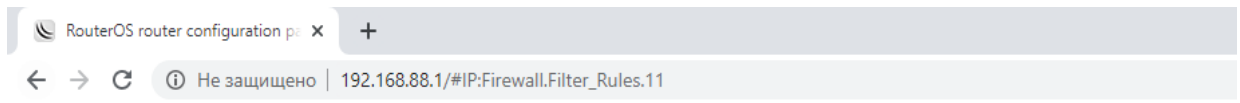
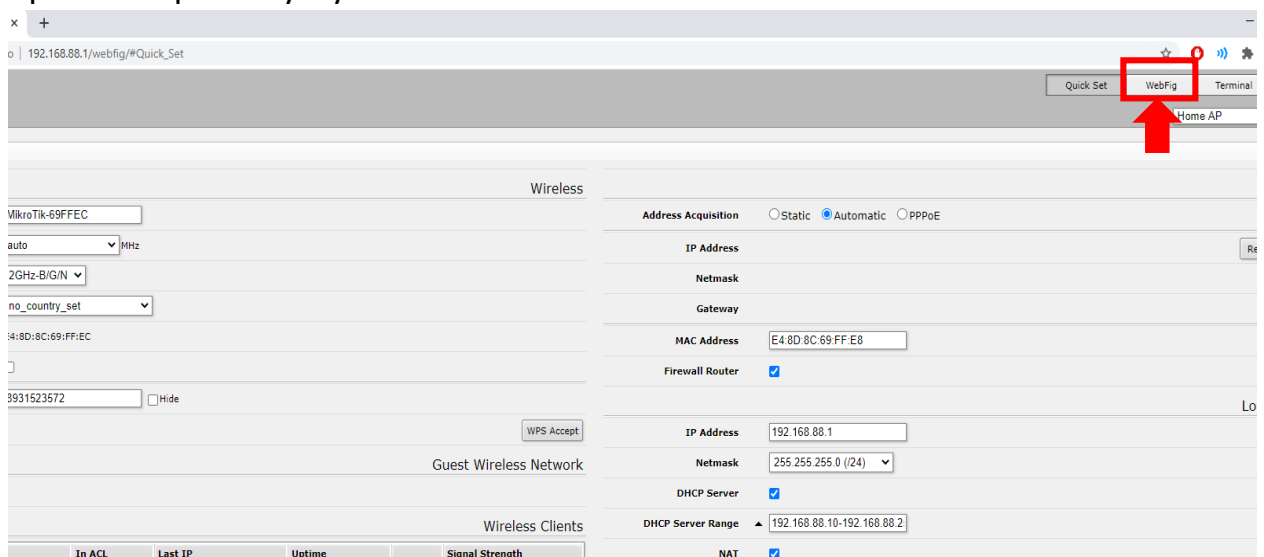


# Настройка PPPoE

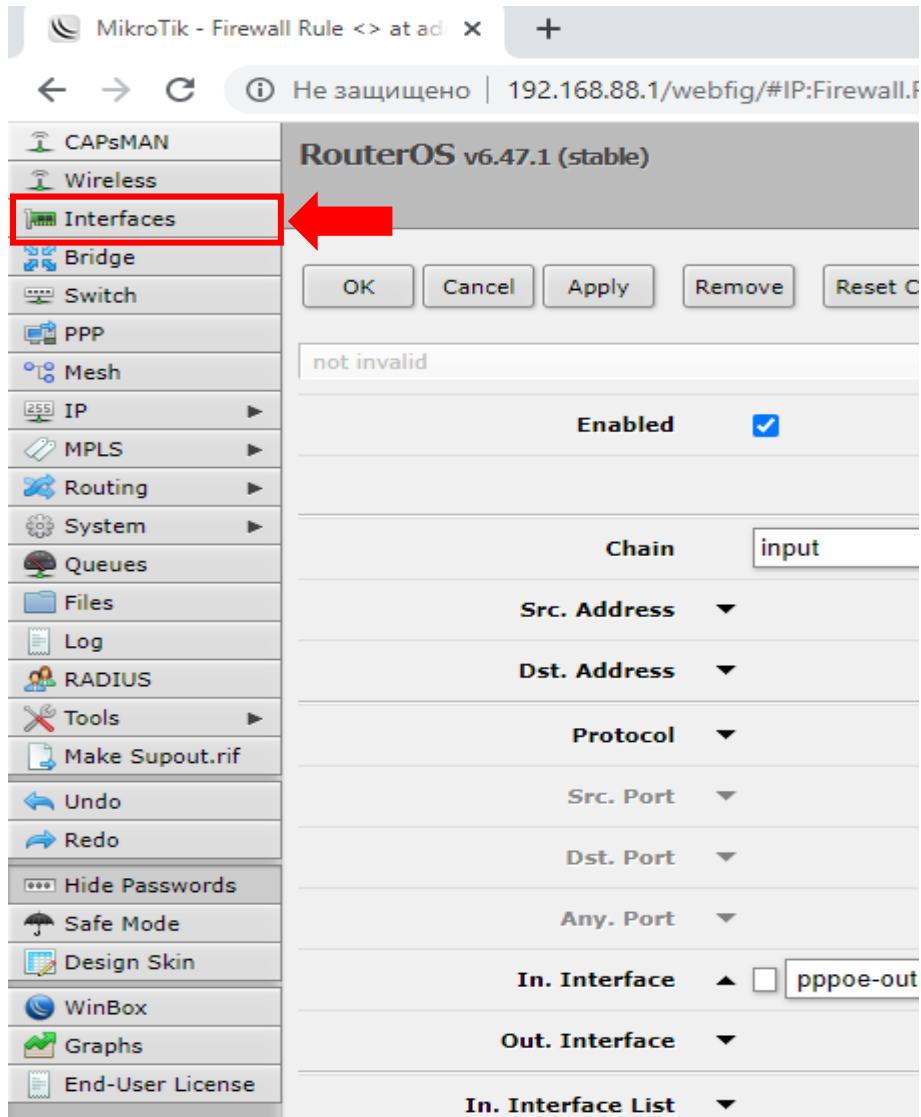
1 Заходим в Web-интерфейс роутера по 192.168.88.1. Стандартные данные для входа: Login – admin, Password – ‘пусто’



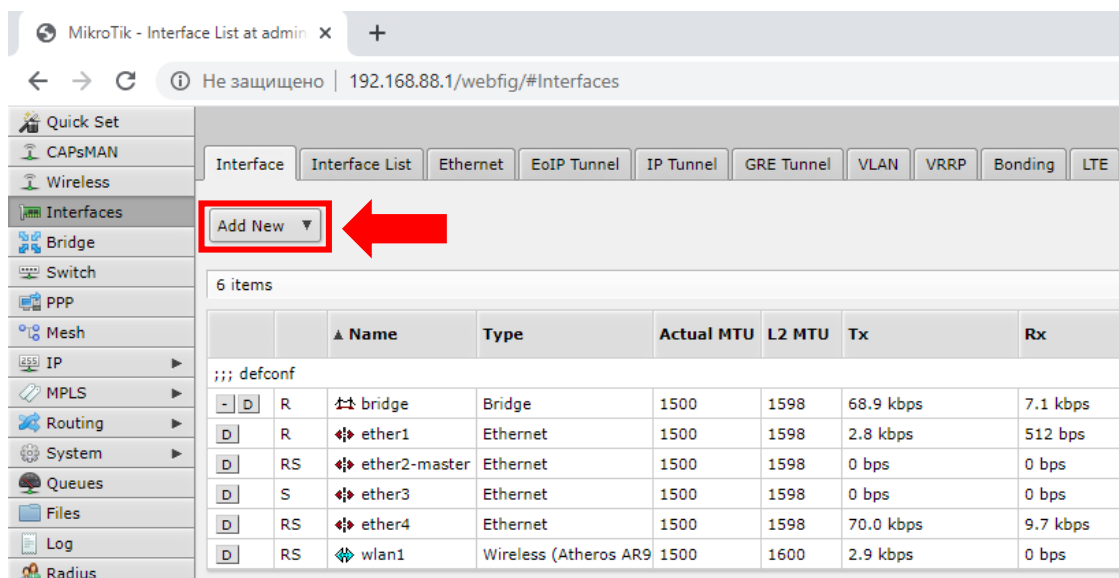
2 По умолчанию открывается страница QuickSet. Переходим на WebFig в правом верхнем углу



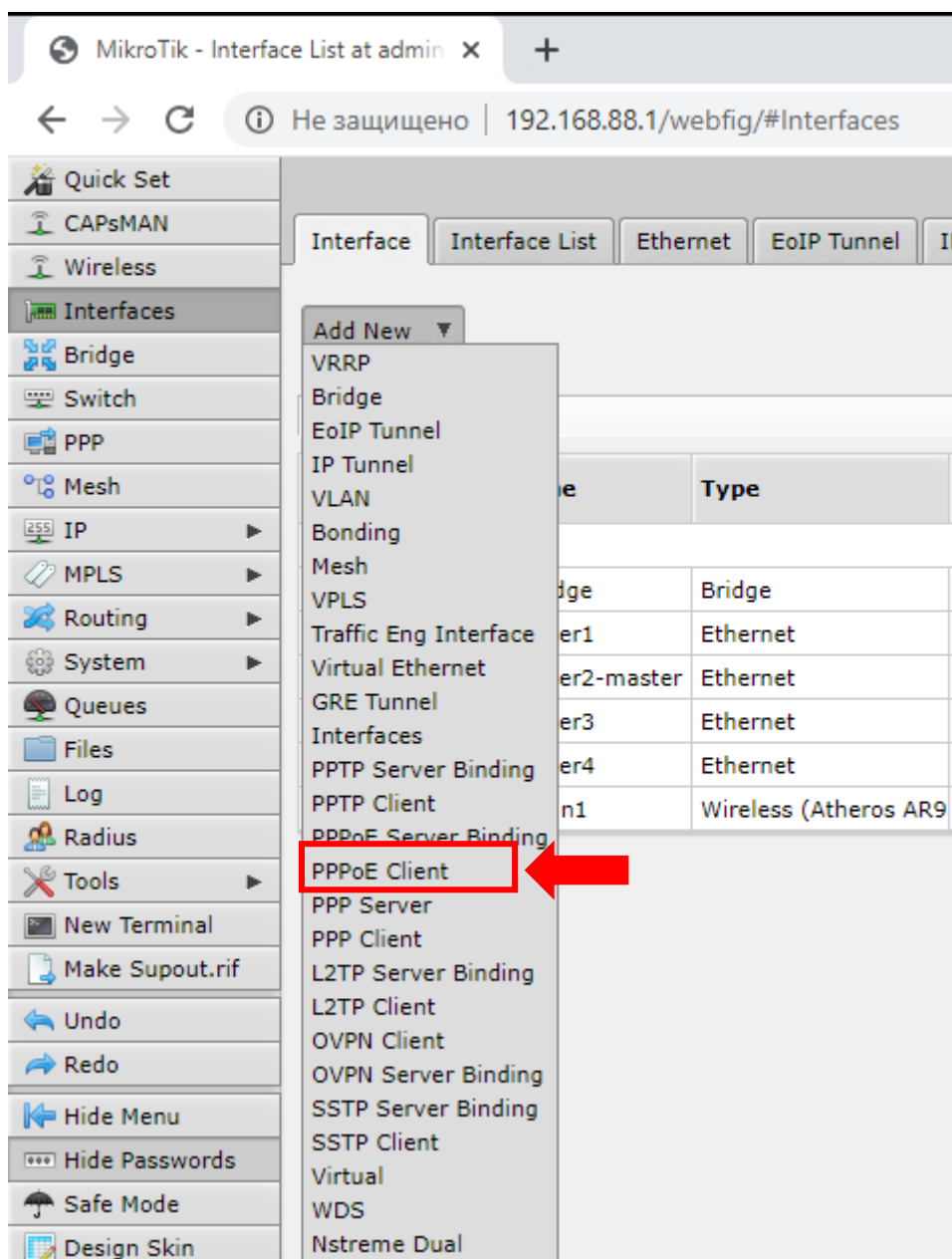
3 Слева появляется меню с разделами. Выбираем раздел Interfaces



4 Появляется список всех доступных интерфейсов. Нажимаем Add New, чтобы создать PPPoE соединение



5 Открывается список соединений, которые можно создать. Выбираем PPPoE client



6 Настраиваем непосредственно PPPoE соединение:

- **Обязательно** меняем MTU и MRU на 1440, иначе можно получить неоткрывающиеся страницы.
- В Interfaces выбираем Ether1, который по умолчанию является портом WAN
- Вводим логин и пароль PPPoE в User и Password соответственно
- Ставим галочки Use Peer DNS и Add Default Route, снимаем галочку Dial On Demand, если она стоит
- Ставим все галочки в разделе Allow

## - Жмём ОК для сохранения

The screenshot shows the MikroTik WinBox interface for configuring a new PPPoE Client. The left sidebar contains various system menus. The main area displays the configuration form for the interface 'pppoe-out1'. At the top of the form, there are buttons for 'OK', 'Apply', 'PPPoE Scan', and 'Torch'. The 'OK' button is highlighted with a red box, and a red arrow points to it from the left. Below the buttons, the configuration details are as follows:

- Enabled:
- Name: pppoe-out1
- Type: PPPoE Client
- Actual MTU: Max MTU (1440), Max MRU (1440), MRRU
- Interfaces: ether1
- Service: (dropdown)
- AC Name: (dropdown)
- User: v44100027
- Password: (masked)
- Profile: default
- Keepalive Timeout: (dropdown)
- Dial On Demand:
- Use Peer DNS:
- Add Default Route:
- Default Route Distance: 0
- Allow:  mschap2,  mschap1,  chap,  pap

## 7 В списке интерфейсов должно появиться PPPoE соединение

The screenshot shows the MikroTik WinBox interface for the 'Interface List'. The 'Interface List' tab is selected. Below the 'Add New' button, there is a table with 7 items. The table has the following columns: Name, Type, Actual MTU, L2 MTU, Tx, Rx, Tx Packet (p/s), and Rx Packet (p/s). The row for 'pppoe-out1' is highlighted with a red box.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	
;;;	defconf								
[D]	R	bridge	Bridge	1500	1598	68.6 kbps	7.9 kbps	6	9
[D]	R	ether1	Ethernet	1500	1598	4.7 kbps	512 bps	8	1
[D]	RS	ether2-master	Ethernet	1500	1598	0 bps	0 bps	0	0
[D]	S	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0
[D]	RS	ether4	Ethernet	1500	1598	69.8 kbps	10.3 kbps	8	13
[D]	R	pppoe-out1	PPPoE Client	1440		1920 bps	0 bps	5	0
[D]	RS	wlan1	Wireless (Atheros AR9	1500	1600	424 bps	0 bps	1	0

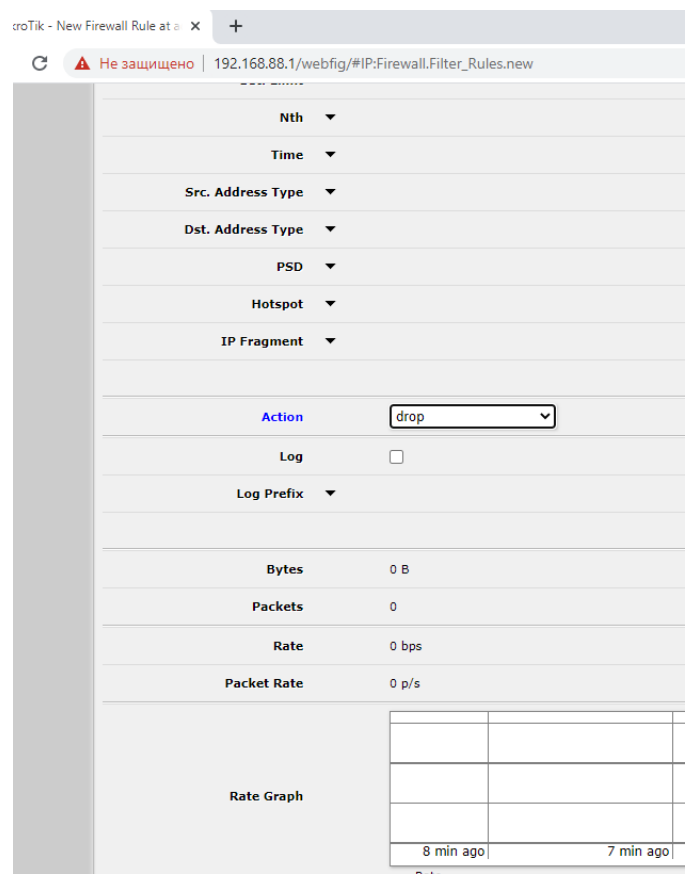
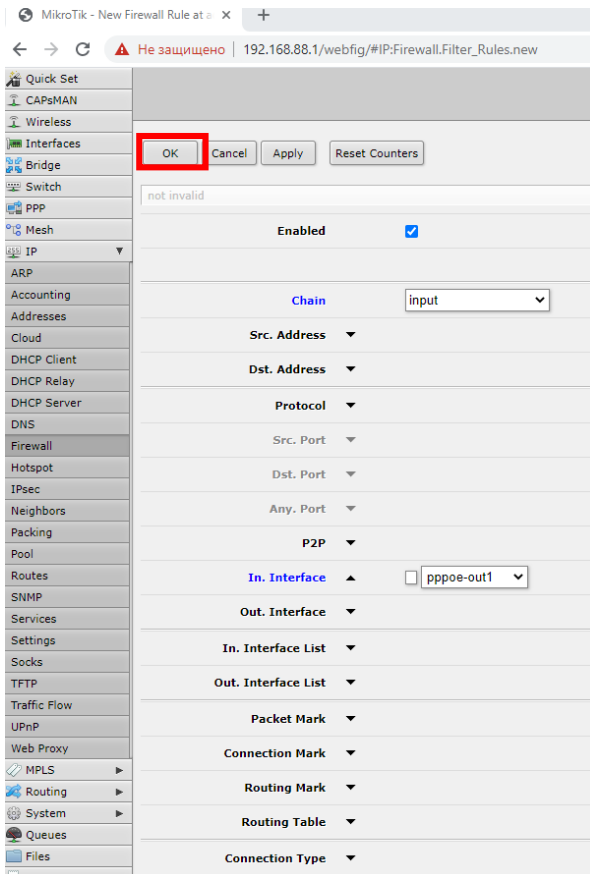
8 Сессия уже должна стоять, но страницы открываться не будут, т.к. необходимо настроить сетевой экран роутера, чтобы он разрешал пропускать трафик, через созданное соединение.

Для этого переходим в раздел **IP > Firewall > Filter Rules** и создаём правило для входящего соединения. Нажимаем Add New

	#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	Bytes	Packets
;;; special dummy rule to show fasttrack counters													
- [D]	0	passthro	forward									857.7 MiB	980 297
;;; defconf: accept ICMP													
- [D]	1	accept	input			1 (icmp)						81.7 KiB	698
;;; defconf: accept established,related													
- [D]	2	accept	input									2162.5 KiB	13 189
;;; defconf: drop all from WAN													
- [D]	3	drop	input							ether1		0 B	0
;;; defconf: fasttrack													
- [D]	4	fasttrack	forward									3301.4 KiB	16 568
;;; defconf: accept established,related													
- [D]	5	accept	forward									3301.4 KiB	16 568
;;; defconf: drop invalid													
- [D]	6	drop	forward									14.9 KiB	382
;;; defconf: drop all from WAN not DSTNATed													
- [D]	7	drop	forward							ether1		0 B	0

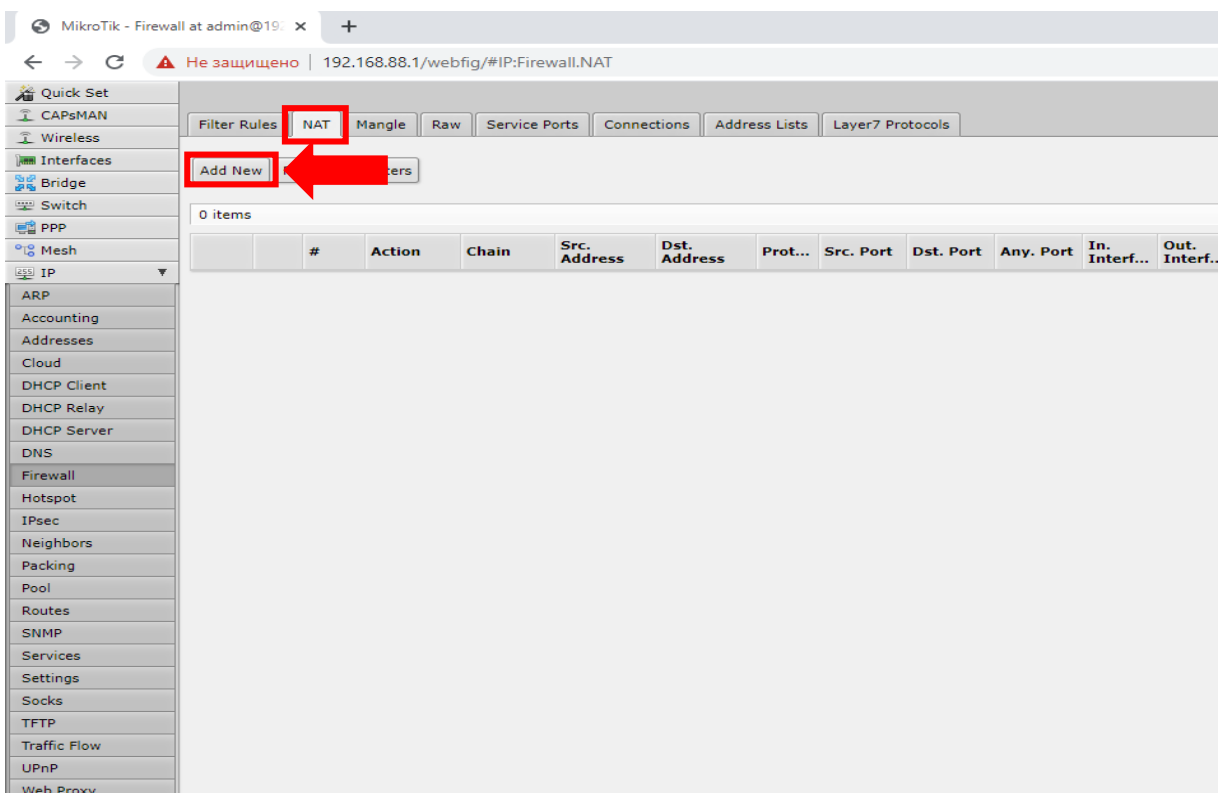
9 Открывается окно создания правила для брандмауэра.

- Ставим галочку **Enabled**
- В **Chain** указываем input
- В **In. Interface** указываем имя нашего созданного PPPoE соединения. В нашем случае **pppoe-out1**.
- Ниже в **Action** выбираем **drop**
- Нажимаем **Ok** для сохранения правила



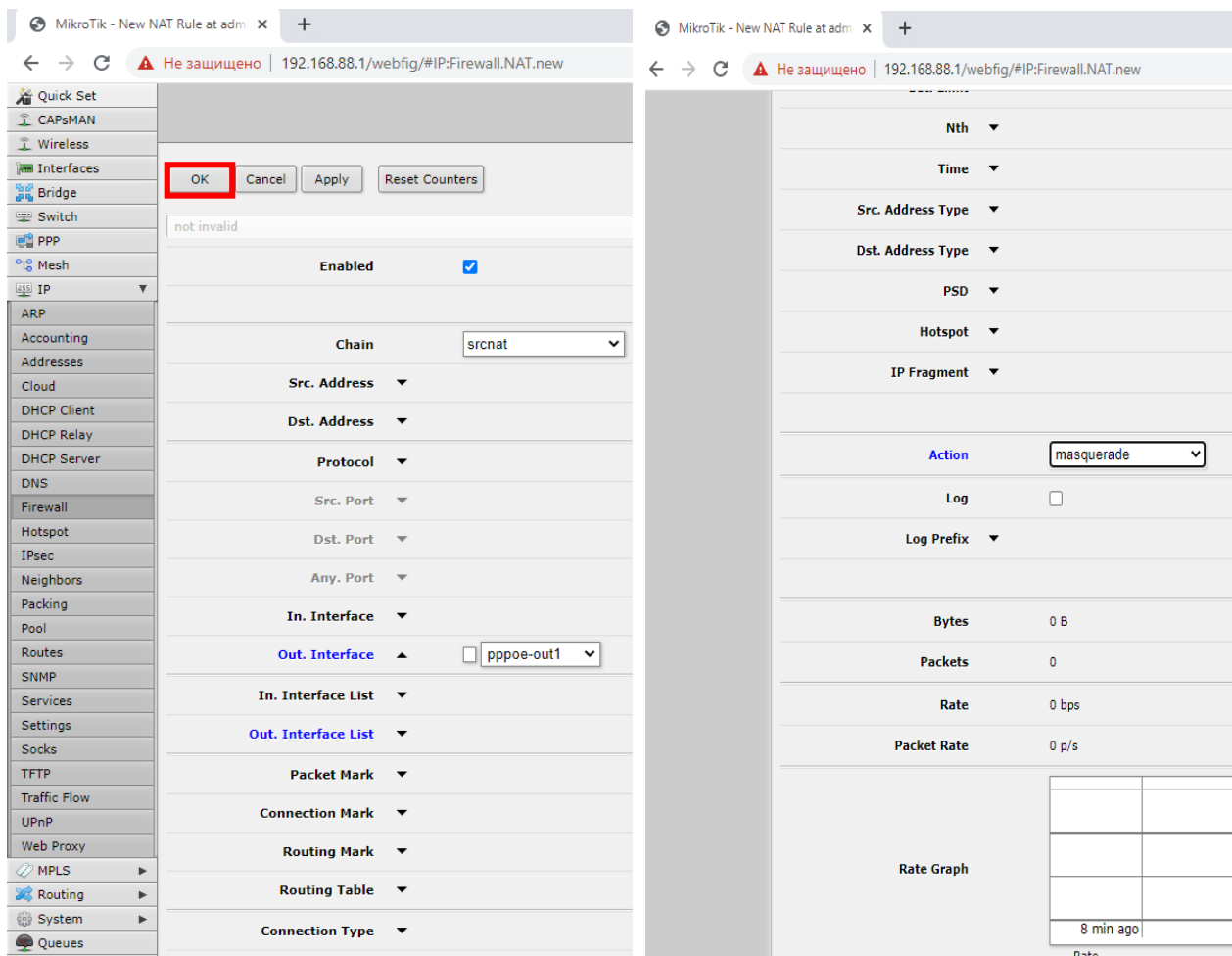
10 Теперь нужно настроить NAT, чтобы устройства локальной сети могли получить доступ к соединению

Для этого в том же разделе **Firewall** переходим на вкладку **NAT** и нажимаем **Add New**



11 Открывается окно для создания правила работы NAT.

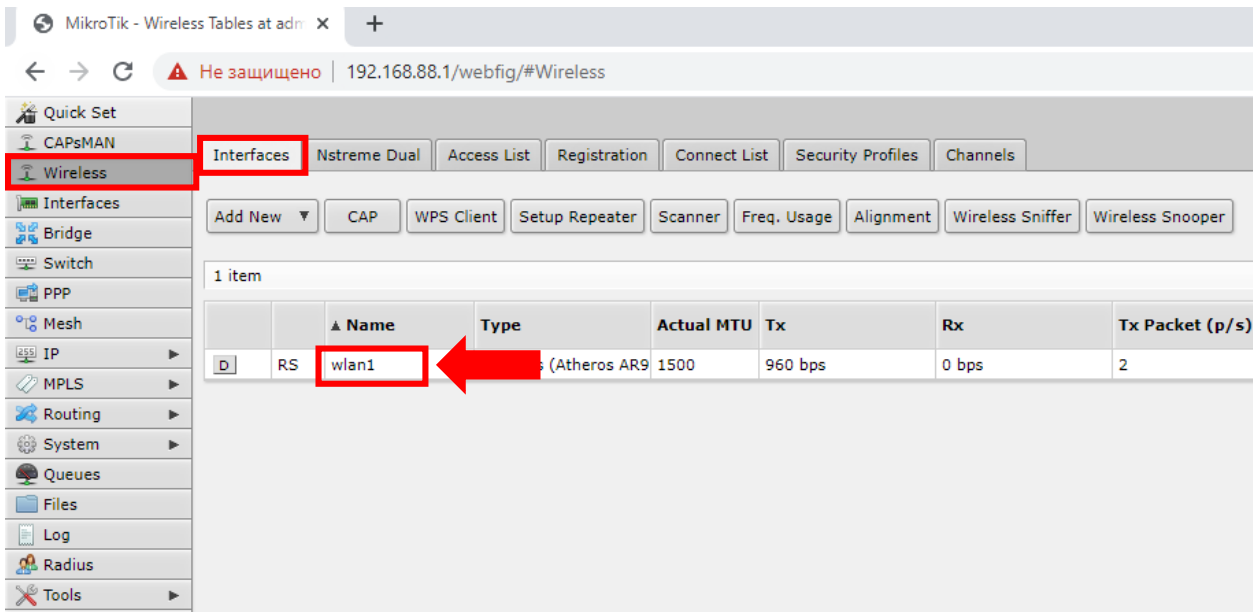
- Ставим галочку **Enabled**
- В **Chain** выбираем **srcnat**
- В **Out. Interface** выбираем наше PPPoE соединение **pppoe-out1**
- В **Action** ставим **masquerade**
- Нажимаем **Ok**



12 Профит! Доступ в интернет на устройствах должен появиться.

# Настройка Wi-Fi

## 1 Переходим на вкладку **Wireless** > **Interfaces**



The screenshot shows the MikroTik WinBox interface. The left sidebar has 'Wireless' selected. The top navigation bar has 'Interfaces' selected. Below the navigation bar are buttons for 'Add New', 'CAP', 'WPS Client', 'Setup Repeater', 'Scanner', 'Freq. Usage', 'Alignment', 'Wireless Sniffer', and 'Wireless Snooper'. A table displays one interface:

	Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)
D	RS wlan1	(Atheros AR9	1500	960 bps	0 bps	2

По умолчанию в таблице уже будет созданный интерфейс точки доступа Wi-Fi, если его нет, то можно создать его кнопкой Add New. Если он есть, то можно отредактировать его настройки, нажав на него.

## 2 Откроется окно настройки Wi-Fi

- Ставим галочку **Enabled**, если она не стоит
- В **Mode** выбираем **AP Bridge**
- В **Band** выбираем частоту и стандарт работы (**2GHz-B/G/N** или **5GHz-A/AC**) в зависимости от того какие стандарты роутер поддерживает и какую сеть необходимо создать
- В **Channel Width** и **Frequency** при необходимости можно изменить ширину канала и канал соответственно
- В **SSID** задаём имя беспроводной сети
- В **Security Profile** выбираем имя профиля безопасности. По умолчанию создан профиль **Default**
- В **WPS** можно выбрать режим работы WPS или отключить его
- Нажимаем **Ok** для сохранения



Quick Set  
CAPsMAN  
Wireless  
Interfaces  
Bridge  
Switch  
PPP  
Mesh  
IP  
MPLS  
Routing  
System  
Queues  
Files  
Log  
Radius  
Tools  
New Terminal  
Make Supout.rif  
Undo  
Redo  
Hide Menu  
Hide Passwords  
Safe Mode  
Design Skin  
Manual  
WinBox  
Graphs  
End-User License  
Logout

OK Apply Advanced Mode WPS Accept WPS Client Setup Repeater

running ap running slave

**Enabled**

**Name** wlan1

**Type** Wireless (Atheros AR9300)

**MTU** 1500

**Actual MTU** 1500

**L2 MTU** 1600

**MAC Address** E4:8D:8C:69:FF:EC

**ARP** enabled

**ARP Timeout** ▼

**Mode** ap bridge

**Band** 2GHz-B/G/N

**Channel Width** 20/40MHz Ce

**Frequency** auto MHz

**SSID** Mikrotik-69FFEC

**Scan List** default

**Wireless Protocol** 802.11

**Security Profile** default

**WPS Mode** push button

**Bridge Mode** enabled

**VLAN Mode** no tag

**VLAN ID** 1

3 Остаётся скорректировать настройки выбранного профиля безопасности Default

Для этого переходим в раздел Security Profiles и Нажимаем в таблице на имя нашего профиля Default

MikroTik - Wireless Tables at admin | 192.168.88.1/webfig/#Wireless.Security\_Profiles

← → ↻ Не защищено | 192.168.88.1/webfig/#Wireless.Security\_Profiles

Quick Set  
CAPsMAN  
Wireless  
Interfaces  
Bridge  
Switch  
PPP  
Mesh  
IP  
MPLS  
Routing  
System  
Queues

Interfaces Nstreme Dual Access List Registration Connect List **Security Profiles** Channels

Add New

1 item

	Name	Mode	Authentica... Types	Unicast Ciphers	Group Ciphers	WPA Pre-Shared Key
-	* default		WPA PSK, WPA	aes ccm	aes ccm	*****

#### 4 Открываются настройки профиля безопасности

- В **Mode** выбираем **Dynamic Keys**
- В **Authentication Types** ставим галочки на **WPA PSK** и **WPA2 PSK**
- В **WPA Pre-Shared Key** и **WPA2 Pre-Shared Key** прописываем пароль для подключения к Wi-Fi сети
- Нажимаем **Ok** для сохранения
- Профит! Можно подключать устройства к Wi-Fi по заданным имени сети и паролю

MikroTik - Security Profile <default> x +

← → ↻ Не защищено | 192.168.88.1/webfig/#Wireless.Security\_Profiles.0

Quick Set  
CAPsMAN  
Wireless  
Interfaces  
Bridge  
Switch  
PPP  
Mesh  
IP  
MPLS  
Routing  
System  
Queues  
Files  
Log  
Radius  
Tools  
New Terminal  
Make Supout.rif  
Undo  
Redo  
Hide Menu  
Hide Passwords  
Safe Mode  
Design Skin  
Manual  
WinBox  
Graphs  
End-User License  
Logout

OK Cancel Apply Remove

default

Name	default
Mode	dynamic keys
Authentication Types	<input checked="" type="checkbox"/> WPA PSK <input checked="" type="checkbox"/> WPA2 PSK <input type="checkbox"/> WPA EAP <input type="checkbox"/> WPA2 EAP
Unicast Ciphers	<input checked="" type="checkbox"/> aes ccm <input type="checkbox"/> tkip
Group Ciphers	<input checked="" type="checkbox"/> aes ccm <input type="checkbox"/> tkip
WPA Pre-Shared Key	.....
WPA2 Pre-Shared Key	.....
Supplicant Identity	MikroTik
Group Key Update	00:05:00
Management Protection	disabled
Management Protection Key	
MAC Authentication	<input type="checkbox"/>
MAC Accounting	<input type="checkbox"/>
EAP Accounting	<input type="checkbox"/>
Interim Update	00:00:00
MAC Format	XX:XX:XX:XX:XX:XX
MAC Mode	as username
MAC Caching Time	disabled
EAP Methods	passthrough