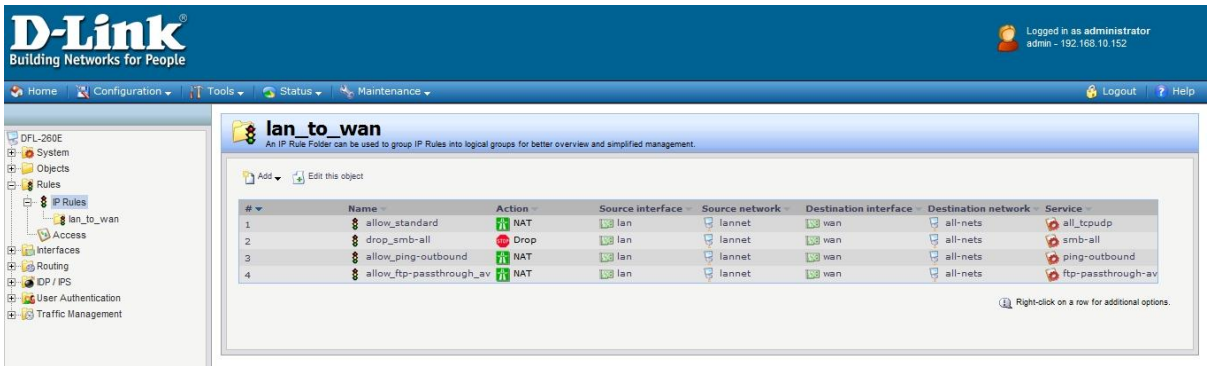
How to Enable Antivirus Protection and WCF
DFL-260/260E/860/860E/1660/2560

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 (260E/860E use https://192.168.10.1)
Enter Username and Password which you specified during the initial setup of the Firewall.

Step 2. Add IP rule; In the menu on the left side of the screen select IP rules > lan_to_wan.
By default the unit already has a rule to NAT traffic from the LAN to the WAN, leave this rule as it is.

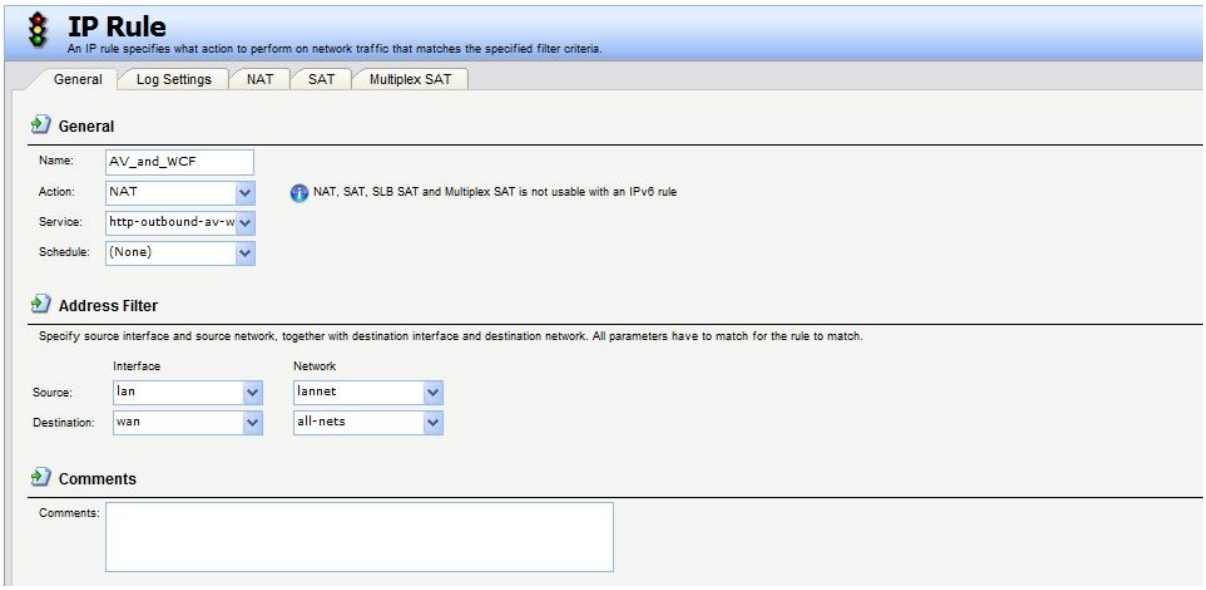


Click on “Add” then “IP Rule”.

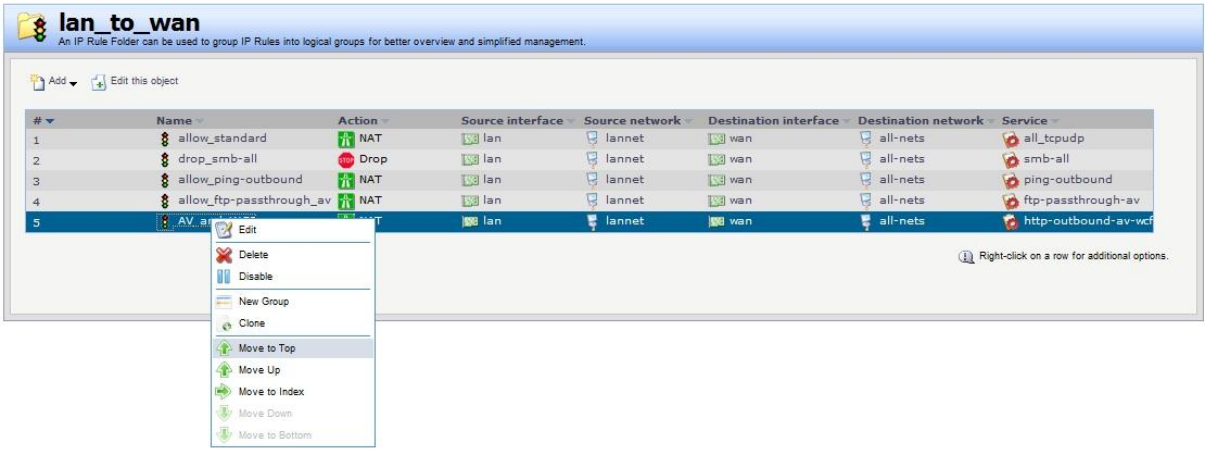
Under IP rule, Enter in a name for the rule, in our example, we called it “AV_and_WCF”
Set Action as “NAT”, Service as “http-outbound-av-wcf”.

Address filter

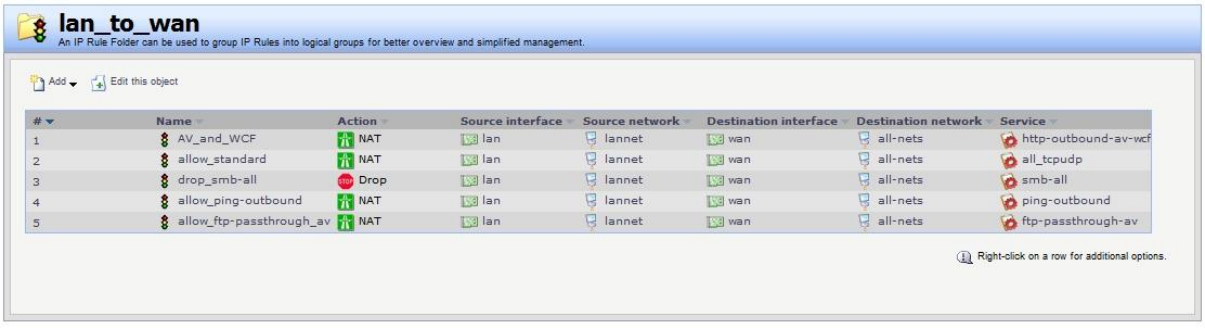
Source Interface: LAN, Network: lannet
Destination Interface: wan, Network: all-nets
Once done click “OK”



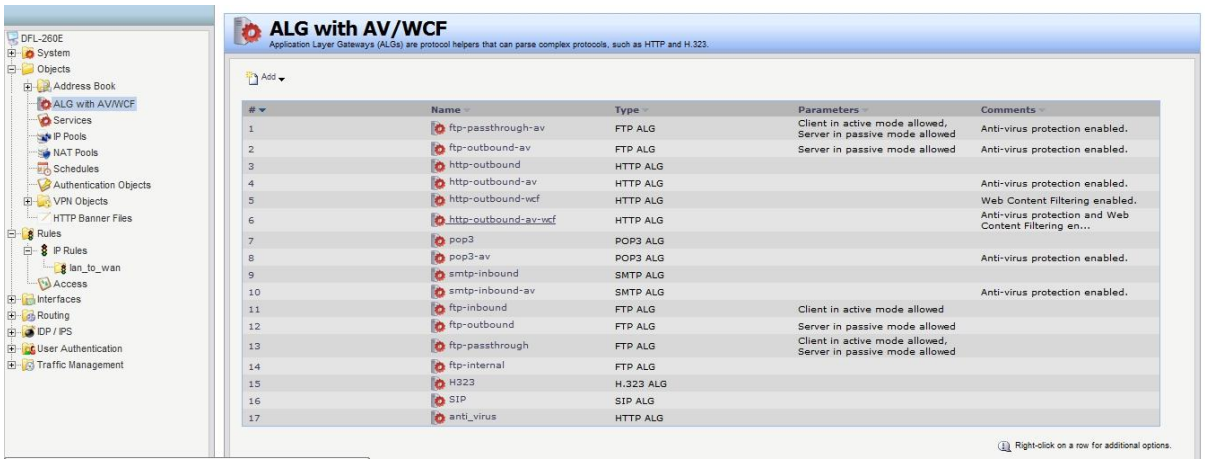
Right click on the rule and click “move to top”



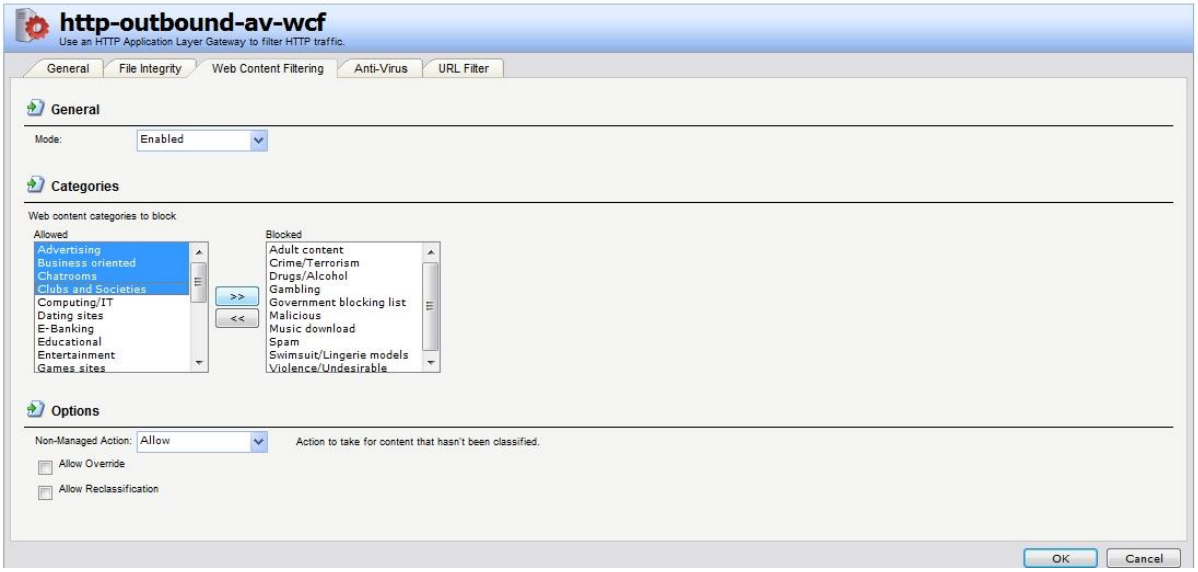
It should look something like the below image.



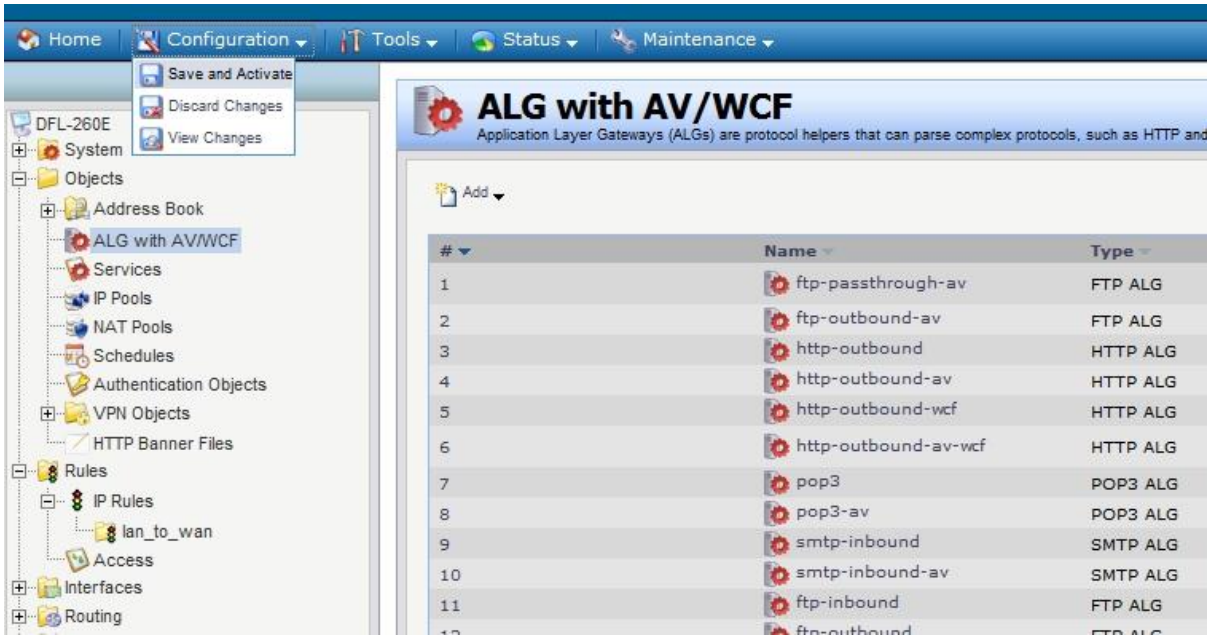
Step 3. Setup AV/WCF: On the left click on Objects > ALG with AV/WCF, next "select http-outound-av-wcf".



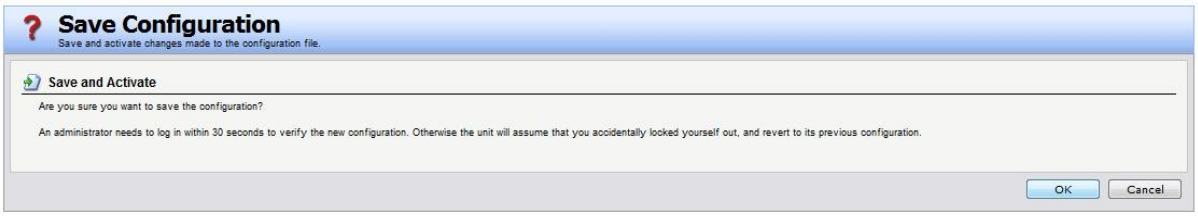
Anti-Virus is automatically enable and WCF will already have Categories selected, however if you would like to add more Categories to the blocked list, select this (as seen below) and then click the right arrow to move them to blocked. Then click "OK".



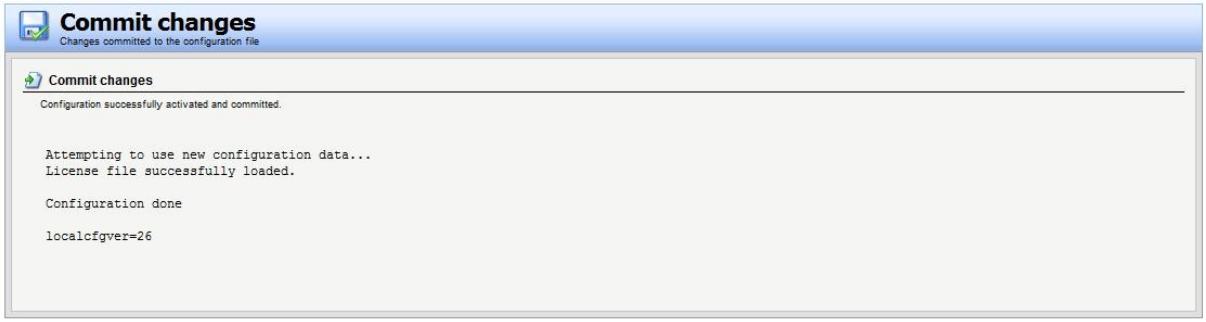
Step 4. Save the settings: Click Configuration > Save and Activate.



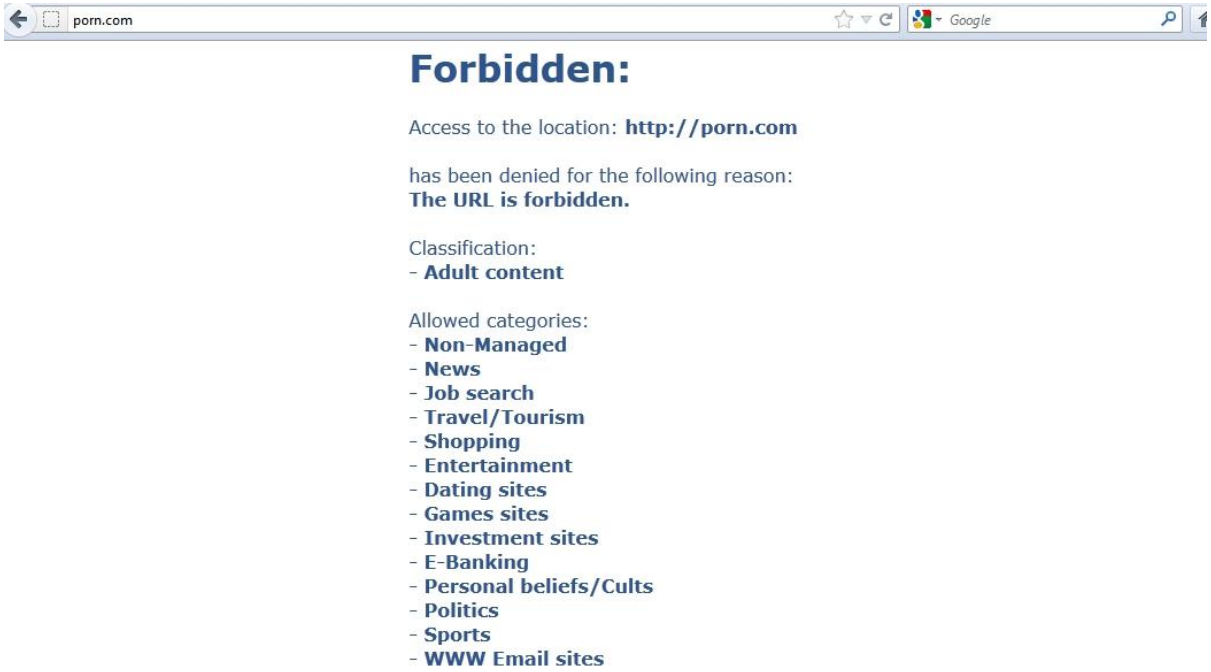
Then “OK”



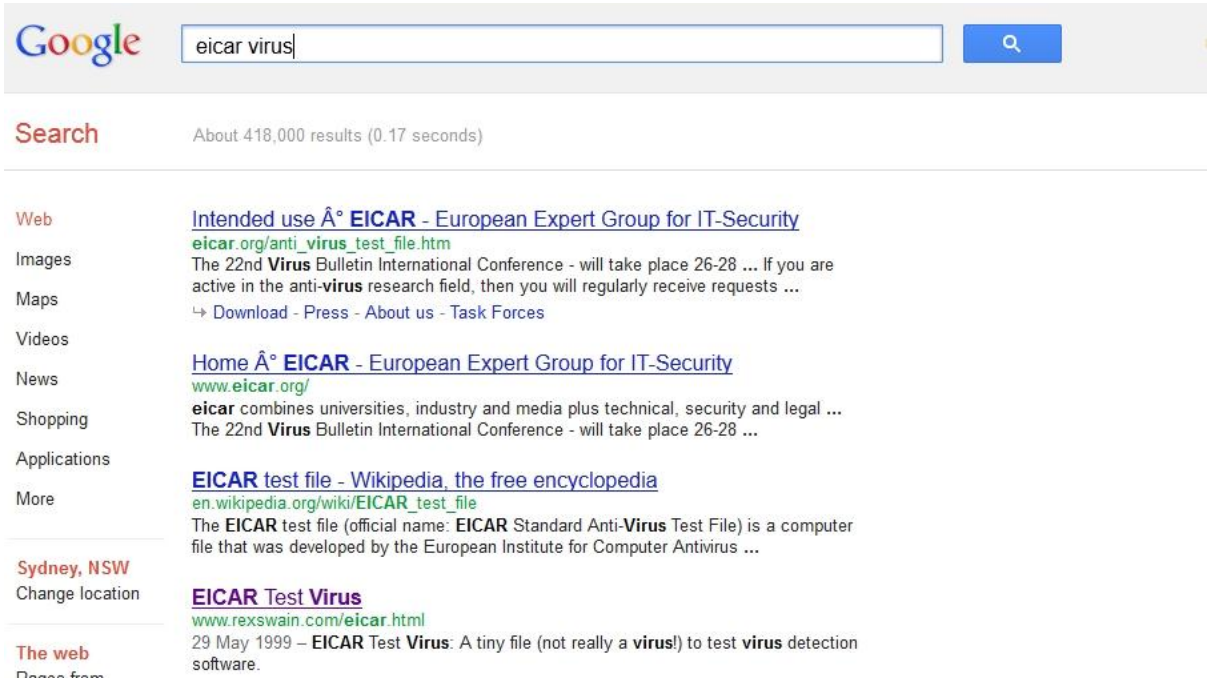
Once saved you should see the below screen.



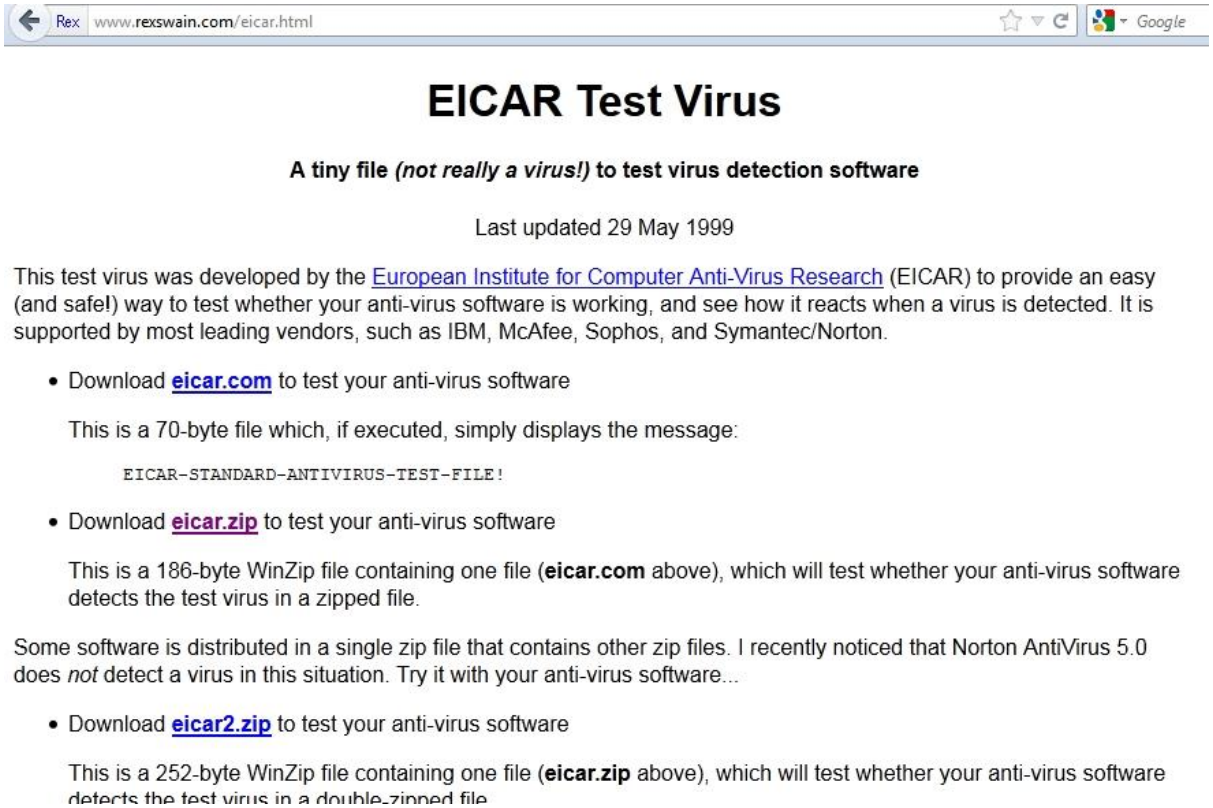
Step 5. Confirm WCF / AV is working; If you now access a site that would have been in the blocked Categories (E.G. Adult Content) it should come up with a message saying "Forbidden" as seen below.



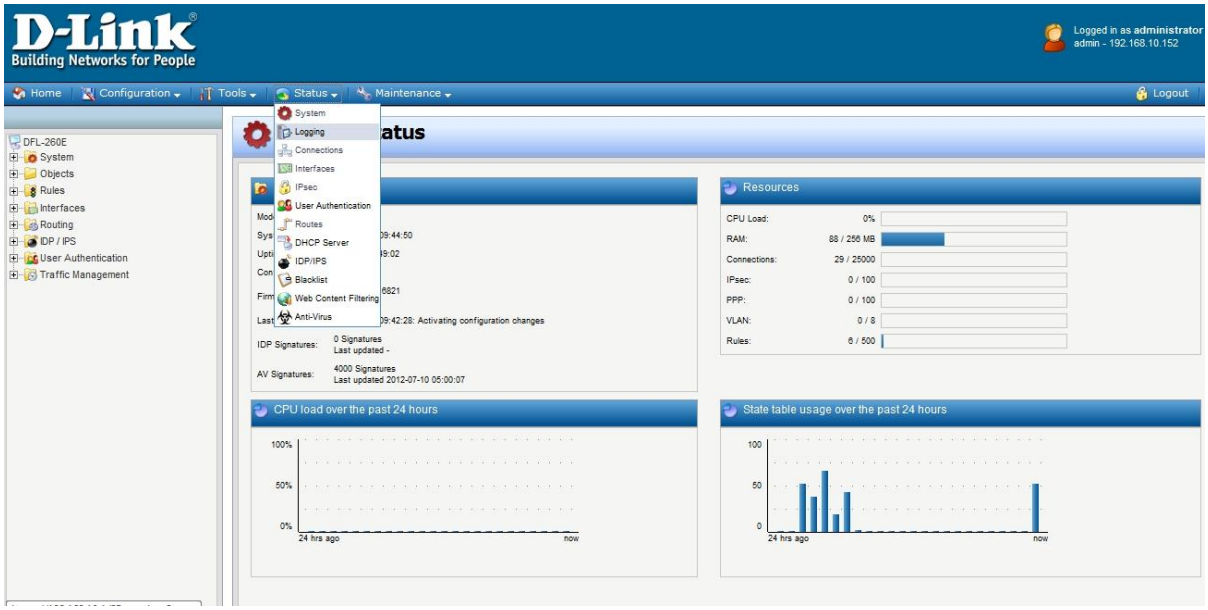
For a Virus test there is a test file called "Eicar" if you search for this on the Internet it should come up as below. Click on the link called titled "EICAR Test Virus"



Once at the site, download the eicar.zip file (save this to your computer, not open file).

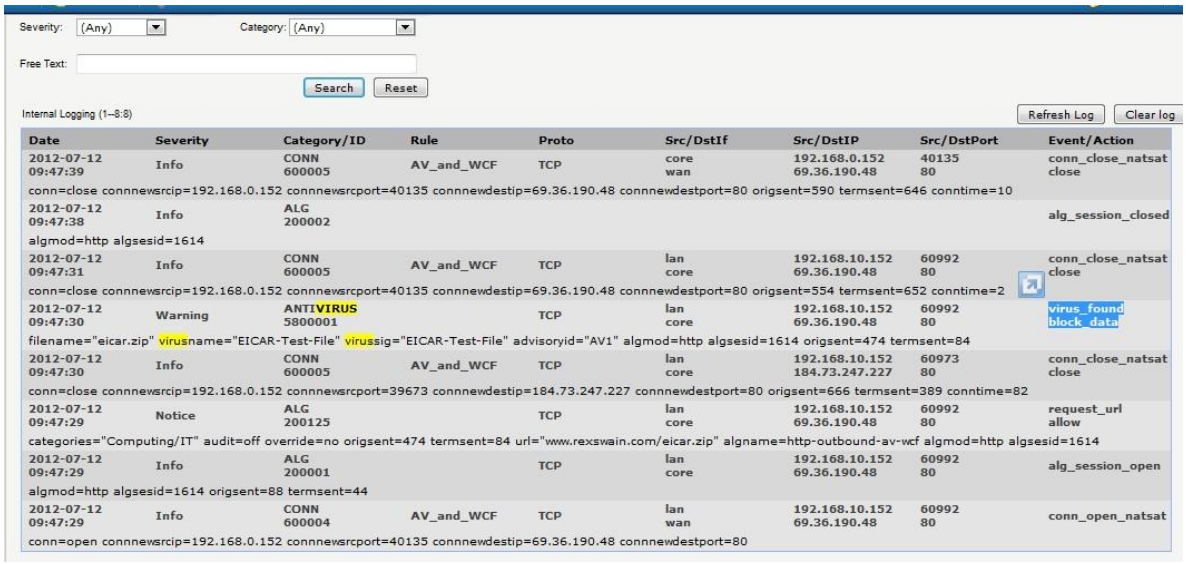


Next on the DFL config page click on Status > Logging



Under the log search for “Virus” you should be able to see something like the below.

On the right (Event/Action) it should say virus_found_block_data



The Eicar.zip file would have downloaded to the computer, however inside the eicar.zip file there is normally another file called “eicar.com”. This would have been removed (By the DFL).

If you disable AV on the DFL and download the same file and then extract the zip file you should see eicar.com

END OF DOCUMENT.