Олег Хныков
Руководитель группы
по направлению сетевой
безопасности

Михаил Кадер
Главный архитектор
стратегических проектов

pt

Архитектура сетевой безопасности предприятия

Дисклеймер

- Эта презентация отражает основные подходы к построению сетевой безопасности современного предприятия и не заменяет собой ее детального проектирования
- Перечень угроз может быть уточнен
- Перечень и функциональность предлагаемых продуктов и решений могут быть изменены

Центр противодействия киберугрозам (ЦПК)

с формальной точки зрения

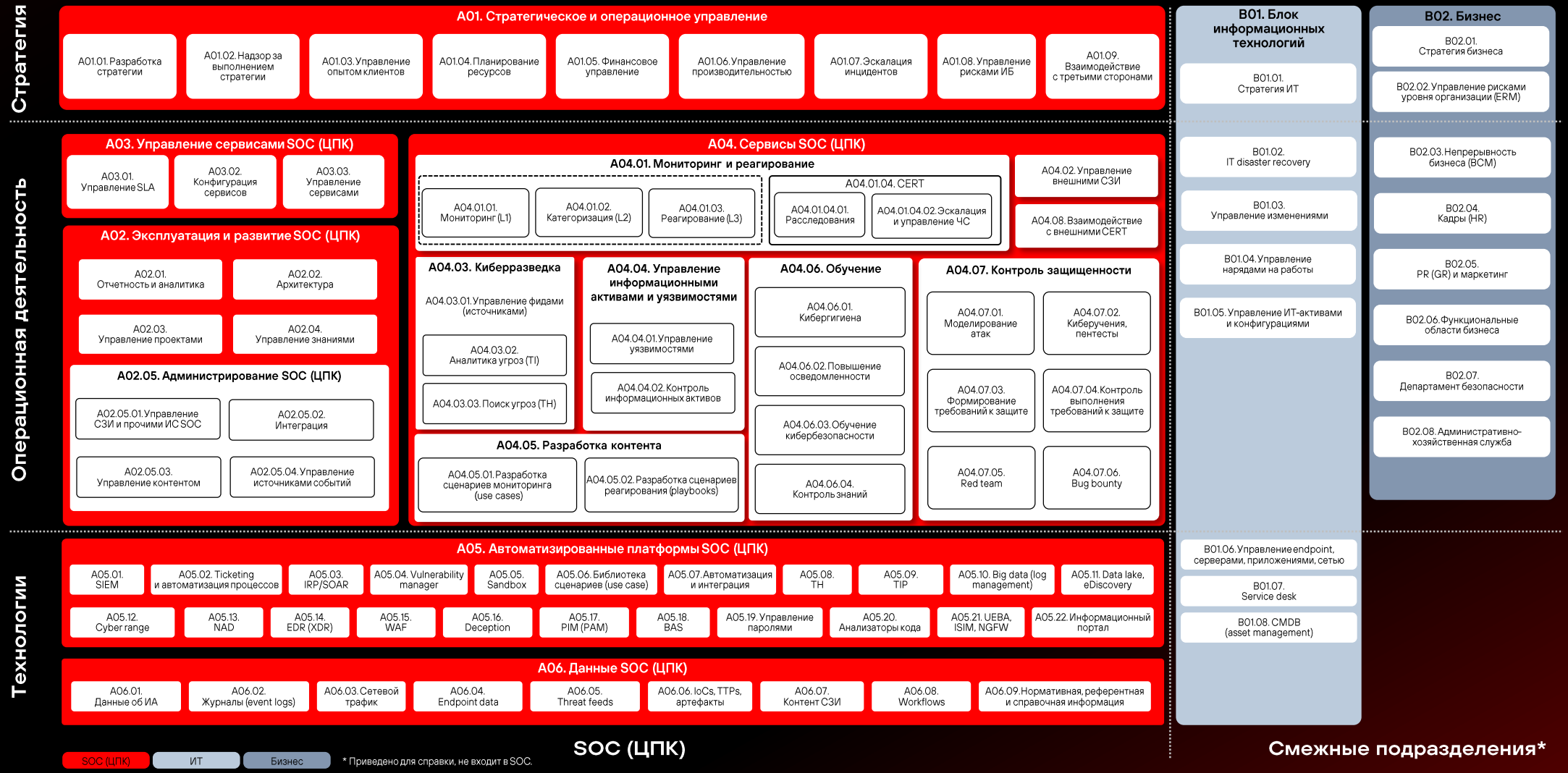
> Киберустойчивость

Обеспечение киберустойчивости предприятия —

набор функций (сервисов) ИБ, распределенных между внутренними и внешними командами (сотрудниками), который описан через десятки процессов стратегического, тактического и оперативного уровней и реализован с использованием технологий детектирования, анализа, корреляции и реагирования для обеспечения невозможности наступления недопустимых событий

Операционная модель ИБ

(один из возможных вариантов)



Основные компоненты ЦПК

Сервисы обеспечения ИБ

A03. Управление сервисами SOC (ЦПК)

- A03.01. Управление SLA
- A03.02. Конфигурация сервисов
- A03.03. Управление сервисами

A02. Эксплуатация и развитие SOC (ЦПК)

- A02.01. Отчетность и аналитика
- A02.02. Архитектура
- A02.03. Управление проектами
- A02.04. Управление знаниями

A02.05. Администрирование SOC (ЦПК)

- A02.05.01. Управление СЗИ и прочими ИС SOC
- A02.05.02. Интеграция
- A02.05.03. Управление контентом
- A02.05.04. Управление источниками событий

A04. Сервисы SOC (ЦПК)

A04.01. Мониторинг и реагирование

- A04.01.01. Мониторинг (L1)
- A04.01.02. Категоризация (L2)
- A04.01.03. Реагирование (L3)
- A04.01.04. CERT
  - A04.01.04.01. Расследования
  - A04.01.04.02. Эскалация и управление ЧС

- A04.02. Управление внешними СЗИ
- A04.08. Взаимодействие с внешними CERT

A04.03. Киберразведка

- A04.03.01. Управление фидами (источниками)
- A04.03.02. Аналитика угроз (TI)
- A04.03.03. Поиск угроз (TH)

A04.04. Управление информационными активами и уязвимостями

- A04.04.01. Управление уязвимостями
- A04.04.02. Контроль информационных активов

A04.05. Разработка контента

- A04.05.01. Разработка сценариев мониторинга (use cases)
- A04.05.02. Разработка сценариев реагирования (playbooks)

A04.06. Обучение

- A04.06.01. Кибергигиена
- A04.06.02. Повышение осведомленности
- A04.06.03. Обучение кибербезопасности
- A04.06.04. Контроль знаний

A04.07. Контроль защищенности

- A04.07.01. Моделирование атак
- A04.07.02. Киберучения, пентесты
- A04.07.03. Формирование требований к защите
- A04.07.04. Контроль выполнения требований к защите
- A04.07.05. Red team
- A04.07.06. Bug bounty

Продукты Positive Technologies
для ЦПК и не только

Metaproducts
(MaxPatrol O2, MaxPatrol Carbon)

Vulnerability management (MaxPatrol VM)

Threat intelligence platform (PT Threat Analyzer)

Host compliance control (MaxPatrol HCC)

Incident management (MaxPatrol IM)

Security information and event management (MaxPatrol SIEM)

Asset management (AM)

MaxPatrol Platform

Knowledge base (KB)

Management and configuration (MC)

Network traffic analysis (response) (PT NAD)

Sandbox (PT Sandbox)

Web application firewall (PT Application Firewall)

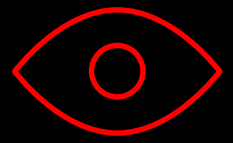
NGFW (PT NGFW)

OT security (SCADA security) (PT ICS, PT ISIM)

Endpoint detection and response (MaxPatrol EDR)

Архитектура СО РКБ

Целеполагание — MaxPatrol O2



Обнаружить

- Увидеть
- Понять
- Проанализировать

Остановить

- Отреагировать
- Взаимодействовать
- Уведомить

Управление инфраструктурой и цепочками атак

Основные задачи — 4У

Укрепить все активы

- Инвентаризация
- Управление уязвимостями
- Парольная политика

Уменьшить поверхность атаки

- Политики взаимодействия
- Сегментация
- Фильтрация

Удлинить цепочку атаки

- Инфраструктурные СЗИ
- Терминальные серверы
- Эшелонированная оборона

Усложнить цепочку атаки

- Защита активов
- Ложные цели

Этапы атаки

Этап проникновения

- Внешняя разведка
- Взлом сервиса на периметре (эксплуатация уязвимости)
- Фишинг
- Атаки через Wi-Fi
- Получение доступа с помощью украденной или скомпрометированной учетной записи
- Компрометация цепочки поставок
- Компрометация доверенной инфраструктуры (например, VPN)

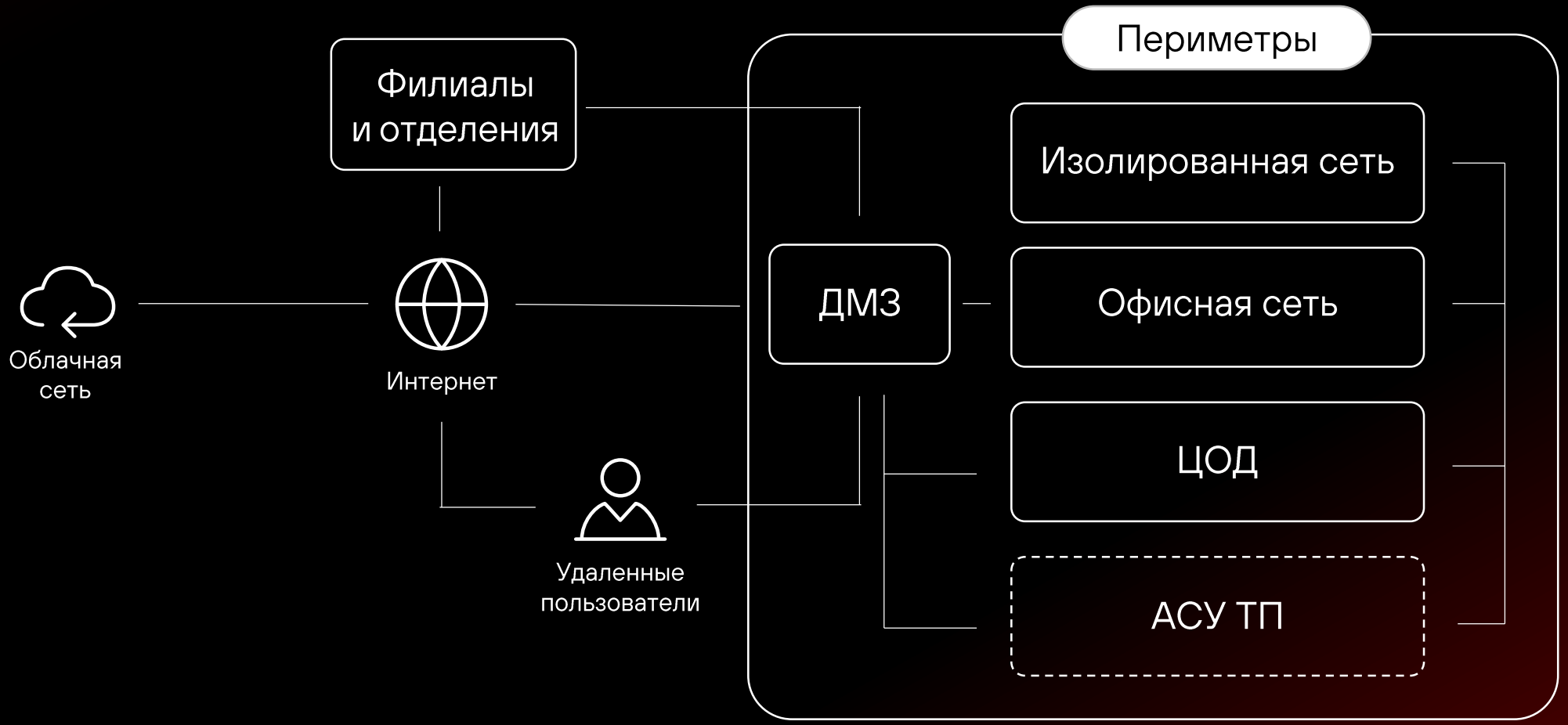
Развитие атаки

- Закрепление в инфраструктуре
- Разведка внутри инфраструктуры (как сетевой, так и доменной)
- Повышение привилегий — как локальных, так и в целом в инфраструктуре
- Передвижение по инфраструктуре
- Взлом ключевых систем

Нанесение ущерба

- Уничтожение данных и (или) систем
- Кража данных
- Взлом целевых систем (кража денег, нарушение производственного процесса и т. д.)

Основные модули инфраструктуры предприятия



Условные обозначения

Проводной канал связи между устройствами

Беспроводной канал связи между устройствами

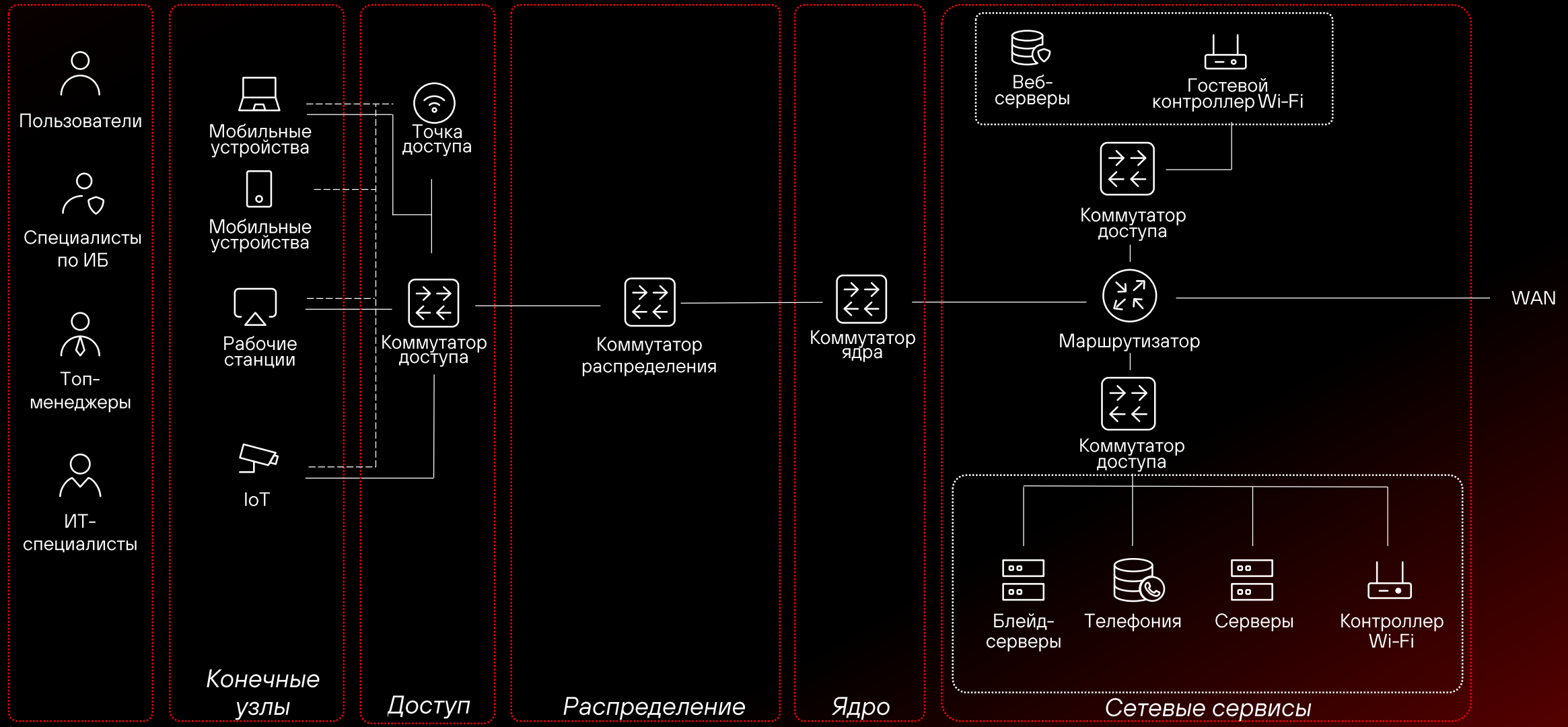
Канал подключения устройства к средству защиты

Зона безопасности

Средства защиты

- PT Next Generation Firewall
- PT Application Firewall
- MaxPatrol VM
- PT Network Attack Discovery
- PT Threat Analyzer
- MaxPatrol EDR
- PT Sandbox
- MaxPatrol SIEM
- PT Container Security

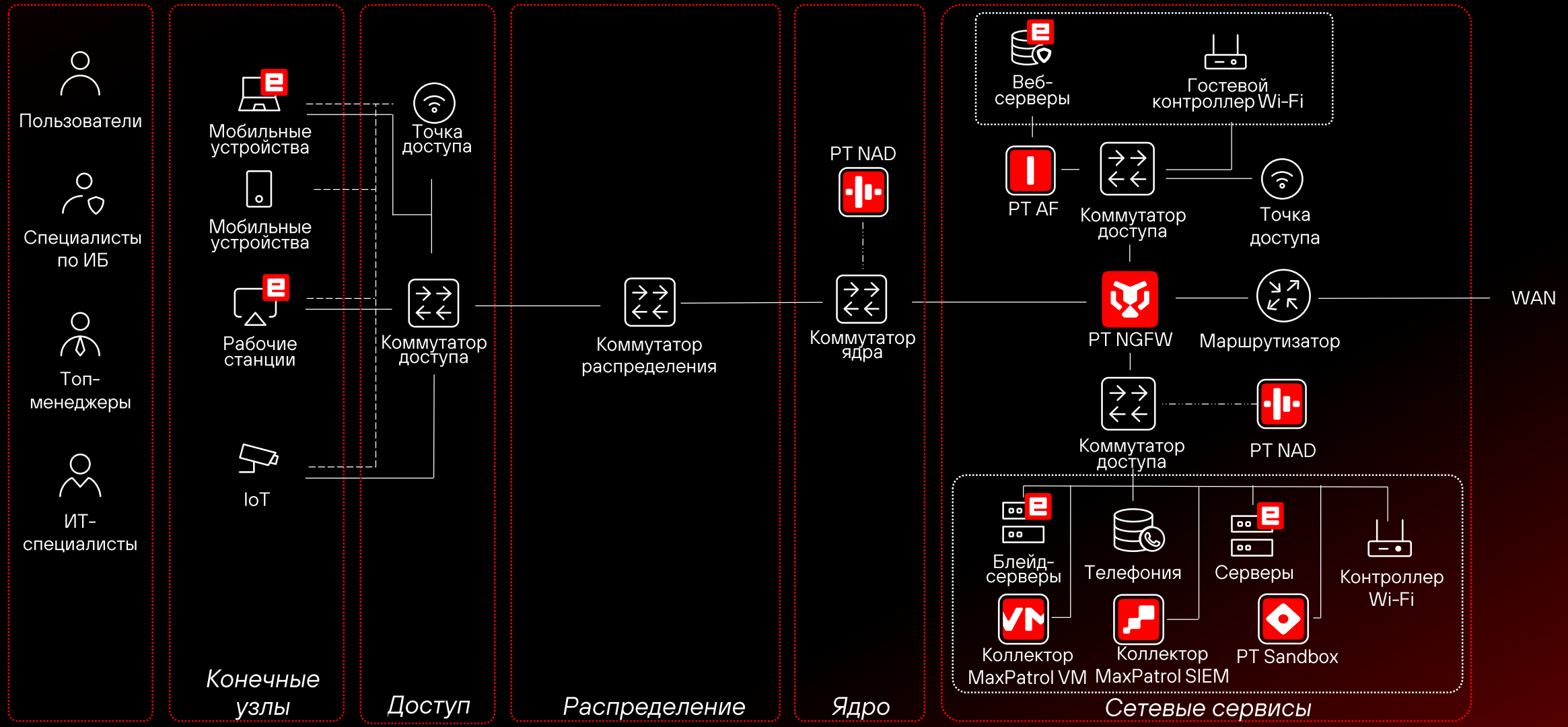
Офисная сеть



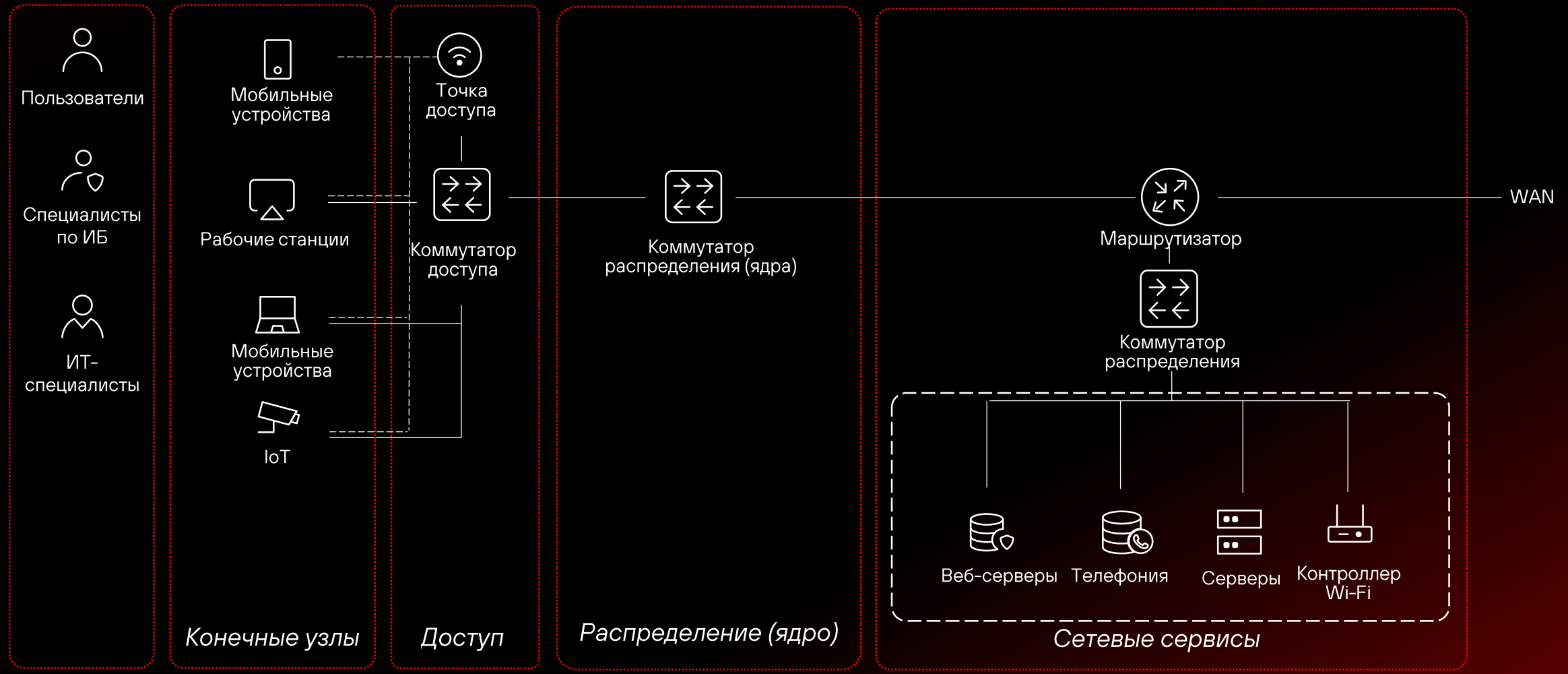
Особенности офисной сети

- Много зон безопасности
- Много рабочих станций
- Корпоративные мобильные устройства
- Личные устройства
- Личные мобильные устройства
- Доступ к интернету
- Гостевые пользователи
- Интернет вещей (управляемых и неуправляемых)
- Служебные серверы
- Квалифицированные специалисты по ИТ и ИБ
- Руководство компании

Защита офисной сети



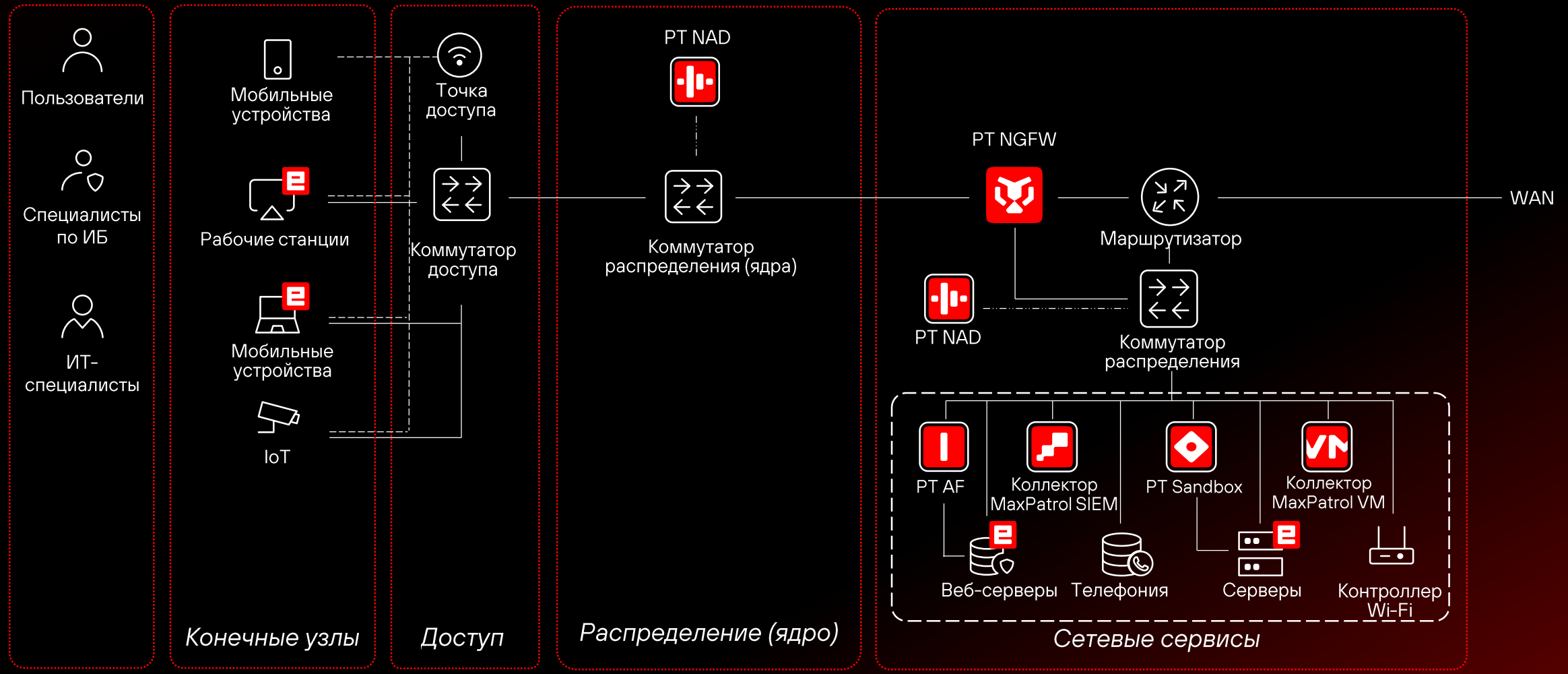
Сеть филиала



Особенности сети филиала

- Несколько зон безопасности
- Много рабочих станций
- Корпоративные мобильные устройства
- Личные устройства
- Личные мобильные устройства
- Может быть доступ к интернету
- Могут быть гостевые пользователи
- Квалифицированные ИТ-специалисты
- Могут отсутствовать квалифицированные специалисты по ИБ
- Может быть руководство
- Служебные серверы
- Интернет вещей (управляемых и неуправляемых)

Защита сети филиала

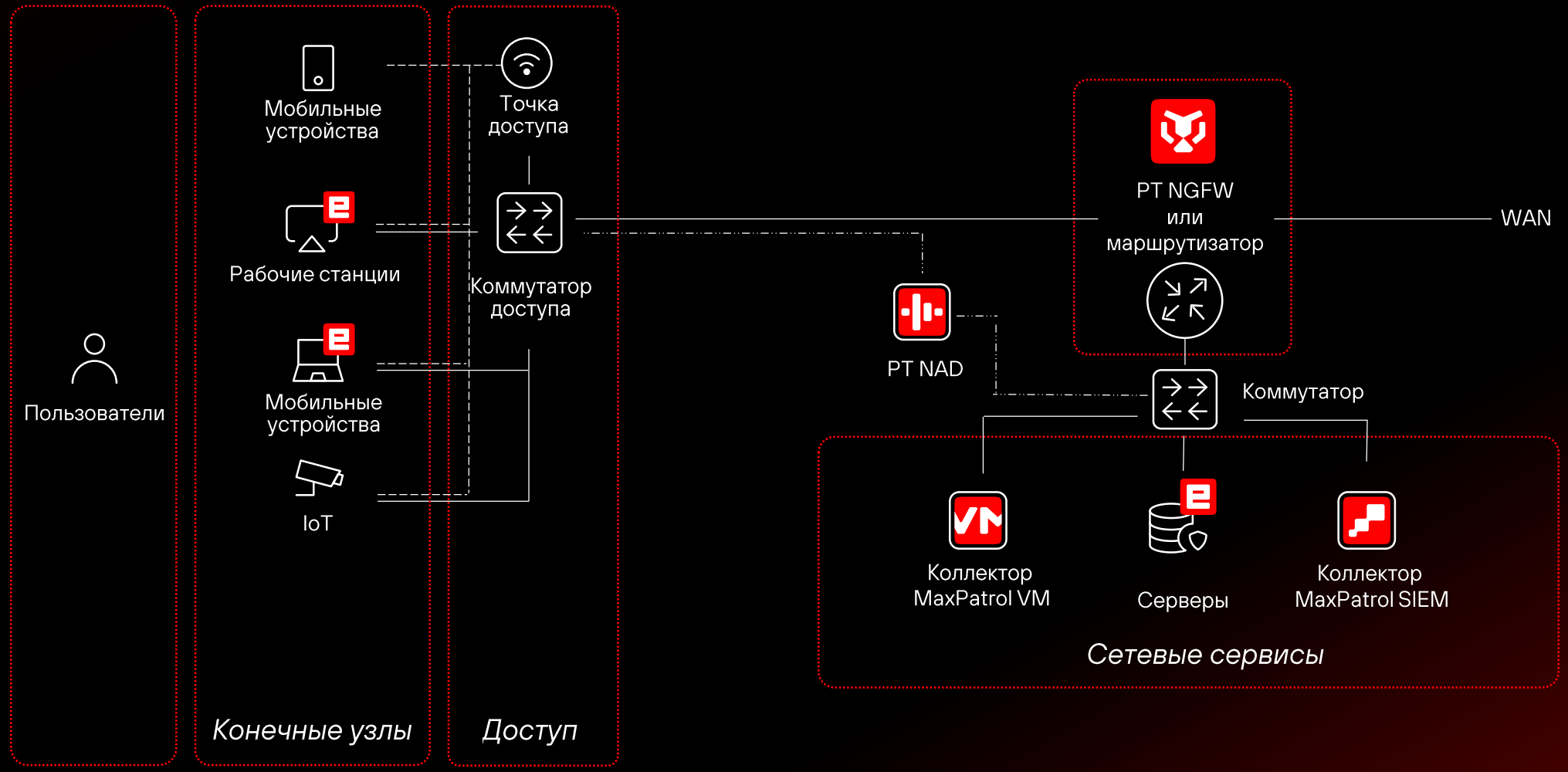


Сеть отделения

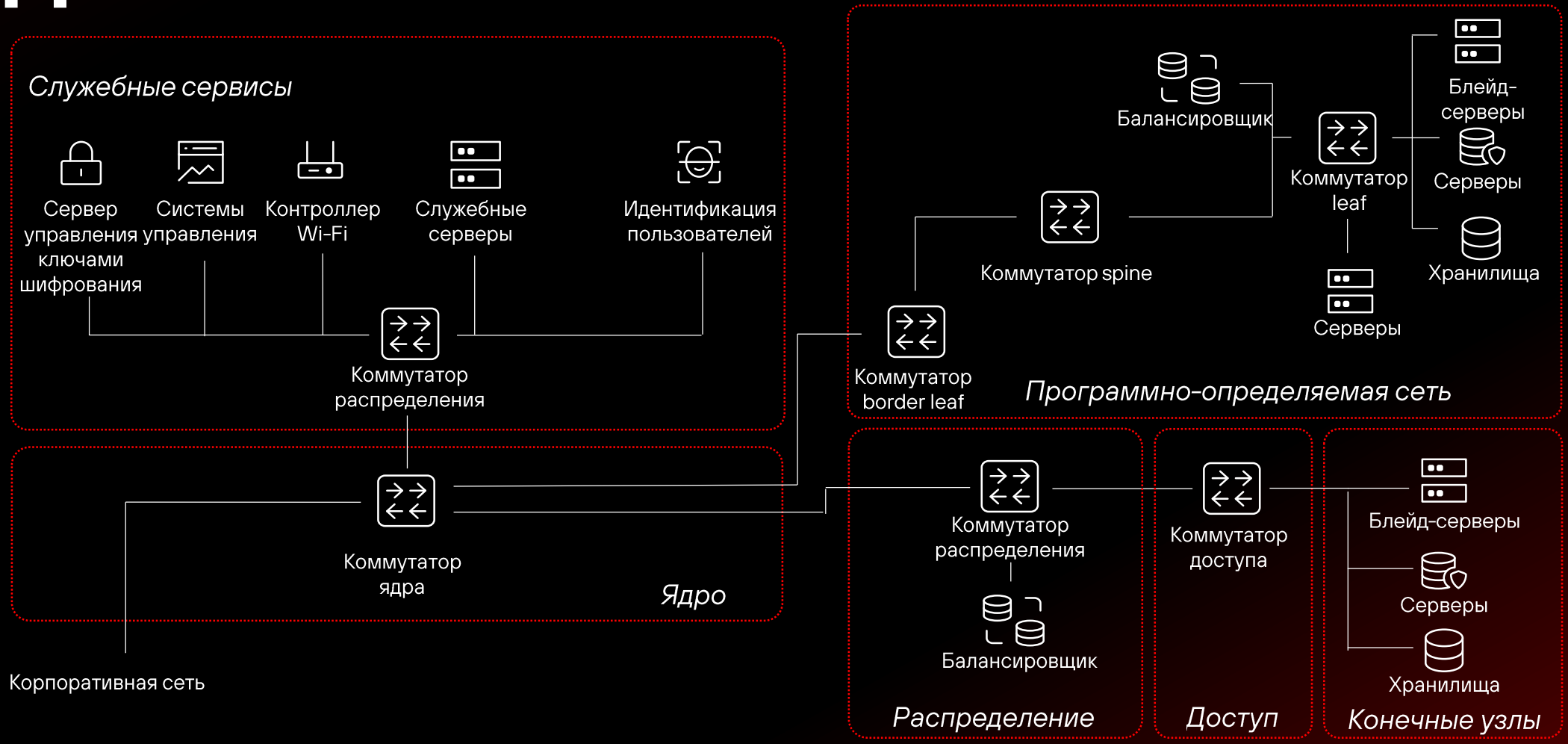
Особенности сети отделения

- Несколько зон безопасности
- Мало рабочих станций
- Корпоративные мобильные устройства
- Личные устройства
- Личные мобильные устройства
- Могут быть гостевые пользователи
- Могут быть локальные серверы
- Могут отсутствовать квалифицированные специалисты по ИТ и(или) ИБ
- Возможен терминальный доступ
- Интернет вещей (управляемых и неуправляемых)
- Может быть доступ к интернету

Защита сети отделения



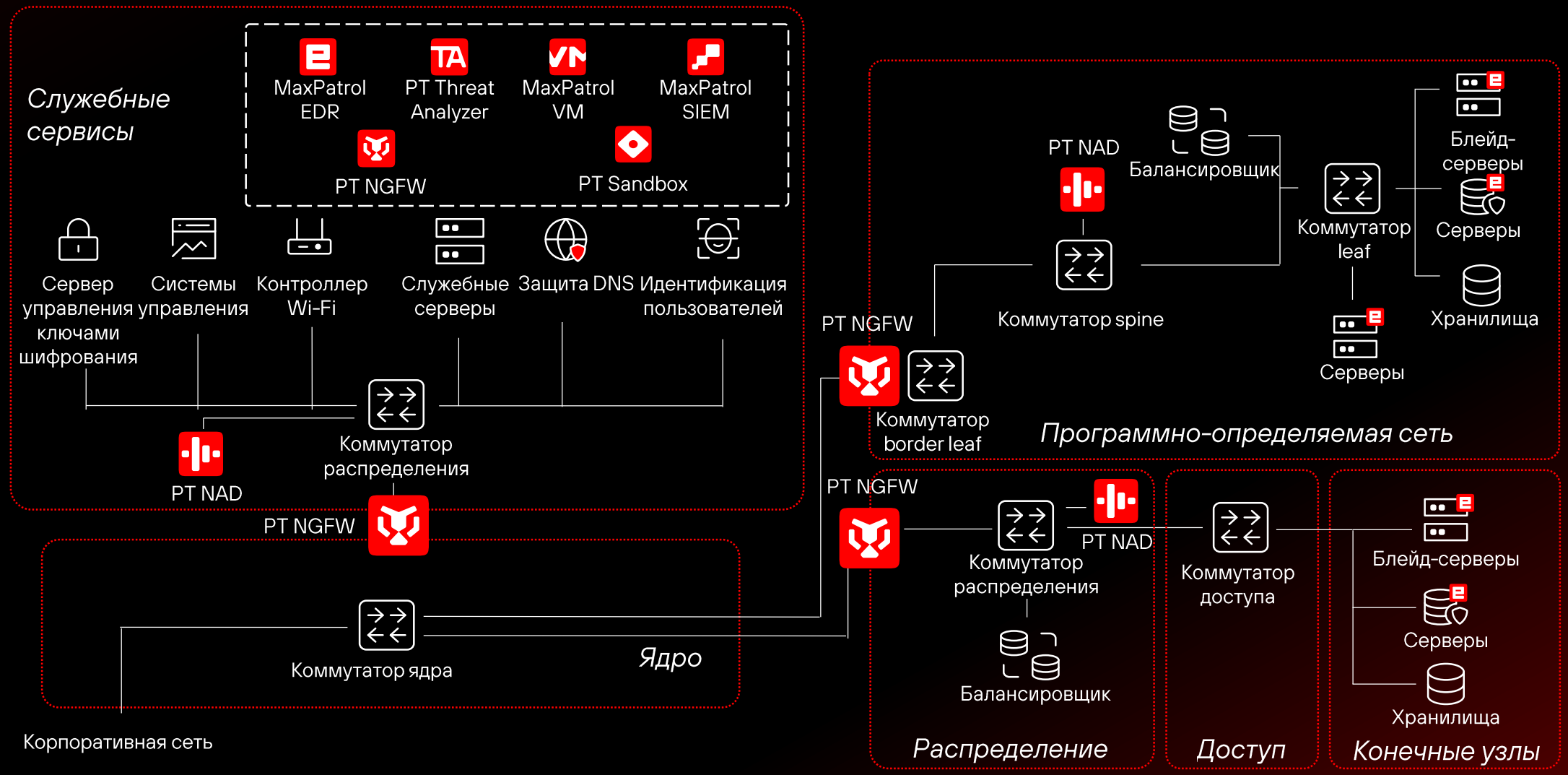
Сеть центра обработки данных



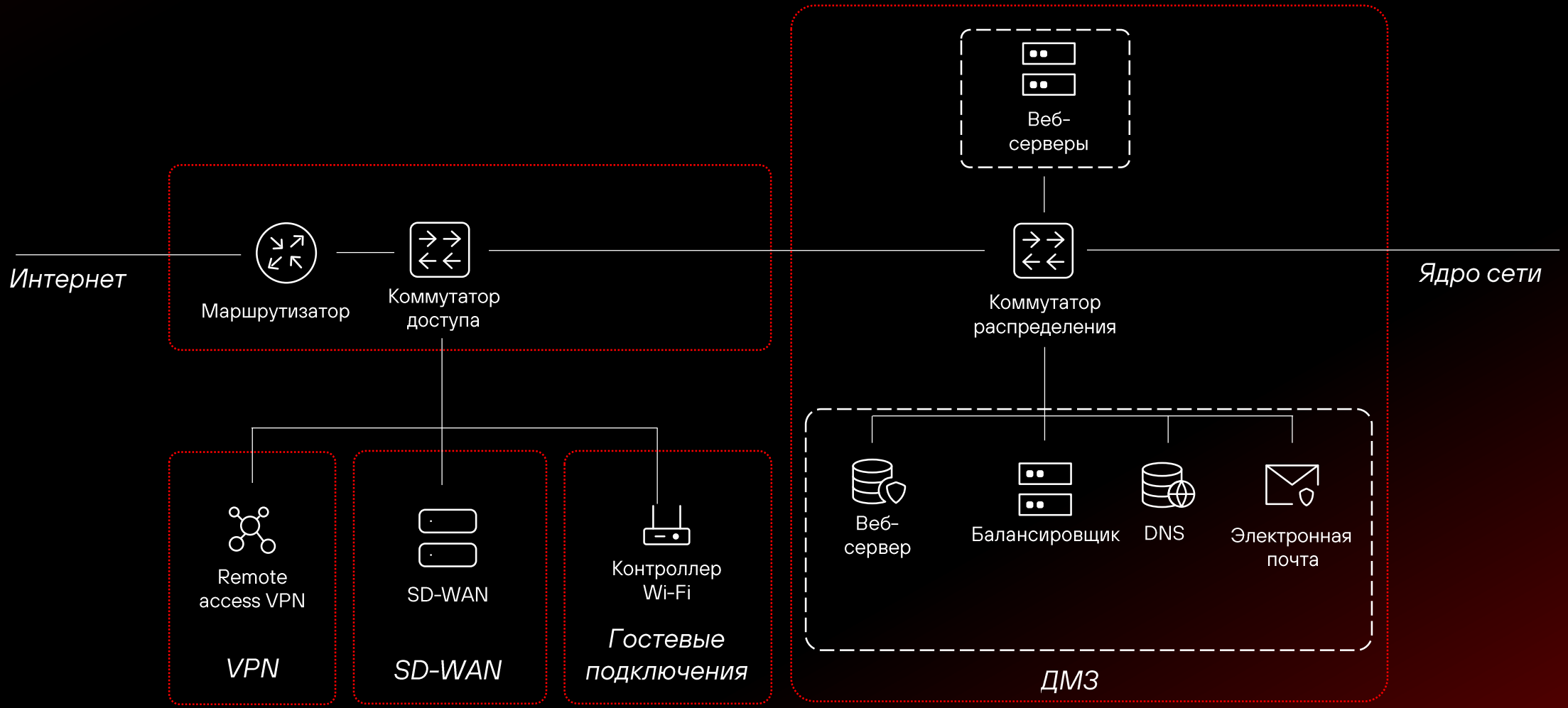
Особенности сети ЦОД

- Много зон безопасности
- Специализированные рабочие станции
- Корпоративные мобильные устройства
- Личные устройства
- Личные мобильные устройства
- Доступ из офисной сети
- Доступ из ДМЗ
- Подрядчики
- Необходимость поддерживать все компоненты и системы ЦОД в рабочем состоянии
- Высокая скорость обновления ПО
- Интернет вещей (управляемых)

Защита ЦОД


Служебные сервисы
MaxPatrol EDR
PT Threat Analyzer
MaxPatrol VM
MaxPatrol SIEM
PT NGFW
PT Sandbox
Сервер управления ключами шифрования
Системы управления
Контроллер Wi-Fi
Служебные серверы
Защита DNS
Идентификация пользователей
PT NAD
Коммутатор распределения
PT NGFW
Коммутатор ядра
Ядро
Корпоративная сеть
PT NAD
Балансировщик
Коммутатор leaf
Блейд-серверы
Серверы
Хранилища
Коммутатор spine
PT NGFW
Коммутатор border leaf
Серверы
Программно-определяемая сеть
PT NGFW
Коммутатор распределения
PT NAD
Балансировщик
Распределение
Коммутатор доступа
Доступ
Блейд-серверы
Серверы
Хранилища
Конечные узлы

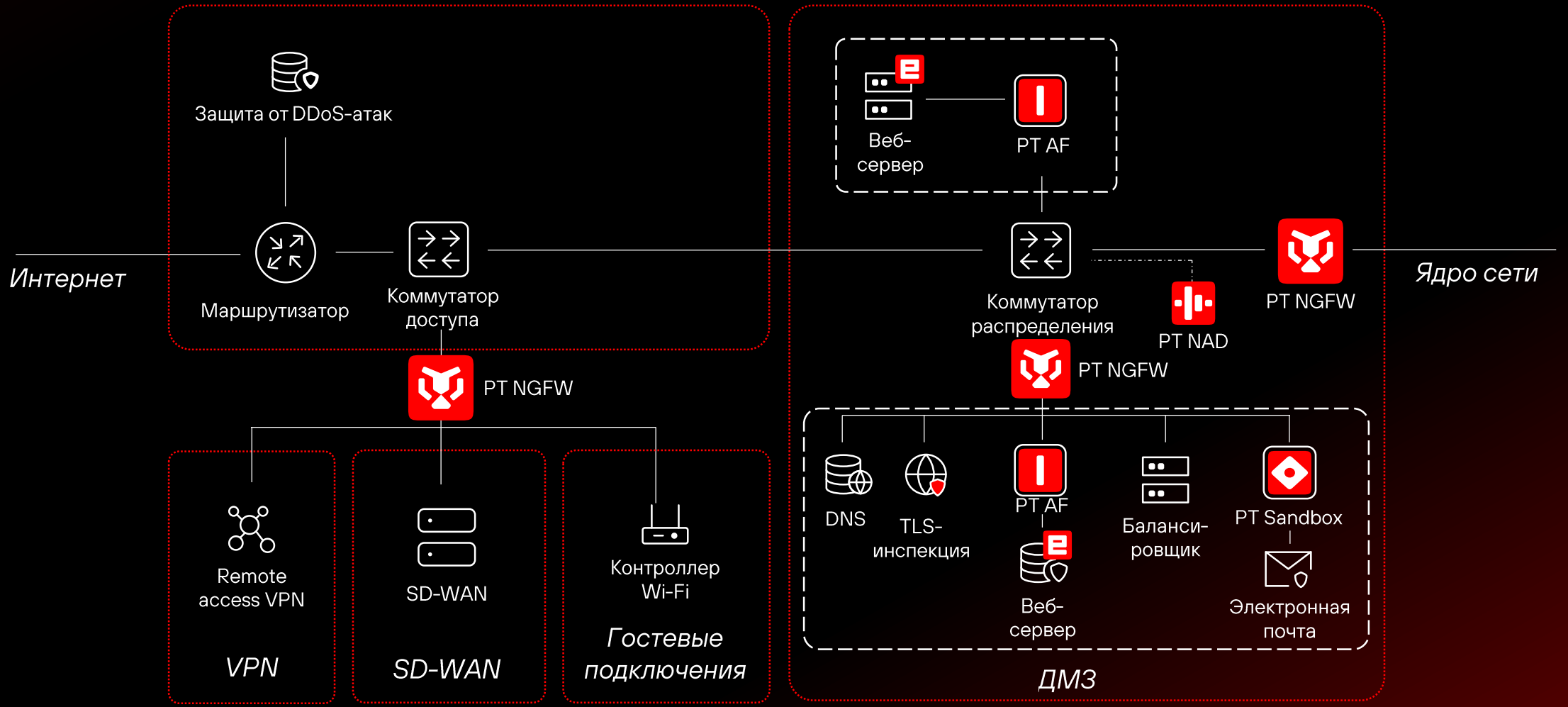
ДМЗ сети


Интернет
Маршрутизатор
Коммутатор доступа
Веб-серверы
Коммутатор распределения
Ядро сети
Remote access VPN
VPN
SD-WAN
SD-WAN
Контроллер Wi-Fi
Гостевые подключения
Веб-сервер
Балансировщик
DNS
Электронная почта
ДМЗ

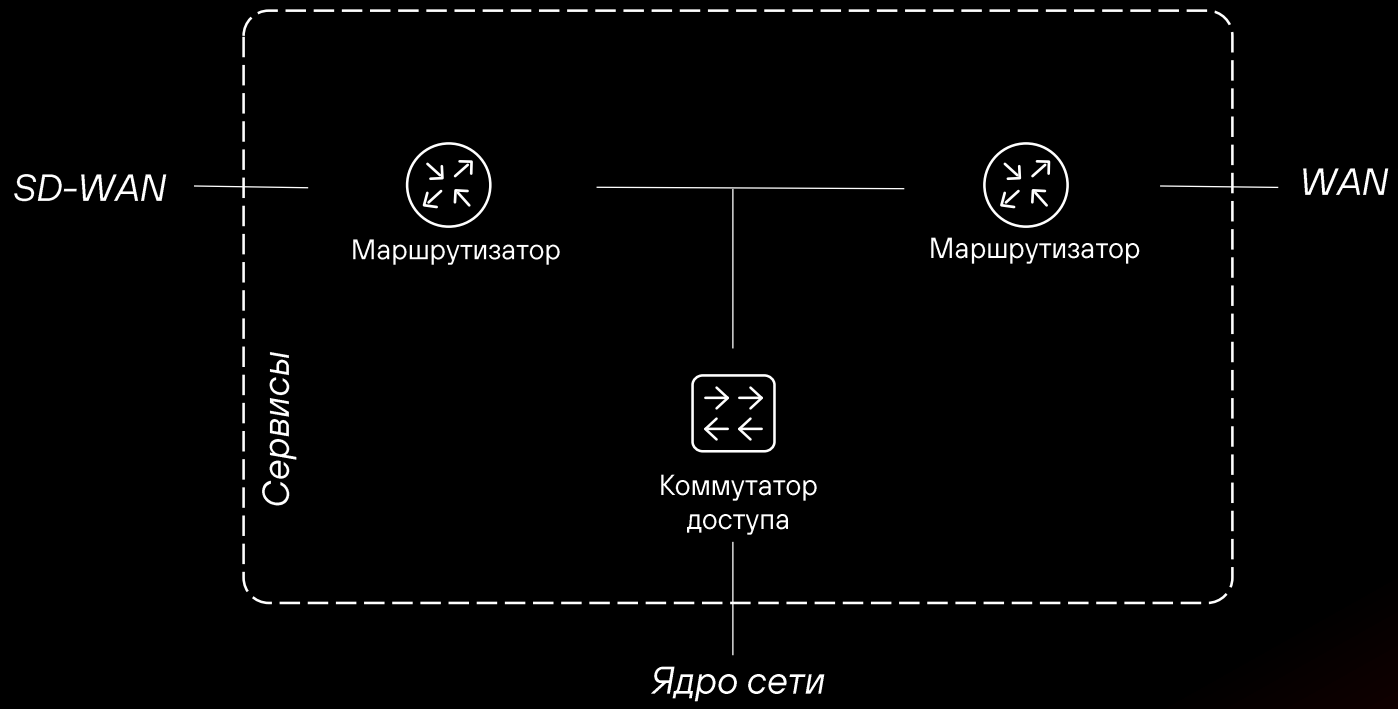
Особенности ДМЗ сети

- Есть опубликованные сервисы
- Нет рабочих станций
- Доступ из интернета
- Подключение удаленных пользователей
- Подключение филиалов или отделений
- Доступ в ЦОД
- Доступ из офисной сети
- Гостевой доступ
- Сквозные служебные сервисы (например, веб, почта, DNS)

Защита ДМЗ сети



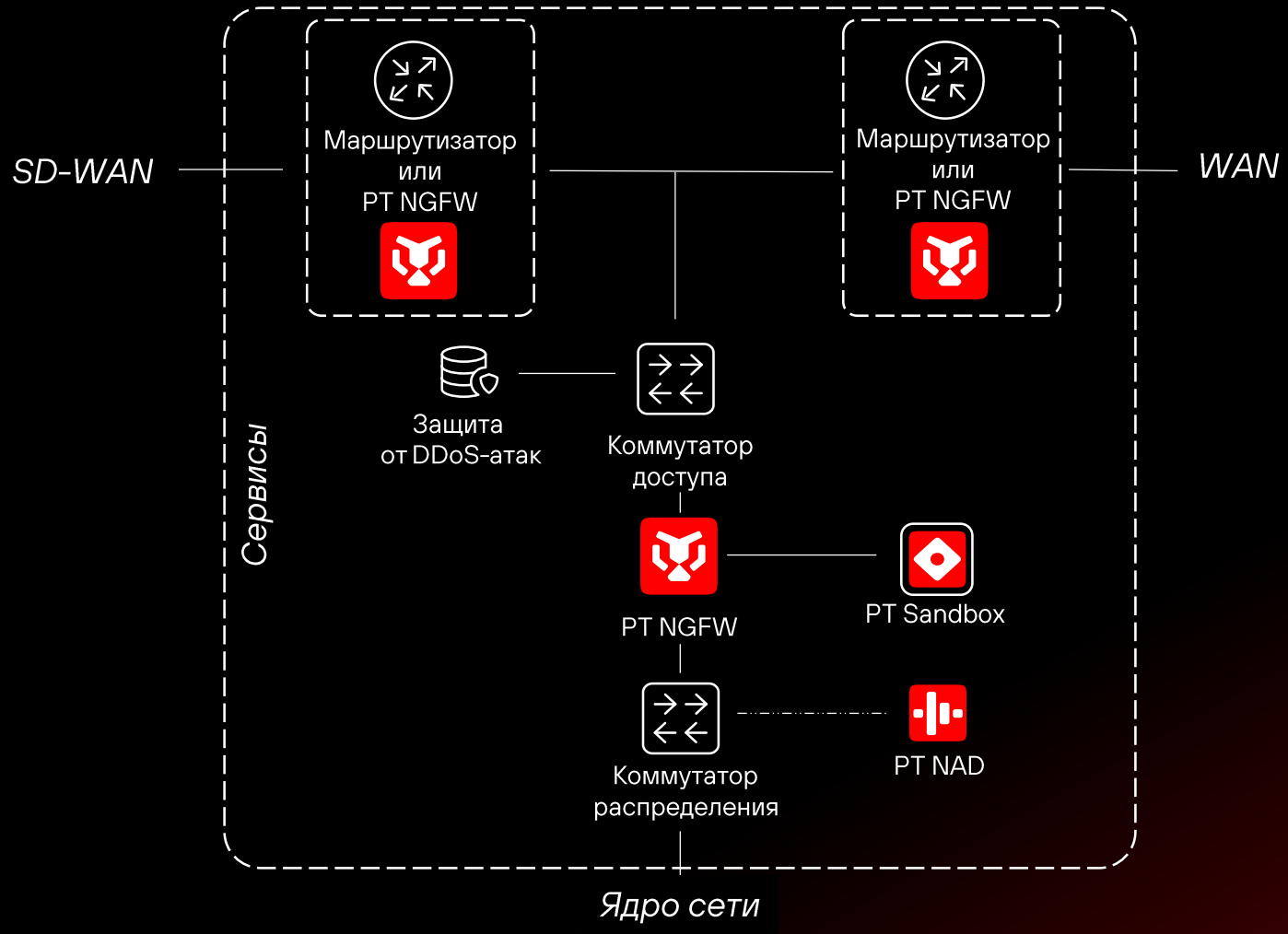
Сеть периметра



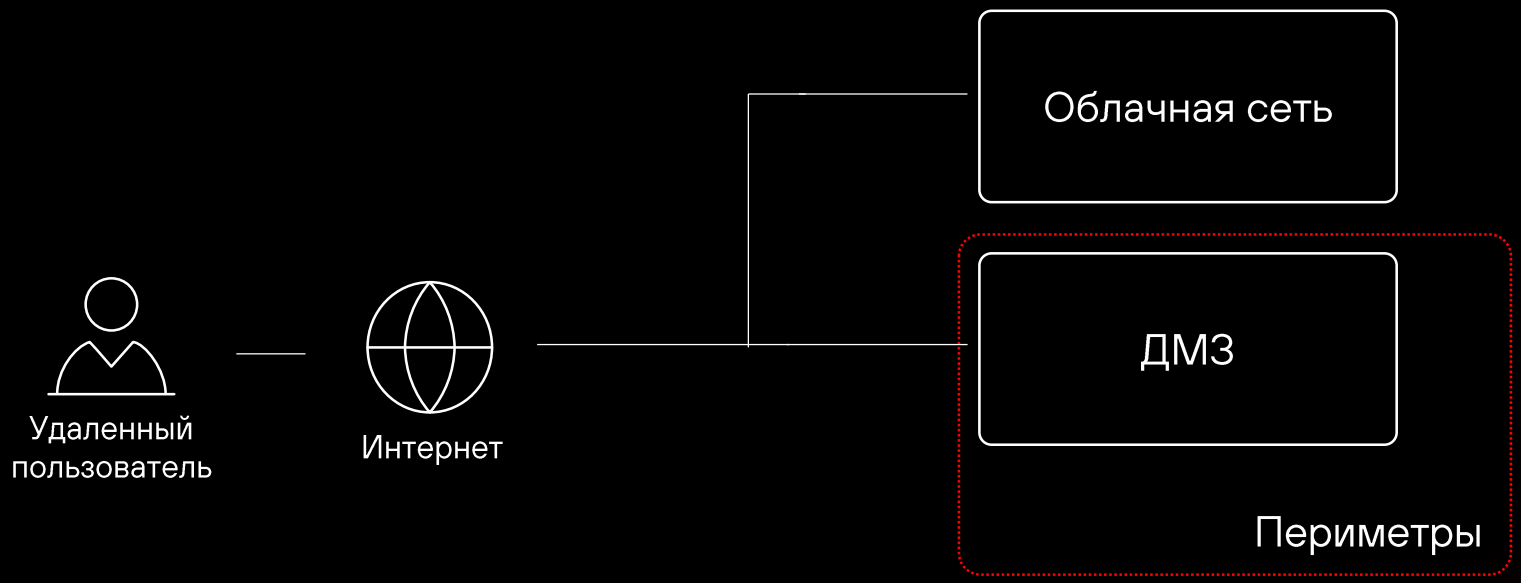
Особенности сети периметра

- Только сетевое оборудование
- Подключение к интернету
- Сервисные учетные записи (в том числе забытые)

Защита сети периметра



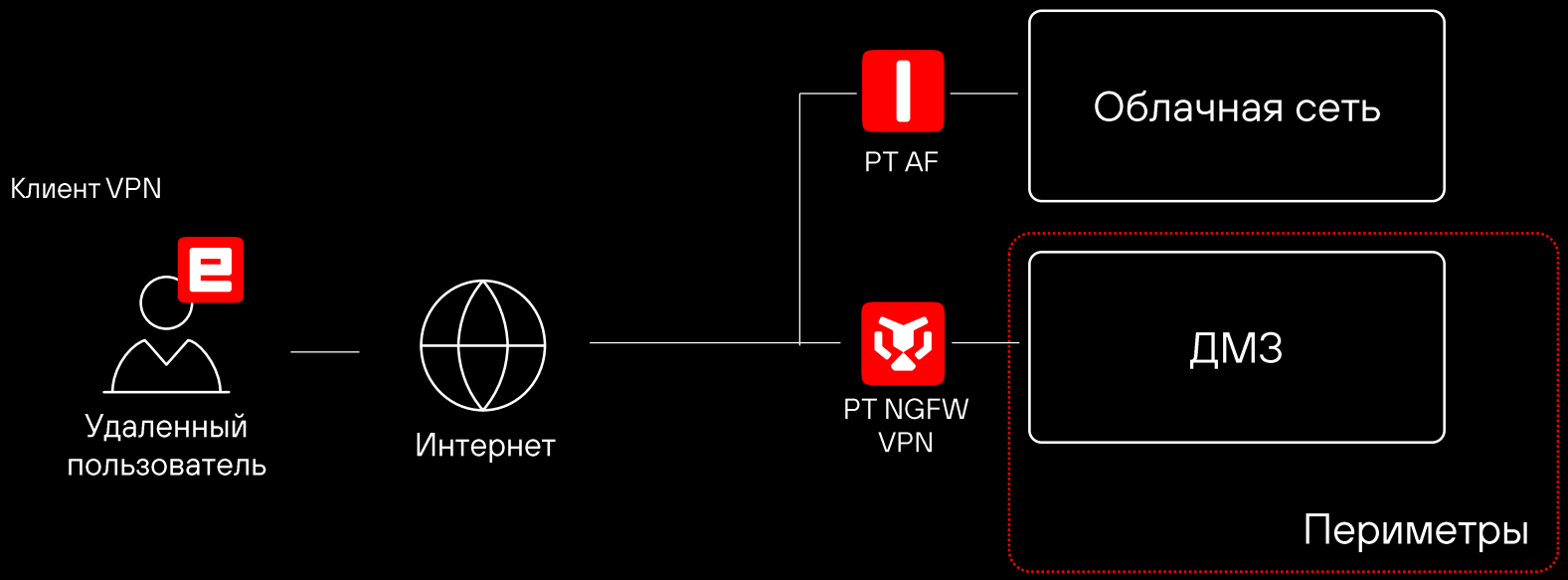
Удаленный пользователь



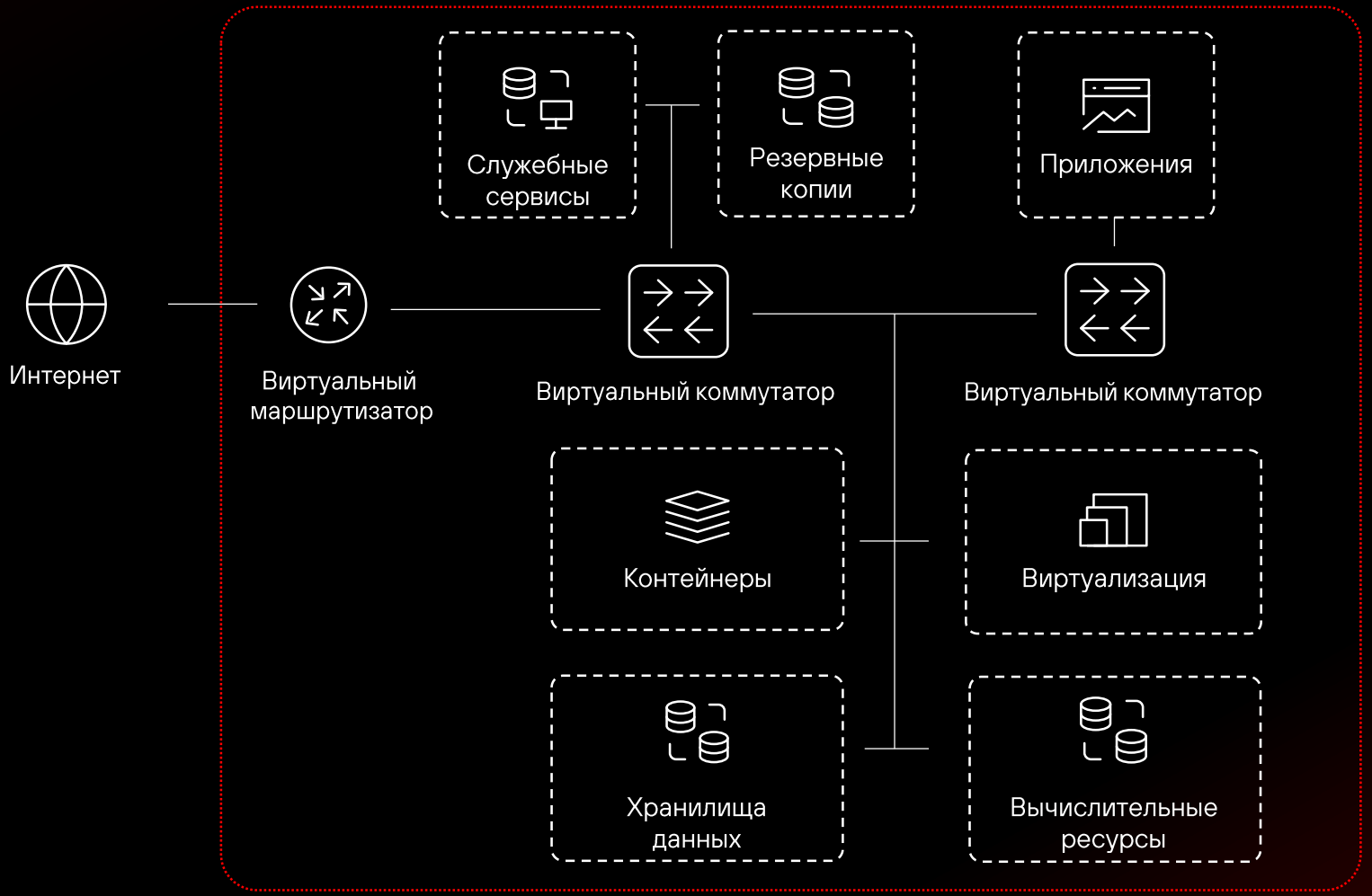
Особенности доступа удаленных пользователей

- Корпоративное устройство
- Корпоративное мобильное устройство
- Личное устройство
- Личное мобильное устройство
- Интернет вещей (неуправляемых)

Защита удаленного пользователя



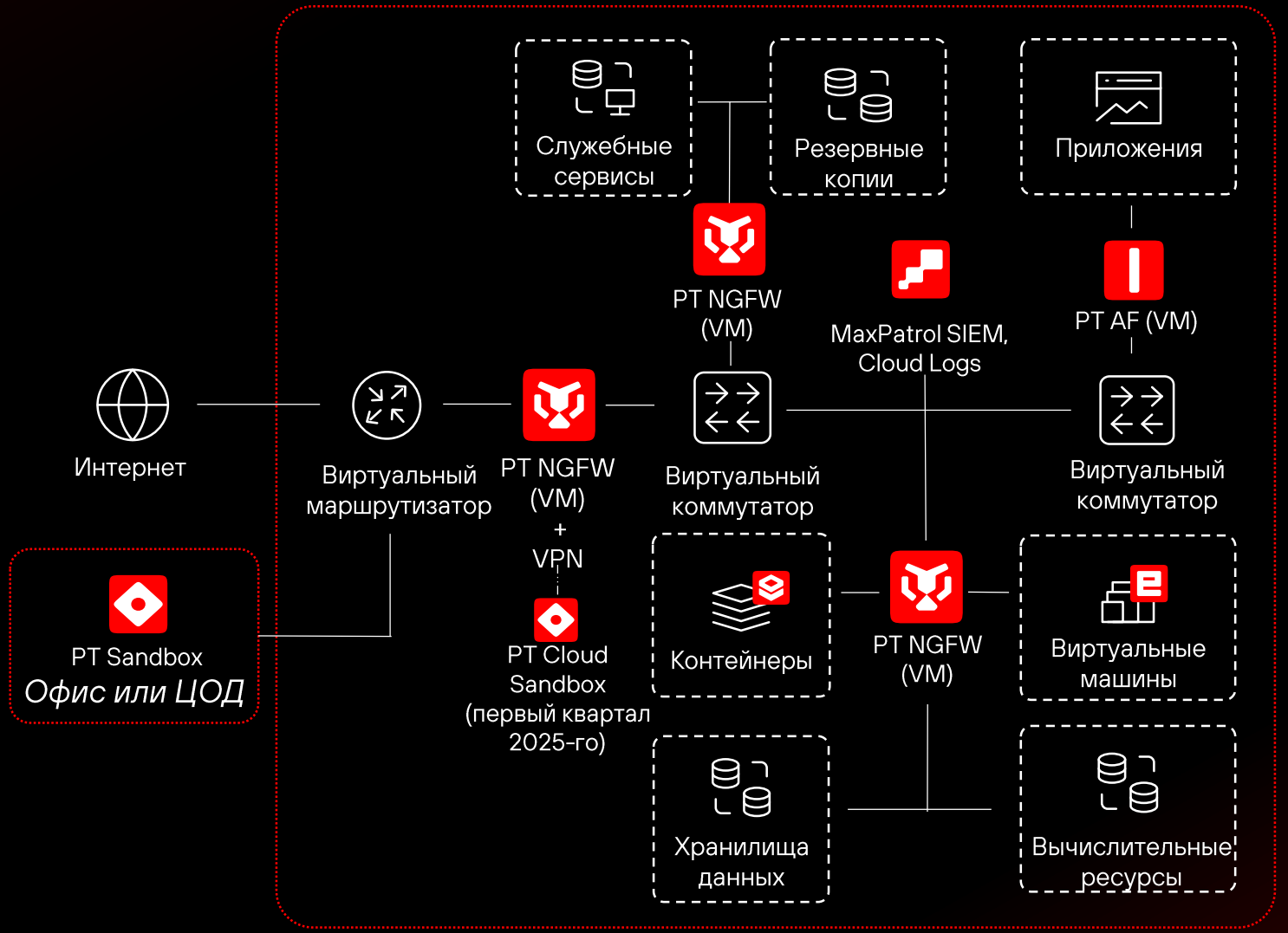
Облачная сеть



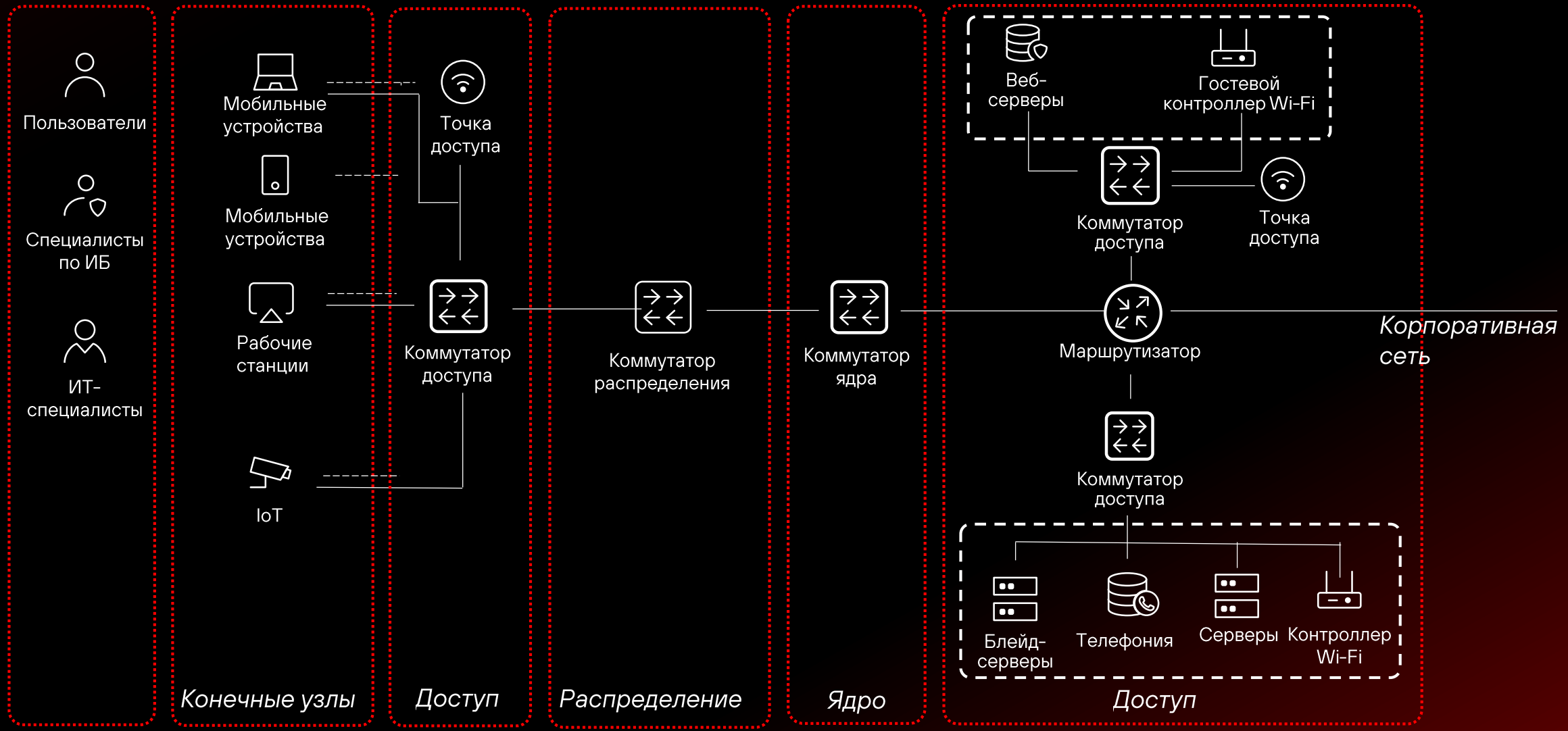
Особенности облачной сети

- Много зон безопасности
- Нет рабочих станций
- Все элементы инфраструктуры могут предоставляться как сервис
- Высокая скорость обновления ПО
- Подрядчики
- Доступ к ЦОД
- Доступ из офисной сети
- Доступ из ДМЗ
- Доступ из интернета
- Подключение удаленных пользователей

Защита облачной сети



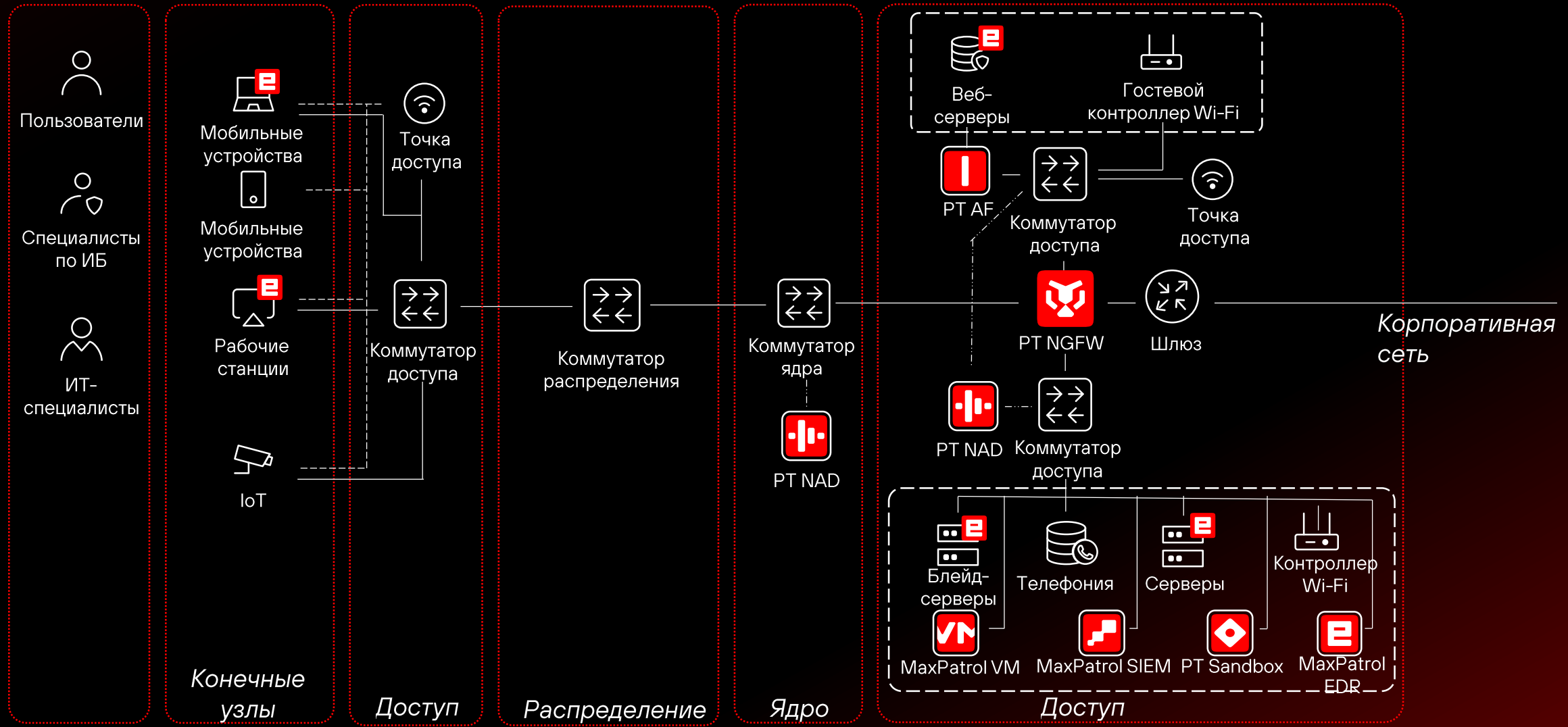
Изолированная сеть



Особенности изолированной сети

- Много зон безопасности
- Много рабочих станций
- Мобильные устройства
- Служебные серверы
- Специализированные шлюзы в корпоративную сеть
- Могут быть квалифицированные специалисты по ИТ и (или) ИБ
- Подрядчики
- Съемные носители

Защита изолированной сети



В заключение

Реальная архитектура СО РКБ индивидуальна для каждой организации

Укрепление и подтверждение надежности ИТ-инфраструктуры является обязательным шагом

При проектировании необходимо учитывать возможные цепочки атаки:

- точки проникновения,
- топологию,
- ключевые и целевые системы.

Непрерывная эволюция — запрос на автоматизацию

Спасибо!