



## Примеры настройки межсетевых экранов D-Link серии NetDefend

**DFL-210/800/1600/2500**

### Сценарий: VLAN и переключение маршрута в случае отказа

Последнее обновление: 2005-10-20

#### Обзор:

В этом документе условное обозначение *Objects->Address book* означает, что в дереве на левой стороне экрана сначала нужно нажать (раскрыть) **Objects** и затем **Address Book**.

Большинство примеров в этом документе даны для межсетевого экрана DFL-800. Те же самые настройки могут использоваться для всех других моделей этой серии. Единственное различие в названиях интерфейсов. Так как модели DFL-1600 и DFL-2500 имеют более одного сетевого интерфейса LAN, lan -интерфейсы называются lan1, lan2 и lan3.

Скриншоты в этом документе приведены для программного обеспечения версии 2.04.00. Если используется более поздняя версия ПО, скриншоты могут отличаться от тех, которые появятся в браузере.

Для предотвращения влияния существующих настроек на настройки, описанные в этом руководстве, перед началом работы сбросьте межсетевой экран к заводским настройкам по умолчанию.

# 4

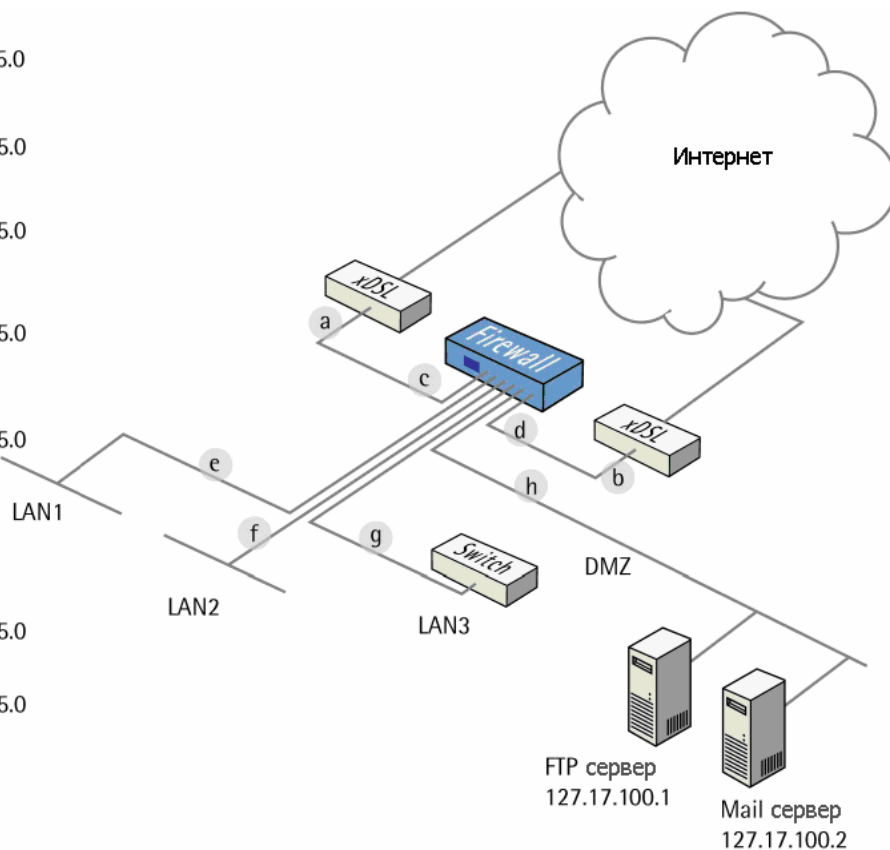
## VLAN и переключение маршрута в случае отказа

Для выполнения этих настроек требуется DFL-1600 или 2500. Однако большинство установок может использоваться и для DFL-210 или DFL-800. В сети lan3, которая подключена к порту коммутатора с поддержкой VLAN 802.1Q, будут созданы две VLAN.

Детали:

- Из lan1, lan2 и lan3: HTTP, HTTPS и DNS подключаются к Интернет через канал wan2.
- Из dmz: входящие и исходящие SMTP-сервисы подключаются к Интернет через wan1.
- Все внутренние сети также могут получить доступ к почтовому серверу в dmz.
- Только сетевые узлы VLAN2 могут получить доступ к FTP- серверу в dmz.
- Если один из wan-интерфейсов отключится, трафик этого интерфейса будет переадресован на другой wan-интерфейс.

- a IP: 192.168.110.254  
Маска подсети: 255.255.255.0
- b IP: 192.168.120.254  
Маска подсети: 255.255.255.0
- c IP: 192.168.110.1  
Маска подсети: 255.255.255.0  
шлюз: 192.168.110.254
- d IP: 192.168.120.1  
Маска подсети: 255.255.255.0  
шлюз: 192.168.110.254
- e IP: 192.168.1.1  
Маска подсети: 255.255.255.0
- f IP: 192.168.2.1  
Маска подсети:
- g VLAN 1 IP: 192.168.5.254  
VLAN 2 IP: 192.168.10.254  
Маска подсети: 255.255.255.0
- h IP: 172.17.100.254  
Маска подсети: 255.255.255.0



## 1. Адреса

Перейти в *Objects* -> *Address book* -> *InterfaceAddresses*

Убедитесь, что настроенные адреса соответствуют следующему списку, и добавьте объекты, которые еще не существуют. Чтобы добавить новые объекты, выберите IP4 Host/Network через выпадающее меню, введите имя и адрес и нажмите ок.

Имя	Адрес
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

Добавить новую группу IP4 Address Group.

Вкладка **General**:

### **General:**

Name:

Group members:

Available	Selected
all-nets	lan1net
ftp-server	lan2net
mail-server	vlan1net
vlan1_ip	vlan2net
vlan2_ip	
wan1_gw	

**Name:** all-lannets

Добавить lan1net, lan2net, vlan1net и vlan2net.

Нажать **Ok**.

## 2. Интерфейс Ethernet

Перейти в *Interfaces* -> *Ethernet*.

Изменить интерфейс **wan1** для использования следующих параметров.

Вкладка **General**:

Name:	<input type="text" value="wan1"/>
IP Address:	<input type="text" value="wan1_ip"/> ▼
Network:	<input type="text" value="wan1net"/> ▼
Default Gateway:	<input type="text" value="wan1_gw"/> ▼

**IP Address: wan1\_ip**

**Network: wan1net**

**Default Gateway: wan1\_gw**

Вкладка **Advanced**:

### **Automatic Route Creation:**

Automatically add commonly used routes related to this interface

Add route for interface network

Add default route if default gateway is specified

Route Metric:

Снять галочки с **Add route for interface network** и **Add default route if default gateway is specified**.

Нажать **Ok**.

Изменить интерфейс **wan2** в соответствии со следующими параметрами.

Вкладка **General**:

### **General:**

**IP Address: wan2\_ip**

**Network: wan2net**

**Default Gateway: wan2\_gw**

Вкладка **Advanced**:

### **Automatic Route Creation:**

Automatically add commonly used routes related to this interface

Add route for interface network

Add default route if default gateway is specified

Route Metric:

Убрать галочки с **Add route for interface network** и **Add default route if default gateway is specified**.

Нажать **Ok**.

### **3. Маршруты**

Перейти в *Routing* -> *Main Routing Table*.

Добавить новый маршрут **Route**.

Вкладка **General**:

#### **General:**

Interface:  ▼

Network:  ▼

Gateway:  ▼

Local IP Address:  ▼

Metric:

**Interface: wan1**

**Network: wan1net**

**Gateway: (None)**

**Local IP Address: (None)**

**Metric: 90**

Вкладка **Monitor**:

#### **Monitoring for Route Failover:**

Monitor This Route

Выбрать **Monitor This Route**

**Method:**

<input checked="" type="checkbox"/> Monitor Interface Link Status
<input type="checkbox"/> Monitor Gateway Using ARP Lookup
<input type="checkbox"/> Manual ARP Lookup Interval: <input type="text" value="1000"/> milliseconds

Выбрать **Monitor Interface Link Status**

Нажать **Ok**.

Добавить новый маршрут **Route**.

Вкладка **General**:

**General:**

Interface:	<input type="text" value="wan1"/>
Network:	<input type="text" value="all-nets"/>
Gateway:	<input type="text" value="wan1_gw"/>
Local IP Address:	<input type="text" value="(None)"/>
Metric:	<input type="text" value="90"/>

**Interface: wan1**

**Network: all-nets**

**Gateway: wan1\_gw**

**Local IP Address: (None)**

**Metric: 90**

Вкладка **Monitor**:

**Monitoring for Route Failover:**

<input checked="" type="checkbox"/> Monitor This Route
--

Select **Monitor This Route**

**Method:**

<input checked="" type="checkbox"/> Monitor Interface Link Status
<input checked="" type="checkbox"/> Monitor Gateway Using ARP Lookup
<input type="checkbox"/> Manual ARP Lookup Interval: <input type="text" value="1000"/> milliseconds

Выбрать **Monitor Interface Link Status**

Выбрать **Monitor Gateway Using ARP Lookup**

Добавить новый маршрут **Route**.

Вкладка **General**:

**General:**

Interface: wan2

Network: wan2net

Gateway: (None)

Local IP Address: (None) Metric: 80

Вкладка **Monitor**:

**Monitoring for Route Failover:**

Выбрать **Monitor This Route**

**Method:**

Выбрать **Monitor Interface Link Status**

Нажать **Ok**.

Добавить новый маршрут **Route**.

Вкладка **General**:

**General:**

Interface: wan2

Network: all-nets

Gateway: wan2\_gw

Local IP Address: (None)

Metric: 80

Вкладка **Monitor**:

**Monitoring for Route Failover:**

Выбрать **Monitor This Route**

**Method:**

Выбрать **Monitor Interface Link Status**

Выбрать **Monitor Gateway Using ARP Lookup**

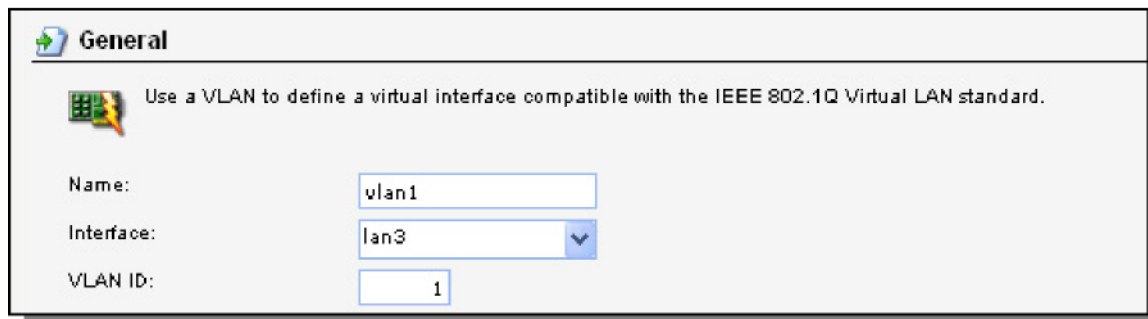
Нажать **Ok**.

#### **4. Интерфейс VLAN**

Перейти в *Interfaces* -> *VLAN*.

Вкладка **General**:

**General:**



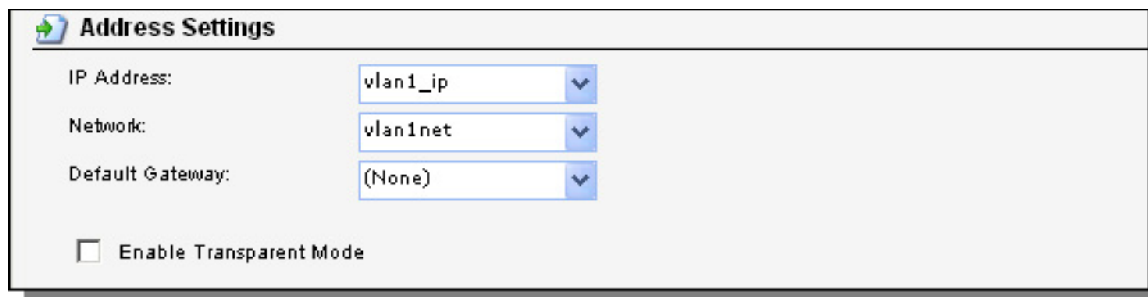
The screenshot shows the 'General' tab of a VLAN configuration window. At the top, there is a header with a folder icon and the word 'General'. Below the header, there is a small icon of a network card and a text instruction: 'Use a VLAN to define a virtual interface compatible with the IEEE 802.1Q Virtual LAN standard.' The configuration fields are: 'Name:' with a text input containing 'vlan1'; 'Interface:' with a dropdown menu showing 'lan3'; and 'VLAN ID:' with a text input containing '1'.

**Name: vlan1**

**Interface: lan3**

**VLAN ID: 1**

**Address Settings:**



The screenshot shows the 'Address Settings' tab of a VLAN configuration window. At the top, there is a header with a folder icon and the words 'Address Settings'. Below the header, there are three dropdown menus: 'IP Address:' with 'vlan1\_ip', 'Network:' with 'vlan1net', and 'Default Gateway:' with '(None)'. At the bottom, there is a checkbox labeled 'Enable Transparent Mode' which is currently unchecked.

**IP Address: vlan1\_ip**

**Network: vlan1net**

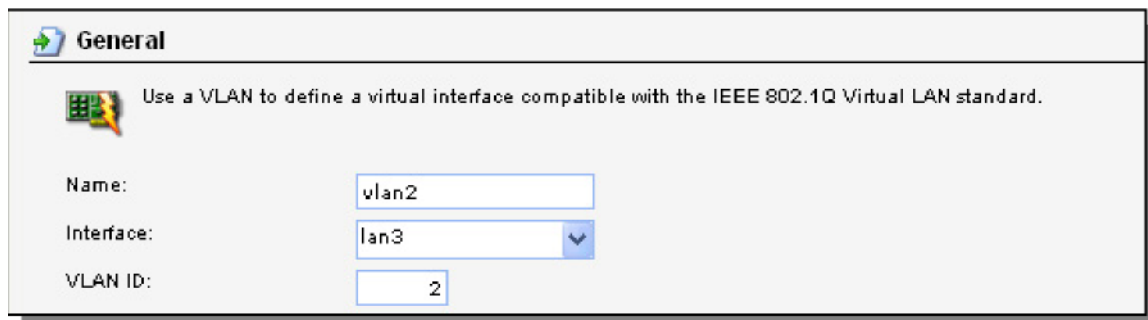
**Default Gateway: (None)**

Нажать **Ok**

Добавить новый VLAN.

Вкладка **General**:

**General:**

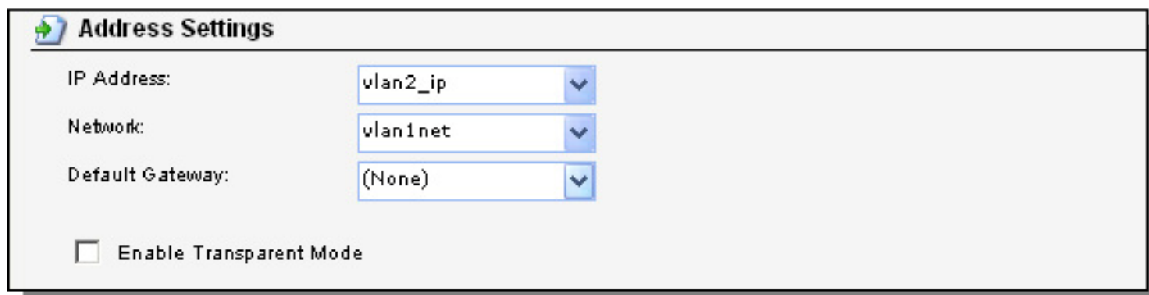


The screenshot shows the 'General' tab of a new VLAN configuration window. At the top, there is a header with a folder icon and the word 'General'. Below the header, there is a small icon of a network card and a text instruction: 'Use a VLAN to define a virtual interface compatible with the IEEE 802.1Q Virtual LAN standard.' The configuration fields are: 'Name:' with a text input containing 'vlan2'; 'Interface:' with a dropdown menu showing 'lan3'; and 'VLAN ID:' with a text input containing '2'.



VLAN ID: 2

**Address Settings:**



**Address Settings**

IP Address:

Network:

Default Gateway:

Enable Transparent Mode

IP Address: **vlan2\_ip**

Network: **vlan2net**

Default Gateway: **(None)**

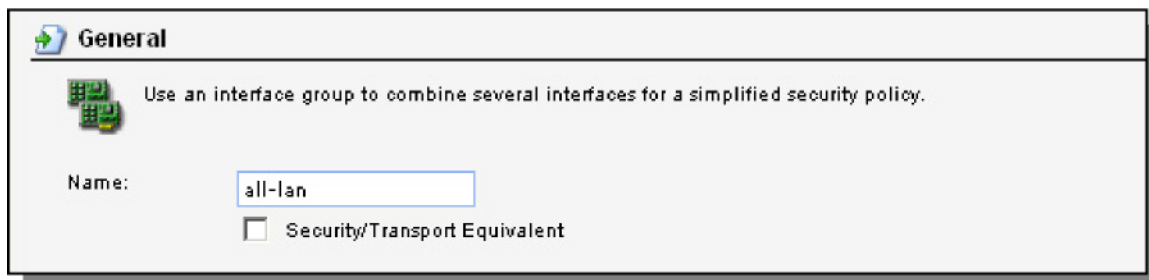
Нажать **Ok**

## 5. Группы интерфейсов

Перейти в *Interfaces* -> *Interface Groups*.

Добавить новую группу интерфейсов **Interface Group**.

**General:**



**General**

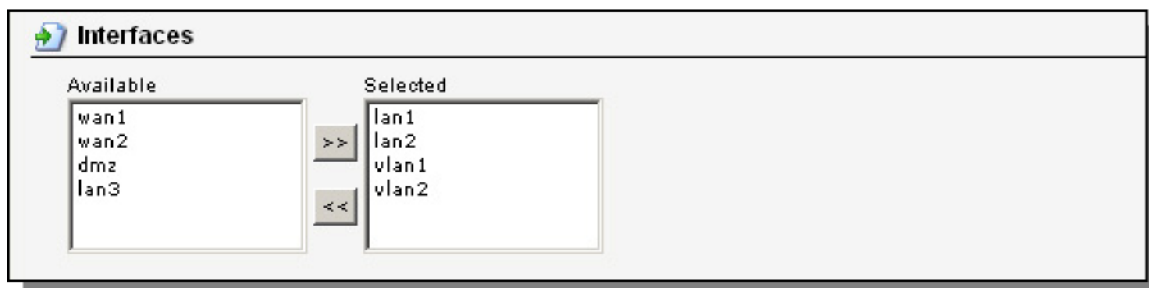
Use an interface group to combine several interfaces for a simplified security policy.

Name:

Security/Transport Equivalent

Name: **all-lan**

**Interfaces:**



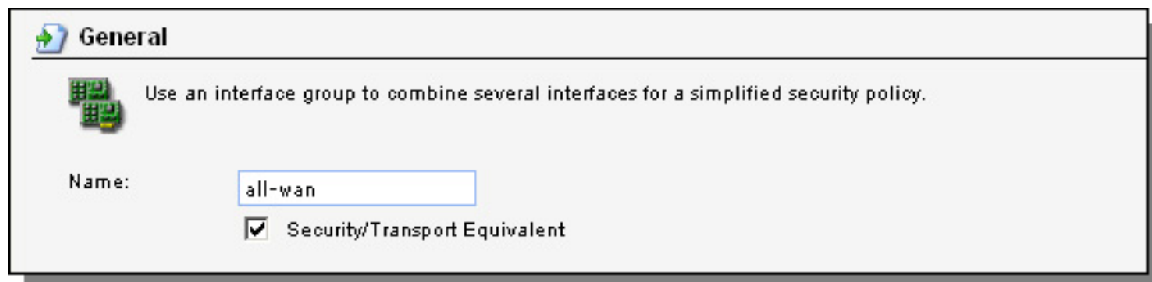
**Interfaces**

Available		Selected
wan1	>>	lan1
wan2	>>	lan2
dmz	>>	vlan1
lan3	>>	vlan2

Добавить **lan1**, **lan2**, **vlan1** и **vlan2** в эту группу.

Добавить новую группу интерфейсов **Interface Group**.

**General:**



**General**

Use an interface group to combine several interfaces for a simplified security policy.

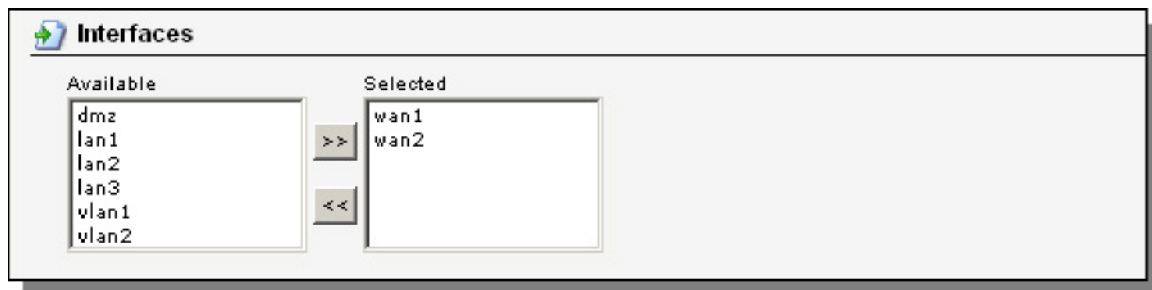
Name:

Security/Transport Equivalent

Name: **all-wan**

Выбрать **Security/Transport Equivalent**

**Interfaces:**



**Interfaces**

Available

- dmz
- lan1
- lan2
- lan3
- vlan1
- vlan2

Selected

- wan1
- wan2

Добавить **wan1** и **wan2** в эту группу.

Нажать **Ok**.

## 6а. Правила, позволяющие подключаться к HTTP, HTTPS и DNS в Интернет

Перейти *Rules* -> *IP Rules*.

Добавить новую папку **IP Rule Folder**, называемую **all-lan\_to\_all-wan**.

В новой папке добавить новое IP-правило **IP Rule** (разрешает HTTP).

Вкладка **General**:

**General:**



Name:

Action:

Service:

Schedule:

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

**Address Filter:**

	Source	Destination
Interface:	<input type="text" value="all-lan"/>	<input type="text" value="all-wan"/>
Network:	<input type="text" value="all-lannets"/>	<input type="text" value="all-nets"/>

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

Нажать **Ok**.

Добавить новое IP-правило **IP Rule** (разрешить исходящий dns-трафик).

Вкладка **General**:

**General:**

Name:	<input type="text" value="allow-dns-all"/>
Action:	<input type="text" value="NAT"/>
Service:	<input type="text" value="dns-all"/>
Schedule:	<input type="text" value="(None)"/>

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

**Address Filter:**

	Source	Destination
Interface:	<input type="text" value="all-lan"/>	<input type="text" value="all-wan"/>
Network:	<input type="text" value="all-lannets"/>	<input type="text" value="all-nets"/>

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

## **6b. Правила, разрешающие исходящий SMTP-трафик от почтового сервера к Интернет**

Добавить новую папку **IP Rule folder** называемую **dmz\_to\_all-wan**.

В новой папке добавить новое IP-правило **IP Rule** (разрешить исходящий smtp-трафик).

Вкладка **General**:

**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

Нажать **Ok**.

## **6c. Правила, разрешающие пользователям Интернет и внутренним пользователям доступ к почтовому серверу**

Добавить новую папку **IP Rule Folder**, называемую **all\_to\_dmz**

В новой папке добавить новое IP-правило (перенаправлять входящий smtp-трафик к почтовому серверу).

Вкладка **General**:

**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

Вкладка **SAT**.

Выбрать **Destination Address**

**New IP Address:** mail-server

Нажать **Ok**.

В папку **all\_to\_dmz** добавить новое IP-правило **IP Rule** (разрешить исходящий smtp-трафик к почтовому серверу).

Вкладка **General**:

**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

Нажать **Ok**.

В папку **all\_to\_dmz** добавить новое IP-правило **IP Rule** (разрешить внутренний smtp-трафик к почтовому серверу).

Вкладка **General**:

**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

Нажать **Ok**.

## **6d. Правила, разрешающие трафик к FTP-серверу из vlan2**

Добавить новую папку **IP Rule folder**, называемую **vlan2\_to\_dmz**.

Добавить новое правило **IP Rule** (разрешить ftp-трафик из vlan2 к dmz).

Вкладка **General**:

**General:**

**Name:** allow-ftp

**Action:** Allow

**Service:** ftp-passthrough

**Address Filter:**

**Source interface:** vlan2

**Source network:** vlan2net

**Destination interface:** dmz

**Destination network:** dmznet

Нажать **Ok**.

## 7. Маршрутизация на основе политик

Перейти в *Routing -> Policy-based Routing Tables*.

Добавить новую таблицу **Policy-based Routing Table**.

**General:**

Name:	<input type="text" value="pbtable"/>
Ordering:	<input type="text" value="Only"/>
	<input type="checkbox"/> Remove Interface IP Routes (make firewall totally transparent)

**Name:** pbtable

**Ordering:** Only

Нажать **Ok**.

В эту таблицу маршрутизации добавить новый маршрут **Route**.

Вкладка **General**:

**General:**

Interface:	<input type="text" value="wan1"/>
Network:	<input type="text" value="all-nets"/>
Gateway:	<input type="text" value="wan1_gw"/>
Local IP Address:	<input type="text" value="(None)"/>
Metric:	<input type="text" value="0"/>

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

Нажать **Ok**.

Добавить новый маршрут **Route**.

Вкладка **General**:

**General:**

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

Нажать **Ok**.

Перейти в *Policy-based Routing Policy*.

Добавить новое правило маршрутизации на основе политик **Policy-based Routing Rule**.

**General:**

Name:	<input type="text" value="pbr-smtp"/>
Forward Table:	<input type="text" value="pbtable"/> ▼
Return Table:	<input type="text" value="&lt;main&gt;"/> ▼
Service:	<input type="text" value="smtp"/> ▼
Schedule:	<input type="text" value="(None)"/> ▼

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

**Address Filter:**

	Source	Destination
Interface:	<input type="text" value="dmz"/> ▼	<input type="text" value="any"/> ▼
Network:	<input type="text" value="dmznet"/> ▼	<input type="text" value="all-nets"/> ▼

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

Нажать **Ok**.

Сохранить и активировать настройки.