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
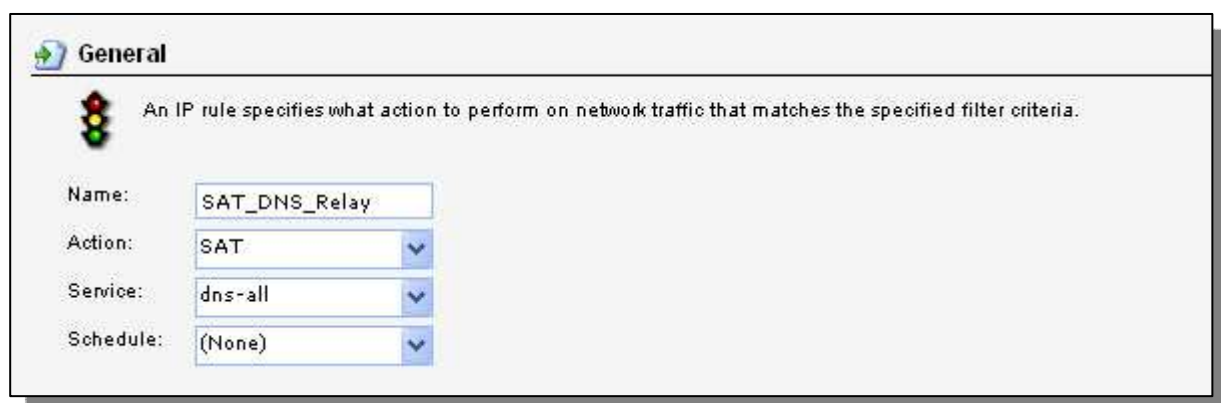
Click **Ok**.

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:
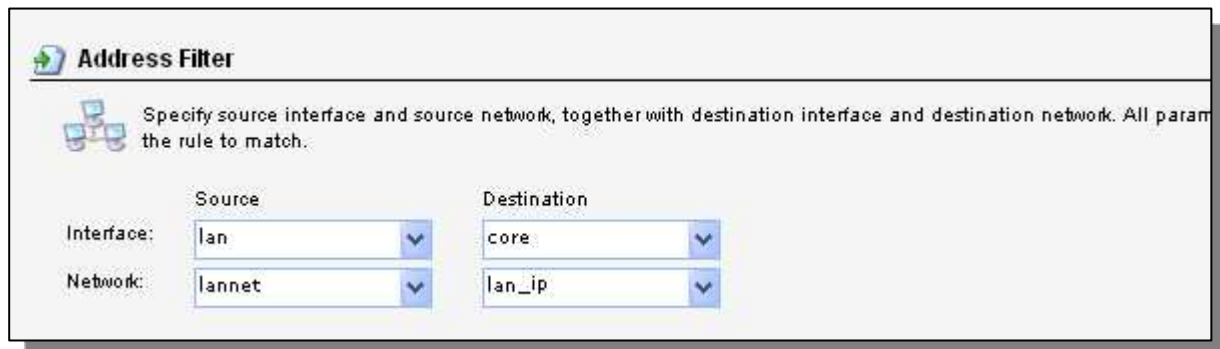
Name: **SAT_DNS_Relay**
Action: **SAT**
Service: **dns_all**
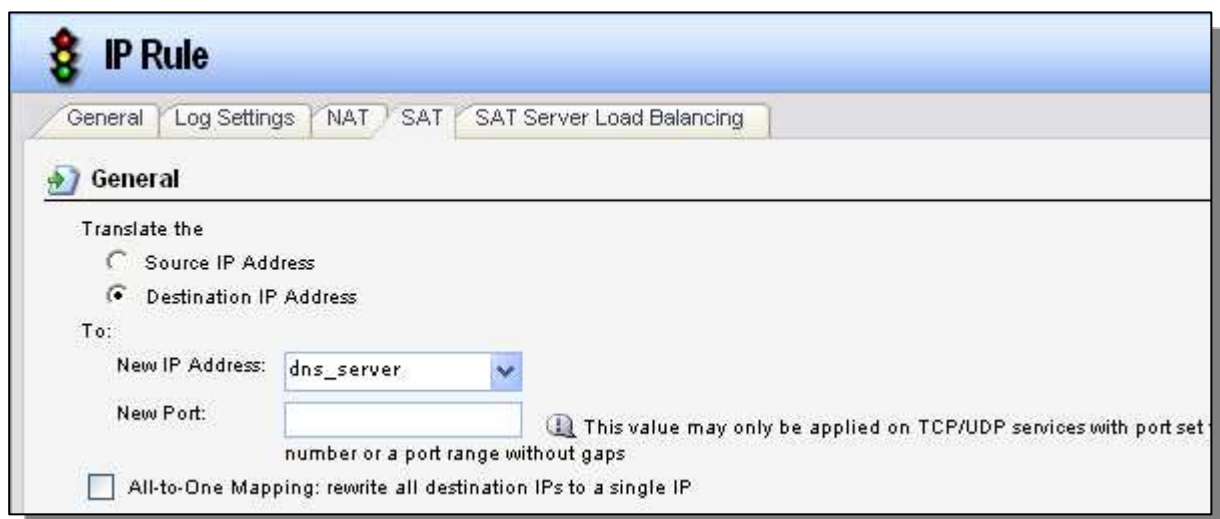
Address Filter:

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

In the SAT tab:

General:

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.
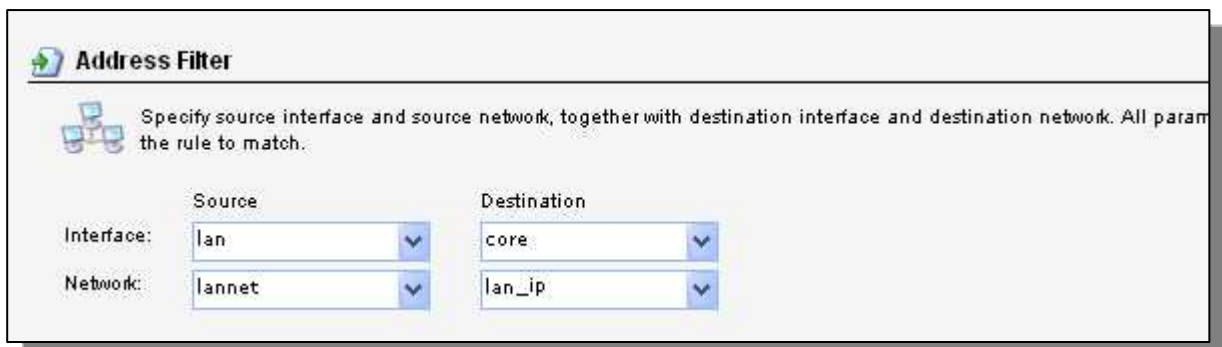
In the **General** tab:

Name: `Allow_DNS_Relay`
Action: `NAT`
Service: `dns_all`

Address Filter:

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