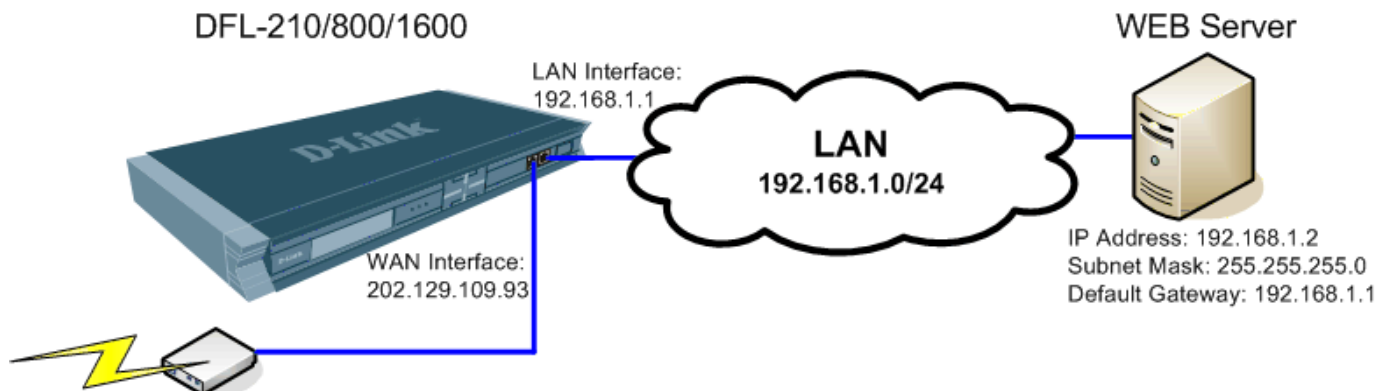


DFL-210, DFL-800, DFL-1600 How to open ports for a WEB server on LAN

This setup example uses the following network settings: the WAN interface has public IP address. The modem is in bridge mode (no NAT). The FTP server is on a network connected to the LAN interface.



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.

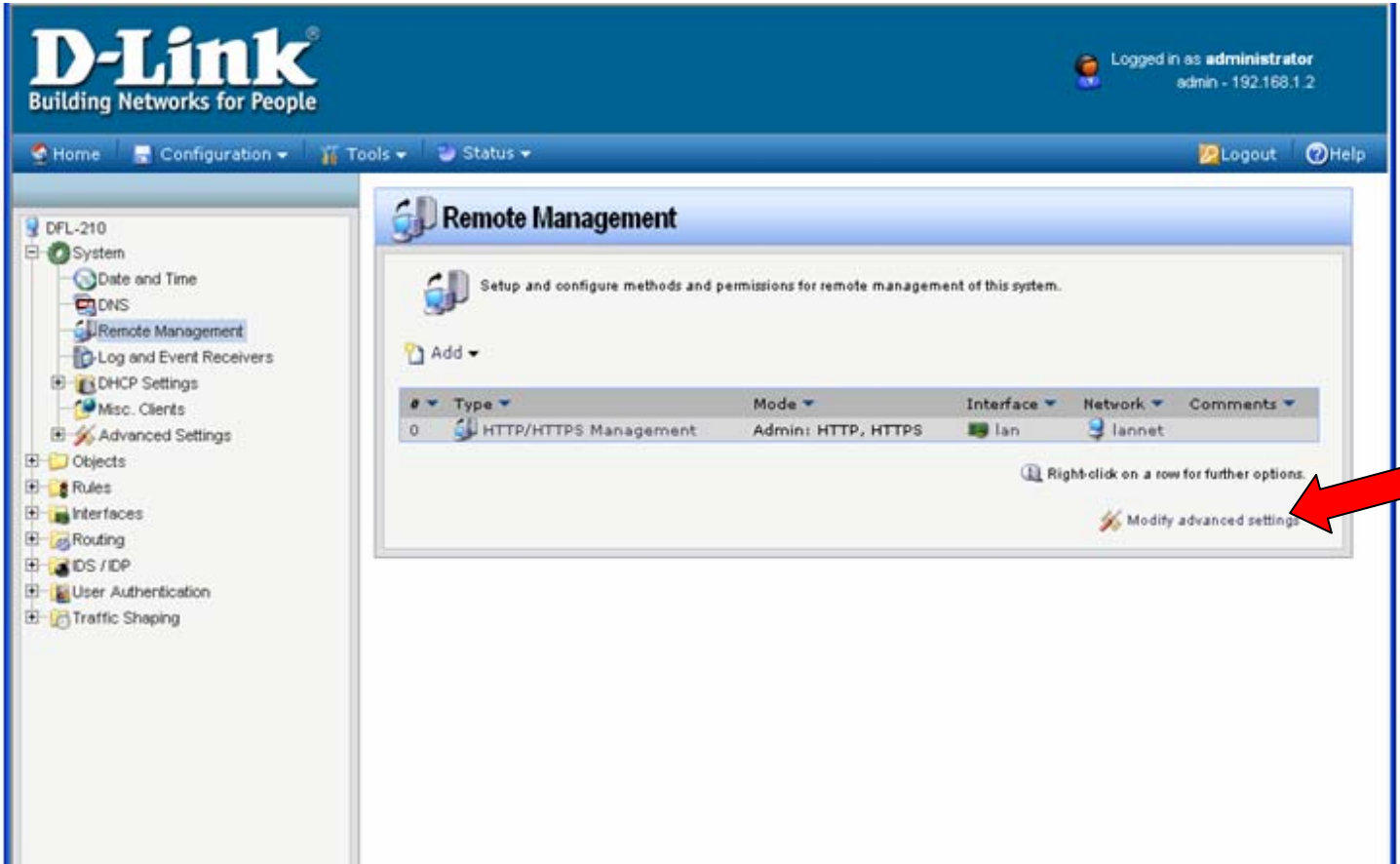
Step 2. If you are setting up a WEB server which uses HTTP port 80, it is advisable to change the default management port of your firewall from 80 to something else. You can set it to be accessed via HTTPS only (port 443) <https://192.168.1.1>. This can be set under System > Remote Management.

The screenshot shows the D-Link firewall web interface. The top navigation bar includes 'Home', 'Configuration', 'Tools', and 'Status'. The user is logged in as 'administrator' with IP '192.168.1.2'. The left sidebar shows a tree view of system settings, with 'Remote Management' selected. The main content area is titled 'HTTP/HTTPS Management' and contains the following sections:

- Remote Access Type:** Select the remote access types that should be enabled. HTTP, HTTPS.
- Access:** 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: lan, Network: lannet.
- Comments:** A text input field for comments.

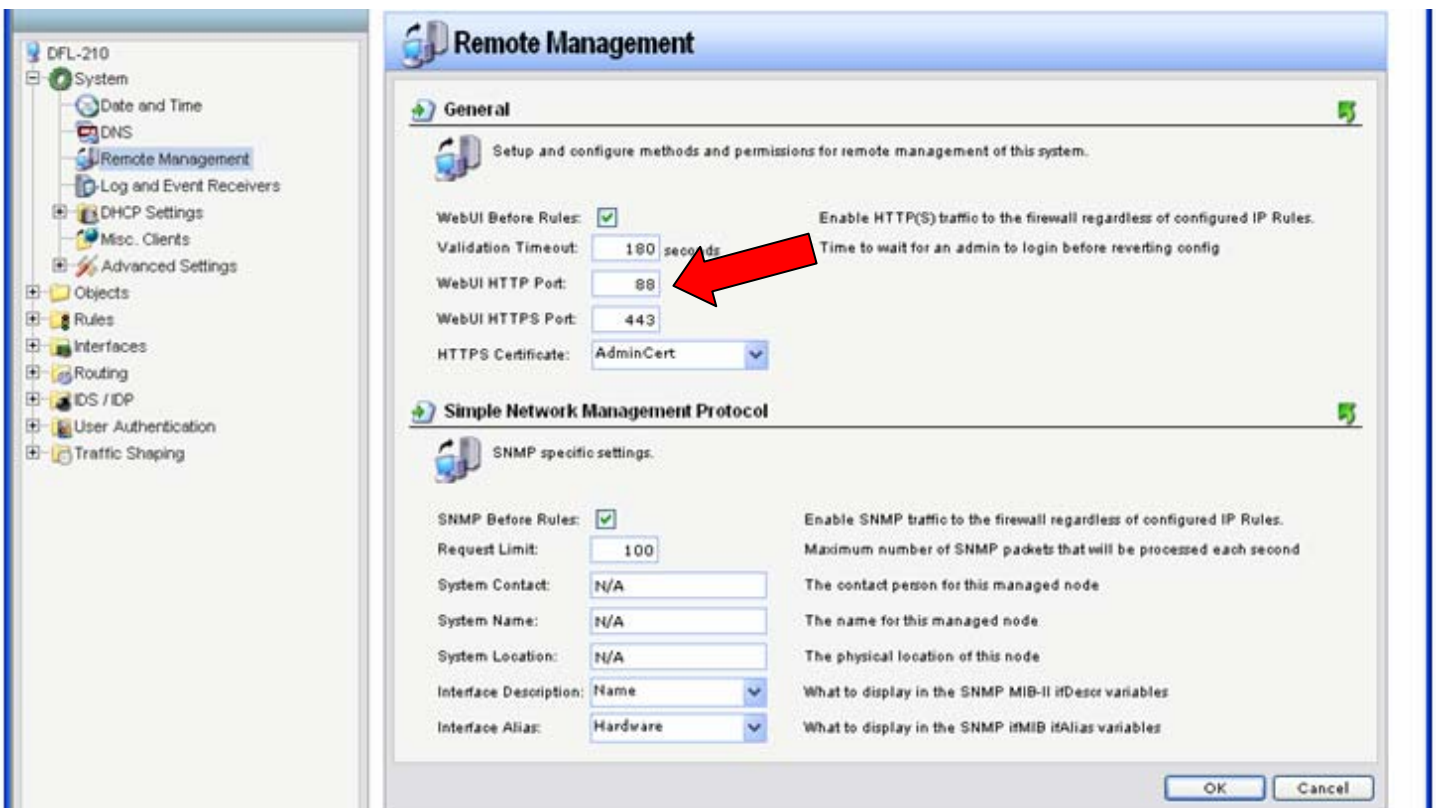
Buttons for 'OK' and 'Cancel' are located at the bottom right of the configuration area.

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).

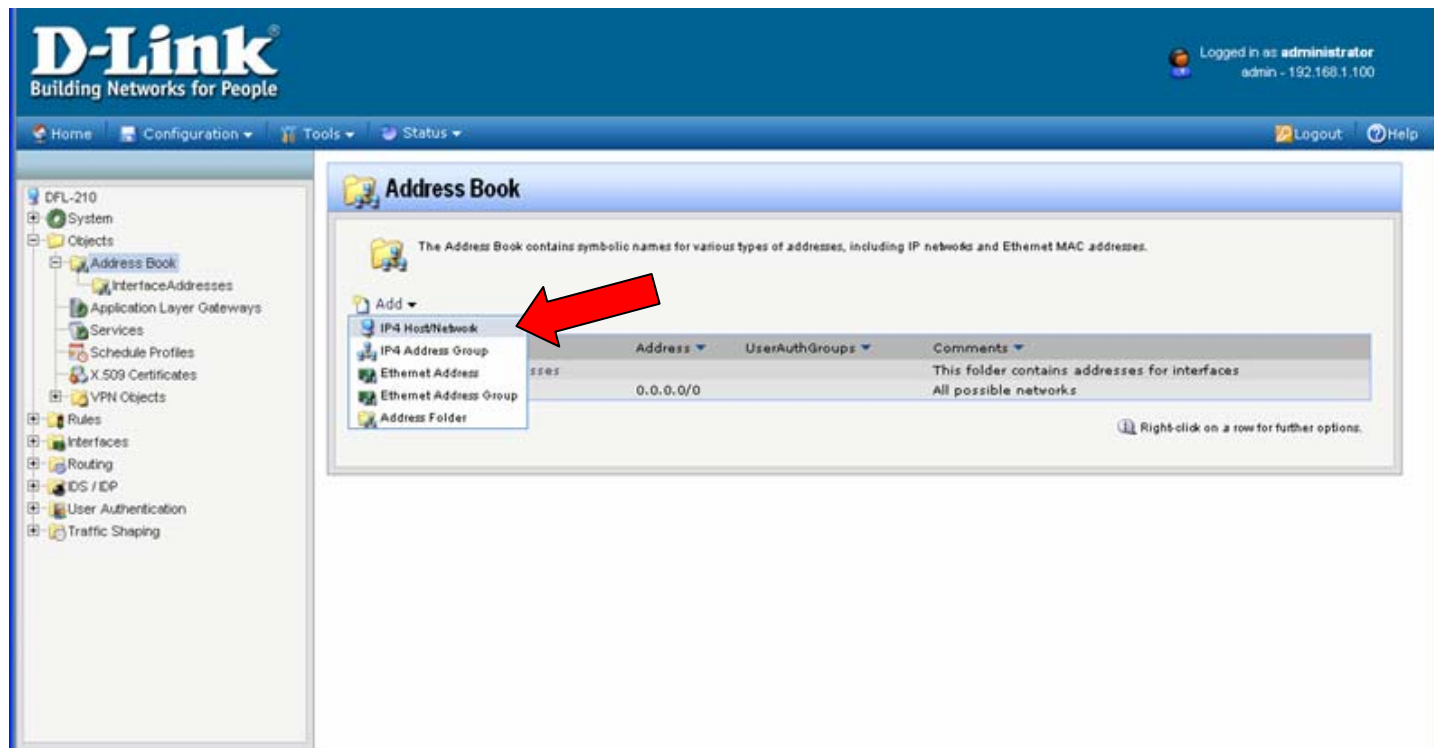
Note that after applying this setting you will need to log into the firewall via new port number: <http://192.168.1.1:88>



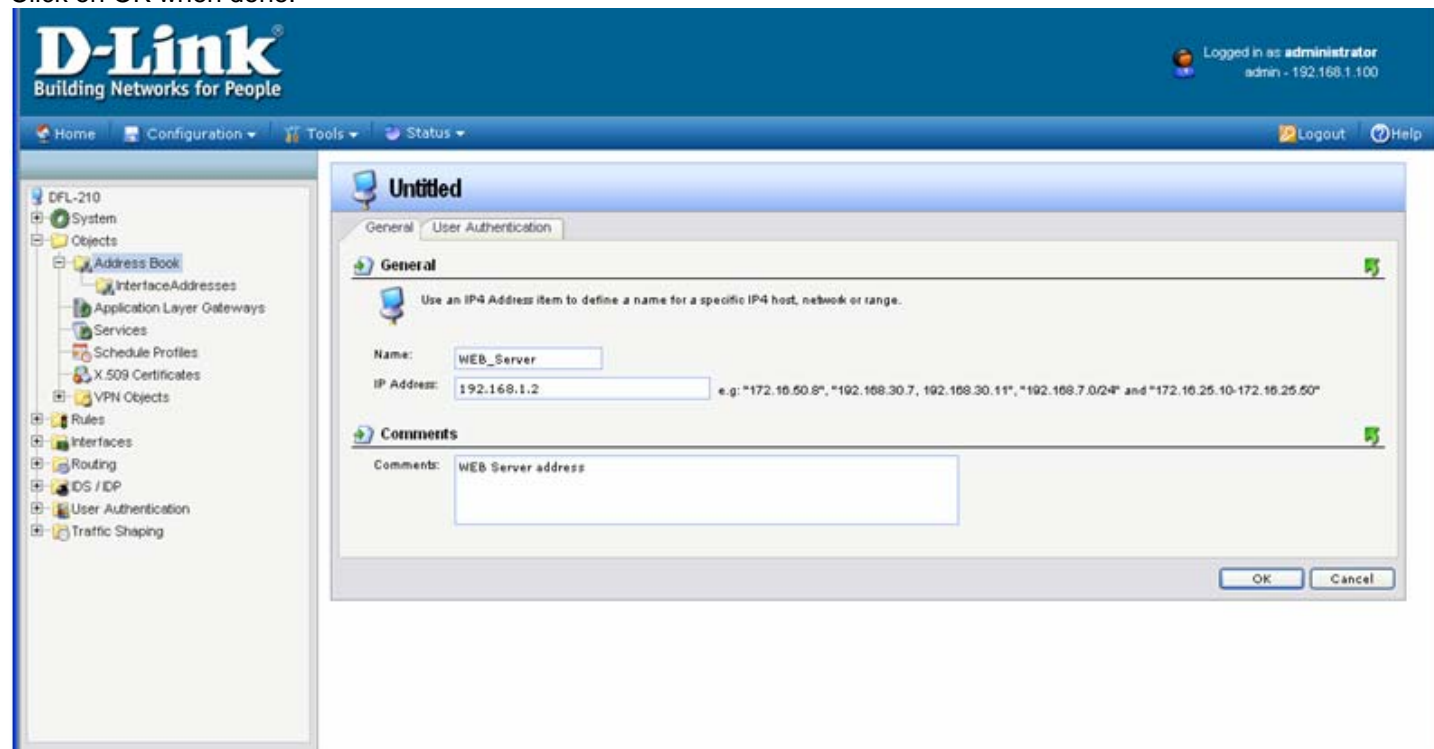
You can also change the validation timeout to 180 sec. That will mean that the firewall will wait for your login for 180 sec before reverting new settings to previous state.

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.

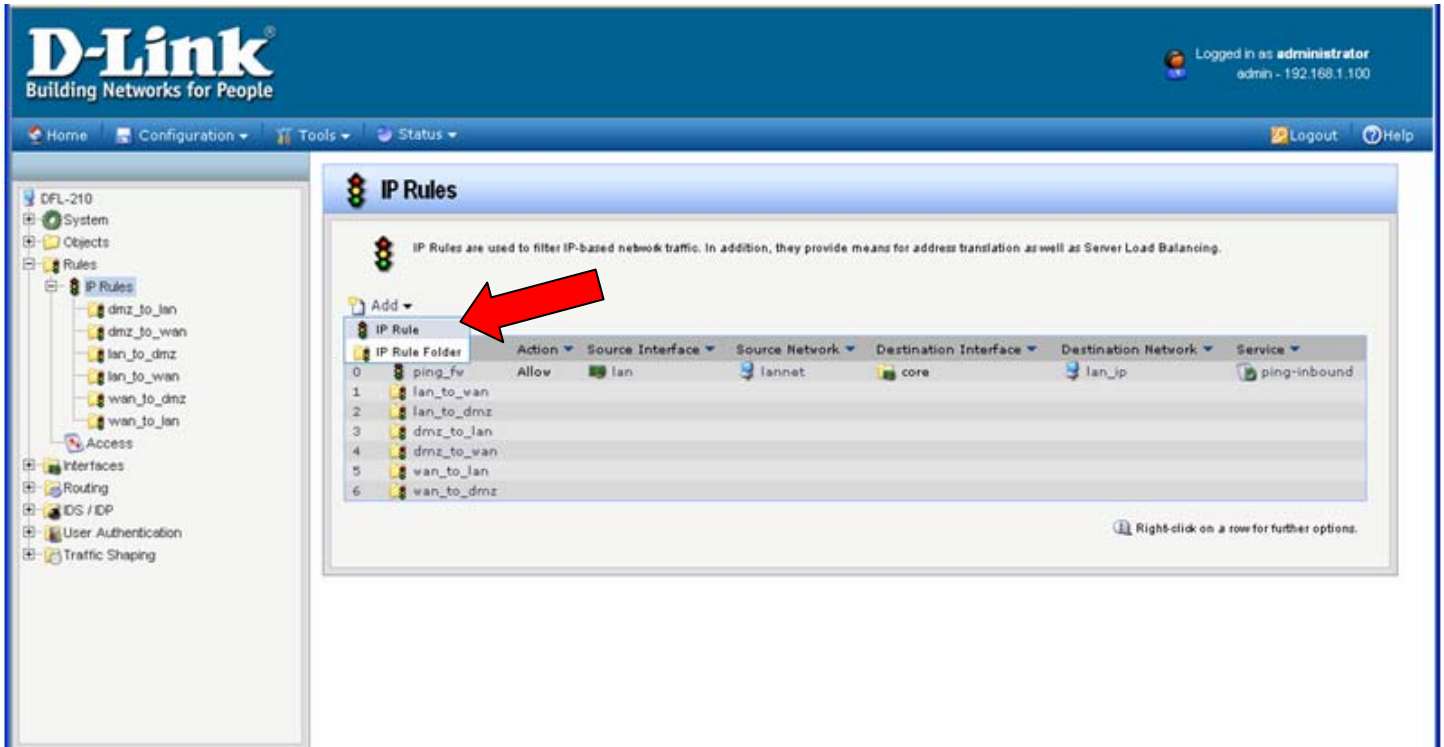
Step 3. Go to Objects > Address Book. Click on Add and select "IP4 Host/Network".



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.



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



Step 6. Specify the new IP rule settings:

Name: Webserver_SAT

Action: SAT

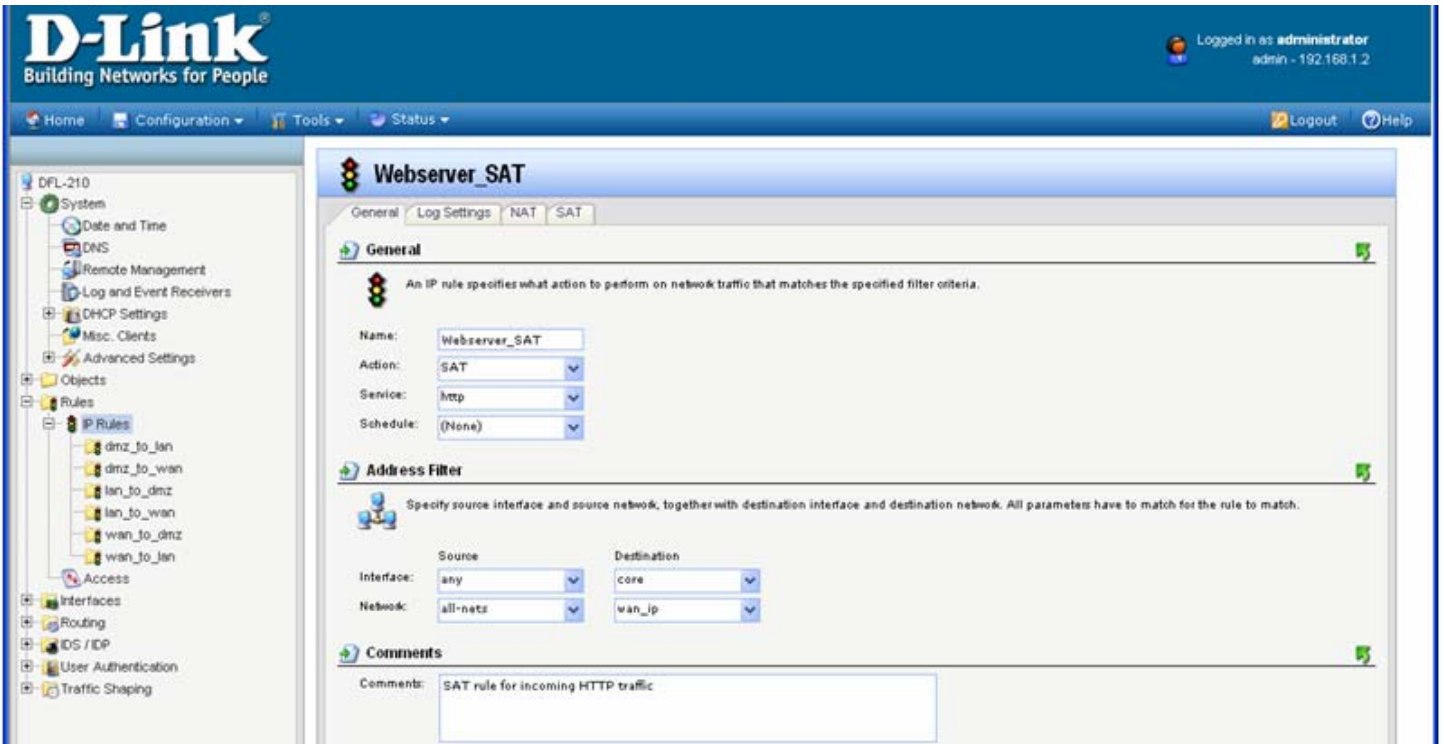
Service: HTTP (You can specify a different service if your server requires a different port to be opened. You can create your own service with required ports under Objects > Services > Add).

Source Interface: any

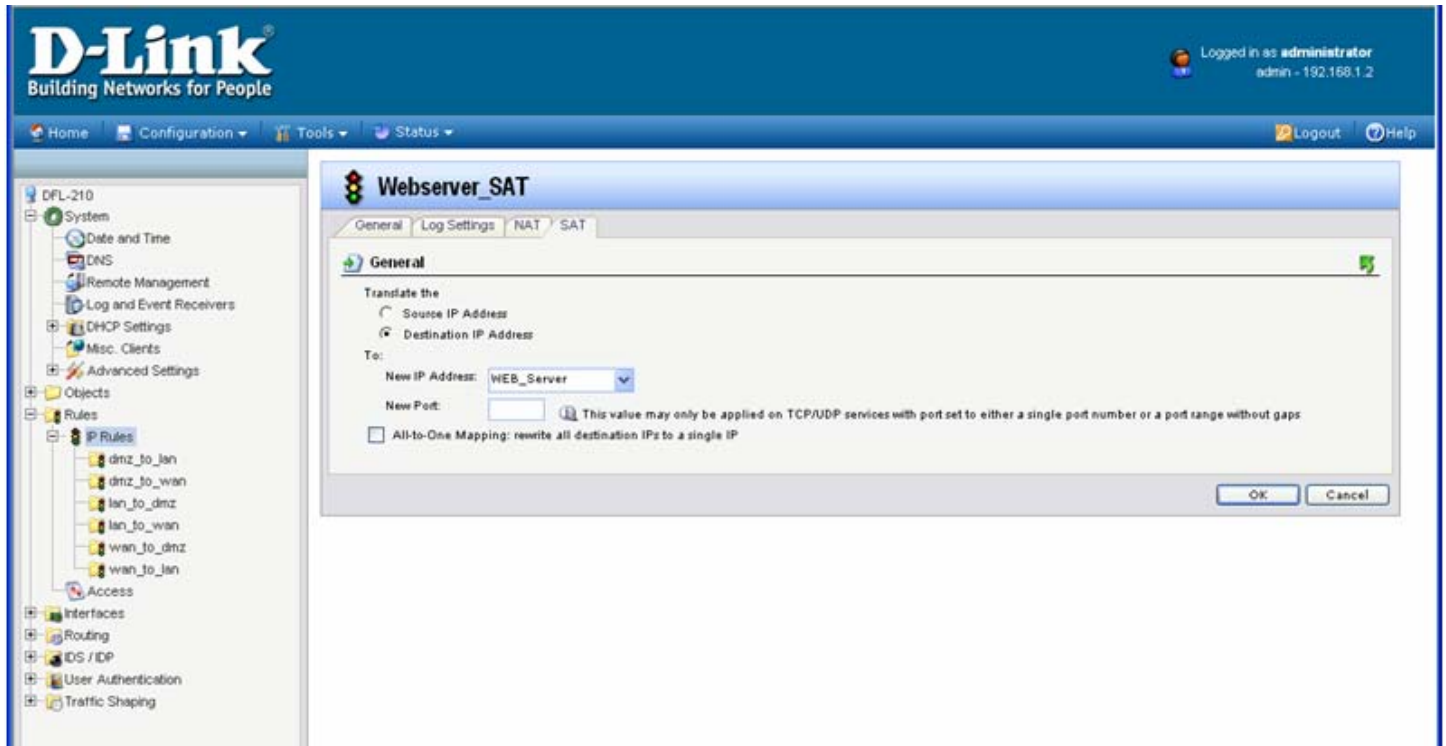
Source Network: all-nets

Destination Interface: core

Destination Network: wan_ip



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

Click on OK.

The screenshot shows the D-Link web management interface. The top navigation bar includes 'Home', 'Configuration', 'Tools', and 'Status'. The user is logged in as 'administrator' with IP '192.168.1.2'. The left sidebar shows a tree view with 'Rules' expanded to 'IP Rules', where 'Webserver_NAT' is selected. The main content area is titled 'Webserver_NAT' and has tabs for 'General', 'Log Settings', 'NAT', and 'SAT'. The 'General' tab is active, showing the following configuration:

- General:** Name: Webserver_NAT, Action: NAT, Service: http, Schedule: (None).
- Address Filter:** Source Interface: any, Source Network: all-nets, Destination Interface: core, Destination Network: wan_ip.
- 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).

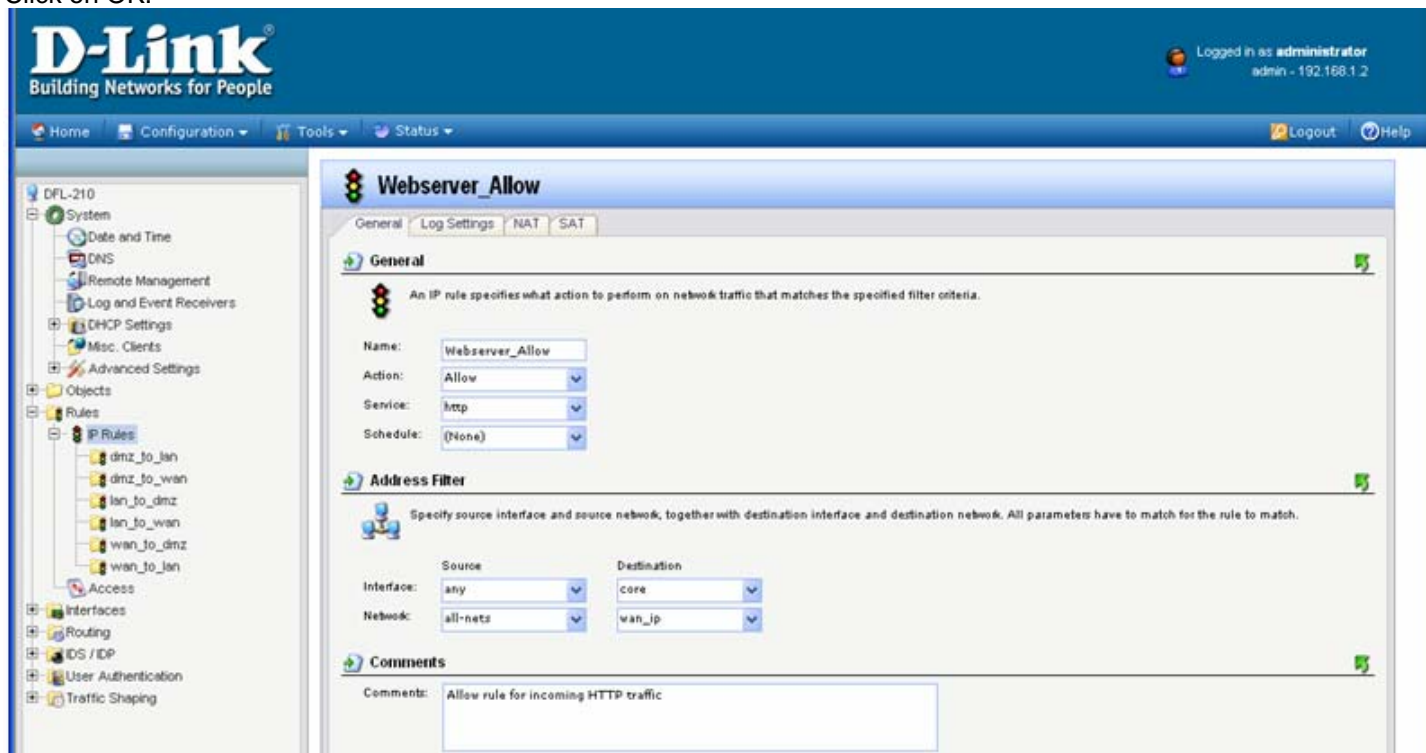
Source Interface: any

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 screenshot shows the D-Link web interface with the IP Rules configuration page. The left sidebar shows a tree view with 'Rules' expanded to 'IP Rules'. The main content area shows a table of IP rules. A context menu is open over the 'Webserver_Allow' rule (row 9), with 'Move to Top' selected. The table below shows the current order of rules:

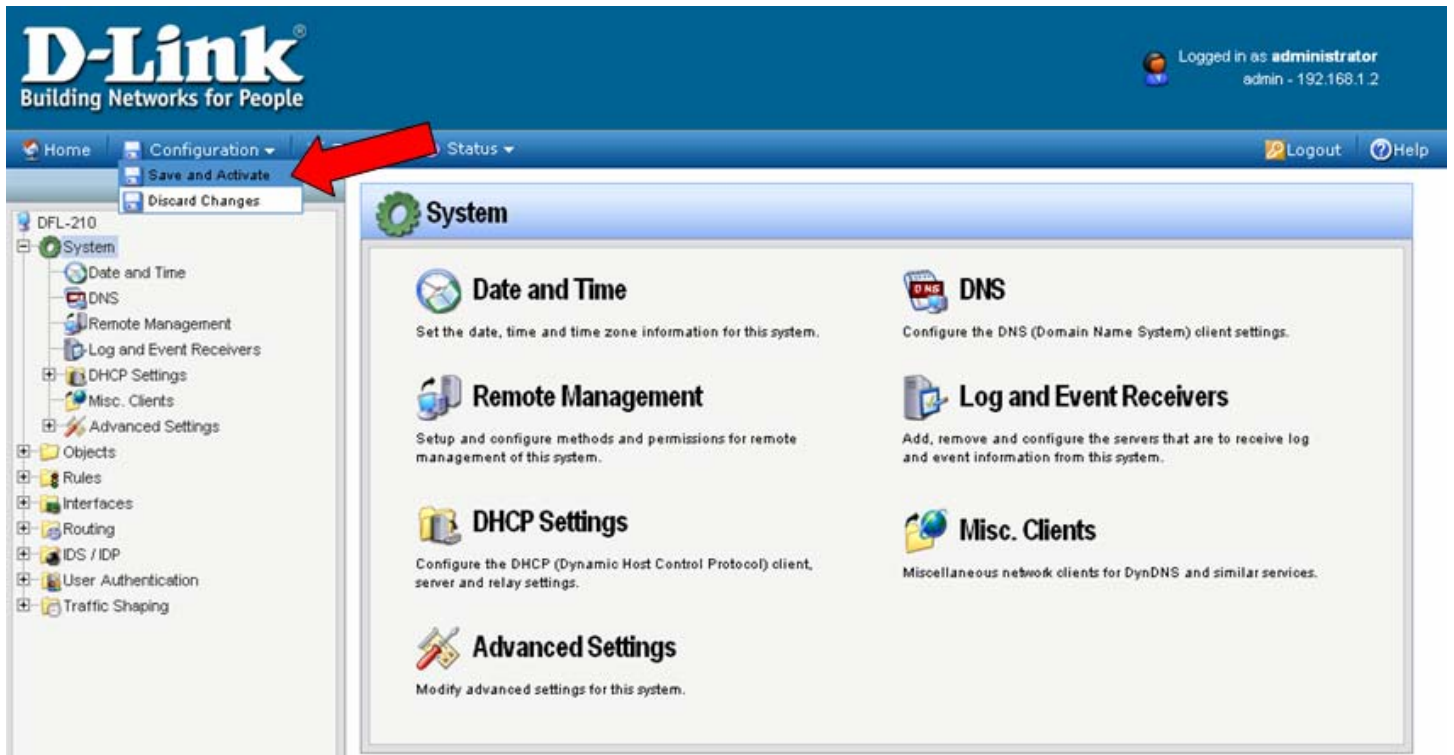
#	Name	Action	Source Interface	Source Network	Destination Interface	Destination Network	Service
0	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
1	lan_to_wan						
2	lan_to_dmz						
3	dmz_to_lan						
4	dmz_to_wan						
5	wan_to_lan						
6	wan_to_dmz						
7	Webserver_SAT	SAT	any	all-nets	core	wan_ip	http
8	Webserver_NAT	NAT	any	all-nets	core	wan_ip	http
9	Webserver_Allow	Allow	any	all-nets	core	wan_ip	http

The final rules arrangement should look like this:

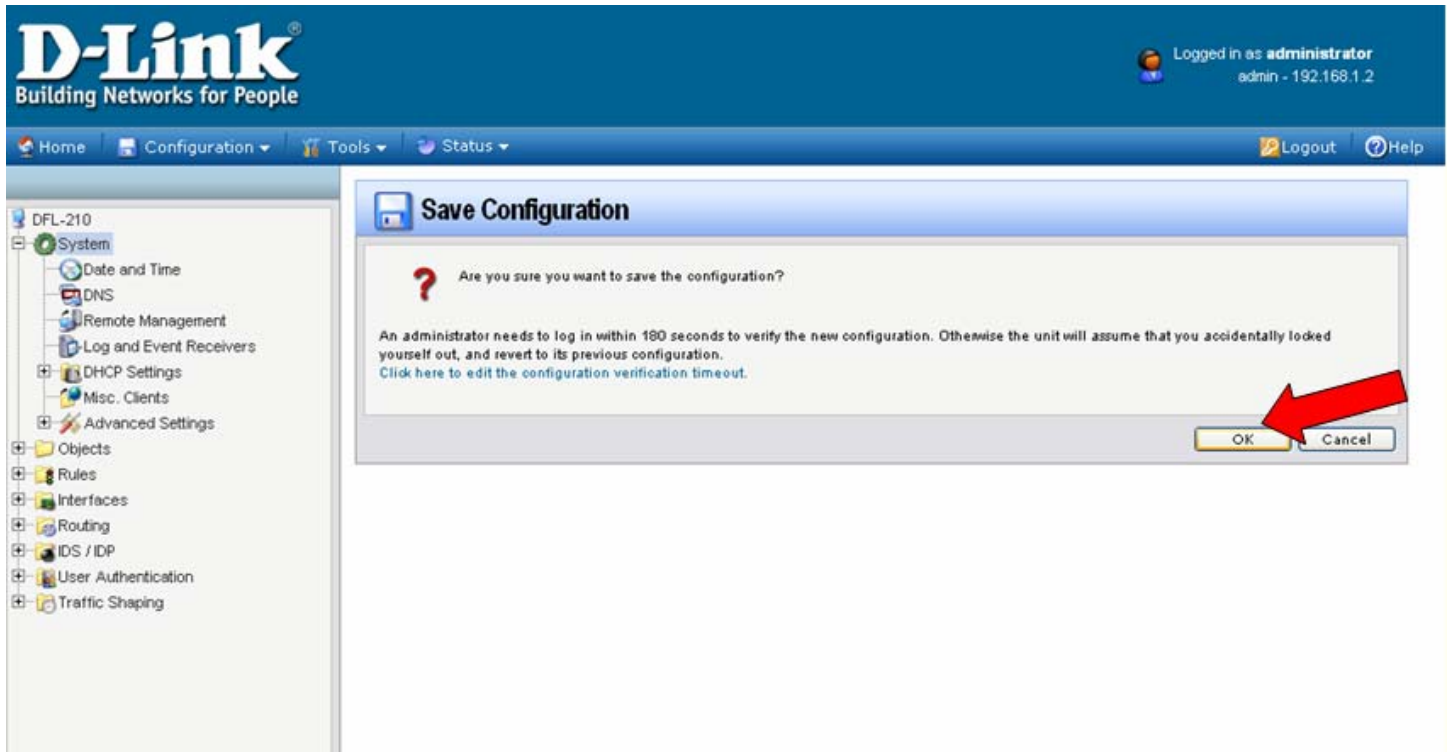
The screenshot shows the D-Link web interface with the IP Rules configuration page. The table below shows the final arrangement of rules:

#	Name	Action	Source Interface	Source Network	Destination Interface	Destination Network	Service
0	Webserver_SAT	SAT	any	all-nets	core	wan_ip	http
1	Webserver_NAT	NAT	any	all-nets	core	wan_ip	http
2	Webserver_Allow	Allow	any	all-nets	core	wan_ip	http
3	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
4	lan_to_wan						
5	lan_to_dmz						
6	dmz_to_lan						
7	dmz_to_wan						
8	wan_to_lan						
9	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.