Configuration examples for the D-Link NetDefend Firewall series

DFL-210/800/1600/2500

Scenario: How to configure VLAN and route failover

Last update: 2007-01-31

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 2.11.02. If you are using a later 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 VLAN and route failover

This example requires a DFL-1600 or 2500 to be fully implemented. Most settings can however also be used on a DFL-210 or DFL-800.

Two tag based VLANs will be created on lan3, that connect to switch port with VLAN tag.

Details:
- From lan1, lan2 and lan3: HTTP, HTTPS and DNS connect to Internet via wan2.
- From dmz: inbound and outbound SMTP services connect to Internet via wan1.
- All internal nets can also access the Mail server in dmz.
- Only VLAN2 can access the FTP server in dmz.
- If anyone of the wan interfaces is disconnected, the traffic from that interface will be redirected to the other wan interface.

a IP: 192.168.110.254
NetMask: 255.255.255.0

b IP: 192.168.120.254
Netmask: 255.255.255.0

c IP: 192.168.110.1
Netmask: 255.255.255.0
gateway: 192.168.110.254

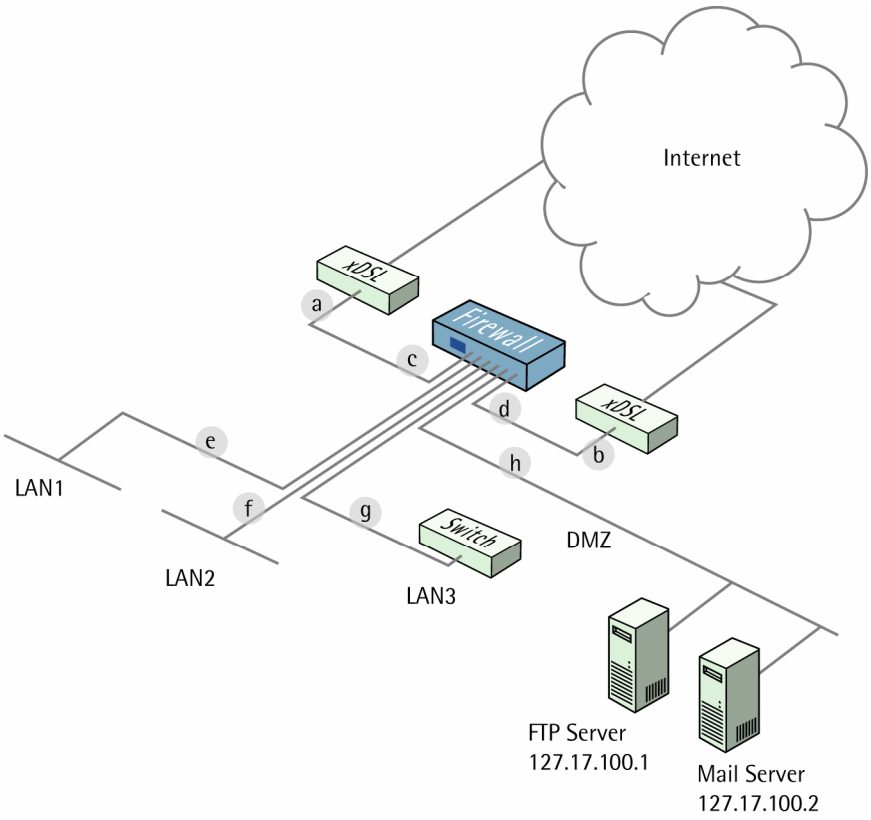
d IP: 192.168.120.1
Netmask: 255.255.255.0
gateway: 192.168.120.254

e IP: 192.168.1.1
Netmask: 255.255.255.0

f IP: 192.168.2.1
Netmask: 255.255.255.0

g VLAN 1 IP: 192.168.5.254
VLAN 2 IP: 192.168.10.254
Netmask: 255.255.255.0

h IP: 172.17.100.254
Netmask: 255.255.255.0



1. Addresses

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

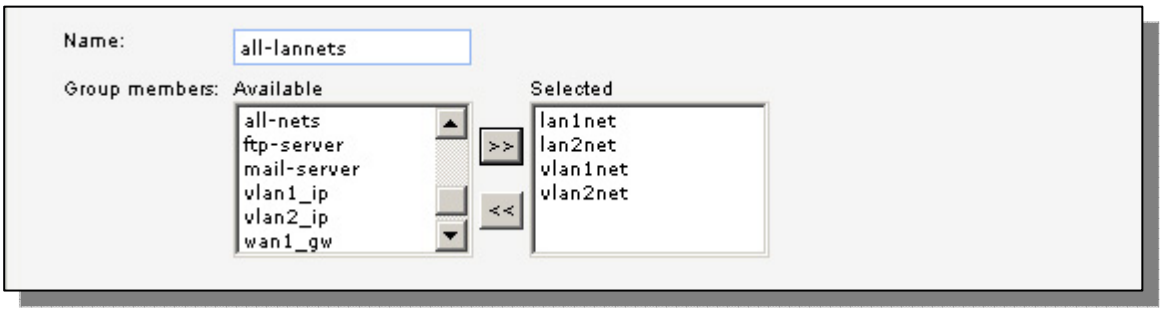
Make sure the configured addresses match the following list, and add the objects that not already exist. To add new objects, select IP address from the add dropdown, enter name and address and click ok.

Name	Address
lan1_ip	192.168.1.1
lan1net	102.168.1.0/24
lan2_ip	192.168.2.1
lan2net	192.168.2.0/24
lan3_ip	192.168.3.1
lan3net	192.168.3.0/24
dmz_ip	172.17.100.254
dmznet	172.17.100.0/24
wan1_ip	192.168.110.1
wan1net	192.168.110.0/24
wan1-gw	192.168.110.254
wan2_ip	192.168.120.1
wan2net	192.168.120.0/24
wan2-gw	192.168.120.254
vlan1_ip	192.168.5.254
vlan1net	192.168.5.0/24
vlan2_ip	192.168.10.254
vlan2net	192.168.10.0/24
ftp-server	172.17.100.1
mail-server	172.17.100.2

Add a new IP4 Group.

In the General tab:

General:



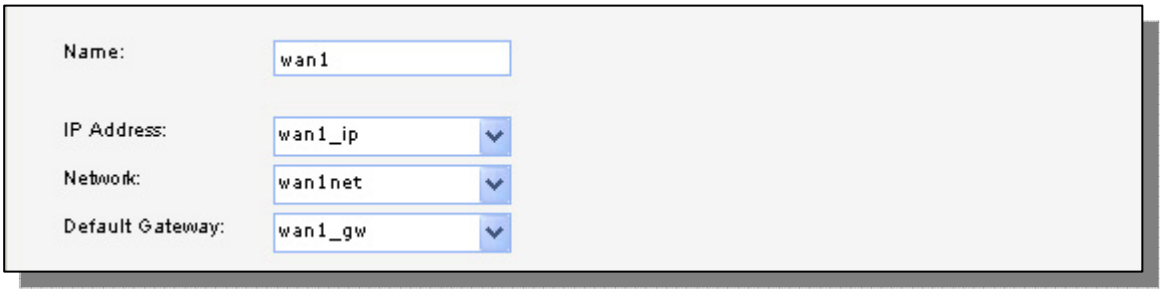
Name: **`all-lannets`**
Add **`lan1net`**, **`lan2net`**, **`vlan1net`** and **`vlan2net`**.

Click Ok.

2. Ethernet interfaces

Go to *Interfaces -> Ethernet*.

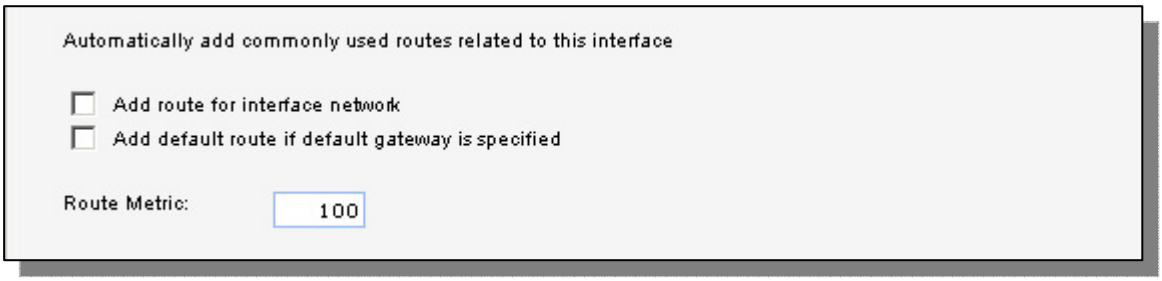
Edit the **wan1** interface to use the following settings.
In the General tab:



IP Address: **wan1_ip**
Network: **wan1net**
Default Gateway: **wan1_gw**

In the Advanced tab:

Automatic Route Creation:



Deselect **Add route for interface network** and **Add default route if default gateway is specified**.

Click Ok.

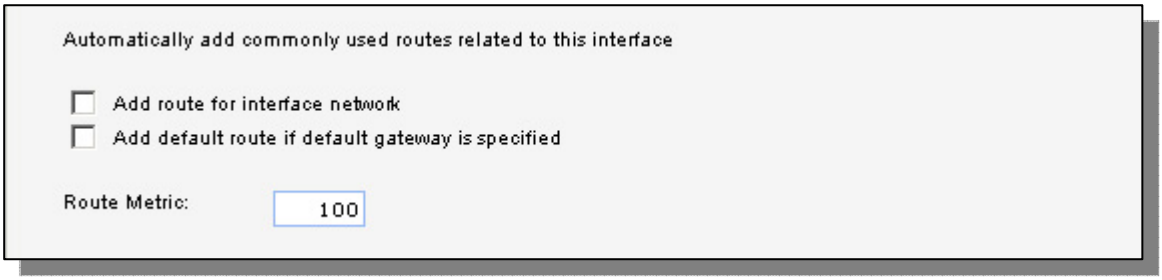
Edit the **wan2** interface according to the following settings.

In the General tab:

General:
IP Address: **wan2_ip**
Network: **wan2net**
Default Gateway: **wan2_gw**

In the Advanced tab:

Automatic Route Creation:



Deselect **`Add route for interface network`** and **`Add default route if default gateway is specified`**.

Click Ok.

3. Routes

Go to *Routing -> Routing Tables*.

Select main routing table and add a new Route. (This route is mainly for WAN1 interface routeing with link status monitoring only)

In the General tab:

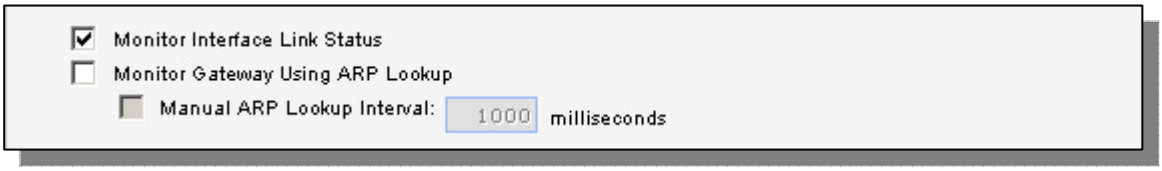
Interface: **`wan1`**
Network: **`wan1net`**
Gateway: **`(None)`**
Local IP Address: **`(None)`**
Metric: **`90`**

In the Monitor tab:

Monitoring for Route Failover:

Select **`Monitor This Route`**

Method:



Select **Monitor Interface Link Status**

Click Ok.

Add a new Route in main routing table. (This route is mainly for WAN1 default route with link status and ARP lookup monitoring)

In the General tab:

General:

Interface: **wan1**
Network: **all-nets**
Gateway: **wan1_gw**
Local IP Address: **(None)**
Metric: **90**

In the Monitor tab:

Monitoring for Route Failover:

Select **Monitor This Route**

Method:

Select **Monitor Interface Link Status**
Select **Monitor Gateway Using ARP Lookup**

Click Ok.

Add a new Route in main routing table. (This route is mainly for WAN2 interface route with link status monitoring only)

In the General tab:

General:
Interface: **wan2**
Network: **wan2net**
Gateway: **(None)**
Local IP Address: **(None)**
Metric: **80**

In the Monitor tab:

Monitoring for Route Failover:
Select **Monitor This Route**

Method:
Select **Monitor Interface Link Status**

Click Ok.

Add a new Route in main routing table. (This route is mainly for WAN2 default route with link status and ARP lookup monitoring)

In the General tab:

General:
Interface: **wan2**
Network: **all-nets**
Gateway: **wan2_gw**
Local IP Address: **(None)**
Metric: **80**

In the Monitor tab:

Monitoring for Route Failover:
Select **Monitor This Route**

Method:
Select **Monitor Interface Link Status**
Select **Monitor Gateway Using ARP Lookup**

Click Ok.

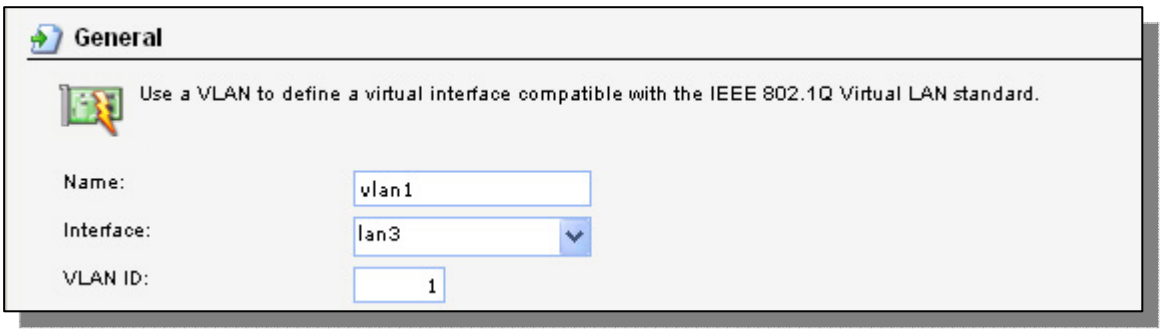
4. VLAN interfaces

Go to *Interfaces -> VLAN*.

Add a new VLAN.

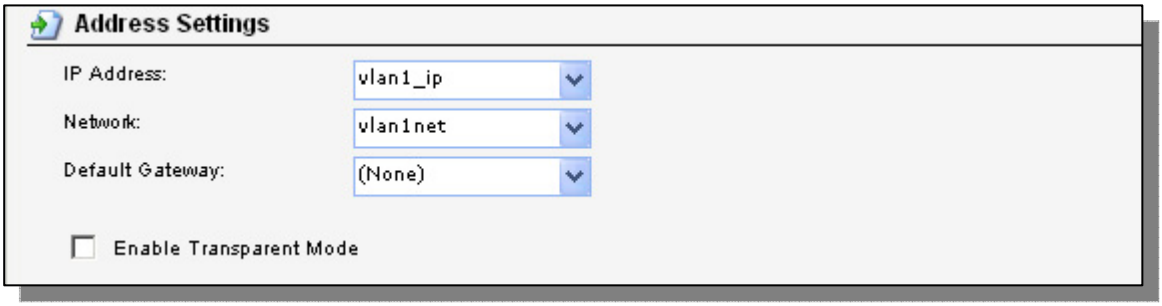
In the General tab:

General:



Name: **vlan1**
Interface: **lan3**
VLAN ID: **1**

Address Settings:

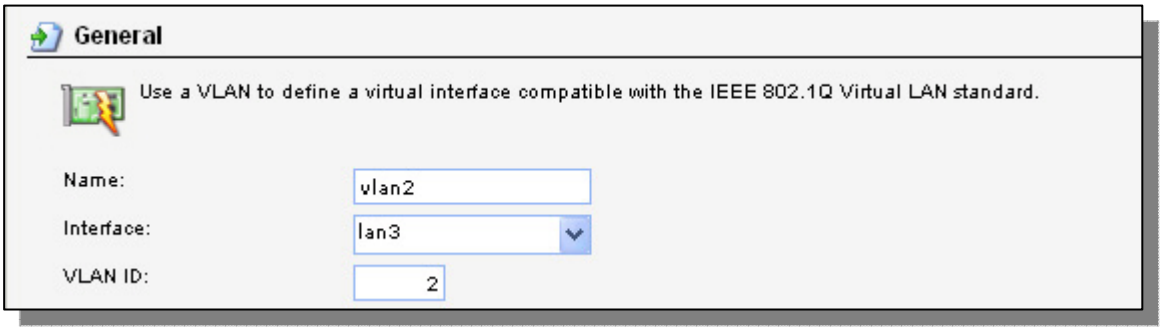


IP Address: **vlan1_ip**
Network: **vlan1net**
Default Gateway: **(None)**

Click Ok
Add a new VLAN.

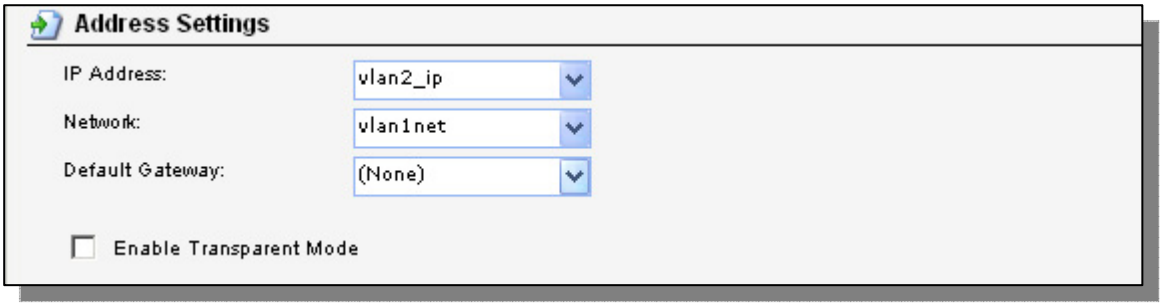
In the General tab:

General:



Name: **vlan2**
Interface: **lan3**
VLAN ID: **2**

Address Settings:



IP Address: **vlan2_ip**
Network: **vlan2net**
Default Gateway: **(None)**

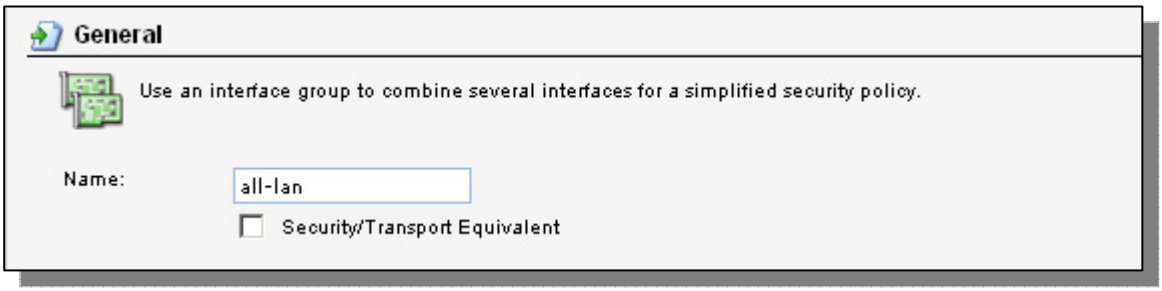
Click Ok

5. Interface groups

Go to *Interfaces -> Interface Groups*.

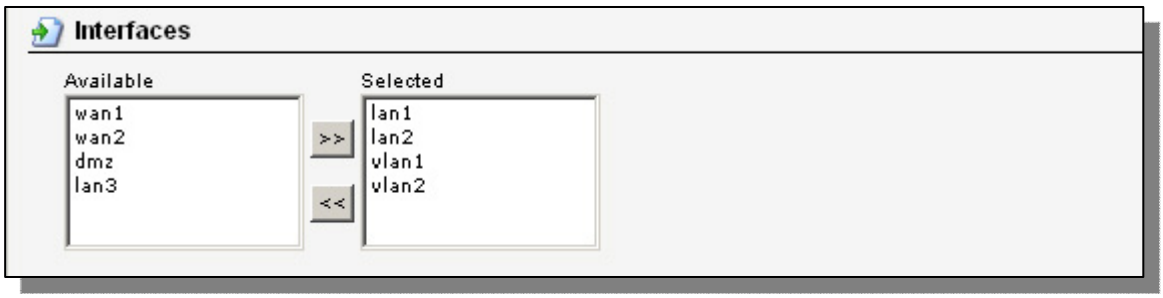
Add a new Interface Group.

General:



Name: **all-lan**

Interfaces:

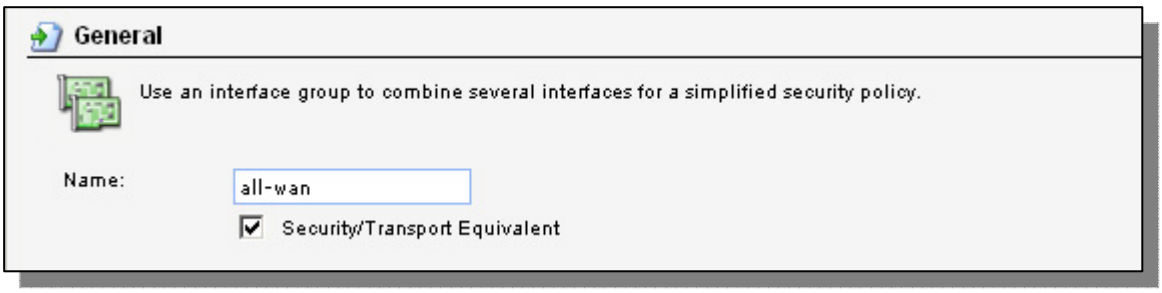


Add **lan1**, **lan2**, **vlan1** and **vlan2** to this group.

Click Ok.

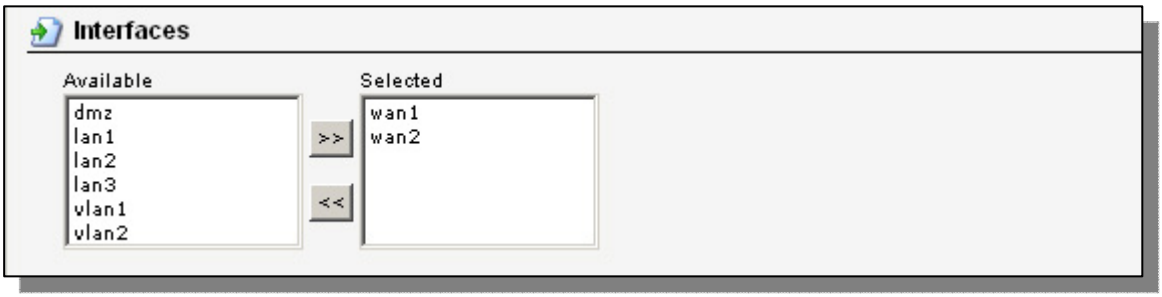
Add a new Interface Group.

General:



Name: **`all-wan`**
Select **`Security/Transport Equivalent`**

Interfaces:



Add **`wan1`** and **`wan2`** to this group.

Click Ok.

6a. Rules to allow HTTP, HTTPS and DNS to Internet

Go to *Rules -> IP Rules*.

Add a new IP Rule Folder called **`all-lan_to_all-wan`**.

In the new folder, add a new IP Rule (to allow outgoing HTTP).

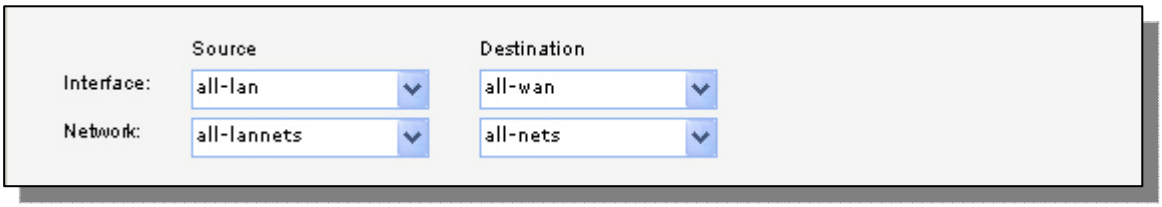
In the General tab:

General:

Name: **`allow-http-all`**

Action: **NAT**
Service: **http-all**

Address Filter:



Source interface: **all-lan**
Source network: **all-lannet**
Destination interface: **all-wan**
Destination network: **all-nets**

Click Ok.

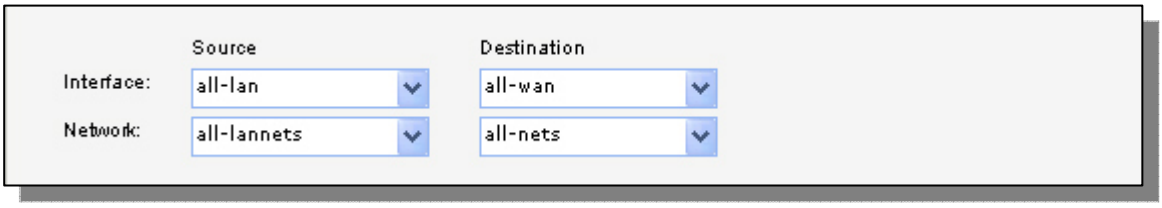
Add a new IP Rule (to allow outgoing dns).

In the General tab:

General:

Name: **allow-dns-all**
Action: **NAT**
Service: **dns-all**

Address Filter:



Source interface: **all-lan**
Source network: **all-lannet**
Destination interface: **all-wan**
Destination network: **all-nets**

Click Ok.

6b. Rules to allow outgoing SMTP from mail server to Internet

Add a new IP Rule folder called **dmz_to_all-wan**.

In the new folder, add a new IP Rule (to allow outgoing smtp).

In the General tab:

General:
Name: **allow-smtp-out**
Action: **NAT**
Service: **smtp**

Address Filter:
Source interface: **dmz**
Source network: **mail-server**
Destination interface: **all-wan**
Destination network: **all-nets**

Click Ok.

6c. Rules to allow Internet and internal users to access mail server

Add a new IP Rule Folder called **all_to_dmz**

In the new folder, add a new IP Rule (to translate incoming smtp traffic to mailserver).

In the General tab:

General:
Name: **allow-smtp-ext**
Action: **SAT**
Service: **smtp**

Address Filter:
Source interface: **wan1**
Source network: **all-nets**
Destination interface: **core**
Destination network: **wan1_ip**

In the SAT tab.

Select **Destination Address**
New IP Address: **mail-server**

Click Ok.

In the **all_to_dmz** folder, add a new IP Rule (to allow incoming smtp traffic to mailserver).

In the General tab:

General:
Name: **allow-smtp-ext**

Action: **Allow**
Service: **smtp**

Address Filter:
Source interface: **wan1**
Source network: **all-nets**
Destination interface: **core**
Destination network: **wan1_ip**

Click Ok.

In the **all_to_dmz** folder, add a new IP Rule (to allow internal smtp traffic to mailserver).

In the General tab:

General:
Name: **allow-smtp-int**
Action: **Allow**
Service: **smtp**

Address Filter:
Source interface: **any**
Source network: **all-nets**
Destination interface: **dmz**
Destination network: **mail-server**

Click Ok.

6d. Rules to allow traffic to FTP server from vlan2

Add a new IP Rule folder called **vlan2_to_dmz**.

Add a new IP Rule (to allow ftp from vlan2 to dmz).

In the General tab:

General:
Name: **allow-ftp**
Action: **Allow**
Service: **ftp-passthrough**

Address Filter:
Source interface: **vlan2**
Source network: **vlan2net**
Destination interface: **dmz**
Destination network: **dmznet**

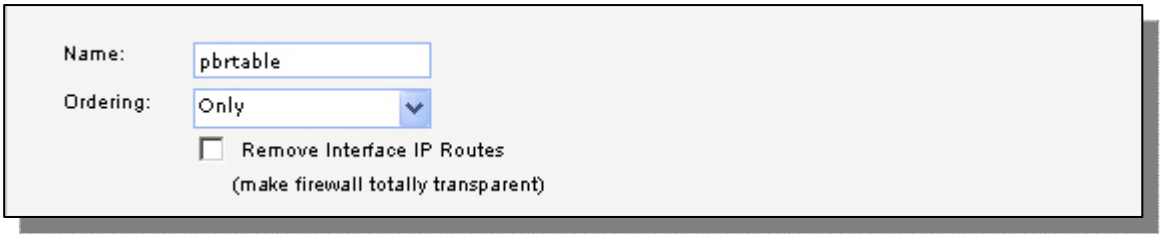
Click Ok.

7. Policy-based Routing

Go to *Routing -> Routing Tables*.

Add a new Routing Table.

General:



Name: **pbrtable**
Ordering: **Only**

Click Ok.

In this routing table, add a new Route.

In the General tab:

General:

Interface: **wan1**
Network: **all-nets**
Gateway: **wan1_gw**
Local IP Address: **(None)**
Metric: **0**

Click Ok.

Add a new Route.

In the General tab:

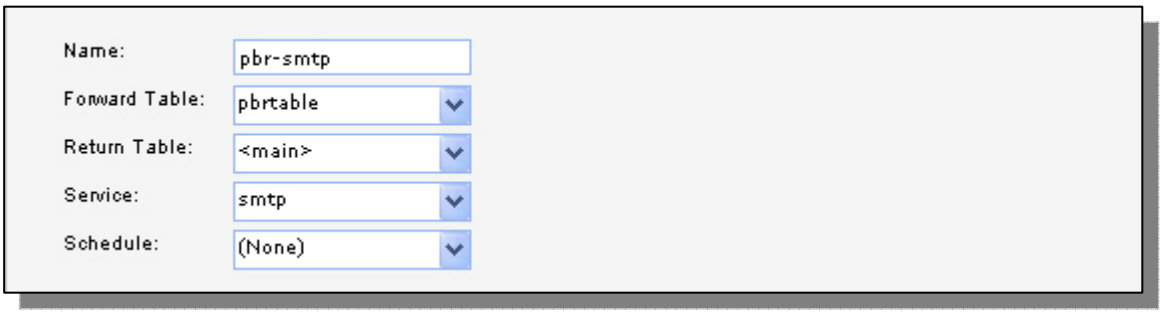
General:
Interface: **wan2**
Network: **all-nets**
Gateway: **wan2_gw**
Local IP Address: **(None)**
Metric: **1**

Click Ok.

Go to *Routing -> Routing rules*.

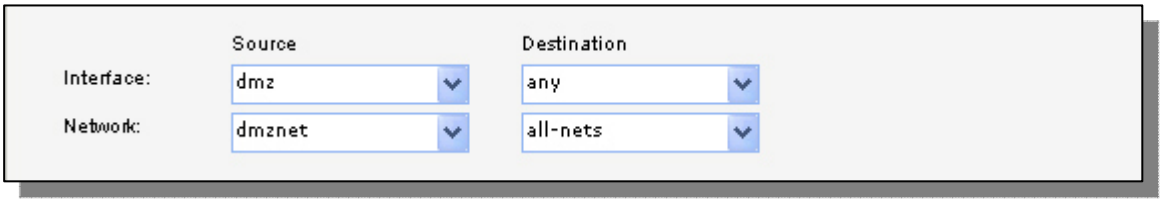
Add a new RoutingRule.

General:



Name: **pbr-smtp**
Forward Table: **pbrtable**
Return Table: **<main>**
Service: **smtp**
Schedule: **(None)**

Address Filter:



Source Interface: **dmz**
Source Network: **dmznet**
Destination Interface: **any**
Destination Network: **all-nets**

Click Ok.

Save and activate the configuration