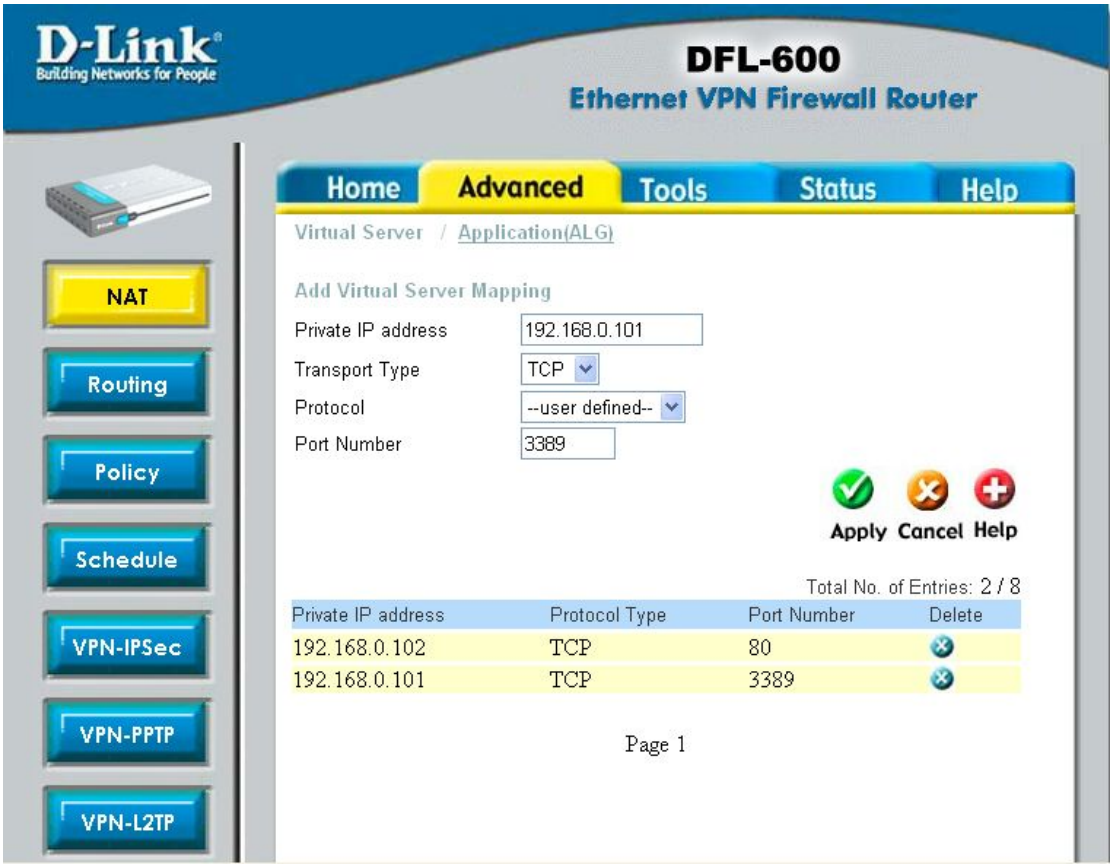
How to configure policies in the DFL-600

Example:

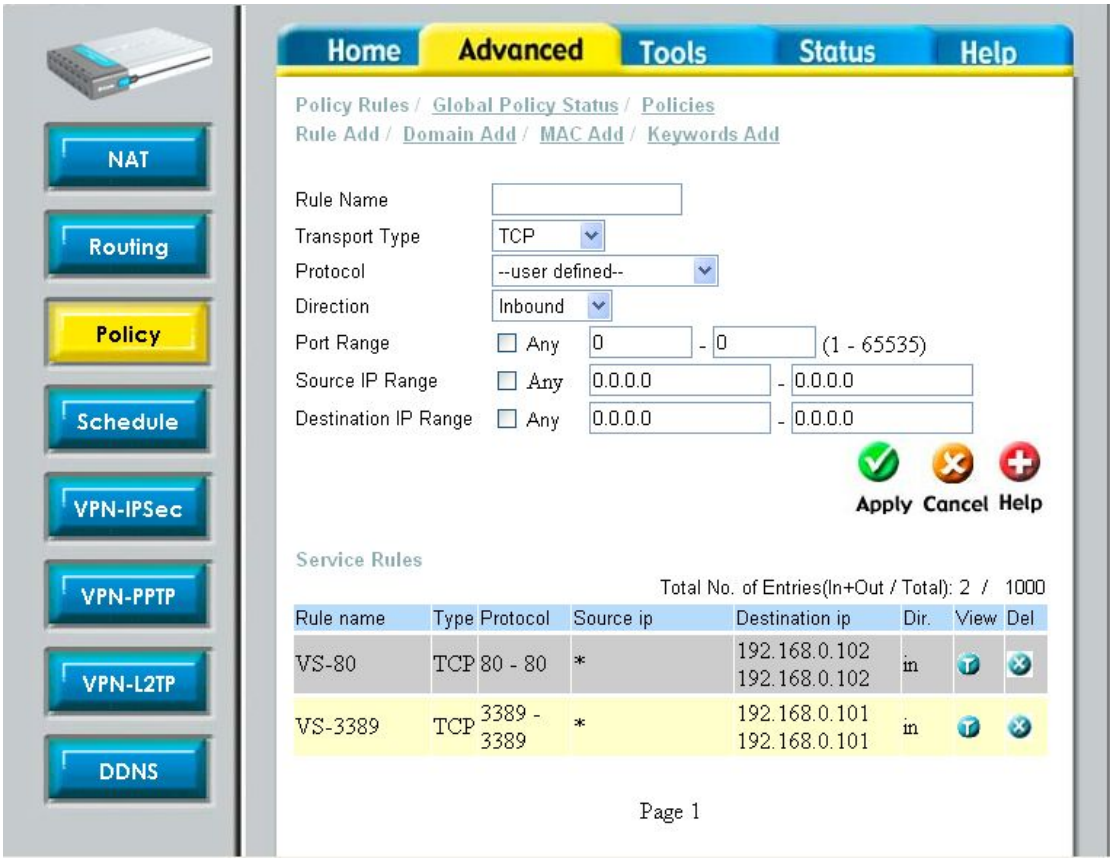
-Allow port redirection on port 80 TCP for ANY IP address (anyone can see the web site)

-Allow port redirection on port 3389 TCP for certain IP address only, e.g. 201.2.2.2 (only 201.2.2.2 can use Remote Desktop connection).

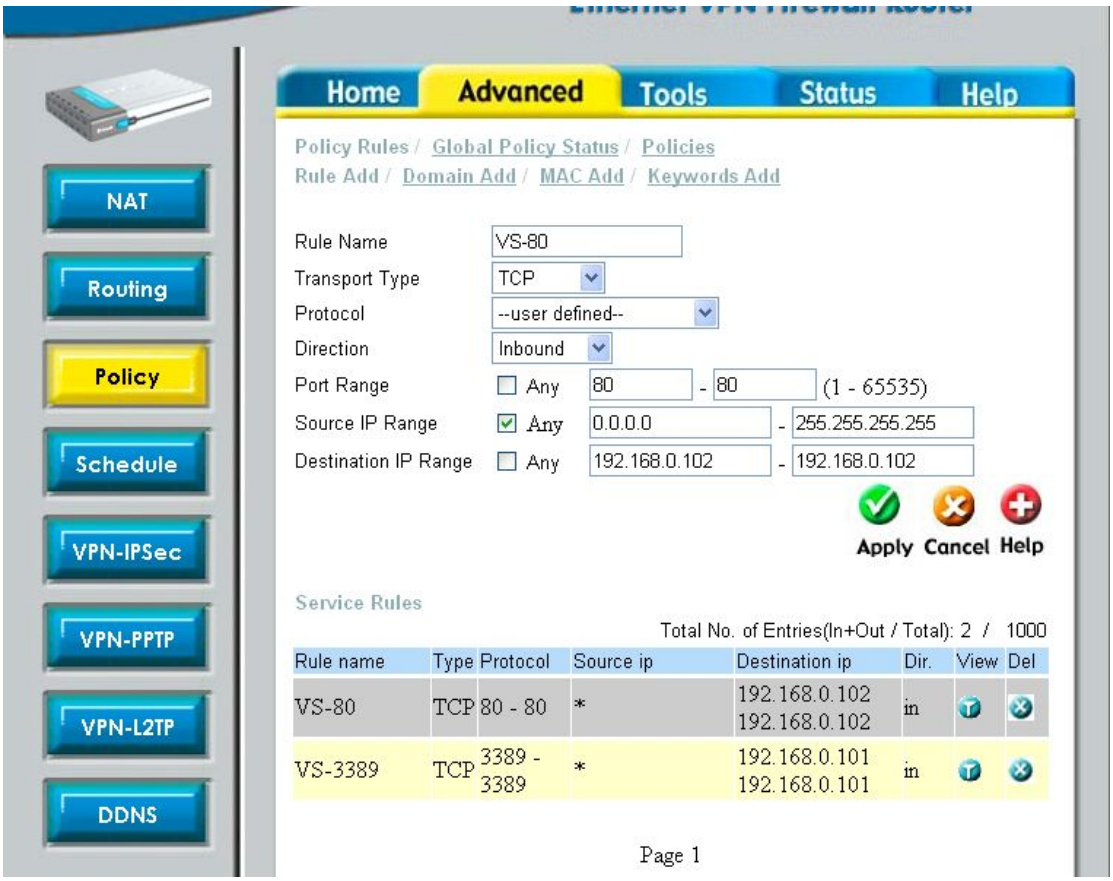
1. Add two virtual servers to redirect TCP port 80 and 3389 to internal servers.



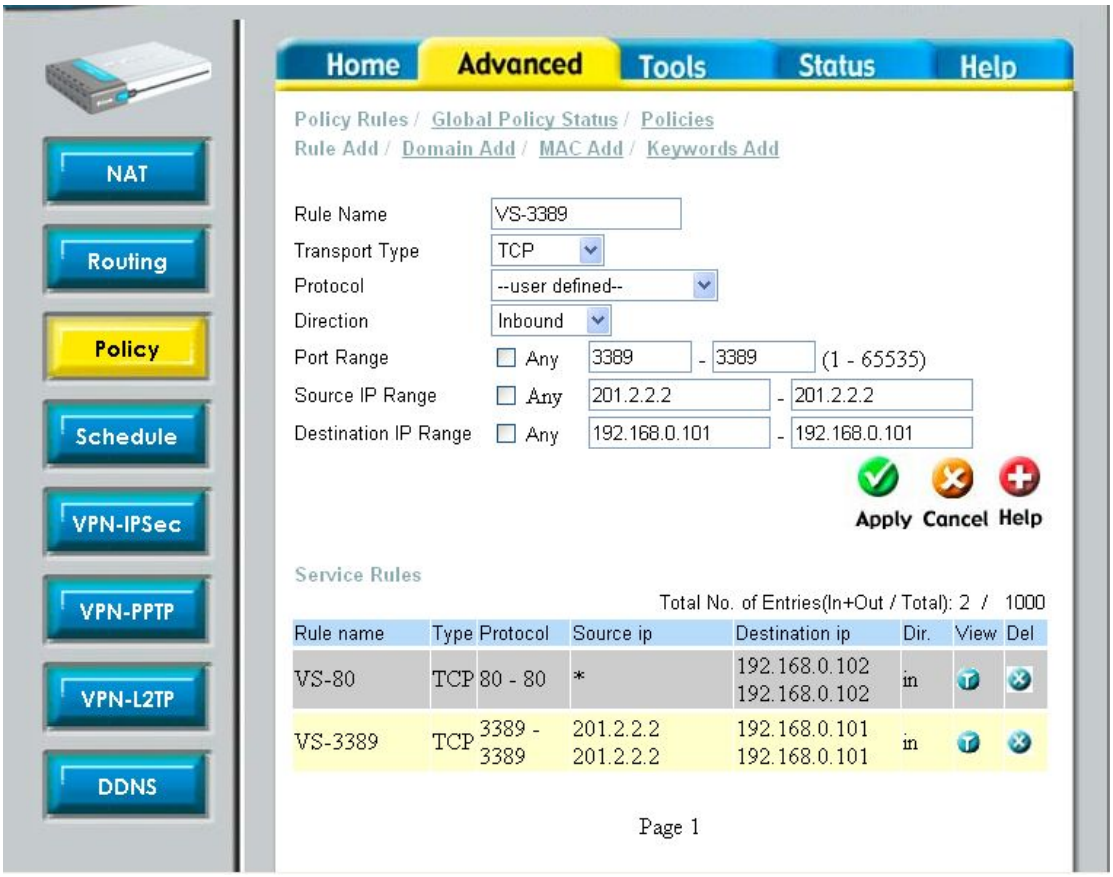
2. After adding 2 virtual servers as above, add two policy rules as below:



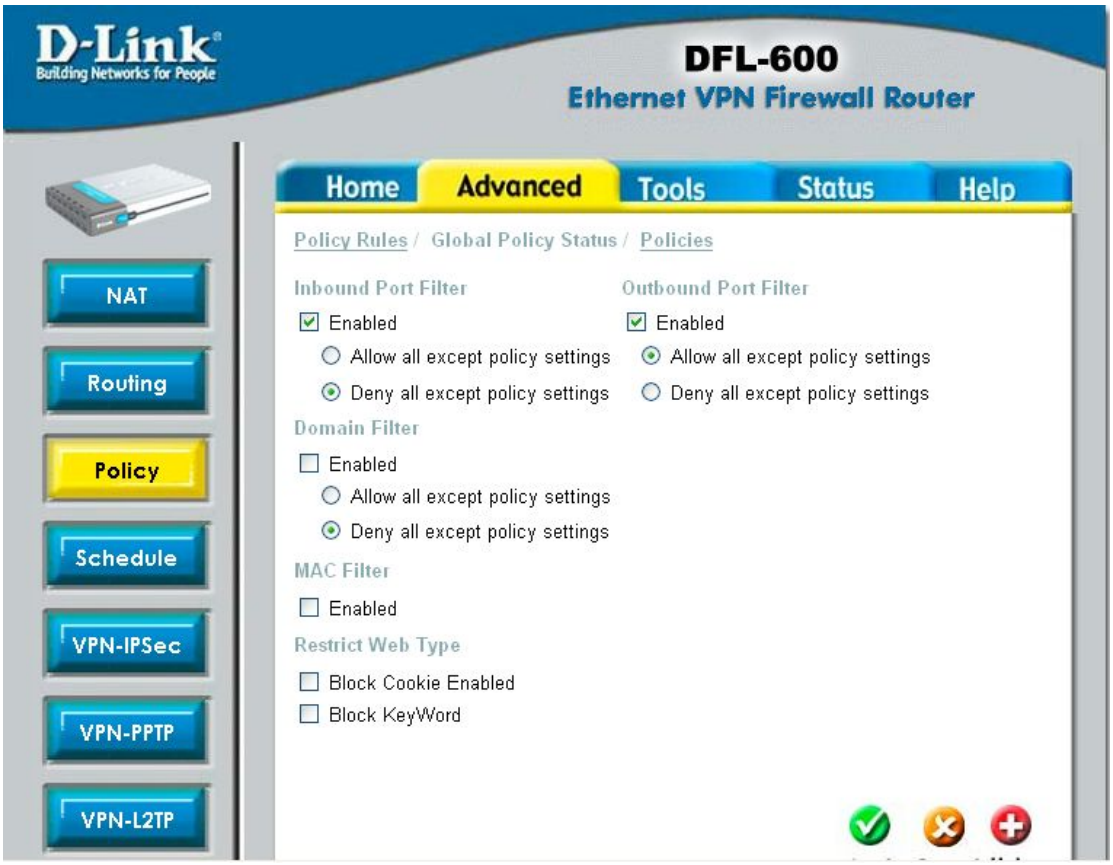
3. Edit these two rules. Press  in “View” field to edit these two rules to meet your requirements. For rule VS-80 (anyone can see the web site), Source IP range set to “ANY”.



For rule VS-3389 (only 201.2.2.2 can use Remote Desktop connection), Source IP Range must have “201.2.2.2-201.2.2.2.

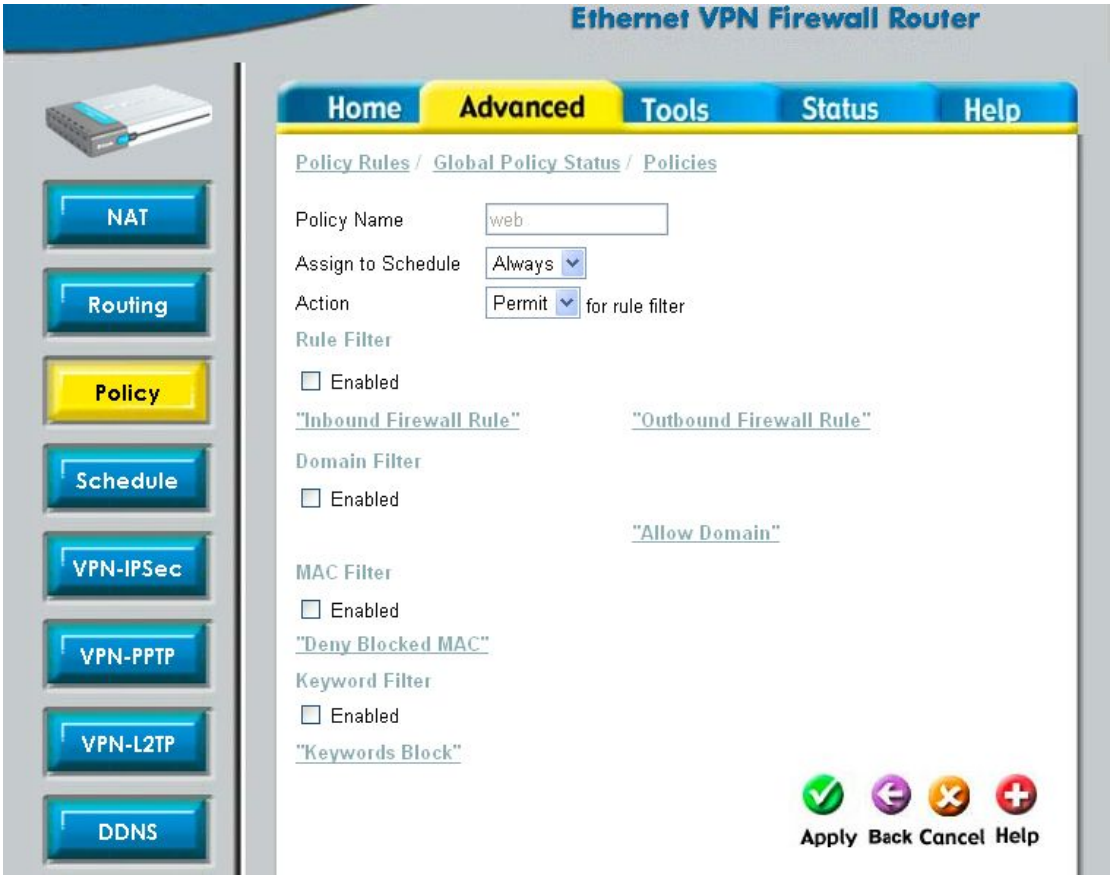


4. Configure “Global Policy Status” as below. In Inbound Port Filter enable ”Deny all except policy settings”.

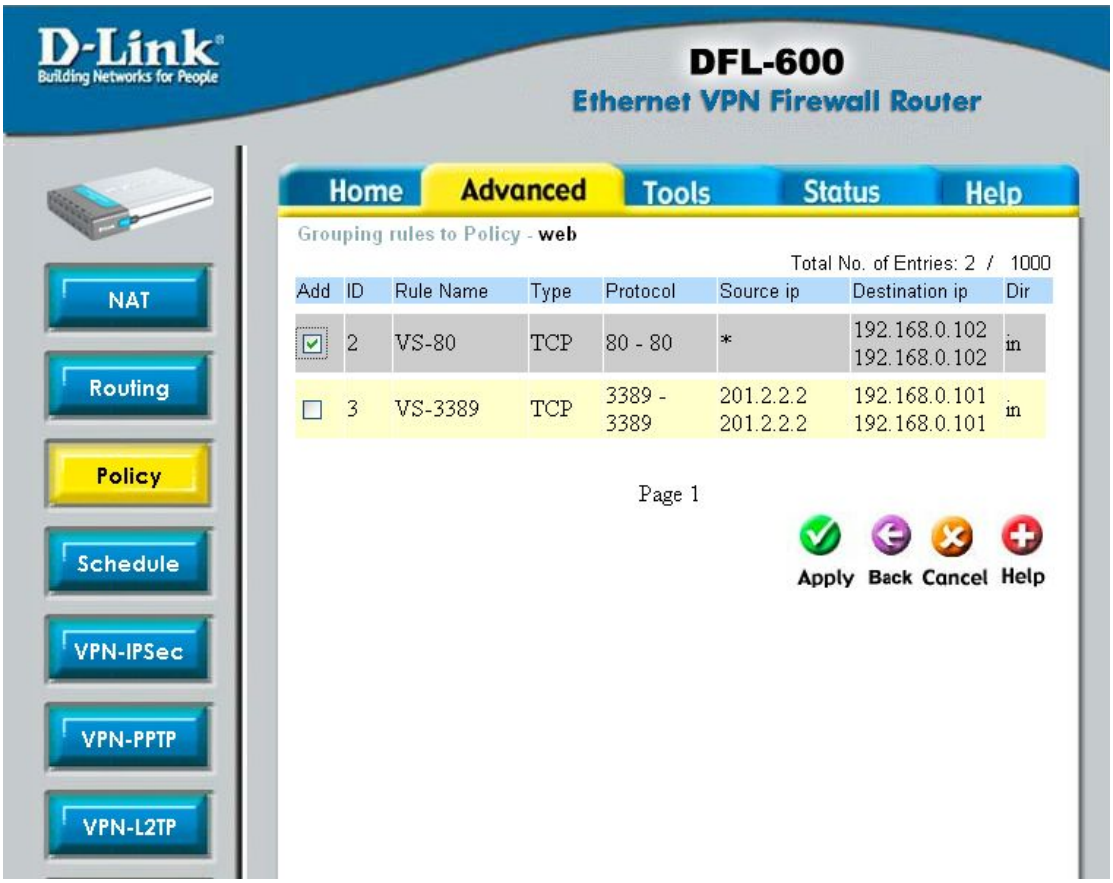


5. Configure Policies. Add two policies as below:

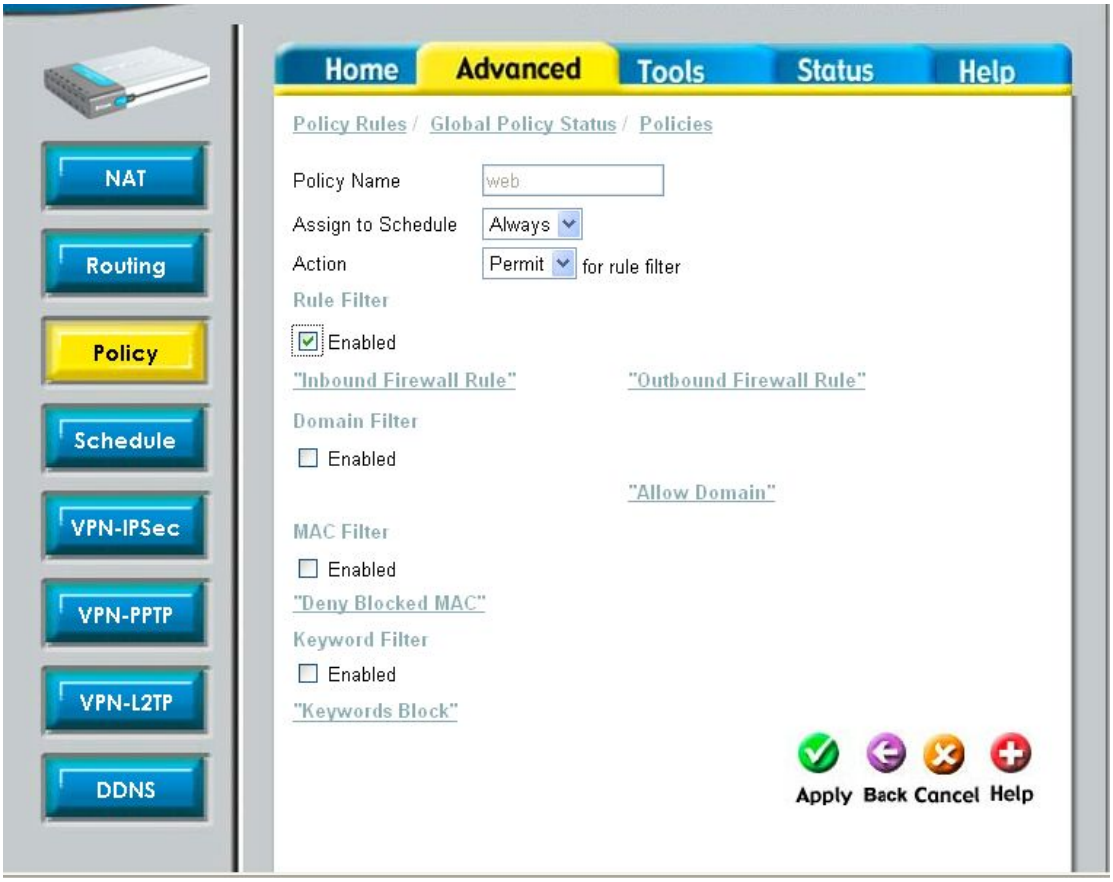
5-1. Edit “web” policy.



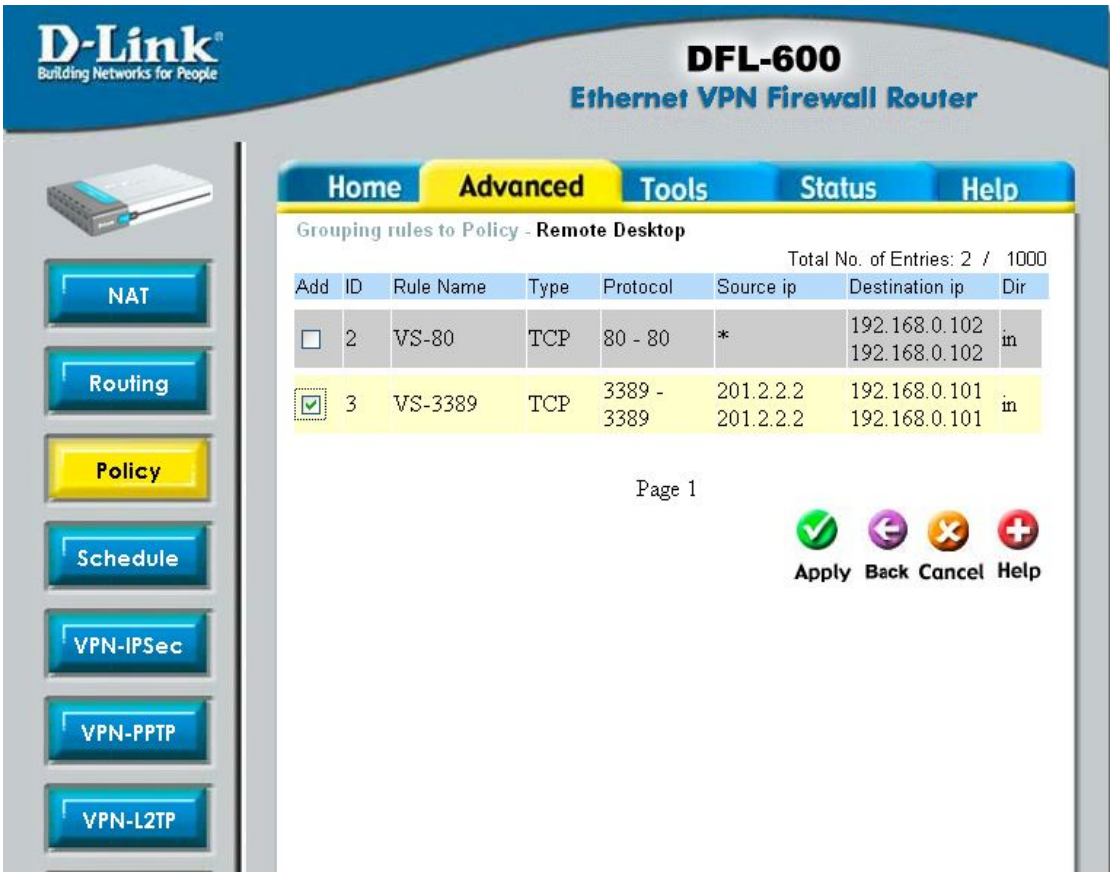
Go to “Inbound Firewall Rule” to choose rules.



Enable “Inbound Firewall Rule”.



5-2. Edit Remote Desktop policy. Go to “Inbound Firewall Rule” to choose rules.



Enable “Inbound Firewall Rule”.

6. You should see these two policies are enabled:

~ End of Document ~