Client VPN et IPsec DR

Guide de configuration

Dernière mise à jour : 25 octobre 2023
Référence du document : 20231025_CG_ALL_7.4_FR_1.0

www.thegreenbow.com

TheGreenBow est un nom commercial déposé.

Microsoft et Windows 10 sont soit des marques déposées, soit des marques commerciales de Microsoft Corp. aux États-Unis et/ou dans d'autres pays.

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.

Android, Google Chrome, Google Play et le logo Google Play sont des marques commerciales de Google, LLC.

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

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

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2023-10-25	Toutes	Version initiale	FB, SM, BB

1 Introduction

1.1 Objectif du guide

Ce guide décrit comment configurer les clients VPN TheGreenBow Windows, Android et macOS pour établir des connections VPN avec des passerelles configurées en mode IPsec Diffusion Restreinte (IPsec DR).

1.2 Contexte

L'instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles, le texte de référence régissant en France la protection des systèmes d'information sensibles, donne les définitions suivantes dans son article premier :

- les **informations sensibles** sont celles dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre ;
- les **informations *Diffusion Restreinte*** sont celles qui portent la mention *Diffusion Restreinte* ou ses équivalentes européennes ou internationales.

La mention Diffusion Restreinte ou DR n'est pas un niveau de classification mais une mention de protection.

Selon l'ANSSI, « l'intérêt de qualifier une information Diffusion Restreinte est de soumettre l'ensemble des personnes amenées à la manipuler à une restriction de diffusion. Ainsi, l'accès à une information DR est régi par le principe de restriction du besoin d'en connaître : seules les personnes ayant une nécessité impérieuse d'en prendre connaissance dans le cadre de leur fonction et pour une mission précise sont autorisées à y accéder. Cette restriction de diffusion s'applique en cas de transfert de l'information vers une autre entité juridique. Cette dernière doit traiter les données DR conformément à la réglementation, sur un SI où les mesures de sécurité propres à la protection des informations DR sont mises en œuvre. »

L'ANSSI précise en outre que « contrairement aux informations DR, les informations sensibles non DR ne bénéficient pas par défaut d'une protection juridique lorsqu'elles sont transférées à une entité tierce. Il existe toutefois des solutions permettant de dépasser cette limitation. Le *secret des affaires* créé par la loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires est un exemple de réponse à ce besoin. »

Les entreprises qui traitent des savoir-faire et des informations commerciales de valeur ont donc tout à fait intérêt à les protéger de la même manière.

☞ Pour en savoir davantage sur les objectifs et les mesures de sécurité minimales relatifs à la protection des informations sensibles, notamment celles relevant du niveau Diffusion Restreinte (DR), consultez l'instruction interministérielle n° 901/SGDSN/ANSSI (II 901) du 28 janvier 2015 disponible à l'adresse : https://www.legifrance.gouv.fr/circulaire/id/39217.

☞ Pour en savoir davantage sur la protection d'informations sensibles ou Diffusion Restreinte, consultez le guide *Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte* de l'ANSSI disponible à l'adresse : https://www.ssi.gouv.fr/guide/recommandations-pour-les-architectures-des-systemes-dinformation-sensibles-ou-diffusion-restreinte/.

☞ Pour savoir comment utiliser la mention de protection Diffusion Restreinte, consultez la fiche n° 5 du guide *Fiches pratiques à destination des personnes habilitées* disponible à l'adresse : http://www.sgdsn.gouv.fr/uploads/2021/10/fiches-pratiques-psdn-personnes-habilitees-num-v20211001.pdf.

1.3 Référentiel IPsec Diffusion Restreinte

Internet Protocol Security (IPsec) est un ensemble de protocoles, utilisant des algorithmes destinés à protéger le transport de données sur un réseau IP, défini par l'*Internet Engineering Task Force* (IETF). Il est souvent utilisé pour créer des réseaux privés virtuels ou VPN. Dans ce cadre, il est fréquemment associé à un mécanisme de négociation reposant sur l'échange de clés appelé *Internet Key Exchange* (IKE), également défini par l'IETF.

L'ANSSI a élaboré un corpus IPsec DR destiné à définir « un périmètre restreint d'algorithmes cryptographiques » et à clarifier « leur utilisation sur les réseaux de Diffusion Restreinte (DR) ». Il est constitué d'une note cryptographique référentiel IPsec DR qui détaille les exigences, trois RFC associées à IPsec et IKE, et un document récapitulatif qui liste les principales exigences et recommandations.

☞ Le *Corpus documentaire IPsec DR* produit par l'ANSSI est disponible à l'adresse https://www.ssi.gouv.fr/guide/ipsec-dr/.

Parmi les exigences et recommandations de l'ANSSI relatives au référentiel IPsec DR, on peut citer les suivantes :

- Seule la version 2 d'IKE peut être utilisée.
- Seuls les mécanismes cryptographiques AES-GCM, AES-CTR et AUTH_HMAC_SHA2_256_128 sont activés pour assurer la confidentialité et l'intégrité des données du démon IKEv2 et de la pile IPsec.
- La prise en charge des deux courbes elliptiques BrainpoolP256r1 et secp256r1 est imposée.
- Les seuls groupes Diffie-Hellman autorisés sont ceux construits sur les deux courbes elliptiques de 256 bits imposées, soit les groupes DH 19 et DH 28.
- Les nonces produits par le démon IKEv2 ont exactement une taille de 16 octets. Tout nonce reçu d'un homologue qui a une taille strictement différente de 16 octets résulte en un arrêt de l'échange.
- Le démon IKEv2 implémente, négocie et impose la prise en charge de l'initiation *Childless* SA définie dans la [RFC 6023].
- Le démon IKEv2 implémente ECDSA ou ECSDSA comme mécanisme d'authentification asymétrique, ou utilise PRF_HMAC_SHA2_256 comme mécanisme d'authentification symétrique.
- L'utilisation de certains algorithmes (MD5, SHA-1, RSA, DH sur groupe d'entiers) ou de fonctionnalités comme EAP est interdite.
- Étant donné que l'utilisation d'un système de traduction d'adresses (NAT) en conjonction avec IPsec peut poser plusieurs problèmes, l'emploi du « NAT-Traversal » (NAT-T), qui consiste à encapsuler le trafic IKE puis ESP dans des datagrammes UDP utilisant de manière standard le port 4500, est recommandée.

Différentes passerelles du marché proposent une configuration en mode IPsec Diffusion Restreinte (IPsec DR) conforme aux recommandations de l'ANSSI pour les architectures des systèmes d'information Diffusion Restreinte et relatives à IPsec pour la protection des flux réseau.

2 Configuration du Client VPN TheGreenBow

2.1 Introduction

Ce chapitre décrit comment configurer les Clients VPN TheGreenBow pour se connecter à une passerelle configurée en IPsec DR.

Pour satisfaire aux exigences de l'ANSSI relatives au mode IPsec DR côté client VPN, nous allons mettre en place une configuration présentant les caractéristiques suivantes :

- Protocole : IKEv2
- Diffie-Hellman : DH28
- Chiffrement : AES-GCM 256
- Authentification : certificat utilisant la méthode 9 (ECDSA SHA-2 [256 bits] sur la courbe P-256)
- Taille du nonce : 16 octets exactement
- Port UDP : 4500
- La valeur `Certification Auhtority` dans le payload CERTREQ doit être en SHA-2
- Révocation des certificats : CRL activée

2.2 Versions logicielles

Ce guide de configuration concerne les versions suivantes des clients VPN TheGreenBow :

- Client VPN Windows Enterprise v7.4,
- Client VPN Android v6.4,
- Client VPN macOS v2.4.

Les exemples de configuration fournis sont basés sur la version 7.4 du Client VPN Windows Enterprise.

Pour le Client VPN Android, il est recommandé de réaliser la configuration à l'aide du client Windows, puis de l'importer dans le client Android.

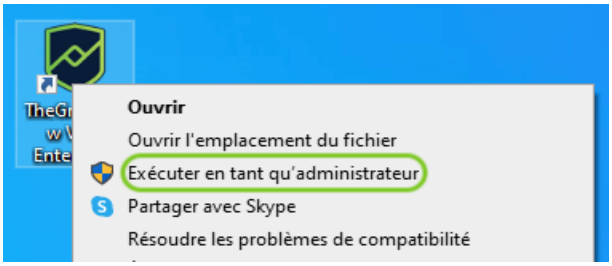
Pour le Client VPN macOS, les écrans se présentent essentiellement de la même manière que pour Windows. En cas de différences importantes, celles-ci sont signalées dans un encadré d'information comme celui-ci.

Retrouvez la documentation complète de ces produits sur le site de TheGreenBow à l'adresse : https://www.thegreenbow.com/fr/support/documentation-produits/.

2.3 Lancement du Client VPN

Le cas échéant, assurez-vous d'avoir lancé le Client VPN TheGreenBow avec les droits d'administration, afin de pouvoir accéder à son **Panneau de Configuration**.

Par exemple, pour le Client VPN Windows Enterprise, cliquez sur l'icône **TheGreenBow VPN Enterprise** avec le bouton droit de la souris, puis sélectionnez l'option de menu **Exécuter en tant qu'administrateur**.



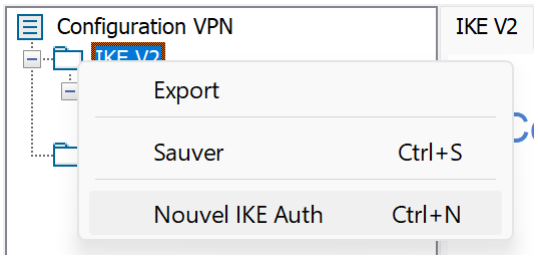
Pour le Client VPN macOS, il suffit de lancer l'application. L'accès au **Panneau de Configuration** n'est pas protégé comme pour le Client VPN Windows Enterprise.

2.4 Création d'un nouvel IKE Auth

Les négociations IKE permettant d'établir un canal sécurisé sur lequel deux parties peuvent communiquer sont appelées authentification IKE, ou « IKE Auth ».

Pour mettre en place cet échange de négociation, configurez le Client VPN TheGreenBow tel que décrit ci-dessous.

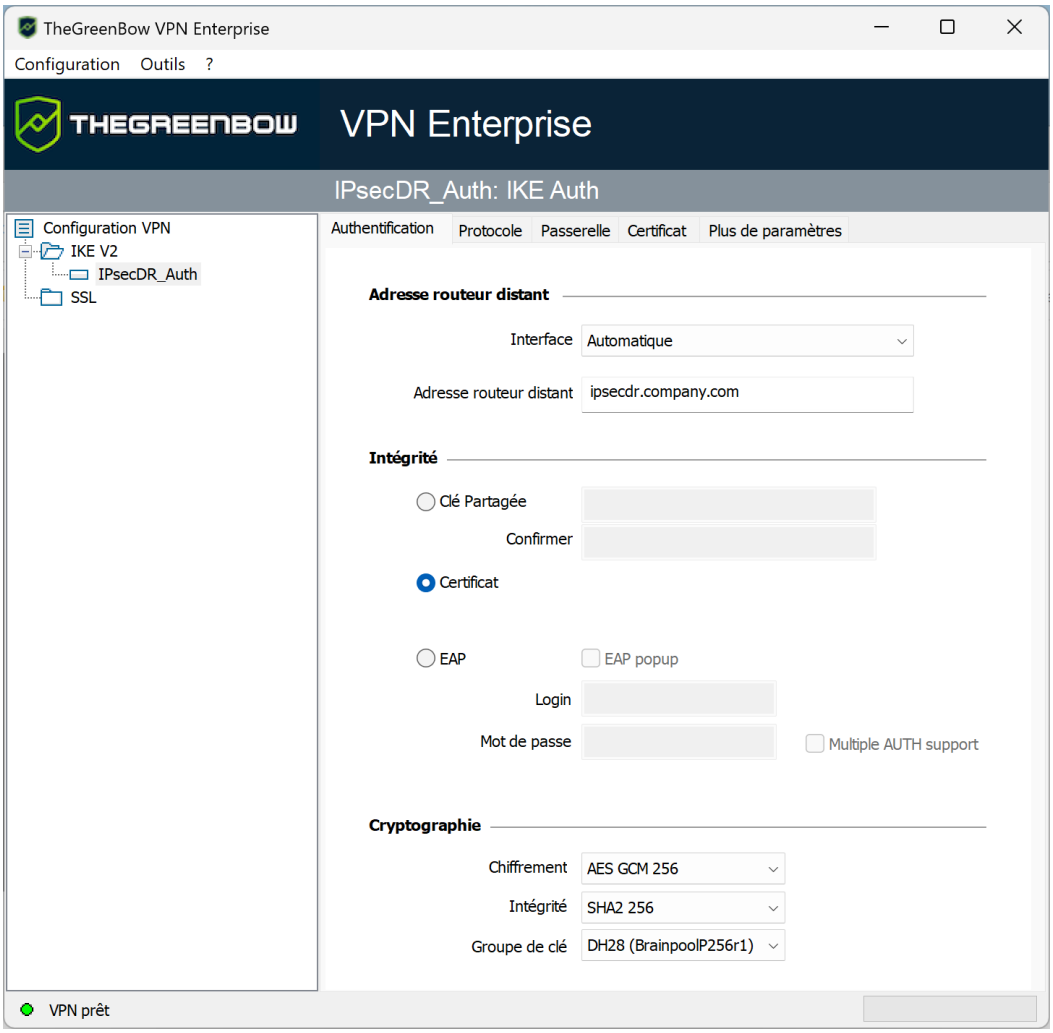
Commencez par créer un nouvel IKE Auth IKEv2. Pour cela, cliquez avec le bouton droit de la souris sur la branche **IKE V2** dans l'arborescence de la configuration VPN, puis sélectionnez **Nouvel IKE Auth**.



2.4.1 Onglet Authentification

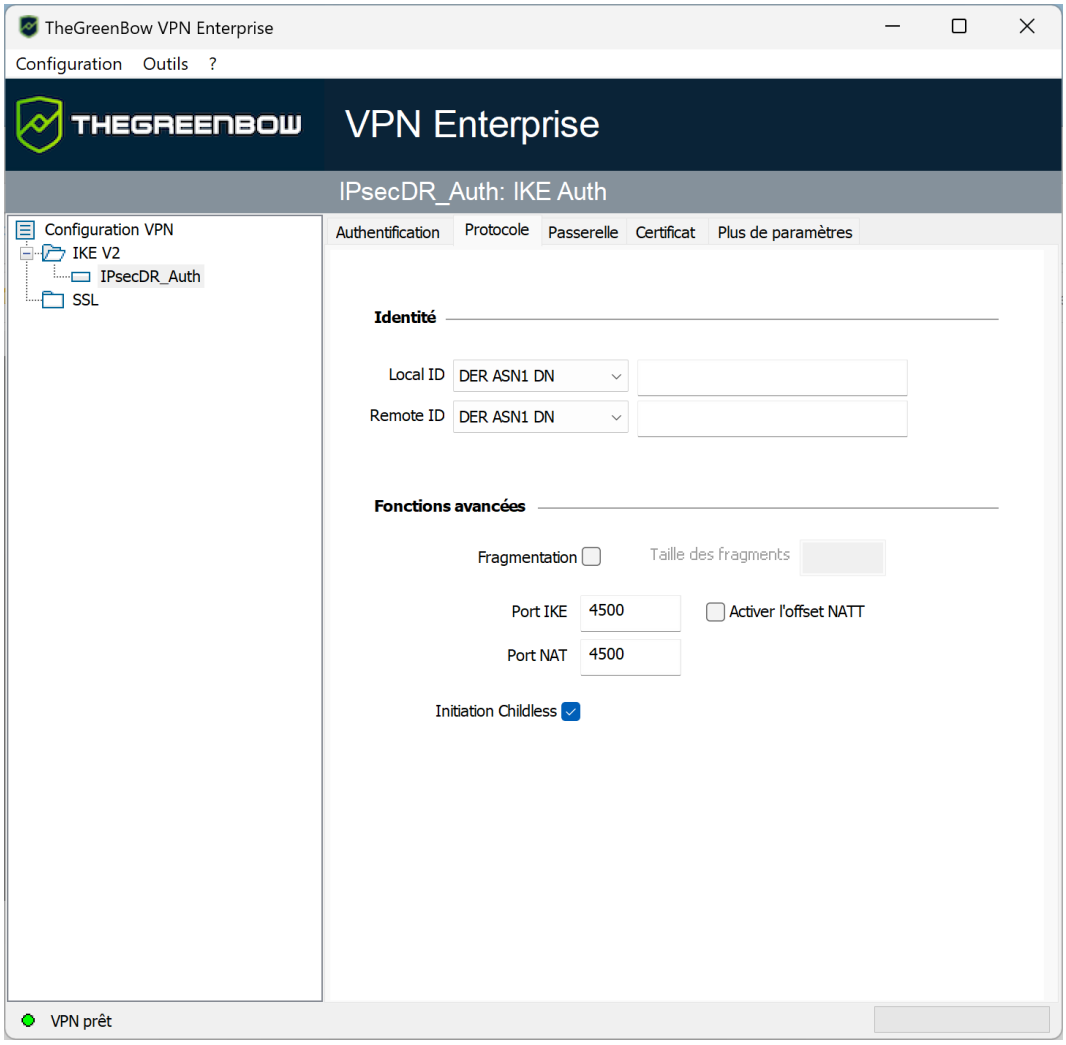
Sélectionnez l'onglet **Authentification**, puis configurez les paramètres suivants :

- Interface : Automatique
- Adresse routeur distant : l'adresse de la passerelle sur votre réseau
- Intégrité : Certificat
- Cryptographie :
  - Chiffrement : AES GCM 256
  - Intégrité : SHA2 256
  - Groupe de clé : DH28 (BrainpoolP256r1)



2.4.2 Onglet Protocole

Configurez les paramètres complémentaires suivants dans l'onglet **Protocole** :



Le **Local ID** `DER ASN1 DN` sera automatiquement mis à jour avec l'objet du certificat importé (voir ci-dessous).

Le **Remote ID** doit être de type `DER ASN1 DN` et contenir la même valeur que le champ **Local ID** de la passerelle, par exemple :

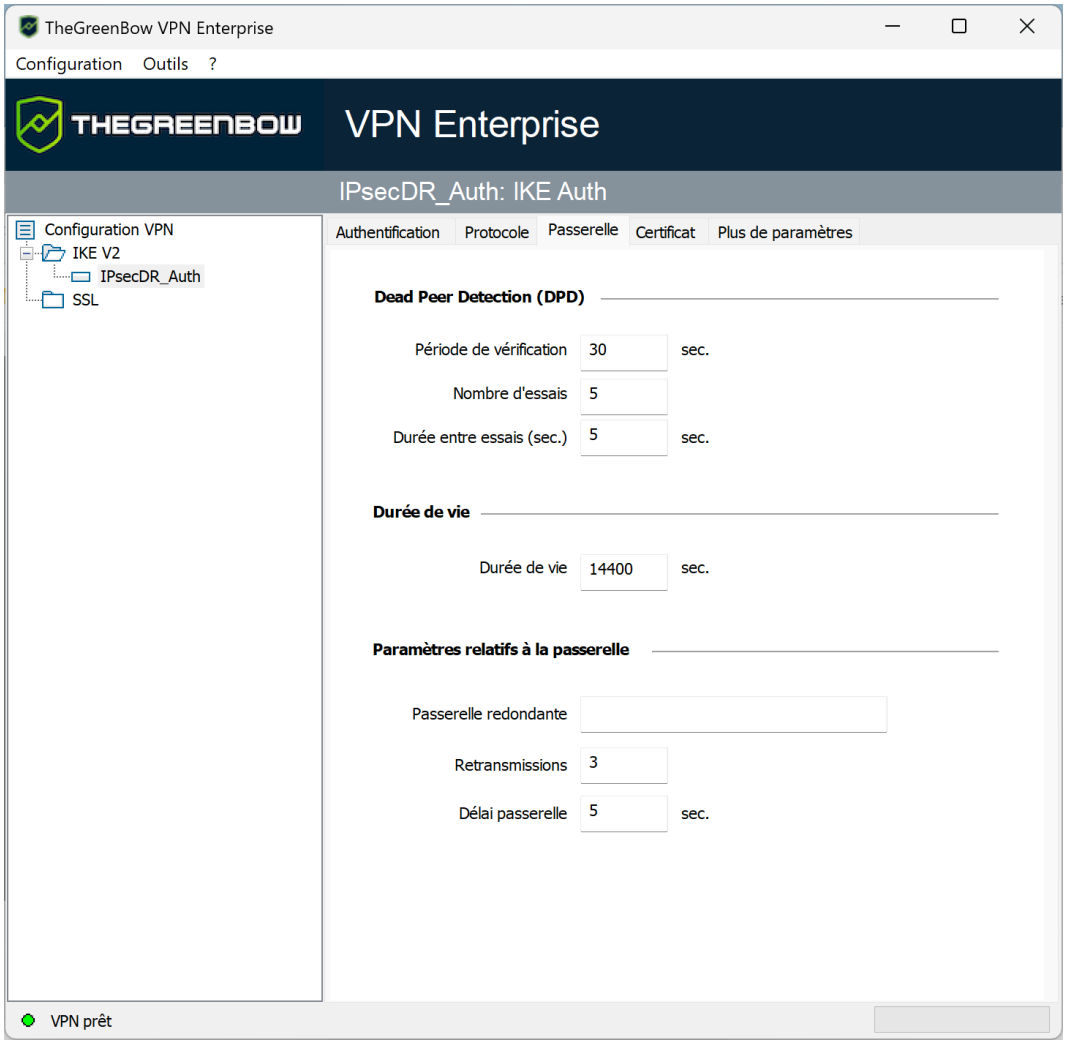
```
C=FR,ST=Ile-De-
France,L=Paris,O=TheGreenBow,OU=CXP,CN=firewallecdsa.cxp
```

Sous les **Fonctions avancées**, configurez les paramètres suivants :

- Port IKE : 4500
- Port NAT : 4500
- Initiation Childless : coché

2.4.3 Onglet Passerelle

Vous pouvez conserver les réglages par défaut de l'onglet **Passerelle** ou les modifier en fonction de vos besoins.

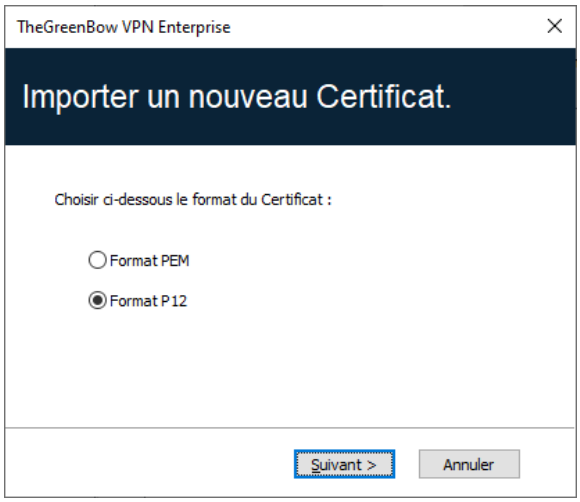


Il est recommandé de configurer dans le Client VPN une valeur de **Durée de vie** inférieure à celle configurée au niveau de la passerelle, afin que les renégociations soient initiées par le Client VPN (p. ex. 14400 dans le Client VPN et 28800 dans la passerelle.

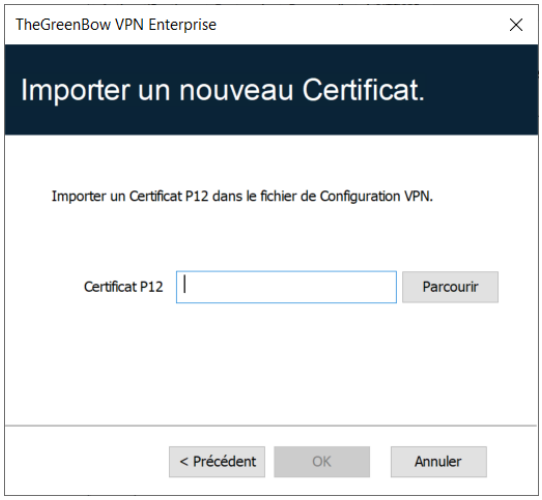
2.4.4 Onglet Certificat

Pour importer le certificat utilisateur, procédez comme suit :

1. Sélectionnez l'onglet **Certificat**.
2. Cliquez sur **Importer un Certificat...**.

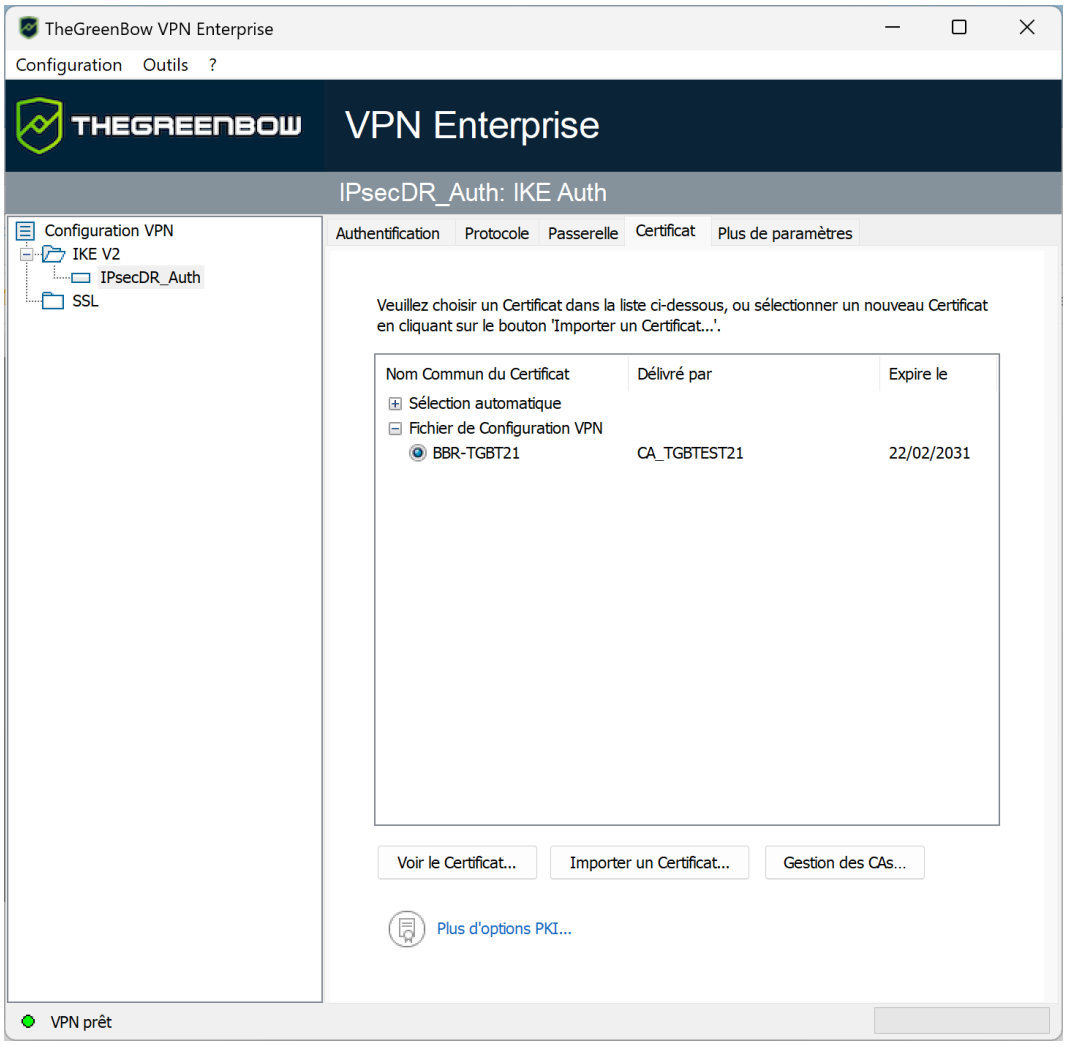


3. Choisissez **Format P12**.
4. Cliquez sur **Suivant >**.



5. Cliquez sur **Parcourir**.
6. Sélectionnez le certificat généré à partir de la passerelle.
7. Saisissez le mot de passe lorsque vous y êtes invité.
8. Cliquez sur **OK** pour valider.

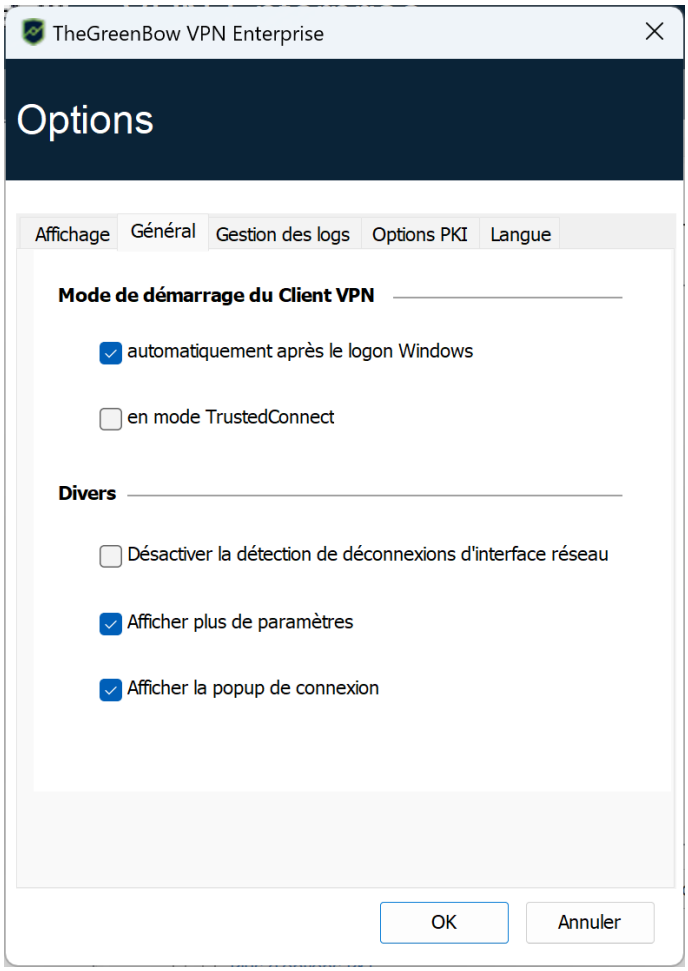
Vous devriez désormais voir un écran qui ressemble à celui-ci-dessous :



2.4.5 Onglet Plus de paramètres

Pour afficher l'onglet **Plus de paramètres**, dans le Client VPN Windows Enterprise, sélectionnez l'option de menu **Outils** > **Options**, puis l'onglet **Général** et cochez la case **Afficher plus de paramètres**.

Pour le Client VPN macOS, il n'est pas nécessaire d'activer d'option. L'onglet **Plus de paramètres** est disponible directement à partir de la branche du Child SA.



Sur l'onglet **Plus de paramètres**, ajoutez les paramètres dynamiques suivants :

- `NoNATTNegotiation` défini à la valeur `true` ;

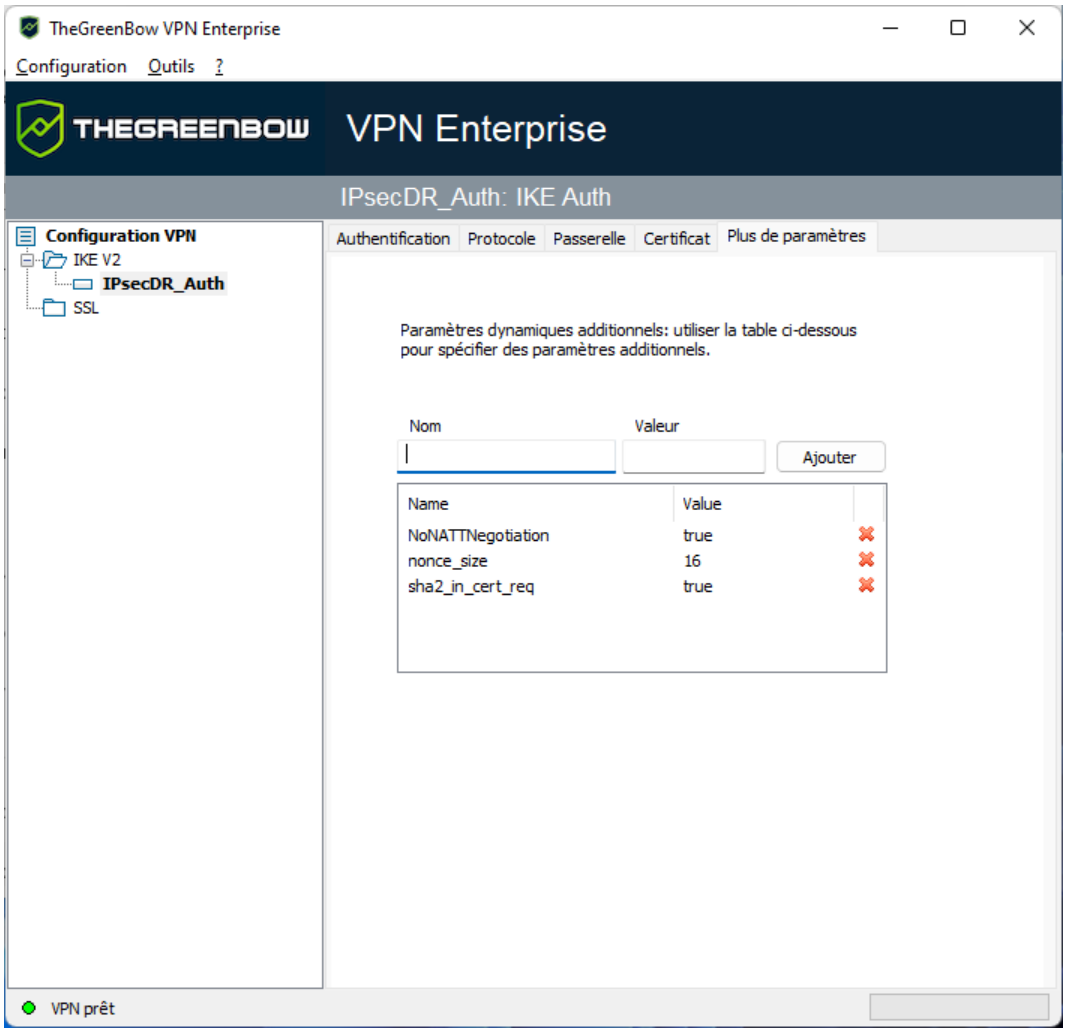
Ce paramètre empêche le Client VPN de négocier NAT-T avec la passerelle, ce qui est interdit en mode IPsec DR.

- `nonce_size` défini à la valeur 16 ;

Ce paramètre définit la taille du nonce à 16 octets exactement, ce qui est requis en mode IPsec DR.

- `sha2_in_cert_req` défini à la valeur `true`.

Ce paramètre définit la valeur `Certification Auhtority` dans la charge utile de demande de certificat (CERTREQ payload) sous la forme d'une liste concaténée de condensats SHA-2 des clés publiques des autorités de certification de confiance.

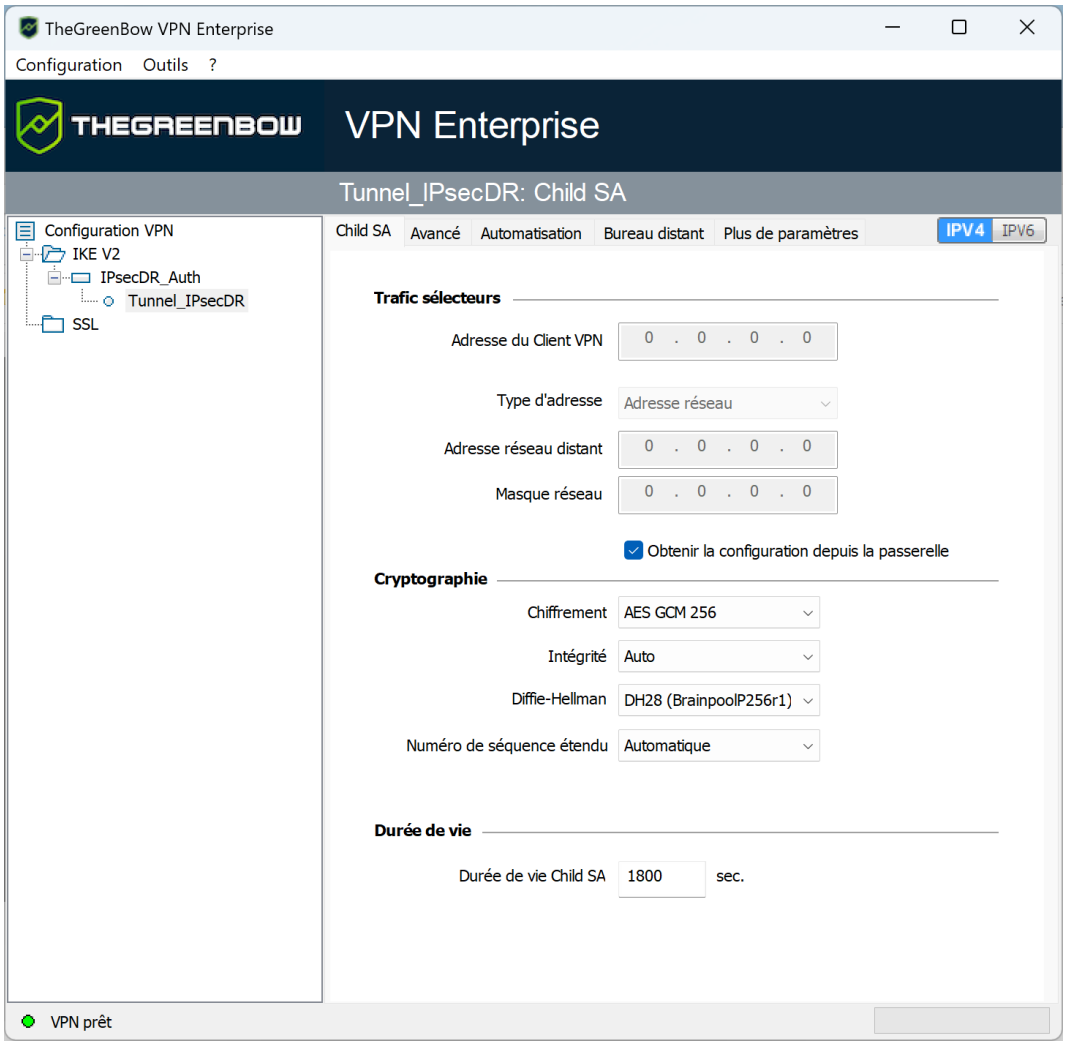


2.5 Création d'un nouveau Child SA

L'association de sécurité IPsec d'un tunnel VPN, également appelée « Child SA », sert à la négociation des paramètres de sécurité qui seront appliqués aux données transmises dans le tunnel VPN.

Pour configurer le Client VPN TheGreenBow pour un Child SA, commencez par créer un nouveau Child SA. Pour cela, cliquez avec le bouton droit de la souris sur la branche **Ikev2Gateway** que vous venez de créer dans l'arborescence de la configuration VPN, puis sélectionnez **Nouveau Child SA**.

Configurez ensuite les paramètres comme indiqué dans la capture d'écran ci-dessous :



1. Cochez **Obtenir la configuration depuis la passerelle**.
2. Sous **Cryptographie**, sélectionnez les valeurs suivantes :
   - Chiffrement : AES GCM 256
   - Intégrité : Auto
   - Diffie-Hellman : DH28 (BrainpoolP256r1)
   - Numéro de séquence étendu : Automatique
3. Sous **Durée de vie**, entrez `1800` dans le champ **Durée de vie Child SA**.

Il est recommandé de configurer dans le Client VPN une valeur de **Durée de vie** inférieure à celle configurée au niveau de la passerelle, afin que les renégociations soient initiées par le Client VPN.

2.6 Enregistrement de la configuration

Pour enregistrer la configuration, sélectionnez l'option de menu **Configuration** > **Sauver**, afin de prendre en compte toutes les modifications que vous avez apportées à votre configuration VPN.

Si la configuration doit être utilisée avec le Client VPN Android, il conviendra en outre de l'exporter depuis le Client VPN Windows ou macOS, puis de l'importer dans le Client VPN Android. Consultez les sections idoines des produits concernés pour savoir comment procéder.

2.7 Ouverture de la connexion VPN

Dès lors que la passerelle et le Client VPN TheGreenBow ont été configurés comme décrit ci-dessus, vous pouvez ouvrir des connexions VPN.

Pour savoir comment ouvrir une connexion VPN dans votre Client VPN TheGreenBow, reportez-vous à la documentation du produit concerné.

Généralement, une icône verte s'affiche à côté du Child SA lorsque l'établissement de la connexion a réussi.

3 Dépannage

Si vous n'arrivez pas à établir la connexion VPN, vérifiez le journal (*log*) de la **Console** du Client VPN TheGreenBow afin de déterminer si l'un des messages indiqués correspond à l'un de ceux décrits dans les sections suivantes.

3.1 Passerelle

Pour dépanner les problèmes liés à la passerelle, reportez-vous au guide de configuration spécifique du produit concerné.

☞ Vous trouverez une liste des passerelles compatibles avec les Clients VPN TheGreenBow ainsi que les guides de configuration correspondants sur notre site à l'adresse : https://www.thegreenbow.com/fr/support/guides-dintegration/passerelles-vpn-compatibles/.

La passerelle Stormshield SNS v4.2 est actuellement la seule de cette liste à mettre en œuvre un mode IPsec DR.

3.2 Client VPN TheGreenBow

3.2.1 NO_PROPOSAL_CHOSEN

Si vous rencontrez une erreur de type `NO_PROPOSAL_CHOSEN`, il se peut que vous n'ayez pas configuré correctement la Phase 1 [IKE Auth]. Assurez-vous que les algorithmes de chiffrement sont identiques aux deux extrémités de la connexion VPN.

```
20XX0913 16:08:53:387 TIKEV2_Tunnel SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)]
[KE][VID][N(FRAGMENTATION_SUPPORTED)]
20XX0913 16:08:53:419 TIKEV2_Tunnel RECV IKE_SA_INIT
[HDR][N(NO_PROPOSAL_CHOSEN)]
```

3.2.2 AUTHENTICATION_FAILED

Si vous rencontrez une erreur de type `AUTHENTICATION_FAILED`, cela signifie que le certificat envoyé par le Client VPN ne correspond pas à ce qui est attendu par la passerelle. Assurez-vous que le certificat utilisateur du Client VPN est correctement configuré sur la passerelle.

```
20XX0913 16:15:22:032 TIKEV2_Tunnel RECV IKE_AUTH
[HDR][N(AUTHENTICATION_FAILED)]
20XX0913 16:15:22:032 TIKEV2_Tunnel Remote endpoint sends error
AUTHENTICATION_FAILED
```

3.2.3 No user certificate available for the connection

Assurez-vous que le certificat utilisateur a été correctement importé dans le Client VPN.

```
20XX0913 16:18:07:491 TIKEV2_Tunnel RECV IKE_SA_INIT
[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_
IP)][CERTREQ][N(FRAGMENTATION_SUPPORTED)][N(MULTIPLE_AUTH_SUPPORTED)]
20XX0913 16:18:07:491 TIKEV2_Tunnel IKE SA I-SPI 8D4467C52C91C316 R-SPI
9DF0F0E4A91F8867
20XX0913 16:18:07:491 TIKEV2_Tunnel No user certificate available for the
connexion
20XX0913 16:18:07:491 TIKEV2_Tunnel Connection aborted.
```

3.2.4 Remote IDr rejected

Le type ou la valeur du `Remote ID` envoyé par la passerelle ne correspond pas à ce qui est attendu par le Client VPN (voir section 2.4.2 Onglet Protocole). Configurez le type et la valeur du **Remote ID** dans le Client VPN en fonction du **Local ID** de la passerelle.

```
20180913 16:24:32:087 TIKEV2_Tunnel ID types do not match. Expecting
ID_RFC822_ADDR. Receiving ID_DER_ASN1_DN
20180913 16:24:32:087 TIKEV2_Tunnel Remote IDr rejected
```

3.2.5 FAILED_CP_REQUIRED

Si vous rencontrez une erreur de type `FAILED_CP_REQUIRED`, cela signifie que la passerelle est configurée pour utiliser le mode CP (Configuration Payload), mais pas le Client VPN. Dans ce cas, dans l'onglet **Child SA** sous **Trafic sélecteurs**, cochez la case **Obtenir la configuration depuis la passerelle** (voir section 2.5 Création d'un nouveau Child SA).

```
20XX0913 16:29:46:780 TIKEV2_Tunnel RECV IKE_AUTH
[HDR][IDr][CERT][AUTH][N(AUTH_LIFETIME)][N(FAILED_CP_REQUIRED)][N(TS_UNACCEPT
ABLE)]
20180913 16:29:46:780 TIKEV2_Tunnel Remote endpoint sends error
FAILED_CP_REQUIRED
20XX0913 16:29:46:780 TIKEV2_Tunnel Remote endpoint is expecting a
configuration request from the client
```

4 Contact

4.1 Information

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

4.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

4.3 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/.

Vos connexions protégées
en toutes circonstances

28, rue Auber
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com