# Table of contents

1 Introduction .................................................................................................................................................... 3
1.1 Goal of this document ............................................................................................................................ 3
1.2 VPN Network topology ........................................................................................................................... 3
1.3 Billion BiGuard 10 Restrictions ............................................................................................................... 3
1.4 Billion BiGuard 10 VPN Gateway ........................................................................................................... 3
1.5 Billion BiGuard 10 VPN Gateway product info ....................................................................................... 4
2 Billion BiGuard 10 VPN configuration ............................................................................................................ 5
3 TheGreenBow IPSec VPN Client configuration ............................................................................................. 8
3.1 VPN Client Phase 1 (IKE) Configuration................................................................................................ 8
3.2 VPN Client Phase 2 (IPSec) Configuration .......................................................................................... 10
3.3 Open IPSec VPN tunnels ..................................................................................................................... 11
4 Tools in case of trouble ................................................................................................................................ 12
4.1 A good network analyser: Wireshark ............................................................................................ ....... 12
5 VPN IPSec Troubleshooting ..................................................................................................................... 13
5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) ................................................................. 13
5.2 « INVALID COOKIE » error .................................................................................................................. 13
5.3 « no keystate » error ............................................................................................................................ 13
5.4 « received remote ID other than expected » error ................................................................................ 13
5.5 « NO PROPOSAL CHOSEN » error .................................................................................................... 14
5.6 « INVALID ID INFORMATION » error .................................................................................................. 14
5.7 I clicked on “Open tunnel”, but nothing happens ................................................................................. 14
5.8 The VPN tunnel is up but I can’t ping ! ................................................................................................. 14
6 Contacts....................................................................................................................................................... 16
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Billion BiGuard 10 VPN router.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Billion BiGuard 10 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 Billion BiGuard 10 Restrictions

No known restrictions.

1.4 Billion BiGuard 10 VPN Gateway

Our tests and VPN configuration have been conducted with Billion BiGuard 10 firmware release 2.03.
1.5 Billion BiGuard 10 VPN Gateway product info

It is critical that users find all necessary information about Billion BiGuard 10 VPN Gateway. All product info, User Guide and knowledge base for the Billion BiGuard 10 VPN Gateway can be found on the Billion website: [http://www.billion.com/](http://www.billion.com/).

|-------------------------------|------------------------------------------------------|
2 Billion BiGuard 10 VPN configuration

This section describes how to build an IPSec VPN configuration with your Billion BiGuard 10 VPN router. Once connected to your Billion BiGuard 10 VPN gateway, you must select “Configuration”, “VPN”, “IPSec” and “IPSec Policy” tabs.

In this part, you click on “Create” in order to make a new IPSec Policy.
It will bring you to that page in which you will fill in all parameters:

<table>
<thead>
<tr>
<th>IPSec</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td></td>
</tr>
<tr>
<td>Connection Name</td>
<td>Gateway1</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Local</strong></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>IP Address</td>
</tr>
<tr>
<td>Network</td>
<td>Subnet</td>
</tr>
<tr>
<td><strong>Remote</strong></td>
<td></td>
</tr>
<tr>
<td>Secure Gateway</td>
<td>Dynamic IP</td>
</tr>
<tr>
<td>ID</td>
<td>IP Address</td>
</tr>
<tr>
<td>Network</td>
<td>Single Address</td>
</tr>
<tr>
<td>Proposal</td>
<td></td>
</tr>
<tr>
<td>Secure Association</td>
<td>Main Mode</td>
</tr>
<tr>
<td>Method</td>
<td>ESP</td>
</tr>
<tr>
<td>Encryption Protocol</td>
<td>AES 128</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>SHA-1</td>
</tr>
<tr>
<td>Perfect Forward Secure</td>
<td>Enabled</td>
</tr>
<tr>
<td>Key Group</td>
<td>MODP 1024 (GROUP 2)</td>
</tr>
<tr>
<td>PreShared Key</td>
<td>0123456789</td>
</tr>
<tr>
<td>IKE Life Time</td>
<td>28800 seconds</td>
</tr>
<tr>
<td>Key Life Time</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Netbios Broadcast</td>
<td>Enabled</td>
</tr>
<tr>
<td>DPD Setting</td>
<td></td>
</tr>
<tr>
<td>DPD Function</td>
<td>Enabled</td>
</tr>
<tr>
<td>Detection Interval</td>
<td>7200 seconds</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>4 consecutive times</td>
</tr>
<tr>
<td>Keep Alive Setting</td>
<td></td>
</tr>
<tr>
<td>Keep Alive Function</td>
<td>Enabled</td>
</tr>
<tr>
<td>Ping to the IP</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td><strong>VPN Client IP Address</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>172 16 10 254</td>
</tr>
<tr>
<td>Netmask</td>
<td>255 255 255 0</td>
</tr>
<tr>
<td>ID</td>
<td>10.10.10.1</td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>10 10 10 1</td>
</tr>
<tr>
<td>Netmask</td>
<td>0 0 0 0</td>
</tr>
</tbody>
</table>

The local ID (172.16.10.254) in this router corresponds to the Remote ID in the VPN Client whereas the remote ID (10.10.10.1) to the LocalID in Phase 1 Advanced in VPN Client software.

The local network corresponds to Remote LAN Address and for the remote network (10.10.10.1); it is for the VPN Client Address.

Then we selected the Aggressive Mode with an ESP method (using AES128 and SHA1), a Preshared Key (0123456789), and activated the PFS (Modp 1024).
After having configured all these parameters of the Billion BiGuard router, you click on Apply! You will see the below page:

Click “Save Config to Flash” and “Apply”.

Now you’ve completed the configuration of the Billion BiGuard 10 VPN router for TheGreenBow VPN Client software.
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Billion BiGuard 10 VPN router.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.

3.1 VPN Client Phase 1 (IKE) Configuration

So, here you find the same parameters as in the router Billion BiGuard (see page 5).

The ‘Remote Gateway’ shall match the ‘WAN address’ of the Billion BiGuard 10 VPN router.
Then click on ‘P1 Advanced’.

In this Phase 1 Advanced, select “Aggressive Mode” as we do in the Billion BiGuard router.

The “Local ID” in the VPN Client shall match the “Remote ID” and the “Remote ID”, the “Local ID” in the Billion BiGuard 10 VPN router.

Click on “Ok”.

Now you’ve completed configuration of the VPN Client Phase 1 software.
3.2 VPN Client Phase 2 (IPSec) Configuration

The part ESP shall match the Phase2 group in the Billion BiGuard 10 (in the part “Proposal”, Encryption Protocol Authentication Protocol and PFS) VPN router.

Click on “Save & Apply”.

And you have finished the configuration of the TheGreenBow VPN Client software.
3.3 Open IPSec VPN tunnels

Once both Billion BiGuard 10 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 Billion BiGuard 10 VPN router.
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 http://www.wireshark.org. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (http://www.wireshark.org/docs/).
5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

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

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

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

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
5.5 « NO PROPOSAL CHOSEN » error

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:

5.6 « INVALID ID INFORMATION » error

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 (http://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: http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com