

5 июня 2024 📍 Москва, LOFT HALL#2

БЕКОН²⁴

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Все ли Service Mesh одинаково полезны для ИБ

Максим Чудновский

CPO Synapse Service Mesh, СберТех

Обо мне

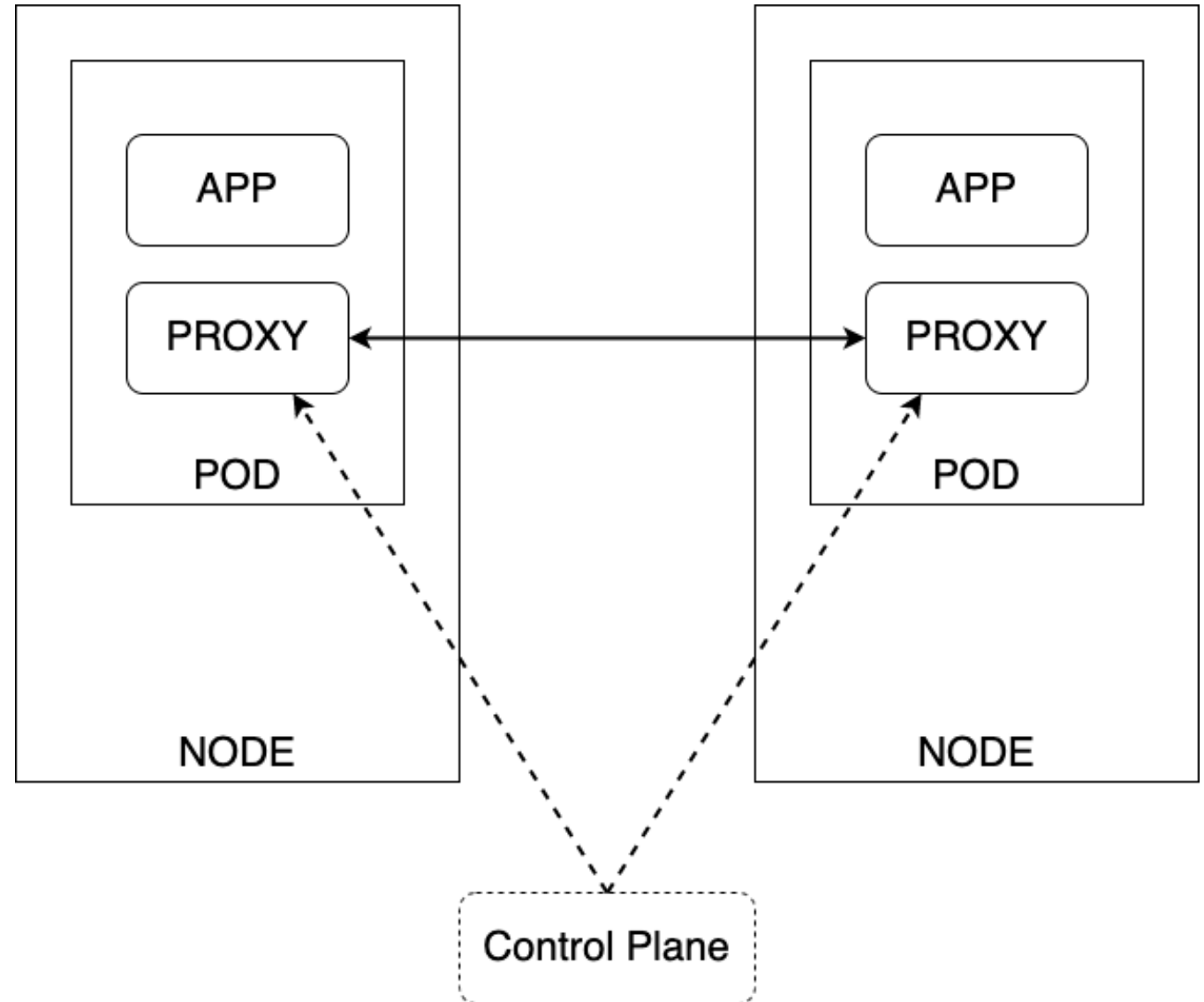
- В разработке Service Mesh с 2018 года;
- Масштаб эксплуатации Service Mesh:
 - 300+ продуктовых команд;
 - 200+ кластеров Kubernetes;
 - 20K+ подов в Service Mesh;
- Дополнительно разрабатываю много полезного вокруг Service Mesh и Kubernetes;
- Подробнее о Synapse: getsynapse.io

Архитектура Service Mesh

Архитектура Service Mesh

4

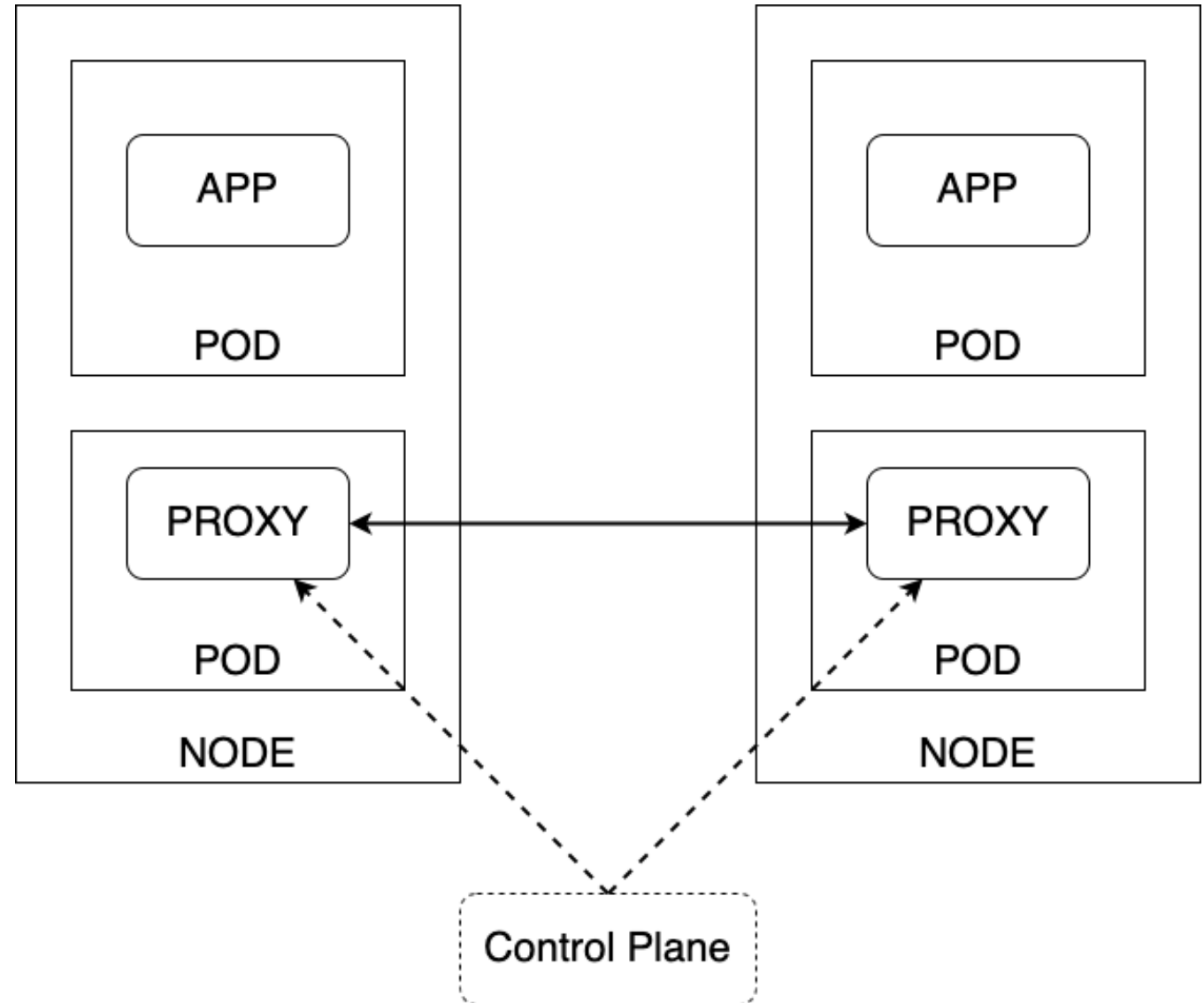
➤ Sidecar Based



Архитектура Service Mesh

5

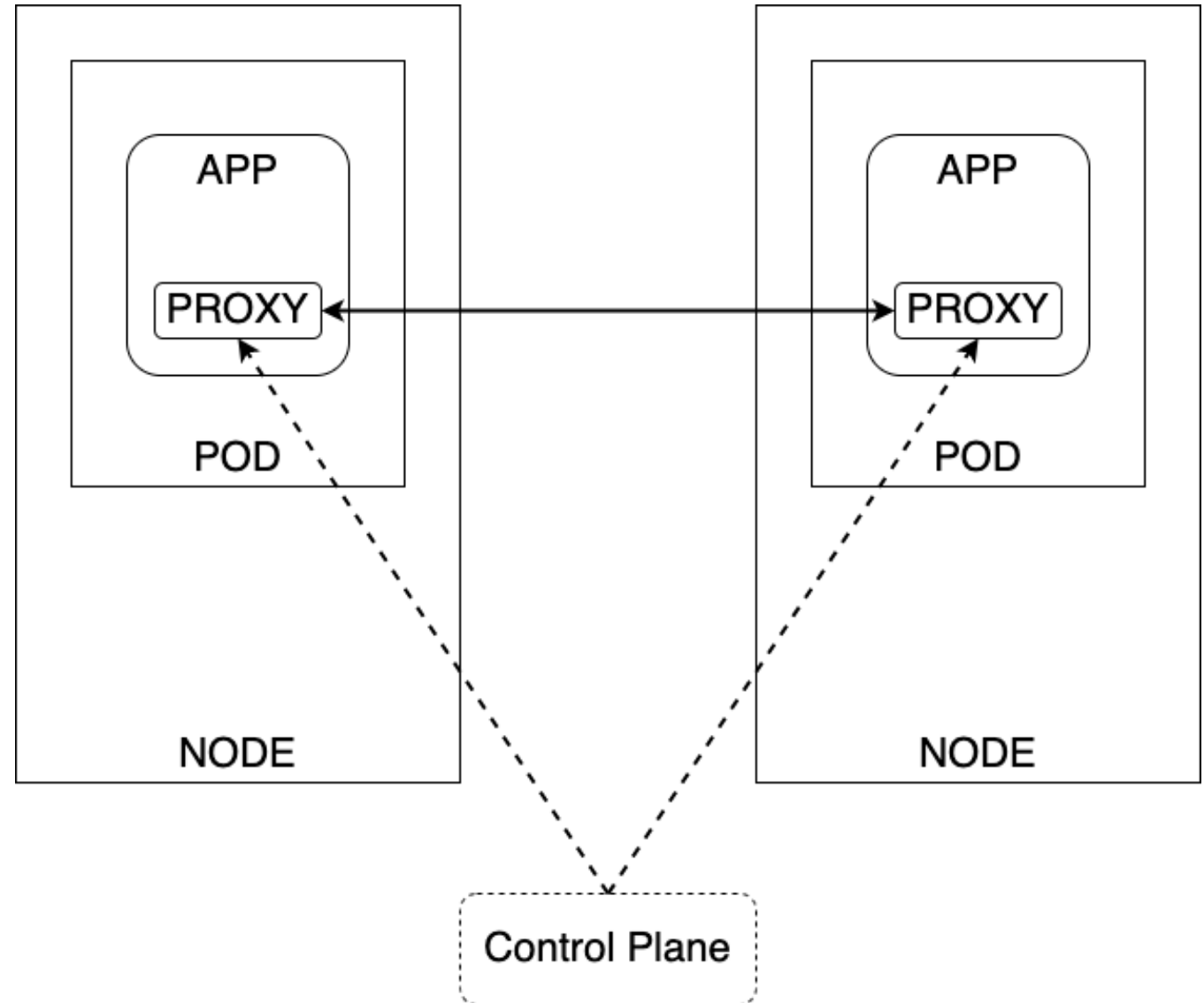
- Sidecar **Based**
- Sidecar **Less**



Архитектура Service Mesh

6

- Sidecar **Based**
- Sidecar **Less**
- Proxy **Less**



Summary #1

Sidecar Based	Sidecar Less	Proxy Less

Summary #1

Sidecar Based	Sidecar Less	Proxy Less
ISTIO		

Summary #1

Sidecar Based	Sidecar Less	Proxy Less
ISTIO	CILIUUM, ISTIO	

Summary #1

Sidecar Based	Sidecar Less	Proxy Less
ISTIO	CILUM, ISTIO	ISTIO

Summary #1

Sidecar Based	Sidecar Less	Proxy Less
ISTIO	CILIUM, ISTIO	ISTIO

Подробнее про архитектуру Service Mesh:

<https://highload.ru/moscow/2022/abstracts/9551>

Подробнее про Istio Ambient:

<https://devopsconf.io/moscow/2024/abstracts/11549>

Безопасность в Service Mesh

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 😊.

Cilium Security APIs

➤ CiliumNetworkPolicy;

```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "l7-rule"
spec:
  endpointSelector:
    matchLabels:
      app: myService
  ingress:
    - toPorts:
      - ports:
        - port: '80'
          protocol: TCP
      rules:
        http:
          - method: GET
            path: "/path1$"
```

Cilium Security APIs

- CiliumNetworkPolicy;
➤ CiliumEnvoyConfig 😊.

Что нас интересует?

- Traffic Processing;

Что нас интересует?

- Traffic Processing;
- PKI;

Что нас интересует?

- Traffic Processing;
- PKI;
- mTLS.

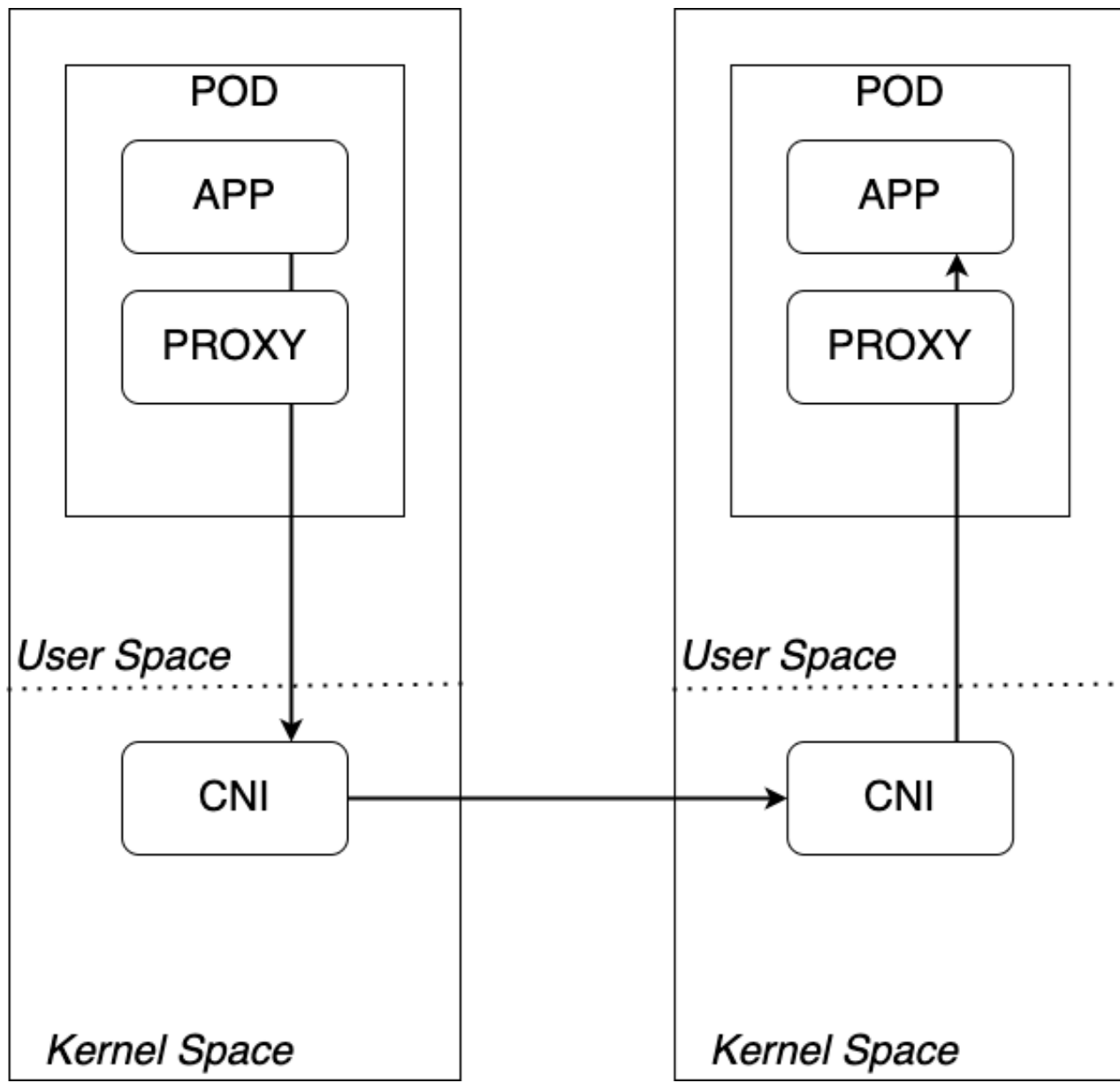
Что нас интересует?

- Traffic Processing;
- PKI;
- mTLS.

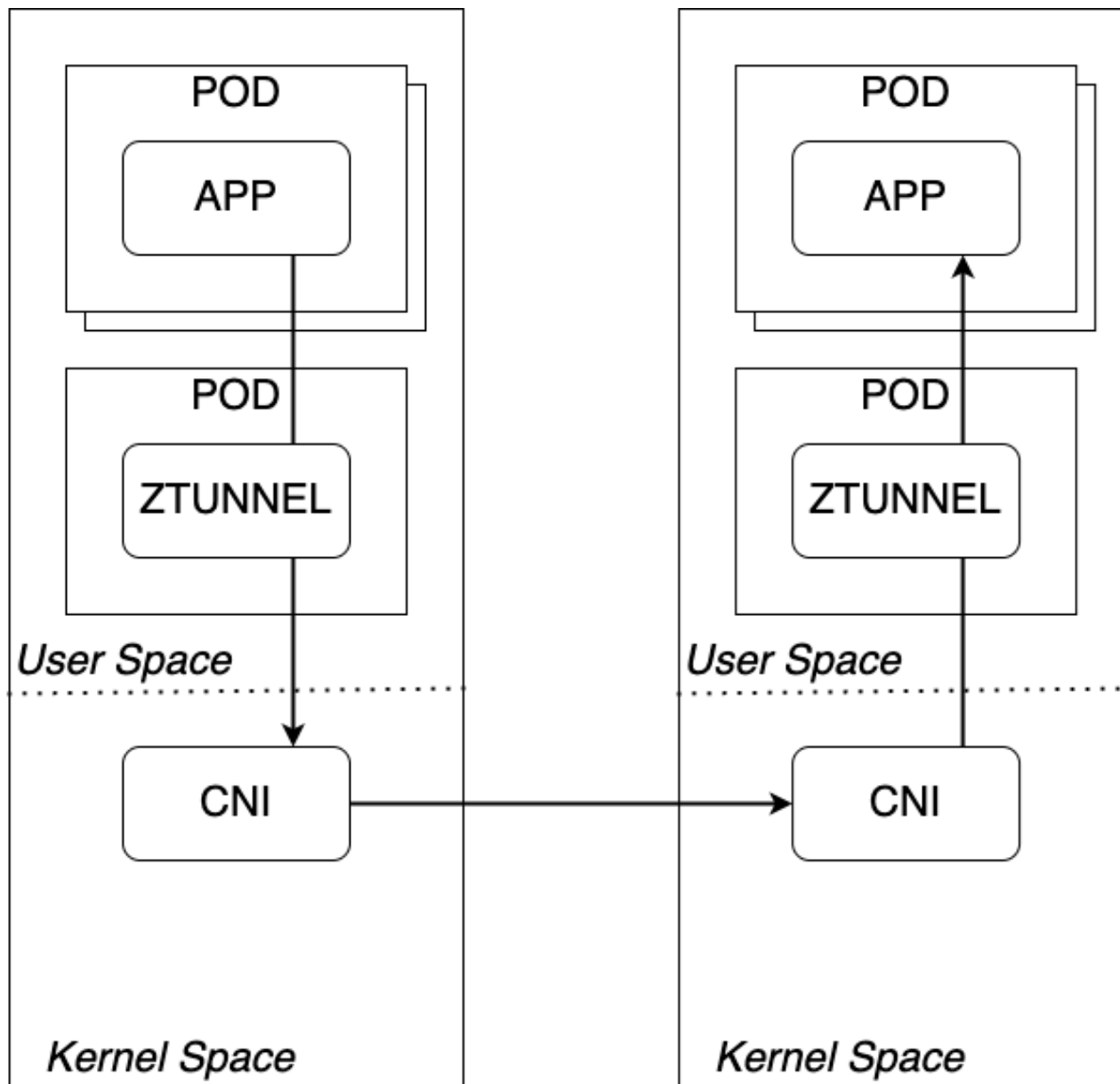
RBAC отдельно не рассматриваем, потому что у всех **Envoy Based** реализация.

Traffic Processing

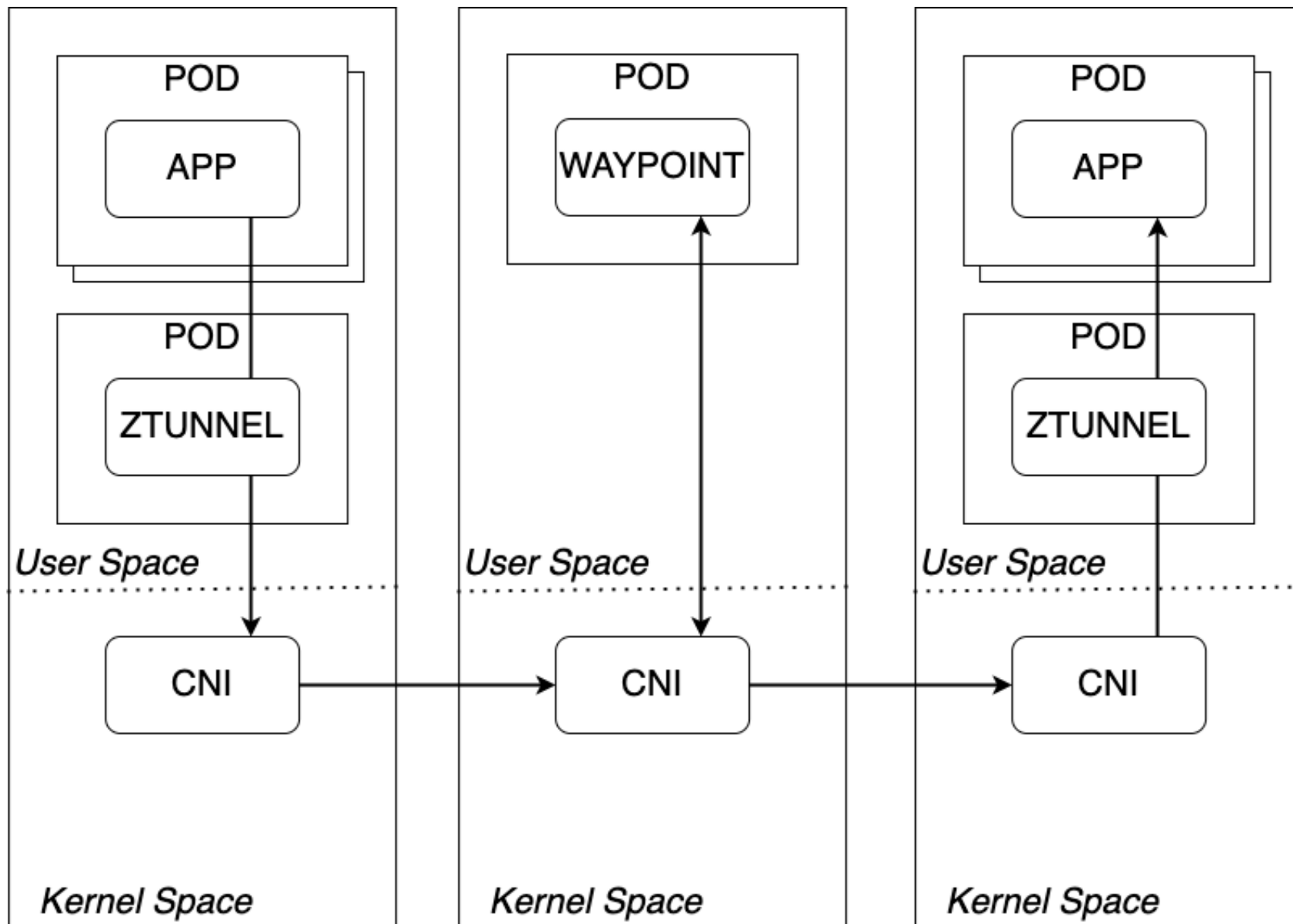
ISTIO L4/L7



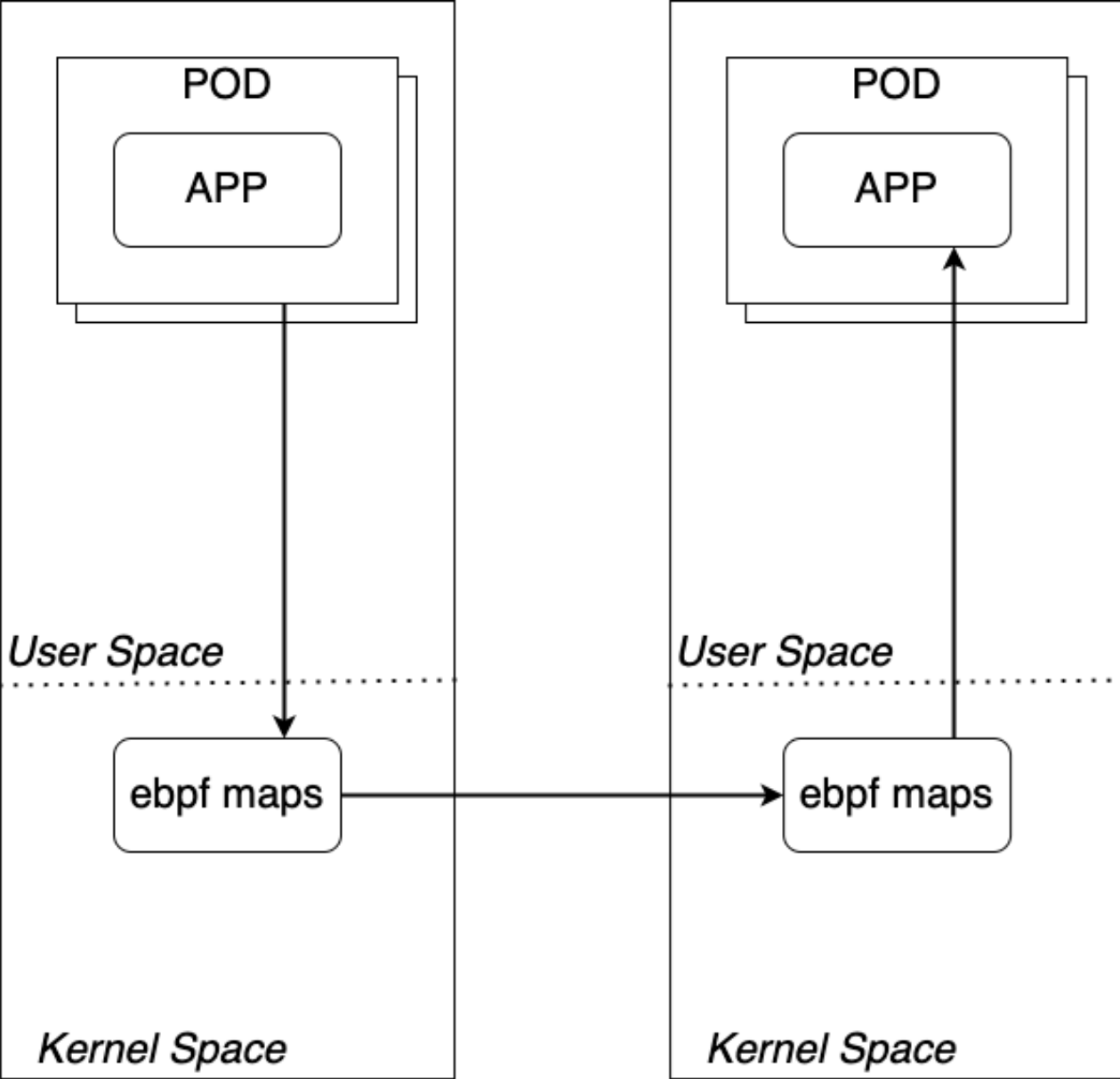
ISTIO AMBIENT L4



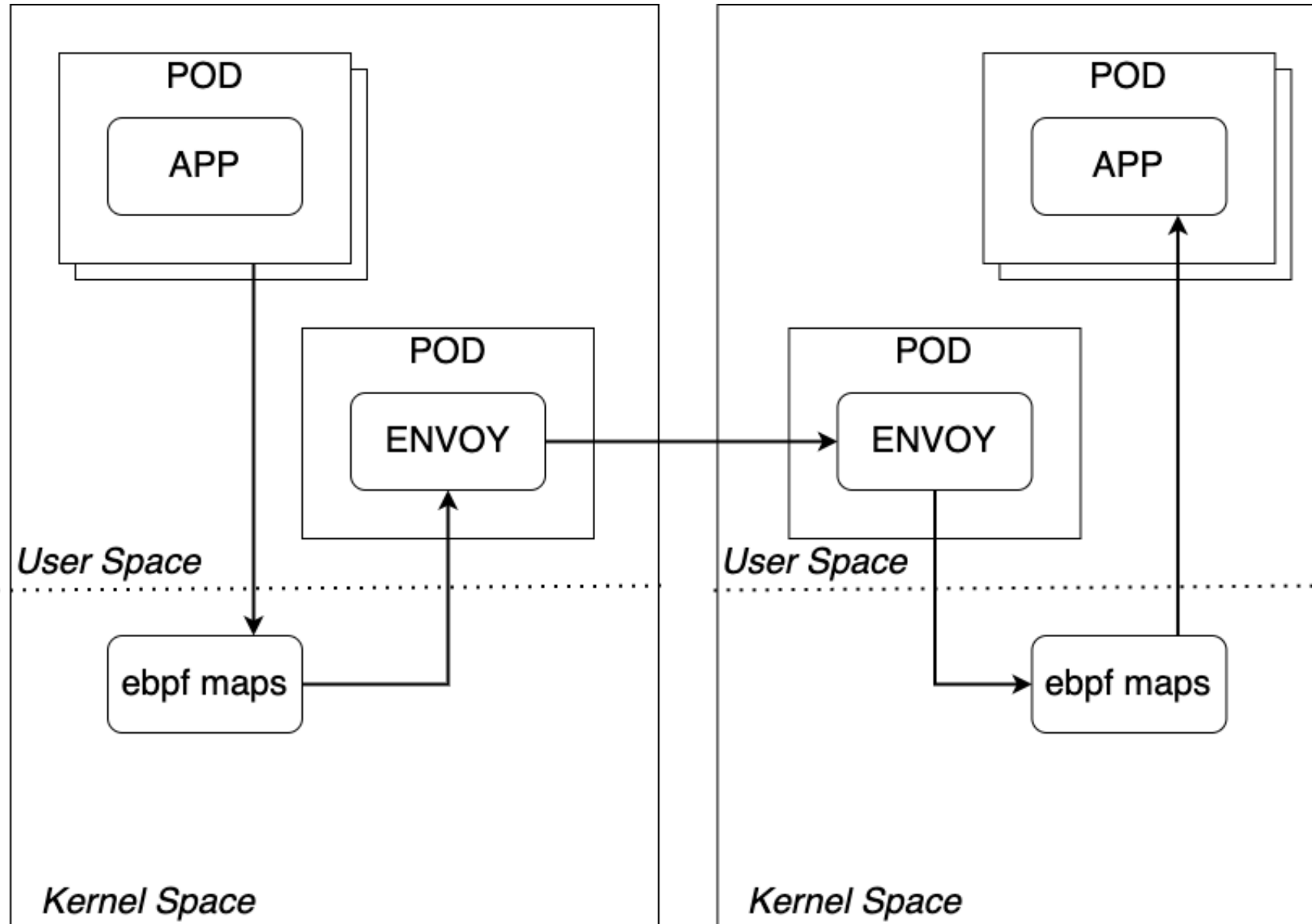
ISTIO AMBIENT L7



CILIUM L4



CILIUM L7



Summary #2

➤ ISTIO:

- Всегда User Space;
- Все в периметре пода.

Summary #2

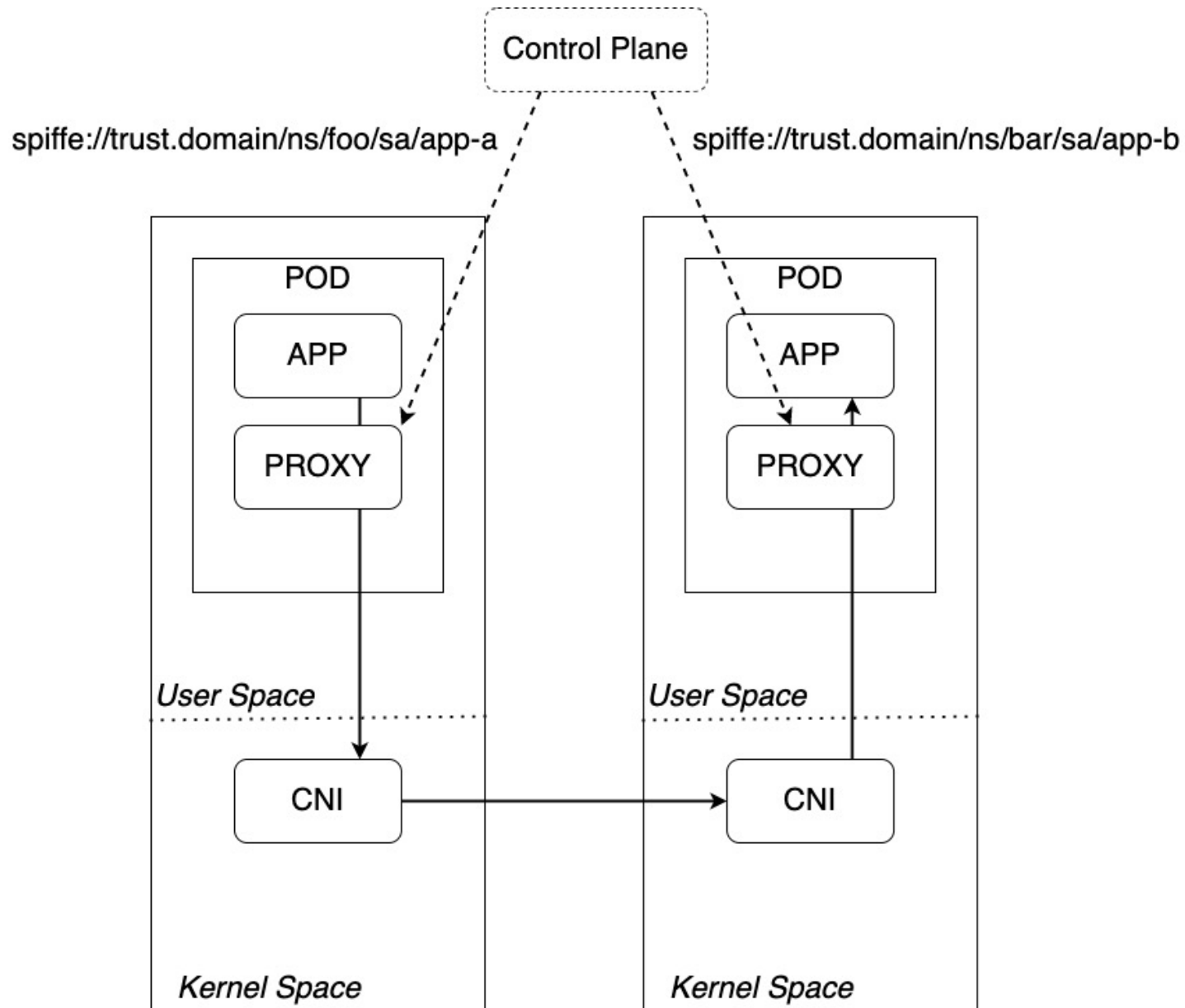
- ISTIO:
 - Всегда User Space;
 - Все в периметре пода.
- ISTIO AMBIENT:
 - Всегда User Space;
 - L4 в периметре хоста, L7 в периметре кластера (ns/workload).

Summary #2

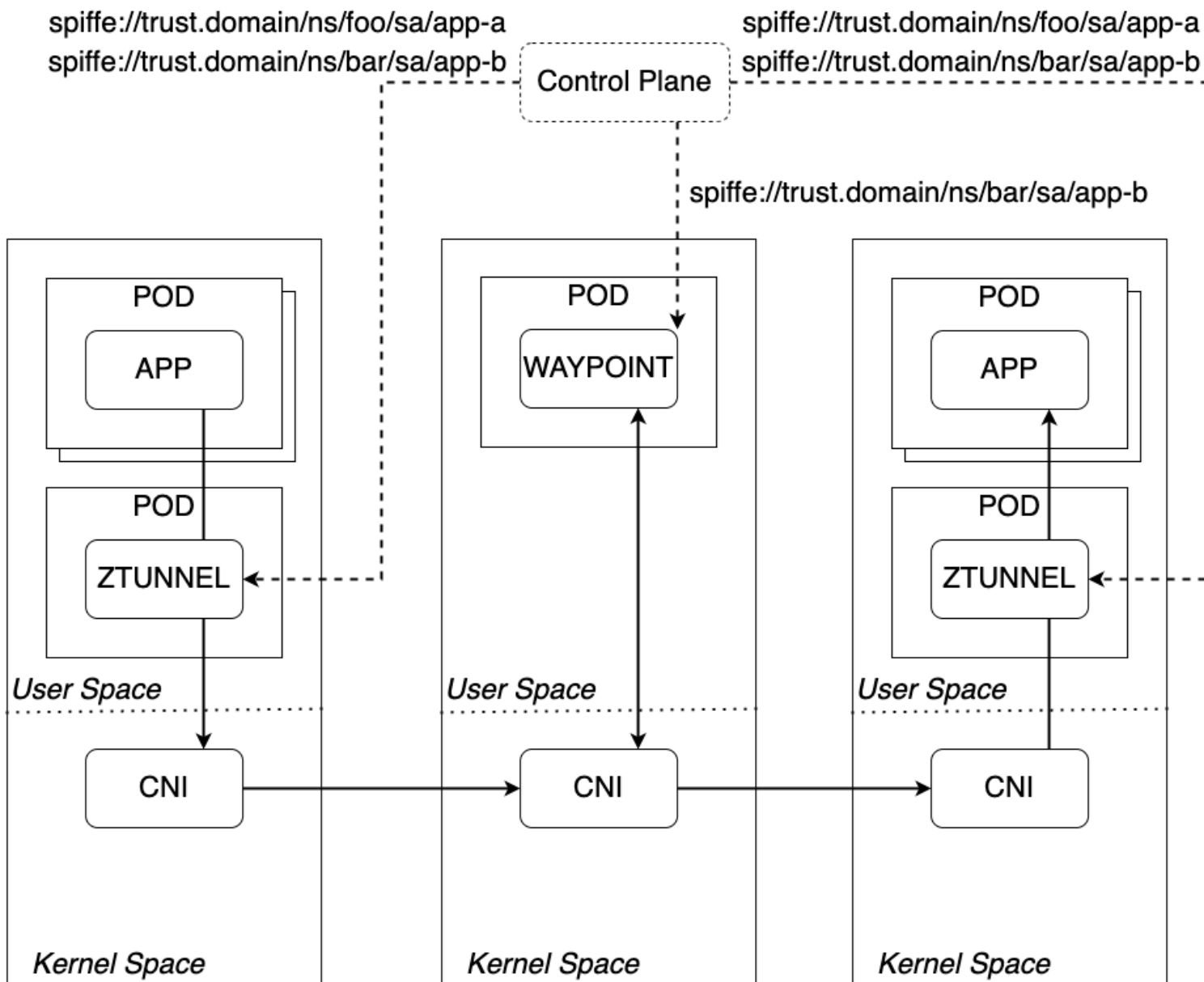
- ISTIO:
 - Всегда User Space;
 - Все в периметре пода.
- ISTIO AMBIENT:
 - Всегда User Space;
 - L4 в периметре хоста, L7 в периметре кластера (ns/workload).
- CILIUUM:
 - L4 Kernel Space, L7 User Space;
 - Всегда в периметре хоста.

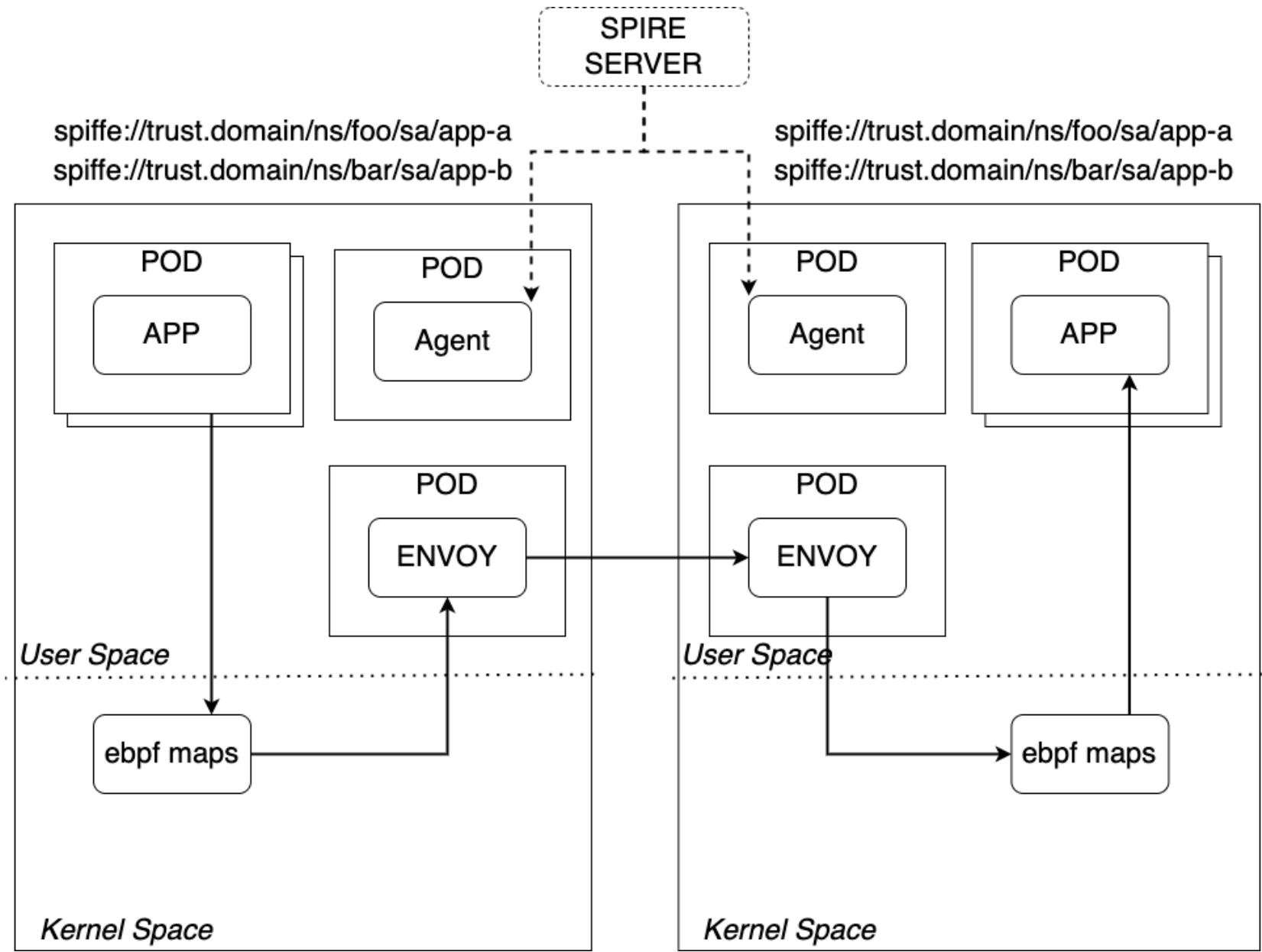
БЕКОН

PKI



ISTIO AMBIENT





Summary #3

➤ ISTIO:

- Выпуск секретов через Control Plane;
- Всегда в периметре пода.

Summary #3

- ISTIO:

- Выпуск секретов через Control Plane;
- Всегда в периметре пода.

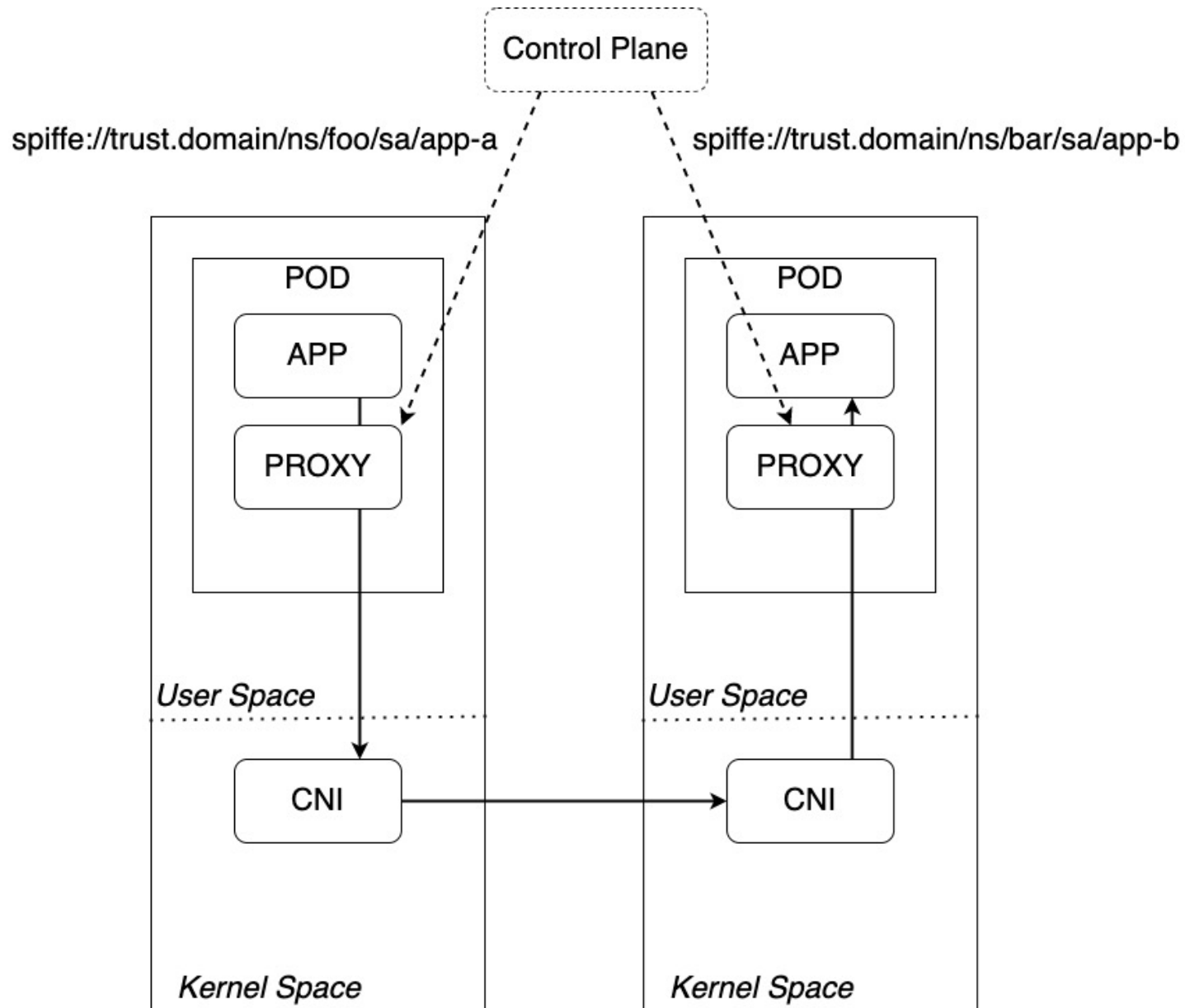
- ISTIO AMBIENT:

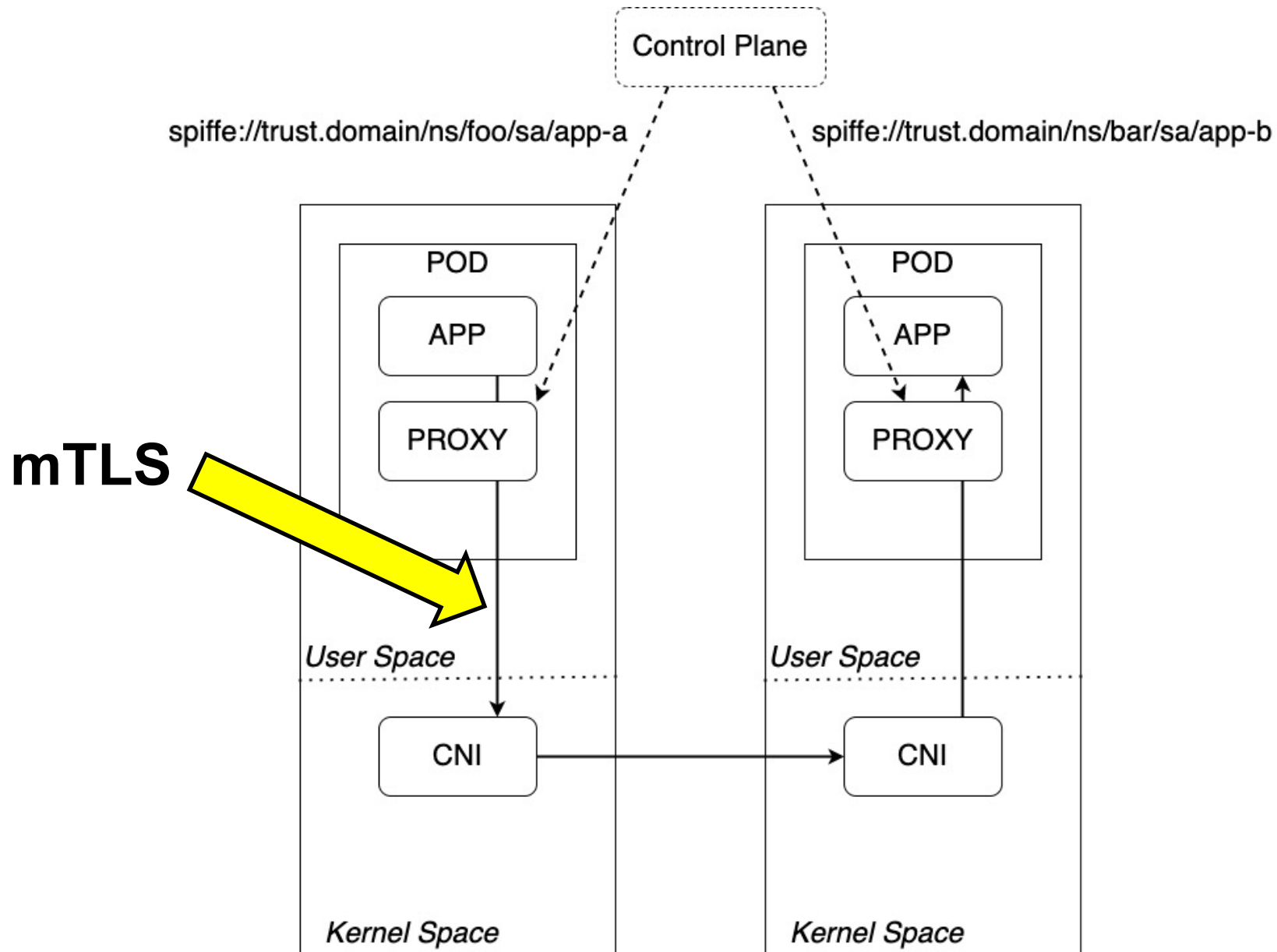
- Выпуск через Control Plane;
- Всегда в периметре хоста, если есть L7, то **дополнительно** в пределах workload или namespace

Summary #3

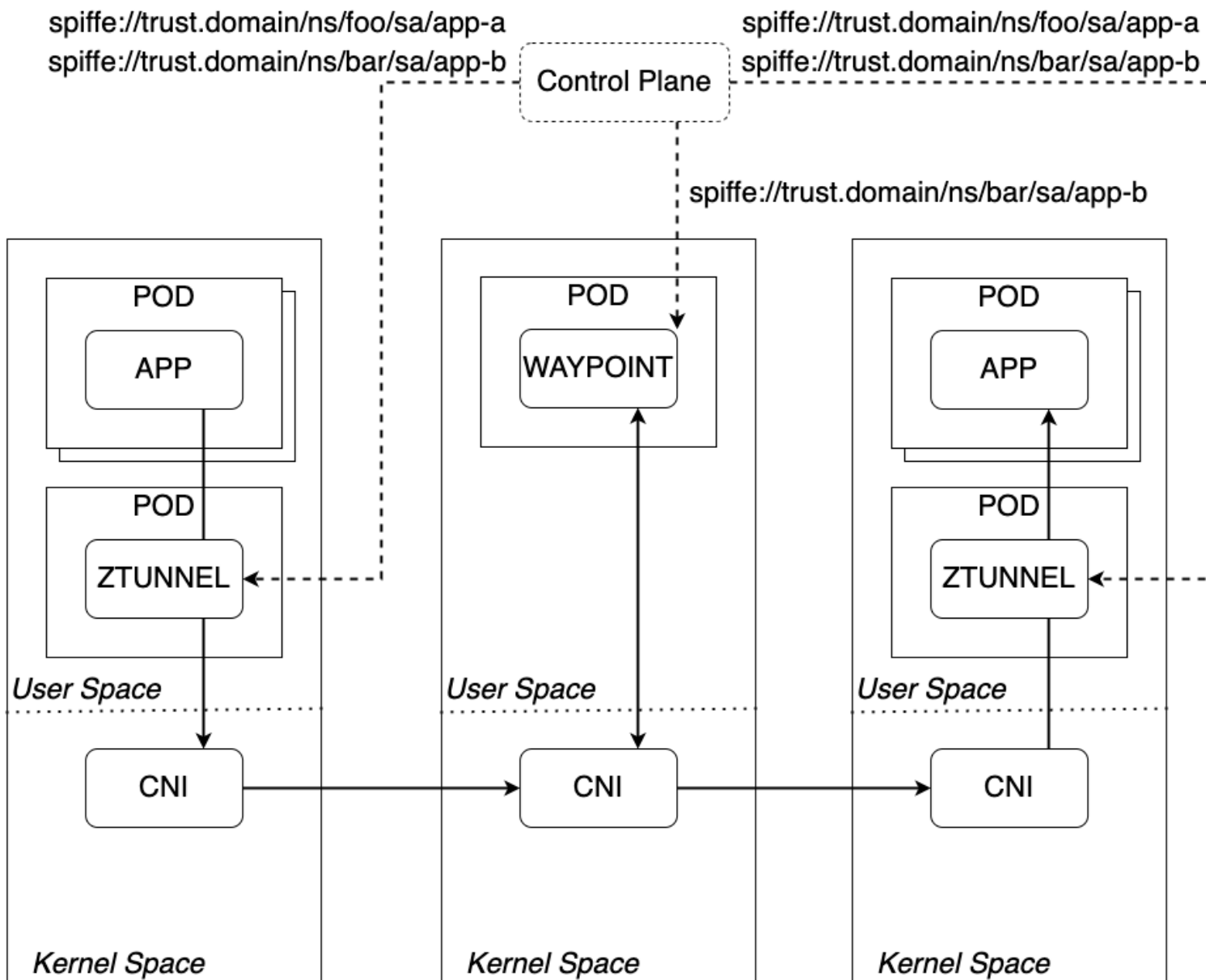
- ISTIO:
 - Выпуск секретов через Control Plane;
 - Всегда в периметре пода.
- ISTIO AMBIENT:
 - Выпуск через Control Plane;
 - Всегда в периметре хоста, если есть L7, то **дополнительно** в пределах workload или namespace
- CILIUМ:
 - Выпуск через дополнительный Spire Server;
 - Всегда в периметре хоста.

mTLS

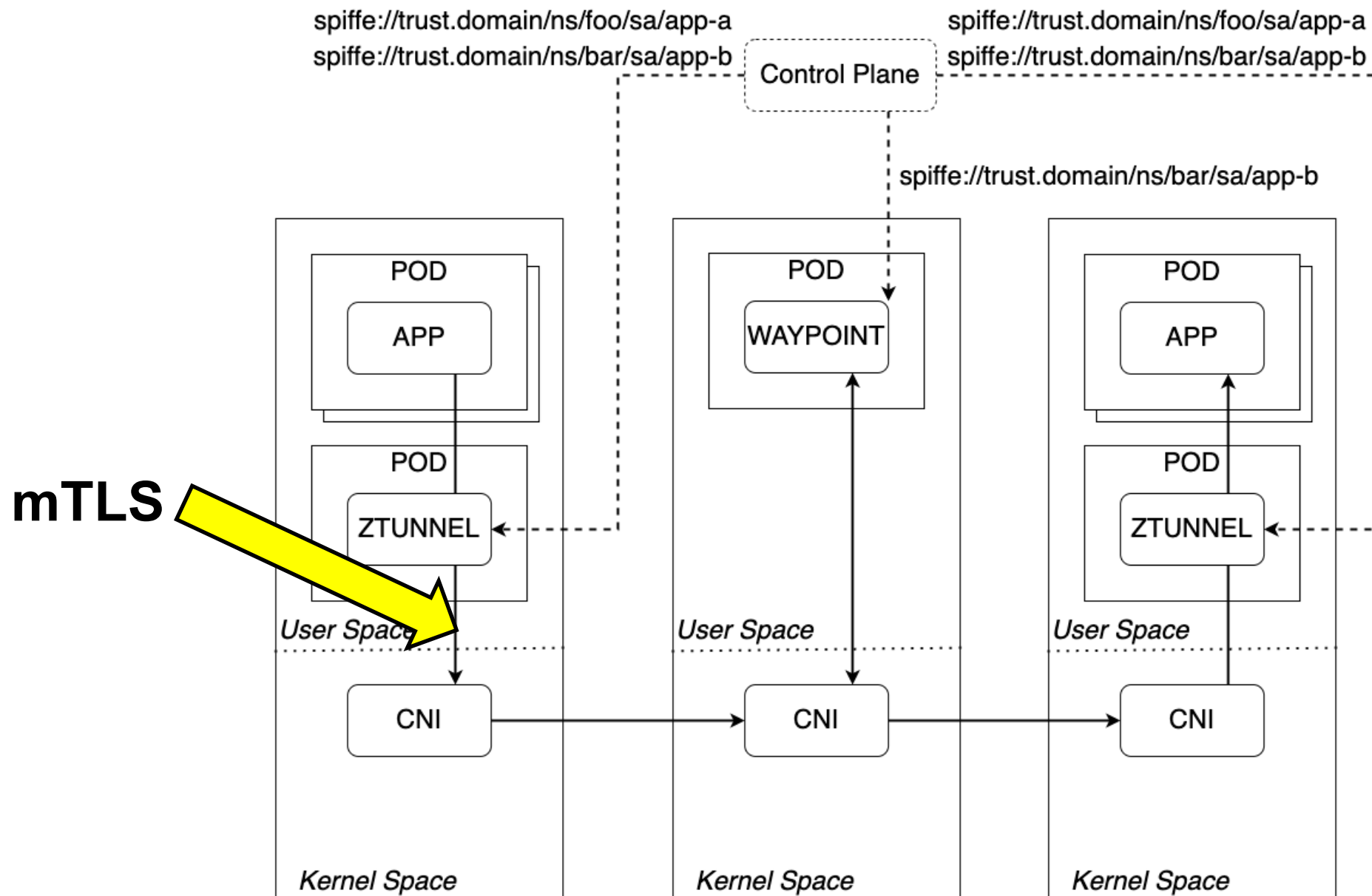




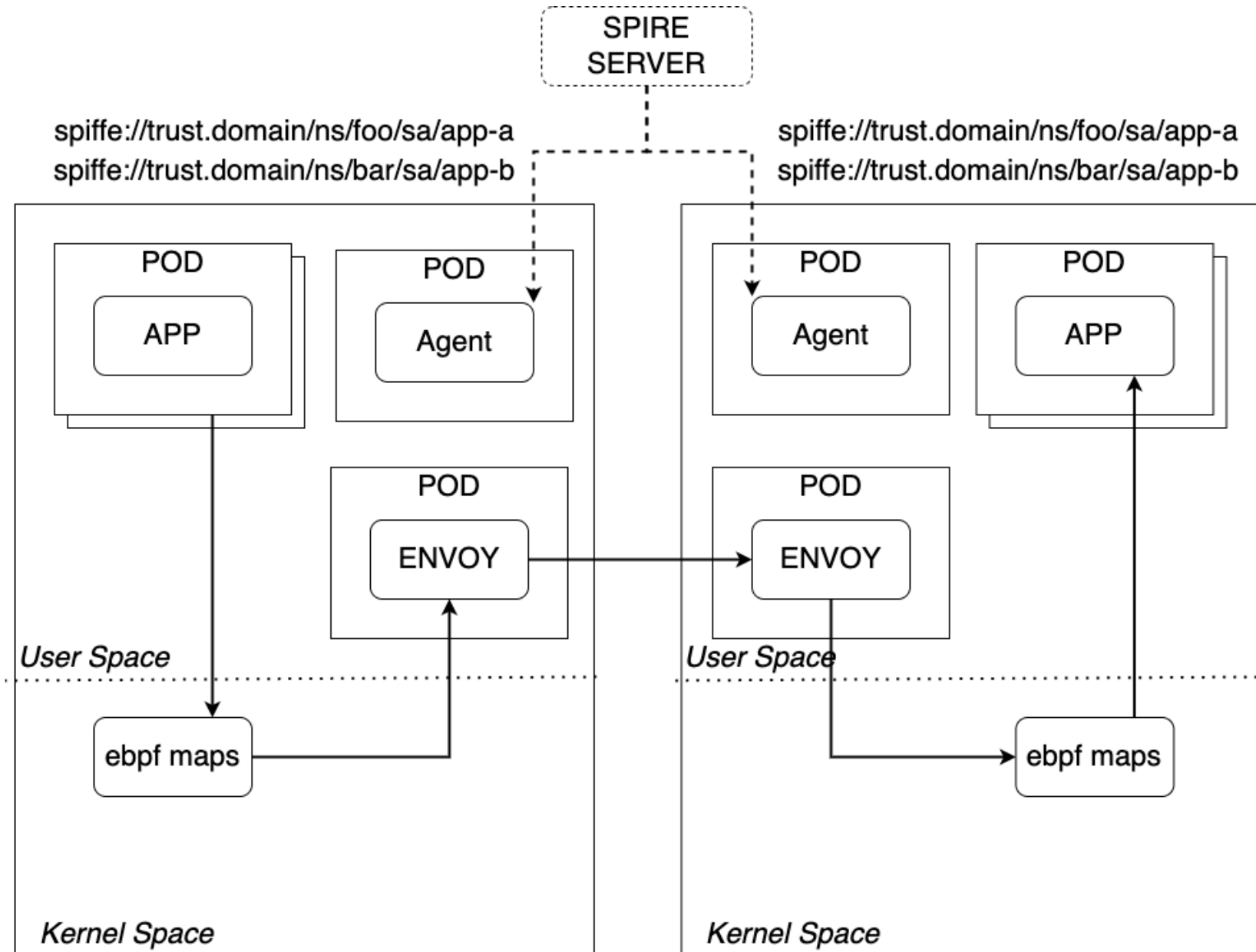
ISTIO AMBIENT



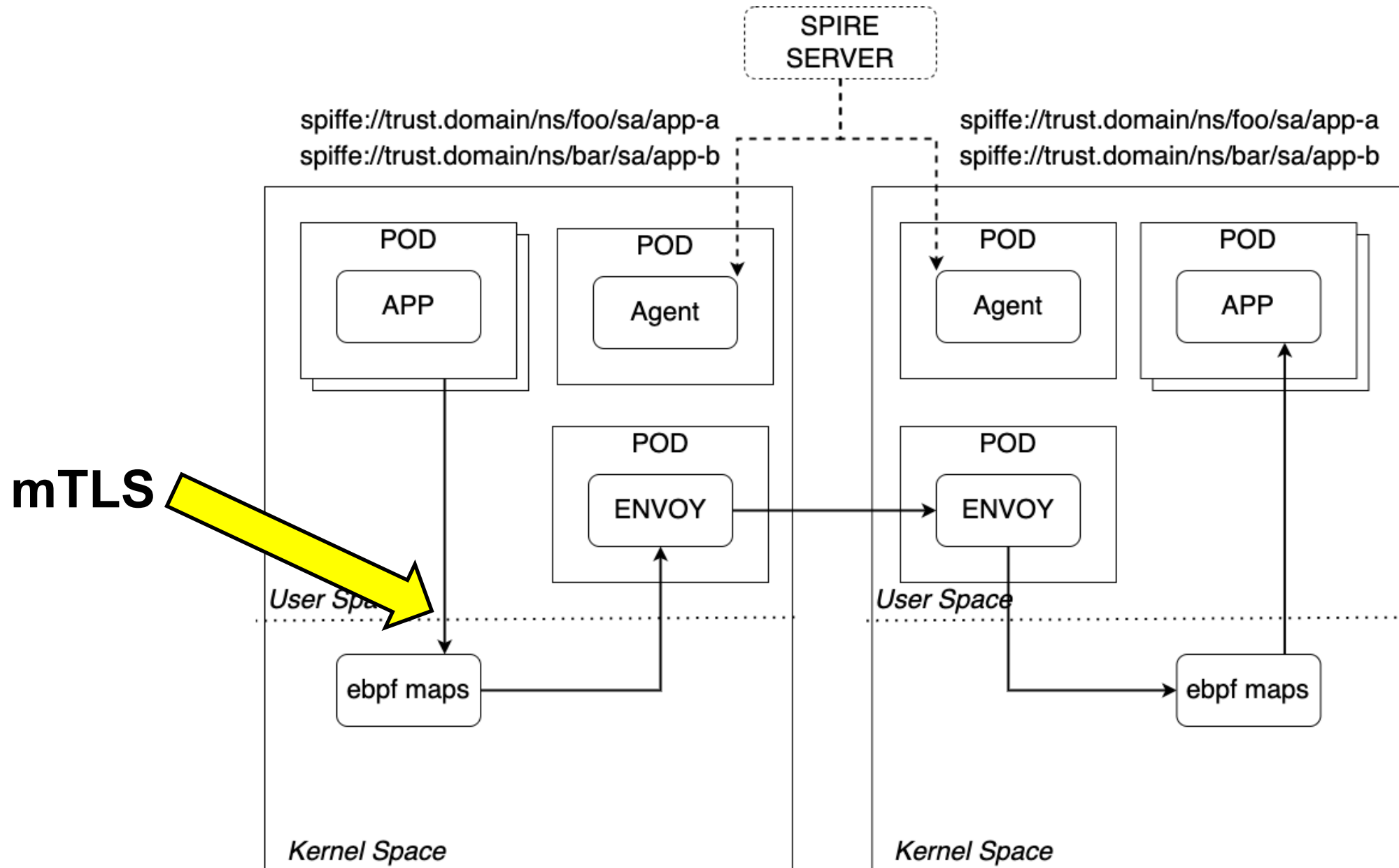
ISTIO AMBIENT



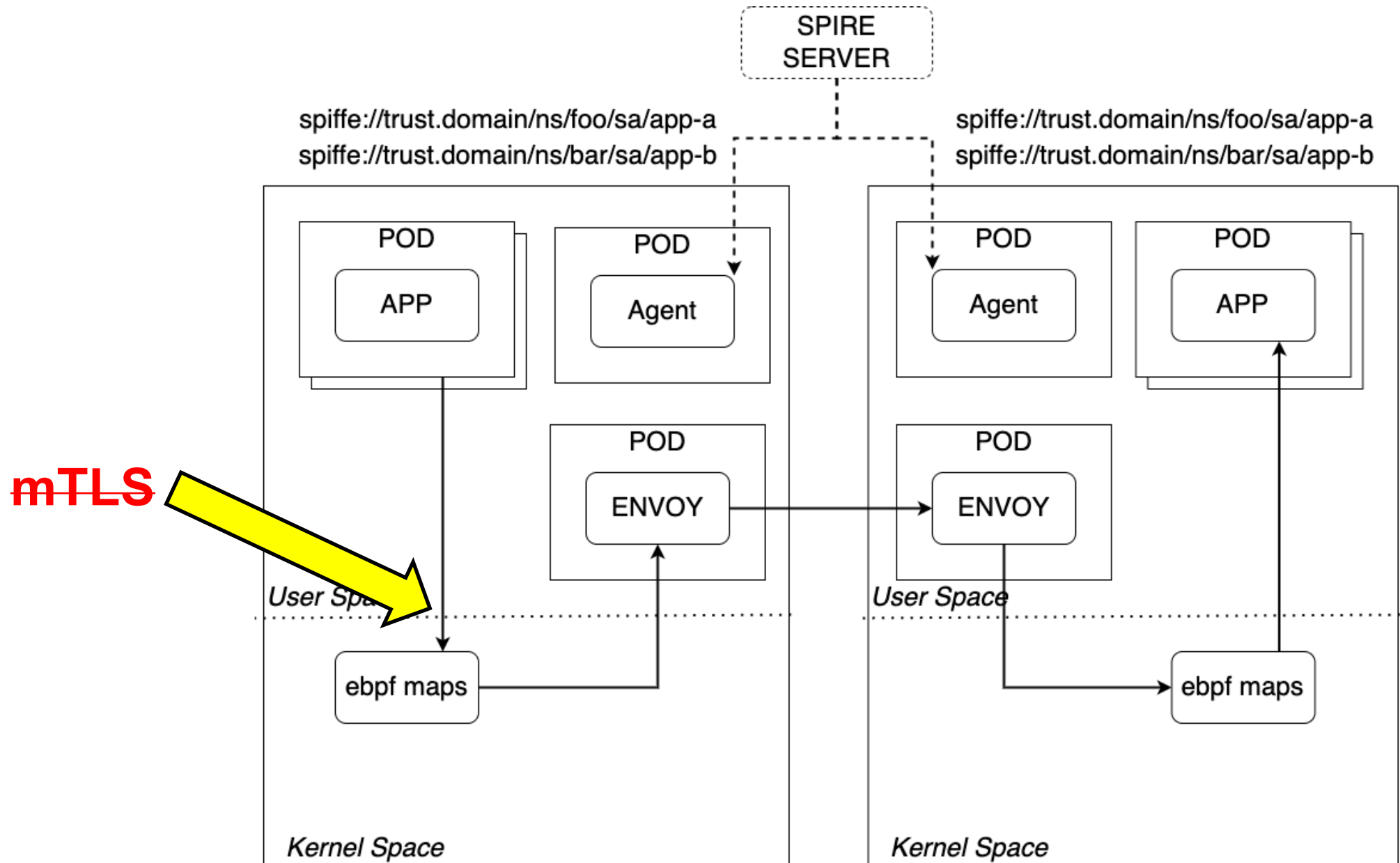
CILIUM



CILIUM

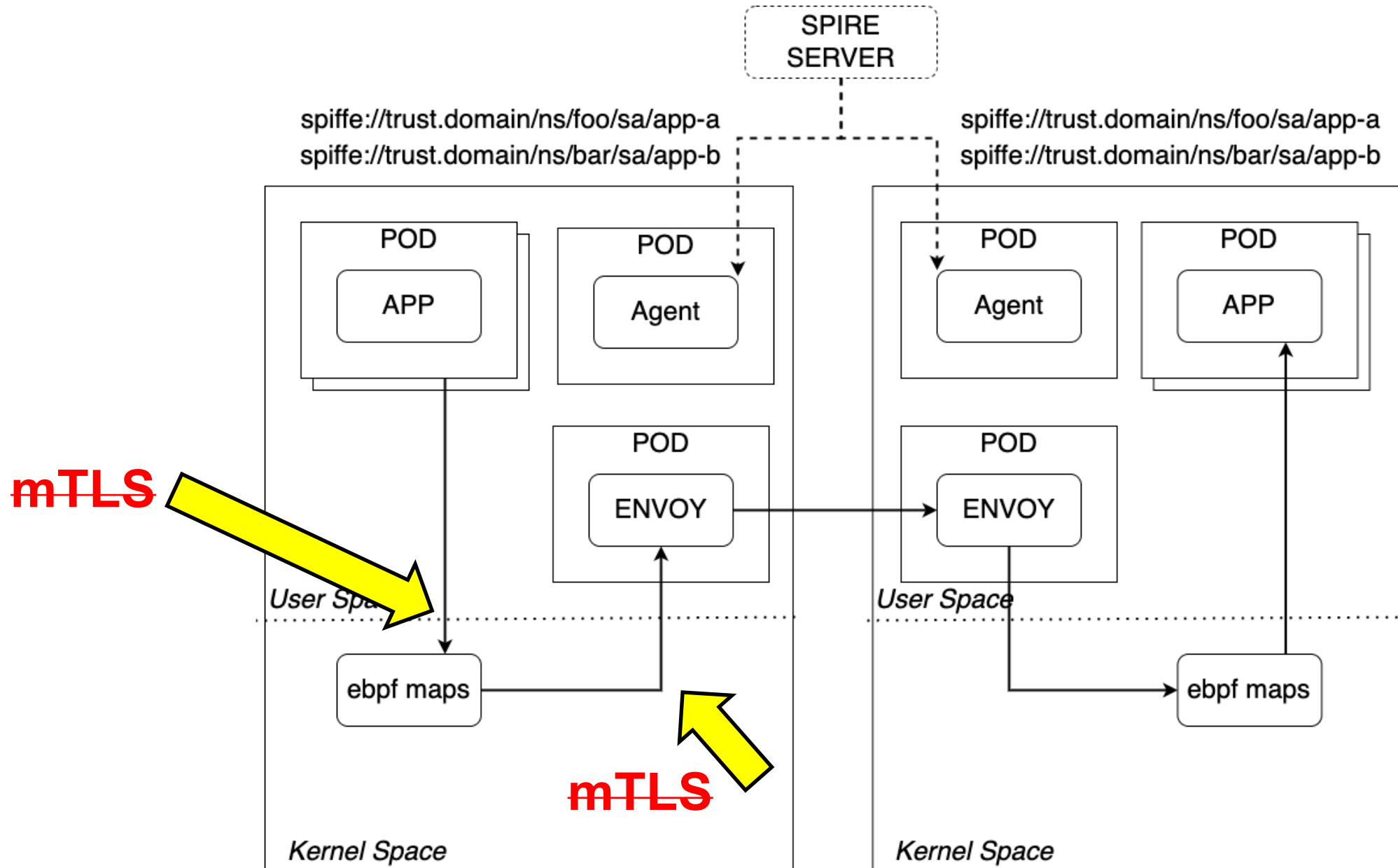


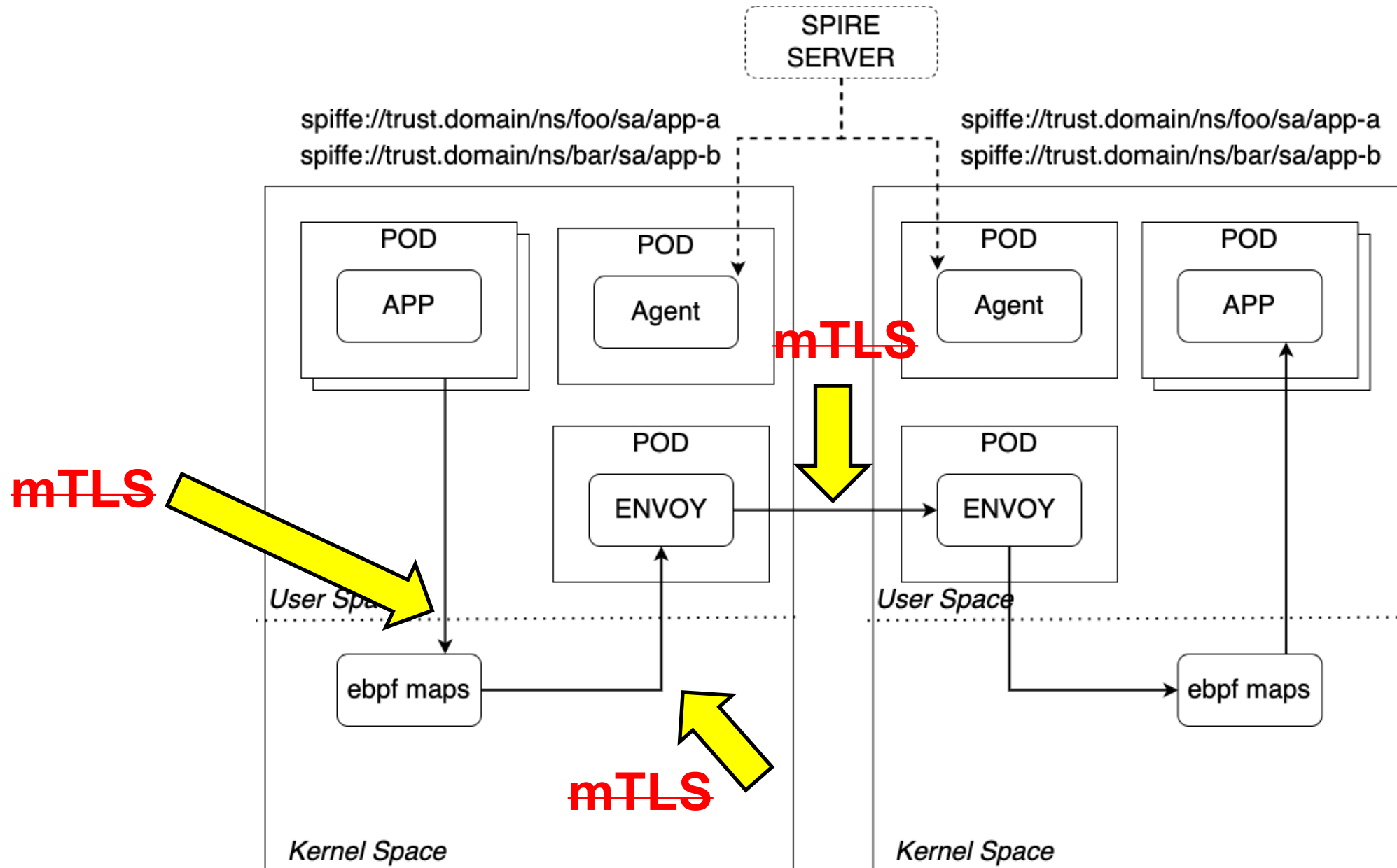
CILIUM



CILIUM

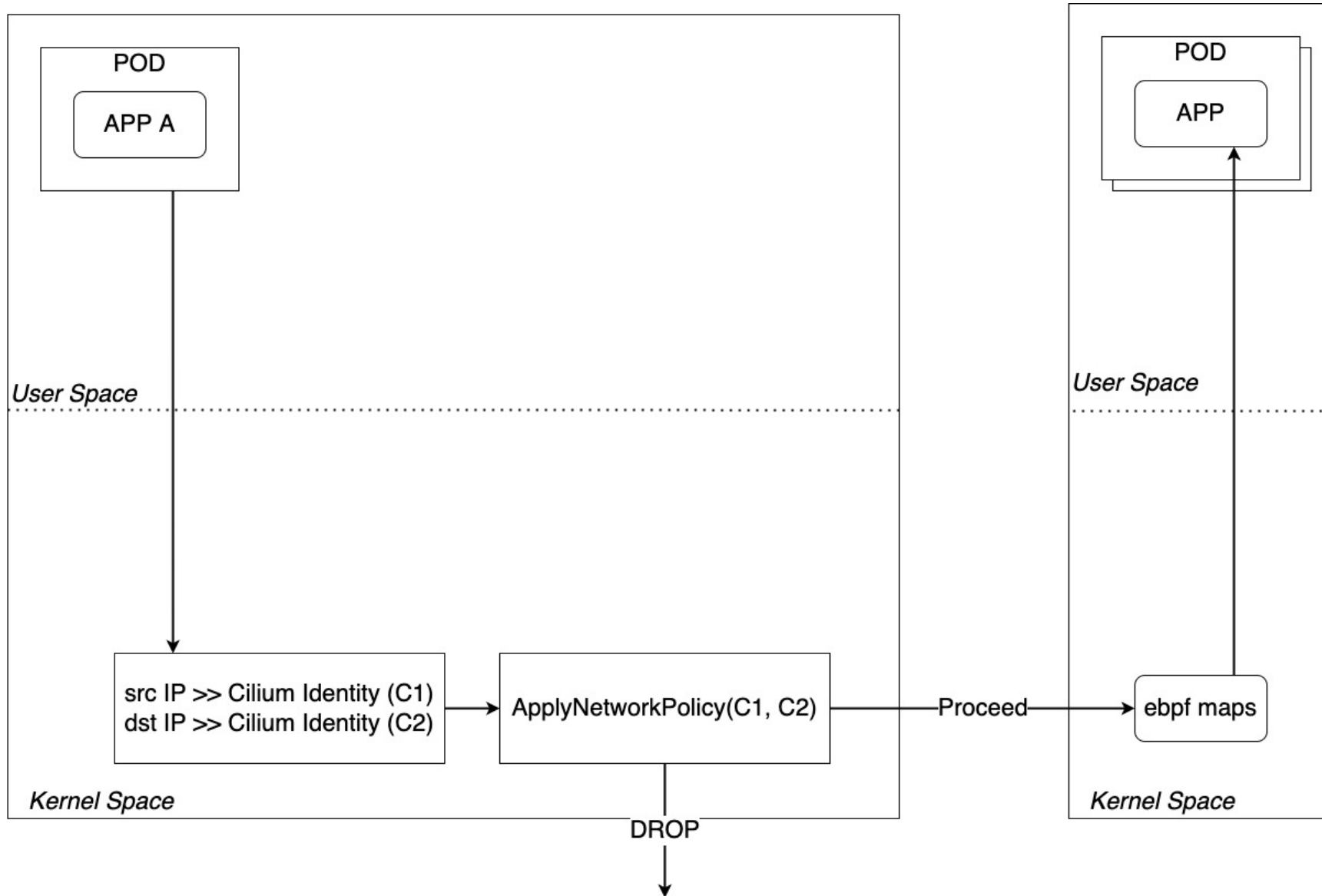
48





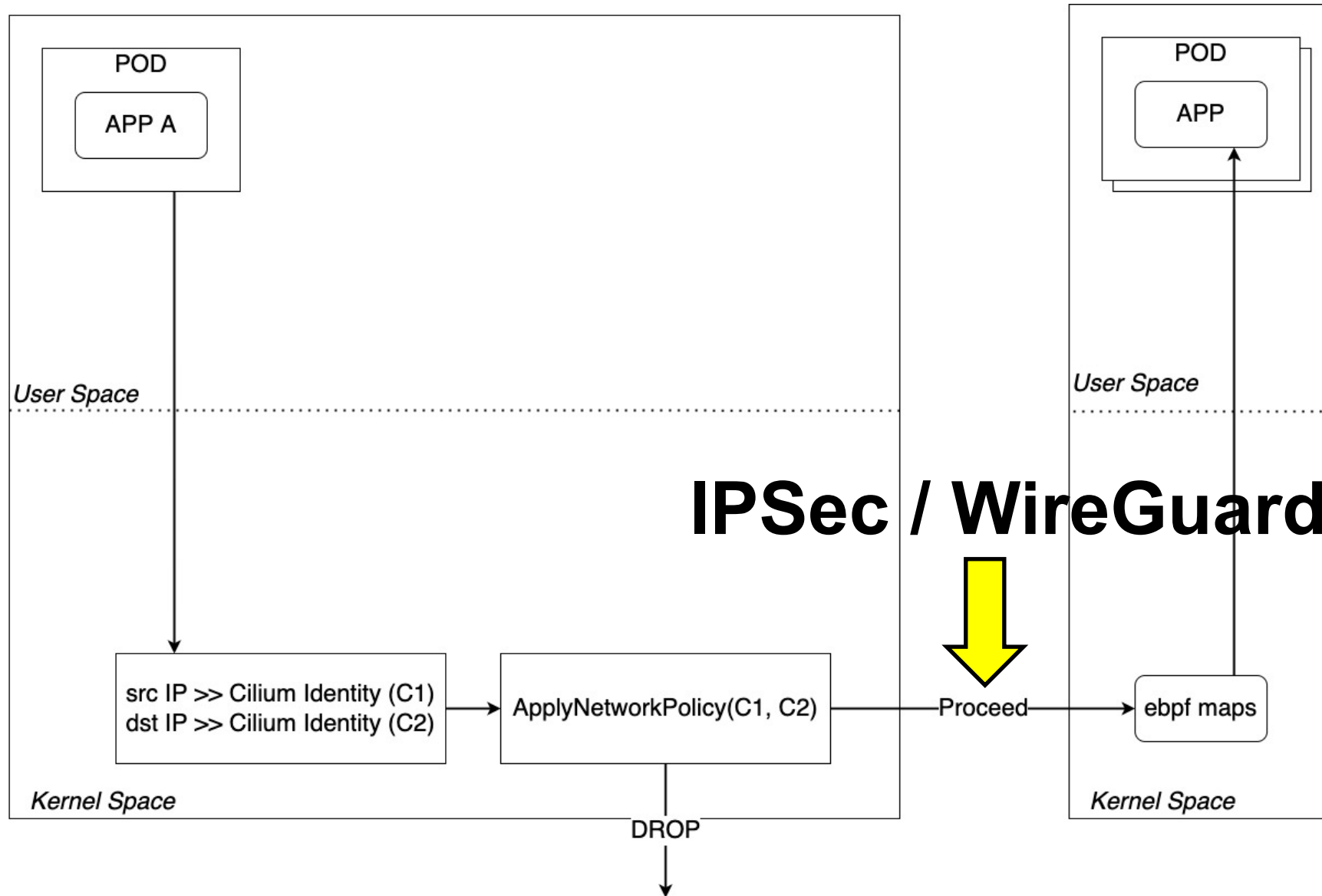
CILIUM NETWORK POLICY

50



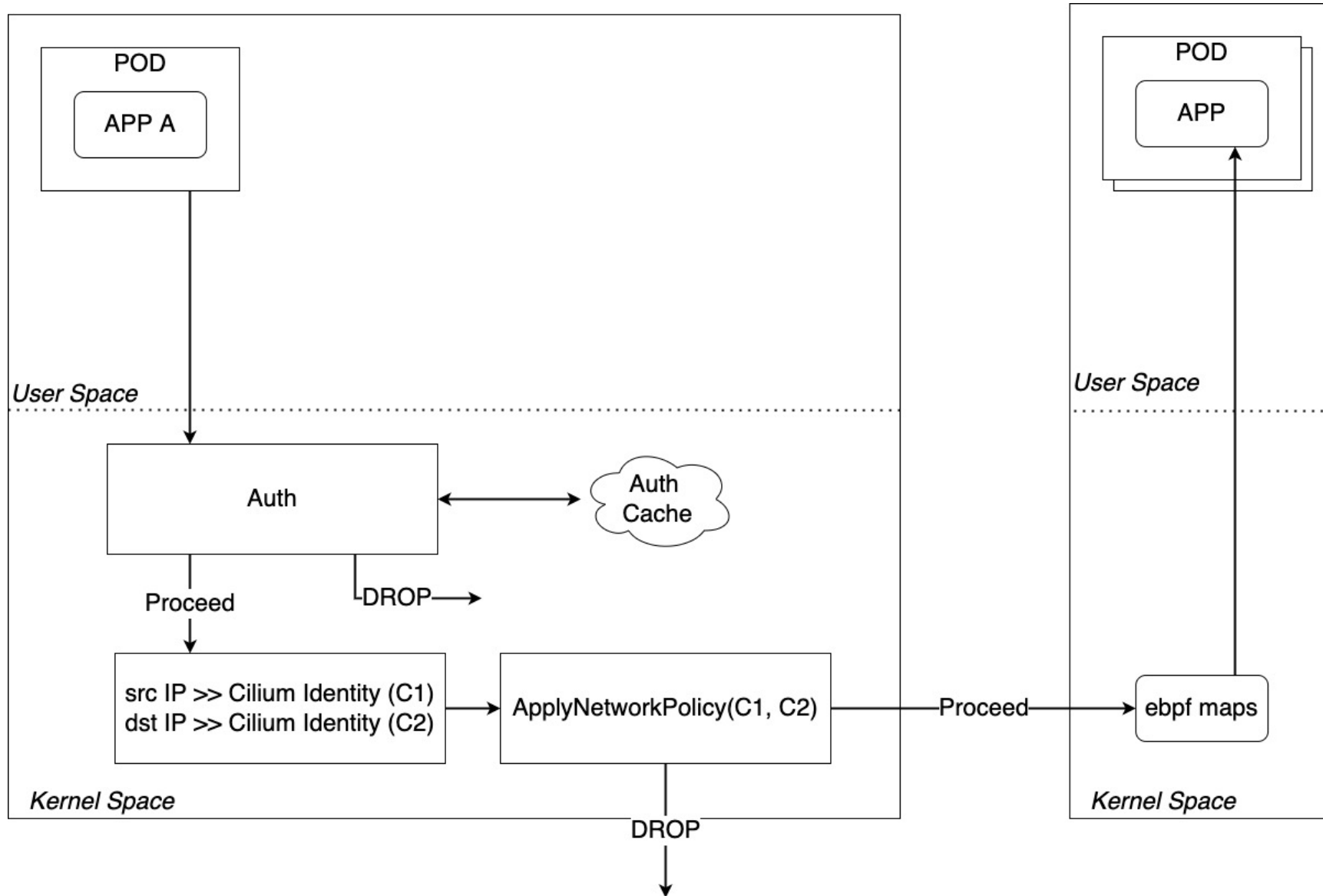
CILIUM NETWORK POLICY

51



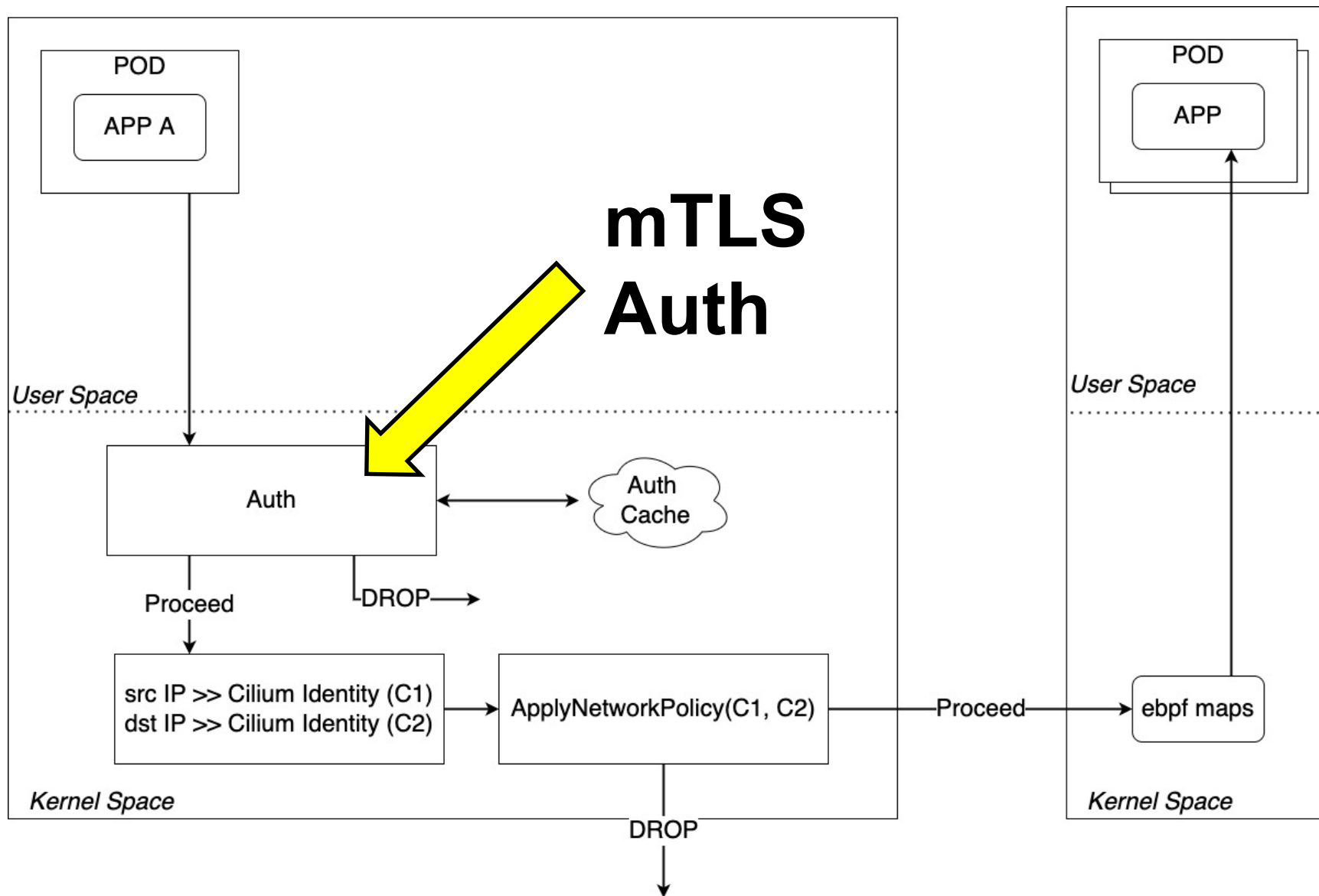
CILIUM AUTH

52



CILIUM AUTH

53



Summary #4

➤ISTIO:

- Аутентификация Workload To Workload;
- Шифрование Workload To Workload;
- Identity – POD SA.

Summary #4

- ISTIO:
 - Аутентификация Workload To Workload;
 - Шифрование Workload To Workload;
 - Identity – POD SA.
- ISTIO AMBIENT:
 - Аутентификация Workload To Workload;
 - Шифрование Workload To Workload;
 - Identity – POD SA.

Summary #4

- ISTIO:
 - Аутентификация Workload To Workload;
 - Шифрование Workload To Workload;
 - Identity – POD SA.
- ISTIO AMBIENT:
 - Аутентификация Workload To Workload;
 - Шифрование Workload To Workload;
 - Identity – POD SA.
- CILIUM:
 - Аутентификация Workload To Workload;
 - Шифрование Node To Node;
 - Identity Mapping – POD IP // POD SA // CILIUM Identity.

ИТОГИ

Все в одной таблице

	ISTIO	ISTIO AMBIENT	CILIUM
Обработка трафика	User Space	User Space	L4 Kernel Space L7 User Space
Identity	POD SA	POD SA	Cilium Identity (Pod IP / Pod Labels)
Шифрование	Workload to Workload	Workload to Workload	Node to Node
Аутентификация	Workload to Workload	Workload to Workload	Workload to Workload
Авторизация	Envoy Based	Envoy Based	Envoy Based
Blast Radius	Workload	Node / Namespace	Node

Final Summary

- Разные Service Mesh похожи по объему ИБ-функциональности;
- Разные Service Mesh различаются в деталях реализации ИБ-функциональности;
- Выбор конкретной реализации Service Mesh должен учитывать требования ИБ.

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



Максим Чудновский
maksim.chudnovskii@gmail.com

tg: [@mchudnovskiy](https://t.me/mchudnovskiy)
getsynapse.io