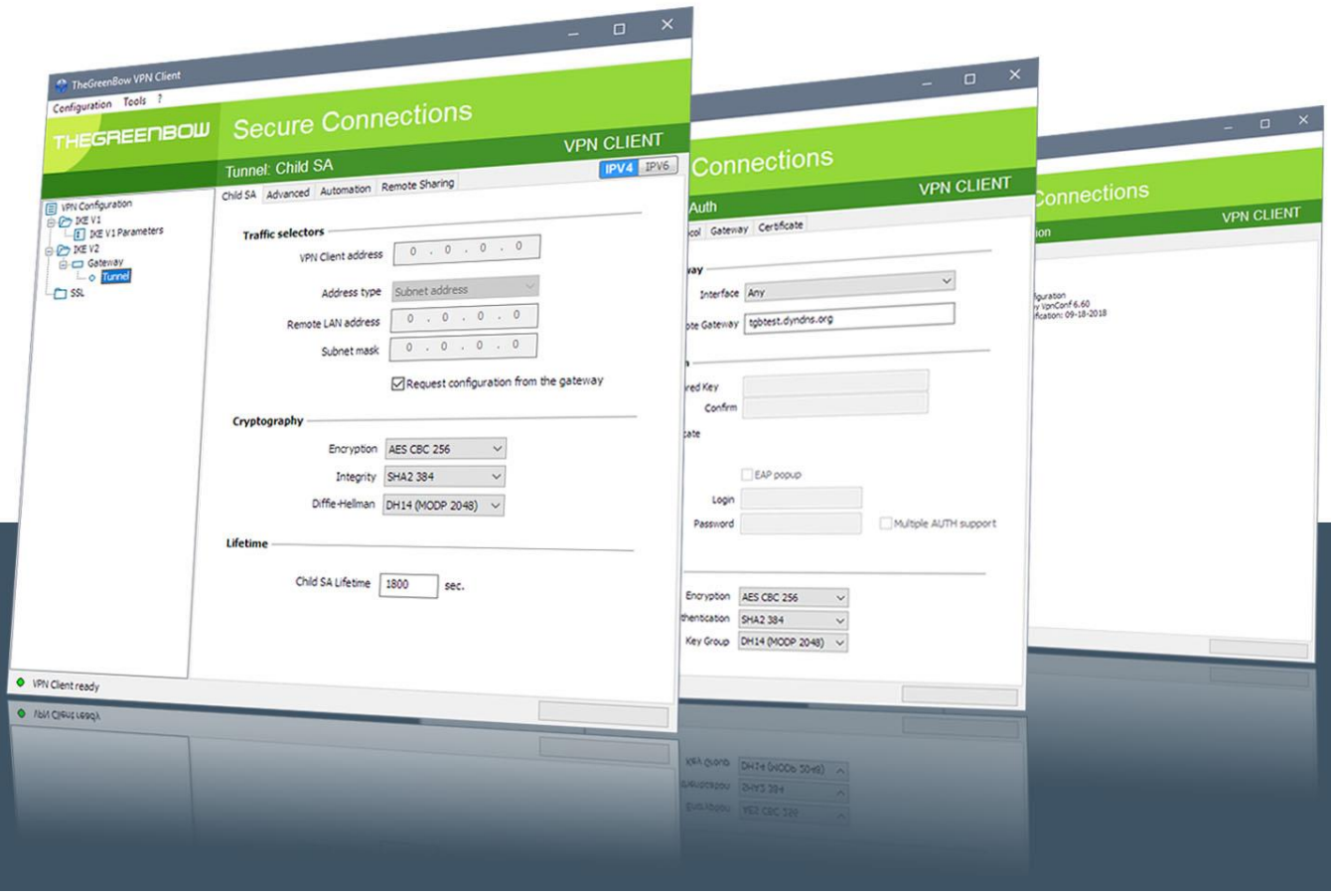


TheGreenBow IPsec VPN Client

Configuration Guide
ZyXEL USG20-VPN

Protocol – IKEv1

Website: **www.thegreenbow.com**
Contact: **support@thegreenbow.com**

Table of Contents

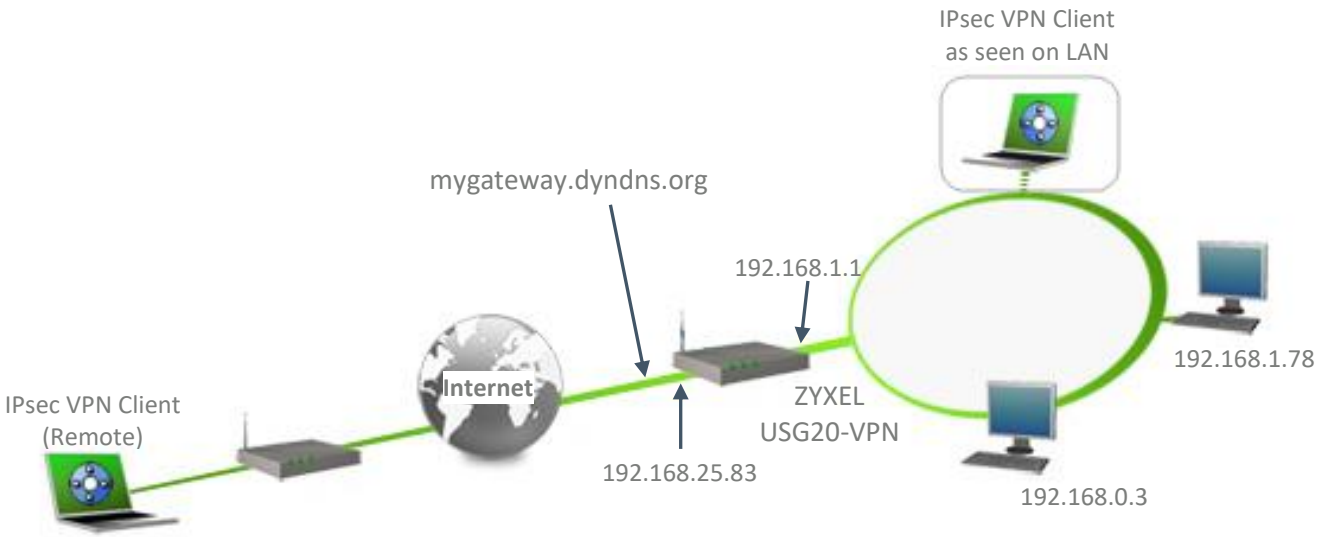
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a ZyXEL USG20-VPN 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

Depending on the firmware version, ZyXEL USG20-VPN may not support NAT-T and as a consequence the IPsec VPN Client software could not connect if standing on a LAN behind (e.g. router at home, ...).

1.4 ZyXEL USG20-VPN Gateway

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

1.5 ZyXEL USG20-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**

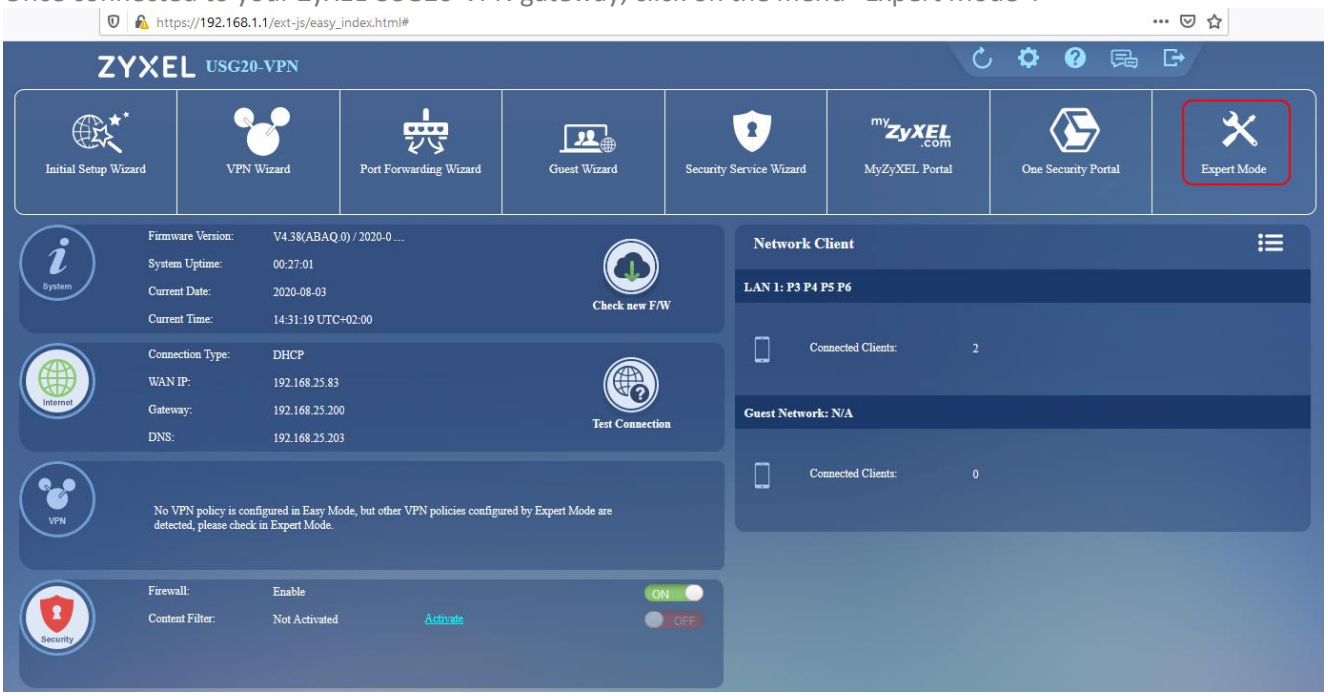
ZyXEL USG20-VPN Product page	**https://www.zyxel.com/products_services/Business-Firewall-USG20-VPN-USG20W-VPN/**
ZyXEL USG20-VPN User Guide	**ftp://ftp.zyxel.fr/ftp_download/USG20W-VPN/user_guide/USG20W-VPN_V4.16_Ed1.pdf**

2 ZyXEL USG20-VPN configuration

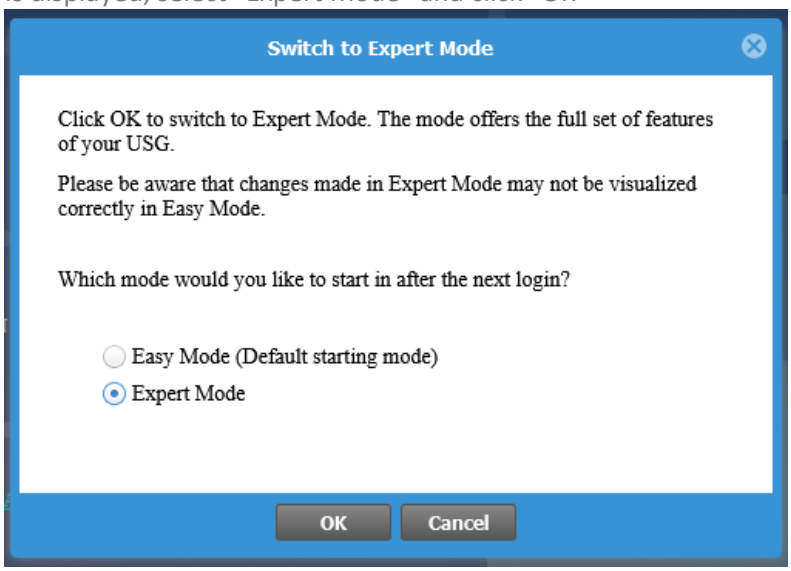
This section describes how to build an IPsec VPN configuration with your ZyXEL USG20-VPN router.

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”:

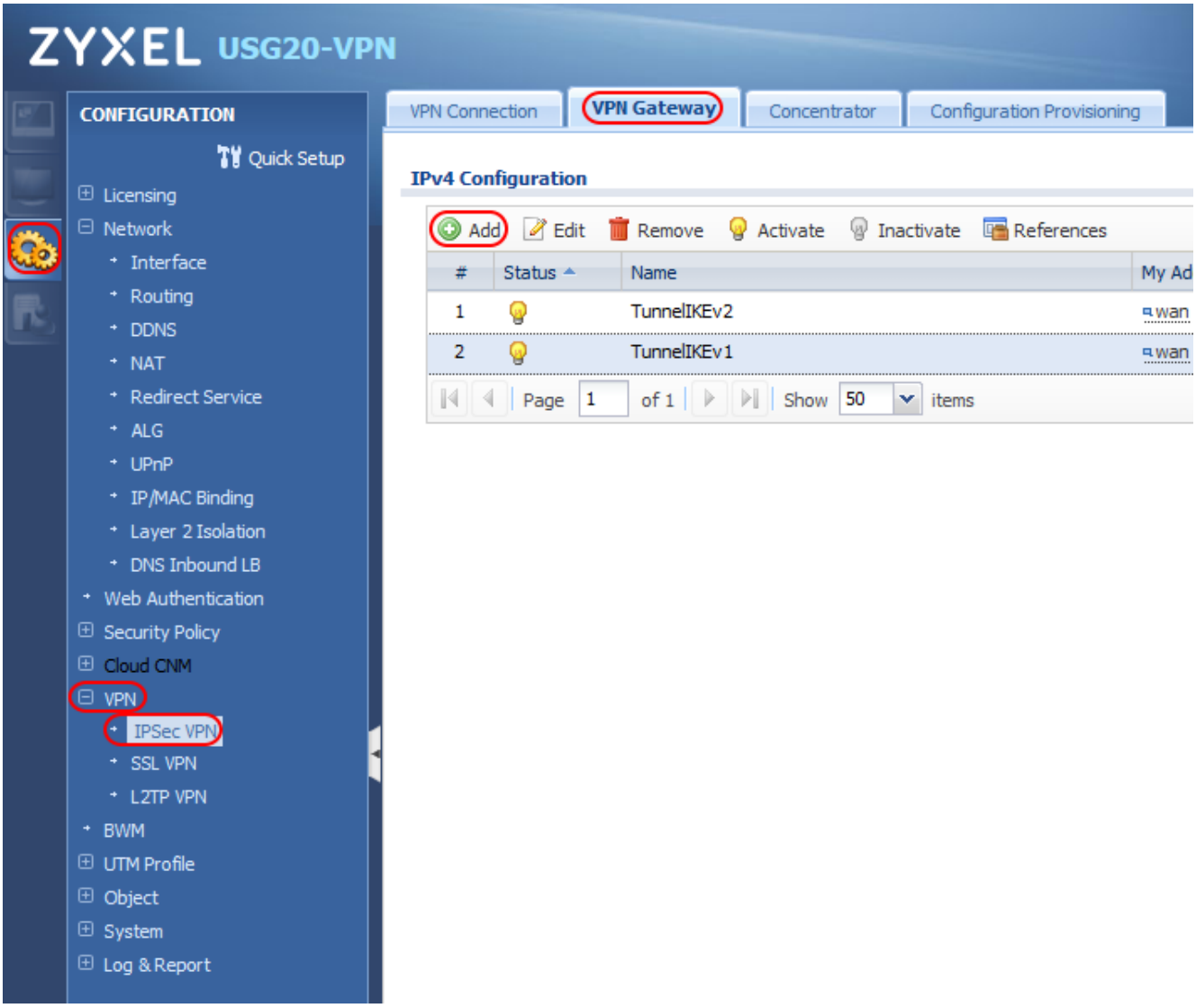


The following window is displayed, select “Expert Mode” and click “OK”



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 TunnelIKEv1

Hide Advanced Settings | Create New Object

General Settings

Enable

VPN Gateway Name: TunnelIKEv1

IKE Version

IKEv1

IKEv2

Gateway Settings

My Address

Interface: wan — DHCP client -- 192.168.25.83/255.255.255.0

Domain Name / IPv4

Peer Gateway Address

Static Address — Primary: 0.0.0.0 — Secondary: 0.0.0.0

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

Dynamic Address

Authentication

Pre-Shared Key: ••••••••• (123456789)

unmasked

Certificate: default (See My Certificates)

User Based PSK: admin

Advance

Local ID Type: IPv4

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Advance

Proposal

Add | Edit | Remove

#	Encryption	Authentication
1	AES128	SHA1

Key Group: DH2

NAT Traversal

Dead Peer Detection (DPD)

X-Auth

Enable Extended Authentication

Server Mode

AAA Method: Please select one...

Allowed User: Please select one...

Client Mode

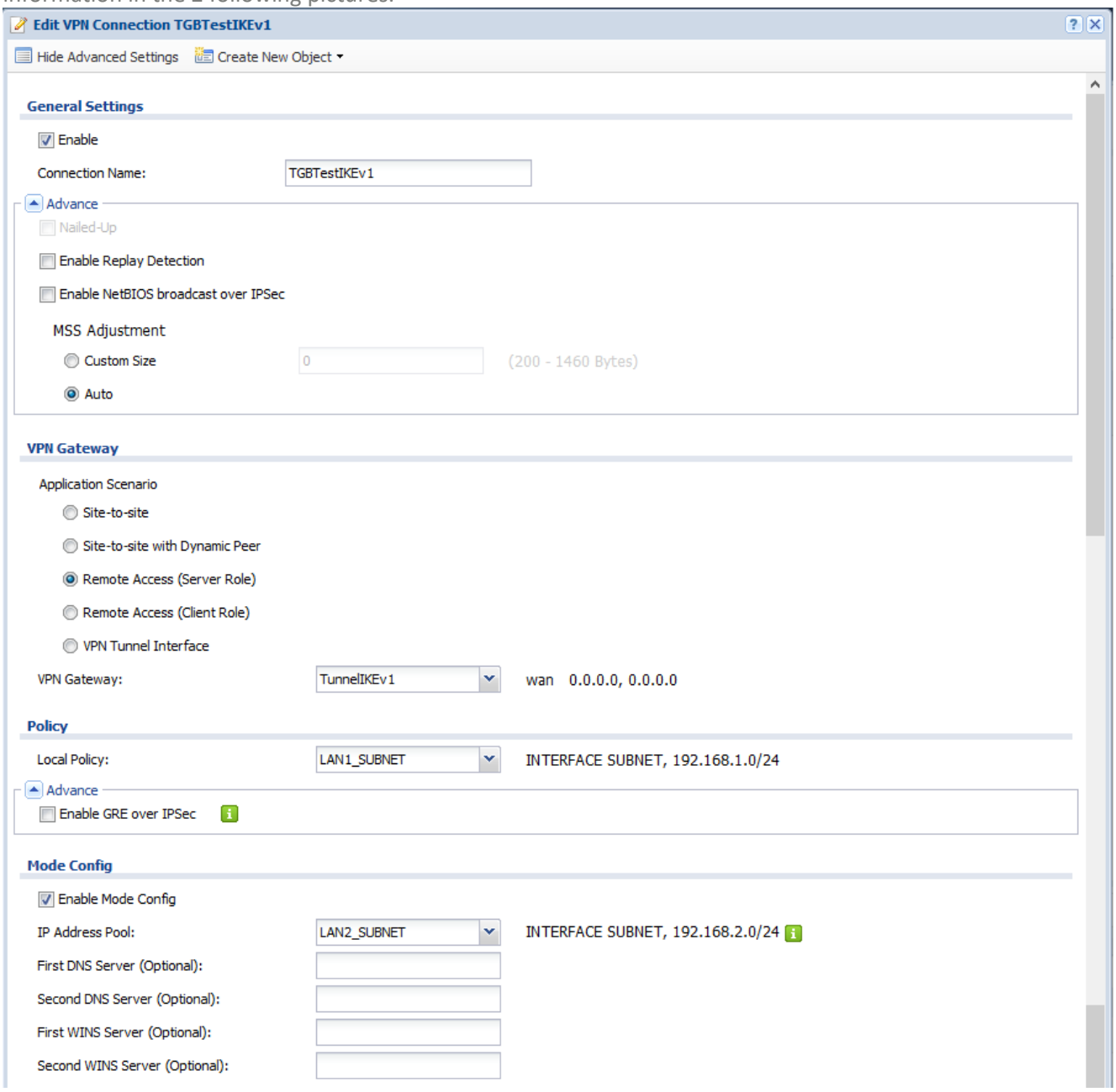
User Name :

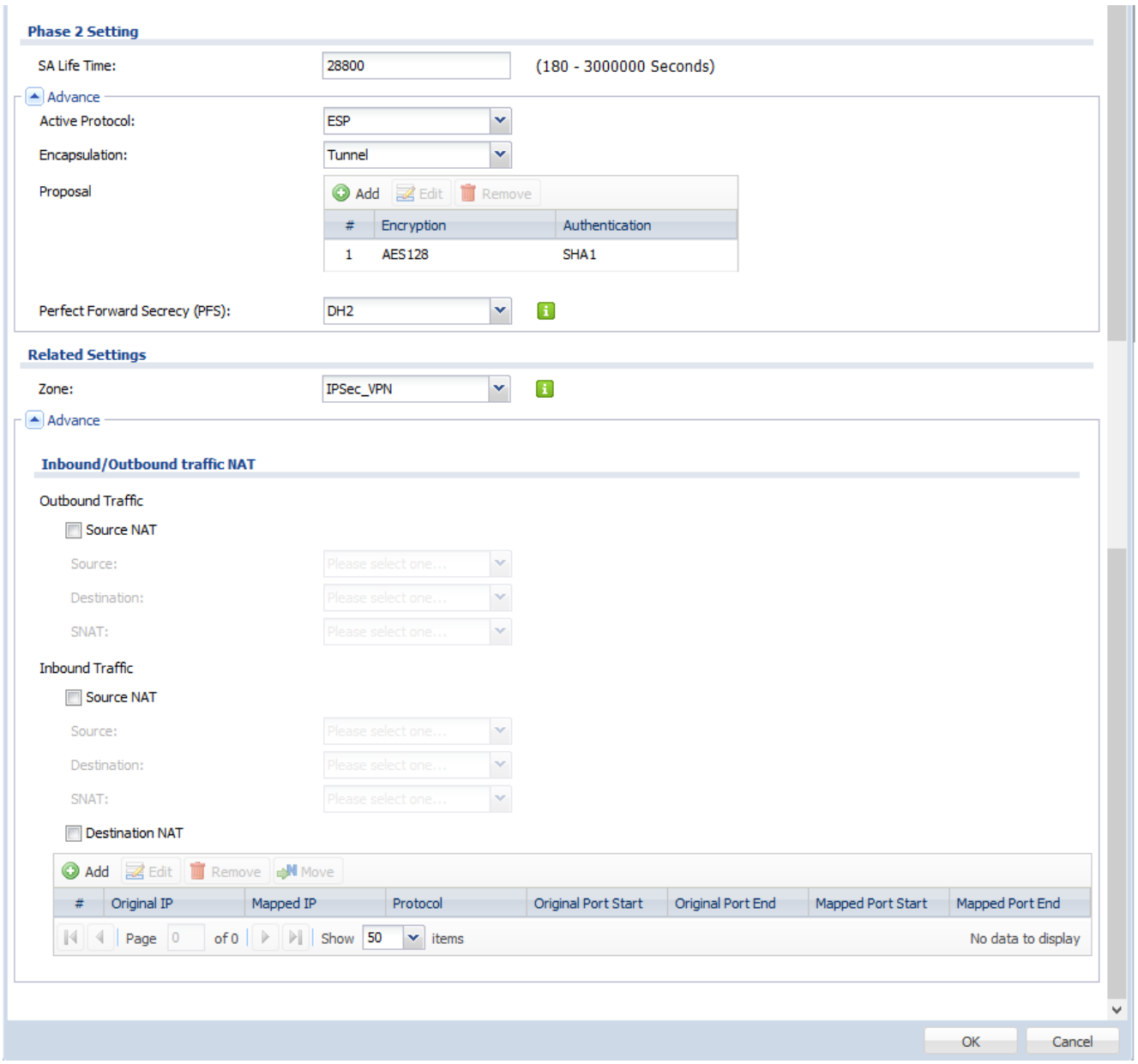
Password:

Retype to Confirm:

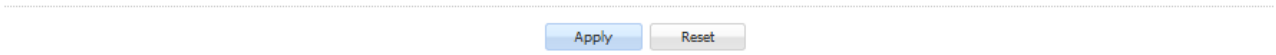
OK | Cancel

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





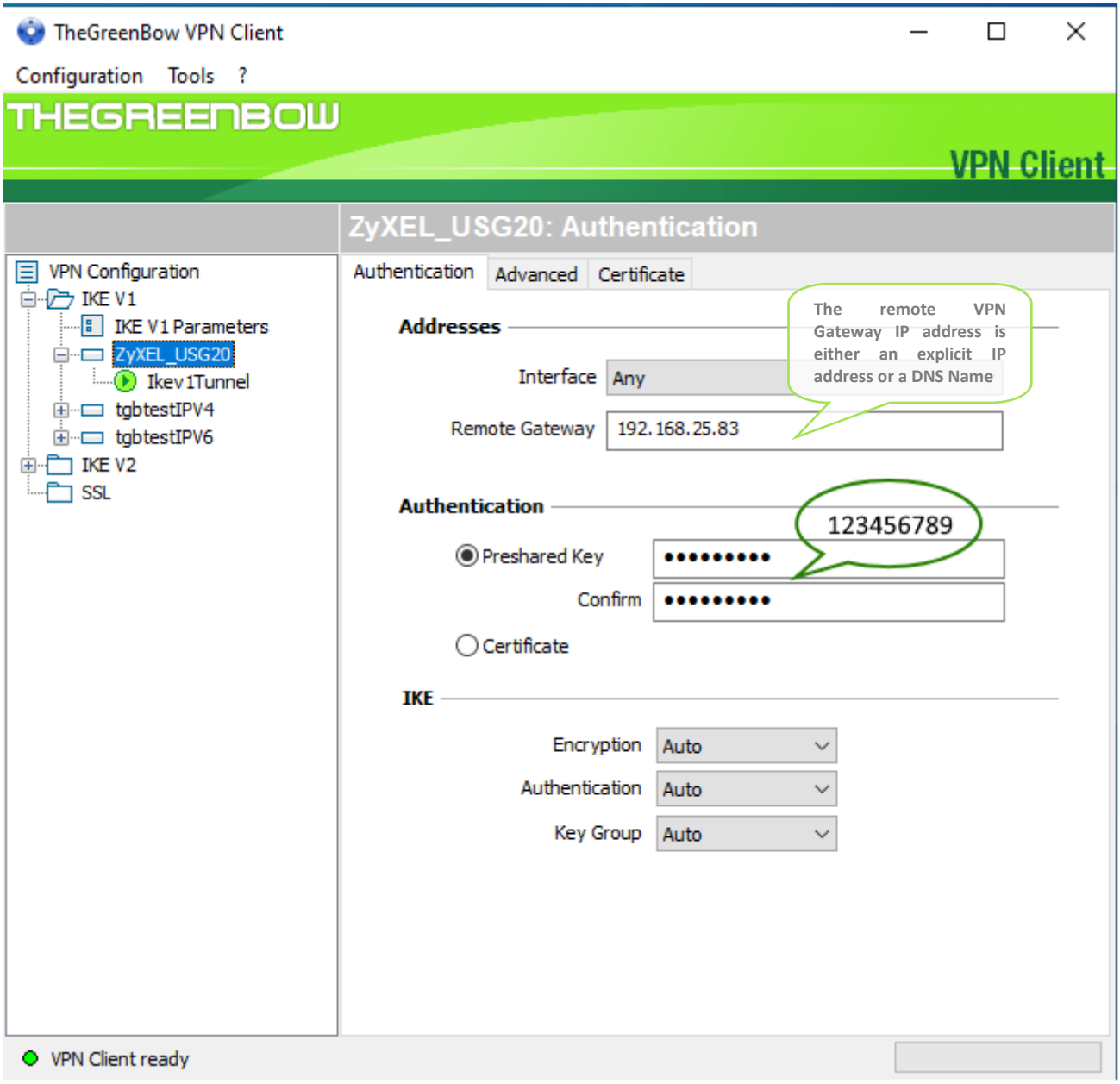
Once all those configuration done, click on the button “Apply” at the bottom of the router window.

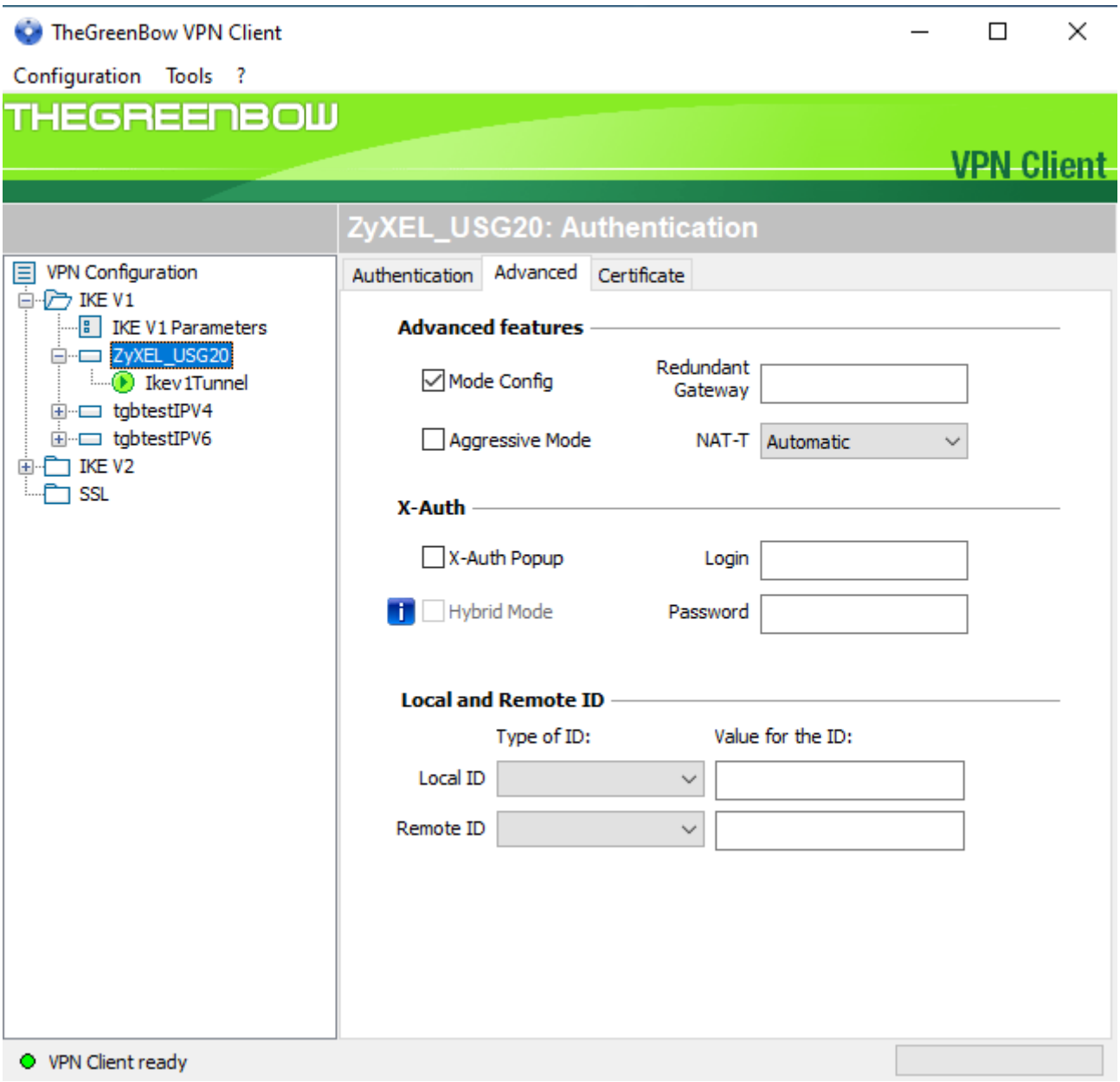


3 TheGreenBow IPsec VPN Client configuration

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.**

3.1 VPN Client Phase 1 (IKE) Configuration

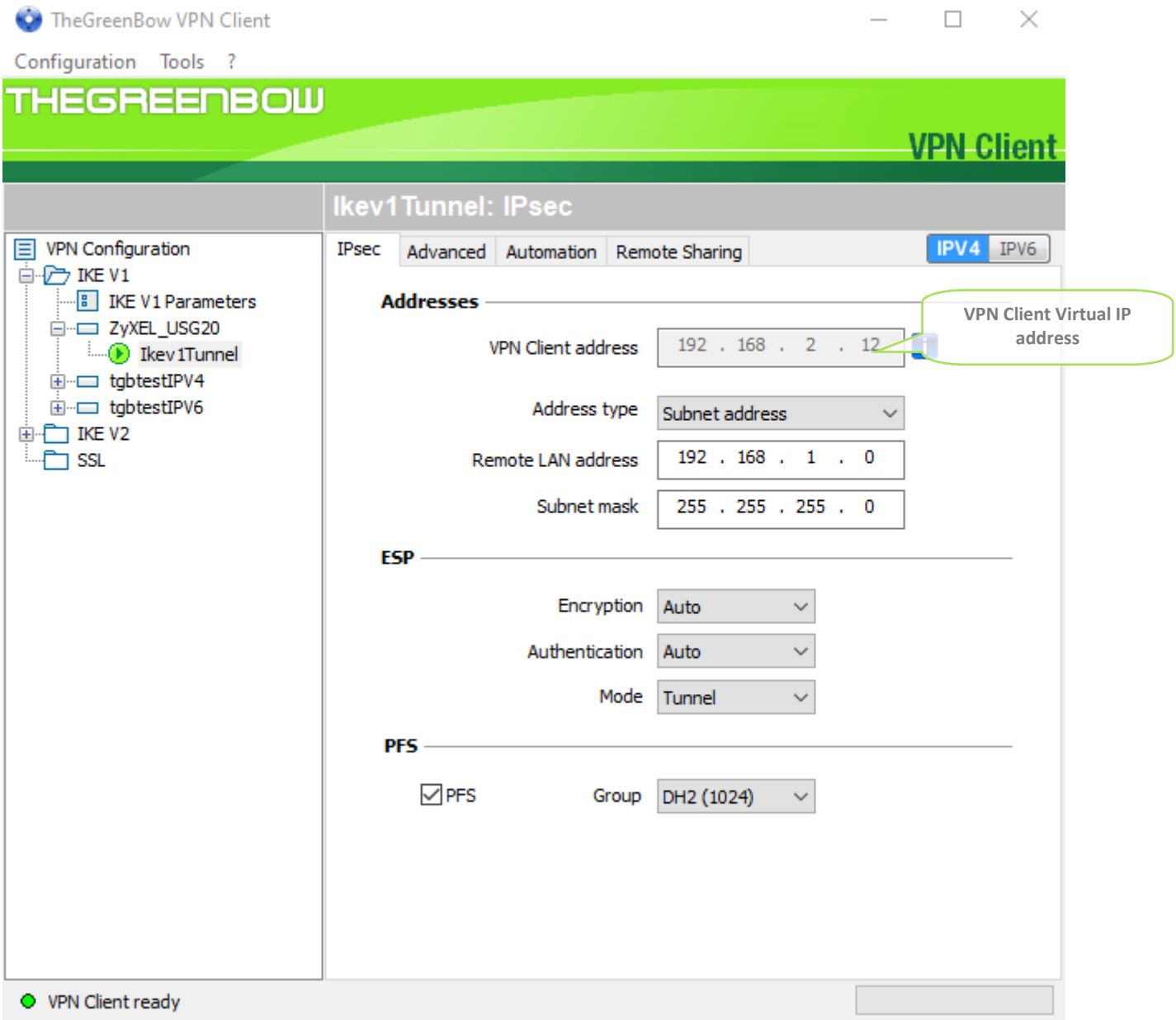




The configuration of the “Certificate” tabs is left by default

You may use either Pre-shared key, Certificates, USB Tokens, OTP Token (One Time Password) or X-Auth combined for User Authentication with the ZyXEL USG20-VPN router. 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 (IPsec) Configuration



The configuration of the other tabs is left by default

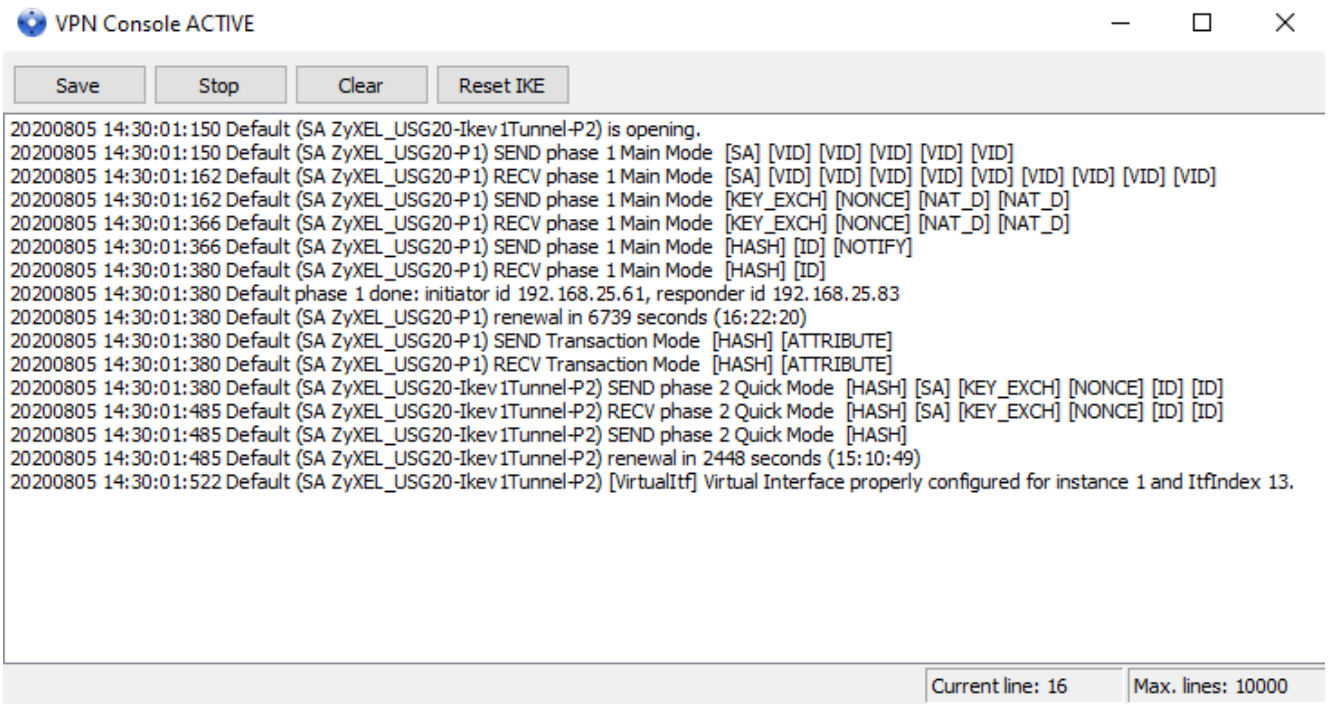
3.3 Open IPsec VPN tunnels

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.

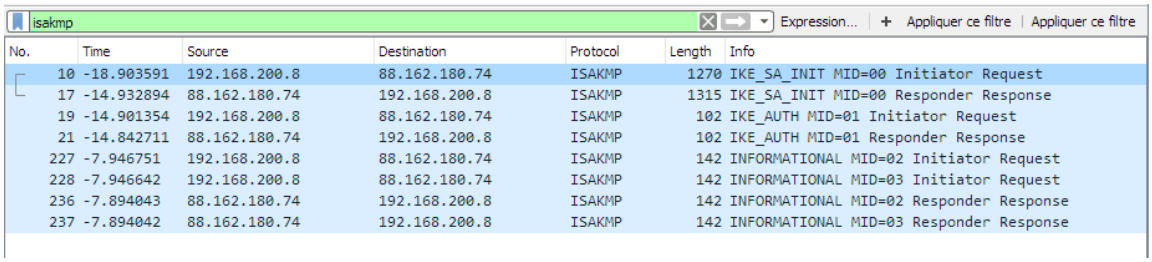


4 Tools in case of trouble

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**. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (**www.wireshark.org/docs/**).



isakmp | Expression... | + Appliquer ce filtre | Appliquer ce filtre

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 “PAYLOAD MALFORMED” error (wrong Phase 1 [SA])

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an “PAYLOAD MALFORMED” error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 “INVALID COOKIE” error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
```

If you have an “INVALID COOKIE” error, it means that one of the endpoints is using a SA that is no more in use. Reset the VPN connection on each side.

5.3 “no keystate” error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default IPsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Check if the Pre-shared key is correct or if the local ID is correct (see “Advanced” tab). You should have more information in the remote endpoint logs.

5.4 “received remote ID other than expected” error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected support@thegreenbow.fr
```

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

5.5 “NO PROPOSAL CHOSEN” error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72:
195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode  [SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

If you have an “NO PROPOSAL CHOSEN” error, check that the “Phase 2” encryption algorithms are the same on each side of the VPN Tunnel.

Check “Phase 1” algorithms if you have this:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 “INVALID ID INFORMATION” error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72:
195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode  [SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

If you have an “INVALID ID INFORMATION” error, check if “Phase 2" ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type (“Subnet address” and “Single address”). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

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

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPsec Client uses UDP port 500 and protocol ESP (protocol 50).

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 Phase 2 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
- 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**) 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**

Technical support by email at: **support@thegreenbow.com**

Sales contacts by email at: **sales@thegreenbow.com**

Secure, Strong, Simple

TheGreenBow Security Software