DECK AUTH

Внедряем NAC. Выбор стратегии.

Хаванкин Максим
mkhavank@deck.lc

План семинара

- Несколько фактов о **DECK AUTH**
- Сценарии контроля доступа
  - Какие сценарии контроля доступа существуют?
  - Какие сценарии реализовать в первую очередь?
- Гранулярность политик
  - Как устроены политики контроля доступа?
  - Насколько гранулярными они должны быть?
- Изменения на уровне сети
  - Базовый минимум
  - Как может измениться дизайн сети при внедрении NAC?
- Изменения на уровне конечных устройств
  - Базовый минимум
  - Какой контекст с устройств может использовать NAC?

Несколько фактов о DECK AUTH

История компании DECK

Какую проблему решает система?

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

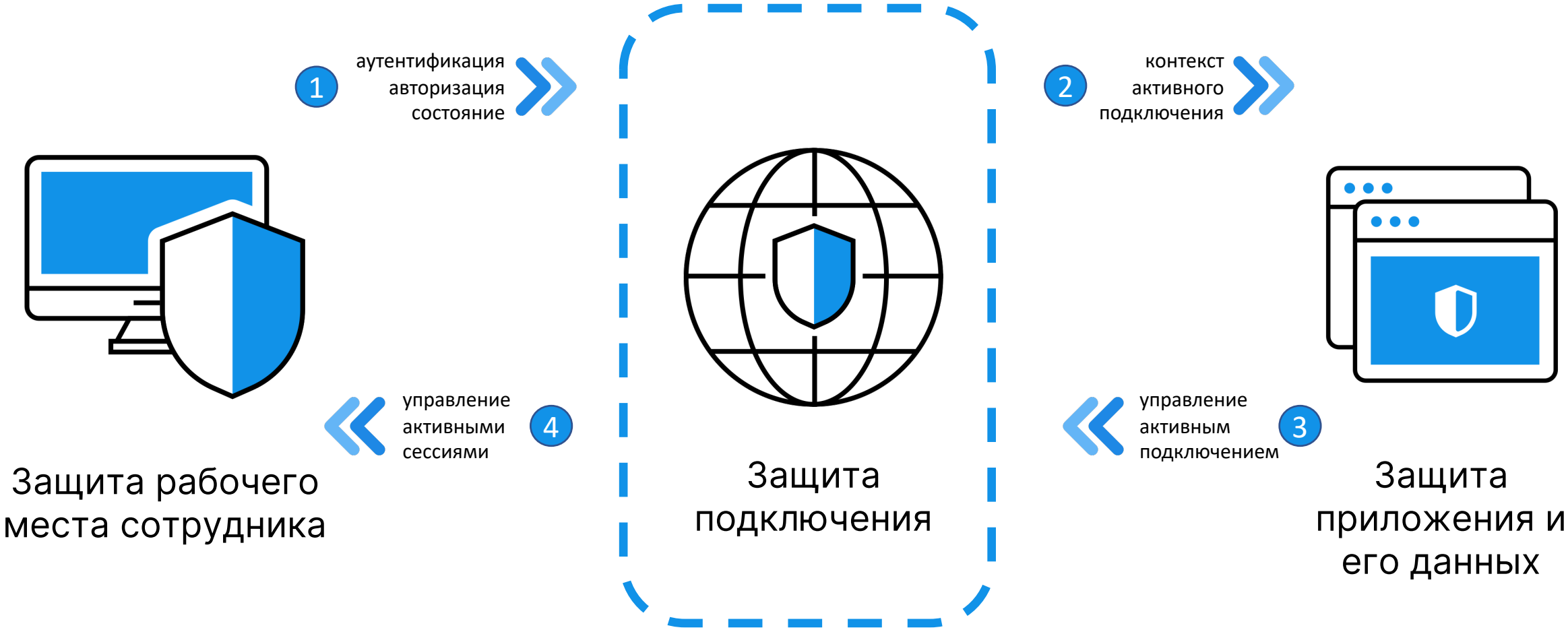
Основной класс:

02.07 Серверное и связующее программное обеспечение

*PCRF - Policy and Charging Rules Function

DECKAUTH

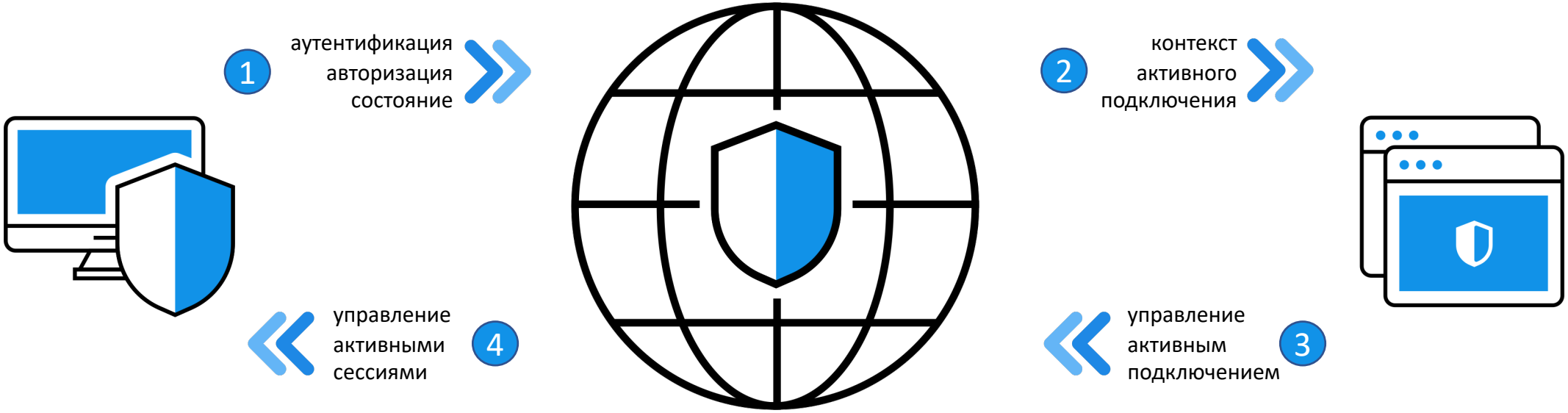
NAC фокусируется на защите подключений



DECKAUTH

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

Сценарии сетевого контроля доступа

Какие сценарии сетевого контроля доступа существуют?

Какие сценарии реализовать в первую очередь?

Сценарии сетевого контроля доступа

Проводные подключения

- Сотрудники
- Устройства
- Подрядчики
- Гости

Беспроводные подключения

- Сотрудники
- Устройства
- Подрядчики
- Гости

VPN подключения

- Сотрудники
- Подрядчики

Консольные подключения

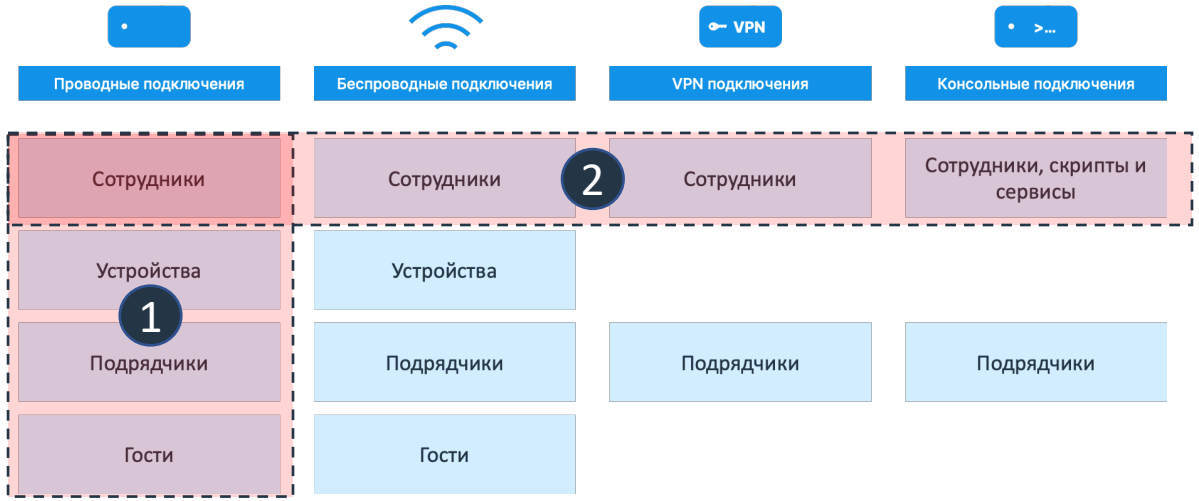
- Сотрудники, скрипты и сервисы
- Подрядчики

DECKAUTH

Какие сценарии реализовать в первую очередь?

Возможная стратегия	Пример
Контроль доступа к критичным для бизнеса данным и системам	802.1x аутентификация проводных подключений сотрудников, с рабочих мест которых реализуется доступ к АБС
Контроль за эксплуатацией самых простых в реализации векторов атак	Переход с известного всем WEP-ключа на индивидуальные сертификаты при контроле доступа за 802.1x беспроводными подключениями
Контроль за самыми массовыми подключениями	Контроль за гостевыми беспроводными подключениями при проведении массовых мероприятий
Быстрая реализация сложных методов на ограниченном количестве пользователей, чтобы убедить бизнес в зрелости технологии	802.1x аутентификация ИТ-администраторов при их подключении с корпоративных устройств к проводной сети для управления сетевым оборудованием

Какую стратегию относительно сценариев выбрать?



1 Комплексная реализация для всех типов и методов доступа внутри сценария

- Например, активация контроля за проводными подключениями на всех портах сетевого оборудования всех производителей (Cisco, Huawei, Eltex и т.д.)
- Реализация контроля для сотрудников, устройств, подрядчиков и гостей
- Контроль «**в глубину**»

2 Контроль за всеми методами подключения без исключения

- Если на сети используется метод подключения, то для него требуется контроль
- Например контроль за проводными, беспроводными, VPN и TACACS+ подключениями, если они используются
- Контроль **«в ширину»**

DECKAUTH

Производитель автомобилей

Задача

- Миграция с существующих RADIUS-серверов собственной разработки
- Фокус на поддержке беспроводных сценариев подключения для производственной площадки
- Интеграция с существующими системами по управлению гостевыми беспроводными подключениями
- Ограниченное время на реализацию проекта

Решение

- Использование DECK AUTH в следующих сценариях:
  - контроль беспроводного доступа (PEAP, EAP-TLS)
  - контроль VPN подключений
  - контроль за подключениями операторов и администраторов при помощи TACACS+
- Интеграция с ПО сервис-деск собственной разработки Заказчика при помощи REST API, встроенных в DECK AUTH
- Услуги профессионального сервиса по настройке и запуску системы
- Лицензия на 15 000 подключений
- Январь – май, 2025 год, проект завершен

Преимущества

- Миграция настроек, с существующих RADIUS-серверов **без простоя** процессов аутентификации и авторизации
- **Полная** поддержка всего спектра оборудования, которое используется для БЛВС подключений (3 поколения устройств, несколько производителей)
- **Надежное и предсказуемое** поведение системы для беспроводных устройств занятых в производственном процессе (ПК, технологическое оборудование, тележки и т.д.)
- Простой и безопасный процесс подключения гостей к БЛВС, за счет **интеграции** сервис-деск системой Заказчика и поддержки источника аутентификации на основе многоразовых кодов доступа

* имеется возможность организации референс-визита

Производитель автомобилей

Последовательная реализация сценариев «в глубину»

Проводные подключения	Беспроводные подключения	VPN подключения	Консольные подключения
Сотрудники	Сотрудники	Сотрудники	Сотрудники, скрипты и сервисы
Устройства	Устройства		
Подрядчики	Подрядчики	Подрядчики	Подрядчики
Гости	Гости		
ФАЗА № 4	ФАЗА № 1	ФАЗА № 2	ФАЗА № 3

Банк

Задача

- Миграция с существующей системы NAC
- Поддержка всех существующих сценариев контроля доступа, которые используются в Банке
- Обмен контекстом с существующим оборудованием ИБ для контроля за подключениями ОС на ПК, отличных от Microsoft
- Оптимизация существующих политик аутентификации и авторизации

Решение

- Использование DECK AUTH в следующих сценариях:
  - контроль проводного и беспроводного доступа (EAP-TLS, PEAP)
  - контроль VPN подключений
  - контроль за подключениями операторов и администраторов при помощи TACACS+
- Интеграция с Checkpoint Identity Collector для обмена контекстом с существующим оборудованием ИБ
- Использование контекстных переменных для уменьшения количества политик
- Услуги профессионального сервиса по настройке и запуску системы
- Лицензия на 30 000 подключений
- Поэтапная миграция в 2025 и 2026 году

Преимущества

- Миграция настроек, политик с существующей системы **без простоя** процессов аутентификации и авторизации
- Повышение **уровня защищенности** в части контроля за TACACS+ подключениями за счет встроенного механизма автоматически регистрирующего сессии и поддержки **особенностей оборудования** отечественных производителей
- Уменьшение количества политик для некоторых сценариев **в десятки раз**, за счет использования политик контроля имени пользователя и контекстных переменных

Банк

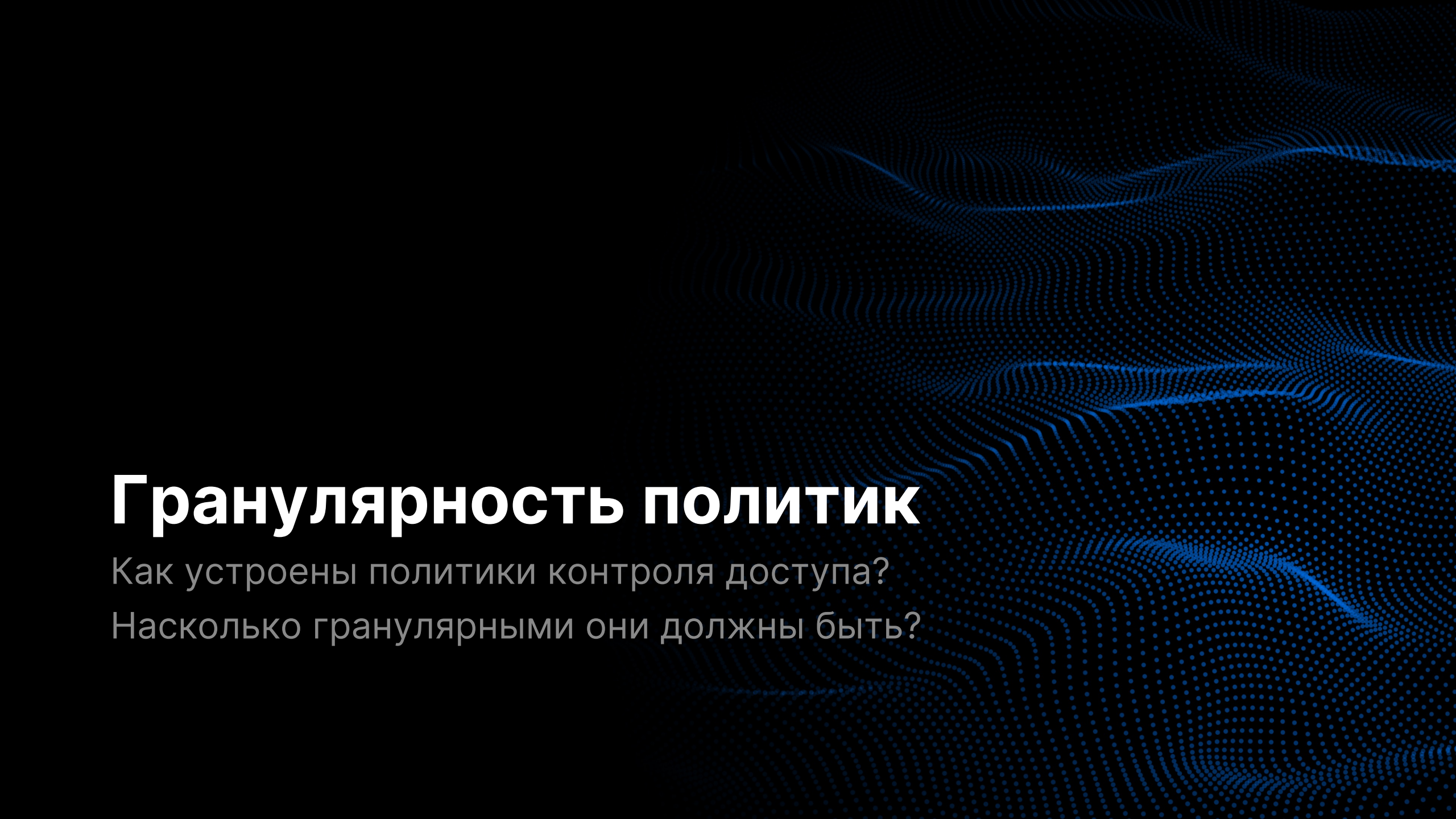
Стратегия «замещения» и «в глубину» и «в ширину» одновременно

Проводные подключения	Беспроводные подключения	VPN подключения	Консольные подключения
Сотрудники	Сотрудники	Сотрудники	Сотрудники, скрипты и сервисы
Устройства	Устройства	ФАЗА № 2	ФАЗА № 1
Подрядчики	Подрядчики	Подрядчики	Подрядчики
Гости	Гости	ФАЗА № 3	

DECKAUTH

Стратегия внедрения NAC

- Определить сценарии внедрения
  - Реализуем сценарий «в глубину» на всех портах, типах оборудования и клиентах
  - Реализуем сценарии «в ширину» - ни один метод доступа к сети не оставляем без контроля

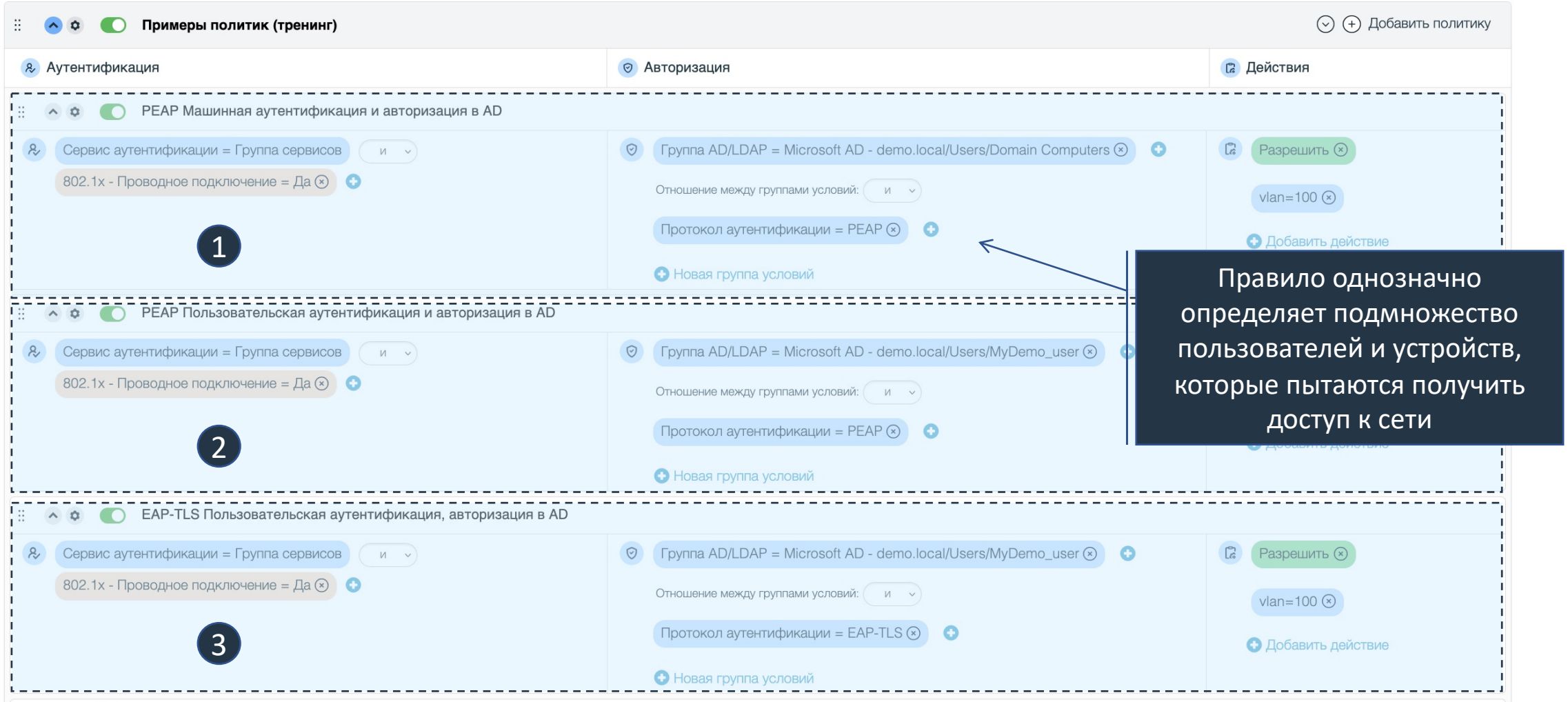


Гранулярность политик

Как устроены политики контроля доступа?

Насколько гранулярными они должны быть?

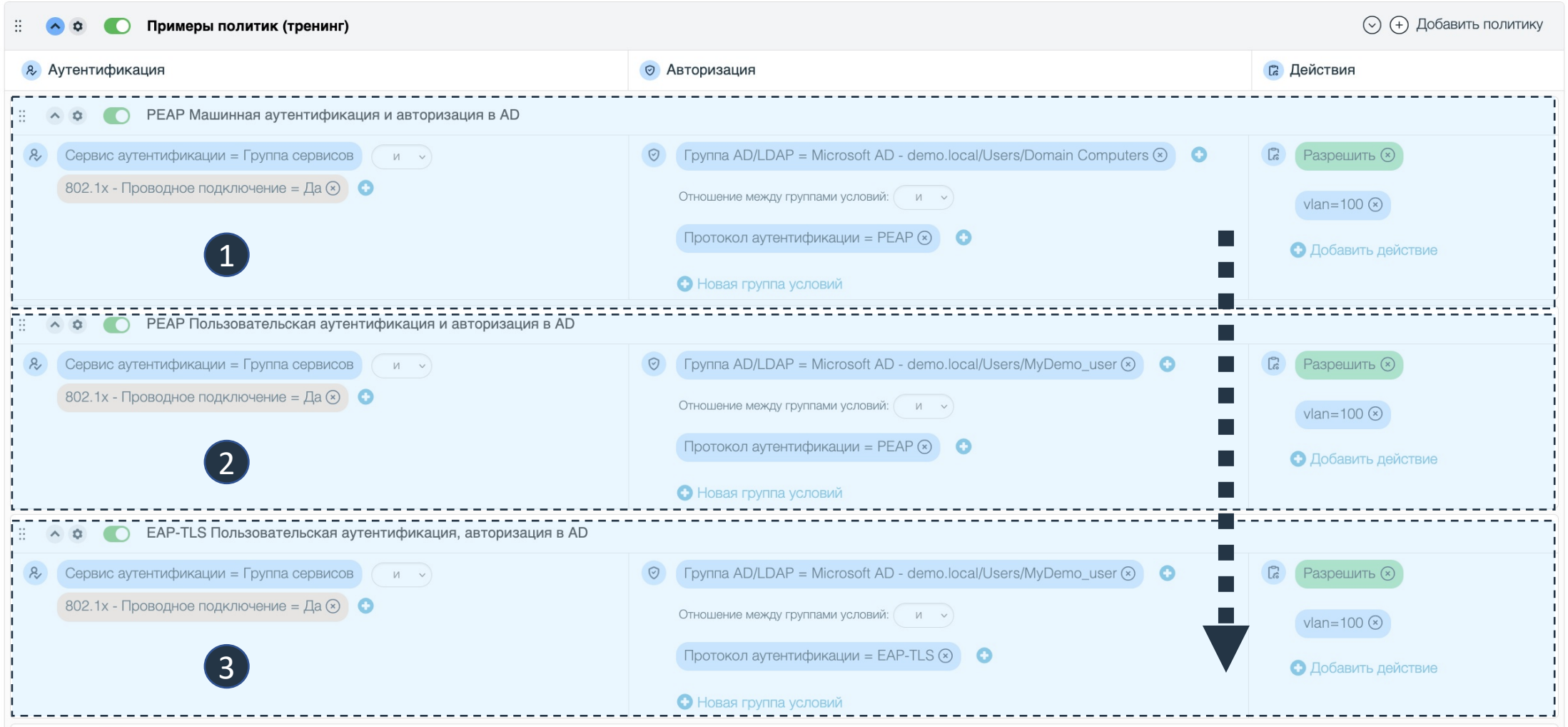
Гранулярность политик
Как устроены политики доступа



DECKAUTH

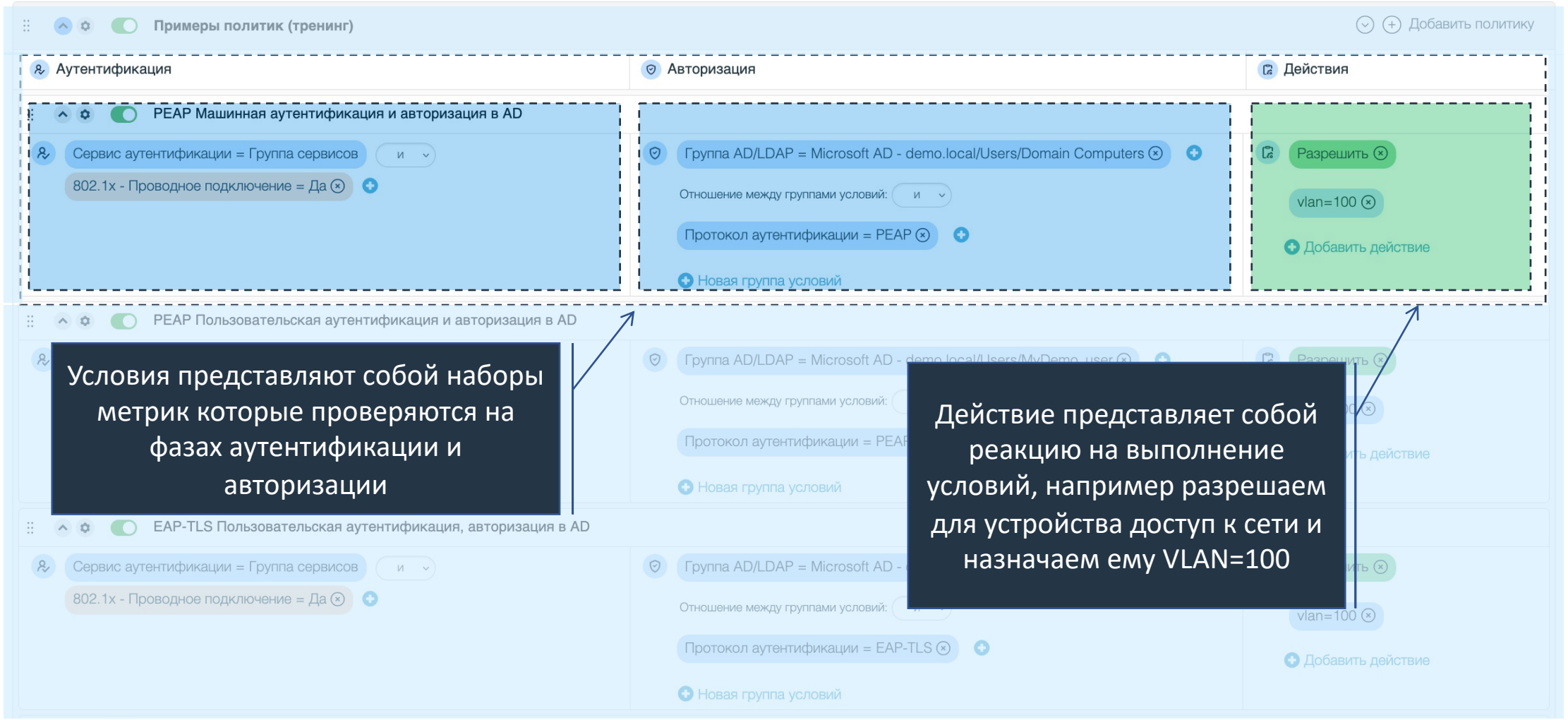
Гранулярность политик

Порядок выполнения правил сверху вниз = классический ACL



DECKAUTH

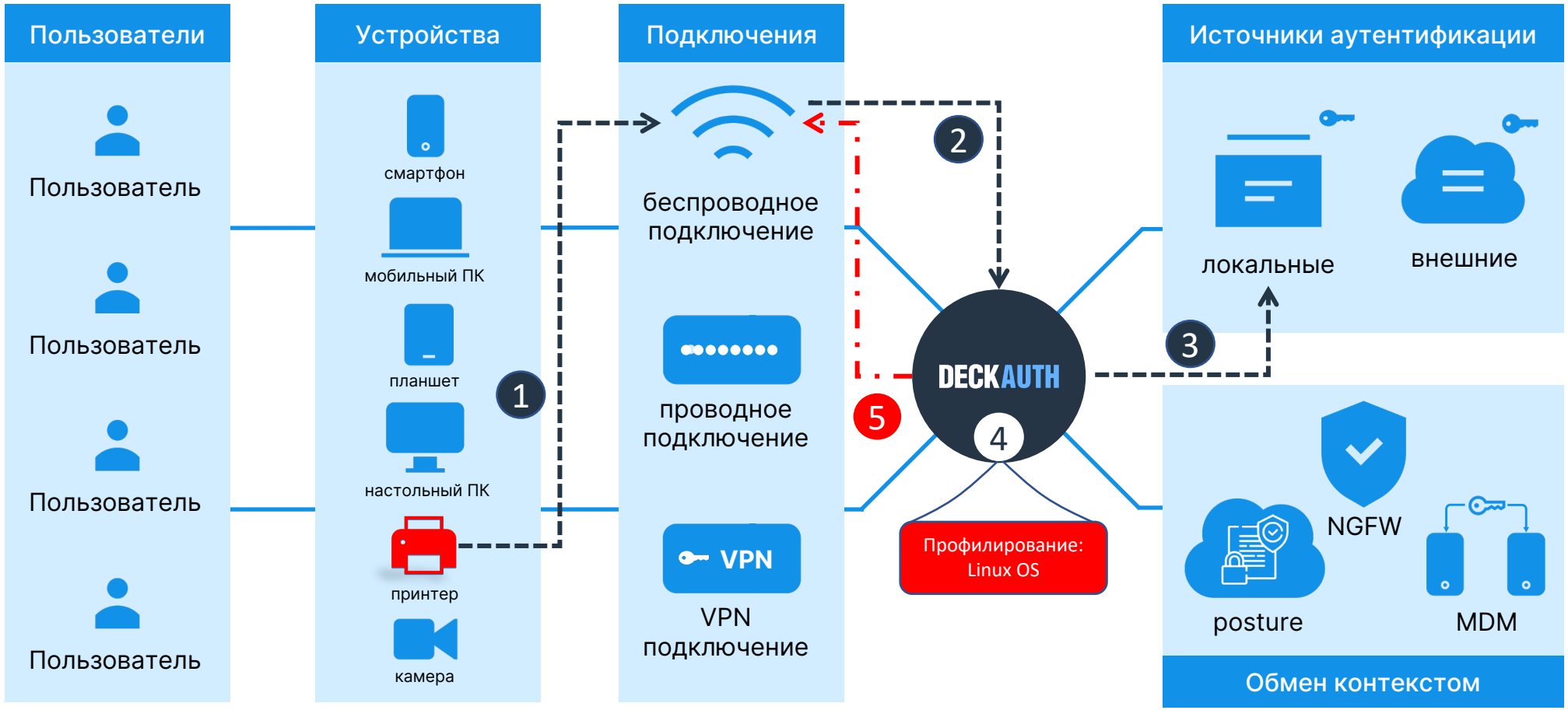
Гранулярность политик
Правило это комбинация условий и действий



DECKAUTH

Насколько гранулярной должна быть политика при внедрении NAC?

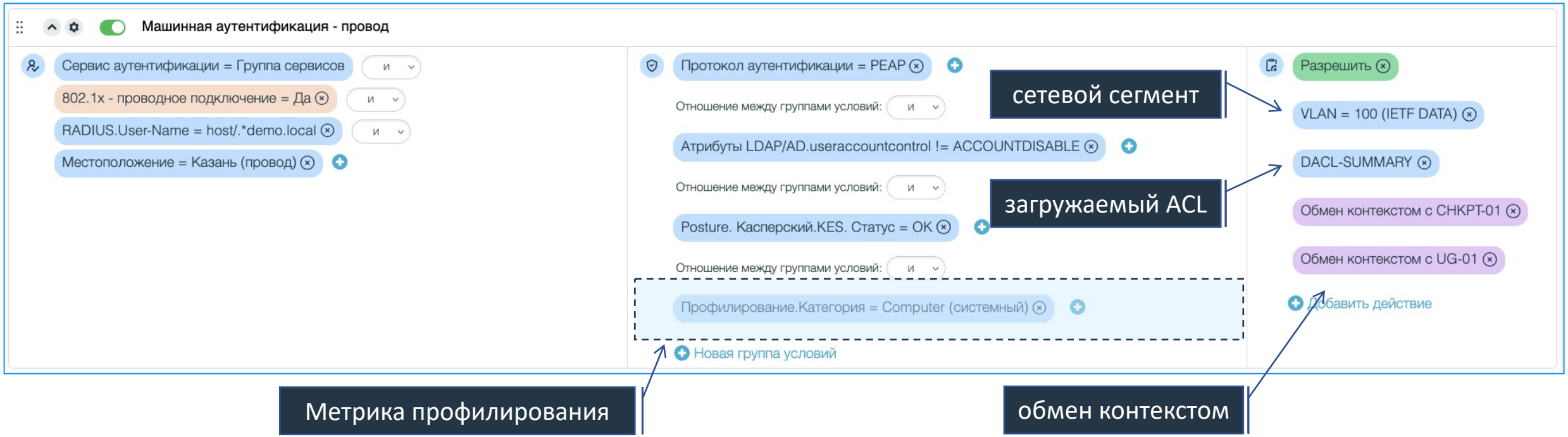
Разберем на примере профилирования



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

Гранулярность политик
Профилирование устройств



- По результату профилирования определяется «категория/семейство/устройство» конечного хоста, который подключается к сети
- Хосты без профилей или с профилями, которые не соответствуют политикам, подключаются в карантинный сегмент (см след. раздел об изменениях на сети), им назначаются ACL, происходит обмен контекстом с МСЭ/NGFW

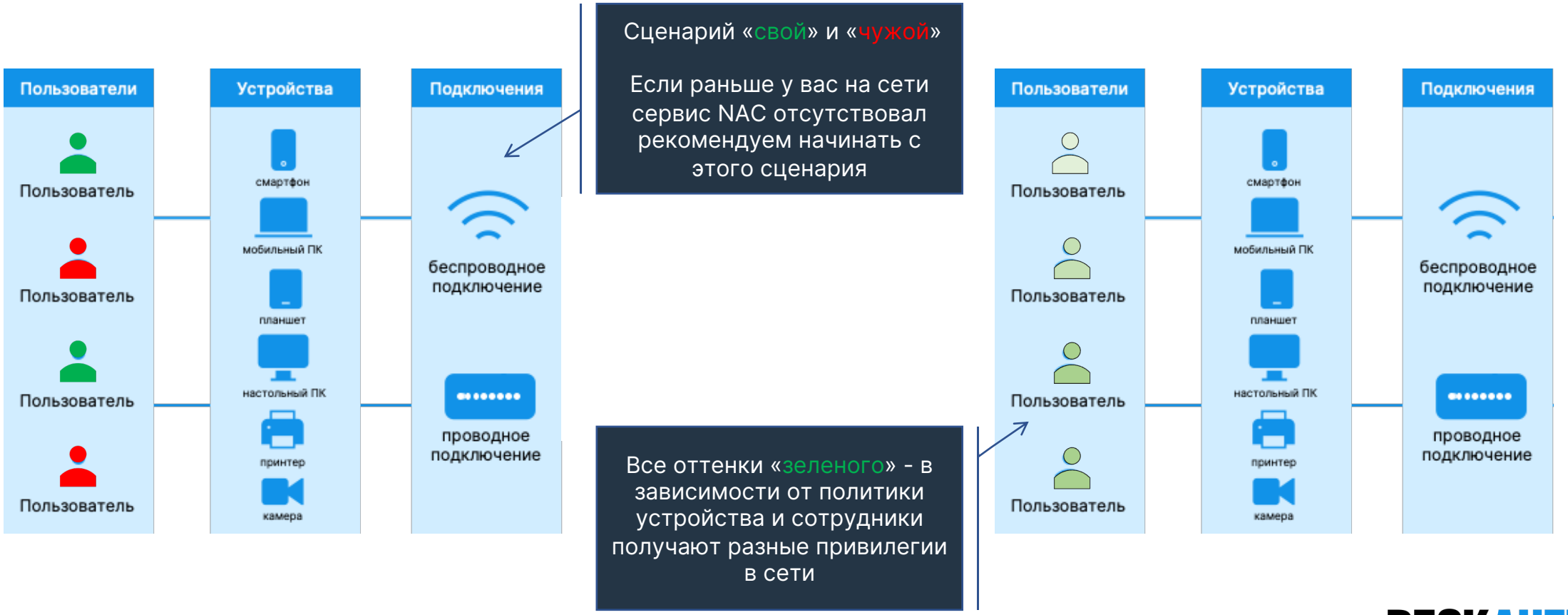
DECKAUTH

К чем ведет увеличение гранулярности политик?

- Увеличивается количество сегментов, в которые подключаются пользователи и устройства
  - макросегмент – VRF
  - сегмент – VLAN
- Увеличивается количество правил фильтрации на порту доступа
  - именованный ACL (RADIUS filter-id)
  - загружаемый ACL (RADIUS AV-pairs)
- Увеличивается количество контекста, которым система делится с МСЭ/NGFW
- Увеличивается сложность настройки системы
  - количество правил растет
  - усложняется поиск и устранение неисправностей

Общая рекомендация по гранулярности правил
Сначала базовый сценарий и только потом расширенный!

- Базовый сценарий
- Расширенный сценарий



DECKAUTH

Стратегия внедрения NAC

- Определить сценарии внедрения
  - Реализуем сценарий «в глубину» на всех портах, типах оборудования и клиентах
  - Реализуем сценарии «в ширину» - ни один метод доступа к сети не оставляем без контроля
- Гранулярность правил доступа
  - Начинать с базового сценария «свой» - «чужой»
  - Расширенный сценарий возможен только после подготовки изменений на сети

Изменения на уровне сети

Базовый минимум

Как может измениться дизайн сети при внедрении NAC?

Изменения на уровне сети
Базовый минимум

- Настройка RADIUS-сервера
  - активируем accounting
  - активируем динамическую авторизацию – отправку CoA или Disconnect

```
aaa new-model

aaa group server radius deck
 server name deck-cluster
 ip radius source-interface <идентификатор>

aaa authentication dot1x default group deck
aaa authorization network default group deck
aaa authorization network deck group deck

aaa accounting update periodic 10
aaa accounting include auth-profile framed-ip-address
aaa accounting dot1x default start-stop group deck

aaa server radius dynamic-author
 client <AUTH-VIP> server-key <ключ>

radius server deck-cluster
 address ipv4 <AUTH-VIP> auth-port 1812 acct-port 1813
 key <ключ>
```

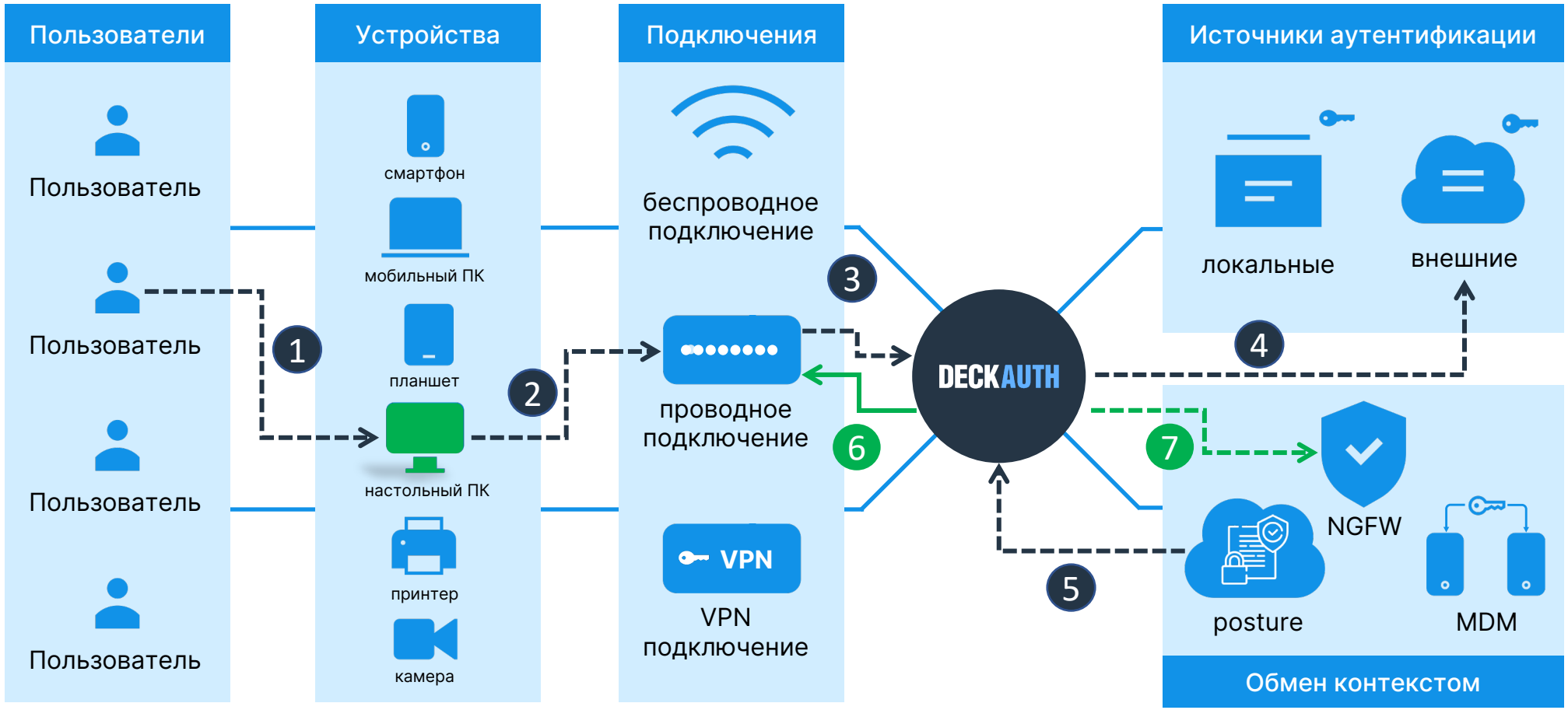
Изменения на уровне сети
Базовый минимум

- Настройка RADIUS-сервера
  - активируем dot1x
  - активирум MAB

```
interface <идентификатор порта>
 description 802.1x
 switchport access vlan <VLAN-по-умолчанию>
 ip device tracking maximum 10
 no ip address
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

Как может измениться дизайн сети при внедрении NAC?

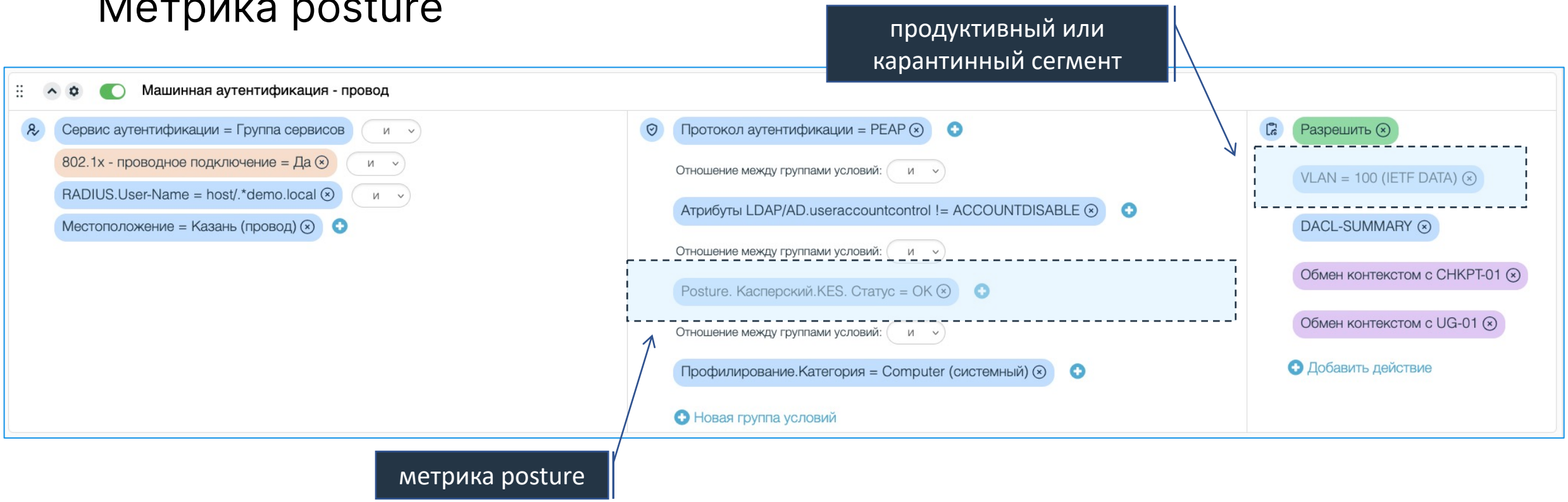
Разберем на примере posture



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

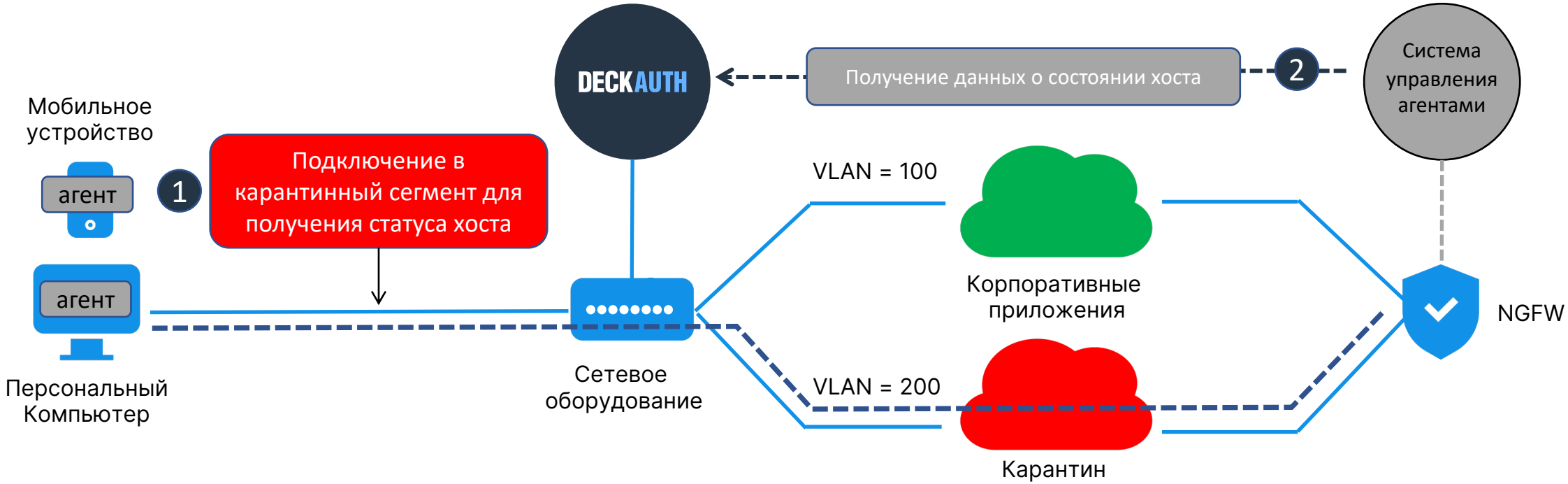
Гранулярность политик
Метрика posture



- По результату анализа состояния хоста назначается сегмент – продуктивный или карантинный
- Из карантинного сегмента должна быть обеспечена связанность с системой управления агентами

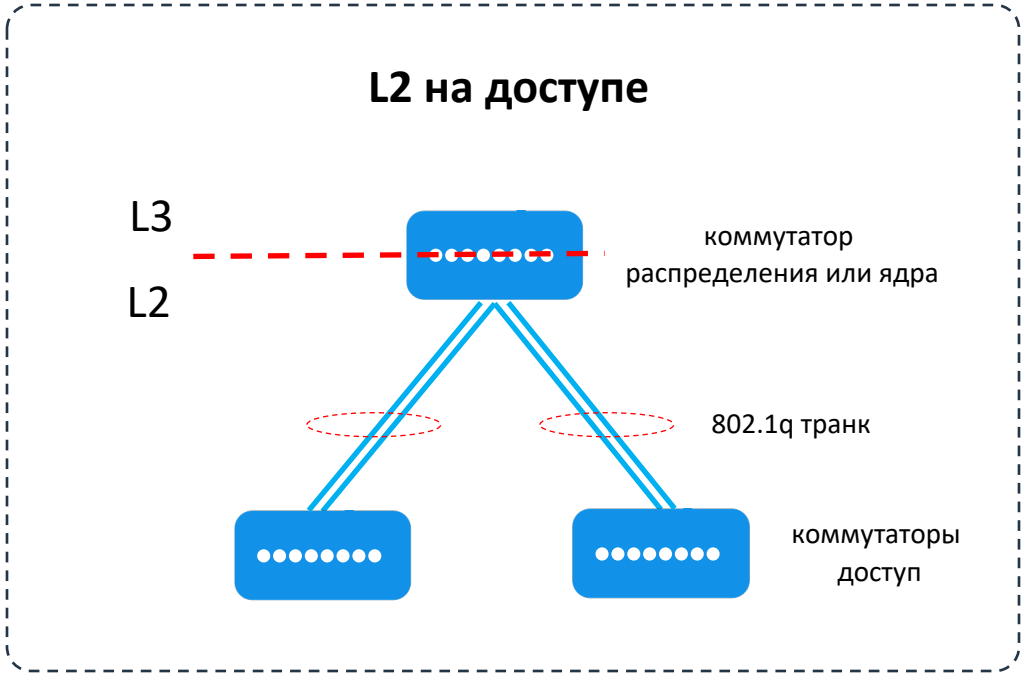
DECKAUTH

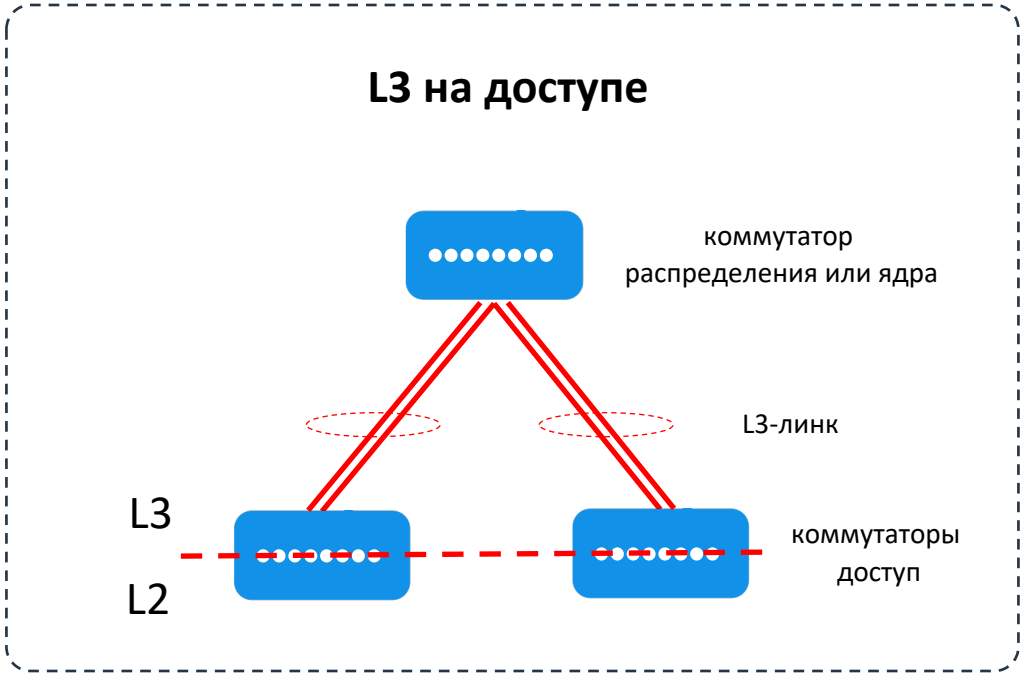
Posture (анализ состояния хоста)
Требует карантинный сегмент



- Первоначально хост подключается в карантинный сегмент, поскольку статус хоста от агента отсутствует
- Агент с хоста доставляет информацию о своем состоянии в централизованную систему управления агентами
- DECK AUTH получает данные о состоянии хоста из системы управления агентами

Как меняется дизайн сети при внедрении NAC?





- в 802.1q транки добавляются VLAN-ы
  - карантин, подрядчики, гости, etc.
- в точки терминации SVI-интерфейсов добавляются новые сегменты и механизмы фильтрации
  - VRF для карантина
  - ACL для сервисов
  - контекст МСЭ/NGFW

- на уровне доступа добавляются VLAN-ы
  - карантин, подрядчики, гости, etc.
- на уровне доступа настраиваются новые механизмы фильтрации
  - VRF для карантина
  - ACL для сервисов

Стратегия внедрения NAC

- Определить сценарии внедрения
  - Реализуем сценарий «в глубину» на всех портах, типах оборудования и клиентах
  - Реализуем сценарии «в ширину» - ни один метод доступа к сети не оставляем без контроля
- Гранулярность правил доступа
  - Начинать с базового сценария «свой» - «чужой»
  - Расширенный сценарий возможен только после подготовки изменений на сети
- Дизайн сети
  - Будьте готовы добавлять новые сегменты на уровне доступа
  - Продумайте стратегию изоляции трафика для них (ACL, VRF, МСЭ/NGFW)

Изменения на уровне конечных устройств

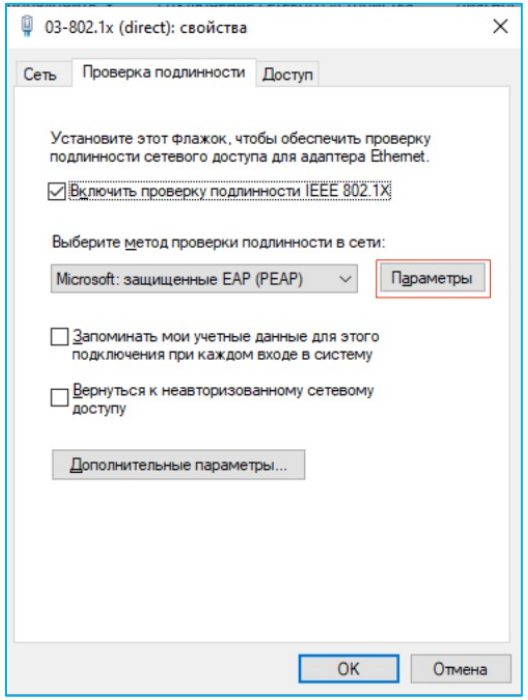
Базовый минимум

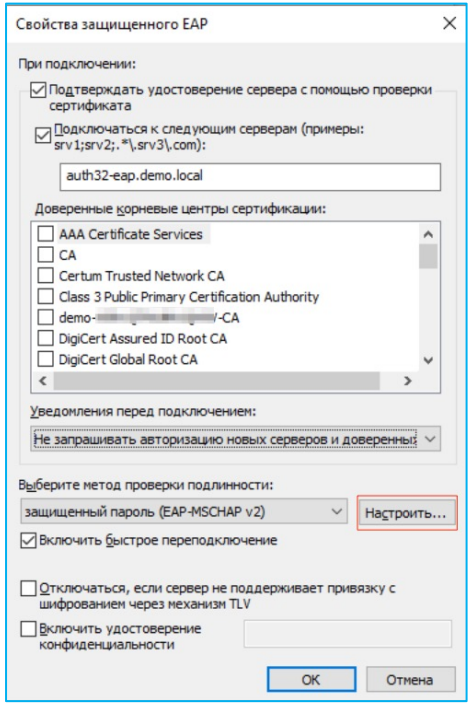
Какой контекст с устройств может использовать NAC?

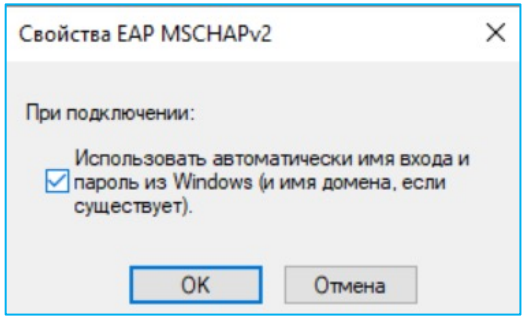
Изменения на уровне конечных хостов

Базовый минимум

- Активация 802.1x супликанта
  - Выписка и доставка сертификата
  - Настройка супликанта при помощи групповых политик или правил автоматизации







DECKAUTH

Какой контекст с устройств может использовать NAC?

Интеграция с SAFE MOBILE, НИИ СОКБ
Детальная информация о мобильном устройстве из MDM

Safe Mobile

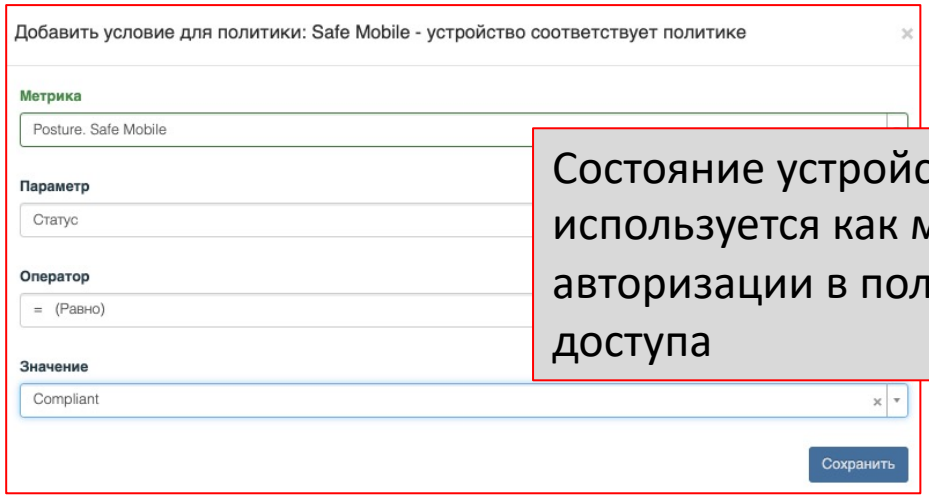
Общая информация

Название коннектора	SM SMM
Тип источника Posture	Safe Mobile
IP	192.168
UDID	a75
Тип устройства	Смартфон
Название модели устройства	realme RMX
Название ОС	Android
Версия ОС	14
Корпоративный идентификатор устройства	OJIC-IVQ4-(-Q3AB-M
Название ОШС (организационной штатной структуры)	DECK
Версия Safe Mobile	14.0.0.32
Имя владельца устройства	
Время последней активности	2026-04-16T05:12:26.408089
Время последней синхронизации с источником Posture	2026-04-16 08:17:01
Время регистрации устройства	-
Данные пришли из Accounting-сообщения	Нет

Статусы устройства

Статус	Compliant
Статус блокировки устройства	Не заблокирован
Статус управления устройством	Находится под управлением
Статус соединения	В сети

Получение деталей о типе, модели, версии устройства



Состояние устройства в MDM используется как метрика авторизации в политике доступа

Статус соответствия мобильного устройства корпоративным политикам

Стратегия внедрения NAC

- Определить сценарии внедрения
  - Реализуем сценарий «в глубину» на всех портах, типах оборудования и клиентах
  - Реализуем сценарии «в ширину» - ни один метод доступа к сети не оставляем без контроля
- Гранулярность правил доступа
  - Начинать с базового сценария «свой» - «чужой»
  - Расширенный сценарий возможен только после подготовки изменений на сети
- Дизайн сети
  - Будьте готовы добавлять новые сегменты на уровне доступа
  - Продумайте стратегию изоляции трафика для них (ACL, VRF, МСЭ/NGFW)
- Задействуйте сбор информации с существующих хостов
  - End Point Security / End Point Protection
  - Mobile Device Management


DECK AUTH
https://auth.deck.lc