Better External Authorization

Yangmin Zhu
Istio Maintainer, Security WG
SWE@Google

What/Why External Authorization?

Custom logic for authorization decision, customers need better extensibility in authorization:

- Your In-house authz system cannot be replaced by Istio authz
- You need 3rd-party solution, like OPA or OAuth2-proxy
- Istio authz lacks necessary semantics for your use case

Pain Points (1/2)

Before 1.9, this is usually solved by using Envoy ext_authz filter with Istio EnvoyFilter API, it works but comes with some big pain points:

1. Usability: EnvoyFilter is powerful but easy to make mistakes

    - Mistyped url in the filter config: discuss/7095
    - EnvoyFilter doesn't merge bool value properly: issues/18169, issue/24548
    - EnvoyFilter is a breaking-class low-level API, improper use could crash your istiod
    - etc.

2. Maintainability: EnvoyFilter is hard to maintain

    - Envoy API changes could silently break your EnvoyFilter without prior notice
    - You need slightly different EnvoyFilter in each Istio version, hard to maintain at scale

Pain Points (2/2)

3. Troubleshoot: ext-authz config has too much low-level details

   - If using gRPC, You need to figure out the cluster name (e.g. "outbound|50051||ext-authz-server.foo.svc.cluster.local") to be used in the config. However, the cluster name and its format is a complete internal implementation detail, Isito could change it anytime
   - What's worse, you would need another EnvoyFilter to rename this internal cluster name so that it does not include the "|" character because otherwise it still won't work as "|" is invalid for being used as gRPC request host
   - issue/21841, issue/16676, etc.

4. Feature: NO way to trigger the ext-authz flow conditionally

   - you can NOT enable/disable for a specific route based on path/host/IP/etc. (e.g. skip ext-authz for health check)
   - issue/24462, issue/26805, etc.

Pain Points (summary)

- Not saying you should never use EnvoyFilter API, the EnvoyFilter API has its legit use cases
- But it is not the proper API that you should use for a critical security-related workflow in your production environment at scale
- Need better first-class support!

New in 1.9: Authorization Extensibility

Infrastructure-level and First-class API support of better **extensibility** in Istio authorization:

- Added "**CUSTOM**" action in AuthorizationPolicy to specify **where/when** to trigger the ext-authz service
  - In AuthorizationPolicy, you refer to the extension provider by its unique name

- Added "**Extension Provider**" concept in MeshConfig to specify **where/how** to talk to the ext-authz service
  - Each extension provider has an unique name
  - Currently the only supported extension provider is the Envoy ext-authz filter

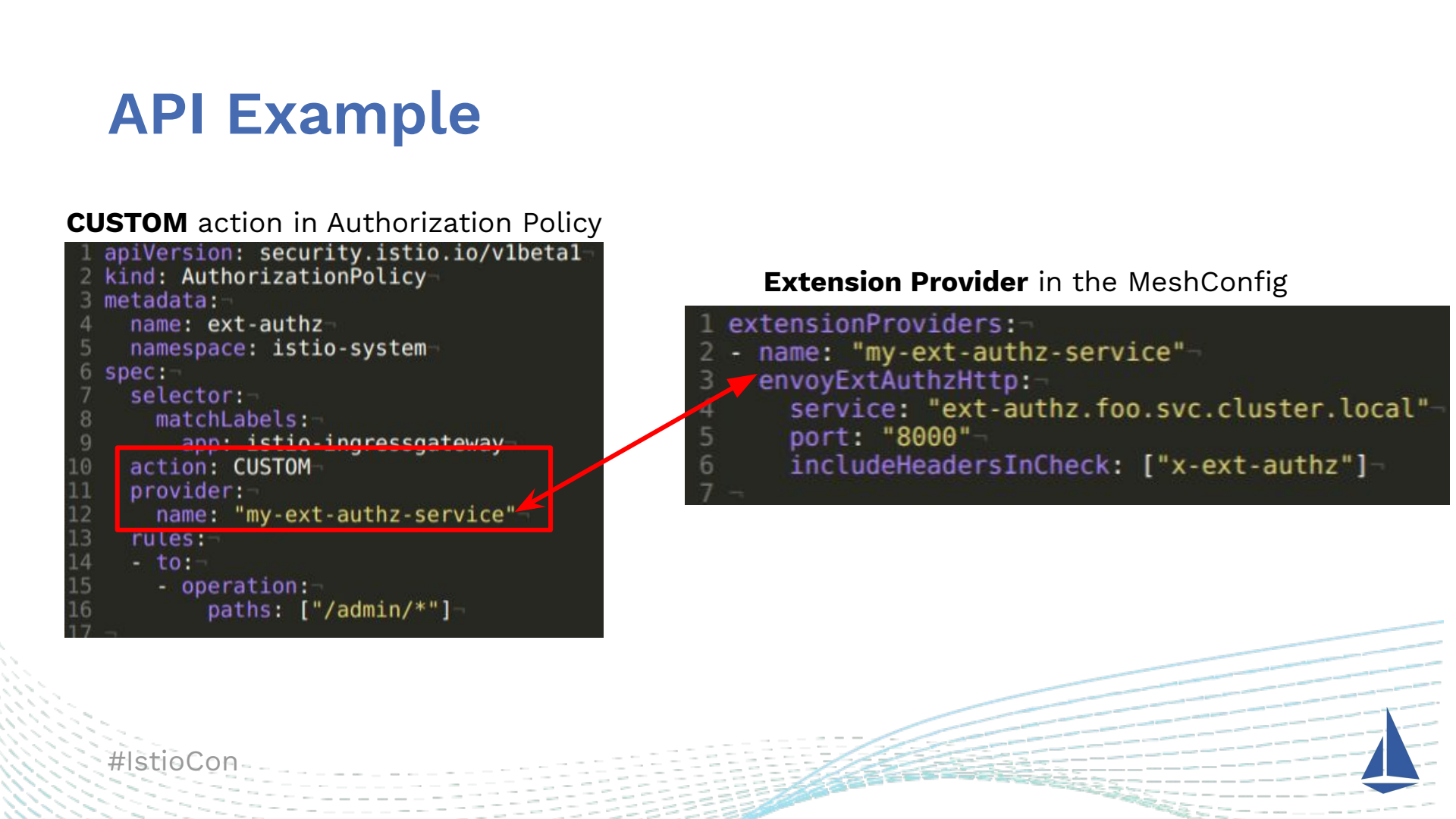
API Example

CUSTOM action in Authorization Policy

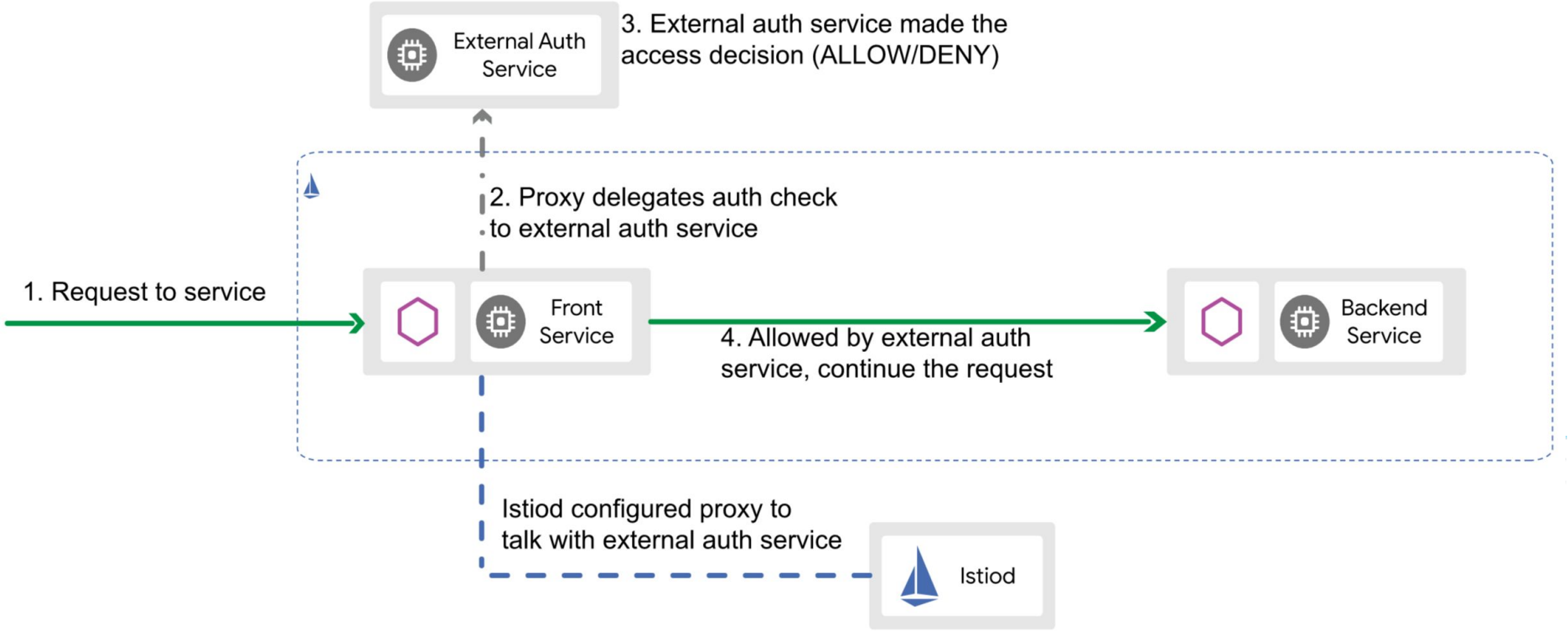
```yaml
apiVersion: security.istio.io/v1beta1
kind: AuthorizationPolicy
metadata:
  name: ext-authz
  namespace: istio-system
spec:
  selector:
    matchLabels:
      app: istio-ingressgateway
  action: CUSTOM
  provider:
    name: "my-ext-authz-service"
  rules:
  - to:
    - operation:
        paths: ["/admin/*"]
```

Extension Provider in the MeshConfig

```yaml
extensionProviders:
- name: "my-ext-authz-service"
  envoyExtAuthzHttp:
    service: "ext-authz.foo.svc.cluster.local"
    port: "8000"
    includeHeadersInCheck: ["x-ext-authz"]
```

Architecture



Benefits

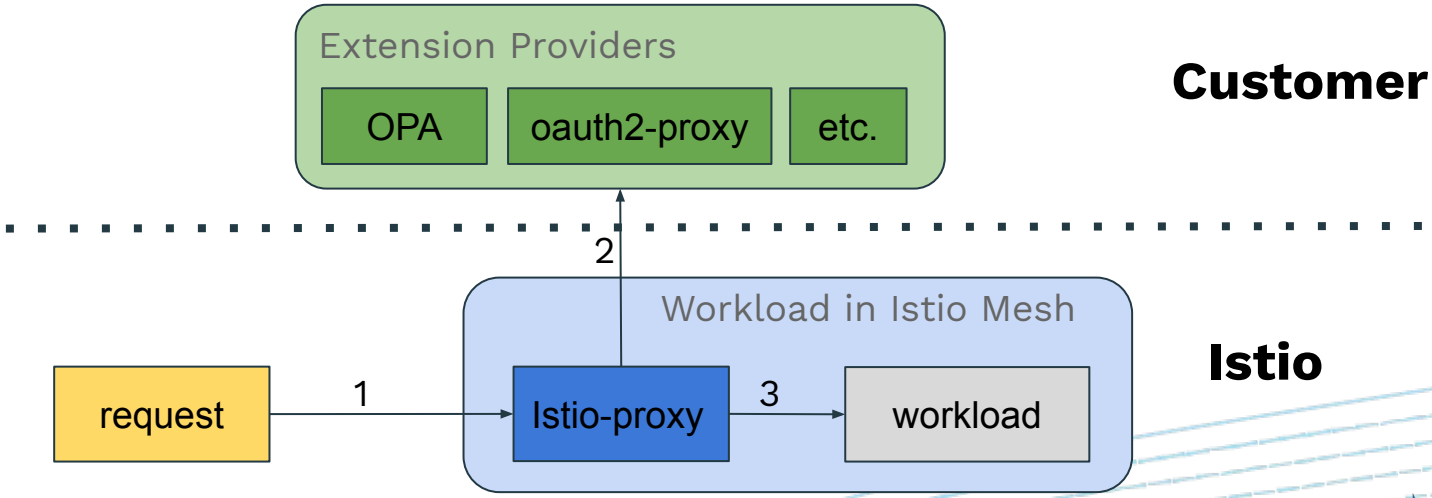
- No more EnvoyFilter, easier usage and simpler troubleshooting
- First-class API support, more reliable and stable
  - Changes in the Envoy won't break your configuration in Istio
  - Same configuration will work stably during upgrade
    - (*currently this feature is in experimental stage.)*
  - Tested, maintained and supported by Istio team
- Allow triggering the ext-authz flow conditionally
  - Trigger only for host "example.com"
  - Trigger for all paths except "/health"
  - etc.

Links

- Design: Design doc (join istio-team-drive-access for access)
- Documentation: Blog Post for this new feature
- Documentation: Task Page for using the CUSTOM action
- API: CUSTOM action
- API: Extension Provider
- Feedback Appreciated!
  - Please let us know your thoughts and suggestions on this, we are working continuously to improve it in following releases
  - https://discuss.istio.io/c/security
  - https://github.com/istio/istio/issues

DEMO: Extensibility Example

The new API in 1.9 allows Istio authorization extensibility, examples being like OPA, oauth2-proxy and etc.



Thank you!

 @yangminzhu123

 @yangminzhu

#IstioCon