InGuardians™

KUBERNETES ATTACK & DEFENSE REAL GENIUS EDITION

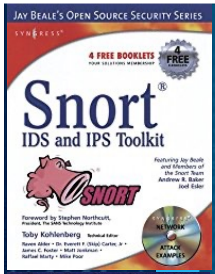
Jay Beale, CEO, CTO

@jaybeale / @InGuardians

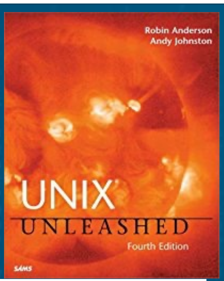
Wild West Hackin' Fest – Way West

June 16, 2021

Graphical Bio

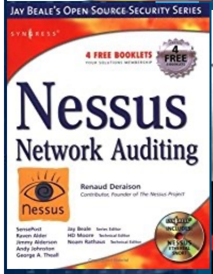

Jay Beale's Open Source Security Series

Snort IDS and IPS Toolkit

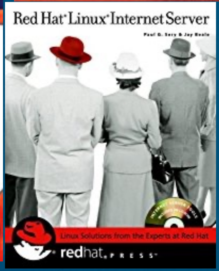

UNIX Unleashed

Fourth Edition

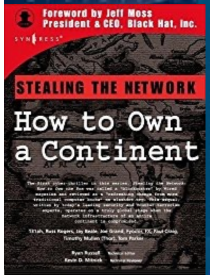
Robin Anderson, Andy Johnston


Jay Beale's Open Source Security Series

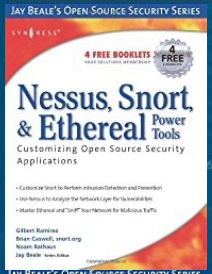
Nessus Network Auditing


Red Hat Linux Internet Server

redhat press

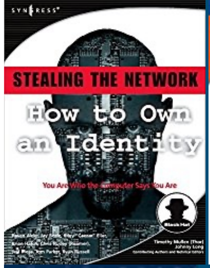

Foreword by Jeff Moss President & CEO, Black Hat, Inc.

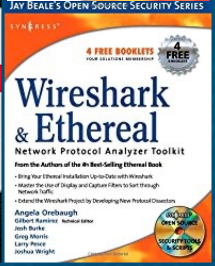
Stealing the Network: How to Own a Continent


Jay Beale's Open Source Security Series

Nessus, Snort, & Ethereal Power Tools

Customizing Open Source Security Applications


Stealing the Network: How to Own an Identity


Jay Beale's Open Source Security Series

Wireshark & Ethereal Network Protocol Analyzer Toolkit

black hat

A PURPLE TEAM VIEW: ATTACKING AND DEFENDING LINUX, DOCKER AND KUBERNETES

JAY BEALE, INGUARDIANS | JULY 31-AUGUST 3

BASTILLE

http://bastille-linux.sourceforge.net/

CAN SEC WEST

Information Security

Going the Distance

CIS. Center for Internet Security

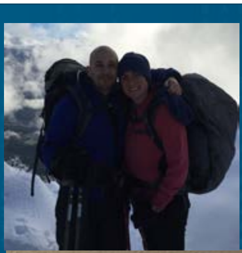
DEFCON

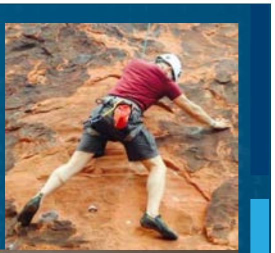
toorcon

SecurityFocus™

OVAL

SANS





InGuardians™ Red Team

InGuardians™

What Are We Going to See?

Attack

Multi-cluster Attack Scenario

Abusing Kube2IAM, kops and AWS STS Assume Roles

Integrating CVE-2020-8554

Defense Considerations

CVE-2020-8554 Mitigations

Stronger Alternatives to Kube2IAM

Admission Control

Service Meshes

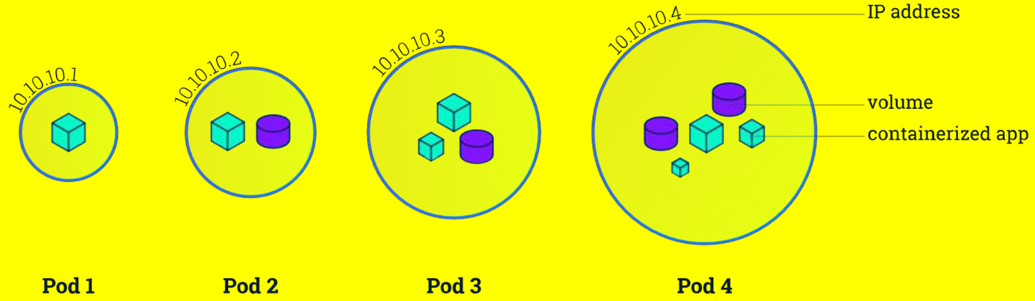
Quick Review: What Does Kubernetes Do?

- Bin Packing (Assigning work to machines)
- Self Healing
- Horizontal Scaling
- Service Discovery and Load Balancing
- Secret and Configuration Management
- Storage Orchestration
- Automated Rollouts and Rollbacks
- A/B Testing

Software-defined Datacenter via Container Orchestration

Refresher/Intro: Pods

Pods are the smallest unit of compute in Kubernetes



All containers in a pod share an IP address and may share the volumes defined in that pod.

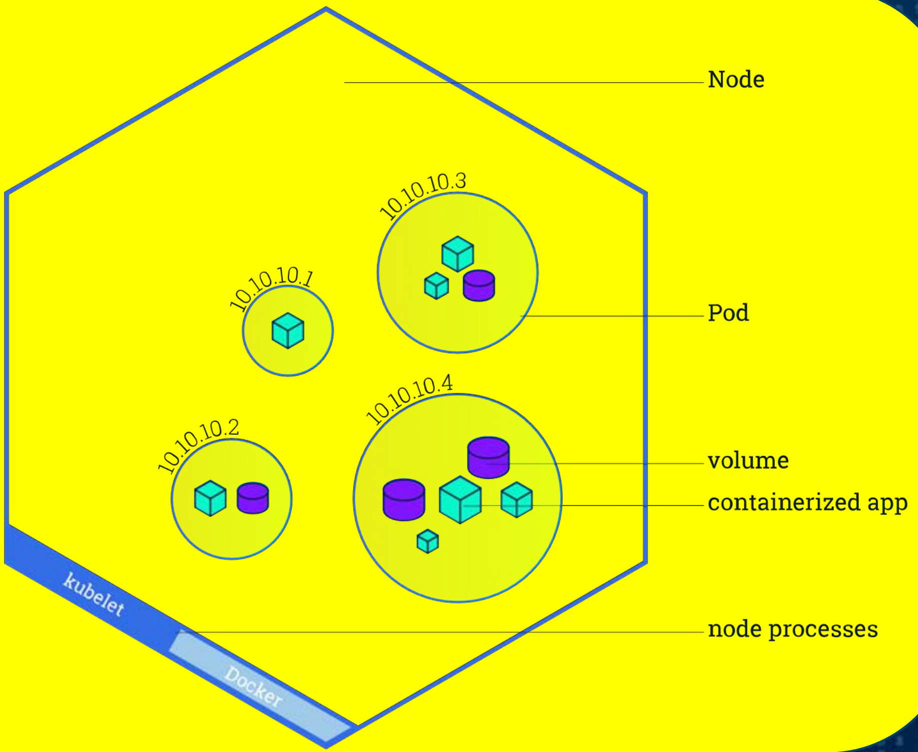
Refresher/Intro: Nodes

Nodes run:

- **Kubelet**
- **Container Runtime**

(Docker, containerd, ...)

- **Kube-Proxy**



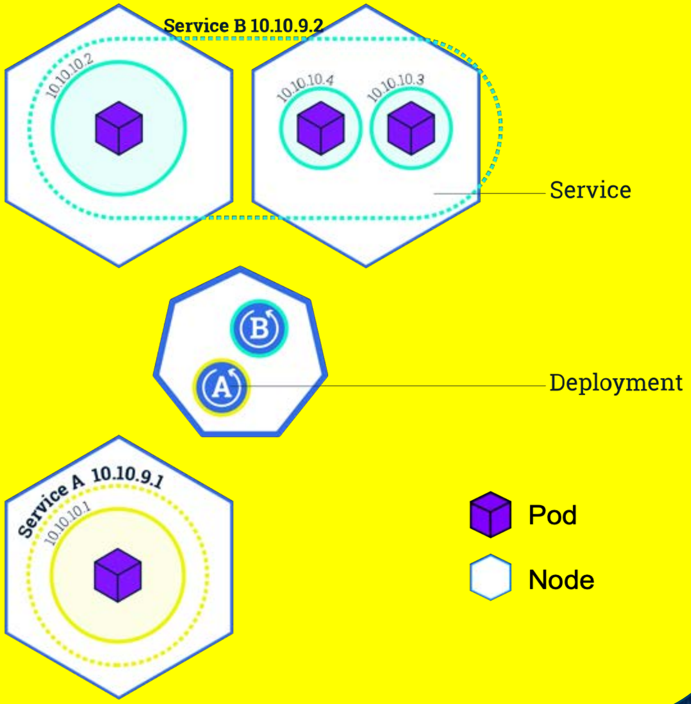
Refresher/Intro: Services (Load Balancers)

Service: a load balancer

A service creates:

- **a DNS name**
- **IP address**
- **port**

These redirect traffic they receive to the pods that match the labels specified by the Service's description.



Let's See the Demo!

Themed on Real Genius

Watch the Scene

https://www.youtube.com/watch?v=ZnDAxtCRsIU

Defending Against Each Stage in the Attack

How do we defend against each of these steps?

- Monkey in the Middle (MitM) Attack on Outgoing Traffic
- Privileged and HostNetwork Pods
- Kops S3-based State Store
- STS Assume-Role / Kube2IAM Design Weakness

Defending Against the Outgoing MitM

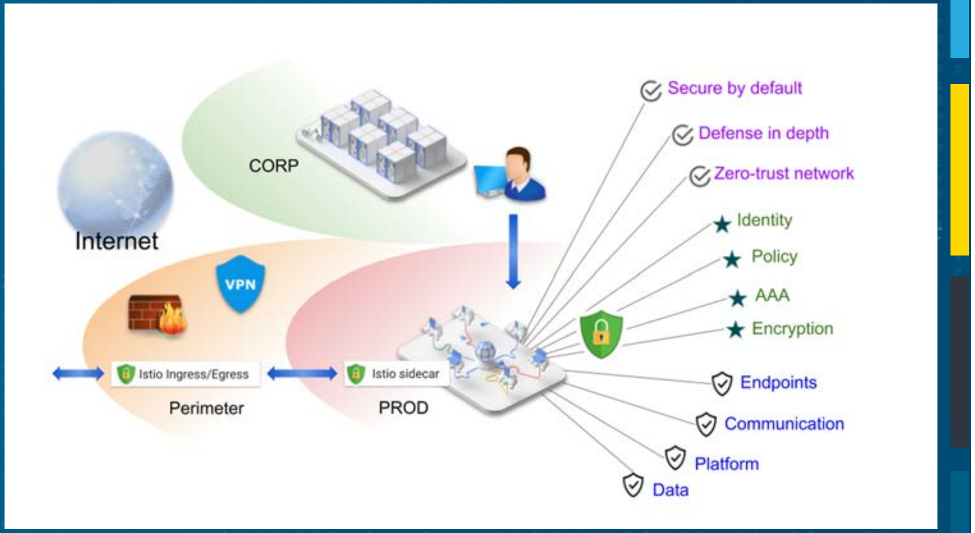
- The Kubernetes project created a webhook to create an IP address allow-list that all ExternalIP services are checked against: https://bit.ly/2TyX17c

- You can create an OPA Gatekeeper policy.
- Sample Gatekeeper template that creates an Allow List: https://bit.ly/3q5Jhgj

Defense: Service Meshes (Istio)

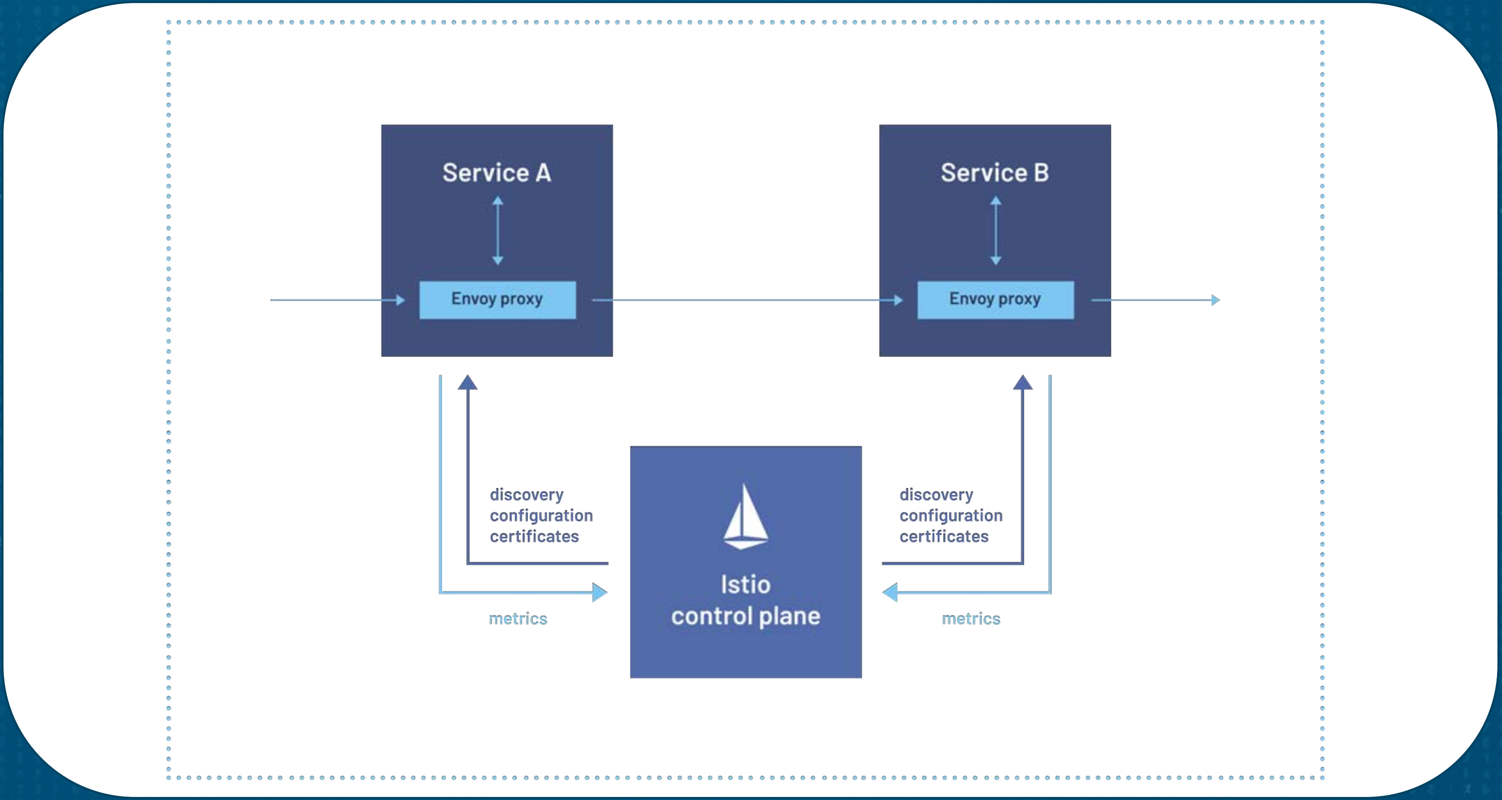
- Service meshes bring encryption, service authentication, traffic control and observation to Kubernetes, among other features.

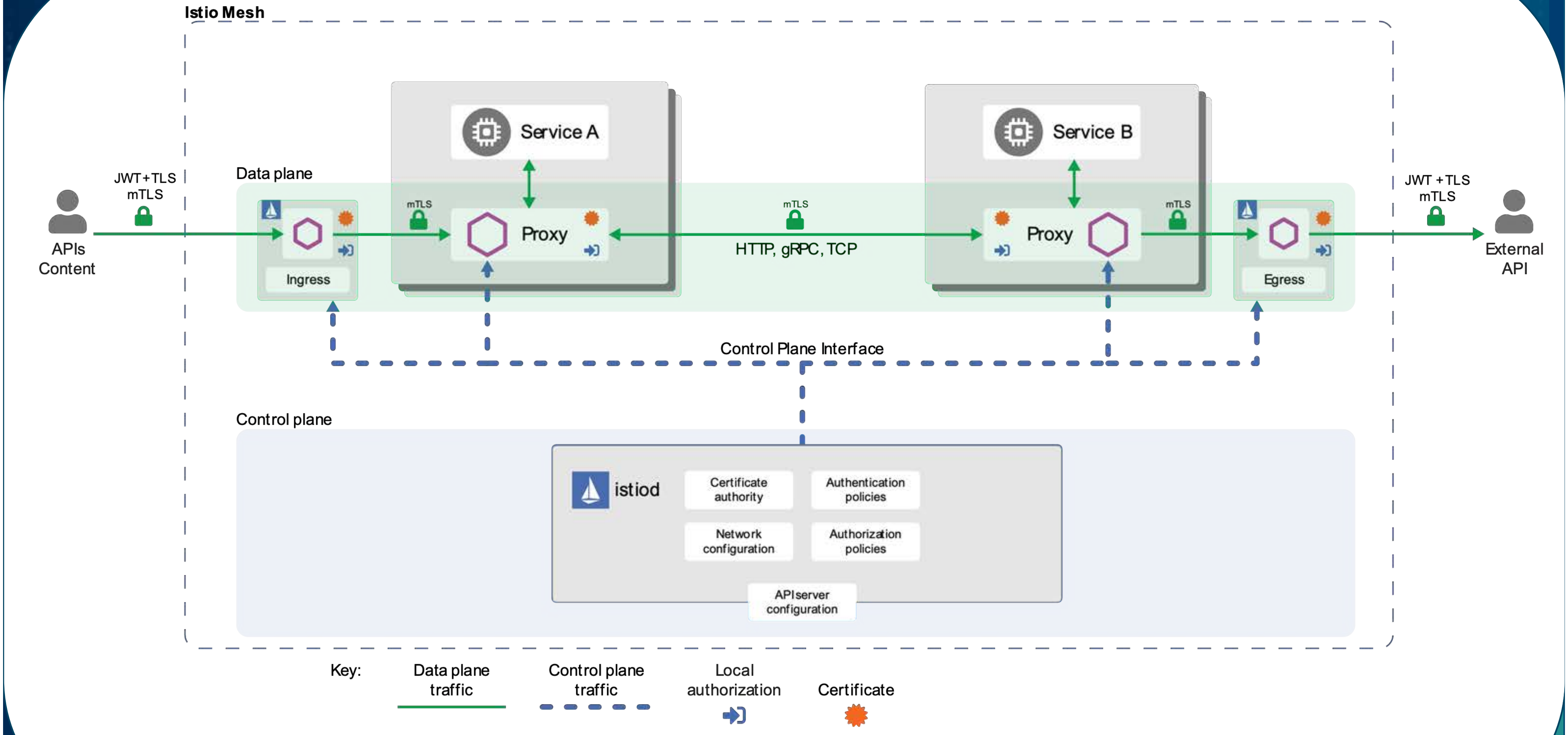
- Istio is one example, wherein each pod is given a sidecar proxy through which all network traffic will flow.



InGuardians™

Istio’s Envoy Proxy Containers Mediate All Traffic





Istio Mesh

APIs Content

JWT+TLS
mTLS

Data plane

Ingress

mTLS

Service A

Proxy

mTLS

HTTP, gRPC, TCP

Service B

Proxy

mTLS

Egress

JWT +TLS
mTLS

External API

Control Plane Interface

Control plane

istiod

Certificate authority

Authentication policies

Network configuration

Authorization policies

APIserver configuration

Key:

Data plane traffic

Control plane traffic

Local authorization

Certificate

Defense for Privileged/HostNetwork Pods: Admission Control

You have multiple options:

- Open Policy Agent Gatekeeper
- K-rail
- kyverno
- Pod Security Policies (deprecated in v1.21, removed in 1.25)

Pod Admission Control Links

- Pod Security Standards Policies
  - https://kubernetes.io/docs/concepts/security/pod-security-standards/
- Open Policy Agent Gatekeeper
  - https://github.com/open-policy-agent/gatekeeper
- K-rail
  - https://github.com/cruise-automation/k-rail
- Kyverno
  - https://github.com/kyverno/kyverno

Kops S3 State Store Defenses

- Keep the state store's bucket inaccessible to all but a few IAM principals.
- Keep the state store in a local file.

Assume-Role / Kube2IAM Defenses

- Replace Kube2IAM with KIAM, AWS’s native identity management, or another option.
- Ensure the node isn’t allow to transition to a role that can read dangerous S3 buckets: default deny vs default allow.

Come Visit InGuardians Booth – Physical and Discord

- Drawing to Win a Laptop Running the Bust-a-Kube Kubernetes cluster: online and booth
- Hack It to Win It: Raspberry Pi Kubernetes Cluster:

  (physical booth only, THURSDAY 10 am – 6 pm)

- Come talk Kubernetes and InfoSec with us at our Booth!
- Booth Talks And Demos on Thursday – announced on Discord
- Free Kubernetes Attack and Defense Virtual Lab in July – register via the laptop drawing
- Come find InGuardians on Discord!

Check out our learning cluster!

https://BustaKube.com

Help Develop Peirates!

https://inguardians.com/peirates/