

*Mikro**Tiik**.Me*

MikroTik.Me

- **Васильев Кирилл**
- **Санкт-Петербург**
- **Курсы MikroTik**
- **Поддержка**
- **Разработка ПО**
- **Продажа**



Оптимизация Firewall

Name	CPU	Usage
total		97.0 
firewall		82.5 

2672	✓ acc	forward
2673	✓ acc	forward
2674	✗ drop	forward



2675 items (1 selected)

Фильтры RouterOS

- **External Filter**

Фильтры RouterOS

- **External Filter**
- **Flags connection-tracker**

Фильтры RouterOS

- **External Filter**
- **Flags connection-tracker**
- **From IP Header**

Фильтры RouterOS

- **External Filter**
- **Flags connection-tracker**
- **From IP Header**
- **From Protocol Header**

Фильтры RouterOS

- **External Filter**
- **Flags connection-tracker**
- **From IP Header**
- **From Protocol Header**
- **Used connection-tracker**

Фильтры RouterOS

- **External Filter**
- **Flags connection-tracker**
- **From IP Header**
- **From Protocol Header**
- **Used connection-tracker**
- **From payload**

External Filter

- Данные из вышестоящего заголовка (например Ethernet)
 - mac address
- Данные из пройденных процессов RouterOS
 - interface
 - mark-packet
 - routing-mark и routing-table
 - Hotspot status

Flags connection-tracker

- Состояние соединения на момент прохождения пакета
 - new, invalid, established, related
- Флаги NAT-а
 - srcnat и dstnat

From IP Header

- src и dst адреса
- TTL
- Protocol
- Packet size

From Protocol Header

- src и dst порты для tcp или udp протокола
- tcp-mss (для tcp)
- tcp-flags (для tcp)
- icmp-options (для icmp)

Use connection-tracker

- connection-bytes
- connection-rate
- connection-limit
- per-connection-classifier

From payload

- content
- tls-host
- layer7-protocol

Стенд

- Forward – 1 000 000pps
- CPU – avg 15%

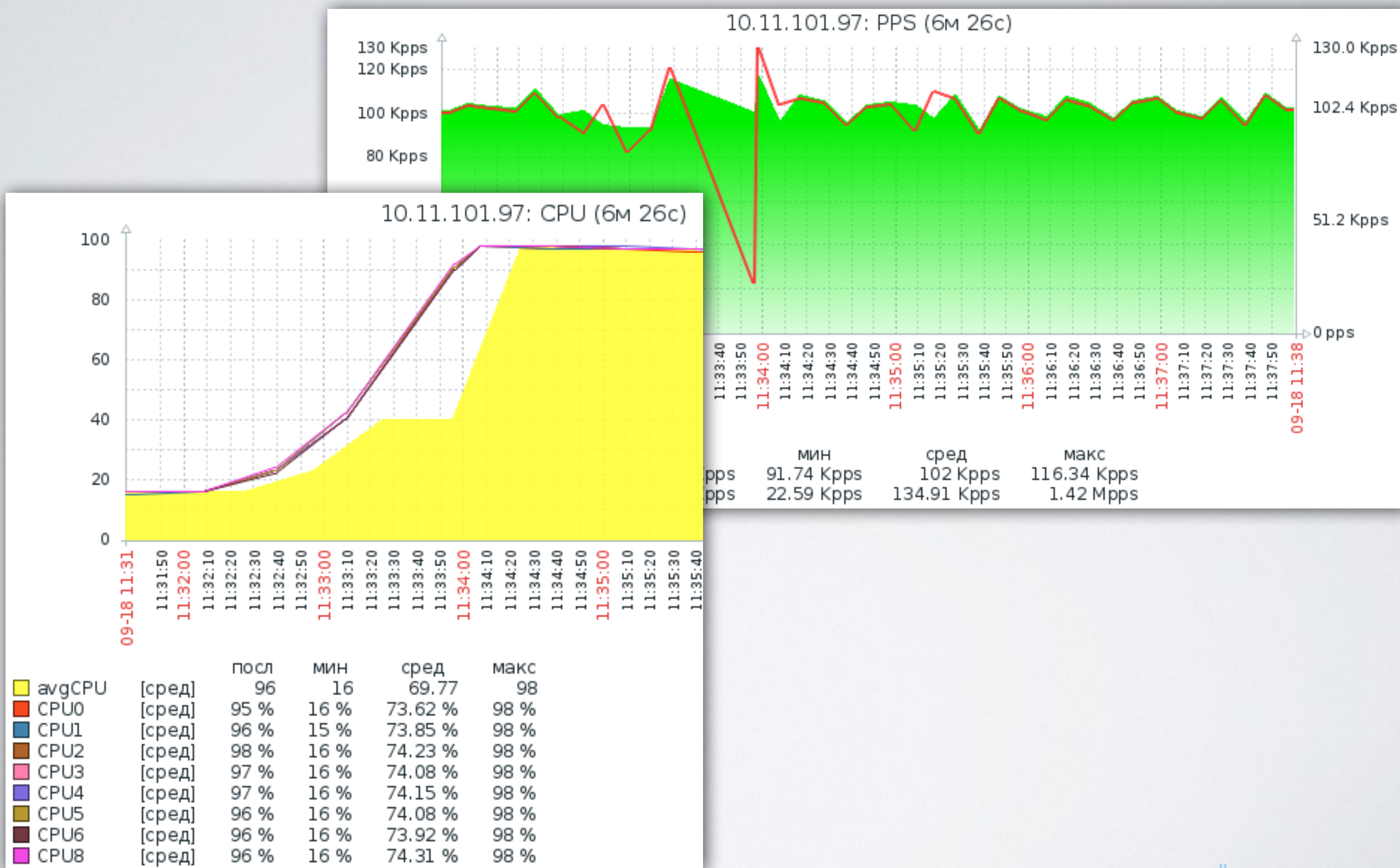
Сте́нд

::: A1								
R	ether1	Ethernet	9000	10222	61.0 kbps	823.6 Mbps	57	102 979
R	↔vlan2	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 360
R	↔vlan3	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 358
R	↔vlan4	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 360
R	↔vlan5	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 359
R	↔vlan6	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 360
R	↔vlan7	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 360
R	↔vlan8	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 359
R	↔vlan9	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 359
R	↔vlan10	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 359
R	↔vlan11	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 359
R	↔vlan12	VLAN	1500	10218	3.5 kbps	74.5 Mbps	3	9 360
	ether2	Ethernet	1500	1580	0 bps	0 bps	0	0
	ether3	Ethernet	1500	1580	0 bps	0 bps	0	0
	ether4	Ethernet	1500	1580	0 bps	0 bps	0	0

Connection-Tracking

- Chain = **forward**
- **Accept** = Established, Related, **Untrack**
- **Block** = Invalid
- CPU **96%**

Connection-Tracking



Drop all Forward

- Настраиваем «закрытый» firewall
- Chain=forward action=**drop**
- CPU 35%

Разрешить трафик

- Interface – vlan2-6 (~45kpps)
- Network – 192.168.2-6.0/24
- Allow to all

Разрешить трафик

- In-interface-list = +21% CPU (56%)

Разрешить трафик

- In-interface-list = +21% CPU (56%)
- src-address-list = +24% CPU (59%)

Разрешить трафик

- In-interface-list = +21% CPU (56%)
- src-address-list = +24% CPU (59%)
- Raw / untrack = +0% CPU (35%)

NAT-им

- Interface – vlan7 (9kpps)
- Network – 192.168.7.0/24
- dstnat – to 192.168.255.7

NAT-им

- NAT Rule (dstnat)
- Firewall in-interface
 - dst-nat flag = +24% CPU (59%)
 - dst-address 192.168.255.7 and port = +11% CPU (46%)

NAT

srcnat

/ip firewall nat

**add chain=srcnat out-interface=ether1 **
action=src-nat to-address=5.19.245.3

/interface gre

**add local-address=5.19.245.3 **
remote-address=3.3.3.3

srcnat

```
/ip firewall raw
```

```
add chain=output out-interface=ether1 \  
    action=notrack
```

```
/ip route
```

```
set pref-src=5.19.245.3 \  
    [ find dst-address=0.0.0.0/0 ]
```

4%

#НАБОЛЕЛО

DSTNAT

*«Для наших целей подходит dst-nat и netmap.
Последнее является более новым и улучшенным вариантом первого,
логично использовать его.»*

DSTNAT

/ip firewall nat

**add chain=dstnat dst-address=5.19.245.3 protocol=tcp **
**dst-port=25 in-interface=ether1 action=netmap **
to-addresses=192.168.100.2 to-ports=25

DSTNAT

/ip firewall nat

**add chain=dstnat dst-address=5.19.245.3 protocol=tcp **
**dst-port=25 in-interface=ether1 action=netmap **
to-addresses=192.168.100.2 to-ports=25

1. Не указывайте порт, если он не меняется
2. Не указывайте адрес, если он один на интерфейсе
3. **netmap** не для «пробросов» портов. Используйте **dstnat**

DSTNAT

/ip firewall nat

**add chain=dstnat dst-address=5.19.245.3 protocol=tcp **
**dst-port=25 in-interface=ether1 action=netmap **
to-addresses=192.168.100.2 to-ports=25

/ip firewall nat

**add chain=dstnat protocol=tcp dst-port=25 **
**in-interface=ether1 action=dst-nat **
to-addresses=192.168.100.2

x10

3%

DSTNAT

- **netmap**

- алгоритм расчёта адреса
- изменение адреса в заголовке пакета

- **dst-nat**

- изменение адреса в заголовке пакета

DSTNAT

- **RBI 100AHx2**
- **netmap** = 910Mbps (CPU 100%)
- **dst-nat** = 980Mbps

7%

IPSEC и Firewall

IPSEC и Firewall

/ip ipsec policy

```
add dst-address=192.168.1.0/24 src-address=192.168.100.0/24 \  
sa-dst-address=4.4.4.4 sa-src-address=5.19.245.3 \  
level=unique tunnel=yes
```


IPSEC и Firewall

/ip ipsec policy

```
add dst-address=192.168.1.0/24 src-address=192.168.100.0/24 \  
sa-dst-address=4.4.4.4 sa-src-address=5.19.245.3 \  
level=unique tunnel=yes
```

/ip firewall nat

```
add chain=dstnat protocol=tcp dst-port=25 \  
in-interface=ether1 action=dst-nat \  
to-addresses=192.168.100.2
```

IPSEC и Firewall

- Логический интерфейс отсутствует
- После снятия ESP заголовка интерфейс остаётся прежним (ether1)
- В заголовке пакета
 - src 192.168.1.0/24
 - dst 192.168.100.0/24
- При обращении на 25 порт трафик попадёт под правило NAT

IPSEC и Firewall

/ip firewall raw

**add chain=prerouting in-interface=ether1 **
ipsec-policy=in,ipsec action=notrack

IPSEC и Firewall

- Пакет предназначенный для IPsec трансформации
- Попадёт под правило srcnat и уже не попадёт под IPsec policy так как заголовок будет изменён
- Было 192.168.100.100 -> 192.168.1.55
- Стало 5.19.245.3 -> 192.168.1.55

IPSEC и Firewall

/ip firewall raw

**add chain=prerouting in-interface=Bridge-Local **
ipsec-policy=in,ipsec action=notrack

PPP

PPP

```
/interface l2tp-client
```

```
add connect-to=6.6.6.6 name=l2tp-outl \  
  password=userl user=passl
```

```
/ip firewall mangle
```

```
add chain=forward out-interface=l2tp-outl \  
  protocol=tcp tcp-flags=syn tcp-mss=1421-65535 \  
  action=change-mss new-mss=1420
```

```
add chain=forward in-interface=l2tp-outl \  
  protocol=tcp tcp-flags=syn tcp-mss=1421-65535 \  
  action=change-mss new-mss=1420
```

PPP

- Туннель с минимальным jitter
- Стабильное соединение
- Через PPP (должно*) проходит много больших пакетов (> 1000)
 - Видео
 - Синхронизация данных
- Jumbo frame (> 1500)

PPP MLPPP

- Фрагментация IP пакета на PPP пакеты
- Контроль последовательности PPP пакетов
- Сборка на другом конце в исходный IP пакет
- +4 байта к заголовку
- Поддержка MLPPP с двух сторон

PPP MLPPP

- Вычислите правильно MTU у PPP интерфейса
- Укажите MTU на PPP интерфейсе
- Укажите MRRLU равным максимальному размеру пакета в вашей сети +4 байта

PPP MLPPP

Interface <l2tp-out1>

General | Dial Out | Status | Traffic

Name: l2tp-out1

Type: L2TP Client

Actual MTU: 9000

Max MTU: 1460

Max MRU: 1460

MRRU: 9004

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

L2TP Server

☒ Enabled

Max MTU: 1460

Max MRU: 1460

MRRU: 9004

Keepalive Time: 30

Default: default

M Sessions:

Authentication: ☒ mschap2 ☐ mschap1
☐ chap ☐ pap

Use IPsec: no

IPsec Secret:

Caller ID Type: ip address

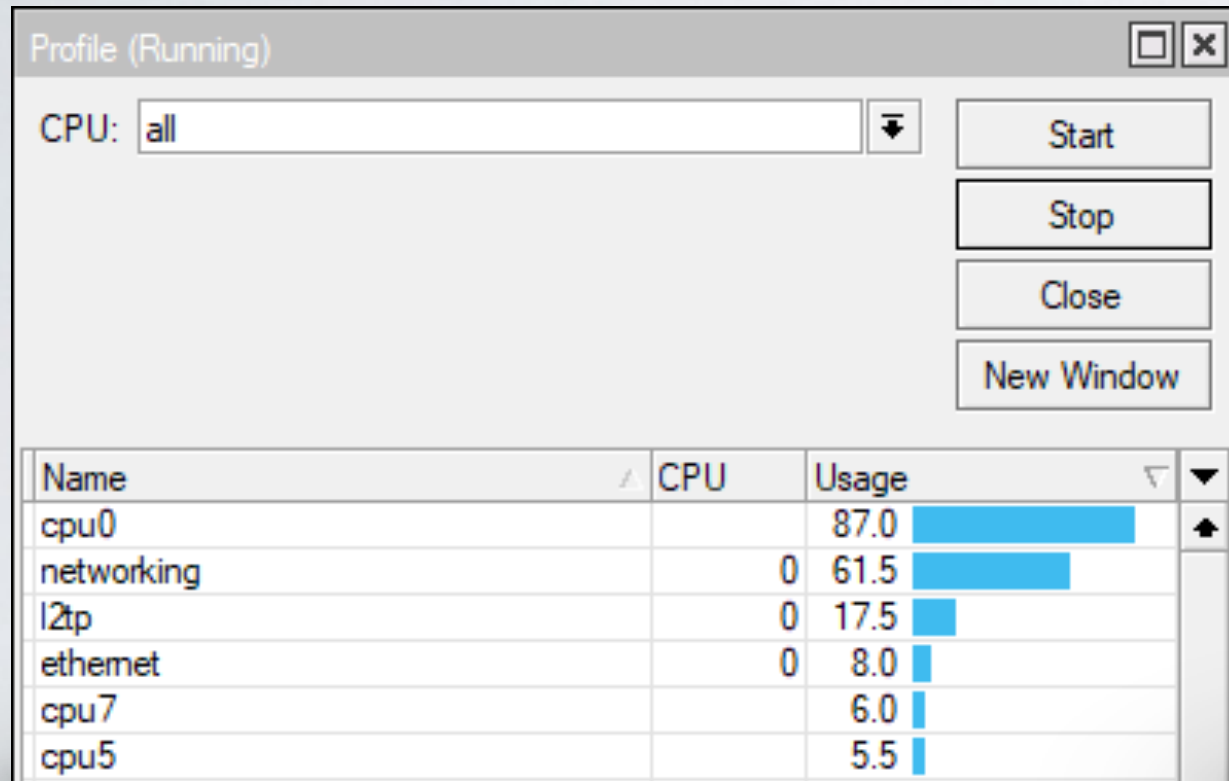
☐ One Session Per Host
☐ Allow Fast Path

OK
Cancel
Apply

MLPPP

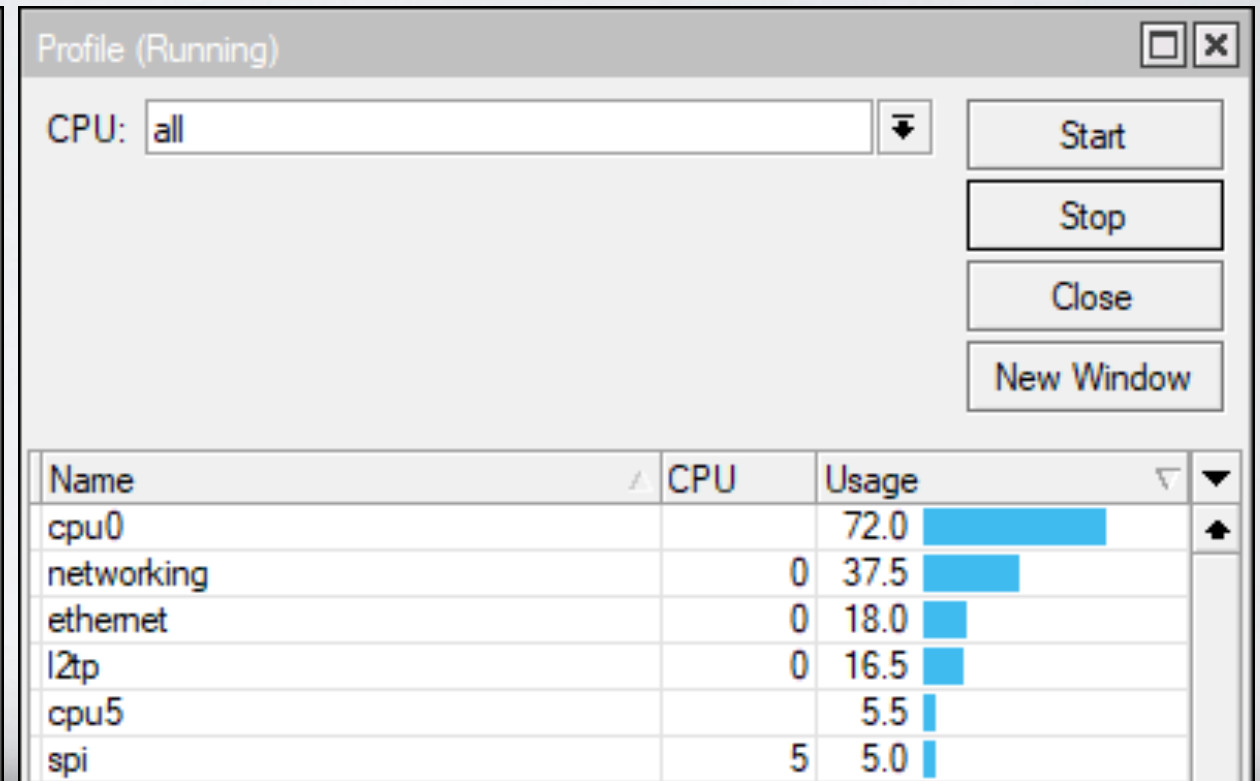
PPP MLPPP

Jumbo Frame 9k



IP
Fragmentation

~15%



PPP
Fragmentation

Multicast

Multicast

- Большой pps (igmp)
- Большие пакеты (igmp)
- igmp, ospf
- Не используйте connection-tracker

Multicast

```
/ip firewall raw
```

```
add chain=prerouting in-interface=ether1 \  
    dst-address-type=multicast action=notrack
```

Custom chain

1. Forward
2. Forward
3. Forward
4. Forward
5. Forward
6. Forward
7. Forward
8. ...
2673. Forward

Custom chain

- Свои цепочки для контроля трафика
- Jump - перейти в цепочку
- Return - выйти из цепочки

Custom chain

- Порядок:

1. Самые объёмные правила по pps

2. interface

3. Ip Header

4. Protocol Header

5. Payload

Custom chain

- Найдите общие признаки для правил (направление трафика)
- Interfaces (external filter)
- Addresses, protocol (ip header)

Custom chain

/ip firewall filter

**add chain=forward in-interface-list=wifi **
action=jump target=chain-wifi

**add chain=chain-wifi protocol=tcp dstport=80,443 **
action=accept

**add chain=chain-wifi protocol=udp dstport=53 **
action=accept

add chain=chain-wifi action=drop

Закрывать доступ к сайтам

Необходимо закрыть доступ к социальным сетям

Заккрыть доступ к сайтам

- Создать address-list с доменными именами закрытых сайтов
- Создать правило в filter
 - Адрес dst находится в address-list
 - Drop всех пакетов

Закрывать доступ к сайтам

```
/ip firewall address-list
```

```
add list=Site-VK address=vk.com
```

```
add list=Site-VK address=www.vk.com
```

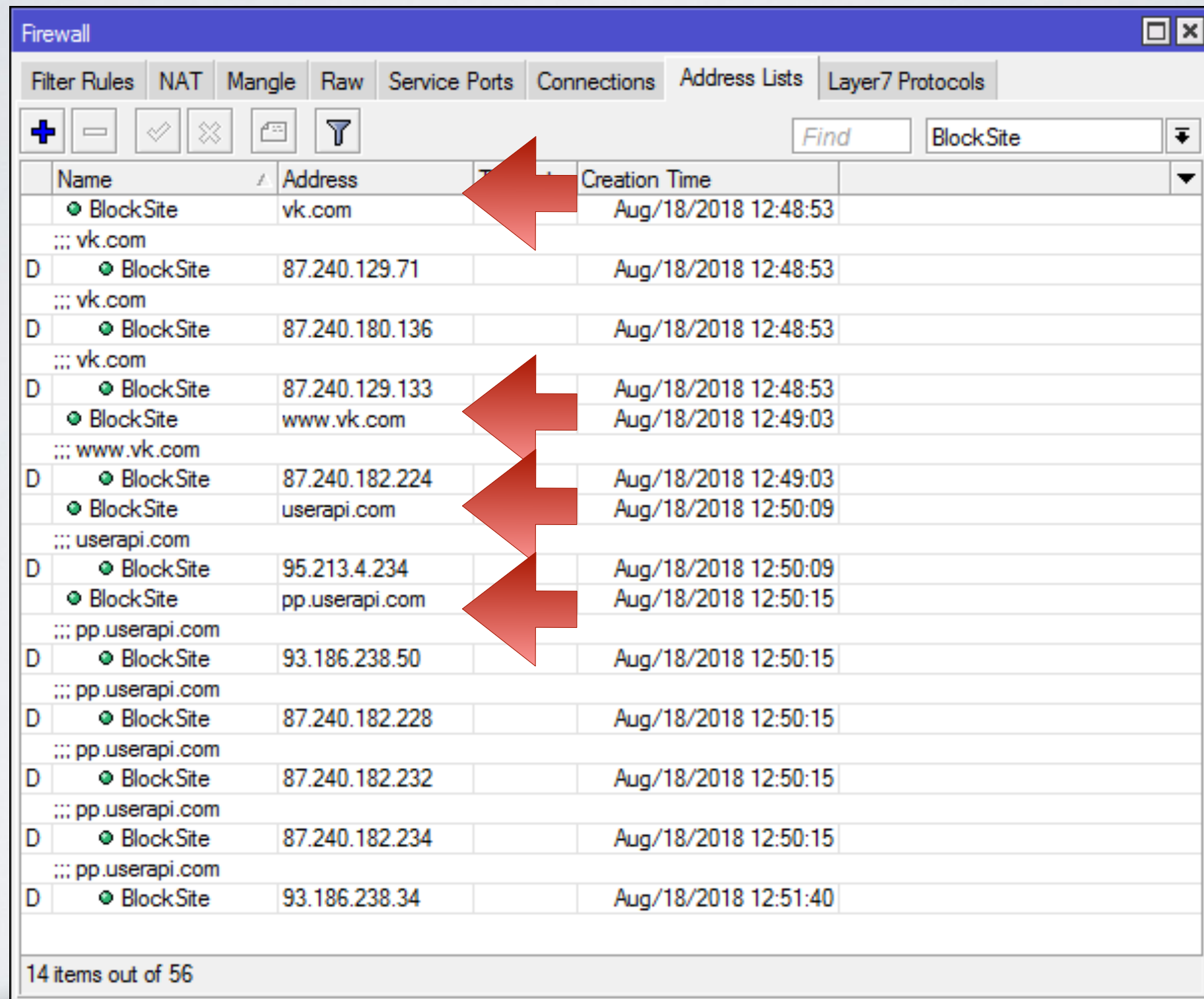
```
add list=Site-VK address=userapi.com
```

```
add list=Site-VK address=pp.userapi.com
```

```
/ip firewall filter
```

```
add chain=forward out-interface=ether1 \  
    dst-address-list=Site-VK action=drop
```

Закрывать доступ к сайтам



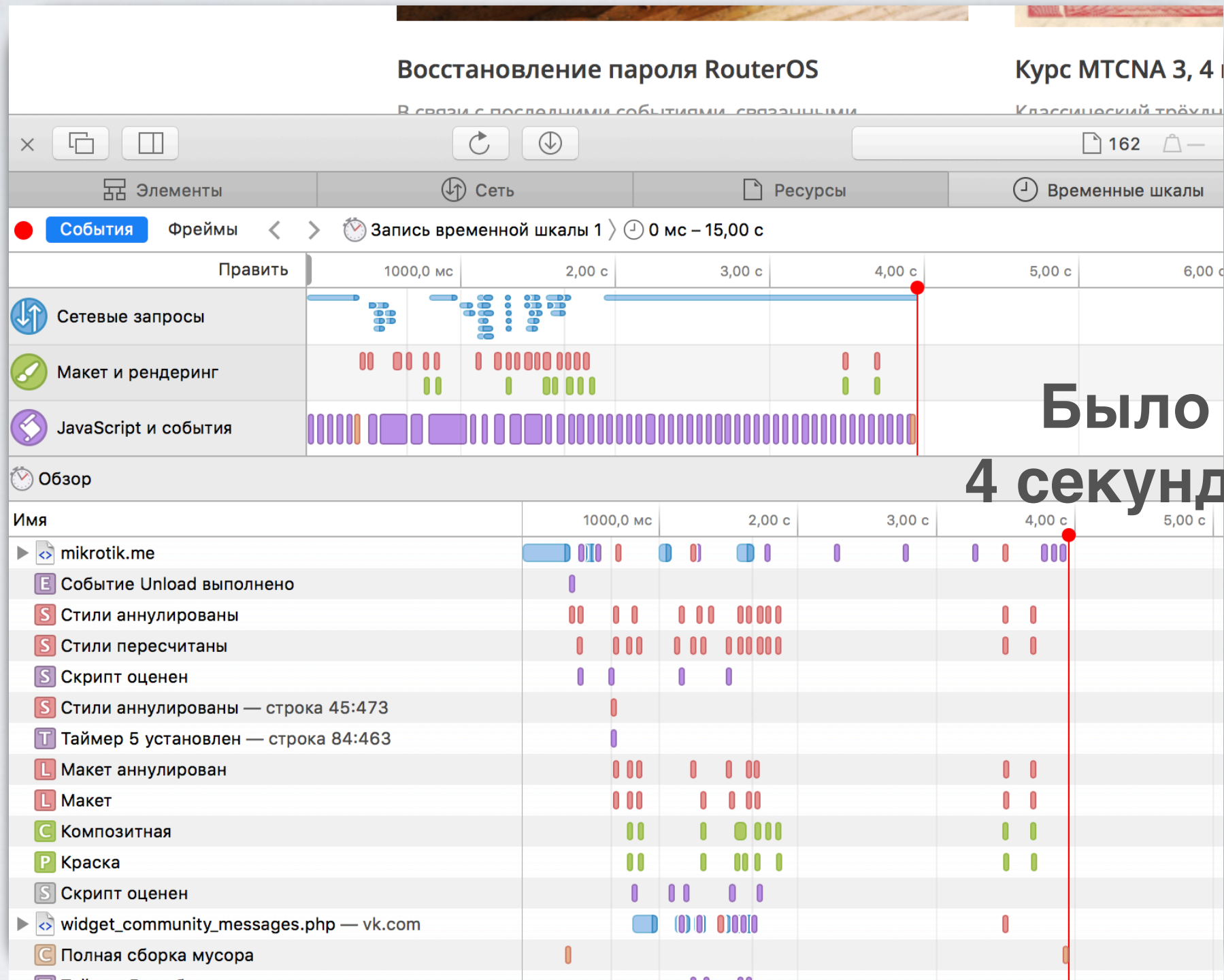
	Name	Address	Creation Time
	BlockSite	vk.com	Aug/18/2018 12:48:53
	vk.com		
D	BlockSite	87.240.129.71	Aug/18/2018 12:48:53
	vk.com		
D	BlockSite	87.240.180.136	Aug/18/2018 12:48:53
	vk.com		
D	BlockSite	87.240.129.133	Aug/18/2018 12:48:53
	BlockSite	www.vk.com	Aug/18/2018 12:49:03
	www.vk.com		
D	BlockSite	87.240.182.224	Aug/18/2018 12:49:03
	BlockSite	userapi.com	Aug/18/2018 12:50:09
	userapi.com		
D	BlockSite	95.213.4.234	Aug/18/2018 12:50:09
	BlockSite	pp.userapi.com	Aug/18/2018 12:50:15
	pp.userapi.com		
D	BlockSite	93.186.238.50	Aug/18/2018 12:50:15
	pp.userapi.com		
D	BlockSite	87.240.182.228	Aug/18/2018 12:50:15
	pp.userapi.com		
D	BlockSite	87.240.182.232	Aug/18/2018 12:50:15
	pp.userapi.com		
D	BlockSite	87.240.182.234	Aug/18/2018 12:50:15
	pp.userapi.com		
D	BlockSite	93.186.238.34	Aug/18/2018 12:51:40

14 items out of 56

Закрывать доступ к сайтам Проблема

Стал медленно работать Интернет

Закрывать доступ к сайтам



Закрывать доступ к сайтам

Восстановление пароля RouterOS

Курс MTCNA 3, 4 и 5 октября 20

https://mikrotik.me/blog/50

Elements Console Sources Network Performance Memory Application Security Audits

View: [Icons] Group by frame [] Preserve log [x] Disable cache [] Offline Online [v]

Filter [] Hide data URLs [All] XHR JS CSS Img Media Font Doc WS Manifest Other

20000 ms 40000 ms 60000 ms 80000 ms 100000 ms 120000 ms 140000 ms

Name	Status	Type	Ini
jquery.min.js?10	200	script	(in
main.css?10	200	stylesheet	(in
mem5YaGs126MiZpBA-UNirkOUuHp.woff2	200	font	jq
mem5YaGs126MiZpBA-UNirkOVuHpOqc.woff2	200	font	jq
mem8YaGs126MiZpBA-UFUZ0bbck.woff2	200	font	jq
mem8YaGs126MiZpBA-UFVZ0b.woff2	200	font	jq
mikrotik.me	200	document	Ot
openapi.js?146	(failed)	script	(in
openapi.js?146	(failed)	script	(in
pricetable.css?10	200	stylesheet	(in
recaptcha__ru.js	200	script	ap
rtrg?p=VK-RTRG-36315-aIEJ5	(failed)		(in
share.js?95	(failed)	script	(in
style.css?10	200	stylesheet	(in
team.css?10	200	stylesheet	(in
watch.js	200	script	(in

5 requests | 1.4 MB transferred | Finish: 2.8 min | DOMContentLoaded: 2.3 min | Load: 2.3 min

Стало
3 минуты

Проблема

- Многие сайты используют библиотеки\API социальных сетей
- Лайки, чаты, виджеты и т.п.д.
- Каждый внешний ресурс (css, js...) в html коде устанавливает соединение.

Проблема

- Каждое соединение ТСР ожидает пакет с флагами syn,ack
- Пауза между попытками установить новое соединение
- Несколько попыток установить новое соединение
- Экспоненциальный рост времени загрузки, в зависимости от количества внешних ресурсов

Решение

Сообщить клиенту, что соединение невозможно

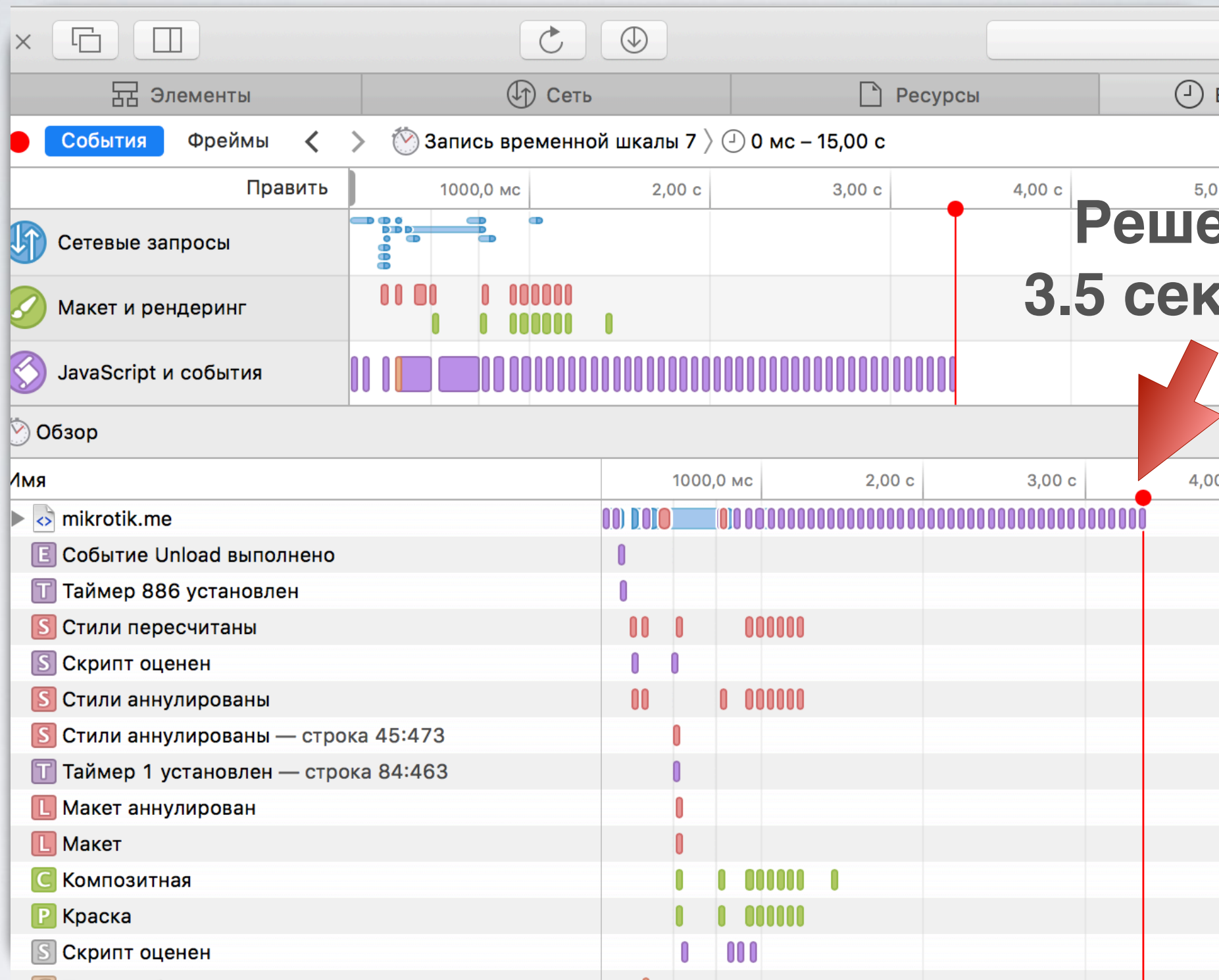
Решение

/ip firewall filter

```
add chain=forward out-interface=ether1 \  
dst-address-list=Site-VK protocol=tcp \  
action=reject reject-with=tcp-reset
```

```
add chain=forward out-interface=ether1 \  
dst-address-list=Site-VK action=drop
```

Решение

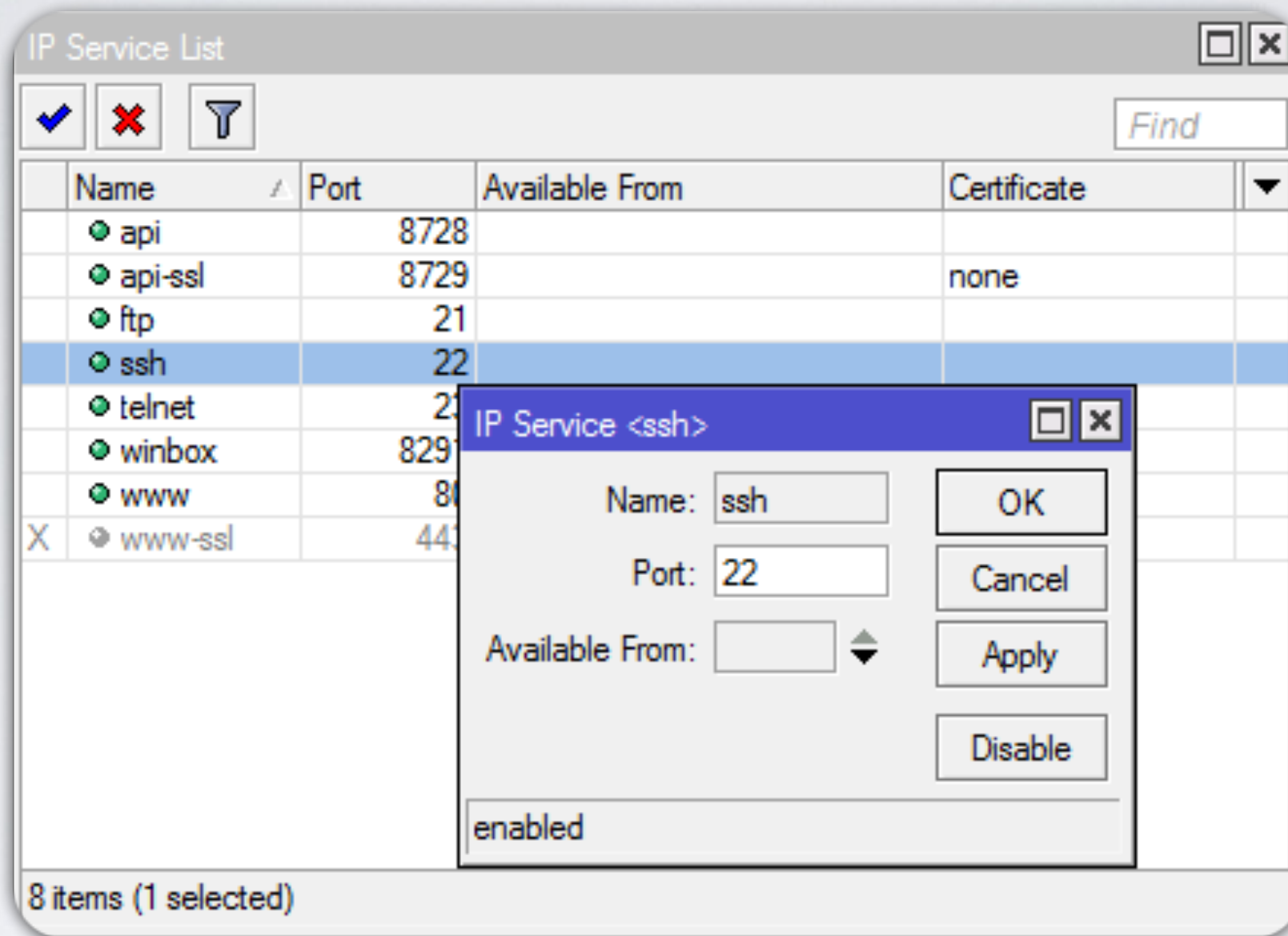


Решение
3.5 секунды

Другой порт SSH

Изменить порт SSH со стороны ISP

Другой порт SSH



Изменить порт только со стороны провайдера

Проблема

- Нет возможности указать несколько портов
- Нет возможности создать несколько instance
- Нет возможности привязать к интерфейсу

Решение

Использовать NAT

Другой порт SSH

```
/ip firewall nat
```

```
add chain=dst-nat in-interface=ether1 \  
    protocol=tcp dst-port=5555 \  
    action=redirect to-port=22
```

Другой порт SSH

```
/ip firewall nat
```

```
add chain=dst-nat in-interface=ether1 \  
    protocol=tcp dst-port=5555 \  
    action=redirect to-port=22
```

```
/ip firewall filter
```

```
add chain=input in-interface=ether1 \  
    protocol=tcp dst-port=22 action=accept \  
    
```

Другой порт SSH

```
/ip firewall nat
```

```
add chain=dst-nat in-interface=ether1 \  
    protocol=tcp dst-port=5555 \  
    action=redirect to-port=22
```

```
/ip firewall filter
```

```
add chain=input in-interface=ether1 \  
    protocol=tcp dst-port=22 action=accept \  
    connection-nat-state=dstnat
```


Вопросы?

- MikroTik.Me
- VasilevKirill.com
- <https://t.me/mikrotikme>
- <https://vk.com/mikrotikrus>