

Topic / Issue: IPSec VPN Configuration between BiGuard2/30 and Lockdown SME

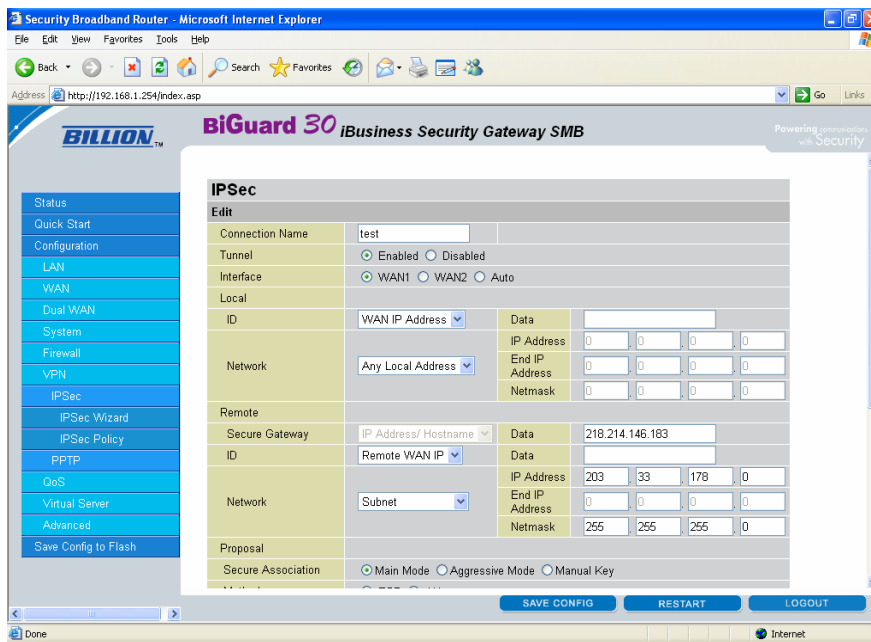
Written By: Steven Sismanis

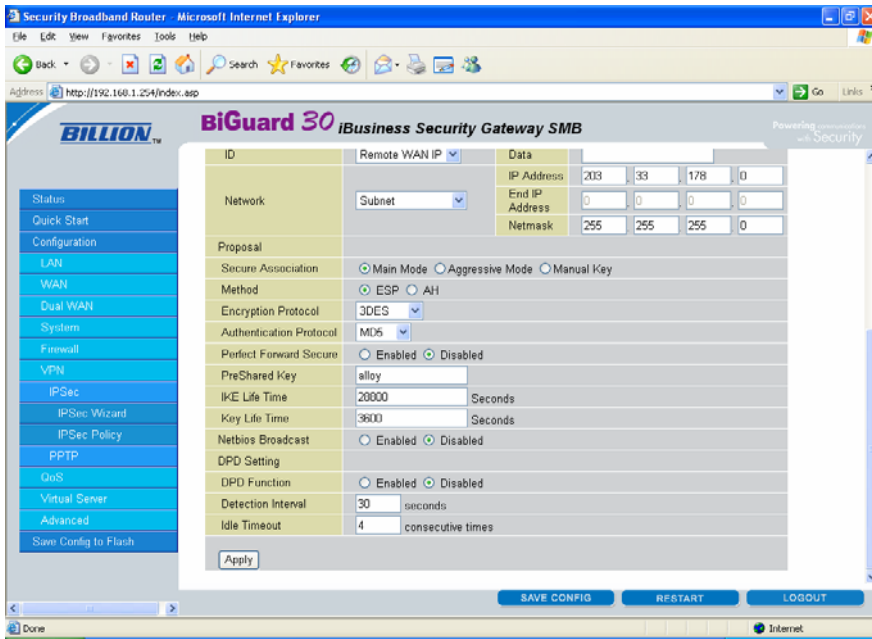
This guide assumes that both the BiGuard2/30 and Lockdown have internet access and are configured with a Static WAN IP address.

Configuration of the BiGuard2/30

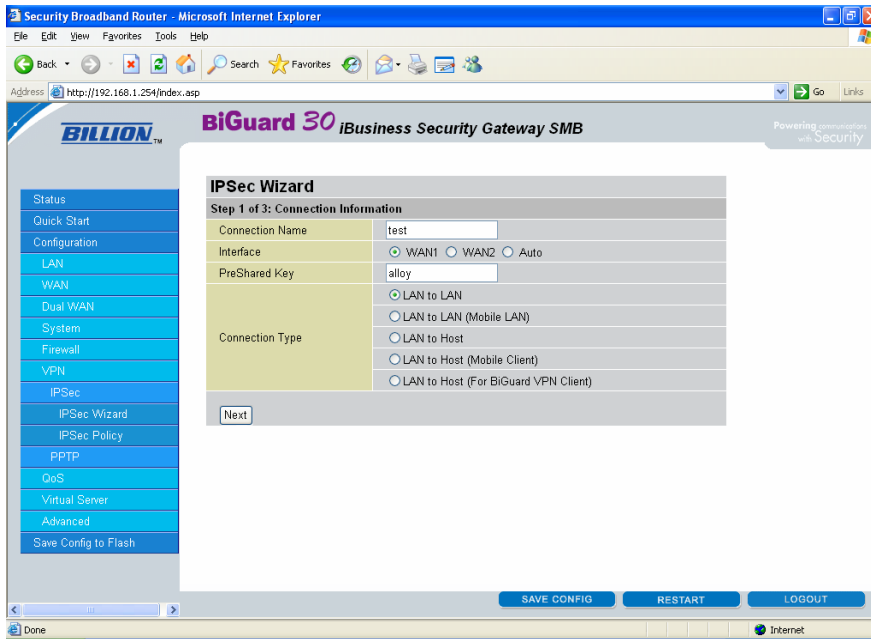
The following 2 screenshots show configuration settings for a manually configured IPSec tunnel.

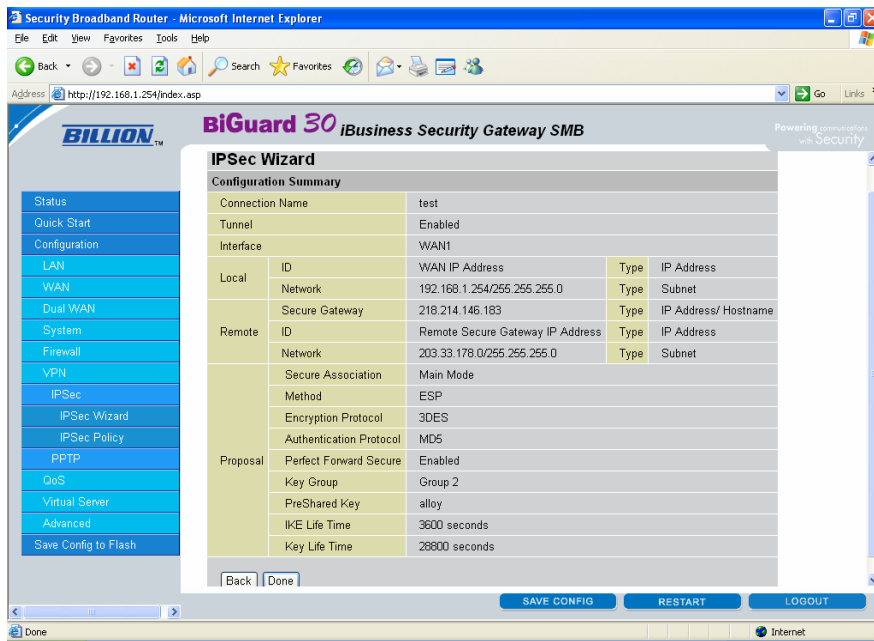
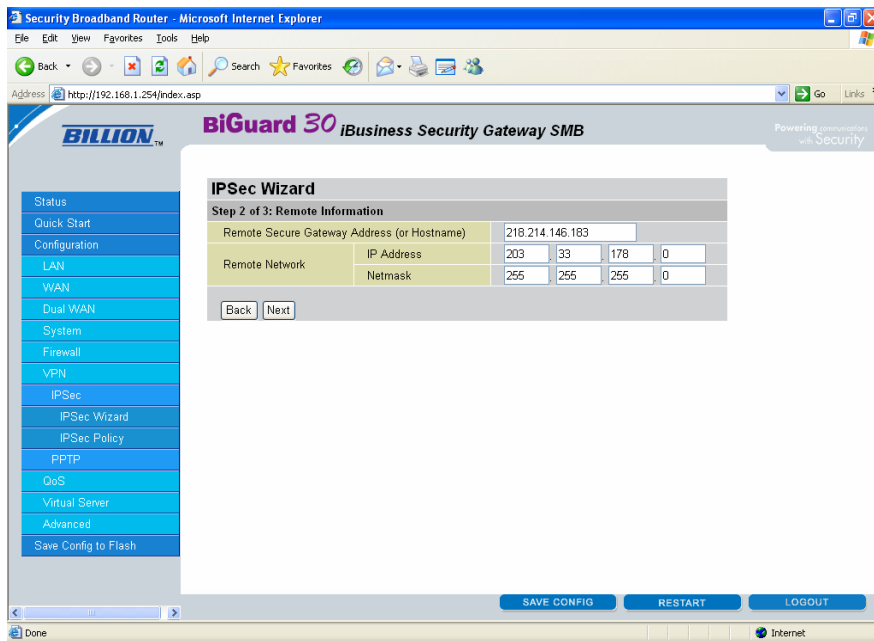
1. Give your connection a **name**
2. Select **Enable** in the Tunnel option and select **WAN1** as the interface
3. Select **WAN IP Address** for the Local ID and **Any Local Address** in the Network option, or optionally you can enter your local LAN subnet address
4. Enter in the **remote WAN IP address** 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

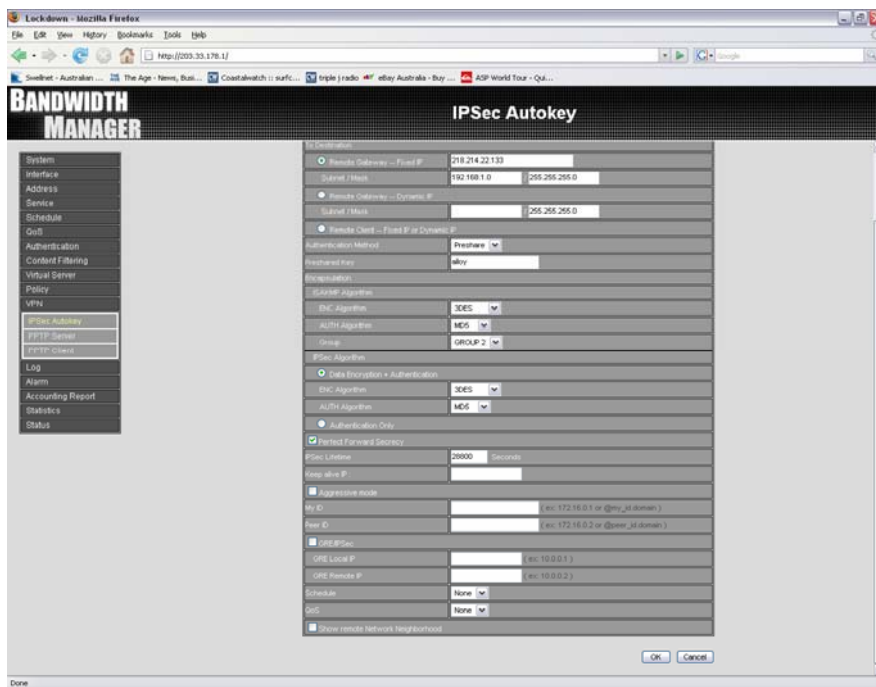
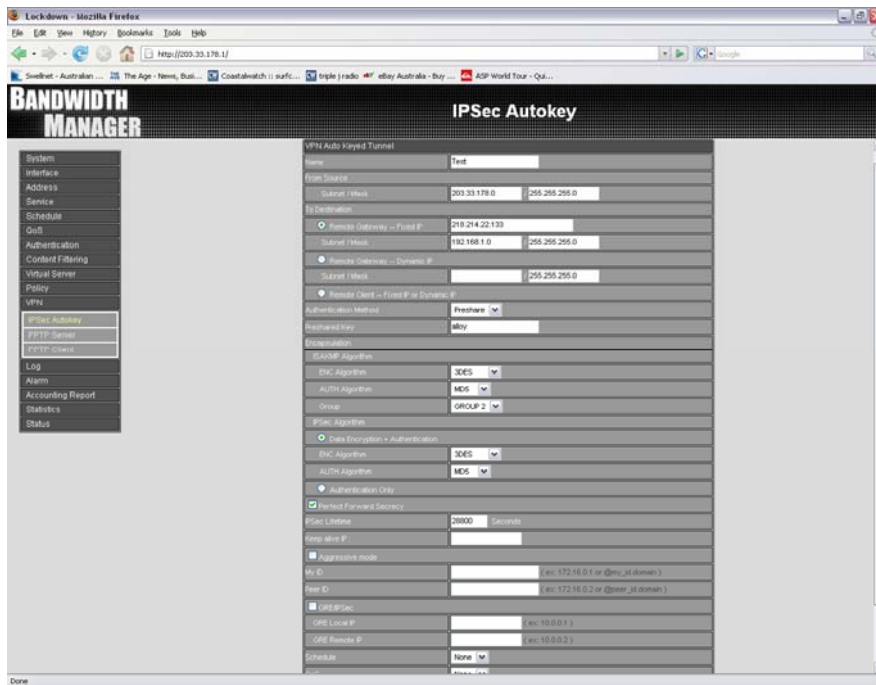




Configuration of the Lockdown SME

The following 2 screenshots show how to configure an IPsec tunnel on the Lockdown SME

1. Give the policy a **name**
2. In the from source field enter in your **local IP address and Netmask**
3. In the To Destination field enter in the **remote WAN ip address** and their **local IP address range** in the IP address and Netmask fields
4. The Authentication method will be **Preshare** and enter in your matching **Preshared Key**
5. ENC Algorithm will be **3DES**, AUTH Algorithm **MD5** and the group set to **Group 2**
6. Select Data Encryption + Authentication, ENC Algorithm will be **3DES** and AUTH Algorithm will be set to **MD5**
7. Select **Perfect Forward Secrecy** (ensure PFS is disabled if disabled in the BiGuard2/30, if you wish to use PFS, enable it on both devices)
8. Select OK



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)