



Cliente VPN IPSec TheGreenBow

Guia de Configuração

GatePRO


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

Contacto: support@thegreenbow.pt

Guia de Configuração escrito por:

Escritor: Equipe de Suporte

Empresa: Interage S.A. (<http://interage.com.br>)

	Doc.Ref	tgbvpn_cg_GatePRO_pt
	Doc.version	Mar 2012
	VPN version	5.x

Lista de Conteúdos

1	Introdução.....	3
1.1	Objectivo deste documento.....	3
1.2	Topologia de Rede VPN	3
1.3	Restrições GatePRO.....	3
1.4	Informação sobre o GatePRO.....	3
2	Configuração VPN GatePRO	4
3	Configuração do Cliente VPN IPSec TheGreenBow	6
3.1	Cliente VPN - Configuração Fase 1 (IKE).....	6
3.2	Cliente VPN - Configuração Fase 2 (IPSec)	7
3.3	Estabelecer Túnel VPN em IPSec	7
4	Problemas de Ligação VPN IPSec	9
4.1	Erro : « PAYLOAD MALFORMED » (Fase 1 [SA] errada)	9
4.2	Erro : « INVALID COOKIE »	9
4.3	Erro : « no keystate »	9
4.4	Erro : « received remote ID other than expected »	9
4.5	Erro : « NO PROPOSAL CHOSEN »	10
4.6	Erro : « INVALID ID INFORMATION »	10
4.7	Cliquei em "Estabelecer Túnel", mas não aconteceu nada.....	10
4.8	Túnel VPN está estabelecido mas não consigo fazer pings!	10
5	Contactos	12

1 Introdução

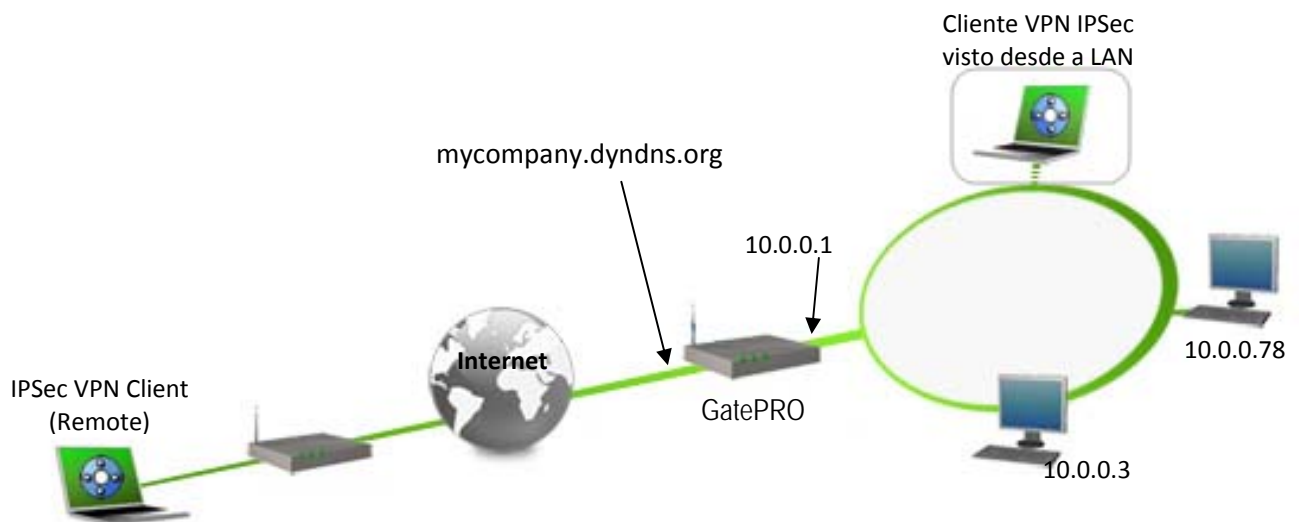
1.1 Objectivo deste documento

Este Guia de Configuração pretende descrever como configurar o Cliente VPN IPsec TheGreenBow com um GatePRO a fim de estabelecer uma conexão VPN de acesso remoto a rede corporativa.

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 GatePRO. 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 Restrições GatePRO

O GatePRO deve estar ligado a Internet com um endereço IP válido e estático. É possível que alguns roteadores ADSL necessitem de ajustes na configuração para permitir o tráfego do protocolo IPsec.

Os nossos testes e a configuração VPN foram realizados com GatePRO versão 2.10.5.

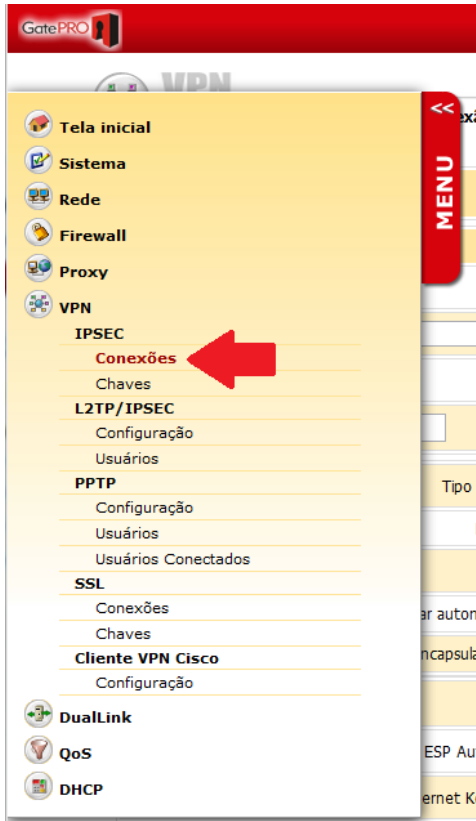
1.4 Informação sobre o GatePRO

É fundamental que todos os utilizadores tenham toda a informação sobre o GatePRO. Todas as informações sobre o produto, o Guia do Utilizador assim como uma base de conhecimento sobre o GatePRO podem ser encontrados no site: <http://www.GatePRO.com.br>.

2 Configuração VPN GatePRO

Esta seção descreve como estabelecer um Túnel VPN com o GatePRO.

Clique no menu do GatePRO e selecione "VPN / IPSEC / Conexões" conforme tela abaixo:



Depois clique no botão "Nova Conexão":



Será apresentada a tela a seguir com os dados da conexão VPN que será criada:

The screenshot shows the 'Nova Conexão' (New Connection) configuration page in GatePRO. The interface is divided into several sections:

- Nome Conexão:** A text field containing 'greenbow'. A callout points to it with the text 'Nome da conexão VPN'.
- Configuração Local:**
 - Endereço IP:** A dropdown menu set to 'Usar rota padrão'. A callout points to it with the text 'Endereço IP do GatePRO'.
 - Subrede:** A dropdown menu set to 'Especificar' followed by the IP address '10.0.0.0/8'. A callout points to it with the text 'Endereço da rede local ligada ao GatePRO'.
 - Gateway:** A dropdown menu set to 'Usar rota padrão'.
 - ID @:** A text field containing 'vpn-server'.
- Configuração remota:**
 - Endereço IP:** A dropdown menu set to 'Qualquer'.
 - Subrede:** A dropdown menu set to 'Qualquer rede privada (RFC1918)'.
 - Gateway:** A dropdown menu set to 'Nenhum'.
 - ID @:** An empty text field.
- Tipo de Conexão:** A dropdown menu set to 'PSK'.
- Habilitar PFS:** Radio buttons for 'Sim' and 'Não', with 'Não' selected.
- PFS Group:** A dropdown menu set to 'Nenhum'.
- Iniciar automaticamente:** An unchecked checkbox.
- Forçar ESP no encapsulamento UDP:** An unchecked checkbox.
- Chave PSK:** A text field containing '<chavepsk>'. A callout points to it with the text 'Use os mesmos dados informados no cliente VPN'.
- ESP Authentication:** A dropdown menu set to 'aes256-sha1'.
- IKE (Internet Key Exchange):** A dropdown menu set to 'aes256-sha1'.

No campo "Nome Conexão" especifique um nome amigável para esta conexão. Este nome é usado apenas para identificar a conexão entre as outras conexões configuradas neste GatePRO.


Na tabela "Configuração Local" deve-se especificar os parâmetros da rede local que está ligada diretamente ao GatePRO. Especifique o endereço IP do GatePRO no campo "Endereço IP" (em casos onde o GatePRO está ligado a um ADSL com IP inválido é necessário especificar o IP real do GatePRO e não o IP válido).

O parâmetro "Subrede" define o endereço da rede que está sendo interligada via VPN. Em "Gateway" pode-se usar o IP do roteador do GatePRO ou a opção "Usar rota padrão".

Na tabela "Configuração remota" deve-se especificar os parâmetros das redes ou usuários remotos que estão se conectando nesta VPN. Neste caso, para usuários móveis (ou usuários que não tem um endereço IP fixo) o campo "Endereço IP" deve ser preenchido com a opção "Qualquer". O campo "Subrede" deve conter o valor "Qualquer rede privada (RFC1918)" e o "Gateway" pode ser definido como "Nenhum".

Selecione o "Tipo de Conexão" como "PSK". Não é necessário habilitar PFS. Finalmente selecione a "Chave PSK" e os parâmetros de "ESP" e "IKE". Finalmente clique em "Salvar".

Lembre-se de ajustar as regras de firewall para permitir o tráfego entre o cliente VPN e a rede interna.

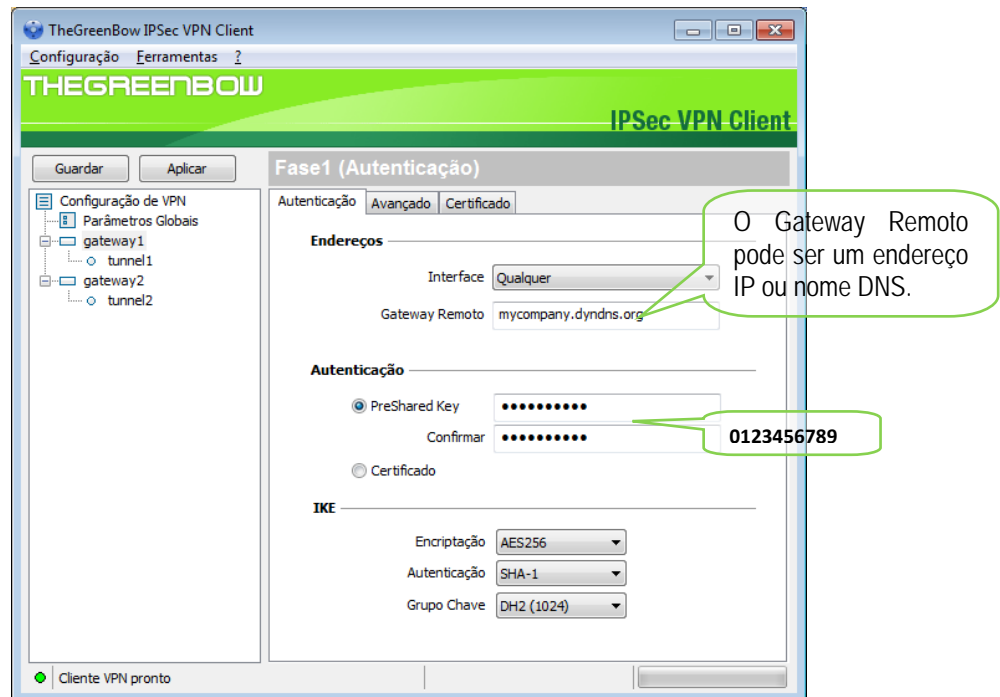
	Doc.Ref	tgbvpn_cg_GatePRO_pt
	Doc.version	Mar 2012
	VPN version	5.x

3 Configuração do Cliente VPN IPSec TheGreenBow

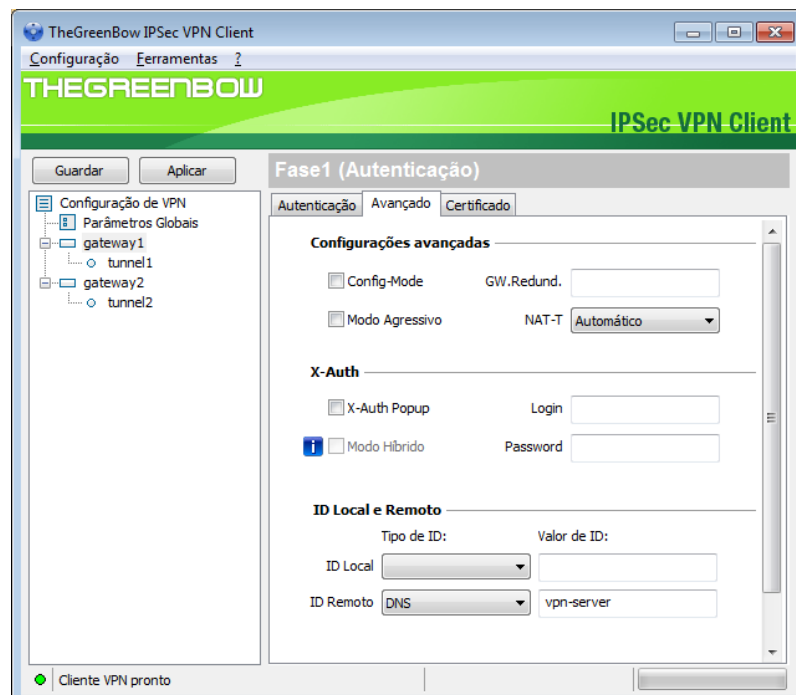
Esta secção descreve a configuração necessária para se conectar ao GatePRO.

Para fazer o download da última versão do software cliente VPN IPSec TheGreenBow, por favor, vá para http://www.thegreenbow.pt/vpn_down.html.


3.1 Cliente VPN - Configuração Fase 1 (IKE)



Configuração Fase 1 - Autenticação

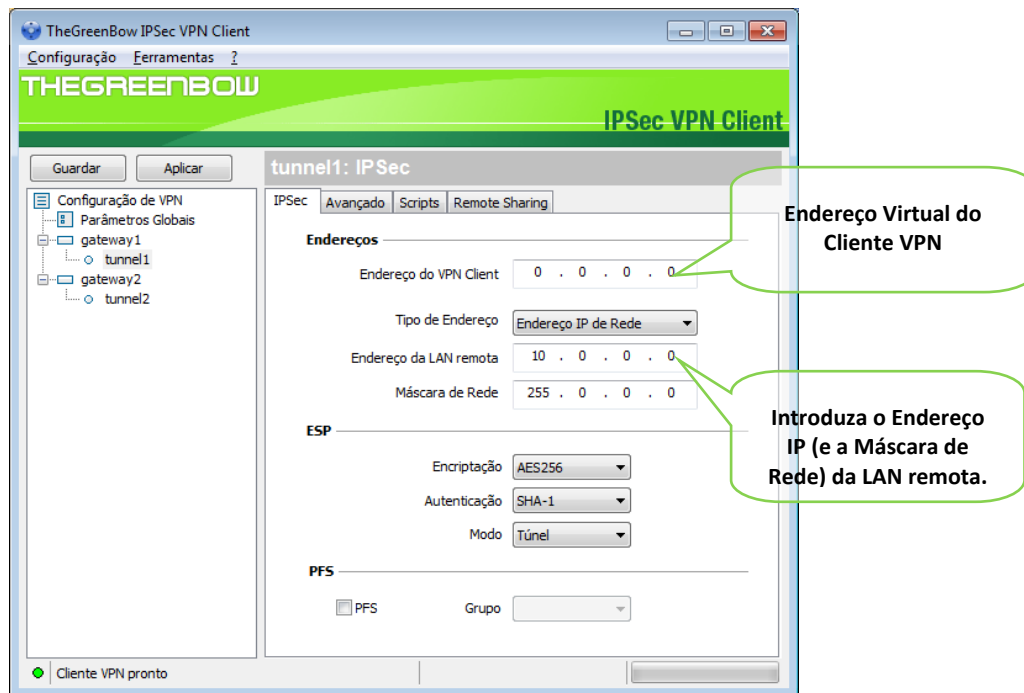


Configuração Fase 1 - Avançado

	Doc.Ref	tgbvpn_cg_GatePRO_pt
	Doc.version	Mar 2012
	VPN version	5.x

Você pode usar tanto Preshared Key, Certificados, pen USB ou X-auth para a autenticação do usuário com o roteador GatePRO. Este é um exemplo de configuração do que pode ser realizado para a autenticação do usuário. Você pode querer referir-se quer ao Guia do Utilizador do GatePRO ou ao Guia do Utilizador do Cliente VPN IPSec para obter mais detalhes sobre as opções de autenticação do usuário.

3.2 Cliente VPN - Configuração Fase 2 (IPSec)



Configuração Fase 2

3.3 Estabelecer Túnel VPN em IPSec

Assim que o GatePRO 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 **“Abrir 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 **“Consola”** para visualizar log's das ligações VPN IPSec, conforme exemplo.

Doc.Ref	tgbvpn_cg_GatePRO_pt
Doc.version	Mar 2012
VPN version	5.x

```

20080409 131143 Default (SA Test_VPN-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [MD] [MD] [MD]
20080409 131143 Default (SA Test_VPN-P1) RECV phase 1 Main Mode [SA] [VID] [VID]
20080409 131143 Default (SA Test_VPN-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080409 131143 Default (SA Test_VPN-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080409 131143 Default (SA Test_VPN-P1) SEND phase 1 Main Mode [HASH] [ID]
20080409 131143 Default (SA Test_VPN-P1) RECV phase 1 Main Mode [HASH] [ID]
20080409 131143 Default phase 1 done: initiator id 192.168.6.100, responder id 192.168.1.10
20080409 131143 Default (SA Test_VPN-Test-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080409 131143 Default (SA Test_VPN-Test-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080409 131143 Default (SA Test_VPN-Test-P2) SEND phase 2 Quick Mode [HASH]

```


	Doc.Ref	tgbvpn_cg_GatePRO_pt
	Doc.version	Mar 2012
	VPN version	5.x

4 Problemas de Ligação VPN IPsec

4.1 Erro : « PAYLOAD MALFORMED » (Fase 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 *Fase 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.

	Doc.Ref	tgbvpn_cg_GatePRO_pt
	Doc.version	Mar 2012
	VPN version	5.x

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 *Fase 2* são os mesmos em ambos os lados do Túnel.

Verifique a *Fase 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 *Fase 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 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 *Fase 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 GatePRO, os pacotes poderão estar a ser bloqueados por alguma regra de firewall.
- Confirme se o seu ISP suporta o protocolo ESP.

THEGREENBOW 01010101 01010101	Doc.Ref	tgbvpn_cg_GatePRO_pt
	Doc.version	Mar 2012
	VPN version	5.x

- Verifique se o “default gateway” do computador remoto está devidamente configurado (neste caso terá de estar configurado para o endereço IP do GatePRO).
- Não tente aceder aos computadores remotos pelo seu nome. Especifique antes o seu endereço IP de Rede.
- Recomendamos a instalação do software Wireshark (<http://www.wireshark.com>) para analisar a transmissão de pacotes de rede.

THEGREENBOW 03941903 0311103	Doc.Ref	tgbvpn_cg_GatePRO_pt
	Doc.version	Mar 2012
	VPN version	5.x

5 Contactos

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

Suporte Técnico via email em support@thegreenbow.pt

Contacto Comercial via email em sales@thegreenbow.pt

Secure, Strong, Simple.

TheGreenBow Security Software