conditionnées 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.pdf).

24 Options

24.1 Contrôle d'accès

Voir le chapitre "[Contrôle d'accès à la politique de sécurité VPN](#)".

24.2 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)

Affichage | Général | Gestion des logs | Options PKI | Langue

Bloquer l'accès à l'interface

Entrez un mot de passe pour bloquer l'accès à l'interface principale. Cette fonction permet aussi de bloquer le Client VPN en mode "Panneau des connexions".

Mot de passe :

Confirmer

Visualiser en menu de barre des tâches

Console

Panneau des Connexions

Panneau de Configuration

Quitter

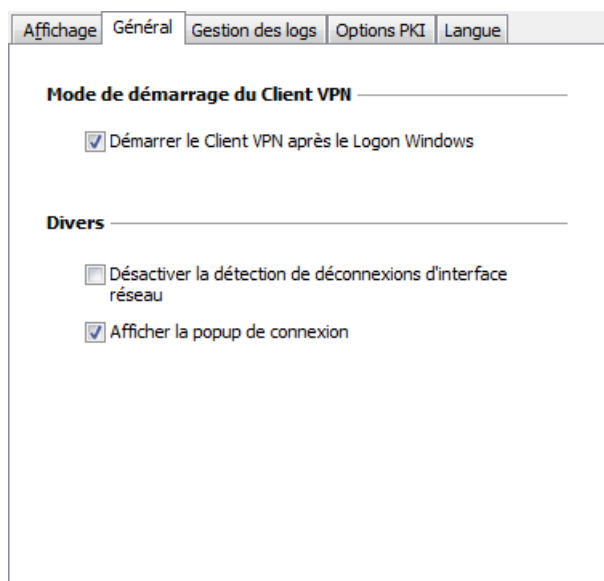
Popup de barre des tâches

Ne pas afficher la 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)

24.3 Général



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](#)".

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.

Afficher la popup de connexion

Une fenêtre de connexion est automatiquement affichée à chaque connexion VPN établie.

Il est possible ici de désactiver l'affichage de cette fenêtre en décochant la case "Afficher la popup de connexion".

24.4 Gestion des logs

Cf. chapitre 25.1 "[Logs administrateur](#)".

24.5 Options PKI

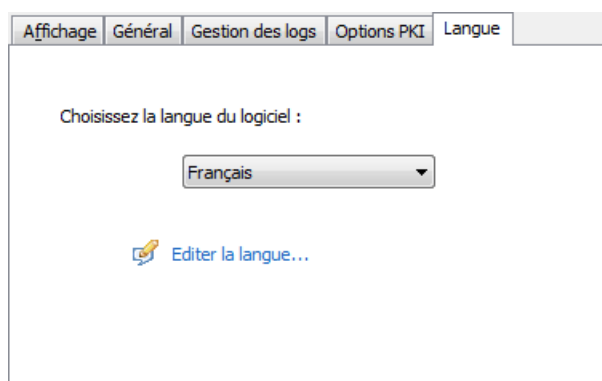
Cf. chapitre 18.4 "[Options PKI : Caractériser le certificat et son support](#)".

24.6 Gestion des langues

24.6.1 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.

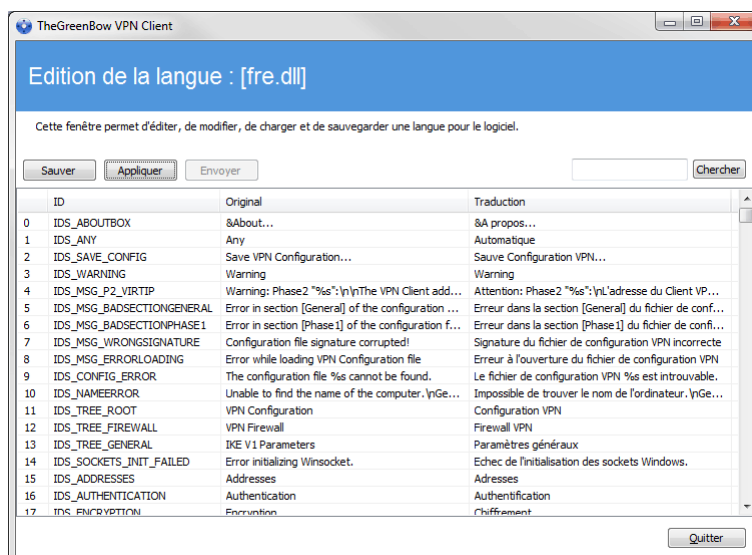
Pour choisir une autre langue, ouvrir le menu " Outils > Options " et sélectionner l'onglet "Langue". Choisir la langue souhaitée dans la liste déroulante proposée :



La liste des langues disponibles en standard dans le logiciel est donnée en annexe au chapitre "[Liste des langues disponibles](#)".

24.6.2 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.

25 Logs administrateur, console et traces

Le Client VPN TheGreenBow propose 3 types de logs :

- 1/ les logs "administrateur" sont spécifiquement dédiés au rapport d'activité et d'utilisation du logiciel.
- 2/ la "Console" détaille les informations et les étapes des ouvertures et fermeture des tunnels. Elle est principalement constituée des messages IKE et apporte une information de haut niveau sur l'établissement du tunnel VPN. Elle est destinée à l'administrateur, pour l'aider à identifier d'éventuels incidents de connexions VPN.
- 3/ le mode "traçant" fait produire par chaque composant du logiciel le log de son fonctionnement interne. Ce mode est destiné au support TheGreenBow pour le diagnostic d'incident logiciels.

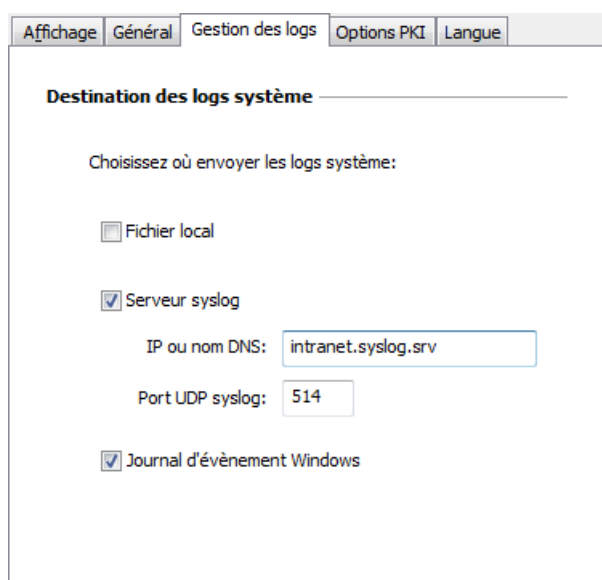
25.1 Logs administrateur

Le Client VPN TheGreenBow permet de collecter des logs de type "administrateur" : ouverture de tunnel, certificat expiré, durée de connexion, login/mot de passe erroné, modification de la configuration VPN, import ou export de cette configuration, etc. Les logs "administrateur" offrent en particulier un premier niveau d'analyse sur les problèmes rencontrés.

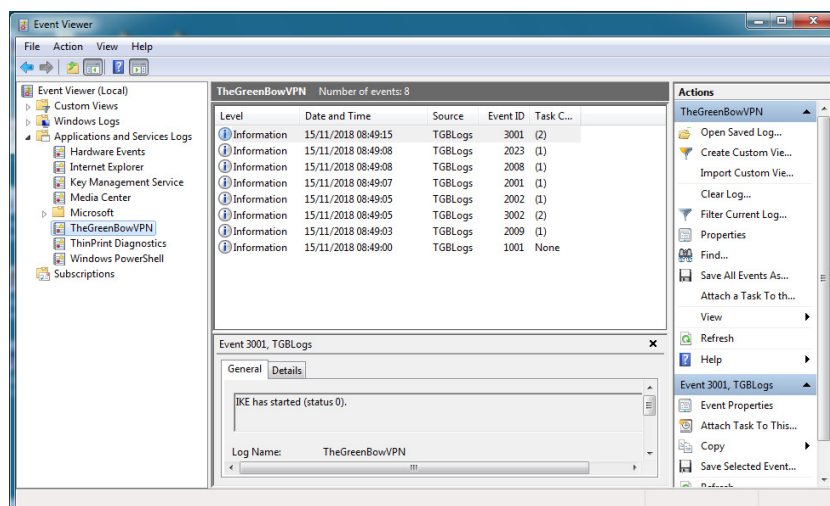
Les logs collectés peuvent être au choix et/ou simultanément :

- stockés dans un fichier local
- journalisés dans le journal d'événements Windows
- envoyés au format syslog à un serveur Syslog

Le paramétrage des log administrateur s'effectue dans la fenêtre "Outils > Options...", dans l'onglet "Gestion des logs".



Note : Le chemin d'accès aux logs du Client VPN TheGreenBow dans le gestionnaire d'événements Windows (Event Viewer) est le suivant :



Note : Les logs administrateur sont listés en annexe [28.3 Logs administrateur](#)

Note : le flux syslog peut être envoyé dans le tunnel VPN ou pas, suivant la configuration du Client VPN.

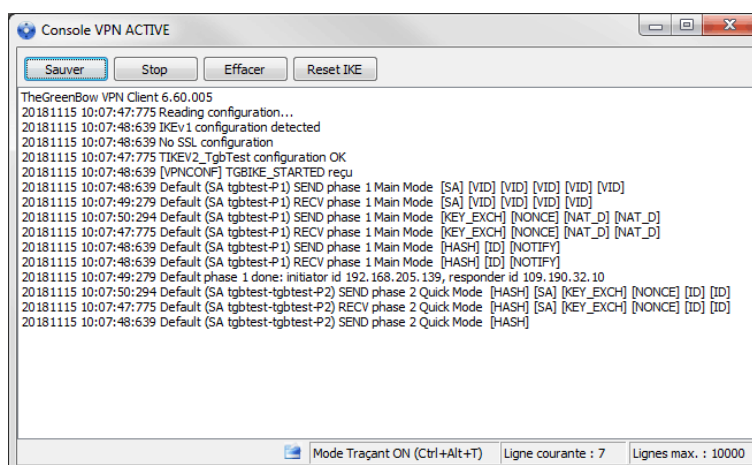
Note : Les fonctions de journalisation dans le journal d'événement Windows ou d'envoi de logs à un serveur syslog ne sont disponibles que dans la version Premium ou Certified.

Note : Lorsque les logs administrateur sont stockés dans un fichier local, le chemin de ces logs est le sous-répertoire "System" du répertoire des logs Debug : "C:\ProgramData\TheGreenBow\TheGreenBow VPN\LogFiles\System". Ce répertoire peut être lu dans tous les modes, mais n'est accessible en écriture qu'en mode Administrateur.

25.2 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 :

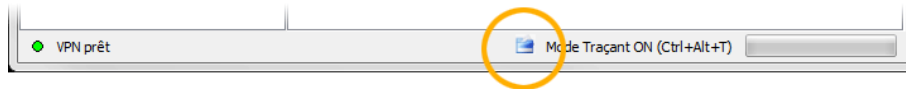
- Sauver : Sauvegarde dans un fichier la totalité des traces affichées dans la fenêtre
- Start / Stop : Démarre / arrête la capture des traces
- Effacer : Efface le contenu de la fenêtre
- Reset IKE : Redémarre le service IKE

25.3 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).



25.4 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.

Les logs traçants sont conservés 10 jours. Au delà de cette période, le logiciel purge automatiquement les fichiers.

A noter : Les logs "administrateur" lorsqu'ils sont mémorisés dans un fichier local ne sont pas purgés.

26 Recommandations de sécurité

26.1 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.

26.2 Recommandations

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

26.2.1 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.

26.2.2 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](#)

26.2.3 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](#)"

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).

26.2.4 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, certificats, token et cartes à puce" (tgbvpn_ug_pki_smartcard_fr).



Dans cette configuration, pour éviter toute exploitation de la vulnérabilité [2018 7293](#), il est impératif 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 13.4.6 "Child SA : Child SA" et 13.4.7 "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) |

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](#).

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 | عربي | Arabe | AR |
| 1081 | हिन्दी | Hindi | HI |
| 1030 | Danske | Danois | DK |
| 1029 | Český | Tchèque | CZ |
| 1038 | Magyar nyelv | Hongrois | HU |
| 1044 | Bokmål | Norvégien | NO |
| 1065 | فارسی | Persan | FA |
| 1042 | 한국어 | Coréen | KO |

28.3 Logs administrateur

| ID Log define | ID Log value | Severity | Log string |
|---------------------------|--------------|--------------|---|
| LOGID_STARTERINIT | 1001 | Notice | Starter service is started. |
| LOGID_VPNCONFSTARTING | 2001 | Notice | GUI is starting. |
| LOGID_VPNCONFSTOPPED | 2002 | Notice | GUI has closed. |
| LOGID_PWDSET | 2004 | Info | Admin password has been changed. |
| LOGID_PWDCHECK | 2005 | Error/Info | Admin password has been verified (status %d). |
| LOGID_PWDRESET | 2006 | Warning | Admin password has been reset. |
| LOGID_TGBIKESTARTED | 3001 | Notice | IKE has started (status %d). |
| LOGID_TGBIKESTOPPED | 3002 | Notice | IKE has stopped. |
| LOGID_TUNNELOPEN | 3004 | Info | Tunnel %s is asked to open. |
| LOGID_VPNCONFCRASHED | 2003 | Notice | GUI crashed (state %d). |
| LOGID_TGBIKECRASHED | 3003 | Notice | IKE crashed (state %d). |
| LOGID_STARTERSTOP | 1002 | Notice | Starter service is stopped. |
| LOGID_RESETIKE | 2007 | Warning | IKE is asked to reset. |
| LOGID_VPNCONFSTARTED | 2008 | Notice | GUI has started from user %s. |
| LOGID_VPNCONFSTOPPING | 2009 | Notice | GUI is stopping from user %s. |
| LOGID_VPNCONFLOADERROR | 2010 | Error | Configuration couldn't load (reason: %s). |
| LOGID_VPNCONFOPEN TUNNEL | 2011 | Info | GUI opens tunnel (source: %s). |
| LOGID_VPNCONF CLOSETUNNEL | 2012 | Info | GUI closes tunnel (source: %s). |
| LOGID_VPNCONFSAVE | 2013 | Notice | New configuration is saved. |
| LOGID_VPNCONFIMPORT | 2014 | Info | %s has been imported. |
| LOGID_VPNCONFIMPORTERR | 2015 | Error | %s could not be imported (status %d). |
| LOGID_VPNCONFEXPORT | 2016 | Info | %s has been exported. |
| LOGID_TOKENINSERT | 2017 | Info | Token %s has been inserted. |
| LOGID_TOKENEXTRACT | 2018 | Info | Token %s has been extracted. |
| LOGID_USBINSERT | 2019 | Info | USB Key has been inserted |
| LOGID_USBEXTRACT | 2020 | Info | USB Key has been extracted |
| LOGID_INSTALLATION | 2021 | Info | VPN running for the 1st time. |
| LOGID_UPDATE | 2022 | Info | VPN software has been updated to version %s. |
| LOGID_VERSION | 2023 | Info | VPN Version is %s. |
| LOGID_GINASTARTED | 4001 | Notice | Gina has started. |
| LOGID_GINASTOPPING | 4002 | Notice | Gina is stopping. |
| LOGID_GINAOPEN TUNNEL | 4003 | Info | GINA opens tunnel (source: %s). |
| LOGID_GINACLOSETUNNEL | 4004 | Info | GINA closes tunnel (source: %s). |
| LOGID_TUNNELAUTH_OK | 3005 | Info | Tunnel authentication Ok (%s). |
| LOGID_TUNNELTRAFFIC_OK | 3006 | Info | Tunnel ??? Ok |
| LOGID_TUNNELAUTH_NOK | 3007 | Error | Tunnel authentication failed (reason %d). |
| LOGID_TUNNELTRAFFIC_NOK | 3008 | Error | Tunnel ??? Failed (reason %d). |
| LOGID_AUTHREKEYING | 3009 | Info | Tunnel %s initiated rekey (source %d). |
| LOGID_AUTHREKEYED | 3010 | Info | Tunnel %s rekeyed. |
| LOGID_TUNNELREKEYING | 3011 | Info | Tunnel %s initiated rekey (source %d). |
| LOGID_TUNNELREKEYED | 3012 | Info | Tunnel %s rekeyed. |
| LOGID_PINCODE | 3013 | Notice/Error | Pincode is entered (status %d). |
| LOGID_DRIVERNOK | 3014 | Critical | Driver could not be loaded (status %d). |
| LOGID_IKEEXT_STOP | 1003 | Warning | IKEEXT service is stopped. |
| LOGID_IKEEXT_RESTART | 1004 | Notice | IKEEXT service is restarted. |
| LOGID_IKEEXT_ERROR | 1005 | Critical | IKEEXT could not be stopped (status %d). |
| SYSTEMLOGID_VIRTIFOK | 3015 | Info | Virtual interface created successfully (instance %d). |
| SYSTEMLOGID_VIRTIFNOK | 3016 | Error | Virtual interface couldn't not be created (error %d). |
| LOGID_TUNNELCLOSED | 3017 | Notice | %s tunnel successfully closed (%d min). |
| LOGID_TUNNELCLOSED_ERR | 3018 | Error | %s tunnel closed unexpectedly (%d). |
| LOGID_CERTERROR | 3019 | Error | Error %d when handling certificate %s. |
| LOGID_TUNNELDATA_UL | 3020 | Info | %d bytes sent inside the tunnel. |
| LOGID_TUNNELDATA_DL | 3021 | Info | %d bytes received inside the tunnel. |

28.4 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 (simplifié), 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'installateur, 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 Log administrateur : fichier local, journal d'événements Windows, serveur syslog. |
| 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.) |

28.5 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