

# TheGreenBow IPsec VPN Client

## Configuration Guide

### ZyXEL USG20-VPN

Protocol - IKEv2

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

## Table of Contents

1	Introduction .....	3
1.1	Goal of this document.....	3
1.2	VPN Network topology .....	3
1.3	ZyXEL USG20-VPN Restrictions .....	3
1.4	ZyXEL USG20-VPN VPN Gateway .....	3
1.5	ZyXEL USG20-VPN VPN Gateway product info .....	3
2	ZyXEL USG20-VPN VPN configuration .....	4
3	TheGreenBow IPsec VPN Client configuration .....	9
3.1	VPN Client - IKE Auth Configuration .....	9
3.2	VPN Client Phase 2 (Child SA) Configuration .....	10
3.3	Open IPsec VPN tunnels.....	11
4	Tools in case of trouble.....	12
4.1	A good network analyser: Wireshark.....	12
5	VPN IPsec Troubleshooting.....	13
5.1	“NO_PROPOSAL_CHOSEN” error (wrong IKE Auth).....	13
5.2	“AUTHENTICATION_FAILED” error .....	13
5.3	“No user certificate available for the connection” error.....	13
5.4	“Remote ID rejected” error.....	13
5.5	“NO_PROPOSAL_CHOSEN” error (wrong CHILD SA).....	14
5.6	“FAILED_CP_REQUIRED” error.....	14
5.7	I clicked on “Open tunnel”, but nothing happens. ....	14
5.8	The VPN tunnel is up but I can’t ping! .....	15
6	Contacts .....	16

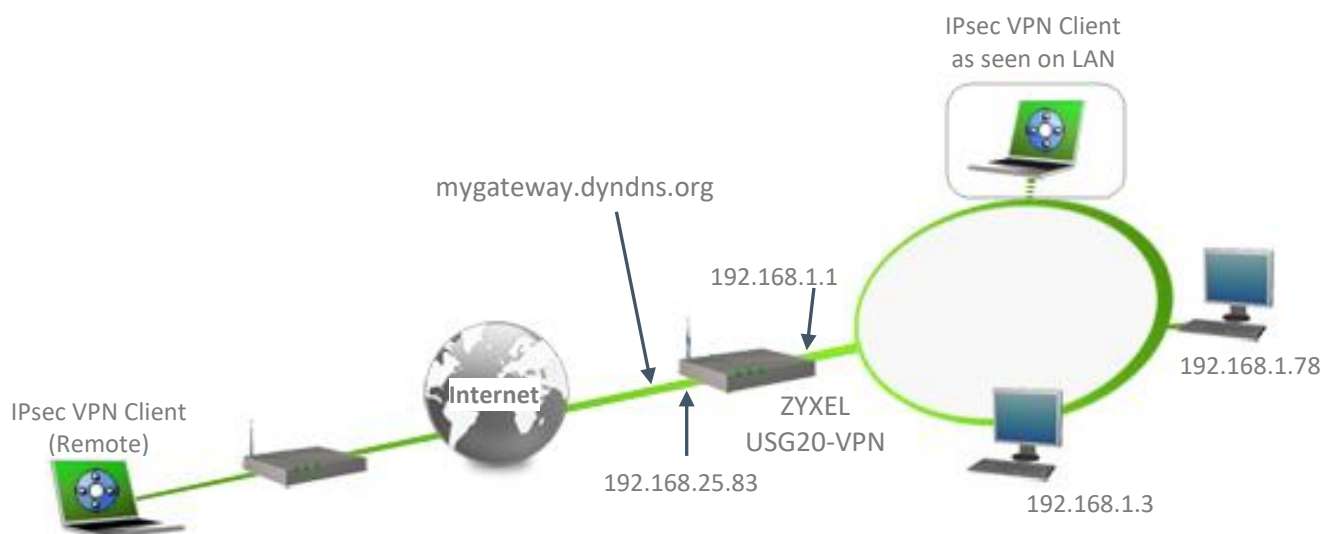
## 1 Introduction

### 1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a ZyXEL USG20-VPN VPN router to establish VPN connections for remote access to corporate network.

### 1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client software to the LAN behind the ZyXEL USG20-VPN router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



### 1.3 ZyXEL USG20-VPN Restrictions

No known restrictions

### 1.4 ZyXEL USG20-VPN VPN Gateway

Our tests and VPN configuration have been conducted with ZyXEL USG20-VPN version 4.38(ABAQ.0).

### 1.5 ZyXEL USG20-VPN VPN Gateway product info

It is critical that users find all necessary information about ZyXEL USG20-VPN Gateway. All product info, User Guide and knowledge base for the ZyXEL USG20-VPN Gateway can be found on the ZyXEL USG20-VPN website: [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)

ZyXEL USG20-VPN Product page

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

ZyXEL USG20-VPN User Guide

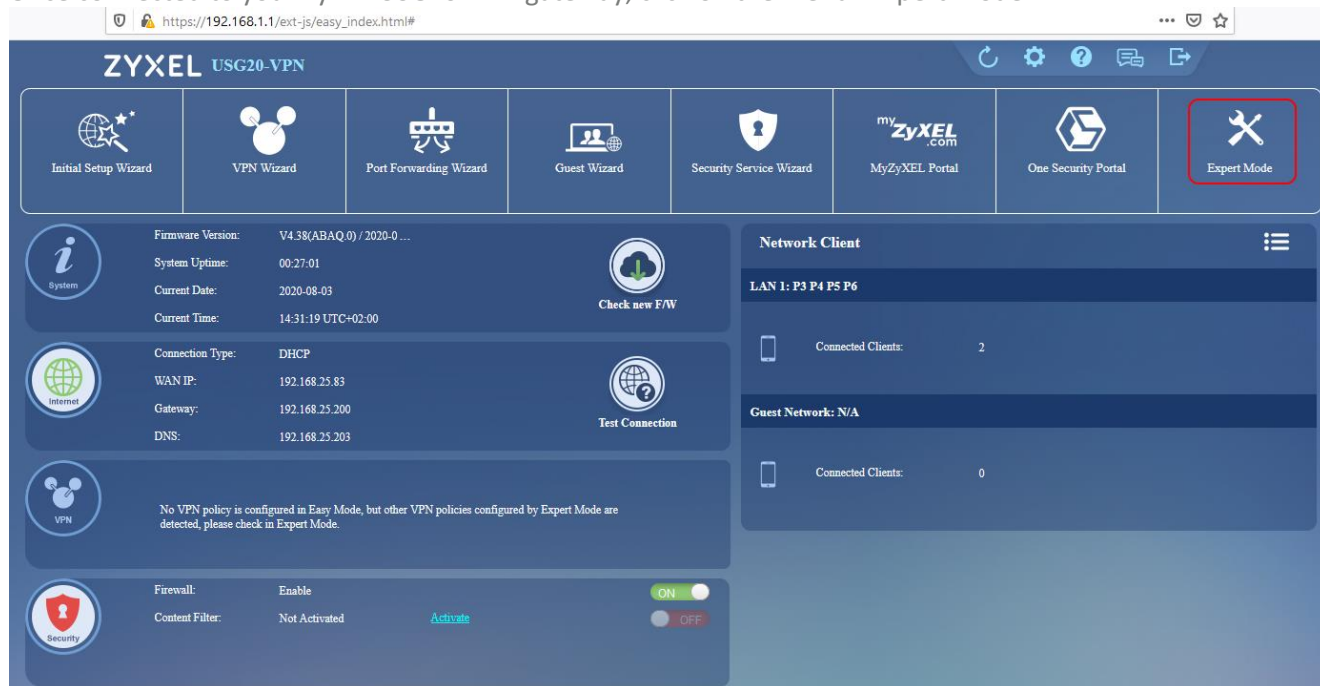
[ftp://ftp.zyxel.fr/ftp\\_download/USG20W-VPN/user\\_guide/USG20W-VPN\\_V4.16\\_Ed1.pdf](ftp://ftp.zyxel.fr/ftp_download/USG20W-VPN/user_guide/USG20W-VPN_V4.16_Ed1.pdf)

## 2 ZyXEL USG20-VPN VPN configuration

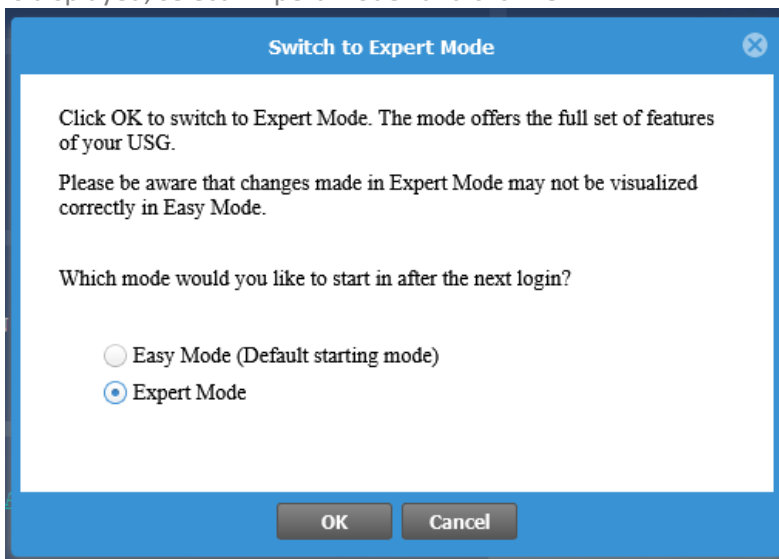
This section describes how to build an IPsec VPN configuration with your ZyXEL USG20-VPN router.

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

Once connected to your ZyXEL USG20-VPN gateway, click on the menu “Expert Mode”:



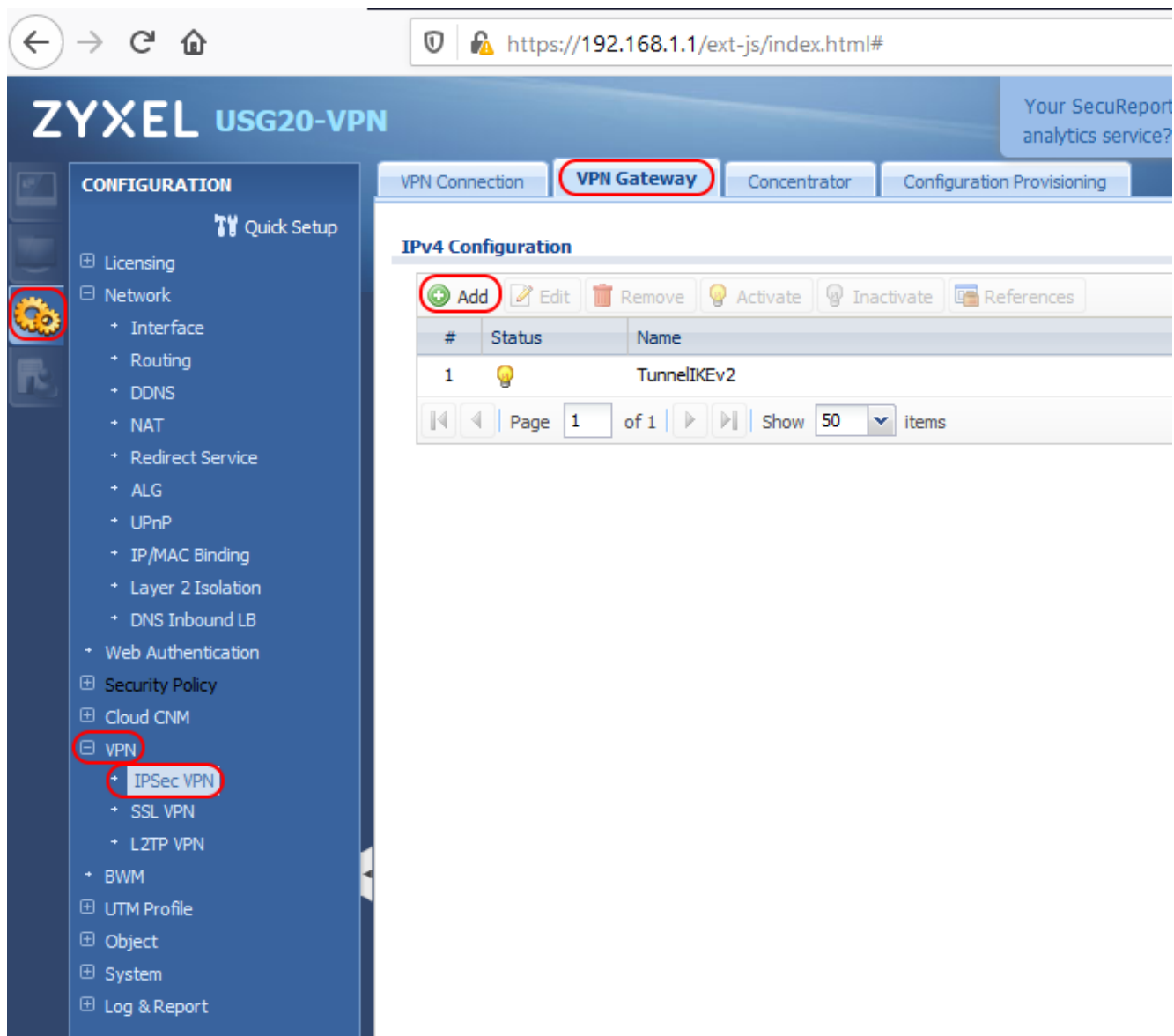
The following window is displayed, select “Expert Mode” and click “OK”



# Configuration Guide

Click on :

- The menu “Configuration”,
- The menu “VPN”,
- The submenu “IPSec VPN”,
- The “VPN Gateway” tab,
- Click on “Add”.



Enter all the information in the following picture. This is the equivalent of the Phase 1 on the TheGreenBow VPN client.

**Edit VPN Gateway TunnelIKEv2** ? X

Show Advanced Settings + Create New Object +

---

### General Settings

Enable

VPN Gateway Name:

**IKE Version**

IKEv1

IKEv2

---

### Gateway Settings

**My Address**

Interface  DHCP client -- 192.168.25.83/255.255.255.0

Domain Name / IPv4

**Peer Gateway Address**

Static Address i

Primary

Secondary

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval:  (60-86400 seconds)

Dynamic Address i

---

### Authentication

Pre-Shared Key  i

unmasked

Certificate  (See [My Certificates](#))

**Advance**

Local ID Type:

Content:

Peer ID Type:

Content:

---

### Phase 1 Settings

SA Life Time:  (180 - 3000000 Seconds)

**Advance**

Proposal

+ Add Edit Remove		
#	Encryption	Authentication
1	AES128	SHA1

Key Group:

---

### Extended Authentication Protocol

Enable Extended Authentication Protocol i

Allowed Auth Method:

Server Mode

AAA Method:

Allowed User:

Client Mode

User Name:

Password:

Retype to Confirm:

OK Cancel

# Configuration Guide

Then select the “VPN Connection” tab and click on “Add” in the part “IPv4 Configuration”. Enter all the information in the 2 following pictures.

**Edit VPN Connection TGBTestIKEv2**

Hide Advanced Settings Create New Object

---

**General Settings**

Enable

Connection Name: TGBTestIKEv2

**Advance**

Nailed-Up

Enable Replay Detection

Enable NetBIOS broadcast over IPSec

MSS Adjustment

Custom Size 0 (200 - 1460 Bytes)

Auto

Narrowed

---

**VPN Gateway**

Application Scenario

Site-to-site

Site-to-site with Dynamic Peer

Remote Access (Server Role)

Remote Access (Client Role)

VPN Tunnel Interface

VPN Gateway: TunnelIKEv2 wan 0.0.0.0, 0.0.0.0

---

**Policy**

Local Policy: LAN1\_SUBNET INTERFACE SUBNET, 192.168.1.0/24

**Advance**

Enable GRE over IPSec

---

**Configuration Payload**

Enable Configuration Payload

IP Address Pool: LAN2\_SUBNET INTERFACE SUBNET, 192.168.2.0/24

First DNS Server (Optional):

Second DNS Server (Optional):

First WINS Server (Optional):

Second WINS Server (Optional):

# Configuration Guide

**Phase 2 Setting**

SA Life Time:  (180 - 3000000 Seconds)

**Advance**

Active Protocol:

Encapsulation:

Proposal

Add Edit Remove		
#	Encryption	Authentication
1	AES128	SHA1

Perfect Forward Secrecy (PFS):  ⓘ

---

**Related Settings**

Zone:  ⓘ

**Advance**

**Inbound/Outbound traffic NAT**

**Outbound Traffic**

Source NAT

Source:

Destination:

SNAT:

**Inbound Traffic**

Source NAT

Source:

Destination:

SNAT:

Destination NAT

Add Edit Remove Move							
#	Original IP	Mapped IP	Protocol	Original Port Start	Original Port End	Mapped Port Start	Mapped Port End
No data to display							

Page 0 of 0 Show 50 items

OK Cancel

Once all those configuration done, click on the button “Apply” at the bottom of the router window.

Apply Reset

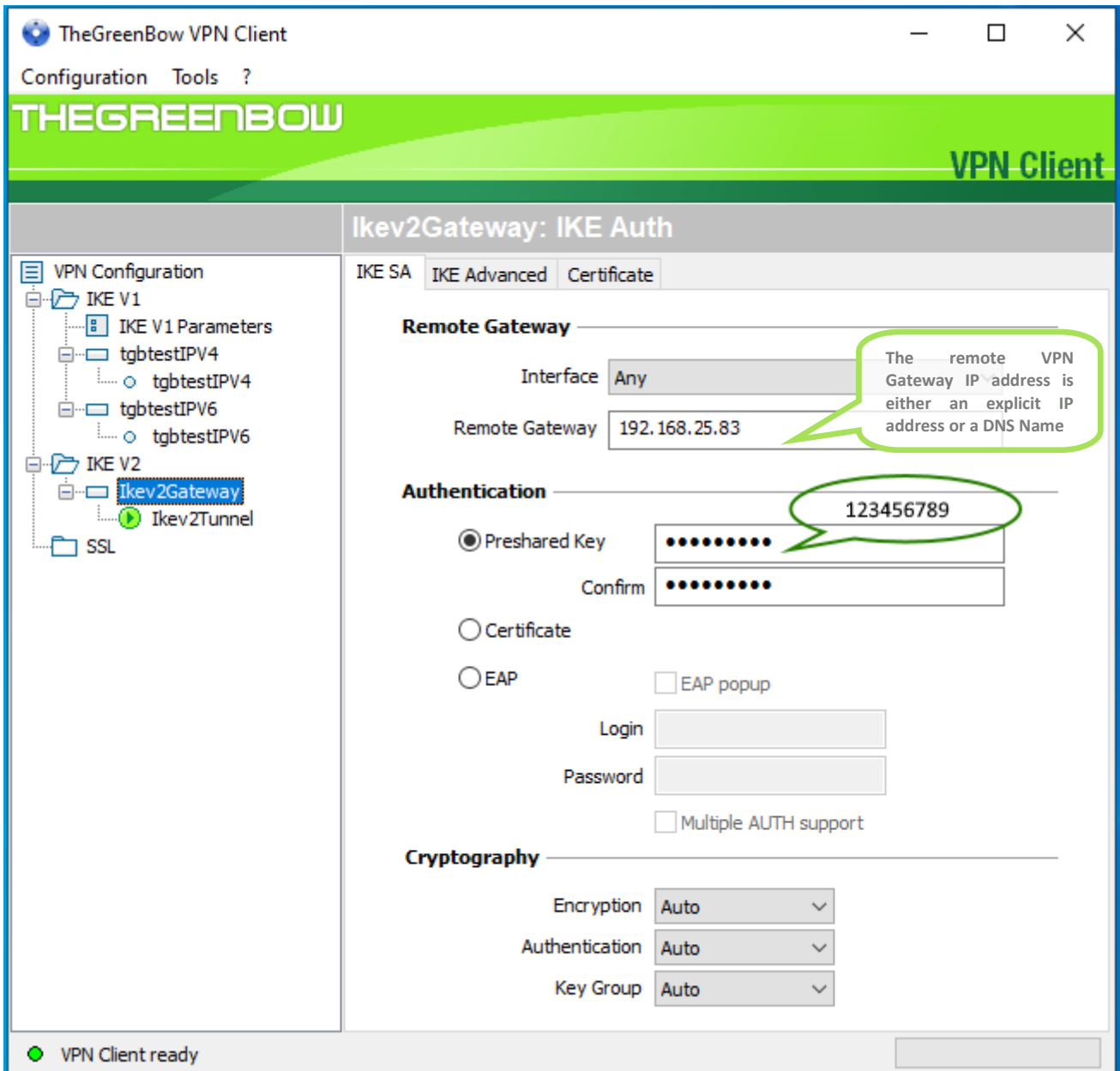


## 3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a ZyXEL USG20-VPN router via VPN connections.

To download the latest release of TheGreenBow IPsec VPN Client software, please go to [www.thegreenbow.com/vpn\\_down.html](http://www.thegreenbow.com/vpn_down.html).

### 3.1 VPN Client - IKE Auth Configuration



The configuration of the other tabs is left by default

This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the ZyXEL USG20-VPN router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.

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

The screenshot shows the 'TheGreenBow VPN Client' configuration window. The title bar includes 'Configuration Tools ?'. The main header features 'THEGREENBOW' on the left and 'VPN Client' on the right. A left-hand navigation pane shows a tree structure under 'VPN Configuration', including 'IKE V1', 'IKE V2', and 'SSL'. The 'IKE V2' folder is expanded, and 'Ikev2Tunnel' is selected. The main area is titled 'Ikev2Tunnel: Child SA' and has tabs for 'Child SA', 'Advanced', 'Automation', and 'Remote Sharing'. The 'Child SA' tab is active, and the 'IPV4' sub-tab is selected. The configuration fields are as follows:

- Traffic selectors:**
  - VPN Client address: 192 . 168 . 2 . 4
  - Address type: Subnet address
  - Remote LAN address: 192 . 168 . 1 . 0
  - Subnet mask: 255 . 255 . 255 . 0
  - Request configuration from the gateway
- Cryptography:**
  - Encryption: AES 128
  - Integrity: SHA1
  - Diffie-Hellman: DH2 (1024)
- Lifetime (sec.):**
  - Child SA Lifetime (sec): 1800

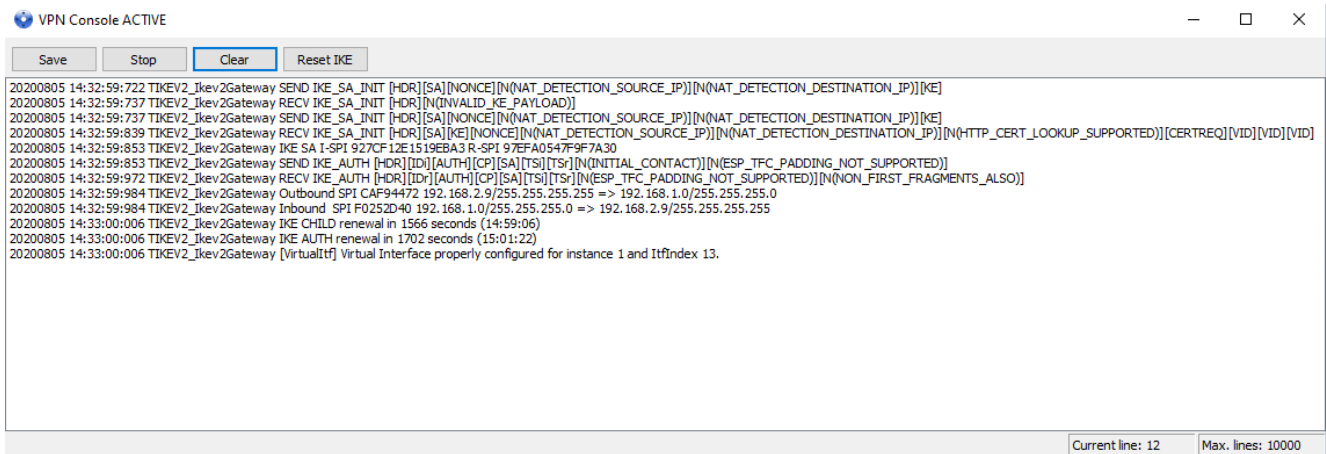
A callout box points to the 'VPN Client address' field with the text: 'Virtual IP address and Remote LAN address/subnet will be sent by Gateway through Mode CP'. At the bottom left, a green dot indicates 'VPN Client ready'.

The configuration of the other tabs is left by default

## 3.3 Open IPsec VPN tunnels

Once both ZyXEL USG20-VPN router and TheGreenBow IPsec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPsec traffic.

- 1/ Select menu "**Configuration**" and "**Save**" to take into account all modifications we've made on your VPN Client configuration.
- 2/ Double Click on your Child SA tunnel name or Click "**Open**" button in Connection panel to open tunnel.
- 3/ Select menu "**Tools**" and "**Console**" if you want to access to the IPsec VPN logs. The following example shows a successful connection between TheGreenBow IPsec VPN Client and a ZyXEL USG20- VPN router.



The screenshot shows a window titled "VPN Console ACTIVE" with a toolbar containing "Save", "Stop", "Clear", and "Reset IKE" buttons. The main area displays a log of network events. The log entries are as follows:

```
20200805 14:32:59:722 TIKEV2_Ikev2Gateway SEND IKE_SA_INIT [HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20200805 14:32:59:737 TIKEV2_Ikev2Gateway RECV IKE_SA_INIT [HDR][N(INVALID IKE_PAYLOAD)]
20200805 14:32:59:737 TIKEV2_Ikev2Gateway SEND IKE_SA_INIT [HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20200805 14:32:59:839 TIKEV2_Ikev2Gateway RECV IKE_SA_INIT [HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][N(HTTP_CERT_LOOKUP_SUPPORTED)][CERTREQ][VID][VID]
20200805 14:32:59:853 TIKEV2_Ikev2Gateway IKE SA I-SPI 927CF12E1519EBA3 R-SPI 97EFA0547F9F7A30
20200805 14:32:59:853 TIKEV2_Ikev2Gateway SEND IKE_AUTH [HDR][ID][AUTH][CP][SA][TSr][N(INITIAL_CONTACT)][N(ESP_TFC_PADDING_NOT_SUPPORTED)]
20200805 14:32:59:972 TIKEV2_Ikev2Gateway RECV IKE_AUTH [HDR][IDr][AUTH][CP][SA][TSr][N(ESP_TFC_PADDING_NOT_SUPPORTED)][N(NON_FIRST_FRAGMENTS_ALSO)]
20200805 14:32:59:984 TIKEV2_Ikev2Gateway Outbound SPI CAF94472 192.168.2.9/255.255.255.255 => 192.168.1.0/255.255.255.0
20200805 14:32:59:984 TIKEV2_Ikev2Gateway Inbound SPI F0252D40 192.168.1.0/255.255.255.0 => 192.168.2.9/255.255.255.255
20200805 14:33:00:006 TIKEV2_Ikev2Gateway IKE CHILD renewal in 1566 seconds (14:59:06)
20200805 14:33:00:006 TIKEV2_Ikev2Gateway IKE AUTH renewal in 1702 seconds (15:01:22)
20200805 14:33:00:006 TIKEV2_Ikev2Gateway [VirtualIf] virtual interface properly configured for instance 1 and IfIndex 13.
```

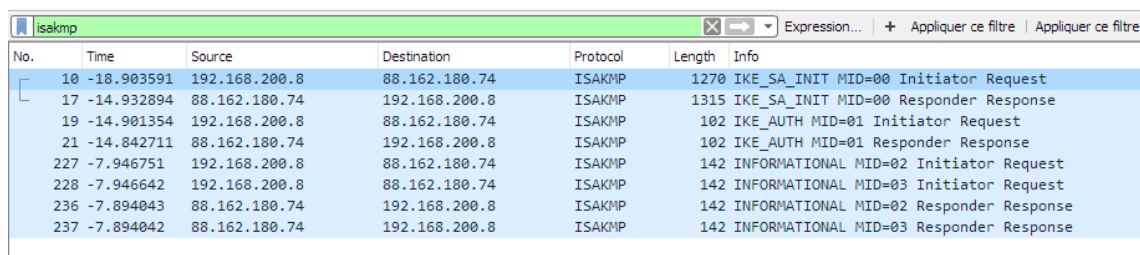
At the bottom right of the console window, it indicates "Current line: 12" and "Max. lines: 10000".

## 4 Tools in case of trouble

Configuring an IPsec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

### 4.1 A good network analyser: Wireshark

Wireshark is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website [www.wireshark.org](http://www.wireshark.org). It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation ([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 VPN IPsec Troubleshooting

### 5.1 “NO\_PROPOSAL\_CHOSEN” error (wrong IKE Auth)

```
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)]
```

If you have an “NO\_PROPOSAL\_CHOSEN” error you might have a wrong Phase 1 [IKE Auth], check if the encryption algorithms are the same on each side of the VPN tunnel.

### 5.2 “AUTHENTICATION\_FAILED” error

```
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
```

If you have an “AUTHENTICATION\_FAILED” error, it means that the certificate or the Pre-shared key is not matching. Check the Gateway if the user certificate or Pre-shared key is valid.

### 5.3 “No user certificate available for the connection” error

```
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.
```

Check if the certificate is selected or the Token (smartcard) is available on the computer.

### 5.4 “Remote ID rejected” error

```
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
```

The “Remote ID” value (see “Protocol” tab) does not match what the remote endpoint is expected.

## 5.5 “NO\_PROPOSAL\_CHOSEN” error (wrong CHILD SA)

```
20XX0913      16:25:14:933      TIKEV2_Tunnel      SEND      IKE_SA_INIT
[HDR] [SA] [NONCE] [N(NAT_DETECTION_SOURCE_IP)] [N(NAT_DETECTION_DESTINATION_IP)] [KE] [N(FRAGMENTATION_SUPPORTED)]
20XX0913      16:25:15:118      TIKEV2_Tunnel      RECV      IKE_SA_INIT
[HDR] [SA] [KE] [NONCE] [N(NAT_DETECTION_SOURCE_IP)] [N(NAT_DETECTION_DESTINATION_IP)] [CERTREQ] [N(MULTIPLE_AUTH_SUPPORTED)]
20XX0913 16:25:15:118 TIKEV2_Tunnel IKE SA I-SPI E389FC49EE7078F1 R-SPI 00F37D557ED307FC
20XX0913      16:25:15:118      TIKEV2_Tunnel      SEND      IKE_AUTH
[HDR] [IDi] [CERT] [CERTREQ] [AUTH] [CP] [SA] [TSi] [TSr] [N(INITIAL_CONTACT)] [N(ESP_TFC_PADDING_NOT_SUPPORTED)]
20XX0913      16:25:15:165      TIKEV2_Tunnel      RECV      IKE_AUTH
[HDR] [IDr] [CERT] [AUTH] [CP] [N(AUTH_LIFETIME)] [N(NO_PROPOSAL_CHOSEN)]
20XX0913 16:25:15:165 TIKEV2_Tunnel IKE AUTH renewal in 1654 seconds (16:52:49)
20XX0913      16:25:15:165      TIKEV2_Tunnel      SEND      CHILD_SA
[HDR] [SA] [NONCE] [KE] [TSi] [TSr] [N(ESP_TFC_PADDING_NOT_SUPPORTED)]
20XX0913 16:25:15:202 TIKEV2_Tunnel RECV CHILD_SA [HDR] [N(NO_PROPOSAL_CHOSEN)]
20XX0913 16:25:15:202 TIKEV2_Tunnel Remote endpoint sends error NO_PROPOSAL_CHOSEN
20XX0913 16:25:15:202 TIKEV2_Tunnel SEND INFORMATIONAL [HDR] [DELETE]
```

If you have an “NO\_PROPOSAL\_CHOSEN” error, check that the “Child SA” encryption algorithms are the same on each side of the VPN Tunnel.

## 5.6 “FAILED\_CP\_REQUIRED” error

```
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
```

If you have an “FAILED\_CP\_REQUIRED” error, then the Gateway is configured to use Mode CP. Go to Traffic selectors and enable "Request configuration from the gateway".

## 5.7 I clicked on “Open tunnel”, but nothing happens.

```
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.
```

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPsec Client uses UDP port 500.

Check if the remote server is online.

## 5.8 The VPN tunnel is up but I can't ping!

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Child SA settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP and if the protocol 50 is allowed to pass traffic in your firewalls.
- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark for example). You will have an indication that encryption works.
- Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install Wireshark ([www.wireshark.org](http://www.wireshark.org)) on one of your target computers. You can check that your pings arrive inside the LAN.

## 6 Contacts

News and updates on TheGreenBow web site: [www.thegreenbow.com](http://www.thegreenbow.com)

Technical support by email at: [support@thegreenbow.com](mailto:support@thegreenbow.com)

Sales contacts by email at: [sales@thegreenbow.com](mailto:sales@thegreenbow.com)



# **Secure, Strong, Simple**

TheGreenBow Security Software