# Windows VPN Client

## Fortinet Configuration Guide

Latest update: 1 December 2021
Document reference number: 20211201_CG_Fortinet_EN_1.0



www.thegreenbow.com

# Table of contents

# Document revision history

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

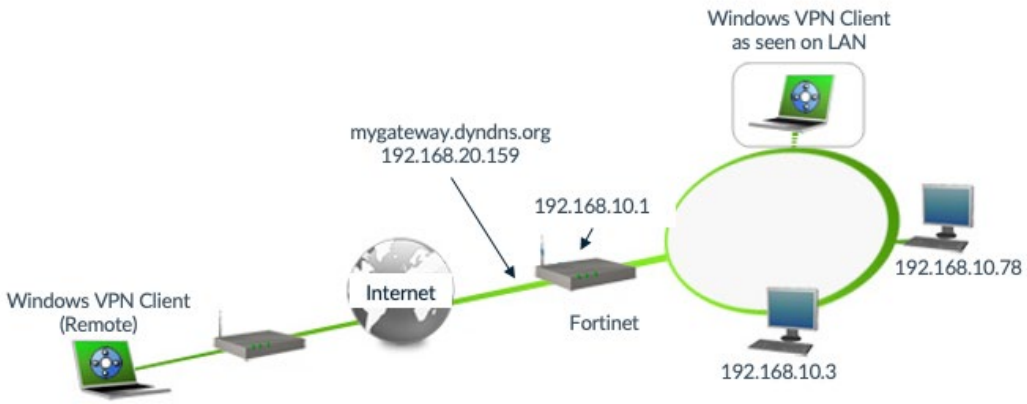
# 1 Introduction

## 1.1 Purpose of document

This configuration guide describes how to configure TheGreenBow Windows VPN Client software with a FortiGate Next Generation 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 VPN Client software to the LAN behind the FortiGate Next Generation 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 FortiGate Next Generation Firewall

Our tests and VPN configuration have been conducted with Fortinet VM firmware version 6.2.4.

## 1.4 FortiGate Next Generation Firewall product info

It is essential for users to find all the required information regarding the FortiGate Next Generation Firewall. All product information for the FortiGate Next Generation Firewall can be found on the Fortinet website at: https://www.fortinet.com/.

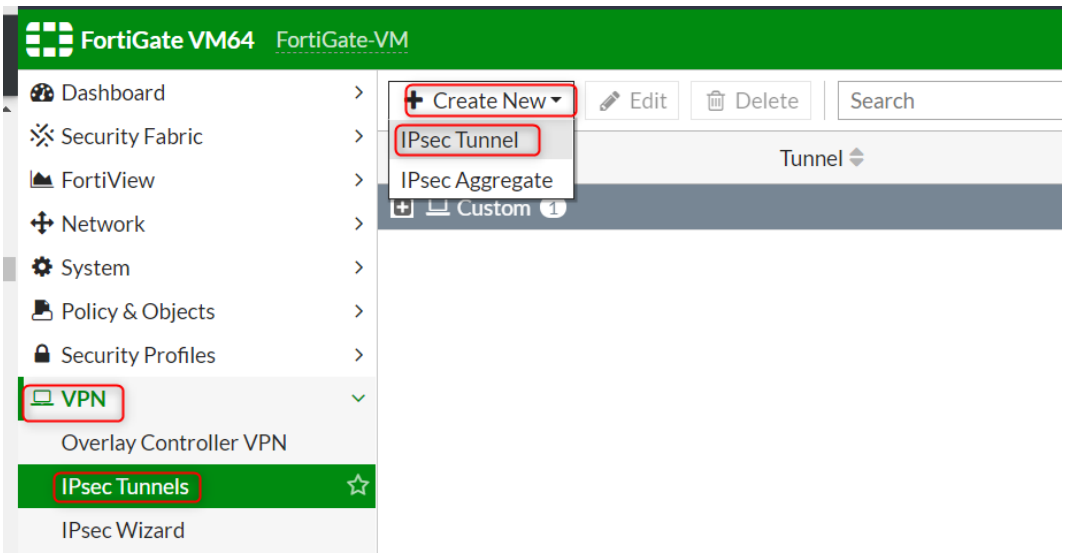
| | |
|---|---|
| Fortinet Product page | https://docs.fortinet.com/ |
| FortiGate/FortiOS 6.2.4 Cookbook | https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/954635/getting-started |
| FortiGate Knowledge Base | https://community.fortinet.com/t5/FortiGate/tkb-p/TKB20 |

# 2 Configuring VPN on Fortinet firewall

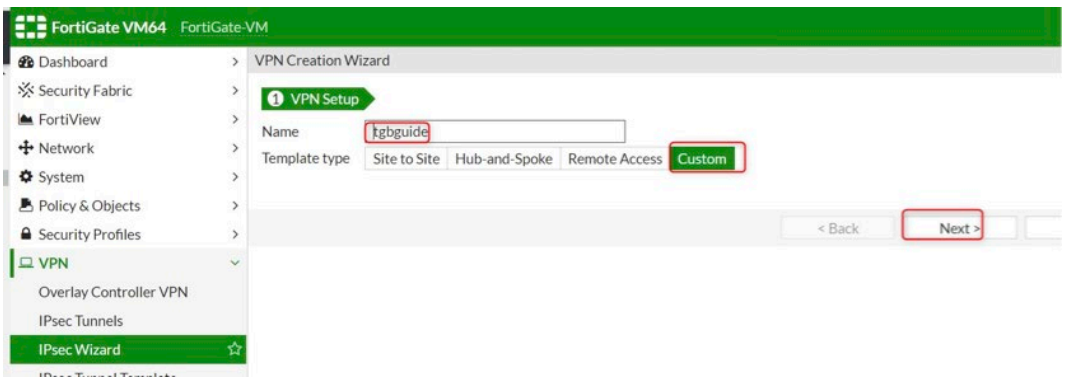
This section describes how to build a VPN configuration for your FortiGate Next Generation Firewall.

Once you have logged into your FortiGate Next Generation Firewall, proceed as follows in the user interface:

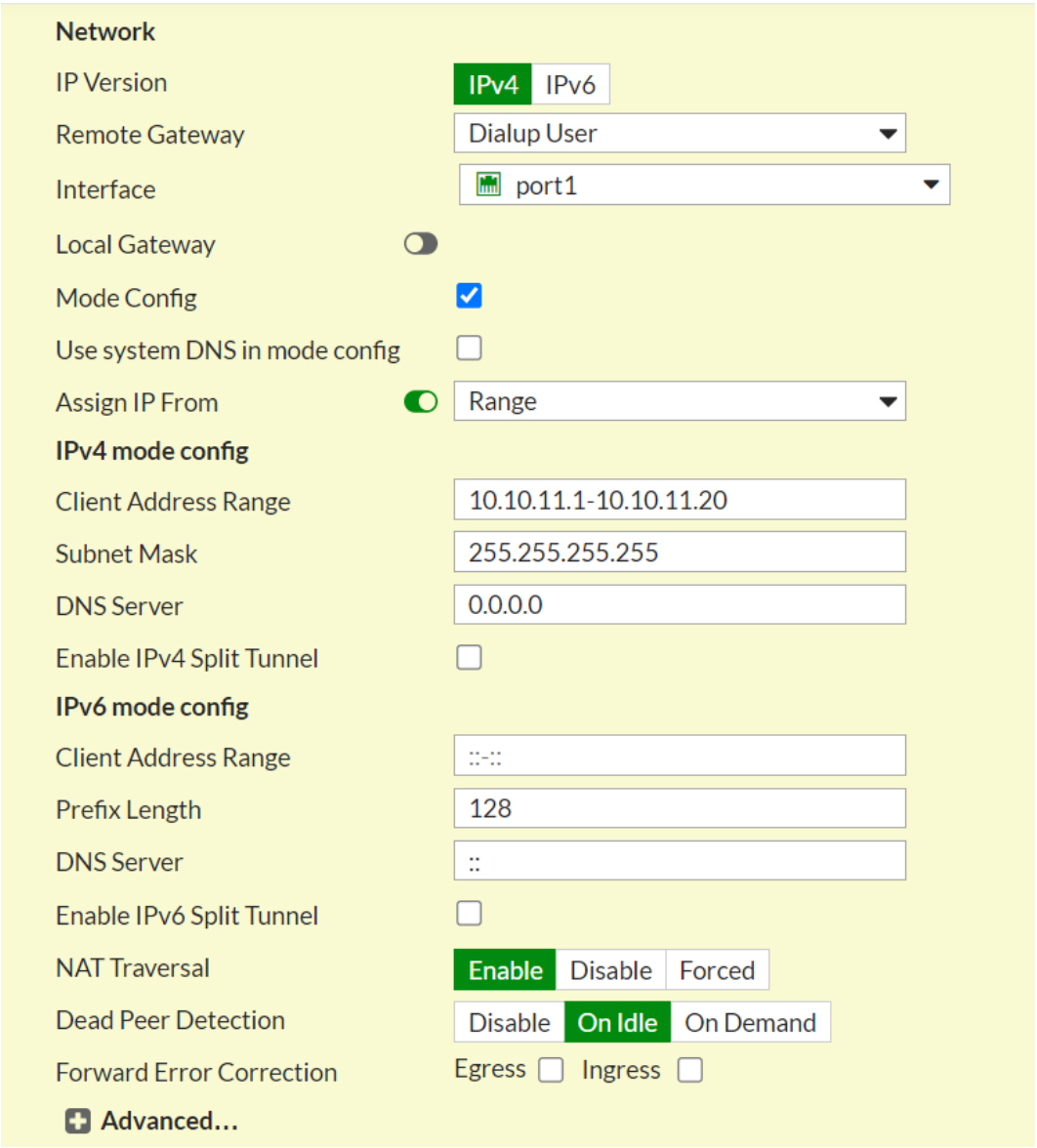
1. In the left menu, choose **VPN**, and then **IPsec Tunnels**.
2. Click **+ Create New**, and then select **IPsec Tunnel** to create a new VPN IPsec tunnel.



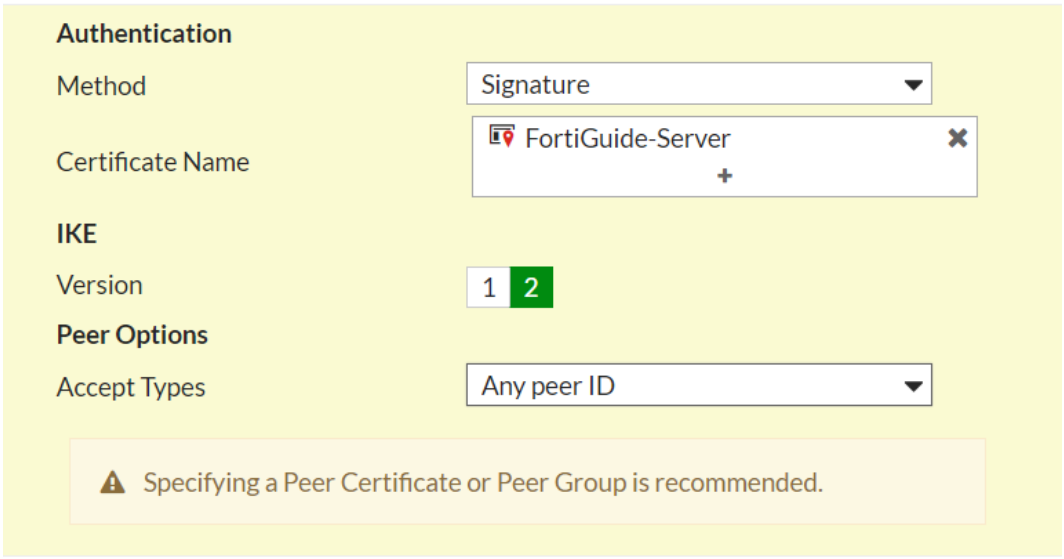

3. In the **IPsec Wizard**, enter a name for the VPN connection that you wish to create.
4. Choose the **Custom** template type.
5. Click **Next >**.



You will then see the following screen:

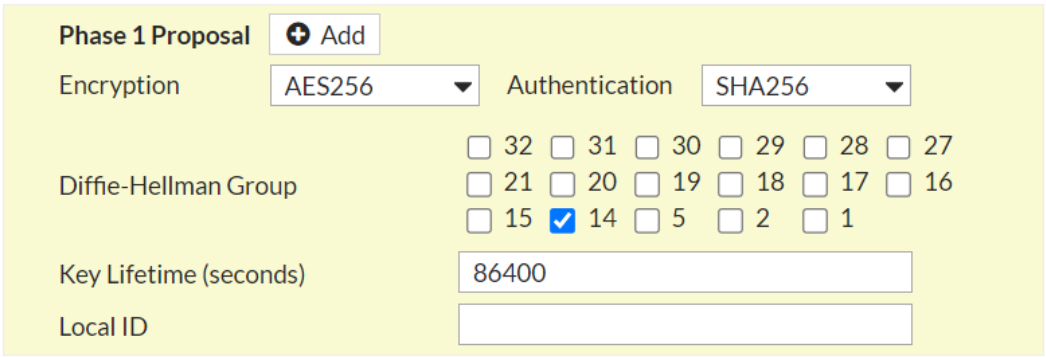



6. Click on **Advanced...** to make the **Authentication** section appear and select an existing certificate.

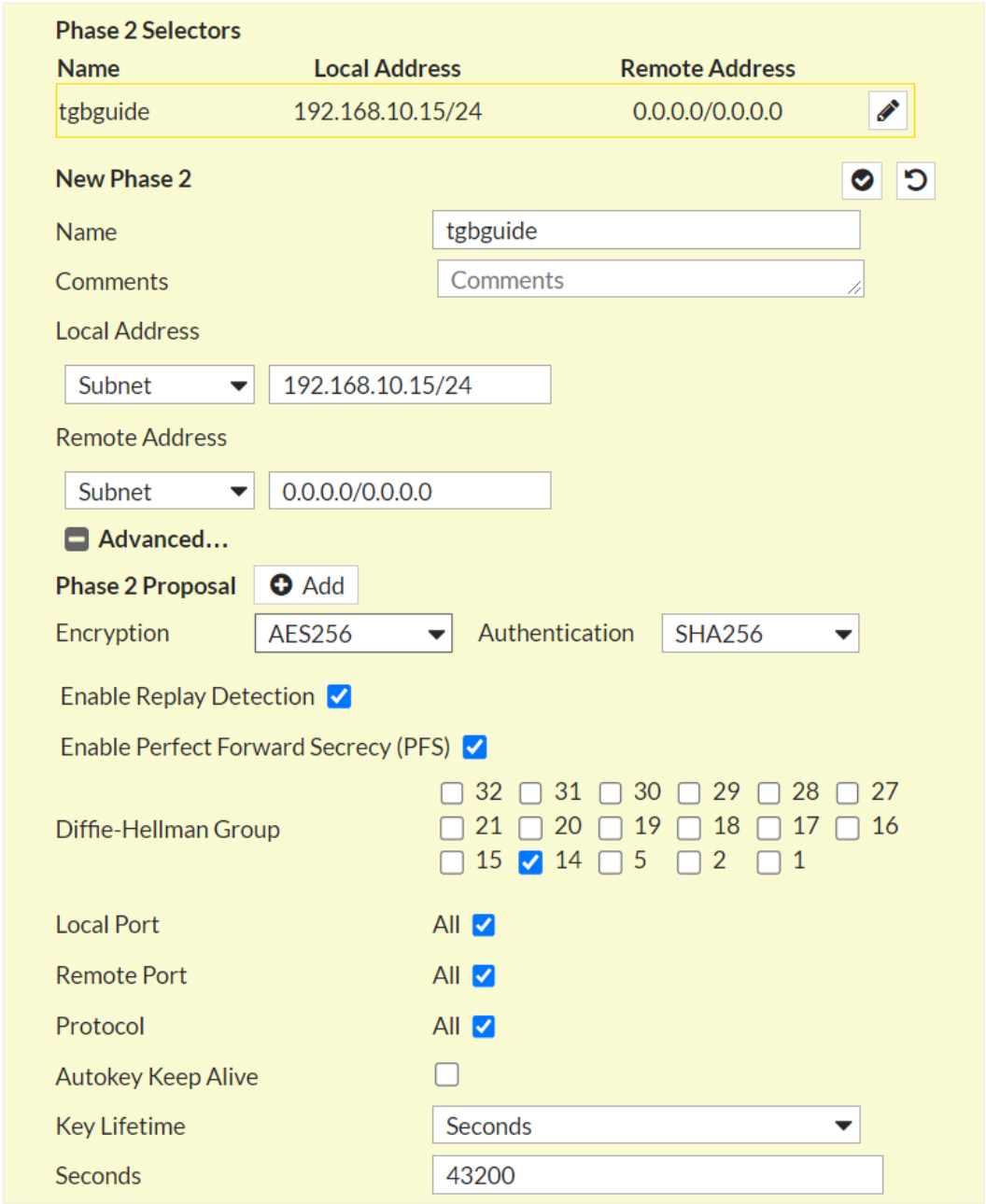



You may need to create a new certificate. In this case, follow the instructions provided on the following page: https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/825073/purchase-and-import-a-signed-ssl-certificate.

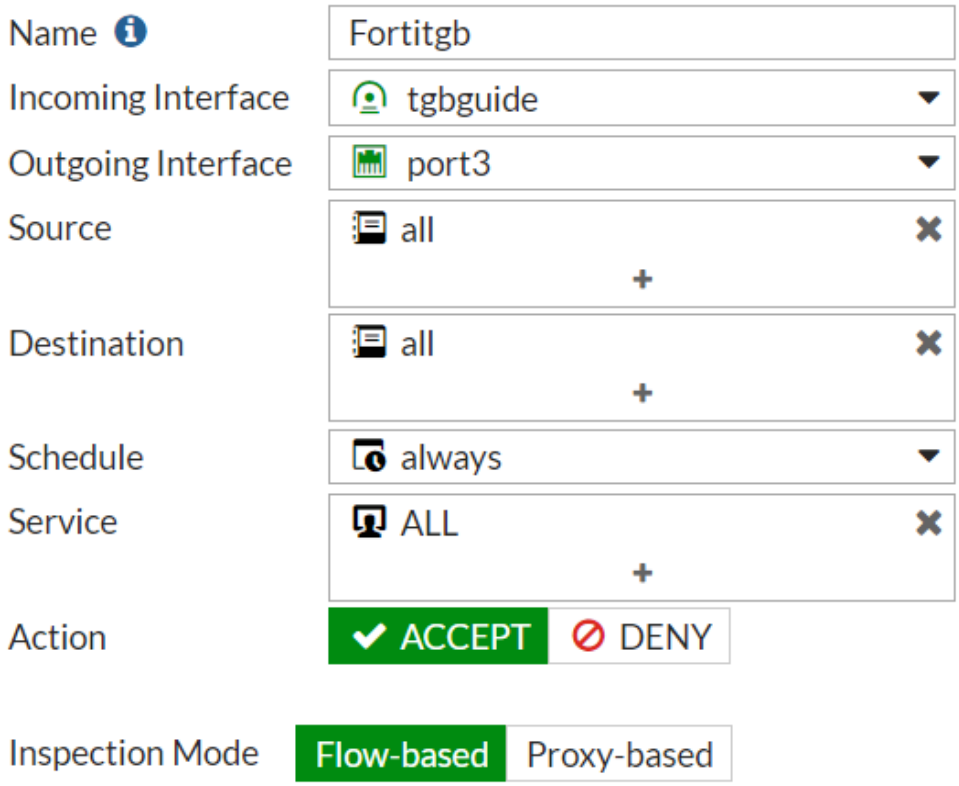
7. Fill in the **Phase 1 Proposal** section according to your needs (please refer to the technical characteristics described TheGreenBow VPN Client's documentation to find out which Diffie-Hellman groups are available for your version of the product).



8. Fill in the **Phase 2 Selectors** section as shown below.

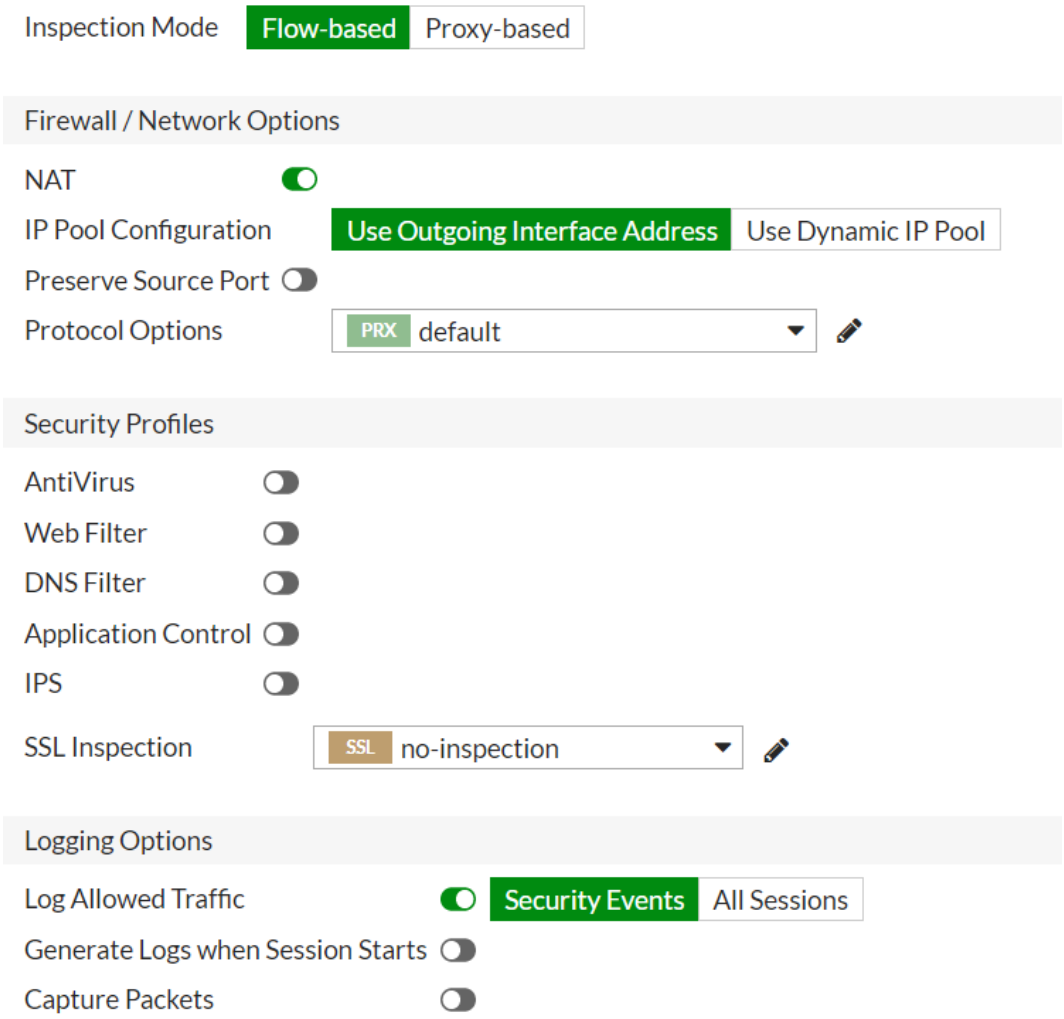


9. Select the **Policy** menu item to create a new policy according to the following screenshot:




The **Incoming Interface** should be the name of the VPN connection that you just created, and **Outgoing Interface** should be the LAN port.

10. Fill in the second half of **Configuration** window, as shown below:

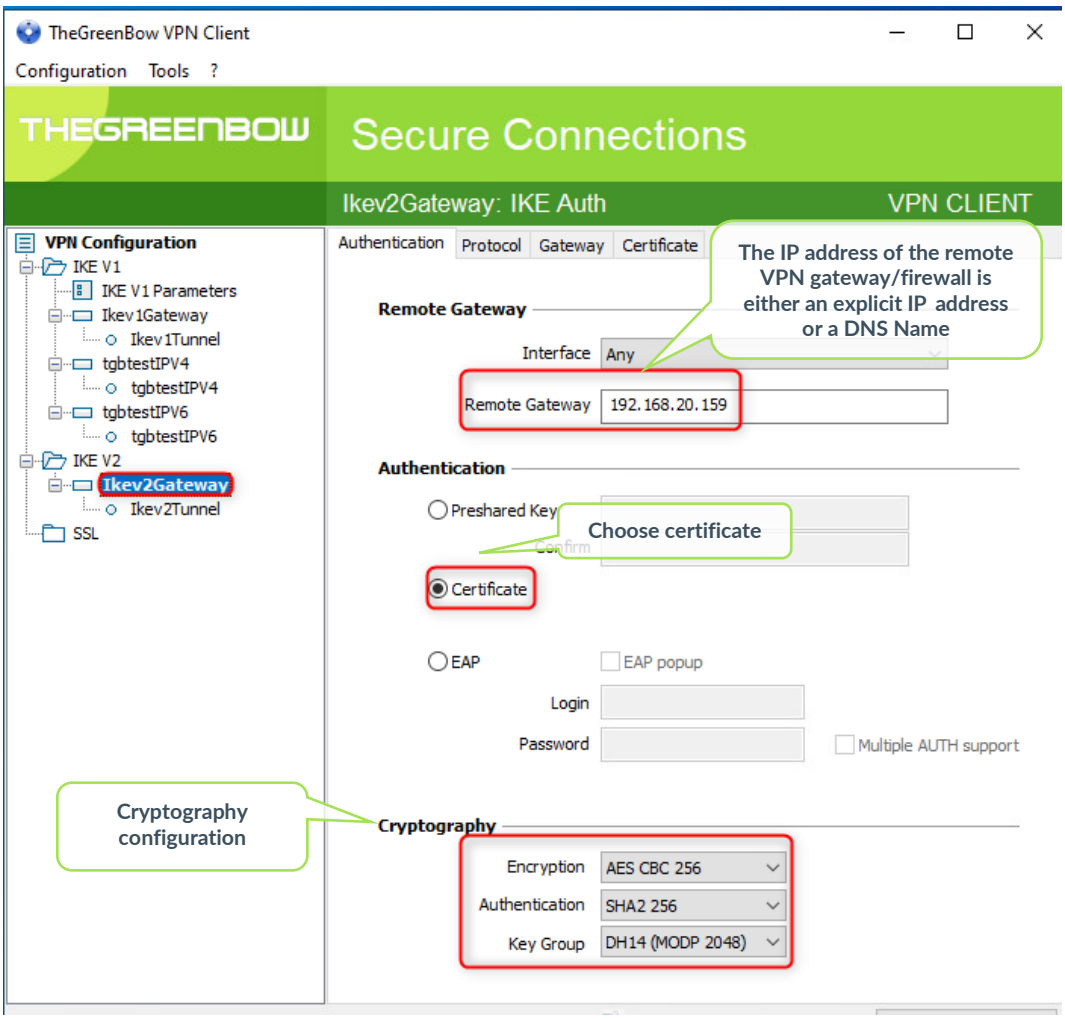


# 3 Configuring the VPN Client

This section describes the required configuration for TheGreenBow's Windows VPN Client to connect to a FortiGate Next Generation Firewall.

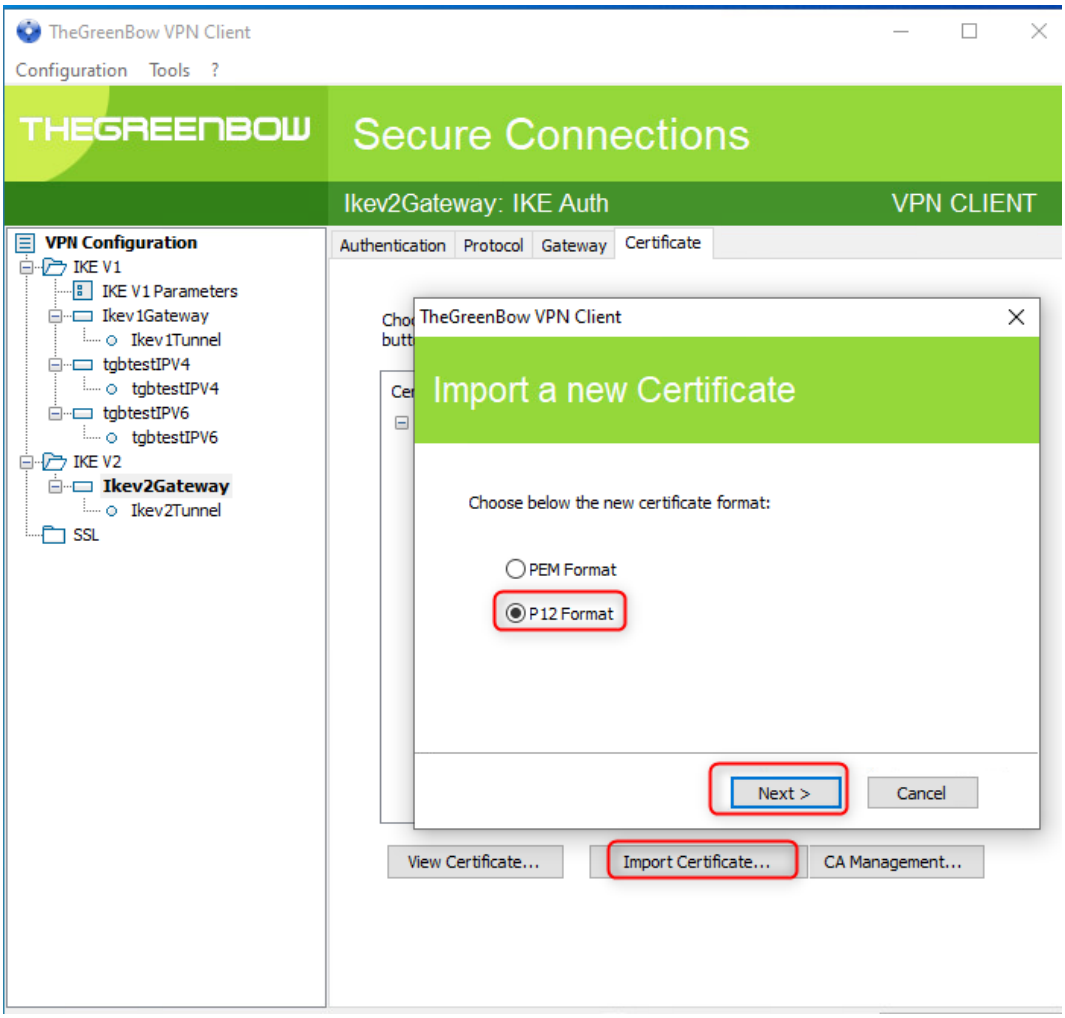
## 3.1 Configuring the VPN Client for a Phase 1 (IKE Auth)

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



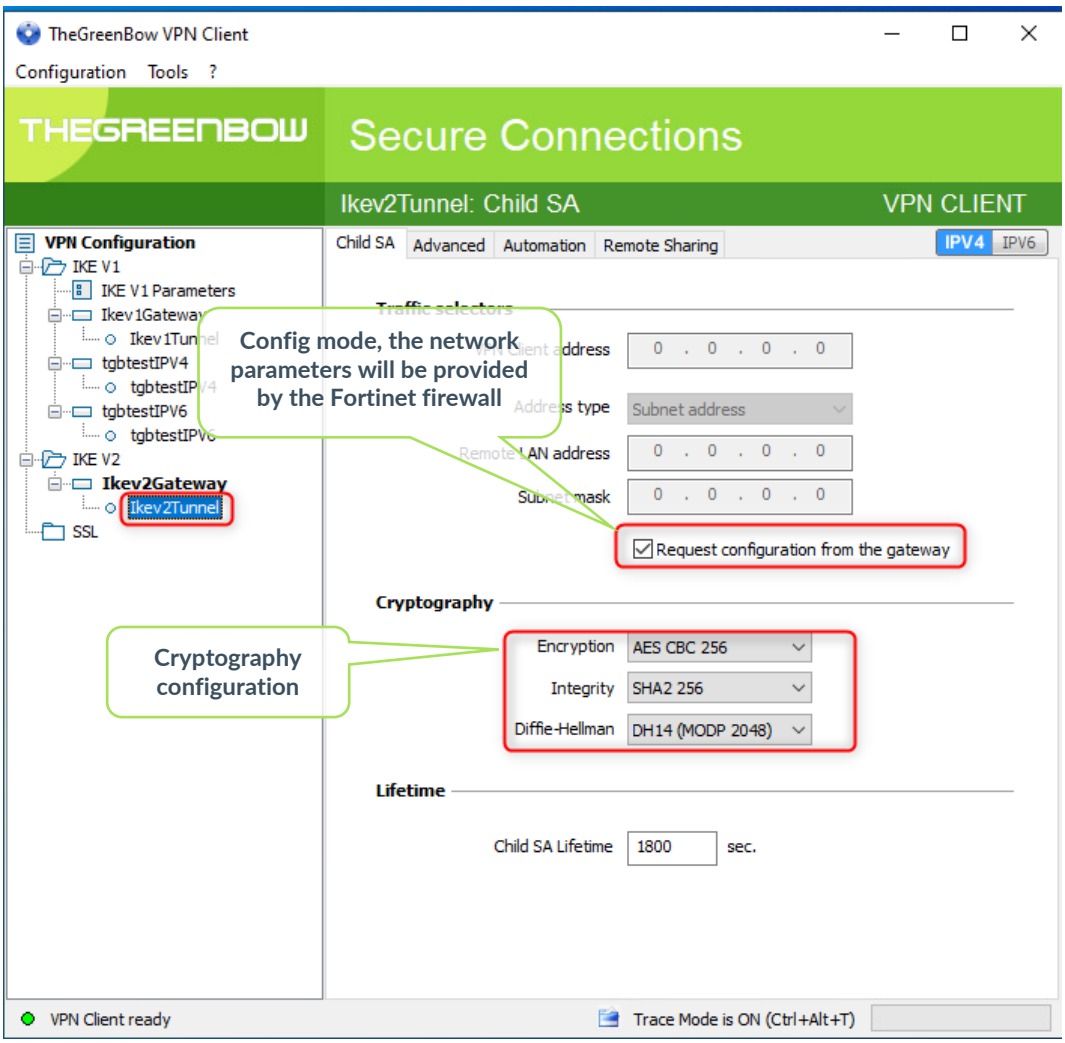

The above screenshot depicts TheGreenBow's Windows Standard VPN Client, but you may use any edition, as long as you use compliant settings.

On the **Certificate** tab, click **Import Certificate...**, choose **P12 Format**, and then click **Next >** to add a certificate.



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

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

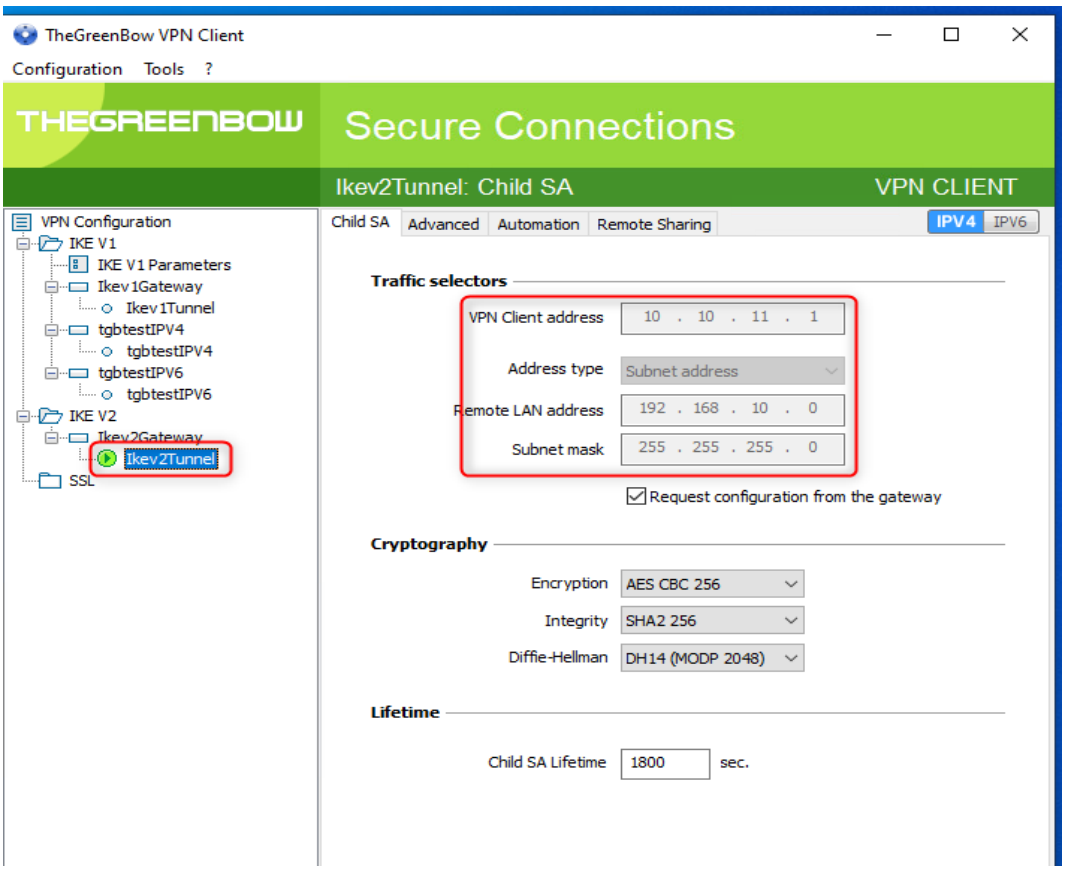



1. Click **Save & Apply** to account for all the changes you've made to your VPN Client configuration.
2. Click **Open Tunnel**.

## 3.3 Opening the VPN connection

Once both the FortiGate Next Generation Firewall and your TheGreenBow Windows 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 VPN Client and a FortiGate Next Generation Firewall:



# 4 Troubleshooting

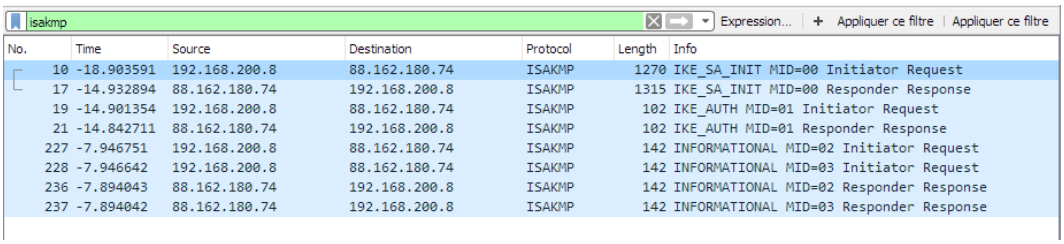
If the VPN connection cannot be established, start by checking that no parameters are missing. Also check the Console log in TheGreenBow VPN Client for any relevant information.

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:




## 4.2 Troubleshooting TheGreenBow VPN Client

### 4.2.1 “PAYLOAD_MALFORMED” error (wrong Phase 1 [SA])

If you encounter a “PAYLOAD_MALFORMED” error, you might have a wrong Phase 1 [SA]. Check whether the encryption algorithms are the same on both ends of the VPN tunnel.

```
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
```

### 4.2.2 "INVALID_COOKIE" error

If you encounter an "INVALID_COOKIE" error, this means that one of the endpoints is using an SA that is no longer in use. Reset the VPN connection at both ends.

```
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
```

### 4.2.3 "no keystate" error

Make sure the preshared key is correct or that the local ID is correct. There should be more information in the remote endpoint logs.

```
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
```

### 4.2.4 "received remote ID other than expected" error

The "Remote ID" value does not match what the remote endpoint is expecting.

```
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
```

### 4.2.5 "NO_PROPOSAL_CHOSEN" error

If you encounter a "NO_PROPOSAL_CHOSEN" error, make sure the "Phase 2" encryption algorithms are the same at both ends of the VPN connection.

```
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
```

Check “Phase 1” algorithms if you encounter the following:

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

### 4.2.6 “INVALID_ID_INFORMATION” error

If you encounter an “INVALID_ID_INFORMATION” error, check whether the “Phase 2" ID (local address and network address) is correct and matches what the remote endpoint expects.

Also check the ID type (“Subnet address” and “Single address”). If network mask is not checked, you are using an IPV4_ADDR type (and not an IPV4_SUBNET type).

```
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
```

## 4.3 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.

## 4.4 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 Phase 2 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. A firewall between the VPN Client and the remote server may block this protocol. Make sure that every device between the client and the VPN server accepts ESP.
- Check your logs on the firewall. One of its rules may drop packets.
- Check whether your ISP supports ESP.
- If you still cannot ping, follow ICMP traffic on the firewall'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 firewall's LAN. A computer on your remote LAN may receive pings but no answer, because 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

14, rue Auber
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com