Примеры настройки межсетевых экранов D-Link серии NetDefend

DFL-210/800/1600/2500

Сценарий: настроить управление полосой пропускания

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 -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.

3 Как настроить управление полосой пропускания

Описание сценария:
- Каналы WAN1 и WAN2 используют статический IP-адрес при подключении к сетям различных провайдеров xDSL. Обе схемы подключения обеспечивают полосу пропускания равную 1 Мбит/с (в этом случае принимаем 1Мб =1000 Кб).

Распределение полосы:

- WAN1: Для входящего и исходящего трафика **HTTP** и **HTTPS**, максимальная полоса пропускания 500 Кб.

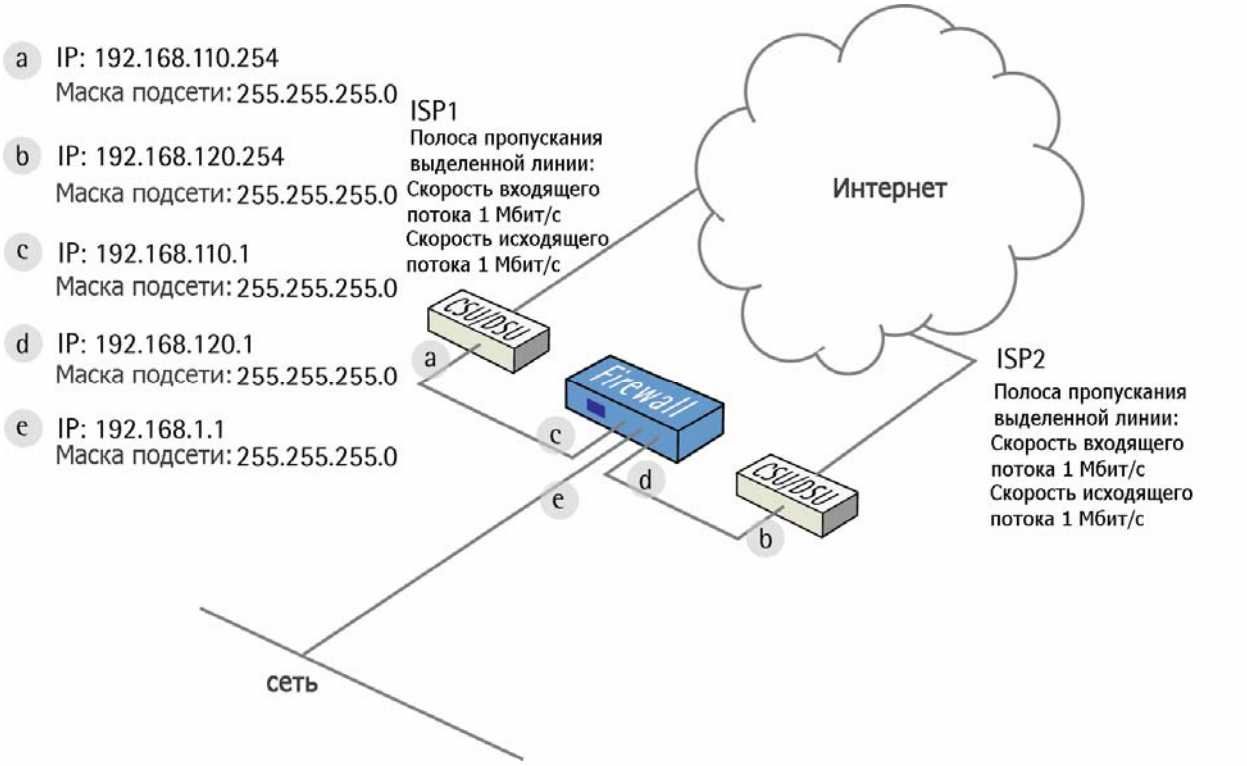
- WAN1: Для входящего и исходящего трафика **POP3 гарантированная** полоса пропускания 300 Кб (**максимальная** полоса пропускания 1000 Кб).

- WAN1: Для **других** входящих и исходящих сервисов **максимальная** полоса пропускания 200 Кб.

- WAN2: Для входящего и исходящего трафика **SMTP гарантированная** полоса пропускания 500 Кб (**максимальная** полоса пропускания 1000 Кб)

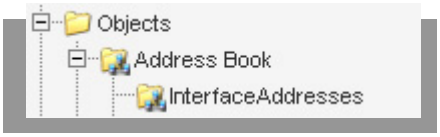
- WAN2: Для входящего и исходящего трафика **FTP максимальная** полоса пропускания 250 Кб.

- WAN2: Для входящего и исходящего трафика **VoIP гарантированная** полоса пропускания 250 Кб.



1. Адреса

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



Изменить следующие пункты:
Заменить **lan_ip** на **192.168.1.1**
Заменить **lannet** на **192.168.1.0/24**

Заменить **wan1_ip** на **192.168.110.1**
Заменить **wan1net** на **192.168.110.0/24**

Заменить **wan2_ip** на **192.168.120.1**
Заменить **wan2net** на **192.168.120.0/24**

Добавить новый **IP4 Host/Network**:
Имя: **wan1-gw**
IP-адрес: **192.168.110.254**

Нажать **Ok**

Добавить новый **IP4 Host/Network**:
Имя: **wan2-gw**
IP-адрес: **192.168.120.254**

Нажать **Ok**

2. Интерфейс Ethernet

Перейти в *Interfaces -> Ethernet*:

Изменить настройки интерфейса **wan1** .

Разрешить **IP Address** в качестве **wan1_ip** и **Network** в качестве **wan1net**.
Выбрать **wan1-gw** в качестве **Default Gateway** (шлюза по умолчанию).

Нажать **Ok**.

3. Сервисы

Перейти в *Objects -> Services*:

Добавить новый сервис **TCP/UDP Service**:

General:

Name: **voip**
Type: **TCP**
Source: **0-65535**
Destination: (enter the TCP port number for the VoIP service)

Нажать **Ok**

4. Правила

Перейти в *Rules -> IP Rules -> lan_to_wan1.*

Удалить предварительно созданные правила.

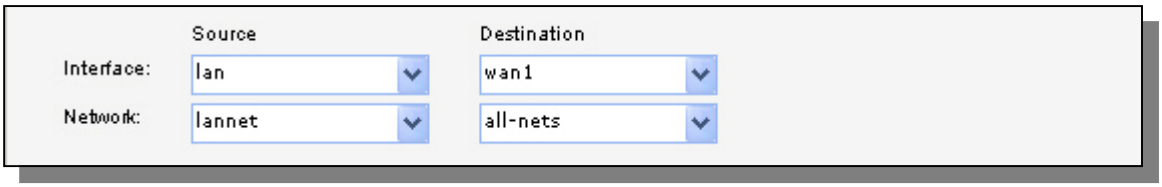
Добавить новое IP-правило **IP Rule**:

Вкладка **General**:

General:

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

Address filter:



Source interface: **lan**
Source network: **lannet**
Destination interface: **wan1**
Destination network: **all-nets**

Нажать **Ok**

Добавьте еще два правила, таким же способом, как и предыдущее:

Name	Action	Service	SourceIf	SourceNet	DestIf	DestNet
allow_pop3	NAT	pop3	lan	lannet	wan1	all-nets
allow_standard	NAT	all_services	lan	lannet	wan1	all-nets

Перейти в *Rules -> IP Rules:*

Добавить новую папку, называемую **lan_to_wan2**.

В новой папке создать три новых правила: **allow_smtp**, **allow_ftp**и **allow_voip**.

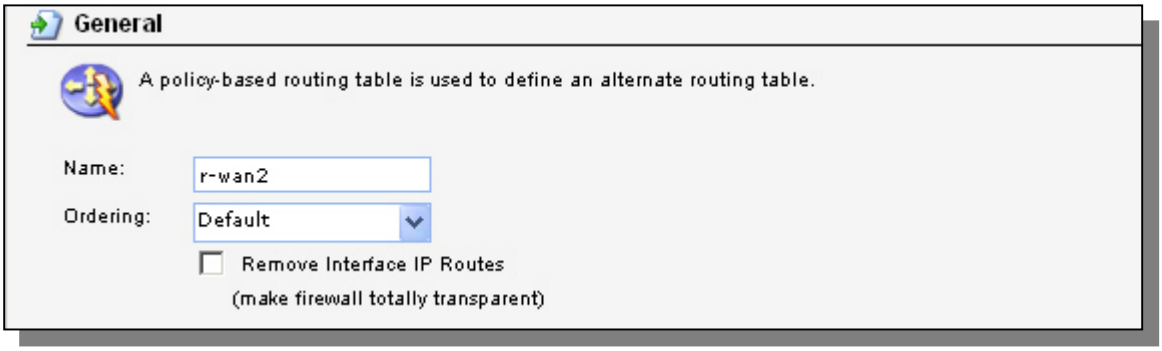
Name	Action	Service	SourceIf	SourceNet	DestIf	DestNet
allow_smtp	NAT	smtp	lan	lannet	wan2	all-nets
allow_ftp	NAT	ftp-passthrough	lan	lannet	wan2	all-nets
allow_voip	NAT	voip	lan	lannet	wan2	all-nets

5. Маршрутизация

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

Добавить новую таблицу **Policy-based Routing table**:

General:

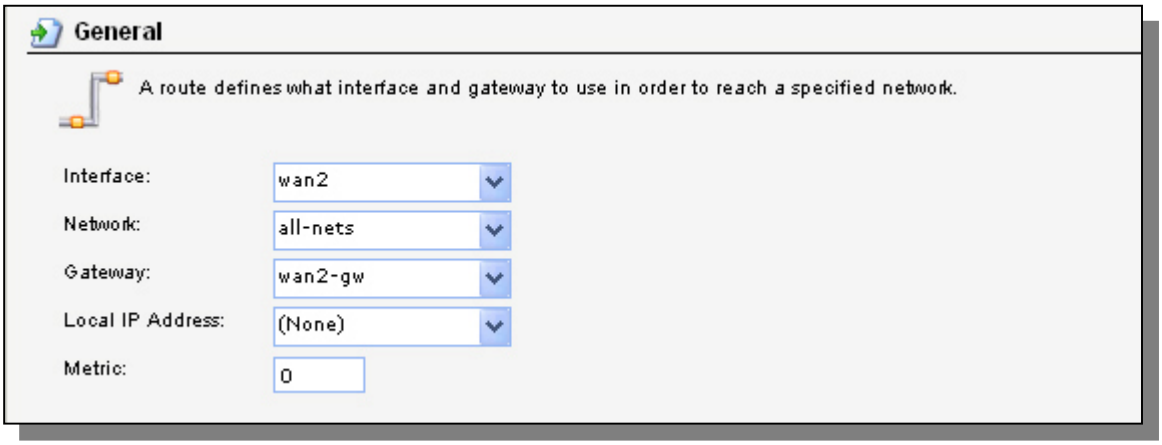


Name: **r-wan2**
Ordering: **Default**

Нажать **Ok**.

В новой таблице создать новый маршрут **Route**:

General:



Interface: **wan2**
Network: **all-nest**
Gateway: **wan2-gw**

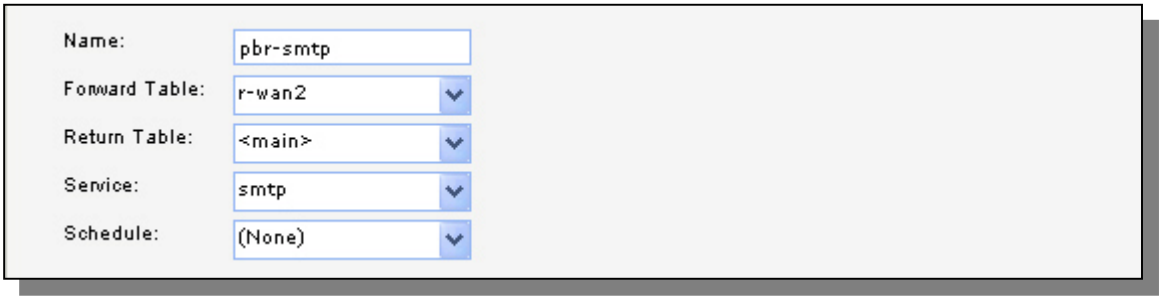
Metric: **0**

Нажать **Ok**.

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

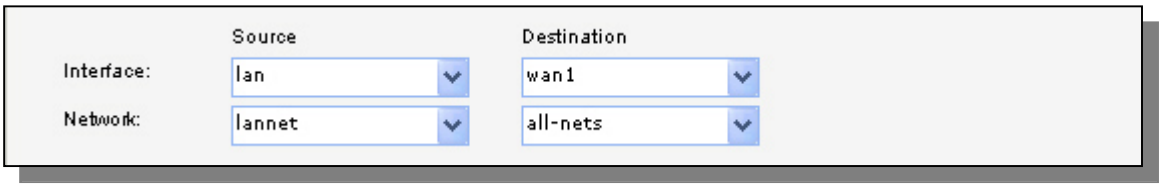
Добавить новое правило **Policy-based Routing**

Rule: ***General:***



Name: **pbr-smtp**
Forward Table: **r-wan2**
Return Table: **<main>**
Service: **smtp**

Address Filter:



Source interface: **lan**
Source network: **lannet**
Destination interface: **wan1**
Destination network: **all-nets**

Нажать **Ok**.

Создать еще три правила **маршрутизации на основе политик,** таким же способом, как и предыдущее.

Name	Forward	Return	Service	SourceIf	SourceNet	DestIf	DestNet
pbr-ftp	r-wan2	<main>	ftp-passthrough	lan	lannet	wan1	all-nets
pbr-voip	r-wan2	<main>	voip	lan	lannet	wan1	all-nets
pbr-all	<main>	r-wan2	all_services	wan2	all-nets	any	all-nets

Первые три правила, которые были созданы (pbr-smtp, pbr-ftp и pbr-voip) направляют SMTP, FTP и VoIP-трафик, полученный через интерфейс LAN на интерфейс WAN2 согласно PRB-таблице **r-wan2**. Ответный трафик будет маршрутизироваться в соответствии с основной таблицей маршрутизации. Последнее правило говорит, что весь трафик, поступающий от второго провайдера, будет передан в соответствии с основной таблицей маршрутизации и ответный трафик будет перенаправлен второму провайдеру по r-wan2.

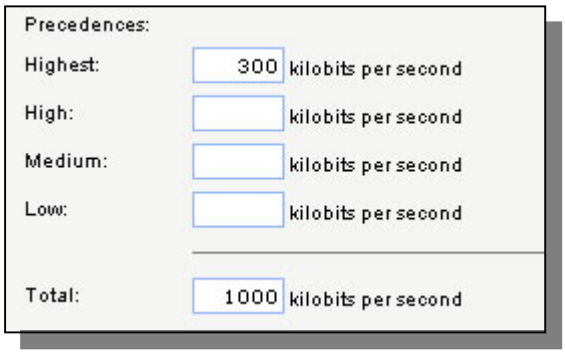
6. Формирование трафика

Перейти в *Traffic Shaping -> Pipes*.

Добавить новый канал **Pipe**:

General:
Name: **wan1-std-in**

Лимит канала:
Задать **Highest** равным **300**
Задать **Total** равным **1000**



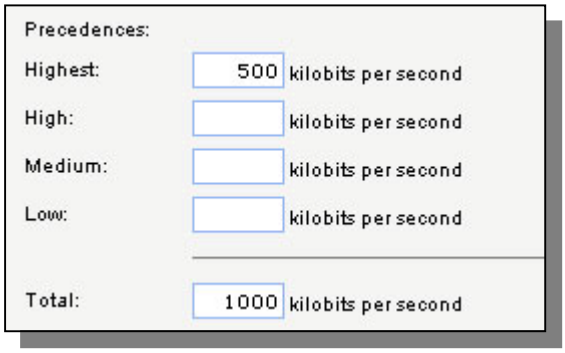
Нажать **Ok.**

Добавьте новый канал **Pipe** называемый **wan1-std-out,** использующий те же самые настройки.

Добавьте новый канал **Pipe**:

General:
Name: **wan2-std-in**

Лимит канала:
Задать **Highest** равным **500**
Задать **Total** равным **1000**



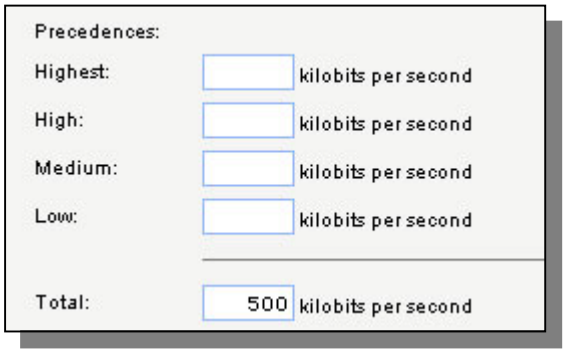
Нажать **Ok**

Добавить новый канал **Pipe** называемый **wan2-std-out,**использующий те же самые настройки.

Добавить новый канал **Pipe**:

General:
Name: **http-in**

Лимит канала:
Задать **Total** равным **500**



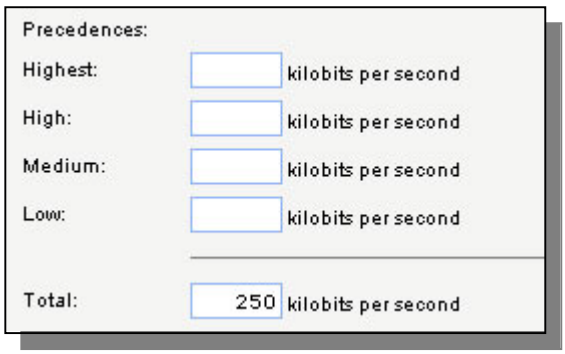
Нажать **Ok**

Добавить новый канал **Pipe** называемый **http-out,** использующий те же самые настройки.

Добавить новый канал **Pipe**:

General:
Name: **ftp-in**

Лимит канала:
Задать **Total** равным **250**



Нажать **Ok**

Добавить новый канал **Pipe** называемый **ftp-out,**использующий те же самые настройки.

Добавить новый канал **Pipe**:

General:
Name: **voip-in**

Pipe Limits:
Задать **Highest** равным **250**

Нажать **Ok**

Добавить новый канал **Pipe** называемый **voip-out,**использующий те же самые настройки.
Список каналов должен быть похож на этот:

#	Name	Grouping	GroupingNetworkSize	LimitKbpsTotal
0	wan1-std-in	None	0	1000
1	wan1-std-out	None	0	1000
2	wan2-std-in	None	0	1000
3	wan2-std-out	None	0	1000
4	http-in	None	0	500
5	http-out	None	0	500
6	ftp-in	None	0	250
7	ftp-out	None	0	250
8	voip-in	None	0	
9	voip-out	None	0	

Перейти в *Traffic Shaping - > Pipe Rules*.

Добавить новое правило канала **Pipe Rule**.

Вкладка **General**:

General:

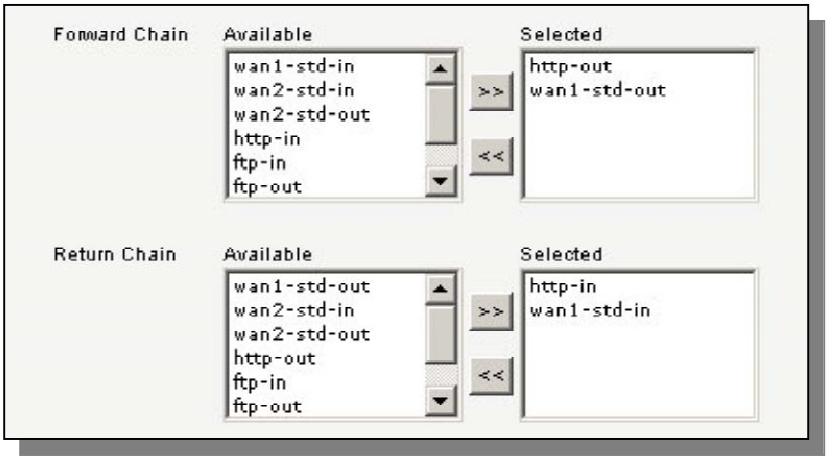
Name: **wan1-http**
Service: http-all

Address filter:

Source interface: **lan**
Source network: **lannet**
Destination interface: **wan1**
Destination network: **all-nets**

Вкладка **Traffic Shaping**:

Pipe Chains:



Добавить **http-out** и **wan1-std-out** для **Forward Chain**.
Добавить **http-in** и **wan1-std-in** для **Return Chain**.

Precedence:

Выбрать **Use Fixed Precedence**и **Medium**

Нажать **Ok**.

Добавить новое правило канала **Pipe Rule**.

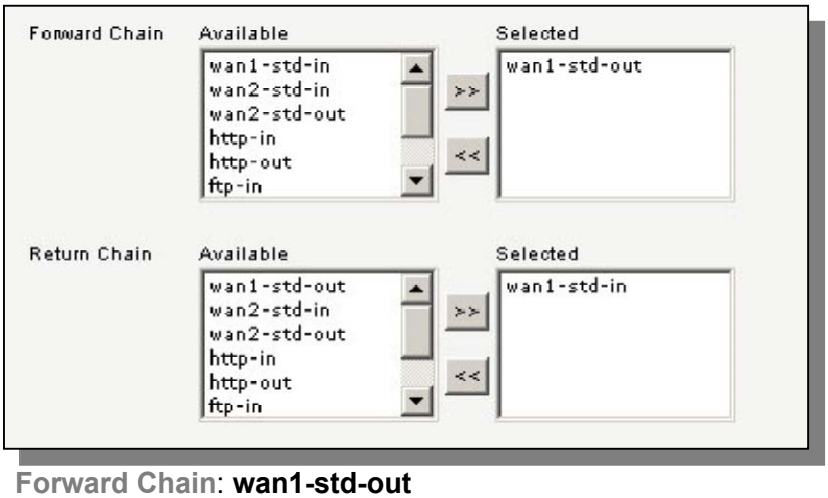
Вкладка **General**:

General:
Name*: wan1-pop3*
Service: **pop3**

Address Filter:
Source interface: **lan Source network**: **lannet Destination interface**: **wan1**
Destination network: **all-nets**

Вкладка **Traffic Shaping**:

Pipe Chains:



Forward Chain: **wan1-std-out**
Return Chain: **wan1-std-in**

Выбрать **Use fixed precedence**и **Highest**

Нажать **Ok**.

Добавить еще одно правило с такими же настройками фильтра адресов тем же способом, что и два предыдущих:

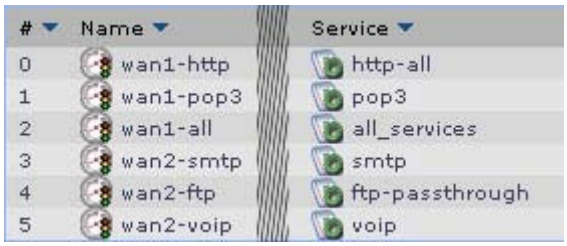
Name	Service	Forward	Return	Precedence
wan1-all	all_services	wan1-std-out	wan1-std-in	Fixed Low

Добавить еще три правила со следующими настройками фильтра адресов.

Source interface: **lan**
Source network: **lannet**
Destination interface: **wan2**
Destination network: **all-nets**

Name	Service	Forward	Return	Precedence
wan2-smtp	smtp	wan2-std-out	wan2-std-in	Fixed Highest
wan2-ftp	ftp-passthrough	ftp-out wan2-std-out	ftp-in wan2-std-in	Fixed Medium
wan2-voip	voip	voip-out wan2-std-out	voip-in wan2-std-in	Fixed Highest

Следующая картинка показывает шесть правил, которые мы сейчас создали. Все правила должны содержать **lan** в качестве **исходного интерфейса**, **lannet** в качестве **исходной сети** и **all-nets** в качестве **сети назначения**. Первые три правила должны содержать **wan1** в качестве **интерфейса назначения**, а последние три – **wan2** в качестве **интерфейса назначения**.



Сохранить и активировать настройки.