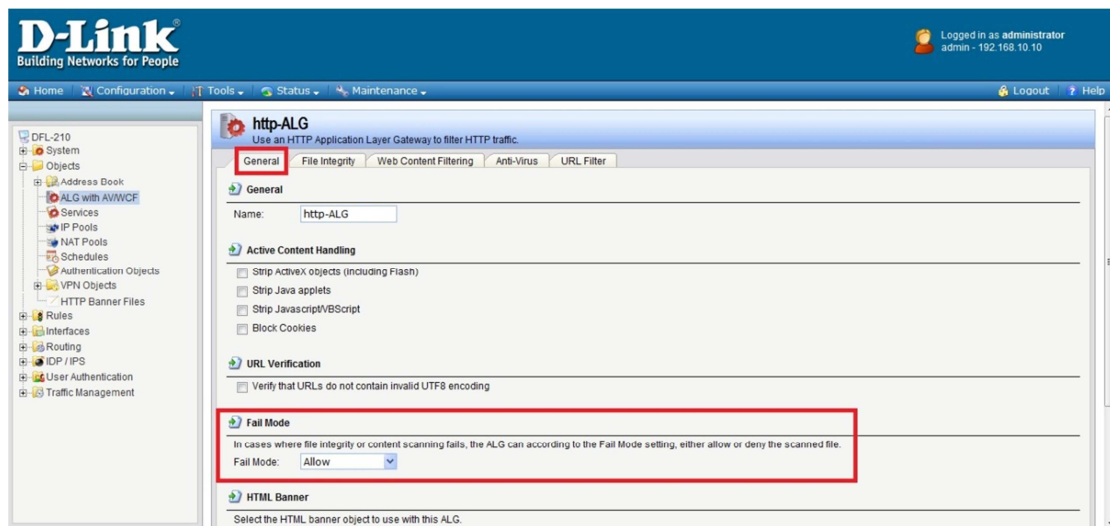
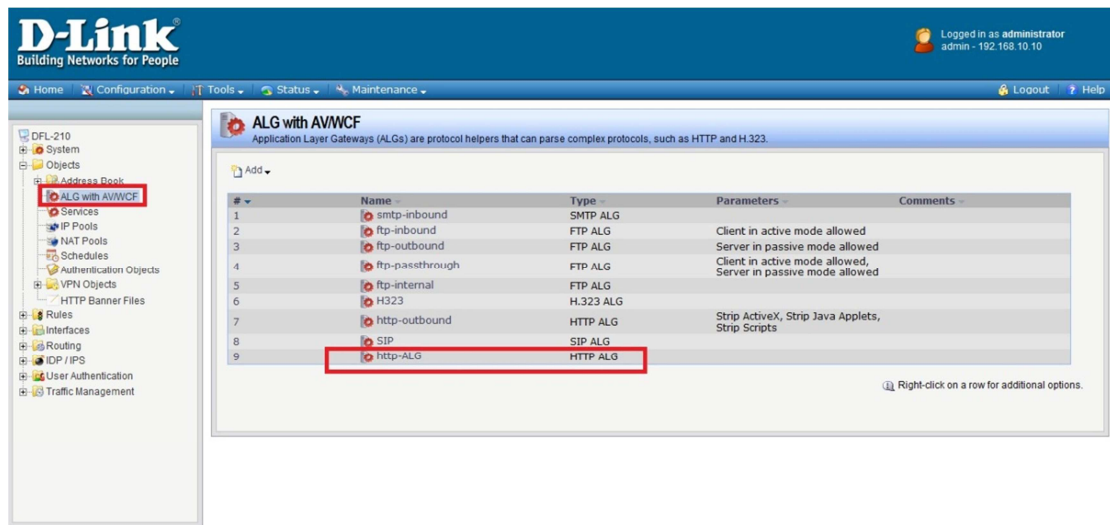


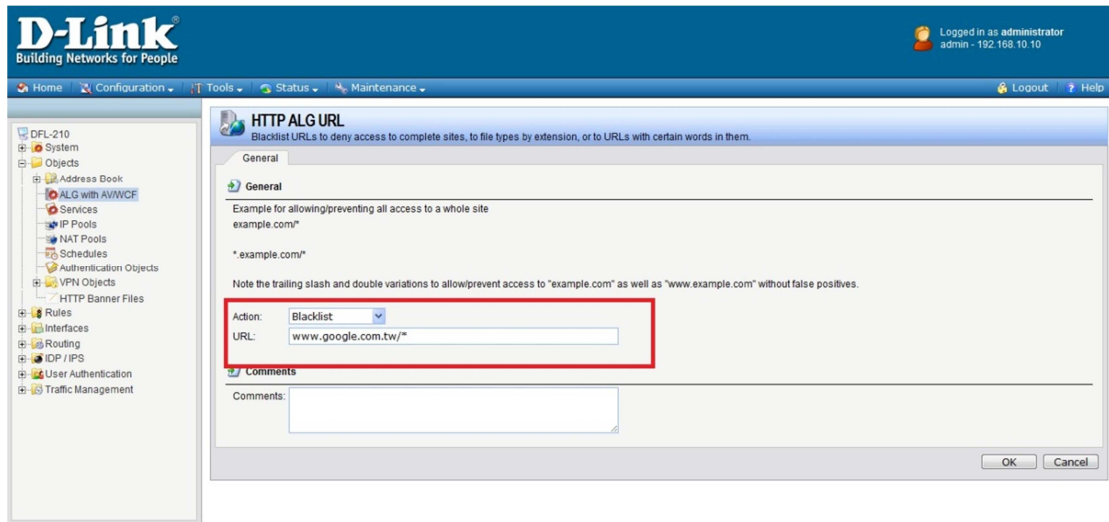
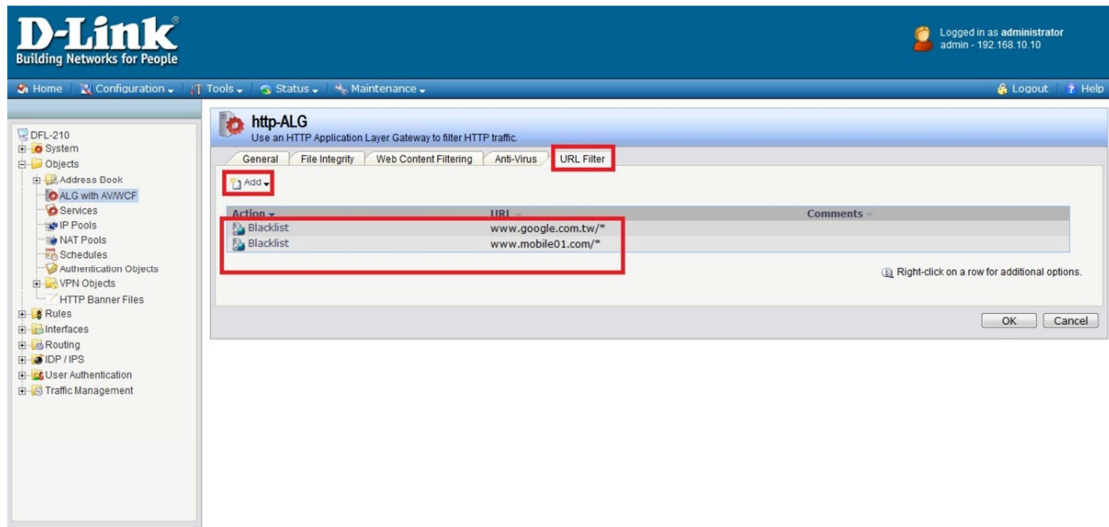
# How to setup static content filtering

Through the HTTP ALG, NetDefendOS can block or permit certain web pages based on configured lists of URLs which called blacklists and whitelists. This type of filtering is also known as Static Content Filtering. The main benefit with Static Content Filtering is that it is an excellent tool to target specific web sites, and make the decision as to whether they should be blocked or allowed.

(1) Adding an HTTP ALG in order to filter HTTP traffic.



- (2) Click the "URL Filter" tab. Now click "Add" and select "HTTP ALG URL" from the menu. Select "Blacklist" as the "Action". Enter [www.google.com.tw/](http://www.google.com.tw/) in the URL textbox.



(3) Adding an "HTTP ALG service" in order to filter HTTP traffic.

The screenshot shows the D-Link configuration interface. In the left sidebar, the 'Services' option is selected. The main area displays a table of services. The first row, 'HTTP-ALG', is highlighted with a red box. The table columns are: #, Name, Type, Parameters, ALG Info, and Comments.

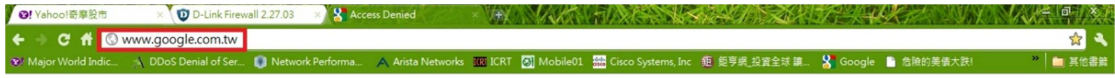
#	Name	Type	Parameters	ALG Info	Comments
1	HTTP-ALG	TCP	80	http-ALG	
2	l2tp-raw	Group	l2tp-ct, l2tp-encap		L2TP control and transport, unencrypted
3	ipsec-esp	IPProto	50		IPsec ESP (encrypted and authenticated)
4	ipsec-ah	IPProto	51		IPsec AH (authenticated only)
5	ipsec-natt	UDP	4500		IPsec NAT-traversal (through udp/4500)
6	ipsec-suite	Group	ipsec-natt, ipsec-ah, ipsec-esp, ike		The IPsec-IKE suite
7	smtp-inbound	TCP	25	smtp-inbound	Simple Mail Transfer Protocol via SMTP ALG.
8	all_services	IPProto	0-255		All possible IP protocols
9	all_tcpudpicmp	Group	all_icmp, all_udp, all_tcp		All ICMP, TCP and UDP services
10	all_tcpudp	TCP/UDP	0-65535		All TCP and UDP services
11	all_icmp	ICMP	All		All ICMP services
12	all_tcp	TCP	0-65535		All TCP services
13	all_udp	UDP	0-65535		All UDP services
14	echo	TCP/UDP	7		Echo service
15	chargen	TCP	19		Character generator
16	ssh	TCP	22		Secure shell
17	ssh-in	TCP	22		Secure shell with SYN flood protection
18	telnet	TCP	23		Telnet

The screenshot shows the configuration page for the 'HTTP-ALG' service. The 'General' tab is active. The 'Name' field is 'HTTP-ALG' and the 'Type' is 'TCP'. The 'Source' is '0-65535' and the 'Destination' is '80'. The 'Application Layer Gateway' section shows 'ALG' set to 'http-ALG' and 'Max Sessions' set to '200'.

(4) Adding an "HTTP-test" IP rule in order to new "HTTP-ALG" service.

The screenshot shows the D-Link configuration interface with the 'IP Rules' section selected. A table of IP rules is displayed. The first rule, 'http-test', is highlighted with a red box. The table columns are: #, Name, Action, Src. If, Src. Net, Dest. If, Dest. Net, and Service.

#	Name	Action	Src. If	Src. Net	Dest. If	Dest. Net	Service
1	http-test	NAT	lan	lan-net	wan	all-nets	HTTP-ALG
2	ping_fw	Allow	lan	lan-net	core	lan_ip	ping-inbound
3	lan_to_wan						



## Forbidden:

Access to the location: <http://www.google.com.tw/>

has been denied for the following reason:  
**Policy prevents this page to be accessed**