UZCLOUD

Zero Trust как непрерывный процесс

IdP, ZTNA, SIEM в единой архитектуре

Мираброр Мирзохидов
Head of Security Products

Содержание

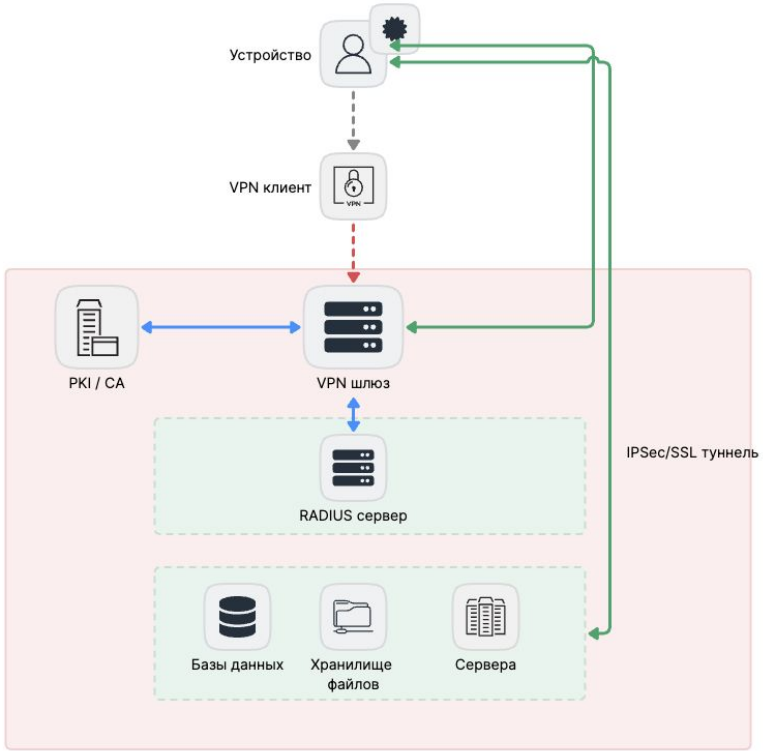
О чем будем говорить

- Классический подход к доступу
- Архитектура Zero Trust по NIST
- Trust Score - как считать доверие
- Три слоя сигналов - IdP, ZTNA, SIEM
- Policy Engine и ZTNA

VPN модель

Классическая модель доступа

- Аутентификация на периметре VPN сервера
- Установка IPSec/SSL туннеля
- Доверие на основе сегмента сети
- Sticky сессии (до явного выхода)
- Статичная авторизация (без пересмотра в runtime)
- Без обратной связи от endpoint



Допущения: аутентификация на входе подтверждает пользователя, сеть = безопасный периметр

Изменения, превращающие доступ в Zero Trust

Zero Trust модель

UZCLOUD

Ресурс имеет свой порог доверия в сети

Передача сигналов доверия в сети

Сравнение Score доверия с порогом ресурса

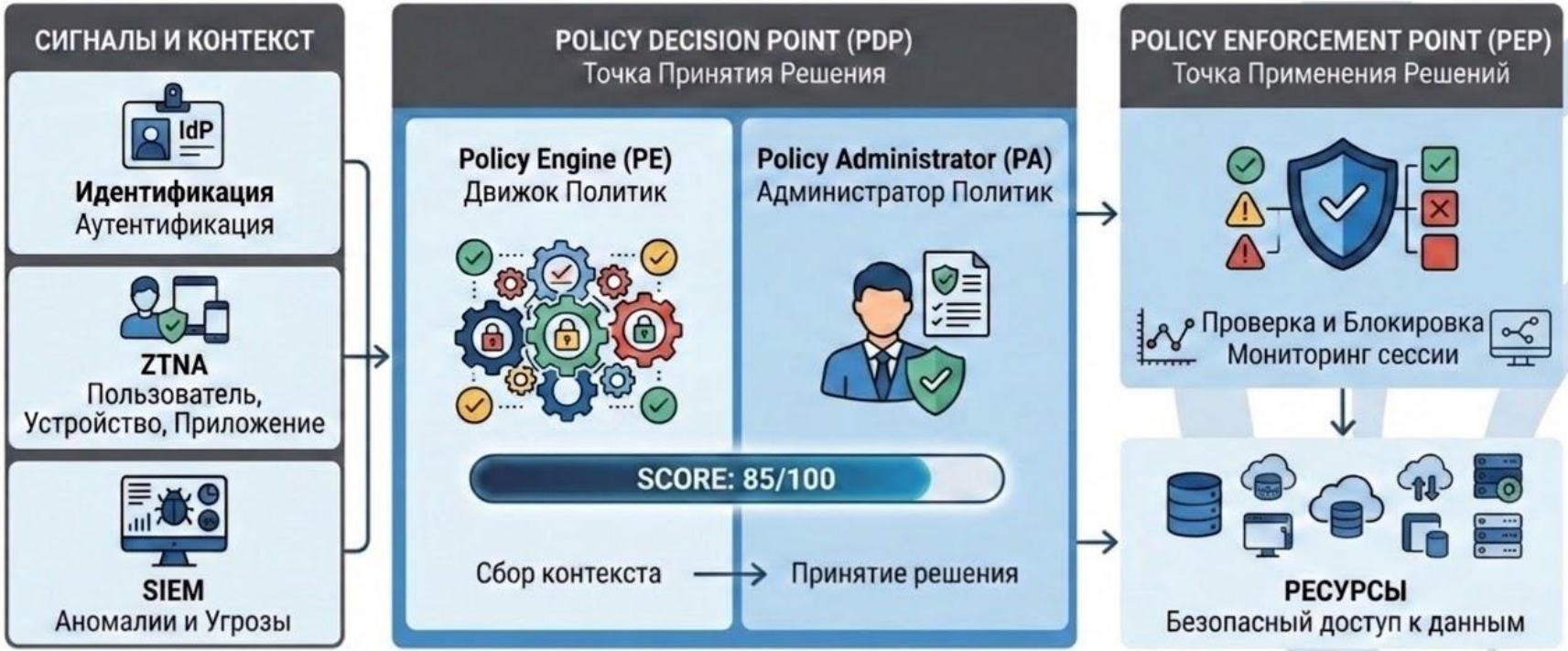
Пересчет скора и пересмотр решения

Policy Engine
Компонент оценки доверия

NIST SP 800-207

Архитектура Zero Trust по стандарту

UZCLOUD



Три категории источников сигналов

IdP, ZTNA, SIEM

UZCLOUD

Identity Provider (IdP)

Кто пользователь (PIP)
Okta, Microsoft Entra

Zero Trust Network Access (ZTNA*)

С какого устройства и из какой сети (PIP + PEP)
Zscaler, Cisco Duo

Security Information and Event Management (SIEM)

Что происходит внутри и вокруг систем (PIP)
Splunk, Elastic Security

**ZTNA != ZTA != Zero Trust*

Механизм подсчетов

Как считается Trust Score

UZCLOUD

- Каталог сигналов и веса в PE (yaml, json)
- Сбор сигналов из IdP, ZTNA, SIEM в кэше (Redis)
- Score = SUM(signal * weight)
- Сравнение с порогом ресурса (allow/deny)
- Пересчет по событию (инвалид. кэша -> решение)

Текущий Score сравнивается с порогом ресурса

Пороги ресурсов

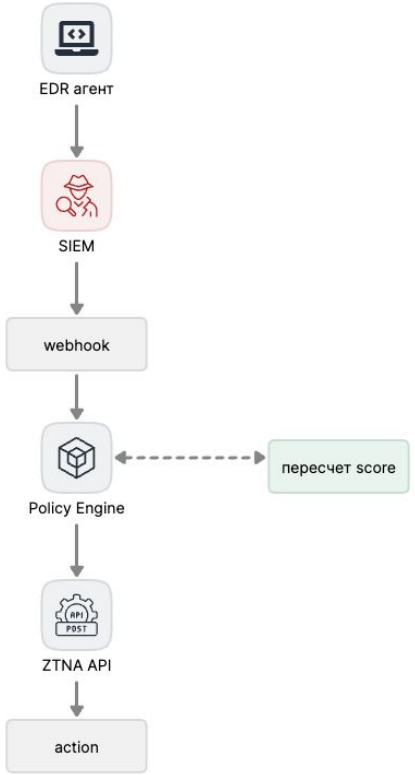
UZCLOUD

- Порог - числовой атрибут ресурса
- Калибровка по критичности данных
- Гранулярность на уровне ресурса
- Решение атомарное:
  - score >= порог -> allow
  - score < порог -> deny

SIEM нашел угрозу - score упал, доступ сократился

Пересчет при угрозе

- Webhook от SIEM
- Инвалидация кэша, изменение веса
- Пересчет score при угрозе
- Закрытие сессий с score ниже порога
- Автоматическое восстановление



Три слоя сигналов

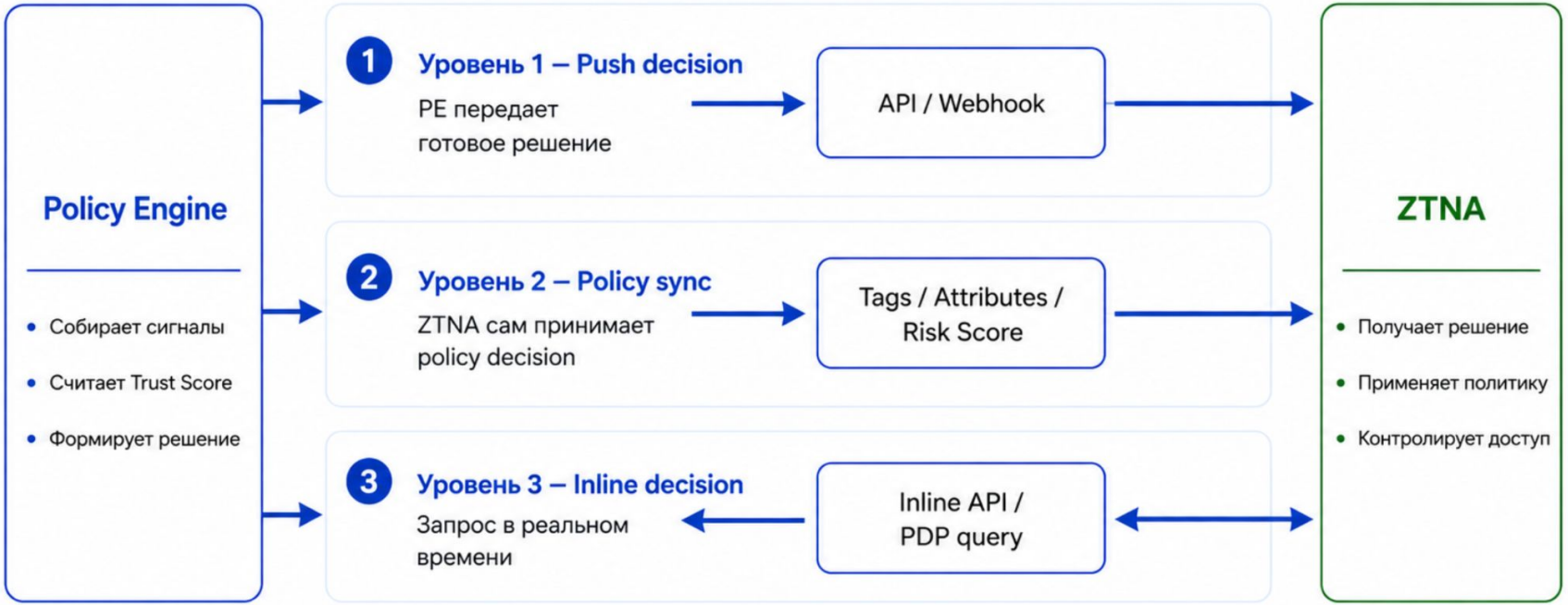
Что дает каждый слой Policy Engine

UZCLOUD

Как PE передает решение в ZTNA

Уровни интеграции PE и ZTNA

UZCLOUD



Финальные тезисы

Выводы из всей архитектуры

UZCLOUD

- Один и тот же IdP, ZTNA и SIEM может быть Zero Trust или нет
- Policy Engine - отдельный компонент, его придётся строить (OPA) (либо как часть платформы)
- Непрерывность строится на trust score, пересчитывается по событиям

Zero Trust = IdP + ZTNA + SIEM + Policy Engine