

Безопасность в MikroTik

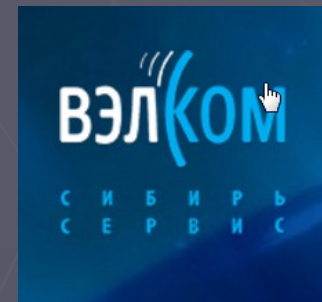
Защита ресурсов сети
и маршрутизатора

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

- ✓ МТСНА
- ✓ МТСРЕ
- ✓ МТСВЕ



- ✓ 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/>


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"?
- 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

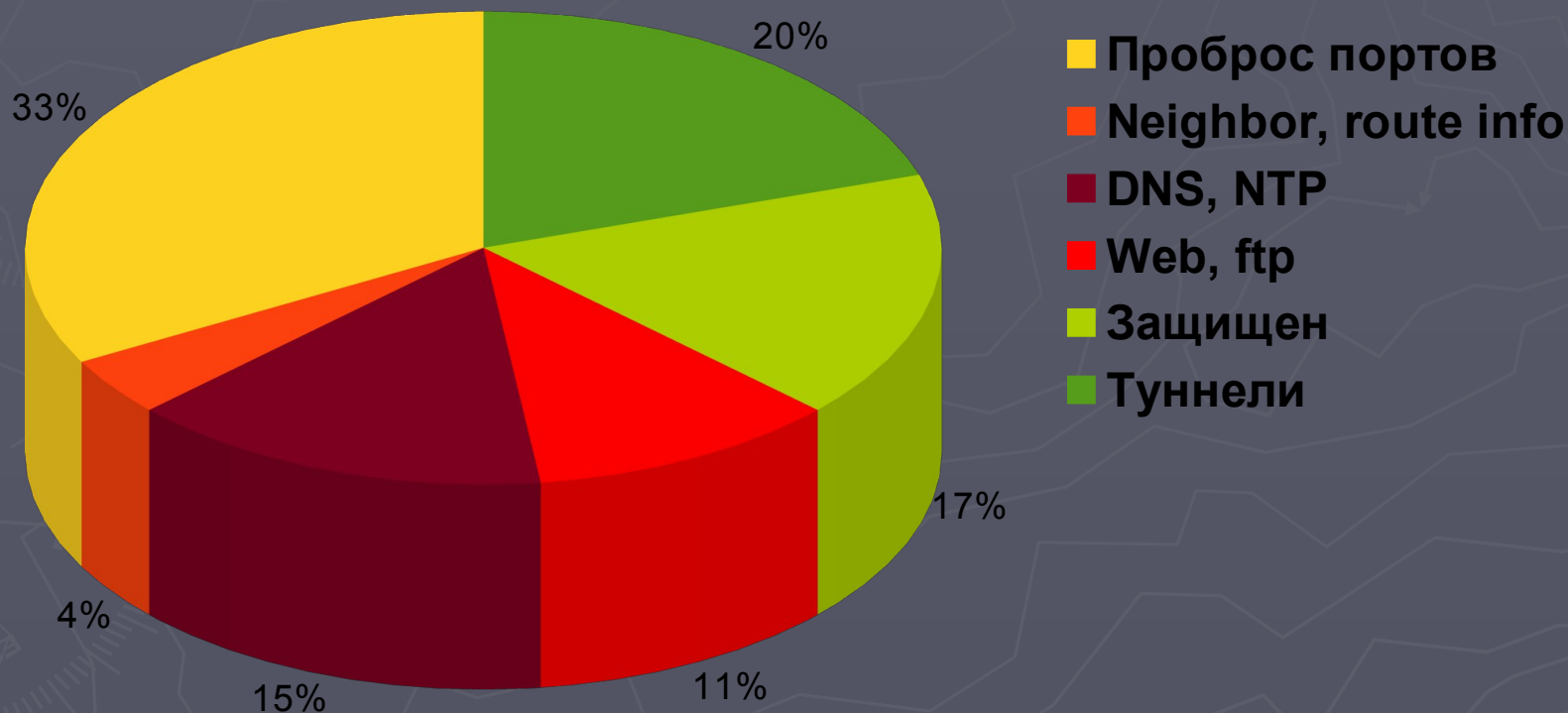
Каталог <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennyye-standarty/377-gosudarstvennyye-standarty>

Стандарты и концепции

Стандарт	Содержание
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

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. 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

Achtung!

По умолчанию Discovery ВКЛЮЧЕН на каждом новом статическом 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. Under the 'Telnet Interfaces' tab, a table lists the following interfaces:

Interface	Discovery
all	X
bridge-local	
ether2-master-local	X
ether4-slave-local	X
ether5	
ether5-slave-local	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 'Neighbors' configuration page. Under the 'Discovery Interfaces' tab, a table lists the following interfaces:

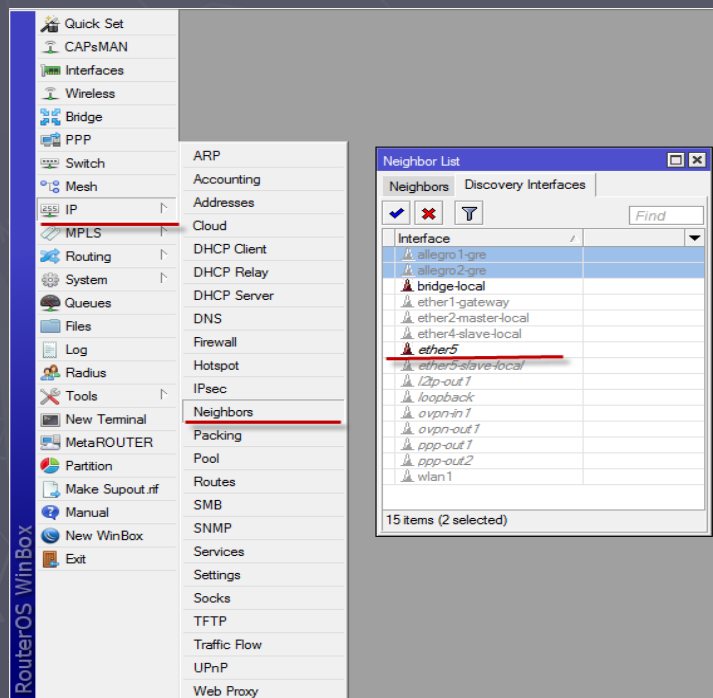
Interface	Discovery
allegro 1-gre	
allegro 2-gre	
bridge-local	
ether1-gateway	
ether2-master-local	
ether4-slave-local	
ether5	
ether5-slave-local	
l2p-out 1	
loopback	
ovpn-in 1	
ovpn-out 1	
ppp-out 1	
ppp-out 2	
wlan1	

Защита каждого L2-интерфейса

Ahtung!

Поведение Discovery умолчанию меняется ТОЛЬКО ЧЕРЕЗ КОНСОЛЬ

Discovery services



/ip neighbors discovery 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 😊

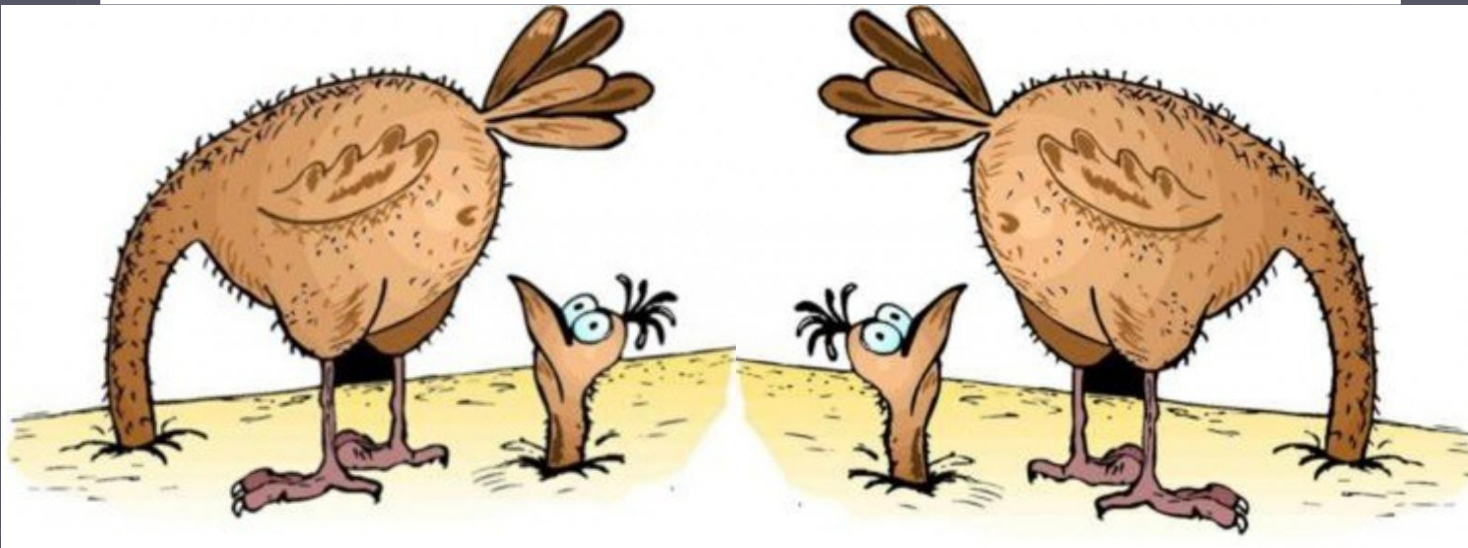
Neighbor – утечка информации

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

The screenshot shows the Mikrotik WinBox interface with the 'mikrotik-cdp-neighbors.pcapng' file open. The main window displays a table of CDP neighbors. The entry with MAC address 01:00:0c:cc:cc:cc is selected, and its details are shown in the lower pane. The details include the device ID 'MT-Tom1', IP address '192.168.88.1', and software version '6.36.2 (stable)'. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

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
```

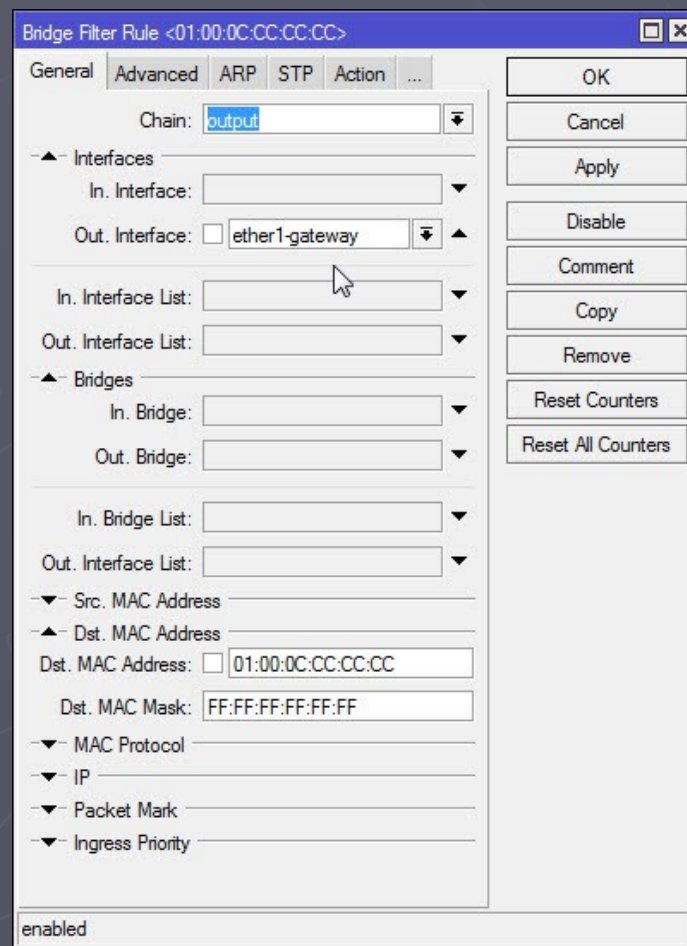
```
0000 01 00 0c cc cc cc e4 8d 8c e1 35 f6 00 5d aa aa .....S..]..
0010 03 00 00 0c 20 00 01 78 8d a8 00 01 00 0b 4d 54 ....x.....MT
0020 2d 54 6f 6d 31 00 02 00 11 00 00 00 01 01 01 cc -Tom1...bridge
0030 00 04 c0 a8 58 01 00 03 00 0e 62 72 69 64 67 65 ...X...hap....
0040 2d 68 61 70 00 04 00 08 00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

Безопасность L2 & MAC

1. Создаем Bridge-WAN

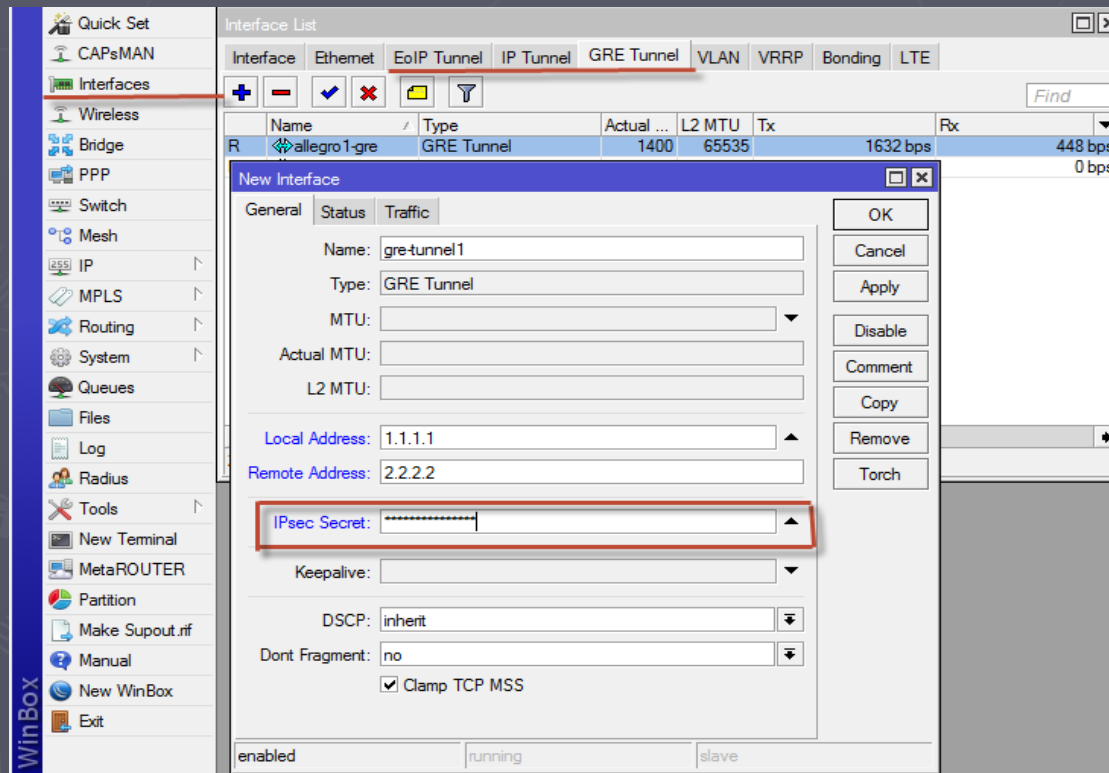
2. Включаем WAN-интерфейс в бридж

3. Создаем Bridge filter с action drop



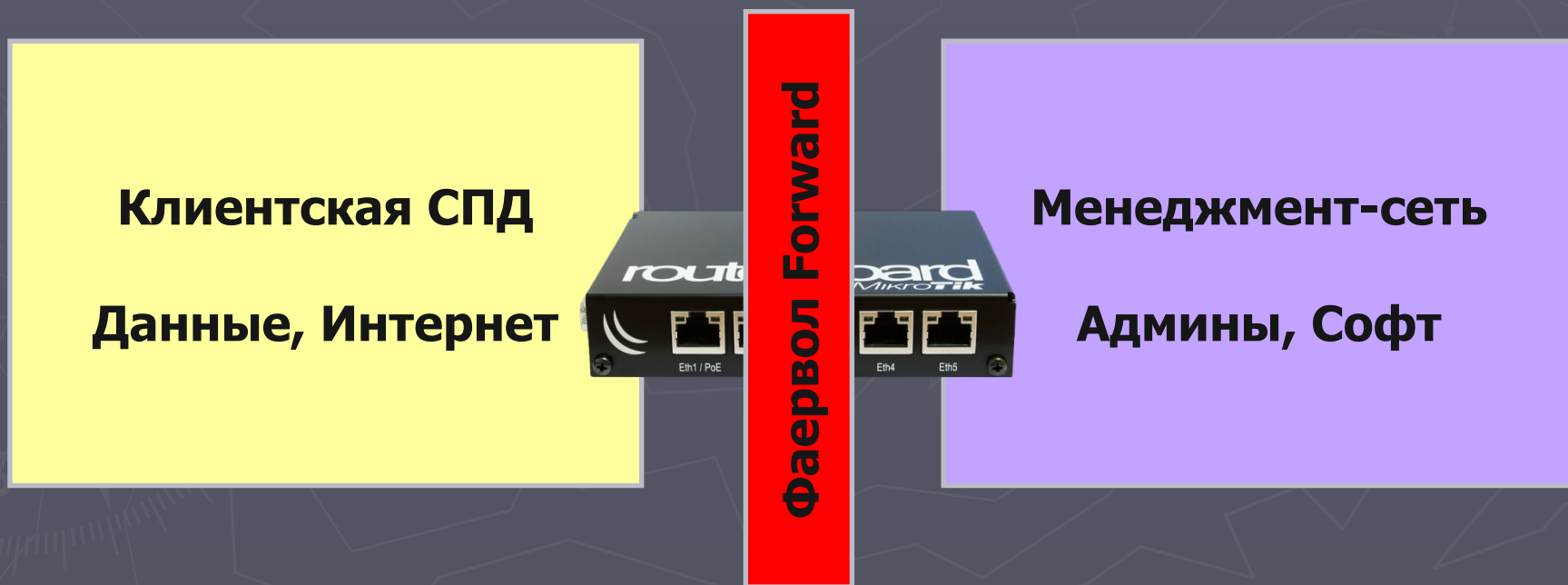
Защита туннелей EoIP/GRE/IPIP

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

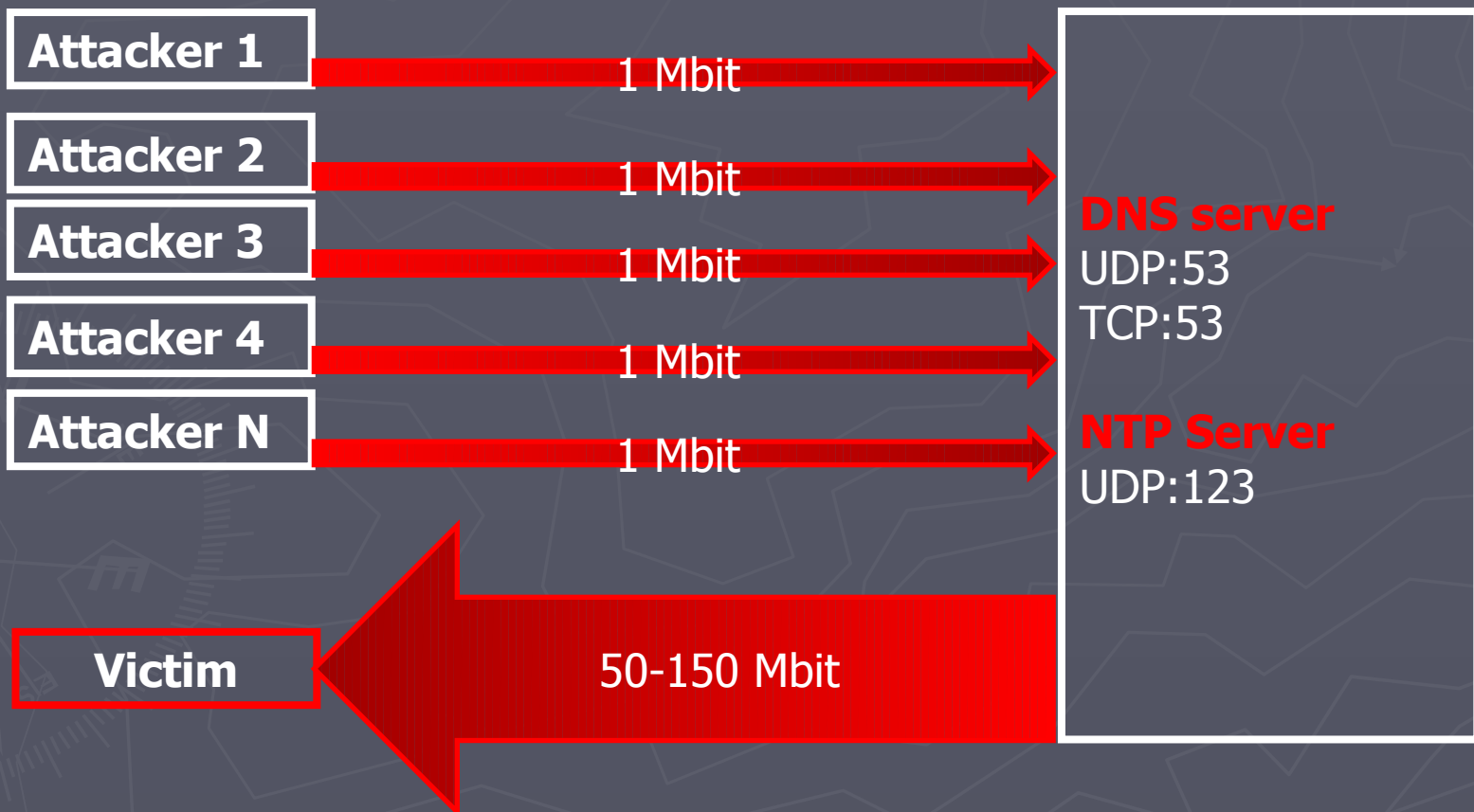
UDP amplification attack

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	<u>GetBulk</u> request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
<u>CharGEN</u>	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
<u>Kad</u>	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

#	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 amplification 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 interface includes standard buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

Защита служб L3/L4

UDP amplification attack solution

- ▶ Ограничить трафик на udp:53 и udp:123 фаерволом

The image shows the RouterOS WinBox interface for configuring a new Firewall Rule. The 'General' tab is active, and the 'Chain' is set to 'input'. The 'Protocol' is set to 'udp', and the 'Dst. Port' is set to '53'. The 'In. Interface' is set to 'bridge-local'. The 'Extra' tab is also visible, showing the 'Connection Limit' section with 'Rate' set to 10 /sec and 'Burst' set to 15. The 'Action' tab is also visible, showing the 'Connection Limit' section with 'Rate' set to 10 /sec and 'Burst' set to 15. The 'Statistics' tab is also visible, showing the 'Connection Limit' section with 'Rate' set to 10 /sec and 'Burst' set to 15.

RouterOS WinBox

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address: []

Dst. Address: []

Protocol: udp

Src. Port: []

Dst. Port: 53

Any. Port: []

P2P: []

In. Interface: bridge-local

Out. Interface: []

Packet Mark: []

Connection Mark: []

Routing Mark: []

Routing Table: []

Connection Type: []

Connection State: []

Connection NAT State: []

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

New Firewall Rule

General Advanced Extra Action Statistics

Connection Limit

Limit

Rate: 10 /sec

Burst: 15

Dst. Limit

Nth

Time

Src. Address Type

Dst. Address Type

PSD

Hotspot

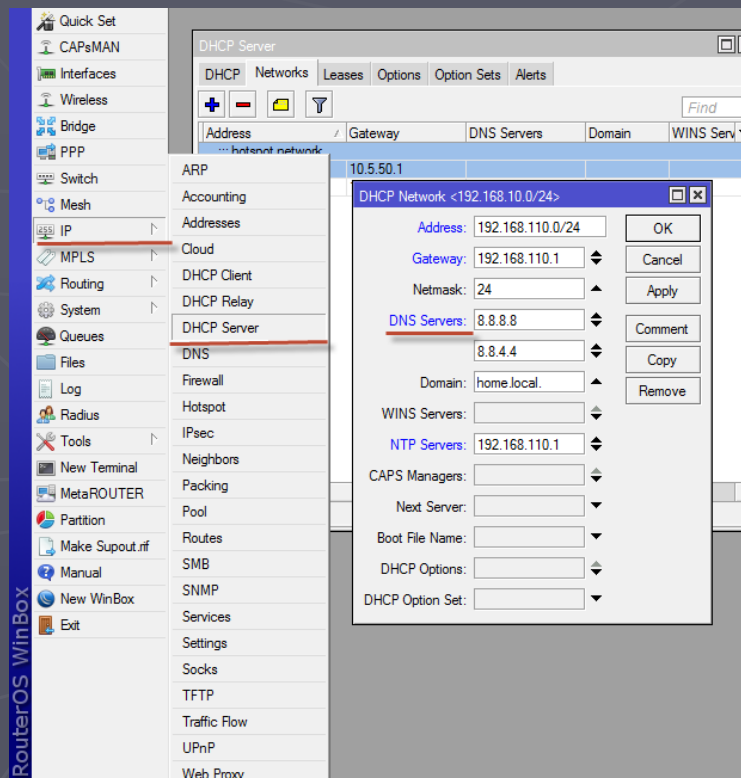
IP Fragment

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

Защита служб L3/L4

UDP amplification 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?

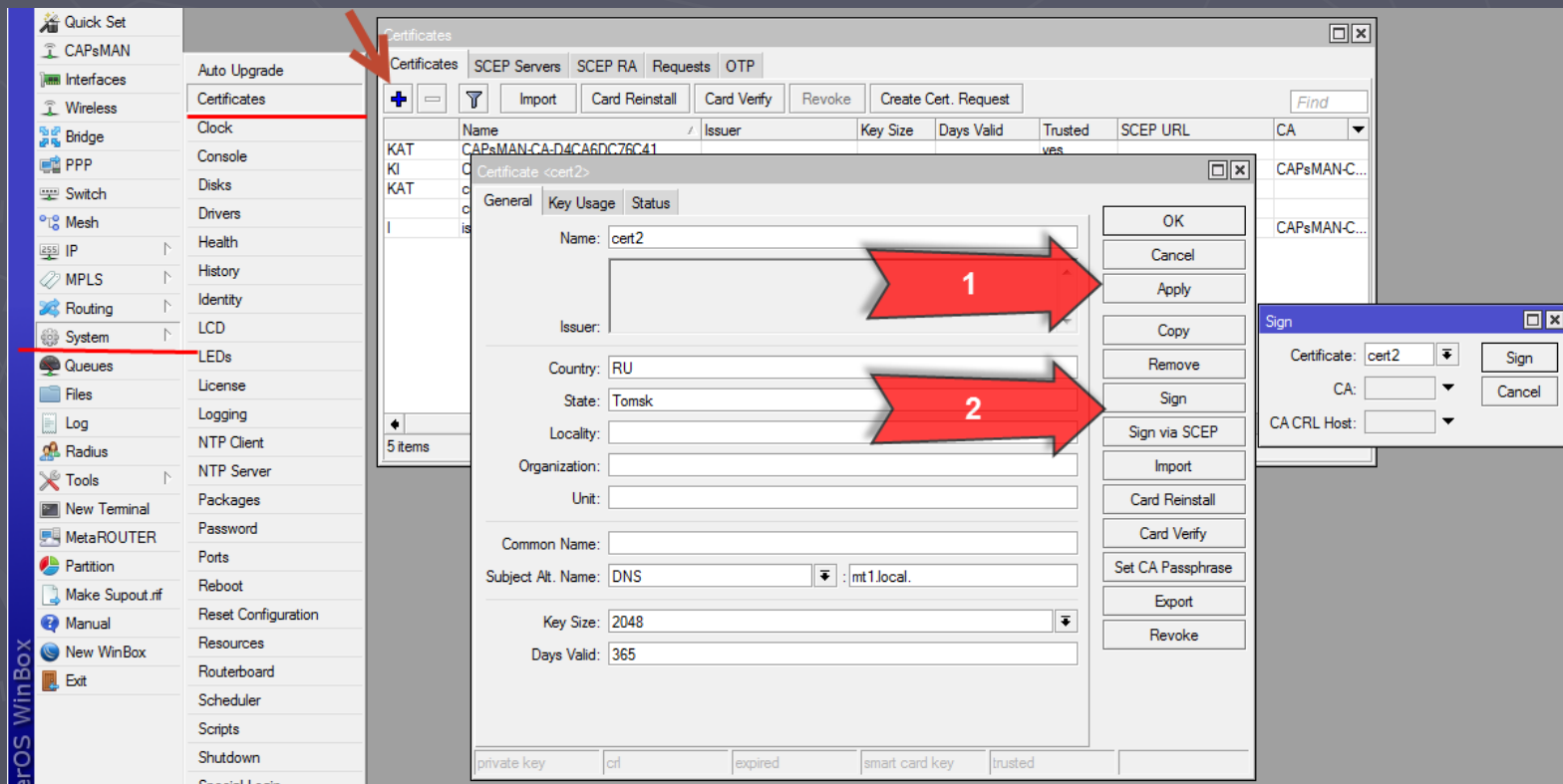
Залить script.rsc.auto?

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 'Services' is selected. The 'IP Service List' window shows a table of services:

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

The 'www-ssl' service is selected. A configuration dialog for 'IP Service <www-ssl>' is open, showing the following settings:

- Name: www-ssl
- Port: 443
- Available From: (empty)
- Certificate: cert1

The 'enabled' checkbox is checked. The 'OK' button is highlighted.

Firewall – проброс портов

DST-NAT + Standart ports → DDoS

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



Firewall – проброс портов

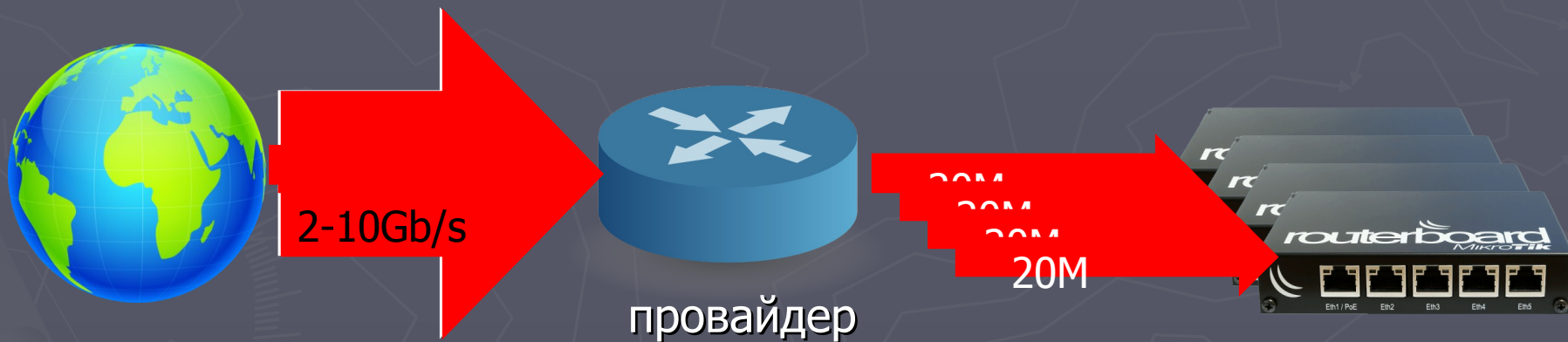
► DST-NAT + Standart ports → **DDoS**



Firewall – проброс портов

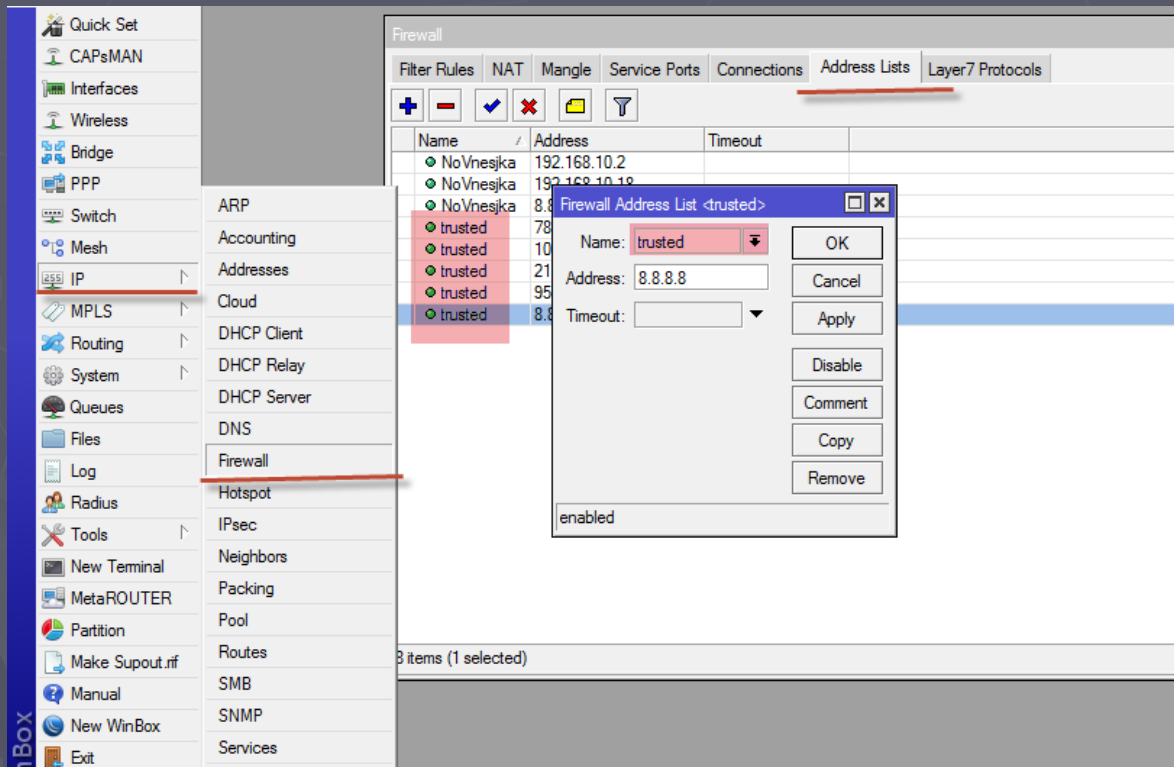
DST-NAT + Standart ports → DDoS

не злите провайдера – вам с ним еще работать



Firewall – проброс портов

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



The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'Address Lists' tab is active, displaying a table with columns 'Name', 'Address', and 'Timeout'. A dialog box titled 'Firewall Address List <trusted>' is open, showing the configuration for a specific address list. The 'Name' is 'trusted', the 'Address' is '8.8.8.8', and the 'Timeout' is empty. The 'enabled' checkbox is checked. The background shows the 'Firewall' configuration window with a table of address lists.

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	

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. The first row shows a rule with Action 'dst-nat' and Chain 'dstnat'.
- NAT Rule <1.1.1.1:13389>:** A configuration window for a NAT rule. The 'Chain' is set to 'dstnat'. The 'Dst. Address' is '1.1.1.1'. The 'Protocol' is '6 (tcp)'. The 'Dst. Port' is '13389', which is highlighted with a red box.
- New NAT Rule:** A configuration window for a new NAT rule. The 'Src. Address List' is set to 'trusted'. The 'Action' is 'dst-nat'. The 'To Ports' is '3389', which is highlighted with a red box.
- General Tab:** Shows the 'Action' dropdown set to 'dst-nat' and the 'Log' checkbox unchecked.

Firewall и IPv6

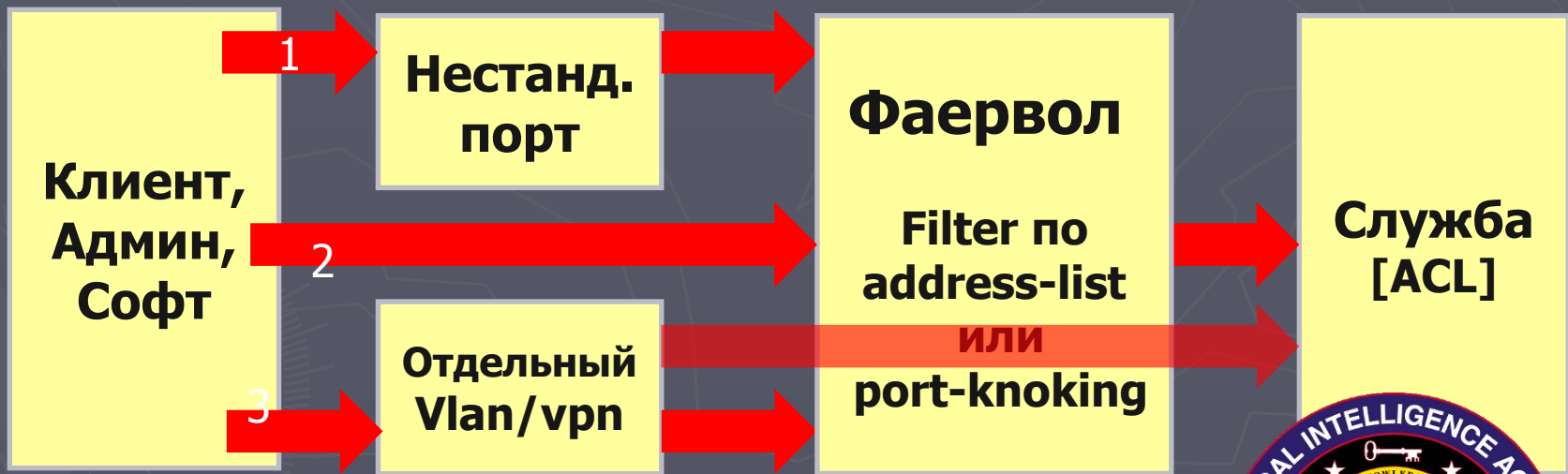
- ✓ IPv6 фаервол по-умолчанию пуст
- ✓ IPv6 фаервол подразумевает АССЕРТ
- ✓ IPv6 запускается на всех интерфейсах
- ✓ IPv6 автоматически создаст себе локальный адрес
- ✓ В IPv6 нет NAT и подсети доступны через forward



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

- 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 («Honeytrap»)

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

Connect to TCP 3389 ? → Blacklist

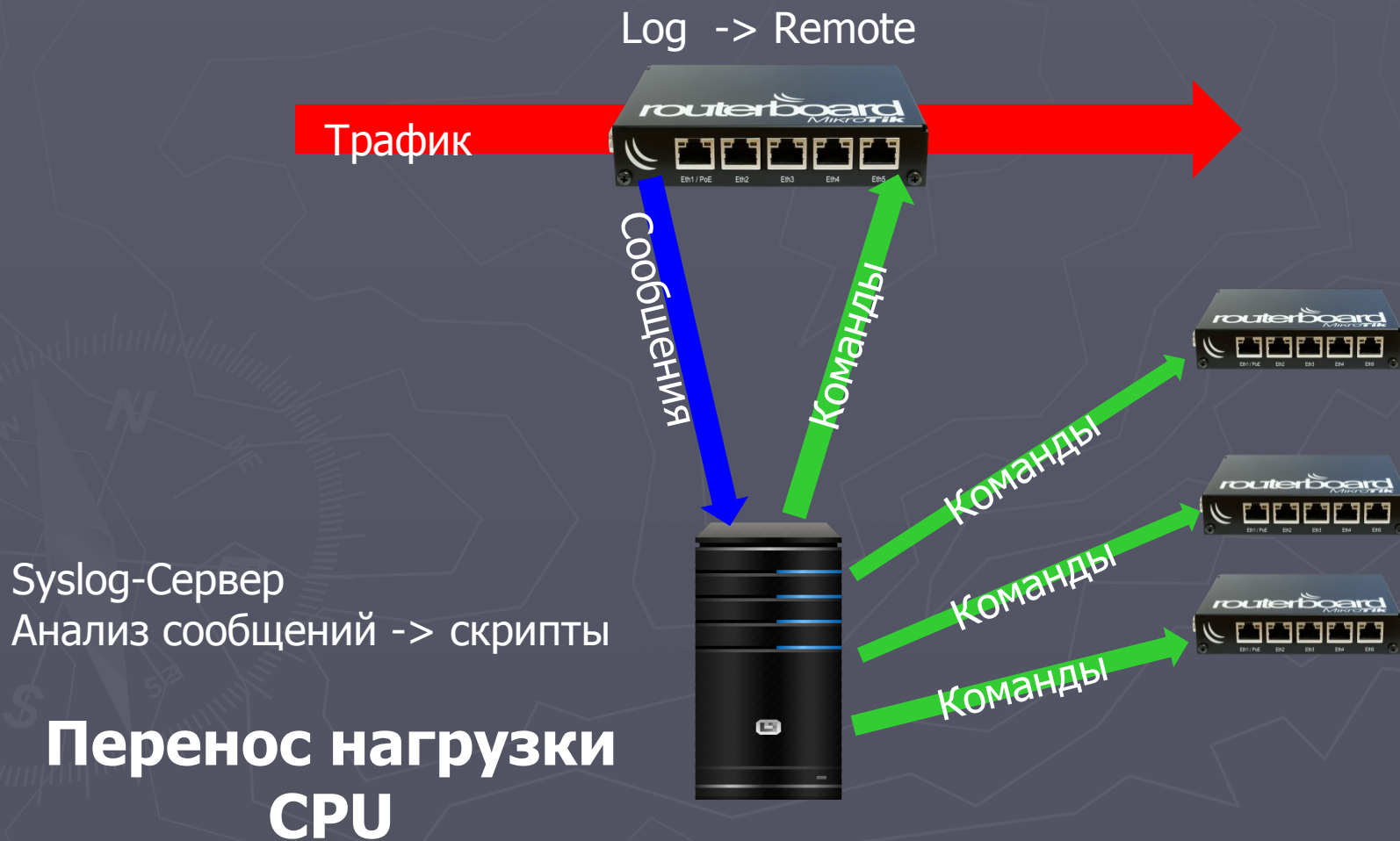
Заносим Src-IP в Address-List “Blacklist”

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"
```

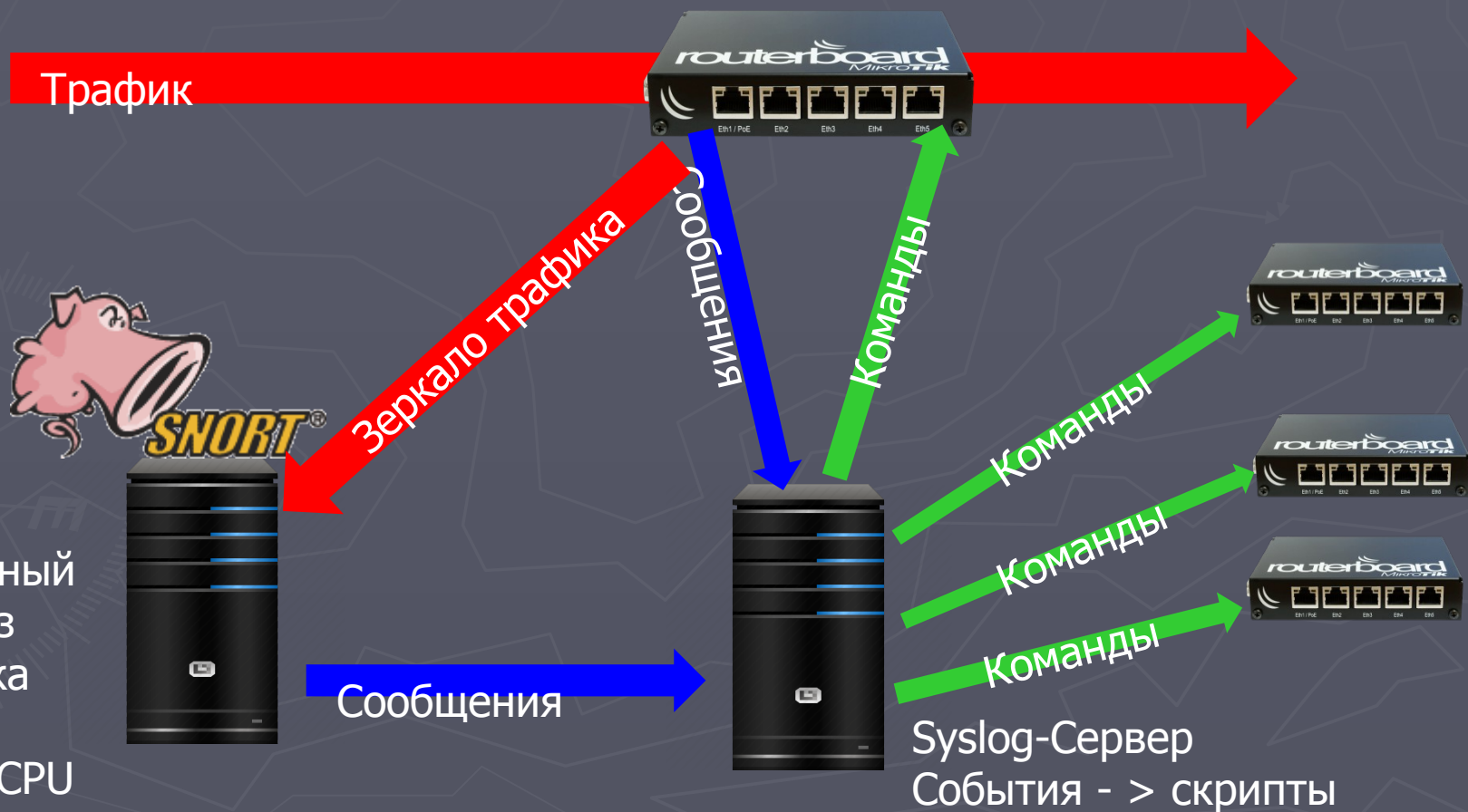
Распределение функций

Экономим ресурсы процессора, делегируя функции



Распределение функций

Экономим ресурсы процессора, делегируя функции



Обработка событий

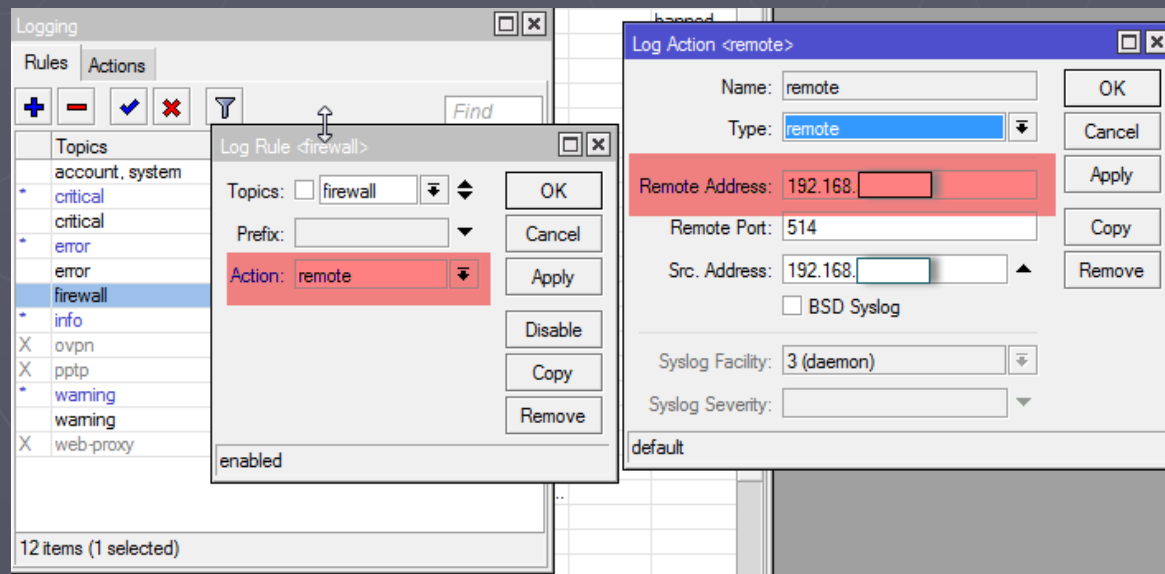
Направляем данные в syslog-сервер:



Сообщения



Syslog-Сервер



The screenshot displays the Mikrotik WinBox interface for configuring a firewall rule. The 'Logging' window is open, showing a list of topics on the left, with 'firewall' selected. The 'Log Rule <firewall>' dialog box is active, showing the 'Action' set to 'remote'. The 'Log Action <remote>' dialog box is also open, showing the configuration for the remote syslog server:

- Name: remote
- Type: remote
- Remote Address: 192.168. (highlighted in red)
- Remote Port: 514
- Src. Address: 192.168. (highlighted in red)
- BSD Syslog:
- Syslog Facility: 3 (daemon)
- Syslog Severity: (dropdown menu)

The 'Log Rule <firewall>' dialog box also shows the 'Topics' set to 'firewall' and the 'Action' set to 'remote'. The 'Log Action <remote>' dialog box has 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' buttons.

Обработка событий

задаем префикс «PortScanDetect»

Firewall Rule <>

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: ether1-gateway

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Firewall Rule <>

General Advanced Extra Action Statistics

Connection Limit

Limit

Det. Limit

Nth

Time

Src. Address Type

Dst. Address Type

PSD

Weight Threshold: 21

Delay Threshold: 00:00:03

Low Port Weight: 3

High Port Weight: 1

Hotspot

IP Fragment

Firewall Rule <>

General Advanced Extra Action Statistics

Action: log

Log

Log Prefix: PortScanDetected

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Обработка событий сервером

Будет запущен bash-скрипт `"/usr/sbin/onportscan.sh"`

► `/etc/rsyslog.conf`

```
#### GLOBAL DIRECTIVES ####
```

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

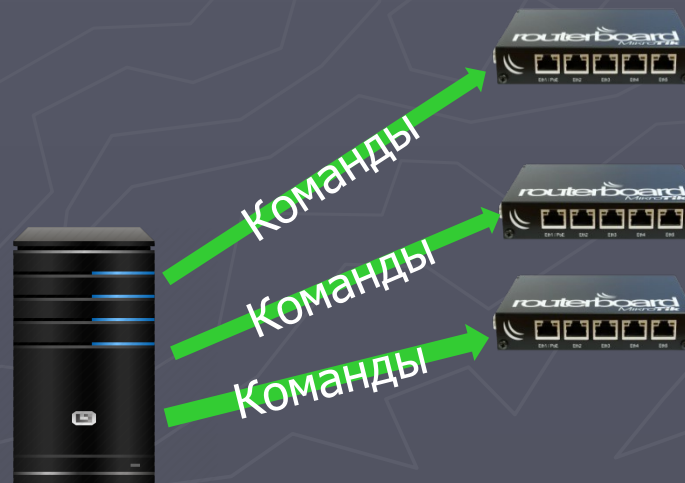
```
#### RULES ####
```

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

Из скрипта запускаем что хотим:

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

Syslog-Сервер



Конкурс HackMe

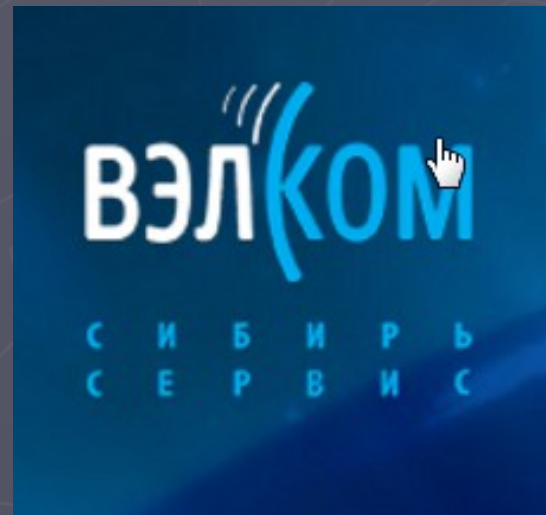
Задача: войти на устройство по WiFi с администраторскими правами и создать пользователя со своим логином

ssid: hackme

MikroTik IP: 192.168.88.1

Login: user

No password



ССЫЛКИ

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