Building an open source IDS/IPS service on AWS with Suricata

Adam Palmer, Specialist Solution Architect, Networking

www.linkedin.com/in/adamlewispalm

Nick Coval, GTM Networking Specialist

https://www.linkedin.com/in/nickcoval/

SURICON BOSTON 2021

OISF

October 20 - 22, 2021

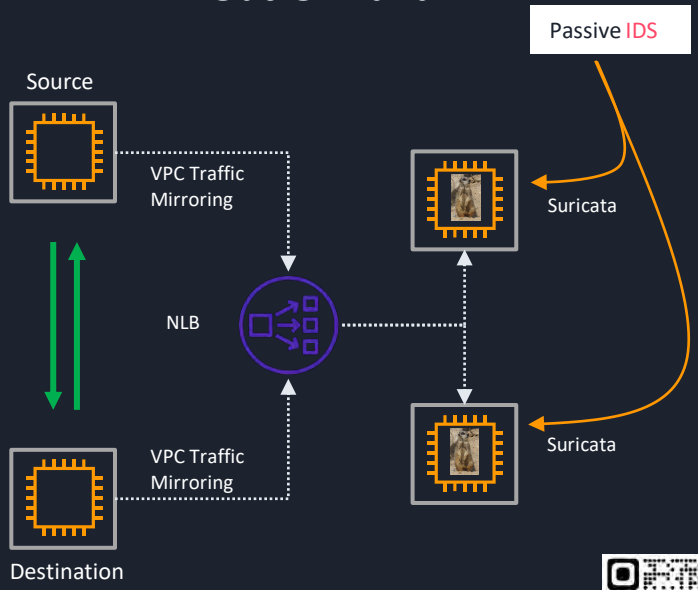
Agenda

- Suricata Inspection use cases
- Network appliance challenges
- How Gateway Load Balancer (GWLB) helps
- Top GWLB use cases and how it works
- How to deploy Suricata in-line on ECS using GWLB
- Demo
- Q&A

SURICON BOSTON 2021 OISF

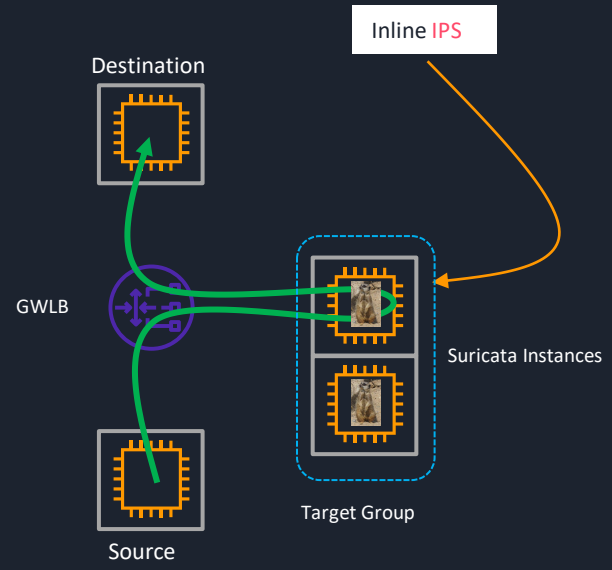
Suricata Inspection Use Cases

Out-Of-Band



AWS Quick Start Guide ->

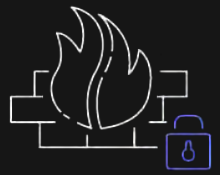
Inline



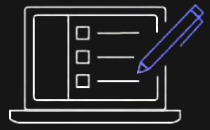
Deep dive in today's session

Network Appliances in the cloud

Inserted in-line for transparent inspection of critical traffic



Easy to add but challenging to manage, scale and maintain



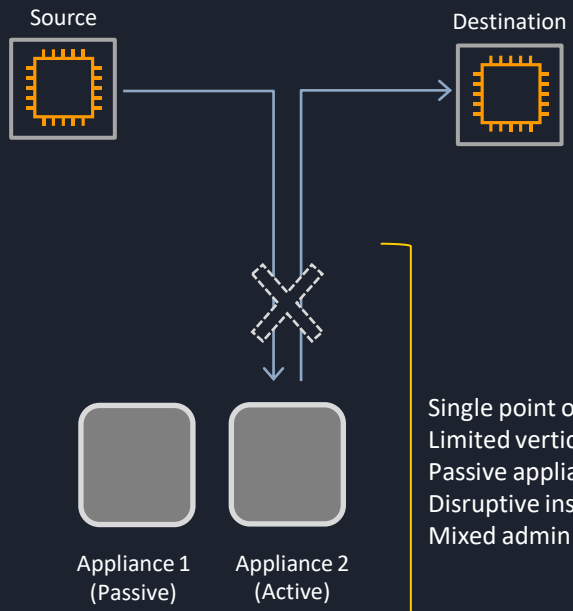
Often required by policy, or due to expertise and investment

Use the same Network Appliances on AWS and on-premises

SURICON BOSTON 2021 OISF

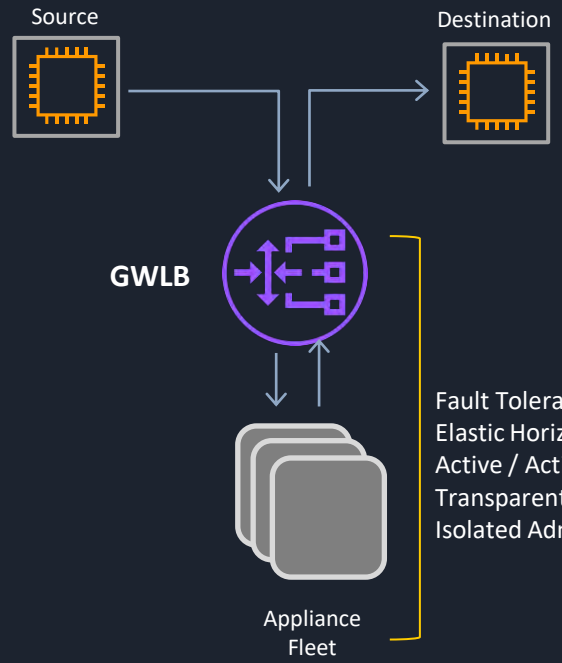
Challenges solved by Gateway Load Balancer

Before Gateway Load Balancer



Single point of failure
Limited vertical scale
Passive appliances sit idle
Disruptive insertion
Mixed admin domains

After Gateway Load Balancer



Fault Tolerant
Elastic Horizontal scaling
Active / Active Fleet
Transparent Insertion
Isolated Admin Domains

Gateway Load Balancer Customer Benefits

Reduce downtime

Eliminate single points of failure and scale horizontally in an active/active mode

Improve Performance

Remove bottlenecks, reduce latency and increase bandwidth

Accelerate Your Cloud Migration

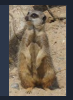
Leverage existing skillsets, tools, and license agreements

Meet compliance and regulatory requirements

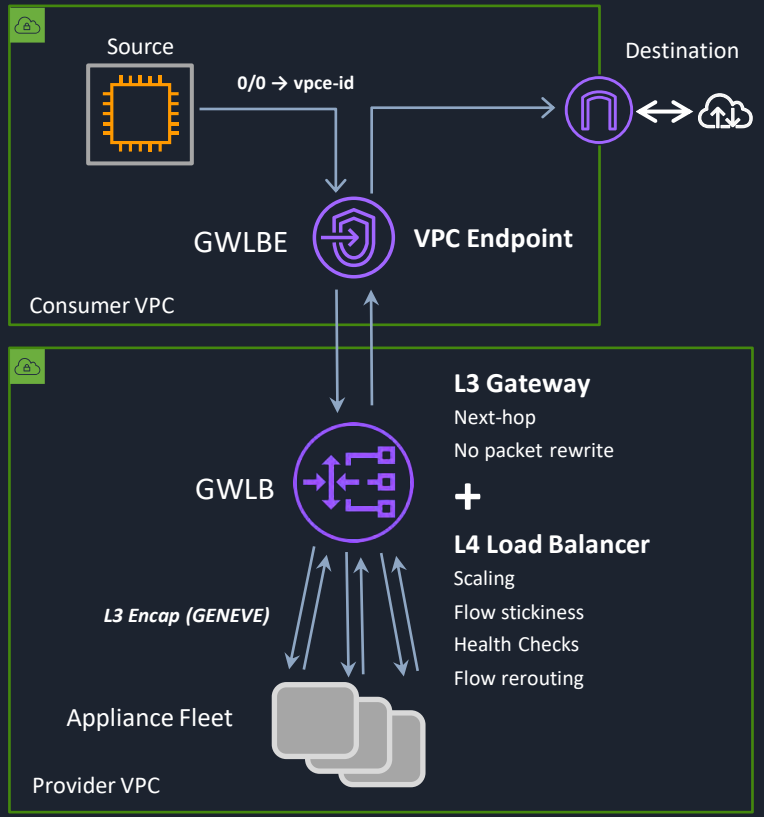
Lower Costs

Eliminate standby appliances, consolidate inspection VPCs and reduce operational overhead

Gateway Load Balancer Top Use Cases

Partner Solutions		DIY 
Firewalls IDS/IPS 	Network Visibility and Analytics 	Custom Linux Inspection Appliances 

How it works: GWLB Components



Components

- Gateway Load Balancer Endpoint (GWLBE) - A new type of VPC endpoint that can be a next-hop in a VPC route table
- Gateway Load Balancer (GWLB) - A new type of load balancer that includes L3 Gateway + L4 Load Balancer capabilities
- Both components powered by AWS Hyperplane

Deployment

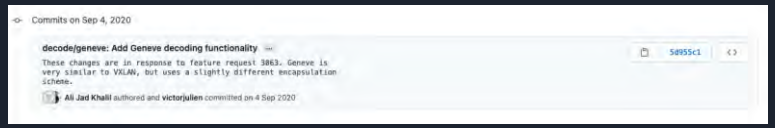
- Create GWLB and appliance fleet using steps similar to NLB
- Send traffic to GWLBE by updating VPC route tables

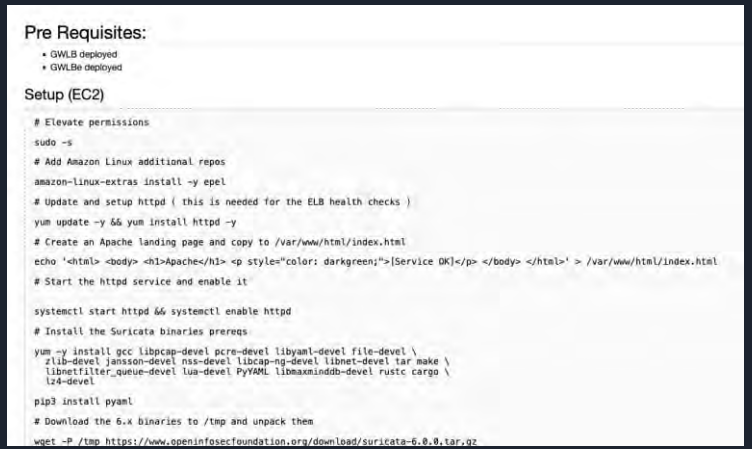
SURICON BOSTON 2021 OISF

Learn & Be Curious

https://www.aboutamazon.co.uk/working-at-amazon/our-culture/our-leadership-principles

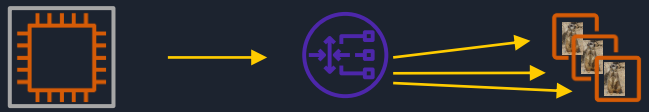
- Launch of AWS Network Firewall sparked interest in IPs/IDs rule building and capabilities
- Need / Want to help customers by giving them options to build themselves
- Which existing services could be harnessed for use with GWLB mechanics?





- PoC it!

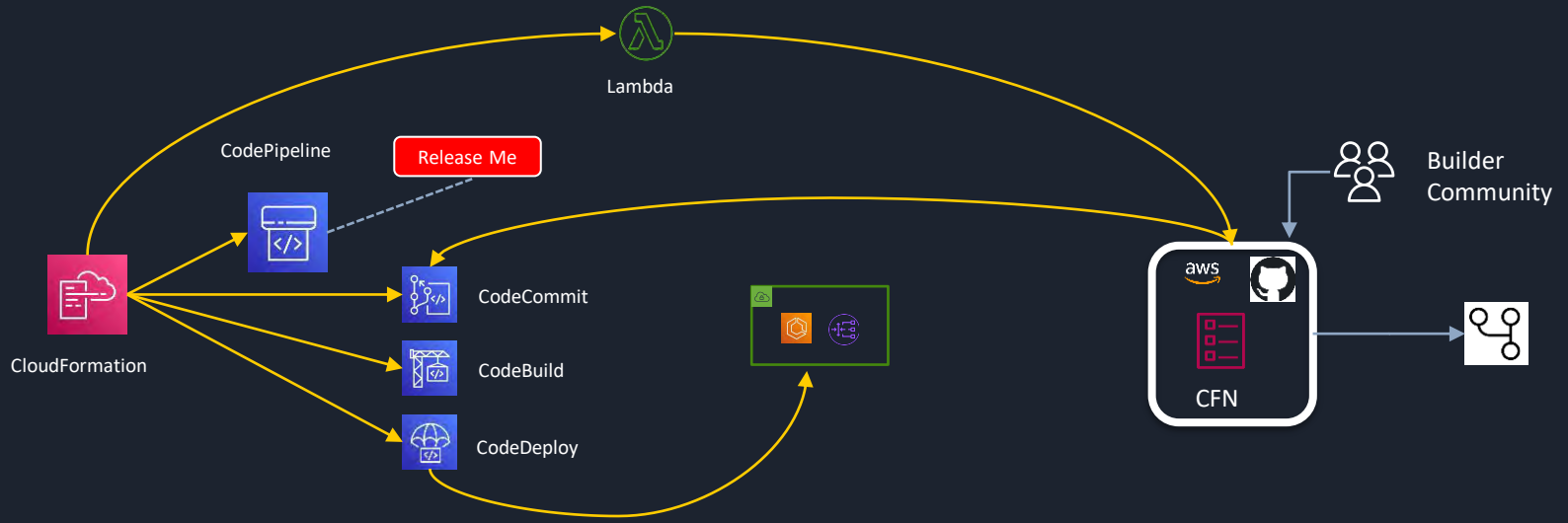
Source



Invent and Simplify

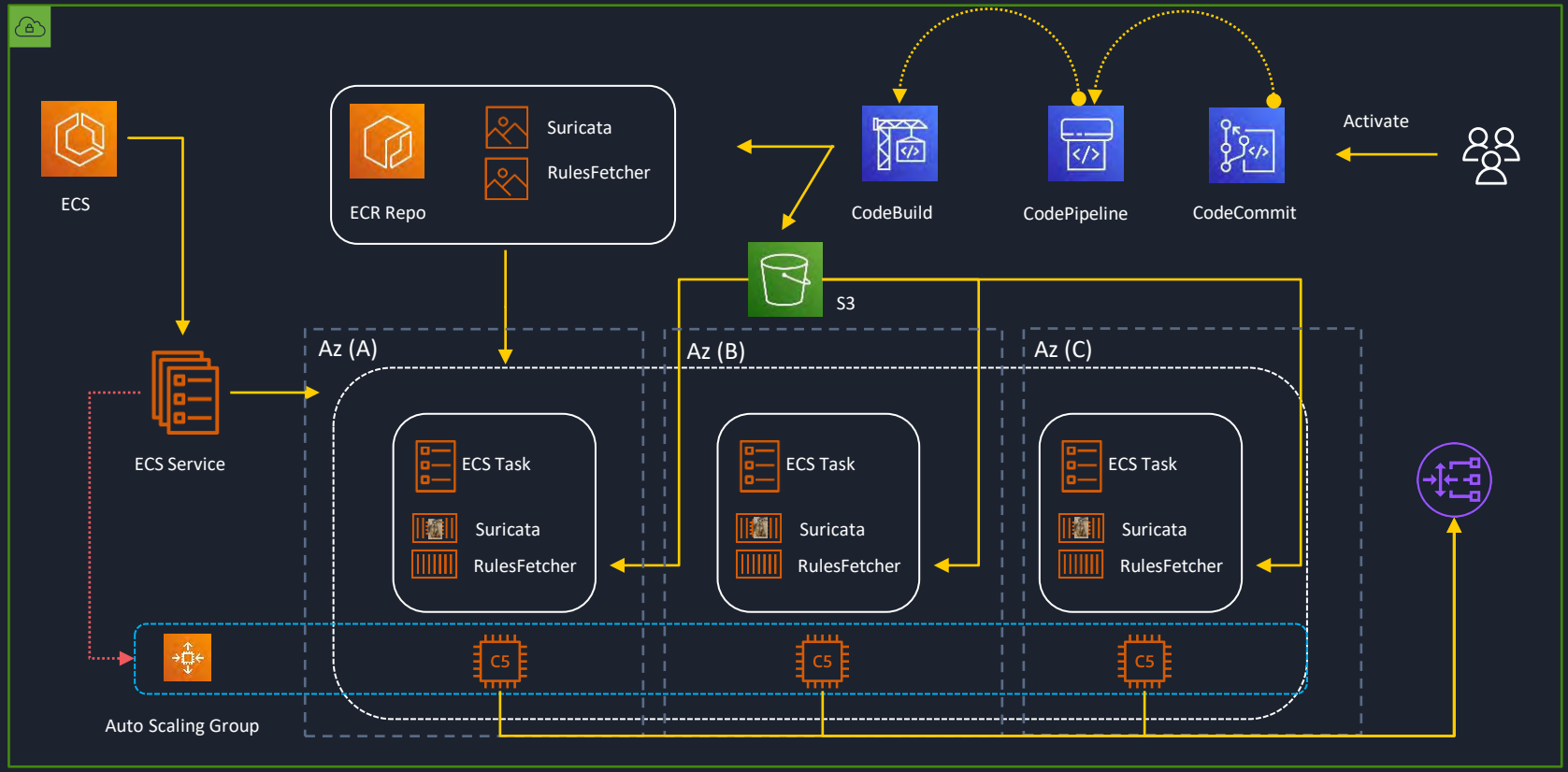
Infrastructure as code and pipelines

- Code compilation and Image packing - Can this process be improved?
- Could it be made portable?
- Desire to use DevOps processes for code release and auditing
- Customizable and extensible



Invent and Simplify

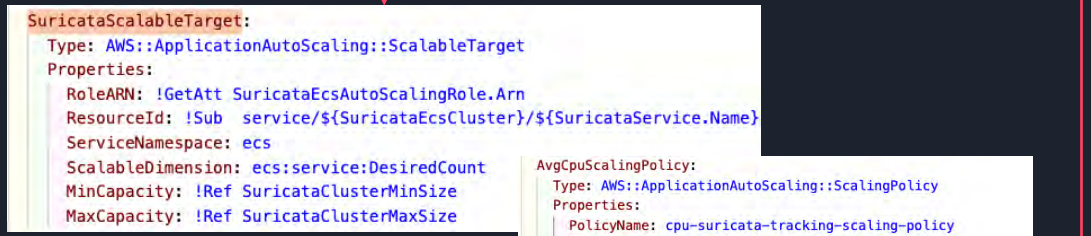
From commits to running code

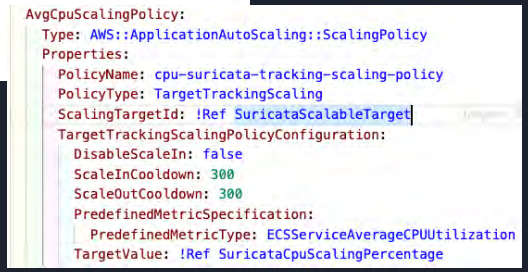


Invent and Simplify

Scaling and Baseline

- Choose a suitable instance with a good network baseline and suitable RAM/CPU allocation
- Use ECS Application Autoscaling and define your Target, Policy and Metric
- Build custom metrics as desired

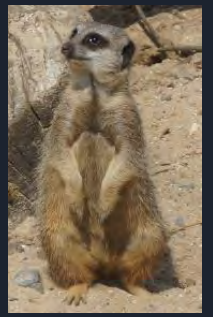




Dive Deep

Things we learned and built along the way

- ECR Public Repo to the rescue - *public.ecr.aws/amazonlinux/amazonlinux:%*
- Docker build steps went Rusty over night - *https://sh.rustup.rs*
- Pcap operations and failing to read the raw Suricata code
- Git driven, rule deployment and engine updates
- Surfacing *log outputs
- Exposing GeoIP and Lua functions
- Go to the Zoo



Think Big

Business networks, blogs and re:Invent

Create a public facing blog

Networking & Content Delivery

Building an Open Source IDS IPS service for Gateway Load Balancer

by Nilson Pulliyer and Jesper Dreiberg | on 20 SEP 2021 | in DevOps, Gateway Load Balancer, Networking & Content Delivery | Permalink | Share

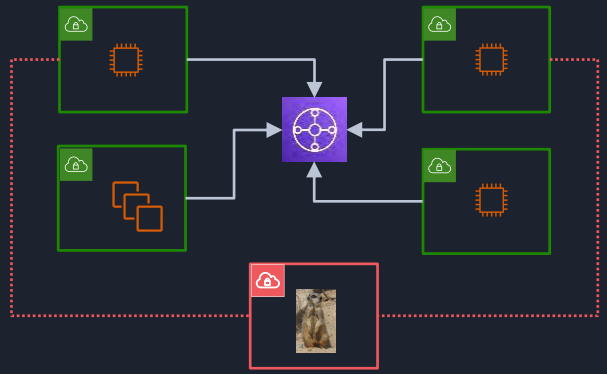
The Gateway Load Balancer (GWLB) service launched with support from the partner network. These partners provide networking appliances that enable customers to perform varying levels of packet inspection on flows that pass through them, taking action as necessary and as defined within their configuration. For a list of partners that support GWLB, refer to the following page. Whilst for some customers, using a partner supplied instance is a preferred choice (perhaps due to existing licensing, expertise or a specific capability), there is a segment of customers that wishes to benefit from all the capabilities that GWLB as a framework provides, but does not have any of the aforementioned considerations. For these customers, embracing open-source capabilities can make sense.

This blog provides the steps to create an open-source IDS/IPS service running in Docker containers, using Amazon Elastic Container Service (ECS) and Amazon Linux 2 (AL2). This service provides stateless packet inspection and logging, whilst leveraging the simplicity, elasticity and scalability that GWLB enables.

2.5k post reads on LinkedIn
1k reads on AWS Blog Channel
250 views, 43 clones and 4 forks on GitHub

re:Invent 2021 Workshop

Open-source security appliances with AWS Gateway Load Balancer



120 minute, gamified workshop
Keep production running
Gain points for compliance
Get stickers ☺

SURICON BOSTON 2021 OISF

Useful Links

Integrating you custom logic or appliance with Gateway Load Balancer

Building and open-source IDS IPS service for Gateway Load Balancer

AWS Samples GitHub repo link

Demo

SURICON BOSTON 2021 OISF

Thank you!

SURICON BOSTON 2021

OISF

