

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC302-R

AWS Network Firewall and DNS Firewall security in multi-VPC architectures

Anandprasanna Gaitonde (he/him)

Sr. Solutions Architect, Digital Native Business
AWS

Pratik Mankad (he/him)

Sr. Specialist Solutions Architect, Networking
AWS



Agenda

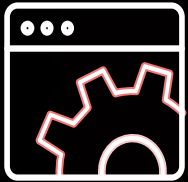
- AWS Network Firewall overview
- Deployment patterns
- DNS Firewall overview
- Event logistics
- Workshop overview

AWS Network Firewall



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

Network Firewall

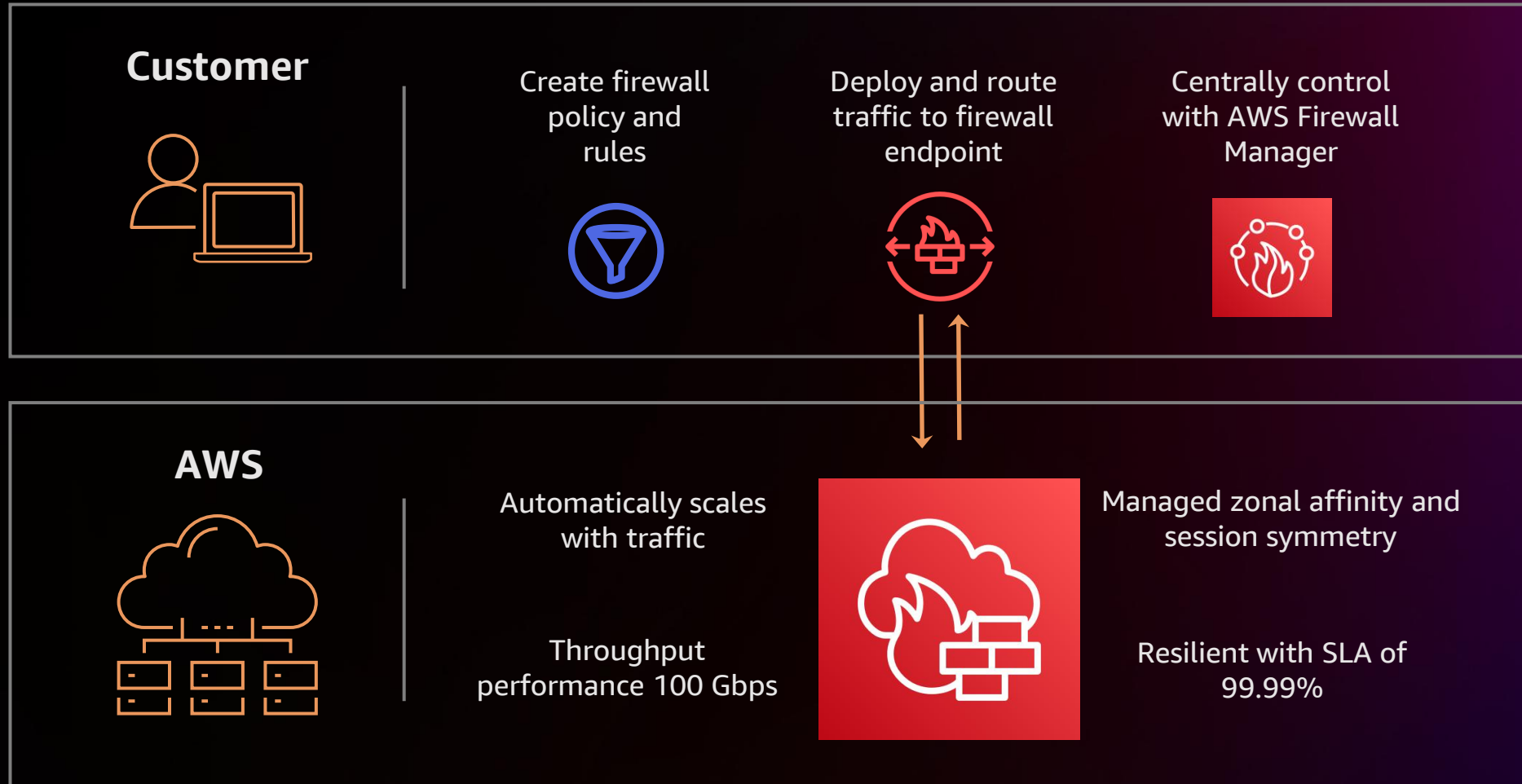
Managed infrastructure for high availability

Flexible protection through fine-grained controls

Consistent policy across VPCs and AWS accounts



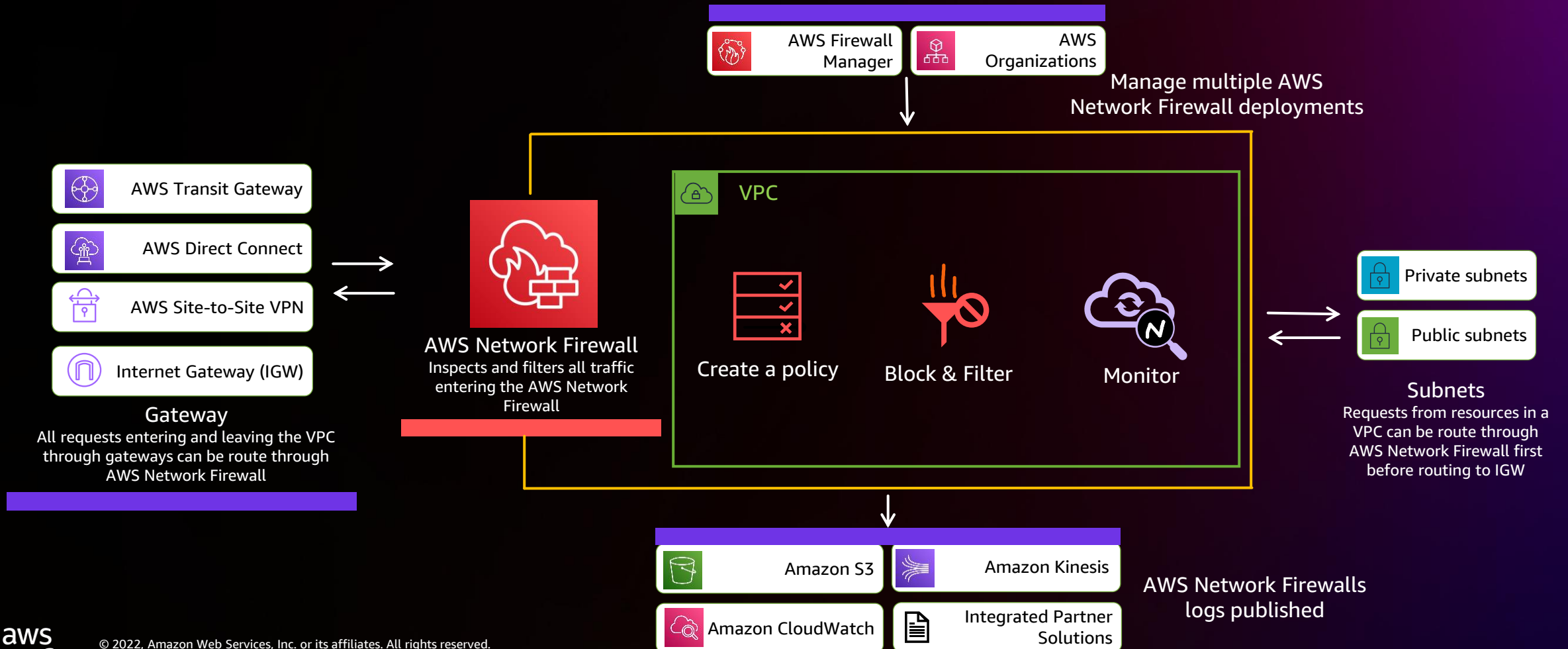
Network Firewall: At a glance



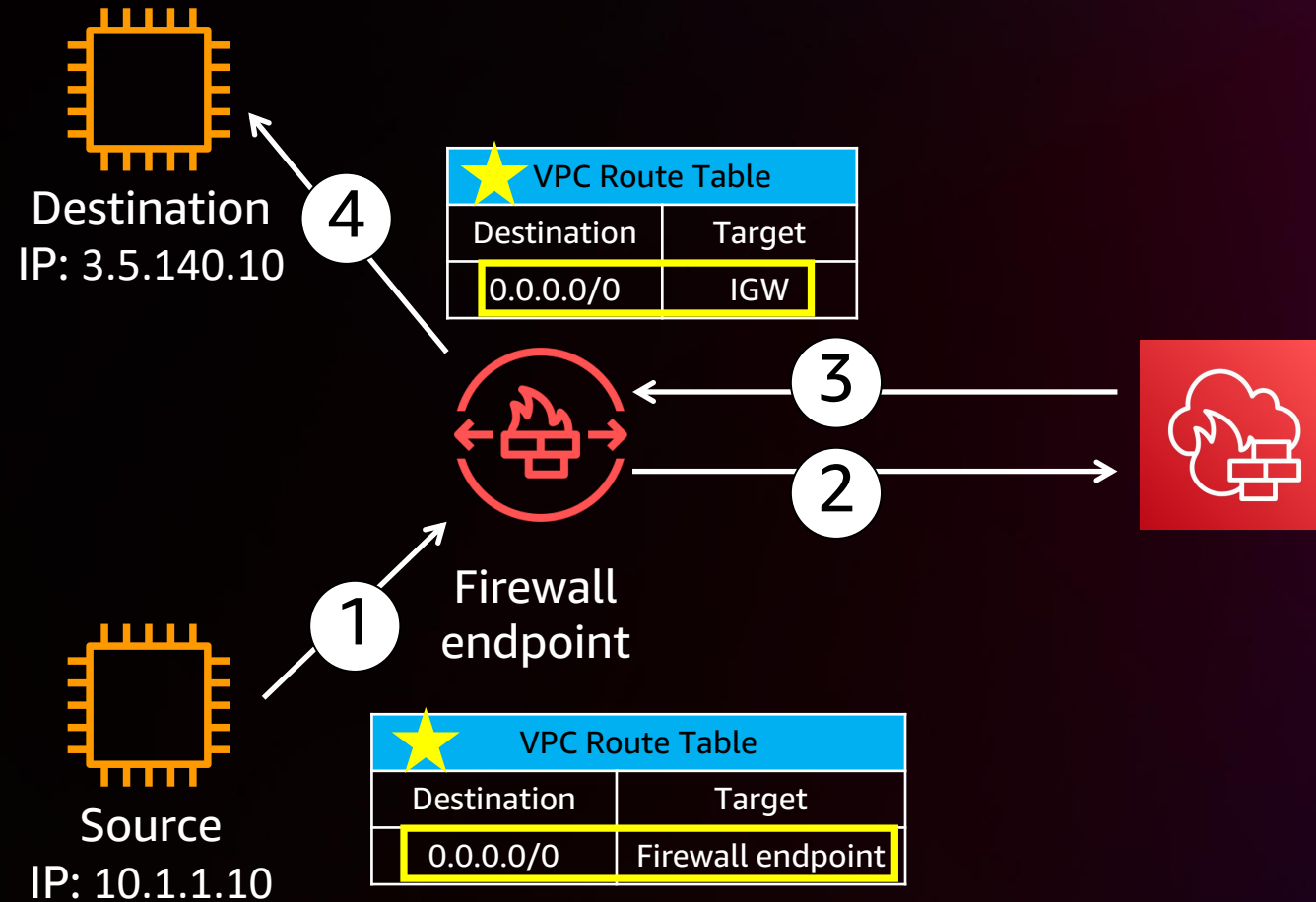
Architectural Constructs - AWS Network Firewall

AWS Network Firewall deploys essential network protections for your Amazon VPCs

It's a managed service that scales automatically with your network traffic, so you don't have to worry about deploying and managing any infrastructure



Routing traffic to and from the firewall



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

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

Central management

- Cross-account management and rule visibility using AWS Firewall Manager
- AWS CloudFormation and Terraform templates
- AWS Resource Access Manager (AWS RAM)

Network Firewall pricing

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

Network Firewall

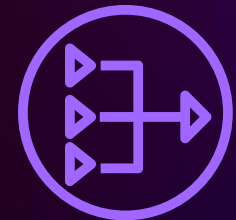
You pay an hourly rate for each firewall endpoint and a per-gigabyte rate for the amount of traffic processed by your firewall endpoint

- \$0.395/hour
- \$0.065/GB



AWS NAT gateway

If you choose to create a 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



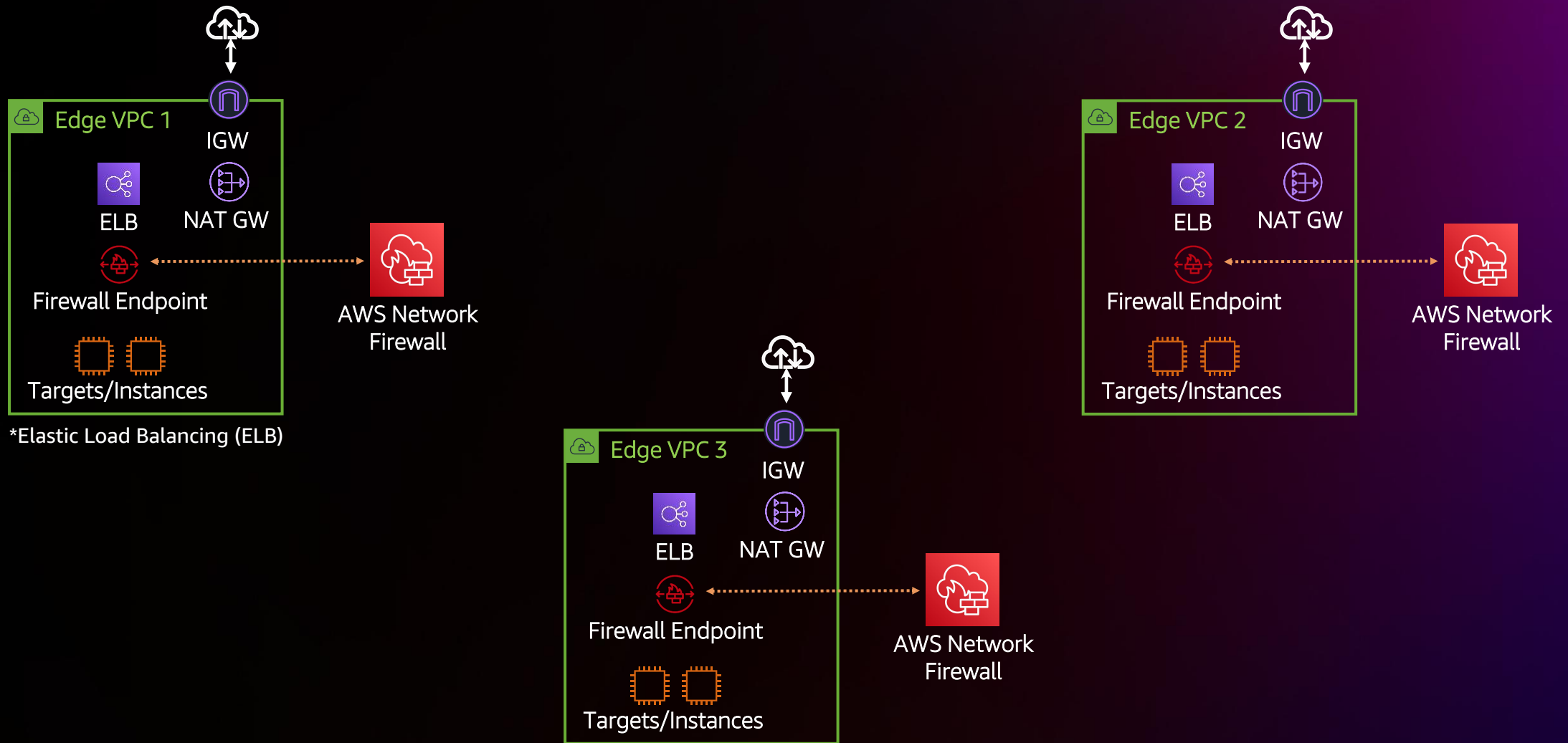
Network Firewall and other AWS security services

	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

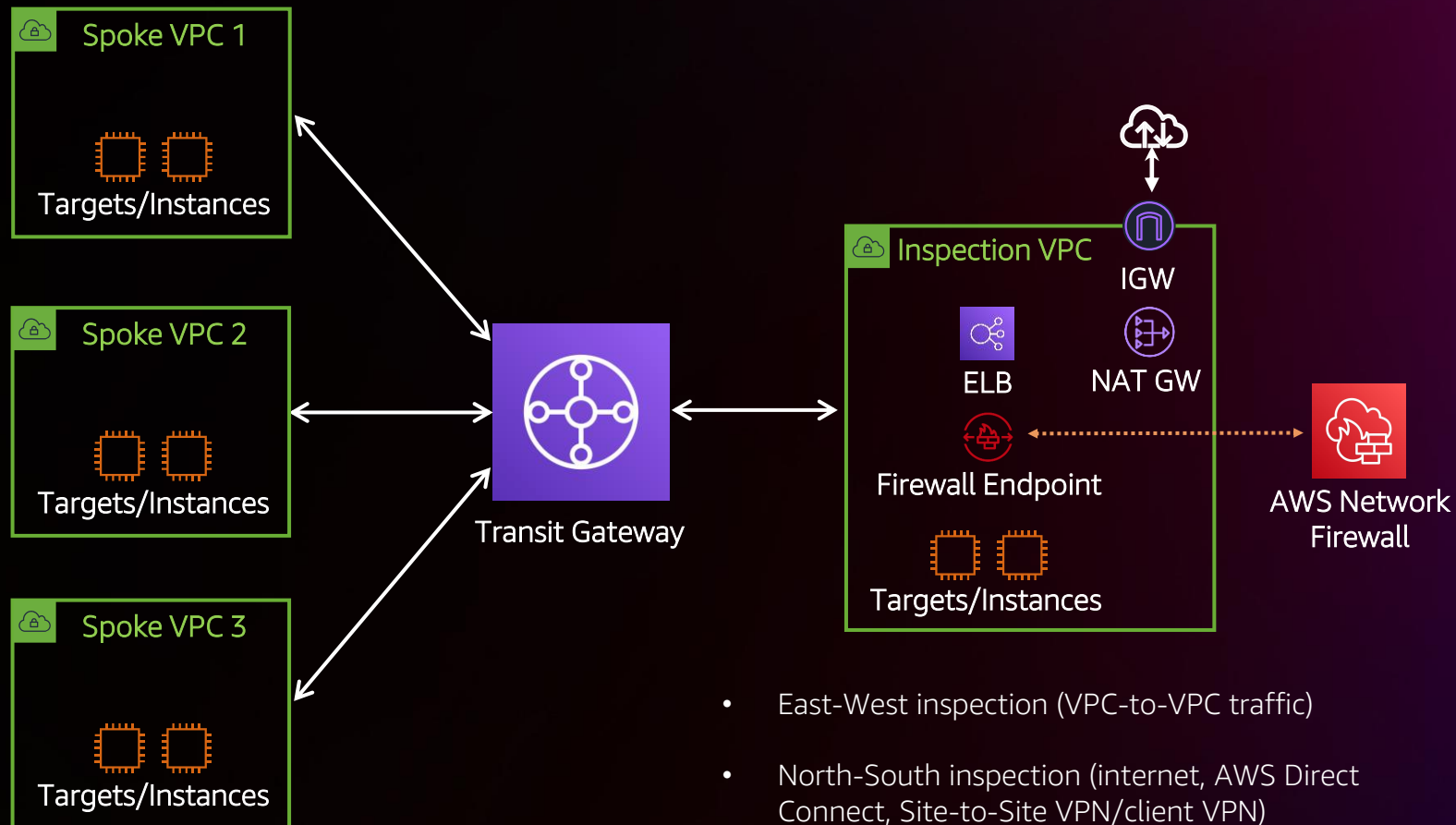
Deployment patterns



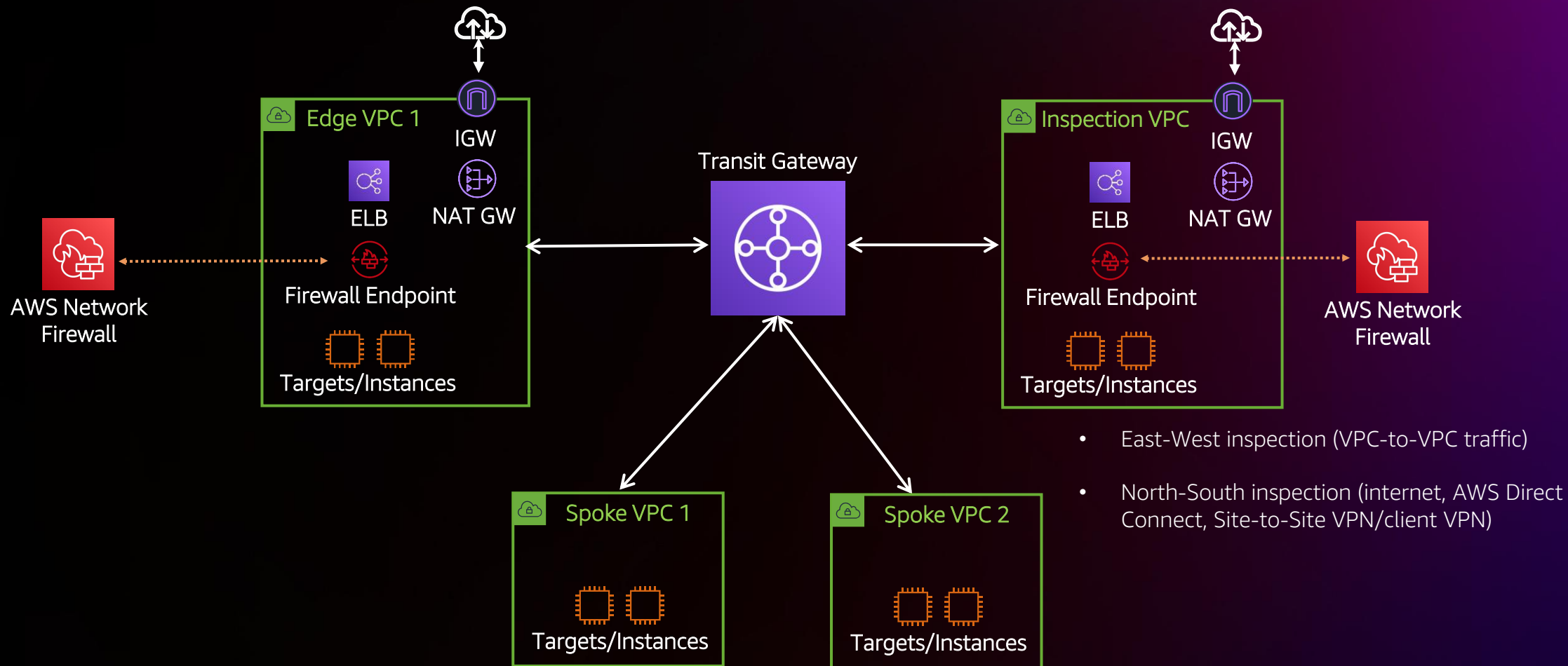
Distributed deployment model



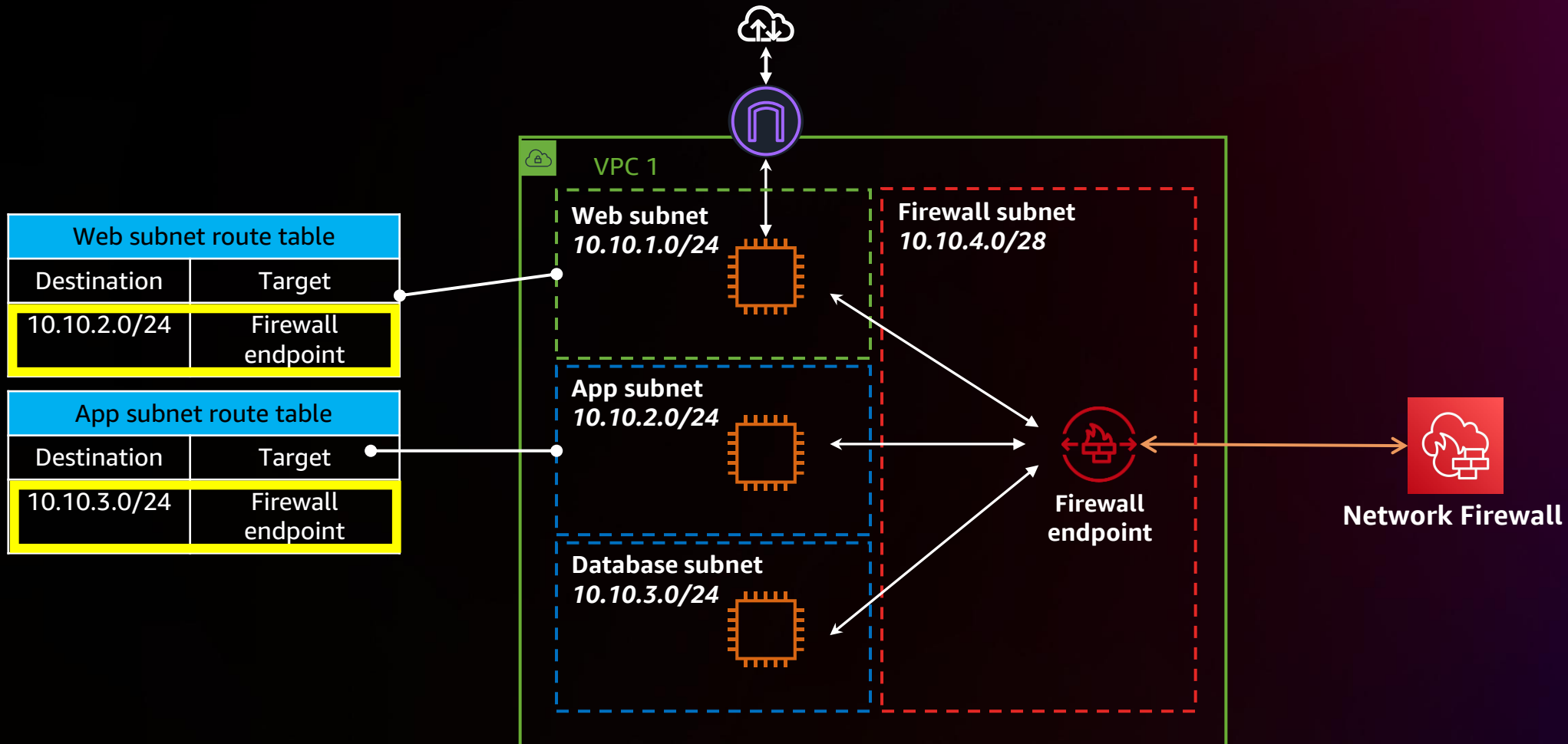
Centralized deployment model



Combined deployment model



Network Firewall with VPC routing enhancements



Deployment model resources

Blog post, part 1:
“Deployment models for AWS
Network Firewall”



Blog post, part 2: “Deployment
models for AWS Network Firewall
with VPC routing enhancements”



Amazon Route 53 DNS Firewall



Amazon Route 53 Resolver DNS Firewall

Firewall for Route 53 Resolver

Easily deny/allow DNS traffic across all
VPCs centrally

Highly available, managed service



DNS Firewall features

DNS filtering

- Domain name-based filtering
- Create denylists, allowlists
- Custom deny actions: NXDOMAIN, OVERRIDE, NoData
- Filtering on Resolver and Resolver endpoints

Managed rules

- Domain name-based lists managed by AWS
- Provide protection against:
 - Malware
 - Botnet command and control (C&C)

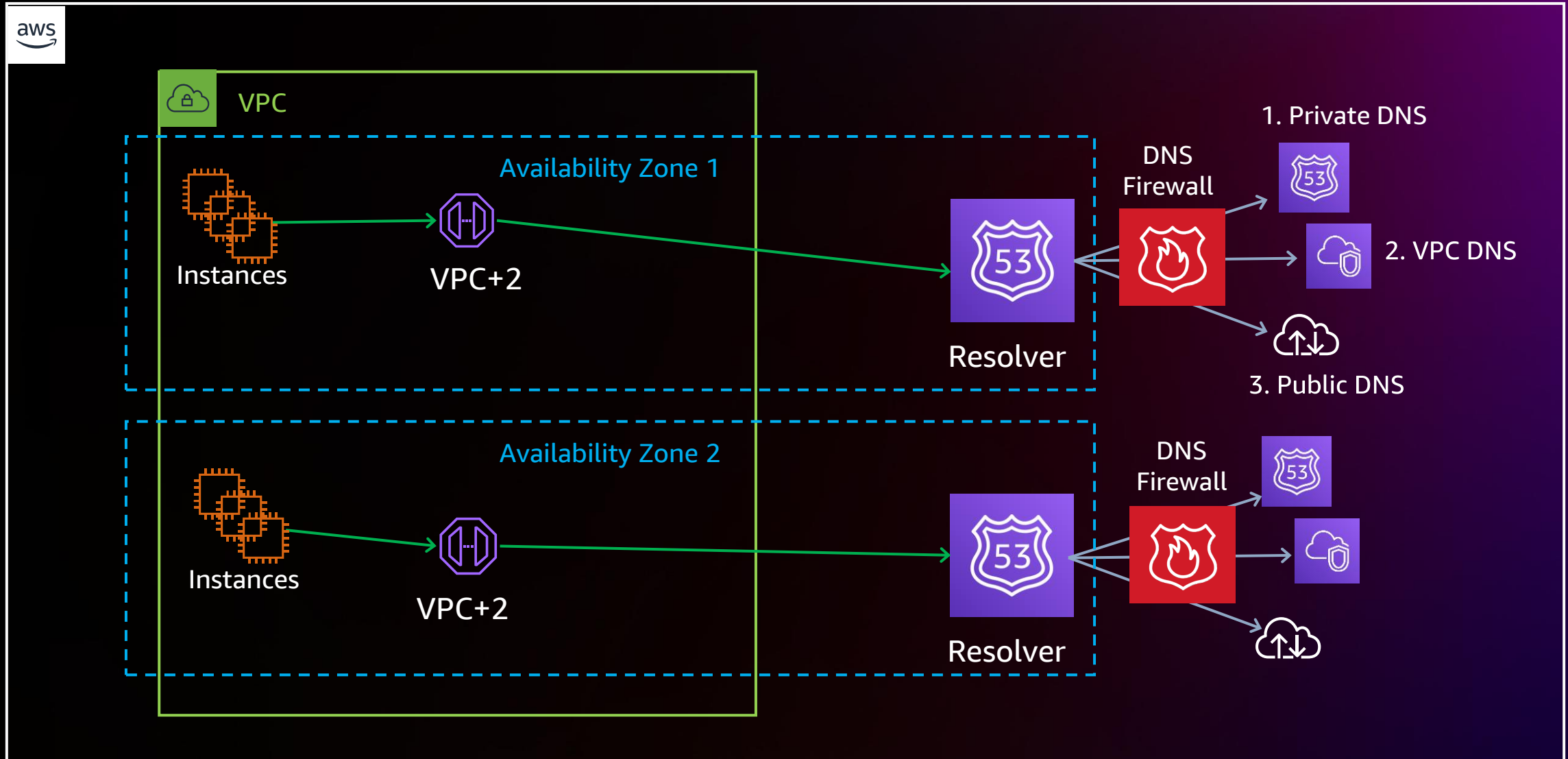
Central management

- Cross-account management using AWS Firewall Manager
- Ensure consistent enforcement of policies
- Rule visibility and management

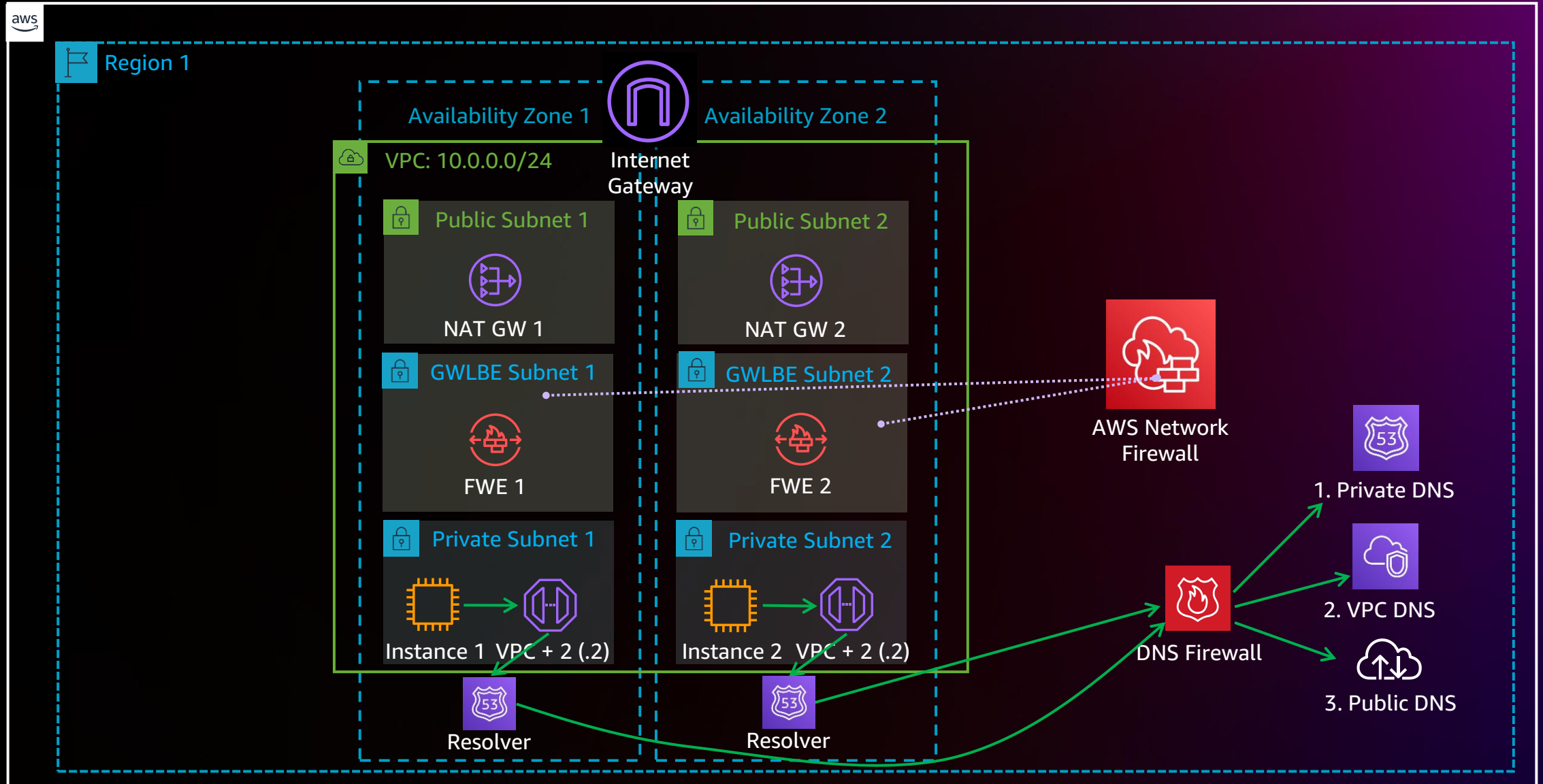
Visibility and reporting

- Per-rule CloudWatch metrics
- Configurable logs sent to Amazon S3, CloudWatch, Kinesis (enabled by VPC query logging)

Deployment model



Architecture: AWS Network Firewall + DNS Firewall



Route 53 DNS Firewall pricing

<https://aws.amazon.com/route53/pricing/>

Domain names

- Fee for each domain name stored in a domain list within a rule group – \$0.0005 per month (prorated hourly)
- No fees are charged for domain names within managed domain lists

Queries

- DNS queries originating from within VPCs that have firewall rule group associations
- DNS queries traversing inbound Resolver endpoints from on-premises networks into VPCs that have firewall rule group associations.

\$0.60 per million queries processed – first 1 billion queries/month

\$0.40 per million queries processed – over 1 billion queries/month



Event logistics



Getting started with this workshop

- As a participant, you will have access to an AWS account with any optional pre-provisioned infrastructure and IAM policies needed to complete this workshop.
- The AWS account will only be available for the duration of this workshop. You will lose access to the account thereafter.
- The optional pre-provisioned infrastructure will be deployed to a specific region. Check your workshop content to determine whether other regions will be used.
- Be sure to review the terms and conditions of the event. Do not upload any personal or confidential information in the account.

Step 1: Sign in via your preferred method

<https://catalog.workshops.aws/join>



aws workshop studio

Workshop Studio > Sign in

Sign in

Choose a preferred sign-in method

Email one-time password (OTP)

Enter your personal or corporate email to receive a one-time password

Login with Amazon

Login with your Amazon.com retail account

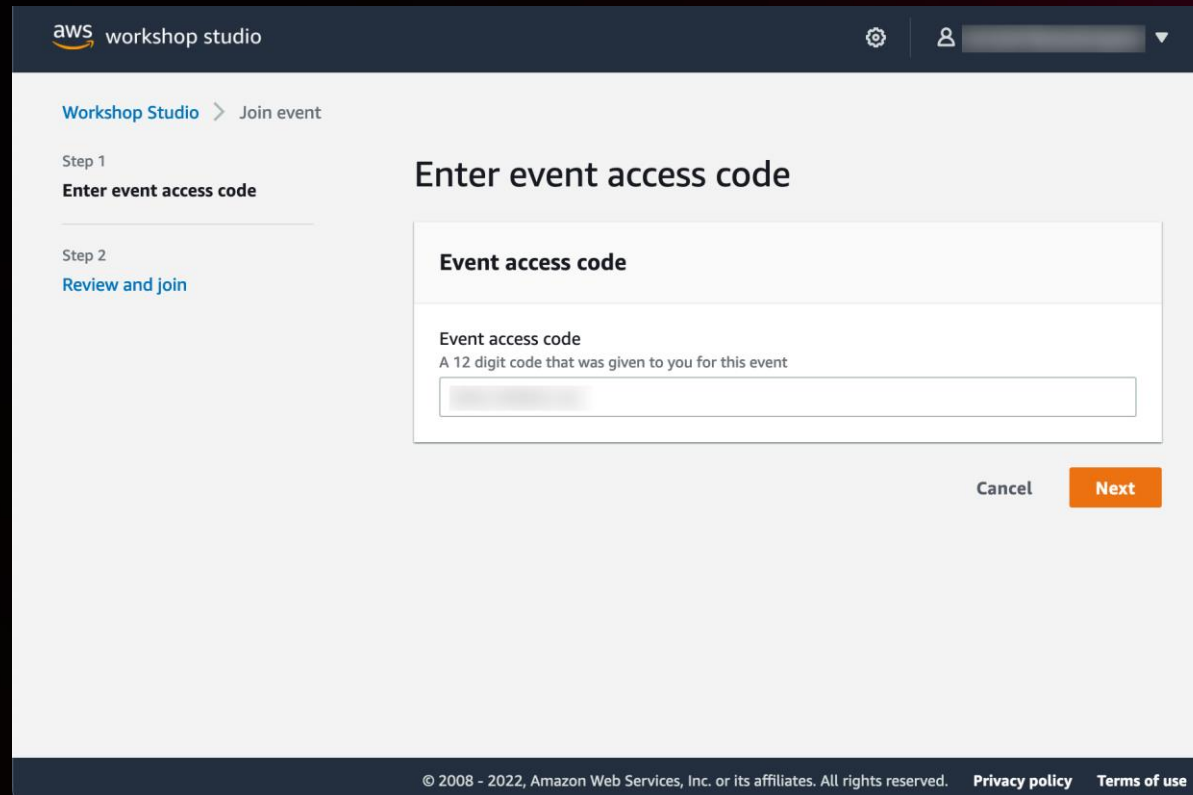
Amazon employee

Login with your Amazon Corporate account. Only for Amazon Employees.

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy policy](#) [Terms of use](#)

Step 2: Enter event access code

Enter the 12-digit event access code. If you were given a one-click join link, you can skip this step.



The screenshot shows the AWS Workshop Studio interface for joining an event. The top navigation bar includes the AWS logo, 'workshop studio', a settings gear icon, and a user profile icon. The breadcrumb trail is 'Workshop Studio > Join event'. On the left, a progress indicator shows 'Step 1 Enter event access code' as the current step and 'Step 2 Review and join' as the next step. The main heading is 'Enter event access code'. Below this, a box titled 'Event access code' contains the text 'Event access code' and 'A 12 digit code that was given to you for this event', followed by a text input field. At the bottom right of the form are 'Cancel' and 'Next' buttons. The footer contains copyright information and links to 'Privacy policy' and 'Terms of use'.

aws workshop studio

Workshop Studio > Join event

Step 1
Enter event access code

Step 2
[Review and join](#)

Enter event access code

Event access code




Event access code
A 12 digit code that was given to you for this event

[Cancel](#) [Next](#)

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy policy](#) [Terms of use](#)

Step 3: Review terms and join event

aws workshop studio

[Workshop Studio](#) > [Join event](#)

Step 1

[Enter event access code](#)

Step 2

Review and join

Review and join

Event details

Name	Start time	Duration	Level
AWS Network Firewall Workshop	11/07/2022 01:19 PM	48 hours	-

Description

This is an event facilitated to allow users to get hands on with AWS Network Firewall and Amazon Route 53 Resolver DNS Firewall.

Terms and Conditions

Read and accept before joining the event

1. By using AWS Workshop Studio for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.
2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivative works of materials provided by AWS, including but not limited to, data sets.
3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.
4. Your use of AWS Workshop Studio will comply with these terms and all applicable laws, and your access to AWS Workshop Studio will immediately and automatically terminate if you do not comply with any of these terms or conditions.

☒ I agree with the Terms and Conditions

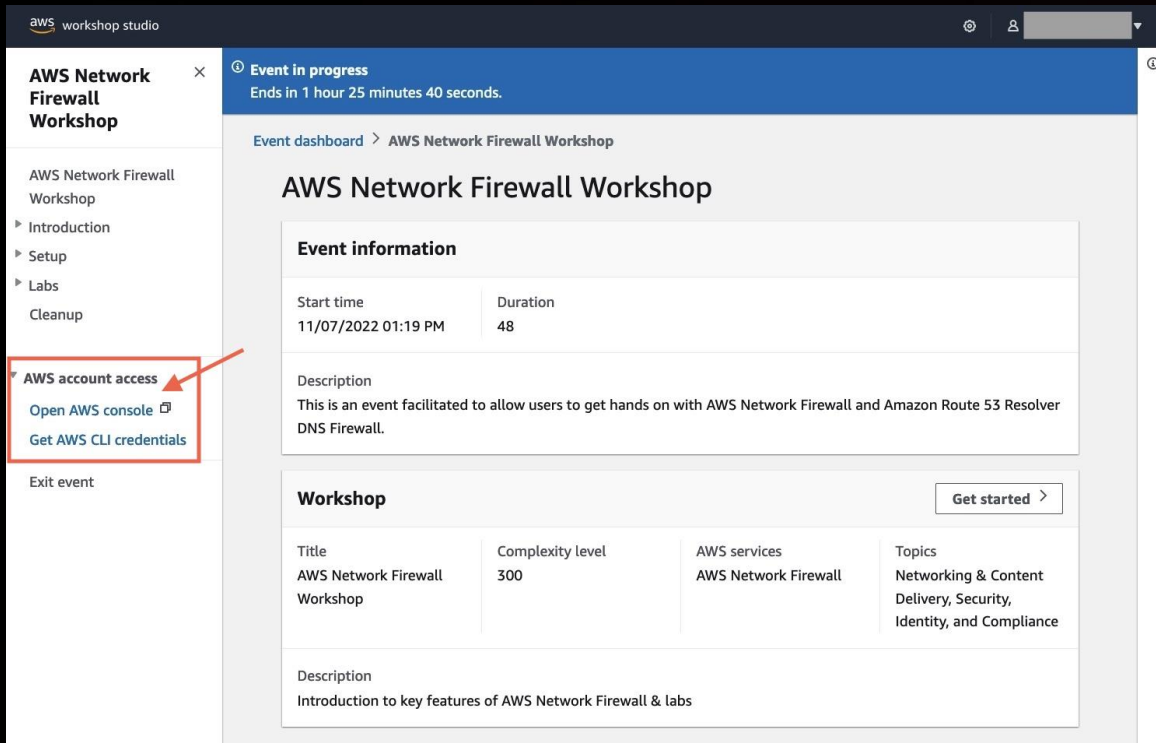
Cancel

Previous

Join event

Step 4: Access AWS account

Access the AWS console, or generate AWS Command Line Interface (AWS CLI) credentials as needed



The screenshot shows the AWS Workshop Studio interface. On the left sidebar, under the 'AWS Network Firewall Workshop' section, the 'AWS account access' link is highlighted with a red box and an arrow. The main content area displays the 'AWS Network Firewall Workshop' details, including event information and a workshop description.

Event information

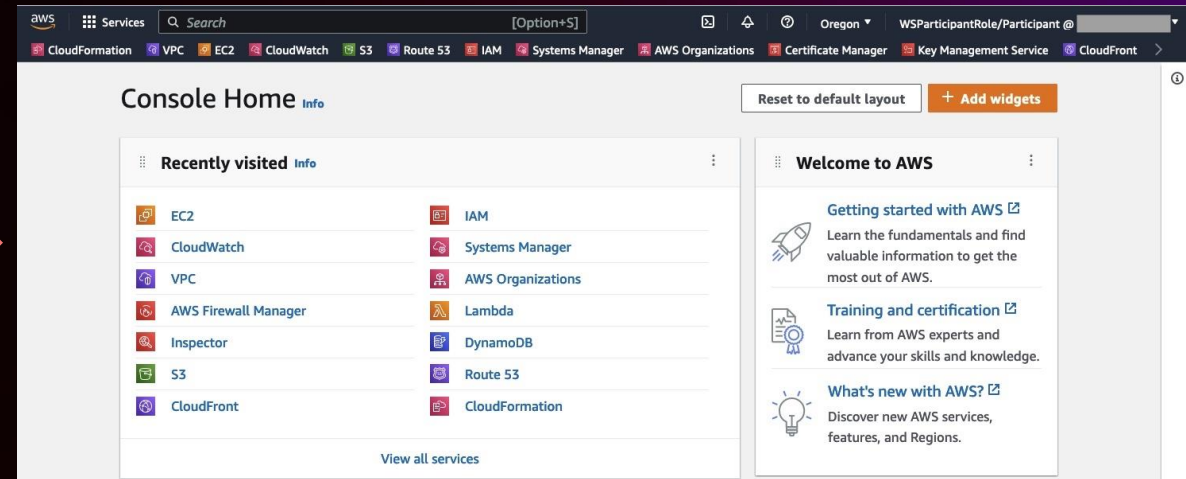
Start time	Duration
11/07/2022 01:19 PM	48

Description
This is an event facilitated to allow users to get hands on with AWS Network Firewall and Amazon Route 53 Resolver DNS Firewall.

Workshop

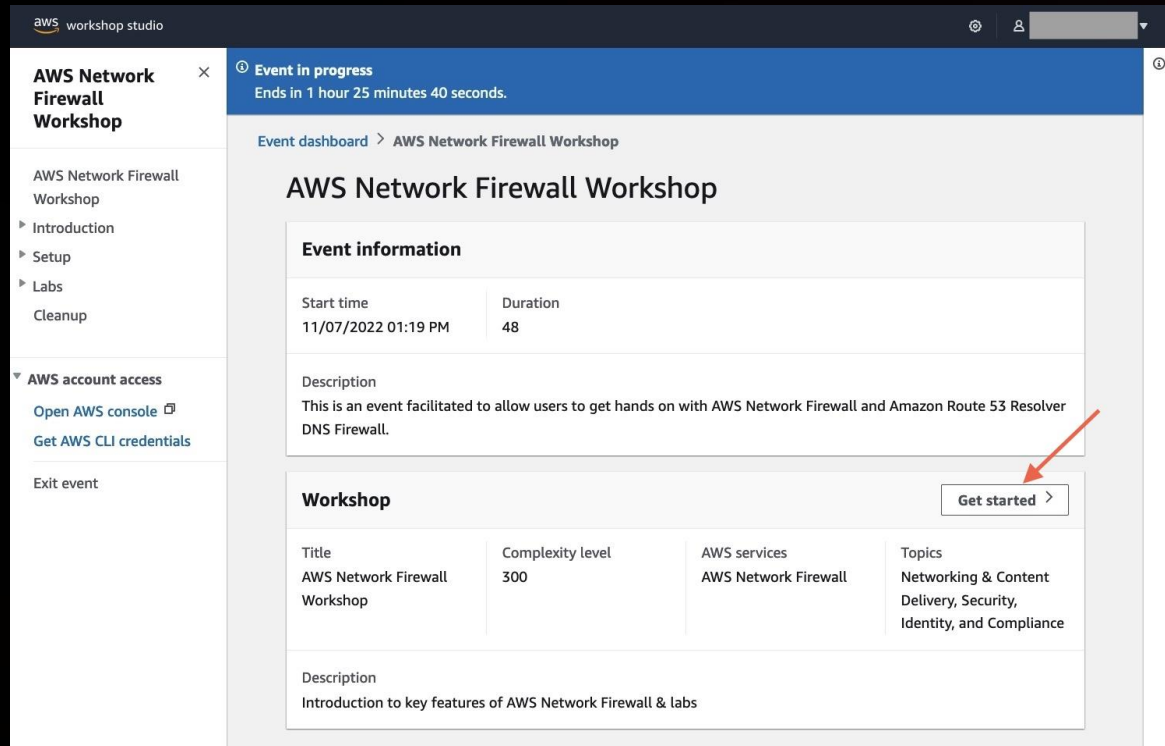
Title	Complexity level	AWS services	Topics
AWS Network Firewall Workshop	300	AWS Network Firewall	Networking & Content Delivery, Security, Identity, and Compliance

Description
Introduction to key features of AWS Network Firewall & labs



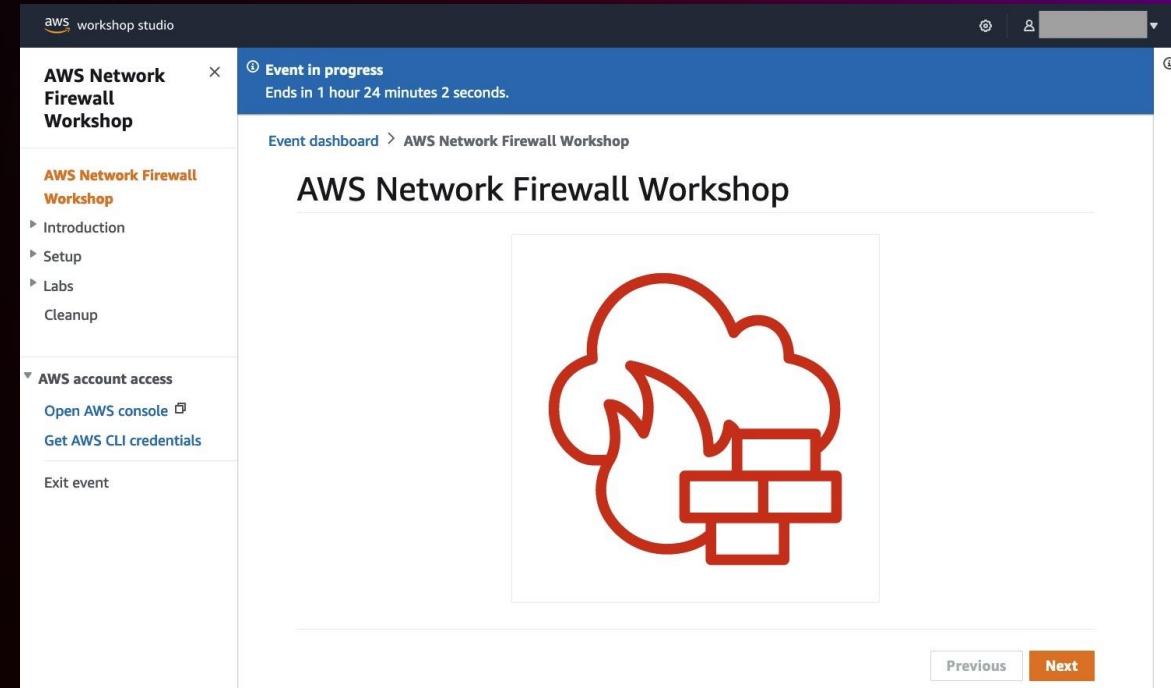
The screenshot shows the AWS Console Home page. The 'Recently visited' section lists various AWS services, including EC2, CloudWatch, VPC, AWS Firewall Manager, Inspector, S3, CloudFront, IAM, Systems Manager, AWS Organizations, Lambda, DynamoDB, Route 53, and CloudFormation. The 'Welcome to AWS' section provides links to 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. A red arrow points from the 'Open AWS console' link in the workshop studio to this console home page.

Step 5: Get started with the workshop



The screenshot shows the 'AWS Network Firewall Workshop' page in the AWS Workshop Studio. The left sidebar contains a navigation menu with sections: 'AWS Network Firewall Workshop' (containing Introduction, Setup, Labs, Cleanup), 'AWS account access' (containing Open AWS console, Get AWS CLI credentials), and 'Exit event'. The main content area has a blue header bar indicating 'Event in progress' and 'Ends in 1 hour 25 minutes 40 seconds.' Below this is the 'Event dashboard > AWS Network Firewall Workshop' breadcrumb. The main title is 'AWS Network Firewall Workshop'. Under 'Event information', there is a table with 'Start time' (11/07/2022 01:19 PM) and 'Duration' (48). A description follows: 'This is an event facilitated to allow users to get hands on with AWS Network Firewall and Amazon Route 53 Resolver DNS Firewall.' Below this is a 'Workshop' section with a table containing details about the workshop, including its title, complexity level, AWS services, and topics. A 'Get started >' button is located at the bottom right of the workshop table, with a red arrow pointing to it.

Event information			
Start time	Duration		
11/07/2022 01:19 PM	48		
Description This is an event facilitated to allow users to get hands on with AWS Network Firewall and Amazon Route 53 Resolver DNS Firewall.			
Workshop			
Title	Complexity level	AWS services	Topics
AWS Network Firewall Workshop	300	AWS Network Firewall	Networking & Content Delivery, Security, Identity, and Compliance
Description Introduction to key features of AWS Network Firewall & labs			



The screenshot shows the 'AWS Network Firewall Workshop' page in the AWS Workshop Studio, which is the 'Next' page after clicking 'Get started'. The left sidebar is identical to the first screenshot. The main content area has a blue header bar indicating 'Event in progress' and 'Ends in 1 hour 24 minutes 2 seconds.' Below this is the 'Event dashboard > AWS Network Firewall Workshop' breadcrumb. The main title is 'AWS Network Firewall Workshop'. A large red outline icon of a cloud with server racks inside is displayed in the center. At the bottom right, there are 'Previous' and 'Next' buttons.

Workshop overview



Workshop logistics

<https://catalog.workshops.aws/networkfirewall>



Workshop logistics

AWS Network Firewall Workshop ✕

► Introduction

▼ Setup

► Distributed Deployment Model

▼ Centralized Deployment Model

Spoke VPCs

Inspection VPC

Internet Egress VPC

Transit Gateway

Deploy Resources

► Deploy Resources (Manually)

▼ Labs

Lab 1 - Verify Firewall Resources

Lab 2 - Egress Web Filtering


Lab 2.1 - Egress DNS Query filtering

Lab 3 - Using Open Source rules with AWS Network Firewall

Lab 4 - Threat Hunting with AWS Network Firewall

AWS Network Firewall Workshop

AWS Network Firewall Workshop



Previous

Next

Workshop logistics

AWS Network Firewall Workshop ✕

▶ Introduction

▼ Setup

- ▶ Distributed Deployment Model
- ▶ Centralized Deployment Model
- ▼ Labs
 - Lab 1 - Verify Firewall Resources
 - Lab 2 - Egress Web Filtering
 - Lab 2.1 - Egress DNS Query filtering
 - Lab 3 - Using Open Source rules with AWS Network Firewall
 - Lab 4 - Threat Hunting with AWS Network Firewall
 - ▶ Lab 5 (Optional): Ingress Traffic Inspection - DIY
 - ▶ Lab 6 (Optional): Custom Suricata rules with Strict Rule ordering

Cleanup

AWS Network Firewall Workshop > Labs

Labs

❗

- You can use either of the deployment models: Distributed Deployment Model or Centralized Deployment Model to go through the labs in this workshop.
- If you plan to deploy both the models in parallel, deploy the templates in separate AWS regions.
- Since both the templates create certain resources with the same name, deploying in the same region will cause a conflict and CloudFormation template for the subsequent deployment model will fail to deploy.

❗

- When running the workshop in your own account, make sure [VPC per region](#) quota does not affect you.
 - Distributed Deployment Model creates one additional VPC.
 - Centralized Deployment Model creates four additional VPCs.
 - Lab 5 creates another additional VPC.

- [Lab 1 - Verify Firewall Resources](#)
- [Lab 2 - Egress Web Filtering](#)
- [Lab 2.1 - Egress DNS Query filtering](#)
- [Lab 3 - Using Open Source rules with AWS Network Firewall](#)
- [Lab 4 - Threat Hunting with AWS Network Firewall](#)
- [Lab 5 \(Optional\): Ingress Traffic Inspection - DIY](#)
- [Lab 6 \(Optional\): Custom Suricata rules with Strict Rule ordering](#)

Event access code

- Event URL: <https://catalog.workshops.aws/join>
- Workshop URL: <https://catalog.workshops.aws/networkfirewall>
- Access Code: **0821-064a24-4e**
- After-session event support: anandprg@amazon.com/pmankad@amazon.com

Thank you!

Anandprasanna Gaitonde

[linkedin.com/in/anandprasannag/](https://www.linkedin.com/in/anandprasannag/)

Pratik Mankad

[linkedin.com/in/pratikrmankad/](https://www.linkedin.com/in/pratikrmankad/)



Please complete the session survey in the **mobile app**



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.