

Configuración de C2G con software Greenbow en routers VPN RV016, RV042, RV042G y RV082

Objetivos

C2G (cliente a puerta de enlace) se configura en el cliente TheGreenBow mediante la página de configuración de puerta de enlace a puerta de enlace, donde está presente la opción NAT-T. TheGreenBow es un software centrado en proporcionar software de seguridad empresarial basado en un conjunto de aplicaciones completamente seguro. TheGreenBow ha desarrollado un software de seguridad empresarial que facilita el acceso remoto y permite a los usuarios remotos acceder a su red corporativa de forma segura.

Este documento explica cómo configurar IPSec VPN C2G con el software Greenbow en los routers VPN RV016, RV042, RV042G y RV082.

Dispositivos aplicables

- RV016
- RV042
- RV042G
- RV082

Versión del software

- v4.2.1.02

Configuración de software de C2G y GreenBow

Paso 1. Inicie sesión en la utilidad de configuración del router para seleccionar VPN > Gateway to Gateway. Se abre la página Gateway to Gateway:

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Desplácese hacia abajo hasta el área Configuración de grupo local.

Local Group Setup

Local Security Gateway Type :

IP Address : 59.105.113.180

Local Security Group Type :

IP Address :

Subnet Mask :

Paso 2. Elija IP Only en la lista desplegable Local Security Gateway Type.

Paso 3. Elija Subnet en la lista desplegable Local Security Group Type.

Paso 4. En el campo IP Address (Dirección IP), introduzca la dirección IP del router.

Paso 5. En el campo Subnet Mask (Máscara de subred), introduzca la máscara de subred

del router.

Paso 6. Desplácese hacia abajo para ir al área Remote Group Setup (Configuración de grupo remoto) de la página.

Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 59.105.113.148

Remote Security Group Type : IP

IP Address : 192.168.2.101

Paso 7. Elija IP Only en la lista desplegable Remote Security Gateway Type.

Paso 8. Elija el tipo de dirección IP en la lista desplegable Remote Security Gateway IP Address Type .

Paso 9. En el campo IP Address (Dirección IP), introduzca la dirección IP de WAN del router remoto.

Paso 10. Seleccione IP en la lista desplegable Remote Security Group Type.

Paso 11. En el campo IP Address (Dirección IP), introduzca la dirección IPv4 del router.

IPSec Setup

Keying Mode : IKE with Preshared key ▼

Phase 1 DH Group : Group 1 - 768 bit ▼

Phase 1 Encryption : DES ▼

Phase 1 Authentication : MD5 ▼

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit ▼


Phase 2 Encryption : DES ▼

Phase 2 Authentication : MD5 ▼

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

Paso 12. Elija IKE with Preshared key en la lista desplegable Keying Mode.

Paso 13. Elija Group 1- 768 bit en la lista desplegable Phase 1 DH Group.

Paso 14. Elija DES en la lista desplegable Phase 1 Encryption.

Paso 15. Elija MD5 en la lista desplegable Phase 1 Authentication.

Paso 16. En el campo Phase 1 SA Life Time (Duración de SA de fase 1), introduzca 2800 segundos.

Paso 17. Elija Group 1- 768 bit en la lista desplegable Phase 2 DH Group.

Paso 18. Elija DES en la lista desplegable Phase 2 Encryption.

Paso 19. Elija MD5 en la lista desplegable Phase 2 Authentication.

Paso 20. En el campo Phase 2 SA Life Time, ingrese 3600 segundos.

Paso 21. En el campo Clave previamente compartida, introduzca la combinación deseada de números o letras. En este caso es "1234678".

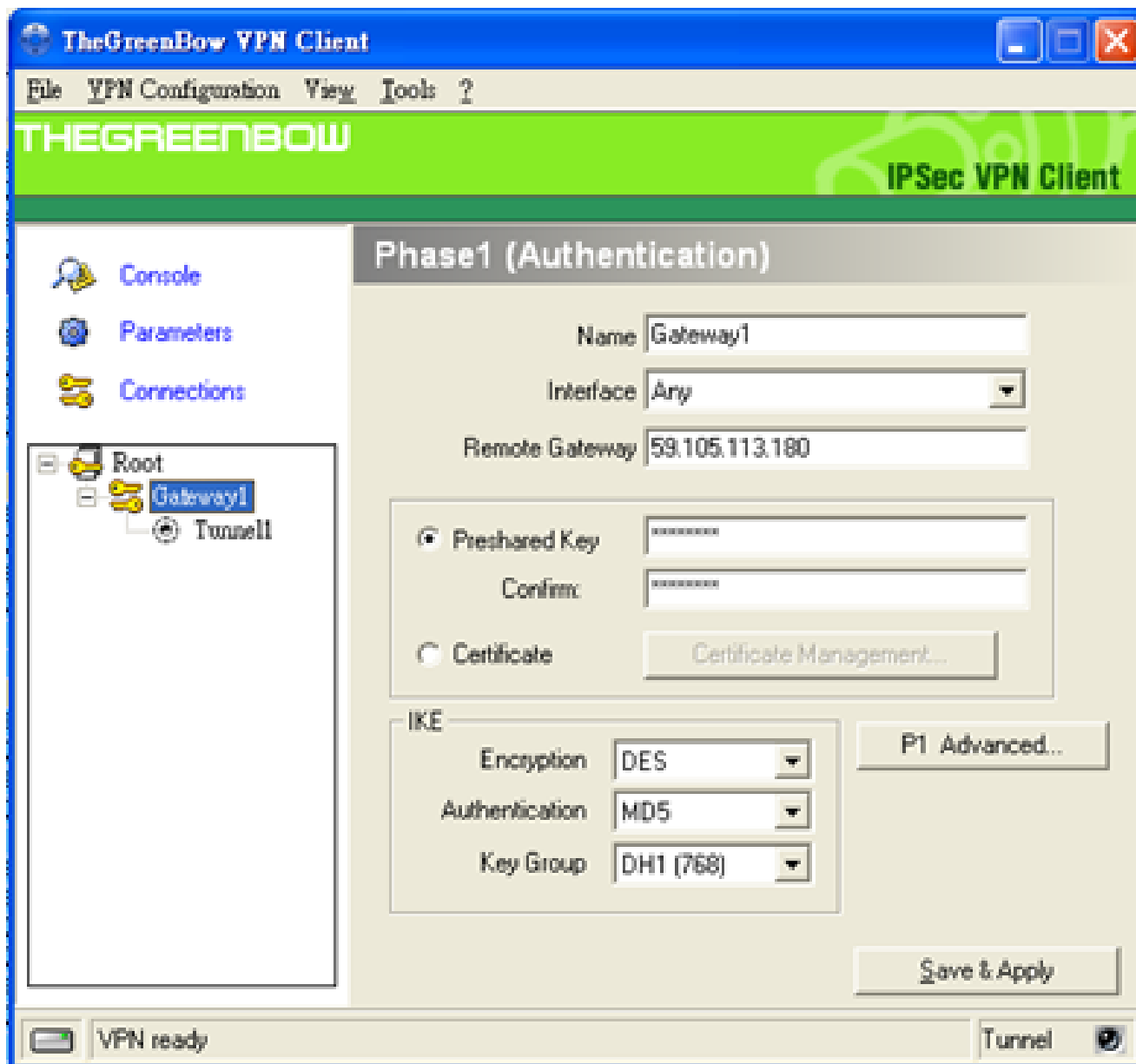
Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval seconds

Paso 22. Haga clic en Advanced +. Se abre la página Advanced:

Paso 23. Marque la casilla de verificación NAT Traversal.

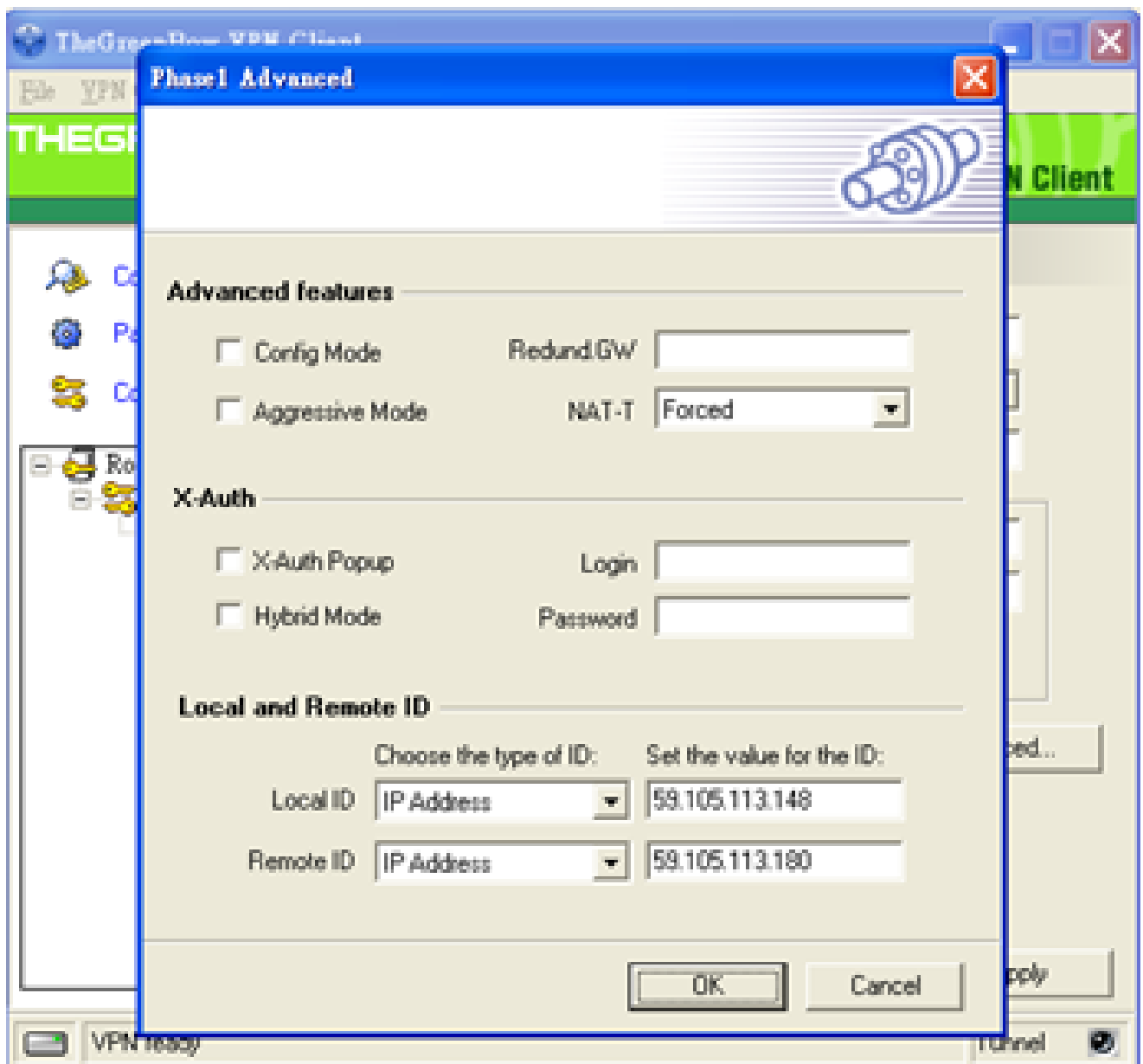
Paso 24. Inicie el software IPSec VPN Client Greenbow en el ordenador.



Paso 25. En el campo Remote Gateway (Gateway remoto), introduzca la dirección IP de WAN del router remoto.



Paso 26. Haga clic en el botón P1 Advanced. Se abre la página Phase1 Advanced:



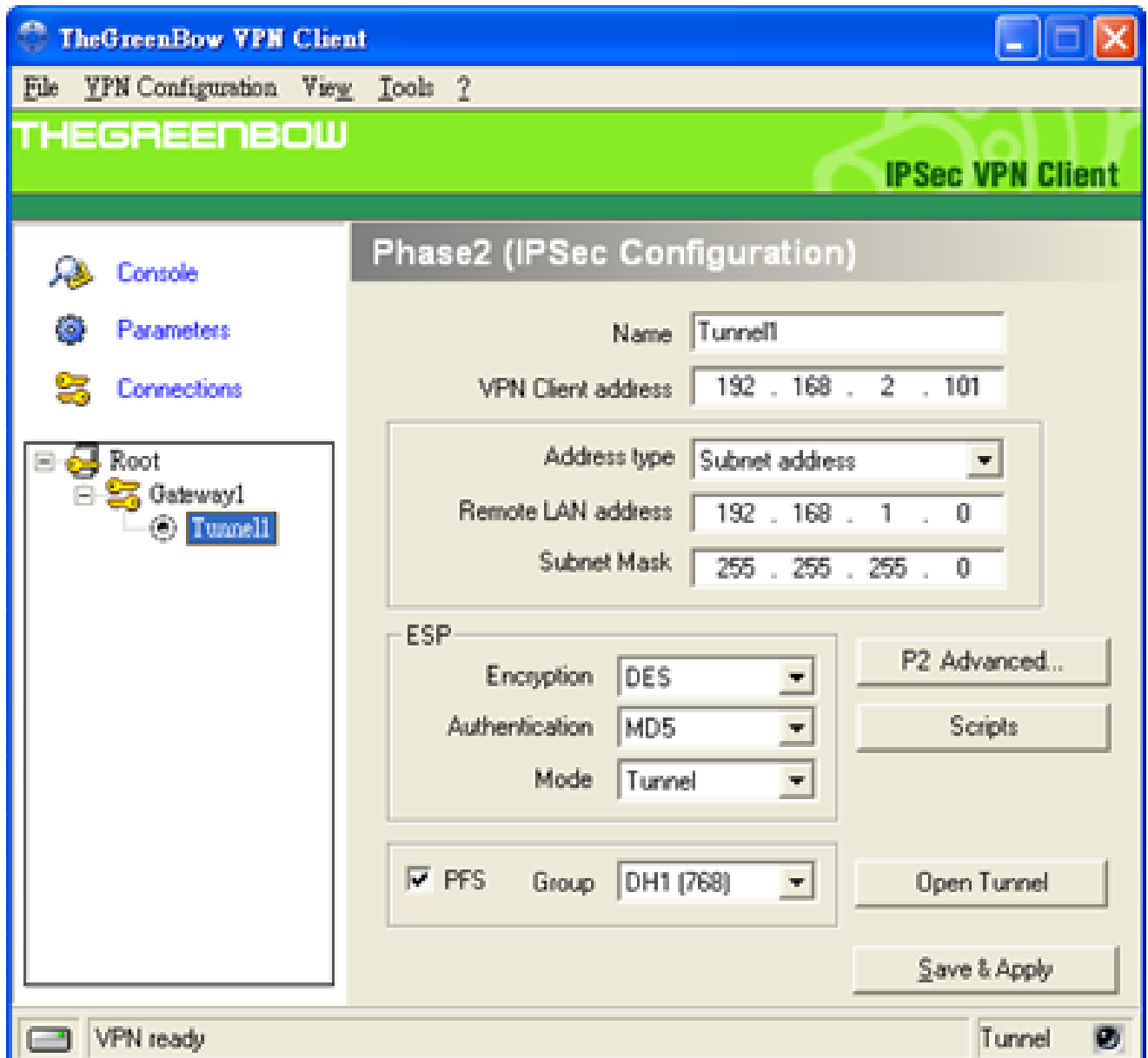
Paso 27. Elija Forced en la lista desplegable NAT-T.

Paso 28. Elija IP Address en la lista desplegable Local ID and Remote ID.

Paso 29. En el campo Local ID (ID local), introduzca la dirección IP de WAN del router.

Paso 30. En el campo Remote ID (ID remota), introduzca la dirección IP de WAN del router remoto.

Paso 31. Click OK.



Paso 32. Haga clic en Tunnel1 para configurar los parámetros de Phase2.

Paso 33. En el campo VPN Client address (Dirección de cliente VPN), introduzca la dirección IPv4 del router.

Paso 34. Elija Subnet address en la lista desplegable Address type .

Paso 35. En el campo Dirección LAN remota, introduzca la dirección LAN del router remoto.

Paso 36. En el campo Subnet Mask (Máscara de subred), introduzca la máscara de subred del router remoto.

Paso 37. Haga clic en Guardar y Aplicar.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).