Open Policy Agent

Securing Kubernetes and APIs
@https://www.meetup.com/orchestructure

Welcome!

Rajesh Jain - Cloud Engineer / Scott Knapp - Technical Sales Mgr

About Prisma Cloud

- Cloud Native Security Platform
- Helping customers secure Applications at Build, Ship, Run
- Spans IaaS / PaaS / Serverless / and Containers

About Palo Alto Networks

- The global Cybersecurity Leader
- 70,000+ customers / $3B FY’19

As a Thank you.....

If interested in a Prisma Cloud BackPack....

Send email to:

arock@paloaltonetworks.com with Subject Backpack.

You will be sent a redemption code and link to claim. Handled by 3rd party. Palo Alto doesn't store or use your information.

Ogio Rockwell Model

Agenda

Open Policy Agent

Rego

Protect and Secure

- Kubernetes
- Envoy, WASM, Use Cases

CNCF and Community

Thread

Kelsey Hightower
@kelseyhightower

The Open Policy Agent project is super dope! I finally have a framework that helps me translate written security policies into executable code for every layer of the stack.

Open Policy Agent
Policy-based control for cloud native environments
openpolicyagent.org

2:43 PM · May 13, 2020 · Twitter Web App

OPA

General Purpose Open Source Policy Engine - Open Policy Agent.

Unify Policy Enforcement across the stack

Decouple Policy Decision Making from Policy Enforcement

Current state ?

Different authz systems, global vs local?

What policies are in place?

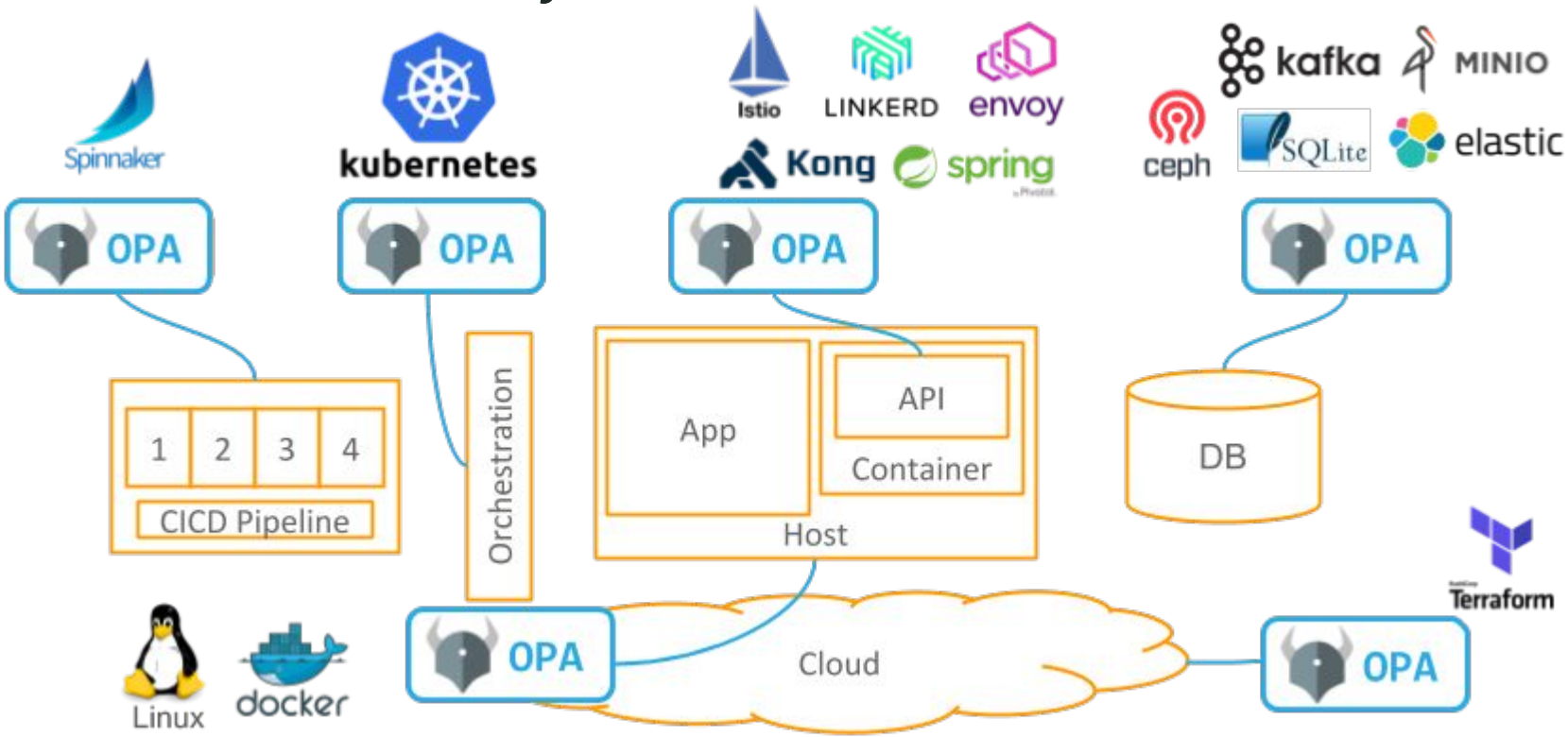
New rules, policy changes?

Audit/Compliance ? Prove to me if a resource is secure, who can access what?

VM’s, Bare metal, Kubernetes, Docker, Databases

Kubernetes : CPU, Memory limitations, Secure Images, Quotas,

OPA: Unified Policy Enforcement Across the Stack



Microservices APIs, Risk Management, Data Protection and Data Filtering

General Purpose

OPA Ecosystem

Showcase of OPA integrations, use-cases, and related projects.
Ordered by the amount of content.

Add or Update Integration

- Kubernetes Admission Control
- Container Network Authorization with Envoy
- Kafka Topic Authorization
- Container Network Authorization with Istio (at the Edge)
- Custom Application Authorization
- Ceph Object Storage Authorization
- HTTP API Authorization in PHP
- Terraform Authorization
- Gloo API Gateway
- HTTP API Authorization in Dart
- Docker controls via OPA Policies
- Elasticsearch Data Filtering
- SQL Database Data Filtering
- GCP audit with Forseti
- Conftest -- Configuration checking
- Authorization for Java Spring Security
- Gradle Build Plugin
- IPTables
- Cloudflare Worker Enforcement of OPA Policies Using WASM
- Container Network Authorization with Istio (as part of Mixer)
- Spinnaker Pipeline Policy Enforcment
- Kubernetes Admission Control using Vulnerability Scanning
- API Gateway Authorization with Kong
- Kubernetes Authorization
- Pomerium Access Proxy
- Boomerang Bosun Policy Gating
- Secure Kubernetes using eBPF & Open Policy Agent
- SSH and Sudo Authorization with Linux
- OpenFaaS Serverless Function Authorization
- AWS API Gateway
- Minio API Authorization
- Kubernetes Provisioning
- Jenkins Job Trigger Policy Enforcement
- Gluu Gateway Authorization
- Library-based Microservice Authorization
- Kubernetes Sysdig Image Scanner Admission Controller
- CoreDNS Authorization
- Traefik API Gateway

Policy Decision Making

Which users can access which resources.

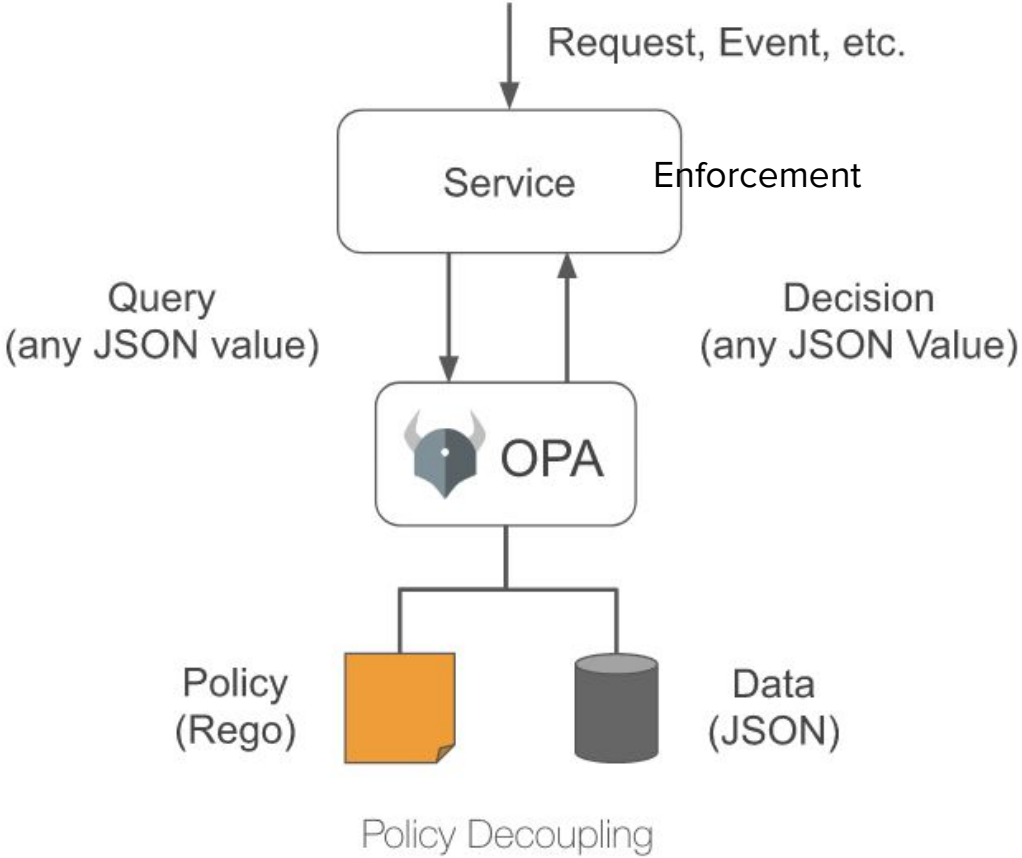
Which subnets egress traffic is allowed to.

Which clusters a workload must be deployed to.

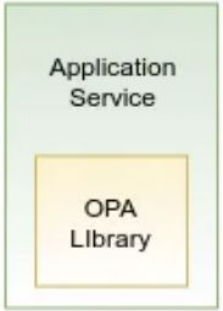
Which registries binaries can be downloaded from.

Which OS capabilities a container can execute with.

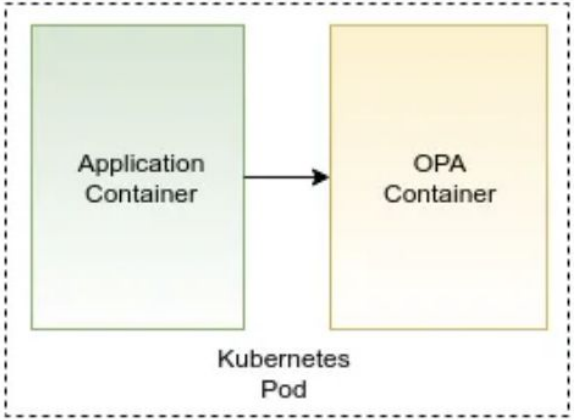
Which times of day the system can be accessed at.



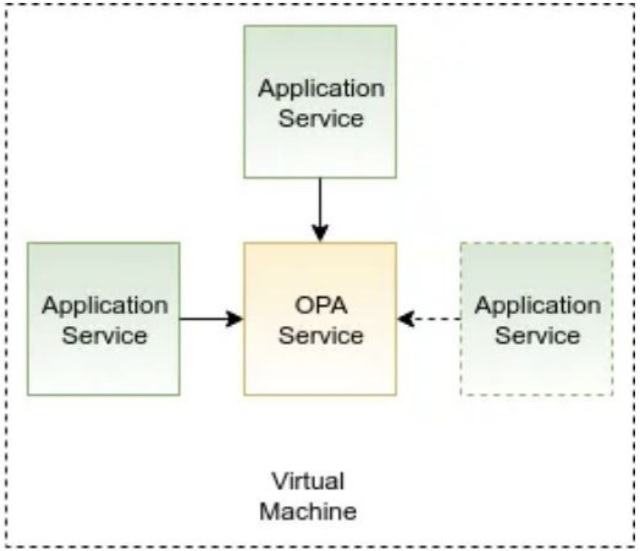
OPA Deployment



a) Link OPA library



b) Deploy OPA as a side-car container



c) Deploy one OPA instance per host

OPA Agent (Written in GO) Sidecar, Host Level Daemon, Library

Policy : In Memory, Low latency, HA.

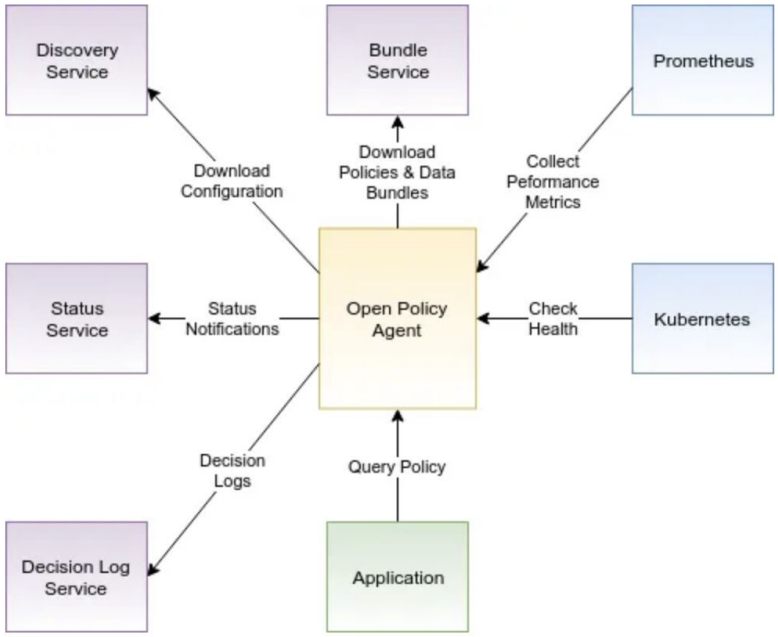
OPA API's

Management API

- Bundle API (to send policy and data)
- Discovery Service
- Status API
- Log API

VS Code Plugin

Author, Test, Debug policy



Rego Policy Language

Query Language: Assertions on data stored in OPA

E.g.

Variables, Sets, Arrays,

Assertions

Rules: Generate Objects, Sets, Definitions, Functions

```
rect := {"width": 2, "height": 4}
```

```
rect == {"height": 4, "width": 2}
```

```
true
```

```
default allow = false

allow {
    input.user == "bob"
    input.method == "GET"
}

allow {
    input.user == "alice"
}
```

When the `allow` document is queried, the return value will be either `true` or `false`.

```
{
    "user": "bob",
    "method": "POST"
}
```

```
false
```

```
authorize = "allow" {
    input.user == "superuser"           # allow 'superuser' to perform any operation.
} else = "deny" {
    input.path[0] == "admin"            # disallow 'admin' operations...
    input.source_network == "external"  # from external networks.
} # ... more rules
```

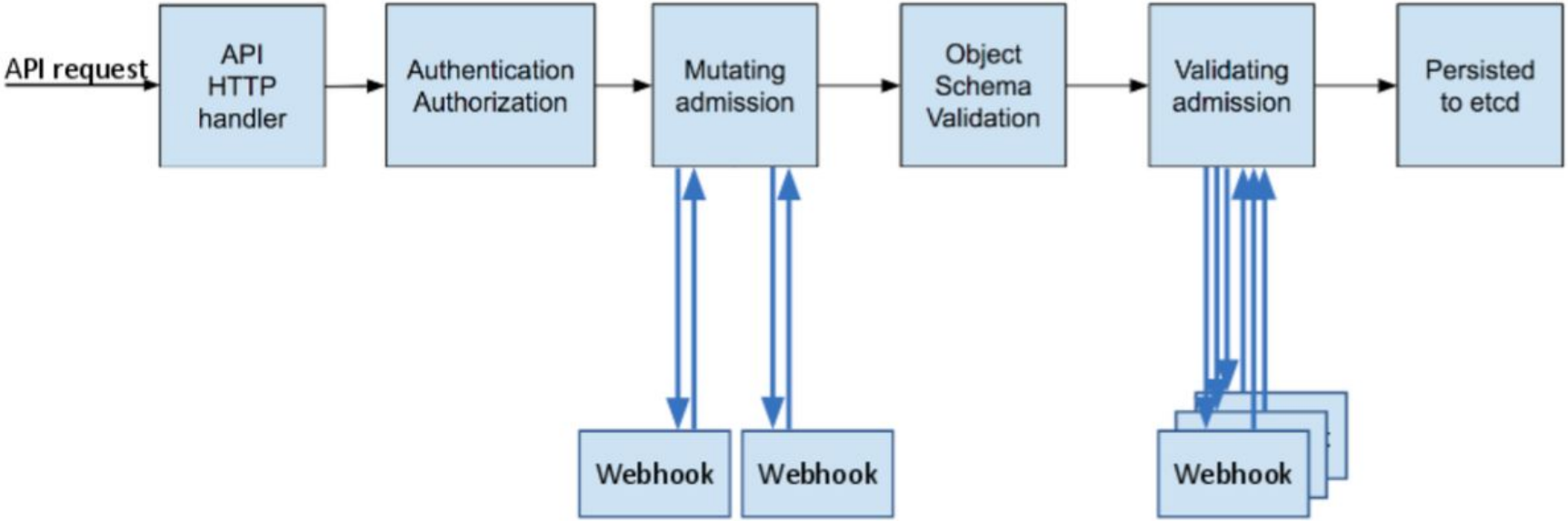
In the example below, evaluation stops immediately after the first rule even though the input matches the second rule as well.

```
{
  "path": [
    "admin",
    "exec_shell"
  ],
  "source_network": "external",
  "user": "superuser"
}
```

```
"allow"
```

Rego Playground Demo

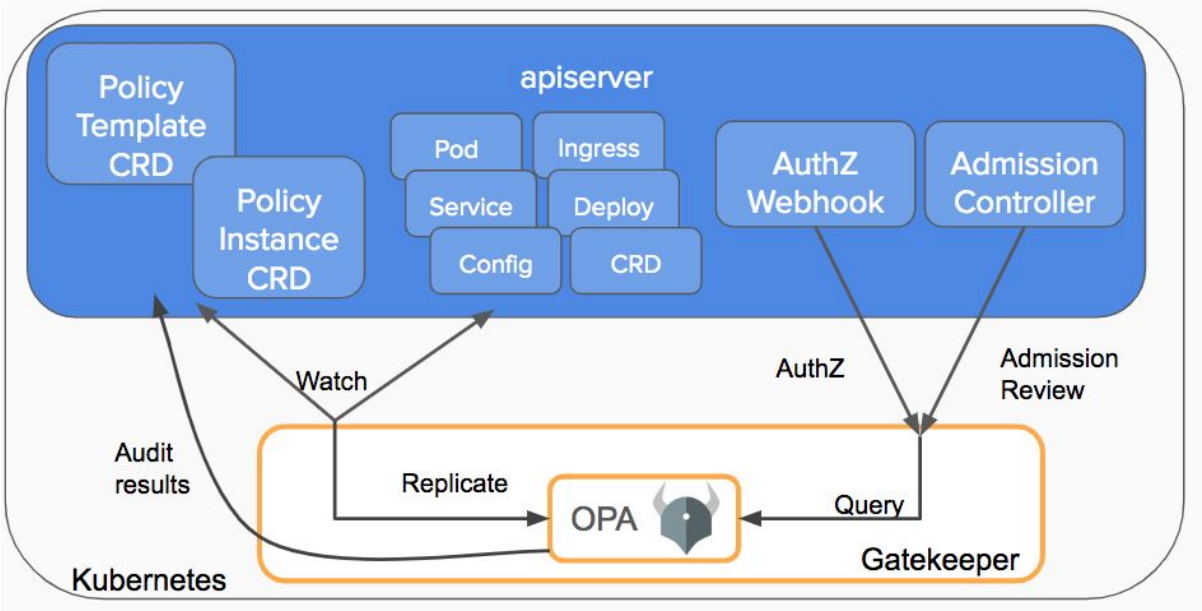
Kubernetes


API request
API HTTP handler
Authentication Authorization
Mutating admission
Object Schema Validation
Validating admission
Persisted to etcd
Webhook
Webhook
Webhook

OPA Gatekeeper

OPA Gatekeeper extends Open Policy Agent to allow users to define OPA policies as native Kubernetes resources. Gatekeeper simplifies the lifecycle of creating and maintaining OPA policies within your Kubernetes cluster and additionally provides the following benefits over standard OPA within a Kubernetes cluster:

- An extensible, parameterized policy library.
- Native Kubernetes CRDs for instantiating the policy library (aka “constraints”).
- Native Kubernetes CRDs for extending the policy library (aka “constraint templates”).
- Audit functionality.



Example

```yaml
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
  name: k8srequiredlabels
spec:
  crd:
    spec:
      names:
        kind: K8sRequiredLabels
        listKind: K8sRequiredLabelsList
        plural: k8srequiredlabels
        singular: k8srequiredlabels
      validation:
        # Schema for the `parameters` field
        openAPIV3Schema:
          properties:
            labels:
              type: array
              items: string
  targets:
    - target: admission.k8s.gatekeeper.sh
      rego: |
        package k8srequiredlabels

        violation[{"msg": msg, "details": {"missing_labels": missing}}] {
          provided := {label | input.review.object.metadata.labels[label]}
          required := {label | label := input.parameters.labels[_]}
          missing := required - provided
          count(missing) > 0
          msg := sprintf("you must provide labels: %v", [missing])
        }
```

Template identifying info

Template values for constraint crd's

Schema

Rego

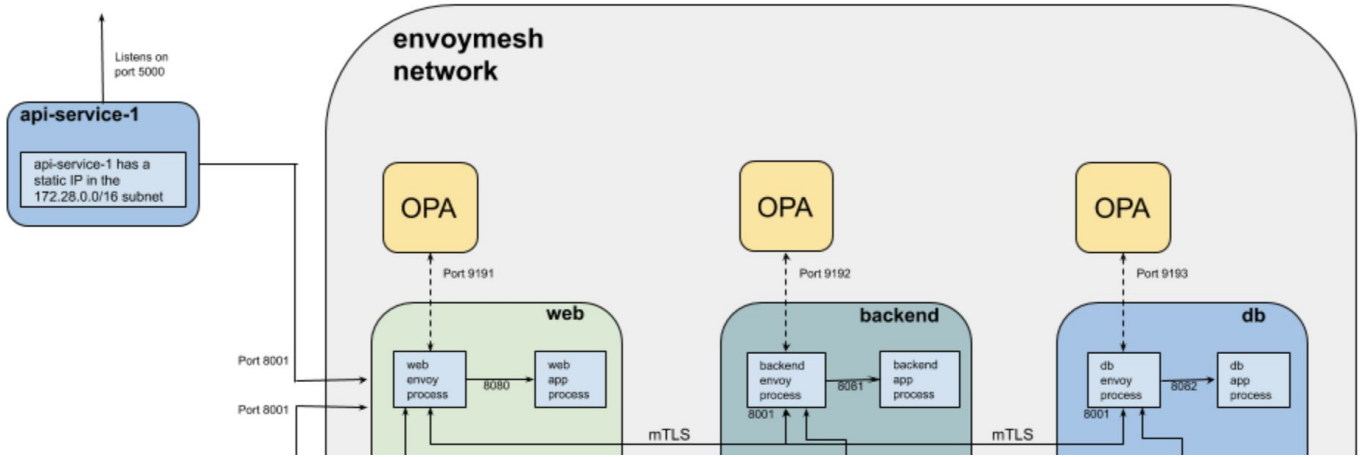
```yaml
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sRequiredLabels
metadata:
  name: ns-must-have-mydemoproject
spec:
  match:
    kinds:
      - apiGroups: [""]
        kinds: ["Namespace"]
  parameters:
    labels: ["mydemoproject"]
```

The CRD above requires namespaces to be created with a label of _mydemoproject . To restrict to a specific set of namespaces provide the list of namespaces it should apply to.

Kubernetes Admission Controller Demo

Envoy and OPA

Envoy proxy calls OPA's gRPC server that implements the Envoy External Authorization API.

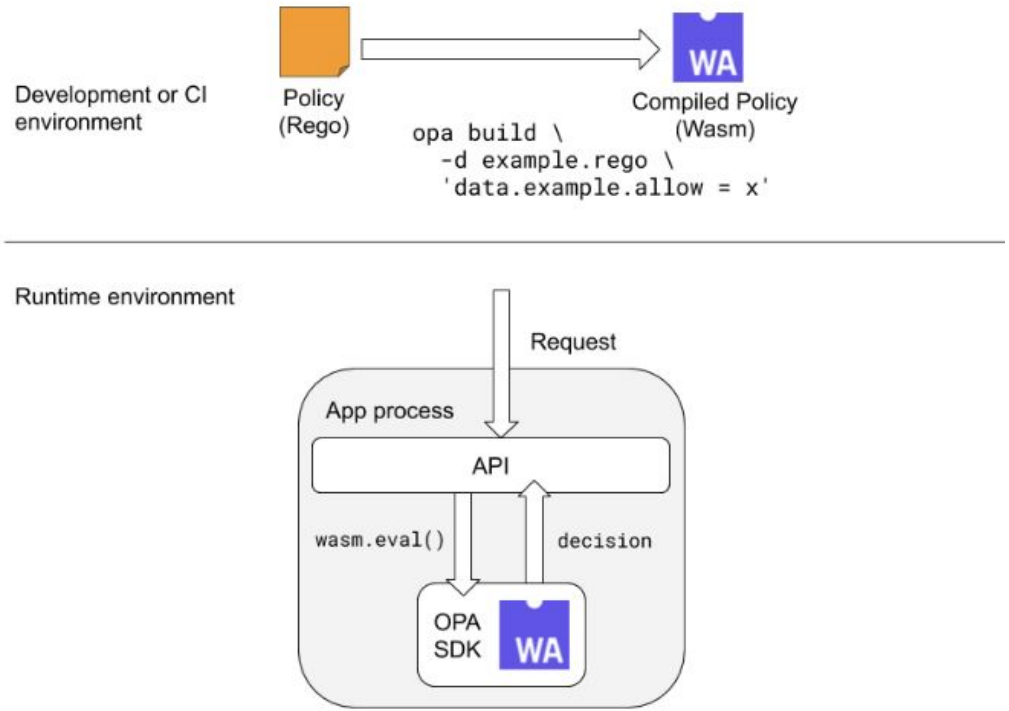


Rego Compiled in WASM

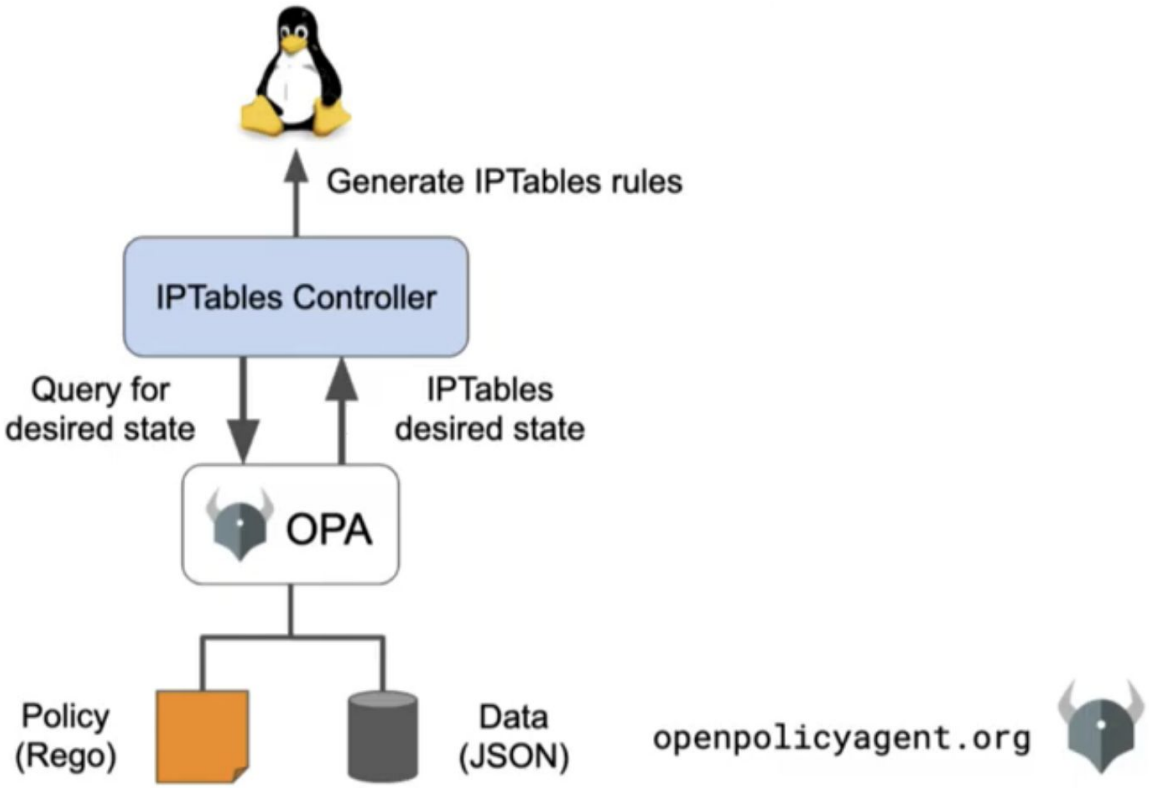
single statement = ~30 KB on disk.

300,000 statements = ~20MB on disk

evaluates ~20x faster with the Wasm compiled version.



IPTables Integration



Examples

Implementations

Netflix enforcing access control in microservices across a variety of languages and frameworks

Pinterest: Kafka. At peak, OPA serves ~450K decisions/second across their clusters

TripAdvisor: Testing framework to mock changes before you promote them

Capital One: Policy check in CI/CD

(https://github.com/open-policy-agent/opa/blob/master/ADOPTERS.md)

Community

CNCF Incubating Project

www.openpolicyagent.org

https://github.com/open-policy-agent (20+ Repos)

Slack : openpolicyagent.slack.com

Rego Playground

Cloud Native Security Bootcamp

June 18th - 11am - 1pm

Workshop for IT professionals focused on learning more about technology to enable DevSecOps

Focused on Prisma Cloud Security Platform. Hands on lab exercises across securing IaaS / PaaS / Serverless / and Containers

Capture the Flag format

$50 Grubhub code for attending / Additional prizes for top finishers

Email sknapp@paloaltonetworks.com or

https://register.paloaltonetworks.com/cloudnativesecuritycamp27may

Q/A

Where do I start?

Rego, OPA, Kubernetes Admission Controllers, Gatekeeper etc.