Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

802.1X + RADIUS: закрываем порты сети на замок

Как мы строим контроль доступа: FreeRADIUS 3.2 + AD, динамические VLAN, MAB и переход на EAP-T...

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Пока порты коммутаторов открыты, любой принесённый ноутбук, «шпионский» мини-роутер или подобранный пароль Wi-Fi даёт полный доступ во внутреннюю сеть — к 1С, файловым шарам и бухгалтерии. Мы внедряем 802.1X: порт не пропускает ничего, кроме EAP, пока RADIUS не подтвердит учётку в AD, а устройство не окажется в своём VLAN со своими правами.

Почему это важно бизнесу

- Розетка в переговорке = доступ к серверу 1С: без 802.1X периметр кончается на входной двери
- Уволенный сотрудник с сохранённым паролем Wi-Fi продолжает видеть сеть компании
- Журнал RADIUS-аккаунтинга отвечает аудитору, кто и когда был в сети — требование при разборе инцидентов
- Гости и подрядчики автоматически падают в изолированный VLAN, а не в общую сеть с бухгалтерией
- Внедрение — это настройка имеющихся коммутаторов и одной VM, без закупки железа

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

3.2.5

FreeRADIUS из репозитория Ubuntu 24.04 (ветка 3.2.x); конфиги пакета — в /etc/freeradius/3.0/

packages.ubuntu.com / freeradius.org, 2026

TLS 1.2

tls_min_version в mods-enabled/eap — отсекаем клиентов со старыми стеками ещё на рукопожатии

наш стандарт + доки FreeRADIUS

1812/1813

UDP-порты auth/acct: открываем их от NAS к обоим RADIUS в ACL, всё остальное к серверу закрыто

RFC 2865/2866

10 с

dot1x timeout tx-period на Cisco: втрое быстрее дефолтных 30 с, DHCP успевает до таймаута клие...

наш стандарт для Catalyst

x2

RADIUS-серверов в aaa group: второй — на другом гипервизоре, иначе падение VM кладёт всю сеть

наш стандарт

2-4 нед

Держим порты в monitor mode (authentication open): собираем отказы в логах до перевода в closed

наша методика раскатки

РЕАЛИЗАЦИЯ 1 ИЗ 3

Ядро аутентификации: FreeRADIUS 3.2 + Active Directory

Что настраиваем

VM Ubuntu 24.04 (2 vCPU/4 ГБ) в серверном VLAN; охват — все коммутаторы и точки доступа площадки

Как мы это делаем

1. Ставим freeradius, freeradius-utils, samba, winbind, krb5-user; сервер вводим в домен net ads join, проверяем wbinfo -t
2. В mods-enabled/mschap прописываем вызов ntlm_auth с --request-nt-key; пользователя freerad добавляем в группу winbindd_priv
3. В clients.conf заводим каждый NAS отдельной записью с индивидуальным shared secret из генератора (20+ символов), не одной подсетью
4. EAP: default_eap_type = peap, внутри mschapv2; серверный сертификат — от внутреннего CA, не самоподписанный из certs/
5. Прогоняем eapol_test с профилем PEAP/MSCHAPv2 и radtest -t mschap до подключения первого коммутатора

РЕЗУЛЬТАТ

Одна точка принятия решений: блокировка учётки в AD мгновенно отрезает человека от LAN и Wi-Fi. Все Access-Accept/Reject пишутся в detail-лог с привязкой к порту и MAC — инцидент разбирается по журналу за минуты.

КЛЮЧЕВОЙ НЮАНС

Проверяем связку ntlm_auth → winbind ДО EAP: 90% проблем внедрения — это права на winbindd_privileged и протухший machine account, а не сам RADIUS.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Порты доступа: Cisco Catalyst + MikroTik, раскатка без простоя

Что настраиваем

Кампусные коммутаторы (IOS) и RouterOS 7 в филиалах; принтеры, телефоны и кассы — через MAB

Как мы это делаем

1. Cisco: aaa new-model, dot1x system-auth-control, две записи radius server в aaa group с deadtime и probe-тестером доступности
2. Порты: authentication port-control auto + authentication open (monitor mode) — аутентификация идёт, но трафик пока не режется
3. Устройства без суппликанта: mab + authentication order mab dot1x, MAC-адреса заводим в RADIUS с VLAN принтеров
4. Отказоустойчивость: authentication event server dead action authorize vlan — при смерти обоих RADIUS порты не «чернеют»
5. MikroTik: /radius add service=dot1x, /interface dot1x server на access-порты; после 2-4 недель чистых логов снимаем open

РЕЗУЛЬТАТ

Включение прошло без единой заявки «пропала сеть»: monitor mode заранее показал все проблемные устройства. VLAN назначается по группе AD через Tunnel-Private-Group-Id — переезд сотрудника между кабинетами больше не требует перенастройки порта.

КЛЮЧЕВОЙ НЮАНС

MAB-инвентаризацию делаем до включения: снимаем таблицы MAC с коммутаторов и сверяем с учётом. Каждое «забытое» устройство в closed mode — это звонок в поддержку в 9:00 понедельника.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Ужесточение: EAP-TLS на сертификатах через AD CS

Что настраиваем

Домены с Windows 11: шаблоны AD CS + автоэнролмент, суппликант — политикой на все PC

Как мы это делаем

1. В AD CS публикуем шаблоны Workstation Authentication (клиенты) и RAS and IAS Server (RADIUS), включаем autoenrollment через GPO
2. CA-цепочку кладём в ca_file FreeRADIUS; в eap переключаем default_eap_type = tls, PEAP оставляем как fallback на время миграции
3. GPO Wired Network (IEEE 802.3) Policies: служба Wired AutoConfig (dot3svc) в Automatic, метод — Smart Card or other certificate
4. В профиле клиента жёстко включаем валидацию серверного сертификата и пиним имя RADIUS-сервера и корневой CA
5. Отзыв сертификата в CA + блокировка в AD = устройство вне сети при следующей реаутентификации

РЕЗУЛЬТАТ

Уходим от паролей в сети совсем: угнанный пароль пользователя больше не даёт подключить чужое устройство. Совместимо с Credential Guard в Windows 11 — PEAP/MSCHAPv2 там доживает последние релизы.

КЛЮЧЕВОЙ НЮАНС

По докам Microsoft Credential Guard (включён по умолчанию с Win11 22H2 Enterprise) блокирует MSCHAPv2-SSO — миграцию на EAP-TLS закладываем в проект сразу, а не «когда-нибудь потом».

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Closed mode сразу на всех портах**
  Один недоучтённый принтер — и этаж без сети. Мы держим authentication open 2-4 недели и переводим в closed по чистым логам, попортово.

- ✕ **Клиент не проверяет сертификат RADIUS**
  Без валидации серверного серта суппликант отдаст хэш пароля любому подставному AP. В GPO жёстко включаем проверку CA и имени сервера.

- ✕ **Credential Guard ломает PEAP-MSCHAPv2**
  Win11 22H2+ Enterprise блокирует MSCHAPv2-SSO по умолчанию. Диагноз — лог Microsoft-Windows-NTLM/Operational; лечение — миграция на EAP-TLS.

- ✕ **Один RADIUS-сервер на всё**
  Падение VM = вся сеть без авторизации. Ставим второй сервер на другом хосте и critical VLAN: server dead action authorize на портах.

- ✕ **Нет прав freerad на winbind**
  ntlm_auth молча возвращает отказ, пока freerad не в группе winbindd_priv и нет chgrp на winbindd_privileged. Проверяем до запуска EAP.

- ✕ **Один shared secret на всю сеть**
  Подсеть в clients.conf одним секретом — компрометация любого NAS раскрывает всё. Секрет 20+ символов индивидуально на устройство.

- ✕ **MAB по всей базе MAC «оптом»**
  MAC подделывается за секунду. MAB-устройства кладём в отдельный VLAN с ACL только до их сервисов (печать, кассовый шлюз), не в общий.

- ✕ **Тайм-ауты по умолчанию**
  tx-period 30 с x3 попытки — DHCP-клиент отваливается раньше конца аутентификации. Ставим tx-period 10 и проверяем выдачу адреса.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- FreeRADIUS 3.2.x + ntlm_auth к AD, PEAP/MSCHAPv2, tls_min_version 1.2
- 802.1X на портах пользователей в monitor mode, гостевой VLAN изолирован
- Индивидуальные shared secret в clients.conf, ACL на UDP 1812/1813
- MAB для принтеров/телефонов в отдельном VLAN с узким ACL

НОРМАЛЬНО

- Второй RADIUS на другом гипервизоре + critical VLAN (server dead action)
- Closed mode на всех access-портах, динамический VLAN по группам AD
- RADIUS-accounting в БД, алерты на всплеск Access-Reject в мониторинг
- Супликант и профили — через GPO (Wired AutoConfig, WLAN AutoConfig)

ХОРОШО

- EAP-TLS: AD CS, автоэнролмент шаблонов, отзыв сертификата = отсечение от сети
- Пиннинг CA и имени сервера в клиентских профилях, запрет legacy-EAP
- Порт-ACL из RADIUS (dACL) поверх VLAN — права точнее, чем сегмент
- Регулярный аудит MAB-базы: сверка MAC с инвентаризацией раз в квартал

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Порт в свободной переговорке пускает EAP-пакеты и ничего больше (closed mode включён)?
- [ ] Блокировка учётки в AD отрезает человека и от кабеля, и от Wi-Fi без ручных действий?
- [ ] RADIUS-серверов два, и они на разных гипервизорах/площадках?
- [ ] На портах настроен critical VLAN на случай смерти обоих RADIUS (server dead action)?
- [ ] Клиентские профили проверяют сертификат RADIUS-сервера и имя CA (не «не проверять»)?
- [ ] Все MAB-устройства есть в инвентаризации и заперты в своём VLAN с ACL?
- [ ] Аккаунтинг пишется и хранится — можно сказать, кто был на порту Gi0/17 во вторник?
- [ ] Есть план миграции с PEAP/MSCHAPv2 на EAP-TLS с учётом Credential Guard в Windows 11?
- [ ] Shared secret уникальны для каждого NAS и длиннее 20 символов?
- [ ] Пилот проходил через monitor mode с разбором логов, а не включением «в бой»?

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 сети и инвентаризация устройств без суппликанта — карта портов и план MAB до включения
- Разворачиваем отказоустойчивую пару FreeRADIUS 3.2 с интеграцией в ваш AD и динамическими VLAN
- Настраиваем 802.1X на Cisco/MikroTik и суппликанты через GPO — раскатка без простоя, с monitor mode
- Строим PKI на AD CS и переводим сеть на EAP-TLS: автоэнролмент, отзыв, мониторинг сроков сертификатов
- Сопровождаем: алерты на Access-Reject, контроль MAB-базы, разбор инцидентов по RADIUS-логам

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 FreeRADIUS Documentation: EAP, mods (mschap, ldap), clients.conf (freeradius.org — 3.2.x)

02 Credential Guard: considerations and known issues (MSCHAPv2) (learn.microsoft.com — 2026)

03 Extensible Authentication Protocol (EAP) for network access (learn.microsoft.com — 2026)

04 Cisco IOS: Configuring IEEE 802.1X Port-Based Authentication, MAB (cisco.com — IOS-XE 17)

05 MikroTik RouterOS 7: Dot1X (server/client), RADIUS (help.mikrotik.com — 7.x)

06 Samba Wiki: Domain Member, winbind и ntlm_auth (wiki.samba.org — 4.x)

07 Шаблон ITfresh: раскатка 802.1X (monitor→closed, критерии перехода) (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.