



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 <u>https://192.168.1.1</u> (260E/860E use <u>https://192.168.10.1</u>) 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

D-Link ilding Networks for People							실 Lo ad	gged in as administrator min - 192.168.10.152
Home 🛛 📉 Configuration 🚽 🗌	🎢 Tools 🗸 🔰 🕤 Status	🗸 🔰 🗞 Maintenance 🗸						👶 Logout 📔 👔 I
e io System → Jobjects → Stules → Stules		die can be deel to group in Roles into ogical dit this object	Action	Source interface -	Source network -	Destination interface	Destination network	Service
🕞 lan_to_wan	1	g allow_standard	NAT NAT	[] lan	🗟 lannet	💟 wan	🗟 all-nets	all_tcpudp
Access	2	g drop_smb-all	Drop	[] lan	🗟 lannet	wan	🖁 all-nets	Smb-all
Interfaces	3	allow_ping-outbound	TAT NAT	🔀 lan	😌 lannet	wan	🖁 all-nets	ping-outbound
6 Routing	4	8 allow_ftp-passthrough_av	TAT NAT	🔝 lan	💡 lannet	🔯 wan	🤤 all-nets	👩 ftp-passthrough-av
User Authentication							(1) Right	click on a row for additional options.

Click on "Add" then "IP Rule".

8 IP Rule							
# •	Name 👻	Action -	Source interface -	Source network -	Destination interface	Destination network	Service
1	8 allow_standard	TNAT NAT	[]an	😓 lannet	🔝 wan	😔 all-nets	all_tcpudp
2	g drop_smb-all	💿 Drop	🔯 lan	😡 lannet	wan 🛛	💡 all-nets	🍘 smb-all
3	8 allow_ping-outbound	MAT NAT	🔝 lan	😽 lannet	🔝 wan	🖁 all-nets	ping-outbound
4	allow_ftp-passthrough_av	INAT NAT	🔝 lan	🖁 lannet	wan	🖁 all-nets	ftp-passthrough-a

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"

8 IP	Rule rule specifies what acti	on to perf	orm on network traffic	that matches the specified t	filter criteria.			
Genera	Log Settings	NAT	SAT Mu	Itiplex SAT				
න Gener	ral							
Name:	AV_and_WCF							
Action:	NAT	*	🚯 NAT, SAT, SL	B SAT and Multiplex SAT is n	ot usable with an IPv6 rul	e		
Service:	http-outbound-av-	w 🗸						
Schedule:	(None)	*						
Specify so	urce interface and source	e network	, together with destina Network	ation interface and destination	n network. All parameters	have to match for th	e rule to match.	
Source:	lan	~	lannet	~				
Destination:	wan	~	all-nets	~				
🛃 Comn	nents							
Comments:								

Right click on the rule and click "move to top"

Add 🚽 🚮	Edit this object						
#*	Name 🛩	Action	Source interface	Source network	Destination interface	Destination network	Service
1	g allow_standard		[]an	😡 lannet	wan	🗟 all-nets	all_tcpudp
2	g drop_smb-all	Drop	🔯 lan	🗟 lannet	🛐 wan	🖁 all-nets	Smb-all
3	allow_ping-outbound	INAT	🔝 lan	🗟 lannet	🔝 wan	all-nets	ping-outbound
4	allow_ftp-passthrough_a	V 🙀 NAT	🔝 lan	🗟 lannet	🛐 wan	🗟 all-nets	oftp-passthrough-av
5	8 AV at 🕑 Edit	T	🎉 lan	💡 lannet	鰯 van	📮 all-nets	🐞 http-outbound-av-w
	Delete					(I) Ri	ght-click on a row for additional opt
	New Group Office	2					
	A Move to Top						
	Move Up Move to Index						
	Wove Down						
	Wove to Bottom						

It should look something like the below image.

# -	Name z	Action	Source interface -	Source network	Destination interface -	Destination network	Samira
1	& AV_and_WCF	NAT	[3] lan	lannet	wan	g all-nets	http-outbound-av-wd
2	allow_standard	INAT NAT	Ian Ian	😔 lannet	wan	all-nets	all_tcpudp
3	g drop_smb-all	Drop	[]an	🖯 lannet	🔝 wan	all-nets	smb-all
4	allow_ping-outbound	INAT NAT	[lan	🖁 lannet	🔯 wan	all-nets	ping-outbound
5	allow_ftp-passthrough_av	NAT	🔝 lan	😔 lannet	🔢 wan	all-nets	ftp-passthrough-av

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

tem					
ects	_ http://				
Address Book					
ALG with AV/WCF	# 🔻	Name =	Туре	Parameters *	Comments -
Services IP Pools	1	ttp-passthrough-av	FTP ALG	Client in active mode allowed, Server in passive mode allowed	Anti-virus protection enabled.
NAT Pools	2	tp-outbound-av	FTP ALG	Server in passive mode allowed	Anti-virus protection enabled.
Authentication Objects VPN Objects HTTP Banner Files Rules	3	ttp-outbound 🔯	HTTP ALG		
	4	b http-outbound-av	HTTP ALG		Anti-virus protection enabled.
	5	ttp-outbound-wcf	HTTP ALG		Web Content Filtering enabled.
	6	http-outbound-av-wcf	HTTP ALG		Anti-virus protection and Web Content Filtering en
	7	pop3	POP3 ALG		
Rules	8	opp3-av	POP3 ALG		Anti-virus protection enabled.
g lan_to_wan	9	o smtp-inbound	SMTP ALG		
CCESS	10	🐞 smtp-inbound-av	SMTP ALG		Anti-virus protection enabled.
aces	11	🄯 ftp-inbound	FTP ALG	Client in active mode allowed	
ing Ips	12	tp-outbound	FTP ALG	Server in passive mode allowed	
Authentication	13	tp-passthrough	FTP ALG	Client in active mode allowed, Server in passive mode allowed	
ic Management	14	tp-internal	FTP ALG		
	15	10 H323	H.323 ALG		
	16	to SIP	SIP ALG		
	17	📸 anti_virus	HTTP ALG		

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".

http-outbound-av-wcf Use an HTTP Application Layer Gateway to filter HTTP traffic.	
General File Integrity Web Content Filtering Anti-Virus URL Filter	
2 General	
Mode: Chabled	
2) Categories	
Web content categories to block Advertising Business oriented Chatroomic Chatroomic Computing Steles Computing Steles E-Banking Educational Entertainment Games sites Violence/Undesirable	
Non-Managed Action: Allow Action to take for content that hasn't been classified. Allow Override Allow Reclassification	
C C	OK Cancel

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



Then "OK"

Save Configuration Save and activate changes made to the configuration file.	
Save and Activate	
e you sure you want to save the configuration?.	
administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.	
	OK Cancel
administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.	ок С:

Once saved you should see the below screen.

Commit changes Changes committed to the configuration file
Commit changes
Configuration successfully activated and committed.
Attempting to use new configuration data
License file successfully loaded.
Configuration done
localcfgver=26

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"

Google	eicar virus Q
Search	About 418,000 results (0.17 seconds)
Web	Intended use ° EICAR - European Expert Group for IT-Security
Images	eicar.org/anti_virus_test_file.htm The 22nd Virus Bulletin International Conference - will take place 26-28 If you are
Maps	active in the anti- virus research field, then you will regularly receive requests
Videos	
News	Home ° EICAR - European Expert Group for IT-Security
Shopping	eicar combines universities, industry and media plus technical, security and legal The 22nd Virus Bulletin International Conference - will take place 26-28
Applications	Construction and Construction and an end of SEC 12 Database region control and an end of control an end of control an end of control and an end of control an end of control and an end of control
More	EICAR test file - Wikipedia, the free encyclopedia en.wikipedia.org/wiki/EICAR_test_file The EICAR test file (official name: EICAR Standard Anti-Virus Test File) is a computer
Sydney, NSW	file that was developed by the European Institute for Computer Antivirus
Change location	EICAR Test Virus
The web	www.rexswain.com/eicar.html 29 May 1999 – EICAR Test Virus: A tiny file (not really a virus!) to test virus detection software.

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

Rex www.rexswain.com/eicar.html



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 <u>European Institute for Computer Anti-Virus Research</u> (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 <u>eicar2.zip</u> 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-zinned file

Next on the DFL config page click on Status > Logging

🌯 Home 🛛 🔣 Configuration 🗸 🗌	🍸 Tools 🗸 👩 Status 🗸 🐁 Maintenance 🗸	😚 Logout
DFL-260E	System	
Objects	I contractors	Se Resources
i Interfaces i	Mod Super Authentication Syst Protes OPCP Server 9:44:50 Upt OPIPS Stackist 821 End September Server Visit 9:42:32 Signatures 9:42:32. Activating configuration changes IDP Signatures: Signatures Av Signatures: Last updated - Av Signatures: Last updated -	CPU Load: 0% RAM: 68 / 260 MB Connections: 28 / 2500 IPsec: 0 / 100 PPP: 0 / 100 VLAN: 0 / 8 Rules: 0 / 500
	CPU load over the past 24 hours	State table usage over the past 24 hours
	00%	50 2 Arbs ago rev

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

		Search	Reset					
ternal Logging (18:8	6)						(Refresh Log Clear
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	тср	core wan	192.168.0.152 69.36.190.48	40135 80	conn_close_natsa close
conn=close conr	newsrcip=192.168.	0.152 connnewsrcport=	40135 connnewdesti	p=69.36.190.48	connnewdestport=80 o	rigsent=590 termsent=	646 conntime=10	
2012-07-12	Info	ALG 200002						alg_session_close
algmod=http alg	gsesid=1614							
2012-07-12 09:47:31	Info	CONN 600005	AV_and_WCF	тср	lan core	192.168.10.152 69.36.190.48	60992 80	conn_close_nats
conn=close conr	newsrcip=192.168.	0.152 connnewsrcport=	40135 connnewdesti	p=69.36.190.48	connnewdestport=80 o	rigsent=554 termsent=	652 conntime=2	2
2012-07-12 09:47:30	Warning	ANTIVIRUS 5800001		тср	lan core	192.168.10.152 69.36.190.48	60992 80	virus_found block_data
ilename="eicar	.zip" <mark>virus</mark> name="E	ICAR-Test-File" virussi	g="EICAR-Test-File" a	advisoryid="AV1"	' algmod=http algsesid	=1614 origsent=474 te	rmsent=84	
2012-07-12 09:47:30	Info	CONN 600005	AV_and_WCF	тср	lan core	192.168.10.152 184.73.247.227	60973 80	conn_close_nats close
onn=close conr	newsrcip=192.168.	0.152 connnewsrcport=	39673 connnewdesti	p=184.73.247.2	27 connnewdestport=80) origsent=666 termsen	t=389 conntime=8	2
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
ategories="Cor	nputing/IT" audit=	off override=no origser	nt=474 termsent=84	url="www.rexswa	in.com/eicar.zip" algna	me=http-outbound-av-v	wcf algmod=http al	gsesid=1614
2012-07-12 09:47:29	Info	ALG 200001		тср	lan core	192.168.10.152 69.36.190.48	60992 80	alg_session_oper
algmod=http alg	gsesid=1614 origse	nt=88 termsent=44						
2012-07-12	Info	CONN	AV_and_WCF	тср	lan	192.168.10.152	60992	conn_open_natsa

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.