

# netshe\_doc\_chap5

Original file



**NETSHe Lab**

## Универсальное программное обеспечение

### NETSHe

#### для сетевых устройств.

Часть 5. Межсетевой экран и другие средства фильтрации.

NETSHe Lab длительное время занимается разработками программного обеспечения для сетевых устройств, провайдеров услуг и операторов связи. Среди программного обеспечения центральное место занимает операционная система NETSHe, которая может быть использована в широком спектре сетевых устройств и сервисов.

Версия 2  
Апрель, 2020

Станислав Корсаков, ООО «Нетше лаб»  
(с) 2009-2020 Ярославль

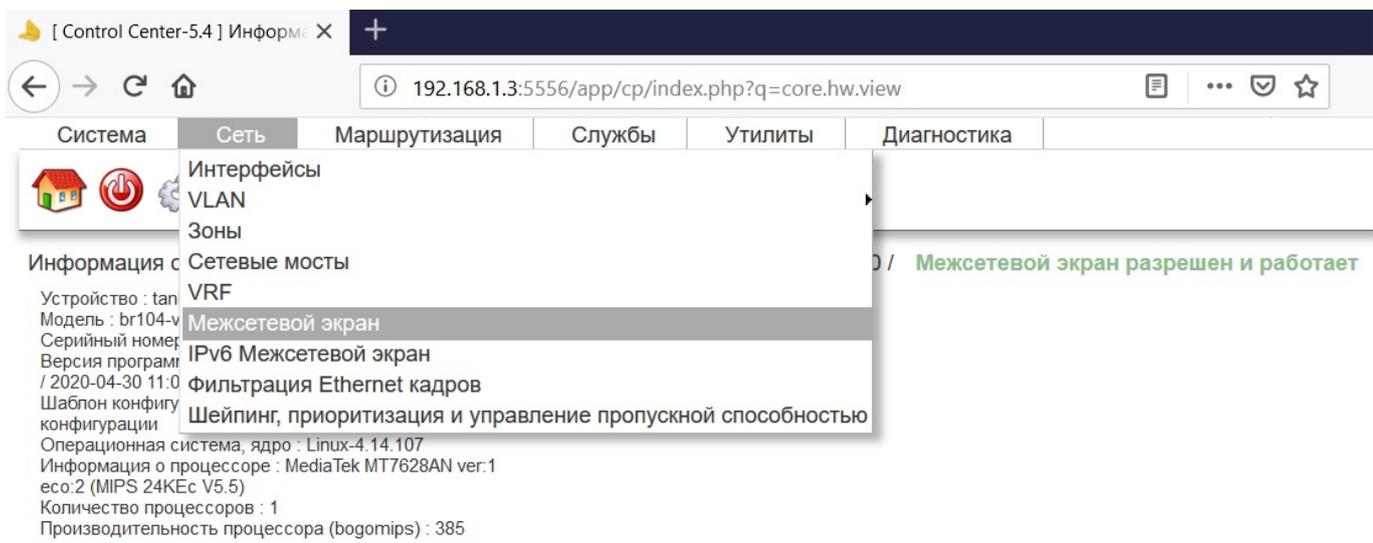
Оглавление

## Межсетевой экран в NETSHe

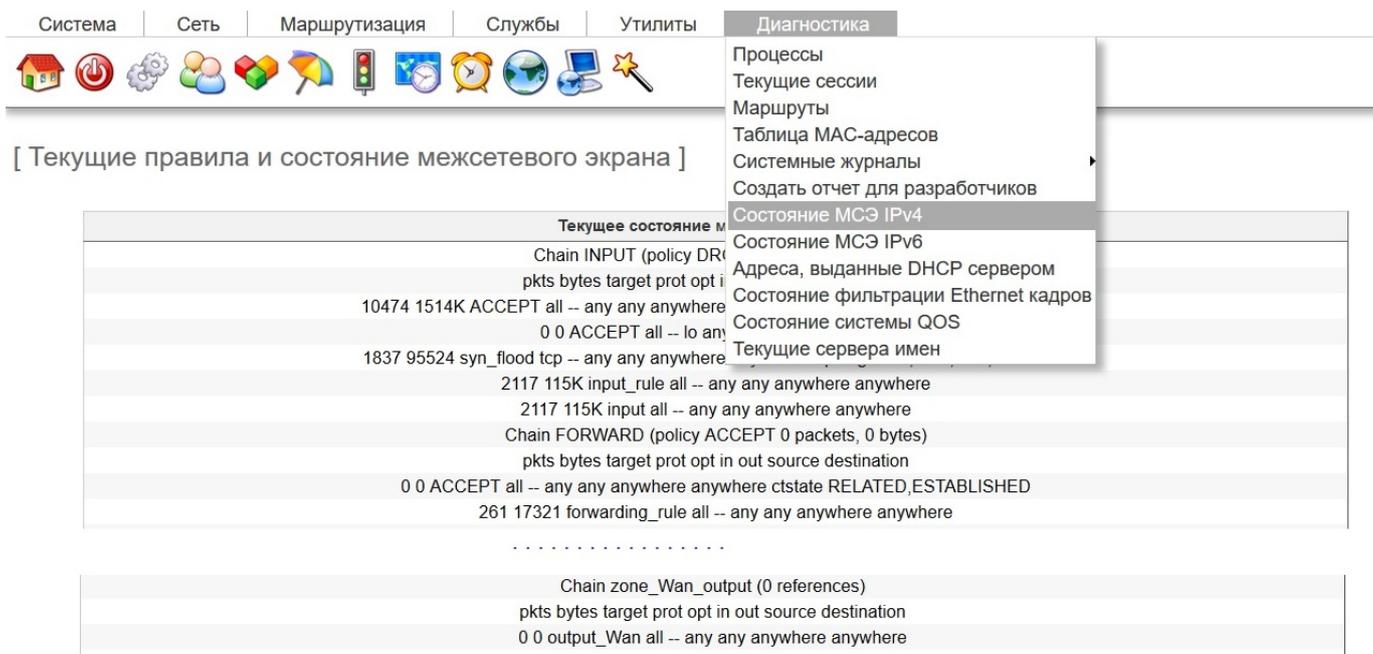
В состав операционной системы NETSHe включен весьма мощный межсетевой экран и средства управления им. К встроенным функциям межсетевого экрана следует отнести:

1. Задание гибких правил для приема, отбрасывания, пересылки трафика на основании IP-адресов/сетей источника и получателя, портов/ протоколов (в том числе протоколов приложений 7-го уровня модели OSI), MAC-адресов источника и т. п.;
2. Зональный принцип работы с автоматическим включением интерфейсов в соответствующую зону;
3. Задание умалчиваемых политик для всего экрана и, отдельно, для каждой из зон;
4. Динамическая трансляция сетевых адресов (NAT);
5. Статическая трансляция сетевых адресов и портов (SNAT/PAT);
6. Прочие виды трансляции сетевых адресов (source NAT, policy NAT)
7. защиту от SYN-flood атак,
8. экспорт данных о потоке трафика, проходящем через экран в формате netflow v5.

Средства управления сетевым экраном собраны в пунктах меню WebUI «Сеть→Межсетевой экран» («Сеть→IPv6 Межсетевой экран»), они представляют собой страницы-вкладки по числу зон, а так же вкладки с общими настройками для всех зон.



WebUI предоставляет визуально ясный и наиболее удобный способ настройки правил межсетевого экрана, который будет подробно описан далее. Помимо этого пользователь может посмотреть, как применяются правила, с помощью меню «Диагностика→Состояние МСЭ IPv4/IPv6»



SSH консоль так же предоставляет некоторые возможности управления межсетевым экраном. В частности, если пользователю не доступен веб-интерфейс с порта отличного от LAN, то он может временно отключить межсетевой экран с помощью CLI-команды:

**nu-fw stop**

**Внимание!** Отключение сетевого экрана не безопасно для сети, поэтому делать это можно только в полностью контролируемом сетевом окружении и исключительно в диагностических целях или временно, для устранения неисправностей.

Если маршрутизатор расположен на периметре сети, сетевой экран должен быть обязательно включен. Если сетевой экран включен, то все интерфейсы маршрутизатора должны принадлежать какой-нибудь зоне. В противном случае трафик интерфейсов вне зон будет

отбрасываться.

## **\*\*Настройка межсетевого экрана\*\***

### **Настройки по умолчанию**

Межсетевой экран в NETSHe имеет определенные предустановки, реализующие выход в Интернет пользователям локальной сети и запрещающие доступ снаружи в локальную сеть и к службам на устройстве под управлением NETSHe.

Все настройки выполняются с помощью веб-интерфейса в пункте меню «Сеть→ Межсетевой экран». Так выглядят настройки общие для всех зон:

Устройство работает с межсетевым экраном, на основе зон. Настроить зоны  
Пожалуйста, определите политику по умолчанию для зоны, набор дополнительных правил, NAT и порт-форвардинг, если необходимо.

Основные настройки Lan Wan Dmz Mgmt Hotspot

Разрешить межсетевой экран :

Политика по умолчанию :

Входящий трафик:  Запретить  Записывать  Исходящий трафик:  Разрешить  Записывать  Транзитный трафик:  Разрешить  Записывать

пакеты, попадающие под правило:  пакеты, попадающие под правило:  пакеты, попадающие под правило:

Защищать от атак типа SYN-flood ? :  Скорость для SYN-пакетов :  Максимальная скорость для SYN-пакетов :

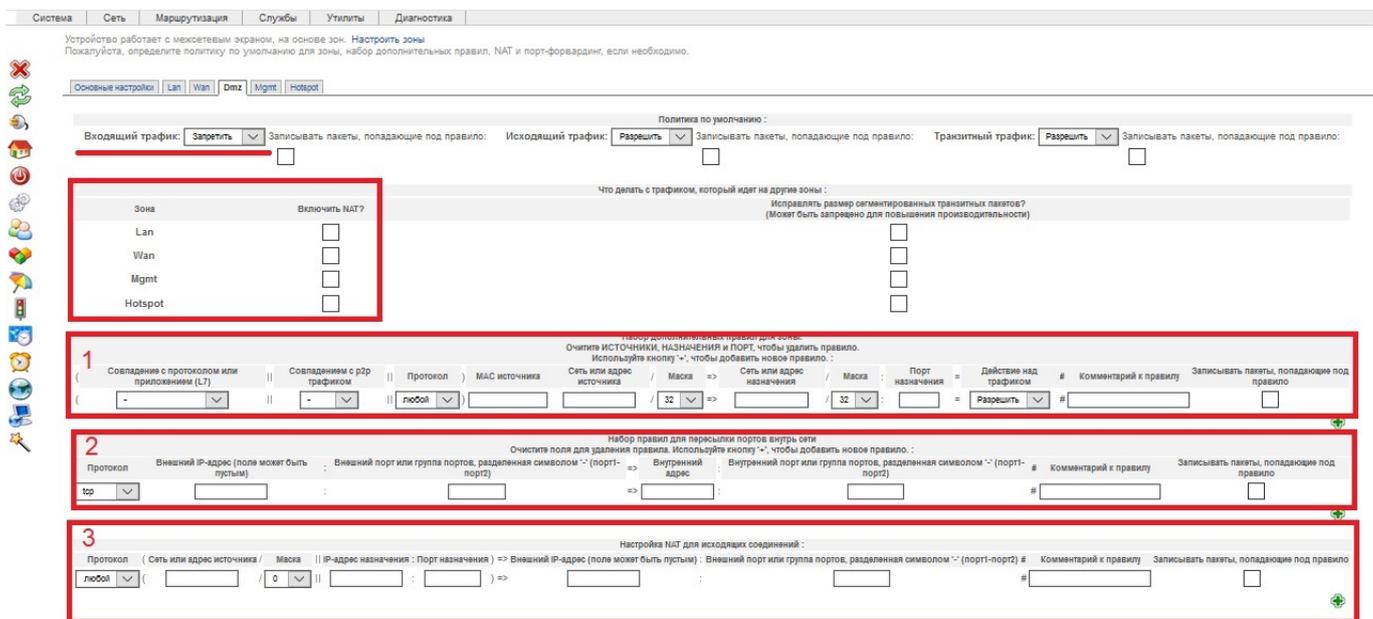
Убивать неправильные пакеты ? :   
Записывать пакеты также и в системный журнал :

Адрес netflow коллектора :   
Порт коллектора :   
Интерфейс для использования сенсором :

Перезапустить сервис(ы) после сохранения ? :  Сохранить

Настройки сетевого экрана любой зоны имеют заголовок и три секции с правилами:

1. В заголовке указано основное действие, которое следует применить к трафику, а так же зоны, в которые включен NAT из данной зоны.
2. Первая секция описывает поведение экрана для входящего трафика зоны. Эти правила разрешают или запрещают трафик в зависимости от заданных TCP/UDP портов и/или IP адресов/подсетей приемника или источника.
3. Вторая секция описывает правила проброса портов (PAT) , как правило, это применяется для входящего трафика на IP адреса внутри сети.
4. Третья секция реализует правила NAT(на базе источника).



В случае Port Forwarding или PAT (Port Address Translation), который используется для доступа к локальным IP-адресам из Интернет, настройки правил имеют следующий вид:

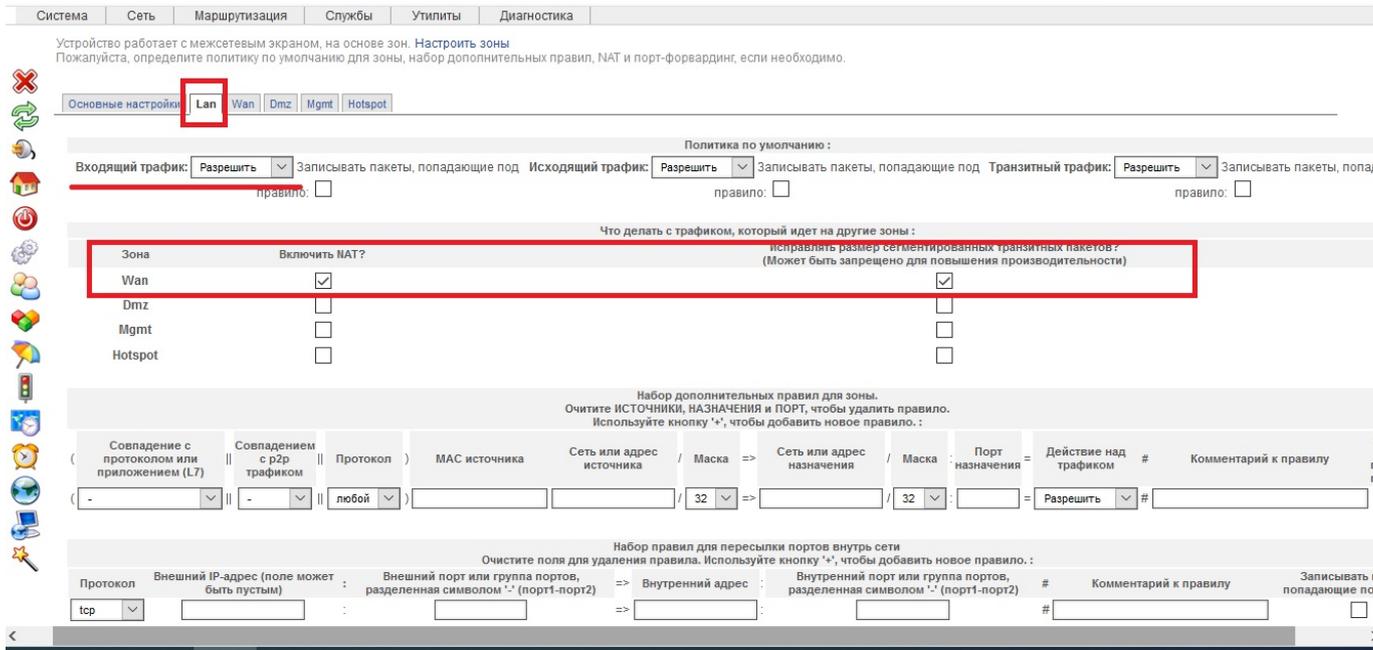
1. Протокол может быть TCP или UDP.
2. 'Внешний IP' это адрес, запрашиваемый из Интернета. Пользователь может его не указывать, тогда запрос на любой адрес будет попадать под это правило.
3. 'Внешний порт' это порт, запрашиваемый из Интернета. В общем случае он может быть случайным, тогда надо это поле в правиле не заполнять.
4. 'Внутренний адрес' это IP адрес из локальной сети, который привязан правилом к внешнему адресу WAN в целях доступности из Интернета.
5. 'Внутренний порт' это порт приложения локального сервера, на который внешний запрос и будет отправлен. Чаще всего это популярные порты TCP типа 443 для SSL.
6. 'Описание' любое понятное описание правила, объясняющее его суть и отличающее его от других правил.

Рассмотрим несколько типичных примеров настройки межсетевого экрана, во всех случаях межсетевого экран должен быть включен, это общий шаг для всех следующих примеров.

## Пример 1. Выход из локальной сети в Интернет

NAT (Network Address Translation) нужен для передачи IP-пакетов локального источника по сети Интернет, заменяя локальный адрес на публичный IP, маршрутизируемый в сети Интернет. Решается такая задача путем пересылки (проброса) портов в межсетевом экране NETSHe.

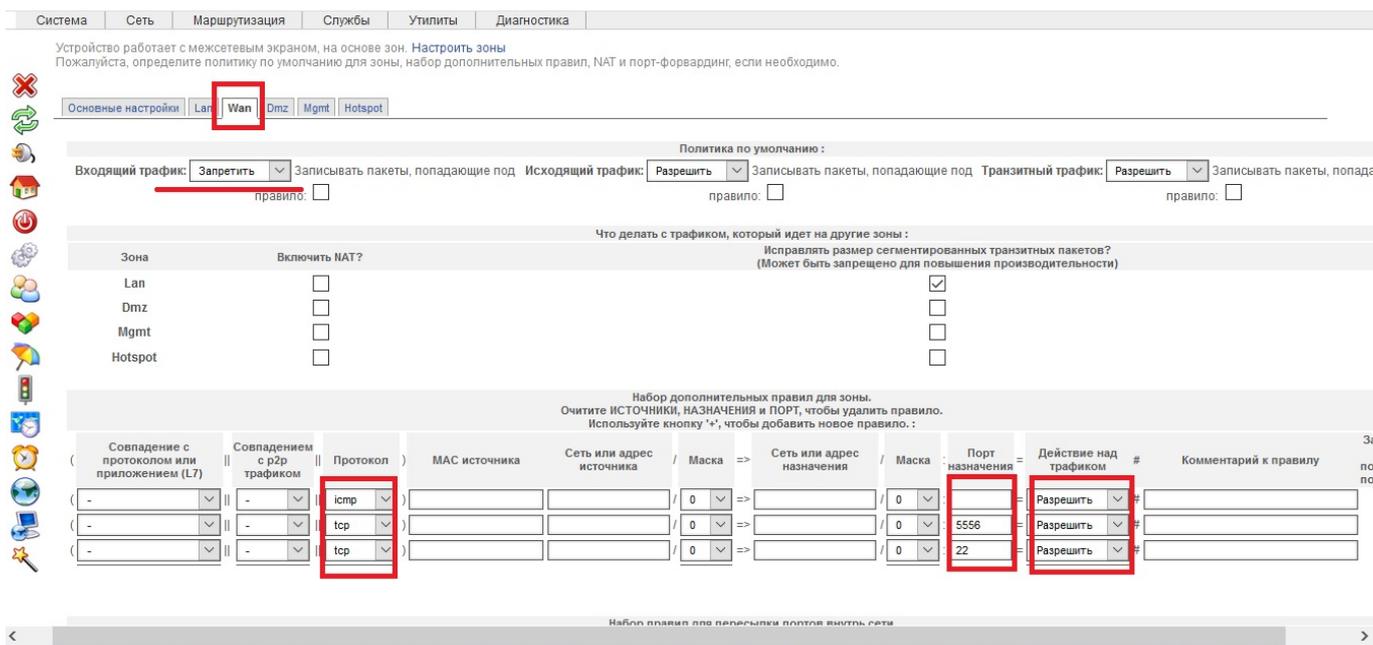
Как уже говорилось выше, эта задача реализована в системе по умолчанию. Достаточно отметить переключатель NAT напротив зоны WAN.



Так же обратите внимание, что в настройках зоны установлено глобальное правило «принимать входящий трафик», по умолчанию такая установка выполнена только для LAN.

## Пример 2. Доступ к управлению NETSHe не из локальной сети

Как говорилось выше, доступ к управлению устройством со стороны LAN открыт по умолчанию, но в ряде случаев требуется разрешить доступ к службам на устройстве под управлением NETSHe снаружи. Например, к веб-интерфейсу и SSH (последний настоятельно не рекомендуется по соображениям безопасности).



Для этого переходим в настройках зоны «WAN» (как показано на иллюстрациях выше) в разделе «Набор дополнительных правил для зоны» вводим правила, каждый раз нажимая иконку с зеленым «+»:

1. Пакеты протокола TCP на внешний порт 22 принять
2. Пакеты протокола TCP на внешний порт 5556 принять.

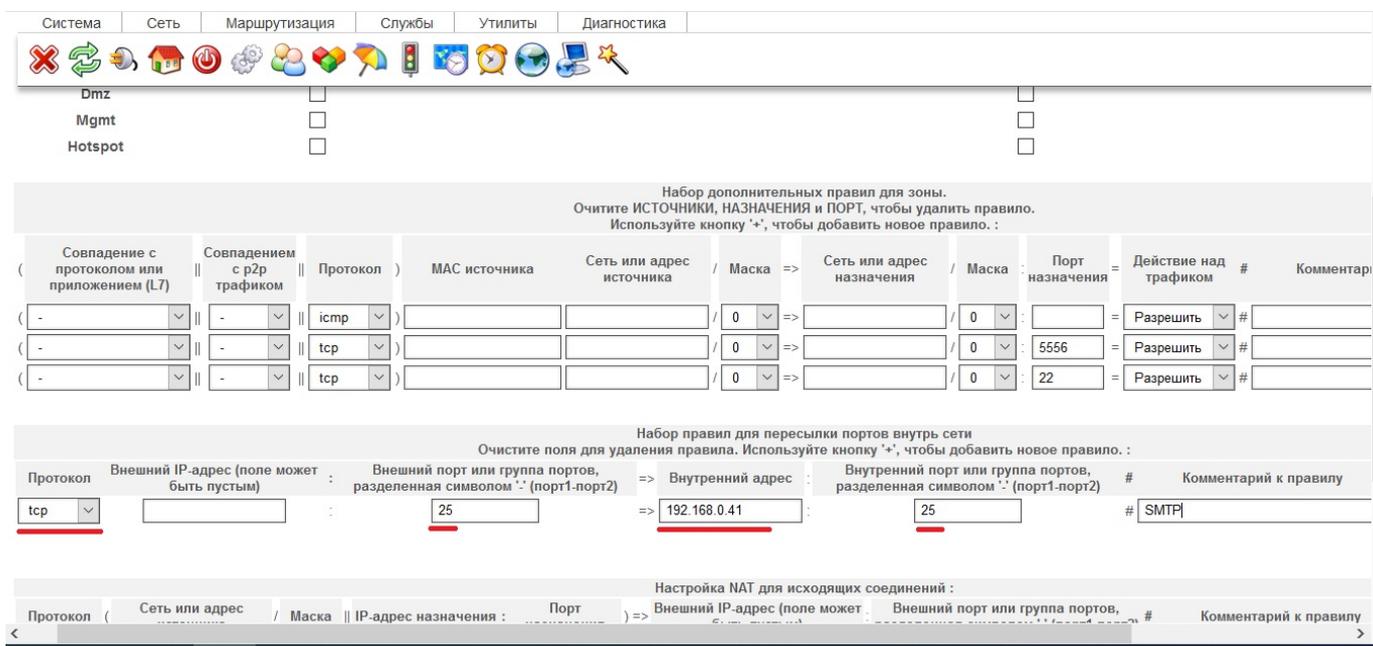
Устанавливаем галочку «Перезапустить сервис после сохранения» и нажимаем кнопку «Сохранить». Веб-интерфейс и удаленный доступ стали возможными снаружи устройства. Аналогично можно настроить доступ с порта любой зоны, на которой установлено глобальное правило «запретить входящий трафик».

### Пример 3. Проброс портов внутрь сети в межсетевом экране NETSHe

Одной из часто возникающих задач является организация доступности какого-либо сервера, расположенного внутри сети, для внешних Интернет-пользователей. Примером такой задачи может являться организация доступа к веб-серверу или получение почты корпоративным почтовым сервером.

Выберем зону «WAN» в межсетевом экране и в разделе «Набор правил для пересылки портов внутрь сети» введем:

1. порт на внешних интерфейсах, что нужно пробросить внутрь сети. (25 протокол SMTP),
2. протокол, пакеты которого требуется пересылать во внутреннюю сеть (TCP),
3. IP-адрес расположенного во внутренней сети компьютера (например, 192.168.0.41),
4. порт этого внутреннего компьютера, на который будет выполняться пересылка (25).



Устанавливаем галочку «Перезапустить сервис после сохранения» и нажимаем кнопку «Сохранить». Введенное нами правило сохраняется в списке правил для пересылки, и при поступлении TCP-пакета на 25 порт любого из наших внешних интерфейсов, такой пакет будет перенаправлен на TCP 25 порт компьютера с адресом 192.168.0.41.

Легко догадаться, что приведенный пример относится к установке внутри сети SMTP-сервера и организации получения им почты извне. Аналогично можно сделать пересылку TCP 80 и 443 для веб-сервера, TCP 20 и 21 для сервера FTP и даже замаскировать доступ к широко

распространенным RDP (TCP 3389) и SSH (TCP 22) со стороны Интернет.

Система | Сеть | Маршрутизация | Службы | Утилиты | Диагностика

Dmz
  Mgmt
  Hotspot

Набор дополнительных правил для зоны.  
 Очитите ИСТОЧНИКИ, НАЗНАЧЕНИЯ и ПОРТ, чтобы удалить правило.  
 Используйте кнопку '+', чтобы добавить новое правило. :

Совпадение с протоколом или приложением (L7)	Совпадением с p2p трафиком	Протокол	MAC источника	Сеть или адрес источника / Маска	=>	Сеть или адрес назначения / Маска	Порт назначения	=	Действие над трафиком	#	Комментар
-	-	icmp		/ 0	=>			=	Разрешить	#	
-	-	tcp		/ 0	=>		5556	=	Разрешить	#	
-	-	tcp		/ 0	=>		22	=	Разрешить	#	

Набор правил для пересылки портов внутрь сети  
 Очистите поля для удаления правила. Используйте кнопку '+', чтобы добавить новое правило. :

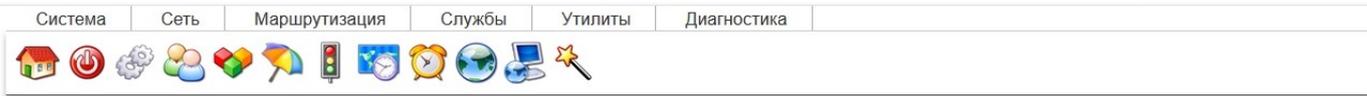
Протокол	Внешний IP-адрес (поле может быть пустым)	:	Внешний порт или группа портов, разделенная символом ':' (порт1-порт2)	=>	Внутренний адрес	:	Внутренний порт или группа портов, разделенная символом ':' (порт1-порт2)	#	Комментарий к правилу
tcp		:	25	=>	192.168.0.41	:	25	#	SMTP
tcp		:	33389	=>	192.168.0.33	:	3389	#	smart RDP

Настройка NAT для исходящих соединений :

**Внимание!** Подмена TCP/UDP порта при трансляции адресов не может рассматриваться как защита от сетевых угроз. Для полноценной защиты следует не менять порт, а использовать предназначенные для этого антивирусные, криптографические средства и пр.

## Фильтрация Ethernet-кадров

Система NETSHe имеет средства для фильтрации трафика на уровне Ethernet-кадров на сетевых мостах, доступные в меню «Сеть→ Фильтрация Ethernet кадров».



Вы можете настроить фильтрацию здесь

br0

Разрешить фильтрацию ? :

Политика по умолчанию для цепочки (INPUT)	Запретить
Применить обратную политику к соответствиям ?	IP v4 <input type="checkbox"/> IP v6 <input type="checkbox"/> ARP <input type="checkbox"/> 802.3 <input type="checkbox"/>
Политика по умолчанию для цепочки (FORWARD)	Запретить
Применить обратную политику к соответствиям ?	IP v4 <input type="checkbox"/> IP v6 <input type="checkbox"/> ARP <input type="checkbox"/> 802.3 <input type="checkbox"/>
Политика по умолчанию для цепочки (OUTPUT)	Запретить
Применить обратную политику к соответствиям ?	IP v4 <input type="checkbox"/> IP v6 <input type="checkbox"/> ARP <input type="checkbox"/> 802.3 <input type="checkbox"/>

Введите правила для отбрасывания Ethernet-кадров с некоторых MAC-адресов. Используйте кнопку (+), чтобы добавить новое правило. Очистите поля для удаления правила

Введите исходный MAC-адрес и входящий интерфейс (Пустой интерфейс означает все интерфейсы в сетевом мосту) :

Введите правила для пересылки Ethernet-кадров с протоколом IPv4 на другой интерфейс. Используйте кнопку (+), чтобы добавить новое правило. Очистите поля для удаления правила

Введите IP-адрес назначений, маску сети, MAC-назначения и входной интерфейс( пустое значение эквивалентно всем интерфейсам, объединенным в мост)	IP-адрес назначения / Маска	MAC-адрес назначения	Интерфейс
	<input type="text"/> / <input type="text"/>	<input type="text"/>	<input type="text"/>

Введите правила для пересылки Ethernet-кадров с протоколом IPv6 на другой интерфейс. Используйте кнопку (+), чтобы добавить новое правило. Очистите поля для удаления правила

Введите IP-адрес назначений, MAC-назначения и входной интерфейс( пустое значение эквивалентно всем интерфейсам, объединенным в мост)	IP-адрес назначения	MAC-адрес назначения	Интерфейс
	<input type="text"/>	<input type="text"/>	<input type="text"/>

Вы можете включить BROUTER. Смотрите руководство по ebttables относительно BROUTER

Включить BROUTER на выбранных интерфейсах ?	eth0.1 <input type="checkbox"/>
	wlan0 <input type="checkbox"/>

Вы можете ввести правила для ebttables вручную

Пожалуйста, введите команду для ebttables (Подобно -A INPUT -p ip -j DROP). Используйте кнопку (+), чтобы добавить новое правило. Очистите поле для удаления правила. :

Разрешить сервис(ы) после сохранения ? :  Сохранить

**Внимание!** Вы не можете использовать данную возможность, если у Вас в системе не определен хотя бы один сетевой мост.

Функция фильтрации трафика будет применяться только к трафику, попадающему на данный сетевой мост, который указан в настройках. Если в системе определено несколько мостов, настройки каждого из них будут располагаться на своей вкладке.

Кроме фильтрации, доступны функции перенаправления кадров с IPv4 и (или) IPv6 пакетами на другой Ethernet интерфейс, создания brouter.

Параметрами для настройки фильтрации являются:

1. Политики по умолчанию;
2. тип Ethernet-кадров (например, 802.3 фрейм);
3. содержимое Ethernet-кадров (протокол IPv4 либо IPv6, ARP запрос);

4. список MAC-адресов и (или) интерфейсов, для которых кадры следует отбросить;
5. Список правил (адрес назначения/маска/MAC-адрес) для перенаправления IP-пакетов на другие интерфейсы;
6. список интерфейсов для создания brouter. (По вопросам создания, настройки и использования brouter смотрите документацию по утилите *ebtables*.)

Данный функционал может быть использован как в целях безопасности (заблокировать трафик устройств с определенными MAC-адресами), так и для решения сетевых проблем (проксирование широковещательного трафика ARP между сегментами сети). Задачи эти довольно специфичны, нет необходимости подробно их описывать в руководстве, обращенному к широкому кругу пользователей. Полный список применений этого и других свойств можно узнать в техподдержке на сайте <http://www.netshe-lab.ru>

From:  
<http://docs.netshe-lab.ru/> - Документация по NETSHe

Permanent link:  
[http://docs.netshe-lab.ru/doku.php?id=%D0%B3%D0%BB%D0%B0%D0%B2%D0%B0\\_5\\_-\\_%D0%BC%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9\\_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD](http://docs.netshe-lab.ru/doku.php?id=%D0%B3%D0%BB%D0%B0%D0%B2%D0%B0_5_-_%D0%BC%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD)

Last update: 2020/07/17 11:44

