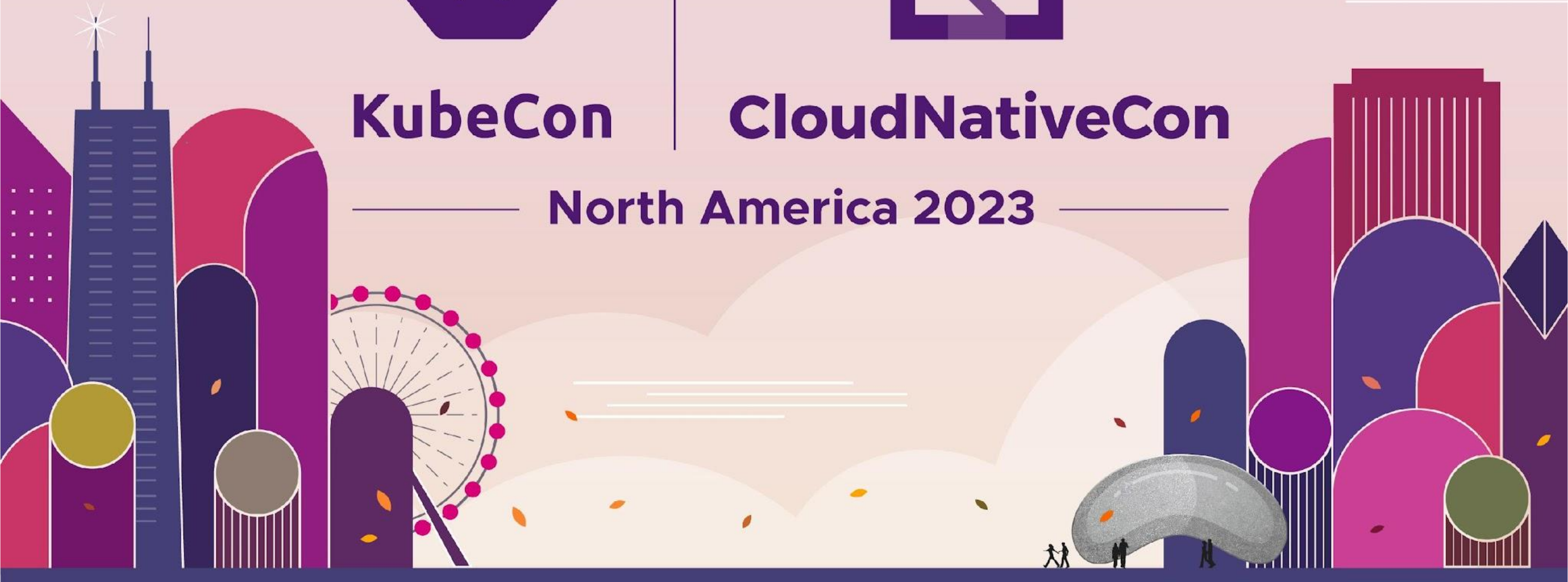
KubeCon | CloudNativeCon

North America 2023



KubeCon | CloudNativeCon

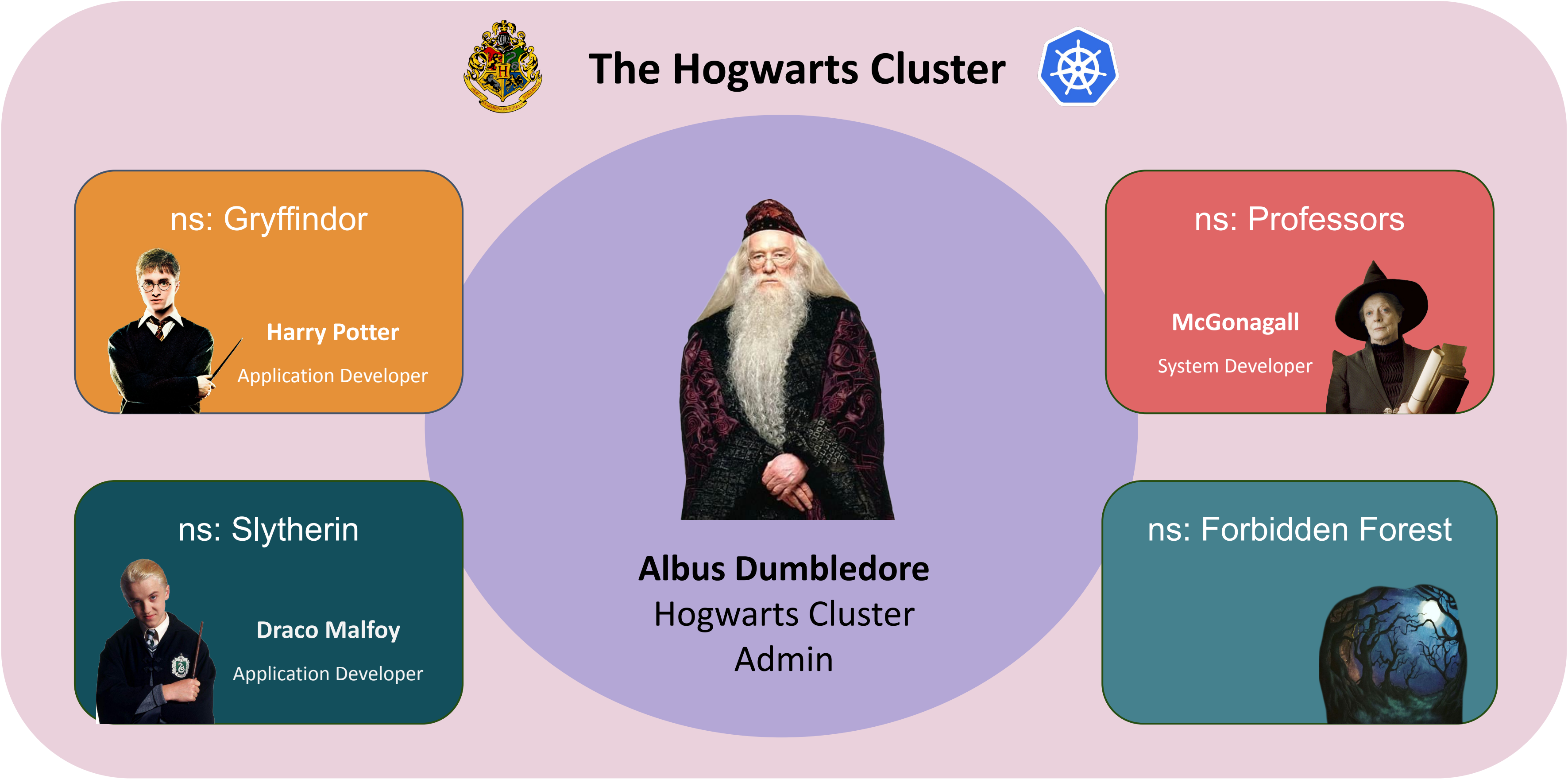
North America 2023

AdminNetworkPolicy

A New Kubernetes-Native API for Comprehensive Cluster-Wide Network Security

Surya Seetharaman, Nadia Pinaeva & Andrew Stoycos, Red Hat
Yang Ding, VMware

Personas



The Hogwarts Cluster

ns: Gryffindor

Harry Potter

Application Developer

ns: Slytherin

Draco Malfoy

Application Developer

Albus Dumbledore
Hogwarts Cluster
Admin

ns: Professors

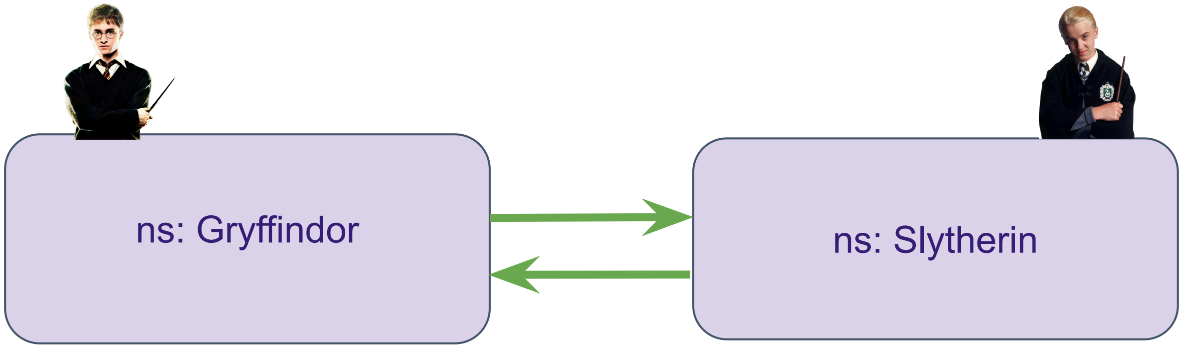
McGonagall

System Developer

ns: Forbidden Forest

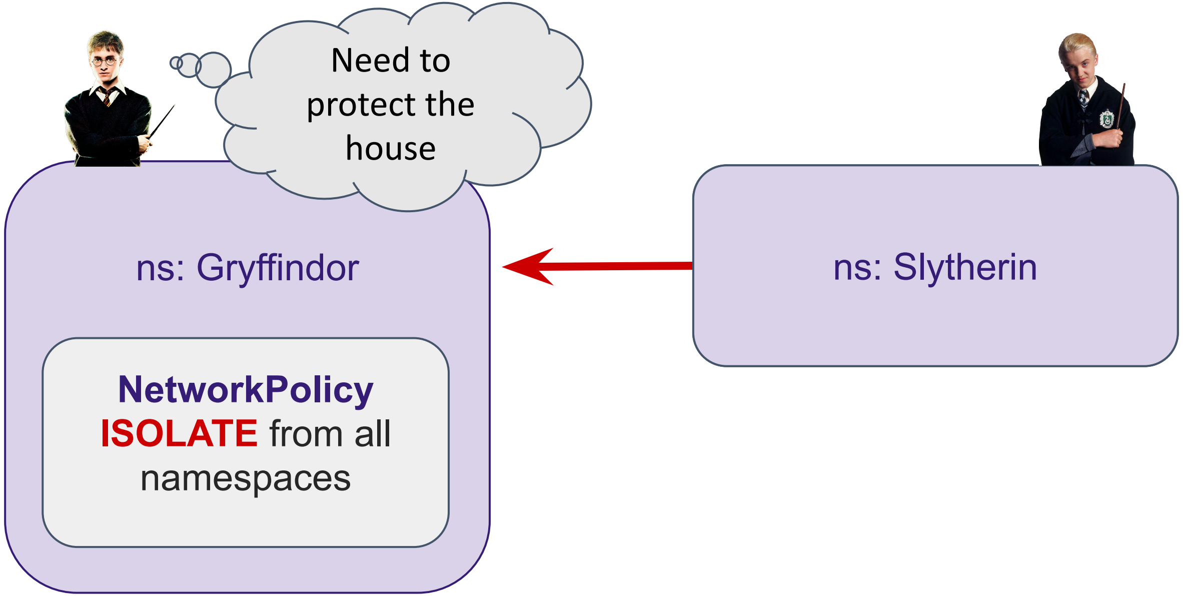
Kubernetes Networking: Always Allow

By default, all connections between pods are **allowed** in a kubernetes cluster.



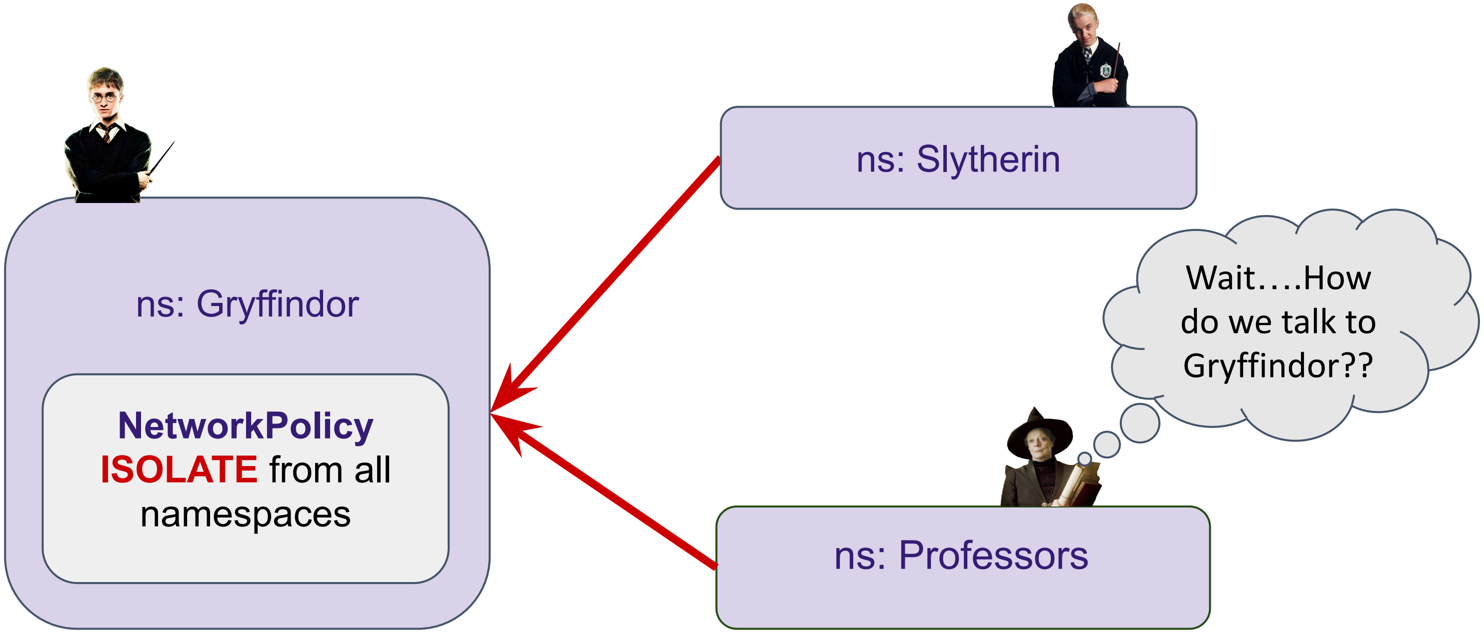
NetworkPolicy API

The **NetworkPolicy API** facilitates namespaced network security for pods.
It utilizes an allowlist model enabling **application developers** to restrict pod connections.



NetworkPolicy API

The **NetworkPolicy API** facilitates namespaced network security for pods.
It utilizes an allowlist model enabling **application developers** to restrict pod connections.

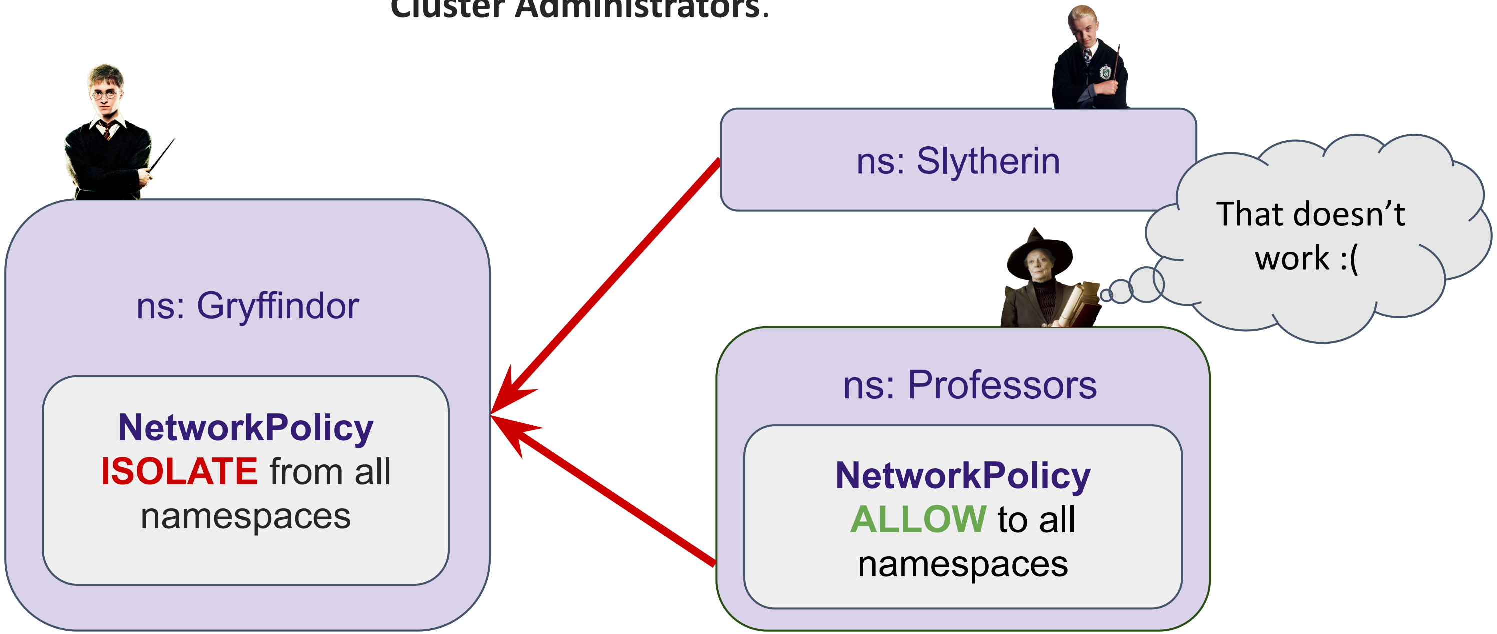


ns: Slytherin
ns: Gryffindor
NetworkPolicy
ISOLATE from all namespaces
Wait….How do we talk to Gryffindor??
ns: Professors

NetworkPolicy API

A connection should be allowed from **both sides** to succeed.

To **override** this behaviour a cluster-level object is required, but the **NetworkPolicy API** was **not** designed for **Cluster Administrators**.



ns: Gryffindor

NetworkPolicy
ISOLATE from all namespaces

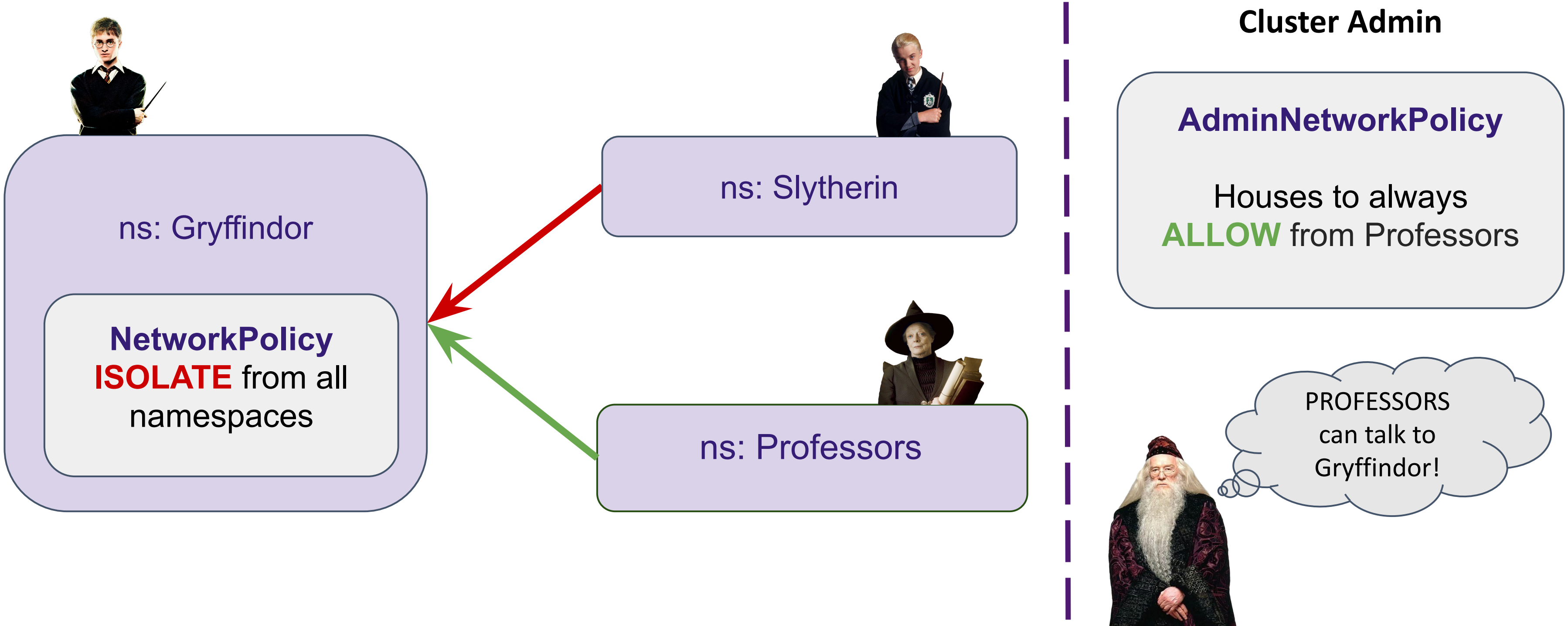
ns: Slytherin

ns: Professors

NetworkPolicy
ALLOW to all namespaces

AdminNetworkPolicy API: Strong ALLOW non-overridable

Cluster Administrators need to enforce security policies that will apply to multiple namespaces in the cluster and cannot be overridden by other cluster personas.



ns: Gryffindor

NetworkPolicy
ISOLATE from all namespaces

ns: Slytherin

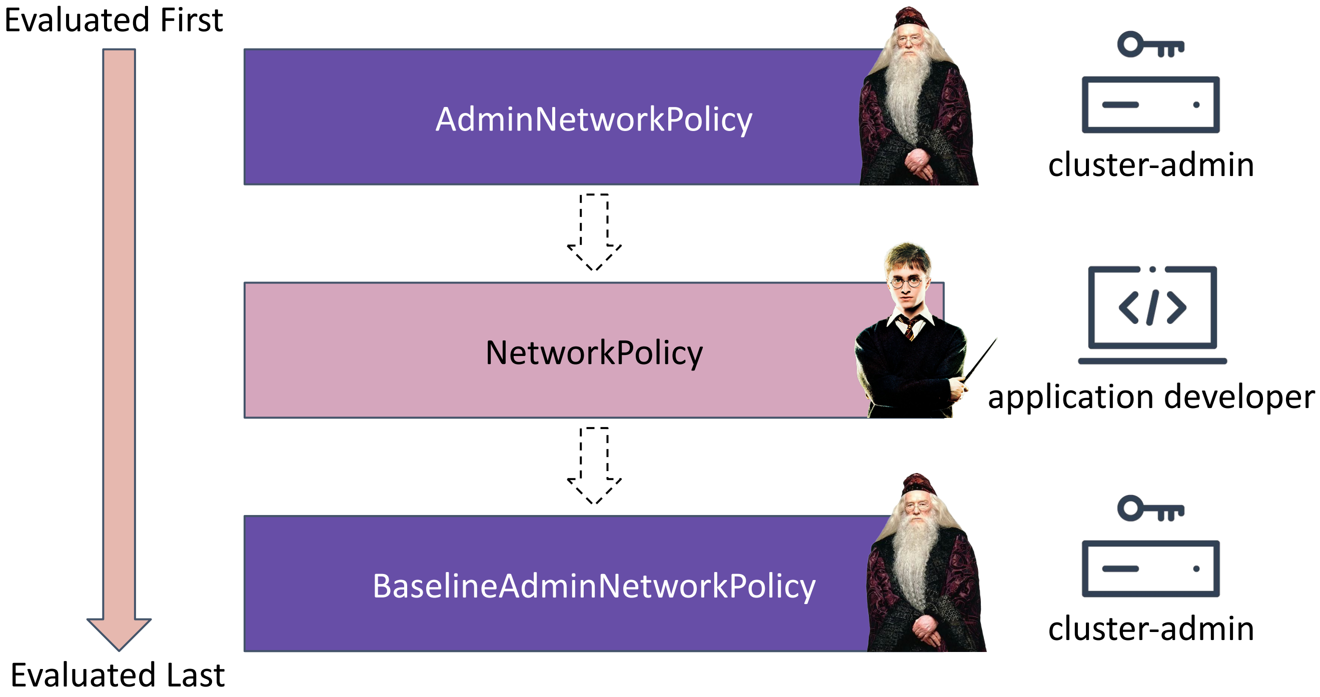
ns: Professors

Cluster Admin

AdminNetworkPolicy

Houses to always **ALLOW** from Professors

AdminNetworkPolicy API: Precedence



Evaluated First

AdminNetworkPolicy

cluster-admin

NetworkPolicy

application developer

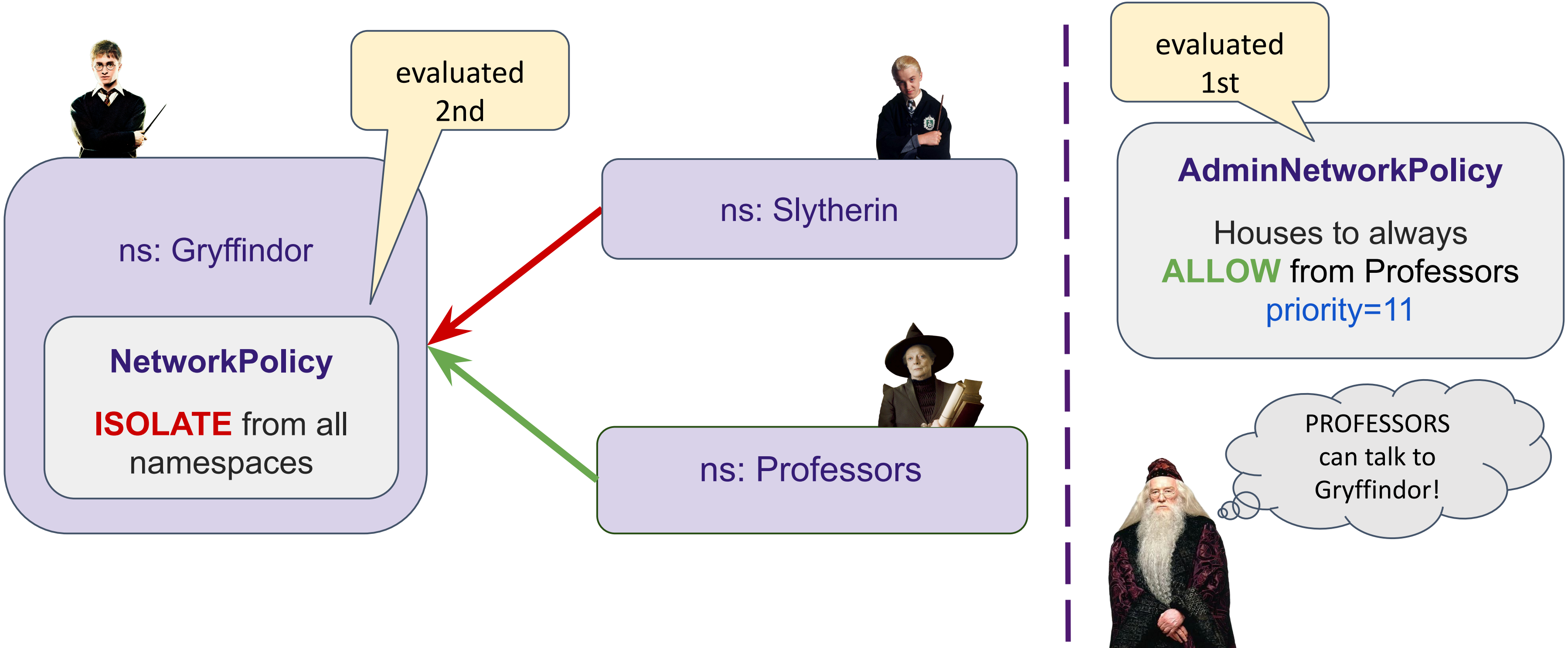
BaselineAdminNetworkPolicy

cluster-admin

Evaluated Last

AdminNetworkPolicy API: Strong ALLOW non-overridable

Cluster Administrators need to enforce security policies that will apply to multiple namespaces in the cluster and cannot be overridden by other cluster personas.



evaluated 2nd

ns: Gryffindor

NetworkPolicy

ISOLATE from all namespaces

ns: Slytherin

ns: Professors

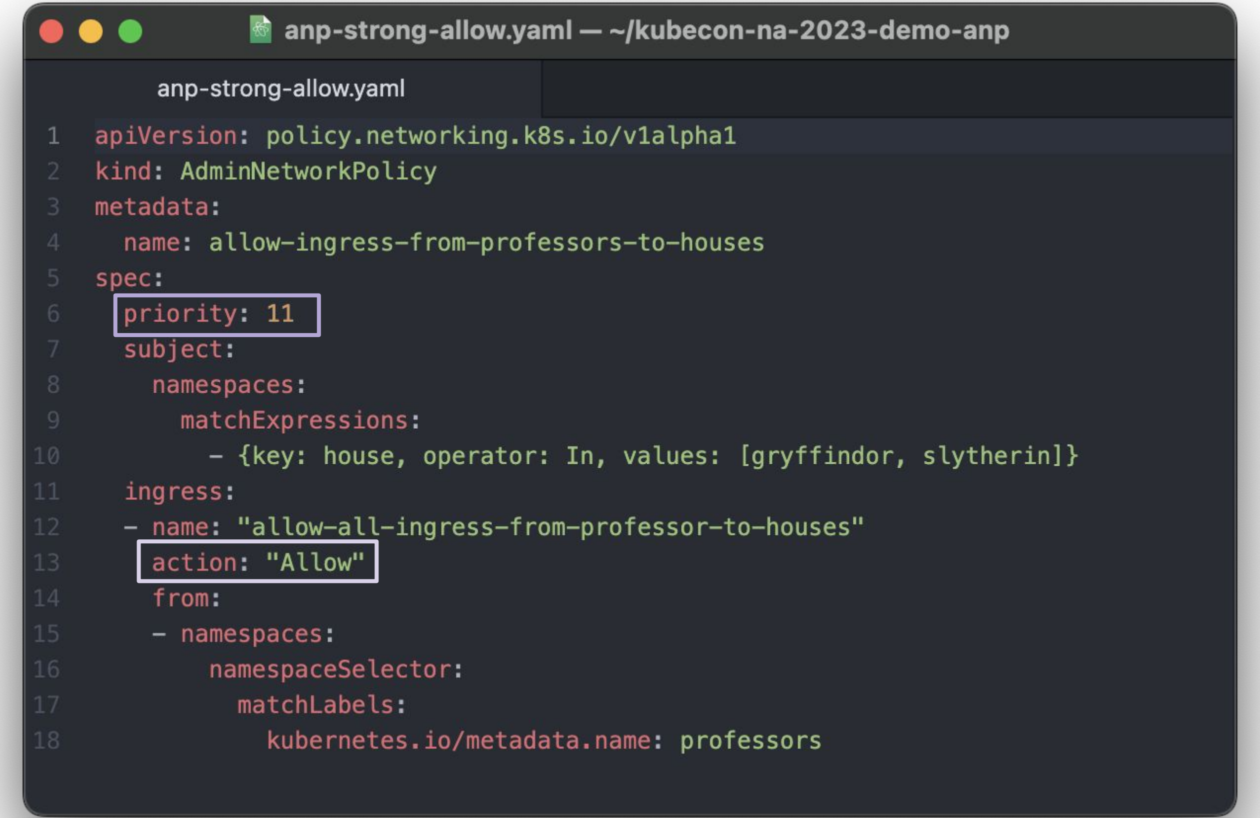
evaluated 1st

AdminNetworkPolicy

Houses to always **ALLOW** from Professors priority=11

PROFESSORS can talk to Gryffindor!

Admin Network Policy Demo: Strong ALLOW



anp-strong-allow.yaml — ~/kubecon-na-2023-demo-anp

anp-strong-allow.yaml

```yaml
apiVersion: policy.networking.k8s.io/v1alpha1
kind: AdminNetworkPolicy
metadata:
  name: allow-ingress-from-professors-to-houses
spec:
  priority: 11
  subject:
    namespaces:
      matchExpressions:
        - {key: house, operator: In, values: [gryffindor, slytherin]}
  ingress:
  - name: "allow-all-ingress-from-professor-to-houses"
    action: "Allow"
    from:
    - namespaces:
        namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: professors
```

AdminNetworkPolicy Demo Part 1 - Strong ALLOW

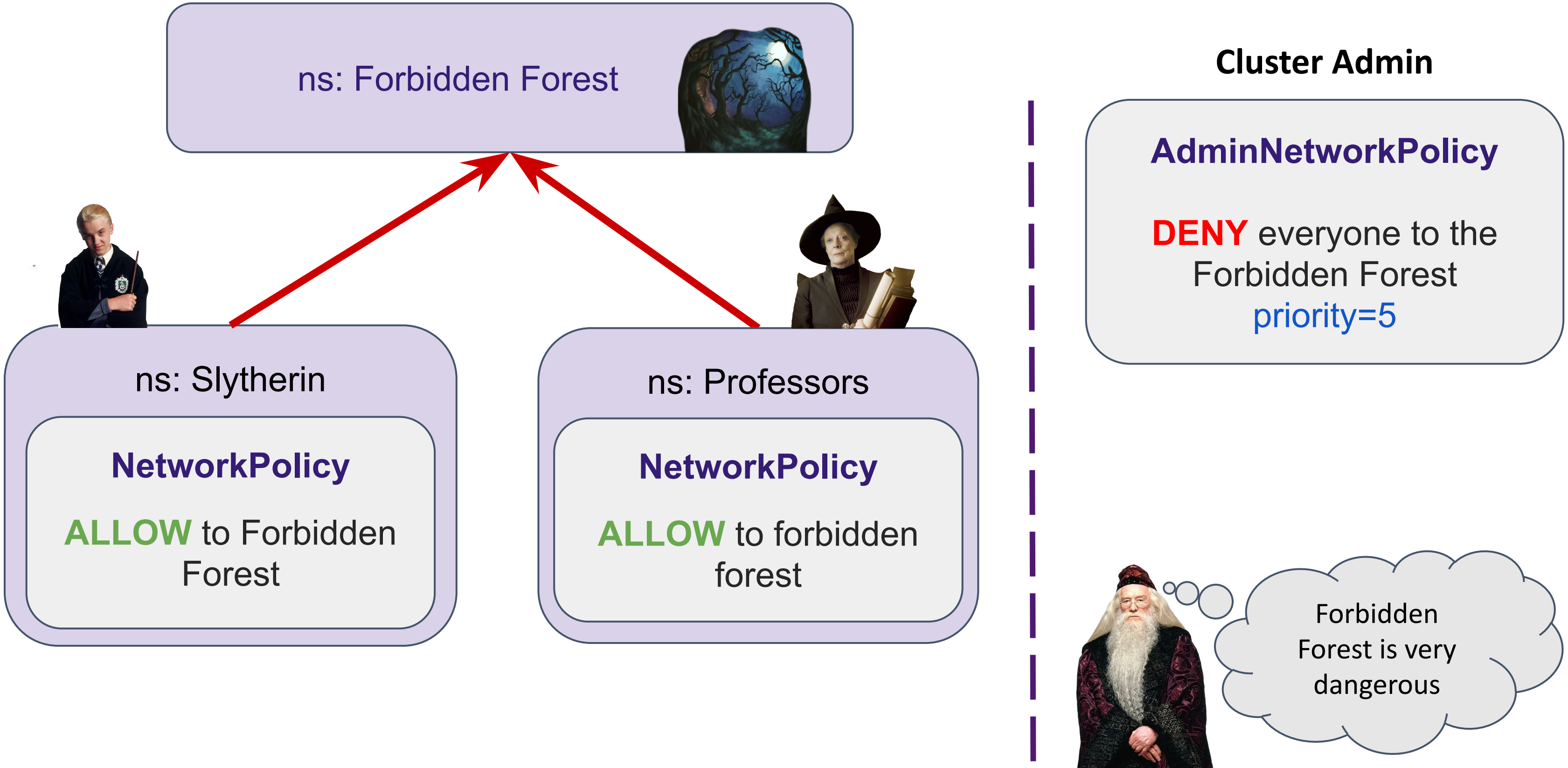
KubeCon | CloudNativeCon
North America 2022

AdminNetworkPolicy

A New Kubernetes-Native API for Comprehensive Cluster-Wide Network Security

Surya Seetharaman, Nadia Pinaeva & Andrew Stoycos, Red Hat
Yang Ding, VMware

AdminNetworkPolicy API: Strong DENY - non-overridable



ns: Forbidden Forest

ns: Slytherin

NetworkPolicy

ALLOW to Forbidden Forest

ns: Professors

NetworkPolicy

ALLOW to forbidden forest

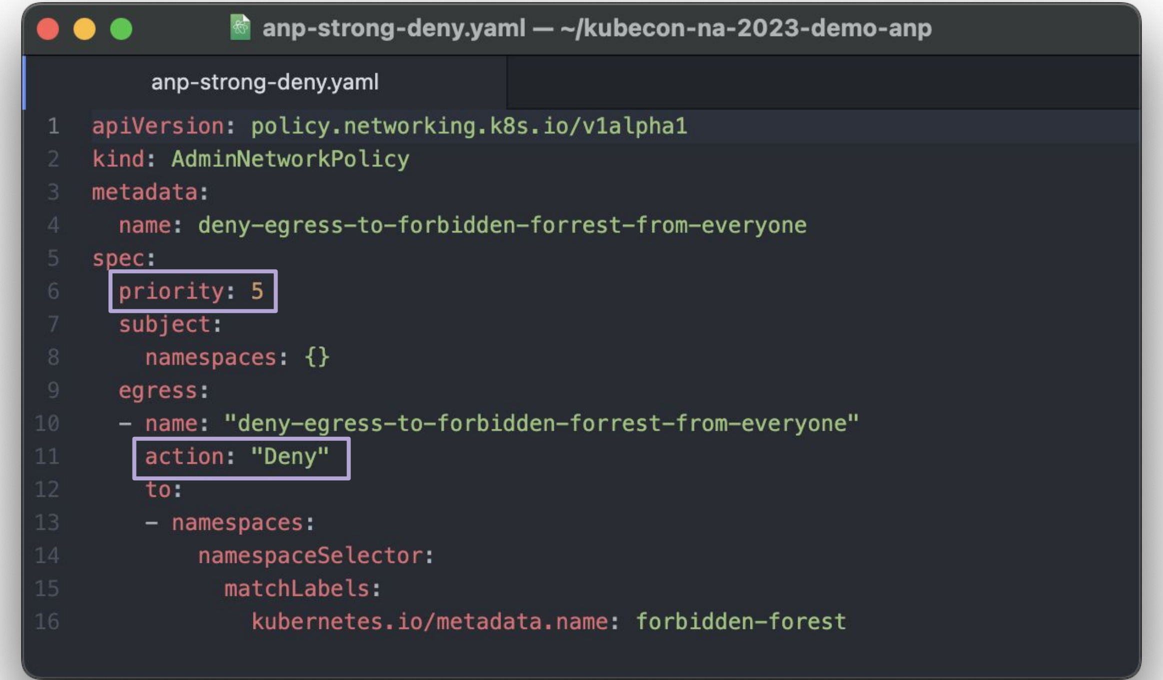
Cluster Admin

AdminNetworkPolicy

DENY everyone to the Forbidden Forest
priority=5

Forbidden Forest is very dangerous

Admin Network Policy Demo: Strong DENY



```yaml
apiVersion: policy.networking.k8s.io/v1alpha1
kind: AdminNetworkPolicy
metadata:
  name: deny-egress-to-forbidden-forrest-from-everyone
spec:
  priority: 5
  subject:
    namespaces: {}
  egress:
  - name: "deny-egress-to-forbidden-forrest-from-everyone"
    action: "Deny"
    to:
    - namespaces:
        namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: forbidden-forest
```

AdminNetworkPolicy Demo Part 1 - Strong DENY

KubeCon | CloudNativeCon

North America 2022

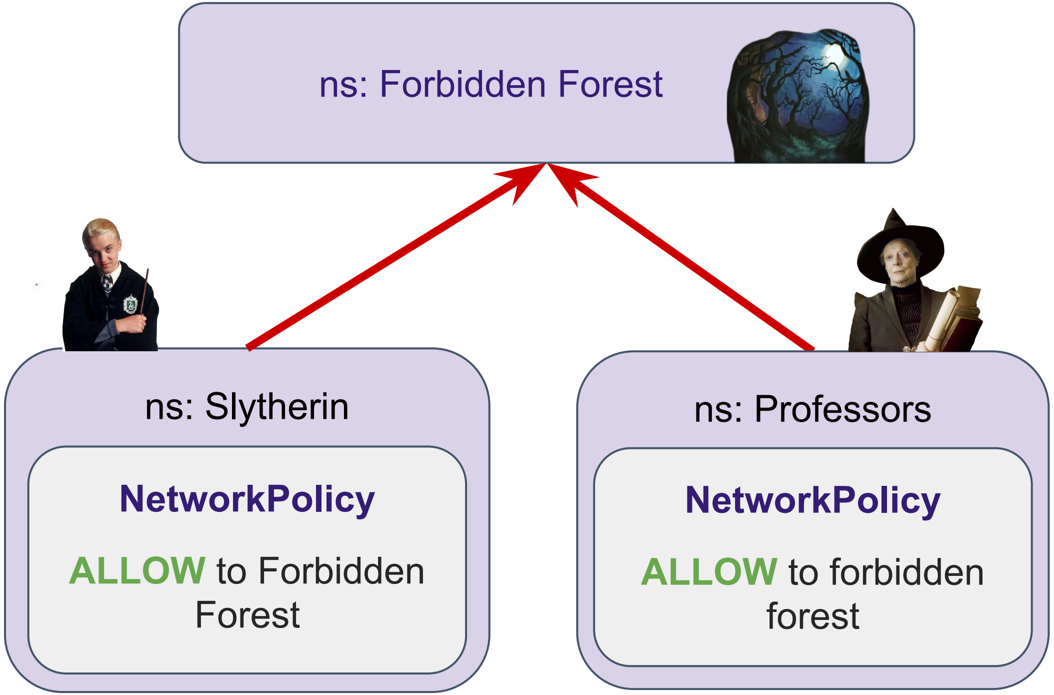
AdminNetworkPolicy

A New Kubernetes-Native API for Comprehensive Cluster-Wide Network Security

Surya Seetharaman, Nadia Pinaeva & Andrew Stoycos, Red Hat

Yang Ding, VMware

AdminNetworkPolicy API: Strong DENY non-overridable



ns: Forbidden Forest

ns: Slytherin

NetworkPolicy

ALLOW to Forbidden Forest

ns: Professors

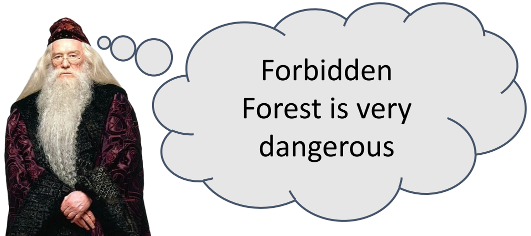
NetworkPolicy

ALLOW to forbidden forest

Cluster Admin

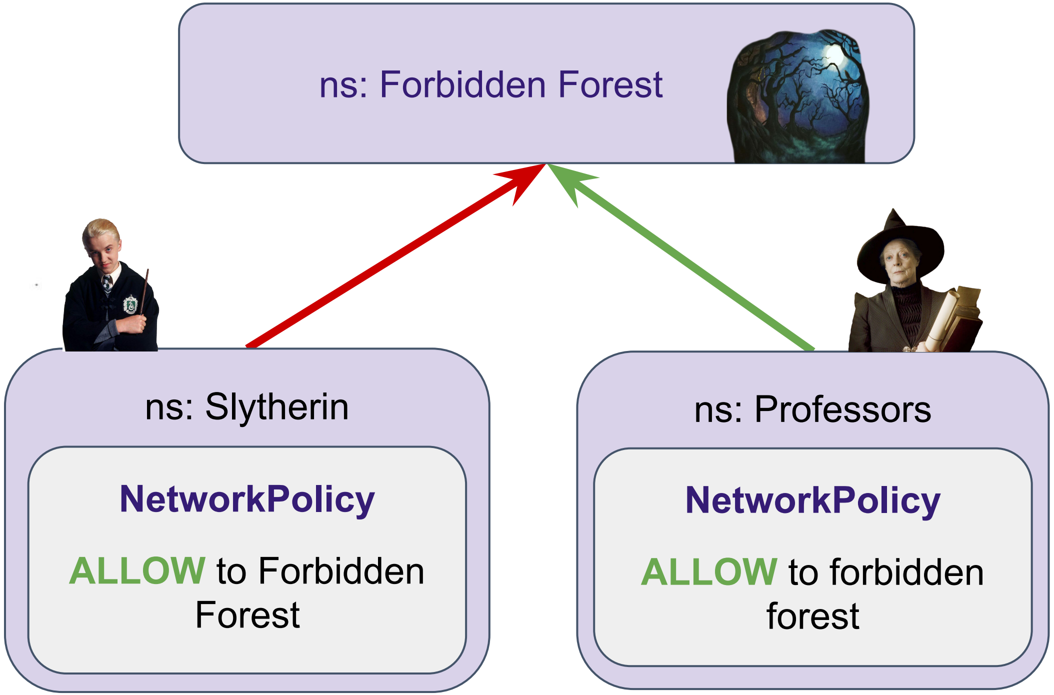
AdminNetworkPolicy

DENY everyone to the Forbidden Forest priority=5



Forbidden Forest is very dangerous

AdminNetworkPolicy API: PASS



ns: Forbidden Forest

ns: Slytherin

NetworkPolicy

ALLOW to Forbidden Forest

ns: Professors

NetworkPolicy

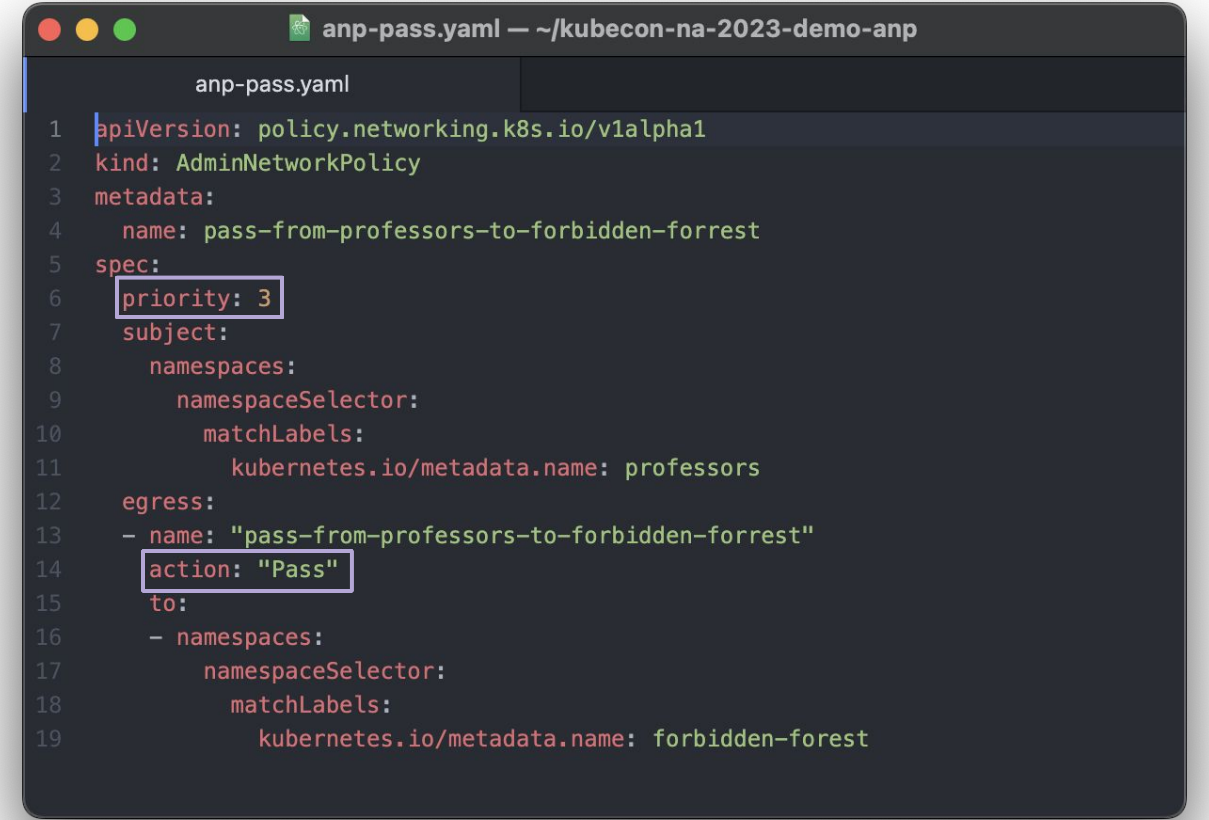
ALLOW to forbidden forest

Cluster Admin

AdminNetworkPolicy
PASS professor to the Forbidden Forest
priority=3

AdminNetworkPolicy
DENY everyone to the Forbidden Forest
priority=5

Admin Network Policy Demo: PASS Action - Delegate to NetPol



```yaml
apiVersion: policy.networking.k8s.io/v1alpha1
kind: AdminNetworkPolicy
metadata:
  name: pass-from-professors-to-forbidden-forrest
spec:
  priority: 3
  subject:
    namespaces:
      namespaceSelector:
        matchLabels:
          kubernetes.io/metadata.name: professors
  egress:
  - name: "pass-from-professors-to-forbidden-forrest"
    action: "Pass"
    to:
    - namespaces:
        namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: forbidden-forest
```

AdminNetworkPolicy Demo Part 2 - PASS to NetPol

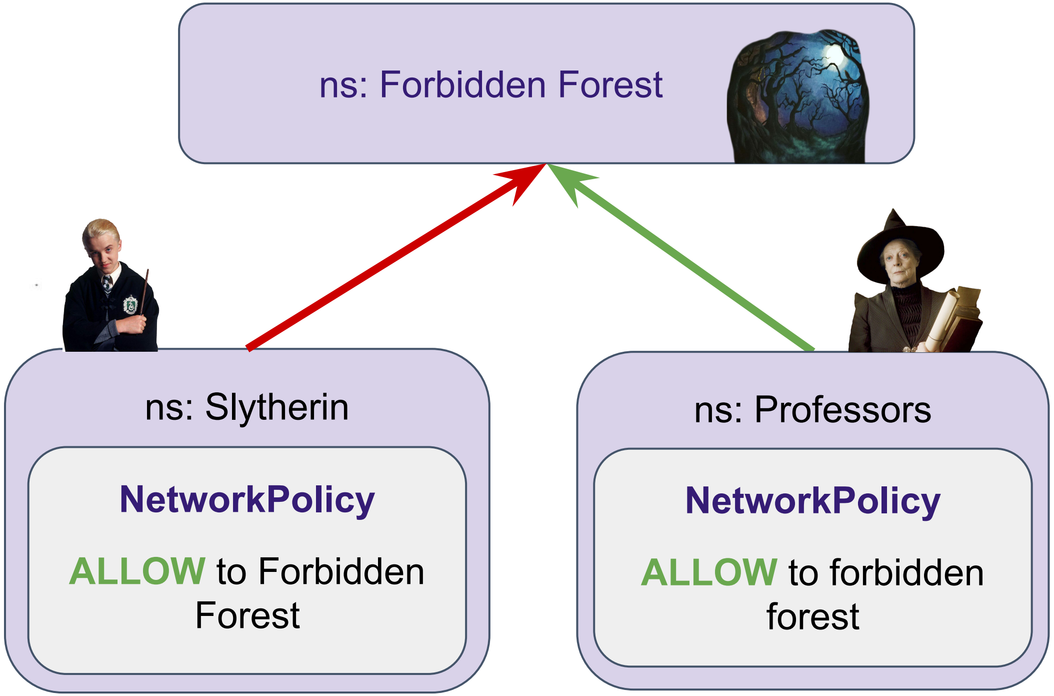
KubeCon | CloudNativeCon
North America 2023

AdminNetworkPolicy

A New Kubernetes-Native API for Comprehensive Cluster-Wide Network Security

Surya Seetharaman, Nadia Pinaeva & Andrew Stoycos, Red Hat
Yang Ding, VMware

AdminNetworkPolicy API: PASS

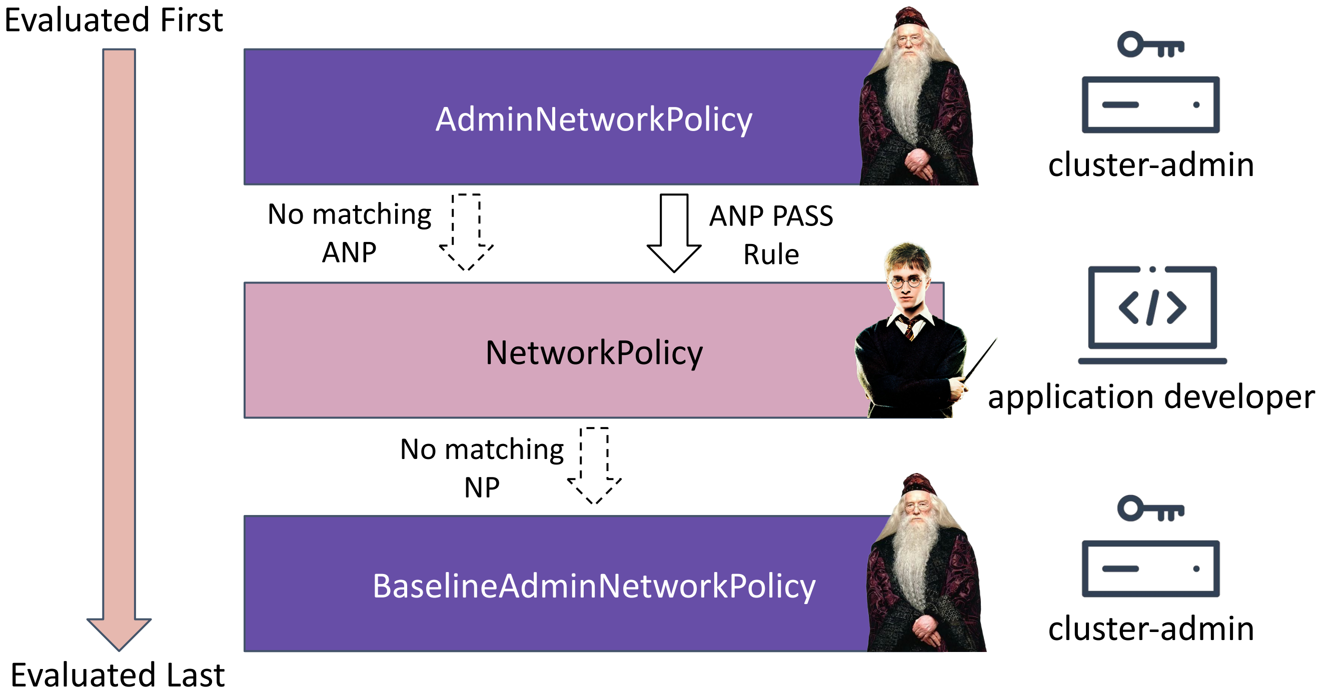


Cluster Admin

AdminNetworkPolicy
PASS professor to the Forbidden Forest
priority=3

AdminNetworkPolicy
DENY everyone to the Forbidden Forest
priority=5

BaselineAdminNetworkPolicy API: Precedence



Evaluated First

AdminNetworkPolicy

cluster-admin

No matching ANP

ANP PASS Rule

NetworkPolicy

application developer

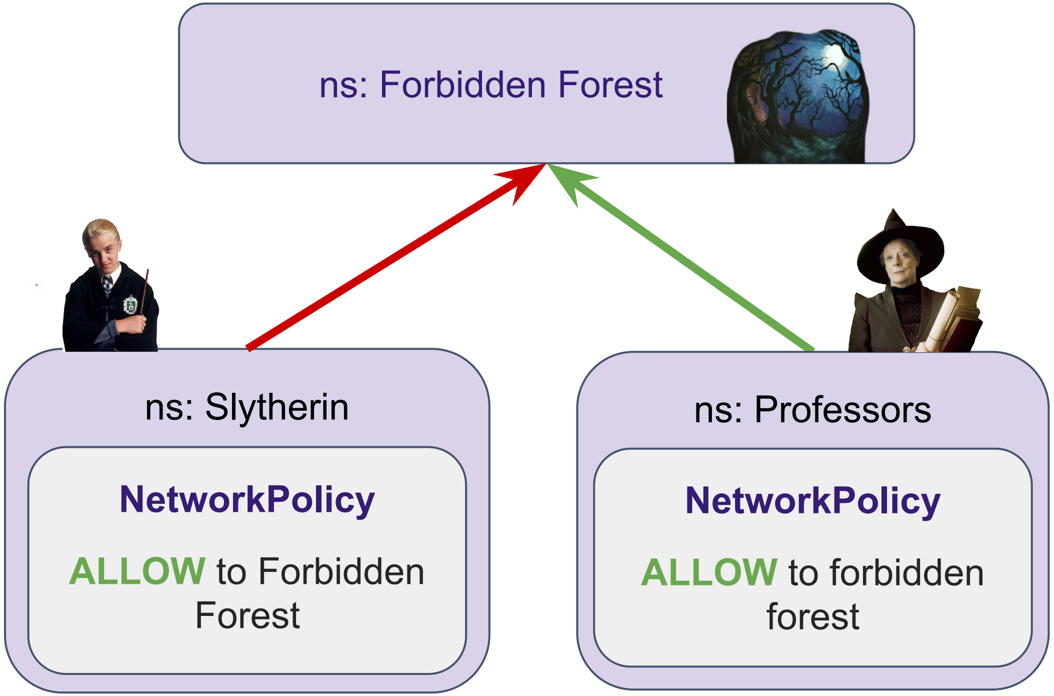
No matching NP

BaselineAdminNetworkPolicy

cluster-admin

Evaluated Last

BaselineAdminNetworkPolicy API



ns: Forbidden Forest

ns: Slytherin

NetworkPolicy

ALLOW to Forbidden Forest

ns: Professors

NetworkPolicy

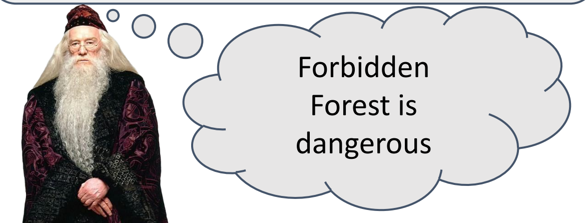
ALLOW to forbidden forest

Cluster Admin

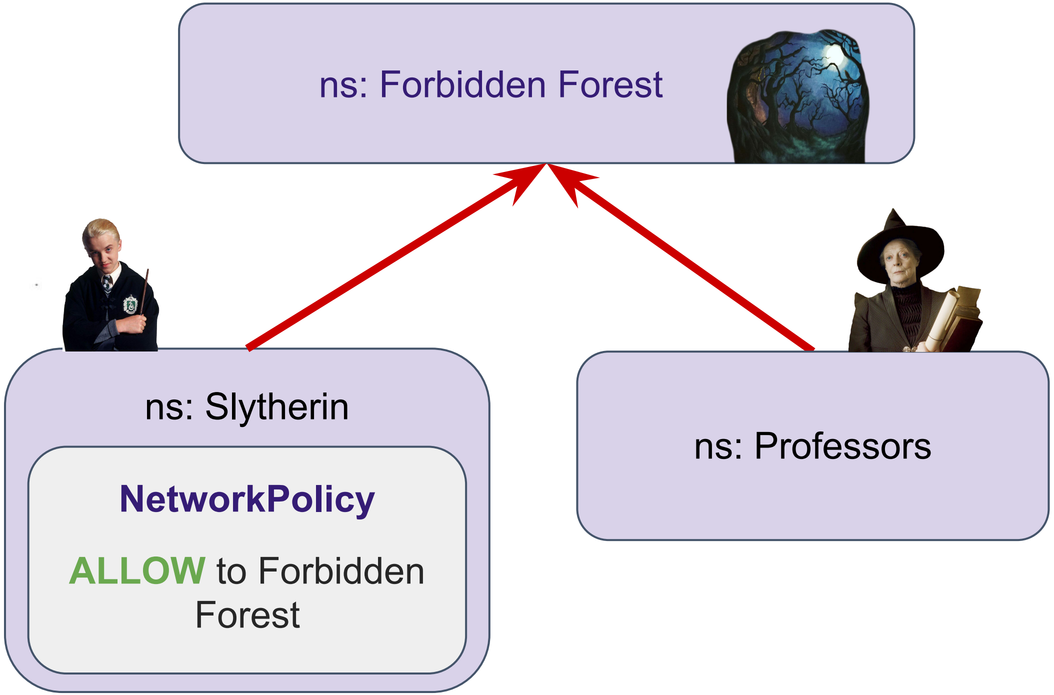
AdminNetworkPolicy
PASS professor to the Forbidden Forest
priority=3

AdminNetworkPolicy
DENY everyone to the Forbidden Forest
priority=5

BaselineAdminNetworkPolicy
DENY to everywhere



BaselineAdminNetworkPolicy API



ns: Forbidden Forest

ns: Slytherin

NetworkPolicy

ALLOW to Forbidden Forest

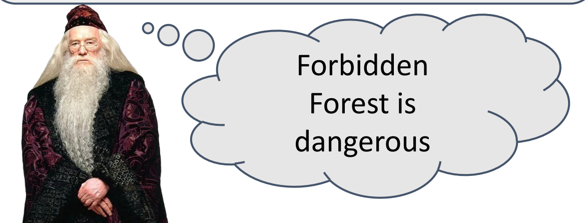
ns: Professors

Cluster Admin

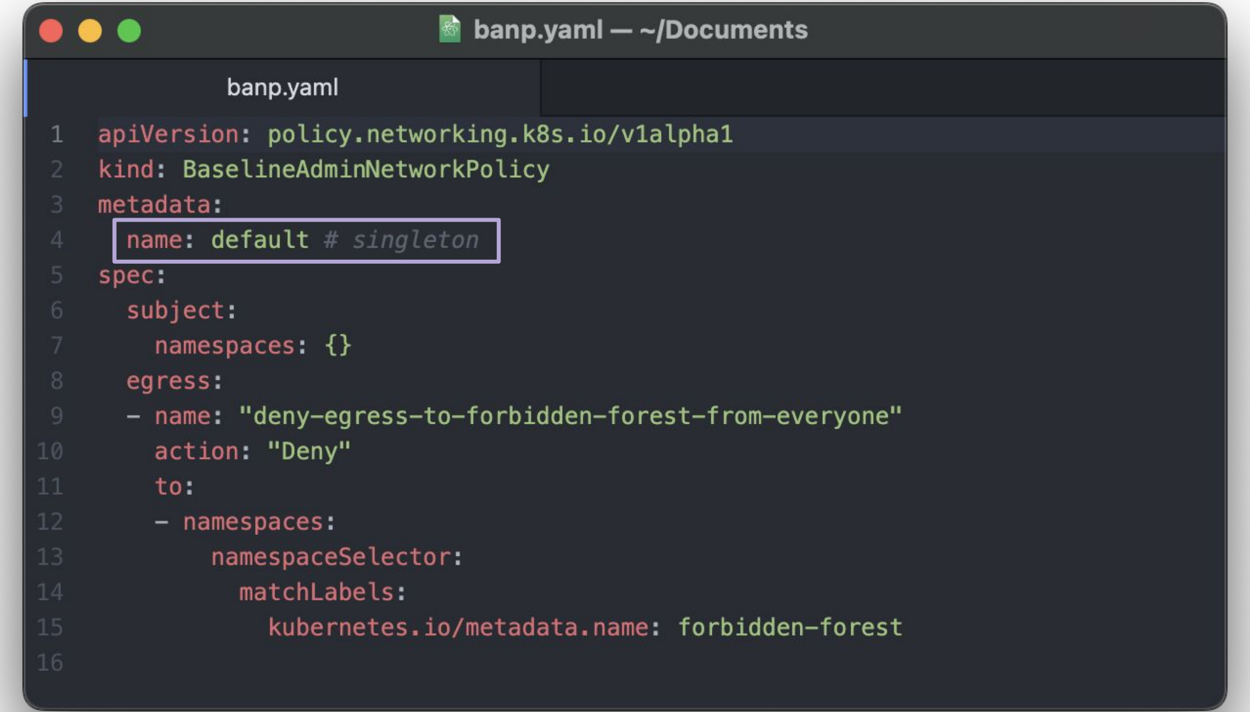
AdminNetworkPolicy
PASS professor to the Forbidden Forest
priority=3

AdminNetworkPolicy
DENY everyone to the Forbidden Forest
priority=5

BaselineAdminNetworkPolicy
DENY to everywhere



BaselineAdminNetworkPolicy API



```yaml
apiVersion: policy.networking.k8s.io/v1alpha1
kind: BaselineAdminNetworkPolicy
metadata:
  name: default # singleton
spec:
  subject:
    namespaces: {}
  egress:
  - name: "deny-egress-to-forbidden-forest-from-everyone"
    action: "Deny"
    to:
    - namespaces:
        namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: forbidden-forest

```

AdminNetworkPolicy Demo Part 2 - BANP

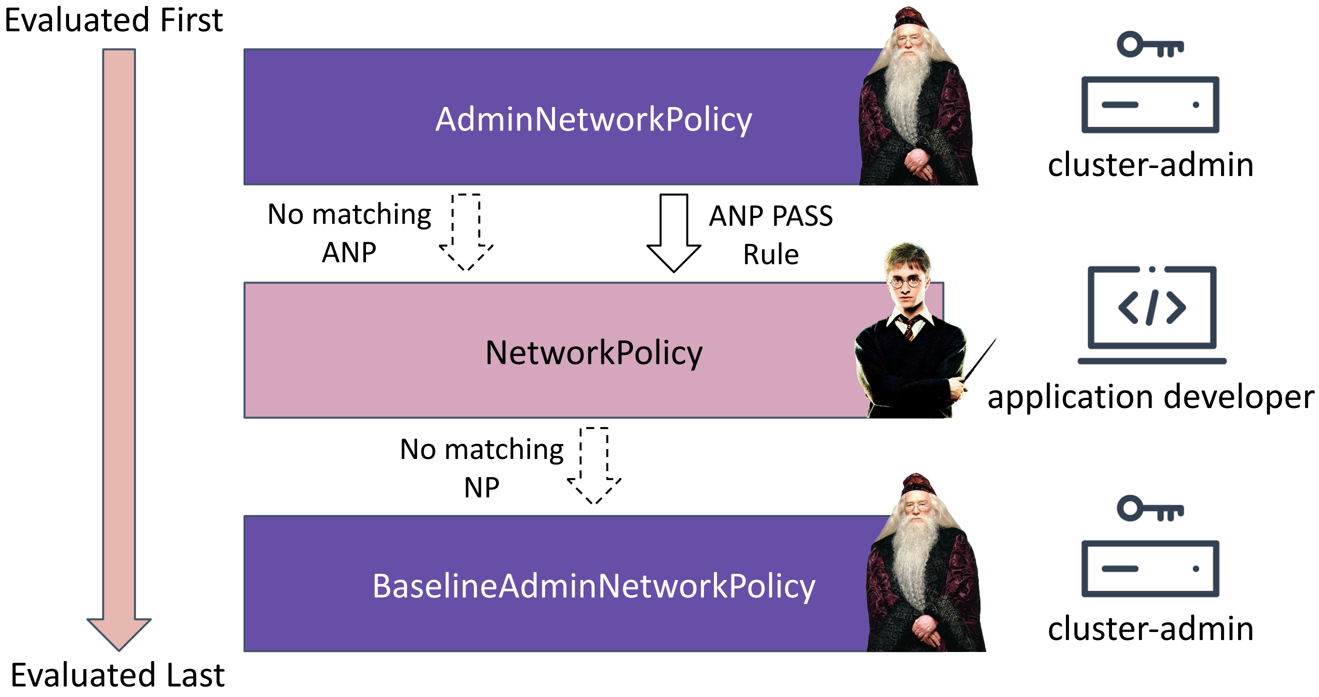
KubeCon CloudNativeCon
North America 2023

AdminNetworkPolicy

A New Kubernetes-Native API for Comprehensive Cluster-Wide Network Security

Surya Seetharaman, Nadia Pinaeva & Andrew Stoycos, Red Hat
Yang Ding, VMware

Key Takeaways!



Evaluated First

AdminNetworkPolicy

cluster-admin

No matching ANP

ANP PASS Rule

NetworkPolicy

application developer

No matching NP

BaselineAdminNetworkPolicy

cluster-admin

Evaluated Last

Get Involved!

Getting Involved in the project!

- **Level 1: Completely new to K8s and Don’t know where to start!?**
  - Checkout the K8s contributor guide!
  - Read the Network Policy V1 documentation
  - Read the AdminNetworkPolicy KEP

- **Level 2: Familiar with the basics but still unsure where to dive in?**
  - Read though our documentation at https://network-policy-api.sigs.k8s.io/ please open issues I am sure there are documentation bugs we’ve yet to find 👿
  - Checkout our help wanted and good first issues
  - Review any of the open PRs

- **Level 3: Want more features! Want more implementations! Want more feedback!**
  - Read about our NPEP (Network Policy Enhancement Proposal) process
  - Propose a new NPEP with an issue.

kubernetes-sigs/network-policy-api

#sig-network-policy-api

https://network-policy-api.sigs.k8s.io

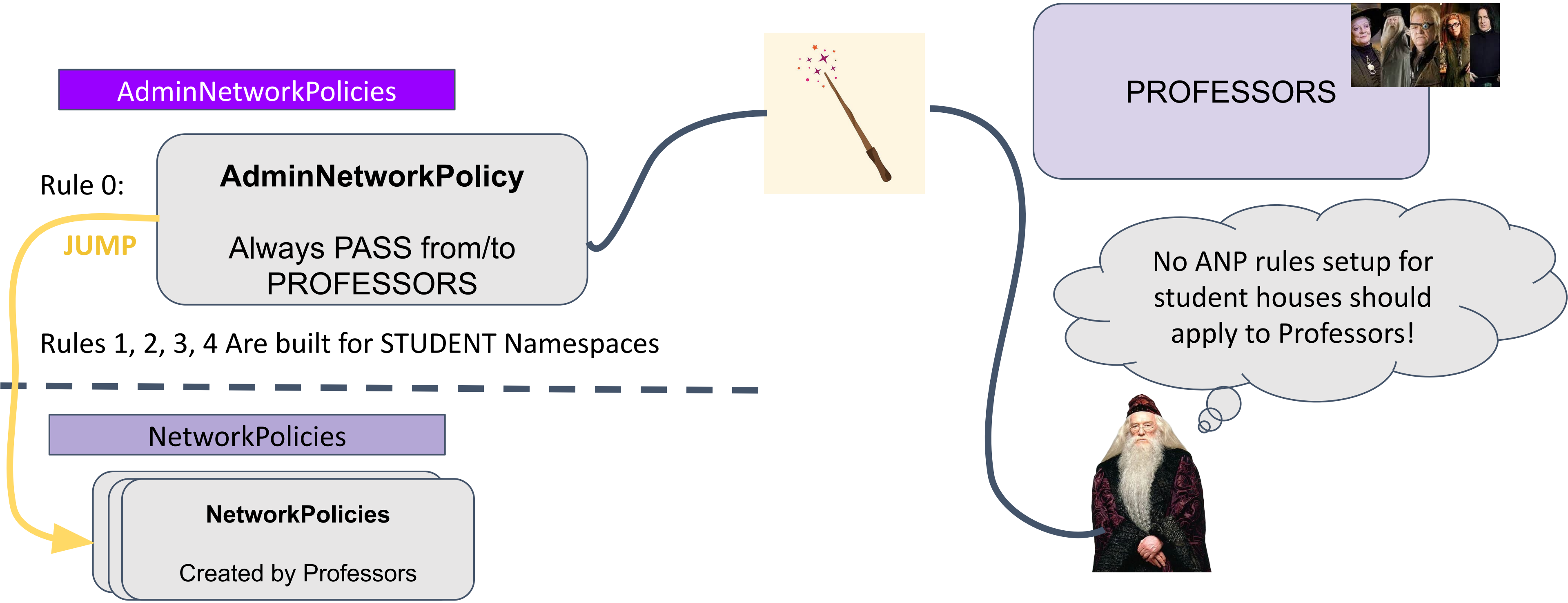
Thank You!

Questions?

**Please scan the QR Code above
to leave feedback on this session**

AdminNetworkPolicy: Pass

Cluster Administrators need to enforce security policies that will allow a single namespace to be an exception to any ANP rules.



AdminNetworkPolicies

Rule 0:

AdminNetworkPolicy

Always PASS from/to PROFESSORS

JUMP

Rules 1, 2, 3, 4 Are built for STUDENT Namespaces

NetworkPolicies

NetworkPolicies

Created by Professors

PROFESSORS

No ANP rules setup for student houses should apply to Professors!