



# **Лабораторные работы по курсу «Основы сетевой безопасности»**

**Часть 1: Межсетевые экраны**

---

**Расширенный курс D-Link**

**Москва, 2014**

---

## Оглавление

<b>ЛАБОРАТОРНЫЙ ПРАКТИКУМ.....</b>	<b>3</b>
<b>Основы администрирования межсетевого экрана D-Link DFL-860 .....</b>	<b>3</b>
Лабораторная работа 1. Основы администрирования межсетевого экрана.....	3
Лабораторная работа 2. Соединение двух локальных сетей, расположенных за межсетевыми экранами	20
<b>Сегментирование сетей на канальном уровне.....</b>	<b>46</b>
Лабораторная работа 3. Сегментирование подсетей с использованием управляемых коммутаторов	46
Лабораторная работа 4. Сегментирование подсетей на основе port-based VLAN .....	52
<b>Межсетевые экраны.....</b>	<b>59</b>
Лабораторная работа 5. Создание политики без проверки состояния .....	59
Лабораторная работа 6. Создание политик для традиционного (или исходящего) NAT .....	62
Лабораторная работа 7. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing .....	67
<b>Системы обнаружения и предотвращения проникновений.....</b>	<b>74</b>
Лабораторная работа 8. Антивирусное сканирование.....	74
Лабораторная работа 9. Обнаружение и предотвращение вторжений.....	82
<b>Приоритезация трафика и создание альтернативных маршрутов.....</b>	<b>100</b>
Лабораторная работа 10. Создание альтернативных маршрутов с использованием статической маршрутизации .....	100
Лабораторная работа 11. Ограничение полосы пропускания трафика .....	108
Лабораторная работа 12. Ограничение полосы пропускания P2P-трафика с использованием IDP	134

# Лабораторный практикум

## Основы администрирования межсетевого экрана D-Link DFL-860

### Лабораторная работа 1. Основы администрирования межсетевого экрана

#### Цель

Рассмотрим общие вопросы администрирования межсетевого экрана.

1. Вход с использованием различных интерфейсов в консоль управления межсетевым экраном.
2. Перезапуск межсетевого экрана, сброс к заводским настройкам по умолчанию, установка даты и времени, DNS, активация и применение изменений.
3. Сброс и загрузка новой конфигурации устройства, автоматическое обновление ПО.
4. Поиск неисправностей.

#### Описание практической работы

##### *Управление межсетевым экраном с помощью различных интерфейсов*

##### *Доступ к межсетевому экрану с рабочей станции*

Новому межсетевому экрану D-Link NetDefend с заводскими настройками по умолчанию система NetDefendOS автоматически назначает внутренний IP-адрес по умолчанию на интерфейсе **lan1** (или интерфейс **lan** на моделях с одним локальным интерфейсом). IP-адрес, назначаемый интерфейсу управления, зависит от модели межсетевого экрана NetDefend:

- Для моделей межсетевых экранов NetDefend DFL-210, 260, 800, 860, 1600 и 2500, IP-адрес интерфейса управления, назначаемый по умолчанию - **192.168.1.1**.
- Для моделей межсетевых экранов NetDefend DFL-1660, 2560, 2560G и 260E/860E, IP-адрес интерфейса управления, назначаемый по умолчанию - **192.168.10.1**.

IP-адреса интерфейса межсетевого экрана, который соединен с рабочей станцией, и интерфейс самой рабочей станции, которая должна выполнять управление межсетевым экраном, должны быть в одной и той же сети. Поэтому интерфейсу рабочей станции вручную должен быть назначен статический IP-адрес из подсети 192.168.1.0/24 и основной шлюз 192.168.1.1:

**IP-адрес:** 192.168.1.30

**Маска подсети:** 255.255.255.0

**Основной шлюз:** 192.168.1.1

##### *Веб-интерфейс*

Система NetDefendOS предоставляет *веб-интерфейс* (WebUI) для управления системой с помощью стандартного веб-браузера.

Первоначальная регистрация в веб-интерфейсе и Мастер установки

Для первоначального доступа к веб-интерфейсу межсетевое экрана с заводскими настройками по умолчанию следует использовать URL <https://192.168.1.1>.

После этого появится диалоговое окно аутентификации пользователя.

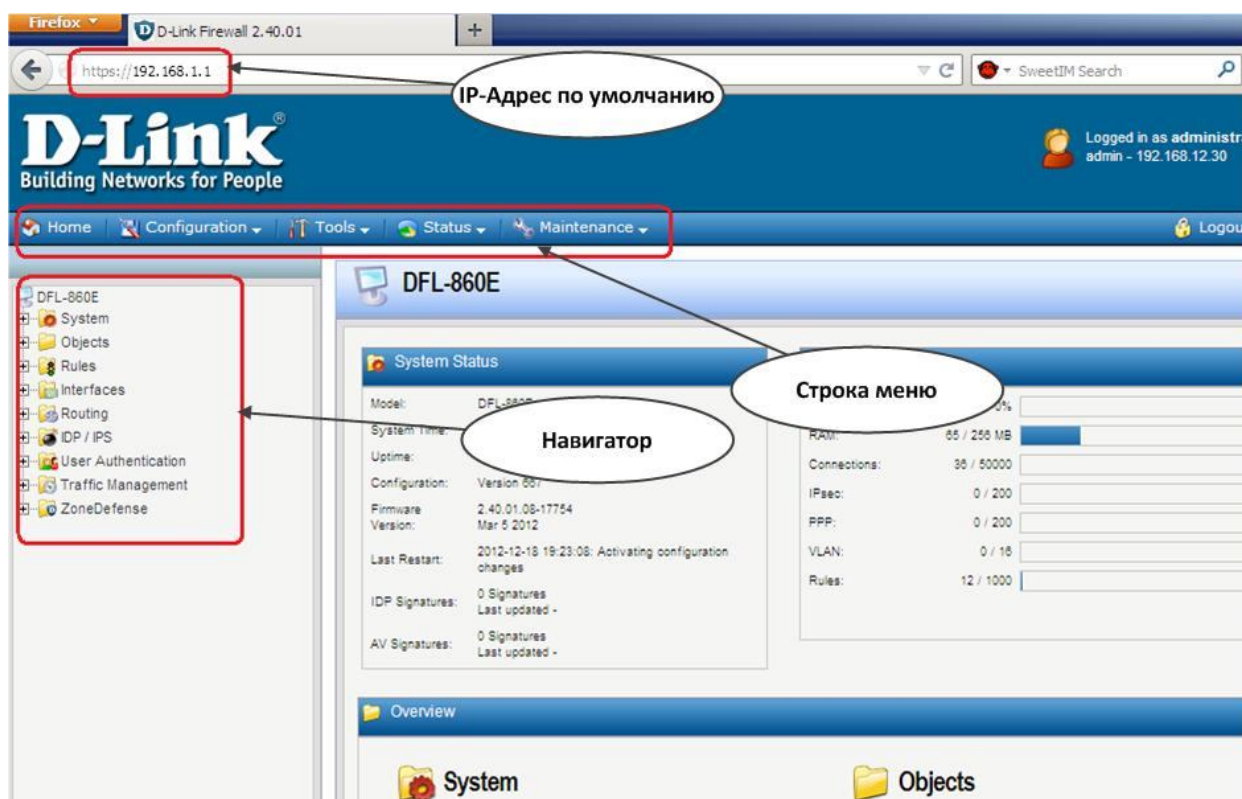


Имя пользователя по умолчанию – **admin**, пароль по умолчанию – **admin**.

Диалоговое окно регистрации в веб-интерфейсе предоставляет возможность выбрать язык интерфейса. Поддержка языка реализована с помощью набора ресурсных файлов.

Если изменения в настройках не были сделаны, запускается Мастер установки, и администратор может выполнить все необходимые шаги по установке публичного доступа к интернет.

Общий вид веб-интерфейса:



Доступ к веб-интерфейсу регулируется настраиваемой политикой удаленного управления. По умолчанию, система разрешает доступ к веб-интерфейсу только из сети, которая подсоединена к интерфейсу **lan**. Будем называть эту сеть внутренней.

Строка меню содержит кнопки и выпадающие меню, используемые для редактирования различных настроек, а также для доступа к различным инструментальным средствам и

просмотру текущих статусов соединений, интерфейсов, аутентифицированных пользователей и т.п.

**Home** – Возврат на главную страницу веб-интерфейса.

#### **Configuration**

**Save and Activate** – Сохранение и активация настроек.

**Discard changes** – Отмена изменений в настройках, выполненных во время текущей сессии.

**View Changes** – Список изменений в настройках с момента последнего сохранения.

**Tools** – Инструментальные средства, необходимые для обслуживания системы.

**Status** – Текущие статусы, используемые для диагностики текущего состояния системы.

**Maintenance** – Обслуживание.

**Update Center** – Обновление сигнатур антивируса и определения вторжений, которое может выполняться как вручную, так и по расписанию.

**License** – Просмотр лицензии и ввод кода активации.

**Backup** – Создание резервной копии настроек на рабочей станции и восстановление предварительно созданной резервной копии.

**Reset** – Перезапуск межсетевого экрана или сброс к заводским настройкам по умолчанию.

**Upgrade** – Обновление программного обеспечения межсетевого экрана.

**Technical support** – Создание на рабочей станции файла, содержащего различные статистические данные о работе межсетевого экрана. Этот файл может быть изучен локально или отправлен специалисту технической поддержки для оказания помощи в исследовании проблемы. Это является крайне важным, так как автоматически собираемая информация содержит множество деталей, которые требуются при поиске и устранении неисправностей.

По умолчанию, доступ к веб-интерфейсу открыт только из внутренней сети. Если необходимо включить доступ с других интерфейсов, кроме интерфейса **lan**, требуется изменить политику удаленного управления.

#### **Веб-интерфейс:**

**System** → **Remote Management** → **Add** → **HTTP/HTTPS Management**

**RemoteMgmtHTTP**  
Configure HTTP/HTTPS management to enable remote management to the system.

**General**

**Remote Access Type**

Name: RemoteMgmtHTTP

HTTP

HTTPS

**Access**

Select the user database to use for login and the access level to grant to the user.

User Database: AdminUsers

Access Level: Admin

**Access Filter**

Remote access is granted from the following interface and network.

Interface: any

Network: all-nets

**Comments**

### Командная строка:

```
add RemoteManagement RemoteMgmtHTTP https Network=all-nets Interface=any
LocalUserDatabase=AdminUsers HTTPS=Yes
```

После завершения работы необходимо выйти из веб-интерфейса, чтобы предотвратить доступ других пользователей к межсетевому экрану. Выход из системы осуществляется нажатием кнопки **Logout**, расположенной справа в строке меню.

### Интерфейс командной строки CLI

Система NetDefendOS предоставляет *интерфейс командной строки (CLI)*, который доступен локально через серийный консольный порт (соединение с которым описывается ниже) или удаленно через один из интерфейсов межсетевого экрана с помощью клиента протокола *Secure Shell (SSH)*.

CLI предоставляет набор команд, обеспечивающих отображение и изменение настроек, а также отображение работы системы и выполнение задач по обслуживанию системы.

Наиболее часто используемые команды CLI:

- **add** – Добавление объекта, например, IP-адреса или правила в настройки межсетевого экрана.
- **set** – Изменение какого-либо свойства объекта.
- **show** – Отображение текущих категорий или значений объекта.
- **delete** – Удаление объекта.

### Структура команд

Большинство команд имеют следующую структуру:

```
<command> [<object_category>] <object_type> <object_name>
[<object_properties>]
```

Например, для отображения IP-адреса объекта `my_address` используется команда:

```
gw-world:/> show Address IP4Address my_address
```

Все настраиваемые сущности (IP-адреса, интерфейсы, правила фильтрации и маршрутизации и т.п.) межсетевого экрана называются объектами. Каждый объект принадлежит определенному типу (`IP4Address`, `Ethernet`, `IPsecTunnel`, `IPRule`, `RoutingRule` и т.п.). Несколько типов могут быть сгруппированы в категорию (`Address`, `Interface`, `Settings` и т.п.).

Команда

```
gw-world:/> help help
```

выводит справочную информацию о системе.

### *История команд*

Навигация по списку использованных команд в интерфейсе командной строки выполняется с помощью клавиш «стрелка вниз» и «стрелка вверх» (аналогично консоли в большинстве версий Microsoft Windows™ и UNIX™). Например, нажатие клавиши «стрелка вверх» вызовет появление последней выполненной команды в текущей строке CLI. После этого ее можно отредактировать и выполнить.

### *Функция Tab Completion*

Система NetDefendOS предоставляет возможность, которая называется *tab completion*. Нажатие клавиши `tab` вызовет автоматическое завершение текущего идентификатора. Если однозначное завершение невозможно, то нажатие клавиши `tab` приведет к автоматическому отображению возможных завершений или опций команды.

Возможность `tab completion` можно также использовать для автоматического заполнения параметров команды значениями по умолчанию. Для этого в качестве значения следует ввести символ "." и нажать клавишу `tab`. Например, если при наборе незаконченной команды:

```
set Address IP4Address lan_ip Address=
```

ввести "." и нажать клавишу `tab`, то отобразится текущее значение параметра `Address`. Если данным значением является, например, `10.6.58.10` будет автоматически создана следующая команда:

```
set Address IP4Address lan_ip Address=10.6.58.10
```

После этого ее можно при необходимости отредактировать и выполнить.

### *Категории объектов*

Ранее упоминалось, что объекты группируются по *типу*, например, `IP4Address`. Типы могут группироваться по *категориям*. Тип `IP4Address` принадлежит категории `Address`. При использовании в категориях функция `tab completion` применяется для поиска типа объекта, который необходимо использовать.

При вводе команды, например `add`, и нажатии клавиши `tab`, отображаются доступные для использования с этой командой категории. После выбора категории и повторного нажатия клавиши `tab`, будут отображены все типы объектов для данной категории.

Не все типы объектов принадлежат категориям. В этом случае после ввода команды и нажатия `tab` будет появляться список возможных типов объектов.

### Выбор категории объектов

Для некоторых команд сначала с помощью команды `cc` необходимо указать категорию и экземпляр, прежде чем отдельные объекты могут создаваться или редактироваться. Это касается, например, правил маршрутизации или фильтрации. Если существует более одной таблицы маршрутизации, для добавления или изменения маршрута необходимо использовать команду `cc` для указания используемой таблицы маршрутизации.

```
gw-world:/> cc RoutingTable main
```

```
gw-world:/main>
```

Обратите внимание, что приглашение изменяется. Теперь можно добавить маршрут:

```
gw-world:/main> add Route Name=new_route1 Interface=lan Network=lannet
```

Для отмены указания текущей категории следует использовать команду `cc` без параметров.

В категориях, в которых перед созданием или редактированием объектов требуется указать экземпляр с помощью команды `cc`, в списке, показываемом командой `show`, после имени категории следует символ «/».

```
192.168.12.10 - PuTTY
[Address]           IGMPSetting           ZoneDefenseSwitch
[ALG]              IKEAlgorithms
[Client]           IPPool
[Driver]           IPRule
[Interface]        IPRuleFolder/
[LogReceiver]      IPsecAlgorithms
[RemoteManagement] LDAPDatabase
[Service]          LDAPServer
[Settings]         LocalUserDatabase/
Access             NATPool
AdvancedScheduleProfile/ OSPFProcess/
ARPND              Pipe
BlacklistWhiteHost PipeRule
Certificate         PSK
COMPortDevice      RadiusAccounting
ConfigModePool     RadiusServer
DateTime           RouteBalancingInstance
Device             RouteBalancingSpilloverSettings
DHCPRelay          RoutingRule
DHCPServer/        RoutingTable/
DNS                ScheduleProfile
DynamicRoutingRule/ SSHClientKey
--- More (1/2) ---
```

### Определение нескольких значений параметров

Иногда параметр команды может иметь несколько значений. Эти значения должны разделяться запятой. Например:

```
AccountingServers=server1 , server2 , server3
```

### Добавление нового правила в список правил

Порядок правил в списке, например, набор правил фильтрации, является важным. По умолчанию новое правило добавляется в конец списка. Если упорядоченность важна, то может быть добавлен параметр `Index=<Номер позиции в списке правил>`.



### *Использование уникальных имен*

Для удобства рекомендуется назначать всем объектам уникальные имена, чтобы эти имена можно было использовать в качестве ссылки на объект. Это особенно часто используется при написании сценариев.

Имена должны быть уникальными в пределах одного типа объекта. По причинам совместимости с более ранними выпусками NetDefendOS существует исключение, связанное с IP-правилами, у которых могут быть двойные имена, тем не менее, рекомендуется избегать этого. Если дублированное имя IP-правила используется в двух IP-правилах, в таком случае только значение **index** может однозначно определить каждое IP-правило в командах. Ссылка на IP-правило с дублированным именем приведет к сообщению об ошибке.

### *Использование dns-имени вместо IP-адреса*

В некоторых командах адрес в виде dns-имени, а не IP-адреса. В этом случае перед именем должен стоять префикс **dns:**, указывающий на то, что необходимо использовать сервис DNS для поиска IP-адреса по имени хоста. Например, dns-имя **host.company.com** следует указывать в командной строке как **dns:host.company.com**.

Параметры, в которых могут употребляться dns-имена в командной строке:

- Удаленная конечная точка для IPsec-, L2TP- и PPTP-туннелей.
- Хост для LDAP-серверов.

Если необходимо использовать сервис DNS, то следует настроить хотя бы один DNS-сервер, который будет выполнять преобразования dns-имена в IP-адреса.

### *Локальный доступ к интерфейсу командной строки*

Серийный порт консоли – это порт RS-232 межсетевое экрана NetDefend, обеспечивающий локальный доступ к интерфейсу командной строки. Порт RS-232 существует на старших моделях DFL 1660/2560. На новых младших моделях DFL консольный порт выполнен в виде Ethernet-разъема.

### *Доступ к интерфейсу командной строки по протоколу SSH (Secure Shell)*

Протокол SSH (Secure Shell) используется для доступа к интерфейсу командной строки с удаленной рабочей станции. Протокол SSH обеспечивает безопасные коммуникации по незащищенным сетям, а также сильную аутентификацию обеих сторон. SSH-клиенты доступны для большинства платформ.

Система NetDefendOS поддерживает версии 1, 1.5 и 2 протокола SSH. Разрешение доступа по протоколу SSH предоставляется с помощью политики удаленного управления, и по умолчанию разрешения доступа по протоколу SSH нет.

### **Веб-интерфейс:**

```
System > Remote Management > Add > Secure Shell Management
```

```
  Name: SSH_1an
```

**SSH\_lan**  
Configure a Secure Shell (SSH) Server to enable remote m

**General**

Name: SSH\_lan

Listening Port: 22

Max Concurrent Clients: 5

Session idle timeout: 1800

Login grace timeout: 30

Greeting Message:

Maximum Authentication Retries: 3

**Authentication Methods**

Client authentication methods that this server supports

Password:

Public Key:

**Host Key Algorithms**

Public Key Algorithms for which the unit has private host keys s authentication.

DSA:

RSA:

**Key Exchange Algorithms**

AES-128  Blowfish

AES-192  3DES

AES-256

**Integrity Algorithms**

SHA1  MD5

SHA1-96  MD5-96

**Access**

Select the user database to use for login and the access level to gran

User Database: AdminUsers

Access Level: Admin

**Access Filter**

Remote access is granted from the following interface and network.

Interface: lan

Network: lanetFW1

**Comments**

### Командная строка:

```
add RemoteManagement RemoteMgmtSSH ssh Network=lanetFW1 Interface=lan
LocalUserDatabase=AdminUsers
```

### Изменение пароля пользователя *admin*

После первоначального запуска рекомендуется как можно скорее изменить пароль по умолчанию **admin** на любой другой. Пароль пользователя может быть любой комбинацией символов и не может содержать более 256 символов.

### Веб-интерфейс:

User Authentication → Local User Databases → AdminUsers

**admin**  
User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec...

General SSH Public Key

**General**

Name:

Password:

Confirm Password:

Groups:

Comma separated list of groups

Users that are members of the 'administrators' group are allowed to change the firewall configuration.  
Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

Add administrators Add auditors

**Per-user IP Configuration (for PPTP, L2TP and SSL VPN)**

Static Client IP Address:

Networks behind user:

Metric for networks:

### Командная строка:

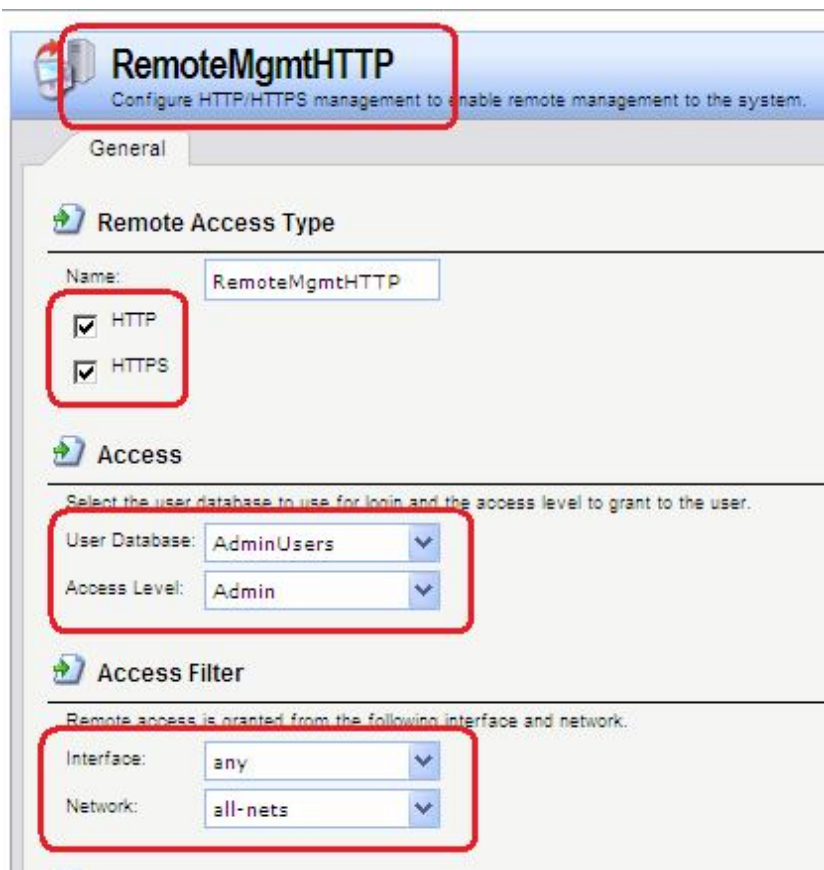
```
cc LocalUserDatabase AdminUsers
set User admin Password=admin
```

### Учетные записи для администрирования межсетевого экрана

Для администрирования межсетевого экрана используются учетные записи пользователей, которые хранятся в локальной базе данных.

По умолчанию имеется локальная база данных **AdminUsers**, которая содержит учетную запись **admin**. Пароль данной учетной записи – **admin**.

Какая именно база данных используется для хранения учетных записей администраторов межсетевого экрана и с каких интерфейсов и сетей возможно администрирование, определяется конфигурационными параметрами.



Для управления межсетевым экраном определены две группы: **Administrators** и **Auditors**.

Учетные записи, принадлежащие группе **Administrators**, обладают правами по чтению и записи всех настроек межсетевого экрана.

Учетные записи, принадлежащие группе **Auditors**, обладают только правами по чтению всех настроек межсетевого экрана.

Если требуется, можно создать дополнительные учетные записи для администрирования межсетевого экрана, указав какой из групп принадлежат создаваемые учетные записи.

Система NetDefendOS запрещает одновременный вход более одной учетной записи с правами администратора. Если выполнен вход под одной учетной записью с правами администратора, то вход под второй учетной записью возможен, но при этом предоставляются права только аудита. Другими словами, вторая учетная запись будет обладать только правами чтения настроек без возможности их изменения.



### Сценарии командной строки

Для простоты хранения и выполнения команд администратором, NetDefendOS поддерживает функцию *CLI scripting*. *CLI script* – это записанная в файл последовательность команд, которые можно выполнить после загрузки файла на межсетевой экран.

Для создания CLI script следует выполнить следующие шаги:

1. Создать текстовый файл, содержащим последовательность команд, по одной команде в строке. Для этих файлов рекомендуется использовать расширение `.sgs` (*Security Gateway Script*). Имя файла, включая расширение, не должно содержать более 16 символов.
2. Загрузить файл на межсетевой экран, используя Secure Copy (SCP). Файлы-сценарии должны храниться в папке `scripts`.
3. Использовать команду CLI `script -execute` для выполнения команд из файла.

Команда `script` – это инструментальное средство, используемое для выполнения определенной последовательности команд. Полный синтаксис команды описан в *Руководстве по интерфейсу командной строки CLI*. Рассмотрим некоторые примеры использования данной команды.

В сценариях можно использовать следующие четыре команды: `add`, `set`, `delete`, `cc`.

Если в сценарии появляется любая другая команда, она игнорируется, при этом генерируется сообщение с предупреждением. Например, команда `ping` будет проигнорирована.

С помощью команды `script -execute` запускается указанный в параметре `-name` файл сценария.

```
script -execute -name=my_script.sgs
```

Файл сценария может содержать любое количество *переменных сценария*, которые обозначаются следующим образом:

```
$1, $2, $3, $4 $n
```

Фактические параметры этих переменных указываются в командной строке `script -execute`.

Если в выполняемом файле сценария возникает ошибка, то по умолчанию сценарий будет прерван. С помощью опции `-force` сценарий будет продолжен даже при возникновении ошибки.

```
script -execute -name=my_script2.sgs -force
```

Все выходные данные выполненного сценария появляются в консоли командной строки. По умолчанию эти выходные данные состоят из сообщений обо всех ошибках, которые произошли во время выполнения. Для вывода на консоль подтверждения выполнения каждой команды используется опция `-verbose`.

```
script -execute -name=my_script2.sgs -verbose
```

При загрузке файла сценария на межсетевой экран, сначала он хранится только в памяти RAM. При перезапуске NetDefendOS все загруженные сценарии будут уничтожены в энергозависимой памяти, и для их следующего выполнения потребуется повторная загрузка. Для сохранения сценариев после перезапусков следует переместить их в энергонезависимую память с помощью команды `script -store`.

```
script -store -name=my_script.sgs
```

Если требуется переместить в энергонезависимую память все сценарии, то используется команда.

```
script -store -all
```

Для удаления сценария используется команда `script -remove`.

Команда **script** без параметров отображает список всех сценариев, размер каждого сценария и тип памяти, в которой хранится сценарий (**Disk** или **Memory**).

Для вывода на консоль содержимого файла сценария используется команда.

```
script -show -name=<имя файла>
```

#### *Автоматическое создание сценариев*

Когда необходимо выполнить создание одних и тех же объектов конфигурации на нескольких межсетевых экранах, следует создать файл сценария и запустить его на каждом устройстве.

Команда

```
script -create <object_type>
```

автоматически создает файл сценария, который содержит команду **add** всех объектов указанного типа, существующих в межсетевом экране.

Например, для создания всех объектов **IP4Address** с одними и теми же параметрами на нескольких межсетевых экранах следует выполнить команду.

```
script -create Address IP4Address -name new_script.sgs
```

Файл **new\_script.sgs** может быть загружен на локальную рабочую станцию и затем скачен и активирован на других межсетевых экранах. После этого у всех устройств в адресных книгах будут находиться одни и те же объекты **IP4Address**.

Некоторые параметры конфигурации, зависящие от аппаратного обеспечения, не могут быть автоматически записаны в сценарий с помощью параметра **-create**.

Строка в файле сценария, которая начинается с символа **#**, является комментарием.

#### *Сценарии, вызывающие другие сценарии*

Один сценарий может вызывать другой. Например, сценарий **my\_script.sgs** может содержать строку.

```
script -execute -name my_script2.sgs
```

Максимальное количество вложенных сценариев – 5.

#### *Дата и время*

##### *Обзор*

Корректная установка даты и времени важны для правильной работы системы межсетевого экрана. Политики по расписанию, авто-обновления IDP и баз данных антивируса, а также других функций продукта требуется точно установленное системное время.

Кроме того, сообщения журнала отмечаются временной меткой для того, чтобы указать, когда произошло определенное событие. Кроме того, время должно быть синхронизировано с другими устройствами в сети.

##### *Протоколы синхронизации времени*

Поддерживается использование протоколов синхронизации времени для автоматической регулировки системных часов с помощью ответов на запросы, отправляемые через интернет, на специальные внешние серверы, которые называют сервера времени (Time Servers).

## Установка даты и времени и установка часового пояса

Установить дату и время можно вручную, это рекомендуется при первоначальном запуске системы.

### Веб-интерфейс:

System → Date and Time

The screenshot shows the 'Date and Time' configuration page. The title is 'Date and Time' with a subtitle 'Set the date, time and time zone information for this system.' The page is divided into sections: 'General', 'Time zone and daylight saving time settings', and 'Automatic time synchronization'. In the 'General' section, the 'Current Date and Time' is '2012-12-20 12:35:43' and there is a 'Set Date and Time' button. In the 'Time zone and daylight saving time settings' section, the 'Time zone' is set to '(GMT+04:00)'. There is an unchecked checkbox for 'Enable daylight saving time' and an 'Offset' of '60 minutes'. The 'Start Date' is 'March 1' and the 'End Date' is 'October 1'. In the 'Automatic time synchronization' section, 'Disabled' is selected, and the 'Time Server Type' is 'SNTP' and the 'Primary Time Server' is '(None)'. Red boxes highlight the 'Set Date and Time' button and the 'Time zone' dropdown.

The screenshot shows the 'Set Date and Time' dialog box. It has a title bar 'Set Date and Time'. The 'Date' field is set to '2014 - May - 6' and the 'Time' field is set to '11:43:33 (HH:MM:SS)'. There are 'OK' and 'Cancel' buttons at the bottom. A red box highlights the date and time input fields.

### Командная строка:

```
time -set YYYY-mm-DD HH:MM:SS  
set DateTime Timezone=GMTplus4
```

### Серверы времени (Time Servers)

Для корректировки аппаратных часов используются сервера времени, с помощью которых возможна автоматическая настройка времени, полученного от одного или нескольких серверов, которые предоставляют точное время.

Поддерживаются следующие протоколы синхронизации времени:

- **SNTP**

Определяется стандартом RFC 2030, простой сетевой протокол синхронизации времени – реализация NTP (RFC 1305). NetDefendOS использует данный протокол для запросов к NTP-серверам.

- **UDP/TIME**

Протокол времени - Time Protocol (UDP/TIME) – более ранний протокол, также обеспечивающий синхронизацию времени через интернет.

Большинство серверов времени поддерживают NTP или SNTP-протоколы.

Могут быть указаны максимально три сервера времени. Если используется более одного сервера для синхронизации времени, то можно избежать ситуации. Когда синхронизация невозможна из-за недоступности одного из серверов. Система получает информацию со всех доступных серверов и вычисляет среднее время.

### Максимальная величина корректировки времени

Чтобы избежать установления некорректного времени, которое может произойти при синхронизации с неисправным сервером, можно установить максимальную величину корректирования времени (*Maximum Adjustment*) (в секундах). Если разница между текущим временем системы и временем, полученным с сервера, будет больше заданной максимальной величины, то данные, полученные с сервера, будут отклонены. Например, значение максимального времени установки равно 60 секунд и текущее время системы NetDefendOS составляет 16:42:35. Если время, полученное с сервера: 16:43:38, то разница составляет 63 секунды, что превышает максимальную величину, т.е. текущее время не будет обновлено.

### Веб-интерфейс:

System → Date and Time

**Automatic time synchronization**

Disabled  
 D-Link (pre-configured timesyno server)  
 Custom

Time Server Type:

Primary Time Server:

Secondary Time Server:

Tertiary Time Server:

Interval between each synchronization:  seconds

**Maximum time drift that a server is allowed to adjust:  seconds**

Interval according to which server responses will be grouped:  seconds



### Командная строка:

```
set DateTime TimeSyncMaxAdjust=40000
```

Значение максимальной регулировки времени можно отключить.

```
time -sync -force
```

При необходимости можно изменить интервал между попытками синхронизации. По умолчанию интервал равен 86 400 секунд (1 день).

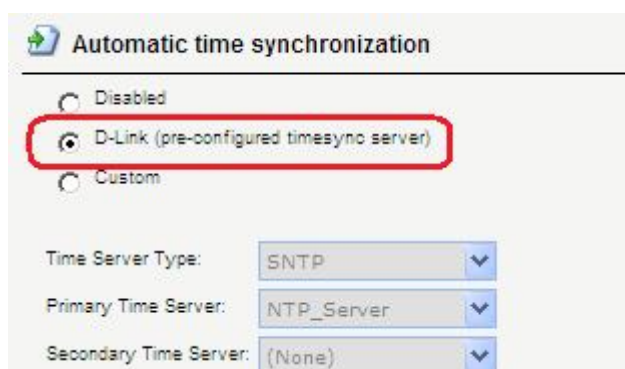
### Серверы синхронизации времени D-Link

При работе с системой NetDefendOS для синхронизации времени рекомендуется использовать серверы синхронизации времени D-Link, путь к которым прописан в опциях системы. Серверы D-Link взаимодействуют с системой по протоколу SNTP.

Когда опция D-Link Server включена, синхронизация осуществляется автоматически.

### Веб-интерфейс:

System → Date and Time



### Командная строка:

```
set DateTime TimeSynchronization=D-Link
```

Следует помнить, что для работы с серверами синхронизации времени D-Link необходимо настроить сервис DNS.

### Серверы DNS

Если в системе настроены DNS-сервера, то вместо IP-адреса можно указывать соответствующее доменное (FQDN) имя.

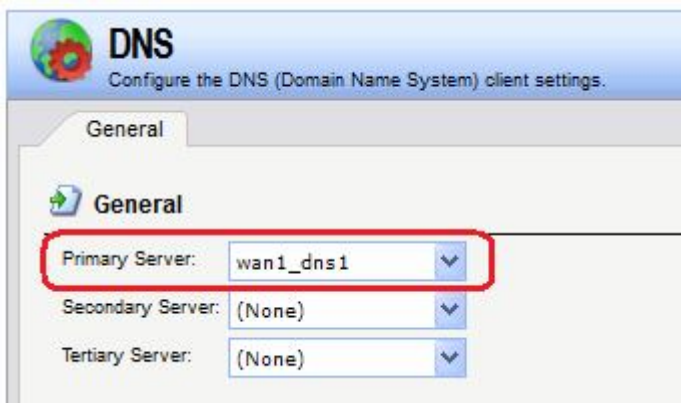
Система NetDefendOS является DNS-клиентом и может использовать три DNS-сервера: Primary Server (первичный сервер), Secondary Server (вторичный сервер) и Tertiary Server (третий сервер).

Настройка хотя бы одного DNS-сервера необходима для функционирования следующих модулей системы NetDefendOS:

- Автоматическая синхронизация времени.
- Доступ к CA для получения сертификатов.
- Доступ к внешним сервисам, содержащим различные базы данных сигнатур, используемые в системе (антивирусные или IDP).

### Веб-интерфейс:

System → DNS



### Командная строка:

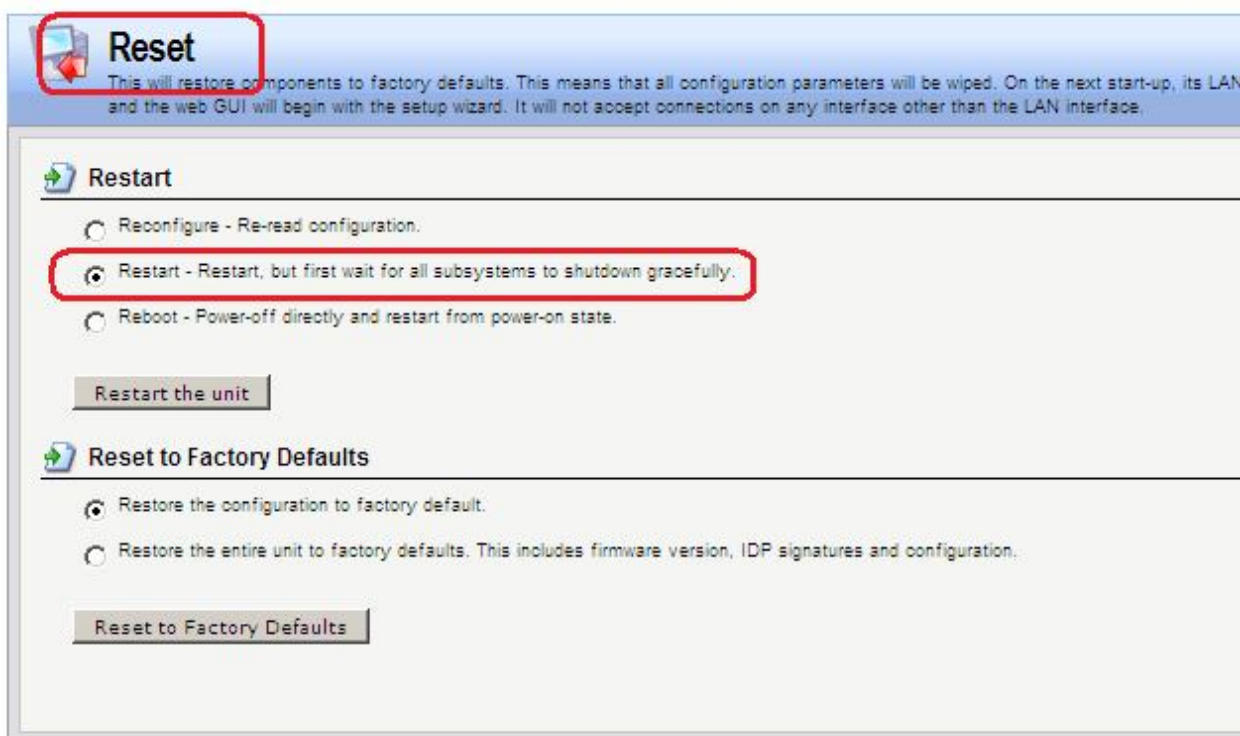
```
set DNS DNSServer1=wan1/wan1_dns1
```

### Перезапуск межсетевого экрана, сброс к заводским настройкам по умолчанию

Сброс к заводским настройкам по умолчанию выполняется для возврата к первоначальным настройкам межсетевого экрана. При выполнении сброса настроек все данные, такие, как база данных провайдера и антивирусная база данных, будут утеряны и должны быть повторно загружены.

### Веб-интерфейс:

Maintenance → Reset



### Командная строка:

```
reset -unit
```

### Активация и применение изменений

После внесения изменений в конфигурацию следует выполнить команды **activate** и **commit**.

Если в течение 30 секунд (по умолчанию) не выполнена команда `commit`, выполненные изменения автоматически отменяются, и происходит восстановление прежних настроек.

### *Управление сессиями с помощью команды `sessionmanager`*

Интерфейс командной строки предоставляет команду `sessionmanager` для управления сессиями. Команда используется для управления всеми типами сессий:

- Сессии командной строки, созданные при использовании протокола SSH.
- Сессия командной строки, созданные через интерфейс серийной консоли RS232.
- Сессии, созданные при использовании протокола Secure Copy (SCP).
- Сессии веб-интерфейса, созданные при использовании протокола HTTP или HTTPS.

Команда без каких-либо опций предоставляет краткую информацию о текущих открытых сессиях. Для просмотра списка всех сессий используется опция `-list`.

#### **Командная строка:**

```
sessionmanager
```

```
sessionmanager -list
```

Если пользователь обладает правами администратора, можно завершить любую сессию с помощью опции `-disconnect`.

### *Поиск неисправностей - команда `pcapdump`*

Важным инструментом диагностики является анализ пакетов, проходящих через интерфейсы межсетевого экрана. Для этого используется команда `pcapdump`, которая позволяет записать поток пакетов, проходящих через интерфейсы, и выполнить фильтрацию этих потоков в соответствии с определенными критериями.

Примеры использования `pcapdump`:

1. Освобождение памяти, использованной командой `pcapdump` и удаление всех файлов, которые были ранее сохранены с помощью команды `pcapdump`.

```
pcapdump -cleanup
```

2. Запись в буфер в оперативной памяти межсетевого экрана всех пакетов, проходящих через интерфейс `lan`. Если интерфейс не указан, то будет выполнен перехват всех пакетов, проходящих через все интерфейсы.

```
pcapdump -start lan
```

3. Запись всех пакетов, прошедших через интерфейс `lan`, из буфера в оперативной памяти в файл `lan_int.cap`. Данные файлы находятся в корневой папке межсетевого экрана.

```
pcapdump -write lan -filename=lan_int.cap
```

4. Отображение перехваченных пакетов в консоли.

```
pcapdump -show
```

5. Останов перехвата пакетов, проходящих через интерфейс `lan`. Если интерфейс не указан, то будет выполнен останов перехвата пакетов, проходящих через все интерфейсы.

```
pcapdump -stop lan
```

### Загрузка выходного файла

После того, как сохранены в файле межсетевых экранов, их следует переписать, например, с помощью программы `scp`, на рабочую станцию.

Для дальнейшего анализа пакетов рекомендуется использовать программу **Wireshark** (ранее известную как *Ethereal*). Данная программа является приложением с открытым исходным кодом и использует библиотеку *Pcap*.

Для получения более подробной информации о программе **Wireshark**, см сайт <http://www.wireshark.org>.

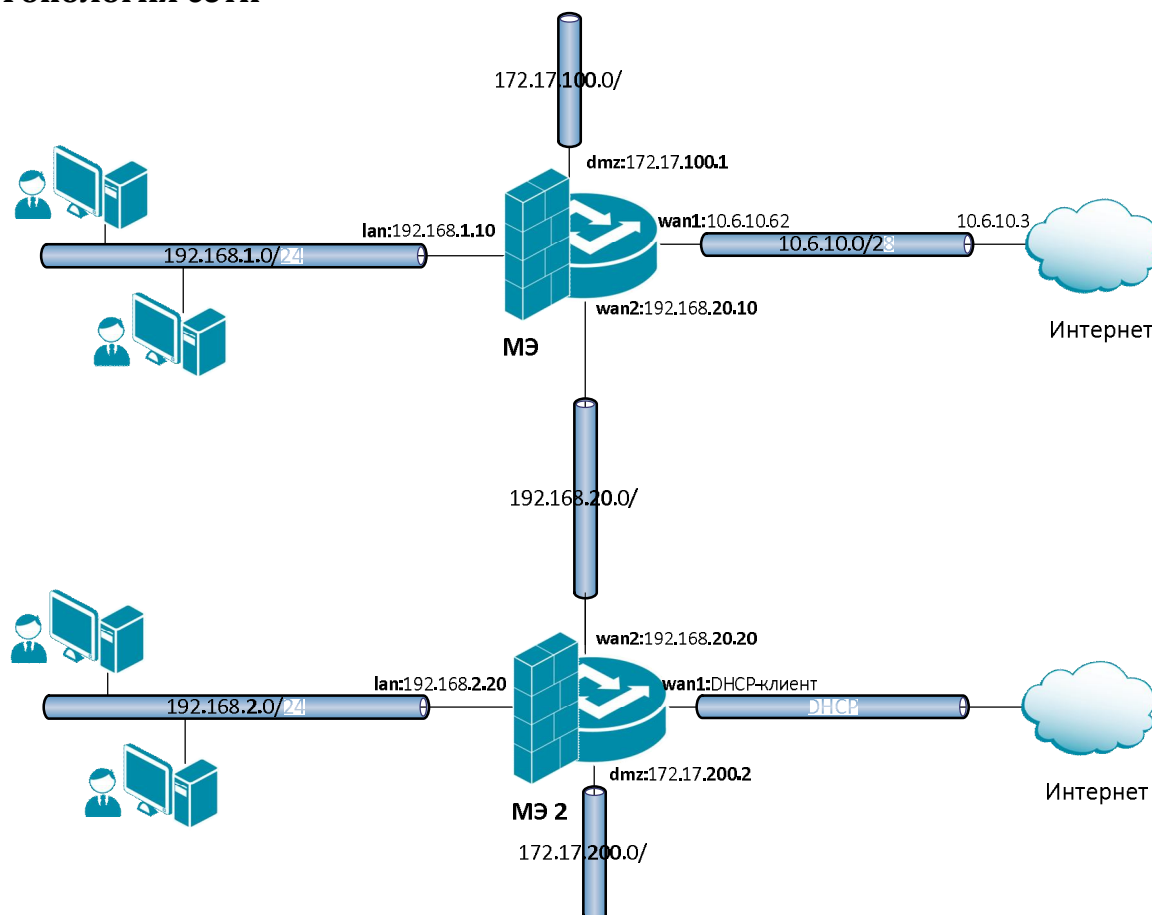
## Лабораторная работа 2. Соединение двух локальных сетей, расположенных за межсетевыми экранами

### Цель

Создать топологию сети, в которой два межсетевых экрана соединяют локальные сети, обеспечивая доступ в локальные сети друг друга и доступ в интернет через одного провайдера.

1. Настроить сервисы DNS на обоих межсетевых экранах.
2. Разрешить доступ из обеих локальных сетей в интернет.
3. Разрешить доступ из локальных сетей к lan-интерфейсам каждого межсетевого экрана и к рабочим станциям в локальных сетях.

### Топология сети



На Межсетевом Экране 1 (МЭ 1) используются четыре интерфейса, которые обозначены `lan`, `dmz`, `wan1` и `wan2`.

Интерфейс **lan** имеет IP-адрес **192.168.1.10** и соединен с подсетью **192.168.1.0/24**, в которой расположены рабочие станции пользователей.

Интерфейс **dmz** имеет IP-адрес **172.17.100.1**, в текущей топологии к нему не подсоединена никакая сеть.

Интерфейс **wan1** имеет IP-адрес **10.6.10.62** и соединен с подсетью **10.6.10.0/28** со шлюзом провайдера, который обеспечивает выход в интернет и имеет IP-адрес **10.6.10.3**.

Интерфейс **wan2** имеет IP-адрес **192.168.20.10** и соединен с подсетью **192.168.20.0/24**, в которой расположен Межсетевой Экран 2 (**МЭ 2**) с IP-адресом **192.168.20.20**.

На Межсетевом Экране 2 (**МЭ 2**) используются четыре интерфейса, которые обозначены **lan**, **dmz**, **wan1** и **wan2**.

Интерфейс **lan** имеет IP-адрес **192.168.2.20** и соединен с подсетью **192.168.2.0/24**, в которой расположены рабочие станции пользователей.

Интерфейс **dmz** имеет IP-адрес **172.17.200.2**, в текущей топологии к нему не подсоединена никакая сеть.

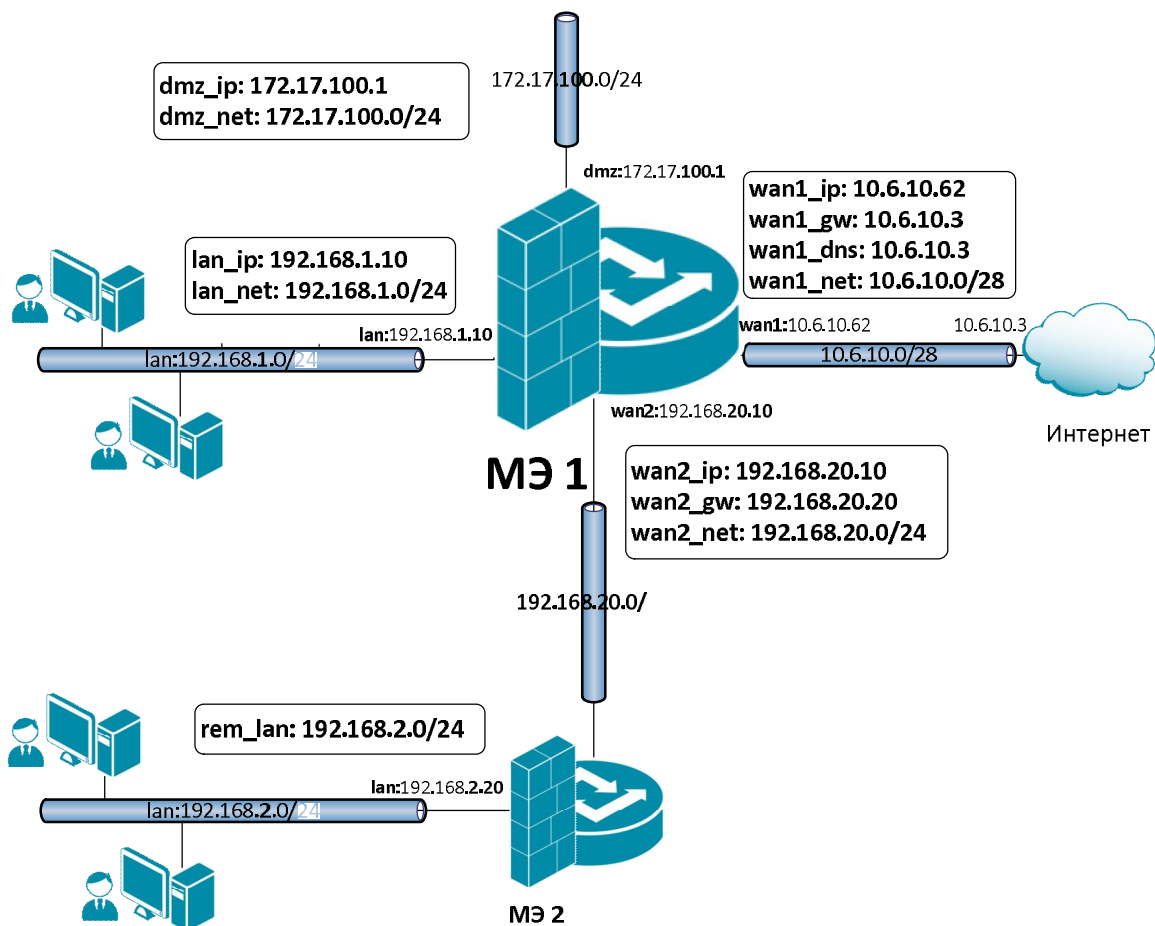
Интерфейс **wan1** является DHCP-клиентом, который получает IP-адрес, маску подсети, шлюз по умолчанию и IP-адрес DNS-сервера от DHCP-сервера провайдера.

Интерфейс **wan2** имеет IP-адрес **192.168.20.20** и соединен с подсетью **192.168.20.0/24**, в которой расположен Межсетевой Экран 1 (**МЭ 1**) с IP-адресом **192.168.20.10**.

## **Описание практической работы**

### ***Сервисы DNS***

#### **Межсетевой Экран 1**



На МЭ1 весь DNS-трафик из своей локальной сети и удаленной локальной сети должен перенаправляться на DNS-сервер провайдера, поэтому Межсетевой Экран 1 должен знать IP-адрес DNS-сервера провайдера. Необходимо выполнить следующие настройки:

1. В Адресной Книжке создать необходимые объекты.
2. Для удобства конфигурирования объединить в одну группу интерфейсы, которые требуют одинаковых Правил фильтрации.
3. Создать Правила фильтрации, перенаправляющие DNS-трафик из локальной сети и dmz-сети к DNS-серверу.
4. При необходимости в таблицу маршрутизации добавить маршруты.

#### *Объекты Адресной Книжки*

В Адресной Книжке создать необходимые объекты.

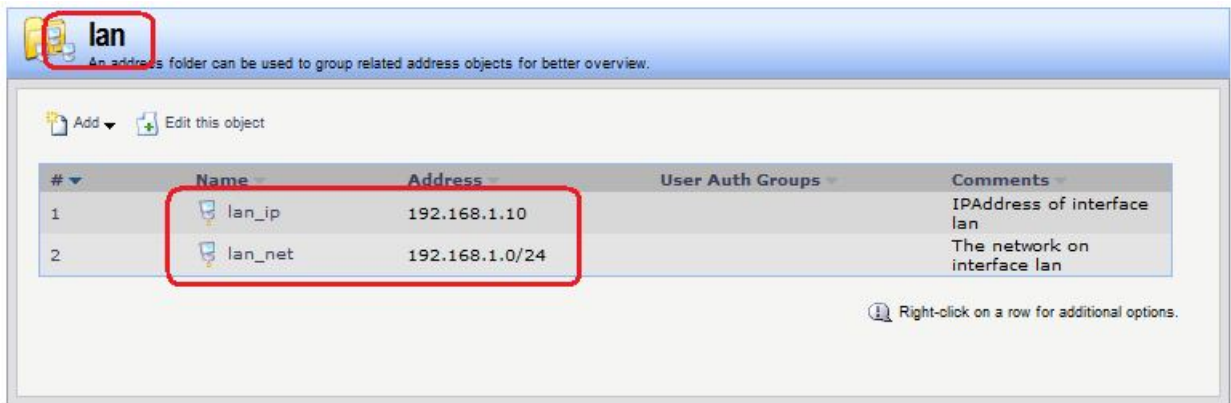
1. Объекты интерфейса **lan**.

#### **Веб-интерфейс:**

Object → Address Book → Add → Address Folder

Name: lan

Object → Address Book → lan



### Командная строка:

```
add Address AddressFolder lan Comments=lan
```

```
cc Address AddressFolder lan
```

```
add IP4Address lan_ip Address=192.168.1.10 Comments='IPAddress of interface lan'
```

```
add IP4Address lan_net Address=192.168.1.0/24 Comments='The network on interface lan'
```

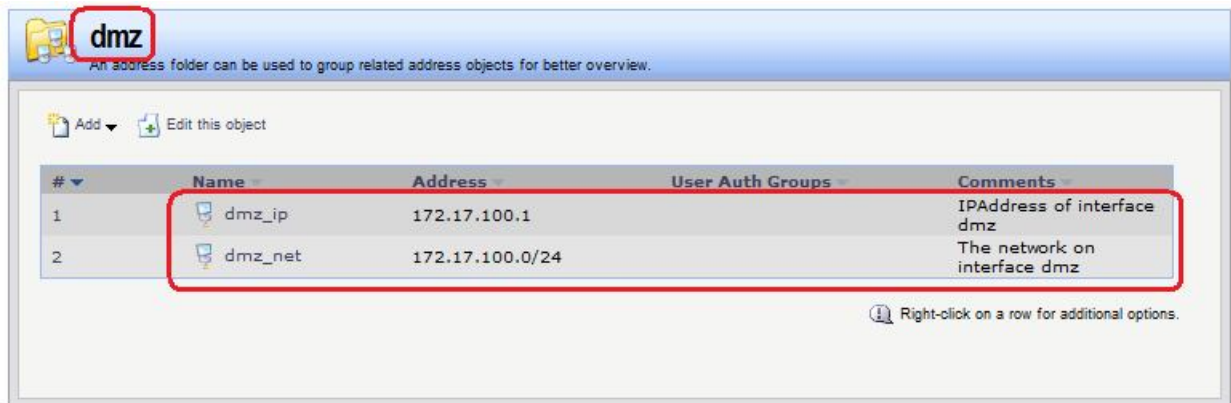
### 2. Объекты интерфейса dmz.

#### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: dmz

Object → Address Book → lan



### Командная строка:

```
add Address AddressFolder dmz Comments=dmz
```

```
cc Address AddressFolder dmz
```

```
add IP4Address dmz_ip Address=172.17.100.1 Comments='IPAddress of interface dmz'
```

```
add IP4Address dmz_net Address=172.17.100.0/24 Comments='The network on interface dmz'
```

### 3. Объекты интерфейса wan1.

#### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: wan1

Object → Address Book → wan1



### Командная строка:

```
add Address AddressFolder wan1 Comments=wan1
cc Address AddressFolder wan1
add IP4Address wan1_ip Address=10.6.10.62 Comments='IPAddress of interface wan1'
add IP4Address wan1_gw Address=10.6.10.3 Comments='Default gateway for interface wan1'
add IP4Address wan1_dns1 Address=10.6.10.3 Comments='Primary DNS server for interface wan1'
add IP4Address wan1_net Address=10.6.10.0/28 Comments='The network on interface wan1'
```

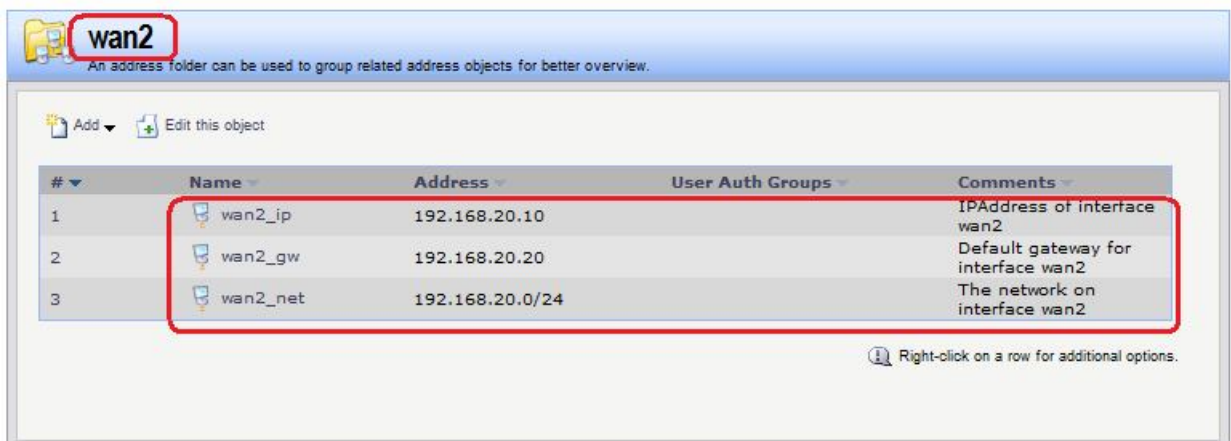
4. Объекты интерфейса wan2.

### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: wan2

Object → Address Book → wan2



### Командная строка:

```
add Address AddressFolder wan2 Comments=wan2
cc Address AddressFolder wan2
```



```
add IP4Address wan2_ip Address=192.168.20.10 Comments='IPAddress of interface wan2'

add IP4Address wan2_gw Address=192.168.20.20 Comments='The network on interface wan2'

add IP4Address wan2_net Address=192.168.20.0/24 Comments='The network on interface wan2'
```

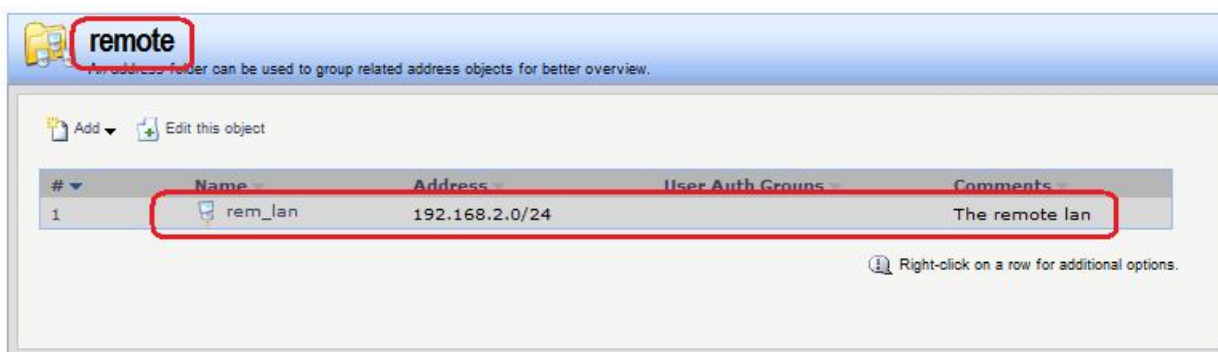
5. Объекты, описывающие LAN-сеть, расположенную за МЭ 2.

### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: remote

Object → Address Book → rem\_lan



### Командная строка:

```
add Address AddressFolder remote Comments='The remote objects'
cc Address AddressFolder remote
add IP4Address rem_lan Address=192.168.2.0/24 Comments='The remote lan'
```

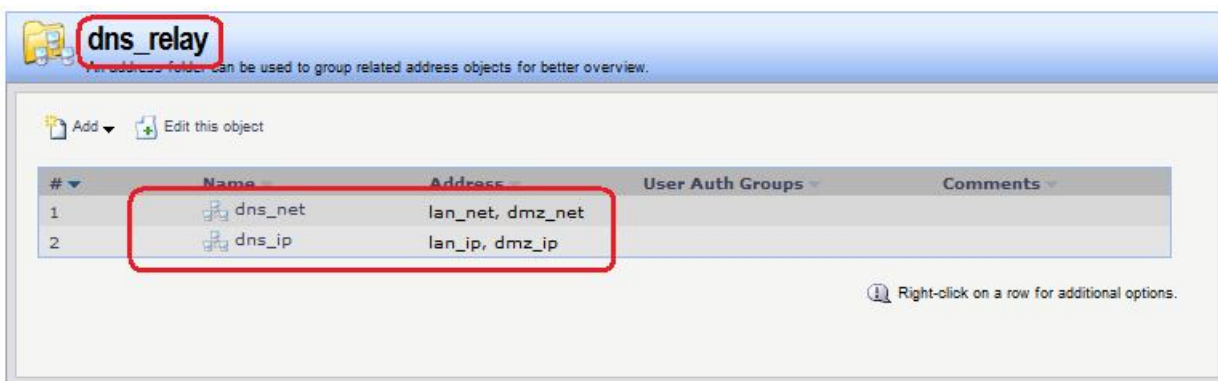
6. Дополнительные объекты, необходимые для удобства администрирования и объединяющие в одну группу сети и IP-адреса, которые необходимы одинаковые сервисы DNS.

### Веб-интерфейс:

Object → Address Book → InterfaceAddresses → Add

```
add Address AddressFolder dns_relay Comments='DNS services'
```

```
cc Address AddressFolder dns_relay
```



### Командная строка:

```
add Address AddressFolder dns_relay Comments='DNS services'
cc Address AddressFolder dns_relay
```

```
add IP4Group dns_net Members =lan/lan_net, dmz/dmz_net
```

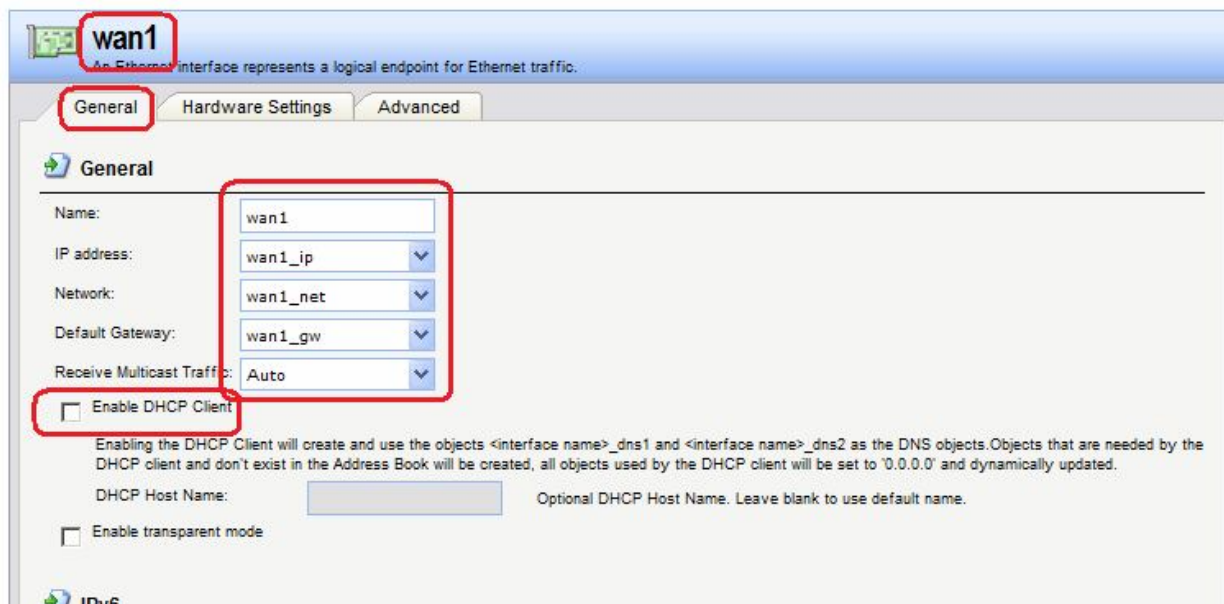
```
add IP4Group dns_ip Members = lan/lan_ip, dmz/dmz_ip
```

### Привязка созданных объектов Адресной Книги к интерфейсам

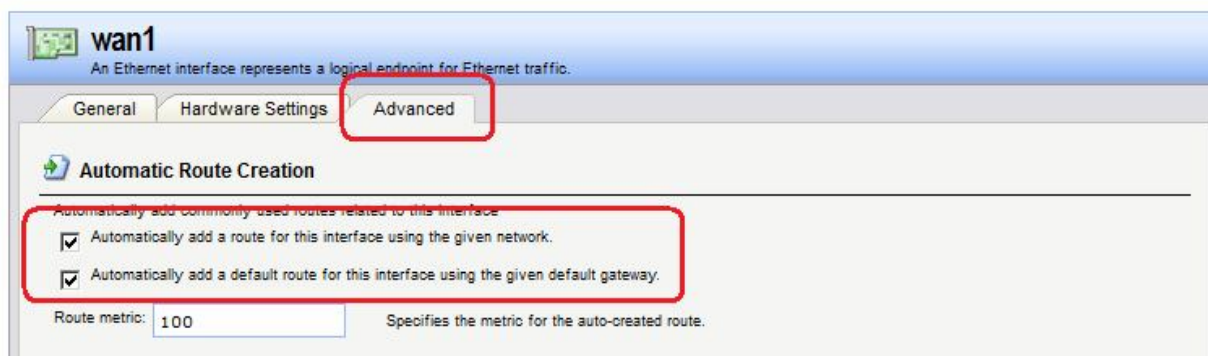
Объекты, созданные в пунктах 1, 2, 3 и 4, должны быть привязаны к соответствующим Ethernet-интерфейсам.

### Веб-интерфейс:

Interfaces → Ethernet → wan1



Если IP-адрес данного интерфейса должен быть получен по протоколу DHCP, то следует установить соответствующий флаг «**Enable DHCP Client**».



На вкладке **Advanced** рекомендуется добавить флаг автоматического добавления маршрута к указанной сети, используя данный интерфейс. Для интерфейса **wan1** следует также установить флаг добавления маршрута по умолчанию к указанному шлюзу через данный интерфейс.

Аналогично привязать созданные объекты к другим интерфейсам.

### Командная строка:

```
set Interface Ethernet lan IP=lan/lan_ip Network=lan/lan_net  
AutoInterfaceNetworkRoute=yes
```

```
set Interface Ethernet dmz IP=dmz/dmz_ip Network=dmz/dmz_net  
AutoInterfaceNetworkRoute=yes
```

```
set Interface Ethernet wan1 IP=wan1/wan1_ip Network=wan1/wan1_net
DefaultGateway=wan1/wan1_gw Name=wan1 AutoInterfaceNetworkRoute=yes
AutoDefaultGatewayRoute=yes
```

```
set Interface Ethernet wan2 IP=wan2/wan2_ip Network=wan2/wan2_net
DefaultGateway=wan2/wan2_gw Name=wan2 AutoInterfaceNetworkRoute=yes
```

В результате заданы следующие параметры интерфейсов:

#	Name	IPv4 Address	IPv6 Address	Network	Default Gateway	Enable DHCP Client	Comments
1	lan	lan_ip		lan_net		No	
2	dmz	dmz_ip		dmz_net		No	
3	wan1	wan1_ip		wan1_net	wan1_gw	No	
4	wan2	wan2_ip		wan2_net	wan2_gw	No	

Таблица маршрутизации следующая:

Routing Table: <main>

Show all routes:  (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: 100

Apply

**IPv4 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
	10.6.10.0/28	wan1			100
	192.168.20.0/24	wan2			100
	172.17.100.0/24	dmz			100
	192.168.1.0/24	lan			100
	0.0.0.0/0	wan1	10.6.10.3		100

**IPv6 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

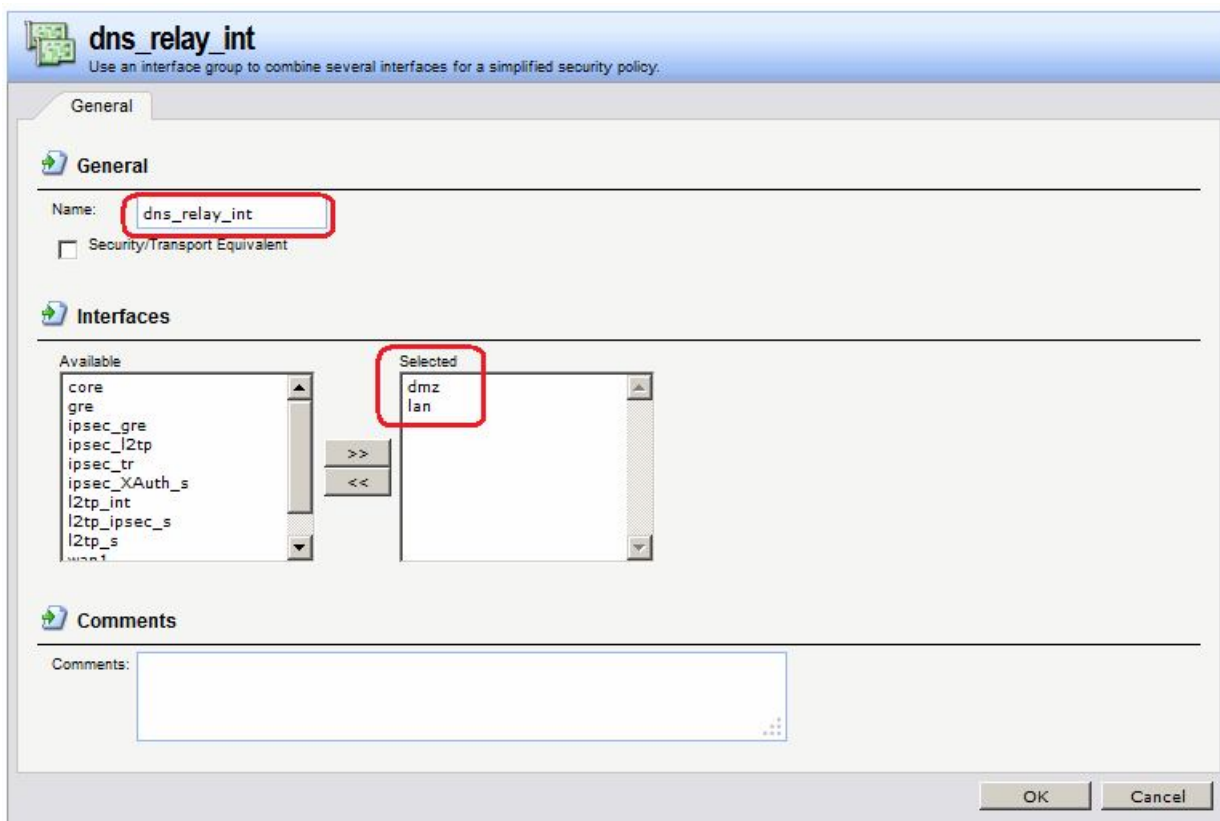
In the "Flags" field of the routing tables, the following letters are used:  
 O: Learned via OSPF X: Route is Disabled  
 M: Route is Monitored A: Published via Proxy ARP  
 D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

### Группа интерфейсов

Объединить интерфейсы в Группу, чтобы несколько интерфейсов можно было указывать одним параметром в Правилах фильтрации.

### Веб-интерфейс:

Interfaces → Interface Group → Add



### Командная строка:

```
add Interface InterfaceGroup dns_relay_int Members=lan,dmz
```

### Правила фильтрации

Создать Правила, перенаправляющие DNS-трафик из локальных сетей к DNS-серверу в интернете. Это можно сделать несколькими способами:

1. Создать правила **SAT** и **NAT** для каждого интерфейса, соединенному с сетями, которым необходим сервис DNS. В качестве сети источника следует указать сеть (группу сетей), которой требуется сервис DNS. В качестве сети назначения следует указать IP-адрес интерфейса.

Правило **SAT** заменяет IP-адрес получателя на IP-адрес, указанный на вкладке **SAT**.

На вкладке **SAT** в качестве адреса назначения следует указать IP-адрес DNS-сервера.

### Веб-интерфейс:

```
Rules → IP Rules → Add → IP Rule Folder
```

```
    Name: dns_relay_multi
```

```
Rules → IP Rules → dns_relay_multi
```

**dns\_relay\_multi**  
An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

Add Edit this object

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	sat_dns_lan	SAT	lan	lan_net	core	lan_ip	dns-all
2	nat_dns_lan	NAT	lan	lan_net	core	lan_ip	dns-all
3	sat_dns_dmz	SAT	dmz	dmz_net	core	dmz_ip	dns-all
4	nat_dns_dmz	NAT	dmz	dmz_net	core	dmz_ip	dns-all

Right-click on a row for additional options.

**sat\_dns\_lan**  
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

**General**

Name: sat\_dns\_lan

Action: SAT NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Service: dns-all

Schedule: (None)

**Address Filter**

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

Source: Interface: lan Network: lan\_net

Destination: core lan\_ip

**Comments**

Comments:

OK Cancel

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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

**General**

Translate the

Source IP

Destination IP

to:

New IP Address: wan1\_dns1

New Port:

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

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

OK Cancel

## Командная строка:

```
add IPRuleFolder Name=dns_relay_multi
cc IPRuleFolder <N folder>

add IPRule Action=SAT SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=core DestinationNetwork=lan/lan_ip Service=dns-all
SATTranslateToIP=wan1/wan1_dns1 Name=sat_dns_lan

add IPRule Action=NAT SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=core DestinationNetwork=lan/lan_ip Service=dns-all
Name=nat_dns_lan

add IPRule Action=SAT SourceInterface=dmz SourceNetwork=dmz/dmz_net
DestinationInterface=core DestinationNetwork=dmz/dmz_ip Service=dns-all
SATTranslateToIP=wan1/wan1_dns1 Name=sat_dns_dmz

add IPRule Action=NAT SourceInterface=dmz SourceNetwork=dmz/dmz_net
DestinationInterface=core DestinationNetwork=dmz/dmz_ip Service=dns-all
Name=nat_dns_dmz
```

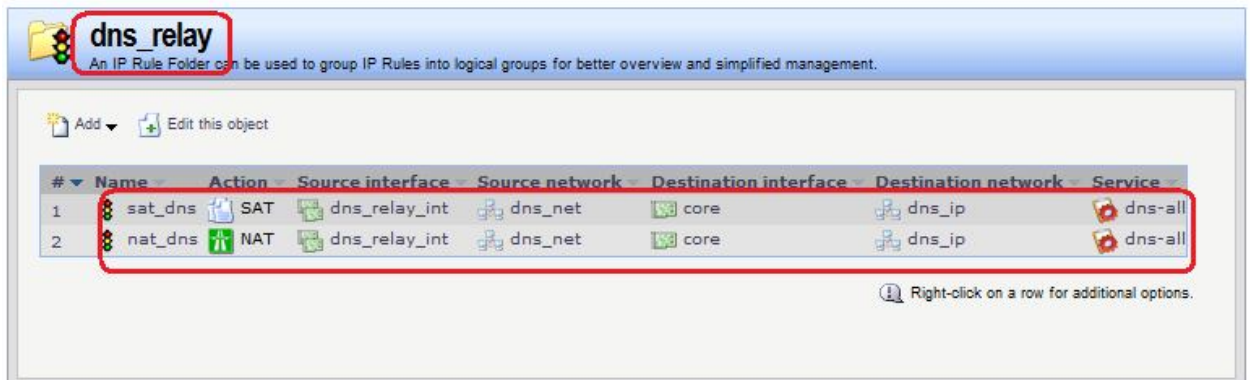
2. Использовать созданные группы IP-сетей, IP-адресов и интерфейсов, для сетей которых необходим сервис DNS. В этом случае будет достаточно одной пары правил SAT-NAT.

## Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: dns\_relay

Rules → IP Rules → dns\_relay → Add



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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

**General**

Name:

Action:  NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Service:

Schedule:

**Address Filter**

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

Source: Interface:  Network:

Destination:

**Comments**

Comments:

OK Cancel

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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

**General**

Translate the

Source IP

Destination IP

to:

New IP Address:

New Port:

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

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

OK Cancel

Второе Правило зависит от требований провайдера. На МЭ 1 указано правило **NAT**. В этом случае провайдер видит только IP-адрес интерфейса **wan1** МЭ1.

### Командная строка:

```
add IPRuleFolder Name=dns_relay
cc IPRuleFolder <N folder>

add IPRule Action=SAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip Service=dns-all SATAllToOne=Yes
SATTranslateToIP=wan1/wan1_dns1 Name=sat_dns

add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip Service=dns-all Name=nat_dns
```

Результирующий трафик следующий.

На интерфейс **lan** приходит трафик:

159	6.580000	192.168.1.121	192.168.1.10	DNS	70	Standard query A www.rbc.ru
160	6.580000	192.168.1.10	192.168.1.121	DNS	196	Standard query response A 194.186.25.27 A 195.

С интерфейса **wan1** уходит трафик:

164	6.530000	10.6.10.62	10.6.10.3	DNS	70	Standard query A www.rbc.ru
165	6.530000	10.6.10.3	10.6.10.62	DNS	196	Standard query response A 194.186.2

1. Адрес получателя тот, который указан на вкладке **SAT** правила **SAT**.
2. Адрес отправителя соответствует правилу **NAT**.

### Статическая маршрутизация

В таблице маршрутизации уже существуют маршруты ко всем сетям, которые непосредственно доступны с интерфейсов. В результате таблица маршрутизации на МЭ1 выглядит следующим образом:

**Routing Table Contents**

Routing Table: **<main>**

Show all routes:  (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: **100**

**Apply**

**IPv4 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
	10.6.10.0/28	wan1			100
	192.168.20.0/24	wan2			100
	172.17.100.0/24	dmz			100
	192.168.1.0/24	lan			100
	0.0.0.0/0	wan1	10.6.10.3		100

**IPv6 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

In the "Flags" field of the routing tables, the following letters are used:  
O: Learned via OSPF X: Route is Disabled  
M: Route is Monitored A: Published via Proxy ARP  
D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

### Проверка доступности DNS-сервисов из локальной сети

Проверить из командной строки на рабочей станции, расположенной в локальной сети, возможность обрабатывать DNS-запросы с помощью команды **nslookup**:



```

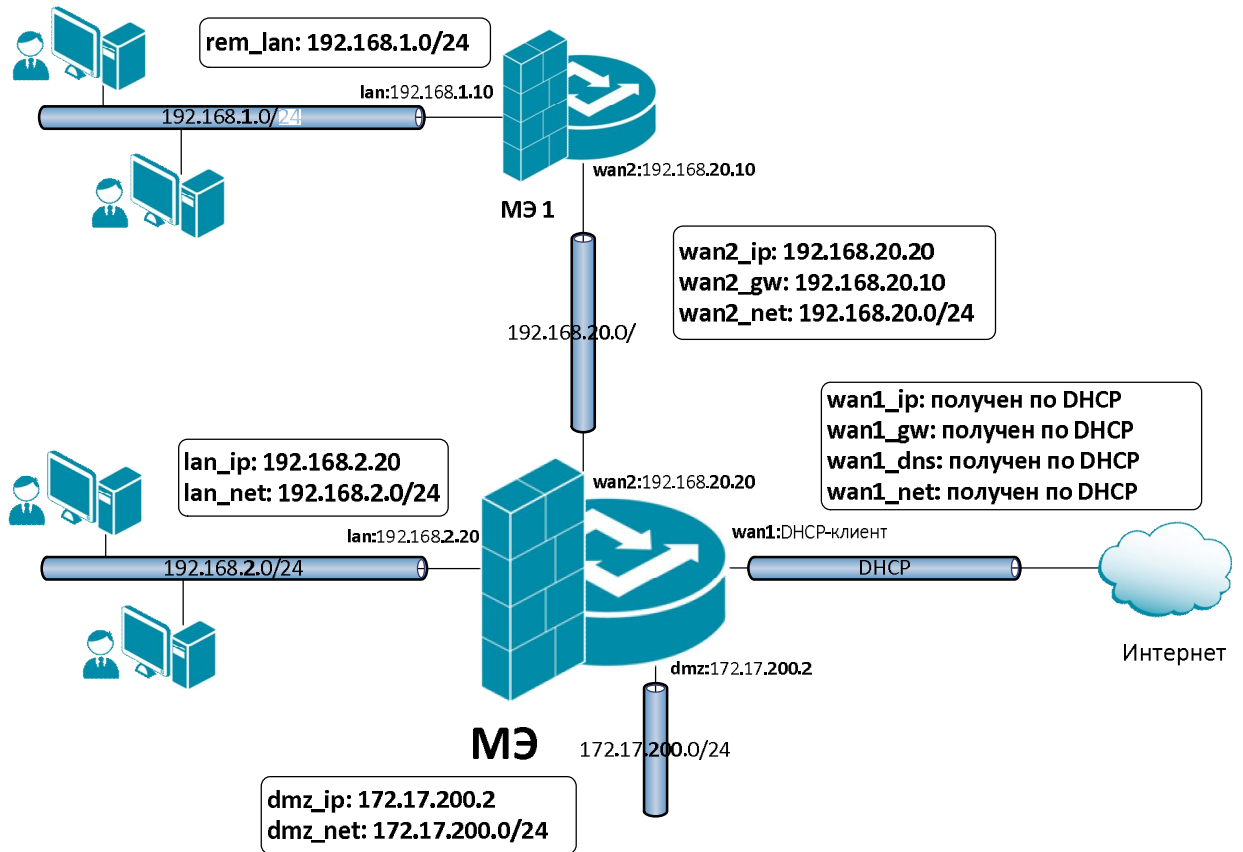
Command Prompt - nslookup
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>nslookup
Default Server: UnKnown
Address: 192.168.1.10

> rbc.ru
Server: UnKnown
Address: 192.168.1.10

Non-authoritative answer:
Name: rbc.ru
Addresses: 194.186.25.27
           195.16.126.158
           194.186.25.25

```

## Межсетевой Экран 2



На Межсетевом Экране 2 следует выполнить аналогичные настройки.

1. В Адресной Книжке создать необходимые объекты.
2. Для удобства конфигурирования объединить в одну группу интерфейсы, которые требуют одинаковых правил фильтрации.
3. Создать правила, перенаправляющие DNS-трафик из локальной сети и dmz-сети к DNS-серверу.
4. При необходимости в таблицу маршрутизации добавить маршруты.

## Объекты Адресной Книги

В Адресной Книге создать необходимые объекты.

1. Объекты интерфейса lan.

### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: lan

Object → Address Book → lan



### Командная строка:

```
add Address AddressFolder lan
```

```
cc Address AddressFolder lan
```

```
add IP4Address lan_ip Address=192.168.2.20 Comments='IPAddress of interface lan'
```

```
add IP4Address lan_net Address=192.168.2.0/24 Comments='The network on interface lan'
```

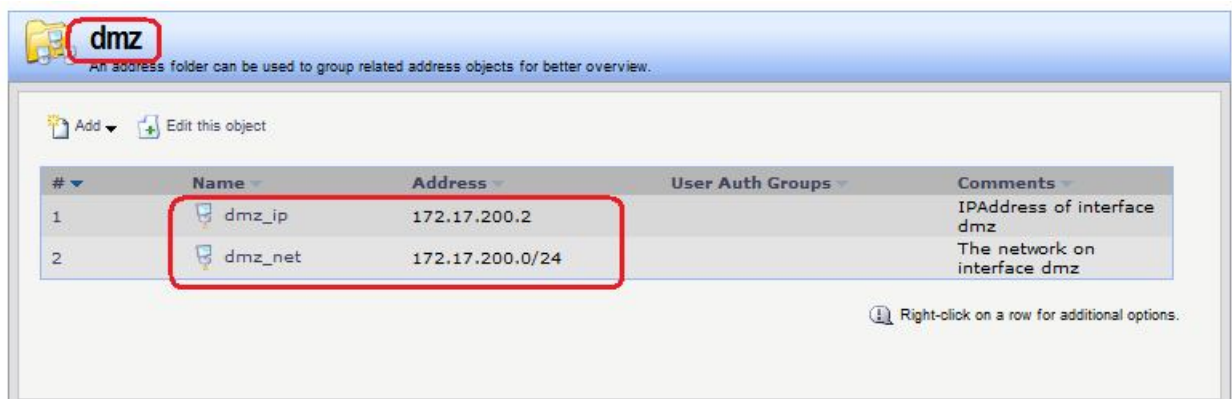
2. Объекты интерфейса dmz.

### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: dmz

Object → Address Book → dmz



### Командная строка:

```
add Address AddressFolder dmz
```

```
cc Address AddressFolder dmz
```

```
add IP4Address dmz_ip Address=172.17.200.20 Comments='IPAddress of interface dmz'
```

```
add IP4Address dmz_net Address=172.17.200.0/24 Comments='The network on interface dmz'
```

### 3. Объекты интерфейса wan2.

#### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: wan2

Object → Address Book → wan2



#### Командная строка:

```
add Address AddressFolder wan2
```

```
cc Address AddressFolder wan2
```

```
add IP4Address wan2_ip Address=192.168.20.20 Comments='IPAddress of interface wan2'
```

```
add IP4Address wan2_gw Address=192.168.20.10 Comments='Default gateway for interface wan2'
```

```
add IP4Address wan2_net Address=192.168.20.0/24 Comments='The network on interface wan2'
```

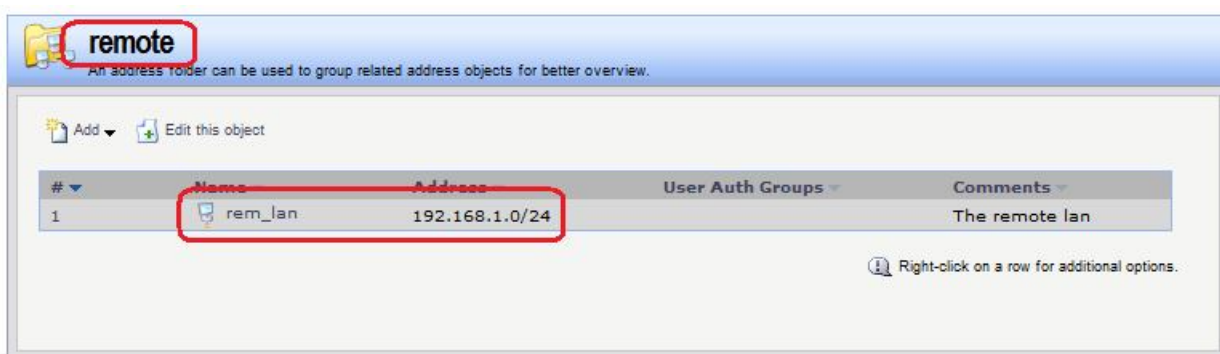
### 4. Объекты, описывающие сети, расположенные за МЭ 1.

#### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: remote

Object → Address Book → remote



#### Командная строка:

```
add Address AddressFolder remote Comments='The remote objects'
cc Address AddressFolder remote
add IP4Address rem_lan Address=192.168.1.0/24 Comments='The remote lan'
```

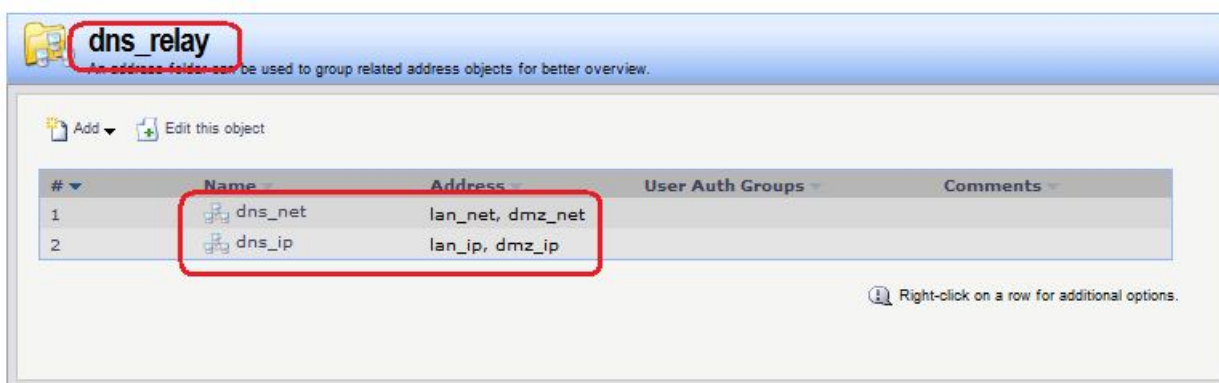
5. Дополнительные объекты, необходимые для удобства администрирования и объединяющие в одну группу сети и IP-адреса, которые необходимы одинаковые сервисы DNS.

### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: dns\_relay

Object → Address Book → dns\_relay



### Командная строка:

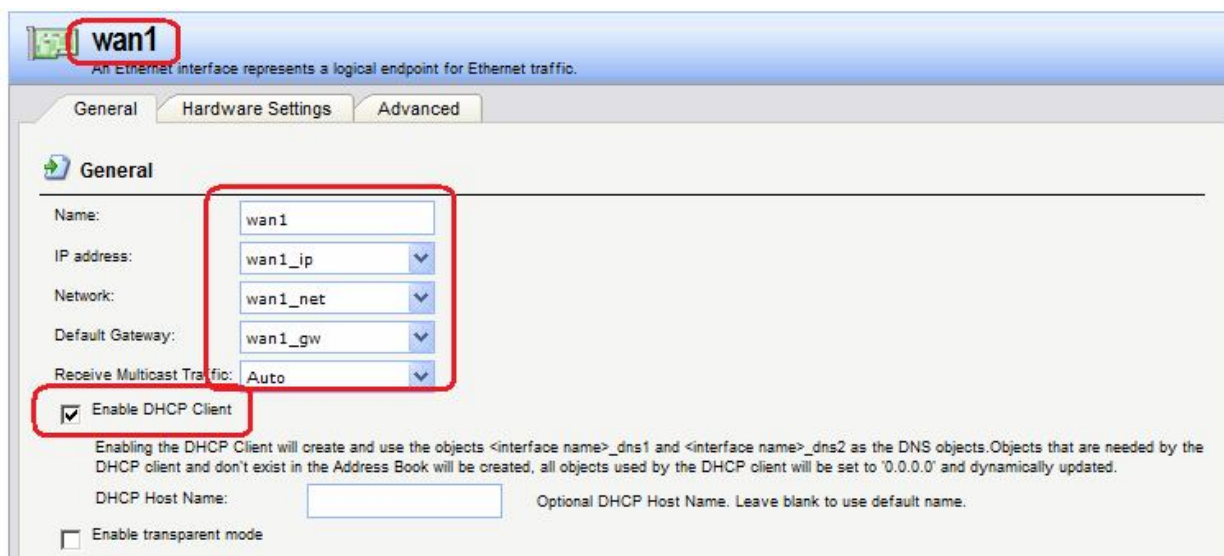
```
add Address AddressFolder dns_relay Comments='DNS services'
cc Address AddressFolder dns_relay
add IP4Group dns_net Members =lan/lan_net, dmz/dmz_net
add IP4Group dns_ip Members = lan/lan_ip, dmz/dmz_ip
```

### Привязка созданных объектов Адресной Книги к интерфейсам

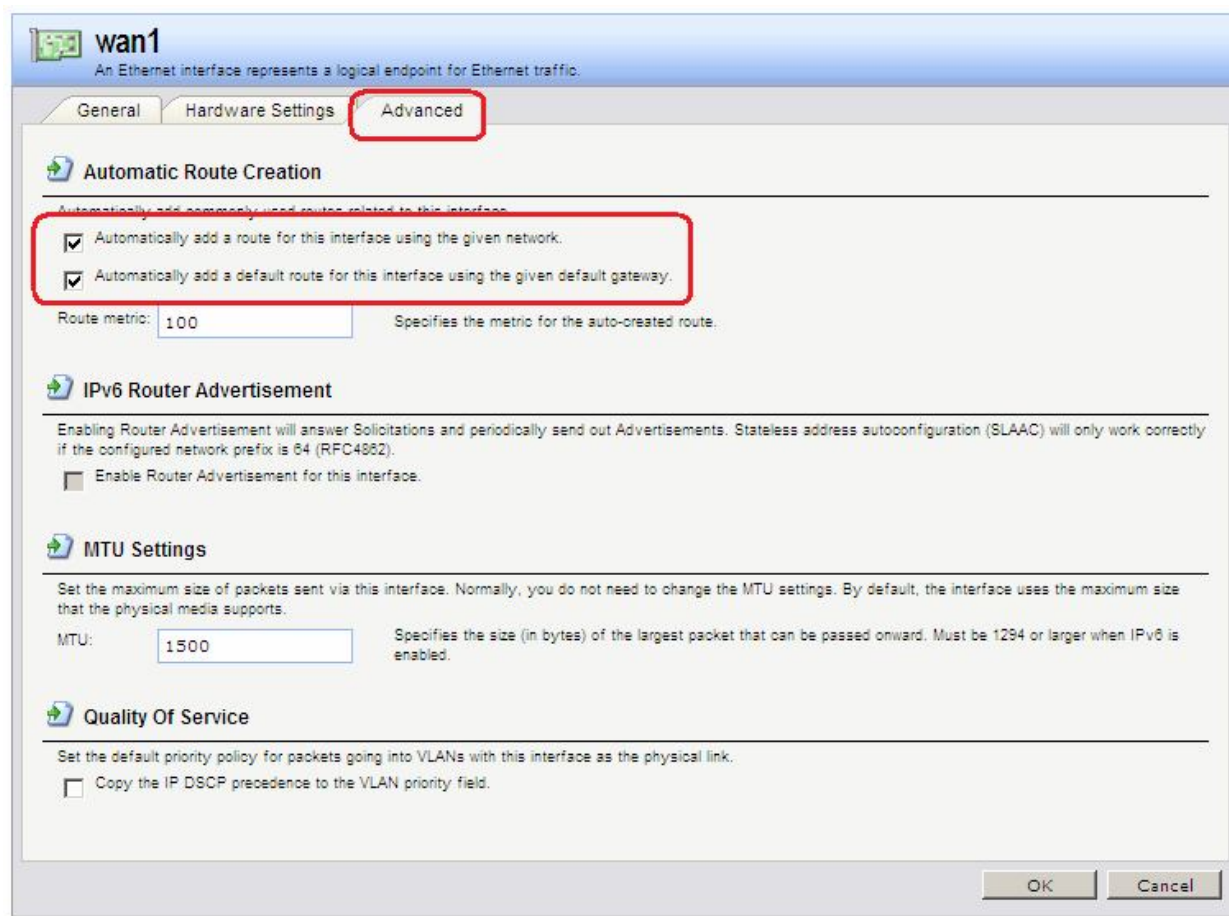
Объекты, созданные в пунктах 1, 2 и 3, должны быть привязаны к соответствующим Ethernet-интерфейсам.

### Веб-интерфейс:

Interfaces → Ethernet → wan1



Если IP-адрес данного интерфейса должен быть получен по протоколу DHCP, то следует установить соответствующий флаг «**Enable DHCP Client**».



На вкладке **Advanced** рекомендуется добавить флаг автоматического добавления маршрута к указанной сети, используя данный интерфейс. Для интерфейса **wan1** следует также установить флаг добавления маршрута по умолчанию к указанному шлюзу через данный интерфейс.

Аналогично привязать созданные объекты к другим интерфейсам.

### Командная строка:

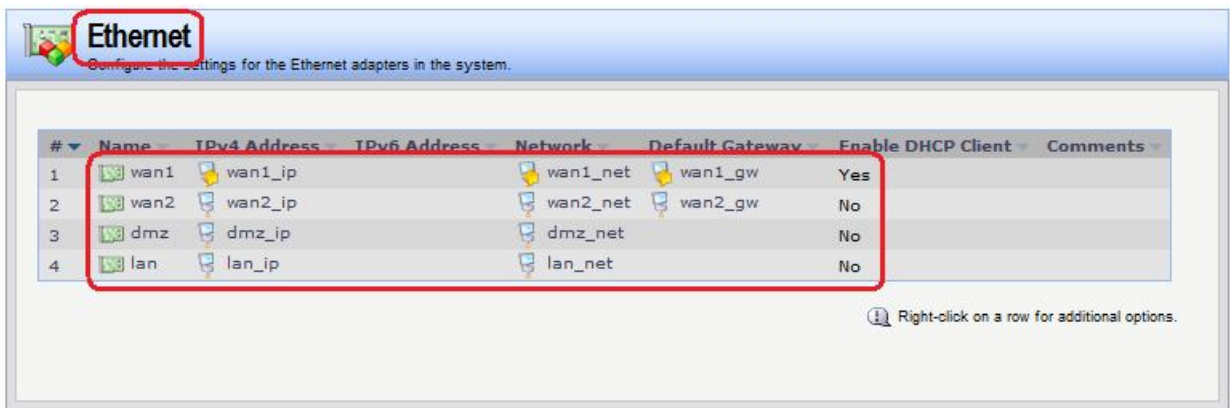
```
set Interface Ethernet lan IP=lan/lan_ip Network=lan/lan_net Name=lan  
AutoInterfaceNetworkRoute=yes
```

```
set Interface Ethernet dmz IP=dmz/dmz_ip Network=dmz/dmz_net Name=dmz  
AutoInterfaceNetworkRoute=yes
```

```
set Interface Ethernet wan1 IP=wan1/wan1_ip Network=wan1/wan1_net  
DefaultGateway=wan1/wan1_gw Name=wan1 AutoInterfaceNetworkRoute=yes  
DefaultGateway= wan1/wan1_gw DHCPEnabled=Yes
```

```
set Interface Ethernet wan2 IP=wan2/wan2_ip Network=wan2/wan2_net Name=wan2  
AutoInterfaceNetworkRoute=yes
```

В результате заданы следующие параметры интерфейсов:

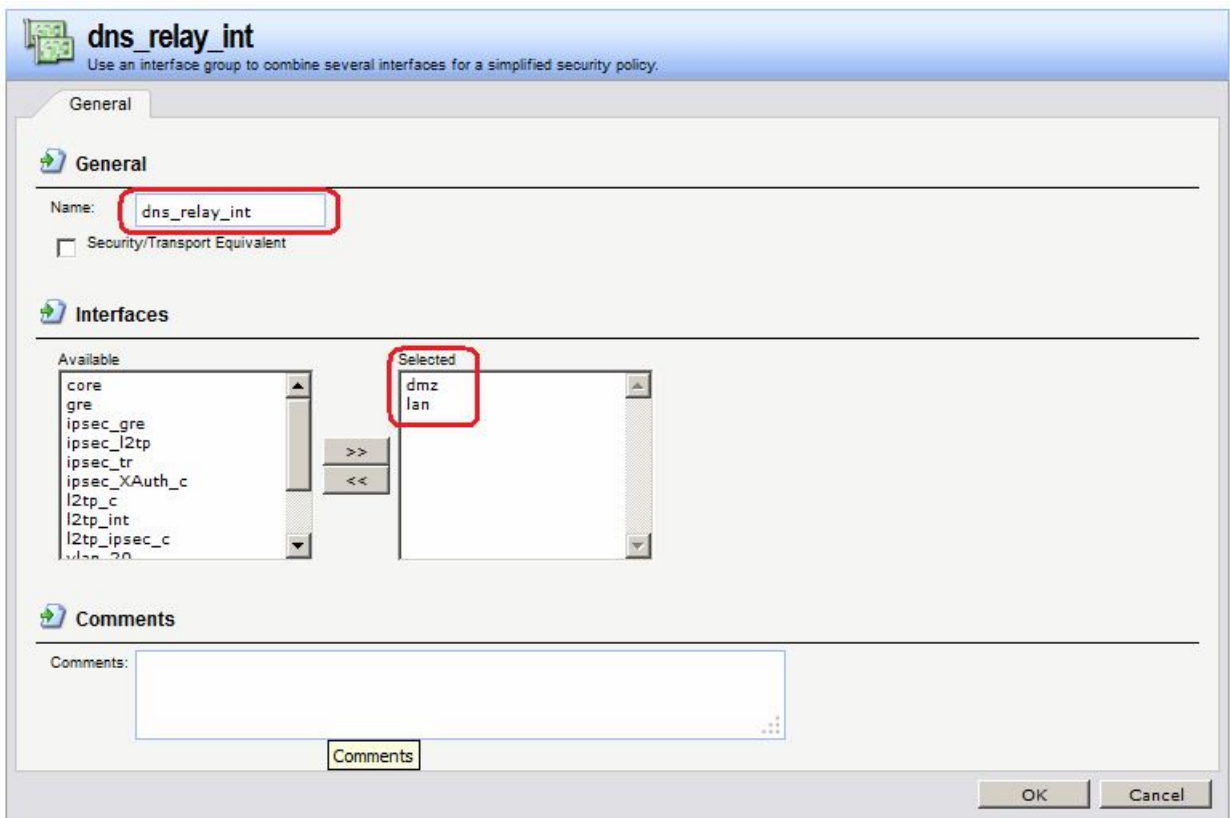


### Группа интерфейсов

Для удобства можно создать группу интерфейсов, в которой перечислены интерфейсы, трафик с которых можно объединить в одно Правило фильтрации. В нашем случае это интерфейсы **dmz** и **lan**.

### Веб-интерфейс:

Interfaces → Interface Groups → Add → Interface Group



### Командная строка:

```
add Interface InterfaceGroup dns_relay_int Members=lan,dmz
```

### Правила фильтрации

### Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: dns\_relay

Rules → IP Rules → dns\_relay

**dns\_relay**  
An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

Add Edit this object

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	sat_dns	SAT	dns_relay_int	dns_net	core	dns_ip	dns-all
2	nat_dns	NAT	dns_relay_int	dns_net	core	dns_ip	dns-all

Right-click on a row for additional options.

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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

**General**

Name: sat\_dns  
Action: SAT  
Service: dns-all  
Schedule: (None)

NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

**Address Filter**

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

Source: Interface: dns\_relay\_int Network: dns\_net  
Destination: core dns\_ip

**Comments**

Comments:

OK Cancel

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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

**General**

Translate the

Source IP  
Destination IP

to:

New IP Address: wan1\_dns1  
New Port:

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

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

OK Cancel

Вторым правилом на МЭ2 является правило **NAT**.

**Командная строка:**

```

add IPRuleFolder Name=dns_relay
cc IPRuleFolder <N folder>

add IPRule Action=SAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip SATAllToOne=Yes
SATTranslateToIP=wan1/wan1_dns1 Service=dns-all Name=sat_dns

add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_net DestinationInterface=core
DestinationNetwork=dns_relay/dns_ip Service=dns-all Name=nat_dns

```

### Статическая маршрутизация

В таблице маршрутизации уже созданы все необходимые маршруты.

**Routing Table Contents**

Routing Table:

Show all routes:  (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display:

**IPv4 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	0.0.0.0/0	wan1	10.0.4.1		100

**IPv6 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

In the "Flags" field of the routing tables, the following letters are used:  
 O: Learned via OSPF    X: Route is Disabled  
 M: Route is Monitored    A: Published via Proxy ARP  
 D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

## Доступ в интернет

### Межсетевой Экран 1

На МЭ 1 все необходимые объекты в Адресной Книге уже созданы и маршруты определены. Осталось добавить Правила фильтрации, разрешающие доступ в интернет.

### Правила фильтрации

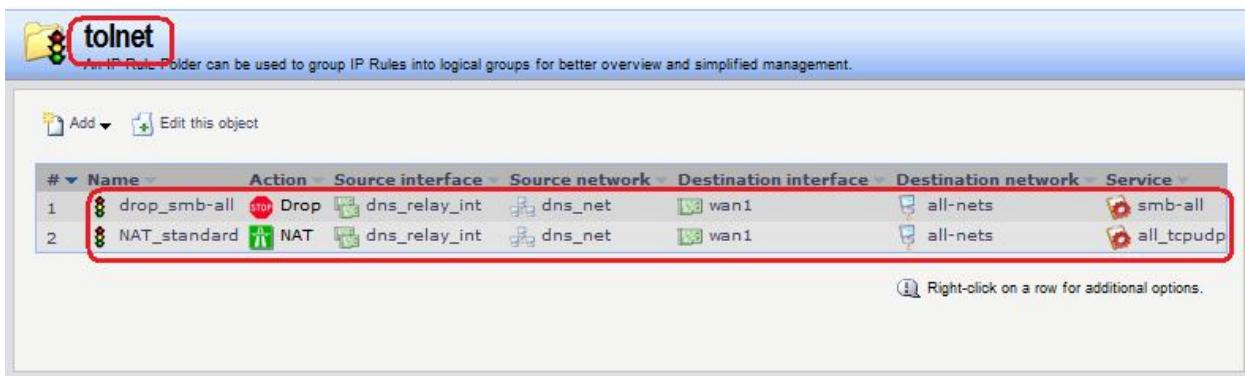
#### Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: toInet

Rules → IP Rules → toInet





### Командная строка:

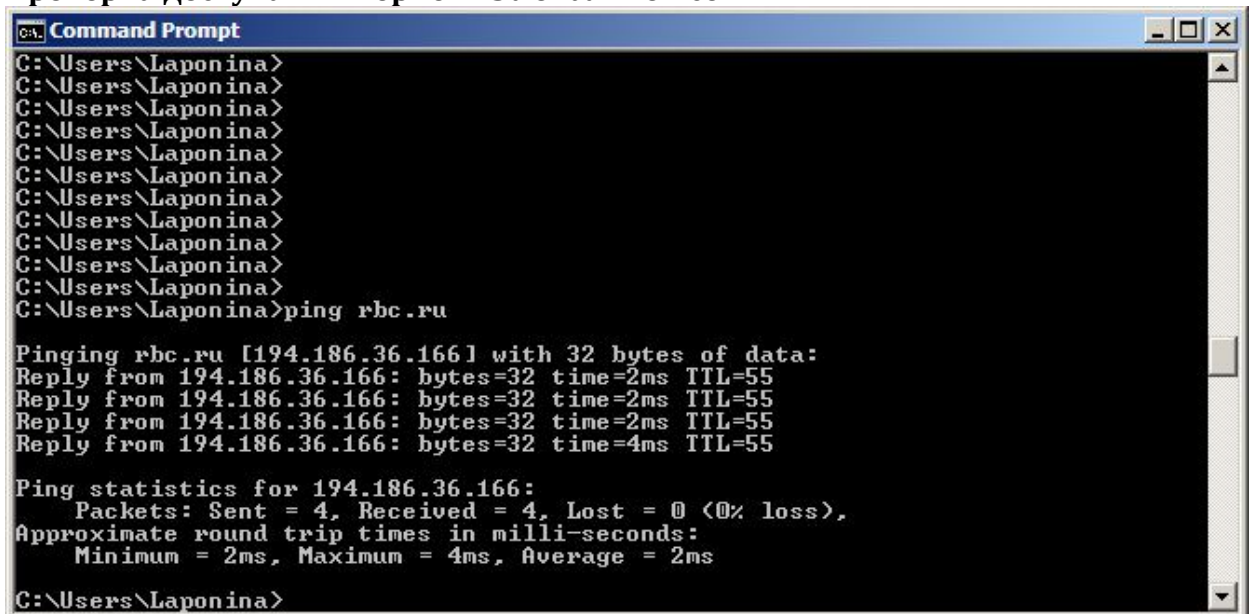
```
add IPRuleFolder Name=toInet

cc IPRuleFolder <N folder>

add IPRule Action=Drop SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=wana2
DestinationNetwork=all-nets Service=smb_all Name=drop_smb-all

add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_relay_net DestinationInterface=wana2
DestinationNetwork=all-nets Service=all_tcpudp Name=NAT_standard
```

### Проверка доступа в интернет из локальной сети



### Межсетевой Экран 2

На МЭ1 все необходимые объекты в Адресной Книге уже созданы и маршруты определены. Осталось добавить Правила фильтрования, разрешающие доступ в интернет. Для удобства конфигурирования Правил фильтрования был создан объект в Адресной Книге, который объединяет все сети, из которых необходим доступ в интернет.

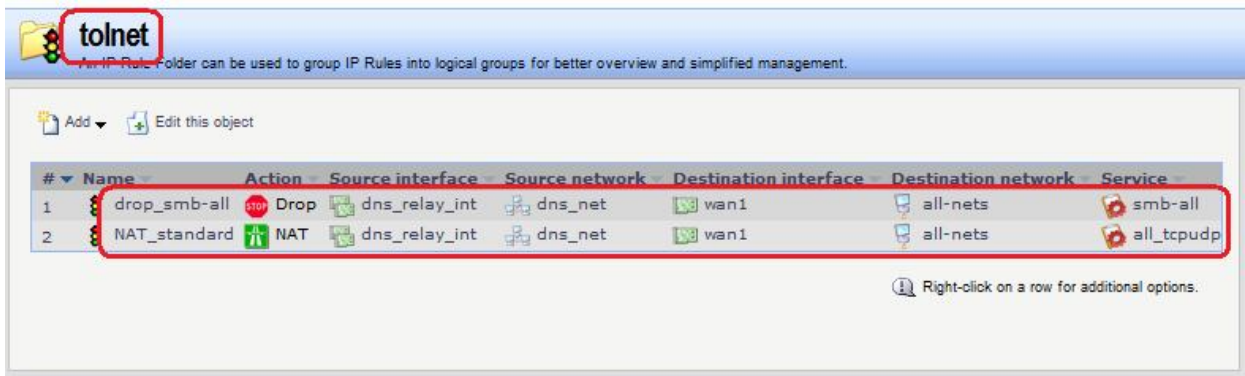
#### Правила фильтрования

##### Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: toInet

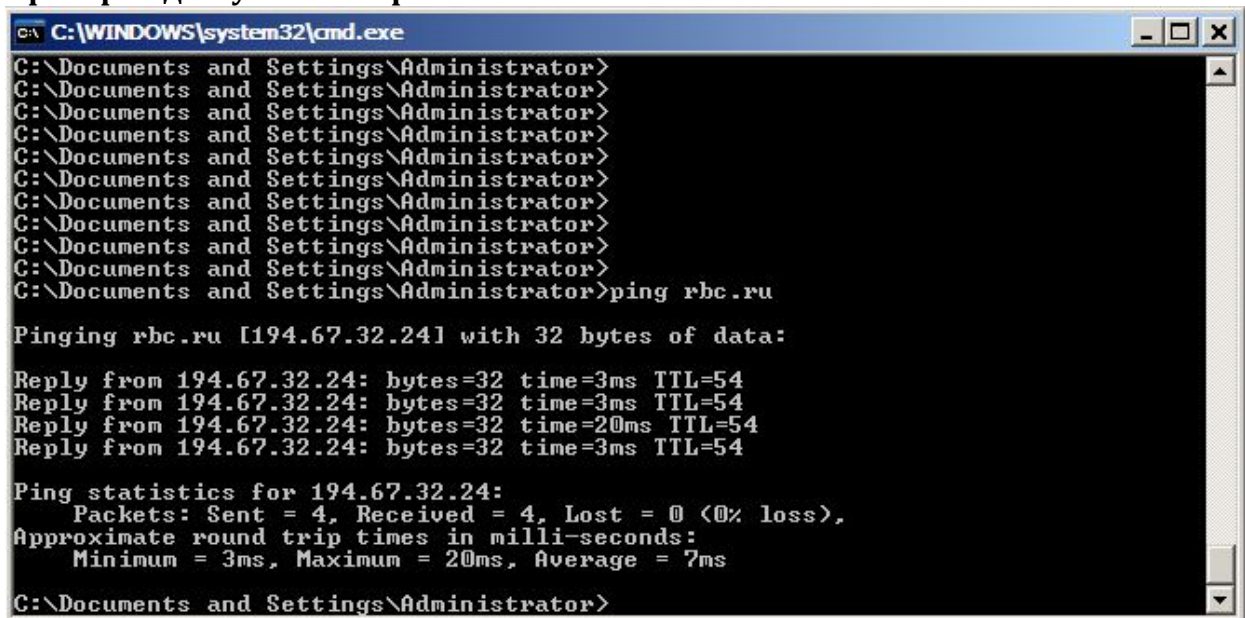
Rules → IP Rules → toInet



### Командная строка:

```
add IPRuleFolder Name=toInet
cc IPRuleFolder <N folder>
add IPRule Action=NAT SourceInterface=dns_relay_int
SourceNetwork=dns_relay/dns_net DestinationInterface=wlan1
DestinationNetwork=all-nets Service=all_tcpudp Name=NAT_standard
```

### Проверка доступа в интернет из локальной сети



### Доступ из локальных сетей к каждому межсетевому экрану

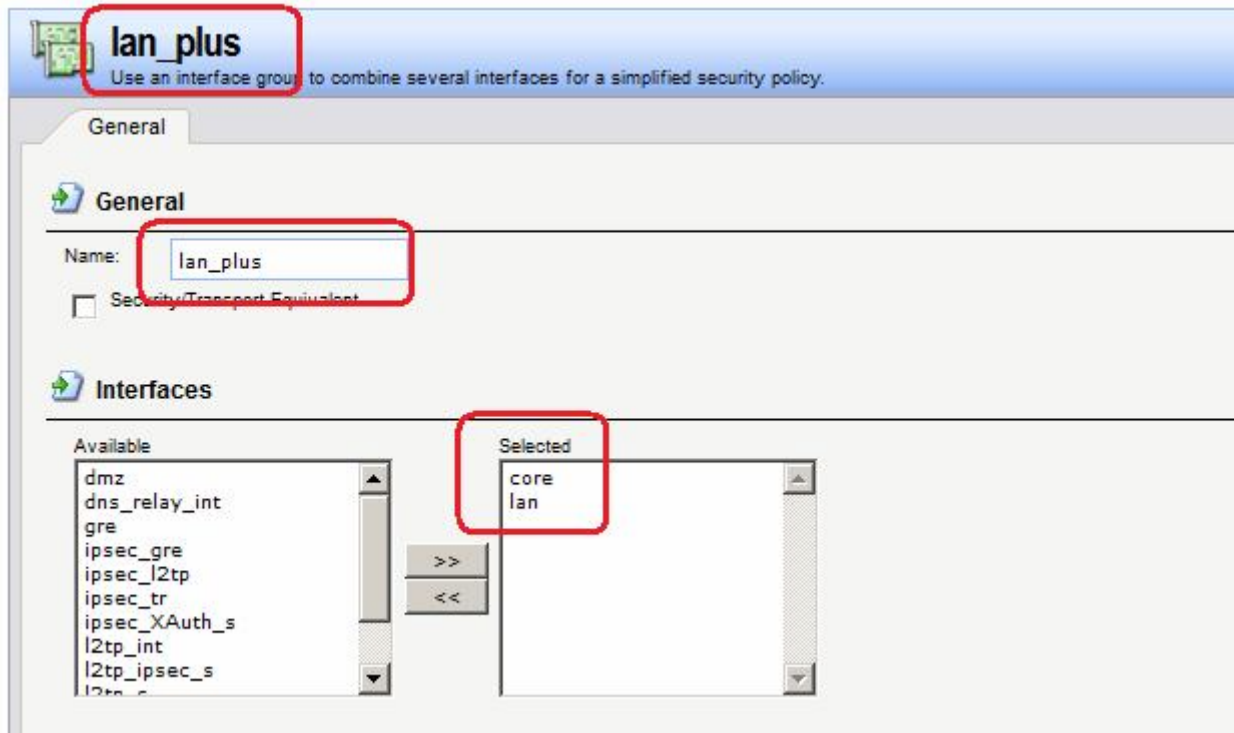
#### Межсетевой Экран 1

#### Группа интерфейсов

Объединить интерфейсы lan и core в одну группу, чтобы разрешить доступ как к рабочим станциям в локальной сети, так и к lan-интерфейсу межсетевого экрана.

#### Веб-интерфейс:

Interfaces → Interface Groups → Add → Interface Group



**Командная строка:**

```
add Interface InterfaceGroup lan_plus Members=core,lan
```

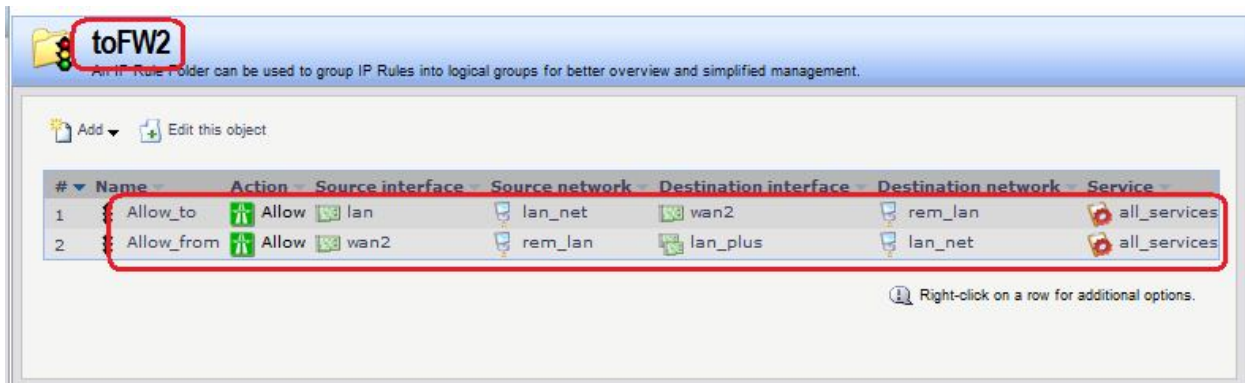
*Правила фильтрации*

**Веб-интерфейс:**

Rules → IP Rules → Add → IP Rule Folder

Name: toFW2

Rules → IP Rules → toFW2



**Командная строка:**

```
add IPRuleFolder Name=toFW2
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan2 DestinationNetwork=remote/rem_lan
Service=all_services Name=Allow_to
```

```
add IPRule Action=Allow SourceInterface=wan2 SourceNetwork=remote/rem_lan
DestinationInterface=lan_plus DestinationNetwork=lan/lan_net
Service=all_services Name=Allow_from
```

## Статическая маршрутизация

### Веб-интерфейс:

Routing → Routing Tables → main → Add → Route IPv4

The screenshot shows the 'Route IPv4' configuration window in Mikrotik WinBox. The 'General' tab is selected. The 'Interface' dropdown is set to 'wan2', 'Network' to 'rem\_lan', 'Gateway' to 'wan2\_gw', 'Local IP address' to '(None)', and 'Metric' to '100'. A red box highlights these fields. The 'Comments' field is empty. 'OK' and 'Cancel' buttons are at the bottom right.

### Командная строка:

```
cc RoutingTable main
```

```
add Route Interface=wan2 Network=remote/rem_lan Gateway=wan2/wan2 Metric=100
```

### Межсетевой Экран 2

Следует выполнить настройки, аналогичные настройкам, сделанным на Межсетевом Экране 1.

### Проверка конфигурации

Проверяем доступ (команда `ping`) с lan-интерфейса межсетевого экрана 1 к рабочей станции в локальной сети (IP-адрес 192.168.1.122) и к lan-интерфейсу межсетевого экрана 1.

```
192.168.2.20 - PuTT /
DFL-860E:/>
DFL-860E:/> ping 192.168.1.122 -v -recvif=lan
Rule and routing information for ping:
PBR selected by rule "iface_member_main" - PBR table "main"
  allowed by rule "Allow_to"

Sending 1 4-byte ICMP ping to 192.168.1.122 from 192.168.2.20
  sent via route "192.168.1.0/24 via wan2, gw 192.168.20.10" in PBR table "main"
ICMP Reply from 192.168.1.122  seq=0  time=<10 ms  TTL=127

Ping Results:  Sent: 1, Received:1, Avg RTT: 10.0 ms

DFL-860E:/> ping 192.168.1.10 -v -recvif=lan
Rule and routing information for ping:
PBR selected by rule "iface_member_main" - PBR table "main"
  allowed by rule "Allow_to"

Sending 1 4-byte ICMP ping to 192.168.1.10 from 192.168.2.20
  sent via route "192.168.1.0/24 via wan2, gw 192.168.20.10" in PBR table "main"
ICMP Reply from 192.168.1.10  seq=0  time=<10 ms  TTL=255

Ping Results:  Sent: 1, Received:1, Avg RTT: 10.0 ms

DFL-860E:/> █
```

## Сегментирование сетей на канальном уровне

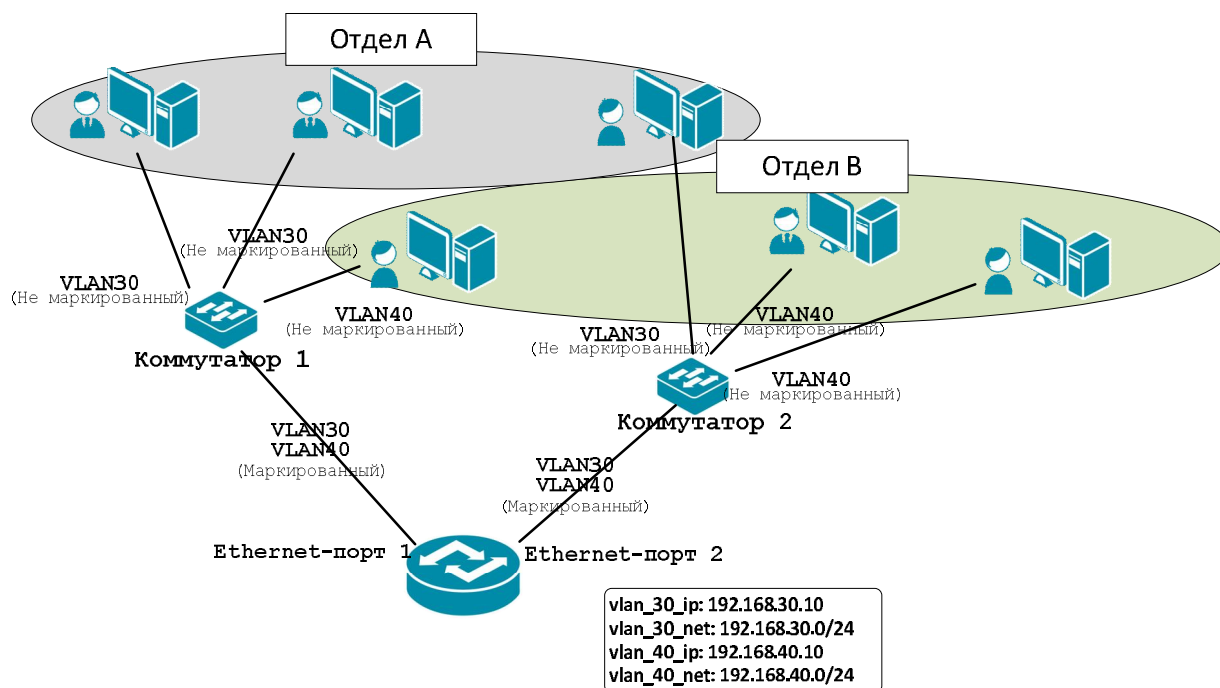
### Лабораторная работа 3. Сегментирование подсетей с использованием управляемых коммутаторов

#### Цель

Создать для разных отделов отдельные виртуальные сети.

#### Топология

Предположим, что в организации есть два отдела **А** и **В**. Будем считать, физическую топологию сети удобнее создавать с использованием двух коммутаторов, причем часть рабочих станций отделов **А** и **В** следует подключить к **Коммутатору 1**, а оставшиеся рабочие станции отделов **А** и **В** подключить к **Коммутатору 2**. Для увеличения производительности широковещательного трафика между отделами не должно быть, также желательно иметь возможность фильтровать трафик между отделами.



#### Описание практической работы

##### Коммутатор 1

При такой топологии порты коммутаторов, к которым подключены рабочие станции пользователей, должны быть настроены как немаркированные порты соответствующей vlan.

В нашем случае рабочие станции отдела **А** подключены портам **02** и **03** **Коммутатора 1**. Эти порты входят в vlan с VID 30 как немаркированные (untagged) порты. Рабочая станция отдела **В** подключена к порту **04** **Коммутатора 1**. Данный порт входит в vlan с VID 40 как немаркированный (untagged) порт.

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02,03	01	Rename	Delete VID
40	deptB	04	01	Rename	Delete VID

Uplink-порт коммутатора, подключенного к маршрутизатору или межсетевому экрану, должен быть настроен как маркированный и являться членом всех vlan, настроенных на коммутаторе.

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02,03	01	Rename	Delete VID
40	deptB	04	01	Rename	Delete VID

## Коммутатор 2

Рабочая станция отдела **A** подключена порту 02 **Коммутатора 2**. Данный порт входит в vlan с VID 30 как немаркированный (untagged) порт. Рабочие станции отдела **B** подключены к портам 03 и 04 **Коммутатора 2**. Данные порты входят в vlan с VID 40 как немаркированные (untagged) порты.

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02	01	Rename	Delete VID
40	deptB	03,04	01	Rename	Delete VID

Uplink-порт коммутатора, подключенного к маршрутизатору или межсетевому экрану, должен быть настроен как маркированный и являться членом всех VLAN, настроенных на коммутаторе.

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
01	default	05,06,07,08		Rename	Delete VID
30	deptA	02	01	Rename	Delete VID
40	deptB	03,04	01	Rename	Delete VID

## Межсетевой Экран

### Объекты Адресной Книги

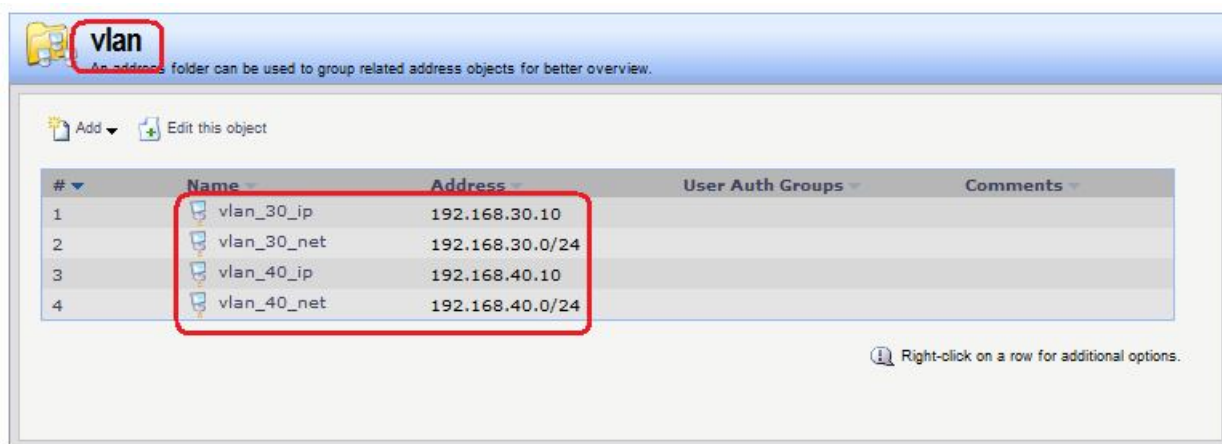
Создать объекты с IP-адресами vlan-интерфейса и vlan-сети.

### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: vlan

Object → Address Book → vlan → Add



### Командная строка:

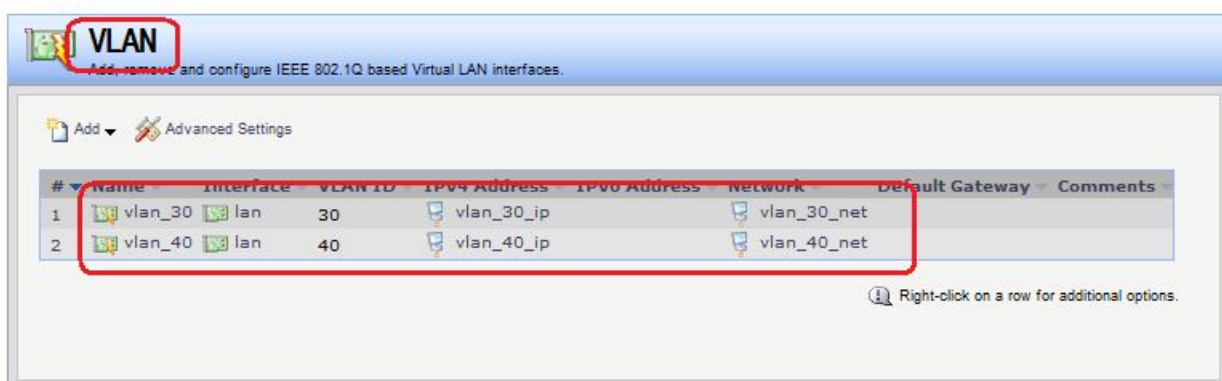
```
add Address AddressFolder vlan
cc Address AddressFolder vlan
add IP4Address vlan_30_ip Address=192.168.30.10
add IP4Address vlan_30_net Address=192.168.30.0/24
add IP4Address vlan_40_ip Address=192.168.40.10
add IP4Address vlan_40_net Address=192.168.40.0/24
```

### VLAN-Интерфейс

Создать интерфейс `vlan`, связав его с `lan`-интерфейсом и указав `VLAN ID`.

### Веб-интерфейс:

Interfaces → VLAN → Add



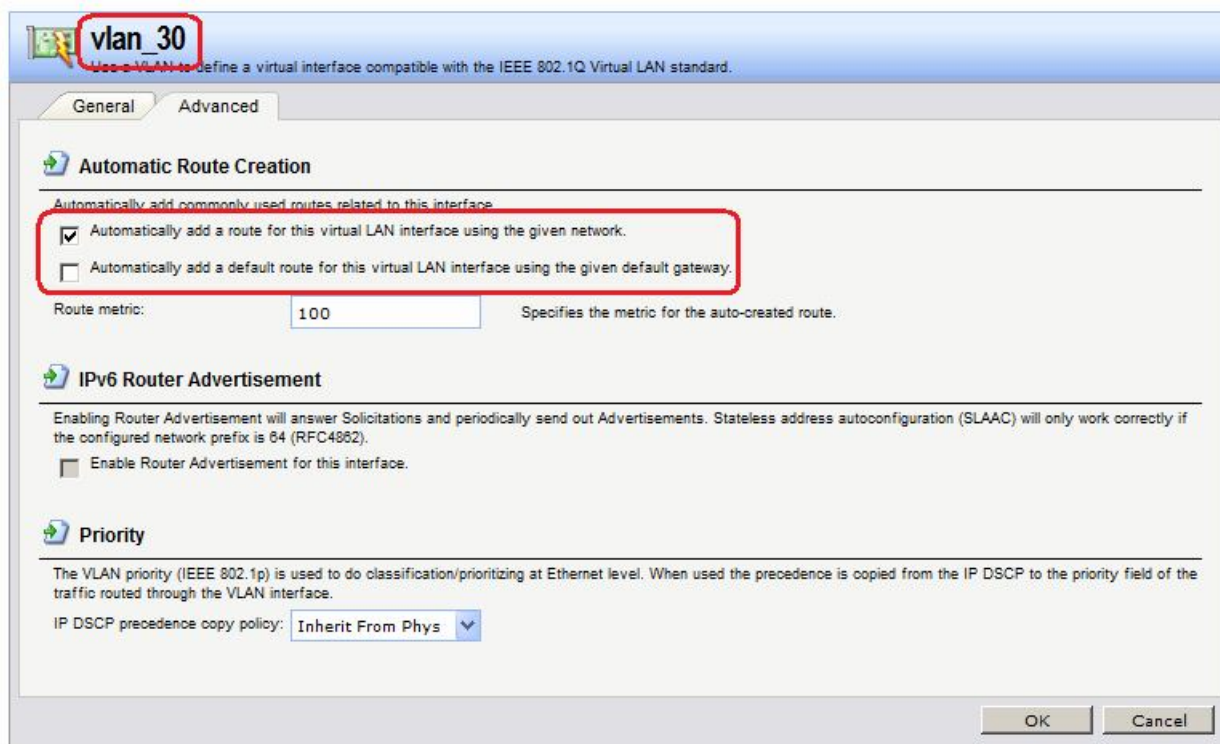
### Командная строка:

```
add Interface VLAN vlan_30 Ethernet=lan IP=vlan/vlan_30_ip
Network=vlan/vlan_30_net VLANID=30
add Interface VLAN vlan_40 Ethernet=lan IP=vlan/vlan_40_ip
Network=vlan/vlan_40_net VLANID=40
```

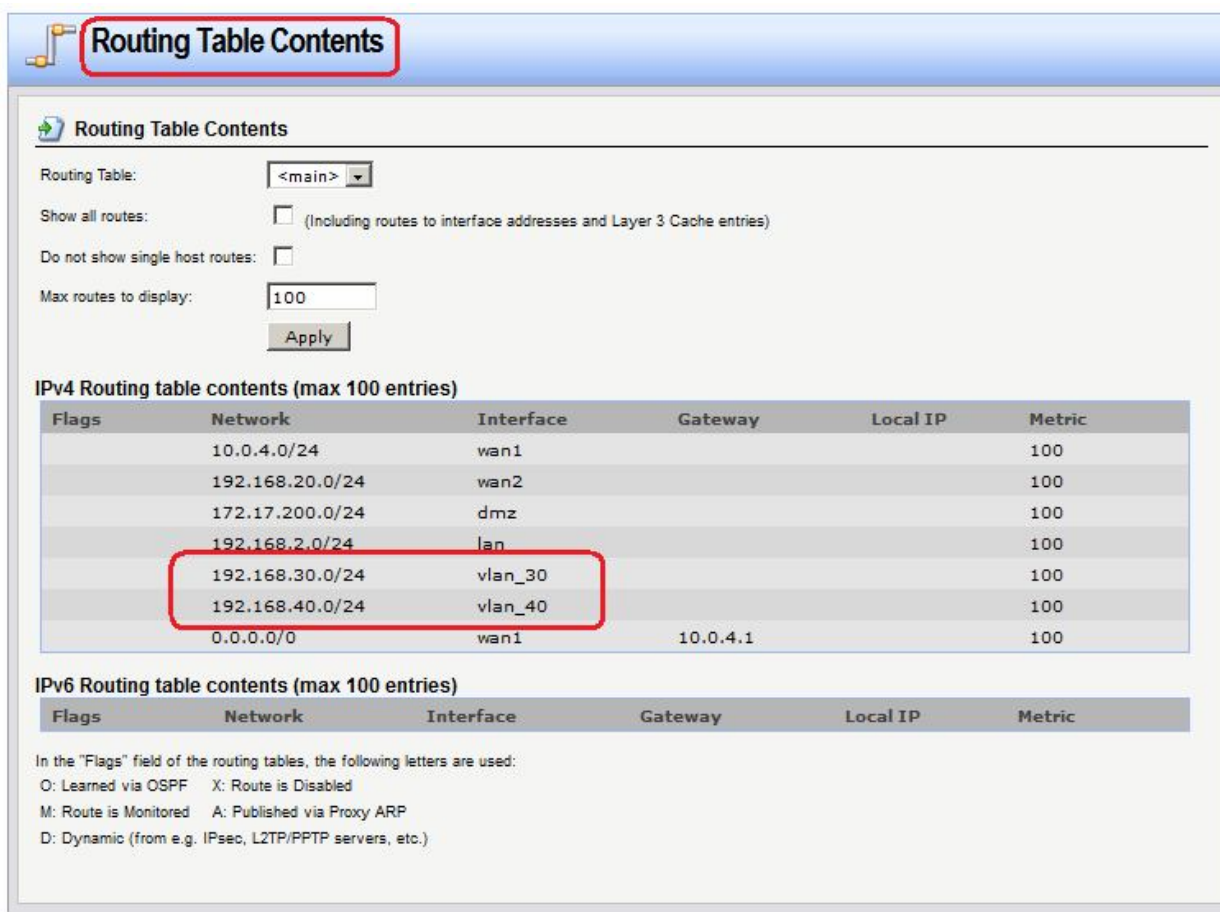
### Статическая маршрутизация

При необходимости следует добавить правило маршрутизации, если были изменены настройки по умолчанию.





Следует также проверить созданные маршруты.



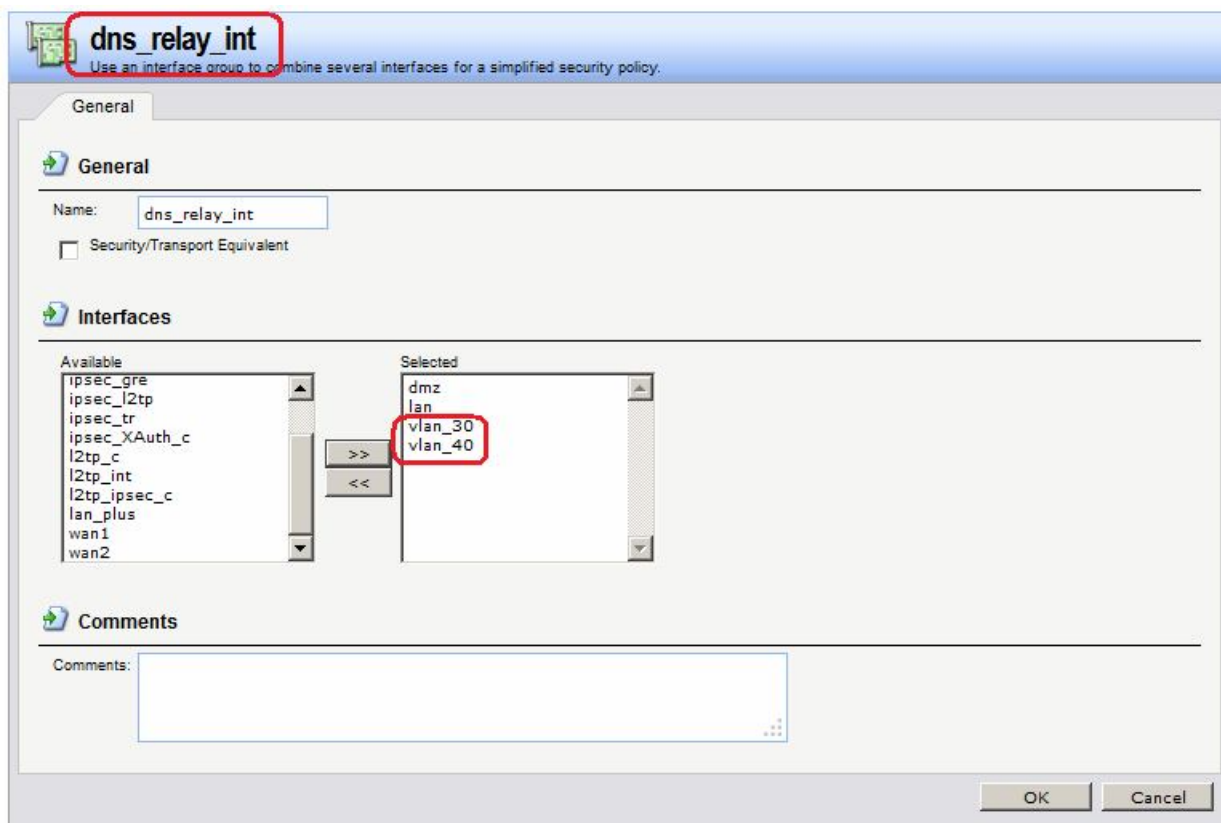
### Правила фильтрации

Добавить необходимые правила фильтрации, указав в качестве интерфейса и сети источника созданные интерфейсы и сети **vlan**, либо добавив созданные интерфейсы и

сети vlan в необходимые группы интерфейсов и сетей. Для разрешения доступа в интернет достаточно добавить созданные интерфейсы и сети в уже существующие группы.

### Веб-интерфейс:

Interfaces → Interface Groups

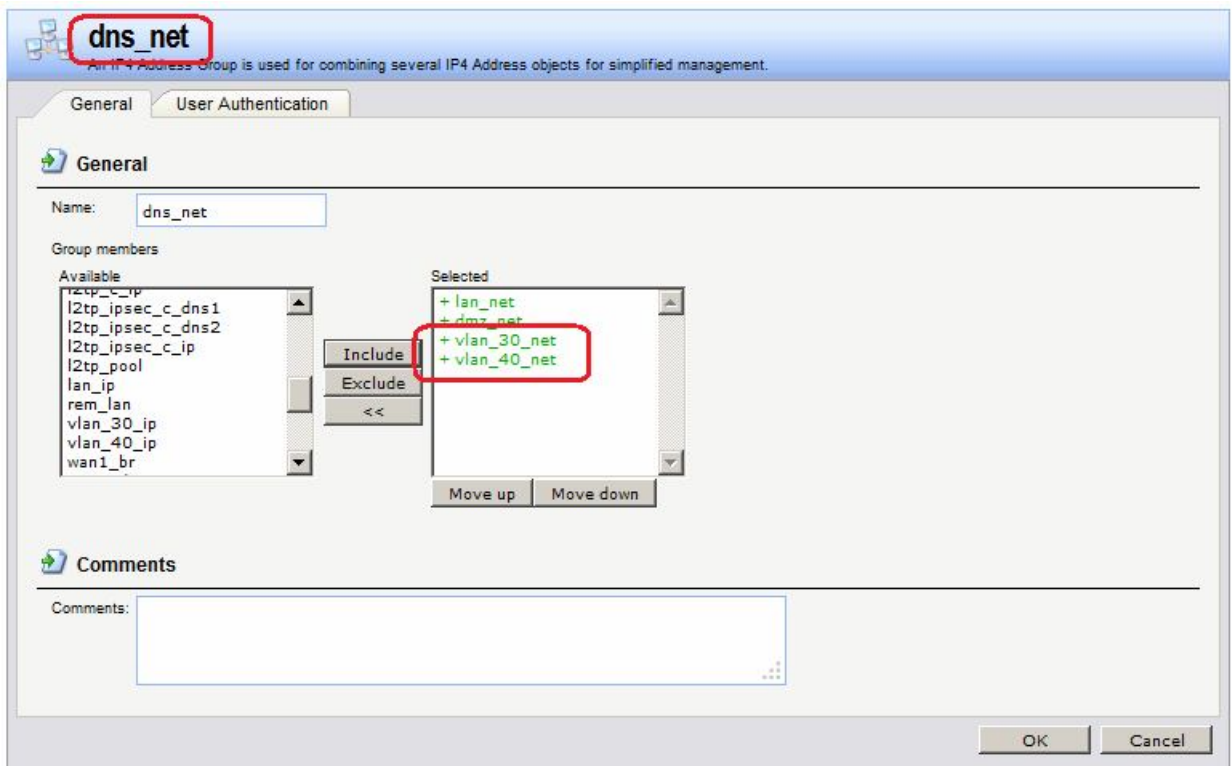


### Командная строка:

```
set Interface InterfaceGroup dns_relay_int Members=vlan_30,vlan40
```

### Веб-интерфейс:

Objects → Address Book → dns\_relay → dns\_net

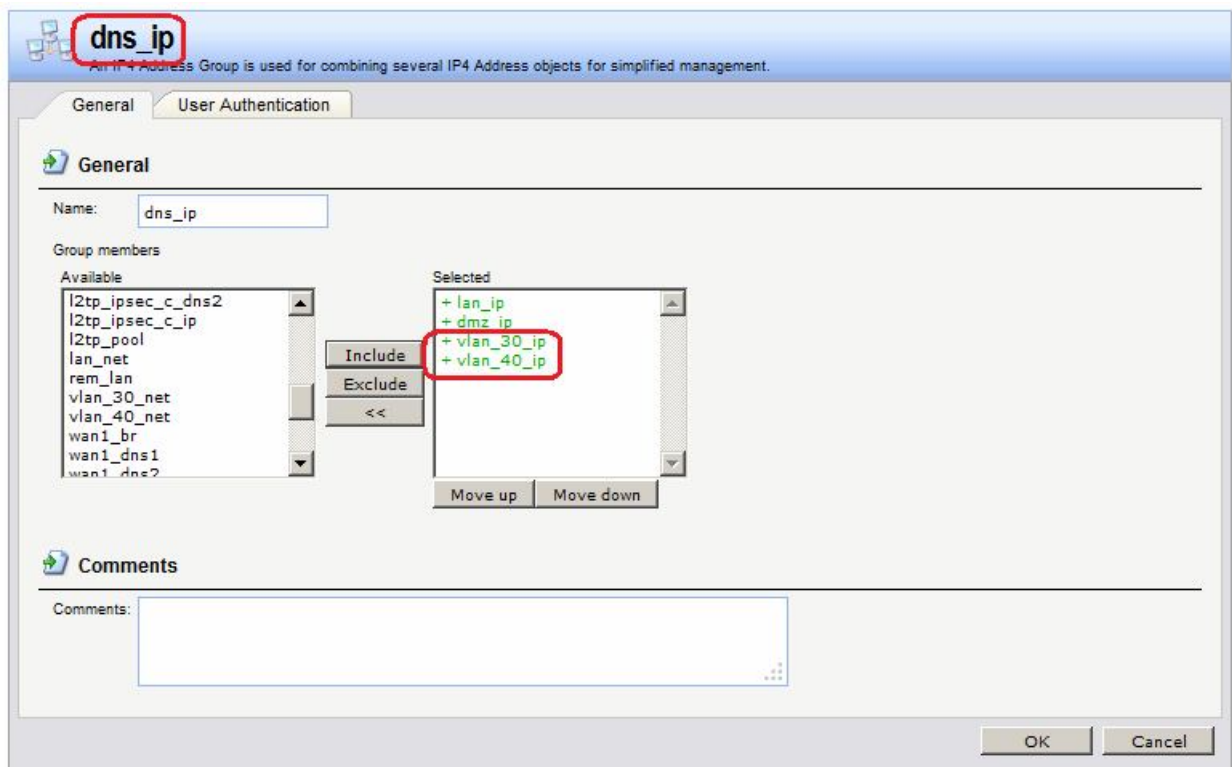


**Командная строка:**

`set IP4Group dns_net Members=vlan/vlan_30_net,vlan/vlan_40_net`

**Веб-интерфейс:**

Objects → Address Book → dns\_relay → dns\_ip



**Командная строка:**

`set IP4Group dns_net Members=vlan/vlan_30_ip,vlan/vlan_40_ip`

## Проверка конфигурации

Проверяем созданную конфигурацию, используя команду `ping`.

Connections

Filter state table display

Source: Destination:

IP Address:

Interface:

IP Protocol:

Port:

State table contents (max 100 entries)

State	Proto	Source	Destination	Timeout
PING	ICMP	vlan_30:192.168.30.30:512	core:192.168.20.20:512	7

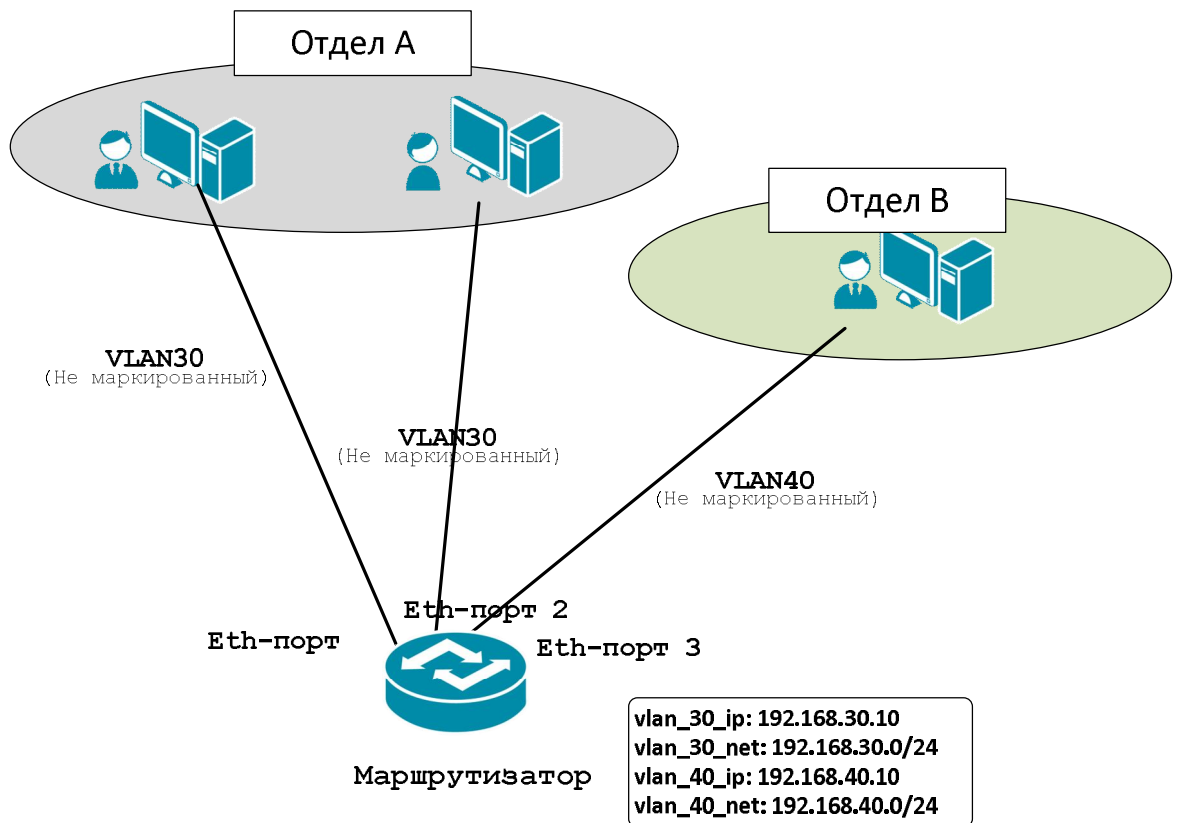
## Лабораторная работа 4. Сегментирование подсетей на основе port-based VLAN

### Цель

Создать для разных отделов отдельные виртуальные сети без использования управляемых коммутаторов.

### Топология

Предположим, что в организации есть два отдела **а** и **в**. Будем считать, физическую топологию сети требуется создать без использования управляемых коммутаторов, т.е. рабочие станции отделов подключаются непосредственно к lan-портам маршрутизатора. Для увеличения производительности широковещательного трафика между отделами не должно быть, также желательно иметь возможность фильтровать трафик между отделами.



## Межсетевой Экран

### Объекты Адресной Книги

Создать объекты с IP-адресами vlan-интерфейса и vlan-сети.

#### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: vlan

Object → Address Book → vlan → Add

vlan

An address folder can be used to group related address objects for better overview.

Add Edit this object

#	Name	Address	User Auth Groups	Comments
1	vlan_30_ip	192.168.30.10		
2	vlan_30_net	192.168.30.0/24		
3	vlan_40_ip	192.168.40.10		
4	vlan_40_net	192.168.40.0/24		

Right-click on a row for additional options.

#### Командная строка:

```
add Address AddressFolder vlan
```

```
cc Address AddressFolder vlan
```

```
add IP4Address vlan_30_ip Address=192.168.30.10
```

```
add IP4Address vlan_30_net Address=192.168.30.0/24
```

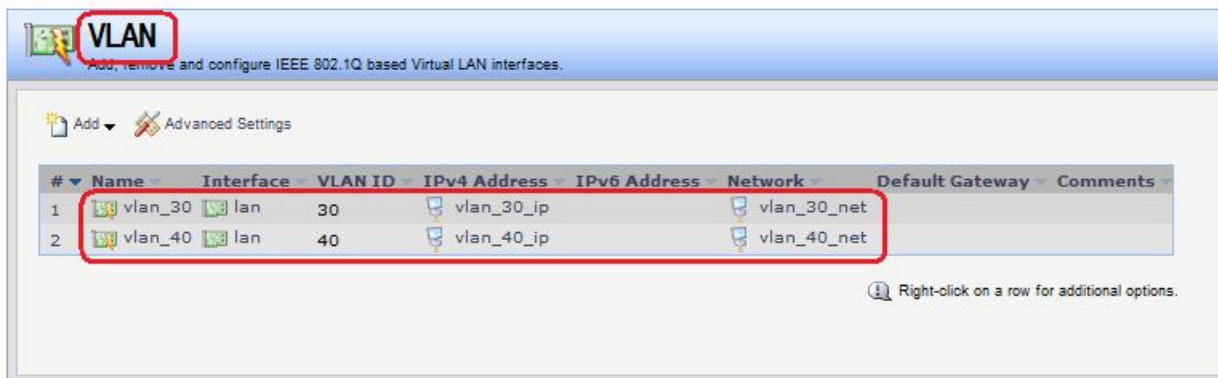
```
add IP4Address vlan_40_ip Address=192.168.40.10
add IP4Address vlan_40_net Address=192.168.40.0/24
```

### VLAN-Интерфейс

Создать интерфейс `vlan`, связав его с `lan`-интерфейсом и указав `VLAN ID`.

### Веб-интерфейс:

Interfaces → VLAN → Add



### Командная строка:

```
add Interface VLAN vlan_30 Ethernet=lan IP=vlan/vlan_30_ip
Network=vlan/vlan_30_net VLANID=30
add Interface VLAN vlan_40 Ethernet=lan IP=vlan/vlan_40_ip
Network=vlan/vlan_40_net VLANID=40
```

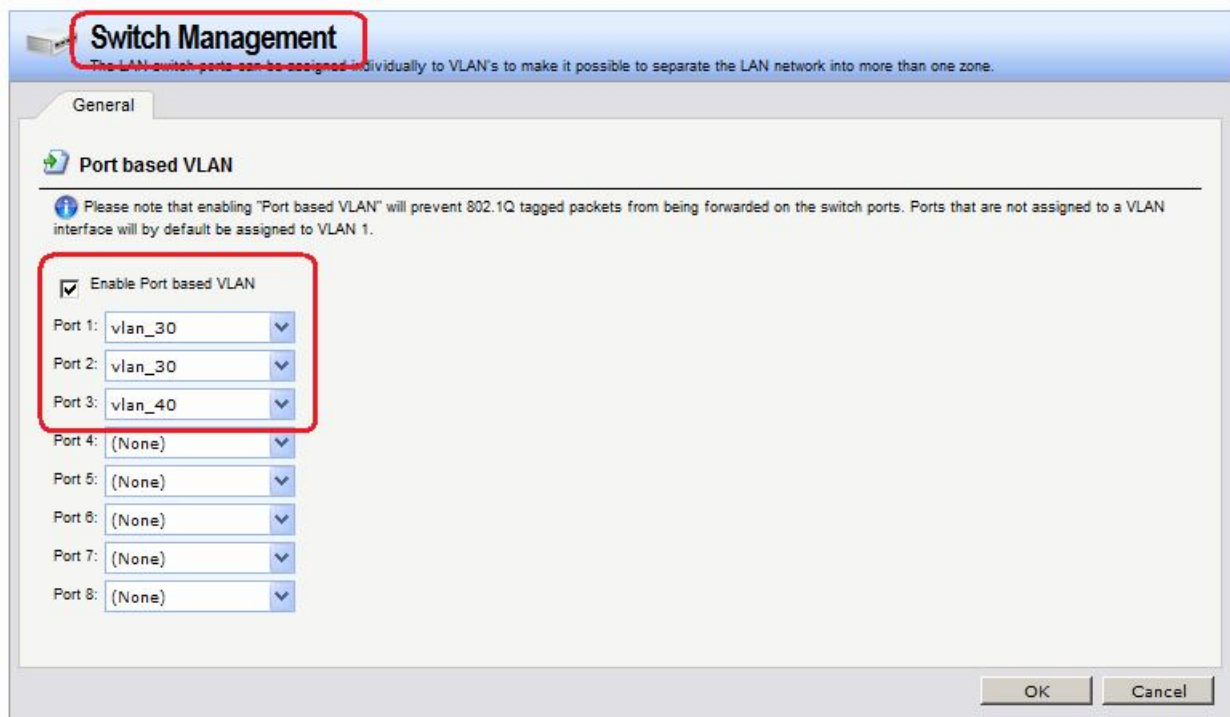
Далее следует указать номер порта коммутатора, на котором сконфигурирован данный `vlan`.

### Веб-интерфейс:

Interfaces → Switch Management

Поставить флаг `Enable Port based VLAN`

В строке, соответствующей номеру порта, к которому подключен Ethernet-кабель, выбрать созданный `vlan`-интерфейс.

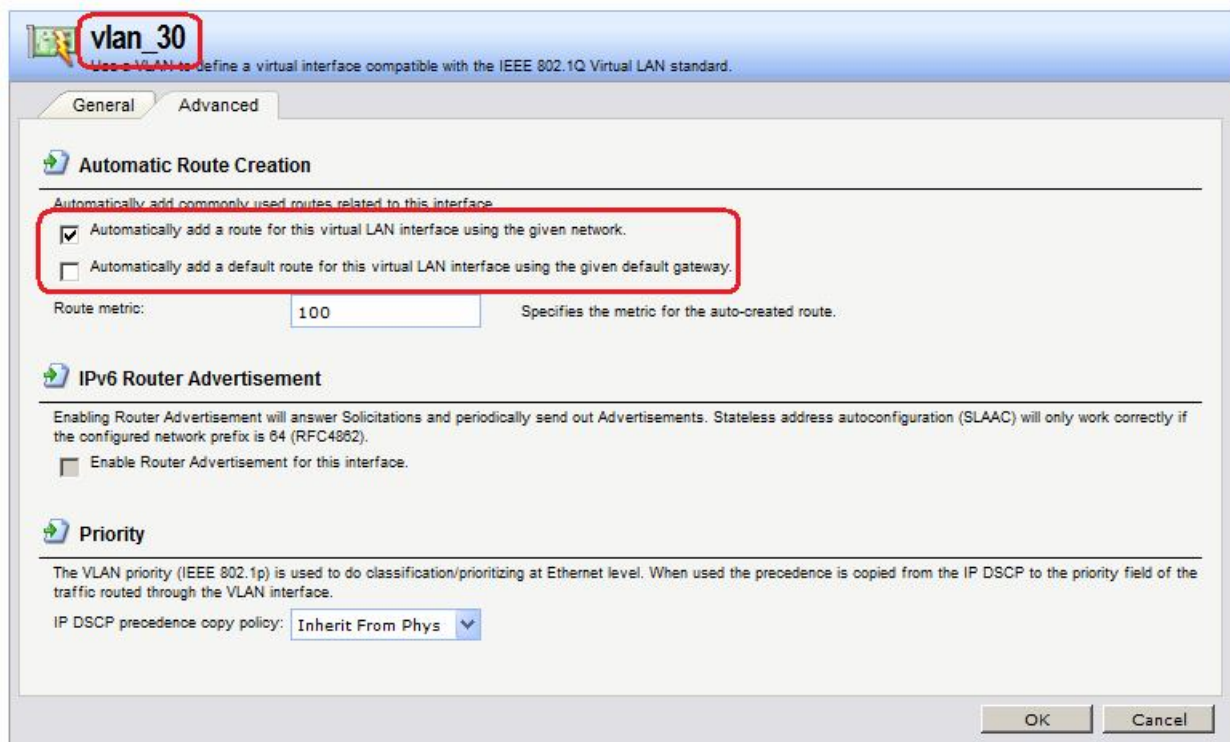


### Командная строка:

```
set SwitchManagement Port1=vlan_30 Port2=vlan_30 Port3=vlan_40
```

### Статическая маршрутизация

При необходимости следует добавить правило маршрутизации, если были изменены настройки по умолчанию.



Следует также проверить созданные маршруты.

## Routing Table Contents

---

**Routing Table Contents**

Routing Table:

Show all routes:  (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display:

**IPv4 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	192.168.30.0/24	vlan_30			100
	192.168.40.0/24	vlan_40			100
	0.0.0.0/0	wan1	10.0.4.1		100

**IPv6 Routing table contents (max 100 entries)**

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

In the "Flags" field of the routing tables, the following letters are used:  
 O: Learned via OSPF    X: Route is Disabled  
 M: Route is Monitored    A: Published via Proxy ARP  
 D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

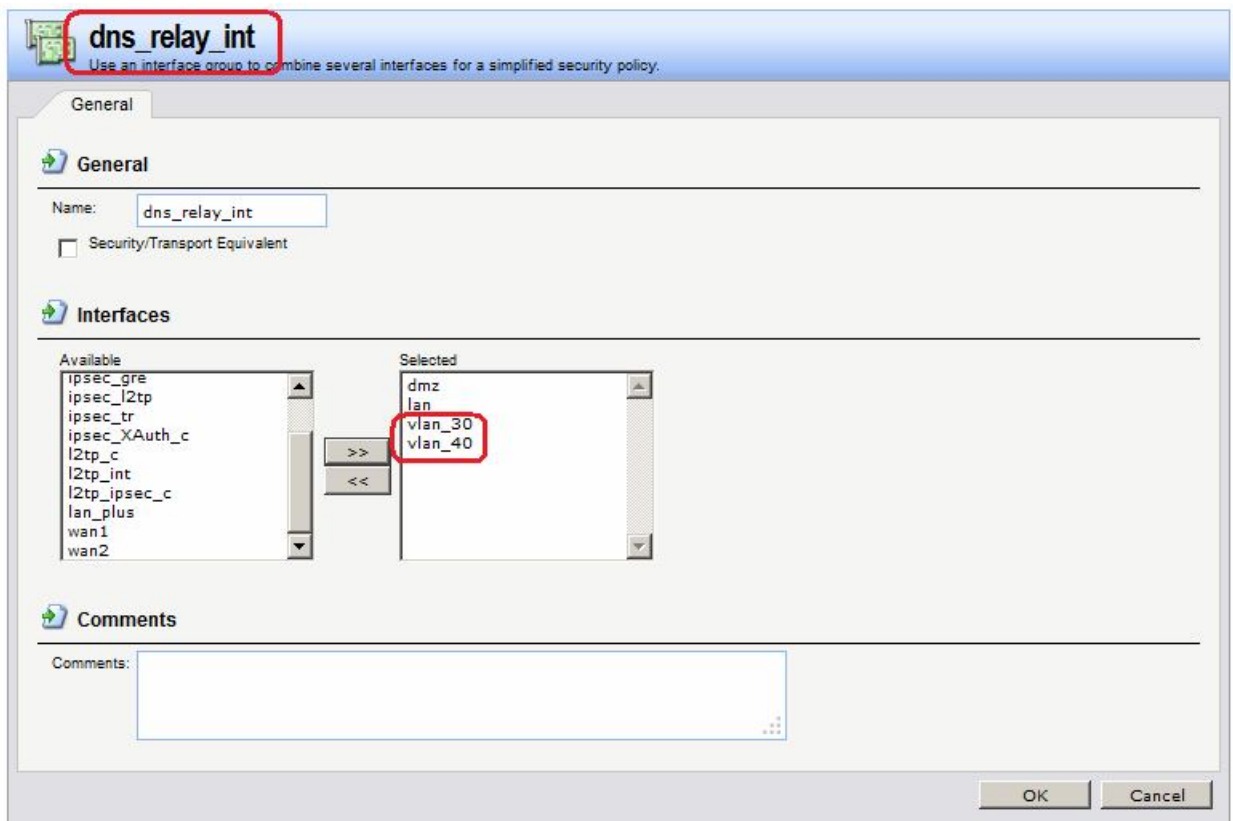
### ***Правила фильтрации***

Добавить необходимые правила фильтрации, указав в качестве интерфейса и сети источника созданные интерфейсы и сети vlan, либо добавив созданные интерфейсы и сети vlan в необходимые группы интерфейсов и сетей. Для разрешения доступа в интернет достаточно добавить созданные интерфейсы и сети в уже существующие группы.

### **Веб-интерфейс:**

**Interfaces** → **Interface Groups**



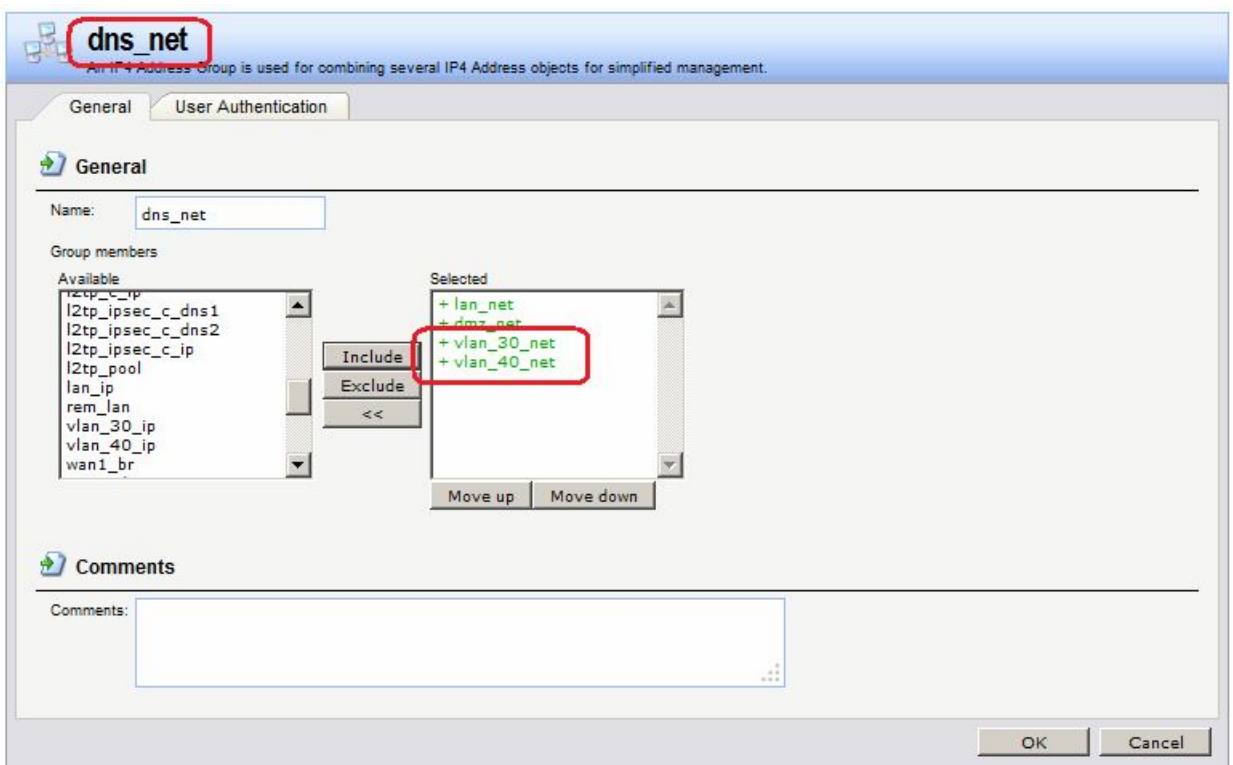


**Командная строка:**

```
set Interface InterfaceGroup dns_relay_int Members=vlan_30,vlan_40
```

**Веб-интерфейс:**

Objects → Address Book → dns\_relay → dns\_net

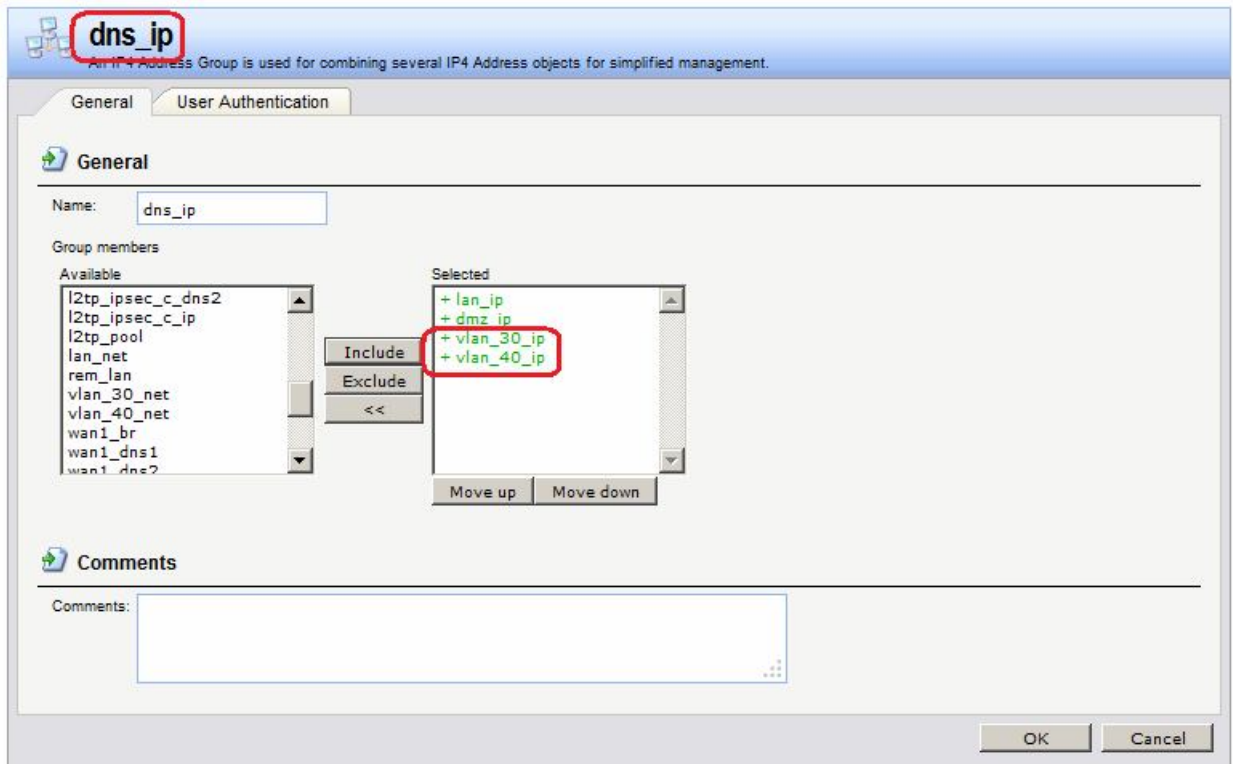


**Командная строка:**

```
set IP4Group dns_net Members=vlan/vlan_30_net,vlan/vlan_40_net
```

## Веб-интерфейс:

Objects → Address Book → dns\_relay → dns\_ip

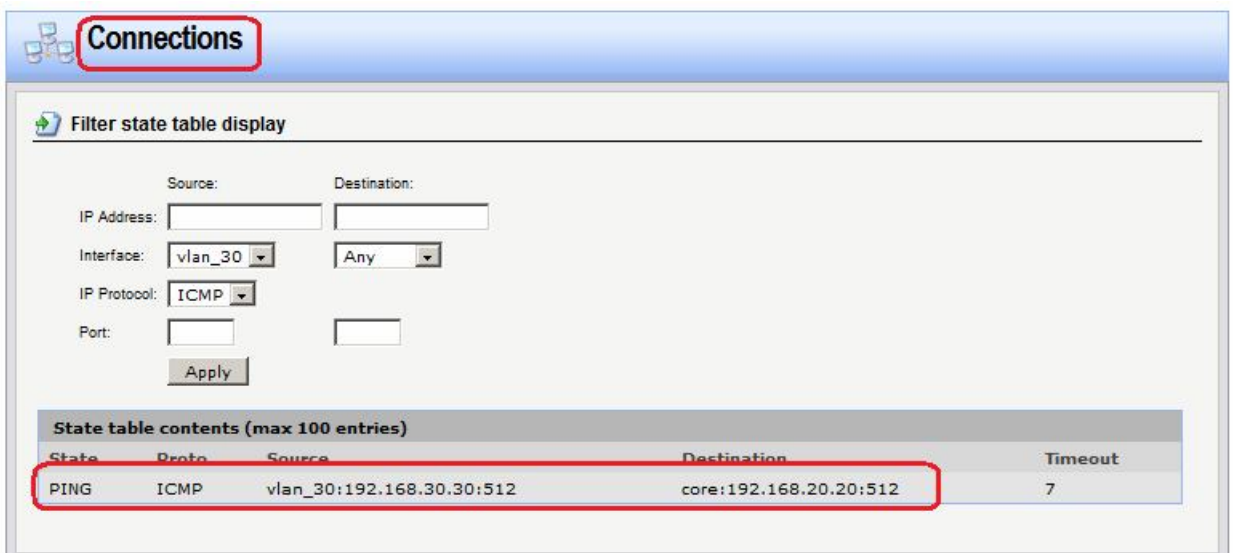


## Командная строка:

```
set IP4Group dns_net Members=vlan/vlan_30_ip,vlan/vlan_40_ip
```

## Проверка конфигурации

Проверяем созданную конфигурацию, используя команду ping.



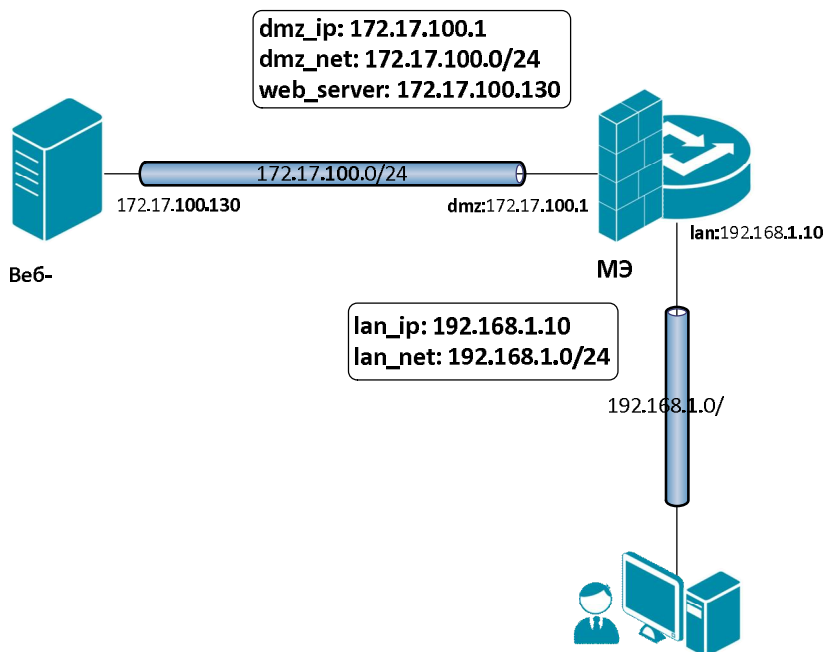
## Межсетевые экраны

### Лабораторная работа 5. Создание политики без проверки состояния

#### Цель

Создать политику без проверки состояния, которая должна разрешать http-трафик из локальной сети 192.168.1.0/24 к веб-серверу, расположенному в DMZ и имеющему IP-адрес 172.17.100.130.

#### Топология сети



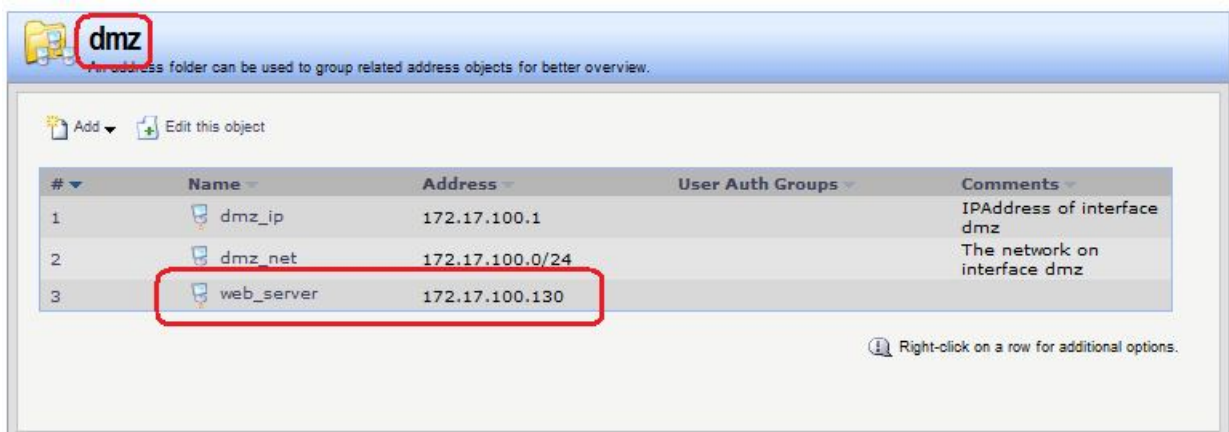
#### Описание практической работы

##### Объекты Адресной Книги

В адресную книгу следует добавить объект, указывающий IP-адрес веб-сервера.

##### Веб-интерфейс:

Object → Address Book → dmz



### Командная строка:

```
cc Address AddressFolder dmz  
add IP4Address web_server Address=172.17.100.130
```

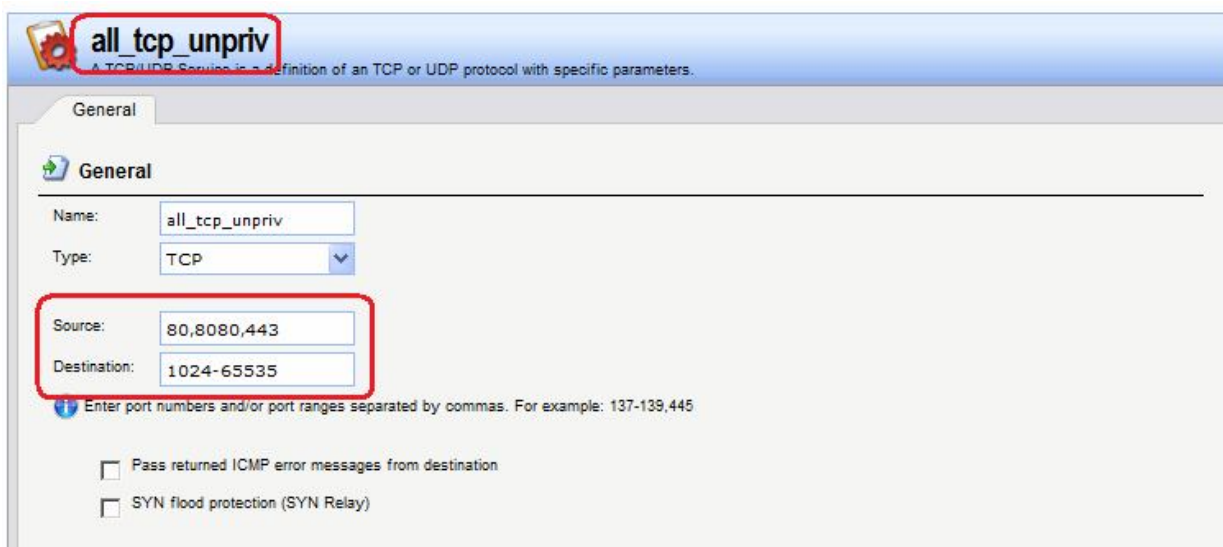
### Правила фильтрации

Правила без проверки состояния будем создавать на межсетевом экране 1 (МЭ 1).

1. Создаем сервис, в котором в качестве портов отправителя указаны все необходимые порты HTTP, а в качестве портов получателя указаны все непривилегированные порты (так называемые порты с «большими» номерами).

### Веб-интерфейс:

Object → Services → Add



### Командная строка:

```
add Service ServiceTCPUDP all_tcp_unpriv DestinationPorts=1024-65535  
SourcePorts=80,8080,443
```

2. Создаем два правила фильтрации с действием **FwdFast**. В первом правиле в качестве сервиса указываем стандартный сервис **http-all**, в котором в качестве портов отправителя указаны все порты с непривилегированными («большими») номерами, а в качестве портов получателя указаны порты, необходимые веб-серверу. Во втором правиле в качестве сервиса указываем созданный в п.1 сервис. Для входящего трафика (**web\_in**) открыты только порты, необходимые для протокола http. Для исходящего трафика (**web\_out**) открыты все непривилегированные порты, так как на стороне клиента порт может быть любой.

### Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: webS

Rules → IP Rules → webS → Add



### Командная строка:

```
add IPRuleFolder Name=webS
cc IPRuleFolder <N folder>

add IPRule Action=FwdFast SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=dmz DestinationNetwork= dmz/web_server Service=http-all
Name=web_in

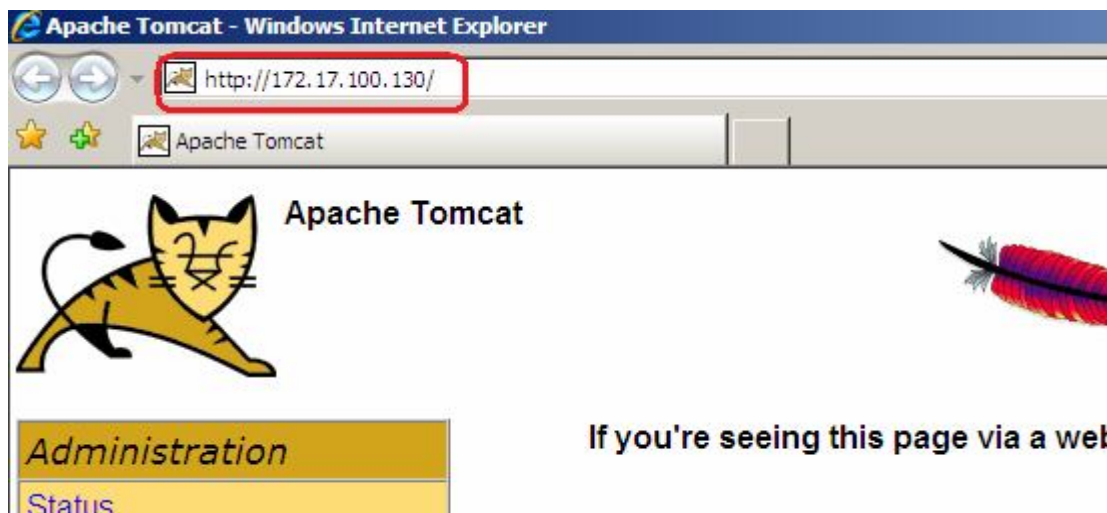
add IPRule Action=FwdFast SourceInterface=dmz SourceNetwork=dmz/web_server
DestinationInterface=lan DestinationNetwork=lan/lan_net
Service=all_tcp_unpriv Name=web_out
```

### Статическая маршрутизация

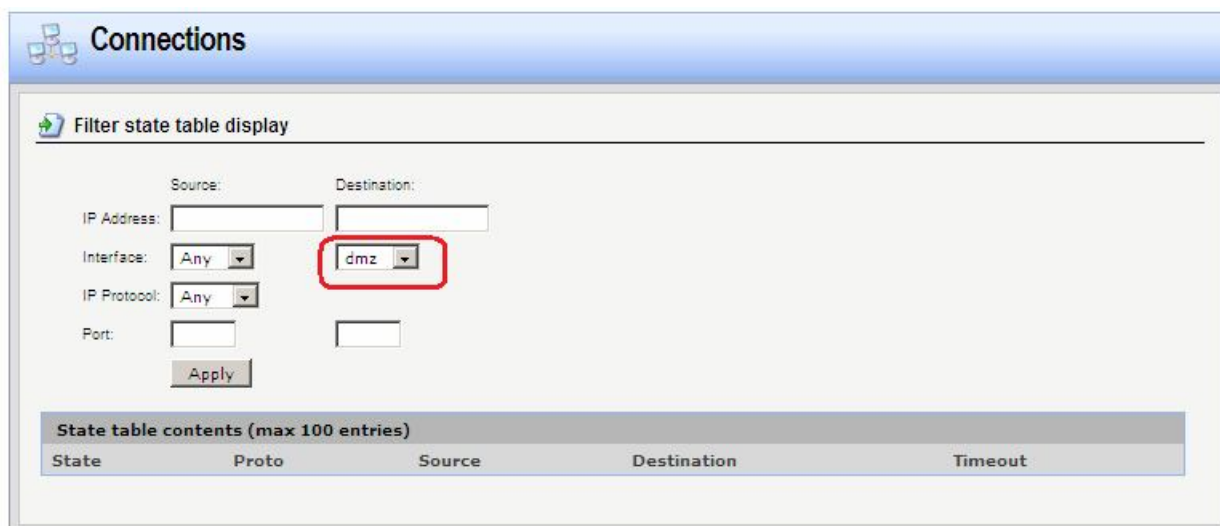
Правила маршрутизации созданы автоматически при определении параметров Ethernet-интерфейсов.

### Проверка конфигурации

Лабораторная работа 5. Используем браузер, в качестве адреса указываем IP-адрес.



Лабораторная работа 6. Проверяем, что таблица состояний для интерфейса **dmz** пустая.

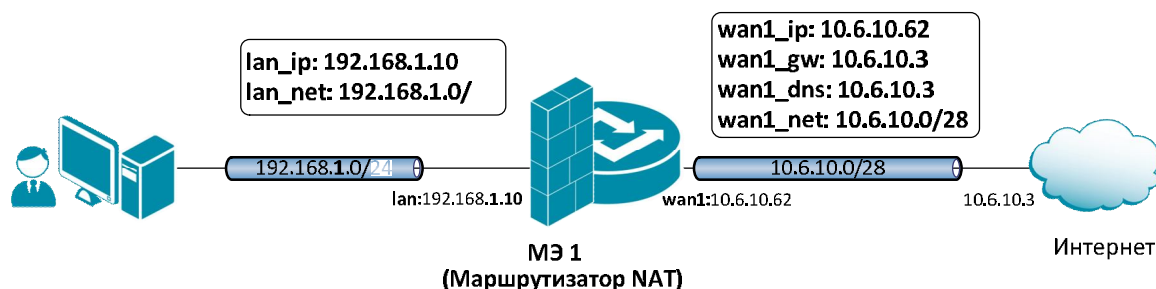


## Лабораторная работа 6. Создание политик для традиционного (или исходящего) NAT

### Цель

Создать политики для доступа пользователей, расположенных за NAT, во внешнюю сеть.

### Топология сети



### Описание практической работы

#### Статическая маршрутизация

Правила маршрутизации созданы автоматически при определении параметров Ethernet-интерфейсов.

#### Правила фильтрации

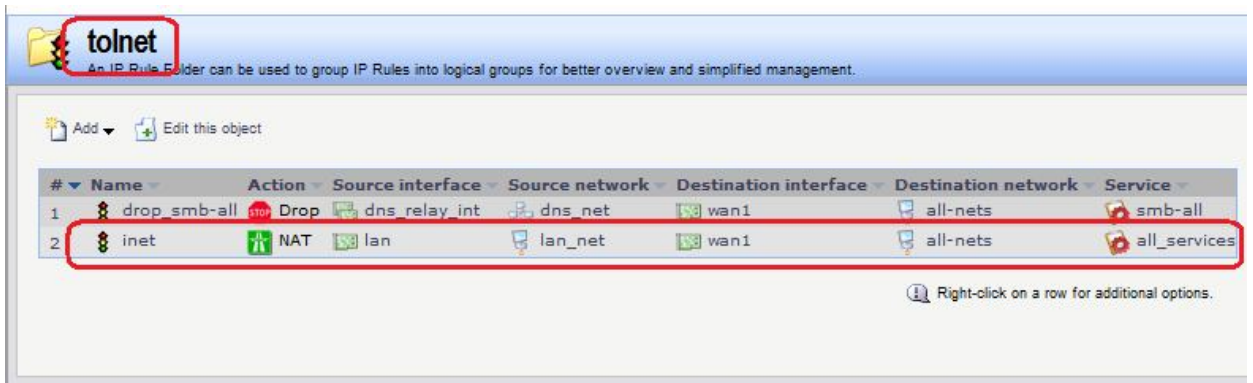
Создаем правило с действием NAT.

#### Веб-интерфейс:

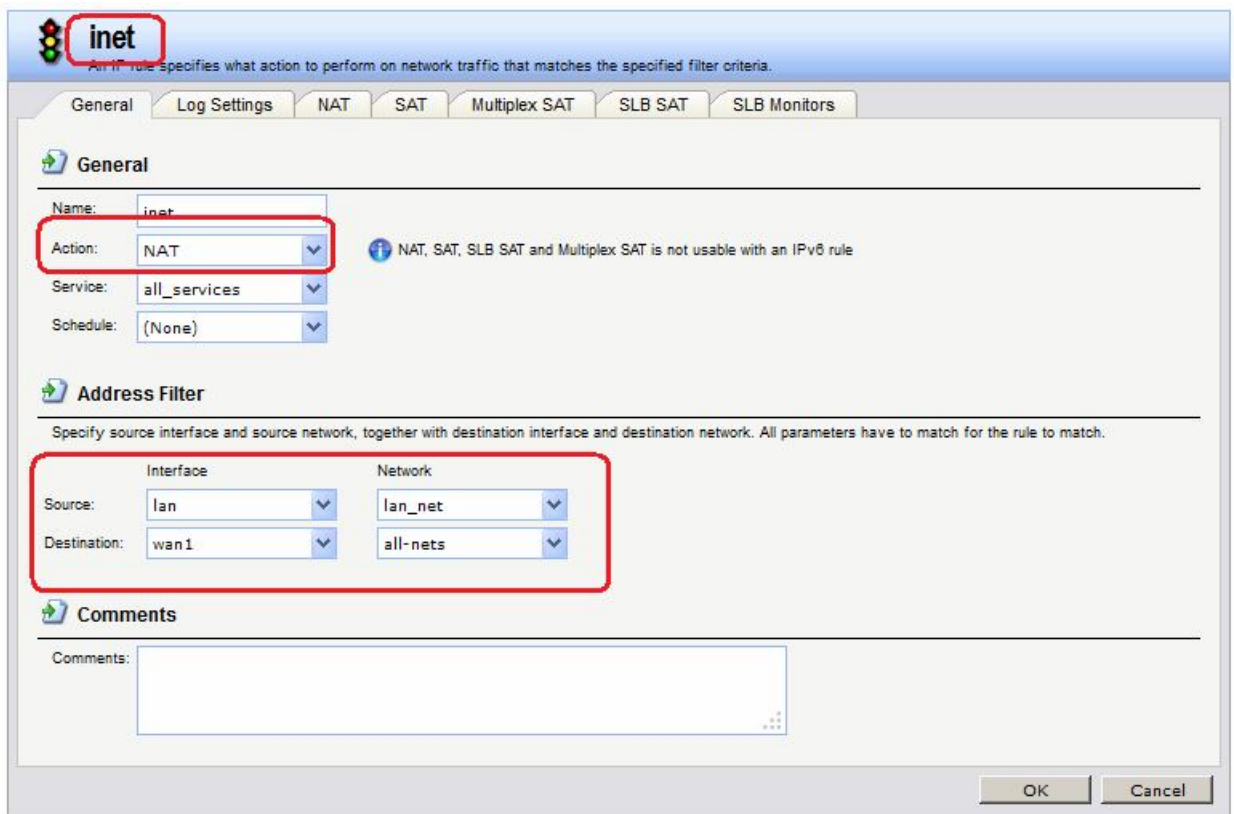
Rules → IP Rules → Add → IP Rule Folder

Name: toInet

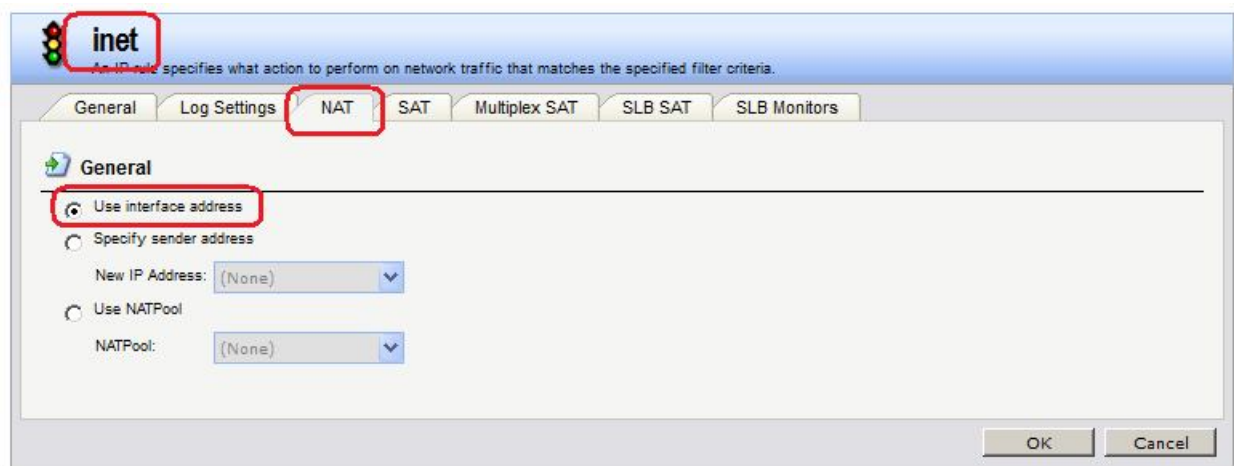
Rules → IP Rules → Add → toInet



На вкладке **General** указано действие **NAT** и интерфейсы и сети источника и получателя:



1. На вкладке **NAT** указано использование адреса интерфейса в качестве адреса источника:



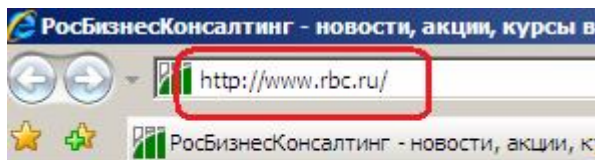
**Командная строка:**

```
add IPRuleFolder Name=toInet
```

```
cc IPRuleFolder <N folder>
```

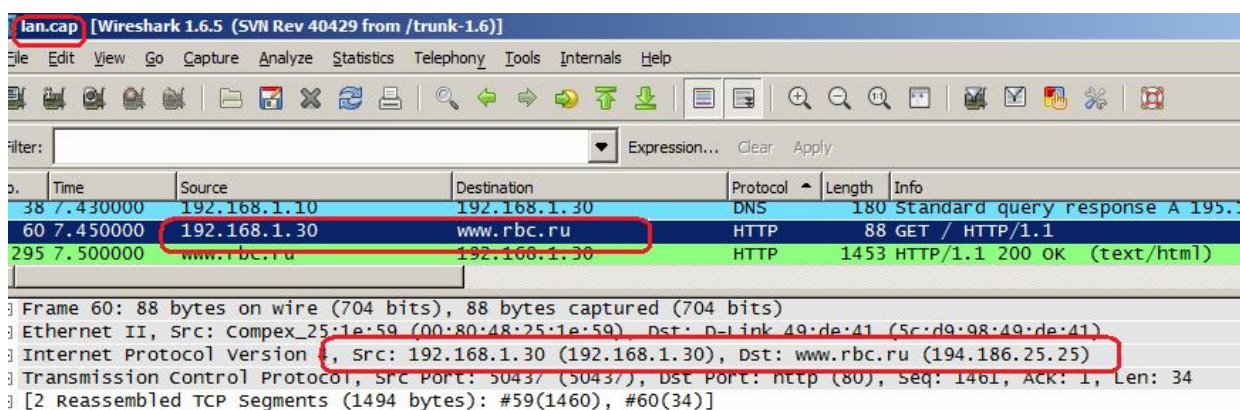
```
add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net  
DestinationInterface=wan1 DestinationNetwork= all-nets Service=all_services  
Name=inet
```

Проверяем возможность выхода в интернет.

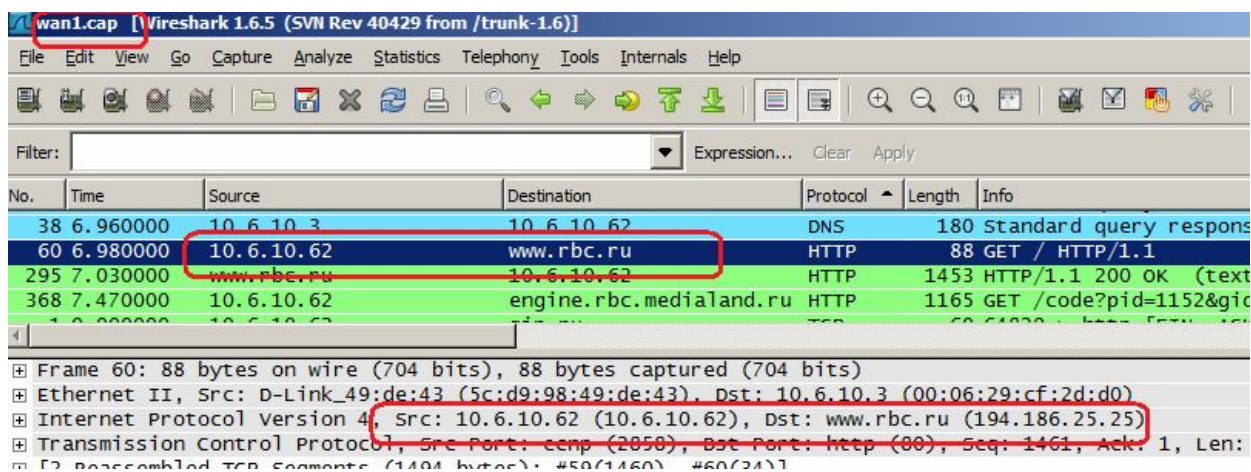


Проверяем выполнение преобразования NAT.

До преобразования NAT:



После преобразования NAT:



2. На вкладке **NAT** указан IP-адрес, который будет использоваться в качестве IP-адреса источника. Данный IP-адрес должен быть предварительно создан в Адресной Книге.

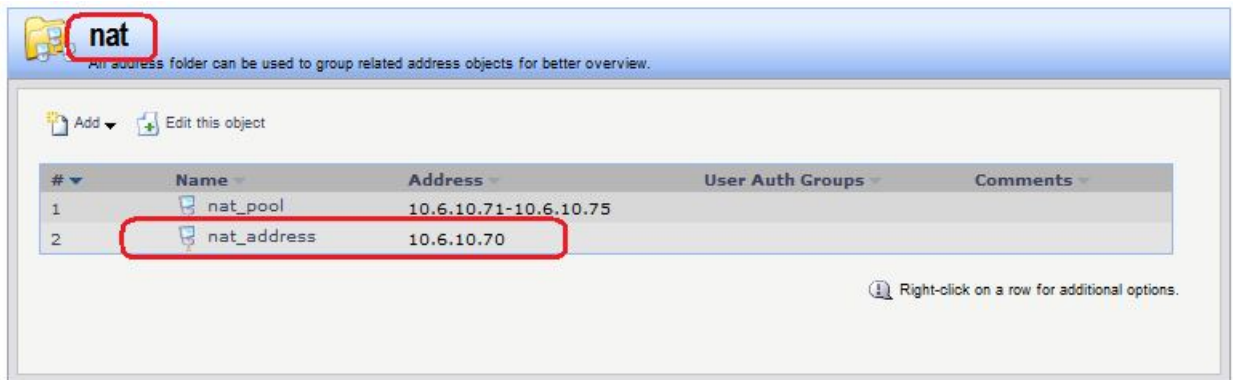
### Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: nat

Object → Address Book → nat





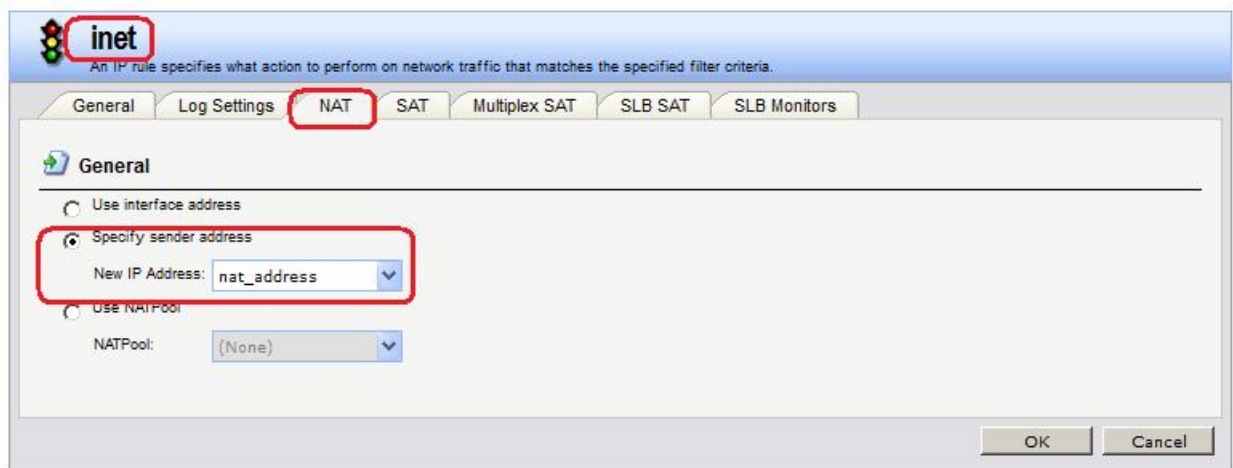
### Командная строка:

```
add Address AddressFolder nat
```

```
cc Address AddressFolder nat
```

```
add IP4Address nat_address Address=10.6.10.70
```

### Веб-интерфейс:



### Командная строка:

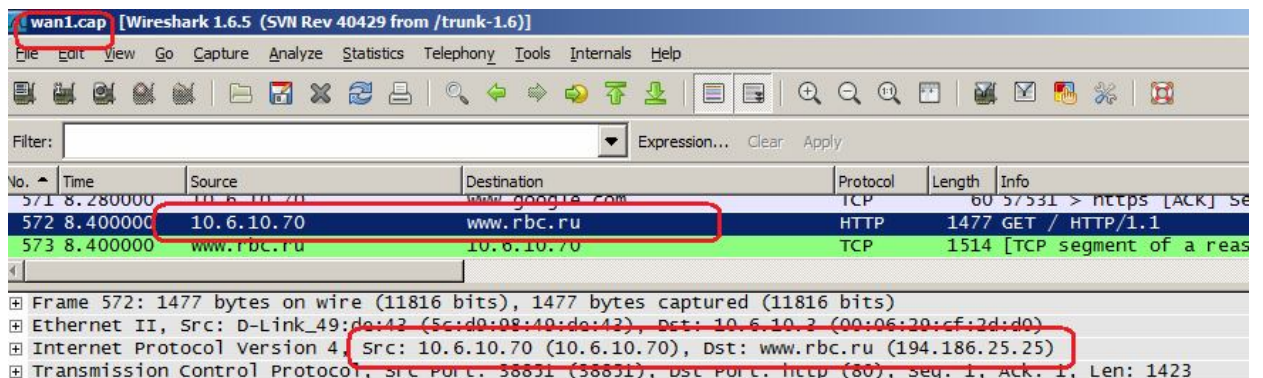
```
cc IPRuleFolder <N folder>
```

```
set IPRule <N rule> NATAction=SpecifySenderAddress
```

```
NATSenderAddress=nat/nat_address
```

Проверяем выполнение преобразования NAT.

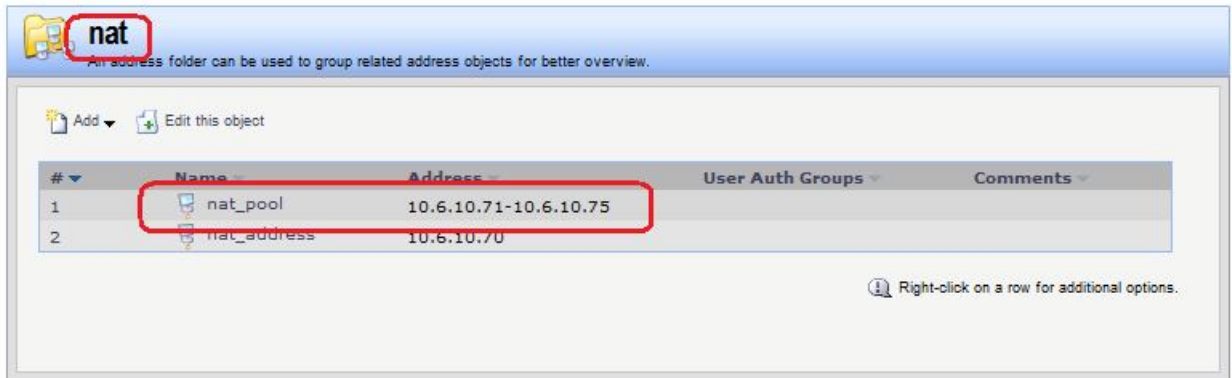
После преобразования NAT:



Лабораторная работа 7. На вкладке **NAT** указано использование NAT-пула, IP-адреса из которого будут использоваться в качестве IP-адреса источника. Данный NAT-пул должен быть предварительно создан.

**Веб-интерфейс:**

Object → Address Book → nat

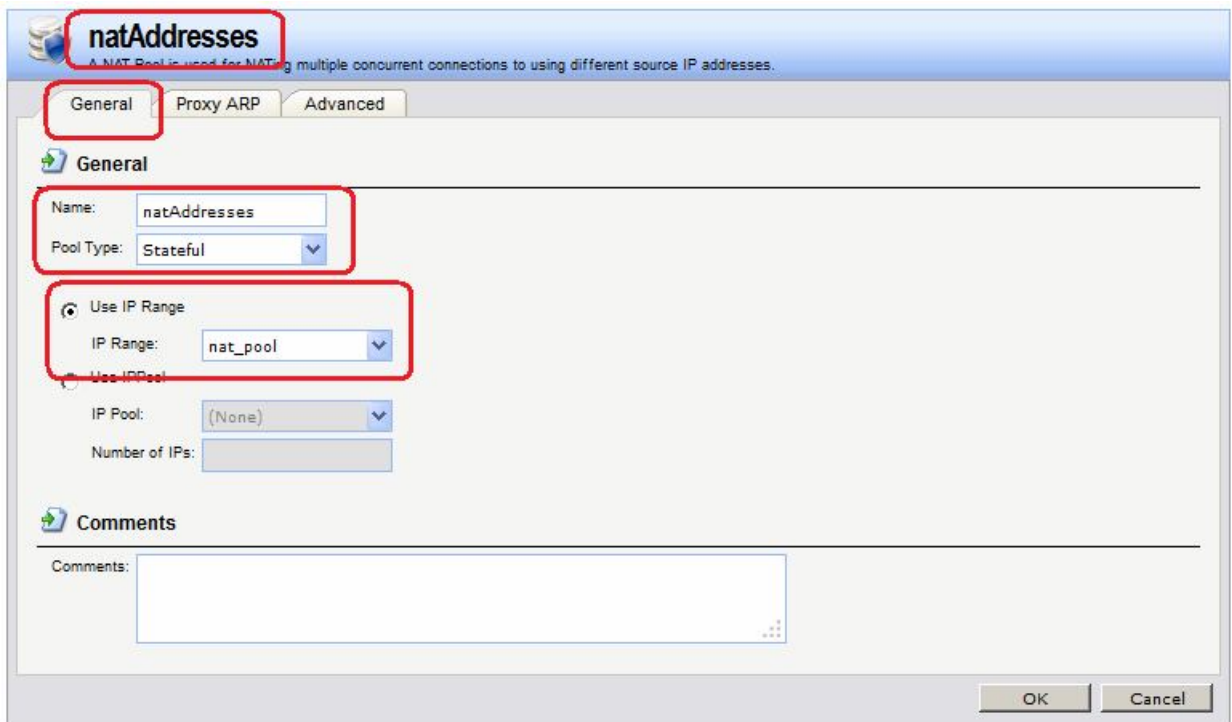


**Командная строка:**

```
cc Address AddressFolder nat
add IP4Address nat_pool Address=10.6.10.71-10.6.10.75
```

**Веб-интерфейс:**

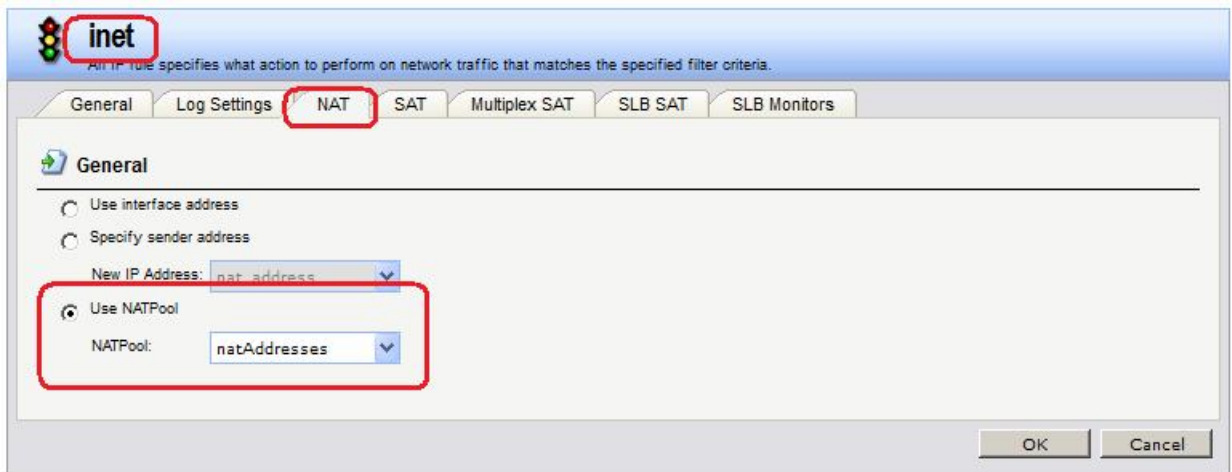
Object → NAT Pools → Add



**Командная строка:**

```
add NATPool natAddresses IPRange=nat/nat_pool
```

**Веб-интерфейс:**



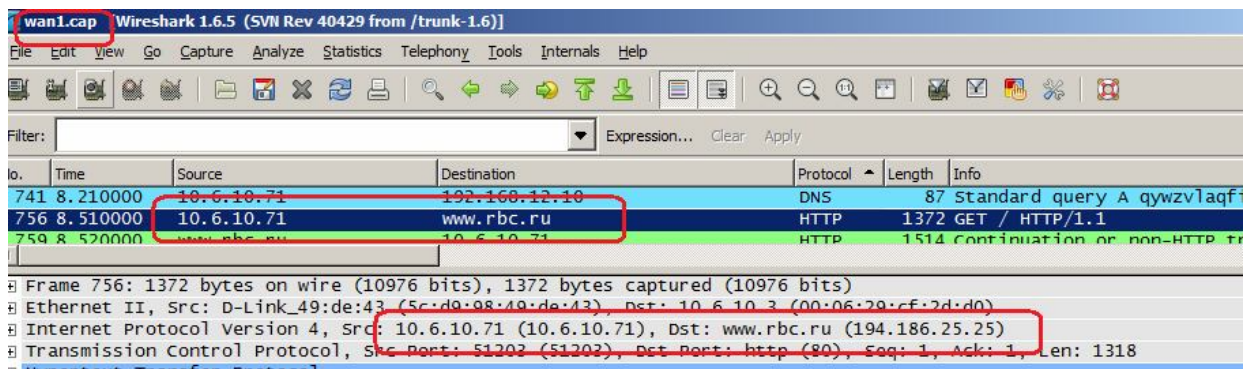
### Командная строка:

```
cc IPRuleFolder <N folder>
```

```
set IPRule <N rule> NATAction=UseNATPool NATPool=natAddresses
```

Проверяем выполнение преобразования NAT.

После преобразования NAT:

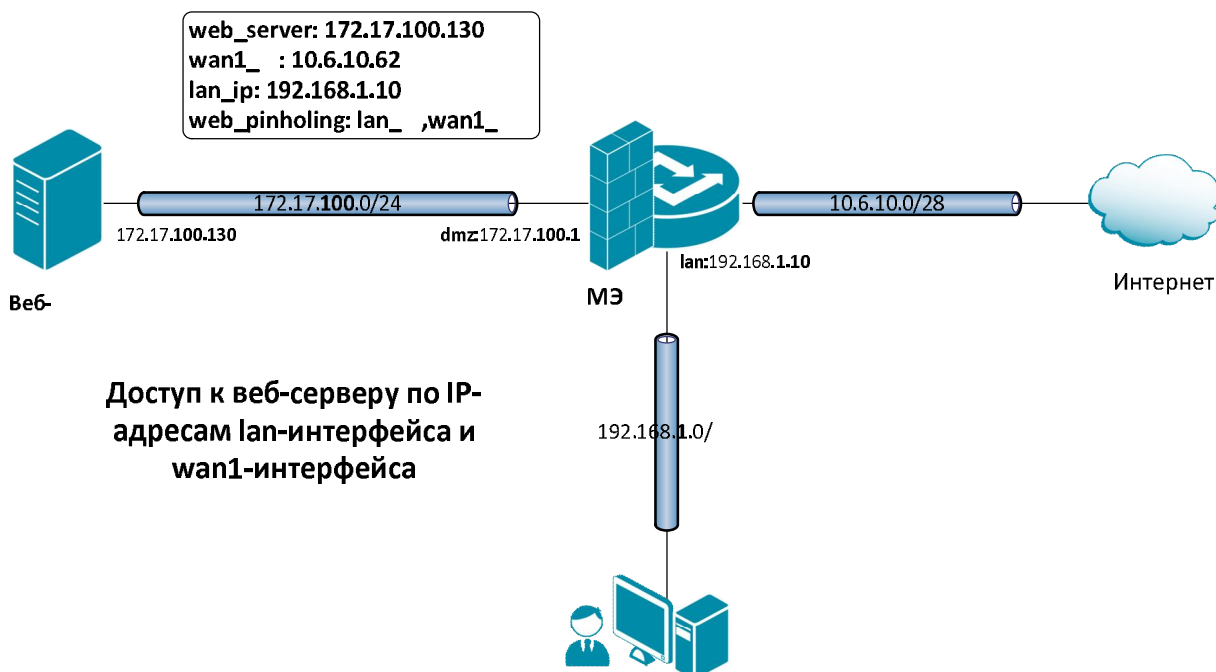


## Лабораторная работа 7. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing

### Цель

Создать политики для доступа к серверу, расположенному за NAT, используя метод pinholing, т.е. используя IP-адрес межсетевого экрана.

## Топология сети



## Описание практической работы

### **Проверка отсутствия конфликта по портам**

Метод pinholing некоторые производители называют SAT.

К веб-серверу будут обращаться по IP-адресу МЭ 1, поэтому следует гарантировать отсутствие конфликта по портам с удаленным администрированием МЭ 1. Это можно сделать несколькими способами.

1. Указать номер порта для удаленного администрирования, отличный от номера порта веб-сервера.

### **Веб-интерфейс:**

System → Remote Management → Advanced Settings

## Remote Management Settings

Setup and configure methods and permissions for remote management of this system.

General

### General

SSH Before Rules:  Enable SSH traffic to the security gateway regardless of configured IP R...

Local Console Timeout:  Number of seconds of inactivity until the local console user is automatica

Validation Timeout:  Specifies the amount of seconds to wait for the administrator to log in bef previous configuration.

### WebUI

WebUI Before Rules:  Enable HTTP(S) traffic to the security gateway regardless of configured IP

WebUI Idle timeout:  Number of seconds of inactivity until the HTTP(S) session is closed.

WebUI HTTP port:  Specifies the HTTP port for the web user interface.

WebUI HTTPS port:  Specifies the HTTPS port for the web user interface.

WebUI Allow Login Auto Complete:  Allow the web browser to remember the username and password on the log

HTTPS Certificate:  Specifies which certificate to use for HTTPS traffic. Only RSA certificate:

### Командная строка:

```
set Settings RemoteMgmtSettings WWWSrv_HTTPPort=82 WWWSrv_HTTPSPort=444
```

- Указать номер порта для доступа к веб-серверу, отличный от номера порта для удаленного администрирования. При этом номер порта на самом веб-сервере можно не изменять, достаточно создать новый http-сервис с номером порта, отличным от порта удаленного администрирования. Будем предполагать, что используется второй способ.

### Веб-интерфейс:

Object → Services → Add

Name: http\_8080

## http\_8080

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

### General

Name:

Type:

Source:

Destination:

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

Pass returned ICMP error messages from destination

SYN flood protection (SYN Relay)

### Командная строка:

```
add Service ServiceTCPUDP http_8080 DestinationPorts=8080 SourcePorts=0-65535
```

### Объекты Адресной Книги

Чтобы иметь возможность использовать в качестве адреса веб-сервера IP-адреса интерфейсов, к которым подсоединены сети, а также для того, чтобы в правилах фильтрации доступ к веб-серверу описать с помощью единственного правила, создадим дополнительные объекты в Адресной Книге.

### Веб-интерфейс:

Object → Address Book → nat



### Командная строка:

```
cc Address AddressFolder nat
```

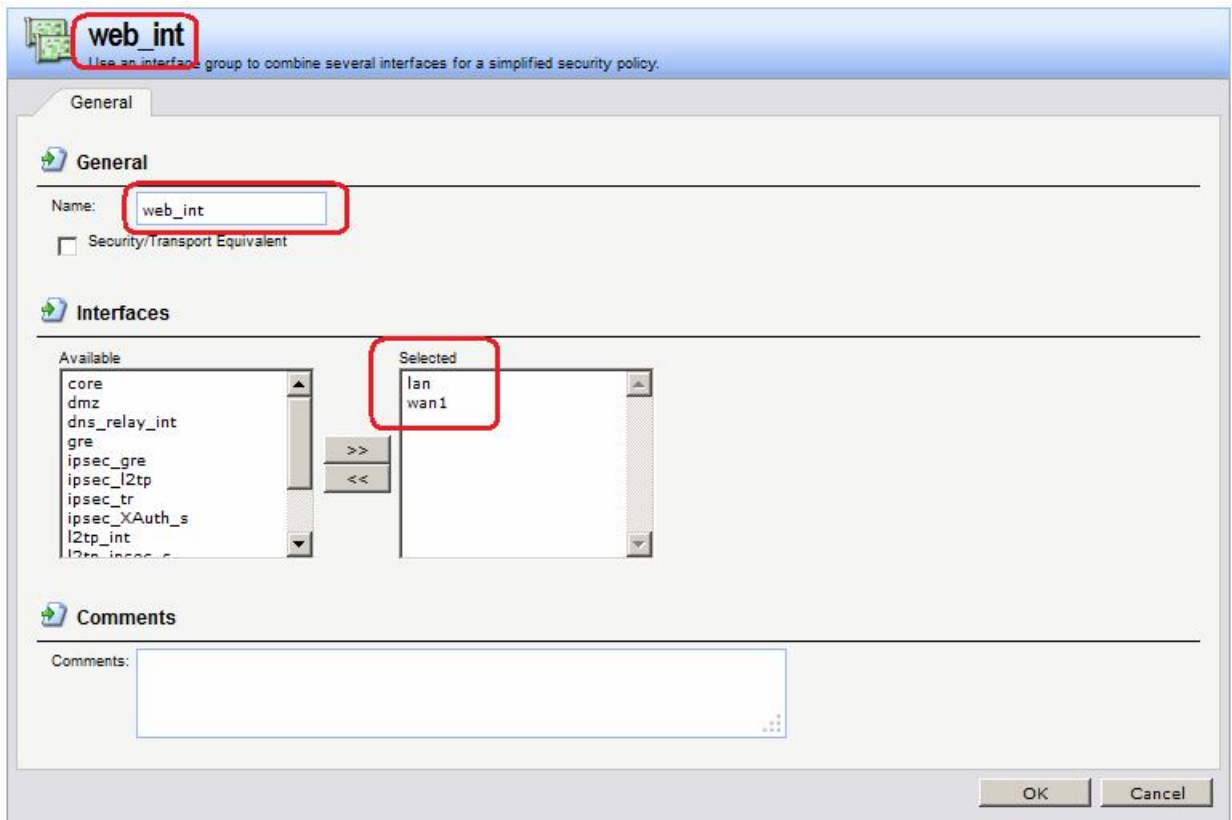
```
add IP4Group web_pinholing Members =lan/lan_ip, wan1/wan1_ip
```

### Группа интерфейсов

Объединить интерфейсы в Группу, чтобы несколько интерфейсов можно было указывать одним параметром в Правилах фильтрации.

### Веб-интерфейс:

Interfaces → Interface Group → Add



### Командная строка:

```
add Interface InterfaceGroup web_int Members=lan,wan1
```

### Правила фильтрации

Создать два правила фильтрации с действием **SAT**. В первом правиле качестве сервиса указать http, во втором правиле - https. Интерфейсом получателя должен быть core. Адрес получателя – IP-адреса интерфейсов, которые будут указываться клиентом в качестве веб-сервера. В нашем случае это группа интерфейсов web\_int.

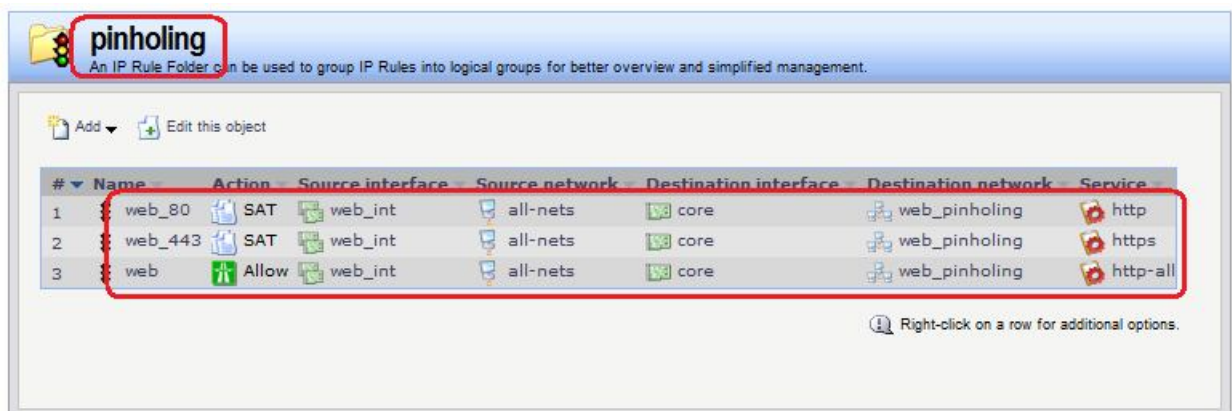
Создать правило фильтрации с действием **Allow**.

### Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: pinholing

Rules → IP Rules → pinholing → Add



На вкладке **SAT** указать адрес веб-сервера и порт, который он слушает. Если необходимо, чтобы веб-сервер слушал несколько портов, например, 80 (http) и 443 (https), то требуется два правила **SAT**.

The screenshot shows the configuration window for an IP rule named 'web\_80'. The 'SAT' tab is selected. Under the 'General' section, 'Destination IP' is selected for translation. The 'New IP Address' is set to 'web\_server' and the 'New Port' is set to '80'. The 'All-to-One Mapping' checkbox is checked. A tooltip indicates that the port value is only applicable for TCP/UDP services with a single port or a port range without gaps. 'OK' and 'Cancel' buttons are at the bottom right.

The screenshot shows the configuration window for an IP rule named 'web\_443'. The 'SAT' tab is selected. Under the 'General' section, 'Destination IP' is selected for translation. The 'New IP Address' is set to 'web\_server' and the 'New Port' is set to '443'. The 'All-to-One Mapping' checkbox is checked. A tooltip indicates that the port value is only applicable for TCP/UDP services with a single port or a port range without gaps. 'OK' and 'Cancel' buttons are at the bottom right.

### Командная строка:

```
cc IPRuleFolder <N Folder>
```

```
add IPRule Action=SAT SourceInterface=web_int SourceNetwork=all-nets  
DestinationInterface=core DestinationNetwork=nat/web_pinholing Service=http  
SATTranslateToIP=dmz/web_server SATAllToOne=Yes SATTranslateToPort=80  
Name=web_80
```

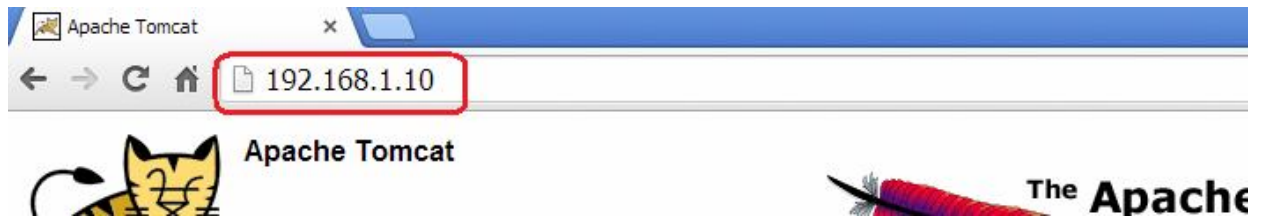
```
add IPRule Action=SAT SourceInterface=web_int SourceNetwork=all-nets  
DestinationInterface=core DestinationNetwork=nat/web_pinholing Service=https  
SATTranslateToIP=dmz/web_server SATAllToOne=Yes SATTranslateToPort=443  
Name=web_443
```

```
add IPRule Action=Allow SourceInterface=web_int SourceNetwork=all-nets  
DestinationInterface=core DestinationNetwork=nat/web_pinholing Service=http-  
all Name=web
```

### Проверка конфигурации

Заходим браузером по IP-адресу МЭ 1 и сконфигурированному номеру порта.





# Системы обнаружения и предотвращения проникновений

## Лабораторная работа 8. Антивирусное сканирование

### Принципы использования антивирусной защиты

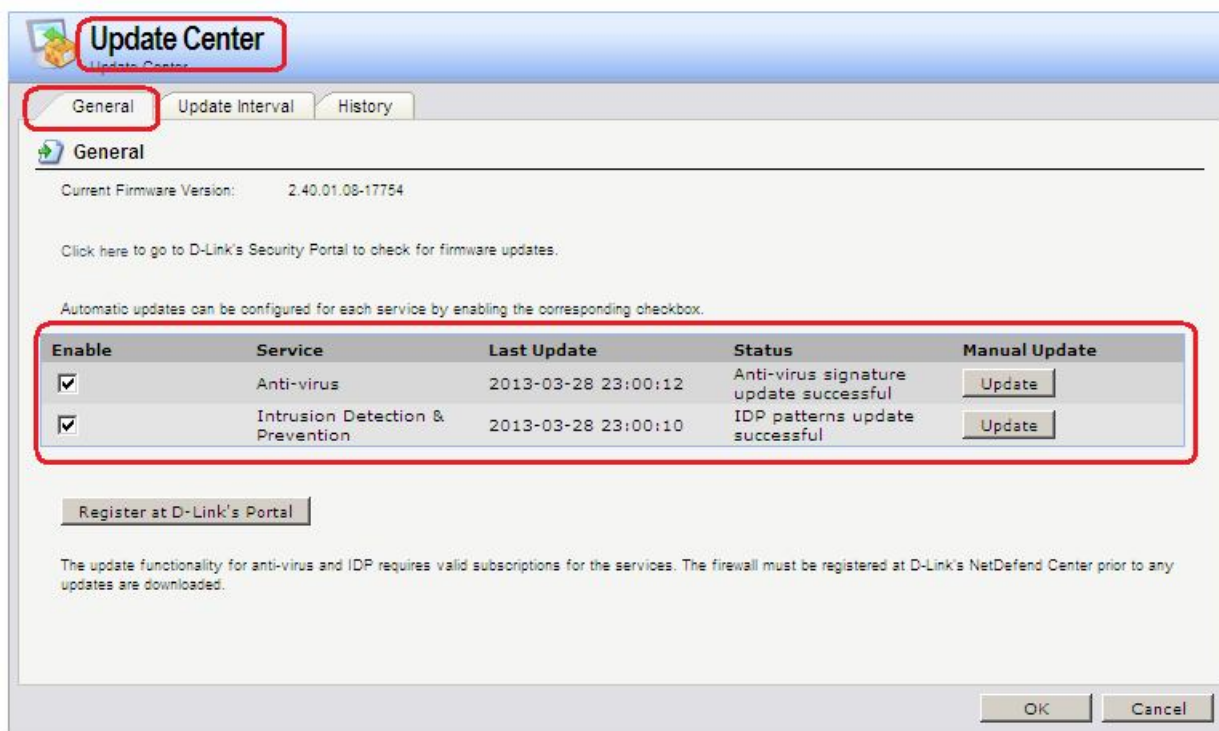
Антивирусный модуль NetDefendOS обеспечивает защиту от вредоносного кода, который может содержаться в файлах, загружаемых из интернет. Файлы могут быть загружены как часть веб-страницы, полученной по протоколу HTTP, могут быть загружены по протоколу FTP или получены в виде вложений в электронную почту по протоколу SMTP. Вредоносный код во всех этих примерах может использоваться для различных целей, начиная от программ раздражающего воздействия до более злонамеренных действий, например, получение паролей, номеров кредитных карт и другой конфиденциальной информации. Термин «вирус» может быть использован как общее описание для всех видов вредоносного кода, переносимого файлами.

#### 1. Настройка корректного системного времени и проверка наличия обновлений

Очень важно установить правильное системное время, если функция автоматического обновления антивирусных баз данных включена. Неправильное время может означать, что автоматическое обновление отключено.

#### Веб-интерфейс:

Maintenance → Update Center



#### Командная строка:

```
updatecenter -status
```

- Совместное использование с клиентским антивирусным сканированием

В отличие от системы обнаружения и предотвращения вторжений (IDP), которая в основном применяется для защиты серверов, антивирусное сканирование применяется для защиты клиентов при загрузках файлов. Антивирус NetDefendOS разработан как дополнение к стандартному антивирусному сканированию, которое обычно выполняется локально специализированным программным обеспечением, установленным на клиентских компьютерах. Антивирусное сканирование не предназначено для полноценной замены локального сканирования, а скорее является дополнительной функцией для повышения безопасности. Оно может также выступать в качестве резервной защиты, когда локальному клиенту не доступно антивирусное сканирование.

- **Сканирование потока**

Так как передача файлов выполняется через межсетевой экран, то, если антивирусный модуль включен, система NetDefendOS будет сканировать поток данных на наличие вирусов. Так как файлы представляют собой поток трафика и не хранятся целиком в памяти, для такого сканирования требуется меньший объем памяти, и, как следствие, влияние на общую пропускную способность будет минимальным.

- **Сопоставление с шаблоном**

Процесс проверки основан на сопоставлении с базой данных известных вирусов, что с высокой степенью достоверности помогает определить наличие вируса. Как только в передаваемом файле обнаружен вирус, загрузка прекращается.

- **Типы сканируемых загружаемых файлов**

Как описано выше, антивирусное сканирование запускается как часть ALG и может анализировать загружаемые файлы, передаваемые по протоколам HTTP, FTP, SMTP и POP3. В частности:

- Может быть просканирован любой тип несжатого файла, с которым связан соответствующий ALG.
- Если загружаемый файл сжат, то форматы ZIP и GZIP также могут быть просканированы.

Можно запретить загрузку определенных файлов, а также указать ограничение размера сканируемых файлов. Если размер не указан, то по умолчанию максимальный размер файлов не ограничен.

- **Одновременное выполнение нескольких сканирование**

Не существует ограничения, сколько антивирусных сканирований может быть одновременно выполнено на одном межсетевом экране. Количество одновременных выполнений сканирований определяется доступным объемом памяти.

- **Учет специфики конкретного протокола**

Так как антивирусное сканирование реализовано с использованием ALG, может учитываться специфика конкретного протокола. Например, для FTP сканирование выполняется как для потока команд, так и для потока данных. Если обнаружен вирус, то команда на прекращение загрузки посылается через управляющее соединение.

- **Взаимосвязь с IDP**

Порядок, в котором выполняются антивирусное сканирование и IDP-сканирование, не важен, так как эти процессы выполняются на разных уровнях стека протокола. Поэтому антивирусное сканирование и IDP-сканирование могут происходить одновременно.

Если функция IDP включена, выполняется сканирование всех пакетов, которые соответствуют определенному правилу IDP, без учета семантики протоколов более

высокого уровня, таких как HTTP. В противоположность этому антивирус осведомлен о семантике протоколов более высокого уровня и просматривает только данные, относящиеся к этим протоколам. Антивирусное сканирование является частью шлюза прикладного уровня, а IDP нет.

- **База данных сигнатур SafeStream**

Антивирусное сканирование выполняется системой NetDefendOS D-Link с использованием баз данных сигнатур вирусов SafeStream. База данных SafeStream создана и поддерживается лабораторией Касперского – компанией, которая является мировым лидером в области обнаружения вирусов. База данных обеспечивает защиту от всех известных вирусов, включая троянские программы, «червей», «backdoor» и другие.

- **Обновление базы данных**

База данных SafeStream обновляется ежедневно, добавляя сигнатуры новых вирусов. Старые сигнатуры редко удаляются, вместо этого они заменяются более общими сигнатурами, которые охватывают несколько вирусов. Поэтому локальная копия NetDefendOS базы данных SafeStream должна регулярно обновляться, и этот сервис обновления является частью подписки на Антивирус D-Link.

## **Описание практической работы**

### ***Использование шлюза прикладного уровня (ALG) для активизация антивирусного сканирования***

#### **1. Реакция на невозможность выполнения проверки на наличие вирусов**

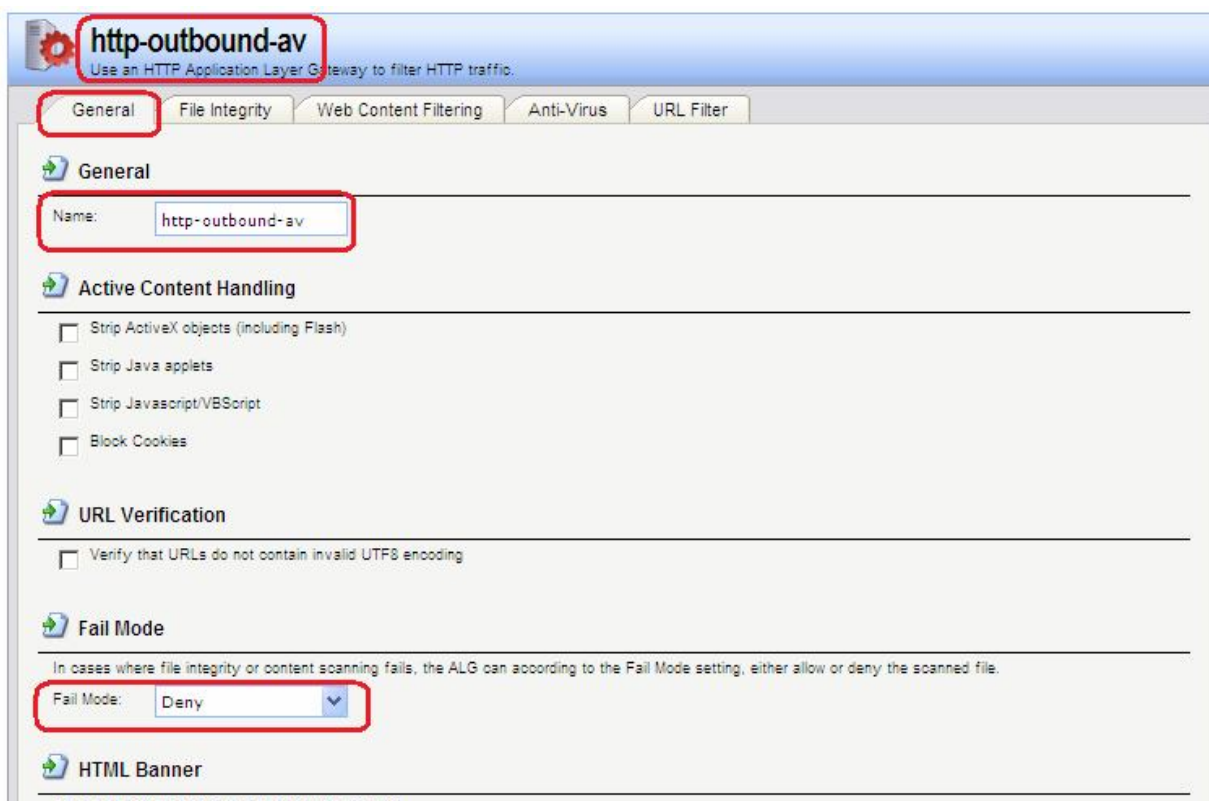
Антивирус NetDefendOS активизируется с помощью шлюза прикладного уровня (ALG), который связан с соответствующим протоколом. Активизация доступна для загружаемых файлов, связанных со следующими ALG и включается непосредственно в самом ALG:

- **HTTP ALG**
- **FTP ALG**
- **POP3 ALG**
- **SMTP ALG**

Если по какой-либо по причине не удастся выполнить проверку на наличие вирусов, то при режиме **Deny** дальнейшая передача данных прекращается, при этом данное событие регистрируется в логах. Если установлен режим **Allow**, то ситуация, когда антивирусные базы не доступны или текущая лицензия не действительна, не приведет к запрещению пересылки. В этом случае пересылка файлов будет разрешена, и будет сгенерировано сообщение в логах, указывающее на то, что произошел сбой.

#### **Веб-интерфейс:**

**Object → ALG with AV/WCF → Add → HTTP ALG**



## 2. Режим сканирования

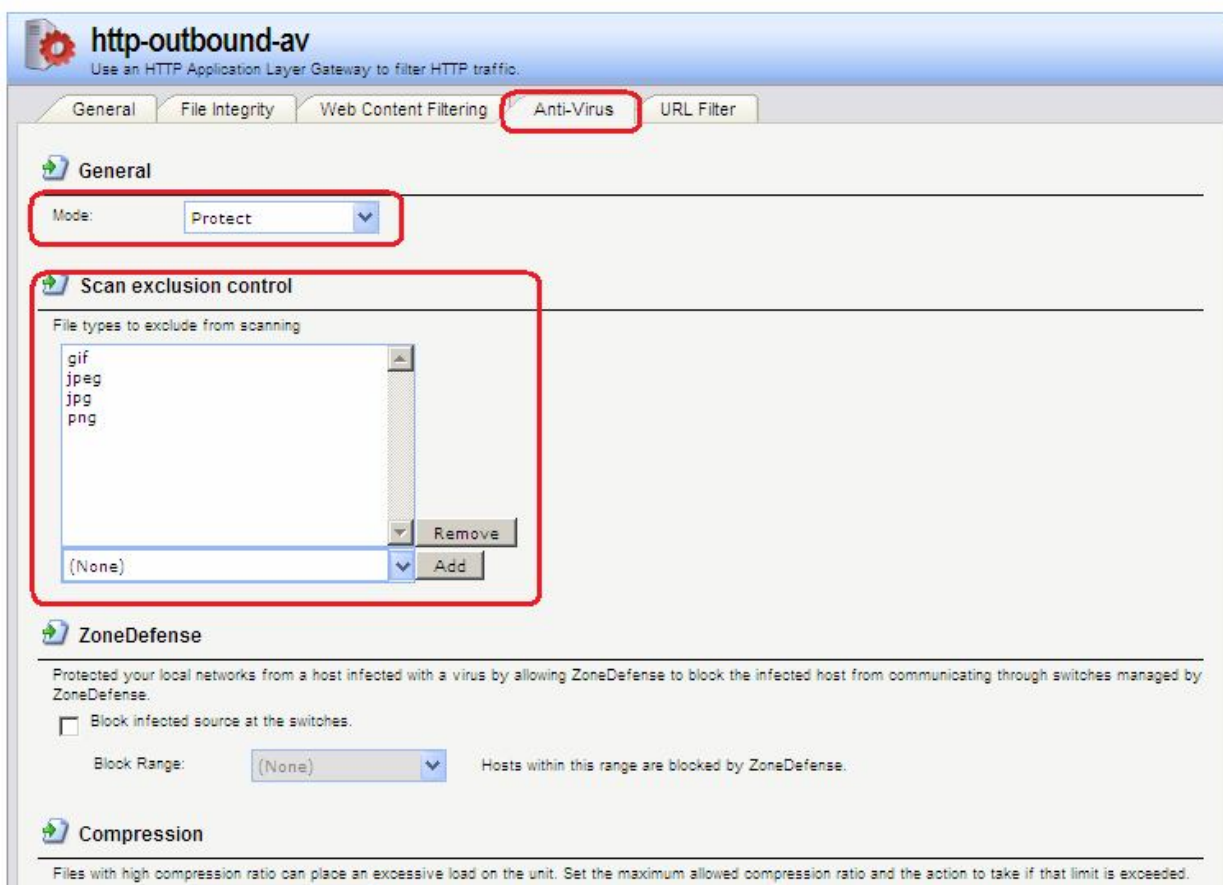
Режим сканирования может быть следующим:

- **disabled** – Функция Антивируса выключена.
- **Audit** – Сканирование активизировано, но единственным действием является ведение логов.
- **Protect** – Функция Антивируса активизирована. Подозрительные файлы будут удалены, информация об этом будет записана в логи.

## 3. Исключение из сканирования

При необходимости можно явно отменить сканирование файлов с определенным расширением. Данное действие может увеличить общую пропускную способность, если загрузка файлов с данным расширением часто используется в каком-либо протоколе, например, HTTP.

NetDefendOS выполняет проверку всех MIME-расширений файлов, чтобы установить, что расширение файла корректно и затем посмотреть, не находится ли это расширение в списке исключенных.



#### 4. Ограничение степени сжатия

При сканировании сжатых файлов файл сначала распаковывается. В некоторых случаях распакованный файл намного больше сжатого. Это означает, что сравнительно небольшое вложение сжатого файла может значительно израсходовать ресурсы межсетевого экрана и заметно снизить пропускную способность.

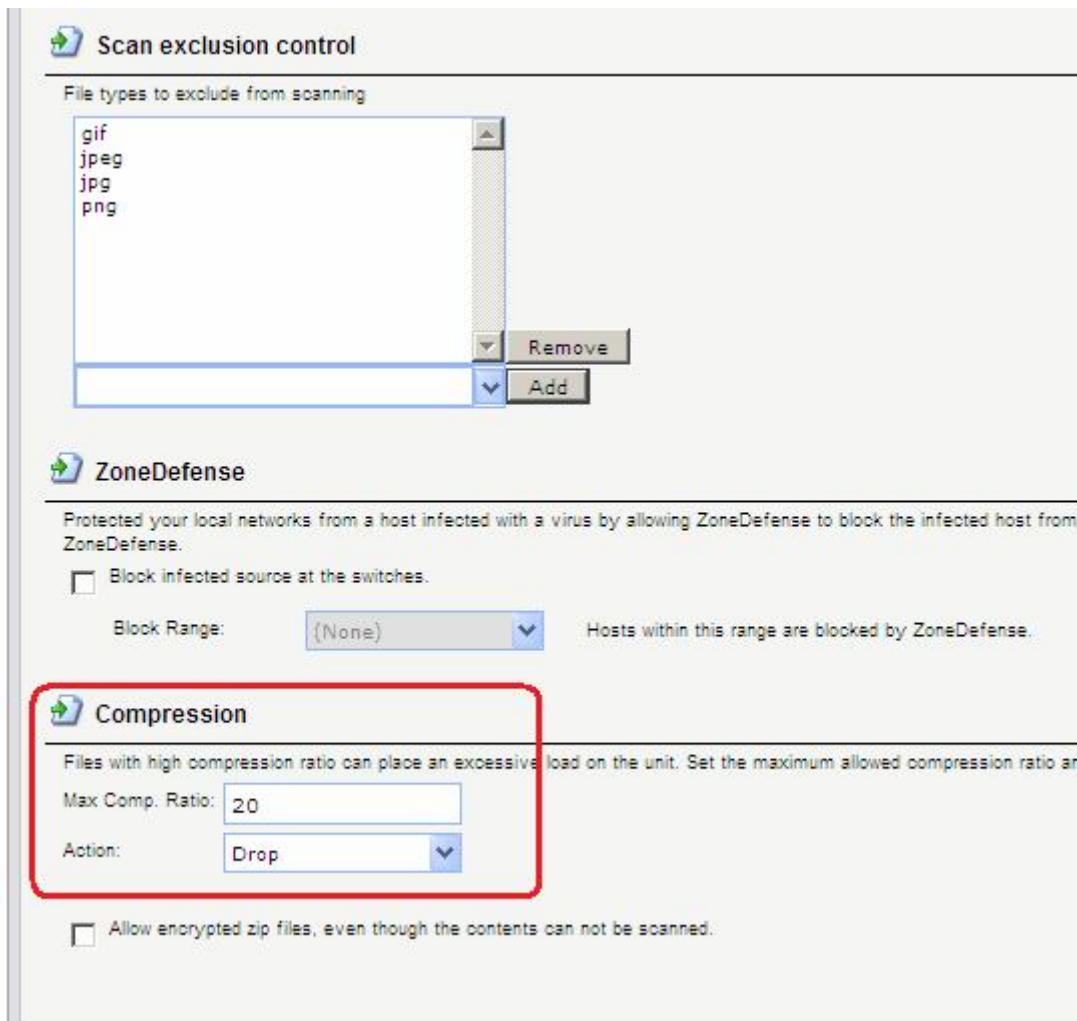
Для предотвращения подобной ситуации, следует указать предел степени сжатия (**Compression Ratio**). Если предел степени сжатия указан 20, то это будет означать, что, если несжатый файл в 20 раз больше, чем сжатый, то следует выполнить одно из следующих действий:

**Allow** – Разрешить передачу файла без проверки на наличие вирусов

**Scan** – Сканировать файл на наличие вирусов

**Drop** – Отбросить файл

В любом случае данное событие заносится в логи.

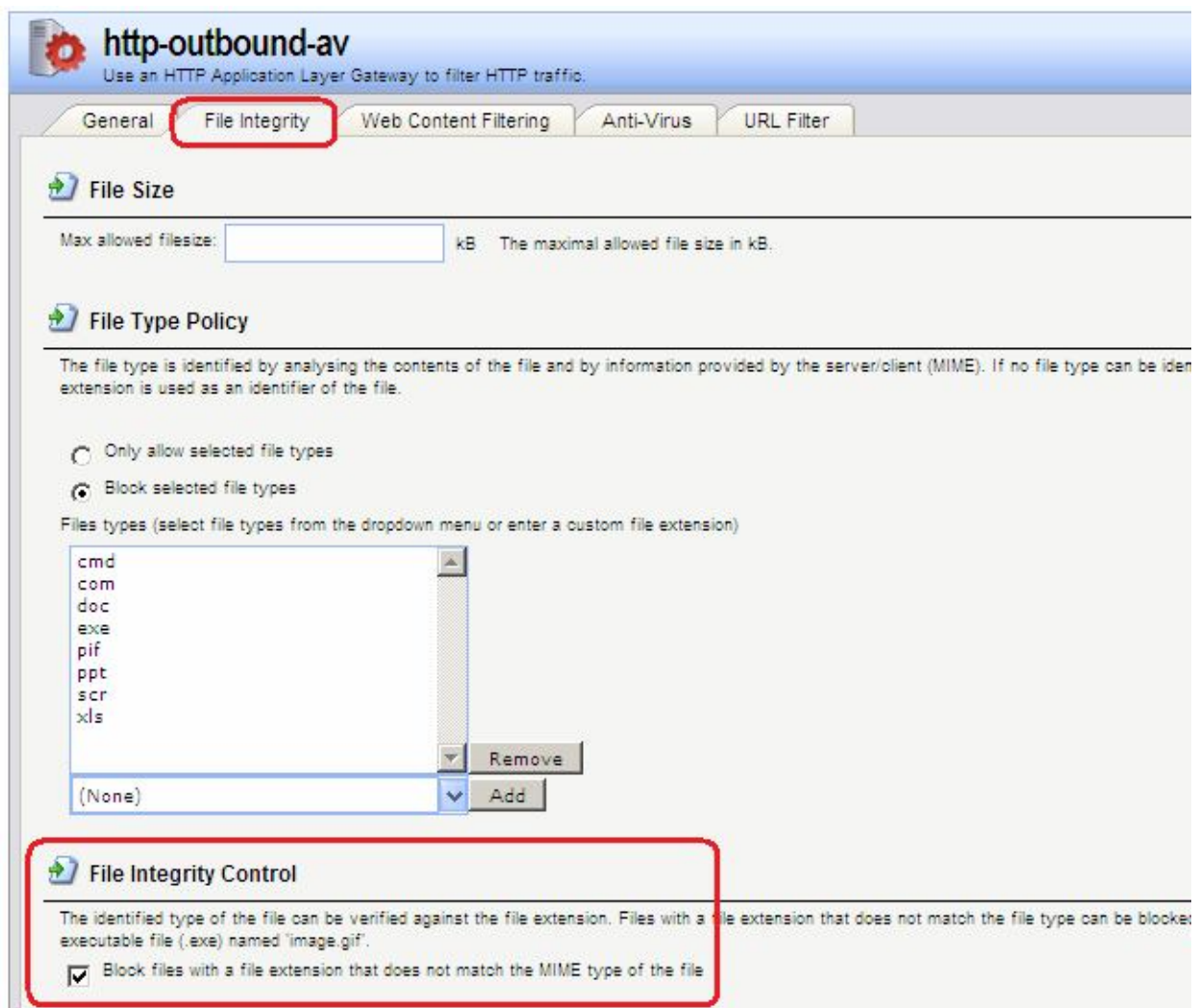


## 5. Проверка файлов на соответствие типам MIME

Параметр ALG **File Integrity** могут быть использован совместно с антивирусным сканированием для того, чтобы проверить, соответствует ли содержание файла типу MIME.

MIME-тип определяет тип файла. Например, файл может быть определен как **.gif** и, следовательно, должен содержать данные этого типа. Некоторые вирусы могут пытаться скрыться внутри файлов, используя ложное расширение. Файл может быть указан как **.gif**, но содержимое файла не будет соответствовать данным этого типа, так как он заражен вирусом.

Включение этой функции рекомендуется для того, чтобы предотвратить прохождение вируса.



### Командная строка:

```
set ALG ALG_HTTP http-outbound-av Antivirus=Protect
```

*Создание сервиса с ALG с установленной антивирусной защитой*

### Веб-интерфейс:

Object → Services → Add → TCP/UDP Services



**http-outbound-av**  
 A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

**General**

Name:

Type:

Source:

Destination:

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

Pass returned ICMP error messages from destination

SYN flood protection (SYN Relay)

**Application Layer Gateway**

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG:

Max Sessions:  Specifies how many concurrent sessions that are permitted using this service.

**Comments**

Comments:

**Командная строка:**

```
add Service ServiceTCPUDP http-outbound-av DestinationPorts=80,8080,90.8090
SourcePorts=0-65535 ALG=http-outbound-av
```

**Определение правила фильтрации с созданным сервисом**

**Веб-интерфейс:**

Rules → IP Rules → toInet → Add → IP Rule

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

General | Log Settings | NAT | SAT | Multiplex SAT | SLB SAT | SLB Monitors

**General**

Name: http\_av  
 Action: NAT  
 Service: http-outbound-av  
 Schedule: (None)

**Address Filter**

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

Source: Interface: lan, Network: lan\_net  
 Destination: Interface: wan1, Network: all-nets

**Comments**

Comments:

OK Cancel

### Командная строка:

```
add IPRuleFolder Name=toInet
cc IPRuleFolder <N folder>
add IPRule Action=NAT SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=http-outbound-
av Name=http_av
```

## Лабораторная работа 9. Обнаружение и предотвращение вторжений

### Принципы использования IDS

Обнаружение и предотвращение вторжений (IDP) является подсистемой NetDefendOS, которая предназначена для защиты от попыток вторжения. Система просматривает сетевой трафик, проходящий через межсетевой экран, и ищет трафик, соответствующий шаблонам. Обнаружение такого трафика указывает на попытку вторжения. После обнаружения подобного трафика IDP выполняет шаги по нейтрализации как вторжения, так и его источника.

Для обнаружения и предотвращения вторжения, необходимо указать следующую информацию:

1. Какой трафик следует анализировать.
2. Что следует искать в анализируемом трафике.
3. Какое действие необходимо предпринять при обнаружении вторжения.

Эта информация указывается в **IDP-правилах**.

### Maintenance u Advanced IDP

Компания D-Link предоставляет два типа IDP:

## 1. Maintenance IDP

*Maintenance IDP* является основой системы IDP и включено в стандартную комплектацию NetDefend DFL-210, 800, 1600 и 2500.

*Maintenance IDP* является упрощенной IDP, что обеспечивает базовую защиту от атак, и имеет возможность расширения до более комплексной *Advanced IDP*.

IDP не входит в стандартную комплектацию DFL-260, 860, 1660, 2560 и 2560G; для этих моделей межсетевых экранов необходимо приобрести подписку на *Advanced IDP*.

## 2. Advanced IDP

*Advanced IDP* является расширенной системой IDP с более широким диапазоном баз данных сигнатур и предъявляет более высокие требования к оборудованию. Стандартной является подписка сроком на 12 месяцев, обеспечивающая автоматическое обновление базы данных сигнатур IDP.

Эта опция IDP доступна для всех моделей D-Link NetDefend, включая те, в стандартную комплектацию которых не входит *Maintenance IDP*.

*Maintenance IDP* можно рассматривать, как ограниченное подмножество *Advanced IDP*. Рассмотрим функционирование *Advanced IDP*.

*Advanced IDP* приобретается как дополнительный компонент к базовой лицензии NetDefendOS. Подписка означает, что база данных сигнатур IDP может быть загружена на NetDefendOS, а также, что база данных регулярно обновляется по мере появления новых угроз.

Обновления базы данных сигнатур автоматически загружаются системой NetDefendOS через сконфигурированный интервал времени. Это выполняется с помощью HTTP-соединения с сервером сети D-Link, который предоставляет последние обновления базы данных сигнатур. Если на сервере существует новая версия базы данных сигнатур, она будет загружена, заменив старую версию.

Термины Intrusion Detection and Prevention (IDP), Intrusion Prevention System (IDP) и Intrusion Detection System (IDS) взаимозаменяют друг друга. Все они относятся к функции IDP.

### **Последовательность обработка пакетов**

Последовательность обработки пакетов при использовании IDP является следующей:

1. Пакет приходит на межсетевой экран. Если пакет является частью нового соединения, то первым делом ищется соответствующее IP-правило фильтрации. Если пакет является частью существующего соединения, он сразу же попадает в модуль IDP. Если пакет не является частью существующего соединения или отбрасывается IP-правилом, то дальнейшей обработки данного пакета не происходит.
2. Адреса источника и назначения пакета сравниваются с набором правил IDP. Если найдено подходящее правило, то пакет передается на обработку системе IDP, в которой ищется совпадение содержимого пакета с одним из шаблонов. Если совпадения не обнаружено, то пакет пропускается системой IDP. Могут быть определены дальнейшие действия в IP-правилах фильтрации, такие как NAT и создание логов.

## Поиск на соответствие шаблону

### Сигнатуры

Для корректного определения атак система IDP использует *шаблоны*, связанные с различными типами атак. Эти предварительно определенные шаблоны, также называемые *сигнатурами*, хранятся в локальной базе данных и используются системой IDP для анализа трафика. Каждая сигнатура имеет уникальный номер.

Рассмотрим пример простой атаки, состоящий в обращении к FTP-серверу. Неавторизованный пользователь может попытаться получить файл паролей `passwd` с FTP-сервера с помощью команды FTP `RETR passwd`. Сигнатура, содержащая текстовые строки ASCII `RETR` и `passwd`, обнаружит соответствие, указывающее на возможную атаку. В данном примере шаблон задан в виде текста ASCII, но поиск на соответствие шаблону выполняется аналогично и для двоичных данных.

### Распознавание неизвестных угроз

Злоумышленники, разрабатывающие новые атаки, часто просто модифицируют старый код. Это означает, что новые атаки могут появиться очень быстро как расширение и обобщение старых. Чтобы противостоять этому, D-Link IDP использует подход, при котором модуль выполняет сканирование, учитывая возможное многократное использование компонент, выявляя соответствие шаблону общих блоков, а не конкретного кода. Этим достигается защита как от известных, так и от новых, недавно разработанных, неизвестных угроз, созданных модификацией программного кода атаки.

### Описания сигнатур

Каждая сигнатура имеет пояснительное текстовое описание. Прочитав текстовое описание сигнатуры, можно понять, какую атаку или вирус поможет обнаружить данная сигнатура. В связи с изменением характера базы данных сигнатур, текстовые описания не содержатся в документации D-Link, но доступны на Web-сайте D-Link: <http://security.dlink.com.tw>

### Типы сигнатур IDP

В IDP имеется три типа сигнатур, которые предоставляют различные уровни достоверности в определении угроз:

- **Intrusion Protection Signatures (IPS)** – Данный тип сигнатур обладает высокой точностью, и соответствие трафика данному шаблону в большинстве случаев означает атаку. Для данных угроз рекомендуется указывать действие `Protect`. Эти сигнатуры могут обнаружить действия, направленные на получение прав администратора, и сканеры безопасности.
- **Intrusion Detection Signatures (IDS)** – У данного типа сигнатур меньше точности, чем у IPS, и они могут дать иметь ложные срабатывания, таким образом, поэтому перед тем как указывать действие `Protect` рекомендуется использовать действие `Audit`.
- **Policy Signatures** - Этот тип сигнатур обнаруживает различные типы прикладного трафика. Эти сигнатуры могут использоваться для блокировки некоторых приложений, предназначенных для совместного использования приложений и мгновенного обмена сообщениями.

## ***Предотвращение атак Denial-of-Service***

### *Механизмы DoS-атак*

DoS-атаки могут выполняться самыми разными способами, но все они могут быть разделены на три основных типа:

- Исчерпание вычислительных ресурсов, таких как полоса пропускания, дисковое пространство, время ЦП.
- Изменение конфигурационной информации, такой как информация маршрутизации.
- Порча физических компонентов сети.

Одним из наиболее часто используемых методов является исчерпание вычислительных ресурсов, т.е. невозможность нормального функционирования сети из-за большого количества запросов, часто неправильно сформатированных, и расходования ресурсов, используемых для запуска критически важных приложений. Могут также использоваться уязвимые места в операционных системах Unix и Windows для преднамеренного разрушения системы.

Перечислим некоторые из наиболее часто используемых DoS-атак:

- Ping of Death / атаки Jolt
- Перекрытие фрагментов: Teardrop / Bonk / Boink / Nестea
- Land и LaTierra атаки
- WinNuke атака
- Атаки с эффектом усиления: Smurf, Papasmurf, Fraggle
- TCP SYN Flood
- Jolt2

### *Атака Ping of Death и Jolt*

«Ping of Death» является одной из самых ранних атак, которая выполняется на 3 и 4 уровнях стека протоколов. Один из простейших способов выполнить эту атаку - запустить `ping -l 65510 1.2.3.4` на Windows 95, где 1.2.3.4 - это IP-адрес компьютера-жертвы. «Jolt» – это специально написанная программа для создания пакетов в операционной системе, в которой команда `ping` не может создавать пакеты, размеры которых превышают стандартные нормы.

Смысл атаки состоит в том, что общий размер пакета превышает 65535 байт, что является максимальным значением, которое может быть представлено 16-битным целым числом. Если размер больше, то происходит переполнение.

Защита состоит в том, чтобы не допустить фрагментацию, приводящую к тому, что общий размер пакета превышает 65535 байт. Помимо этого, можно настроить ограничения на длину IP-пакета.

Атаки Ping of Death и Jolt регистрируются в логах как отброшенные пакеты с указанием на правило «LogOversizedPackets». Следует помнить, что в этом случае IP-адрес отправителя может быть подделан.

### *Атаки, связанные с перекрытием фрагментов: Teardrop, Bonk, Boink и Nестea*

Teardrop - это атака, связанная с перекрытием фрагментов. Многие реализации стека протоколов плохо обрабатывают пакеты, при получении которых имеются

перекрывающиеся фрагменты. В этом случае возможно как исчерпание ресурсов, так и сбой.

NetDefendOS обеспечивает защиту от атак перекрытия фрагментов. Перекрываемым фрагментам не разрешено проходить через систему.

Teardrop и похожие атаки регистрируются в логах NetDefendOS как отброшенные пакеты с указанием на правило «IllegalFragments». Следует помнить, что в этом случае IP-адрес отправителя может быть подделан.

#### *Атака Land u LaTierra*

Атаки Land и LaTierra состоят в посылке такого пакета компьютеру-жертве, который заставляет его отвечать самому себе, что, в свою очередь, генерирует еще один ответ самому себе, и т.д. Это вызовет либо полную остановку работы компьютера, либо крах какой-либо из его подсистем

Атака состоит в использовании IP-адреса компьютера-жертвы в полях **Source** и **Destination**.

NetDefendOS обеспечивает защиту от атаки Land, используя защиту от IP-спуфинга ко всем пакетам. При использовании настроек по умолчанию все входящие пакеты сравниваются с содержанием таблицы маршрутизации; если пакет приходит на интерфейс, с которого невозможно достигнуть IP-адреса источника, то пакет будет отброшен.

Атаки Land и LaTierra регистрируются в логах NetDefendOS как отброшенные пакеты с указанием на правило по умолчанию **AutoAccess**, или, если определены другие правила доступа, указано правило доступа, в результате которого отброшен пакет. В данном случае IP-адрес отправителя не представляет интереса, так как он совпадает с IP-адресом получателя.

#### *Атака WinNuke*

Принцип действия атаки WinNuke заключается в подключении к TCP-сервису, который не умеет обрабатывать «out-of-band» данные (TCP-пакеты с установленным битом **URG**), но все же принимает их. Это обычно приводит к заикливанию сервиса и потреблению всех ресурсов процессора.

Одним из таких сервисов был NetBIOS через TCP/IP на WINDOWS-машинах, которая и дала имя данной сетевой атаке.

NetDefendOS обеспечивает защиту двумя способами:

- Политики для входящего трафика как правило разработаны достаточно тщательно, поэтому количество успешных атак незначительно. Извне доступны только публичные сервисы, доступ к которым открыт. Только они могут стать жертвами атак.
- Удаление бита **URG** из всех TCP-пакетов.

#### **Веб-интерфейс**

**Advanced Settings** → **TCP** → **TCPUrg**

TCP MSS Max:	1460	Maximum allowed TCP MSS (Maximum Segment Size).
TCP MSS VPN Max:	1400	Limits TCP MSS for VPN connections; minimizes fragmentation.
TCP MSS on High:	Adjust	How to handle too high MSS values.
TCP MSS Log Level:	7000	When to log regarding too high TCP MSS, if not logged by "TCP MSS on high".
TCP Auto Clamping:	<input checked="" type="checkbox"/>	Automatically clamp TCP MSS according to MTU of involved interfaces - in addition to "TCP MSS max".
TCP Zero Unused ACK:	<input checked="" type="checkbox"/>	Force unused ACK fields to zero; helps prevent connection spoofing.
TCP Zero Unused URG:	<input checked="" type="checkbox"/>	Force unused URG fields to zero; prevents small information leak.
TCP Option WSOPT:	ValidateLogBad	The WSOPT (Window Scale) option (common).
TCP Option SACK:	ValidateLogBad	The SACK/SACKPERMIT (Selective ACK) options (common).
TCP Option TSOPT:	ValidateLogBad	The TSOPT (Timestamp) option (common).
TCP Option ALTCHKREQ:	StripLog	The ALTCHKREQ (Alternate Checksum Request) option.
TCP Option ALTCHKDATA:	StripLog	The ALTCHKDATA (Alternate Checksum Data) option.
TCP Option Connection Timeout:	StripLogBad	The CC (Connection Count) option series (semi common).
TCP Option Other:	StripLog	How to handle TCP options not specified above.
TCP SYN/URG:	DropLog	The TCP URG flag together with SYN; normally invalid (strip=strip URG).
TCP SYN/PSH:	StripSilent	The TCP PSH flag together with SYN; normally invalid but always used by some IP stacks (strip=strip PSH).
TCP SYN/RST:	DropLog	The TCP RST flag together with SYN; normally invalid (strip=strip RST).
TCP SYN/FIN:	DropLog	The TCP FIN flag together with SYN; normally invalid (strip=strip FIN).
TCP FIN/URG:	DropLog	The TCP URG flag together with FIN; normally invalid (strip=strip URG).
TCP URG:	StripLog	The TCP URG flag; many operating systems cannot handle this correctly.
TCP ECN:	StripLog	The Explicit Congestion Notification (ECN) flags. Previously known as "XMAS"/"YMAS" flag. Also used in OS fingerprinting.

Как правило, атаки WinNuke регистрируются в логах как отброшенные пакеты с указанием на правило, запретившего попытку соединения. Для разрешенных соединений появляется запись категории «TCP» или «DROP» (в зависимости от настройки TCPUrg), с именем правила «TCPUrg». IP-адрес отправителя может быть не поддельным, так как соединение должно быть полностью установлено к моменту отправки пакетов «out-of-band».

#### *Атаки, приводящие к увеличению трафика: Smurf, Parasmurf, Fraggle*

Эта категория атак использует некорректно настроенные сети, которые позволяют увеличивать поток трафика и направлять его целевой системе. Целью является интенсивное использование полосы пропускания жертвы. Атакующий с широкой полосой пропускания может не использовать эффект усиления, позволяющий полностью загрузить всю полосу пропускания жертвы. Эти атаки позволяют атакующим с меньшей полосой пропускания, чем у жертвы, использовать усиление, чтобы занять полосу пропускания жертвы.

- «Smurf» и «Parasmurf» отправляют эхо-пакеты ICMP по широковещательному адресу, указывая в качестве IP-адреса источника IP-адрес жертвы. После этого все компьютеры посылают ответные пакеты жертве.
- «Fraggle» базируется на «Smurf», но использует эхо-пакеты UDP и отправляет их на порт 7. В основном, атака «Fraggle» имеет более слабое усиление, так как служба echo активирована у небольшого количества хостов.

Атаки Smurf регистрируются в логах NetDefendOS как большое число отброшенных пакетов ICMP Echo Reply. Для подобной перегрузки сети может использоваться поддельный IP-адрес. Атаки Fraggle также отображаются в логах NetDefendOS как большое количество отброшенных пакетов. Для перегрузки сетb используется поддельный IP-адрес.

При использовании настроек по умолчанию пакеты, отправленные по адресу широковещательной рассылки, отбрасываются.

## Веб-интерфейс

**Advanced Settings → IP → DirectedBroadcasts**

В политиках для входящего трафика следует учитывать, что любая незащищенная сеть может также стать источником подобных атак усиления.

### Защита на стороне компьютера-жертвы

Smurf и похожие атаки являются атаками, расходующими ресурсы соединения. В общем случае межсетевой экран является узким местом в сети и не может обеспечить достаточную защиту против этого типа атак. Когда пакеты доходят до межсетевого экрана, ущерб уже нанесен.

Тем не менее система NetDefendOS может уменьшить нагрузку на внутренние сервера, делая их сервисы доступными изнутри или через альтернативное соединение, которое не стало целью атаки.

- Типы flood-атак Smurf и Parasmurf на стороне жертвы выглядят как ответы ICMP **Echo Response**. Если не используются правила **FwdFast**, таким пакетам не будет разрешено инициировать новые соединения независимо от того, существуют ли правила, разрешающие прохождение пакетов.
- Пакеты Fraggle могут прийти на любой UDP-порт назначения, который является мишенью атакующего. В этой ситуации может помочь увеличение ограничений в наборе правил.

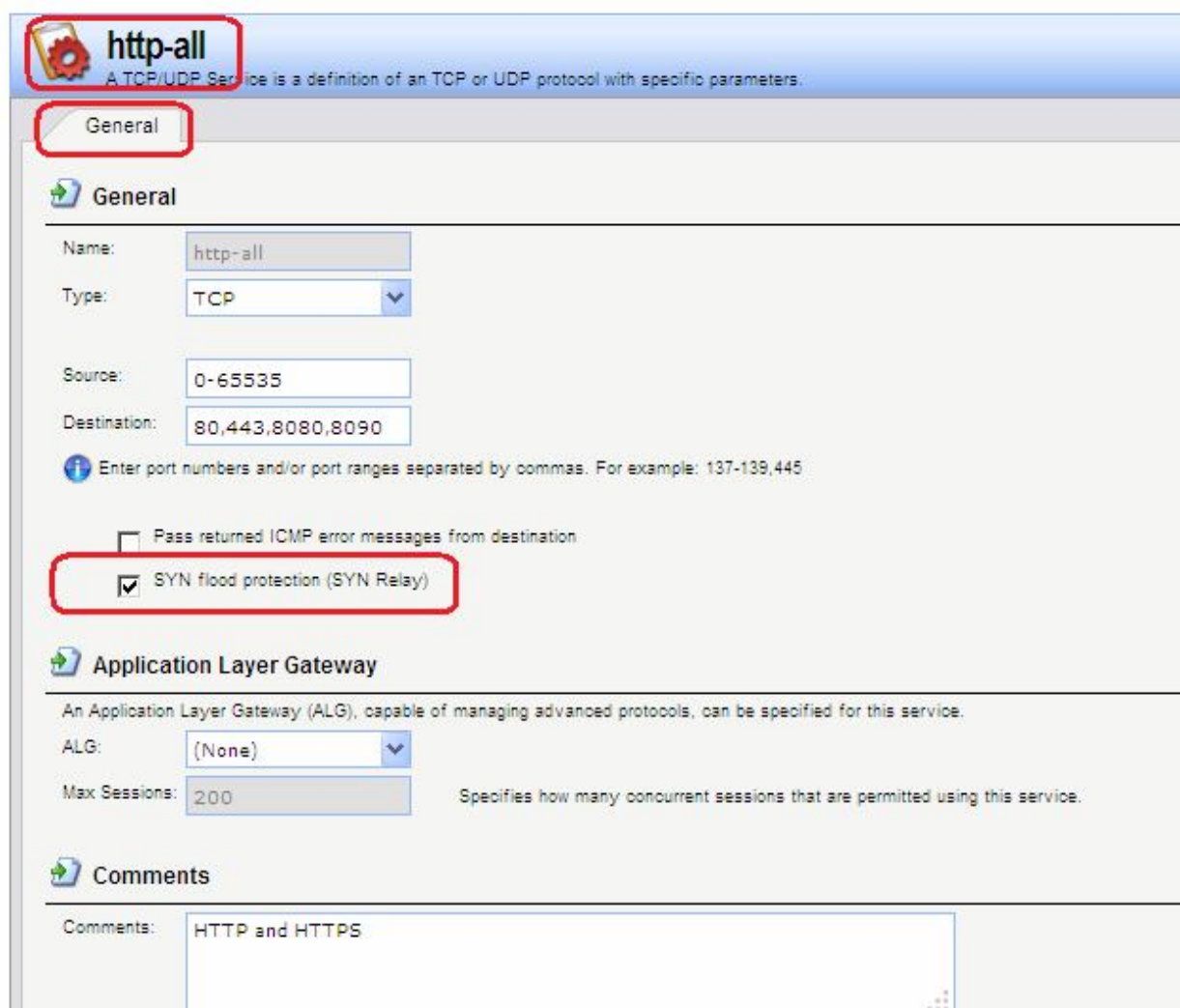
Шейпинг трафика также помогает предотвращать некоторые flood-атаки на защищаемые сервера.

### Атаки TCP SYN Flood

Принцип атак *TCP SYN Flood* заключается в отправке большого количества TCP-пакетов с установленным флагом **SYN** на определенный порт и в игнорировании отправленных в ответ пакетов с установленными флагами **SYN ACK**. Это позволяет исчерпать ресурсы стека протоколов на сервере жертвы, в результате чего он не сможет устанавливать новые соединения, пока не истечет таймаут существования полуоткрытых соединений.

Система NetDefendOS обеспечивает защиту от flood-атак TCP SYN, если установлена опция **SYN Flood Protection** в соответствующем сервисе, который указан в IP-правиле фильтрации. Иногда опция может обозначаться как **SYN Relay**.





Защита от flood-атак включена по умолчанию в таких сервисах, как **http-in**, **https-in**, **smtp-in** и **ssh-in**.

### Механизм защиты от атак SYN Flood

Защиты от атак SYN Flood выполняется в течение трехкратного рукопожатия, которое происходит при установлении соединения с клиентом. В системе NetDefendOS как правило не происходит исчерпание ресурсов, так как выполняется более оптимальное управление ресурсами и отсутствуют ограничения, имеющие место в других операционных системах. В операционных системах могут возникнуть проблемы уже с 5 полуконечными соединениями, не получившими подтверждение от клиента, NetDefendOS может заполнить всю таблицу состояний, прежде чем будут исчерпаны какие-либо ресурсы. Когда таблица состояний заполнена, старые неподтвержденные соединения отбрасываются, чтобы освободить место для новых соединений.

### Обнаружение SYN Floods

Атаки TCP SYN flood регистрируются в логах NetDefendOS как большое количество новых соединений (или отброшенных пакетов, если атака направлена на закрытый порт). Следует помнить, что в этом случае IP-адрес отправителя может быть подделан.

### ALG автоматически обеспечивает защиту от flood-атак

Следует отметить, что нет необходимости включать функцию защиты от атак SYN Flood для сервиса, для которого указан ALG. ALG автоматически обеспечивает защиту от атак SYN flood.

### *Атака Jolt2*

Принцип выполнения атаки Jolt2 заключается в отправке непрерывного потока одинаковых фрагментов компьютеру-жертве. Поток из нескольких сотен пакетов в секунду останавливает работу уязвимых компьютеров до полного прекращения потока.

NetDefendOS обеспечивает полную защиту от данной атаки. Первый полученный фрагмент ставится в очередь до тех пор, пока не придут предыдущие по порядку фрагменты, чтобы все фрагменты могли быть переданы в нужном порядке. В случае наличия атаки ни один фрагмент не будет передан целевому приложению. Последующие фрагменты будут отброшены, так как они идентичны первому полученному фрагменту.

Если выбранное злоумышленником значение смещения фрагмента больше, чем ограничения, указанные в настройках **Advanced Settings** → **Length Limit Settings** в NetDefendOS, пакеты будут немедленно отброшены. Атаки Jolt2 могут быть зарегистрированы в логах. Если злоумышленник выбирает слишком большое значение смещения фрагмента для атаки, это будет зарегистрировано в логах как отброшенные пакеты с указанием на правило **LogOversizedPackets**. Если значение смещения фрагмента достаточно маленькое, регистрации в логах не будет. IP-адрес отправителя может быть подделан.

### *Атака Distributed DoS (DDoS)*

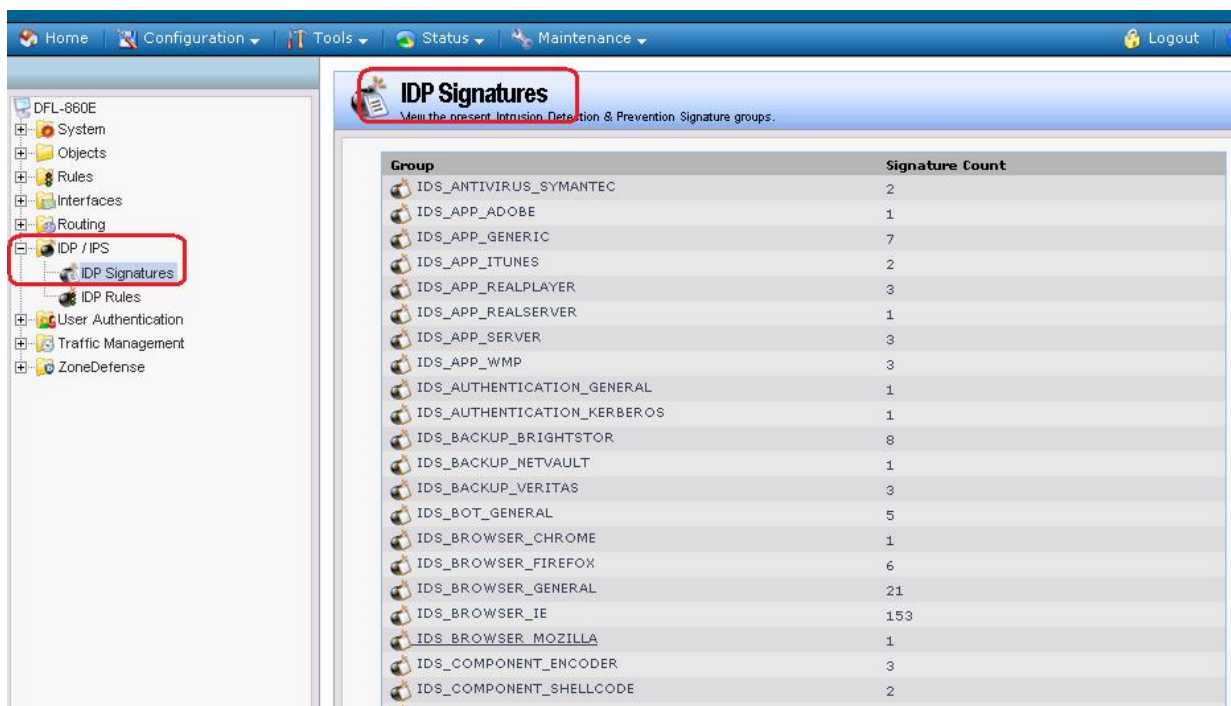
Наиболее сложной DoS-атакой является атака *Distributed Denial of Service*. Хакеры используют сотни или тысячи компьютеров по всей сети интернет, устанавливая на них программное обеспечение для выполнения DDoS-атак и управляя всеми этими компьютерами для осуществления скоординированных атак на сайты жертвы. Как правило эти атаки расходуют полосу пропускания, вычислительные мощности маршрутизатора или ресурсы для обработки стека протоколов, в результате чего сетевые соединения с жертвой не могут быть установлены.

Хотя последние DDoS-атаки были запущены как из частных, так и из публичных сетей, хакеры, как правило, часто предпочитают корпоративные сети из-за их открытого и распределенного характера. Инструменты, используемые для запуска DDoS-атак, включают Trin00, TribeFlood Network (TFN), TFN2K и Stacheldraht.

## **Описание практической работы**

### ***Общий список сигнатур***

В веб-интерфейсе все сигнатуры перечислены в разделе **IDP/IPS** → **IDP Signatures**.



### **IDP-правила**

Правило IDP определяет, какой тип трафика необходимо анализировать. Правила IDP создаются аналогично другим правилам, например, IP-правилам фильтрации. В правиле IDP указывается комбинация адреса/интерфейса источника/назначения, сервиса, определяющего какие протоколы будут сканироваться. Главное отличие от правил фильтрации в том, что правило IDP определяет **Действие**, которое следует предпринять при обнаружении вторжения.

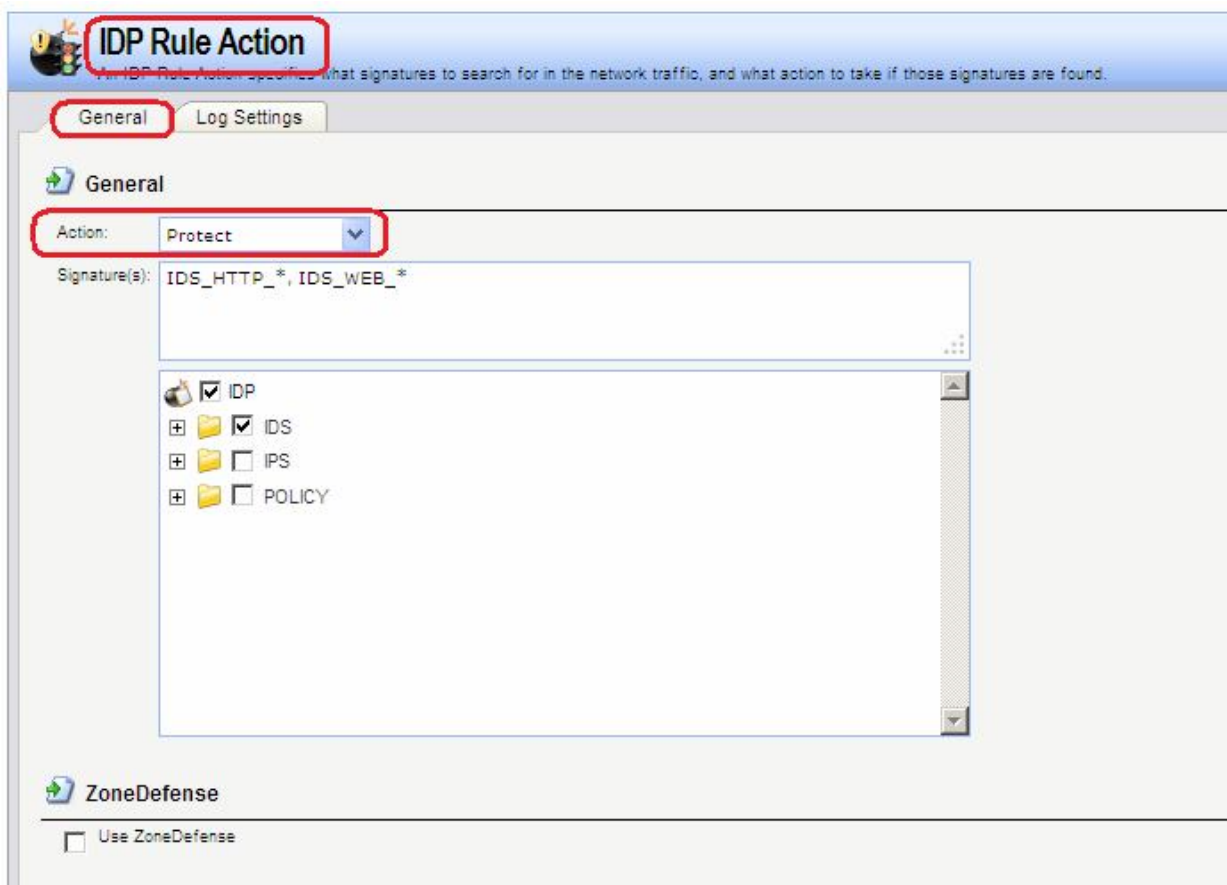
### **Веб-интерфейс:**

IDP / IPS → IDP Rules → Add → IDP Rule

### *Действия IDP*

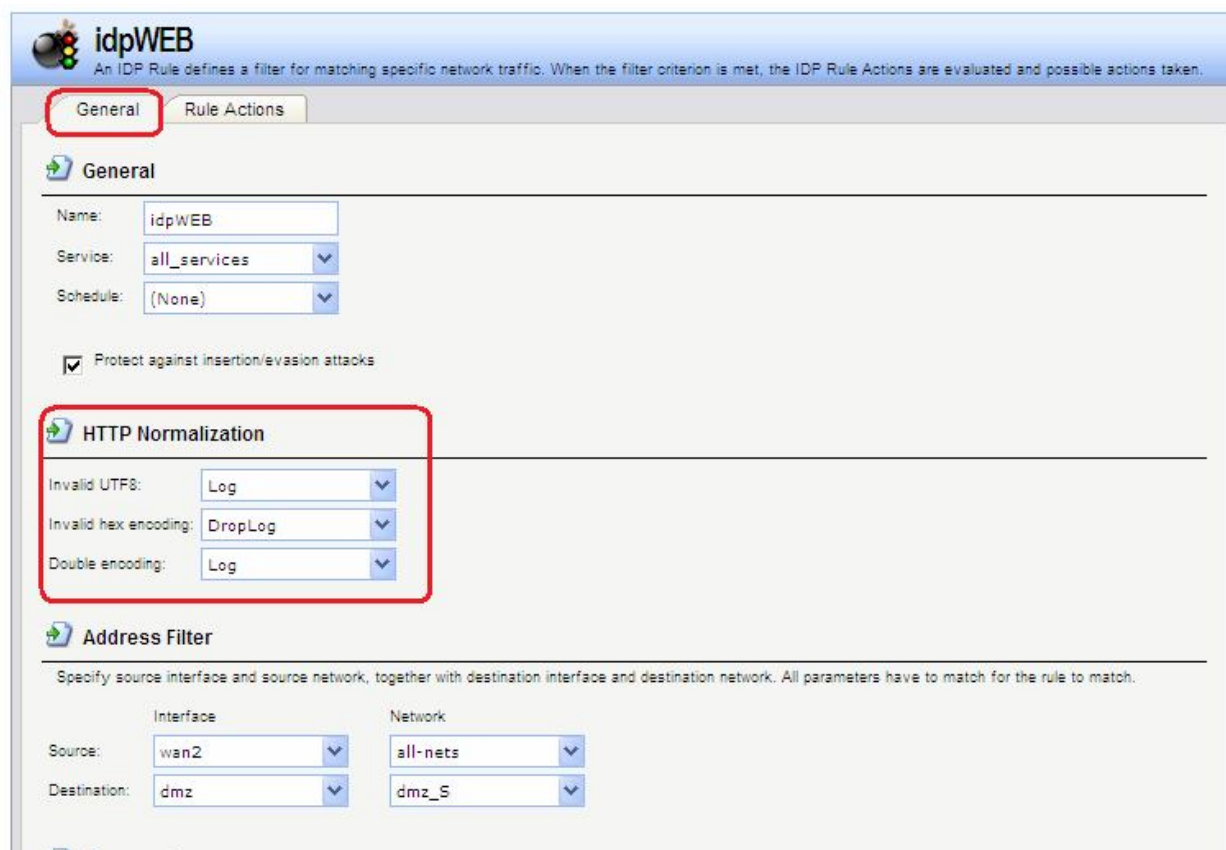
При выявлении вторжения будет выполнено действие, указанное в правиле IDP. Может быть указано одно из трех действий:

1. **Ignore** – Если обнаружено вторжение, не выполнять никаких действий и оставить соединение открытым.
2. **Audit** – Оставить соединение открытым, но зарегистрировать событие.
3. **Protect** – Сбросить соединение и зарегистрировать событие. Возможно использовать дополнительную опцию занесения в «черный список» источник соединения.



### *Нормализация HTTP*

IDP выполняет *нормализацию HTTP*, т.е. проверяет корректность URI в HTTP-запросах. В IDP-правиле можно указать действие, которое должно быть выполнено при обнаружении некорректного URI.



IDP может определить следующие некорректные URI:

### Некорректная кодировка UTF8

Выполняется поиск любых недействительных символов UTF8 в URI.

### Некорректный шестнадцатеричный код

Корректной является шестнадцатеричная последовательность, где присутствует знак процента, за которым следуют два шестнадцатеричных значения, являющихся кодом одного байта. Некорректная шестнадцатеричная последовательность – это последовательность, в которой присутствует знак процента, за которым не следуют шестнадцатеричные значения, являющиеся кодом какого-либо байта.

### Двойное кодирование

Выполняется поиск любой шестнадцатеричной последовательности, которая сама является закодированной с использованием других управляющих шестнадцатеричных последовательностей. Примером может быть последовательность %2526, при этом %25 может быть интерпретировано HTTP-сервером как %, в результате получится последовательность %26, которая будет интерпретирована как &.

### Предотвращение атак, связанных со вставкой символов или обходом механизмов IDP

В IDP-правиле можно установить опцию **Protect against Insertion/Evasion attack**. Это защита от атак, направленных на обход механизмов IDP. Данные атаки используются тот факт, что в протоколах TCP/IP пакет может быть фрагментирован, и отдельные пакеты могут приходить в произвольном порядке. Атаки, связанные со вставкой символов и обходом механизмов IDP, как правило используют фрагментацию пакетов и проявляются в процессе сборки пакетов.

### Атаки вставки

Атаки вставки состоят в такой модификации потока данных, чтобы система IDP пропускала полученную в результате последовательность пакетов, но данная последовательность будет являться атакой для целевого приложения. Данная атака может быть реализована созданием двух различных потоков данных.

В качестве примера предположим, что поток данных состоит из 4 фрагментов пакетов: **p1**, **p2**, **p3** и **p4**. Злоумышленник может сначала отправить фрагменты пакетов **p1** и **p4** целевому приложению. Они будут удерживаться и системой IDP, и приложением до прихода фрагментов **p2** и **p3**, после чего будет выполнена сборка. Задача злоумышленника состоит в том, чтобы отправить два фрагмента **p2'** и **p3'** системе IDP и два других фрагмента **p2** и **p3** приложению. В результате получаются различные потоки данных, который получены системой IDP и приложением.

### Атаки обхода

У атак обхода такой же конечный результат, что и у атак вставки, также образуются два различных потока данных: один видит система IDP, другой видит целевое приложение, но в данном случае результат достигается противоположным способом, который заключается в отправке фрагментов пакетов, которые будут отклонены системой IDP, но приняты целевым приложением.

### Обнаружение подобных атак

Если включена опция **Insertion/Evasion Protect attacks**, и атака вставки или обхода обнаружена, межсетевой экран автоматически корректирует поток данных, удаляя данные, связанные с атакой.

The screenshot shows the configuration page for an IDP rule named 'idpWEB'. The 'General' tab is active. The 'Name' field is 'idpWEB', 'Service' is 'all\_services', and 'Schedule' is '(None)'. A checkbox labeled 'Protect against insertion/evasion attacks' is checked. Under 'HTTP Normalization', 'Invalid UTF8' is set to 'Log', 'Invalid hex encoding' to 'DropLog', and 'Double encoding' to 'Ignore'. The 'Address Filter' section is configured with 'Source' interface 'wan1' and network 'all-nets', and 'Destination' interface 'dmz' and network 'web\_server'. The 'Comments' section is empty.

### Запись в лог событий, связанных с атаками вставки и обхода

Подсистема, предотвращающая атаки вставки и обхода, может создавать два типа сообщений в логах:

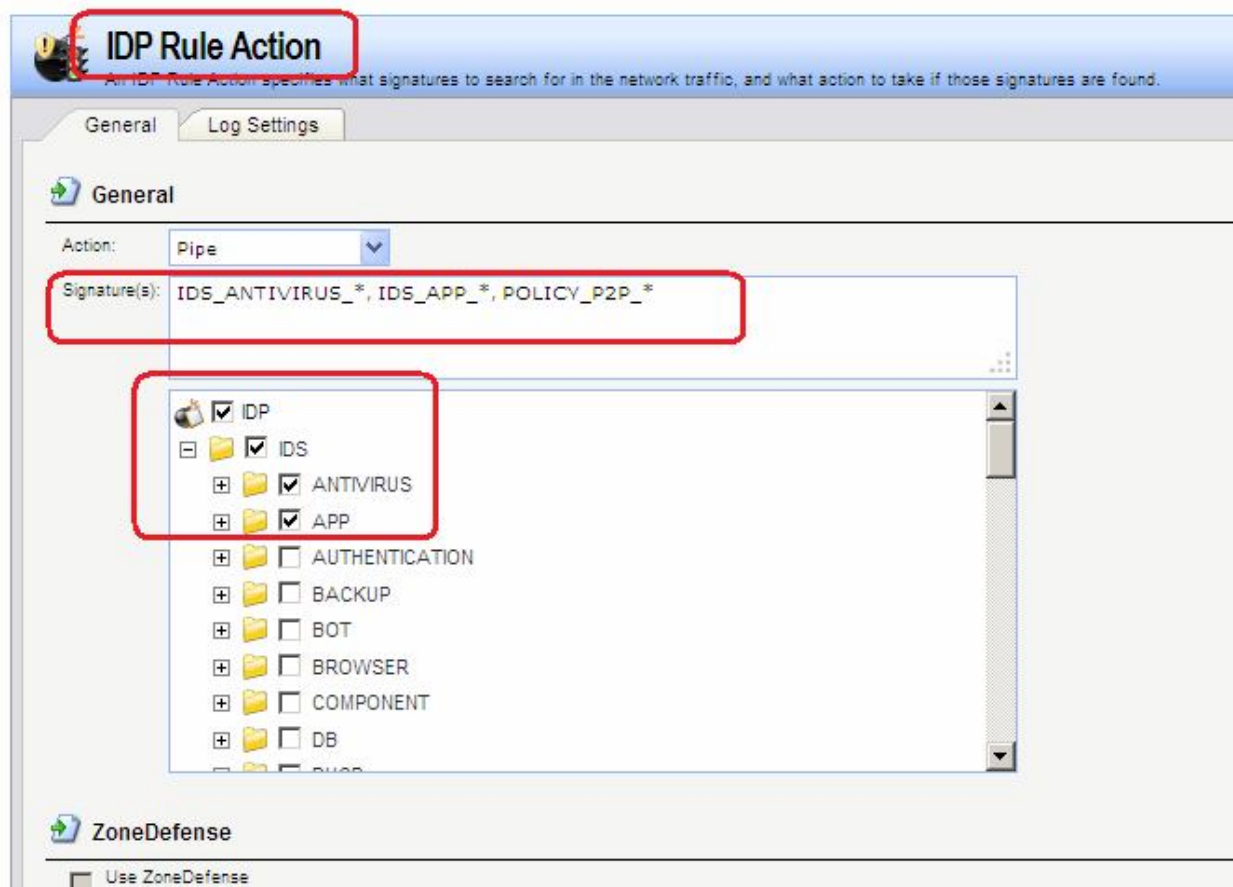
- Сообщение **Attack Detected**, указывающее на то, что атака была обнаружена и предотвращена.
- Сообщение **Unable to Detect**, уведомляющее о том, что система NetDefendOS не смогла выявить возможную атаку при сборке потока TCP/IP, хотя подобная атака могла присутствовать. Эта ситуация возможна при редких и сложных шаблонах данных.

### Рекомендуемые настройки

По умолчанию, защита от атак вставки и обхода включена для всех IDP-правил, и это рекомендуемая настройка для большинства конфигураций. Существует две причины для отключения опции:

- **Требуется увеличение пропускной способности.** Если необходима высокая пропускная способность, следует выключить функцию, так как это обеспечит небольшое увеличение скорости обработки.
- **Чрезмерное количество ложных срабатываний.** Если наблюдается большое количество ложных срабатываний при обнаружении атак вставки и обхода, то целесообразно выключить данную опцию до выяснения причин этих ложных срабатываний.

### Группы сигнатур IDP



Как правило, для каждого протокола существует несколько типов атак, и наилучшим подходом во время анализа сетевого трафика является обнаружение всех атак. Для простоты указания всех типов атак сигнатуры, описывающие атаки на определенный протокол, сгруппированы вместе. Например, образуют группу все сигнатуры, которые относятся к FTP-протоколу. При создании правил удобнее указывать группу, которая относится к определенному протоколу, чем перечислять отдельные сигнатуры. При

необходимости повышения производительности поиск следует выполнять для минимального количества сигнатур.

Группы сигнатур IDP имеют три уровня иерархии. На верхнем уровне указывается тип группы сигнатур, на втором указывается тип приложения или протокола и на третьем указывается отдельное приложение или протокол. Примером является **IDS\_AUTHENTICATION\_KERBEROS**, где **IDS** означает тип сигнатуры, **AUTHENTICATION** – тип протокола и **KERBEROS** – конкретный протокол. Определены следующие типы групп сигнатур и приложений:

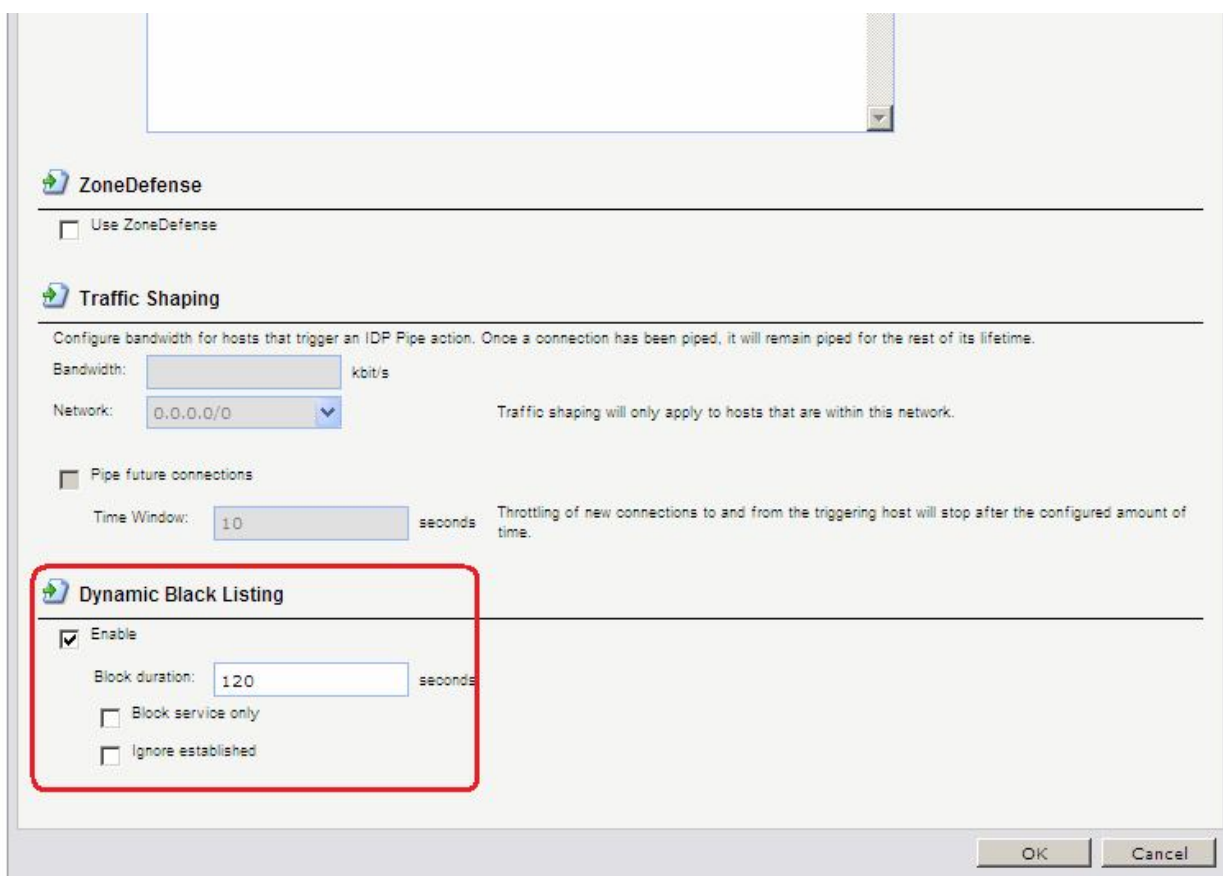
### Использование подстановки символов (Wildcarding) в сигнатурах IDP

Для выбора более одной группы сигнатур IDP можно использовать метод подстановки (Wildcarding). Символ «?» используется для подстановки единственного знака в имени группы. Символ «\*» используется для замены любого количества символов.

Для увеличения производительности следует использовать минимальное количество сигнатур. Например, использование **IDS\_WEB\***, **IPS\_WEB\***, **IDS\_HTTP\*** и **IPS\_HTTP\*** будет достаточным для защиты HTTP-сервера.

### «Черный список» хостов и сетей

Если указано действие **Protect**, можно добавлять в «черный список» отдельные хосты или сети, на которых сработало данное правило. В этом случае весь последующий трафик, идущий с источника, который находится в «черном списке», будет автоматически отклонен.



Можно включить функцию автоматического занесения в «черный список» хоста или сети в IDP и в правилах порога, указав действие **Protect** в правиле. Существуют три параметра «черного списка»:

**Time to Block** Хост или сеть, которые являются источником трафика,



<b>Host/Network in Seconds</b>		остаются в «черном списке» в течение указанного времени, а затем удаляются. Если тот же источник содержится в другой записи в «черном списке», то в таком случае будет восстановлено первоначальное время блокировки, т.е. суммирования не происходит.
<b>Block only this Service</b>		По умолчанию «черный список» блокирует все сервисы с данного хоста.
<b>Exempt established connections Blacklisting</b>	<b>already from</b>	Если существуют установленные соединения с тем же источником, что и новая запись в «черном списке», то они не будут удалены, если установлена данная опция.

IP-адреса или сети добавляются в список, после этого трафик с этих источников блокируется на указанный период времени. При перезапуске межсетевого экрана «черный список» не уничтожается.

Для просмотра, а также для управления содержимым «черного» и «белого списков» используется команда **blacklist**.

#### **Командная строка:**

```
add IDPRule Service=http-all SourceInterface=wan2 SourceNetwork=all-nets
DestinationInterface=dmz DestinationNetwork=dmz/dmz_net Name=idpWEB
```

#### ***Получение по e-mail сообщений о событиях IDP***

Для того чтобы получать уведомления по электронной почте о событиях IDP, необходимо настроить **SMTP Log receiver**. Получаемое сообщение электронной почты будет содержать краткое описание событий IDP, которые произошли за установленный период времени.

После того, как произошло событие IDP, NetDefendOS ожидает несколько секунд (определяется параметром **Hold Time**) прежде, чем отправить уведомление по электронной почте. При этом сообщение будет отправлено только в том случае, если число событий, произошедших в этот период времени, больше или равно, чем значение **Log Threshold**. После отправки уведомления NetDefendOS ожидает несколько секунд (**Minimum Repeat Time**) прежде, чем отправить новое сообщение.

Для указания получения логов по протоколу SMTP, необходимо указать IP-адрес SMTP-сервера, доменное имя в данном случае использоваться не может.

#### **Веб-интерфейс:**

**System → Log and Event Receivers → Add → SMTP Event Receiver**

**IDS\_log**  
An SMTP event receiver is used for receiving emails for IDP events.

**General**

Name:

SMTP Server:

Server Port:

1st Email Receive:

2nd Email Receive:

3rd Email Receive:

Sender:

Subject:

Minimum Repeat Delay:

Hold Time:

Log Threshold:

**Comments**

Comments:

OK Cancel

### Командная строка:

```
add LogReceiver LogReceiverSMTP IDS_log1
IPAddress=InterfaceAddresses/Default_dns Receiver1=admin@oit.cmc.msu.ru
```

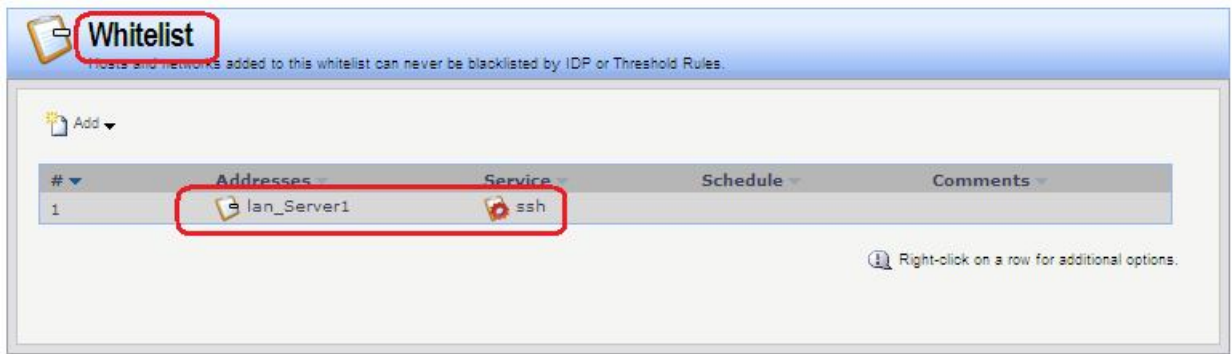
### «Белый список» хостов и сетей

Для того чтобы трафик, поступающий из надежных источников, таких как рабочие станции управления, не попал в «черный список» ни при каких обстоятельствах, система NetDefendOS также поддерживает «белый список». Любой IP-адрес объекта может быть добавлен в этот «белый список».

Важно помнить, что хотя использование «белого списка» предотвращает занесение в «черный список» определенных IP-адресов источников, это не мешает механизмам NetDefendOS отбрасывать соединения с этого источника. «Белый список» предотвращает только добавление источника в «черный список», если это может произойти в результате срабатывания правила.

### Веб-интерфейс:

System → Whitelist → Add → Whitelist Host



**Командная строка:**

```
add BlacklistWhiteHost Addresses=lan/lan_Server1 Service=ssh
```

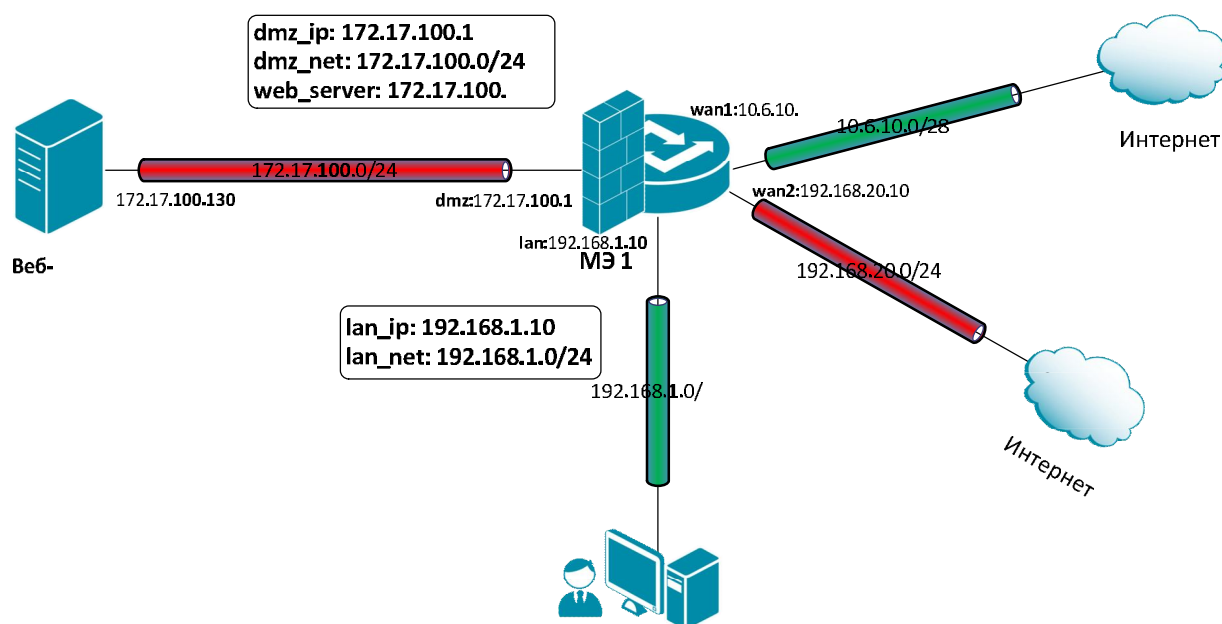
## Приоритезация трафика и создание альтернативных маршрутов

### Лабораторная работа 10. Создание альтернативных маршрутов с использованием статической маршрутизации

#### Цель

Использовать два выхода в интернет: один канал использовать для доступа в интернет из локальной сети, в другой для доступа из DMZ-сети.

#### Топология сети



Следует использовать статическую маршрутизацию на основе правил (Policy-Based Routing - PBR) для создания сети с двумя выходами в интернет.

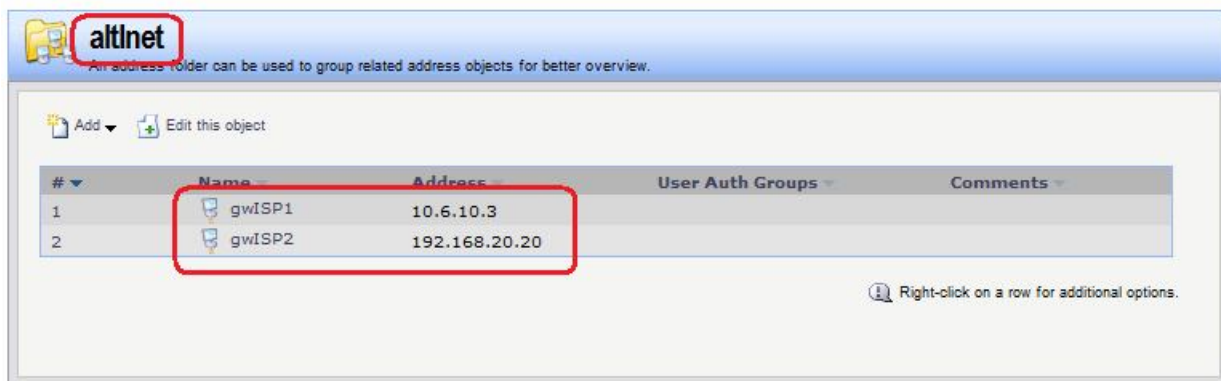
#### Описание практической работы

Создать статическую маршрутизацию и политики доступа, которые обеспечивают доступ в интернет компьютеров из локальной сети LAN через канал, подключенный к wan1-интерфейсу маршрутизатора и доступ в интернет из DMZ-сети через канал, подключенный к wan2-интерфейсу маршрутизатора. Для этого следует использовать статическую маршрутизацию на основе правил.

#### Маршрутизация на основе адреса источника

##### Объекты Адресной Книги

В Адресной Книге создать объекты, описывающие альтернативные шлюзы интернет-провайдеров.



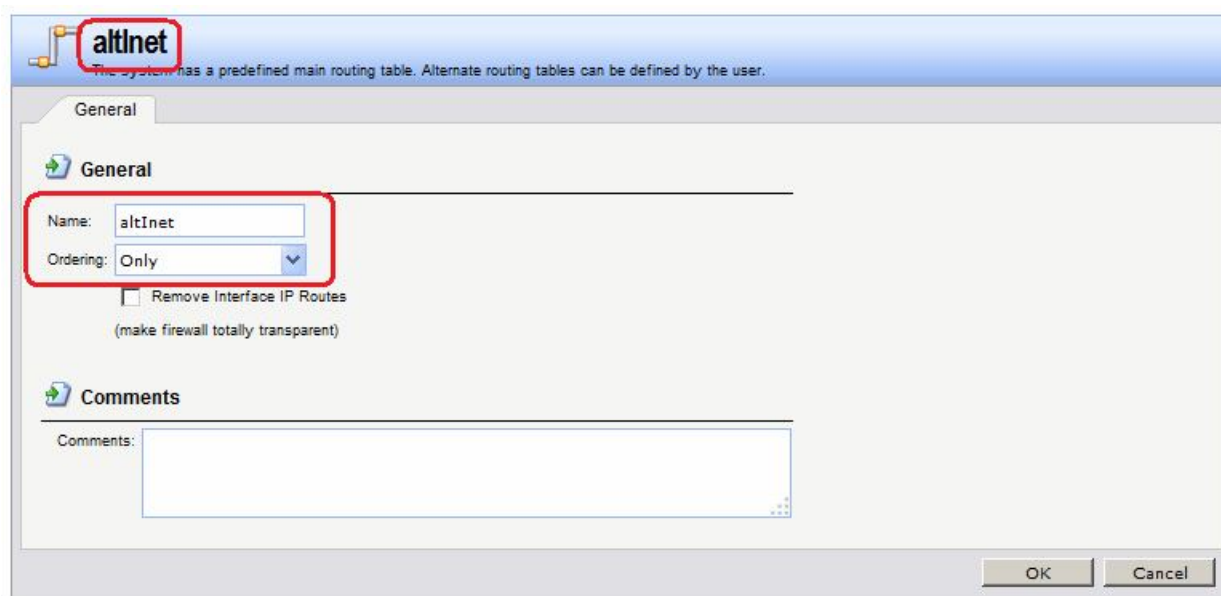
*Альтернативная таблица маршрутизации*  
Создать альтернативную таблицу маршрутизации.

**Веб-интерфейс:**

Routing → Routing Tables → Add → Routing Table

Name: altInet

Ordering: Only



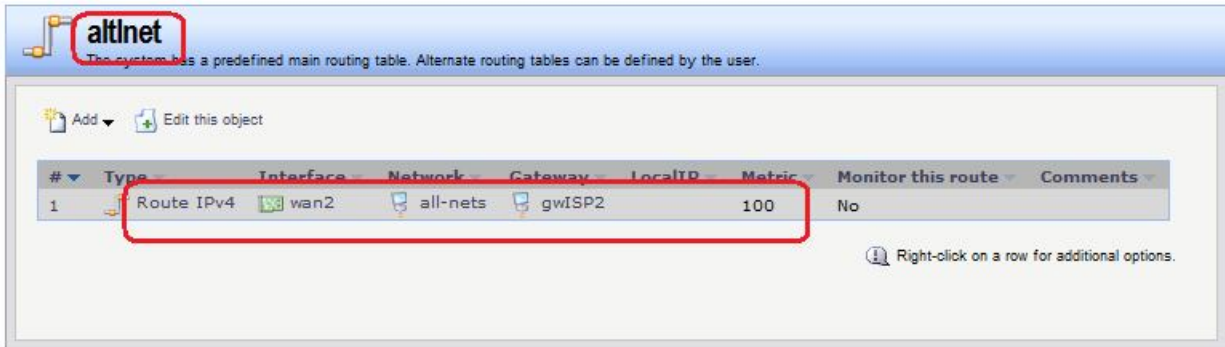
**Командная строка:**

```
add RoutingTable altInet Ordering=Only
```

В созданной таблице создать маршрут по умолчанию к ISP2 через интерфейс wan2.

**Веб-интерфейс:**

Routing → Routing Tables → altInet → Add



**Командная строка:**

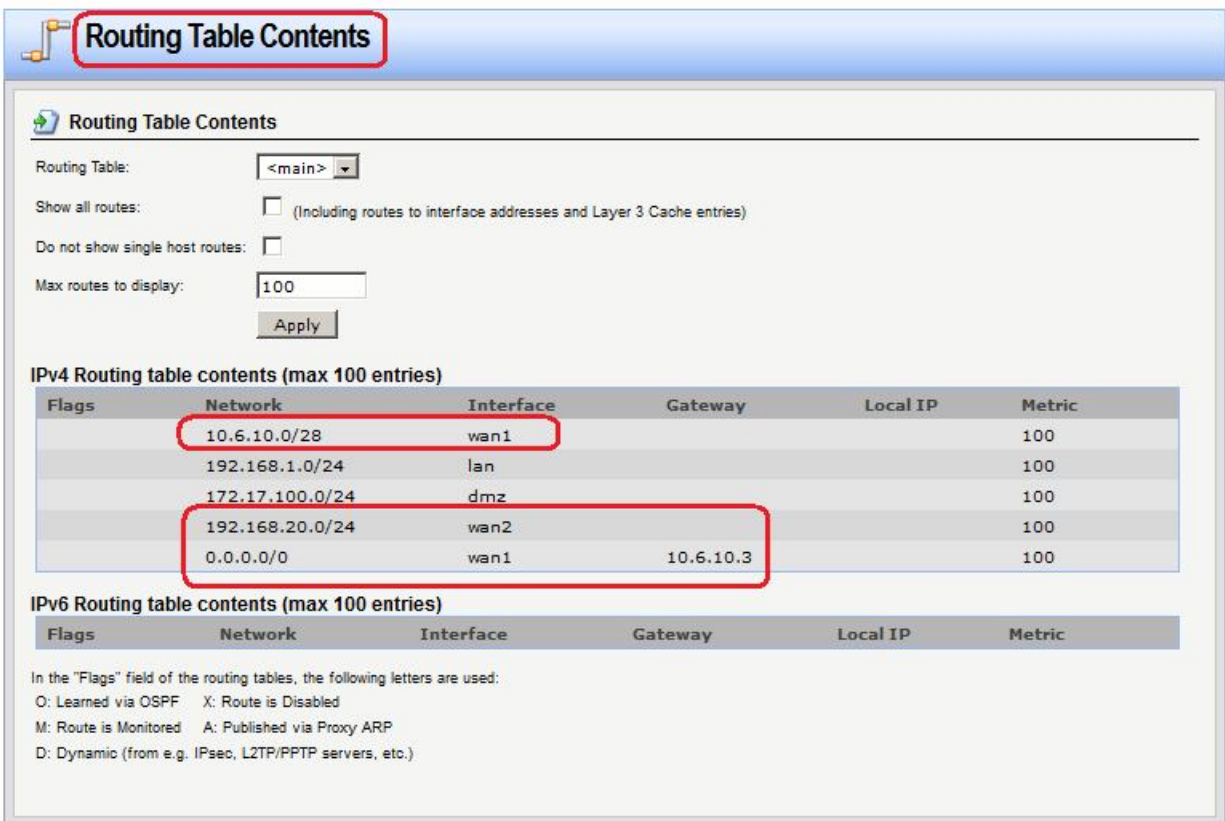
```
cc RoutingTable altInet
```

```
add Route Interface=wan2 Network=all-nets Gateway=altInet/gwISP2 Metric=100
```

В таблице маршрутизации **main** проверить наличие маршрутов по умолчанию к ISP2 через интерфейс **wan2**, а также остальных необходимых маршрутов.

**Веб-интерфейс:**

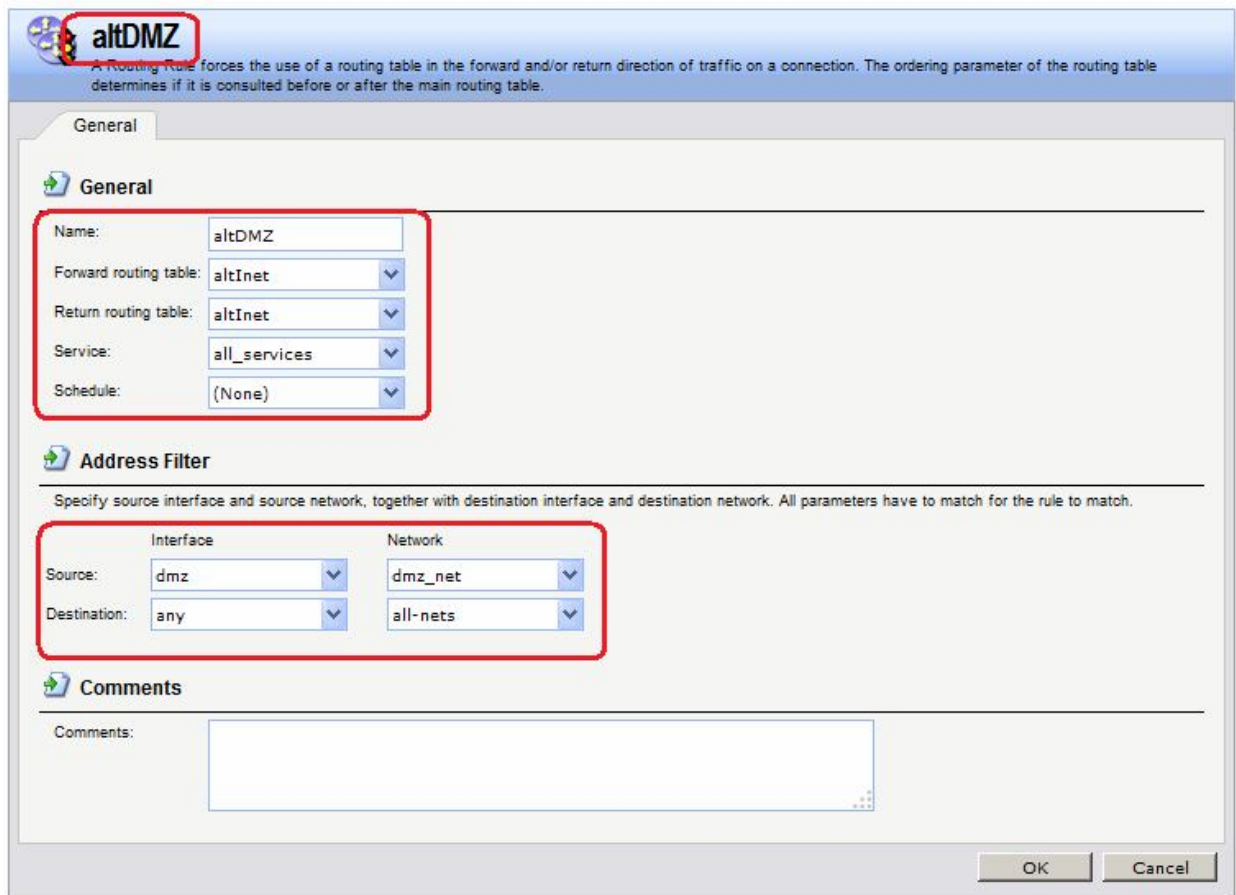
Routing → Routing Tables → main → Add



*Правило выбора таблицы маршрутизации PBR*

**Веб-интерфейс:**

Routing → Routing Rules → Add → Routing Rule



**Командная строка:**

```
add RoutingRule ForwardRoutingTable=altDMZ ReturnRoutingTable=altDMZ
SourceInterface=dmz SourceNetwork= dmz/dmz_net DestinationInterface=any
DestinationNetwork=all-nets Service=all_services Name=altDMZ
```

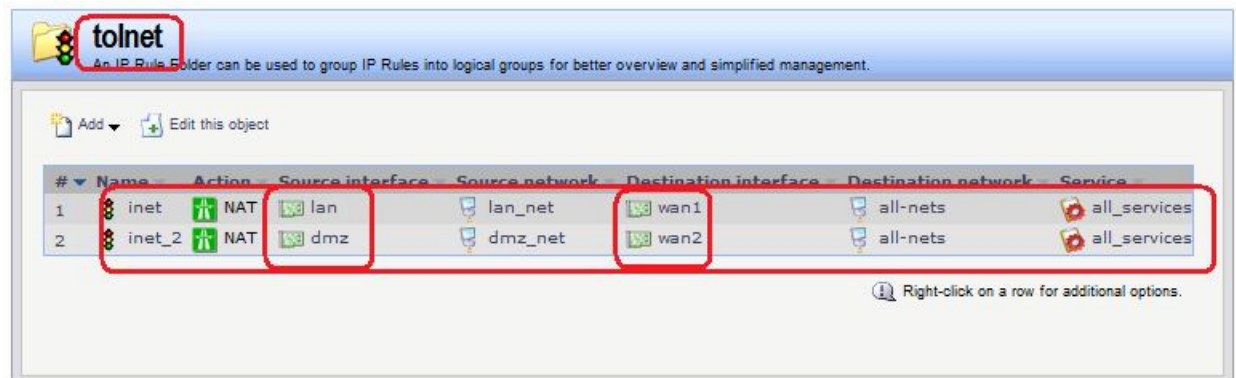
*Правила фильтрация*

**Веб-интерфейс:**

Rules → IP Rules → Add → IP Rule Folder

Name: toInet

Rules → IP Rules → toInet → Add → IP Rule



**Командная строка:**

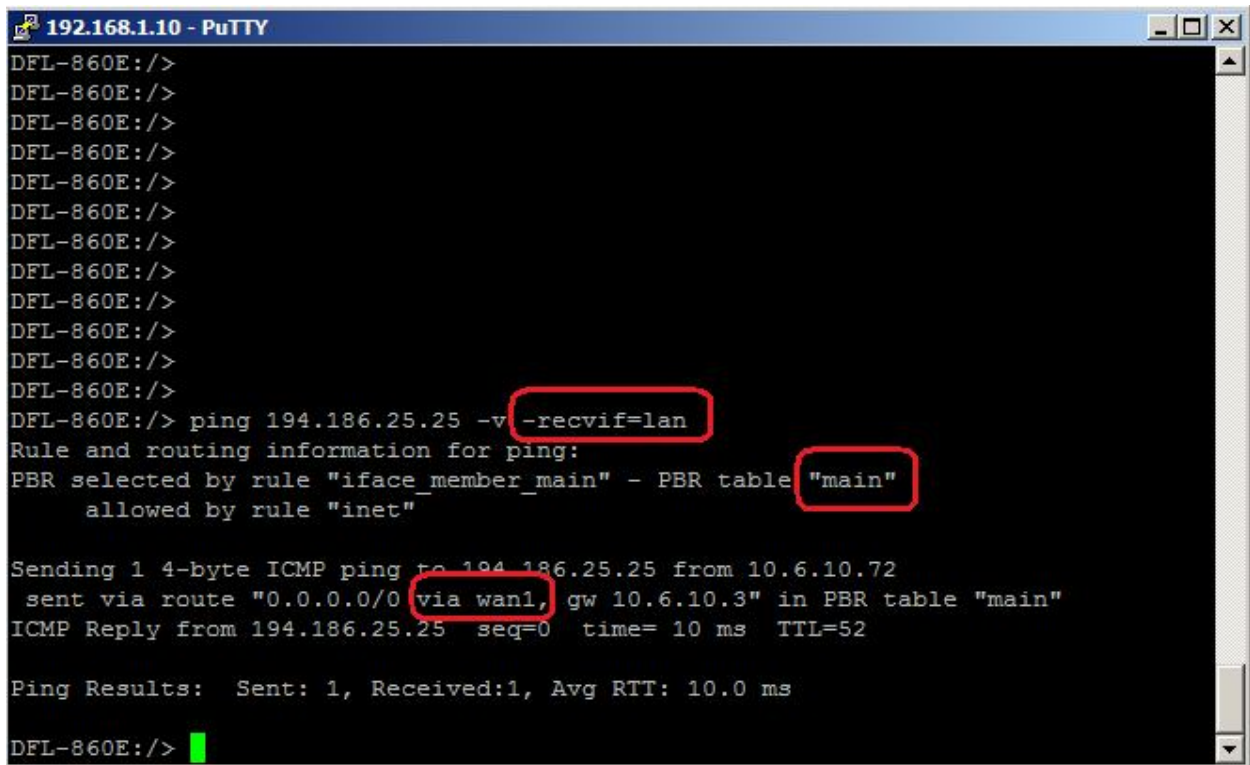
```
add IPRuleFolder Name=toInet
cc IPRuleFolder <N folder>
```

```
add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
Name=inet
```

```
add IPRule Action=NAT SourceInterface=dmz SourceNetwork=dmz/dmz_net
DestinationInterface=wan2 DestinationNetwork=all-nets Service=all_services
Name=inet_2
```

### Проверка конфигурации

1. Выполняем выход в интернет с интерфейса `lan` и проверяем, что соединение установлено через интерфейс `wan1`.



```
192.168.1.10 - PuTTY
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/> ping 194.186.25.25 -v -recvfif=lan
Rule and routing information for ping:
PBR selected by rule "iface_member_main" - PBR table "main"
  allowed by rule "inet"

Sending 1 4-byte ICMP ping to 194.186.25.25 from 10.6.10.72
  sent via route "0.0.0.0/0 via wan1, gw 10.6.10.3" in PBR table "main"
ICMP Reply from 194.186.25.25 seq=0 time= 10 ms TTL=52

Ping Results:  Sent: 1, Received:1, Avg RTT: 10.0 ms

DFL-860E:/>
```

2. Выполняем выход в интернет с интерфейса `dmz` и проверяем, что соединение установлено через интерфейс `wan1`.



```
192.168.1.10 - PuTTY
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/> ping 194.186.25.25 -v -recvif=dmz
Rule and routing information for ping:
PBR selected by rule "altDMZ" - PBR table "altInet"
    allowed by rule "inet_2"

Sending 1 4-byte ICMP ping to 194.186.25.25 from 192.168.20.10
  sent via route "0.0.0.0/0 via wan2, gw 192.168.20.20" in PBR table "altInet"
ICMP Reply from 194.186.25.25 seq=0 time= 10 ms TTL=51

Ping Results:  Sent: 1, Received:1, Avg RTT: 10.0 ms

DFL-860E:/> █
```

### ***Маршрутизация на основе сервиса***

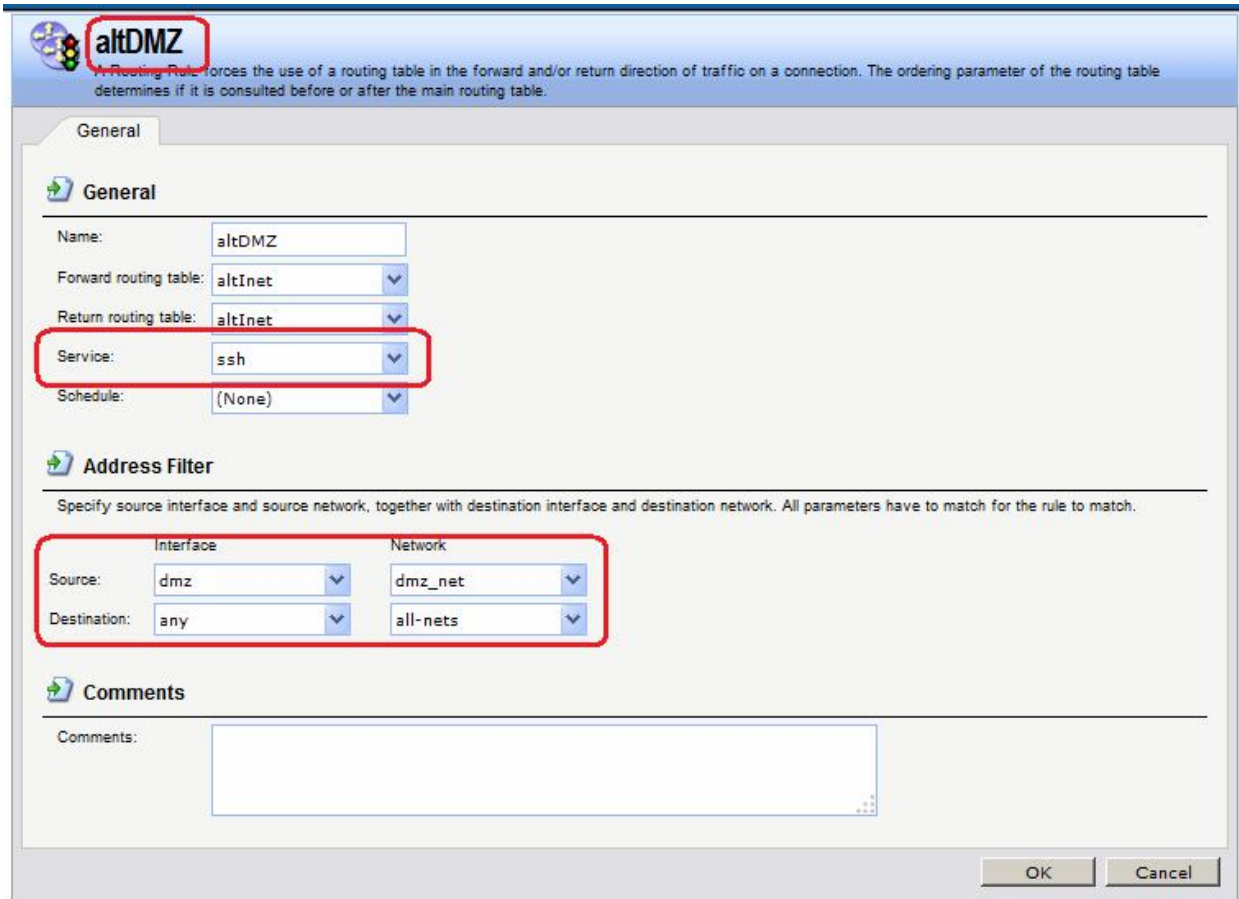
#### *Альтернативная таблица маршрутизации*

Альтернативная таблица маршрутизации создается аналогично маршрутизации на основе адреса источника.

#### *Правило выбора таблицы маршрутизации PBR*

#### **Веб-интерфейс:**

Routing → Routing Rules → Add → Routing Rule



**Командная строка:**

```
add RoutingRule ForwardRoutingTable=altInet ReturnRoutingTable=altInet
SourceInterface=dmz SourceNetwork=dmz/dmz_net DestinationInterface=any
DestinationNetwork=all-nets Service=ssh Name=altDMZ
```

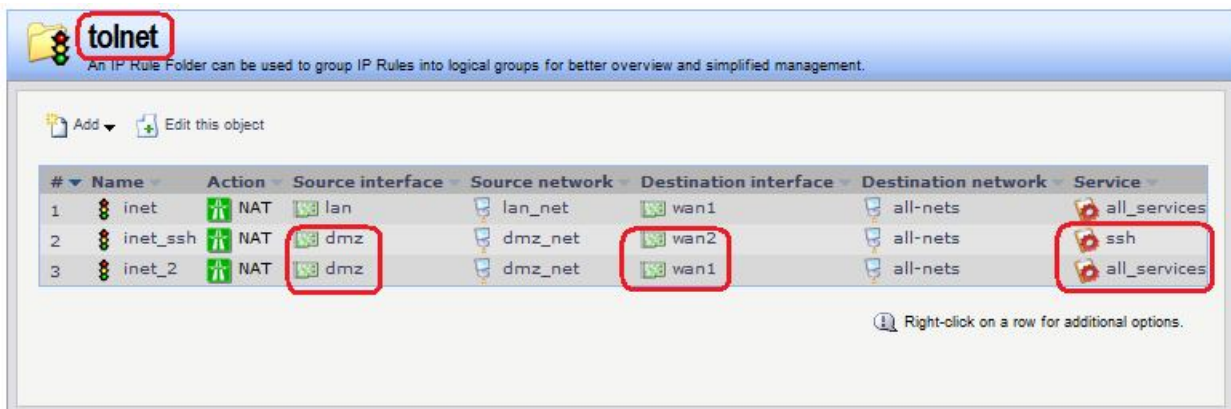
*Правила фильтрация*

**Веб-интерфейс:**

Rules → IP Rules → Add → IP Rule Folder

Name: toInet

Rules → IP Rules → toInet → Add → IP Rule



**Командная строка:**

```
add IPRuleFolder Name=toInet
```

```

cc IPRuleFolder <N folder>

add IPRule Action=NAT SourceInterface=lan SourceNetwork= lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
Name=inet

add IPRule Action=NAT SourceInterface=dmz SourceNetwork= dmz/dmz_net
DestinationInterface=wan2 DestinationNetwork=all-nets Service=ssh
Name=inet_ssh

add IPRule Action=NAT SourceInterface=dmz SourceNetwork= dmz/dmz_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
Name=inet_2

```

### Проверка конфигурации

Лабораторная работа 10. Выполняем выход в интернет по протоколу ssh с dmz-интерфейса.

```

192.168.1.10 - PuTTY
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/> ping 10.6.10.3 -v -recvif=dmz -tcp -port=22
Rule and routing information for ping:
TCP: 172.17.100.1:56965 -> 10.6.10.3:22 PBR selected by rule "altDMZ" - PBR table "altInet"
    TCP: 172.17.100.1:56965 -> 10.6.10.3:22 allowed by rule "inet_ssh"

Sending 0-byte TCP ping to 10.6.10.3:22 from 192.168.20.10:56965
  sent via route "0.0.0.0/0 via wan2, gw 192.168.20.20" in PBR table "altInet"
TCP Reply from 10.6.10.3:22 to 172.17.100.1:56965 seq=0 SYN+ACK time= 10 ms TTL=63
TCP Reply from 10.6.10.3:22 to 172.17.100.1:56965 seq=0 ACK time= 10 ms TTL=63

TCP Ping Results:  Sent: 1, RST/ACKs Received:1, Loss: 0%, Avg RTT: 10.0 ms

DFL-860E:/>

```

Лабораторная работа 11. Выполняем выход в интернет по протоколу ICMP с dmz-интерфейса.

```
192.168.1.10 - PuTTY
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/>
DFL-860E:/> ping 194.186.25.25 -v -recvif=dmz
Rule and routing information for ping:
PBR selected by rule "iface_member_main" - PBR table "main"
  allowed by rule "inet_2"

Sending 1 4-byte ICMP ping to 194.186.25.25 from 10.6.10.62
  sent via route "0.0.0.0/0 via wan1, gw 10.6.10.3" in PBR table "main"
ICMP Reply from 194.186.25.25 seq=0 time= 10 ms TTL=52

Ping Results: Sent: 1, Received:1, Avg RTT: 10.0 ms

DFL-860E:/>
```

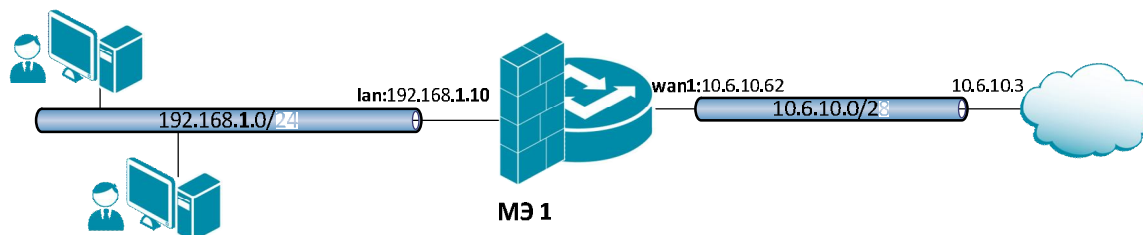
## Лабораторная работа 11. Ограничение полосы пропускания трафика

### Цель

Рассмотреть возможные способы ограничения полосы пропускания для входящего и исходящего трафиков.

1. Ограничить полосу пропускания для входящего трафика до 2 Мбит/с независимо от типа трафика.
2. Ограничить полосу пропускания в обоих направлениях до 2 Мбит/с независимо от типа трафика.

### Топология сети



### Описание практической работы

#### Ограничение полосы пропускания для входящего трафика

##### Каналы (Pipes)

Необходимо создать канал, который ограничивает весь проходящий через него трафик до 2 Мбит/с, независимо от типа трафика.

## Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipes → Add → Pipe

The screenshot shows the 'total\_in' pipe configuration window with the 'General' tab selected. The 'Name' field is set to 'total\_in'. The 'Precedences' section has three input fields: Minimum (0), Default (0), and Maximum (7). The 'Grouping' section has 'Grouping' set to 'None' and 'Network Size' set to 0. There is an unchecked checkbox for 'Enable dynamic balancing of groups'. The 'Comments' section is empty. 'OK' and 'Cancel' buttons are at the bottom right.

**total\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | Pipe Limits | Group Limits

**General**

Name: total\_in

Precedences: Minimum: 0, Default: 0, Maximum: 7

**Grouping**

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping: None

Network Size: 0

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

The screenshot shows the 'total\_in' pipe configuration window with the 'Pipe Limits' tab selected. It features a table for setting bandwidth limits per precedence. The 'Total' field is set to 2000. An information icon notes that bandwidth units are multiples of 1000. 'OK' and 'Cancel' buttons are at the bottom right.

**total\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | Pipe Limits | Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second
7:		
6:		
5:		
4:		
3:		
2:		
1:		
0:		

Total: 2000

OK Cancel

## Командная строка:

```
add Pipe total_in LimitKbpsTotal=2000
```

### Правила каналов (Pipe Rules)

Какой трафик должен проходить через канал указывается в Правиле канала.

Будем использовать созданный выше канал для ограничения входящего трафика. Это ограничение применяется к пакетам, а не к соединениям. При выполнении шейпинга трафика важно направление, в котором передаются данные, а не сторона, инициировавшая соединение.

Следует создать правило, разрешающее прохождение любого исходящего трафика. Добавляем созданный канал в *обратную цепочку* (return chain). Это означает, что пакеты, идущие в *обратном направлении* данного соединения, должны проходить через канал `total-in`.

### Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipe Rules → Add → Pipe Rule

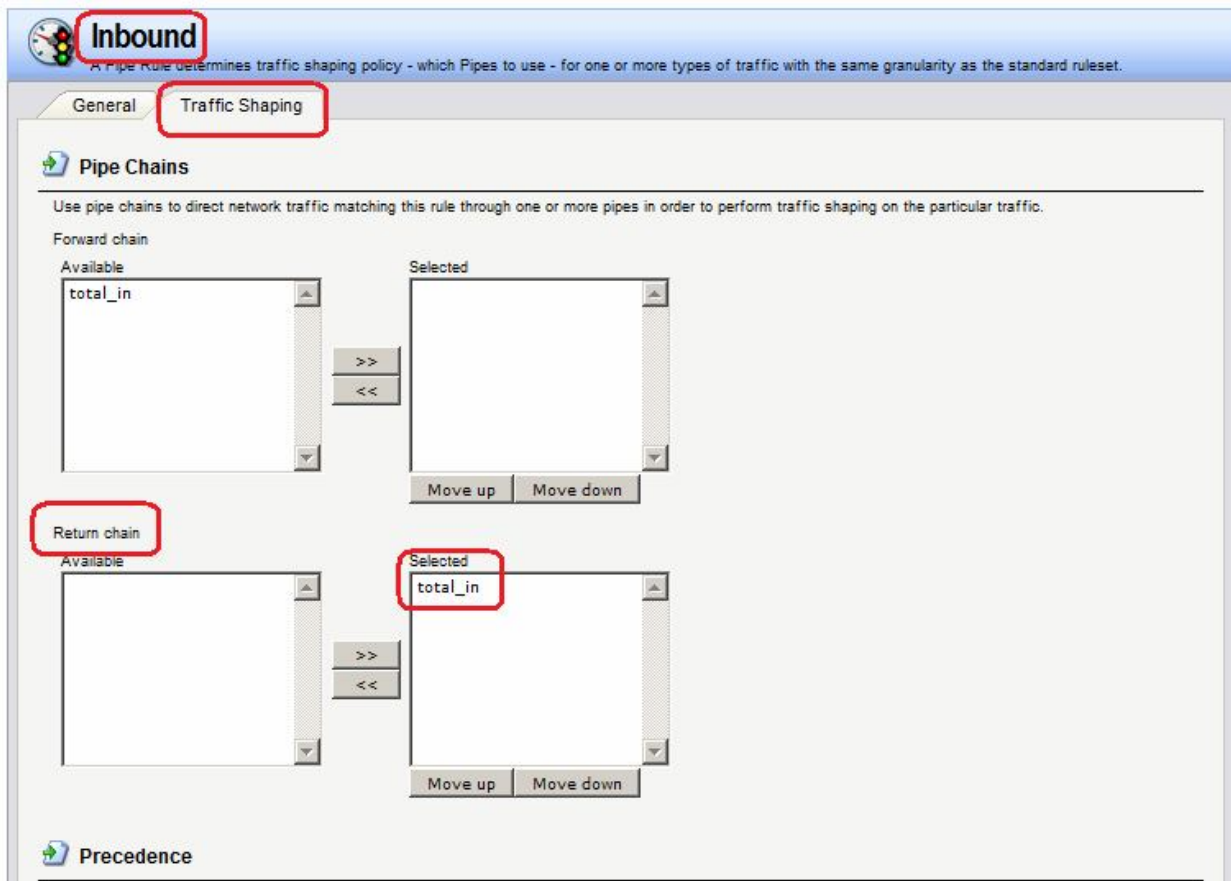
The screenshot shows the 'Add Pipe Rule' dialog box in Mikrotik WinBox. The 'Inbound' tab is selected. The 'General' section contains the following fields:

- Name: Inbound
- Service: all\_services
- Schedule: (None)

The 'Address Filter' section contains the following fields:

- Source Interface: lan
- Source Network: lan\_net
- Destination Interface: wan1
- Destination Network: all-nets

The 'Comments' section is empty. The 'OK' and 'Cancel' buttons are located at the bottom right of the dialog.



### Командная строка:

```
add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
ReturnChain=total_in Name=Inbound
```

### *Ограничение полосы пропускания в обоих направлениях*

Использование одного и того же канала для обоих направлений не решает проблему.

Направление трафика, проходящего через канал, не имеет значения, так как учитывается только суммарное количество трафика. Один и тот же канал может использоваться как для входящего, так и для исходящего трафика, при этом не будет отдельного подсчета трафика в каждом направлении.

В предыдущем примере полоса пропускания ограничена только для входящего направления. В большинстве случаев необходимо ограничивать именно входящий трафик. Но что делать, если необходимо ограничить исходящий трафик таким же образом?

Помещение `std-in` в прямую цепочку (forward chain) не принесет результата, если требуется получить ограничение до 2 Мбит/с для исходящего трафика отдельно от ограничения до 2 Мбит/с для входящего. Если помимо исходящего трафика (2 Мбит/с) через канал проходит входящий трафик (2 Мбит/с), то общий поток трафика составит 4 Мбит/с. Так как ограничение канала составляет 2 Мбит/с фактическая величина потока будет близка к значению в 1 Мбит/с в каждом направлении.

Увеличение общего ограничения до 4 Мбит/с не решит проблему, так как для одного канала это не означает ограничения 2 Мбит/с для входящего и 2 Мбит/с для

исходящего трафика. В результате может быть 3 Мбит/с исходящего и 1 Мбит/с входящего трафика, так как это также составляет 4 Мбит/с.

Для управления полосой пропускания в обоих направлениях рекомендуется использовать два отдельных канала: один для входящего, а другой для исходящего трафика. В данном сценарии в целях достижения оптимального результата для каждого канала установлено ограничение 2 Мбит/с.

### Каналы (Pipes)

Необходимо создать два канала, каждый из которых ограничивают весь проходящий через него трафик до 2 Мбит/с, независимо от типа трафика. Дополнительно к каналу, созданному ранее, добавляем канал для исходящего трафика.

### Веб-интерфейс:

**Traffic Management** → **Traffic Shaping** → **Pipes** → **Add** → **Pipe**

The screenshot shows a configuration window titled "total\_out" with a subtitle: "A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes." The window has three tabs: "General", "Pipe Limits", and "Group Limits". The "General" tab is selected and contains the following fields:

- Name:** total\_out
- Precedences:** Minimum: 0, Default: 0, Maximum: 7
- Grouping:** Grouping: None, Network Size: 0, and a checkbox for "Enable dynamic balancing of groups" which is unchecked.
- Comments:** A text area for entering comments.

At the bottom right of the window are "OK" and "Cancel" buttons.



**total\_out**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General **Pipe Limits** Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

### Командная строка:

```
add Pipe total_out LimitKbpsTotal=2000
```

### Правила каналов (Pipe Rules)

Traffic Management → Traffic Shaping → Pipe Rules → Add → Pipe Rule

**in\_out**  
A pipe rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General **Traffic Shaping**

**General**

Name:

Service:

Schedule:

**Address Filter**

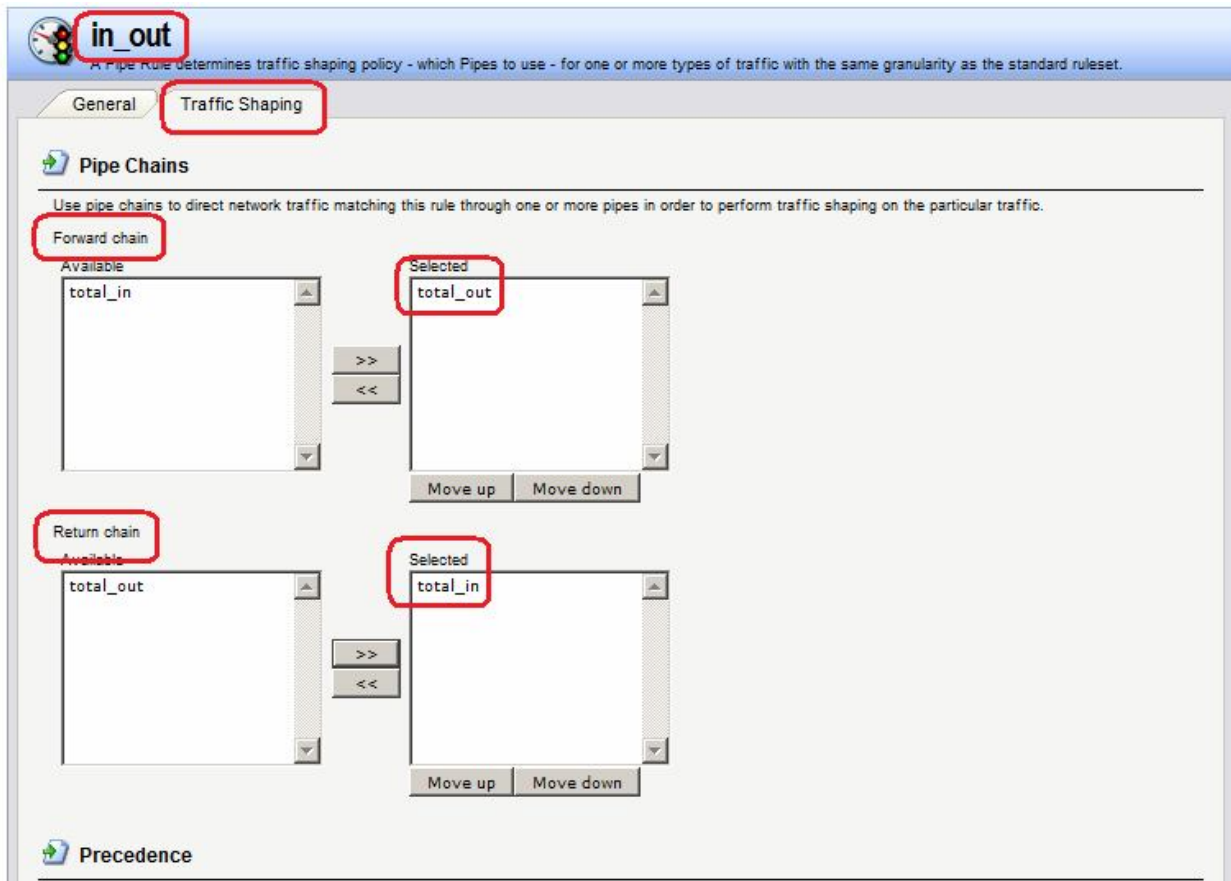
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	<input type="text" value="lan"/>	<input type="text" value="lan_net"/>
Destination:	<input type="text" value="wan1"/>	<input type="text" value="all-nets"/>

**Comments**

Comments:

OK Cancel



### Командная строка:

```
add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
ReturnChain=total_in ForwardChain=total_out Name=in_out
```

### Ограничение полосы пропускания в зависимости от типа трафика

Для простоты будем рассматривать ограничение только входящего трафика, так как в клиент-серверных приложениях как правило входящий трафик больше, чем исходящий.

#### Каналы (Pipes)

В предыдущих примерах выполнялось ограничение трафика для всех исходящих соединений. Что делать, если необходимо ограничить навигацию по веб-страницам больше, чем остальной трафик? Предположим, что ширина общей полосы пропускания – 250 кбит/с, из которых 125 кбит/с должны быть выделены для веб-трафика.

Если создать два канала, один **http-in** для ограничения входящего веб-трафика с ограничением в 125 кбит/с, а другой канал **all-in** для всего остального трафика с ограничением в 250 кбит/с, то желаемый результат достигнут не будет, так как результирующий объем трафика будет равен сумме ограничений в каждом канале, т.е. 375 кбит/с.

Для решения подобной задачи следует создать *цепочку*, состоящую из канала **all-in** и канала **http-in** для веб-трафика. Входящий веб-трафик сначала проходит через канал **http-in**, максимальное ограничение в котором 125 кбит/с. Далее трафик проходит через канал **all-in** вместе с остальным входящим трафиком. Для второго канала установлено ограничение в 250 кбит/с.

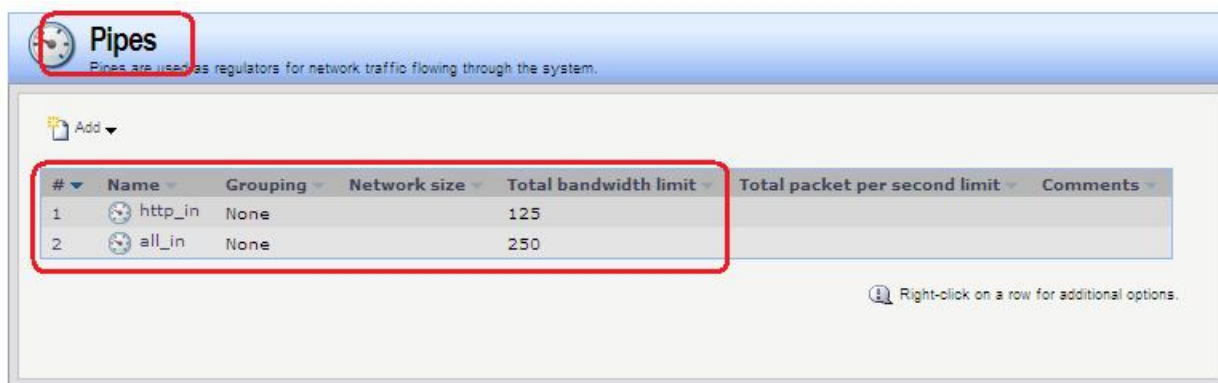
Если веб-трафик полностью потребляет 125 кбит/с, эти 125 кбит/с займут половину канала `http-in`, оставшиеся 125 кбит/с будут использоваться для остального трафика. Если веб-трафик отсутствует, то все 250 кбит/с, отведенные для канала `http-in`, могут использоваться для другого трафика.

Это не обеспечивает гарантируемую полосу пропускания для веб-трафика, но устанавливает ограничение для него до 125 кбит/с и гарантирует полосу пропускания 125 кбит/с для всего остального трафика. Для веб-трафика в канале `http-in` применяются стандартные правила: трафик будет проходить на общих основаниях наравне с другим трафиком. Это означает ограничение в 125 кбит/с, при этом возможна более низкая скорость, если канал загружен.

Подобный способ задания каналов определяет ограничения на максимальные значения для некоторых типов трафика и не задает приоритеты для различных типов конкурирующего трафика.

### Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipes → Add → Pipe



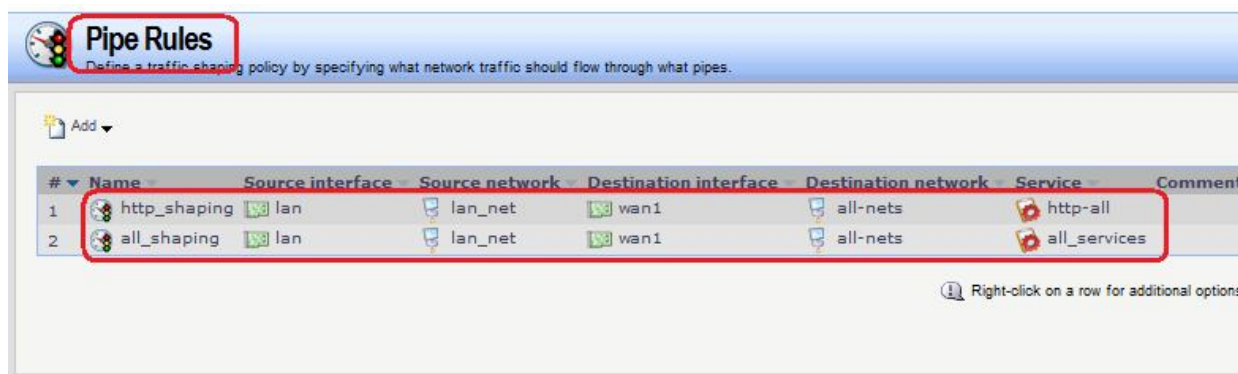
### Командная строка:

```
add Pipe http_in LimitKbpsTotal=125
```

```
add Pipe all_in LimitKbpsTotal=250
```

### Правила каналов (Pipe Rules)

Traffic Management → Traffic Shaping → Pipe Rules → Add → Pipe Rule



**http\_shaping**  
 A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**General**

Name: http\_shaping

Service: http-all

Schedule: (None)

**Address Filter**

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

Source: Interface: lan Network: lan\_net

Destination: wan1 all-nets

**Comments**

Comments:

OK Cancel

**http\_shaping**  
 A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**Pipe Chains**

Use pipe chains to direct network traffic matching this rule through one or more pipes in order to perform traffic shaping on the particular traffic.

Forward chain

Available: all\_in, http\_in

Selected:

Move up Move down

Return chain

Available:

Selected: all\_in, http\_in

Move up Move down

**Precedence**

**all\_shaping**  
A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**General**

Name: all\_shaping

Service: all\_services

Schedule: (None)

**Address Filter**

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

Source: Interface: lan Network: lan\_net

Destination: wan1 all-nets

**Comments**

Comments:

OK Cancel

**all\_shaping**  
A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**Pipe Chains**

Use pipe chains to direct network traffic matching this rule through one or more pipes in order to perform traffic shaping on the particular traffic.

Forward chain

Available: all\_in, http\_in

Selected:

Move up Move down

Return chain

Available: http\_in

Selected: all\_in

Move up Move down

**Precedence**

### Командная строка:

```
add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=http-all
ReturnChain=http_in,all_in Name=http_shaping
```

```
add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
ReturnChain=all_in Name=all_shaping
```

## **Использование приоритетов**

### *Каналы (Pipes)*

Добавим в предыдущий пример требование, что трафик SSH должен иметь более высокий приоритет по сравнению с остальным трафиком. Для этого добавим Правило канала специально для SSH и установим в правиле более высокий приоритет – например, 2. В данном новом правиле мы указываем каналы, используемые для остального трафика.

Результатом этого будет назначение более высокого приоритета SSH-пакетам, при этом отправка этих пакетов выполняется через тот же канал, что и остальной трафик. Механизм каналов гарантирует, что при превышении ограничения полосы пропускания, указанного в настройках канала, пакеты с более высоким приоритетом будут отправлены в первую очередь. Пакеты с более низким приоритетом будут помещены в буфер и отправлены, если используемая пропускная способность меньше, чем максимальная величина, указанная для канала. Процесс буферизации иногда приводит к обратному эффекту, так как уменьшается скорость потока.

Указание ограничения для приоритета гарантирует минимальное количество полосы пропускания для данного приоритета. Трафик, проходящий через канал, получит гарантированную полосу пропускания, указанную для приоритета, за счет урезания трафика с более низким приоритетом.

Если исходящий трафик с приоритетом 2 превышает 100 кбит/с, то приоритет той части трафика, которая превышает данное ограничение, понижается до приоритета негарантированной доставки (best effort). Весь трафик с приоритетом негарантированной доставки (best effort) будет отправлен в порядке поступления.

### **Веб-интерфейс:**

**Traffic Management → Traffic Shaping → Pipes → Add → Pipe**

**ssh\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**General**

Name:

Precedences: Minimum:  Default:  Maximum:

**Grouping**

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping:

Network Size:

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

**ssh\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second.
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text" value="100"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

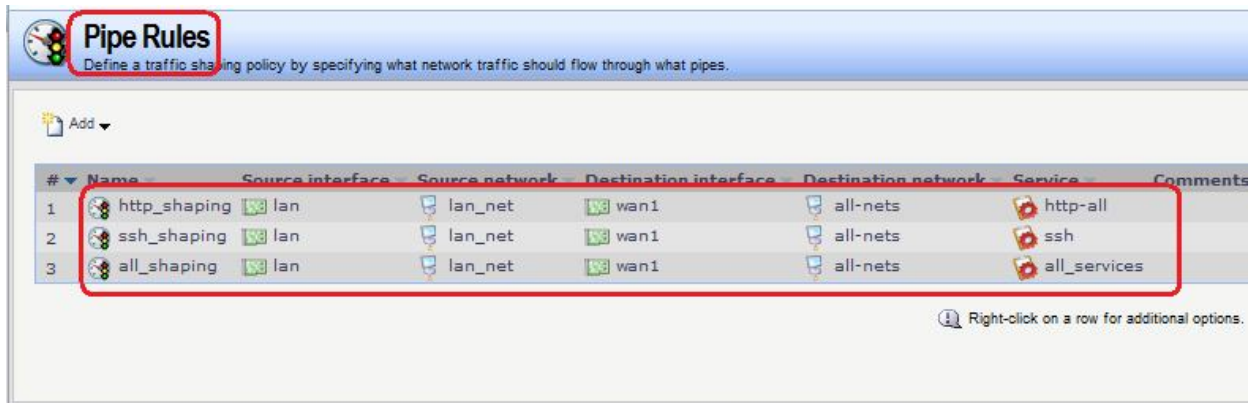
**Командная строка:**

`add Pipe ssh_in LimitKbpsTotal=250 LimitKbps2=100`

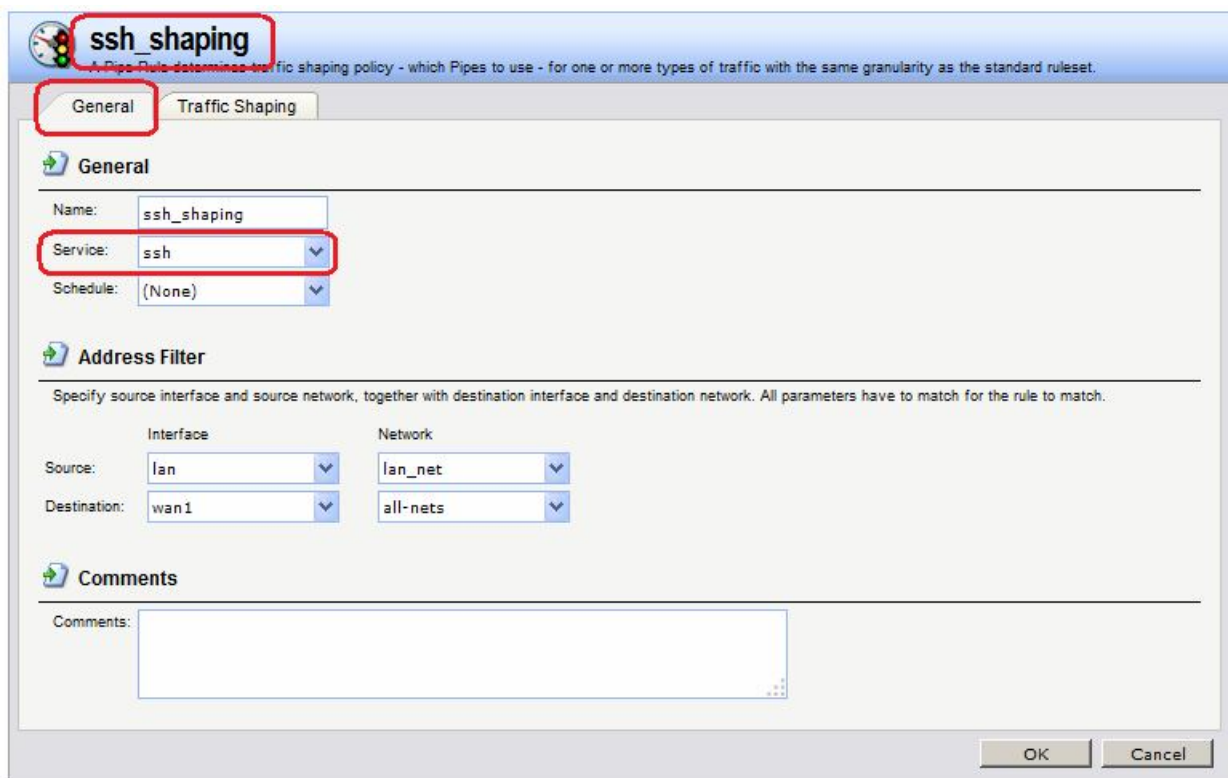
## Правила каналов (Pipe Rules)

### Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipe Rules → Add → Pipe Rule



#	Name	Source interface	Source network	Destination interface	Destination network	Service	Comments
1	http_shaping	lan	lan_net	wan1	all-nets	http-all	
2	ssh_shaping	lan	lan_net	wan1	all-nets	ssh	
3	all_shaping	lan	lan_net	wan1	all-nets	all_services	



**General** Traffic Shaping

**General**

Name: ssh\_shaping

Service: ssh

Schedule: (None)

**Address Filter**

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

Source: Interface: lan Network: lan\_net

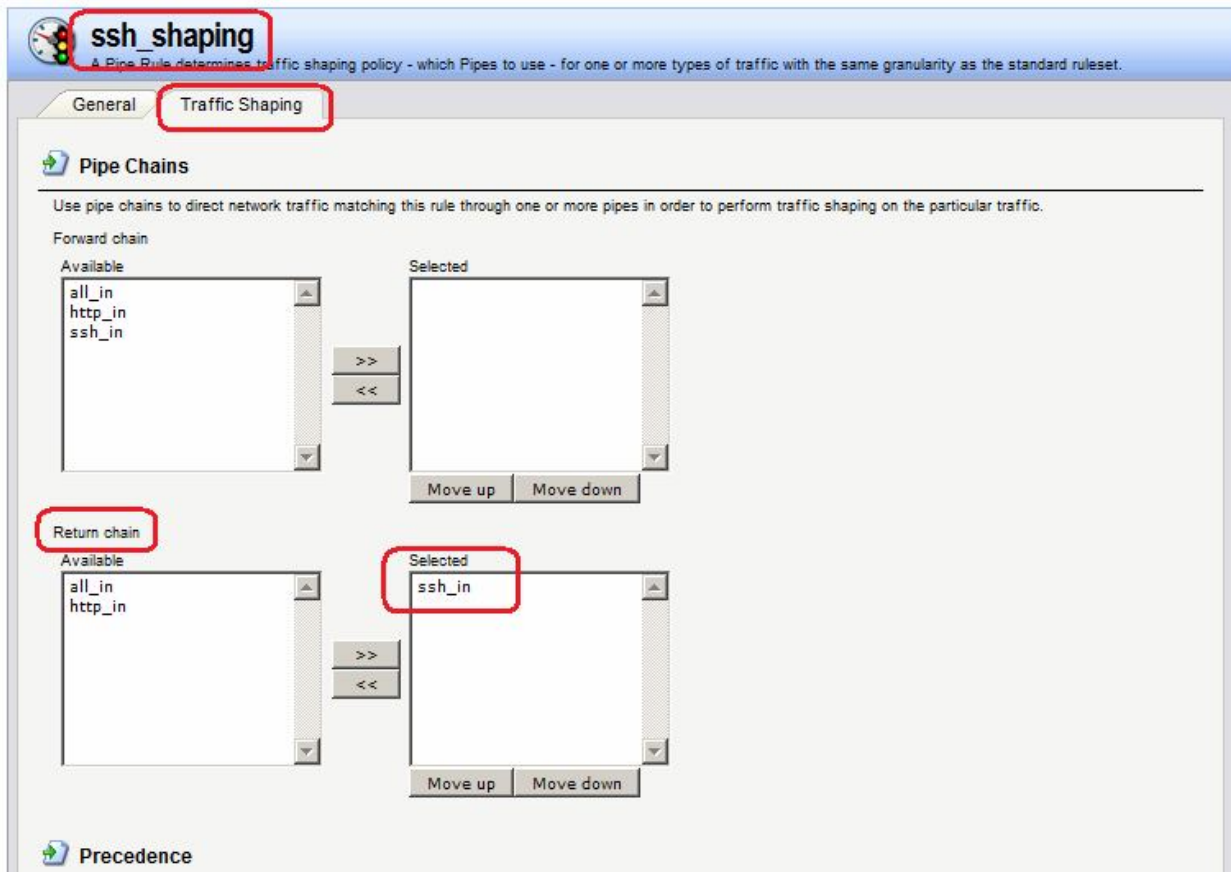
Destination: Interface: wan1 Network: all-nets

**Comments**

Comments:

OK Cancel





### Командная строка:

```
add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=ssh
ReturnChain=ssh_in Name=ssh_shaping
```

### *Различные гарантий полосы пропускания для разных сервисов*

#### *Каналы (Pipes)*

Иногда требуется предоставить различные гарантии полосы пропускания разным сервисам, например, гарантию в 32 кбит/с HTTP-трафику и гарантию в 64 кбит/с SSH-трафику. Можно было бы задать ограничение в 32 кбит/с для приоритета 2, 64 кбит/с для приоритета 4 и затем указать различным типам трафика разные приоритеты. При таком подходе можно столкнуться с ограниченным количеством различных приоритетов

Решение этой проблемы заключается в создании двух каналов: один для HTTP-трафика и другой для SSH-трафика. Для обоих каналов следует указать приоритет 2 в качестве приоритета по умолчанию, и задать ограничения для приоритета 2, соответственно, 32 и 64 кбит/с.

### Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipes → Add → Pipe

**std\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**General**

Name:

Precedences: 

	Minimum	Default	Maximum
Precedences:	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="7"/>

**Grouping**

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping:

Network Size:

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

**std\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences: 

	Kilobits per second	Packets per second
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

**std\_out**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**General**

Name:

Precedences: 

	Minimum	Default	Maximum
Precedences:	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="7"/>

**Grouping**

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping:

Network Size:

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

**std\_out**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

**ssh\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**General**

Name:

Precedences: 

	Minimum	Default	Maximum
Precedences:	<input type="text" value="0"/>	<input type="text" value="2"/>	<input type="text" value="7"/>

**Grouping**

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping:

Network Size:

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

**ssh\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences: 

	Kilobits per second	Packets per second
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text" value="64"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

**http\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**General**

Name:

Precedences: 

	Minimum	Default	Maximum
Precedences:	<input type="text" value="0"/>	<input type="text" value="2"/>	<input type="text" value="7"/>

**Grouping**

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping:

Network Size:

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

**http\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences: 

Precedences:	Kilobits per second	Packets per second
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text" value="32"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

### Командная строка:

```
add Pipe std_out LimitKbpsTotal=250
```

```
add Pipe std_in LimitKbpsTotal=250
```

```
add Pipe ssh_in PrecedenceDefault=2 LimitKbps2=64
```

```
add Pipe http_in PrecedenceDefault=2 LimitKbps2=32
```

### Правила каналов (Pipe Rules)

Следует создать два правила для HTTP-трафика и SSH-трафика.

В качестве прямой цепочки для обоих правил следует указать только канал **std-out**.

В качестве обратной цепочки в правиле для SSH-трафика следует указать канал **ssh-in**, затем канал **std-in**. В качестве обратной цепочки в правиле для HTTP-трафика следует указать канал **http-in**, затем канал **std-in**.

В качестве значения приоритета в обоих правилах следует выбрать установить флаг **Use defaults from first pipe**. Для обоих каналов **ssh-in** и **http-in** приоритетом по умолчанию является приоритет 2.

Использование данного подхода является более рациональным решением, чем указание приоритета 2 в наборе правил, так как в этом случае можно легко изменить приоритет всего трафика, как SSH, так и HTTP, поменяв приоритет по умолчанию каналов **ssh-in** и **http-in**.

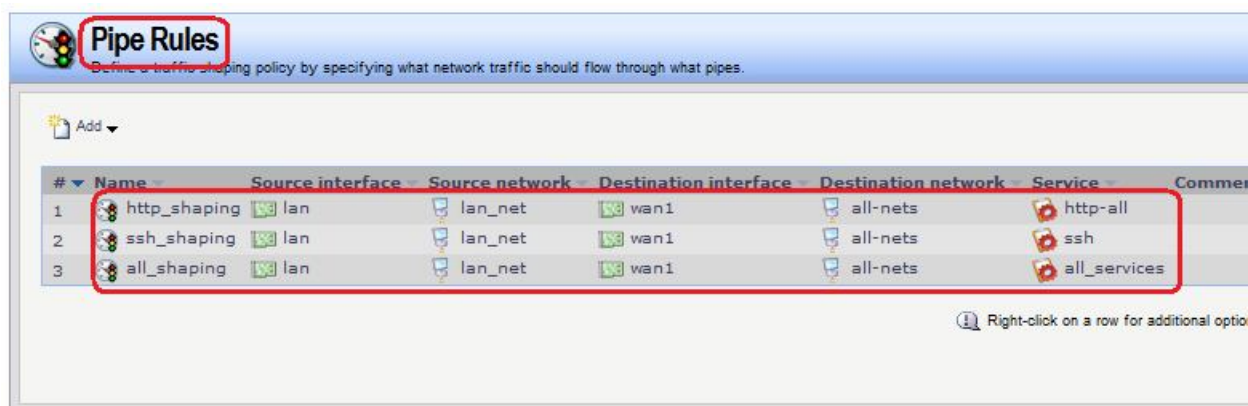
Можно не задавать общее ограничение для каналов **ssh-in** и **http-in**, так как общее ограничение будет указано в канале **std-in**, который является последним в каждой из цепочек.

Каналы **ssh-in** и **http-in** действуют в качестве фильтров приоритетов. Благодаря им через канал **std-in** будет проходить только зарезервированное количество трафика с приоритетом 2 (64 и 32 кбит/с соответственно). Остальная часть трафика SSH и HTTP, превысившего эти значения, пройдет через канал **std-in** с приоритетом 0, который является приоритетом негарантированной доставки для каналов **std-in** и **ssh-in**.

Порядок цепочек важен. Если указать канал **std-in** перед **ssh-in** и **http-in**, то трафик пройдет через канал **std-in** с наименьшим приоритетом и, следовательно, будет конкурировать за 250 кбит/с доступной полосы пропускания с остальным трафиком.

### Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipe Rules → Add → Pipe Rule



**http\_shaping**  
 A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**General**

Name: http\_shaping

Service: http-all

Schedule: (None)

**Address Filter**

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

Source: Interface: lan Network: lan\_net

Destination: wan1 all-nets

**Comments**

Comments:

OK Cancel

**http\_shaping**  
 A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**Pipe Chains**

Use pipe chains to direct network traffic matching this rule through one or more pipes in order to perform traffic shaping on the particular traffic.

**Forward chain**

Available: http\_in, ssh\_in, std\_in

Selected: std\_out

Move up Move down

**Return chain**

Available: ssh\_in, std\_out

Selected: http\_in, std\_in

Move up Move down

**Precedence**

**ssh\_shaping**  
 A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**General**

Name: ssh\_shaping

Service: ssh

Schedule: (None)

**Address Filter**

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

Source: Interface: lan Network: lan\_net

Destination: wan1 all-nets

**Comments**

Comments:

OK Cancel

**ssh\_shaping**  
 A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**Pipe Chains**

Use pipe chains to direct network traffic matching this rule through one or more pipes in order to perform traffic shaping on the particular traffic.

**Forward chain**

Available: http\_in, ssh\_in, std\_in

Selected: std\_out

Move up Move down

**Return chain**

Available: http\_in, std\_out

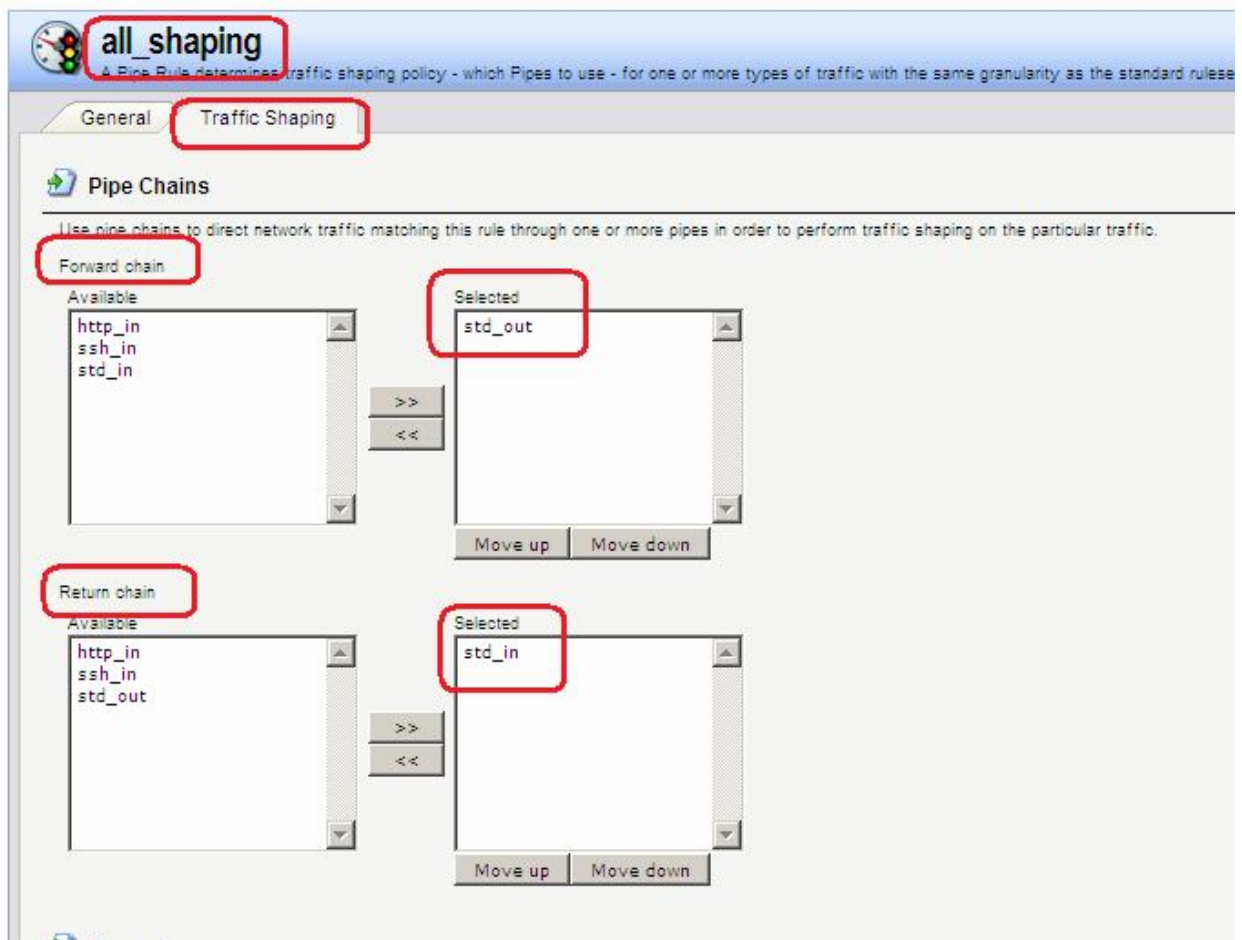
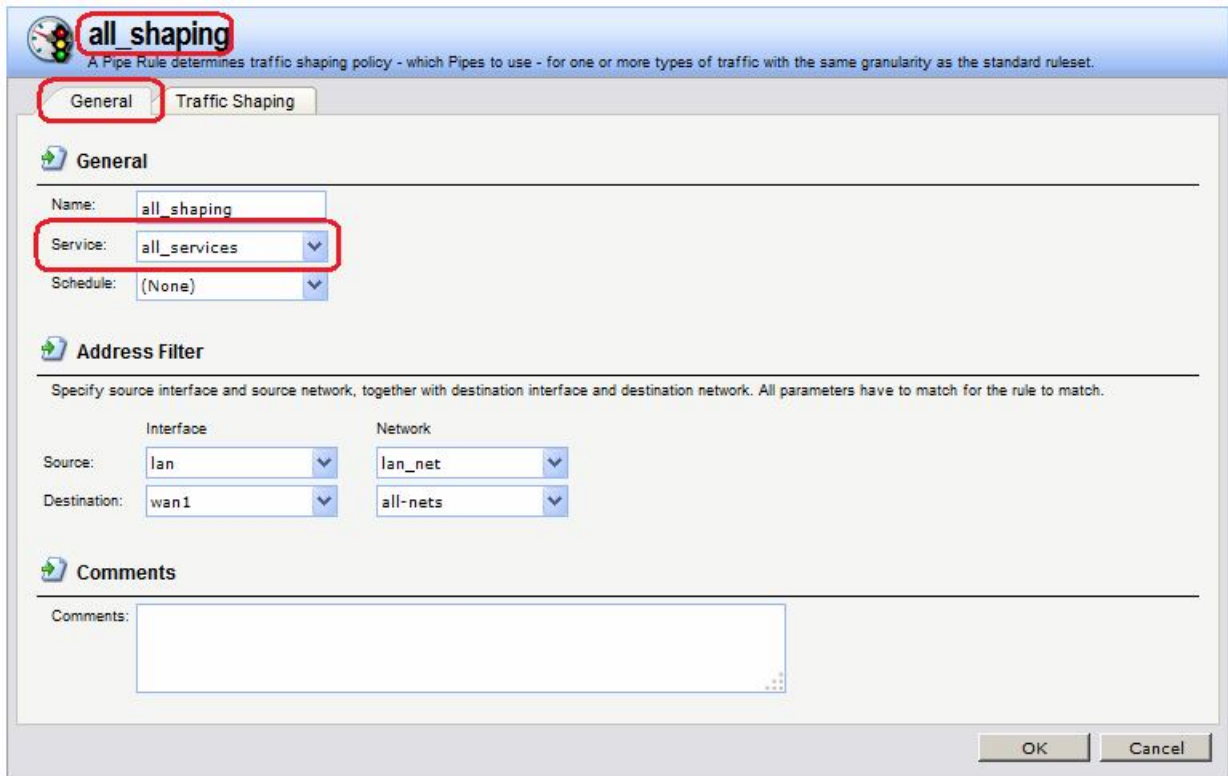
Selected: ssh\_in, std\_in

Move up Move down

**Precedence**

Use defaults from first pipe





**Командная строка:**

```

add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=http-all
ForwardChain=std_out ReturnChain=http_in,std_in Name=http_shaping

add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=ssh
ForwardChain=std_out ReturnChain=ssh_in,std_in Name=ssh_shaping

add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
ForwardChain=std_out ReturnChain=std_in Name=all_shaping

```

## Использование групп

### Каналы (Pipes)

Рассмотрим другую ситуацию, в которой общее ограничение полосы пропускания канала составляет 400 бит/с. Если необходимо разделить эту полосу пропускания среди нескольких IP-адресов назначения таким образом, чтобы на отдельный IP-адрес приходилось не более 100 кбит/с полосы пропускания, необходимо выполнить следующие шаги:

- Задать обычным способом ограничение канала – 400 кбит/с.
- Установить в канале опцию **Grouping** в значении **Destination IP**.
- На вкладке **Group Limits** задать общее ограничение канала для группы – 100 кбит/с.

Теперь полоса пропускания распределяется по принципу живой очереди, однако, ни один IP-адрес назначения не сможет получить более 100 кбит/с. Независимо от количества подключений общая ширина полосы пропускания все же не сможет превысить ограничение для канала в 400 кбит/с.

Рассмотрим взаимосвязь значений, указанных для приоритетов для каналов и групп

Предположим, что опция создания группы включена с помощью выбора одного из параметров, например, IP-адреса источника, и значения некоторых приоритетов указаны на вкладке **Group Limits**. Рассмотрим, как эти значения взаимосвязаны со значениями, указанными для этих же приоритетов на вкладке **Pipe Limits**.

В данном случае значение приоритета на вкладке **Group Limits** является гарантией полосы пропускания, а значение для того же приоритета на вкладке **Pipe Limits** является ограничением трафика. Например, если трафик группируется по IP-адресу источника, и на вкладке **Group Limits** для приоритета 5 задано значение 5 Кбит/с, а на вкладке **Pipe Limits** приоритету 5 присвоено значение 20 Кбит/с, то после подключения четвертого IP-адреса источника ( $4 \times 5 = 20$  Кбит/с) будет достигнуто ограничение приоритета, и далее гарантии полосы пропускания не будут обеспечиваться.

Вместо указания общего ограничения на группу можно включить опцию **Dynamic Balancing**. Это обеспечивает одинаковое разделение полосы пропускания между всеми участниками группы, не зависимо от их количества.

Если при включенной опции динамической балансировки также задано общее ограничение на группу, например, 100 бит/с, то это означает, что ни один участник группы не сможет получить больше данной величины полосы пропускания.

### Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipe Rules → Add → Pipe Rule

**std\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | Pipe Limits | Group Limits

**General**

Name:

Precedences: Minimum:  Default:  Maximum:

**Grouping**

Grouping enables per-port/network static bandwidth limits as well as dynamic balancing between groups.

Grouping:

Network Size:

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

**std\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | Pipe Limits | Group Limits

**Pipe Limits**

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

**std\_in**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General | **Pipe Limits** | **Group Limits**

**Group Limits**

Use group limits to specify bandwidth limits per precedence and group in the pipe. If dynamic balancing is used, the actual limits may be lower than what is configured here.

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

OK Cancel

**std\_out**  
A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

**General** | Pipe Limits | Group Limits

**General**

Name:

Precedences:	Minimum	Default	Maximum
	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="7"/>

**Grouping**

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping:

Network Size:

Enable dynamic balancing of groups.

**Comments**

Comments:

OK Cancel

**Командная строка:**

```
add Pipe std_in LimitKbpsTotal=400 Grouping=DestinationIP
UserLimitKbpsTotal=100
add Pipe std_out
```

## Правила каналов (Pipe Rules)

Правило каналов достаточно простое. В данном случае достаточно одного правила.

### Веб-интерфейс:

Traffic Management → Traffic Shaping → Pipe Rules → Add → Pipe Rule

**Pipe Rules**  
Define a traffic shaping policy by specifying what network traffic should flow through what pipes.

Add ▾

#	Name	Source interface	Source network	Destination interface	Destination network	Service	Comments
1	all_shaping	lan	lanetFW1	wan2	all-nets	all_services	

Right-click on a row for additional options

**all\_shaping**  
A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

General Traffic Shaping

**General**

Name: all\_shaping

Service: all\_services

Schedule: (None)

**Address Filter**  
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

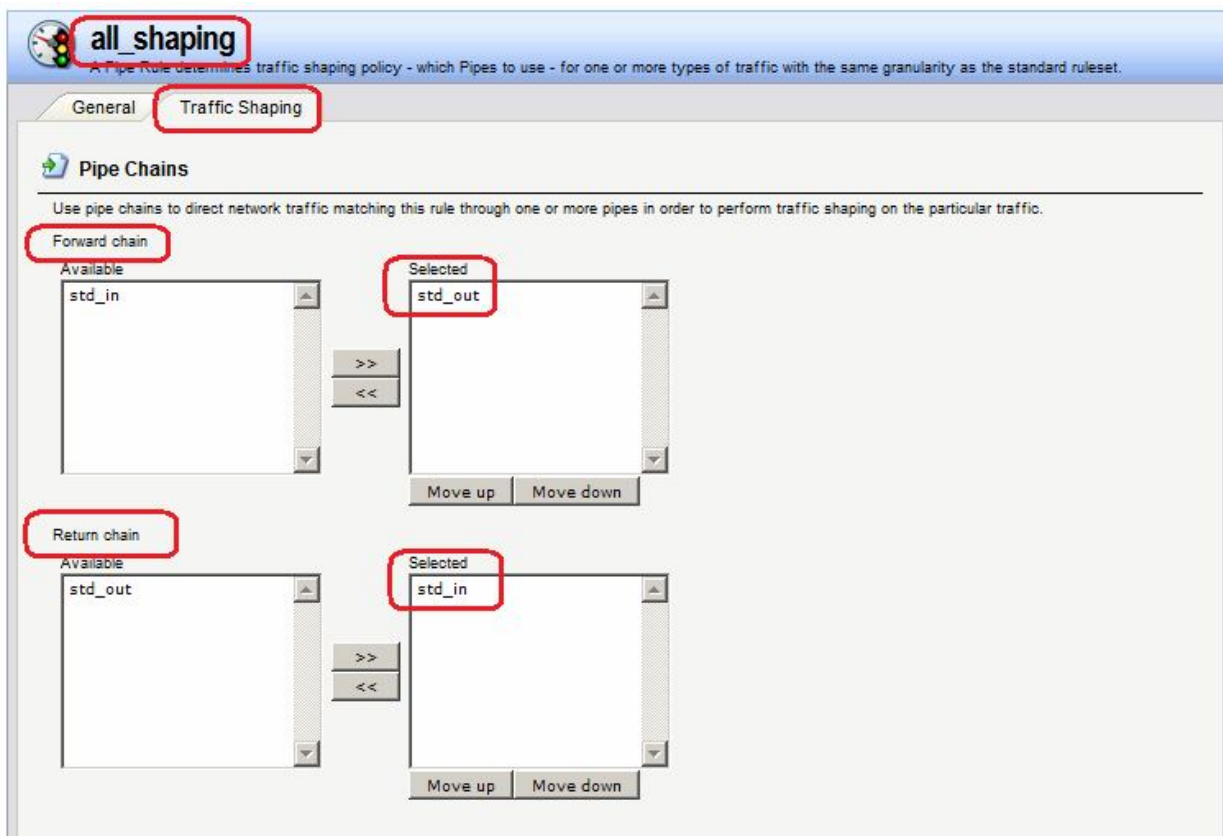
Source: Interface: lan Network: lan\_net

Destination: Interface: wan1 Network: all-nets

**Comments**

Comments:

OK Cancel



### Командная строка:

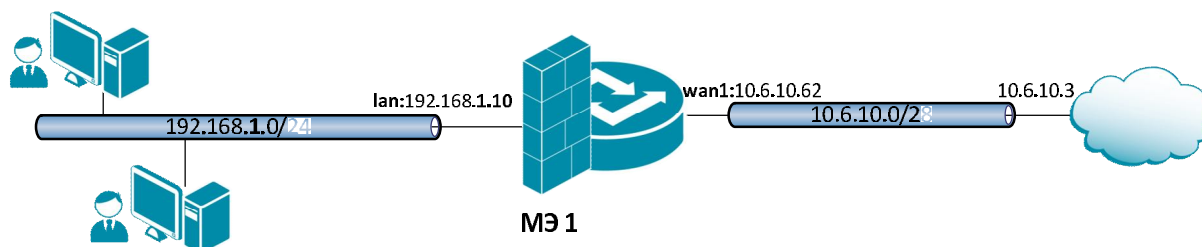
```
add PipeRule SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
ForwardChain=std_out ReturnChain=std_in Name=all_shaping
```

## Лабораторная работа 12. Ограничение полосы пропускания P2P-трафика с использованием IDP

### Цель

Рассмотреть возможность ограничения P2P-трафика, используя IDP для обнаружения P2P-трафика.

### Топология сети



### Описание практической работы

Рассмотрим типичный сценарий использования передачи данных по P2P-протоколу. Последовательность событий выглядит следующим образом:

- Клиент с IP-адресом 192.168.1.30 инициирует передачу файлов по P2P-

протоколу.

- Данное соединение запускает IDP-правило, связанное с сигнатурой IDP, целевыми объектами для которой являются P2P-приложения.
- Действие **Pipe** в правиле создает канал для шейпинга трафика с заданной пропускной способностью, и соединение направляется в этот канал.
- Последующее зависимое соединение выполняется в пределах временного интервала IDP-правила, поэтому трафик данного соединения направлен в канал и подвергается шейпингу.

## Определение правила IDP

Веб-интерфейс:

IDP / IPS → IDP Rules → Add → IDP Rule

**idpP2P**  
An IDP Rule defines a filter for matching specific network traffic. When the filter criterion is met, the IDP Rule Actions are evaluated and possible actions taken.

General Rule Actions

**General**

Name:

Service:

Schedule:

Protect against insertion/evasion attacks

**HTTP Normalization**

Invalid UTF8:

Invalid hex encoding:

Double encoding:

**Address Filter**

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

	Interface	Network
Source:	<input type="text" value="lan"/>	<input type="text" value="lan_ws"/>
Destination:	<input type="text" value="wan1"/>	<input type="text" value="all-nets"/>

**Comments**

**idpP2P**  
An IDP Rule defines a filter for matching specific network traffic. When the filter criterion is met, the IDP Rule Actions are evaluated and possible actions taken.

General Rule Actions

Add ▼

#	Action	Signature(s)
1	Pipe	POLICY_P2P_*

Right-click on a row for additional options.

OK Cancel

## IDP Rule

An IDP Rule defines a filter for matching specific network traffic. When the filter criterion is met, the IDP Rule Actions are evaluated and possible actions taken.

**General** | Rule Actions

### General

Name:

Service:

Schedule:

Protect against insertion/evasion attacks

### HTTP Normalization

Invalid UTF8:

Invalid hex encoding:

Double encoding:

### Address Filter

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

	Interface	Network
Source:	<input type="text" value="wan1"/>	<input type="text" value="all-nets"/>
Destination:	<input type="text" value="lan"/>	<input type="text" value="lan_ws"/>

## IDP Rule Action

An IDP Rule Action specifies what signatures to search for in the network traffic, and what action to take if those signatures are found.

**General** | Log Settings

### General

Action:

Signature(s): POLICY\_P2P\_\*

- IDP
- IDS
- IPS
- POLICY



**ZoneDefense**

Use ZoneDefense

**Traffic Shaping**

Configure bandwidth for hosts that trigger an IDP Pipe action. Once a connection has been piped, it will remain piped for the rest of its lifetime.

Bandwidth:  kbit/s

Network:

Traffic shaping will only apply to hosts that are within this network.

Pipe future connections

Time Window:  seconds

Throttling of new connections to and from the triggering host will stop after the configured amount of time.

**Dynamic Black Listing**

### Командная строка:

```
add IDPRule SourceInterface=lan SourceNetwork=lan/lan_ws
DestinationInterface=wan1 DestinationNetwork=all-nets Service=all_services
Name=idpP2P
```

```
cc IDPRule 1
```

```
add IDPRuleAction Action=Pipe PipeLimit=5 PipeNetwork=lan/lan_ws
PipeNewConnections=Yes PipeTimeWindow=100 Signatures=POLICY_P2P_*
```

### Просмотр объектов шейпинга трафика

- Просмотр хостов

Шейпинг трафика на основе IDP поддерживает специальную команду `idppipes`, с помощью которой можно осуществлять наблюдение и управление хостами, являющимися в данный момент объектами для шейпинга.

- Просмотр каналов

При шейпинге трафика с использованием IDP используются стандартные каналы, которые создаются автоматически. Эти каналы всегда получают наивысший приоритет, и при шейпинге используют особенности настройки для групп.

Созданные каналы не видны через веб-интерфейс, но их просмотр и управление можно выполнить с помощью команды `pipes`.

Каналы шейпинга трафика на основе IDP можно определить по автоматическому добавлению к имени префикса `IDP`.