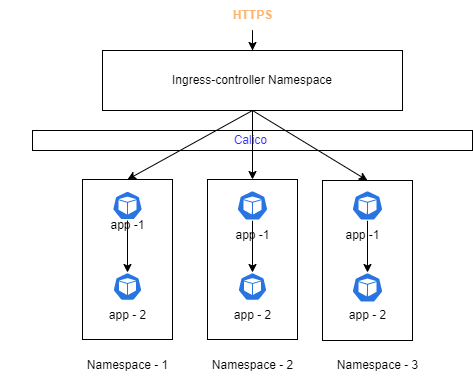
# AKS Network Policies

Network Policies is a Kubernetes feature to configure how groups of pods are allowed to communicate with each other and other network endpoints. In other words, it creates firewalls between pods running on a Kubernetes cluster. By default, Kubernetes does not restrict traffic between pods running inside same cluster. This means any pod can connect to any other pod as there are no firewalls controlling the intra-cluster traffic. Network Policies give you a way to declaratively configure which pods are allowed to connect to each other. Example Use Cases

[DENY all traffic from other namespaces](https://github.com/ahmetb/kubernetes-networkpolicy-tutorial/blob/master/04-deny-traffic-from-other-namespaces.md)



**AKS Default Network Policy**

* The Kubernetes Namespace Network policy allows communication between pods in the same namespace and it denies pods to communicate to another namespaces.
* The Kubernetes Network Namespace policy allows Ingress (inbound) traffic only from Ingress-controller namespace. All Egress (outbound) traffics are allowed .
* The Kubernetes Network Namespace policy allows Ingress traffic from other namespaces only if the namespace is explicitly allowed in the network policy .
* Default Network policy will be implemented as part of namespace creation through pipeline. HaCT team allows application team to do the changes in the network policies ,but they cannot remove the network policies .

**Global Network Policy**

* All HaCT managed clusters have a global network policy in the cluster level, that blocks all inbound communication by default into the application namespaces.
* This enforces the definition of a namespace network policy that allows communication from the ingress controller namespace. Hence application teams cannot just delete the namespace network policy to allow all traffic.
* Global Network Policy is fully managed by HaCT team

**Below is the default network policy Yaml file.**

apiVersion: [networking.k8s.io/v1](http://networking.k8s.io/v1)

kind: NetworkPolicy

metadata:

name: kubernetes-namespace-network-policy

namespace: #{ applicablenamespace}#

spec:

podSelector:

matchLabels:

policyTypes:

- Ingress

- Egress

ingress:

- from:

- podSelector: {}

- from:

- namespaceSelector:

matchLabels:

environment: ingresscontroller