

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>

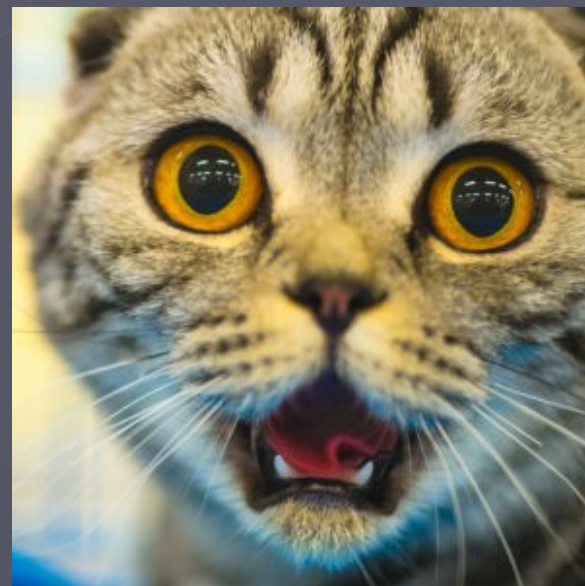
Безопасность

- ▶ 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

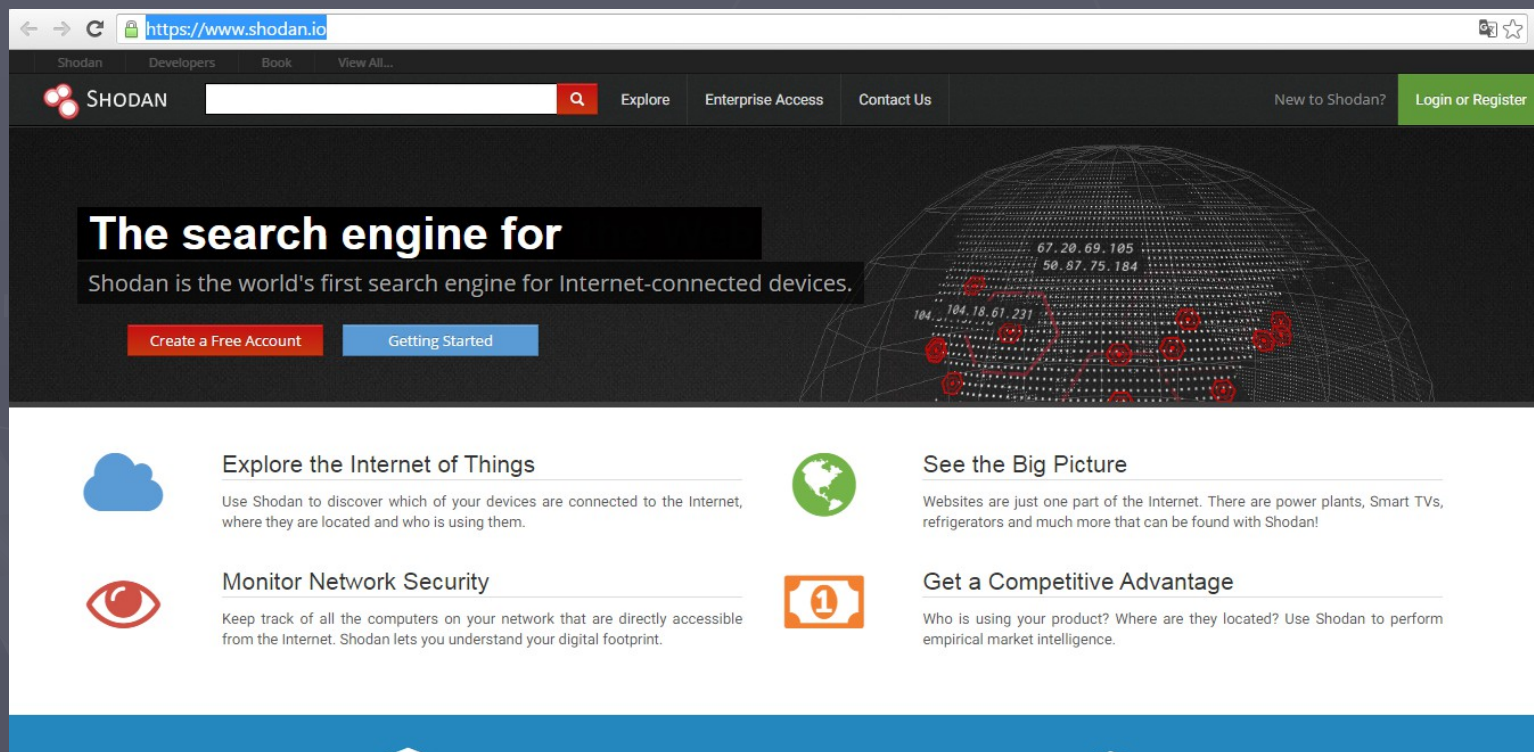


Инструменты

- ✓ NMap
- ✓ WireShark
- ✓ Fing (on android-based smartphone)
- ✓ MikroTik "Torch" tool ☺
- ✓ Some bruteforce tools to get passwords

ИНСТРУМЕНТЫ

✓ <https://www.shodan.io/>



The screenshot shows the Shodan website homepage. At the top, there's a navigation bar with links to Shodan, Developers, Book, and View All... A search bar is prominently displayed with a magnifying glass icon. To the right of the search bar are links for Explore, Enterprise Access, and Contact Us. Further right are links for New to Shodan? and a green button for Login or Register. The main content area features a large banner with the text "The search engine for" in white, followed by "Shodan is the world's first search engine for Internet-connected devices." in a smaller font. Below this text are two buttons: "Create a Free Account" in red and "Getting Started" in blue. The background of the banner shows a wireframe globe with various IP addresses and red circular markers. Below the banner, there are four sections, each with an icon and a title. The first section has a cloud icon and is titled "Explore the Internet of Things". The second section has a globe icon and is titled "See the Big Picture". The third section has an eye icon and is titled "Monitor Network Security". The fourth section has a ticket icon and is titled "Get a Competitive Advantage". Each section contains a brief description of the service.

Shodan Developers Book View All...

SHODAN [Search Bar] Explore Enterprise Access Contact Us New to Shodan? Login or Register

The search engine for

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



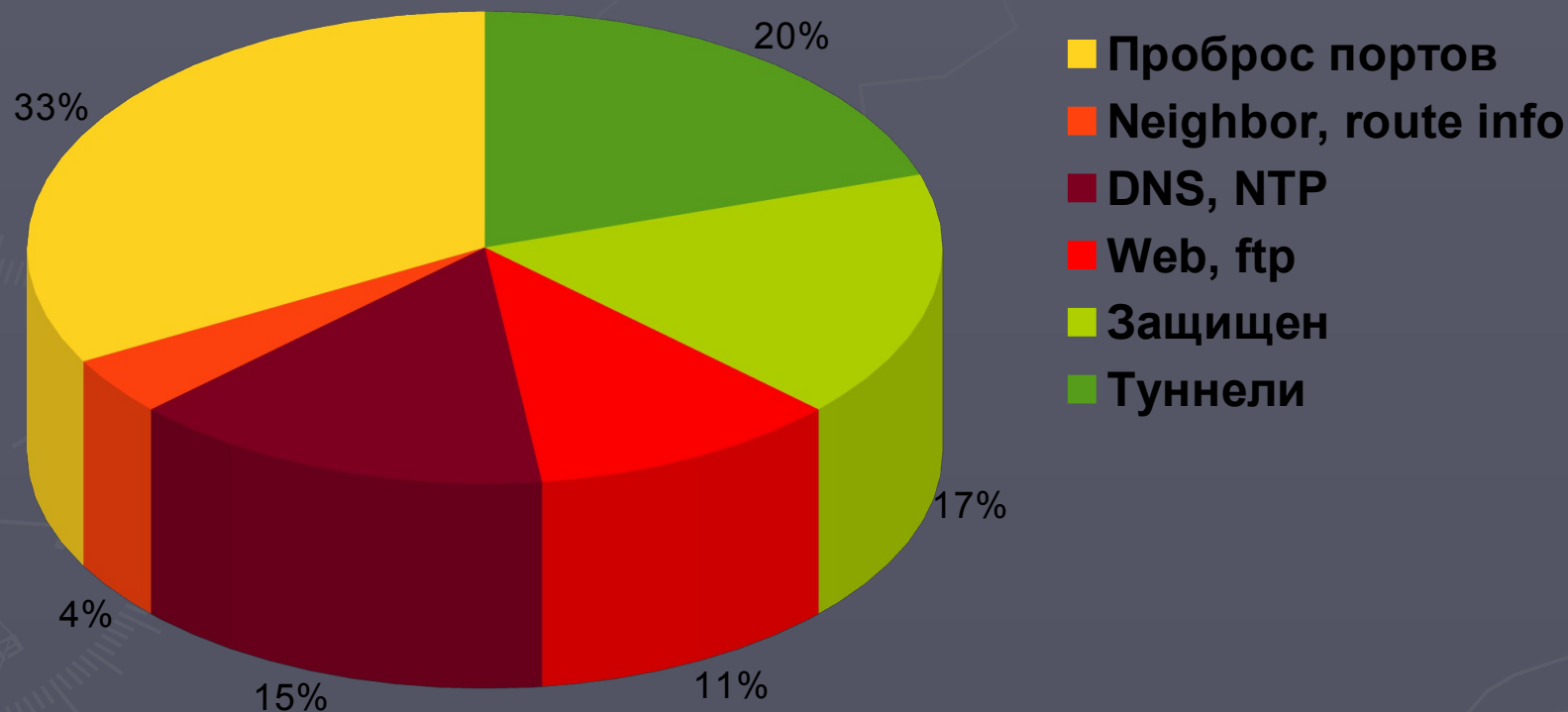
Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

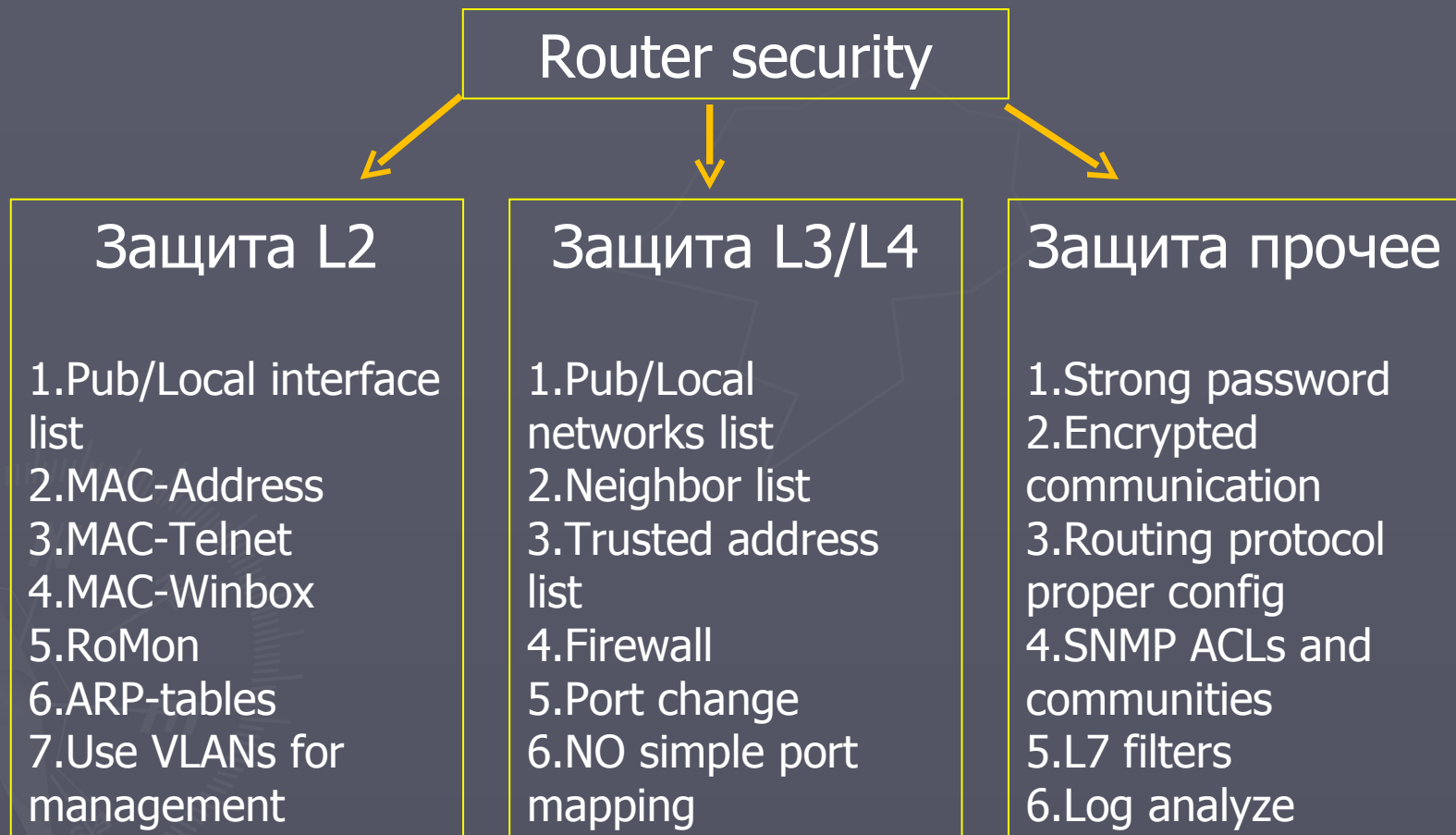
Чек-лист (what about You?)

- ☐ 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!

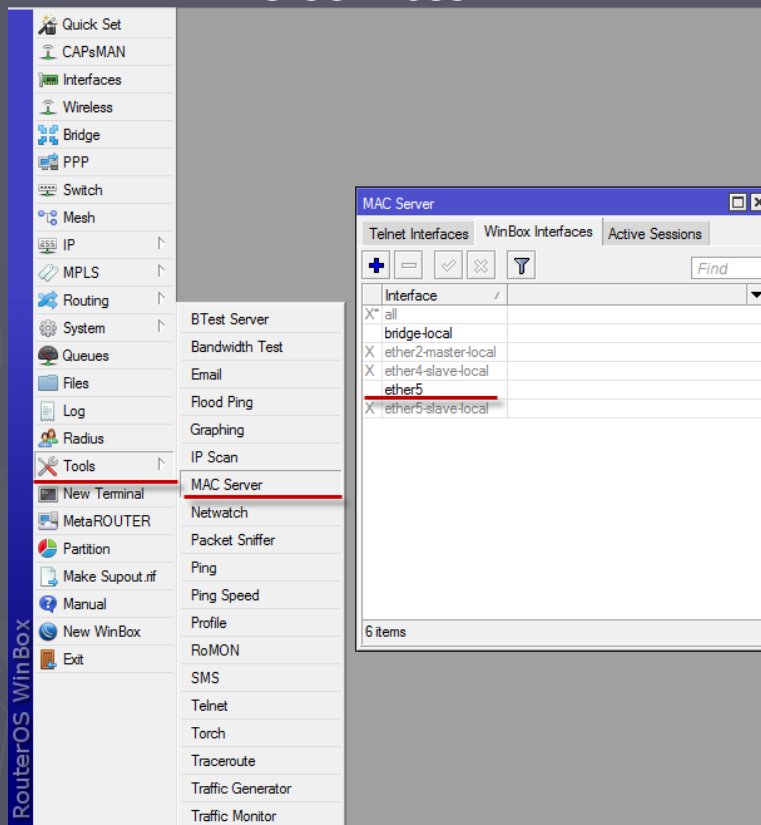
Внешний интерфейс
Mac-Winbox

ВЫКЛЮЧИТЬ!

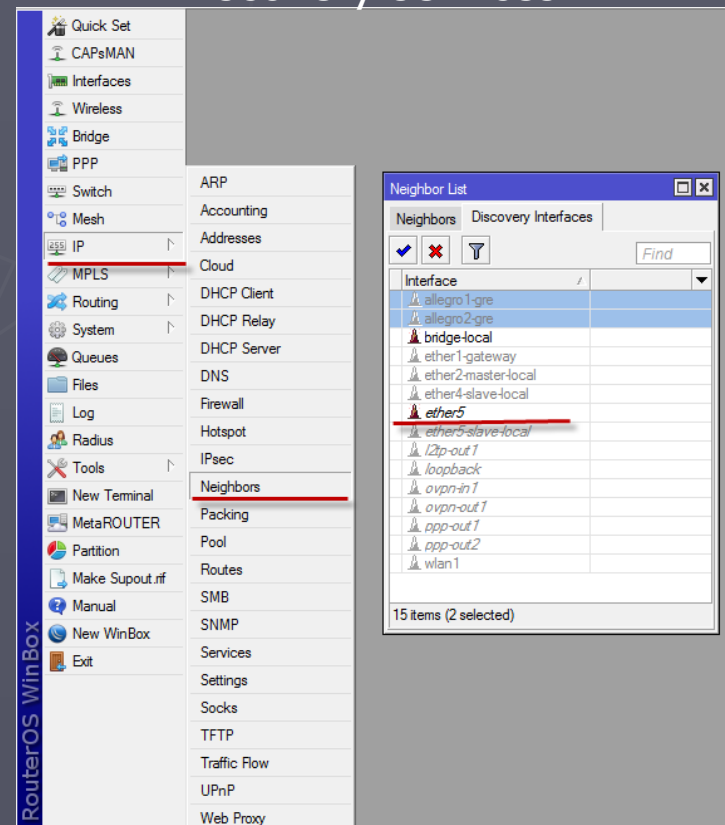
Защита каждого L2-интерфейса

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 ☺

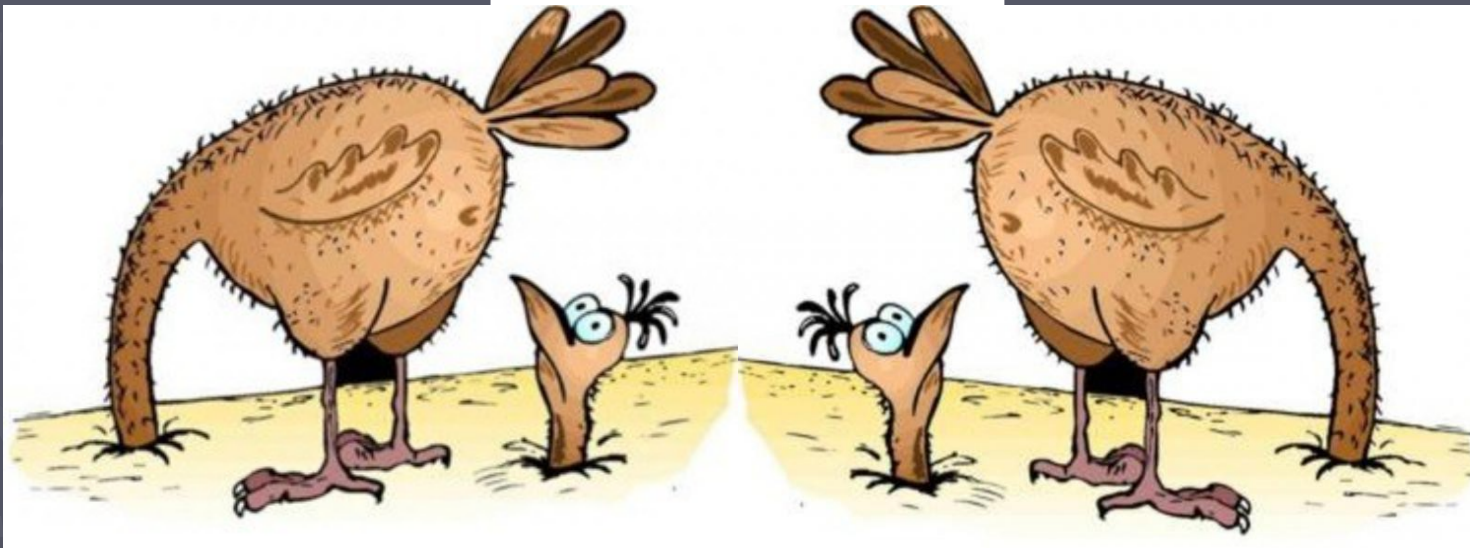
Neighbor – утечка информации

Желающие подсмотреть за соседями по сети делают так:



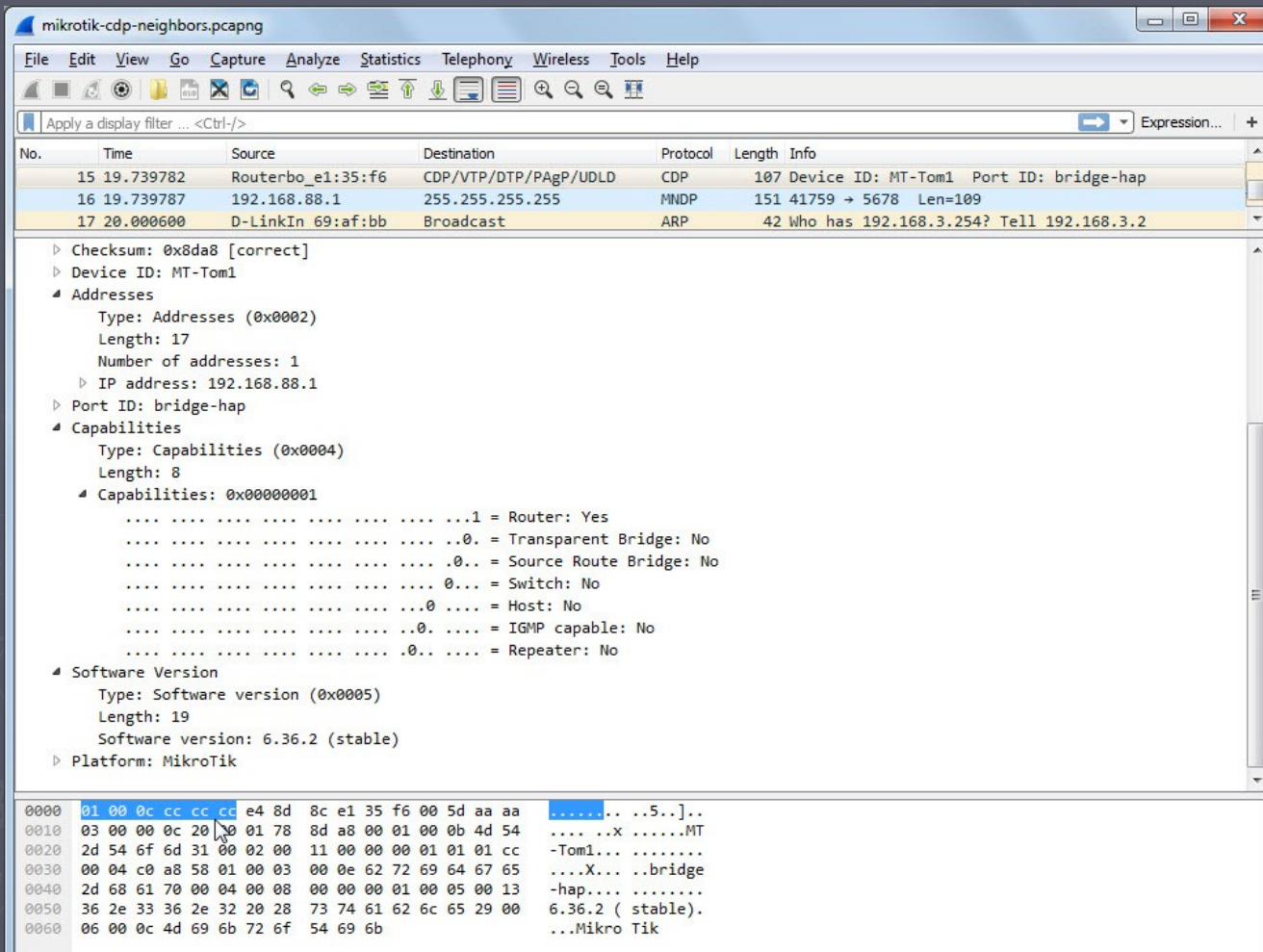
```
/ip firewall filter add chain=output action=drop protocol=udp dst-port=5678 out-interface=Wan
```

CDP/VDP



Neighbor – CDP протокол L2

Фильтруется по MAC: **01:00:0c:cc:cc:cc** на бридже



mikrotik-cdp-neighbors.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
15	19.739782	Routerbo_e1:35:f6	CDP/VTP/DTP/PagP/UDLD	CDP	107	Device ID: MT-Tom1 Port ID: bridge-hap
16	19.739787	192.168.88.1	255.255.255.255	MNDP	151	41759 → 5678 Len=109
17	20.000600	D-LinkIn 69:af:bb	Broadcast	ARP	42	Who has 192.168.3.254? Tell 192.168.3.2

Checksum: 0x8da8 [correct]
Device ID: MT-Tom1

Addresses
Type: Addresses (0x0002)
Length: 17
Number of addresses: 1
IP address: 192.168.88.1
Port ID: bridge-hap

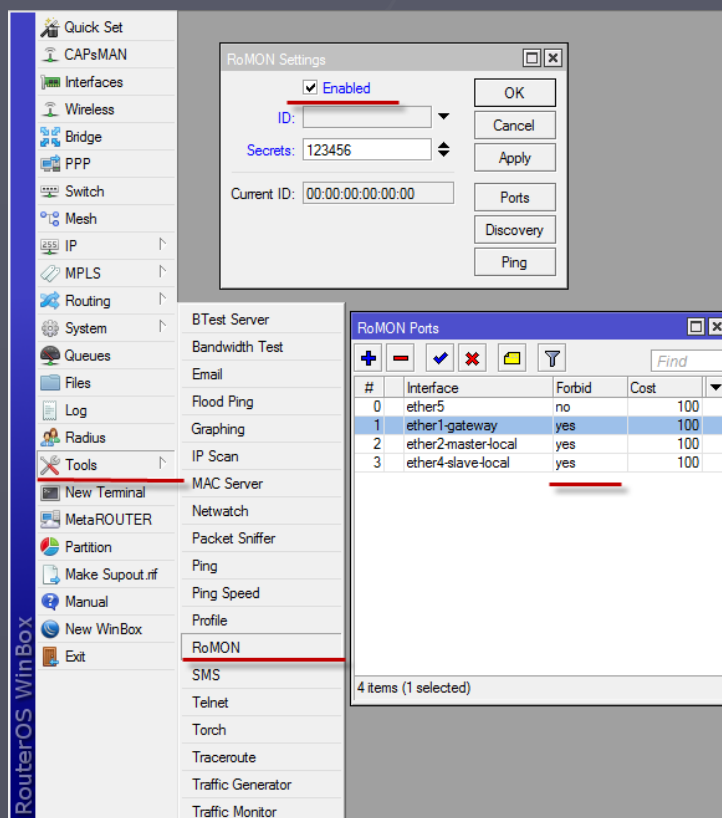
Capabilities
Type: Capabilities (0x0004)
Length: 8
Capabilities: 0x00000001
...1 = Router: Yes
...0 = Transparent Bridge: No
...0 = Source Route Bridge: No
...0 = Switch: No
...0 = Host: No
...0 = IGMP capable: No
...0 = Repeater: No

Software Version
Type: Software version (0x0005)
Length: 19
Software version: 6.36.2 (stable)
Platform: MikroTik

0000 01 00 0c cc cc cc e4 8d 8c e1 35 f6 00 5d aa aaS...]
0010 03 00 00 0c 20 00 01 78 8d a8 00 01 00 0b 4d 54X.....MT
0020 2d 54 6f 6d 31 00 02 00 11 00 00 00 01 01 01 cc -Tom1...
0030 00 04 c0 a8 58 01 00 03 00 0e 62 72 69 64 67 65X...bridge
0040 2d 68 61 70 00 04 00 08 00 00 00 01 00 05 00 13 -hap...
0050 36 2e 33 36 2e 32 20 28 73 74 61 62 6c 65 29 00 6.36.2 (stable).
0060 06 00 0c 4d 69 6b 72 6f 54 69 6b ...Mikro Tik

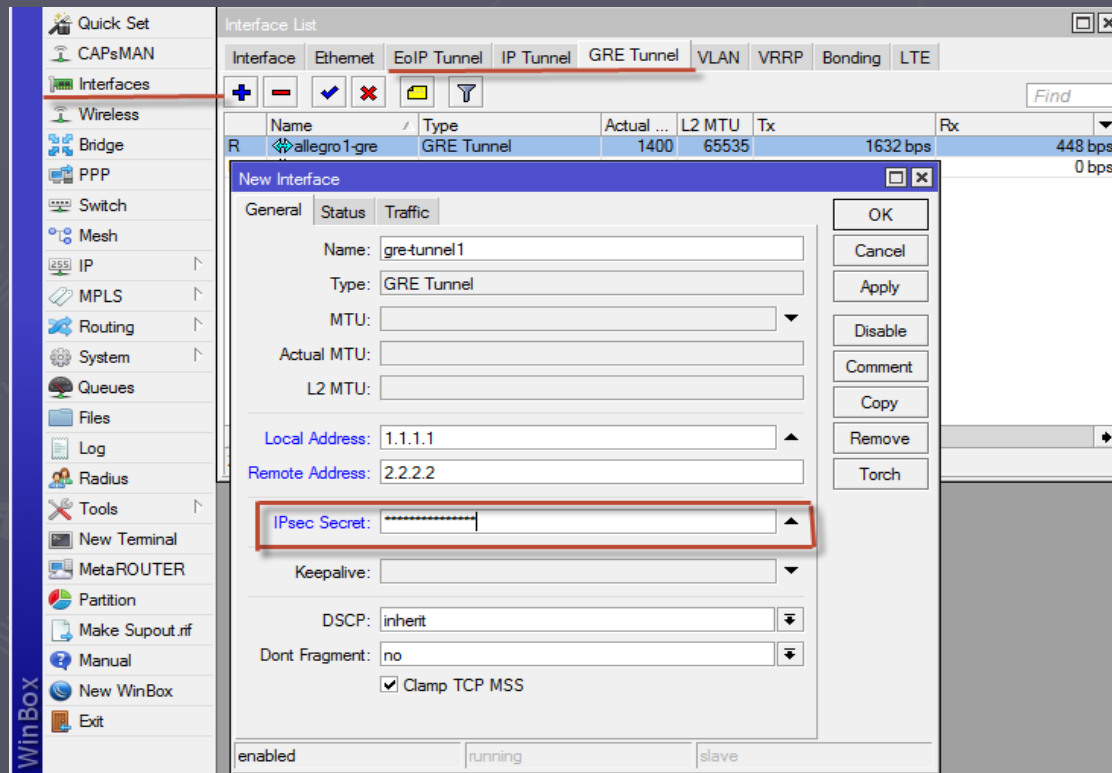
Безопасность L2 & MAC

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



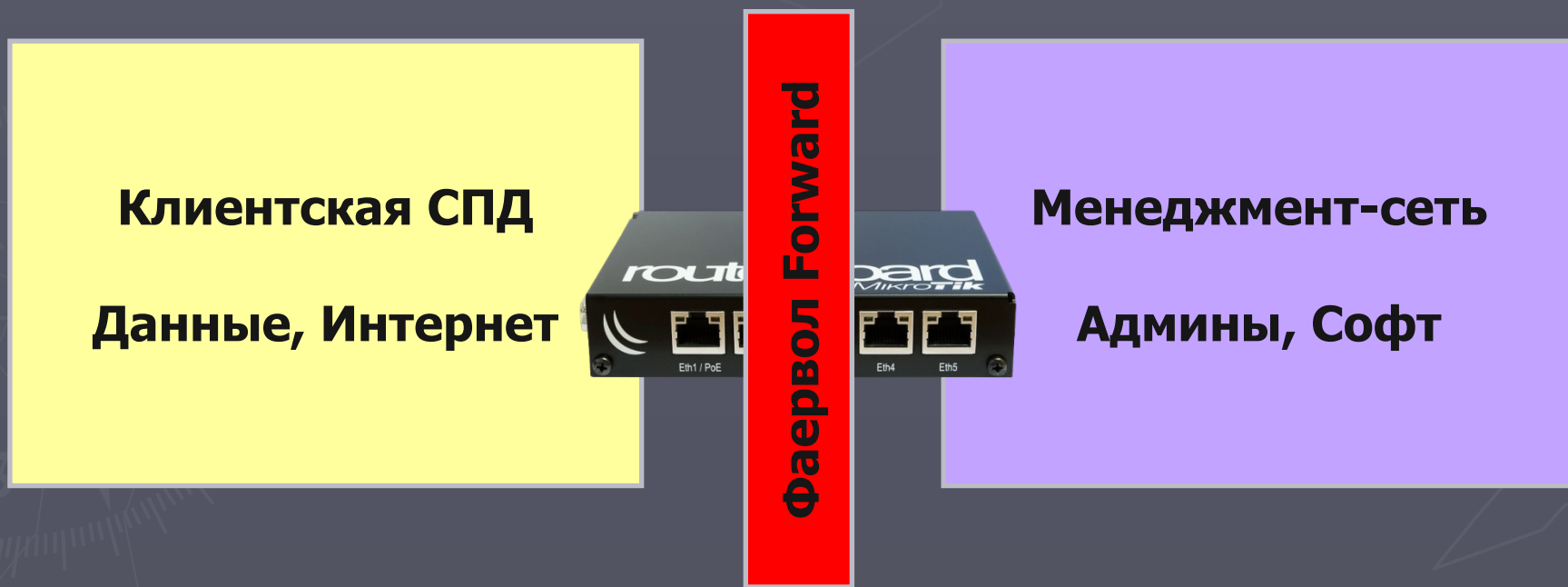
Защита туннелей EoIP/GRE/IPIP

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

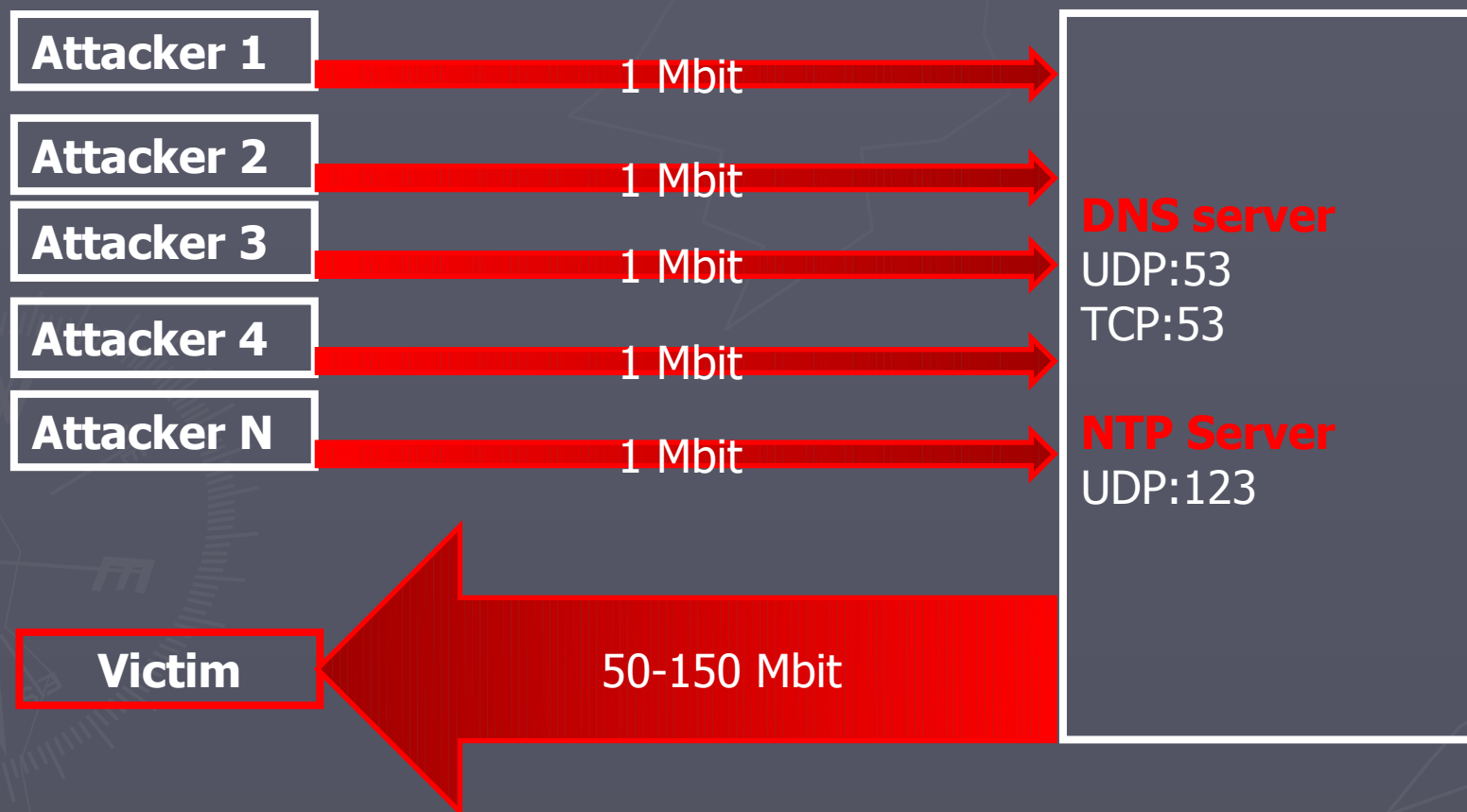
UDP magnification attack

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

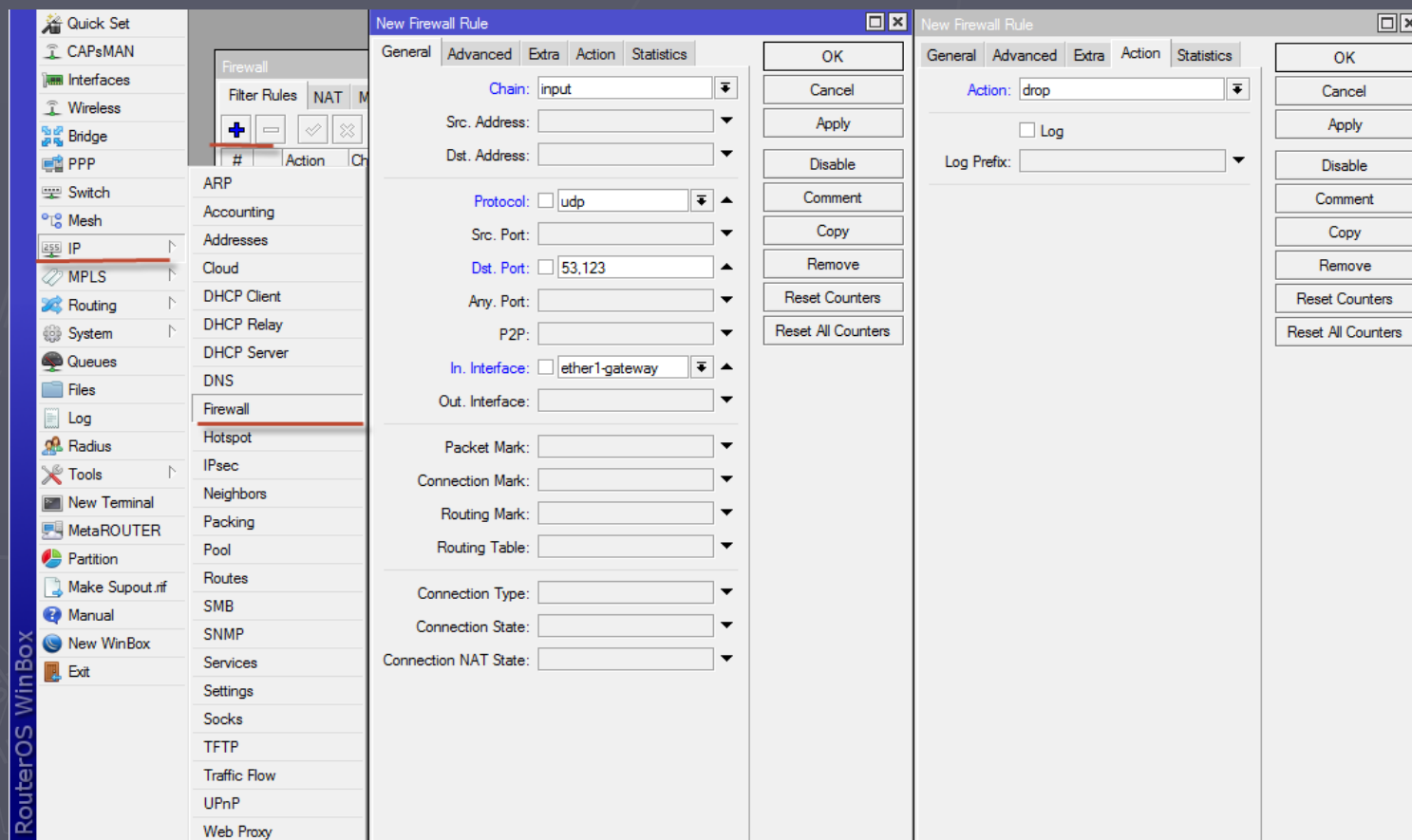
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
1 X	tarpit	input			6 (tcp)		21,22,8291			0 B	0
2 X	drop	input			6 (tcp)					0 B	0
3 X	add...	input			6 (tcp)					0 B	0
5	acc...	input			1 (ic...					23.5 KiB	401
6	acc...	input			2 (ig...					2151.8 KiB	68 856
8	acc...	input			47 (g...					2007.3 MiB	2 082 575
9	acc...	input						ether1-...		13.7 MiB	159 746
10	acc...	input						ether1-...		392 B	5
11	acc...	input		224.0.0.0/4	17 (u...			ether1-...		10.0 MiB	7 847
12	drop	input		224.0.0.5				ether1-...		0 B	0
15	drop	input								24.3 MiB	168 176

11 items out of 19 (1 selected)

Защита служб L3/L4

UDP magnification attack solution

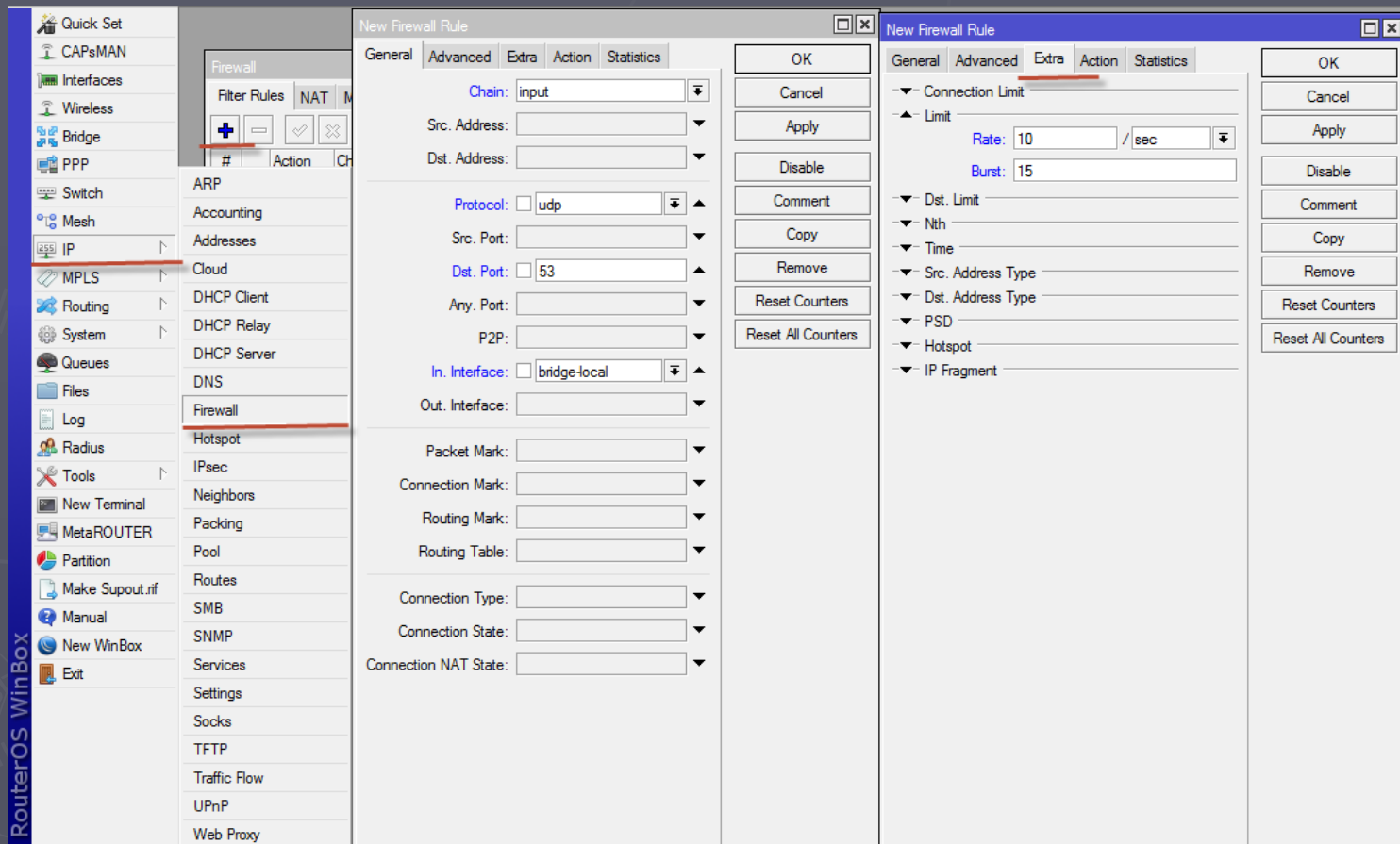
- ▶ Закрывать порты 123 udp, 53 tcp&udp из Интернет.



Защита служб L3/L4

UDP magnification attack solution

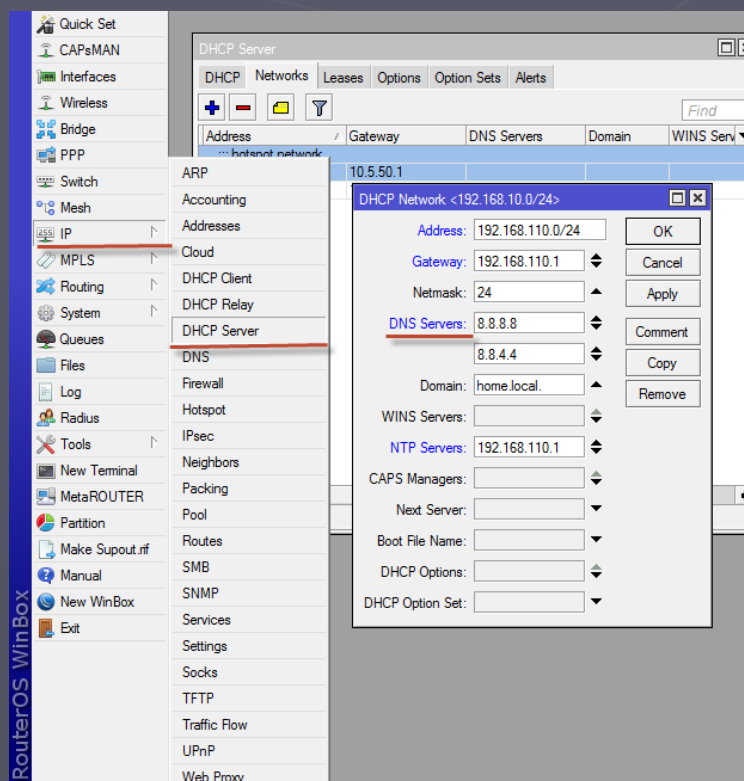
- ▶ Ограничить трафик на udr:53 udr:123 фаерволом



Защита служб L3/L4

UDP magnification attack solution

- ▶ Давать доступ к DNS только доверенным узлам
- ▶ Использовать внешние DNS-серверы (е.х. 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"?

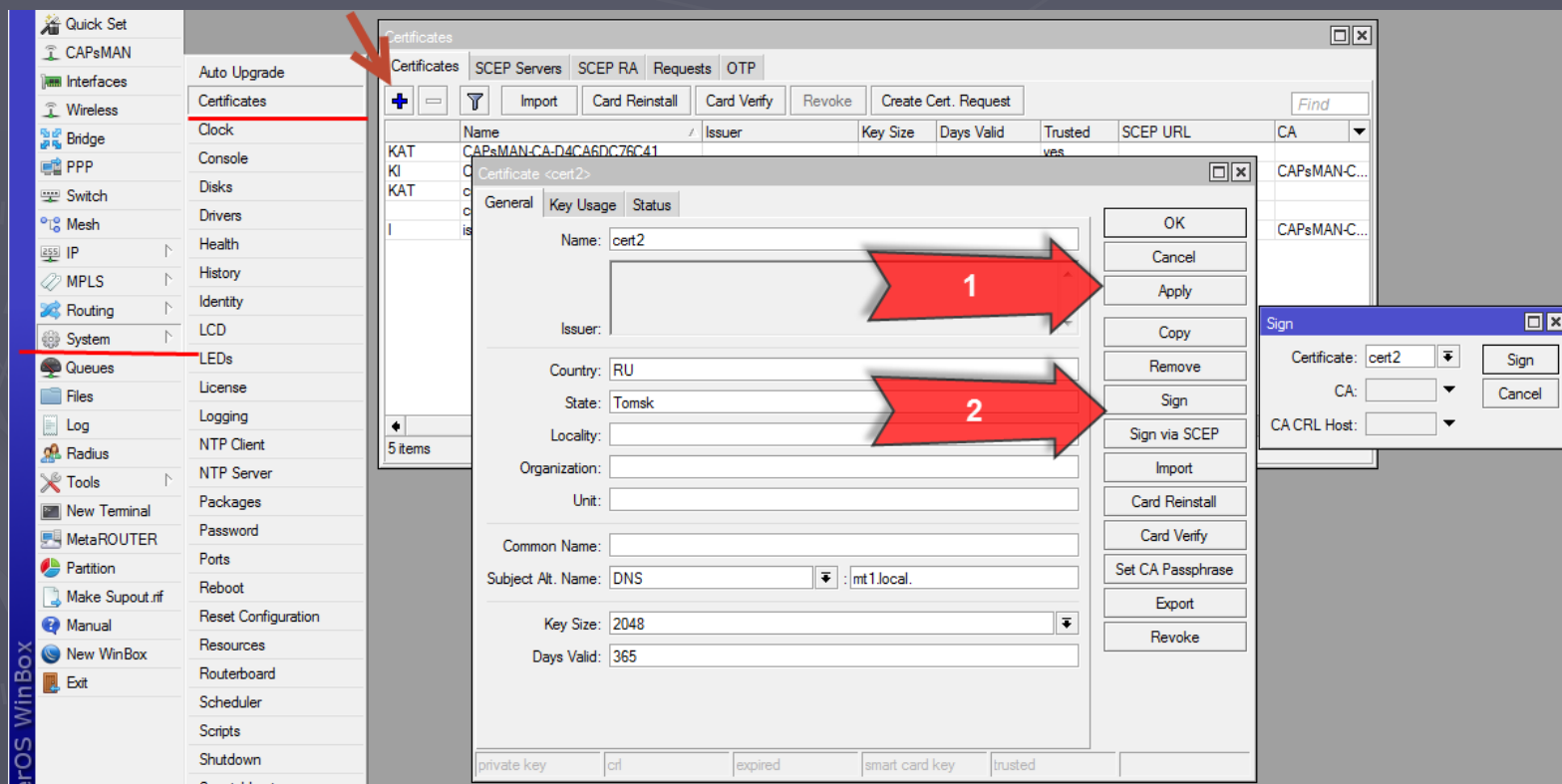
Приглашение для подбора паролей?

Залить script.rsc.auto?

Защита WebFig и API

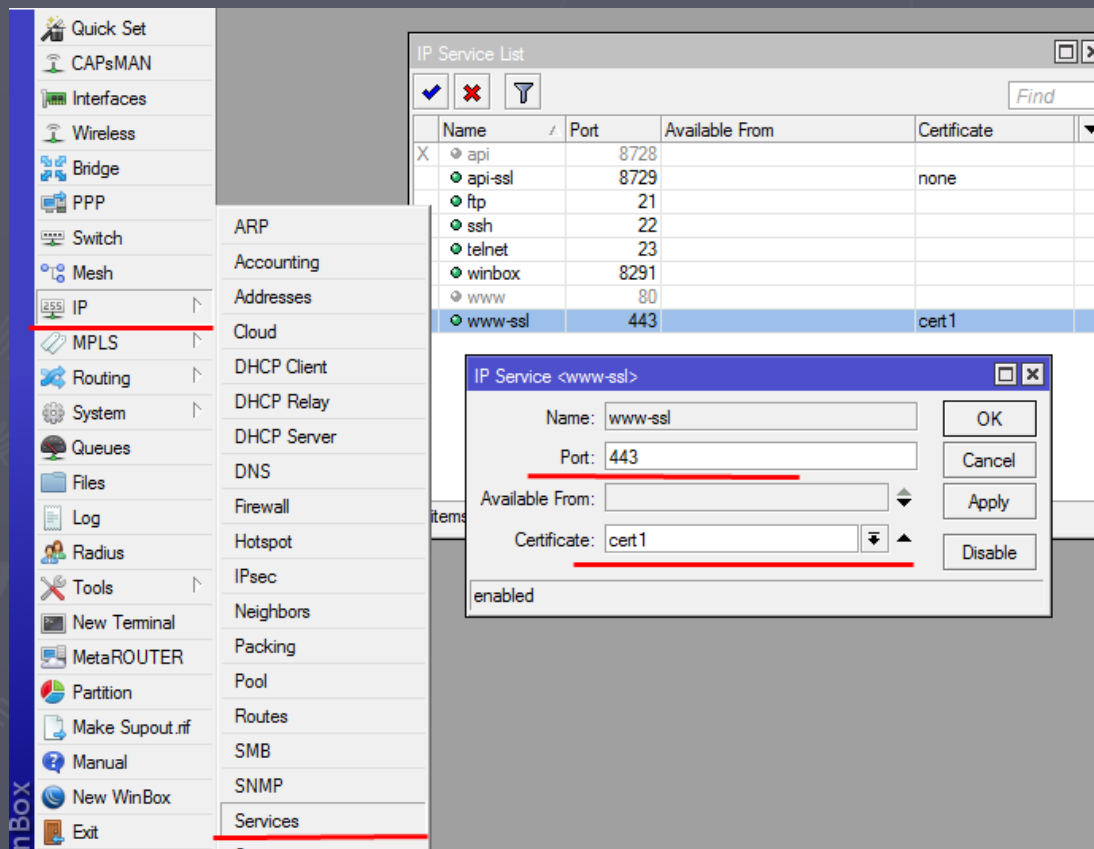
- ▶ Http передает данные в открытом виде
- ▶ HttpS по-умолчанию не работает

Для работы HTTPS нужен сертификат. Любой 😊



Защита WebFig и API

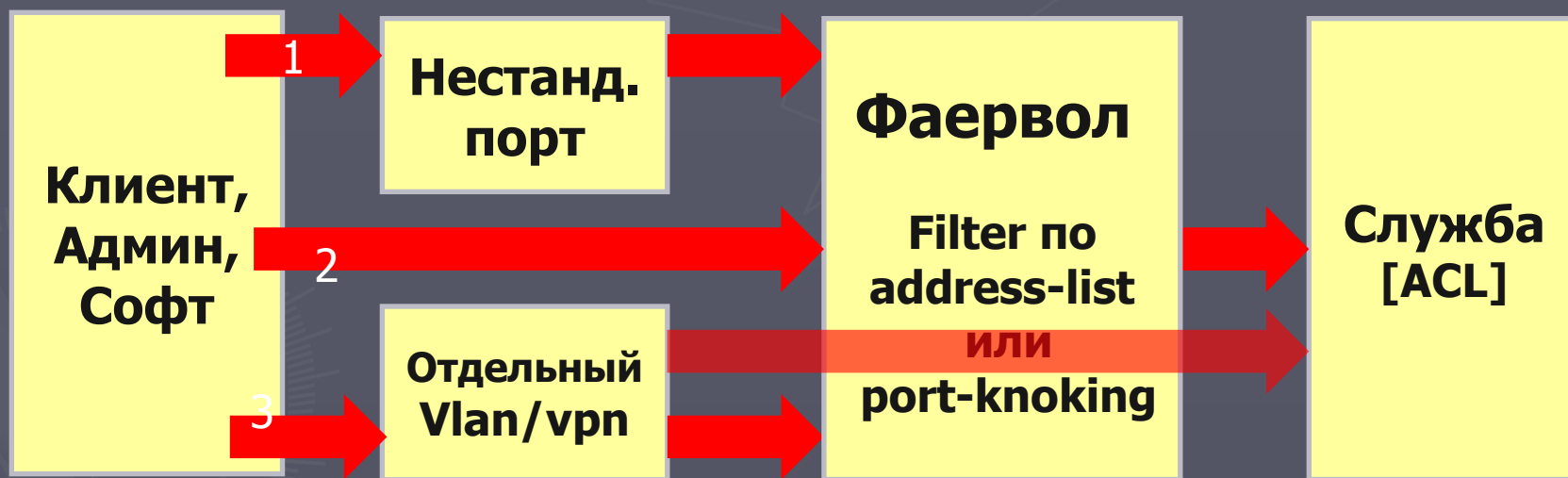
- Устанавливаем сертификат к службе, меняем порт



Защита служб

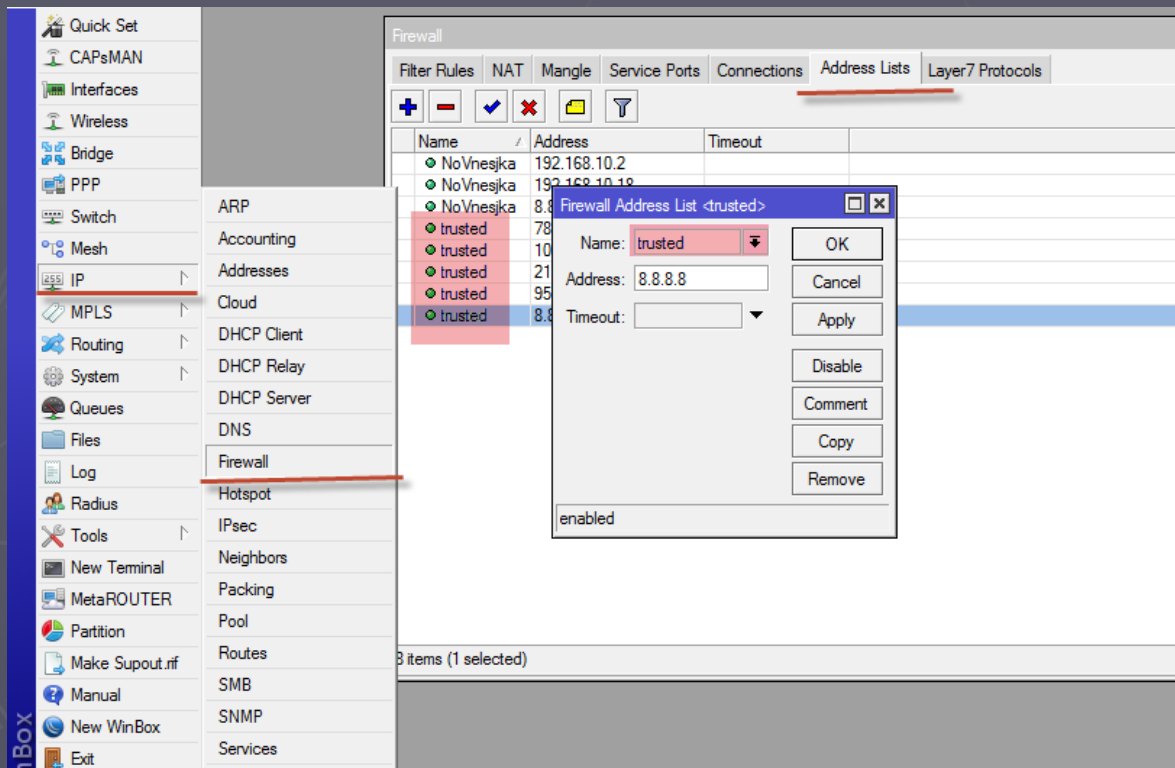
Схема доступа для настоящих админов ☺

Собственная ACL сервиса может иметь уязвимости.



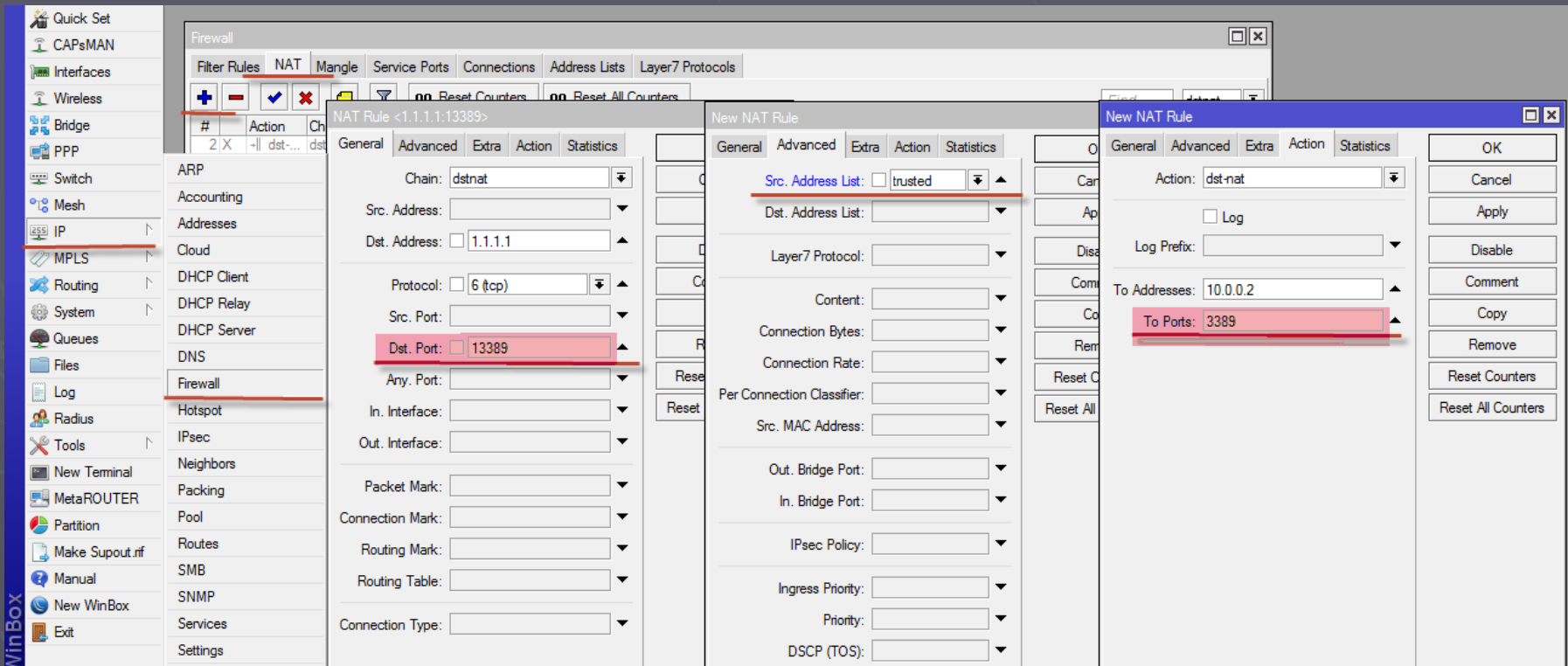
Firewall – проброс портов

- ▶ 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



RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.tif
Manual
New WinBox
Exit

Firewall Filter Rules

#	Act
0	D ✓
1	D ✓
2	D ✓
3	X ✓
4	X ✓
5	X ✓
6	X ✓
7	X ✓
8	
9	
10	
11	
12	
13	X ✓
14	
15	
16	
17	
18	
19	
23 items (1 se	

Mangle Rule <>

General Advanced Extra Action Statistics

Chain: postrouting

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface: ether1-gateway

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK
Cancel
Apply
Enable
Comment
Copy
Remove
Reset Counters
Reset All Counters

New Mangle Rule

General Advanced Extra Action Statistics

Action: change DSCP (TOS)

Log Prefix:

New DSCP (TOS):

OK
Cancel
Apply
Enable
Comment
Copy
Remove
Reset Counters
Reset All Counters

accept
add dst to address list
add src to address list
change DSCP (TOS)
change MSS
change TTL
clear DF
fasttrack connection
jump
log
mark connection
mark packet
mark routing
passthrough
return
set priority
sniff PC
sniff T2SP
strip IPv4 options

Различия между IDS и IPS

IDS

- Фиксирует подозрительные действия и шлет оповещения
- Сама не защищает ресурсы
- Не воздействует на атакующего
 - Состояние системы не изменяется
- Пассивная система

IPS

- Активно реагирует на подозрительные действия
- Защищает ресурсы сети
- Может воздействовать на атакующего
- Состояние системы может меняться
- 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 😊

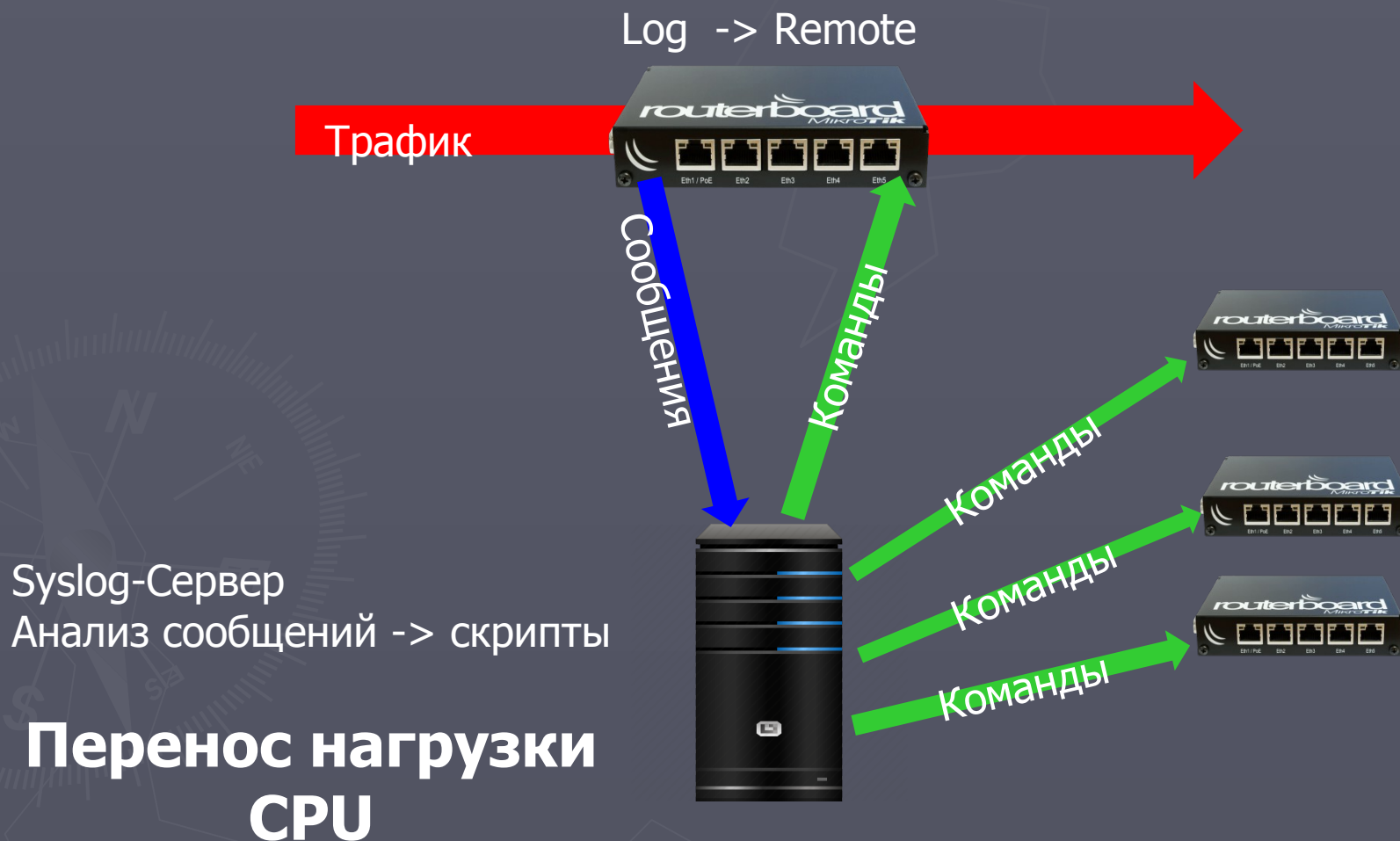
1. Берем по одному адреса из dynamic-list
2. Добавляем по одному в static-list

- ▶

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

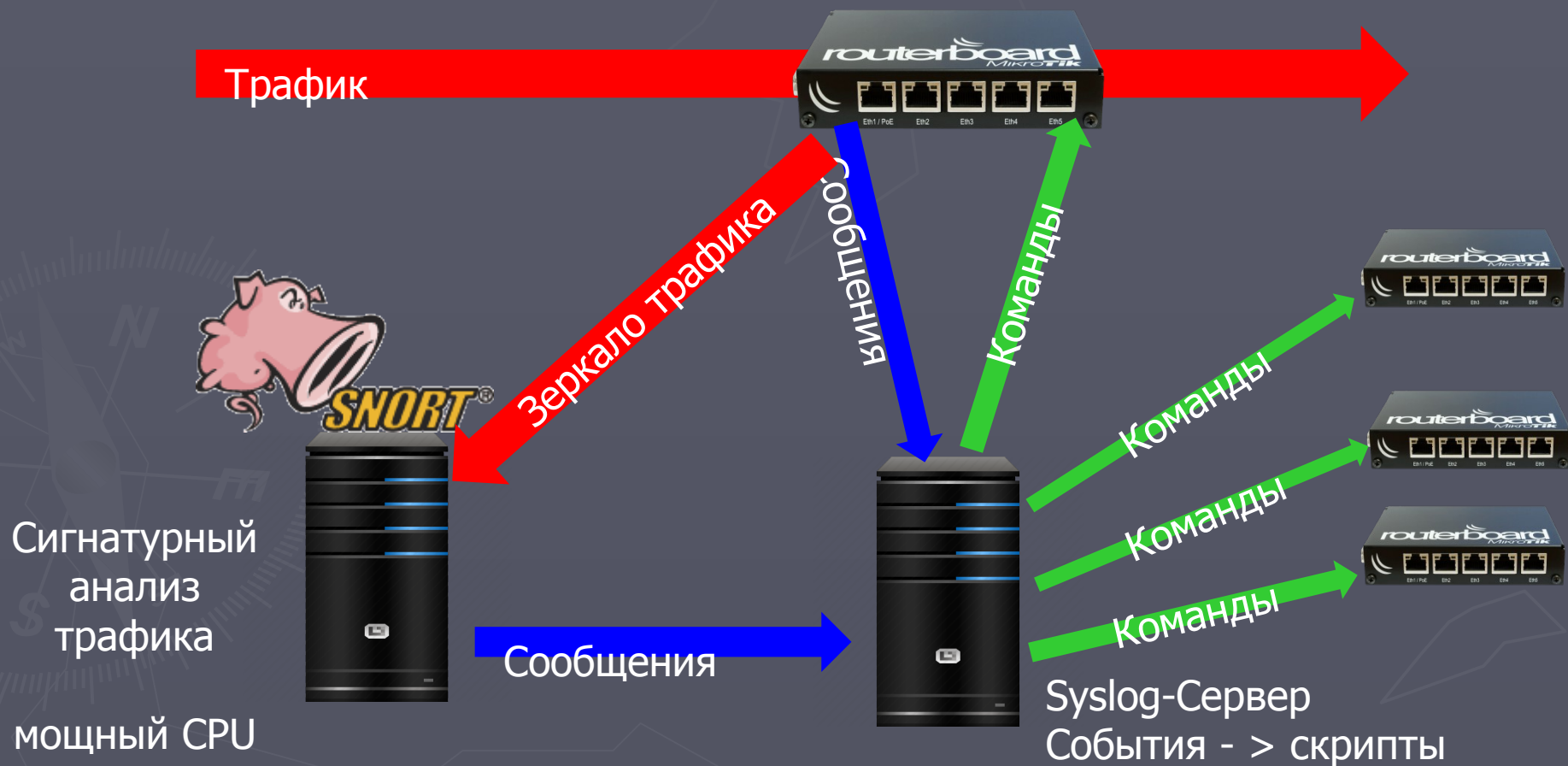

Распределение функций

Экономим ресурсы процессора, делегируя функции



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