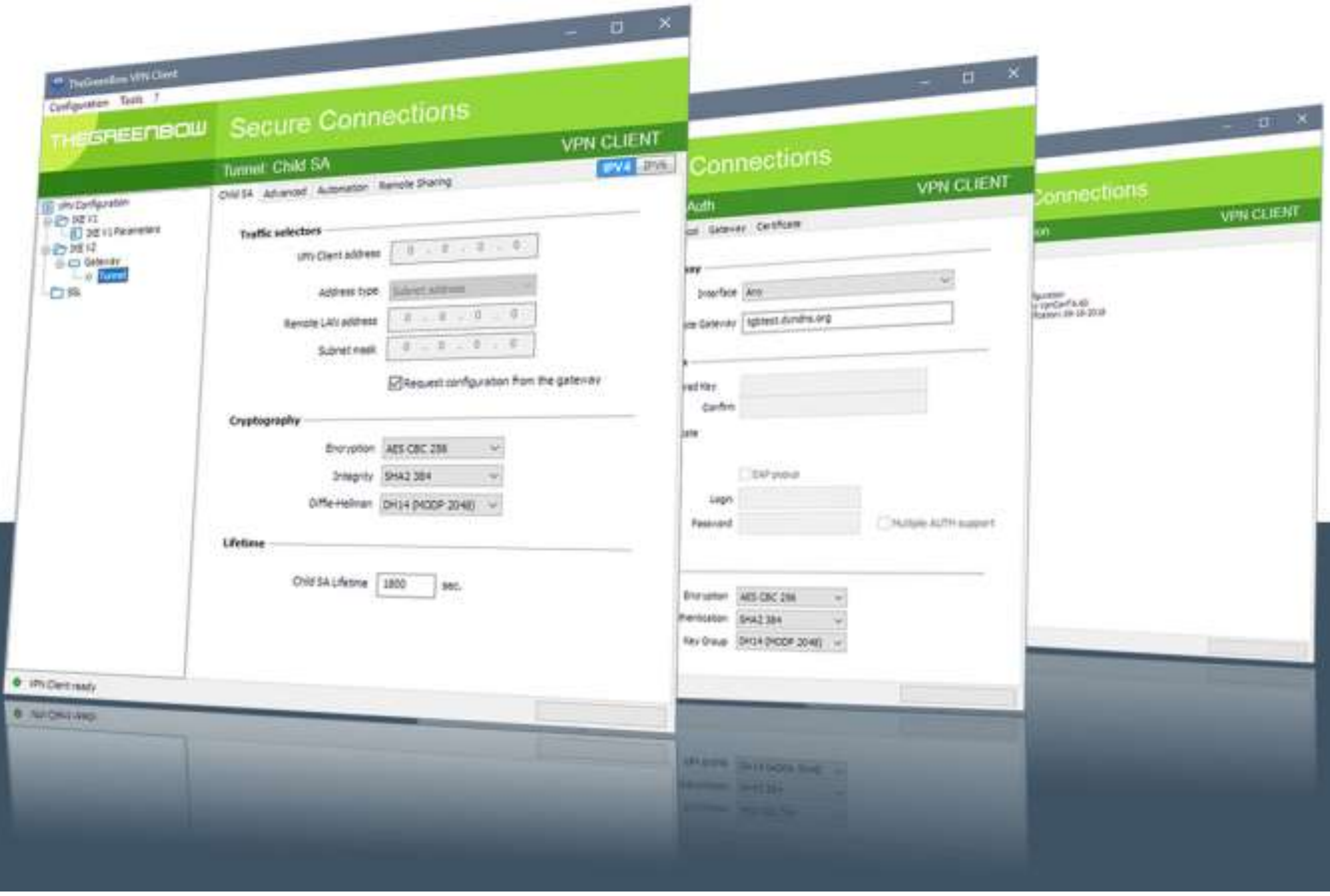


TheGreenBow IPsec VPN Client

Configuration Guide SOPHOS XG Firewall

IKEv1

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

Table of Contents

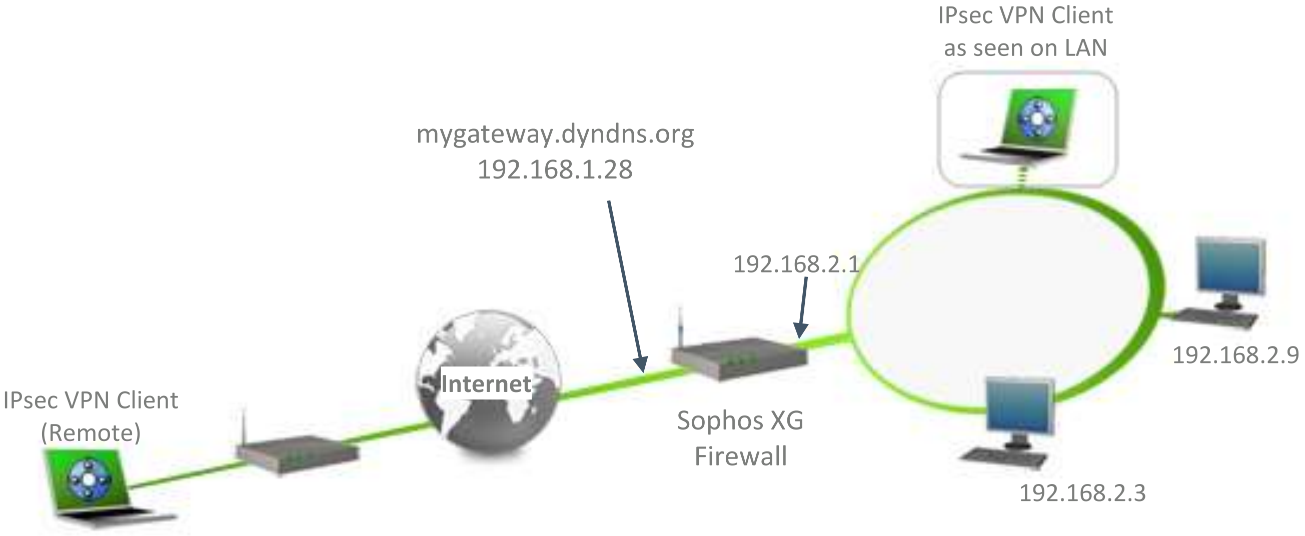
1 Introduction

1.1 Goal of this document

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

No known restrictions.

1.4 SOPHOS XG Firewall VPN Gateway

Our tests and VPN configuration have been conducted with SOPHOS XG Firewall firmware release 17.5.14.

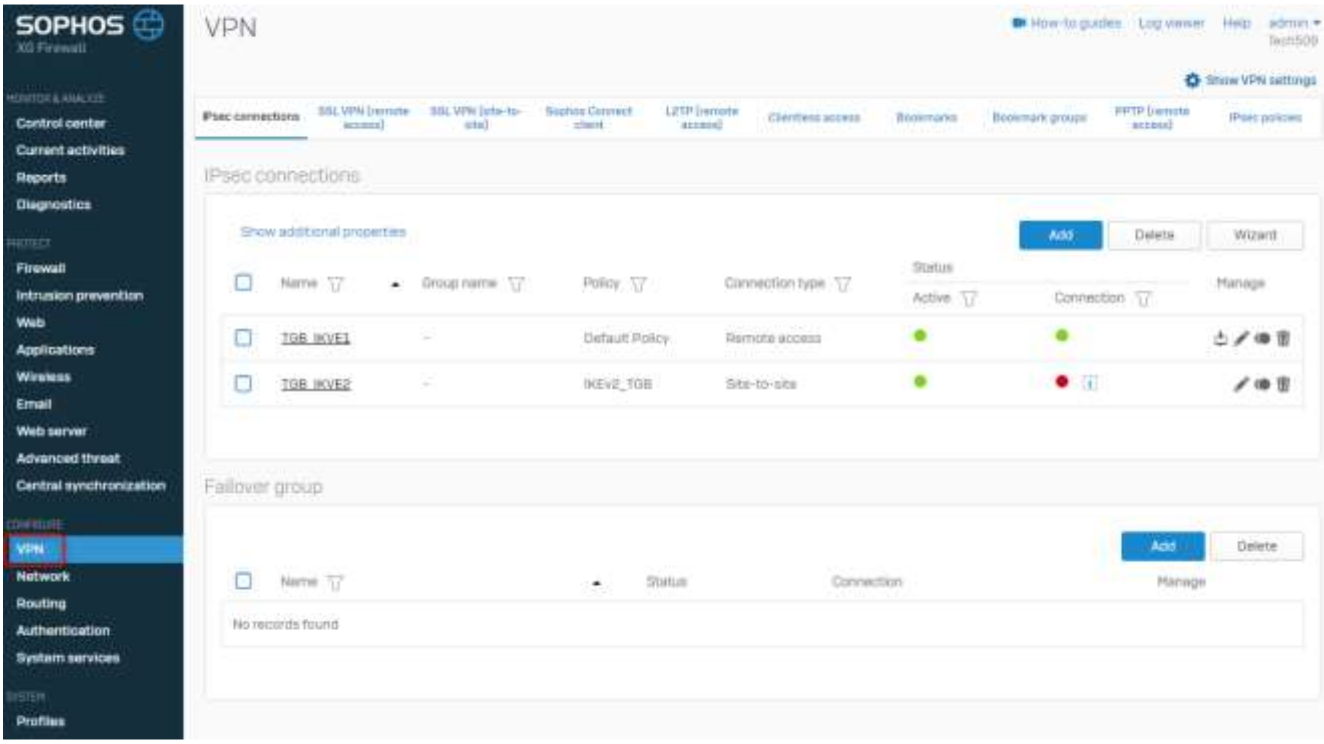
1.5 SOPHOS XG Firewall VPN Gateway product info

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 /FAQ/Knowledge Base	**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, you must select VPN.



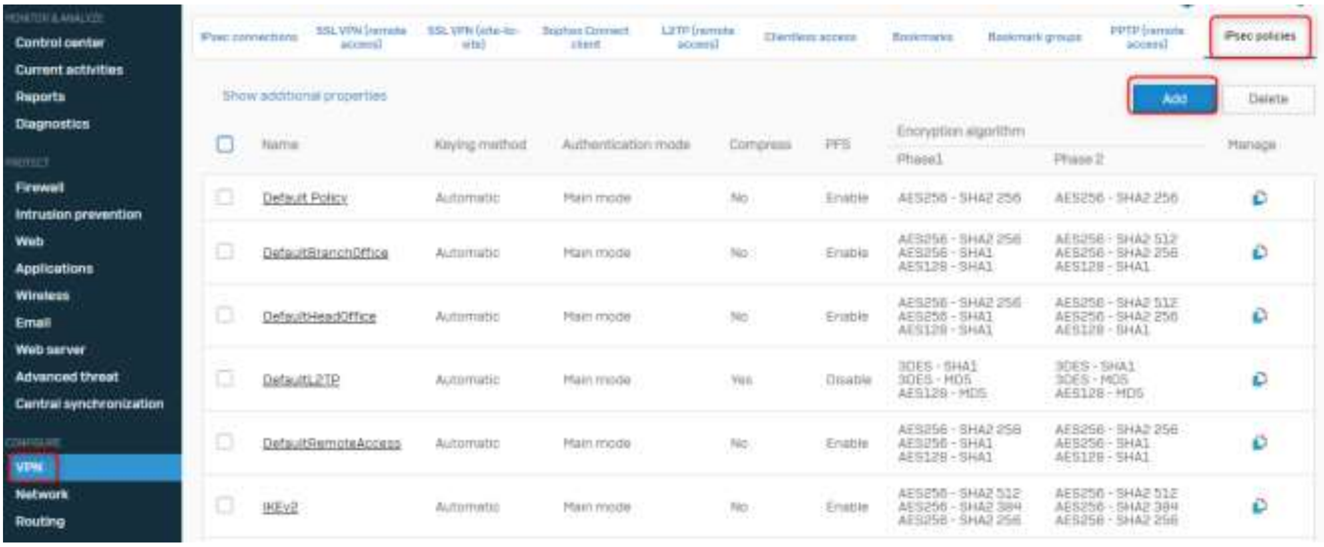
IPsec connections

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

Failover group

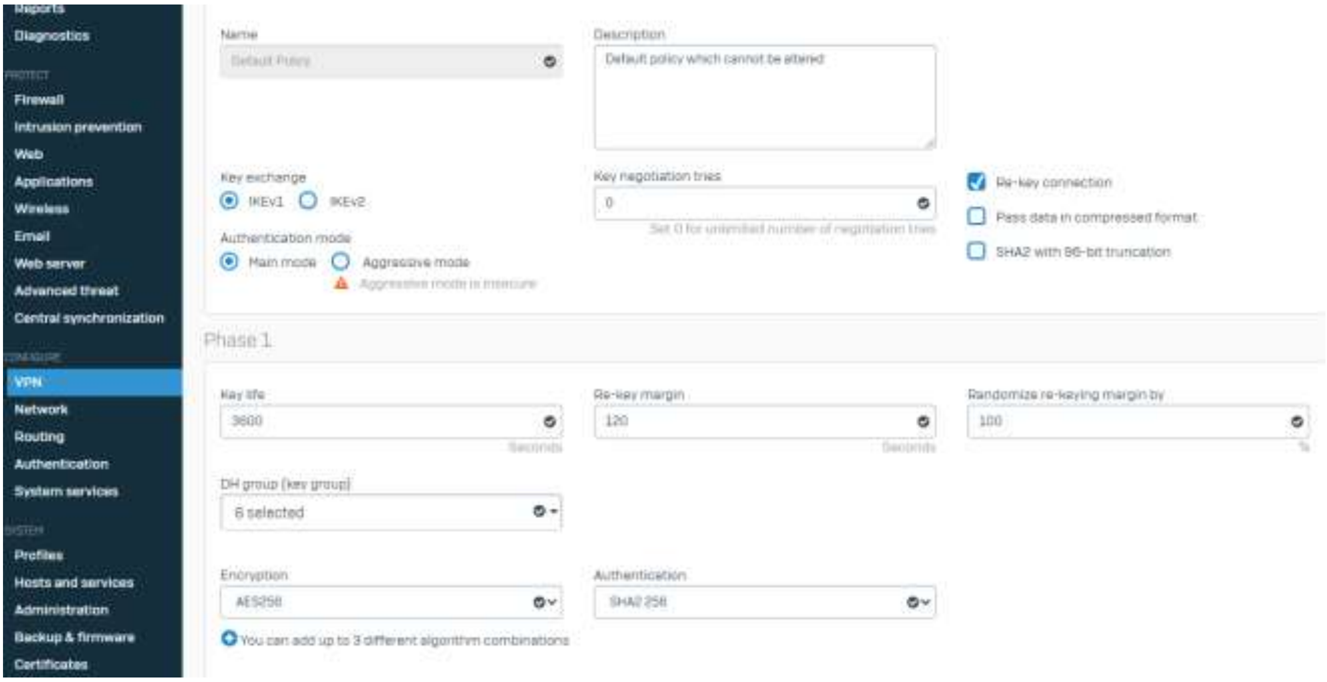
□	Name	Status	Connection	Manage
	No records found			

Firstly, we will configure IPsec policies.
To configure IPsec policies, click on IPsec policies like:



□	Name	Keying method	Authentication mode	Compress	PFS	Encryption algorithm: Phase1	Encryption algorithm: Phase 2	Manage
□	Default Policy	Automatic	Main mode	No	Enable	AES256 - SHA2 256	AES256 - SHA2 256	
□	DefaultBranchOffice	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 512 AES256 - SHA2 256 AES128 - SHA1	
□	DefaultHeadOffice	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 512 AES256 - SHA2 256 AES128 - SHA1	
□	DefaultL2TP	Automatic	Main mode	Yes	Disable	3DES - SHA1 3DES - MD5 AES128 - MD5	3DES - SHA1 3DES - MD5 AES128 - MD5	
□	DefaultRemoteAccess	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	
□	IKEv2	Automatic	Main mode	No	Enable	AES256 - SHA2 512 AES256 - SHA2 384 AES256 - SHA2 256	AES256 - SHA2 512 AES256 - SHA2 384 AES256 - SHA2 256	

Policies Phase 1



Name: Default Policy

Description: Default policy which cannot be altered

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

Key life: 3600 Seconds

Re-key margin: 120 Seconds

Randomize re-keying margin by: 100 %

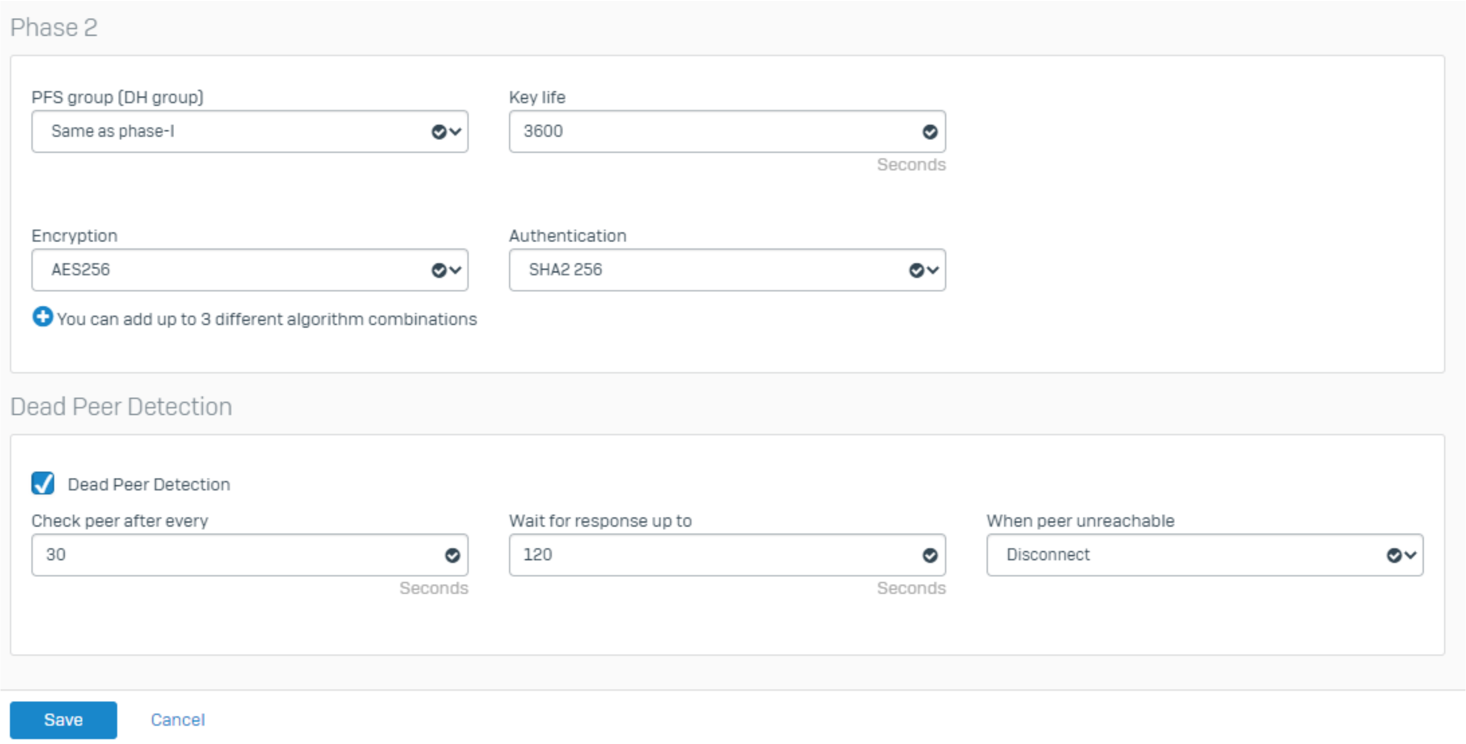
DH group (key group): 6 selected

Encryption: AES256

Authentication: SHA2 256

You can add up to 3 different algorithm combinations

Policies Phase 2



Phase 2

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

Key life: 3600 Seconds

Encryption: AES256

Authentication: SHA2 256

You can add up to 3 different algorithm combinations

Dead Peer Detection

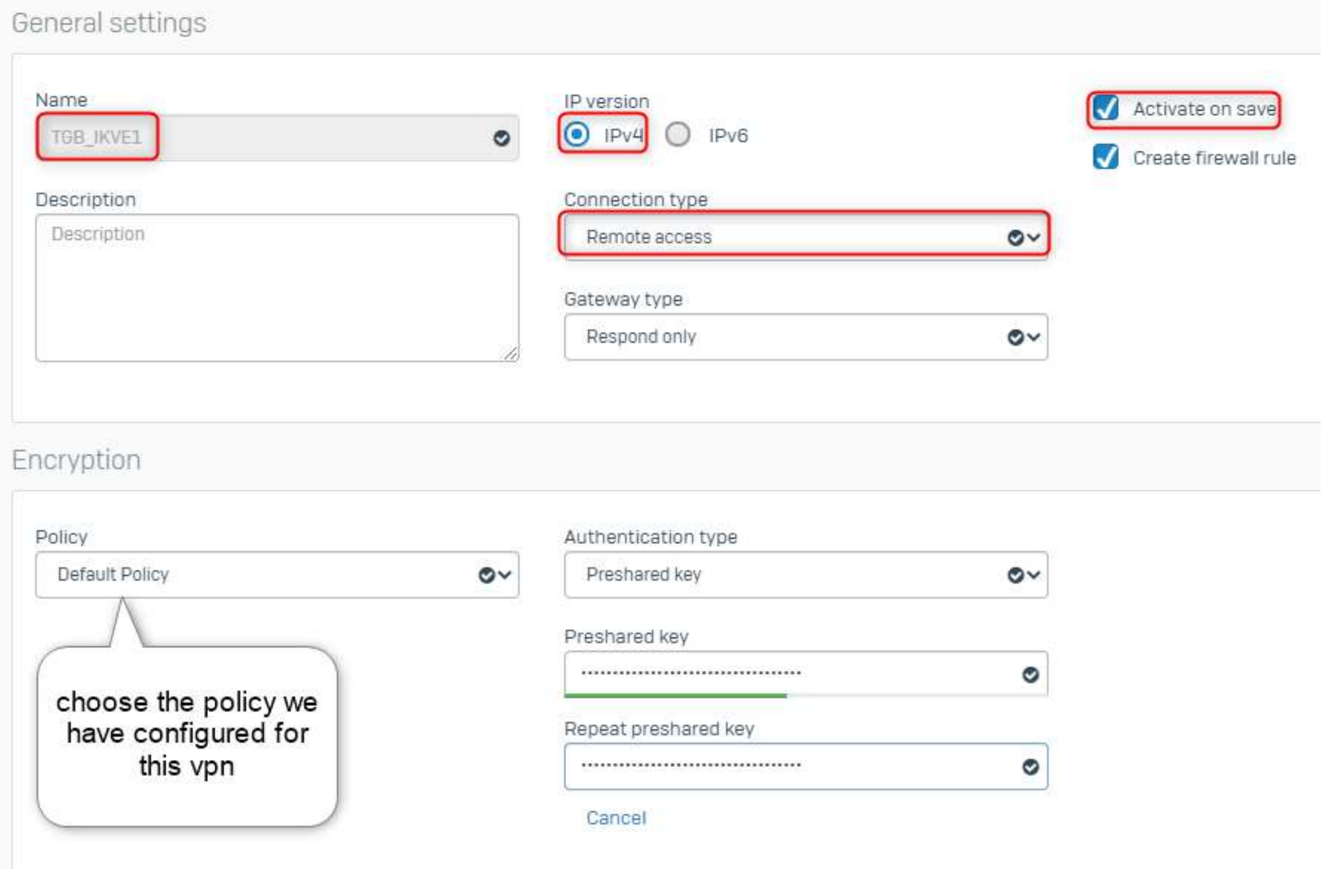
☑ Dead Peer Detection

Check peer after every: 30 Seconds

Wait for response up to: 120 Seconds

When peer unreachable: Disconnect

Now, we will configure the VPN remote access.



General settings

Name: TGB_IKVE1

IP version: ● IPv4 ○ IPv6

☑ Activate on save

☑ Create firewall rule

Description: Description

Connection type: Remote access

Gateway type: Respond only

Encryption

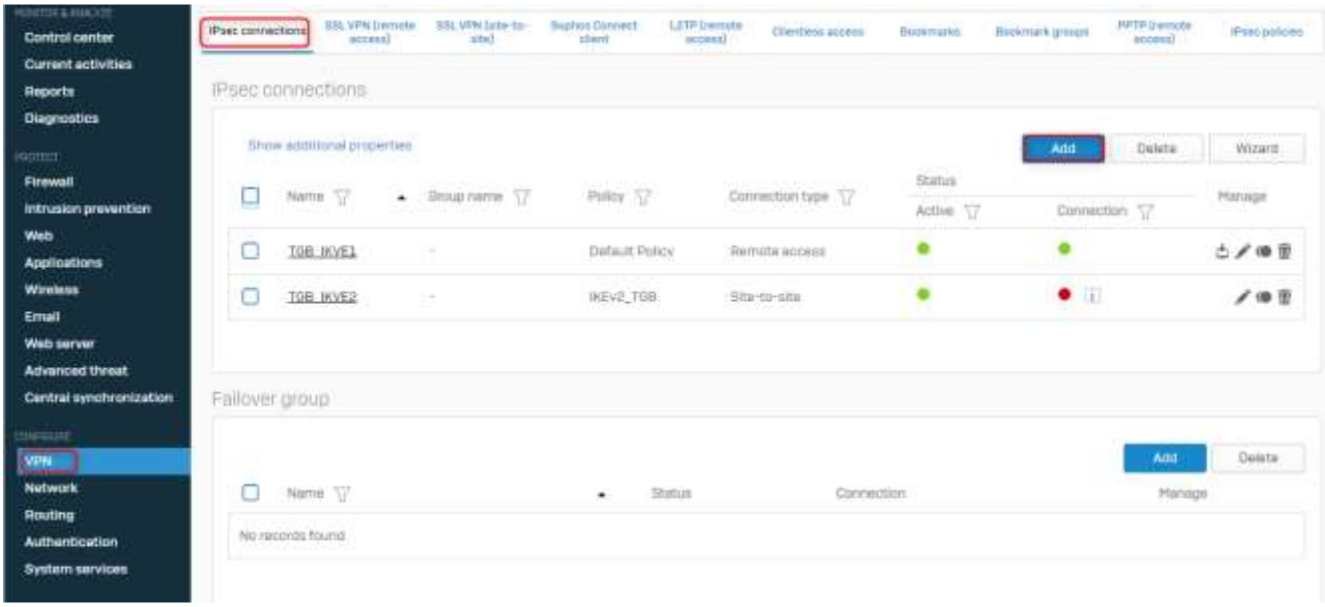
Policy: Default Policy

Authentication type: Preshared key

Preshared key: ••••••••••••••••••••••••••••••••••

Repeat preshared key: ••••••••••••••••••••••••••••••••••

choose the policy we have configured for this vpn

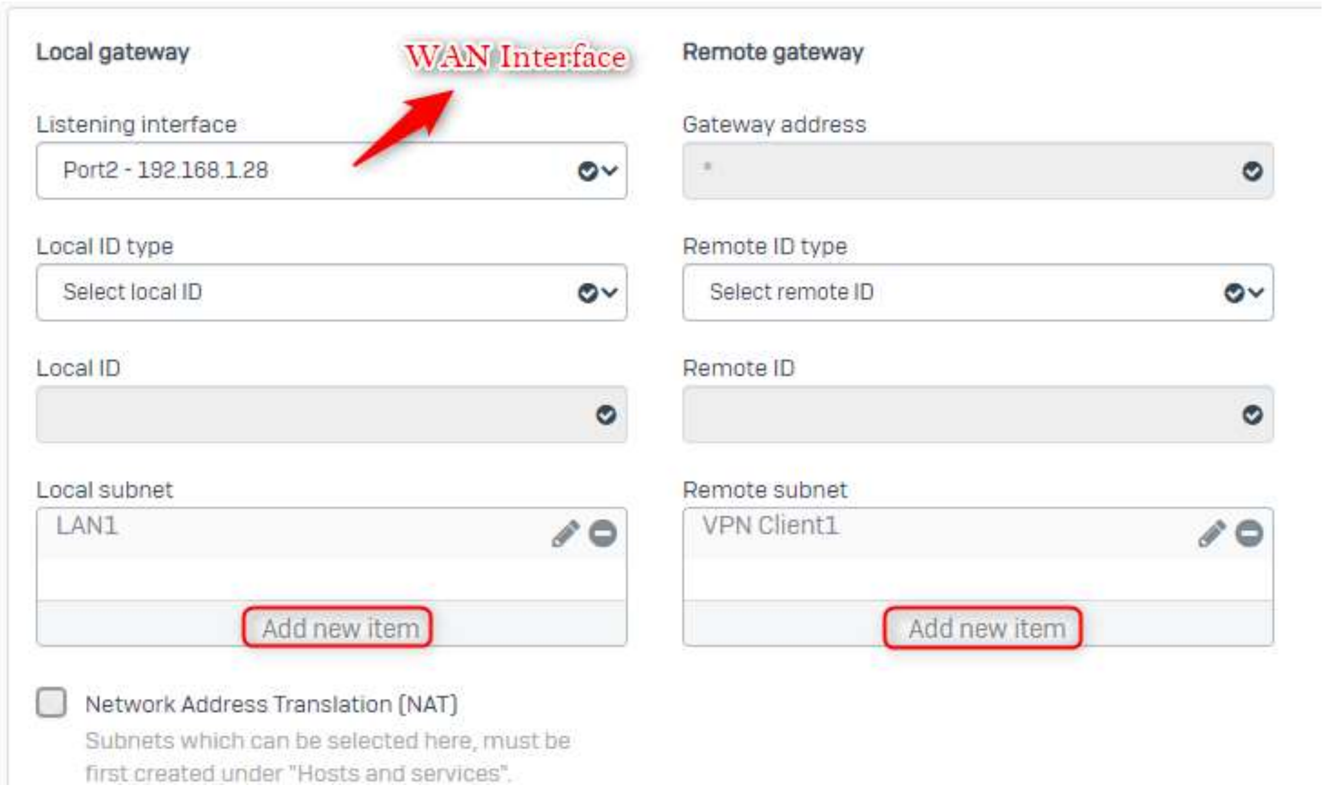


IPsec connections

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

Failover group

☐	Name	Status	Connection	Manage
No records found				



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

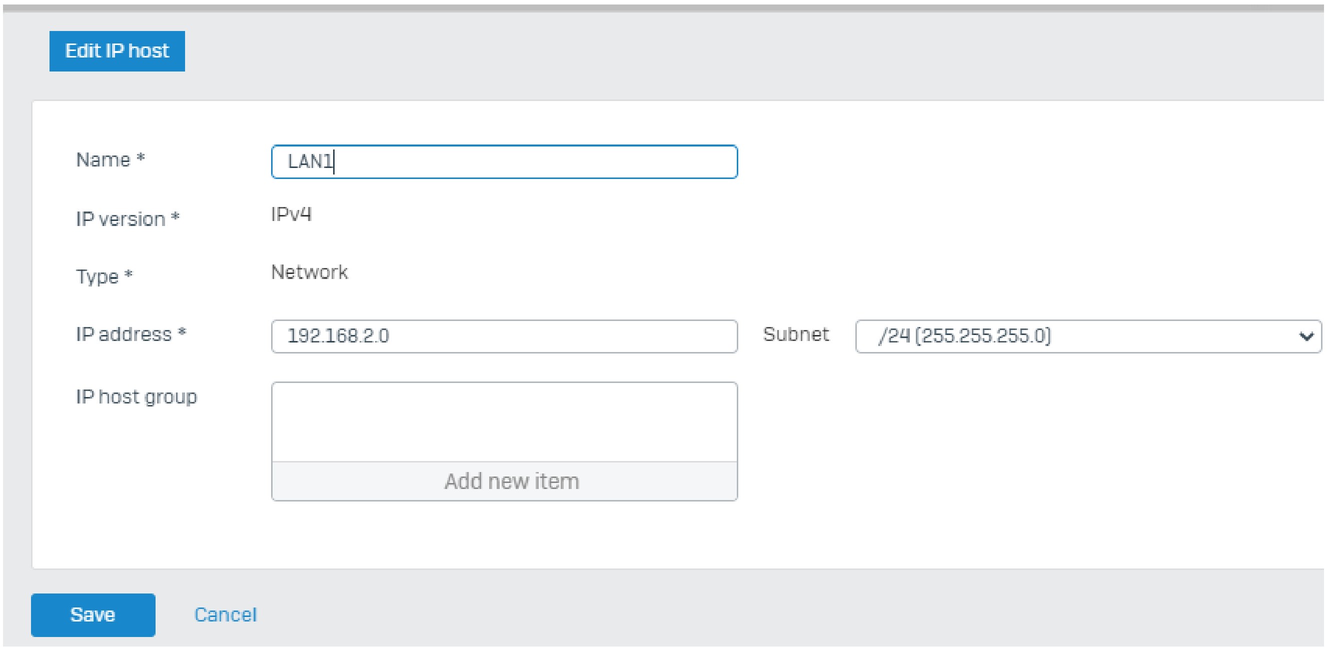
Remote ID:

Remote subnet: VPN Client1

□ Network Address Translation (NAT)

Subnets which can be selected here, must be first created under "Hosts and services".

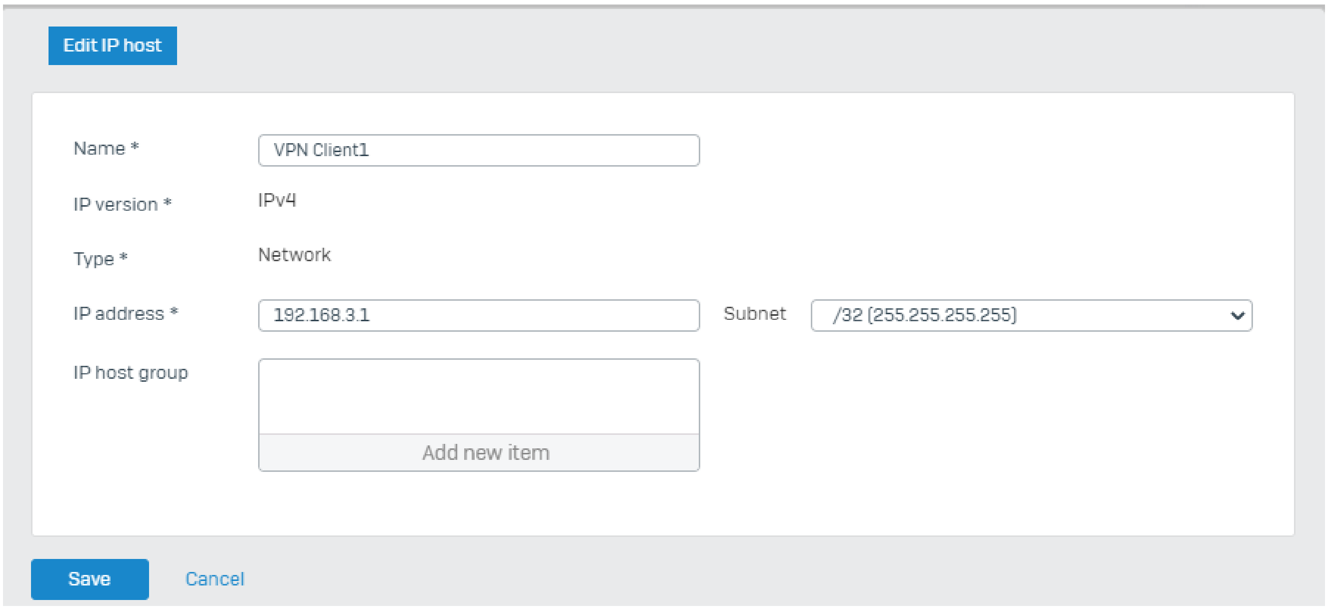
Local subnet



Edit IP host

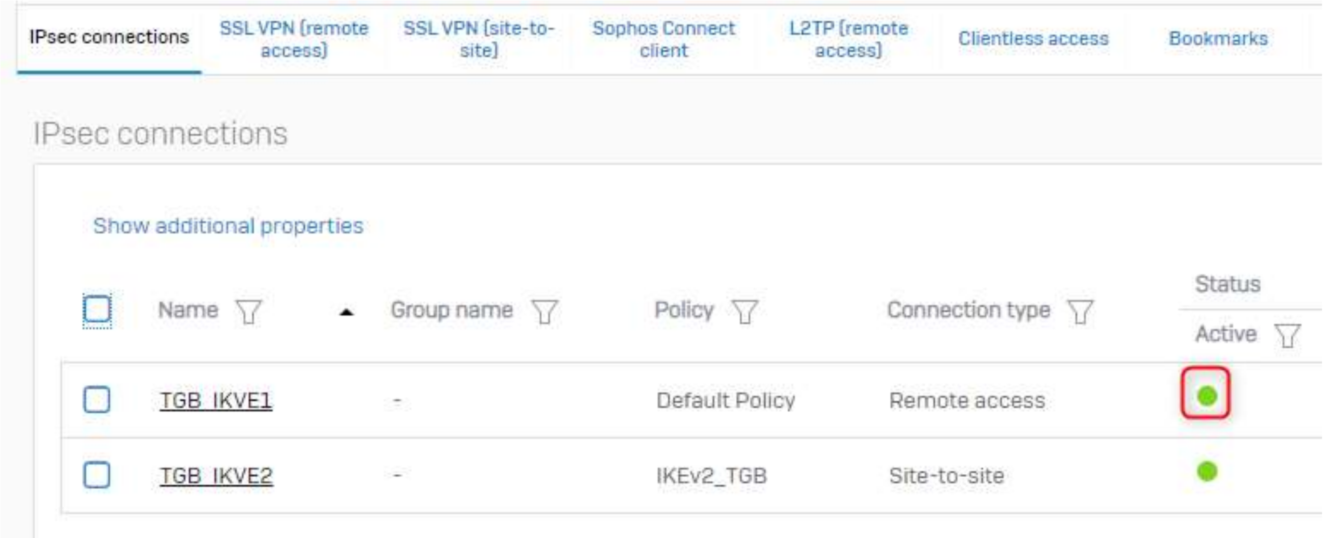
Name *	LAN1
IP version *	IPv4
Type *	Network
IP address *	192.168.2.0
Subnet	/24 (255.255.255.0)
IP host group	

Remote subnet – Range of IP for VPN Clients.



Name *	VPN Client1		
IP version *	IPv4		
Type *	Network		
IP address *	192.168.3.1	Subnet	/32 (255.255.255.255)
IP host group	Add new item		

Make sure that the vpn is actived on the gateway before configure the client VPN

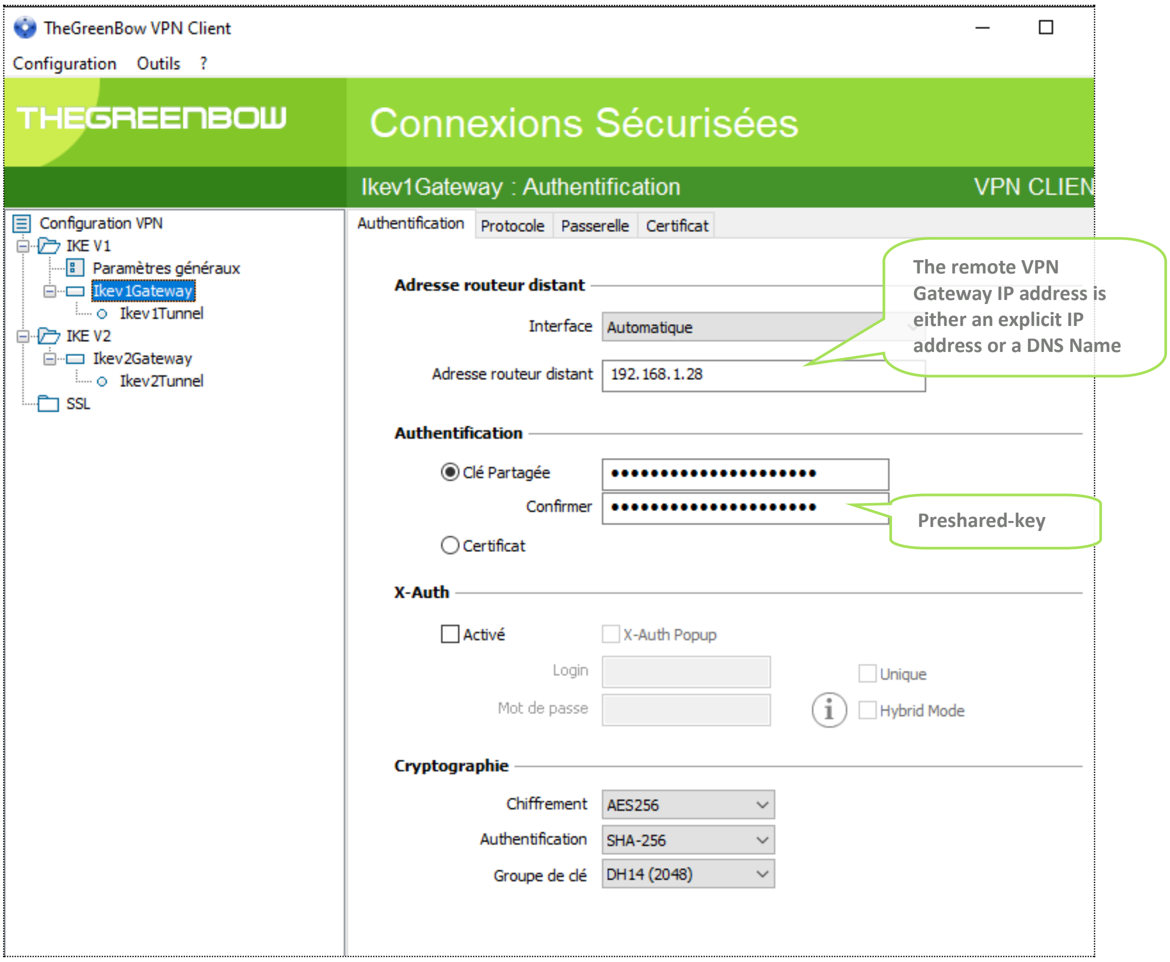


	Name	Group name	Policy	Connection type	Status Active
□	TGB_IKVE1	-	Default Policy	Remote access	●
□	TGB_IKVE2	-	IKEv2_TGB	Site-to-site	●

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 Phase 1 (IKE) Configuration



Adresse routeur distant

Interface: Automatique

Adresse routeur distant: 192.168.1.28

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

Authentification

● Clé Partagée: ••••••••••••••••••••

Confirmer: ••••••••••••••••••••

Preshared-key

○ Certificat

X-Auth

□ Activé

□ X-Auth Popup

Login

Mot de passe

□ Unique

□ Hybrid Mode

Cryptographie

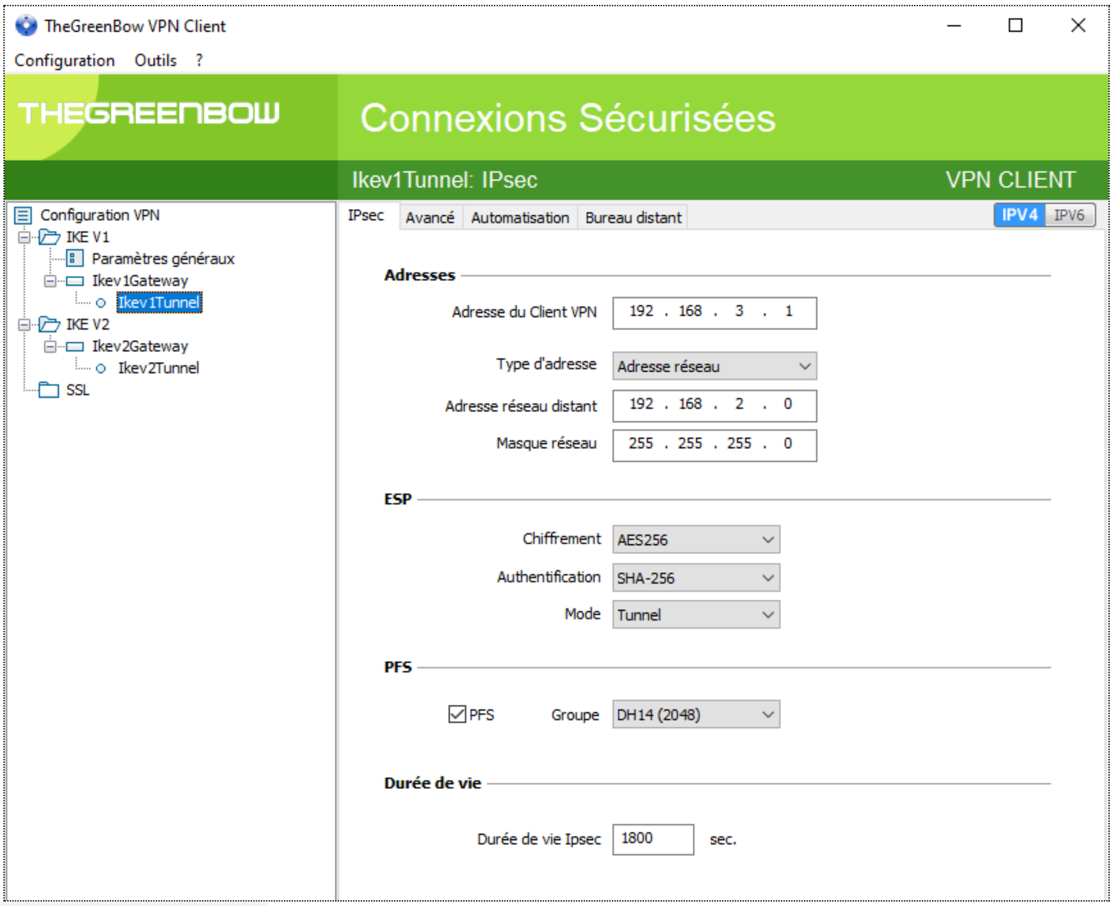
Chiffrement: AES256

Authentification: SHA-256

Groupe de clé: DH14 (2048)

Phase 1 configuration

3.2 VPN Client Phase 2 (IPsec) Configuration



Ikev1Tunnel: IPsec

Adresses

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

ESP

Chiffrement: AES256

Authentification: SHA-256

Mode: Tunnel

PFS

☑ PFS   Groupe: DH14 (2048)

Durée de vie

Durée de vie Ipsec: 1800 sec.

Phase 2 Configuration

You may use either Preshared key, Certificates, USB Tokens, OTP Token (One Time Password) or X-Auth combined with RADIUS Server for User Authentication with the SOPHOS XG Firewall router. 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.

3.3 Open IPsec VPN tunnels

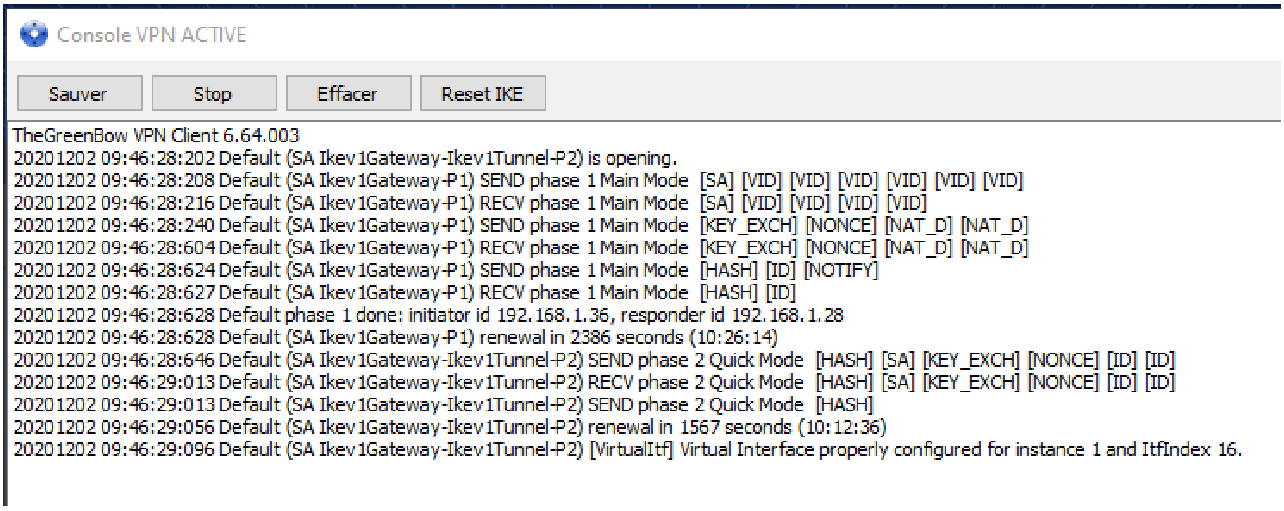
Once both SOPHOS XG Firewall router and TheGreenBow IPsec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPsec traffic.

1/ Click on "**Save & Apply**" to take into account all modifications we've made on your VPN Client configuration.

2/ Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPsec VPN Tunnel (e.g. ping, IE browser).

3/ Select "**Connections**" to see opened VPN Tunnels.

4/ Select "**Console**" if you want to access to the IPsec VPN logs and adjust filters to display less IPsec messaging. The following example shows a successful connection between TheGreenBow IPsec VPN Client and a SOPHOS XG Firewall VPN router.



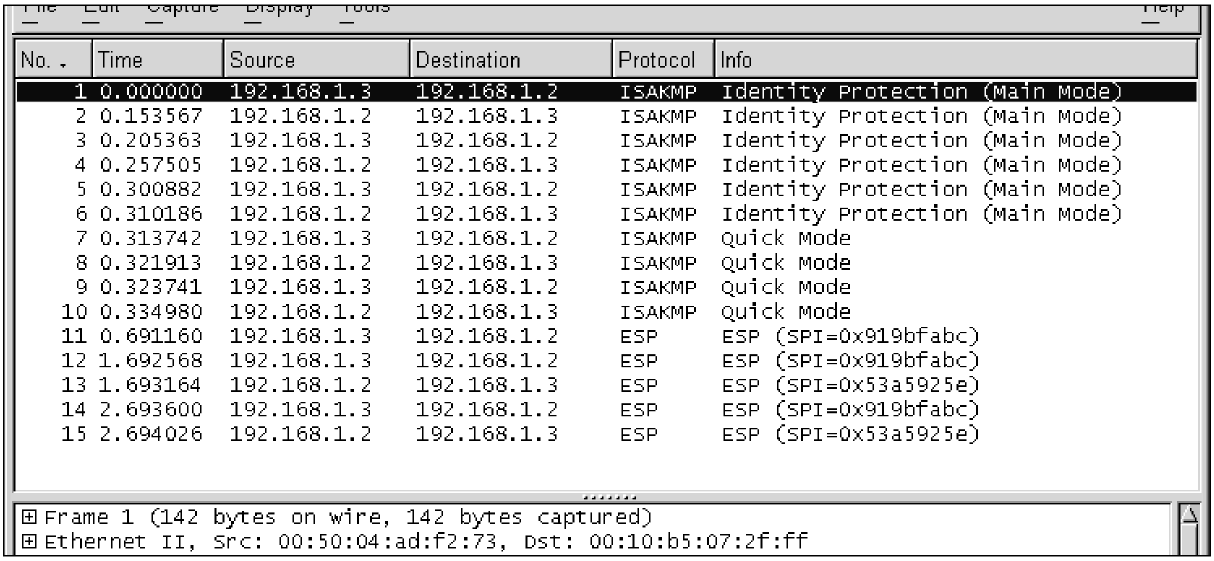
```
TheGreenBow VPN Client 6.64.003
20201202 09:46:28:202 Default (SA Ikev1Gateway-Ikev1Tunnel-P2) is opening.
20201202 09:46:28:208 Default (SA Ikev1Gateway-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID] [VID] [VID]
20201202 09:46:28:216 Default (SA Ikev1Gateway-P1) RECV phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID]
20201202 09:46:28:240 Default (SA Ikev1Gateway-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20201202 09:46:28:604 Default (SA Ikev1Gateway-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20201202 09:46:28:624 Default (SA Ikev1Gateway-P1) SEND phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20201202 09:46:28:627 Default (SA Ikev1Gateway-P1) RECV phase 1 Main Mode  [HASH] [ID]
20201202 09:46:28:628 Default phase 1 done: initiator id 192.168.1.36, responder id 192.168.1.28
20201202 09:46:28:628 Default (SA Ikev1Gateway-P1) renewal in 2386 seconds (10:26:14)
20201202 09:46:28:646 Default (SA Ikev1Gateway-Ikev1Tunnel-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20201202 09:46:29:013 Default (SA Ikev1Gateway-Ikev1Tunnel-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20201202 09:46:29:013 Default (SA Ikev1Gateway-Ikev1Tunnel-P2) SEND phase 2 Quick Mode  [HASH]
20201202 09:46:29:056 Default (SA Ikev1Gateway-Ikev1Tunnel-P2) renewal in 1567 seconds (10:12:36)
20201202 09:46:29:096 Default (SA Ikev1Gateway-Ikev1Tunnel-P2) [VirtualItf] Virtual Interface properly configured for instance 1 and ItfIndex 16.
```

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  Info
    1 0.000000  192.168.1.3    192.168.1.2    ISAKMP   Identity Protection (Main Mode)
    2 0.153567  192.168.1.2    192.168.1.3    ISAKMP   Identity Protection (Main Mode)
    3 0.205363  192.168.1.3    192.168.1.2    ISAKMP   Identity Protection (Main Mode)
    4 0.257505  192.168.1.2    192.168.1.3    ISAKMP   Identity Protection (Main Mode)
    5 0.300882  192.168.1.3    192.168.1.2    ISAKMP   Identity Protection (Main Mode)
    6 0.310186  192.168.1.2    192.168.1.3    ISAKMP   Identity Protection (Main Mode)
    7 0.313742  192.168.1.3    192.168.1.2    ISAKMP   Quick Mode
    8 0.321913  192.168.1.2    192.168.1.3    ISAKMP   Quick Mode
    9 0.323741  192.168.1.3    192.168.1.2    ISAKMP   Quick Mode
   10 0.334980  192.168.1.2    192.168.1.3    ISAKMP   Quick Mode
   11 0.691160  192.168.1.3    192.168.1.2    ESP      ESP (SPI=0x919bfabc)
   12 1.692568  192.168.1.3    192.168.1.2    ESP      ESP (SPI=0x919bfabc)
   13 1.693164  192.168.1.2    192.168.1.3    ESP      ESP (SPI=0x53a5925e)
   14 2.693600  192.168.1.3    192.168.1.2    ESP      ESP (SPI=0x919bfabc)
   15 2.694026  192.168.1.2    192.168.1.3    ESP      ESP (SPI=0x53a5925e)

⊞ Frame 1 (142 bytes on wire, 142 bytes captured)
⊞ Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff
```

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 endpoint 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 preshared key is correct or if the local ID is correct (see “Advanced” button). 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” Button) 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 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