Чек-лист | Эксперт

Базовая настройка Mikrotik

ADM Service Check List basic Mikrotik sets

1. Прошивка

- [ ] **1.1** Сброс
  Полный сброс БЕЗ default config

- [ ] **1.2** Обновить прошивку до последней
  ТОЛЬКО Stable версия. general packet

2. Интерфейсы

- [ ] **2.1** Подписать все интерфейсы
  Все LAN, WAN, VLAN по принципу LAN-Port2, WAN-Port1 etc

- [ ] **2.2** Настроить модуль Wi-Fi (если есть)
  SSID, security profile, WPS - OFF! Канал, частота и т.д

- [ ] **2.3** Создать LAN Bridge
  Только нужные порты. Ничего лишнего не включать.

3. Адреса и DNS

- [ ] **3.1** Назначить IP адресацию
  LAN, WAN (если не DHCP) и VLAN если нужно

- [ ] **3.2** DHCP

Client на WAN если нужно и Сервер на LAN Bridge (если нужно)

- [ ] **3.3** Настроить DNS

  Адреса пересылки провайдера или локальный DNS (если есть). Так же сделать Allow remote req

4. Firewall

- [ ] **4.1** Разрешить удаленное управление с наших адресов

  SSH, WinBox. Остальное - отключить в Services

- [ ] **4.2** Создать правила established и related

  И на input и на forward, сильно снижает нагрузку на ЦП Пример: chain=input action=accept connection-state=established log=no

- [ ] **4.3** Разрешить DNS

  udp, port 53 chain=input

- [ ] **4.4** Allow Ping

  chain=input, protocol=icmp

- [ ] **4.5** Drop all

  Последним правилом. Не забываем указывать in-interface=WAN (или pppoe)

5. NAT

- [ ] **5.1** src-nat

  Если нужно для VPN например - ставим первыми

- [ ] **5.2** dst-nat

  Пробрасываем что нужно ТОЛЬКО в крайних случаях, рекомендуем использовать VPN для таких целей

- [ ] **5.3** Маскардинг

Ставим только нужные подсети на out-interface WAN (pppoe)

6. Services

- [ ] **6.1** Проверяем и отключаем ненужные сервисы

  В нашем случае: api, api-ssl, ftp, telnet

7. Финальные проверки

- [ ] **7.1** Проверяем наличие интернета

  Как с самого Mikrotik так и с клиентских устройств

- [ ] **7.2** Проверяем проброс портов

  Если есть

- [ ] **7.3** Проверяем удаленное управление

  с наших внешних адресов

- [ ] **7.4** Меняем имя устройства

  *System-Identify пишем по принципу *client*-*router№* Например - ADM-R1*

- [ ] **7.5** Настраиваем время

  NTP Client до ru.pool.ntp.org

- [ ] **7.6** Делаем backup настроек!

  Либо через WinBox files либо export / file=production-backup1

8. VPN

- [ ] **8.1** Настраиваем VPN туннели и VPN сервер

  Если необходимо

- [ ] **8.2** Проверка подключений по VPN

проверяем подключения

9. Финализация

- [ ] **9.1** Рестартуем роутер и проверяем после рестарта работу

ДВАЖДЫ проверь настройки перед выходом!!!

Создано с помощью онлайн сервиса Чек-лист | Эксперт: https://checklists.expert

как это убрать?