## DFL-210, DFL-600, DFL-1600 How to open ports for a WEB server on LAN

This setup example uses the following network settings:



**Step 1.** Log into the Firewall by opening Internet Explorer and typing the LAN address of the Firewall. In our example we are using 192.168.0.1. Enter Username and Password which you specified during the initial setup of the Firewall.

**Step 2.** If you are setting up a WEB server which uses HTTP port 80, it is advisable to change the default management port of your firewall from 80 to something else. You can set it to be accessed via HTTPS only (port 443) <a href="https://192.168.1.1">https://192.168.1.1</a>. This can be set under System > Remote Management.

D-Link Building Networks for People		Logged in as administrator admin - 192.168.1.2
Section - 👔	Tools 🕶 😼 Status 👻	😕 Logout 🕜 Help
DFL-210	JU HTTP/HTTPS Management	
Objects     Objects     Objects     Objects     Objects     Objects     Objects	Remote Access Type Select the remote access types that should be enabled. HTTP HTTPS Access	5
Copies     Copies	Select the user database to use for login and the access level to grant to the user. User Database: AdminUsers Access Level: Admin	~
	Access Filter      Remote access is granted from the following interface and network.      Interface:     Ian     V Network:     Iannet	<u>15</u>
	Comments Comments	<u>5</u>
		OK Cancel

If you want to leave HTTP management active but change the port to something different for port 80 (e.g. port 88), select "Modify Advanced Settings" under System > Remote Management.



Set WebUI HTTP Port to a different value (e.g. 88).

Note that after applying this setting you will need to log into the firewall via new port number: <u>http://192.168.1.1:88</u>

OSystem	Sperienote management	
ODate and Time	🔊 General	
CONS     Remote Management     Log and Event Receivers     DHCP Settings     Misc. Clients     Mi	Setup and configure methods a WebUI Before Rules: Validation Timeout: 180 seco WebUI HTTP Port: 88 WebUI HTTPS Port: 443 HTTPS Certificate: AdminCert Simple Network Management P	end permissions for remote management of this system. Enable HTTP(S) traffic to the firewall regardless of configured IP Rules. Time to wait for an admin to login before reverting config
Traffic Shaping	SNMP specific settings. SNMP Before Rules: Request Limit: 100 System Contact: N/A System Name: N/A System Location: N/A Interface Description: Name Interface Alias: Hardware	Enable SNMP traffic to the firewall regardless of configured IP Rules. Maximum number of SNMP packets that will be processed each second The contact person for this managed node The name for this managed node The physical location of this node What to display in the SNMP MIB-II ifDescr variables What to display in the SNMP ifMIB ifAlias variables

You can also change the validation timeout to 180 sec. That will mean that the firewall will wait for your login for 180 sec before reverting new settings to previous state.

Click on OK when done. Apply these new settings by clicking on Configuration > Save and Activate > OK. Re-login into the firewall via new port number or via HTTPS.

Step 3. Go to Objects > Address Book. Click on Add and select "IP4 Host/Network".

D-Link Building Networks for People				Cogged in as admin	administrato - 192.168.1.10	<b>r</b> 0
SHome 📑 Configuration 🗸 🎁 To	ols 👻 🥥 Status 🕶			1	Logout	@Help
CFL-210 CFL-210 Citiects Citiects Content aceAddresses Address Book Citiects Content aceAddresses Schedule Profiles Citiects C	Address Book	k contains symbolic names for var Address ▼ sses 0.0.0.0/0	ious types of addresses, includin UserAuthGroups 💌	ng IP netwoks and Ethemet MAC addresses. Comments This folder contains addresses for interfaces All possible networks Right-click on a rowfort	uther options.	

**Step 4.** Under Name enter "WEB\_Server" and under IP Address specify the IP address of the server on your LAN. In our example it is 192.168.1.2. Click on OK when done.

D-Link Building Networks for People	Cogged in as admin	administrator - 192.168.1.100
Seconfiguration 👻 🕌 To	ools 👻 🧉 Status 🕶	Logout @Help
DFL-210 System Colects Application Layer Cateways Schedule Profiles X 509 Certificates VPN Objects Rules Rules Colection C	Image: Server         IP Address:         IP Address:	25.50°
	OK	Cancel

Step 5. Go to Rules > IP Rules. Click on Add and select "IP Rule".

Home 📑 Configuration 👻 🧃	🖌 Tools 👻 🥹 Status 👻					Logout	C
FL-210 System Coljects Rules Prules Coljects Rules Coljects	Add + P Rules P Rule P Rules P Rules	d to filter IP-based network traffic. In . Action V Source Interface V Allov Blan	addition, they provide m Source Network ~ g lannet	eans for address translation as w Destination Interface * i core	will as Server Load Balancing. Destination Network ¥ ¥ Ian_ip	Service • ping-inbount	ŝ
Routing DS / IDP User Authentication Traffic Shaping	5 🔓 wan_to_lan 6 🕻 wan_to_dmz				() Right-click on J	e row for further option	6.

Step 6. Specify the new IP rule settings:

Name: Webserver\_SAT

Action: SAT

Service: HTTP (You can specify a different service if your server requires a different port to be opened. You can create your own service with required ports under Objects > Services > Add).

Source Interface: any Source Network: all-nets

Destination Interface: core

Destination Network: wan\_ip

Building Networks for People								Cogged in as admini admin - 192	strator 168.1.2
Home 🛛 💂 Configuration 👻 🍟	Tools 🗸 😺 Statu:	5 🕶						2000	ut ØHe
DFL-210	8 Webse	erver_SAT							
O System	General Lo	g Settings NA	T SAT						
- BONS	🛃 General								5
Log and Event Receivers     Log and Event Receivers     DHCP Settings     Misc. Clients      Xdvanced Settings	Name: Action:	Webserver_SA	Nat action to p	perform on netwo	e tramo that m	atches the specif	fied filter ontena.		
Objects	Service:	http	~						
E PRules	Schedule:	(None)	~						
g dmz_to_lan	🛃 Address	Filter							5
-is lan_to_wan	Spe-	cify source interfa	ice and source	network, togethe	er with destinati	on interface and	d destination network. All para	imeters have to match for the rule to match.	
wan_to_lan		Source		Destination					
Access	Interface:	any	~	core	*				
Routing	Network	all-nets	*	wan_ip	*				
BDS / IDP	S Comment								1.00
User Authentication	Comments	SAT rule for in	ncoming HTT	P traffic					~

Click on SAT tab and under Destination IP Address select "WEB\_Server". Click on OK when done.



Step 7. Specify the new IP rule settings: Name: Webserver\_NAT Action: NAT Service: HTTP (You can specify a different service if your server requires a different port to be opened. You can create your own service with required ports under Objects > Services > Add). Source Interface: any Source Network: all-nets Destination Interface: core Destination Network: wan\_ip

Building Networks for People		Logged in as <b>administrator</b> admin - 192.168.1.2
Section - Configuration -	🎬 Tools 🗸 🗳 Status 🗸	😕 Logout 🕐 H
Q DFL-210	Webserver_NAT	
System	General Log Settings NAT SAT	
B- 📁 Objects B- 🚺 Bules	D General	
emz_so_wan lan_to_dmz lan_to_wan wan_to_dmz wan_to_lan Access E Monterfaces E Routing C Inp	Name: Webserver_NAT Action: NAT V Service: http V Schedule: (None) V	5
B- User Authentication B- C Traffic Shaping	Specify source interface and source network, together with destination interf match for the rule to match.	ace and destination network. All parameters have to
	Interface: any v core v	
	Network all-nets van_ip v	
	Orments	5
	Comments: NAT for loopback	

Step 8. Add another IP rule with the following settings:

Name: Webserver\_Allow Action: Allow Service: HTTP (You can specify a different service if your server requires a different port to be opened. You can create your own service with required ports under Objects > Services > Add). Source Interface: any Source Network: all-nets Destination Interface: core Destination Network: wan\_ip

## Click on OK.



**Step 9.** Rearrange the IP rules so the "Webserver\_SAT" rule is on top, followed by "Webserver\_NAT" and "Webserver\_Allow". To do that right-click on the rule and select "Move Up" or "Move to Top".



The final rules arrangement should look like this:

S Ad	IP Rules are use Batancing.	d to filter IP-b	ased network traff	ic. In addition, the	y provide means for	address translation as	well as Server Lo
- 1	Name 💌	Action 🔻	Source	Source	Destination	Destination	Service 👻
	8 Webserver_SA	T SAT	any	3 all-nets	core	g van_ip	http
	Webserver_NA	T NAT	any	3 all-nets	core	g van_ip	http
	8 Webserver_All	wollA wo	any	🤤 all-nets	core	😌 van_ip	http
	g ping_fv	Allow	时 lan	🤤 lannet	📷 core	🤤 lan_ip	inbound
	alan_to_wan						
	alan_to_dmz						
	g dmz_to_lan						
	g dmz_to_wan						
	# wan_to_lan						
	s wan_to_dmz						

Step 10. 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.