Client VPN macOS v2.4

Guide de l'administrateur

Dernière mise à jour : 9 février 2024
Référence du document : 20240209_AG_VPM_2.4_FR_1.0

Propriété de TheGreenBow © 2024

TheGreenBow est un nom commercial déposé.

Apple, le logo Apple, iPhone, iOS, Mac et macOS sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays et régions.

D'autres marques de commerce appartenant à des tiers et mentionnées dans ce document demeurent la propriété intellectuelle de ces tiers.

Tous les droits de reproduction sont réservés, y compris pour les représentations iconographiques ou photographiques. La reproduction de tout ou partie de ce document sur quelque support que ce soit est formellement interdite sauf notre autorisation expresse.

Toutes les informations fournies sont sujettes à modification à tout moment et sans préavis.

Malgré tous les soins apportés à la réalisation de ce document et à sa mise à jour régulière, des erreurs peuvent s'être glissées dans les informations présentées. Si vous en constatez n'hésitez pas à nous le faire savoir en nous contactant, nous procéderons aux rectifications correspondantes.

Table des matières

1 Introduction 1
1.1 Les Clients VPN TheGreenBow 1
1.2 Fonctionnalités du Client VPN macOS 2
1.3 Nouveautés de la version 2.4 2
1.3.1 Fonctionnalités 2
1.3.2 Cryptographie 3
1.3.3 SSL / OpenVPN 3
1.3.4 Authentification et révocation des certificats 3
1.4 Interface graphique 3
1.5 Limitations actuelles 4
2 Installation 5
2.1 Installation et mises à jour 5
2.1.1 Introduction 5
2.1.2 Prérequis pour l'installation 5
2.1.3 Procédure d'installation 7
2.1.4 Premier lancement de l'application 9
2.1.5 Installations précédentes d'un Client VPN depuis l'App Store 13
2.2 Période d'évaluation 13
2.3 Configuration de test 15
2.4 Désinstallation 17
3 Activation 21
3.1 Étape 1 21
3.2 Étape 2 22
3.3 Erreurs d'activation 22
3.4 Licence et logiciel activé 23
3.5 Affichage de la fenêtre d'activation 24
4 Interface utilisateur 25
4.1 Aperçu 25
4.2 Menus 26

4.3 Raccourcis claviers 27
4.4 Arborescence de la configuration VPN 27
4.4.1 Introduction 27
4.4.2 Menus contextuels 29
4.4.3 Raccourcis 31
4.4.4 Boutons de l'arborescence de la configuration VPN 31
5 Fenêtre « À propos... » 34
6 Import et export de configurations VPN 35
6.1 Importer une configuration VPN 35
6.2 Exporter une configuration VPN 35
7 Configuration d'un tunnel VPN 36
7.1 Modification et enregistrement d'une configuration VPN 36
7.2 Configuration d'un tunnel IPsec IKEv2 36
7.2.1 IKE Auth : Authentification 37
7.2.2 IKE Auth : Protocole 40
7.2.3 IKE Auth : Passerelle 43
7.2.4 IKE Auth : Certificat 45
7.2.5 Child SA : Child SA 45
7.2.6 Child SA : Avancé 49
7.2.7 Child SA : Plus de paramètres 50
7.3 Configuration d'un tunnel SSL / OpenVPN 51
7.3.1 SSL : Authentification 52
7.3.2 SSL : Sécurité 54
7.3.3 SSL : Passerelle 56
7.3.4 SSL : Établissement 58
7.3.5 SSL : Certificat 60
8 Passerelle redondante 61
9 Gestion des certificats 62
9.1 Introduction 62
9.2 Certificat utilisateur 62
9.3 Sélectionner un certificat (onglet Certificat) 63
9.4 Importer un certificat 64
9.4.1 Importer un certificat au format PEM/PFX 64
9.4.2 Importer un certificat au format PKCS#12 65

9.4.3 Contraintes relatives à l'extension Key Usage 66
9.4.4 Contraintes relatives à l'extension Extended Key Usage 67
9.5 Gestion des autorités de certification 68
9.5.1 Généralités 68
9.5.2 Importer une autorité de certification 68
9.5.3 Mode IPsec DR 70
10 Logs 71
10.1 Console 71
10.2 Mode traçant 72
10.3 Logs Système 72
11 Recommandations de sécurité 73
11.1 Hypothèses 73
11.1.1 Profil et responsabilités des administrateurs 73
11.1.2 Profil et responsabilités de l'utilisateur 73
11.1.3 Respect des règles de gestion des éléments cryptographiques 73
11.2 Poste de l'utilisateur 74
11.3 Configuration VPN 74
11.3.1 Données sensibles dans la configuration VPN 74
11.3.2 Authentification de l'utilisateur 74
11.3.3 Authentification de la passerelle VPN 75
11.3.4 Protocole 75
11.3.5 Recommandations de l'ANSSI 75
12 Contact 76
12.1 Information 76
12.2 Commercial 76
12.3 Support 76
13 Annexes 77
13.1 Notions élémentaires de cryptographie 77
13.1.1 Algorithmes SHA, RSA et ECDSA 77
13.1.2 Format des certificats 78
13.1.3 Méthodes d'authentification des certificats 80
13.2 Caractéristiques techniques du Client VPN macOS 81
13.2.1 Principales fonctions 81
13.2.2 Langues 81

13.2.3 OS compatibles 81
13.2.4 Cryptographie et authentification 82

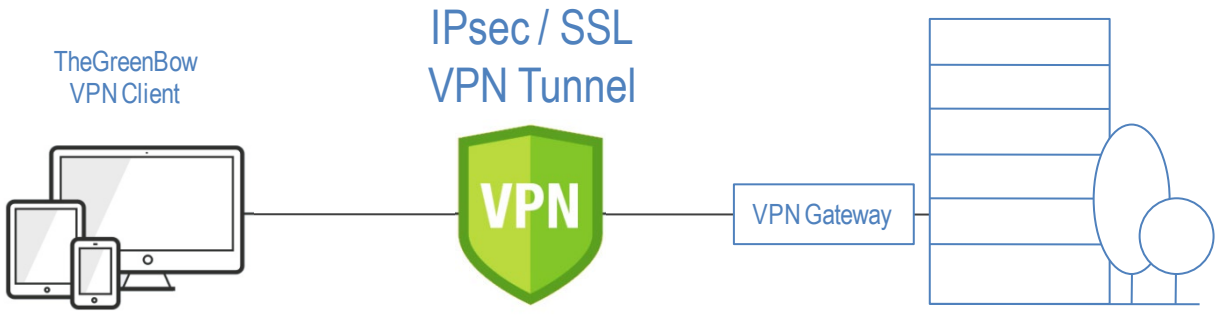
Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2024-02-09	Toutes	Version initiale	FB, FH, BB

1 Introduction

1.1 Les Clients VPN TheGreenBow

Les logiciels Client VPN TheGreenBow sont conçus pour sécuriser les connexions au système d'information dans toutes les situations. Quel que soit le réseau utilisé, quel que soit le système d'authentification adopté, quel que soit l'équipement à sécuriser, quelle que soit la passerelle VPN utilisée, les Clients VPN TheGreenBow sont particulièrement faciles à déployer, à configurer et à utiliser.



Disponibles sur toutes les plateformes

Certifiés sur Windows et Linux, les Clients VPN TheGreenBow sont également disponibles sur macOS, iOS et Android.

Ils peuvent être téléchargés depuis le site www.thegreenbow.com et utilisés gratuitement pendant une période d'essai de 30 jours.

Compatibles avec toutes les passerelles

Compatibles avec toutes les passerelles VPN, leur ergonomie inégalée et leur capacité d'intégration rapide en font des solutions de confiance uniques sur le marché. Une liste de guides de configuration VPN pour les passerelles et les Clients VPN TheGreenBow est disponible ici : www.thegreenbow.com/vpn_gateway.html.

Fonctionnent sur tous types de réseaux

Quel que soit le contexte d'utilisation, le réseau ou l'équipement utilisé, les Clients VPN TheGreenBow assurent une connexion VPN fiable et robuste, sur 4G, 5G, Wi-Fi, réseaux filaires, satellites, etc.

1.2 Fonctionnalités du Client VPN macOS

Le Client VPN macOS dispose des fonctionnalités suivantes :

- Compatible avec la majorité des passerelles IPsec et SSL
- Protocoles : SSL, IPsec IKEv2
- Authentification : PSK, EAP, certificats X.509
- Authentification multiple (certificat + EAP)
- Gestion des certificats X.509 : PKCS#12, PFX, PEM
- Fragmentation IP
- Support du NAT-T
- Mode CP (Configuration Payload)
- Chiffrement : AES CBC, CTR et GCM 128 / 192 / 256 bits
- Hash : SHA2-256, SHA2-384, SHA2-512
- Groupes DH : 14-21 & 28
- DPD (Dead Peer Detection) : détection de trafic interrompu avec la passerelle
- Passerelle redondante
- Fragmentation IKEv2
- Local ID, Remote ID
- Suffixes DNS
- Serveurs DNS alternatifs
- Gestion sécurisée des configurations VPN (chiffrage et intégrité)
- Interface de configuration complète et intuitive
- Affichage des logs en temps réel
- Prise en charge des autorités de certification (CA : Certificate Authorities) et vérification du certificat de la passerelle
- Prise en charge de 25 langues (voir liste complète à la section 13.2.2 Langues)

1.3 Nouveautés de la version 2.4

1.3.1 Fonctionnalités

- Prise en charge des RFC 4304 Extended Sequence Number (ESN) et RFC 6023 (Childless IKE Initiation) pour une sécurité accrue
- Ajout de la case à cocher **Popup quand le tunnel s'ouvre** pour les tunnels SSL
- Ajout de la case à cocher **Childless** sur l'onglet **IKE Auth** > **Protocole**
- Ajout de la liste déroulante **Extended Sequence Number** sur l'onglet **Child SA** > **Child SA**

1.3.2 Cryptographie

- Prise en charge du groupe de clé Diffie-Hellman DH 28 (BrainpoolP256r1) [RFC 5639]

1.3.3 SSL / OpenVPN

- Mise à jour d'OpenSSL à la version 1.1.1s pour une sécurité renforcée
- Fin de la prise en charge des algorithmes vulnérables en SSL/OpenVPN : MD5, SHA-1, BF-CBC, TLS 1.1, suite de sécurité « LOW » pour TLS V1.2

1.3.4 Authentification et révocation des certificats

En raison des exigences de sécurité renforcées, de la dépréciation de certains algorithmes et d'une utilisation plus rigoureuse des certificats, la version 2.4 du Client VPN macOS comprend des restrictions sur les certificats.

- Prise en charge des méthodes d'authentification des certificats suivantes :
  - Méthode 1 : RSA Digital Signature avec SHA-2 [RFC 7296]
  - Méthode 9 : ECDSA sur courbe secp256r1 avec SHA-2 (256 bits) [RFC 4754]
  - Méthode 10 : ECDSA sur courbe secp384r1 avec SHA-2 (384 bits) [RFC 4754]
  - Méthode 11 : ECDSA sur courbe secp521r1 avec SHA-2 (512 bits) [RFC 4754]
  - Méthode 14 : Digital Signature Authentication RSASSA PSS avec SHA-2 (256/384/512 bits) [RFC 7427]
  - Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) (uniquement disponible avec des passerelles prenant en charge cette méthode)
- La méthode d'authentification des certificats 14 basée sur l'algorithme de signature RSASSA-PSS est utilisée par défaut pour tous les certificats RSA
- Fin de prise en charge de la Méthode 1 : RSA Digital Signature avec SHA-1 [RFC 7296]
- Refus des certificats RSA de taille inférieure à 2048 bits
- Refus des certificats ECDSA de taille inférieure à 256 bits
- Vérification des Key Usage et Extended Key Usage des certificats

1.4 Interface graphique

- Mise en conformité de l'interface avec la nouvelle charte graphique

1.5 Limitations actuelles

La version actuelle du Client VPN macOS présente les limitations suivantes :

- Le protocole IPv6 n'est pas pris en charge
- L'écran d'activation ne s'affiche pas à chaque démarrage (voir la section 3.5 Affichage de la fenêtre d'activation pour une solution de contournement)

2 Installation

2.1 Installation et mises à jour

2.1.1 Introduction

Le Client VPN macOS est dorénavant disponible comme une image disque Apple « notarisée », au format DMG.

Les mises à jour s'effectuent de la même manière que les installations, sauf lors de la mise à jour d'une application installée depuis l'App Store du Mac (cf. section 2.1.5 Installations précédentes d'un Client VPN depuis l'App Store).

La configuration VPN est conservée lors d'une mise à jour.

Le Client VPN macOS peut être installé sur un Mac avec une puce Apple (M1 ou supérieure). Dans ce cas, si vous ne l'avez pas déjà fait, vous devez installer Rosetta 2 afin de pouvoir exécuter le logiciel conçu pour un processeur Intel. Pour plus d'informations sur Rosetta 2, consultez le site web d'Apple : https://support.apple.com/fr-fr/HT211861.

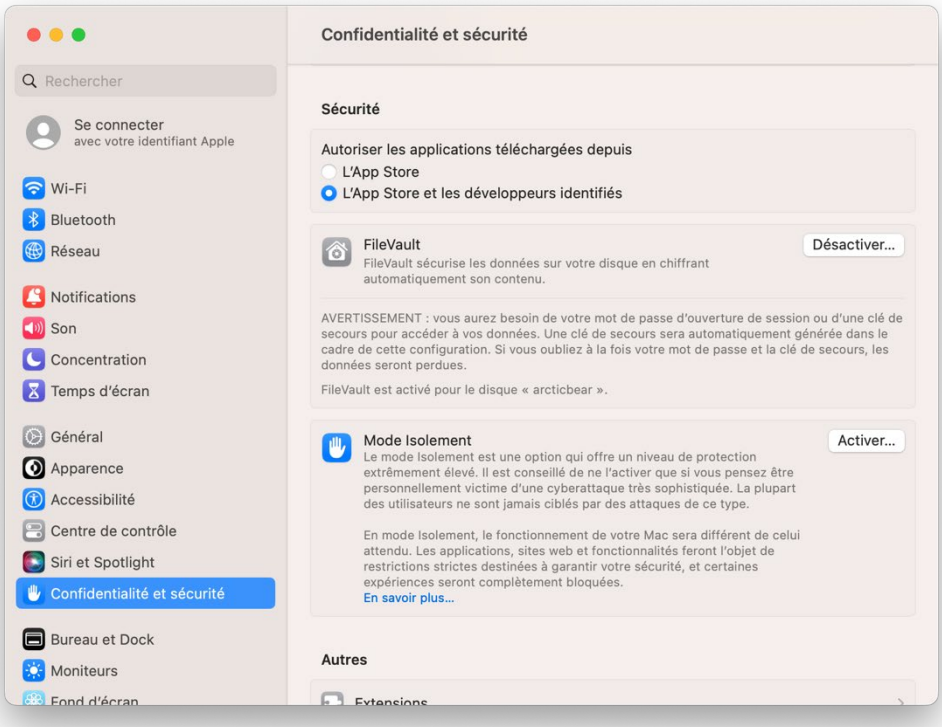
2.1.2 Prérequis pour l'installation

Le Client VPN macOS a été conçu pour les versions macOS 11 (Big Sur) et supérieures du système d'exploitation d'Apple. Il reste néanmoins compatible avec macOS 10.15 (Catalina).

Assurez-vous que l'installation d'applications tierces téléchargées depuis internet est autorisée. Pour cela, procédez de la manière suivante :

Sous macOS 13 (Ventura) et supérieur

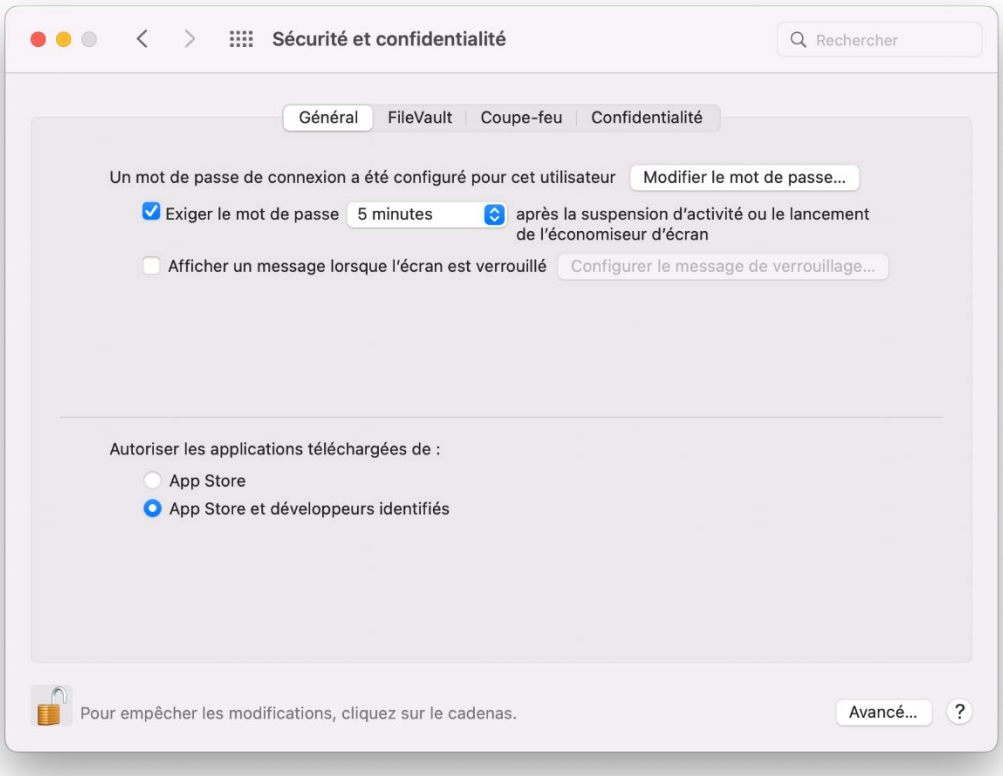
1. Ouvrez les **Réglages Système…** > **Confidentialité et sécurité**, puis faites défiler jusqu'à la section **Sécurité**.
2. Sous **Autoriser les applications téléchargées depuis**, sélectionnez **L'App Store et les développeurs identifiés**.



L'installation d'applications provenant de développeurs identifiés et désormais autorisée. Vous pouvez procéder à l'installation de l'application.

Sous macOS 12 (Monterey) et inférieur

1. Ouvrez les **Préférences Système...** > **Sécurité et confidentialité** > **Général**.
2. Sous **Autoriser les applications téléchargées de :**, sélectionnez **App Store et développeurs identifiés**.

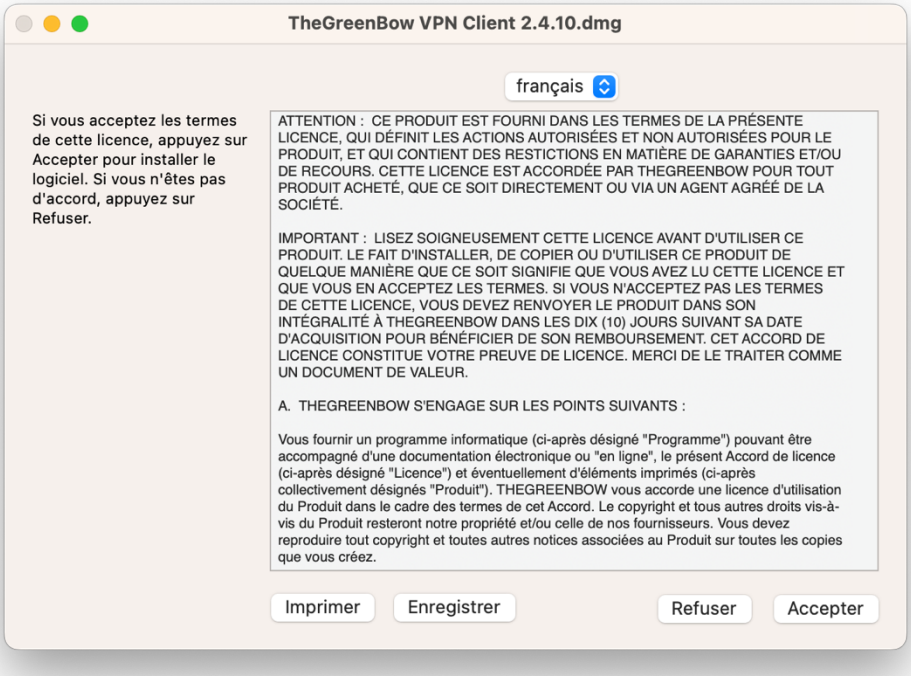


L'installation d'applications provenant de développeurs identifiés et désormais autorisée. Vous pouvez procéder à l'installation de l'application.

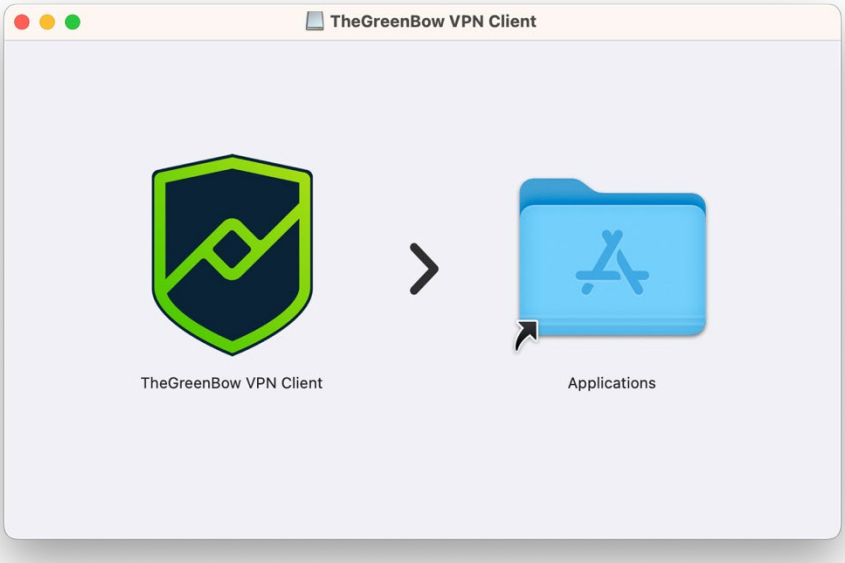
2.1.3 Procédure d'installation

Pour installer l'application, téléchargez le fichier DMG depuis le site internet thegreenbow.com, ou copiez-le sur le poste Mac sur lequel il doit être installé, puis double-cliquez dessus.

Les termes de la licence utilisateur vont s'afficher, et vous devrez les accepter pour utiliser le logiciel.



Une fois acceptée en cliquant sur le bouton **Accepter**, l'image disque sera « montée » et l'écran suivant s'affichera :

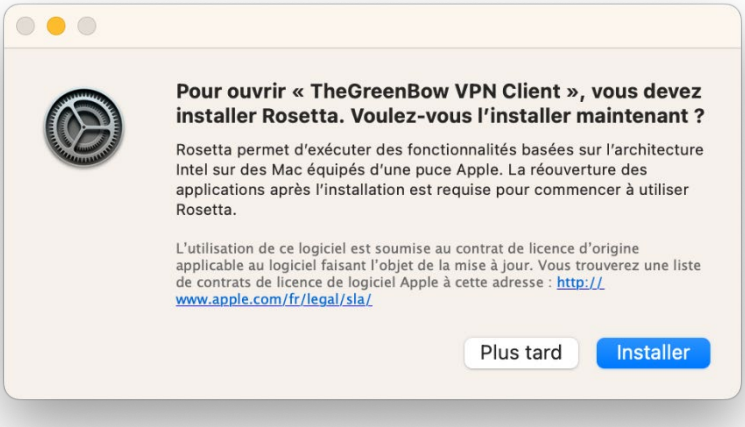


Pour installer l'application, glissez l'icône **TheGreenBow VPN Client** vers l'icône du dossier **Applications**. Ceci copiera l'application dans le dossier **Applications** de votre poste.

Le fichier DMG peut maintenant être « démonté », en le glissant vers la **Corbeille**, car il n'est désormais plus utile.

2.1.4 Premier lancement de l'application

Lorsque l'application est lancée pour la première fois sur un Mac équipé d'une puce Apple (M1 ou supérieure) et si vous n'avez pas encore installé Rosetta 2, une boîte de dialogue s'affiche pour vous demander si vous souhaitez l'installer maintenant :



Cliquez sur **Installer**. L'installation se déroule automatiquement et ne dure généralement pas plus de quelques secondes.

Pour plus d'informations sur Rosetta 2, consultez le site web d'Apple : https://support.apple.com/fr-fr/HT211861.

Lors du premier lancement de l'application, une boîte de dialogue s'affiche pour vous demander de confirmer l'ouverture d'une application téléchargée depuis internet.

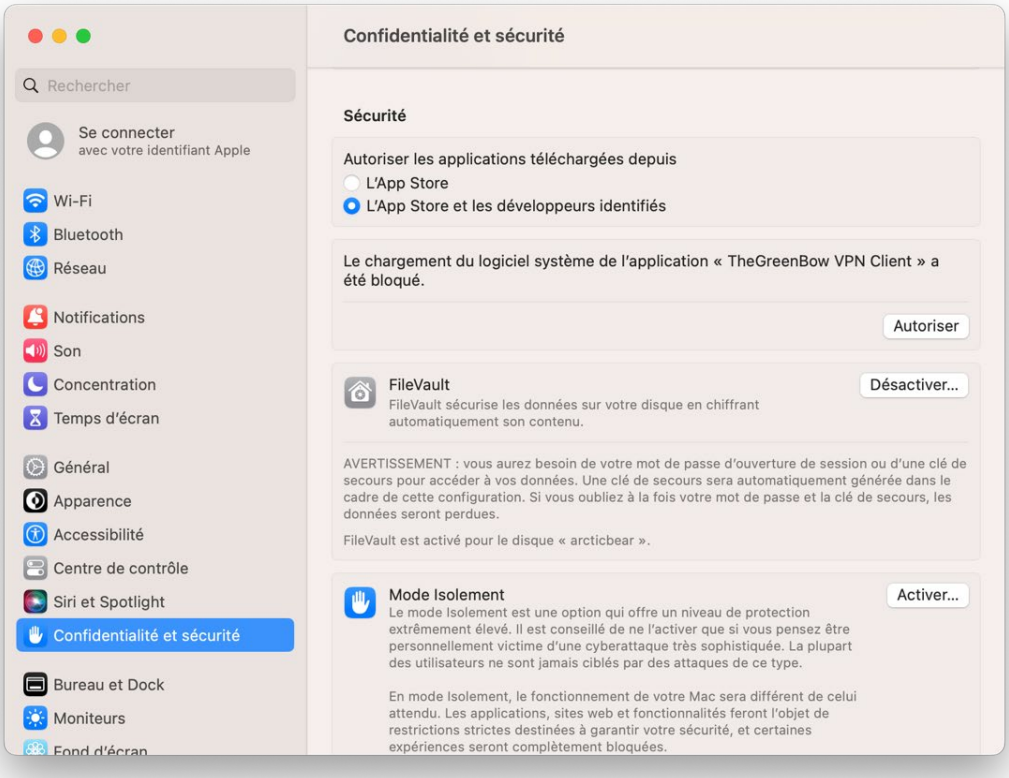
Cliquez sur **Ouvrir** pour confirmer l'ouverture de l'application.

Ensuite, une autre boîte de dialogue s'affiche pour demander la permission de débloquer une extension système. Cette extension système, développée par TheGreenBow, a la responsabilité de gérer les tunnels VPN et d'implémenter les protocoles VPN. Par conséquent, si l'extension système n'est pas débloquée, aucun tunnel VPN ne pourra être ouvert.

L'extension système peut être débloquée comme suit :

Sous macOS 13 (Ventura) et supérieur

1. Cliquez sur **Ouvrir Réglages Système**, ou cliquez sur **OK**, puis ouvrez les **Réglages Système...** > **Confidentialité et sécurité**, puis faites défiler jusqu'à la section **Sécurité**.
2. Sous l'option pour autoriser les applications téléchargées, un message devrait indiquer que **Le chargement du logiciel système de l'application « TheGreenBow VPN Client » a été bloqué**, suivi du bouton **Autoriser**.

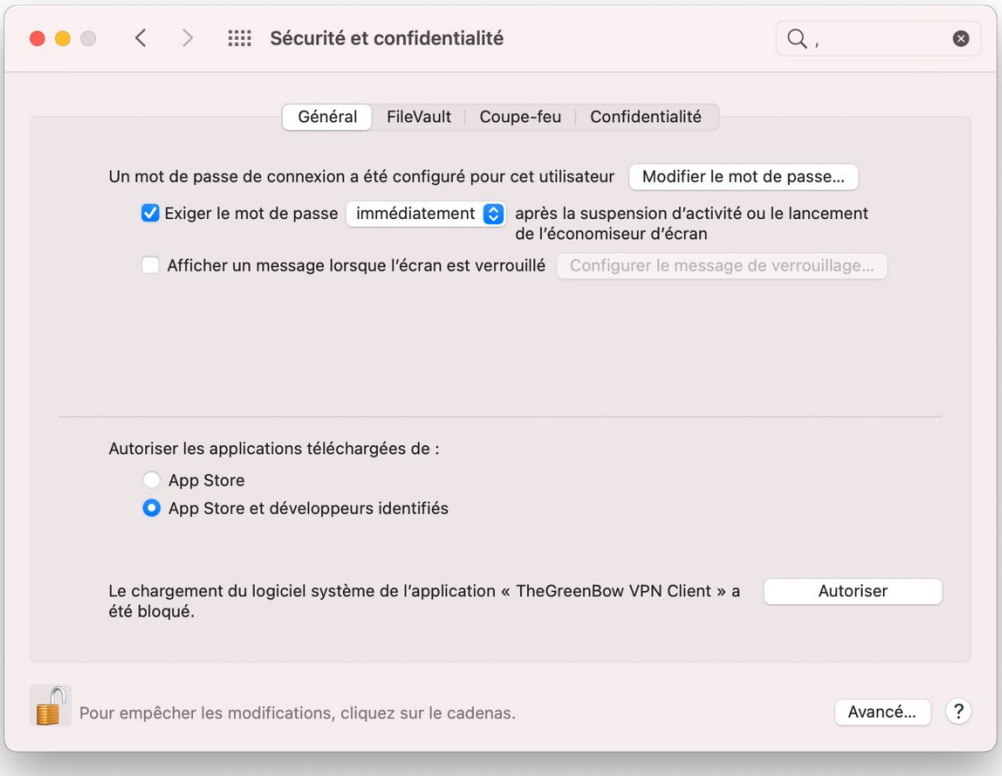


3. Cliquez sur le bouton **Autoriser**.
4. Un message s'affiche pour vous demander de confirmer la modification des **Réglages Système**. Identifiez-vous pour autoriser l'opération.

L'extension système est maintenant débloquée. Vous pouvez fermer les **Réglages Système**.

Sous macOS 12 (Monterey) et inférieur

1. Cliquez sur **Ouvrir les préférences de Sécurité**, ou cliquez sur **OK**, puis ouvrez **Préférences Système...** > **Sécurité et confidentialité** > **Général**.



2. Pour modifier les paramètres, vérifiez que le cadenas en bas à gauche de la fenêtre est ouvert. Si ce n'est pas le cas, cliquez dessus et entrez votre mot de passe.
3. En bas de la fenêtre, un message devrait indiquer que **Le chargement du logiciel système de l'application « TheGreenBow VPN Client » a été bloqué**, suivi du bouton **Autoriser**.
4. Cliquez sur le bouton **Autoriser**.

L'extension système est maintenant débloquée. Vous pouvez fermer les **Préférences Système**.

2.1.5 Installations précédentes d'un Client VPN depuis l'App Store

Dans le cas où une version précédente du Client VPN macOS a déjà été installée depuis l'App Store sur Mac, celle-ci doit être désinstallée avant l'installation de la nouvelle version.

Pour désinstaller une application provenant de l'App Store sur Mac, procédez de la manière suivante :

1. Lancez le **Launchpad**.
2. Positionnez le pointeur de la souris sur l'icône de l'application.
3. Cliquez en maintenant la pression jusqu'à ce que les icônes commencent à gigoter.
4. Cliquez sur la croix au-dessus de l'icône de l'application.
5. Confirmez en cliquant sur le bouton **Supprimer**.

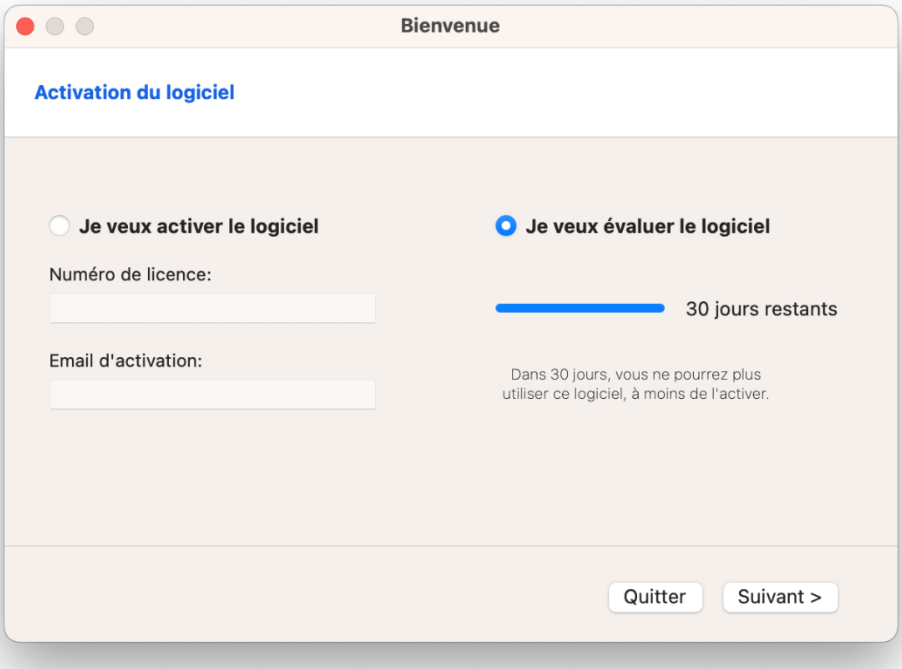
Il est également recommandé de supprimer à la main tous les tunnels qui ont été ajoutés par l'application dans les **Préférences/Réglages Système**.

Pour supprimer un tunnel ajouté dans les **Préférences/Réglages Système**, allez dans **Préférences/Réglages Système...** > **Réseau** et cherchez les tunnels qui ont comme **Application VPN** `TheGreenBow VPN Client`.

2.2 Période d'évaluation

Le Client VPN macOS peut être évalué gratuitement pendant 30 jours. Pendant cette période d'évaluation, le Client VPN est complètement opérationnel : toutes les fonctions sont disponibles.

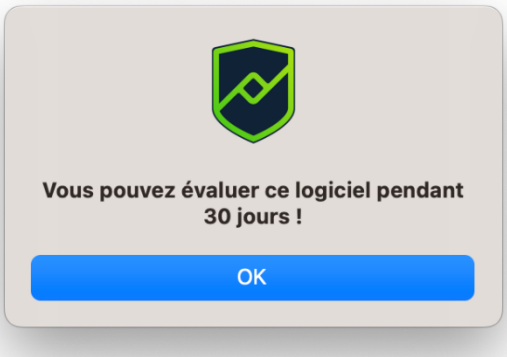
Une fenêtre d'activation s'affiche lors du premier lancement du logiciel. Elle vous permet d'activer ou d'évaluer le logiciel et indique le nombre de jours d'évaluation restants.



Pour évaluer le logiciel, sélectionnez **Je veux évaluer le logiciel**, puis cliquez sur **Suivant >** pour lancer le logiciel.

Vous pouvez retrouver le nombre de jours d'évaluation restants à tout moment dans la fenêtre **À propos...** (cf. section 5 Fenêtre « À propos... »).

Pendant la période d'évaluation, une fenêtre indiquant le nombre de jours d'évaluation restants s'affiche à chaque démarrage du logiciel.



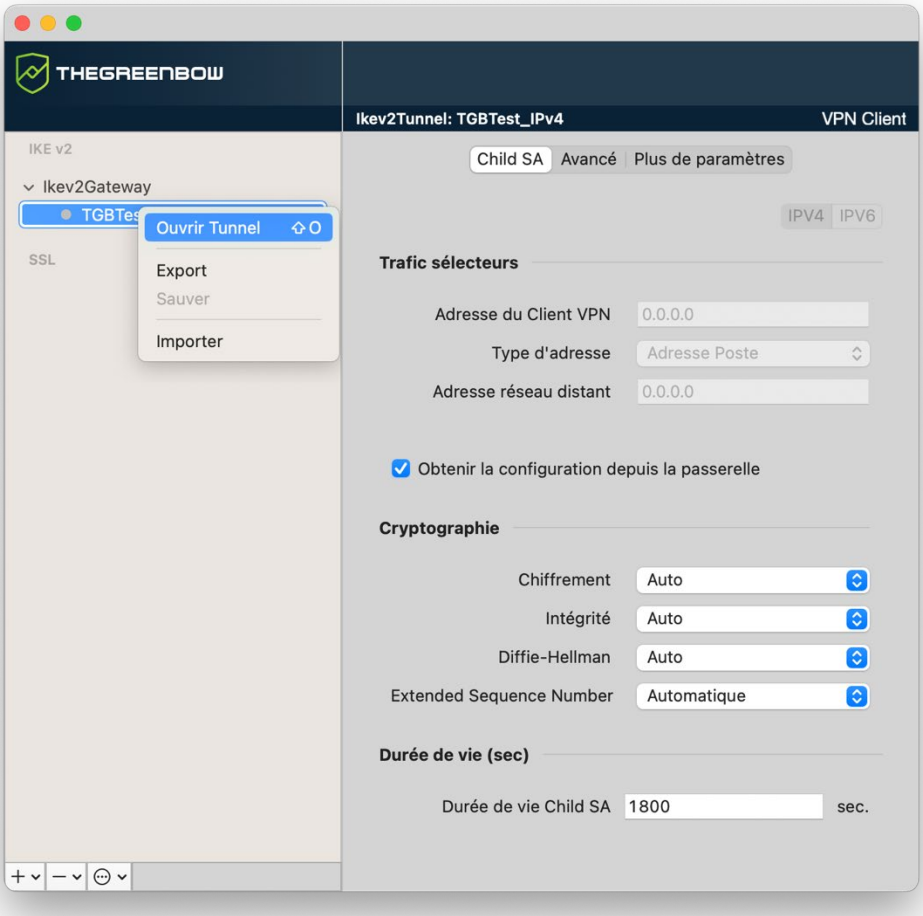
Lorsque la période d'évaluation a expiré, l'application doit être activée pour pouvoir continuer à l'utiliser.

⚠ Dans la version actuelle du logiciel, la fenêtre d'activation ne s'affiche que lors du premier lancement. Pour savoir comment l'afficher de nouveau, reportez-vous à la section 3.5 Affichage de la fenêtre d'activation.

☞ Pour savoir comment activer le logiciel, reportez-vous au chapitre 3 Activation.

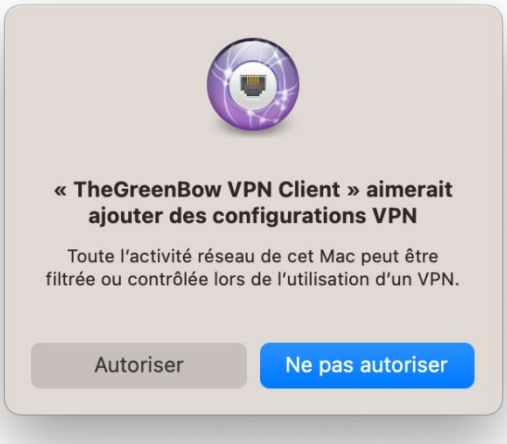
2.3 Configuration de test

Une fois l'application installée, une configuration VPN de test est automatiquement ajoutée à la liste des configurations VPN. Cette configuration de test peut être utilisée pour vérifier que le Client VPN macOS est opérationnel.



Pour ouvrir le tunnel `TGBTest_IPv4`, double cliquez sur le nom ou sélectionnez le tunnel, puis ouvrez le menu contextuel et sélectionnez **Ouvrir**

Tunnel ou utilisez le raccourci ⌘O. Une fenêtre s'affiche pour vous demander d'autoriser l'ajout de configurations VPN.



Cliquez sur **Autoriser**. Le tunnel devrait alors s'ouvrir.

Une fois le tunnel ouvert, vous devriez pouvoir envoyer une requête ping à l'adresse IP `192.168.175.50` ou visiter la page web http://192.168.175.50/

dans votre navigateur web. Dans ce cas, vous devriez voir le site web de test TheGreenBow s'afficher :

2.4 Désinstallation

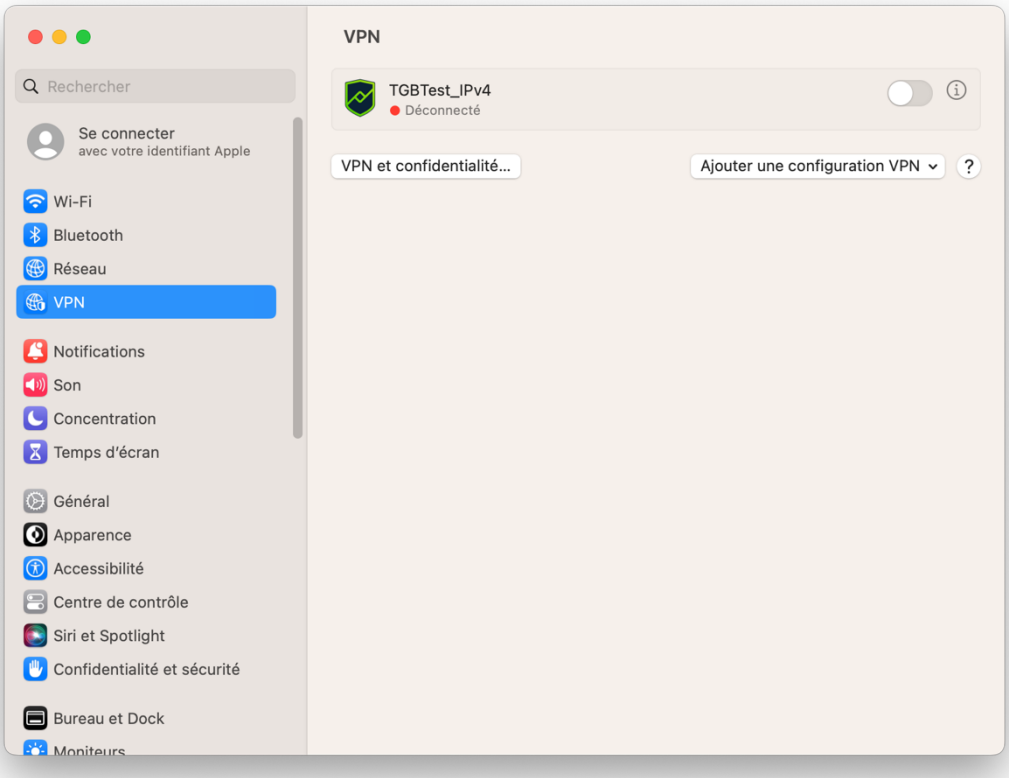
L'application peut être désinstallée en glissant son icône depuis le dossier des **Applications** vers la **Corbeille**.

Après la désinstallation, il est possible que des tunnels restent affichés dans la section **Réseau** des **Préférences/Réglages Système**. Ces tunnels sont identifiés par le nom `TheGreenBow VPN Client` comme **Application VPN**.

Pour les supprimer, procédez de la manière suivante :

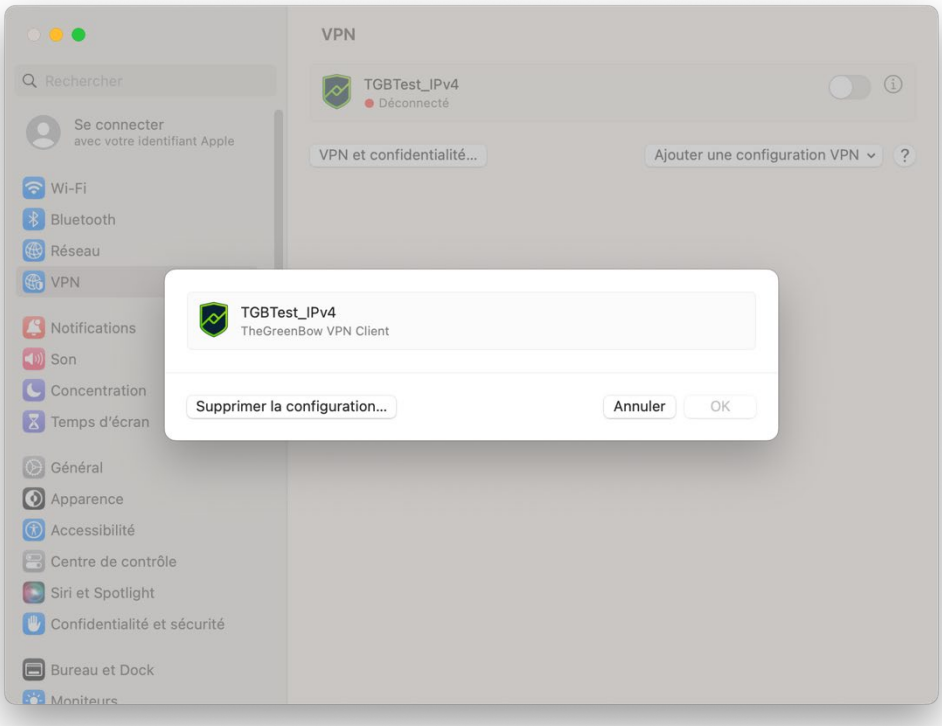
Sous macOS 13 (Ventura) et supérieur

1. Ouvrez les **Réglages Système...** > **VPN** (si des filtres réseau sont installés, le menu s'appelle **VPN et filtres)**.



2. Cliquez sur le bouton d'information ⓘ à droite du bouton bascule. La première fois que vous cliquez sur ce bouton, une fenêtre s'affiche vous demandant d'autoriser la modification de vos réglages système.

3. Saisissez votre mot de passe, puis cliquez sur **Modifier les réglages**. Une boîte de dialogue s'affiche.

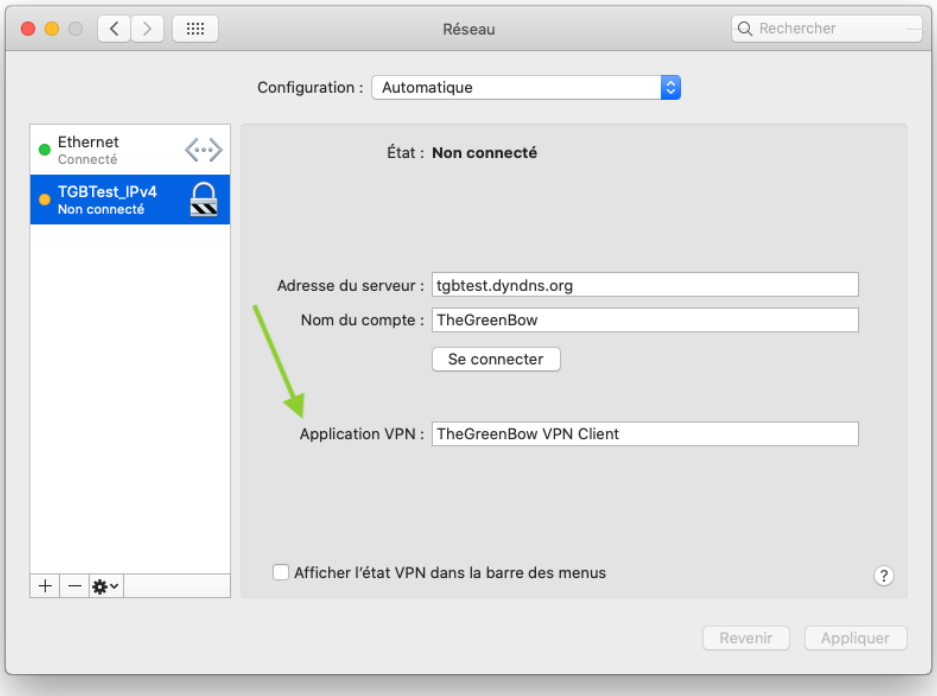


4. Cliquez sur **Supprimer la configuration...**

5. Répétez l'opération pour tous les tunnels que vous souhaitez supprimer des **Réglages Système**.

Sous macOS 12 (Monterey) et inférieur

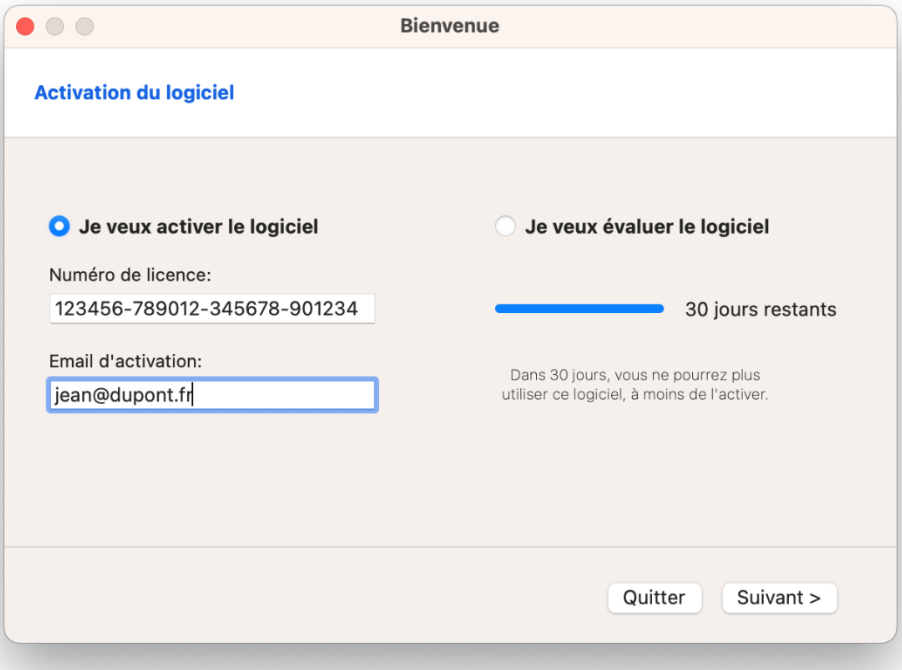
1. Ouvrez les **Préférences Système...** > **Réseau**.
2. Dans la colonne de gauche, sélectionnez le tunnel à supprimer.
3. Cliquez sur le bouton **moins**.
4. Cliquez ensuite sur **Appliquer** pour valider la suppression des tunnels.



3 Activation

L'activation du Client VPN macOS peut être effectuée au premier lancement du logiciel ou à tout moment pendant la période d'évaluation (cf. section 2.2 Période d'évaluation).

Si vous avez choisi d'évaluer le logiciel avant de l'activer, vous devez suivre la procédure décrite à la section 3.5 Affichage de la fenêtre d'activation pour accéder à la fenêtre d'activation.



Pour activer le logiciel, suivez les étapes décrites dans les sections ci-dessous.

3.1 Étape 1

Si vous n'avez pas encore de licence, accédez à la boutique en ligne TheGreenBow à l'adresse https://store.thegreenbow.com/. Sélectionnez macOS. Cliquez sur le bouton **Acheter**, puis suivez les instructions pour acheter une ou plusieurs licences.

Dans le champ **Numéro de licence**, entrez le numéro de licence reçu par e-mail. Le numéro de licence peut être copié-collé depuis l'e-mail de confirmation d'achat directement dans le champ.

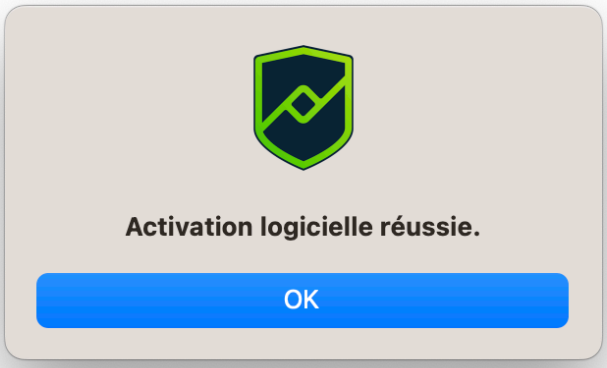
Le numéro de licence est uniquement composé de caractères [0..9] et [A..F], éventuellement regroupés par 6 et séparés par des tirets.

Dans le champ **Email d'activation**, entrez l'adresse e-mail permettant d'identifier votre activation. Cette information permet de retrouver, en cas de perte, les informations sur votre activation.

3.2 Étape 2

Cliquez sur **Suivant >**. Le processus d'activation en ligne s'exécute automatiquement.

Lorsque l'activation aboutit, cliquez sur **OK** pour lancer le logiciel.



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 Erreurs d'activation

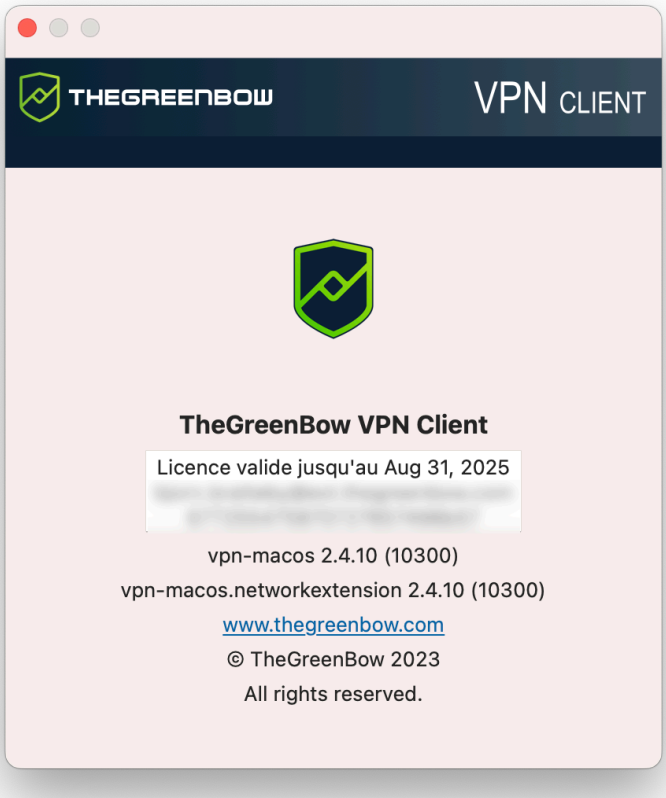
L'activation du logiciel peut ne pas aboutir pour différentes raisons. Chaque erreur est indiquée sur la fenêtre d'activation. Elle est accompagnée, le cas échéant, par un lien qui permet d'obtenir des informations complémentaires, ou qui propose une opération permettant de résoudre le problème.

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

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 logiciel du 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 ou pour un proxy. Le cas échéant, configurer le firewall pour laisser passer la communication, ou le proxy pour la rediriger correctement.

3.4 Licence et logiciel activé

Lorsque le logiciel est activé, la licence et l'adresse e-mail utilisées pour l'activation sont consultables dans la fenêtre **À propos...** du logiciel.



3.5 Affichage de la fenêtre d'activation

Dans la version actuelle du logiciel, la fenêtre d'activation ne s'affiche que lors du premier lancement. Si vous avez choisi d'évaluer le logiciel avant de l'activer, suivez la procédure décrite ci-dessous pour afficher la fenêtre d'activation lorsque la période d'évaluation a expiré ou dès que vous êtes prêt à activer le logiciel.

1. Si le logiciel est en cours d'exécution, quittez-le.
2. Dans le **Finder**, maintenez la touche Option enfoncée et sélectionnez l'option de menu **Aller** > **Bibliothèque**.
3. Naviguez jusqu'au dossier `Group Containers/HCZ5L8U556.group.com.thegreenbow.vpn/Library/Application Support/`.
4. Dans ce dossier, supprimez tous les fichiers avec l'extension `.dat` et `.json`.
5. Le cas échéant, répétez l'opération dans le dossier `Group Containers/HCZ5L8U556.group.com.thegreenbow.vpn/Library/Caches/`.

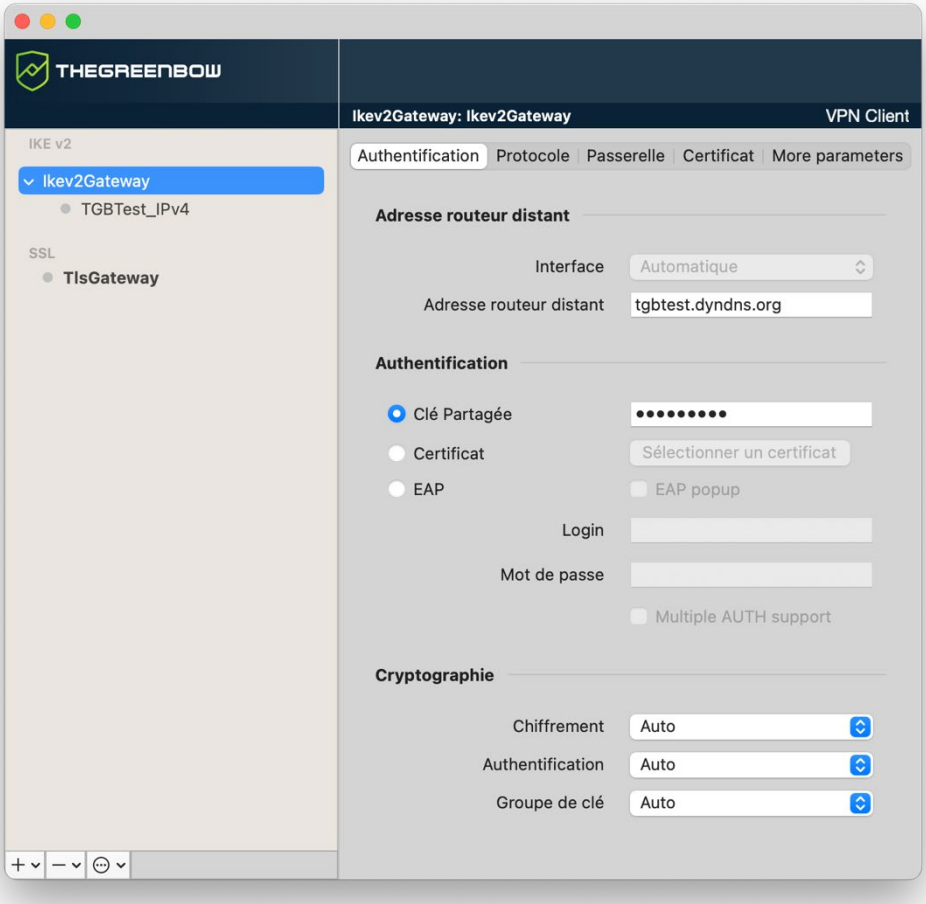
La fenêtre d'activation s'affichera de nouveau lors du prochain lancement du logiciel. Vous pouvez procéder à l'activation en suivant les étapes décrites à partir de la section 3.1 Étape 1 ci-dessus.

4 Interface utilisateur

4.1 Aperçu

Une fois le Client VPN démarré, le **Panneau de Configuration** et les menus sont visibles. Le **Panneau de Configuration** est composé des éléments suivants :

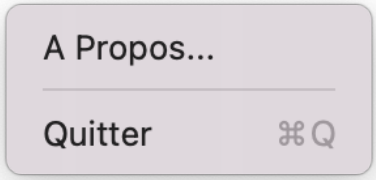
- l'arborescence de la configuration VPN qui se trouve sur le côté gauche du panneau,
- les onglets de configuration pour les tunnels VPN qui se trouvent sur le côté droit du panneau.



Le contenu de l'onglet de configuration changera en fonction de l'élément sélectionné dans l'arborescence de la configuration VPN.

4.2 Menus

TheGreenBow VPN Client



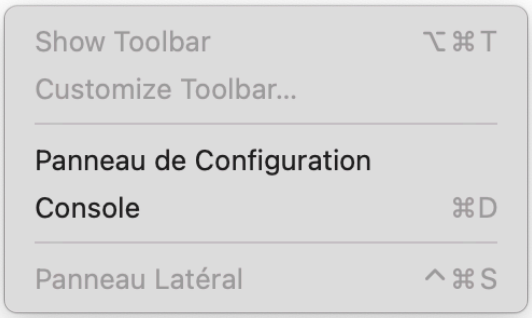
- **À propos...** : affiche le numéro de version du logiciel, le numéro de licence et sa durée de validité
- **Quitter** : ferme l'application.

Fermer l'application ne ferme pas le tunnel ouvert.

Configuration

- **Sauver** : enregistre les configurations
- **Nouveau** : crée une nouvelle configuration **IKE Auth**, **Child SA** ou **TLS**
- **Importer** : importe une configuration à partir d'un fichier `.tgb`
- **Exporter** : exporte la configuration sélectionnée
- **Exporter tout** : exporte toutes les configurations
- **Ouvrir/Fermer le tunnel** : ouvre ou ferme le tunnel sélectionné

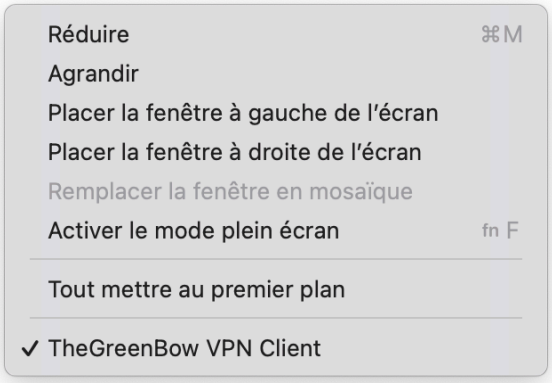
Affichage



- **Panneau de Configuration** : ouvre la fenêtre de configuration VPN
- **Console** : ouvre la **Console** macOS

Les options **Show Toolbar**, **Customize Toolbar...** et **Panneau Latéral** sont grisées, car elles ne sont pas disponibles dans cette version.

Fenêtre



- Contient les options habituelles du système relatives à la gestion des fenêtres de l'application.

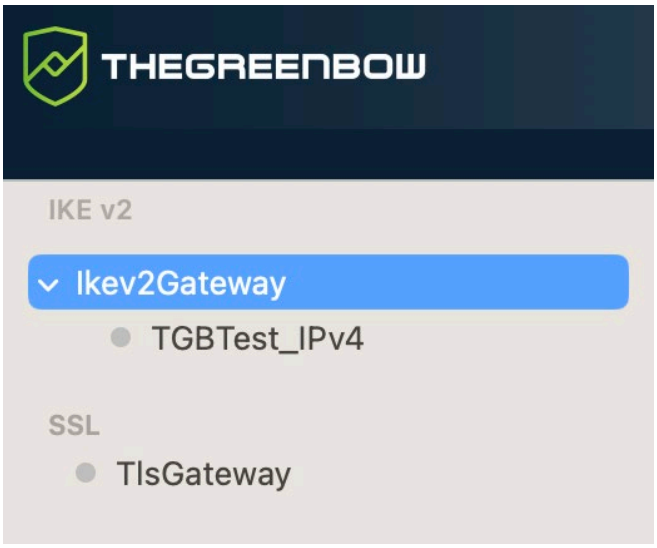
4.3 Raccourcis claviers

⌘S	Enregistre toutes les configurations VPN
⌘H	Importe une nouvelle configuration VPN
⌘Q	Quitte l'application
⌘D	Ouvre la **Console** de logs
⌘O	Ouvre le tunnel sélectionné
⌘W	Ferme le tunnel sélectionné

4.4 Arborescence de la configuration VPN

4.4.1 Introduction

Le côté gauche du **Panneau de Configuration** présente la configuration VPN sous la forme d'une arborescence. Celle-ci peut contenir un nombre illimité de tunnels VPN.



Sous la racine de la configuration VPN, deux niveaux permettent de créer respectivement :

- des tunnels IPsec IKEv2, caractérisés par une IKE Auth et une Child SA, chaque IKE Auth pouvant contenir plusieurs Child SA ;
- des tunnels SSL / TLS.

Un clic sur un élément IKE Auth, Child SA ou TLS dans l'arborescence de la configuration VPN ouvre dans la partie droite du **Panneau de Configuration** les onglets de configuration VPN associés. Voir dans les sections suivantes :

1. Tunnel IPsec IKEv2
    - IKEv2 (IKE Auth) : Authentification
    - IKEv2 (Child SA) : IPsec
2. Tunnel SSL (OpenVPN)
    - SSL : TLS

Une entrée au niveau racine vous permet de consulter, d'éditer ou de créer des configurations IPsec en utilisant IKEv2 avec plusieurs connexions IKE Auth[1] et Child SA[2]. Chaque IKE Auth peut contenir plusieurs Child SA.

L'icône à gauche du tunnel indique son statut :

⚪	Tunnel fermé. Double-cliquer pour l'ouvrir si aucun autre tunnel n'est monté.
🟢	Tunnel ouvert. Double-cliquer pour le fermer.
🔴	Tunnel en cours d'ouverture ou de fermeture.

Pour renommer un élément, sélectionnez-le, puis cliquez sur celui-ci ou appuyez sur la touche Entrée du clavier.

[1] Nom par défaut : `Ikev2Gateway`.
[2] Nom par défaut : `Ikev2Tunnel`.

Une configuration non enregistrée est indiquée par le passage en caractères gras du nom. Il repassera en caractères normaux après l'enregistrement.

La commande **Sauver** enregistre toutes les configurations, pas les configurations individuelles.

4.4.2 Menus contextuels

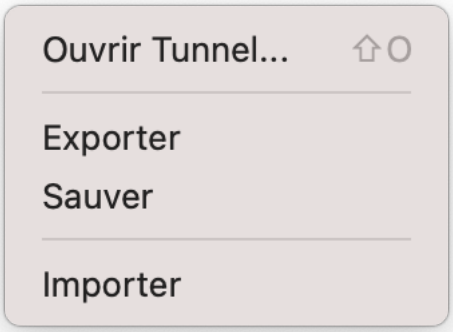
4.4.2.1 IKEv2 et SSL

Maintenez la touche Contrôle enfoncée pendant que vous cliquez sur l'élément IKEv2 ou SSL pour afficher le menu contextuel suivant :

Ouvrir / Fermer le tunnel	Ouvre le tunnel sélectionné / Ferme le tunnel ouvert (IKEv2 ou SSL).
Renommer	Cet élément de menu n'est pas actif.
Exporter	Exporte toutes les configurations IKEv2 / SSL.
Sauver	Enregistre toutes les modifications apportées aux configurations (IKEv2 et SSL).
Importer	Importe un fichier de configuration `.tgb`.

4.4.2.2 IKE Auth

Maintenez la touche Contrôle enfoncée pendant que vous cliquez sur un élément IKE Auth[1] pour ouvrir le menu contextuel suivant :

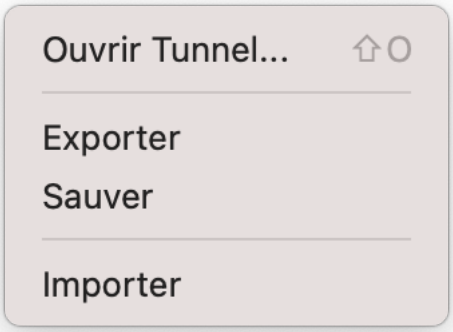


Ouvrir / Fermer Tunnel	Ouvre le tunnel sélectionné / Ferme le tunnel ouvert.
Exporter	Exporte le nœud IKE Auth et tous ses nœuds Child SA.
Sauver	Enregistre toutes les modifications effectuées.
Importer	Importe un fichier de configuration `.tgb`.

[1] Nom par défaut : `Ikev2Gateway`.

4.4.2.3 Child SA

Maintenez la touche Contrôle enfoncée pendant que vous cliquez sur un élément Child SA[1] pour afficher le menu contextuel suivant :



Ouvrir / Fermer Tunnel	Ouvre le tunnel sélectionné / Ferme le tunnel ouvert.
Exporter	Exporte le nœud IKE Auth et tous ses nœuds Child SA.
Sauver	Enregistre toutes les modifications effectuées.
Importer	Importe un fichier de configuration `.tgb`.

4.4.3 Raccourcis

Les raccourcis suivants sont disponibles :

⌘S	Enregistre toutes les configurations.
⌘W	Ferme le tunnel ouvert.
⌘⇧O	Ouvre le tunnel sélectionné.

4.4.4 Boutons de l'arborescence de la configuration VPN

Sous l'arborescence de la configuration VPN, on trouve les boutons suivants :

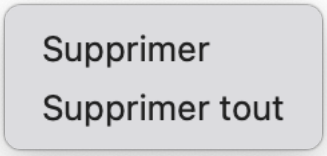
[1] Nom par défaut : `Ikev2Tunnel`.

Cliquez sur un des boutons pour ouvrir les menus contextuels correspondants. Le menu associé à chaque bouton est décrit dans les sous-sections suivantes.

4.4.4.1 Bouton +

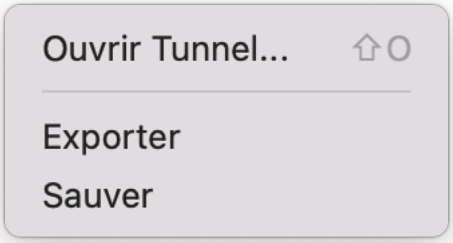
Nouvel IKE Auth	Crée un nouveau nœud IKE Auth.
Nouveau Child SA	Crée un nouveau nœud Child SA. Si un nœud IKE Auth était sélectionné dans l'arborescence de la configuration VPN, alors le nœud Child SA nouvellement créé sera un élément fils du nœud IKE Auth sélectionné. Autrement, une paire de nouveaux nœuds IKE Auth et Child SA seront créés simultanément.
Nouveau TLS	Crée un nouveau nœud SSL.
Importer	Importe un fichier de configuration `.tgb`.

4.4.4.2 Bouton —



Supprimer	Supprime le nœud sélectionné (et tous ses éléments fils) de l'arborescence de la configuration VPN
Supprimer tout	Supprime tous les nœuds de l'arborescence de la configuration VPN

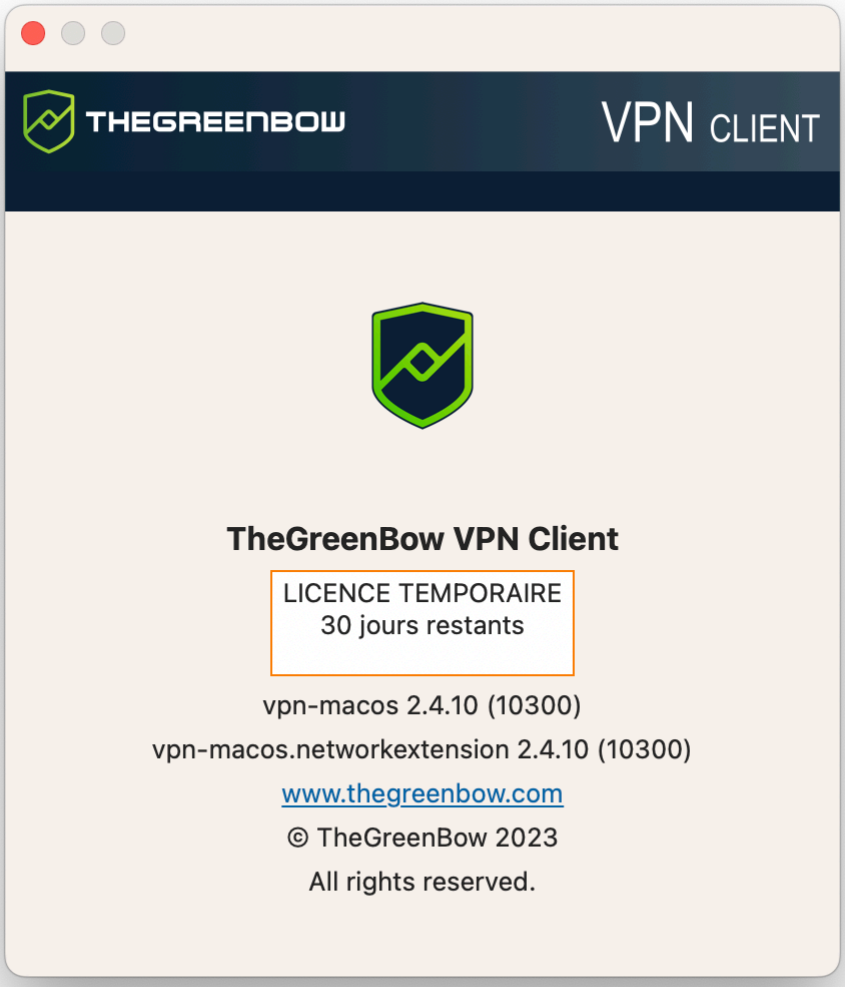
4.4.4.3 Bouton ⋯



Ouvrir / Fermer Tunnel...	Ouvre le tunnel sélectionné / Ferme le tunnel ouvert
Exporter	Exporte la configuration du nœud sélectionné ainsi que tous ses éléments fils. Si un nœud Child SA est sélectionné, alors le nœud IKE Auth correspondant est exporté également.
Sauver	Enregistre toutes les modifications effectués

5 Fenêtre « À propos… »

La fenêtre **À propos…** est accessible par l'option de menu **TheGreenBow VPN Client** > **À propos**.



La fenêtre **À propos…** donne les informations suivantes :

- le nom et la version du logiciel ;
- le nom et la version de l'extension réseau ;
- lien internet vers 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.

6 Import et export de configurations VPN

6.1 Importer une configuration VPN

Le Client VPN macOS vous permet d'importer une configuration VPN à l'aide de l'option de menu **Configuration** > **Import**.

Les fichiers de configuration VPN ont une extension `.tgb`.

Si la configuration VPN a été enregistrée avec un mot de passe, il sera demandé à l'utilisateur.

Aucune vérification n'est effectuée pour savoir si un tunnel portant le même nom existe déjà dans le Client VPN et si un nom est en double ça ne génère pas d'erreur.

6.2 Exporter une configuration VPN

Pour exporter un tunnel VPN de la liste, procédez de l'une des façons suivantes :

- Sélectionnez l'option de menu **Configuration** > **Export**.
- Maintenez la touche Contrôle enfoncée pendant que vous cliquez sur l'élément à exporter et choisissez l'option **Exporter** du menu contextuel.
- Utilisez le raccourci ⌘⌥H.

Pour exporter tous les tunnels, sélectionnez l'option **Exporter tout** du menu **Configuration**.

7 Configuration d'un tunnel VPN

7.1 Modification et enregistrement d'une configuration VPN

Il est possible de modifier la configuration VPN (par exemple la modification des paramètres d'un tunnel) et de tester cette modification « à la volée » sans avoir à l'enregistrer.

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

La configuration VPN peut être enregistrée à tout moment en utilisant :

- le raccourci clavier ⌘S,
- l'option de menu **Configuration** > **Sauver**.

7.2 Configuration d'un tunnel IPsec IKEv2

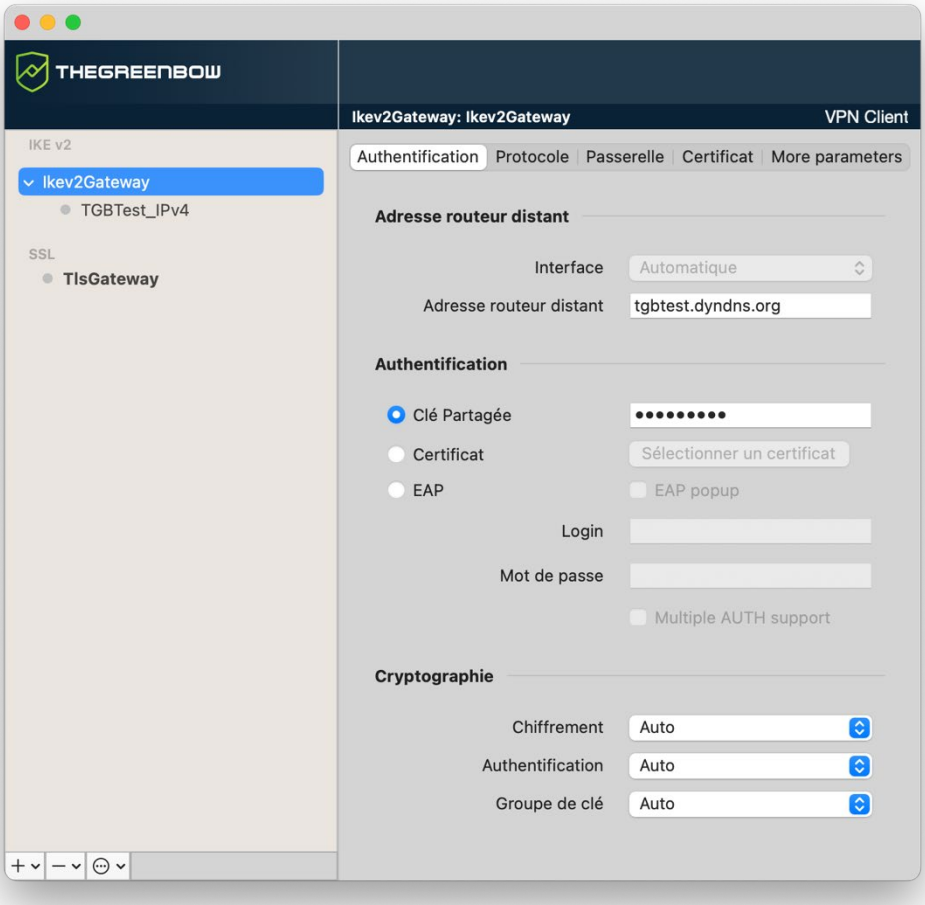
Un tunnel VPN IKE Auth constitue la phase d'authentification dans IKEv2.

IKE Auth a pour objectif de négocier des ensembles de stratégies IKE, d'authentifier les extrémités et de configurer un canal sécurisé entre les extrémités. Dans le cadre de IKE Auth, chaque extrémité du système doit s'identifier et s'authentifier auprès de l'autre.

Pour configurer IKE Auth, sélectionnez un élément IKE Auth[1] dans l'arborescence de la configuration VPN du **Panneau de Configuration**. Les paramètres sont configurés dans les onglets sur le côté droit du **Panneau de Configuration**.

[1] Nom par défaut : `Ikev2Gateway`.

7.2.1 IKE Auth : Authentification



7.2.1.1 Adresse routeur distant

Interface	*(Cette fonctionnalité n'est actuellement pas configurable.)* Nom de l'interface réseau de l'ordinateur à travers laquelle la connexion VPN est établie. Sélectionner **Automatique** permet au Client VPN de choisir automatiquement l'interface appropriée. Le choix **Automatique** permet, par exemple, de configurer un tunnel qui sera déployé sur d'autres ordinateurs.
Adresse routeur distant	Adresse IP (IPv4) ou adresse DNS de la passerelle distante. Ce champ est obligatoire.

7.2.1.2 Authentification

Clé partagée	Mot de passe ou clé partagée par la passerelle distante. La clé partagée (preshared key) est un moyen simple de configurer un tunnel VPN. Elle apporte toutefois moins de souplesse dans la gestion de la sécurité que l'utilisation de certificats. Se reporter au chapitre 11 Recommandations de sécurité.
Certificat	Utilisation d'un certificat pour l'authentification de la connexion VPN. L'utilisation de l'option **Certificat** apporte une plus grande sécurité dans la gestion des connexions VPN (authentification mutuelle, vérification des durées de vie, révocation, etc.). Se reporter au chapitre 11 Recommandations de sécurité. ☞ Se reporter au chapitre dédié 9 Gestion des certificats.
EAP	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. Lorsque le mode EAP est sélectionné, il est possible de choisir entre le fait que le login / mot de passe EAP soient demandés à chaque ouverture de tunnel (via la case **EAP popup**), ou qu'ils soient mémorisés dans la configuration VPN en les configurant dans les champs **Login** et **Mot de passe**. Ce dernier mode n'est pas recommandé (cf. chapitre 11 Recommandations de sécurité).
Multiple AUTH Support	Active la combinaison des deux authentifications par certificat puis par EAP.[1]

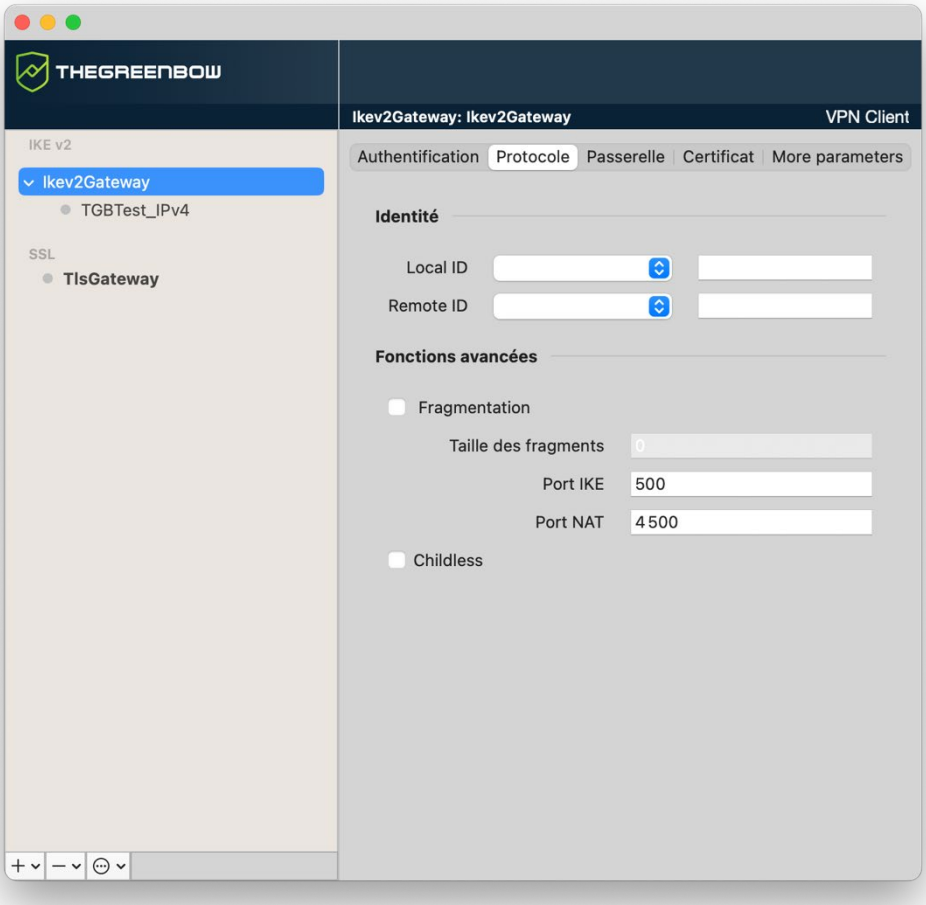
[1] Le Client VPN prend en charge la double authentification « certificat puis EAP ». Le Client VPN ne prend pas en charge la double authentification « EAP puis certificat ».

7.2.1.3 Cryptographie

Chiffrement	Algorithme de chiffrement négocié au cours de la phase d'authentification[1] : Auto[2], 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[3] : Auto[4], SHA2 256, SHA2 384, SHA2 512.
Groupe de clé	Longueur de la clé Diffie-Hellman[5] : Auto[6], DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521) DH28 (BrainpoolP256r1).

[1] Se reporter au chapitre 11 Recommandations de sécurité pour le choix de l'algorithme.
[2] **Auto** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.
[3] Voir note 1.
[4] Voir note 2.
[5] Voir note 1.
[6] Voir note 2.

7.2.2 IKE Auth : Protocole



Si vous utilisez une passerelle IPsec DR, il convient d'ajouter le paramètre dynamique `nonce_size` (voir section 7.2.7 Child SA : Plus de paramètres) et de le définir à la valeur 16. En effet, ces passerelles ne prennent pas en charge de nonce avec une taille différente.

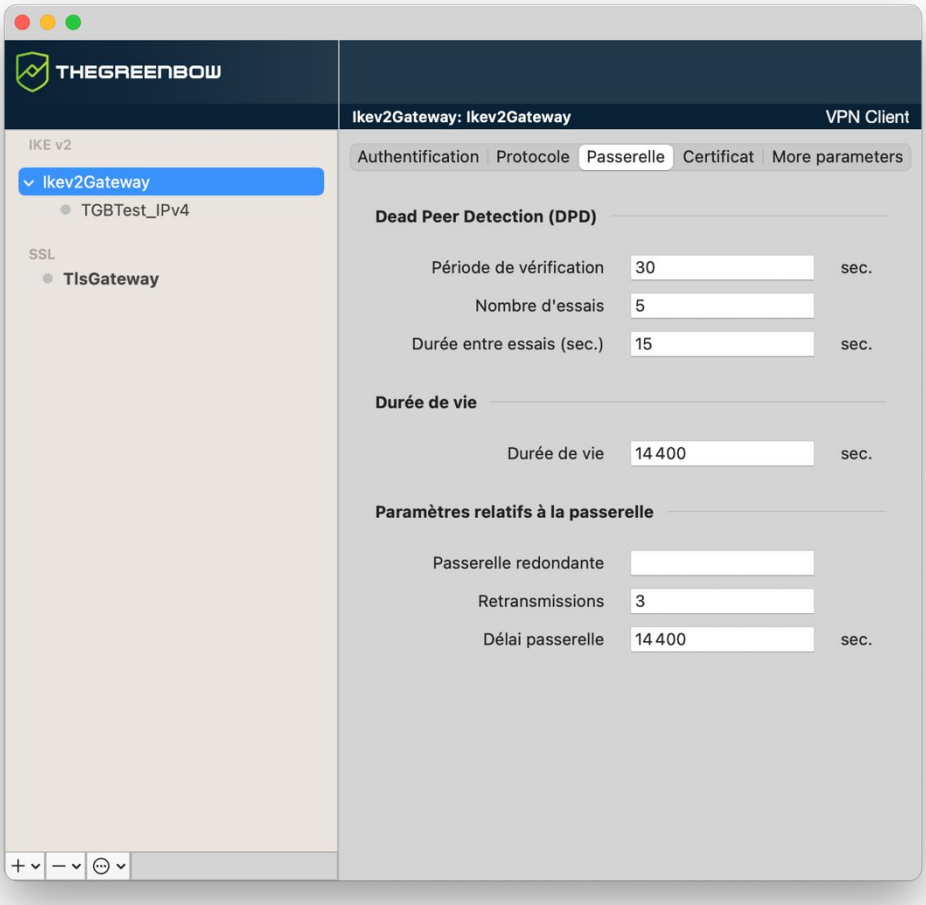
7.2.2.1 Identité

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 : • Adresse IPV4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 195.100.205.101 • DNS : un nom de domaine (type = FQDN), p. ex. gw.mondomaine.net • Email : une adresse email (type = USER FQDN), p. ex. support@thegreenbow.com • Adresse IPV6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3 • DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) • KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123456 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 de la phase d'authentification que le Client VPN s'attend à recevoir de la passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : • Adresse IPV4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 80.2.3.4 • DNS : un nom de domaine (type = FQDN), p. ex. routeur.mondomaine.com • Email : une adresse email (type = USER FQDN), p. ex. admin@mondomaine.com • Adresse IPV6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3 • DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) • KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123456 Quand ce paramètre n'est pas renseigné, le Client VPN accepte sans vérification tout identifiant envoyé par la passerelle.

7.2.2.2 Fonctions Avancées

Fragmentation	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. En général, il convient de spécifier une taille de fragment inférieure de 200 octets à la MTU de l'interface physique, par exemple 1300 octets dans le cas d'une MTU classique de 1500 octets.
Port IKE	Les échanges IKE Auth (Authentification) s'effectuent sur le protocole UDP, en utilisant par défaut le port 500. Le paramétrage du port IKE permet de passer les équipements réseau (pare-feux, routeurs) qui filtrent ce port 500. La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Auth sur un port différent de 500.
Port NAT	Les échanges IKE Child SA (IPsec) s'effectuent sur le protocole UDP, en utilisant par défaut le port 4500. Le paramétrage du port NAT permet de passer les équipements réseau (pare-feux, routeurs) qui filtrent ce port 4500. La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Child SA sur un port différent de 4500.
Childless	Lorsque ce mode est activé, le Client VPN tentera d'effectuer l'initiation des échanges IKE sans création de Child SA, conformément au RFC 6023. Ce mode est recommandé.

7.2.3 IKE Auth : Passerelle



7.2.3.1 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.

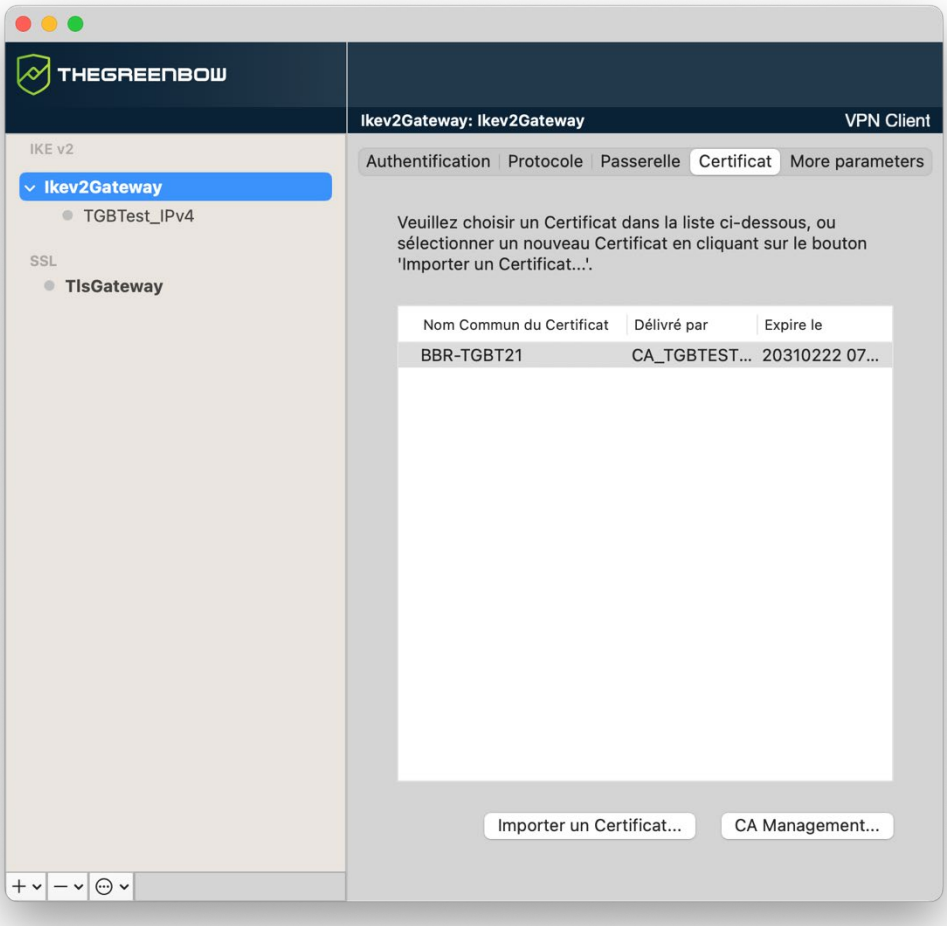
7.2.3.2 Durée de vie

Durée de vie	Durée de vie de la phase IKE Auth. La durée de vie est exprimée en secondes. Sa valeur par défaut est de 1 800 secondes (30 min).

7.2.3.3 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 8 Passerelle redondante.
Retransmissions	Nombre de retransmissions de messages protocolaires IKE avant échec.
Délai passerelle	Délai entre chaque retransmission

7.2.4 IKE Auth : Certificat



Cet onglet est uniquement disponible lorsque le mode Certificat ou EAP (pour la double-authentification EAP + certificat) est choisi dans l'onglet **Authentification**.

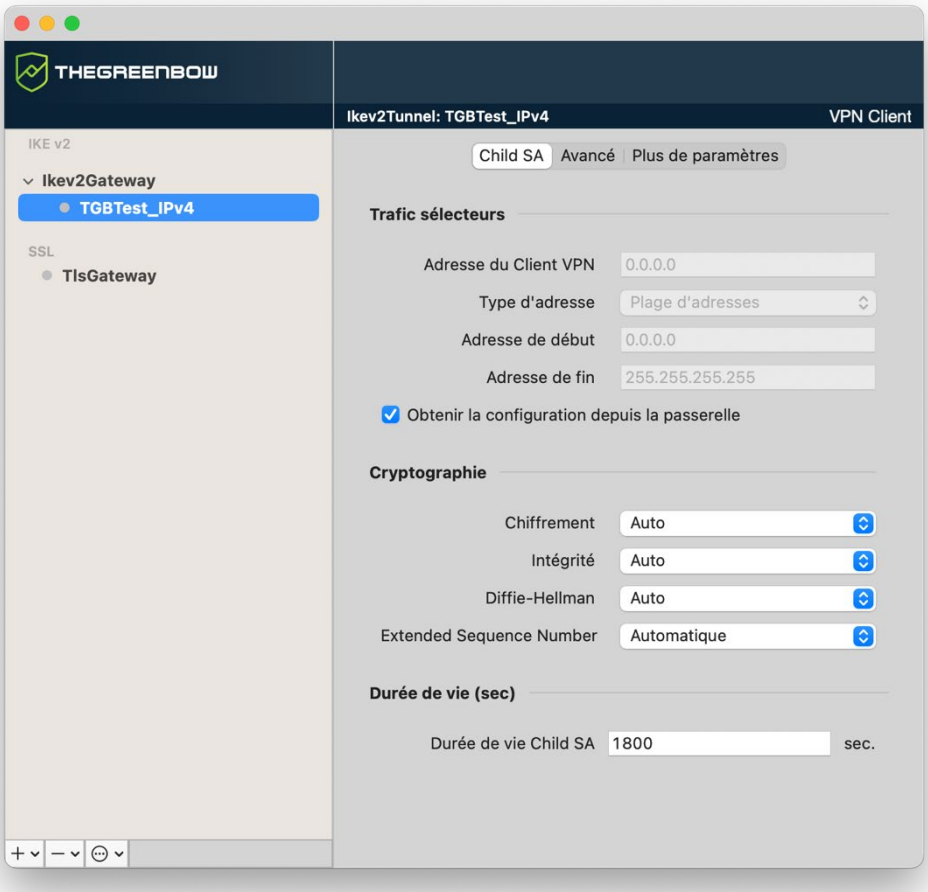
☞ Voir le chapitre 9 Gestion des certificats.

7.2.5 Child SA : Child SA

La « Child SA » (Security Association IPsec) d'un tunnel VPN 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, sélectionnez cette Child SA dans l'arborescence de la configuration VPN 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 de la configuration VPN. Il n'est pas nécessaire d'enregistrer la configuration VPN pour que celle-ci soit prise en compte : le tunnel peut être testé immédiatement avec la configuration modifiée.

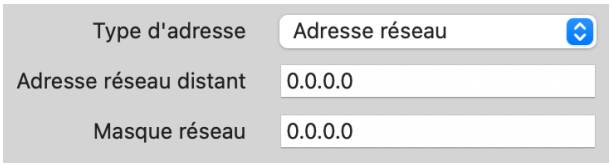
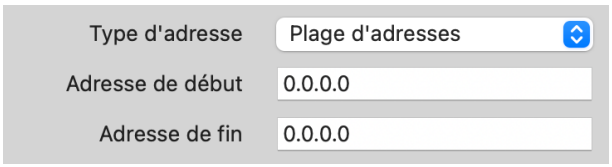


7.2.5.1 Trafic sélecteurs

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 la section 7.2.5.2 Configuration du type d'adresse ci-dessous.

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, masque réseau 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 Mode CP.

7.2.5.2 Configuration du type d'adresse

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

Si l'adresse IP du Client VPN fait partie du plan d'adressage IP du réseau distant (par exemple @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, sélectionnez le type d'adresse **Adresse réseau** et indiquer `0.0.0.0` comme **Adresse réseau distant** et **Masque réseau**.

☞ De nombreux guides de configuration du Client VPN avec différentes passerelles VPN sont disponibles sur le site web TheGreenBow : https://thegreenbow.com/fr/support/guides-dintegration/passerelles-vpn-compatibles/.

7.2.5.3 Cryptographie

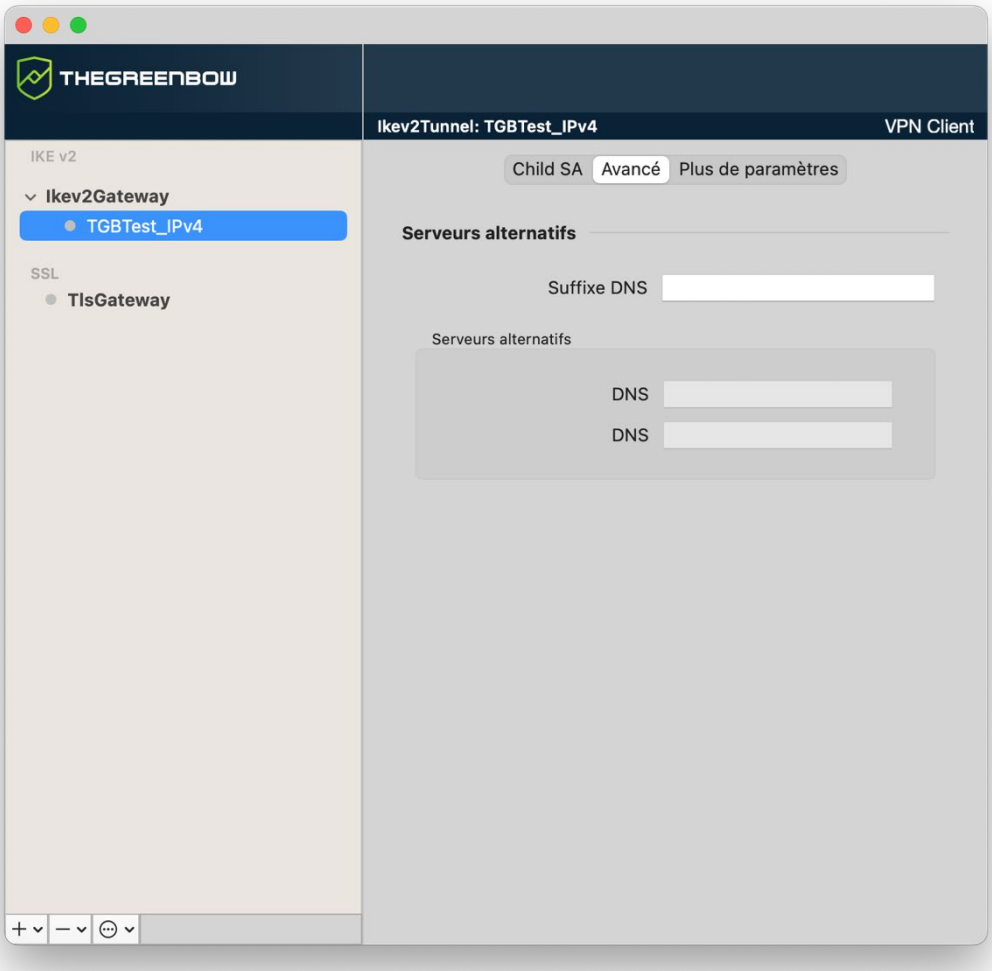
Chiffrement	Algorithme de chiffrement négocié au cours de la phase IPsec[1] : Auto[2], AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Intégrité	Algorithme d'authentification négocié au cours de la phase IPsec[3] : Auto[4], SHA2 256, SHA2 384, SHA2 512.
Diffie-Hellman	Longueur de la clé Diffie-Hellman[5] : Auto[6], DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521), DH28 (BrainpoolP256r1).
Extended Sequence Number	Permet l'usage de numéros de séquence étendus de taille 64 bits (cf. RFC 4304) : Automatique[7], Non, Oui. Il est recommandé d'activer le mode ESN.

7.2.5.4 Durée de vie (sec)

Durée de vie Child SA	Durée en secondes entre deux renégociations. La valeur par défaut pour la durée de vie Child SA est de 1 800 s (30 min).

[1] Reportez-vous au chapitre 11 Recommandations de sécurité pour le choix de l'algorithme.
[2] **Auto** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.
[3] Voir note 1.
[4] Voir note 2.
[5] Voir note 1.
[6] Voir note 2.
[7] Voir note 2.

7.2.6 Child SA : Avancé



7.2.6.1 Serveurs alternatifs

Suffixe DNS Suffixe de domaine à ajouter à chaque nom de machine, par exemple : `mozart.dev.thegreenbow`.

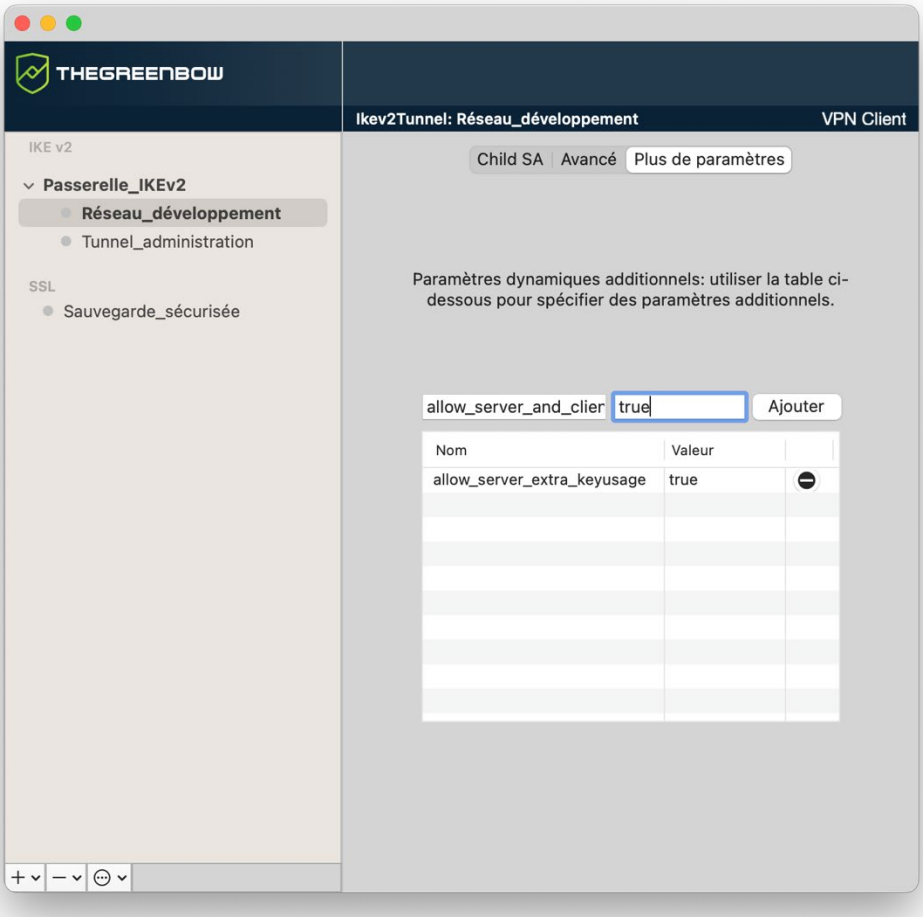
Ce paramètre est optionnel. Lorsqu'il est spécifié, le Client VPN essaye de traduire l'adresse de la machine sans ajouter le suffixe DNS. Puis, si la traduction échoue, il ajoute le suffixe DNS et essaye à nouveau de traduire l'adresse.

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, étant donné que l'IPv6 n'est pas pris en charge dans la version actuelle du produit.

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.

7.2.7 Child SA : Plus de paramètres



Le Client VPN macOS permet si besoin de configurer des paramètres dynamiques additionnels au niveau de la configuration IKE Auth, dont seuls les suivants sont documentés dans le présent guide :

- Spécifier la taille du nonce pour les passerelles IPsec DR
  - `nonce_size` (cf. section 7.2.2)
- Utiliser l'algorithme de hachage SHA-2 dans la charge utile de demande de certificat
  - `sha2_in_cert_req` (cf. section 9.5.3)
- Valider le certificat même s'il ne se conforme pas aux contraintes relatives à l'extension Key Usage
  - `allow_server_extra_keyusage` (cf. section 9.4.3)
- Valider le certificat même s'il ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage
  - `allow_server_and_client_auth` (cf. section 9.4.4)
- Employer d'autres méthodes d'authentification des certificats
  - `Method14_RSASSA_PKCS1` (cf. section 13.1.3)
  - `Method1_PKCS1v15_Scheme` (cf. section 13.1.3)

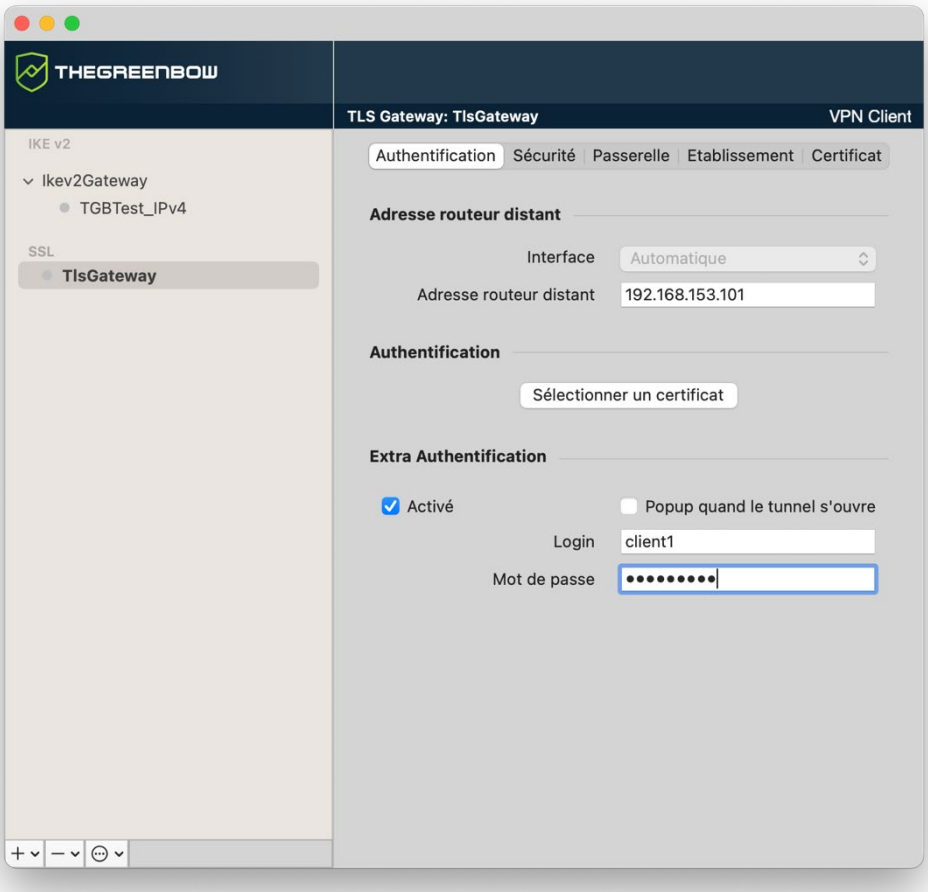
Dans certaines circonstances, le support TheGreenBow peut vous proposer d'ajouter d'autres paramètres dynamiques (Nom, Valeur), non documentés dans le présent guide, qui permettront de gérer des cas d'usage particuliers, soit sur la version du logiciel installée, soit sur des patches qui vous seront fournis.

7.3 Configuration d'un tunnel SSL / OpenVPN

Le Client VPN macOS permet d'ouvrir des tunnels VPN SSL.

Les tunnels VPN SSL du Client VPN macOS sont compatibles OpenVPN et permettent d'établir des connexions sécurisées avec toutes les passerelles qui implémentent ce protocole.

7.3.1 SSL : Authentification



7.3.1.1 Adresse routeur distant

Interface	*(Cette option n'est actuellement pas modifiable.)* 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 (IPv4, car IPv6 n'est pas pris en charge actuellement) ou adresse DNS de la passerelle VPN distante. Ce champ doit être obligatoirement renseigné.

7.3.1.2 Authentification

Sélectionner un certificat Sélection du Certificat pour l'authentification de la connexion VPN.

☞ Se reporter au chapitre dédié 9 Gestion des certificats.

7.3.1.3 Extra Authentification

Cette option apporte un niveau de sécurité supplémentaire en demandant à l'utilisateur la saisie d'un login / mot de passe à chaque ouverture du tunnel.

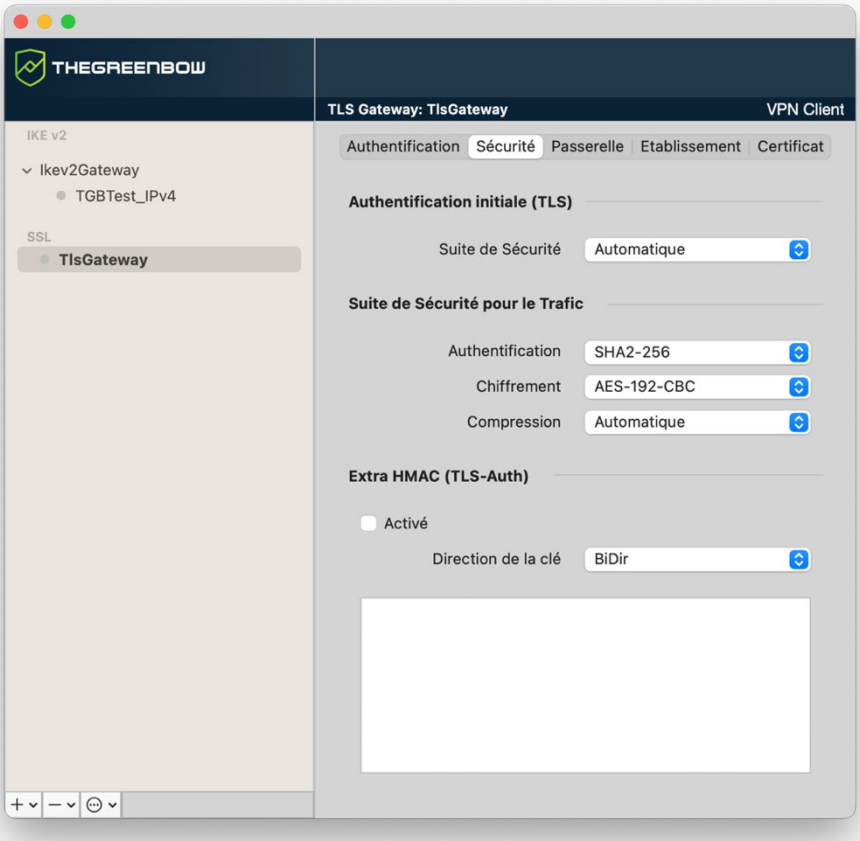
Activé Active ou désactive ce niveau de sécurité supplémentaire.

Popup quand le tunnel s'ouvre Lorsque cette case est cochée, le login et le mot de passe seront demandés à l'utilisateur à chaque ouverture du tunnel. Lorsqu'elle est décochée, le login et le mot de passe doivent être saisis ici de manière permanente. L'utilisateur n'aura alors pas besoin de les saisir à chaque ouverture du tunnel.

Login Le nom d'utilisateur enregistré auprès de la passerelle VPN.

Mot de passe Le mot de passe correspondant au login.

7.3.2 SSL : Sécurité



7.3.2.1 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/man1.1.1/man1/ciphers.html

7.3.2.2 Suite de Sécurité pour le Trafic

Authentification	Algorithme d'authentification négocié pour le trafic : Automatique[1], SHA-224, SHA-256, SHA-384, SHA-512.
Chiffrement	Algorithme de chiffrement du trafic : Automatique[2], AES-128-CBC, AES-192-CBC, AES-256-CBC.
Compression	Compression du trafic : Automatique[3], LZO, Non, LZ4.

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.

7.3.2.3 Extra HMAC (TLS-Auth)

Activé

Cette option ajoute un niveau d'authentification aux paquets échangés entre le Client VPN et la passerelle VPN. Pour être opérationnelle, cette option doit aussi être configurée sur la passerelle (sur une passerelle, cette option est souvent appelée « TLS-Auth »)

Quand cette option est sélectionnée, une clé doit être saisie dans le champ situé en dessous de la case cochée. Cette clé doit être saisie à l'identique sur la passerelle. C'est une suite de caractères hexadécimaux, dont le format est :

```
-----BEGIN Static key-----
362722d4fbff4075853fbe6991689c36
b371f99aa7df0852ec70352122aee7be
…
515354236503e382937d1b59618e5a4a
cb488b5dd8ce9733055a3bdc17fb3d2d
-----END Static key-----
```

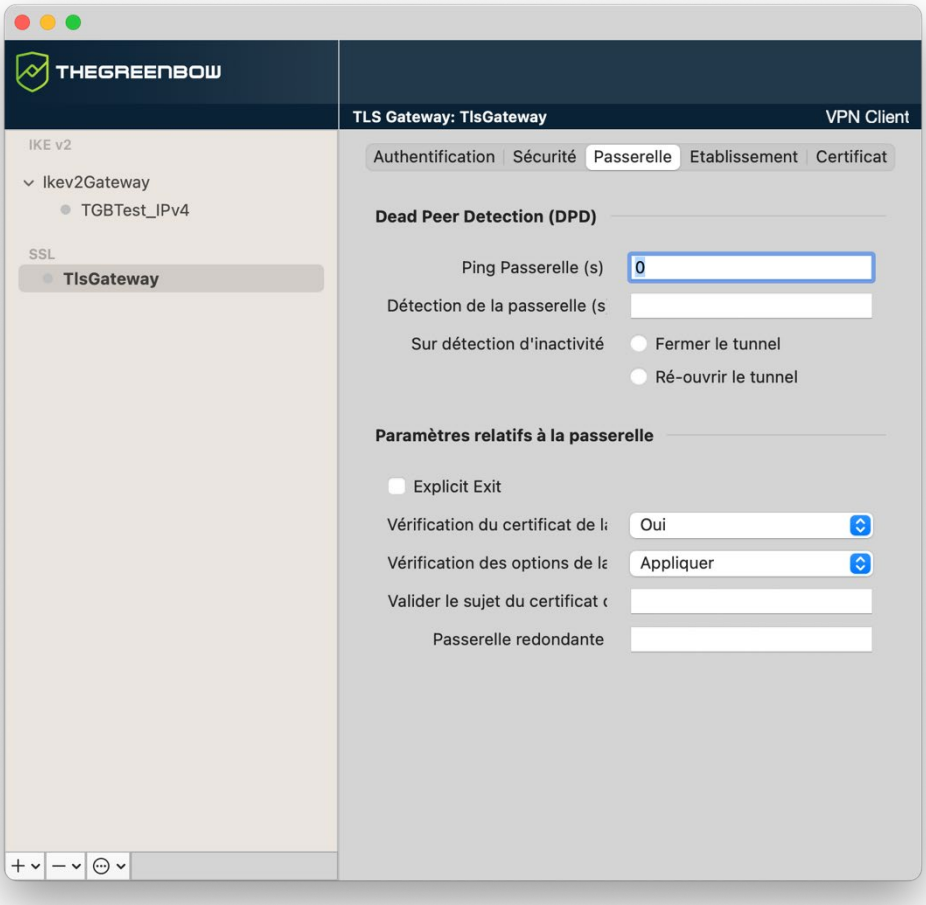
Direction de la clé

Lorsque l'option Extra HMAC est activée, il convient de choisir la direction de la clé dans cette liste déroulante :

- **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**.

[1] **Automatique** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.
[2] idem
[3] idem

7.3.3 SSL : Passerelle



7.3.3.1 Dead Peer Detection (DPD)

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

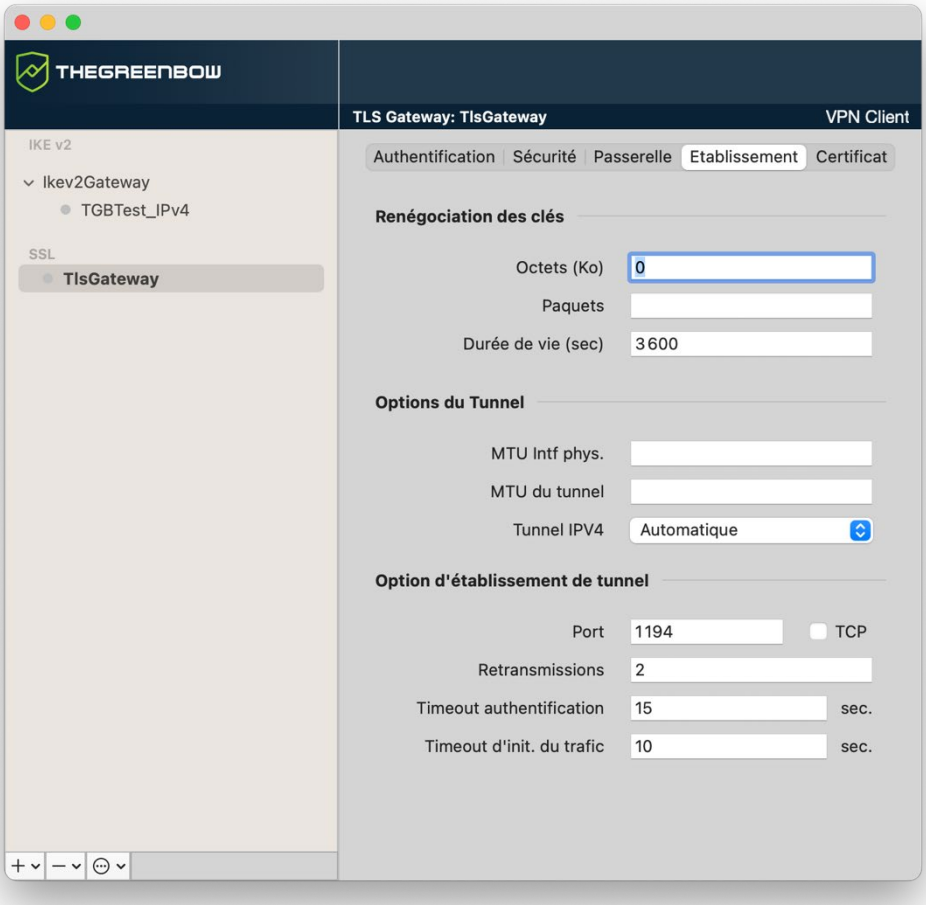
Ping Passerelle (s)	Période exprimée en seconde d'envoi par le Client VPN d'un « ping » vers la passerelle. Cet envoi permet à la passerelle de déterminer que le Client VPN est toujours présent.
Détection de la passerelle (s)	Durée en secondes à l'issue de laquelle, si aucun « ping » n'a été reçu de la passerelle, celle-ci est considérée comme indisponible.
Sur 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 rouvrir.

[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.

7.3.3.2 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 appliqué au 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 un usage futur. Il est équivalent au choix **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 8 Passerelle redondante.

7.3.4 SSL : Établissement



7.3.4.1 Renégociation des clés

Octets (Ko), Paquets, Duréede vie (sec)

Les clés peuvent être renégociées sur échéance de 3 critères (qui peuvent être combinés) :

- Quantité de trafic, exprimée en Ko
- Quantité de paquets, exprimée en nombre de paquets
- Durée de vie, exprimée en seconde

Si plusieurs critères sont configurés, les clés sont renégociées sur échéance du premier critère vérifié

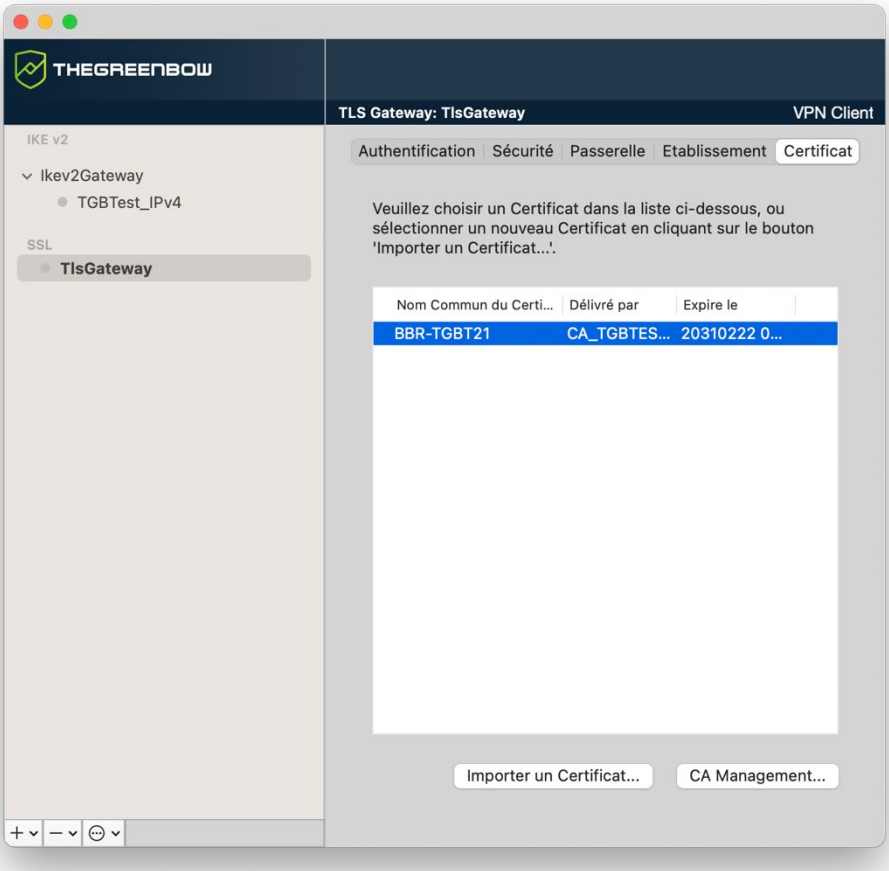
7.3.4.2 Options du tunnel

MTU Interf phys.	Taille maximale des paquets OpenVPN. Permet de spécifier une taille de paquet de telle sorte 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.
Tunnel IPV4	Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv4 : • **Automatique** : Accepte ce qui est envoyé par la passerelle • **Oui** : Vérifie que ce qui est envoyé par la passerelle correspond au comportement configuré. Si ce n'est pas le cas, un message d'alerte est affiché dans la console et le tunnel ne se monte pas. • **Non** : Ignore

7.3.4.3 Option d'établissement de 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.
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 authentification	Délai d'établissement de la phase d'authentification au bout duquel on considère que le tunnel ne s'ouvrira pas. À échéance de ce timeout, 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.

7.3.5 SSL : Certificat



☞ Voir le chapitre 9 Gestion des certificats.

8 Passerelle redondante

Le Client VPN macOS 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 rouvrir 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 deux 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.

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.

Le Client VPN n'essaye pas de contacter la passerelle redondante si la passerelle initiale est inaccessible à cause d'un problème de résolution DNS.

9 Gestion des certificats

9.1 Introduction

Le Client VPN macOS offre un ensemble de fonctions permettant l'exploitation de certificats, issus de PKI / IGC de tout type et stockés dans des fichiers.

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

- Prise en compte des formats de certificats X.509 : PKCS#12, PEM, PFX
- Gestion des certificats côté utilisateur (côté client VPN), comme des certificats de la passerelle VPN, incluant la gestion des dates de validité, des chaînes de certification, des certificats racines et des CRL
- Gestion des autorités de certification (Certificate Authority : CA)
- Validation des certificats client et passerelle : authentification mutuelle, avec autorité de certification identiques ou différentes (importation de CA spécifiques)

La configuration et la caractérisation des certificats peut être effectuée dans l'onglet **Certificat** du tunnel concerné : IKE Auth (IKEv2) ou TLS (SSL).

Les types de certificat suivants sont pris en charge :

- RSASSA-PKCS1-v1.5 avec SHA-2 (uniquement si le paramètre dynamique correspondant est configuré, cf. section 13.1.3 Méthodes d'authentification des certificats)
- RSASSA-PSS avec SHA-2 (uniquement si le paramètre dynamique correspondant est configuré, cf. section 13.1.3 Méthodes d'authentification des certificats)
- ECDSA « secp256r1 » avec SHA-2 (256 bits)
- ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits)

☞ Pour en savoir davantage sur les méthodes d'authentification et la cryptographie utilisées dans le Client VPN macOS, consultez la section 13.1 Notions élémentaires de cryptographie dans l'annexe.

9.2 Certificat utilisateur

Le certificat utilisateur est envoyé par le Client VPN à la passerelle pour qu'elle puisse authentifier l'utilisateur.

Il doit se conformer aux contraintes suivantes (recommandations de sécurité de l'ANSSI) :

- L'extension Key Usage doit être présente, marquée comme critique, et contenir uniquement la valeur `digitalSignature`.
- L'extension Extended Key Usage doit être présente, marquée comme non-critique, et uniquement contenir la valeur `id-kp-clientAuth`.

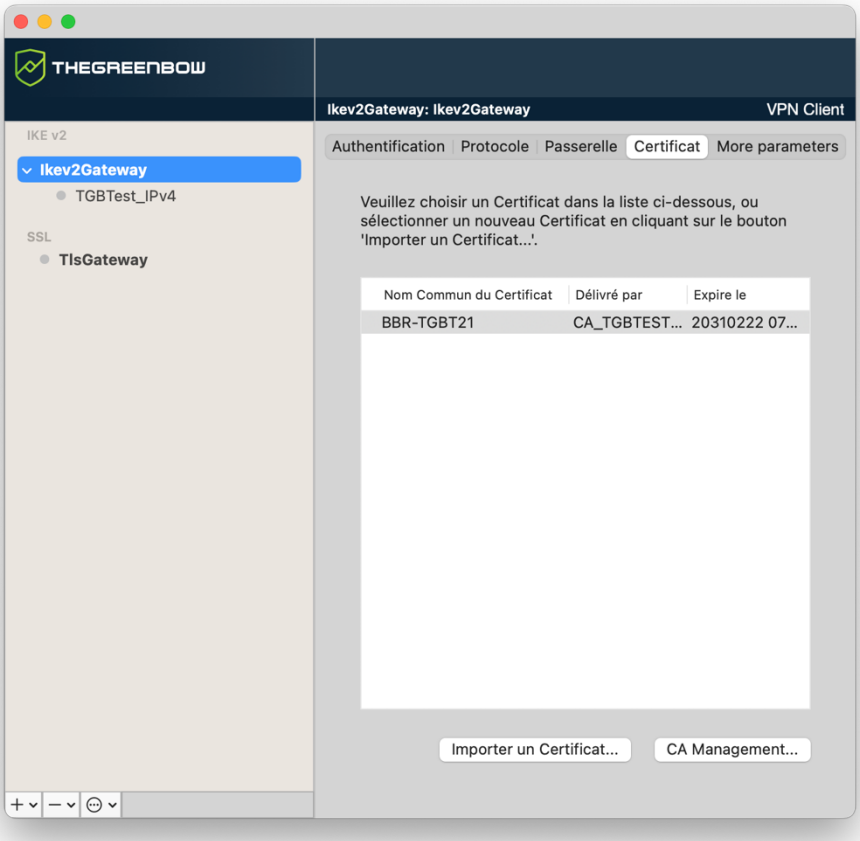
Si ces contraintes ne sont pas respectées, le Client VPN affichera un avertissement dans la **Console** mais n'empêchera pas la communication avec la passerelle. Celle-ci devrait néanmoins refuser l'authentification du Client VPN.

9.3 Sélectionner un certificat (onglet Certificat)

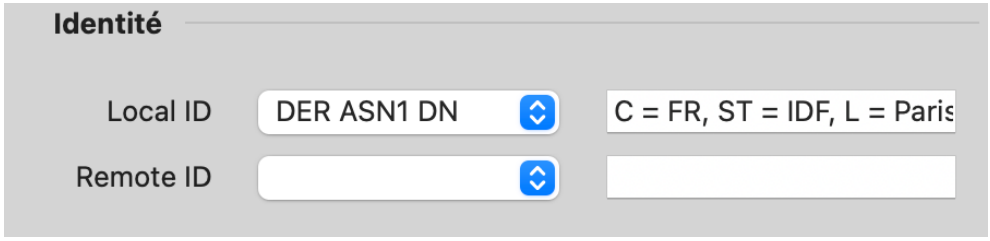
Le Client VPN macOS permet d'affecter un certificat utilisateur à un tunnel VPN.

Il ne peut y avoir qu'un seul certificat par tunnel, mais chaque tunnel peut avoir son propre certificat.

L'onglet **Certificat** affiche le certificat actuellement utilisé dans la configuration du tunnel.



Une fois le certificat sélectionné, le type de Local ID du tunnel passe automatiquement à **DER ASN1 DN**, et le sujet du certificat est utilisé par défaut comme valeur de ce **Local ID**. Voir ci-dessous pour renseigner automatiquement une valeur de DNS ou d'e-mail issue du certificat.



Depuis la version 2.4 du Client VPN macOS, vous pouvez sélectionner le type **DNS** ou **Email** dans la liste déroulante **Local ID**, afin d'affecter automatiquement au Local ID une valeur de DNS ou d'e-mail récupérée du certificat.

9.4 Importer un certificat

Le Client VPN macOS permet d'importer des certificats au format PKCS#12 et PEM dans la configuration VPN.

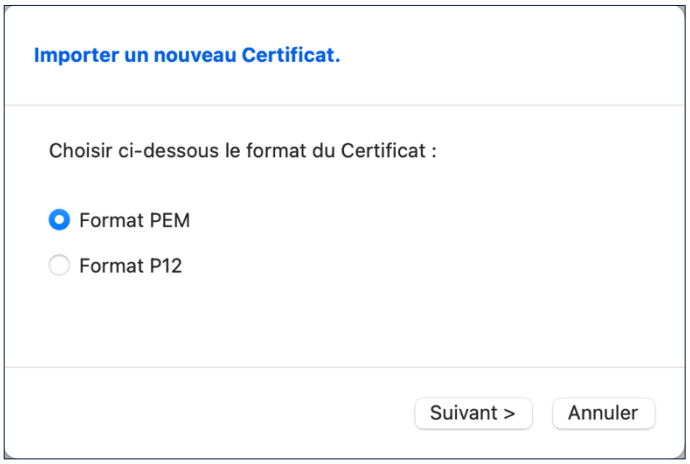
Cette solution présente l'avantage de regrouper le certificat (propre à un utilisateur) et la configuration VPN (a priori générique) dans un fichier unique, facile à transmettre vers le poste utilisateur et à importer dans le Client VPN.

Néanmoins, l'inconvénient de transporter les certificats dans une configuration VPN est que chaque configuration devient alors propre à chaque utilisateur. Cette solution, n'est donc pas préconisée pour un déploiement conséquent.

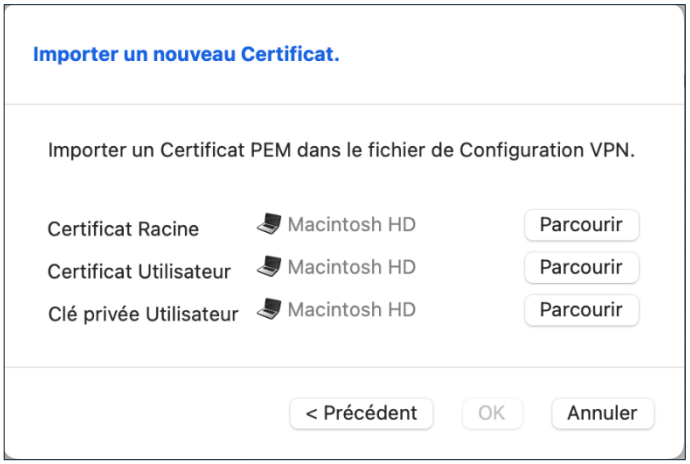
Dès lors qu'un certificat est importé dans une configuration VPN, il est fortement recommandé lors de l'exportation du fichier de configuration, de le protéger par un mot de passe (cf. section 6.2 Exporter une configuration VPN), pour éviter que le certificat ne soit visible en clair.

9.4.1 Importer un certificat au format PEM/PFX

1. Dans l'onglet **Certificat**, cliquez sur **Importer un Certificat...**



2. Choisissez le **Format PEM**, puis cliquez sur **Suivant >**.



3. Cliquez sur **Parcourir** pour sélectionner le **Certificat Racine**, le **Certificat Utilisateur** et la **Clé privée Utilisateur** à importer.
4. Cliquez sur **OK** pour valider.

Le certificat apparaît et est sélectionné dans la liste des certificats de l'onglet **Certificat**.

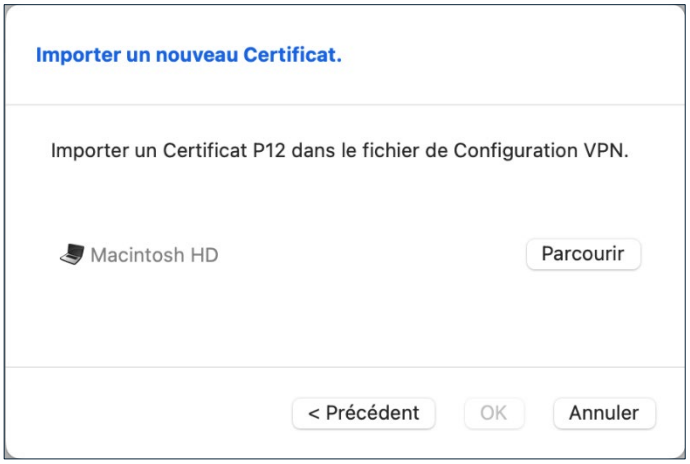
Enregistrez la configuration VPN : le certificat est enregistré dans la configuration VPN.

Le fichier avec la clé privée ne doit pas être chiffré.

9.4.2 Importer un certificat au format PKCS#12

1. Dans l'onglet **Certificat**, cliquez sur **Importer un Certificat...**

2. Choisissez le **Format P12**, puis cliquez sur **Suivant >**.



3. Cliquez sur **Parcourir** pour sélectionner le certificat PKCS#12 à importer.
4. S'il est protégé par un mot de passe, saisissez le mot de passe et cliquez sur **OK** pour valider.

Le certificat apparaît et est sélectionné dans la liste des certificats de l'onglet **Certificat**.

Enregistrez la configuration VPN : le certificat est enregistré dans la configuration VPN.

Toutes les CA au format PKCS#12 présentes dans le fichier seront également importées dans la configuration VPN.

9.4.3 Contraintes relatives à l'extension Key Usage

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Key Usage. Elle doit :

- être présente,
- être marquée comme critique et
- contenir uniquement les valeurs `digitalSignature` et/ou `keyEncipherment`.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le paramètre dynamique `allow_server_extra_keyusage` défini à la valeur `true`.

Dans cette configuration, le certificat sera également validé si l'extension Key Usage contient l'une des combinaisons de valeurs suivantes :

- `digitalSignature` + `keyEncipherment` + `keyAgreement`
- `digitalSignature` + `keyAgreement`
- `nonRepudiation`
- `nonRepudiation` + `keyEncipherment`
- `nonRepudiation` + `keyEncipherment` + `keyAgreement`
- `nonRepudiation` + `keyAgreement`
- `keyEncipherment` + `keyAgreement`

De plus, dans cette configuration l'extension Key Usage peut être marquée comme non critique.

9.4.4 Contraintes relatives à l'extension Extended Key Usage

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Extended Key Usage. Elle doit :

- être présente,
- marquée comme non-critique et
- uniquement contenir la valeur `id-kp-serverAuth`.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le paramètre dynamique `allow_server_and_client_auth` défini à la valeur `true`.

Dans cette configuration, le certificat sera également validé si l'extension Extended Key Usage contient la combinaison de valeurs suivante :

- `id-kp-ServerAuth` + `id-kp-ClientAuth`

9.5 Gestion des autorités de certification

9.5.1 Généralités

Le Client VPN macOS authentifie systématiquement les certificats du client et de la passerelle à partir des autorités de certification (Certificate Authority : CA) présents dans la configuration VPN. Il est donc nécessaire que les certificats CA soient importés dans le Client VPN.

Lorsque le Client VPN macOS est configuré pour vérifier les certificats passerelle, les autorités de certification (CA) doivent être également accessibles.

La CA racine de la passerelle doit obligatoirement être importée dans la configuration.

Si la passerelle n'est pas configurée pour envoyer les CA, alors il est également nécessaire d'importer les CA intermédiaires dans la configuration.

Les types de CA intermédiaires suivants sont pris en charge :

- RSASSA-PKCS1-v1.5 avec SHA-2
- RSASSA-PSS avec SHA-2
- ECDSA « secp256r1 » avec SHA-2
- ECDSA « BrainpoolP256r1 » avec SHA-2

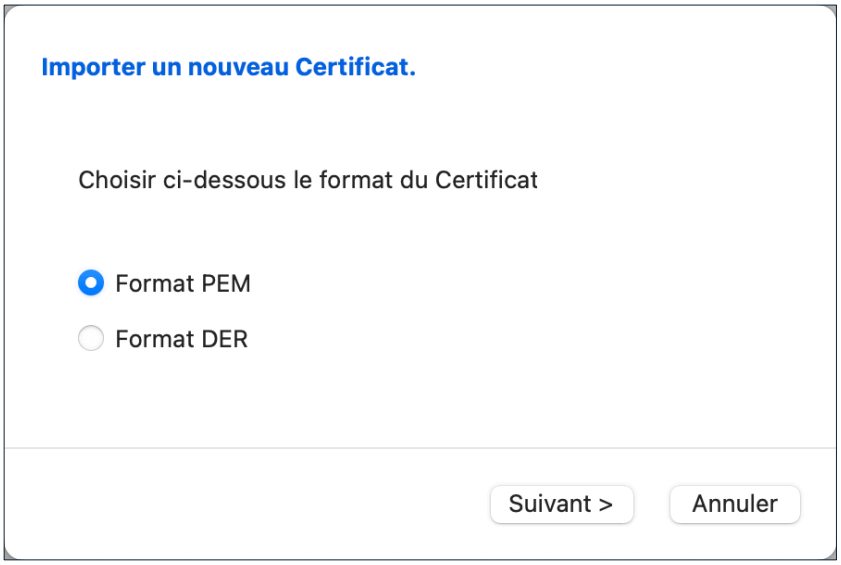
Les types de CA racine suivants sont pris en charge :

- RSASSA-PKCS1-v1.5 avec SHA-2
- RSASSA-PSS avec SHA-2
- ECDSA « secp256r1 » avec SHA-2
- ECDSA « BrainpoolP256r1 » avec SHA-2

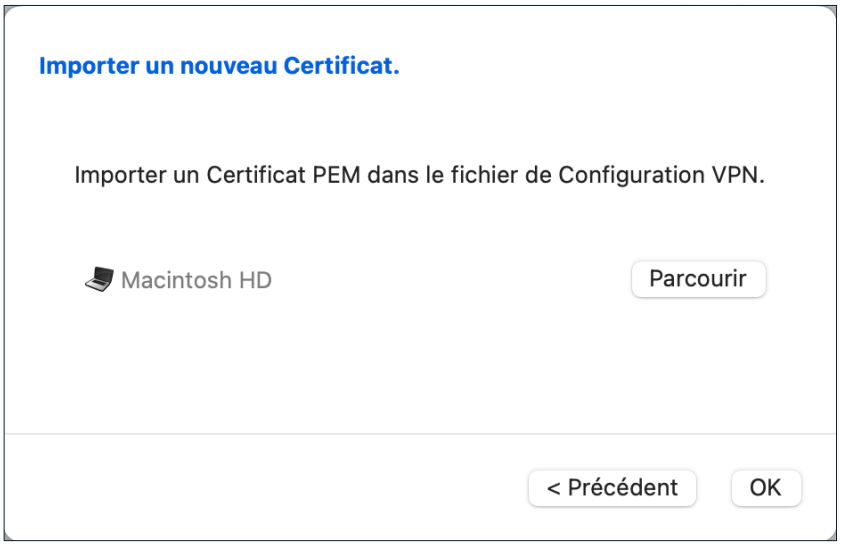
9.5.2 Importer une autorité de certification

1. Dans l'onglet **Certificat**, cliquez sur **CA Management**, la boîte de dialogue **Gestion de l'autorité des certificats** s'affiche.

2. Cliquez sur **Ajouter CA**. La boîte de dialogue **Importer un nouveau Certificat** s'affiche.



3. Choisissez le type de certificat CA souhaité (PEM ou DER), puis cliquez sur **Suivant >**.



4. Cliquez sur **Parcourir** pour sélectionner le CA à importer.

9.5.3 Mode IPsec DR

Pour pouvoir utiliser le Client VPN macOS en mode IPsec DR, l'une des exigences du référentiel IPsec DR de l'ANSSI est que la valeur `Certification Auhtority` dans la charge utile de demande de certificat (CERTREQ payload) est une liste concaténée de condensats SHA-2 des clés publiques des autorités de certification de confiance.

Pour cela, vous devez ajouter le paramètre dynamique `sha2_in_cert_req` défini à la valeur `true` (voir section 7.2.7 Child SA : Plus de paramètres).

☞ Pour savoir comment configurer le Client VPN macOS en vue de l'utiliser avec une passerelle configurée en mode IPsec DR, consultez le guide de configuration « Client VPN et IPsec DR » disponible sur le site TheGreenBow.

10 Logs

Le Client VPN macOS propose trois types de logs :

1. la **Console** macOS, qui fournit des informations sur les étapes d'ouverture et de fermeture du tunnel ;
2. le mode traçant qui fournit des informations détaillées ;
3. les logs Système, qui indiquent des évènements généraux, comme l'ouverture ou la fermeture des tunnels.

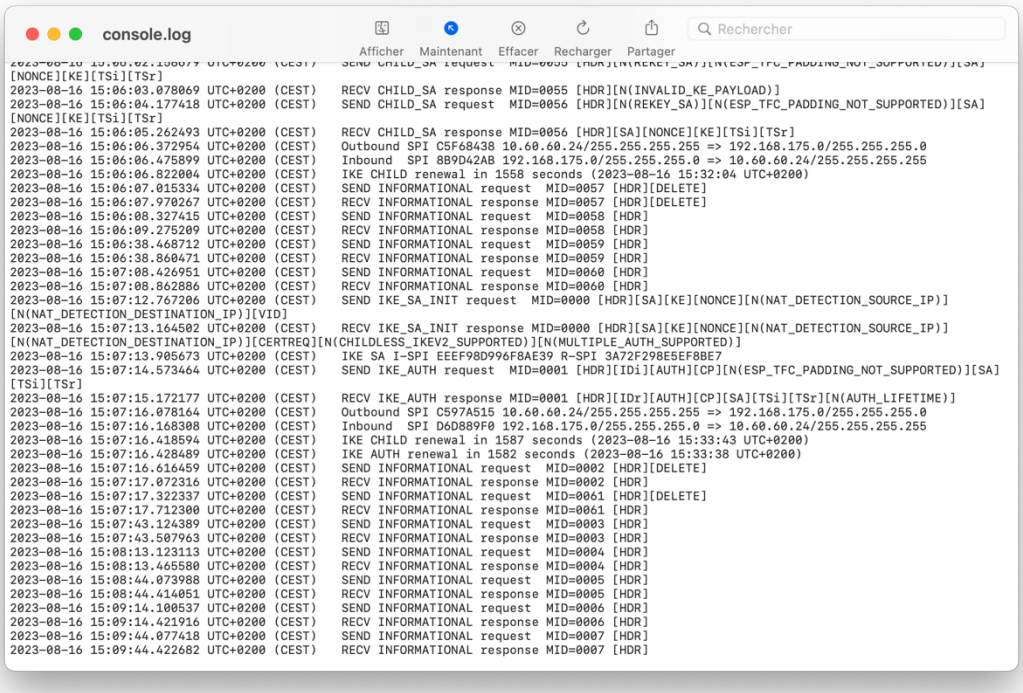
Cet outil est conçu pour aider l'administrateur réseau à diagnostiquer un problème lors de l'ouverture des tunnels, ou l'équipe de support TheGreenBow pour identifier les incidents du logiciel.

10.1 Console

La Console peut être affichée par les moyens suivants :

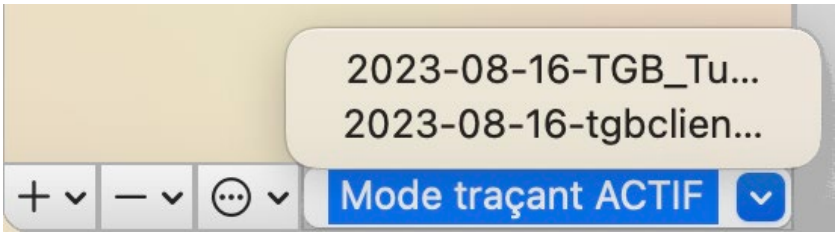
- option de menu **Affichage** > **Console** dans le **Panneau de Configuration** (interface principale) ;
- raccourci ⌘**D** lorsque le **Panneau de Configuration** est ouvert.

Ceci ouvrira le fichier `console.log` dans la **Console** native de macOS.



10.2 Mode traçant

Le mode traçant peut être activé ou désactivé en utilisant la combinaison de touches ⌘⇧T. Un nouveau bouton apparaîtra en dessous de la liste des tunnels VPN. Ce bouton permet de voir la liste des logs détaillés disponibles.



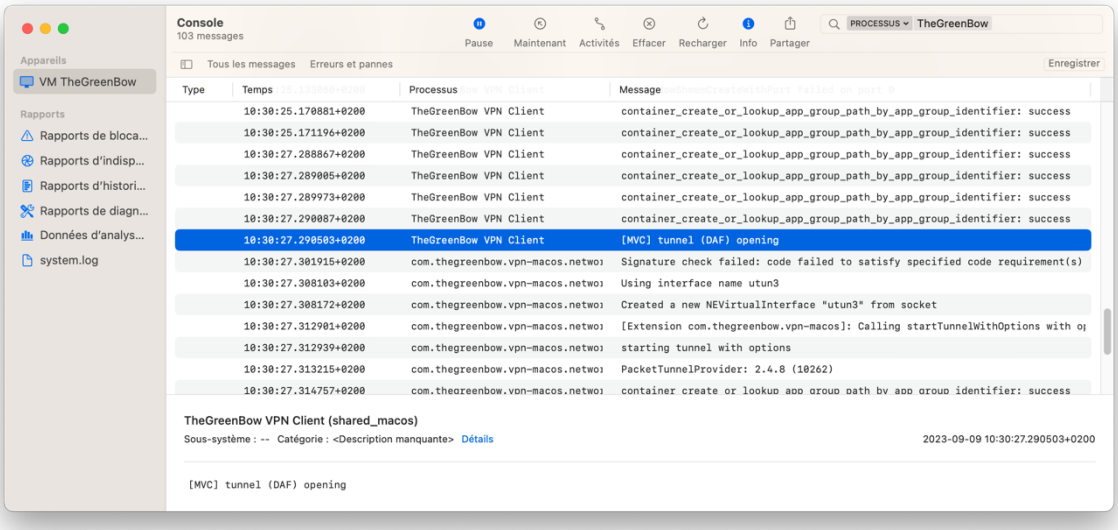
Une fois sélectionné, le log détaillé sera affiché dans l'application **Console** de macOS.

10.3 Logs Système

Les logs Système sont affichés par défaut à l'ouverture de la **Console** de macOS.

Veillez à bien sélectionner la fenêtre **Console** générique, et non l'une des fenêtres spécifiques (comme celle ouverte pour afficher `console.log` dans la section 10.1 Console ou dans la section 10.2 Mode traçant ci-dessus).

Dans l'application **Console** de macOS, il est possible de filtrer les messages provenant du processus VPN `TheGreenBow VPN` en utilisant les termes : `Processus : TheGreenBow VPN Client` ou `Processus : com.thegreenbow.vpn-macos.networkextension`.



11 Recommandations de sécurité

11.1 Hypothèses

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

11.1.1 Profil et responsabilités des administrateurs

L'administrateur système et réseau et l'administrateur sécurité chargés respectivement de l'installation du logiciel et de la définition des politiques de sécurité VPN sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et les procédures d'administration.

L'administrateur sécurité s'assure régulièrement que la configuration du produit est conforme à celle qu'il a mise en place et effectue les mises à jour requises le cas échéant.

La fonction de journalisation du produit est activée et correctement configurée. Les administrateurs sont responsables de la consultation régulière des journaux.

11.1.2 Profil et responsabilités de l'utilisateur

L'utilisateur du logiciel est une personne non hostile et formée à son utilisation. En particulier, l'utilisateur exécute les opérations dont il a la charge pour le bon fonctionnement du produit et ne divulgue pas les informations utilisées pour son authentification auprès de la passerelle VPN.

11.1.3 Respect des règles de gestion des éléments cryptographiques

Les bi-clés et les certificats utilisés pour ouvrir le tunnel VPN sont gérés (génération, révocation) par une autorité de certification de confiance qui garantit le respect des règles dans la gestion de ces éléments cryptographiques et plus particulièrement les recommandations issues de [RGS_B1] et [RGS_B2].

11.2 Poste de l'utilisateur

La machine sur laquelle est installé et exécuté le logiciel Client VPN macOS doit être saine et correctement administrée. En particulier :

- Elle dispose d'un anti-virus dont la base de données est régulièrement mise à jour.
- 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.
- Son système d'exploitation est à jour des différents correctifs.
- 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
- Mot de passe

11.3 Configuration VPN

11.3.1 Données sensibles dans la configuration VPN

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

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

- Ne pas utiliser le mode EAP (mot de passe / login) seul, mais uniquement en combinaison avec un certificat,
- Dans le cas où EAP est utilisé, ne pas mémoriser le login / mot de passe EAP dans la configuration VPN (fonction décrite à la section 7.2.1.2 Authentification),
- Ne pas importer de certificat dans la configuration VPN (fonction décrite à la section 9.4 Importer un certificat),
- Ne pas exporter la configuration VPN en clair, c'est-à-dire non protégée par un mot de passe (fonction décrite à la section 6.2 Exporter une configuration VPN).

11.3.2 Authentification de l'utilisateur

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

En particulier, il est à noter qu'une authentification par clé partagée (preshared 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
EAP	
EAP popup	
Certificat mémorisé dans la configuration VPN	forte

11.3.3 Authentification de la passerelle VPN

Il est recommandé de ne pas configurer le Client VPN pour valider les certificats non conformes aux contraintes relatives aux extensions Extended Key Usage et Key Usage (ne pas utiliser le paramètre dynamique `allow_server_and_client_auth`).

11.3.4 Protocole

Il est recommandé de ne configurer que des tunnels IPsec / IKEv2 (et pas SSL / OpenVPN).

11.3.5 Recommandations 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.

12 Contact

12.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur le site : https://thegreenbow.com/.

12.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

12.3 Support

Le site TheGreenBow propose plusieurs pages concernant le support technique des logiciels :

Aide en ligne

https://thegreenbow.com/fr/support/assistance/

FAQ

https://thegreenbow.com/fr/faq/

Formulaire de contact

Le support technique est accessible via un formulaire disponible sur le site TheGreenBow à l'adresse : https://thegreenbow.com/fr/support/assistance/support-technique/.

13 Annexes

13.1 Notions élémentaires de cryptographie

13.1.1 Algorithmes SHA, RSA et ECDSA

Les signatures numériques font généralement intervenir deux algorithmes différents :

- un algorithme de hachage (SHA ou *secure hash algorithm*) et
- un algorithme de signature (RSA : initiales des trois inventeurs ou ECDSA : *elliptic curve digital signature algorithm*.

La force du chiffrement RSA dépend de la taille de la clé utilisée. Dès lors que la taille est doublée, l'opération de déchiffrage va demander une puissance de traitement six à sept fois supérieure.

Selon l'ANSSI et le NIST, la taille de clé minimale recommandée est de 2048 bits.

Les algorithmes de hachage peuvent subir deux types d'attaques :

- la collision et
- la pré-image.

Une collision a lieu lorsque deux fichiers différents produisent le même condensat et qu'il est donc possible de substituer l'un pour l'autre.

La pré-image consiste à déterminer la valeur d'un fichier à partir de son condensat. Une pré-image secondaire consiste à produire à partir du condensat une valeur différente que celle à l'origine du hachage.

Selon l'ANSSI, la famille de fonctions de hachage SHA-1 n'est plus conforme à son référentiel général de sécurité et il convient par conséquent d'utiliser la famille SHA-2. Le NIST encourage de la même manière les agences fédérales étatsuniennes d'abandonner le SHA-1 au profit du SHA-2.

Les règles appliquées par le Client VPN macOS suivent les recommandations de l'ANSSI et du NIST. Toutefois, si la PKI implémentée ne répond pas à ces exigences, il est possible de débrider le logiciel à l'aide de paramètres dynamiques.

On trouve plusieurs notations pour les algorithmes de la famille SHA-2. Par exemple, SHA-2 (256 bits) s'écrit aussi SHA-256, SHA-2 (384 bits) s'écrit aussi SHA-384 et ainsi de suite.
Il en va de même pour les courbes elliptiques. Par exemple, pour secp256r1 on parle aussi de « courbe P-256 », pour secp384r1 de « courbe P-384 » et pour secp521r1 de « courbe P-521 ».

13.1.2 Format des certificats

À partir de la version 2.4 du Client VPN macOS, le format des certificats doit respecter une taille de clé et un algorithme de hachage précis.

Obligatoire

- Longueur de clé (en bits) : dans le cas des certificats RSA, la taille doit être de 2048 ou plus
- Algorithme de prise d'empreinte (ou *digest algorithm*) : doit être SHA-256, SHA-384 ou SHA-512

Optionnel

La vérification de la CRL du certificat utilisateur.

13.1.2.1 Certificat passerelle

Partie Key Usage extension

- doit être présente,
- doit être marquée comme critique et
- ne doit contenir que les valeurs `digitalSignature` et/ou `keyEncipherment`.

☞ Si ce n'est pas le cas, référez-vous au paramètre dynamique `allow_server_extra_keyusage` décrit dans la section 9.4.3 Contraintes relatives à l'extension Key Usage.

Partie Extended Key Usage extension

- doit être présente,
- doit être marquée comme non-critique et
- ne doit contenir que la valeur `id-kp-serverAuth`.

☞ Si ce n'est pas le cas, référez-vous au paramètre dynamique `allow_server_and_client_auth` décrit dans la section 9.4.4 Contraintes relatives à l'extension Extended Key Usage.

13.1.2.2 Exemple de log d'un certificat

Les extensions sont présentes dans un log de certificat (fichier `tgbikeng.log`) :

```
20220826 17:20:23:953    Local0.Info         [11204]
X509v3 extensions
20220826 17:20:23:956    Local0.Info         [11204]
Basic constraints :
20220826 17:20:23:960    Local0.Info         [11204]
CA:FALSE
20220826 17:20:23:965    Local0.Info         [11204]
Netscape Certificate comment :
20220826 17:20:23:968    Local0.Info         [11204]
TheGreenBow PKI generated server certificate
20220826 17:20:23:971    Local0.Info         [11204]
Subject key identifier :
20220826 17:20:23:974    Local0.Info         [11204]
FB:D6:5A:EF:FE:1B:DC:68:90:66:B9:D7:47:45:EA:B5:86:97:4
A:B3
20220826 17:20:23:978    Local0.Info         [11204]
Authority key identifier :
20220826 17:20:23:981    Local0.Info         [11204]
keyIdentifier:
6F:6D:B8:A5:0B:EA:64:82:2E:B4:5F:0A:35:53:8B:80:05:4C:7
B:0E
20220826 17:20:23:984    Local0.Info         [11204]
authorityCertIssuer: C = FR, ST = Ile-de-France, L =
Paris, O = TheGreenBow, OU = QA40, CN = Root CA
20220826 17:20:23:988    Local0.Info         [11204]
authorityCertSerialNumber: 10:00
20220826 17:20:23:990    Local0.Info         [11204]
Key usage : critical
20220826 17:20:23:995    Local0.Info         [11204]
Digital signature
20220826 17:20:24:000    Local0.Info         [11204]
Extended key usage :
20220826 17:20:24:003    Local0.Info         [11204]
Server authentication
```

13.1.2.3 Certificat utilisateur

Dans le cas d'un certificat utilisateur, il peut il y avoir des avertissements, mais il n'est pas nécessaire de débrider le Client VPN. Les messages sont affichés dans la **Console**.

13.1.3 Méthodes d'authentification des certificats

Le Client VPN macOS prend en charge les méthodes d'authentification des certificats suivantes :

- Méthode 1 : signature numérique RSA avec SHA-2 [RFC 7296]
- Méthode 9 : ECDSA « secp256r1 » avec SHA-2 (256 bits) sur la courbe P-256 [RFC 4754]
- Méthode 10 : ECDSA « secp384r1 » avec SHA-2 (384 bits) sur la courbe P-384 [RFC 4754]
- Méthode 11 : ECDSA « secp521r1 » avec SHA-2 (512 bits) sur la courbe P-521 [RFC 4754]
- Méthode 14 : signature numérique RSASSA-PSS et RSASSA-PKCS1-v1_5 avec SHA-2 (256/384/512 bits) [RFC 7427]
- Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) sur la courbe BrainpoolP256r1 (uniquement disponible avec des passerelles prenant en charge cette méthode)

Par défaut, la méthode d'authentification utilisée pour les certificats de type RSA (RSASSA-PSS ou RSASSA-PKCS1-v1_5) est la méthode 14 avec signature RSASSA-PSS. Si la passerelle / le pare-feu utilise la méthode 14 avec la signature RSASSA-PKCS1-v1.5, le Client VPN va rejeter le certificat, avec le message suivant dans la **Console** :

```
RSASSA-PKCS1-v1_5 signature scheme not supported with
authentication method 14
```

Dans le cas où la passerelle ne prend pas en charge la méthode 14 avec la signature `RSASSA-PSS`, il est possible de configurer le Client VPN pour employer la méthode 14 avec la signature `RSASSA-PKCS1-v1_5`, en ajoutant le paramètre dynamique `Method14_RSASSA_PKCS1` défini à la valeur `true` ou `yes` (voir section 7.2.7 Child SA : Plus de paramètres).

Dans le cas où la passerelle ne prend pas non plus en charge la méthode 14 avec la signature `RSASSA-PKCS1-v1_5`, il est possible de configurer le Client VPN pour employer la méthode 1 avec signature numérique RSA et SHA-2, en ajoutant le paramètre dynamique `Method1_PKCS1v15_Scheme` défini à la valeur `04` (SHA-256), `05` (SHA-384) ou `06` (SHA-512) (voir section 7.2.7 Child SA : Plus de paramètres). Toute autre valeur sera rejetée par le Client VPN.

La méthode d'authentification utilisée pour les certificats de type ECDSA (courbes elliptiques) dépend de la courbe elliptique utilisée dans le certificat : ECDSA avec SHA-256 sur la courbe P-256, ECDSA avec SHA-384 sur le courbe P-384, ECDSA avec SHA-512 sur la courbe P-521 ou ECDSA avec SHA-256 sur la courbe BrainpoolP256r1.

L'utilisation de l'algorithme SHA-1 dans les signatures numériques n'est pas possible.

Les certificats RSA avec une clé de taille inférieure à 2048 bits seront refusés par le Client VPN macOS.

Les certificats ECDSA avec une clé de taille inférieure à 256 bits seront refusés par le Client VPN macOS.

13.2 Caractéristiques techniques du Client VPN macOS

13.2.1 Principales fonctions

- Configuration et établissement de connexions VPN IPsec / IKEv2
- Gestion des authentifications par EAP ou par certificat
- Gestion du mode Configuration Payload (CP)
- Fonction DPD (Dead Peer Detection) et gestion de passerelle redondante
- Interface de configuration complète et intuitive
- Configuration et établissement de connexions SSL / OpenVPN

13.2.2 Langues

Français, Anglais, Arabe, Tchèque, Danois, Allemand, Grec, Espagnol, Finnois, Hongrois, Hindi, Italien, Japonais, Coréen, Néerlandais, Norvégien, Polonais, Portugais, Roumain, Slovène, Bosniaque, Thaï, Turc, Chinois, Farsi.

13.2.3 OS compatibles

Le système d'exploitation minimal requis pour le Client VPN macOS est macOS 10.15.

13.2.4 Cryptographie et authentification

Chiffrement, Groupes de clé, Hachage (IKEv2)	Symétrique : AES CBC, GCM, CTR 128/192/256 bits Asymétrique : RSA, ECP Diffie-Hellmann : DH 14 (MODP 2048), DH 15 (MODP 3072), DH 16 (MODP 4096), DH 17 (MODP 6144), DH 18 (MODP 8192), DH 19 (ECP 256), DH 20 (ECP 384), DH 21 (ECP 521), DH 28 (BrainpoolP256r1) Hachage : SHA-2 (256/384/512 bits)
Suites de sécurité TLS (OpenVPN)	TLS 1.2 – Medium TLS 1.2 – High TLS 1.3 : • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256
Chiffrement, Hachage (OpenVPN)	Symétrique : AES-128-CBC, AES-192-CBC, AES-256-CBC Hachage : SHA-2 (224/256/384/512 bits)
Authentification	• Clé partagée • EAP-MSCHAPv2 • Certificats X.509 • Multiple Auth
Méthodes d'authentification des certificats	• Méthode 1 : signature numérique RSA avec SHA-2 [RFC 7296] • Méthode 9 : ECDSA « secp256r1 » avec SHA-2 (256 bits) sur la courbe P-256 [RFC 4754] • Méthode 10 : ECDSA « secp384r1 » avec SHA-2 (384 bits) sur la courbe P-384 [RFC 4754] • Méthode 11 : ECDSA « secp521r1 » avec SHA-2 (512 bits) sur la courbe P-521 [RFC 4754] • Méthode 14 : signature numérique RSASSA-PSS et RSASSA-PKCS1-v1_5 avec SHA-2 (256/384/512 bits) [RFC 7427] • Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) sur la courbe BrainpoolP256r1 (uniquement disponible avec des passerelles prenant en charge cette méthode)
IGC / PKI	• Prise en charge des certificats X.509 • Import de certificats au format PKCS#12, PEM/PFX • Vérification complète de la chaîne des certificats « utilisateur » et « passerelle »

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris – France
sales@thegreenbow.com