

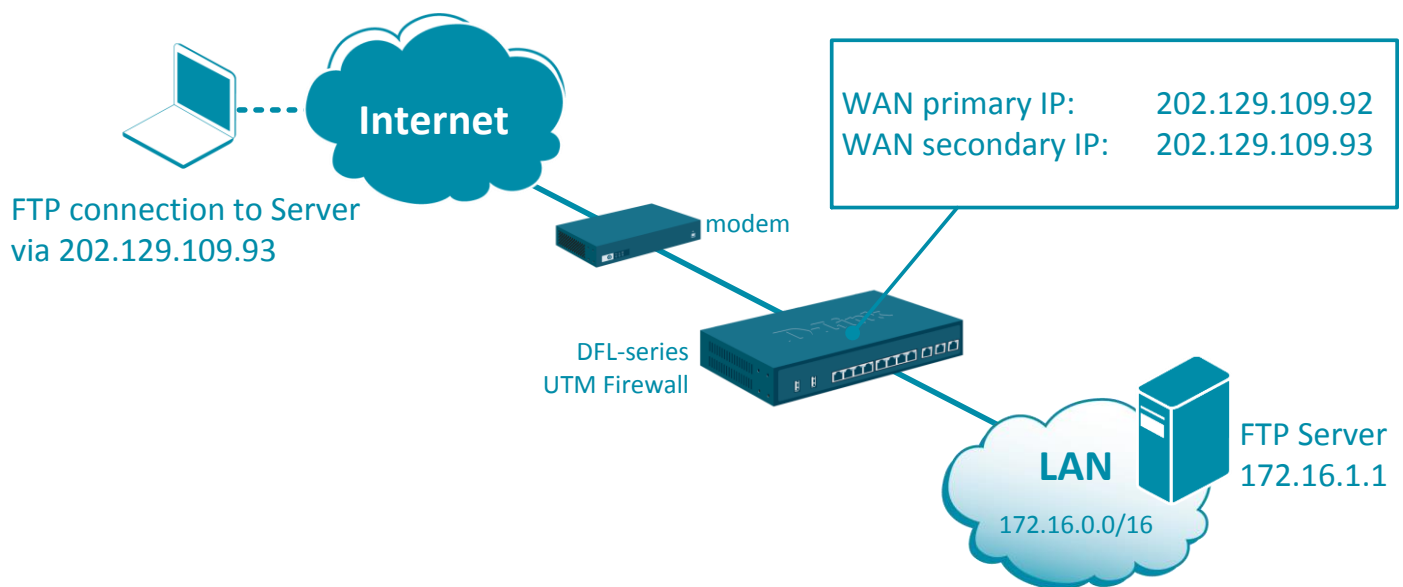
NETDEFEND

Configuration examples for the D-Link NetDefend Firewall series



Adding additional IP addresses to WAN interface

This configuration example is based on the following setup:



FTP connection to Server via 202.129.109.93

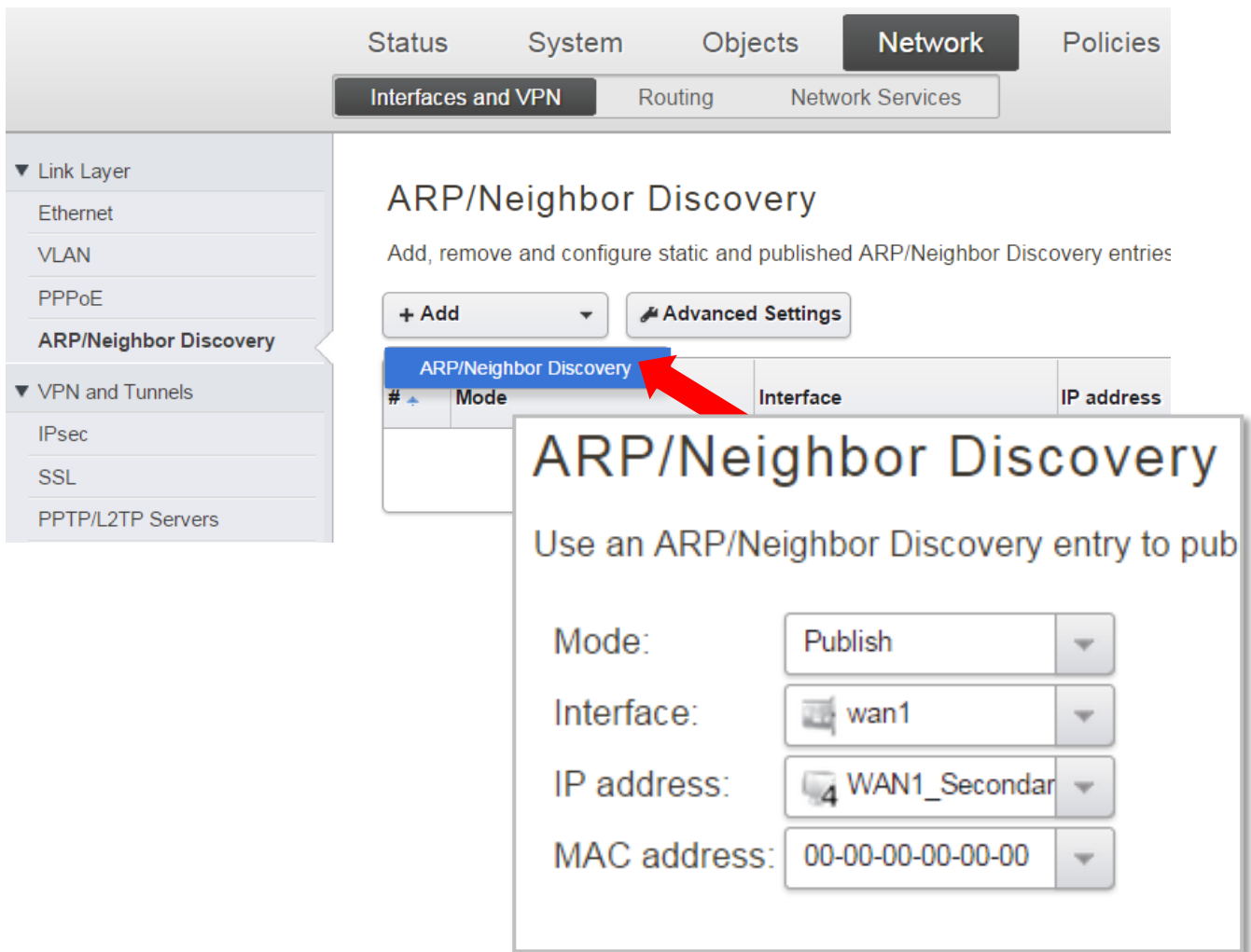
Step 1. Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is “admin” and password is “admin”.

Step 2. Go to Objects > Address Book > Interface Addresses. Add two new objects: Secondary WAN IP and the IP address of the FTP Server.

The screenshot shows the 'Objects' tab in the D-Link firewall web interface. The left sidebar shows the navigation menu with 'Address Book' selected. The main area displays the 'Address Book' configuration page. A red arrow points to the 'IP4 Address' option in the 'Add' dropdown menu. Two 'IP4 Address' configuration windows are shown. The first window is for 'WAN1_Secondary_IP' with the address '202.129.109.93'. The second window is for 'FTP_Server' with the address '172.16.1.1'. Both windows have 'General' and 'User Authentication' tabs, with 'General' selected.

Step 3. Go to Network > Interfaces and VPN > ARP/Neighbor Discovery.

Add a new entry to publish the secondary Public IP Address on WAN.



The screenshot shows the D-Link web interface with the following structure:

- Top navigation: Status, System, Objects, **Network**, Policies
- Sub-navigation: **Interfaces and VPN**, Routing, Network Services
- Left sidebar: Link Layer (Ethernet, VLAN, PPPoE, **ARP/Neighbor Discovery**), VPN and Tunnels (IPsec, SSL, PPTP/L2TP Servers)
- Main content area: ARP/Neighbor Discovery

ARP/Neighbor Discovery

Add, remove and configure static and published ARP/Neighbor Discovery entries

+ Add [dropdown] [Advanced Settings]

#	Mode	Interface	IP address

ARP/Neighbor Discovery

Use an ARP/Neighbor Discovery entry to pub

Mode: [Publish] [dropdown]

Interface: [wan1] [dropdown]

IP address: [WAN1_Secondar] [dropdown]

MAC address: [00-00-00-00-00-00] [dropdown]

Step 4. If you need to add port forwarding rules for the secondary IP address on WAN:

Go to Policies > Main IP Rules. Create a new SAT rule for incoming FTP traffic.

Note that the Destination Interface is WAN (not Core) and the Destination Network is the WAN Secondary IP address.

The screenshot shows the configuration page for a rule named 'FTP_SAT'. The 'General' tab is selected. The rule name is 'FTP_SAT', the action is 'SAT', the service is 'ftp-inbound', and the schedule is '(None)'. An information icon indicates that NAT, SAT, and SLB services are supported. The 'Address Filter' section is partially visible, showing source and destination settings.

FTP_SAT

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

General Log Settings NAT SAT M

Name:

Action: ⓘ NAT, SAT, SLB SA

Service:

Schedule:

Address Filter

Specify source interface and source network, together with de

Source: Interface Network

Destination:

Click on the SAT tab and select the server you want to forward the traffic to.

The screenshot shows the configuration page for the 'FTP_SAT' rule, with the 'SAT' tab selected. The 'General' tab is also visible. The 'Translate the' section has 'Destination IP' selected. The 'New IP Address' is set to 'FTP_Server'. The 'New Port' field is empty. An information icon indicates that the port value may only range without gaps. The 'All-to-One Mapping' checkbox is unchecked.

General Log Settings NAT **SAT** Multiplex

Translate the

Source IP

Destination IP

to:

New IP Address:

New Port:

ⓘ This value may only range without gaps

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 FTP 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").

FTP_ALLOW
An IP rule specifies what action to perform on network traffic

General Log Settings NAT SAT

Name:

Action: ⓘ NAT, SAT, SLB SA

Service:

Schedule:

Address Filter
Specify source interface and source network, together with c

Source: Interface Network

Destination:

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

3	▶ FTP_SAT	✓	any	all-nets	wan1	WAN1_Secor	ftp-inbound
4	▶ FTP_ALLOW	✓	any	all-nets	wan1	WAN1_Secondar	ftp-inbound

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.

