Мониторинг рабочих мест как решение проблемы «нулевого доверия»

Семён Жейда, руководитель направления ИБ компании «ИТ-Экспертиза»

17.02.2021

Сакура

IT EXPERTISE

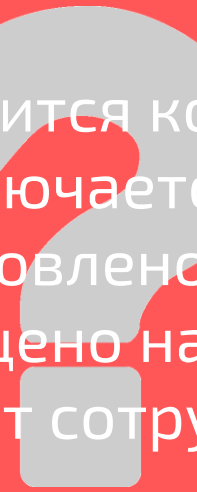
Типичная ситуация в ИБ

Сервер защищен и контролируется

Периметр защищен и контролируется

Внешние компьютеры – слабо защищены и слабо контролируются

ГДЕ находится компьютер
КАК подключается компьютер
ЧТО установлено на компьютере
ЧТО запущено на компьютере
ЧТО делает сотрудник/фрилансер

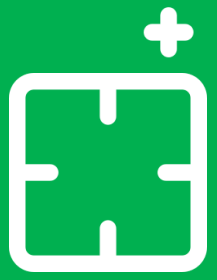


Сакура

IT EXPERTISE

Доверенный периметр

Понятие доверенного периметра фактически исчезло



Необходимо научиться доверять внешним рабочим местам и внешним пользователям

Принцип «нулевого доверия»

1

Отсутствие доверия

Полное отсутствие доверия рабочим местам и пользователям (в том числе внутри периметра)

2

Проверка

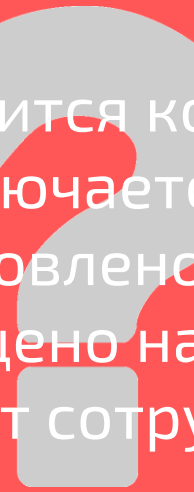
Пользователи и устройства должны проходить проверку при доступе к ресурсам и во время работы с ресурсами

Проблема «нулевого доверия»

Сервер защищен и контролируется

Периметр защищен и контролируется

Внешние компьютеры – слабо защищены и слабо контролируются



ГДЕ находится компьютер
КАК подключается компьютер
ЧТО установлено на компьютере
ЧТО запущено на компьютере
ЧТО делает сотрудник/фрилансер

Сакура

IT EXPERTISE

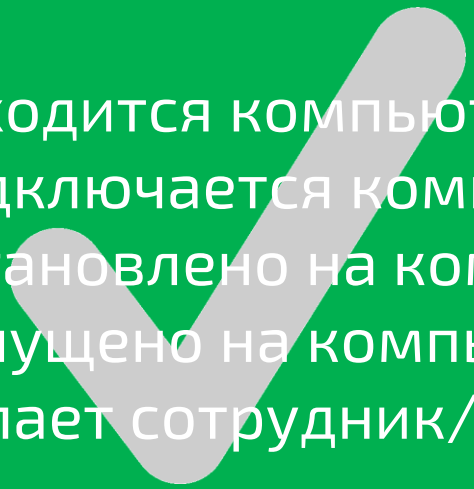
Проблема «нулевого доверия»

Сервер защищен и контролируется

Периметр защищен и контролируется

Внешние компьютеры – защищены и контролируются

ГДЕ находится компьютер
КАК подключается компьютер
ЧТО установлено на компьютере
ЧТО запущено на компьютере
ЧТО делает сотрудник/фрилансер



Что значит «доверять»?

Требуется инструмент, позволяющий в режиме реального времени:

1) **Контролировать** политики ИБ:

Программное и аппаратное обеспечение

Настройку ОС

Установку, настройку, актуальность ПО, в том числе СЗИ

Тип и состав USB устройств

Запущенные в ОС процессы

Logon/logoff пользователей

2) **Управлять** рабочим местом (уведомление, блокировка доступа, карантин)

Сакура

IT EXPERTISE

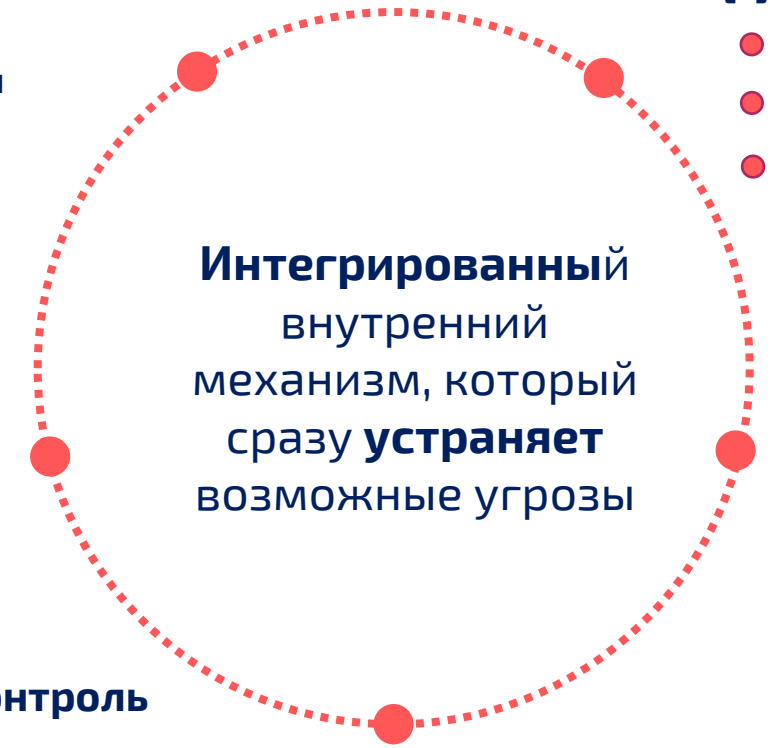
Как решить проблему

Нужно средство мониторинга защищенности и контроля технических параметров ИБ рабочих мест и серверов, которое обеспечит доверенную среду обработки защищаемой информации в режиме 24/7.

Сакура

IT EXPERTISE

Обеспечение доверенной среды



[5] Управление

- Политики безопасности
- Отчётность
- Интеграция

[1] Мониторинг

- Нарушения
- Комплаенс
- Идентификация

[4] Реагирование

- Устранение нарушений
- Автоматическое реагирование
- Ограничение доступа

[2] Регистрация

- Требования ГосСОПКА
- Инвентаризация
- Доступы
- Совместимость
- Подключения

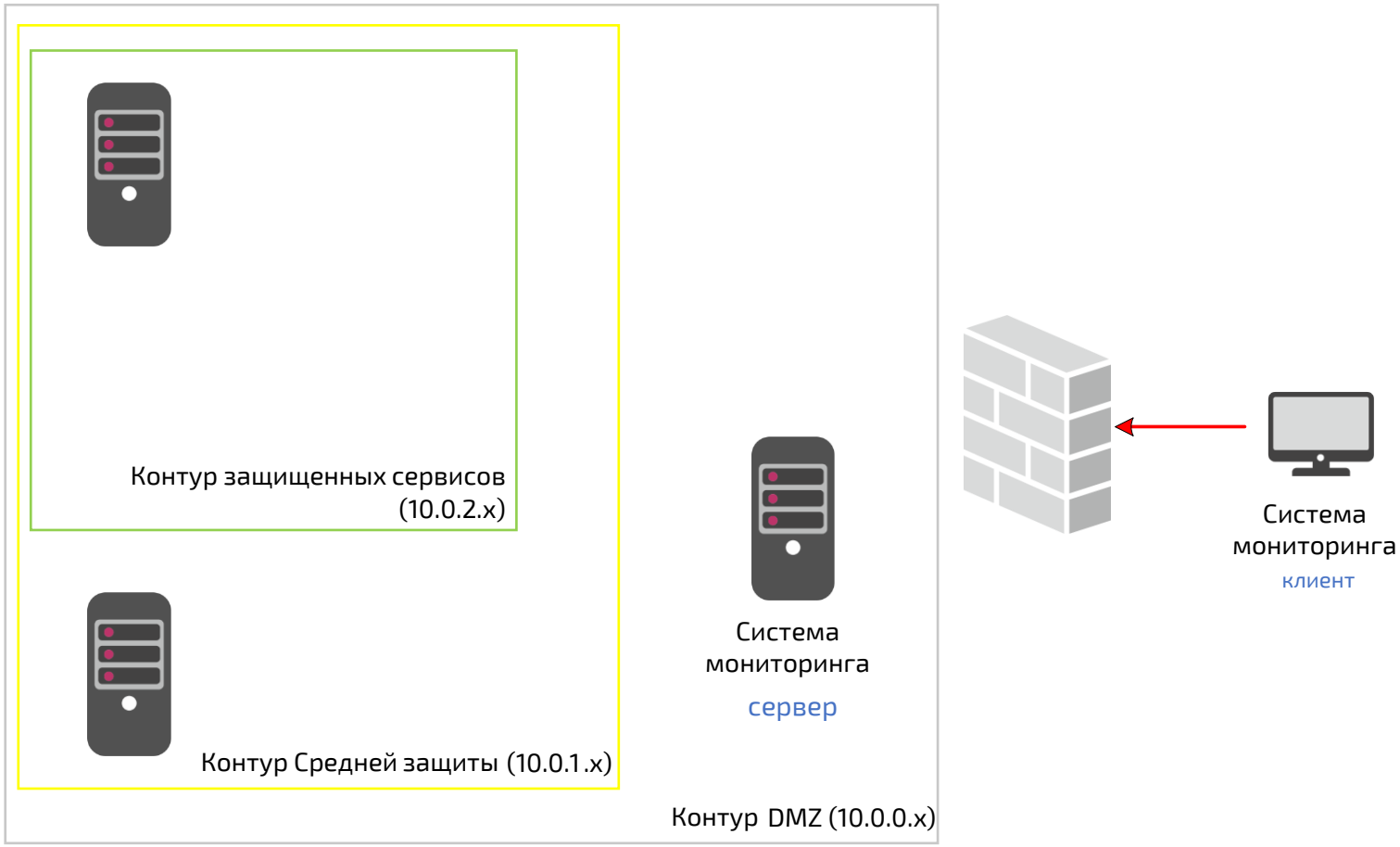
[3] Контроль

- Контроль цикла событий
- Всё на одном экране

Сакура

IT EXPERTISE

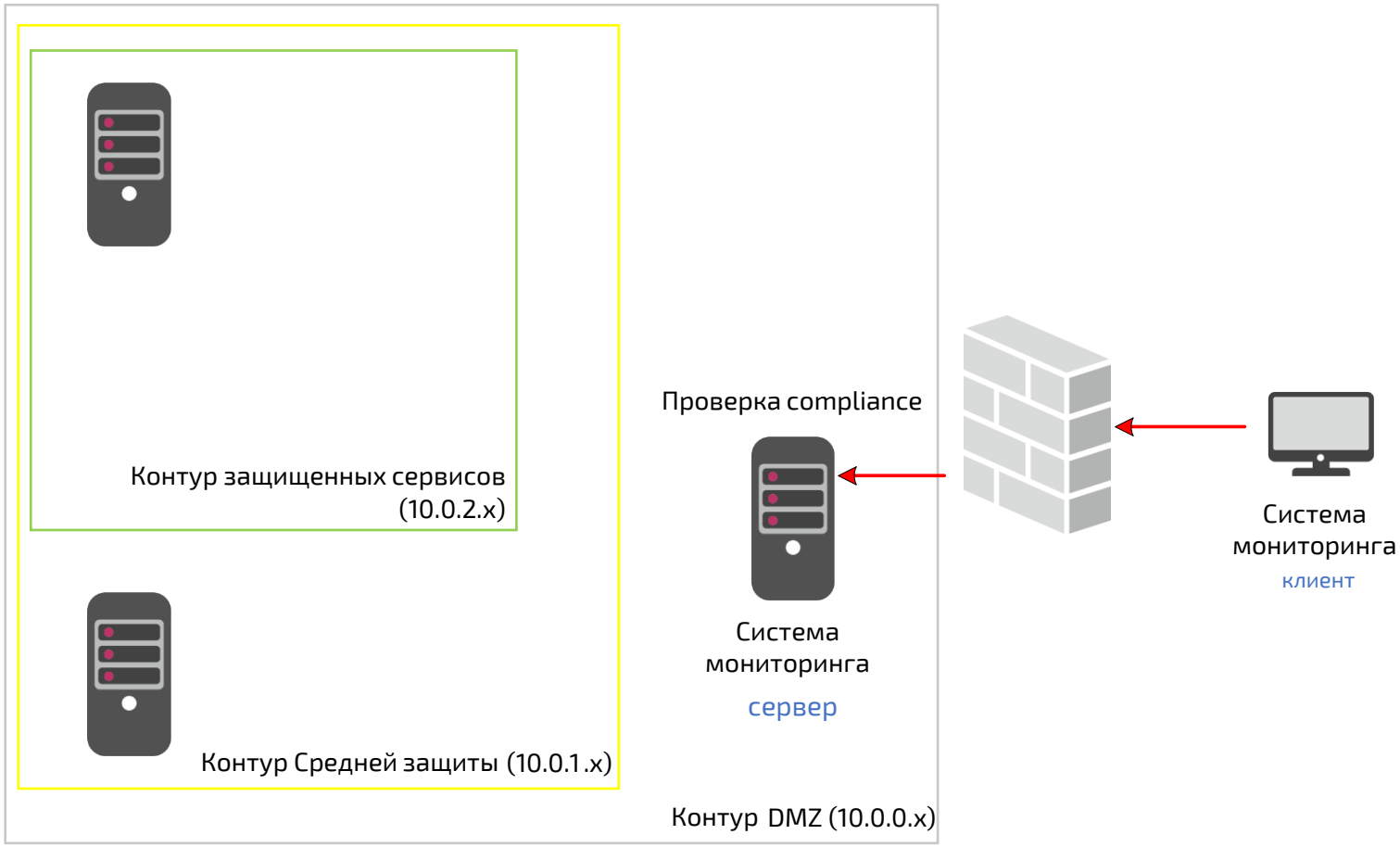
Концепция нулевого доверия



Сакура

IT EXPERTISE

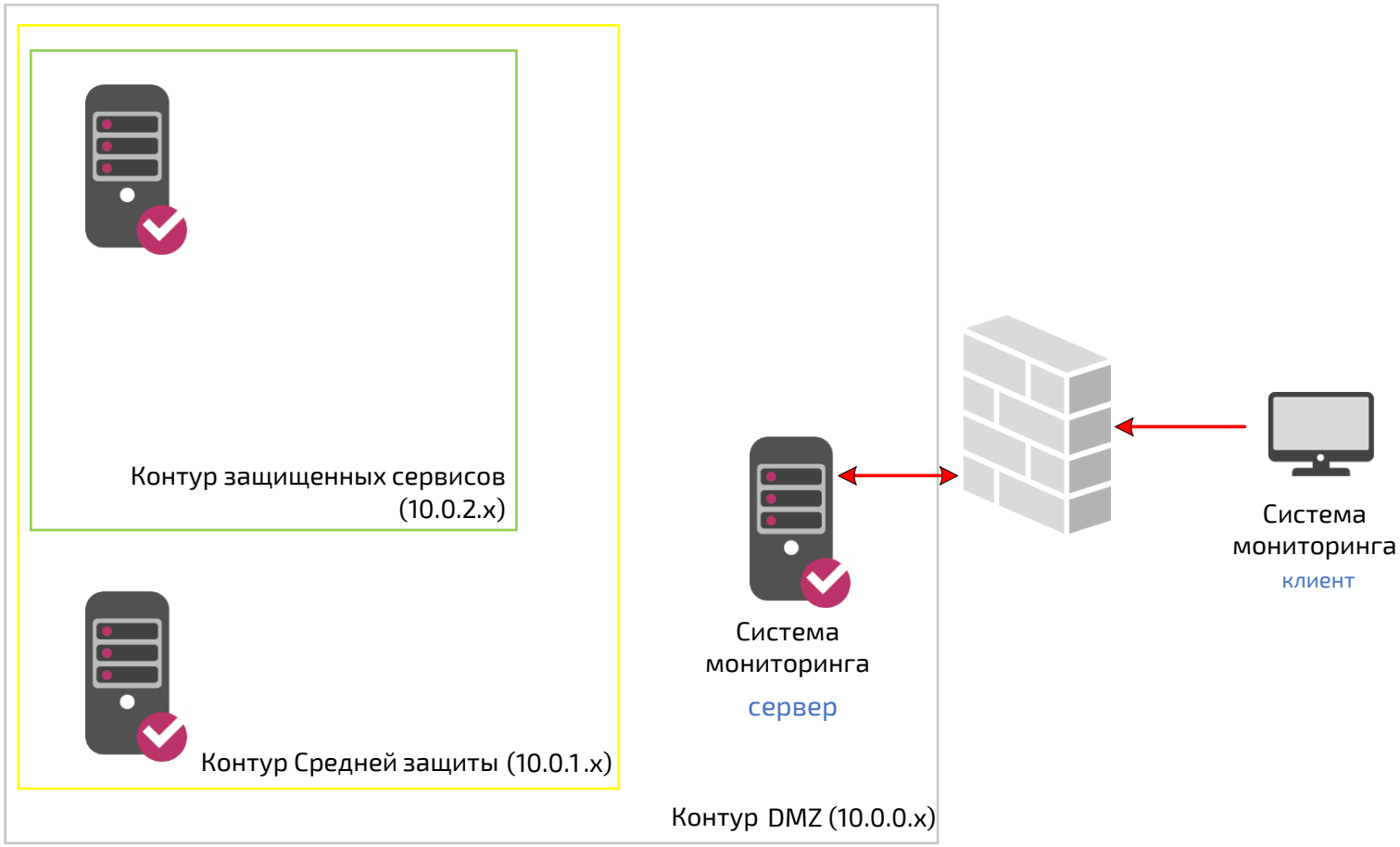
Концепция нулевого доверия



Сакура

IT EXPERTISE

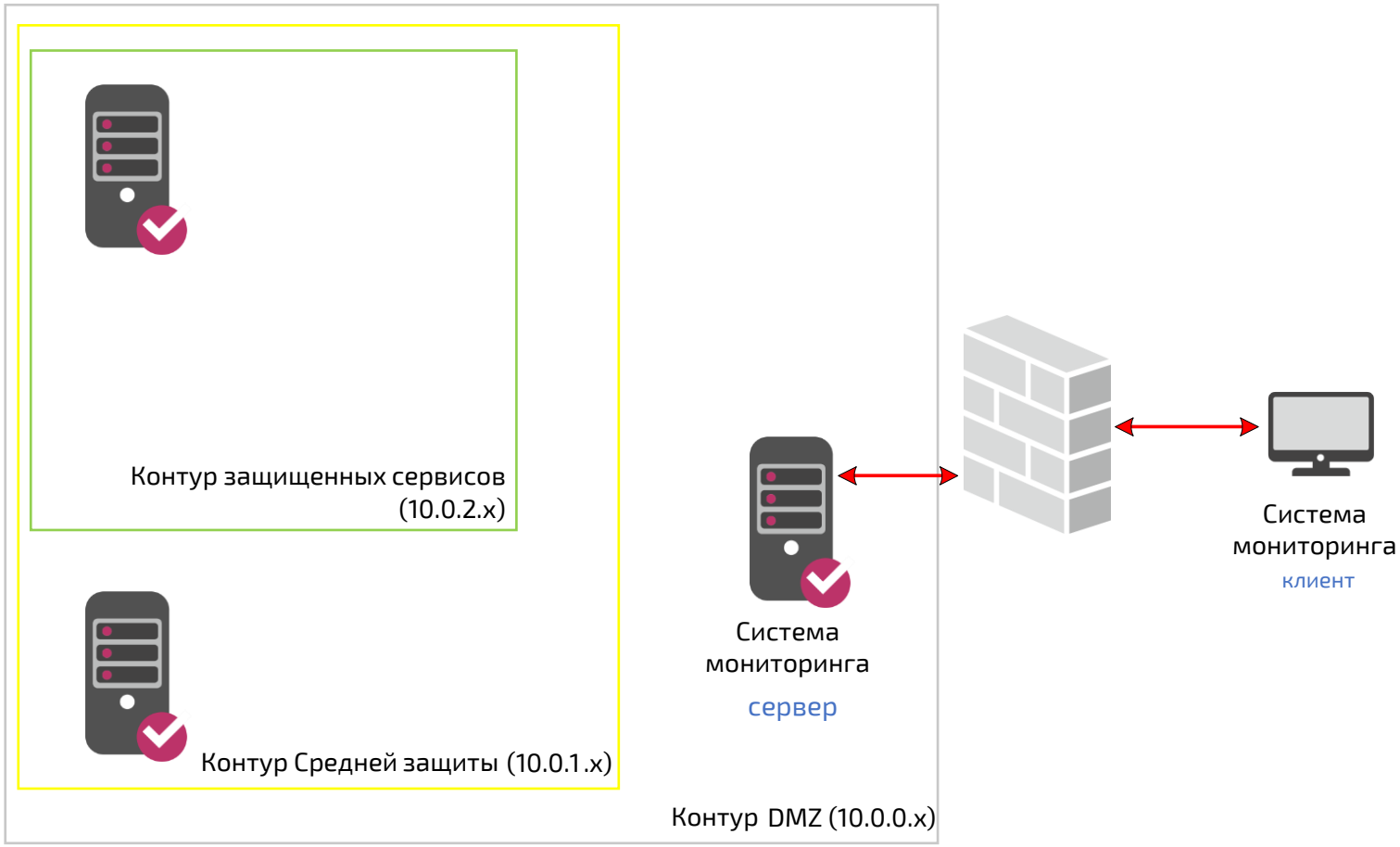
Концепция нулевого доверия



Сакура

IT EXPERTISE

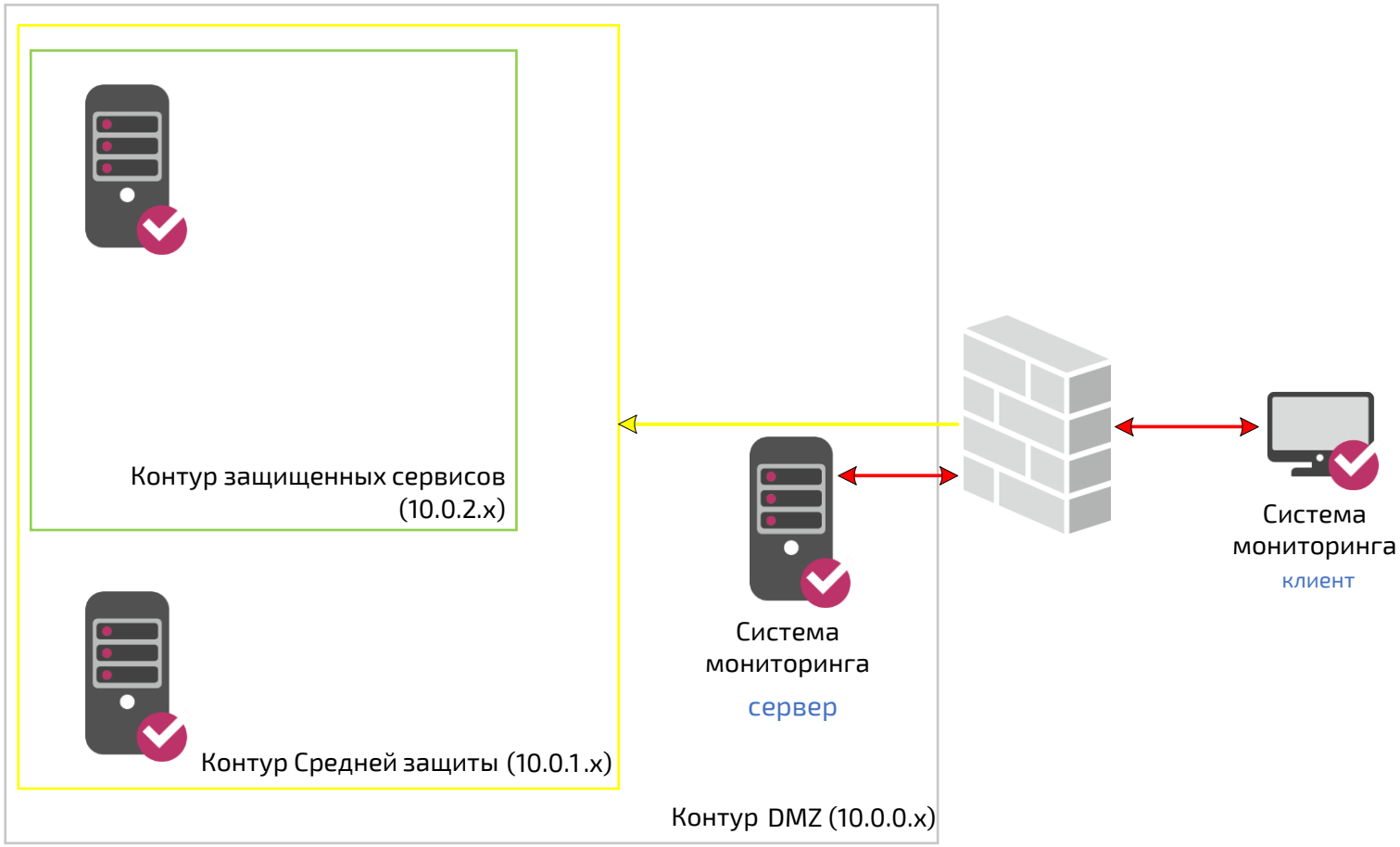
Концепция нулевого доверия



Сакура

IT EXPERTISE

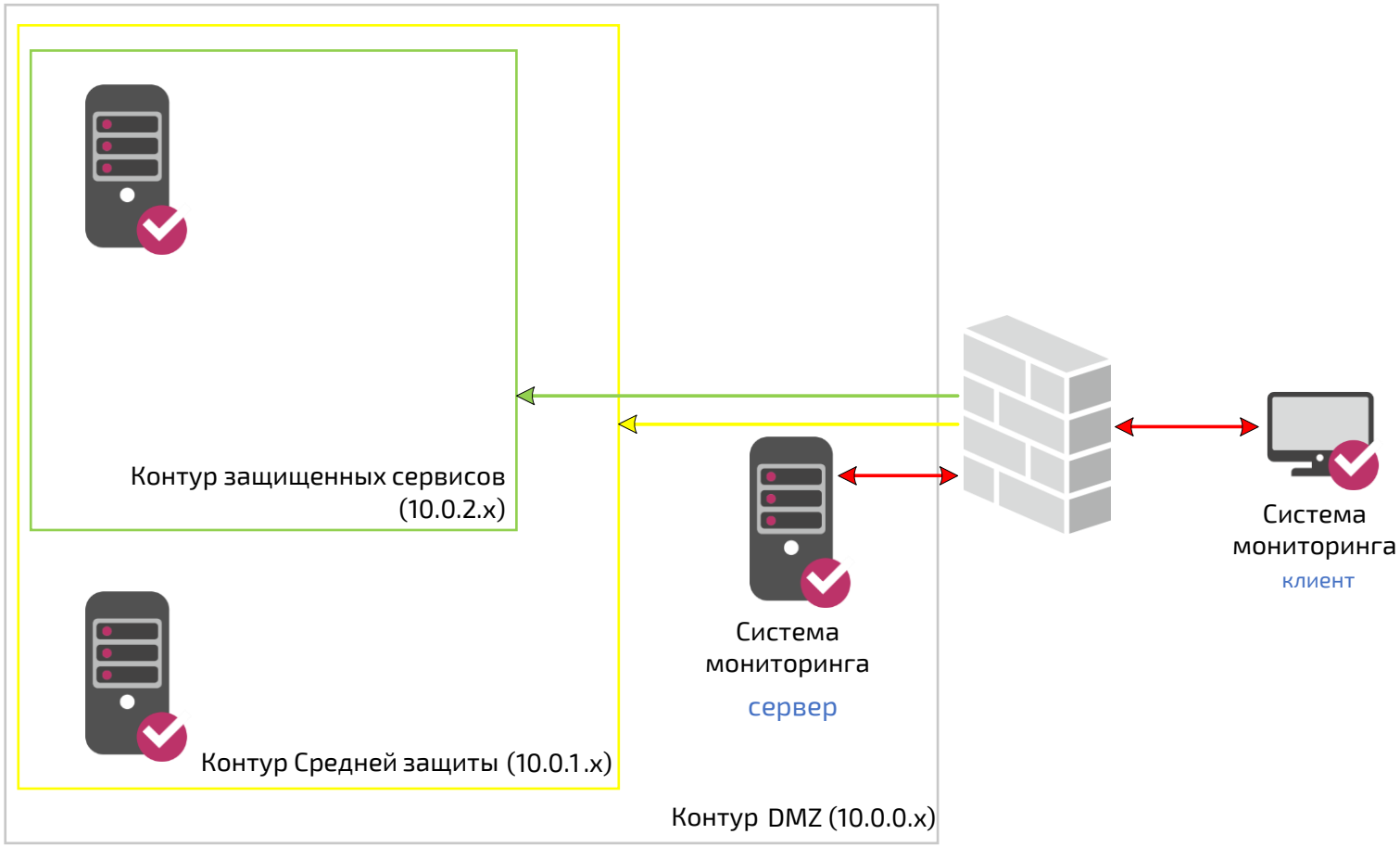
Концепция нулевого доверия



Сакура

IT EXPERTISE

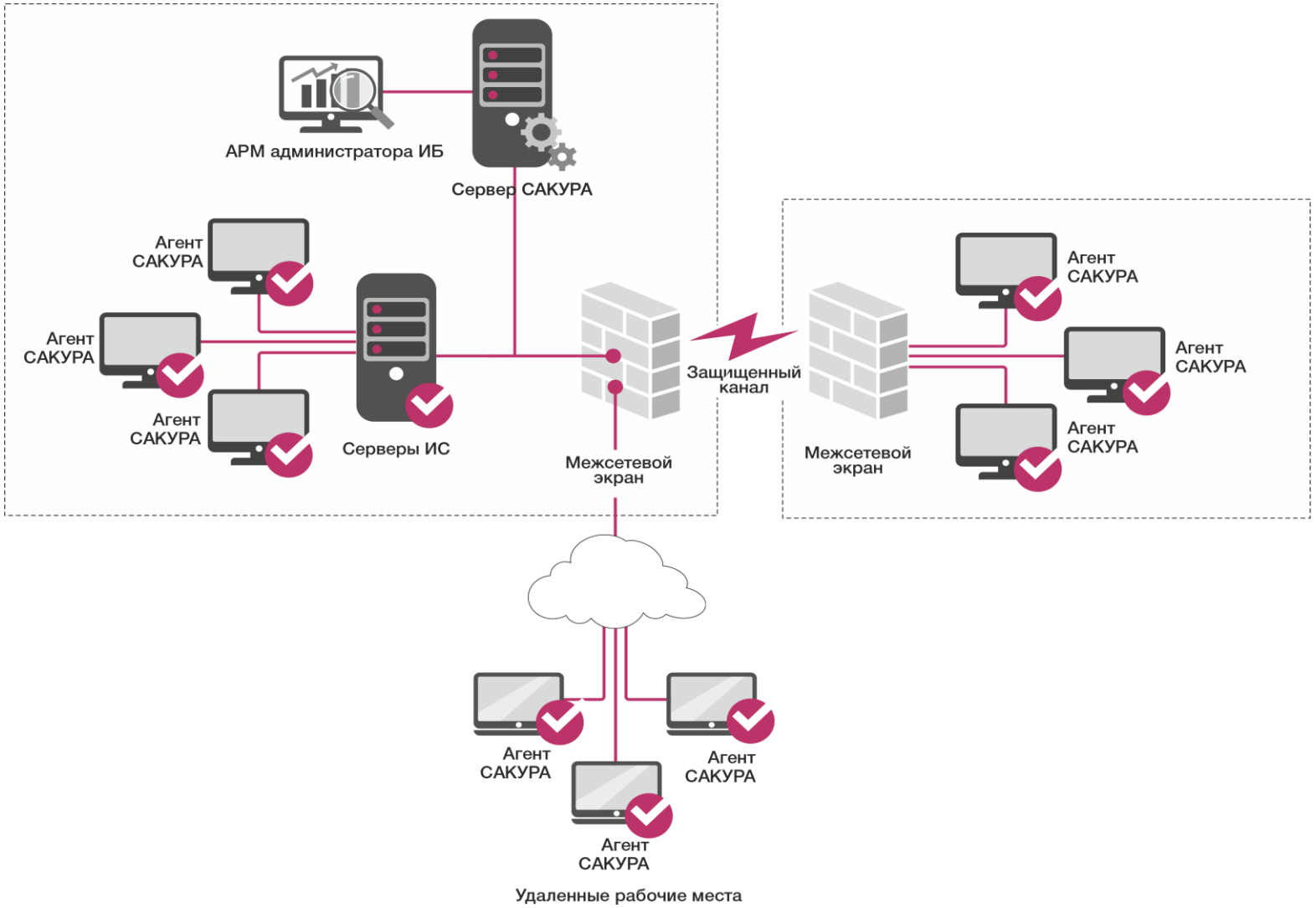
Концепция нулевого доверия



Сакура

IT EXPERTISE

Типовая схема развертывания



Сакура

IT EXPERTISE

О компании «ИТ-Экспертиза»

Решения компании «ИТ-Экспертиза» в области информационной безопасности:

САКУРА – программный комплекс информационной безопасности

Консалтинг по информационной безопасности — аудит и разработка рекомендаций по совершенствованию систем информационной безопасности (ГИС, КИИ, персональные данные), подготовка необходимой документации для регуляторов.

1С:Интеграция КОРП – сервисная шина предприятия (ESB) корпоративного уровня, с универсальным коннектором 1С и открытым кодом

Технологические услуги компании «ИТ-Экспертиза» для решений на платформе 1С :

Корпоративные информационно-техническое сопровождение

Отказоустойчивость и поддержка

Повышение производительности

Разработка на платформе «1С: Предприятие»

В нашем портфеле клиентов: