NET301

Open-source security appliances with AWS Gateway Load Balancer

Adam Palmer
Sr. Network Specialist Solutions Architect,
AWS

Scott Morrison
Sr. Network Specialist Technical Account Manager,
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Introduction to Gateway Load Balancer
- AWS Transit Gateway, appliance mode, and ingress routing
- Introduction to Suricata
- Workshop infrastructure
- Workshop objectives

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Routing and connectivity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introduction to Gateway Load Balancer (GWLB)



Inserted in-line for transparent inspection of critical traffic



Security, monitoring, analytics, and other use cases



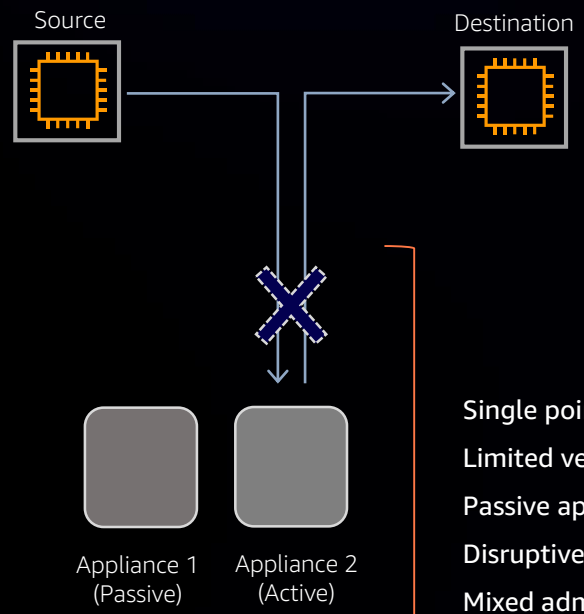
Often required by policy, or due to expertise and investment

Use the same network appliances on AWS and on-premises

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

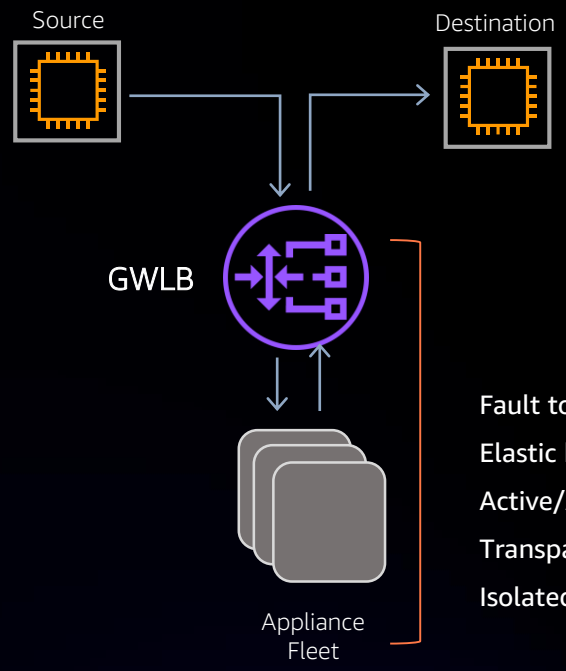
Challenges solved by Gateway Load Balancer

Before Gateway Load Balancer



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

After Gateway Load Balancer



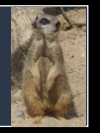
- Fault tolerant
- Elastic horizontal scaling
- Active/Active Fleet
- Transparent insertion
- Isolated admin domains

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Gateway Load Balancer top use cases

Partner solutions

DIY



Firewalls
IDS/IPS



Network visibility
and analytics



Custom Linux
inspection
appliances



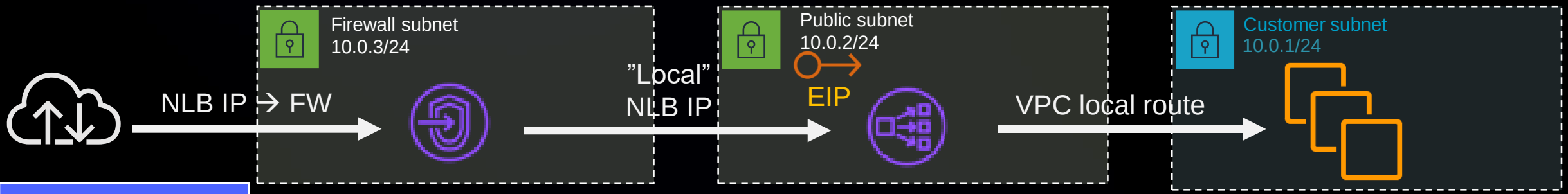
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GWLB: Distributed design pattern



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC ingress routing



IGW edge route table	
10.0.0.0/16	Local
10.0.2/24	**vpce-1234**

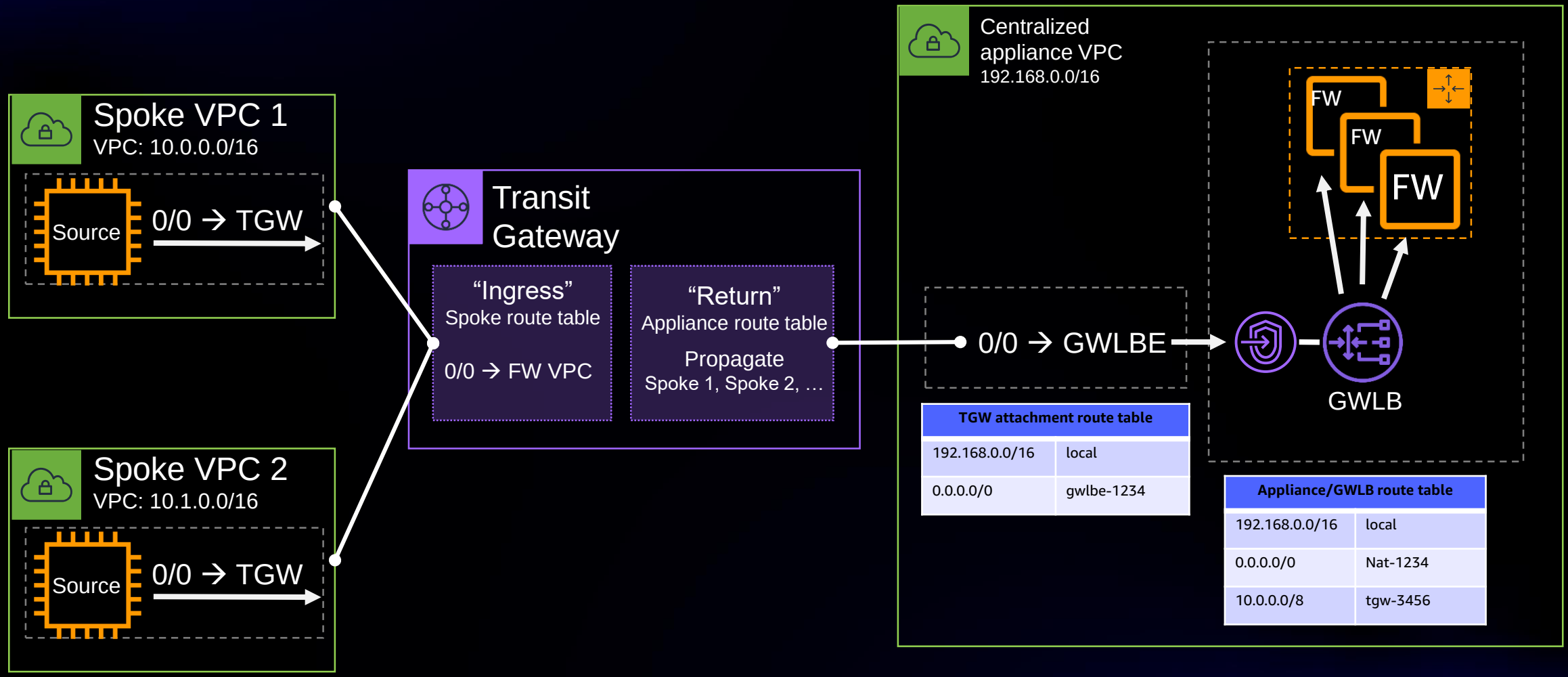
FW route table	
10.0.0.0/16	local
0.0.0.0/0	**Igw-7888**

NLB route table	
10.0.0.0/16	local
0.0.0.0/0	vpce-1234

Application route table	
10.0.0.0/16	local

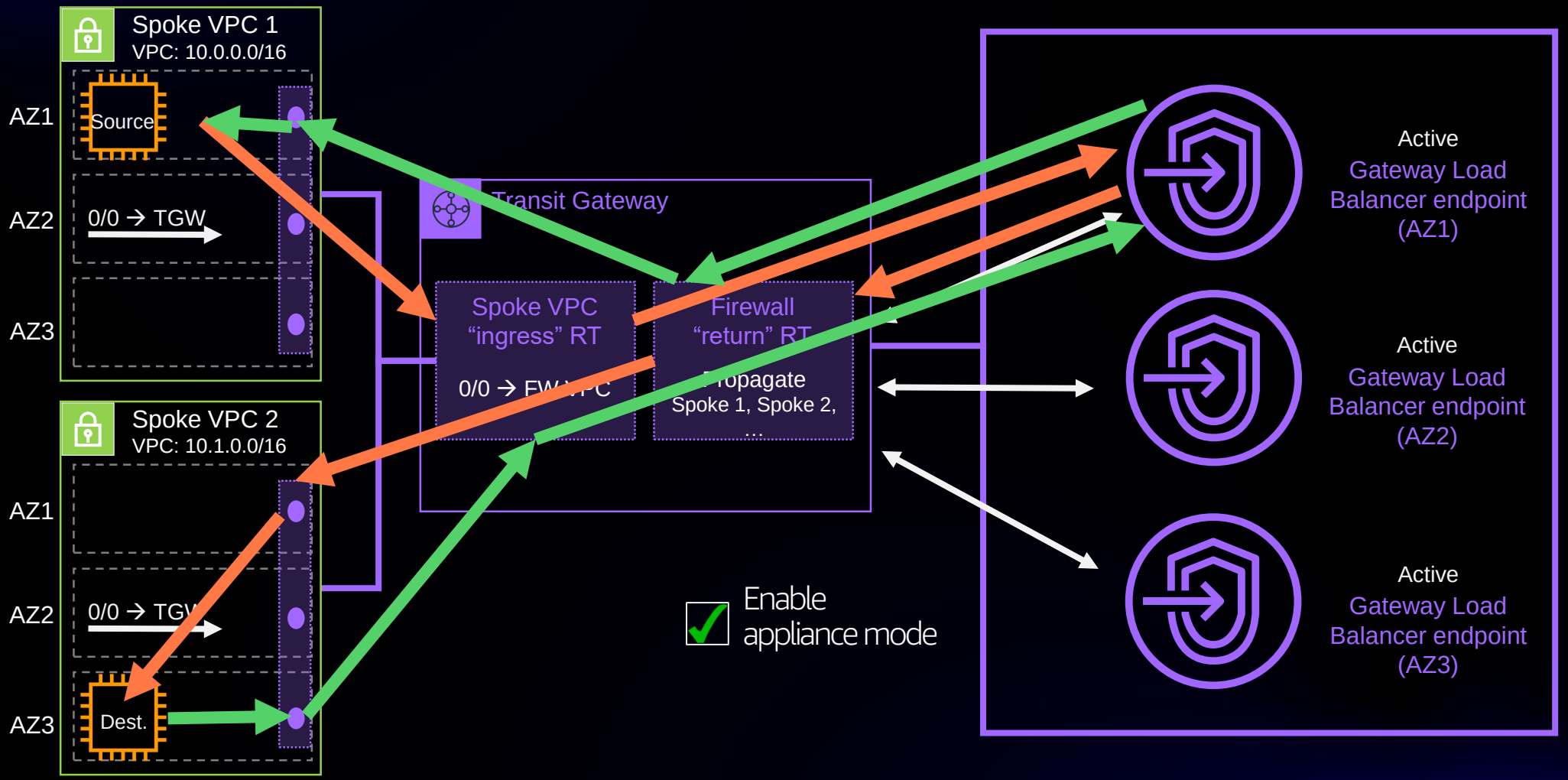
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GWLB: Centralized design pattern



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway and flow hashing



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop infrastructure

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introduction to Suricata



Highlights

- Intrusion detection, prevention, and network security monitoring
- Open-source software (maintained by the OISF)
- Fast, multithreaded user-space application
- Multiple deployment configurations
- Uses rule files and expresses rules as signatures
- Has protocol detection built in and supports additional modules

Rule structure

The general rule format follows:

- *['action' - 'protocol' - 'network' - 'port' - 'direction' - 'network' - 'port' - (rule options and keywords)]*
- *[drop tcp 10.0.0.1/32 any -> any 80 (msg:"dropped http from source";sid:10000;rev:1;)]*

aws

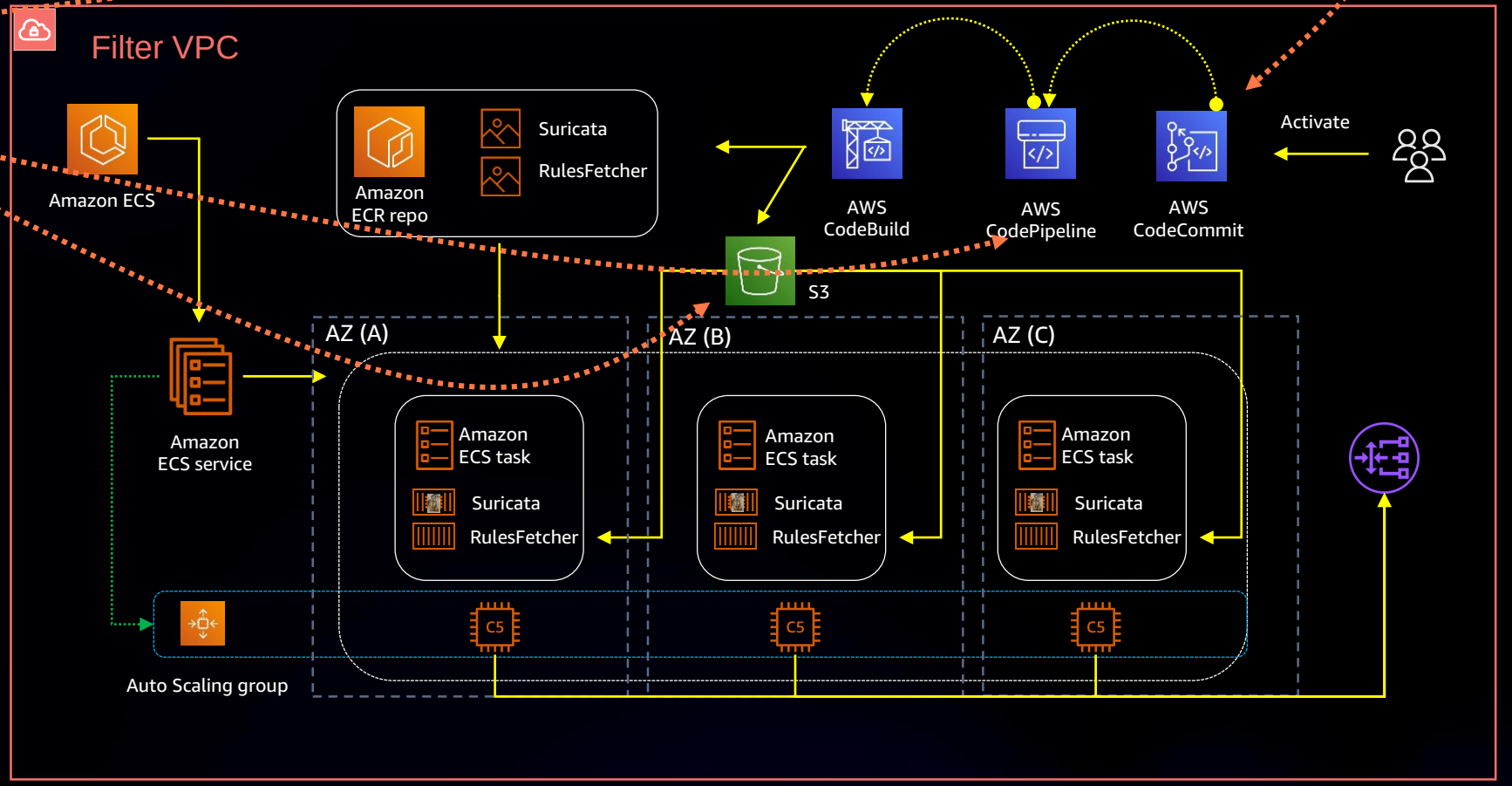
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inspection solution

Filter VPC

- GitOps driven
- Fully automated
- Updated rules and scripts

See the readme for more details



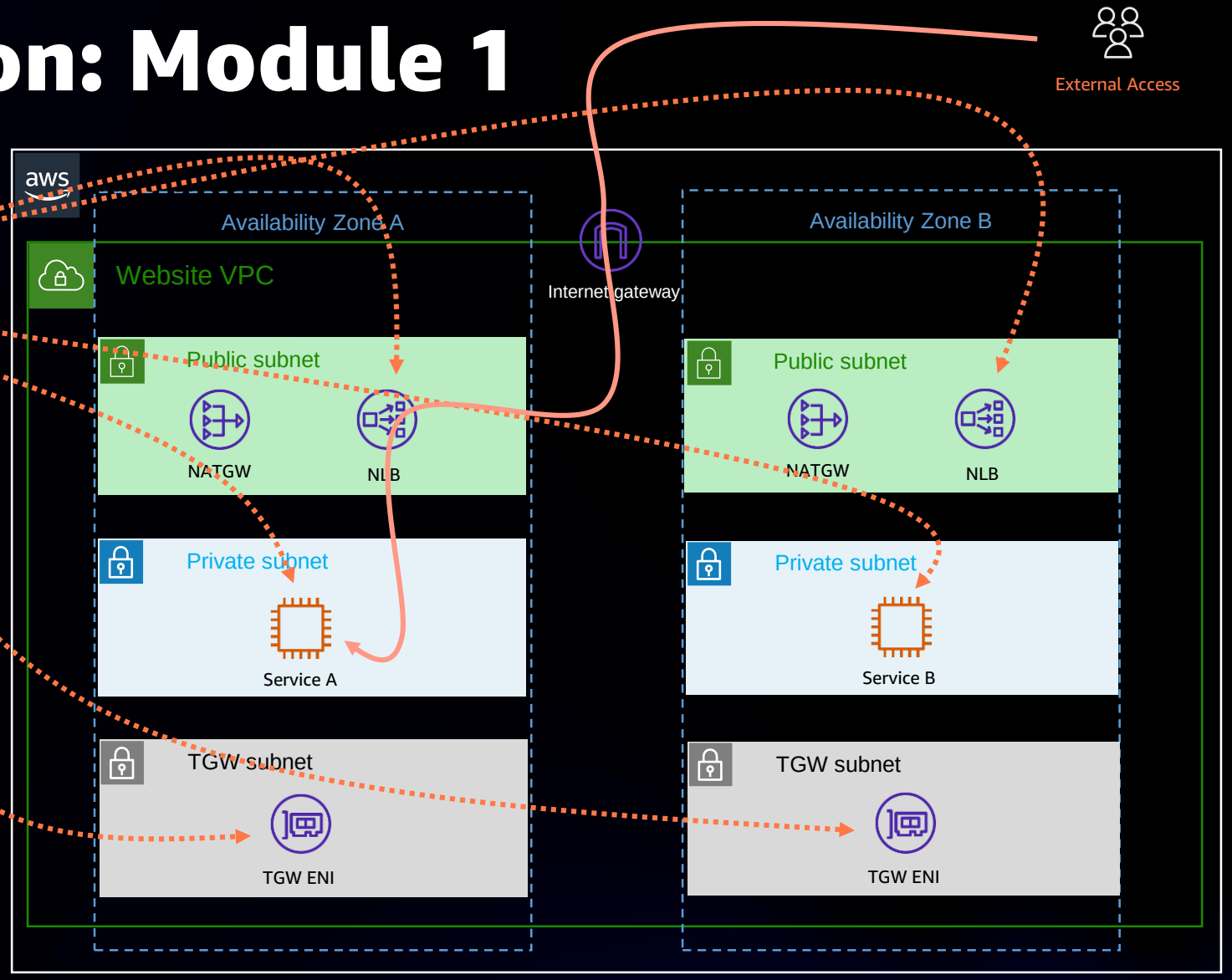
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Website application: Module 1

Website VPC

- Public network load balancer
- Private web application
- Attached to Transit Gateway
- Inbound flow

Access to website application is unfiltered and unprotected

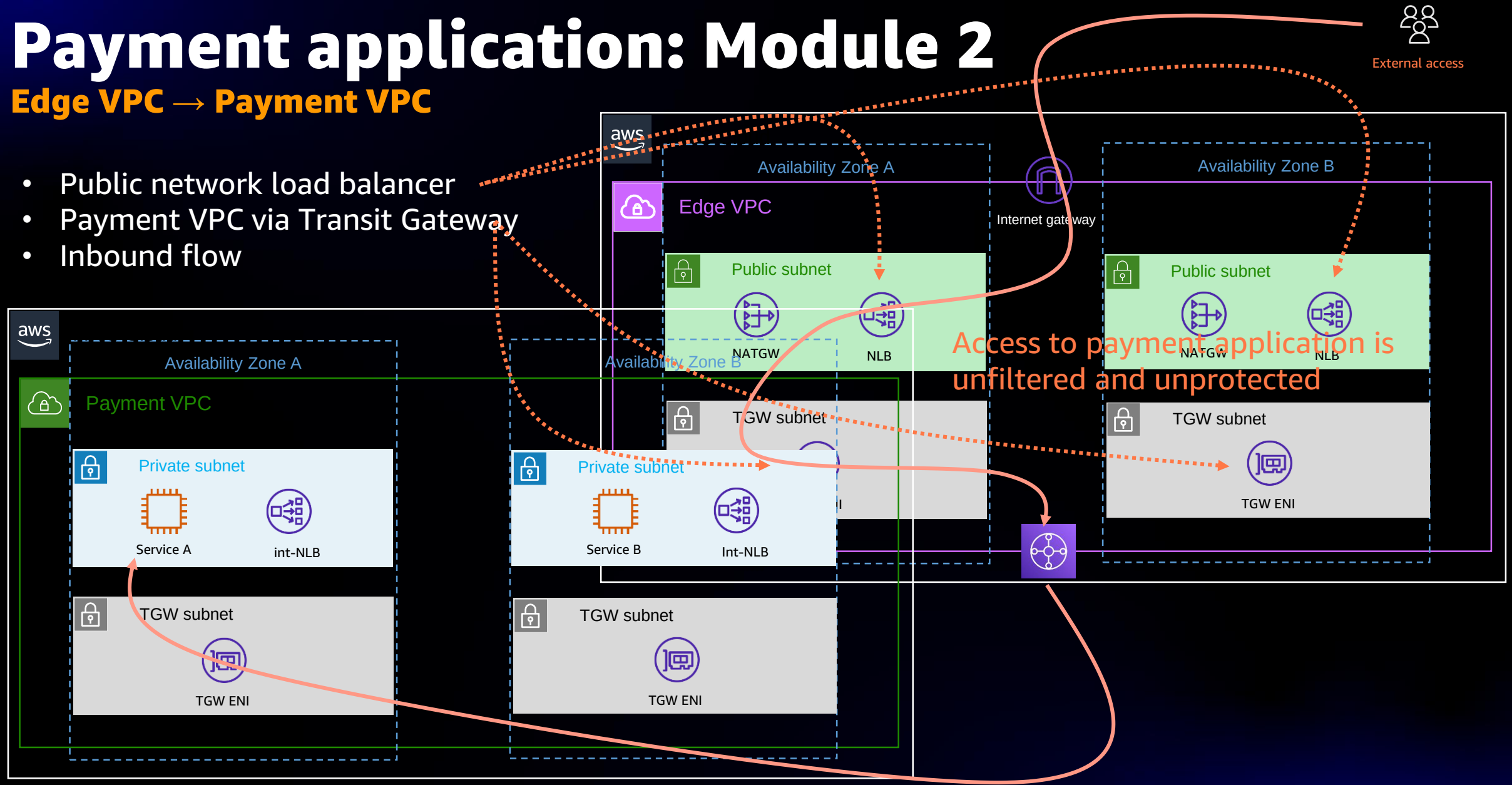


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Payment application: Module 2

Edge VPC → Payment VPC

- Public network load balancer
- Payment VPC via Transit Gateway
- Inbound flow

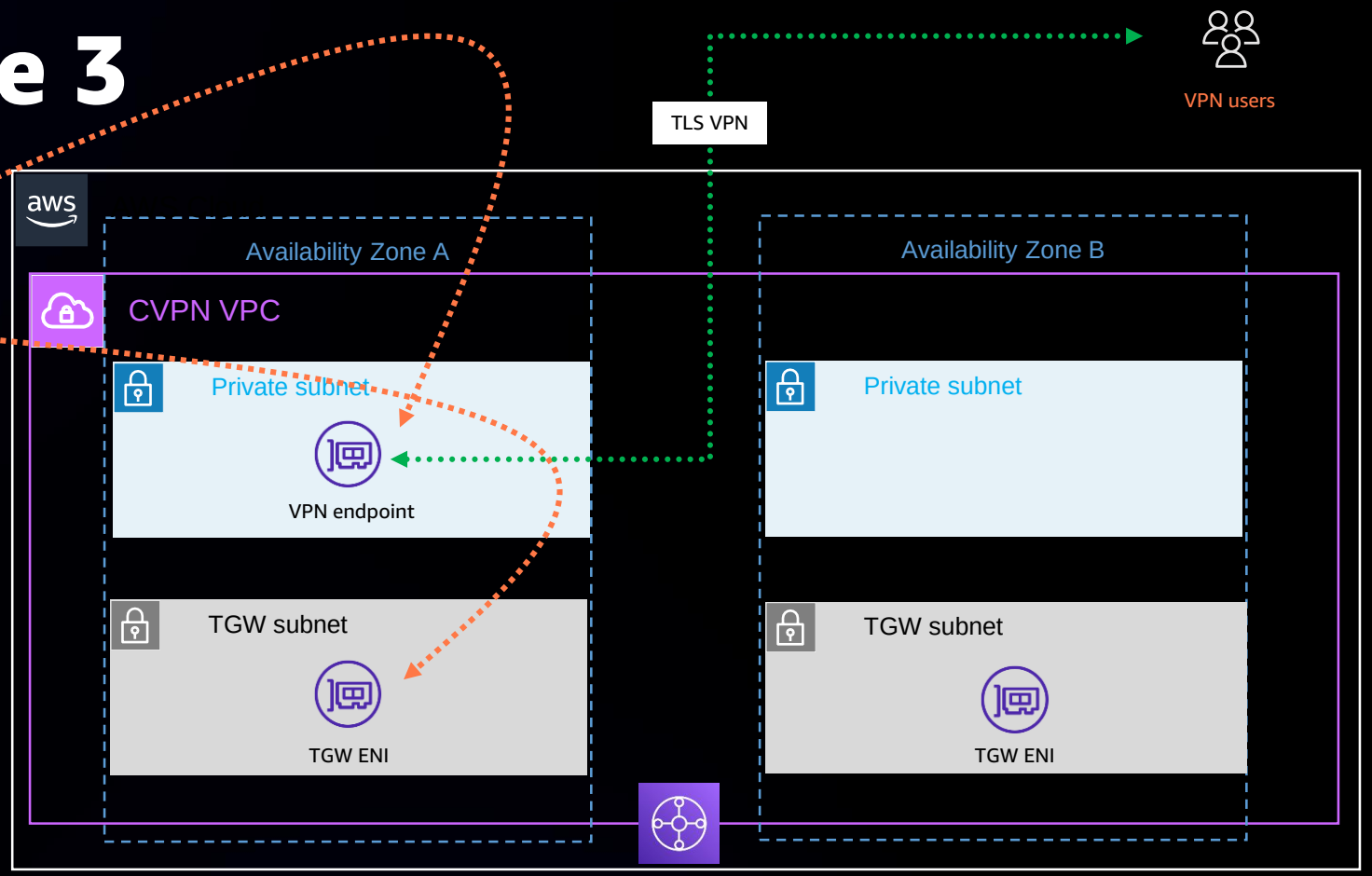


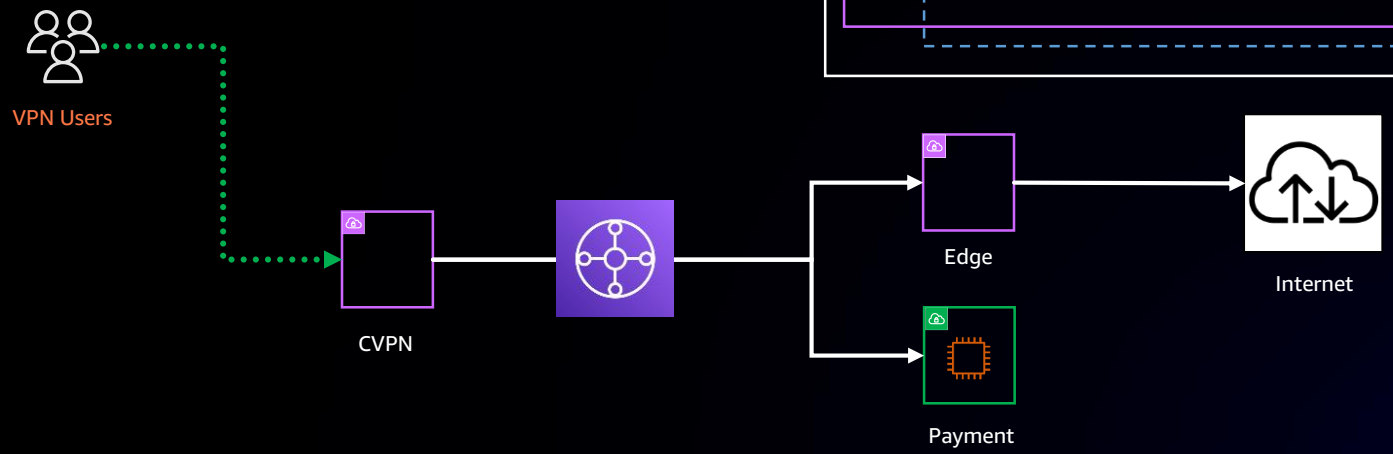
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Client VPN: Module 3

CVPN VPC

- Remote-access entry point
- Attached to Transit Gateway
- Internet access via Edge VPC
- Payment VPC via Transit Gateway





Access to payment application and internet is unfiltered

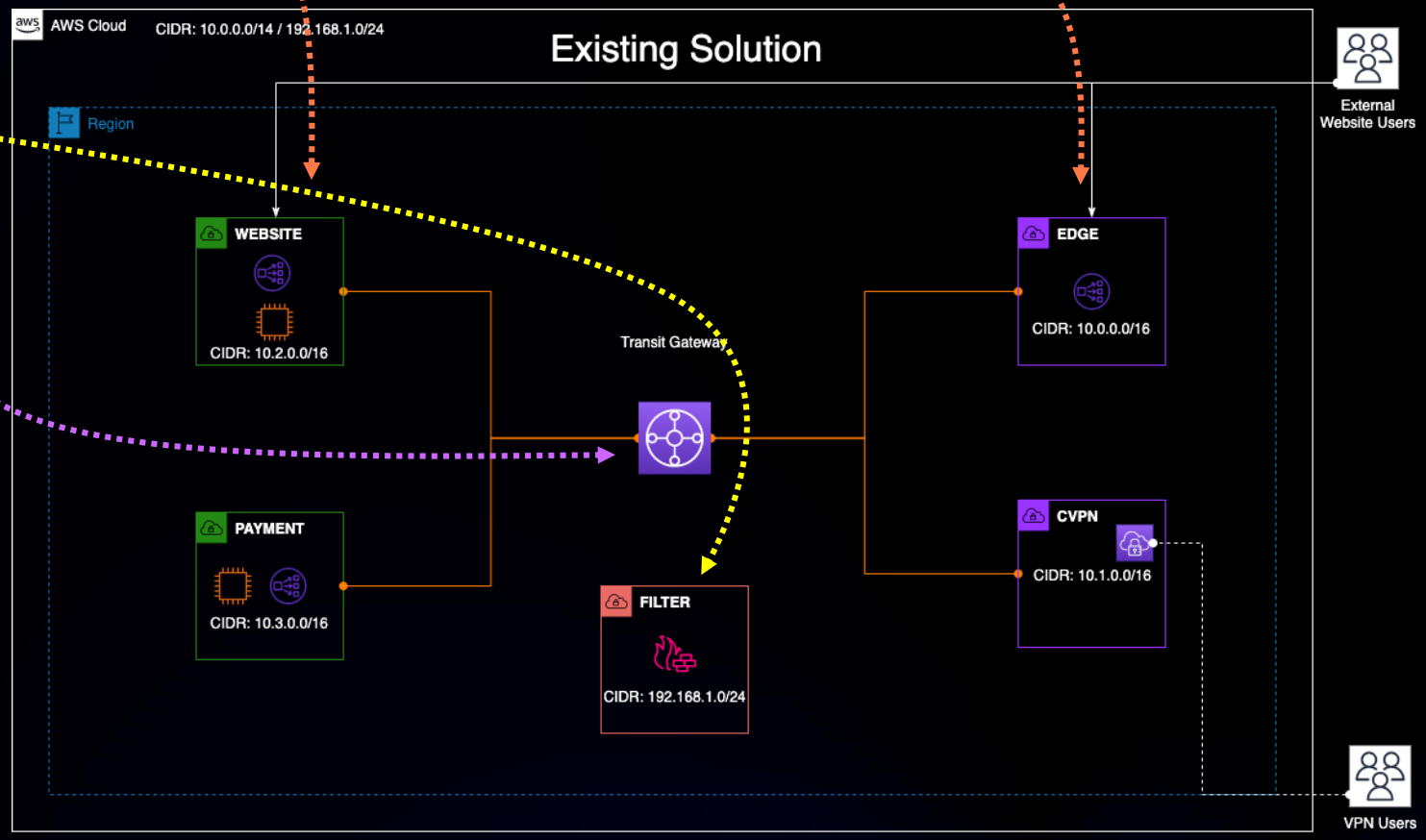
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Default architecture

- Needs ingress routing
- Needs TGW attachments
- Needs TGW route table adjustments

See the readme for more details

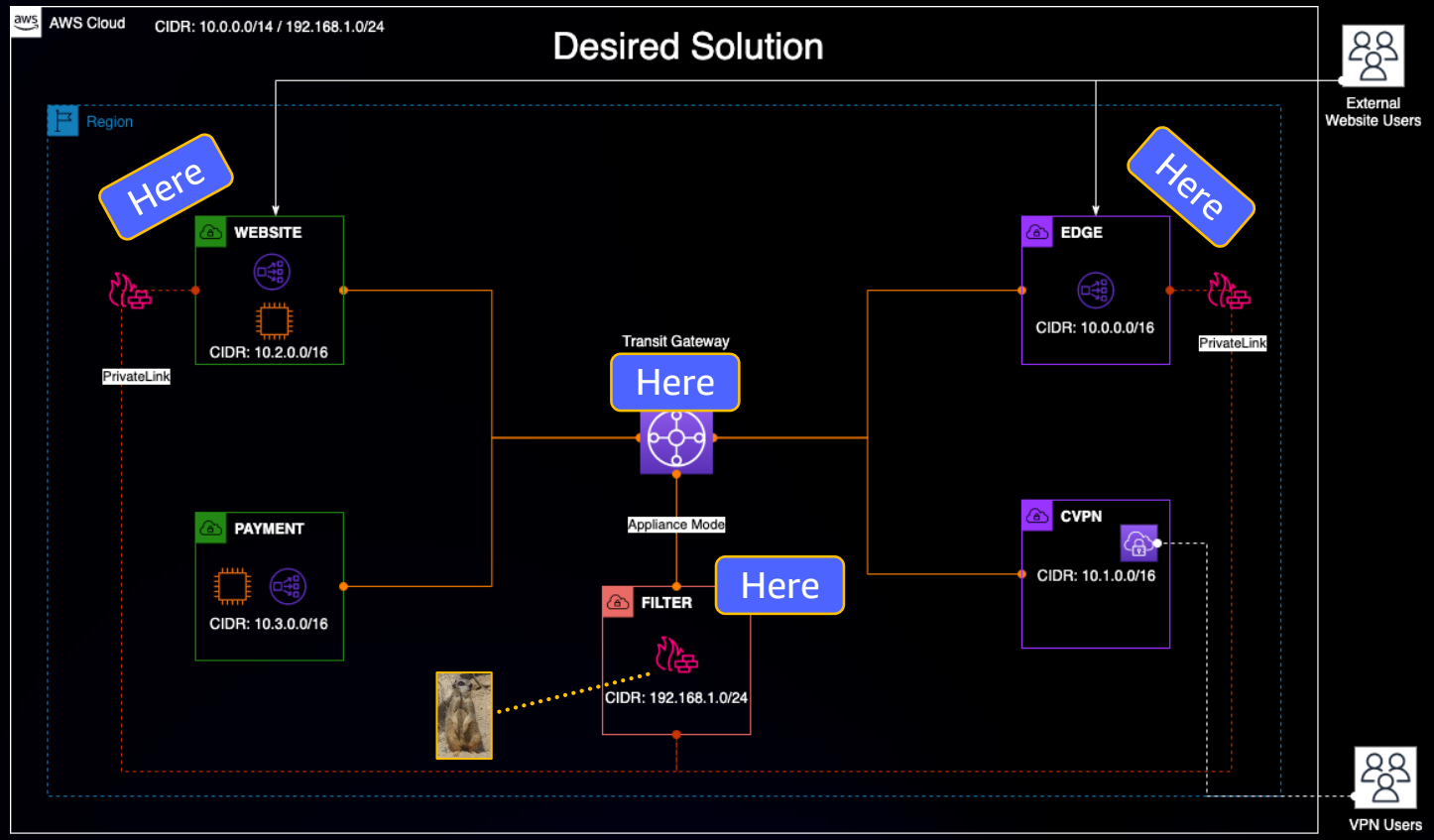


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Completed architecture

- Ingress routing configured and endpoints deployed
- TGW attached and appliance mode enabled
- TGW route tables configured
- IPS rules deployed

See the readme for more details



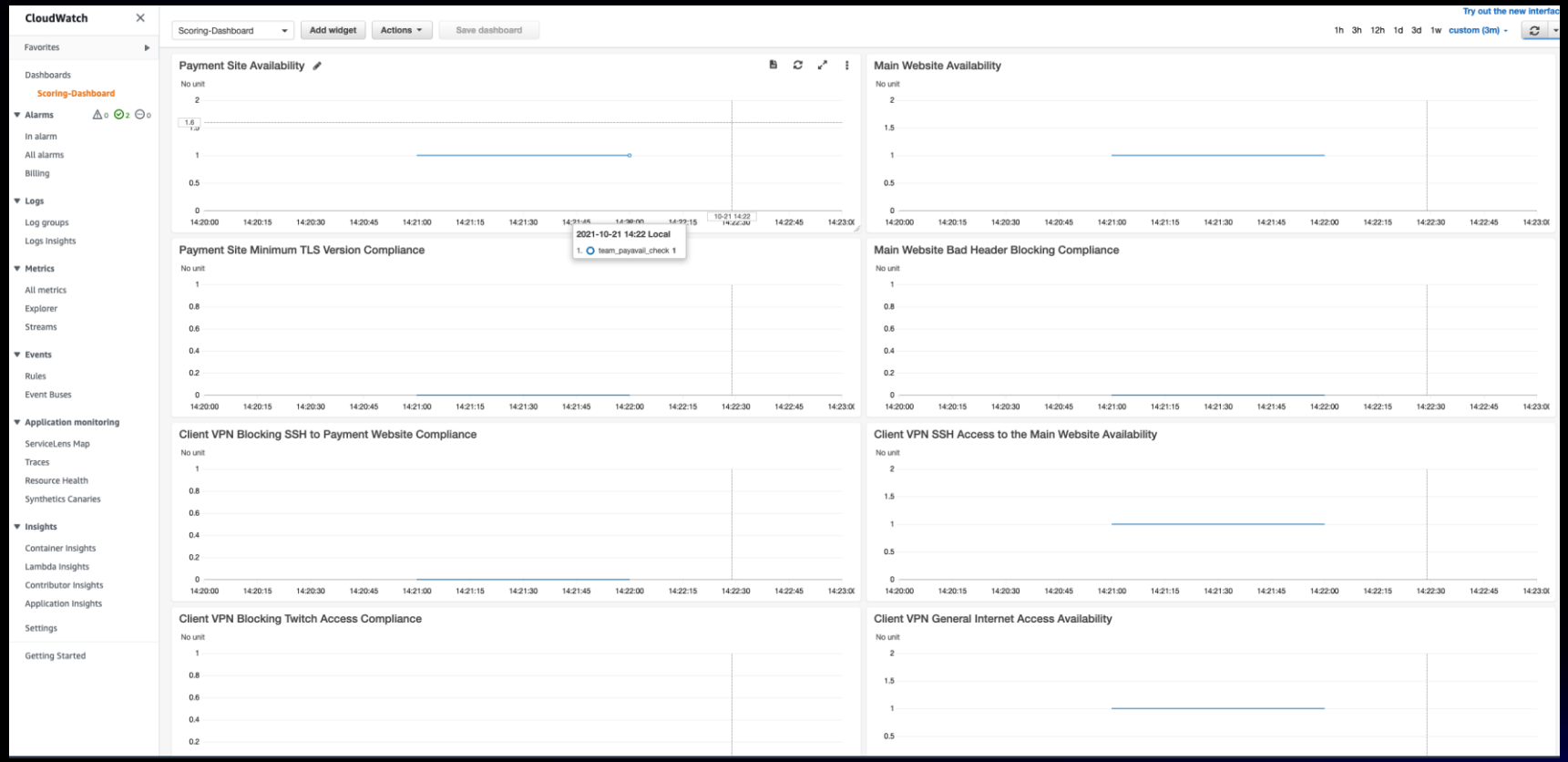
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop objectives

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hands-on: Objective

- Meet the compliancy requirements while maintaining availability of the stack
- Earn points for successfully met compliance checks
- Lose points for unavailability of key resources



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hands-on: Modules

1

Website

- Configure routing
- Investigate PCAP files
- Write a Lua script
- Deploy IPS rules
- Check the health dashboard

2

Payment

- Configure routing
- Setup a GeoIP database
- Deploy IPS rules
- Check the health dashboard

3

VPN

- Configure attachments
- Enable appliance mode
- Configure routing
- Deploy IPS rules
- Check the health dashboard

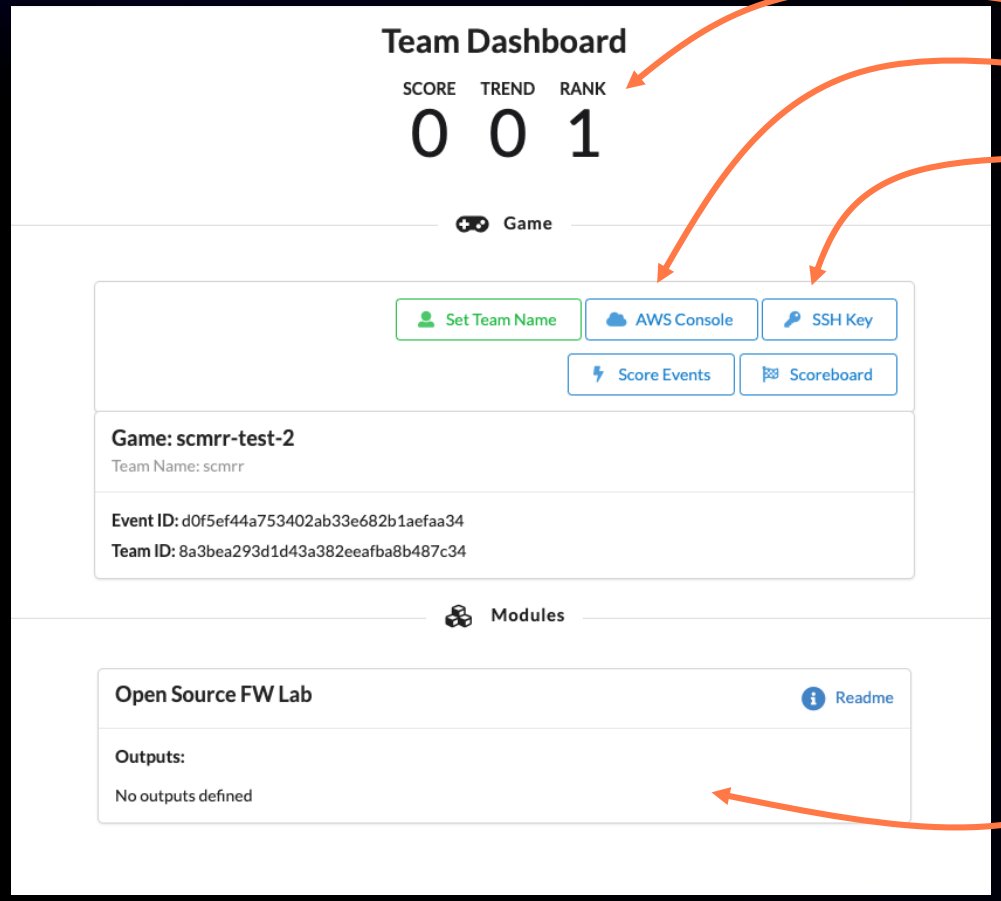
- Focus on Module 1
- Check your health dashboard regularly
- Guidance is given but not click-by-click
- Grab a session support staff when needed

Have fun!

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hands-on: Your dashboard view



- Overall scoring for your account
- Console and CLI credentials
- SSH keys needed for one or more modules
- Rule sets will be published here at the end

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hands-on

Log in to Event Engine and begin!

Login URL: https://bit.ly/3zqeSwg

Course guide and instructions:

https://tiny.amazon.com/y95y4j91/reInventNet301

Get in touch:

reinvent2021-net301@amazon.com



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Adam Palmer

linkedin.com/in/adamlewispalm

Scott Morrison

linkedin.com/in/nvscottmorrison

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.