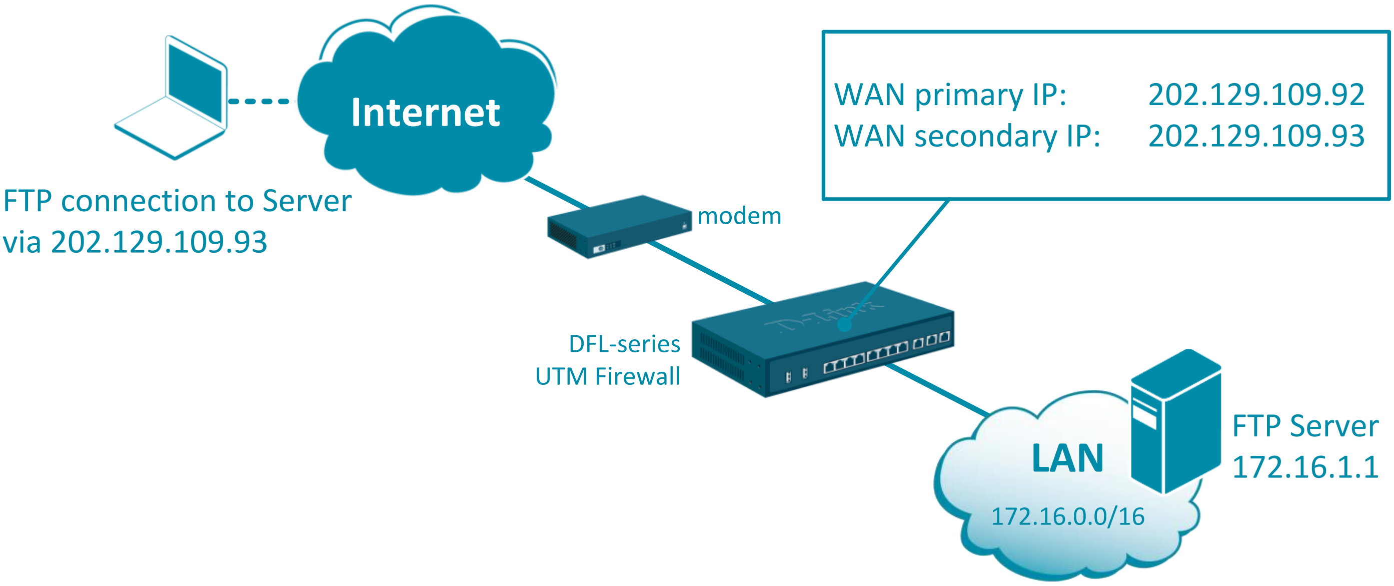
Configuration examples for the D-Link NetDefend Firewall series

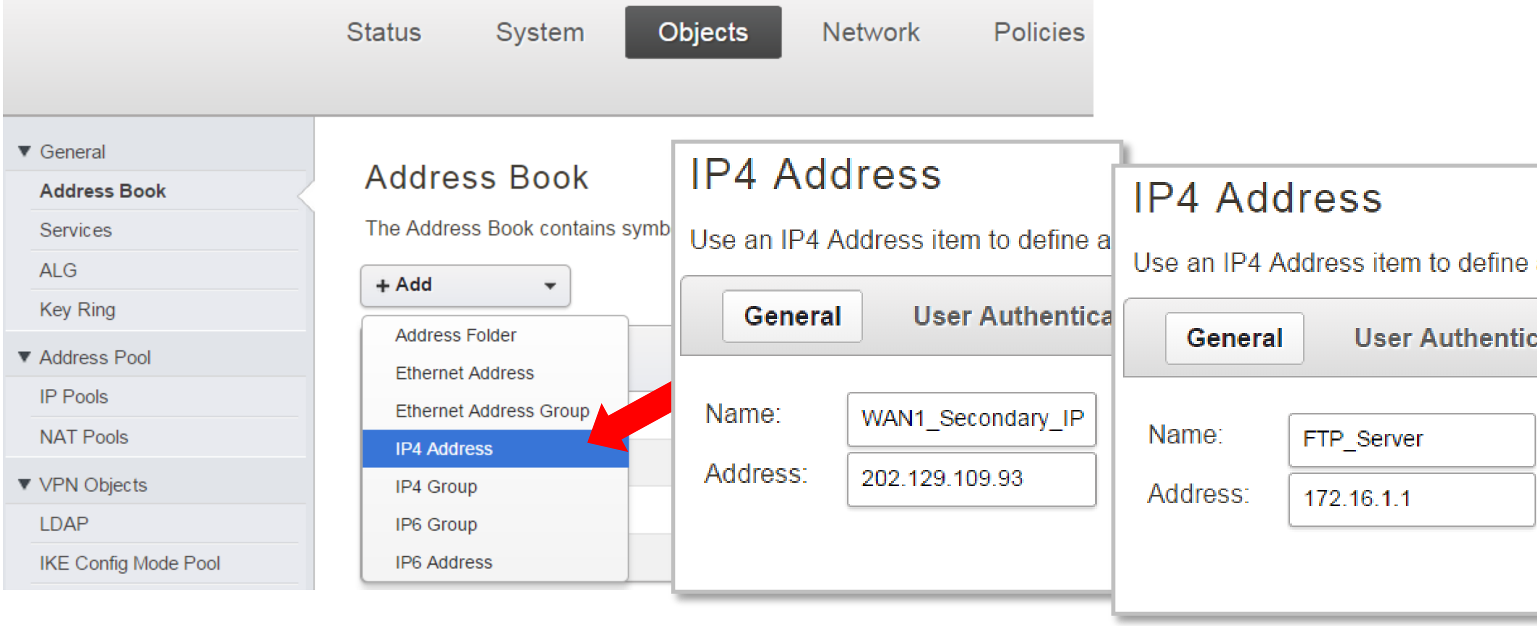
Adding additional IP addresses to WAN interface

This configuration example is based on the following setup:


Internet
WAN primary IP: 202.129.109.92
WAN secondary IP: 202.129.109.93
FTP connection to Server via 202.129.109.93
modem
DFL-series UTM Firewall
LAN
172.16.0.0/16
FTP Server 172.16.1.1

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".

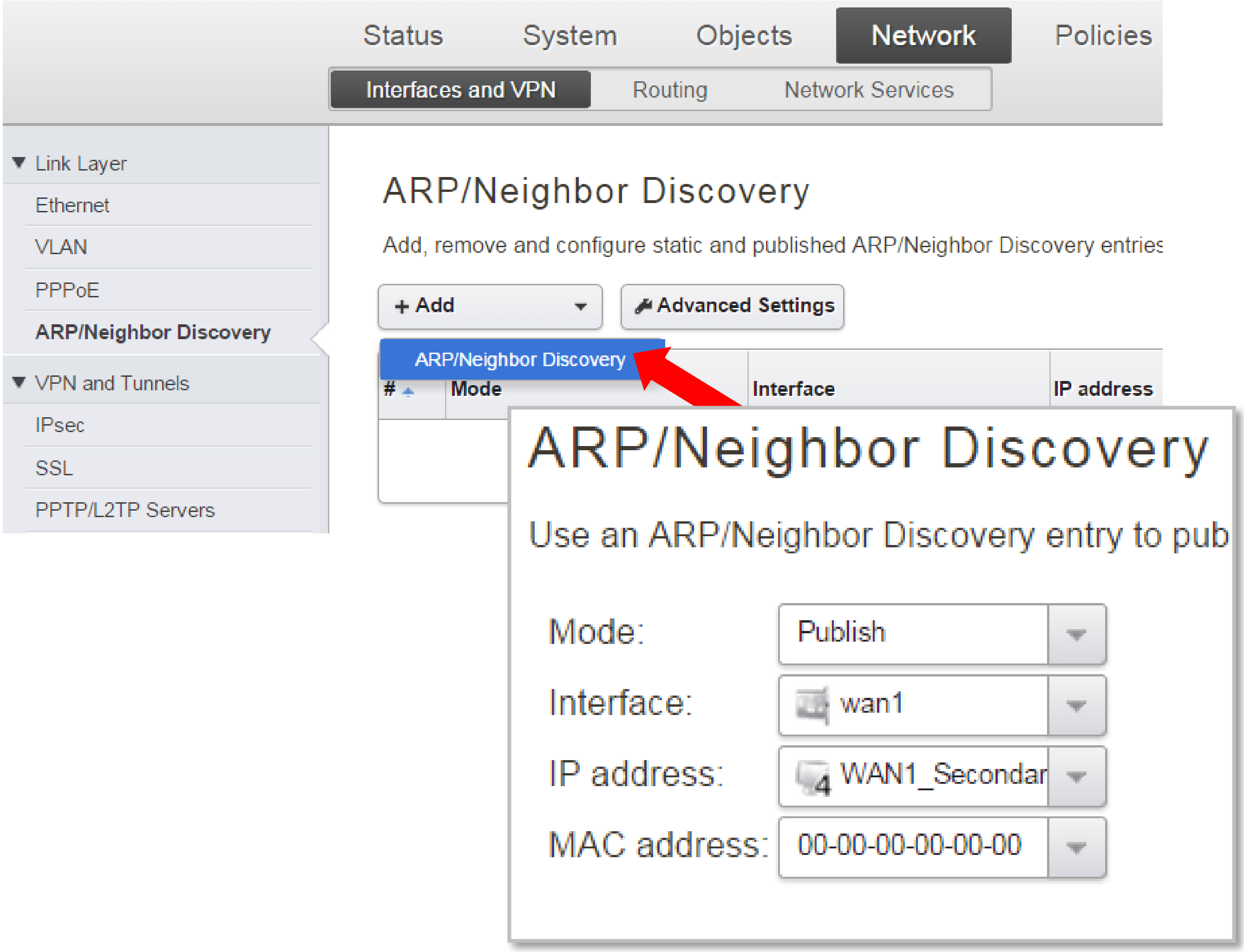
Step 2. Go to Objects > Address Book > Interface Addresses. Add two new objects: Secondary WAN IP and the IP address of the FTP Server.



Name: WAN1_Secondary_IP
Address: 202.129.109.93

Name: FTP_Server
Address: 172.16.1.1

Step 3. Go to Network > Interfaces and VPN > ARP/Neighbor Discovery.
Add a new entry to publish the secondary Public IP Address on WAN.



ARP/Neighbor Discovery

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

ARP/Neighbor Discovery

Use an ARP/Neighbor Discovery entry to pub

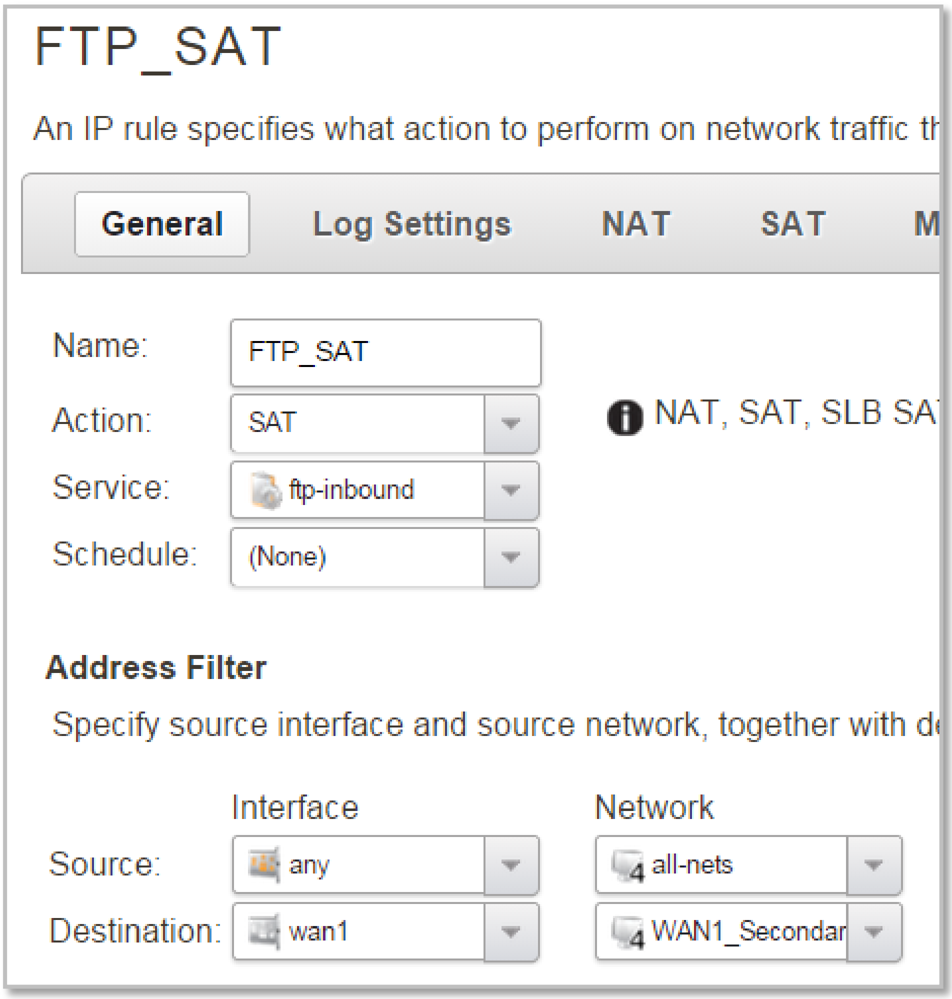
Mode: Publish

Interface: wan1

IP address: WAN1_Secondar

MAC address: 00-00-00-00-00-00

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.



FTP_SAT

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

Name: FTP_SAT

Action: SAT

Service: ftp-inbound

Schedule: (None)

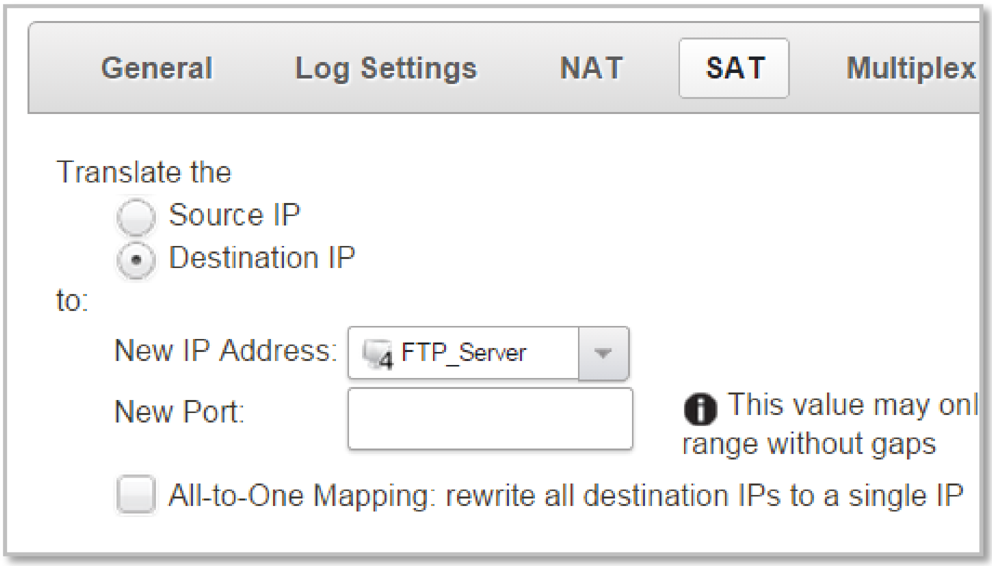
ⓘ NAT, SAT, SLB SA

Address Filter

Specify source interface and source network, together with d

	Interface	Network
Source:	any	all-nets
Destination:	wan1	WAN1_Secondar

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



Translate the
○ Source IP
● Destination IP
to:

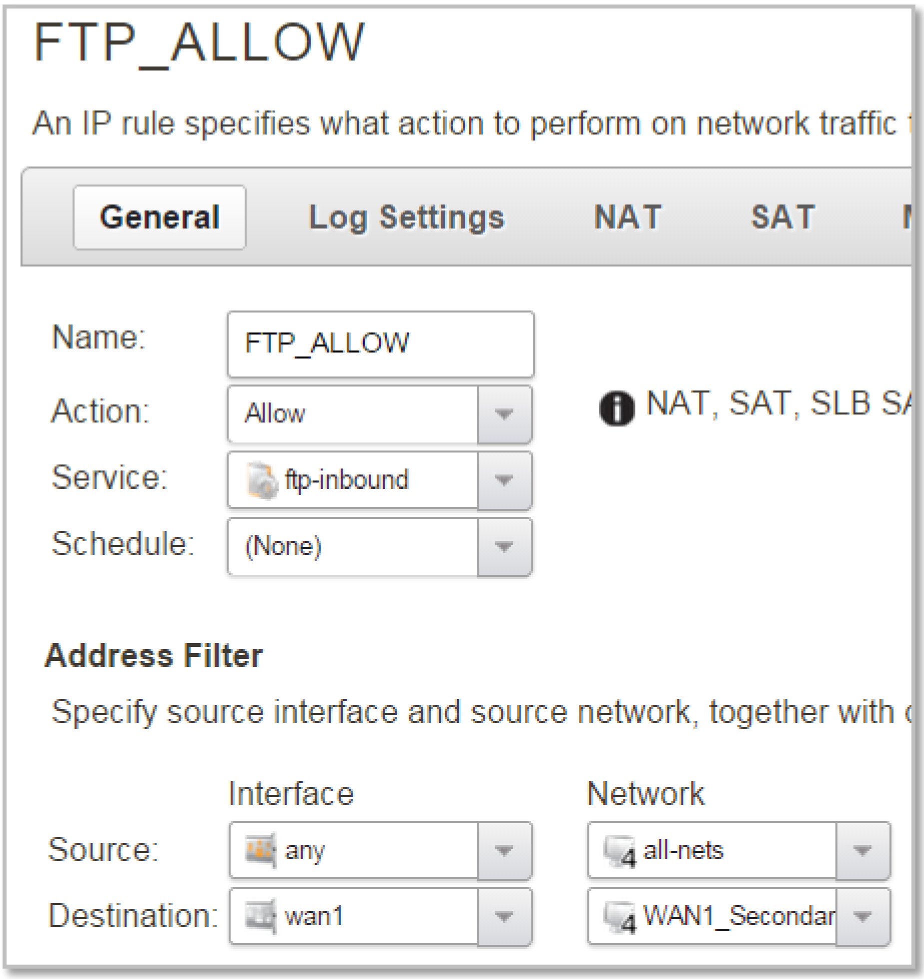
New IP Address: FTP_Server

New Port:

ⓘ This value may onl 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 t

Name: FTP_ALLOW

Action: Allow

Service: ftp-inbound

Schedule: (None)

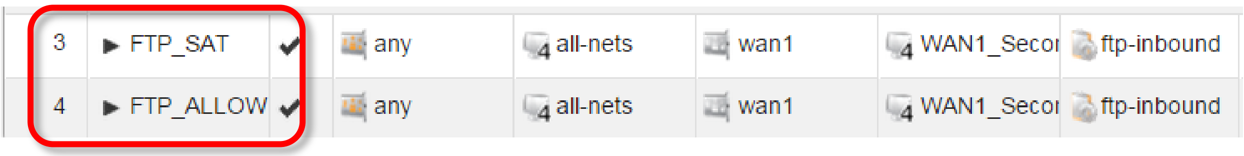
NAT, SAT, SLB SA

Address Filter

Specify source interface and source network, together with d

	Interface	Network
Source:	any	all-nets
Destination:	wan1	WAN1_Secondar

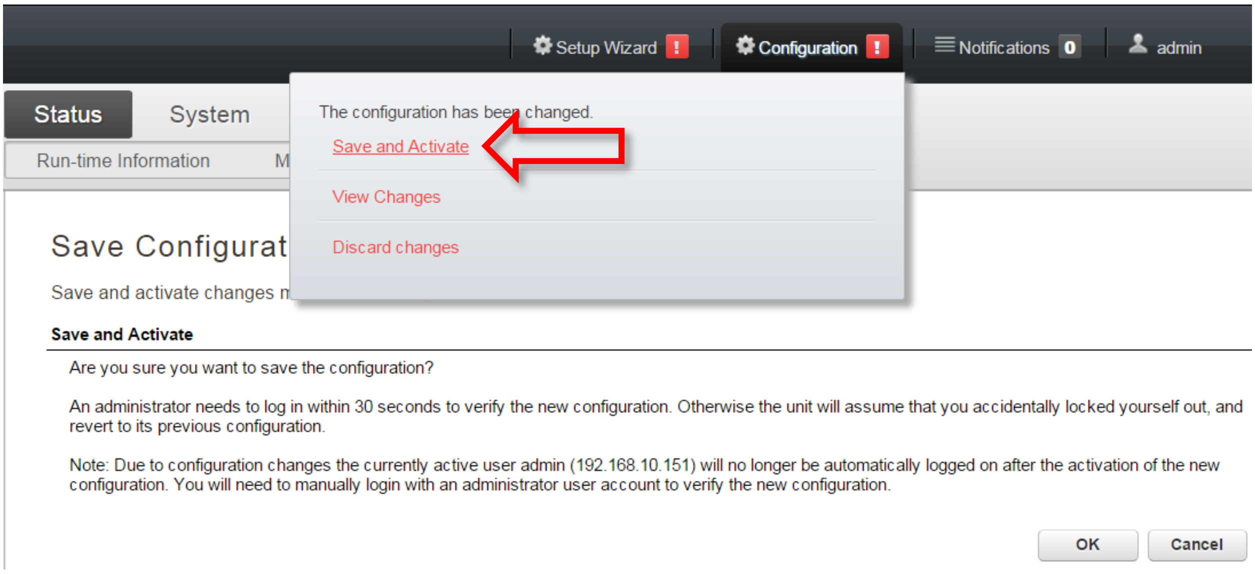
If necessary rearrange the order of the IP rules so that the SAT rule is followed by the ALLOW rule:



3	▶ FTP_SAT	✓	any	all-nets	wan1	WAN1_Secoı	ftp-inbound
4	▶ FTP_ALLOW	✓	any	all-nets	wan1	WAN1_Secoı	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.



The configuration has been changed.

Save and Activate

Are you sure you want to save the configuration?

An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Note: Due to configuration changes the currently active user admin (192.168.10.151) will no longer be automatically logged on after the activation of the new configuration. You will need to manually login with an administrator user account to verify the new configuration.