Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

VLAN в офисе на 50–150 ПК: зачем сегментировать сеть и как это д…

Инженерная методология ITfresh: проектирование VLAN, ACL и миграция плоской сети без простоя о…

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В типичном офисе на 50–150 рабочих мест всё оборудование — компьютеры, серверы, бухгалтерия, гостевой Wi-Fi, камеры и принтеры — подключено в одну «плоскую» сеть: один L2-домен, где любое устройство видит любое другое. Одно заражённое письмо — и шифровальщик по SMB за часы добирается до 1С, файлового сервера и резервных копий. Бизнес узнаёт о проблеме, когда терять уже нечего.

Почему это важно бизнесу

- Шифровальщик в плоской сети распространяется по TCP 445 (SMB) и шифрует всё сразу: файлы, базу 1С и доступные по сети бэкапы
- Одна петля или сбойная сетевая карта в общем L2-домене на 150 устройств вызывает broadcast-шторм и кладёт весь офис разом
- Гостевой Wi-Fi в одном сегменте с персональными данными — риск по 152-ФЗ: с 30.05.2025 штраф за утечку от 3 млн ₽ (ч. 12 ст. 13.11 КоАП)
- Проект сегментации — это 2–3 ночных окна работ; восстановление после инцидента — недели простоя и на порядок дороже

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

1–4094

рабочий диапазон VLAN ID по IEEE 802.1Q (12-битное поле VID, значения 0 и 4095 зарезервированы...

IEEE 802.1Q-2022, формат тега VLAN

6–8

VLAN достаточно офису на 50–150 ПК: рабочие места, бухгалтерия, серверы, бэкапы, гости, IoT/ка...

методология сегментации ITfresh

/24

на сегмент по схеме 10.0.<VLAN>.0/24 — номер VLAN читается прямо из IP-адреса, диагностика и А...

адресный план ITfresh

TCP 445

SMB — главный канал распространения шифровальщика между сегментами; в нашей матрице ACL закрыт...

матрица межсегментных ACL ITfresh

2–3

ночных окна по 2–4 часа занимает миграция офиса на 50–150 ПК с плоской сети на VLAN — без днев...

план миграции ITfresh

3–5 млн ₽

штраф за утечку ПДн от 1 000 до 10 000 субъектов; повторная утечка — 1–3% годовой выручки, но...

КоАП РФ, ст. 13.11 (ред. 420-ФЗ, с 30.05.2025)

РЕАЛИЗАЦИЯ 1 ИЗ 3

Офис на 70 человек: одно письмо — минус вся сеть

Что настраиваем

Торгово-производственная компания, около 70 рабочих мест (обезличено)

Как мы это делаем

1. Сотрудник бухгалтерии открывает вложение «Акт сверки» от якобы знакомого контрагента
2. Шифровальщик сканирует сеть по TCP 445 и за часы добирается до 1С, файлового сервера и NAS с бэкапами — всё в одном L2-домене
3. Работа компании остановлена; резервные копии зашифрованы вместе с рабочими данными
4. Восстановление с нуля и неделя простоя обходятся дороже миллиона рублей

РЕЗУЛЬТАТ

Единственная точка входа — один ПК рядового сотрудника — приводит к потере всех данных компании, включая резервные копии, находившиеся в той же сети. Неделя простоя и расходы на восстановление, сопоставимые с годовым ИТ-бюджетом.

КЛЮЧЕВОЙ НЮАНС

Для компании до 100 рабочих мест минимальная сегментация (рабочие места / серверы / бэкапы / гости) — это разница между заражением одного отдела и потерей всего бизнеса.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Офис на 120 мест: камеры видеонаблюдения как плацдарм

Что настраиваем

Компания сферы услуг, около 120 рабочих мест, два этажа офиса (обезличено)

Как мы это делаем

1. Наш аудит: 32 IP-камеры и видеорегистратор включены в общий L2-домен с серверами и рабочими местами
2. На камерах — прошивка пятилетней давности с уязвимым web-интерфейсом и неизменённым паролем подрядчика
3. Контрольный скан с камеры показал: доступны SMB-шары файлового сервера и RDP серверов 1С — готовый маршрут вглубь сети
4. Камеры и СКУД вынесены в отдельный VLAN с ACL «камера → только видеорегистратор (RTSP 554)»; подрядчику — VPN до одного хоста

РЕЗУЛЬТАТ

До сегментации компрометация любой из 32 камер давала прямой доступ ко всем серверам компании. После выноса в изолированный VLAN поверхность атаки через IoT сведена к одному разрешённому потоку на видеорегистратор.

КЛЮЧЕВОЙ НЮАНС

Камеры, СКУД и «умные» устройства не обновляются годами и не защищаются антивирусом. Их место — отдельный сегмент с ACL на единственный разрешённый поток, а не общая сеть с серверами.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Офис на 130 мест: шифровальщик остановлен на границе VLAN

Что настраиваем

Инжиниринговая компания, около 130 рабочих мест (обезличено)

Как мы это делаем

1. За полгода до инцидента сеть сегментирована: рабочие места, серверы, бэкапы и гости разведены по VLAN, между ними ACL «deny by default»
2. Сотрудник запускает вложение из письма; шифровальщик шифрует локальный диск и начинает сканировать сеть по TCP 445
3. ACL на L3-коммутаторе блокирует SMB из VLAN рабочих мест в серверный сегмент; всплеск denied-пакетов виден в мониторинге в течение минут
4. Итог: переустановка нескольких ПК одного отдела; 1С, файловый сервер и резервные копии не затронуты

РЕЗУЛЬТАТ

Тот же сценарий входа, что и в первом кейсе, но зона поражения — один отдел вместо всей компании. Простой — часы на переустановку рабочих станций, а не неделя восстановления инфраструктуры с нуля.

КЛЮЧЕВОЙ НЮАНС

Периметр рано или поздно пробивают. Исход решает внутренняя архитектура: запрещающие ACL между сегментами лишают атакующего свободы перемещения и дают время на обнаружение по denied-трафику.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Плоская сеть «как исторически сложилось»**
  Один L2-домен на все 150 устройств: любое заражение распространяется по SMB/RDP на всю компанию за часы, а broadcast-шторм кладёт офис целиком.
- ✕ **Бэкапы и NAS в общей сети**
  Копия, доступная по SMB с обычного рабочего места, будет зашифрована вместе с оригиналом. Бэкап-сегмент открываем только серверу резервного копирован…
- ✕ **Гостевой Wi-Fi без изоляции**
  Любой посетитель из переговорки может сканировать рабочую сеть — это и дыра в защите, и риск утечки ПДн по 152-ФЗ.
- ✕ **Камеры и IoT рядом с рабочими местами**
  Уязвимые прошивки камер, СКУД и «умных» устройств — готовый плацдарм: с них видны шары и RDP серверов, если нет ACL.
- ✕ **VLAN нарезаны, а фильтрации между ними нет**
  Сегментация без ACL — формальность: inter-VLAN routing свободно пропускает любой трафик, включая SMB, между сегментами.
- ✕ **Заводские настройки коммутаторов**
  Native VLAN 1, автосогласование транков (DTP) и управление из любого порта открывают VLAN hopping и сводят эффект сегментации к нулю.
- ✕ **Нет схемы сети и адресного плана**
  Никто не знает, что и куда подключено; изменения делаются наугад, а расследование инцидента по логам без документации невозможно.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Гостевой Wi-Fi — в отдельный VLAN и SSID: только интернет, client isolation включена…
- NAS с бэкапами — в изолированный VLAN: доступ только серверу резервного копирования;…
- Сменить дефолтные пароли коммутаторов, отключить Telnet и web-доступ из пользователь…

НОРМАЛЬНО

- Нарезать 6–8 VLAN (PM, бухгалтерия, серверы, бэкапы, гости, IoT, management) с плано…
- ACL «deny by default» между сегментами; разрешения точечно: например, PM → серверы 1…
- Management-VLAN для коммутаторов и точек доступа: вход только из подсети администрат…
- Задокументировать адресный план, схему L2/L3 и матрицу ACL; любые изменения — только…

ХОРОШО

- 802.1X на портах доступа с RADIUS (Windows Server NPS, EAP-TLS/PEAP): без аутентифик…
- DHCP snooping и Dynamic ARP Inspection в пользовательских VLAN, BPDU Guard и nonegot…
- NetFlow/sFlow с межсегментных стыков в коллектор; алерты на denied-трафик ACL в стор…
- Раз в год проверять сегментацию сканом (nmap) из гостевого и IoT VLAN: снаружи сегме…

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Гость с ноутбуком в переговорке гарантированно не «видит» ваши серверы и рабочие компьютеры?
- [ ] Бухгалтерия с банк-клиентом отделена от остальных рабочих мест на уровне сети?
- [ ] Резервные копии недоступны по сети с обычного рабочего места даже под учёткой администратора?
- [ ] Камеры, принтеры и «умные» устройства вынесены в отдельный сегмент с запретом трафика к серверам?
- [ ] Между сегментами действует «запрещено всё, кроме разрешённого», а не свободная маршрутизация?
- [ ] Управление коммутаторами и Wi-Fi доступно только из management-VLAN через VPN, а не из интернета?
- [ ] У вас есть актуальная схема сети, адресный план и матрица ACL, а не только «в голове у админа»?
- [ ] Вы знаете, сколько часов простоя переживёт бизнес, если вся сеть ляжет разом?

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: обследуем топологию, найдём плоские зоны, риски и нарушения 152-ФЗ за 1–2 дня
- Проект сегментации под ключ: схема VLAN, ACL, гостевой Wi-Fi, миграция по ночам без простоя офиса
- Сопровождение: мониторинг межсегментного трафика, актуальная документация, обновления оборудования

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 IEEE 802.1Q-2022 — Bridges and Bridged Networks (формат тега VLAN, поле VI... (standards.ieee.org — 2022)

02 Cisco IOS XE 17.x — VLAN Configuration Guide (Catalyst 9300) (cisco.com — 2025)

03 Cisco IOS XE 17.x — Security Configuration Guide: DHCP Snooping, Dynamic A... (cisco.com — 2025)

04 MikroTik RouterOS 7 — Bridge VLAN Filtering (vlan-filtering, tagged/untagg... (mikrotik.com — 2025)

05 Microsoft — Network Policy Server (NPS): развёртывание 802.1X для проводны... (learn.microsoft.com — 2025)

06 КоАП РФ, ст. 13.11 в редакции 420-ФЗ от 30.11.2024 (ответственность за уте... (pravo.gov.ru — 2025)

07 ITfresh — внутренний стандарт: адресный план, матрица межсегментных ACL, п... (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.