



## 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.

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	allow_standard	NAT	lan	lannet	wan	all-nets	all_tcpudp
2	drop_smb-all	Drop	lan	lannet	wan	all-nets	smb-all
3	allow_ping-outbound	NAT	lan	lannet	wan	all-nets	ping-outbound
4	allow_ftp-passthrough_av	NAT	lan	lannet	wan	all-nets	ftp-passthrough-av

Click on “Add” then “IP Rule”.

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	allow_standard	NAT	lan	lannet	wan	all-nets	all_tcpudp
2	drop_smb-all	Drop	lan	lannet	wan	all-nets	smb-all
3	allow_ping-outbound	NAT	lan	lannet	wan	all-nets	ping-outbound
4	allow_ftp-passthrough_av	NAT	lan	lannet	wan	all-nets	ftp-passthrough-av

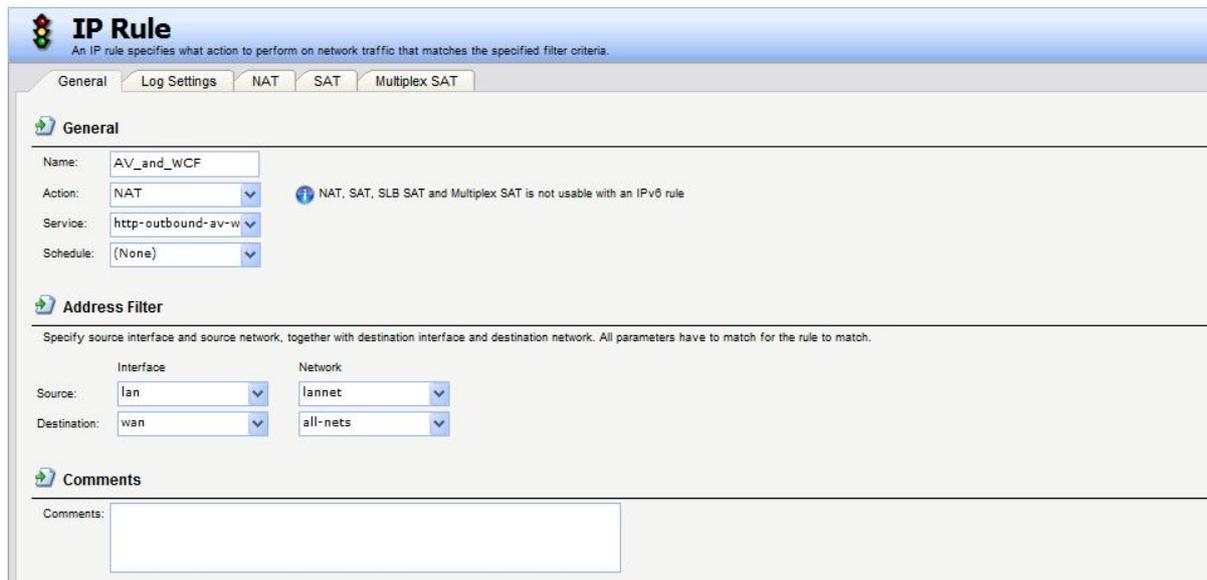
Under IP rule, Enter in a name for the rule, in our example, we called it “AV\_and\_WCF”  
 Set Action as “NAT”, Service as “http-outbound-av-wcf”.

**Address filter**

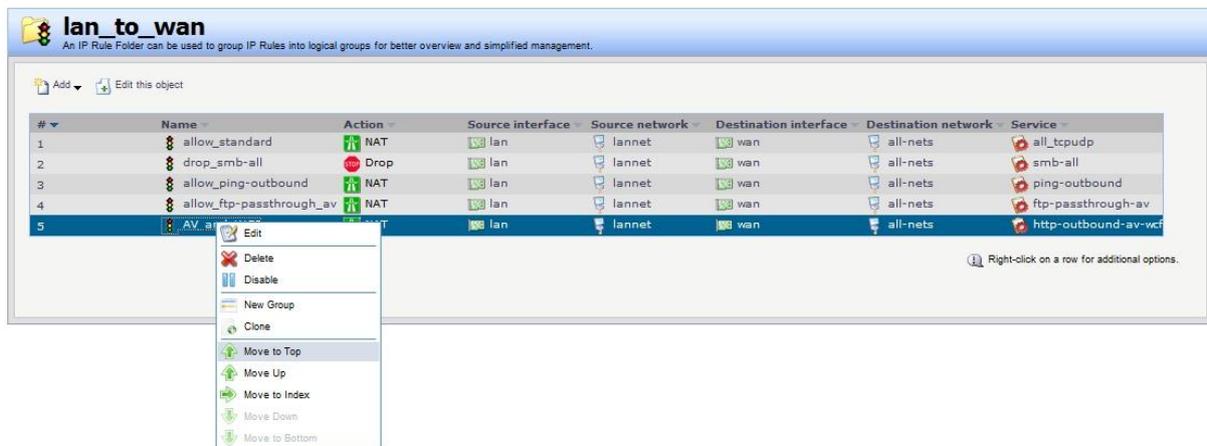
Source Interface: LAN, Network: lannet

Destination Interface: wan, Network: all-nets

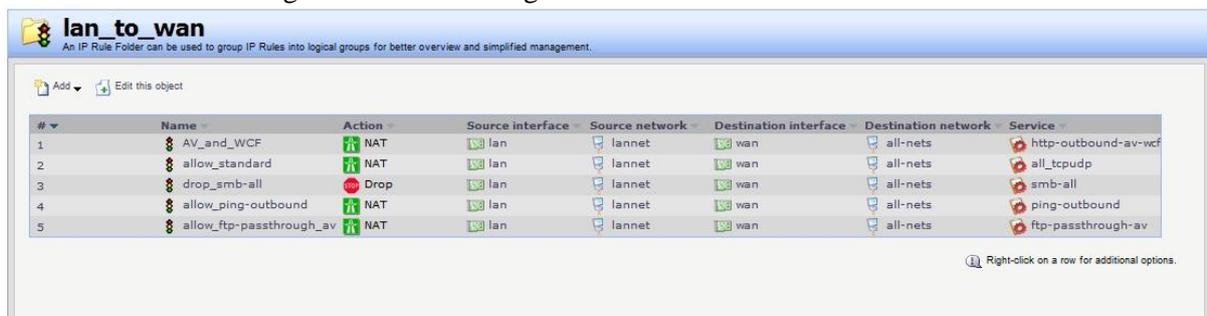
Once done click “OK”



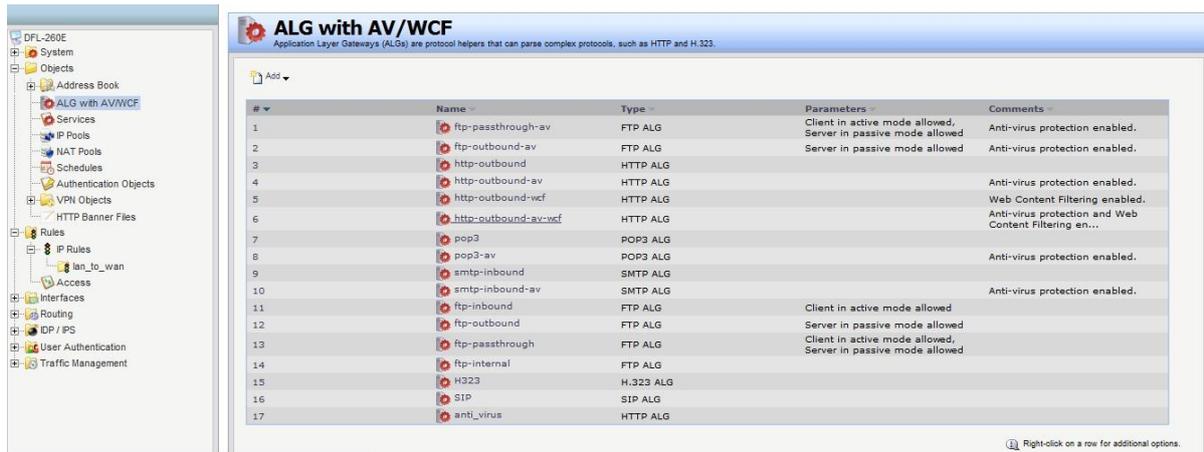
Right click on the rule and click “move to top”



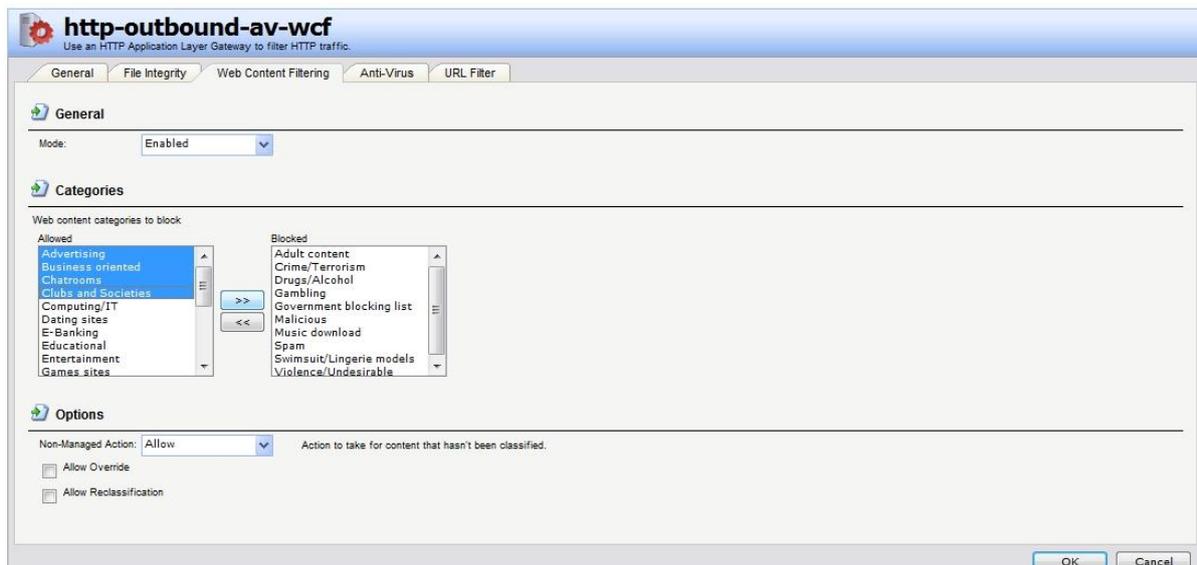
It should look something like the below image.



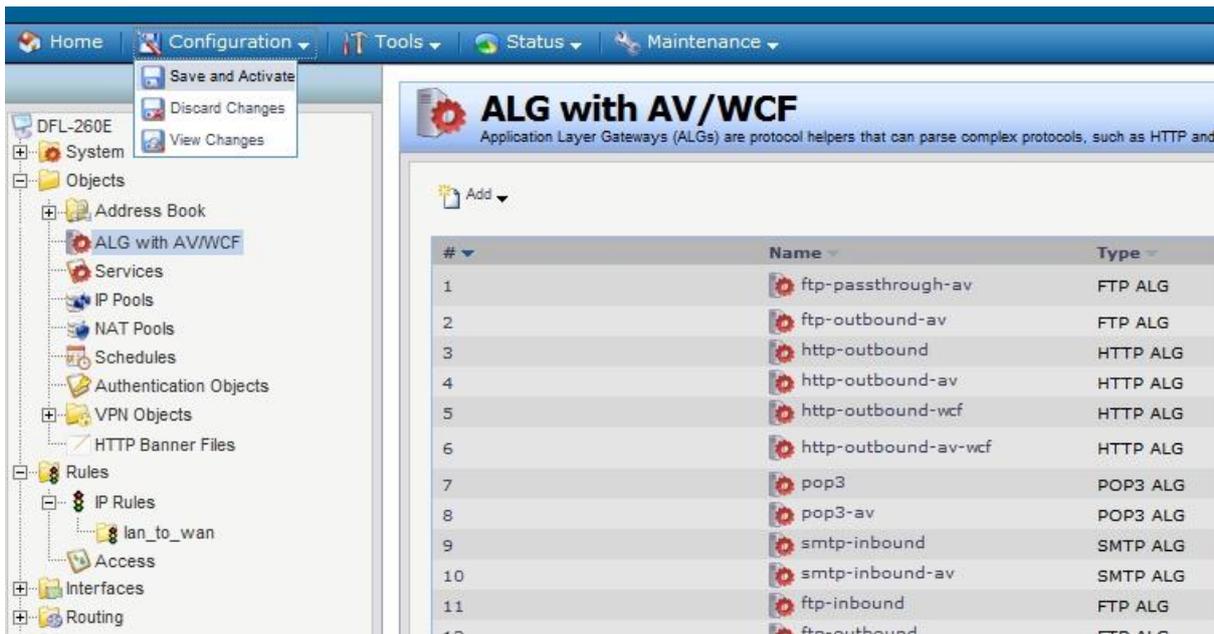
**Step 3. Setup AV/WCF:** On the left click on Objects > ALG with AV/WCF, next “select http-outbound-av-wcf”.



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”.



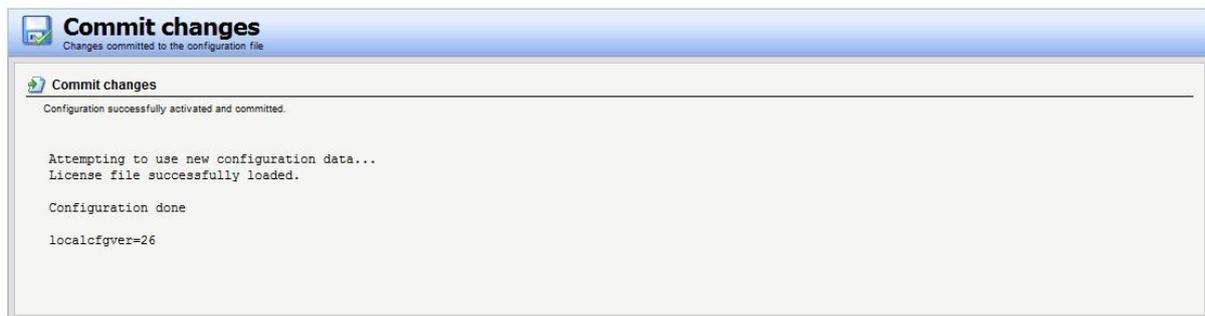
**Step 4. Save the settings:** Click Configuration > Save and Activate.



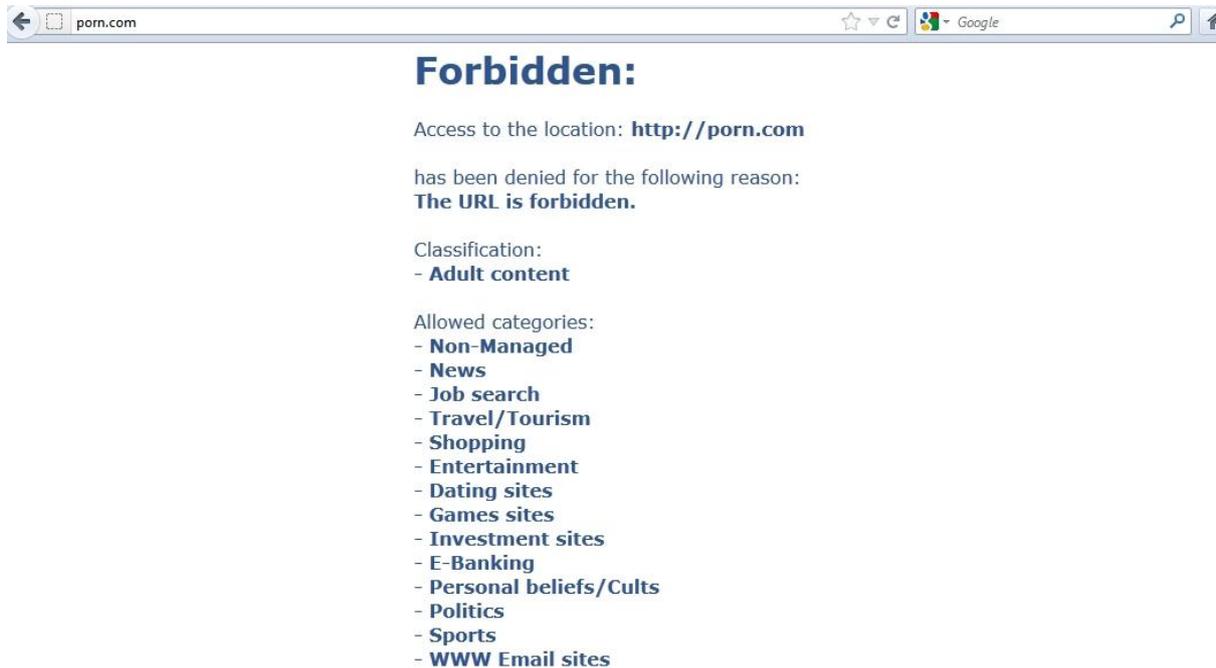
Then “OK”



Once saved you should see the below screen.

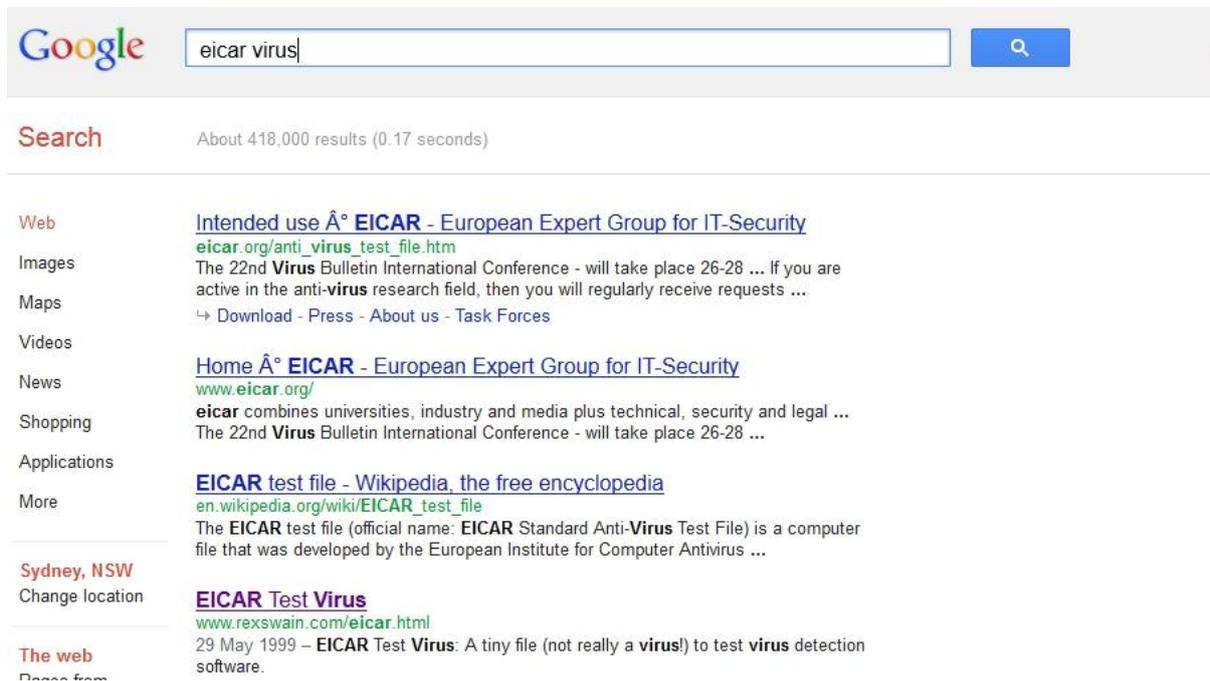


**Step 5. Confirm WCF / AV is working;** If you now access a site that would have been in the blocked Categories (E.G. Adult Content) it should come up with a message saying “Forbidden” as seen below.



The screenshot shows a web browser window with the address bar containing 'porn.com'. The main content area displays a 'Forbidden:' error message. The text reads: 'Access to the location: <http://porn.com> has been denied for the following reason: **The URL is forbidden.**' Below this, it lists the classification as '- **Adult content**' and provides a list of allowed categories: '- **Non-Managed**', '- **News**', '- **Job search**', '- **Travel/Tourism**', '- **Shopping**', '- **Entertainment**', '- **Dating sites**', '- **Games sites**', '- **Investment sites**', '- **E-Banking**', '- **Personal beliefs/Cults**', '- **Politics**', '- **Sports**', and '- **WWW Email sites**'.

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”



The screenshot shows a Google search page with the search query 'eicar virus' entered in the search bar. The search results show approximately 418,000 results in 0.17 seconds. The results are categorized by type: Web, Images, Maps, Videos, News, Shopping, Applications, and More. The top result is a web page titled 'Intended use Å° EICAR - European Expert Group for IT-Security' with the URL 'eicar.org/anti\_virus\_test\_file.htm'. The second result is a news article titled 'Home Å° EICAR - European Expert Group for IT-Security' with the URL 'www.eicar.org/'. The third result is a Wikipedia entry titled 'EICAR test file - Wikipedia, the free encyclopedia' with the URL 'en.wikipedia.org/wiki/EICAR\_test\_file'. The fourth result is a page titled 'EICAR Test Virus' with the URL 'www.rexswain.com/eicar.html' and a date of 29 May 1999. The page also shows a location of 'Sydney, NSW' and a 'Change location' link.

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



## EICAR Test Virus

A tiny file (*not really a virus!*) to test virus detection software

Last updated 29 May 1999

This test virus was developed by the [European Institute for Computer Anti-Virus Research](#) (EICAR) to provide an easy (and safe!) way to test whether your anti-virus software is working, and see how it reacts when a virus is detected. It is supported by most leading vendors, such as IBM, McAfee, Sophos, and Symantec/Norton.

- Download [eicar.com](#) to test your anti-virus software

This is a 70-byte file which, if executed, simply displays the message:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

- Download [eicar.zip](#) to test your anti-virus software

This is a 186-byte WinZip file containing one file ([eicar.com](#) above), which will test whether your anti-virus software detects the test virus in a zipped file.

Some software is distributed in a single zip file that contains other zip files. I recently noticed that Norton AntiVirus 5.0 does *not* detect a virus in this situation. Try it with your anti-virus software...

- Download [eicar2.zip](#) to test your anti-virus software

This is a 252-byte WinZip file containing one file ([eicar.zip](#) above), which will test whether your anti-virus software detects the test virus in a double-zipped file

Next on the DFL config page click on Status > Logging

The screenshot shows the D-Link web management interface. The top navigation bar includes Home, Configuration, Tools, Status, and Maintenance. The main content area is titled 'Status' and contains several sections:

- System:** A tree view on the left shows the configuration hierarchy, including System, Objects, Rules, Interfaces, Routing, IDP / IPS, User Authentication, and Traffic Management.
- Logging:** A section showing system logs with columns for Mod, Sys, Upt, Con, Firm, and Last. The 'Anti-Virus' entry is highlighted, showing '0 Signatures' and 'Last updated -'.
- Resources:** A section displaying system resources with progress bars and values: CPU Load (0%), RAM (88 / 256 MB), Connections (29 / 25000), IPsec (0 / 100), PPP (0 / 100), VLAN (0 / 8), and Rules (6 / 500).
- CPU load over the past 24 hours:** A line graph showing CPU usage over time, with a peak around 50%.
- State table usage over the past 24 hours:** A bar chart showing state table usage over time, with a peak around 50%.

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

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2012-07-12 09:47:39	Info	CONN 600005	AV_and_WCF	TCP	core wan	192.168.0.152 69.36.190.48	40135 80	conn_close_natsat close
conn=close connnewsrrip=192.168.0.152 connnewsrport=40135 connnewdestip=69.36.190.48 connnewdestport=80 origsent=590 termsent=646 conntime=10								
2012-07-12 09:47:38	Info	ALG 200002						alg_session_closed
algmod=http algsesid=1614								
2012-07-12 09:47:31	Info	CONN 600005	AV_and_WCF	TCP	lan core	192.168.10.152 69.36.190.48	60992 80	conn_close_natsat close
conn=close connnewsrrip=192.168.0.152 connnewsrport=40135 connnewdestip=69.36.190.48 connnewdestport=80 origsent=554 termsent=652 conntime=2								
2012-07-12 09:47:30	Warning	ANTIVIRUS 5800001		TCP	lan core	192.168.10.152 69.36.190.48	60992 80	virus_found_block_data
filename="eicar.zip" virusname="EICAR-Test-File" virussig="EICAR-Test-File" advisoryid="AV1" algmod=http algsesid=1614 origsent=474 termsent=84								
2012-07-12 09:47:30	Info	CONN 600005	AV_and_WCF	TCP	lan core	192.168.10.152 184.73.247.227	60973 80	conn_close_natsat close
conn=close connnewsrrip=192.168.0.152 connnewsrport=39673 connnewdestip=184.73.247.227 connnewdestport=80 origsent=666 termsent=389 conntime=82								
2012-07-12 09:47:29	Notice	ALG 200125		TCP	lan core	192.168.10.152 69.36.190.48	60992 80	request_url allow
categories="Computing/IT" audit=off override=no origsent=474 termsent=84 url="www.rexswain.com/eicar.zip" algname=http-outbound-av-wcf algmod=http algsesid=1614								
2012-07-12 09:47:29	Info	ALG 200001		TCP	lan core	192.168.10.152 69.36.190.48	60992 80	alg_session_open
algmod=http algsesid=1614 origsent=88 termsent=44								
2012-07-12 09:47:29	Info	CONN 600004	AV_and_WCF	TCP	lan wan	192.168.10.152 69.36.190.48	60992 80	conn_open_natsat
conn=open connnewsrrip=192.168.0.152 connnewsrport=40135 connnewdestip=69.36.190.48 connnewdestport=80								

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.