



Configuration Examples for the D-Link NetDefend Firewall Series

Scenario: How to configure DNS Relay

Platform Compatibility: All NetDefend Firewall Series

Last update: 2008-03-07

Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

The screenshots in this document is from firmware version 2.20.00. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

How to configure DNS Relay

This example describes about firewalls support to relay DNS query packets from LAN to Internet for domain name resolving. All DFL firewalls (DFL-210/800/1600/2500) support this feature from firmware v2.04 and later.

Note: About this feature, it performs relay/forward DNS packets only since D-Link DFL firewalls don't built-in DNS server in system kernel. Therefore, it can not instead of real DNS server to provide domain name resolving and related functionality.

Details:

- LAN IP on firewall: 192.168.1.1 (with the function of DNS relay)
- Lannet on firewall: 192.168.1.0/24
- DNS Server on Internet: 12.0.0.1

1. Addresses

Go to *Objects -> Address book -> InterfaceAddresses*

Create an IP Address called dns_server with address 12.0.0.1

Click Ok.

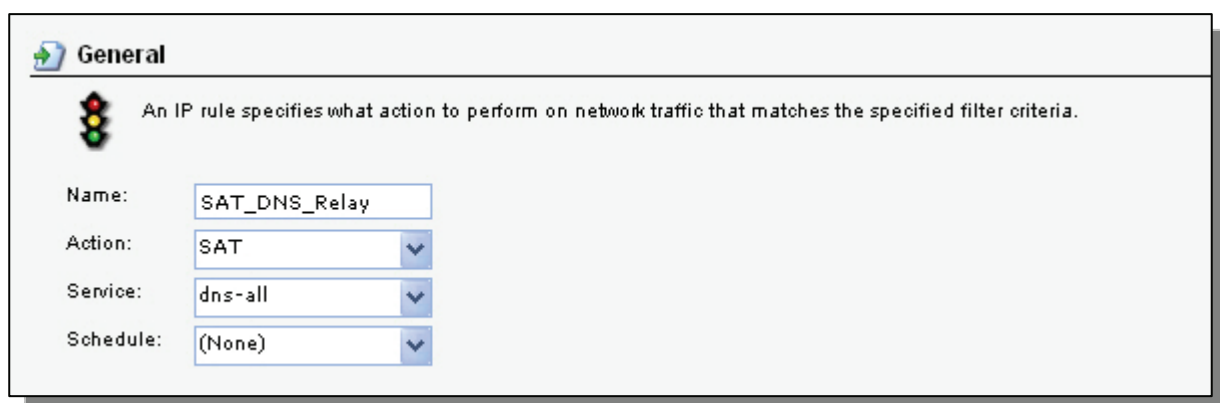
2. Create IP Rules to redirect DNS packets to Internet

Go to *Rules -> IP Rules*


Create a new IP Rule with SAT action.

In the **General** tab:

General:



General

 An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

Name:

Action:

Service:

Schedule:

Name: **SAT_DNS_Relay**

Action: **SAT**

Service: **dns_all**

Address Filter:

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters are required to match the rule to match.

Interface: Source: lan Destination: core

Network: lannet lan_ip

Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **core**
Destination Network: **lan_ip**

In the SAT tab:

General:

IP Rule

General Log Settings NAT SAT SAT Server Load Balancing

General

Translate the

Source IP Address

Destination IP Address

To:

New IP Address: dns_server

New Port: This value may only be applied on TCP/UDP services with port set to a single number or a port range without gaps

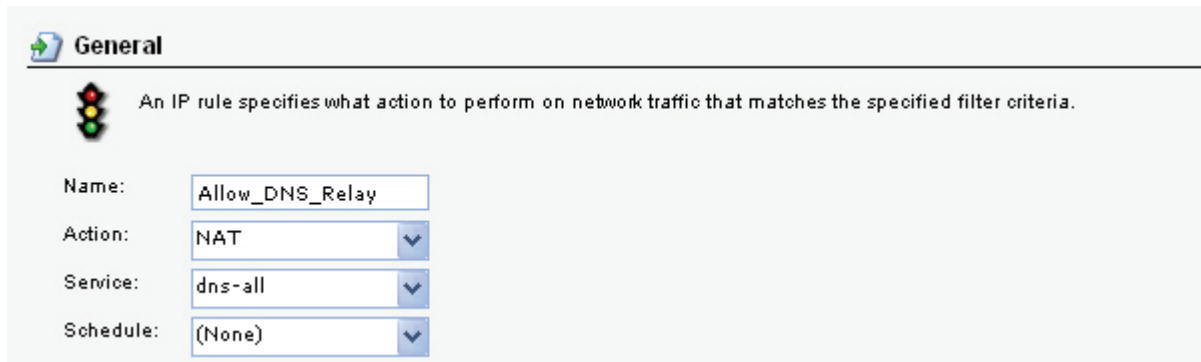
All-to-One Mapping: rewrite all destination IPs to a single IP

Translate the: **Destination IP Address**
New IP Address: **dns_server**

Click Ok.

Create an identical IP Rule with NAT action. If the environment is not NAT, create a ALLOW rule instead.

In the General tab:



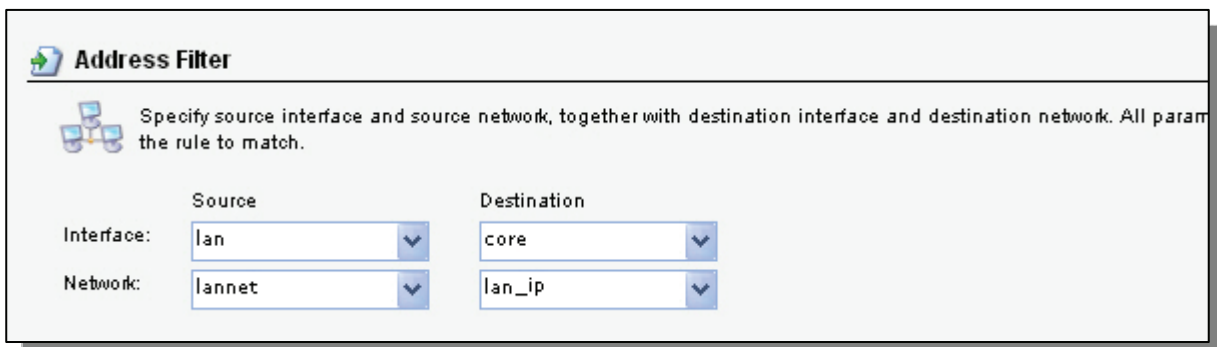
The screenshot shows the 'General' tab of an IP rule configuration. It features a traffic light icon and a descriptive text: 'An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.' Below this, there are four fields: 'Name' with the value 'Allow_DNS_Relay', 'Action' with a dropdown menu set to 'NAT', 'Service' with a dropdown menu set to 'dns-all', and 'Schedule' with a dropdown menu set to '(None)'.

Name: **Allow_DNS_Relay**

Action: **NAT**

Service: **dns_all**

Address Filter:



The screenshot shows the 'Address Filter' tab of an IP rule configuration. It features a network diagram icon and a descriptive text: 'Specify source interface and source network, together with destination interface and destination network. All parameters must be specified for the rule to match.' Below this, there are four fields arranged in a 2x2 grid. The top row is labeled 'Interface' and the bottom row is labeled 'Network'. The left column is labeled 'Source' and the right column is labeled 'Destination'. The values are: Source Interface: 'lan', Source Network: 'lannet', Destination Interface: 'core', and Destination Network: 'lan_ip'.

Source Interface: **lan**

Source Network: **lannet**

Destination Interface: **core**

Destination Network: **lan_ip**

Click Ok.

Make sure these two rules are triggered before any generic rules (e.g. allow_standard rules).

And also, configure all PCs to have the firewall lan_ip (192.168.1.1) as DNS server.

Save and activate the configuration on firewall