

**Topic / Issue:** IPSec VPN Configuration between BiGuard2/30 and IP470VPN

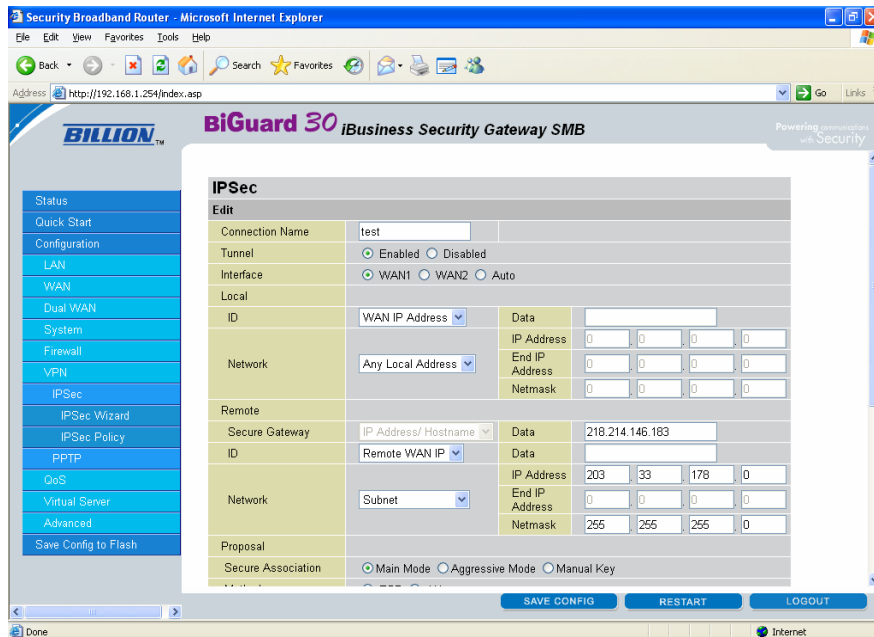
**Written By:** Steven Sismanis

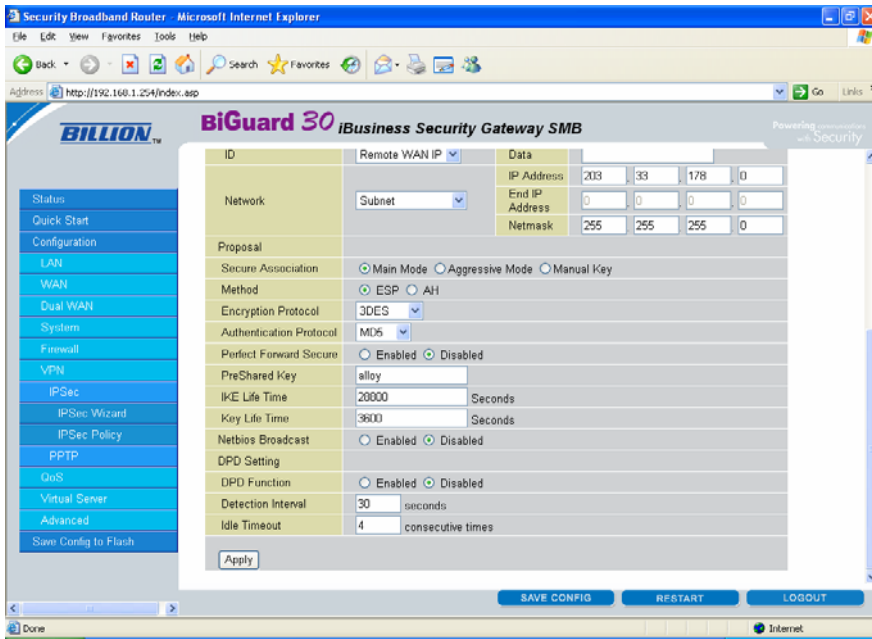
This guide assumes that both the BiGuard2/30 and IP470 have internet access and are configured with a Static WAN IP address.

### Configuration of the BiGuard2/30

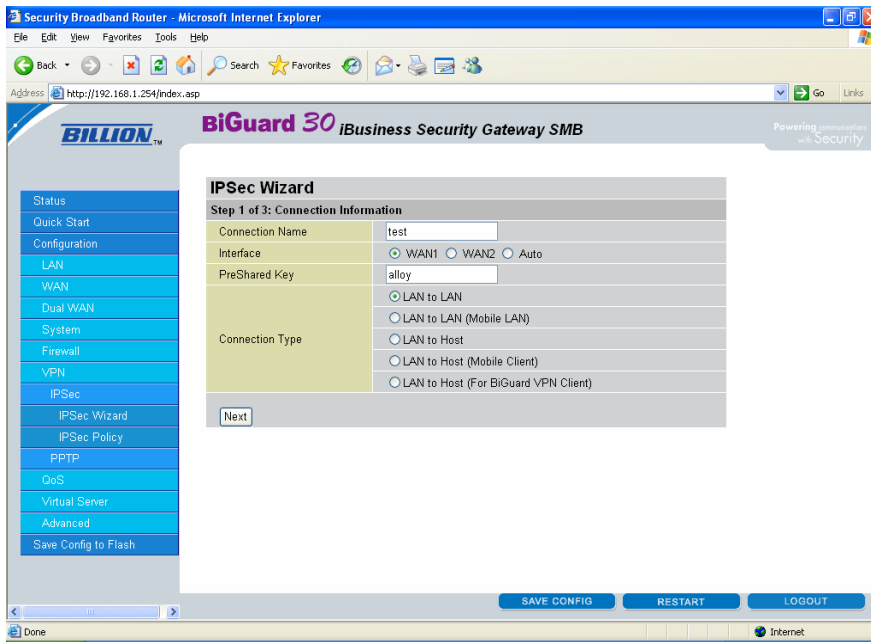
The following 2 screenshots show configuration settings for a manually configured IPSec tunnel.

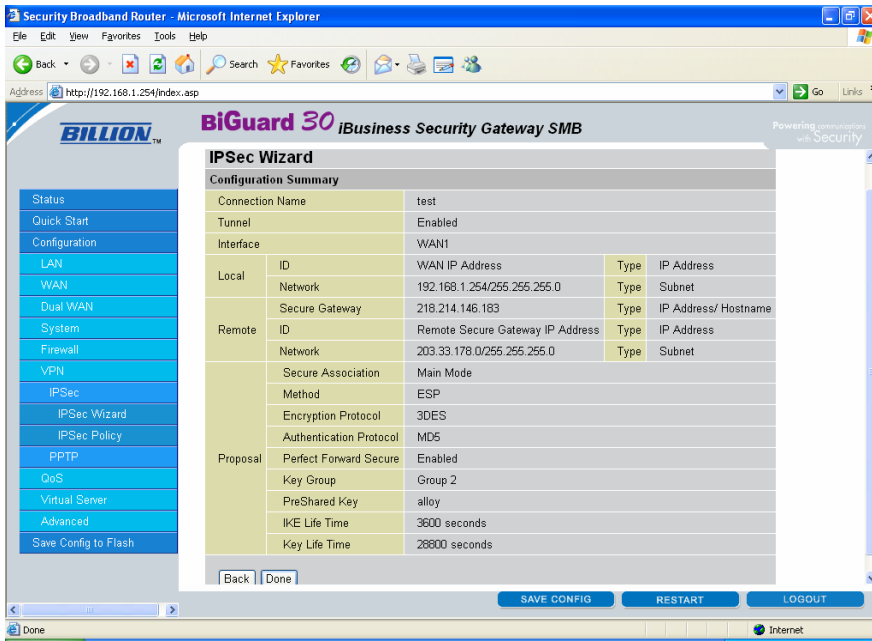
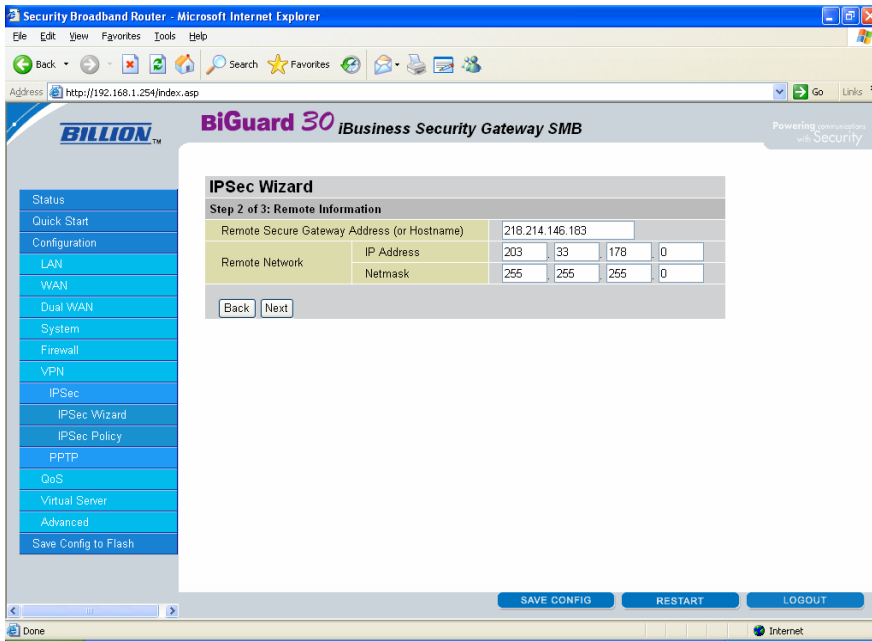
1. Give your connection a **name**
2. Select **Enable** in the Tunnel option and select **WAN1** as the interface
3. Select **WAN IP Address** for the Local ID and **Any Local Address** in the Network option, or optionally you can enter your local LAN subnet address
4. Enter the **remote WAN IP address** in the Secure Gateway field. This is the public IP address of the remote site and select **Remote WAN IP** in the ID option
5. Enter in the **remote Local network** IP address range in the Network fields
6. Select **Main Mode** in the Secure Association option
7. Set the method option to **ESP** and the Encryption and Authentication protocols to **3DES** and **MD5**
8. Give the policy a **Pre Shared Key** (which will match remote end)
9. Disable **Perfect Forward Secure, NetBIOS Broadcast** and **DPD function**
10. Apply all these settings and then Save Config at the bottom of the page





The BiGuard2/30 allows for both a manual configuration of an IPSec tunnel and also has an IPSec Wizard for a quicker setup process, however you are limited in the settings that you can configure via the wizard and you may find you need to edit the policy once configured to further customise your settings. The following 3 screenshots show the Wizard setup using the same settings as above

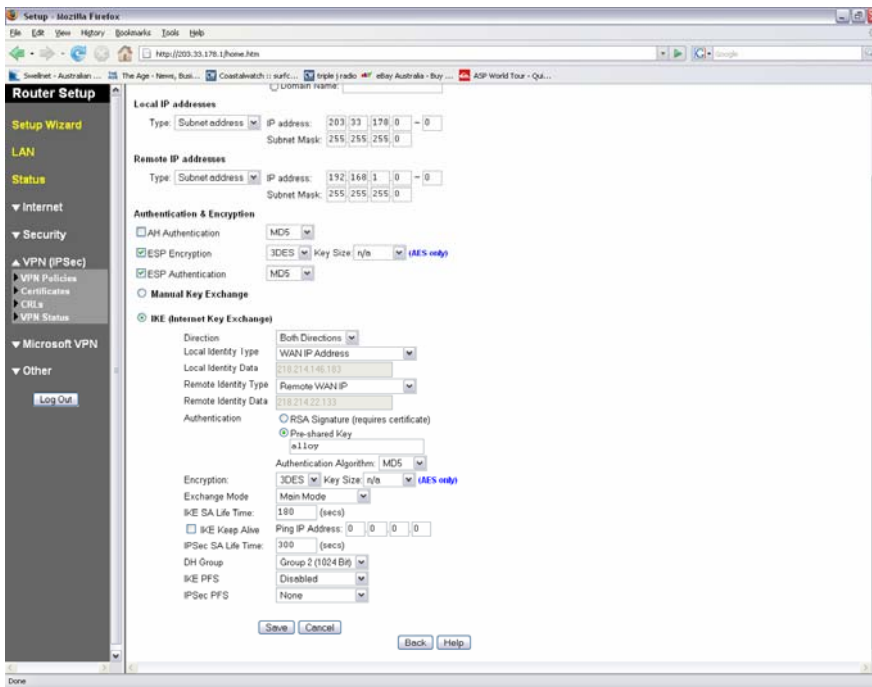
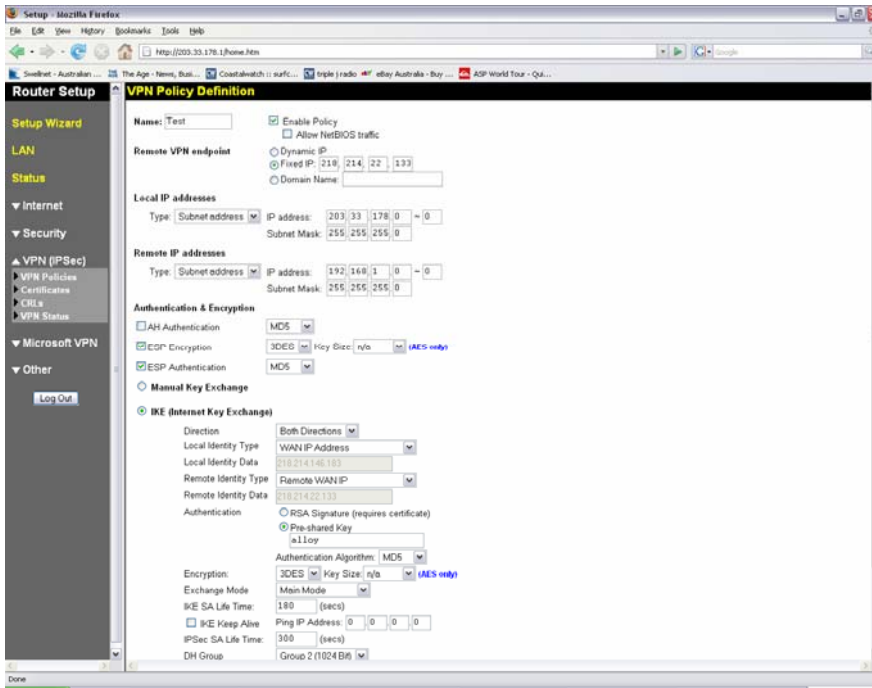




## Configuration of the IP470VPN

The following 2 screenshots show the configuration settings for an IPsec tunnel

1. Give your connection a **name** and **enable the policy**
2. Enter in the **remote WAN IP address** in the Remote VPN endpoint field
3. Enter in both the **Local and Remote IP address ranges** in their corresponding fields
4. Enable **ESP Encryption** and **ESP Authentication** and select **3DES** and **MD5**
5. Select **IKE** and set the direction to **Both Directions**, Local Identity Type will be set to **WAN IP address**, Remote Identity Type will be set to **Remote WAN IP**
6. Select **Pre-Shared Key** and enter in your matching key
7. Authentication Algorithm set to **MD5** and Encryption **3DES**
8. Exchange mode set to **Main Mode**
9. Set the DH Group to **Group 2** (must match in both devices)
10. Disable **IKE PFS** and **IPsec PFS** will be set to none
11. Save the settings



Your IPsecVPN tunnel is now configured correctly, to establish a VPN connection ping a remote pc from a local pc on your network.  
There are a couple of options for instance "allow NetBIOS traffic" that can be enabled on both devices if necessary.

**Summary:**  
(If required)