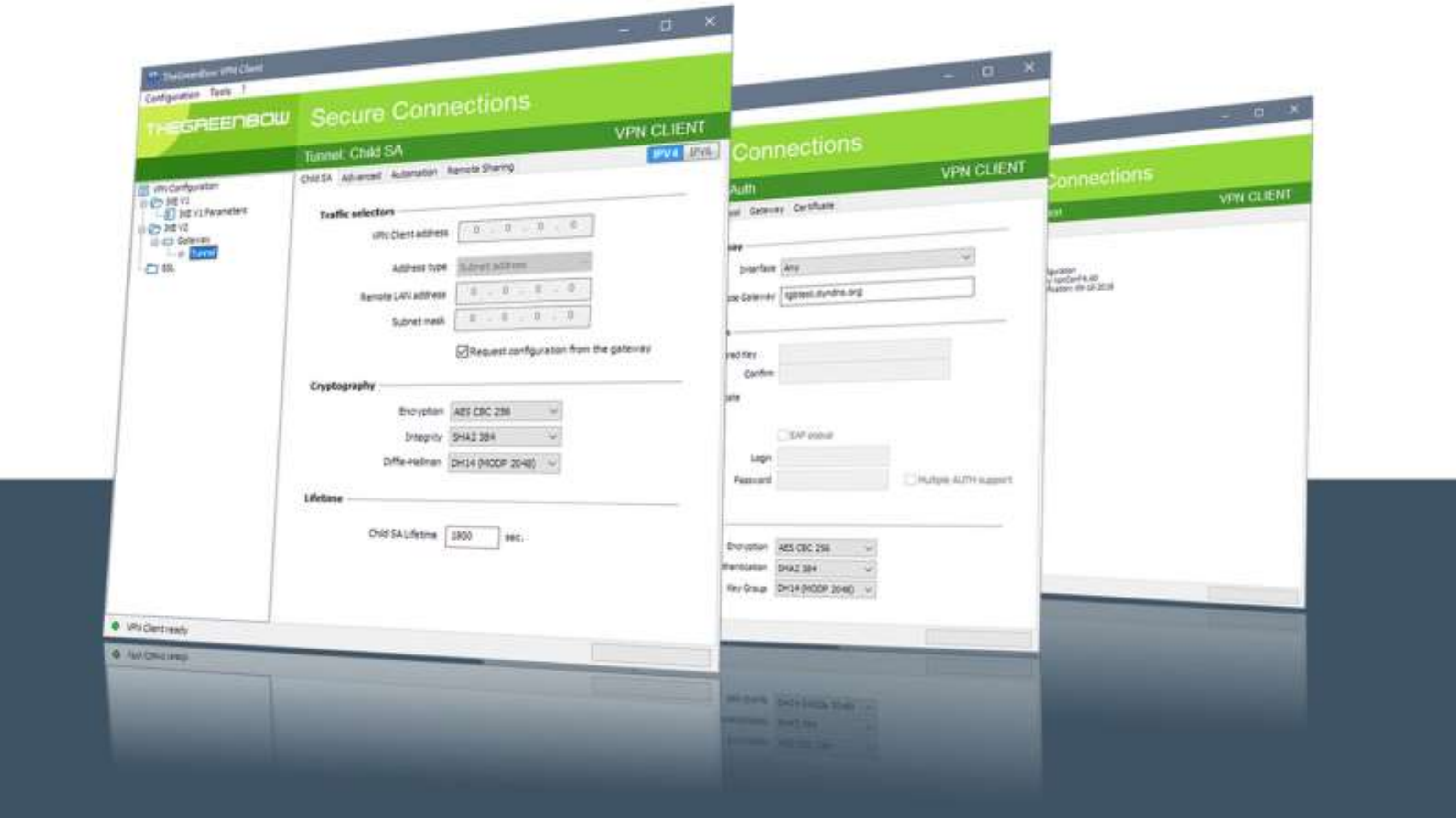


TheGreenBow IPsec VPN Client

Configuration Guide SOPHOS XG Firewall

IKEv2

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

Table of Contents

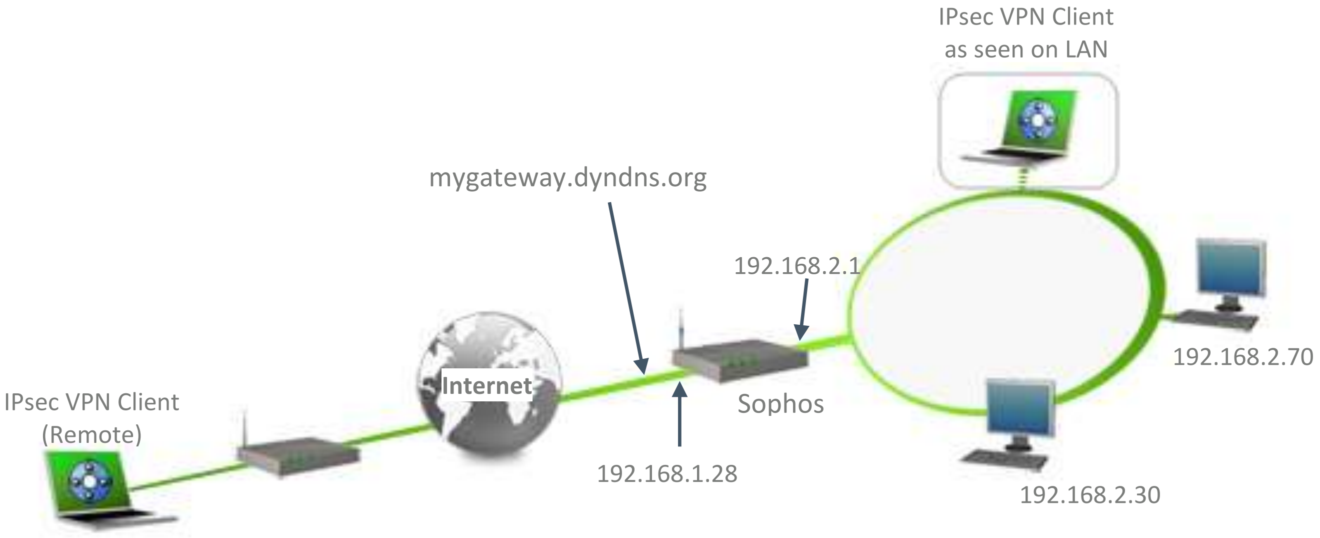
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a SOPHOS XG Firewall 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 SOPHOS XG Firewall 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 SOPHOS XG Firewall Restrictions

Sophos is not compatible to IKVE2 in Remote Access. We need to use Site-to-site or host to host to configure IKVE2 tunnel.

1.4 SOPHOS XG Firewall VPN Gateway

Our tests and VPN configuration have been conducted with SOPHOS XG Firewall version 5.5.

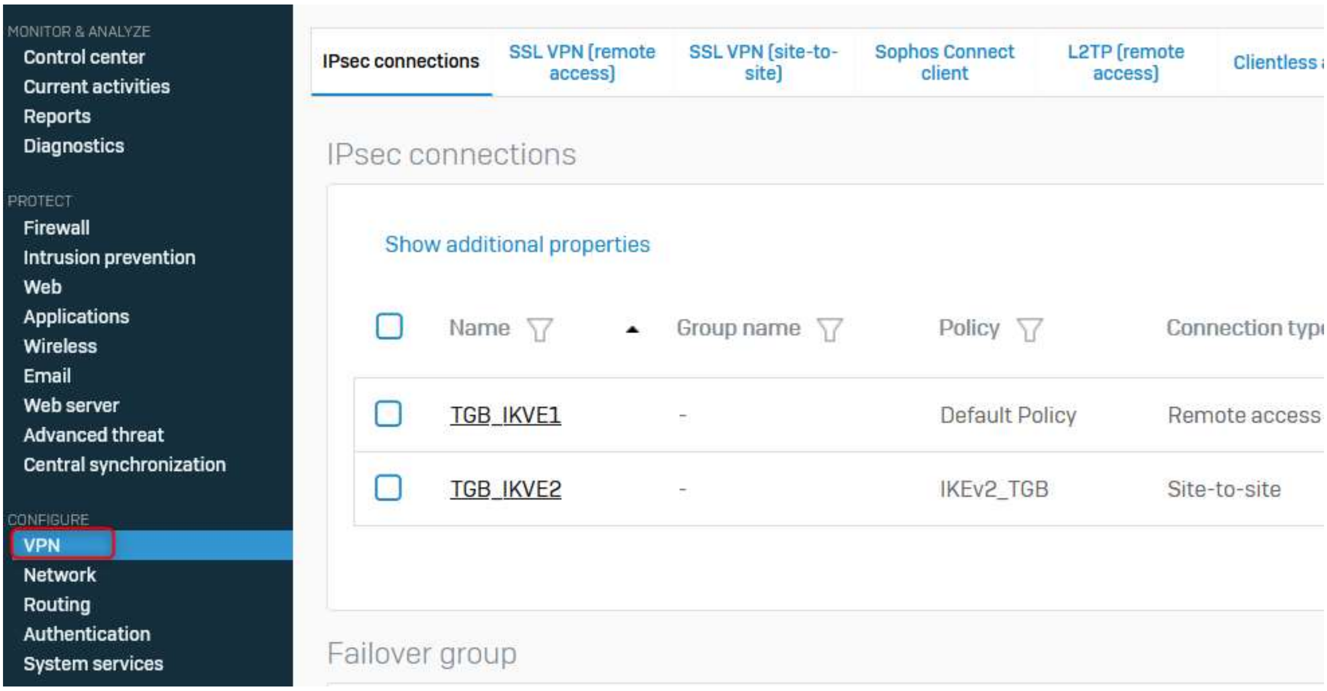
1.5 SOPHOS XG Firewall VPN Gateway product info

It is critical that users find all necessary information about SOPHOS XG Firewall VPN Gateway. All product info, User Guide and knowledge base for the SOPHOS XG Firewall VPN Gateway can be found on the SOPHOS website: **https://www.sophos.com/fr-fr/support/documentation/sophos-xg-firewall.aspx**

SOPHOS XG Firewall Product page	**https://www.sophos.com/en-us/medialibrary/PDFs/documentation/SophosFirewall/v165/Sophos-XG-Firewall-Web-Interface-Reference-Guide.pdf**
SOPHOS XG Firewall User Guide	**https://community.sophos.com/xg-firewall/f/discussions/110481/xg-setup-guide-for-new-users**

2 SOPHOS XG Firewall VPN configuration

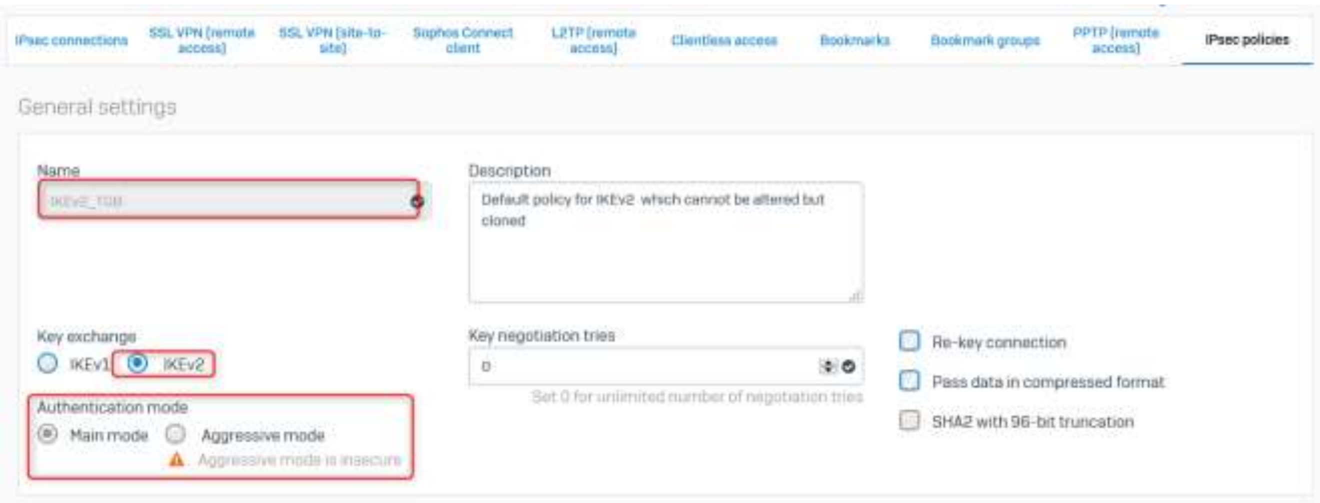
This section describes how to build an IPsec VPN configuration with your SOPHOS XG Firewall VPN router. Once connected to your SOPHOS XG Firewall VPN gateway, go to menu VPN.



IPsec connections

□	Name	Group name	Policy	Connection typ
□	TGB_IKVE1	-	Default Policy	Remote access
□	TGB_IKVE2	-	IKEv2_TGB	Site-to-site

Firstly create the policies : IPsec policies >> Add



General settings

Name: IKEv2_TGB

Description: Default policy for IKEv2 which cannot be altered but cloned

Key exchange: ○ IKEv1 ● IKEv2

Authentication mode: ● Main mode ○ Aggressive mode

Aggressive mode is insecure

Key negotiation tries: 0

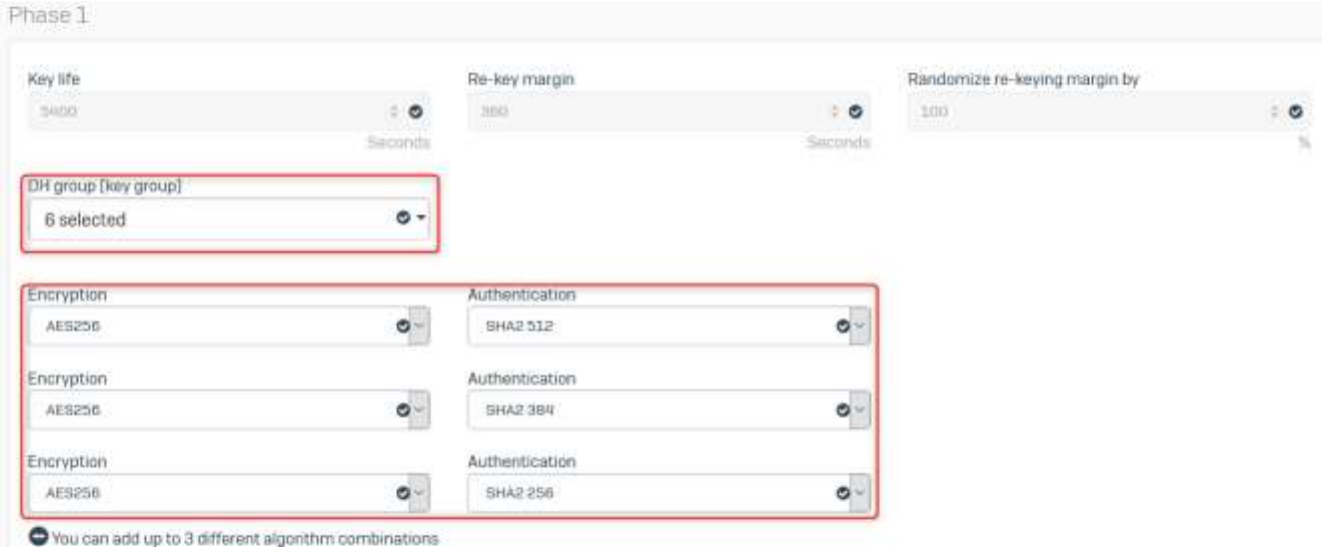
Set 0 for unlimited number of negotiation tries

□ Re-key connection

□ Pass data in compressed format

□ SHA2 with 96-bit truncation

Phase 1



Phase 1

Key life: 5400 Seconds

Re-key margin: 360 Seconds

Randomize re-keying margin by: 100 %

DH group [key group]: 6 selected

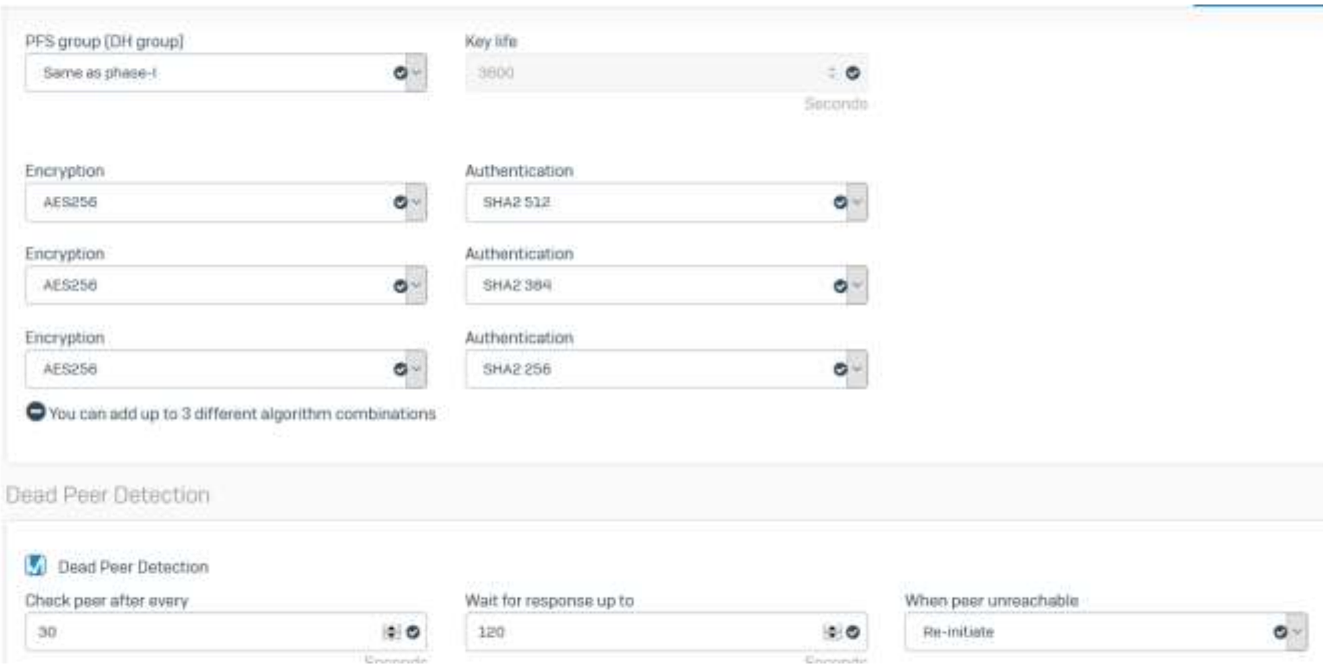
Encryption: AES256 — Authentication: SHA2 512

Encryption: AES256 — Authentication: SHA2 384

Encryption: AES256 — Authentication: SHA2 256

You can add up to 3 different algorithm combinations

Phase 2



PFS group (DH group): Same as phase-I

Key life: 3600 Seconds

Encryption: AES256 — Authentication: SHA2 512

Encryption: AES256 — Authentication: SHA2 384

Encryption: AES256 — Authentication: SHA2 256

You can add up to 3 different algorithm combinations

Dead Peer Detection

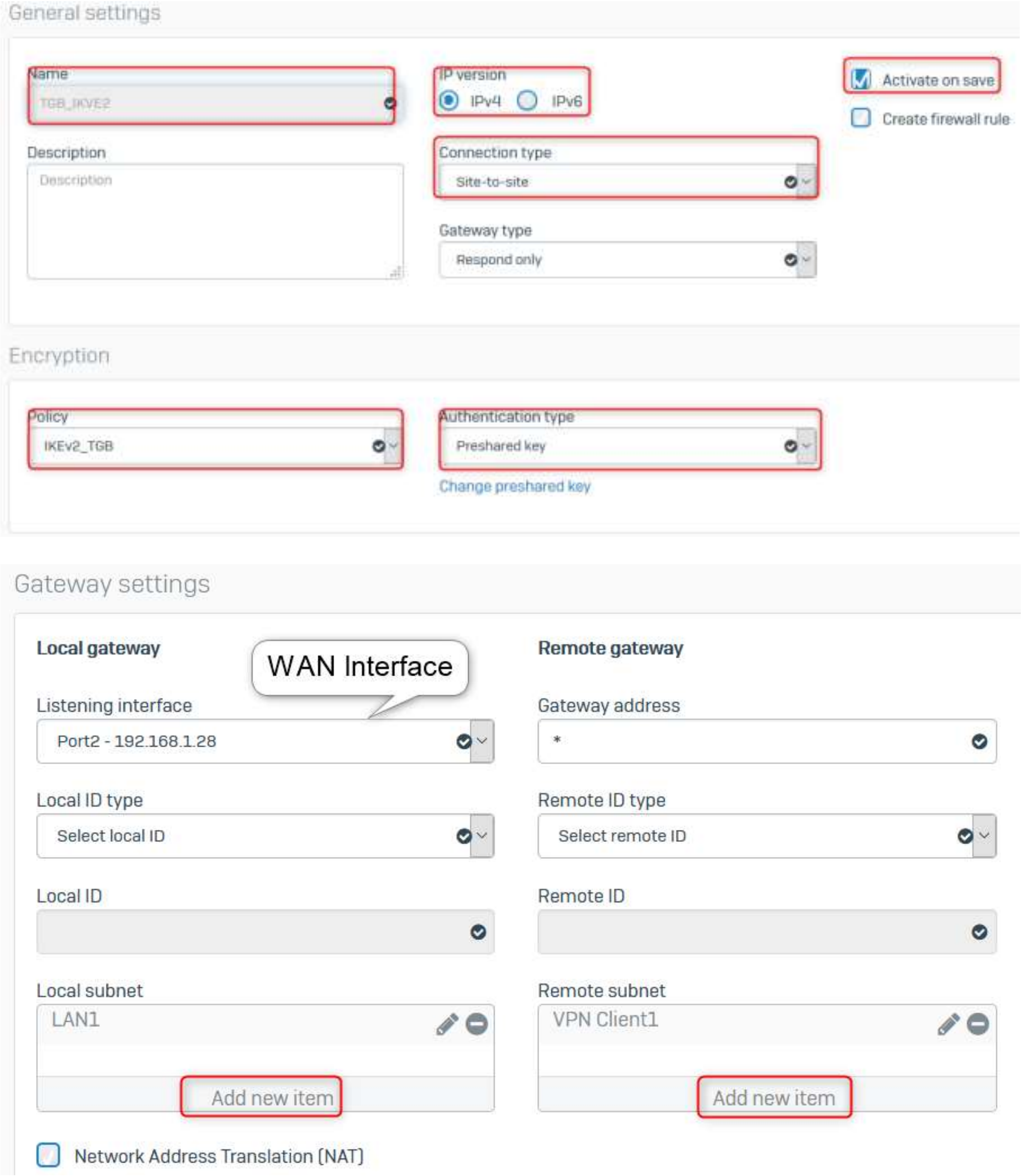
☑ Dead Peer Detection

Check peer after every: 30 Seconds

Wait for response up to: 120 Seconds

When peer unreachable: Re-initiate

Configure the VPN



General settings

Name: TGB_IKVE2

Description: Description

IP version: ● IPv4 ○ IPv6

Connection type: Site-to-site

Gateway type: Respond only

☑ Activate on save

☐ Create firewall rule

Encryption

Policy: IKEv2_TGB

Authentication type: Preshared key

Change preshared key

Gateway settings

Local gateway

Listening interface: Port2 - 192.168.1.28

Local ID type: Select local ID

Local ID:

Local subnet: LAN1

Remote gateway

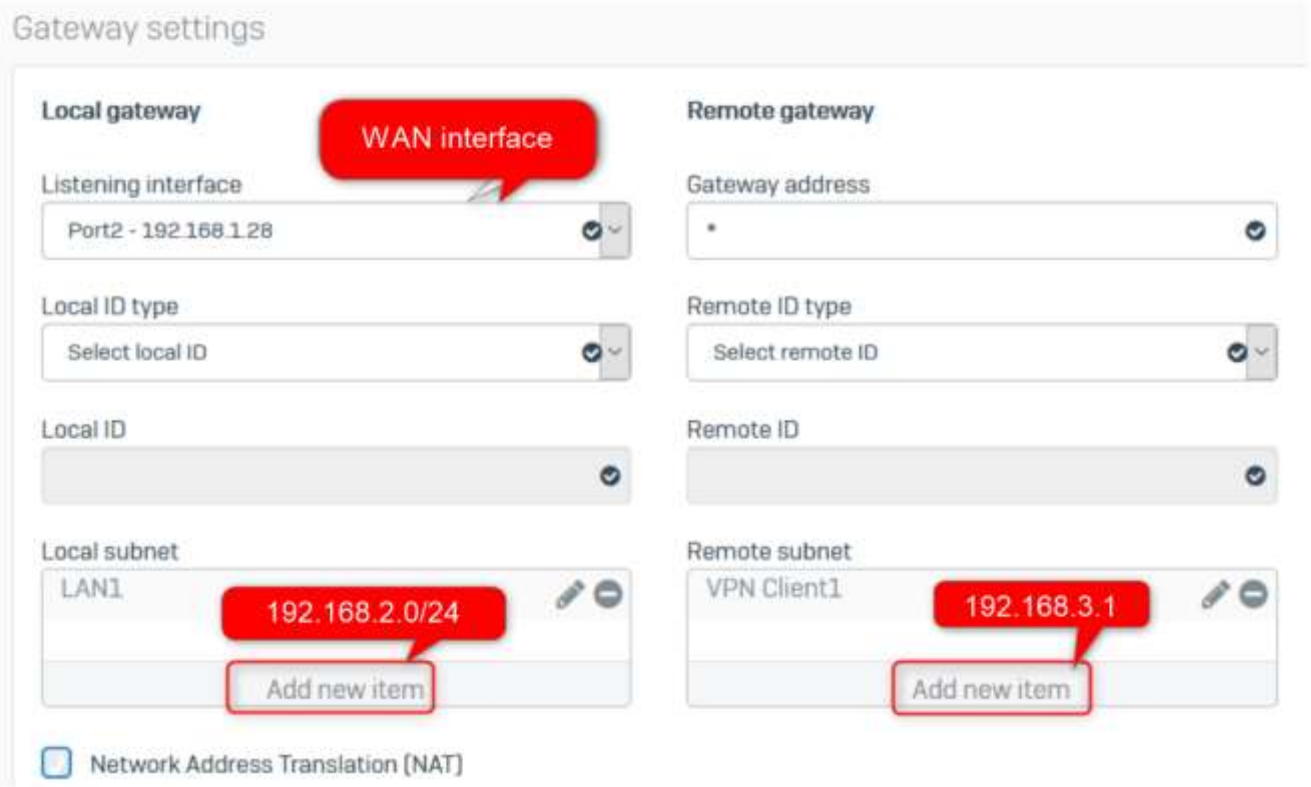
Gateway address: *

Remote ID type: Select remote ID

Remote ID:

Remote subnet: VPN Client1

☐ Network Address Translation (NAT)



Gateway settings

Local gateway

Listening interface: Port2 - 192.168.1.28

Local ID type: Select local ID

Local ID:

Local subnet: LAN1

Add new item

Remote gateway

Gateway address: *

Remote ID type: Select remote ID

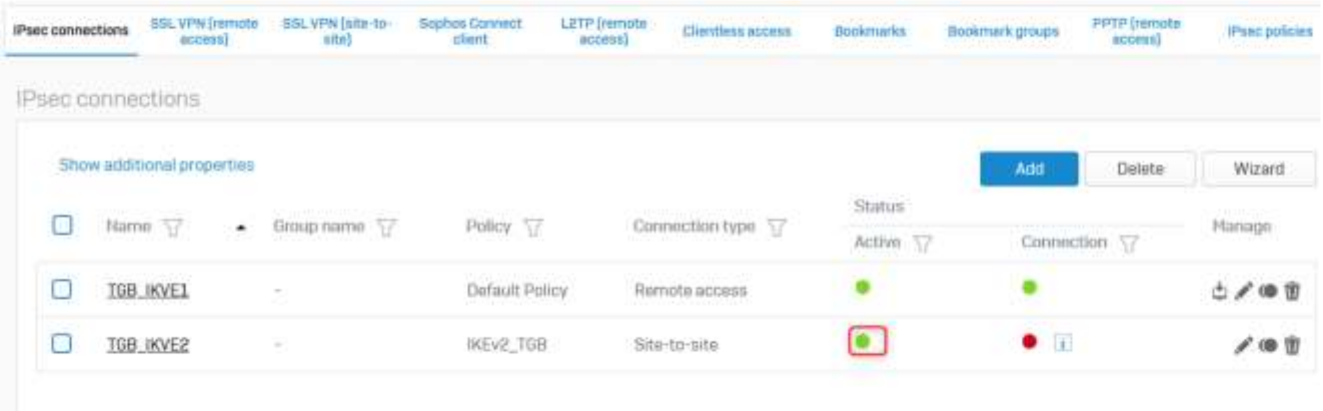
Remote ID:

Remote subnet: VPN Client1

Add new item

□ Network Address Translation (NAT)

Make sure that VPN status is enable:



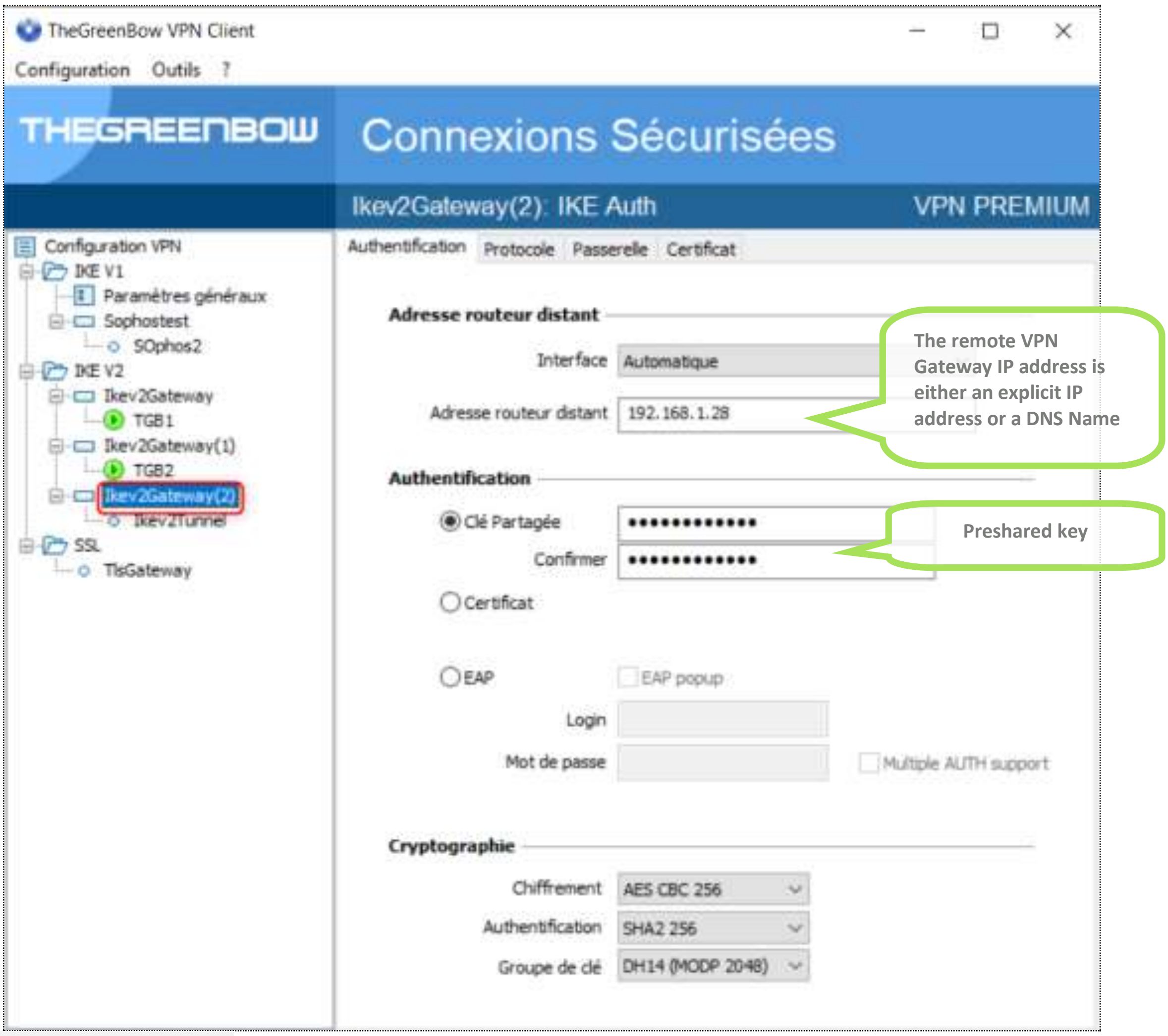
IPsec connections

□	Name	Group name	Policy	Connection type	Status: Active	Status: Connection	Manage
□	TGB_IKVE1	-	Default Policy	Remote access	●	●	
□	TGB_IKVE2	-	IKEv2_TGB	Site-to-site	●	●	

3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a SOPHOS XG Firewall 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 - IKE Auth Configuration



Adresse routeur distant

Interface: Automatique

Adresse routeur distant: 192.168.1.28

Authentification

● Clé Partagée: •••••••••••••

Confirmer: •••••••••••••

○ Certificat

○ EAP □ EAP popup

Login:

Mot de passe:

□ Multiple AUTH support

Cryptographie

Chiffrement: AES CBC 256

Authentification: SHA2 256

Groupe de clé: DH14 (MODP 2048)

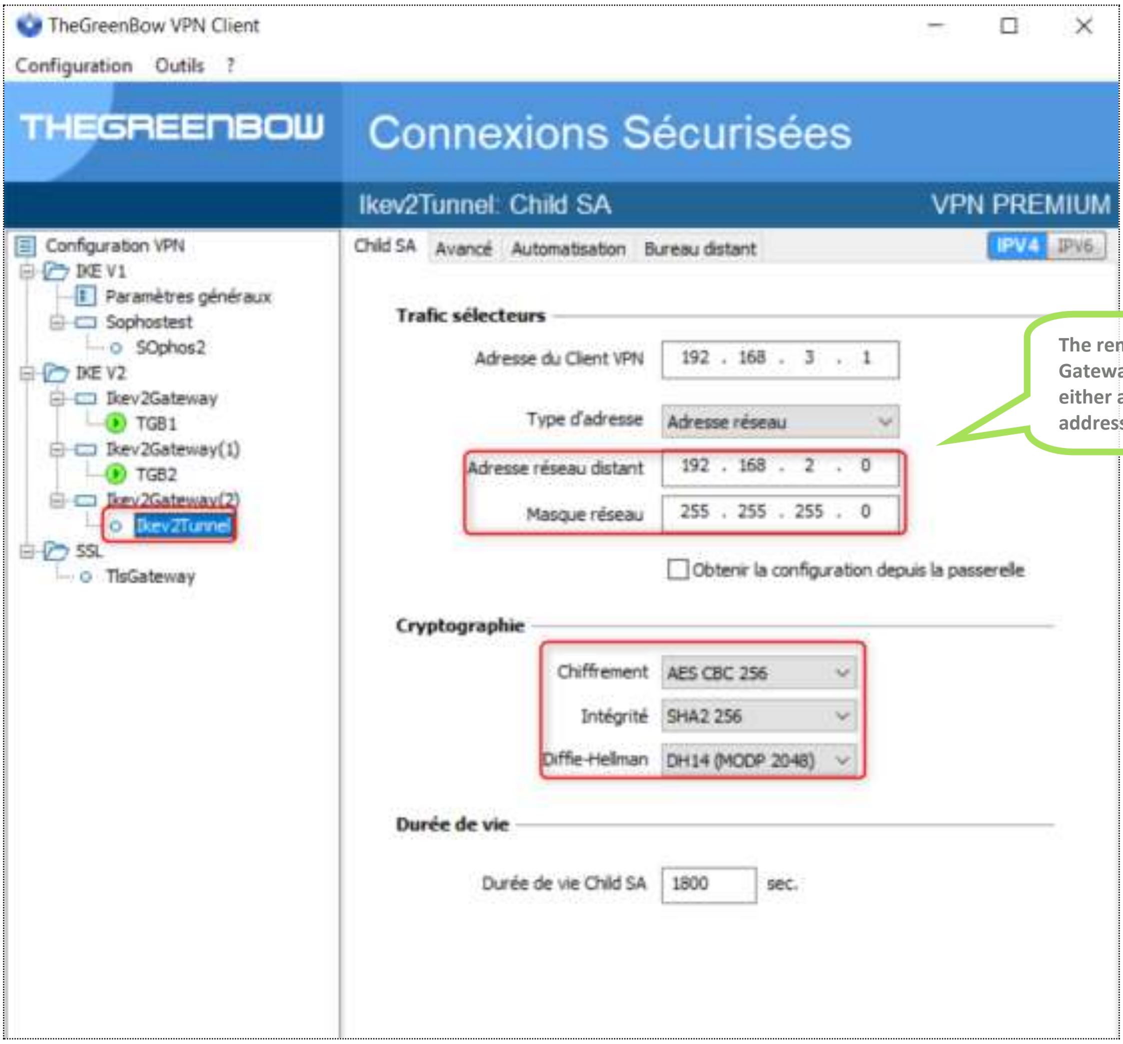
The remote VPN Gateway IP address is either an explicit IP address or a DNS Name

Preshared key

IKE Auth configuration

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

VPN Client Phase 2 (Child SA) Configuration



Trafic sélecteurs

Adresse du Client VPN: 192 . 168 . 3 . 1

Type d'adresse: Adresse réseau

Adresse réseau distant: 192 . 168 . 2 . 0

Masque réseau: 255 . 255 . 255 . 0

□ Obtenir la configuration depuis la passerelle

Cryptographie

Chiffrement: AES CBC 256

Intégrité: SHA2 256

Diffie-Hellman: DH14 (MODP 2048)

Durée de vie

Durée de vie Child SA: 1800 sec.

The remote VPN Gateway IP address is either an explicit IP address or a DNS Name

Child SA Configuration

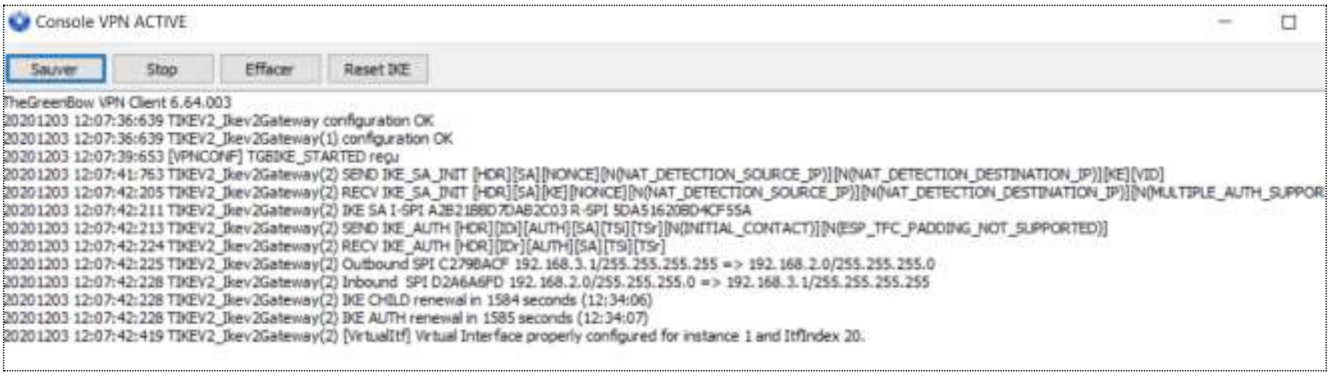
3.2 Open IPsec VPN tunnels

Once both SOPHOS XG Firewall 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 SOPHOS XG Firewall VPN router.



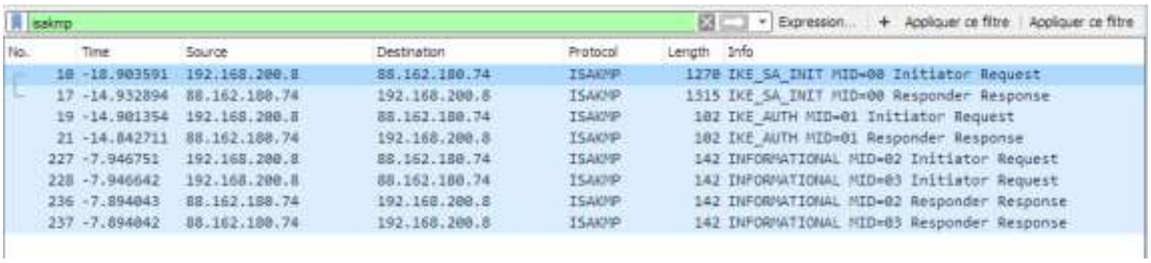
```
TheGreenBow VPN Client 6.64.003
20201203 12:07:36:639 TIKEV2_Ikev2Gateway configuration OK
20201203 12:07:36:639 TIKEV2_Ikev2Gateway(1) configuration OK
20201203 12:07:39:653 [VPNCONF] TGBIKE_STARTED reçu
20201203 12:07:41:763 TIKEV2_Ikev2Gateway(2) SEND IKE_SA_INIT [HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE][VID]
20201203 12:07:42:205 TIKEV2_Ikev2Gateway(2) RECV IKE_SA_INIT [HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][N(MULTIPLE_AUTH_SUPPOR
20201203 12:07:42:211 TIKEV2_Ikev2Gateway(2) IKE SA I-SPI A2B21BBD7DAB2C03 R-SPI 5DA51620BD4CF55A
20201203 12:07:42:213 TIKEV2_Ikev2Gateway(2) SEND IKE_AUTH [HDR][IDi][AUTH][SA][TSi][TSr][N(INITIAL_CONTACT)][N(ESP_TFC_PADDING_NOT_SUPPORTED)]
20201203 12:07:42:224 TIKEV2_Ikev2Gateway(2) RECV IKE_AUTH [HDR][IDr][AUTH][SA][TSi][TSr]
20201203 12:07:42:225 TIKEV2_Ikev2Gateway(2) Outbound SPI C2798ACF 192.168.3.1/255.255.255.255 => 192.168.2.0/255.255.255.0
20201203 12:07:42:228 TIKEV2_Ikev2Gateway(2) Inbound  SPI D2A6A6FD 192.168.2.0/255.255.255.0 => 192.168.3.1/255.255.255.255
20201203 12:07:42:228 TIKEV2_Ikev2Gateway(2) IKE CHILD renewal in 1584 seconds (12:34:06)
20201203 12:07:42:228 TIKEV2_Ikev2Gateway(2) IKE AUTH renewal in 1585 seconds (12:34:07)
20201203 12:07:42:419 TIKEV2_Ikev2Gateway(2) [VirtualItf] Virtual Interface properly configured for instance 1 and ItfIndex 20.
```

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/**).



No.	Time	Source	Destination	Protocol	Length	Info
18	-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	-14.842711	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(FR
AGMENTATION_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 preshared key is not matching. Check the Gateway if the user certificate or preshared key is valid.

5.3 “No user certificate available for the connexion” 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(FRAGMEN
TATION_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**) on one of your target computer. 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