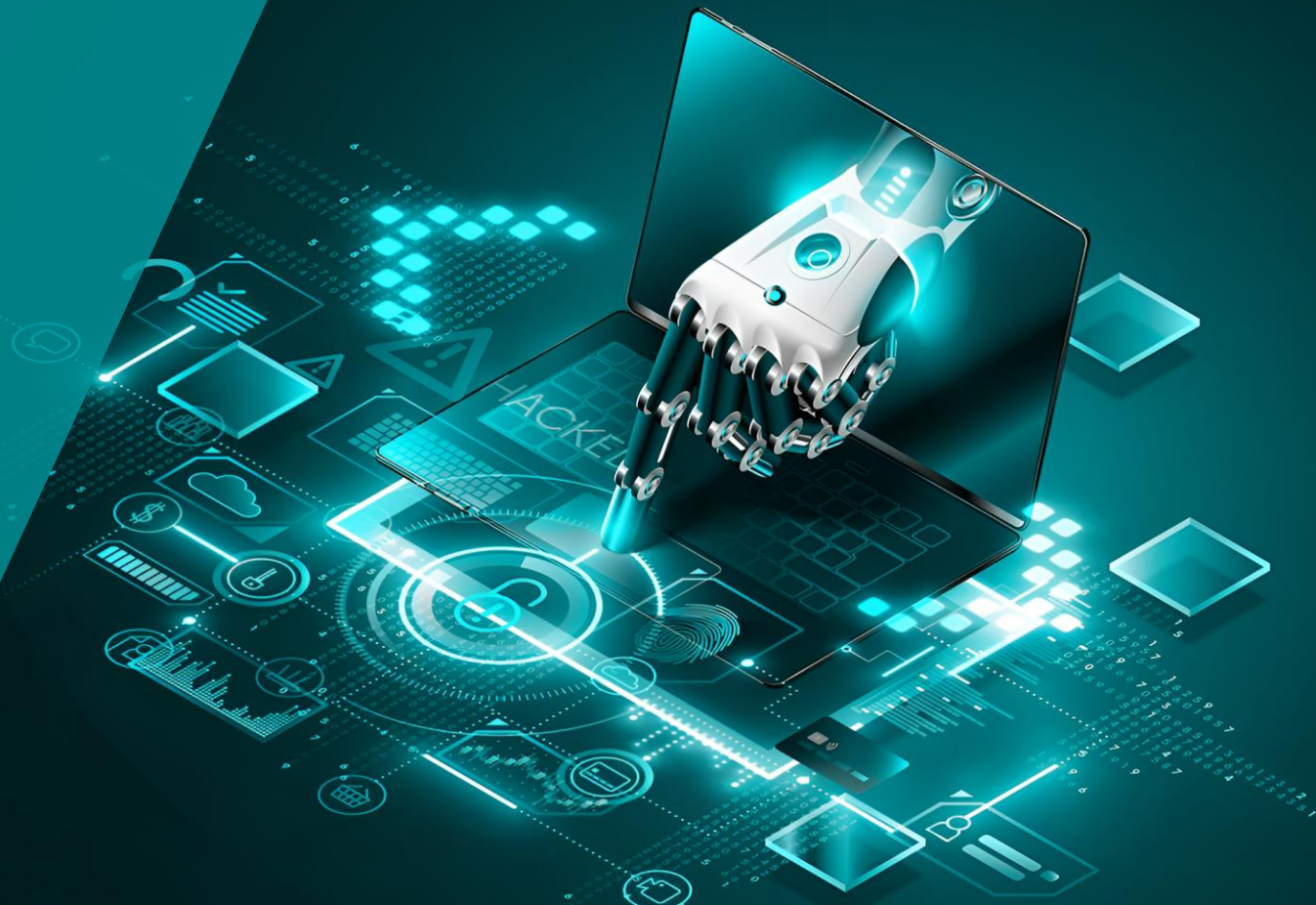


АРХИТЕКТУРА ЗАЩИТЫ УДАЛЕННОГО ДОСТУПА: КАК ПОСТРОИТЬ ЭФФЕКТИВНЫЙ КОМПЛЕКС СИСТЕМ

Владимир Арышев
Эксперт по комплексным проектам
информационной безопасности



Владимир Арышев

Эксперт по комплексным проектам
информационной безопасности STEP LOGIC

15 лет в сфере информационной безопасности.

Имеет опыт работы с различными классами решений – от сетевой безопасности до DevSecOps. С 2022 года отвечает за развитие комплексных проектов информационной безопасности в компании STEP LOGIC.

Обладает экспертизой по созданию систем информационной безопасности заказчиков компании.



Содержание

- 1 Типы удаленного доступа
- 2 Пользователи
- 3 Инфраструктура корпоративной сети

Типы удаленного доступа. Клиентский доступ

Устройство пользователя оказывается во внутренней сети компании. Требуется специализированное ПО либо встроенный в ОС клиент.

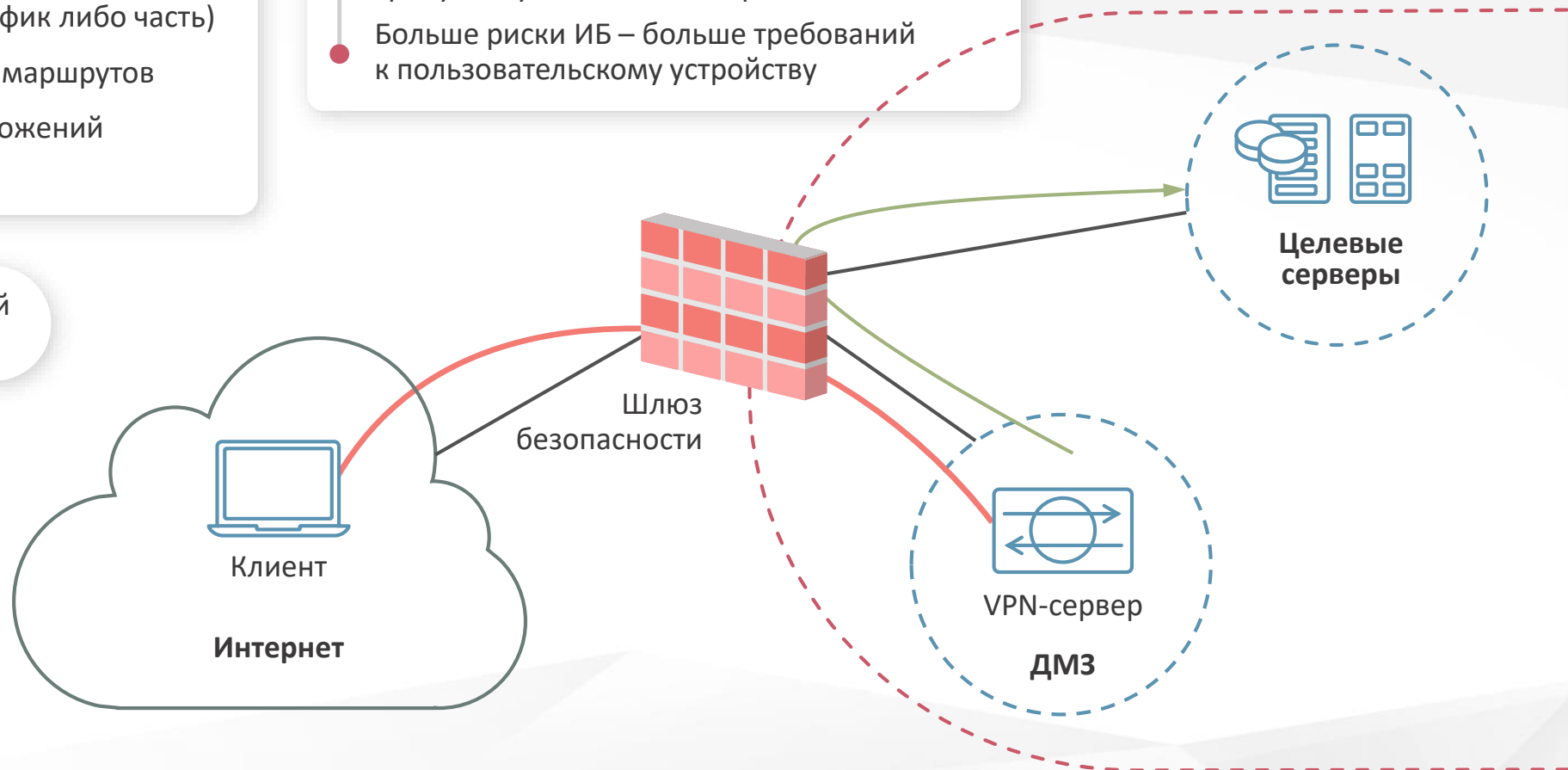
Плюсы

- Полноценный сетевой туннель (маршрутизируется весь трафик либо часть)
- Гибкая настройка политик и маршрутов
- Поддержка всех типов приложений (не только веб)

Частный случай – защищенный корпоративный контейнер.

Минусы

- Требуется установка и настройка клиента
- Больше риски ИБ – больше требований к пользовательскому устройству



Типы удаленного доступа. Бесклиентский доступ

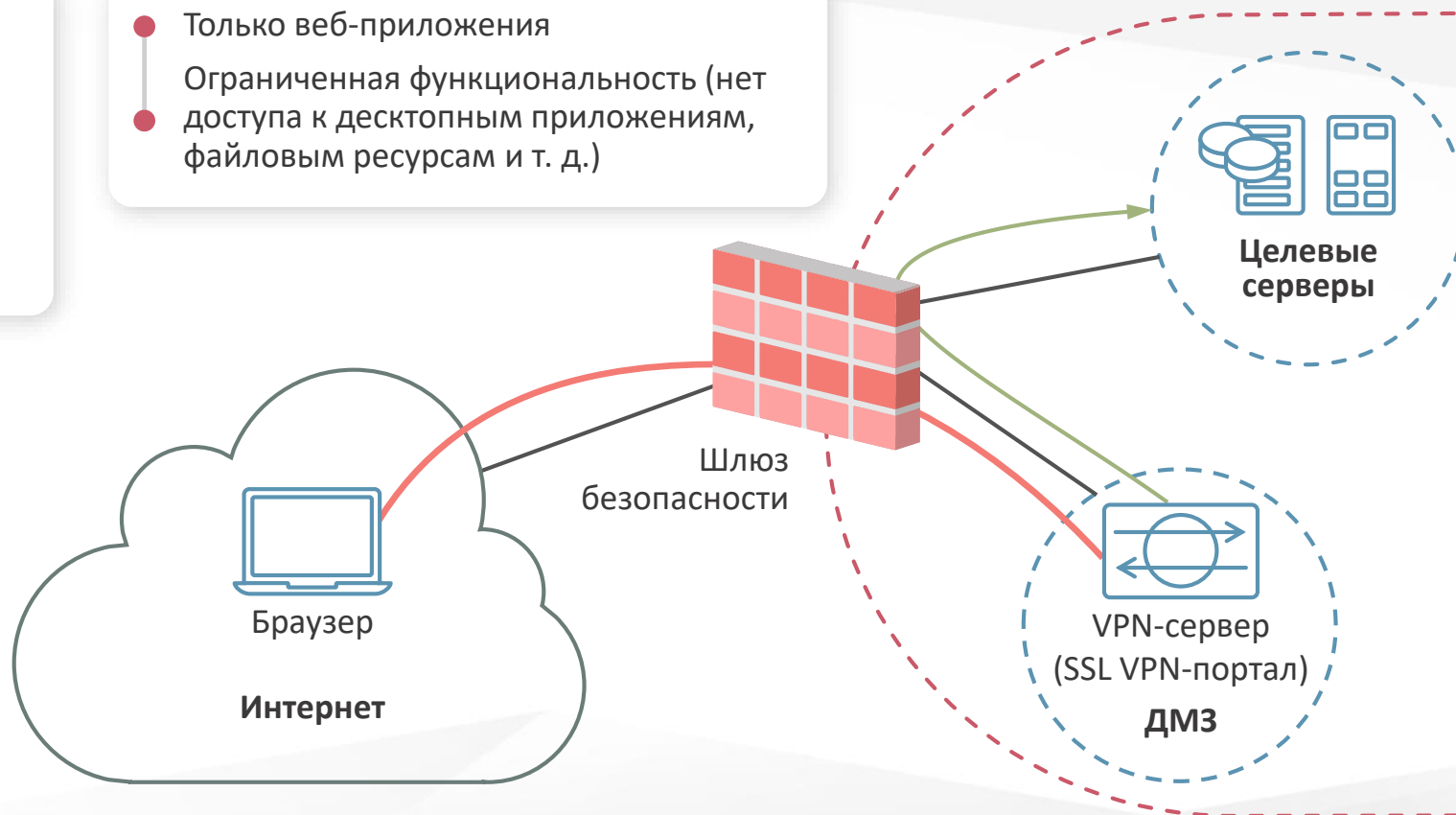
Пользователь подключается к веб-приложениям при помощи браузера.
Веб-приложения опубликованы на VPN-сервере (SSL VPN-портале).

Плюсы

- Удобство для внешних пользователей и подрядчиков
- Быстрое подключение «из любого места» через браузер
- Нет необходимости устанавливать и настраивать дополнительное ПО

Минусы

- Только веб-приложения
- Ограниченная функциональность (нет доступа к десктопным приложениям, файловым ресурсам и т. д.)



Пользователи

Интеграция с LDAP

- Получение информации о пользователях: имя, логин, принадлежность к группам, роли и пр.
- Централизованное управление правами доступа через существующую корпоративную инфраструктуру

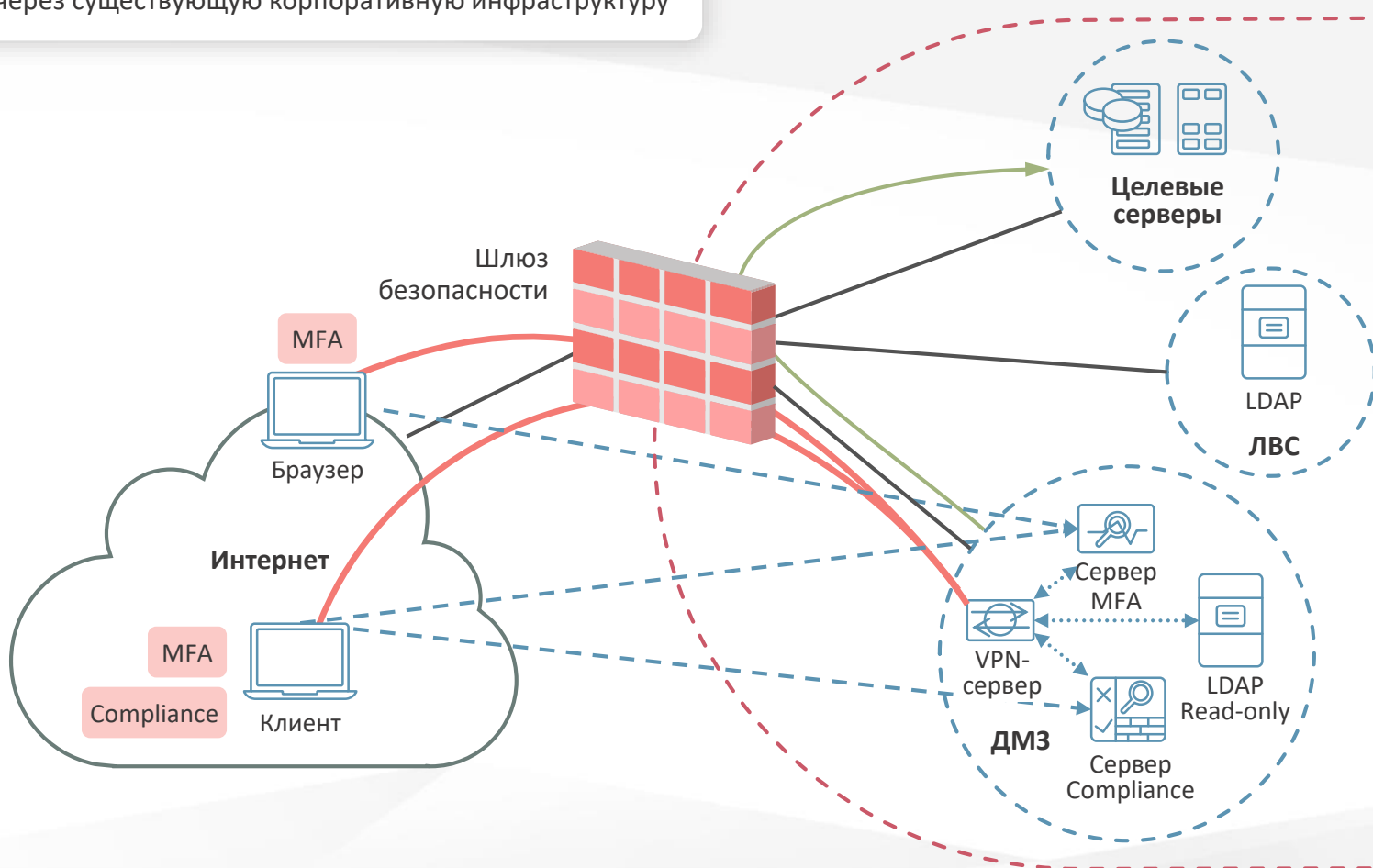
Интеграция с MFA*

- Добавляет второй фактор при подключении (например, OTP-код, push-уведомление или аппаратный токен)
- Значительно снижает риски при компрометации пароля

Интеграция с Compliance-системами

для проверки конечного устройства перед допуском в сеть на соответствие политике ИБ:

- наличие антивируса,
- обновления ОС,
- включён ли firewall,
- зашифрован ли диск.



* системами многофакторной аутентификации

Инфраструктура корпоративной сети. Прямой доступ

После установления VPN-соединения весь трафик пользователя расшифровывается на VPN-сервере и направляется напрямую к целевым системам в сети.

Плюсы

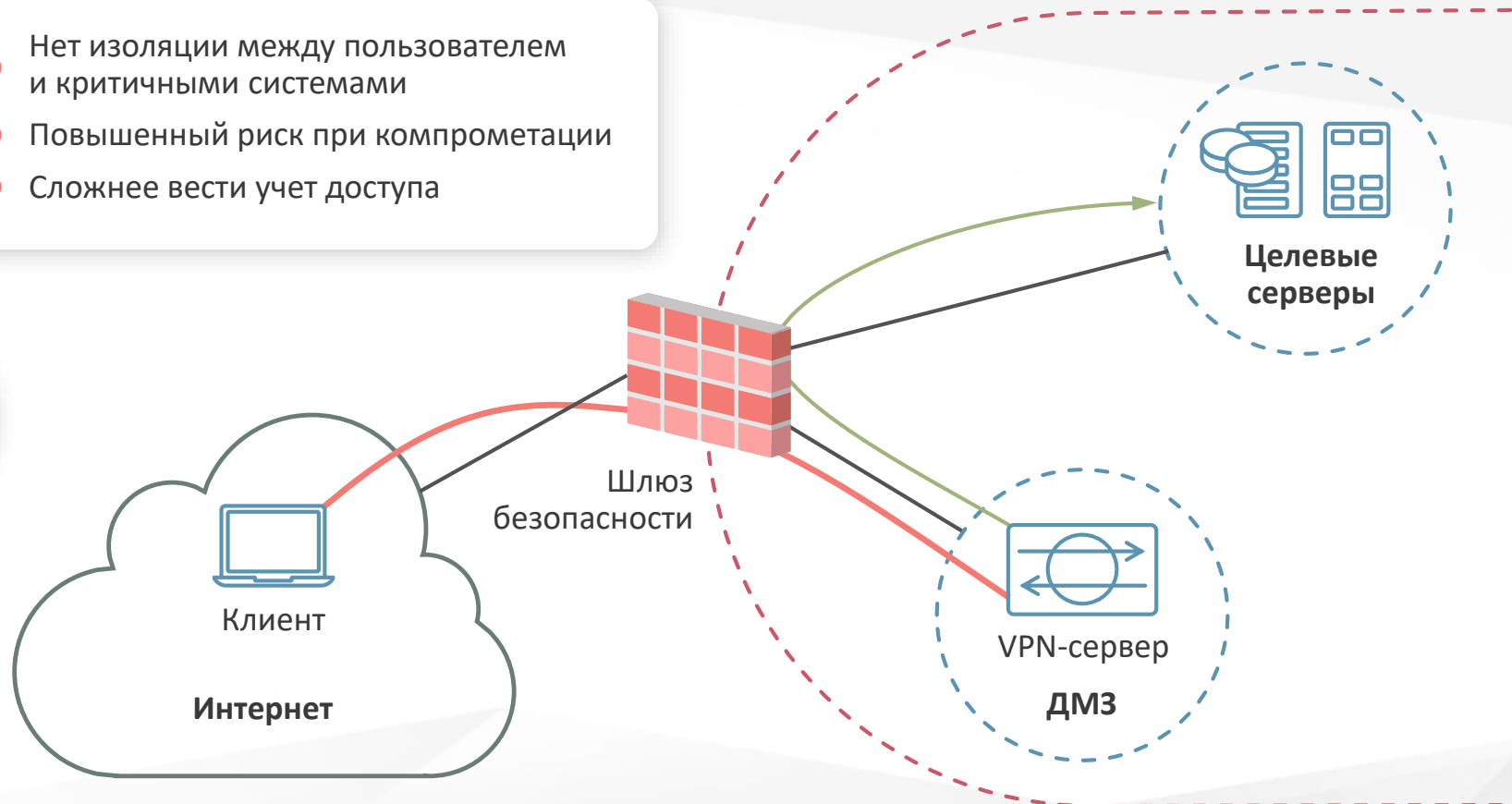
- Простая настройка
- Высокая производительность
- Удобно для постоянных сотрудников

Минусы

- Нет изоляции между пользователем и критичными системами
- Повышенный риск при компрометации
- Сложнее вести учет доступа

Применение:

Офисные сотрудники, которым нужен постоянный доступ к корпоративной инфраструктуре.



Инфраструктура корпоративной сети. Доступ через VDI

Пользователь подключается к VPN-серверу, после чего получает доступ только к виртуальной машине инфраструктуры VDI в корпоративной сети, а уже оттуда – к нужным сервисам.

Плюсы

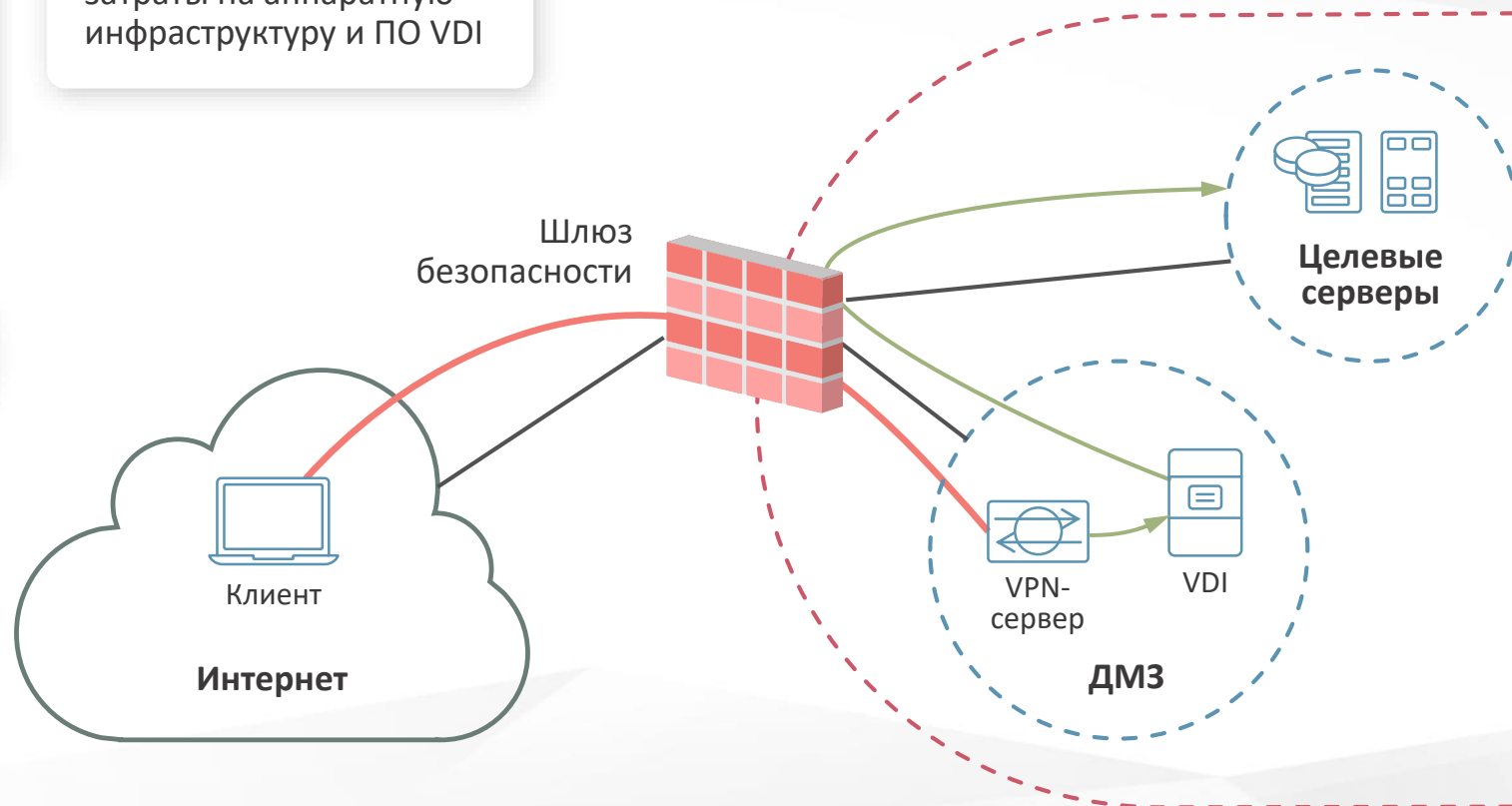
- Изоляция рабочих процессов
- Данные не покидают корпоративную инфраструктуру
- Централизованный контроль

Минусы

Значительные затраты на аппаратную инфраструктуру и ПО VDI

Применение:

Работа с чувствительными данными, внешние сотрудники, удалённые разработчики.



Инфраструктура корпоративной сети. Доступ через РАМ

VPN-соединение обеспечивает доступ только к РАМ-системе, которая, в свою очередь, предоставляет управляемый доступ к целевым сервисам.

Плюсы

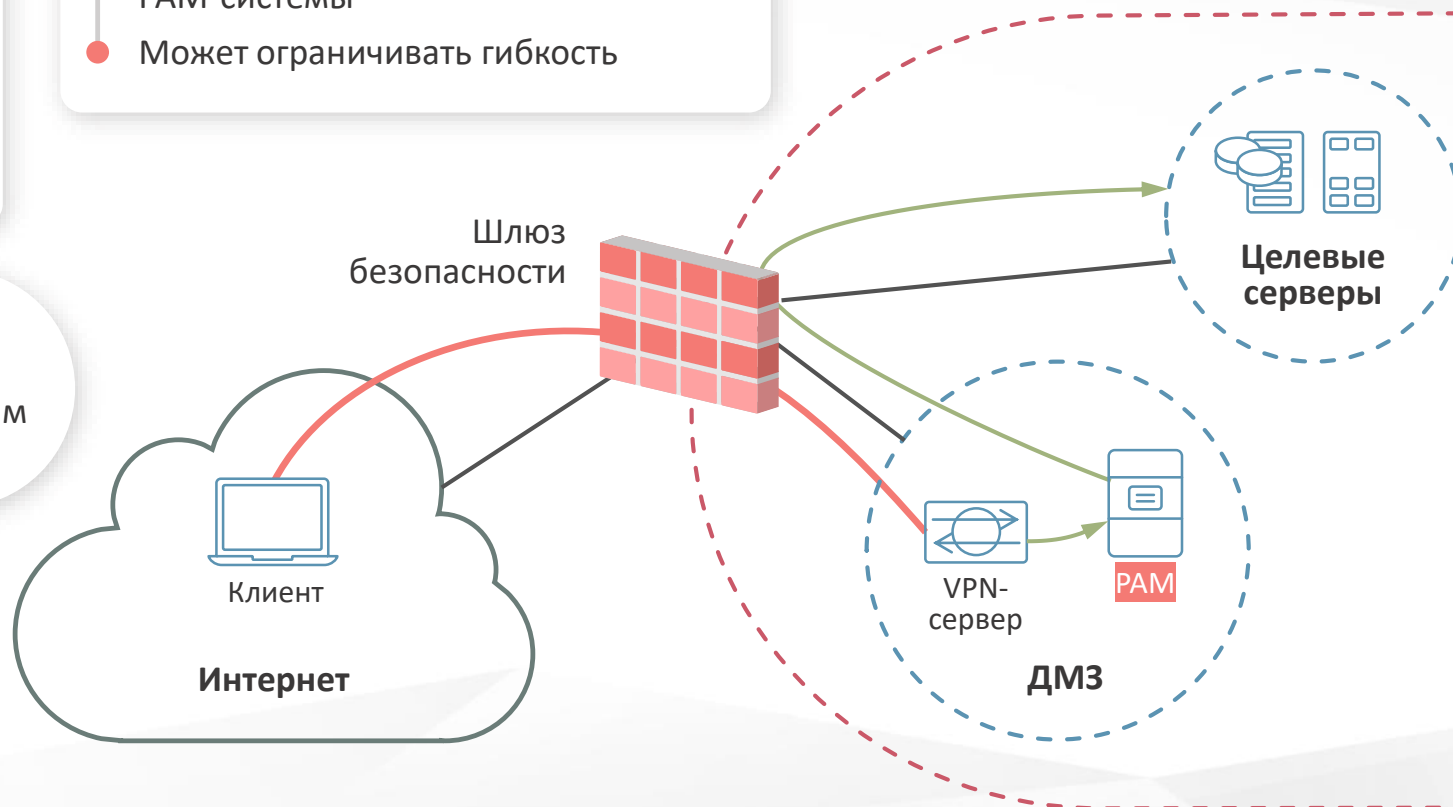
- Гранулярный контроль доступа
- Все действия записываются (аудит сессий – текст, видео)
- Процесс согласования (workflow) вплоть до конкретных команд

Применение:

Системные администраторы, подрядчики, доступ к критичным системам (БД, сетевое оборудование, серверы).

Минусы

- Значительные затраты на внедрение РАМ-системы
- Может ограничивать гибкость



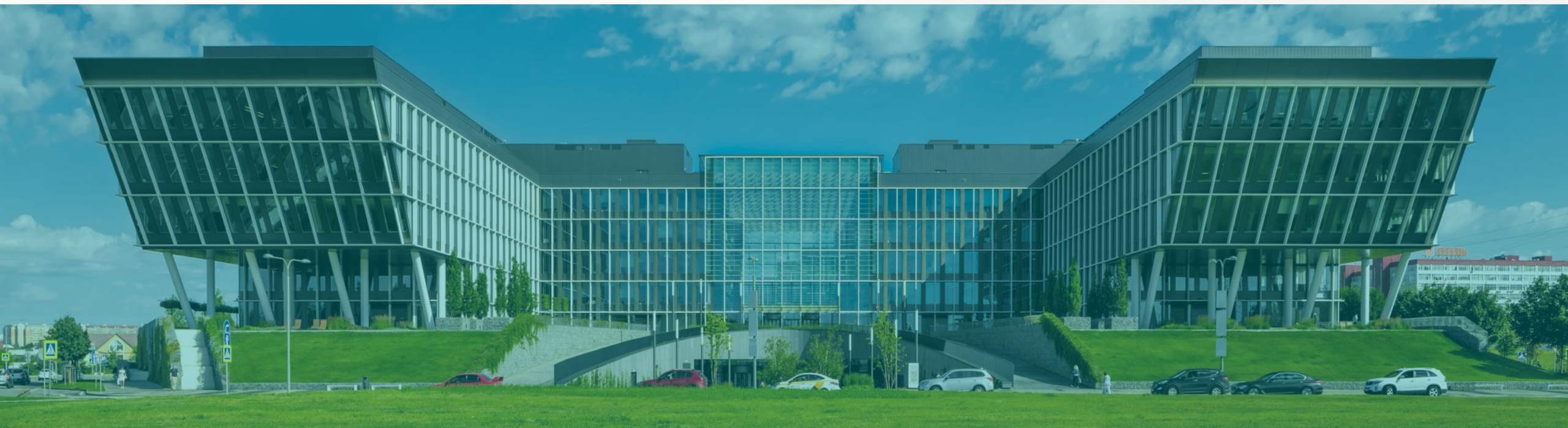
Контакты

Владимир Арышев

эксперт по комплексным проектам
информационной безопасности STEP LOGIC
+7 (953) 604-14-35
V_Aryshev@step.ru

Виртуальная визитка





Россия, 108811, Москва, район Солнцево,
Киевское ш., 22-й км., БЦ Комсити, дв. 6, стр.1
+ 7 (495) 775 31 20
info@step.ru | step.ru