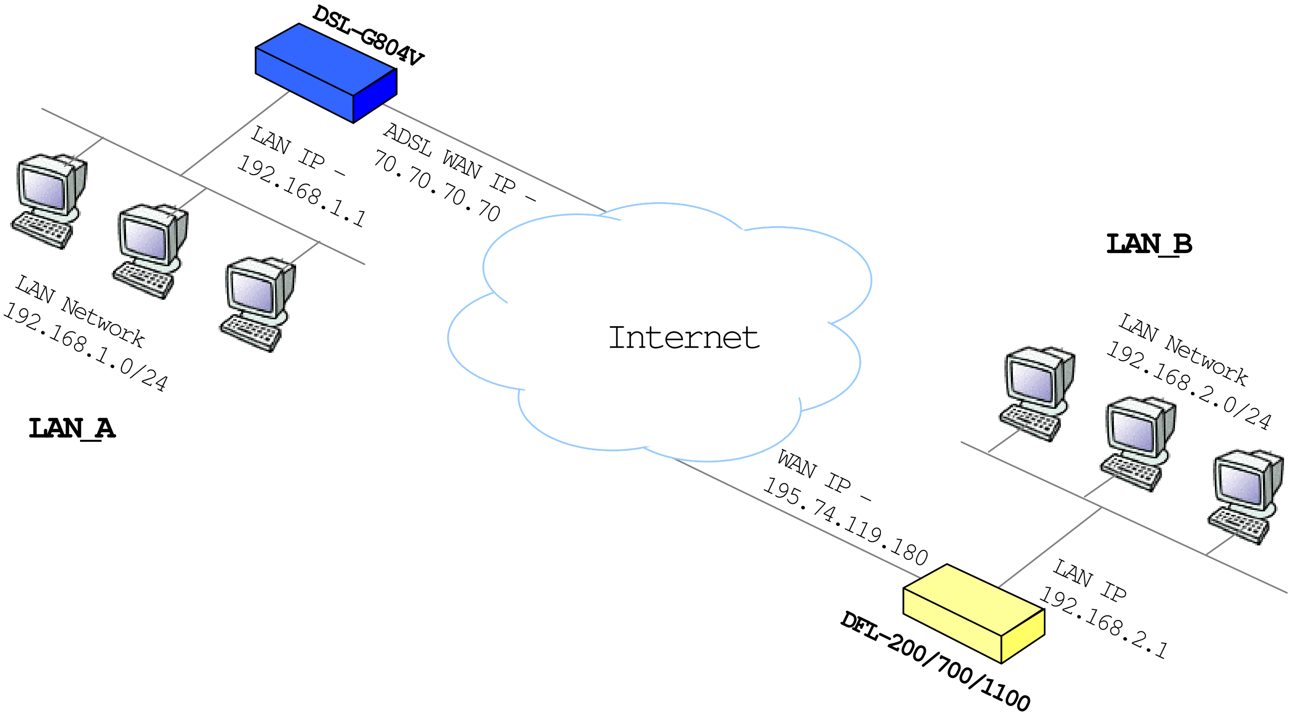
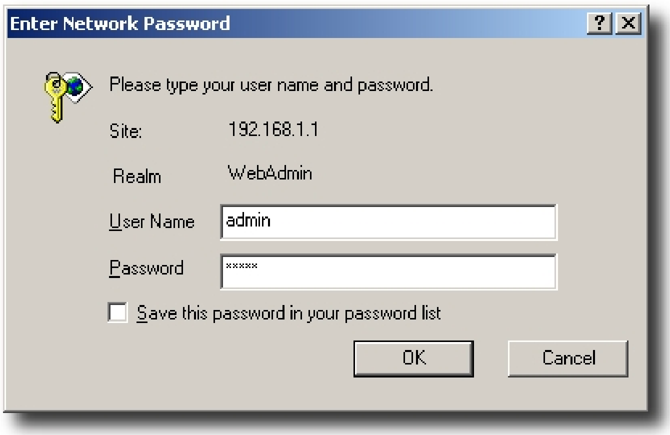
How do I configure a VPN tunnel between the DSL-G804V and the DFL-200/DFL-700/DFL-1100 firewall?



Configuring the DSL-G804V

1. Open a web browser and type the IP address of the DSL-G804V in the address bar (default is 192.168.1.1). Press **Enter**.
2. Enter the username and password (default is admin/admin). Click on **OK** to login.


Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

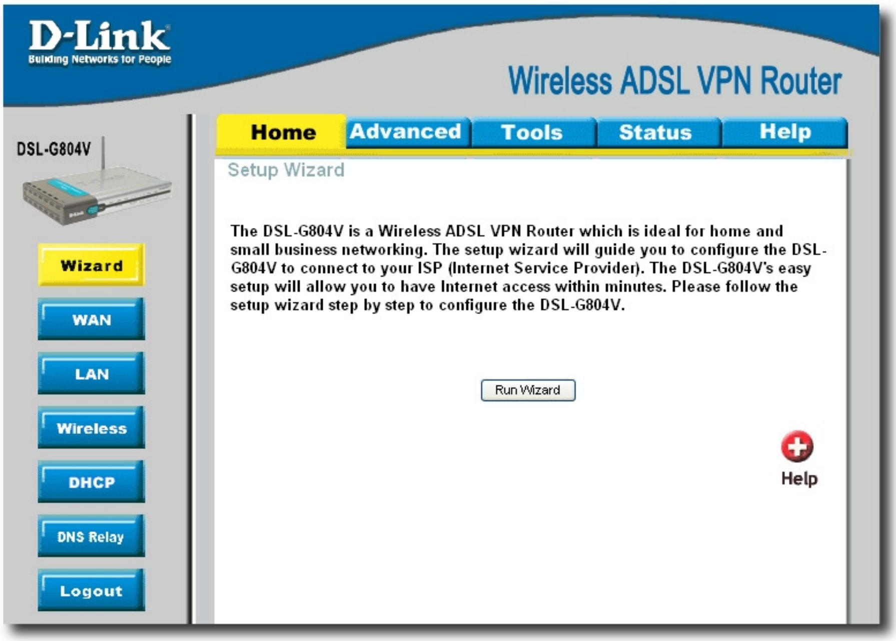
Realm WebAdmin

User Name admin

Password *****

□ Save this password in your password list

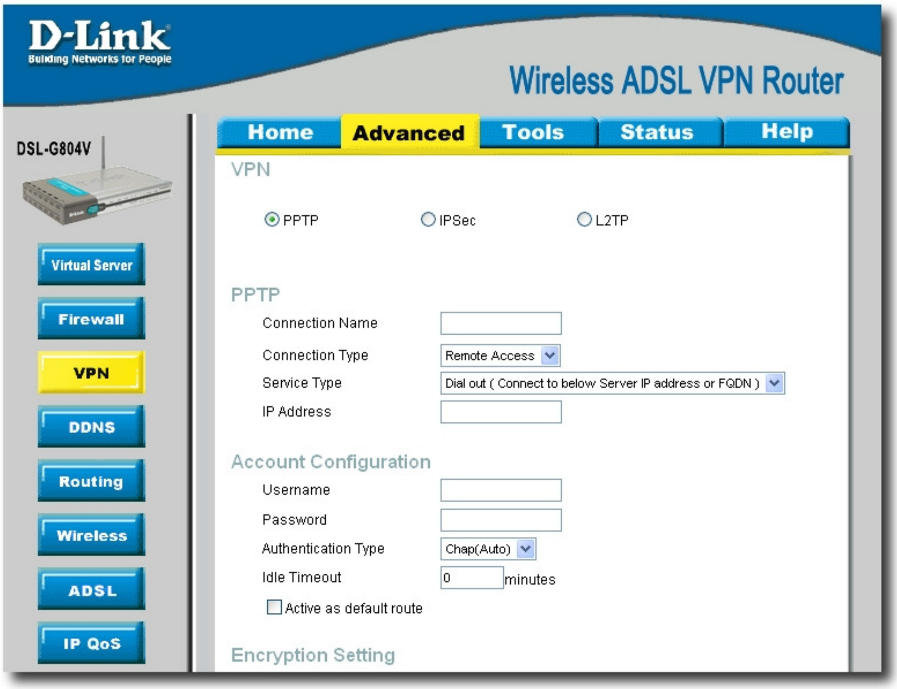
3. Click on **Advanced** at the top. Click on **VPN** on the left side.



Setup Wizard

The DSL-G804V is a Wireless ADSL VPN Router which is ideal for home and small business networking. The setup wizard will guide you to configure the DSL-G804V to connect to your ISP (Internet Service Provider). The DSL-G804V's easy setup will allow you to have Internet access within minutes. Please follow the setup wizard step by step to configure the DSL-G804V.

4. Click on the **IPsec** option button.



VPN

● PPTP ○ IPSec ○ L2TP

PPTP

Connection Name

Connection Type: Remote Access

Service Type: Dial out (Connect to below Server IP address or FQDN)

IP Address

Account Configuration

Username

Password

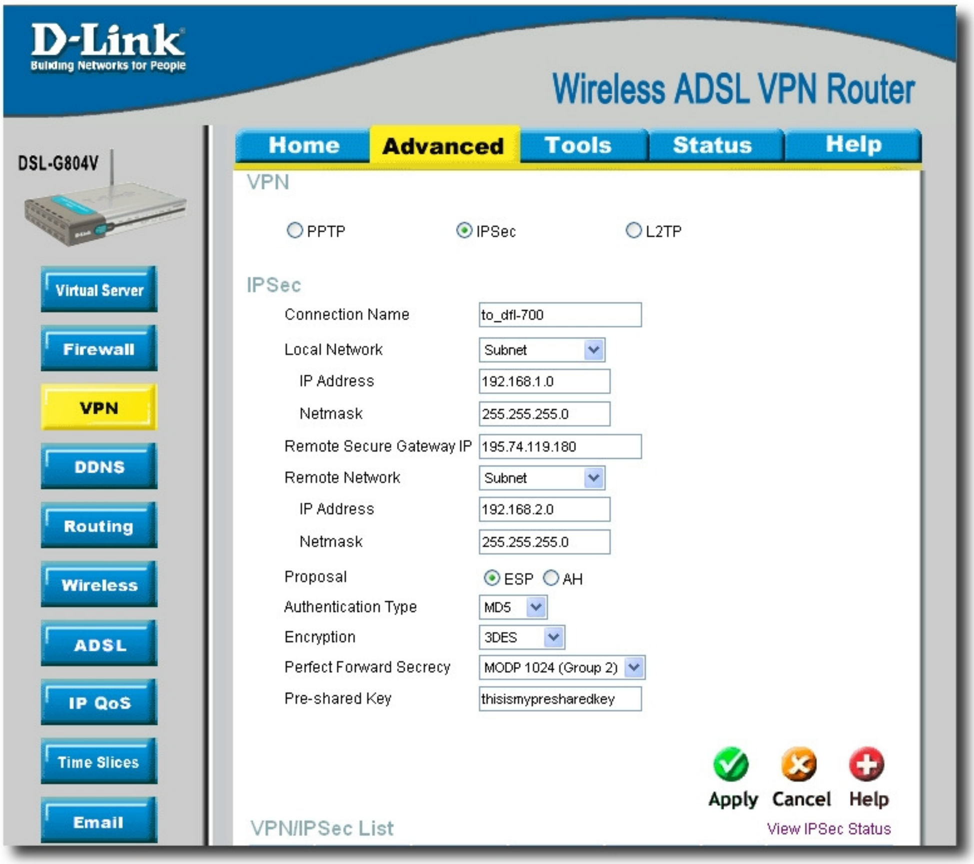
Authentication Type: Chap(Auto)

Idle Timeout: 0 minutes

□ Active as default route

Encryption Setting

5. Configure the following to create IPsec connection to the DFL-700:



VPN

○ PPTP ● IPSec ○ L2TP

IPSec

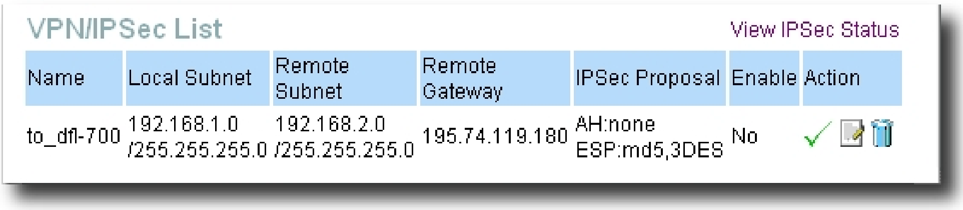
Connection Name	to_dfl-700
Local Network	Subnet
IP Address	192.168.1.0
Netmask	255.255.255.0
Remote Secure Gateway IP	195.74.119.180
Remote Network	Subnet
IP Address	192.168.2.0
Netmask	255.255.255.0
Proposal	● ESP ○ AH
Authentication Type	MD5
Encryption	3DES
Perfect Forward Secrecy	MODP 1024 (Group 2)
Pre-shared Key	thisismypresharedkey

VPN/IPSec List

a) **Connection Name** – type in the connection name
b) **Local Network** – Select subnet
c) **IP address** – type in the local IP network (192.168.1.0)
d) **Netmask** – type in the local IP subnet (255.255.255.0)
e) **Remote Secure Gateway** – type in the remote gateway (195.74.119.180)
f) **Remote Network** – Select subnet
g) **IP address** – type in the local IP network (192.168.2.0)
h) **Netmask** – type in the local IP subnet (255.255.255.0)
i) **Proposal** – select ESP
j) **Authentication Type** – select the authentication type (MD5)
k) **Encryption** – select the Encryption type (3DES)
l) **Perfect Forward Secrecy** – select the PFS group (Group2)
m) **Pre-shared key** – type the pre-shared key

Click on **Apply** when done.

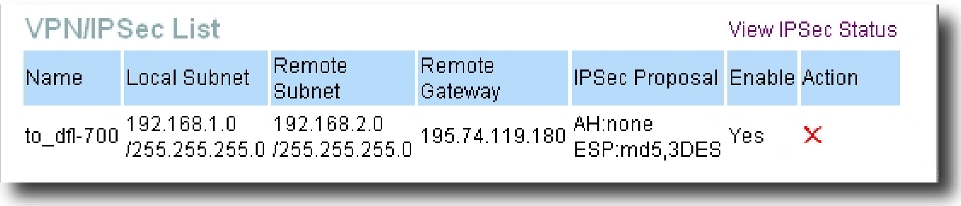
6. The profile will now be shown at the bottom of the screen. Click on the green check icon to enable the profile.



VPN/IPSec List View IPSec Status

Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Enable	Action
to_dfl-700	192.168.1.0 /255.255.255.0	192.168.2.0 /255.255.255.0	195.74.119.180	AH:none ESP:md5,3DES	No	✓

7. The profile will now show up as enabled.

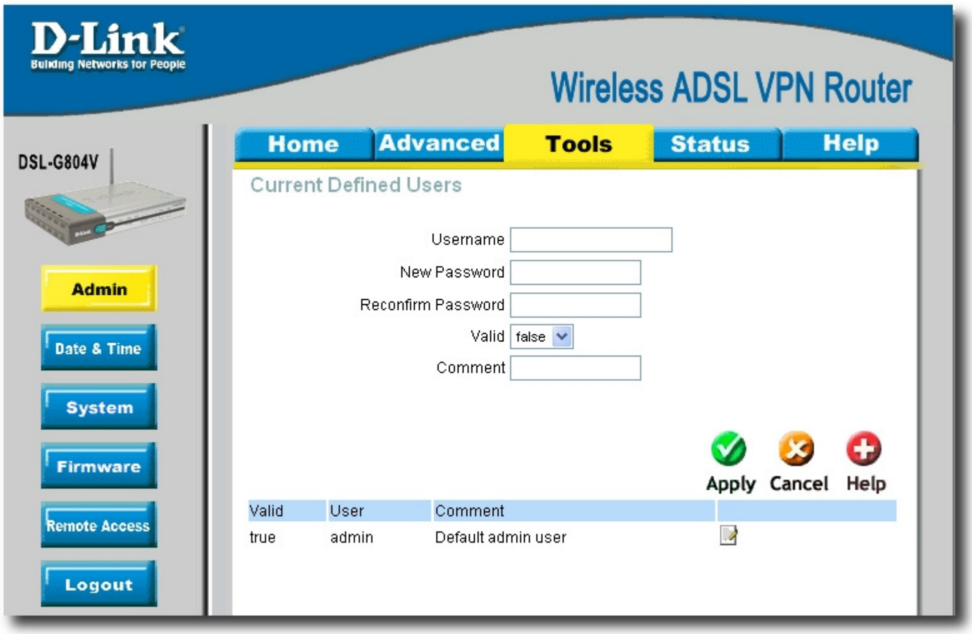


VPN/IPSec List

View IPSec Status

Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Enable	Action
to_dfl-700	192.168.1.0 /255.255.255.0	192.168.2.0 /255.255.255.0	195.74.119.180	AH:none ESP:md5,3DES	Yes	✗

8. Click on **Tools** at the top.



Current Defined Users

Username

New Password

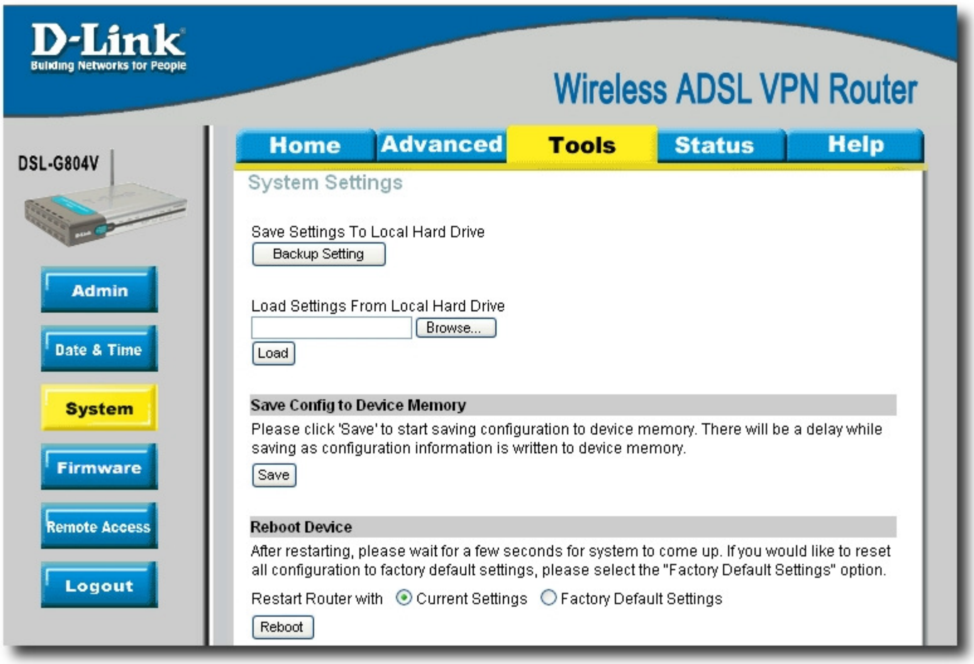
Reconfirm Password

Valid false

Comment

Valid	User	Comment	
true	admin	Default admin user	

9. Click on **System** on the left side. Click on the **Save** button to permanently save the changes to device memory.



System Settings

Save Settings To Local Hard Drive

Backup Setting

Load Settings From Local Hard Drive

Browse...

Load

Save Config to Device Memory

Please click 'Save' to start saving configuration to device memory. There will be a delay while saving as configuration information is written to device memory.

Save

Reboot Device

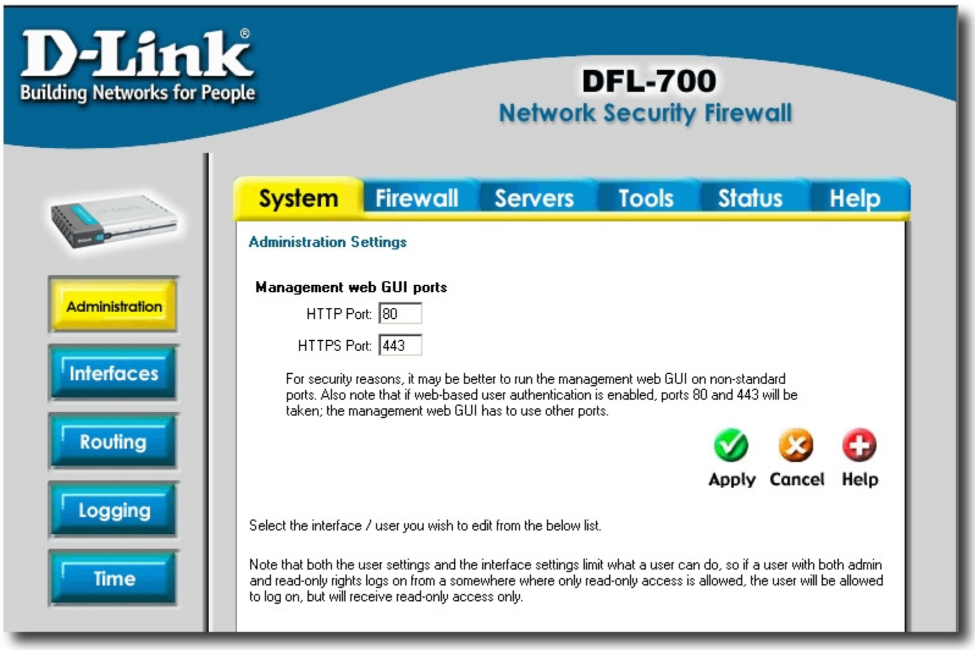
After restarting, please wait for a few seconds for system to come up. If you would like to reset all configuration to factory default settings, please select the "Factory Default Settings" option.

Restart Router with ● Current Settings ○ Factory Default Settings

Reboot

Configuring the DFL-700

10. Open up a web browser and type in the IP address of the DFL-700 (i.e. https://192.168.2.1). Press **Enter**.
11. Login to the DFL-700 with the username and password. At the Main page, click on **Firewall** at the top.



Administration Settings

Management web GUI ports

HTTP Port: 80

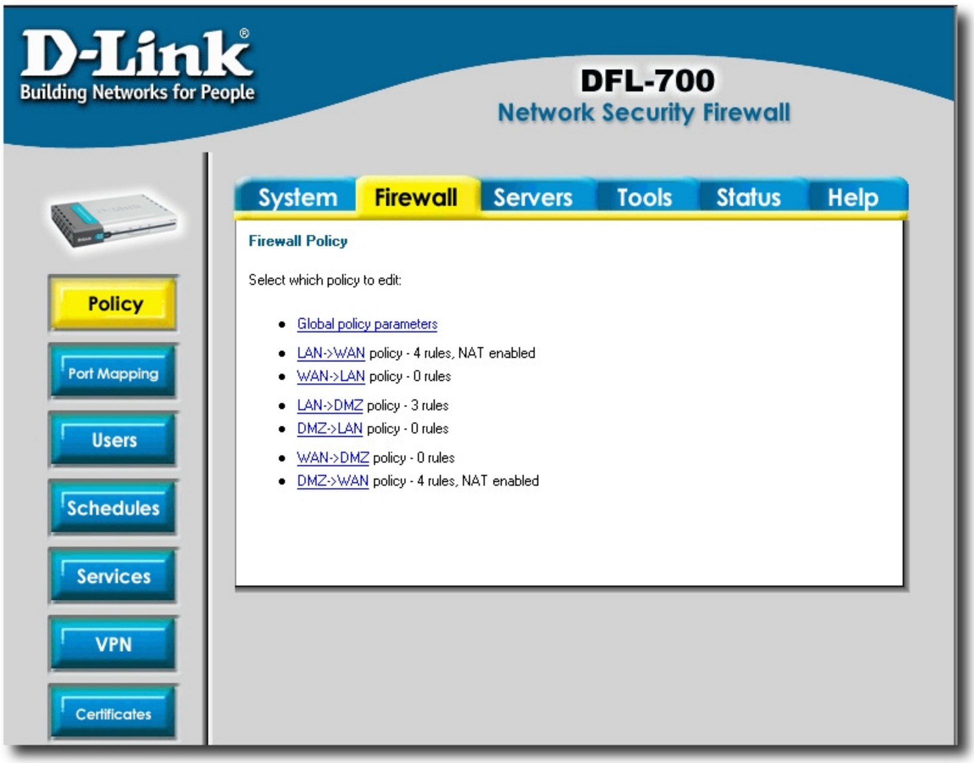
HTTPS Port: 443

For security reasons, it may be better to run the management web GUI on non-standard ports. Also note that if web-based user authentication is enabled, ports 80 and 443 will be taken; the management web GUI has to use other ports.

Select the interface / user you wish to edit from the below list.

Note that both the user settings and the interface settings limit what a user can do, so if a user with both admin and read-only rights logs on from a somewhere where only read-only access is allowed, the user will be allowed to log on, but will receive read-only access only.

12. Click on **VPN** on the left side.

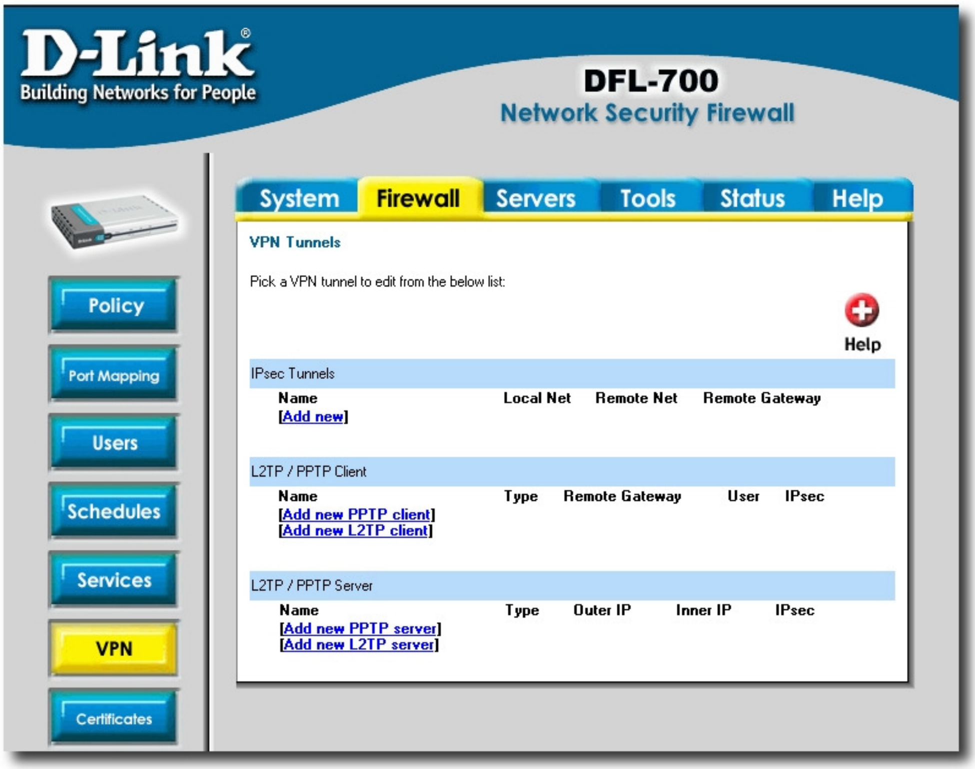


Firewall Policy

Select which policy to edit:

- Global policy parameters
- LAN->WAN policy - 4 rules, NAT enabled
- WAN->LAN policy - 0 rules
- LAN->DMZ policy - 3 rules
- DMZ->LAN policy - 0 rules
- WAN->DMZ policy - 0 rules
- DMZ->WAN policy - 4 rules, NAT enabled

13. Click on **Add New** under IPsec Tunnels.



VPN Tunnels

Pick a VPN tunnel to edit from the below list:

Help

IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway
[Add new]			

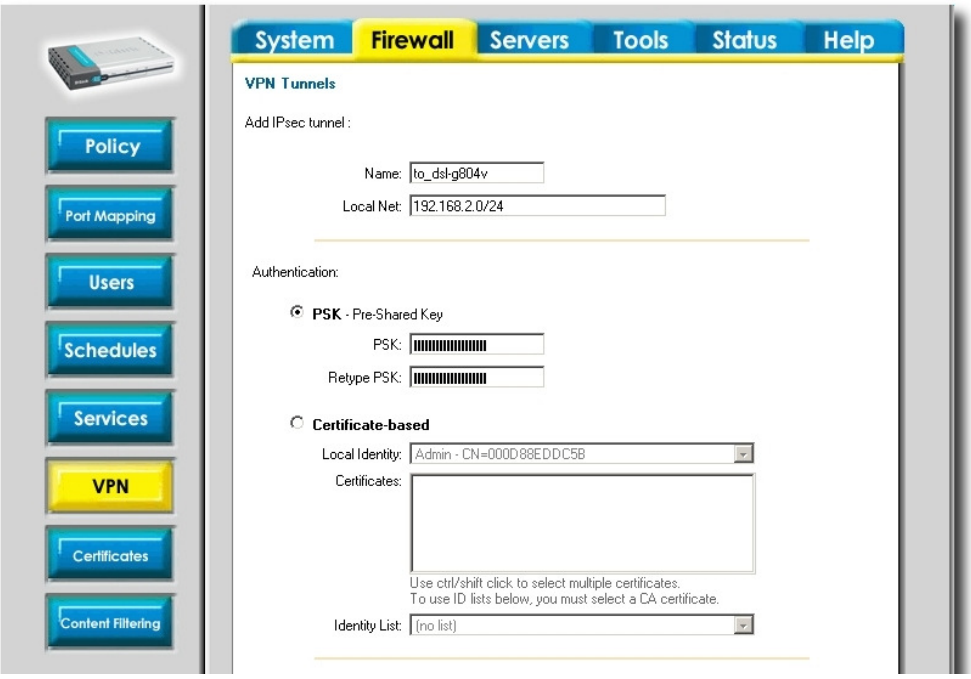
L2TP / PPTP Client

Name	Type	Remote Gateway	User	IPsec
[Add new PPTP client] [Add new L2TP client]				

L2TP / PPTP Server

Name	Type	Outer IP	Inner IP	IPsec
[Add new PPTP server] [Add new L2TP server]				

14. Configure the following to add the to_dsl-g804v profile.



VPN Tunnels

Add IPsec tunnel :

Name: to_dsl-g804v

Local Net: 192.168.2.0/24

Authentication:

● **PSK** - Pre-Shared Key

PSK: ||||||||||||||||||||

Retype PSK: ||||||||||||||||||||

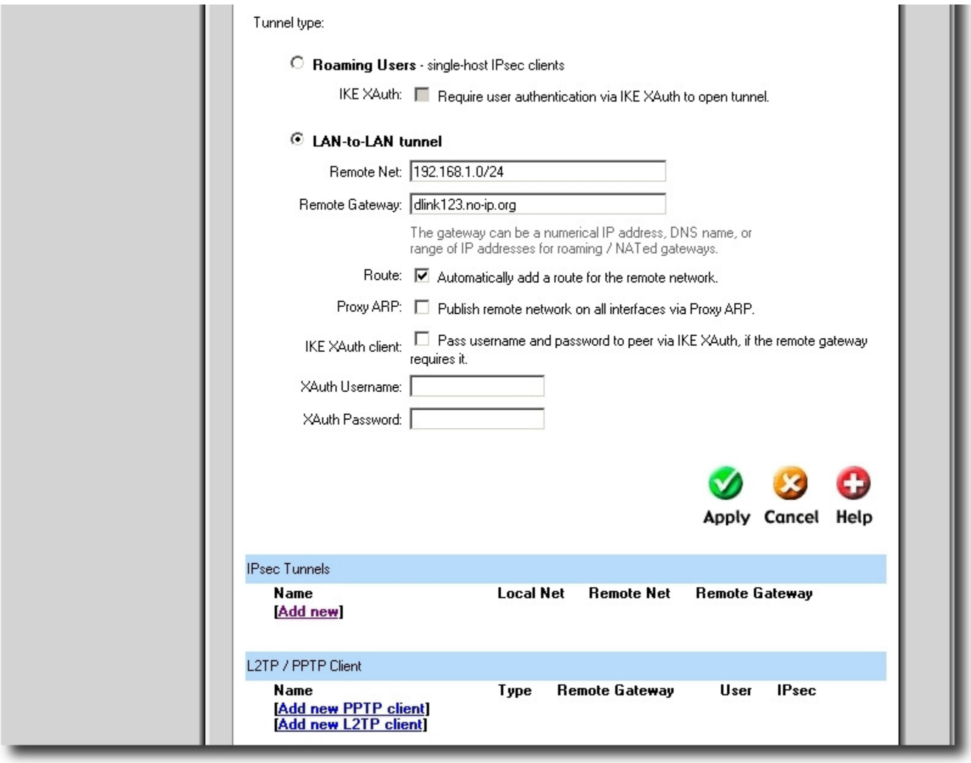
○ **Certificate-based**

Local Identity: Admin - CN=000D88EDDC5B

Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: (no list)



Tunnel type:

○ **Roaming Users** - single-host IPsec clients

IKE XAuth: □ Require user authentication via IKE XAuth to open tunnel.

● **LAN-to-LAN tunnel**

Remote Net: 192.168.1.0/24

Remote Gateway: dlink123.no-ip.org

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Route: ☑ Automatically add a route for the remote network.

Proxy ARP: □ Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client: □ Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway
[Add new]			

L2TP / PPTP Client

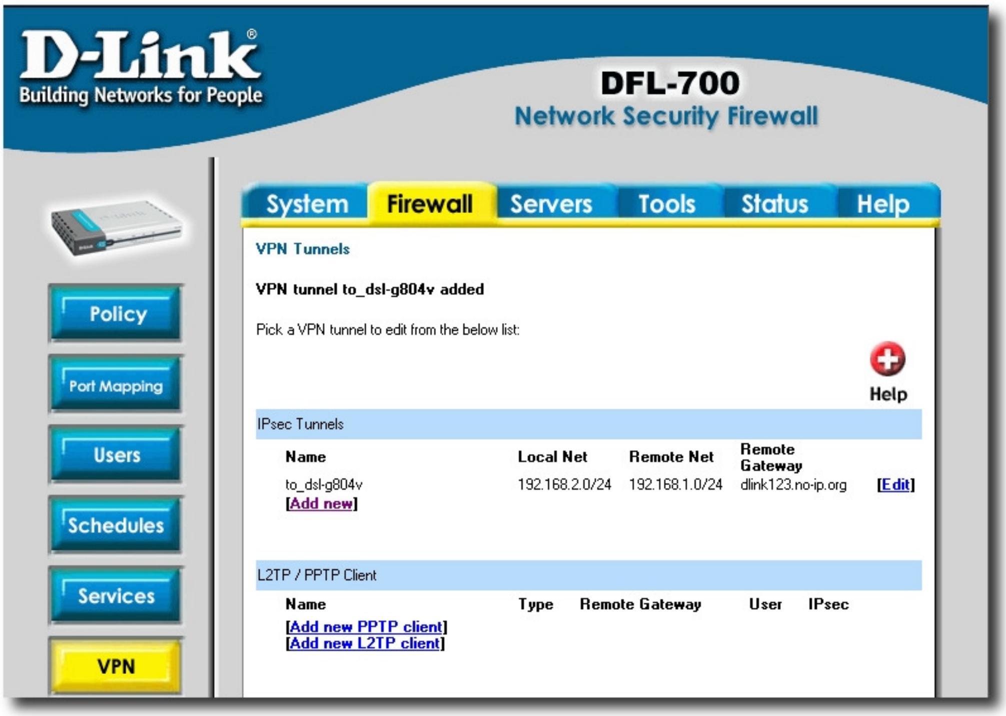
Name	Type	Remote Gateway	User	IPsec
[Add new PPTP client] [Add new L2TP client]				

a) **Name –** type in the name for the IPsec tunnel
b) **Local Net** – type in the local IP network with the subnet in decimal notation (i.e. 192.168.2.0/24)
c) **Authentication** – set authentication to **PSK – Pre-shared Key**. Type in the Pre-shared key
d) **Tunnel Type** – set tunnel type to LAN-to-LAN tunnel**.**
e) **Remote Net** – set the remote net (i.e. 192.168.1.0/24)
f) **Remote Gateway** – type in the remote gateway. You can put in the DSL-G804V WAN IP address (70.70.70.70). If the DSL-G804V is using Dynamic DNS, type in the hostname (i.e. dlink123.no-ip.org).

Leave the remaining fields as default.

Click on the **Apply** button to apply changes.

15. The new 'to_dsl-g804v' profile will now be added. Clcik on **Edit** next to the new profile.



VPN Tunnels

VPN tunnel to_dsl-g804v added

Pick a VPN tunnel to edit from the below list:

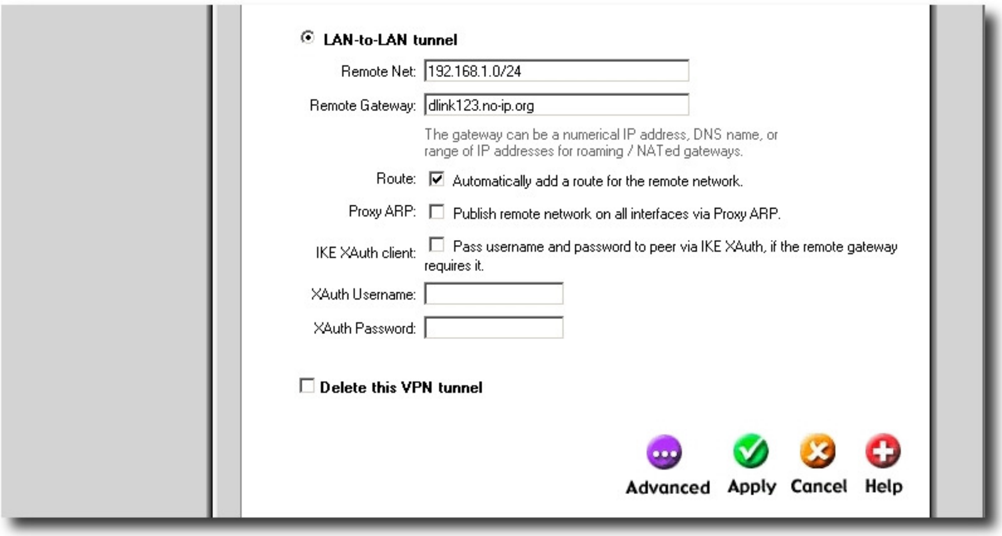
IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway	
to_dsl-g804v	192.168.2.0/24	192.168.1.0/24	dlink123.no-ip.org	[Edit]
[Add new]				

L2TP / PPTP Client

Name	Type	Remote Gateway	User	IPsec
[Add new PPTP client]				
[Add new L2TP client]				

16. Click on the **Advanced** button at the bottom of the screen.



● LAN-to-LAN tunnel

Remote Net: 192.168.1.0/24

Remote Gateway: dlink123.no-ip.org

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Route: ☑ Automatically add a route for the remote network.

Proxy ARP: □ Publish remote network on all interfaces via Proxy ARP.

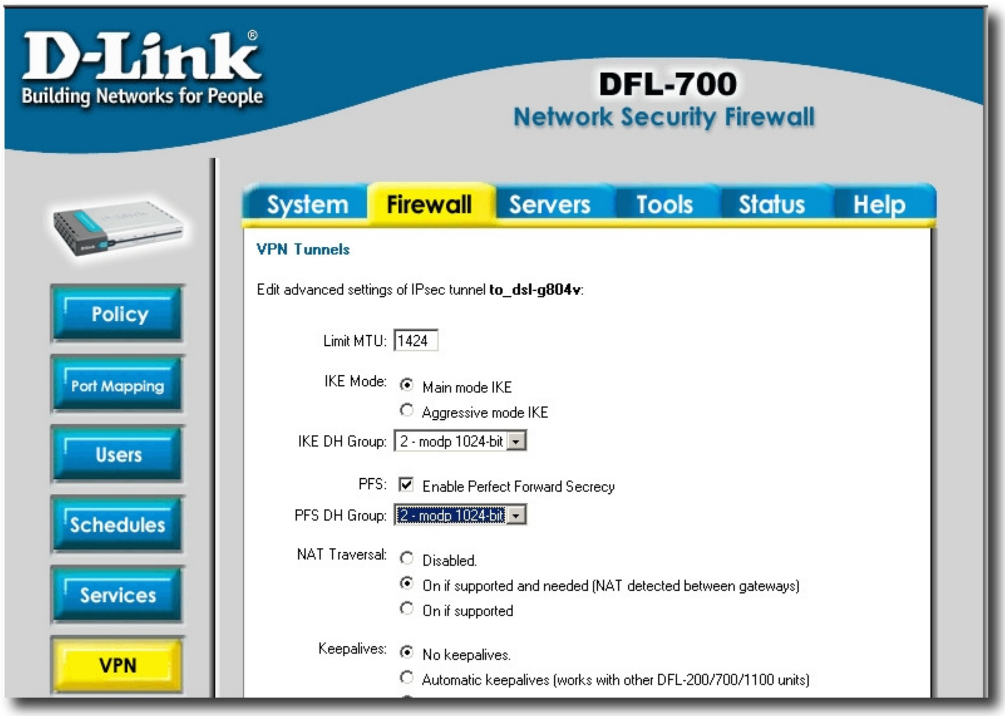
IKE XAuth client: □ Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

□ Delete this VPN tunnel

17. Enable the **PFS – Enable Perfect Forward Secrecy**. Set the **PFS DH Group** to '2 – modp 1024 bits'



VPN Tunnels

Edit advanced settings of IPsec tunnel **to_dsl-g804v**:

Limit MTU: 1424

IKE Mode: ● Main mode IKE ○ Aggressive mode IKE

IKE DH Group: 2 - modp 1024-bit

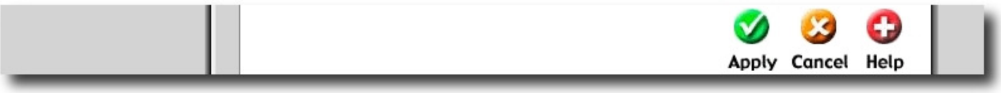
PFS: ☑ Enable Perfect Forward Secrecy

PFS DH Group: 2 - modp 1024-bit

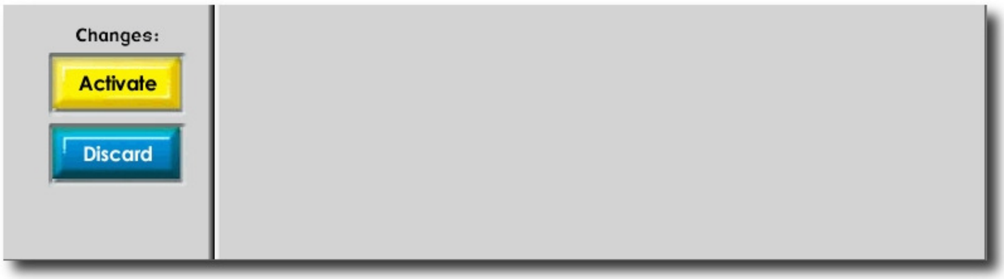
NAT Traversal: ○ Disabled. ● On if supported and needed (NAT detected between gateways) ○ On if supported

Keepalives: ● No keepalives. ○ Automatic keepalives (works with other DFL-200/700/1100 units)

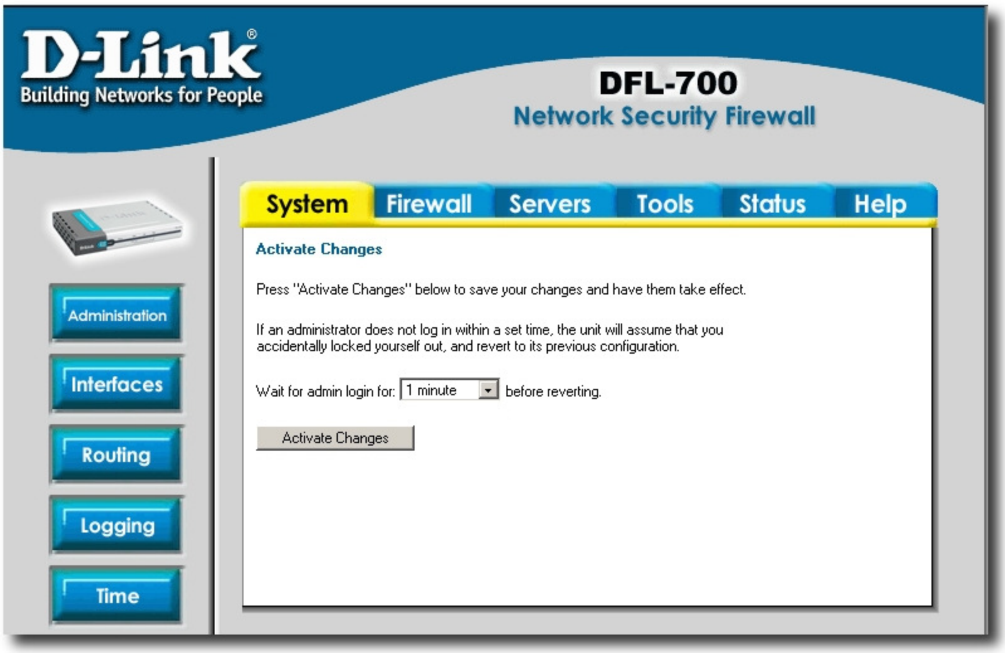
18. Click on the **Apply** button at the bottom of the screen to apply the changes.



19. Click on the **Activate** button to activate the changes



20. Click on **Activate Changes** to activate the changes.



Activate Changes

Press "Activate Changes" below to save your changes and have them take effect.

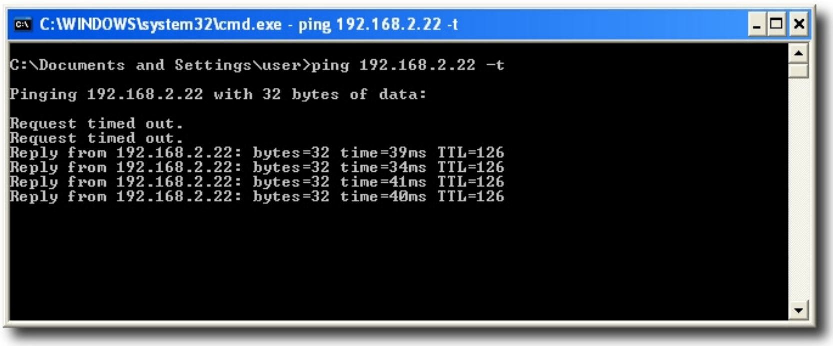
If an administrator does not log in within a set time, the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Wait for admin login for: 1 minute before reverting.

Activate Changes

Testing the Configuration

21. Open up the **Command Prompt** on a machine in the DSL-G804V network.
22. Start a ping to the a PC on the DFL-700 LAN network (192.168.2.22)



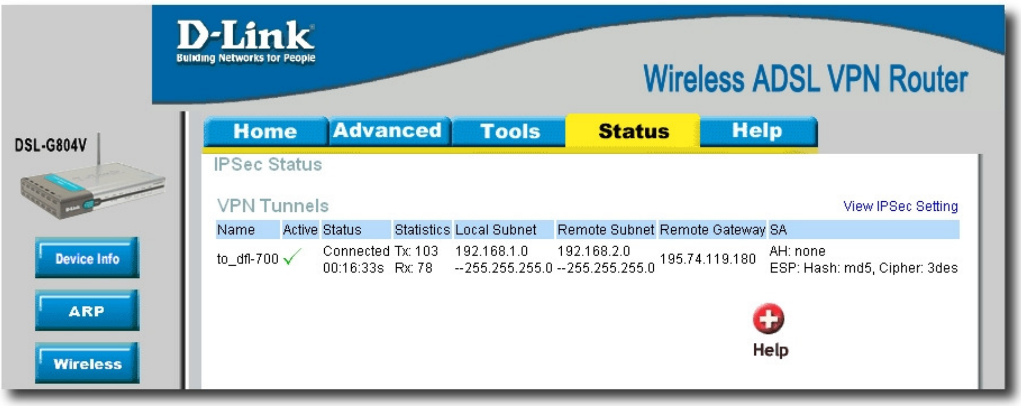
```
C:\WINDOWS\system32\cmd.exe - ping 192.168.2.22 -t

C:\Documents and Settings\user>ping 192.168.2.22 -t

Pinging 192.168.2.22 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.2.22: bytes=32 time=39ms TTL=126
Reply from 192.168.2.22: bytes=32 time=34ms TTL=126
Reply from 192.168.2.22: bytes=32 time=41ms TTL=126
Reply from 192.168.2.22: bytes=32 time=40ms TTL=126
```

23. Log in to the web interface of the DSL-G804V. Click on **Status→ IPsec Status** on the left hand side. The screen will show the Connection status for the to_dfl-700 VPN tunnel.



IPSec Status

VPN Tunnels View IPSec Setting

Name	Active	Status	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA
to_dfl-700	✓	Connected 00:16:33s	Tx: 103 Rx: 78	192.168.1.0 --255.255.255.0	192.168.2.0 --255.255.255.0	195.74.119.180	AH: none ESP: Hash: md5, Cipher: 3des