В очередной раз про удаленный доступ

Михаил Кадер

Опять как независимый эксперт

Hype цикл технологий и архитектур ИБ в реальной жизни

- Концепция
- Красивое название и аббревиатура
- Маркетинг
- Реализация

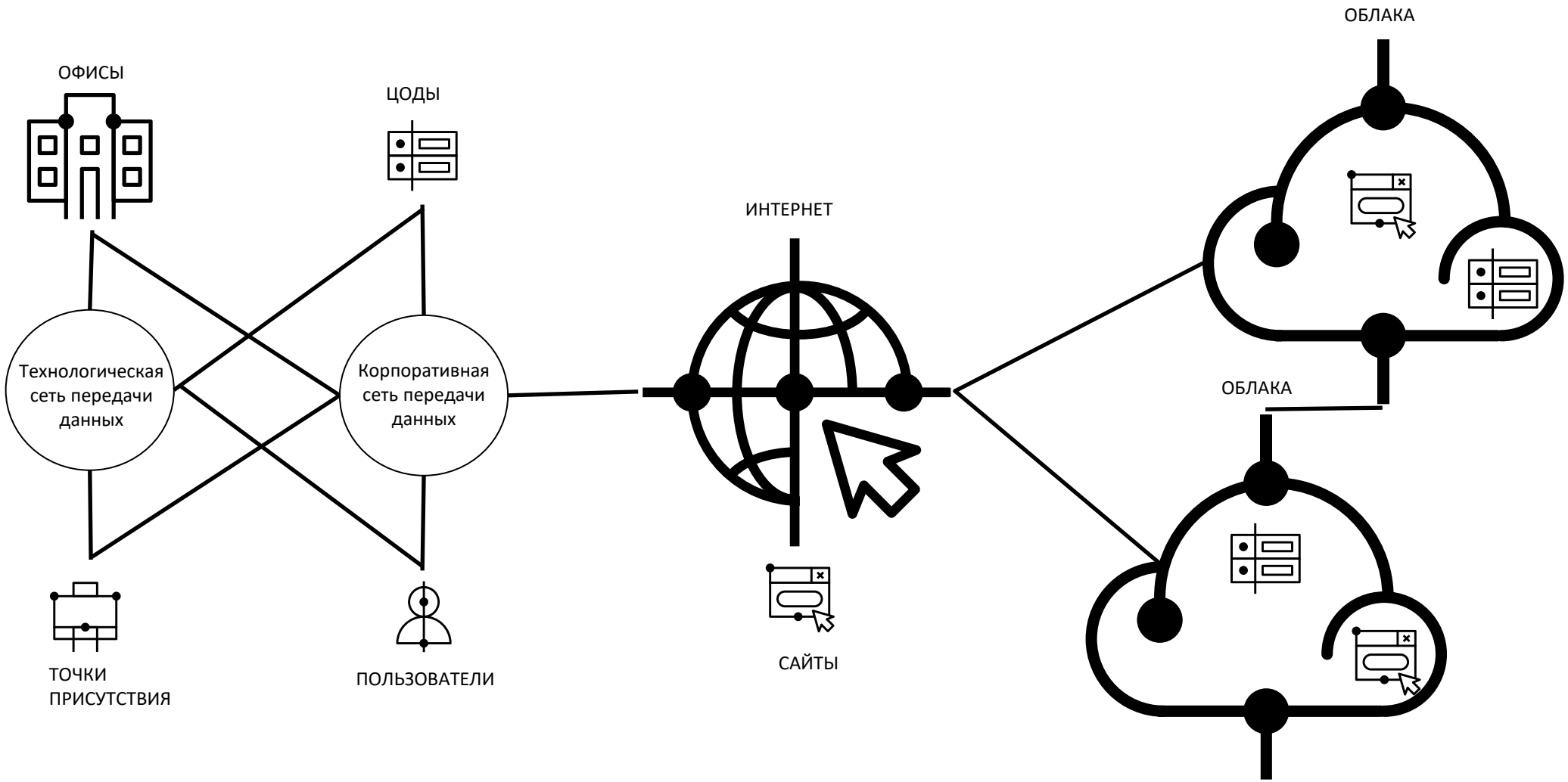
ZTNA - Хороший пример

- Концепция Zero Trust Network Access
  - Никому не доверяем, всех постоянно проверяем
- Реальность (по отчету пентестеров Positive Technologies за 2024 год)
  - Аутентификация
  - Уязвимости
  - Сегментация

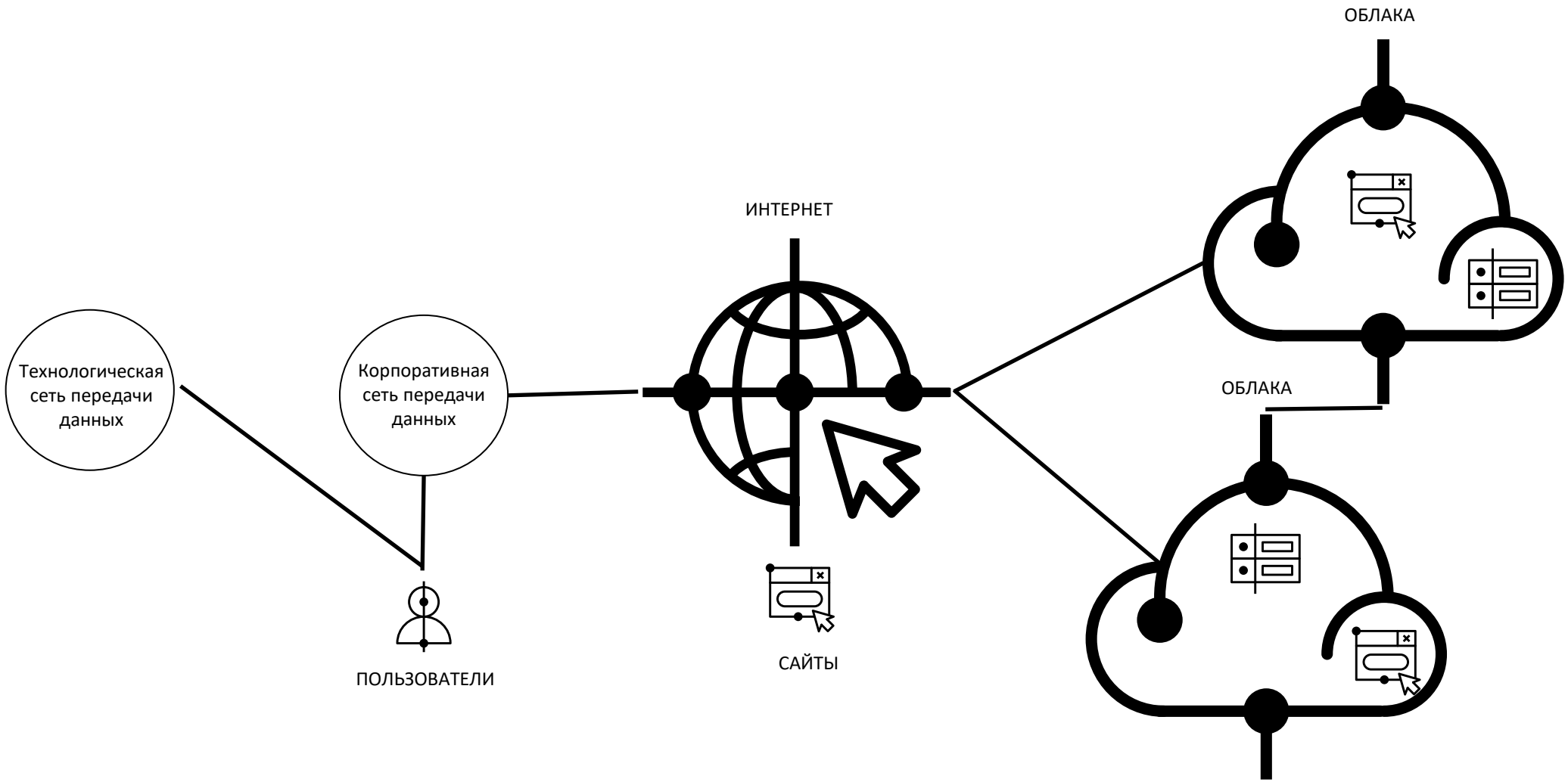
Почему все так «странно»?

- Отсутствие технического понимания целевого результата
- Бюджет
- Малый выбор продуктов
- Зоны ответственности и задачи подразделений
- Нехватка персонала
- И вообще люди ☹

Общая ЛОГИЧЕСКАЯ схема инфраструктуры



Уберем то, про что не сегодня



Инструменты доверия к недоверенному?

- Сценарии
  - Контроль при доступе к доверенным приложениям
  - Защита при доступе к недоверенным приложениями

Инструменты доверия к недоверенному? *Клиент*

- Корпоративный браузер
  - (Не)доверие к клиенту
  - Проверка среды
  - Идентификация клиента и сессий
  - Доверенные плагины
  - И прочее – см. Яндекс Браузер
- RBI – Remote Browser Isolation
  - Практически терминал для WEB приложений

Инструменты доверия к недоверенному? *Приложения*

- WAF - Доверенный клиент к корпоративным приложениям
  - Корпоративный браузер
  - RBI
- SWG/NGFW – доверенный клиент к недоверенным внешним приложениям
- SWG/CASB – доверенный клиент к доверенным внешним приложениям

Выводы

- Разрешительные списки – наше все
- Корпоративный браузер – достойная идея
- RBI – современная замена терминальным серверам
- Помнить про размещение приложений, включая SaaS

Пообсуждаем ☺