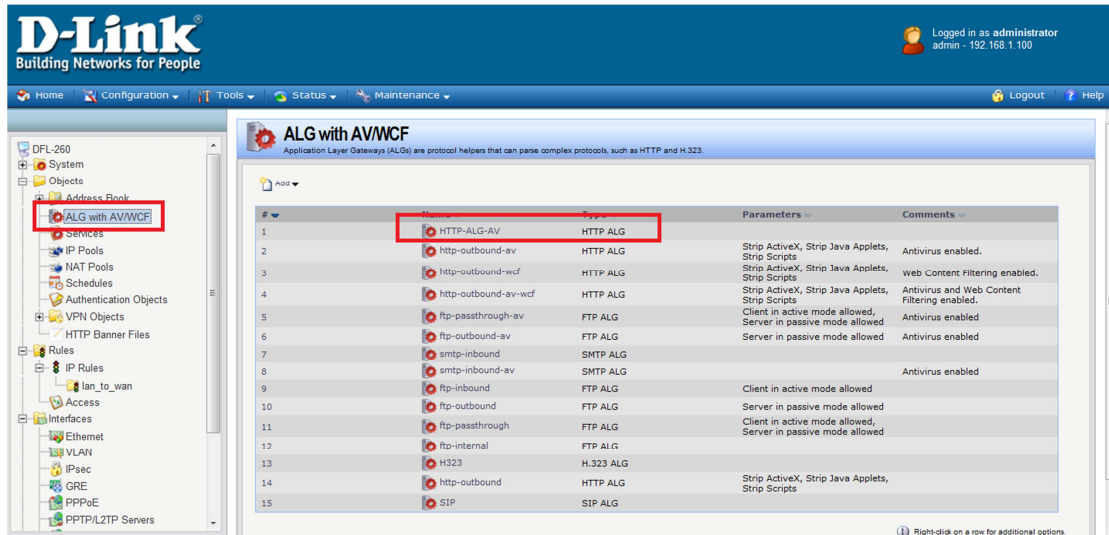


How to setup Anti-Virus Scanning

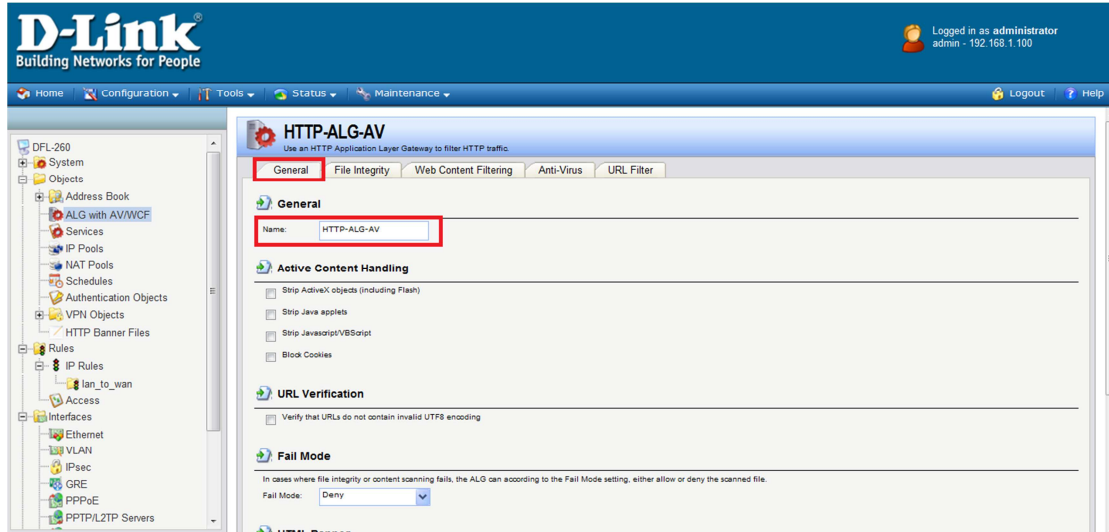
This example shows how to setup an Anti-Virus scanning policy for HTTP traffic from “LAN” to “all-nets”. We will assume there is already a NAT rule defined in the IP rule set to NAT this traffic.

(1) Create an HTTP ALG Object “HTTP-ALG-AV”.



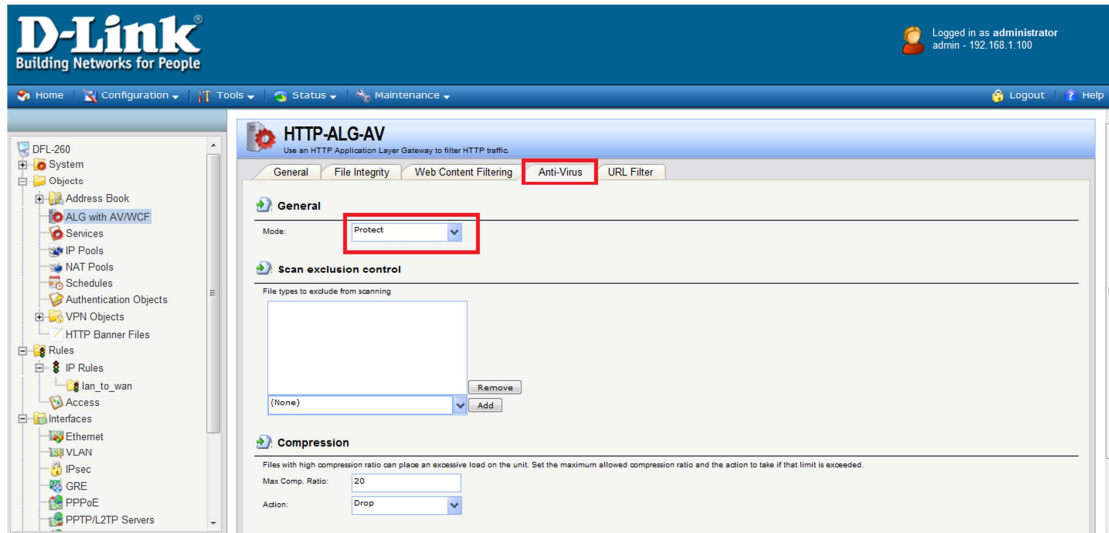
The screenshot shows the D-Link configuration interface. The left sidebar shows the navigation tree with "ALG with AV/WCF" highlighted. The main content area displays a table of ALG objects. The first row, "HTTP-ALG-AV", is highlighted with a red box. The table columns are Name, Type, Parameters, and Comments.

#	Name	Type	Parameters	Comments
1	HTTP-ALG-AV	HTTP ALG		
2	http-outbound-av	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	Antivirus enabled.
3	http-outbound-wcf	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	Web Content Filtering enabled.
4	http-outbound-av-wcf	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	Antivirus and Web Content Filtering enabled.
5	ftp-passthrough-av	FTP ALG	Client in active mode allowed, Server in passive mode allowed	Antivirus enabled
6	ftp-outbound-av	FTP ALG	Server in passive mode allowed	Antivirus enabled
7	smtp-inbound	SMTP ALG		
8	smtp-inbound-av	SMTP ALG		Antivirus enabled
9	ftp-inbound	FTP ALG	Client in active mode allowed	
10	ftp-outbound	FTP ALG	Server in passive mode allowed	
11	ftp-passthrough	FTP ALG	Client in active mode allowed, Server in passive mode allowed	
12	ftp-internal	FTP ALG		
13	H323	H.323 ALG		
14	http-outbound	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	
15	SIP	SIP ALG		

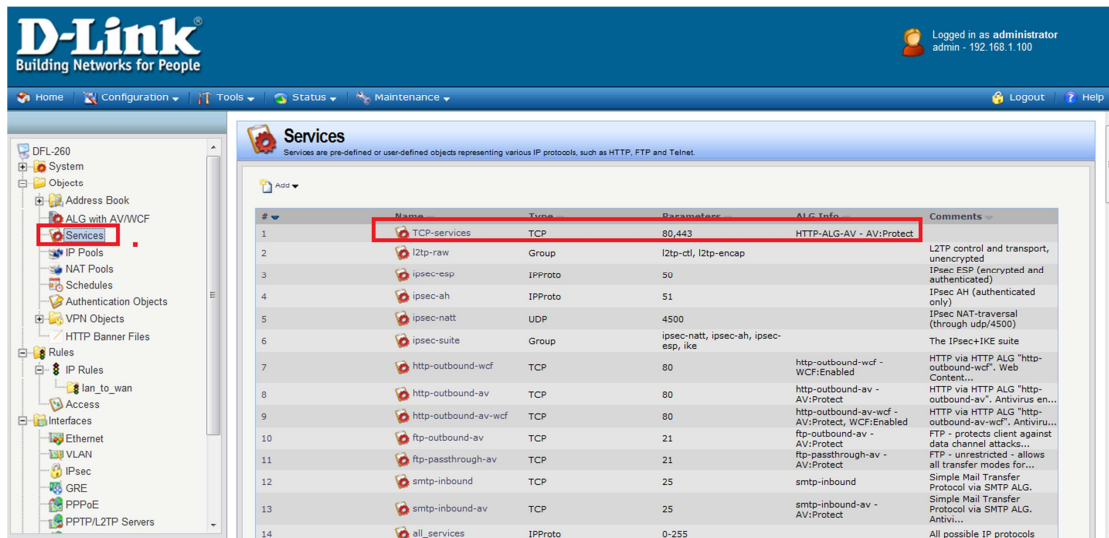


The screenshot shows the configuration page for the "HTTP-ALG-AV" object. The "General" tab is selected. The "Name" field is set to "HTTP-ALG-AV". The "Active Content Handling" section has checkboxes for "Strip ActiveX objects (including Flash)", "Strip Java applets", "Strip Javascript/VBScript", and "Block Cookies". The "URL Verification" section has a checkbox for "Verify that URLs do not contain invalid UTF8 encoding". The "Fail Mode" section has a dropdown menu set to "Deny".

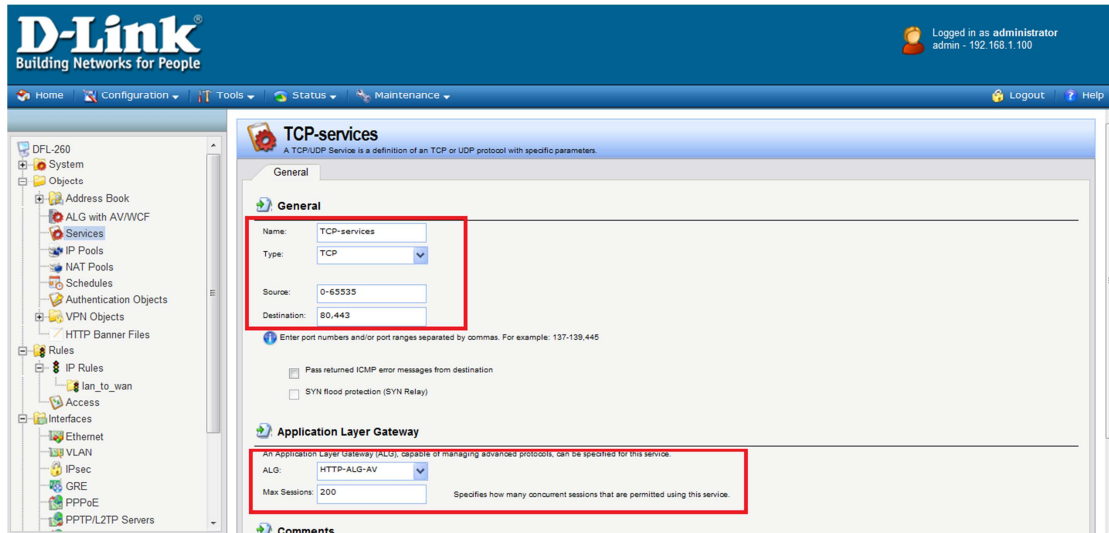
(2) Select “Protect” in the “Mode” dropdown list.



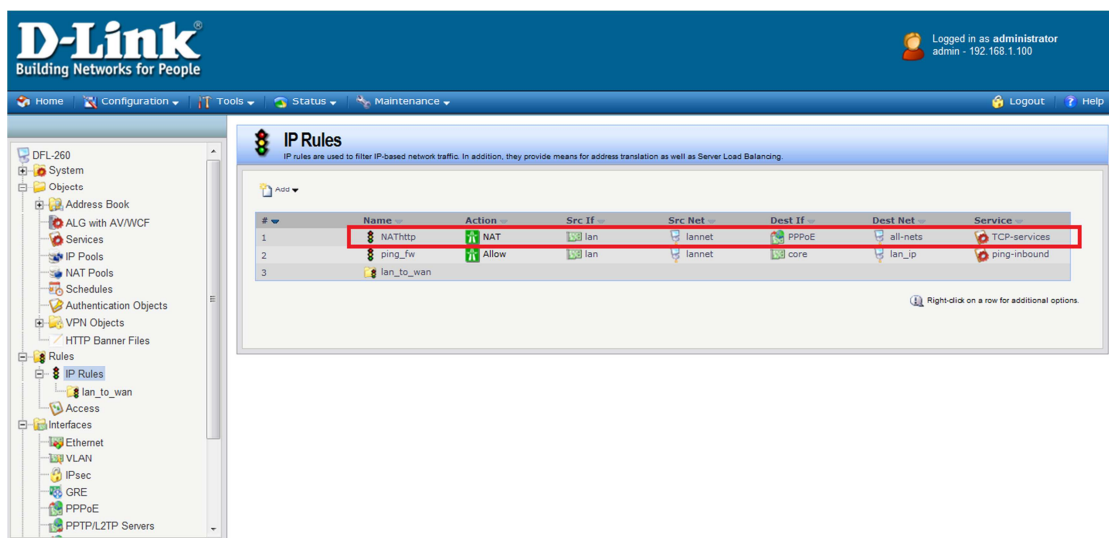
(3) Then, create a “Service object” using the new “HTTP AFG”.

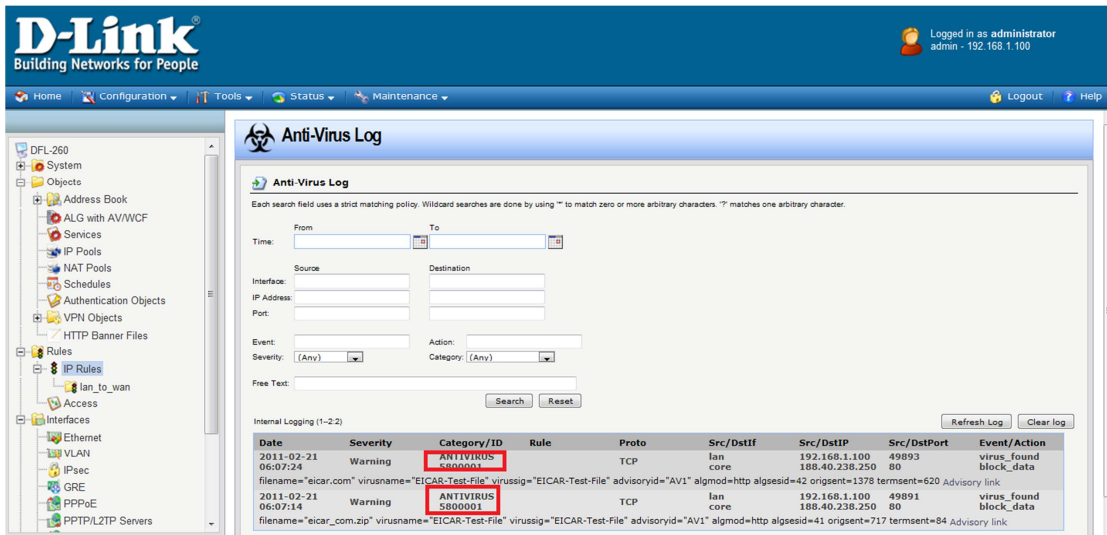
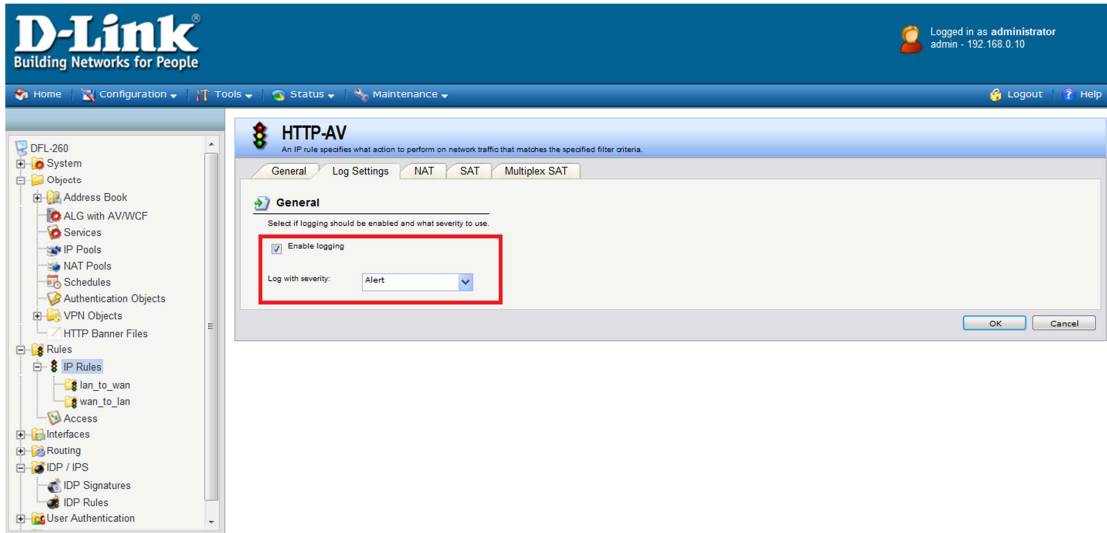


- (4) Select the “TCP” in the “Type” dropdown list. Enter 80 and 443 in the “Destination Port” textbox. Select the “HTTP-ALG-AV” just created in the ALG dropdown list.



- (5) Create a new IP Rule. Select the new service, “TCP-services”, in the “Service” dropdown list. Anti-Virus scanning is now activated for all web traffic from “lanet” to “all-nets”.





Anti-Virus scanning is now activated for all web traffic from “lanet” to “all-nets”.