Configuração de C2G com software Greenbow nos roteadores VPN RV016, RV042, RV042G e RV082

Objetivos

C2G (Cliente para Gateway) é configurado no cliente do GreenBow usando a página de configuração Gateway-to-gateway onde a opção NAT-T está presente. O GreenBow é um software voltado para o fornecimento de software de segurança empresarial baseado em um conjunto completamente seguro. A GreenBow desenvolveu um software de segurança empresarial que simplifica o acesso remoto, permite que usuários remotos acessem sua rede corporativa com segurança.

Este documento explica como configurar o IPSec VPN C2G com software Greenbow nos roteadores VPN RV016, RV042, RV042G e RV082.

Dispositivos aplicáveis

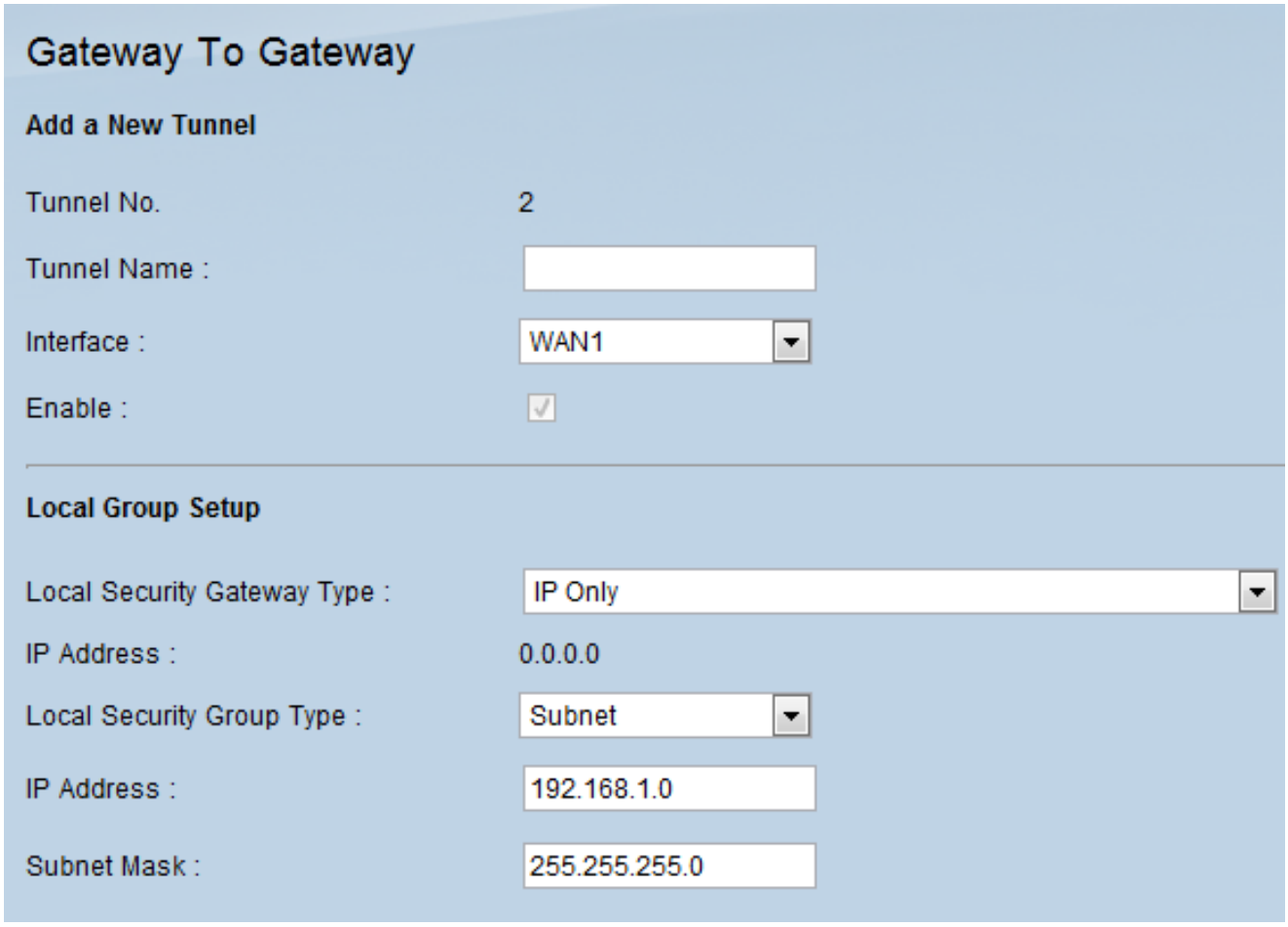
- RV016
- RV042
- RV042G
- RV082

Versão de software

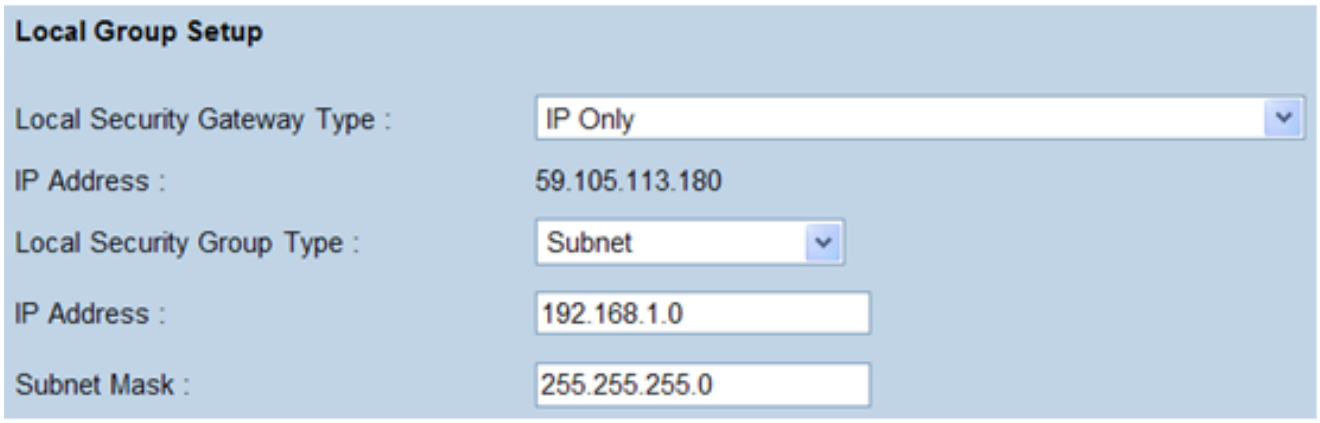
- v4.2.1.02

Configuração do software C2G e GreenBow

Etapa 1. Efetue login no Utilitário de configuração do roteador para escolher **VPN > Gateway to Gateway**. A página *Gateway to Gateway* é aberta:



Role para baixo até a área Local Group Setup (Configuração do grupo local).



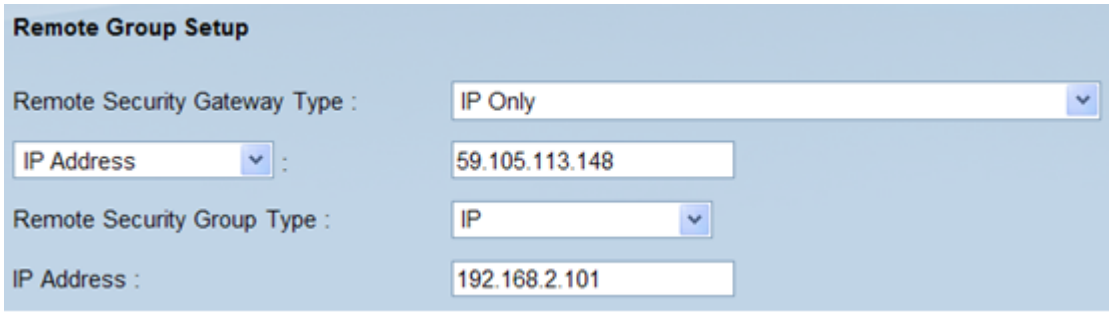
Etapa 2. Escolha **IP Only** na lista suspensa Local Security Gateway Type.

Etapa 3. Escolha **Sub-rede** na lista suspensa Tipo de grupo de segurança local.

Etapa 4. No campo Endereço IP, insira o endereço IP do roteador.

Etapa 5. No campo Máscara de sub-rede, insira a máscara de sub-rede do roteador.

Etapa 6. Role para baixo até acessar a área de Configuração do grupo remoto da página.



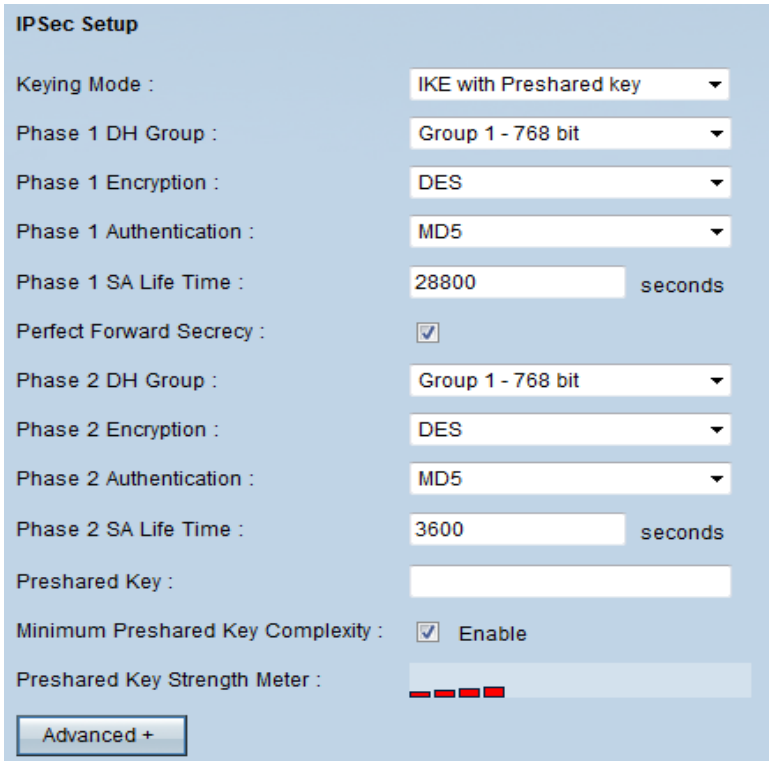
Passo 7. Escolha **Somente IP** na lista suspensa Tipo de gateway de segurança remota.

Etapa 8. Escolha o tipo de **endereço IP** na lista suspensa Remote Security Gateway IP Address Type.

Etapa 9. No campo Endereço IP, insira o endereço IP da WAN do roteador remoto.

Etapa 10. Selecione **IP** na lista suspensa Tipo de grupo de segurança remota.

Etapa 11. No campo Endereço IP, insira o endereço IPv4 do roteador.



Etapa 12. Escolha **IKE com chave pré-compartilhada** na lista suspensa Modo de chaveamento.

Etapa 13. Escolha **Grupo de 1 a 768 bits** na lista suspensa Grupo DH Fase 1.

Etapa 14. Escolha **DES** na lista suspensa Phase 1 Encryption.

Etapa 15. Escolha **MD5** na lista suspensa Fase 1 Autenticação.

Etapa 16. No campo Período de vida da SA da Fase 1, insira **28800** segundos.

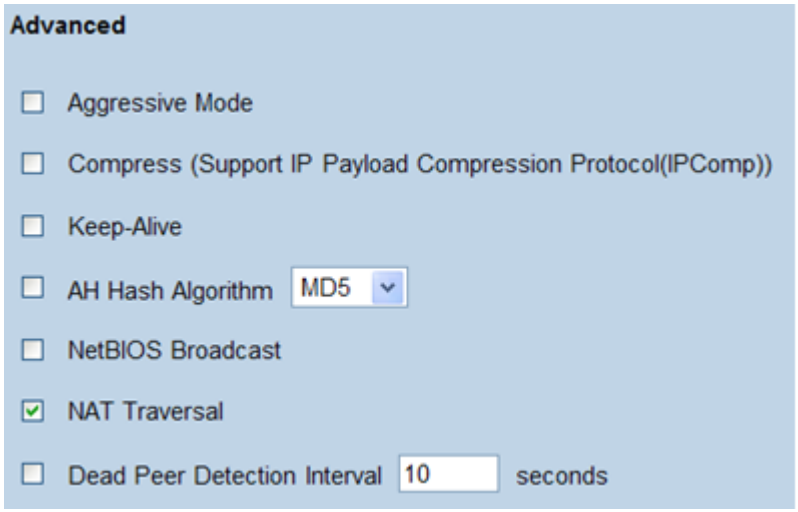
Etapa 17. Escolha **Grupo de 1 a 768 bits** na lista suspensa Grupo DH Fase 2.

Etapa 18. Escolha **DES** na lista suspensa Phase 2 Encryption.

Etapa 19. Escolha **MD5** na lista suspensa Fase 2 Autenticação.

Etapa 20. No campo Período de vida da SA da Fase 2, insira **3600** segundos.

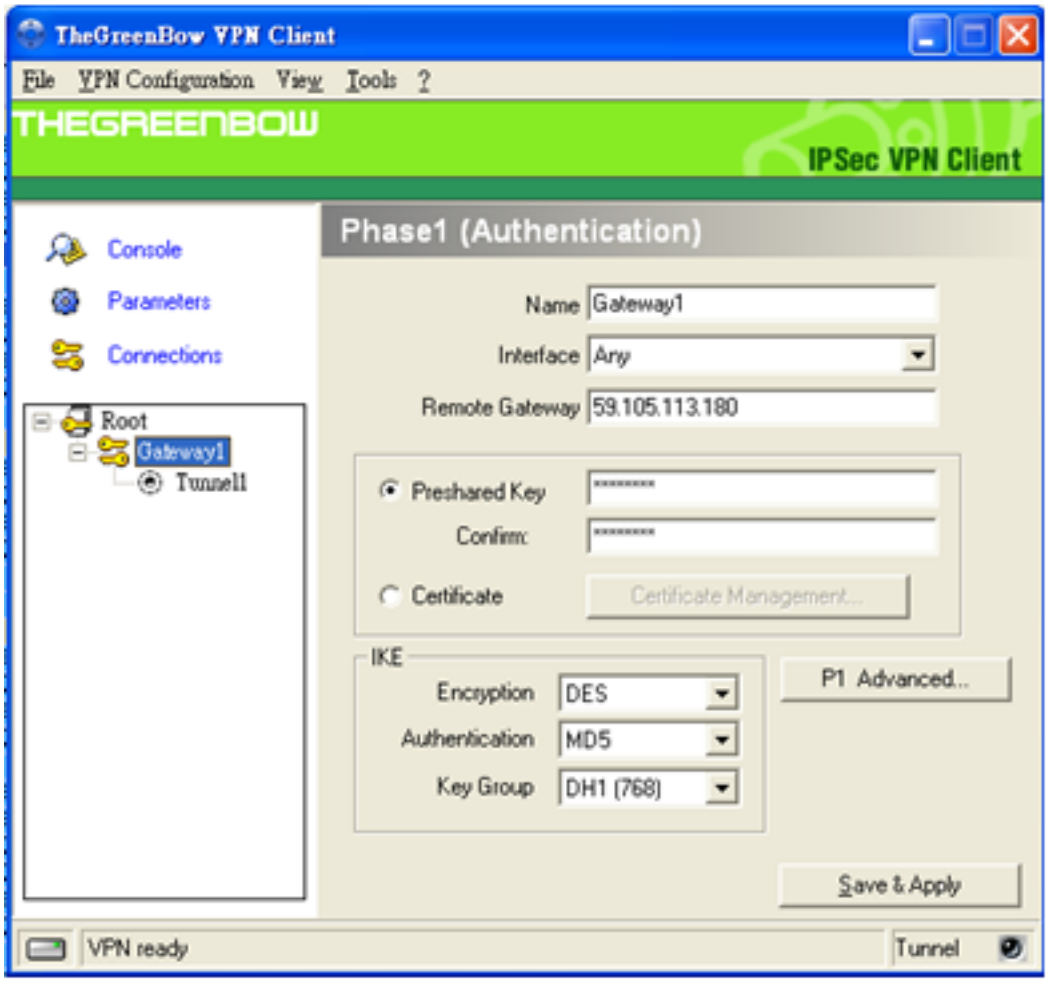
Etapa 21. No campo Chave pré-compartilhada, insira a combinação desejada de números e/ou letras. Nesse caso, é "1234678".



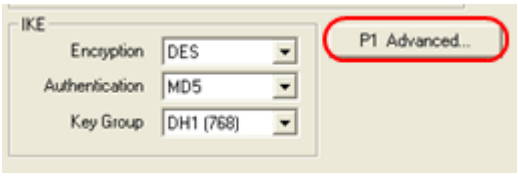
Etapa 22. Clique em **Avançado +**. A página *Avançado* é aberta:

Etapa 23. Marque a caixa de seleção **NAT Traversal**.

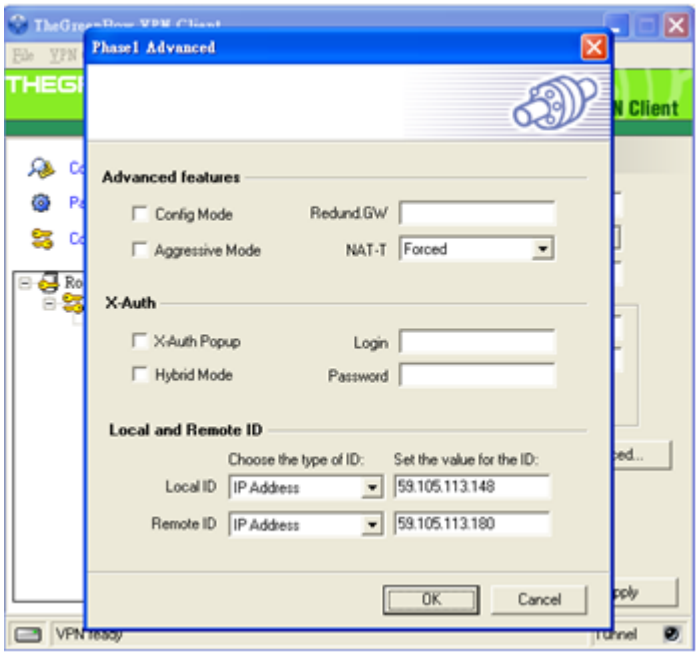
Etapa 24. Inicie o software IPSec VPN Client Greenbow em seu computador.



Etapa 25. No campo Gateway remoto, insira o endereço IP da WAN do roteador remoto.



Etapa 26. Clique no botão **P1 Advanced**. A página *Avançado da Fase1* é aberta:



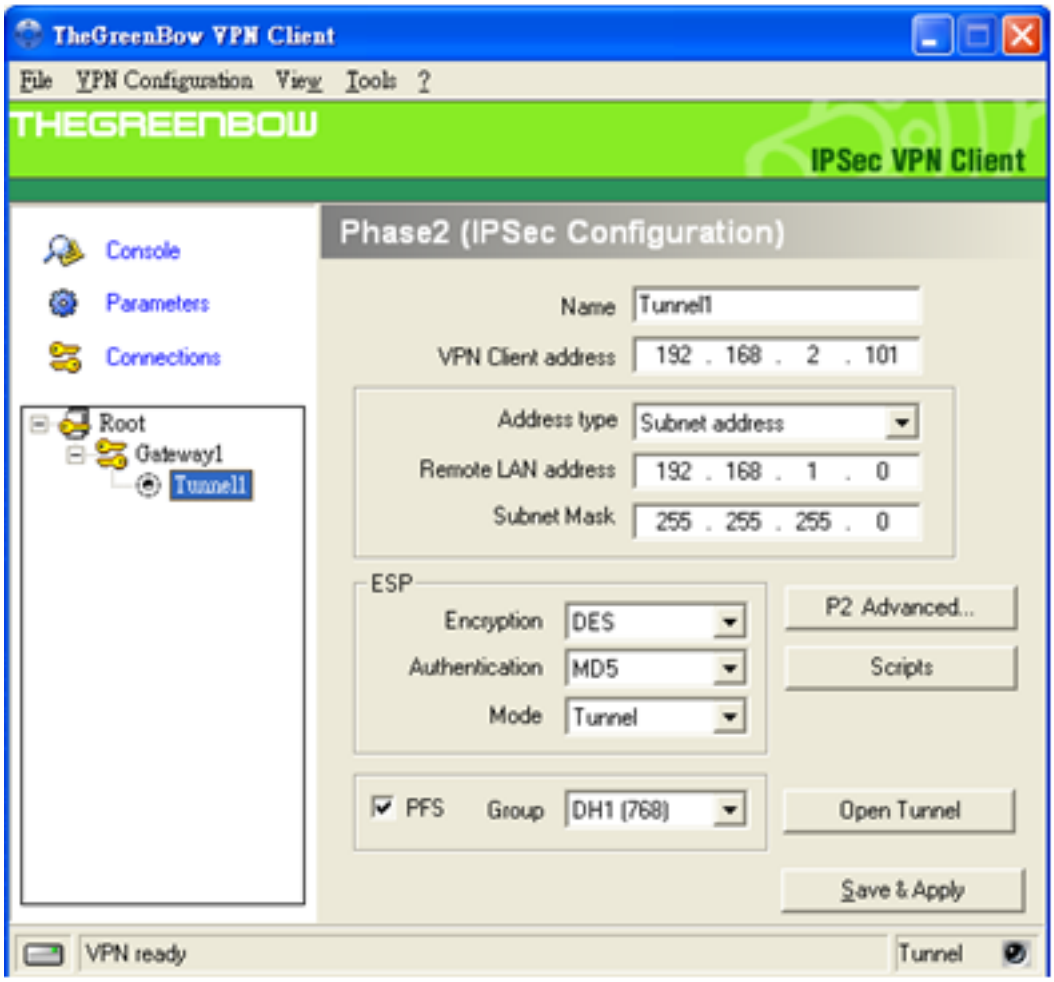
Etapa 27. Escolha **Forçado** na lista suspensa NAT-T.

Etapa 28. Escolha **Endereço IP** na lista suspensa ID local e ID remoto.

Etapa 29. No campo ID local, insira o endereço IP da WAN do roteador.

Etapa 30. No campo ID remoto, insira o endereço IP da WAN do roteador remoto.

Etapa 31. Click **OK**.



Etapa 32. Clique em **Tunnel1** para definir as configurações de Phase2.

Etapa 33. No campo de endereço do VPN Client, insira o endereço IPv4 do roteador.

Etapa 34. Escolha **Endereço de sub-rede** na lista suspensa Tipo de endereço.

Etapa 35. No campo Endereço da LAN remota, insira o endereço da LAN do roteador remoto.

Etapa 36. No campo Máscara de sub-rede, insira a máscara de sub-rede do roteador remoto.

Etapa 37.Clique em **Salvar e aplicar**.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.