DECK AUTH

Контроль сессий в NAC. Как?

Хаванкин Максим
mkhavank@deck.lc

Факты о DECK AUTH

- Компания DECK основана в 2014 году
- Кодовая база DECK AUTH развивается с момента основания
- Фундамент продукта
  - Контроль доступа в беспроводных сетях операторского класса
  - Модульная архитектура с возможностями горизонтального масштабирования
- Опыт команды разработки
  - Captive, Location - WiFi/Beacon, PCRF*
- DECK AUTH внесен в реестр отечественного ПО в 2020 году

АТС Смольного
СВЯЗЬ ВРЕМЕН

Location

PCRF

Запись в реестре №6091 от 13.01.2020 произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.01.2020 №4

Класс программного обеспечения по классификатору программного обеспечения, утвержденному приказом от 31.12.2015 № 621

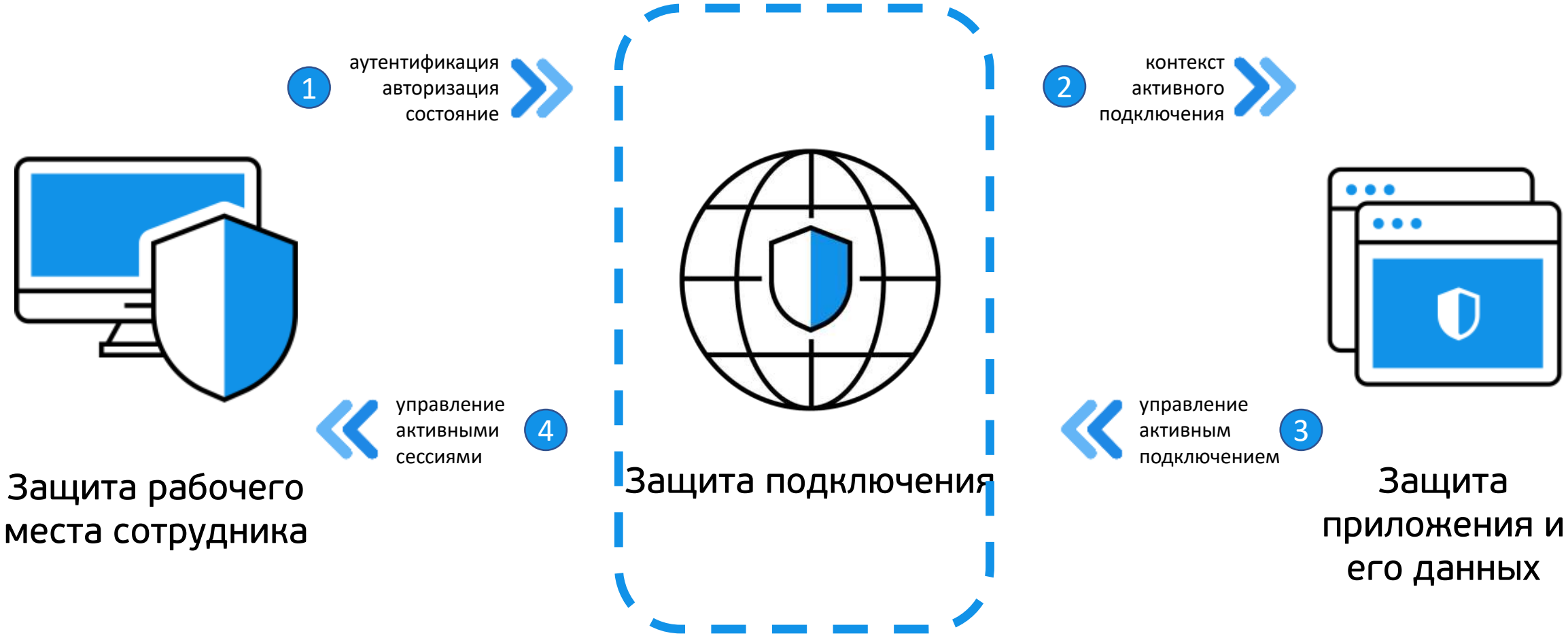
Основной класс:

02.07 Серверное и связующее программное обеспечение

*PCRF - Policy and Charging Rules Function

DECKAUTH

NAC фокусируется на защите подключений

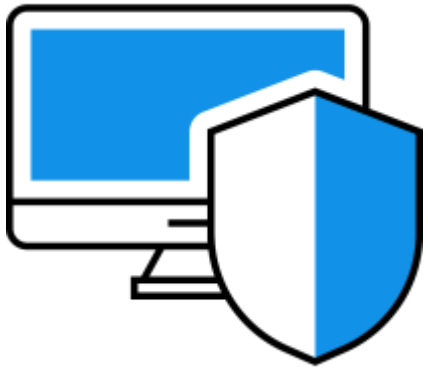


DECKAUTH

Проблема зрелости при выборе NAC

Фокус только на аутентификации и авторизации

1 аутентификация
авторизация
состояние



Защита подключения

2 контекст активного подключения

3 управление активным подключением

Защита приложения и его данных

Фокус только на аутентификации и авторизации

Обмен контекстом, активное управление подключениями, вмешательств в состояние сессий не являются приоритетом

DECKAUTH

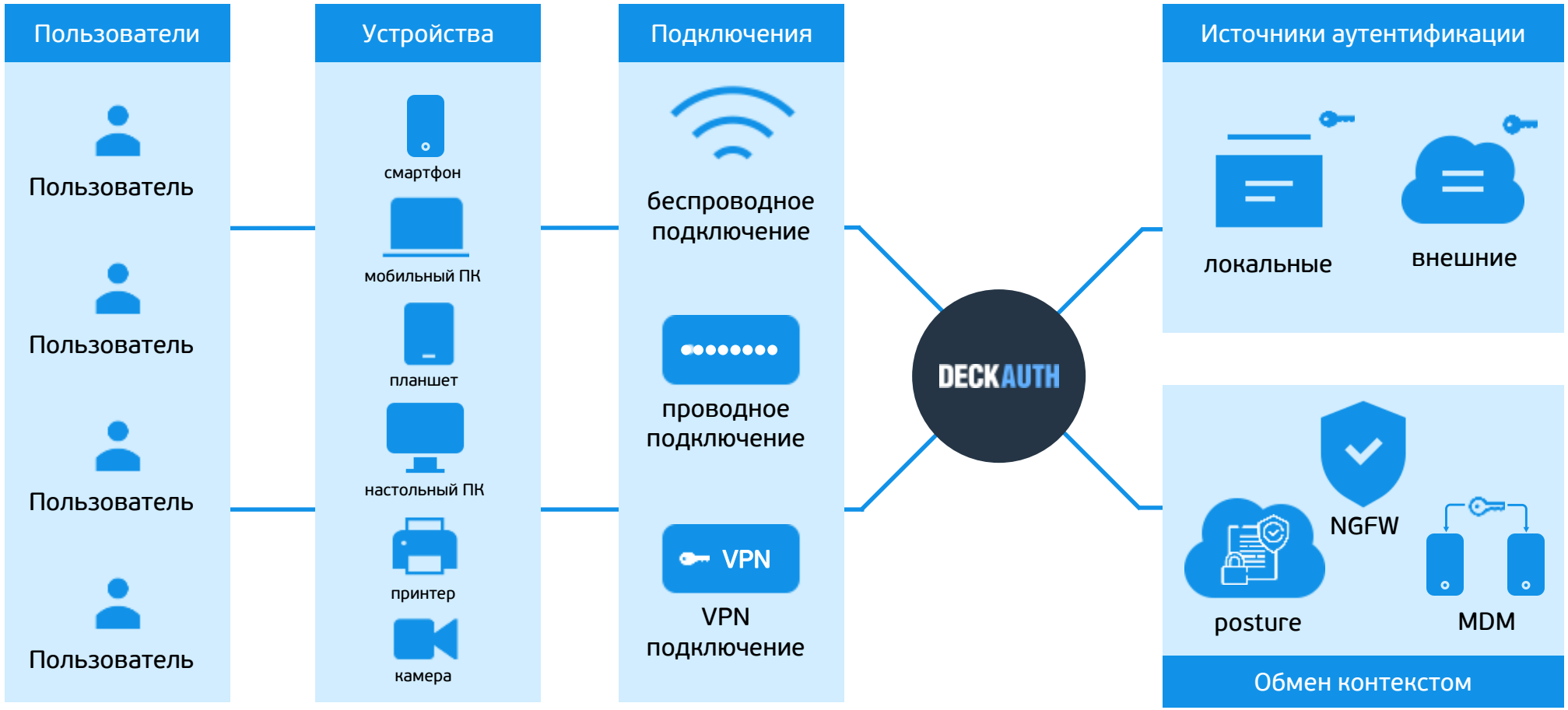
Представляем DECK AUTH

Управление всем жизненным циклом подключения

Система управления политиками для проводных, беспроводных и VPN-подключений на базе 802.1x, RADIUS и TACACS+, включая профилирование, анализ состояния конечных устройств и обмен контекстом с системами ИТ и ИБ

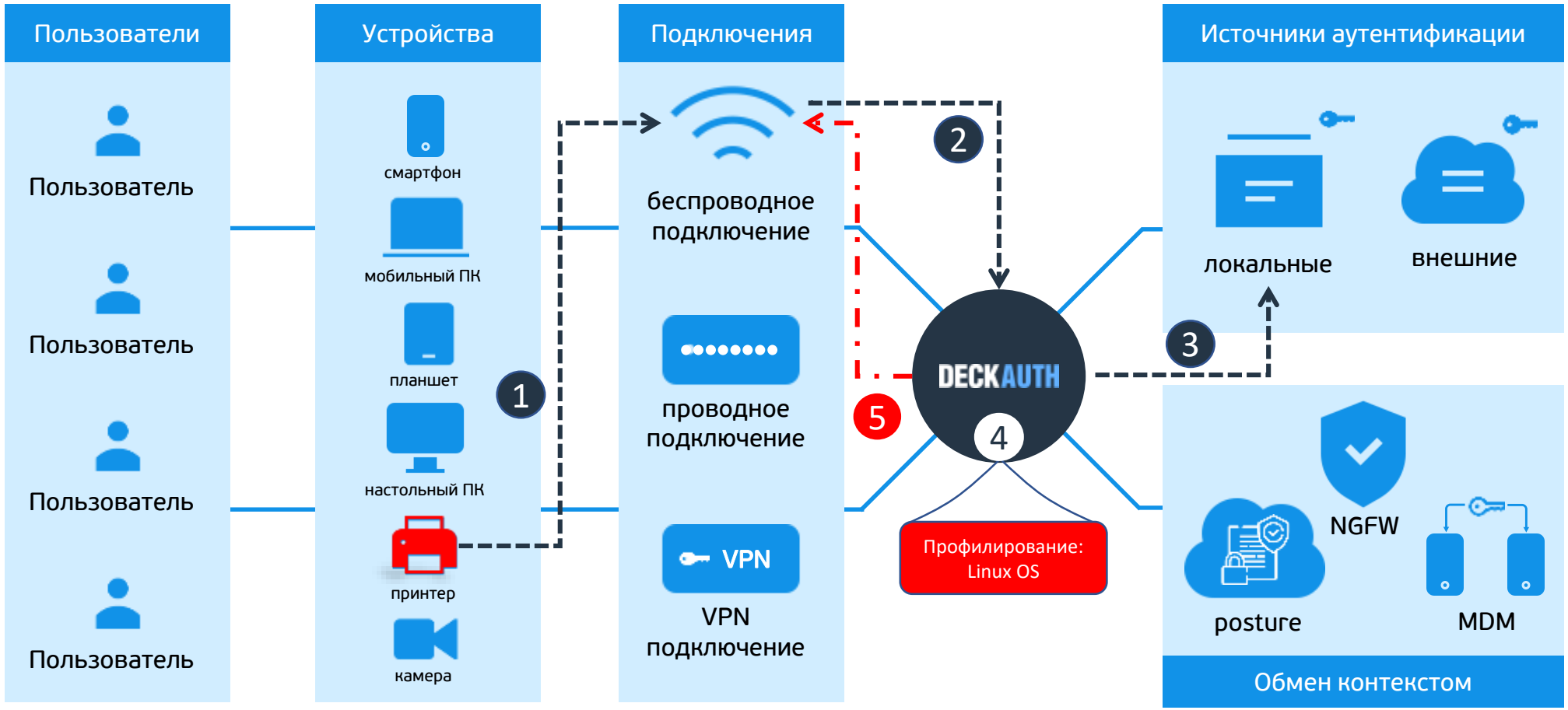
DECKAUTH

Место DECK AUTH в ИТ и ИБ инфраструктуре



DECKAUTH

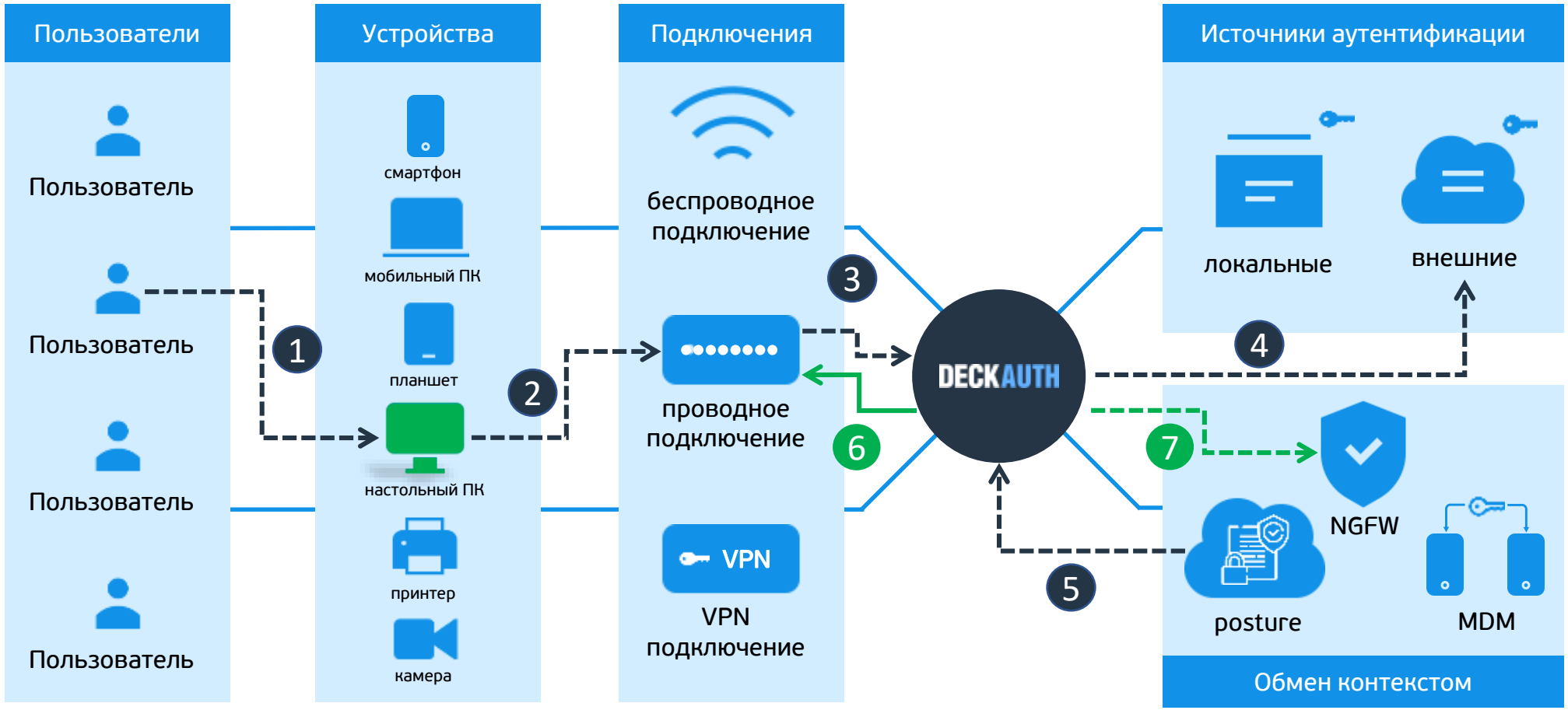
Пример – запрет на подключение устройства
Профилирование



1. Устройство «похожее на принтер» подключается к БЛВС
2. Supplicant стартует 802.1x процесс
3. NAC для аутентификации использует встроенную БД и успешно идентифицирует MAC-адрес, как «известный»
4. Процесс профилирования определяет что устройство представляет собой Linux OS
5. NAC запрещает подключение к сети устройству, «похожему на принтер»

DECKAUTH

Пример – успешное подключение ПК пользователя
Posture + обмен контекстом с NGFW



1. Пользователь включает ПК
2. Supplicant стартует 802.1x процесс
3. NAD отправляет запрос на NAC
4. NAC для аутентификации использует внешний источник
5. NAC получает состояние ПК из системы управления агентами
6. NAC разрешает подключение ПК к сети, отправляя ответ на NAD
7. NGFW получает контекст о сетевом подключении

DECKAUTH

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Встраивание

Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Встраивание

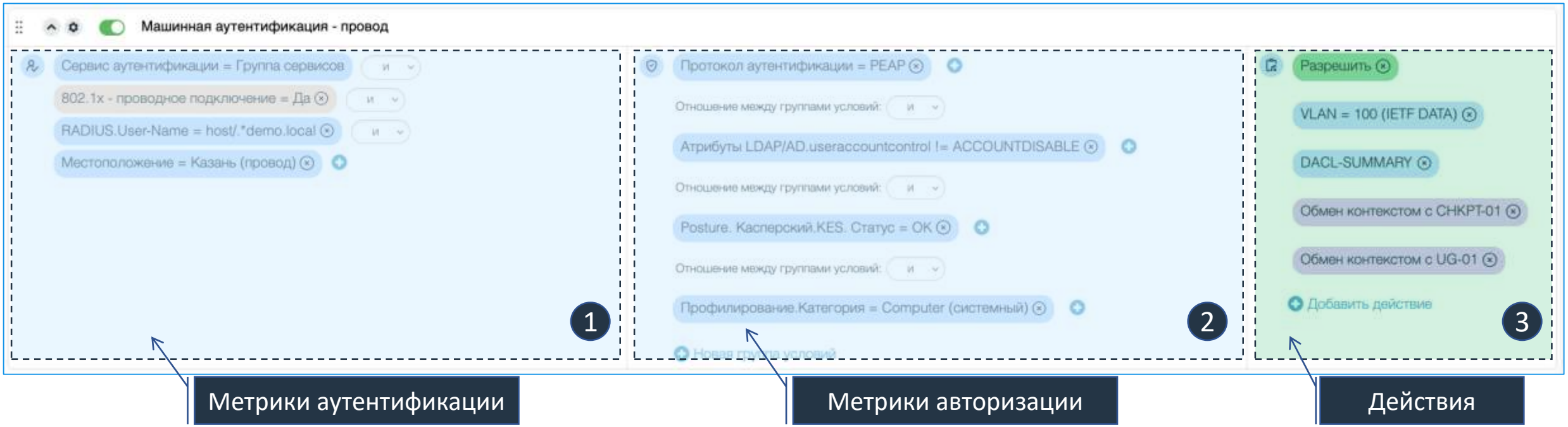
Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Принципы работы DECK AUTH
Управление сегментацией при помощи гибкого конструктора



- «Плоская» конструкция политики
  - Не копируем, делаем проще!
- Все метрики, которые должны «сработать» представлены на одном экране
  - Профилирование, Posture, другие
  - Когнитивная нагрузка на автора политики меньше, по сравнению с другими системами
- Действия != авторизационный профиль
  - реализуют обмен контекстом и интеграции (более детально эта инновация обсуждается далее)

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Встраивание

Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Встраивание

Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Контроль за сетевыми подключениями при помощи RADIUS
Жизненный цикл сессии

- **аутентификация** – происходит проверка подлинности учетных данных пользователя или устройства
- **авторизация** – определяется область видимости и формируются права на доступ к ресурсам
- **активная** – устройство подключено и может передавать данные
- **accounting** – для активной сессии происходит учет потребленных сетевых ресурсов
- **динамическая авторизация** – возможность контроля за состоянием сессии – временное отключение, повторная аутентификация и авторизация
- **завершена** – устройство или пользователь отключились от сети передачи данных

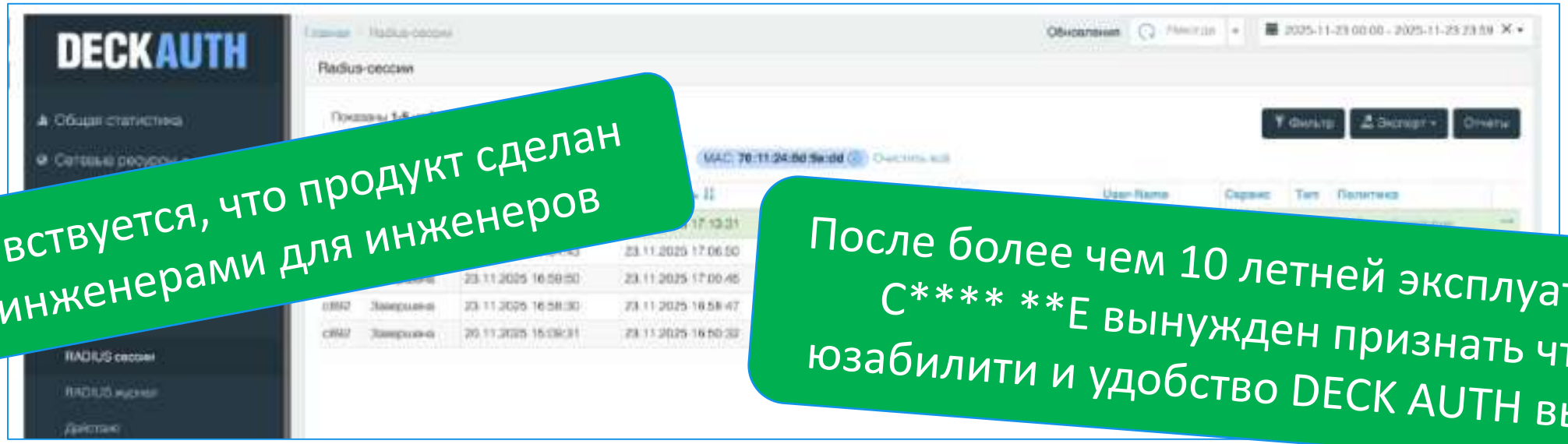
Контроль за сетевыми подключениями при помощи RADIUS

Активируйте RADIUS accounting!

- Фокус на фазе аутентификации и авторизации
  - accounting из виду упускают
- RADIUS-accounting включается только для событий start-stop
  - Как тогда ответить на вопрос – а подключено ли все еще устройство?
  - Interim-update в RADIUS accounting зачастую игнорируют
  - Настройка Interim-update может содержать некорректные интервалы – 1 раз в 8 или 24 часа
- Сетевое оборудование
  - не отражает атрибут class
  - не поддерживает RADIUS accounting
  - не поддерживает RADIUS interim-update

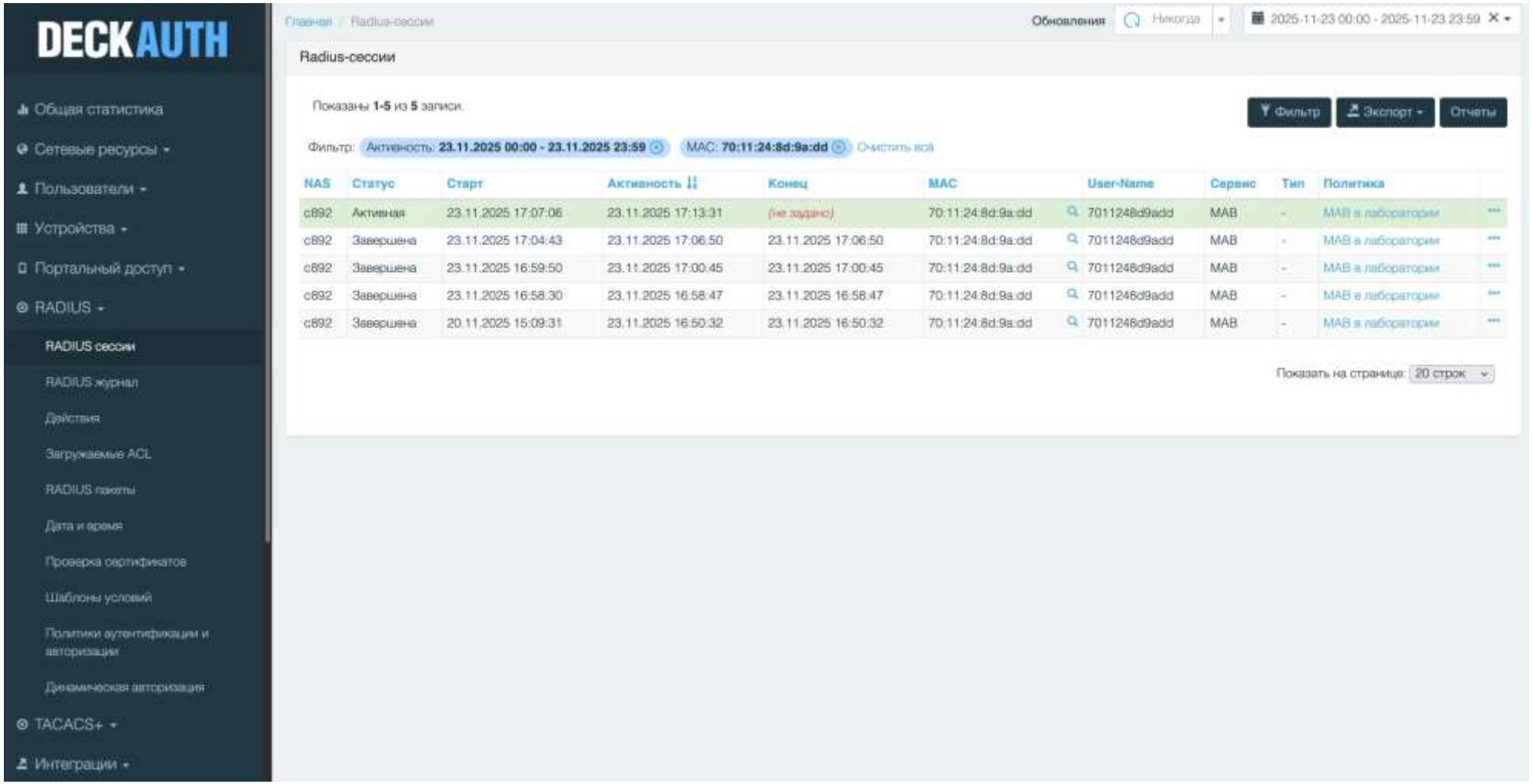
Как статус RADIUS-сессии обновляется при помощи RADIUS-accounting и почему это важно?

ВИДЕО



- Начало сессии
  - Accounting Start
- Сессия все еще активна
  - Accounting interim-update
- Сессия завершена
  - Accounting Stop

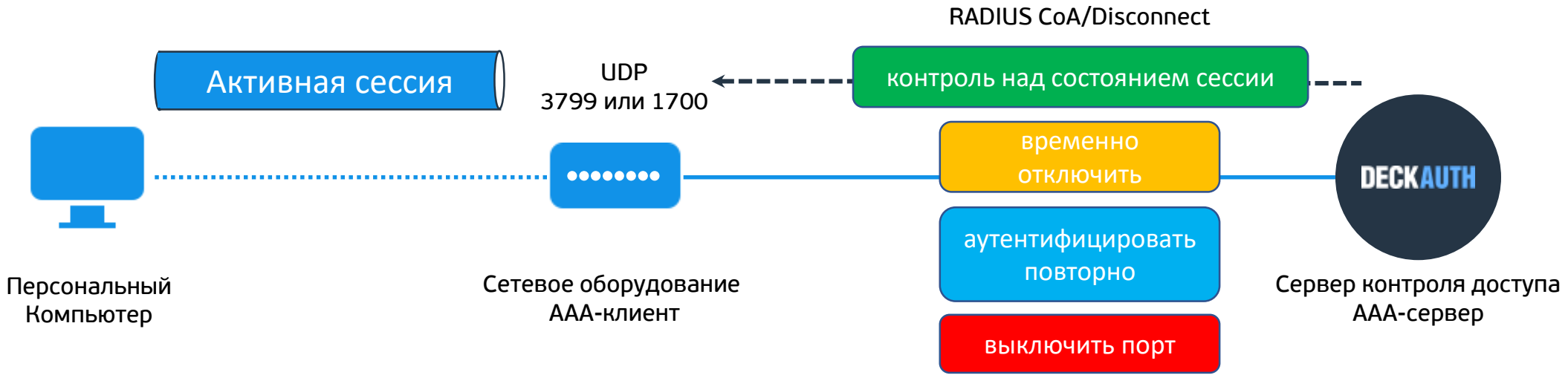
DECKAUTH


DECKAUTH
Общая статистика
Сетевые ресурсы
Пользователи
Устройства
Портальный доступ
RADIUS
RADIUS сессии
RADIUS журнал
Действия
Загружаемые ACL
RADIUS пакеты
Дата и время
Проверка сертификатов
Шаблоны условий
Политики аутентификации и авторизации
Динамическая авторизация
TACACS+
Интеграции
Главная / Radius-сессии
Обновления
Никогда
2025-11-23 00:00 - 2025-11-23 23:59
Radius-сессии
Показаны 1-5 из 5 записи.
Фильтр
Экспорт
Отчеты
Фильтр: Активность: 23.11.2025 00:00 - 23.11.2025 23:59 MAC: 70:11:24:8d:9a:dd Очистить всё
NAS Статус Старт Активность Конец MAC User-Name Сервис Тип Политика
c892 Активная 23.11.2025 17:07:06 23.11.2025 17:13:31 (не задано) 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 17:04:43 23.11.2025 17:06:50 23.11.2025 17:06:50 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 16:59:50 23.11.2025 17:00:45 23.11.2025 17:00:45 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 16:58:30 23.11.2025 16:58:47 23.11.2025 16:58:47 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 20.11.2025 15:09:31 23.11.2025 16:50:32 23.11.2025 16:50:32 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
Показать на странице: 20 строк

Контроль за сетевыми подключениями при помощи RADIUS
Настраивайте динамическую авторизацию!

- Вы не можете контролировать то, статус чего вам неизвестен
  - Помните RADIUS accounting?
  - Без него статус сессии может быть неактуальным
- Динамическая авторизация дает возможность
  - временно отключить порт так чтобы ОС «увидела» событие выключения порта (port bounce)
  - запустить повторную аутентификацию CoA
  - отправить команду на постоянное (port shutdown) или временное (disconnect) отключение порта

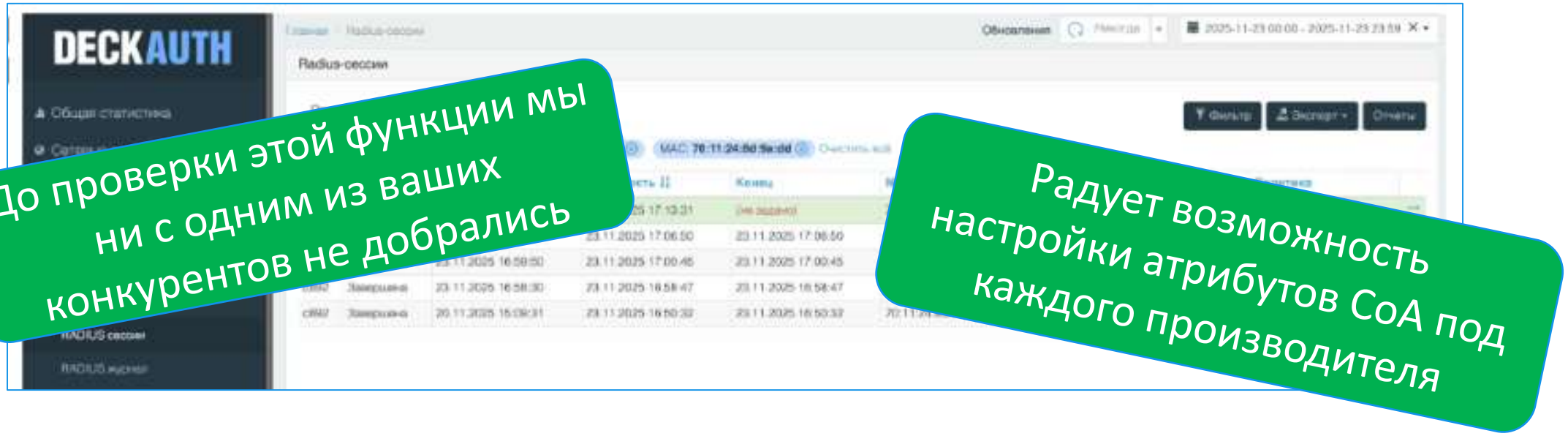
Контроль за сетевыми подключениями при помощи RADIUS
Проблемы с динамической авторизацией



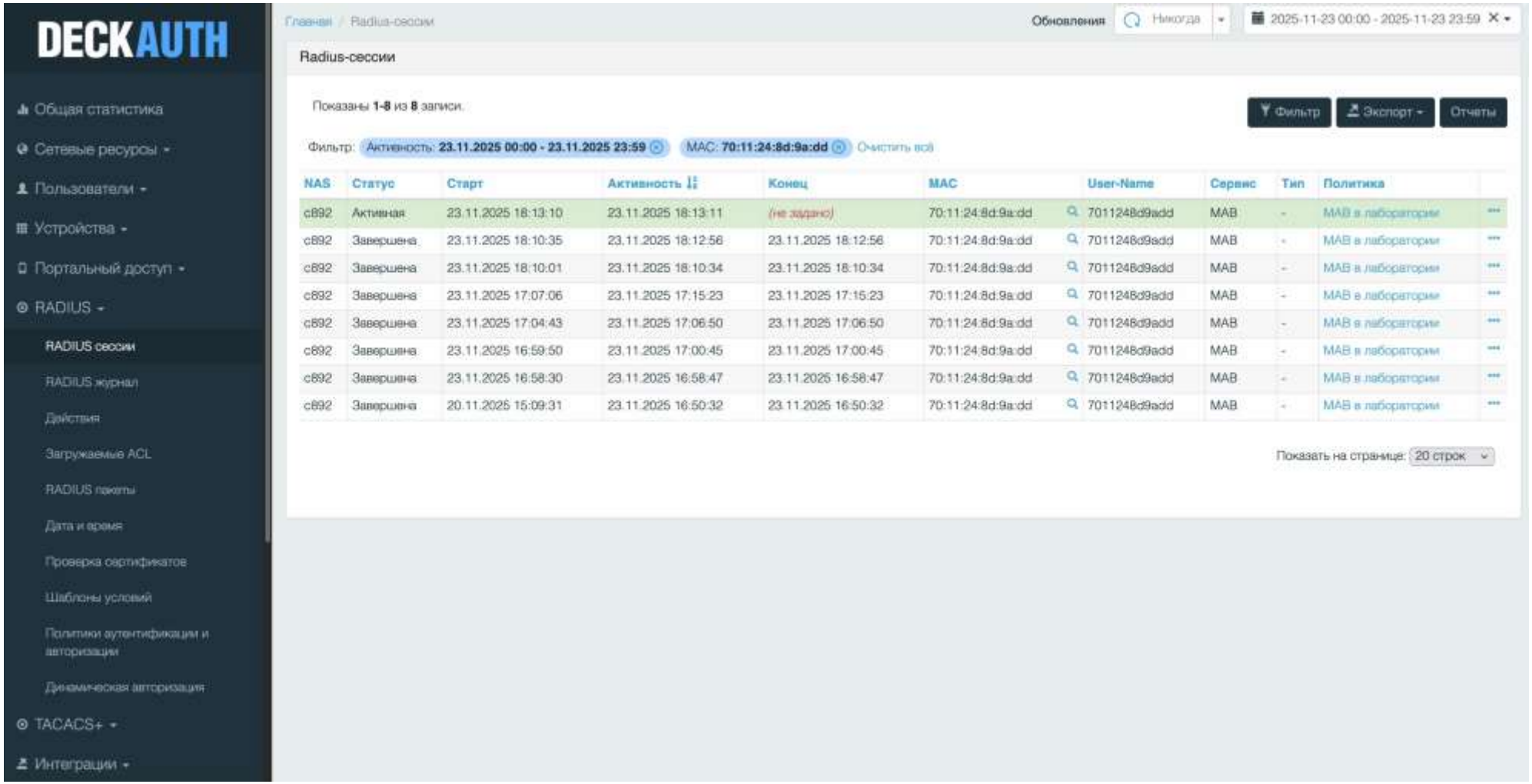
- Сетевое оборудование
  - Не поддерживает динамическую авторизацию совсем
  - Не поддерживает на нужных сетевых элементах, например контроллер БЛВС, а не точка доступа
- Сеть
  - Фильтрует, не забывайте открыть порты

Как RADIUS-сессии управляются при помощи динамической авторизации

ВИДЕО



- Источником может быть
  - процесс профилирования или posture
  - действие в web-интерфейсе системы
  - действие через REST-API со стороны SIEM, SOAR и т.д.


DECKAUTH
Общая статистика
Сетевые ресурсы
Пользователи
Устройства
Портальный доступ
RADIUS
RADIUS сессии
RADIUS журнал
Действия
Загружаемые ACL
RADIUS пакеты
Дата и время
Проверка сертификатов
Шаблоны условий
Политики аутентификации и авторизации
Динамическая авторизация
TACACS+
Интеграции
Главная / Radius-сессии
Обновления
Никогда
2025-11-23 00:00 - 2025-11-23 23:59
Radius-сессии
Показаны 1-8 из 8 записи.
Фильтр
Экспорт
Отчеты
Фильтр: Активность: 23.11.2025 00:00 - 23.11.2025 23:59 MAC: 70:11:24:8d:9a:dd Очистить всё
NAS Статус Старт Активность Конец MAC User-Name Сервис Тип Политика
c892 Активная 23.11.2025 18:13:10 23.11.2025 18:13:11 (не задано) 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 18:10:35 23.11.2025 18:12:56 23.11.2025 18:12:56 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 18:10:01 23.11.2025 18:10:34 23.11.2025 18:10:34 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 17:07:06 23.11.2025 17:15:23 23.11.2025 17:15:23 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 17:04:43 23.11.2025 17:06:50 23.11.2025 17:06:50 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 16:59:50 23.11.2025 17:00:45 23.11.2025 17:00:45 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 23.11.2025 16:58:30 23.11.2025 16:58:47 23.11.2025 16:58:47 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
c892 Завершена 20.11.2025 15:09:31 23.11.2025 16:50:32 23.11.2025 16:50:32 70:11:24:8d:9a:dd 7011248d9add MAB - MAB в лаборатории
Показать на странице: 20 строк

Контроль за подключениями операторов и администраторов при помощи протокола TACACS+

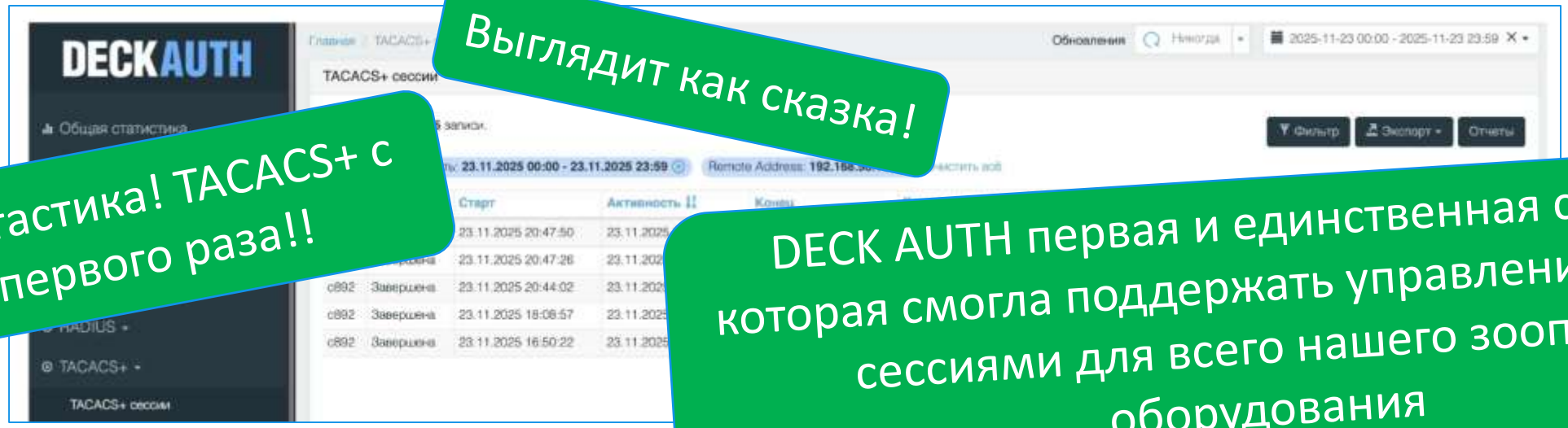
- **аутентификация** – происходит проверка подлинности учетных данных пользователя
- **авторизация** – определяется уровень привилегий в рамках сессии
- **активная** – сессия активирована и пользователь или скрипт могут вводить команды
- **accounting** – для активной сессии происходит учет вводимых команд
- **авторизация команд** – возможность контроля за вводимыми в рамках сессии командами
- **завершена** – сессия была закрыта пользователем

Контроль за подключениями операторов и администраторов при помощи протокола TACACS+

- TACACS+ подключение представляет собой множество TCP-сессий
- Сетевое оборудование
  - «не знает», что есть авторизация сессии
  - не поддерживает авторизацию команд
  - хаос в назначении атрибутов Remote-Address и Port у сессии на разных фазах
- Тем не менее DECK AUTH
  - «Склеивает» множество активностей в одну логическую TACACS+ сессию, чтобы вы могли получить полный контроль

Как DECK AUTH управляет TACACS+ сессией?
Отзывы Заказчиков

ВИДЕО

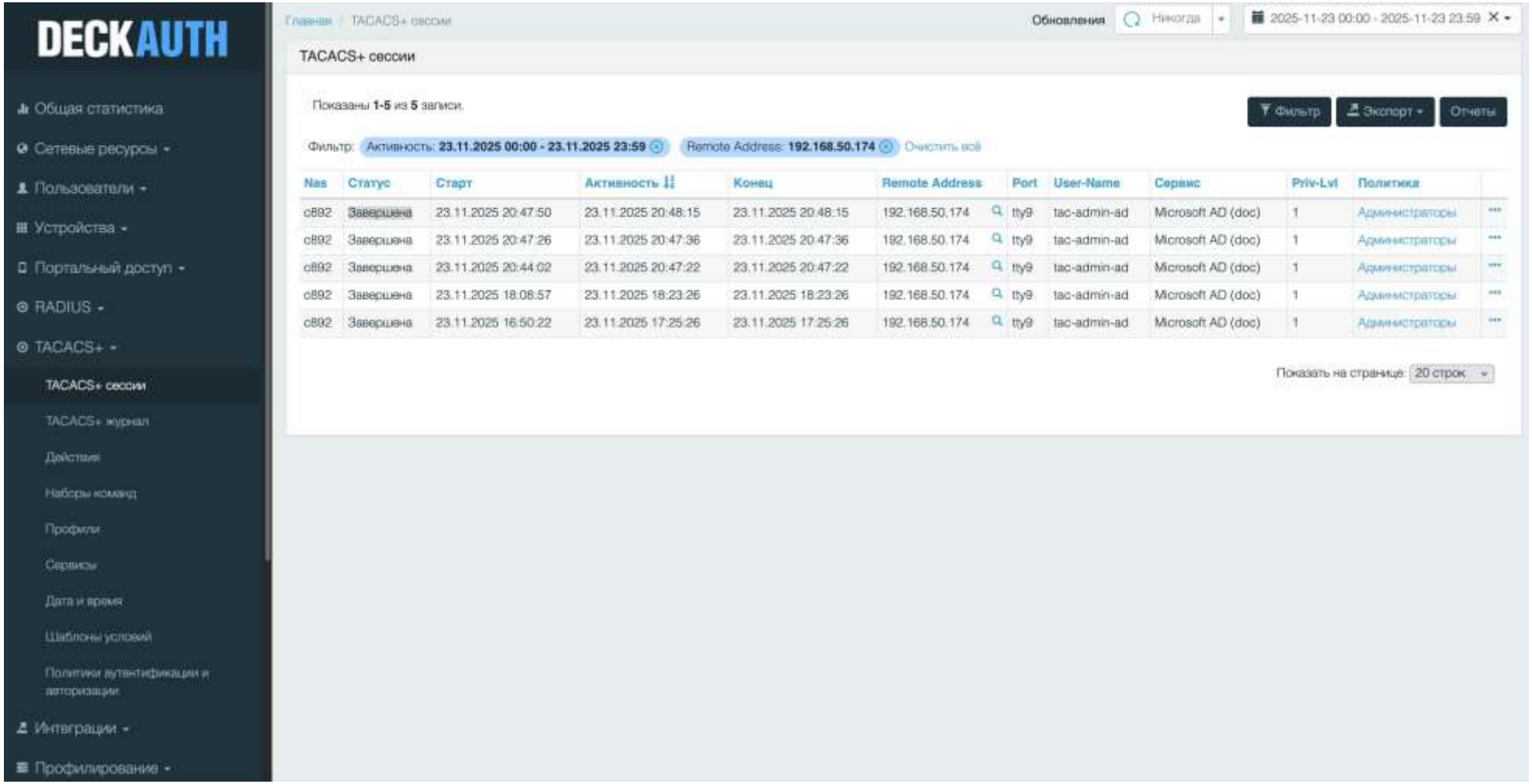


- Аутентификация и авторизация сессии
- Контроль за вводимыми командами
- Перевод сессии в статус «Завершена» после отключения от сетевого устройства

DECKAUTH

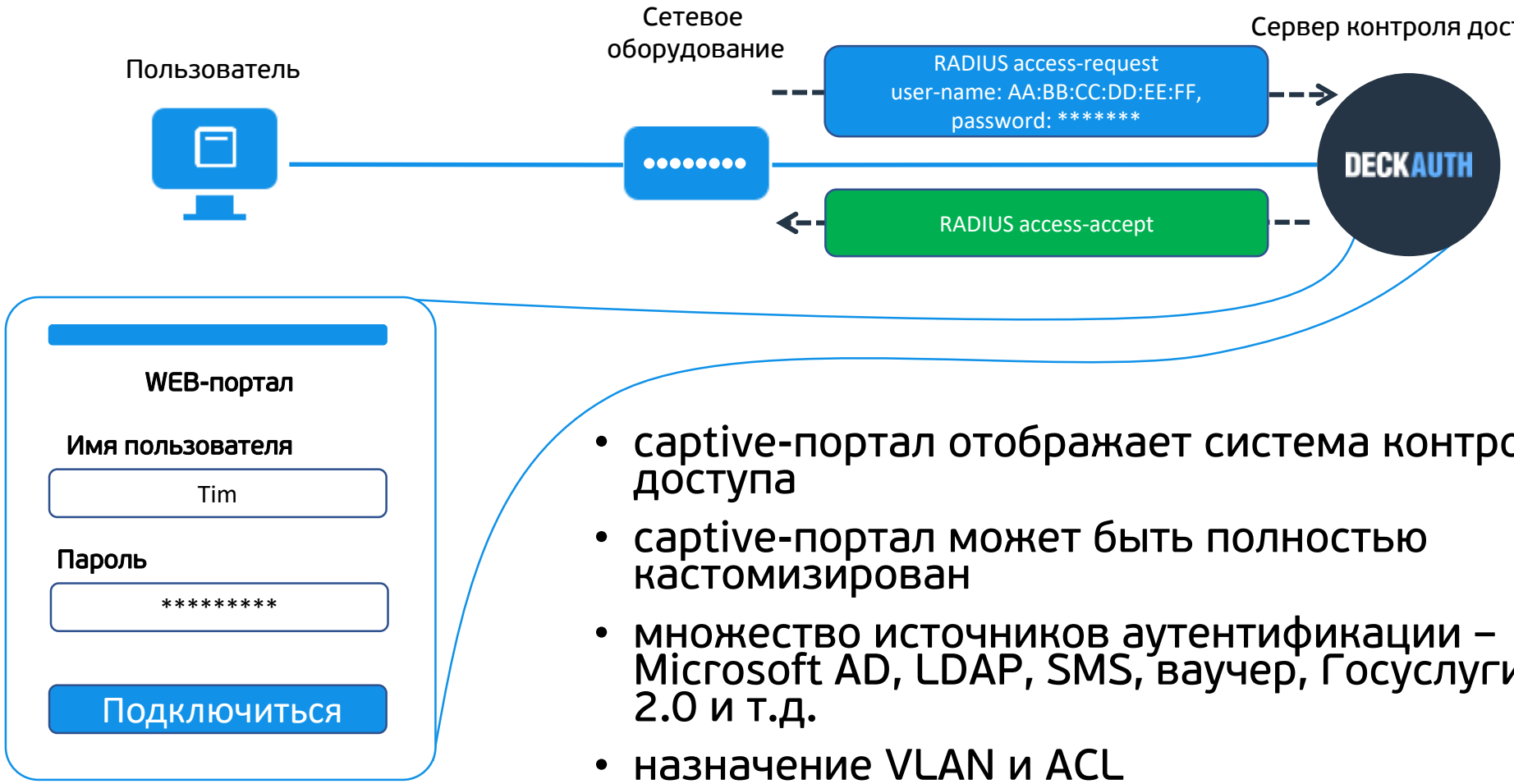
Как DECK AUTH управляет TACACS+ сессией?

ВИДЕО



DECKAUTH

Централизованная WEB-аутентификация



- captive-портал отображает система контроля доступа
- captive-портал может быть полностью кастомизирован
- множество источников аутентификации – Microsoft AD, LDAP, SMS, ваучер, Госуслуги, OAuth 2.0 и т.д.
- назначение VLAN и ACL
- управление при помощи портальной сессии

DECKAUTH

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Встраивание

Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Встраивание

Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Технологическая нейтральность – залог успеха для встраивания NAC в ИТ и ИБ инфраструктуру

- Технологическая нейтральность для 802.1x, RADIUS, TACACS+ и правил перенаправления на порталы для WEB-аутентификации

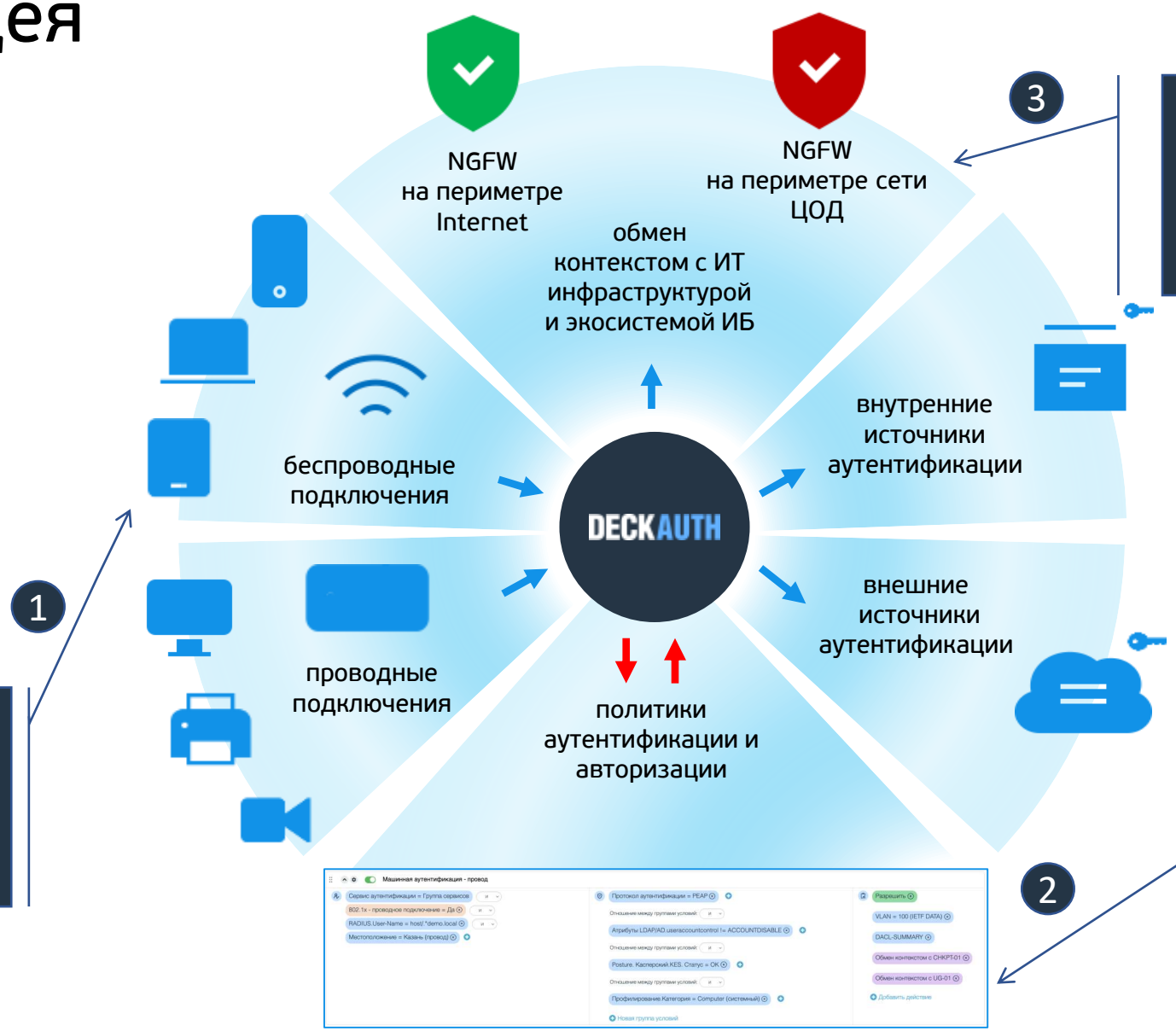
aruba cisco D-Link ELTEX H3C HUAWEI MikroTik Ruijie tp-link

AQUARIUS CUMULUS DCN QTECH MAIPU MITIGATOR Ruckus UBIQUITI BEKTOP

- Органично вписывающиеся в архитектуру системы инновационные интеграции
  - NGFW
  - MDM
  - Posture на основе агентов 3-тих производителей
  - SIEM/SOAR
  - NTA/NDR

DECKAUTH

Встраивание при помощи обмена контекстом
Общая идея



1

Информация о зоне/сегменте безопасности и IP-адресе аутентифицированного устройства

2

Правила по которым система передает информацию внешним устройствам удобно встроены в конструктор политик

3

Динамическое наполнение групп (dynamics objects, Security Group и т.д.) IP-адресами аутентифицированных пользователей и устройств

Глубокое встраивание в системамы ИТ и ИБ

Контроль доступа к ресурсам с использованием контекста из NAC

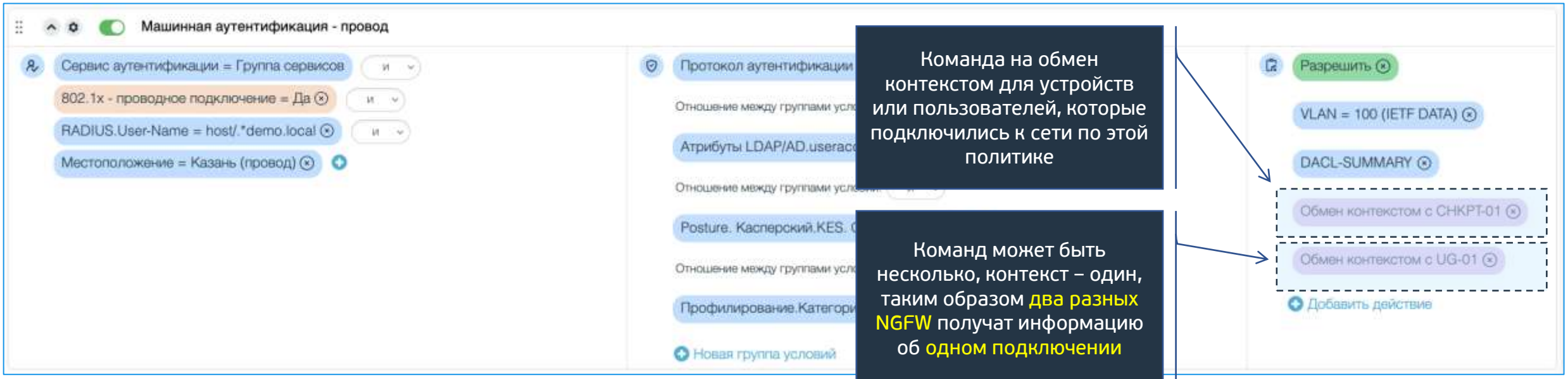
Типовые политики безопасности			
Система	Название объекта	Источник (source)	Получатель (destination)
NGFW	Object-group, Dynamic Object etc.	Пользователь, устройство	Приложение (ВМ или контейнер)
Контейнерные среды	Security Group etc.	Пользователь, устройство	Приложение (контейнер)
Публичные облака	Security Group etc.	Пользователь, устройство	Приложение (ВМ или контейнер)

NAC имеет возможность поддерживать актуальность этой части политики безопасности автоматически

- Автоматизация формирования политик безопасности повышает общую защищенность ИТ-инфраструктуры предприятия
- Как минимум половина политики всегда в актуальном состоянии! ☺

DECKAUTH

Принципы работы DECK AUTH
Настройка обмена контекстом на уровне политики



- Высокая гранулярность управления обменом контекста
  - На уровне конкретной политики, в отличие от подхода «транслирую все и всем»
- Множественные действия как реакция на подключение
  - Отправка сообщения syslog
  - Отправка RADIUS-accounting
  - Выполнение произвольного REST-API вызова с контекстом сессии

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Встраивание

Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Принципы работы DECK AUTH

Сегментация

Гибкий конструктор политик для управления минимизацией размера зон доверия и прав доступа

Прозрачность

Прозрачная и понятная работа с RADIUS, TACACS+ и портальными (Captive) сессиями

Встраивание

Автоматизация встраивания в экосистему ИТ и ИБ, включая обмен контекстом

Простота

Готовая система работающая «из коробки», а не наборы «сделай сам» или «склей два продукта»

DECKAUTH

Готовый кластер «из коробки»

- Микросервисный кластер
  - встроенная отказоустойчивость средств хранения политик и журналов
  - встроенная балансировка нагрузки на элементы системы, которые отвечают за рендер политик

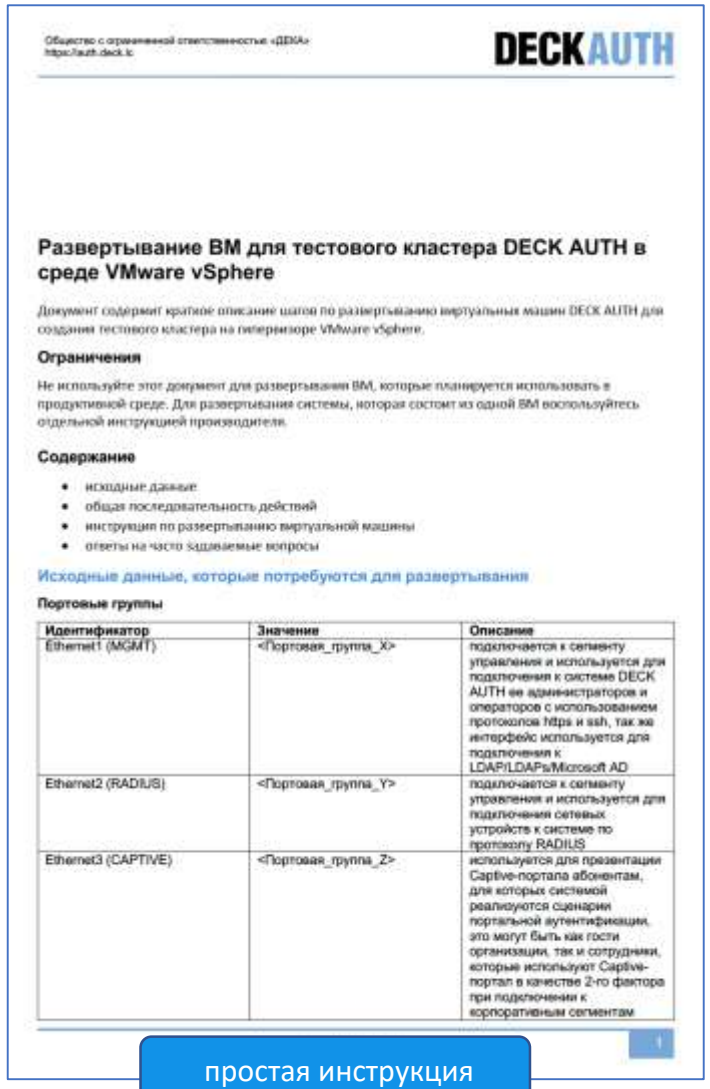
- Работы с кластеров полностью автоматизирована за счет HOB = Host Operations Backend
  - Установка
  - Обновление
  - Резервное копирование и восстановление после сбоев
  - Операции с сертификатами (K8S API)
  - Операции по анализу трафика/поведения в сети (trace, ping, tcpdump)

- Простота работы с системой != архитектурные компромиссы

Конкурентные решения могут предлагать наборы «сделай сам», вместо NAC «под ключ»

Для эксплуатации системы «сделай сам» требуется привлекать команду DevOps, либо эти компетенции иметь внутри команды NAC

Работа с системой через WEB-интерфейс



Общество с ограниченной ответственностью «ДЕКА»
https://auth.deck.ic

DECKAUTH

Развертывание ВМ для тестового кластера DECK AUTH в среде VMware vSphere

Документ содержит краткое описание шагов по развертыванию виртуальных машин DECK AUTH для создания тестового кластера на гипервизоре VMware vSphere.

Ограничения

Не используйте этот документ для развертывания ВМ, которые планируется использовать в продуктивной среде. Для развертывания системы, которая состоит из одной ВМ воспользуйтесь отдельной инструкцией производителя.

Содержание

- исходные данные
- общая последовательность действий
- инструкция по развертыванию виртуальной машины
- ответы на часто задаваемые вопросы

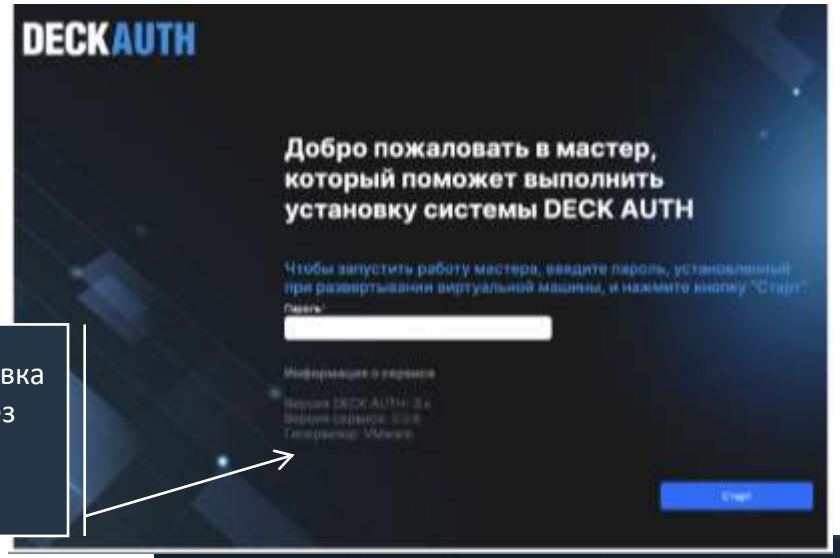
Исходные данные, которые потребуются для развертывания

Портовые группы

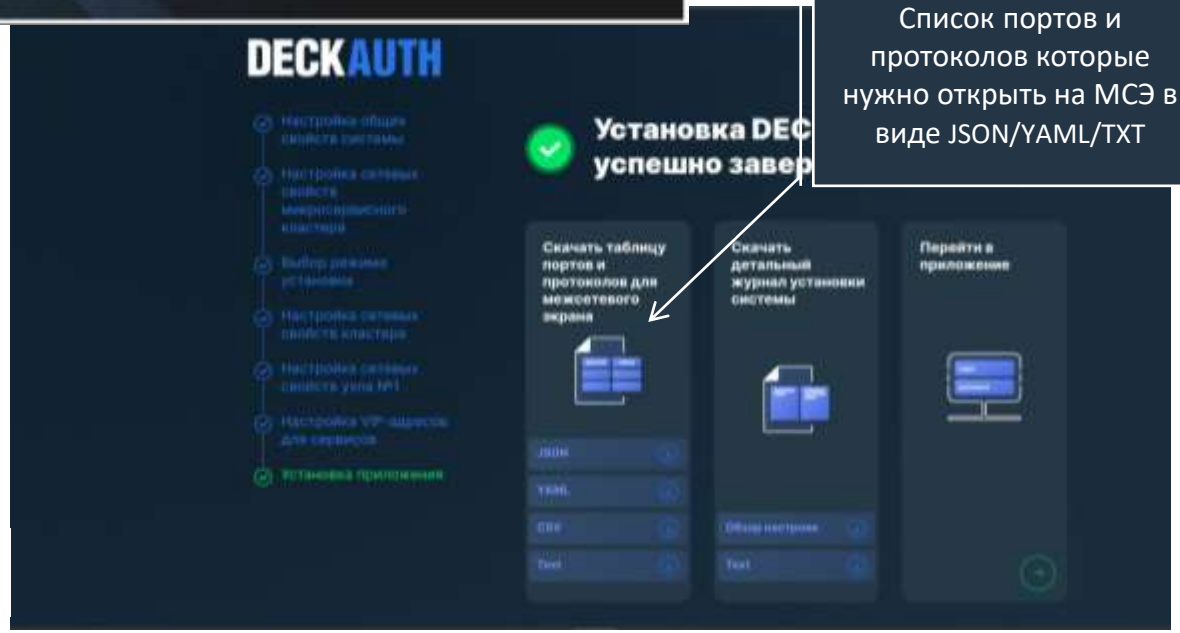
Идентификатор	Значение	Описание
Ethernet1 (MGMT)	<Портовая_группа_X>	подключается к сегменту управления и используется для подключения к системе DECK AUTH ее администраторов и операторов с использованием протоколов https и ssh, так же интерфейс используется для подключения к LDAP/LDAPs/Microsoft AD
Ethernet2 (RADIUS)	<Портовая_группа_Y>	подключается к сегменту управления и используется для подключения сетевых устройств к системе по протоколу RADIUS
Ethernet3 (CAPTIVE)	<Портовая_группа_Z>	используется для презентации Captive-портала абонентам, для которых системой реализуются сценарии портальной аутентификации, это могут быть как гости организации, так и сотрудники, которые используют Captive-портал в качестве 2-го фактора при подключении к корпоративным сегментам

1

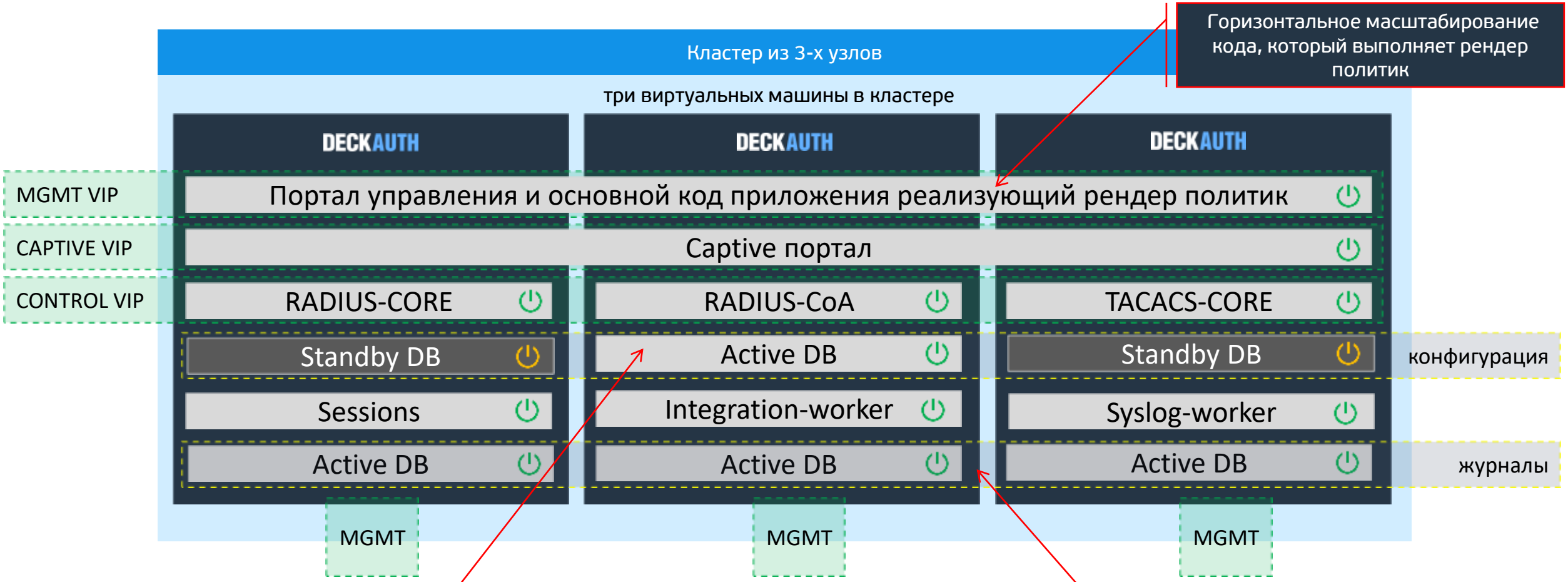
простая инструкция



Сборка и установка кластера через графический интерфейс



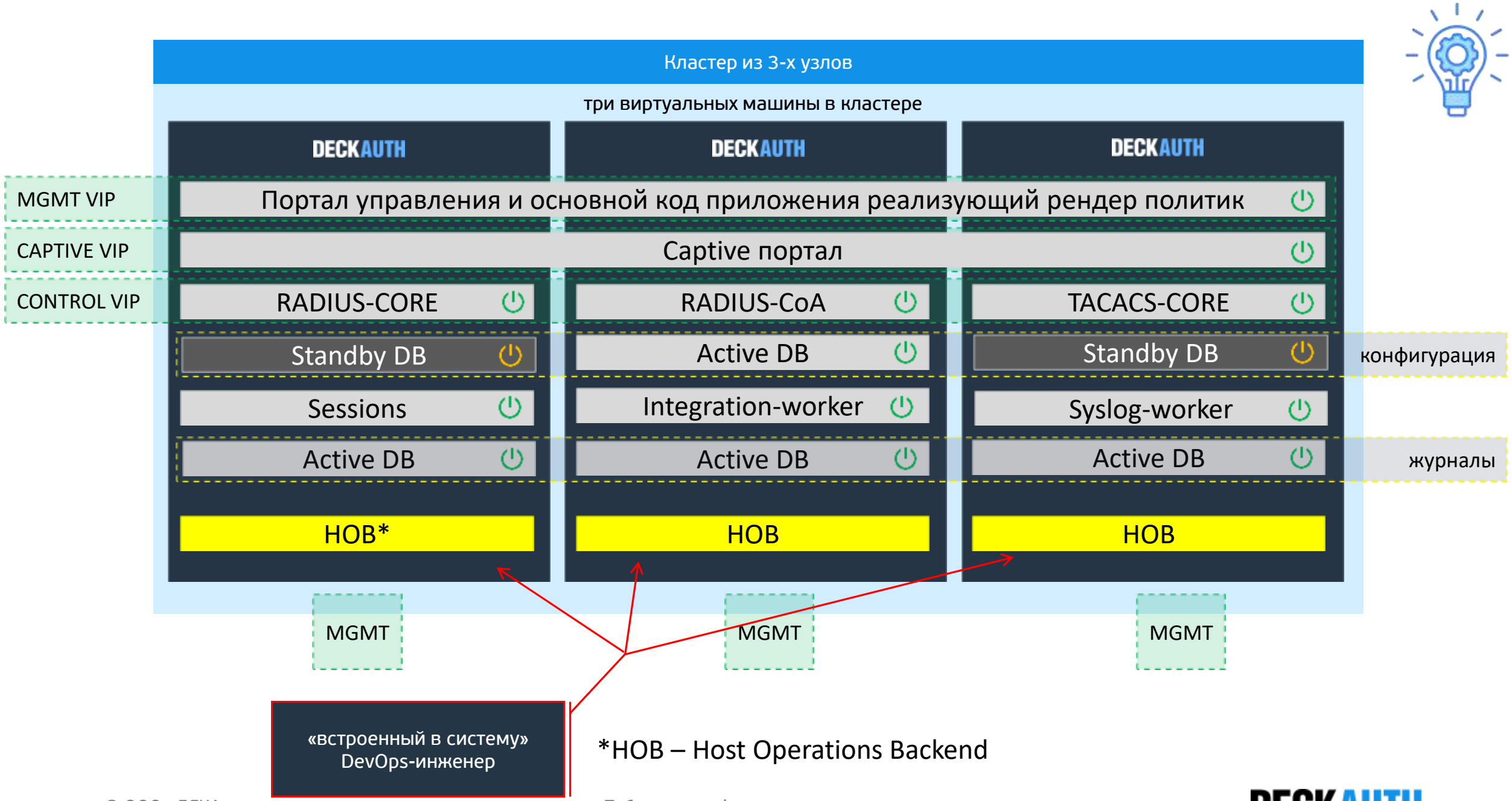
Список портов и протоколов которые нужно открыть на МСЭ в виде JSON/YAML/TXT



- RADIUS-CORE - аутентификация пользователей и устройств
- RADIUS-CoA – интерактивный обмен с оборудованием
- TACACS-CORE – аутентификация операторов и администраторов
- Integration worker – обмен контекстом с оборудованием

- Active DB - активный экземпляр БД
- Standby DB – экземпляр БД в горячем резерве
- Syslog-worker - отправка syslog-сообщений
- Sessions – сервис мониторинга состояния сессий

DECKAUTH



DECKAUTH

Заинтересовало решение?

Заходите на стенд!

DECKAUTH


DECK AUTH
https://auth.deck.lc