

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/>

Shodan Developers Book View All...

SHODAN 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.



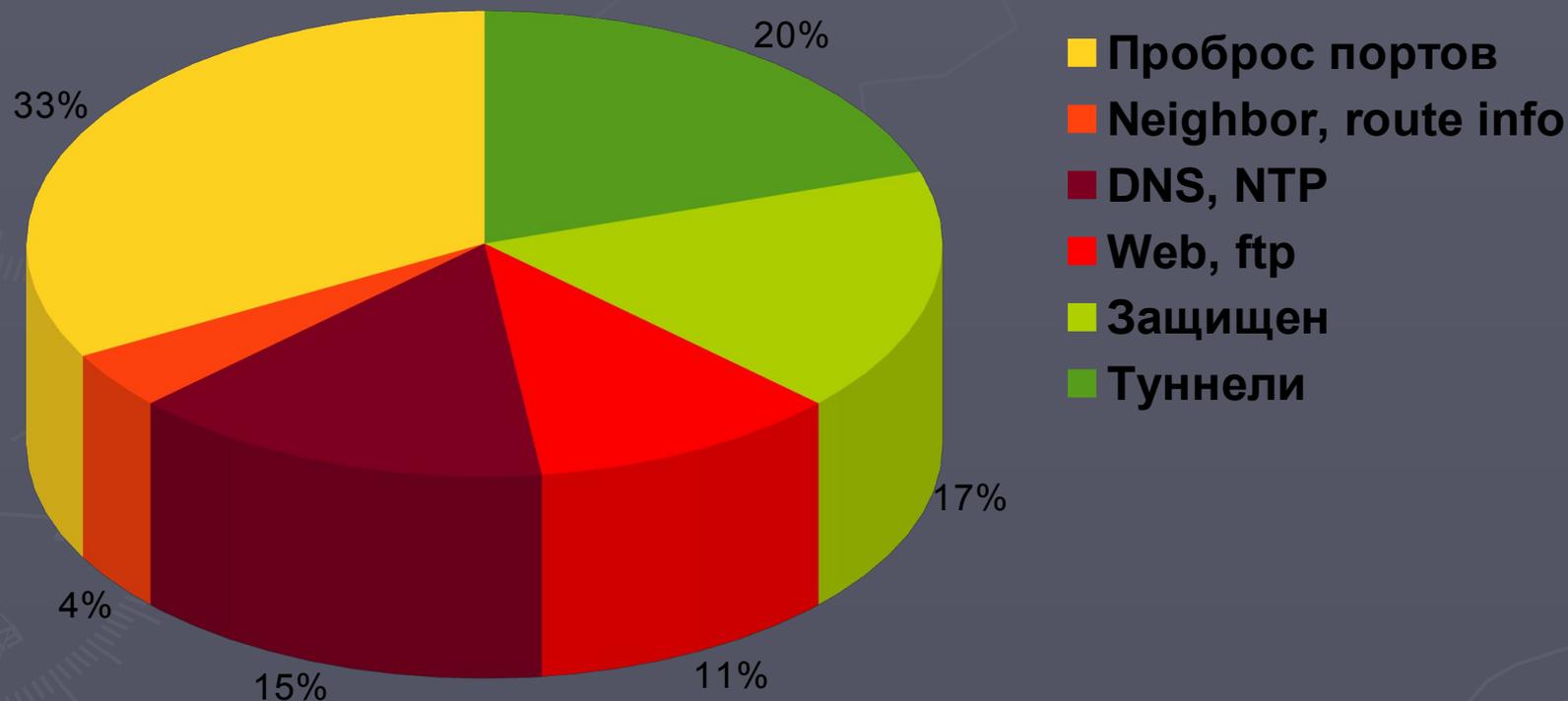
Get a Competitive Advantage

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

Router security

```
graph TD; A[Router security] --> B[Защита L2]; A --> C[Защита L3/L4]; A --> D[Защита прочее];
```

Защита L2

1. Pub/Local interface list
2. MAC-Address
3. MAC-Telnet
4. MAC-Winbox
5. RoMon
6. ARP-tables
7. Use VLANs for management

Защита L3/L4

1. Pub/Local networks list
2. Neighbor list
3. Trusted address list
4. Firewall
5. Port change
6. NO simple port mapping

Защита прочее

1. Strong password
2. Encrypted communication
3. Routing protocol proper config
4. SNMP ACLs and communities
5. L7 filters
6. Log analyze

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.

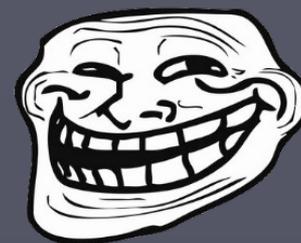
Безопасность L2 & MAC

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

The screenshot shows the RouterOS WinBox interface. On the left, the 'Tools' menu is open, and 'MAC Server' is selected. The main window displays the 'MAC Server' configuration page. The 'Telnet Interfaces' tab is active, showing a list of interfaces with checkboxes for enabling services. The 'ether5' interface is highlighted with a red underline.

Interface	all	bridge-local	ether2-master-local	ether4-slave-local	ether5	ether5-slave-local
X			X	X	X	X

Discovery services

The screenshot shows the RouterOS WinBox interface. On the left, the 'Tools' menu is open, and 'Neighbors' is selected. The main window displays the 'Neighbor List' configuration page. The 'Discovery Interfaces' tab is active, showing a list of interfaces with checkboxes for enabling services. The 'ether5' interface is highlighted with a red underline.

Interface	allegro 1-gre	allegro 2-gre	bridge-local	ether1-gateway	ether2-master-local	ether4-slave-local	ether5	ether5-slave-local	l2p-out 1	loopback	ovpn-in 1	ovpn-out 1	ppp-out 1	ppp-out 2	wlan1
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							

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 😊

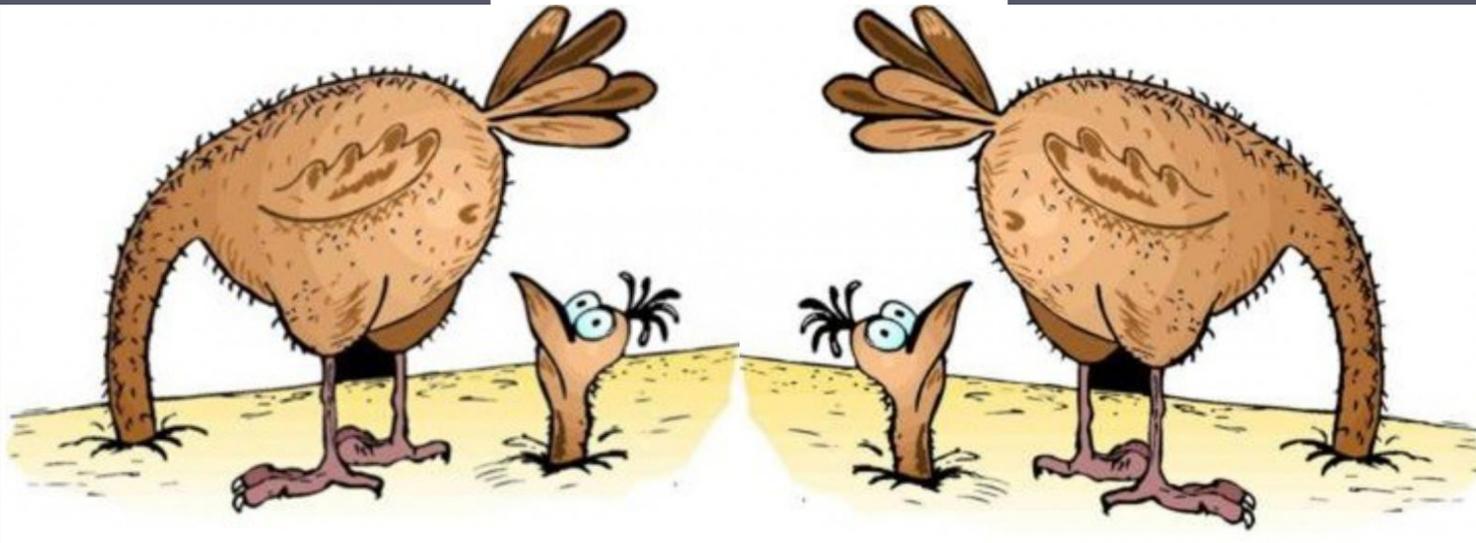
Neighbor – утечка информации

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

The screenshot shows the Mikrotik WinBox interface with the 'mikrotik-cdp-neighbors.pcapng' file open. The main window displays a table of CDP neighbors and a detailed view of the selected neighbor.

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

Neighbor Details:

- 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

Raw Packet Data:

```
0000 01 00 0c cc cc cc e4 8d 8c e1 35 f6 00 5d aa aa .....].S.]..
0010 03 00 00 0c 20 00 01 78 8d a8 00 01 00 0b 4d 54 ....x.....MT
0020 2d 54 6f 6d 31 00 02 00 11 00 00 00 01 01 01 cc -Tom1... ..bridge
0030 00 04 c0 a8 58 01 00 03 00 0e 62 72 69 64 67 65 ...X... ..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

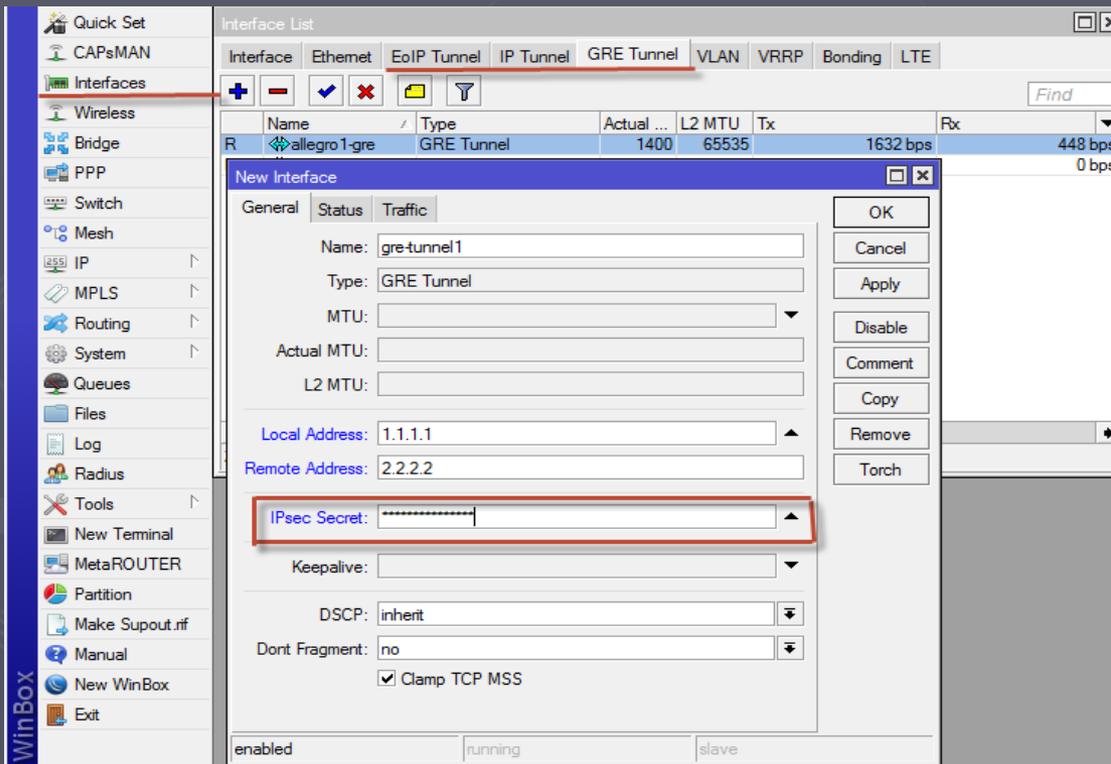
The screenshot displays the RouterOS WinBox interface. On the left is a navigation tree with categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, and a 'New WinBox' section. The 'Tools' category is expanded, showing various diagnostic tools, with 'RoMON' highlighted. Two windows are open:

- RoMON Settings:** A dialog box where the 'Enabled' checkbox is checked. The 'ID' field is empty, 'Secrets' is set to '123456', and 'Current ID' is '00:00:00:00:00:00'. Buttons for 'OK', 'Cancel', 'Apply', 'Ports', 'Discovery', and 'Ping' are visible.
- RoMON Ports:** A table window showing the configuration for four ports. The 'ether1-gateway' port is selected.

#	Interface	Forbid	Cost
0	ether5	no	100
1	ether1-gateway	yes	100
2	ether2-master-local	yes	100
3	ether4-slave-local	yes	100

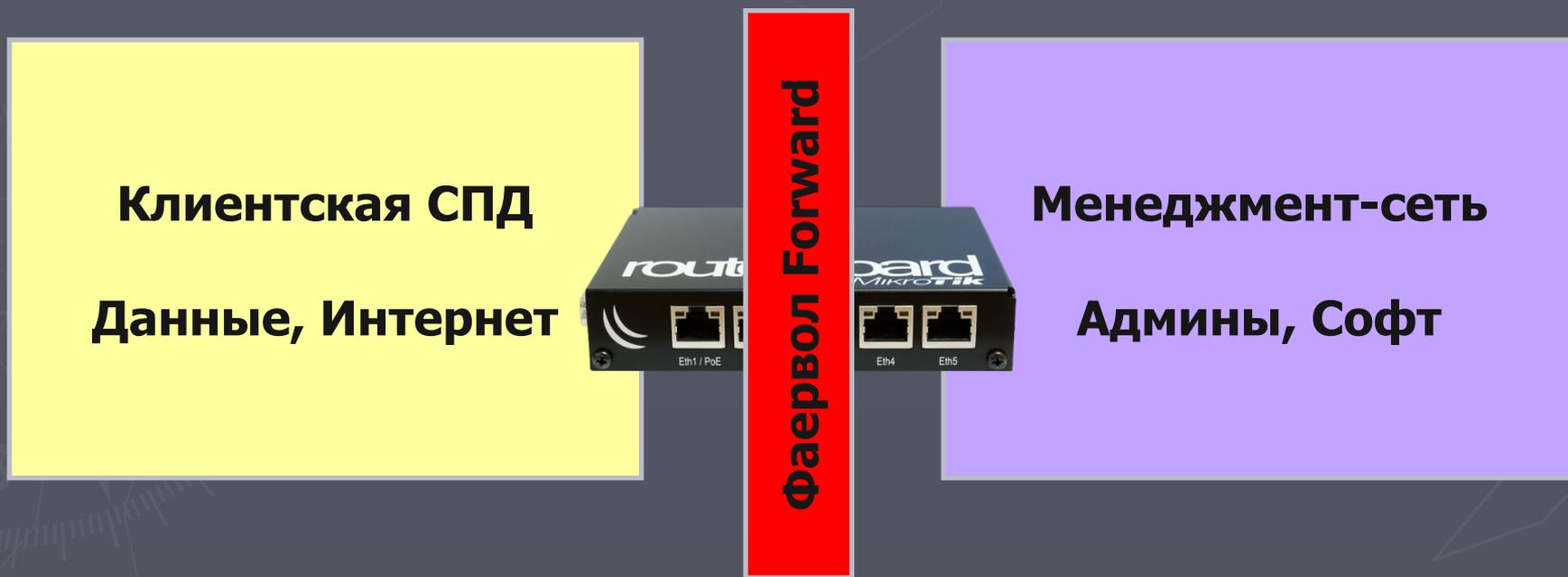
Защита туннелей **EoIP**/GRE/IPIP

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

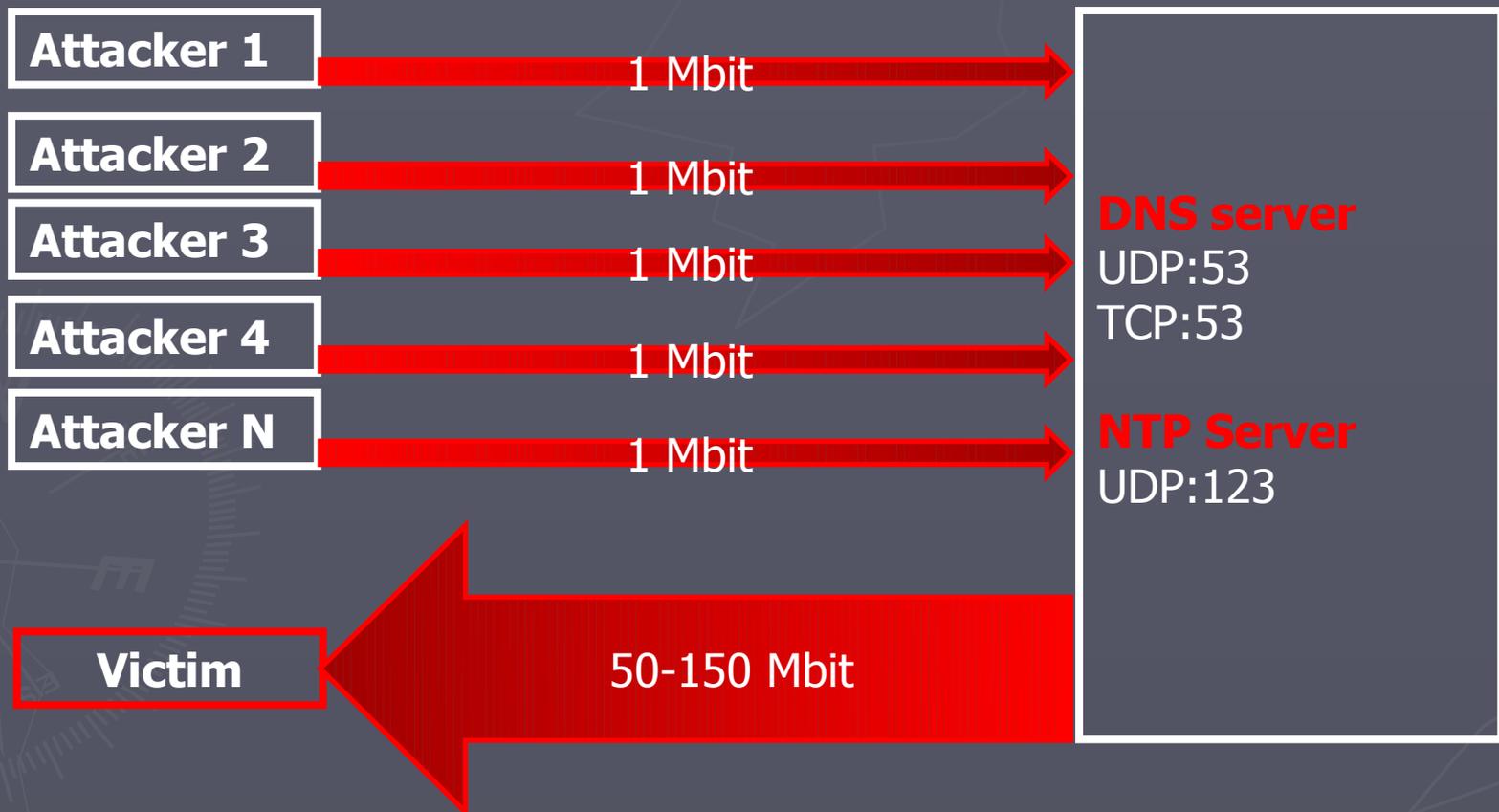
UDP magnification attack

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

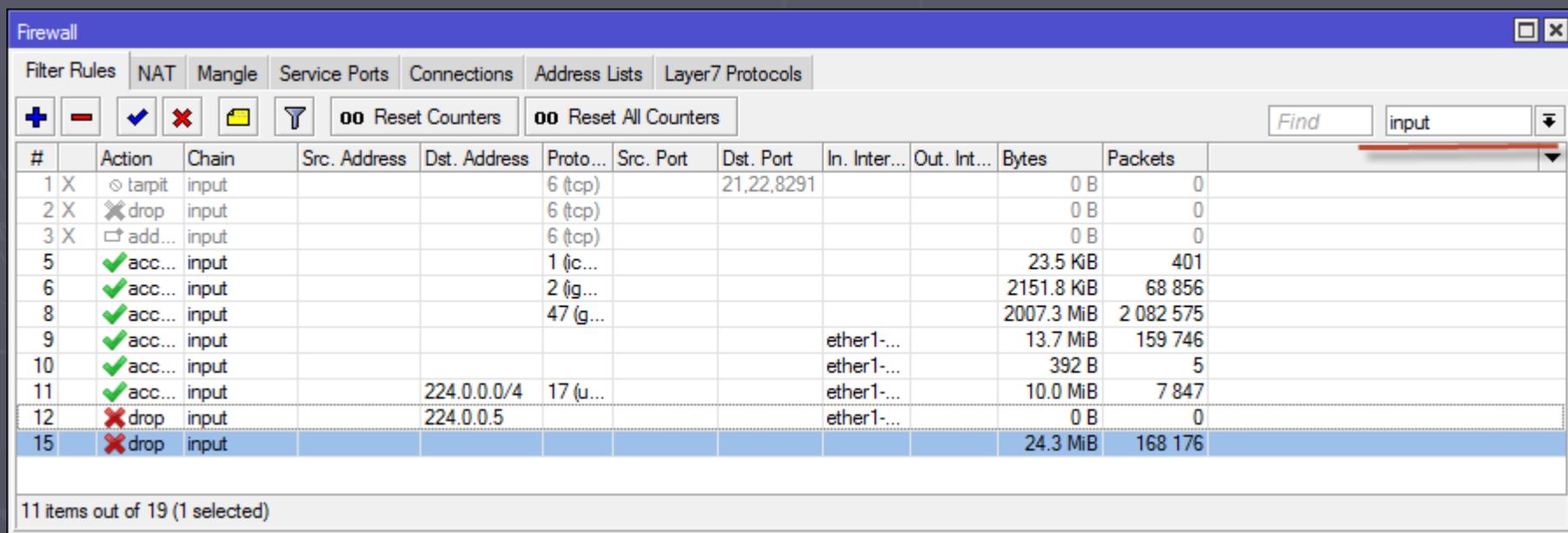
UDP magnification attack



Защита служб L3/L4

Фаерволл по-умолчанию

- ▶ Рекомендуется закрывать всё, что явно не разрешено



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active, and the 'input' chain is selected. The table below lists 15 filter rules with their actions and statistics.

#	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	X drop	input		224.0.0.5				ether1-...		0 B	0
15	X 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.

The screenshot displays the RouterOS WinBox interface for configuring a new firewall rule. The left sidebar shows the 'Firewall' menu item selected. The main window is titled 'New Firewall Rule' and is divided into several tabs: General, Advanced, Extra, Action, and Statistics. The 'General' tab is active, showing the following configuration:

- Chain: input
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: udp
- Src. Port: (empty)
- Dst. Port: 53,123
- Any. Port: (empty)
- P2P: (empty)
- In. Interface: ether1-gateway
- Out. Interface: (empty)
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Routing Table: (empty)
- Connection Type: (empty)
- Connection State: (empty)
- Connection NAT State: (empty)

The 'Action' tab is also visible, showing the following configuration:

- Action: drop
- Log
- Log Prefix: (empty)

The right side of the window contains buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

Защита служб L3/L4

UDP magnification attack solution

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

The screenshot displays the RouterOS WinBox interface for configuring a new firewall rule. The left sidebar shows the 'Firewall' menu item selected. The main window is titled 'New Firewall Rule' and is divided into several tabs: General, Advanced, Extra, Action, and Statistics. The 'General' tab is active, showing the following configuration:

- Chain: input
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: udp
- Src. Port: (empty)
- Dst. Port: 53
- Any. Port: (empty)
- P2P: (empty)
- In. Interface: bridge-local
- Out. Interface: (empty)
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Routing Table: (empty)
- Connection Type: (empty)
- Connection State: (empty)
- Connection NAT State: (empty)

The 'Extra' tab is also visible, showing the 'Connection Limit' section with the following settings:

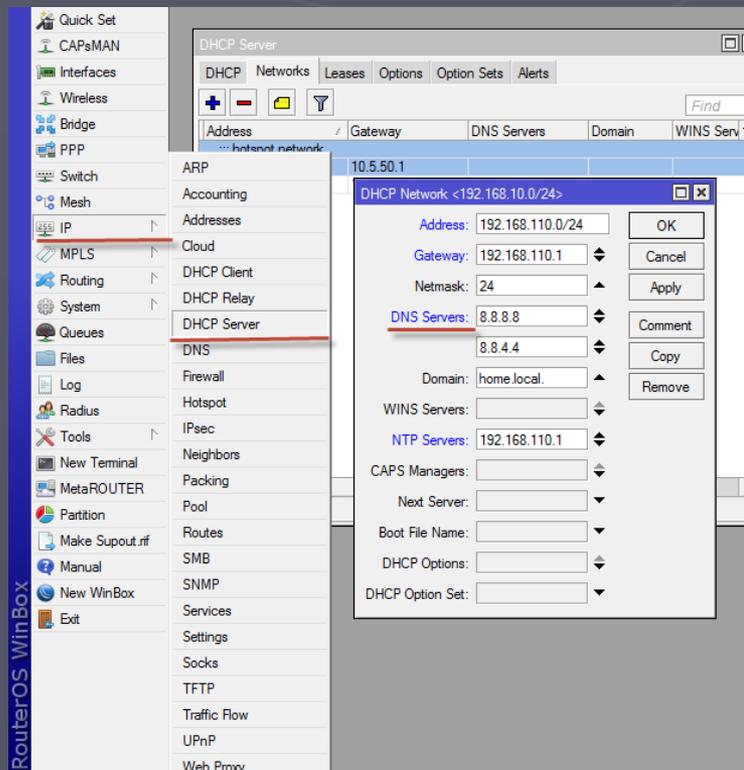
- Limit: Rate: 10 /sec, Burst: 15
- Dst. Limit: (empty)
- Nth: (empty)
- Time: (empty)
- Src. Address Type: (empty)
- Dst. Address Type: (empty)
- PSD: (empty)
- Hotspot: (empty)
- IP Fragment: (empty)

The interface includes standard window controls (OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters) for each tab.

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"?

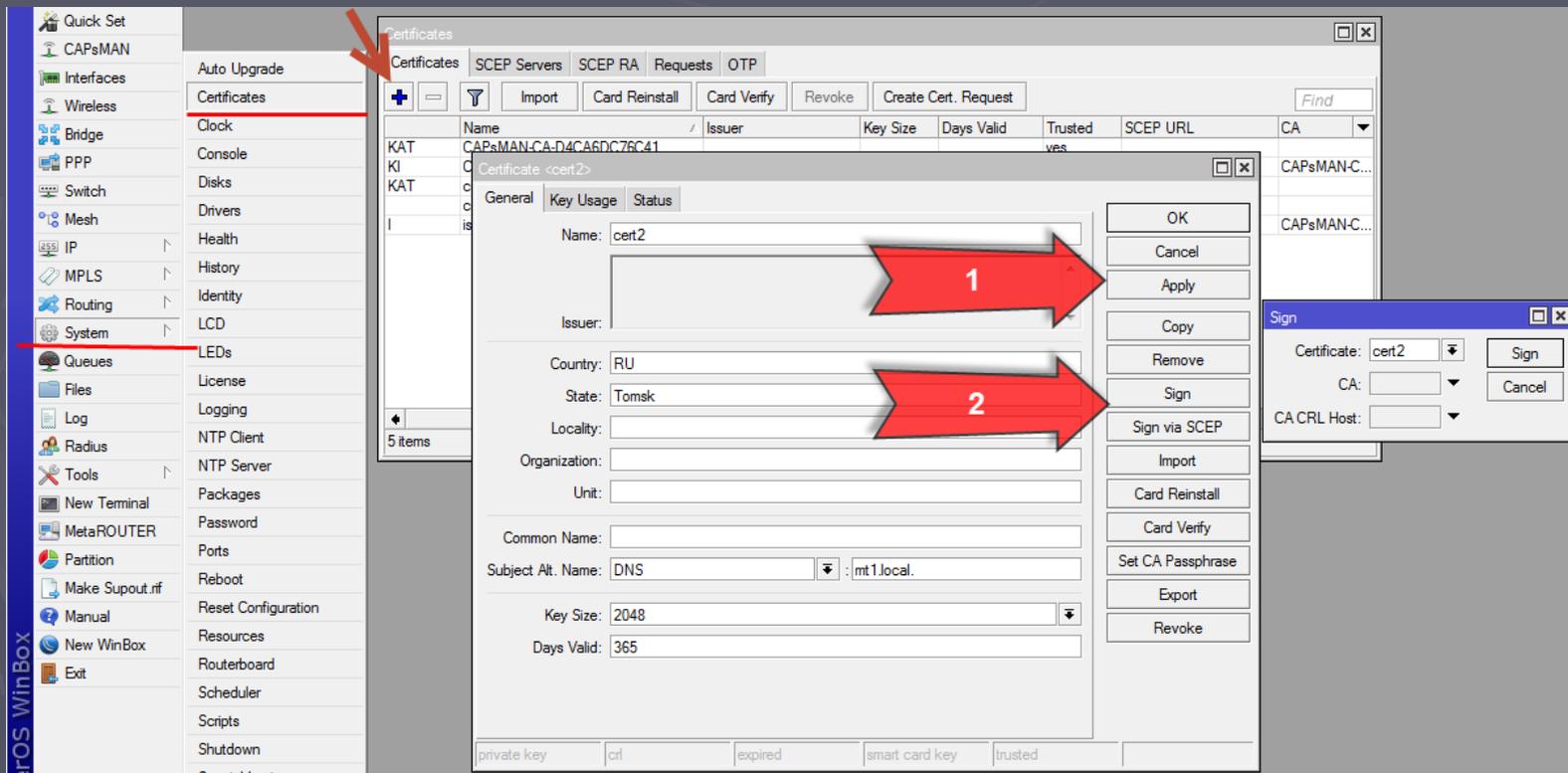
Приглашение для подбора паролей?

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

The screenshot displays the Mikrotik WinBox interface. On the left, the 'IP' menu is expanded, and the 'Services' option is selected. The 'IP Service List' window is open, showing a table of services. The 'www-ssl' service is highlighted. A secondary window, 'IP Service <www-ssl>', is open, showing the configuration for this service. The 'Name' field is 'www-ssl', the 'Port' is '443', and the 'Certificate' is 'cert1'. The service status is 'enabled'.

Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		none
ftp	21		
ssh	22		
telnet	23		
winbox	8291		
www	80		
www-ssl	443		cert1

IP Service <www-ssl>

Name: www-ssl

Port: 443

Available From: [dropdown]

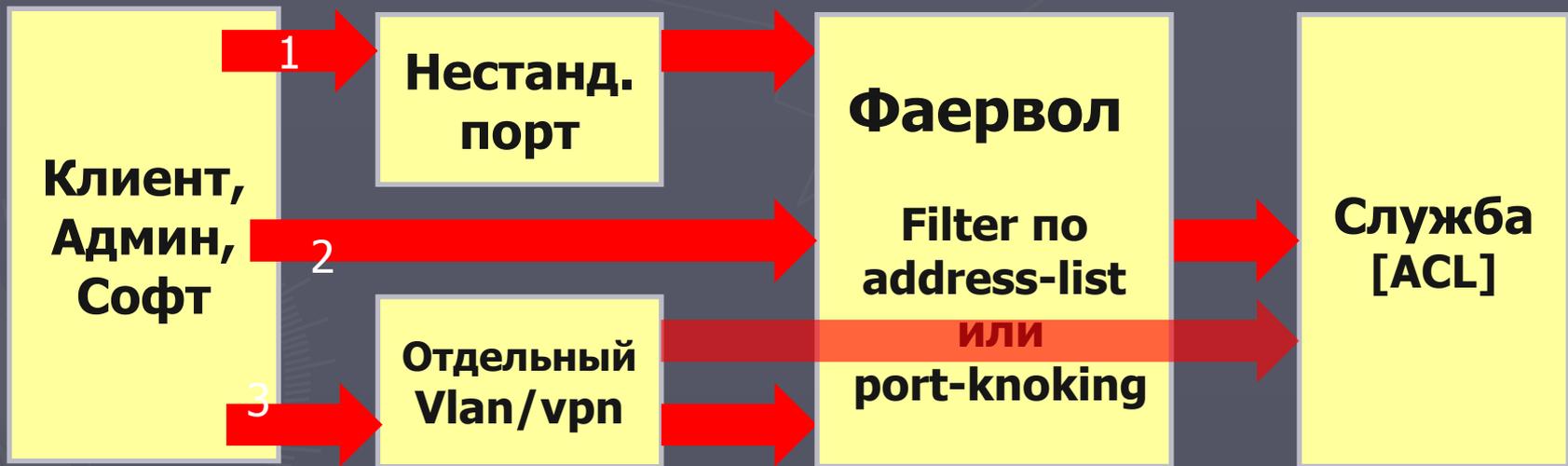
Certificate: cert1

enabled

Защита служб

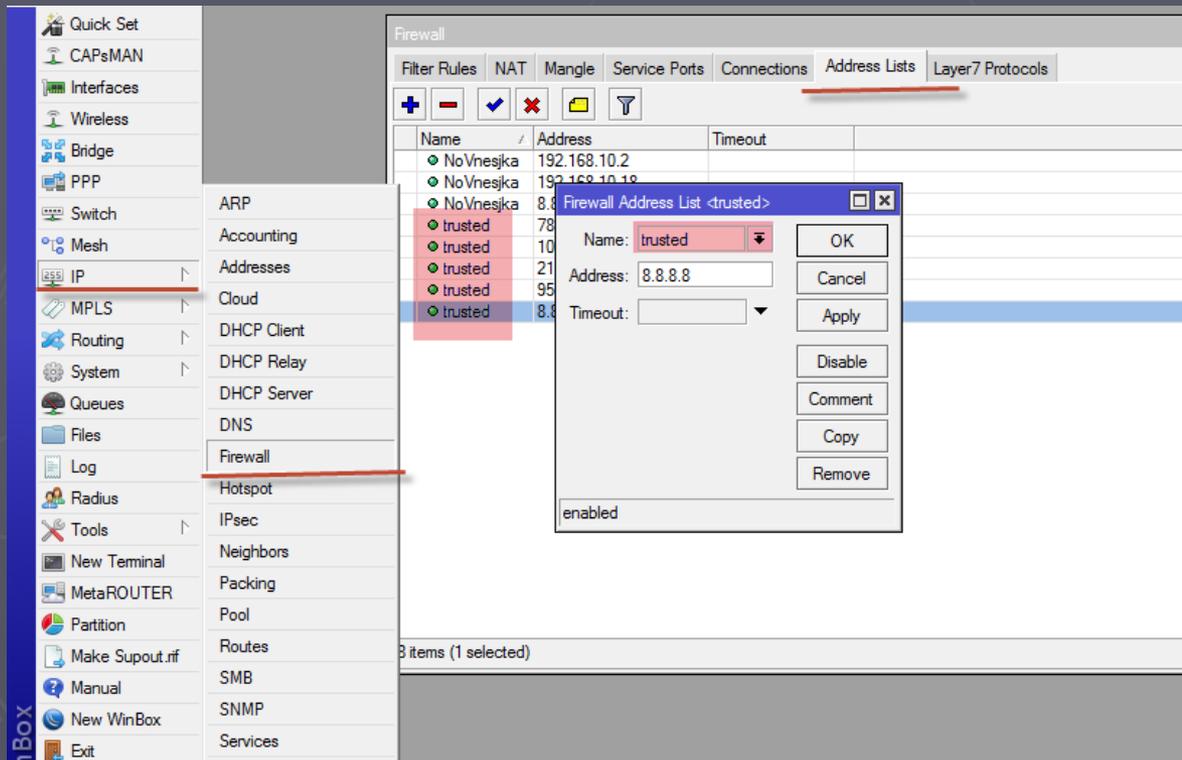
Схема доступа для настоящих админов ☺

Собственная ACL сервиса может иметь уязвимости.



Firewall – проброс портов

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



The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'Address Lists' tab is selected, displaying a table of address lists. A dialog box titled 'Firewall Address List <trusted>' is open, showing the configuration for the 'trusted' address list. The dialog box contains the following fields:

Name	Address	Timeout
● NoVnesjka	192.168.10.2	
● NoVnesjka	192.168.10.18	
● NoVnesjka	8.8.8.8	
● trusted	78	
● trusted	10	
● trusted	21	
● trusted	95	
● trusted	8.8.8.8	

The dialog box 'Firewall Address List <trusted>' has the following fields:

- Name: trusted
- Address: 8.8.8.8
- Timeout: (empty)

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove. Status: enabled

Firewall – проброс портов

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

The screenshot displays the Mikrotik WinBox Firewall configuration interface. The left sidebar shows the 'Firewall' menu item selected. The main window is divided into several panes:

- Filter Rules:** A table with columns for #, Action, and Chain. A rule is visible with Action 'dst-nat' and Chain 'dstnat'.
- NAT Rule <1.1.1.1:13389>:** A configuration window for a NAT rule. The 'General' tab is active, showing:
 - Chain: dstnat
 - Src. Address: (empty)
 - Dst. Address: 1.1.1.1
 - Protocol: 6 (tcp)
 - Src. Port: (empty)
 - Dst. Port: 13389 (highlighted in red)
 - Any. Port: (empty)
 - In. Interface: (empty)
 - Out. Interface: (empty)
 - Packet Mark: (empty)
 - Connection Mark: (empty)
 - Routing Mark: (empty)
 - Routing Table: (empty)
 - Connection Type: (empty)
- New NAT Rule:** A configuration window for a new NAT rule. The 'General' tab is active, showing:
 - Src. Address List: trusted (highlighted in red)
 - Dst. Address List: (empty)
 - Layer7 Protocol: (empty)
 - Content: (empty)
 - Connection Bytes: (empty)
 - Connection Rate: (empty)
 - Per Connection Classifier: (empty)
 - Src. MAC Address: (empty)
 - Out. Bridge Port: (empty)
 - In. Bridge Port: (empty)
 - IPsec Policy: (empty)
 - Ingress Priority: (empty)
 - Priority: (empty)
 - DSCP (TOS): (empty)
- New NAT Rule:** A configuration window for a new NAT rule. The 'General' tab is active, showing:
 - Action: dst-nat
 - Log: (unchecked)
 - Log Prefix: (empty)
 - To Addresses: 10.0.0.2
 - To Ports: 3389 (highlighted in red)

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



The screenshot displays the Mikrotik WinBox interface for configuring a Firewall Mangle Rule. The left sidebar shows the RouterOS WinBox menu with 'IP' selected. The main window is divided into three panes:

- Filter Rules:** A list of existing rules, with rule 5 highlighted.
- Mangle Rule <>:** The configuration window for a new rule. The 'Chain' is set to 'postrouting'. The 'Out. Interface' is 'ether1-gateway'. The 'Action' is 'change DSCP (TOS)'. The 'New DSCP (TOS)' list includes options like 'accept', 'add dst 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 TZSP', and 'strip IPv4 options'. The 'strip IPv4 options' option is highlighted in red.
- New Mangle Rule:** A dialog box for creating a new rule, with the 'Action' set to 'change DSCP (TOS)'. The 'New DSCP (TOS)' list is also visible, with 'strip IPv4 options' highlighted in red.

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 😊

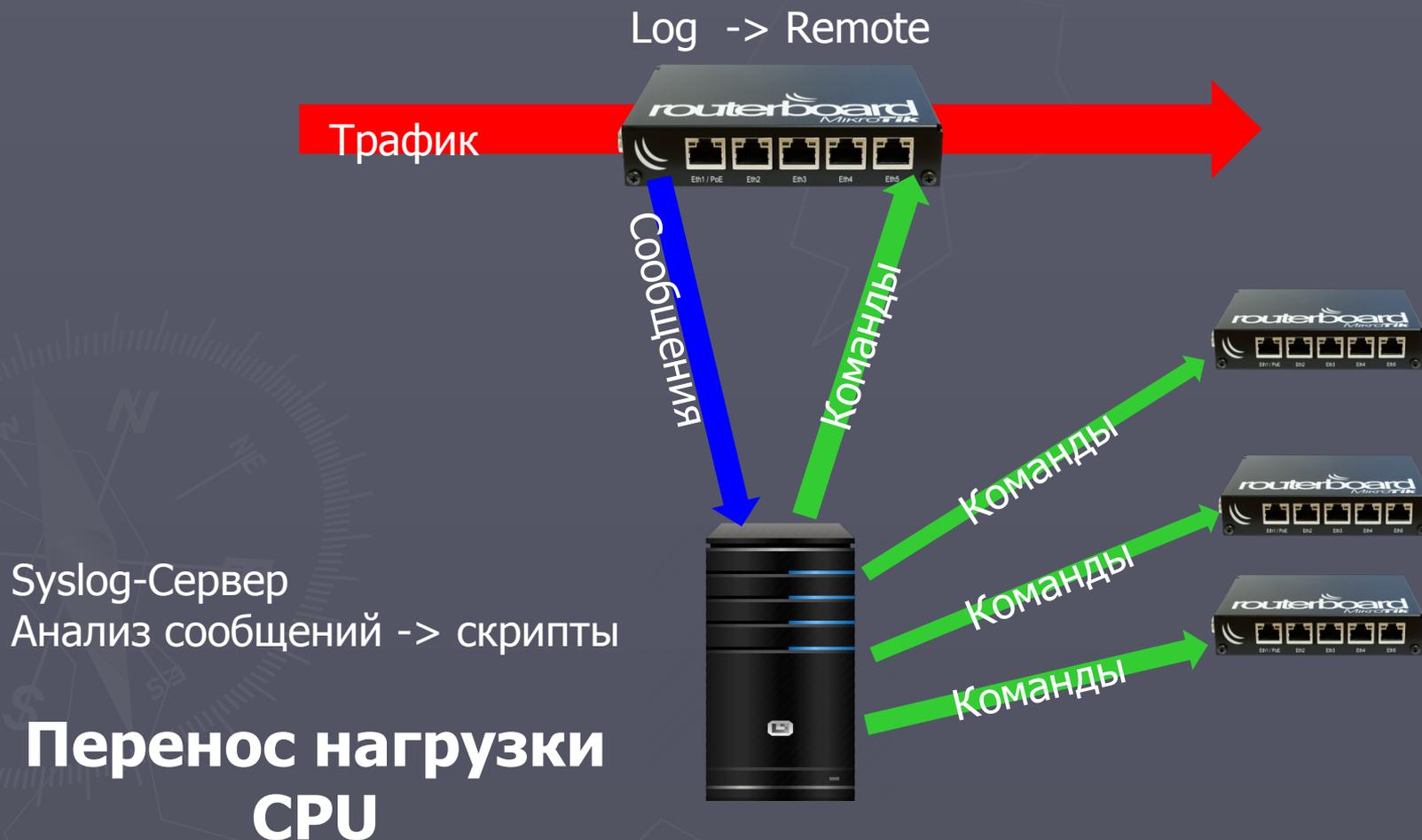
1. Берем по одному адреса из dynamic-list
2. Добавляем по одному в static-list

- ▶

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

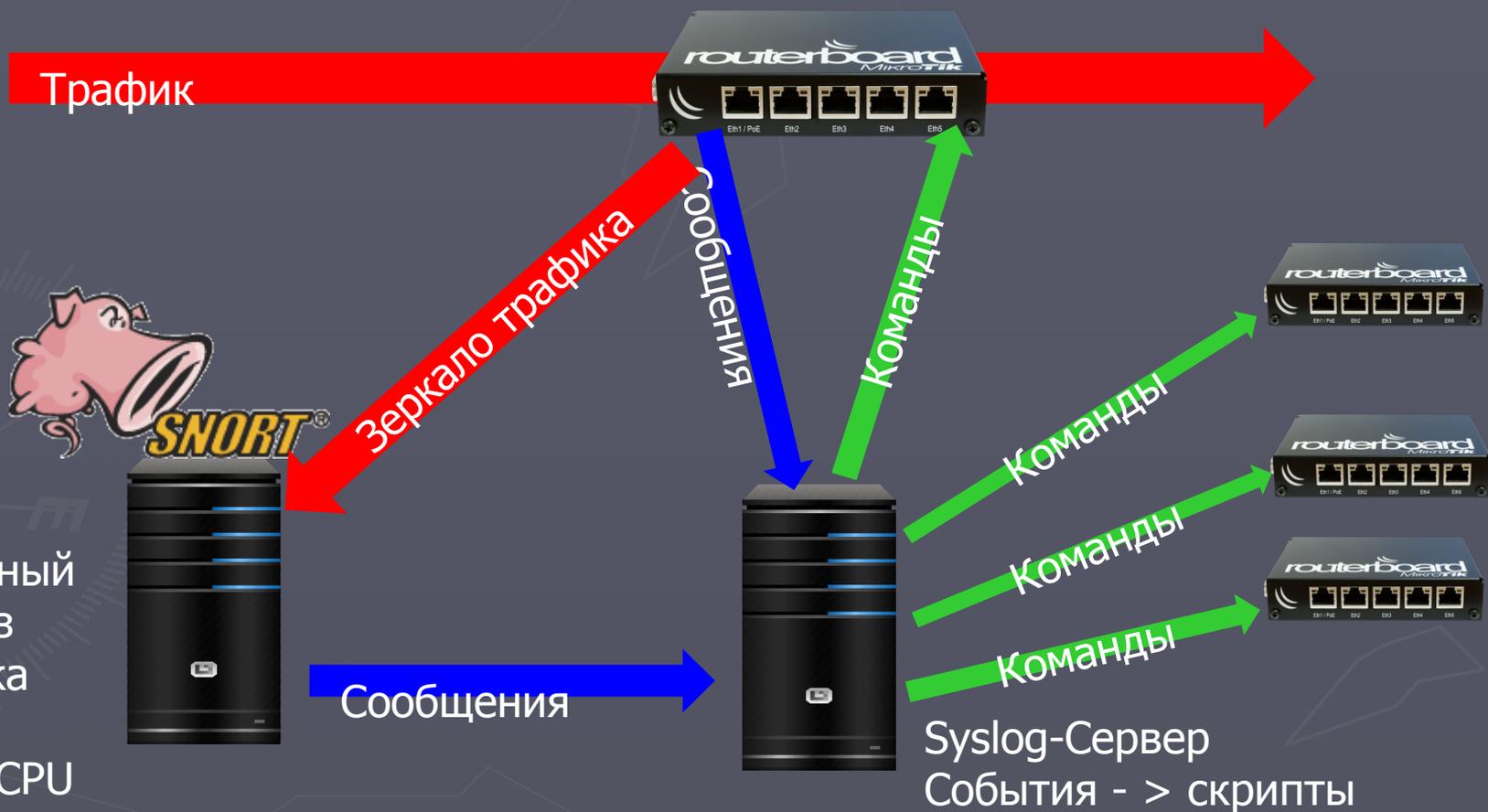
Распределение функций

Экономим ресурсы процессора, делегируя функции



Распределение функций

Экономим ресурсы процессора, делегируя функции



ССЫЛКИ

- ▶ <http://wiki.mikrotik.com> – Документация от вендора
- ▶ <https://www.shodan.io> – Поиск 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