

Защита Mikrotik от внешних угроз

Содержание вебинара

- Что производит компания MikroTik? Где узнать подробности
- Выбор оборудования для офиса
- Выбор беспроводного оборудования
- X86(CHR) vs Tile

Общие концепции обеспечения защиты RouterOS

- Все порты управления должны быть закрыты
- Все что не используется должно быть отключено
- Не доверяем любым «зашифрованным» протоколам
- Всегда считаем что уязвимо все

RouterOS Services

Различные способы подключения и управления RouterOS

- **API** - Application Programming Interface
- **FTP** - файловый протокол для загрузки и выгрузки файлов с RouterOS

Name	Port	Available From	Certificate
X • api	8728		
X • api-ssl	8729		none
• ftp	21	192.168.88.5	
• ssh	22		
• telnet	23		
• winbox	8291		
• www	80		
X • www-ssl	443		none

8 items

IP → Services

RouterOS Services

- **SSH** - шифрованный command line interface
- **Telnet** – не шифрованный command line interface
- **WinBox** - GUI доступ
- **WWW** – доступ через веб

	Name	Port	Available From	Certificate
X	• api	8728		
X	• api-ssl	8729		none
•	ftp	21	192.168.88.5	
•	ssh	22		
•	telnet	23		
•	winbox	8291		
•	www	80		
X	• www-ssl	443		none

8 items

IP → Services

RouterOS Services

- Возможно отключить неиспользуемые службы
- Указать доступ из конкретных подсетей
- Возможно изменить порты по умолчанию



	Name	Port	Available From	Certificate
X	• api	8728		
X	• api-ssl	8729		none
	• ftp	21	192.168.88.5	
	• ssh	22		
	• telnet	23		
	• winbox	8291		
	• www	80		
X	• www-ssl	443		none

8 items

IP → Services

Frequently Used Ports

Port	Service
80/tcp	HTTP
443/tcp	HTTPS
22/tcp	SSH
23/tcp	Telnet
20,21/tcp	FTP
8291/tcp	WinBox
5678/udp	MikroTik Neighbor Discovery
20561/udp	MAC WinBox

MikroTik Neighbor Discovery

- Протокол MikroTik Neighbor Discovery (MNDP) и LLDP позволяет «находить» другие устройства, совместимые с MNDP или CDP (Протокол обнаружения Cisco) или LLDP в широковещательном домене Layer2
- По умолчанию Discovery ВКЛЮЧЕН на каждом новом статическом интерфейсе.
- **Neighbor service распространяет информацию:**
 - О модели устройства;
 - О версии OS
 - О MAC и IP адресах;
 - Об UpTime
 - наличии IPv6 и прочее

MikroTik Neighbor Discovery

The screenshot shows the 'Neighbor List' window in MikroTik WinBox. It contains a table of discovered neighbors and a 'Discovery Settings' dialog box.

Neighbor List Table:

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
bridge1		0C:C4:7A:FB:22:20							
			MikroTik	6.40.8 (...)	RB750Gr3		no	26	00:00:00
			MikroTik	6.41.2 (...)	CHR		no	1	230d 03:38:17
			MikroTik	6.41 (st...	CHR		no	7	253d 04:50:02
			MikroTik	6.42.6 (...)	CCR100...		no	46	58d 05:00:34
			MikroTik	6.42.1 (...)	CHR		no	43	159d 22:18:50
			MikroTik	6.40.8 (...)	RB750Gr3		no	27	5d 05:27:18
			MikroTik	6.42.6 (...)	RB750Gr3		no	31	9d 11:53:26
			MikroTik	6.43.2 (...)	CHR		no	36	2d 07:16:09
			MikroTik	6.42.6 (...)	CHR		no	1	69d 03:43:33

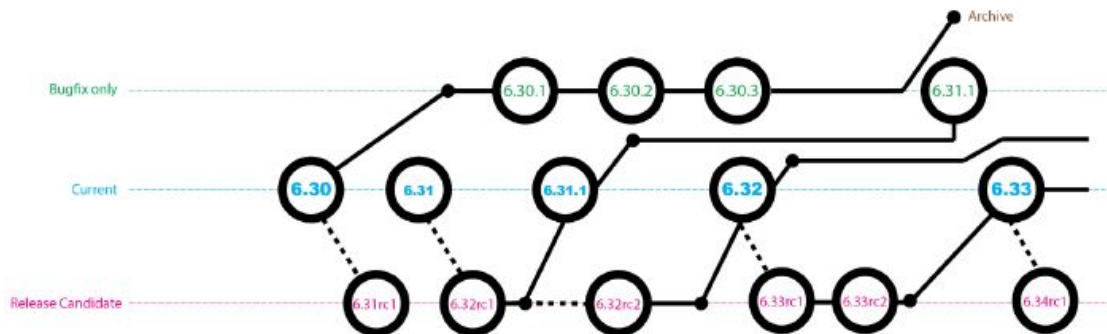
Discovery Settings Dialog:

Interface: WAN

Buttons: OK, Cancel, Apply

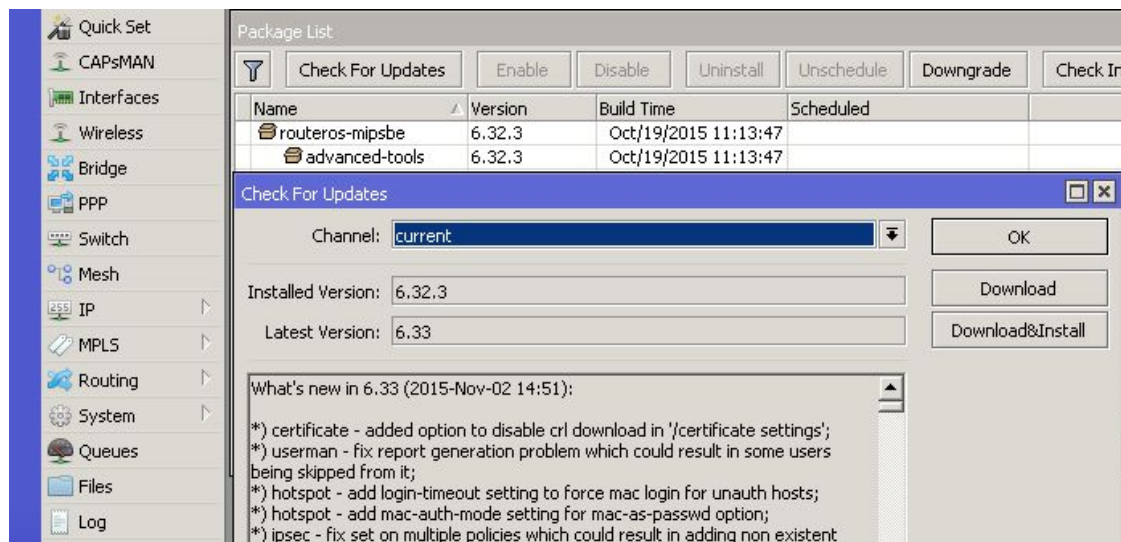
RouterOS Версии

- **Long-term** – исправление ошибок
- **Stable** – Исправление ошибок и новый функционал
- **Testing** – ночные сборки



Обновление RouterOS

Простой способ обновления



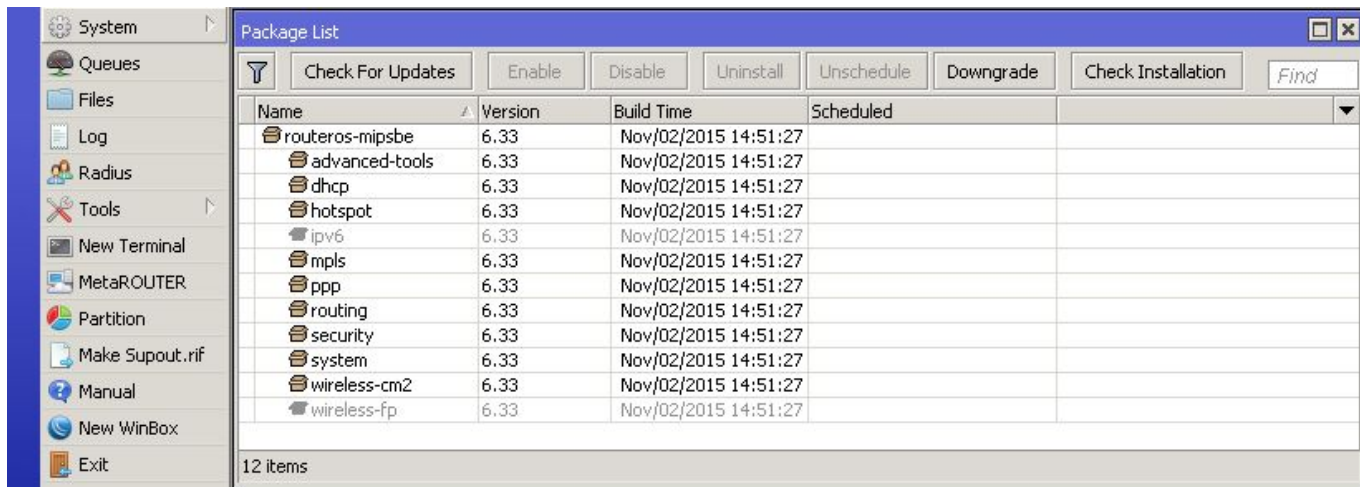
System → Packages → Check For Updates

Обновление RouterOS

- Скачайте обновление со страницы www.mikrotik.com/download
- Проверьте архитектуру процессора Вашего роутера
- Перетащить файл обновления в окно WinBox
- Другие пути: WebFig Files menu, FTP, sFTP
- Перезагрузите роутер

Package Management

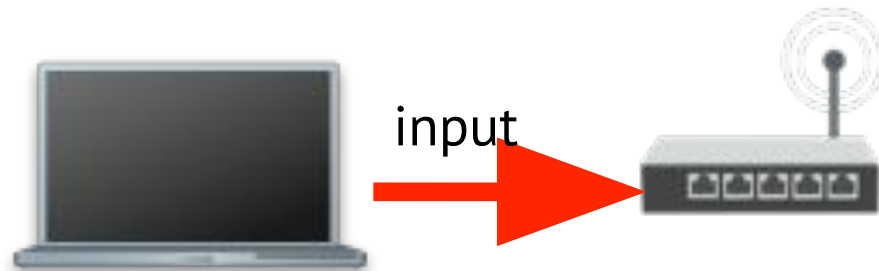
В RouterOS возможно отключать и включать пакеты
(enabled/disabled)



System → Packages

Chain: input

- Защищает сам маршрутизатор
- Либо из Интернета, либо из внутренней сети



Типы сетевых вторжений

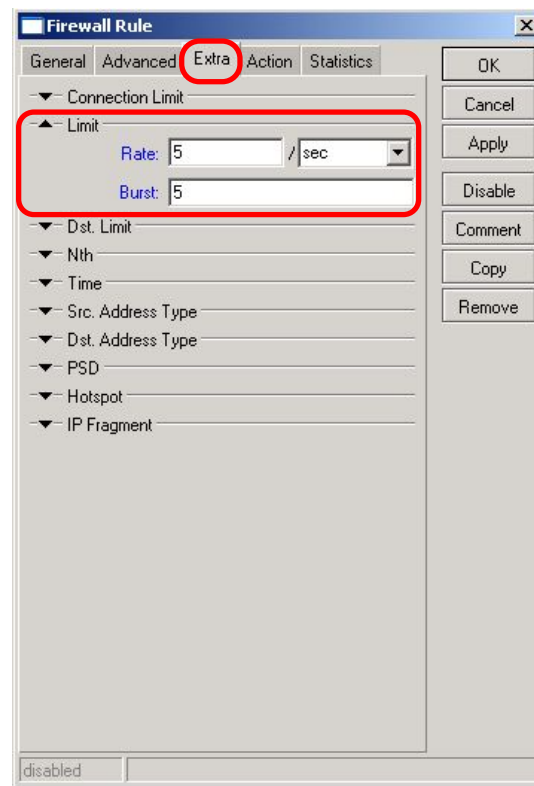
Сетевое вторжение представляет собой серьезную угрозу безопасности, которая может привести не только к временному отказу, но и к общему отказу от сетевого обслуживания

Мы разберем 4 типа сетевых вторжений:

- Ping flood
- Port scan
- DoS attack
- DDoS attack

Ping Flood

- Ping flood обычно состоят из томов случайных сообщений
- ICMP с условием «limit» можно связать скорость соответствия правила с заданным пределом
- Это условие часто используется с действием "log"



ICMP Message Types

Типичный IP-маршрутизатор использует только пять типов сообщений ICMP (type:code)

- For PING - messages **0:0** and **8:0**
- For TRACEROUTE – messages **11:0** and **3:3**
- For Path MTU discovery – message **3:4**

Другие типы сообщений ICMP должны быть заблокированы

ICMP Message Rule Example

The screenshot shows the 'Firewall Rule' configuration window with the 'General' tab selected. The 'Chain' dropdown is set to 'ICMP'. The 'Protocol' dropdown is set to '1 (icmp)'. The status at the bottom is 'disabled'.

Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: ICMP

Src. Address:
Dst. Address:
Protocol: 1 (icmp)
Src. Port:
Dst. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
Routing Mark:
Connection State:
Connection Type:
disabled

The screenshot shows the 'Firewall Rule' configuration window with the 'Advanced' tab selected. The 'ICMP Options' section is expanded, showing 'ICMP Type' set to '8 (echo request)' and 'ICMP Code' checked and set to '0'. The status at the bottom is 'disabled'.

Firewall Rule

General | Advanced | Extra | Action | Statistics

Src. Address List:
Dst. Address List:
Content:
Connection Bytes:
MAC Address:
Out. Bridge Port:
In. Bridge Port:
IPv4 Options:
TOS:
TCP MSS:
Packet Size:
Random:
TCP Flags:
ICMP Options:
ICMP Type: 8 (echo request)
ICMP Code: 0
disabled

ICMP Flood Lab

Сделать новую цепочку – ICMP

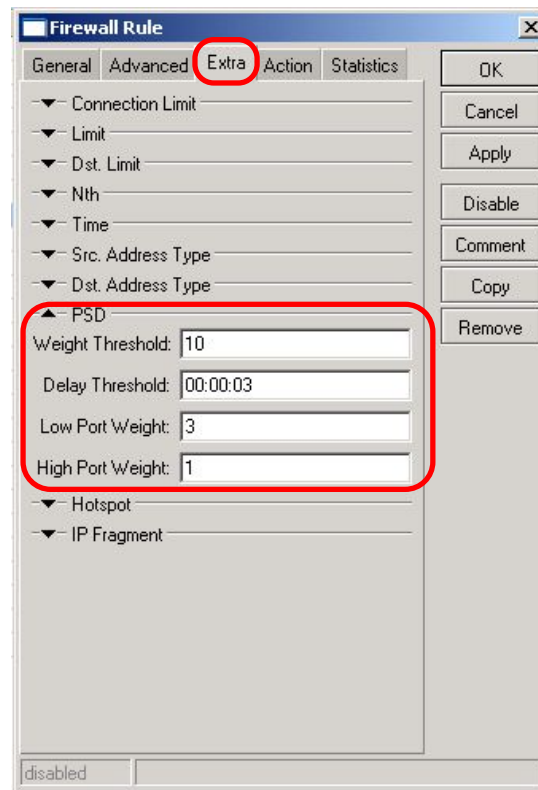
- Принять 5 необходимых сообщений ICMP
- Установите rate до 5 pps с возможностью пакетной всплеска
- Drop все остальные ICMP packets

Поместить все ICMP-пакеты в цепочку ICMP

- Create an action “**jump**” rule in the chain Input
- Place it accordingly
- Create an action “**jump**” rule in the chain Forward
- Place it accordingly

Port Scan

- Port Scan - последовательное отслеживание портов TCP (UDP)
- PSD (обнаружение сканирования портов) возможно только для протокола TCP
- Low ports
- From 0 to 1023
- High ports
- From 1024 to 65535



DoS Attacks

- Основной целью DoS-атак является потребление ресурсов, таких как процессорное время или пропускная способность, поэтому стандартные службы получают отказ в обслуживании (DoS)
- Обычно маршрутизатор заполняется пакетами TCP / SYN (запрос на соединение). Вызов сервера для ответа с помощью пакета TCP / SYN-ACK и ожидание пакета TCP / ACK.
- В основном DoS-атакующие - это зараженные вирусом клиенты

DoS Attack Protection

- Все IP-адреса с более чем 10 подключениями к маршрутизатору должны рассматриваться как DoS-атакующие
- С каждым удаленным соединением TCP мы разрешаем злоумышленнику создавать новое соединение
- Мы должны внедрить защиту DoS в 2 этапа:
 - Обнаружение - создание списка злоумышленников DoS на основе ограничения connection-limit
 - Подавление - применение ограничений для обнаруженных злоумышленников DoS

DoS Attack Detection

New Firewall Rule

General Advanced **Extra** Action Statistics

OK Cancel Apply Disable Comment Copy Remove

Connection Limit

Limit: 10

Netmask: 32

Limit

Dst. Limit

Nth

Time

Src. Address Type

Dst. Address Type

PSD

Hotspot

IP Fragment

disabled

New Firewall Rule

General Advanced Extra **Action** Statistics

OK Cancel Apply Disable Comment Copy Remove

Action: add src to address list

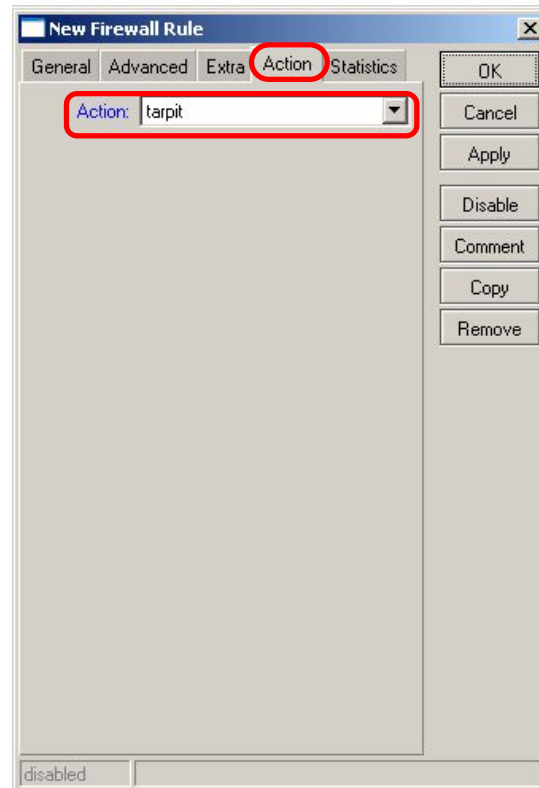
Address List: black_list

Timeout: 1d 00:00:00

disabled

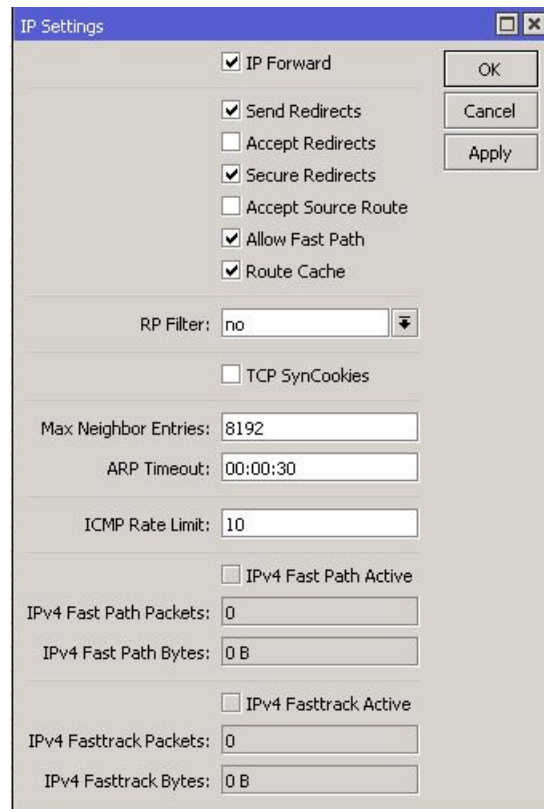
DoS Attack Suppression

- Чтобы остановить атакующего от создания новых подключений, мы будем использовать действие «tarpit»
- Мы должны поставить это правило перед правилом обнаружения, иначе запись адреса-списка будет переписываться все время



DDoS attacks

- Атака распределенного отказа в обслуживании очень похожа на атаку DoS, только она идет из нескольких скомпрометированных систем
- Единственное, что может помочь, это вариант «TCPSyn Cookie» в системе /ip settings



IP Settings

☒ IP Forward

☒ Send Redirects

☐ Accept Redirects

☒ Secure Redirects

☐ Accept Source Route

☒ Allow Fast Path

☒ Route Cache

RP Filter: no

☐ TCP SynCookies

Max Neighbor Entries: 8192

ARP Timeout: 00:00:30

ICMP Rate Limit: 10

☐ IPv4 Fast Path Active

IPv4 Fast Path Packets: 0

IPv4 Fast Path Bytes: 0 B

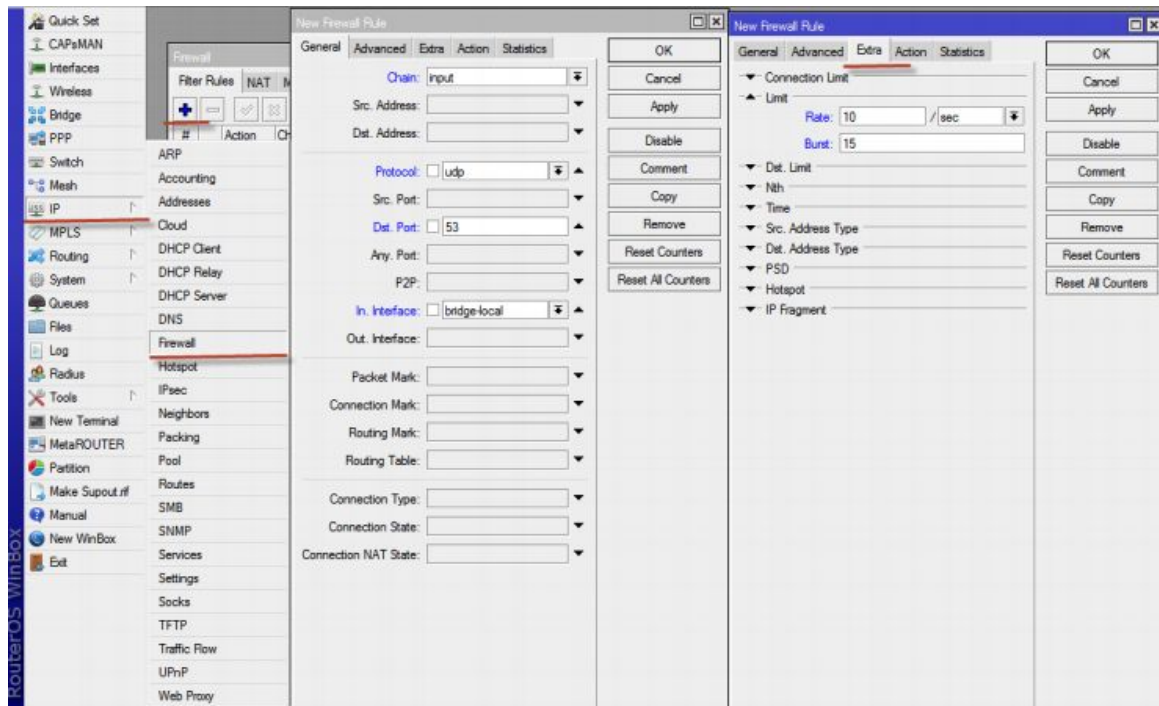
☐ IPv4 Fasttrack Active

IPv4 Fasttrack Packets: 0

IPv4 Fasttrack Bytes: 0 B

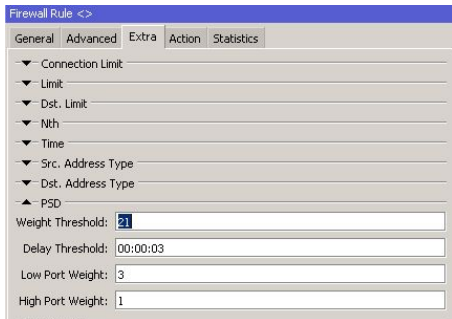
Защита DNS

Защищаем
кеширующий
сервер из
локальной сети



Защита от сканирования портов

- Закрываете выход из локальной сети по sip портам
- Возможно запрещать выход в интернет по времени для ip телефонной станции



Port Scan Detect. Опция позволяющая настроить определение события сканирования портов.

Поля:

- **Weight Threshold** = При каком значении работает.
- **Delay Threshold** = Максимальная задержка между пакетами с разными портами назначения, пришедшими с одного адреса.
- **Low Port Weight** = сколько при подсчете стоит каждый порт в диапазоне 0-1023.
- **High Port Weight** = сколько при подсчете стоит каждый порт в диапазоне 1024-65535.



20-21 СЕНТЯБРЯ | МОСКВА

ASTERCONF

'19

ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ
ПО ASTERISK



300
УЧАСТНИКОВ В МОСКВЕ



150
УЧАСТНИКОВ
В ОНЛАЙН-ТРАНСЛЯЦИИ



30+
ДОКЛАДОВ И МАСТЕР-КЛАССОВ



МАЛЫЙ ЗАЛ
ДЛЯ МАСТЕР-КЛАССОВ



БОЛЬШОЙ ЗАЛ
ДЛЯ ДОКЛАДОВ

<http://asterconf.ru>

voxl**ink**

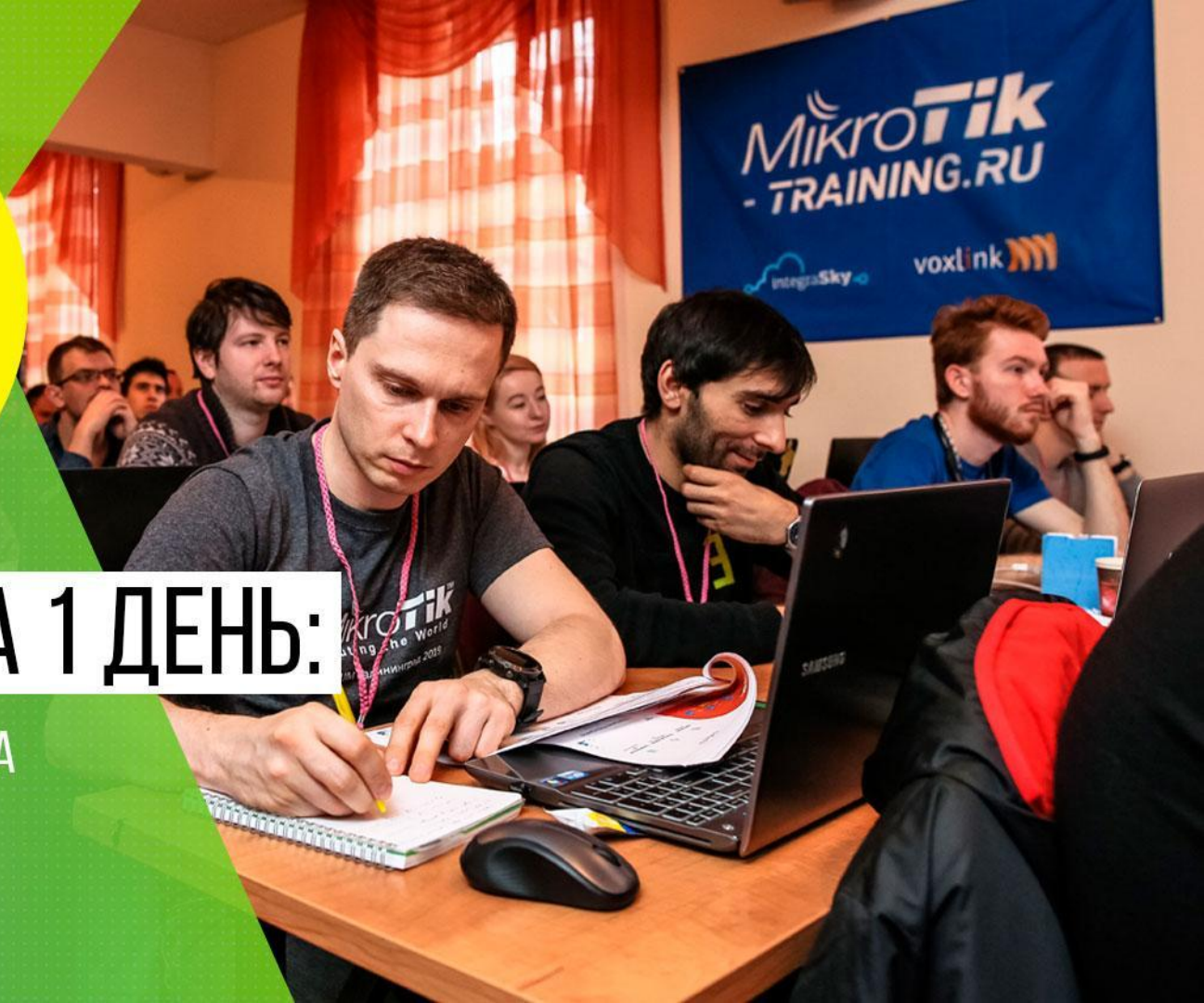


4 и 5
ОКТАБРЯ

МІКРОТІК ЗА 1 ДЕНЬ:

КУРС МОЛОДОГО БОЙЦА

КУРС ПО ЗАЩИТЕ СЕТИ
С ПОМОЩЬЮ МІКРОТІК



MikroTik

MUM

MIKROTIK USER MEETING

**WiFlow - система
сбора MAC-адресов
и регистрации в WiFi
на Mikrotik**

RUSSIA ON SEPTEMBER 06 - 07, 2019



Сергей Грушко
(Voxlink, Россия)

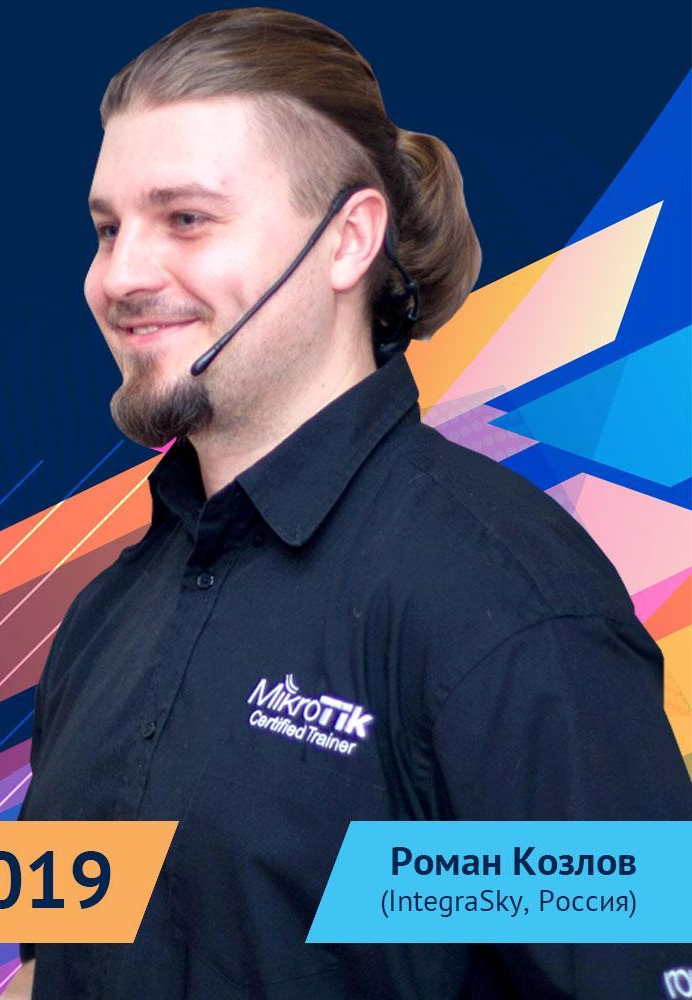
MikroTik

MUM

MIKROTIK USER MEETING

Использование возможностей коммутаторов на RouterOS

RUSSIA ON SEPTEMBER 06 - 07, 2019



Роман Козлов
(IntegraSky, Россия)

СПАСИБО ЗА ВНИМАНИЕ

Приходите на наши курсы по
Mikrotik и Asterisk

