Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Cisco ACL: как мы закрываем доступ к серверам в офисной сети

Сегментация VLAN 10/20/30/99 и расширенные ACL на IOS XE 17.x: от матрицы доступов до TCAM

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В офисах до 50 РМ сеть обычно «плоская»: гостевой Wi-Fi, принтеры и любая станция видят сервер 1С напрямую. Мы делим сеть на VLAN и расширенными ACL на Cisco IOS XE закрываем серверный сегмент по матрице доступов: кто, откуда, на какой порт. Без этого заражённый ноутбук или гость получает SMB/RDP до серверов — утечка базы и шифровальщик на всём парке.

Почему это важно бизнесу

- Утечка базы 1С — уход клиентов к конкурентам и риски по 152-ФЗ; ACL отрезает сам сетевой путь до сервера, а не только пароль
- Шифровальщик в плоской сети кладёт все машины за ночь; блок SMB/RDP между сегментами ограничивает ущерб одним VLAN
- Простой сервера 1С на день — стоп продаж и бухгалтерии; сегментация снижает риск на уже купленном железе, без новых лицензий
- ACL исполняется в TCAM коммутатора — защита не замедляет сеть и не требует агентов на каждом ПК
- Матрица доступов делает сеть проверяемой: любой аудит или смена админа проходят по документу, а не по памяти

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

17.x

ветка IOS XE в наших конфигах: именованные ACL, sequence numbers, object-groups, time-range

Cisco IOS XE 17.x Sec Guide

шаг 10

шаг sequence numbers: правило вставляем в середину списка без пересборки (resequence 10 10)

IOS XE 17.x: Seq Numbering

5 мин

интервал кэша ACL-логов: deny в syslog идёт батчами; ранний сброс — порогом log-update thresho…

IOS XE 17.x: ACL Logging

1 in/1 out

на интерфейс — один ACL на направление, поэтому правила сегмента собираем в один список

архитектура Cisco IOS

1541–1591

TCP-порты кластера 1С: 1541 (rmngr) и 1560–1591 (rphost) — открыты только бухгалтерии и термин…

наш стандарт

4 VLAN

минимум сегментации: 10 users, 20 servers, 30 mgmt, 99 guest; ACL на SVI серверов и гостей

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Серверный VLAN: ACL PROTECT-1C на SVI

Что настраиваем

Catalyst 9300 / ISR 4000 (IOS XE 17.x), SVI Vlan20 серверного сегмента: 1С, файловый сервер, терминалка

Как мы это делаем

1. Снимаем матрицу доступов «кто→куда→порт→зачем»: бухгалтерия 192.168.10.0/24 → 1С TCP 1541 (rmngr) и 1560–1591 (rphost); IT из VLAN 30 → RDP/SSH; остальным — deny
2. Собираем object-group network OG-BUH, OG-ADMINS и object-group service SVC-1C — состав групп правится без переписывания ACE
3. ip access-list extended PROTECT-1C: permit-строки по матрице, затем deny ip any host 192.168.20.10 log, в конце permit ip any any для прочих серверов
4. Вешаем ip access-group PROTECT-1C out на interface Vlan20 — фильтруем трафик, идущий К серверам; in на SVI матчил бы трафик ОТ них. Прогоняем тесты с эталонных маши…
5. Сверяем show ip access-lists PROTECT-1C: счётчики matches по каждому ACE до и после теста, нулевые permit-строки разбираем отдельно

РЕЗУЛЬТАТ

Сервер 1С принимает соединения только из бухгалтерии, с терминального сервера и из management-VLAN. Заражённая машина из пользовательского сегмента не дотягивается даже до порта: deny отрабатывает в TCAM коммутатора, а источник попытки виден в syslog.

КЛЮЧЕВОЙ НЮАНС

ACL в IOS не stateful: обратный TCP-трафик сам не разрешится. Для ответов на сессии, инициированные изнутри, используем ключ established — поведение сверяем по IP Access List Overview в доке IOS XE 17.x.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Гостевой Wi-Fi и management-плоскость

Что настраиваем

SVI Vlan99 (гости) и line vty 0 15 на всех маршрутизаторах и L3-коммутаторах клиента

Как мы это делаем

1. GUEST-FILTER: первой строкой permit udp any host <DNS> eq 53 (иначе внутренний DNS попадёт под deny), затем deny ip any в 10/8, 172.16/12, 192.168/16 с log, в конце...
2. ip access-group GUEST-FILTER in на Vlan99; там, где офис работает по графику, добавляем time-range WORKING-HOURS (periodic weekdays 9:00 to 21:00)
3. Standard ACL VTY-ALLOW: permit management-подсети и IP нашего шлюза, deny any log; line vty 0 15 → access-class VTY-ALLOW in + transport input ssh
4. Логи deny шлём на внешний syslog; батч уходит раньше 5-минутного кэша, когда набран порог ip access-list log-update threshold (порог задаётся в пакетах)

РЕЗУЛЬТАТ

Гость видит только интернет: ни серверов, ни принтеров, ни веб-интерфейса роутера. CLI оборудования доступен только из management-VLAN и только по SSH — подбор пароля из LAN невозможен, а каждая попытка фиксируется в syslog с адресом источника.

КЛЮЧЕВОЙ НЮАНС

access-class на vty закрывает управление сразу через все интерфейсы, а интерфейсный ACL пришлось бы дублировать на каждом SVI — поэтому защиту management начинаем именно с VTY-ACL и SSH.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Эксплуатация: правки, отладка, откат

Что настраиваем

Регламент изменений ACL на всём парке клиента: вставка правил, контроль счётчиков, безопасная удалённая правка

Как мы это делаем

1. Перед правкой: show run | section access-list в бэкап и reload in 10 на удалённом узле — при ошибочном deny узел сам вернётся на сохранённый конфиг
2. Новые ACE вставляем по sequence numbers, место готовим командой ip access-list resequence NAME 10 10; после reload номера возвращаются к шагу 10 — итог фиксируем в…
3. Тест: clear ip access-list counters NAME, генерируем эталонный трафик с проверочной машины, смотрим matches в show ip access-lists NAME
4. log оставляем только на deny-строках: матч с log уходит с TCAM на CPU, поэтому массовые permit никогда не логируем
5. После проверки — write memory и reload cancel; изменение фиксируем в матрице доступов клиента с датой и причиной

РЕЗУЛЬТАТ

Правки ACL на работающем офисе проходят без окна простоя: ошибочная строка не отрезает нас от узла благодаря reload in, а счётчики matches показывают, работает ли правило, раньше, чем прилетит жалоба пользователей.

КЛЮЧЕВОЙ НЮАНС

Удаление одной строки нумерованного ACL командой no access-list N сносит весь список — это поведение живо и в IOS XE 17.x. Поэтому работаем только именованными списками с sequence numbers и держим бэкап секции…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ Implicit deny в конце

Каждый ACL завершается неявным deny ip any any: забытый permit отрежет весь сегмент. Финальные строки пишем явно и проверяем счётчиками.

✕ Wildcard вместо маски

В ACE используется wildcard: /24 — это 0.0.0.255, а не 255.255.255.0. Перепутанная маска матчит не те сети; считаем wildcard по шаблону, не в уме.

✕ Порядок ACE решает

Список читается сверху вниз до первого совпадения: permit ip any any в начале обнуляет всё ниже. Частные правила всегда выше общих.

✕ Перепутанное in/out на SVI

in на SVI серверного VLAN матчит трафик ОТ серверов, а не к ним — защита «не работает» при верных ACE. Для входящего к серверам трафика ACL вешаем ou…

✕ log на permit-правилах

Матч строки с log обрабатывает CPU в обход TCAM — на потоке это кладёт узел. log оставляем только на deny и на время отладки.

✕ ACL не stateful

Обратный TCP-трафик не разрешается автоматически: добавляем established или явные ответные permit; полноценный stateful — это уже ZBF.

✕ Правка по живому без отката

Ошибочный deny на WAN-узле отрезает удалённый доступ. Перед правкой — reload in 10 и бэкап секции, после проверки — reload cancel.

✕ Второй ACL на направление

На интерфейсе живёт один ACL in и один out: повторный ip access-group молча заменяет прежний. Все правила сегмента держим в одном списке.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Гостевой Wi-Fi в отдельном VLAN, ACL: deny в RFC1918-сети, permit в интернет
- VTY закрыт access-class + transport input ssh на всех управляемых узлах
- Deny-строки с log, syslog уходит на внешний сервер
- Бэкап конфига до и после каждой правки ACL

НОРМАЛЬНО

- 4 VLAN (users/servers/mgmt/guest), серверный SVI закрыт расширенным ACL (out — к сер…
- Именованные ACL с remark, вставка правил по sequence numbers
- SMB (445/139) и RDP (3389) закрыты между пользовательскими сегментами
- Матрица доступов «кто→куда→порт→зачем» в документации клиента

ХОРОШО

- Object-groups для подсетей и сервисов — правки без переписывания ACE
- Time-based ACL для гостевых сегментов, established для обратного трафика
- Регламент правок: reload in, clear counters, контроль matches, reload cancel
- Мониторинг deny-счётчиков и syslog в Zabbix с алертом на всплеск

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Гость из Wi-Fi может открыть веб-интерфейс роутера или шару сервера? Проверяли реальным ноутбуком?
- [ ] Сервер 1С доступен по TCP 1541 и 1560–1591 только из нужных подсетей, а не из всей сети?
- [ ] На line vty стоит access-class и разрешён только SSH (transport input ssh)?
- [ ] SMB (445/139) и RDP (3389) закрыты между пользовательскими сегментами?
- [ ] ACL серверного SVI повешен в нужном направлении (out — к серверам), а не «куда получилось»?
- [ ] У каждого блока ACE есть remark, а у компании — актуальная матрица доступов?
- [ ] Правки ACL идут по sequence numbers с бэкапом секции конфига?
- [ ] Deny-события с log уходят на внешний syslog, и кто-то на них реагирует?
- [ ] Есть регламент отката (reload in / archive) при ошибочной правке удалённого узла?
- [ ] Счётчики matches проверяются после каждой правки, а не «настроили и забыли»?

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: снимаем конфиги и строим фактическую матрицу «кто до чего дотягивается»
- Сегментация офиса на VLAN и внедрение ACL без остановки работы — правки в нерабочие окна
- Шаблоны PROTECT-1C / GUEST-FILTER / VTY-ALLOW под вашу адресацию и приложения
- Syslog + Zabbix-мониторинг deny-счётчиков с алертами в Telegram
- Паспорт сети и регламент изменений ACL для вашего штатного администратора

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 Security and VPN Config Guide, IOS XE 17.x — IP Access List Overview (cisco.com — 17.x)

02 IP Access List Entry Sequence Numbering (IOS XE 17.x) (cisco.com — 17.x)

03 Object Groups for ACLs (IOS XE 17.x) (cisco.com — 17.x)

04 Security Configuration Guide, Catalyst 9300 — IPv4 ACLs (cisco.com — 17.3.x)

05 Understanding Access Control List Logging (Cisco Security Center) (cisco.com — 2024)

06 Шаблон ITfresh: матрица доступов и нейминг ACL для офисов до 50 PM (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.