DFL-210/DFL-260/260E/800/860/860E/1660/2560 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".

D-Link Building Networks for People					Logged in as administrato admin - 192.168.1.100	r
😚 Home 🔣 Configuration 🗸 🕴 👬 To	ools 🚽 📔 🕤 Status 🗸 🕴	👆 Maintenance 🗸			😚 Logout	👔 Help
DFL-260	ALG with A	WWCF steways (ALGs) are protocol helpers that can parse com	plex protocols, such as HTTP and i	4.323.		Í
E-Government	Add 🛩					
Address Book						
ALG with AV/WCF	# 🐨			Parameters 🔝	Comments 🤝	
Services	1	tTTP-ALG-AV	HTTP ALG			
- 1 Pools	2	ttp-outbound-av	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	Antivirus enabled.	
	3	http-outbound-wcf	HTTP ALG	Strip ActiveX, Strip Java Applets,	Web Content Filtering enabled.	
		http://www.cf	HTTP ALC	Strip Scripts Strip ActiveX, Strip Java Applets,	Antivirus and Web Content	
Authentication Objects	4	intep-outbound-av-wei	HTTP ALG	Strip Scripts	Filtering enabled.	
	5	tp-passthrough-av	FTP ALG	Server in passive mode allowed	Antivirus enabled	
HTTP Banner Files	6	🔯 ftp-outbound-av	FTP ALG	Server in passive mode allowed	Antivirus enabled	
E- S Rules	7	to smtp-inbound	SMTP ALG			
E- \$ IP Rules	8	to smtp-inbound-av	SMTP ALG		Antivirus enabled	
an_to_wan	9	tp-inbound	FTP ALG	Client in active mode allowed		
- O Access	10	tp-outbound	FTP ALG	Server in passive mode allowed		
E Interfaces	11	tp-passthrough	FTP ALG	Client in active mode allowed,		
Ethernet	12	tp-internal	FTP ALG	Server in passive mode anowed		
- LIQ VLAN	13	H323	H.323 ALG			
	14	http-outbound	HTTPALG	Strip ActiveX, Strip Java Applets,		
GKE				Strip Scripts		
	15	SIP SIP	SIP ALG			
PPTP/L2TP Servers					(1) Right-click on a row for additional optic	ns. 👻

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"**

D-Link Building Networks for People	Logged in : admin - 19	as administrator 2.168.1.100	
😚 Home 📉 Configuration 🗸 🕴 👬 Too	ols 🗸 📔 💁 Status 🗸 🛛 💑 Maintenance 🗸	😚 Logout	👔 Help
DFL-260 Dejects Objects Objects Objects Objects Devices Pools NAT Pools Schedules Objects PRules Inowen Access Enternet VAN Psec GRE GRE PPPOE	With the Application Layer Gateway to filter HTTP traffic General File Integrity Web Content Filtering Anti-Virus Use an HTTP Application Layer Gateway to filter HTTP traffic Image: Protect Image: Protect Image: Protect<		
THIP/LZIP Servers			

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"**.

D-Link Building Networks for People					2	Logged in as administrat or admin - 192.168.1.100	ŗ
📀 Home 🛛 📉 Configuration 🗸 🛛 👬 Tools	🗸 🛛 🕤 Status 🗸 🛛 🔩 Mai	ntenance 🚽				👶 Logout	👔 Help
DFL-260	Services Services are pre-defined or use	er-defined objects representing va	rious IP protocols, such as HTTP, F	IP and Telnet.			E
ALG with AV/WCF	2 w	Name	Типе	Daramotore	ALC Info	Comments 🤝	
Services	1	G TCP-services	тср	80	HTTP-ALG-AV - AV:Protect		
IP Pools	2	12tp-raw	Group	l2tp-ctl, l2tp-encap		L2TP control and transport, unencrypted	
B: jo System B: jo Objects B: jo Address Book D: Pools D: Pools <	General Constant of the services Constant	In anges separated by commas. For renessages from destination rvit Relay) evray Cocapable of managing savando Specifies how m	example: 137-139,445 a protocolit, can be specified for fin any concurrent sessions that are pe	service.			

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).

D-Link Building Networks for Peop	® le							Sector 2 Log	ged in as administrator nin - 192.168.1.100
😚 Home 🛛 📉 Configuration 🗸	👔 Tools 🚽	o Status 🗸	🌯 Maintenance 🗸						👶 Logout 🛛 👔 Help
DFL-260 System Dipolects		IP Rules	o filter IP-based network traff	ic. In addition, they pro	vide means for address trans	llation as well as Server Load	Balancing.		
Address Book		= -	Name 📼	Action	Src If 🛩	Src Net 📼	Dest If 🚽	Dest Net -	Service -
Services	1	1	8 NAThttp	T NAT	🔝 lan	🗟 lannet	PPPoE	🖁 all-nets	TCP-services
IP Pools	2	2	§ ping_fw	Allow	🔝 lan	😽 lannet	core	😽 lan_ip	ping-inbound
	3	3	🕞 lan_to_wan						
Schedules Authentication Objects VPN Objects HTTP Banner Files	E							(1) Right-	click on a row for additional options.

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

D-Link Building Networks for People		Logged in as administrator admin - 192.168.0.10
😵 Home 🔣 Configuration 🗸 📔 🎢 Too	ils 🗸 📔 🧟 Status 🗸 🛛 🔩 Maintenance 🗸	😚 Logout 🔰 🍞 Help
DFL-260 Dect-260 Dect-260 Dects Dects Dects Address Book Dects Dects	HTTP-AV An IP rule specifies what action to perform on network tailing that matches the specified filter oriteria. A IP rule specifies what action to perform on network tailing that matches the specified filter oriteria. Ceneral Second action of the specified filter oriteria. Evaluation of the specified filter oriteria. Second action of the specified filter oriteria. Second action of the specified filter oriteria. Second action of the specified filter oriteria.	OK Cancel
User Authentication		

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 and searching for "download viruses eicar". The first link should be www.eicar.org

Click on the link in the search results (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.

D-Link Building Networks for People								실 Logg admi	ed in as administrator n - 192.168.1.100	
😵 Home 🛛 💐 Configuration 🗸 🛛 👬 Too	ls 🚽 📔 🕤 Status 🖣	🗸 🛛 🗞 Mainter	nance 🚽						😚 Logout	👔 Help
DFL-260	Anti-Vi	us Log								
Dijects	Anti-Virus I	log								_
ALG with AV/WCF Genices IP Pools AlT Pools Genices Alt Pools Genices Authentication Objects Genices IP Rules Genices And Pools In Course	Time: From Source Interface: IP Address: Port: Event: Event: Any Free Text: Free Text:		To Destination Action: Category: (Any) Sear	ch Reset						
E Ethernet	Internal Logging (12	::2)							Refresh Log Clear le	og
-WUAN - 👸 IPsec	Date 2011-02-21 06:07:24	Severity	Category/ID ANTIVIRUS 5800001	Rule	TCP	Src/DstIf lan core	Src/DstIP 192.168.1.100 188.40.238.250	5rc/DstPort 49893 80	Event/Action virus_found block_data	
-₩ GRE -∰ PPPoE	filename="eicar. 2011-02-21 06:07:14	warning	ANTIVIRUS 5800001	ag="EICAR-Tes	TCP	/1 algmod=http algse: lan core	sid=42 origsent=1378 t 192.168.1.100 188.40.238.250	ermsent=620 Ac 49891 80	lvisory link virus_found block_data	
PPTP/L2TP Servers	filename="eicar	_com.zip" virusna	me="EICAR-Test-File" v	irussig="EICAR-	Test-File" advisoryid:	="AV1" algmod=http al	lgsesid=41 origsent=71	.7 termsent=84 /	Advisory link	