Чек-лист
по настройке маршрутизатора MikroTik

В этом документе приведены пункты, по которым можно сверить, все ли настроено на маршрутизаторе фирмы MikroTik. Чек-лист подходит для основной массы ситуаций, когда устройство используется в сетях с количеством сотрудников до 100 единиц и одним филиалом. Подключать маршрутизатор к Интернету можно только после того, как будет выполнена полная настройка. В противном случае существует большой риск взлома устройства.

В документе используются термины:

- Локальная сеть – сеть, в которой работают сотрудники.
- Гостевая сеть – сеть, из которой не должно быть доступа в локальную сеть, но должен быть доступ в Интернет. Пример использования: Wi-Fi для клиентов организации.

Предварительная подготовка

1. Установить последнюю версию RouterOS. Использовать версию Long-term или Stable. В приоритете Long-term, как более стабильная ветка.
2. Установить последнюю версию загрузчика RouterBOOT. *Применимо только для аппаратных платформ от MikroTik. Для виртуальных машин или RouterOS, установленных на платформу x86, не применимо.*
3. Полностью удалить всю имеющуюся конфигурацию. *Рекомендуем использовать именно полную очистку конфигурации. Для того, чтобы устройство можно было полностью подстроить под свои задачи.*

Базовая настройка

4. Назначить IP-адрес внешнему интерфейсу.
5. Создать маршрут по умолчанию.
6. Создать bridge-интерфейс для локальной сети.
7. Интерфейсы, которые должны быть в локальной сети, поместить в bridge-интерфейс локальной сети.
8. Назначить IP-адрес bridge-интерфейсу локальной сети.
9. Настроить NAT.
10. Настроить DHCP-сервер для локальной сети.
11. Настроить DNS-сервер:
    11.1. прописать вышестоящие DNS-серверы;
    11.2. разрешить запросы к DNS-серверу от других устройств.
12. SNTP-клиент.

Основная беспроводная сеть

13. Для каждого частотного диапазона создать беспроводную сеть для доступа в локальную сеть (основная беспроводная сеть).
14. Добавить основные беспроводные сети в bridge-интерфейс локальной сети.

Файрвол

NAT

15. Настроить пробросы портов (при необходимости).

Filter

16. Для цепочки Input настроить файрвол в нормально закрытый режим для доступа из всех сетей, кроме локальной. Для локальной сети оставить нормально открытый режим работы.
17. Для цепочки Forward настроить файрвол в нормально закрытый режим доступа из всех сетей, кроме локальной. Для локальной сети оставить нормально открытый режим работы. Не забыть сделать исключения для правил проброса портов.

Доступ к сервисам, которые дают возможность обслуживать маршрутизатор (SSH, WinBox и т.д.), предоставлять только из локальной сети. При необходимости доступа к таким службам из других сетей давать к ним доступ только с помощью VPN, белого списка IP-адресов или технологии port-knocking.

QoS

18. Настроить равномерное распределение трафика между пользователями в случае, если ресурсов интернет-канала не хватает.

Прочее

19. Отключить службы, которые не будут использоваться.
20. Изменить имя пользователя по умолчанию и задать ему пароль.
21. Службу mac-telnet и обнаружение с помощью протокола MNDP оставить доступными только для локальной сети.

Гостевая беспроводная сеть

22. Создать bridge-интерфейс для гостевой сети (*при необходимости*).
23. Назначить IP-адрес bridge-интерфейсу гостевой сети.
24. Для каждого частотного диапазона создать беспроводную сеть для доступа в гостевую сеть.
25. Добавить гостевые беспроводные сети в bridge-интерфейс гостевой сети.
26. Настроить DHCP-сервер для гостевой сети.
27. В файрволе настроить правила для блокировки гостевой беспроводной сети.
28. В очередях настроить правила, которые будут контролировать излишнее потребление трафика гостевой сетью. *Необходимо для того, чтобы не возникло ситуации, когда в локальной сети плохой Интернет из-за того, что кто-то из гостевой сети активно использует ресурсы интернет-канала.*

Надеюсь, что этот чек-лист будет вам полезен!
Дмитрий Скоромнов,
официальный тренер MikroTik (TR0680)