
# TheGreenBow IPSec VPN Client

# Configuration Guide

# m0n0wall

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com

# Table of contents

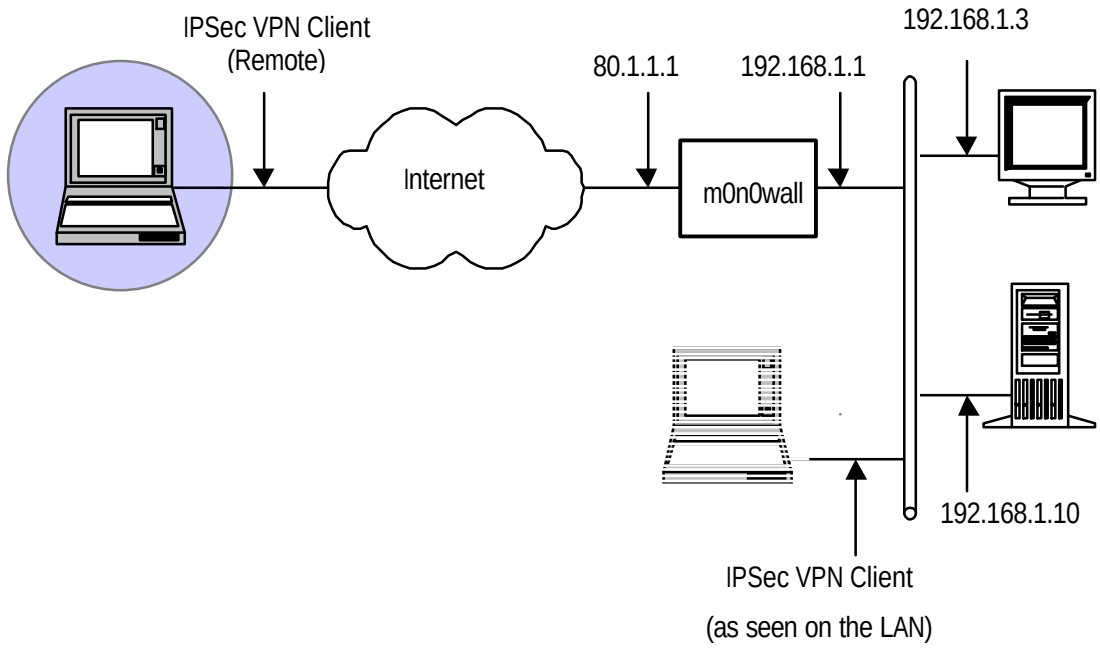
# 1 Introduction

## 1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a firewall system that runs m0n0wall software (http://m0n0.ch/wall).

## 1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the m0n0wall. 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 purposes only.




## 1.3 m0n0wall limitations

At the time of this writing, m0n0wall did not support NAT-T. However, it should still be possible to establish a VPN connection with a client behind NAT if the NAT router doesn't drop ESP packets.

## 1.4 Tested m0n0wall versions

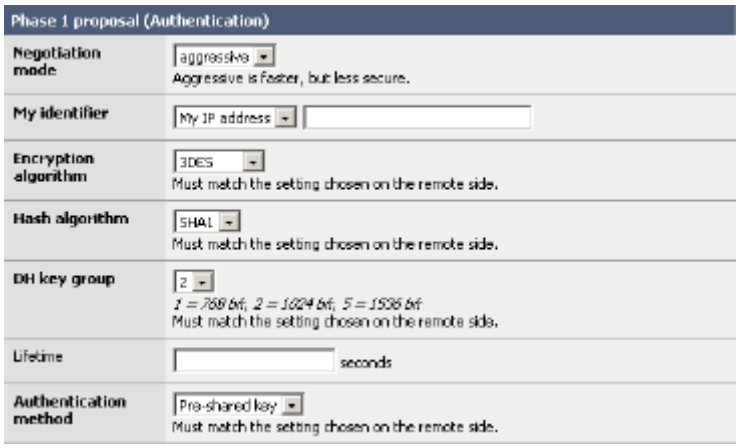
m0n0wall versions 1.11 and 1.2 were tested and confirmed to work with TheGreenBow IPSec VPN Client.

# 2 m0n0wall mobile client VPN configuration

This section describes how to configure your m0n0wall for mobile client IPsec VPN.

Connect to your m0n0wall's webGUI as usual. Log in when prompted to do so. Select **VPN** ✍ **IPsec** in the navigation bar and then click the "**Mobile clients**" tab. Click the "**Allow mobile clients**" checkbox to enable mobile client IPsec VPN.

## 2.1 Phase 1 configuration

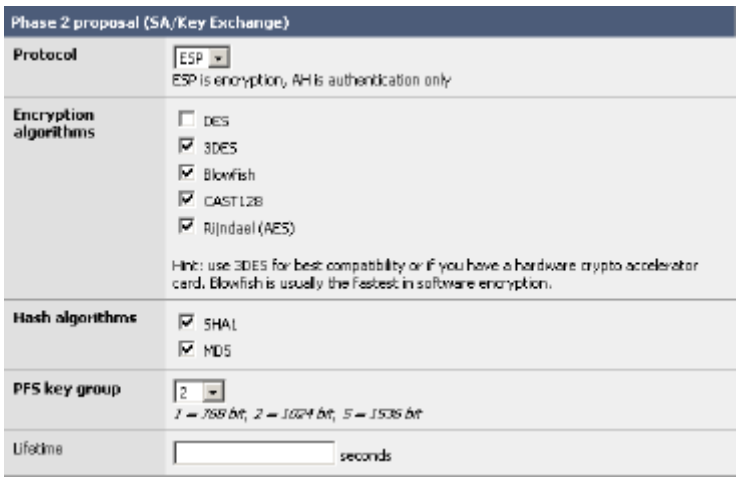



You can use either aggressive or main negotiation mode. Main mode is slower, but more secure. On the other hand, only IP addresses may be used as IDs in main mode, so if your mobile clients don't have static external IP addresses (typically they don't), you'll have to use **aggressive mode**. Leave the "My identifier" setting set to "**My IP address**".

You can use any of the available encryption or hash algorithms for phase 1; however for optimal security and interoperability it is recommended that you use **3DES** as the encryption algorithm and **SHA1** as the hash algorithm. Set the "DH key group" to **2**.

The lifetime field should be left empty. For 1.2 versions, set the authentication mode to "**Pre-shared key**" (in 1.11 this is the default and cannot be changed).

## 2.2 Phase 2 configuration

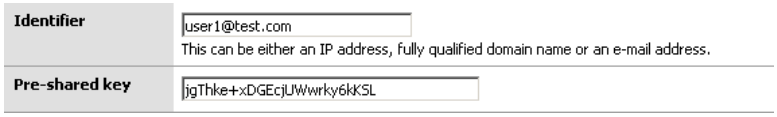



Make sure that the protocol is set to **ESP**. The default selection of accepted encryption/hash algorithms (everything except for DES) is fine. Set the "PFS key group" to **2**. As with phase 1, leave the lifetime field empty.

**Click the "Save" button to save your changes.**

## 2.3 Adding Pre-shared keys

Switch to the "**Pre-shared keys**" tab. Click the + button to add a new key.




The identifier can be either an IP address (main or aggressive mode; applies only when the client has a static external IP address), an FQDN (aggressive mode only) or an e-mail address (also referred to as User-FQDN; aggressive mode only). In this example, we'll use an e-mail address as the identifier.

Enter the user's pre-shared key in the corresponding field. For maximal security, your pre-shared key should be long (> 8 characters) and should consist of a combination of lowercase and uppercase characters and digits.

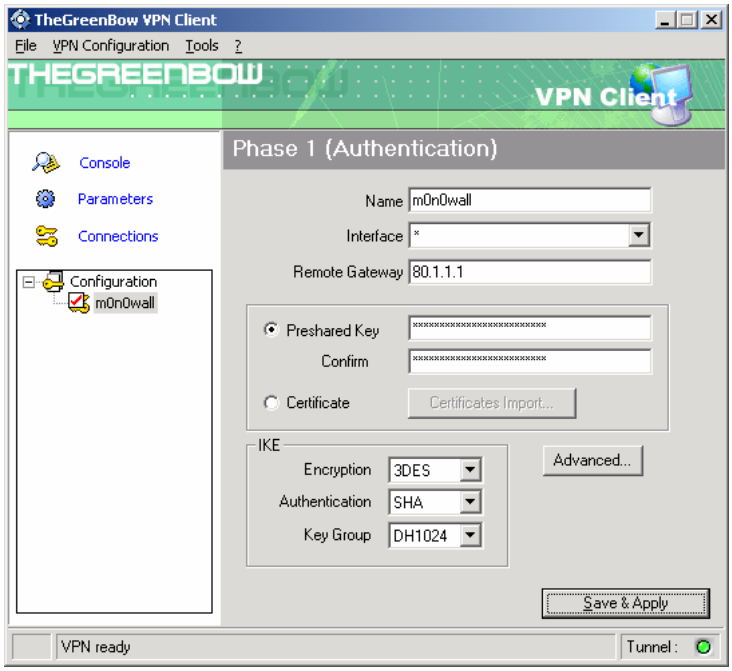
Repeat this step for any additional mobile clients that you might have.

## 2.4 Enabling IPsec VPN

Switch to the "Tunnels" tab and click "**Enable IPsec**". Then click the "Save" button below.

# 3 TheGreenBow IPSec VPN Client configuration

## 3.1 VPN Client Phase 1 (IKE) Configuration



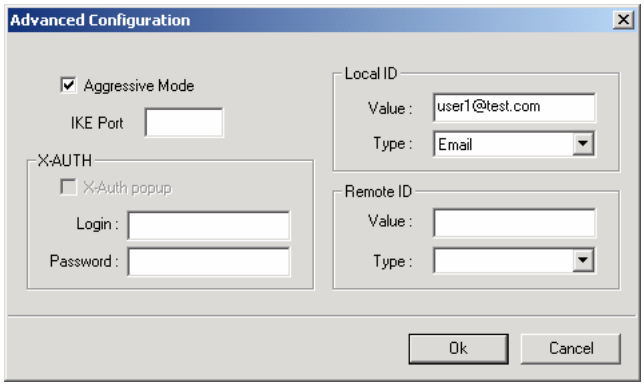

Phase 1 configuration

Open TheGreenBow VPN Client. Right-click on "Configuration" and select "**New Phase 1**". Enter any descriptive name in the "Name" field. Choose a specific interface to use if desired, or select "*" to use any available interface. Put the **remote m0n0wall's WAN IP address** into the "Remote Gateway" field.

Enter the pre-shared key for the user that you added on the "Pre-shared keys" tab of m0n0wall's VPN: IPsec configuration page. The encryption and authentication algorithms as well as the key group need to match the corresponding settings for Phase 1 on the "Mobile clients" tab of m0n0wall's VPN: IPsec configuration page. If you've followed the example, you'll need to select **3DES** as the encryption algorithm and **SHA** as the authentication algorithm. The key group "**DH1024**" corresponds to "DH 2" in m0n0wall.

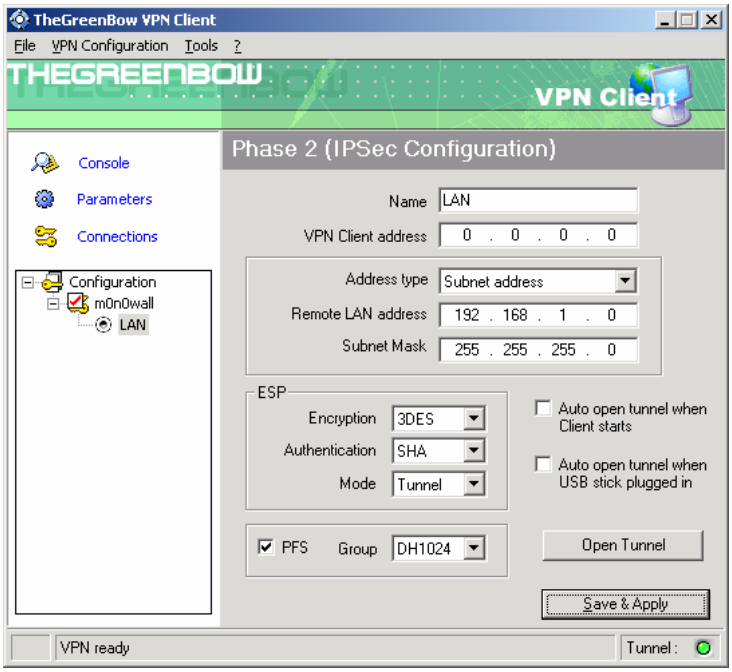
| **m0n0wall** | **TheGreenBow VPN Client** |
|---|---|
| DH 1 | DH768 |
| DH 2 | DH1024 |
| DH 5 | DH1536 |

Click the "Advanced... " button.



In the advanced configuration window that pops up, click the "**Aggressive Mode**" checkbox if you've chosen aggressive mode on m0n0wall. Enter the same value for the "**Local ID**" that you used as the identifier when you defined the pre-shared key on m0n0wall. Set the proper type as well. In our example, we'll use an E-mail address as the identifier. Leave the other fields blank.

## 3.2 VPN Client Phase 2 (IPSec) Configuration




**Phase 2 Configuration**

Right-click the phase 1 configuration that you created in the previous step and choose "Add Phase 2". Again, use any descriptive name in the "Name" field, e.g. "LAN". The VPN Client address can usually be left at "**0.0.0.0**", in which case the current IP address on the VPN client's interface will be used. In some cases, this has to be changed if multiple VPN clients use the same IP address on their Internet-connected interface. However, do not use an IP address from your m0n0wall's LAN subnet here – otherwise the VPN client will not be able to talk to other hosts on the LAN that is connected to m0n0wall.

Choose "**Subnet address**" as the address type. The remote LAN address in this example is **192.168.1.0** with a subnet mask of **255.255.255.0** (this must match the configuration of m0n0wall's LAN interface).

**3DES** as the encryption algorithm and **SHA** as the authentication algorithm is generally a good choice. For some extra security, you may also use AES128 as the encryption algorithm. Make sure **Tunnel mode** is selected.

The PFS setting must match the setting on m0n0wall. In our example, **PFS is turned on** and group 2 (= **DH1024**) is used.

When you've finished entering the settings, click "**Save & Apply**".

## 3.3 Open IPSec VPN tunnels

Once both your m0n0wall and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels.

1. Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)
2. Select "**Connections**" to see open VPN Tunnels

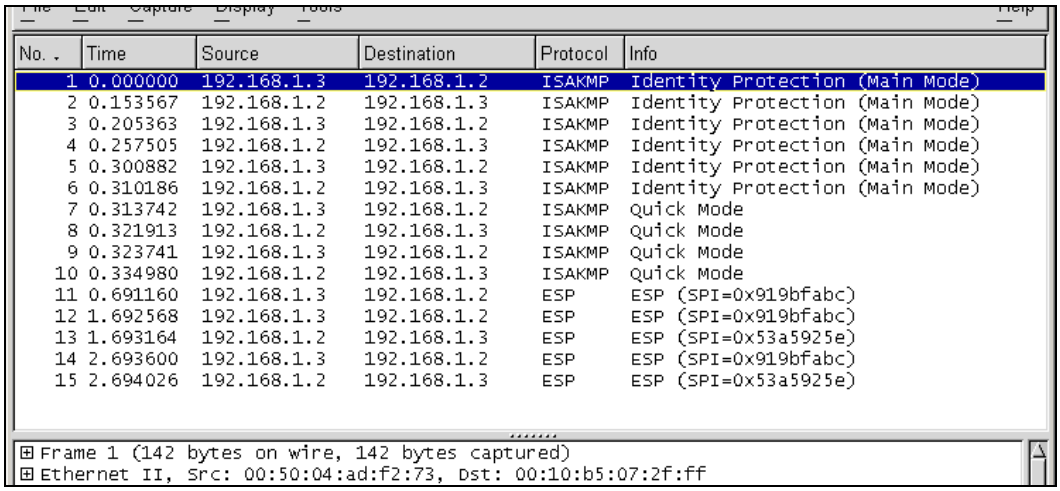
3. Select "**Console**" if you want to access the IPSec VPN logs and adjust filters to display fewer IPSec messages.

# 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: ethereal

Ethereal 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 from http://www.ethereal.com/. It can be used to follow protocol exchanges between two devices. For installation and use details, read its specific documentation.



# 5 VPN IPSec Troubleshooting

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

```
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 Informat ional  [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have a «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

```
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
```

If you have an «INVALID COOKIE» error, it means that one endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

## 5.3 «no keystate» error

```
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 key  state in ISAKMP SA 00B57C50
```

Check if the pre-shared key is correct or if the local ID is correct (see «Advanced» button). You should have more information in the remote endpoint's logs.

## 5.4 «received remote ID other than expected» error

```
120348 Default (SA CNX VPN1-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 Defau lt (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
```

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

## 5.5 «NO PROPOSAL CHOSEN» error

```
115911 Default (SA CNXVPN1 -P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1 -P1) RECV ph ase 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
```

If you have a «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:

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

## 5.6 «INVALID ID INFORMATION» error

```
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 (S A 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: 195.1  00.205.112, 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_INFOR   MATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1 -P1 deleted
```

If you have an «INVALID ID INFORMATION» error, check if the «Phase 2» ID (local address and network address) is correct and matches what is expected by the remote endpoint.

Check the ID type ("Subnet address" and "Single address") as well. If "network mask" is not checked, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

## 5.7 I clicked on "Open tunnel", but nothing happened.

Read the 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, the VPN Client's IP address should not belong to the remote LAN subnet
- Once the VPN tunnel is up, packets are sent with the ESP protocol. This protocol can be blocked by firewalls. Check that every device between the client and the VPN server accepts ESP.
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Make sure that your ISP supports ESP.

- If you still cannot ping, follow ICMP traffic on the VPN server's LAN interface and on a LAN computer's interface (with Ethereal for example). You will have an indication that encryption works.
- Check the "default gateway" value on LAN hosts. A target on your remote LAN can receive pings but does not answer if there is a no "Default gateway" setting.
- You cannot access 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 computers. 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 at +33 1 43 12 39 37 or by email at info@thegreenbow.com