

TheGreenBow IPsec VPN Client

Guide de Configuration

Dynfi

Protocole - IKEv2

Site Internet : www.thegreenbow.com
Contact: 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 Dynfi	3
1.4	Le routeur Dynfi	3
1.5	Information produit du routeur Dynfi	3
2	Dynfi VPN configuration	4
3	Configuration IPsec du client VPN TheGreenBow	10
3.1	Configuration IKE Auth du client VPN TheGreenBow	10
3.2	Configuration VPN Client IPsec Phase 2 (Child SA)	13
3.3	Ouvrir un tunnel VPN IPsec	14
4	Outils en cas de problème	15
4.1	Wireshark : Un bon analyseur de réseau	15
5	Résolution des problèmes VPN IPsec	16
5.1	Erreur VPN083 : "No proposal chosen" (Algorithme de Phase 1 différent)	16
5.2	Erreur VPN084 : "No proposal chosen" (Algorithme de Phase 2 différent)	16
5.3	Erreur "AUTHENTICATION_FAILED"	16
5.4	Erreur "No user certificate available for the connection"	17
5.5	Erreur "Remote ID rejected"	17
5.6	Erreur "FAILED_CP_REQUIRED"	17
5.7	J'ai cliqué "Open tunnel" mais rien ne se passe	18
5.8	Le tunnel VPN est ouvert mais je ne peux rien pinger !	18
6	Contacts	19

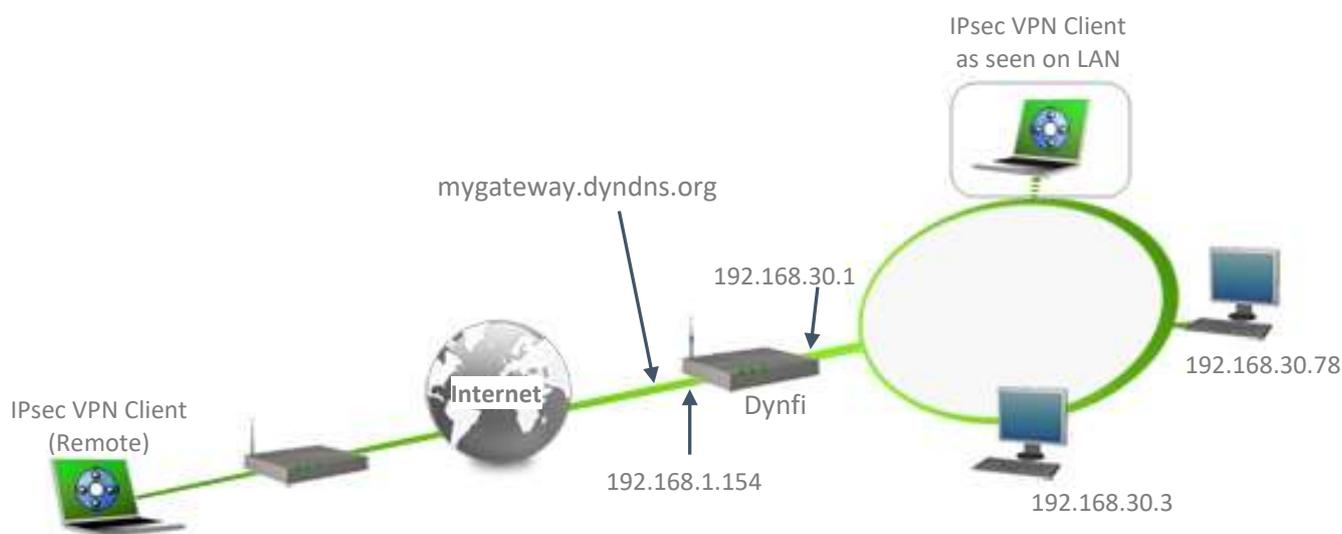
1 Introduction

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 décrivons 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
Guide utilisateur Dynfi
FAQ Dynfi

<https://dynfi.com/fr>
<https://dynfi.com/documentation/>
<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 :

The screenshot displays the Dynfi web interface for configuring an IPsec tunnel. The left sidebar shows the navigation menu with 'VPN' and 'Tunnel Settings' highlighted. The main content area is titled 'VPN: IPsec: Tunnel Settings' and includes a 'Log' button and a 'Status' dropdown. The configuration is organized into several sections:

- General information:** Includes a 'Disabled' checkbox (unchecked), a 'Mode' dropdown set to 'Tunnel IPv4', and a 'Description' text field.
- Local Network:** Includes a 'Type' dropdown set to 'Network', an 'Address' text field containing '192.168.30.0', and a dropdown set to '24'.
- Phase 2 proposal (SA/Key Exchange):** Includes a 'Protocol' dropdown set to 'ESP'.
- Encryption algorithms:** Includes a checked 'AES' checkbox, a '256 bits' dropdown, and several other options: 'aes128gcm16', 'aes192gcm16', 'aes256gcm16' (checked), 'Blowfish', '3DES', 'CAST128', 'DES', and 'NULL (no encryption)'.
- Hash algorithms:** Includes a dropdown set to 'SHA384, SHA512'.
- PFS key group:** Includes an empty text field and a note: 'Set globally in mobile client options'.
- Lifetime:** Includes a text field set to '3600' and the unit 'seconds'.
- Advanced Options:** Includes an 'Automatically ping host' checkbox (unchecked).

A 'Save' button is located at the bottom of the configuration page.

- Dashboard
- Reporting
- System
- Interfaces
- Firewall
- VPN**
 - IPsec 
 - Act
 - Tunnel Settings**
 - Mobile Clients
 - Pre-Shared Keys
 - RSA Key Pairs
 - Advanced Settings
 - OpenVPN 
- Services
- Manager
- Power
- Support

VPN: IPsec: Tunnel Settings

[Log](#) [Status](#)   

General information [full help](#)

Disabled Disable this phase1 entry

Connection method default

Key Exchange version V2

Internet Protocol IPv4

Interface WAN

Description

Phase 1 proposal (Authentication)

Authentication method Mutual RSA

My identifier My IP address

My Certificate 192.168.1.154

My Certificate Authority CATGBDynFi

Phase 1 proposal (Algorithms)

Encryption algorithm AES
256

Hash algorithm SHA384

DH key group 14 (2048 bits)

Lifetime 28800

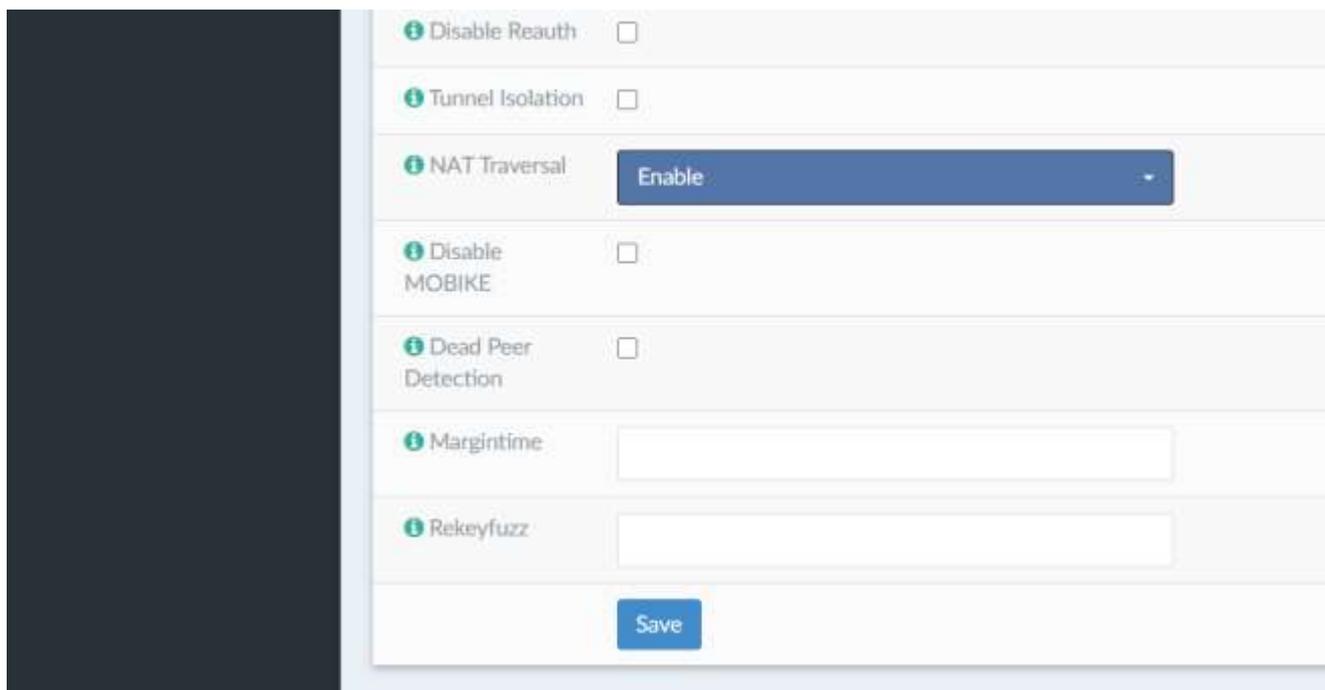
Advanced Options

Install policy

Disable Rekey

Disable Reauth

Tunnel Isolation



The screenshot shows a configuration panel for a VPN router. On the left is a dark sidebar. The main panel contains several rows of settings, each with an information icon (i) on the left and a control element on the right:

- Disable Reauth**:
- Tunnel Isolation**:
- NAT Traversal**: A dropdown menu currently showing "Enable".
- Disable MOBIKE**:
- Dead Peer Detection**:
- Margintime**: An empty text input field.
- Rekeyfuzz**: An empty text input field.

At the bottom of the configuration area is a blue button labeled "Save".

Valider la configuration en cliquant sur le bouton "Save".

Cliquer ensuite sur le menu “Mobile Clients”

The screenshot displays the DynFi web interface for configuring Mobile Clients. The left sidebar contains a navigation menu with the following items: Dashboard, Reporting, System, Interfaces, Firewall, VPN (highlighted), IPsec, Act, Tunnel Settings, Mobile Clients (highlighted), Pre-Shared Keys, RSA Key Pairs, Advanced Settings, OpenVPN, Services, Manager, Power, and Support. The main content area is titled "VPN: IPsec: Mobile Clients" and includes a "Log" button, a "Status" dropdown, and a play button. The configuration options are as follows:

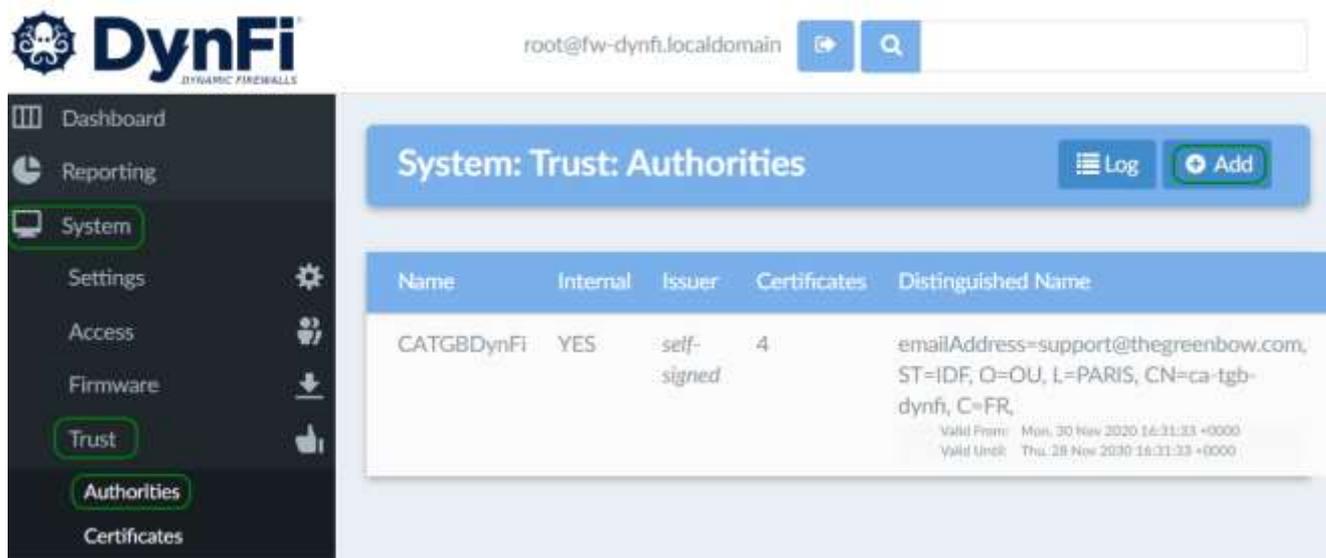
- IKE Extensions** (full help):
 - Enable: Enable IPsec Mobile Client Support
- Extended Authentication (Xauth)**:
 - Backend for authentication: Local Database
 - Enforce local group: vpnuser
- Client Configuration (mode-cfg)**:
 - Virtual Address Pool: Provide a virtual IP address to clients. Value: 10.70.70.0, 24.
 - Network List: Provide a list of accessible networks to clients.
 - Save Xauth Password: Allow clients to save Xauth passwords (Cisco VPN client only)
 - DNS Default Domain: Provide a default domain name to clients.
 - Split DNS: Provide a list of split DNS domain names to clients.
 - DNS Servers: Provide a DNS server list to clients.
 - WINS Servers: Provide a WINS server list to clients.
 - Phase 2 PFS Group: 14 (2048 bits)
 - Login Banner: Provide a login banner to clients.

A "Save" button is located at the bottom of the configuration area.

Valider la configuration en cliquant sur le bouton “Save”.

Guide de Configuration

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



The screenshot shows the DynFi web interface. The top navigation bar includes the DynFi logo, the user 'root@fw-dynfi.localdomain', and a search bar. The left sidebar contains a menu with items: Dashboard, Reporting, System (highlighted), Settings, Access, Firmware, Trust, Authorities (highlighted), and Certificates. The main content area is titled 'System: Trust: Authorities' and features a 'Log' button and an 'Add' button. Below the title is a table with the following data:

Name	Internal	Issuer	Certificates	Distinguished Name
CATGBDynFI	YES	self-signed	4	emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=ca-tgb-dynfi, C=FR, Valid From: Mon, 30 Nov 2020 16:31:33 +0000 Valid Until: Thu, 28 Nov 2030 16:31:33 +0000

Il est possible d'importer plusieurs certificats

root@fw-dynfi.localdomain

System: Trust: Certificates

Name	Issuer	Distinguished Name	In Use
● Server Cert	CATGBDynFi	emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=fw-dynfi, C=FR, CA: No, Server: Yes	
● fw-dynfi-client1	CATGBDynFi	emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=fw-dynfi-client1, C=FR, CA: No, Server: No	
● qa	CATGBDynFi	emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=qa, C=FR, CA: No, Server: No	User Cert
● 192.168.1.154	CATGBDynFi	subjectAltName=IP:192.168.1.154, emailAddress=support@thegreenbow.com, ST=IDF, O=OU, L=PARIS, CN=fwdynfi, C=FR, CA: No, Server: Yes	IPsec Tunnel

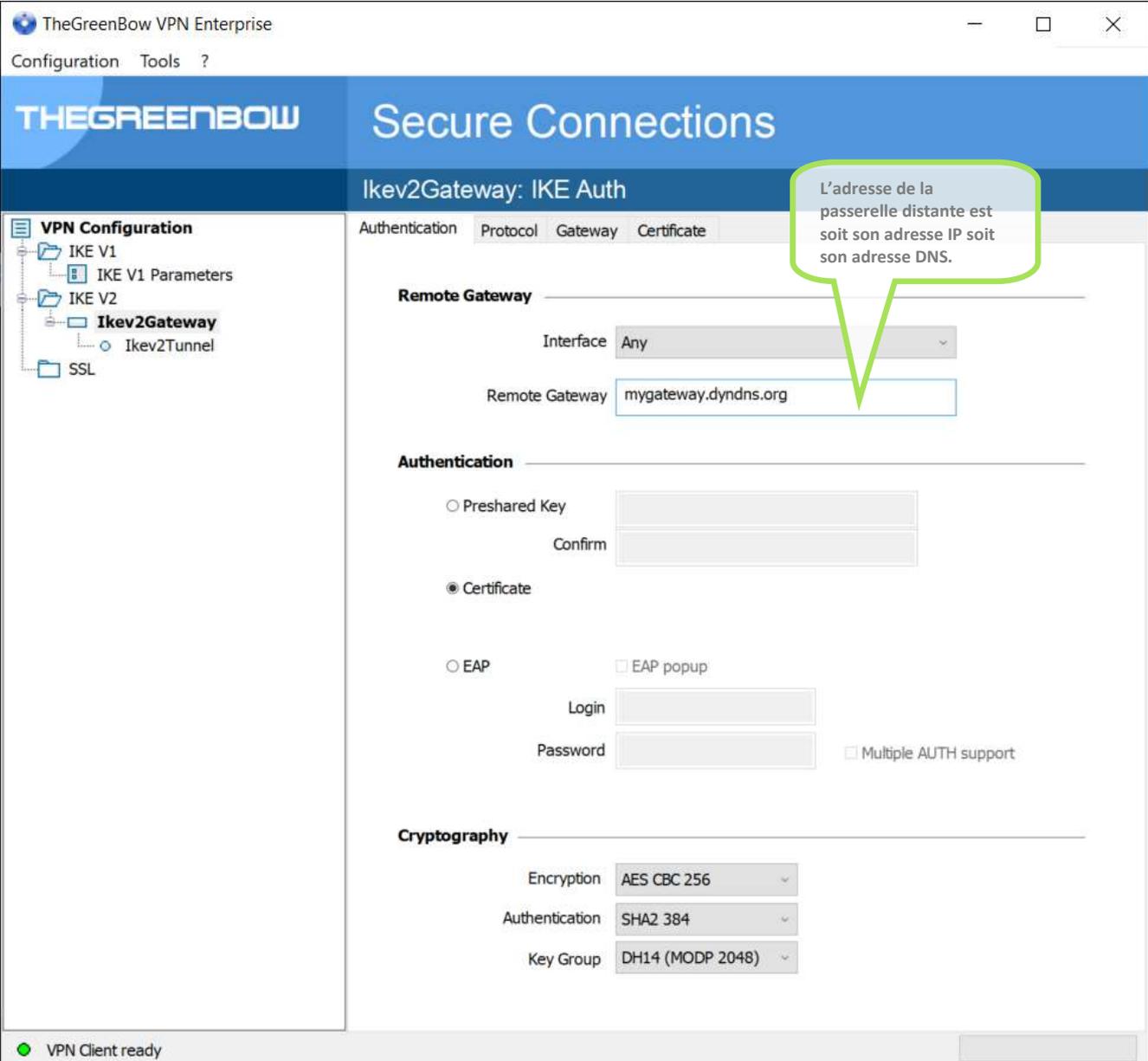
3 Configuration IPsec du client VPN TheGreenBow

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.



The screenshot shows the 'TheGreenBow VPN Enterprise' configuration window. The main title is 'Secure Connections' and the current configuration is for 'Ikev2Gateway: IKE Auth'. The interface is divided into several sections:

- VPN Configuration:** A tree view on the left showing the configuration structure: IKE V1, IKE V1 Parameters, IKE V2, Ikev2Gateway (selected), Ikev2Tunnel, and SSL.
- Authentication:** A tabbed interface with 'Authentication' selected. It contains:
 - Remote Gateway:** 'Interface' is set to 'Any' and 'Remote Gateway' is 'mygateway.dyndns.org'. A callout box points to this field with the text: 'L'adresse de la passerelle distante est soit son adresse IP soit son adresse DNS.'
 - Authentication Method:** 'Certificate' is selected with a radio button. 'Preshared Key' and 'EAP' are unselected.
 - EAP Settings:** 'EAP popup' is unselected. 'Login' and 'Password' fields are present. 'Multiple AUTH support' is unselected.
- Cryptography:** Contains three dropdown menus:
 - Encryption: AES CBC 256
 - Authentication: SHA2 384
 - Key Group: DH14 (MODP 2048)

At the bottom left, there is a status indicator: a green dot followed by 'VPN Client ready'.

The screenshot shows the configuration window for 'Ikev2Gateway: IKE Auth' in TheGreenBow VPN Enterprise. The interface includes a left-hand navigation tree under 'VPN Configuration' with sub-items: IKE V1, IKE V1 Parameters, IKE V2, Ikev2Gateway (selected), Ikev2Tunnel, and SSL. The main area has tabs for 'Authentication', 'Protocol', 'Gateway', and 'Certificate'. The 'Authentication' tab is active, showing the 'Identity' section with 'Local ID' set to 'DER ASN1 DN' and 'C = FR, ST = IDF, L = PARIS, O = OU', and 'Remote ID' set to 'IPV4 Address' and '192.168.1.154'. The 'Advanced features' section includes 'Fragmentation' (unchecked), 'Fragment size' (input field), 'IKE Port' (500), 'NAT Port' (4500), 'Enable NATT offset' (unchecked), and 'Childless' (unchecked). A status bar at the bottom left indicates 'VPN Client ready' with a green dot.

The screenshot shows the 'TheGreenBow VPN Enterprise' configuration window. The main title is 'Secure Connections' and the sub-title is 'Ikev2Gateway: IKE Auth'. The interface is divided into a left-hand navigation pane and a main content area.

VPN Configuration

- IKE V1
 - IKE V1 Parameters
- IKE V2
 - Ikev2Gateway**
 - Ikev2Tunnel
- SSL

Authentication Protocol Gateway Certificate

Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...':

Certificate Common Name	Delivered by	Expires
<input type="checkbox"/> VPN Configuration File		
<input checked="" type="radio"/> qa	ca-tgb-dynfi	03-05-2023
<input type="checkbox"/> Axalto Cryptoflex .NET		

VPN Client ready

3.2 Configuration VPN Client IPsec Phase 2 (Child SA)

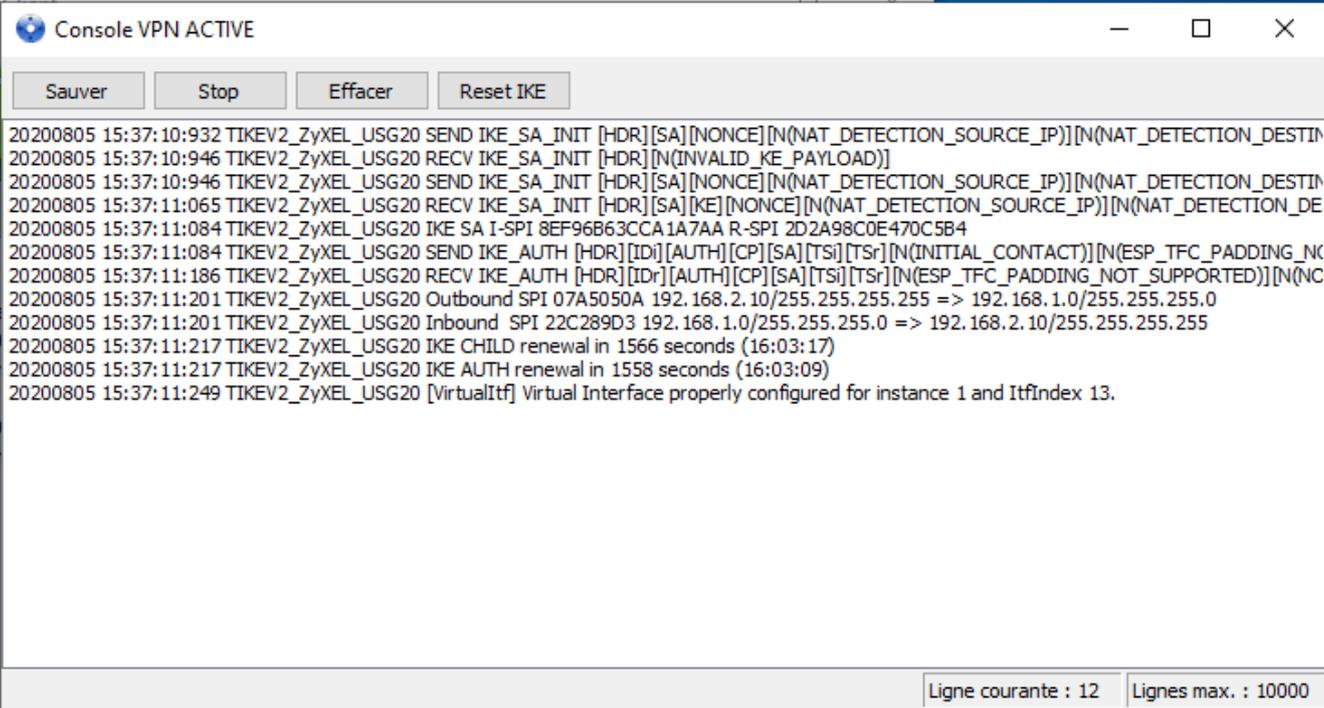
The screenshot shows the configuration window for 'Ikev2Tunnel: Child SA' in TheGreenBow VPN Enterprise. The interface includes a left-hand navigation tree under 'VPN Configuration' with sub-items for IKE V1, IKE V2, IKEv2Gateway, and SSL. The main area is divided into tabs: 'Child SA', 'Advanced', 'Automation', and 'Remote Sharing'. The 'Advanced' tab is active, showing fields for 'Traffic selectors' (VPN Client address, Address type, Remote LAN address, Subnet mask) and 'Cryptography' (Encryption, Integrity, Diffie-Hellman, Extended Sequence Number). A 'Lifetime' section shows 'Child SA Lifetime' set to 1800 seconds. A green callout bubble points to the address fields with the text: 'L'adresse du client VPN ainsi que l'adresse réseau distant et le masque réseau sont fournis par le routeur.' The status bar at the bottom indicates 'VPN Client ready'.

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.



```
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.
```

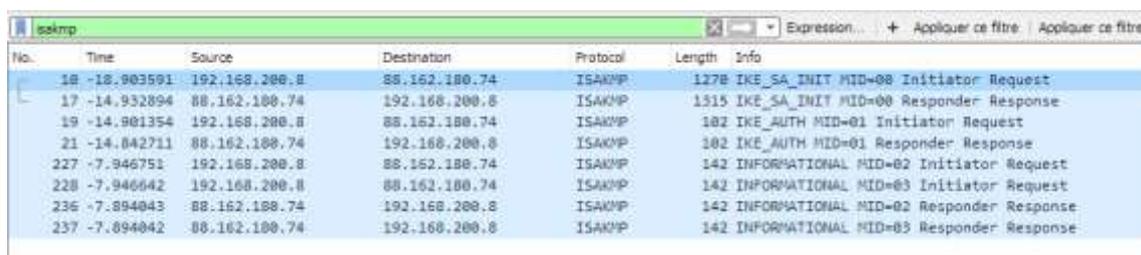
Exemple de console

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 lien : www.wireshark.org/docs/.



No.	Time	Source	Destination	Protocol	Length	Info
16	-18.903591	192.168.200.8	88.162.180.74	ISAKMP	1278	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	-14.042711	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_TunnelRemote 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) 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