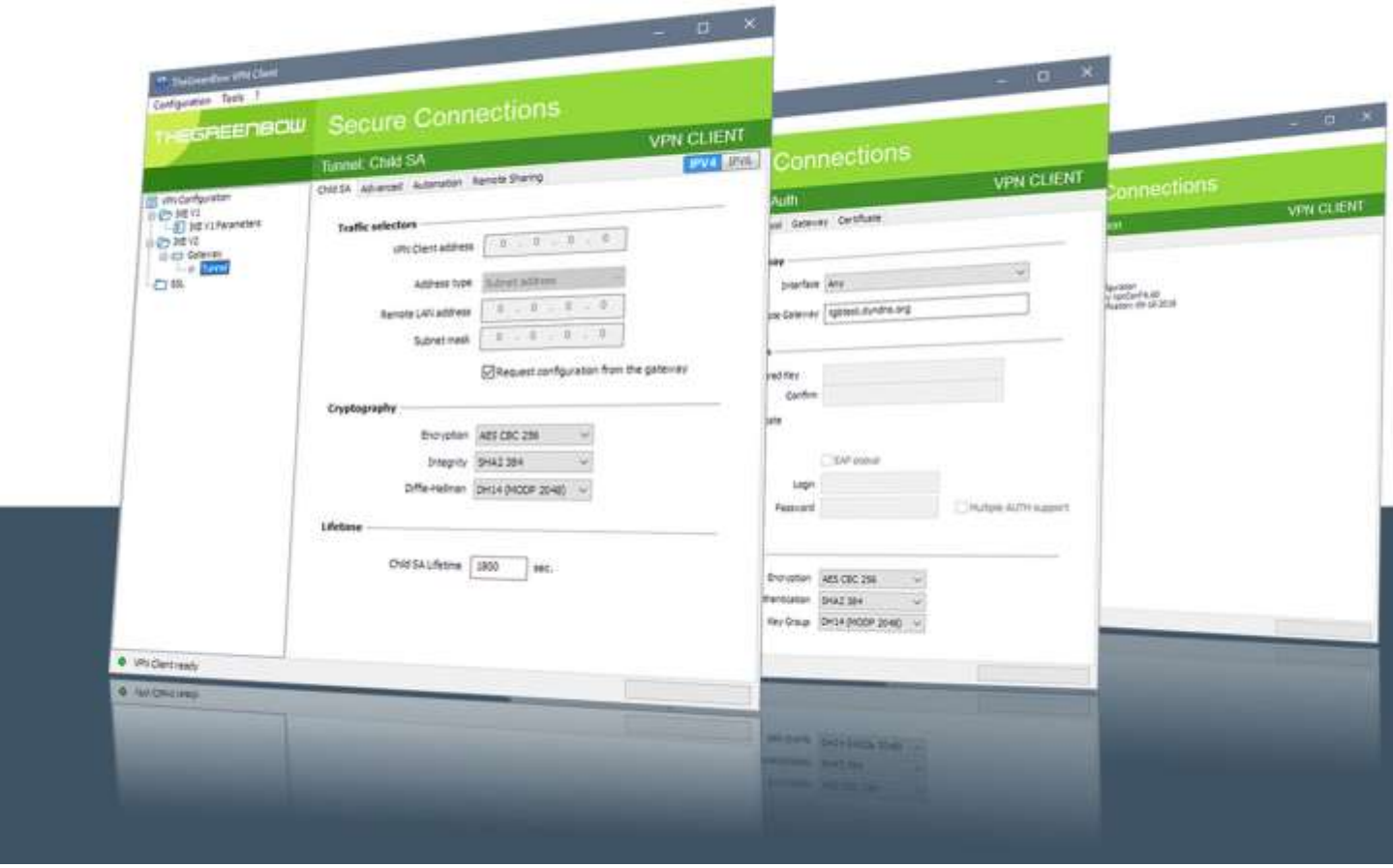


TheGreenBow IPsec VPN Client

Guide de Configuration Dynfi

Protocole - IKEv2

Site Internet : **www.thegreenbow.com**
Contact: **support@thegreenbow.com**

Table des matières

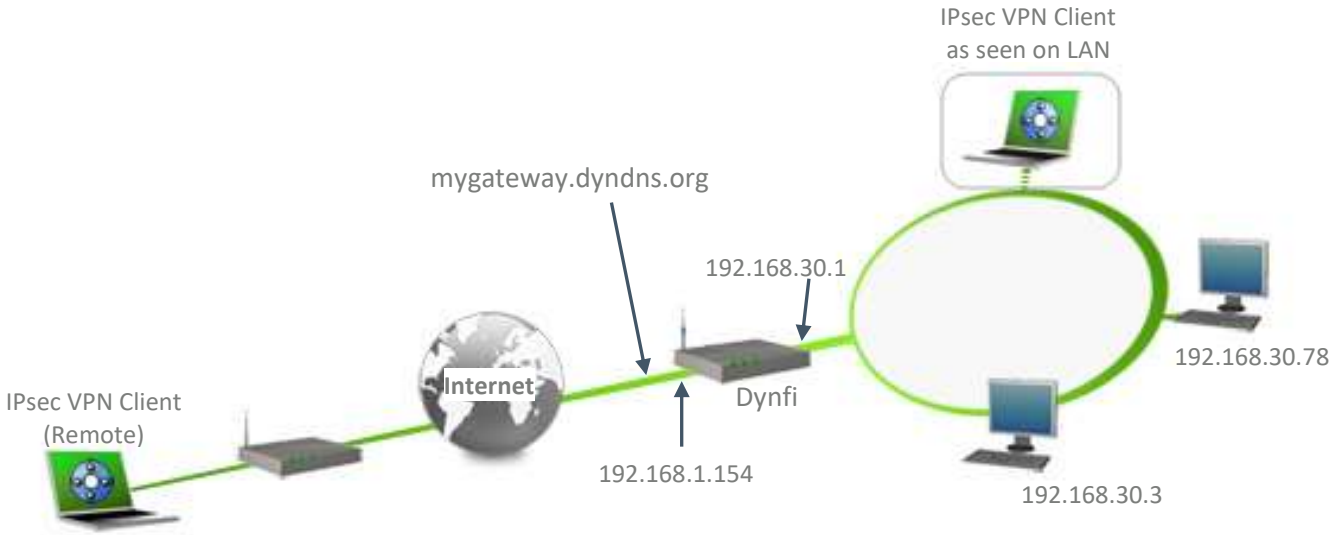
1 Introduction

1.1 But de ce document

Ce document décrit la configuration du Client VPN IPsec TheGreenBow avec un routeur Dynfi pour établir des connexions VPN pour l'accès à distance au réseau de l'entreprise.

1.2 Description de l'environnement réseau

Dans notre document, nous décrirons un exemple de connexion entre le client TheGreenBow VPN et le réseau local se trouvant derrière le routeur Dynfi. Le client VPN est connecté à l'Internet par son FAI. Dans le réseau local, le client utilisera une adresse IP virtuelle. Toutes les adresses dans ce document sont données à titre d'exemple.



1.3 Restrictions du Dynfi

Pas de restrictions connues.

1.4 Le routeur Dynfi

Nos tests et configuration VPN ont été réalisés avec un routeur Dynfi 20.0.

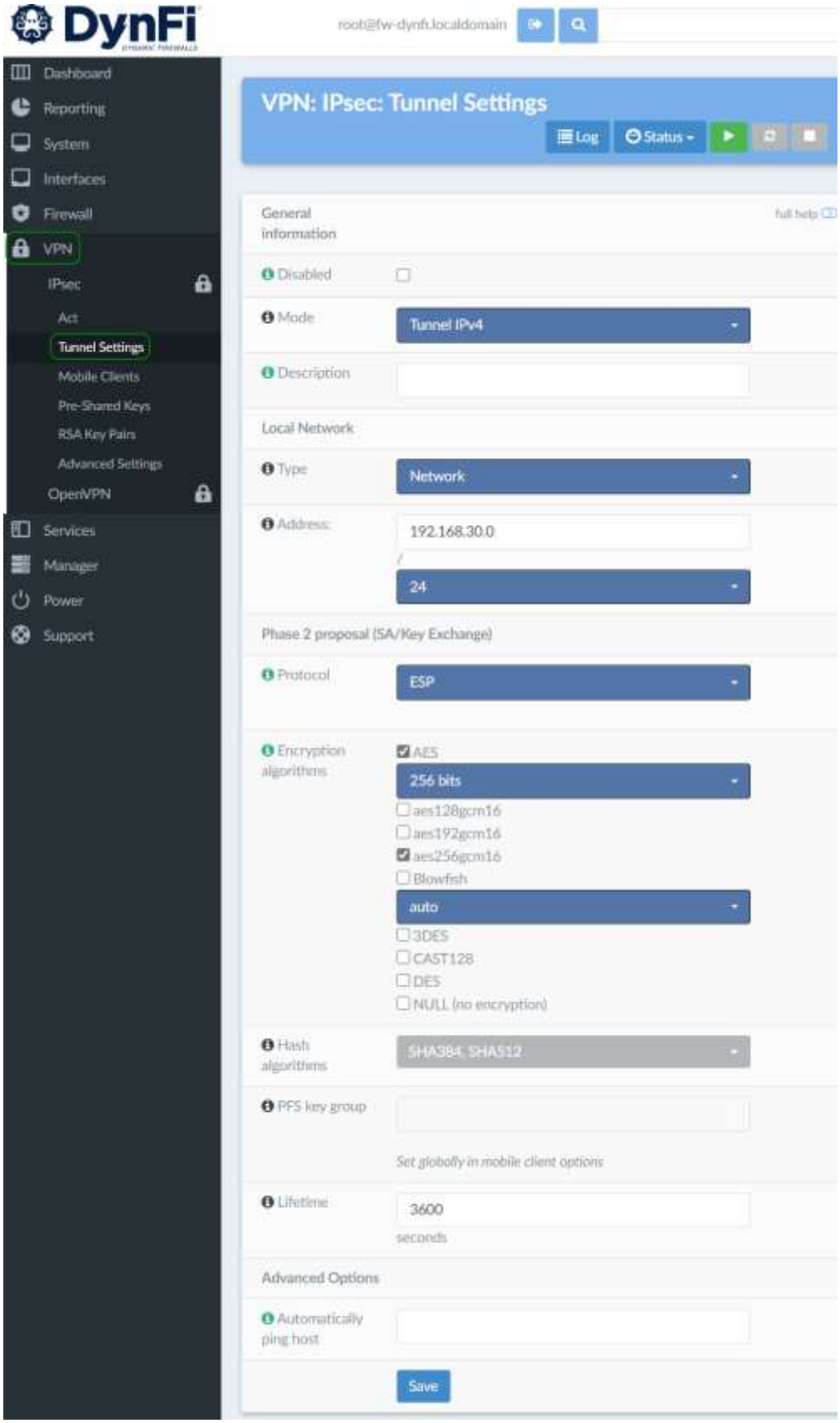
1.5 Information produit du routeur Dynfi

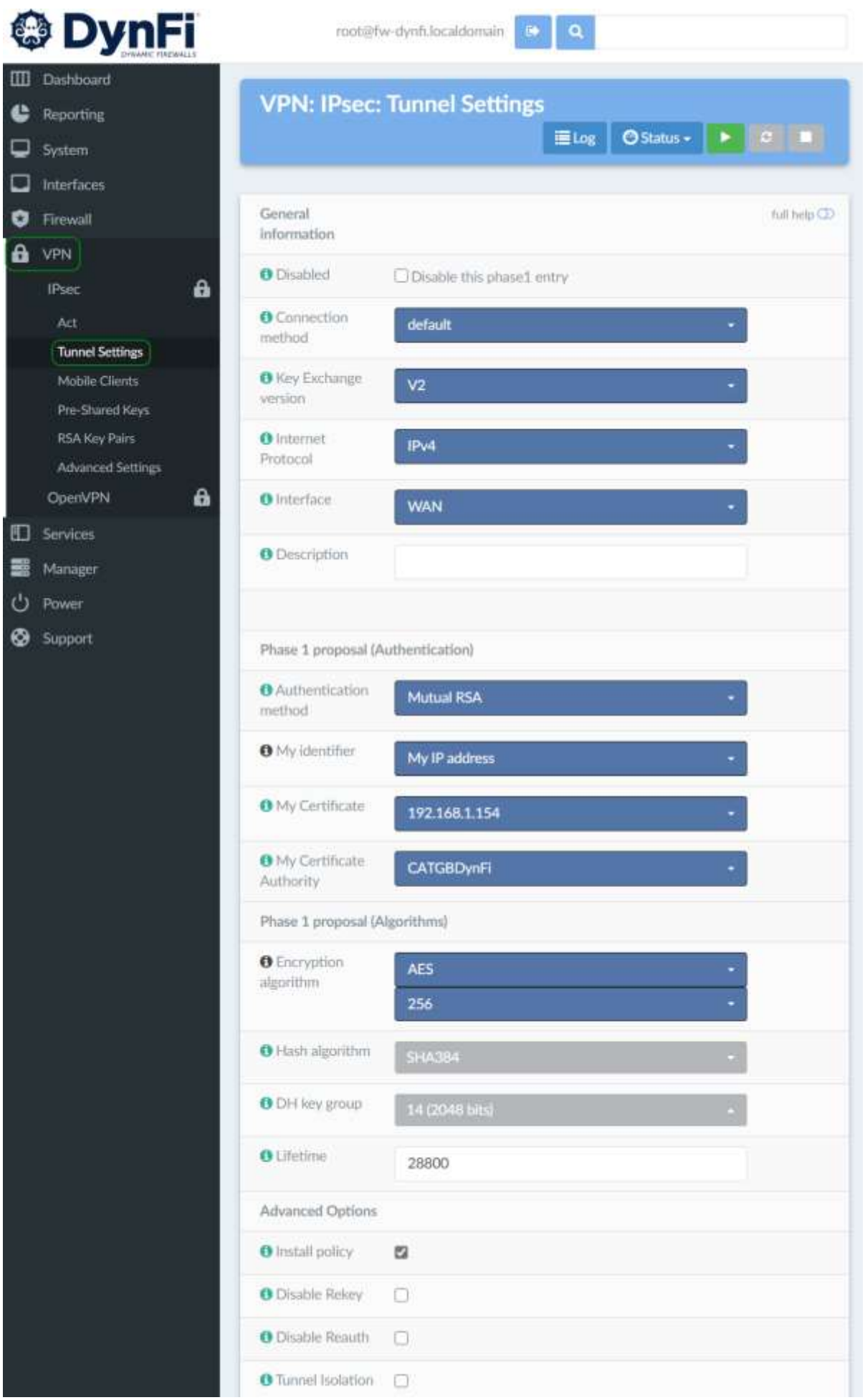
Il est important que les utilisateurs trouvent toutes les informations nécessaires concernant le routeur Dynfi. Toutes les informations produit, guide utilisateur et base de connaissance peuvent être trouvées sur le site Internet : **https://dynfi.com/documentation/**

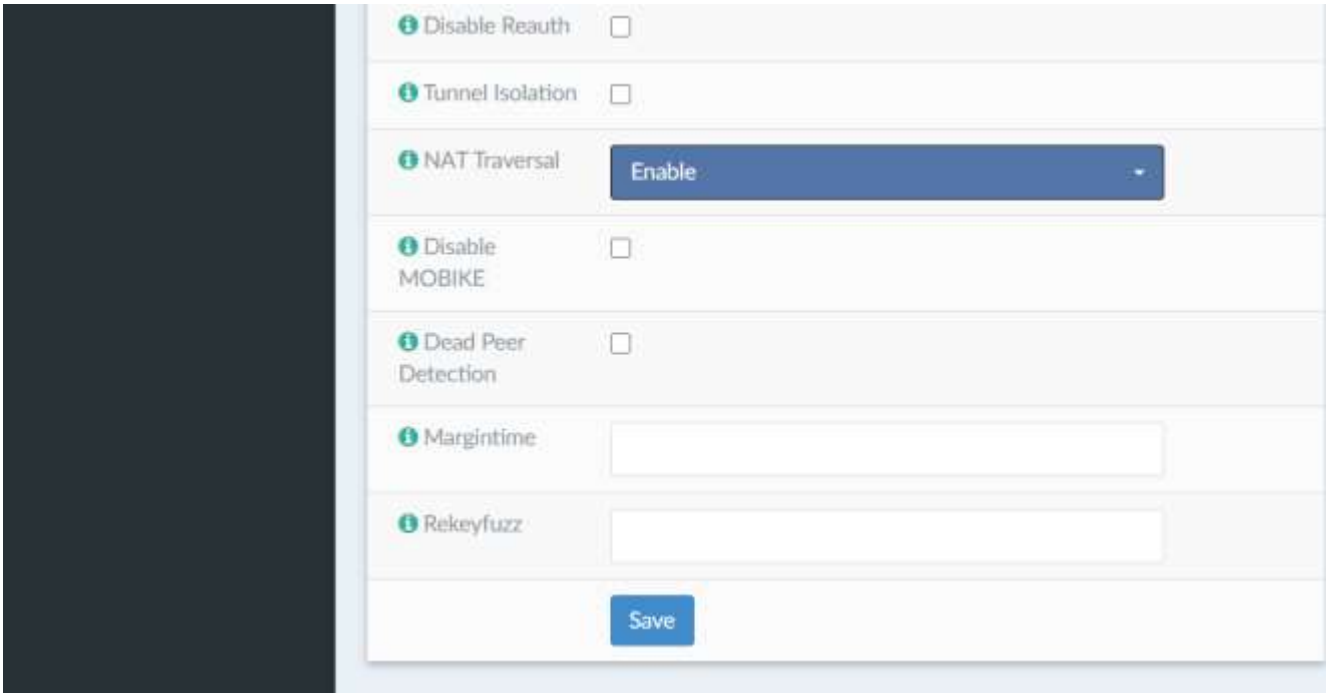
Page produit Dynfi	**https://dynfi.com/fr**
Guide utilisateur Dynfi	**https://dynfi.com/documentation/**
FAQ Dynfi	**https://dynfi.com/fr/faq**

2 Dynfi configuration

Cette section décrit la configuration VPN de votre routeur Dynfi.
Une fois connecté à votre routeur Dynfi, cliquer sur le menu “VPN > Tunnel Settings” puis configurer le routeur comme suit :

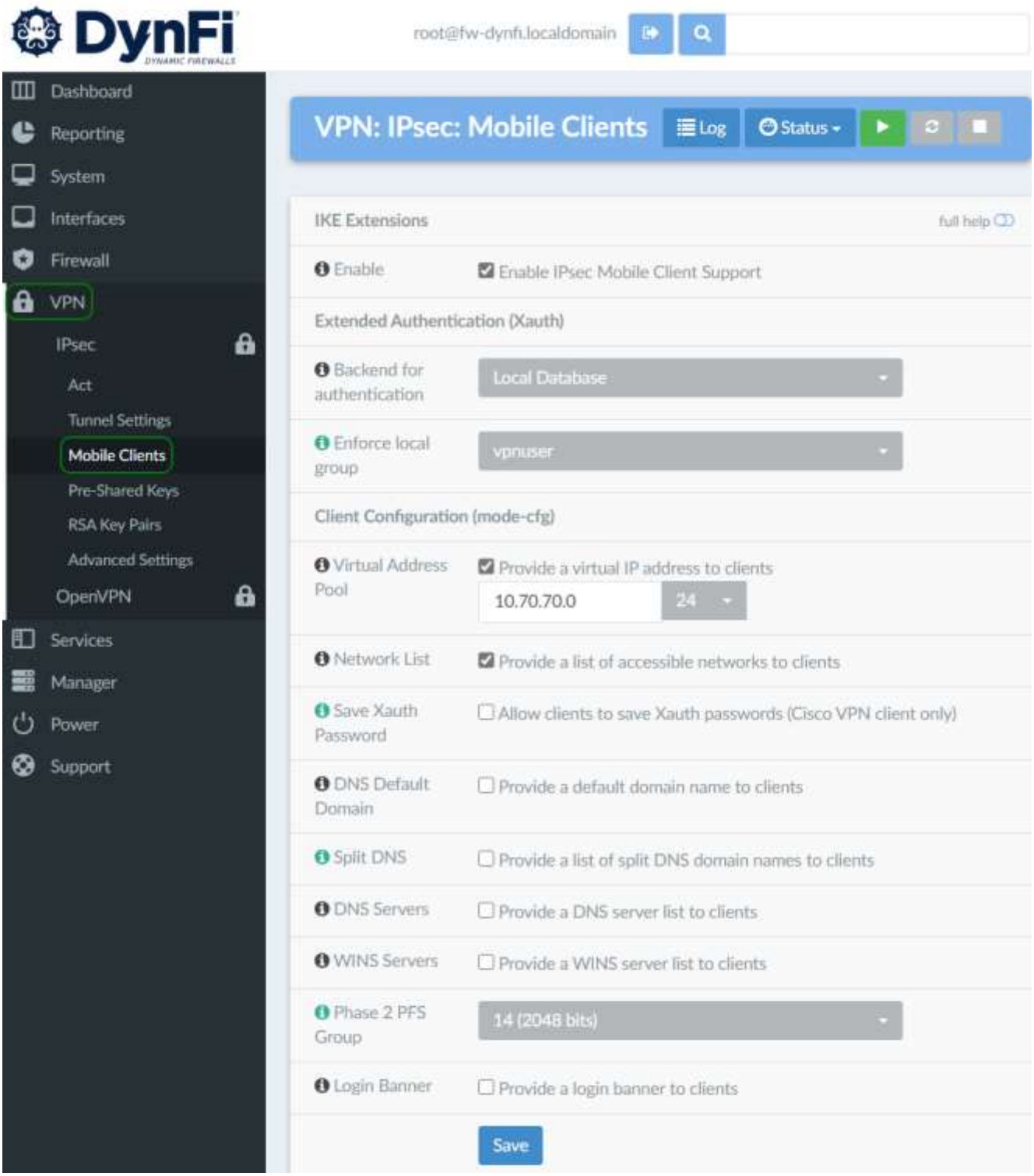






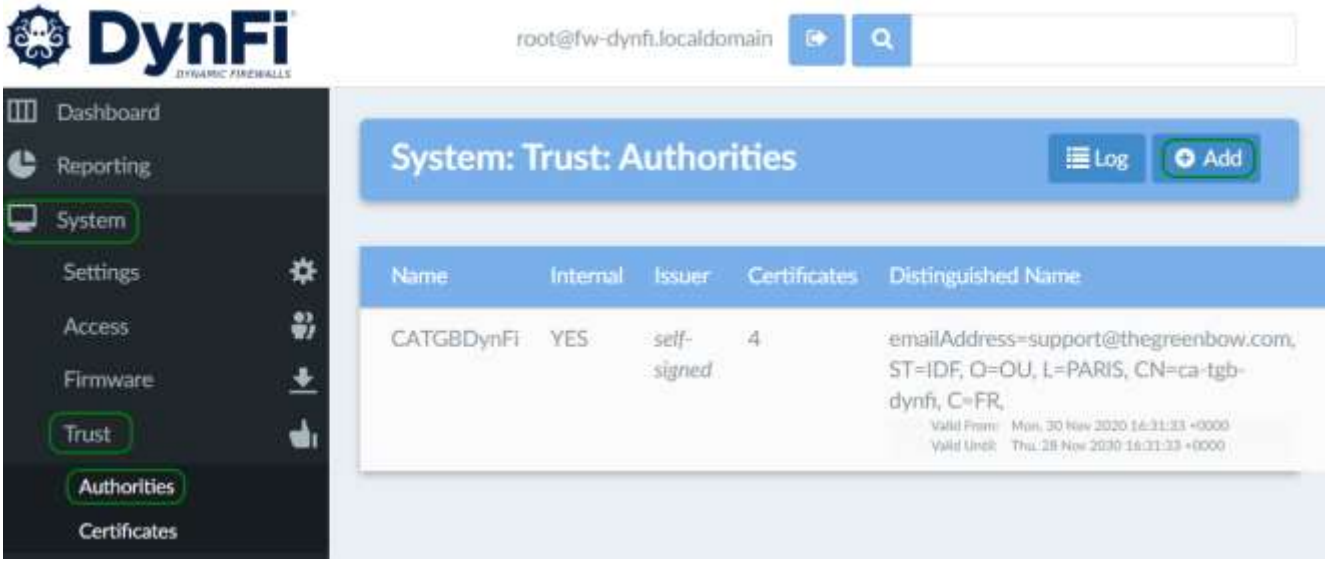
Valider le configuration en cliqant sur le bouton “Save”.

Cliquer ensuite sur le menu “Mobile Clients”

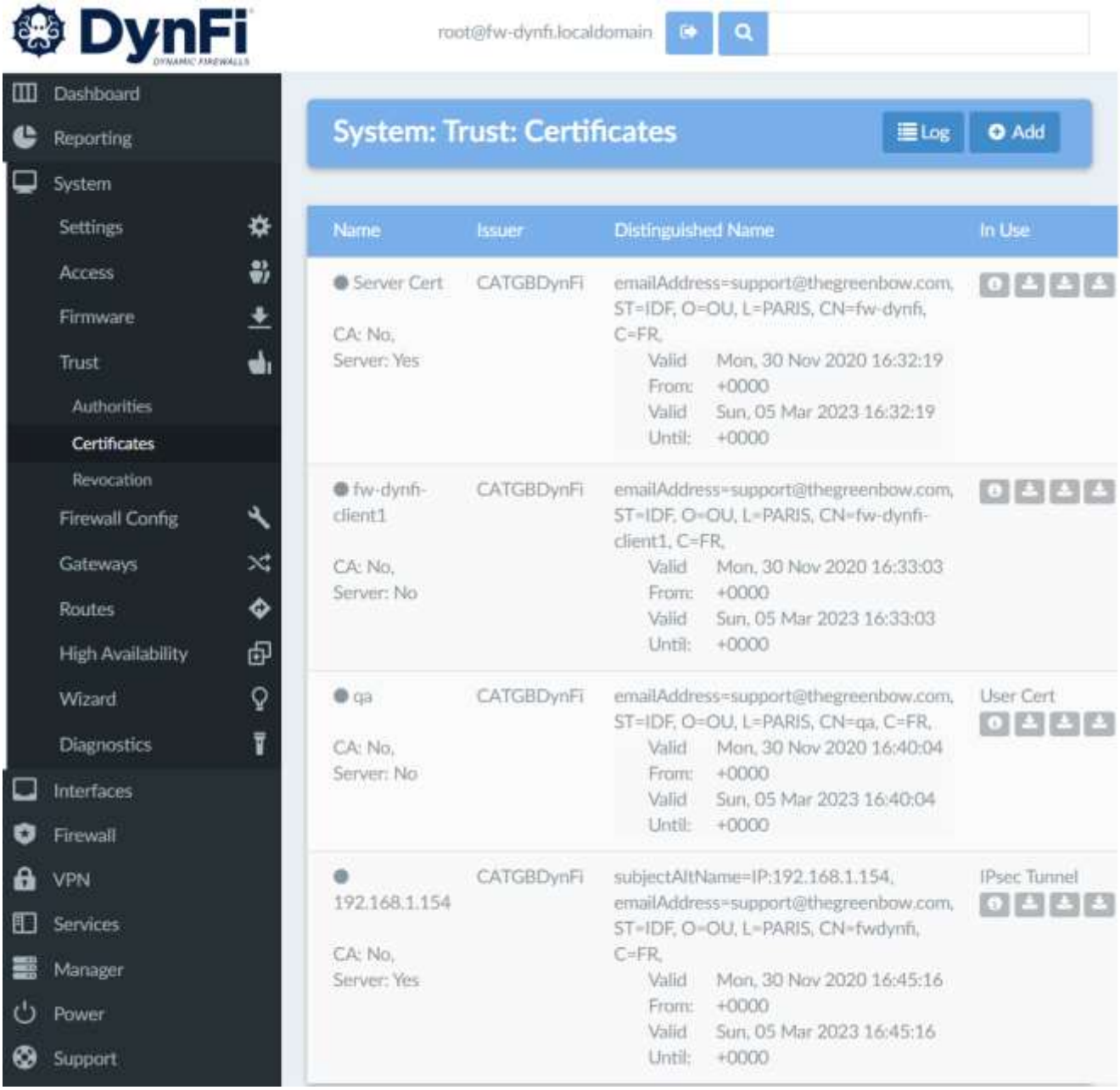


Valider le configuration en cliqant sur le bouton “Save”.

Cliquer maintenant sur le menu “System > Trust > Authorities” pour importer les certificats. Cliquer sur le bouton “Add”.



Il est possible d'importer plusieurs certificats



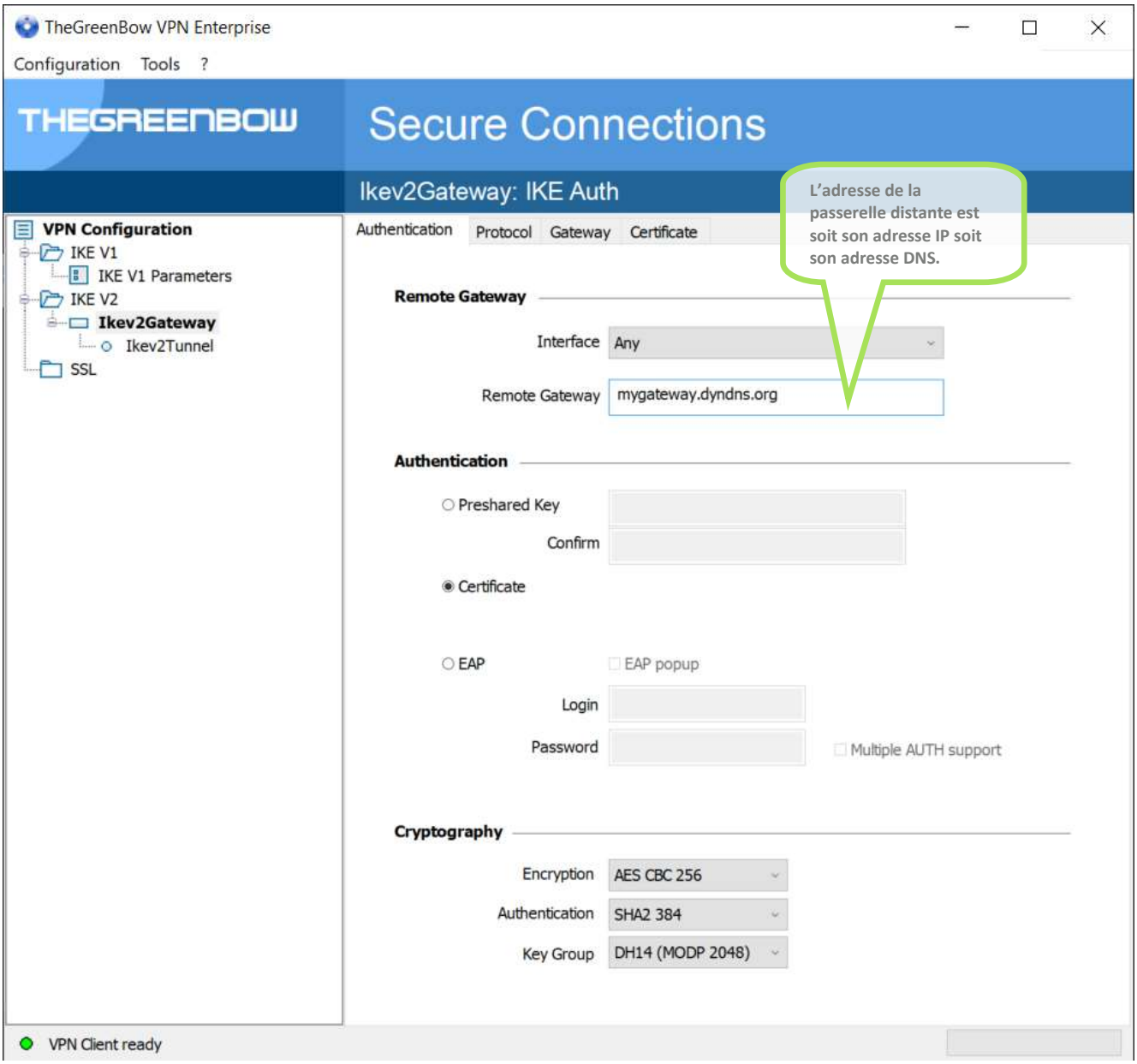
3 Configuration IPsec du client VPN TheGreenBow

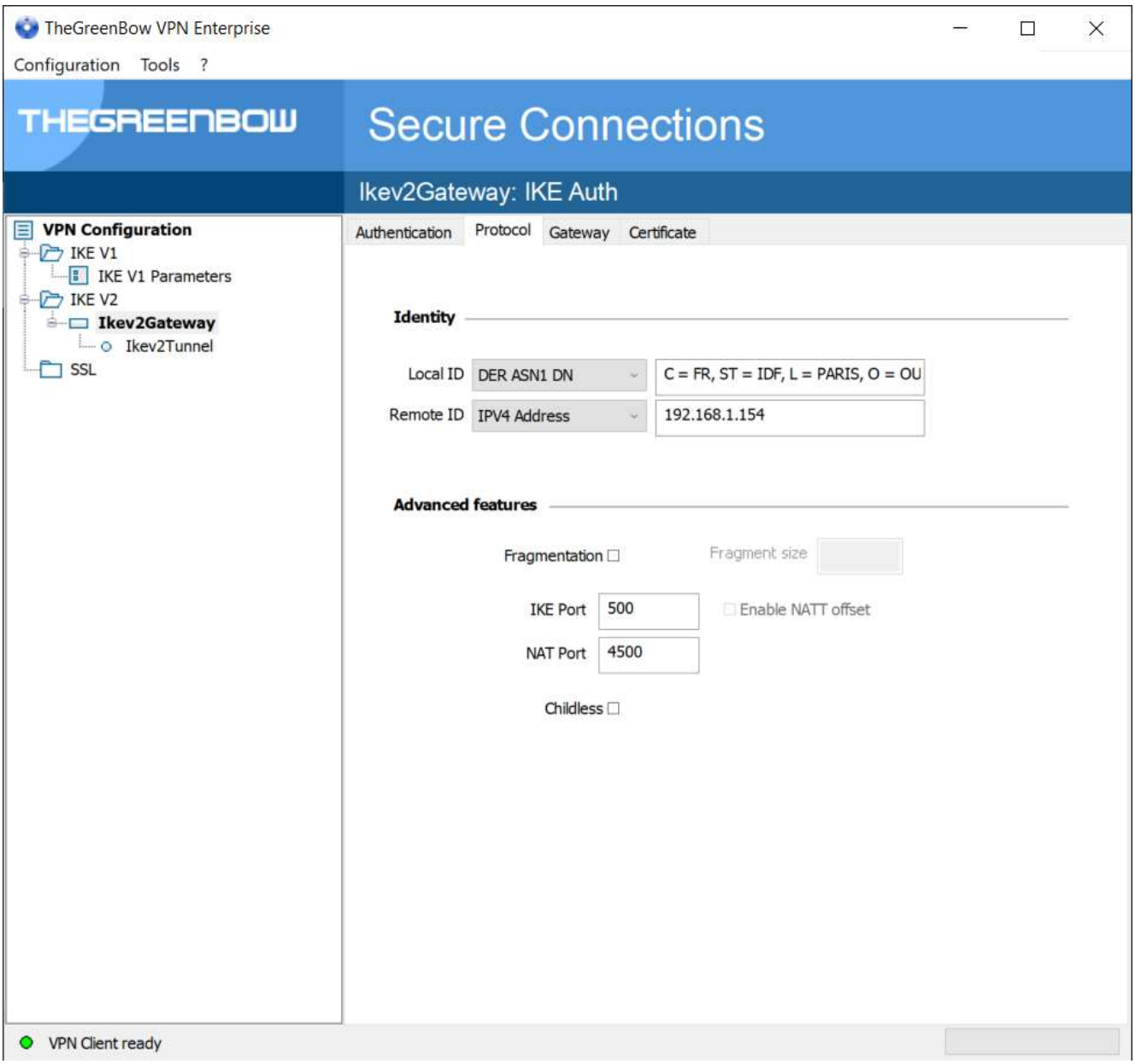
Cette section décrit la configuration requise pour se connecter au routeur Dynfi via une connexion VPN.
Pour télécharger la dernière version du client IPsec VPN TheGreenBow, aller sur le site : **http://www.thegreenbow.com/vpn_products.html**

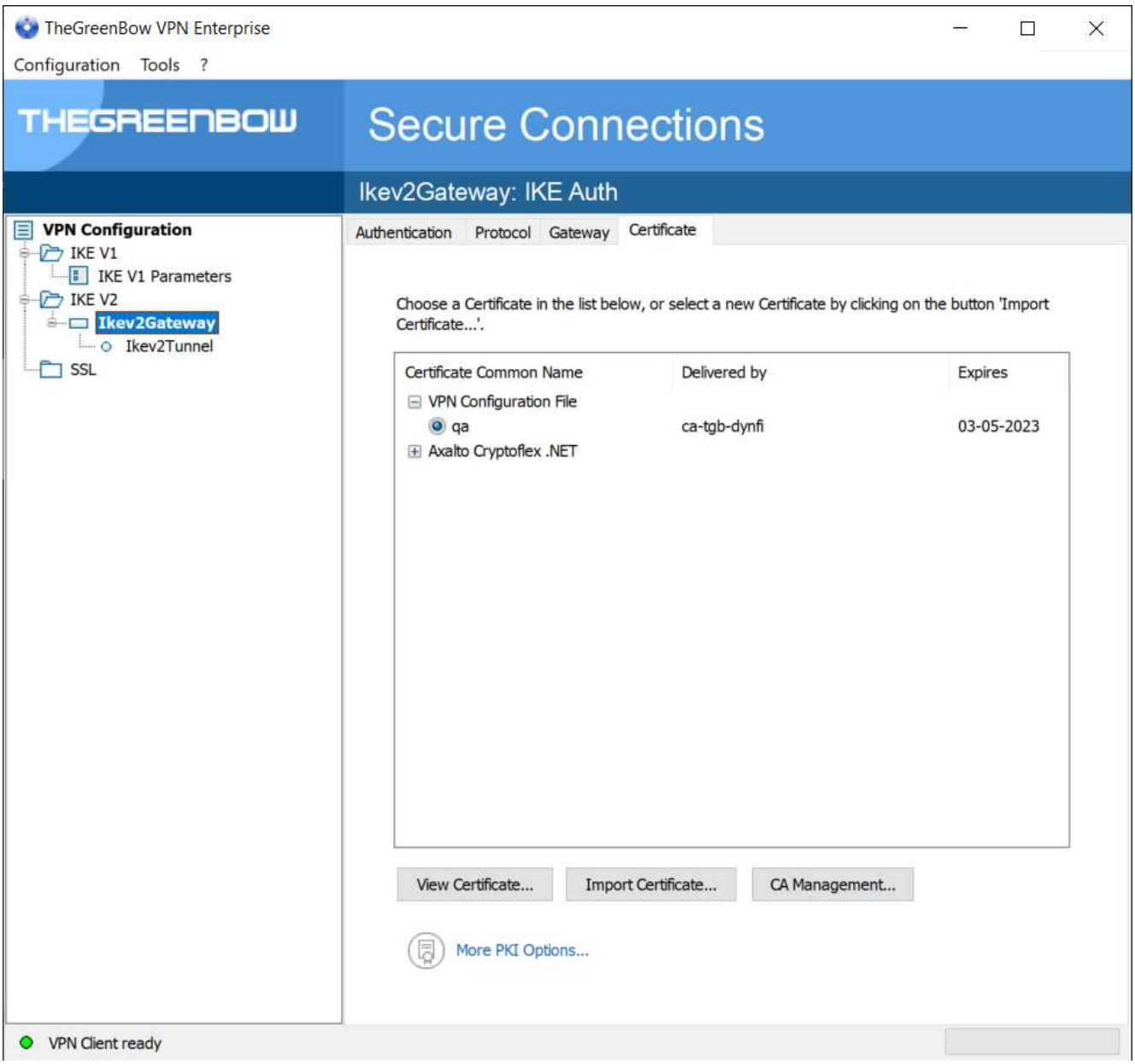
3.1 Configuration IKE Auth du client VPN TheGreenBow

La configuration des autres onglets est laissée par défaut.

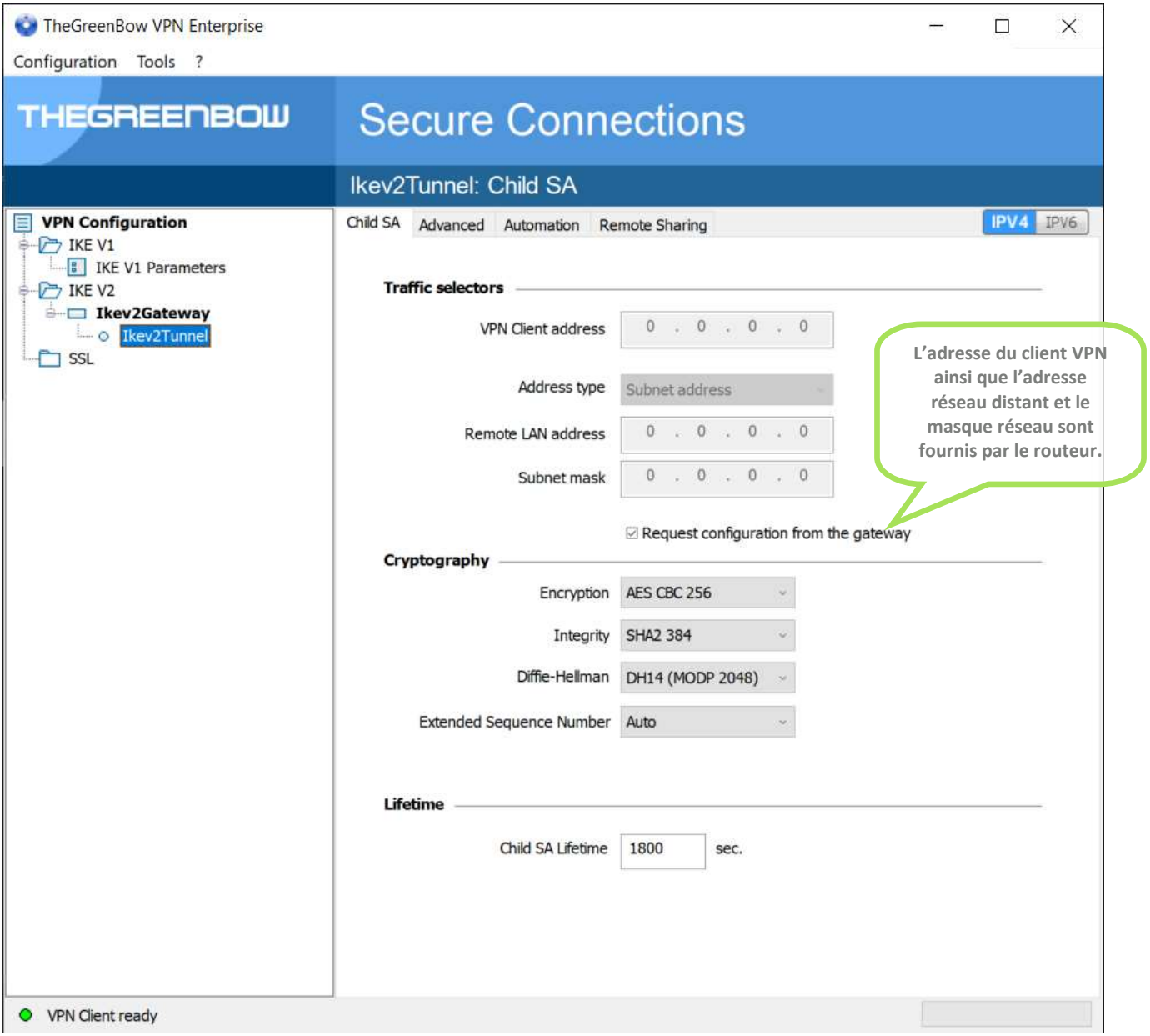
Cette configuration est un exemple de ce qui doit être renseigné pour l'authentification utilisateur. Vous pouvez vous référer au guide utilisateur du routeur Dynfi ou au guide utilisateur TheGreenBow IPsec VPN Client pour plus de détails sur l'authentification utilisateur.




TheGreenBow VPN Enterprise
Configuration
Tools
?
THEGREENBOW
Secure Connections
Ikev2Gateway: IKE Auth
VPN Configuration
IKE V1
IKE V1 Parameters
IKE V2
Ikev2Gateway
Ikev2Tunnel
SSL
Authentication
Protocol
Gateway
Certificate
Identity
Local ID
DER ASN1 DN
C = FR, ST = IDF, L = PARIS, O = OU
Remote ID
IPV4 Address
192.168.1.154
Advanced features
Fragmentation
Fragment size
IKE Port
500
Enable NATT offset
NAT Port
4500
Childless
VPN Client ready



3.2 Configuration VPN Client IPsec Phase 2 (Child SA)



La configuration des autres onglets est laissée par défaut.

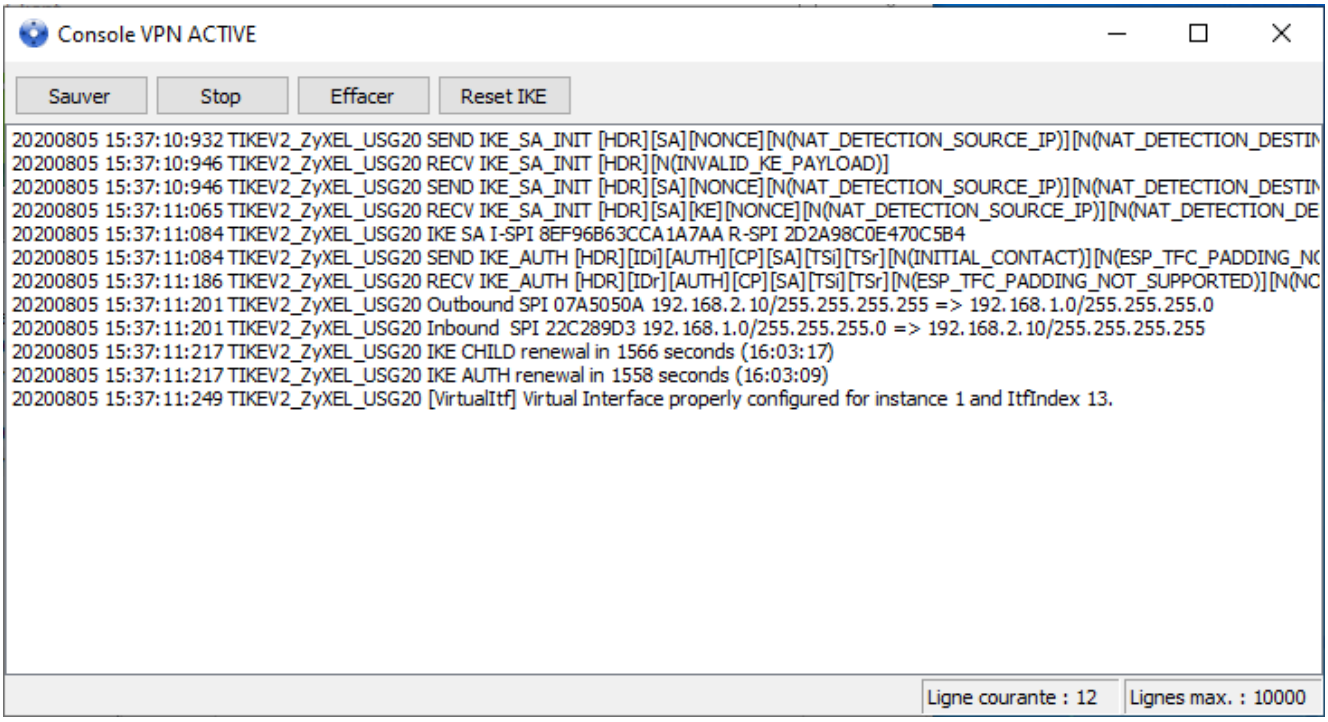
3.3 Ouvrir un tunnel VPN IPSec

Lorsque le Routeur VPN Dynfi et le Client VPN TheGreenBow ont été configuré comme décrit précédemment, vous êtes prêt pour établir des tunnels VPN IPSec. Soyez d'abord certain d'autoriser le trafic VPN IPSec dans votre Firewall.

1/ Sélectionner le menu "**Configuration**" et "**Sauver**" pour prendre en compte les dernières modifications faites à votre configuration VPN.

2/ Double Cliquer sur le nom du tunnel Child SA.

3/ Cliquer sur le menu "**Outils**" et "**Console**" pour accéder aux logs VPN L'exemple suivant indique une connexion réussie entre le client VPN IPsec TheGreenBow et le routeur Dynfi.



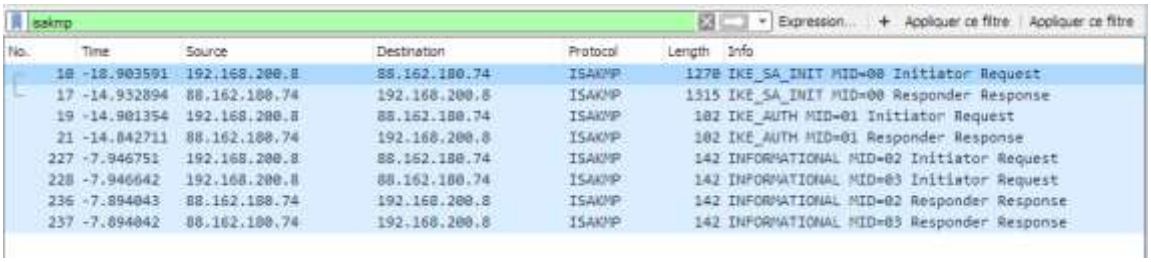
Exemple de console

4 Outils en cas de problème.

Configurer un tunnel VPN en IPsec peut s'avérer difficile. Un paramètre manquant peut empêcher la connexion VPN de s'établir. Des outils sont disponibles pour trouver la source des problèmes pendant la création du tunnel.

4.1 Wireshark : Un bon analyseur de réseau.

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie. Cet outil est disponible sur le site **www.wireshark.org**. Pour l'installation et l'utilisation du logiciel Wireshark, la documentation est accessible via ce lient : **www.wireshark.org/docs/**.



5 Résolution des problèmes VPN IPsec

5.1 Erreur VPN083 : "No proposal chosen" (Algorithme de Phase 1 différent).

```
20090429 115905 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
20090429 115905 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
20090429 115905 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
20090429 115911 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
20090429 115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

Le message "No proposal chosen" a été reçu lors d'un échange avec IKE : L'algorithme de chiffrement de la Phase 1 ou un autre paramètre de la Phase 1 ne correspond pas à celui configuré sur la passerelle.

Vous pouvez :

- Vérifier que l'algorithme de chiffrement de la Phase 1 du Client VPN correspond à celui de la passerelle (ou poste).
- Vérifier les plages d'adresses IP.
- Vérifier le Local ID et le Remote ID.
  Avertissement : le Local ID sur le routeur est le Remote ID sur le Client VPN et inversement !
- Vérifier que le PFS est activé ou non sur le Client VPN (Panneau Phase 2) et sur la passerelle.
- Redémarrer la passerelle.

5.2 Erreur VPN084 : "No proposal chosen" (Algorithme de Phase 2 différent).

```
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(FR
AGMENTATION_SUPPORTED)]
20XX0913 16:08:53:419 TIKEV2_Tunnel RECV IKE_SA_INIT [HDR][N(NO_PROPOSAL_CHOSEN)]
```

Le message "No proposal chosen" a été reçu lors d'un échange avec IKE : L'algorithme de chiffrement de la Phase 2 ne correspond pas à celui configuré sur la passerelle.

Vous pouvez :

- Vérifier que l'algorithme de chiffrement de la Phase 2 du Client VPN correspond à celui de la passerelle (ou poste).

5.3 Erreur “AUTHENTICATION_FAILED”.

```
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
```

Le message “AUTHENTICATION_FAILED” signifie que le certificat ou que la clé partagée (Pre-Sahred Key) ne correspond pas.

Vous pouvez :

- Vérifier sur le routeur / passerelle que le certificat utilisateur ou la clé partagée est valide.

5.4 Erreur “No user certificate available for the connection”

```
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.
```

Le message “No user certificate available for the connection” signifie que le certificat utilisateur n’est pas accessible.

Vous pouvez :

- Vérifier que le certificat est sélectionné ou si le Token (smartcard) est disponible sur l’ordinateur

5.5 Erreur “Remote ID rejected”.

```
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
```

Le message “Remote ID rejected” signifie que la valeur “Adresse routeur distant” ne correspond pas à la valeur attendue par le routeur / passerelle.

Vous pouvez :

- Vérifier dans l’onglet “Protocole” que l’adresse du routeur distant soit la bonne.

5.6 Erreur “FAILED_CP_REQUIRED”.

```
20XX0913 16:29:46:780 TIKEV2_Tunnel RECV IKE_AUTH
[HDR][IDr][CERT][AUTH][N(AUTH_LIFETIME)][N(FAILED_CP_REQUIRED)][N(TS_UNACCEPTABLE)]
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
```

Le message “FAILED_CP_REQUIRED” signifie que le routeur / passerelle est configuré pour utiliser le Mode Config.

Vous pouvez :

- Dans le panneau de configuration, sélectionner la phase 2 de la connexion. Dans l’onglet “Child SA”, cocher “Obtenir la configuration depuis la passerelle”

5.7 J'ai cliqué "Open tunnel" mais rien ne se passe.

```
20XX1003 11:08:34:031 [VPNCONF] TGBIKE_STARTED received
20XX1003          11:21:34:379          TIKEV2_vRHEL75          SEND          IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003          11:21:39:397          TIKEV2_vRHEL75          SEND          IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003          11:21:44:409          TIKEV2_vRHEL75          SEND          IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003 11:21:49:423 TIKEV2_vRHEL75 3 attempts with no response. Aborting connection.
```

Vous pouvez :

- Lire les logs de chaque bout de tunnel (client VPN et routeur / passerelle)
- Les requêtes IKE peuvent être annulées par les pare feu.
- Vérifier le port UDP utilisé, un client VPN IPsec utilise le port UDP 500.
- Vérifier si le serveur distant est en ligne / accessible.

5.8 Le tunnel VPN est ouvert mais je ne peux rien pinger !

Si le tunnel VPN est ouvert mais que vous ne pouvez pas pinger le réseau distant, voici quelques conseils :

- Vérifier les paramètres "Adresse du Client VPN" et "Adresse réseau distant" dans l'onglet "Child SA". Habituellement, l'adresse IP du client VPN ne doit pas appartenir au sous-réseau LAN distant.
- Une fois que le tunnel VPN est en place, les paquets sont envoyés avec le protocole ESP. Ce protocole peut être bloqué par un pare-feu. Vérifier que chaque appareil entre le client et le serveur VPN accepte le protocole ESP.
- Vérifier les logs du serveur VPN. Les paquets peuvent être rejetés par l'une des règles de son pare-feu.
- Vérifier si votre FAI supporte ESP et si le protocole 50 est autorisé à passer le trafic dans vos pares-feux.
- Si vous ne pouvez toujours pas faire de ping, suivez le trafic ICMP sur l'interface LAN du serveur VPN et sur l'interface informatique LAN (avec Wireshark par exemple). Vous aurez une indication que le cryptage fonctionne.
- Vérifiez la valeur "default gateway" dans le LAN du serveur VPN. Une cible sur votre réseau local distant peut recevoir des pings mais ne répond pas car il n'y a pas de paramètre "default gateway".
- Vous ne pouvez pas accéder aux ordinateurs du réseau local par leur nom. Vous devez spécifier leur adresse IP à l'intérieur du réseau local.
- Nous vous recommandons d'installer Wireshark (**www.wireshark.org**) sur l'un de vos ordinateurs cibles. Vous pouvez vérifier que vos pings arrivent à l'intérieur du réseau local.

6 Contacts

Nouveautés et mises-à-jour sur le site Internet TheGreenBow : **www.thegreenbow.com**

E-mail du support technique : **support@thegreenbow.com**

E-mail de l'équipe commerciale : **sales@thegreenbow.com**

Secure, Strong, Simple

TheGreenBow Security Software