

Configuring Snapgear Router as a Firewall and VPN

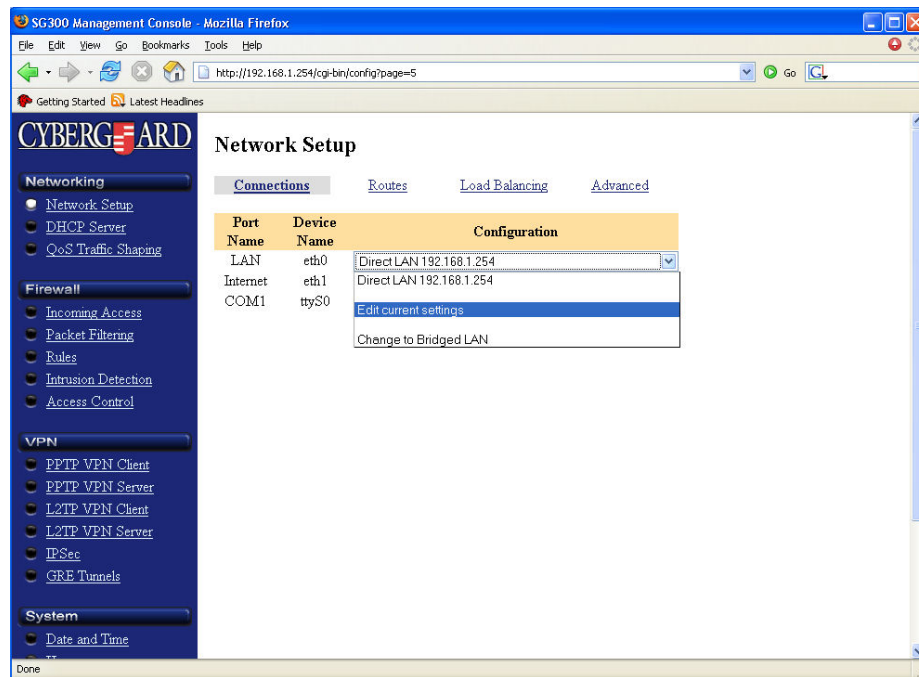
1. By default the snapgear has an IP address of 192.168.0.1
2. Configure your pc or server to an address on this network, and open the IP in a web browser
3. Click on Network Setup on the left.



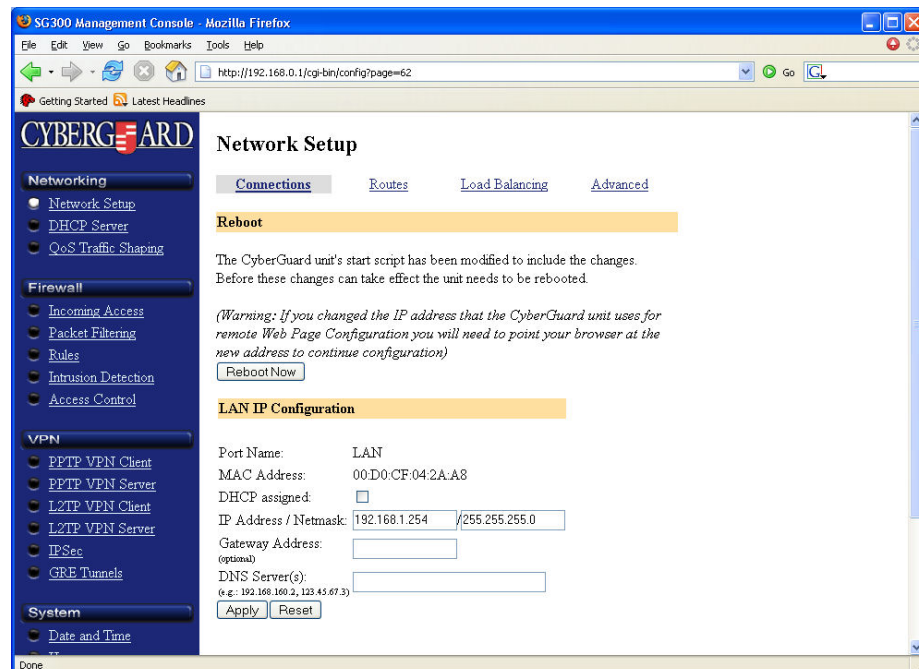
4. You should now be prompted for a username and password. The default username is root, and the password is default.
5. After logging in, you will be prompted to change the password. Do so now. Configure the password to the standard Root password for a linux server.



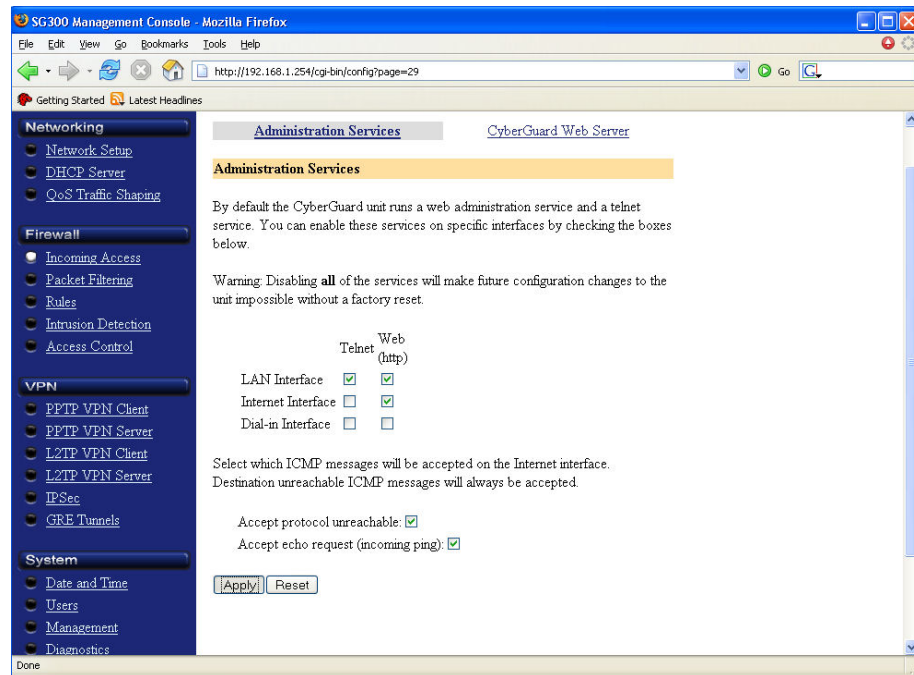
6. Click Apply. This will take you to your interface configuration screen.
7. On LAN, click the drop down menu and choose Edit Current Settings. Since you just changed the password, you will be prompted for the username and password again..



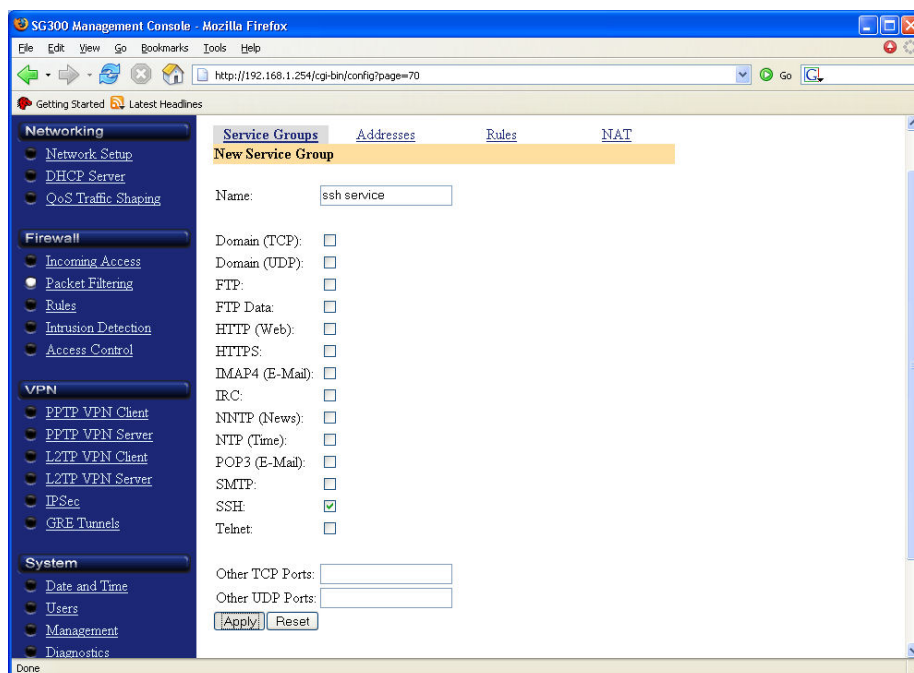
8. Type in the LAN IP and subnet for the router. This will usually be 192.168.1.254/255.255.255.0. Then click Apply, and Reboot Now.



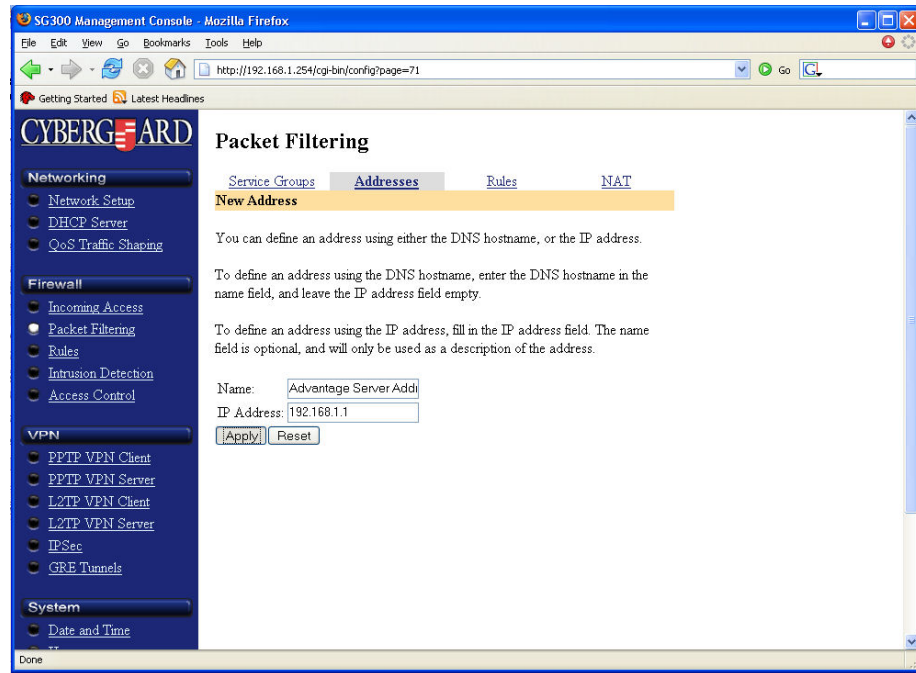
9. Input the new IP address in your web browser, then click on Incoming Access.
10. You will be asked to login. This is root, and the password you setup earlier.
11. Make sure that both columns (telnet and web) are checked for the LAN Interface, neither are checked for the Dial-in Interface, and that Web is checked for the WAN Interface. Put a check in Accept Echo Requests, then click Apply.



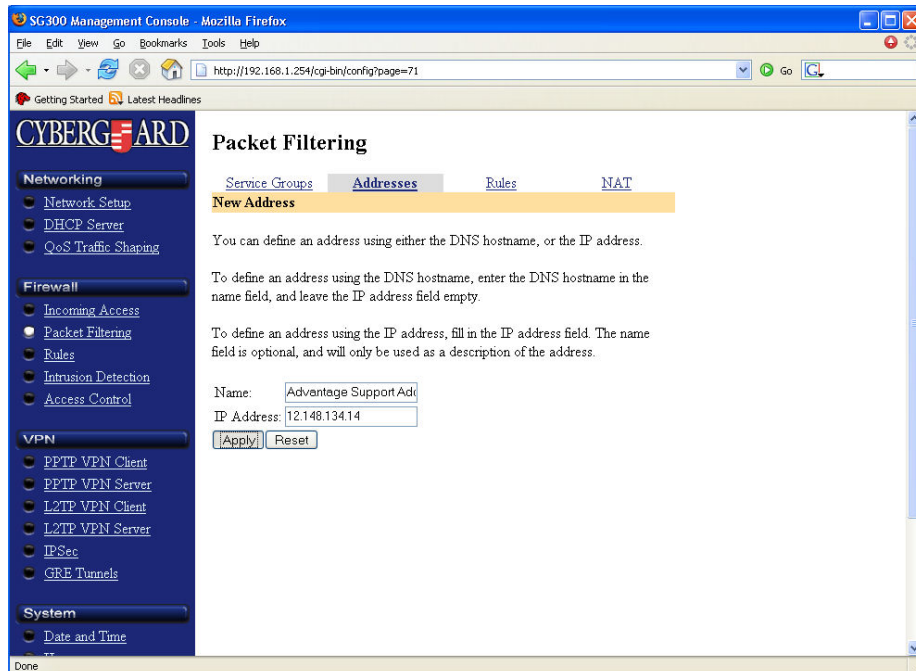
12. Click on Packet Filtering on the left. Then click on Service Groups at the top.
13. Create a New service called SSH Service. Choose the Check box next to SSH and click Apply.



- Click on Addresses at the top, and add a New Address. Call it Advantage Server Address, and put in the IP of the Advantage Server (usually 192.168.1.1), then click Apply.

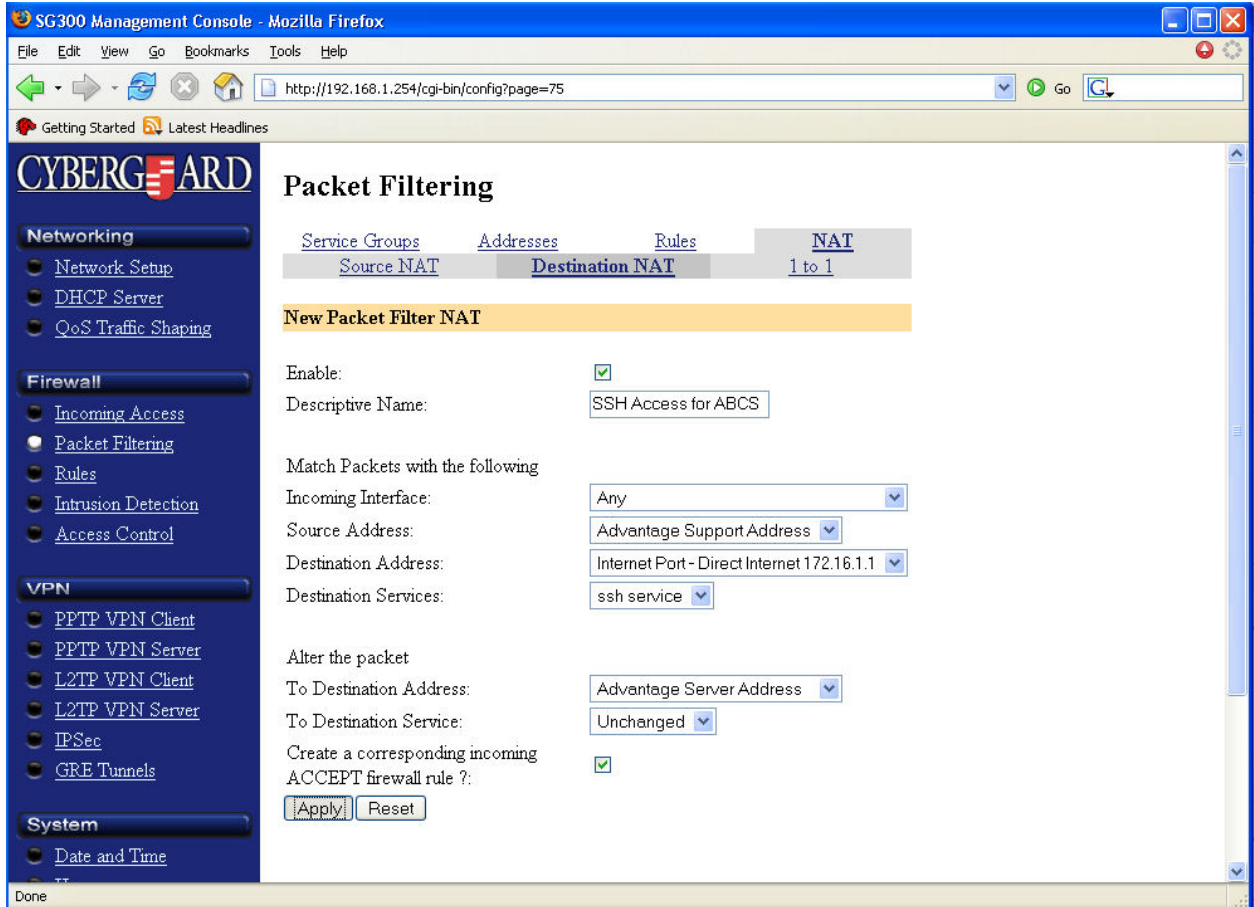


- Click New name it Advantage Support Address. This will be our Internet IP Address, which is 12.148.134.14. Click Apply to save.

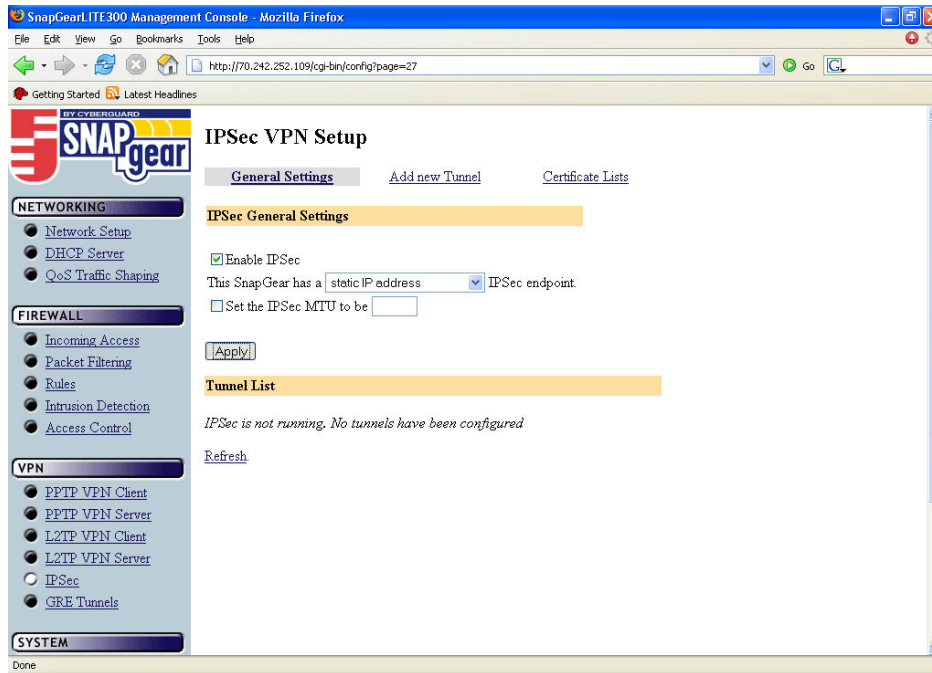


- Click on NAT at the top, then Destination NAT

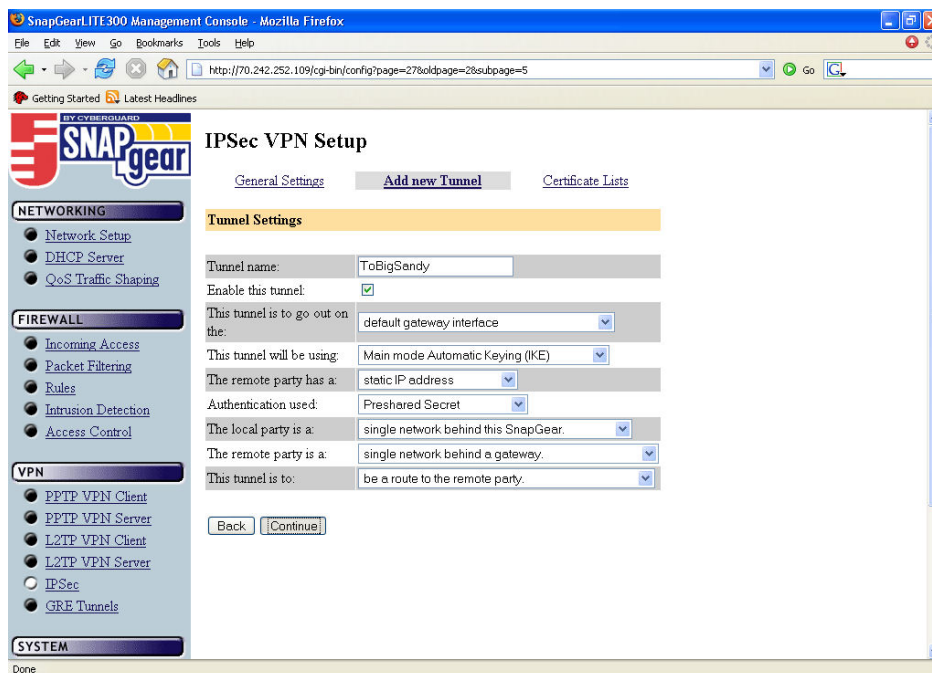
17. Set the Name to SSH Access for ABCS. The Incoming Interface is Any, Source Address you should choose Advantage Support Address, Destination Address should be the Internet Port, Destination Service should be SSH Service. After the packet: To Destination Address should be Advantage Server Address, and To Destination Service should be unchanged. Ensure there is a check for Create a corresponding incoming ACCEPT firewall rule, and click Apply to save.



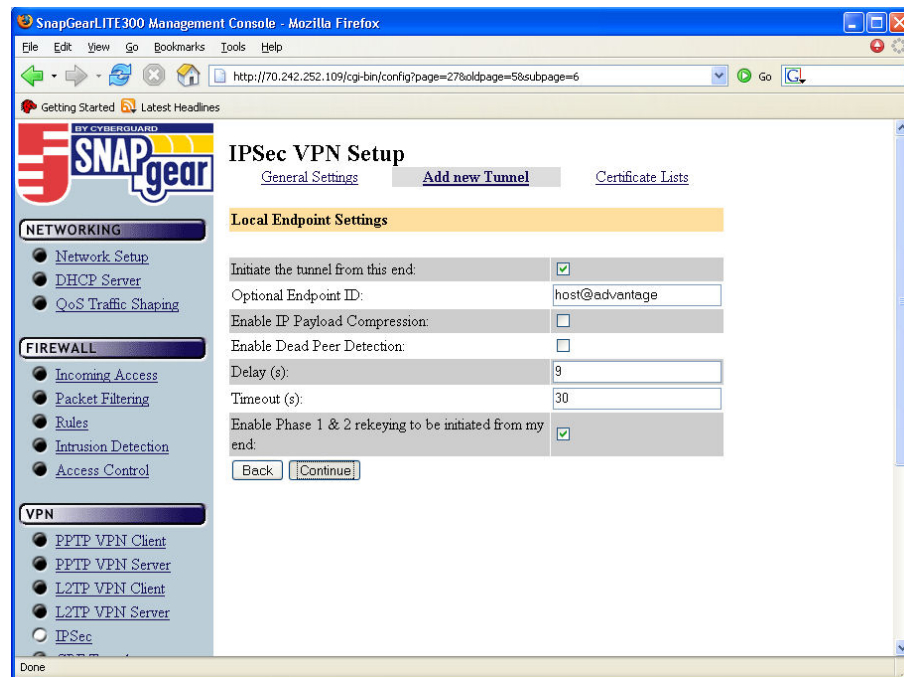
18. On the left hand side, Click on IPsec.
19. Verify that Enable IPsec is checked, and This SnapGear has a Static IP Address is chosen.



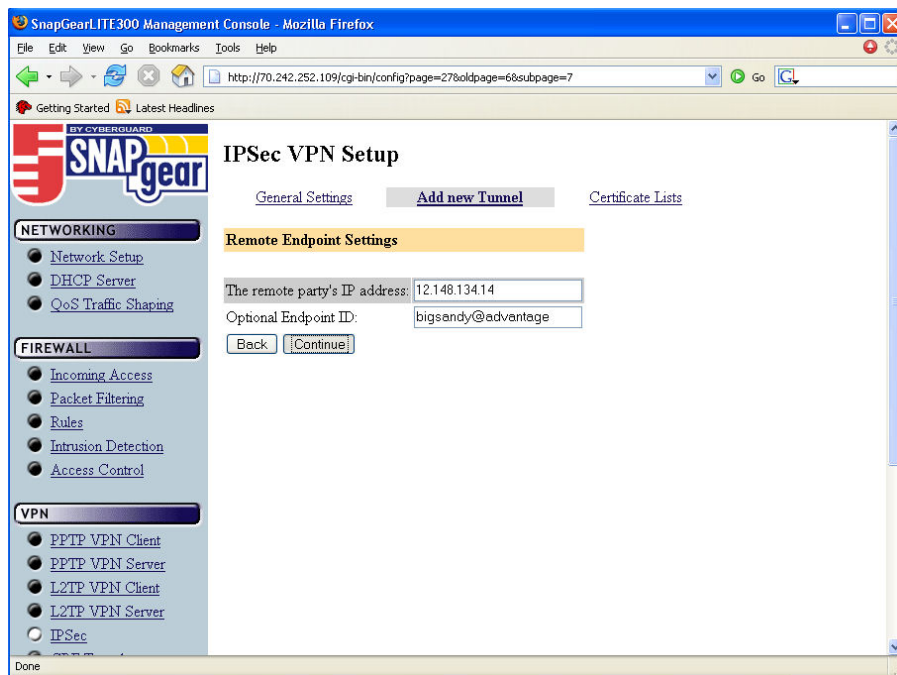
20. Click on Add new Tunnel, and name it ToCity where City is the name of the city the other snapgear is in. All other settings should remain the same, but you can verify them: Enable this Tunnel should be checked, This Tunnel goes out on the: default gateway interface, This tunnel will be using: Main mode Automatic Keying (IKE), The remote party has a: static IP address, Authentication used: Preshared Secret, The local party is a: single network behind this SnapGear, The remote party is a: single network behind a gateway, and This tunnel is to: be a route to the remote party. Then click Continue. **NOTE: All references to remote location is remote to the snapgear, not to the server. If this snapgear is at a customer's remote location, this will be referring to the MAIN location. All References to Local is the location of the snapgear.**



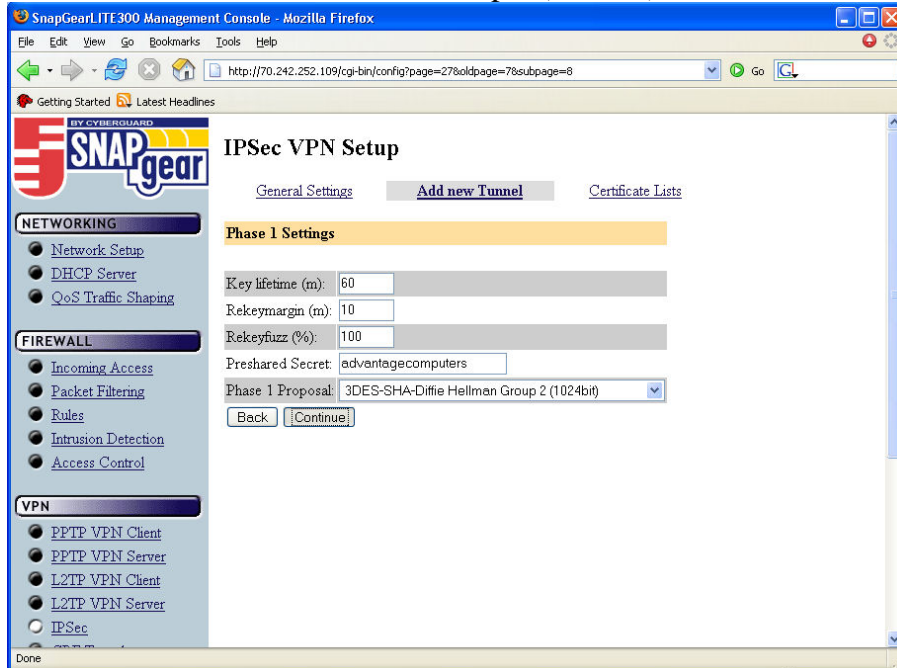
21. On Local Endpoint Settings, Ensure that Initiate the Tunnel from this end is checked. Set the Optional Endpoint ID to [host@companyname](#) for the host location, or [city@companyname](#) for remote location. Enable IP Payload Compression and Dead Peer Detection can both be unchecked. Delay should be 9, and timeout of 30. Enable Phase 1 and 2 rekeying from this end: should be checked. Click Continue.



22. Remote Endpoint Settings: In The Remote party's IP address: put in the internet IP address of the remote location. Set the Optional Endpoint ID to [host@companyname](#) for the host location, or [city@companyname](#) for remote location.
NOTE: All references to remote location is remote to the snapgear, not to the server. If this snapgear is at a customer's remote location, this will be referring to the MAIN location. All References to Local is the location of the snapgear.

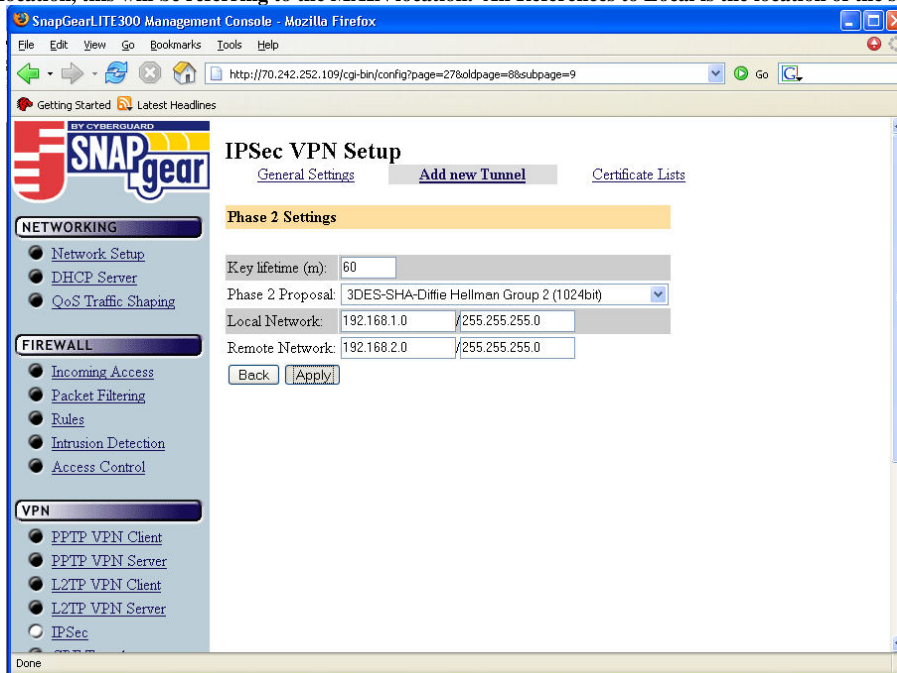


23. Phase 1 Settings: Key Lifetime: should be 60, rekey margin: should be 10, rekey fuzz: should be 100, Preshared Secret: should be advantagecomputers, and Phase 1 Proposal: should be 3DES-SHA-Diffie Hellman Group 2 (1024bit). Hit Continue.



24. Phase 2 Settings: Key Lifetime: should be 60, Phase 2 Proposal: should be 3DES-SHA-Diffie Hellman Group 2 (1024bit), Local Network: Should be the network and subnet of the local store, and Remote Network: Should be the network and subnet of the Remote Location

NOTE: All references to remote location is remote to the snapgear, not to the server. If this snapgear is at a customer's remote location, this will be referring to the MAIN location. All References to Local is the location of the snapgear.



25. Hit Apply, and You are done. Configure the other router the same way, and the tunnel should come up.
26. When the tunnel comes up, it should show running
NOTE: You will have to click the refresh button to show the new status.
27. Label the LAN and WAN IP Addresses to the Snapgear device and box.