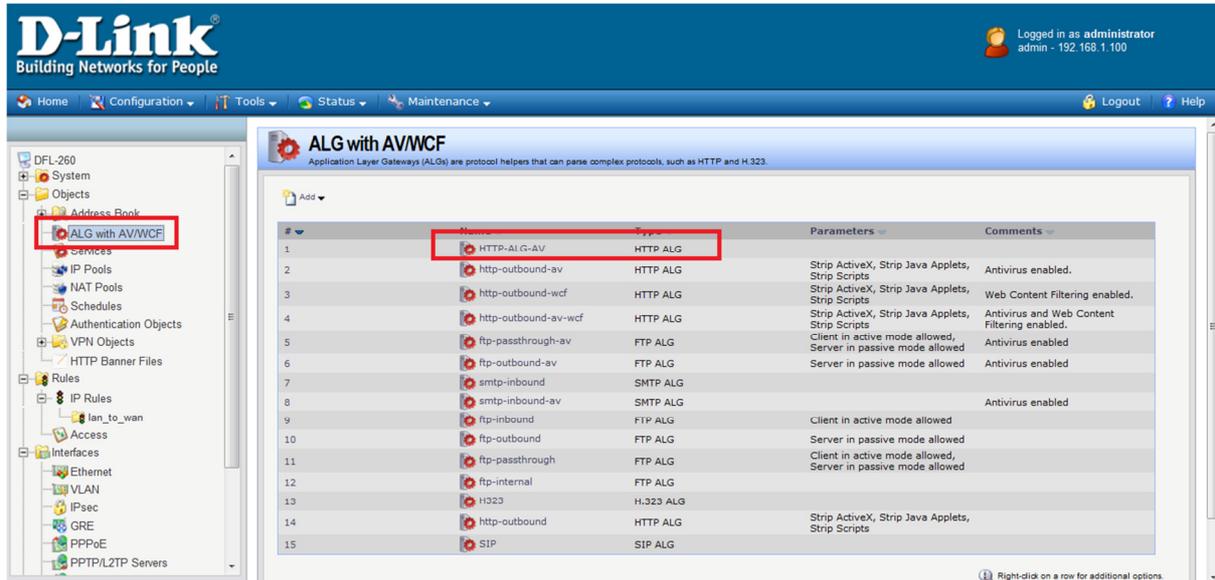


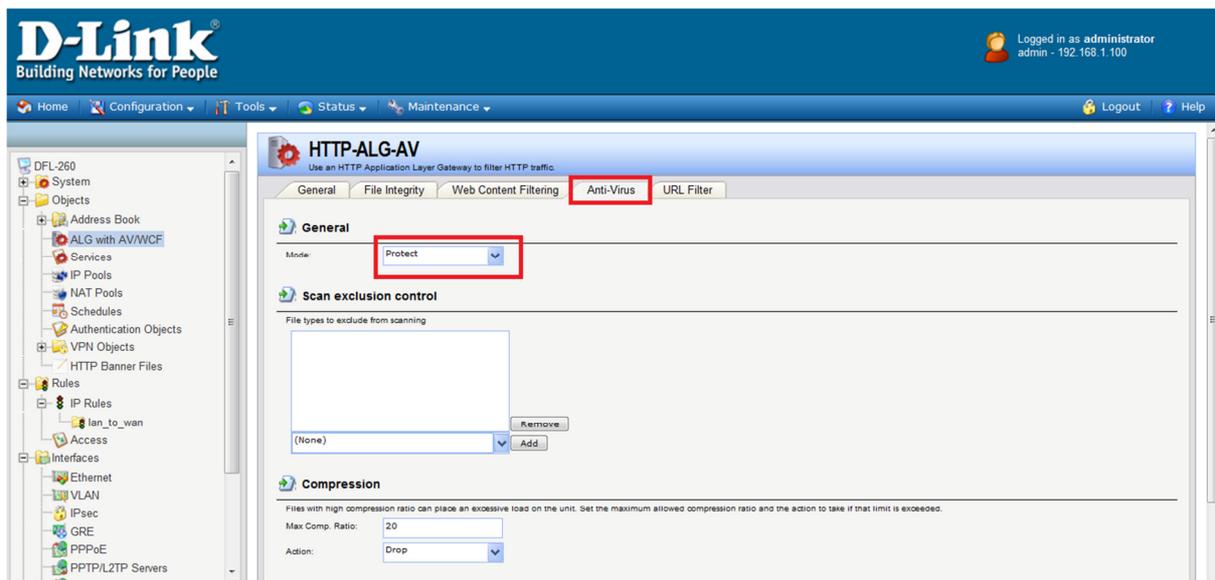
## How to Enable Antivirus Protection.

**Step 1.** Log into the Firewall by opening Internet Explorer and typing the LAN address of the Firewall. The default address is <https://192.168.1.1>. Enter Username and Password which you specified during the initial setup of the Firewall.

**Step 2.** In the menu on the left side of the screen select Objects > ALG with AV/VCF. Under Name select **"HTTP-ALG-AV"**.



**Step 3.** Click on the Antivirus tab and make sure the Mode has been set to **"Protect"** and the Action as **"Drop"**. Click on **"OK"**



**Step 4.** Click on Objects > Services. Select TCP-services, under the parameters use the below:

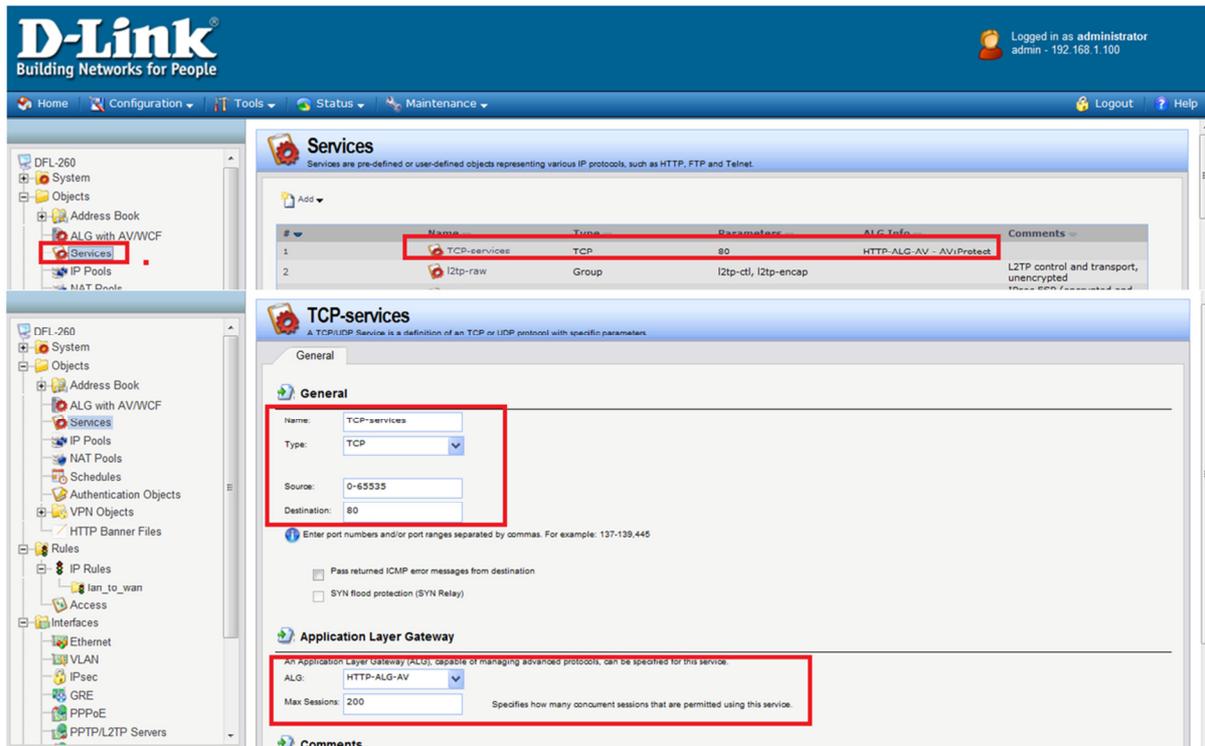
Type: TCP

Source: 0-65535

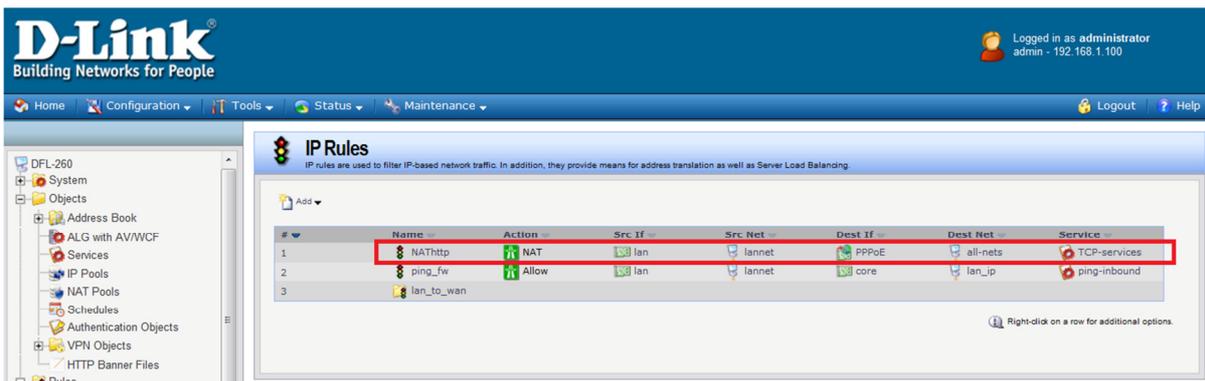
Destination: 80

ALG: select or the name that you gave to the AWL with AV/WCF object in Step 2 (in our example it is **"HTTP-ALG-AV"**).

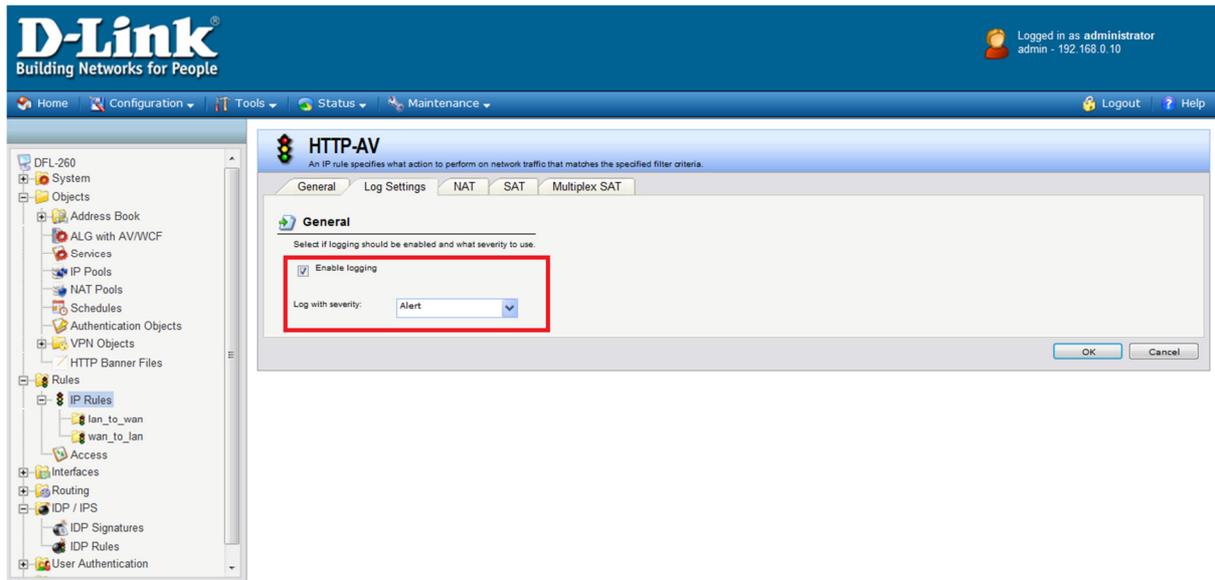
Click on **"OK"**.



**Step 5.** Click on Access Rules > IP Rules >. Add a new rule named NAThttp. Set the Action as **"NAT"**, Service as **"HTTP-ALG-AV"**, Source interface as lan, Network as lan-net. Set the Destination Interface as wan (if using a dynamic or static IP), or for ADSL select PPPoE (or the name of the PPPoE connection).



**Step 6.** Click on **“Log Settings”** tab at the top and make sure enable logging is enabled. Once done Click on **“OK”**.



**Step 7.** Save the new configuration. In the top menu bar click on Configuration and select **“Save and Activate”**.

Click on **“OK”** to confirm the new settings activation, Wait 15 seconds for the Firewall to apply the new settings.

### How to test if your antivirus protection is working.

You can test to see if the rules are working by going to [www.google.com.au](http://www.google.com.au) and searching for **“download viruses eicar”**. The first link should be [www.eicar.org](http://www.eicar.org)

Click on the link in the search results ([www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)). Your Internet browser will try to open the site which has a virus. Do not worry about getting infected because the virus is inside a zip file (compressed). Even if your antivirus protection is not working, you will not get infected unless you open the zip file and run the application (executable) inside it.



Next check under the Status > Anti-Virus Log, to see that the Anti-Virus is working.

The screenshot shows the D-Link web interface for a DFL-260 device. The user is logged in as administrator. The main content area is titled "Anti-Virus Log" and contains a search interface and a table of log entries. The search interface includes fields for Time, Source, Destination, Interface, IP Address, Port, Event, Action, Severity, and Category, along with a Free Text field and Search/Reset buttons. The table below shows internal logging for the Anti-Virus system.

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2011-02-21 06:07:24	Warning	ANTIVIRUS 5800001		TCP	lan core	192.168.1.100 188.40.238.250	49893 80	virus_found block_data
filename="eicar.com" virusname="EICAR-Test-File" virussig="EICAR-Test-File" advisoryid="AV1" algmod=http algsesid=42 origsent=1378 termsent=620 Advisory link								
2011-02-21 06:07:14	Warning	ANTIVIRUS 5800001		TCP	lan core	192.168.1.100 188.40.238.250	49891 80	virus_found block_data
filename="eicar_com.zip" virusname="EICAR-Test-File" virussig="EICAR-Test-File" advisoryid="AV1" algmod=http algsesid=41 origsent=717 termsent=84 Advisory link								