

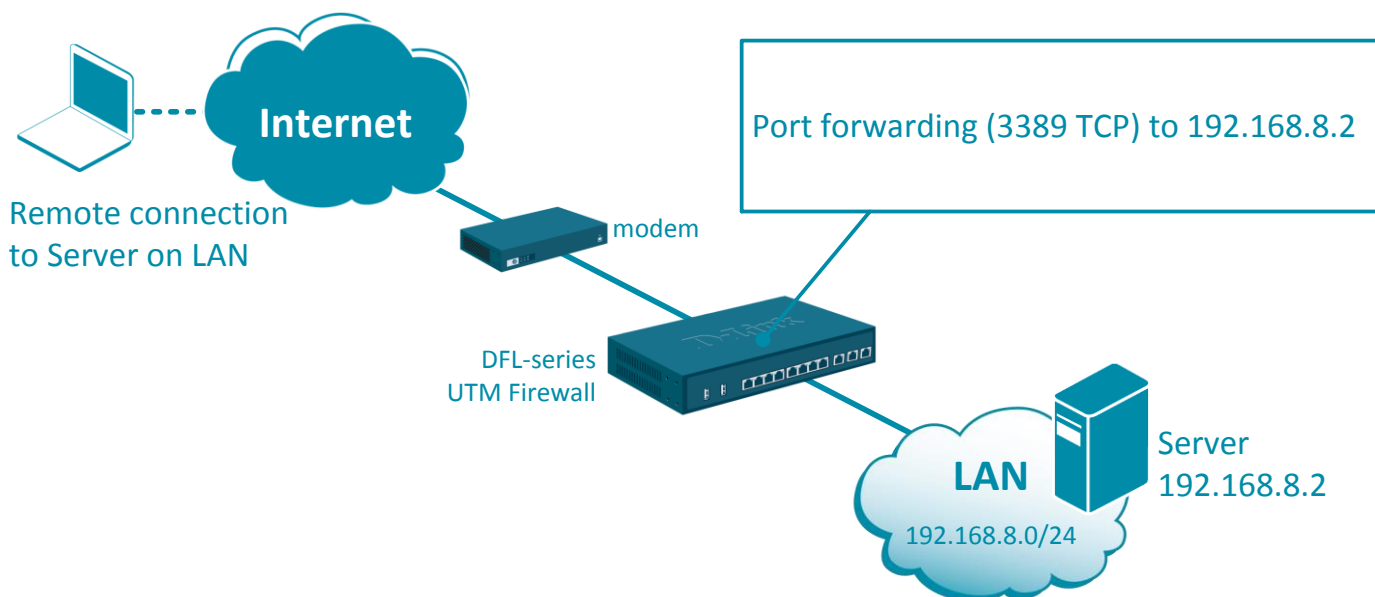
NETDEFEND

Configuration examples for the D-Link NetDefend Firewall series



How to setup port forwarding from WAN to LAN

This configuration example is based on the following setup:



Step 1. Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is "admin" and password is "admin".

Step 2. Go to Objects > Address Book. Add a new object: the private IP of the RDP Server.

The screenshot shows the D-Link firewall web interface. The "Objects" tab is selected. In the left sidebar, "Address Book" is expanded. The "Address Book" page shows a list of objects, with "IP4 Address" selected. A red arrow points to the "IP4 Address" option in the list. A modal window titled "IP4 Address" is open, showing the configuration details. The "Name" field is "RDP_Server", the "Address" field is "192.168.8.2", and the "Comments" field is "My RDP Server on LAN".

Step 3. Go to Objects > Services. Check if the port/service you require to open is already in the list. If not - add a new TCP/UDP Service. In our example it is Remote_Desktop with port 3389 TCP.

The screenshot shows the D-Link web interface with the 'Objects' tab selected. The 'Services' section is active, displaying a list of services. A red arrow points from the '+ Add' dropdown menu to the 'TCP/UDP Service' option. The configuration window for 'TCP/UDP Service' is open, showing the following fields:

- Name: Remote_Desktop
- Type: TCP
- Source: 0-65535
- Destination: 3389

A red box highlights the Name, Type, and Destination fields. A red arrow points from the 'TCP/UDP Service' menu item to the configuration window.

Step 4. Go to IP Rules.

Add a rule for Remote_Desktop traffic with action "SAT".

Set Source Interface/Network as "Any/All-nets".

Set Destination Interface/Network as "Core/WAN IP".

The screenshot shows the 'Policies' tab in the D-Link firewall configuration interface. The 'Main IP Rules' section is active, and the 'IP Rule' configuration window is open. The 'IP Rule' configuration includes the following fields:

- Name:** RDP_SAT
- Action:** SAT
- Service:** Remote_Desktop
- Schedule:** (None)
- Address Filter:**
 - Source:** Interface: wan1, Network: all-nets
 - Destination:** Interface: core, Network: wan1_ip

Click on the SAT tab. Specify the Destination IP Address (the RDP Server).

The screenshot shows the 'SAT' configuration page in the D-Link firewall configuration interface. The 'SAT' tab is selected. The configuration includes the following fields:

- Translate the:**
 - Source IP
 - Destination IP
- to:**
- New IP Address:** RDP_Server
- New Port:** (empty field)
- All-to-One Mapping:** rewrite all destination IPs to a single IP

Step 5. The SAT rule needs to be followed by an ALLOW rule.

Add an ALLOW rule to allow RDP traffic to go through (use the same parameters as the SAT rule. In fact you can CLONE the SAT rule and change Action to "Allow").

IP Rule

An IP rule specifies what action to perform on network traffic that m

General Log Settings NAT SAT Multip

Name: RDP_ALLOW

Action: **Allow** ⓘ NAT, SAT, SLB SAT an

Service: Remote_Desktop

Schedule: (None)

Address Filter

Specify source interface and source network, together with destin

Source: Interface: any Network: all-nets

Destination: core wan1_ip

If necessary rearrange the order of the IP rules so that the SAT rule is followed by the ALLOW rule:

Main IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translati

+ Add

| # | Name | Log | Src If | Src Net | Dest If | Dest Net | Service |
|---|-------------|-----|--------|----------|---------|----------|--------------|
| 1 | ▶ ping_fw | | lan | lanet | core | lan_ip | ping-inbound |
| 2 | lan_to_wan1 | | | | | | |
| 3 | ▶ RDP_SAT | | any | all-nets | core | wan1_ip | Remote_Des |
| 4 | ▶ RDP_ALLOW | | any | all-nets | core | wan1_ip | Remote_Des |

Step 6. After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.

