

Windows VPN Client

Stormshield Configuration Guide

TheGreenBow is a registered trademark.

Microsoft and Windows 10 are either registered trademarks or brand names owned by Microsoft Corp. in the U.S.A. and/or in other countries.

Stormshield is a trademark of Stormshield in France and other countries.

Any other third-party trademarks mentioned in this document are the property of their respective owners.

All reproduction rights are reserved, including for iconographic or photographic representations. No part of this document may be copied and/or published by any means whatsoever without our express written consent.

All the information provided is subject to modifications at any time and without notice.

Despite our utmost care and attention in producing this document and its regular updates, errors may have been introduced in the information provided. If you notice any issues, please feel free to contact us and let us know. We will make the necessary changes.

Table of contents

1	Introduction	1
1.1	Purpose of document.....	1
1.2	VPN network topology.....	1
1.3	Stormshield VPN firewall	1
2	Configuring VPN on Stormshield firewall	2
3	Configuring the VPN Client	8
3.1	General configuration	8
3.2	Configuring the VPN Client for a Phase 1 (IKE Auth)	9
3.3	Configuring the VPN Client for a Phase 2 (Child SA)	12
3.4	Opening the VPN connection	12
4	Troubleshooting	14
4.1	A good network analyzer: Wireshark	14
4.2	Troubleshooting TheGrenBow VPN Client	14
4.2.1	“NO_PROPOSAL_CHOSEN” error (wrong IKE Auth)	14
4.2.2	“AUTHENTICATION_FAILED” error	15
4.2.3	“No user certificate available for the connection” error.....	15
4.2.4	“Remote ID rejected” error	15
4.2.5	“NO_PROPOSAL_CHOSEN” error (wrong CHILD SA)	15
4.2.6	“FAILED_CP_REQUIRED” error.....	16
4.2.7	I clicked on “Open tunnel”, but nothing happens	16
4.2.8	The VPN tunnel is up but I can’t ping!	17
5	Contact	18
5.1	Information.....	18
5.2	Sales.....	18
5.3	Support	18



Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2021-12-01	All	Initial draft	BB

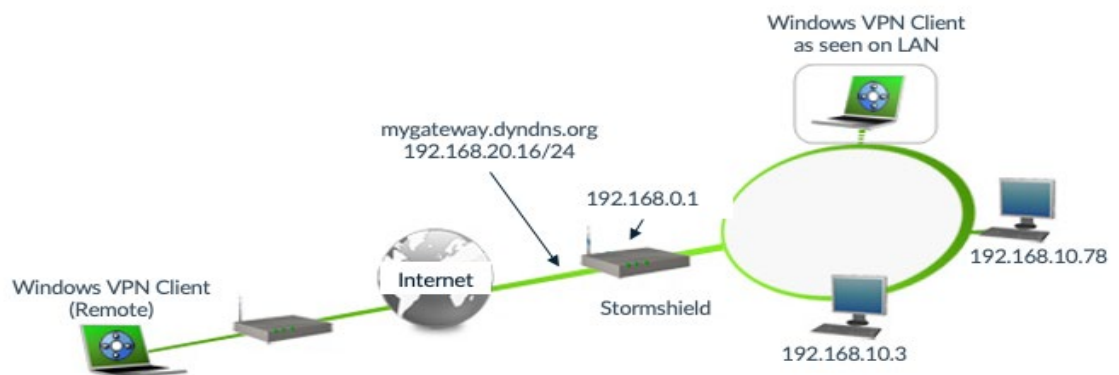
1 Introduction

1.1 Purpose of document

This configuration guide describes how to configure TheGreenBow Windows Enterprise VPN Client software with a Stormshield firewall to establish VPN connections for remote access to a corporate network.

1.2 VPN network topology

In our VPN network example (see diagram below), we will connect TheGreenBow Windows Enterprise VPN Client software to the LAN behind the Stormshield firewall. The VPN client is connected to the internet over a DSL connection or through a LAN. All addresses in this document merely serve as examples.



1.3 Stormshield VPN firewall

Our tests and VPN configuration have been conducted with Stormshield SNS version 4.2.0.

Refer to the following page for more information on the Stormshield SNS v4 firewall:

https://documentation.Stormshield.eu/SNS/v4/en/Content/User_Configuration_Manual_SNS_v4/Configuration/General_configuration_tab.htm.

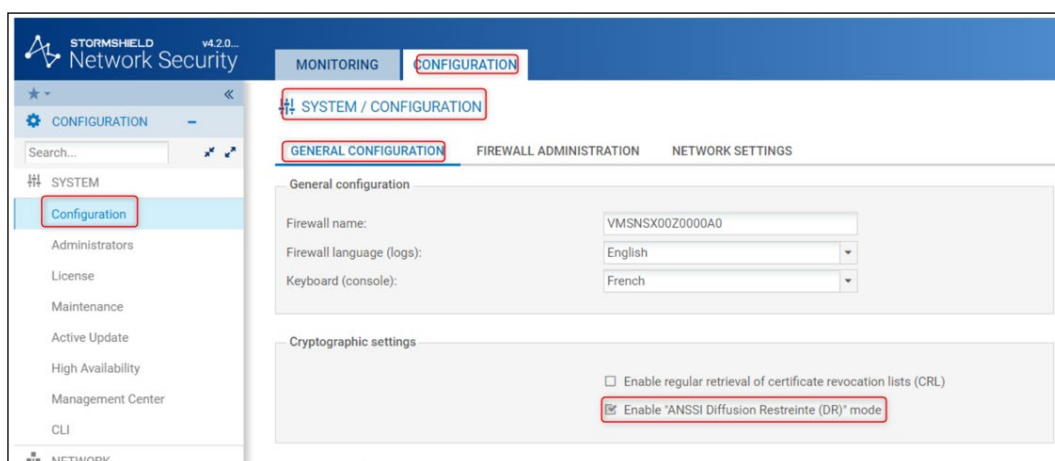
It is essential for users to find all the required information regarding the Stormshield firewall. All product information, User's Guides, and knowledge base articles for the Stormshield VPN firewall can be found on the Stormshield website at: <https://www.Stormshield.com/>.

2 Configuring VPN on Stormshield firewall

This section describes how to build a VPN configuration for your Stormshield firewall.

Once you have logged in to your Stormshield firewall, proceed as follows in the user interface:

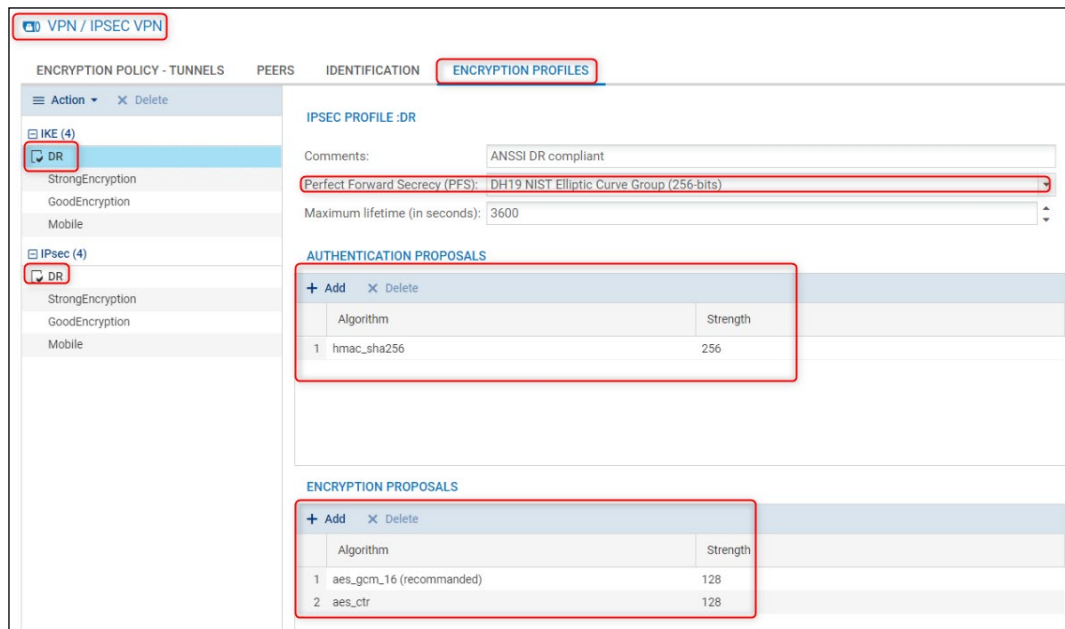
1. From the left menu, select **System** and then **Configuration**.
2. Under **General Configuration**, click **Enable "ANSSI Diffusion Restreinte (DR)" mode**.



3. From the left menu, select **Network** and then **Interfaces**.
4. Configure the WAN (**out**) and LAN (**in**) network interfaces.

NETWORK / INTERFACES				
Enter a filter Edit Add Delete Monitor				
Interface	P...	Type	Sta...	IPv4 address
out	1	Eth...		192.168.20.16/24 (DHCP)
in	2	Eth...		172.168.0.1/24

5. Navigate to **VPN / IPsec VPN** and configure the options according to the following screenshot:



6. Navigate to **Objects / Certificate and PKI**, and configure the DR Encryption profile by creating a set of ECDSA SECP256 certificates (CA certificate, Server Certificate, Client Certificate).

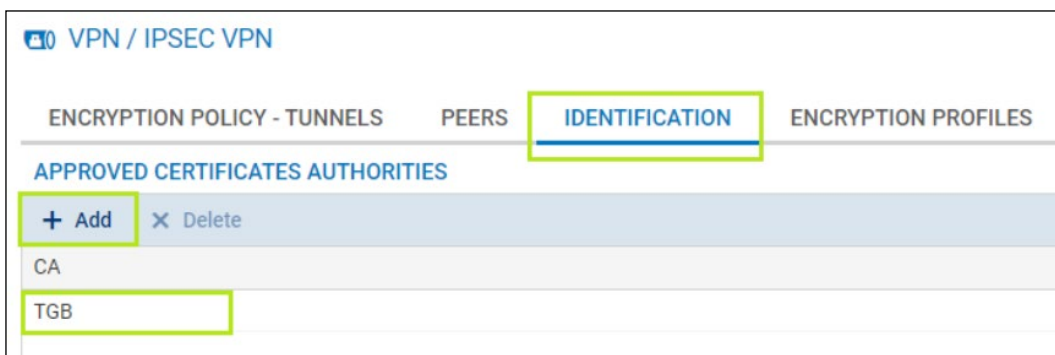
In the screenshot below, the configuration is as follows:

- CA certificate is **TGB**
- Server certificate is **firewallecdsa**
- Client certificate is **mobile**

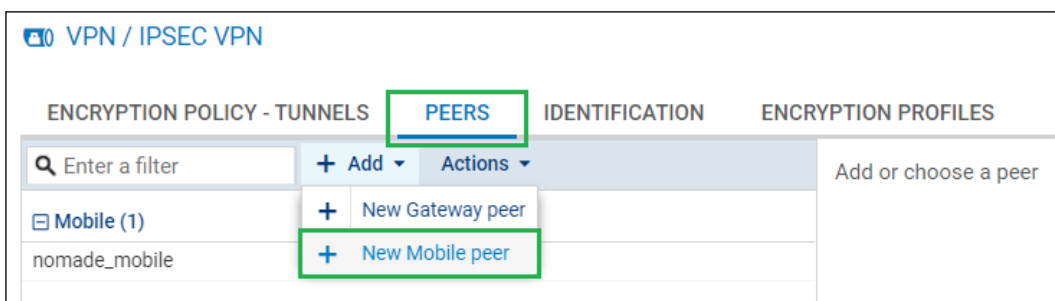
7. Import this certificate to the VPN Client



8. Navigate back to **VPN / IPsec VPN** and configure the certificates in the **Identification** tab according to the following screenshot:



9. In the **Peers** tab, add a new mobile peer.



The following window will be displayed:



10. Select **IKEV2**.

The following screen will be displayed:

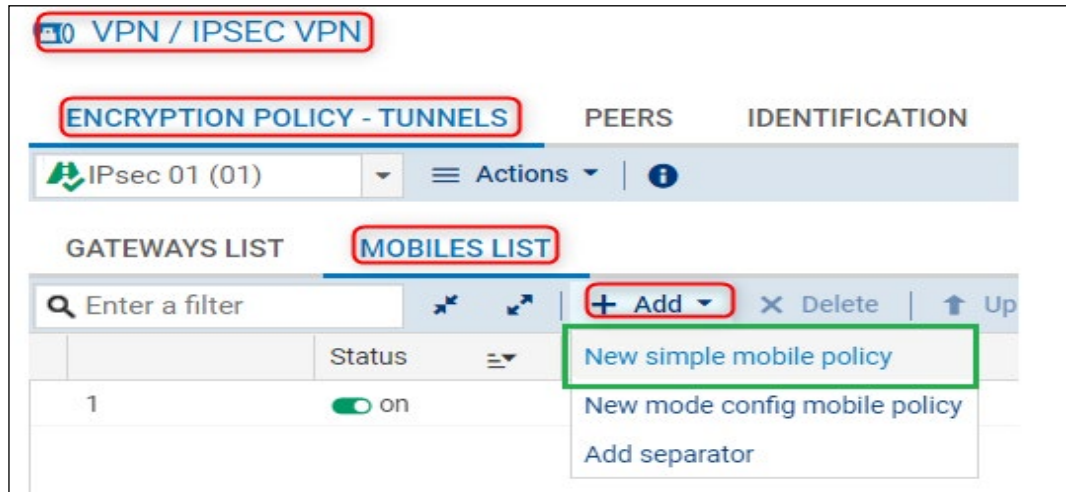
11. Choose **Certificate**, and then click » **Next**.

12. Select a server certificate as shown in the following screenshot:

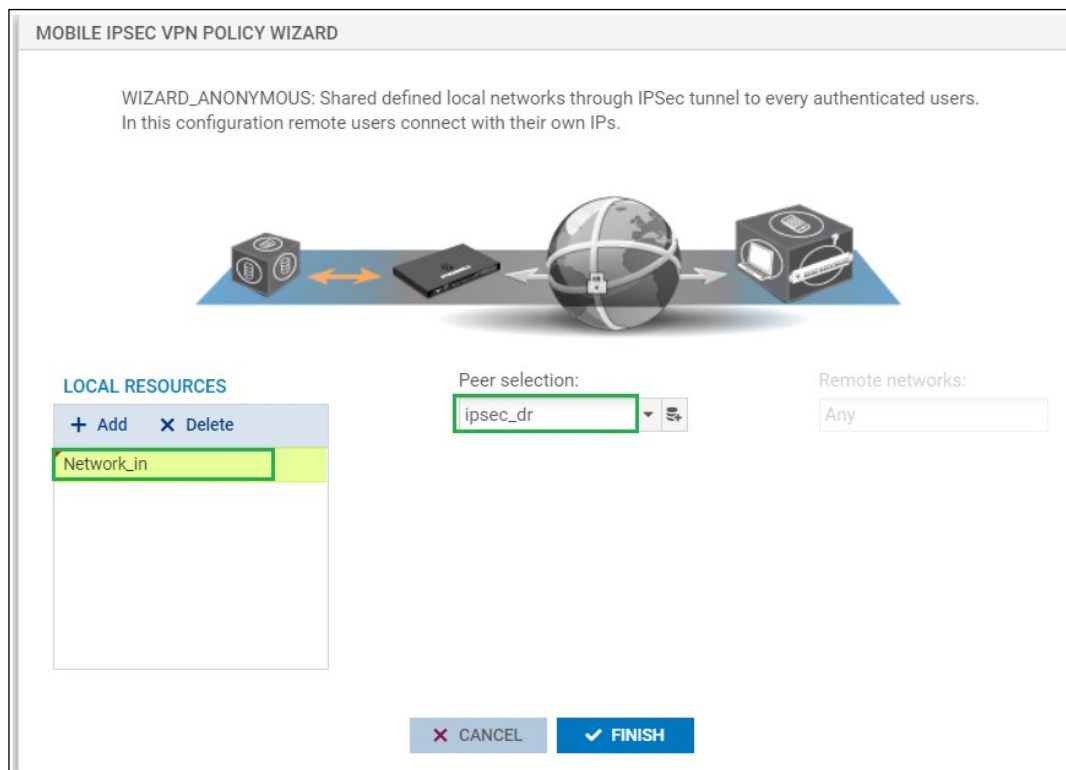
The following screen shows a summary of the IKE Auth configuration on the Stormshield SNS firewall:

Now, proceed with configuring the “Child SA” part of the IPsec IKEv2 connection.

1. Navigate to **VPN / IPsec VPN** and select the **Encryption Policy – Tunnels** tab.



2. Select **Mobiles List** and click **+ Add**.
3. Choose **New simple mobile policy**. The following screen will be displayed:



4. Select the network interfaces that you want to use for the VPN connection, and then click **Finish**.

The following screen shows a summary of the Child SA configuration on the Stormshield SNS firewall:

The screenshot displays the 'VPN / IPSEC VPN' configuration page. The 'ENCRYPTION POLICY - TUNNELS' tab is active, showing a list of tunnels. A dropdown menu is open, displaying 'IPsec 01 (01)'. Below the dropdown, there are tabs for 'GATEWAYS LIST' and 'MOBILES LIST'. The 'MOBILES LIST' tab is selected, showing a table with the following data:

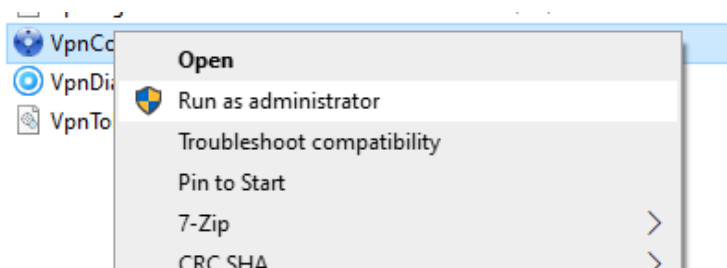
	Status	Local network	Peer	Remote network	Conf	modeconfig
1	on	Network_in	ipsec_dr	Any	DR	off

3 Configuring the VPN Client

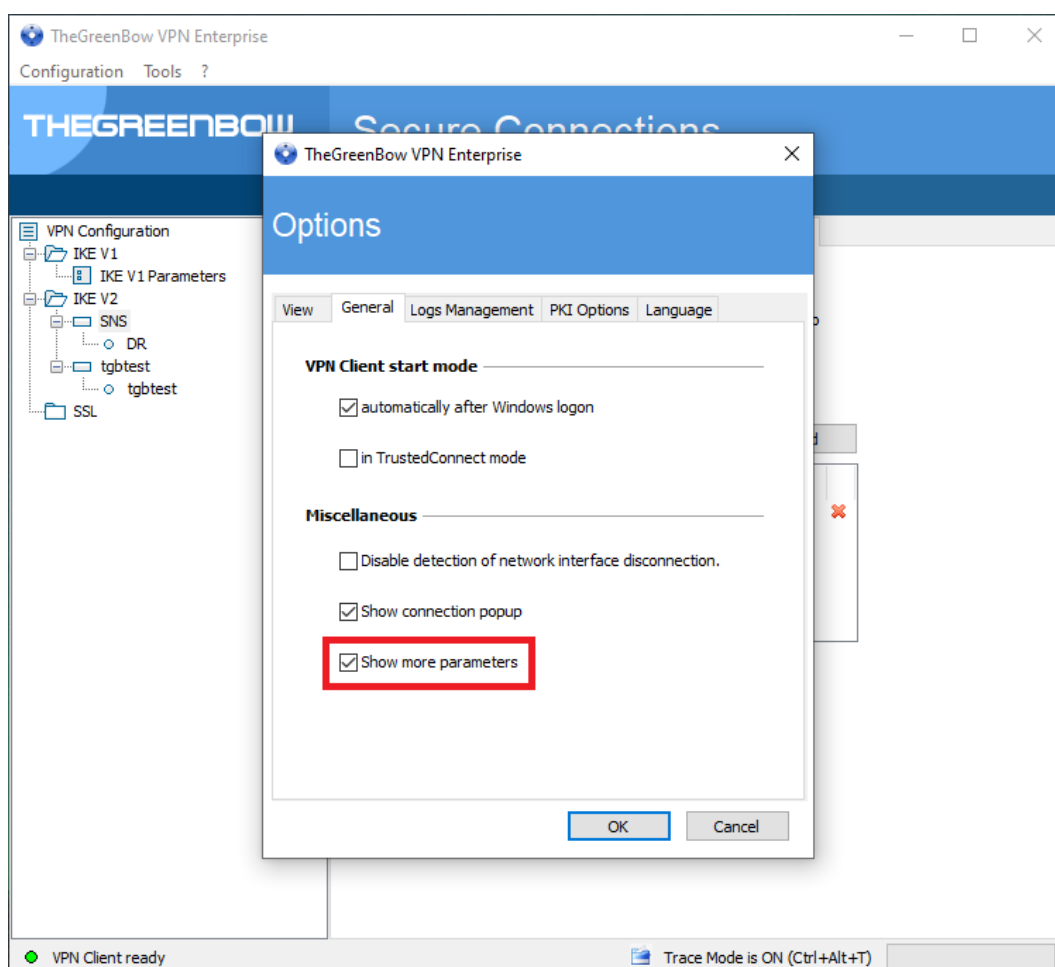
This section describes the required configuration for TheGreenBow's Windows Enterprise VPN Client to connect to a Stormshield firewall.

3.1 General configuration

By default, only administrators can access the Windows Enterprise VPN Client Configuration Panel. Therefore, right-click **vpnconf.exe** in the **File Explorer** and select **Run as administrator**.

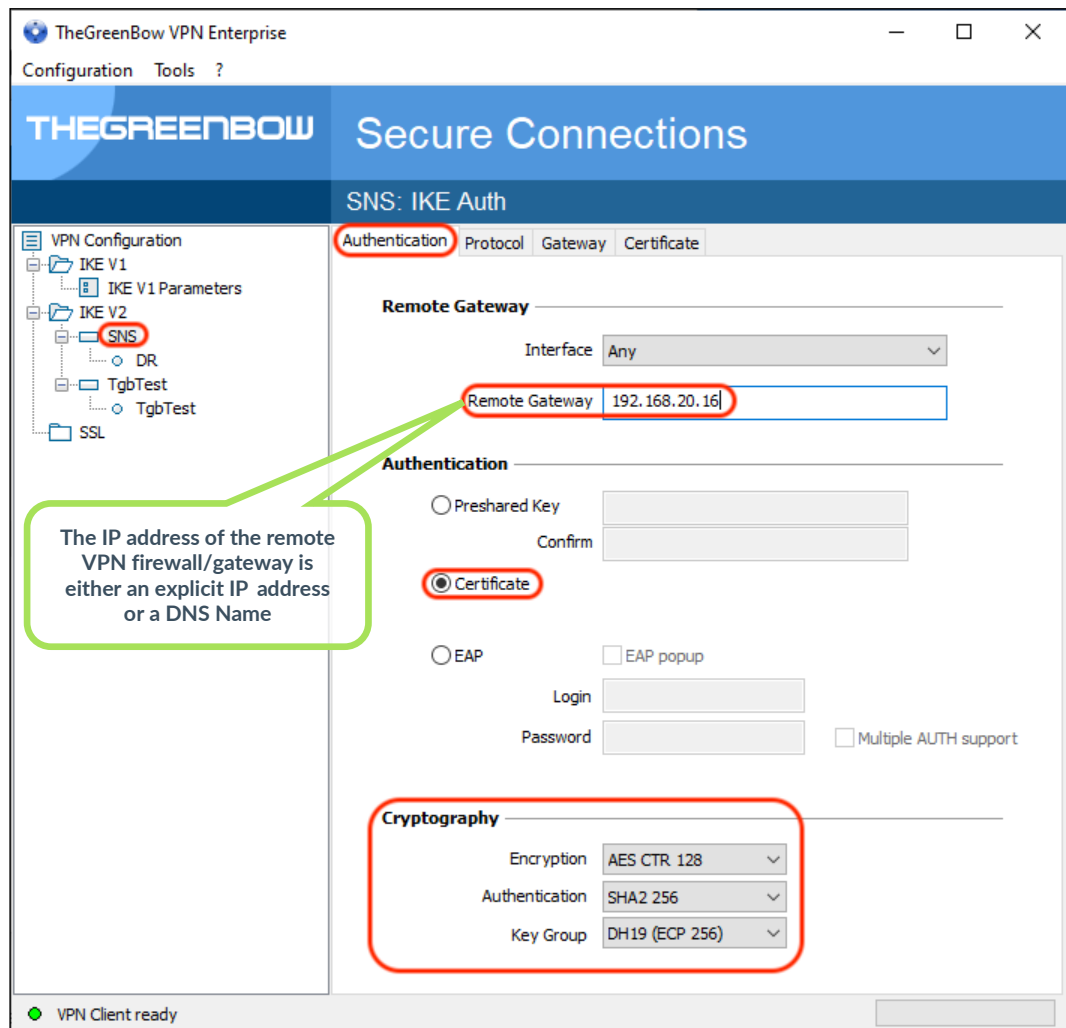


From the **Tools** menu, choose **Options**, and then select the **General** tab. Make sure the **Show more parameters** item is checked.

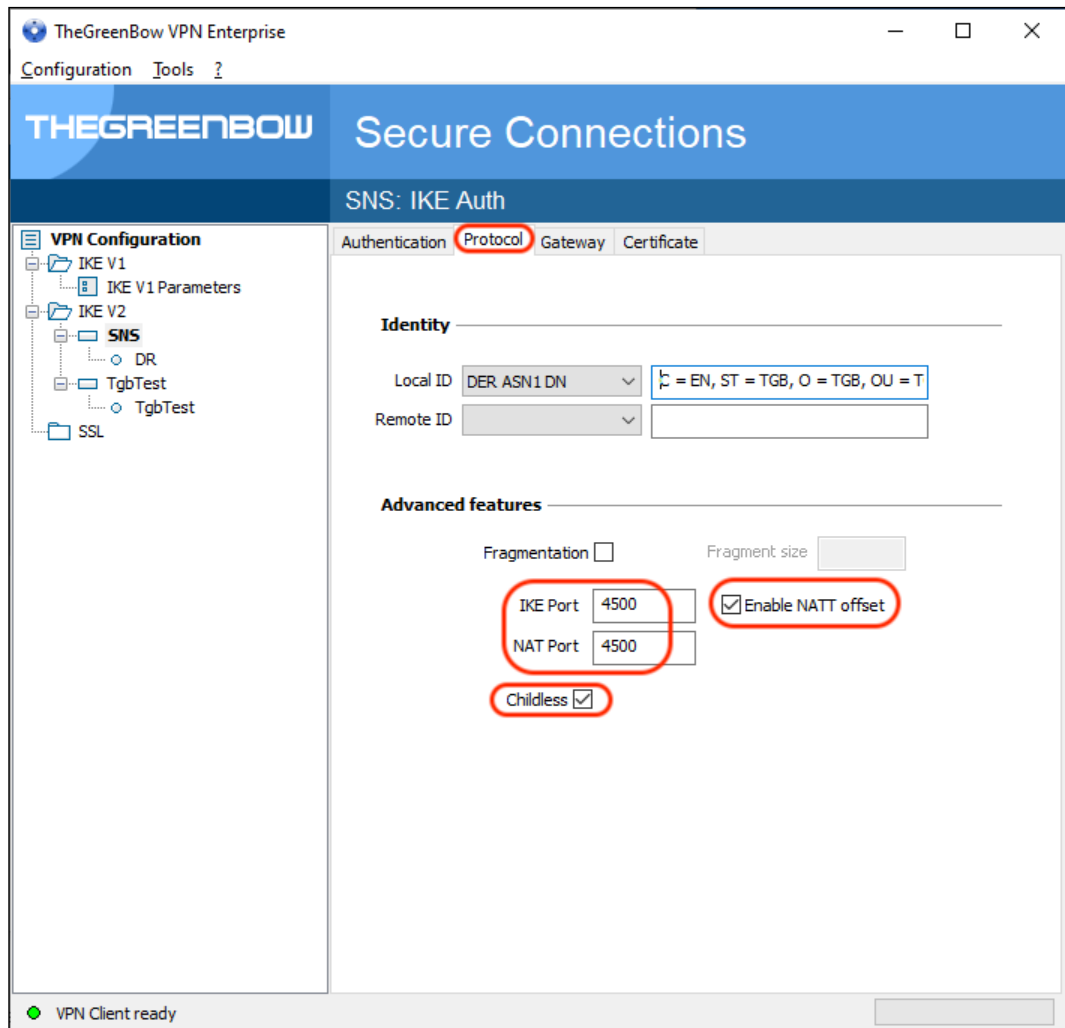


3.2 Configuring the VPN Client for a Phase 1 (IKE Auth)

To configure TheGreenBow Windows Enterprise VPN Client for a Phase 1 (IKE Auth), proceed as shown in the following screenshot:



Set the following additional parameters in the **Protocol** tab:

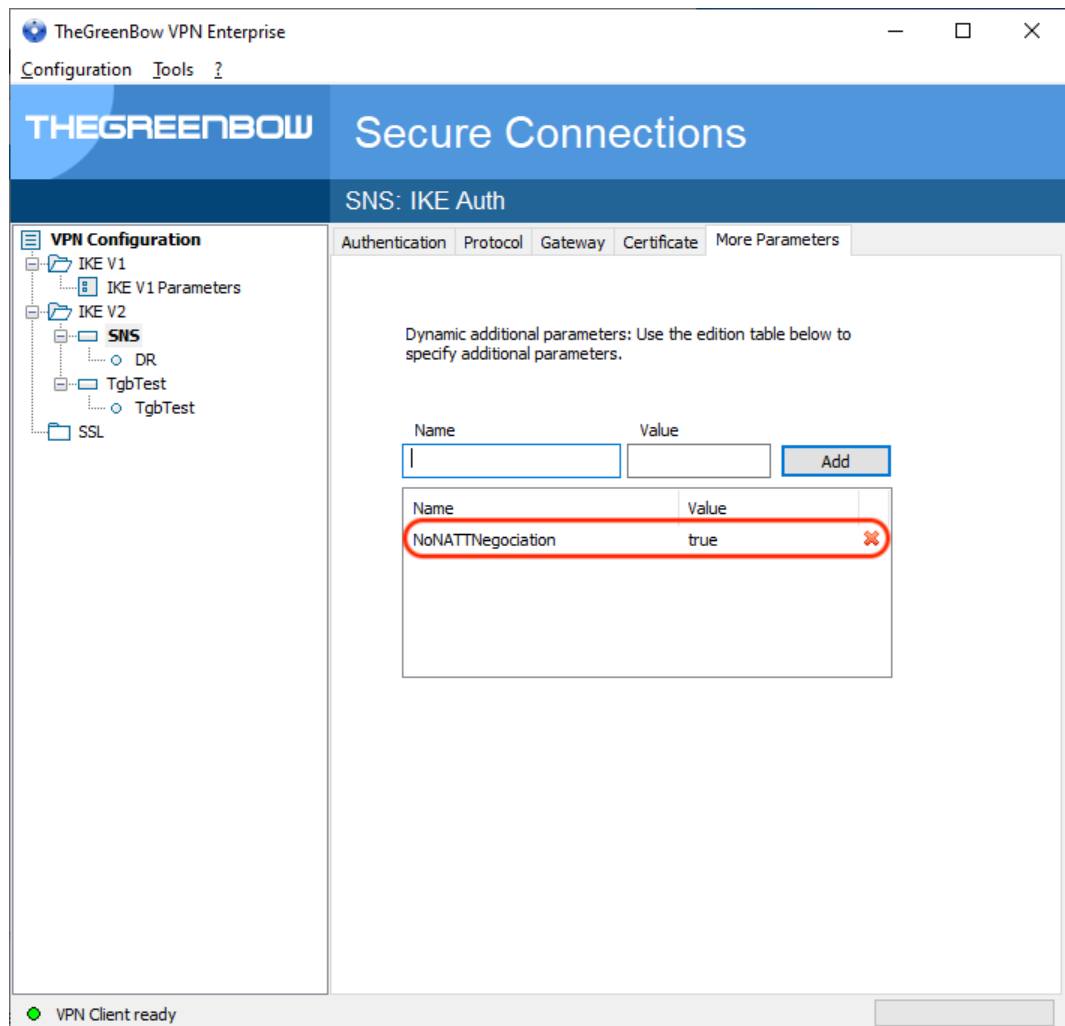


The screenshot shows the 'TheGreenBow VPN Enterprise' configuration window. The 'Secure Connections' section is active, and the 'SNS: IKE Auth' configuration is selected. The 'Protocol' tab is highlighted, showing the following settings:

- Identity:**
 - Local ID: DER ASN1 DN (dropdown menu)
 - Remote ID: (empty dropdown menu)
- Advanced features:**
 - Fragmentation: ☐ (unchecked)
 - Fragment size: (empty text box)
 - IKE Port: 4500 (text box)
 - NAT Port: 4500 (text box)
 - Childless: ☒ (checked)
 - Enable NATT offset: ☒ (checked)

The status bar at the bottom indicates 'VPN Client ready'.

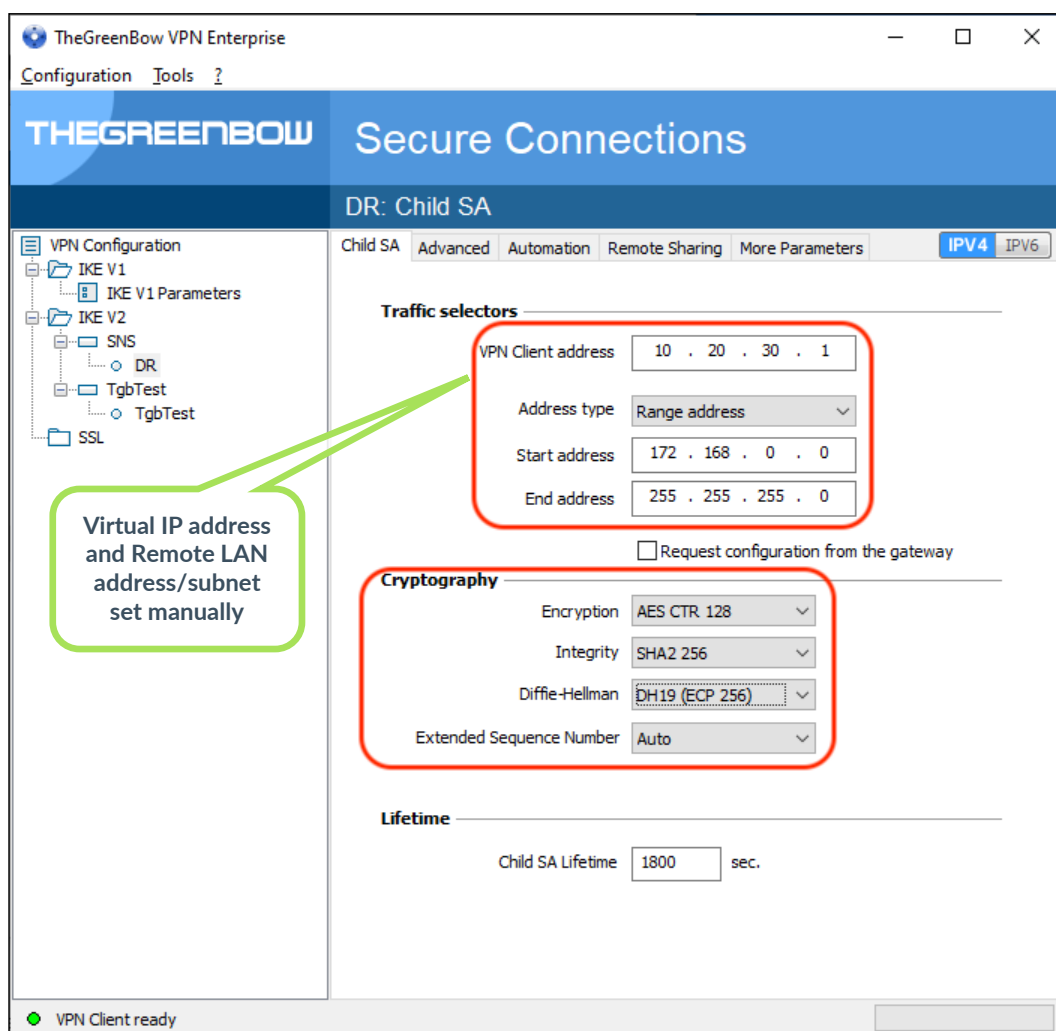
On the **More parameters**¹ tab, add a dynamic parameter named **NoNATTNegociation** with its value set to **true**:



¹ If you do not see the **More parameters** tab, you need to activate it in the options. To do this, from the **Tools** menu, selection **Options...**, select the **General** tab, and then check the **Show more parameters** box.

3.3 Configuring the VPN Client for a Phase 2 (Child SA)

To configure TheGreenBow Windows Enterprise VPN Client for a Phase 2 Child SA), proceed as shown in the following screenshot:

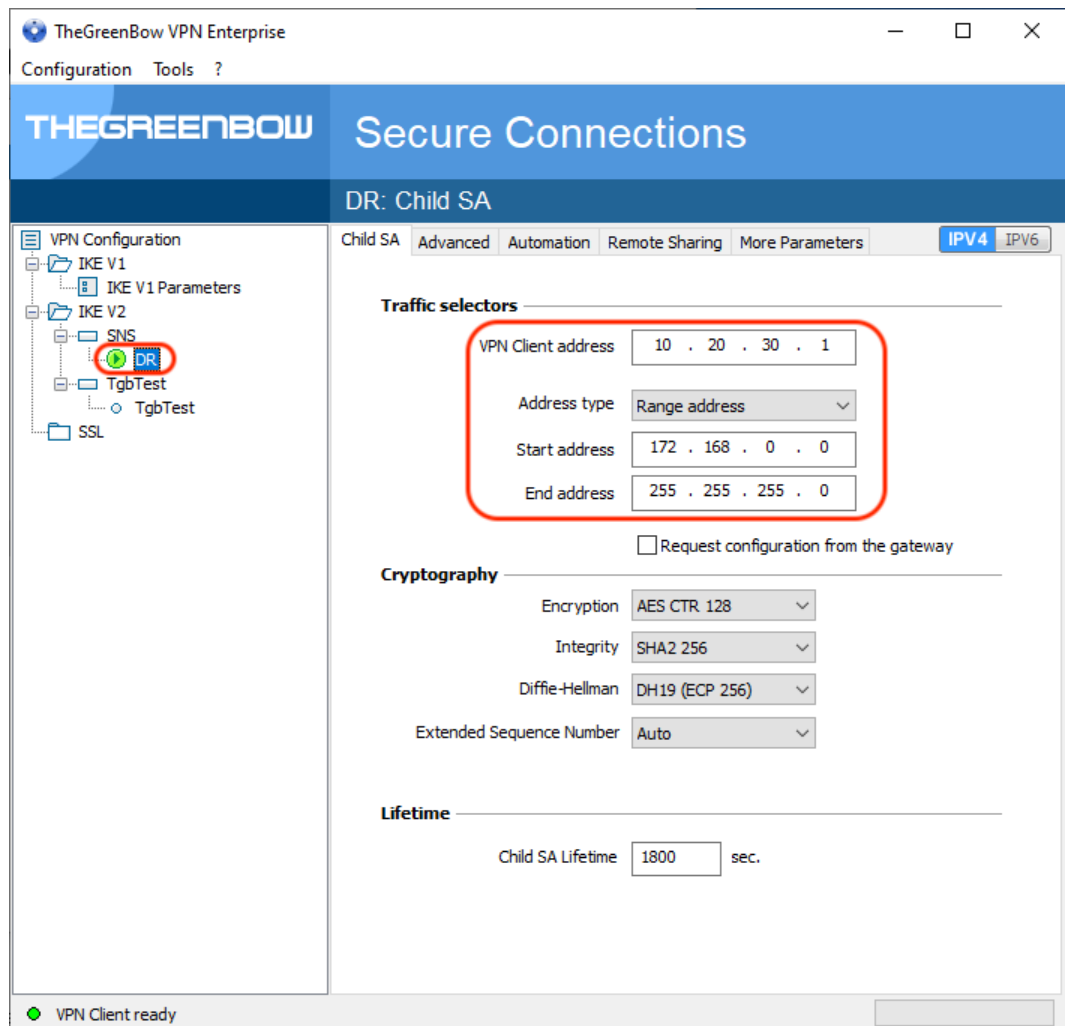


1. In TheGreenBow Windows Enterprise VPN Client, from the **Configuration** menu, select **Save** to account for all the changes you've made to your VPN configuration.
2. Double-click your Child SA tunnel name or click **Open** in the **Connection Panel** to open a tunnel.

3.4 Opening the VPN connection

Once both the Stormshield firewall and TheGreenBow Windows Enterprise VPN Client have been configured as described above, you are ready to open VPN connections.

The following screenshot shows a successful connection between TheGreenBow Windows Enterprise VPN Client and a Stormshield firewall:





4 Troubleshooting

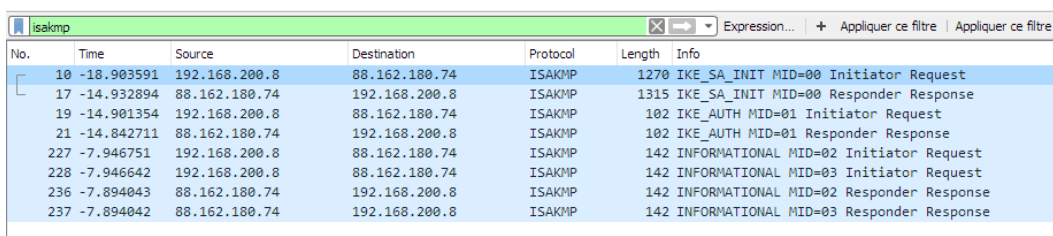
If the VPN connection cannot be established, start by checking that no parameters are missing. Also check the Console log in TheGreenBow VPN Client for any relevant information.

If you are still stuck, there are a few troubleshooting tools available that will help you find the source of issues when establishing a VPN connection. For instance, you can try using Wireshark (see next section).

4.1 A good network analyzer: Wireshark

Wireshark is free software that you can use for packet and traffic analysis. It shows IP or TCP packets received on and sent from a network card. This tool is available on www.wireshark.org. It can be used to follow protocol exchanges between two devices. For installation and use details, refer to the Wireshark documentation (www.wireshark.org/docs/).

The following screenshot shows an example of IPsec packets received by the network card and displayed in Wireshark:



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

4.2 Troubleshooting TheGreenBow VPN Client

4.2.1 “NO_PROPOSAL_CHOSEN” error (wrong IKE Auth)

If you encounter a “NO_PROPOSAL_CHOSEN” error, you might have a wrong Phase 1 [IKE Auth]. Check whether the encryption algorithms are the same at both ends of the VPN connection.

```
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)]
```

4.2.2 “AUTHENTICATION_FAILED” error

If you encounter an “AUTHENTICATION_FAILED” error, this means that the certificate or the preshared key does not match. Check whether the user certificate or preshared key is valid on the firewall/gateway.

```
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
```

4.2.3 “No user certificate available for the connection” error

Check whether the certificate is selected or if the token (smart card) is available on the computer.

```
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.
```

4.2.4 “Remote ID rejected” error

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

```
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
```

4.2.5 “NO_PROPOSAL_CHOSEN” error (wrong CHILD SA)

If you encounter a “NO_PROPOSAL_CHOSEN” error, make sure the “Child SA” encryption algorithms are the same at both ends of the VPN connection.



```
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_I
P)][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_TF
C_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
```

4.2.6 “FAILED_CP_REQUIRED” error

If you encounter a “FAILED_CP_REQUIRED” error, the firewall/gateway is configured to use Mode CP. In TheGreenBow Windows Enterprise VPN Client, go to **Traffic selectors** and enable **Request configuration from the gateway**.

```
20XX0913 16:29:46:780 TIKEV2_Tunnel RECV IKE_AUTH
[HDR][IDr][CERT][AUTH][N(AUTH_LIFETIME)][N(FAILED_CP_REQUIRED)][N(TS_UNACCEPTA
BLE)]
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
```

4.2.7 I clicked on “Open tunnel”, but nothing happens

Read the logs of each VPN tunnel endpoint. Some firewalls drop IKE requests. An IPsec Client uses UDP port 500 and protocol ESP.

Check whether the remote server is online.

```
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.
```

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

If the VPN tunnel is up, but you still cannot ping the remote LAN, you can try applying the following guidelines:

- In the VPN Client, check Child SA settings: VPN Client address and Remote LAN address. Usually, the VPN Client's IP address should not belong to the remote LAN subnet.
- Once the VPN tunnel is up, packets are sent using the ESP protocol. The firewall may block this protocol. Make sure that every device between the client and the VPN server accepts ESP.
- Check your VPN server logs. One of its firewall rules may drop packets.
- Check whether your ISP supports ESP.
- If you still cannot ping, follow ICMP traffic on the VPN server's LAN interface and on the computer's LAN interface (e.g. using Wireshark). You will have an indication of whether encryption is working.
- Check the "default gateway" value on the VPN Server LAN. A target on your remote LAN can receive pings but does not answer, because there is no "Default gateway" setting is enabled.
- You cannot access the computers in the LAN using their name. You must specify their IP address inside the LAN.
- We recommend that you install Wireshark (www.wireshark.org) on one of your target computers. You will thus be able to check whether your pings reach inside the LAN.



5 Contact

5.1 Information

All the information on TheGreenBow products is available on our website:
<https://thegreenbow.com/>.

5.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

5.3 Support

There are several pages related to the software's technical support on our website:

Online help

<https://www.thegreenbow.com/en/support/online-support/>

FAQ

<https://www.thegreenbow.com/en/frequently-asked-questions/>

Contact form

Technical support can be reached using the form on our website at the following address: <https://www.thegreenbow.com/en/support/online-support/technical-support/>.

Protect your connections
in any situation