Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

MikroTik в офисе: наша методика hardening RouterOS 7

Как мы закрываем поверхность управления, режем сеть на VLAN и переводим роутер на регулярную э…

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Периметровый MikroTik чаще всего настроен один раз при заезде в офис и годами не обслуживается: открытый из интернета Winbox, заводская учётка admin, устаревшая RouterOS 6.x, плоская сеть без сегментации. Такой роутер рано или поздно становится чужим прокси-узлом или точкой входа шифровальщика — со всеми последствиями для 1С, бухгалтерии и репутации внешнего IP компании.

Почему это важно бизнесу

- Через роутер идёт весь трафик компании: банк-клиент, 1С, почта — его компрометация равна компрометации всего офиса
- Чужой ботнет на вашем IP — блокировки со стороны провайдера и попадание внешнего адреса в спам-листы
- Плоская сеть превращает один заражённый ноутбук в простой всей бухгалтерии на дни
- VPN на устаревших протоколах — утечка паролей сотрудников при работе из кафе и дома
- Восстановление после взлома без бэкапа конфигурации — это сутки простоя вместо 30 минут

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.21.x

Ветка long-term RouterOS, на которой держим парк офисных роутеров; обновляем вместе с routerbo…

по докам MikroTik, 7.21.5

0

Сервисов управления, доступных с WAN: Winbox и SSH — только из management-VLAN или через WireG…

наш стандарт

4

Минимум VLAN-сегментов в офисе: рабочие места, 1С/финансы, гости, IoT/камеры — через bridge vl…

наш стандарт

24 ч

Максимальный возраст копии конфигурации: ночной /export + /system backup уходят по SFTP на вне…

наш стандарт

16+

Длина паролей именованных учёток; заводской admin удаляем, для мониторинга — отдельная read-гр…

наш стандарт

60 с

Интервал опроса роутера по SNMPv3 в Zabbix: CPU, память, температура, трафик, состояние VPN-пи…

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Поверхность управления: сервисы, доступы, учётки

Что настраиваем

Периметровый роутер клиента (hEX S / hAP ax2 / RB4011 / CCR2004) — выполняем при первичном hardening за одно окно работ

Как мы это делаем

1. /ip service: telnet, ftp, www, api, api-ssl — disabled; ssh co strong-crypto=yes; winbox — только с address= подсети управления
2. /tool mac-server и mac-winbox: allowed-interface-list=none; /ip neighbor discovery-settings: discover-interface-list=none — роутер не отвечает на L2-обнаружение
3. Гасим socks, web-proxy, upnp, cloud ddns и bandwidth-server; /ip dns allow-remote-requests=yes — только при drop udp/tcp 53 на input с WAN
4. Учётки: admin удаляем после создания именованных, group=full только у инженеров; для Zabbix и бэкапов — отдельные ограниченные группы
5. Firewall input: accept established,related → drop invalid → accept из address-list MGMT → drop all: политика default deny

РЕЗУЛЬТАТ

Снаружи роутер отвечает только на WireGuard-порт: брутфорс Winbox/SSH и эксплуатация уязвимостей сервисов управления отсекаются до появления патча. Любой вход в конфигурацию — персональный, виден в логах по имени инженера.

КЛЮЧЕВОЙ НЮАНС

Смена порта Winbox — не защита: сканеры находят сервис по отпечатку ответа. Работает только связка address-list + VPN; в разделе «Securing your router» документации MikroTik это прямое требование, а не пожелан…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Сегментация: bridge VLAN filtering + межсегментный firewall

Что настраиваем

Офис до 50 PM: рабочие станции, 1С и финансы, гостевой Wi-Fi, камеры и IoT — на одном роутере, без дополнительных лицензий

Как мы это делаем

1. Один bridge с vlan-filtering=yes; таблица /interface bridge vlan: tagged — транк к коммутатору и точкам доступа, untagged+pvid — на access-портах
2. На access-портах frame-types=admit-only-untagged-and-priority-tagged — отсекаем VLAN-hopping тегированными кадрами
3. 4 сегмента: VLAN10 офис, VLAN20 1С/финансы, VLAN30 гости, VLAN40 IoT; каждому — свой /ip address, DHCP-сервер и DNS
4. Forward между VLAN — default deny: офис→1С только по портам кластера 1С (1541, 1560-1591) и печати; гости и IoT — только в интернет
5. Management-VLAN 99: Winbox/SSH слушают только в нём, попадание — через WireGuard либо физический порт в серверной

РЕЗУЛЬТАТ

Инцидент остаётся в своём сегменте: шифровальщик с рабочей станции не дотягивается до сервера 1С, уязвимая камера не сканирует офисную сеть, гостевой ноутбук вообще не видит инфраструктуру. Диагностика ускоряется — трафик считается per-VLAN.

КЛЮЧЕВОЙ НЮАНС

vlan-filtering включаем только после заполнения таблицы VLAN и добавления management-VLAN на сам bridge — иначе локаут. Перед внедрением проверяем по докам поддержку hw-offload у конкретной модели, чтобы не пр…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Удалёнка на WireGuard + перевод в регулярную эксплуатацию

Что настраиваем

VPN для сотрудников и филиалов + обвязка эксплуатации: Zabbix, удалённый syslog, ночные бэкапы конфигурации

Как мы это делаем

1. /interface wireguard: выделенный listen-port, на input — единственный accept udp с WAN; каждому пиру allowed-address /32 из адресного плана VPN
2. Филиалы — site-to-site WireGuard, маршруты через allowed-address; L2TP/IPsec оставляем только там, где клиента поставить нельзя
3. Scheduler 03:00: /export show-sensitive + /system backup save, выгрузка по SFTP на наш бэкап-сервер; конфиги — в git, любой diff правки виден
4. /system logging action=remote на syslog-сервер: topics info, account, critical, firewall — локальный буфер роутера теряется при ребуте
5. SNMPv3 (authPriv) в Zabbix: CPU, память, температура, трафик per-VLAN, доступность WG-пиров; алерты — в Telegram дежурному инженеру

РЕЗУЛЬТАТ

Удалённые сотрудники подключаются за минуты по конфигу/QR, филиалы связаны без проброса RDP наружу. Роутер перестаёт быть чёрным ящиком: любая правка конфигурации видна в git-diff, деградация или недоступность ловится мониторингом до звонка клиента.

КЛЮЧЕВОЙ НЮАНС

Бинарный .backup привязан к модели и не встаёт на другое железо — восстановление на замену возможно только из /export. Храним оба артефакта и раз в квартал проверяем восстановление на тестовом устройстве.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Обновили RouterOS, забыли firmware**
  Пакеты ставятся, а routerboard firmware остаётся старой. После апгрейда всегда выполняем /system routerboard upgrade и контролируемый reboot

- ✕ **«Спрятали» Winbox сменой порта**
  Сканеры находят сервис по отпечатку ответа на любом порту. Закрываем только address-list на /ip service плюс доступ через WireGuard

- ✕ **Fasttrack раньше правил фильтрации**
  Правило fasttrack-connection уводит трафик мимо firewall и queues. Ставим его только для established,related и после защитных правил input/forward

- ✕ **NAT-пробросы открыты всему миру**
  dst-nat на RDP/камеры без ограничений — готовая точка входа. Каждый проброс — только с src-address-list доверенных IP или целиком за VPN

- ✕ **MAC-доступ жив на всех портах**
  mac-winbox и mac-telnet по умолчанию доступны из LAN: любой в розетке имеет канал к роутеру. Ставим allowed-interface-list=none

- ✕ **Открытый DNS-резолвер наружу**
  allow-remote-requests=yes без drop udp/53 на input с WAN делает роутер участником DNS-amplification. Закрываем input, оставляем резолв только LAN

- ✕ **Бэкап только в формате .backup**
  Бинарный backup не восстанавливается на другую модель. Ночью снимаем и .backup, и текстовый /export — второй пригоден для переноса и diff

- ✕ **Одна учётка admin на всех**
  Общий пароль нельзя отозвать при смене подрядчика и нечего искать в логах. Именованные учётки по ролям, admin удаляем, входы пишем в syslog

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- RouterOS на актуальной long-term 7.21.x + routerboard firmware, план обновлений
- Winbox/SSH только из LAN/VPN; telnet, ftp, www, api, socks, upnp — отключены
- Firewall input по default deny: established/related, drop invalid, drop all
- Именованные учётки с паролями 16+, заводской admin удалён

НОРМАЛЬНО

- Сегментация bridge vlan-filtering: офис / 1С-финансы / гости / IoT
- WireGuard для сотрудников и филиалов вместо PPTP и голого L2TP
- Ночной /export + /system backup по SFTP на внешний сервер, глубина 30 дней
- Удалённый syslog и SNMPv3-мониторинг в Zabbix с алертами

ХОРОШО

- Management-VLAN + address-list на сервисы, SSH только по ключам
- Конфигурации в git: diff каждой правки, алерт на изменение вне регламента
- Пороговые алерты в Telegram: CPU, память, падение VPN-пиров, шторм трафика
- Регламент патчей: обкатка на пилотном роутере, затем парк за 2 недели

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Обновлена ли RouterOS до актуальной long-term-ветки 7.21.x вместе с routerboard firmware?
- [ ] Доступен ли Winbox или SSH с внешнего IP роутера? (правильный ответ — нет)
- [ ] Удалена ли заводская учётка admin и заведены ли именованные учётки по ролям?
- [ ] Отключены ли socks, web-proxy, upnp, cloud DDNS, bandwidth-server и MAC-доступ на LAN?
- [ ] Стоит ли на input-цепочке firewall политика default deny с drop invalid?
- [ ] Разделена ли сеть на VLAN и закрыт ли forward между сегментами по умолчанию?
- [ ] Ходит ли удалёнка и связь филиалов через WireGuard, а не через пробросы портов?
- [ ] Снимается ли ежесуточно /export и .backup на внешний сервер и проверялось ли восстановление?
- [ ] Уходят ли логи роутера на внешний syslog и стоит ли роутер в мониторинге с алертами?
- [ ] Есть ли письменный отчёт подрядчика по каждому пункту hardening?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит MikroTik с проверкой признаков компрометации: учётки, шедулер, прокси, NAT, DNS — письменный отчёт
- Hardening под ключ по нашему шаблону ITF-MTK-BASE: сервисы, firewall, учётки, обновление до long-term
- Сегментация офиса на VLAN и WireGuard для удалёнки и филиалов без доп. лицензий
- Абонентское обслуживание: мониторинг в Zabbix, ночные бэкапы, патчи, реагирование на инциденты
- Очистка скомпрометированного роутера с восстановлением чистой конфигурации из бэкапа

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Securing your router — RouterOS knowledge base (help.mikrotik.com — 7.x)

02 Bridging and Switching — Bridge VLAN Filtering (help.mikrotik.com — 7.x)

03 WireGuard — Virtual Private Networks (help.mikrotik.com — 7.x)

04 IP Services, User management (help.mikrotik.com — 7.x)

05 RouterOS changelog, ветка long-term (mikrotik.com — 7.21.5)

06 Шаблон ITfresh ITF-MTK-BASE (hardening + VLAN + WG) (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.