How do I configure the content filtering to block URL web access?

Step 1: Open a web browser and type the IP address of the firewall into the address bar (default is **192.168.1.1**). Press Enter.

Step 2: The default username is **admin** (all lower case) and the password is **admin** (all lower case). Click on **OK**.

Step 3: Click on the plus sign next to Objects and then select Application Layer Gateways.

CFL-210	b ALG	b ALG				
Schedules	Application Lay	Application Layer Gateways (ALGs) are protocol helpers that can parse comple				
Authentication Objects	Name 💌	Type 💌	Parameters 🔻			
E Pulae	tp-inbound	FTP ALG	Client in active mode allowed			
	tp-internal	FTP ALG				
co uniterraces	tp-outbound	FTP ALG	Server in passive mode allowed			
C GRouting	tp-passthrough	FTP ALG	Client in active mode allowed, Ser			
E IDP / IPS	Ю Н323	H.323 ALG				
E Guser Authentication	ttp-outbound	HTTP ALG	Strip ActiveX, Strip Java Applets, S			
E G Traffic Management						

Step 4: Select http-outbound, click on Add, and then select HTTP ALG URL.

GDFL-210	by http-outbound
E System	
E Objects	Use an HTTP Application Layer Gateway to filter HTTP traffic.
E Address Book	
ALG	
Schedules	🔊 Add =
Schedules	
Admentication Objects	Action T
E Sules	
Generations	
E Bouting	
F DP/IPS	
E User Authentication	
E- 75 Traffic Management	

Step 5: Create the *Content Filtering* list as followed:

- Action: Blacklist
- **URL:** Key in desired filter URL in the format of Asterisk,dot,yahoo.com, forward slash, asterisk (*.yahoo.com/* in this example)

Click on **OK**.

CDFL-210	b HTTP A	LG URL		
Objects Objects Objects Address Book Objects Al.G Schedules Objects Objects	General Solution Solution	st URLs to deny access t lowing/preventing all a , , , , , , , , , , , , , , , , , , ,	to complete sites, to file type: ccess to a whole site ations to allow/prevent acces	s to "example
	Comments Comments:			

Step 6: Click on the plus sign next to **Rules**, select **IP Rules**, click on **Add**, and then select **IP Rule Folder**.

• Name: name the folder as desired

Click on **OK**.

	🗧 🏮 IP Rules			
DFL-210 System Objects Address Book ALG Services Schedules	IP Rules are used to filter IP-based network traffic. In addition, they provide the second			
Authentication Objects Authen	# Thame Action SourceInterface SourceNetwork De 1 ping_fw Allow Ian Iannet Ian 2 Ian Iannet Ian Iannet Ian 2 Ian Iannet Ian Iannet Ian 3 IP Rule IP Rule In Ian Ian 5 I dmz_to_wan Ian Ian Ian Ian 6 Image: Ian Image: Ian Image: Ian Image: Ian Image: Ian 7 Image: Ian Image: Ian Image: Ian Image: Ian Image: Ian 6 Image: Ian Image: Ian Image: Ian Image: Ian Image: Ian 7 Image: Ian Image: Ian Image: Ian Image: Ian Image: Ian 7 Image: Ian Image: Ian Image: Ian Image: Ian Image: Ian 7 Image: Ian Image: Ian Image: Ian Image: Ian Image: Ian 7 Image: Ian Image: Ian Image: Ian Image: Ian Image: Ian 7 Im			
wan_to_dmz				

Step 7: Click on Add and select IP Rule and configure as followed:

- Name: name as desired
- Action: NAT
- Service: http-outbound
- Schedule: None
- Source Interface: lan
- Source Network: lannet
- Destination Interface: wan
- **Destination Network:** all-nets

Click on **OK**.

😨 DFL-210	8 IP Rui	e			
System System	General Lo	og Settings YNAT	SAT	1	
ALG	8 An Name: Action:	IP rule specifies wha block_yahoo NAT	t action t	o perform on netwo	ik traffic that ma
B- Rules	Service:	http-outbound	~		
E PRules Ban_to_wan Ban_to_dmz C a dmz_to_lan	Address	(None) Filter	and sour	ce network togethe	r with destinatio
wan_to_lan	ETE the	rule to match. Source	_	Destination	
filter_rule	Interface;	lan	~	wan	~

Step 8: Click on the **Configuration** tab and select **Save and Activate** from the dropdown menu. Click on **OK** to activate and save your changes.

