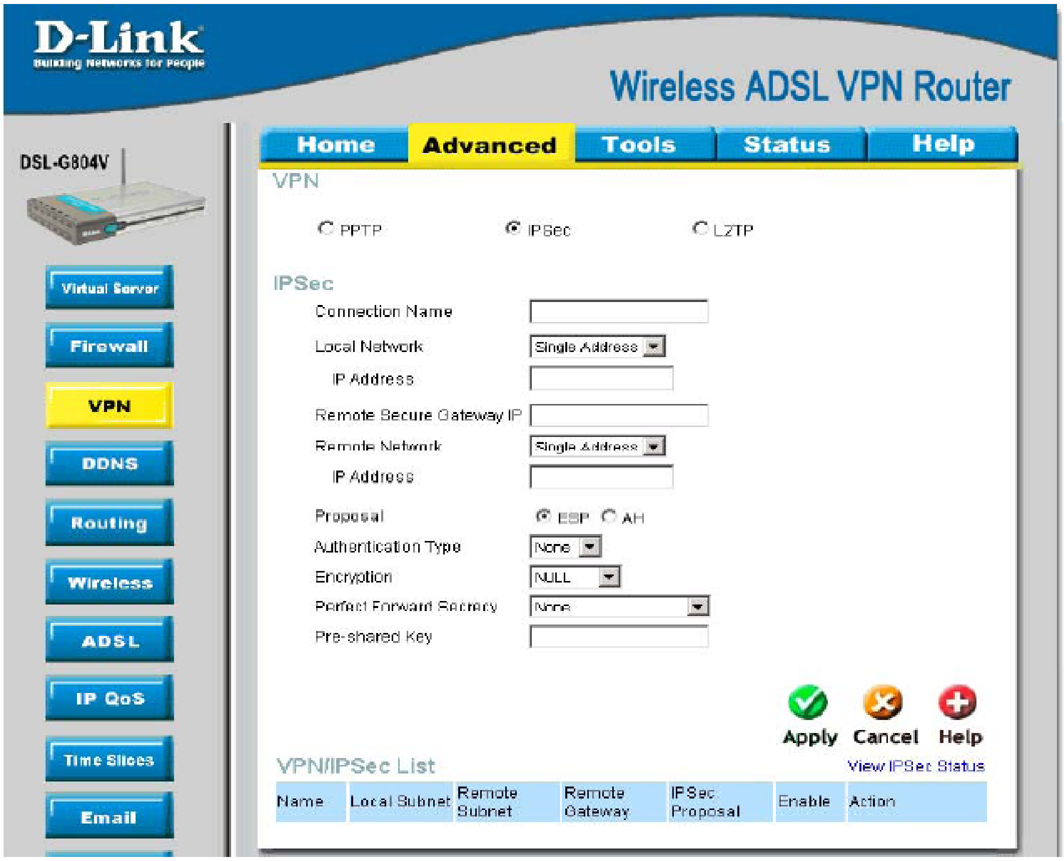
IPSec Setup DSL-G804V

IPSec (IP Security Protocol)



VPN

○ PPTP ● IPSec ○ L2TP

IPSec

Connection Name	
Local Network	Single Address
IP Address	
Remote Secure Gateway IP	
Remote Network	Single Address
IP Address	
Proposal	● ESP ○ AH
Authentication Type	None
Encryption	NULL
Perfect Forward Secrecy	None
Pre-shared Key	

VPN/IPSec List

Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Enable	Action

Figure 4-13. VPN – IPSec

Parameter	Description
Connection Name	A user-defined name for the connection. No digital number is allowed.
Local Network	Set the Single address, subnet or IP range of the local network. **IP Address:** The IP address of the local host. **Netmask:** The subnet of the local network. For example, IP: 192.168.0.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.0.1 (i.e. 192.168.1.1 through to 192.168.1.254) **End IP:** The IP address range of the local network. For example, IP: 192.168.0.1, end IP: 192.168.0.10
Remote Secure Gateway IP	The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.
Remote Network	Set the Single address, subnet or IP range of the remote network. **IP Address:** The IP address of the remote host. **Netmask:** The subnet of the remote network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254). **End IP:** The IP address range of the remote network. For example, IP: 192.168.1.1, end IP: 192.168.1.10.
Proposal	Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.

Parameter	Description
Authentication Type	Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.
Encryption	Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES**, **AES (128, 192 and 256)** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.
Perfect Forward Secrecy	Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.
Pre-shared Key	This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).
View IPSec Status	IPSec Status shows details of your configured IPSec VPN connections.

Click **Apply** to save the setting.