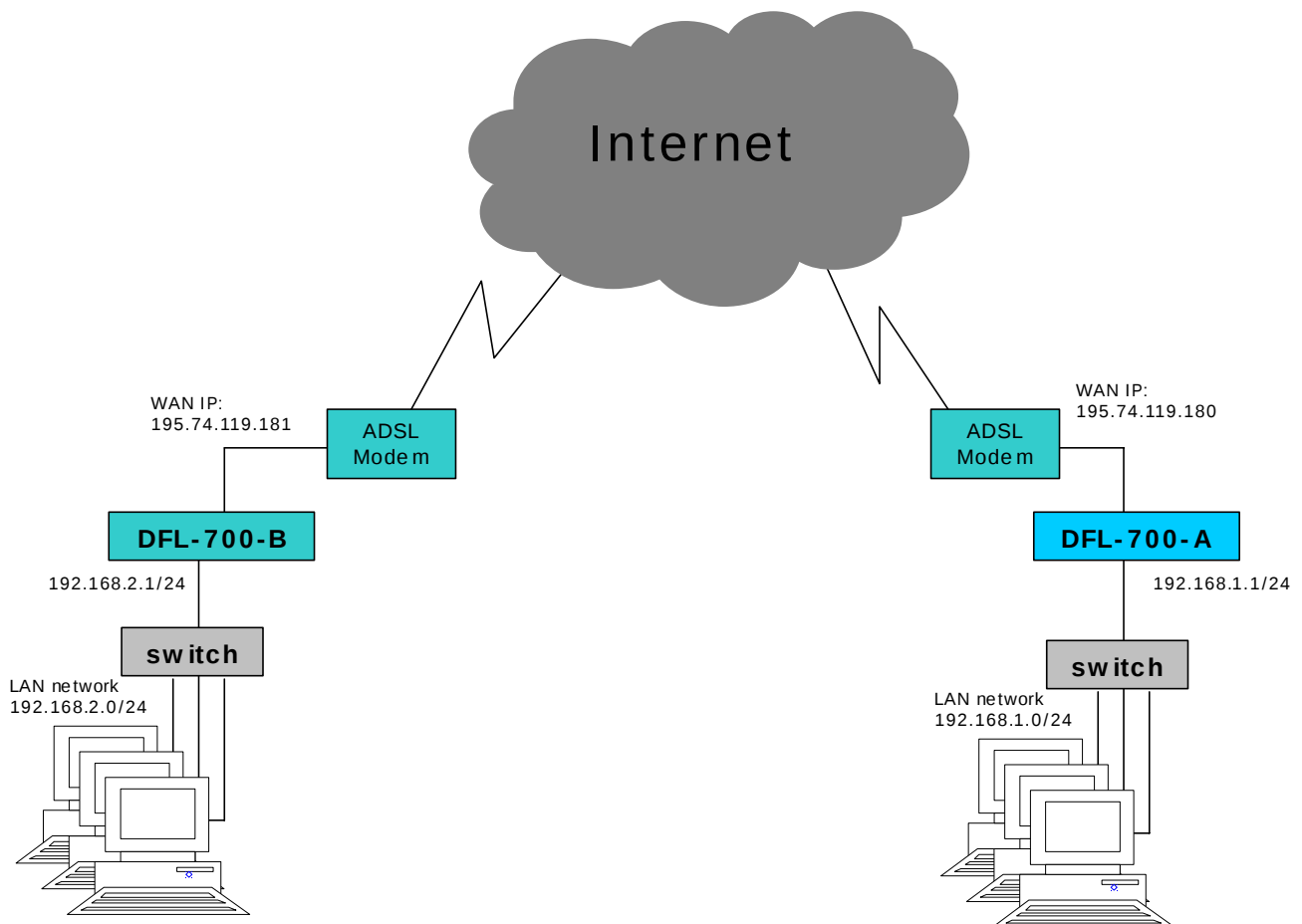


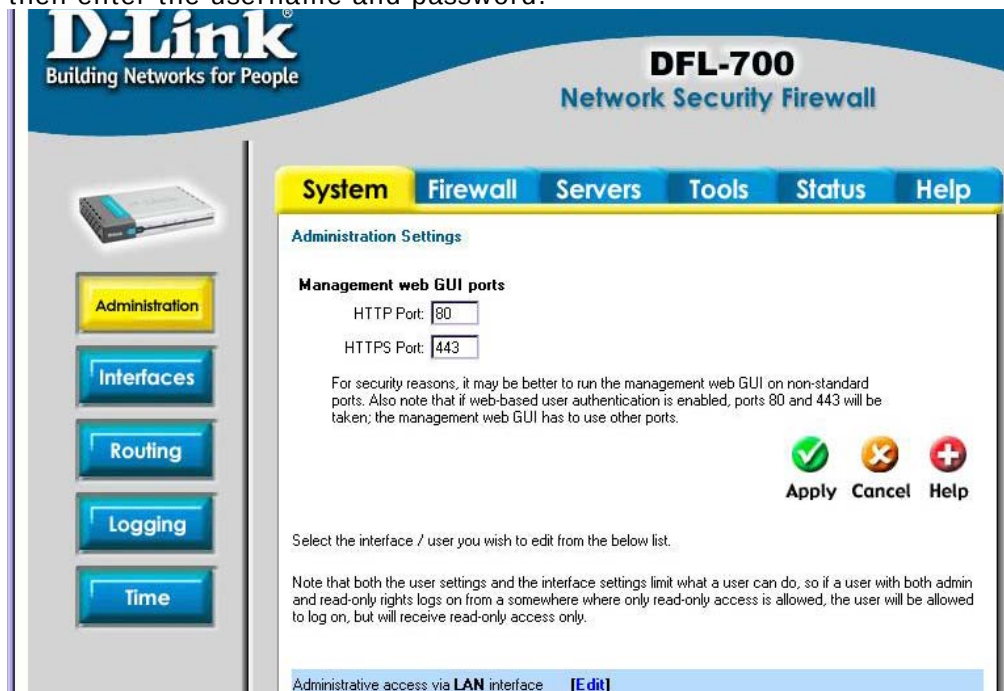
DFL-700 with DFL-700 IPsec VPN Configuration Guide

This configuration shows how to connect a DFL-700 to another DFL-700 with an IPsec tunnel. Please check the D-Link AUS FTP Site at <ftp://202.129.109.68> for updates on the firmware.

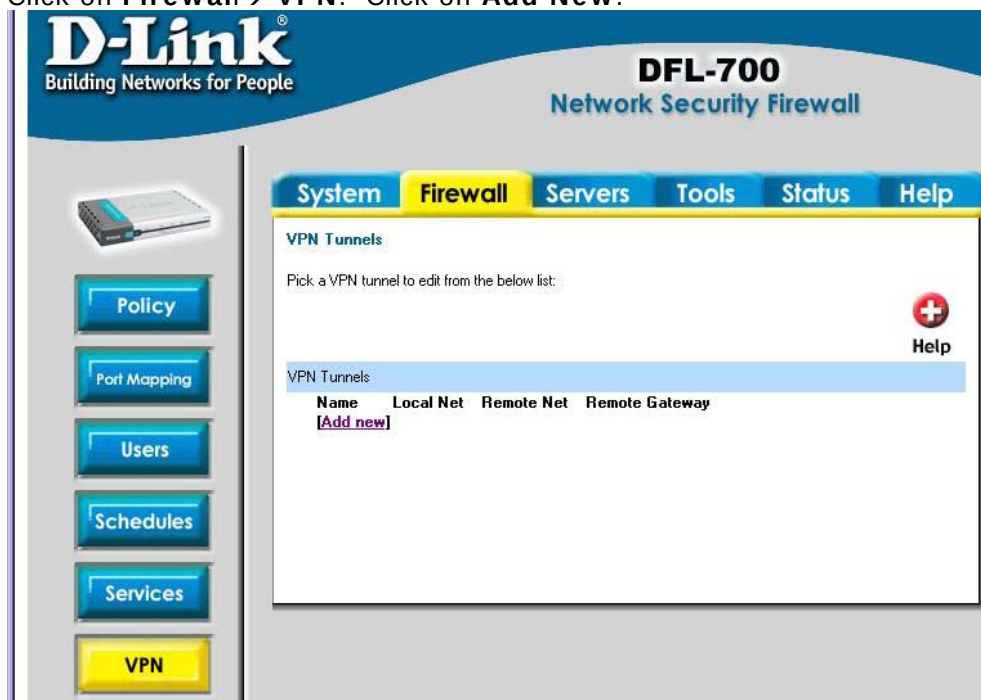


DFL-700-A configuration

- 1) Log into the DFL-700 using its IP address (https://192.168.1.1 in this example) and then enter the username and password.



- 2) Click on **Firewall** → **VPN**. Click on **Add New**.



- 3) Enter the details for the Tunnel.

Name: DFL-700-B
Local Net: 192.168.1.0/24
Authentication: PSK
Pre-shared key: dlinktest
LAN-to-LAN tunnel

Remote net: 192.168.2.0/24
 Remote gateway: 195.74.119.181

System **Firewall** Servers Tools Status Help

VPN Tunnels

Add VPN tunnel:

Name:

Local Net:

Authentication:

☒ **PSK - Pre-Shared Key**

PSK:

Retype PSK:

☐ **Certificate-based**

Local Identity:

Certificates:

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

Identity List:

Tunnel type:

☐ **Roaming Users** - single-host VPN clients

IKE XAuth: ☐ Require user authentication via IKE XAuth to open tunnel

☒ **LAN-to-LAN tunnel**

Remote Net:

Remote Gateway:

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

Proxy ARP: ☐ Publish remote network on all interfaces via Proxy ARP

Click on **Apply** when done

- 4) Click on **Edit** on the newly created **DFL-700-B** profile

System **Firewall** Servers Tools Status Help

VPN Tunnels

VPN tunnel DFL-700-B added

Pick a VPN tunnel to edit from the below list:



Help

Name	Local Net	Remote Net	Remote Gateway	
DFL-700-B	192.168.1.0/24	192.168.2.0/24	195.74.119.181	[Edit]

[\[Add new\]](#)

- 5) Click on **Advanced**. Set IKE mode to 'Main Mode' (default), IKE DH Group '2 – modp 1024-bit' (default). Check the PFS option. Set the PFS DH Group to '2-modp 1024-bit'. Set NAT traversal to 'On if supported and needed'. Click on **Apply** when done.

The screenshot shows the 'Firewall' tab in the configuration interface. The 'VPN Tunnels' section is active, showing settings for VPN tunnel DFL-700-B. The settings are as follows:

- 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-700/1100 units), ☐ Manually configured keepalives:
 - Source IP: []
 - Destination IP: []

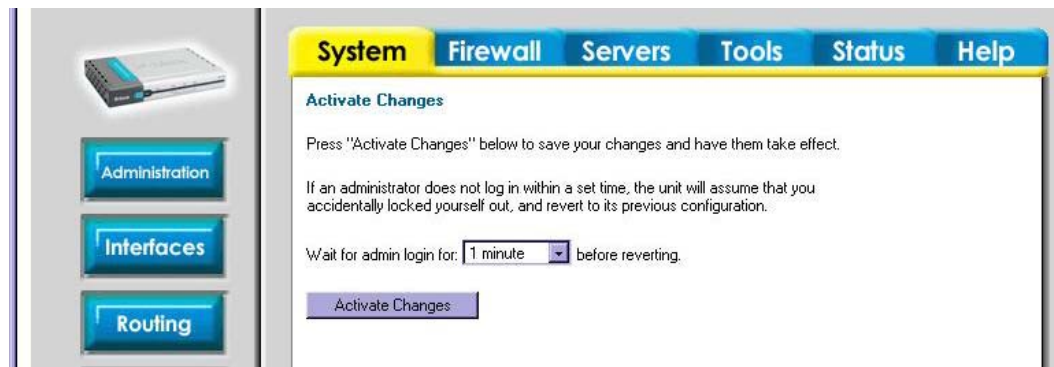
Below the settings is the 'IKE Proposal List' table:

	Cipher	Hash	Life KB	Life Sec
#1:	AES-128 Allowed:128-256	SHA-1	0	3600
#2:	AES-128 Allowed:128-256	MD5	0	3600
#3:	3DES	MD5	0	3600
#4:	DES	MD5	0	3600
#5:	-	MD5	0	0
#6:	-	MD5	0	0
#7:	-	MD5	0	0
#8:	-	MD5	0	0

- 6) Click on **Activate** on the bottom left hand corner of the screen.

The screenshot shows the bottom left corner of the configuration interface. It includes buttons for 'Certificates' and 'Content Filtering'. Below these is a 'Changes:' section with two buttons: 'Activate' (highlighted in yellow) and 'Discard'.

- 7) Click on the **Activate Changes** button.

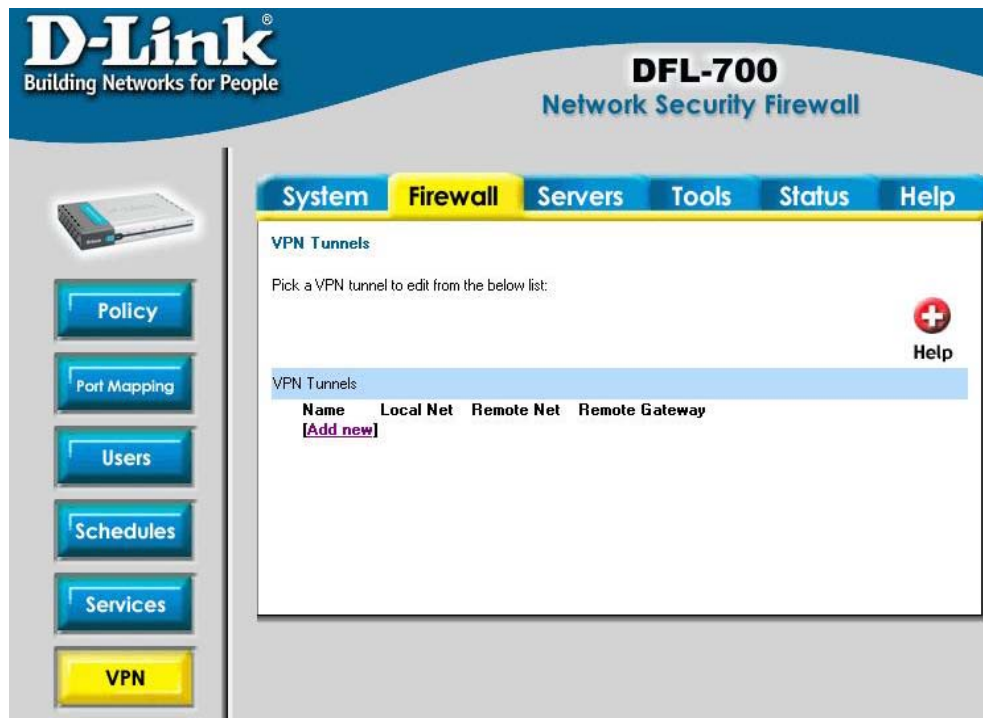


DFL-700-B configuration

- 1) Log into the DFL-700 using its IP address (https://192.168.2.1 in this example) and then enter the username and password.

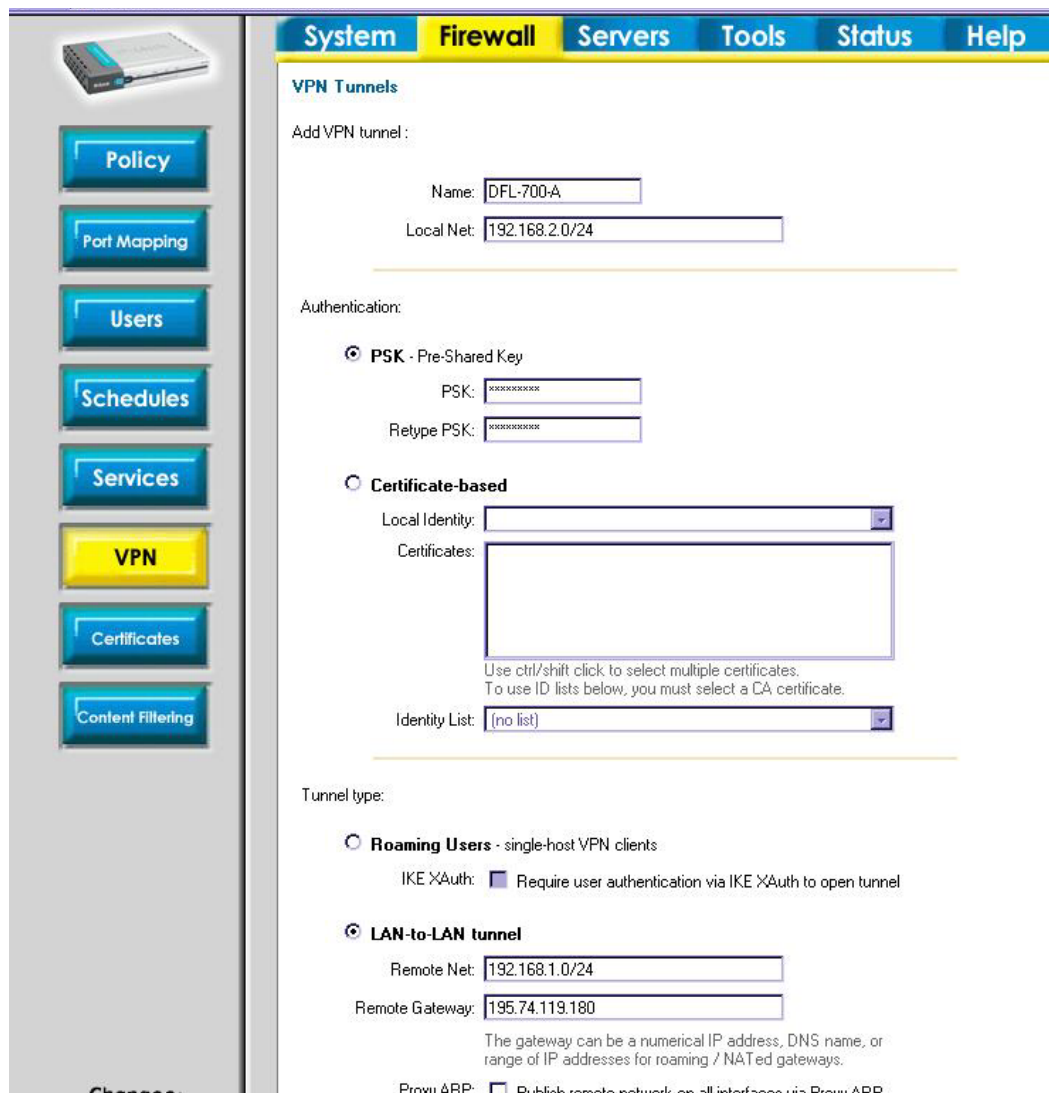


- 2) Click on **Firewall**→ **VPN**. Click on **Add New**.



3) Enter the details for the Tunnel.

Name: DFL-700-A
Local Net: 192.168.2.0/24
Authentication: PSK
Pre-shared key: dlinktest
LAN-to-LAN tunnel
Remote net: 192.168.1.0/24
Remote gateway: 195.74.119.180



System Firewall Servers Tools Status Help

VPN Tunnels

Add VPN tunnel:

Name:

Local Net:

Authentication:

☒ **PSK - Pre-Shared Key**

PSK:

Retype PSK:

☐ **Certificate-based**

Local Identity:

Certificates:

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

Identity List:

Tunnel type:

☐ **Roaming Users** - single-host VPN clients

IKE XAuth: ☐ Require user authentication via IKE XAuth to open tunnel

☒ **LAN-to-LAN tunnel**

Remote Net:

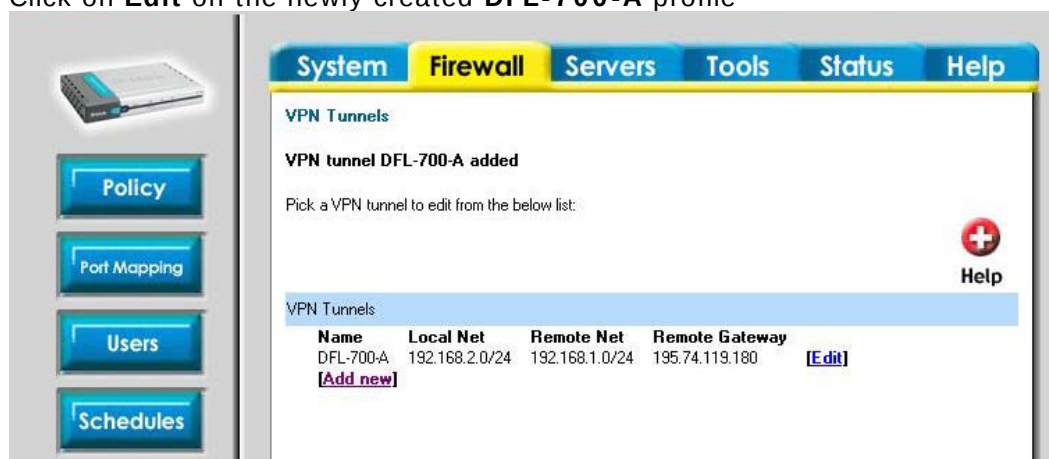
Remote Gateway:

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

Proxy ARP: ☐ Publish remote network on all interfaces via Proxy ARP

Click on **Apply** when done.

- 4) Click on **Edit** on the newly created **DFL-700-A** profile



System Firewall Servers Tools Status Help

VPN Tunnels

VPN tunnel DFL-700-A added

Pick a VPN tunnel to edit from the below list:

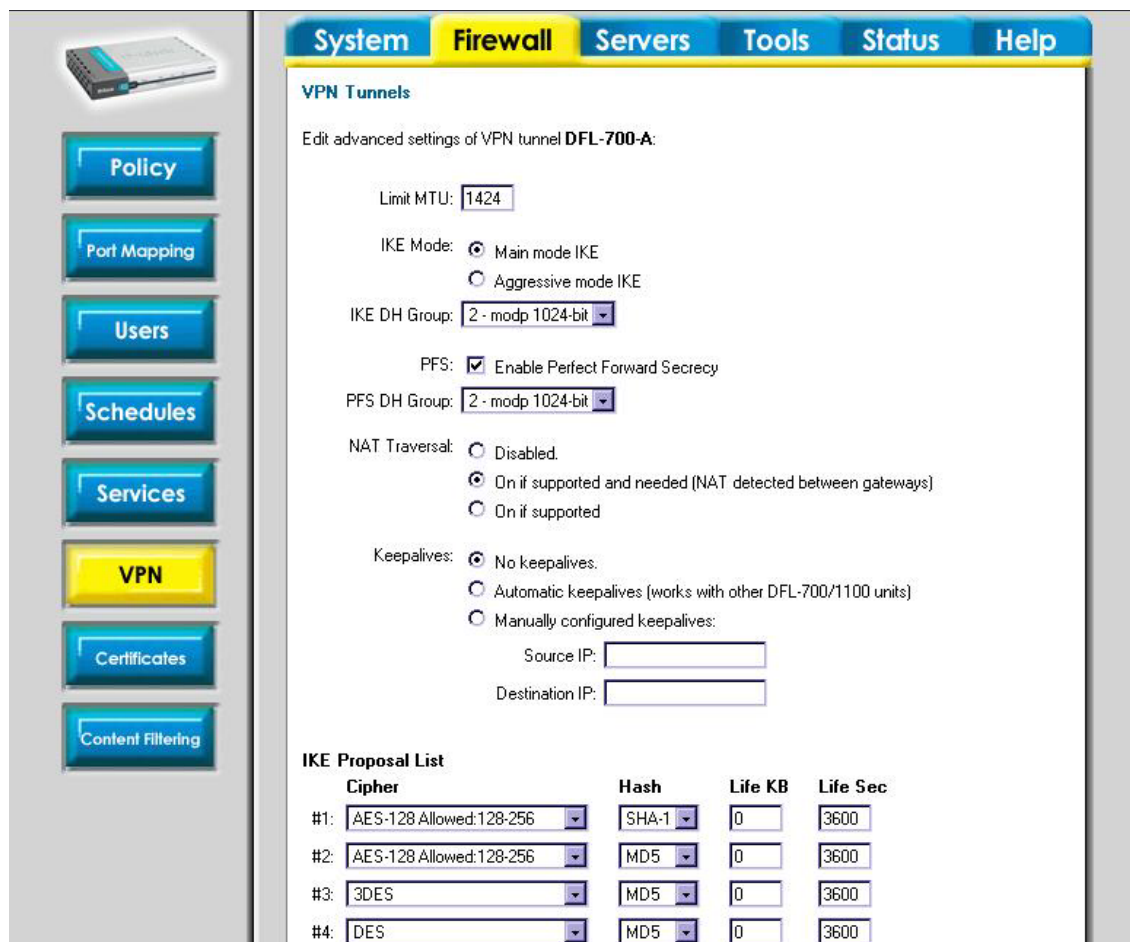


Help

Name	Local Net	Remote Net	Remote Gateway	
DFL-700-A	192.168.2.0/24	192.168.1.0/24	195.74.119.180	[Edit]

[\[Add new\]](#)

- 5) Click on **Advanced**. Set IKE mode to 'Main Mode' (default), IKE DH Group '2 – modp 1024-bit' (default). Check the PFS option. Set the PFS DH Group to '2-modp 1024-bit'. Set NAT traversal to 'On if supported and needed'. Click on **Apply** when done.



System **Firewall** Servers Tools Status Help

VPN Tunnels

Edit advanced settings of VPN tunnel **DFL-700-A**:

Limit MTU:

IKE Mode: ☒ Main mode IKE
☐ Aggressive mode IKE

IKE DH Group:

PFS: ☒ Enable Perfect Forward Secrecy

PFS DH Group:

NAT Traversal: ☐ Disabled
☒ On if supported and needed (NAT detected between gateways)
☐ On if supported

Keepalives: ☒ No keepalives.
☐ Automatic keepalives (works with other DFL-700/1100 units)
☐ Manually configured keepalives:
Source IP:
Destination IP:

IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	AES-128 Allowed:128-256	SHA-1	0	3600
#2:	AES-128 Allowed:128-256	MD5	0	3600
#3:	3DES	MD5	0	3600
#4:	DES	MD5	0	3600

- 6) Click on 'Activate' on the bottom left hand corner of the screen.



Certificates

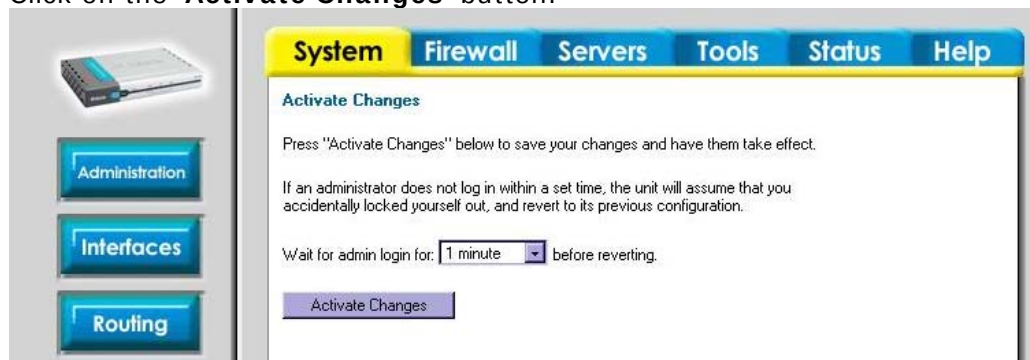
Content Filtering

Changes:

Activate

Discard

- 7) Click on the 'Activate Changes' button.



System **Firewall** Servers Tools Status Help

Activate Changes

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

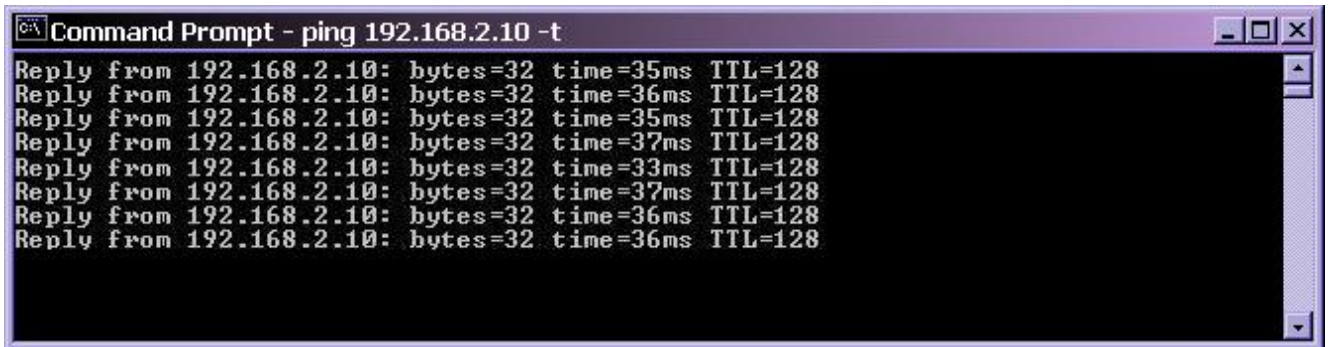
If an administrator does not log in within a set time, the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Wait for admin login for: before reverting.

Activate Changes

Testing the connection

From the DFL-700-A side, you can initiate a ping to a machine on the LAN side of the DFL-700-B (i.e. 192.168.2.10). The tunnel should then be generated and then you should get a response as shown below.



```
Command Prompt - ping 192.168.2.10 -t
Reply from 192.168.2.10: bytes=32 time=35ms TTL=128
Reply from 192.168.2.10: bytes=32 time=36ms TTL=128
Reply from 192.168.2.10: bytes=32 time=35ms TTL=128
Reply from 192.168.2.10: bytes=32 time=37ms TTL=128
Reply from 192.168.2.10: bytes=32 time=33ms TTL=128
Reply from 192.168.2.10: bytes=32 time=37ms TTL=128
Reply from 192.168.2.10: bytes=32 time=36ms TTL=128
Reply from 192.168.2.10: bytes=32 time=36ms TTL=128
```