

RouterOS RouterOS RouterOS

RouterOS

Ниже приведены рекомендации по дополнительной защите вашего устройства при уже настроенных строгих правилах брандмауэра.

RouterOS RouterOS

Начните с обновления версии RouterOS. В некоторых старых версиях присутствовали уязвимости, которые были исправлены. Поддерживайте устройство в актуальном состоянии, чтобы обеспечить безопасность. В WinBox или WebFig нажмите "проверить обновления" для обновления. Рекомендуем следить за объявлениями в нашем блоге о безопасности, чтобы быть в курсе новых проблем.

RouterOS RouterOS

RouterOS RouterOS

Измените стандартное имя пользователя **admin** на другое. Индивидуальное имя помогает защитить доступ к роутеру, если кто-то имеет прямой доступ к вашему устройству:

```
/user add name=myname password=mypassword group=full
/user disable admin
```

RouterOS RouterOS

MikroTik роутеры требуют настройки пароля. Мы рекомендуем использовать генераторы паролей для создания безопасных, уникальных паролей. Под безопасным паролем подразумевается:

- Минимум 12 символов;
- Включение цифр, символов, заглавных и строчных букв;
- Отсутствие слов из словаря или их комбинаций;
- Обращайте внимание на кавычки в пароле — их нужно экранировать.

```
/user set myname password="!={Ba3N!40TyX+GvKBz?jTLIUcx/,",
```

RouterOS RouterOS

Чтобы предотвратить удалённый доступ к вашему устройству, настроен предустановленный брандмауэр, который блокирует соединения с WAN (интернет стороны). Это сделано намеренно. Не удаляйте эти правила, если не уверены в безопасности соединения.

Если вам нужно открыть удалённый доступ, рекомендуем использовать VPN, например WireGuard.

Руководство по настройке WireGuard VPN доступно [здесь](#).

?????? ?? MAC (RouterOS MAC-access)

В RouterOS есть встроенные опции для удобного административного доступа к сетевым устройствам. Рекомендуется отключить следующие сервисы на рабочих сетях:

- **MAC-Telnet**
- **MAC-WinBox**
- **MAC-Ping**

```
/tool mac-server set allowed-interface-list=none  
/tool mac-server mac-winbox set allowed-interface-list=none  
/tool mac-server ping set enabled=no
```

????????????? ??????? (Neighbor Discovery)

Протокол MikroTik Neighbor Discovery используется для отображения и распознавания других роутеров MikroTik в сети. Рекомендуется отключить обнаружение соседей на всех интерфейсах:

```
/ip neighbor discovery-settings set discover-interface-list=none
```

??????? ?????????????? ?????????????? (Bandwidth server)

Сервер пропускной способности используется для тестов между двумя роутерами MikroTik. Его стоит отключить в рабочей среде:

```
/tool bandwidth-server set enabled=no
```

DNS ???

В роутере может быть включён DNS кеш, который ускоряет разрешение DNS-запросов с клиентов к удалённым серверам. Если кеш не нужен или используется другой роутер для этих целей, отключите его:

```
/ip dns set allow-remote-requests=no
```

??????? ?????????????? ?????????

MikroTik RouterOS может иметь включённые дополнительные сервисы (по умолчанию они отключены). Это прокси, socks, UPnP и облачные сервисы:

```
/ip proxy set enabled=no  
/ip socks set enabled=no  
/ip upnp set enabled=no  
/ip cloud set ddns-enabled=no update-time=no
```

????? ?????????? ?????? ?? SSH

Можно включить более строгие настройки SSH (добавить aes-128-ctr и запретить hmac sha1 и группы с sha1):

```
/ip ssh set strong-crypto=yes
```

???????????? ????????

Ethernet/SFP ????????????

Рекомендуется отключать все неиспользуемые интерфейсы на вашем роутере, чтобы снизить риск несанкционированного доступа:

```
/interface print  
/interface set X disabled=yes
```

где **X** — номера неиспользуемых интерфейсов.

??-???????? (LCD)

Некоторые RouterBOARD имеют ЖК-модуль для отображения информации. Можно установить PIN код:

```
/lcd/pin/set pin-number=3659 hide-pin-number=yes
```

Или отключить ЖК-дисплей полностью:

```
/lcd/set enabled=no
```

Revision #1

Created 11 November 2025 11:01:18 by Admin

Updated 11 November 2025 11:01:53 by Admin