Lab5. Сетевая политика с OVNKubernetes

Оригинал примера https://examples.openshift.pub/networking/network-policy/OVNKubernetes/

Применяется на основе меток или аннотаций в рамках проекта

Пустой селектор метки соответствует всем

Разрешающие правила

Ingress - кто может подключиться к этому поду

Egress - куда этот под может подключиться

Правила

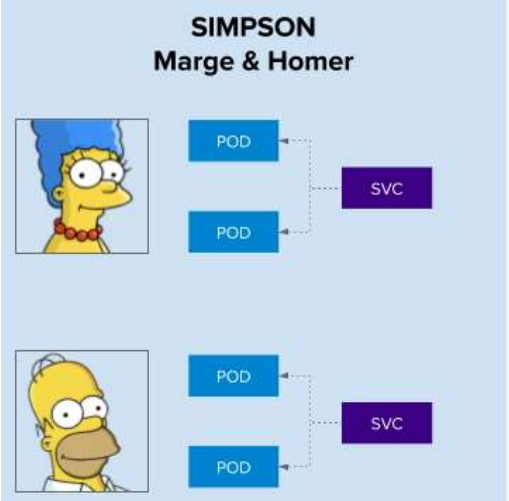
трафик разрешен, если только сетевая политика не выбирает под.

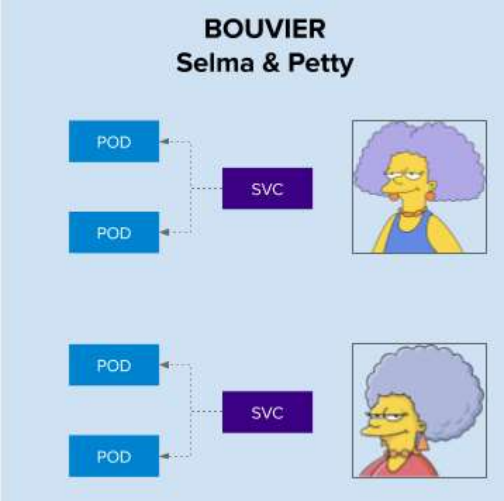
трафик запрещен, если под выбран в политиках, но ни одна из них не имеет разрешающих правил

Можете создавать только правила, разрешающие трафик

Область действия: пространство имен

Разверните демонстрационную среду





Шаг 1. Создание проектов.

Создайте проект bouvier

oc new-project bouvier

Создайте приложение patty

oc new-app quay.io/openshift-examples/simple-http-server:micro --name patty

Создайте маршрут

oc create route edge patty --service=patty

Создайте приложение selma

oc new-app quay.io/openshift-examples/simple-http-server:micro --name selma

oc create route edge selma --service=selma

Создайте проект simpson

oc new-project Simpson

Создайте приложение homer

oc new-app quay.io/openshift-examples/simple-http-server:micro --name homer

oc create route edge homer --service=homer

Создайте приложение marge

oc new-app quay.io/openshift-examples/simple-http-server:micro --name marge

oc create route edge marge --service=marge

Шаг 2. Опционально. Можно выполнить, если хостовая система Linux

Загрузите скрипты для визуализации тестирования коммуникаций

git clone https://github.com/openshift-examples/network-policies-tests.git

cd network-policies-tests/

Запустите скрипт для визуализации коммуникаций

./run-tmux.sh apps.<cluster_name>.<base_domain>

Подставьте свои значения имени кластера и домена.

Обратите внимание на доступность подов. Изначально каждый может общаться с каждым

Шаг 3. Проверьте созданную среду

Выведите список подов

oc get pods -o wide -n simpson

oc get pods -o wide -n bouvier

Шаг 4. Применение политик.

Кейс 1. Simpson - default-deny

oc apply --n simpson -f default-deny.yml

Создайте default-deny.yml вида:

kind: NetworkPolicy

apiVersion: networking.k8s.io/v1

metadata:

  name: default-deny

spec:

```
  podSelector: {}
```

Запустите проверку скриптом ./OVNKubernetes/dump-net.sh master-0 master-0.case

Кейс 2. Симпсон разрешает трафик из пространств имен openshift-ingress

Создайте openshift-ingress.yml

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-from-openshift-ingress
spec:
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          network.openshift.io/policy-group: ingress
  podSelector: {}
  policyTypes:
  - Ingress
```

```
oc apply -f openshift-ingress.yml
```

Ввиду доступа HostNetwork к OpenShift Ingress необходимо применить метку к пространству имен по умолчанию:

```
oc label namespace default 'network.openshift.io/policy-group=ingress'
```

Кейс 3. Simpson разрешает внутрении коммуникации

Создайте allow-same-namespace.yml

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-same-namespace
spec:
  podSelector:
  ingress:
  - from:
    - podSelector: {}
```

oc apply -f allow-same-namespace.yml

Запустите скрипт $ ./OVNKubernetes/dump-net.sh master-0 master-0.case3

Кейс 4. Selma и Patty хотят общаться с Marge

Шаг 1. Пометьте пространство имен bouvier:

oc label namespace/bouvier name=bouvier

Шаг 2. Примените Network Policy

Создайте allow-from-bouviers-to-marge.yml

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-from-bouviers-to-marge
spec:
  podSelector:
    matchLabels:
      deployment: marge
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          name: bouvier
```

Примените Network Policy

oc apply -f allow-from-bouviers-to-marge.yml

Запустите скрипт ./OVNKubernetes/dump-net.sh master-0 master-0.case4

Шаг 3. Удалите демонстрационную среду

oc delete project simpson bouvier