Cliente VPN IPSec TheGreenBow

Manual do Usuário

Contacto: support@thegreenbow.pt

Website: www.thegreenbow.pt

Cliente VPN IPSec TheGreenBow - Manual do Usuário

Editado: October 2008 no Estoril.

Sumário

Parte

Apresentação do Cliente VPN IPSec TheGreenBow

1 Apresentação do Cliente VPN IPSec TheGreenBow

1.1 O que é o Cliente VPN IPSec TheGreenBow ?

O Cliente VPN IPSec TheGreenBow é um software VPN IPSec para todas as versões do Windows que permite estabelecer conexões seguras através da Internet geralmente entre um trabalhador distante e a Intranet Corporativa. IPSec é a maneira mais segura para conectar-se à empresa ao fornecer autenticação forte do usuário, encriptação forte do túnel, com capacidade de integrar-se na configuração da rede existente.
O Cliente VPN IPSec TheGreenBow é o resultado de muitos anos de experiência na segurança de redes e no desenvolvimento de controladores de rede para Windows, como também da investigação feita nessas áreas.
O Cliente VPN IPSec completa a nossa gama de produtos de segurança de redes e tal como todos os nossos produtos é extremamente fácil de usar e instalar.

1.2 Solução Multi Gateway VPN

A estratégia de TheGreenBow é de ser compatível com o maior número de gateways e appliances VPN, disponível no mercado afim de oferecer uma verdadeira solução multi-vendedor aos seus clientes. As novas Gateways VPN IPSec ou appliances são testadas nos nossos laboratórios. A lista de routers VPN certificados está disponível no nosso website e aumenta todos os dias, por isso não hesite em verificar regularmente as novas gateways VPN compatíveis.

1.3 Solução Multi Token USB e SmartCard

Existe muitos Tokens USB e SmartCards disponíveis no mercado. É nossa missão suportar o maior número de construtores de Token USB e SmartCard, afim de oferecer uma verdadeira soluução multi-vendedor aos nossos clientes. Novos dispositivos Token USB e SmartCard são testados nos nossos laboratórios. A lista de Tokens USB certificados está disponível no nosso website e aumenta todos os dias, por isso não hesite em verificar regularmente os novos Tokens USB compatíveis.

No caso do seu Token USB não estar na lista, por favor contacte o nosso Suporte Técnico para nós o certificarmos.

1.4 Suporte de Appliances Linux

TheGreenBow suporta várias implementações Linux de VPN IPSec como StrongS/WAN e FreeS/WAN. Portanto o Cliente VPN IPSec TheGreenBow é compatível com a maioria dos routers/appliances IPSec baseadas nessas implementações Linux. No futuro suportaremos mais implementações Linux. A lista das appliances VPN Linux suportadas está disponível no nosso website.

1.5 Funcionalidades do Cliente VPN IPSec TheGreenBow

Versões do Windows	Win2000, WinXP, Vista (32bit)
Idiomas	Chinês (simplificado), Holandês, Inglês, Finlandês, Francês, Alemão, Grego, Italiano, Japonês, Polaco, Português, Russo, Sérvio, Esloveno, Espanhol e Turco.
Modos de Conexão	Funciona tanto no modo VPN "ponto-a-ponto" como também "ponto-a-múltiplos", sem servidor ou gateway. Todos os tipos de conexões como Dial up, DSL, Cabo, GSM/GPRS e WiFi são suportados. Permite rede Range IP. Pode funcionar em sessão RDP (conexão Remote Desktop).
Tunneling Protocol	Suporte IKE completo: A nossa implementação IKE é baseada na implementação OpenBSD 3.1 (ISAKMPD), isso oferece a melhor compatibilidade com os roteadores IPSec existentes. Suporte IPSec completo: • Main mode e Aggressive mode • Algoritmos de hash MD5 e SHA • Mudança da porta IKE
NAT Traversal	NAT Traversal Draft 1 (avançado), Draft 2 e 3 (implementação completa) • Incluindo suporte NAT_OA • Incluindo NAT keepalive • Incluindo NAT T Aggressive Mode Modo NAT-Traversal forçado.
Encriptação	Fornece vários algoritmos de encriptação: • Encriptação 3DES, DES e AES 128/192/256bits. • Suporte dos Grupos DH 1, 2, 5 e 14 (i.e. 768, 1024, 1536 e 2048).
Autenticação do Usuário	• Suporte X-AUTH • Suporte PreShared key e Certificados X509. É compatível com a maioria dos roteadores IPSec existentes • Suporte Token USB & SmartCard • Suporte flexível de Certificados: PEM, PKCS#12... Os certificados podem ser importados directamente a partir da interface do usuário. Capacidade para configurar um Certificado diferente por túnel. • Suporte do Método de Autenticação Hybrid.
Dead Peer Detection (DPD)	DPD é uma extensão da Internet Key Exchange (IKE) (i.e. RFC3706) para detectar uma ponta IKE morta.
Redundant Gateway	Redundant Gateway permite oferecer aos utilizadores distantes uma conexão segura e extremamente fiável a rede da empresa. A funcionalidade Redundant Gateway permite ao Cliente VPN TheGreenBow abrir um túnel IPSec com uma gateway alternativa no caso de a principal ter caído ou não responder.
Mode Config	"Mode Config" é uma extensão da Internet Key Exchange (IKE) que permite receber da gateway VPN IPSec a configuração LAN para o computador do utilizador distante (i.e. Cliente VPN IPSec). Com Config-Mode o utilizador pode resolver todos os servidores da rede distante usando os respectivos nomes de rede (ex: //myserver/ marketing/budget) em vez dos seus endereços IP.
Pen USB	As configurações VPN e os elementos sensíveis (certificados, preshared key,…) podem ser guardados numa Pen USB afim de remover as informações sensíveis (ex: autenticação) do computador. Pode abrir e fechar automaticamente os túneis VPN com o plugin/plugoff da Pen USB.
Smart Card e Token USB	O Cliente VPN IPSec TheGreenBow consegue ler os Certificados de uma Smart Cards para explorar os cartões electrónicos

	existentes das empresas ou dos empregados que contêm certificados digitais.
Consola de Log	Todas as mensagens de fase são registradas para facilitar os testes e ver as fases do processo.
Interface do Utilizador flexível	A instalação silenciosa e a interface gráfica invisível permite aos administradores de TI distribuir a solução impedindo qualquer mudança indevida da configuração pelo utilizador. O Painel de Conexão simples e o Painel de Configuração VPN podem estar disponíveis aos utilizadores de forma separada com Acesso Controlado. Drag & drop de Configurações VPN no Cliente VPN IPSec. Varios atalhos de teclado para facilitar a utilização do Cliente VPN IPSec
Scripts	Scripts ou aplicações podem ser lançados automáticamente em diversos eventos (ex.. antes e depois da abertura dos túneis, antes e depois do encerramento dos túneis).
Gestão da Configuração	Interface do Utilizador e Linhas de Comando. Ficheiro de Configuração VPN protegido por password. Ficheiro de configuração VPN específico pode ser prestado dentro da instalação. Configuração VPN embutida para testar com os servidores TheGreenBow online.
Live update	Capacidade para verificar a existência de actualização online.
Licenças	Licenças definitivas, temporarias ou por versão do software estão disponíveis

1.6 OEM e Customização do Software

A nossa oferta é especialmente dirigido para Cliente OEM ou Integradores de Sistemas VPN. Fornecemos um solução Cliente VPN totalemente funcionale para asim completar as suas ofertas existentes. O Nosso >%PRODUCT%> pode ser rebranded ou seja pode ser customizado para a sua empresa.

Parte II

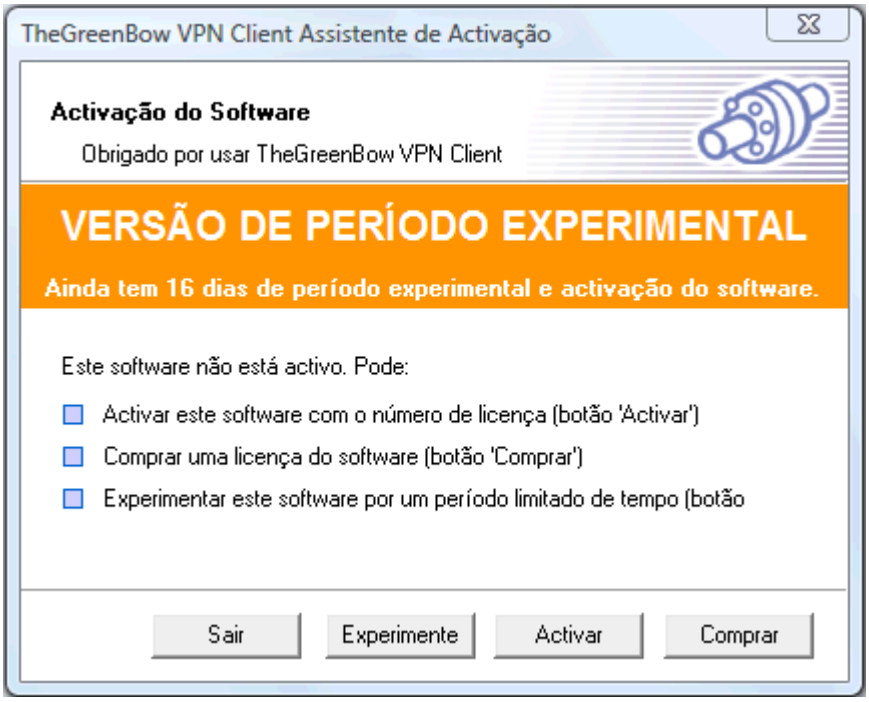
Instalar o Cliente VPN IPSec TheGreenBow

2 Instalar o Cliente VPN IPSec TheGreenBow

2.1 Instalação do Software

A instalação do Cliente VPN TheGreenBow é uma instalação clássica no Windows que não requer informações especificas. Depois de completar a instalação será lhe pedido para reiniciar o seu computador.
Depois de reiniciar e de fazer o login aparecerá uma janela com as seguintes opções:

- "Sair' fecha a janela e o software.
- "Experimente' permite -lhe continuar a versão experimental do software. O período experimental restante poderá ser visualizado na barra laranja.
- "Activar' permite-lhe activar o software online. Isso requer o número de licença. Quando clicar no botão "Activar", iniciará um Assistente de activação.
- "Comprar' permite -lhe ir directamente comprar licenças do Software TheGreenBow na loja online.



Atenção: No Windows 2000, XP e Vista, precisa de ter os direitos de administrador. Se não for o caso, a instalação para depois de ter escolhido a língua com uma mensagem de erro.

Atalhos: Depois da instalação do software, pode iniciar o cliente VPN TheGreenBow :

- desde o ambiente de trabalho, clicando duas vezes no atalho do VPN TheGreenBow
- desde o ícone disponível na barra de tarefas Cliente VPN
- do menu Iniciar > Programas > TheGreenBow > TheGreenBow VPN > TheGreenBow Cliente VPN

Nota: A instalação do software pode ser personalizada com vários parâmetros de opções em linha de comando. Para mais detalhes por favor veja o documento "Guia de distribuição" disponível na nossa página web.

2.1.1 Direitos de acesso

Um utilizador pode ter direitos de acesso restritos no windows de um computador. Veja na tabela o que os utilizadores podem ter acesso:

Acções	Admin	User
Instalação Software	yes	no
Activação Software	yes	yes
Uso Software	yes	yes

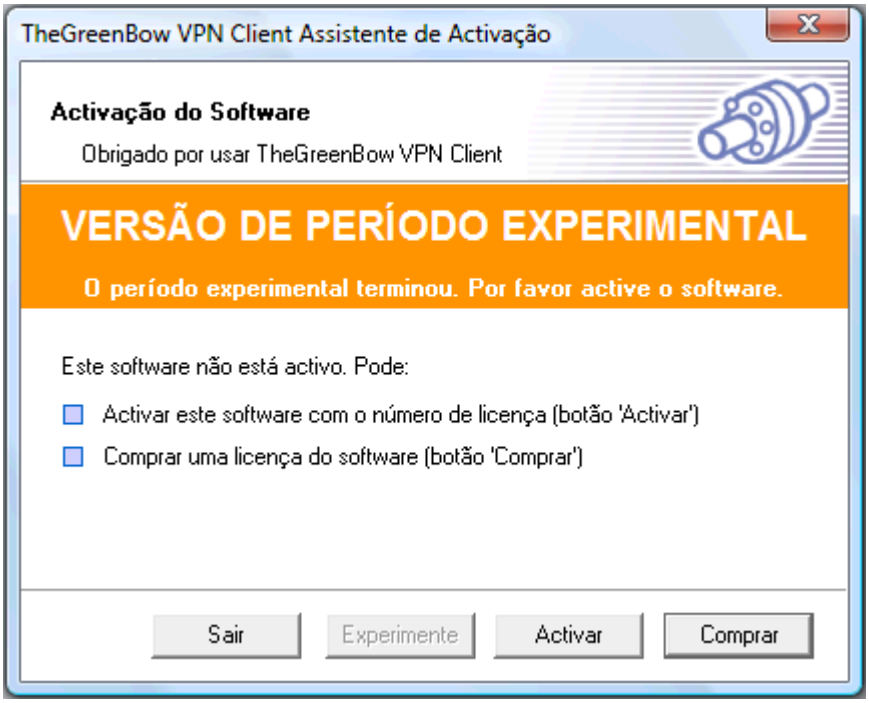
Para facilitar, o Cliente VPN IPSec TheGreenBow cria novas regras na Firewall do Windows Vista Firewall assim o tráfico VPN IPSec traffic é permitido. Veja as regras da Firewall Windows Vista:

nome da regra Vista Firewall	Acção
tgbphase1	autorizar UDP 500
tgbphase2	autorizar UDP 4500

2.2 Avaliação Software

É possível usar Cliente VPN IPSec TheGreenBow durante o período experimental (i.e. limitado a 30 dias) clicando no botão de "Avaliação". Quando o Cliente VPN IPSec está no modo de " Avaliação", a janela de registo aparece em cada iniciação do Cliente VPN IPSec.O período de experimental restante pode ser visualizado na barra laranja.

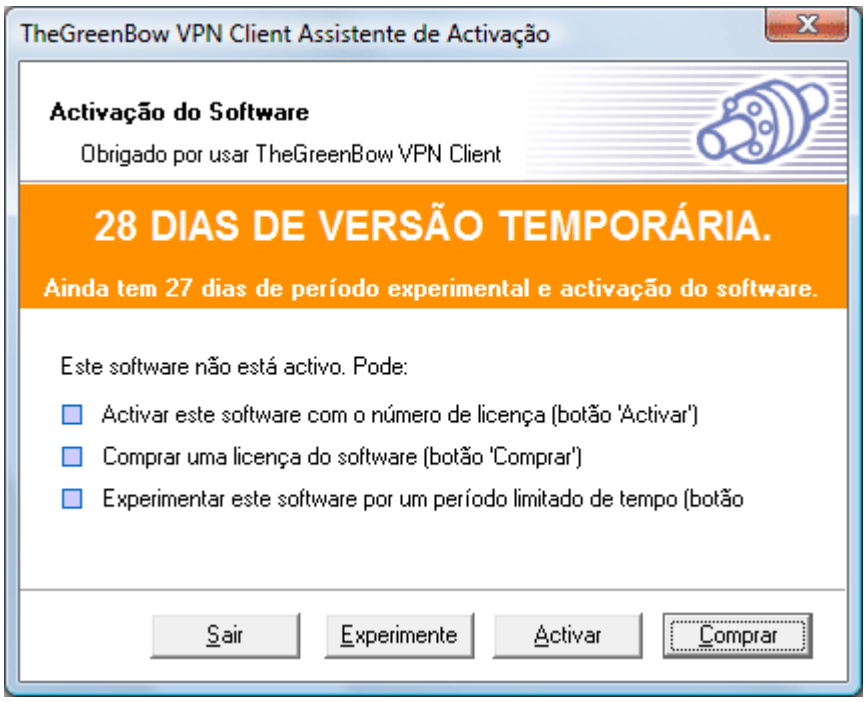
Depois do período experimental expirar, o botão de "Avaliação" não está mais disponível e o software é desactivado.



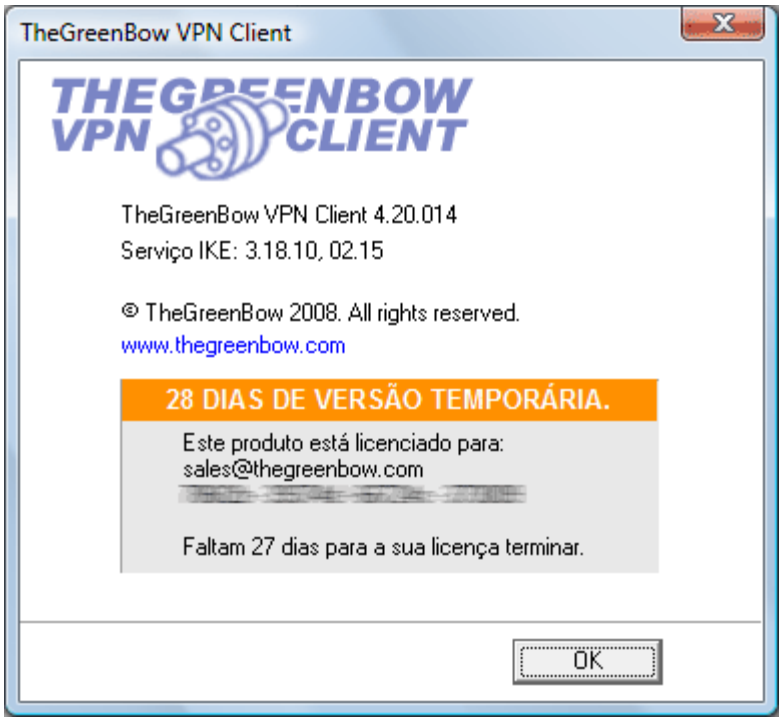
2.3 Licença de Software temporária

Um número de licença software temporária pode ser dada, para testar. O período de validade é entre 1 e 35 semanas. Para receber um número de licença software temporário, pode contactar a nossa equipa comercial: sales@thegreenbow.pt.

O período de validade do número de licença do software temporária e o período de uso são mostrados na primeira janela do Cliente VPN IPSec.
No fim do período de avaliação o software não pode ser iniciado.



Durante o tempo de utilização do número de lincença de software temporário, a janela de activação está disponível no Painel de Configurações. Permite assim ao utilizador activar uma nova licença, por exemplo uma licença definitiva de software em vez de uma temporária.
Durante esse período, a visualização do tempo restante está disponível no menu 'Sobre' como se segue no quadro:



Quando o número de Licença de Software Temporário expira, o botão de " Avaliação"é desactivado. O utilizador pode Comprar e Activar a licença definitiva de software.

2.4 Activação do Software

2.4.1 Assistente de Activação do Software

Para usar depois do período de avaliação,o software Cliente VPN IPSec TheGreenBow tem de estar activado no seu computador. Para usar o número de licença num novo computador, precisa de desintalar o software do antigo computador, a desactivação será feita automaticamente. A Activação do Software é um processo em duas etapas que requer o número de licença e um endereço de email.

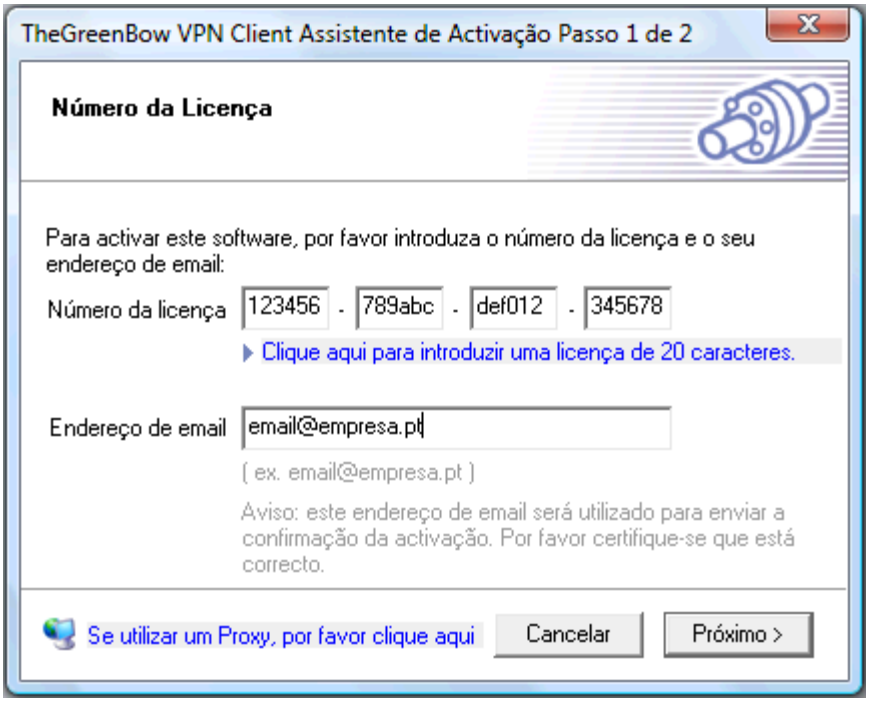
O 'Assistente de Activação' pode ser lançado do software Cliente VPN como o seguinte:

- Clique no botão 'Activar' na janela inicial quando começar o Cliente VPN.
- Clique no menu 'Ajuda' e depois clique "Assistente de Activação...".

2.4.2 Etapa 1de 2: Colocar o Número de Licença

Software de Activação requer um Número de Licença.

Coloque o seu Número de Licença, o seu endereço de email e clique "Seguinte" como é demonstrado no quadro:



Aviso: Se tem um Número de Licença com 20 caracteres, clique na opção " Clique aqui para introduzir uma licença de 20 caracteres" para poder coloca- la no campo indicado.

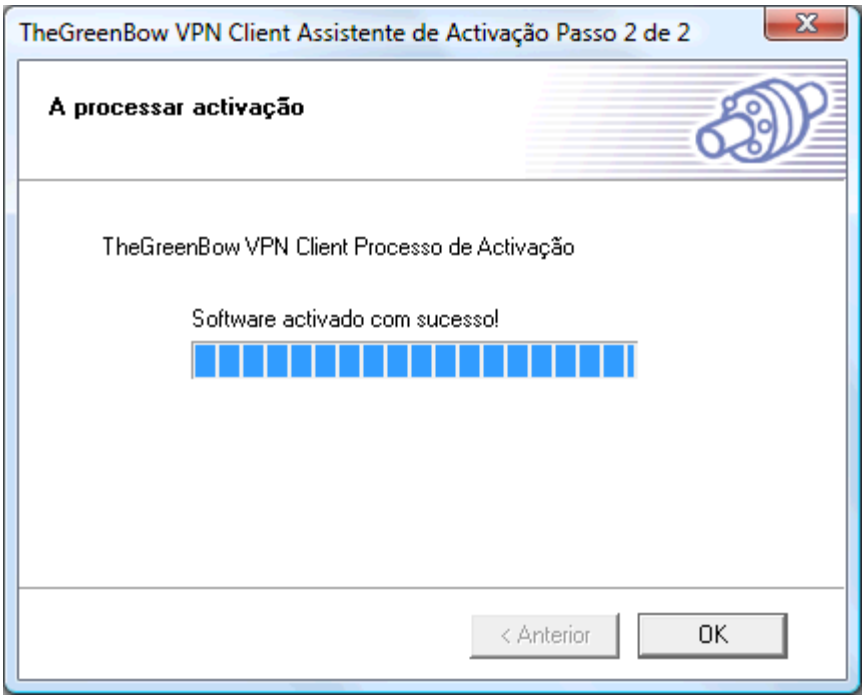
Nota: Atenção se o seu endereço de email está correcto porque será usado para mandar a confirmação da activação.

Nota: O endereço de email pode não ser pedido: Administradores IT podem configurar o valor na instalação, assim não será exibido pelo Assistente de Activação do Software. Esta funcionalidade pode ser usada para centralizar todos os emails de confirmação de Activação do Software num único endereço de email.

2.4.3 Etapa 2 de 2: Activação Online

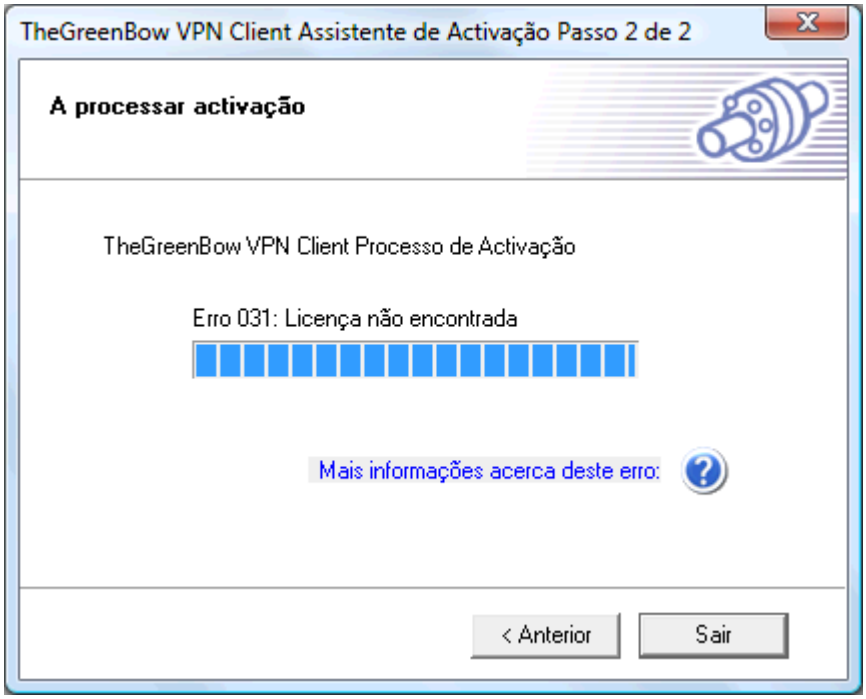
O 'Assistente de Activação' conecta automaticamente ao servidor de activação online para activar o software Cliente VPN. Pode voltar atrás a qualquer momento para mudar o Número de Licença.

O 'Assistente de Activação' terminará com uma Activação bem sucedida.



2.4.4 Problemas de Activação

Podem ocorrer erros durante o processo de activação. Cada erro de activação está sumariamente explicado na etapa 2 da Activação Online. Pode aceder online a todas explicações e recomendações de como solucionar o problema clicando no campo " Mais informações acerca deste erro" situado em baixo da barra do progresso.



A maior parte dos erros resolvem-se verificando os seguintes pontos:

1. Verifique que introduziu o correcto Número de Licença (error 031).
2. A comunicação com o nosso servidor online de activação pode estar filtrada por um proxy (error 053 or error 054). Pode configurar o proxy na etapa 1 no Assistente de Activação do Software clicando no link em baixo na janela.
3. A comunicação com o nosso servidor online de activação pode estar filtrada por uma firewall (error 053 or error 054). Verifique se a sua firewall pessoal ou a da empresa está filtrando as comunicações.
4. O nosso servidor de activação pode estar inacessível temporariamente. Tente activar o software uns minutos depois.
5. O seu Número de Licença já está activado (error 033). Contacte a nossa equipa comercial: sales@thegreenbow.pt.

Todos os erros de activação estão detalhados online no nosso website:
www.thegreenbow.pt/help.html?subject=osa&id=001

Nota: Se não consegue activar o software apesar das anteriores recomendações, é sempre possível activar manualmente o software no nosso website: www.thegreenbow.pt/activation/osa_manual.html. Esta opção permite aos seus usuários efectuar uma activação completa e imediata do software.

2.5 Actualização do Software

Atenção: Tem de activar o software Cliente VPN depois de cada actualização do software. Demora apenas uns segundos. Consoante o contrato de manutenção, a activação da actualização pode ser rejeitada. Por favor leia atentamente as seguintes recomendações e verifique o estado actual do seu contrato clicando no menu " Ajuda" depois "Verificar actualizações" no Painel de Configuração.

O êxito da activação do software actualizado depende do seu contrato de manutenção:

1. Todas as activações e actualizações do software são permitidas no período de manutenção (que começa com a sua primeira activação).
2. Quando expira o período de activação (ou se não tem contrato de manutenção), só poderá actualizar versões de manutenções. Pode identificar as actualizações de manutenção pelo último digito da versão.

Exemplo: O meu período de manutenção expirou e a minha actual versão do programa é 3.12. Só pode actualizar as versões 3.13 al 3.19. Não pode actualizar as versões 3.20, 3.30 ou 4.00.

Se deseja estender ou subscrever o contrato de manutenção, por favor contacte com a nossa equipa de vendas: sales@thegreenbow.pt

Nota: A Configuração VPN é guardada durante a Actualização do Software e automaticamente aparecerá disponível com uma nova versão.

2.6 Desinstalação Software

Cliente VPN IPSec TheGreenBow pode ser desintalado:

- a partir do Painel de Controlo do Windows seleccionando 'Adicionar/ Remover programas'
- a partir do Menu Iniciar > Programas > TheGreenBow > VPN > 'Desinstalar Cliente VPN IPSec'

Parte

Instrucções Básicas

3 Instrucções Básicas

3.1 Como abrir um túnel VPN

Como abrir um túnel (quando a Configuração VPN já existe):
- Painel de Conexão > Abrir
- SystemTray > clique no 'Abrir xxx'
- 'Automaticamente ao detectar tráfego'
- 'Automaticamente ao ligar PEN USB'
- 'Automaticamente ao arranque do MS Windows ' (antes ou depois de logon)
- Duplo clique numa configuração VPN (ex. icone no ambiente de trabalho, anexado ao email)
- Linha de Comandos permite abrir e fechar túneis

3.2 Como resolver os problemas com túneis VPN?

Como resolver os problemas com túneis VPN ?

Para solucionar os erros de um túnel, pode recorrer aos seguintes documentos disponíveis no nosso site:
- Documento de resolução de problemas (pdf).
- Ajuda online (html).
- Ajuda sobre a activação do Software online (html).
- Use a Configuração VPN de teste para certificar a sua rede.
- FAQs do Cliente VPN.

3.3 Como importar uma Configuração VPN com simples duplo clique?

Também conhecido como 'Dial up mode': um túnel pode ser aberto com um duplo- clique na configuração VPN (i.e. ficheiro com extensão '.tgb'). Esta funcionalidade permite criar várias Configurações VPN no seu ambiente de trabalho e abrir túneis clicando no ícone de atalho de Configuração VPN.

Como criar um atalho de uma Configuração VPN no seu ambiente de trabalho:
Etapa 1: Configure o túnel no 'Painel de Configuração'
Etapa 2: Nas 'Opções Avançadas de Fase 2', configure o túnel para 'Estabelecer túnel automaticamente no inicio do Cliente VPN '
Etapa 3: Exportar a Configuração VPN para o seu ambiente de trabalho.

Nota: Pode proteger a Configuração VPN com uma senha ao exporta-la. Esta senha será pedida cada vez que clicar no túnel.

Parte IV

Navegando na Interface Utilizador

4 Navegando na Interface Utilizador

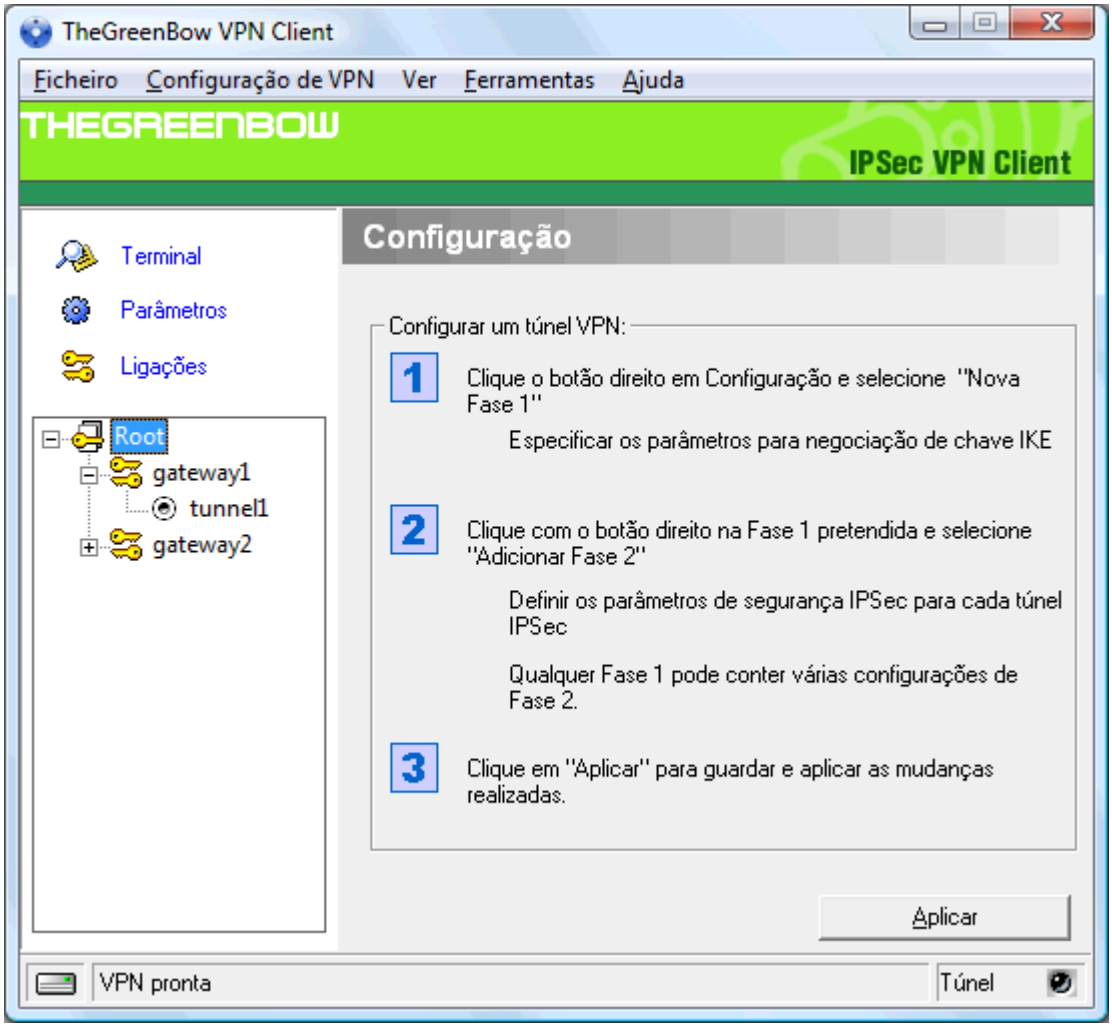
4.1 Interface do Usuário

O Cliente VPN IPSec TheGreenBow é totalmente autónomo e pode abrir e fechar túneis sem a intervenção do usuário, dependendo do tráfego para determinados destinos. Contudo isto requer uma configuração do VPN.

A configuração Cliente VPN IPSec está definida num arquivo de configuração VPN. O interface do software permite criar, modificar, guardar, exportar e importar configurações VPN com elementos de segurança (ex. Chaves Partilhadas, Certificados, ...).

O Interface do Usuário é feito de vários elementos:

- Painel de Configuração
- Painel de Conexão
- Menus Principais
- System Tray Icon & Popup
- Barra de Estado
- Assistente
- Preferências



4.2 Ícone de Barra de Ferramentas

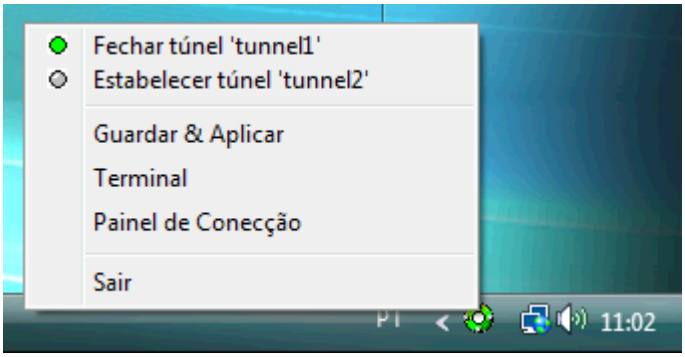
A interface do usuário Cliente VPN pode iniciar-se fazendo duplo-clique no ícone de aplicação (no ambiente de trabalho ou no Menu Iniciar) ou um simples clique no ícone da barra de ferramentas. Quando aberto o Cliente VPN mostra um ícone na barra de ferramentas que indica o estado dos túneis com uma cor.

A definição das cores do Cliente VPN é a seguinte

Ícone azul: não há nenhum túnel VPN aberto

Ícone verde: pelo menos um túnel está aberto

Um clique com o botão esquerdo no rato sobre o ícone VPN abrirá a configuraçãoda interface do usuário.



Um clique com o botão direito mostra o seguinte menu:

- "Sair' fecha os túneis VPN estabelecidos e pára a configuração da interface do usuário.
- "Salvar & Aplicar' fecha os túneis VPN estabelecidos, aplica a última modificação da configuração e abre de novo todos os túneis VPN que foram configurados para começar automaticamente.
- "Terminal' mostra a janela de registos (Console de log).
- "Painel de Conexões" abre o Painel de Conexões que permite abrir, fechar e obter informações sobre os túneis.
- Lista dos túneis configurados com o seu estado actual. Os túneis também podem ser abertos ou fechados apartir deste menu.

Uma mensagem sobre o ícone Cliente VPN mostra o estado da conexão do do túnel VPN:

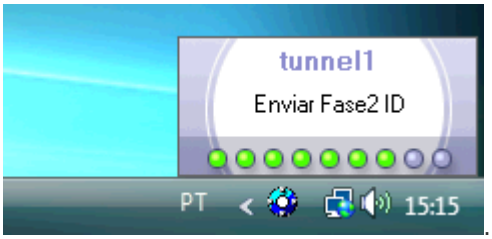
- "Túnel <nomedotunel>' quando se estabelece um ou mais túneis
- "Espere VPN pronta...' quando o serviço de IKE reinicie
- "TheGreenBow Cliente VPN' quando o Cliente VPN está funcionando sem nenhum túnel aberto.

4.3 System Tray Popup

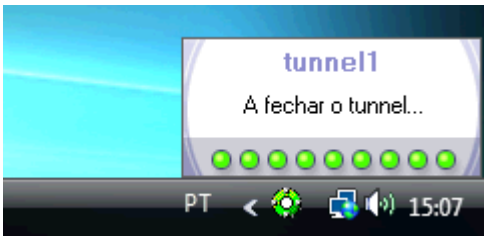
Um pequeno popup aparece cada vez que o túnel abre-se ou fecha-se.

Este pequeno popup tem um comportamento muito simples:

1. O popup mostra a abertura de túnel com diferentes fases e desaparece depois de 6 segundos a menos que o rato se mova sobre ele.



2. O popup mostra também o encerramento do túnel.



3. Caso o túnel não se abra, mostrará um aviso com um link para mais informações no nosso site.

4.4 Keyboard Shortcuts

Esta opção facilita o acesso às funcionalidades mais frequentes do programa.

Shortcut	Acção
Ctrl + Enter	Alternar entre o 'Painel Configuração' e o 'Painel Conexão'. Nota: no caso do painel de configuração estar protegido por uma senha in case, será pedida essa senha quando o utilizador tentar mudar o Painel de Configuração.
Ctrl + D	Abre a 'Consola' VPN para 'Debug' de conexão.
Ctrl + S	'Salvar & Aplicar' a configuração VPN.

4.5 Painel de Conexão

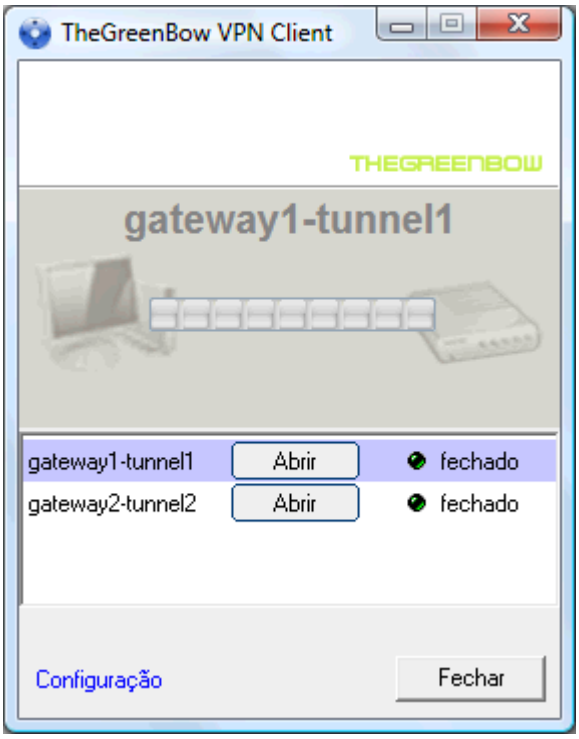
O Painel de Conexão permite aos usuários abrir, fechar e obter informação clara sobre cada túnel que foi configurado. Esta é a funcionalidade que todos os usuários finais precisam para abrir e fechar.
Esta caracteristica ajuda claramente ambos os Administradores (que configuram as conexões VPN) e os utilizadores (que apenas abram ou fechem as conexões VPN) para o seu uso próprio.

O Painel de Configuração é feito de vários elementos:

- Um diagrama animado mostra a informação do túnel (em cima)
- Uma lista de todos os túneis configurados com um botão 'abrir/fechar' (diagrama abaixo)

- Um link para o 'Painel Configuração' (botão esquerdo)

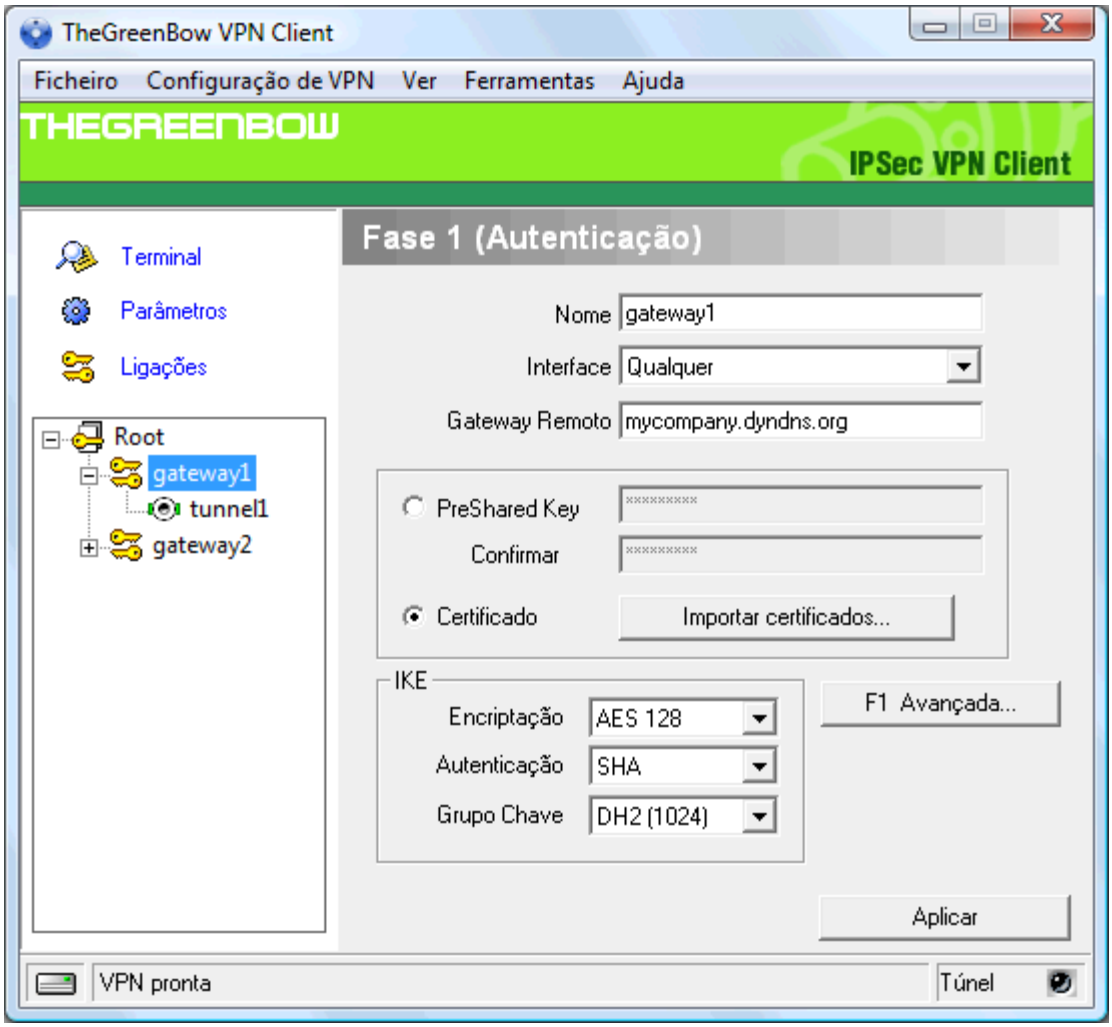
É possível alternar entre o 'Painel de Conexão' e o 'Painel de Configuração' usando o atalho 'Ctrl + Enter' (ver secção 'Atalhos').



4.6 Painel configurações

O Painel de Configuração permite criar uma Configuração VPN e é feito de vários elementos:

- Três botões 'Consola', 'Paramêtros' e 'Connexões' (coluna esquerda)
- A janela de arborescência (coluna esquerda) contem todas as configurações IKE e IPSec
- Uma janela de configuração (coluna direita) mostra o nível associado.



Pode arrastar e soltar um ficheiro de configuração VPN (i.e. extensão '.tgb') no Painel de Configurações. Esta funcionalidade permite aplicar facilmente uma nova configuração VPN. Se um túnel está configurado para "abrir-se quando o Cliente VPN iniciar' (ver secção 'Opções de Fase2 Avançada'), este abrirá imediatamente quando a configuração VPN for aplicada ('Aplicar').

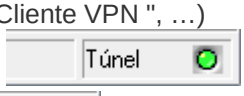
4.6.1 Menu Principal

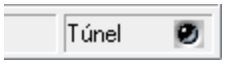
Há vários menus como os seguintes:

- O menu **'Ficheiro'** é usado para Importar ou Exportar a configuração.É também usado para escolher o local da Configuração VPN: local, USB, servidor, Token. É também usado para configurar várias opções como a maneira que o Cliente VPN deve iniciar (ex. antes ou depois do logon, ...).
- O menu **'Configuração de VPN '** contem todas as acções sobre a arborescência de configuração. O menu de 'Configuração' também dá acesso ao 'Assistente Configuração'.
- O menu **'Ver'** permite configurar ao que o utilizador pode aceder.
- O menu **'Ferramentas'** contem as opções 'Terminal', 'Ligações' e 'Reset IKE'.
- O menu **'Ajuda'** permite aceder a procurar actualizações, suporte online e a janela 'Sobre'. Também permite aceder ao 'Assistente Configuração'.

4.6.2 Barra de Estado

A barra de Estado oferece várias informações:

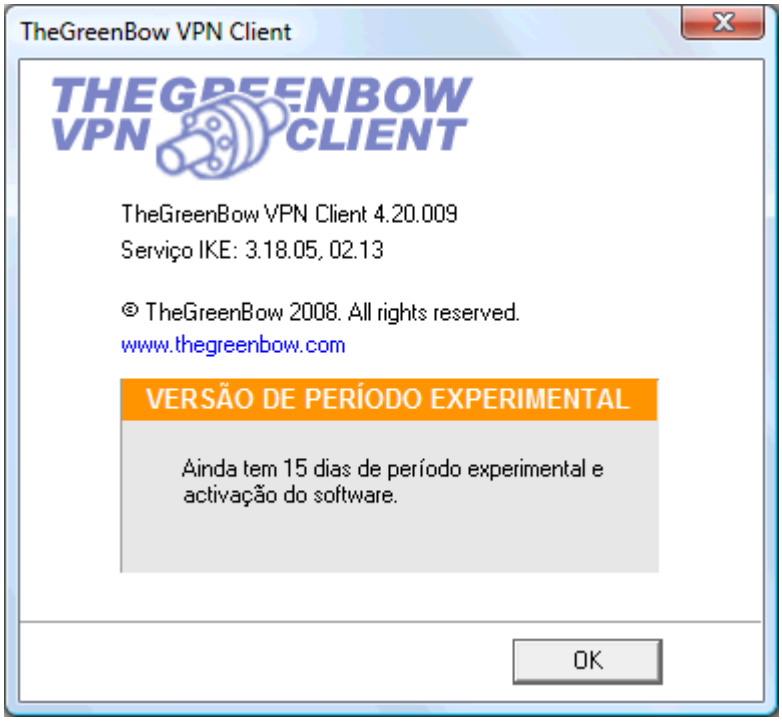
- A parte esquerda da barra indica a localização da configuração VPN. Por exemplo, se estamos em "Modo USB" , a imagem mostrará uma PEN USB, activa ou não conforme a presença de uma PEN USB VPN válida.
- A parte central da barra dá informação sobre o estado do software Cliente VPN (ex. "abrir túnel em progresso", "aplicar as configurações de VPN", "iniciando o Cliente VPN ", …)
- A luz na parte direita informa sobre o estado dos túneis (ex. Luz verde 

significa que pelo menos um túnel está aberto, luz Cinzenta 

significa que nenhum túnel está aberto.)

4.6.3 Janela Sobre

A janela "Sobre" indica a versão do software Cliente VPN e informações sobre a activação do software. Também encontrará um link do nosso web site.



4.6.4 Controlo de Acesso & Interface Oculta

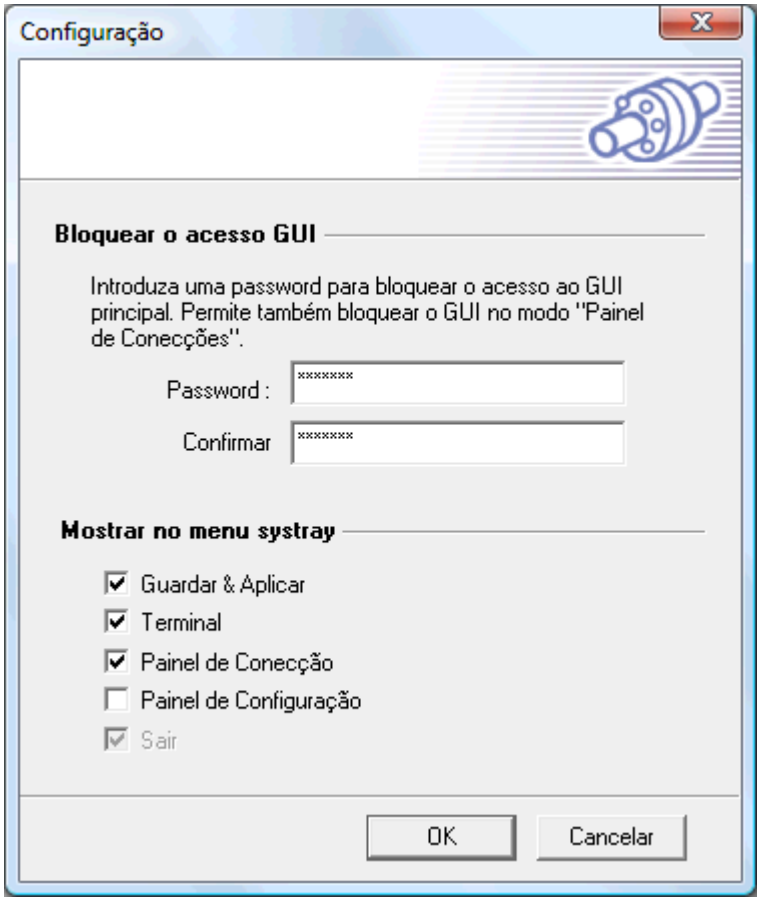
Esta funcionalidade é especialmente dedicada aos Administradores IT. Permite bloquear o acesso ao Paine de Configuração, e restringir o acesso ao Painel de Conexão do Cliente VPN IPSec com uma password. Assim, os utilizadores não podem modificar a configuração VPN evitando assim erros.

Uma vez configurado, o utilizador deverá colocar a sua senha:

1. quando clicar no ícone systray do Cliente VPN IPSec
2. quando alternar entre "Painel Conexão" para "Painel Configuração".

Esta senha pode ser configurada como opção na instalação (ver secção 'Opções de Instalação').

A janela de bloqueio de acesso está disponível no menu 'Ver > Configuraçãon' no Painel de Conexão que também permite configurar as opções do menu systray. Assim, os administradores podem restringir o software desde um acesso completo até uma interface completamente oculta.

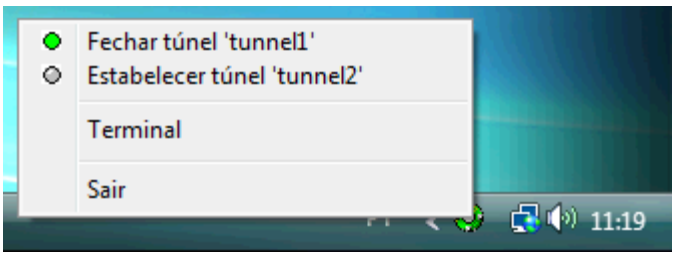


Para remover o Controlo de Acesso basta esvaziar ambos os campos 'Password' e 'Confirmar' depois clique 'OK'.

Nota:O campo 'Sair' para o menu systray está indisponível na versão standart do software. No entanto pode ser removido durante a instalação do software, através da opção do setup "`-menuitem`" (ver 'Opções de Instalação')

O controlo de acesso com password só afecta o 'Painel de Configuração'. O acesso ao 'Painel de Conexão' não se pode controlar com password.

No caso de controlo de acesso estar activado, o 'Painel de Configuração' não pode ser aberto nem por duplo clique no ícone do ambiente do trabalho, nem pelo menu iniciar. Clique direito no ícone na barra de tarefas restringe o acesso à "Terminal", deixando o software, e abrindo/ fechando os túneis configurados:



4.6.5 Assistentes

Há dois Assistentes disponíveis:

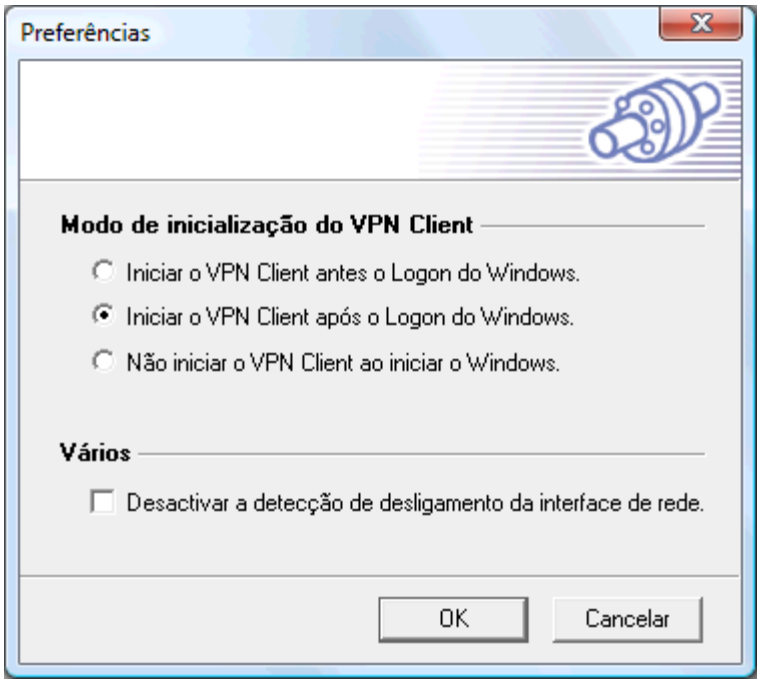
- Assistente de Configuração VPN pode ser lançado do menu 'Configuração de VPN' > 'Assistente Configuração'.
- Assistente de Activação do Software pode ser lançado do menu 'Ajuda' > 'Assistente de Activação'.

4.6.6 Preferências

A janela 'Preferências' permite definir:

- O modo de inicio do programa. Pode configurar os diferentes modos durante a instalação (ver secção 'Opção Instalação').
- Permitir/Não permitir a detecção da desconexão da interface

As Preferências estão disponíveis no Menu 'Ficheiro' fazendo clique 'Preferências'.



Modo de inicialização do Cliente VPN
Cliente VPN IPSec TheGreenBow dispõe de diferentes modos de inicio, tais como:

- Iniciar Cliente VPN IPSec antes do logon MS Windows: este modo pode ser usado para assegurar um inicio de de sessão remoto
- Start Cliente VPN IPSec depois de logon MS Windows
- Não iniciar Cliente VPN IPSec quando começa MS Windows: Cliente VPN IPSec inicia-se manualmente pelo usuário (modo "manual")

Diversos
Não deixar a detecção da desconexão da interface permite que o Cliente VPN IPSec mantenha os túneis abertos enquanto o interface se desconecta momentaneamente mas não muitas vezes. Este tipo de comportamento ocorre quando a interface que se utiliza para abrir túneis é instável como WiFi, GPRS e todos interfaces 3G.

Parte V

Painel de Conexão

5 Painel de Conexão

5.1 Base do Painel de Conexão

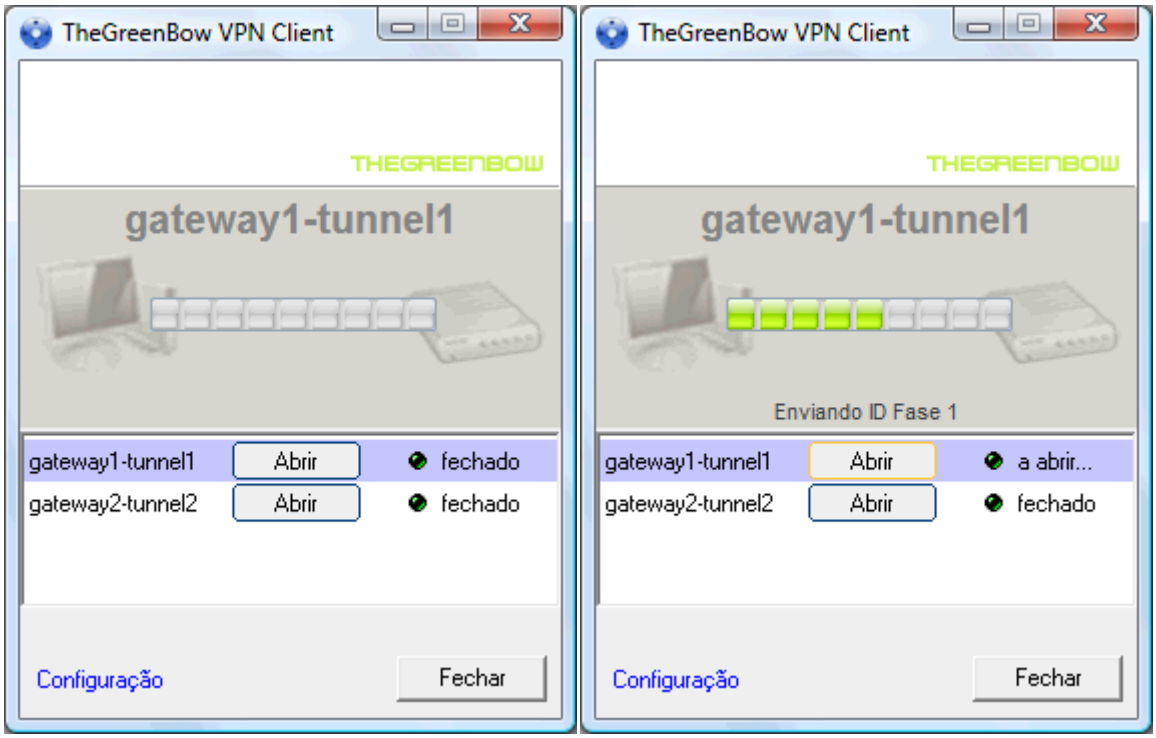
O Painel de Conexão permite aos utilizadores abrir, fechar e obter uma clara informação sobre cada um dos túneis configurados. Esta é a funcionalidade que todos os usuários finais precisam para abrir e fechar.

O Painel de Configuração é feito de vários elementos:

- Um diagrama animado mostra a informação do túnel (em cima)
- Uma lista de todos os túneis configurados com um botão 'abrir/fechar' (diagrama abaixo)

Para abrir um túnel o usuário tem de fazer simplesmente um clique no botão " Abrir". O botão " Abrir" modifica automaticamente para " Fechar" quando o túnel tiver aberto. Um clique no nome do túnel abre automaticamente o "Painel Configuração", que permite modificar a configuração do túnel. Esta opção não é permitida quando o Painel de Controlo é protegido por uma password (ver secção 'Controlo Acesso').

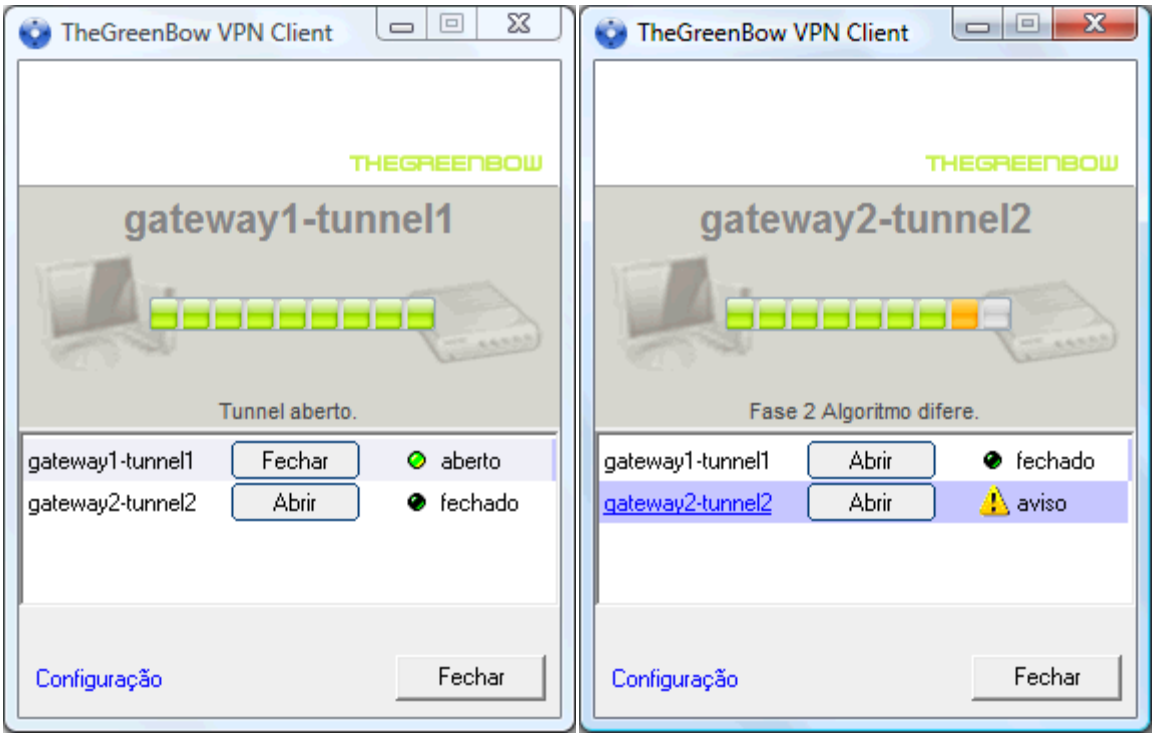
É possível alternar entre 'Painel de Conexão' e o 'Painel Configuraçãol' usando o atalho 'Ctrl + Enter' (ver secção 'Atalhos').



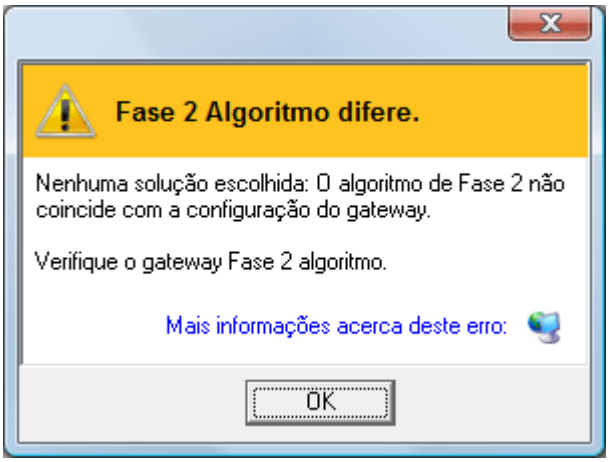
Também é possível aplicar automaticamente uma nova Configuração VPN ao fazer um drag & drop de uma Configuração VPN no Painel de Conexão. Se o túnel está configurado para abrir-se automaticamente quando o Cliente VPN inicie (ver secção 'Parâmetros Avançados de Fase2'), este será aberto imediatamente.

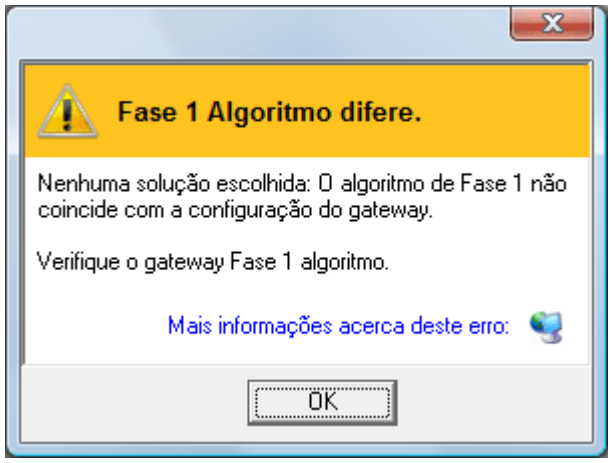
5.2 Mais info sobre Conexões

Se ocorrer um problema durante o processo da abertura do túnel, aparecerá um aviso à direita da lista do túnel.



Fazendo clique no aviso abre-se automaticamente uma janela que mostra o problema de maneira detalhada. Os popups de aviso ajudam aos usuários como aos administradores a identificar o problema. Estes popups também o colocam em contacto com as nossas páginas web de ajuda online (seleccionando "mais informações"), que detalham os erros e propõem soluções possíveis.





Parte VI

Painel de Configuração

6 Painel de Configuração

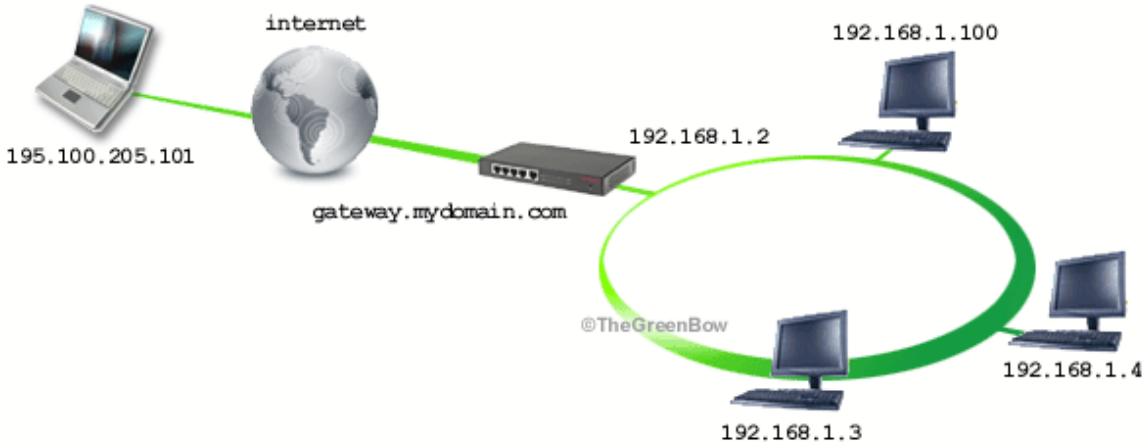
6.1 Assistente de Configuração

6.1.1 Assistente de Configuração em três etapas

O Cliente VPN IPSec TheGreenBow dispõe de um Assistente de Configuração que permite criar uma configuração VPN em três etapas fáceis. Este Assistente de Configuração é designado para computadores remotos que precisam de conectar-se à LAN da empresa através da gateway VPN, ou para fazer uma VPN peer to peer.

Observemos o seguinte exemplo:

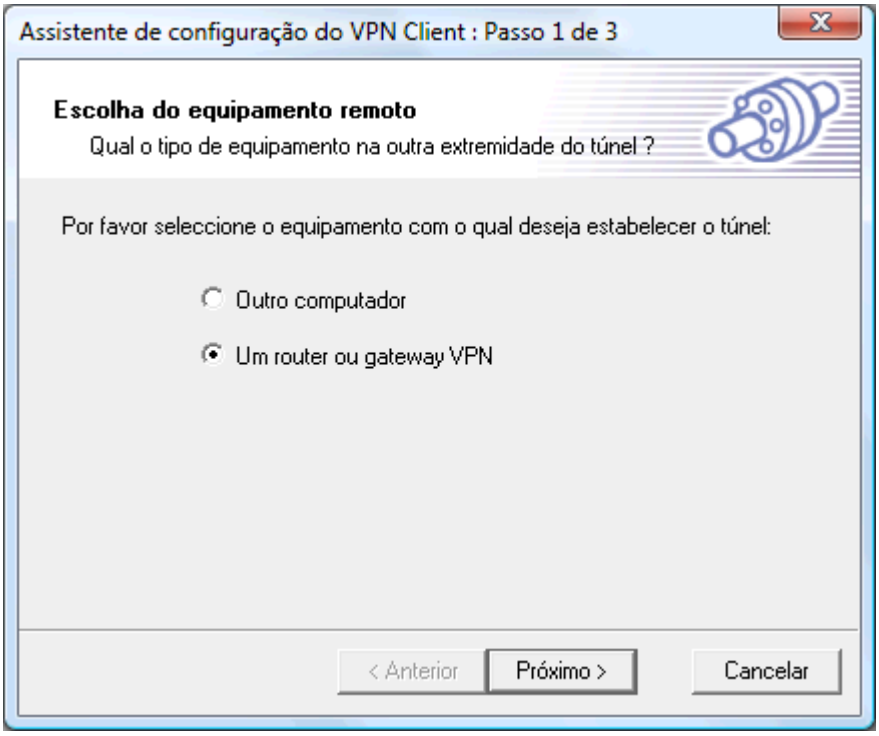
- O computador remoto tem um endereço IP público dinâmico.
- Tenta conectar-se à LAN corporativa atrás de uma router VPN que tem como endereço DNS "gateway.mydomain.com".
- Os endereços da LAN corporativa são 192.168.1.xxx. ex. o computador distante quer alcançar um servidor com um endereço IP: 192.168.1.100.



Para configurar esta conexão, abra a janela do assistente seleccionando o menu "Configuração de VPN > Assistente de Configuração"

6.1.2 Etapa 1 de 3: Escolha do equipamento distante

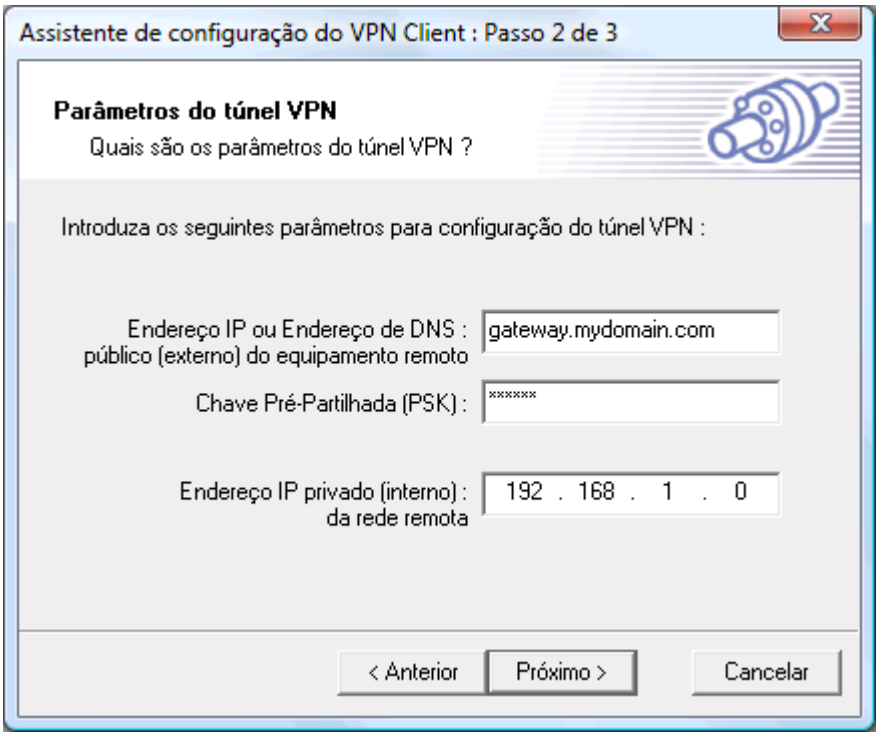
Deve especificar o tipo de equipamento que está no fim do túnel: Gateway VPN.



6.1.3 Etapa 2 de 3: Parâmetros do túnel VPN

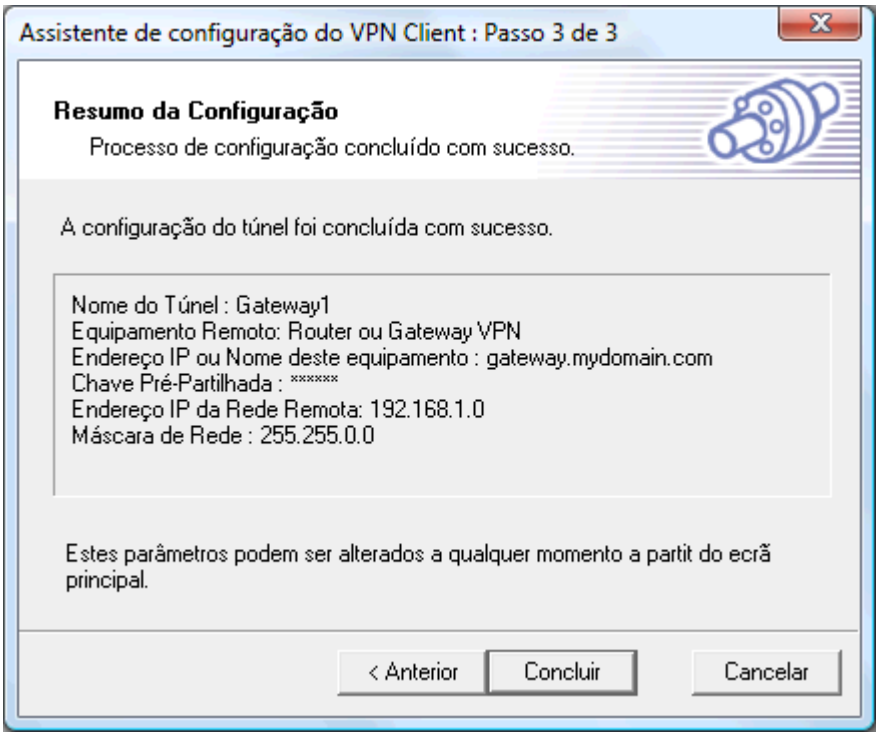
Deve especificar a seguinte informação:

- O endereço público (lado WAN) da Gateway remota
- A Chave Pre- partilhada (PSK) que será utilizada para este túnel (essa chave deve ser a mesma que a da gateway)
- O endereço IP da rede LAN da empresa (ex.192.168.1.0)



6.1.4 Etapa 3 de 3: Sumário

A terceira etapa resume a sua nova configuração VPN. Pode configurar outros parâmetros através do 'Painel Configuração' (ex. Certificados, um endereço IP virtual, etc..).

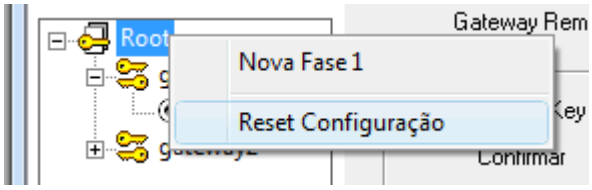


6.2 Configuração do Túnel VPN

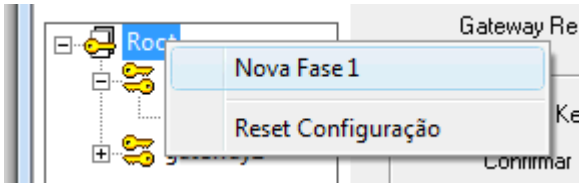
6.2.1 Como criar um túnel VPN?

Para criar um túnel VPN desde o Painel de Configuração (sem usar Assistente de Configuração), deverá seguir as seguintes etapas:

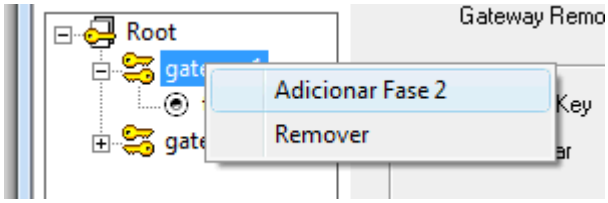
1. Reset o Painel de Configuração para eliminar qualquer configuração anterior.



2. Faça clique direito em " Root" na arborescência e seleccione 'Nova Fase 1'.



3. Configure a Fase de Autenticação (Fase 1).
4. Faça clique direito na ' nova Fase 1' na arborescência e seleccione 'adicionar Fase 2'.



5. Configure a Fase IPSec (Fase 2).
6. Uma vez que os parâmetros estejam configurados clique em 'Aplicar' para ter em conta a nova configuração. Assim o servio IKE funcionará com os novos parâmetros.
7. Clique em 'Estabelecer Túnel' para abrir um túnel VPN IPSec (só na janela " Configuração IPSec").

Por favor refira -se à Fase 1 e Fase 2 para mais descrições dos parâmetros.

6.2.2 Fases Autenticação ou Configuração IPSec Múltiplas

Várias fases de autenticação (Fase1) podem ser configuradas. Assim um computador pode estabelecer conexões VPN IPSec VPN com vários routers VPN ou outros computadores (peer to peer).

Da mesma forma, várias Configurações IPSec (Fase 2) podem ser criadas para a mesma Fase de Autenticação (Fase 1).

6.2.3 Opções Avançadas

Opções avançadas podem ser definidas para as Fase 1 e Fase 2.

As definições da Fase 1 serão aplicadas a todas as Fases 2 de configuração VPN usada:

- Activar/Desactivar Config-Mode
- Activar/Desactivar Modo Agressivo
- Activar/Desactivar Redundant Gateway
- Seleccionar o NAT-T mode (Forçar, Desligar, automático)
- Define X-Auth Login/password com opção popup

As definições da Fase 2 só se aplicam à Fase associada:

- Modo de Estabelecimento Automático
- Escolher Script/Applicações a executar na abertura do túnel
- Endereços dos servidores DNS/WINS distantes

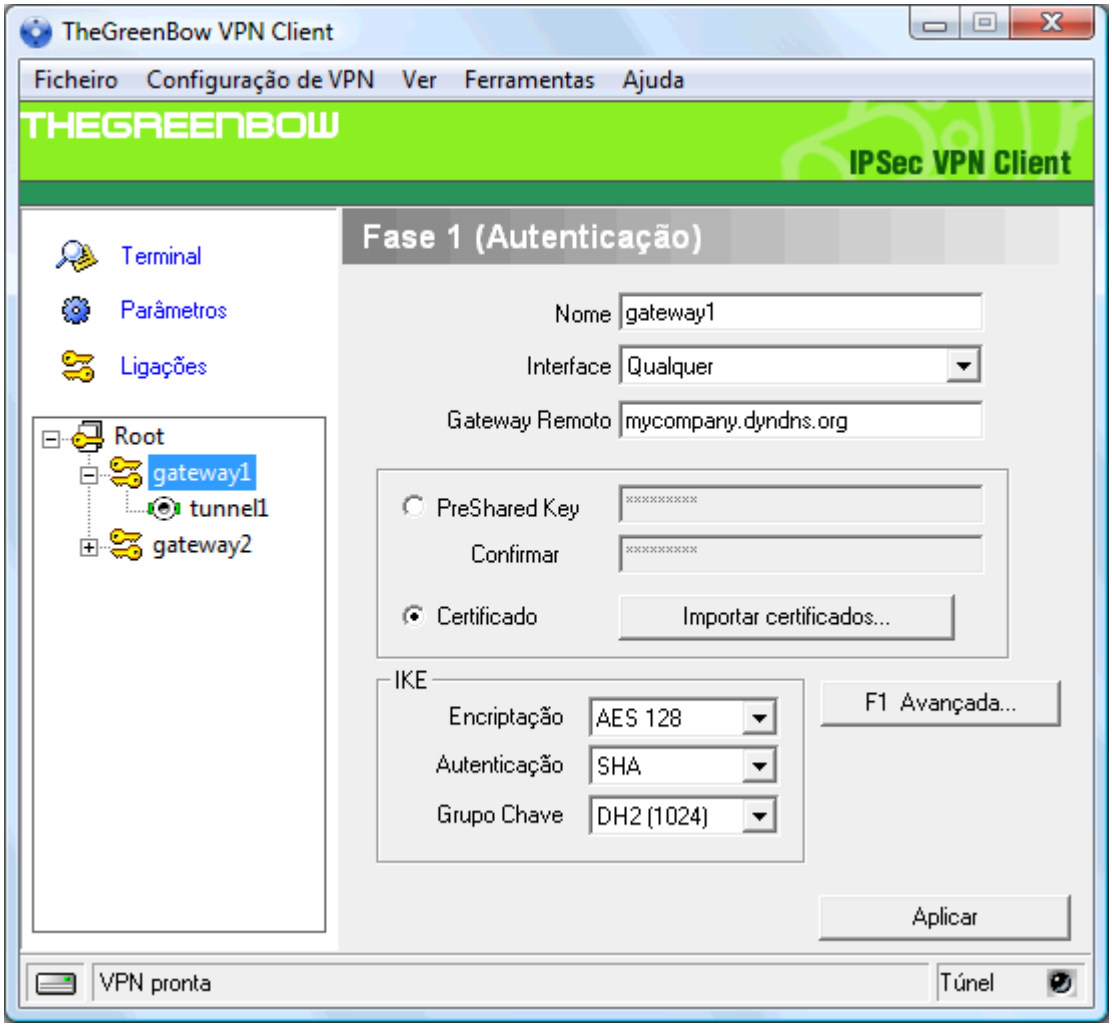
6.3 Autenticação ou Fase 1

6.3.1 O que é a Fase 1?

A janela Fase 1 ou 'Autenticação' é sobre os parâmetros para a Fase de Autenticação ou Fase 1 que também é conhecido como Fase de Negociação IKE.

O objectivo da Fase 1 é de negociar os parâmetros de Segurança IKE, de autenticar os pontos, e de estabelecer um canal seguro entre as extremidades. Como parte da Fase 1, cada extremidade deve identificar e autenticar-se para o outro.

6.3.2 Descrição dos Parâmetros de Fase 1

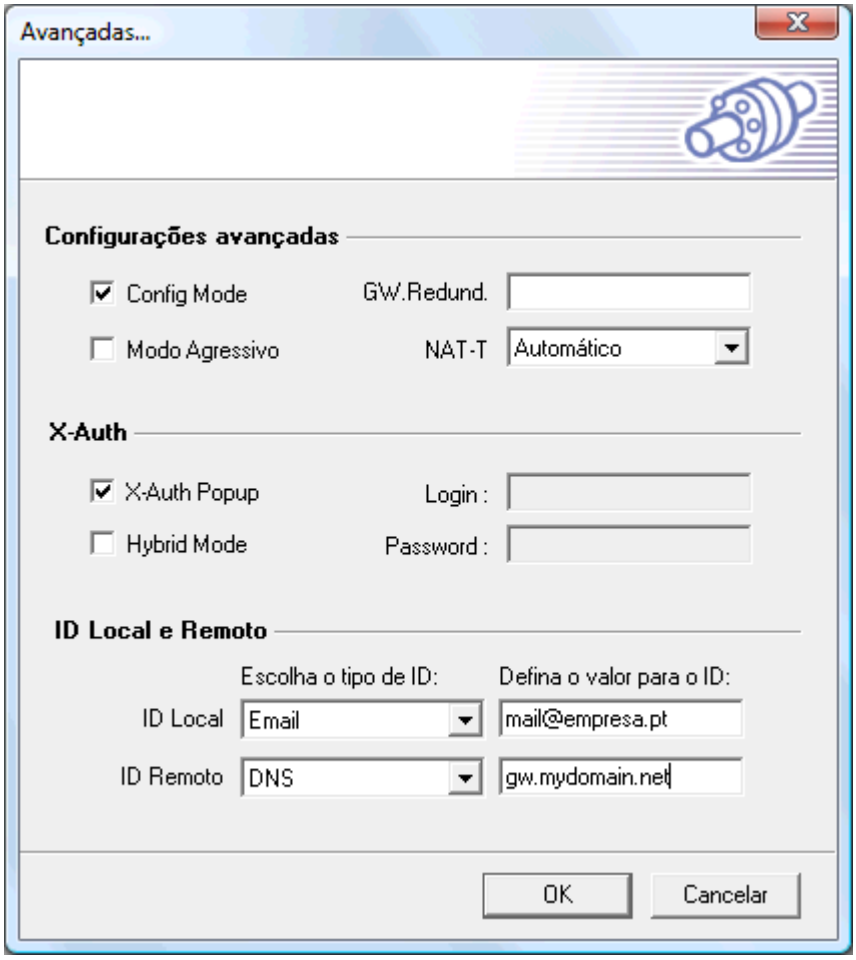


Nome	Etiqueta para a Fase de Autenticação usado só para a configuração da Interface do Usuário. Este valor nunca é usado na negociação IKE. É possível mudar o nome a qualquer momento e lê-lo na arborescência. Duas Fases 1 não podem ter o mesmo nome.
Interface	Endereço IP da interface de rede do computador, através da qual a conexão VPN é estabelecida. Se o endereço IP pode mudar (com uma conexão dinâmica de um ISP por exemplo) seleccione "Qualquer".
Gateway Remoto	Endereço IP ou Endereço DNS da gateway remota (no nosso exemplo: mycompany.dyndns.org). **Este campo é obrigatório**.
Pre-shared key	Password ou chave partilhada com a gateway remota.
Certificado	Certificado X509 usado por o Cliente VPN. Clique em 'Importar certificados...' para selecionar a origem do certificado: ficheiro PEM, ficheiro PKCS#12 ou SmartCard (ver secção Como configurar Certificados). Um Certificado por túnel pode ser configurado.
Encriptação IKE	Algoritmo de Encriptação usado na Fase de Autenticação (3DES, AES, ...).
Autenticação IKE	Algoritmo de Autenticação usado na Fase de Autenticação (MD5, SHA, ...).
Grupo Chave IKE	Tamanho da Chave Diffie-Hellman.

Para mais parâmetros avançados, clique em 'F1 Avançada'.

6.3.3 Descrição dos Parâmetros Avançados de Fase 1

Para funcionalidades e parâmetros avançados, clique no botão 'F1 Avançada' no Painel da Fase 1.



Config-Mode Se seleccionado, o Cliente VPN ira activar o Config-Mode para este túnel. Config-Mode permite ao Cliente VPN recuperar algumas informações da Configuração VPN desde a Gateway VPN. Se o Config-Mode está activado e suportado na Gateway VPN , os seguintes parâmetros serão negociados entre o Cliente VPN e a Gateway remota durante a negociação IKE (Fase 1):

- Endereço IP Virtual do Cliente VPN
- Endereço do Servidor DNS (opcional)
- Endereço do Servidor WINS server (opcional)

No caso em que o Config-Mode não esteja disponível na gateway remota, poderá nos parâmetros de 'Fase 2 Avançada' configurar manualmente os endereços dos Servidores DNS e WINS no Cliente VPN IPSec.

Modo Agressivo Se seleccionado, o Cliente VPN usará o modo agressivo como modo de negociação com a gateway remota.

GW. Redund. Permite ao Cliente VPN abrir um túnel IPSec com uma gateway alternativa no caso em que a primeira gateway caiu ou não respondeu. Tanto pode Colocar o endereço IP ou a url da Gateway Redundante (ex.: router. dyndns.com).

- O Cliente VPN TheGreenBow entrará em contacto com a primeira gateway para estabelecer o túnel. Se não conseguir depois de várias tentativas (por defeito são 5 vezes, configurável no Painel "Parâmetros " > campo "Retransmissões") a Gateway Redundante será usada como extremidade para o túnel VPN. Intervalo entre duas tentativas é de 10 segundos.
- No caso em que a primeira gateway responde mas o estabelecimento do túnel falha (ex.: problema de configuração VPN) então o Cliente VPN não tentará abrir um túnel com a Gateway Redundante. Deverá então modificar a Configuração VPN.
- Se um túnel foi estabelecido com êxito com a primeira gateway com a funcionalidade DPD (i.e. Dead Peer Detection) negociadas nos dois lados, quando a primeira gateway deixa de responder (ex.: DPD detecta gateway remota que não responde) o Cliente VPN abrirá imediatamente um novo túnel com a Gateway Redundante.
- O mesmo comportamento será aplicado com a gateway redundante. Isto quer dizer que o Cliente VPN tentará abrir a gateway principal ou a redundante até que o utilizador feche o software ou clique em "Aplicar'.

Modo NAT-T

O modo NAT-T pode ser forçado, desligado automático.
"Desligar" NAT-T impede o Cliente VPN IPSec e a gateway VPN de iniciar NAT-Traversal.
O modo NAT-T "Automático" deixa a gateway VPN Gateway e Cliente VPN negociar o NAT-Traversal.
Com o modo "Forçar" NAT-T, o Cliente VPN IPSec TheGreenBow forçará o NAT-T a fazer um encapsulamento UDP dos pacotes IPSec para resolver os problemas com os routers NAT intermediários.

ID Local

ID Local é a identificação que o Cliente VPN enviará à gateway VPN na Fase 1. Esta identidade pode ser:

- Um endereço IP (tipo = Endereço IP), por exemplo: 195.100.205.101
- Um nome de domínio (tipo = DNS), ex. mydomain.com
- Um endereço de email (tipo = Email), ex. support@thegreenbow.pt
- Uma sequência (tipo = ID da Chave), ex. 123456
- Um certificado (tipo=DER ASN1 DN) (veja a Configuração dos Certificados) Se essa identidade não é fornecida,o endereço IP do Cliente VPN será usado.

ID Remoto

O ID Remoto é a identificação que o Cliente VPN está à espera de receber da gateway VPN durante a Fase 1. Esta identidade pode ser:

- Um endereço IP (tipo = Endereço IP), por exemplo: 80.2.3.4
- Um nome de domínio (tipo = DNS), ex. gateway.mydomain.com
- Um endereço email (tipo = Email), ex. admin@mydomain.com
- Um certificado (tipo = ID Chave), ex. 123456
- Um certificado (tipo=DER ASN1 DN) (veja a Configuração dos Certificados) Se essa identidade não é fornecida, o endereço IP da gateway será usado.

X-Auth

Defina o login e a senha para a negociação IPSec X-Auth. Se "X-Auth popup" está seleccionada, uma janela popup pedirá o login e a senha cada vez que a autenticação é necessária para abrir um túnel com a gateway remota. O utilizador final tem 60 segundos (i.e. defeito) para colocar o seu login e password antes que a autenticação X-Auth falhe.
Se a autenticação X-Auth falha o estabelecimento do túnel também.

Modo Hybrid Autenticação

O modo Hybrid é um método de autenticação específico usado na Fase 1 IKE. Este método assume uma assimetria entre as entidades autenticadas. Uma entidade autentifica usando técnicas de chave pública enquanto a outra entidade autentifica usando técnicas de "Challenge response". Este método de autenticação é usado para estabelecer, no fim da Fase1, uma SA IKE com autenticação unidireccional.
Para que este IKE seja autenticado bi-direccionalmente, a Fase 1 é seguida imediatamente por uma negociação X-Auth [XAUTH]. A negociação X-Auth é usada para autenticar o utilizador remoto. O uso

deste método de autenticação é denominado modo de autenticação Hybrid. O Cliente VPN IPSec TheGreenBow implementa a RFC 'draft-ietf-ipsec-isakmp-hybrid-auth-05.txt'.

6.3.4 Mudar a duração Popup X- Auth

É possível modificar o tempo de visualização da janela X-Auth. O valor por defeito é de 60 segundos. Em alguns casos,pode ser interessante aumentar a duração. Nesta versão do software, a modificação só pode ser feita no ficheiro de configuração VPN Configuration com um editor de texto.

Nota: Lembre-se que o ficheiro de Configuração VPN não pode ser modificado se está encriptado. Se necessita da protecção por password, modifique os parâmetros **`Xauth-interval`** no ficheiro de configuração VPN, depois importe a configuração VPN modificada e depois vá a" Ficheiro" > 'Exportar Configuração VPN' e seleccione 'Proteger a Configuração VPN exportada'.

```
[General]
Shared-SADB = Defined
Retransmits = 5
Exchange-max-time = 15
Default-phase-1-lifetime = 28800,300:28800
Bitblocking = 0
Xauth-interval = 60
DPD-interval = 15
DPD_retrans = 2
DPD_wait = 15
```

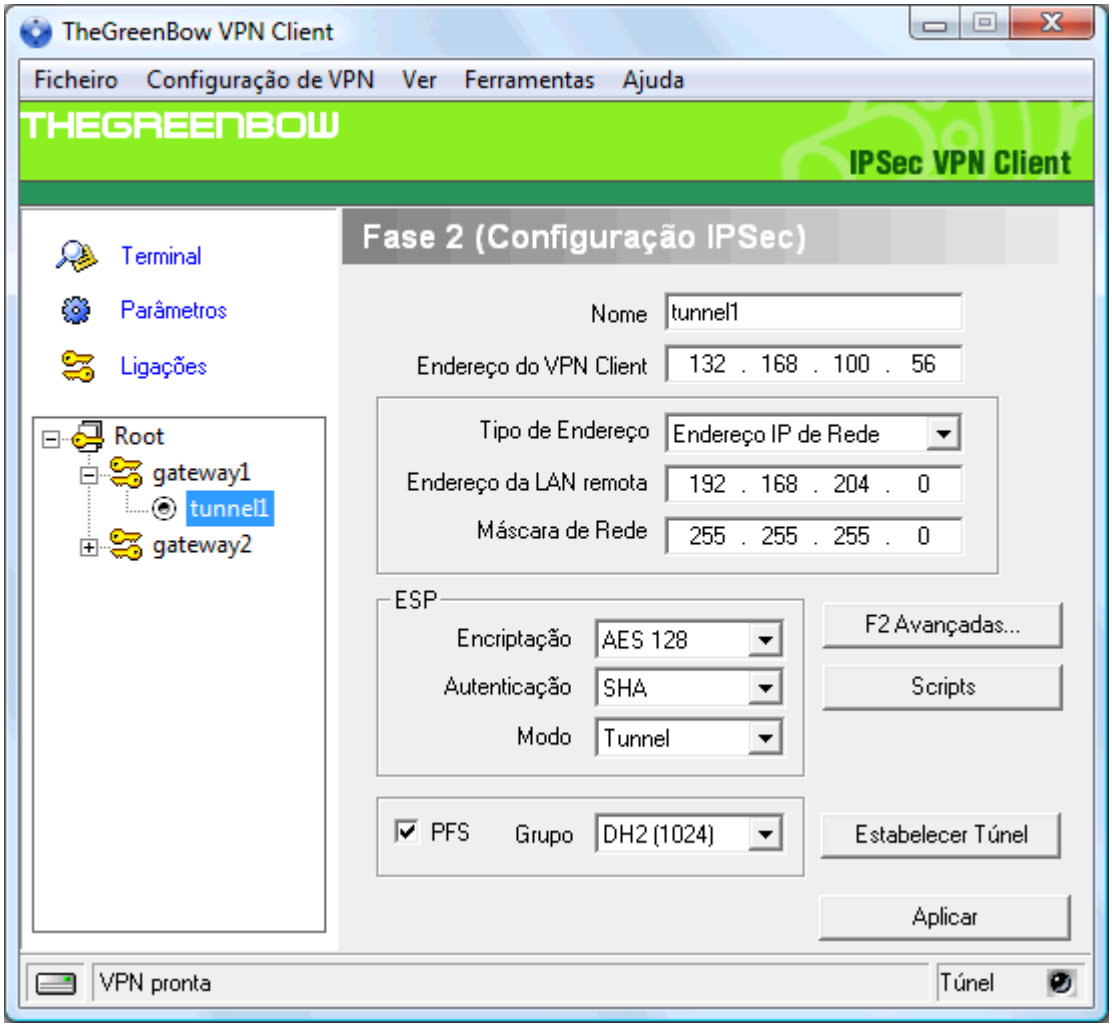
6.4 Configuração IPSec ou Fase 2

6.4.1 O que é a Fase 2 ?

A janela 'Configuração IPSec' ou 'Fase 2' é sobre os parâmetros da Fase 2.

O objectivo da Fase 2 é negociar os parâmetros de segurança IPSec que se aplicam ao tráfego dos túneis negociados na Fase 1.

6.4.2 Descrição dos Parâmetros da Fase 2



Nome	Etiqueta para Configuração IPSec é apenas usada pelo Cliente VPN. Este parâmetro nunca é transmitido na Negociação IPSec. É possível mudar o nome a qualquer momento e lê-lo na arborescência. Duas Fases não podem ter o mesmo nome.
Endereço do Cliente VPN	Endereço do IP Virtual é utilizado por o Cliente VPN dentro da LAN remota: O computador aparecerá na rede distante com este endereço IP. Este endereço IP pode pertencer ao mesmo subnet da LAN distante (ex., neste exemplo, tem como endereço IP 192.168.204.10) Neste caso, é importante ler a nota abaixo.
Tipo de Endereço	A extremidade remota pode ser uma LAN ou um computador. No caso em que seja uma LAN, escolha "Endereço IP de rede" ou "Range Address". Quando selecciona "Endereço IP de rede", os dois campos "Endereço da LAN Remota" e "Máscara de Rede" tornam-se disponíveis. Quando selecciona"Range Address", os dois campos "IP de início" e "IP de fim" tornam-se disponíveis, permitindo ao Cliente VPN IPSec TheGreenBow estabelecer um túnel apenas com uma gama pré- definida de endereços IP.A gama de endereços IP pode ser somente um endereço IP. Se a extremidade remota é um único computador, seleccione " Endereço IP Único". Quando selecciona "Endereço IP Único", só o campo "Endereço do Host Remoto" está disponível.
Endereço Remoto	Este campo pode ser "Endereço do Host Remoto" ou "Endereço da

	LAN remota" conforme o tipo de endereço.É o Endereço IP remoto, ou Endereço da Rede LAN da gateway que abre o túnel VPN.
Máscara de Rede	Máscara de Rede da LAN remota. Só disponível quando o tipo de Endereço é igual a "Endereço IP de rede".
Encriptação ESP	Algoritmo de encriptação negociado durante a fase IPSec (3DES, AES, ...)
Autenticação ESP	Algoritmo de autenticação negociado durante a fase IPSec (MD5, SHA, ...)
Modo ESP	Modo de encapsulamento: tunnel ou transport
Grupo PFS group	Tamanho de chave Diffie-Hellman.
Estabelecer Túnel	Este botão permite abrir o túnel. Este botão muda para "Fechar Túnel" assim que o túnel é aberto.
Scripts	Scripts podem ser configurados na janela Configuração de Script.

Nota1: A funcionalidade "IP Range" combinada com a funcionalidade "Abrir túnel com tráfego" permite abrir automáticamente o túnel quando o tráfego é detectado para uma gama de Endereço IP específica. No entanto a gama de Endereço IP tem de ser autorizada na configuração da gateway VPN.

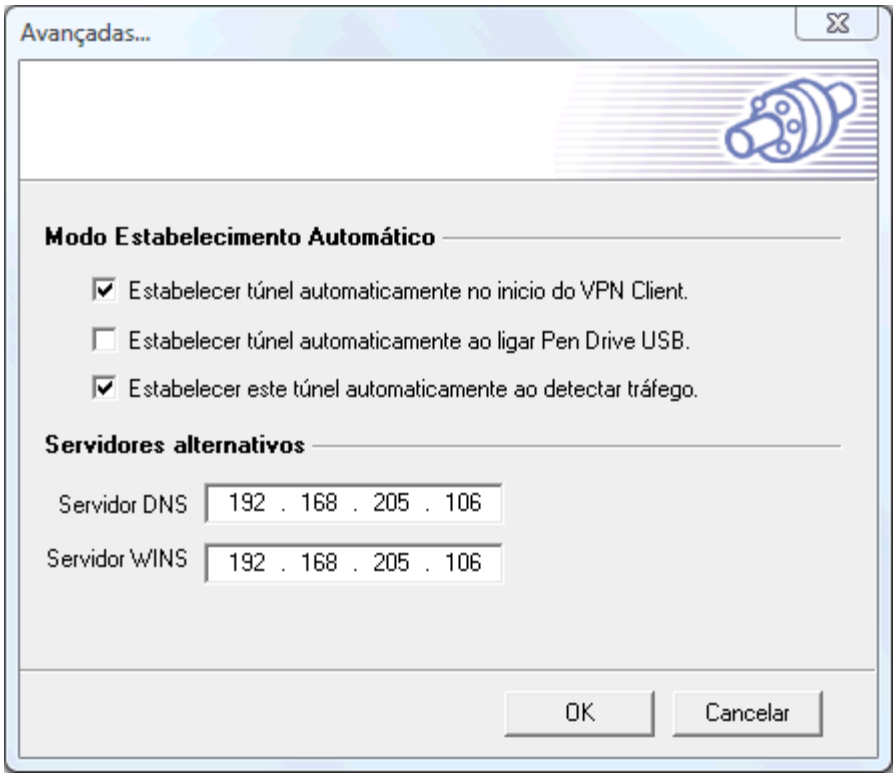
Nota2: É possível ter o endereço IP do seu computador e o endereço da LAN remota na mesma rede. Para ser possível tem de seleccionar "Abrir automáticamente ao detectar tráfego" (F2 Avançada). Uma vez o túnel VPN aberto nesta configuração todo o tráfego com a LAN remota é permitido mas a comunicação com a rede local é agora impossível.

Para mais parâmetros avançados, clique em 'F2 Avançada'.

Uma vez estabelecido os parâmetros, clique em 'Salvar & Aplicar' para salvar e ter em conta a nova configuração.
Poderá encontrar um conjunto de documentos úteis para configurar o Cliente VPN para cada gateway VPN que certificamos. Por favor consulte o nosso website.

6.4.3 Descrição dos parâmetros avançados da Fase 2

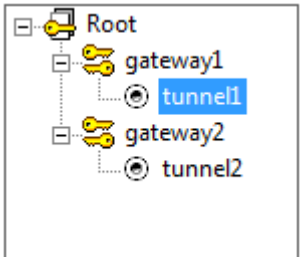
Para funcionalidades e parâmetros avançados clique no botão 'F2 Avançada' no Painel da Fase 2.



Modo Estabelecimento Automático

O Cliente VPN pode abrir automáticamente um túnel específico em determinadas situações como:

- Estabelecer túnel automaticamente no início do Cliente VPN.
- Estabelecer túnel automaticamente ao ligar Pen Drive USB (ver secção "Modo USB").
- Estabelecer este túnel automaticamente ao detectar tráfego para a LAN remota. Se seleccionado, o ícone da Fase 2 na Arborescência de Configuração muda a forma e côr para demonstrar a activação da funcionalidade:

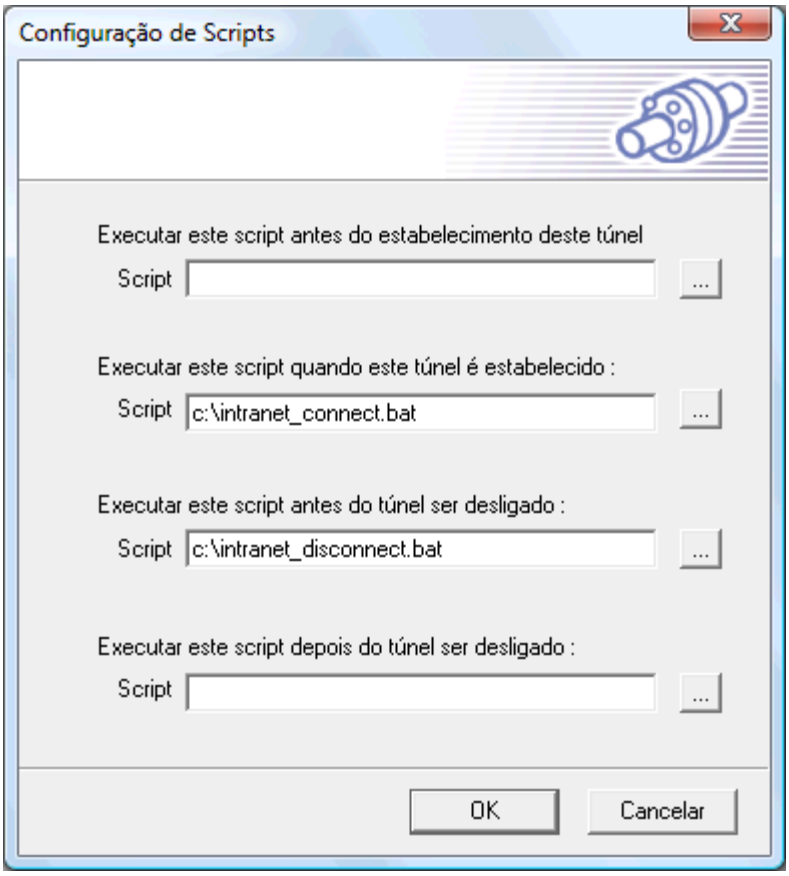


Servidores Alternativos

Os endereços IP dos servidores DNS e WINS da rede distante podem ser introduzidos aqui, para ajudar a resolver os nomes dos servidores da rede. Os endereços DNS ou WINS são tidos em conta logo que o túnel é aberto e enquanto tiver aberto.

6.4.4 Configuração Script

Os scripts podem ser configurados na janela de configuração de Script. Esta janela pode ser aberta através do botão 'Scripts' no Painel da Fase 2.



Os Scripts ou aplicações podem ser executados para cada etapa do processo de abertura e encerramento de um túnel VPN:

- Antes do estabelecimento do túnel
- Uma vez o túnel aberto
- Antes de fechar o túnel
- Uma vez o túnel fechado

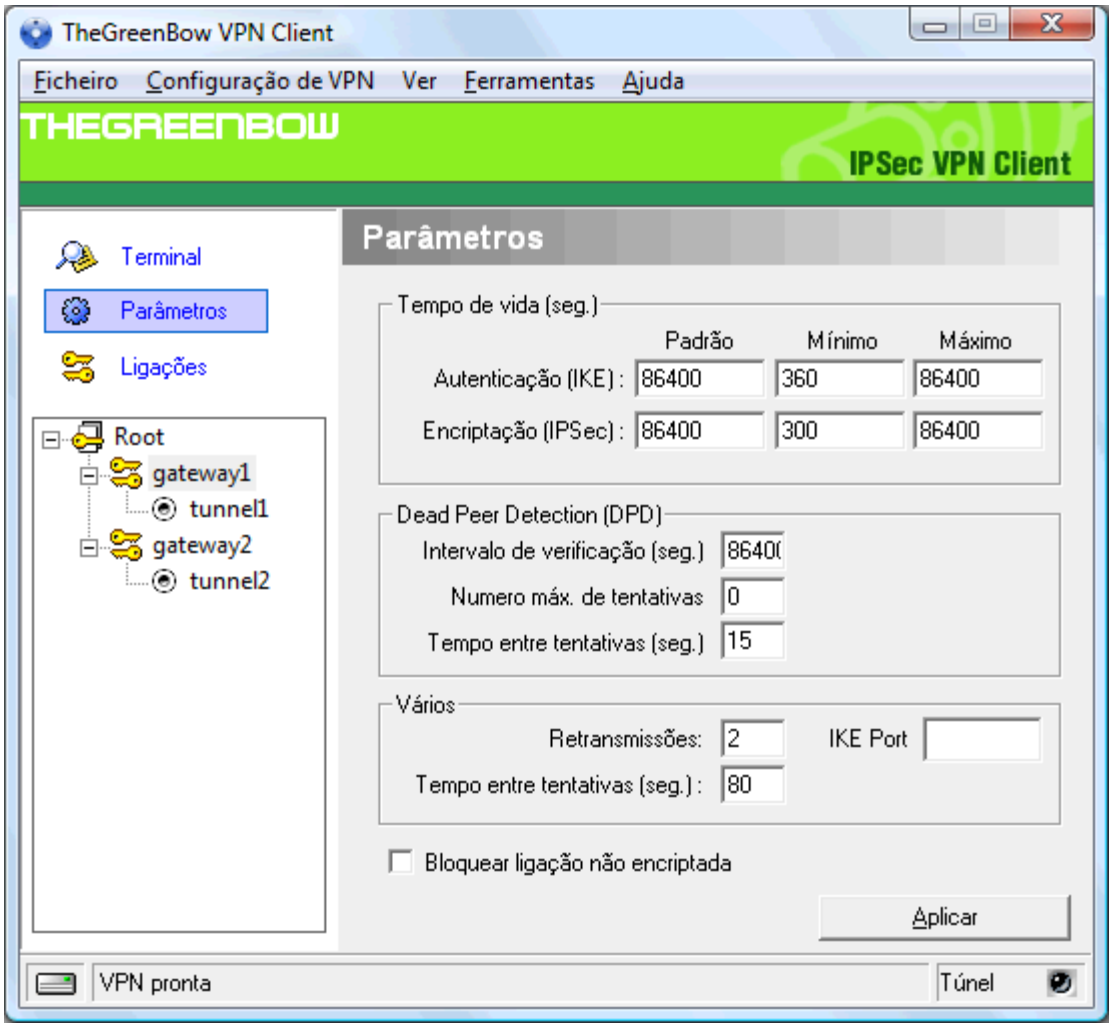
Esta funcionalidade permite executar scripts (batches, scripts, aplicações...) a cada passo de uma conexão de um túnel para uma variedade de propostas ex. para verificar a versão actual do programa, a disponibilidade da base de dados antes de abrir a aplicação de backup, se um programa está a funcionar, se a sessão foi estabelecida...

Também permite configurar várias configurações de rede antes, durante e depois de estabelecer um túnel.

6.5 Parâmetros Globais

6.5.1 Descrição dos Parâmetros Globais

Os parâmetros globais são parâmetros genéricos que são aplicados a todos os túneis VPN configurados. Uma vez modificados, clique em 'Aplicar' para ter em conta as suas modificações.



- **Tempo de Vida (sec.)**
  - **IKE default lifetime** — Tempo Padrão para renegociação IKE.
  - **IKE minimal lifetime** — Tempo Mínimo para renegociação IKE.
  - **IKE maximal lifetime** — Tempo Máximo para renegociação IKE.
  - **IPSec default lifetime** — Tempo Padrão para renegociação IPSec.
  - **IPSec maximal lifetime** — Tempo Máximo para renegociação IPSec.
  - **IPSec minimal lifetime** — Tempo Mínimo para renegociação IPSec.
- **Dead Peer Detection (DPD)**
  - **Intervalo de verificação (seg.)** — Intervalo entre mensagens DPD.
  - **Número Máx de tentativas** — Número de mensagens DPD enviadas.
  - **Tempo entre tentativas (seg.)** — Intervalo entre as mensagens DPD quando não há resposta da gateway remota.
- **Vários**
  - **Retransmissões** — Número de vezes que uma mensagens deve ser retransmitida antes de abandonar.
  - **Tempo entre tentativas (seg.)** — Tempo mínimo antes de qualquer tentativa para reiniciar a negociação IKE
  - **Bloquear ligação não encriptada** — Quando esta opção está seleccionada, apenas a comunicação vpn está autorizada
  - **IKE Port** — Os utilizadores podem mudar a porta para a negociação IKE. A negociação em sempre em UDP mas pode ser numa porta diferente da 500 no caso em que um firewall bloquea a porta 500. A gateway remota deve suportar esta funcionalidade.

Dead Peer Detection (i.e. DPD) é uma extensão do Internet Key Exchange (IKE) (i.e. RFC3706) para detectar uma extremidade IKE morta. O Cliente VPN IPSec TheGreenBow usa o DPD:

- para apagar uma SA aberta no Cliente VPN quando a extremidade foi considerada morta.
- para reiniciar uma negociação IKE negotiations com a Gateway Redundante se activado no Painel de Configuração 'Fase1 Avançada'.

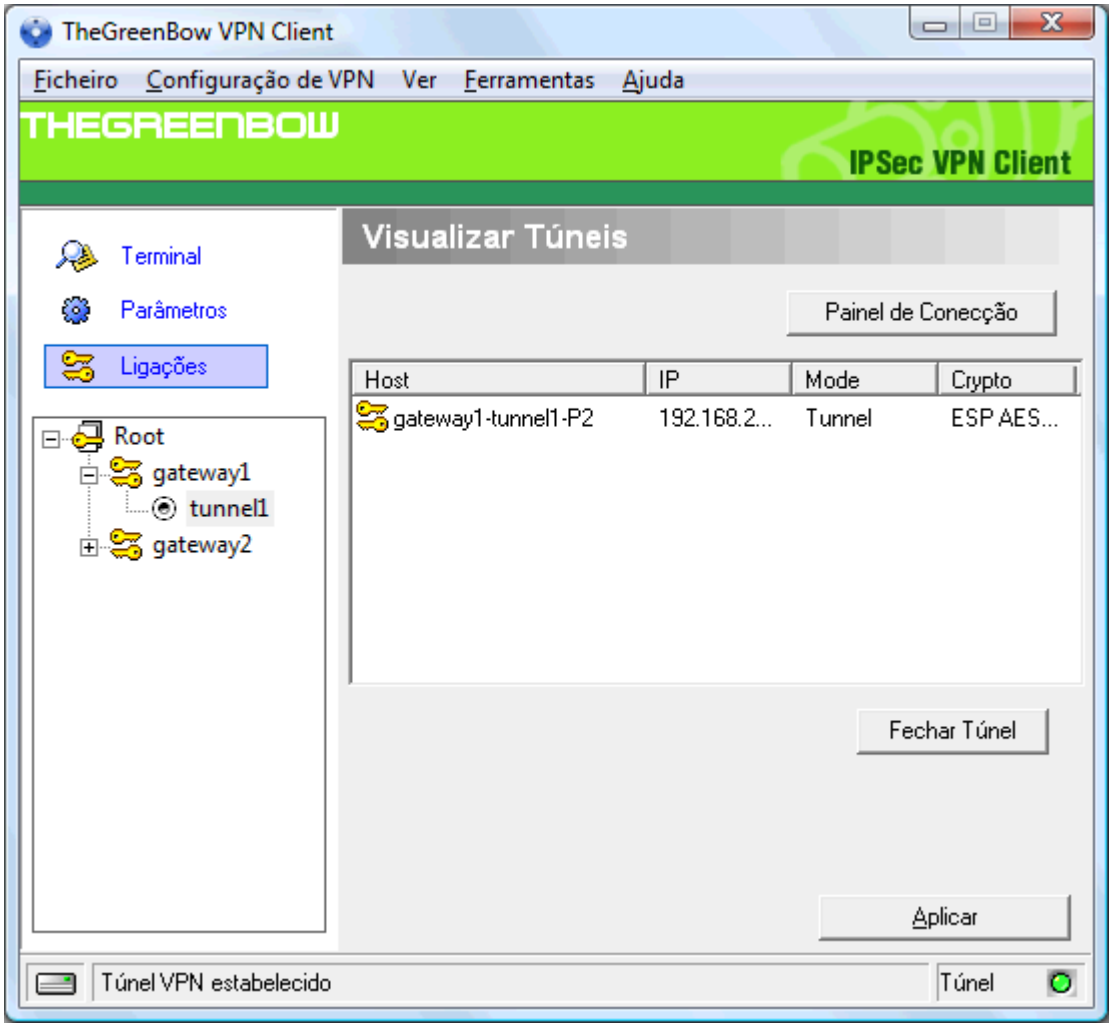
Uma vez os parâmetros configurados, clique em " Aplicar" para salvar e ter em conta a novas configurações.

6.6 Visualizar túneis VPN

6.6.1 Como visualizar os túneis abertos?

A janela 'Visualizar Túneis' mostra os túneis vpn que estão abertos. Esta janela também pode ser usada para fechar os túneis abertos. Para Fechar um Túnel VPN, seleccione o túnel na lista e clique em 'Fechar Túnel'. Os Túneis também podem ser vistos, abertos e fechados directamente do menu no ícone systray e desde o 'Painel de Conexão'.

O Painel de Conexão pode ser aberto com o botão 'Painel de Conexão'. É possivel alternar entre o 'Painel de Conexão' e o 'Painel de Configuração' usando o atalho 'Ctrl + Enter' (ver secção 'Atalhos').



6.7 Modo USB

6.7.1 O que é Modo USB?

O Cliente VPN TheGreenBow oferece a capacidade de assegurar as Configurações VPN e os parâmetros VPN sensíveis (ex.: PreShared key, Certificados, …) com o uso de uma PEN USB.

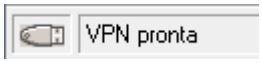
Quando selecciona o "Modo USB", a Configuração VPN e o elementos sensíveis contidos na configuração são guardados no Stick USB na primeira inserção da PEN USB.

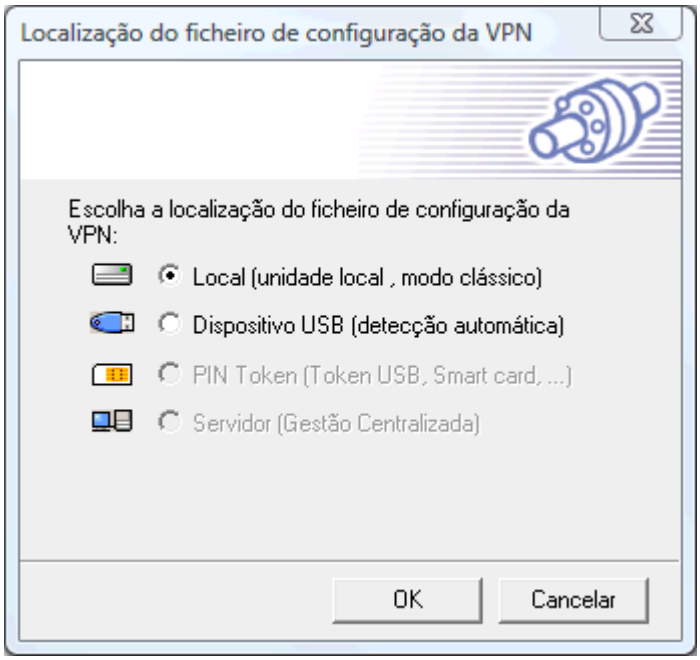
Uma vez feito, só precisa de inserir a PEN USB para abrir automaticamente os túneis vpn. E só precisa de remover a PEN USB para fechar automaticamente os túneis vpn estabelecidos.

6.7.2 Como configurar o Modo USB

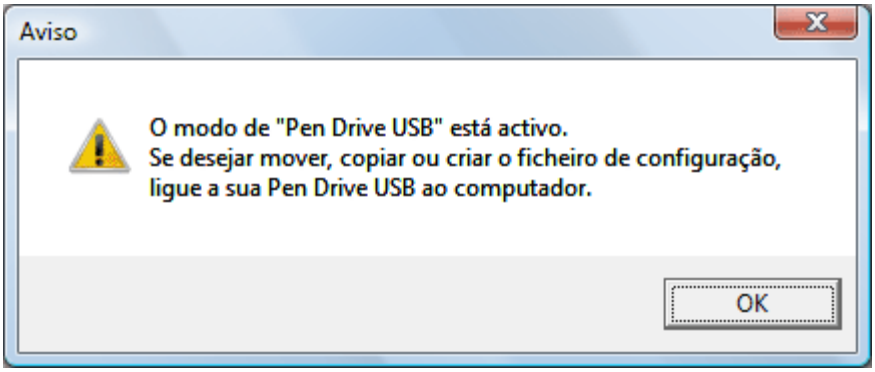
O Modo USB pode ser activado clicando na ícone 'Dispositivo USB' na barra de estado do Painel de Configuração ou através do menu:

- Seleccione o menu 'Ficheiro' > 'Ficheiro de Configuração de VPN...'
- Seleccione 'Dispositivo USB'

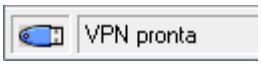


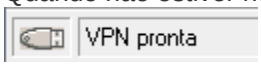


Nota: Nesta etapa, se uma PEN USB que contem uma Configuração VPN está conectada, será automaticamente reconhecida. Note também que não é necessário inserir uma PEN USB nesta etapa. Quando inserir uma Pen USB, a seguinte janela será aberta:



Depois de activar o modo USB, no lado esquerdo da barra de estado mostrará um ícone de um stick USB.

Quando uma Pen USB estiver inserida, o ícone aparece em azul: 

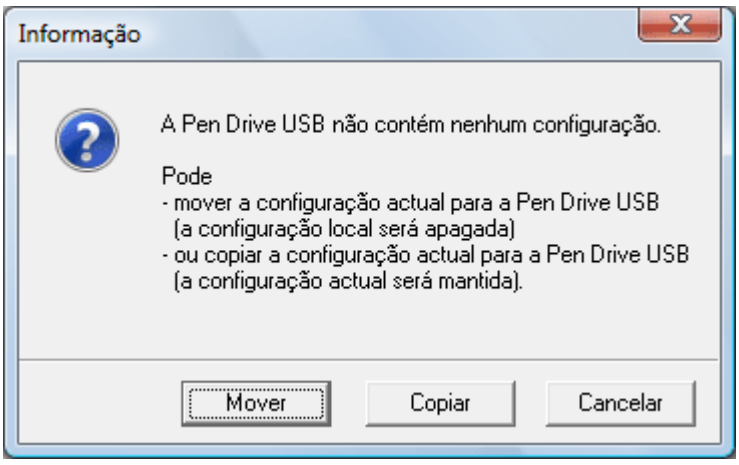
Quando não estiver nenhuma Pen USB inserida, o ícone aparece em cizento:


6.7.3 Como activar uma nova Pen USB?

Pode activar uma nova Pen USB (sem dados) copiando a Configuração VPN e os elementos sensíveis nela.

Quando inserir um novo Stick USB, o Cliente VPN IPSec propõe-lhe automaticamente activar o Stick USB através das seguintes opções:

- **Copiando** a Configuração VPN e os elementos sensíveis na memória USB: o Cliente VPN copiará as informações sensíveis na Pen USB e deixará uma copia no computador. Esta funcionalidade é especificamente útil aos Administradores IT para criar vários Sticks USB para vários utilizadores sem perda de tempo.
- **Movendo** a configuração para o Stick USB: o Cliente VPN IPSec copiará as informações sensíveis na Pen USB e apagará todas as informações sensíveis do computador. Este método é usado para assegurar a Configuração VPN uma vez a Configuração finalizada.

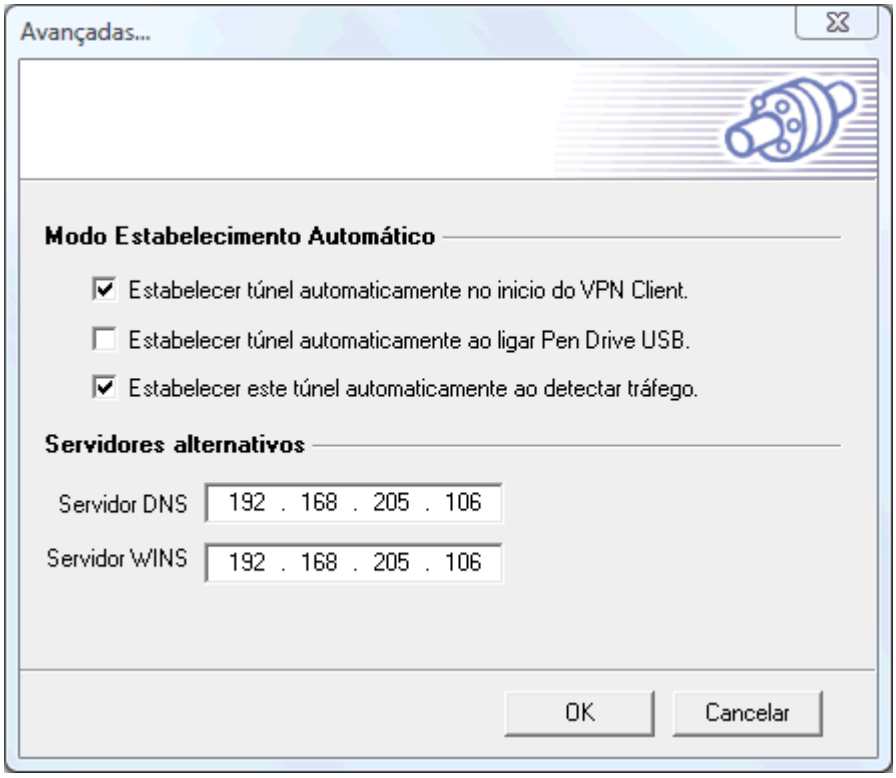


6.7.4 Como abrir automáticamente túneis ao inserir um Stick USB

Cada um dos túneis deve ser configurado de maneira individual:

- Na Configuração IPSec (Fase 2) do túnel, clique no botão 'F2 Avançada'

- Seleccione o modo 'Estabelecer túnel automaticamente ao ligar Pen Drive USB'



6.8 Configuração de Certificados

6.8.1 Vista Global da Gestão de Certificados

O Cliente VPN IPSec TheGreenBow pode utilizar certificados a partir de Ficheiros PEM, Ficheiros PKCS#12 ou SmartCard.

Nota: O Cliente VPN TheGreenBow não permite criar Certificados. Os Certificados têm que ser criados (e guardado numa SmartCard por exemplo) por um software terceiro. Encontrará informação adicional nos documentos "Como Criar Certificados" or "Como converter os formatos dos Certificados" no nosso website.

6.8.2 Como configurar o Cliente VPN IPSec com Cerrtificados PKCS#12

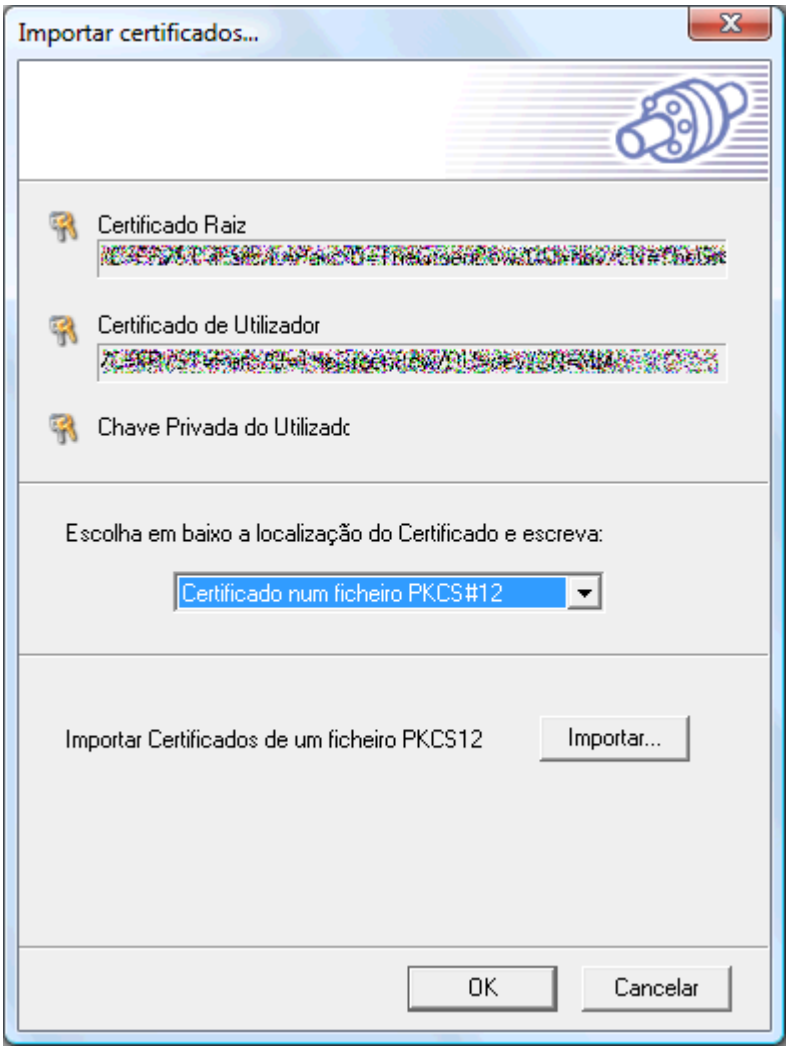
Certificados PKCS#12 são suportados por muitas gateways. O Cliente VPN IPSec TheGreenBow pode importar Certificados PKCS#12 numa Configuração VPN, desde a interface principal. Um certificado PKCS#12 pode ser definido por túnel. Portanto, é possível conectar-se a várias gateways que não utilizem a mesma PKI (Public Key Infrastructure).

Para configurar o Cliente VPN IPSec com **Certificados PKCS#12** deve seguir as seguintes etapas:

Etapa 1: Seleccione o botão 'Certificado' na janela da 'Fase 1' e clique em 'Importar Certificados...'

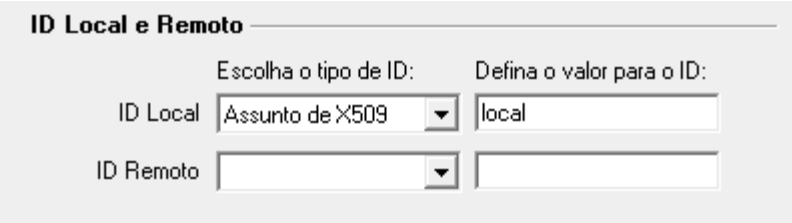
Etapa 2: Seleccione 'Certificado num ficheiro PKCS#12 ' na lista e depois clique no botão 'Importar...'

Etapa 3: Seleccione o Certificado PKCS#12 que deseja importar. Se o Certificado PKCS#12 for protegido, coloque a password na janela popup. Uma vez que o Certificado foi correctamente importado, os campos serão automáticamente preenchidos no topo da janela 'Importar Certificados...'. Também, os ícones de chaves serão visualizados ao lado de cada componente do certificado (certificado raíz, certificado do utilizador, chave privada do utilizador).



Etapa 4: Os Certificados PKCS#12 serão guardados dentro do ficheiro de Configuração VPN assim que clicar em "Aplicar".

Nota: Uma vez importado o Certificado, o assunto será usado como ID local da Fase 1 associada. Poderá ser visualizado na janela F1 Avançada com as seguintes indicações:



6.8.3 Como configurar o Cliente VPN IPSec com Certificados PEM

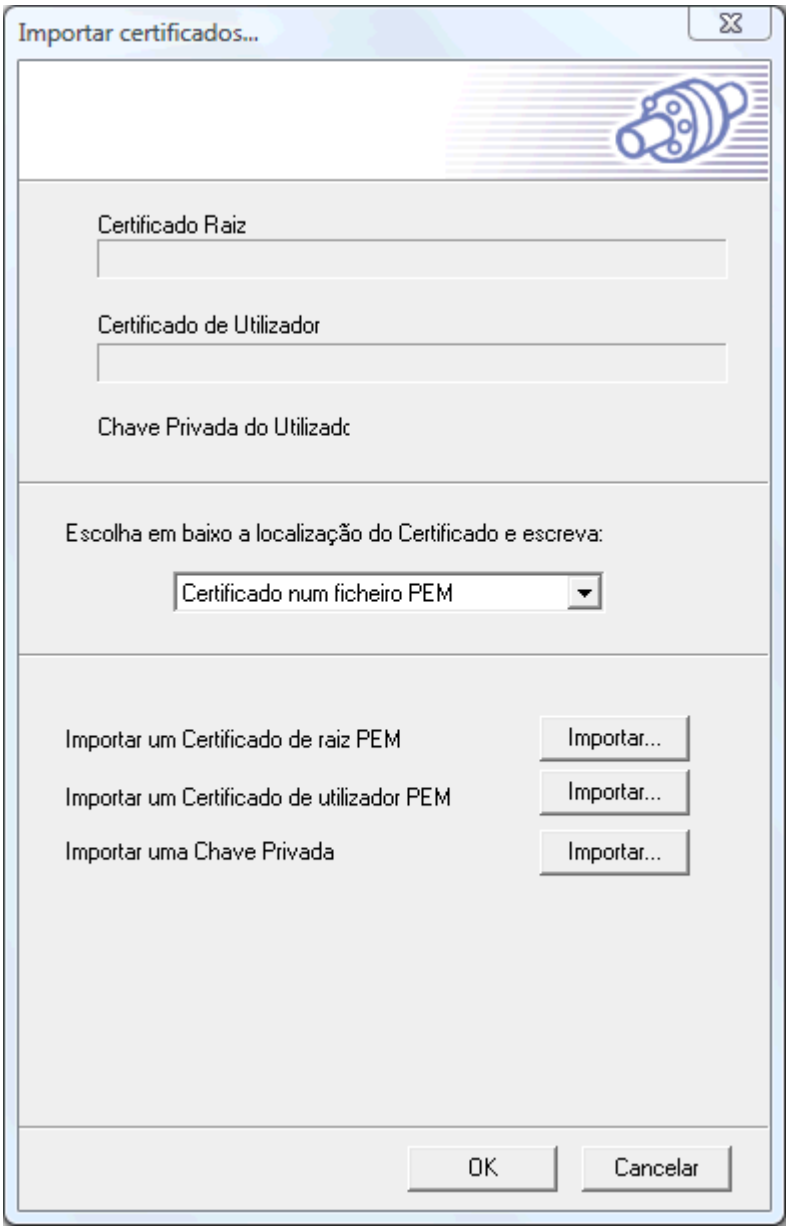
O Cliente VPN IPSec TheGreenBow pode importar Certificados PEM numa Configuração VPN, desde o Painel de Configuração. Um certificado PEM pode ser definido por túnel. Portanto, é possível conectar-se a várias gateways que não utilizem a mesma PKI (Public Key Infrastructure).

Para configurar o Cliente VPN IPSec com **Certificados** PEM deve seguir as seguintes etapas:

Etapa 1: Seleccione o botão 'Certificado' na janela da 'Fase 1' e clique em 'Importar Certificados...'

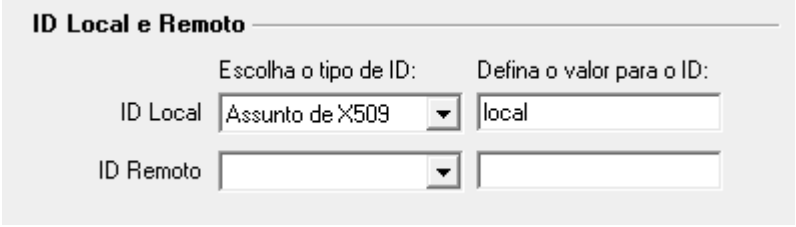
Etapa 2: Seleccione 'Certificado num ficheiro PEM' na lista e depois clique no botão 'Importar...'

Etapa 3:Importe o Certificado de Raiz, o Certificado do utilizador e a Chave privada clicando nos botões correspondentes. Uma vez o certificado correctamente importado, os assuntos serão automáticamente preenchidos ' Importar Certificados'.



Etapa 4: Os Certificados PEM serão guardados dentro do ficheiro de Configuração VPN assim que clicar em "Aplicar".

Nota: Uma vez importado o Certificado, o assunto será usado como ID local da Fase 1 associada. Poderá ser visualizado na janela F1 Avançada com as seguintes indicações:



Nota: O ficheiro PEM que contem a Chave Privada não pode ser encriptado ou protegido com uma password.

6.8.4 Smart Card e Token Management

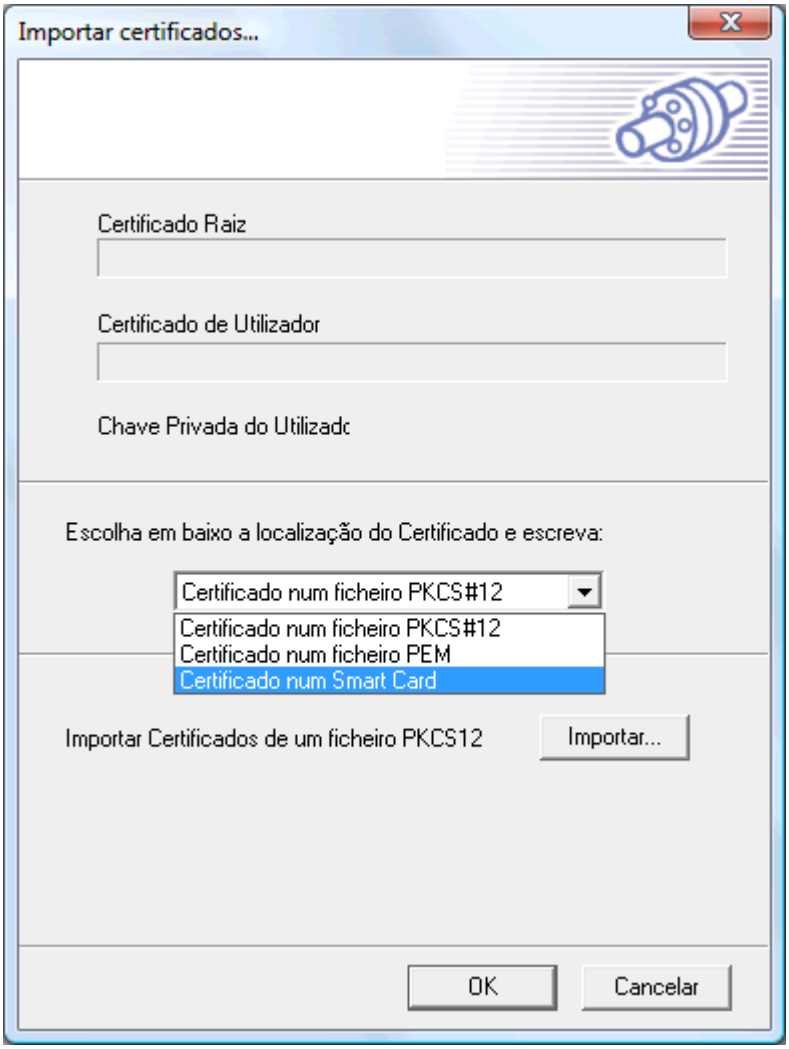
6.8.4.1 Como configurar um túnel com Certificados de uma SmartCard?

O Cliente VPN IPSec TheGreenBow pode ler Certificados de uma Smart Cards. Smart Cards pode ser usada para assegurar os Certificados X509 que podem ser protegidos com um código PIN.

Para configurar um túnel com Certificados a partir de uma Smart Cards siga as etapas seguintes:

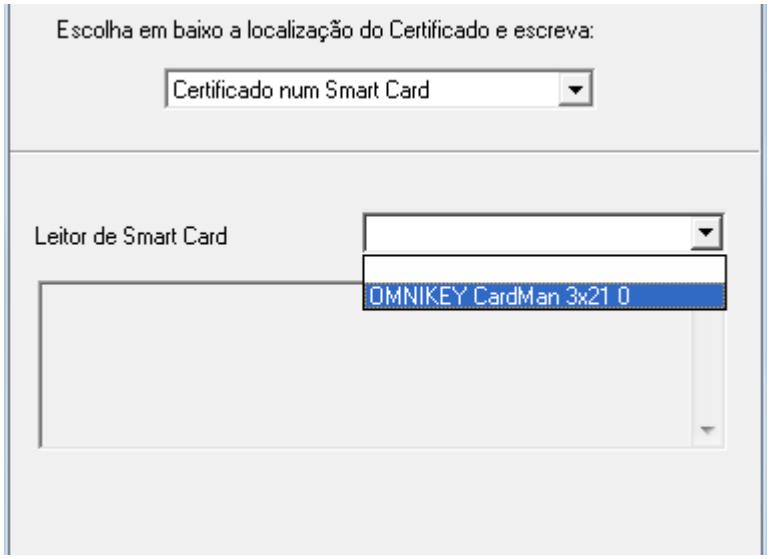
Etapa 1: Seleccione o botão 'Certificado' na janela 'Fase 1' e clique em 'Importar Certificados...'

Etapa 2: Seleccione 'Certificado num SmartCard' na lista. A parte de baixo da janela mostrará uma lista de leitores de SmartCard.

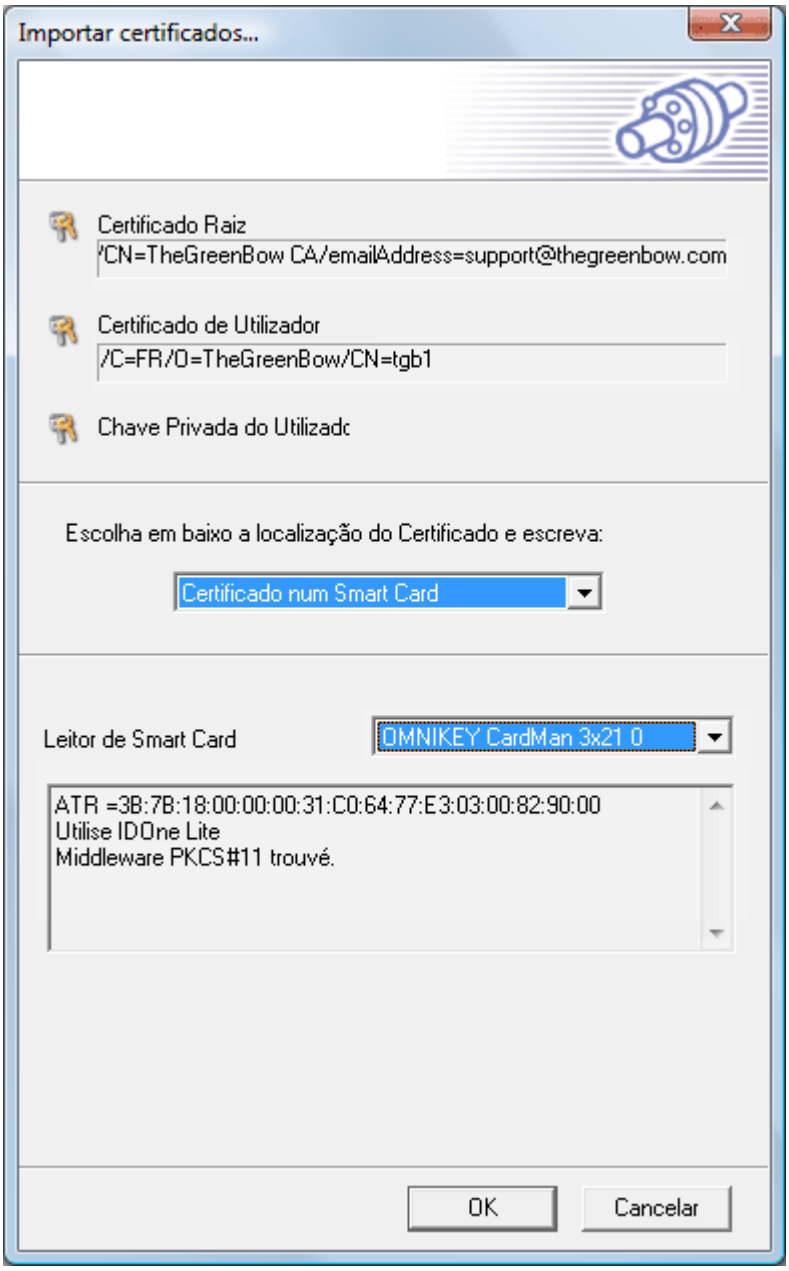


Etapa 3: Seleccione o Leitor SmartCard que você deseja usar. O processo de identificação do

Leitor SmartCard Reader iniciará e o código PIN será pedido. Coloque o seu 'código PIN SmartCard ' e clique 'OK'.



Uma vez a SmartCard lida com êxito, aparecerá informação acerca do Leitor do SmartCard e de SmartCard na área de texto em baixo, enquanto o assunto dos Certificados serão preenchidos nos campos da janela:



Etapa 4: As informações do Leitor do SmardCard Reader serão guardadas no ficheiro de Configuração VPN assim que clicar em "Aplicar".

.

6.8.4.2 Como utilizar um túnel com Certificados de uma SmartCard?

Quando um túnel está configurado para utilizar Certificados a partir de uma SmartCard, o código PIN de uma SmartCard será pedido ao utilizador cada vez que o túnel se abre (excepto nas renegociações VPN automáticas).

Assim, para abrir um túnel com Certificados a partir de uma SmartCard, deverá ter:

1. Um Leitor SmartCard correctamente instalado e configurado com o Cliente VPN IPSec
2. Uma SmartCard legível inserida no Leitor do SmartCard
3. O código PIN correcto para ler a SmartCard.

Casa problema que surge usando uma SmartCard aparecerá na Consola do Software. Ver a seguinte secção 'Problemas com SmartCard.

6.8.4.3 Problemas com SmartCard

Os utilizadores podem encontrar problemas ao configurar a SmartCard e o Leitor SmartCard.

Problema com SmartCard	Messagem (*)
Nenhum Leitor de SmartCard foi encontrado	`No smart card found`

Se nenhum SmartCard foi encontrado, é provável que seja porque o middleware do Leitor da SmartCard está faltando. O processo para instalar facilmente um middleware de um Leitor SmartCard aparecerá na zona de texto debaixo da lista.	`No ATR`
	`Unknown ATR: this smart card may not be supported.`
	`No PKCS#11 middleware for this smart card was found.`
	`You can set PKCS#11 middleware with the command line:`
	`Vpnconf.exe /addmiddleware:path_to_the_dll`

A SmartCard não pode ser lido	`ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00`
	`Using IDOne Lite`
	`PKCS#11 middleware found`
	`Error 0x00000015`

O código PIN está errado	`ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00`
	`Using IDOne Lite`
	`PKCS#11 middleware found`
	`Wrong PIN code`

Nenhum certificado foi encontrado na SmartCard	`ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00`
	`Using IDOne Lite`
	`PKCS#11 middleware found`
	`No configuration or no certificate found in the smart card`

(*) Messagem mostrada na área de texto debaixo da lista SmartCard.

Utilizadores podem encontrar problemas ao abrir um túnel que requer um Certificado de uma SmartCard.

Problemas com a Smart Card	Messagem na Consola.
Nenhum Leitor de SmartCard foi encontrado	`Missing SmartCard Reader`
O código PIN está errado	`Wrong PIN code`
Nenhum certificado foi encontrado na SmartCard ou a SmartCard não pode ser lida	`Empty or unreadable SmartCard`

6.9 Gestão da Configuração VPN

6.9.1 Importar ou Exportar uma Configuração VPN via menu

O Cliente VPNTheGreenBow pode importar ou exportar as Configurações VPN. Com esta funcionalidade, os Administradores IT podem preparar a configuração e envia-las a outros utilizadores.

- Para importar a configuração, seleccione "Ficheiro > Importar Configuração de VPN".
- Para exportar uma configuração, seleccione "Ficheiro > Exportar Configuração VPN".

Um ficheiro de configuração VPN exportado terá uma extensão ".tgb".

Uma configuração VPN exportada pode ser protegida por uma senha. Quando o utilizador desejar exportar uma configuração, uma janela perguntará automaticamente se deseja proteger ou não a configuração VPN com uma password.

Quando uma Configuração VPN é protegida por password, a sua importação pedirá automaticamente ao utilizador a password. Uma Configuração VPN exportada não protegida por password será importada automaticamente.

Nota: Importar/Exportar no 'Modo USB'
Quando o Cliente VPN é configurado em "Modo USB" e quando a PEN USB é inserida, a importação da Configuração VPN é directamente escrita na PEN USB. Se o Cliente VPN é configuradp em "Modo USB" mas nenhuma PEN está inserida (o ícone USB no canto inferior esquerdo do GUI está desactivado), a exportação e a importação da Configuração VPN não é permitida.

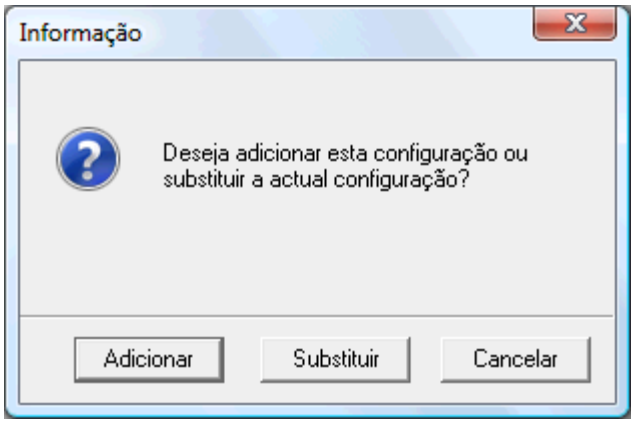
Nota: A Configuração VPN também pode ser importada via linha de comando.

6.9.2 Juntar Configurações VPN

O Cliente VPN IPSec TheGreenBow pode importar um ou vários túneis numa configuração VPN existente. Com essa funcionalidade, administradores IT podem juntar uma nova configuração VPN de uma nova gateway com a Configuração VPN existente e enviar-la ao utilizador ou a um grupo de utilizadores.

Pode juntar Configurações VPN com as seguintes formas:

1. Importar nova Configuração VPN via 'Ficheiro'>'Importar Configuração VPN' e seleccionar 'Adicionar' em vez de 'Substituir'.



2. Drag&drop uma nova Configuração VPN dentro do software com uma configuração VPN existente já aberta. A mesma janela (ver acima) aparecerá perguntadno se o utilizador quer 'Adicionar' ou 'Substituir' a configuração VPN existente.

3. Importar nova Configuração VPN via linhas de comando.

   " **`[path]\vpnconf.exe /add:[file.tgb]`** " onde **`[path]`** é a pasta de instalação do Cliente VPN, e **`[file.tgb]`** é ficheiro de Configuração VPN. Este comando não reconhece caminhos relativos (ex. "..\..\file.tgb"). Para mais detalhes, ver importar linhas de comandos.

Desde que escolha importar uma Configuração VPN, aqui estão comportamentos comuns:

- Parâmetros Globais não são importados quando pelo menos um túnel já estava configurado e o utilizador seleccione "Adicionar" Configuração VPN.
- Parâmetros Globais são importados quando o utilizador selecciona 'Substituir' ou se nenhum túnel estava configurado antes da importação.
- Conflitos com os nomes dos túneis existentes e importados são resolvidos automaticamente pelo software adicionando um número incrementado entre parêntesis ex. tunnel_office(1) aos nomes dos túneis importados (i.e. tanto na Fase1 como na Fase 2).

6.9.3 Dividir Configuração VPN

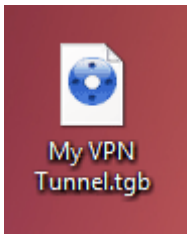
O Cliente VPN IPSec TheGreenBow pode exportar um único túnel de uma Configuração VPN existente. Com esta funcionalidade, administradores IT podem dividir uma Configuração VPN existente numa Configuração VPn mais pequena e envia-la ao utilizador ou ao grupo de utilizadores.

Para exportar um único túnel, tem de seguir os seguintes passos:

1. Faça clique direito na Fase 2 do túnel da sua Configuração VPN e seleccione 'Exportar Túnel'.

2. Uma janela perguntará se deseja proteger a Configuração VPN com uma password.

3. Uma vez exportada, a Configuração VPN pode ser enviada aos utilizadores ou pode clicar duas vezes nela para iniciar o Cliente VPN IPSec TheGreenBow.



Nota:

- Exportar uma Fase 2 também exportar a Fase 1 associadal. Isto significa que também exporta os Certificados definidos na Fase 1.
- Exportar uma Fase 2 também exportar os Parâmetros Globais.

6.9.4 Integra a sua Configuração VPN na instalação do Cliente VPN IPSec

Uma Configuração VPN (previamente criada) pode ser integrada na instalação do Cliente VPN IPSec. Integrar uma ConfiguraçãoVPN na instalação do Cliente VPN IPSec permite aos administradores IT distribuir o software Cliente VPN IPSec pré- configurado num único pacote para todos os utilizadores da empresa.

6.9.5 Configuração VPN por Defeito

A instalação do Cliente VPN IPSec integra uma Configuração VPN por defeito. Esta Configuração VPN permite abrir um túnel com o nosso servidor de demo TheGreenBow assim que o software Cliente VPN IPSec seja instalado.

É especialmente prático para verificar que um túnel pode ser aberto a partir do meu computador para uma rede distante operacional destinada para teste e eventualmente para debug.

Parte VII

Distribuição

7 Distribuição

7.1 Configuração VPN Integrada

Durante a instalação do software, o Cliente VPN IPSec pode importar automaticamente um ficheiro de configuração VPN ".tgb" integrado na instalação do Cliente VPN IPSec (descomprimido, ver 'Guia de Distribuição' no nosso website.

O processo para criar uma instalação com uma configuração VPN integrada é o seguinte:

1. Criar a Configuração VPN que vai ser integrada ao Setup. Esta etapa deve ser realizada num Cliente VPN IPSec previamente instalado de onde a Configuração VPn será exportada (ex. "myconfig.tgb").
2. Criar uma instalação silenciosa, ou simplesmente unzip o Setup do Cliente VPN IPSec.
3. Copiar o ficheiro de Configuração VPN (ex. "myconfig.tgb") dentro da pasta do setup descomprimido.
4. Distribuir o pacote ao utilizador (a Configuração VPN será usada durante a instalação)

Nota importante: a instalação não pode importar e usar uma Configuração VPN encriptada (protegida). Quando criar a Configuração VPN certifique-se que a exporta sem protecção.

7.2 Opções de Instalação

7.2.1 Vista Global das Opções de Instalação

Varias opções estão disponíveis com a instalação do Cliente VPN IPSec.

1. Configuração do modo GUI (Interface Gráfica do Utilizador): *'full'*, *'user'* or *'hidden' ('completa', 'utilizador' ou 'oculta').*
2. Protecção com o modo Acesso Controlado ao GUI com password.
3. Configuração dos elementos do menu Systray.
4. Outras opções para o Inicio do Software, Número de Licença, Activação do Software automática, nenhuma janela de avaliação, idiomas e Email para Activação.

Exemplo de sintaxe:

```
Setup.exe /S --license=0123456789ABCDEF0123 --start=1
--activmail=smith@smith.com
```

> Atenção: as opções '**`--guidefs`**', '**`--menuitem`**', '**`--license`**', '**`--start`**', **`'--activmail'`**, **`'--password`**, **`'--autoactiv`**, **`'--noactivwin`**, **`'--lang'`** só podem ser usadas com o parâmetro '/S' (modo de instalação silenciosa, com letra maiúscula).

Para mais detalhes, por favor veja 'Guia de Distribuição' no nosso website.

7.2.2 Opções de Setup para o modo GUI

Sintaxe: **`--guidefs=full|user|hidden`**
permite definir a aparência da Interface Gráfica do Utilizador (GUI) quando o Cliente VPN IPSec inicie.

"**`full`**": [Defeito] Aparece o Painel de Configuração.
"**`user`**": Aparece o Painel de Conexão.
"**`hidden`**": Nem o Painel de Configuração, nem o Painel de Conexão podem ser visualizados. Simplesmente o menu Systray pode ser aberto. Os túneis podem ser aberto através do menu

Systray.

7.2.3 Opções de Setup para o modo Acesso Controlado ao GUI

Sintaxe: **`--password=mypwd`**
permite controlar o acesso ao GUI do Cliente VPN com uma password.

Uma password será pedida ao utilizador:

- Quando o utilizador clicar na ícone VPN do systray.
- Quando o utilizador quiser passar do Painel de Conexão para o Painel de Configuração.

Examplo: **`--guidefs=user --password=admin01`**
Estas duas opções permitem bloquear o GUI ao 'Painel de Conexão', enquanto o acesso ao Painel de Configuração é protegido por uma password.

7.2.4 Opções de Setup para o menu Systray

Sintaxe: **`--menuitem=[0...31]`**
Permite especificar os elementos do menu systray que o Administrador IT quer guardar disponíveis.

O valor é um campo 'bitfield': **`1 = Sair, 2 = Painel de Conexão, 4 = Terminal, 8 = Guardar&Aplicar, 16 = Painel de Configuração, Por Defeito é 31: Todos os menus.`**

Exemplo: **`--menuitem=5`** configurará o menu systray só com os elementos: Sair + Terminal (Consola).

Nota 1: Os túneis aparecem sempre no menu systray, e podem sempre ser abertos ou encerrados desde o menu systray.

Nota 2: **`'menuitem'`** e **`'guidefs=hidden'`**.
Por defeito, **`guidefs=hidden`** configura o menu Systray com Sair + Terminal. (Os elementos 'Guardar&Aplicar' e 'Painel de Conexão' não estão visíveis). No entanto, o uso de **`'menuitem'`** é

prioritário a **'guidefs'**.
Isto significa que: "**--guidefs=hidden --menuitem=1**" configurará o menu Systray só com o elemento 'Sair'.

7.2.5 Outras Opções de Setup

As outras opções para o Setup são:

Sintaxe: **--license=[license_number]**
Permite configurar o Número de Licença. O Número de Licença é um conjunto de 24 caracteres hexadecimais. Números de Licença antigos podem ter 20 caracteres hexadecimais.

Sintaxe: **--start==[1|2|3]**
Permite configurar quando o Cliente VPN iniciar: **depois do logon windows [1], durante o boot [3], ou manualmente [2]. Por defeito é [1].**

Sintaxe: **--activmail=[activation_email]**
Permite forçar o endereço email do processo de activação. Durante o processo de activação, o campo para entrar o endereço email estará desactivado.

Sintaxe: **--autoactiv=1**
No caso de uma actualização do Software (i.e. o número de licença e o email de activação já foram colocados numa instalação anterior) com a opção --autoactiv=1 , o software vai tentar activar automaticamente o produto quando se iniciar se a rede estiver disponível ou então na abertura de um túnel se a rede não estava disponível no inicio.

Sintaxe: **--noactiv=1**
Não visualização da 'Janela de Avaliação' quando o software inicie atá ao fim do período de experimentação. O Utilizador não sabe se está em período de avaliação e o software não estará disponível no final do período de experimentação. Isto significa que se um utilizador lança o software depois do fim do periodo de experimentação, o programa iniciará e abrirá a 'janela de Avaliação' mas o botão 'Avaliar' estará desactivado.

Sintaxe: **--lang=[language code]**
Esta opção especifica o idioma do software Cliente VPN IPSec TheGreenBow software e da sua instalação. Os idiomas disponíveis são os seguintes.

ISO 639-2 code	código do idioma	Nome em Inglês
EN	1033 (default)	English
FR	1036	French
ES	1034	Spanish
PT	2070	Portuguese
DE	1031	German
NL	1043	Dutch
IT	1040	Italian
ZH	2052	Chinese simplified
SL	1060	Slovenian
TR	1055	Turkish
PL	1045	Polish
EL	1032	Greek

RU	1049	Russian
JA	1041	Japanese
FI	1035	Finnish
SR	2074	Serbian

Exemplo:
TheGreenBow_VPN_Client.exe /S --license=0123456789ABCDEF0123 --start=1 --activmail=smith@smith.com

7.3 Linha de Comandos

7.3.1 Opções Linha de Comando

Várias linhas de comando estão disponíveis, foram feitas para ser usadas por administradores IT para adaptar o Cliente VPN IPSec às suas necessidades e para ajudar na integração de outras aplicações.

- Fechar Cliente VPN IPSec
- Importar ou Exportar Configurações VPN
- Abrir ou Fechar túneis VPN

Para mais detalhes, por favor veja o 'Guia de Distribuição no nosso website.

7.3.2 Fechar o Cliente VPN IPSec: opção "/stop"

O Cliente VPN TheGreenBow pode ser encerrado a qualquer momento com a linha de comando:

" **[path]\vpnconf.exe /stop** " onde **[path]** é a pasta de instalação do Cliente VPN IPSec

Se estiverem vários túneis activos serão fechados correctamente.

Esta funcionalidade pode ser usada, por exemplo, num script que lança o Cliente VPN depois de estabelecer uma conexão dialup e fecha-o antes da desconexão.

7.3.3 Importar ou Exportar uma Configuração VPN

O Cliente VPN TheGreenBow pode importar uma determinada Configuração VPN com a seguinte linha de comando:

" **[path]\vpnconf.exe /import:[file.tgb]** " onde **[path]** é a pasta de instalação do Cliente VPN, e **[file.tgb]** é o ficheiro de Configuração VPN. Este comando não resolve caminhos relativos (ex.: "..\..\file.tgb"). Aspas duplas são suportadas o que permite caminhos com espaços.

" **/import:** " pode ser usado com o Cliente VPN a funcionar ou não. Quando o Cliente VPN já está funcionando, importa de maneira dinâmica a nova configuração e é automaticamente aplicada (i-e: o serviço IKE é reiniciado). Se o Cliente VPN não está em execução, será lançado com a nova configuração.

" **/importonce:** " permite importar uma Configuração VPN sem ter o Cliente VPN a funcionar. Esta opção é especialmente útil para a scripts de instalação: Permite fazer uma instalação silenciosa e importar uma configuração automaticamente.

" **/replace:** " permite substituir a Configuração VPN existente por uma nova Configuração VPN . Esta funcionalidade está disponível desde a versão do software 4.1, e pode ser usada em vez da opção /importonce para importar uma Configuração VPN sem ter o Cliente VPN a funcionar.

" **/export:** " permite exportar a Configuração VPN corrente (incluindo os Certificados) num ficheiro especifico. Este comando lança o Cliente VPN se não estiver executado.

" **/exportonce:** " permite exportar a Configuração VPN corrente (incluindo os Certificados) num ficheiro especifico. Este comando não lança o Cliente VPN se não estiver já a funcionar.

" **/add:** " permite importar uma nova Configuração VPN dentro da Configuração VPN corrente, junta assim as duas configurações numa só Configuração VPN. Este comando pode ser usado com o Cliente VPN a funcionar ou não. Este comando não lança o Cliente VPN se não estiver já a funcionar.

" **/pwd:[password]**" permite especificar a password para a importação de Configuração VPN. Esta opção deve ser usada juntamente com as opções /import ou /importonce.

As 6 opções "**import**", "**importonce**", "**export**", "**exportonce**", "**replace**" e "**add**" são exclusivas e não podem ser usadas ao mesmo tempo.

7.3.4 Abrir ou Fechar Túnel VPN

O Cliente VPN TheGreenBow Cliente VPN pode abrir ou fechar um túnel VPN em linha de comando. As duas linhas de comando pode ser executadas quando Cliente VPN IPSec TheGreenBow esta lançado:

" **[path]\vpnconf.exe /open:[phase1-phase2]** " onde **[path]** é a pasta de instalação do Cliente VPN, e **[phase1-phase2]** são os nomes da Fase 1 y da Fase 2 na Configuração VPN. Este comando não resolve caminhos relativos (ex.: "..\..\file.tgb"). Aspas duplas são suportadas o que permite usar caminhos com espaços.
Se o túnel já estiver aberto, esta linha de comando não tem qualquer efeito.

" **[path]\vpnconf.exe /close:[phase1-phase2]** " onde **[path]** é a pasta de instalação do Cliente VPN, e **[phase1-phase2]** são os nomes da Fase 1 y da Fase 2 na Configuração VPN. Este comando não resolve caminhos relativos (ex.: "..\..\file.tgb"). Aspas duplas são suportadas o que permite usar caminhos com espaços.
Se o túnel já estiver fechado, esta linha de comando não tem qualquer efeito.

As duas opções "**open**" e "**close**" são exclusivas e não podem ser usadas ao mesmo tempo.

Nota de restrição:
- A execução destas linhas de comando abrirá a Interface Gráfica do Utilizador do Software (GUI). Esta restrição será corrigida numa próxima versão do software.

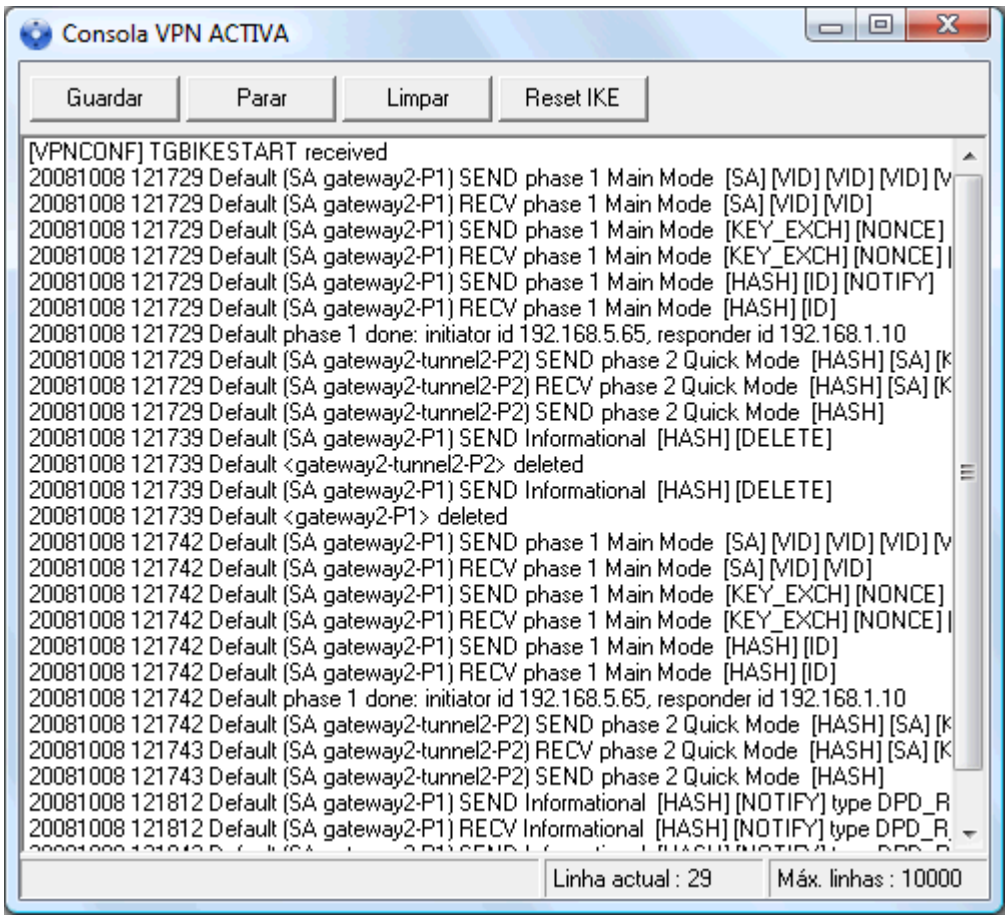
Parte VII

Consola e Logs

8 Consola e Logs

8.1 Terminal de Registros

A janela 'Consola' pode ser aberta desde o menu Systray ou desde o botão 'Terminal' no Painel de Configuração. Esta janela pode ser usada para analisar os túneis VPN. Esta ferramenta é particularmente útil aos administradores IT quando estão a configurar a rede vpn.



Botão	Descrição
Guardar	Guarda os Logs num ficheiro. Os registros futuros não serão salvados no ficheiro.
Iniciar/Parar	Inicia/Pare de receber os logs.
Limpar	Limpa a janela de registros
Reset IKE	Reinicie o Serviço IKE.

Parte IX

Tradução do Software

9 Tradução do Software

A tradução do Cliente VPN IPSec é agora possível, mesmo por um terceiro.
Todas as sequências do Cliente VPN estão listadas na nossa ferramenta de tradução, prontos a ser traduzidos.

Etapa1: Download a ferramente de tradução do Cliente VPN no nosso website.
Step2: Traduza todos os elementos na sua lingua
Step3: Envia-nos o ficheiro das sequencias do Cliente VPN para: support@thegreenbow.pt
Step4: Incluiremos o seu idioma na próxima versão oficial do Cliente VPN IPSec. Pode ver no nosso website quem já contribuiu.

Todo o processo para criar uma tradução está descrito na página: www.thegreenbow.pt/vpn_local.html.

Parte X

Contactos

10 Contactos

Informações e actualizações estão disponíveis em: www.thegreenbow.pt
Apoio Técnico pelo email: support@thegreenbow.pt
Contacto Comercial pelo email: sales@thegreenbow.pt

Índice

- P -

- R -

- S -

Secure, Strong, Simple.

TheGreenBow Security Software