01. Blacklist policies using source and destination globalnetworksets
02. Blacklist ports - 20:21, 23, 25, 69, 111
04. External access whitelist/blacklist per tenant/application/environment
03. Compliance controls - Pass policies per environment/application/tenant

01. DNS-ALLOW-ALL
02. Access to private repo based on DNS policies and ports
03. Access to external tools based on globalnetworksets (logging, datalake)
04. Access for cluster tools (monitoring,logging, security etc.)
05. Access to Git repo/GitOps tools using DNS policies
06. Policies for ingress controller
07. Access to API Service

01. Policies to permit traffic within applications/namespaces if required

01. Granular/Micro-segmentation policies per deployment

01. Global default deny
02. Default deny per namespace
03. Failsafe policies

security tier

- threatfeed
- insight-appdev (QA)
- insight-appdev (DEV)
- security-default-pass

security team

01. Limit allow and pass global network policies to the security and platform tier
02. Default pass in the bottom of the tier to ensure that subsequent tiers are evaluated for policies since global network policies match all endpoints

01. For further control you can specify the namespaces in the default pass

platform tier

- dns-allow-all
- load-balancer
- kube-system
- platform-default-pass

platform team

application tier

- [dep1]-iGuard-Allow
- implicit Deny for selected endpoints

platform team

Note that there is an implicit deny for the selected endpoints in each policy in the tier.

appsec tier

- [dep1]-tyk-frontend
- [dep2]-tyk-middle
- [dep3]-tyk-backend
- implicit Deny for selected endpoints

App developers

default tier

- [tyk]-default-deny
- [iGuard]-default-deny
- [new-app]-default-deny
- failsafe-allow
- global-deny

Default deny per namespace and failsafe allows during policy staging and testing

security team

```
apiVersion: projectcalico.org/v3
kind: GlobalNetworkPolicy
metadata:
name: deny-app-policy
spec:
namespaceSelector: has(projectcalico.org/name) && projectcalico.org/name not in {"kube-system", "calico-system", "tigera-system"}
types:
- Ingress
- Egress
egress:
# allow all namespaces to communicate to DNS pods
- action: Allow
protocol: UDP
destination:
selector: 'k8s-app == "kube-dns"'
ports:
- 53
```

Omit critical namespaces from the global deny policy

- global network policies
- namespace scope network policies
- pass and deny rules inside policy
- only pass rules inside policy
- only allow rules in policy
- only deny rules inside policy

HOOPP - Calico Cloud Security Policy Framework

Prepared by: Aadhil A. Majeed (Tigera) - Solutions Architect - Customer Success
Date - 08/26/2022