# Безопасность в MikroTik

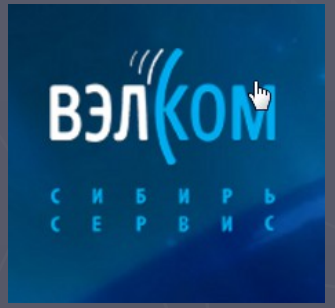
Защита ресурсов сети
и маршрутизатора

# Обо Мне

- Руководитель ИТ-службы
- MikroTik certified engineer, consultant
- MikroTik Trainer
- Сертификаты: ccna, mtcna, mtcre, mtcwe, ФЗ-152
- Работаю с микротик с 2008
- Контакты: info@mikrotik-sibir.ru
  https://vk.com/id228714012

# Тренинги MIkroTik

- ✓ MTCNA
- ✓ MTCRE
- ✓ MTCWE




- ✓ Тренинги в городах Западной Сибири и в Казахстане

www.mikrotik-sibir.ru velcom-s.ru

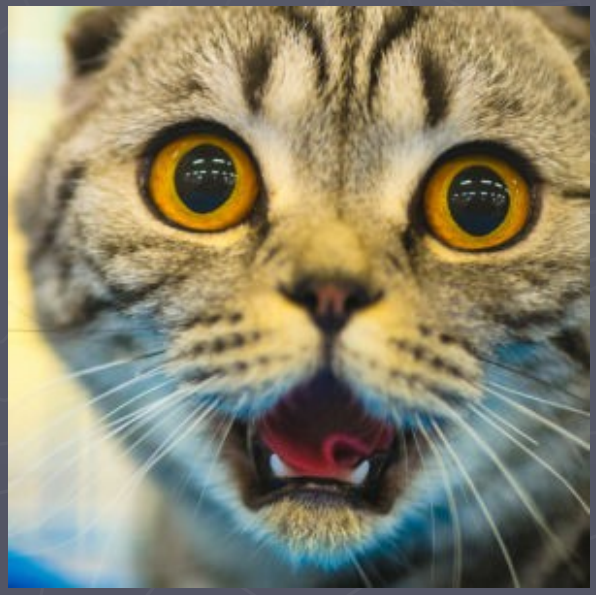
# Безопасность

- Это общая проблема IT. Вы должны быть уверены, откуда берете и куда отправляете информацию.
- Защита канала роутера
- Защита канала клиента
- Защита ресурсов в сети

# Проблема

- https://blog.kaspersky.ru/security-week-1624/12262/ **«черный рынок угнанных RDP»**

информация для доступа к одному из 70
с лишним тысяч серверов по всему миру
по протоколу RDP



# Эскалация проблемы

- ✓ https://wikileaks.org/ciav7p1/

**«CIA Vault 7 – информация о взломах»**

Информация о взломах тысяч устройств,
операционных систем и служб.
Репорты и служебная переписка.
Инструменты – Perseus, ChimayRed, TshPatcher


Попытки взлома устройств MikroTik:
RB1100, RB450, RB493,…

**Взлом ориентирован на сервисы**

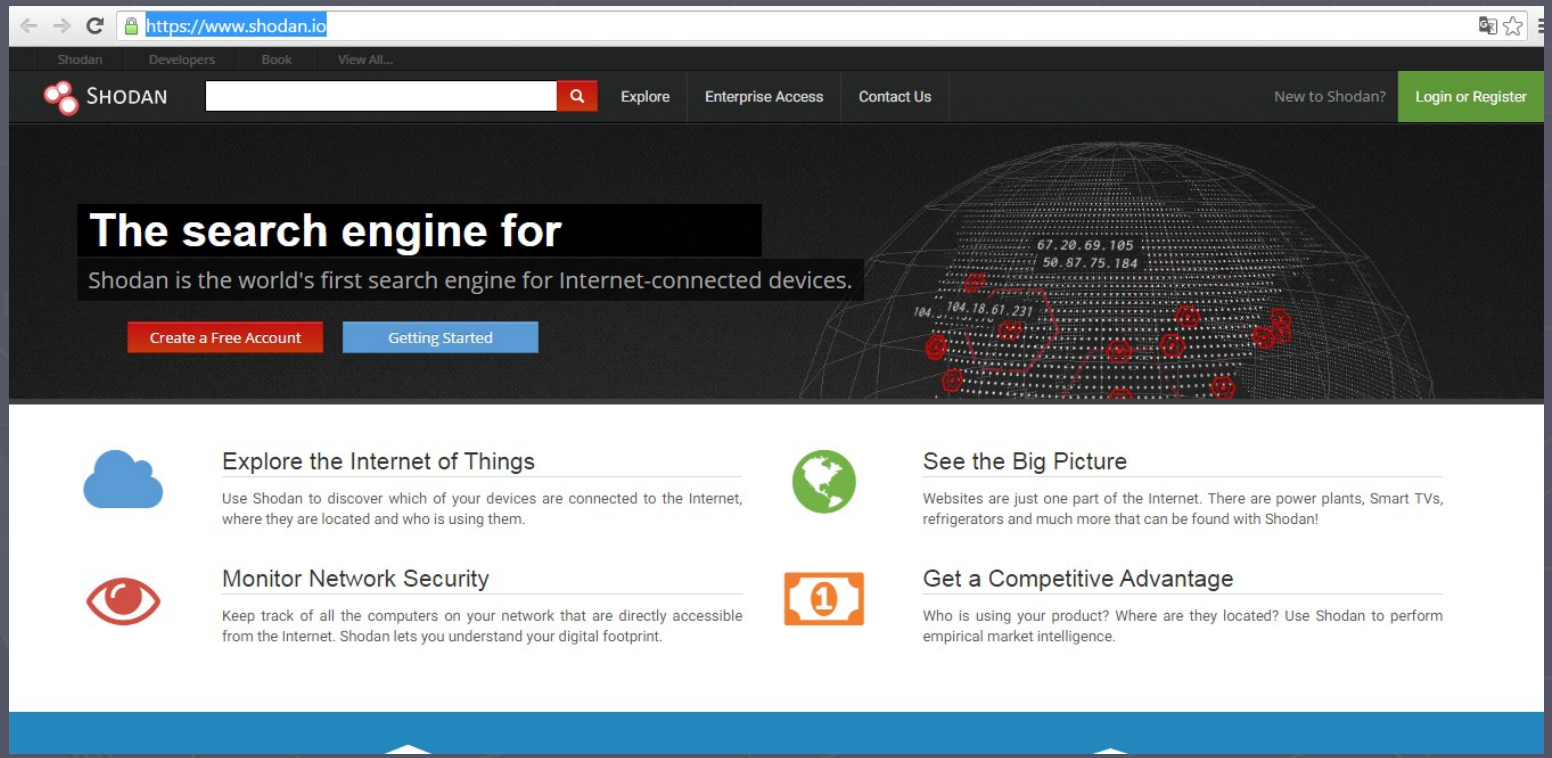
# Инструменты

- ✓ NMap
- ✓ WireShark
- ✓ Fing (on android-based smartphone)
- ✓ MikroTik “Torch” tool ☺

- ✓ Some bruteforce tools to get passwords

# Инструменты

- ✓ https://www.shodan.io/



# Чек-лист (what about You?)

- Используется  имя пользователя  “admin” ?
- Используется HTTP для управления?
- Служба neighbor на всех интерфейсах?
- Включен доступ к управлению на всех интерфейсах?
- Включен MAC-Winbox & MAC-Telnet  на всех интерфейсах ?
- Сделан Dst-NAT (portmap) без address-list ?
- SNMP community – “Public”?
- RouterOS < 6.37.5 ?

# Что означают цифры

«15408-1», «15408-2», «15408-3» ?
«27033-1», «27033-2», «27033-3» ?

# Стандарты и концепции

- ITSM, ITIL, ISO 20000, ISO 38500, MOF

- ГОСТ Р 15408-1(2,3)-2013
- ГОСТ Р ИСО/МЭК 27033-1(2,3)-2014
- Требования ФСТЭК

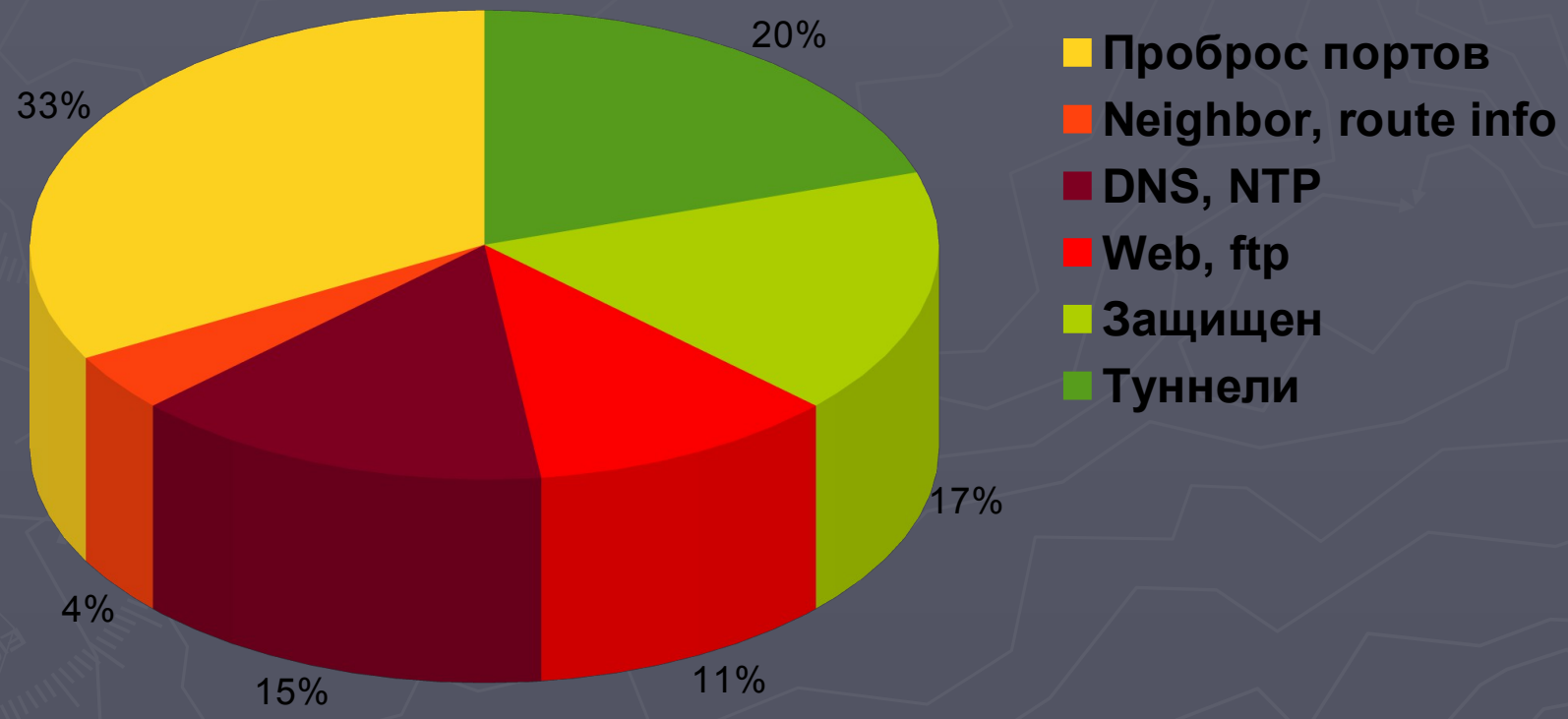
Каталог http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty

# Стандарты и концепции

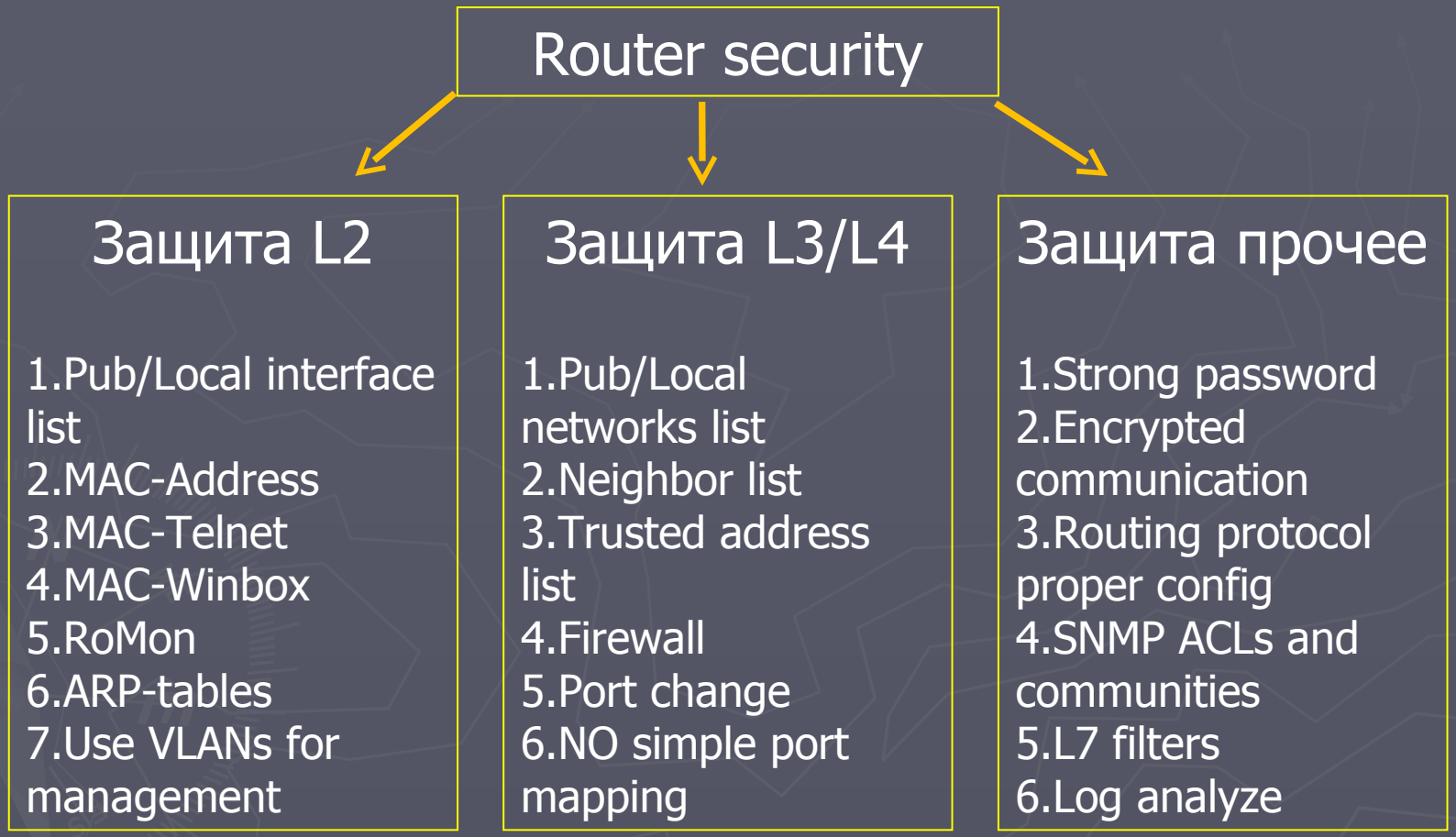
| | |
|---|---|
| ГОСТ Р ИСО/МЭК 15408-3-2013 | Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности |
| ГОСТ Р ИСО/МЭК ТО 15446-2008 | Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности |
| ГОСТ Р ИСО/МЭК ТО 18044-2007 | Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности |
| ГОСТ Р ИСО/МЭК 18045-2013 | Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий |
| ГОСТ Р ИСО/МЭК ТО 19791-2008 | Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем |
| ГОСТ Р ИСО/МЭК 21827-2010 | Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса |
| ГОСТ Р ИСО/МЭК 27000-2012 | Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология |
| ГОСТ Р ИСО/МЭК 27001-2006 | Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования |
| ГОСТ Р ИСО/МЭК 27002-2012 | Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности |
| ГОСТ Р ИСО/МЭК 27003-2012 | Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности |
| ГОСТ Р ИСО/МЭК 27004-2011 | Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения |
| ГОСТ Р ИСО/МЭК 27005-2010 | Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности |
| ГОСТ Р ИСО/МЭК 27006-2008 | Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности |
| ГОСТ Р ИСО/МЭК 27007-2014 | Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности |
| ГОСТ Р ИСО/МЭК 27013-2014 | Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1 |
| ГОСТ Р ИСО/МЭК 27033-1-2011 | Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции |
| ГОСТ Р ИСО/МЭК 27033-3-2014 | Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления |
| ГОСТ Р ИСО/МЭК 27034-1-2014 | Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия |
| ГОСТ Р ИСО/МЭК 27037-2014 | Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме |
| ГОСТ Р ИСО/МЭК 29100-2013 | Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности |
| Рекомендации по стандартизации Р 50.1.050-2004 | Защита информации. Система обеспечения качества техники защиты информации. Общие положения |
| Рекомендации по стандартизации Р 50.1.053-2005 | Информационные технологии. Основные термины и определения в области технической защиты информации |
| Рекомендации по стандартизации Р 50.1.056-2005 | Техническая защита информации. Основные термины и определения |

пример каталога на сайте

# Состояние маршрутизаторов MikroTik в соседних сетях



# Уровни и Объекты Защиты



# Минимальные задачи защиты

1. Скрыть тип устройства маршрутизации

2. Скрыть информацию специфичную для вендора. Модель, версию прошивки, дату производства и т.п.

3. Скрыть информацию о ПО: версию ОС, номер билда, версии работающих служб и приложений.

# Безопасность L2 & MAC

1. MAC адрес содержит информацию о производителе устройства. Смените его. Будьте осторожны, избегайте конфликта MAC-адресов. В IPv6 MAC тоже «виден»

(*/interface ethernet  set ether1 mac-address = d4:9a:20:0d:0e:0a*)


d4:9a:20:xx:xx:xx

# Безопасность L2 & MAC

1. MAC адрес содержит информацию о производителе устройства. Смените его. Будьте осторожны, избегайте конфликта MAC-адресов. (*/interface ethernet set ether1 mac-address =0a:0b:0c:0d:0e:0f* )
2. MAC-telnet, MAC-Winbox ищет специальные кадры среди поступающих на интерфейс. Это может немного снижать производительность. Отключите службы MAC на внешних и на нагруженных интерфейсах (*/tool mac-server set [ find default=yes ] interface=trusted_interface* )
3. Установите опцию ARP “reply only”, и занесите MAC аплинка и интерфейс в таблицу ARP. Защита от подмены аплинка. От подмены DHCP.
   (*/interface ethernet set ether1 arp=reply-only* )

# Безопасность L2 & MAC

**Внешний интерфейс**
**MAC-Address**
СМЕНИТЬ!

**Чужой vendor-id!**
*(/interface ethernet set ether1 mac-address =0a:0b:0c:0d:0e:0f )*

**Внешний интерфейс**
**MAC-Ping**
ВЫКЛЮЧИТЬ!

**Внешний интерфейс**
**RoMon**
ВЫКЛЮЧИТЬ!

**Внешний интерфейс**
**MAC-Telnet**
ВЫКЛЮЧИТЬ!

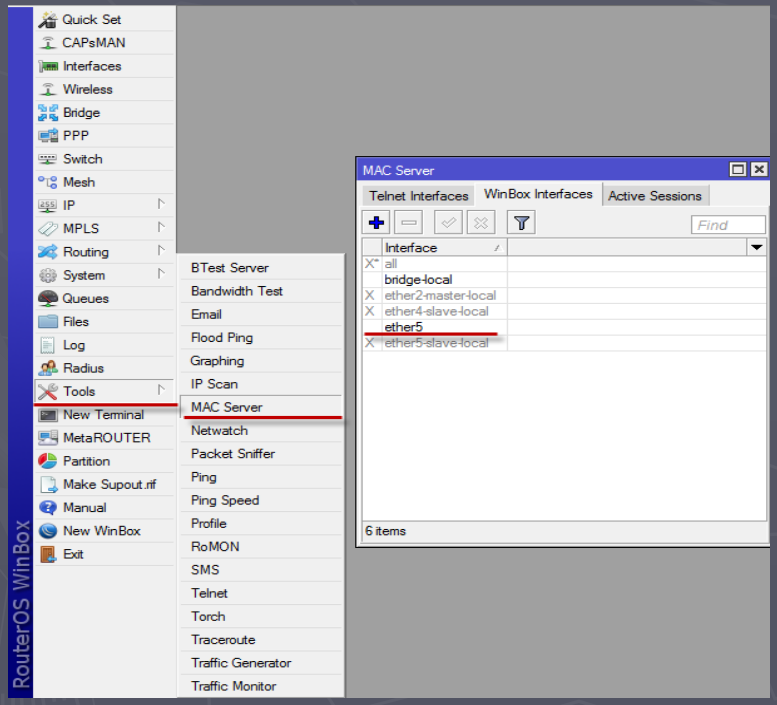
**Внешний интерфейс**
**Mac-Winbox**
ВЫКЛЮЧИТЬ!

# Защита каждого L2-интерфейса

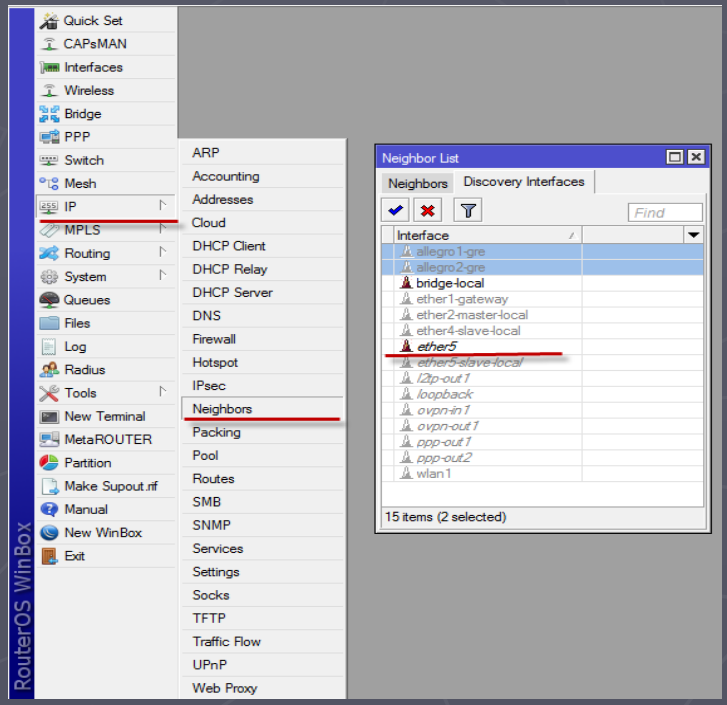
**Ahtung!**

По умолчанию Discovery ВКЛЮЧЕН на каждом новом статическом интерфейсе.

MAC-services




Discovery services

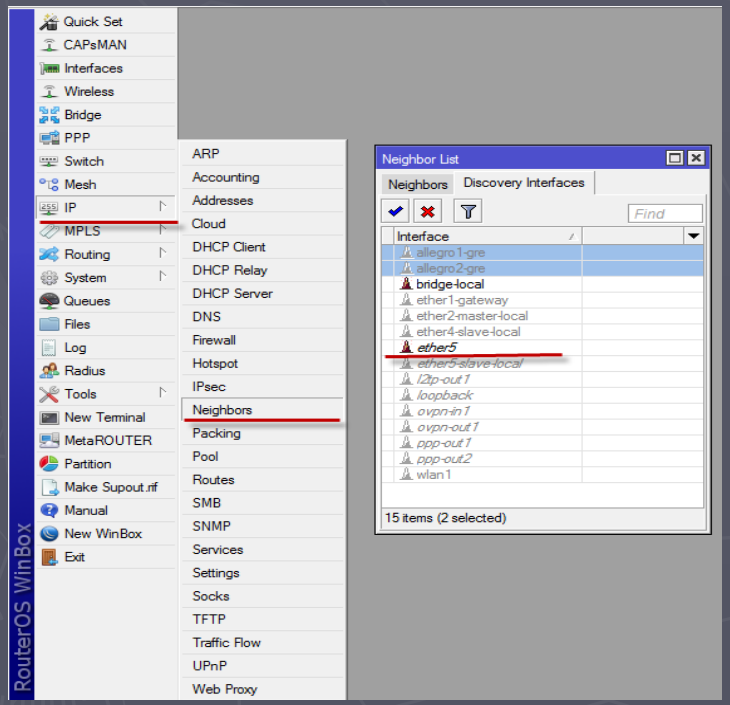


# Защита каждого L2-интерфейса

**Ahtung!**

Поведение Discovery  умолчанию меняется ТОЛЬКО ЧЕРЕЗ КОНСОЛЬ

Discovery services




/ip neighbors descovery settings

set default=no

set default-for-dynamic=no

# Neighbor – утечка информации

Neighbor service распространяет информацию:

- О модели устройства;
- О версии OS;
- О MAC и IP адресах;
- Об UpTime, наличии IPv6 и прочее

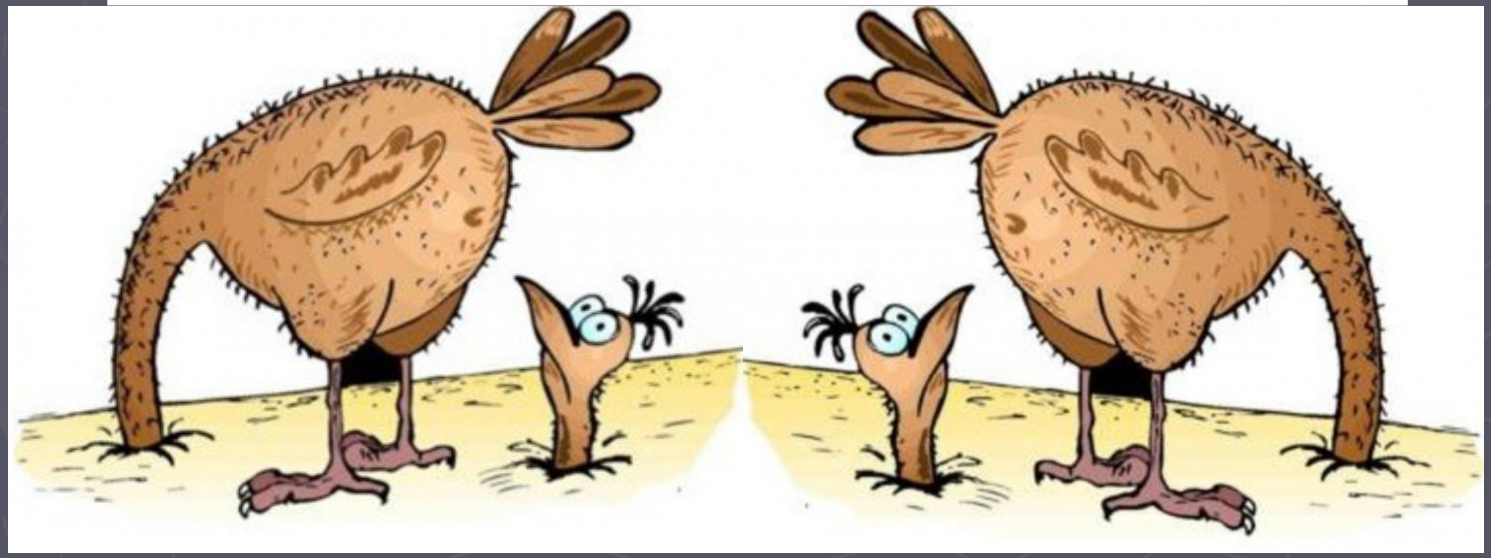
Желающие подсмотреть за соседями по сети дропают исходящий трафик neighbor discovery service ☺

# Neighbor – утечка информации

Желающие подсмотреть за соседями по сети делают так: ☺

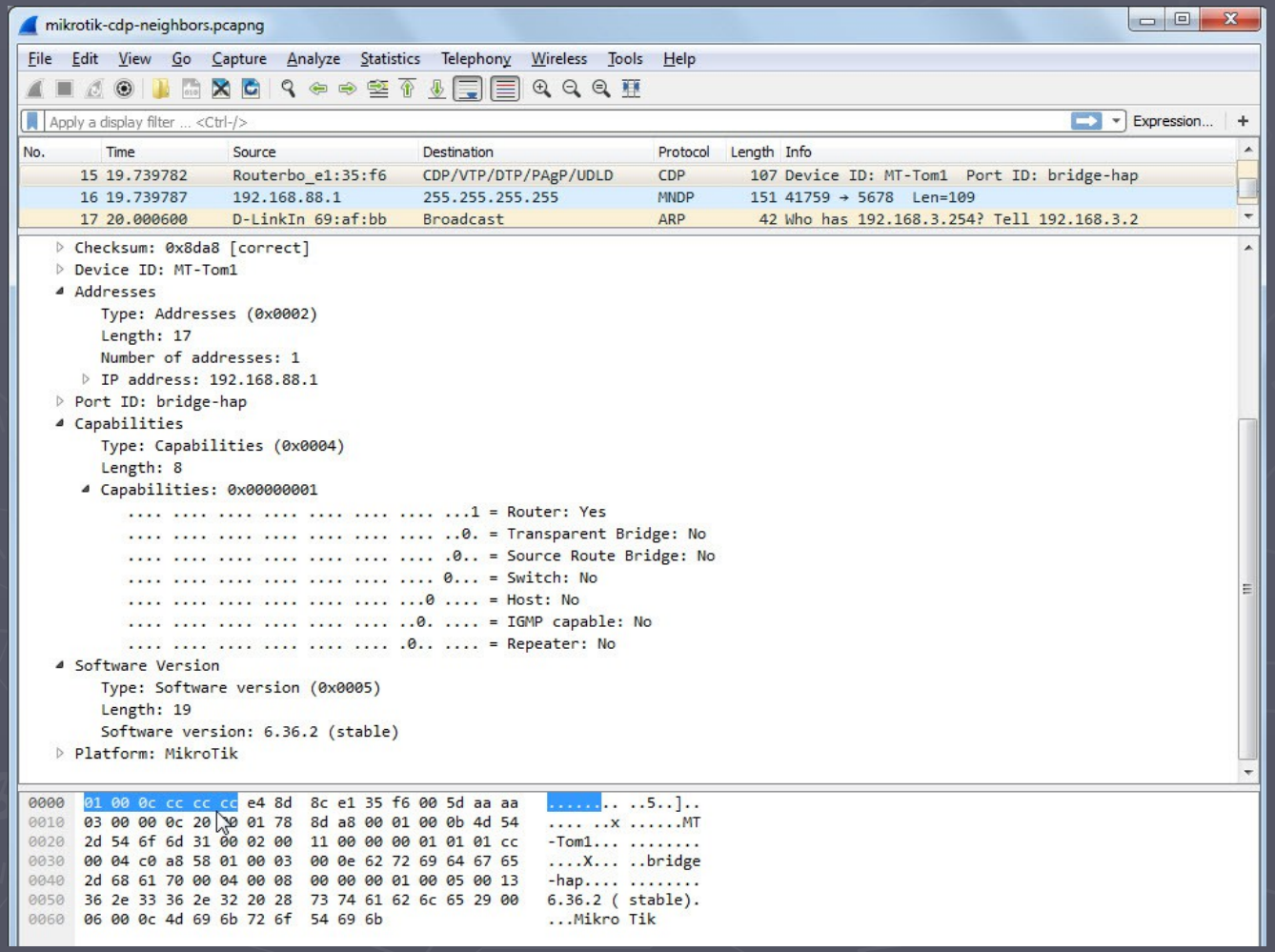
/ip firewall filter add chain=output action=drop protocol=udp dst-port=5678 out-interface=Wan

**CDP/VDP/(LLDP from 6.38)**



# Neighbor – CDP протокол L2

Фильтруется по MAC: 01:00:0C:CC:CC:CC на бридже

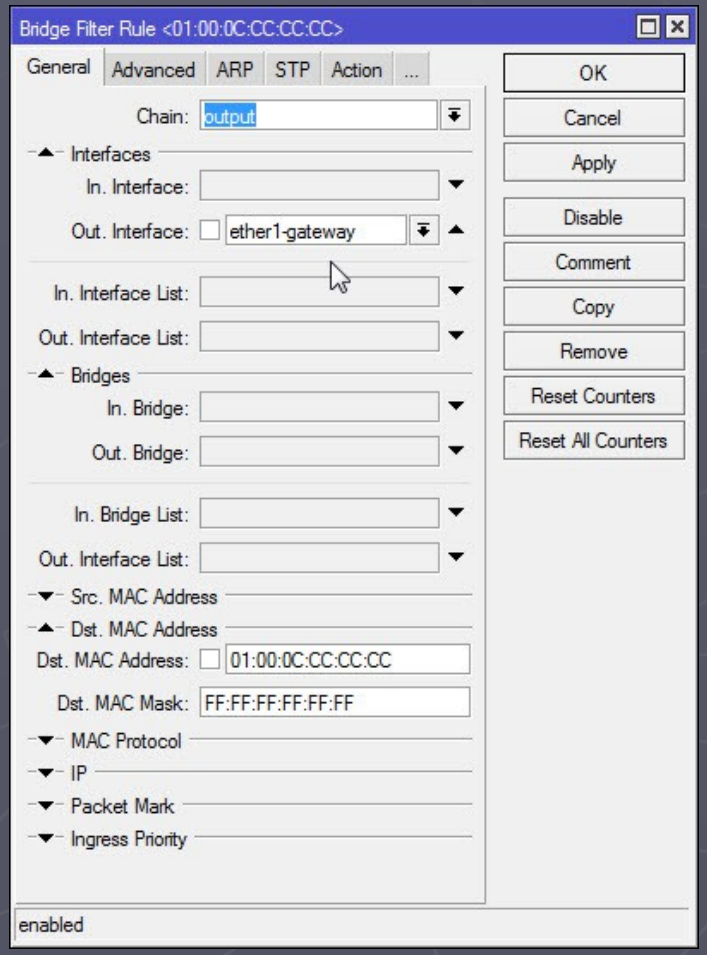


# Безопасность L2 & MAC

1. Создаем Bridge-WAN

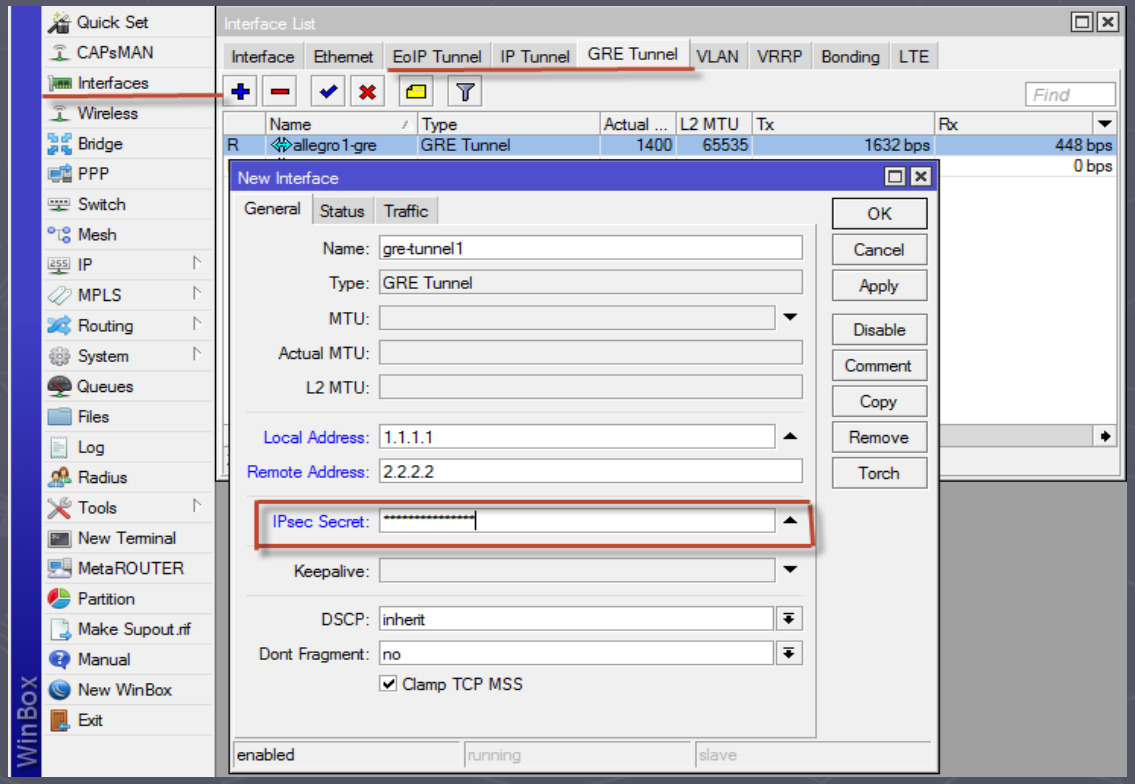
2. Включаем WAN-интерфейс в бридж

3. Создаем Bridge filter с action drop



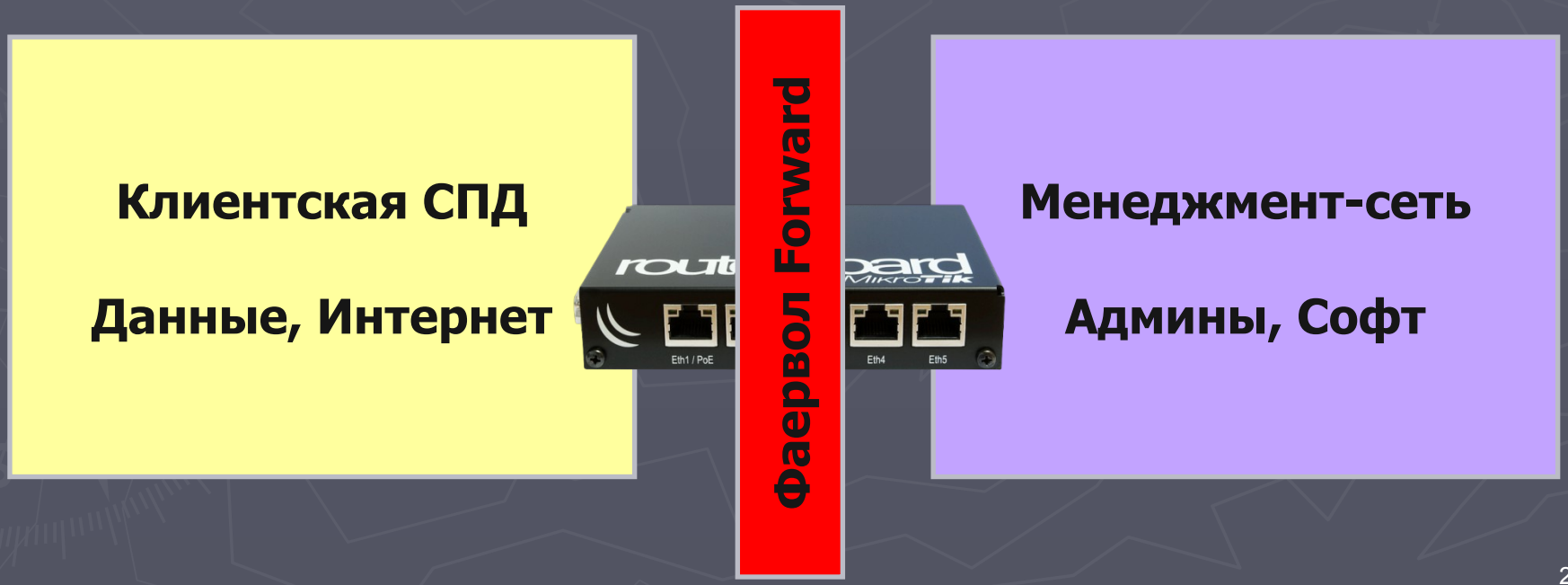
# Защита туннелей EoIP/GRE/IPIP

1. Обычно данные передаются в открытом виде, инкапсулированные в еще один пакет IP
2. Используйте шифрование IPSEC (RoS >6.30)



# Безопасность L3. Ресурсы сетей

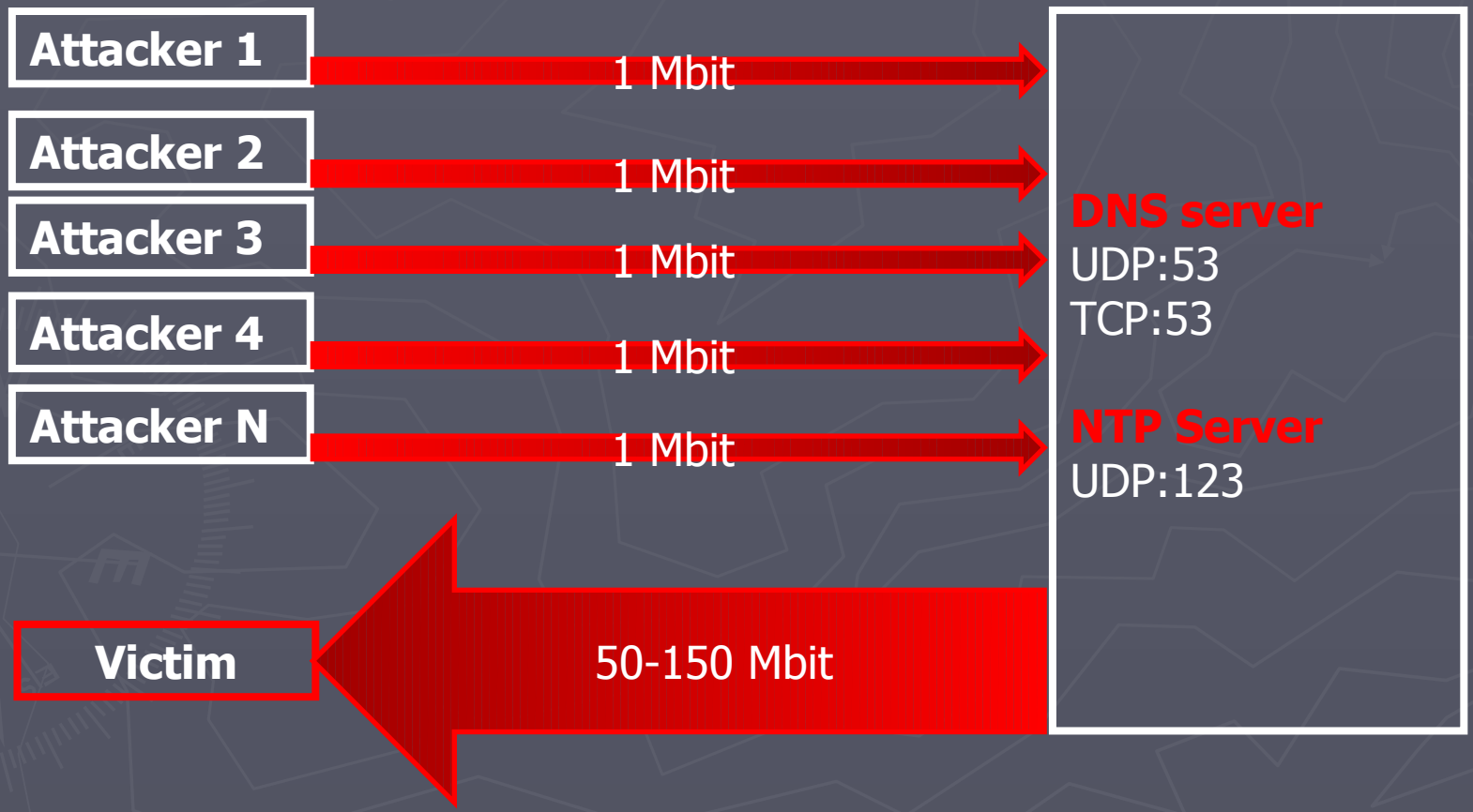
1. Убедитесь, что внешние интерфейсы НЕ соединяются в бридж с доверенными интерфейсами управления
2. Проверьте настройки фаервола, для исключения форвардинга в management-подсеть.



# Защита служб L3/L4
# UDP amplification attack

1. Злодей отправляет UDP-запрос с SRC IP-address жертвы
2. DNS/NTP сервер отвечает большим UDP-пакетом жертве
3. Жертва попадает под DDoS-атаку большими UDP-пакетами от сервера MikroTik, с 53 или 123 порта

# Защита служб L3/L4
# UDP amplification attack

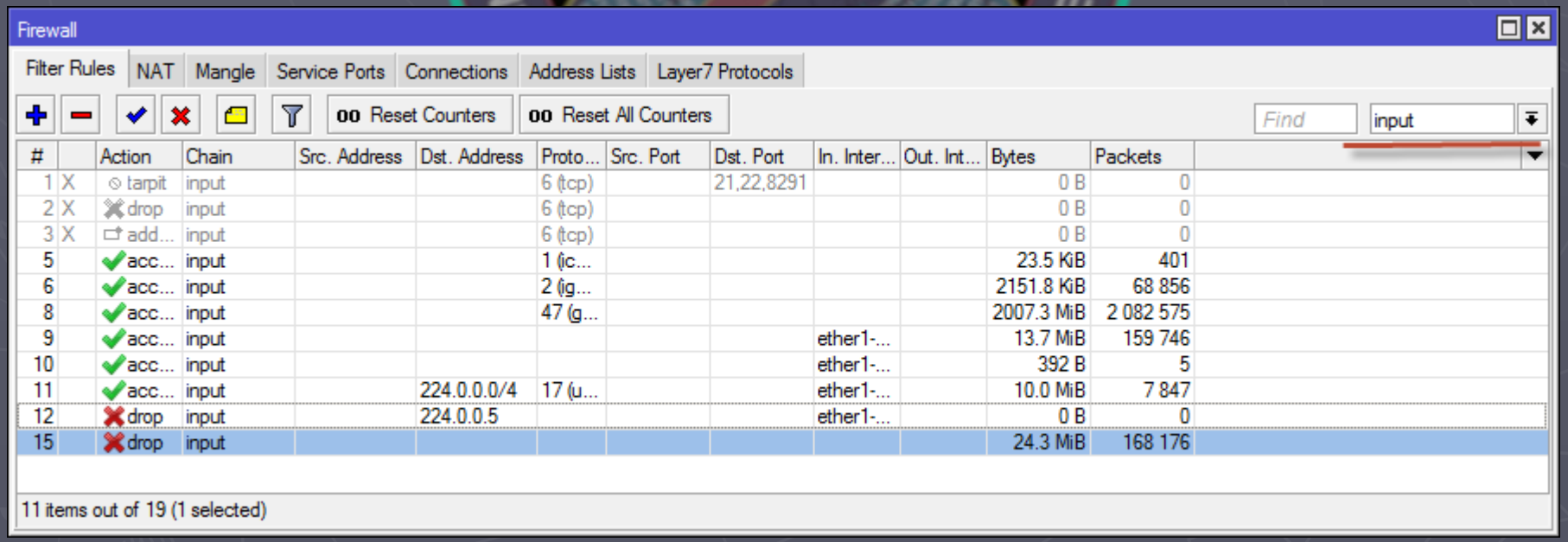


# Защита служб L3/L4
# UDP amplification attack

| Protocol | Bandwidth Amplification Factor | Vulnerable Command |
|---|---|---|
| DNS | 28 to 54 | see: TA13-088A [1] |
| NTP | 556.9 | see: TA14-013A [2] |
| SNMPv2 | 6.3 | GetBulk request |
| NetBIOS | 3.8 | Name resolution |
| SSDP | 30.8 | SEARCH request |
| CharGEN | 358.8 | Character generation request |
| QOTD | 140.3 | Quote request |
| BitTorrent | 3.8 | File search |
| Kad | 16.3 | Peer list exchange |
| Quake Network Protocol | 63.9 | Server info exchange |
| Steam Protocol | 5.5 | Server info exchange |

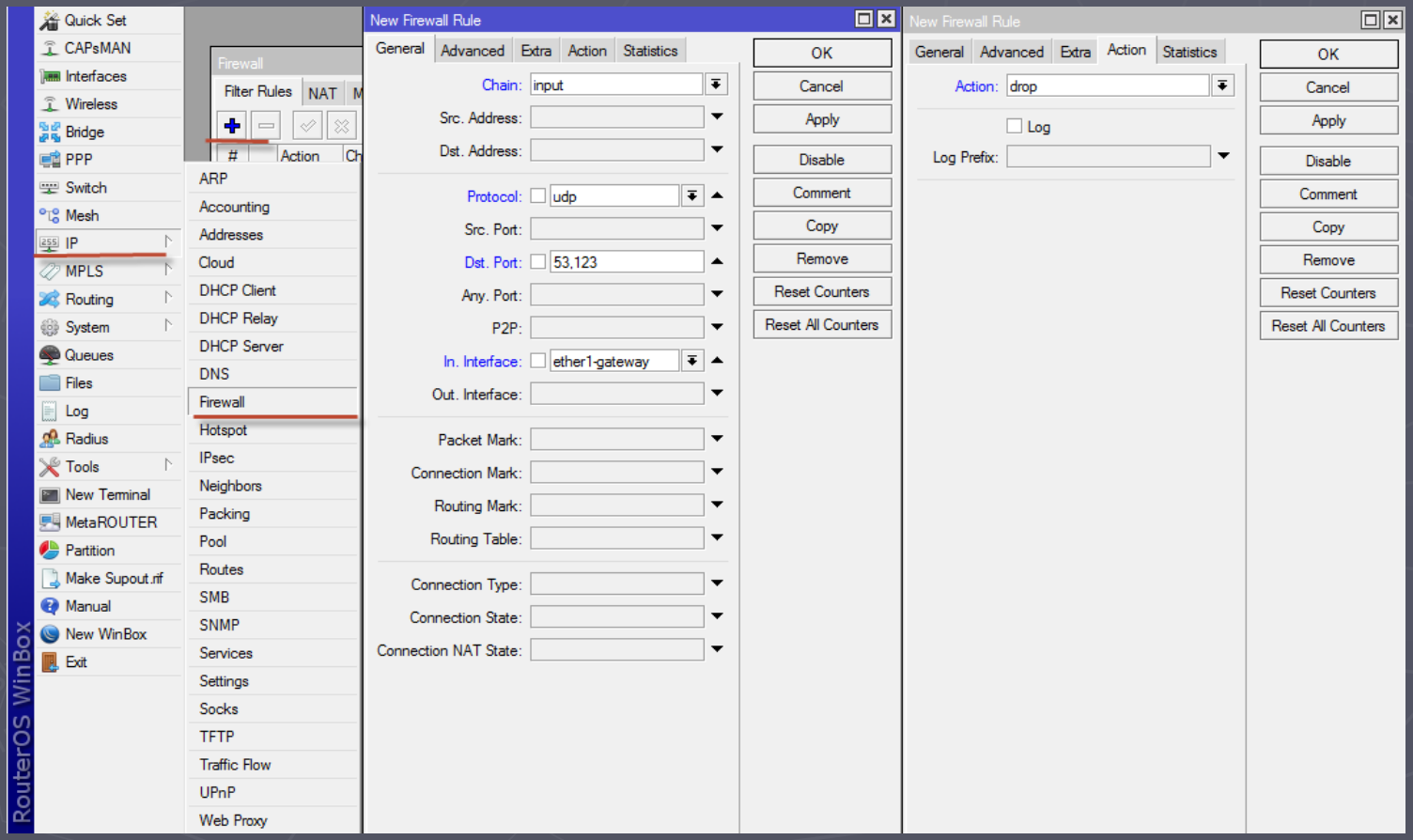
# Защита служб L3/L4
# Фаерволл по-умолчанию

- Рекомендуется закрывать всё, что явно не разрешено



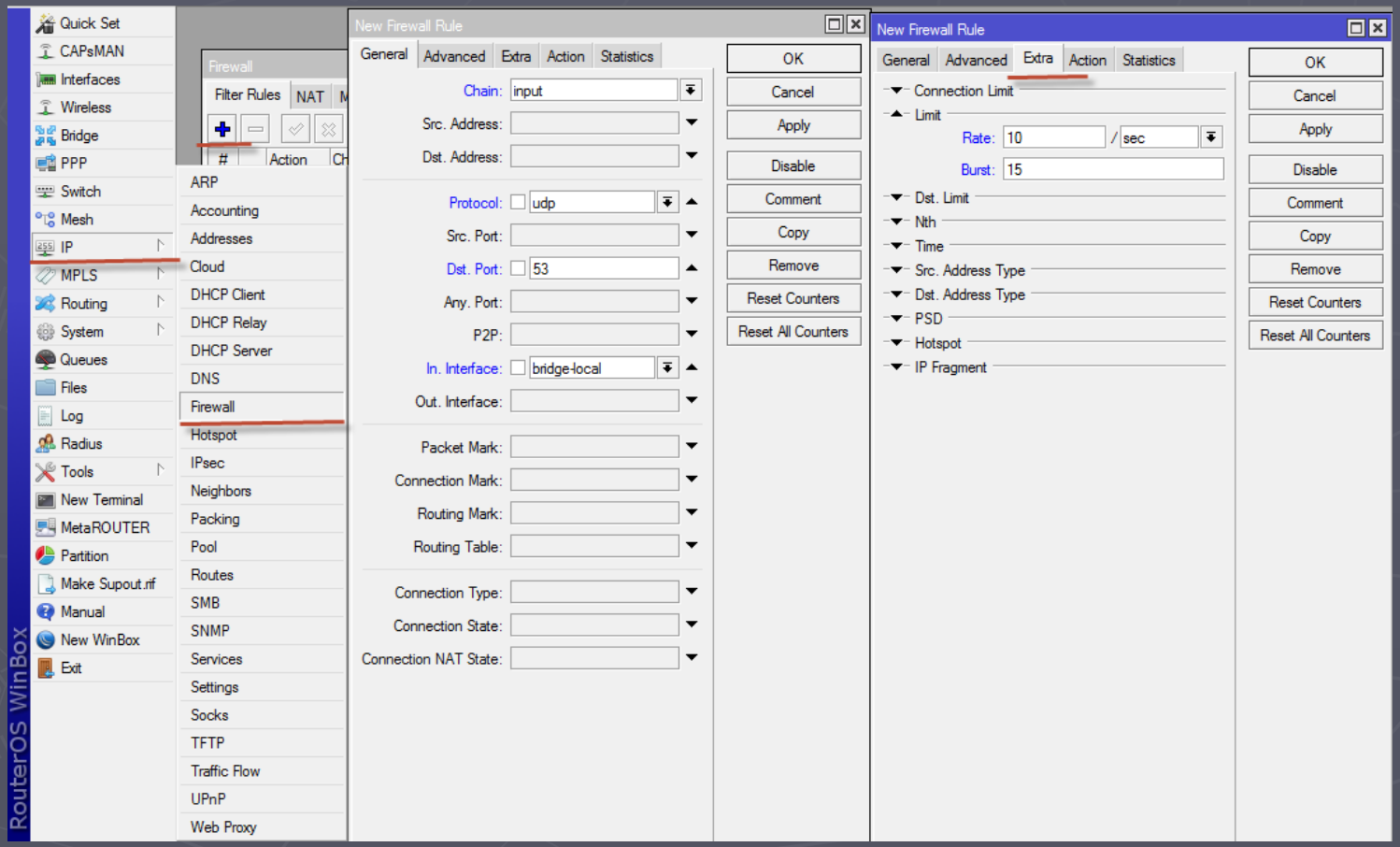
# Защита служб L3/L4
# UDP amplification attack solution

- Закрыть порты 123 udp, 53 tcp&udp из Интернет.



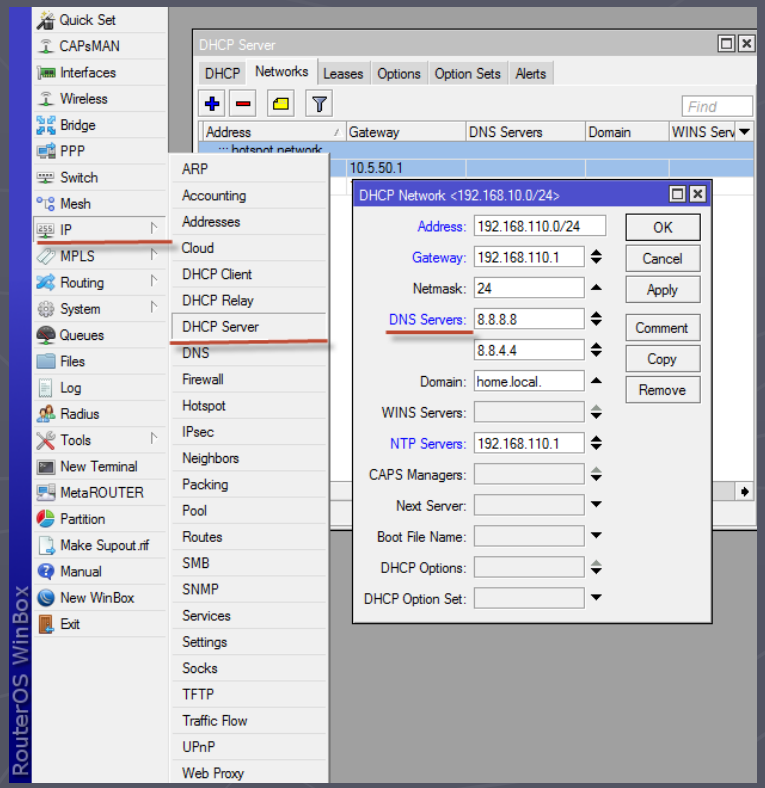
# Защита служб L3/L4
# UDP amplification attack solution

- Ограничить трафик на udp:53 udp:123 фаерволом



# Защита служб L3/L4
# UDP amplification attack solution

- Давать доступ к DNS только доверенным узлам
- Использовать внешние DNS-серверы (e.x. google DNS)



# Служба FTP

Открытие доступа пользователей к службе FTP может быть опасным!

Пример баннера при Telnet-подключении:

”220 MikroTik-951 FTP server (MikroTik 6.36.3) ready”

- Показывает производителя
- Показывает модель устройства ☹
- Показывает версию RouterOS ☹
- Можно попытаться загрузить свои пакеты типа “system”?

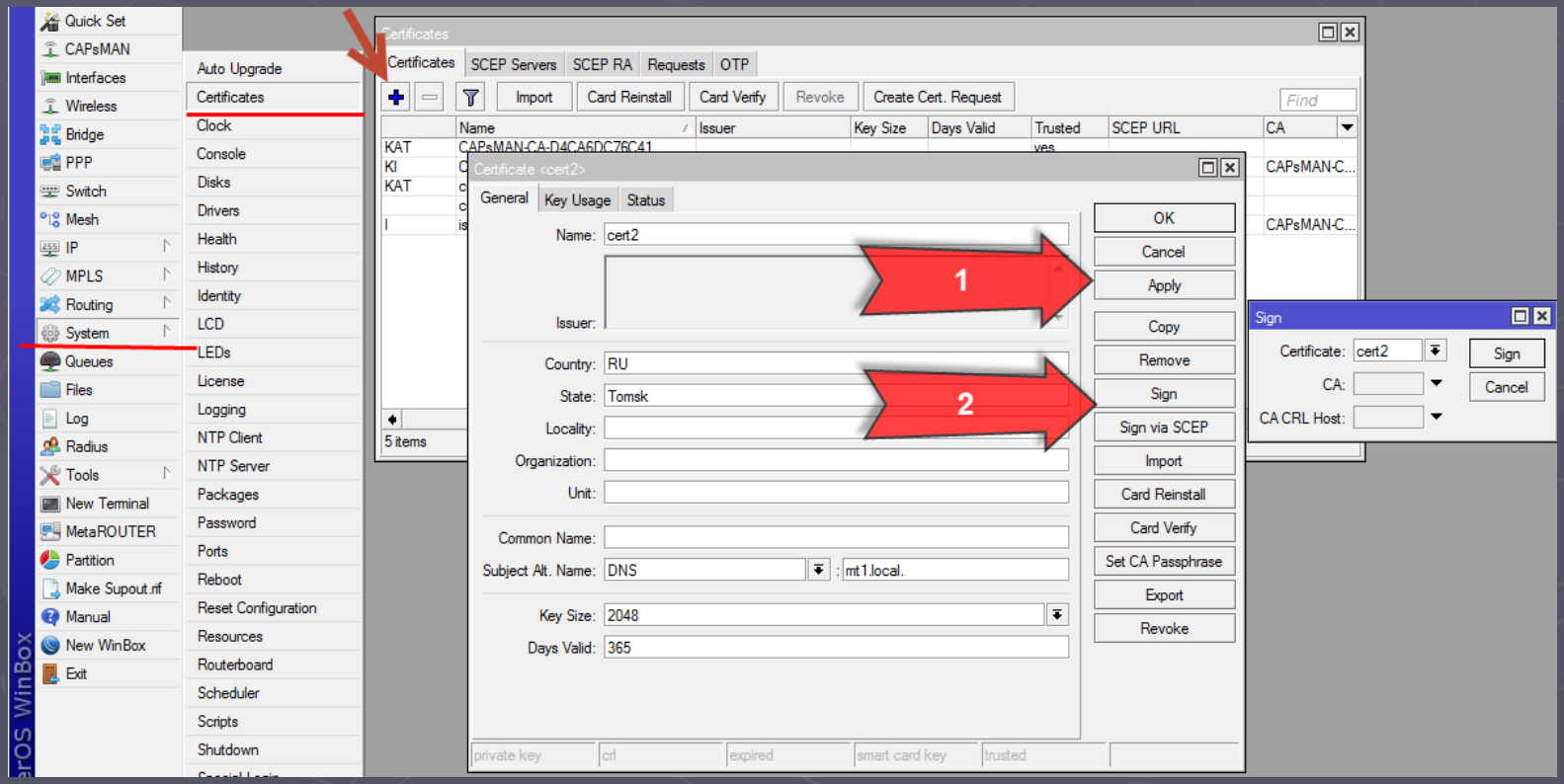
Приглашение для подбора паролей?

Залить script.rsc.auto?

# Защита WebFig и API

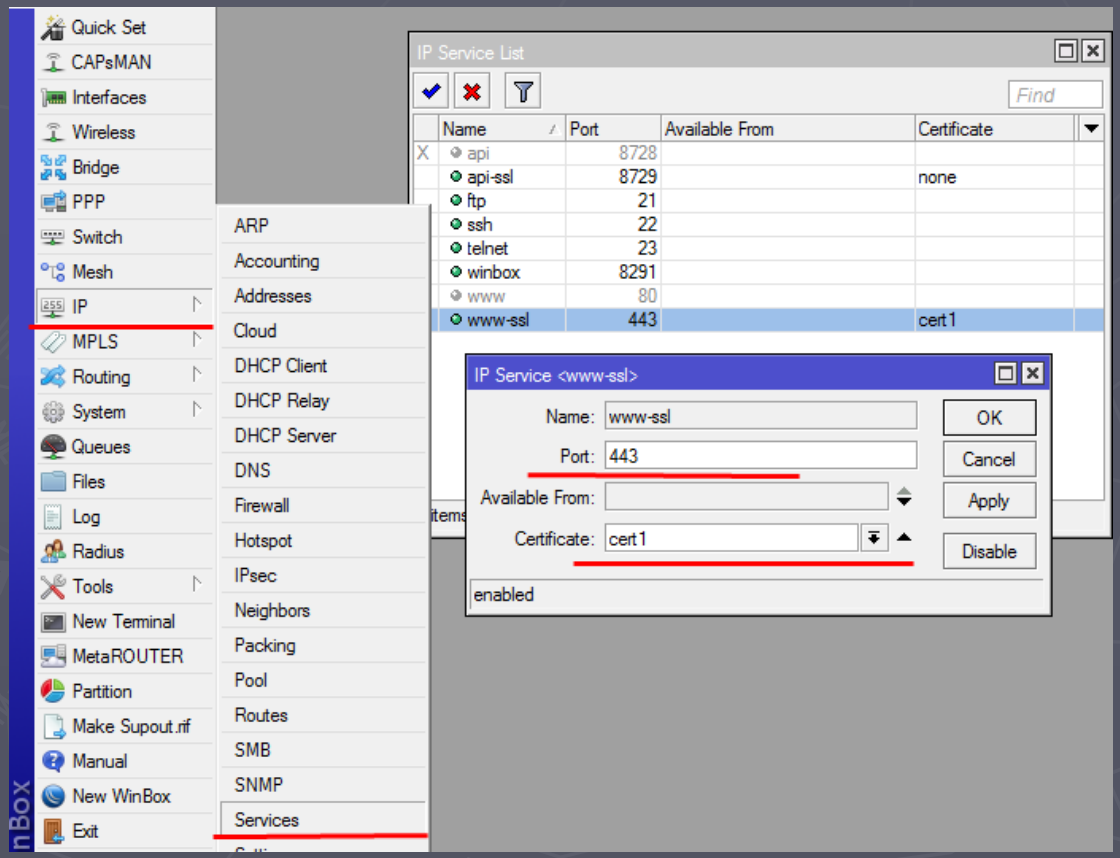
- Http передает данные в открытом виде
- HttpS по-умолчанию не работает

Для работы HTTPS нужен сертификат. Любой ☺



# Защита WebFig и API

- Устанавливаем сертификат к службе, меняем порт



# Firewall – проброс портов

DST-NAT + Standart ports → DDoS

- Пароль не спасает от DDoS
- Пароль не спасает от багов и уязвимости служб

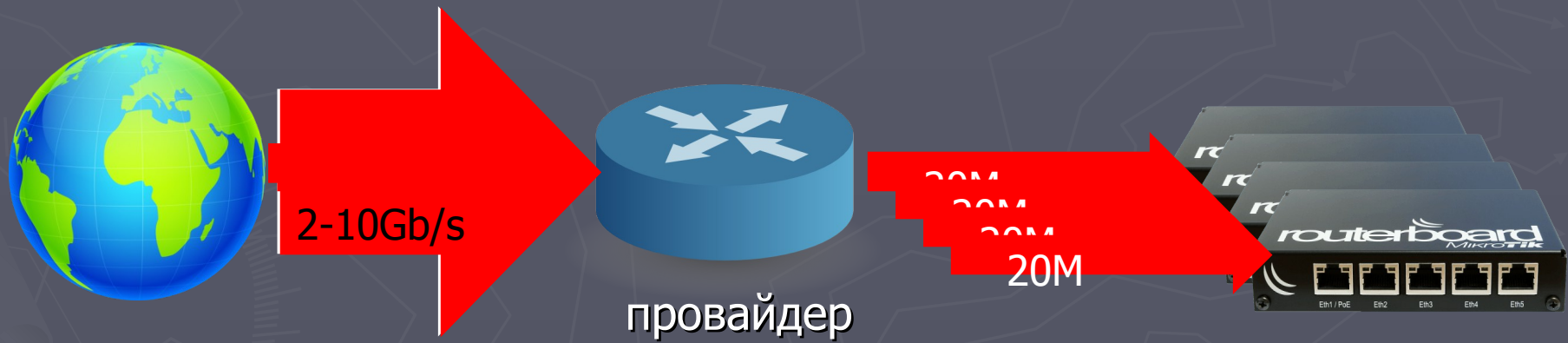
# Firewall – проброс портов

- DST-NAT + Standart ports → DDoS


# Firewall – проброс портов

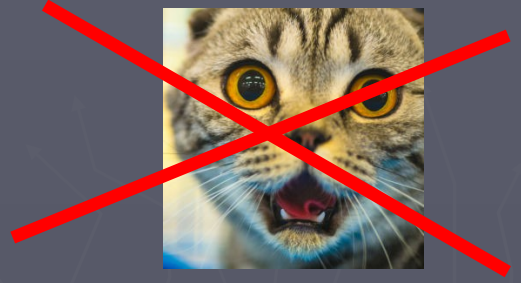
DST-NAT + Standart ports → DDoS

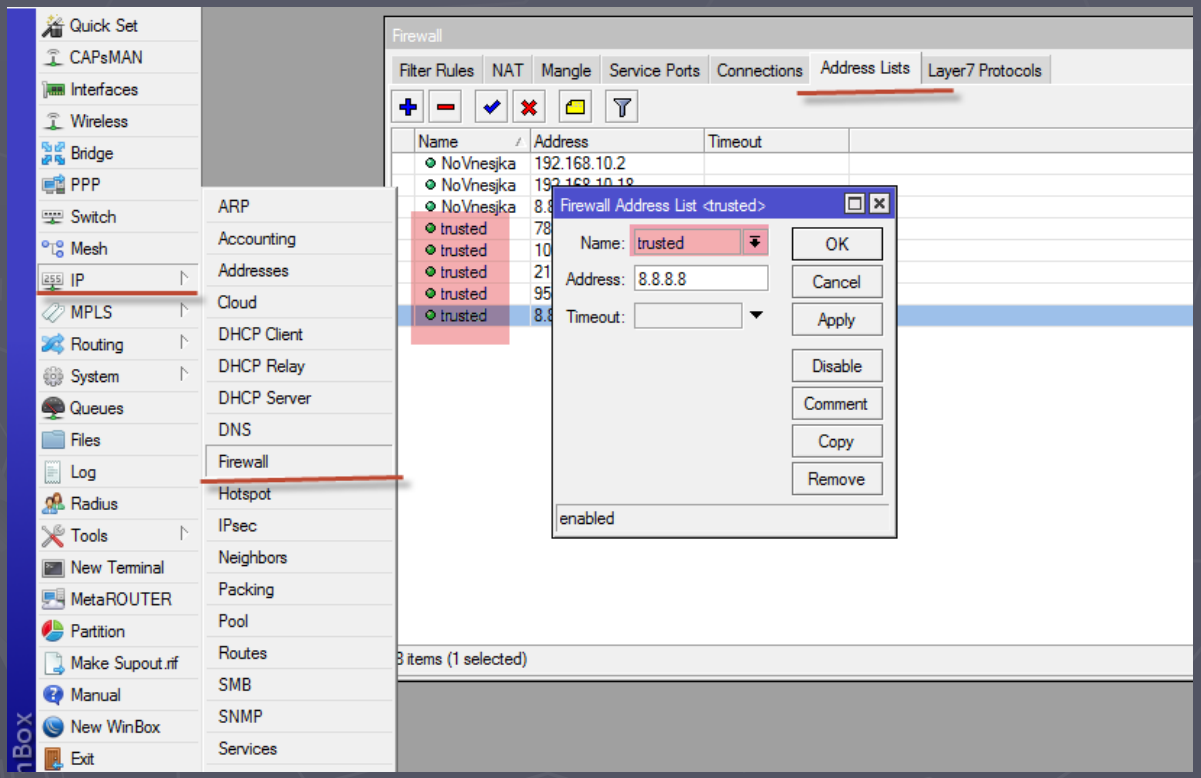
не злите провайдера – вам с ним еще работать



# Firewall – проброс портов

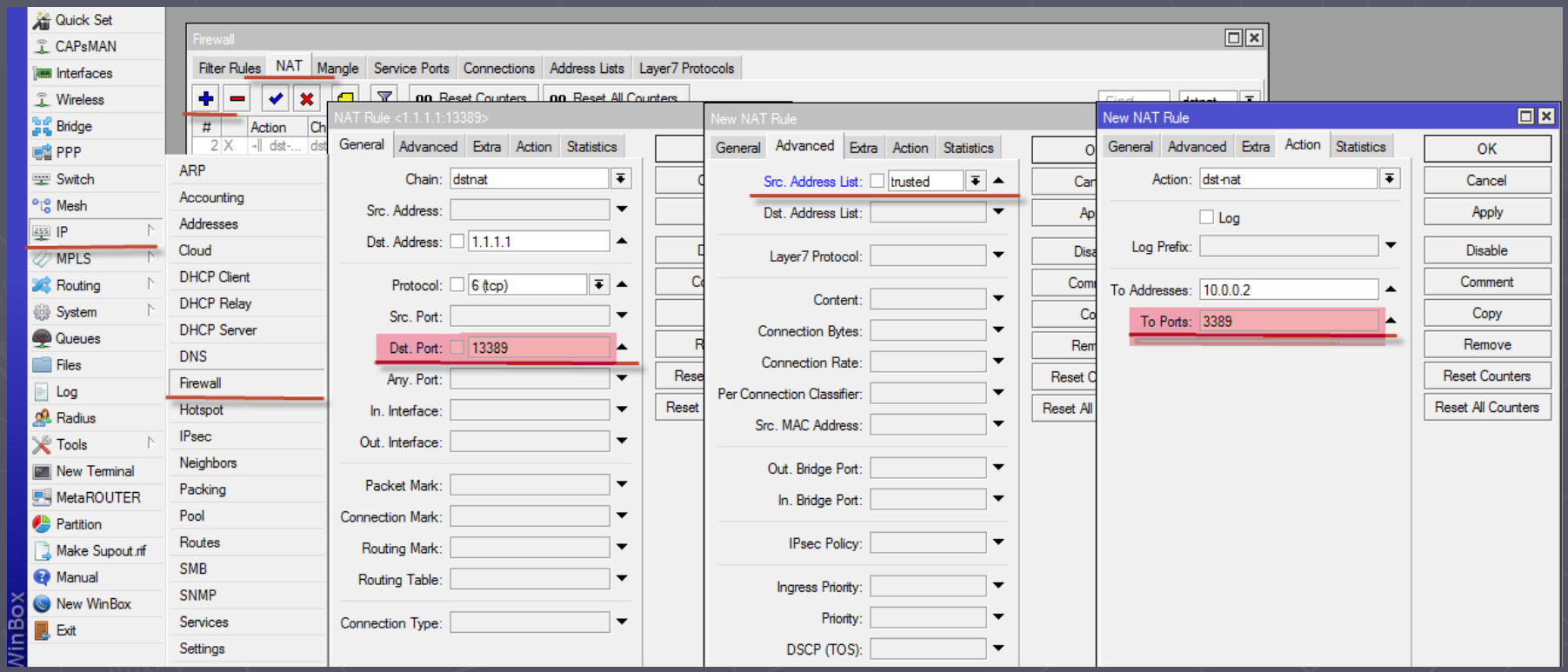
- DST-NAT + Address-List
- Forward + Address-List





# Firewall – проброс портов

- DST-NAT + Address-List
- Forward + Address-List



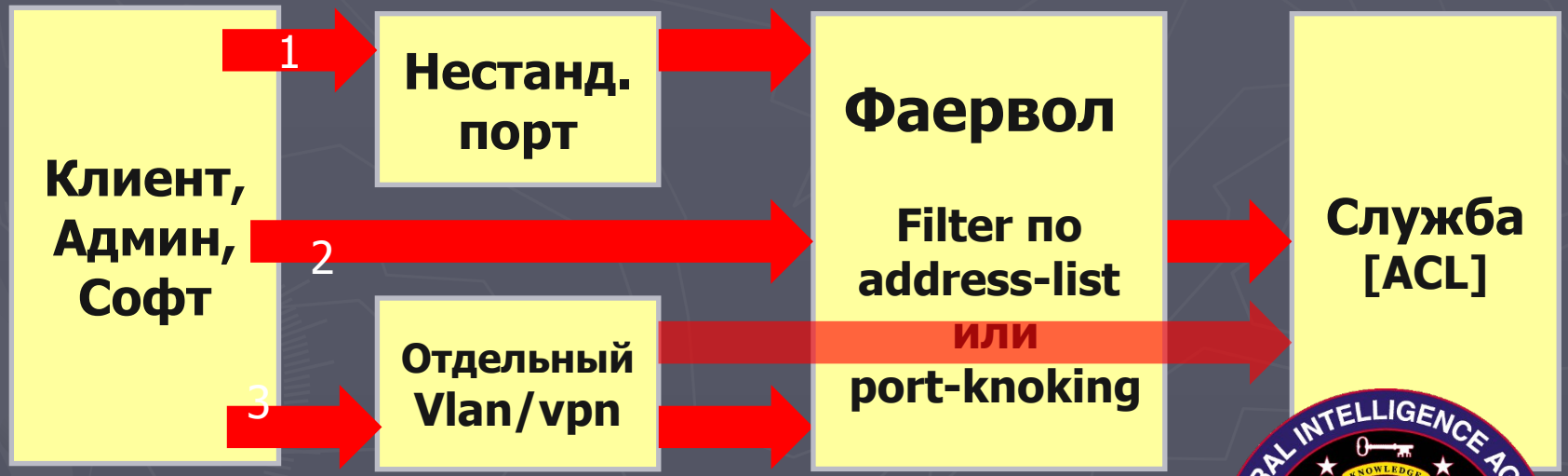
# Firewall и IPv6

- IPv6 фаервол по-умолчанию пуст
- IPv6 фаервол подразумевает ACCEPT
- IPv6 запускается на всех интерфейсах
- IPv6 автоматически создет себе локальный адрес
- В IPv6 нет NAT и подсети доступны через forward

# Защита служб

Схема доступа для настоящих админов ☺

Собственная ACL сервиса может иметь уязвимости.



# Вопрос

Кто такой Joshaven Potter?

www.joshaven.com

# Полезняшки от mr.Potter

Joshaven Potter сделал

- ✓Готовые
- ✓Автообновляемые
- ✓Исполняемые скрипты «address-list»

1. OpenBl.org
2. SpamHaus.org
3. Dshield
4. Malc0de

Доступно для скачивания на www.joshaven.com

# Различия между IDS и IPS

| IDS | IPS |
| --- | --- |
| ➢Фиксирует подозрительные действия и шлет оповещения | ➢Активно реагирует на подозрительные действия |
| ➢Сама не защищает ресурсы | ➢Защищает ресурсы сети |
| ➢Не воздействует на атакующего | ➢Может воздействовать на атакующего |
| ➢Состояние системы не изменяется | ➢Состояние системы может меняться |
| ➢**Пассивная** система | ➢**Активная** система |

# Firewall – порт-ловушка («Honeypot»)

- Неиспользуемый well known service порт вызывает бан при попытке подключения.

Connect to TCP 3389 ? → Blacklist

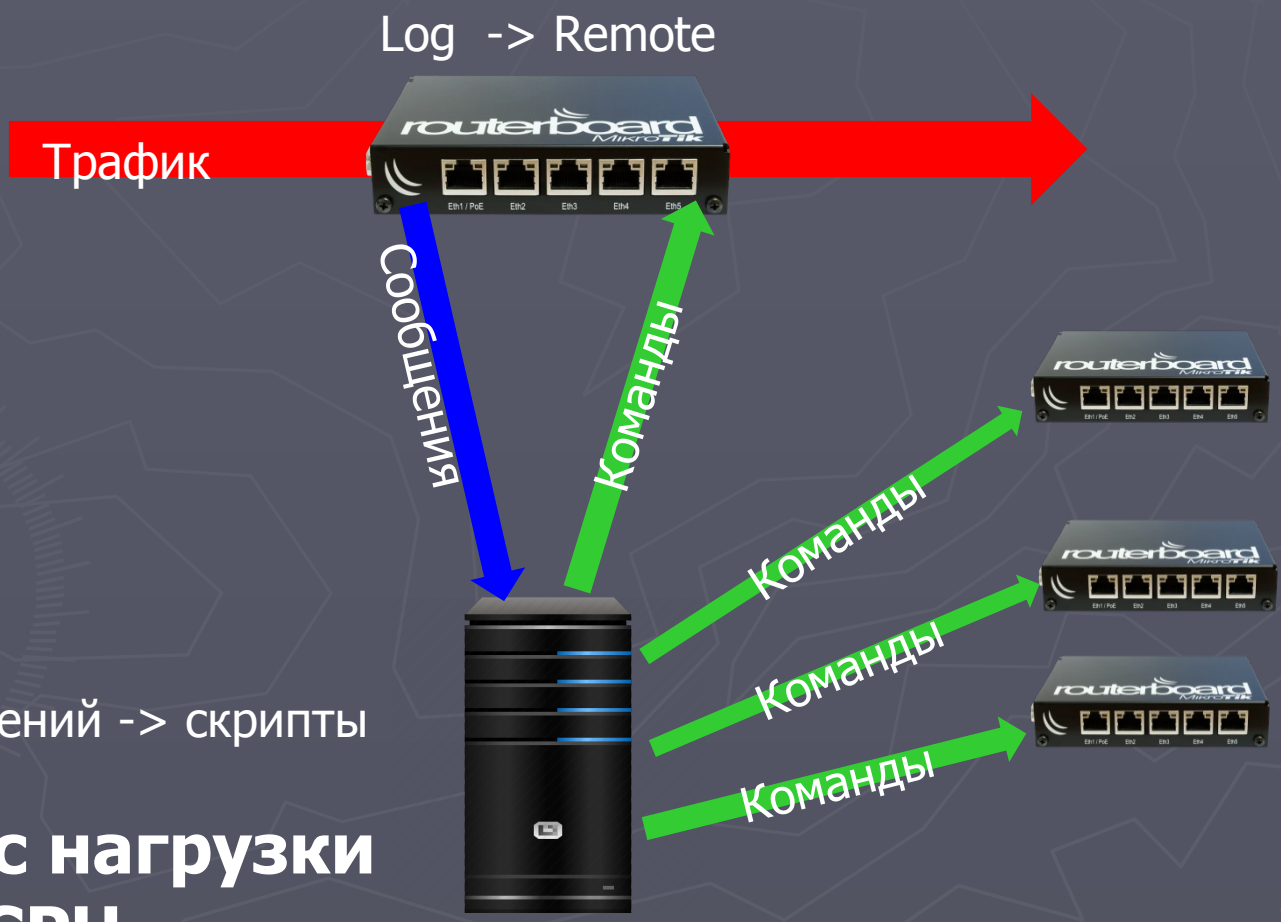
Заносим Src-IP в Address-List “Blacklist”

Время присутствия выбираем согласно своей политике безопасности

```
/ip firewall filter add action=add-src-to-address-list address-list=blacklist address-list-timeout=0s  chain=input protocol=tcp dst-port=3389 comment=“RDP cracker"
```

# Распределение функций

Экономим ресурсы процессора, делегируя функции

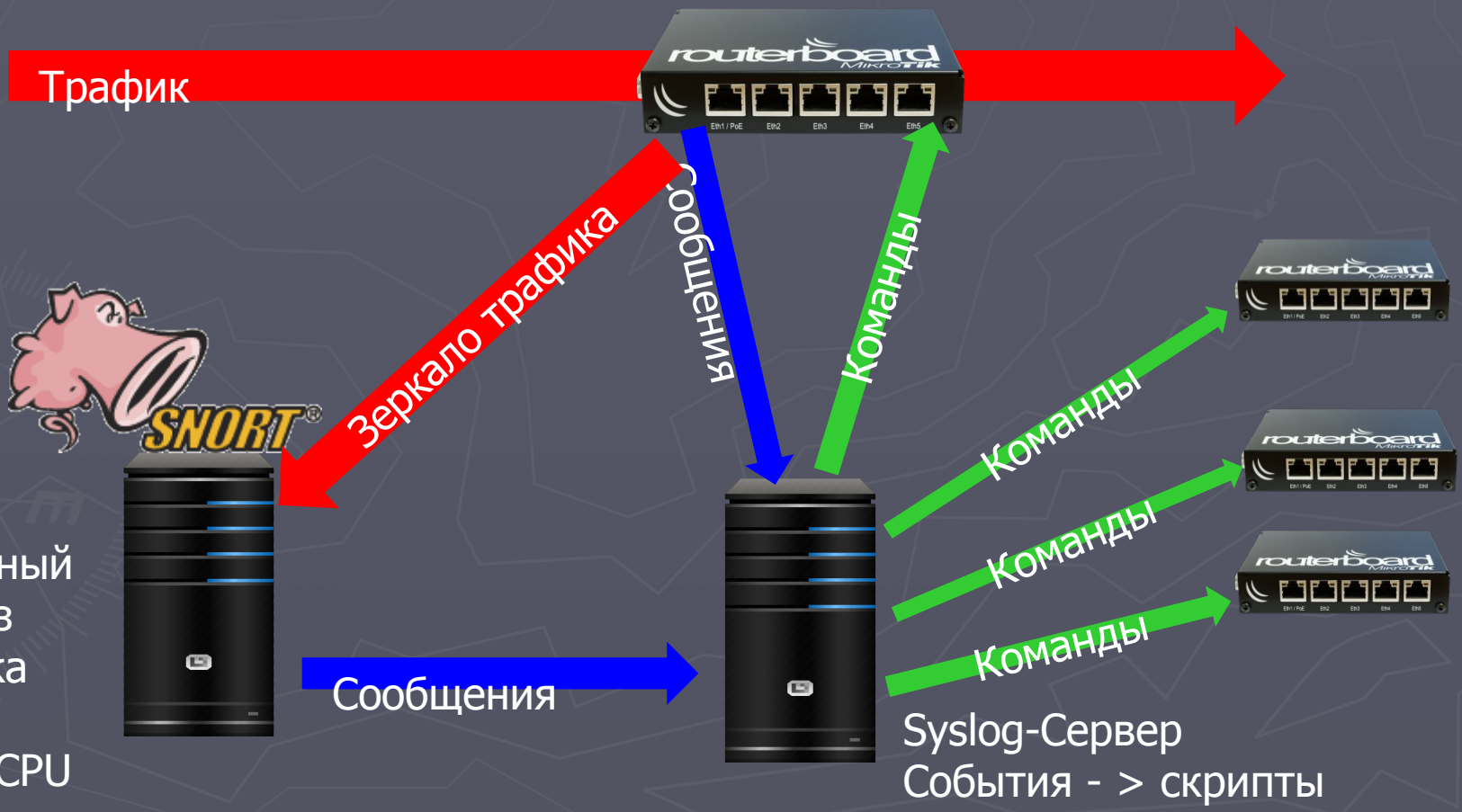



Syslog-Сервер
Анализ сообщений -> скрипты

**Перенос нагрузки CPU**

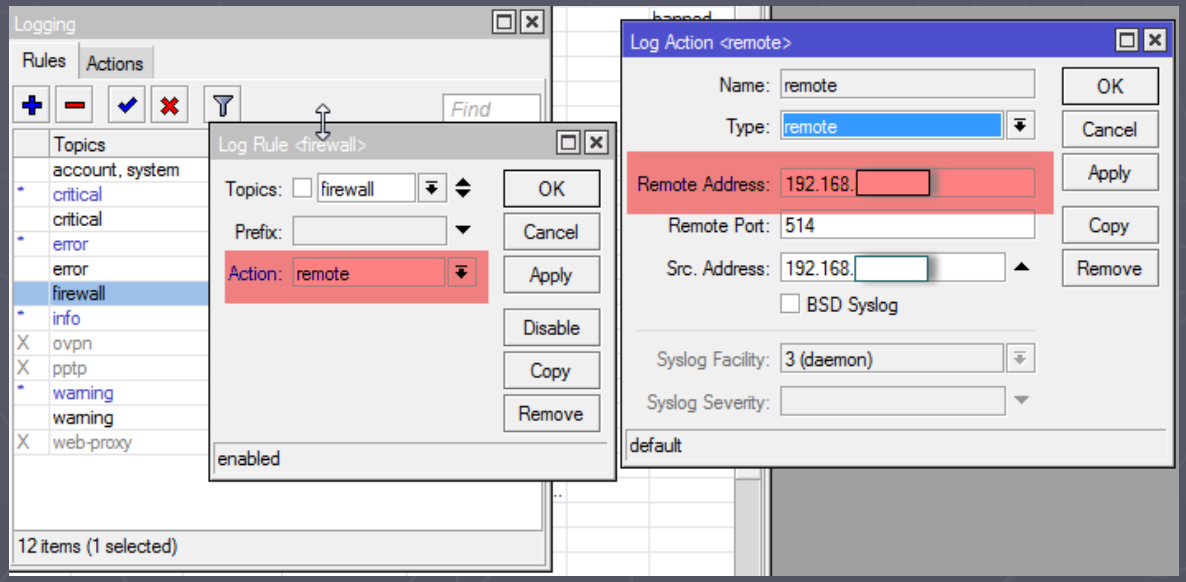
# Распределение функций

Экономим ресурсы процессора, делегируя функции



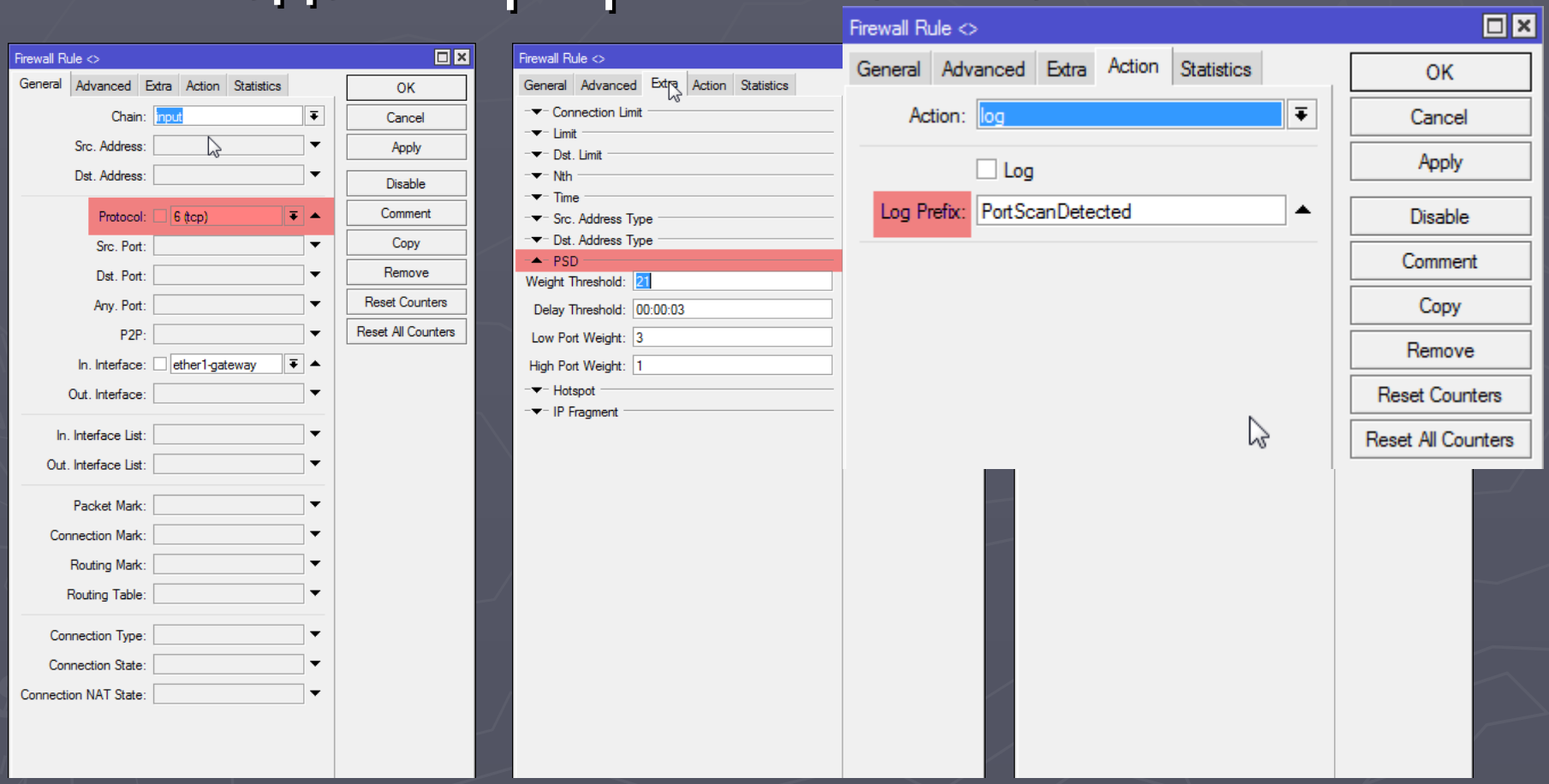
# Обработка событий

## Направляем данные в syslog-сервер:

# Обработка событий

## задаем префикс «PortScanDetect»



# Обработка событий сервером

Будет запущен bash-скрипт “/usr/sbin/onportscan.sh”

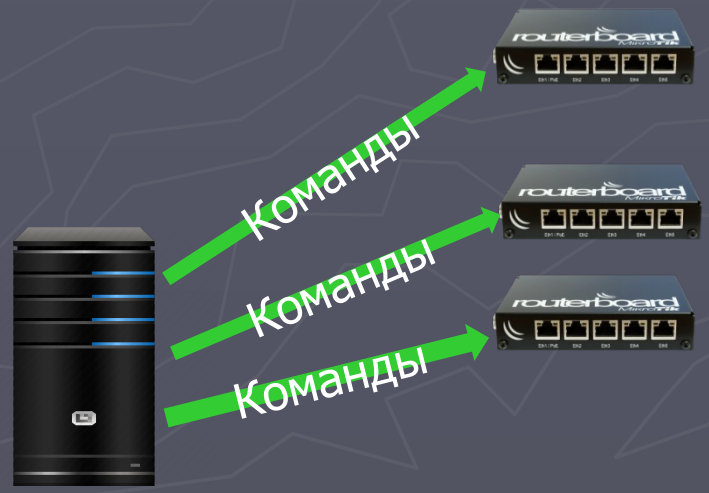
► /etc/rsyslog.conf

```
#### GLOBAL DIRECTIVES ####
$template RFC3164fmt,"<%PRI%>%TIMESTAMP% %HOSTNAME% %syslogtag%%msg%"

#### RULES ####
:msg, contains, “PortScanDetect" ^/usr/sbin/onportscan.sh;RFC3164fmt
```

Из скрипта запускаем что хотим:

- ✓Ansible
- ✓Curl, ssh@host
- ✓SMS, e-mail
- ✓Другие скрипты



# Конкурс HackMe

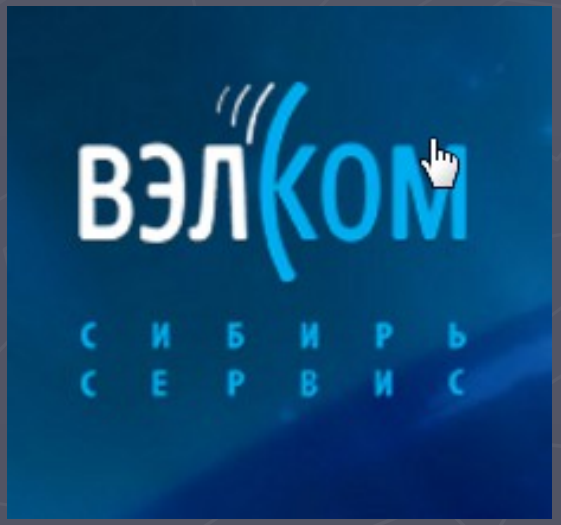
Задача: войти на устройство по WiFi с администраторскими правами и создать пользователя со своим логином

ssid: hackme

MikroTik IP: 192.168.88.1

Login: user

No password



# Ссылки

- http://wiki.mikrotik.com – Документация от вендора
- https://www.shodan.io – Поисковик уязвимых устройств
- http://wireshark.org – Пакетный сниффер
- http://www.snort.org – Snort IDS
- https://www.nmap.org – Сканер nmap
- https://vk.com/mikrotik_os – Группа пользователей
- Http://forum.nag.ru – Форум по сетевым технологиям
- info@mikrotik-sibir.ru – Мой e-mail