




THEGREENBOW

 **Cliente VPN IPSec TheGreenBow**

Guia de Configuração

Router VPN DrayTek

WebSite: <http://www.thegreenbow.com>

Contact: support@thegreenbow.com

Lista de Conteúdos

1	Introdução	3
1.1	Objectivo deste documento	3
1.2	Topologia de Rede VPN	3
1.3	Informação extra sobre o Router VPN DrayTek	3
2	Configuração em IPSec Main Mode	4
2.1	Configuração de Router VPN da DrayTek	4
2.2	Configuração de Cliente VPN IPSec TheGreenBow	6
2.2.1	Configuração de <i>Phase 1 (IKE)</i>	6
2.2.2	Configuração de <i>Phase 2 (IPSec)</i>	7
2.2.3	Estabelecer Túnel VPN em IPSec	8
3	Configuração em IPSec Aggressive Mode	9
3.1	Configuração de Router VPN da DrayTek	9
3.2	Configuração de Cliente VPN IPSec TheGreenBow	11
3.2.1	Configuração de <i>Phase 1 (IKE)</i>	11
3.2.2	Configuração de <i>Phase 2 (IPSec)</i>	13
3.2.3	Estabelecer Túnel VPN em IPSec	14
4	Problemas de Ligação VPN IPSec.....	15
4.1	Erro : « PAYLOAD MALFORMED » (Phase 1 [SA] errada)	15
4.2	Erro : « INVALID COOKIE »	15
4.3	Erro : « no keystate »	15
4.4	Erro : « received remote ID other than expected »	15
4.5	Erro : « NO PROPOSAL CHOSEN »	16
4.6	Erro : « INVALID ID INFORMATION ».....	16
4.7	Cliquei em "Estabelecer Túnel", mas não aconteceu nada.....	16
4.8	O túnel está estabelecido mas não consigo fazer pings!	17
5	Contactos	18

1 Introdução

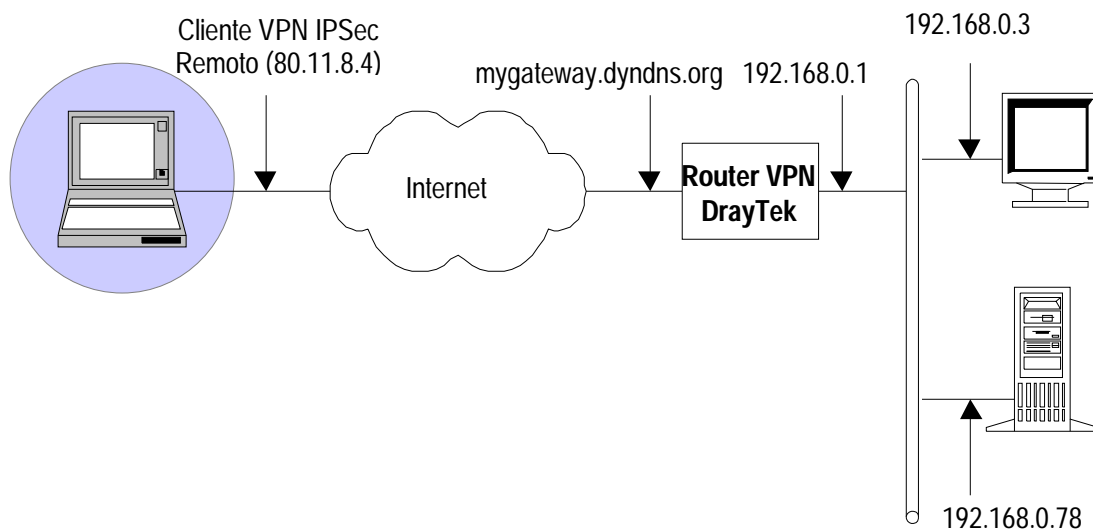
1.1 Objectivo deste documento

Este Guia de Configuração pretende descrever como configurar o Cliente VPN IPsec TheGreenBow com um Router VPN da DrayTek.

1.2 Topologia de Rede VPN

Como Rede VPN de exemplo (diagrama em baixo), vamos estabelecer um túnel IPsec com o Cliente VPN IPsec TheGreenBow para a LAN que se encontra atrás do Router VPN da DrayTek. O Cliente VPN IPsec (Remoto) está ligado á Internet via ligação Dialup/DSL.

(nota : todos os endereços usados neste documento servem apenas como exemplo)



1.3 Informação extra sobre o Router VPN DrayTek

Poderá encontrar mais informações (Manuais, Firmwares, FAQ's) sobre o Router VPN DrayTek no site : www.visus.pt/draytek ou www.draytek.com

2 Configuração em IPSec Main Mode

Esta secção descreve como estabelecer um Túnel VPN em IPSec Main Mode com o Router VPN da DrayTek.

2.1 Configuração de Router VPN da DrayTek

Aceda via browser á página de configuração do seu Router VPN DrayTek, e aceda ao menu **“VPN and Remote Access >> Remote Dial-in User”**

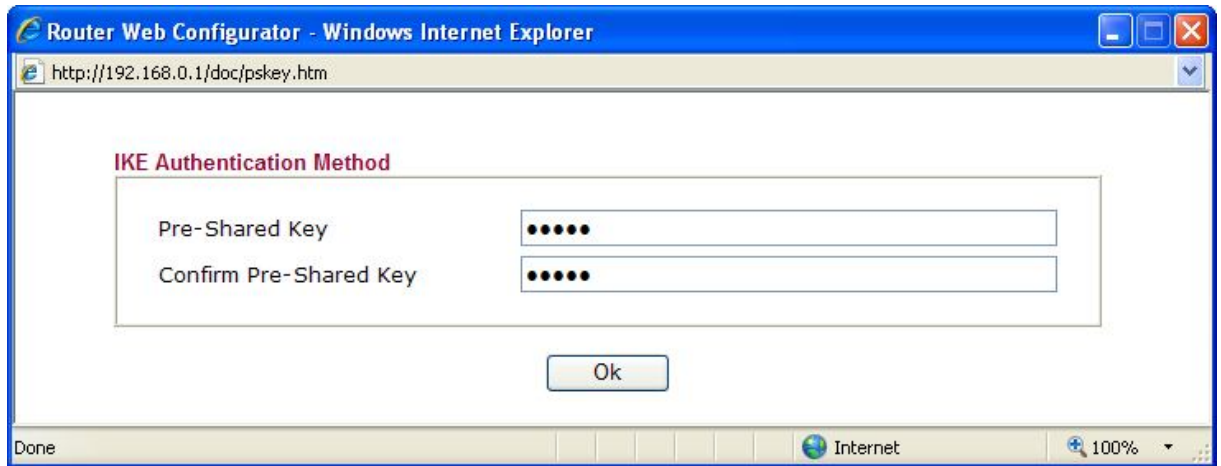
1. Clique num Index de forma a criar um novo utilizador Dial-in, conforme exemplo :

Index No. 1

User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="0"/> second(s)		Username <input type="text"/> Password <input type="text"/>
Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy <input type="text" value="None"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="checkbox"/> Digital Signature (X.509) <input type="text" value="None"/>
<input checked="" type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number <input type="text" value="80.11.8.4"/> or Peer ID <input type="text"/>		IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) <input type="checkbox"/> High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID <input type="text"/> (optional)
Callback Function <input type="checkbox"/> Check to enable Callback function <input type="checkbox"/> Specify the callback number Callback Number <input type="text"/> <input checked="" type="checkbox"/> Check to enable Callback Budget Control Callback Budget <input type="text" value="30"/> minute(s)		

- a. Clique na opção **“Enable this account”** para activar este utilizador.
- b. Coloque um valor de **“Idle Timeout”**. Coloque 0 para desactivar esta funcionalidade.
- c. Selecciono o tipo de protocolo a ser usado, neste caso em **“IPSec Tunnel”**.
- d. Active a opção de **“Specify Remote Node”** e coloque o **endereço IP Público Fixo** do Cliente VPN IPSec.

- e. Feito isto especifique uma password para este utilizador, clicando em **“IKE Pre-Shared Key”**, que abrirá uma janela pop-up, conforme exemplo :



- f. Selecciono o tipo de encriptações suportadas para este utilizador na secção de **“IP Security Method”**. Esta secção é para a *Phase 2*. (Por defeito o Router VPN DrayTek aceita todos os tipos de encriptações propostas pelo Cliente VPN IPSec)

Nota : Se activar a opção de **“Specify Remote Node”** (no ponto d.) este perfil funcionará apenas para um utilizador Remoto com o endereço IP Público Fixo indicado. Se pretende criar apenas um perfil para vários utilizadores, especialmente para quem tem endereços IP dinâmicos, não active esta opção. Neste caso não especifique a password conforme indicado no ponto e. , mas sim no menu **“VPN and Remote Access >> IPSec General Setup”**, conforme exemplo :

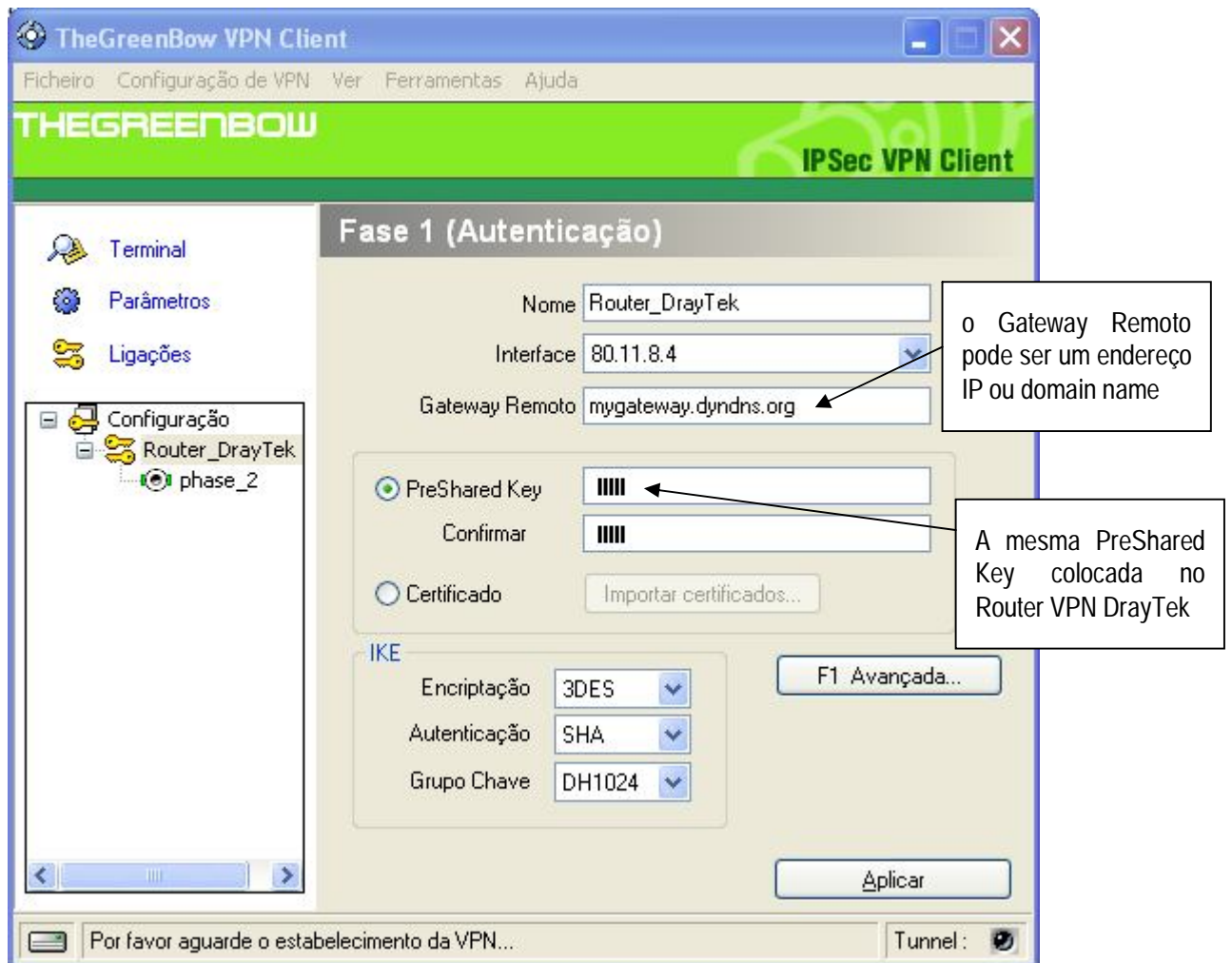
VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method	
Pre-Shared Key	<input type="password"/>
Re-type Pre-Shared Key	<input type="password"/>
IPSec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and authentic.

2.2 Configuração de Cliente VPN IPSec TheGreenBow

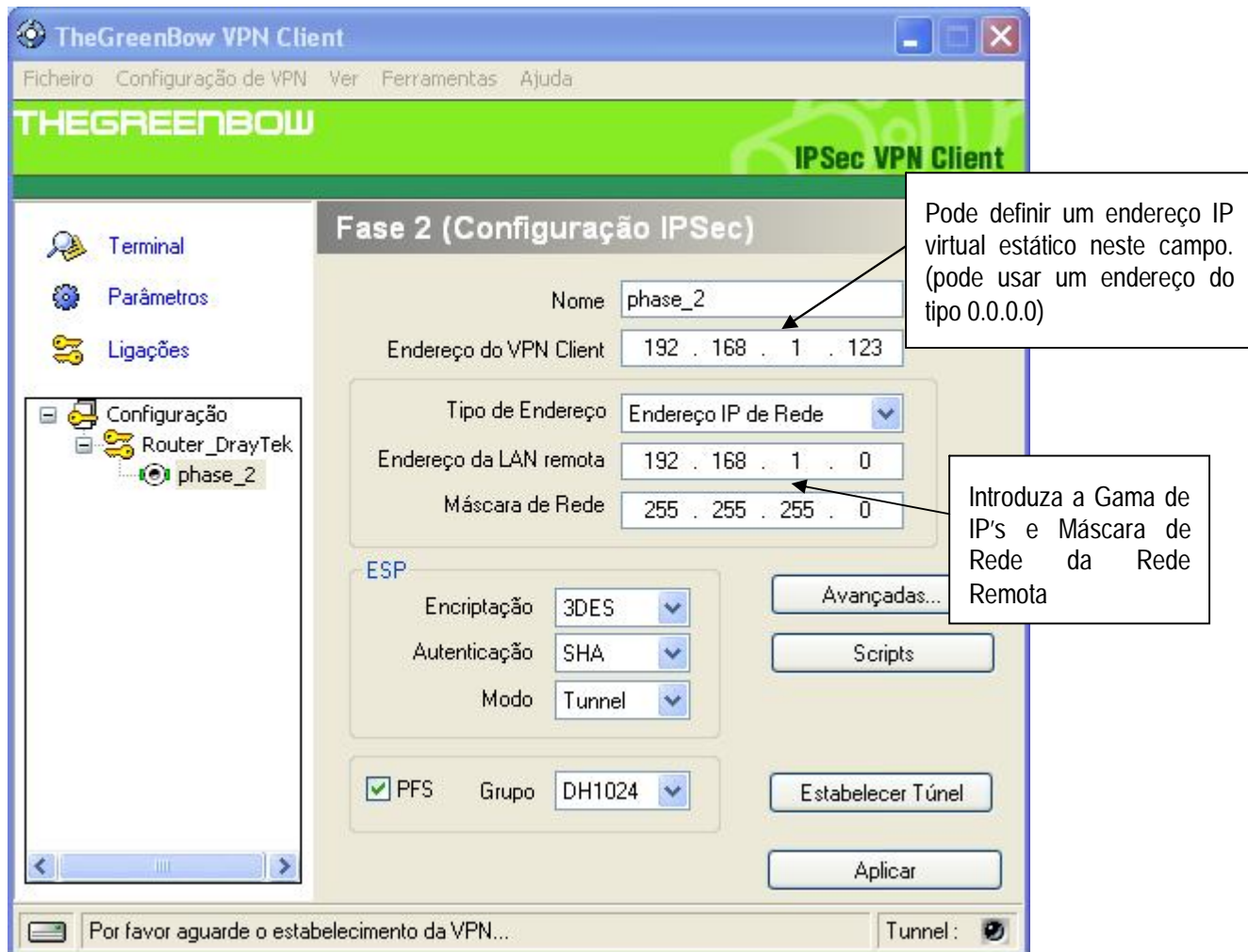
2.2.1 Configuração de *Phase 1 (IKE)*



- No campo "**Interface**" seleccione a placa de rede respectiva (neste caso a que tem o endereço IP Público Fixo). Seleccione "Qualquer", caso o endereço IP fornecido pelo ISP seja dinâmico.
- Coloque o endereço IP ou *domain name* do Router VPN DrayTek no campo "**Gateway Remoto**".
- Introduza a password no campo "**PreShared Key**", conforme especificada no Router VPN DrayTek.
- Na secção "**IKE**", seleccione o tipo de encriptações a serem usadas. O Router VPN DrayTek suporta :

Encriptação : DES / 3DES / AES128
 Autenticação : MD5 / SHA
 Grupo Chave : DH768 / DH1024

2.2.2 Configuração de Phase 2 (IPSec)



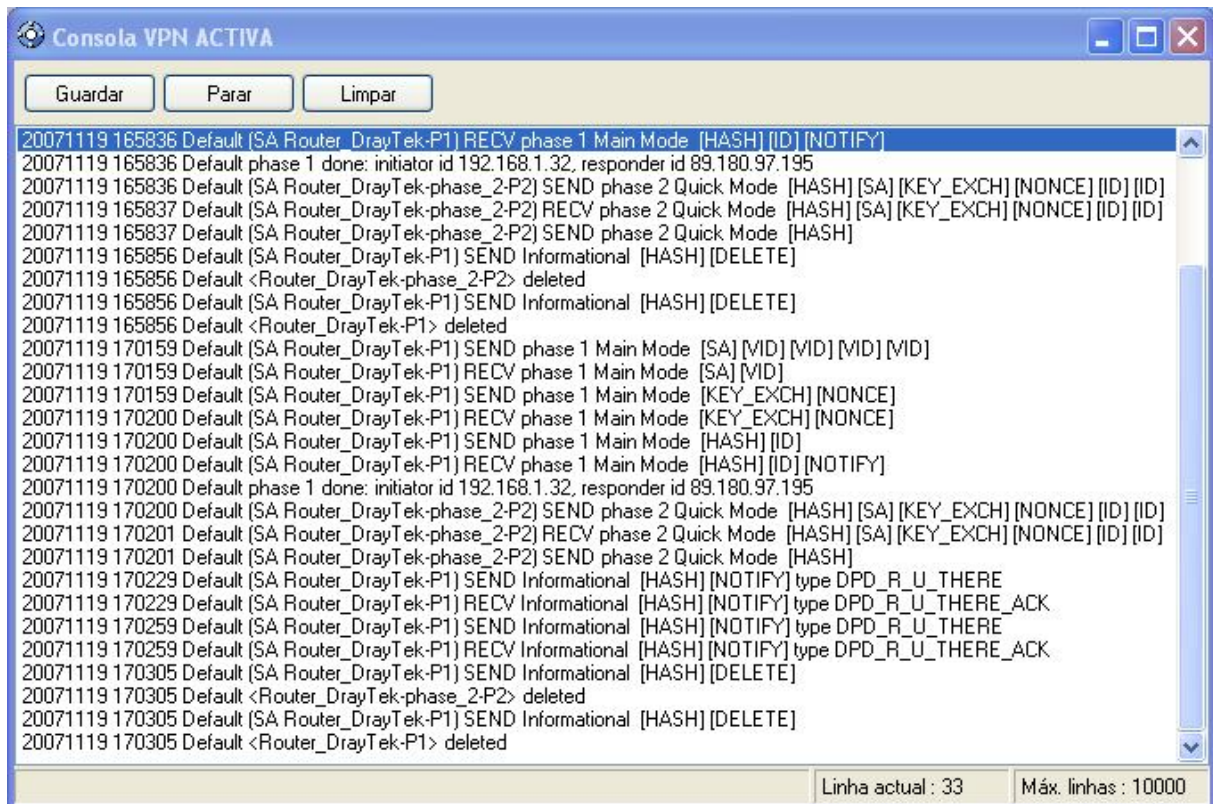
- No campo “**Endereço do VPN Client**” pode definir um endereço IP virtual estático, até pode definir um endereço IP do tipo 0.0.0.0.
- Selecione “Endereço IP de Rede” no campo “**Tipo de Endereço**” e introduza a Gama de IP’s e respectiva Máscara de Rede da Rede Remota.
- Na secção “**ESP**”, selecione o tipo de encriptações a serem usadas. O Router VPN DrayTek suporta :

Encriptação : DES / 3DES / AES128
 Autenticação : MD5 / SHA
 Modo : Tunnel
 Grupo PFS : DH768 / DH1024

2.2.3 Estabelecer Túnel VPN em IPSec

Assim que o Router VPN DrayTek e o Cliente VPN IPSec TheGreenBow se encontrarem devidamente configurados (conforme exemplo) poderá estabelecer o Túnel VPN em IPSec com sucesso. Certifique-se primeiro de que a sua firewall permite tráfego em IPSec.

1. Clique em **“Aplicar”** de forma a gravar todas as modificações efectuadas previamente no Cliente VPN IPSec.
2. Clique em **“Estabelecer Túnel”**, ou gere tráfego de modo a estabelecer o Túnel automaticamente (ex: ping, browser...).
3. Clique em **“Ligações”** para visualizar Túneis VPN estabelecidos.
4. Clique em **“Terminal”** para visualizar log's das ligações VPN IPSec, conforme exemplo :



```

20071119 165836 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [HASH][ID][NOTIFY]
20071119 165836 Default phase 1 done: initiator id 192.168.1.32, responder id 89.180.97.195
20071119 165836 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 165837 Default (SA Router_DrayTek-phase_2-P2) RECV phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 165837 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH]
20071119 165856 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 165856 Default <Router_DrayTek-phase_2-P2> deleted
20071119 165856 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 165856 Default <Router_DrayTek-P1> deleted
20071119 170159 Default (SA Router_DrayTek-P1) SEND phase 1 Main Mode [SA][VID][VID][VID][VID]
20071119 170159 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [SA][VID]
20071119 170159 Default (SA Router_DrayTek-P1) SEND phase 1 Main Mode [KEY_EXCH][NONCE]
20071119 170200 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [KEY_EXCH][NONCE]
20071119 170200 Default (SA Router_DrayTek-P1) SEND phase 1 Main Mode [HASH][ID]
20071119 170200 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [HASH][ID][NOTIFY]
20071119 170200 Default phase 1 done: initiator id 192.168.1.32, responder id 89.180.97.195
20071119 170200 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 170201 Default (SA Router_DrayTek-phase_2-P2) RECV phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 170201 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH]
20071119 170229 Default (SA Router_DrayTek-P1) SEND Informational [HASH][NOTIFY] type DPD_R_U_THERE
20071119 170229 Default (SA Router_DrayTek-P1) RECV Informational [HASH][NOTIFY] type DPD_R_U_THERE_ACK
20071119 170259 Default (SA Router_DrayTek-P1) SEND Informational [HASH][NOTIFY] type DPD_R_U_THERE
20071119 170259 Default (SA Router_DrayTek-P1) RECV Informational [HASH][NOTIFY] type DPD_R_U_THERE_ACK
20071119 170305 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 170305 Default <Router_DrayTek-phase_2-P2> deleted
20071119 170305 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 170305 Default <Router_DrayTek-P1> deleted
  
```

Linha actual : 33 Máx. linhas : 10000

3 Configuração em IPSec Aggressive Mode

Esta secção descreve como estabelecer um Túnel VPN em IPSec Aggressive Mode com o Router VPN da DrayTek.

3.1 Configuração de Router VPN da DrayTek

Aceda via browser á página de configuração do seu Router VPN DrayTek, e aceda ao menu **“VPN and Remote Access >> Remote Dial-in User”**

1. Clique num Index de forma a criar um novo utilizador Dial-in, conforme exemplo :

Index No. 1

User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="0"/> second(s)		Username <input type="text"/> Password <input type="text"/>
Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy <input type="text" value="None"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="checkbox"/> Digital Signature (X.509) <input type="text" value="None"/>
<input checked="" type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number <input type="text"/> or Peer ID <input type="text" value="abc@a.com"/>		IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) <input type="checkbox"/> High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID <input type="text"/> (optional)
Callback Function <input type="checkbox"/> Check to enable Callback function <input type="checkbox"/> Specify the callback number Callback Number <input type="text"/> <input checked="" type="checkbox"/> Check to enable Callback Budget Control Callback Budget <input type="text" value="30"/> minute(s)		

- a. Clique na opção **“Enable this account”** para activar este utilizador.
- b. Coloque um valor de **“Idle Timeout”**. Coloque 0 para desactivar esta funcionalidade.
- c. Selecciono o tipo de protocolo a ser usado, neste caso em **“IPSec Tunnel”**.
- d. Active a opção de **“Specify Remote Node”** e coloque o **“Peer ID”** do Cliente VPN IPSec (correspondente ao campo “ID Local”)

Nota : O campo “Local ID” é opcional. Se especificar este campo, terá de configurar o campo “ID Remoto” no Cliente VPN IPSec TheGreenBow.

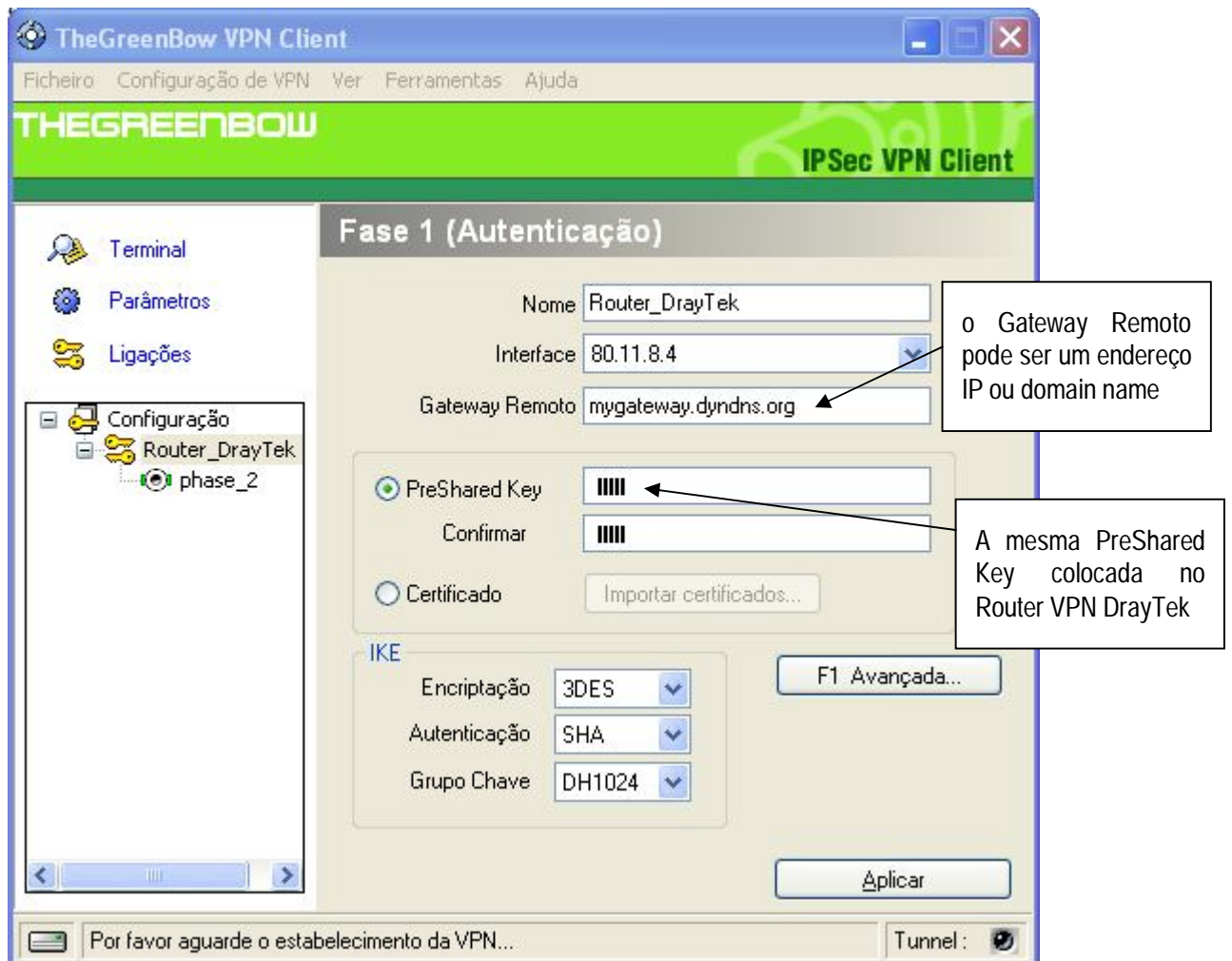
- e. Feito isto especifique uma password para este utilizador, clicando em **"IKE Pre-Shared Key"**, que abrirá uma janela pop-up, conforme exemplo :



- f. Seleccione o tipo de encriptações suportadas para este utilizador na secção de **"IP Security Method"**. Esta secção é para a *Phase 2*. (Por defeito o Router VPN DrayTek aceita todos os tipos de encriptações propostas pelo Cliente VPN IPSec)

3.2 Configuração de Cliente VPN IPSec TheGreenBow

3.2.1 Configuração de *Phase 1 (IKE)*



- No campo "**Interface**" seleccione a placa de rede respectiva (neste caso a que tem o endereço IP Público Fixo). Seleccione "Qualquer", caso o endereço IP fornecido pelo ISP seja dinâmico.
- Coloque o endereço IP ou *domain name* do Router VPN DrayTek no campo "**Gateway Remoto**".
- Introduza a password no campo "**PreShared Key**", conforme especificada no Router VPN DrayTek.
- Na secção "**IKE**", seleccione o tipo de encriptações a serem usadas. O Router VPN DrayTek suporta :

Encriptação : DES / 3DES / AES128
 Autenticação : MD5 / SHA
 Grupo Chave : DH768 / DH1024

- e. Clique no botão “F1 Avançada...”. Na janela de pop-up active a opção “Modo Agressivo” e escolha o **Tipo de ID Local** com o mesmo **Valor de ID** definido no Router VPN DrayTek. (Neste exemplo é do tipo “Email” com o valor abc@a.com)

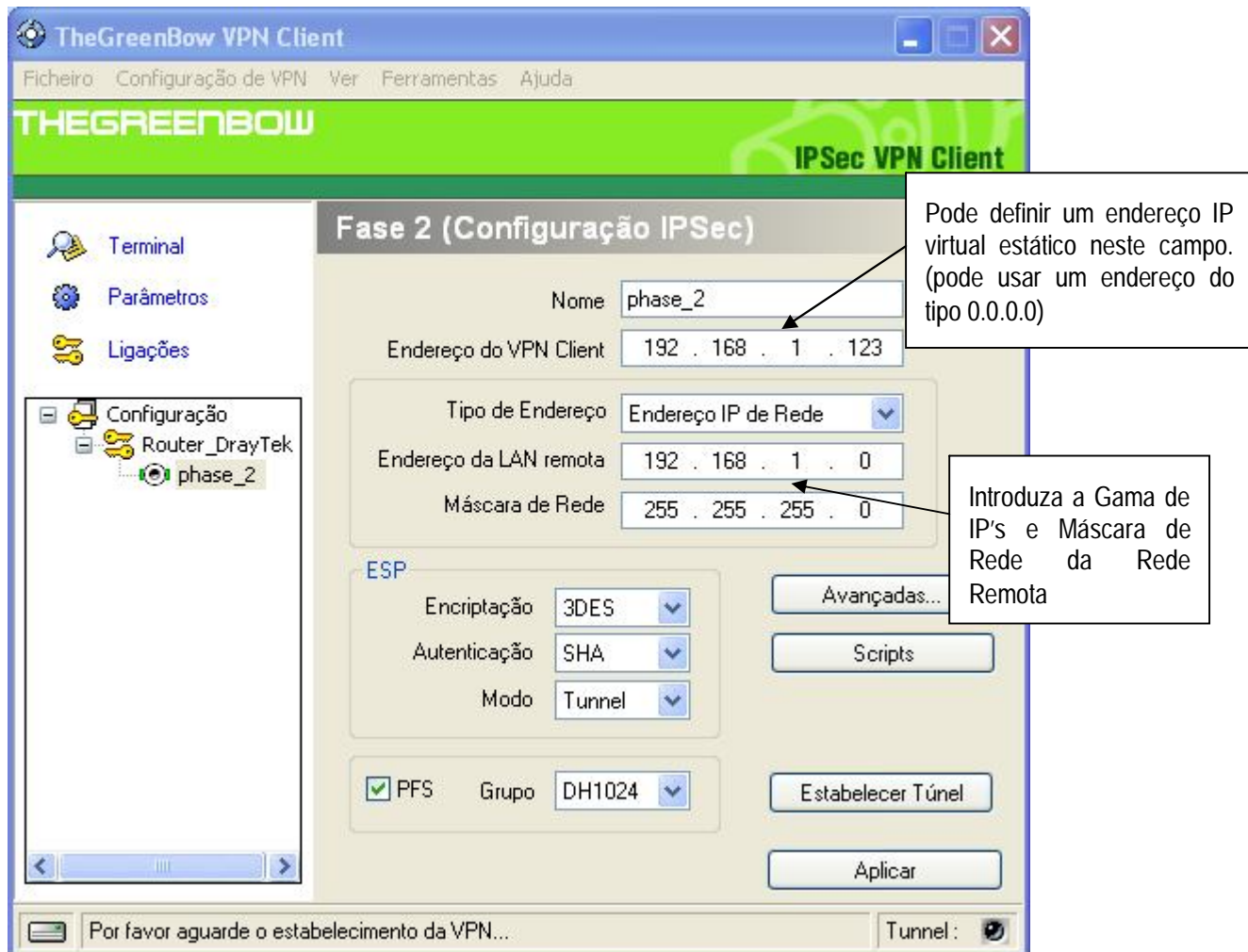
The screenshot shows the 'Avançadas...' configuration window. It has a title bar with a close button. The main content area is divided into sections:

- Configurações avançadas:** Contains a checkbox for 'Modo de Configuraç' (unchecked), a 'GW.Redund.' input field, a checked checkbox for 'Modo Agressivo', and a 'NAT-T' dropdown menu set to 'Automático'.
- X-Auth:** Contains checkboxes for 'X-Auth Popup' (unchecked) and 'Hybrid Mode' (unchecked), and input fields for 'Login:' and 'Password:'.
- ID Local e Remoto:** Contains two rows. The first row has 'ID Local' with a dropdown set to 'Email' and an input field containing 'abc@a.com'. The second row has 'ID Remoto' with a dropdown and an empty input field.

At the bottom right, there are 'Ok' and 'Cancelar' buttons.

Nota : Se configurou o campo “Local ID” no Router VPN DrayTek, terá de configurar o campo “ID Remoto” no Cliente VPN IPsec TheGreenBow.

3.2.2 Configuração de Phase 2 (IPSec)



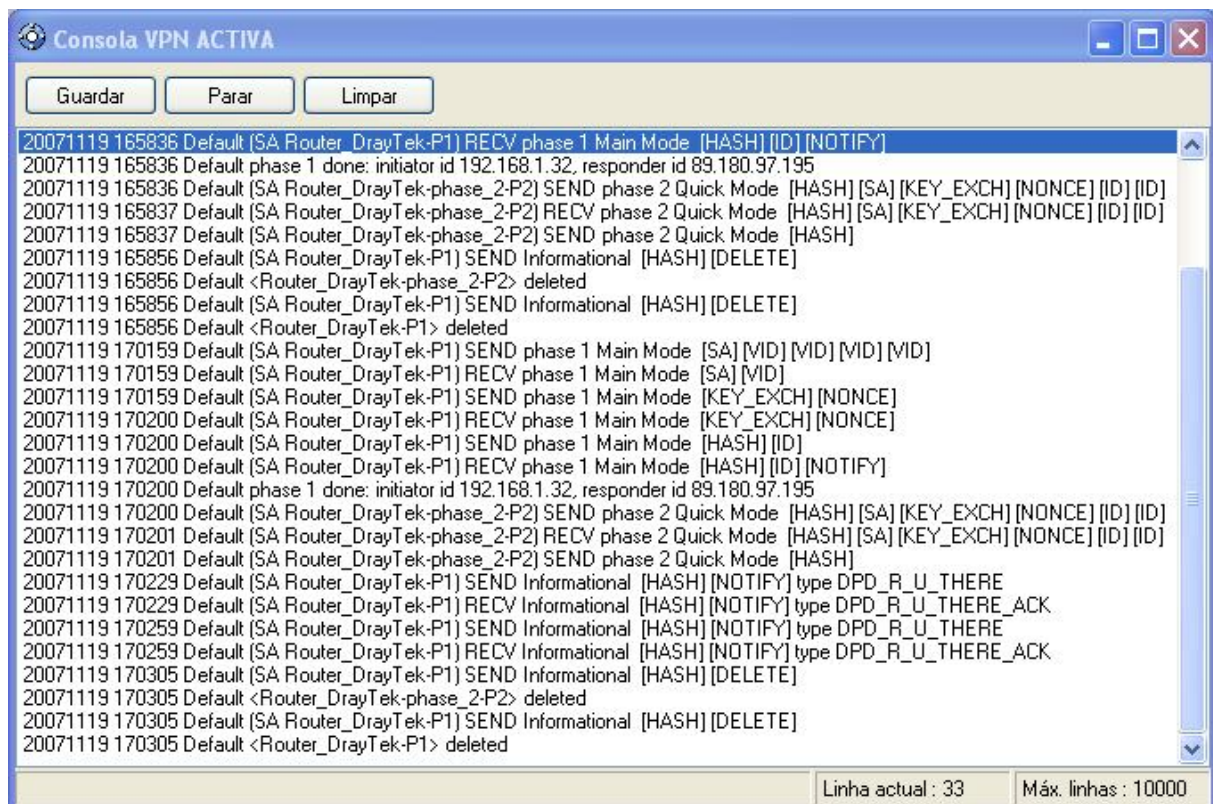
- No campo “**Endereço do VPN Client**” pode definir um endereço IP virtual estático, até pode definir um endereço IP do tipo 0.0.0.0.
- Selecione “Endereço IP de Rede” no campo “**Tipo de Endereço**” e introduza a Gama de IP’s e respectiva Máscara de Rede da Rede Remota.
- Na secção “**ESP**”, selecione o tipo de encriptações a serem usadas. O Router VPN DrayTek suporta :

Encriptação : DES / 3DES / AES128
 Autenticação : MD5 / SHA
 Modo : Tunnel
 Grupo PFS : DH768 / DH1024

3.2.3 Estabelecer Túnel VPN em IPSec

Assim que o Router VPN DrayTek e o Cliente VPN IPSec TheGreenBow se encontrarem devidamente configurados (conforme exemplo) poderá estabelecer o Túnel VPN em IPSec com sucesso. Certifique-se primeiro de que a sua firewall permite tráfego em IPSec.

1. Clique em **“Aplicar”** de forma a gravar todas as modificações efectuadas previamente no Cliente VPN IPSec.
2. Clique em **“Estabelecer Túnel”**, ou gere tráfego de modo a estabelecer o Túnel automaticamente (ex: ping, browser...).
3. Clique em **“Ligações”** para visualizar Túneis VPN estabelecidos.
4. Clique em **“Terminal”** para visualizar log's das ligações VPN IPSec, conforme exemplo :



Consola VPN ACTIVA

Guardar Parar Limpar

```
20071119 165836 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [HASH][ID][NOTIFY]
20071119 165836 Default phase 1 done: initiator id 192.168.1.32, responder id 89.180.97.195
20071119 165836 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 165837 Default (SA Router_DrayTek-phase_2-P2) RECV phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 165837 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH]
20071119 165856 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 165856 Default <Router_DrayTek-phase_2-P2> deleted
20071119 165856 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 165856 Default <Router_DrayTek-P1> deleted
20071119 170159 Default (SA Router_DrayTek-P1) SEND phase 1 Main Mode [SA][VID][VID][VID][VID]
20071119 170159 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [SA][VID]
20071119 170159 Default (SA Router_DrayTek-P1) SEND phase 1 Main Mode [KEY_EXCH][NONCE]
20071119 170200 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [KEY_EXCH][NONCE]
20071119 170200 Default (SA Router_DrayTek-P1) SEND phase 1 Main Mode [HASH][ID]
20071119 170200 Default (SA Router_DrayTek-P1) RECV phase 1 Main Mode [HASH][ID][NOTIFY]
20071119 170200 Default phase 1 done: initiator id 192.168.1.32, responder id 89.180.97.195
20071119 170200 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 170201 Default (SA Router_DrayTek-phase_2-P2) RECV phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20071119 170201 Default (SA Router_DrayTek-phase_2-P2) SEND phase 2 Quick Mode [HASH]
20071119 170229 Default (SA Router_DrayTek-P1) SEND Informational [HASH][NOTIFY] type DPD_R_U_THERE
20071119 170229 Default (SA Router_DrayTek-P1) RECV Informational [HASH][NOTIFY] type DPD_R_U_THERE_ACK
20071119 170259 Default (SA Router_DrayTek-P1) SEND Informational [HASH][NOTIFY] type DPD_R_U_THERE
20071119 170259 Default (SA Router_DrayTek-P1) RECV Informational [HASH][NOTIFY] type DPD_R_U_THERE_ACK
20071119 170305 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 170305 Default <Router_DrayTek-phase_2-P2> deleted
20071119 170305 Default (SA Router_DrayTek-P1) SEND Informational [HASH][DELETE]
20071119 170305 Default <Router_DrayTek-P1> deleted
```

Linha actual : 33 Máx. linhas : 10000

	Doc.Ref	tgbvpn_ug_YYYYYY_en
	Doc.version	3.0 – Nov 2007
	VPN version	4.x

4 Problemas de Ligação VPN IPSec

4.1 Erro : « PAYLOAD MALFORMED » (Phase 1 [SA] errada)

```

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

```

Este erro significa que existiu um erro na negociação de SA na *Phase 1*, verifique se tem as mesmas encriptações em ambos os lados do Túnel.

4.2 Erro : « INVALID COOKIE »

```

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

```

Este erro significa que existe um dos lados a usar uma SA que já não se encontra em uso. Reinicie a VPN em ambos os lados.

4.3 Erro : « no keystate »

```

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

```

Verifique se a "PreShared Key" ou o "ID Local" estão correctos (clique em "F1 Avançada...")

4.4 Erro : « received remote ID other than expected »

```

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

```

O valor "ID Remoto" (clique em "F1 Avançada...") não é o mesmo.

4.5 Erro : « NO PROPOSAL CHOSEN »

```

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

```

Verifique se as encriptações de negociação de *Phase 2* são os mesmos em ambos os lados do Túnel.

Verifique a *Phase 1* se obter esta mensagem :

```

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

```

4.6 Erro : « INVALID ID INFORMATION »

```

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

```

Verifique se o ID de *Phase 2* (Endereço IP de Rede) está correcto, e se o mesmo é válido no outro lado do Túnel.

Verifique também o tipo de ID (“Endereço IP único” e “Endereço IP de Rede”). Se não especificar nenhuma Máscara de Rede, é porque está a usar uma gama do tipo IPV4_ADDR (e não do tipo IPV4_SUBNET).

4.7 Cliquei em “Estabelecer Túnel”, mas não aconteceu nada.

Consulte os logs em cada lado do Túnel. Pedidos de IKE podem ser bloqueados por firewalls. Um Cliente IPsec usa a porta 500 em UDP e protocolo ESP (protocolo 50).

4.8 O túnel VPN está estabelecido mas não consigo fazer pings!

Se o túnel VPN encontra-se estabelecido, mas mesmo assim não consegue fazer pings para a Rede Remota, aqui ficam algumas dicas :

- Verifique as configurações da *Phase 2* : Endereço do VPN Client e da LAN remota. O endereço do VPN Client não deve fazer parte da Rede Remota.
- Assim que o túnel VPN se encontrar estabelecido, serão enviados pacotes via protocolo ESP, este protocolo pode estar a ser bloqueado por uma firewall.
- Consulte os logs do Router VPN DrayTek, os pacotes poderão estar a ser bloqueados por alguma regra de firewall.
- Confirme se o seu ISP suporta o protocolo ESP.
- Verifique se o "default gateway" do computador remoto está devidamente configurado (neste caso terá de estar configurado para o endereço IP do Router VPN DrayTek).
- Não tente aceder aos computadores remotos pelo seu nome. Especifique antes o seu endereço IP de Rede.
- Recomendamos a instalação do software Ethereal (<http://www.ethereal.com>) para analisar a transmissão de pacotes de rede.

THEGREENBOW 0101110101	Doc.Ref	tgbvpn_ug_YYYYYY_en
	Doc.version	3.0 – Nov 2007
	VPN version	4.x

5 Contactos

Notícias e Actualizações para Cliente VPN IPSec TheGreenBowNews no site : <http://www.thegreenbow.com>

Suporte Técnico via email em support@thegreenbow.com

Contacto Comercial via email em sales@thegreenbow.com