Практическое использование функционала Transparent Firewall

Solution.
Production.
Warranty.

MikroTik

официальный дистрибьютор

www.spw.ru

Об авторе

- Илья Князев. г. Санкт-Петербург, Россия.
- Mikrotik Certified Trainer [TR0309]
- MTCNA, MTCTCE, MTCWE, MTCUME, MTCRE, MTCINE, MTCIPv6E
- Технический директор SPW.RU

Для связи

- E-Mail: ikn@spw.ru
- Skype: Ilya.Knyazev
- WWW: https://spw.ru
- Forum: https://spw.ru/forum

Введение

- Одной из наиболее часто встречающихся задач является фильтрация и/или изменение заголовка пакета при помощи функционала предоставляемого IP Firewall маршрутизатора.

- Стандартный файрволл работает на третьем уровне модели OSI. При этом маршрутизатор является IP-шлюзом для проходящих через него пакетов.

- Иногда нам надо управлять трафиком на уровне L2

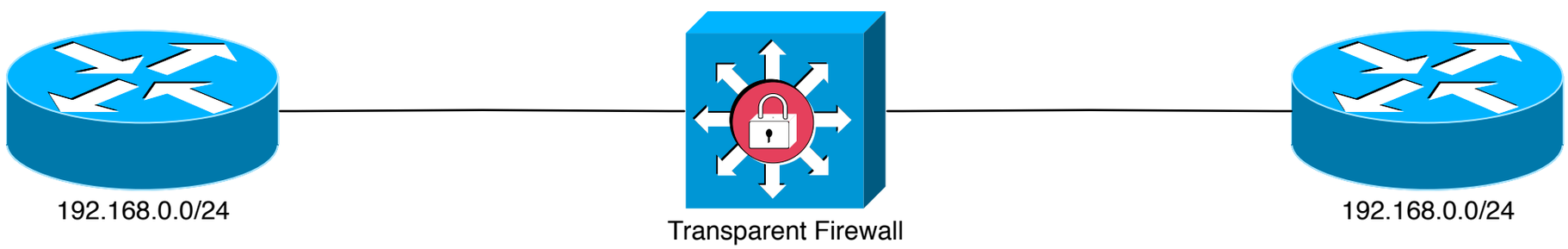
- В этой презентации будут рассмотрены как особенности реализации, так и примеры реальных конфигураций

Принцип работы

- Transparent FIrewall фильтрует трафик проходящий через маршрутизатор, как через L2-устройство.

- Для этого необходимо чтобы ethernet-порты, между которыми планируется обрабатывать трафик были объединены в Bridge.

- Маршрутизатор при этом может не иметь IP-адреса.



Принцип работы

- Как только вы объединили порты в Bridge, у вас появляется возможность пользоваться Bridge NAT и Bridge Filter

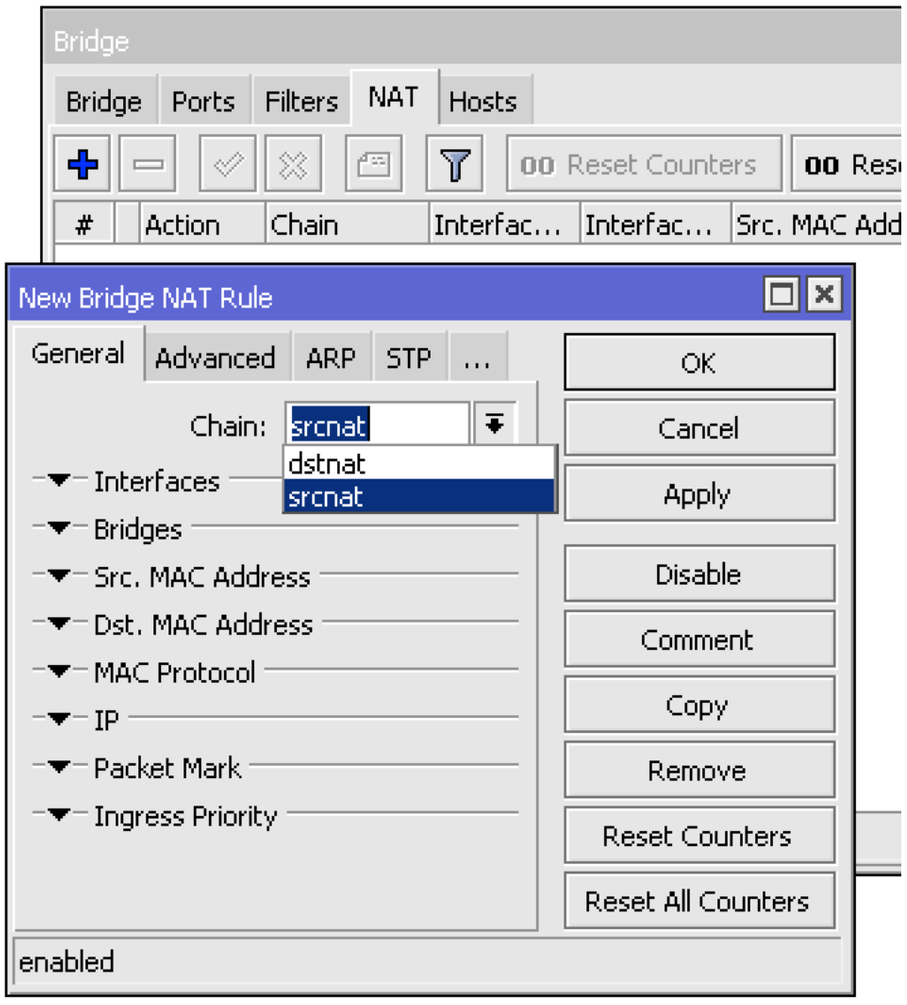
- Bridge NAT позволяет изменять MAC-адреса отправителя и получателя ethernet-фрейма

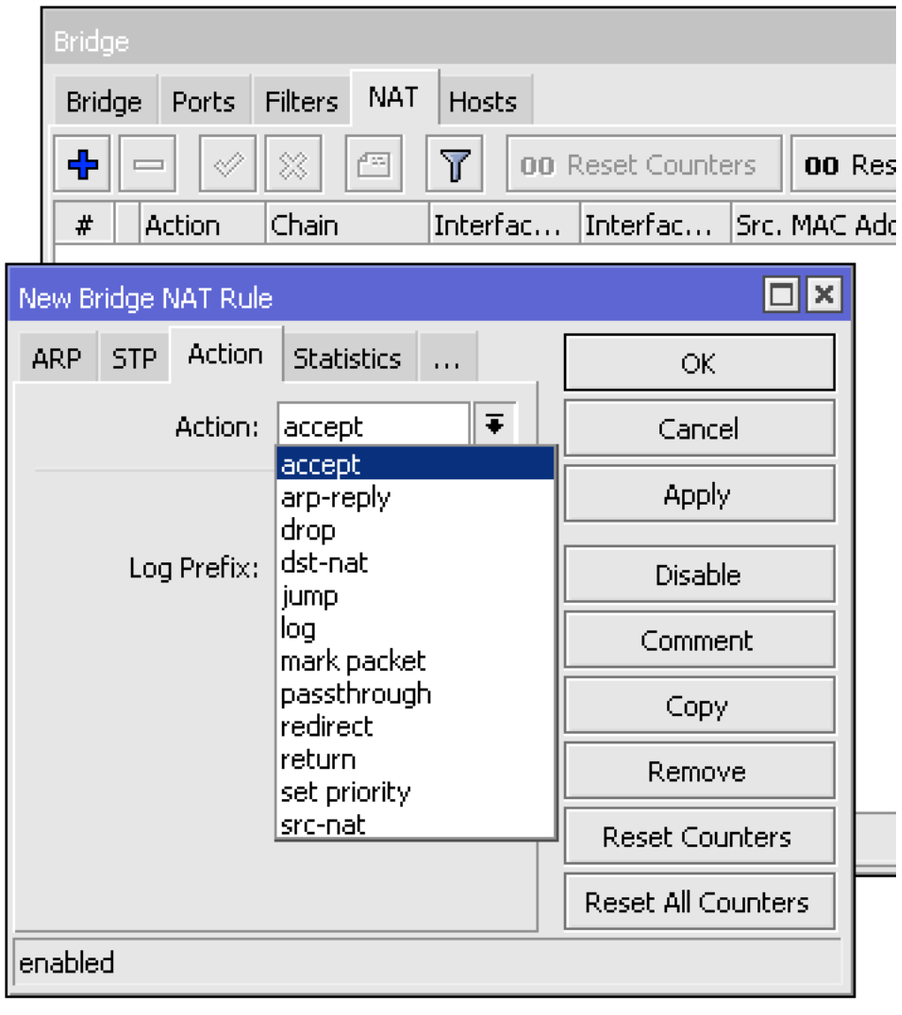
- Bridge Filter позволяет фильтровать пакеты основываясь на заголовке ethernet-фрейма

Bridge NAT

- Существует две цепочки NAT.
- SRC-NAT меняет MAC-адрес отправителя фрейма. Как правило используется для маскировки реального MAC-адреса отправителя фрейма
- DST-NAT меняет MAC-адрес получателя пакета. В основном используется для того, чтобы направить фрейм на устройство отличное от того, куда он должен был попасть изначально.

Bridge NAT

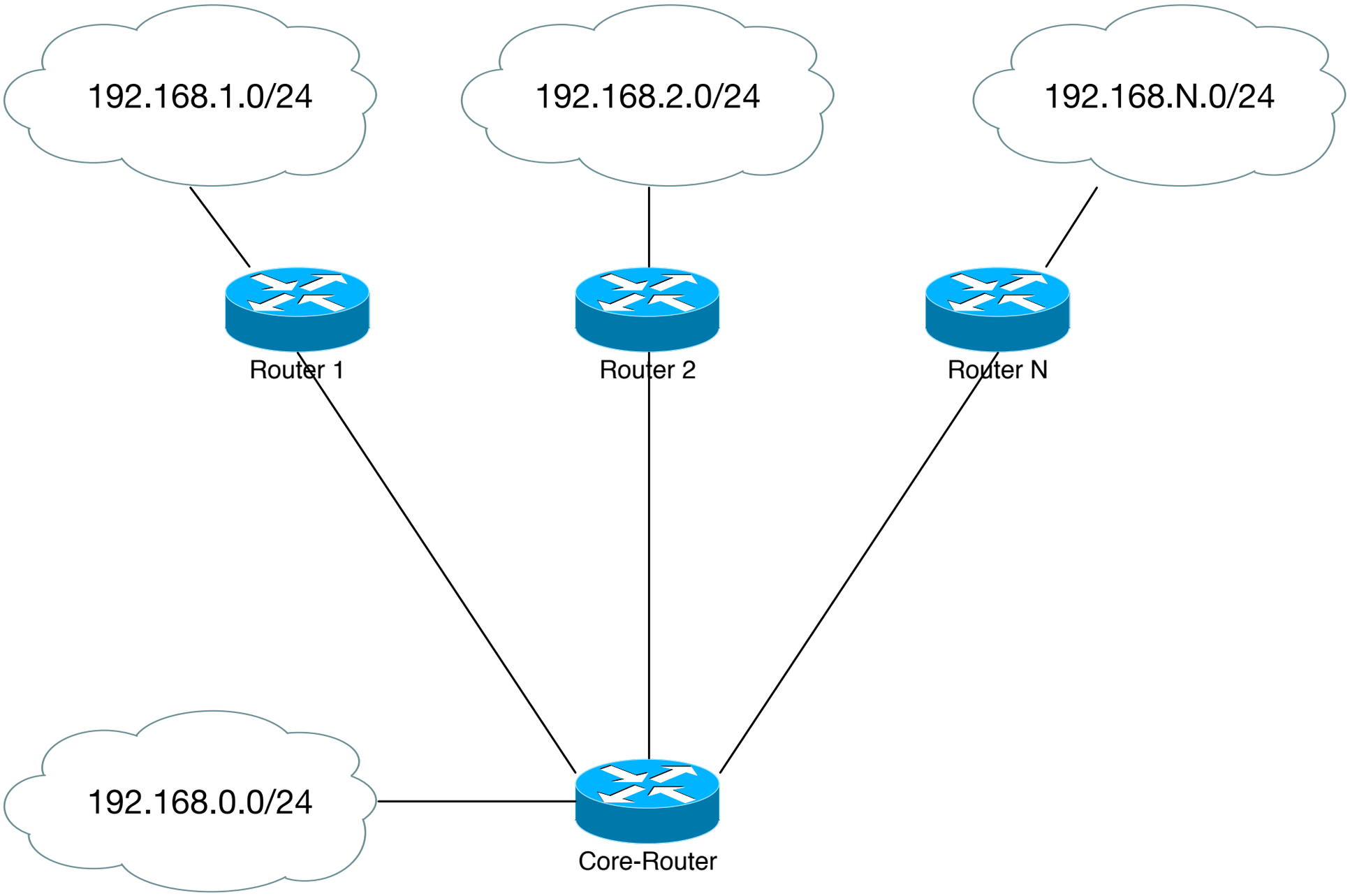

Bridge
Bridge
Ports
Filters
NAT
Hosts
00 Reset Counters
00 Res
#
Action
Chain
Interfac...
Interfac...
Src. MAC Add
New Bridge NAT Rule
General
Advanced
ARP
STP
...
Chain:
srcnat
dstnat
srcnat
Interfaces
Bridges
Src. MAC Address
Dst. MAC Address
MAC Protocol
IP
Packet Mark
Ingress Priority
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled


Bridge
Bridge
Ports
Filters
NAT
Hosts
00 Reset Counters
00 Res
#
Action
Chain
Interfac...
Interfac...
Src. MAC Add
New Bridge NAT Rule
ARP
STP
Action
Statistics
...
Action:
accept
Log Prefix:
accept
arp-reply
drop
dst-nat
jump
log
mark packet
passthrough
redirect
return
set priority
src-nat
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled

Bridge NAT

- Представьте себе что вы устроились на работу в большую компанию.
- В сети компании есть более ста филиалов подключенных к центральному маршрутизатору.
- Предыдущий системный администратор недоступен.
- Вы не знаете пароля ни от одного из маршрутизаторов
- Вам необходимо вернуть сеть в управляемое состояние
- Используется много статической адресации. Подмена адреса шлюза не подходит

Bridge NAT


192.168.1.0/24
192.168.2.0/24
192.168.N.0/24
Router 1
Router 2
Router N
192.168.0.0/24
Core-Router

Bridge NAT

- Для восстановления управления сетью сделаем следующее

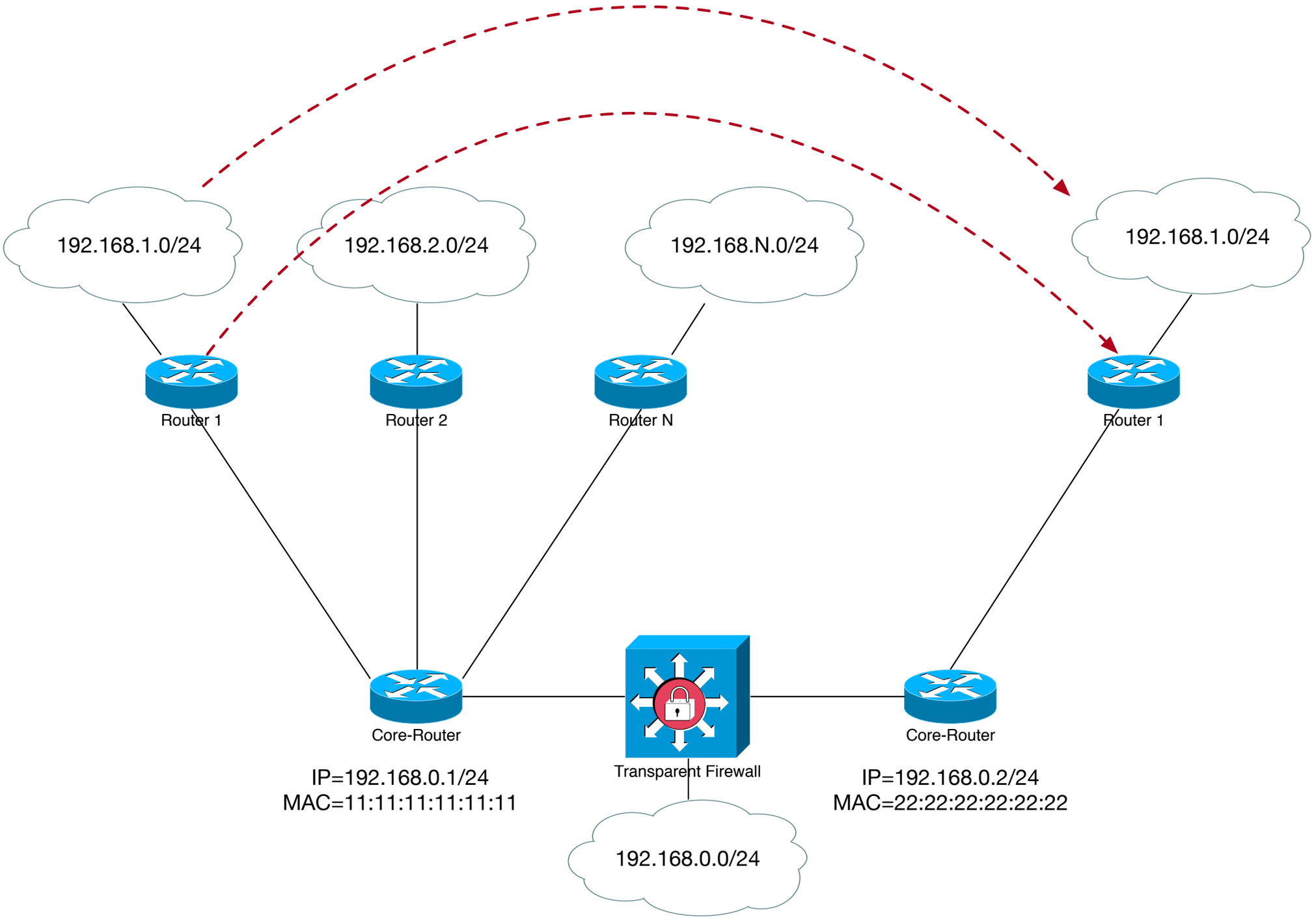
- Добавим в сеть новый Core-Router

- Добавим Transparent Firewall расположив его между сетью 192.168.0.0/24, Старым и новым Core-Routers

- Будем по одному маршрутизатору подключать со сбросом конфигурации на новое ядро

- Для корректного прохождения пакетов одновременно создавая правило DST-NAT в бридже

Bridge NAT


192.168.1.0/24
192.168.2.0/24
192.168.N.0/24
192.168.1.0/24
Router 1
Router 2
Router N
Router 1
Core-Router
Transparent Firewall
Core-Router
IP=192.168.0.1/24
MAC=11:11:11:11:11:11
IP=192.168.0.2/24
MAC=22:22:22:22:22:22
192.168.0.0/24

Bridge NAT

- Теперь необходимо настроить transparent Firewall так, чтобы он пакет идущий на подсеть 192.168.1.0/24 переадресовывал на новый маршрутизатор

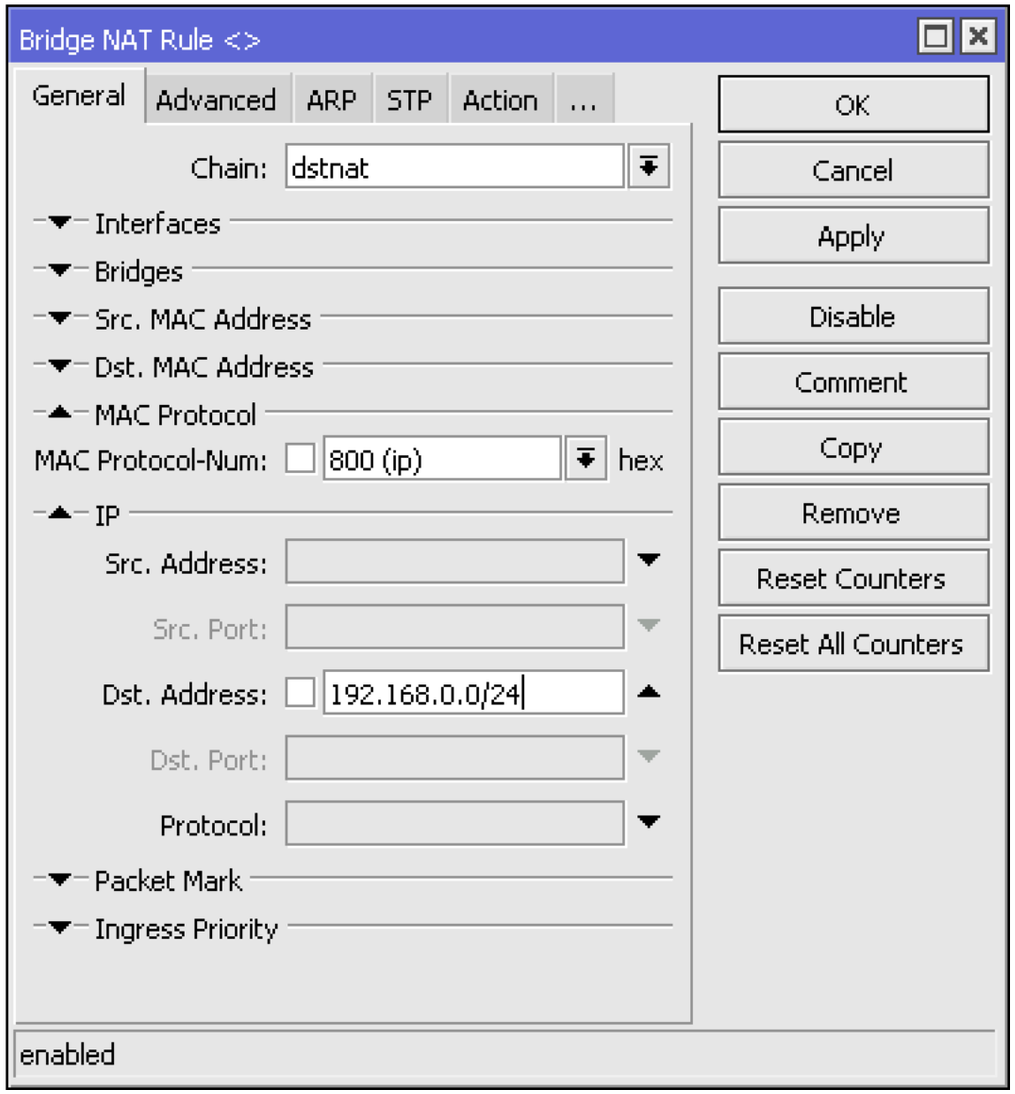
- При этом все должно происходить прозрачно для трафика.

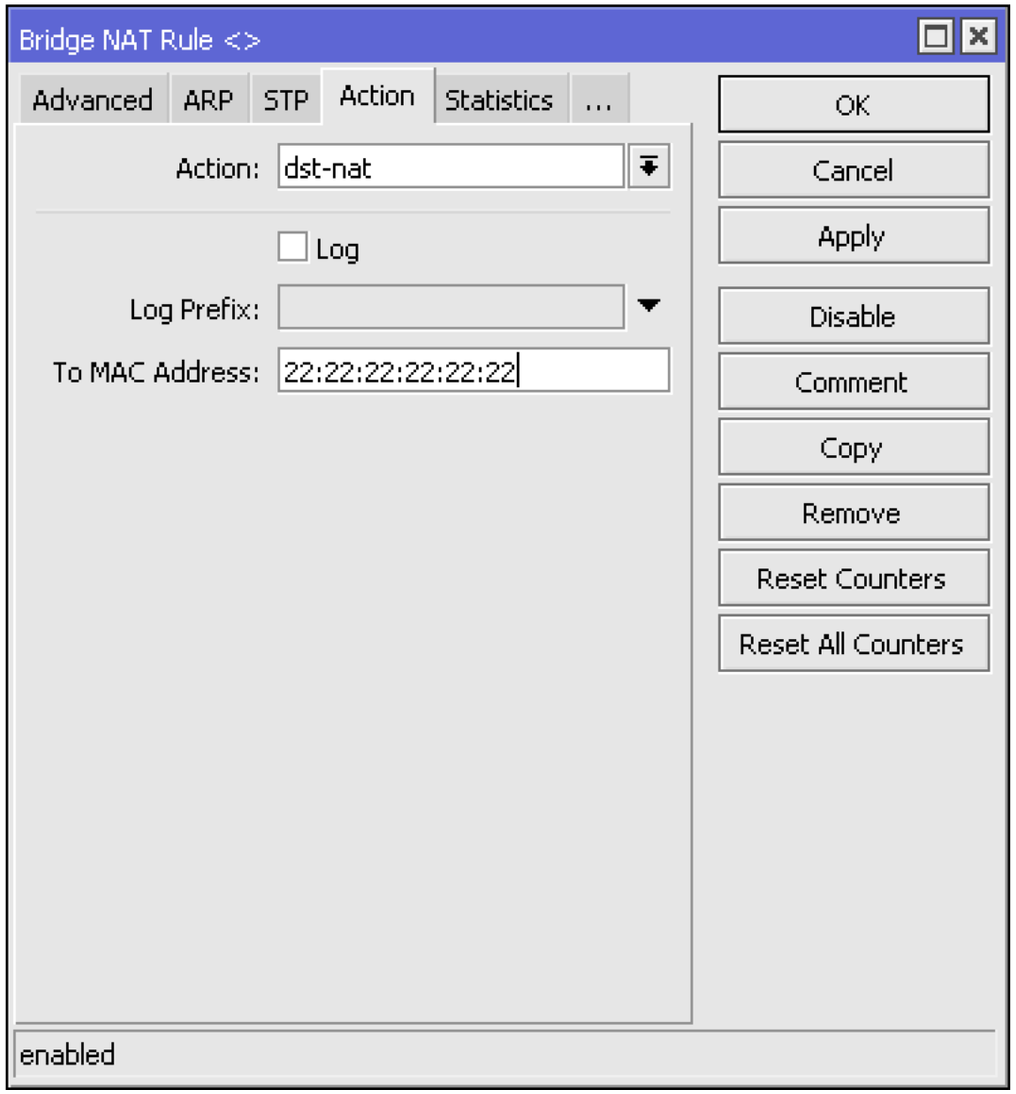
- Вот это правило:

```
/interface bridge nat
add action=dst-nat chain=dstnat \
dst-address=192.168.0.0/24 mac-protocol=ip \
to-dst-mac-address=22:22:22:22:22:22
```

Bridge NAT

- Или оно же в Winbox





Bridge Filter

- Работает на уровне L2
- Позволяет фильтровать пакеты основываясь на заголовке L2 фрейма
- Наиболее часто используется для установки поля приоритета фрейма, которое затем может использоваться в протоколе WMM беспроводного интерфейса
- Так же позволяет делать простые правила фильтрации IP

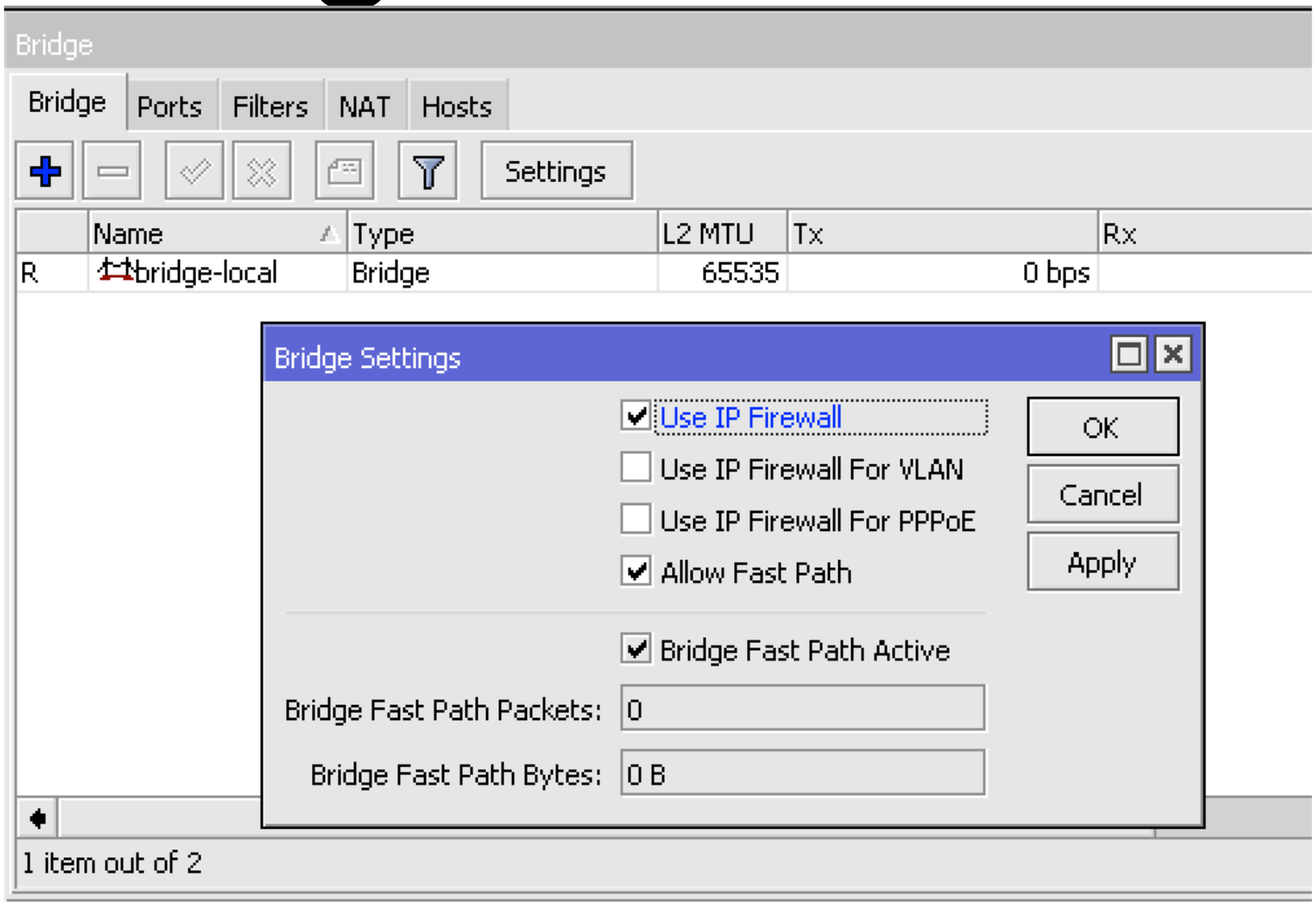
Bridge+IP Firewall

- Если вам недостаточно функционала Bridge FIlter, вы можете расширить его, при помощи включения опции use-ip-firewall.

- Тогда трафик проходящий через Bridge, так же будет попадать в IP-Firewall.

- Это позволяет значительно расширить функционал Transparent Firewall.

Bridge+IP Firewall



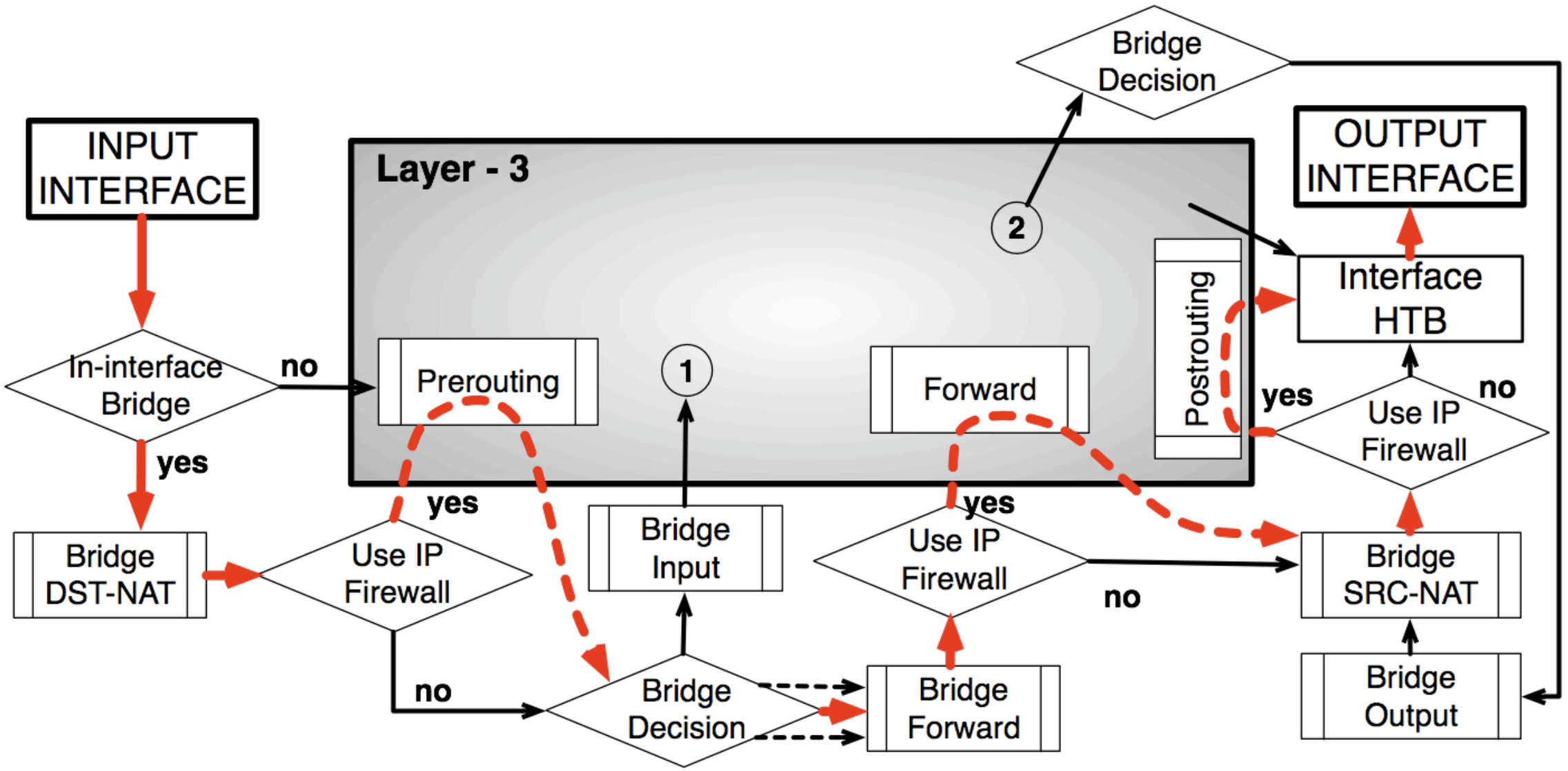

```
/interface bridge settings set use-ip-firewall=yes
```

Bridge+IP Firewall

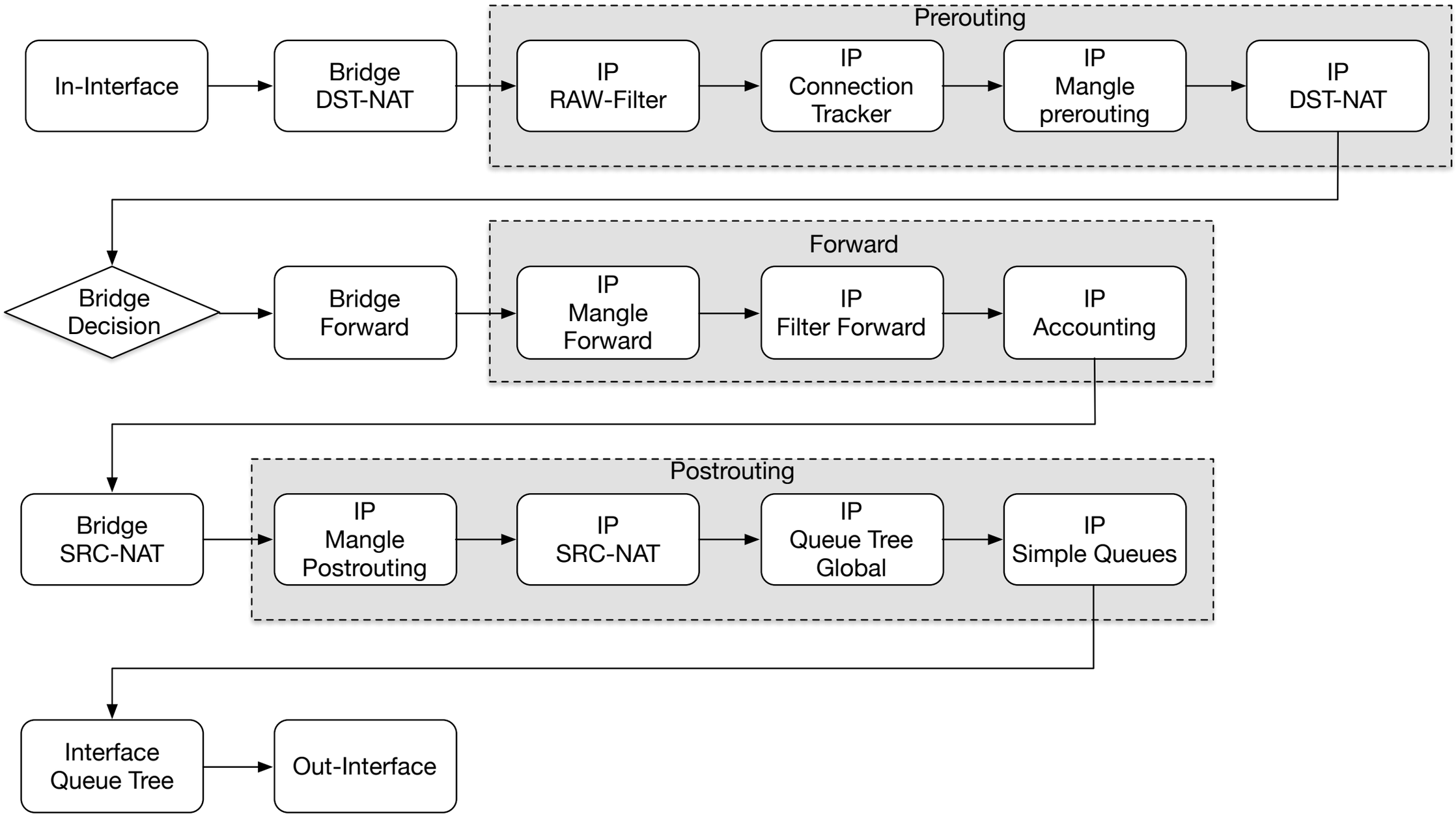
- Включение IP-Firewall происходит на всех Bridge в маршрутизаторе. Нет возможности включить эту опцию только для одного, конкретного Bridge

- После включения этой опции меняется порядок прохождения трафика внутри Bridge

Bridge+IP Firewall



Bridge+IP Firewall

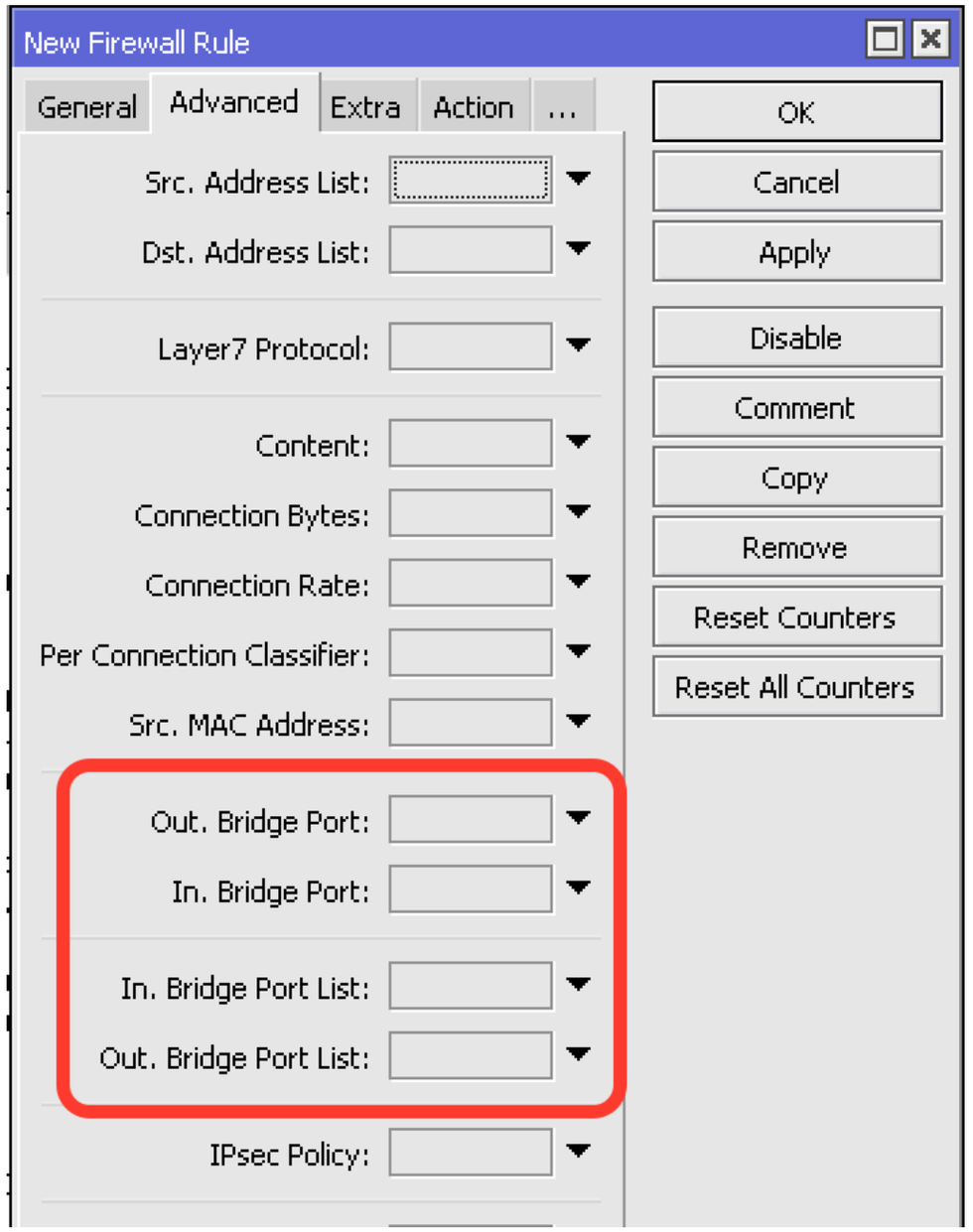


Bridge+IP Firewall

- Включение режима use-ip-firewall увеличивает возможности обработки трафика на уровне L2
- Становится доступен весь функционал IP Firewall и Очереди.
- Таким образом мы можем работать с фильтрацией пакетов, маркировкой пакетов NAT и очередями

Bridge+IP Firewall

- В IP Firewall, если пакет пришел на обработку из Bridge, можно пользоваться свойствами in-bridge-port, out-bridge-port, in-bridge-port-list и out-bridge-port-list для определения трафика проходящего между конкретными портами Bridge



Bridge+IP Firewall

- В сети Transparent FIrewall ставится между двумя сетевыми устройствами, трафик между которыми необходимо обработать.

- Наиболее часто используется с целями фильтрации трафика между узлами внутри одного L2 сегмента или с целью диагностики.

- Далее рассмотрим примеры задач

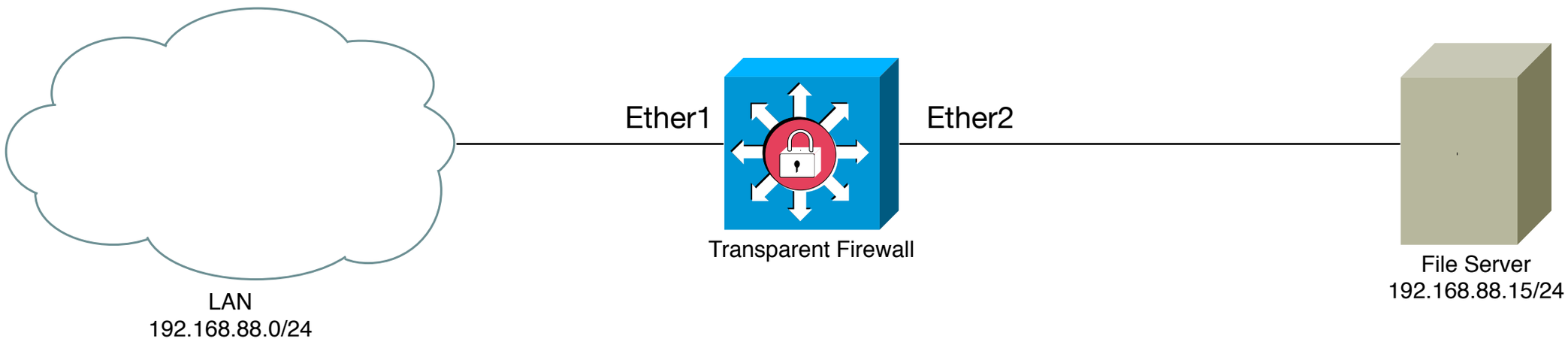
Примеры задач

- Базовые настройки RouterOS для всех задач
- Порты Ether1 и Ether2 объединены в Bridge-Local
- Включено использование IP Firewall (use-ip-firewall=yes)
- Маршрутизатор имеет дополнительный интерфейс с выходом в Интернет (LTE, 3G, WiFi, Ether3…) (в задачах, где это необходимо)

QoS

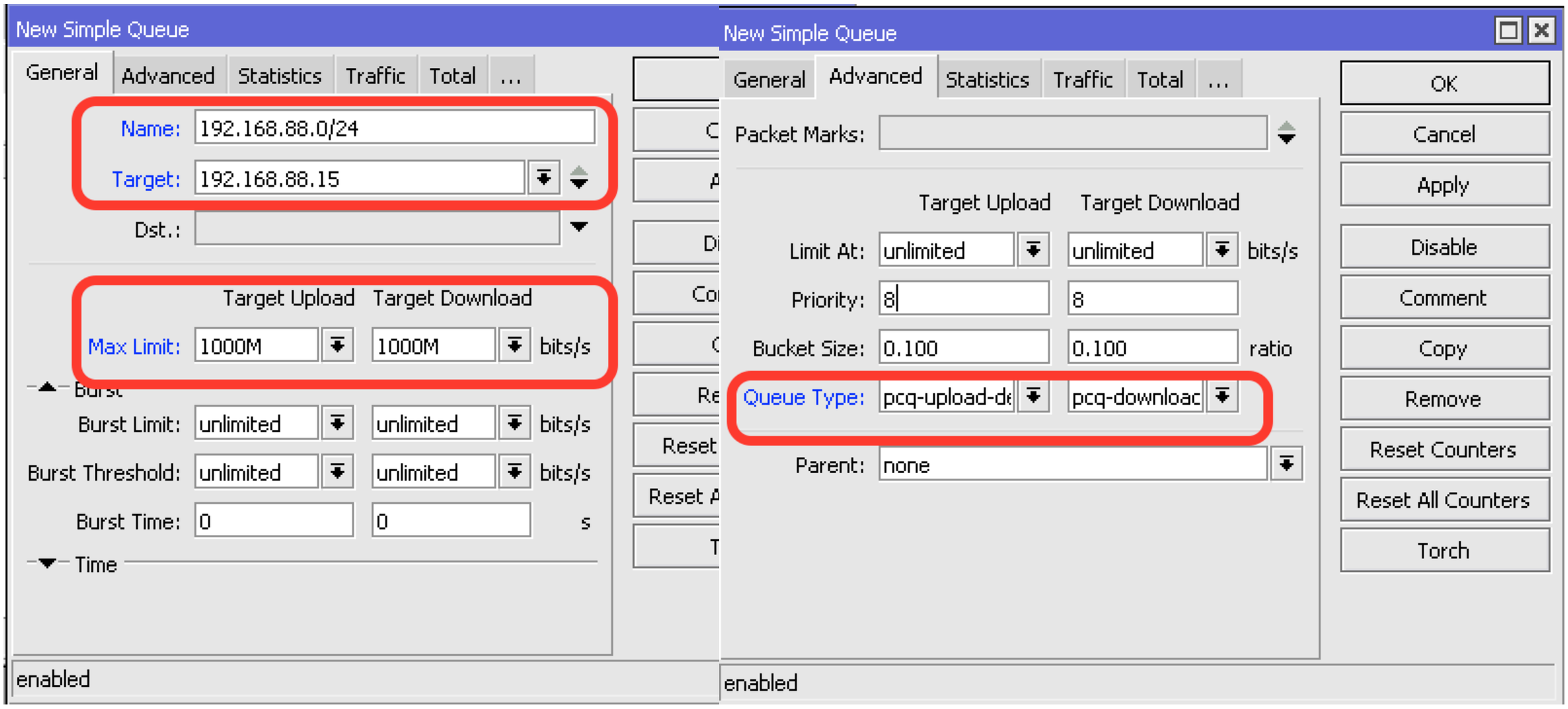
- Необходимо обеспечить пропорциональное распределение нагрузки на файловый сервер организации. Подключенного с порту Ether2 маршрутизатора

- Для этого мы будем использовать Transparent Firewall и Simple Queue типа PCQ

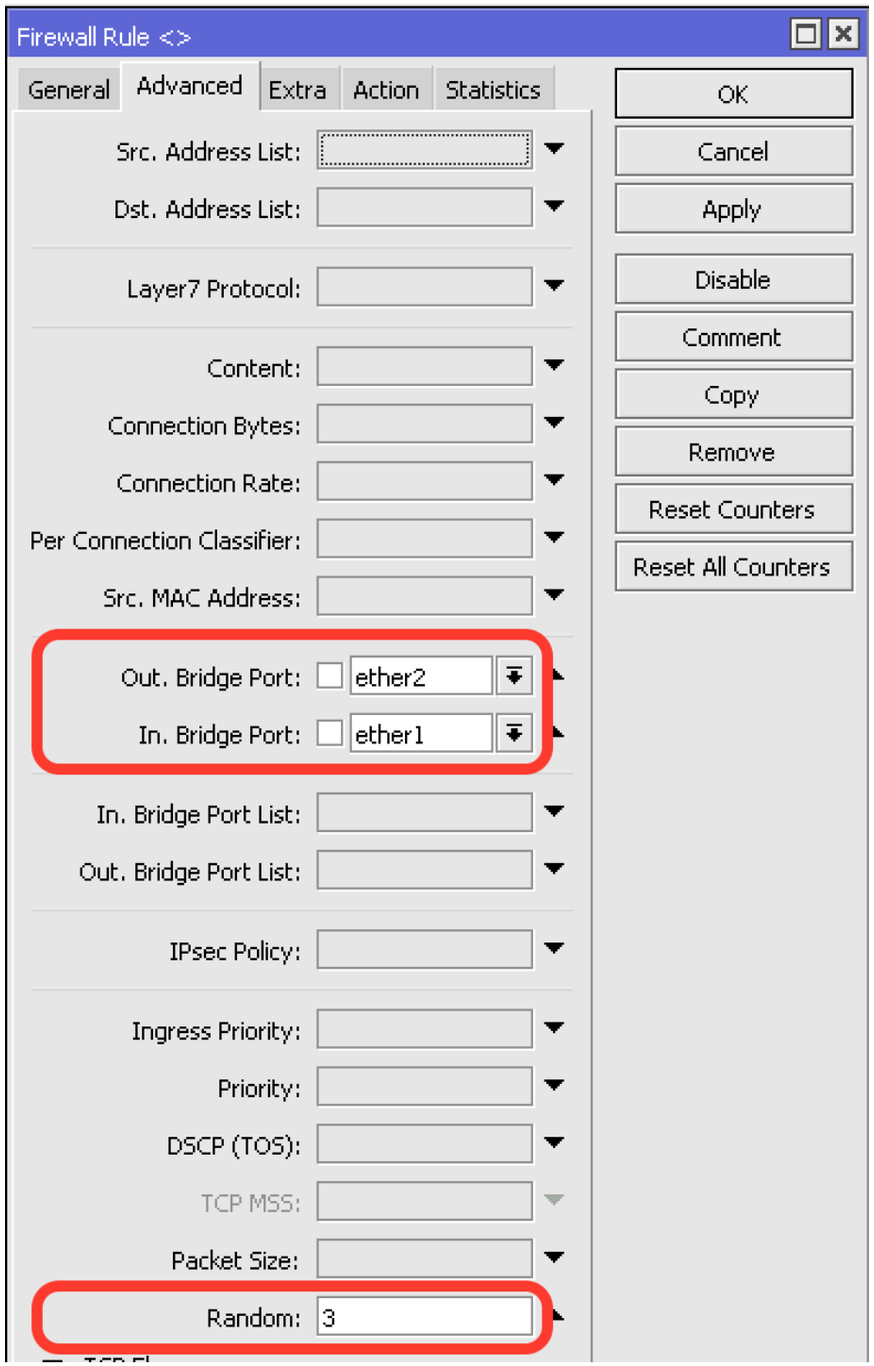


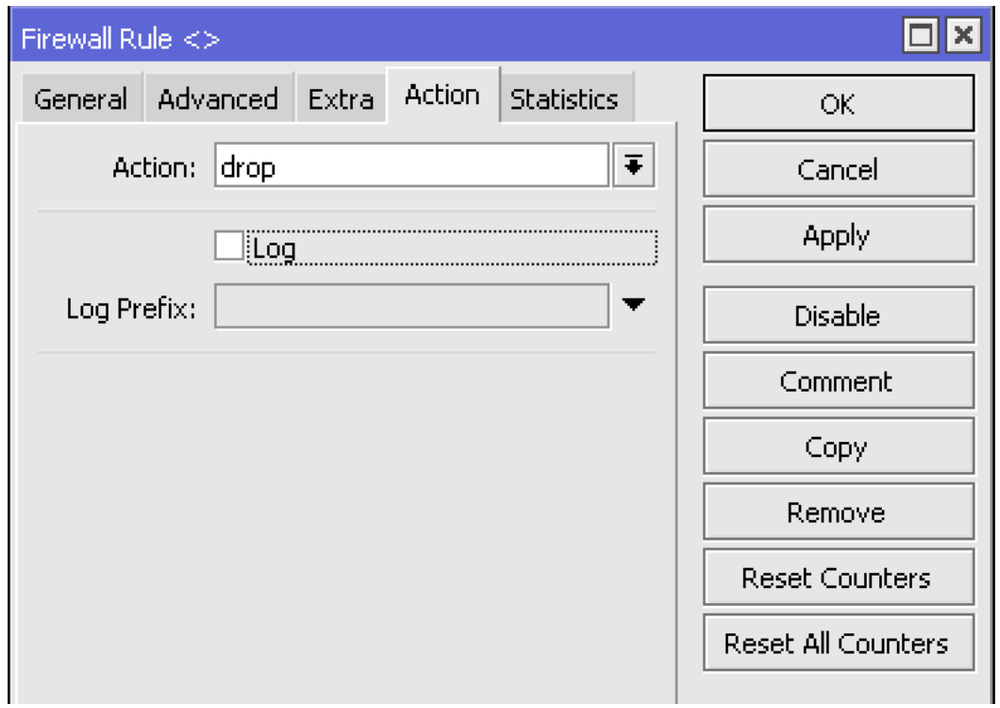
QoS

- Все что нужно для этого сделать - настроить соответствующую Simple Queue

- ```
  /queue simple
  add max-limit=1G/1G name=192.168.88.0/24 queue=\
  pcq-upload-default/pcq-download-default \
  target=192.168.88.15/32
  ```
  ```

QoS


New Simple Queue
General
Advanced
Statistics
Traffic
Total
...
Name: 192.168.88.0/24
Target: 192.168.88.15
Dst.:
Target Upload
Target Download
Max Limit: 1000M 1000M bits/s
Burst
Burst Limit: unlimited unlimited bits/s
Burst Threshold: unlimited unlimited bits/s
Burst Time: 0 0 s
Time
enabled
New Simple Queue
General
Advanced
Statistics
Traffic
Total
...
Packet Marks:
Target Upload
Target Download
Limit At: unlimited unlimited bits/s
Priority: 8 8
Bucket Size: 0.100 0.100 ratio
Queue Type: pcq-upload-de pcq-downloac
Parent: none
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch
enabled

Filter

- Необходимо протестировать работу файл-сервера из предыдущей задачи при 3% потерь пакетов в сети.

- Пакеты «теряются» только в направлении Ether1->Ether2

- Для этого необходимо создать соответствующее правило в /IP Firewall Filter

- ```
  /ip firewall filter
  add action=drop chain=forward in-bridge-port=ether1\
  out-bridge-port=ether2 random=3
  ```
  ```

Filter


Firewall Rule <>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Src. Address List:
Dst. Address List:
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
ether2
In. Bridge Port:
ether1
In. Bridge Port List:
Out. Bridge Port List:
IPsec Policy:
Ingress Priority:
Priority:
DSCP (TOS):
TCP MSS:
Packet Size:
Random:
3


Firewall Rule <>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Action:
drop
Log
Log Prefix:

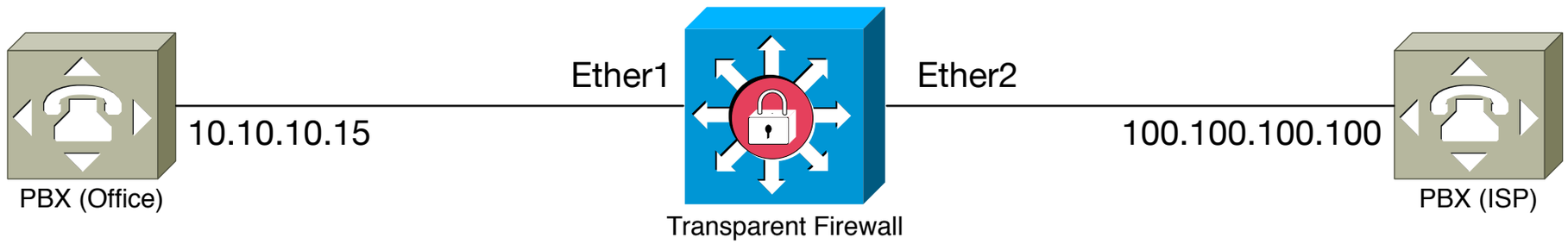
NAT

- У клиента есть IP-PBX.
- Она подключена по протоколу SIP к оператору связи
- Один из операторов принимает регистрацию транка только с порта 5060
- В IP-PBX нет возможности указать исходящий порт

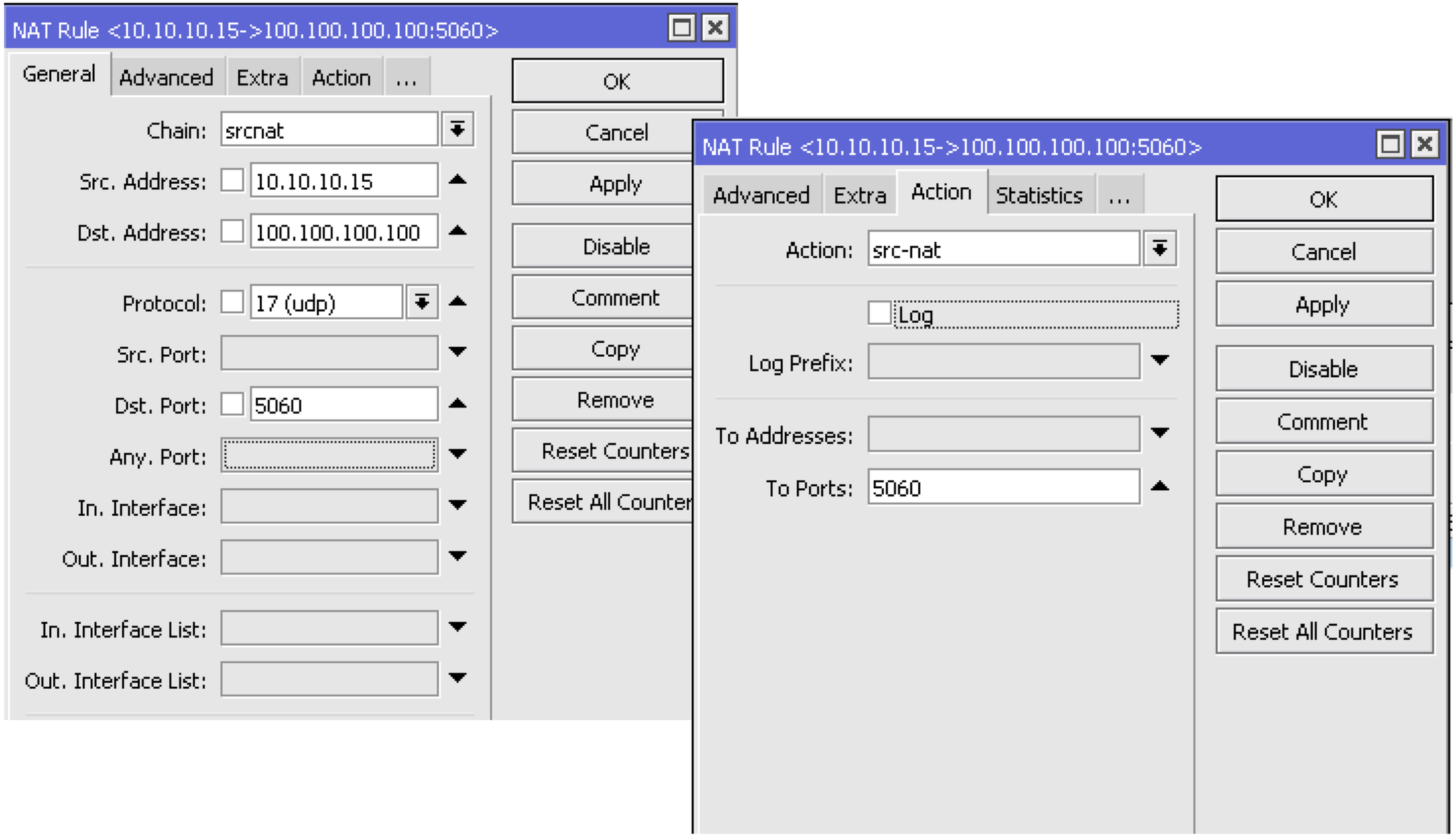
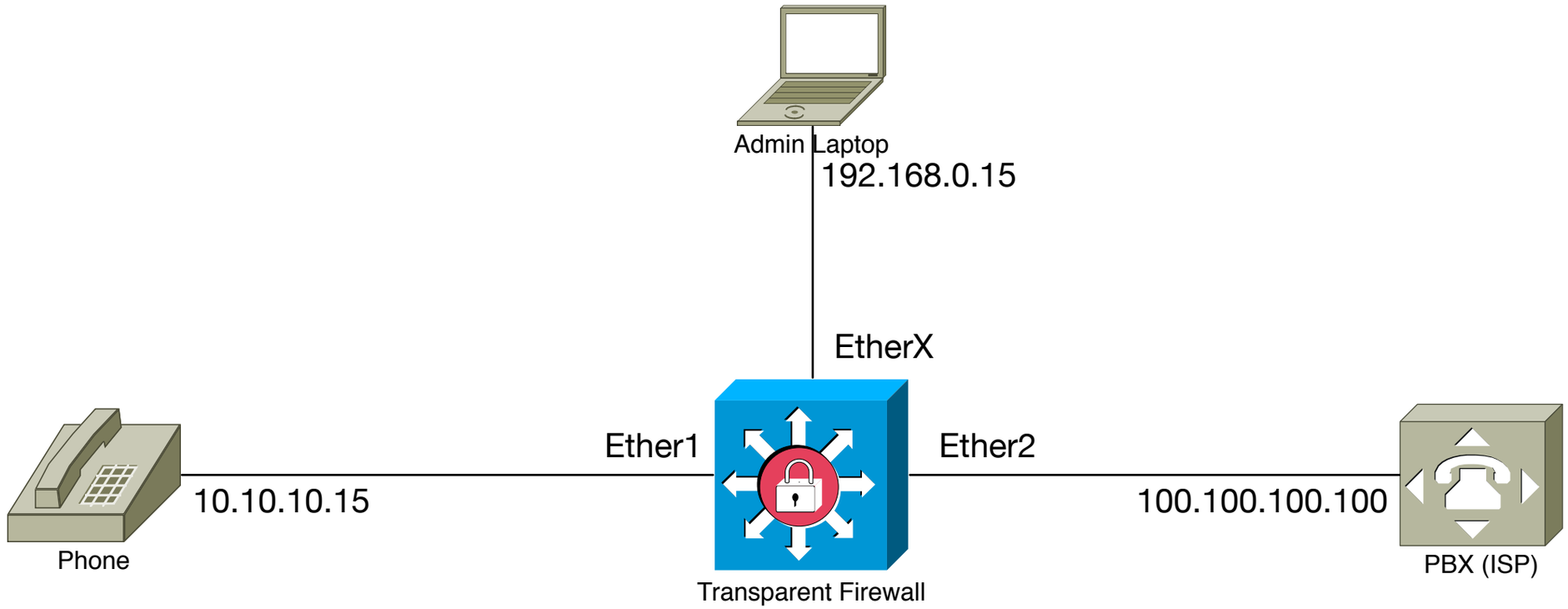
NAT

- Есть несколько вариантов решения этой задачи
- Долго ругаться с провайдером добиваясь разрешения регистрации с любого порта
- Поменять провайдера
- Поменять IP-PBX на ту, в которой можно настроить исходящий порт
- Настроить Transparent Firewall и поставить его в разрыв соединения IP-PBX и ISP

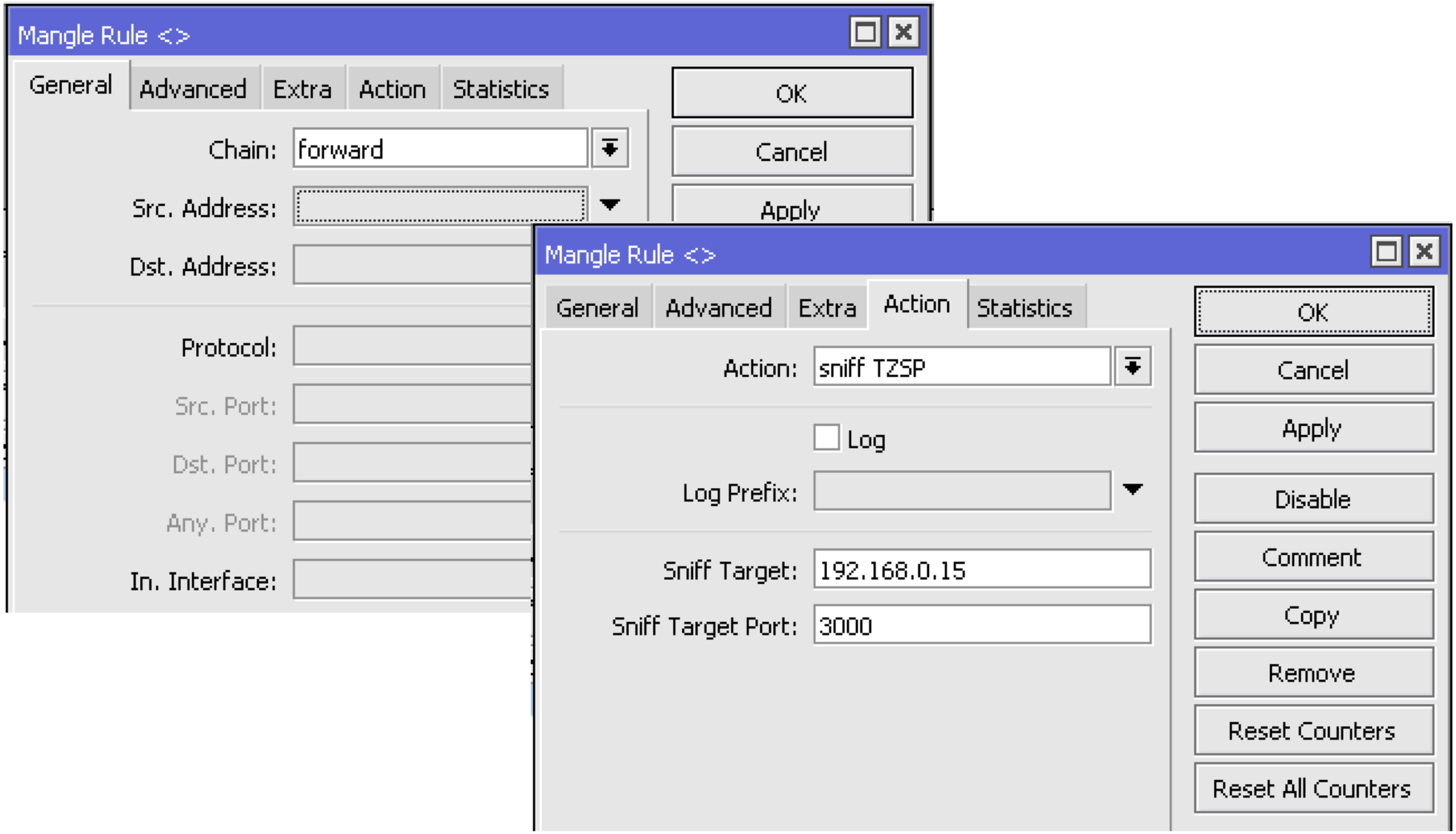
NAT



- Для решения этой задачи, нам необходимо использовать функционал IP Firewall NAT, Создав там следующее правило

- ```
  /ip firewall nat
  add action=src-nat chain=srcnat \
  dst-address=100.100.100.100 dst-port=5060 \
  protocol=udp src-address=10.10.10.15 to-ports=5060
  ```
  ```

NAT


NAT Rule <10.10.10.15->100.100.100.100:5060>
General
Advanced
Extra
Action
...
Chain: srcnat
Src. Address: 10.10.10.15
Dst. Address: 100.100.100.100
Protocol: 17 (udp)
Src. Port:
Dst. Port: 5060
Any. Port:
In. Interface:
Out. Interface:
In. Interface List:
Out. Interface List:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counter
NAT Rule <10.10.10.15->100.100.100.100:5060>
Advanced
Extra
Action
Statistics
...
Action: src-nat
Log
Log Prefix:
To Addresses:
To Ports: 5060
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Sniffer

- Вам необходимо проанализировать трафик проходящий между двумя узлами в L2 сети
- Сами вы находитесь удаленно. То есть Port Mirroring на коммутаторе вам не может помочь
- Такие задачи обычно возникают при необходимости
  - Определить проблему подключения (например SIP-телефон не регистрируется на IP-PBX
  - Посмотреть ошибки протоколов
  - Проанализировать протокол между конкретным узлом и сервером
  - Отправить трафик для анализа на IPS и т.п.

Sniffer

- Задача. Телефон не регистрируется на PBX. PBX у провайдера (доступа нет). Надо определить проблему.



Sniffer

- Для решения этой задачи нам необходим Transparent Firewall имеющий дополнительный интерфейс, через который возможна связь с ПК системного администратора (Прямой линк, Интернет, VPN и т.п.)

- Воспользуемся функцией Sniff TZSP для отправки отловленных пакетов на ПК администратора

- ```
  /ip firewall mangle
  add action=sniff-tzsp chain=forward \
  sniff-target=192.168.0.15 \
  sniff-target-port=3000
  ```
  ```

Sniffer


Mangle Rule <>
General
Advanced
Extra
Action
Statistics
Chain:
forward
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
OK
Cancel
Apply
Mangle Rule <>
General
Advanced
Extra
Action
Statistics
Action:
sniff TZSP
Log
Log Prefix:
Sniff Target:
192.168.0.15
Sniff Target Port:
3000
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Безопасность

- В силу своего функционала, Transparent Firewall может использоваться в злонамеренных целях, таких как:

- Атака вида Man in the middle

- Неправомерный доступ к информации (прослушивание переговоров, посредством сниффинга и, затем, сборки RTP-потока, доступ к иной передаваемой информации, перехват незашифрованных или слабозашифрованных паролей и т.п.

Безопасность

- При этом в силу того, что такое устройство может не иметь адреса внутри сети, размеры части маршрутизаторов невысоки и они могут питаться по PoE или от PowerBank, его обнаружение может быть затруднено.
- Основные методы защиты
  - Ограничивайте количество MAC-адресов на Access-портах коммутаторов
  - Совместно с ограничением адресов используйте протокол 802.1x
  - Используйте шифрование трафика даже внутри локальной сети (IPSec)

Заключение

- Transparent Firewall обладает высоким функционалом, так как объединяет в себе возможность одновременной работы на уровнях L2 и L3 модели OSI

- Существует ряд задач, решение которых без использования Transparent Firewall затруднено или невозможно

- В силу возможности маскировки устройства, нужно более тщательно подходить к обеспечению безопасности локальной сети

Спасибо за внимание

Solution.
Production.
Warranty.

Официальный дистрибьютор оборудования и программного обеспечения Mikrotik в Санкт-Петербурге.

Аудит, проектирование, внедрение и поддержка интеграционных решений в ИТ. Сертифицированное обучение.

www.spw.ru info@spw.ru 8 (800) 700 97 66