

# TheGreenBow IPsec VPN Client

## Guide de Configuration

### ZyXEL USG20-VPN

Protocole - IKEv2

Site Internet : [www.thegreenbow.com](http://www.thegreenbow.com)  
Contact: [support@thegreenbow.com](mailto:support@thegreenbow.com)

## Table des matières

1	Introduction .....	3
1.1	But de ce document .....	3
1.2	Description de l'environnement réseau .....	3
1.3	Restrictions du ZyXEL USG20-VPN .....	3
1.4	Le routeur ZyXEL USG20-VPN .....	3
1.5	Information produit du routeur ZyXEL USG20-VPN.....	3
2	ZyXEL USG20-VPN VPN configuration .....	4
3	Configuration IPsec du client VPN TheGreenBow .....	9
3.1	Configuration IKE Auth du client VPN TheGreenBow .....	9
3.2	Configuration VPN Client IPsec Phase 2 (Child SA) .....	10
3.3	Ouvrir un tunnel VPN IPsec .....	11
4	Outils en cas de problème .....	12
4.1	Wireshark : Un bon analyseur de réseau.....	12
5	Résolution des problèmes VPN IPsec .....	13
5.1	Erreur VPN083 : "No proposal chosen" (Algorithme de Phase 1 différent). .....	13
5.2	Erreur VPN084 : "No proposal chosen" (Algorithme de Phase 2 différent). .....	13
5.3	Erreur "AUTHENTICATION_FAILED" .....	13
5.4	Erreur "No user certificate available for the connection" .....	14
5.5	Erreur "Remote ID rejected" .....	14
5.6	Erreur "FAILED_CP_REQUIRED" .....	14
5.7	J'ai cliqué "Open tunnel" mais rien ne se passe. ....	15
5.8	Le tunnel VPN est ouvert mais je ne peux rien pinger ! .....	15
6	Contacts .....	16

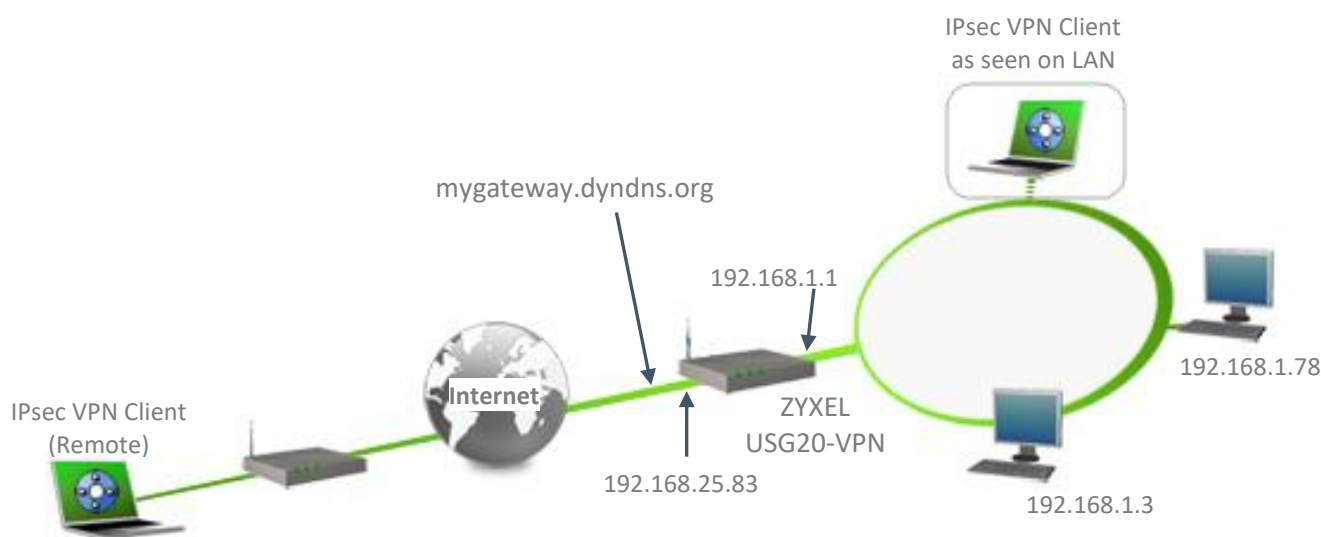
## 1 Introduction

### 1.1 But de ce document

Ce document décrit la configuration du Client VPN IPsec TheGreenBow avec un routeur ZyXEL USG20-VPN 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 décrivons un exemple de connexion entre le client TheGreenBow VPN et le réseau local se trouvant derrière le routeur ZyXEL USG20-VPN. 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 ZyXEL USG20-VPN

Pas de restrictions connues.

### 1.4 Le routeur ZyXEL USG20-VPN

Nos tests et configuration VPN ont été réalisés avec un routeur ZyXEL USG20-VPN version 4.38(ABAQ.0).

### 1.5 Information produit du routeur ZyXEL USG20-VPN

Il est important que les utilisateurs trouvent toutes les informations nécessaires concernant le routeur ZyXEL USG20-VPN VPN Gateway. Toutes les informations produit, guide utilisateur et base de connaissance peuvent être trouvées sur le site Internet : [https://www.zyxel.com/products\\_services/Business-Firewall-USG20-VPN-USG20W-VPN/downloads](https://www.zyxel.com/products_services/Business-Firewall-USG20-VPN-USG20W-VPN/downloads)

Page produit ZyXEL USG20-VPN

[https://www.zyxel.com/products\\_services/Business-Firewall-USG20-VPN-USG20W-VPN/](https://www.zyxel.com/products_services/Business-Firewall-USG20-VPN-USG20W-VPN/)

Guide utilisateur ZyXEL USG20-VPN

[ftp://ftp.zyxel.fr/ftp\\_download/USG20W-VPN/user\\_guide/USG20W-VPN\\_V4.16\\_Ed1.pdf](ftp://ftp.zyxel.fr/ftp_download/USG20W-VPN/user_guide/USG20W-VPN_V4.16_Ed1.pdf)

## 2 ZyXEL USG20-VPN VPN configuration

Cette section décrit la configuration VPN de votre routeur ZyXEL USG20-VPN.

Default Login Details	
LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	1234

Une fois connecté à votre routeur ZyXEL USG20-VPN VPN, cliquer sur le menu “Mode Expert” :

The screenshot shows the ZyXEL USG20-VPN web interface. At the top, there is a navigation bar with several icons. The 'Mode Expert' icon, which is a crossed wrench and screwdriver, is highlighted with a red rectangular box. Below the navigation bar, there are several panels. On the left, there is a 'System' panel with information like 'Version du micrologiciel', 'Temps de fonctionne...', 'Date du jour', and 'Heure actuelle'. Below that is an 'Internet' panel with 'Type de connexion', 'WAN IP', 'Passerelle', and 'DNS'. Further down is a 'VPN' panel with a warning message: 'Les règles VPN ne peuvent pas être configurées en Mode Simplifié, mais celles configurées en Mode Expert restent appliquées. Vérifier en Mode Expert.' At the bottom left is a 'Security' panel with 'Pare-feu' (ON) and 'Filtrage de contenu' (OFF). On the right side, there is a 'Réseau client' panel showing 'LAN 1: P3 P4 P5 P6' and 'Clients connectés: 2'. Below that is a 'Réseau Invités: N/A' section showing 'Clients connectés: 0'.

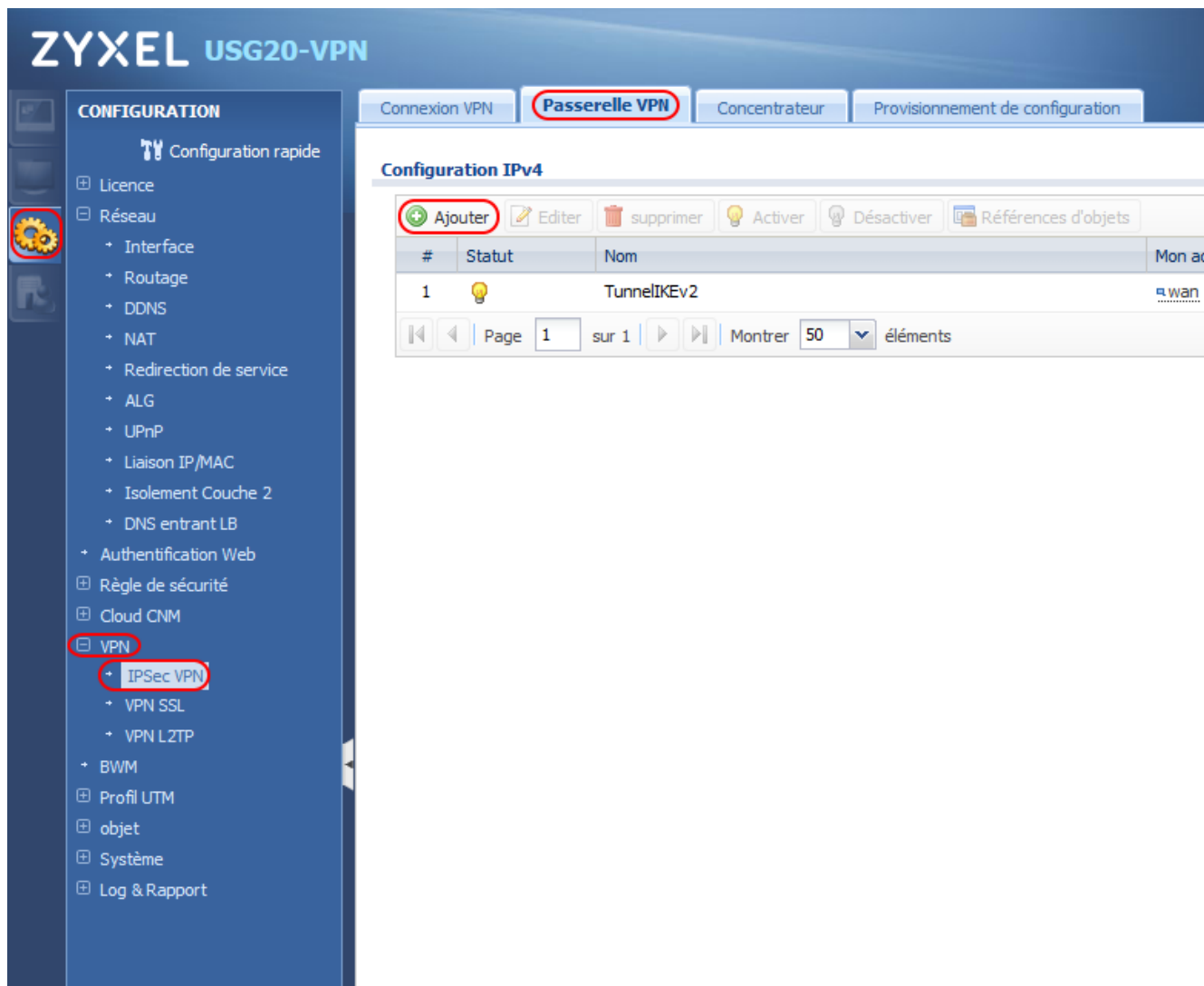
Le fenêtre suivante est affichée, sélectionner “Mode Expert” et cliquer sur “OK”

The dialog box is titled 'Passer en Mode Expert'. It contains the following text: 'Cliquez sur "OK" pour passer en Mode Expert. Ce mode permet de configurer l'ensemble des fonctionnalités de votre USG.' followed by 'Veuillez noter qu'en Mode Simplifié vous risquez de ne pas visualiser les modifications configurées en Mode Expert.' Below this, it asks 'Sur quel mode souhaitez vous démarrer lors de la prochaine connexion ?' with two radio button options: 'Mode Simplifié' and 'Mode Expert'. The 'Mode Expert' option is selected. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

# Guide de Configuration

Cliquer sur :

- L'onglet "Configuration",
- Le menu "VPN",
- The sous-menu "IPSec VPN",
- L'onglet "Passerelle VPN",
- Cliquer sur "Ajouter".



Saisir toutes les informations présentent dans l'image suivante. Cette étape est l'équivalent de la phase 1 pour le client VPN TheGreenBow.

### Edit VPN Gateway TunnelIKEv2

Cacher les paramètres avancés

#### Paramètres Généraux

Activer

Nom passerelle VPN:

#### Version IKE

IKEv1

IKEv2

#### Paramètre passerelle

##### Mon adresse

Interface  DHCP client -- 192.168.25.83/255.255.255.0

Nom de domaine IPV4

##### Adresse passerelle distante

Adresse statique

Primaire

Secondaire

Revenir à la passerelle distante primaire quand c'est possible

Intervalle de vérification de retour:  (60 à 86 400 secondes)

Adresse dynamique

#### Authentification

Clé prépartagée   unmasked

Certificat  (Voir [Mes certificats](#))

#### Avancé

Type d'ID locale:

Contenu:

Type d'ID distant:

Contenu:

#### Paramètres Phase 1

Durée de vie SA:  (180 - 3000000 Secondes)

#### Avancé

Proposition

<input type="button" value="Ajouter"/> <input type="button" value="Editer"/> <input type="button" value="supprimer"/>		
#	Cryptage	Authentification
1	AES128	SHA1

Groupe de clés:

#### Extended Authentication Protocol

Activer protocole d'authentification étendue

Méthode d'authentification autorisée:

Mode serveur

Méthode AAA:

Utilisateur autorisé:

Mode Client

Nom d'utilisateur:

Mot de passe:

Retaper pour confirmer:

Sélectionner ensuite l'onglet "Connexion VPN" et cliquer sur "Ajouter" dans la partie "Configuration IPv4". Saisir toutes les informations des 2 images suivantes.

**Edit VPN Connection TGBTestIKEv2**

Cacher les paramètres avancés Créer un nouvel objet ▾

### Paramètres Généraux

Activer

Nom de connexion: TGBTestIKEv2

**Avancé**

Reconnexion automatique

Activer la détection de réinsertion

Activer la diffusion NetBIOS over IPsec

Réglage du MSS

Personnalisation de la taille 0 (200 - 1460 Bytes)

Auto

Resserré

### Passerelle VPN

Scénario d'application

Site à site

Site à site avec une passerelle dynamique

Accès distant (Rôle du serveur)

Accès à distance (Rôle du client)

Interface VPN

Passerelle VPN: TunnelIKEv2 wan 0.0.0.0, 0.0.0.0

### Stratégie

Stratégie Locale: LAN1\_SUBNET INTERFACE SUBNET, 192.168.1.0/24

**Avancé**

Activer GRE Over IPsec ⓘ

### Configuration chargée

Activer configuration de charge

Pool d'adresse IP: LAN2\_SUBNET INTERFACE SUBNET, 192.168.2.0/24 ⓘ

Premier serveur DNS (Option):

Second serveur DNS (Option):

Premier serveur WINS (Option):

Second serveur WINS (Option):

**Réglage de la phase 2**

Durée de vie SA:  (180 - 3000000 Secondes)

**Avancé**

Protocole d'activation:

Encapsulation:

Proposition

Ajouter			Editer			supprimer		
#	Cryptage	Authentification						
1	AES128	SHA1						

Perfect Forward Secrecy (PFS):

**Paramètres associés**

Zone:

**Avancé**

**NAT trafic d'entrée/sortie**

Trafic de sortie

Source NAT

Source:

Destination:

SNAT:

Trafic d'entrée

Source NAT

Source:

Destination:

SNAT:

NAT de destination

Ajouter								Editer		supprimer		Déplacer	
#	IP originale	IP mappée	Protocole	Début du port origi...	Fin du port original	Start Port mappés	Fin du port mappé						
								Page 0 sur 0		Montrer 50 éléments		Aucune donnée à afficher	

OK Cancel

Une fois toutes ces configurations faites, cliquer sur le bouton "Appliquer" situé en bas de la fenêtre du routeur.

Appliquer Réinitialiser

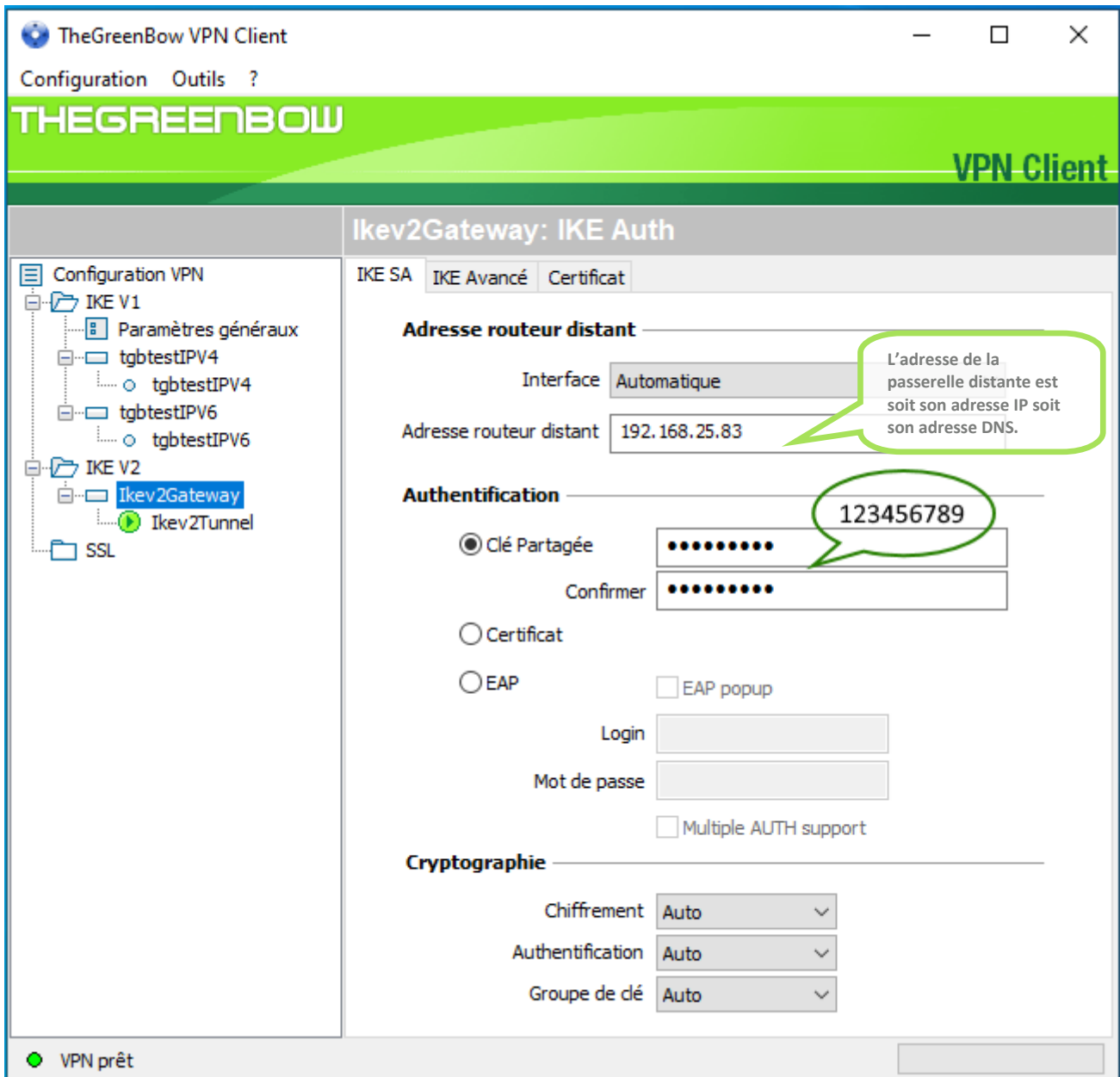


## 3 Configuration IPsec du client VPN TheGreenBow

Cette section décrit la configuration requise pour se connecter au routeur ZyXEL USG20-VPN via une connexion VPN.

Pour télécharger la dernière version du client IPsec VPN TheGreenBow, aller sur le site : [www.thegreenbow.com/vpn\\_down.html](http://www.thegreenbow.com/vpn_down.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 ZyXEL USG20-VPN ou au guide utilisateur TheGreenBow IPsec VPN Client pour plus de détails sur l'authentification utilisateur.

## 3.2 Configuration VPN Client IPsec Phase 2 (Child SA)

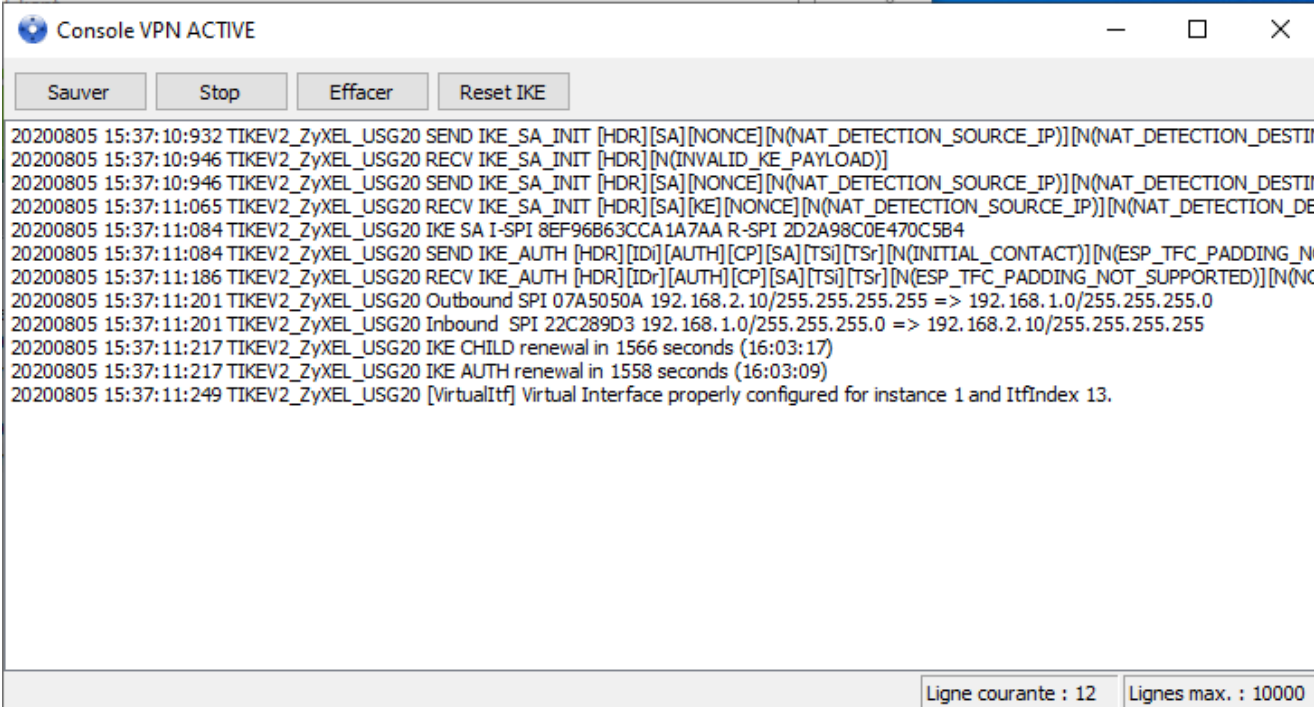
The screenshot shows the 'TheGreenBow VPN Client' configuration window. The title bar includes 'Configuration Outils ?'. The main header features 'THEGREENBOW' and 'VPN Client'. The left sidebar shows a tree view with 'Configuration VPN' expanded, containing 'IKE V1' (with 'Paramètres généraux', 'tgbtestIPV4', and 'tgbtestIPV6'), 'IKE V2' (with 'Ikev2Gateway' and 'Ikev2Tunnel'), and 'SSL'. The 'Ikev2Tunnel' is selected. The main area is titled 'Ikev2Tunnel: Child SA' and has tabs for 'Child SA', 'Avancé', 'Automatisation', and 'Bureau distant'. The 'IPV4' tab is active. Under 'Trafic sélecteurs', the 'Adresse du Client VPN' is '192 . 168 . 2 . 6', 'Type d'adresse' is 'Adresse réseau', 'Adresse réseau distant' is '192 . 168 . 1 . 0', and 'Masque réseau' is '255 . 255 . 255 . 0'. The checkbox 'Obtenir la configuration depuis la passerelle' is checked. Under 'Cryptographie', 'Chiffrement' is 'AES 128', 'Intégrité' is 'SHA1', and 'Diffie-Hellman' is 'DH2 (1024)'. Under 'Durée de vie (sec.)', 'Durée de vie Child SA' is '1800'. A green callout bubble points to the 'Adresse du Client VPN' field with the text: 'L'adresse du client VPN ainsi que l'adresse réseau distant et le masque réseau sont fournis par le routeur.' At the bottom left, a green dot indicates 'VPN prêt'.

La configuration des autres onglets est laissée par défaut.

## 3.3 Ouvrir un tunnel VPN IPSec

Lorsque le Routeur VPN ZyXEL USG20-VPN 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 ZyXEL USG20-VPN.



The screenshot shows a window titled "Console VPN ACTIVE" with a toolbar containing buttons for "Sauver", "Stop", "Effacer", and "Reset IKE". The main area displays a log of IKE negotiations between TIKEV2\_ZyXEL\_USG20 and TheGreenBow. The logs show successful completion of the IKE SA establishment and authentication process, including the receipt of the CHILD SA and the start of the IKE CHILD renewal cycle.

```
20200805 15:37:10:932 TIKEV2_ZyXEL_USG20 SEND IKE_SA_INIT [HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTIN
20200805 15:37:10:946 TIKEV2_ZyXEL_USG20 RECV IKE_SA_INIT [HDR][N(INVALID_KEY_PAYLOAD)]
20200805 15:37:10:946 TIKEV2_ZyXEL_USG20 SEND IKE_SA_INIT [HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTIN
20200805 15:37:11:065 TIKEV2_ZyXEL_USG20 RECV IKE_SA_INIT [HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DE
20200805 15:37:11:084 TIKEV2_ZyXEL_USG20 IKE SA I-SPI 8EF96B63CCA1A7AA R-SPI 2D2A98C0E470C5B4
20200805 15:37:11:084 TIKEV2_ZyXEL_USG20 SEND IKE_AUTH [HDR][IDr][AUTH][CP][SA][TSi][TSr][N(INITIAL_CONTACT)][N(ESP_TFC_PADDING_NC
20200805 15:37:11:186 TIKEV2_ZyXEL_USG20 RECV IKE_AUTH [HDR][IDr][AUTH][CP][SA][TSi][TSr][N(ESP_TFC_PADDING_NOT_SUPPORTED)][N(NC
20200805 15:37:11:201 TIKEV2_ZyXEL_USG20 Outbound SPI 07A5050A 192.168.2.10/255.255.255.255 => 192.168.1.0/255.255.255.0
20200805 15:37:11:201 TIKEV2_ZyXEL_USG20 Inbound SPI 22C289D3 192.168.1.0/255.255.255.0 => 192.168.2.10/255.255.255.255
20200805 15:37:11:217 TIKEV2_ZyXEL_USG20 IKE CHILD renewal in 1566 seconds (16:03:17)
20200805 15:37:11:217 TIKEV2_ZyXEL_USG20 IKE AUTH renewal in 1558 seconds (16:03:09)
20200805 15:37:11:249 TIKEV2_ZyXEL_USG20 [VirtualItf] Virtual Interface properly configured for instance 1 and Itfindex 13.
```

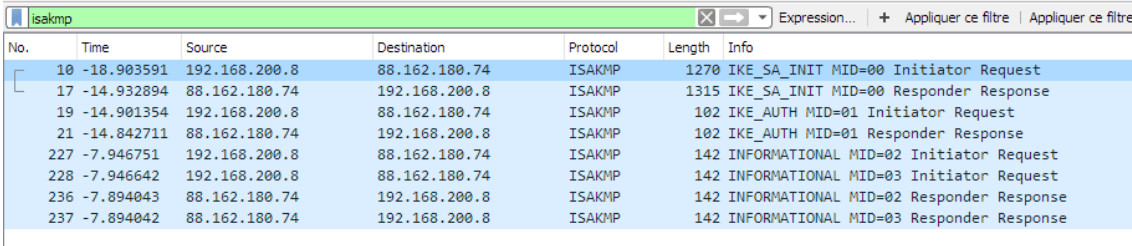
Ligne courante : 12 Lignes max. : 10000

## 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](http://www.wireshark.org). Pour l'installation et l'utilisation du logiciel Wireshark, la documentation est accessible via ce lien : [www.wireshark.org/docs/](http://www.wireshark.org/docs/).



No.	Time	Source	Destination	Protocol	Length	Info
10	-18.903591	192.168.200.8	88.162.180.74	ISAKMP	1270	IKE_SA_INIT MID=00 Initiator Request
17	-14.932894	88.162.180.74	192.168.200.8	ISAKMP	1315	IKE_SA_INIT MID=00 Responder Response
19	-14.901354	192.168.200.8	88.162.180.74	ISAKMP	102	IKE_AUTH MID=01 Initiator Request
21	-14.842711	88.162.180.74	192.168.200.8	ISAKMP	102	IKE_AUTH MID=01 Responder Response
227	-7.946751	192.168.200.8	88.162.180.74	ISAKMP	142	INFORMATIONAL MID=02 Initiator Request
228	-7.946642	192.168.200.8	88.162.180.74	ISAKMP	142	INFORMATIONAL MID=03 Initiator Request
236	-7.894043	88.162.180.74	192.168.200.8	ISAKMP	142	INFORMATIONAL MID=02 Responder Response
237	-7.894042	88.162.180.74	192.168.200.8	ISAKMP	142	INFORMATIONAL MID=03 Responder Response

## 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(FRAGMENTATION_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 pare-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](http://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](http://www.thegreenbow.com)

E-mail du support technique : [support@thegreenbow.com](mailto:support@thegreenbow.com)

E-mail de l'équipe commerciale : [sales@thegreenbow.com](mailto:sales@thegreenbow.com)



# **Secure, Strong, Simple**

TheGreenBow Security Software