

TheGreenBow IPsec VPN Client

Configuration Guide

ZyXEL USG20-VPN

Protocol – IKEv1

Website: www.thegreenbow.com
Contact: 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 Gateway | 3 |
| 1.5 | ZyXEL USG20-VPN Gateway product info | 3 |
| 2 | ZyXEL USG20-VPN configuration | 4 |
| 3 | TheGreenBow IPsec VPN Client configuration | 9 |
| 3.1 | VPN Client Phase 1 (IKE) Configuration | 9 |
| 3.2 | VPN Client Phase 2 (IPsec) Configuration | 11 |
| 3.3 | Open IPsec VPN tunnels..... | 12 |
| 4 | Tools in case of trouble..... | 13 |
| 4.1 | A good network analyser: Wireshark..... | 13 |
| 5 | VPN IPsec Troubleshooting..... | 14 |
| 5.1 | “PAYLOAD MALFORMED” error (wrong Phase 1 [SA]) | 14 |
| 5.2 | “INVALID COOKIE” error | 14 |
| 5.3 | “no keystate” error | 14 |
| 5.4 | “received remote ID other than expected” error | 14 |
| 5.5 | “NO PROPOSAL CHOSEN” error | 15 |
| 5.6 | “INVALID ID INFORMATION” error | 15 |
| 5.7 | I clicked on “Open tunnel”, but nothing happens. | 15 |
| 5.8 | The VPN tunnel is up but I can’t ping! | 16 |
| 6 | Contacts | 17 |

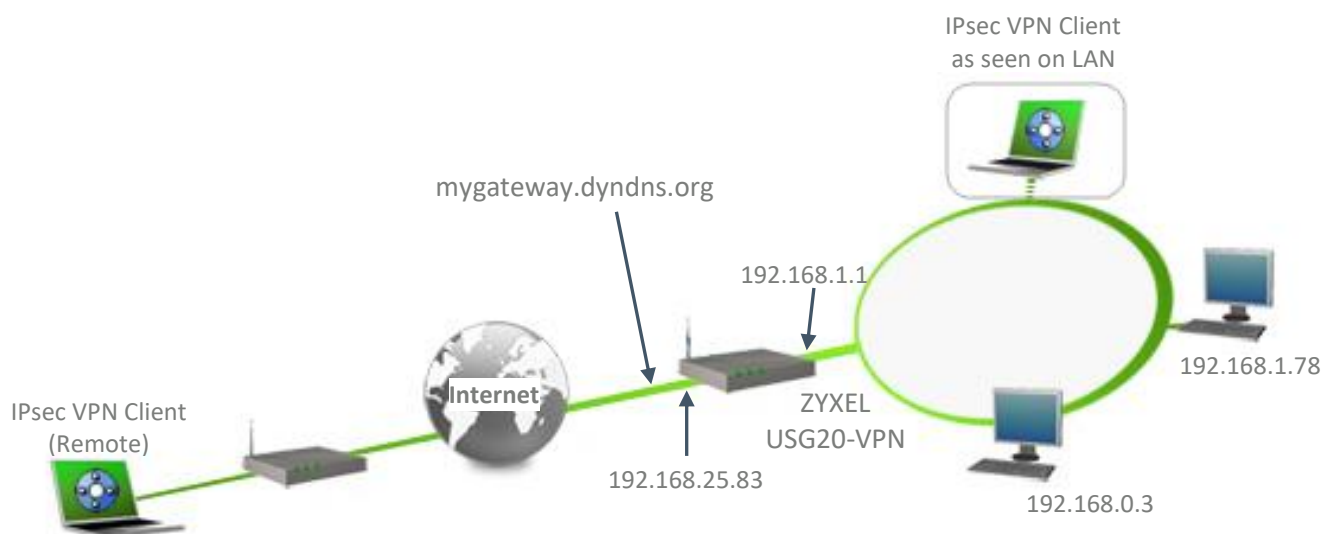
1 Introduction

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

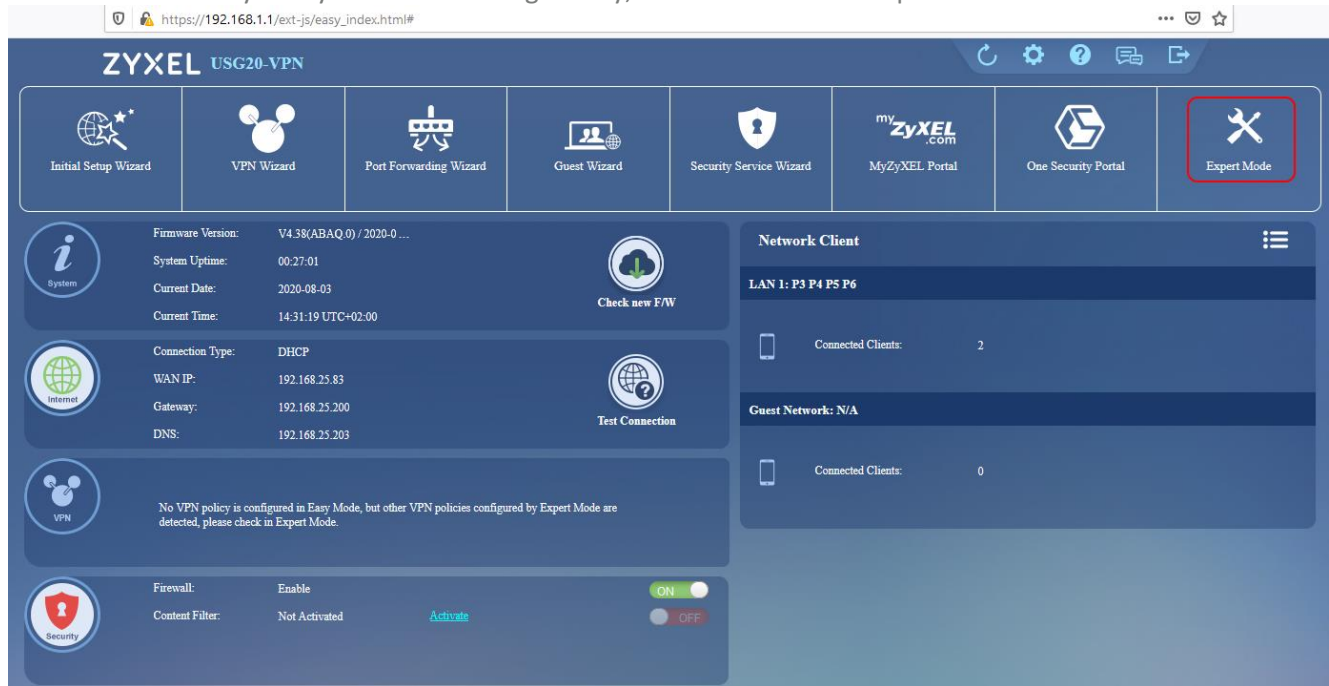
ftp://ftp.zyxel.fr/ftp_download/USG20W-VPN/user_guide/USG20W-VPN_V4.16_Ed1.pdf

2 ZyXEL USG20-VPN configuration

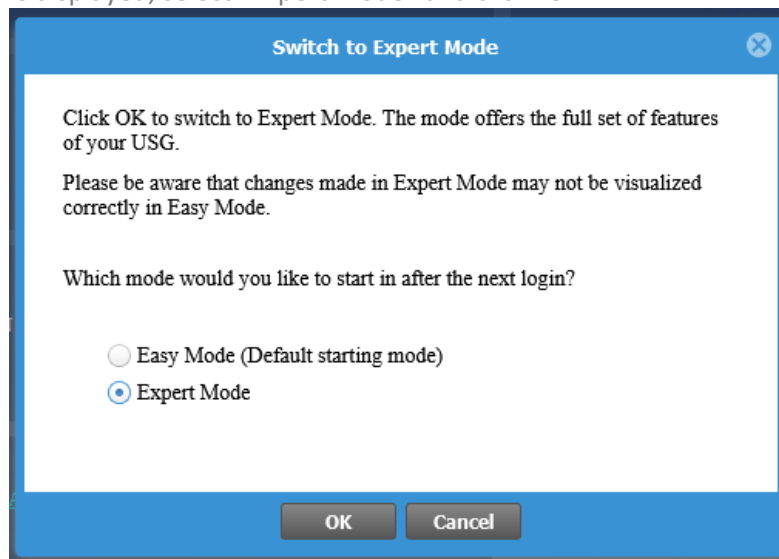
This section describes how to build an IPsec VPN configuration with your ZyXEL USG20-VPN router.

| 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”:



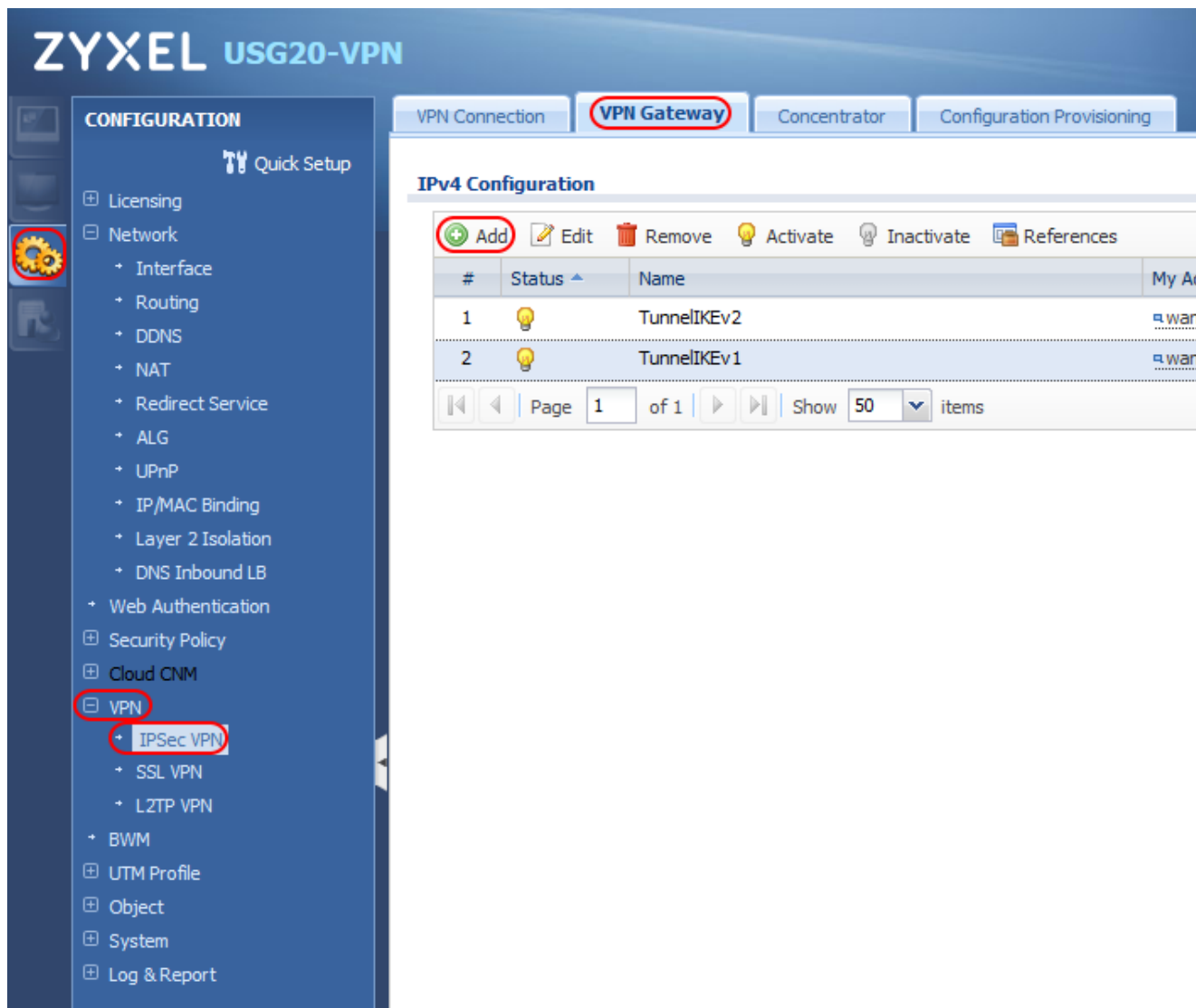
The following window is displayed, select “Expert Mode” and click “OK”



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 TunnelIKEv1 [?] [X]

Hide 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 ⓘ
Primary
Secondary
 Fall back to Primary Peer Gateway when possible
Fall Back Check Interval: (60-86400 seconds)

Dynamic Address ⓘ

Authentication

Pre-Shared Key
 unmasked

Certificate (See [My Certificates](#))
 User Based PSK ⓘ

Advance

Local ID Type:
Content:
Peer ID Type:
Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)
Negotiation Mode:

Advance

Proposal

| Add Edit Remove | | |
|-----------------|------------|----------------|
| # | Encryption | Authentication |
| 1 | AES 128 | SHA1 |

Key Group:

NAT Traversal
 Dead Peer Detection (DPD)

X-Auth

Enable Extended Authentication

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 TGBTestIKEv1

Hide Advanced Settings Create New Object

General Settings

Enable

Connection Name:

Advance

Nailed-Up

Enable Replay Detection

Enable NetBIOS broadcast over IPsec

MSS Adjustment

Custom Size (200 - 1460 Bytes)

Auto

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: wan 0.0.0.0, 0.0.0.0

Policy

Local Policy: INTERFACE SUBNET, 192.168.1.0/24

Advance

Enable GRE over IPsec i

Mode Config

Enable Mode Config

IP Address Pool: INTERFACE SUBNET, 192.168.2.0/24 i

First DNS Server (Optional):

Second DNS Server (Optional):

First WINS Server (Optional):

Second WINS Server (Optional):

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

Advance

Active Protocol:

Encapsulation:

Proposal

| + Add Edit Remove | | |
|-------------------|------------|----------------|
| # | Encryption | Authentication |
| 1 | AES128 | SHA1 |

Perfect Forward Security (PFS): i

Related Settings

Zone: i

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

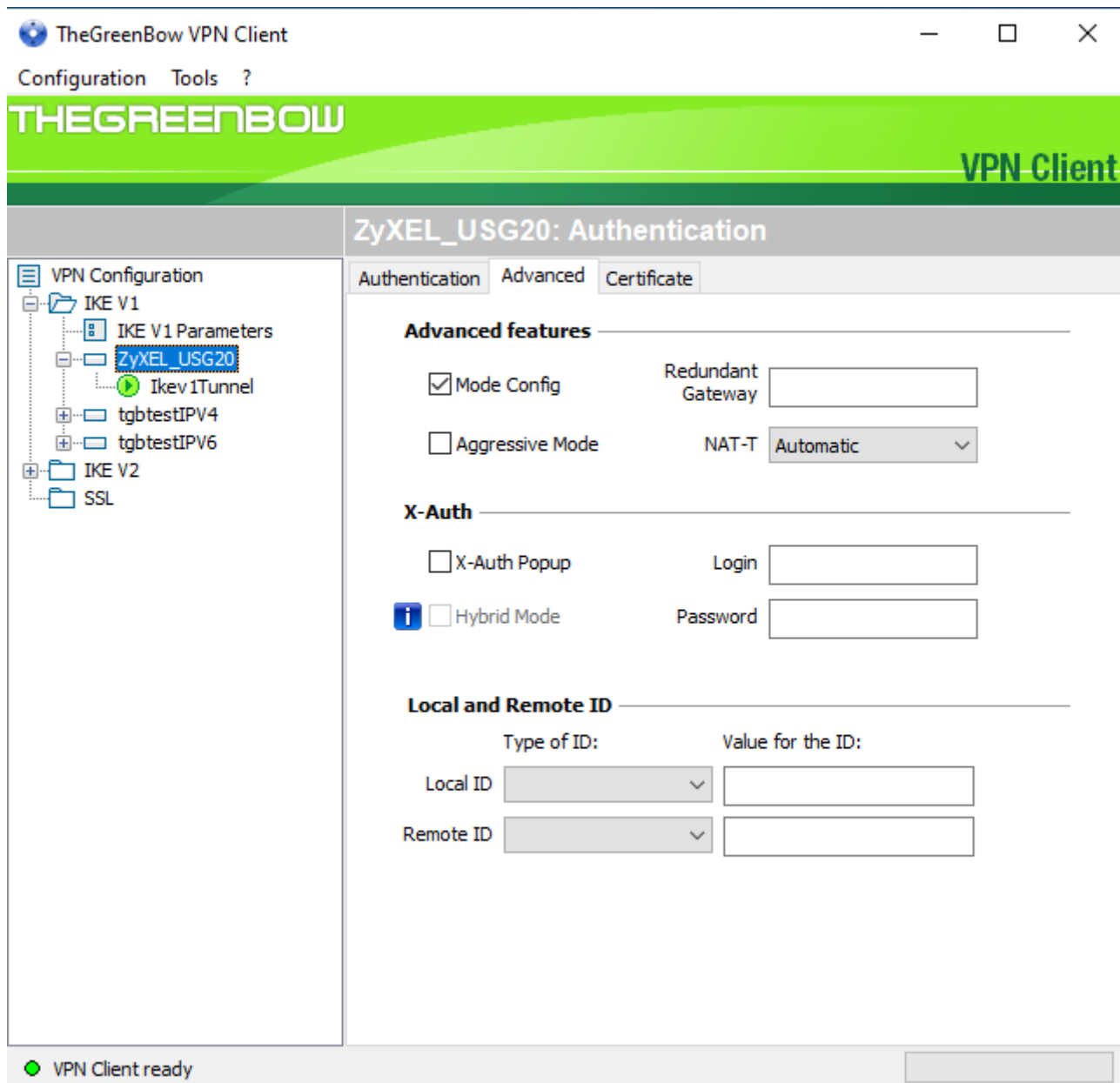
3 TheGreenBow IPsec VPN Client configuration

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.

3.1 VPN Client Phase 1 (IKE) Configuration

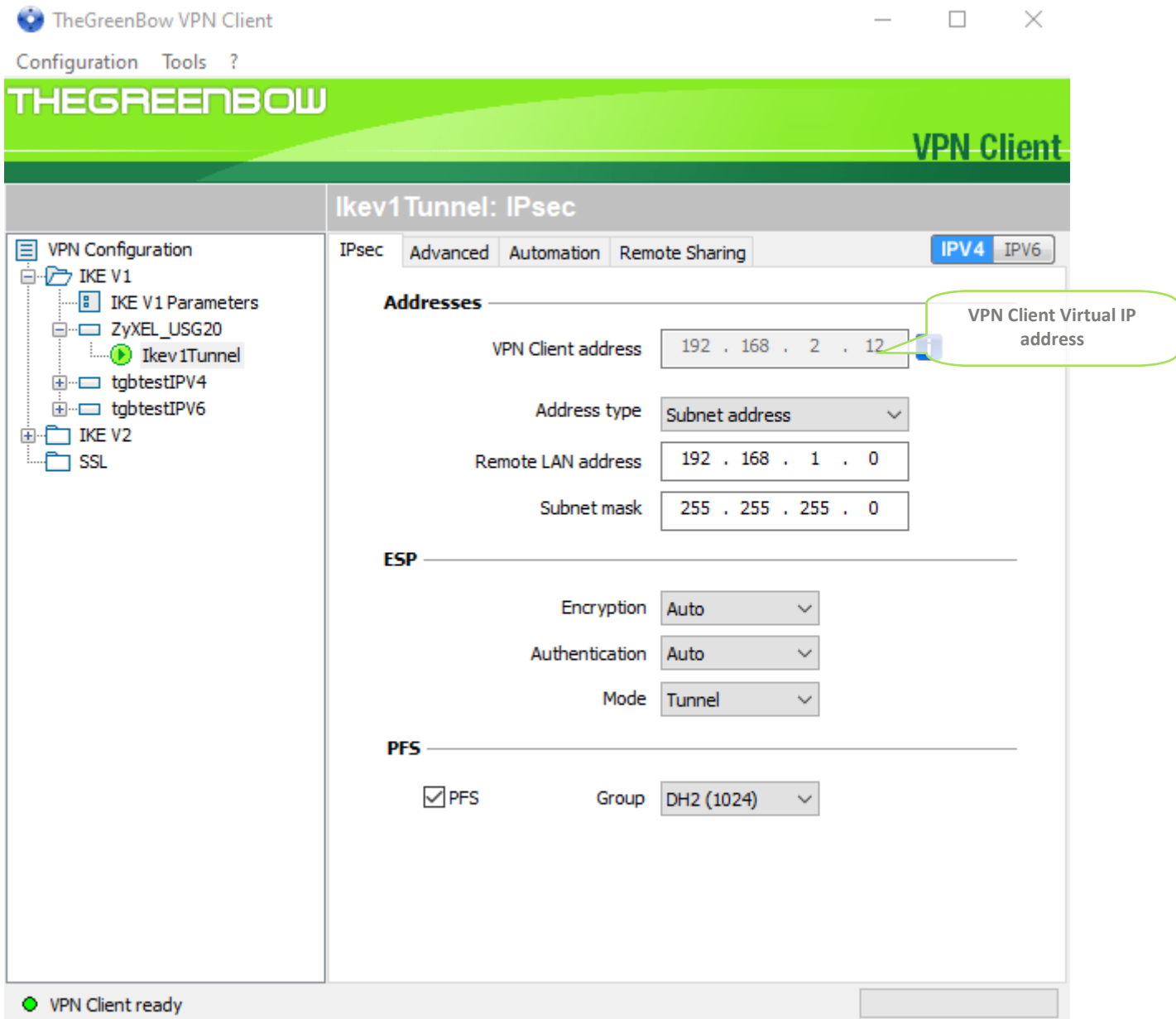
The screenshot shows the 'ZyXEL_USG20: Authentication' configuration window in TheGreenBow VPN Client. The window has a title bar with 'TheGreenBow VPN Client' and standard window controls. Below the title bar is a menu bar with 'Configuration' and 'Tools ?'. The main area is divided into a left sidebar and a right main panel. The sidebar shows a tree view under 'VPN Configuration' with 'IKE V1' expanded, containing 'IKE V1 Parameters', 'ZyXEL_USG20' (selected), 'Ikev1Tunnel', 'tgbtestIPV4', and 'tgbtestIPV6'. Below that are 'IKE V2' and 'SSL'. The main panel has tabs for 'Authentication', 'Advanced', and 'Certificate'. The 'Authentication' tab is active. It contains three sections: 'Addresses', 'Authentication', and 'IKE'. In the 'Addresses' section, 'Interface' is set to 'Any' and 'Remote Gateway' is '192.168.25.83'. A callout bubble points to the 'Remote Gateway' field with the text: 'The remote VPN Gateway IP address is either an explicit IP address or a DNS Name'. In the 'Authentication' section, 'Preshared Key' is selected, and the key '123456789' is entered in the first field, with a callout bubble around it. The 'Confirm' field is empty. The 'Certificate' option is unselected. In the 'IKE' section, 'Encryption', 'Authentication', and 'Key Group' are all set to 'Auto'. At the bottom left, there is a status indicator: a green dot followed by 'VPN Client ready'. At the bottom right, there is a grey button.



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

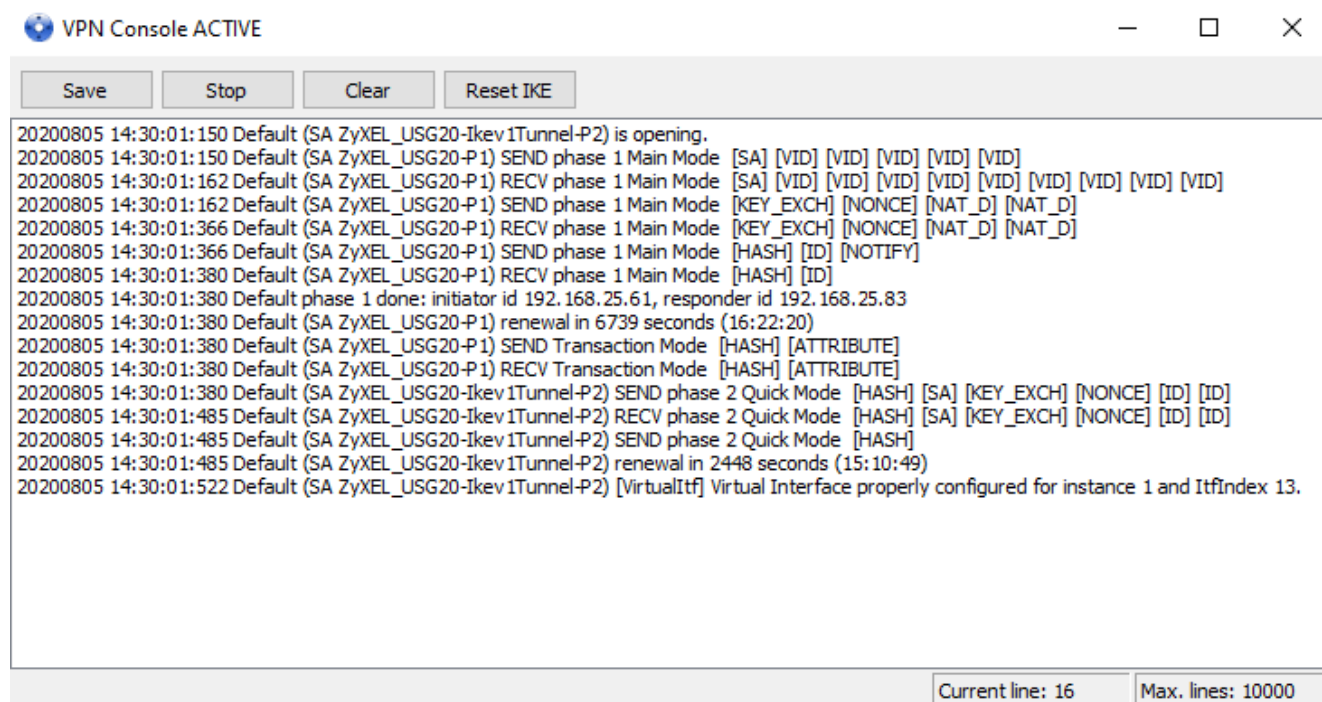


The configuration of the other tabs is left by default

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.



The screenshot shows a window titled "VPN Console ACTIVE" with standard window controls (minimize, maximize, close). Below the title bar is a toolbar with buttons for "Save", "Stop", "Clear", and "Reset IKE". The main area contains a log of system messages. The log shows the following sequence of events:

```
20200805 14:30:01:150 Default (SA ZyXEL_USG20-Ikev1Tunnel-P2) is opening.
20200805 14:30:01:150 Default (SA ZyXEL_USG20-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
20200805 14:30:01:162 Default (SA ZyXEL_USG20-P1) RECV phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID] [VID] [VID] [VID]
20200805 14:30:01:162 Default (SA ZyXEL_USG20-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20200805 14:30:01:366 Default (SA ZyXEL_USG20-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20200805 14:30:01:366 Default (SA ZyXEL_USG20-P1) SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
20200805 14:30:01:380 Default (SA ZyXEL_USG20-P1) RECV phase 1 Main Mode [HASH] [ID]
20200805 14:30:01:380 Default phase 1 done: initiator id 192.168.25.61, responder id 192.168.25.83
20200805 14:30:01:380 Default (SA ZyXEL_USG20-P1) renewal in 6739 seconds (16:22:20)
20200805 14:30:01:380 Default (SA ZyXEL_USG20-P1) SEND Transaction Mode [HASH] [ATTRIBUTE]
20200805 14:30:01:380 Default (SA ZyXEL_USG20-P1) RECV Transaction Mode [HASH] [ATTRIBUTE]
20200805 14:30:01:380 Default (SA ZyXEL_USG20-Ikev1Tunnel-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20200805 14:30:01:485 Default (SA ZyXEL_USG20-Ikev1Tunnel-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20200805 14:30:01:485 Default (SA ZyXEL_USG20-Ikev1Tunnel-P2) SEND phase 2 Quick Mode [HASH]
20200805 14:30:01:485 Default (SA ZyXEL_USG20-Ikev1Tunnel-P2) renewal in 2448 seconds (15:10:49)
20200805 14:30:01:522 Default (SA ZyXEL_USG20-Ikev1Tunnel-P2) [VirtualIf] Virtual Interface properly configured for instance 1 and IfIndex 13.
```

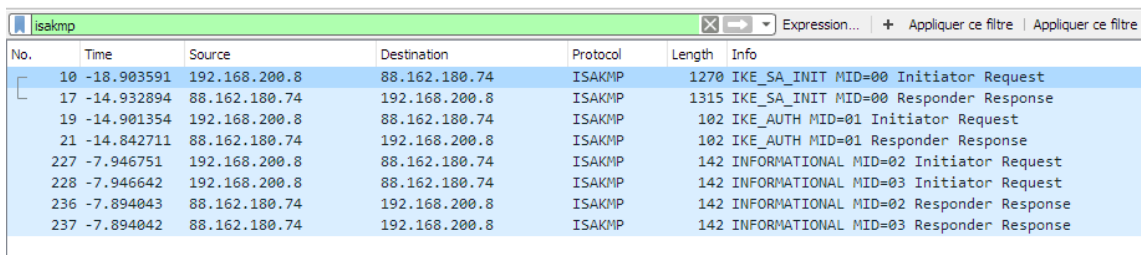
At the bottom right of the console window, there are two status indicators: "Current line: 16" and "Max. lines: 10000".

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



The screenshot shows a Wireshark capture window titled 'isakmp'. The main pane displays a list of captured packets with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The packets are ISAKMP messages between source IP 192.168.200.8 and destination IP 88.162.180.74. The sequence includes an IKE_SA_INIT initiator request (1270 bytes), responder response (1315 bytes), IKE_AUTH initiator request (102 bytes), responder response (102 bytes), and three INFORMATIONAL messages (142 bytes each) for MID=02 and MID=03.

| 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