Безопасность в MikroTik
(записки параноика)

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

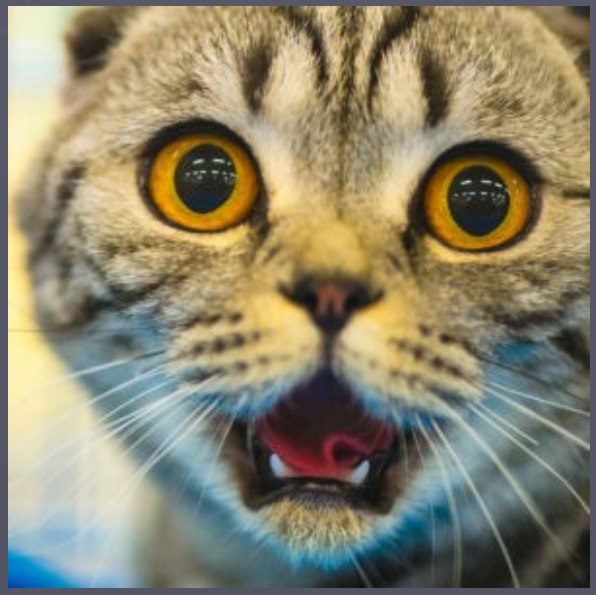
Безопасность

- 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



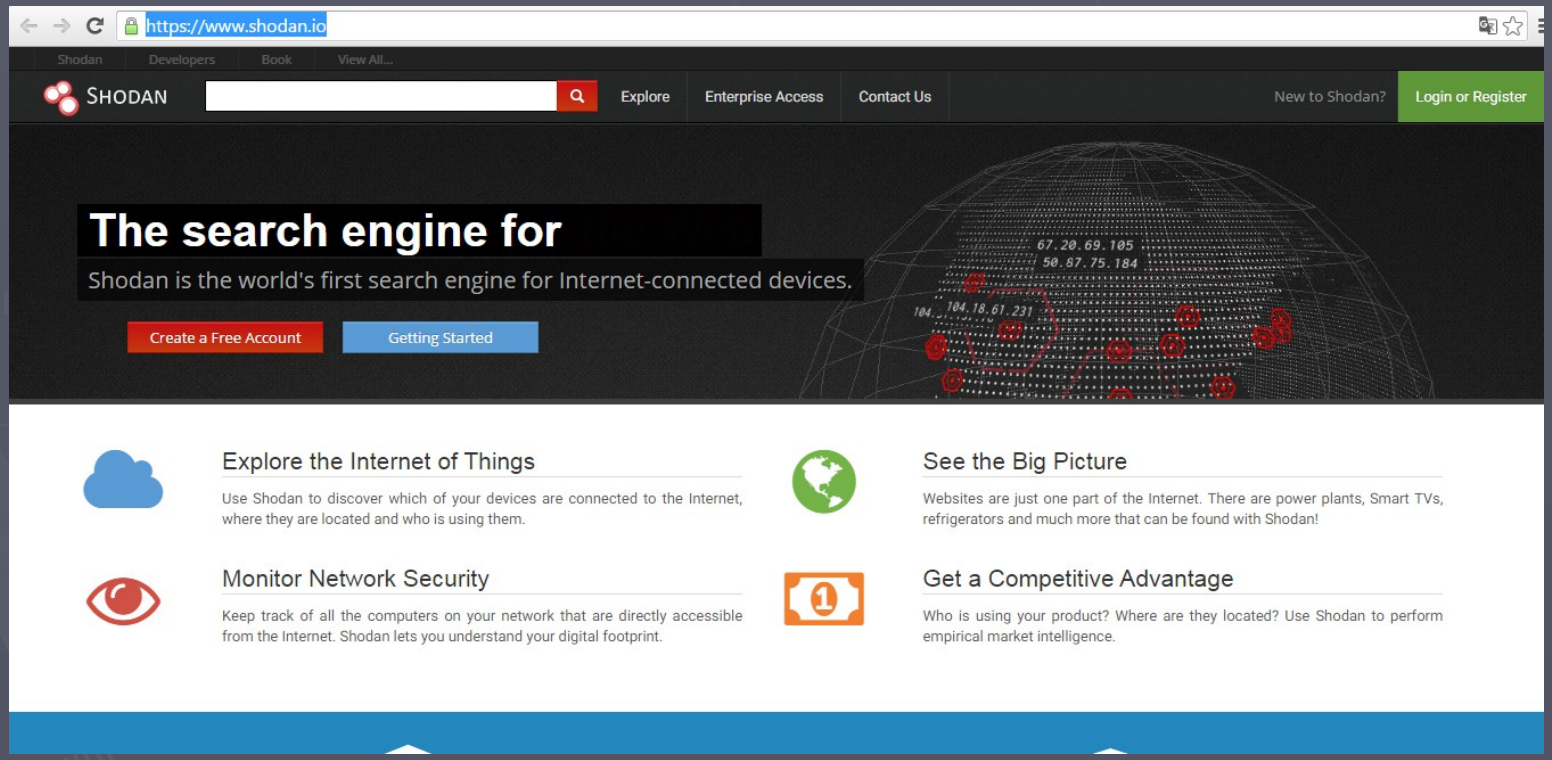
Инструменты

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

- ✓ Some bruteforce tools to get passwords

Инструменты

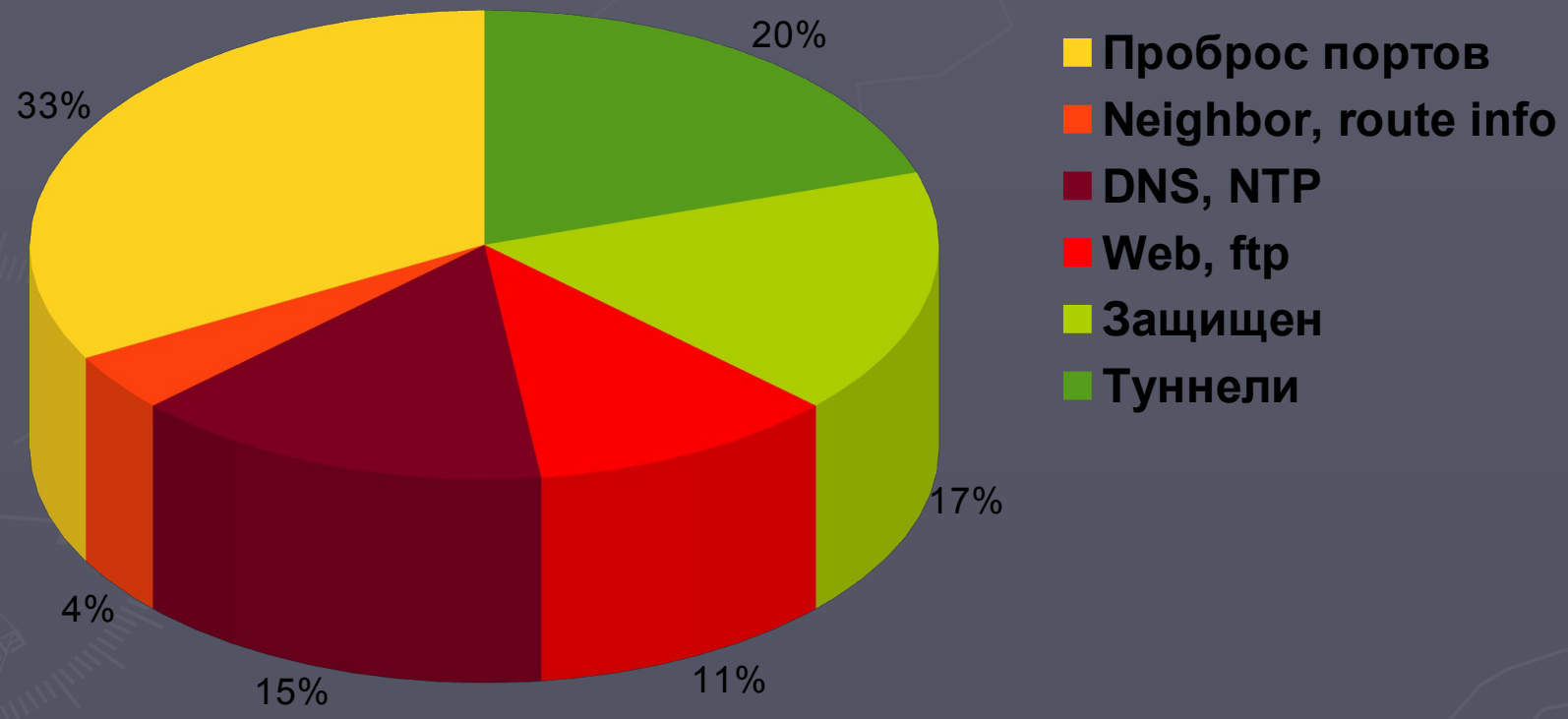
- ✓ https://www.shodan.io/



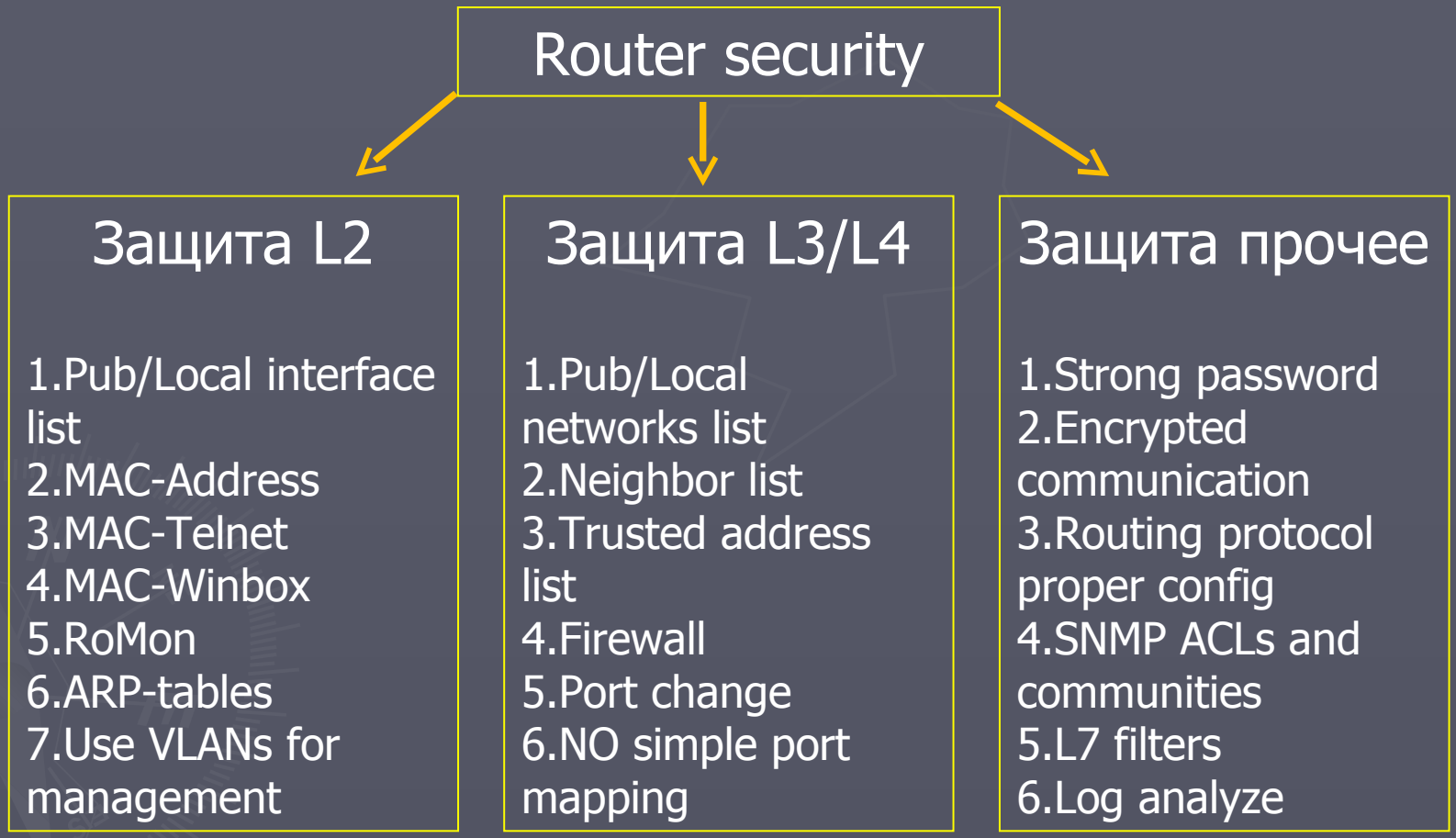
Чек-лист (what about You?)

- 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”?

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.

(*/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.
   (*/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!

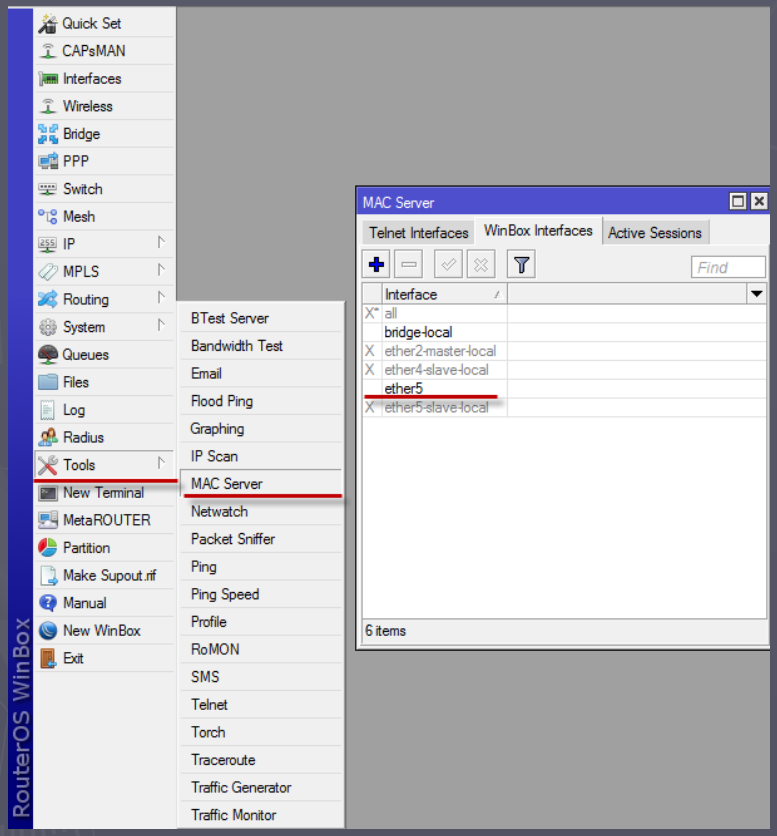
Внешний интерфейс
MAC-Telnet
ВЫКЛЮЧИТЬ!

Внешний интерфейс
Mac-Winbox
ВЫКЛЮЧИТЬ!

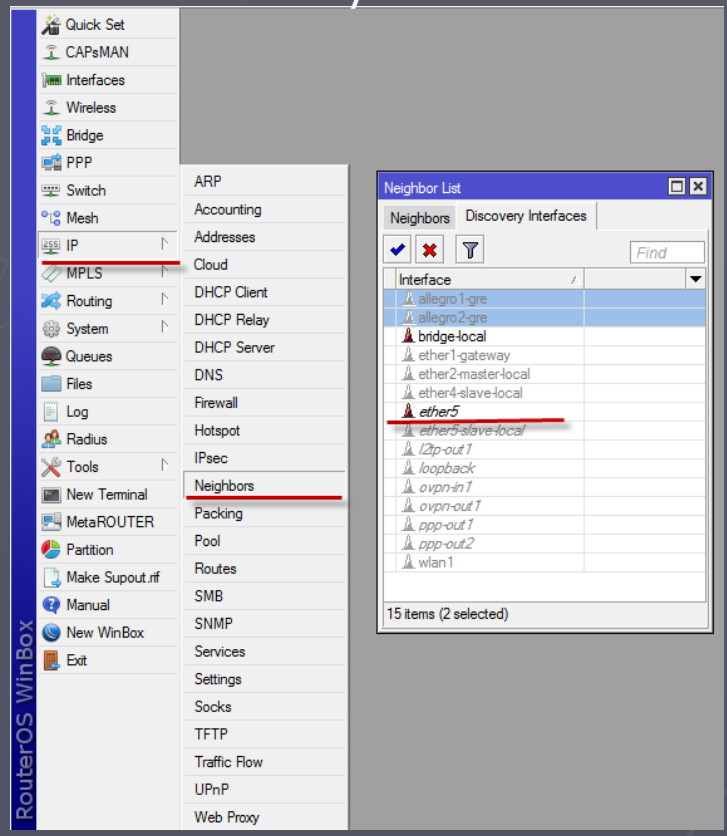
Защита каждого L2-интерфейса

Ahtung! По умолчанию Discovery ВКЛЮЧЕН на каждом новом интерфейсе.

MAC-services



Discovery services



Neighbor – утечка информации

Neighbor service распространяет информацию:

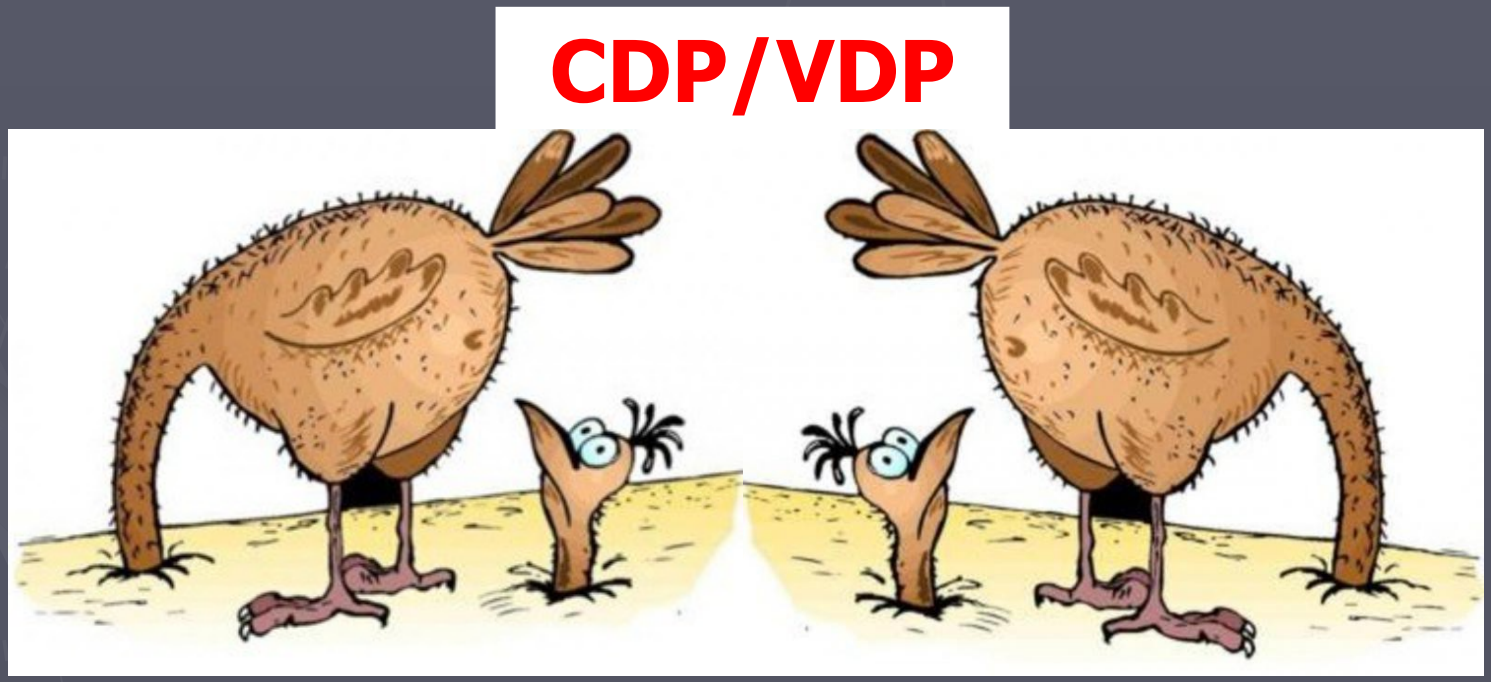
- О модели устройства;
- О версии OS;
- О MAC и IP адресах;
- Об UpTime, наличии IPv6 и прочее

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

Neighbor – утечка информации

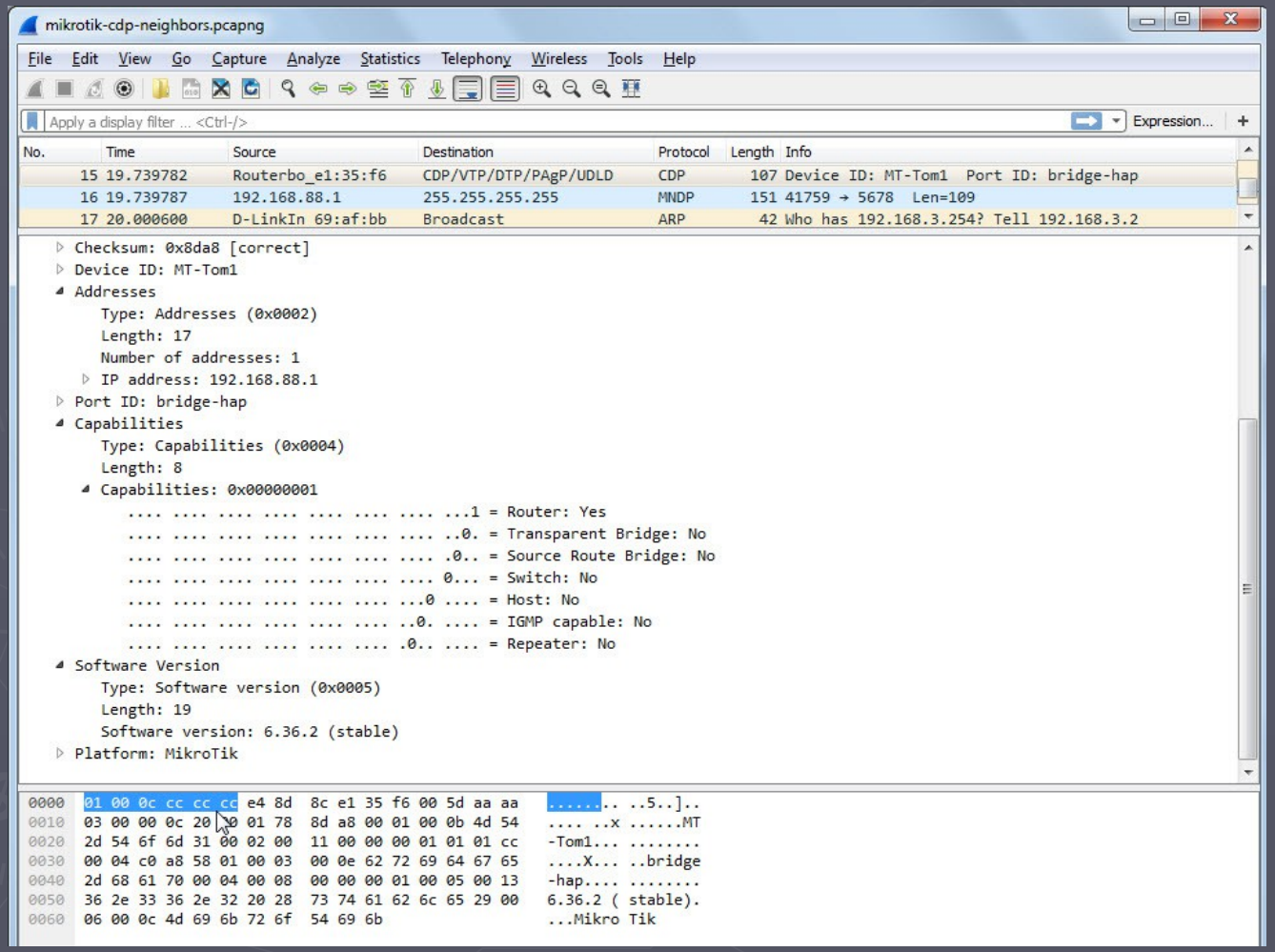
Желающие подсмотреть за соседями по сети делают так: ☺

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



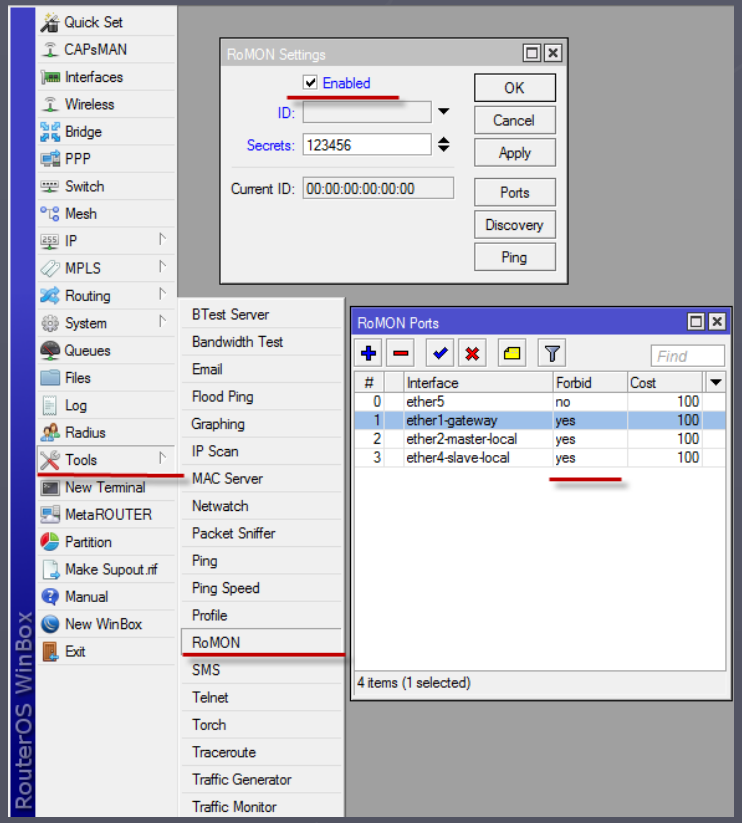
Neighbor – CDP протокол L2

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



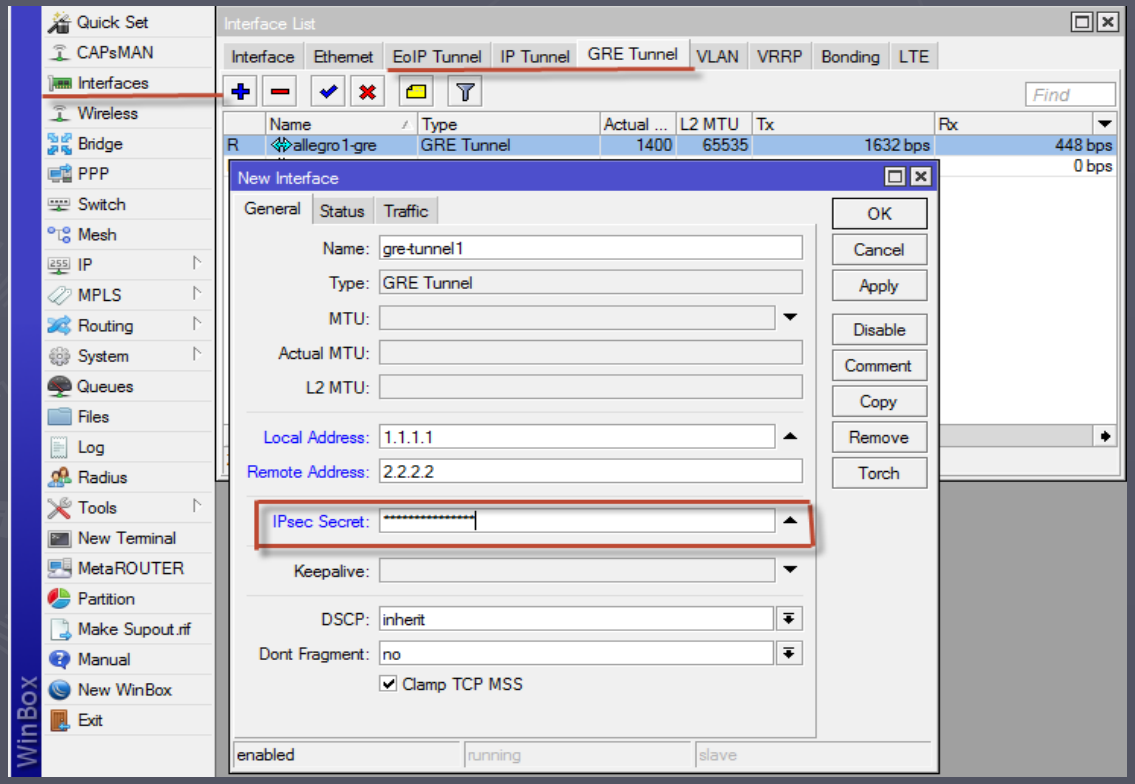
Безопасность L2 & MAC

1. Убедитесь, что служба RoMon ВЫКЛЮЧЕНА на внешних интерфейсах, т.к firewall может не помочь



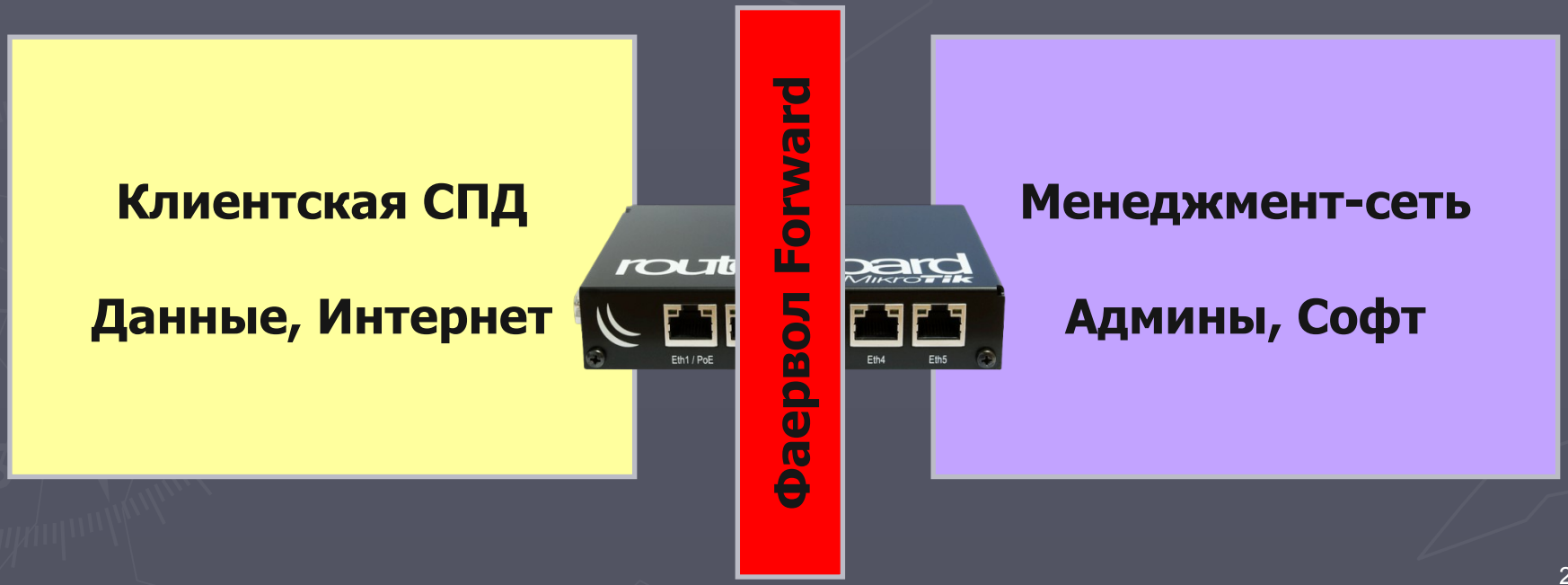
Защита туннелей EoIP/GRE/IPIP

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



Безопасность L3. Ресурсы сетей

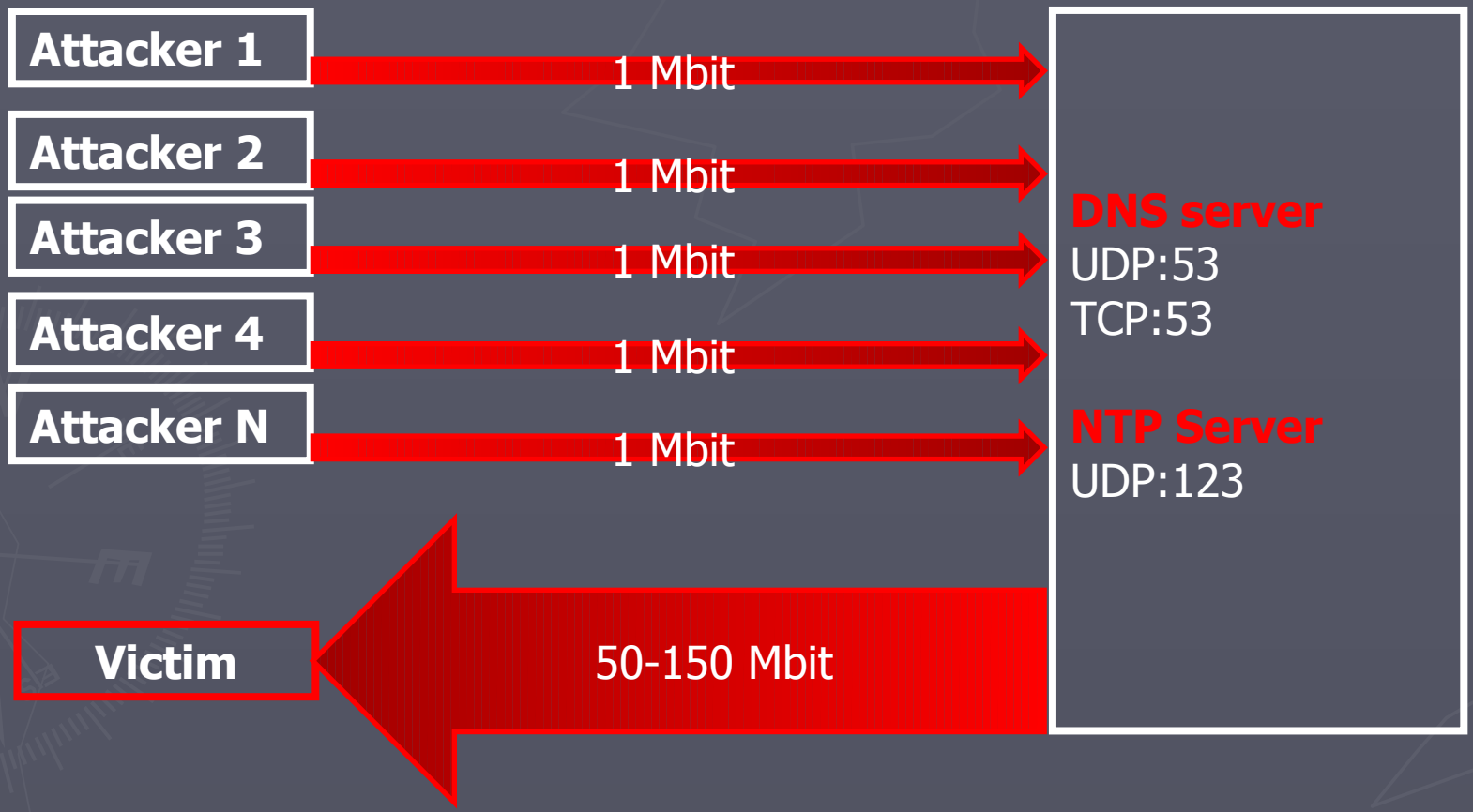
1. Убедитесь, что внешние интерфейсы НЕ соединяются в бридж с доверенными интерфейсами управления
2. Проверьте настройки фаервола, для исключения форвардинга в management-подсеть.



Защита служб L3/L4
UDP magnification attack

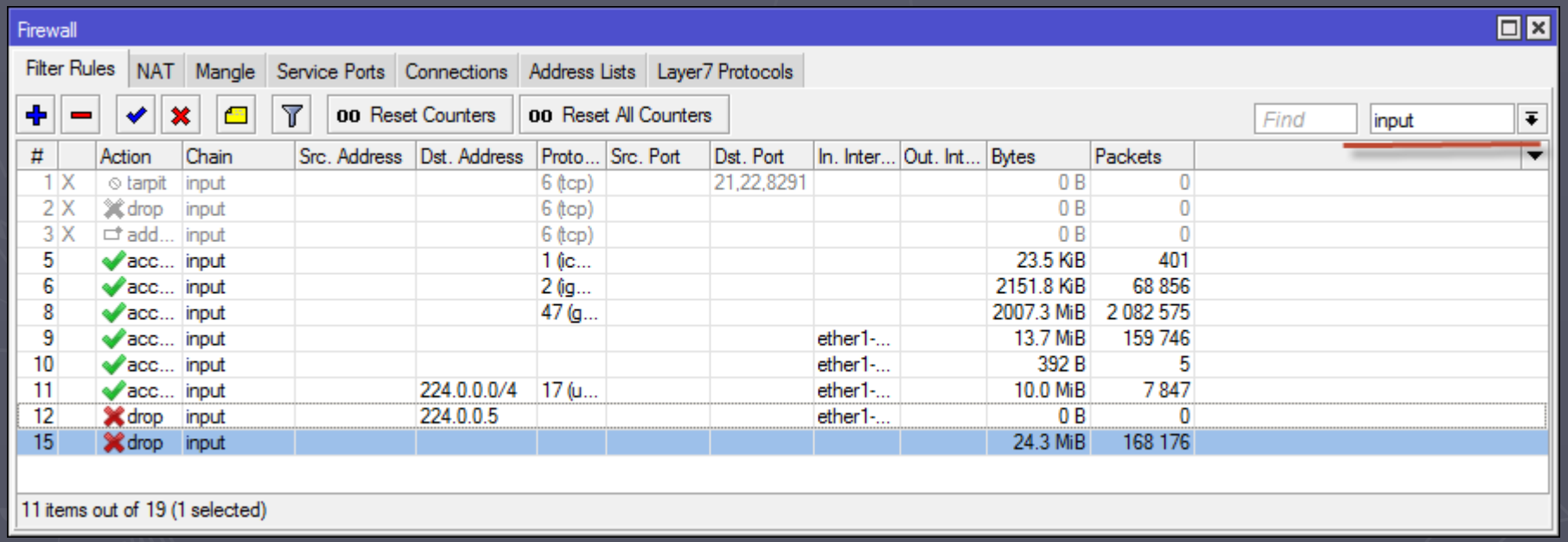
1. Злодей отправляет UDP-запрос с SRC IP-address жертвы
2. DNS/NTP сервер отвечает большим UDP-пакетом жертве
3. Жертва попадает под DDoS-атаку большими UDP-пакетами от сервера MikroTik, с 53 или 123 порта

Защита служб L3/L4
UDP magnification attack



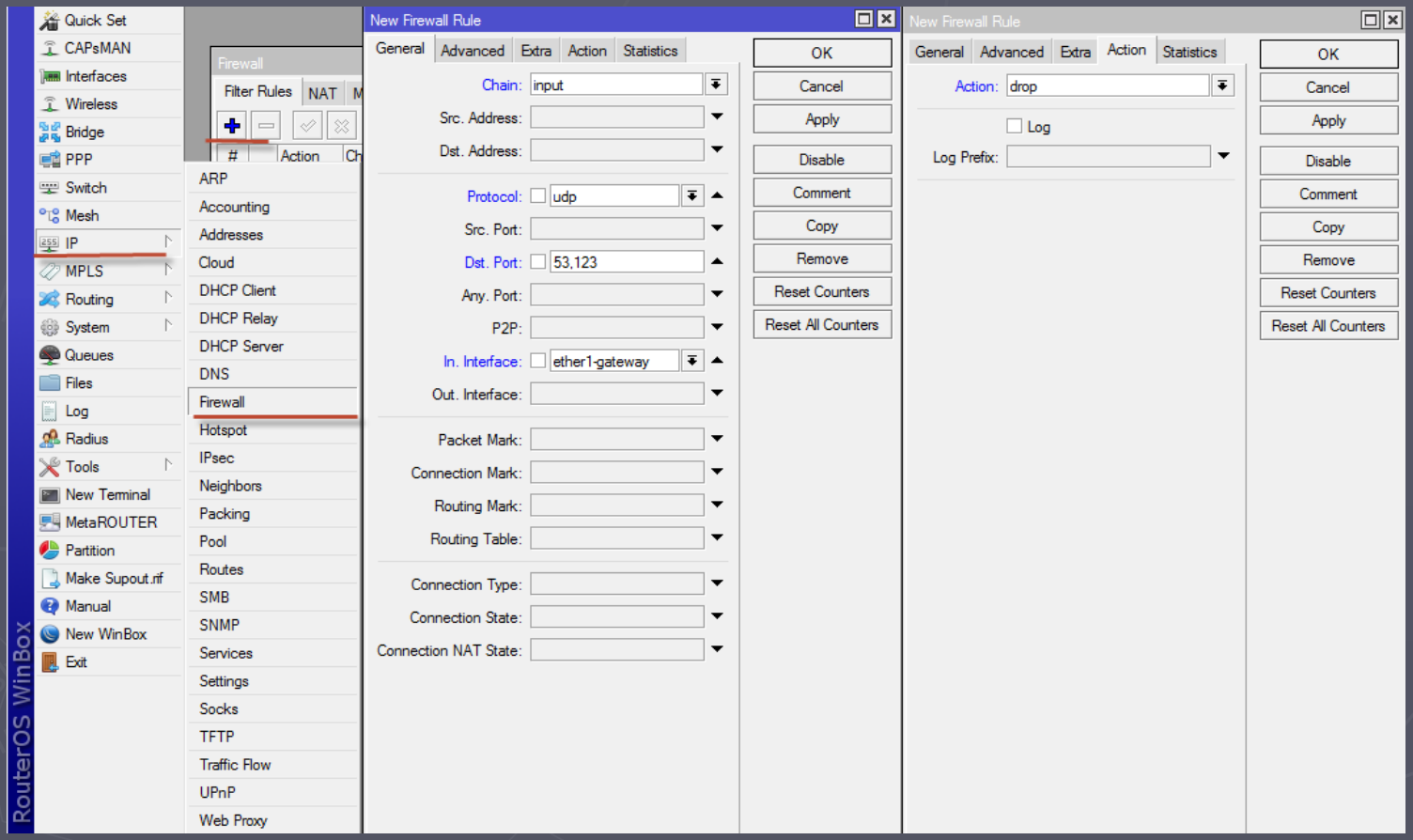
Защита служб L3/L4
Фаерволл по-умолчанию

- Рекомендуется закрывать всё, что явно не разрешено



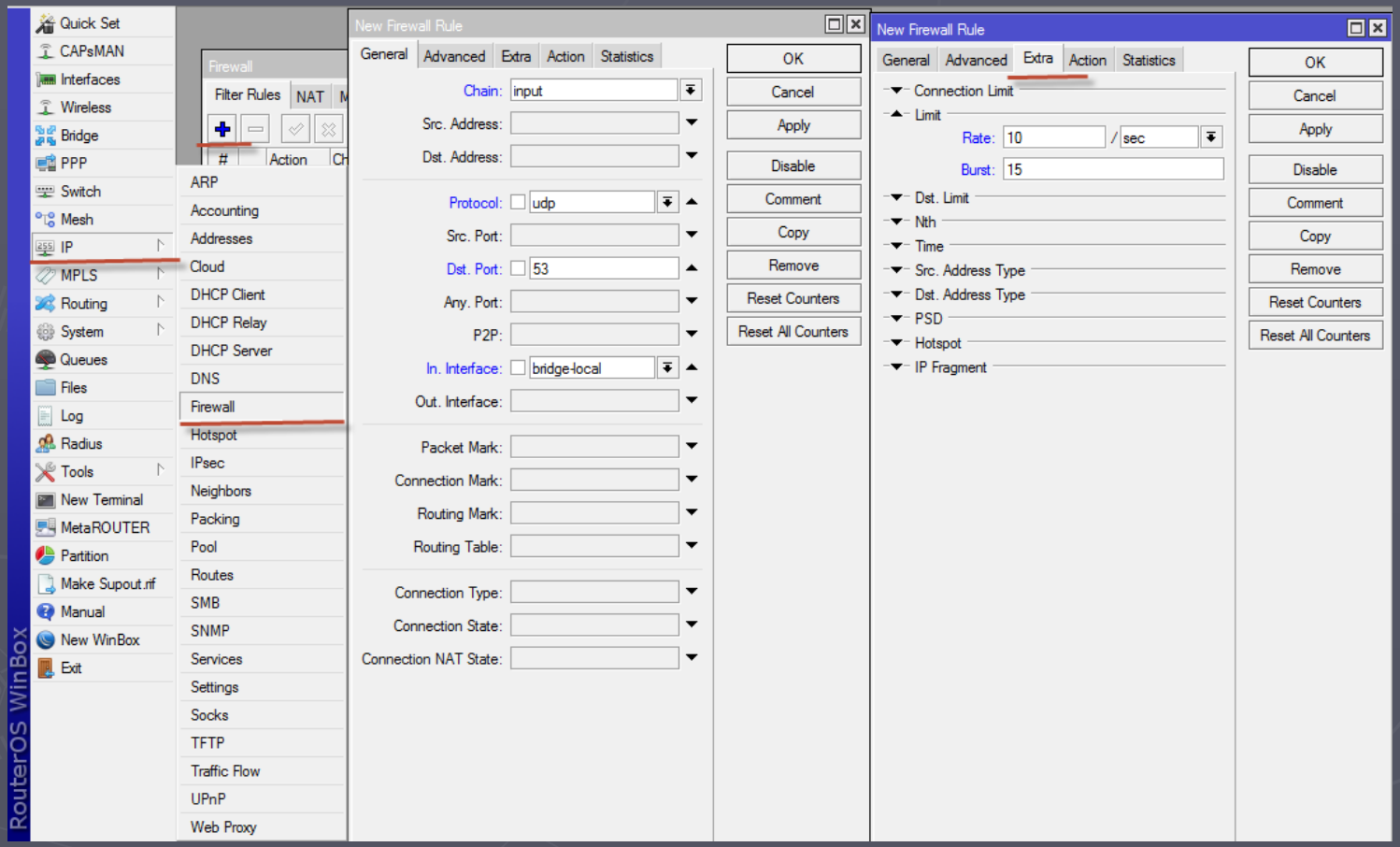
Защита служб L3/L4
UDP magnification attack solution

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



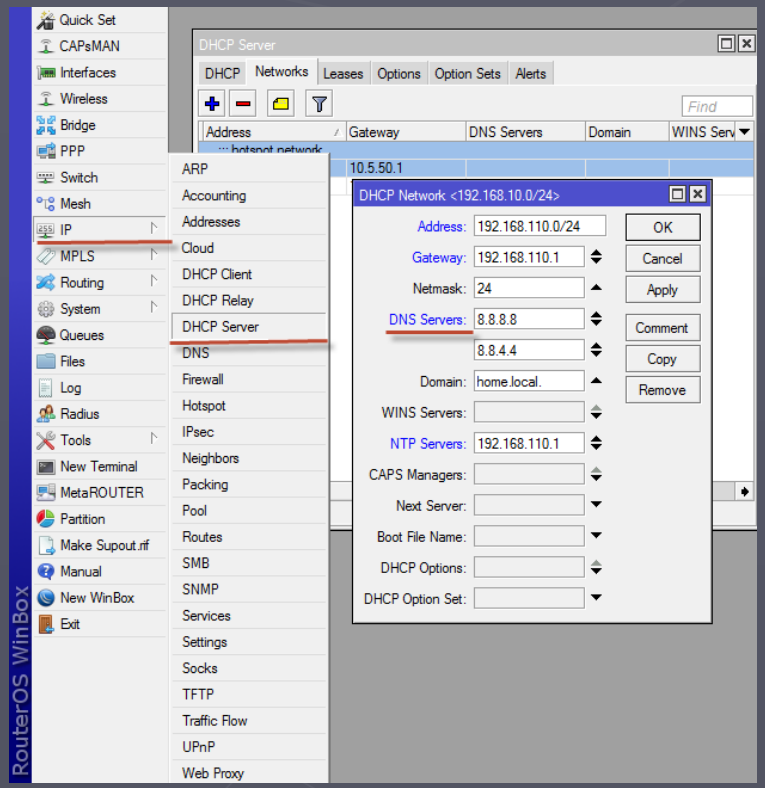
Защита служб L3/L4
UDP magnification attack solution

- Ограничить трафик на udp:53 udp:123 фаерволом



Защита служб L3/L4
UDP magnification 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”?

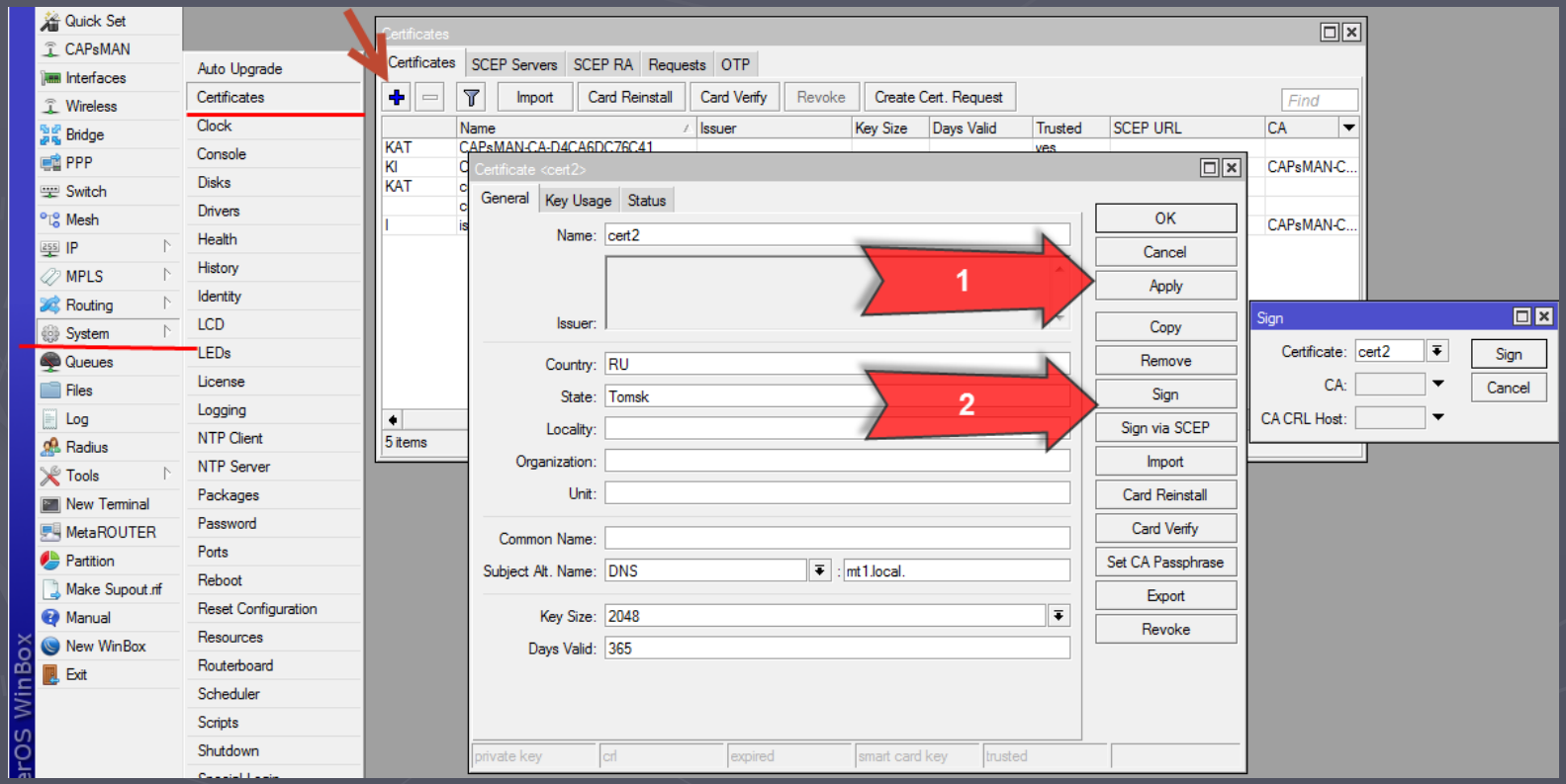
Приглашение для подбора паролей?

Залить script.rsc.auto?

Защита WebFig и API

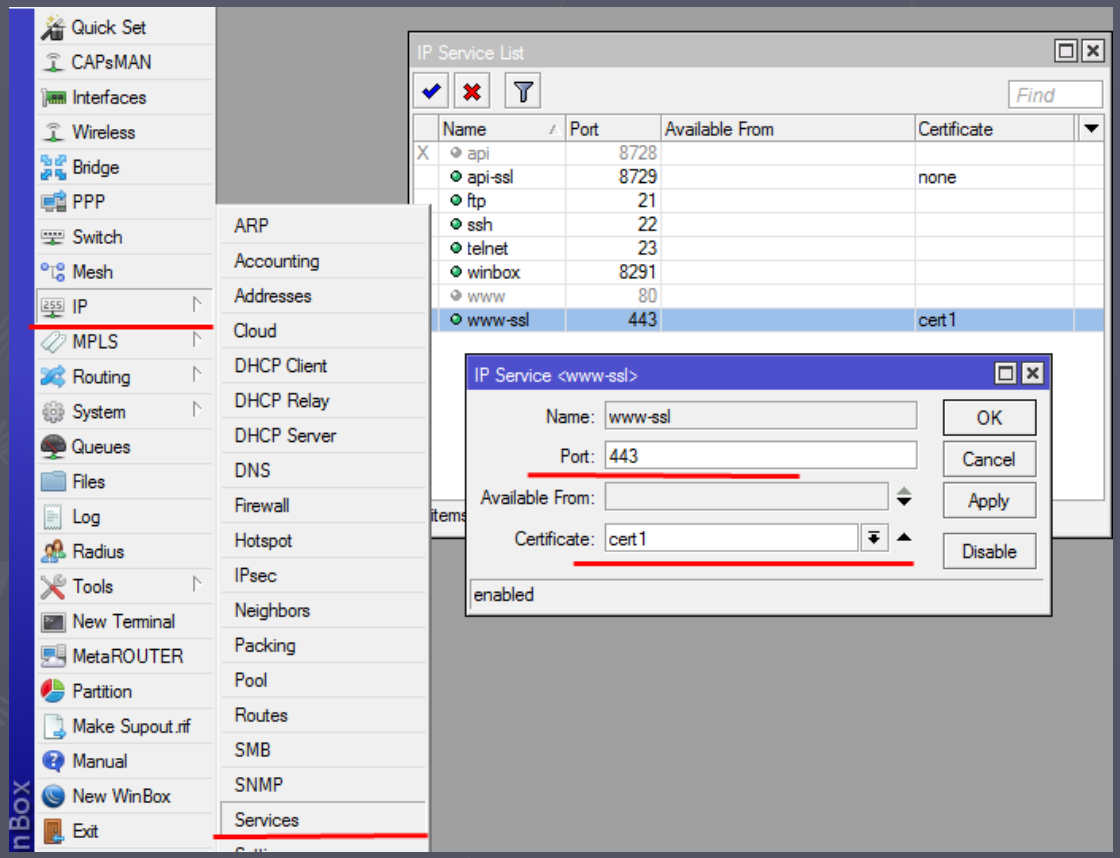
- Http передает данные в открытом виде
- HttpS по-умолчанию не работает

Для работы HTTPS нужен сертификат. Любой ☺



Защита WebFig и API

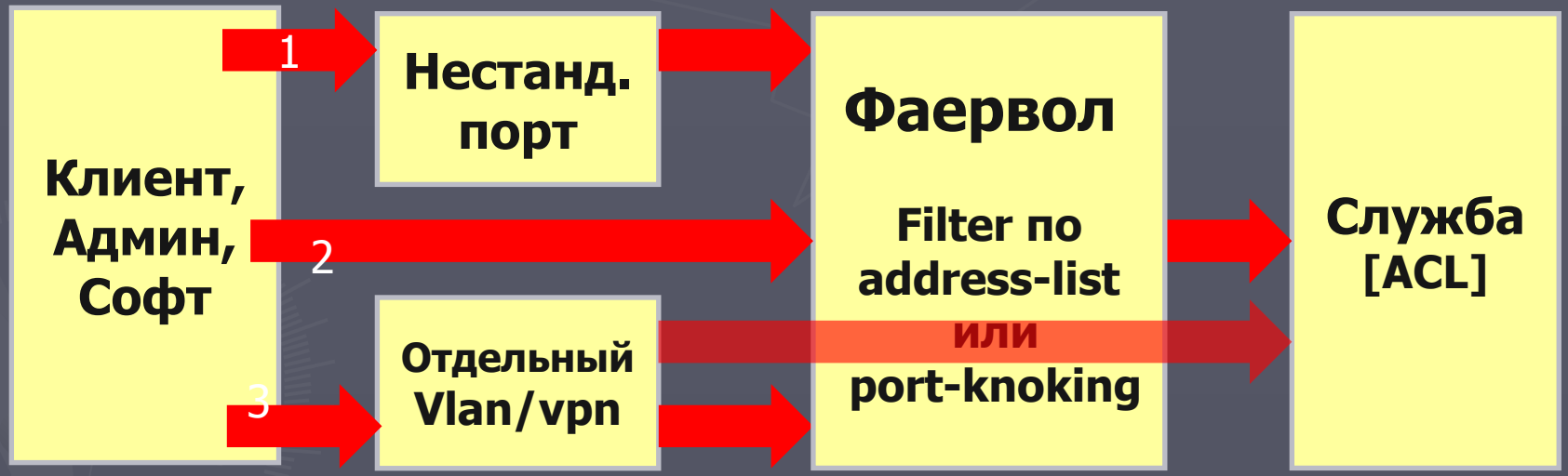
- Устанавливаем сертификат к службе, меняем порт



Защита служб

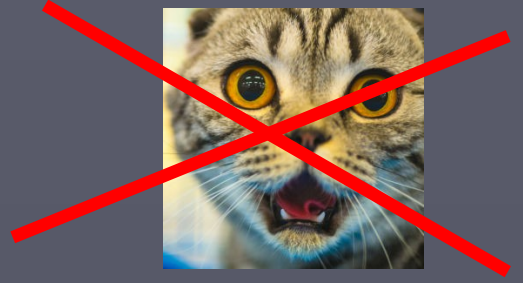
Схема доступа для настоящих админов ☺

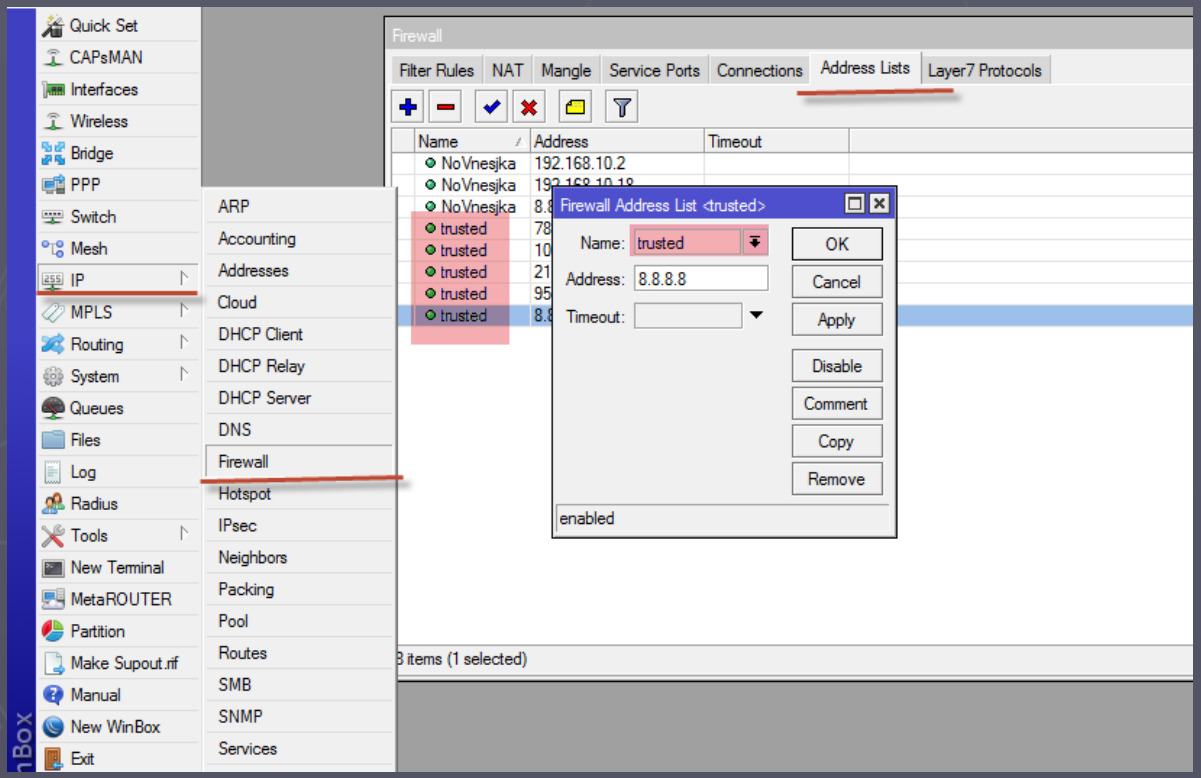
Собственная ACL сервиса может иметь уязвимости.



Firewall – проброс портов

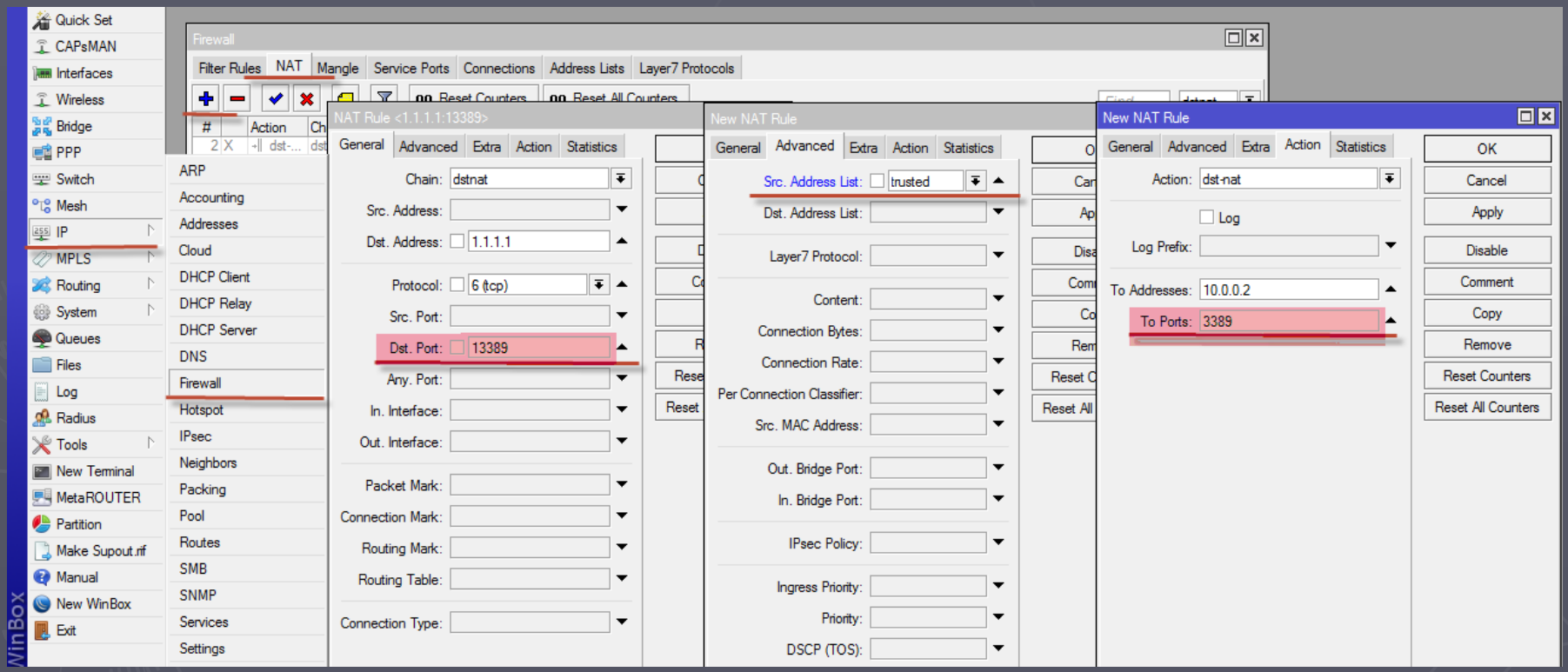
- DST-NAT + Address-List
- Forward + Address-List





Firewall – проброс портов

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



Firewall – прячем инфо о системе

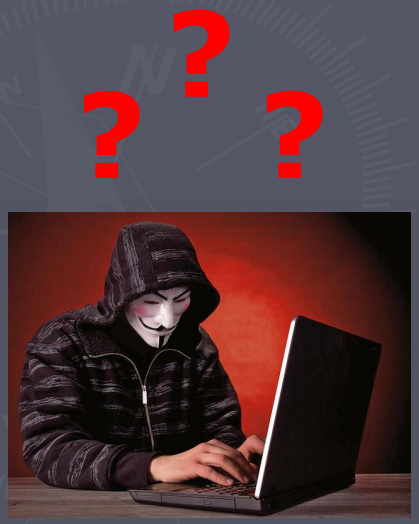
- NetMap – Сканер безопасности.
- Пытается определять версию ОС Оценивает служебные поля, размеры кадров и прочую служебную информацию

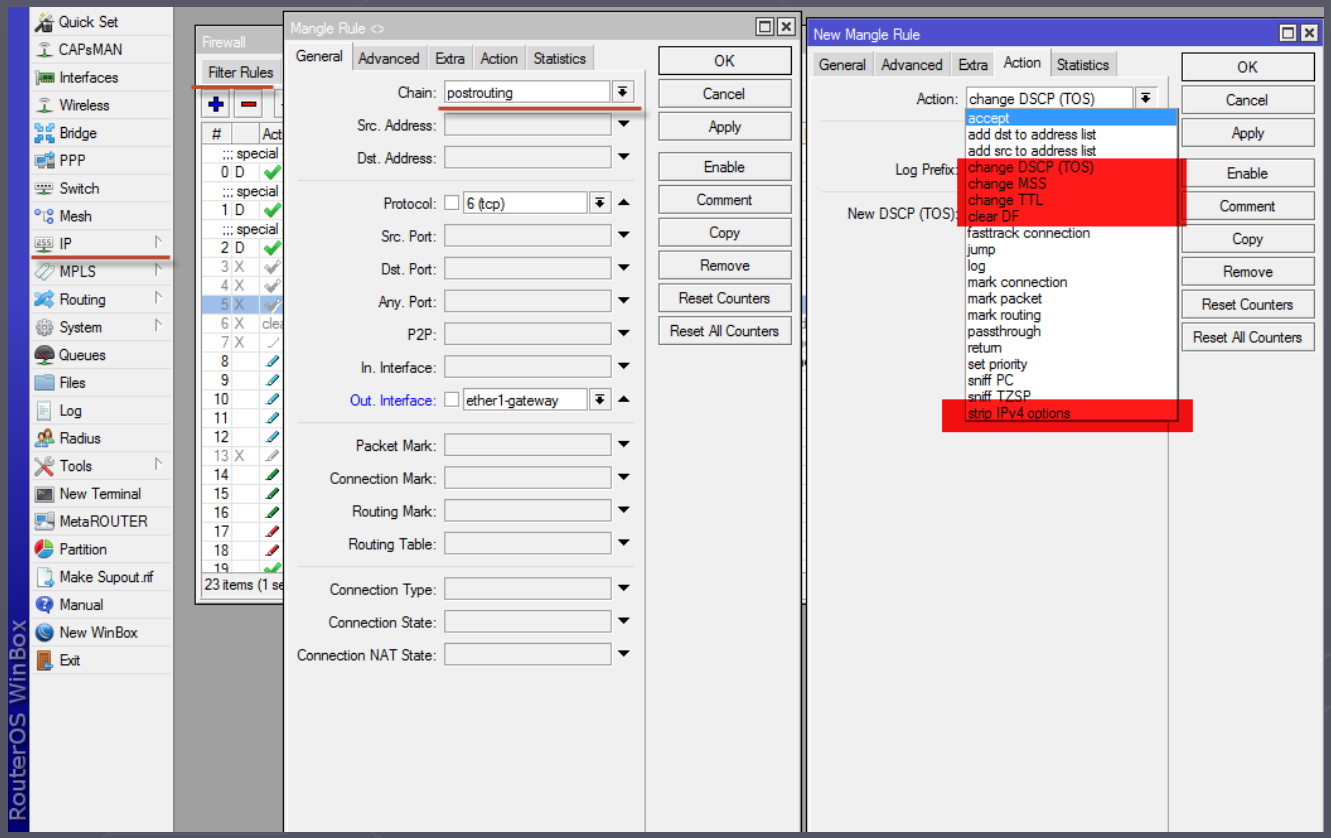
Скрываем версию системы. Изменяем поля:

TTL , DSCP/TOS, DF, IPv4 Options

Firewall – прячем инфо о системе

Скрываем версию системы и платформы хостов в сети.
Изменяем поля: TTL , DSCP/TOS, DF, IPv4 Options





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

- 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"
```

Firewall – fail2ban

- Защищаем простой почтовик на винде от брутфорса POP3.


```
/ip firewall filter add chain=forward action=add-dst-to-address-list protocol=tcp /
    address-list=BlackList address-list-timeout=120s src-port=110  /
content=-ERR Authentication failed log=no  log-prefix=""
```

Firewall – fail2ban

- Защищаем простой почтовик на винде от брутфорса POP3.

```
/ip firewall  filter  add chain=forward action=add-dst-to-address-list protocol=tcp /
dst-address-list=Pop3_stage3 address-list=BlackList address-list-timeout=0s src-port=110 /
content=-ERR Authentication failed log=no log-prefix=""

/ip firewall  filter add chain=forward action=add-dst-to-address-list protocol=tcp /
dst-address-list=Pop3_stage2 address-list=Pop3_stage3 address-list-timeout=1m src-port=110  /
    content=-ERR Authentication failed log=no log-prefix=""

/ip firewall  filter add chain=forward action=add-dst-to-address-list protocol=tcp /
dst-address-list=Pop3_stage1 address-list=Pop3_stage2 address-list-timeout=1m src-port=110 /
    content=-ERR Authentication failed log=no log-prefix=""

/ip firewall  filter add chain=forward action=add-dst-to-address-list protocol=tcp /
address-list=Pop3_stage1 address-list-timeout=1m src-port=110 /
content=-ERR Authentication failed log=no log-prefix=""
```

Firewall – fail2ban

- Защищаем простой почтовик на винде от брутфорса POP3.

```
/ip firewall  filter  add chain=forward /
action=add-dst-to-address-list protocol=tcp /
dst-address-list=Pop3_stage3 address-list=BlackList /
   address-list-timeout=0s src-port=110 /
content=-ERR Authentication failed log=no log-prefix=""
```

Правило финального бана. На сколько времени банит?

address-list-timeout=0s

Firewall – fail2ban

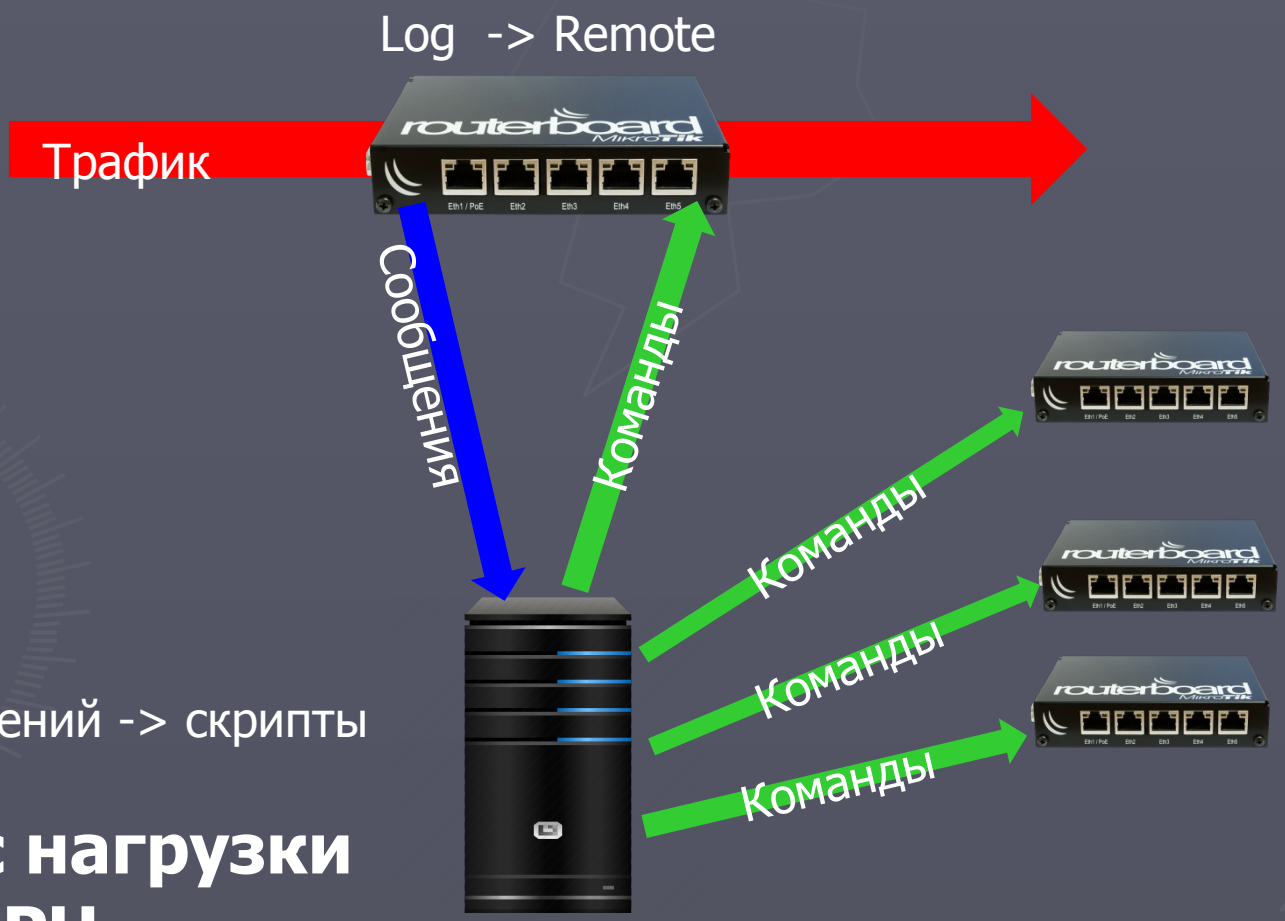
- Приклеиваем пойманных тараканов навсегда ☺

1. Берем по одному адреса из dynamic-list
2. Добавляем по одному в static-list

- ```
  :foreach i in=[/ip firewall addr find list=dynamic-list ] \
    do= {  :set w [/ip fire addr get $i address] ;
       /ip fire add rem [/ip fi add find address=$w] ;
       /ip fire add add list=static-list address=$w }
  ```
  ```

Распределение функций

Экономим ресурсы процессора, делегируя функции

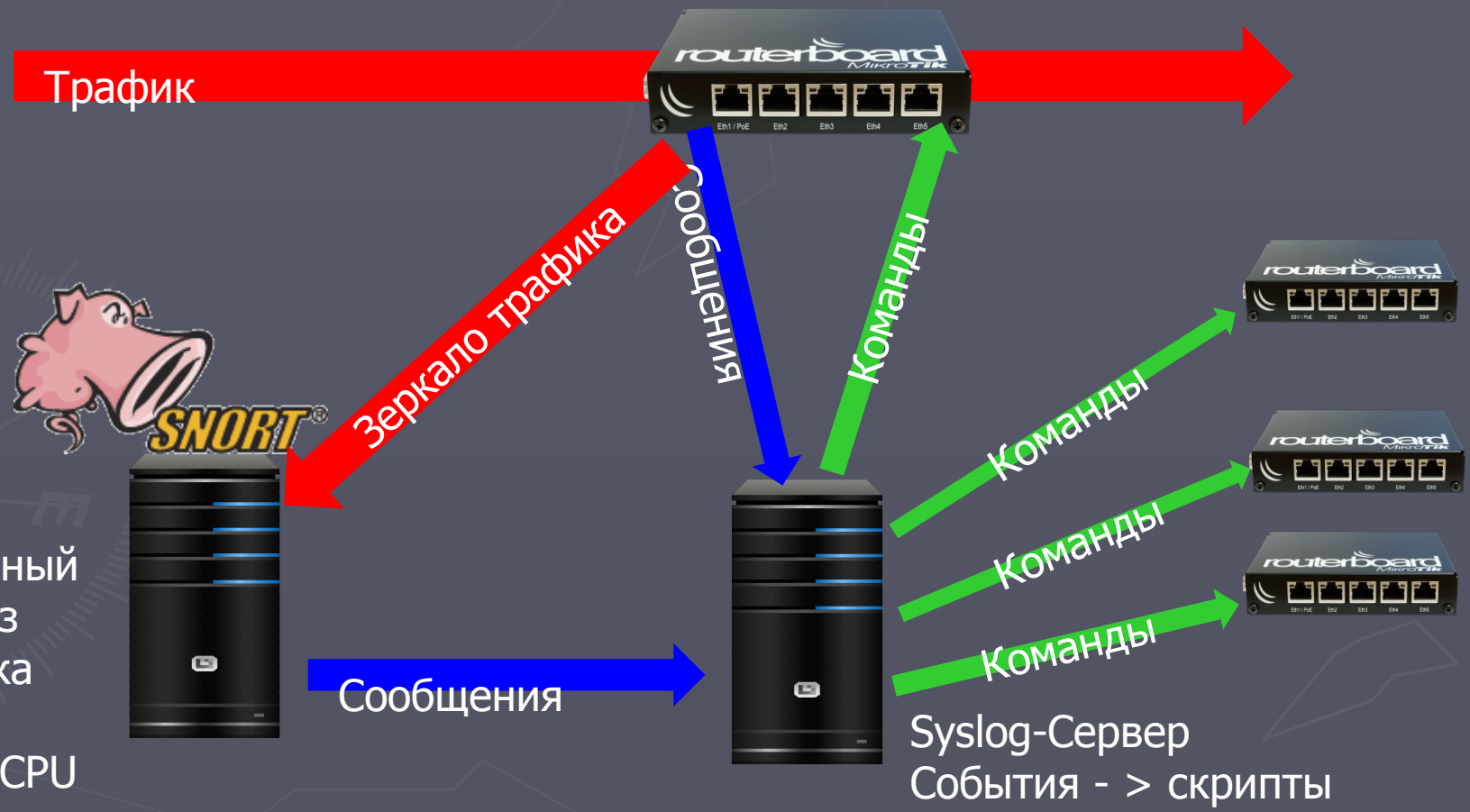


Syslog-Сервер
Анализ сообщений -> скрипты

Перенос нагрузки CPU

Распределение функций

Экономим ресурсы процессора, делегируя функции



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