

# Ограничение доступа для клиентов

Рассмотрим способы фильтрации клиентов роутера по IP-адресам и MAC-адресам .

## Ограничение доступа по IP-адресу

Настройка выполняется через веб-интерфейс.

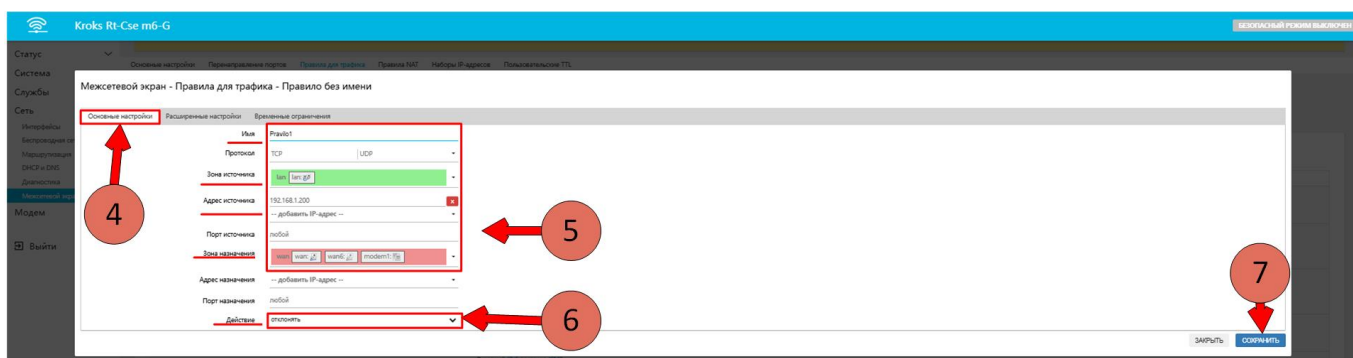
1. Перейдите на вкладку *Сеть - Межсетевой экран*.
2. Затем нажмите на окно **Правила для трафика**.
3. Внизу окна нажмите на кнопку "ДОБАВИТЬ".

Имя	Соответствие	Действие	Включить
wan-dhcp-v4-allow	Видеякий IP-адреса DHCP И: [wan] порт 67 В: [wan-устройство] порт 68	Разрешить входящий трафик	<input checked="" type="checkbox"/>
wan-ping-allow	Видеякий IP-адреса ICMP И: [wan] В: [wan-устройство]	Разрешить входящий трафик	<input type="checkbox"/>
wan-icmp-v4-allow	Видеякий IP-адреса ICMP И: [wan] В: [wan-устройство]	Разрешить входящий трафик	<input checked="" type="checkbox"/>
wan-dhcp-v6-allow	Видеякий IP-адреса DHCP И: [wan] IP-адрес: fe80::/10 порт 547 В: [wan-устройство] IP-адрес: fe80::/10 порт 546	Разрешить входящий трафик	<input checked="" type="checkbox"/>
wan-mid-v6-allow	Видеякий IP-адреса ICMP И: [wan] В: [wan-устройство]	Разрешить входящий трафик	<input checked="" type="checkbox"/>
wan-icmp-v6-allow	Видеякий IP-адреса ICMP И: [wan] В: [wan-устройство]	Разрешить входящий трафик	<input checked="" type="checkbox"/>
wan-ping-v6-forward-allow	Переадресация IP-адреса ICMP И: [wan] В: любой адрес	Разрешить переадресанный трафик	<input type="checkbox"/>
wan-icmp-v6-forward-allow	Переадресация IP-адреса ICMP И: [wan] В: любой адрес	Разрешить переадресанный трафик	<input checked="" type="checkbox"/>
guest-icmp-v4-allow	Видеякий IP-адреса ICMP И: [guest] В: [wan-устройство] IP-адрес: 10.1.1.1 Ограничение до 10 пакетов в секунду	Разрешить входящий трафик	<input checked="" type="checkbox"/>
guest-dns-v4-allow	Видеякий IP-адреса TCP UDP И: [guest] В: [wan-устройство] IP-адрес: 10.1.1.1 порт 53	Разрешить входящий трафик	<input checked="" type="checkbox"/>
guest-dhcp-v4-allow	Видеякий IP-адреса DHCP И: [guest] IP-адрес: 10.1.1.1 порт 67 В: [wan-устройство] IP-адрес: 255.255.255.255 порт 67	Разрешить входящий трафик	<input checked="" type="checkbox"/>

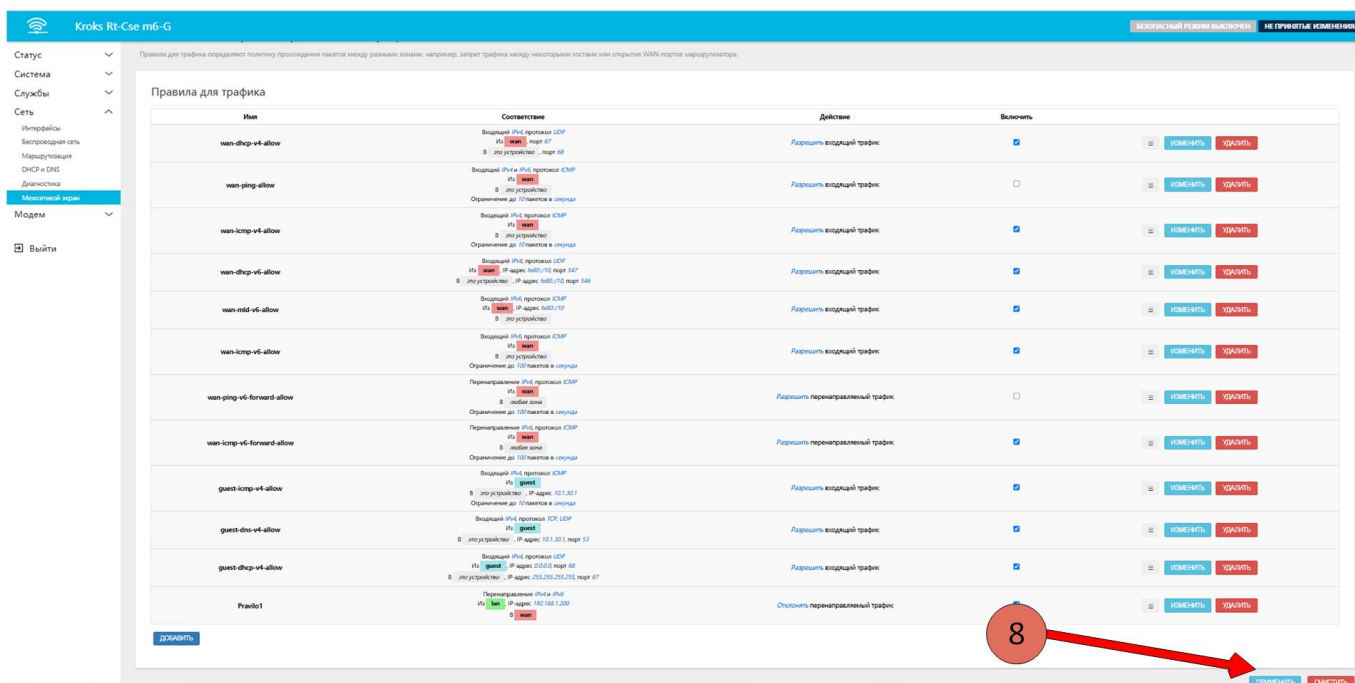
1. Откроется окно **Основные настройки**.
2. Необходимо настроить следующие пункты:
  - Имя - имя вашего правила
  - Зона источника - выберите lan
  - Адрес источника - выберите устройство, которому хотите запретить доступ, из списка или введите адрес вручную
  - Зона назначения - выберите wan (если хотите запретить доступ в Интернет)

1. Выберите действие из выпадающего списка - отклонять

1. Нажмите кнопку сохранить.

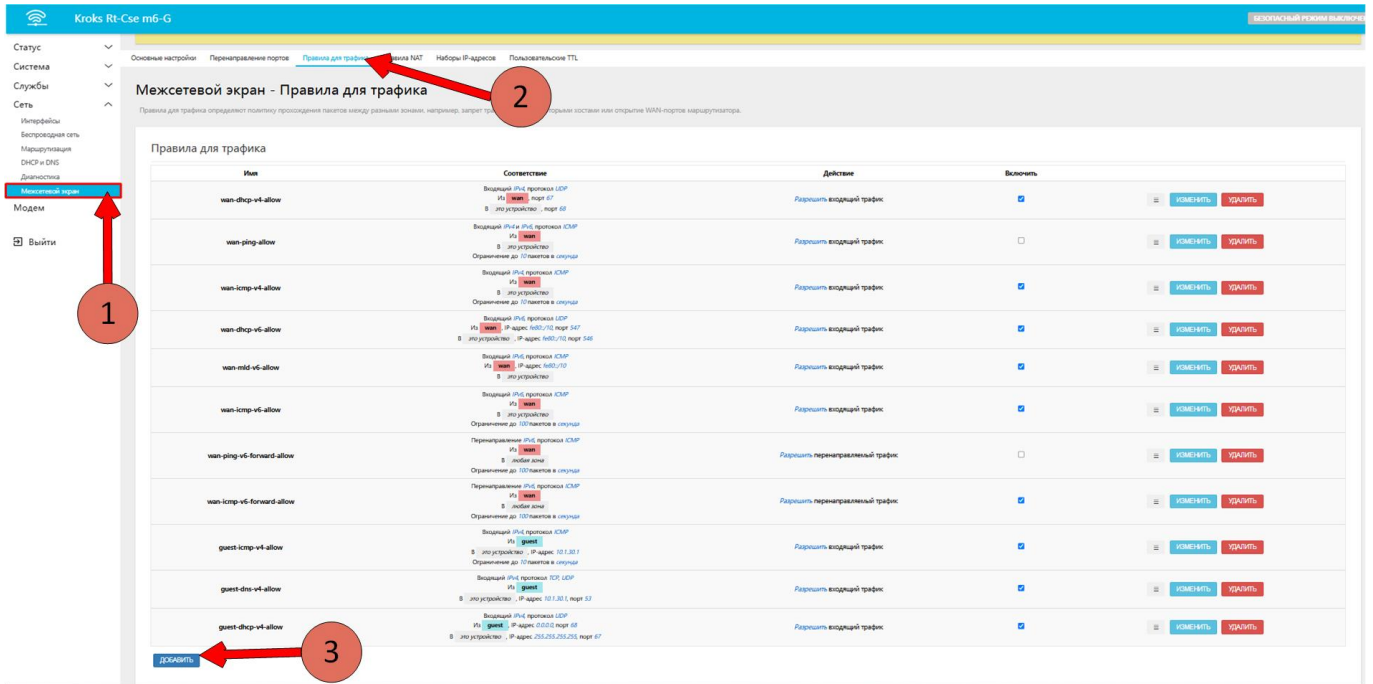


1. Нажмите кнопку “ПРИМЕНИТЬ” во вновь открывшемся окне.



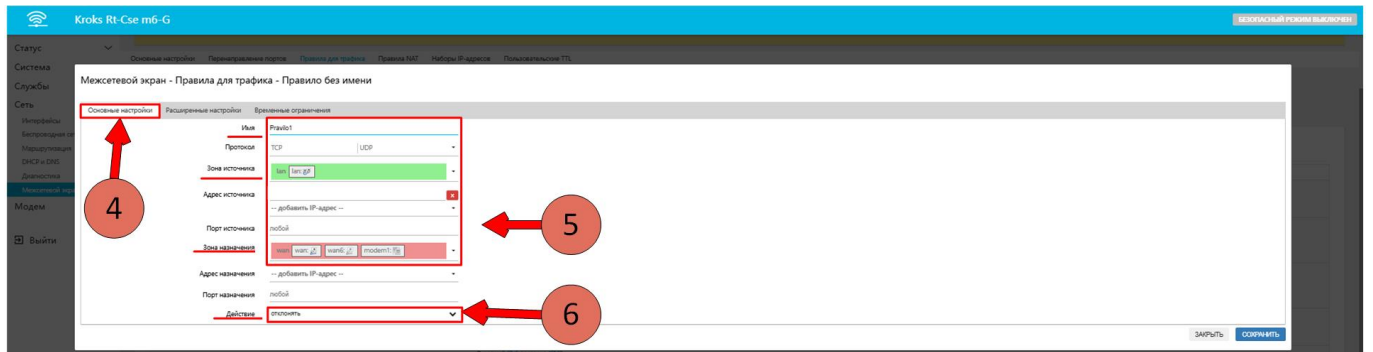
## Ограничение доступа по MAC-адресу

1. Перейдите на вкладку *Сеть* - *Межсетевой экран*.
1. Затем нажмите на окно **Правила для трафика**.
1. Внизу окна нажмите на кнопку “ДОБАВИТЬ”.

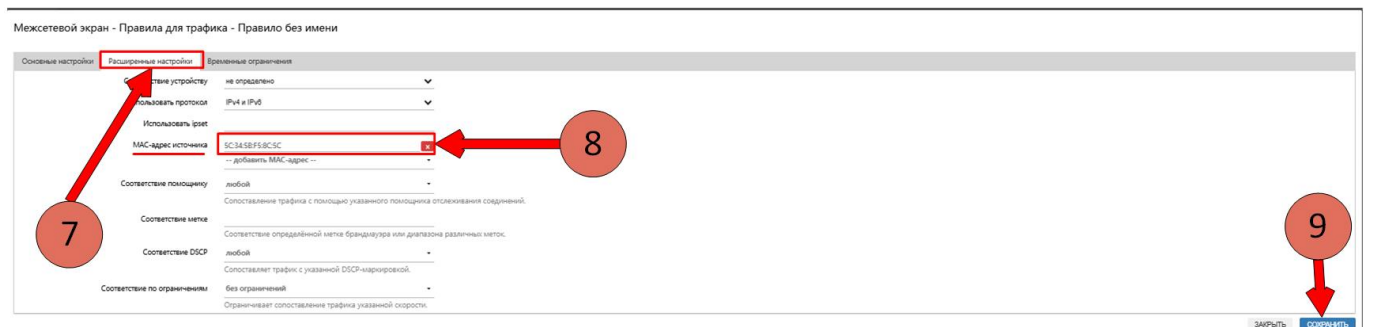


1. Откроется окно **Основные настройки**.
2. Необходимо настроить следующие пункты:
  - o Имя - имя вашего правила
  - o Зона источника - выберите lan
  - o Зона назначения - выберите wan (если хотите запретить доступ в Интернет)

1. Выберите действие из выпадающего списка - отклонять



1. Затем перейдите в окно *Расширенные настройки*.
2. Введите MAC адрес источника (устройство которое вы хотите ограничить в доступе к Интернету)
3. Нажмите кнопку сохранить



1. Нажмите кнопку "ПРИМЕНИТЬ" во вновь открывшемся окне.

Крокс Rt-Cse m6-G

Правила для трафика определяют политику прохождения пакетов между разными зонами, например, запрет трафика между некоторыми зонами или открыты WAN-порты маршрутизатора.

Имя	Состояние	Действие	Включить	ИЗМЕНИТЬ	УДАЛИТЬ
wan-dhcp-v4-allow	Включен IPsec политика ICMP Имя: wan S: (любая сеть) D: (любая сеть) - порт 68	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
wan-ping-allow	Включен IPsec политика ICMP Имя: wan S: (любая сеть) D: (любая сеть) Ограничение до 10 пакетов в секунду	Разрешить входящий трафик	<input type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
wan-icmp-v4-allow	Включен IPsec политика ICMP Имя: wan S: (любая сеть) D: (любая сеть) Ограничение до 10 пакетов в секунду	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
wan-dhcp-v6-allow	Включен IPsec политика ICMP Имя: wan S: (любая сеть) D: IP адрес: 168.0/10 порт 547 D: (любая сеть) - IP адрес: 168.0/10 порт 548	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
wan-rtsp-v6-allow	Включен IPsec политика ICMP Имя: wan S: (любая сеть) D: (любая сеть)	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
wan-ping-v6-forward-allow	Перенаправление IPsec политика ICMP Имя: wan S: (любая сеть) D: (любая сеть) Ограничение до 10 пакетов в секунду	Разрешить перенаправленный трафик	<input type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
wan-rtsp-v6-forward-allow	Перенаправление IPsec политика ICMP Имя: wan S: (любая сеть) D: (любая сеть) Ограничение до 10 пакетов в секунду	Разрешить перенаправленный трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
guest-icmp-v4-allow	Включен IPsec политика ICMP Имя: guest S: (любая сеть) D: IP адрес: 10.1.30.1 Ограничение до 10 пакетов в секунду	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
guest-dns-v4-allow	Включен IPsec политика TCP UDP Имя: guest S: (любая сеть) D: (любая сеть) - IP адрес: 10.1.30.1 порт 53	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
guest-dhcp-v4-allow	Включен IPsec политика UDP Имя: guest S: (любая сеть) D: IP адрес: 0.0.0.0 порт 68 D: (любая сеть) - IP адрес: 255.255.255.255 порт 67	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ
Private1	Перенаправление IPsec политика ICMP Имя: wan S: (любая сеть) D: (любая сеть)	Отклонить перенаправленный трафик	<input type="checkbox"/>	ИЗМЕНИТЬ	УДАЛИТЬ

ДОБАВИТЬ

10

ИЗМЕНИТЬ УДАЛИТЬ

From: <http://wiki.glschnklx.ru/> - kroks

Permanent link: <http://wiki.glschnklx.ru/routery/chasto-zadavaemye-voprosy/ogranichenie-dostupa-dlya-klientov>

Last update: 2026/01/13 10:54

