

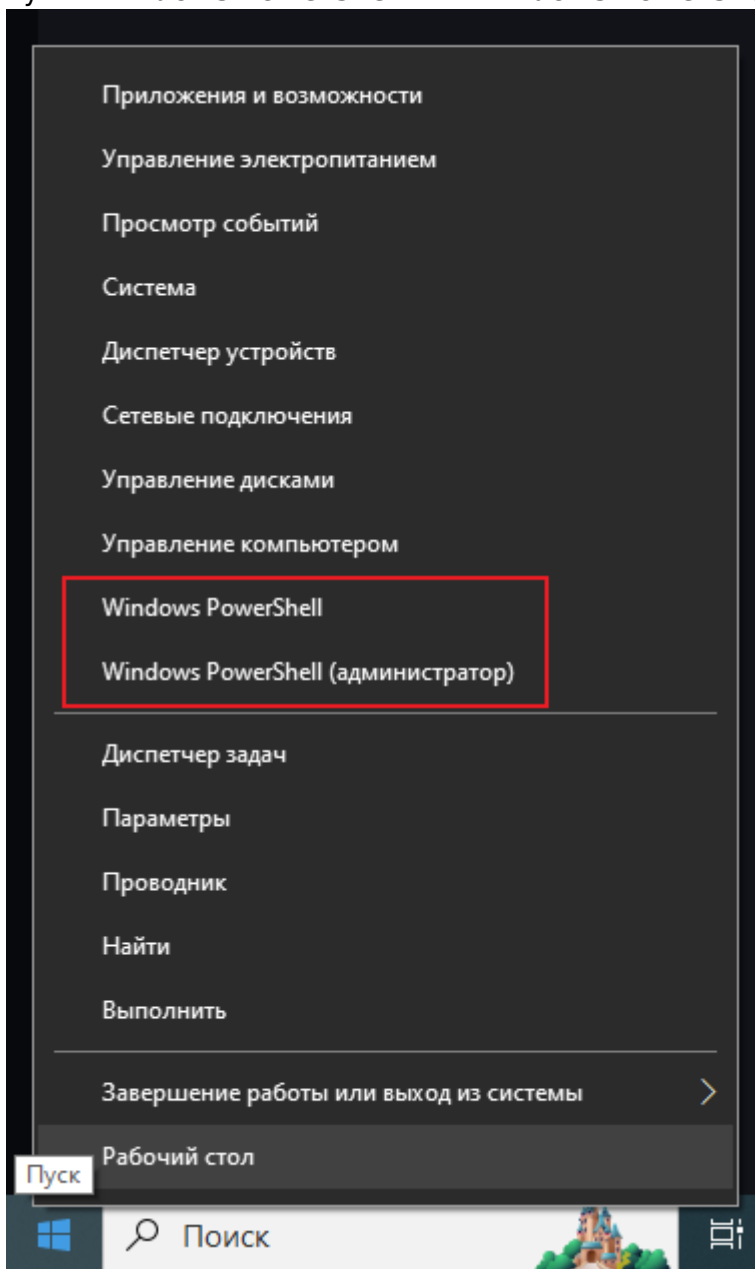
Блокирование сайтов через веб-интерфейс роутера

В данной статье мы разберём способ блокирования доступа к каким-либо определенным ресурсам, через веб-интерфейс роутера Kroks. Для этого понадобится несколько простых действий.

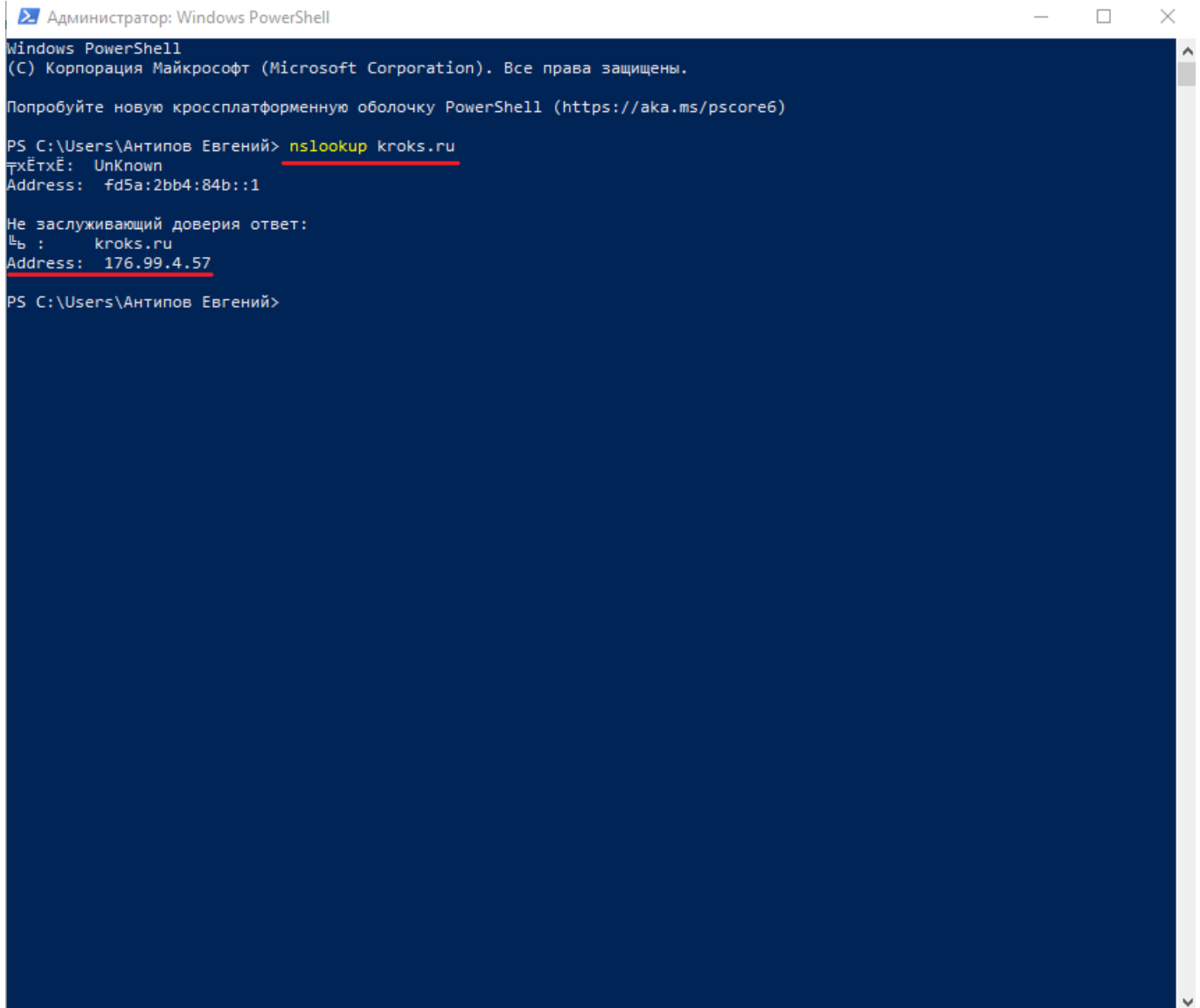
Получение IP адреса необходимого ресурса

Для начала нам понадобится выяснить какие IP-адреса использует нужный вам ресурс. Проверить это можно с помощью **Windows PowerShell**.

Нажмите правой кнопкой мыши на меню **Пуск** и в открывшемся контекстном окне выберите пункт **Windows PowerShell** или **Windows PowerShell (администратор)**.



В открывшемся окне введите команду **nslookup** и адрес нужного вам ресурса (в примере мы используем сайт **kroks.ru**), после чего нажать клавишу **Enter**. После выполнения команды, вы увидите в строке **Address** нужный вам IP-адрес.



```
Администратор: Windows PowerShell
Windows PowerShell
(С) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

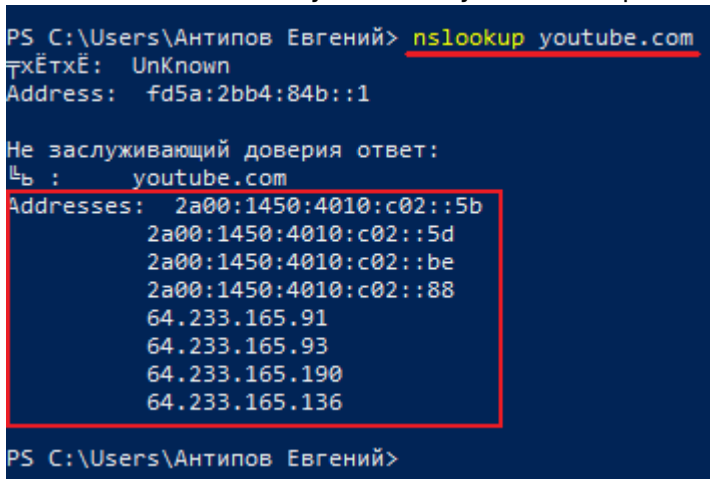
Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/powershell)

PS C:\Users\Антипов Евгений> nslookup kroks.ru
ПхЁтхЁ: UnKnown
Address: fd5a:2bb4:84b::1

Не заслуживающий доверия ответ:
Ь : kroks.ru
Address: 176.99.4.57

PS C:\Users\Антипов Евгений>
```

Обратите внимание, что ресурс может использовать несколько IP-адресов, как формата IPv4, так и IPv6. В таком случае вам нужно скопировать их все.



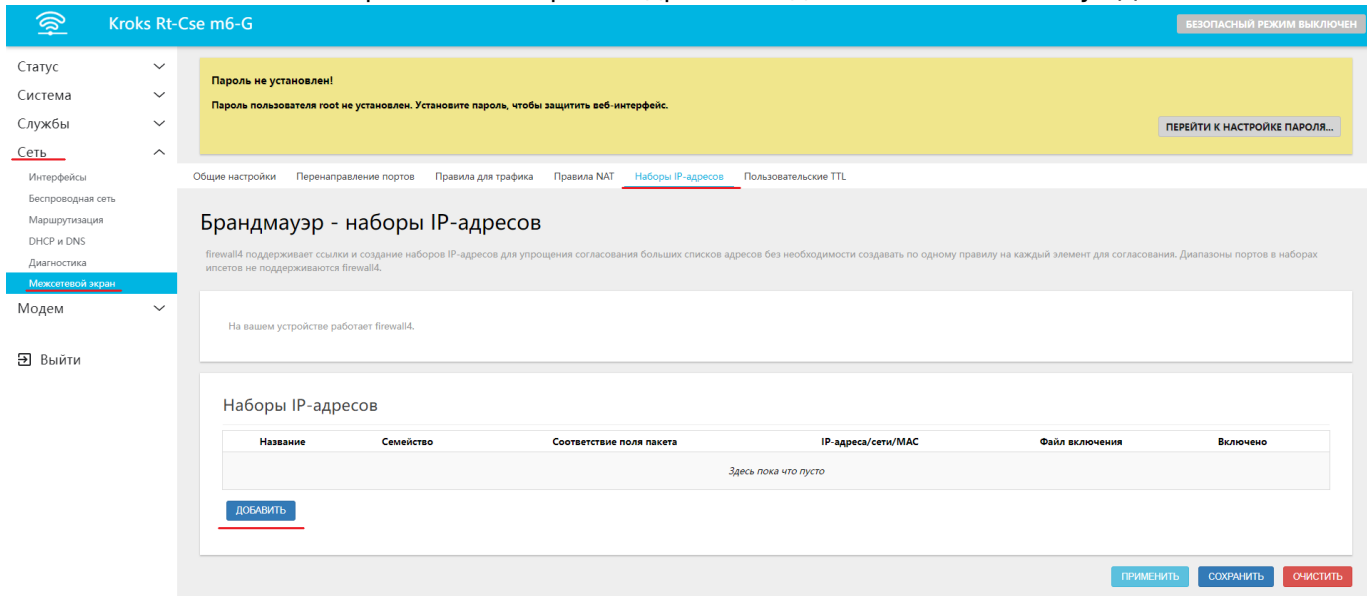
```
PS C:\Users\Антипов Евгений> nslookup youtube.com
ПхЁтхЁ: UnKnown
Address: fd5a:2bb4:84b::1

Не заслуживающий доверия ответ:
Ь : youtube.com
Addresses: 2a00:1450:4010:c02::5b
           2a00:1450:4010:c02::5d
           2a00:1450:4010:c02::be
           2a00:1450:4010:c02::88
           64.233.165.91
           64.233.165.93
           64.233.165.190
           64.233.165.136

PS C:\Users\Антипов Евгений>
```

Набор IP-адресов

Следующим шагом вам необходимо открыть веб-интерфейс роутера и перейти на вкладку "Сеть" → "Межсетевой экран" → "Наборы IP-адресов". Здесь нажмите кнопку "ДОБАВИТЬ".



В открывшемся окне вводим следующие настройки:

Название - любое (в примере kroks);

Семейство - зависит от типа IP-адресов, используемых ресурсом (в примере IPv4);

Соответствие поля пакета - **dest_net: Сеть назначения;**

IP-адреса/сети/MAC - сюда нужно ввести найденные ранее IP-адреса (в пример 176.99.4.57), если адресов несколько, то нажмите на символ "+" для появления дополнительной строки.

Остальные строки рекомендуется оставить без изменений. По окончании настройки нажмите кнопку "СОХРАНИТЬ".

Брандмауэр - наборы IP-адресов

Название

Комментарий

Семейство

Соответствие поля пакета

-- Выберите --

Поля пакета для сопоставления.
Синтаксис: direction datatype, например: src_port, dest_net.
Направления: src, dst. Типы данных: ip, port, mac, net, set.
Префиксы направления необязательны.
*Примечание: тип данных set не поддерживается в fw4.

IP-адреса/сети/MAC

macaddr[ip/cidr]

Максимальное количество записей

Файл включения

Путь к файлу с CIDR, подсетями, IP-адресами хостов и т.д.

Таймаут

Единица измерения: секунды. По умолчанию @ означает, что запись постоянно добавляется в набор.
Максимум: 2147483 секунд.

Счетчики

Включает отслеживание количества пакетов и байтов для набора.

Правила для трафика

Далее перейдите на вкладку “Сеть” → “Межсетевой экран” → “Правила для трафика”, в нижней части страницы нажмите кнопку “ДОБАВИТЬ”.

Название	Соответствие	Действие	Включить
Allow-DHCP-Renew	Входящий IPv4, протокол UDP Из wan В это устройство, порт 68	Разрешить входящий трафик	<input checked="" type="checkbox"/>
Allow-IGMP	Входящий IPv4, протокол IGMP Из wan В это устройство	Разрешить входящий трафик	<input type="checkbox"/>
Allow-IPSec-ESP	Входящий IPv4 и IPv6, протокол IPSEC-ESP Из wan В это устройство	Разрешить входящий трафик	<input type="checkbox"/>
Allow-IPSec-IKE	Входящий IPv4 и IPv6, протокол UDP Из wan В это устройство, порт 500	Разрешить входящий трафик	<input type="checkbox"/>
Allow-IPSec-NAT-T	Входящий IPv4 и IPv6, протокол UDP Из wan В это устройство, порт 4500	Разрешить входящий трафик	<input type="checkbox"/>
Правило без имени	Исходящий IPv4 и IPv6 Из это устройство В это устройство	ничего	<input checked="" type="checkbox"/>

В открывшемся окне введите следующие настройки:

Название - любое (в примере kroks);

Протокол - любой;

Зона источника - lan;

Зона назначения - wan;

Действие - отклонить.

Межсетевой экран - Правила для трафика - kroks

Общие настройки | **Расширенные настройки** | Временные ограничения

Название: kroks

Протокол: Любой

Зона источника: lan

Адрес источника: -- добавить IP-адрес --

Зона назначения: wan

Адрес назначения: -- добавить IP-адрес --

Действие: отклонить

ЗАКРЫТЬ СОХРАНИТЬ

После чего перейдите на вкладку “Расширенные настройки” и укажите здесь созданный вами набор IP-адресов в графе **Использовать ipset**, после чего нажмите кнопку “СОХРАНИТЬ”.

Межсетевой экран - Правила для трафика - kroks

Общие настройки	Расширенные настройки	Временные ограничения
Соответствие устройству	не определено	▼
Использовать протокол	IPv4 и IPv6	▼
Использовать ipset	kroks	▼
MAC-адрес источника	-- добавить MAC-адрес --	▼
Соответствие помощнику	любой	▼
	Сопоставление трафика с помощью указанного помощника отслеживания соединений.	
Соответствие метки		
	Соответствие определённой метке брандмауэра или диапазона различных меток.	
Соответствие DSCP	любой	▼
	Сопоставляет трафик с указанной DSCP-маркировкой.	
Соответствие по ограничениям	без ограничений	▼
	Ограничивает сопоставление трафика указанной скорости.	

ЗАКРЫТЬ **СОХРАНИТЬ**

Теперь нужно нажать кнопку "ПРИМЕНИТЬ" внизу страницы.

Kroks Rt-Cse m6-G
БЕЗОПАСНЫЙ РЕЖИМ ВЫКЛЮЧЕН

Allow-DHCPv6	Ис wan В это устройство , порт 546	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ
Allow-MLD	Входящий IPv6, протокол ICMP Ис wan IP-адрес fe80::10 В это устройство	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ
Allow-ICMPv6-Input	Входящий IPv6, протокол ICMP В это устройство Ограничение до 1000 пакетов в секунда	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ
Allow-ICMPv6-Forward	Перенаправление IPv6, протокол ICMP Ис wan В любая зона Ограничение до 1000 пакетов в секунда	Разрешить перенаправляемый трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ
Allow-Guest-Icmp	Входящий IPv4, протокол ICMP Ис guest В это устройство Ограничение до 10 пакетов в секунда	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ
Allow-Guest-Dns	Входящий IPv4 и IPv6, протокол TCP, UDP Ис guest В это устройство , порт 53	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ
Allow-Guest-Dhcp	Входящий IPv4, протокол UDP Ис guest В это устройство , порт 67	Разрешить входящий трафик	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ
Правило без имени	Исходящий IPv4 и IPv6 Ис это устройство В это устройство	ничего	<input checked="" type="checkbox"/>	ИЗМЕНИТЬ УДАЛИТЬ

ДОБАВИТЬ
ПРИМЕНИТЬ
СОХРАНИТЬ
ОЧИСТИТЬ

После того как веб-интерфейс снова станет доступен, необходимо перезагрузить роутер.

Если необходимый вам ресурс использует сразу и IPv4 и IPv6 адреса, то необходимо аналогичным образом создать для них **набор IP-адресов** и **Правила для трафика**.

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

Permanent link: <http://wiki.glschnklx.ru/routery/prodvinutaya-nastroyka/blokirovanie-saytov-cherez-veb-interfeys-routera>

Last update: 2026/01/13 10:54

