



ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

Zero Trust Network Access: дать доступ и не потерять контроль

Алексей Брыляков

Менеджер по развитию решений
по сетевой безопасности

Александр Щекалев

Пресейл-инженер

sec.uscc.ru



СОДЕРЖАНИЕ

- 01** NAC, VPN и Zero Trust
- 02** Почему ZTNA это больше чем улучшенный VPN
- 03** Основные принципы ZTNA
- 04** Какие есть варианты реализации ZTNA
- 05** Демонстрация одного из вариантов реализации ZTNA



ЧУЖИЕ В СЕТИ

Размытие периметра сети



802.1X, NAC и VPN



Zero Trust





КАК С НИМИ БОРОТЬСЯ



Сделать устройство
доверенным



Опубликовать приложение



Проверять недоверенные устройства

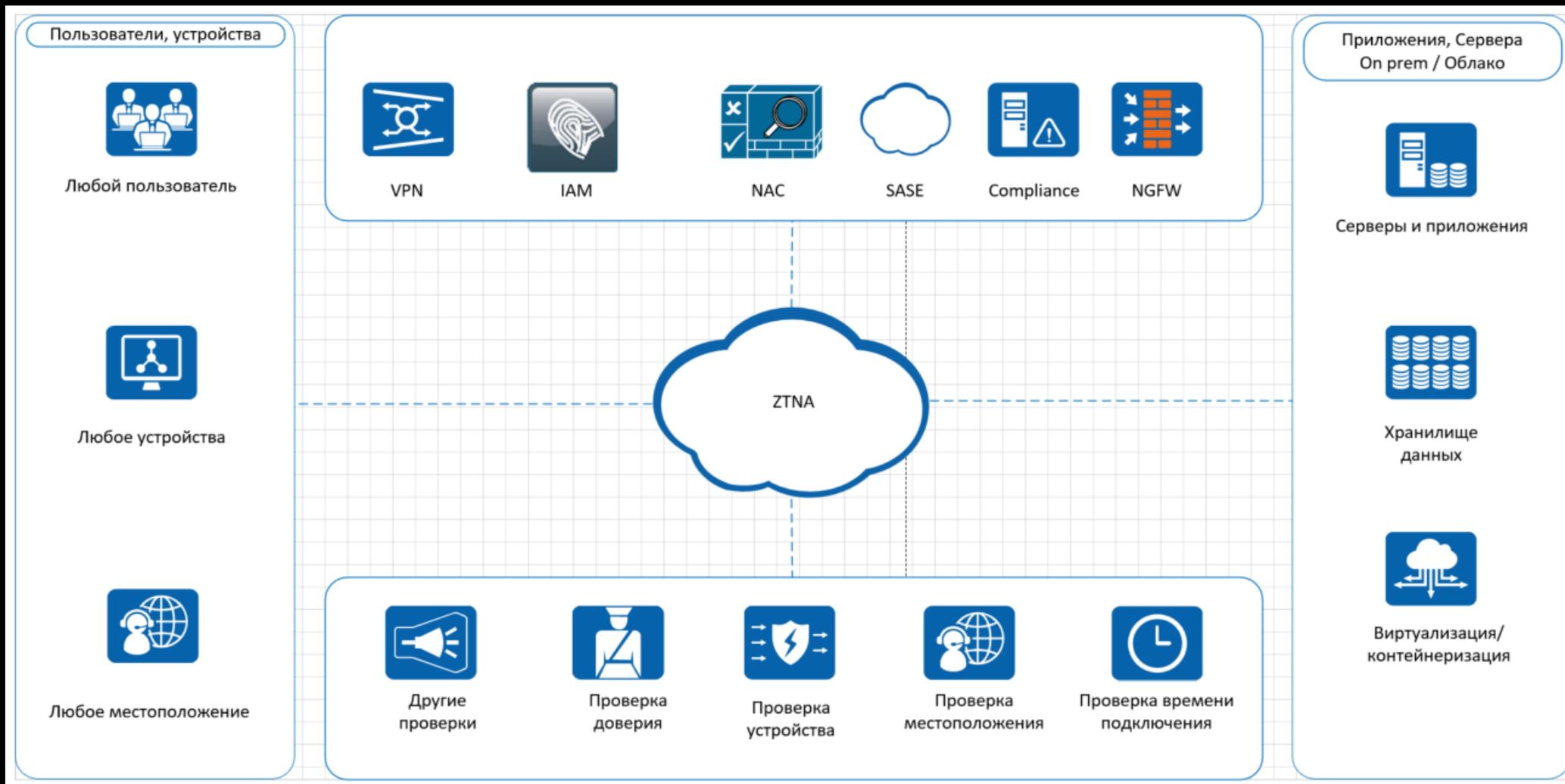


ZERO TRUST NETWORK ACCESS

- 01** Аутентификация с учетом контекста безопасности
- 02** Обязательная многофакторная аутентификация пользователей
- 03** Доступ к нужным сетевым сегментам на уровне приложений
- 04** Постоянная проверка устройств
- 05** Интеграция с другими ИБ продуктами
- 06** Поведенческий анализ и выявление аномалий



АРХИТЕКТУРА ZTNA





ZTNA С ПРИМЕНЕНИЕМ ПОЛИТИКИ ЛОКАЛЬНО

Используется локальный МСЭ

Встроенный VPN-клиент

Простая интеграция с инфраструктуру

Широкая функциональность*

Не подходит для локальных сетей

* Сильно зависит от производителя



ZTNA С РАСПРЕДЕЛЕННЫМ ПРИМЕНЕНИЕМ ПОЛИТИКИ

+ Используются устройства доступа в сеть

Любой поддерживаемый VPN-клиент

Узкоспециализированная функциональность агента

Более сложная но более гибкая интеграция

Подходит для локальной сети



ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

**СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?**

sec.ussc.ru



cybersec@ussc.ru





СХЕМА СТЕНДА

