# Table of Contents

1 Introduction............................................................................................................................................ 3  
1.1 Goal of this document.................................................................................................................... 3  
1.2 VPN Network topology .................................................................................................................. 3  
1.3 FortiGate Restrictions .................................................................................................................... 3  
1.4 FortiGate VPN Gateway ................................................................................................................. 3  
1.5 FortiGate VPN Gateway product info ............................................................................................ 3  
2 FortiGate VPN configuration .................................................................................................................. 4  
3 TheGreenBow IPsec VPN Client configuration ..................................................................................... 11  
3.1 VPN Client - IKE Auth Configuration ............................................................................................ 11  
3.2 VPN Client Phase 2 (Child SA) Configuration ............................................................................... 12  
3.3 Open IPsec VPN tunnels ............................................................................................................... 13  
4 Tools in case of trouble......................................................................................................................... 14  
4.1 A good network analyser: Wireshark........................................................................................... 14  
5 IPsec Troubleshooting............................................................................................................................. 15  
5.1 “NO_PROPOSAL_CHOSEN” error (wrong IKE Auth)................................................................. 15  
5.2 “AUTHENTICATION_FAILED” error ......................................................................................... 15  
5.3 “No user certificate available for the connexion” error .............................................................. 15  
5.4 “Remote IDr rejected” error ........................................................................................................ 15  
5.5 “NO_PROPOSAL_CHOSEN” error (wrong CHILD SA)........................................................... 15  
5.6 “FAILED_CP_REQUIRED” error ................................................................................................. 16  
5.7 I clicked on “Open tunnel”, but nothing happens. ...................................................................... 16  
5.8 The VPN tunnel is up but I can’t ping ! ...................................................................................... 16  
6 Contacts ................................................................................................................................................ 17
# Introduction

## 1.1 Goal of this document

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

![VPN Network Diagram](image)

## 1.3 FortiGate Restrictions

No known restrictions

## 1.4 FortiGate VPN Gateway

Our tests and VPN configuration have been conducted with FortiGate version 6.0.

## 1.5 FortiGate VPN Gateway product info

It is critical that users find all necessary information about FortiGate VPN Gateway. All product info, User Guide and knowledge base for the FortiGate VPN Gateway can be found on the FortiGate website:

- FortiGate Product page: [https://www.fortinet.com/](https://www.fortinet.com/)
- FortiGate User Guide: [https://docs.fortinet.com/fortigate/admin-guides](https://docs.fortinet.com/fortigate/admin-guides)
- FortiGate Knowledge Base: [http://kb.fortinet.com/kb/microsites/microsite.do](http://kb.fortinet.com/kb/microsites/microsite.do)
2 FortiGate VPN configuration

This section describes how to build an IPsec VPN configuration with your FortiGate VPN router. Once connected to your FortiGate VPN gateway, go to menu VPN > IPsec Tunnels. Add a tunnel.

Provide a tunnel name and select "Custom" in Template Type.

Name: tgb
Comments: Comments

Network
- IP Version: IPv4
- Remote Gateway: Dialup User
- Interface: port1
- Local Gateway: 
- Mode Config: 
- Use system DNS in mode config: 
- Assign IP From: Range
- IPv4 mode config:
  - Client Address Range: 10.10.10.1-10.10.10.20
  - Subnet Mask: 255.255.255.255
  - DNS Server: 0.0.0.0
  - Enable IPv4 Split Tunnel: 
- IPv6 mode config:
  - Client Address Range: ::::
  - Prefix Length: 128
  - DNS Server: 
  - Enable IPv6 Split Tunnel: 
- NAT Traversal: Enable
- Dead Peer Detection: Disable

Template Type: Custom
Here we selected Version 2 for IKEv2.

Note:
For IKEv1, simply select Version 1. VPN Client side, configuration needs to be created under IKEv1.
### Phase 2 Selectors

<table>
<thead>
<tr>
<th>Name</th>
<th>Local Address</th>
<th>Remote Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>tgb</td>
<td>192.168.210.0/255.255.255.0</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
</tbody>
</table>

#### Edit Phase 2

- **Name**: tgb
- **Comments**: Comments
- **Local Address**: Subnet - 192.168.210.0/255.255.255.0
- **Remote Address**: Subnet - 0.0.0.0/0.0.0.0

#### Phase 2 Proposal

- **Encryption**: 3DES
- **Authentication**: SHA1
- **Enable Replay Detection**: ✓
- **Enable Perfect Forward Secrecy (PFS)**: ✓
- **Diffie-Hellman Group**: 21, 20, 19, 18, 17, 16, 15, 14, 5, 2, 1
- **Local Port**: All
- **Remote Port**: All
- **Protocol**: All
- **Autokey Keep Alive**: ✓
- **Key Lifetime**: Seconds - 43200
- **Seconds**: 43200
Once configured above tunnel, Create a Policy.

Edit Policy

- **Name**: Incoming VPN TGB
- **Incoming Interface**: tg1
- **Outgoing Interface**: port2
- **Source**: tg1
- **Destination**: all
- **Schedule**: always
- **Service**: ALL
- **Action**: ACCEPT

Firewall / Network Options

- **NAT**: off
- **IP Pool Configuration**: Use Outgoing Interface Address, Use Dynamic IP Pool

Security Profiles

- **AntiVirus**: off
- **Web Filter**: off
- **DNS Filter**: off
- **Application Control**: off
- **IPS**: off
- **Proxy Options**: off
- **SSL Inspection**: off

Logging Options

- **Log Allowed Traffic**: Security Events, All Sessions
- **Generate Logs when Session Starts**: off
- **Capture Packets**: off
- **Comments**: Write a comment...

Enable this policy: on
Once done, Save the policy.
3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a FortiGate 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

![IKE Auth configuration]

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

This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the FortiGate router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.
3.2 VPN Client Phase 2 (Child SA) Configuration

Virtual IP address and Remote LAN address/subnet will be sent by Gateway through Mode CP.
### 3.3 Open IPsec VPN tunnels

Once both FortiGate 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 FortiGate VPN router.

```plaintext
2018-01-15 15:57:06.248 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...  
2018-01-15 15:57:06.250 Default H2K daemon is running...
```
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/).
5 VPN IPsec Troubleshooting

5.1 “NO_PROPOSAL_CHOSEN” error (wrong IKE Auth)

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20XX0913 16:08:53:387</td>
<td>TIKEV2_Tunnel SEND IKE_SA_INIT</td>
<td>[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE][VID][N(FRAGMENTATION_SUPPORTED)]</td>
</tr>
<tr>
<td>20XX0913 16:08:53:419</td>
<td>TIKEV2_Tunnel RECV IKE_SA_INIT [HDR][N(NO_PROPOSAL_CHOSEN)]</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20XX0913 16:15:22:032</td>
<td>TIKEV2_Tunnel RECV IKE_AUTH [HDR][N(AUTHENTICATION_FAILED)]</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20XX0913 16:18:07:491</td>
<td>TIKEV2_Tunnel IKE_SA_INIT</td>
<td>[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][CERTREQ][N(FRAGMENTATION_SUPPORTED)][N(MULTIPLE_AUTH_SUPPORTED)]</td>
</tr>
<tr>
<td>20XX0913 16:18:07:491</td>
<td>TIKEV2_Tunnel No user certificate available for the connexion</td>
<td></td>
</tr>
<tr>
<td>20XX0913 16:18:07:491</td>
<td>TIKEV2_Tunnel Connection aborted.</td>
<td></td>
</tr>
</tbody>
</table>

Check if the certificate is selected or the Token (smartcard) is available on the computer.

5.4 “Remote IDr rejected” error

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20180913 16:24:32:087</td>
<td>TIKEV2_Tunnel ID types do not match. Expecting ID_RPC822_ADDR. Receiving ID_DER_ASN1_DN</td>
<td></td>
</tr>
<tr>
<td>20180913 16:24:32:087</td>
<td>TIKEV2_Tunnel Remote IDr rejected</td>
<td></td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20XX0913 16:25:14:933</td>
<td>TIKEV2_Tunnel SEND IKE_SA_INIT</td>
<td>[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE][N(FRAGMENTATION_SUPPORTED)]</td>
</tr>
<tr>
<td>20XX0913 16:25:15:118</td>
<td>TIKEV2_Tunnel RECV IKE_SA_INIT</td>
<td>[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][CERTREQ][N(MULTIPLE_AUTH_SUPPORTED)]</td>
</tr>
<tr>
<td>20XX0913 16:25:15:118</td>
<td>TIKEV2_Tunnel IKE SA I-SPI 8D4467C52C91C316 R-SPI 9DF0F6E4A91F8867</td>
<td></td>
</tr>
<tr>
<td>20XX0913 16:25:15:118</td>
<td>TIKEV2_Tunnel SEND IKE_AUTH [HDR][IDI][CERT][CERTREQ][AUTH][CP][SA][TSi][TSr][N(INITIAL_CONTACT)][N(ESP_TFC_PADDING_NOT_SUPPORTED)]</td>
<td></td>
</tr>
<tr>
<td>20XX0913 16:25:15:202</td>
<td>TIKEV2_Tunnel SEND INFORMATIONAL [HDR][DELETE]</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Guide

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

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.

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