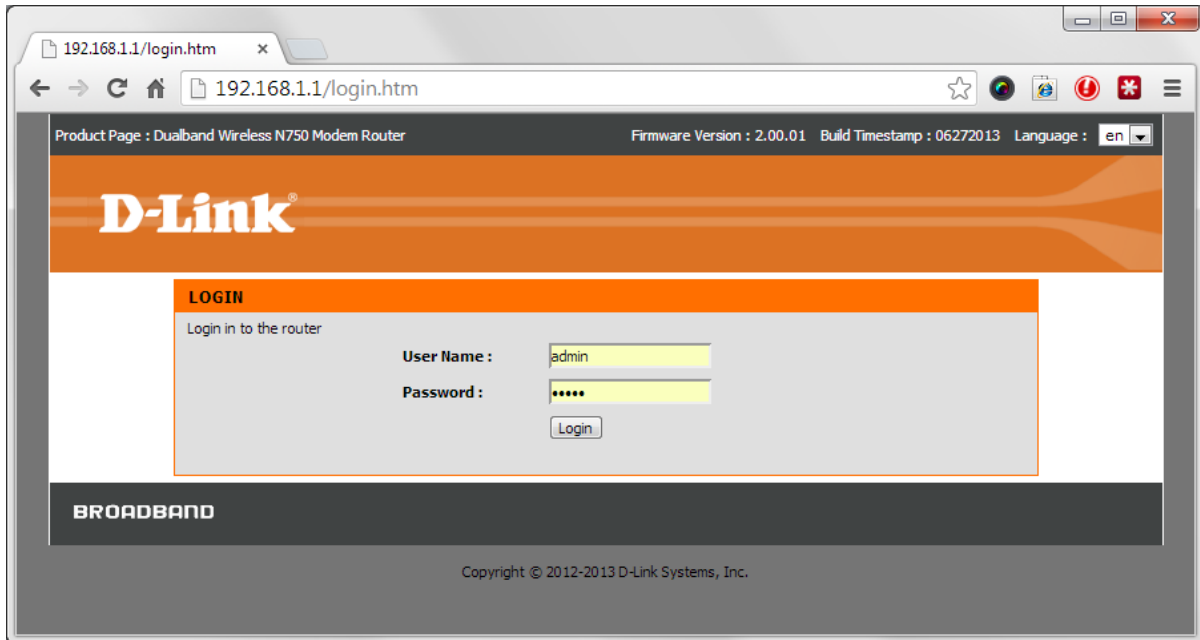


How to open ports in your modem router firewall

This document details how to set port forwarding rules in your modem/router firewall

Please note: It is recommended to set the device you are opening ports for (PC, Xbox, PlayStation, etc.) with a static IP address. Please see your device instructions on how to manually set an IP address.

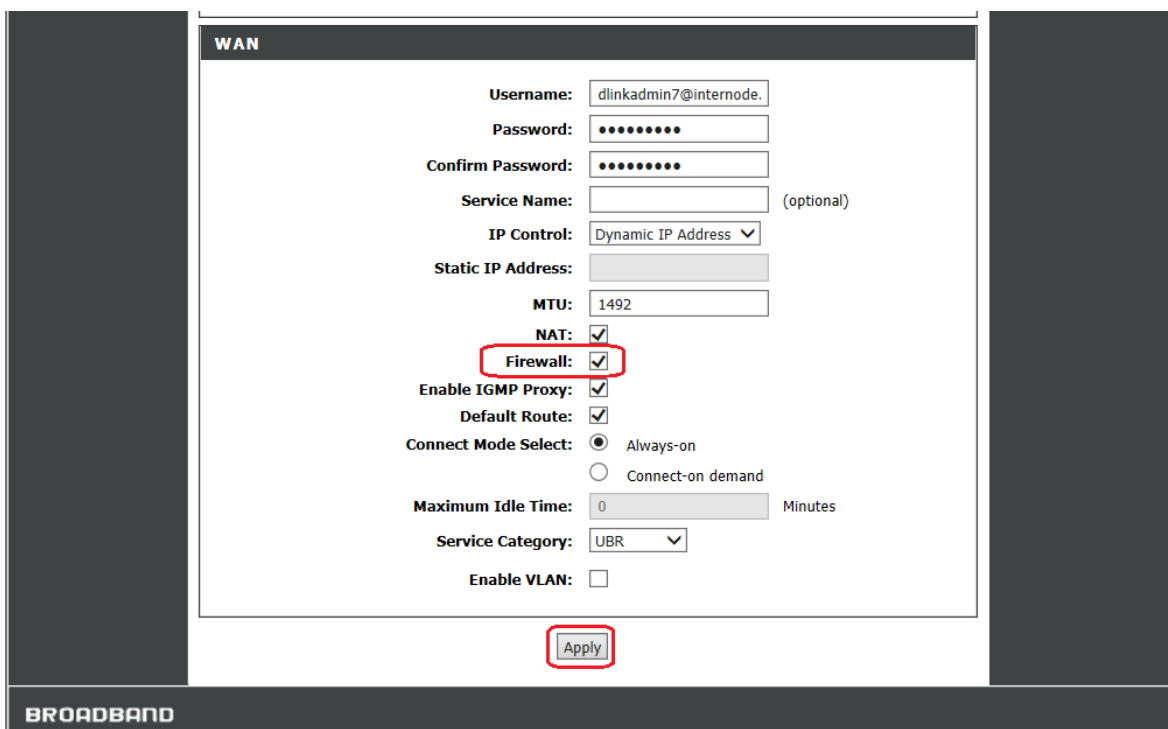
Step 1. Open your Internet Browser and in the address field type in <http://192.168.1.1>.



Step 2. When prompted type in the Username and Password then click on the “Log In” button. If you have not changed the password for the modem administration, the factory settings are:

Username: admin
Password: admin

Step 3. After logging in you will be presented with the modem’s configuration pages. Click on [SETUP] > [WAN SETUP]. Under WAN section please make sure you have “Firewall” option enabled:



Step 4. Click on [ADVANCED] > [INBOUND FILTER].

Create a new filter:

Type in Filter Name (e.g. "Inbound")

Use Interface: ALL

Protocol: TCP/UDP

You can leave all other fields blank. Click on APPLY.

Product: DSL-2880AL Firmware Version: AU_1.01

The screenshot shows the D-Link DSL-2880AL web interface. At the top, the product name 'DSL-2880AL' and firmware version 'AU_1.01' are displayed. The main navigation bar includes 'SETUP', 'ADVANCED' (highlighted with a red box), 'MAINTENANCE', 'STATUS', and 'HELP'. On the left sidebar, 'Inbound Filter' is selected and highlighted with a red box. The main content area is titled 'INBOUND IP FILTER' and contains a note: 'Note: This section only applies when the Firewall is enabled.' Below the note, there is a section for 'ADD INBOUND IP FILTER' with the following fields: 'Filter Name' (Inbound), 'Use Interface' (ALL), 'IP Version' (IPv4), 'Protocol' (TCP/UDP), 'Source IP address', 'Source Subnet Mask', 'Source Port (port or port:port)', 'Destination IP address', 'Destination Subnet Mask', 'Destination Port (port or port:port)', and 'Schedule' (Always). The 'Apply' button is highlighted with a red box. On the right side, there is a 'Helpful Hints...' section with instructions on naming rules and selecting interfaces.

INBOUND IP FILTER

Note: This section only applies when the Firewall is enabled.

By default, all incoming IP traffic that does not originate from the internal network is blocked when the firewall is enabled. Normal outgoing Internet requests created by web browsing, email and other software you run will work as usual as the requests originate from inside your internal network.

The Inbound Filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

ADD INBOUND IP FILTER

Filter Name: Inbound

Use Interface: ALL

IP Version: IPv4

Protocol: TCP/UDP

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Schedule: Always [View Available Schedules](#)

Apply

ACTIVE INBOUND IP FILTER

Helpful Hints...

Give each rule a Name that is meaningful to you.

Each rule can Allow access from the WAN.

The Source IP addresses are WAN-side address and the Destination IP address are LAN-side address.

Click the Save button to store a finished rule in the Rules List.

Click the Remove checkbox in the Rules List then click on the Remove button to permanently remove a rule.

More...

Step 5. Click on [ADVANCED] > [PORT FORWARDING]. Enter the rule details. We are using opening port for Remote Desktop service as an example:

- Name: type in a name for this rule (e.g. "RDP")
- IP Address: type in the IP address of the device you are opening ports for (PC, Xbox, PlayStation, etc.)

Enter port number for TCP or UDP or both:

- Internal Port: the port you are opening
- External Port: the port you are opening

Click on APPLY when finished.

Product: DSL-2880AL Firmware Version: AU_1.01

D-Link

DSL-2880AL // **SETUP** **ADVANCED** MAINTENANCE STATUS HELP

Port Forwarding

Application Rules
QoS Setup
Outbound Filter
Inbound Filter
Wireless Filter
DNS Setup
Firewall & DMZ
Advanced ADSL
Advanced Wireless
Advanced LAN
Port Mapping
SNMP Setup
Parental Control
Routing Setup
Wi-Fi Protected Setup
IPv6 Firewall
IPv6 Routing
Budget Quota
Logout

PORT FORWARDING

This is the ability to open ports in your router and re-direct data through those ports to a single PC on your network.

PORT FORWARDING RULES CONFIGURATION

Remaining number of rules that can be created: 46

		External Port	Internal Port
Name	<< Application Name >>	TCP	TCP
RDP		3389	3389
IP Address	<< Computer Name >>	UDP	UDP
192.168.1.2			
Use Interface:	PPPoE_8_35_1_1/ppp0.0		

ACTIVE PORT FORWARDING RULES

Name	Address	External Port	Internal Port	Protocol	WAN Interface	Edit	Remove
RDP	192.168.1.2	3389	3389	TCP	ppp0.0	Edit	<input type="checkbox"/>

Helpful Hints...

A Virtual Server is defined as service port. All requests to this port of your external IP address are forwarded to a certain internal IP address, e.g. requests via FTP oder POP3.

[More...](#)