AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

NET207

Get hands-on with AWS Network Firewall

Pratik R. Mankad
Sr. Specialist SA, Networking,
AWS

Shakeel Ahmad
Sr. Specialist SA, Networking,
AWS

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

Agenda

- Network Firewall overview
- Deployment patterns
- Event logistics
- Workshop overview

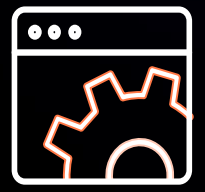
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Firewall

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

How customers secure their cloud network

Homegrown



Self-managed open source or custom-built solutions

Complex, hard to manage

Third party



Virtual firewall appliance in cloud

Costly, integration challenges

On-premises



Cloud traffic directed back on-premises to hardware firewall

Lacks scalability, costly

Cloud native



Security services provided by cloud provider

Cloud-native management experience, focused feature set

aws

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

INTRODUCING

Network Firewall

Managed infrastructure for high availability

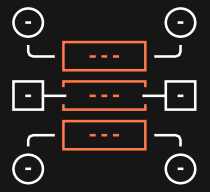
Flexible protection through fine-grained controls

Consistent policy across VPCs and AWS accounts



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

Cloud-native firewall



Scales automatically, AWS managed infrastructure



Highly flexible, high-capacity rule engine



Centrally manage policies, real-time monitoring

No upfront commitments and pay only for what you use

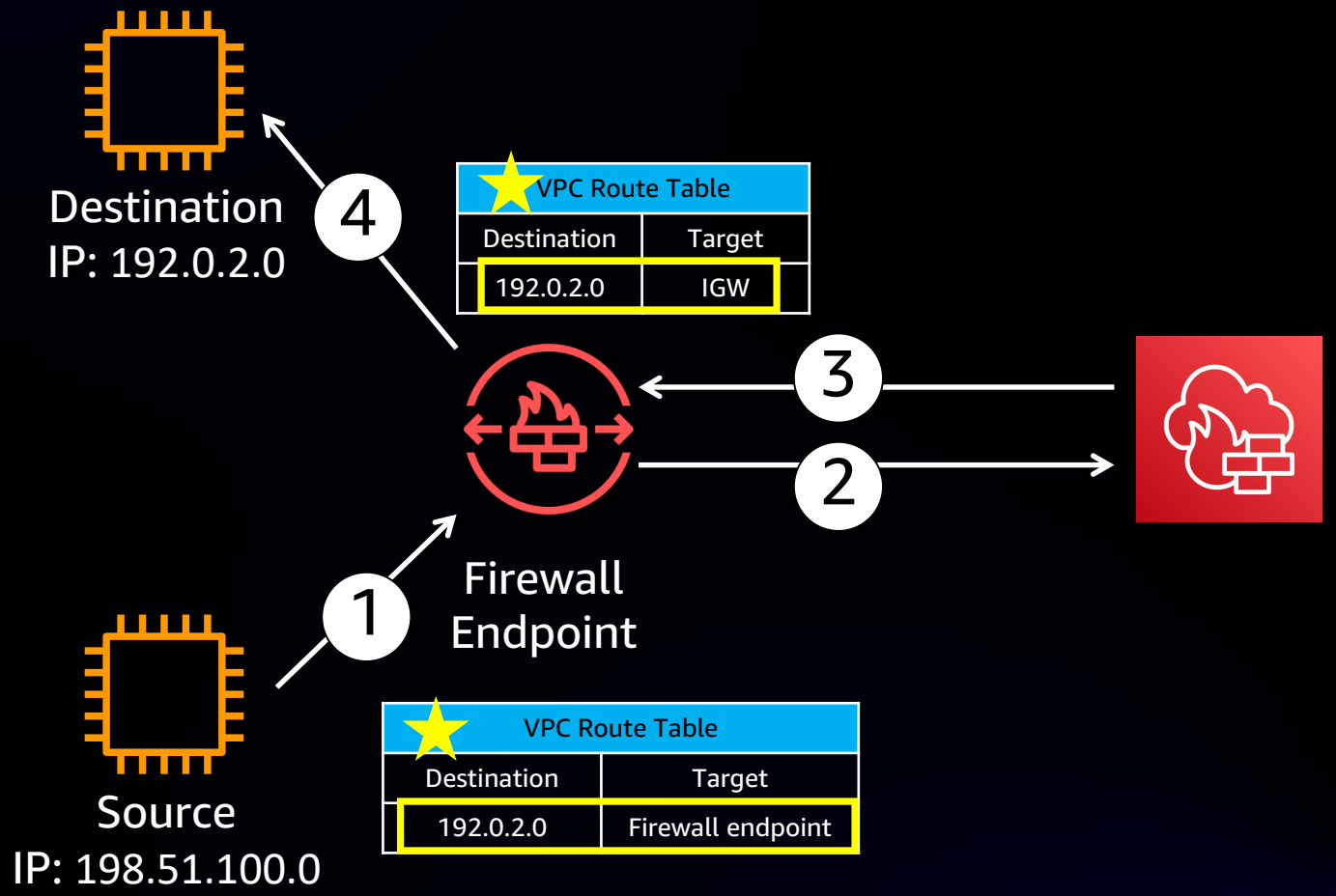
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Firewall constructs



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

Routing traffic to and from the firewall



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

Network Firewall: At a glance

Customer



Create firewall policy and rules



Deploy and route traffic to firewall endpoint



Centrally control with AWS Firewall Manager



AWS



Automatically scales with traffic

Throughput performance >45 Gbps



Managed zonal affinity and session symmetry

Resilient with SLA of 99.99%

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

Network Firewall features

Packet filtering

- Large IP block/allow lists
- Stateless rules: IP | port | protocol
- Stateful rules: IP | port | protocol
- FQDN filtering on HTTP/HTTPS
- Protocol detection, enforcement
- Application rules: IPS/IDS (common open-source rule format)

Visibility and reporting

- CloudWatch rule metrics
- Full network-flow logs
- Event- and rule-based logs
- Log collection to Amazon S3, Amazon CloudWatch Logs, or Amazon Kinesis Data Firehose

Central management

- Cross-account management and rule visibility using Firewall Manager
- AWS CloudFormation and Terraform templates
- AWS RAM

aws

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

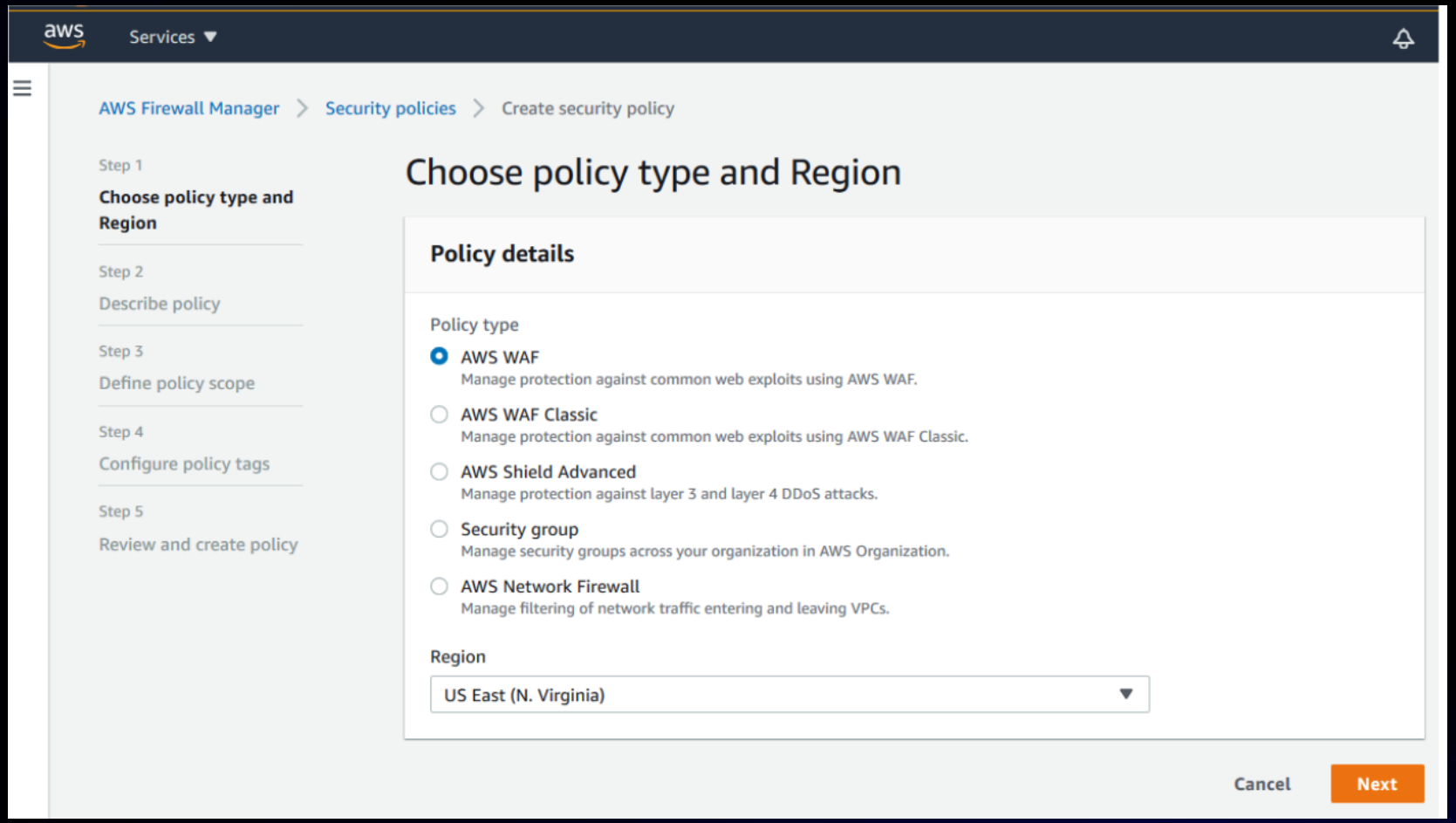
Consistent policy management with Firewall Manager

Network Firewall
L3-7 full network firewall with deep packet inspection as routable endpoint in VPC

AWS WAF
L7 protection on Amazon API Gateway, AWS ALBs, and Amazon CloudFront

AWS Shield Advanced
L3-4 DDoS protection on CloudFront, ELBs, AWS EIPs, and AWS Global Accelerator

Security groups
L3-4 IP filtering protection on EC2s



aws

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

Network Firewall pricing

https://aws.amazon.com/network-firewall/pricing/

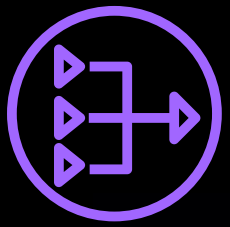
Network Firewall



You pay an hourly rate for each firewall endpoint. You also pay for the amount of traffic, billed by the gigabyte, processed by your firewall endpoint

- $0.395/hour
- $0.065/GB

AWS NAT gateway



If you choose to create an NAT gateway in your VPC along with Network Firewall, the standard NAT gateway processing and per-hour usage charges will be waived on a one-to-one basis with the throughput per gigabyte and usage hours charged for the Network Firewall

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

Network Firewall partners

Security monitoring

- sumo logic
- splunk>
- IBM Security
- DATADOG

Threat intelligence

- FORTINET
- TREND MICRO
- CROWDSTRIKE
- FIREEYE

Policy management

- Check Point SOFTWARE TECHNOLOGIES LTD
- HashiCorp Terraform
- CORTEX BY PALO ALTO NETWORKS
- tufin

Managed security

- accenture
- ALERT LOGIC
- rackspace technology
- IBM Security

aws

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

Network Firewall and other AWS security

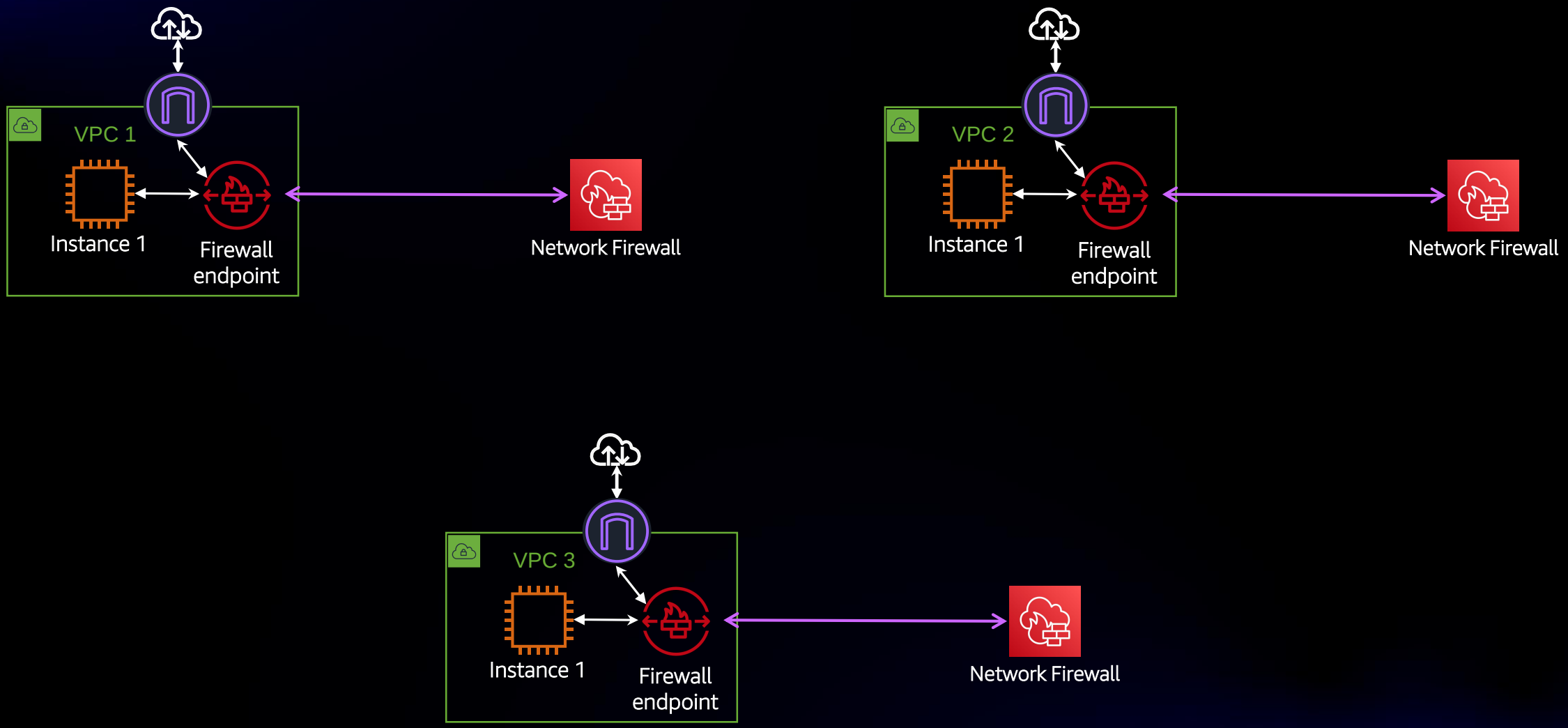
	Network Firewall	VPC security group	Network ACL	AWS WAF
Where is the protection applied?	Route level, based on VPC routes	Amazon EC2-instance level	Subnet level	Endpoint level (API Gateway, ALB, CloudFront)
Stateful or stateless	Both	Stateful	Stateless	Stateless
Which flows are protected?	All ingress/egress flows at perimeter of VPC (e.g., IGW, VGW, DX, VPN, VPC-VPC)	All ingress/egress flows at instance level (EC2-EC2, EC2-IGW, EC2-DX, etc.)	All ingress/egress flows at subnet level (subnet-subnet, subnet-IGW, subnet-DX, etc.)	Ingress only from internet to API Gateway, ALB, CloudFront
Which OSI layer?	L3-7	L4	L3	L7
Features	Stateless/ACL L3 rules, stateful/L4 rules, IPS-IDS/L7 rules, FQDN filtering, protocol detection, deep packet inspection, large IP block/allow lists	IP | port | protocol filtering	IP | port | protocol filtering	Deep application layer filtering, managed rules
Default behavior	Allow	Deny	Allow	Customer chooses

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

Deployment patterns

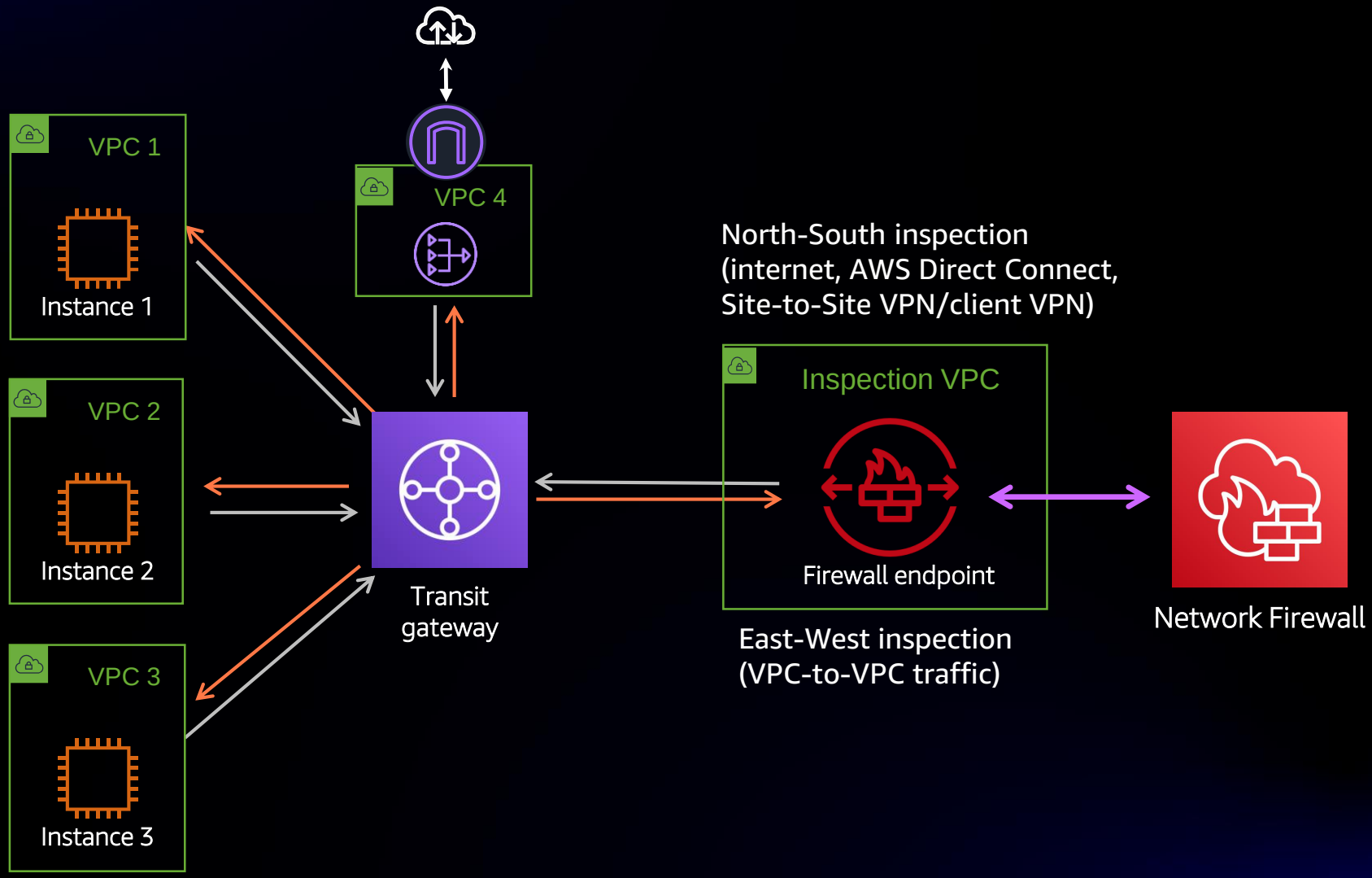
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Distributed deployment model



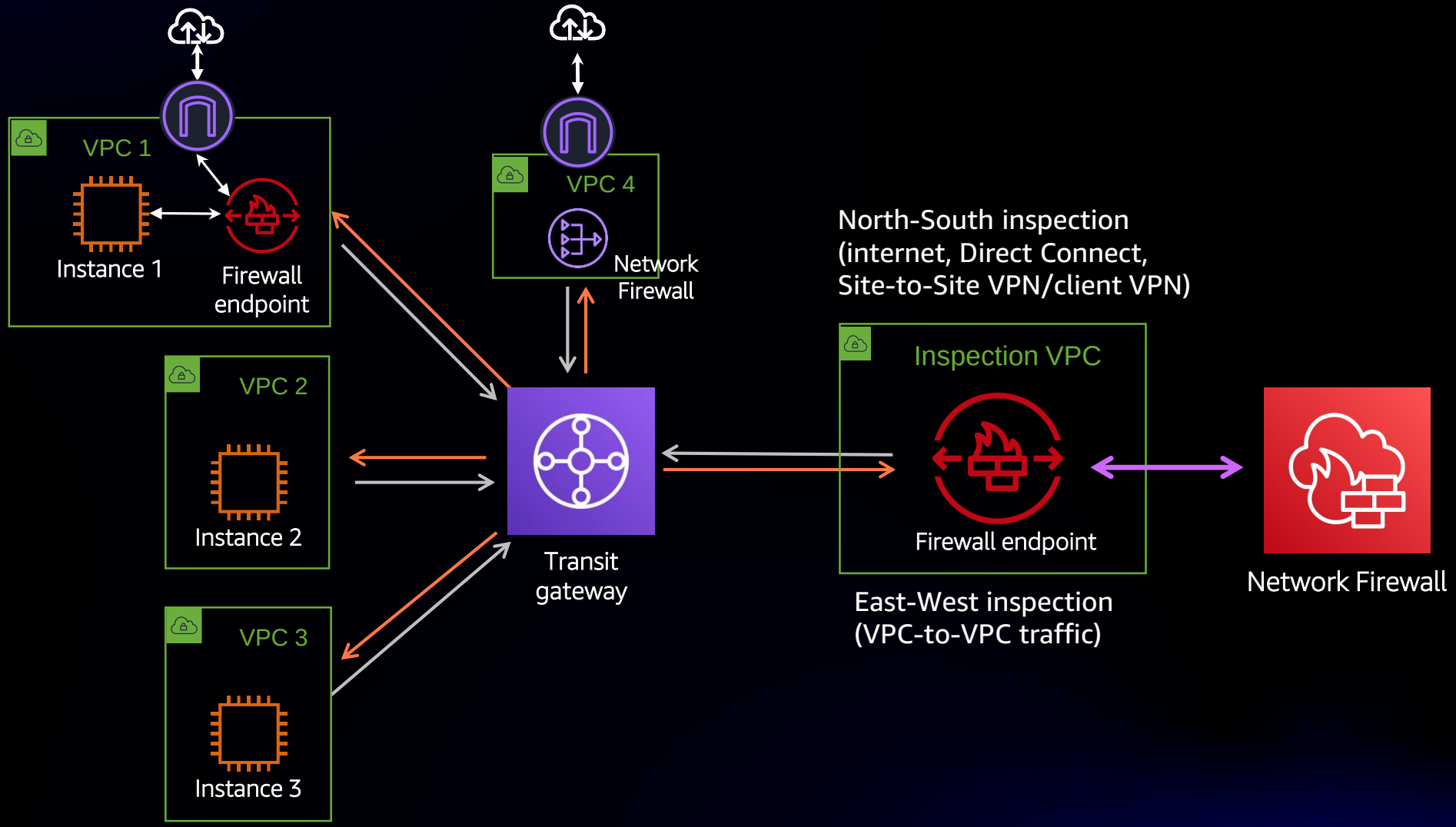
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Centralized deployment model



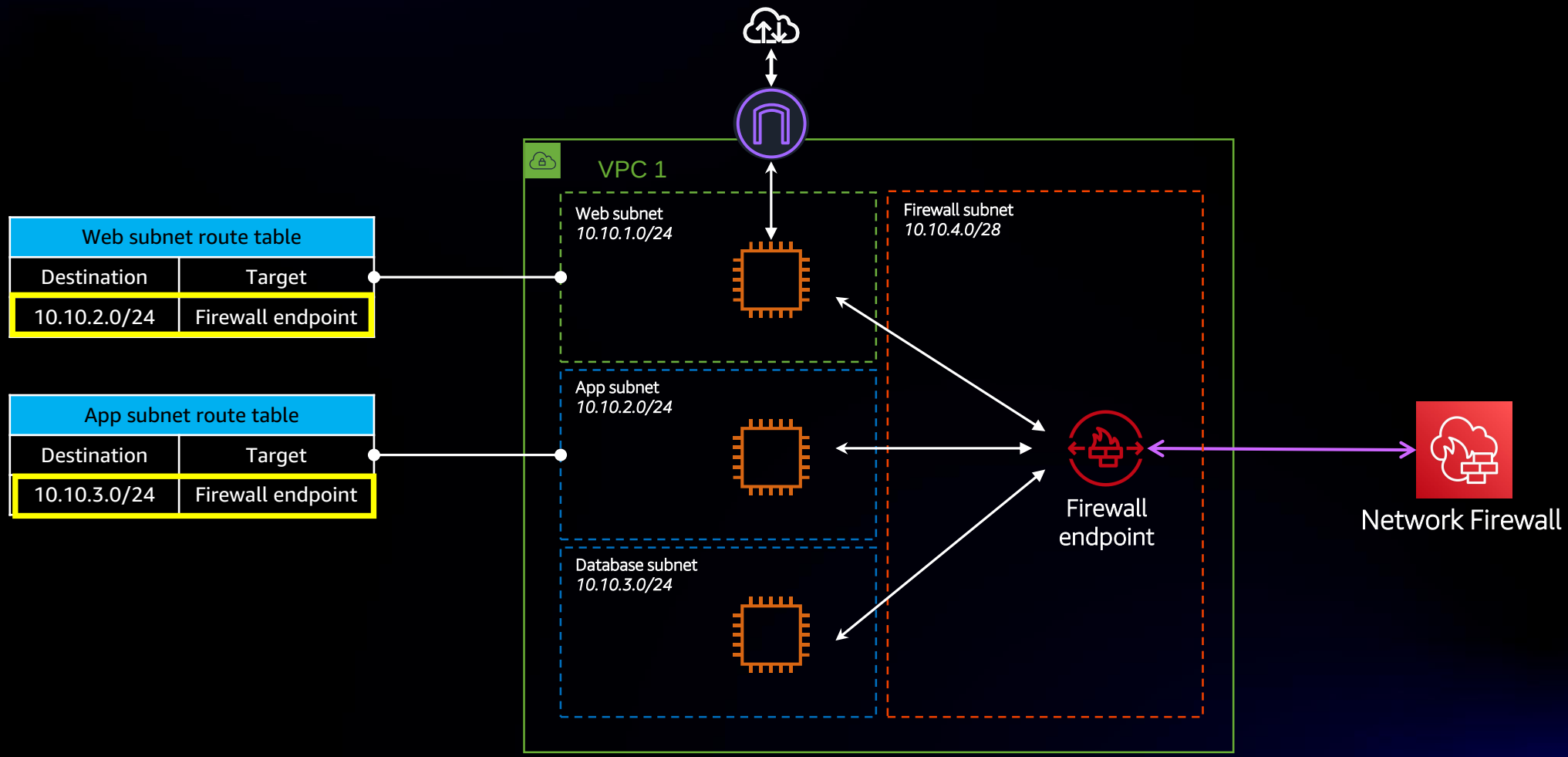
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Combined deployment model



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

Network Firewall with VPC routing enhancements



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

Deployment model resources

Blog post, part 1:
"Deployment model for AWS Network Firewall"

Blog post, part 2:
"Deployment model for AWS Network Firewall with VPC routing enhancements"

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

Event logistics

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

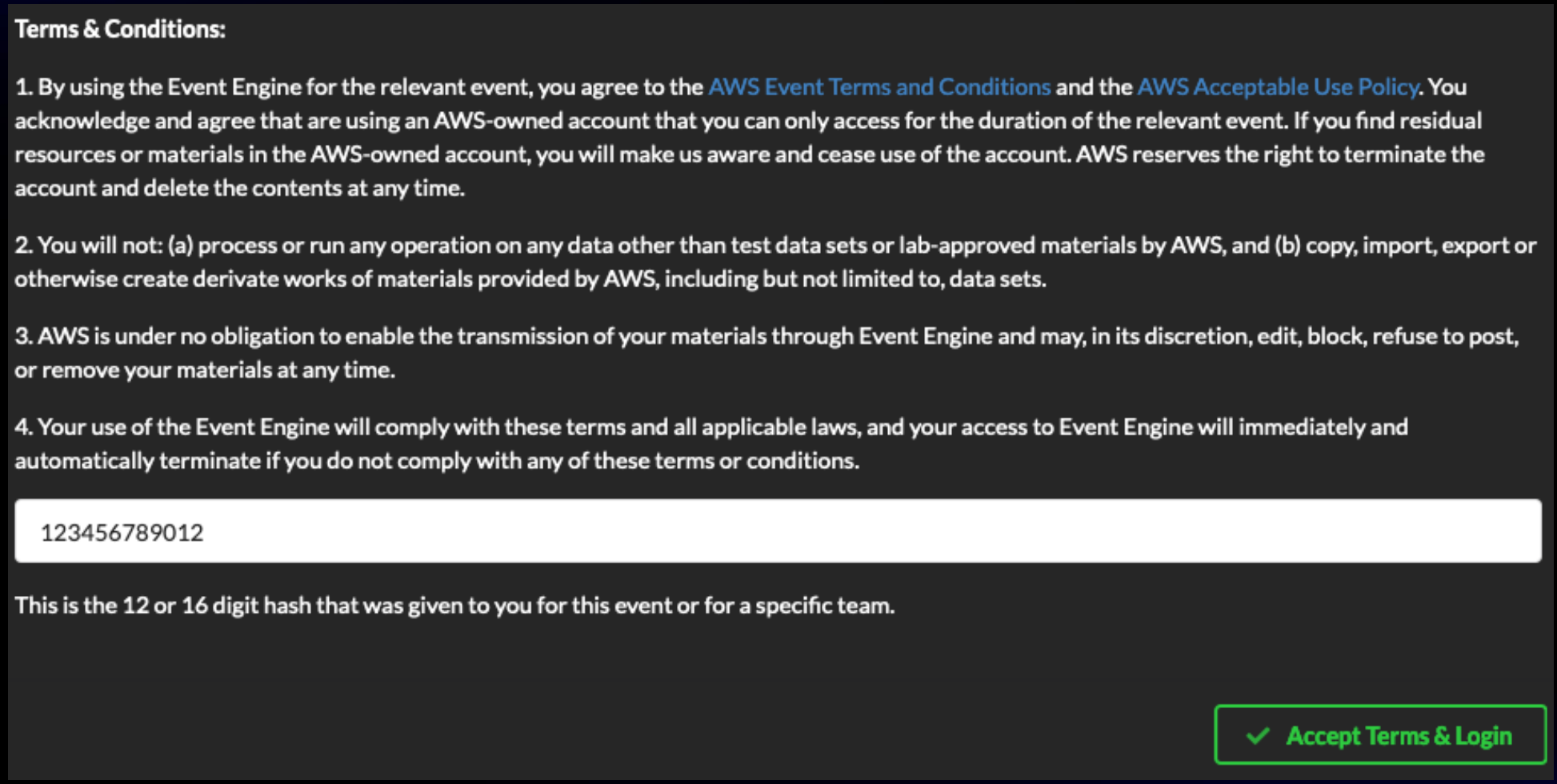
Event Engine

https://dashboard.eventengine.run



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

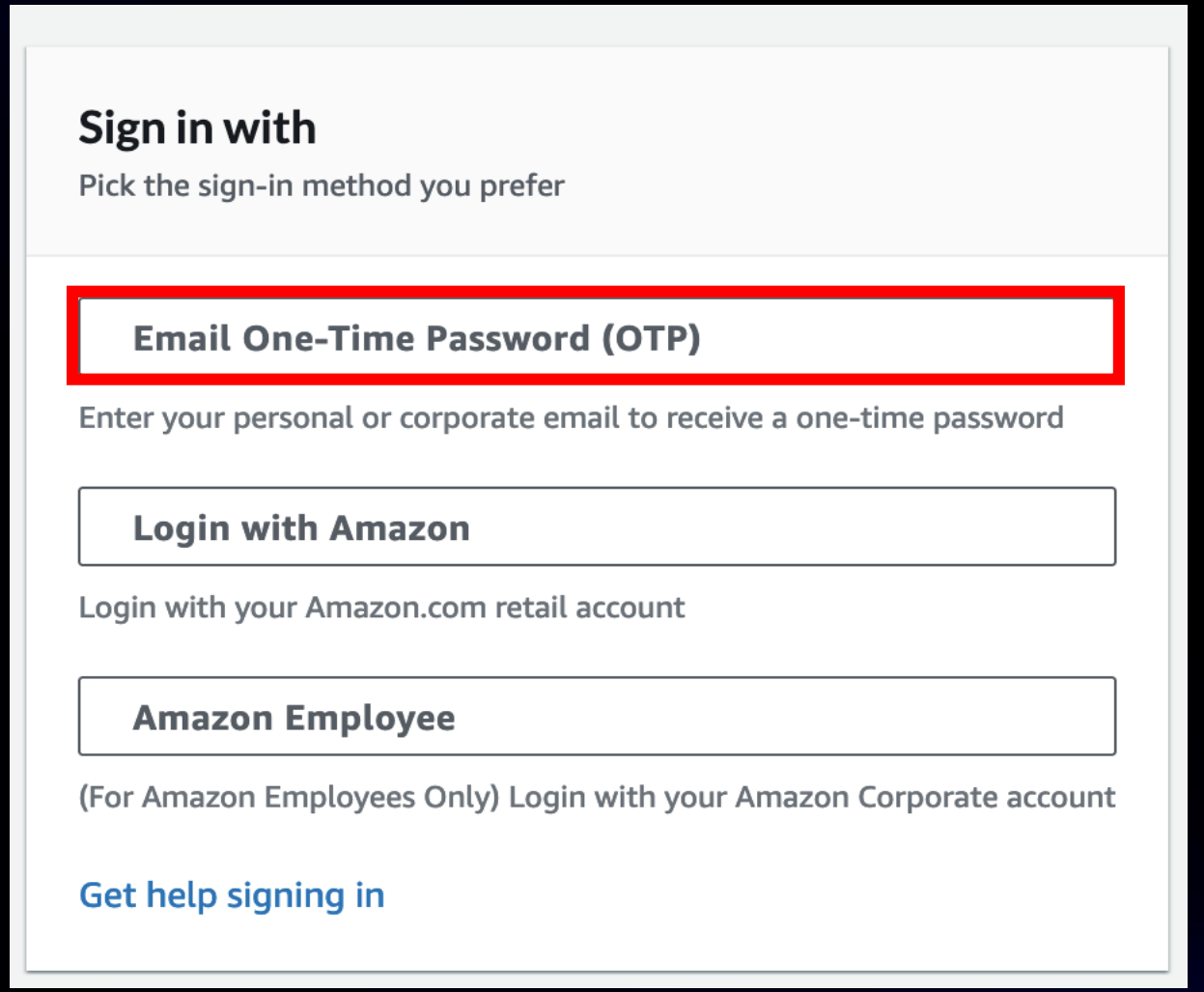
Event Engine



https://dashboard.eventengine.run

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

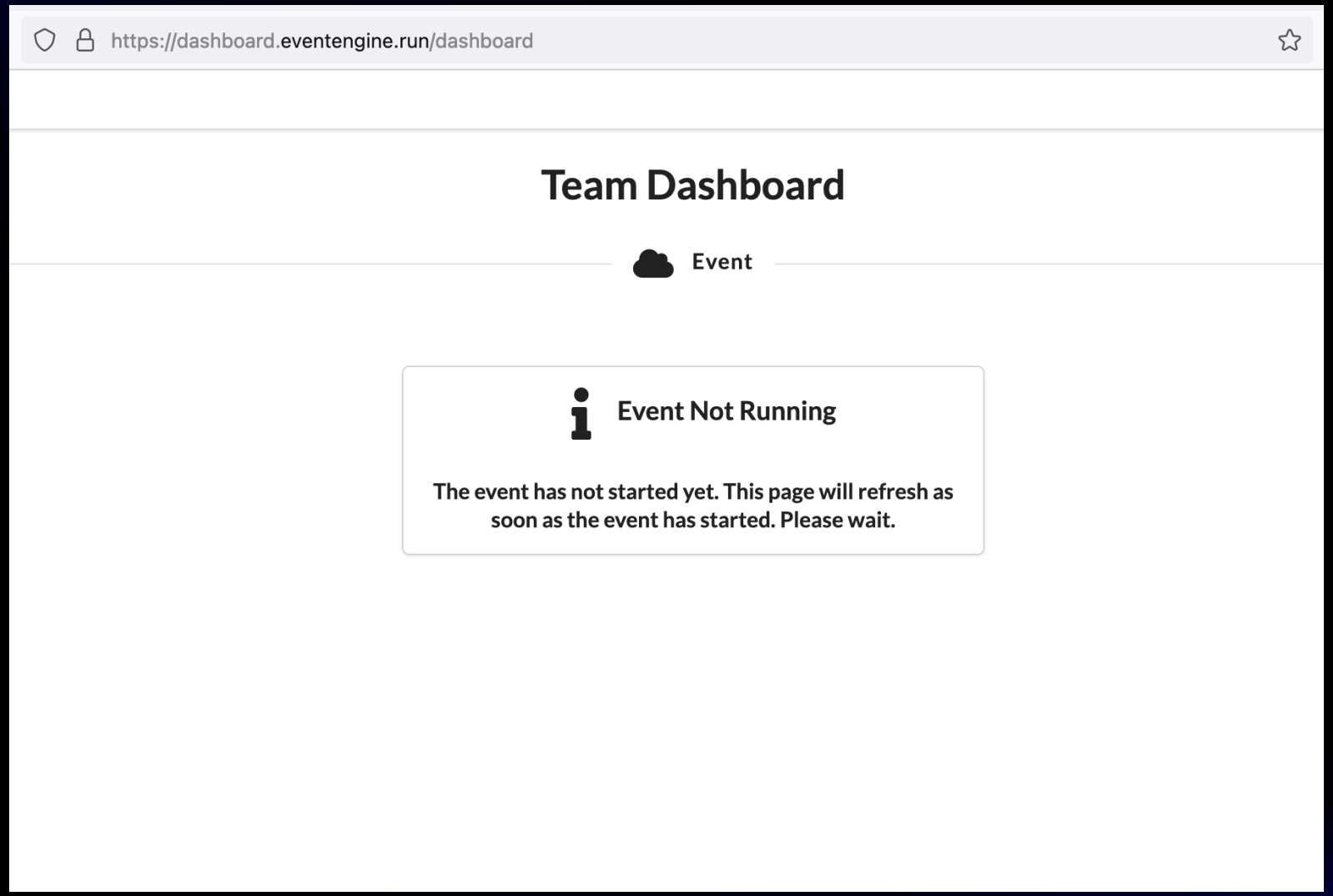
Event Engine



https://dashboard.eventengine.run

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

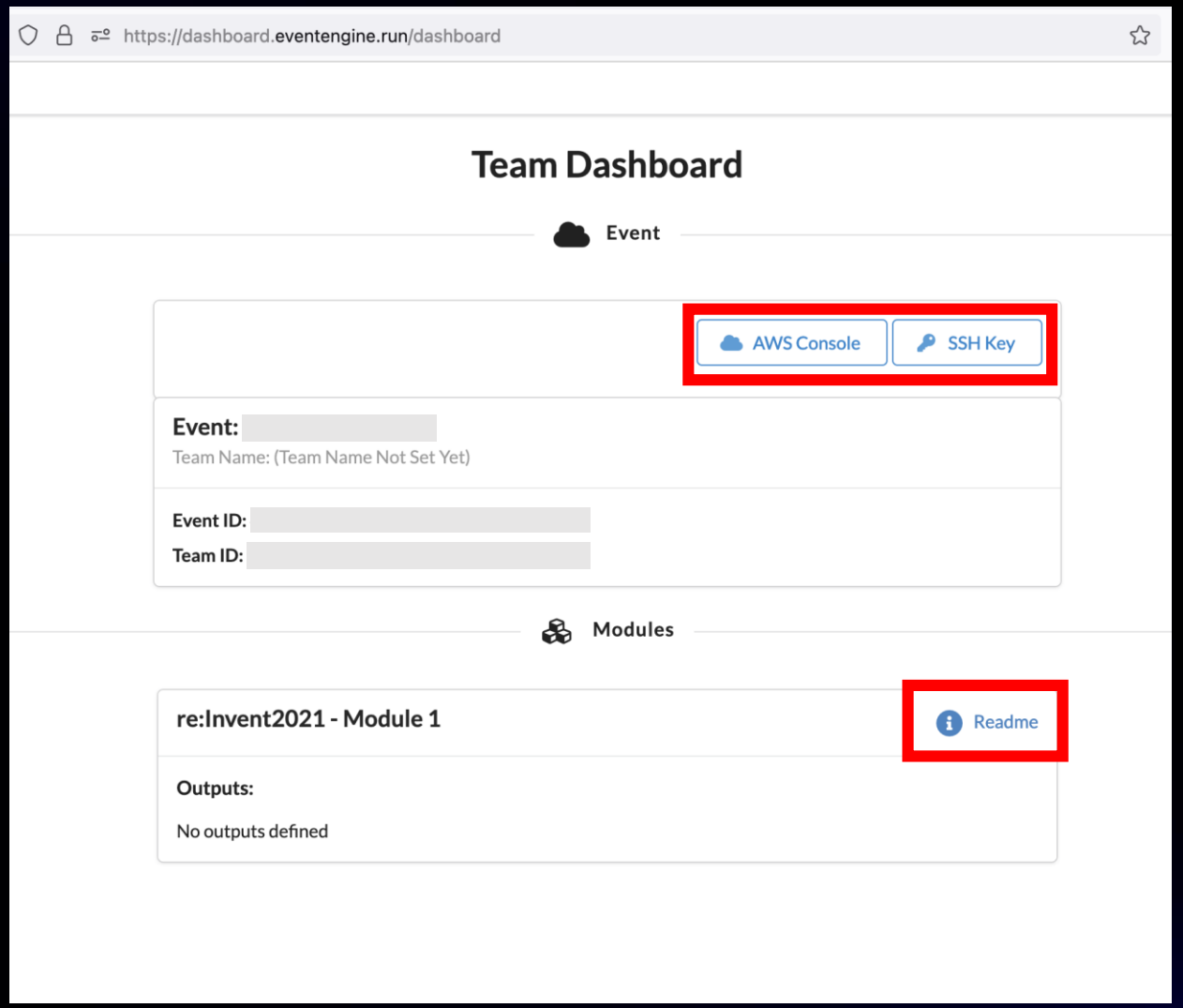
Event Engine



https://dashboard.eventengine.run

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

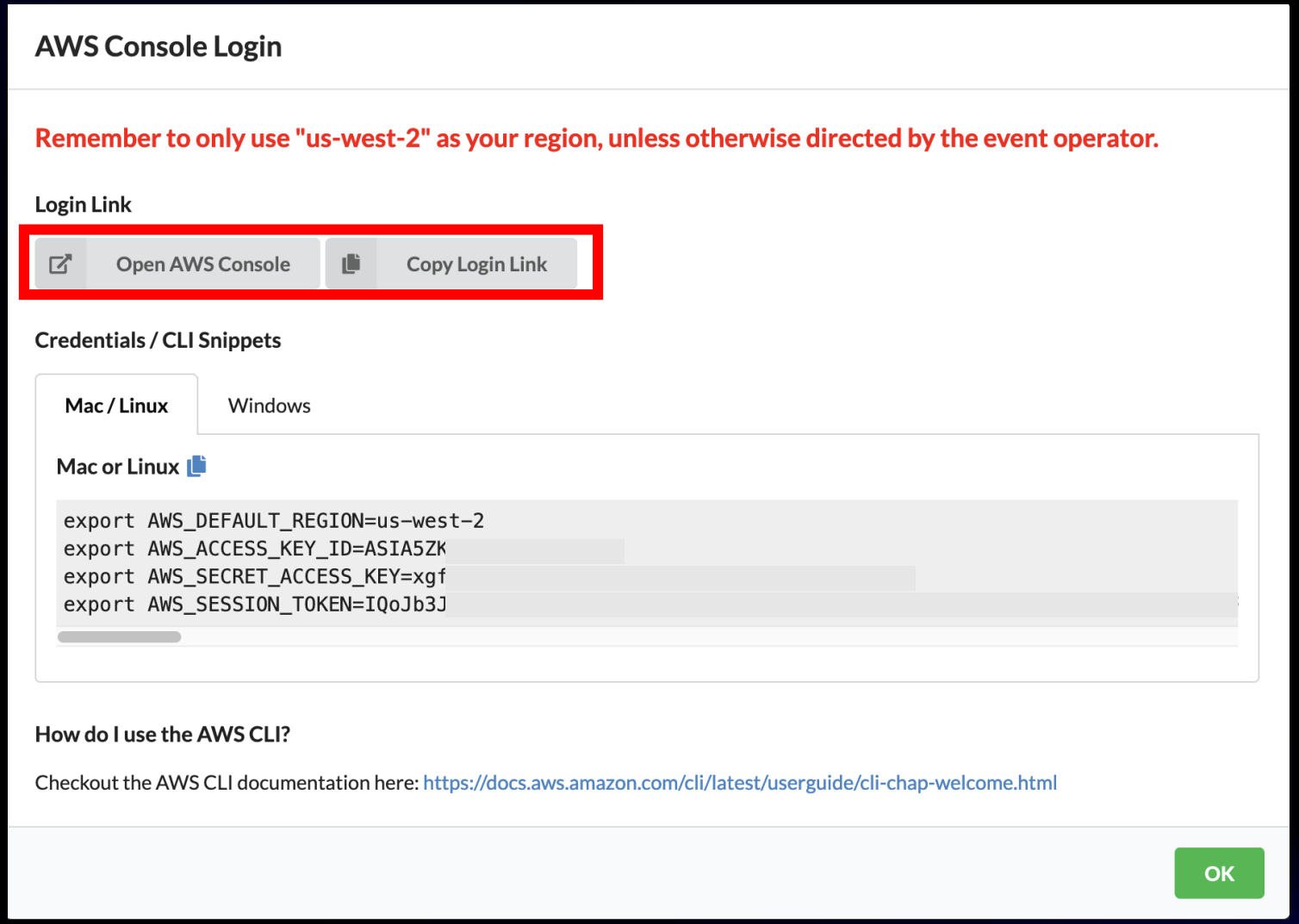
Event Engine



https://dashboard.eventengine.run

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

Event Engine



https://dashboard.eventengine.run

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

Workshop Overview

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

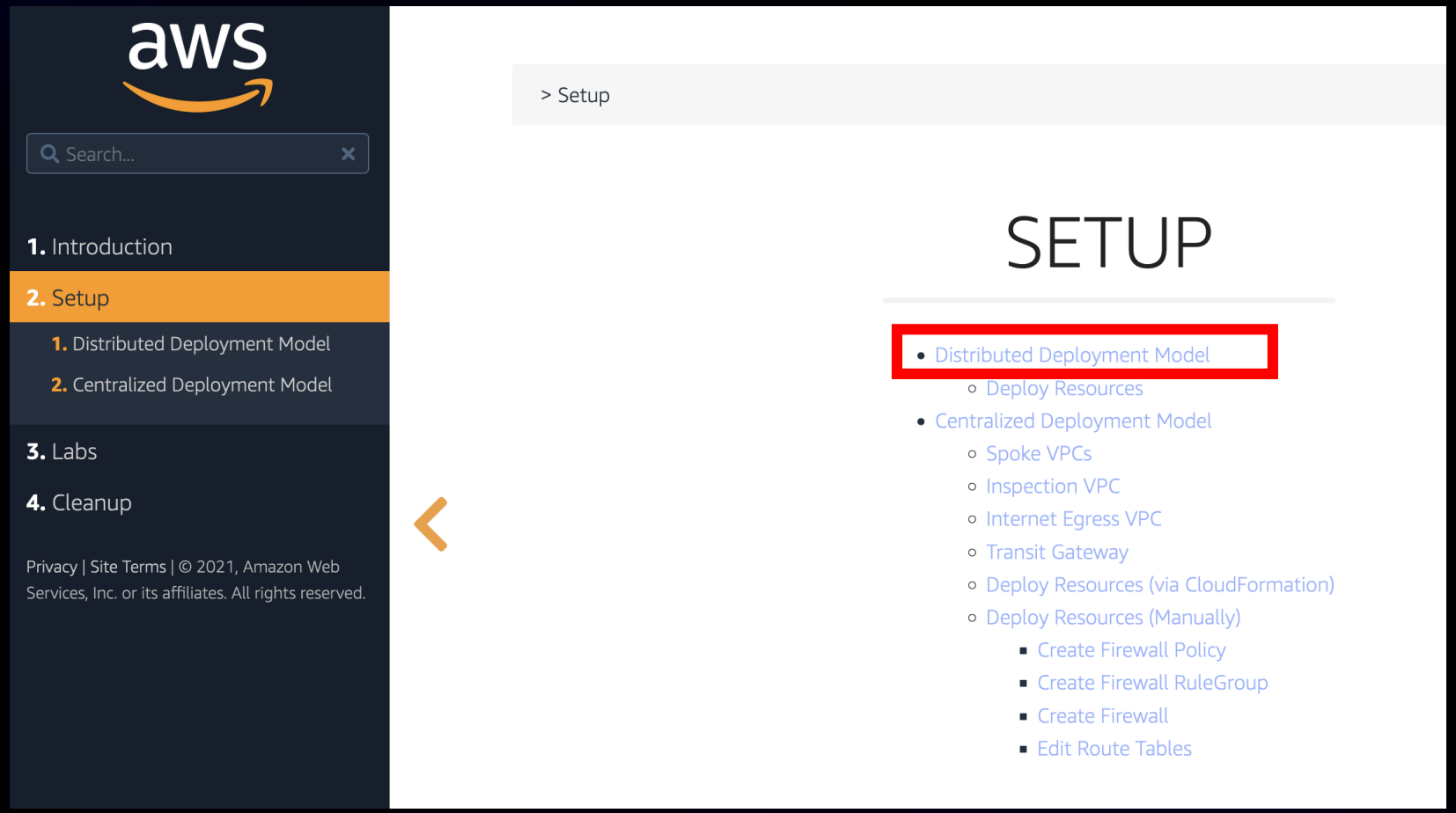
Workshop logistics

https://networkfirewall.workshop.aws



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

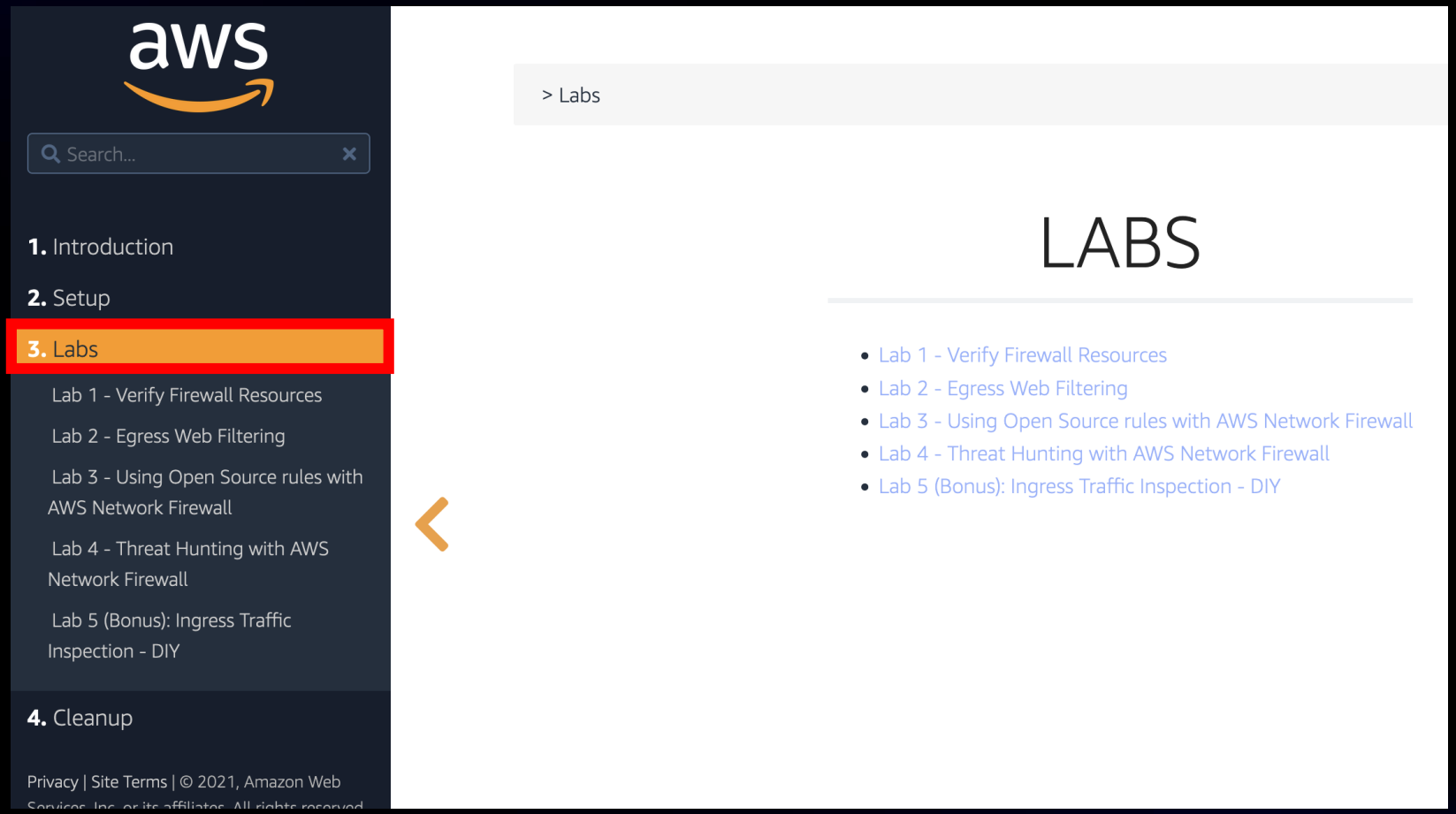
Workshop logistics



https://networkfirewall.workshop.aws

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

Workshop logistics



https://networkfirewall.workshop.aws

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

Thank you!

Pratik R. Mankad

pmankad@amazon.com
Sr. Specialist SA, Networking,
AWS

Shakeel Ahmad

shkahma@amazon.com
Sr. Specialist SA, Networking,
AWS

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