TheGreenBow IPSec VPN Client

Configuration Guide

CNET CWR-854 firmware
v1.2.3.3

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com
## Table of contents

1 Introduction .................................................................................................................................0
   1.1 Goal of this document ...........................................................................................................0
   1.2 VPN Network topology .........................................................................................................0

2 Configuring IPSec Road Warrior connection with CNet CW-854 ................................................0

3 TheGreenBow IPSec VPN Client configuration ..........................................................................0
   3.1 VPN Client Phase 1 Configuration .......................................................................................0
   3.2 VPN Client Phase 2 Configuration .......................................................................................0

4 VPN IPSec Troubleshooting .........................................................................................................0
   4.1 « PAYLOAD MALFORMED » error ....................................................................................0
   4.2 « INVALID COOKIE » error ...............................................................................................0
   4.3 « no keystate » error ............................................................................................................0
   4.4 « received remote ID other than expected » error ...............................................................0
   4.5 « NO PROPOSAL CHOSEN » error ....................................................................................0
   4.6 « INVALID ID INFORMATION » error ................................................................................0
   4.7 I clicked on “Open tunnel”, but nothing happens ...............................................................0
   4.8 The VPN tunnel is up but I can't ping ! ..............................................................................0

5 Contacts .........................................................................................................................................0
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a CNet CWR-854 VPN gateway running firmware v1.2.3.3.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the CWR-854 gateway. 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.

A Road Warrior connection also needs to be configured. The following example makes use of these values:

- External IP of the CWR-854: mygateway.dyndns.org (or public IP address)
- IP Subnet behind the CNet CWR-854: 192.168.1.0/255.255.255.0
2 Configuring IPSec Road Warrior connection with CNet CW-854

This section describes how to build an IPSec VPN configuration with your CNet CW-854 VPN Gateway. There is no mandatory configuration, all settings may be altered to match your needs (speed vs security). Below is a screenshot of a configuration made with the values used above.

The same preshared key must be entered in TheGreenBow vpn client Phase1
**Advanced VPN Setting for IKE**

This page is used to provide advanced setting for IKE mode

<table>
<thead>
<tr>
<th><strong>Tunnel 1</strong></th>
<th><strong>Phase 1:</strong></th>
<th><strong>Phase 2:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Negotiation Mode</strong></td>
<td><strong>Main mode</strong></td>
<td><strong>Active Protocol</strong></td>
</tr>
<tr>
<td><strong>Encryption Algorithm</strong></td>
<td>AES128</td>
<td>ESP</td>
</tr>
<tr>
<td><strong>Authentication Algorithm</strong></td>
<td>SHA1</td>
<td>AES128</td>
</tr>
<tr>
<td><strong>Key Group</strong></td>
<td>DH2(modp1024)</td>
<td>SHA1</td>
</tr>
<tr>
<td><strong>Key Life Time</strong></td>
<td>3600</td>
<td>28800</td>
</tr>
</tbody>
</table>

We used “Main mode” instead of “Aggressive mode” because of the lack of security with “Aggressive” compared to “Main”.

AES algorithm is more efficient than DES or 3DES (faster to cipher data and more secured), but anything can be used.
Here is an overview of the VPN with CNet CWR-854:

**VPN Setup**

This page is used to enable/disable VPN function and select a VPN connection to edit/delete.

- **Enable IPSec VPN**
- **Enable NAT Traversal**

![Options and buttons](image)

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Active</th>
<th>Local Address</th>
<th>Remote Address</th>
<th>Remote Gateway</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>tgb</td>
<td>Y</td>
<td>192.168.1.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Connected</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Buttons](image)

Wan IP address matches Phase1 remote gateway address.
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 Configuration

Now let's add a Phase 1 to the CNET connection. Right click on Configuration in TheGreenbow VPN client and select "Add Phase 1".

Then select the "new phase 1" screen. The values that need to be changed and entered are displayed here:

The preshared key used in this example is intentionally short. Don't use this key length in a production environment, it must be complex enough for maximum security.

IP address 172.1.1.1 was used because of the test platform (Cnet + vpn client) being internal to our network, you MUST change it to match your dyndns or fixed public ip address.
ID used in this example are DNS type. These type and values must match between vpn client and router even though they are just flags that can contain anything (in the example, the values entered are NOT proper dns names, but match between client and router)
3.2 VPN Client Phase 2 Configuration

The VPN client address must not belong to the remote subnet range.

Phase2 advanced is used to enter alternate dns and/or wins servers addresses from the ones the vpn client is using prior to establish the tunnel.
4 VPN IPSec Troubleshooting

4.1 « 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.

4.2 « 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.

4.3 « 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.

4.4 « received remote ID other than expected » error

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
4.5 « 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:

4.6 « 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).

4.7 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, UDP port 4500 and protocol ESP (protocol 50).

4.8 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 Ethereal 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 ethereal (http://www.ethereal.com) on one of your target computer. You can check that your pings arrive inside the LAN.
5 Contacts

News and updates on TheGreenBow web site: http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts at +33 1 43 12 39 37 or by email at info@thegreenbow.com