Cliente VPN IPSec TheGreenBow

Guia de Configuração

Digitel NRX 5122

WebSite: http://www.thegreenbow.pt
Contacto: support@thegreenbow.pt

Guia de Configuração escrito por:

Escritor:	Suporte Técnico Digitel
Empresa:	www.digitel.com.br

Lista de Conteúdos

1 Introdução

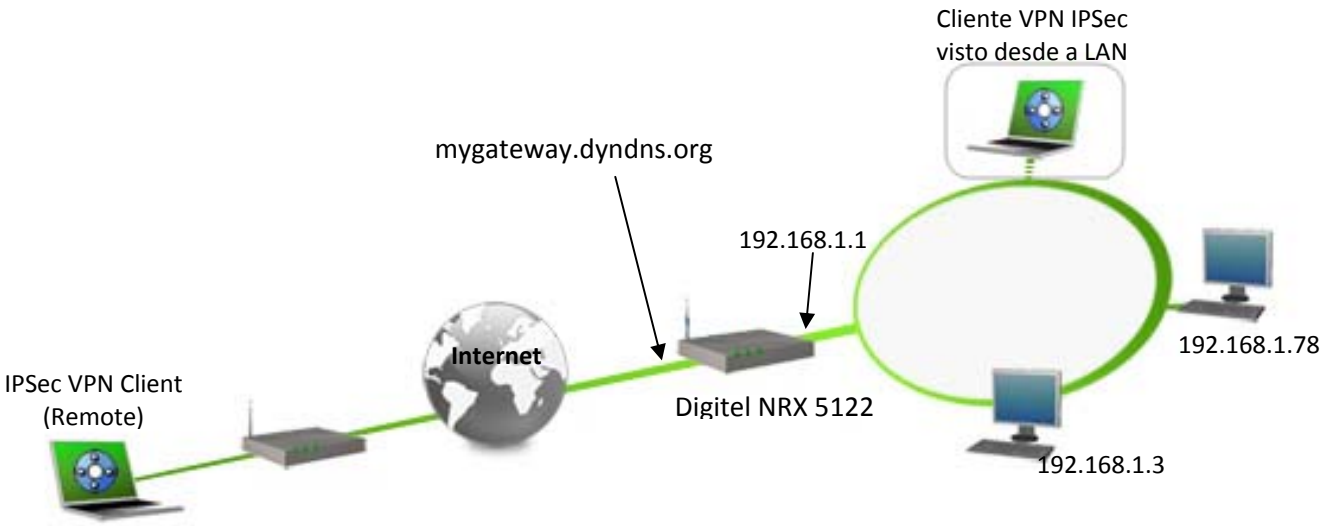
1.1 Objectivo deste documento

Este Guia de Configuração pretende descrever como configurar o Cliente VPN IPSec TheGreenBow com um Router VPN Digitel NRX 5122 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 Router VPN Digitel NRX 5122EG. 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 Digitel

Dependendo da topologia a ser utilizada podem ser necessárias algumas alterações no Script de Configuração do Digitel NRX 5122. Neste caso contate o Suporte da Digitel através do e-mail suporte@digitel.com.br .

1.4 Router VPN Digitel

Os nossos testes e a configuração VPN foram realizados com Digitel NRX 5122EG versão do firmware 79309e.

1.5 Informação sobre o Router VPN Digitel

É fundamental que todos os utilizadores tenham toda a informação sobre o Router VPN Digitel NRX 5122. Todas as informações sobre o produto, o Guia do Utilizador assim como uma base de conhecimento sobre o Router VPN Digitel NRX 5122 podem ser encontrados no site: www.digitel.com.br/pt/produtos/produto.asp?idLinha=11&idCat=36&Id=38

Página do produto NRX 5122	http://www.digitel.com.br/pt/produtos/produto.asp?IdLinha=11&IdCat=36&Id=38
FAQ/Knowledge Base	suporte@digitel.com.br

2 Configuração VPN Digitel NRX 5122

Esta secção descreve como estabelecer um Túnel VPN com o Router VPN Digitel NRX 5122.

```
SET LAN LAN0 MODE AUTO
SET LAN LAN0 IP 192.168.1.254 MASK 255.255.255.0
SET LAN LAN0 UP

SET LAN LAN1 MODE AUTO
SET LAN LAN1 IP 192.168.30.15 MASK 255.255.255.0
SET LAN LAN1 UP

SET ROUTES DEFAULT GW1 192.168.30.1 COST1 1
SET ROUTES UP

SET IPSEC FRAGICMP TRUE NATT TRUE MTU 1412 TYPE DEFAULTROUTE
SET IPSEC CHANNEL0 NAME Teste  MODE TUNNEL
SET IPSEC CHANNEL0 AUTO ADD DPDACTION RESTART DPDDELAY 120 DPDTIMEOUT 120
SET IPSEC CHANNEL0 LEFT ADDRESSTYPE DEFAULTROUTE
SET IPSEC CHANNEL0 LEFT SUBNET TRUE NET 192.168.1.0 MASK 255.255.255.0
SET IPSEC CHANNEL0 RIGHT ADDRESSTYPE ANY
SET IPSEC CHANNEL0 RIGHT SUBNET FALSE
SET IPSEC CHANNEL0 KEY AUTH ESP AUTHBY SECRET PASS digitel
SET IPSEC CHANNEL0 KEY ISAKMP 24H RETRIES 0 KEYLIFE 1H
SET IPSEC CHANNEL0 IKE0 ALG 3DES HASH MD5 DH 2
SET IPSEC CHANNEL0 ESP0 ALG 3DES HASH MD5
SET IPSEC UP
```

Onde:

```
SET LAN LAN0 MODE AUTO
```

Configura a LAN0 para autonegociação.

```
SET LAN LAN0 IP 192.168.1.1 MASK 255.255.255.0
```

Configura o IP da interface ETH0 que neste caso é a Rede Local.

```
SET LAN LAN1 MODE AUTO
```

Configura a LAN1, que neste cenário é a interface que dá acesso a internet. para autonegociação.

```
SET LAN LAN1 IP 192.168.30.15 MASK 255.255.255.0
```

```
SET ROUTES DEFAULT GW1 192.168.30.1 COST1 1
```

Configura a rota de saída do roteador.

```
SET IPSEC FRAGICMP TRUE NATT TRUE MTU 1412 TYPE DEFAULTROUTE
```

Fragmentação de pacotes ICMP habilitada. Nattraversal habilitado, TYPE define o tipo da conexão. Neste caso por Default route.

```
SET IPSEC CHANNEL0 NAME Teste MODE TUNNEL
```

NAME - Define o nome para o canal neste caso Teste com modo de conexão Tunel.

```
SET IPSEC CHANNEL0 AUTO ADD DPDACTION RESTART DPDDELAY 120 DPDTIMEOUT 120
```

AUTO define que operação será feita automaticamente pelo IPSEC neste caso será o ADD (aguarda a conexão). DPDACTION ativa o DPD (Dead PEER Detection) e informa que ação será tomada após o tunel ser considerado morto. DPDDELAY e DPDTIMEOUT definem o intervalo entre os Keepalives do DPD e o tempo sem respostas para que o tunel seja considerado morto respectivamente.

```
SET IPSEC CHANNEL0 LEFT ADDRESSTYPE DEFAULTROUTE
```

Define ao lado local (LEFT) do IPSEC que o concentrador é alcançável pela Rota Default.

```
SET IPSEC CHANNEL0 LEFT SUBNET TRUE NET 192.168.1.0 MASK 255.255.255.0
```

Define a Rede local que fará parte da VPN/IPSEC.

```
SET IPSEC CHANNEL0 RIGHT ADDRESSTYPE ANY
```

Configura o Ipsec para aceitar conexão de qualquer endereço IP.

```
SET IPSEC CHANNEL0 RIGHT SUBNET FALSE
```

Define a Rede remota que fará parte da VPN/IPSEC. Neste caso estão liberadas todas as redes.

```
SET IPSEC CHANNEL0 KEY AUTH ESP AUTHBY SECRET PASS digitel
```

Habilita a troca de chaves (KEY), AUTH define o tipo de autenticação (ESP ou AH), AUTHBY defino o método da autenticação (SECRET= Pre Shared) , PASS é a senha para autenticação.

```
SET IPSEC CHANNEL0 KEY ISAKMP 24H RETRIES 0 KEYLIFE 8H
```

ISAKMP define o tempo de vida da chave antes da renegociação, RETRIES é o números de tentativas de autenticação e o 0 (zero) equivale a ilimitado, KEYLIFE configura o tempo de vida da chave (KEY).

```
SET IPSEC CHANNEL0 IKE0 ALG 3DES HASH MD5 DH 2
```

IKE0 (internet key exchange) Habilita o algoritmo de encriptação e autenticação da conexão, ALG é o parâmetro de defino qual será o algoritmo de criptografia que será utilizado no tunel, HASH configura a criptografia Hash que será usada, e DH define o Diffie-Hellman group para a conexão.

```
SET IPSEC CHANNEL0 ESP0 ALG 3DES HASH MD5
```

ESP0 (Encapsulating Security Payload) habilita o algoritmo de encriptação e autenticação da conexão, ALG é o parâmetro de defino qual será o algoritmo de criptografia que será utilizado no tunel, HASH configura a criptografia Hash que será usada, e DH define o Diffie-Hellman group para a conexão.

```
SET IPSEC UP
```

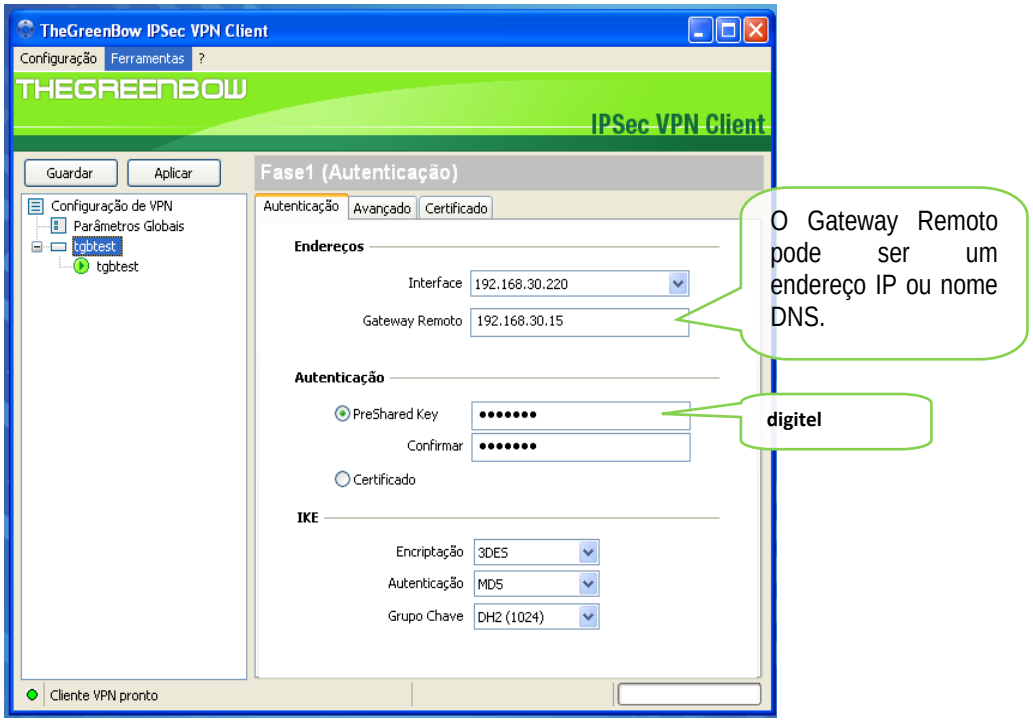
Ativa o funcionamento do módulo IPSEC.

3 Configuração do Cliente VPN IPSec TheGreenBow

Esta secção descreve a configuração necessária para se conectar a um router VPN Digitel NRX 5122.

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

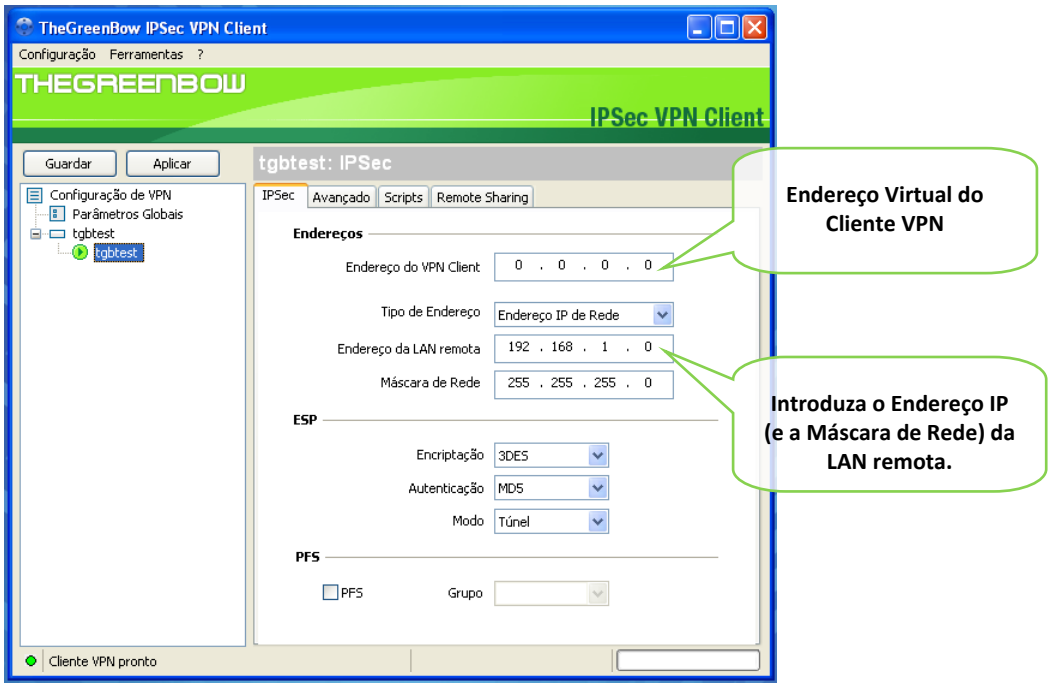
3.1 Cliente VPN - Configuração Fase 1 (IKE)



Configuração Fase 1

Você pode usar tanto Preshared Key, Certificados, ou X-auth para a autenticação do usuário com o roteador Digitel NRX 5122. 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 Roteador Digitel NRX 5122 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 Router VPN Digitel NRX 5122 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 automáticamente (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.

```
20110215 141513 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) RECV phase 2 Quick Mode  [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode  [HASH]
20110215 141524 Default (SA gateway1-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_
20110215 141524 Default (SA gateway1-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_
20110215 141534 Default (SA gateway1-P1) SEND Informational  [HASH] [DELETE]
20110215 141534 Default <gateway1-tunnel1-P2> deleted
20110215 141534 Default (SA gateway1-P1) SEND Informational  [HASH] [DELETE]
```

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.

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 estebelecido, 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 Router VPN Digitel NRX 5122, os pacotes poderão estar a ser bloqueados por alguma regra de firewall.
- Confirme se o seu ISP suporta o protocolo ESP.
- Verifique se o "default gateway" do computador remoto está devidamente configurado (neste caso terá de estar configurado para o endereço IP do Router VPN Digitel NRX 5122).
- 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.

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

Notícias e Actualizações para o Router Digitel NRX 5122 no site: www.digitel.com.br

Suporte Técnico: via email: suporte@digitel.com.br

Comercial via email: vendas_digitel@digitel.com.br

Secure, Strong, Simple.

TheGreenBow Security Software