

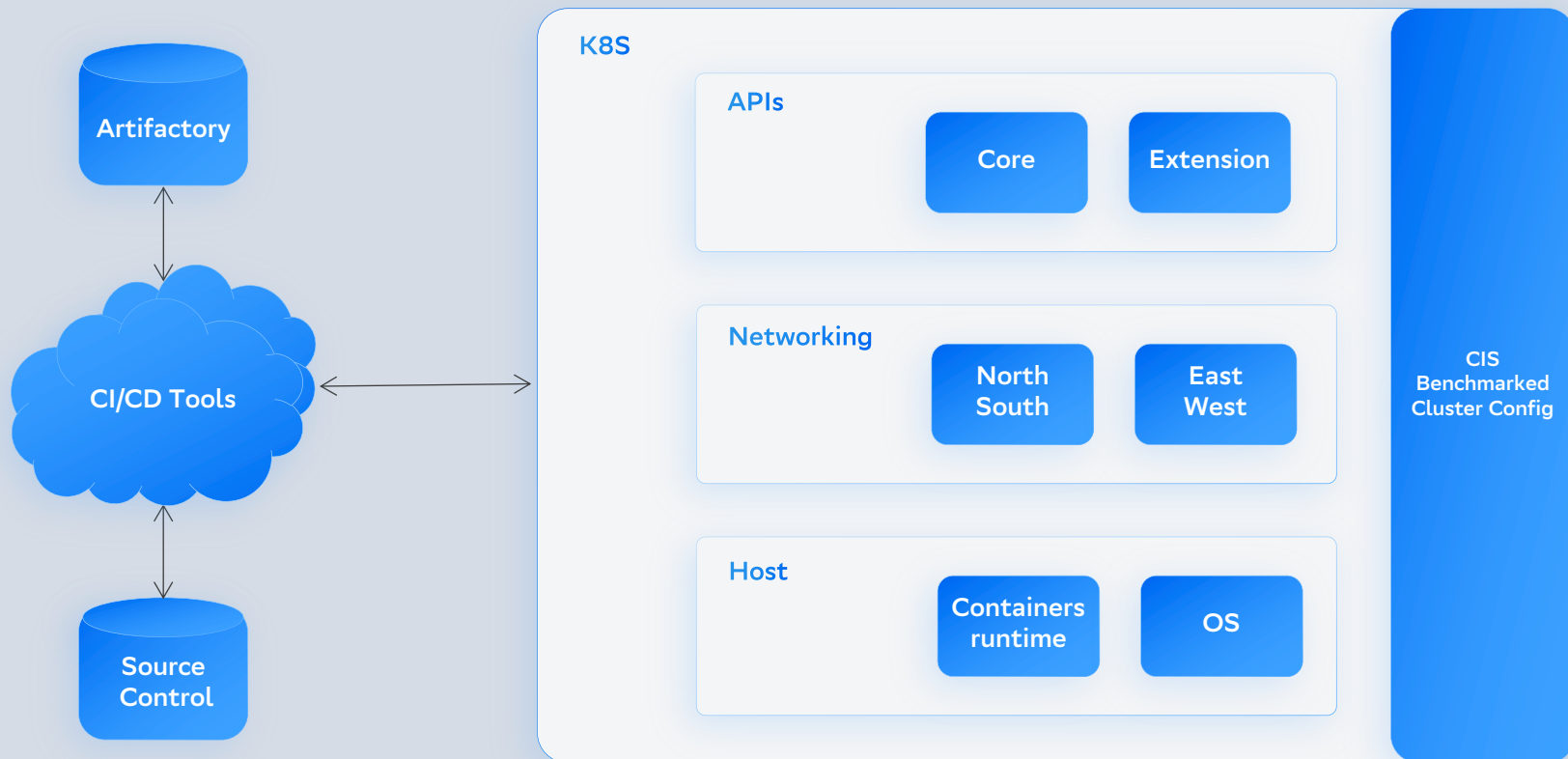
Механизмы безопасности микросервисных и мультиагентных систем в контейнеризованных средах

Максим Чудновский
Исполнительный директор, СберТех



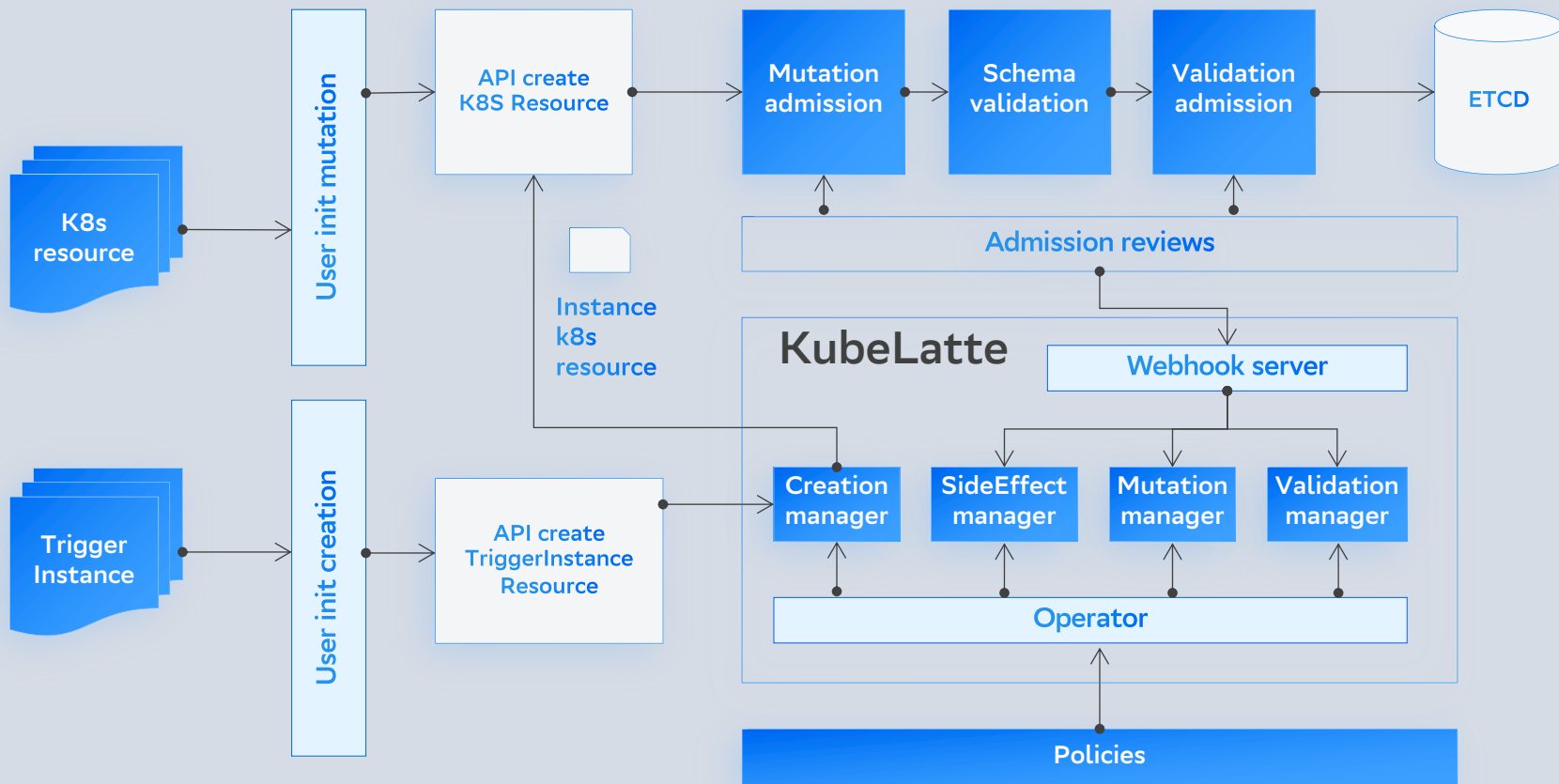
Векторы атак на Kubernetes

Векторы атак на Kubernetes



Контроль API

Что такое Policy Engine?



Что такое Policy Engine?

Зачем использовать

Автоматизация типовых сценариев эксплуатации приложений и кластеров

Обеспечение целостности конфигураций приложений и кластеров для предотвращения инцидентов при запуске и в рантайме

Реализация бесшовной миграции между разными дистрибутивами Kubernetes

Работа с манифестами

Валидация — проверка кода на соответствие спецификации Kubernetes

Мутация — изменение кода манифеста в соответствии со спецификацией Kubernetes

Генерация — создание кода манифеста в соответствии со спецификацией Kubernetes

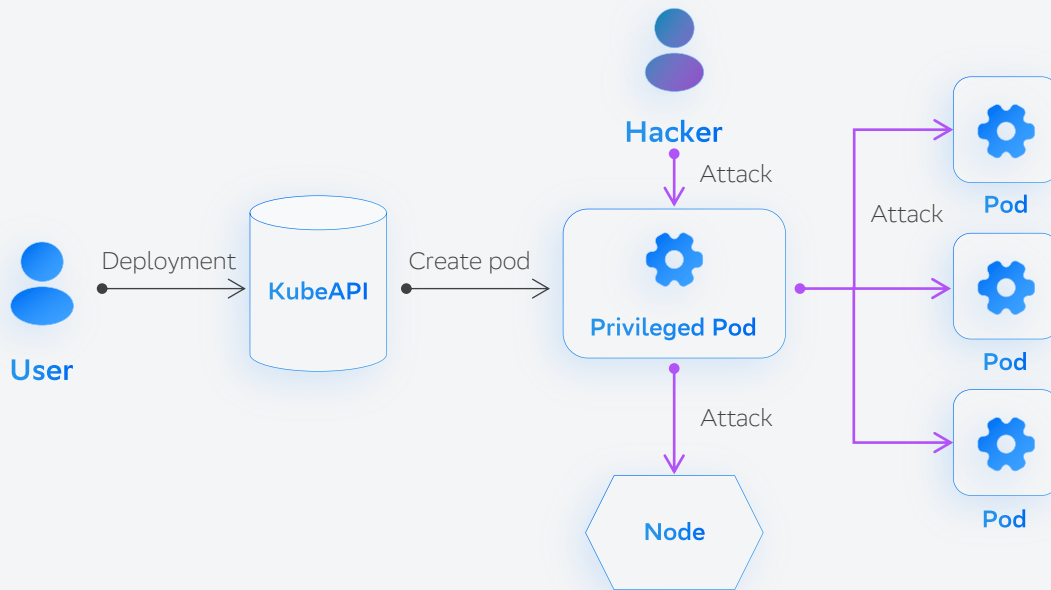
Пример OSS

Доступно на [GitVerse](#)



Кейс — контроль запуска подов

Контроль и валидация securityContext



Кейс — контроль запуска подов

Контроль и валидация securityContext

Без Policy Engine

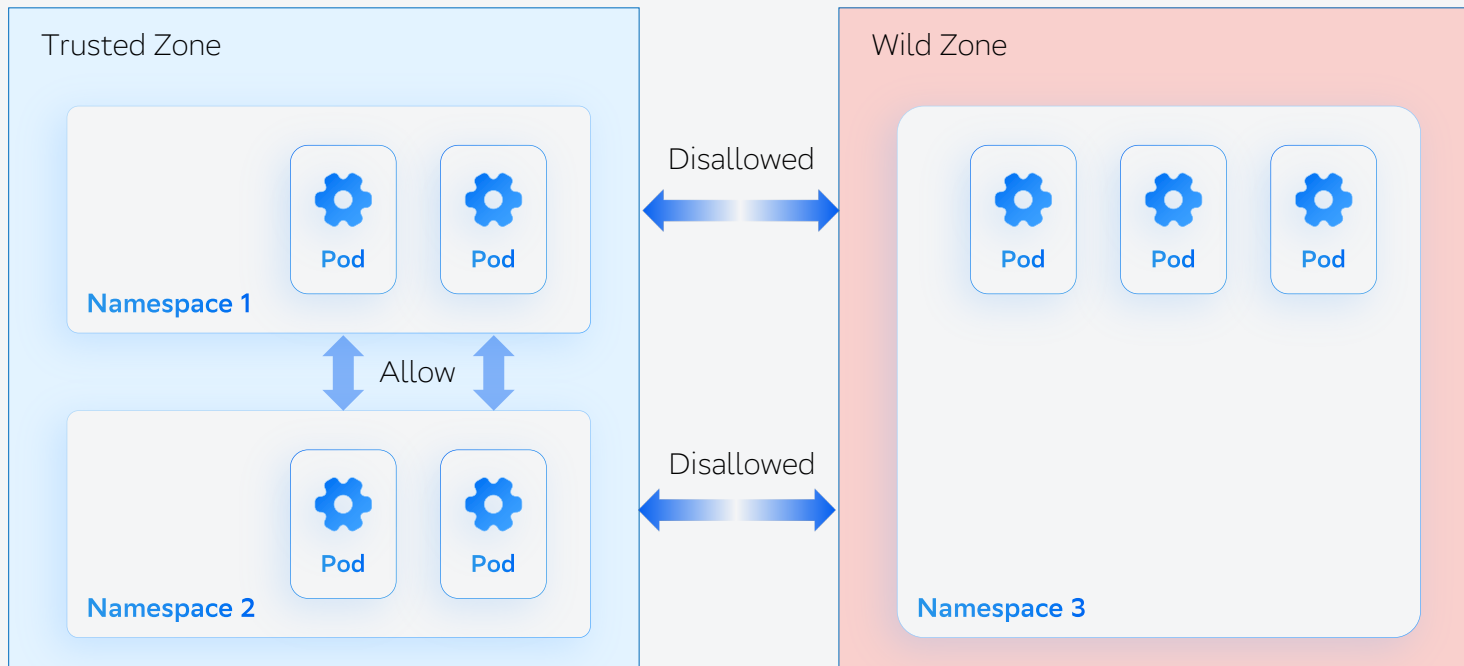
- Запуск в привилегированном режиме
- Нет контроля лишних привилегий
- Нет контроля рутового пользователя
- Ручной контроль каждого пода

С Policy Engine

- 1 конфиг с политиками
- Контроль используемых привилегий
- Запрет повышения привилегий
- Автоматический контроль запускаемых подов

Кейс — дефолтные network policies

Создание дефолтных NetworkPolicy при создании проекта k8s



Кейс — дефолтные network policies

Настройка дефолтных NetworkPolicy при создании проекта k8s

Без Policy Engine

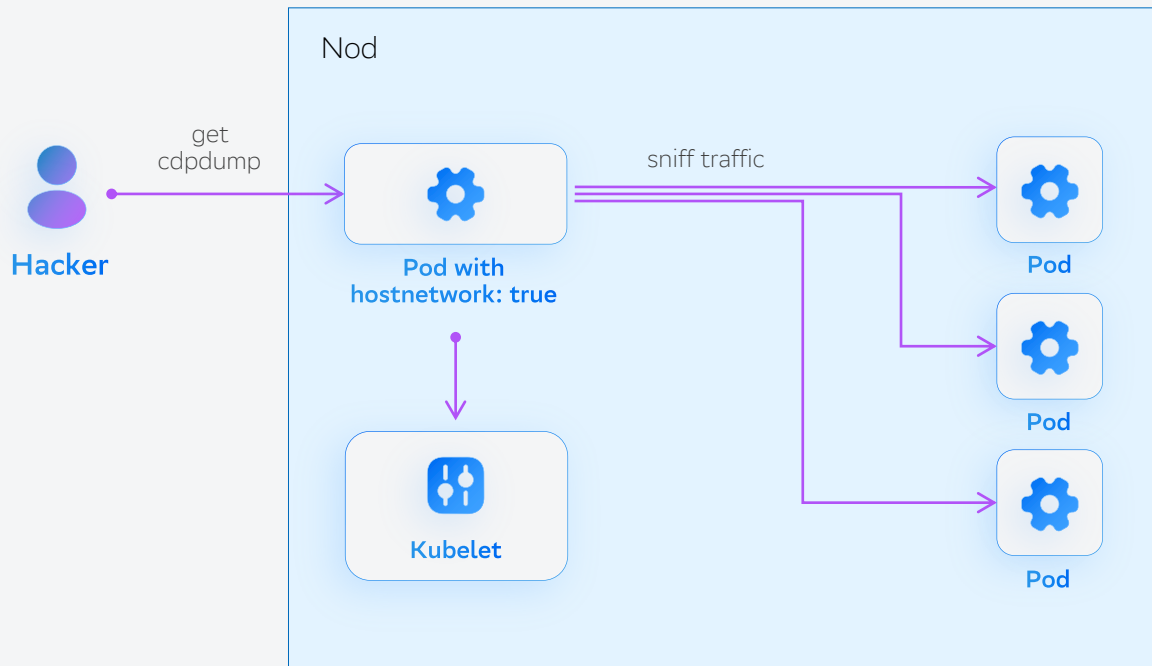
- Настройка под каждый проект сетевого доступа вручную
- Нет контроля, что сетевой доступ ограничен

С Policy Engine

- Автоматическое создание из шаблонов с возможностью параметризации
- Централизованное управление политиками доступа

Кейс — контроль HostNetwork Workload

Запрещено прибегать к HostNetwork



Кейс — контроль HostNetwork Workload

Запрещено прибегать к HostNetwork

Без Policy Engine

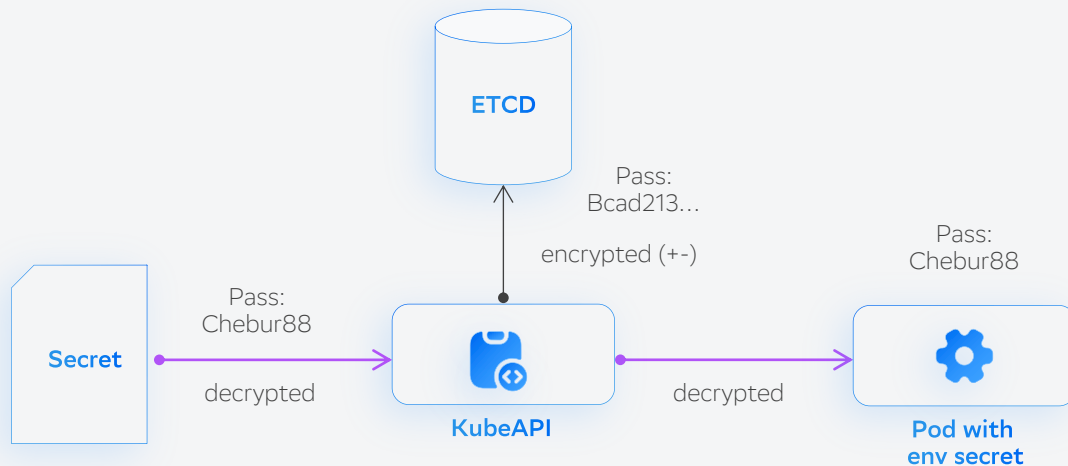
- Использование флага, где не надо
- Нет возможности запретить использование

С Policy Engine

- Контроль исключений
- Запрет в общих случаях использования

Кейс — контроль секретов в CM

Запрещаем экспортировать секреты в ENV



Кейс — контроль секретов в CM

Запрещаем экспортировать секреты в ENV

Без Policy Engine

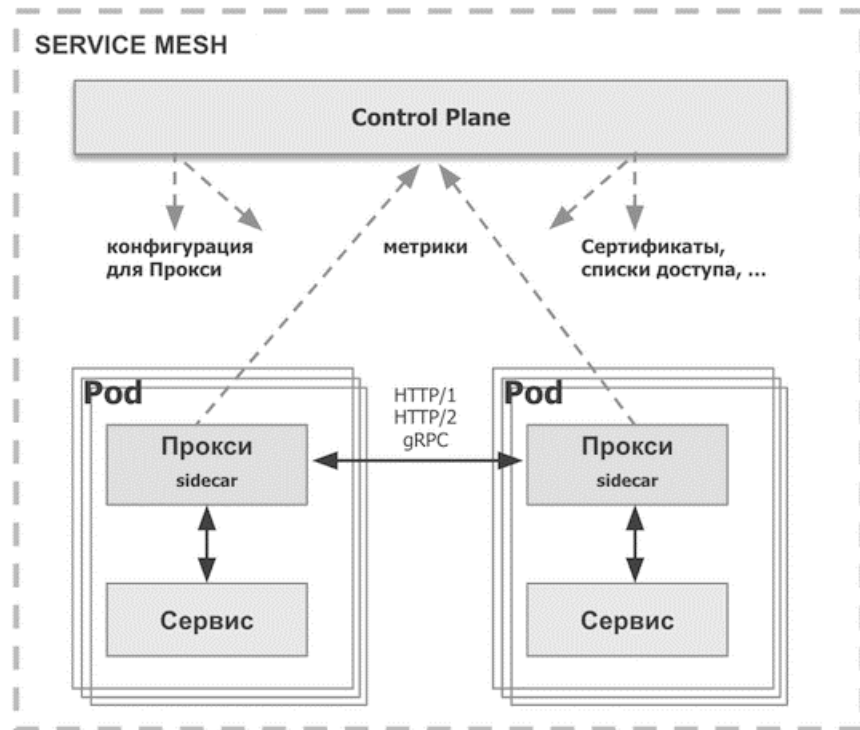
- Нет системы контроля за безопасной доставкой секретов в контейнер
- Есть вероятность компрометации доступов через переменные окружения

С Policy Engine

- Подключение секретов к контейнеру контролируется политиками безопасности, установленными на кластере
- Вероятность компрометации доступов через переменные окружения снижена

Контроль сети

Что такое Service Mesh



Управление общим состоянием кластера

01

Назначение и распространение политик маршрутизации и балансировки трафика

02

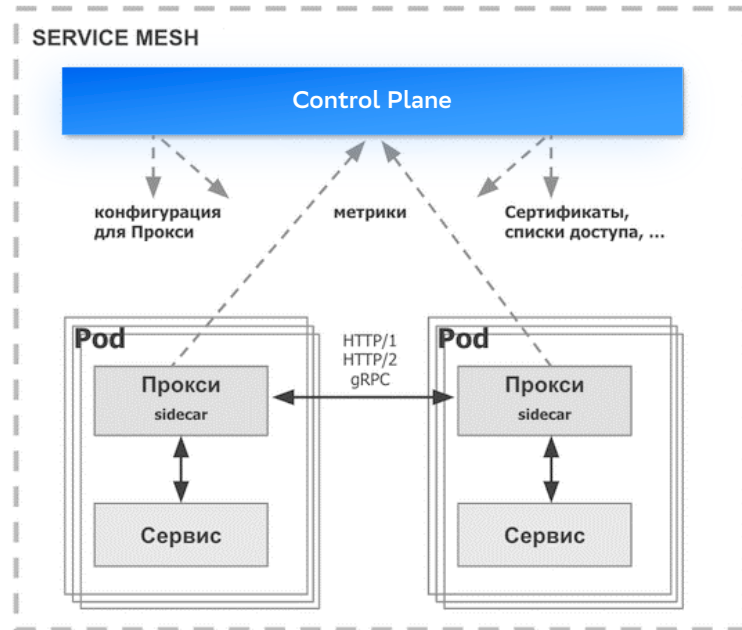
Распространение ключей, сертификатов, токенов

03

Сбор телеметрии, формирование метрик мониторинга

04

Интеграция с инфраструктурой безопасности и мониторинга



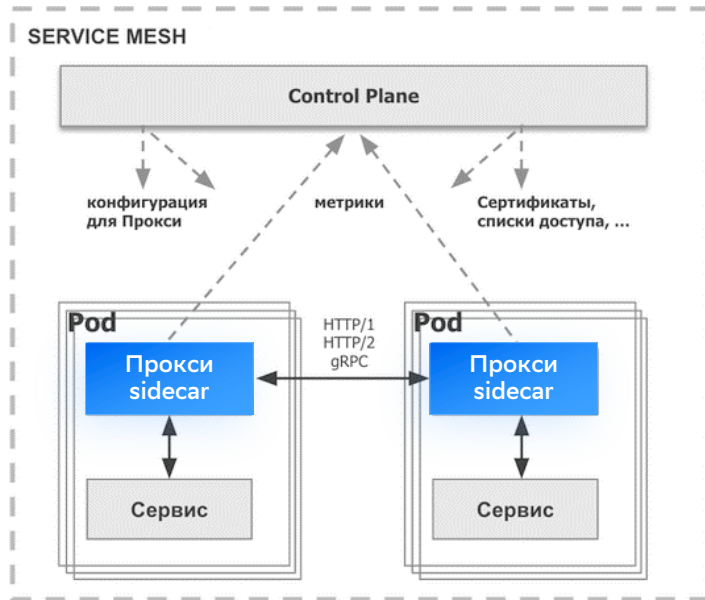
Обработка трафика между контейнерами

Маршрутизация и балансировка

Механизмы сетевой упругости
(тайм-ауты, предохранители и т. д.)

Аутентификация и авторизация
вызовов

Отбрасывание метрик
(observability)



Безопасность в Service Mesh



Аутентификация



Авторизация



Шифрование

Istio Security APIs

PeerAuthentication

```
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: default
  namespace: foo
spec:
  mtls:
    mode: STRICT
```

Istio Security APIs

PeerAuthentication

RequestAuthentication

```
apiVersion: security.istio.io/v1
kind: RequestAuthentication
metadata:
  name: httpbin
  namespace: foo
spec:
  selector:
    matchLabels:
      app: httpbin
  jwtRules:
    - issuer: "issuer-foo"
      jwksUri: https://example.com/.well-known/jwks.json
```

Istio Security APIs

PeerAuthentication

RequestAuthentication

AuthorizationPolicy

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: httpbin
  namespace: foo
spec:
  selector:
    matchLabels:
      app: httpbin
  rules:
    - from:
      - source:
          requestPrincipals: ["*"]
```

Istio Security APIs

PeerAuthentication

RequestAuthentication

AuthorizationPolicy

EnvoyFilter 😊

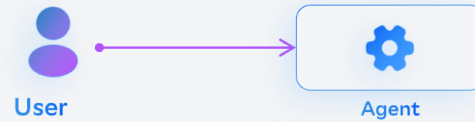
```
apiVersion: networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: ingw-int1-logs
spec:
  configPatches:
    - applyTo: NETWORK_FILTER
      match:
        context: ANY
        listener:
          filterChain:
            filter:
              name:
envoy.filters.network.http_connection_manager
      patch:
        operation: MERGE
        value:
          name:
```

...

AI Networking

AI Traffic

User To Agent



AI Traffic

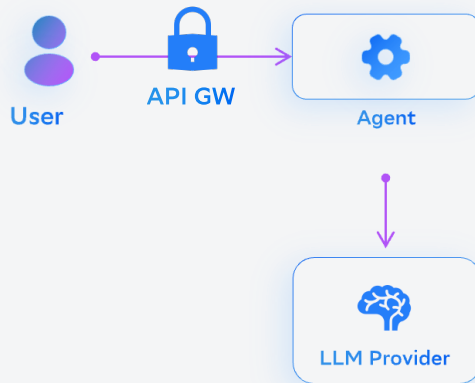
User To Agent



AI Traffic

User To Agent

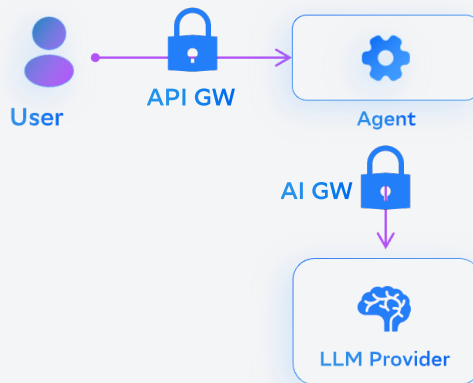
Agent To LLM



AI Traffic

User To Agent

Agent To LLM

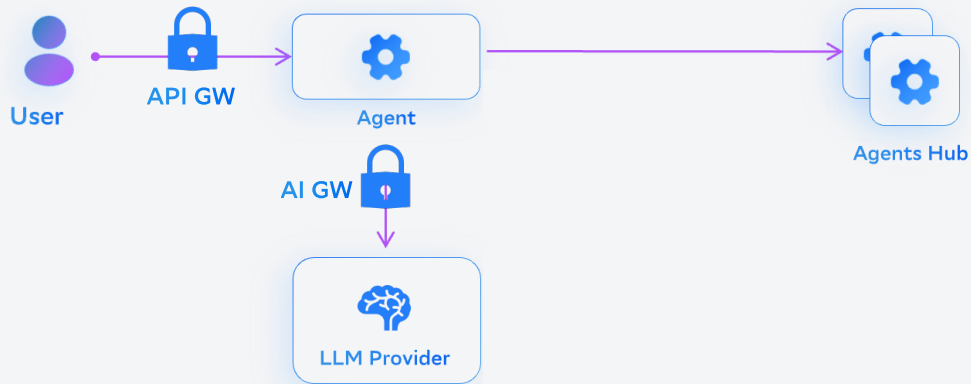


AI Traffic

User To Agent

Agent To LLM

Agent To Agent

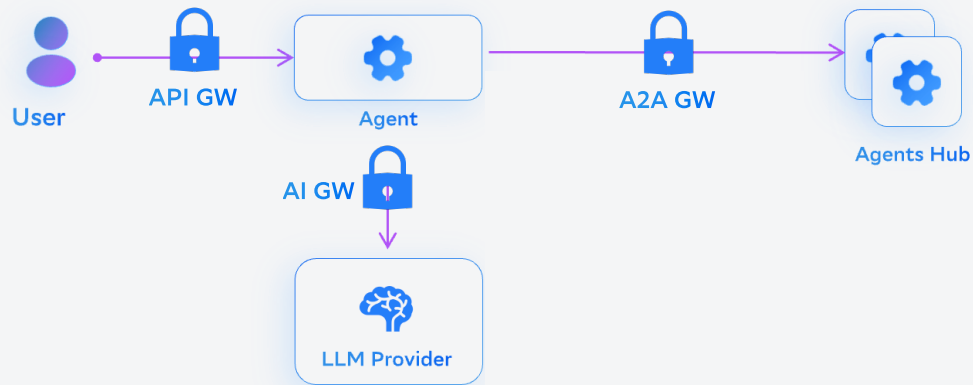


AI Traffic

User To Agent

Agent To LLM

Agent To Agent



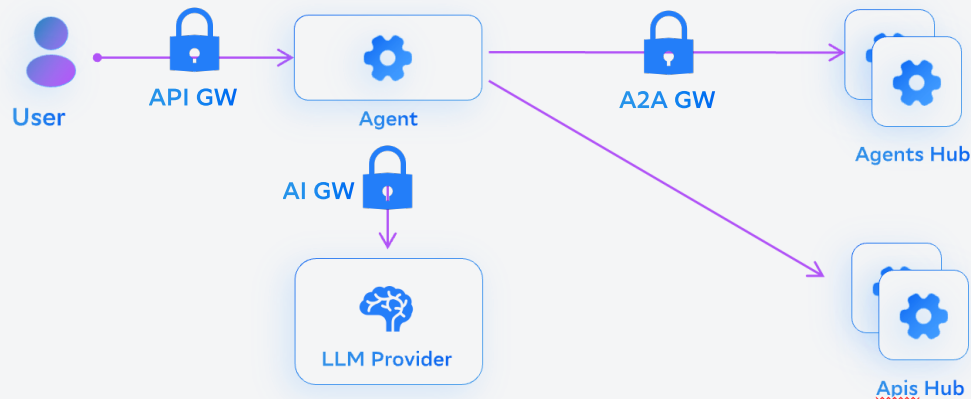
AI Traffic

User to Agent

Agent To LLM

Agent To Agent

Agent To API



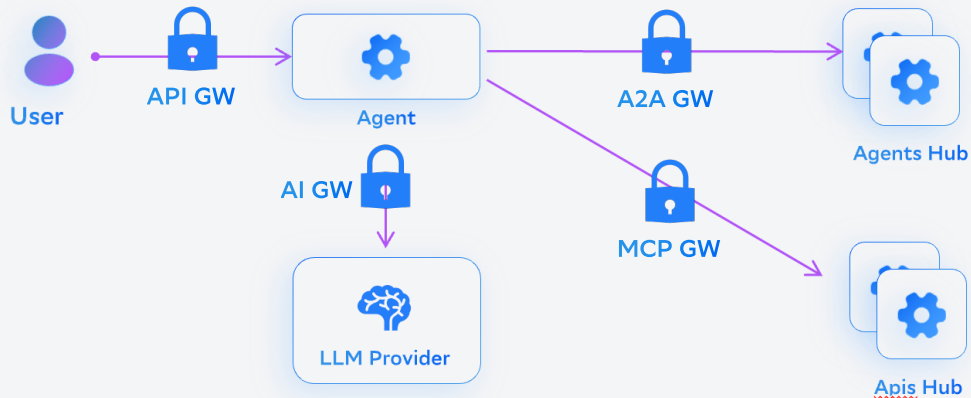
AI Traffic

User to Agent

Agent To LLM

Agent To Agent

Agent To API





**Максим
Чудновский**

Исполнительный
директор, СберТех

Вопросы?

