# DFL-700 FAQ

Table of Contents

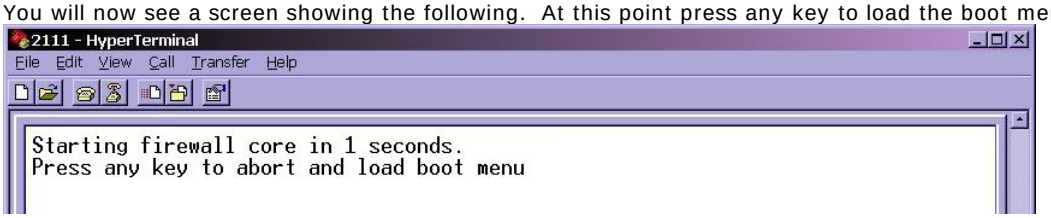

| | Page |
|---|---|
| 1) How do I do a factory reset | 2 |
| 2) How do you backup the DFL-700's configuration? | 2 |
| 3) How do I block URLs using the Content Filtering function? | 3 |
| 4) How do I limit outgoing web (HTTP) traffic using the Traffic Shaping function of the DFL-700? | 6 |
| 5) How do I limit all Internet access to a certain time (9am-6pm) using the Schedule function of the DFL-700? | 9 |
| 6) The service I need to use is not listed in the group of pre-defined services. How do I create a custom service on the DFL-700? | 13 |
| 7) I am running a web server on my network via the DMZ port. How do I open up port 80 (http) to my web server so that it can be accessed from the Internet? | 14 |
| 8) How do I limit Internet access to web browsing (HTTP) and email only but block the rest of the traffic? | 17 |

# How do I do a factory reset on the unit?

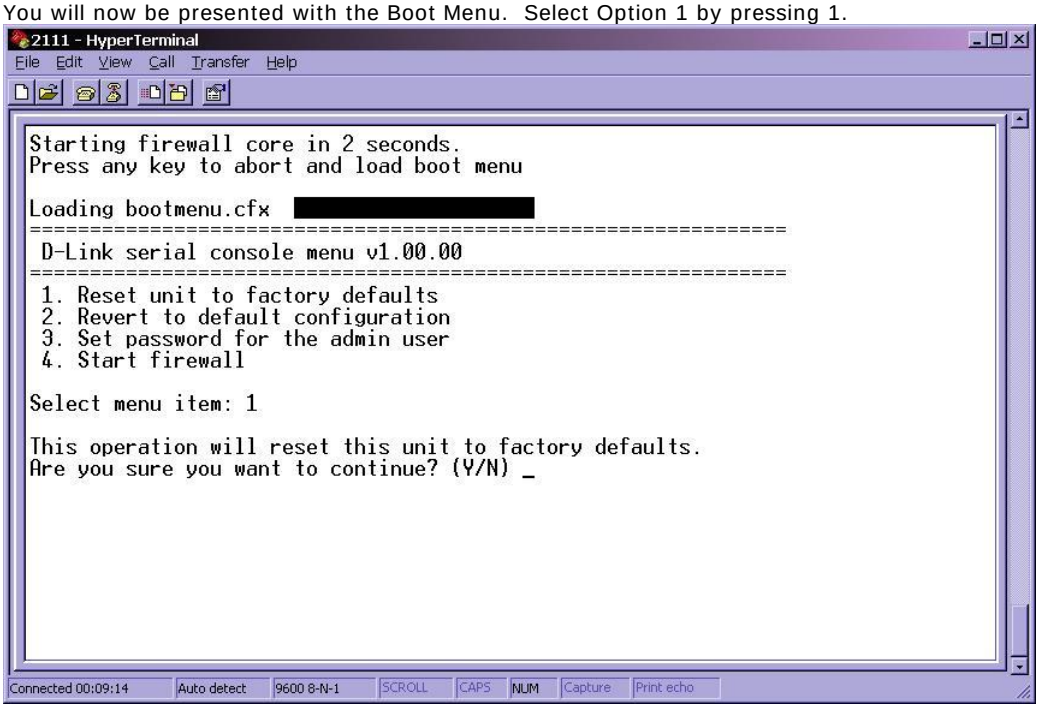
Factory reset using the 'Reset' button.
1) Make sure that the DFL-700 is on.
2) Press and hold the reset button for 10 seconds.
3) Release the button.

Factory Reset using the Web configuration
4) Login to the DFL-700 web interface using its IP address (i.e. https://192.168.1.1)
5) Click on **Tools→ Reset→ Reset to Factory Defaults**

Factory reset using the Console connection
1) Connect one end of the supplied Serial Cable to the DFL-700 and connect the other end to your PC.
2) Run **Hyperterminal** from Start→ Programs→ Accessories→ Communications
3) Create a connection. Enter the Name. Click OK.
4) Under 'Connect Using', select the COM port that the serial cable is connected to. Click OK
5) Set the COM properties to 9600, 8, N, 1, Hardware. Click OK. You will now see a blank screen which shows connected at the bottom left hand corner of the screen.
6) Power off for 5 seconds and then Power on the DFL-700.
7) You will now see a screen showing the following. At this point press any key to load the boot menu.




8) You will now be presented with the Boot Menu. Select Option 1 by pressing 1.



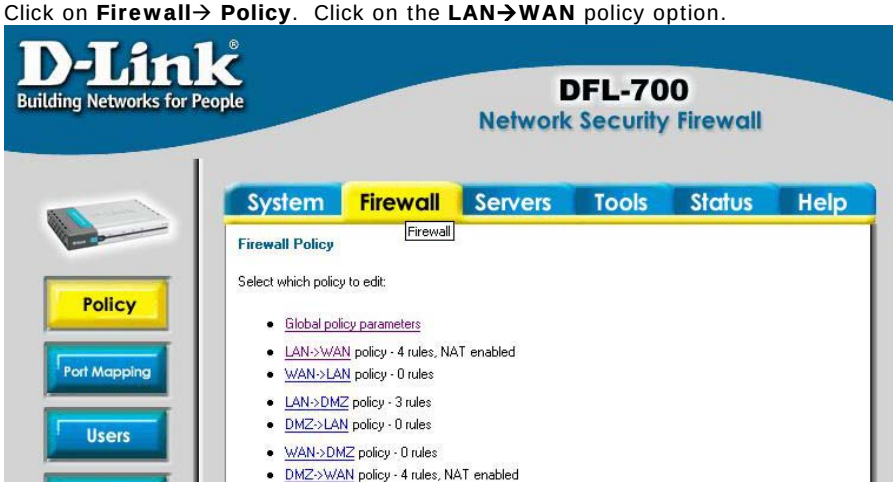

9) Press Y when prompted to continue. The unit will then reboot with the factory default settings.

# How do you backup the DFL-700's configuration?

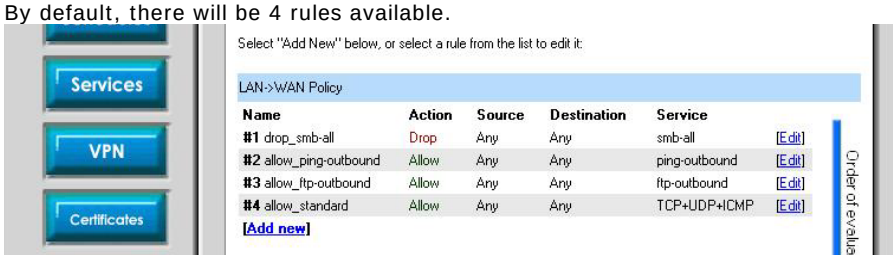
1) Log on to the DFL-700 using its IP address (i.e. https://192.168.1.1).
2) Click on **Tools→ Backup**.
3) Click on the **Download Configuration** button.
4) Save the 'backup.pkg' to your preferred location.

# How do I block URLs using the DFL-700's Content Filtering function?

1. Login to the DFL-700 web interface using its IP address (i.e. https://192.168.1.1).
2. Click on **Firewall→ Policy**. Click on the **LAN→WAN** policy option.

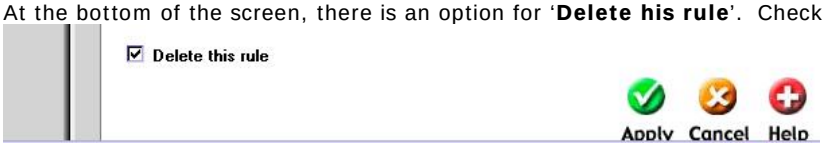



3. By default, there will be 4 rules available.

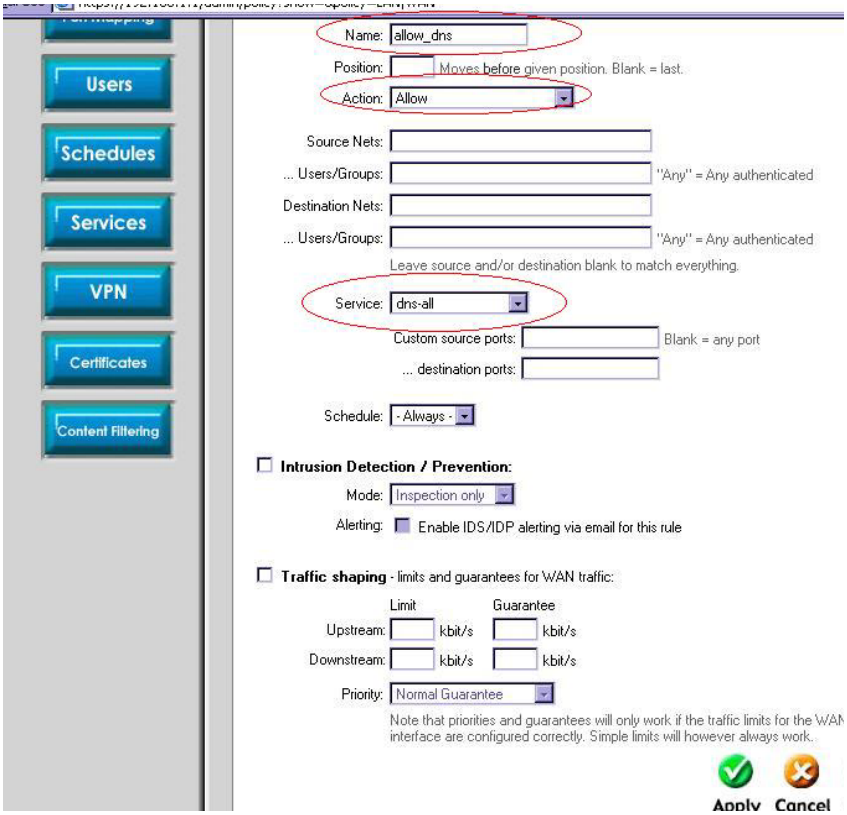



For content filtering to work, all HTTP traffic must go through a single policy, which uses the HTTP ALG. To do this, you must do the following.

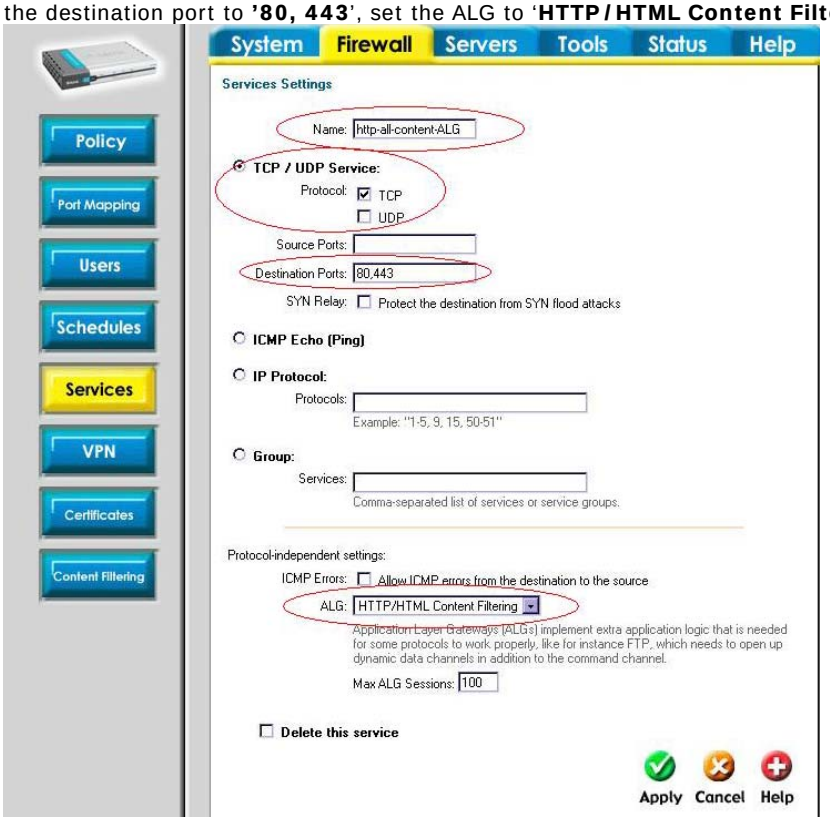
4. Delete the 'allow_standard' rule which allows all traffic from the LAN to go through
   i. Click on 'Edit' on the 'allow_standard' rule
   ii. At the bottom of the screen, there is an option for '**Delete his rule**'. Check this box then click on '**Apply**'



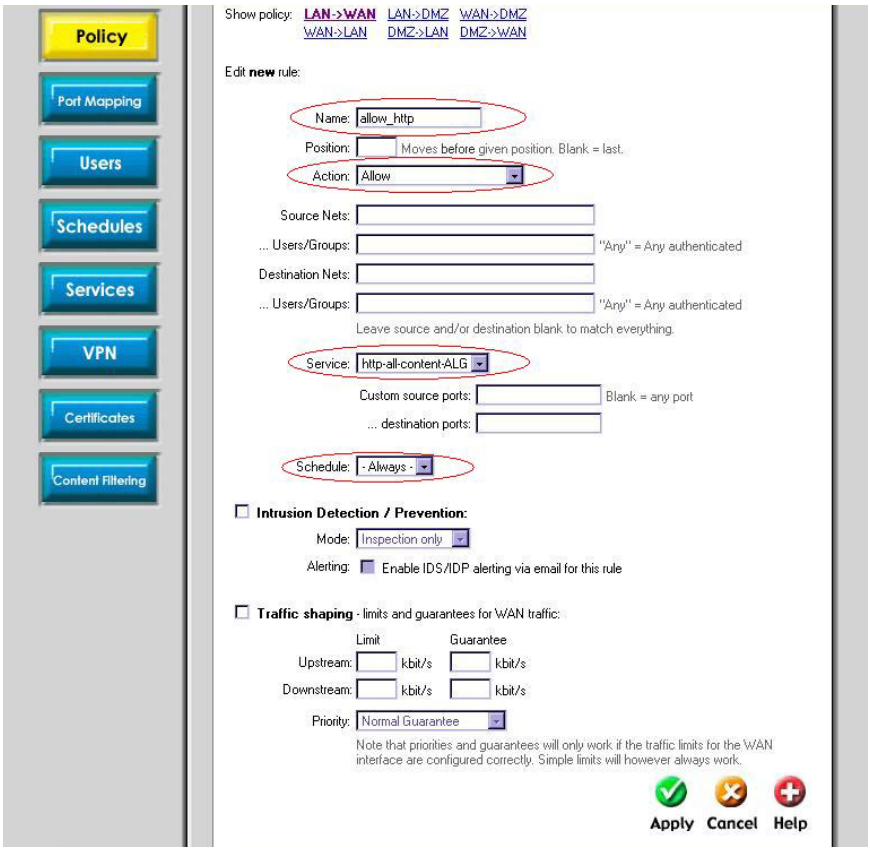

5. Create a rule to allow outgoing DNS
   i. Click on '**Add New**'
   ii. Enter the name as 'allow_dns', set the Action to '**Allow**', set the Service to '**dns-all**', set Schedule to '**Always**' then click on '**Apply**'




6. Create a rule for outgoing HTTP
   i. Click on **Firewall→ Services**, Click on '**Add New**'
   ii. Enter the name as 'http-all-content-ALG', select the **TCP/UDP Service**, check the **TCP** protocol box, set the destination port to **'80, 443**', set the ALG to '**HTTP/HTML Content Filtering**' then click on '**Apply**'

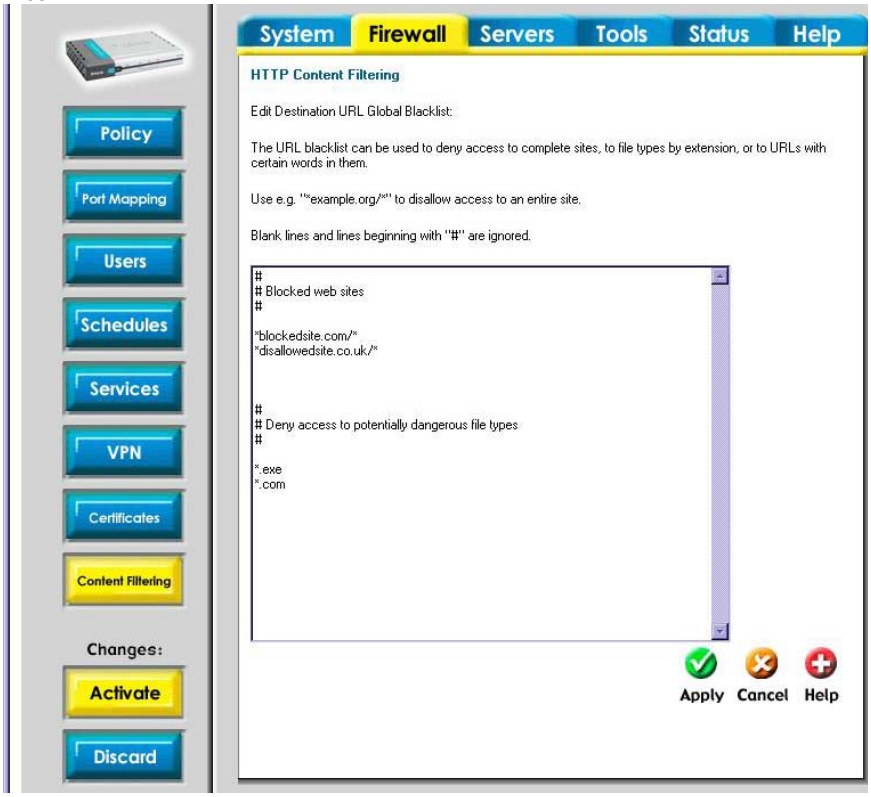



   iii. Click on **Firewall→ Policy→** click on **LAN→WAN** policy option
   iv. Click on '**Add New**'
   v. Enter the name as 'allow_http', set the Action to '**Allow**', set the Service to '**http-all-content-ALG**', set the Schedule to '**Always**' then click on '**Apply**'



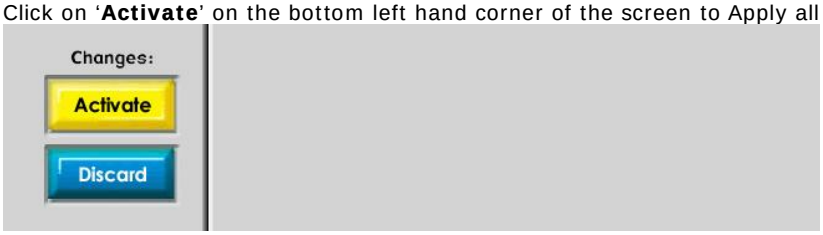

7. Adding URLs to the Blacklist
   i. Click on **Firewall→ Content Filtering,** click on '**Edit URL blacklist**'
   ii. Enter blocked URLs in the following format:
   *blockedsite.com/*
   *disallowedsite.co.uk/*

   iii. To block potentially malicious file types, enter file extensions in the following format:
   *.exe
   *.com

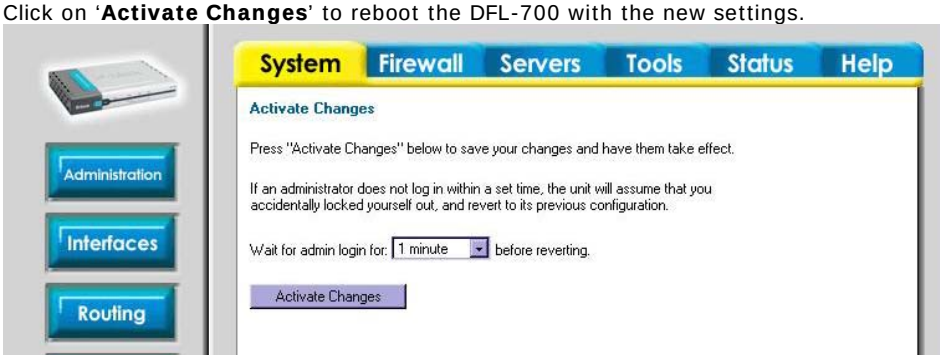


iv. Click on **Apply** when done.

8. Click on '**Activate**' on the bottom left hand corner of the screen to Apply all changes.

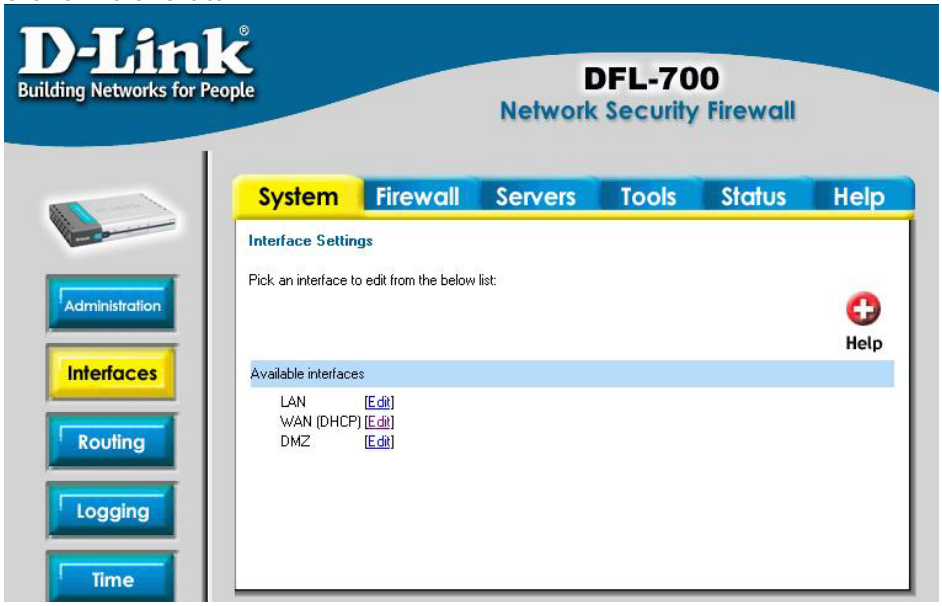



9. Click on '**Activate Changes**' to reboot the DFL-700 with the new settings.

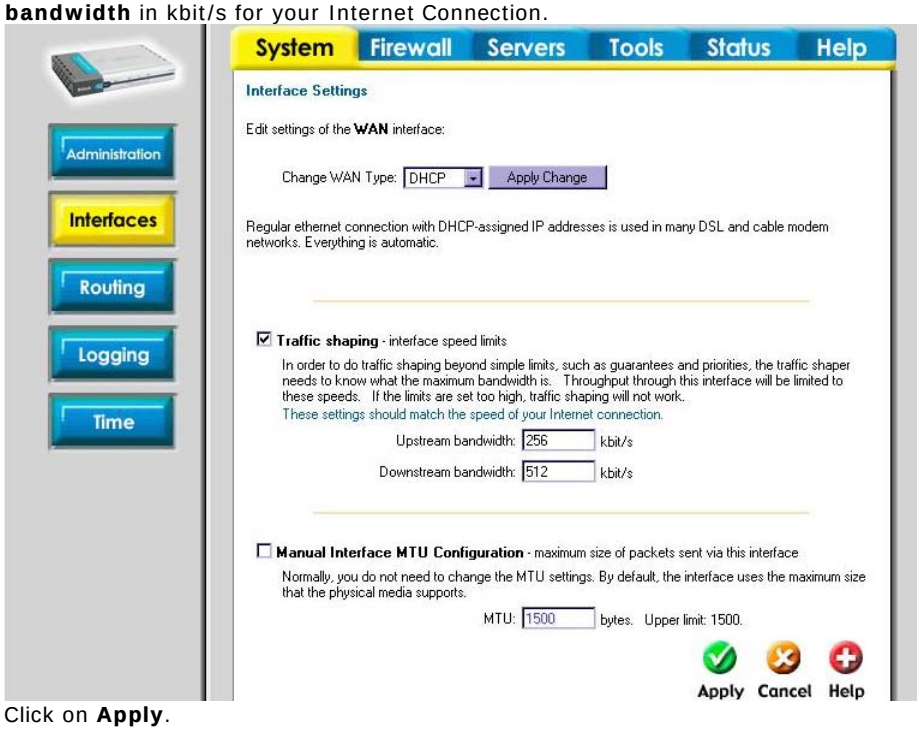


# How do I limit outgoing web (HTTP) traffic using the Traffic Shaping function of the DFL-700?

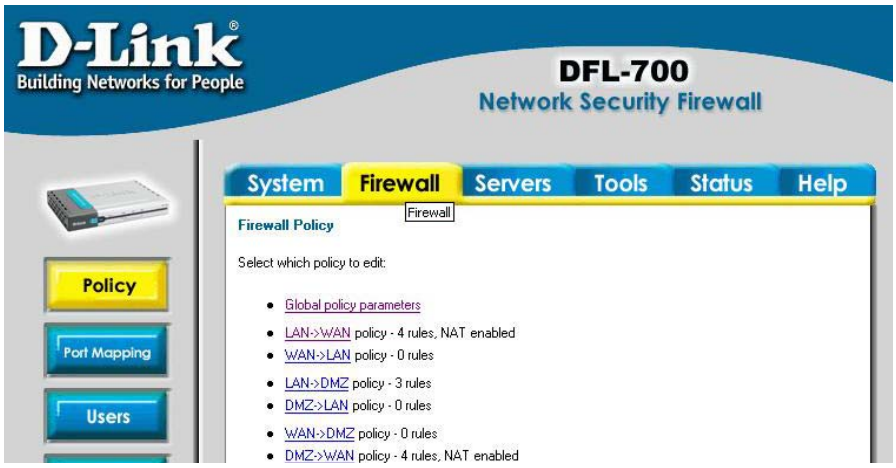
1) Login to the DFL-700 web interface using its IP address (i.e. https://192.168.1.1).
2) Click on **System→ Interfaces→**
3) Click on **Edit** next to **WAN**




10. Check the **Traffic Shaping** – interface speed limits. Set **the Upstream bandwidth** and the **Downstream bandwidth** in kbit/s for your Internet Connection.

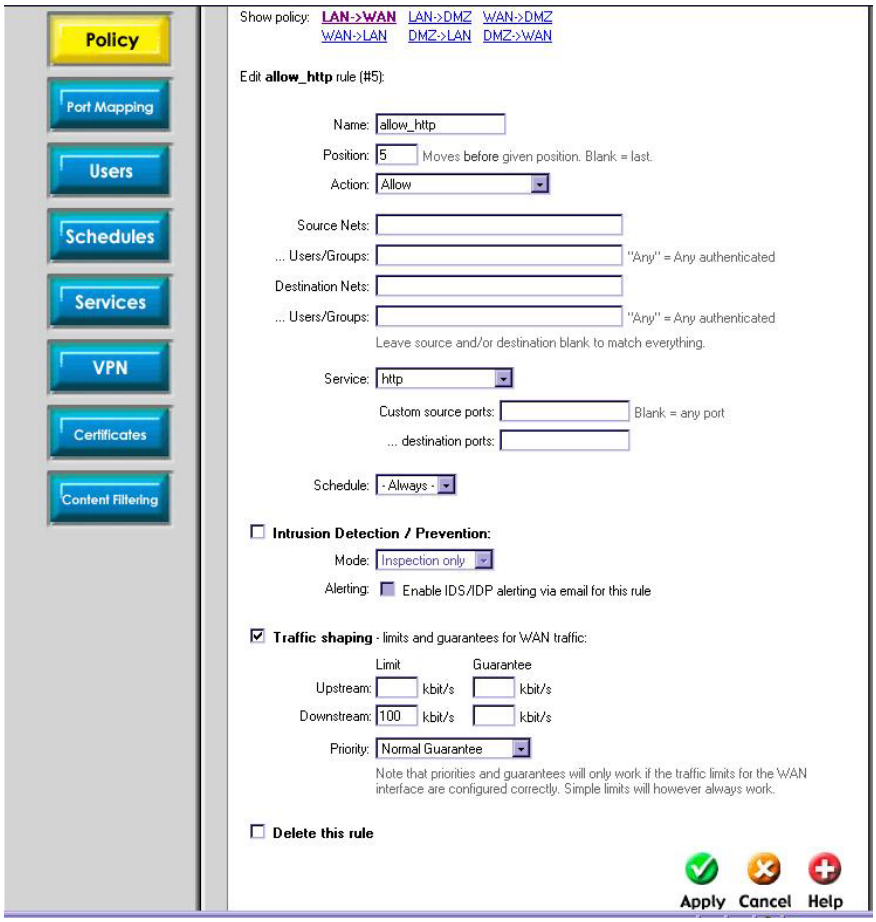



11. Click on **Apply**.
12. Click on **Firewall→ Policy→ 'LAN→WAN'** policy.

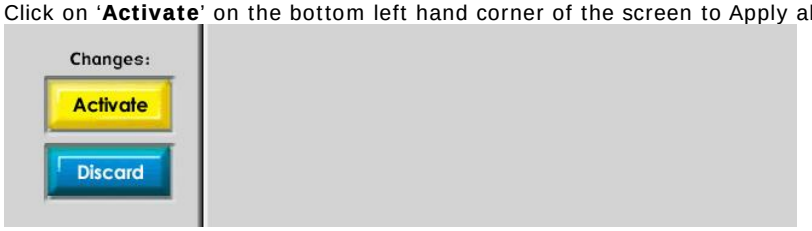



10) Click **Edit** on the policy that you would like to apply the Traffic Shaping to. In this example, it is the '**allow_http**' policy.

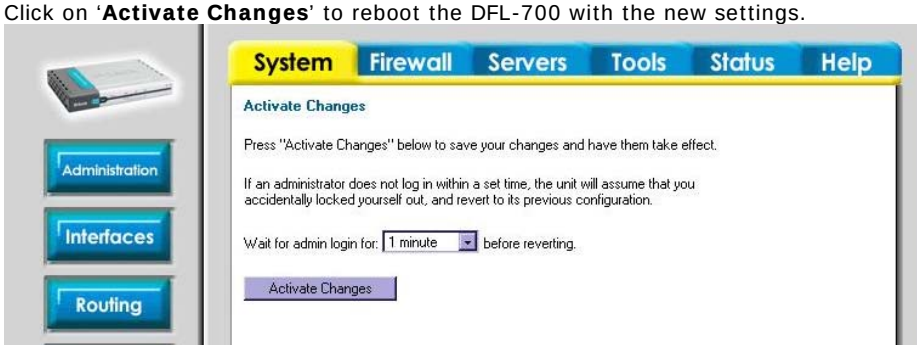

11) Check the **Traffic Shaping** option on the policy and enter the speed that you would like the HTTP Downstream traffic limited to in the **Downstream** option. In this example, it is 100 kbit/s. Click on **Apply**.




12) Click on '**Activate**' on the bottom left hand corner of the screen to Apply all changes.

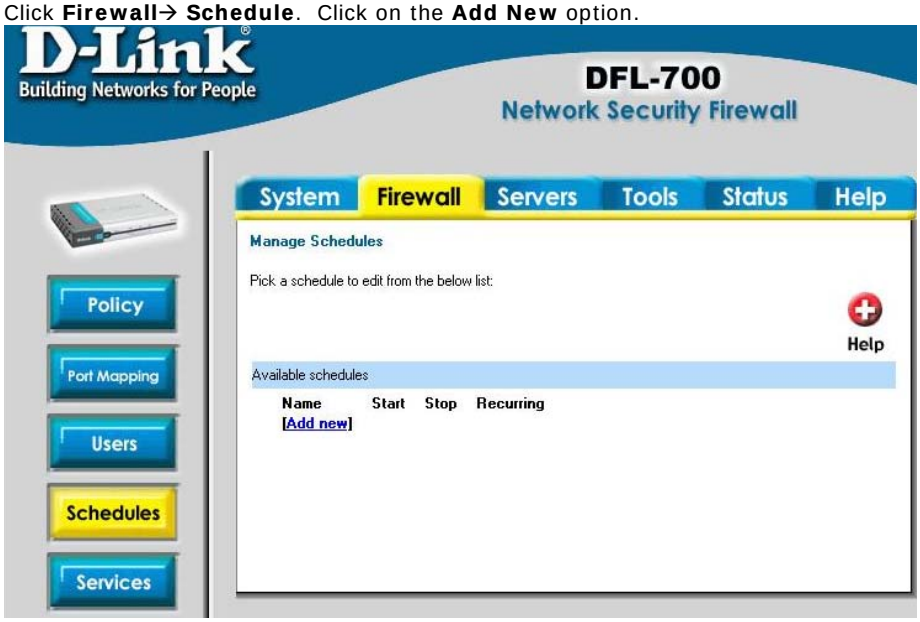



13) Click on '**Activate Changes**' to reboot the DFL-700 with the new settings.

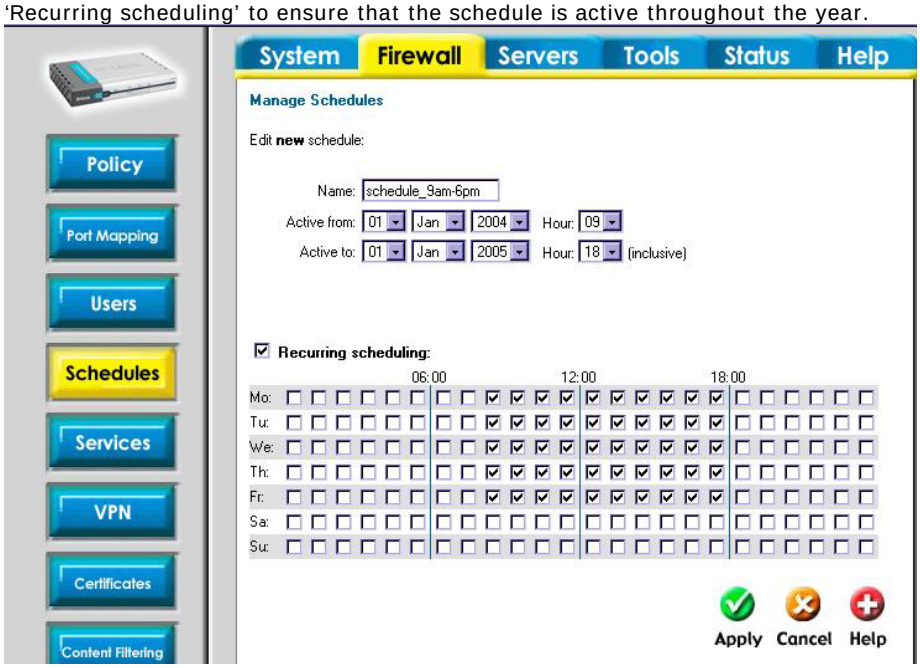


# How do I limit all Internet access to a certain time (9am-6pm) using the Schedule function of the DFL-700?

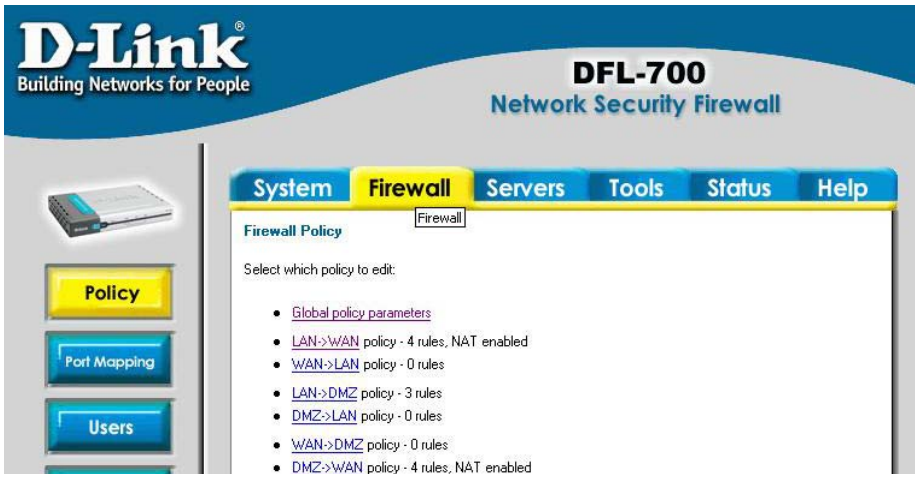
1. Login to the DFL-700 web interface using its IP address (i.e. https://192.168.1.1).
2. Click **Firewall→ Schedule**. Click on the **Add New** option.



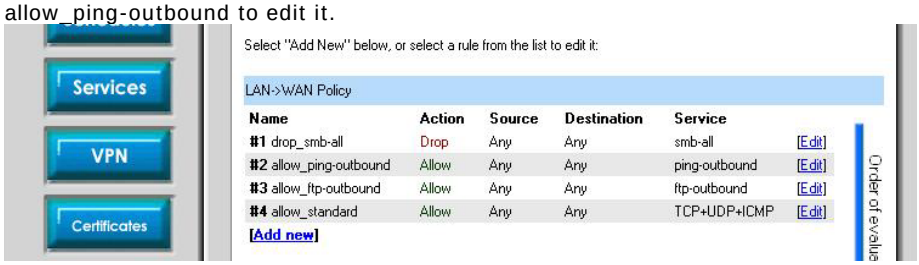

3. Enter the following details for the new Schedule. Set the name as 'schedule_9am-6pm'. Set the Active from date: 01 Jan 2004 and the Hour to 9. Set the Active to date: 01 Jan 2005 and the Hour to 18. Check the 'Recurring scheduling' to ensure that the schedule is active throughout the year.



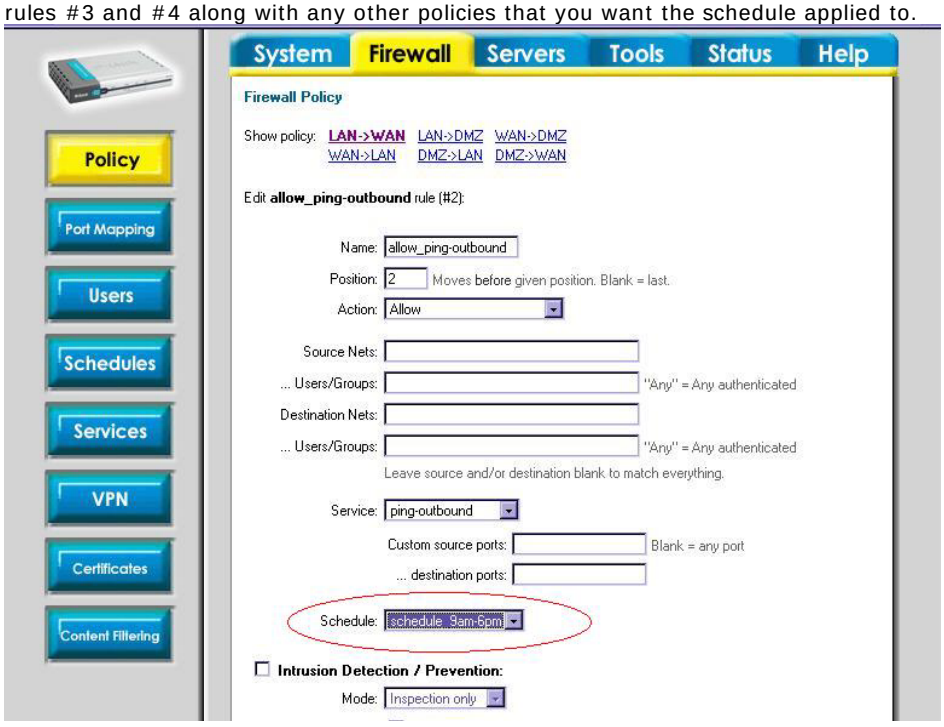

4. Click on **Firewall→ Policy**. Click on the **LAN→WAN** policy option.



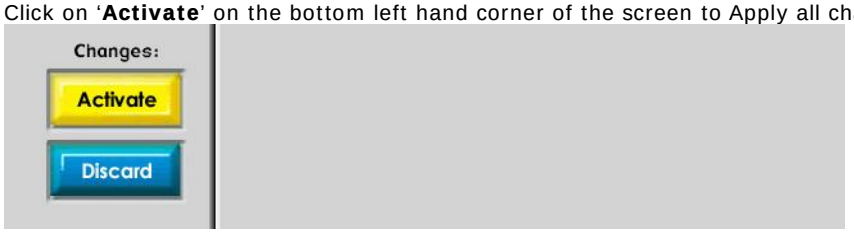

5. By default, there will be 4 rules available. Apply the schedule to rules #2, #3, and #4. Click on **Edit** on #2 allow_ping-outbound to edit it.



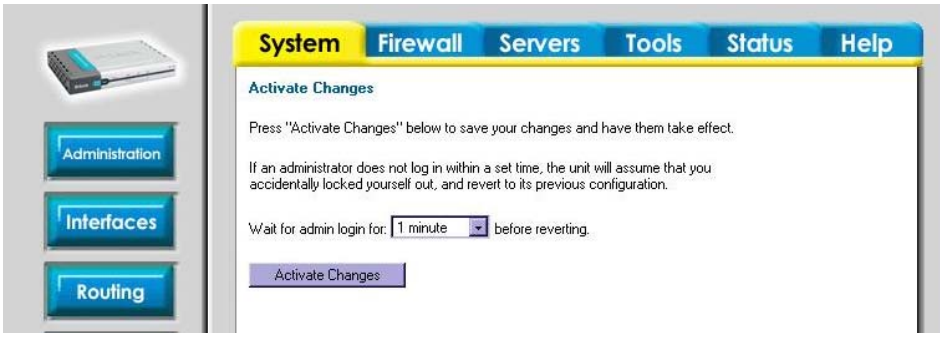

6. Set the **Schedule** option to the newly created schedule 'schedule_9am-6pm'. Click on **Apply**. Do the same for rules #3 and #4 along with any other policies that you want the schedule applied to.




7. Click on '**Activate**' on the bottom left hand corner of the screen to Apply all changes.

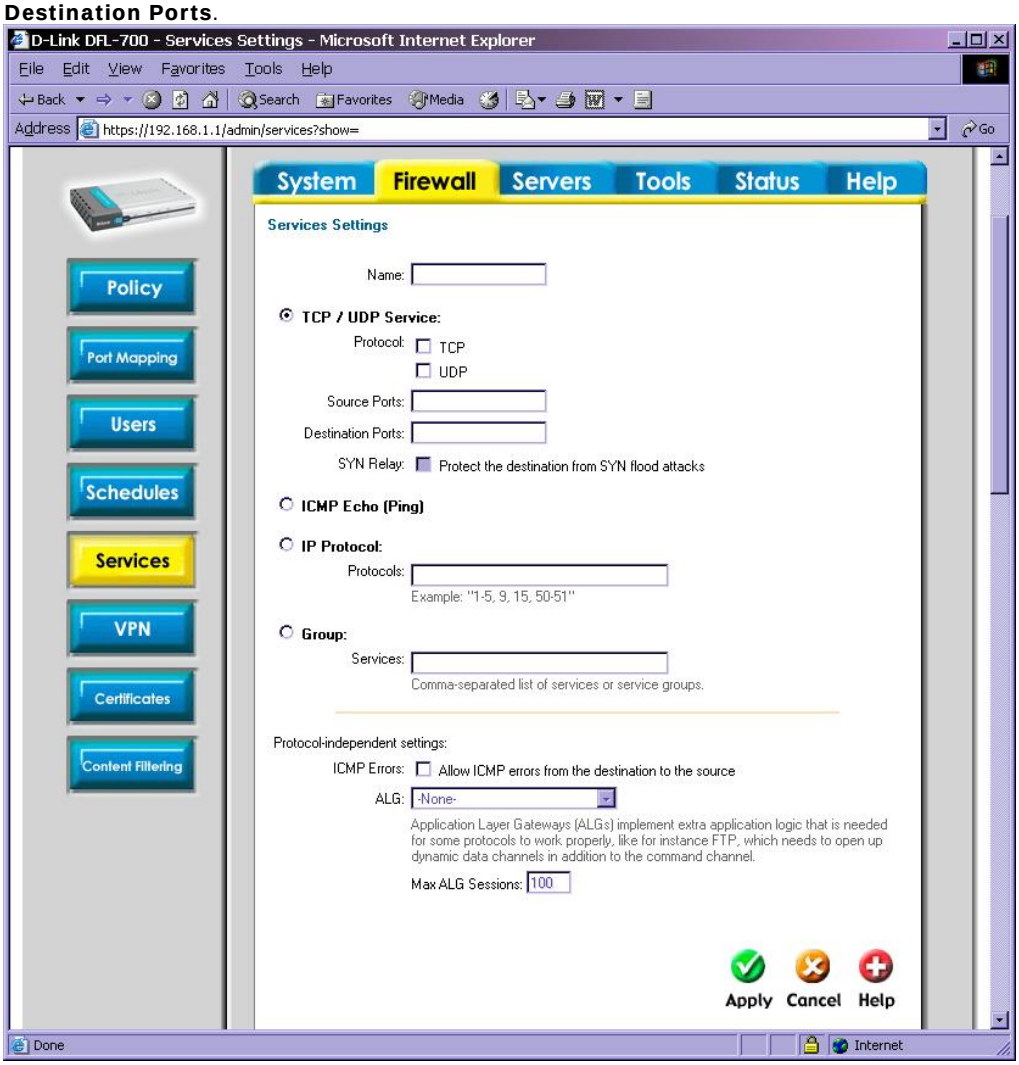



8. Click on '**Activate Changes**' to reboot the DFL-700 with the new settings.


System
Firewall
Servers
Tools
Status
Help
Administration
Interfaces
Routing
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

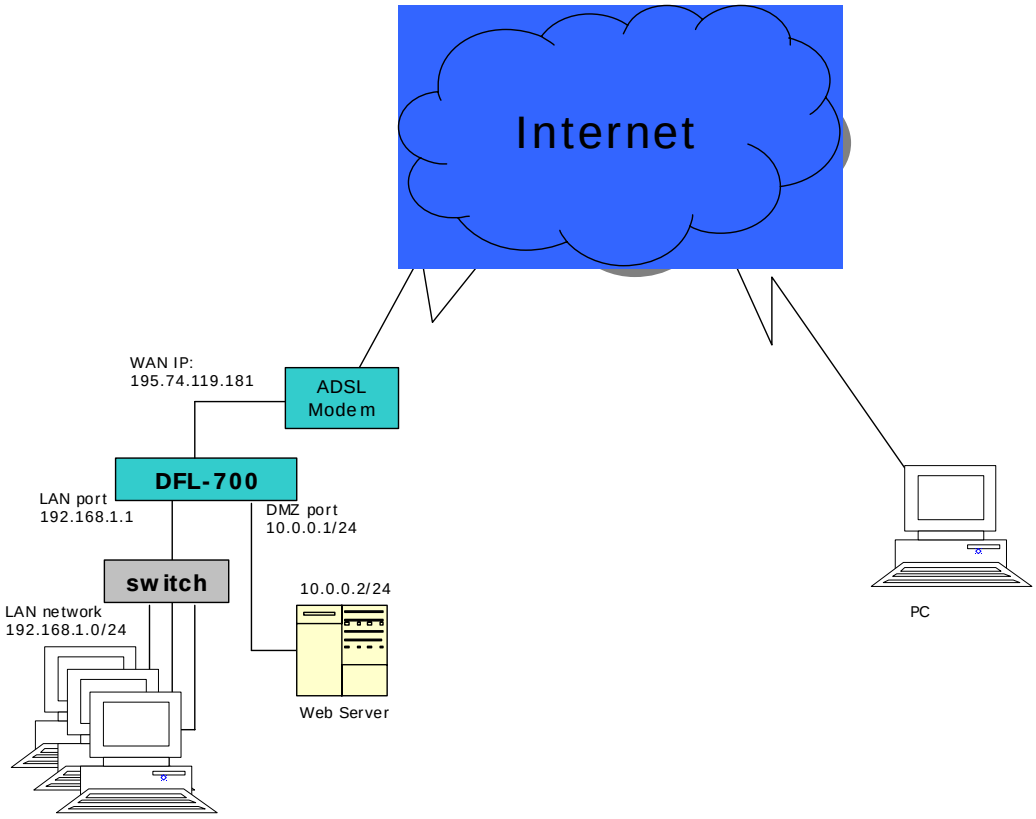
# The service I need to use is not listed in the group of pre-defined services. How do I create a custom service on the DFL-700?

1) Log onto the DFL-700 using its IP address (i.e. https://192.168.1.1).
2) Click on **Firewall→ Services**. This will list the pre-defined services that are available on the DFL-700.
3) Click on **Add New** at the bottom of the screen
4) Enter the name of the new service that you would like to add in the **Name** box.
5) Select the type of service from **TCP/UDP Service**, **ICMP Echo(Ping)**, **IP Protocol**, **Group**
6) When entering a **TCP/UDP Service**, select the protocol type (**TCP** or **UDP**) and enter the **Source Ports** and the **Destination Ports**.

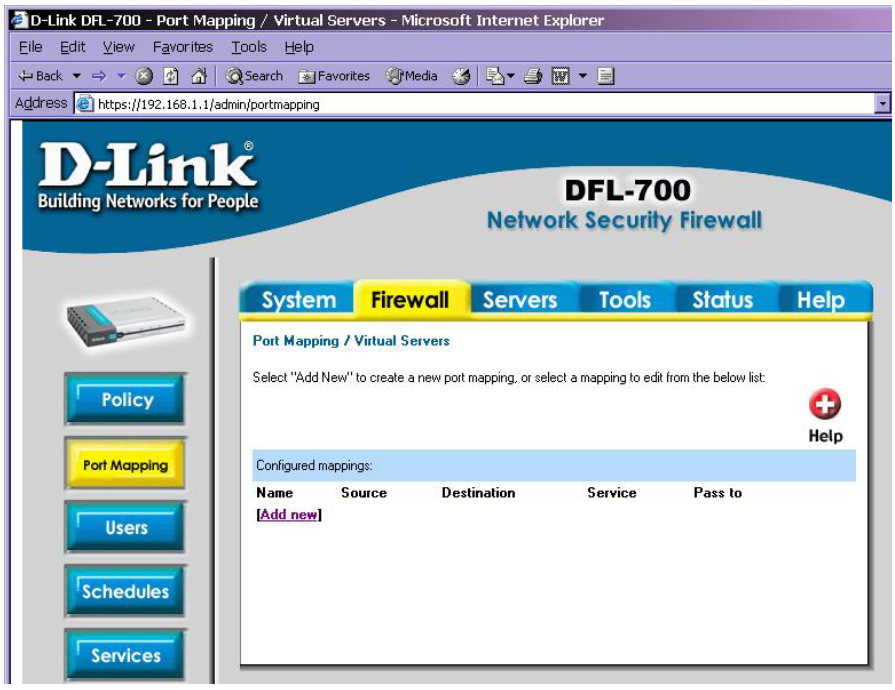



7) Click on **Apply**.
8) Click on **Activate** at the bottom left hand corner of the screen
9) Click on the **Activate Changes** button to restart the DFL-700 with the new settings.
10) On reboot, this new service that you have created will be available when creating a new Firewall Policy and Port Mapping.

# I am running a web server on my network via the DMZ port. How do I open up port 80 (http) to my web server so that it can be accessed from the Internet?

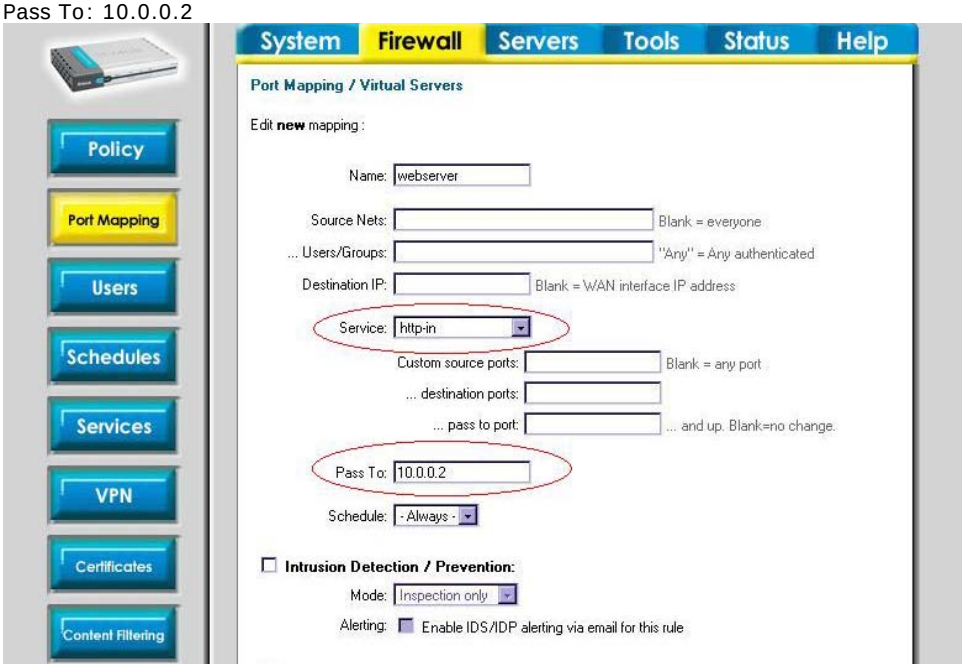



1. Login to the DFL-700 web interface using its IP address (i.e. https://192.168.1.1).
2. Click **Firewall→ Port Mapping**. Click on the **Add New** option.



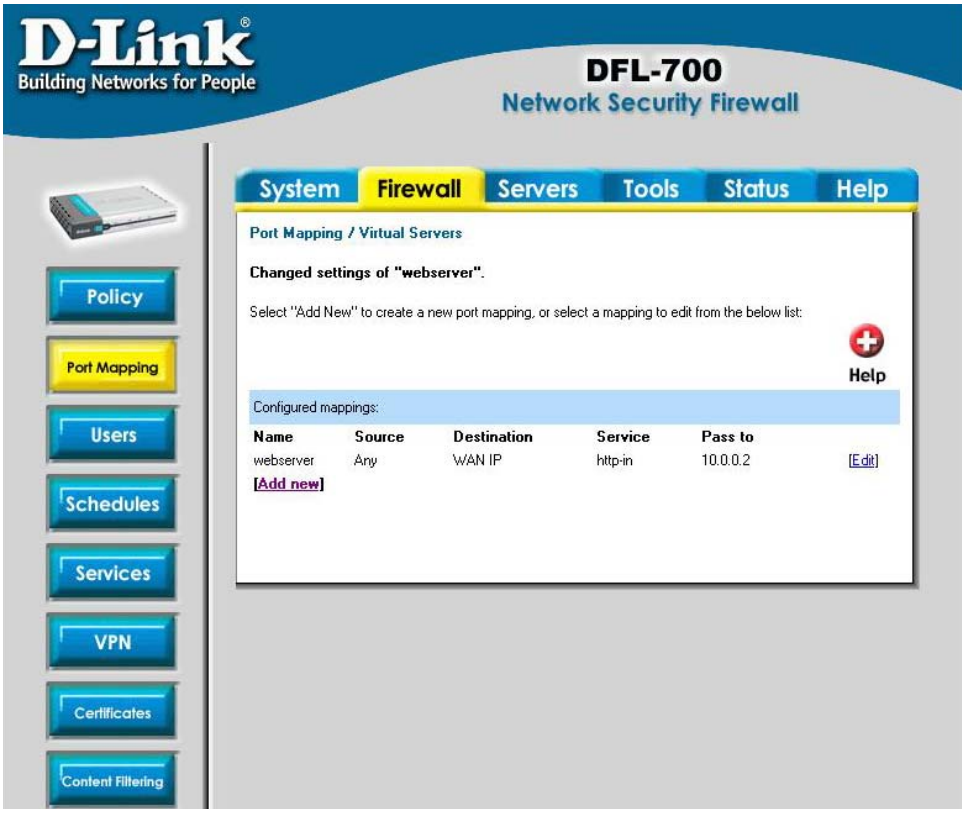

3. In the New port mapping entry, enter the following details:

Name: webserver
Service: http-in
Pass To: 10.0.0.2



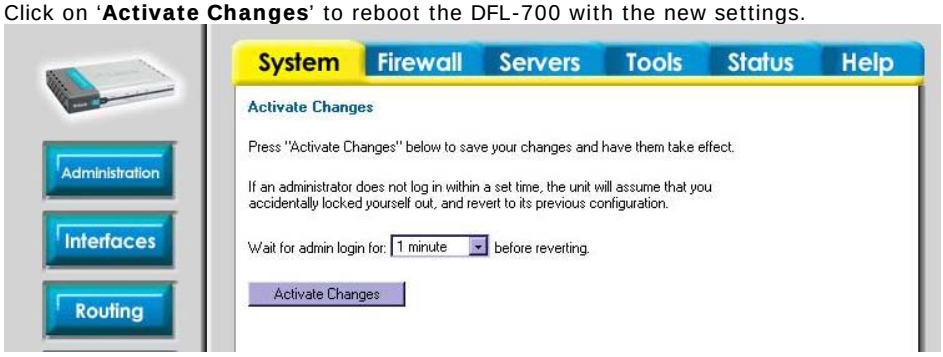

Click on **Apply**.

4. The new port mapping entry will how show under the configured mappings.



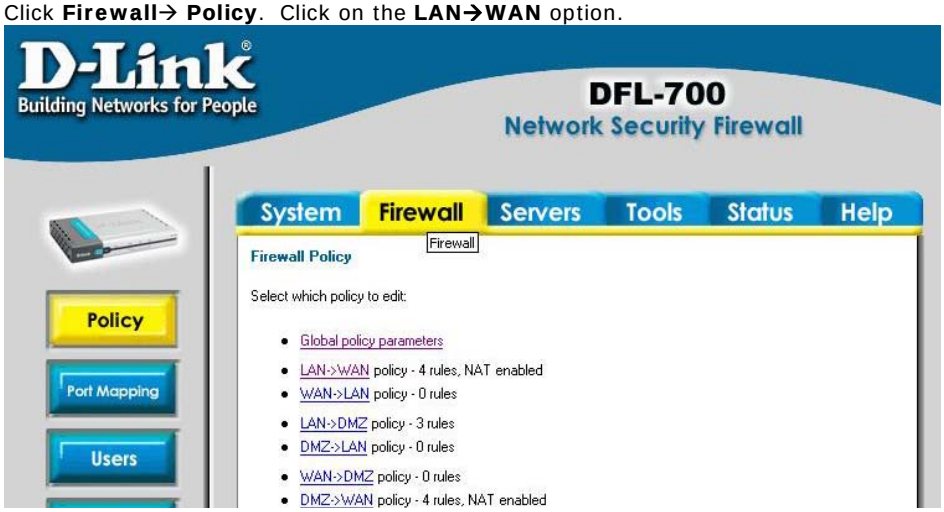

5. Click on '**Activate**' on the bottom left hand corner of the screen to Apply all changes.


6. Click on '**Activate Changes**' to reboot the DFL-700 with the new settings.

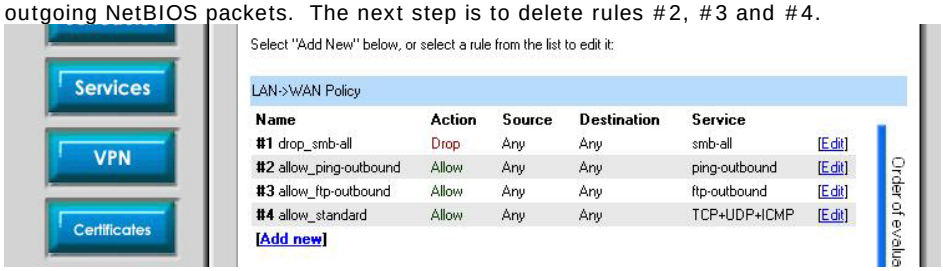


# How do I limit Internet access to web browsing (HTTP) and email only but block the rest of the traffic?

1. Login to the DFL-700 web interface using its IP address (i.e. https://192.168.1.1).
2. Click **Firewall→ Policy**. Click on the **LAN→WAN** option.

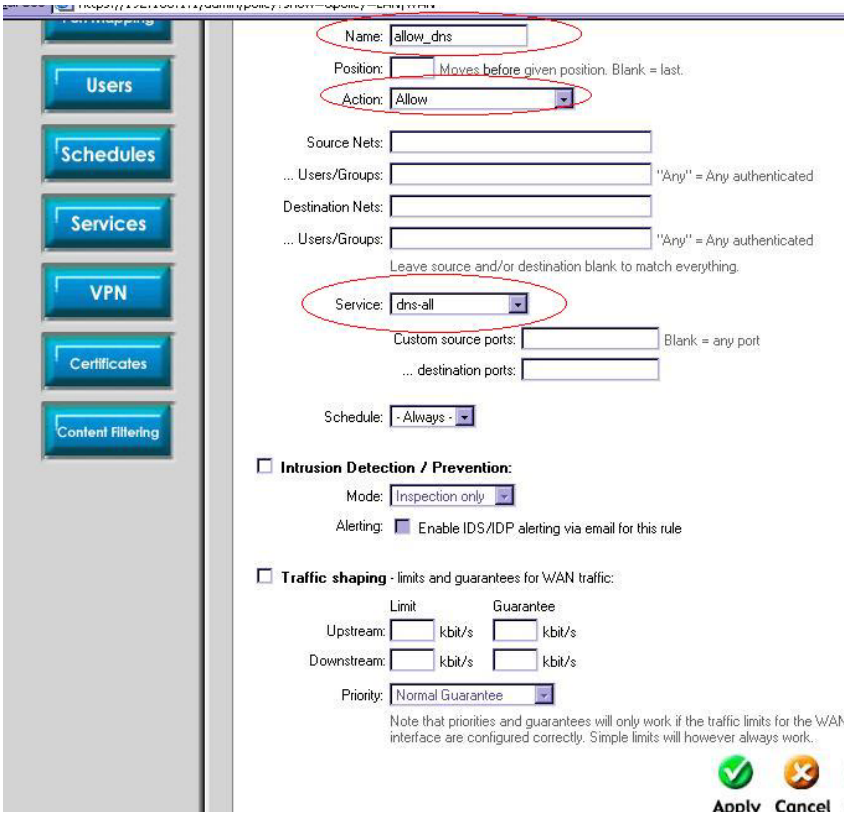



3. The DFL-700 has 4 default LAN→WAN rules available. You can leave the first policy as this one just drops outgoing NetBIOS packets. The next step is to delete rules #2, #3 and #4.

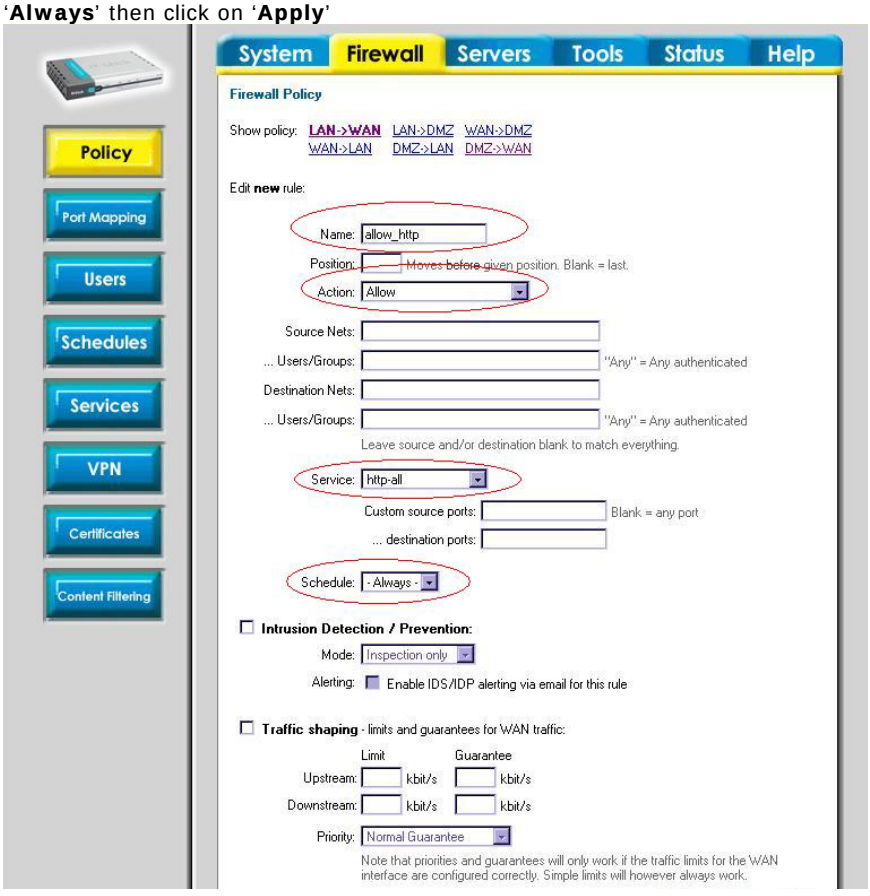



To delete, click on **Edit**, on rule #2. At the bottom of the screen, check the box called '**Delete this rule**' then click on **Apply** to delete the rule. Repeat the same steps for rules #3 and #4.


4. The next step is to add the new rules for traffic that you would like to allow from the LAN through the firewall to the Internet. The first policy is to allow DNS (#2 Allow_DNS) – which is needed for DNS lookup (domain name resolution)
   i. Click on **Firewall→ Policy→ LAN→WAN** policy, Click on '**Add New**'
   ii. Enter the name as 'allow_dns', set the Action to '**Allow**', set the Service to '**dns-all**', set Schedule to '**Always**' then click on '**Apply**'

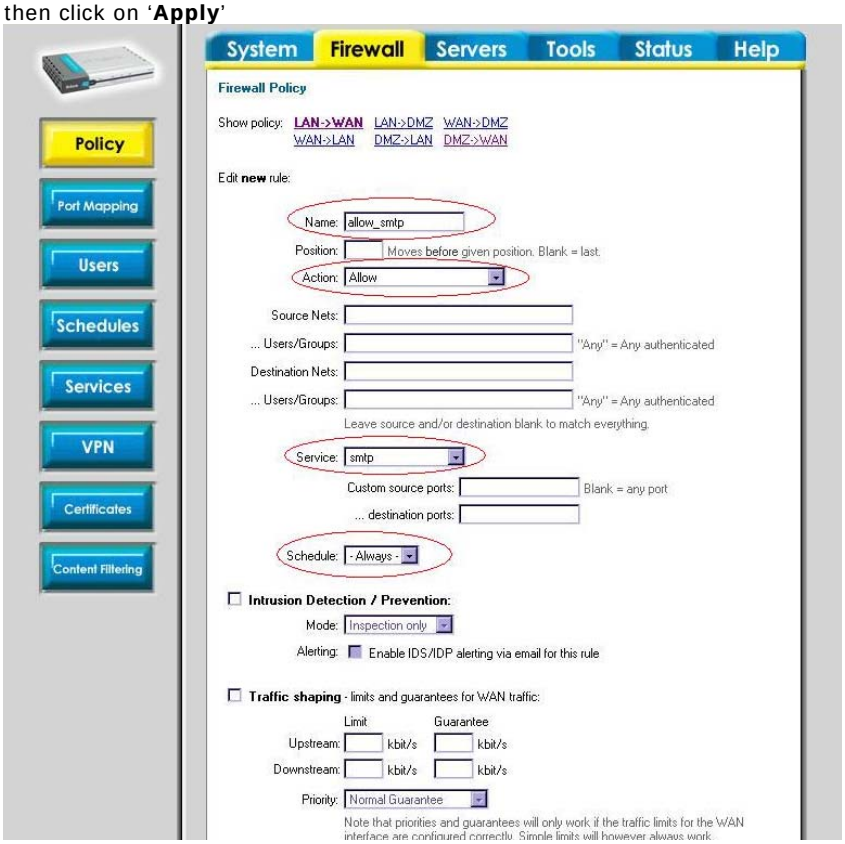



5. Create a policy to allow HTTP requests. #3 Allow_HTTP – rule for outgoing HTTP (web) requests.
   ii. Click on **Firewall→ Policy→ LAN→WAN** policy, Click on '**Add New**'
   iii. Enter the name as 'allow_http', set the Action to '**Allow**', set the Service to '**http-all**', set Schedule to '**Always**' then click on '**Apply**'




6. Create a policy to allow SMTP requests. #3 Allow_SMTP – rule for outgoing SMTP.
   iv. Click on **Firewall→ Policy→ LAN→WAN** policy, Click on '**Add New**'

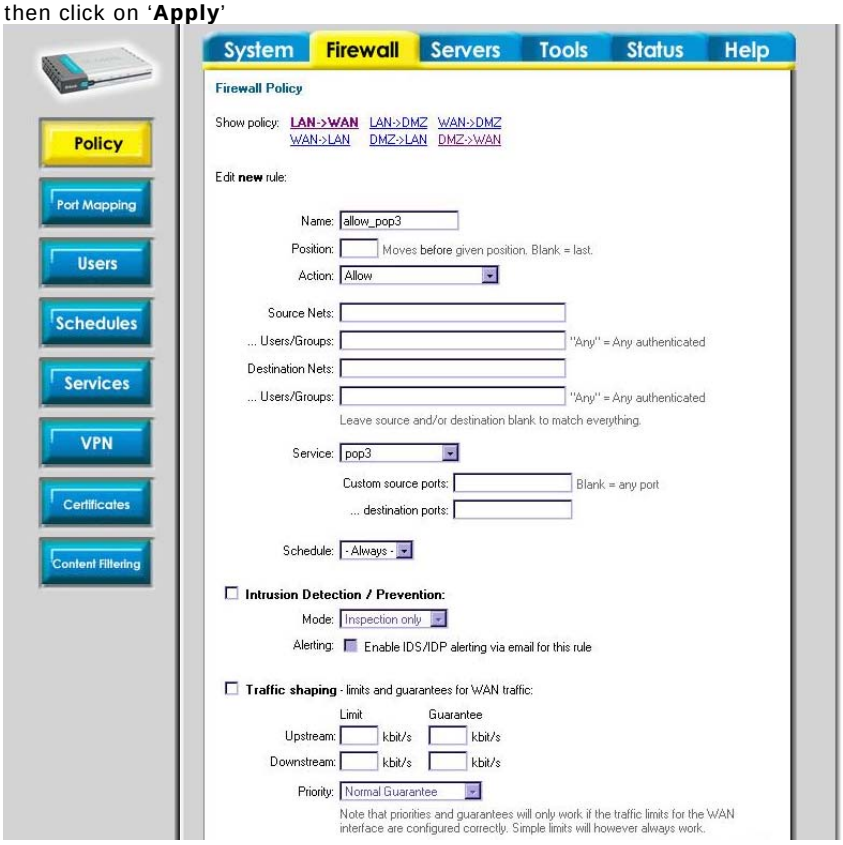
v. Enter the name as 'allow_smtp', set the Action to '**Allow**', set the Service to '**smtp**', set Schedule to '**Always**' then click on '**Apply**'




7. Create a policy to allow POP3 requests. #3 Allow_POP3 – rule for outgoing POP3 requests.

vi. Click on **Firewall→ Policy→ LAN→WAN** policy, Click on '**Add New**'

vii. Enter the name as 'allow_pop3', set the Action to '**Allow**', set the Service to '**pop3**', set Schedule to '**Always**' then click on '**Apply**'




8. Click on '**Activate**' on the bottom left hand corner of the screen to Apply all changes.


9. Click on '**Activate Changes**' to reboot the DFL-700 with the new settings.