Configuration of C2G with Greenbow software on RV016, RV042, RV042G and RV082 VPN Routers

Objectives

C2G (Client to Gateway) is setup on TheGreenBow client using the Gateway-to-gateway configuration page where the NAT-T option is present. TheGreenBow is a software focused on providing enterprise security software based on a completely secure suite. TheGreenBow has developed enterprise security software that makes remote access simple, allows remote users to access their corporate network securely.

This document explains the how to configure IPSec VPN C2G with Greenbow software on RV016, RV042, RV042G, and RV082 VPN Routers.

Applicable Devices

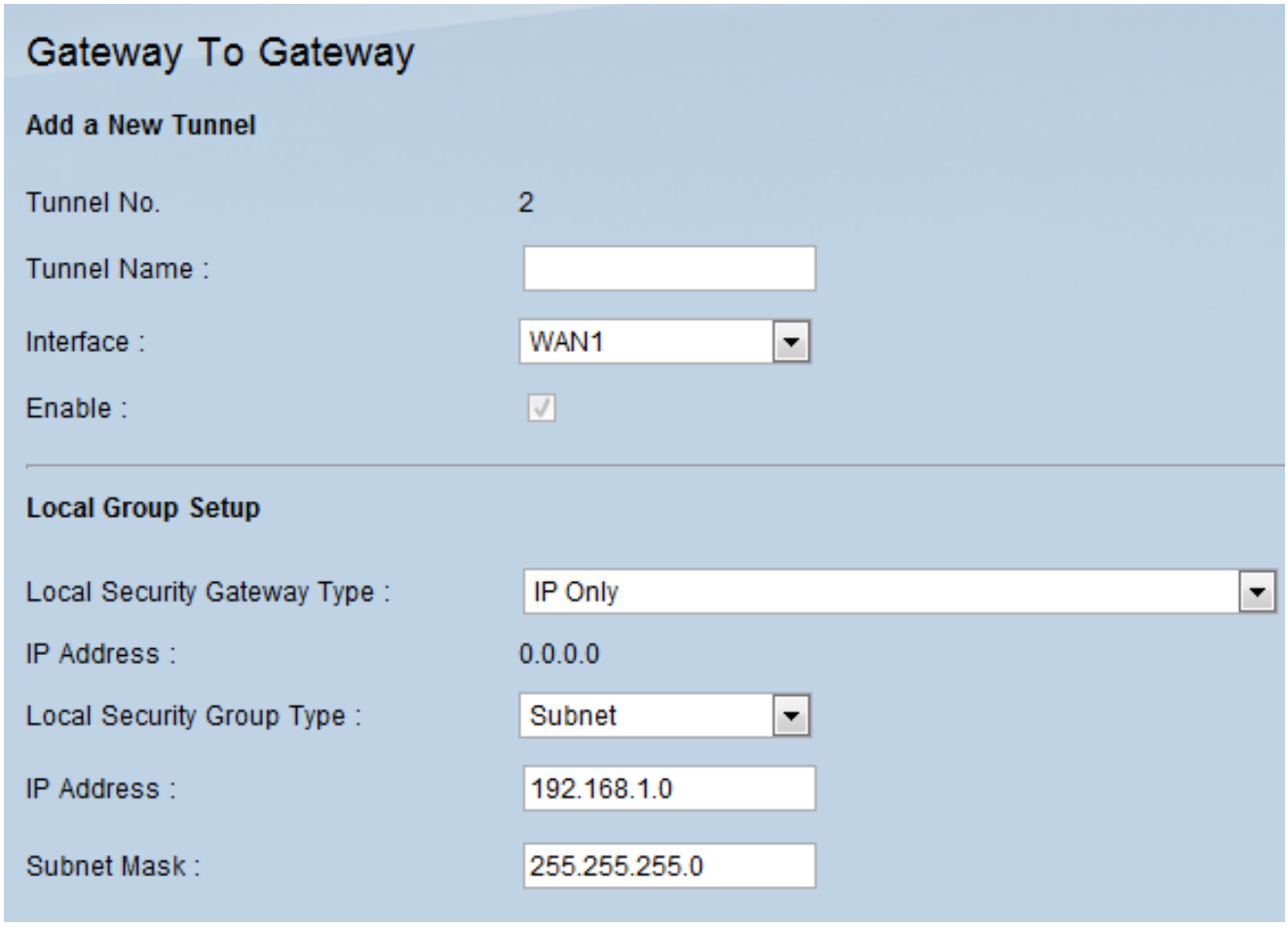
- RV016
- RV042
- RV042G
- RV082

Software Version

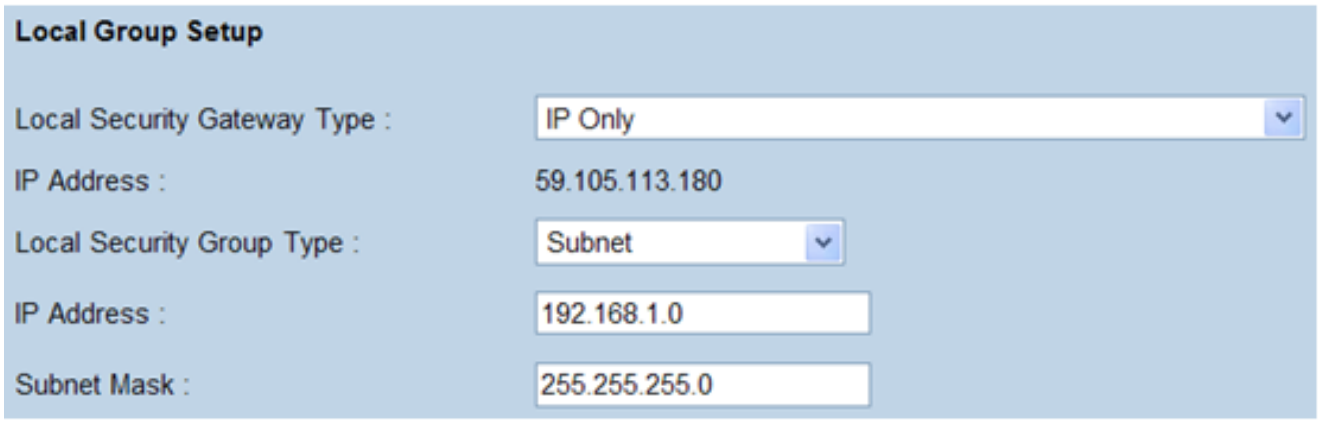
- v4.2.1.02

C2G and GreenBow Software Configuration

Step 1. Log into the Router Configuration Utility to choose **VPN > Gateway to Gateway**. The *Gateway to Gateway* page opens:



Scroll down to the Local Group Setup area.



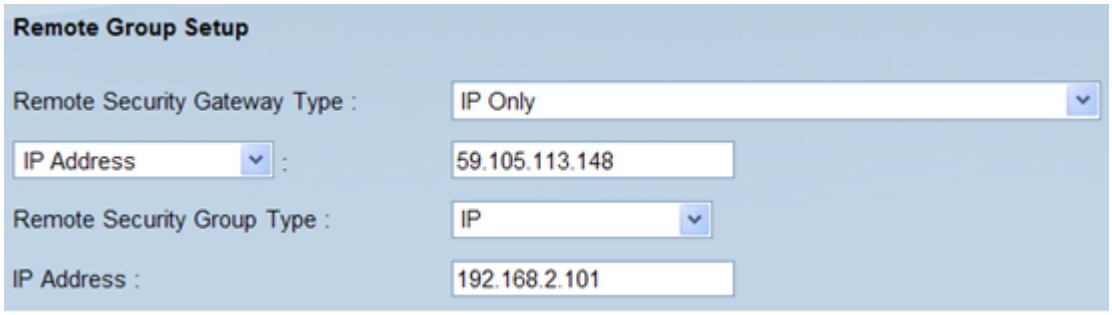
Step 2. Choose **IP Only** from the Local Security Gateway Type drop-down list.

Step 3. Choose **Subnet** from the Local Security Group Type drop-down list.

Step 4. In the IP Address field enter the IP address of the router.

Step 5. In the Subnet Mask field enter the subnet mask of the router.

Step 6. Scroll down to go to the Remote Group Setup area of the page.



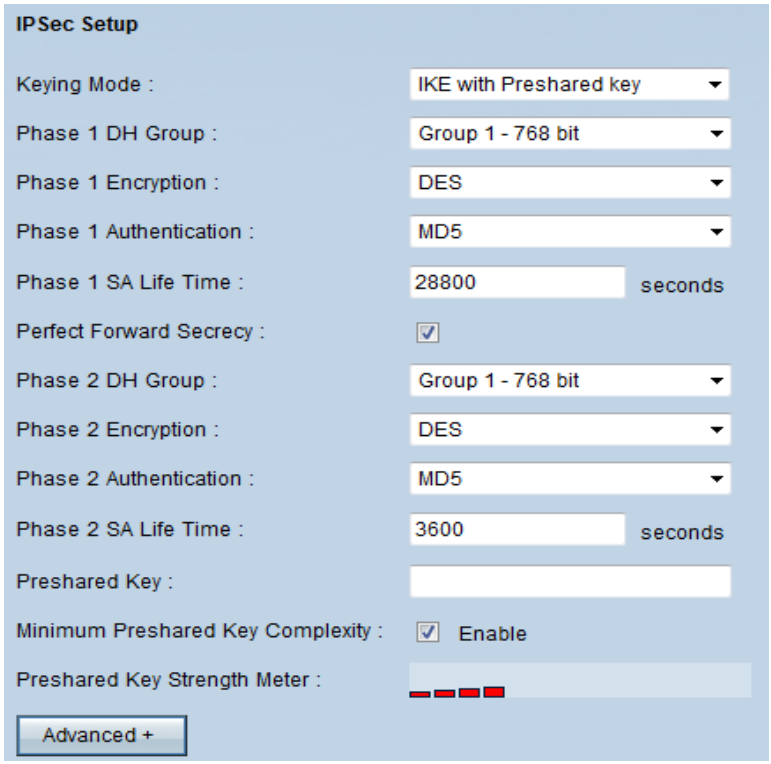
Step 7. Choose **IP Only** from the Remote Security Gateway Type drop-down list.

Step 8. Choose the **IP Address** type from the Remote Security Gateway IP Address Type drop-down list.

Step 9. In the IP Address field enter WAN IP address of the remote router.

Step 10. Select **IP** from the Remote Security Group Type drop-down list.

Step 11. In the IP Address field enter the IPv4 address of the router.



Step 12. Choose **IKE with Preshared key** from the Keying Mode drop-down list.

Step 13. Choose **Group 1- 768 bit** from the Phase 1 DH Group drop-down list.

Step 14. Choose **DES** from the Phase 1 Encryption drop-down list.

Step 15. Choose **MD5** from the Phase 1 Authentication drop-down list.

Step 16. In the Phase 1 SA Life Time field enter **28800** seconds.

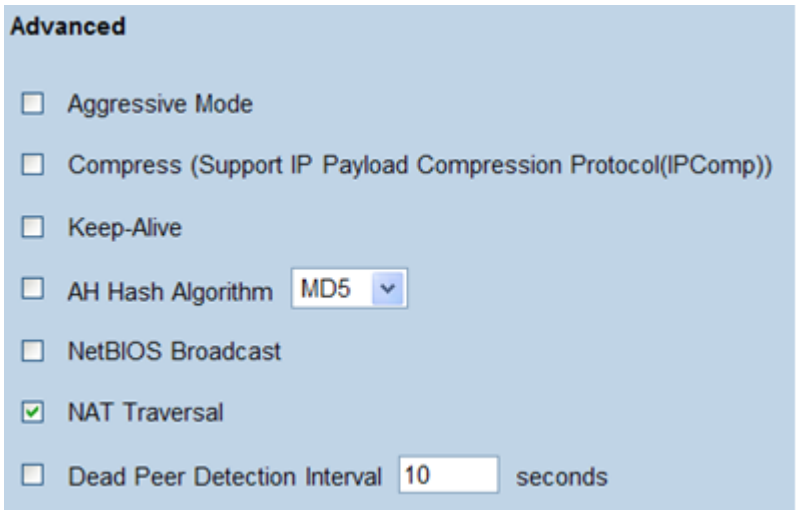
Step 17. Choose **Group 1- 768 bit** from the Phase 2 DH Group drop-down list.

Step 18. Choose **DES** from the Phase 2 Encryption drop-down list.

Step 19. Choose **MD5** from the Phase 2 Authentication drop-down list.

Step 20. In the Phase 2 SA Life Time field enter **3600** seconds.

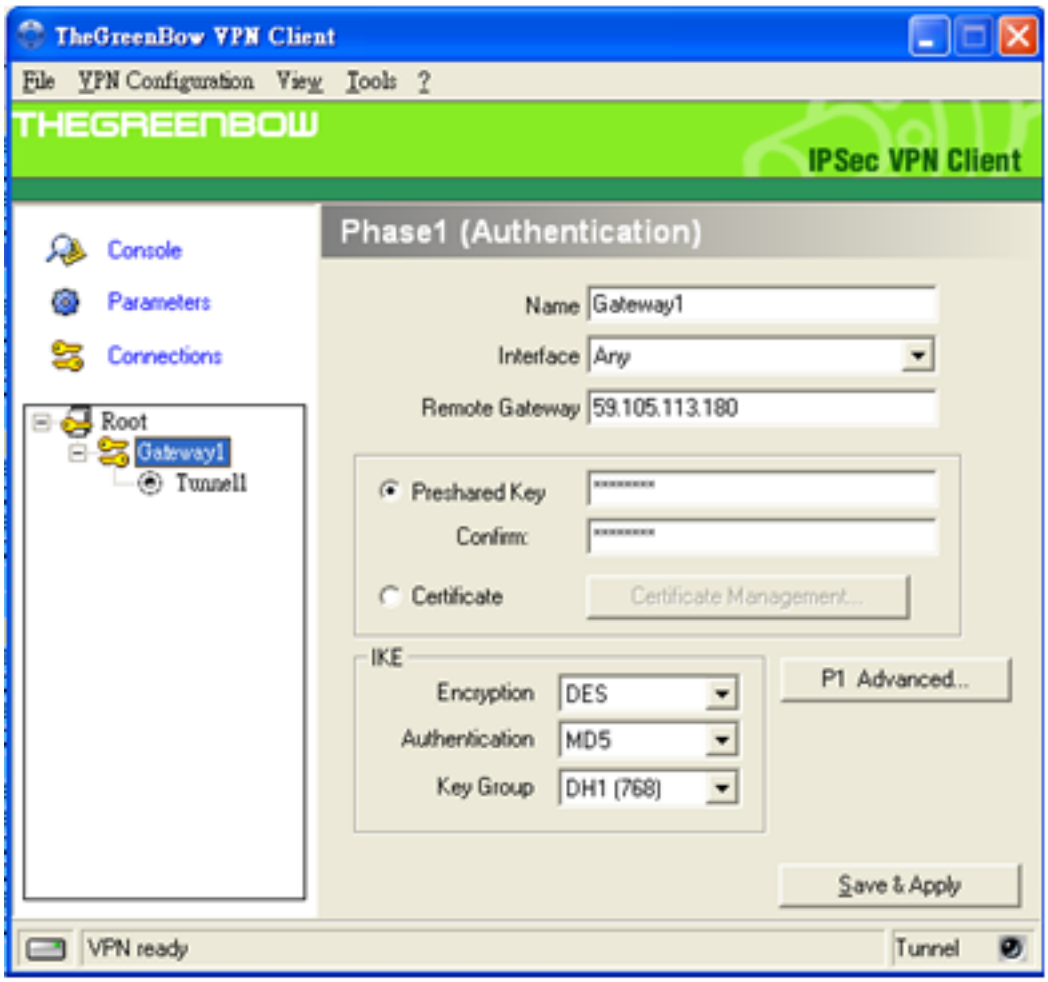
Step 21. In the Preshared Key field enter the desired combination of numbers and/or letters. In this case it is "1234678".



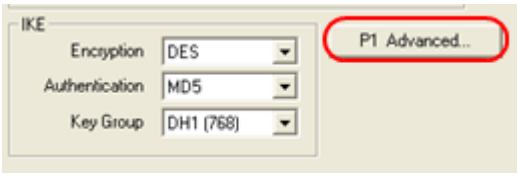
Step 22. Click **Advanced +**. The *Advanced* page opens:

Step 23. Check the **NAT Traversal** check box.

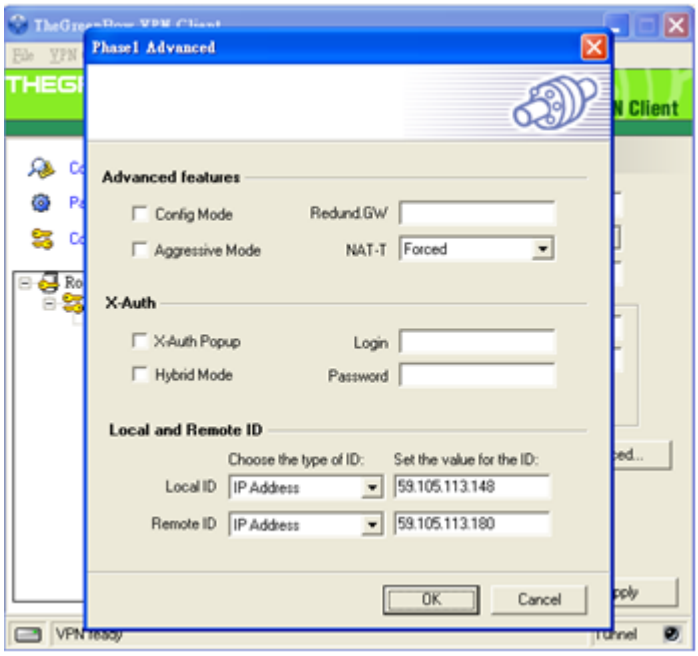
Step 24. Launch the IPSec VPN Client Greenbow software on your computer.



Step 25. In the Remote Gateway field enter WAN IP address of the remote router.



Step 26. Click the **P1 Advanced** button. The *Phase1 Advanced* page opens:



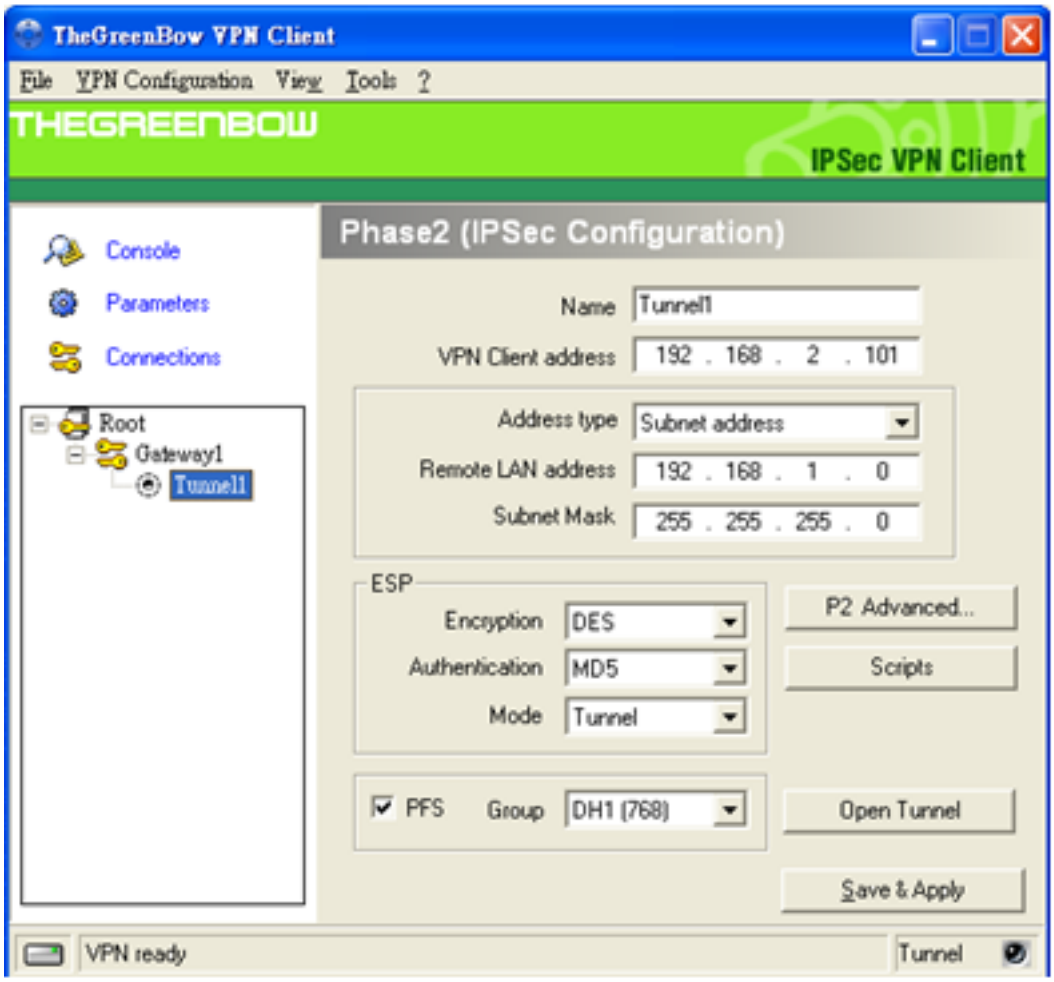
Step 27. Choose **Forced** from the NAT-T drop-down list.

Step 28. Choose **IP Address** in the Local ID and Remote ID drop-down list.

Step 29. In the Local ID field enter the WAN IP address of the router.

Step 30. In the Remote ID field enter WAN IP address of the remote router.

Step 31. Click **OK**.



Step 32. Click **Tunnel1** to configure the Phase2 settings.

Step 33. In the VPN Client address field enter the IPv4 address of the router.

Step 34. Choose **Subnet address** from the Address type drop-down list.

Step 35. In the Remote LAN address field enter LAN address of the remote router.

Step 36. In the Subnet Mask field enter subnet mask of the remote router.

Step 37.Click **Save and Apply**.