5 июня 2024 Москва, LOFT HALL#2

БЕКОН'24

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Строим заборы между сервисами

Андрей Бойцев

AppSec, Yandex Fintech

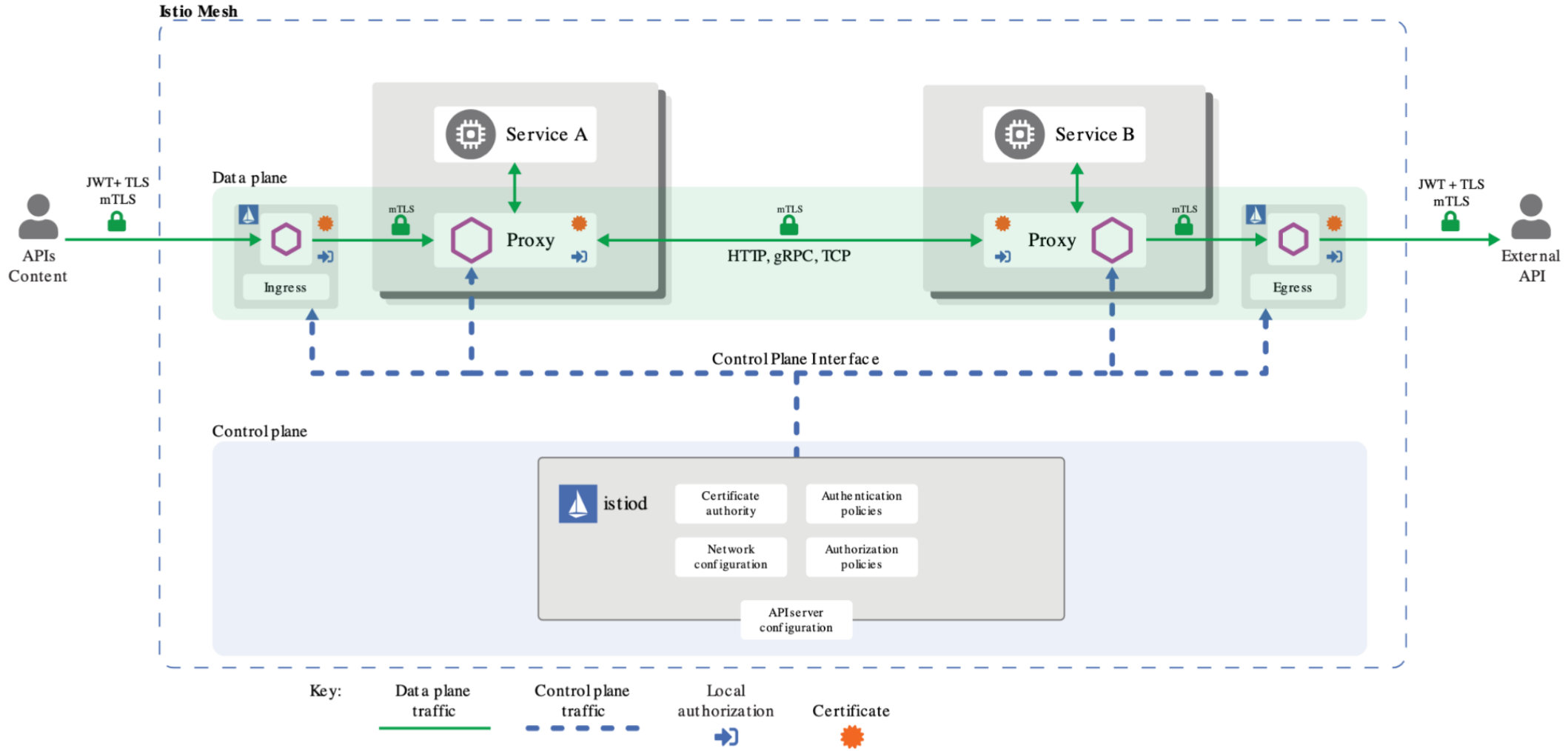
О чём расскажу

1. Istio и authorization policy
2. Как мы всё внедряли
3. Про баги, с которыми можно столкнуться
4. Выводы

01

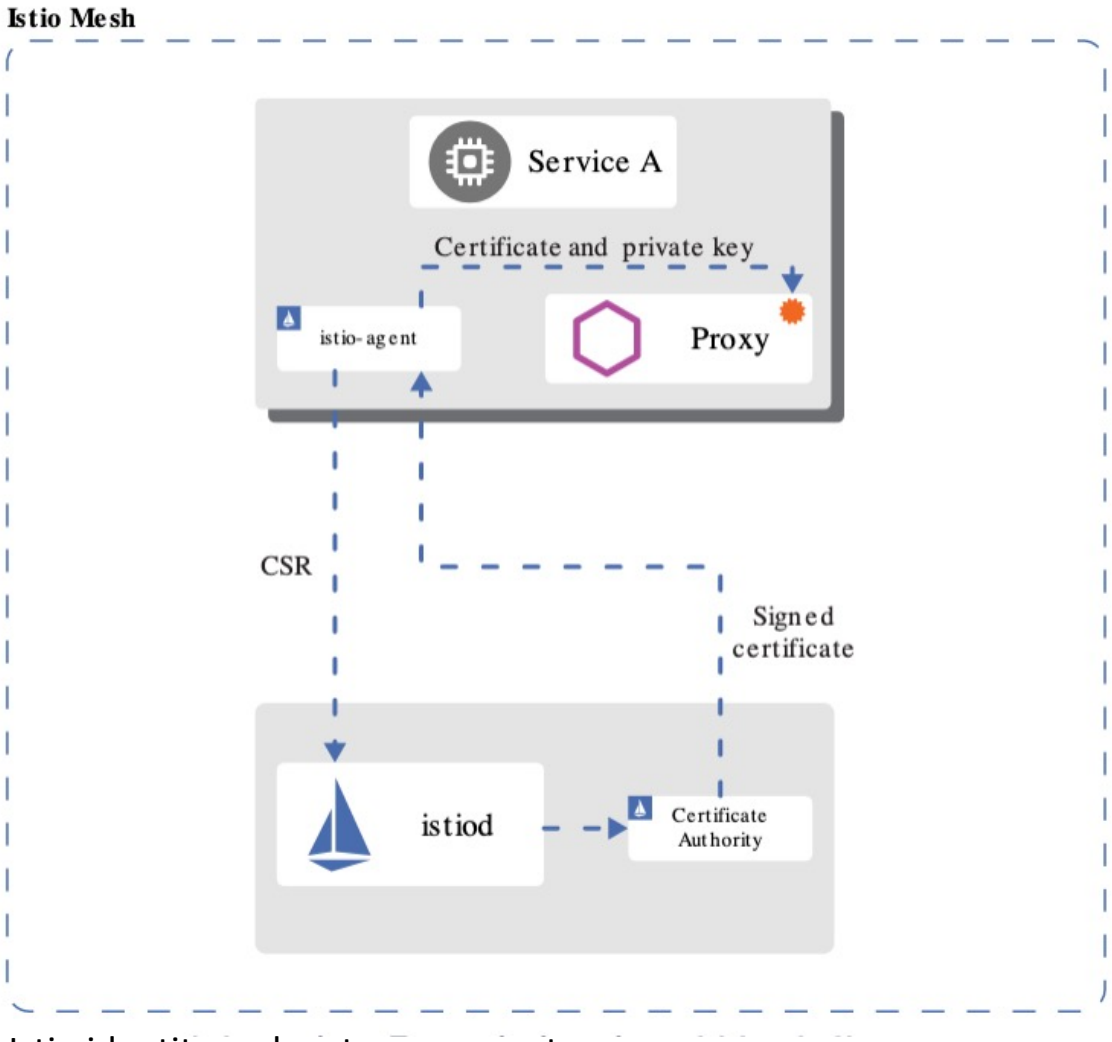
Istio и authorization policy

Control plane / Data plane



Istio hight level architecture

Certificate management



Istio identity and cert managment

Authorization policy

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: some-policy
  namespace: back
spec:
  action: ALLOW, DENY, AUDIT, CUSTOM
```

Authorization policy

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: some-policy
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
        principals: ["cluster.local/ns/back/sa/some-service"]
```

Authorization policy

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: some-policy
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
        principals: ["cluster.local/ns/back/sa/some-service"]
    to:
    - operation:
        methods: ["POST"]
        paths: ["/v1/path/*"]
```

Authorization policy

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: some-policy
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
        principals: ["cluster.local/ns/back/sa/some-service"]
    to:
    - operation:
        methods: ["POST"]
        paths: ["/v1/path/*"]
    when:
    - key: request.auth.claims[iss]
      values: ["https://issuer.some-issuer.ru"]
```

Authorization policy

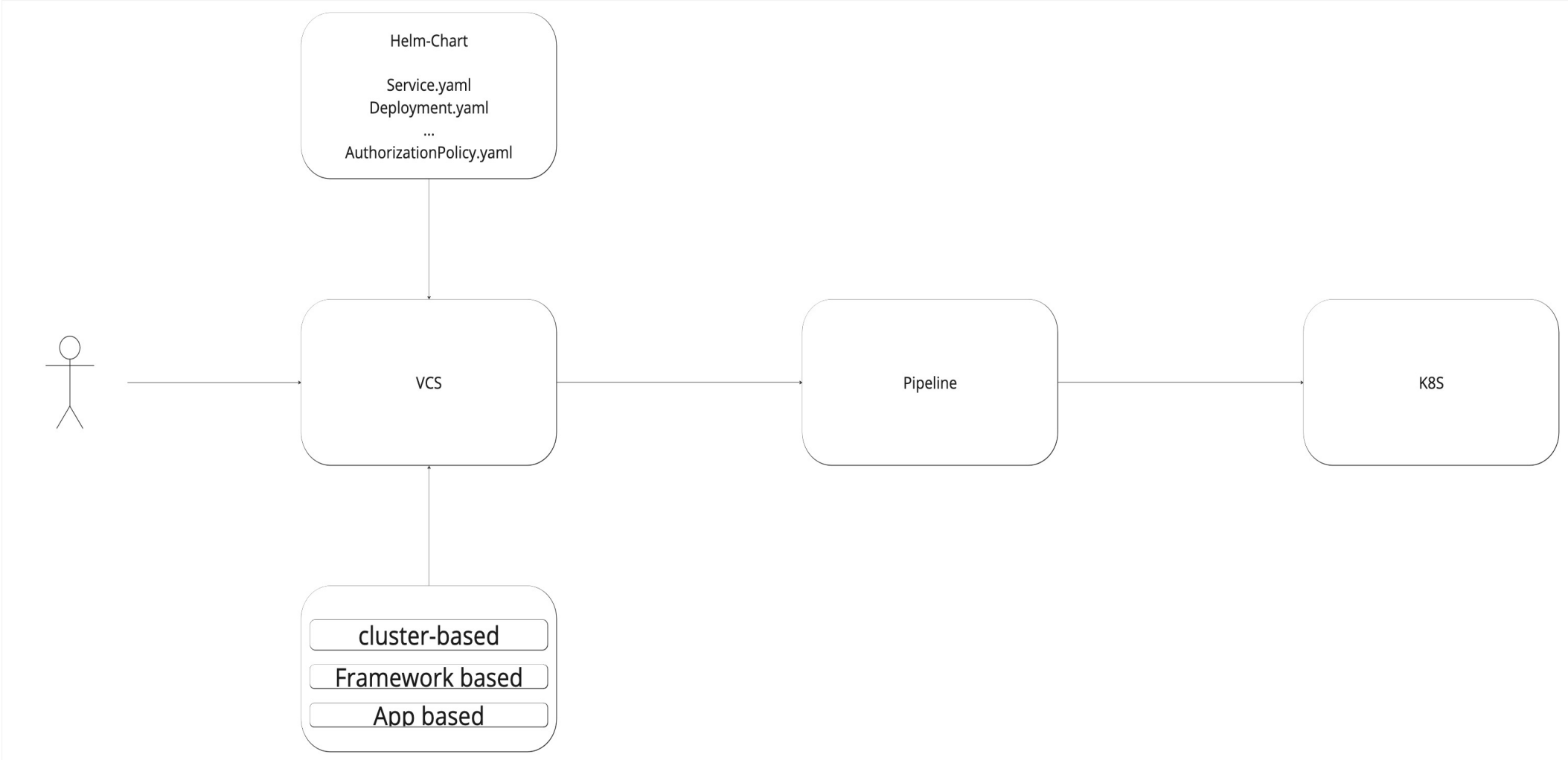
```yaml
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: some-policy
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
        principals: ["cluster.local/ns/back/sa/some-service"]
    to:
    - operation:
        methods: ["POST"]
        paths: ["/v1/path/*"]
    when:
    - key: request.auth.claims[iss]
      values: ["https://issuer.some-issuer.ru"]
```

```
"type.googleapis.com/envoy.extensions.filters.http.rbac.v3.RBAC"
"rules": {
   "policies": {
   "ns[back]-policy[some-policy]-rule[0]": {
"permissions": [
{
"and_rules": {
   "rules": [{
   "or_rules": {
"rules": [{
 "header": {
   "name": ":method",
   "string_match": {
   "exact": "POST"
}}}]}},
{
"or_rules": {
"rules": [
{
 "url_path": {
  "path": {
   "prefix": "/v1/some-path/",
   "principals": [{
"and_ids": {
 "ids": [{
  "or_ids": {
   "ids": [{
    "authenticated": {
     "principal_name": {
      "exact": "spiffe://cluster.local/ns/back/sa/some-service"
}
```

02

Про внедрение

Как мы катим сервисы



С чего мы начинали

- Начинали с allow-all-политики
- Разрешено всё общение внутри кластера
- Запрещены все походы из-за пределов кластера
- Все сервисы катились без оверрайдов authpolicy

```
apiVersion: security.istio.io/v1beta1
kind: AuthorizationPolicy
 rules:
 {{- if .Values.authpolicy.allow_rules }}
 {{- toYaml .Values.authpolicy.allow_rules | nindent 2 }}
 {{- end }}
 - to:
   - operation:
       methods: ["GET"]
       paths:
         - /stats/prometheus
         {{- if .Values.monitoring.enabled }}
         - {{ .Values.monitoring.path }}
         {{- end }}
 {{- if or .Values.authpolicy.default_allow_inside_k8s
.Values.istioingress.commonRemoteIpBlocks
.Values.istioingress.remoteIpBlocks }}
 - from:
   {{- if .Values.authpolicy.default_allow_inside_k8s }}
   - source:
       notNamespaces: ["istio-system"]
       principals: ["*"]
   {{- end }}
```

План

- Описываем дефолтные политики
- Добавляем Authorization Policy в базовые требования к сервисам
- Пишем политики для существующих сервисов
- Проверяем написанные политики
- Переписываем дефолты

Инвентаризируем, что имеем

- Пишем шаблоны для базовых политик
- Инвентаризируем сервисы в кластере
- Инвентаризируем походы в отдельно взятый сервис

Шаблоны для базовых политик

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: foo
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
      principals:["cluster.local/ns/<namespace>/sa/<service-name>"]
    to:
    - operation:
        methods: ["POST"]
        paths: ["controller-prefix"]
```

Шаблоны для базовых политик

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: foo
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
      principals:[”cluster.local/ns/istio-system/sa/istio-ingress"]
    to:
    - operation:
        methods: ["POST"]
        paths: ["controller-prefix"]
    when:
         - key: request.headers[CN]
           values:
             - "CN=certificate-info"
```

Как писать политики

- Пишем всё руками

Как писать политики

- Пишем всё руками
- Генерируем через kiali

Как писать политики

- Пишем всё руками
- Генерируем через kiali
- Автоматизируем

Генератор для политик

- Используем метрики для генерации политик
- Используем шаблоны для новых сервисов
- Используем OpenApi спеки сервисов
- Обходим граф путей сервиса для генерации префиксов

Генератор для политик

```
             aboycev$ ./gatekeeper --service bank-acc           --namespace back --cluster uat authpolicy
authpolicy:
  default_allow_inside_k8s: false
  allow_rules:
  - from:
    - source:
        principals:
        - cluster.local/ns/back/sa/bank-appl
        - cluster.local/ns/back/sa/bank-buid
        - cluster.local/ns/back/sa/bank-comm
        - cluster.local/ns/back/sa/bank-user
    to:
    - operation:
        methods:
        - POST
        paths:
        - /access-control-internal/v1/apply-policies
  - from:
    - source:
        principals:
        - cluster.local/ns/back/sa/bank-wall
    to:
    - operation:
        methods:
        - POST
        paths:
        - /access-control-internal/v2/apply-policies
```

Проверяем политики

- В политике не используются ipBlocks

Проверяем политики

- В политике не используются ipBlocks
- В политике не используется principals: ["*"]

Проверяем политики

- В политике не используются ipBlocks
- В политике не используется principals: ["*"]
- В политике не используются principals: ["istio-ingress"]

Проверяем политики

- В политике не используются ipBlocks
- В политике не используется principals: ["*"]
- В политике не используются principals: ["istio-ingress"]
- Доступ от внешних сервисов только к конкретным путям приложения

03

Про баги, с которыми можно столкнуться

Что не так с этой политикой?

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: foo
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
      principals:["cluster.local/ns/front/sa/front-app"]
    to:
    - operation:
        methods: ["POST"]
        notPaths: ["/v1/approve"]

selector:
    matchLabels:
       app.kubernetes.io: role-approver
```

Что не так с этой политикой?

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: foo
  namespace: back
spec:
  action: ALLOW
  rules:
  - from:
    - source:
      principals:["cluster.local/ns/front/sa/front-app"]
    to:
    - operation:
        methods: ["POST"]
        notPaths: ["/v1/approve"]

selector:
    matchLabels:
       app.kubernetes.io: role-approver
```

- /v1/Approve
- /v1/approve/
- Что ещё?

~~Не~~ придерживаемся базовых правил

Рекомендации от Istio

- Allow with positive matching
- Deny with negative matching

Примеры

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: foo
spec:
  action: ALLOW
  rules:
  - to:
   - operation:
     paths: ["/public"]
```

```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: foo
spec:
  action: DENY
  rules:
  - to:
   - operation:
     notPaths: ["/public"]
```

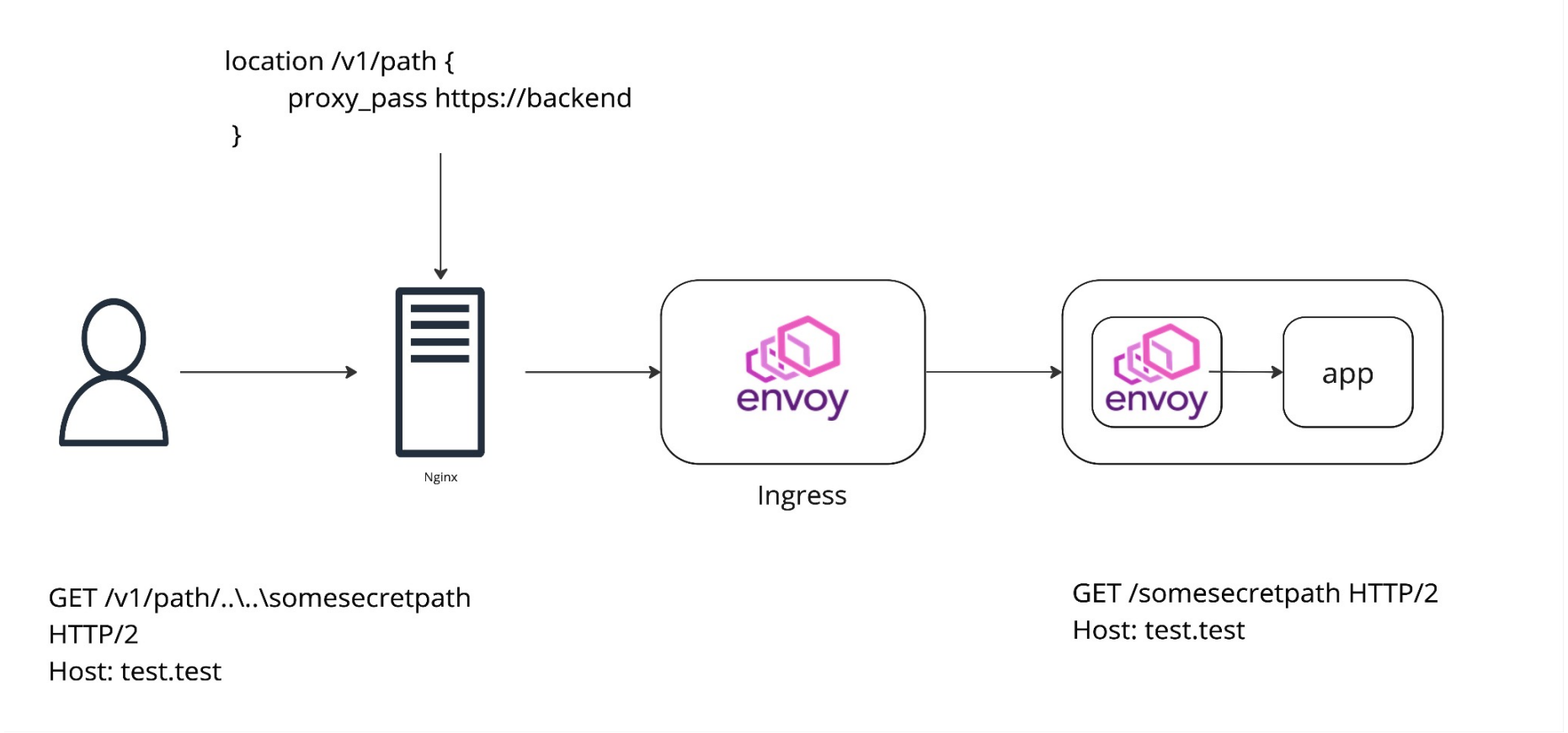
Выводы

- Придерживаемся безопасных паттернов

Нормализация

Тип нормализации	Описание
DEFAULT	Дефолтная нормализация
NONE	Без нормализации
BASE	RFC 3986, конвертация \ в /
MERGE_SLASHES	Base + объединение слешей
DECODE_AND_MERGE_SLASHES	Декодинг + merge_slashes

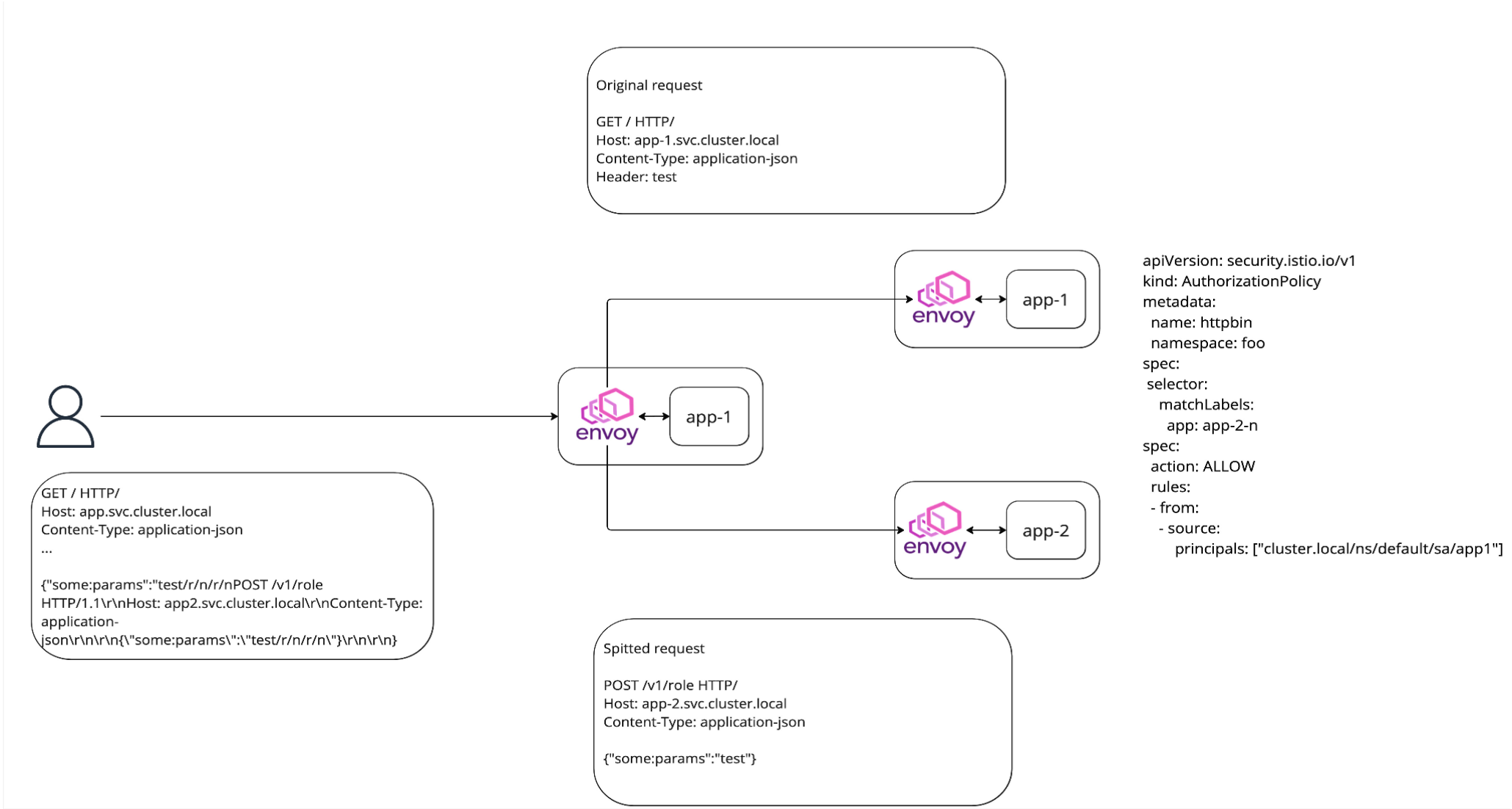
Нормализация



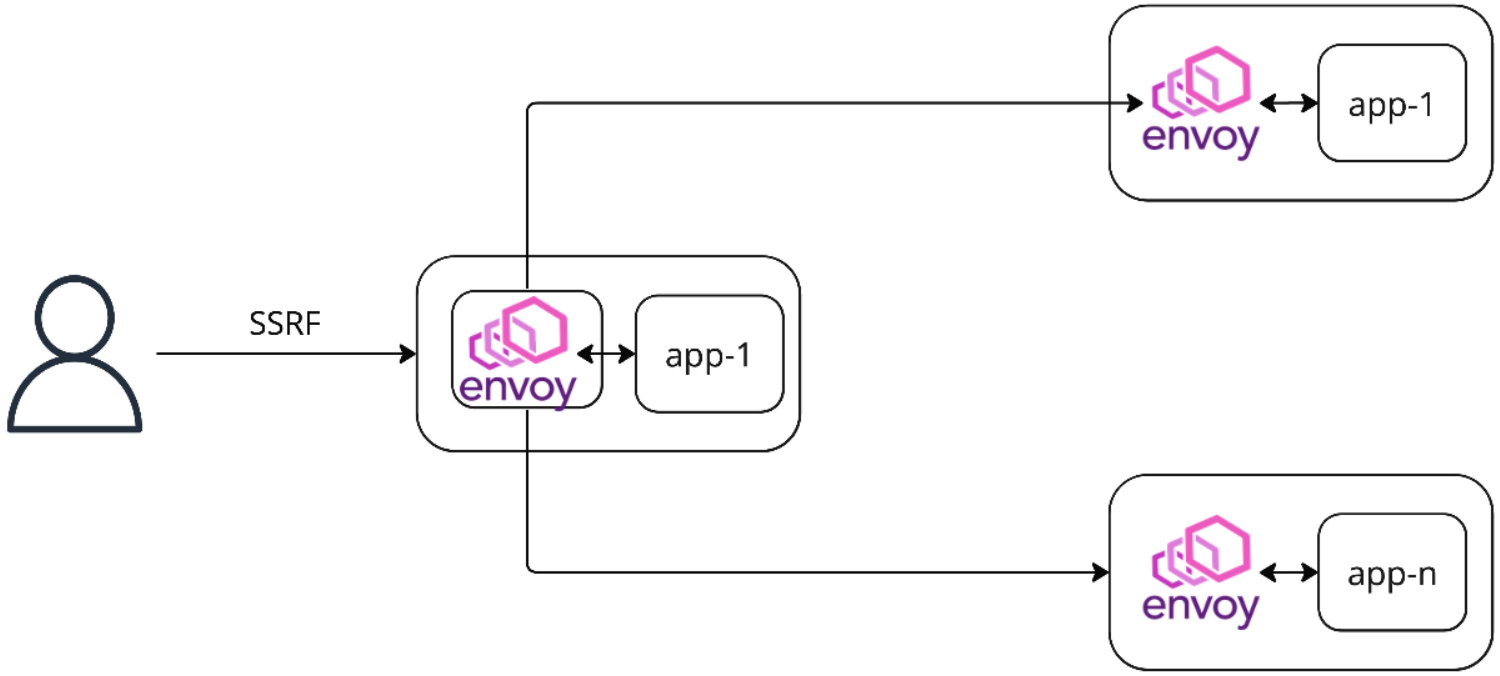
Выводы

- Придерживаемся безопасных паттернов
- Гранулярность наше всё

Про request splitting



Про SSRF




```
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: httpbin
  namespace: foo
spec:
 selector:
    matchLabels:
      app: app-2-n
spec:
  action: ALLOW
  rules:
  - from:
    - source:
        principals: ["cluster.local/ns/default/sa/app1"]
```

Выводы

- Придерживаемся безопасных паттернов
- Гранулярность наше всё
- Не сервисным identity единым

04

Выводы

Выводы

- Придерживаемся безопасных паттернов
- Гранулярность наше всё
- Не сервисным identity единым
- Безопасные дефолты со старта экономят время после


5 июня 2024 Москва, LOFT HALL#2
Конференция по БЕзопасности
КОНтейнеров и контейнерных сред
БЕКОН
UNTRY

Tg: aboycev