TheGreenBow IPSec VPN Client

Configuration Guide

Syswan DuoLinks SW24 VPN

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

Table of contents

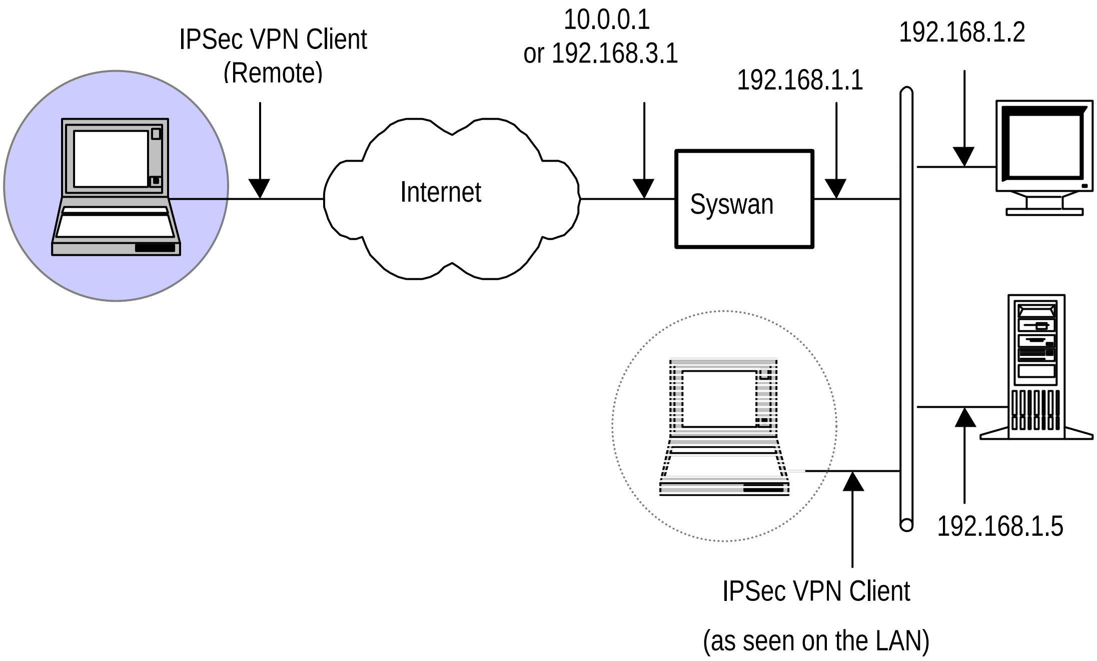
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Syswan DuoLinks SW24 VPN router with redundant gateway capability.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Syswan SW24 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 and might not reflect reality.



1.3 Syswan DuoLinks SW24 VPN Restrictions

There is no Syswan Restrictions

1.4 Syswan DuoLinks SW24 VPN Gateway

Our tests and VPN Configuration have been conducted with Syswan DuoLinks SW24 VPN firmware release version 3.0.

1.5 Syswan DuoLinks SW24 VPN Gateway product info

It is critical that users find all necessary information about Syswan VPN Gateway. All product info, User Guide and knowledge base for the Syswan DuoLinks SW24 VPN Gateway can be found on the Syswan website: www.syswan.com

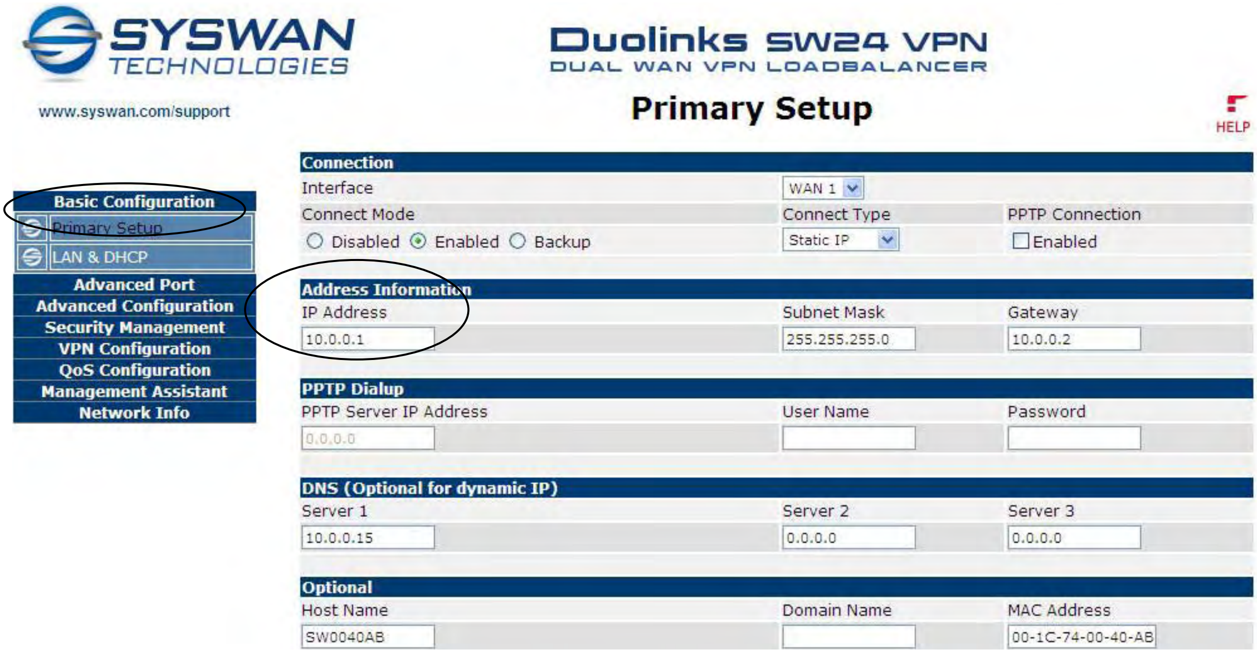
- Syswan DuoLinks SW24 VPN Product page: http://www.syswan.com/SW24VPN_Overview.htm
- Syswan DuoLinks SW24 VPN User Guide: http://www.syswan.com/InstallGuide.htm
- Syswan DuoLinks SW24 VPN FAQ/Knowledge Base: http://www.syswan.com/Knowledgebase.htm

2 Setting up Road Warrior VPN Connection

This section describes how to configure IPSec VPN access on a Syswan DuoLinks SW24 VPN gateway with a Redundant Gateway.

2.1 Syswan SW24 Basic Configuration

First step would be to login and go to 'Primary Setup' under 'Basic Configuration' menu to configure your WANs IP address in 'Address Information' section. Then click 'Update'. So here, it is for the WAN 1:



Primary Setup

Connection

Interface	WAN 1	
Connect Mode	Connect Type	PPTP Connection
○ Disabled ● Enabled ○ Backup	Static IP	□ Enabled

Address Information

IP Address	Subnet Mask	Gateway
10.0.0.1	255.255.255.0	10.0.0.2

PPTP Dialup

PPTP Server IP Address	User Name	Password
0.0.0.0		

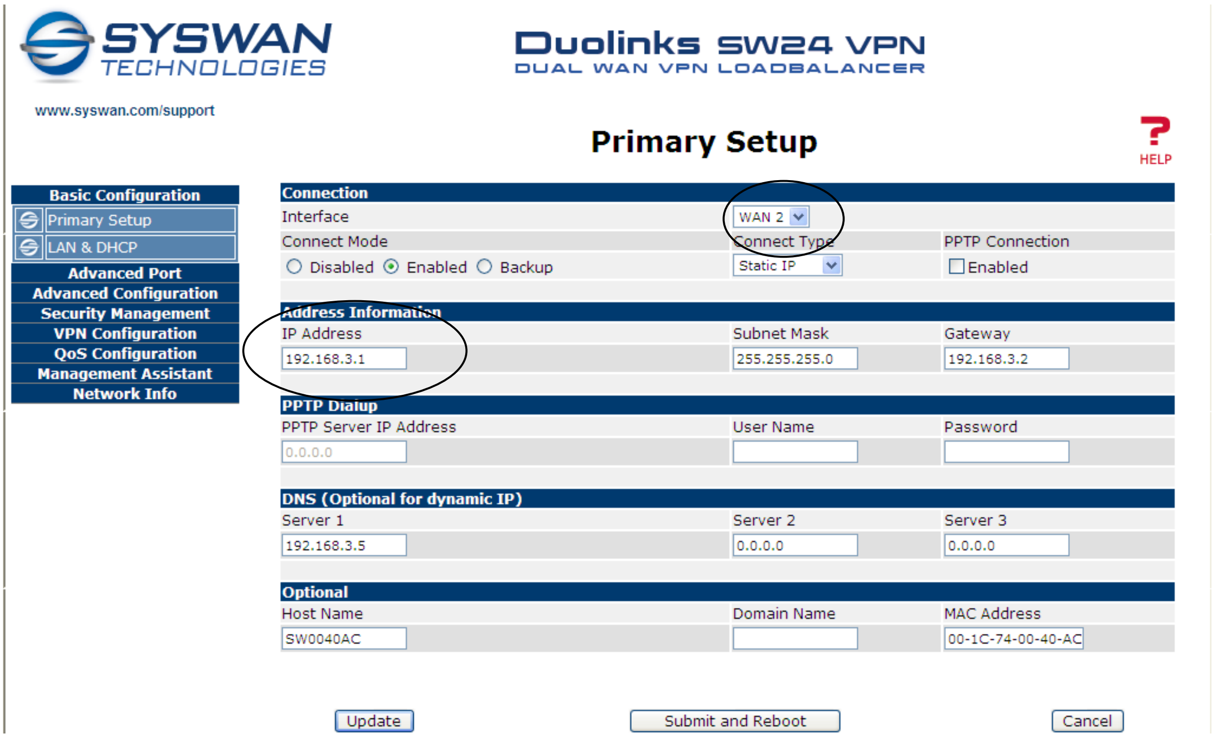
DNS (Optional for dynamic IP)

Server 1	Server 2	Server 3
10.0.0.15	0.0.0.0	0.0.0.0

Optional

Host Name	Domain Name	MAC Address
SW0040AB		00-1C-74-00-40-AB

Then, create a redundant WAN access called WAN2:



Primary Setup

Connection

Interface	WAN 2	
Connect Mode	Connect Type	PPTP Connection
○ Disabled ● Enabled ○ Backup	Static IP	□ Enabled

Address Information

IP Address	Subnet Mask	Gateway
192.168.3.1	255.255.255.0	192.168.3.2

PPTP Dialup

PPTP Server IP Address	User Name	Password
0.0.0.0		

DNS (Optional for dynamic IP)

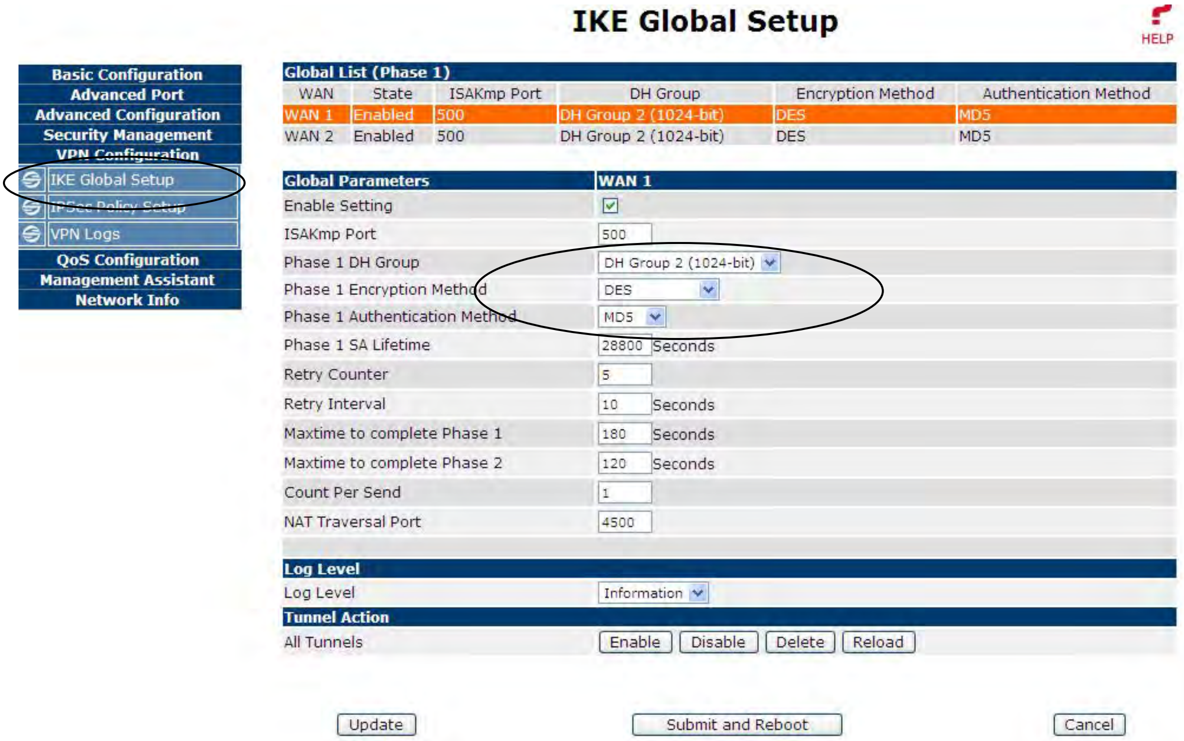
Server 1	Server 2	Server 3
192.168.3.5	0.0.0.0	0.0.0.0

Optional

Host Name	Domain Name	MAC Address
SW0040AC		00-1C-74-00-40-AC

2.2 Syswan SW24 IKE Global Setup

Then, go to 'IKE Global Setup' under 'VPN Configuration' menu.



IKE Global Setup

Global List (Phase 1)

WAN	State	ISAKmp Port	DH Group	Encryption Method	Authentication Method
WAN 1	Enabled	500	DH Group 2 (1024-bit)	DES	MD5
WAN 2	Enabled	500	DH Group 2 (1024-bit)	DES	MD5

Global Parameters	WAN 1
Enable Setting	☑
ISAKmp Port	500
Phase 1 DH Group	DH Group 2 (1024-bit)
Phase 1 Encryption Method	DES
Phase 1 Authentication Method	MD5
Phase 1 SA Lifetime	28800 Seconds
Retry Counter	5
Retry Interval	10 Seconds
Maxtime to complete Phase 1	180 Seconds
Maxtime to complete Phase 2	120 Seconds
Count Per Send	1
NAT Traversal Port	4500

Log Level	
Log Level	Information

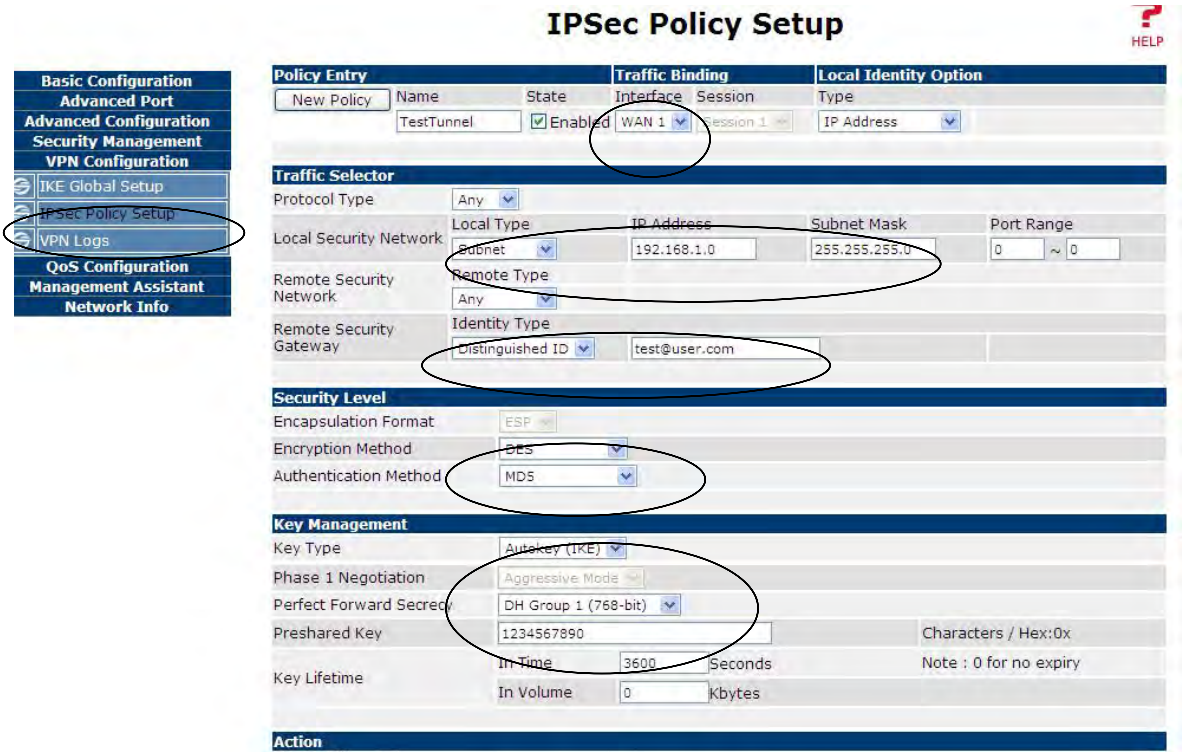
Tunnel Action	
All Tunnels	Enable Disable Delete Reload

All Phase1 parameters (DH Group, Encryption Method and Authentication Method) must be configured. Pick the encryption and authentication method that fit your need. Remember those settings because they must match those parameters in Phase 1 under IKE in TheGreenBow IPSec VPN Client software.

Click on 'Update'.

2.3 Syswan SW24 IPSec Policy Setup

Then, go to 'IPSec Policy Setup' under 'VPN Configuration' menu. You will have to create another configuration with the same parameters for the second WAN.



IPSec Policy Setup

Policy Entry — Name: TestTunnel — State: ☑ Enabled

Traffic Binding — Interface: WAN 1 — Session: Session 1

Local Identity Option — Type: IP Address

Traffic Selector

Protocol Type: Any

Local Security Network — Local Type: Subnet — IP Address: 192.168.1.0 — Subnet Mask: 255.255.255.0 — Port Range: 0 ~ 0

Remote Security Network — Remote Type: Any

Remote Security Gateway — Identity Type: Distinguished ID — test@user.com

Security Level

Encapsulation Format: ESP

Encryption Method: DES

Authentication Method: MD5

Key Management

Key Type: Autokey (IKE)

Phase 1 Negotiation: Aggressive Mode

Perfect Forward Secrecy: DH Group 1 (768-bit)

Preshared Key: 1234567890 — Characters / Hex:0x

Key Lifetime — In Time: 3600 Seconds — Note : 0 for no expiry — In Volume: 0 Kbytes

Action

In ‘Traffic Selector’ and ‘Local Security Network’ sections, you need to enter the LAN IP address and Mask.

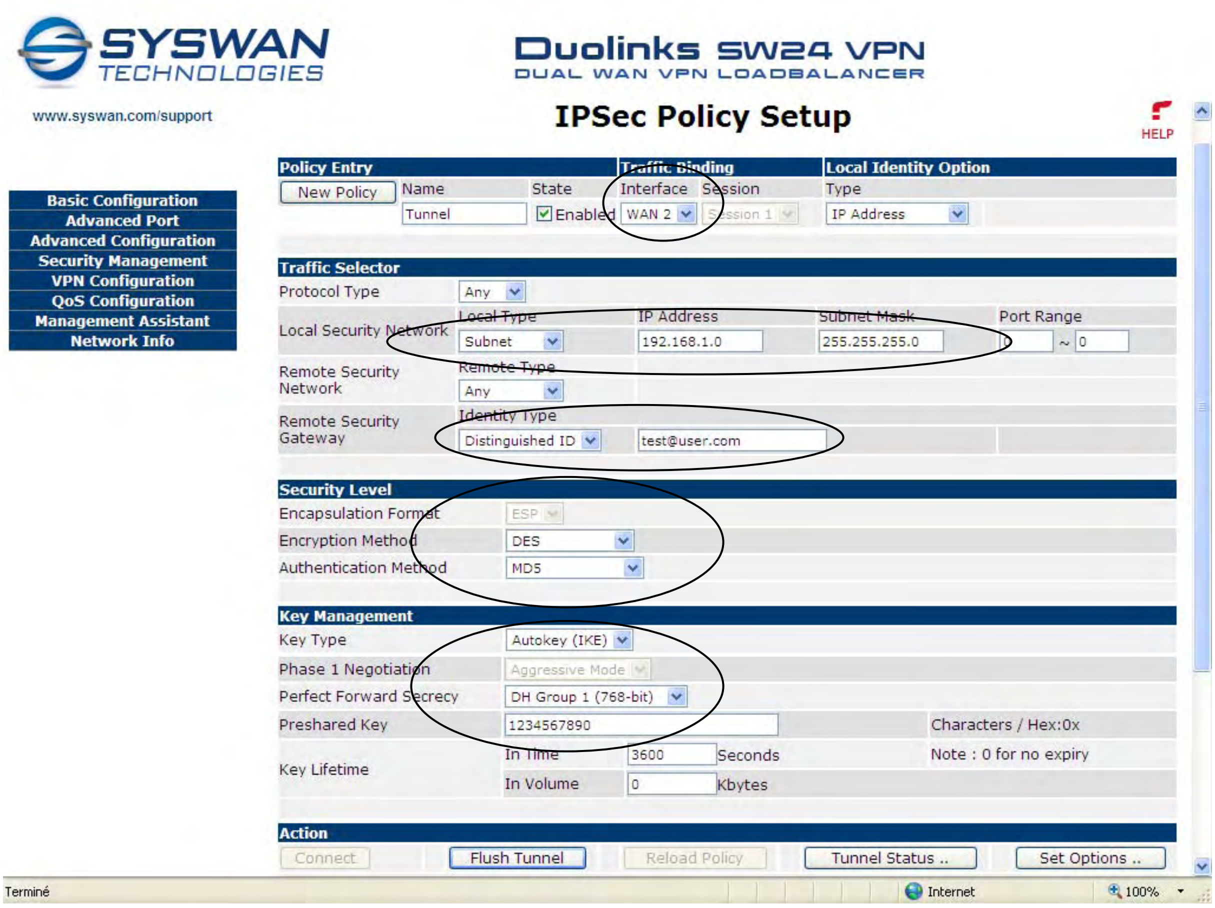
In ‘Traffic Selector’ and ‘Remote Security Gateway’ section, you need to enter the Local ID with email type such as “test@user.com”. The exact same Local ID will be required in ‘Phase 1 Advanced’ Panel in TheGreenBow IPSec VPN Client software.

In ‘Security Level’ section, select the Phase 2 encryption and authentication method that will be required in ‘Phase 2’ Panel under ESP section in TheGreenBow IPSec VPN Client.

Finally, in ‘Key Management’ section, remember that ‘Aggressive Mode’ and DH algorithm Group 1 (DH1024) are selected and the Preshared Key you set up as those settings will be required in TheGreenBow IPSec VPN Client.

Click ‘Submit and Reboot’, you’ve completed the Syswan DuoLinks SW24 VPN gateway configuration for IPSec VPN.

Then do the same things with the WAN 2:



IPSec Policy Setup

Policy Entry

Name: Tunnel
State: ☑ Enabled

Traffic Binding

Interface: WAN 2
Session: Session 1

Local Identity Option

Type: IP Address

Traffic Selector

Protocol Type: Any
Local Security Network: Local Type: Subnet; IP Address: 192.168.1.0; Subnet Mask: 255.255.255.0; Port Range: 0 ~ 0
Remote Security Network: Remote Type: Any
Remote Security Gateway: Identity Type: Distinguished ID; test@user.com

Security Level

Encapsulation Format: ESP
Encryption Method: DES
Authentication Method: MD5

Key Management

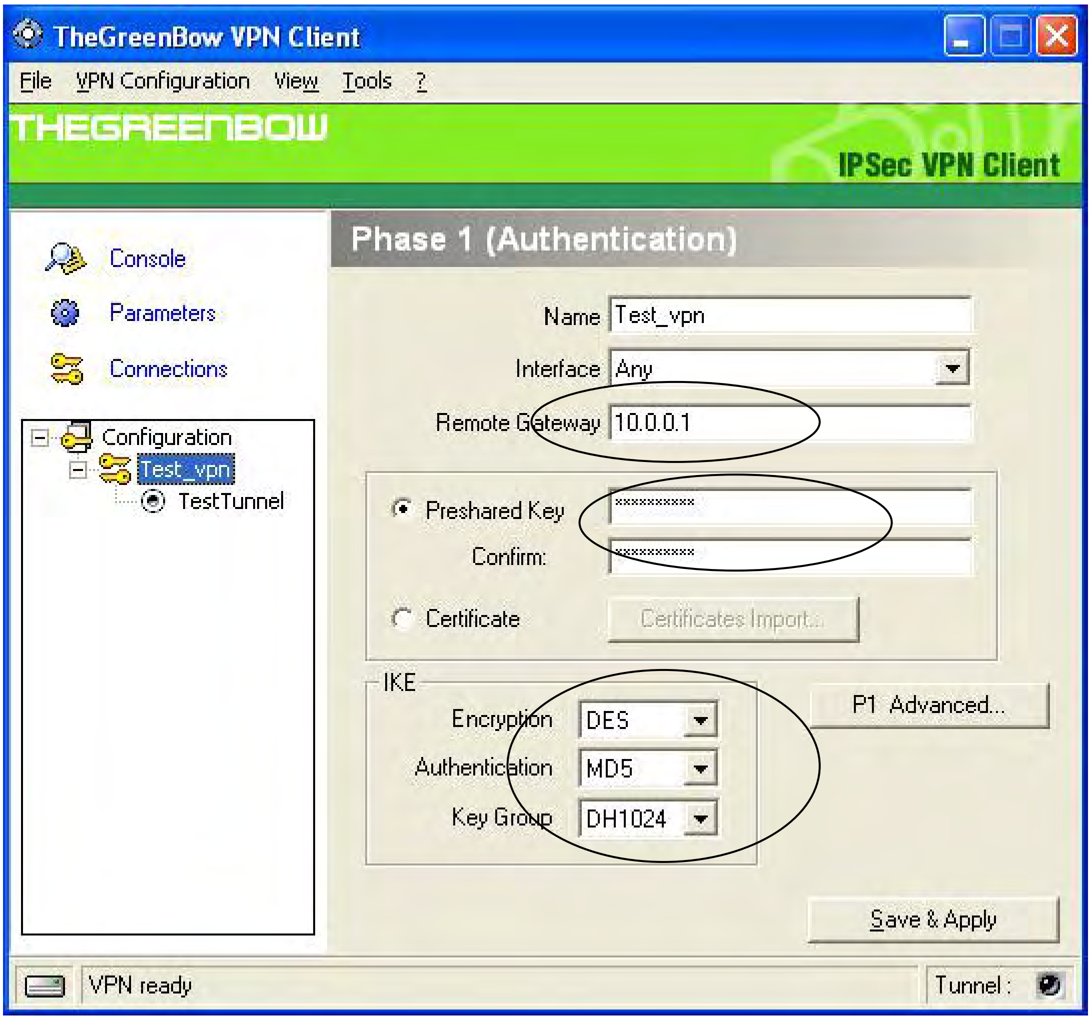
Key Type: Autokey (IKE)
Phase 1 Negotiation: Aggressive Mode
Perfect Forward Secrecy: DH Group 1 (768-bit)
Preshared Key: 1234567890 Characters / Hex:0x
Key Lifetime: In Time 3600 Seconds Note : 0 for no expiry
In Volume 0 Kbytes

Action

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

Right click on Configuration in TheGreenBow IPSec VPN Client software and select "Add Phase 1".



Phase 1 (Authentication)

Name: Test_vpn

Interface: Any

Remote Gateway: 10.0.0.1

● Preshared Key: ***********

Confirm: ***********

○ Certificate

IKE

Encryption: DES

Authentication: MD5

Key Group: DH1024

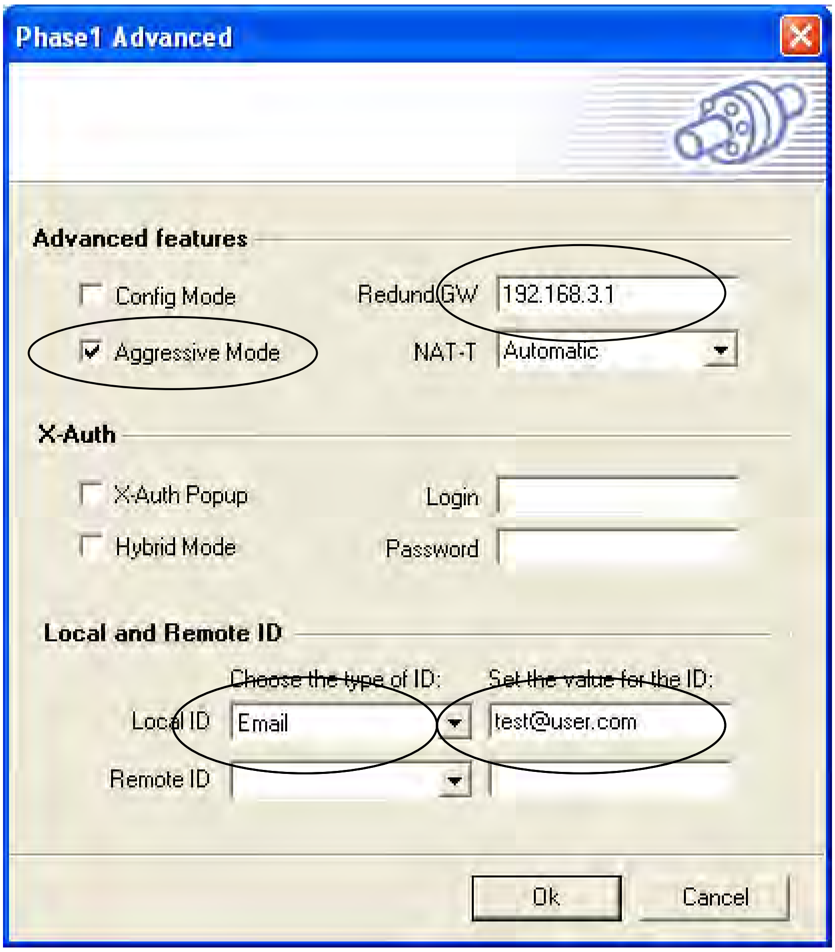
VPN ready

Tunnel :

Make sure you enter the right Preshared Key as setup in the Syswan's configuration as well as IKE algorithms.

We put in the Remote Gateway, the Wan 1 therefore in the Phase 1 advanced you will put in the redundant gateway the address of the Wan 2 which is 192.168.3.1

Then, go to 'P1 Advanced'.



☐ Config Mode

☑ Aggressive Mode

Redund.GW 192.168.3.1

NAT-T Automatic

X-Auth

☐ X-Auth Popup

☐ Hybrid Mode

Login

Password

Local and Remote ID

Choose the type of ID: Set the value for the ID:

Local ID Email test@user.com

Remote ID

Don’t forget to select “Aggressive Mode”. And as we said before, we put the address of the WAN 2 in the redundant gateway field.

Local ID Type must be defined as ‘Email’ according to the Local ID Type defined in the Syswan router.

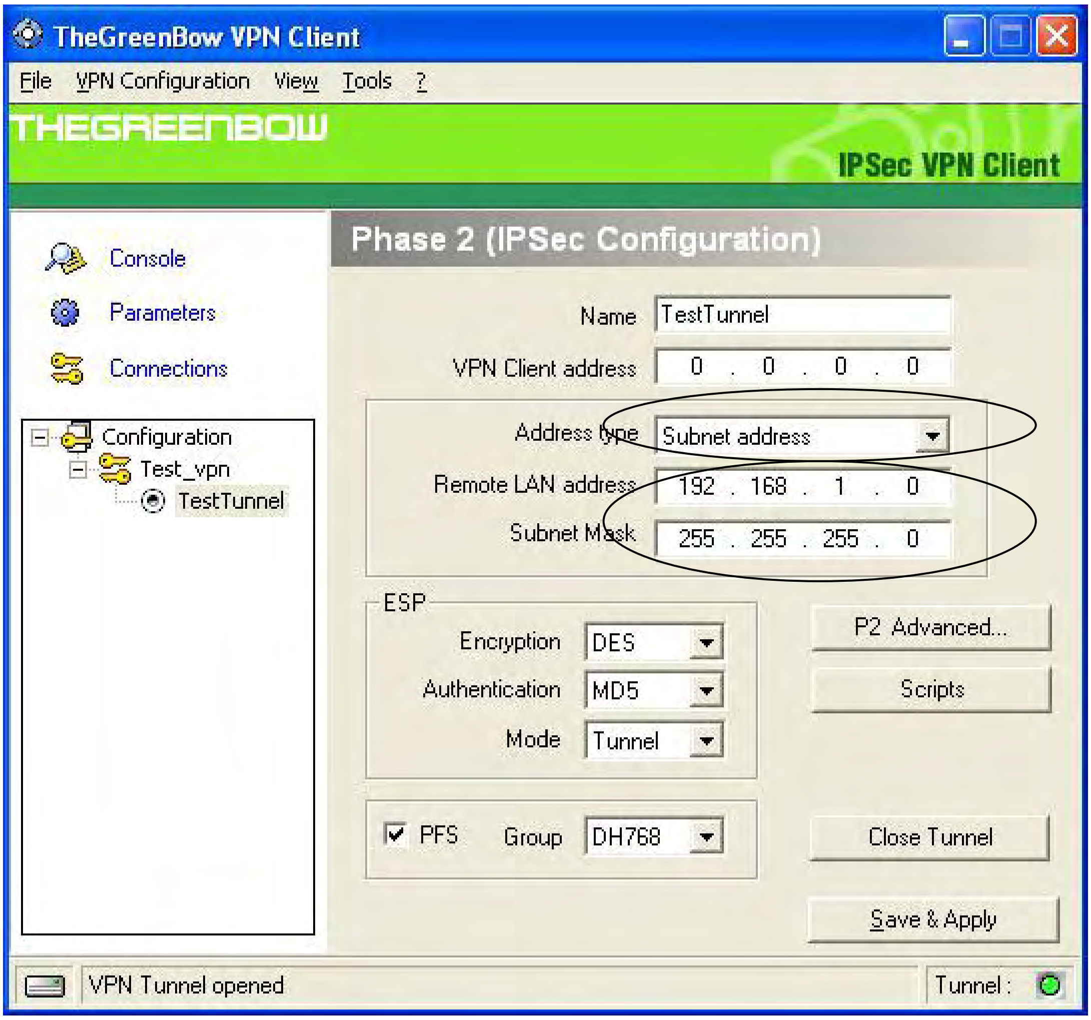
Also enter the Email address for the Local ID Value. In our example, enter “test@user.com”.

Nothing is required in Remote ID type or Value.

Click ‘ok’.

3.2 VPN Client Phase 2 (IPSec) Configuration

Create a Phase 2 by right-clicking on Phase 1.



Phase 2 (IPSec Configuration)

Name: TestTunnel

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: DES

Authentication: MD5

Mode: Tunnel

☑ PFS Group: DH768

VPN Tunnel opened

Tunnel : ●

Modify Address type by choosing subnet address, and add the remote LAN address and mask (must match what was defined on the Syswan router)

Algorithms, PFS and DH Group must match Syswan settings in advanced screen in section 2.1 of this document.

The ‘VPN Client address’ must not belong to the remote subnet range. In our example, we chose 0.0.0.0 meaning the ‘VPN Client address’ is the physical address of the machine dynamically assigned by ISP (e.g. hotel,..).
If the remote worker tries to connect from a LAN where the IP address is 192.168.1.1, the VPN connection won’t establish correctly. In this case, you must specify an IP address in another range (e.g. 10.0.0.1 or 192.168.0.1 or whatever private IP address you wish).

‘Phase2 Advanced’ is used to enter alternate DNS and/or WINS server addresses from the ones the VPN Client software is using prior to establishing the tunnel.

Click on ‘Save & Apply’, go to ‘File’ menu and ‘Export VPN Configuration’ to get the VPN configuration file that you can send to end users. For more about IPSec VPN deployment please refer to our VPN Deployment Guide on our website: www.thegreenbow.com/vpn_doc.html.

3.3 Open IPSec VPN tunnels

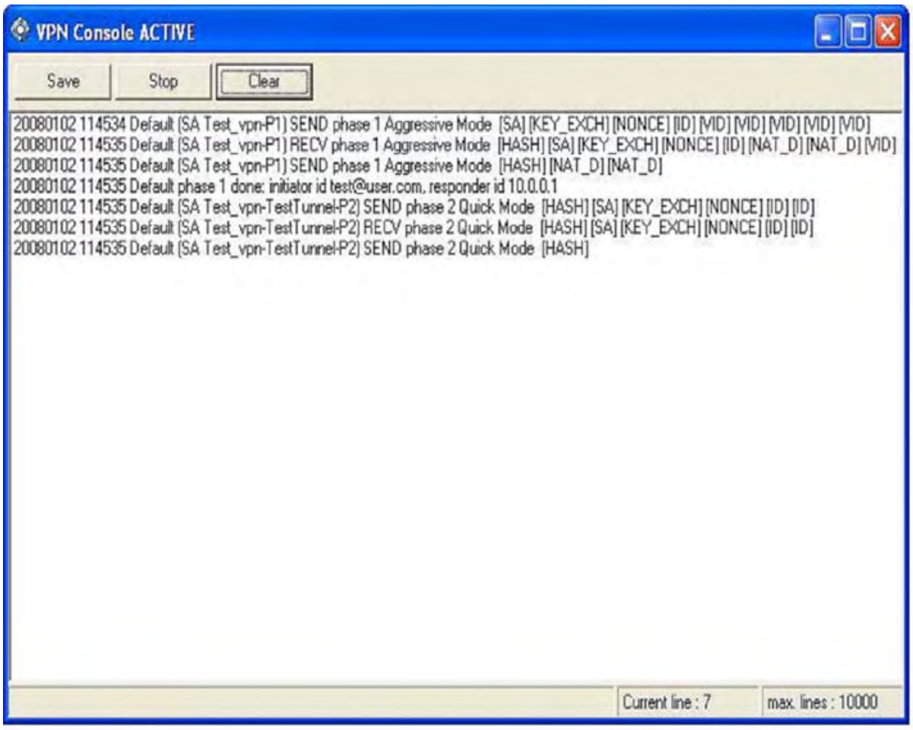
Once both Syswan DuoLinks SW24 VPN router and TheGreenBow IPSec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

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 software and a Syswan DuoLinks SW24 VPN router.



```
20080102 114534 Default (SA Test_vpn-P1) SEND phase 1 Aggressive Mode  [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID]
20080102 114535 Default (SA Test_vpn-P1) RECV phase 1 Aggressive Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID]
20080102 114535 Default (SA Test_vpn-P1) SEND phase 1 Aggressive Mode  [HASH] [NAT_D] [NAT_D]
20080102 114535 Default phase 1 done: initiator id test@user.com, responder id 10.0.0.1
20080102 114535 Default (SA Test_vpn-TestTunnel-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080102 114535 Default (SA Test_vpn-TestTunnel-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080102 114535 Default (SA Test_vpn-TestTunnel-P2) SEND phase 2 Quick Mode  [HASH]
```

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])

```
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
```

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

```
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 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

```
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
```

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

```
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
```

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

5.5 « NO PROPOSAL CHOSEN » error

```
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
```

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:

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

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 website: http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com