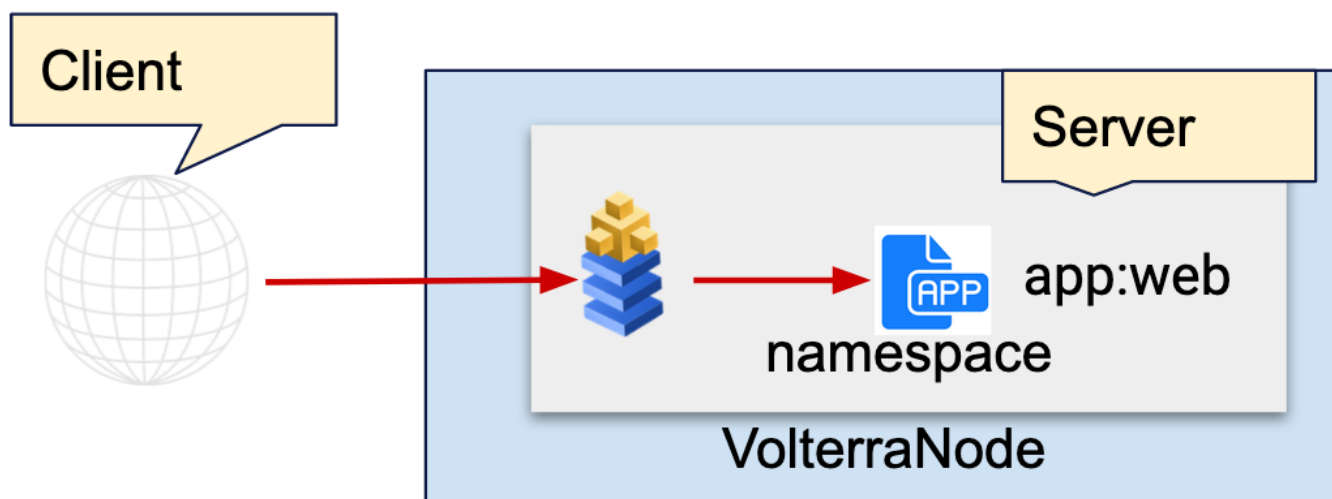
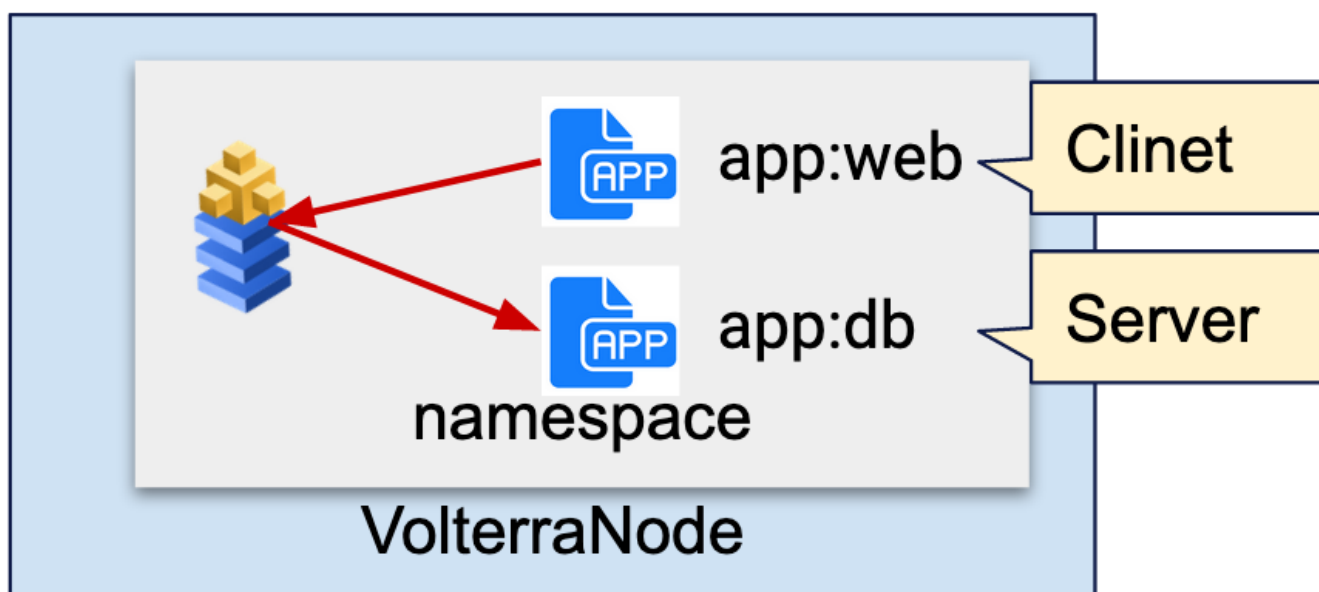


Service Policy (Ingress Gateway)

Ingress GatewayはHTTP ベースのセキュリティを提供します。外部からVolterra Nodeに入ってくるトラフィックをClient、Kubernetes ServiceをServerとなります。例えば以下の場合、外部ネットワーク(Any)となり、Kubernetes Serviceは app:webが設定されたServiceとなります。



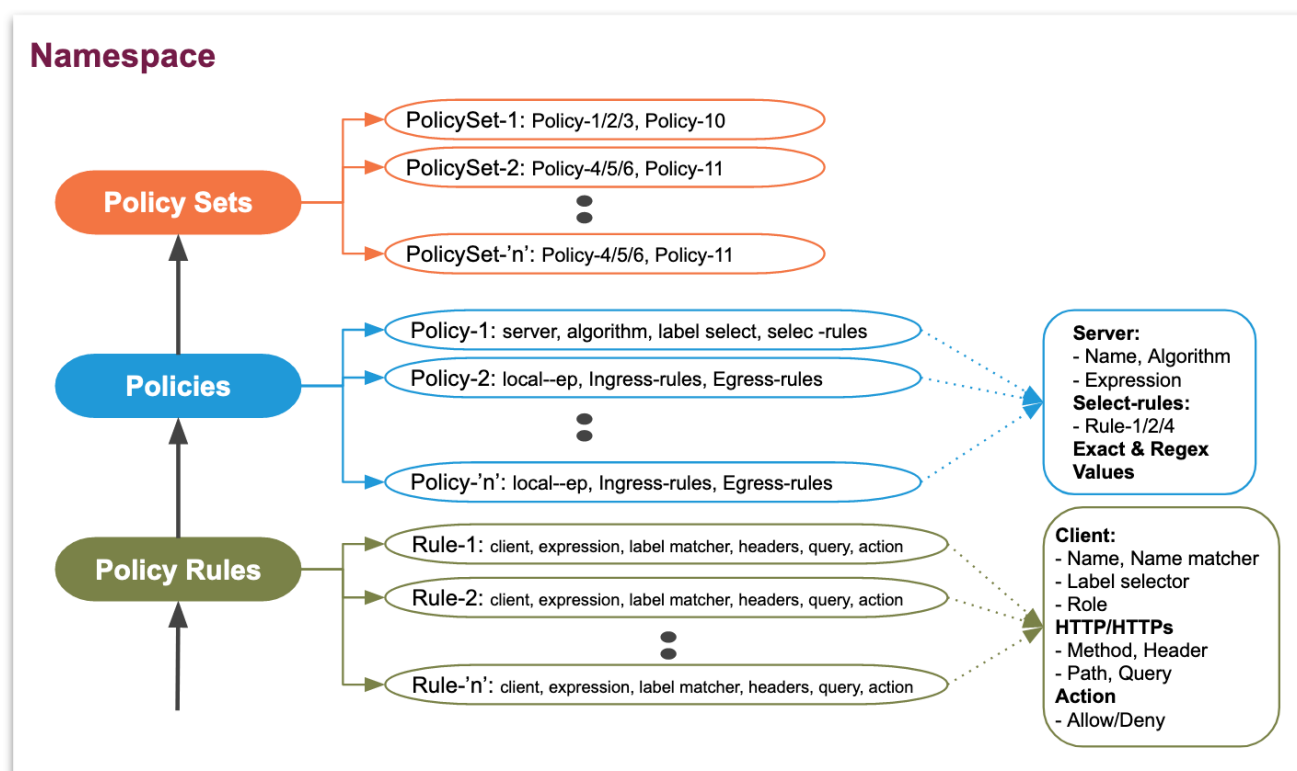
以下の場合、Clientはapp:webが設定されたPodとなり、Serverは app:DBが設定されたServiceとなります。



Service policyの構造

Service Policy RuleでClientnetの条件を作成し、Service PolicyでServerに対してService Policy Ruleを適用します。Service Policy SetでService Policy RuleをNamespaceに対して適用します。

Tenant

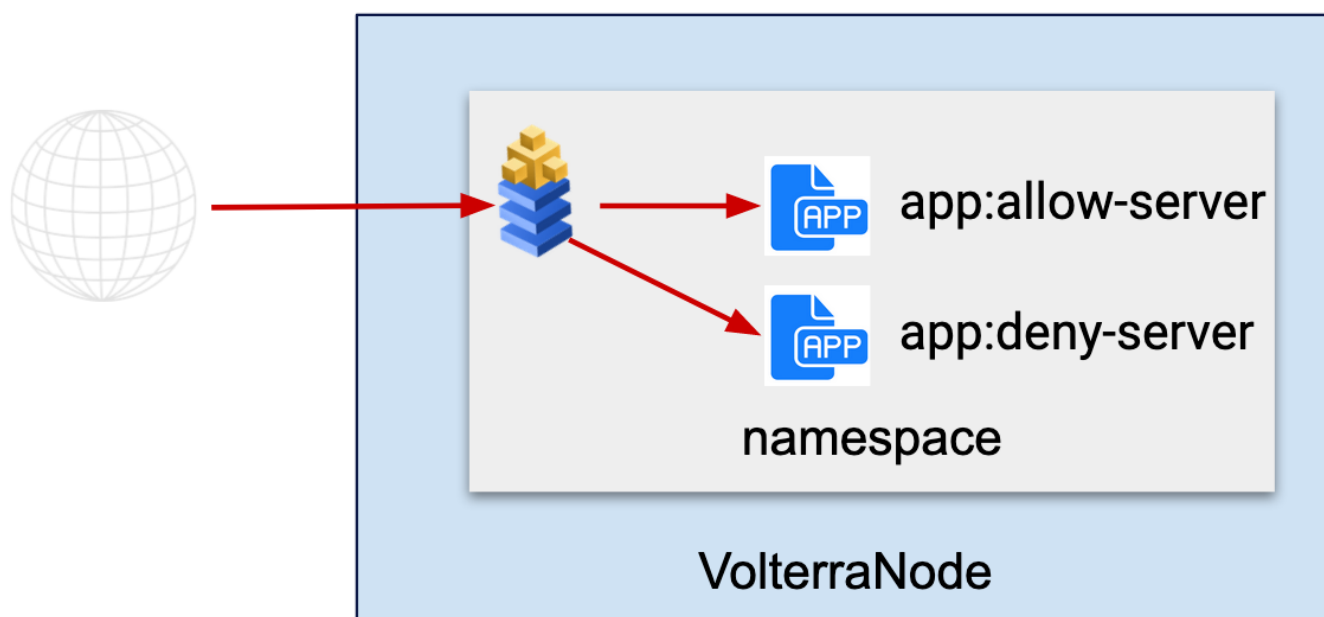


Service Policy

2つのサービスを作成し、外部からdeny-serverをもつサービス(HTTP loadbalancer)は url/deny/のPathへのアクセスを拒否します。

インターネットからの通信制御

2つのサービスを作成し、外部からdeny-serverをもつサービス(HTTP loadbalancer)は url/deny/のPathへのアクセスを拒否します。



Kubenretesの設定

namespaceは`security`とし、virtual-siteは`vsite-adc`を作成します。ラベルが異なる2つのPod, `app:allow-server`と`app:deny-server`を作成します。

allow-server

```
apiVersion: apps/v1
metadata:
  name: allow-server
  namespace: security
  annotations:
    ves.io/virtual-sites: security/vsite-adc
spec:
  replicas: 1
  selector:
    matchLabels:
      app: allow-server
  template:
    metadata:
      labels:
        app: allow-server
    spec:
      containers:
        - name: ce-client
          image: dnakajima/inbound-app:2.0
```

deny-server

```
apiVersion: apps/v1
metadata:
  name: deny-server
  namespace: security
  annotations:
    ves.io/virtual-sites: security/vsite-adc
spec:
  replicas: 1
  selector:
    matchLabels:
      app: deny-server
  template:
    metadata:
      labels:
        app: deny-server
    spec:
      containers:
        - name: ce-client
          image: dnakajima/inbound-app:2.0
```

作成したPodに対応する2つのservice, を作成します。

allow-server

```
apiVersion: v1
metadata:
  name: allow-server
  namespace: security
  annotations:
    ves.io/virtual-sites: security/vsite-adc
spec:
  ports:
    - protocol: TCP
      port: 80
      targetPort: 8080
  selector:
    app: allow-server
  type: ClusterIP
```

deny-server

```
apiVersion: v1
metadata:
  name: deny-server
  namespace: security
  annotations:
    ves.io/virtual-sites: security/vsite-adc
spec:
  ports:
    - protocol: TCP
      port: 80
      targetPort: 8080
  selector:
    app: deny-server
  type: ClusterIP
```

Origin pool の設定

作成したServiceを外部からアクセスできるようにIngress Gatewayを設定します。作成した2つの Serviceを Origin poolとして登録します。 Manage -> Origin Pools で "Add Origin Pool"を選択します。

- Origin server
 - Name: **allow-server**
 - Basic Configuration:
 - Select Type of Origin Server: **k8sService – Name of Origin Ser...**
 - Service Name: **allow-server.security** ("Kubernetes service名 . namespace")
 - Select Site or Virtual Site: **Virtual Site**
 - Virtual Site: **vsite-adc**。
 - Select Network on the Site: **Vk8s Networks on Site**

- Port: 80

The screenshot shows the 'New Origin Pool' configuration interface. On the left, a sidebar lists 'Origin Pool' with sub-items: 'Metadata', 'Basic Configuration' (selected), 'List of Health Check(s)', and 'TLS Configuration'. The main area is titled 'Basic Configuration *' and includes a 'Reset All Fields' link. The configuration is organized into sections: 'Origin Servers *' with a dropdown for 'Select Type of Origin Server *' (set to 'k8s Service Name of Origin Server on ...'), a text field for 'Service Name *' (set to 'allow-server.security'), a dropdown for 'Select Site or Virtual Site *' (set to 'Virtual Site'), a dropdown for 'Virtual Site' (set to 'security/vsite-adc'), and a dropdown for 'Select Network on the site *' (set to 'Vk8s Networks on Site'). An 'Add item' button is below these sections. At the bottom, there are three fields: 'Port' (80), 'LoadBalancer Algorithm' (Enter loadbalancer algorithm), and 'Endpoint Selection' (Local Endpoints Preferred). A 'Cancel and Exit' button is in the bottom left.

HTTP Load Balancerの設定

Manage -> HTTP Load Balancers で “Add HTTP load balancer”を選択します。

- Name: **nginx-lb**
- Domains: **dummy.localhost** (設定するとDNS infoにVolterraからdomain名が払い出されます。設定後に払い出されたドメイン名を設定してください。)
- Select Type of Load Balancer: **HTTP**
- Default Route Origin Pools: **namespace/nginx-endpoint** (上記で作成したOrigin pool)

設定するとDNS infoにVolterraからdomain名が払い出されます。作成したロードヴァランダーのDomainsに設定するか、任意のDNSサーバのCNAMEレコードに設定してください。外部から設定したドメインにアクセスするとNginxのWebUIが表示されます。

サービスへの接続確認

作成したサービスにアクセスできることを確認します。 <http://url/> , <http://url/allow/> , <http://url/deny/> にアクセスできることを確認します。

This is denied page running on deny-server-5bb7c7f74b-hb9tf

This is allowed page running on deny-server-5bb7c7f74b-hb9tf

This pod is running on deny-server-5bb7c7f74b-hb9tf

Service policyの作成

Service Policy Ruleを2つ作成します。

- deny-web-server
 - Action: **Deny**
 - HTTP Path: **Prefix Values : /deny**
- allow-any-server
 - Action: **Allow**

Add service policy rule

Form

Json

Schema

Name * ?

deny-web-server

Labels ?

Select Label Here

Description ?

Enter description

Action * ?

Deny



Rate Limiter ?

+ Select rate limiter

Name	Namespace	UID
------	-----------	-----

No items selected

HTTP Path

Prefix Values ?

+ Add prefix value

Exact Values ?

+ Add exact value

/deny



Regex Values ?

[+ Add regex value](#)

Transformers ?

Service Policy を2つ作成します。

- deny-web-server
 - Server Label Selector: `app:in(deny-server)`
 - Rule Combining Algorithm: `First Rule Match`
 - Select rule: `deny-web-server`
- allow-any-server
 - Rule Combining Algorithm: `First Rule Match`
 - Select rule: `allow-any-server`

Add service policy

Form Json Schema

Rule Combining Algorithm * ⓘ

First Rule Match

✕ ▼

Server Name ⓘ

Enter server name

Server Name Matcher ⓘ

Server Label Selector ⓘ

Selector Expression ⓘ

app

In (deny-server)

Rules ⓘ

⊕ Select rule

	<input type="checkbox"/>	Name	Namespace	UID
1	<input type="checkbox"/>	deny-web-server	security	2776738e-0de9-40cf-84a6-32118db2a6e0

HTTP CONNECT Port Matcher ⓘ

Service Policy SetにService Policyを追加します

- po-set1
 - Policies: Select policy: [1: deny-web-server, 2:allow-any-server]

Edit service policy set po-set1

[Form](#)[Json](#)[Schema](#)Name * 

po-set1

Labels 

Select Label Here

Description 

Enter description

Policies  Select policy

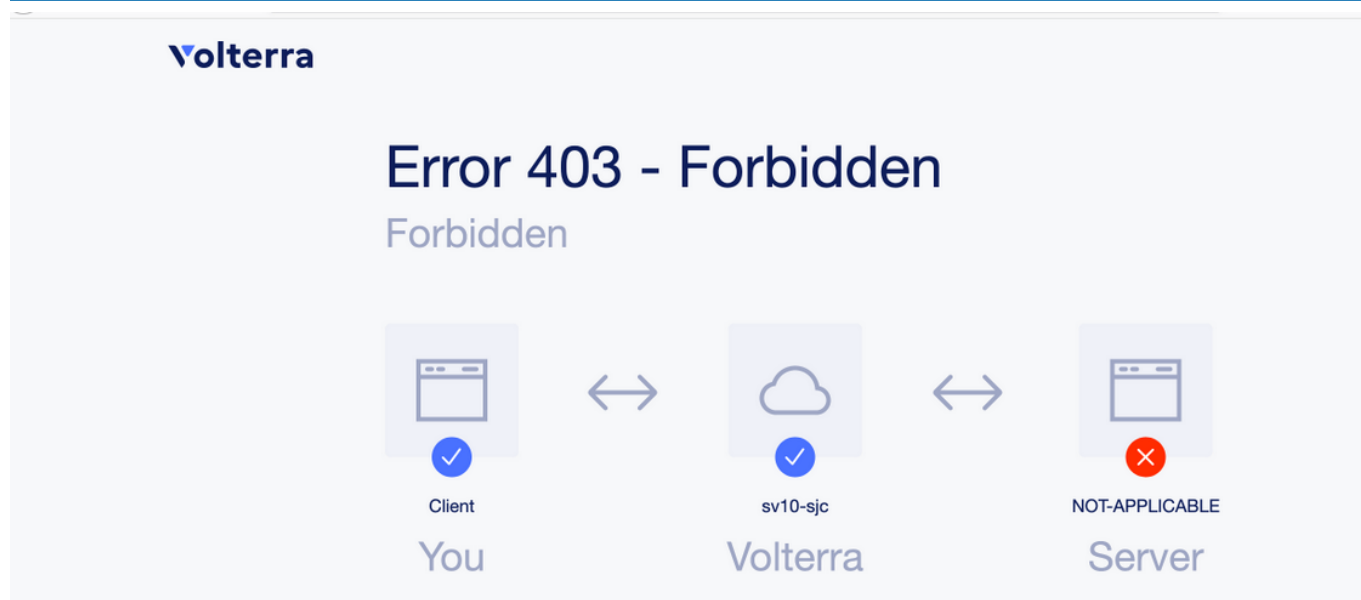
	<input type="checkbox"/>	Name	Namespace	UID
1	<input type="checkbox"/>	deny-web-server	security	08dccdaf-4418-4d9e-b90b-67b5f255f51c
2	<input type="checkbox"/>	allow-any-server	security	7681994c-aa29-45b5-bb4f-d12647459024

設定の確認

作成したサービスにアクセスできることを確認します。deny-web-serverの<http://url/>,<http://url/allow/> は正常に表示されますが、<http://url/deny>は403エラーが返るのを確認します。

This is denied page running on deny-server-5bb7c7f74b-hb9tf

This is allowed page running on deny-server-5bb7c7f74b-hb9tf



作成したサービスにアクセスできることを確認します。allow-web-serverの<http://url/>,<http://url/allow/>,<http://url/deny/> はアクセスが可能です。