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

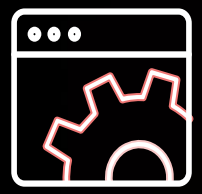
Agenda

- 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

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 100 Gbps

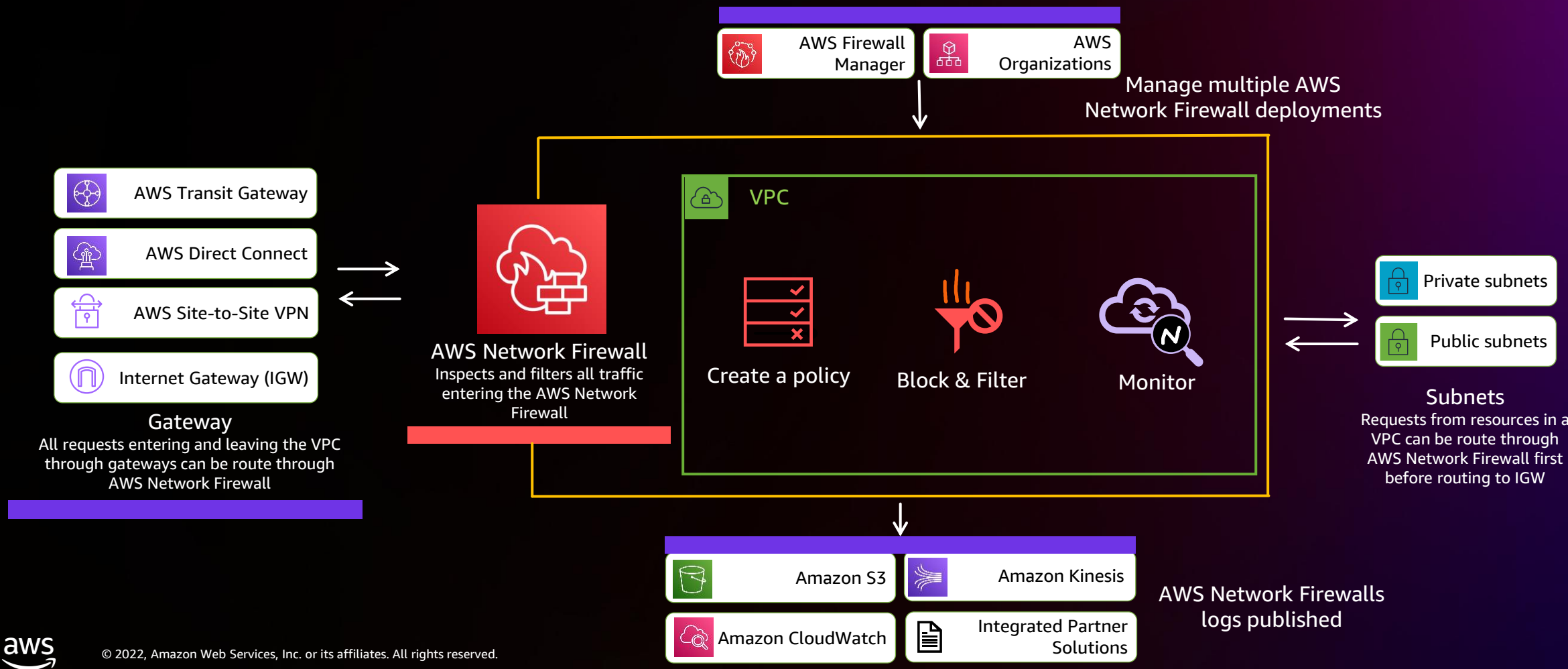
Managed zonal affinity and session symmetry

Resilient with SLA of 99.99%

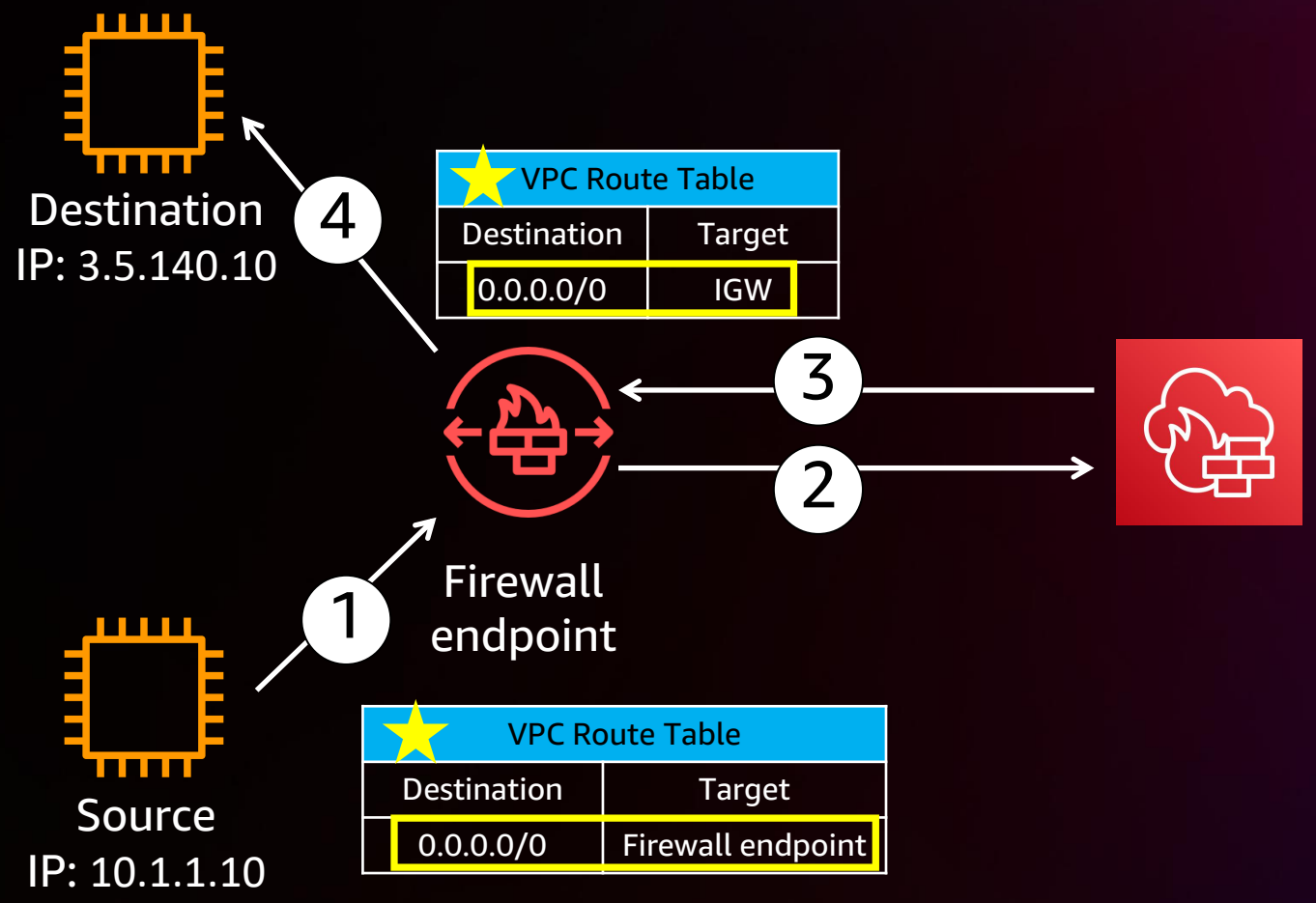
Architectural Constructs - AWS Network Firewall

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

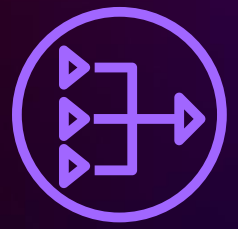
https://aws.amazon.com/network-firewall/pricing/

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



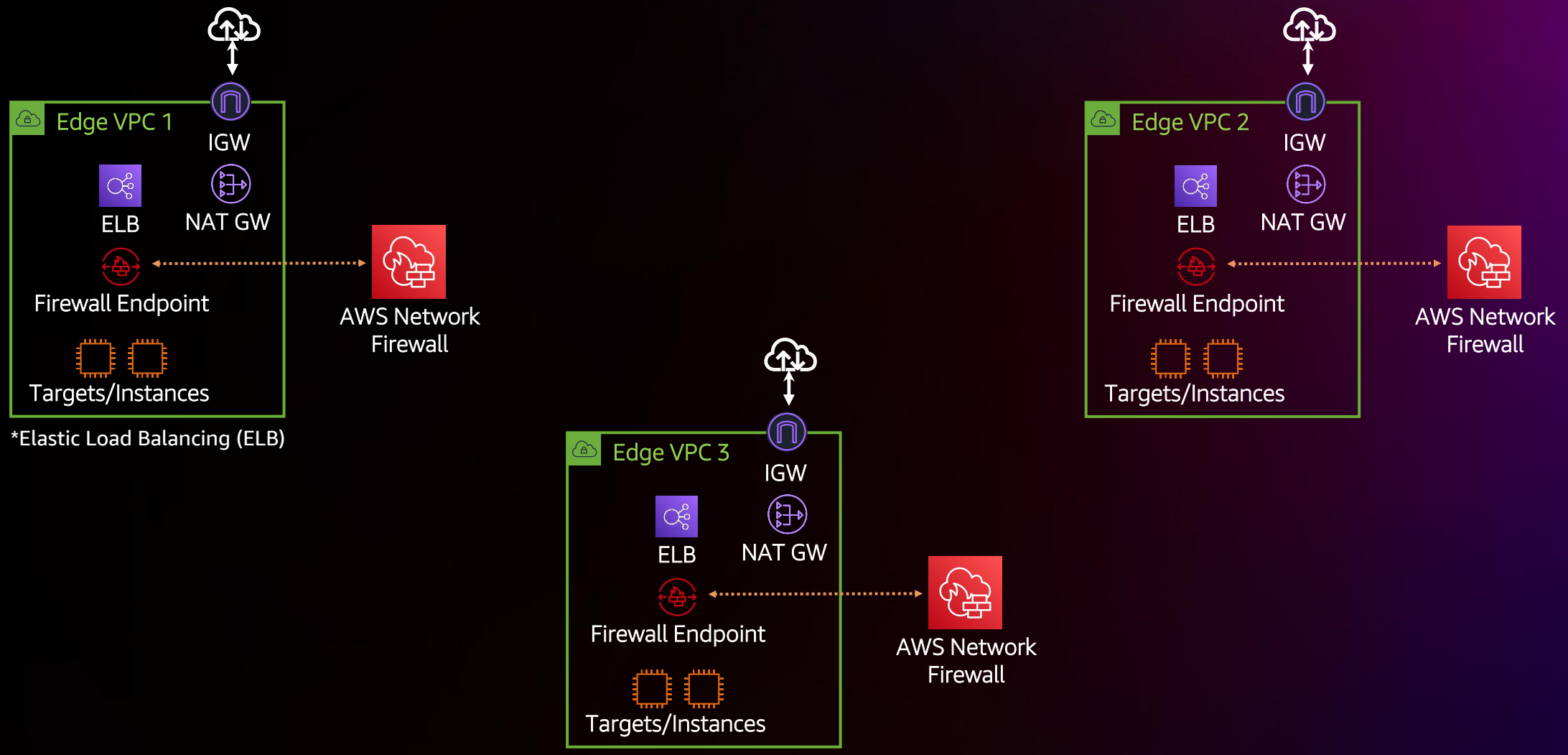
If you choose to create a NAT gateway in your VPC along with Network Firewall, the standard NAT gateway processing and per-hour usage charges will be waived on a one-to-one basis with the throughput per gigabyte and usage hours charged for the Network Firewall

Network Firewall and other AWS security services

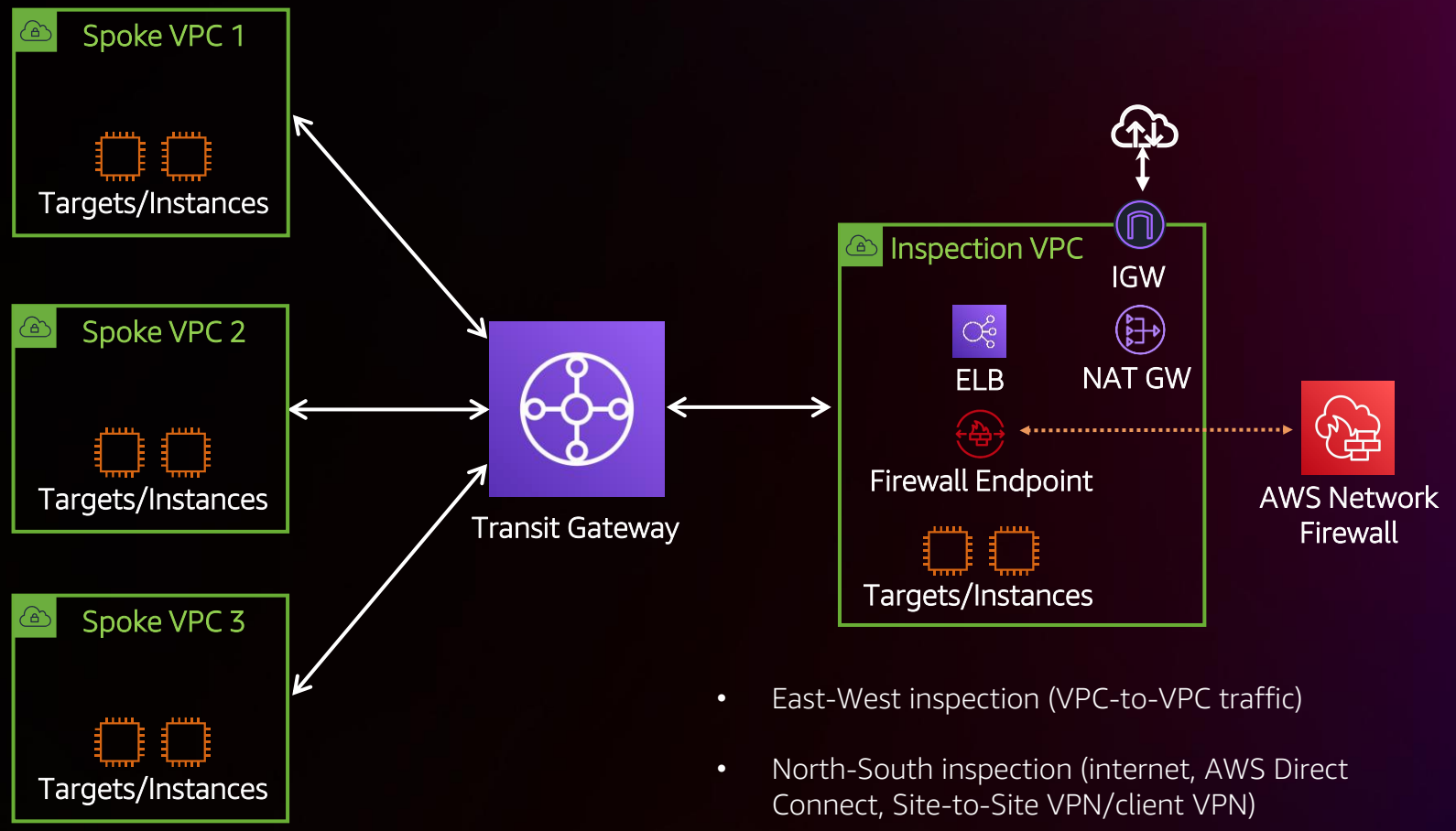
	Network Firewall	VPC security group	Network ACL	AWS WAF
Where is the protection applied?	Route level, based on VPC routes	Amazon EC2-instance level	Subnet level	Endpoint level (API Gateway, ALB, CloudFront)
Stateful or stateless	Both	Stateful	Stateless	Stateless
Which flows are protected?	All ingress/egress 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

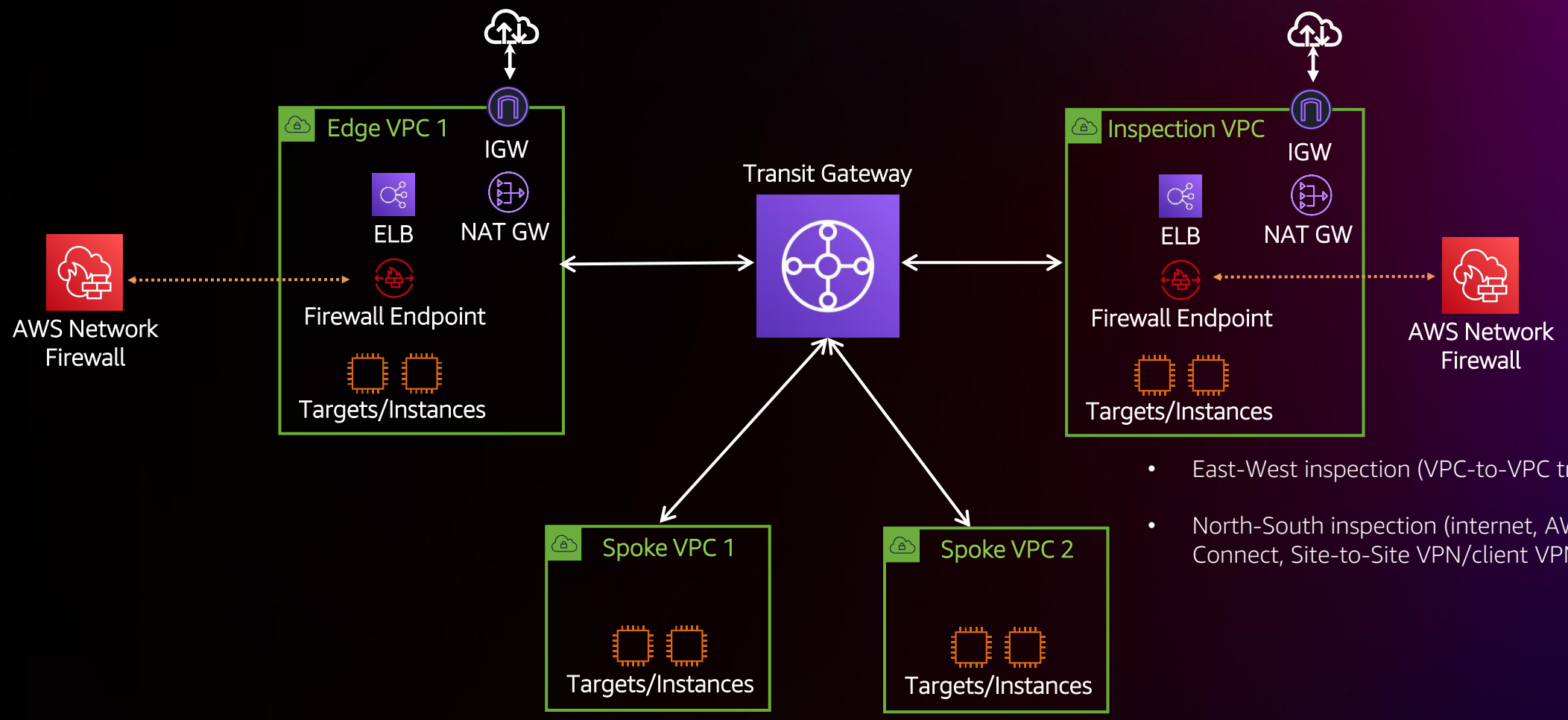


Centralized deployment model



- East-West inspection (VPC-to-VPC traffic)
- North-South inspection (internet, AWS Direct Connect, Site-to-Site VPN/client VPN)

Combined deployment model

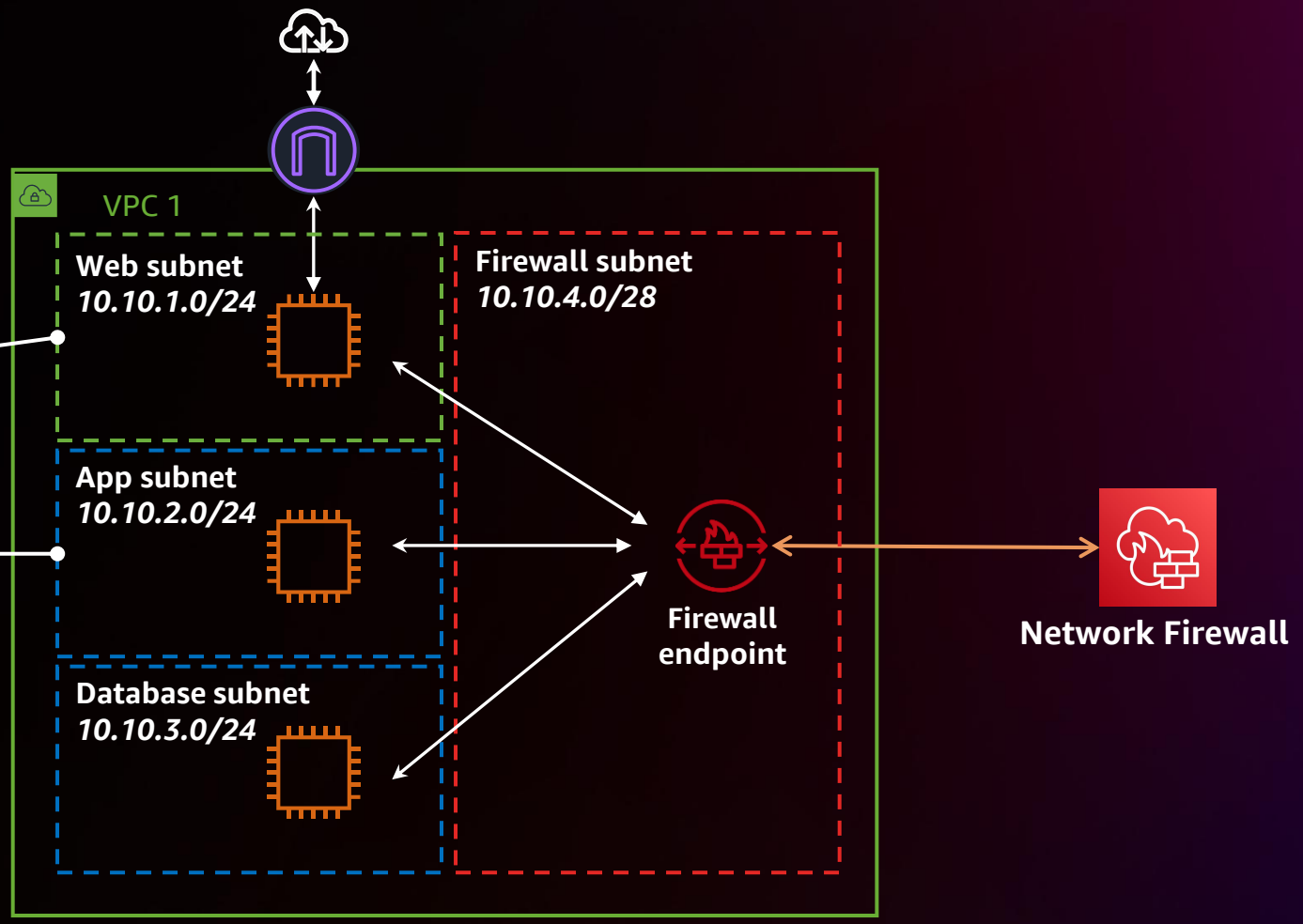


- East-West inspection (VPC-to-VPC traffic)
- North-South inspection (internet, AWS Direct Connect, Site-to-Site VPN/client VPN)

Network Firewall with VPC routing enhancements

Web subnet route table	
Destination	Target
10.10.2.0/24	Firewall endpoint

App subnet route table	
Destination	Target
10.10.3.0/24	Firewall endpoint



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)

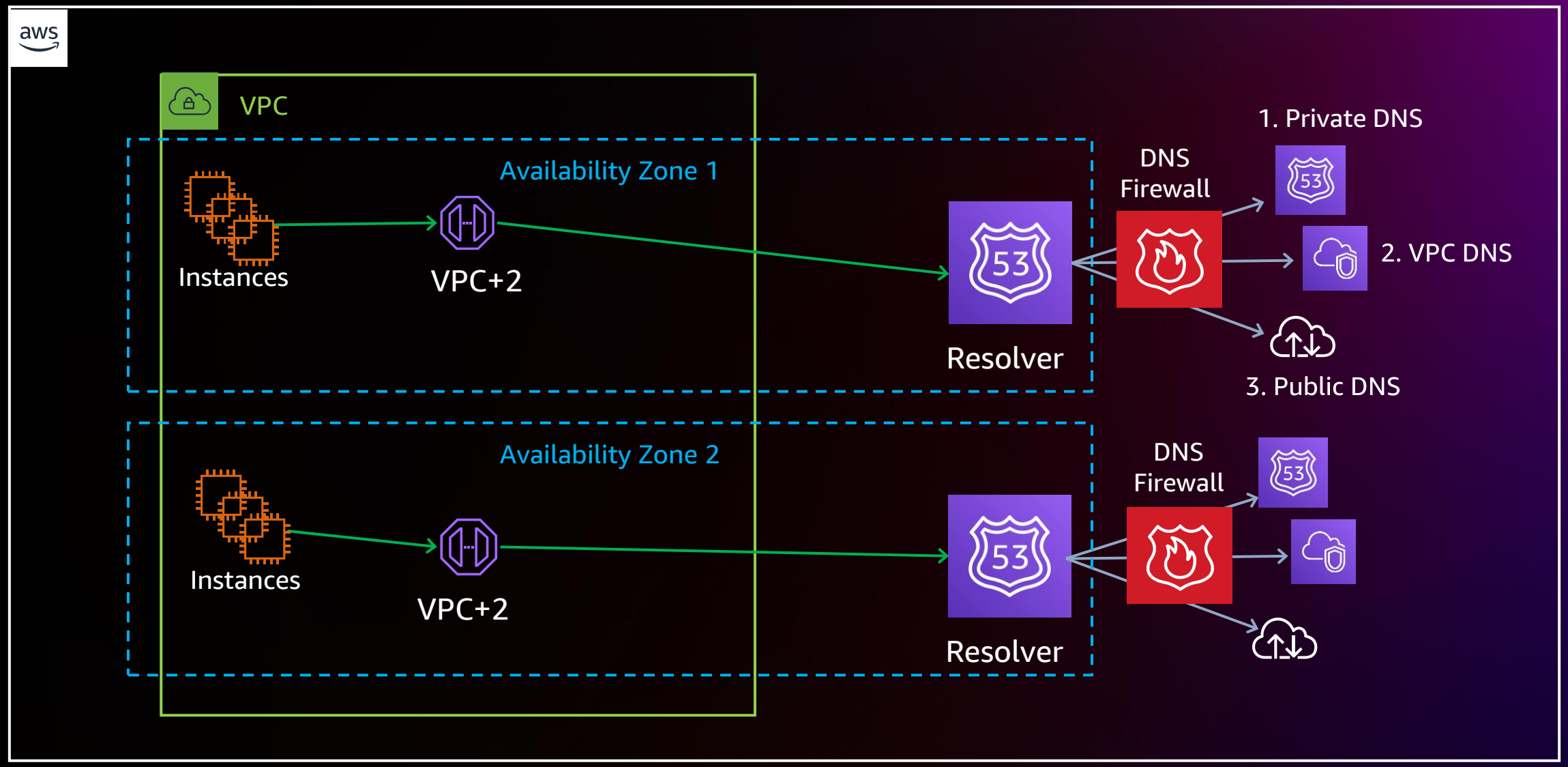
Central management

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

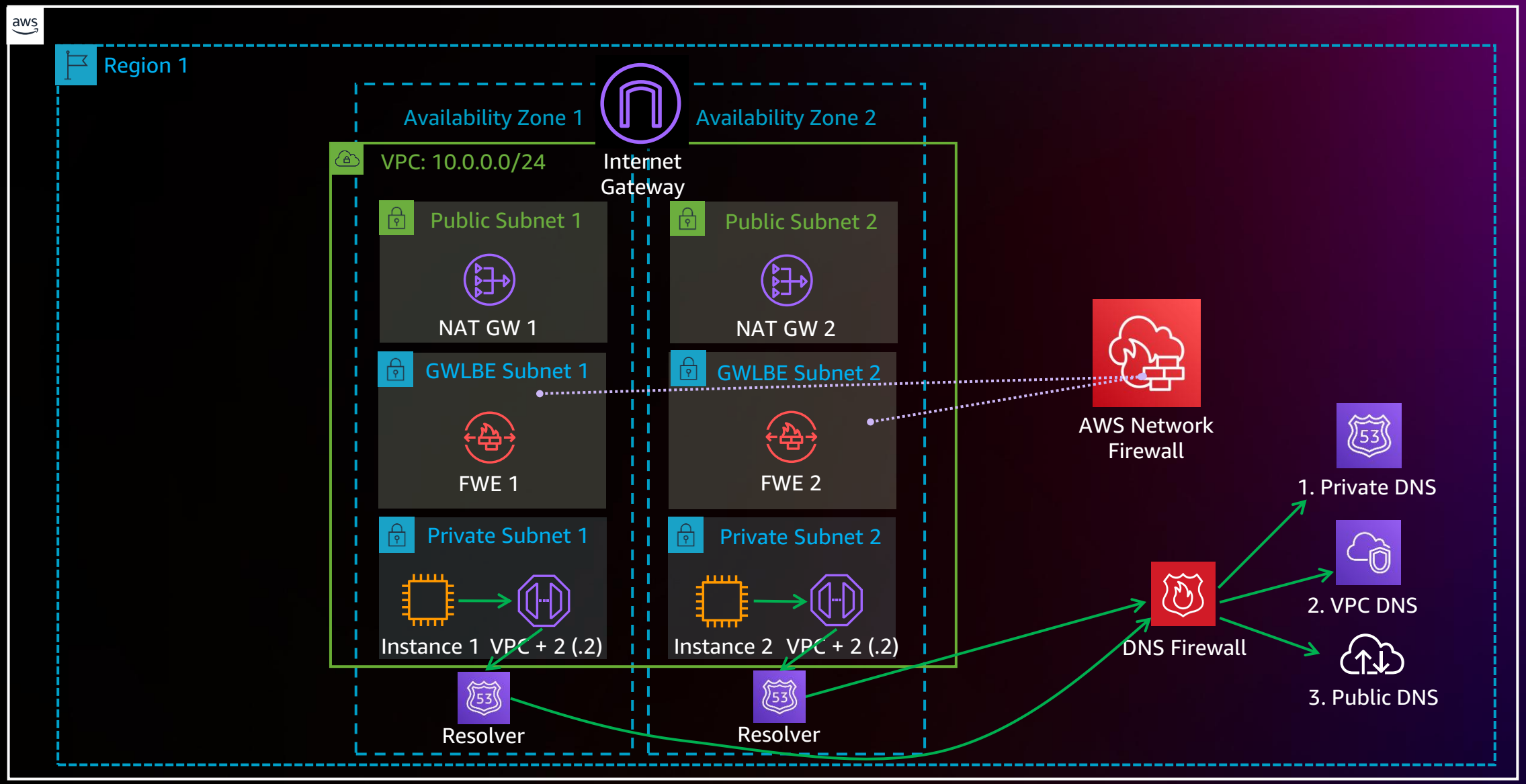
Visibility and reporting

- 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

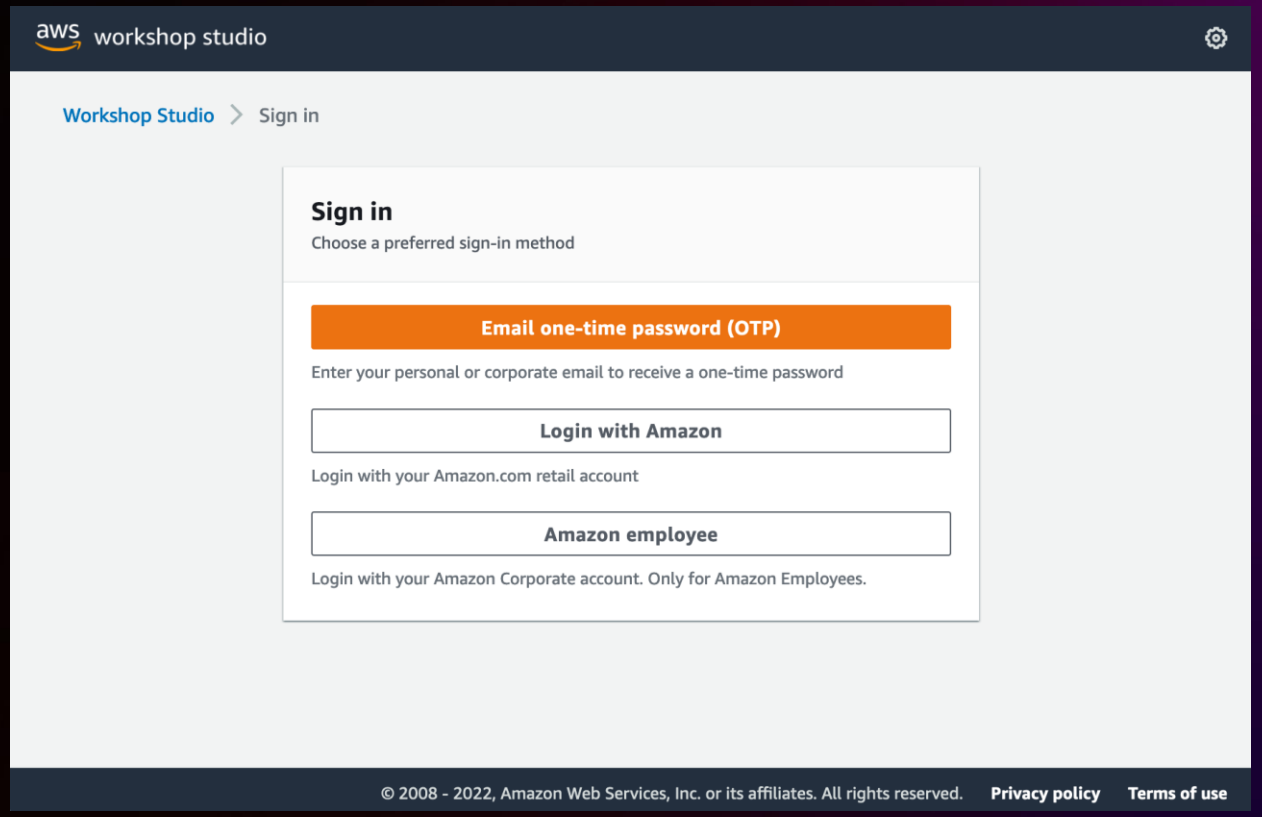
Event logistics

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.

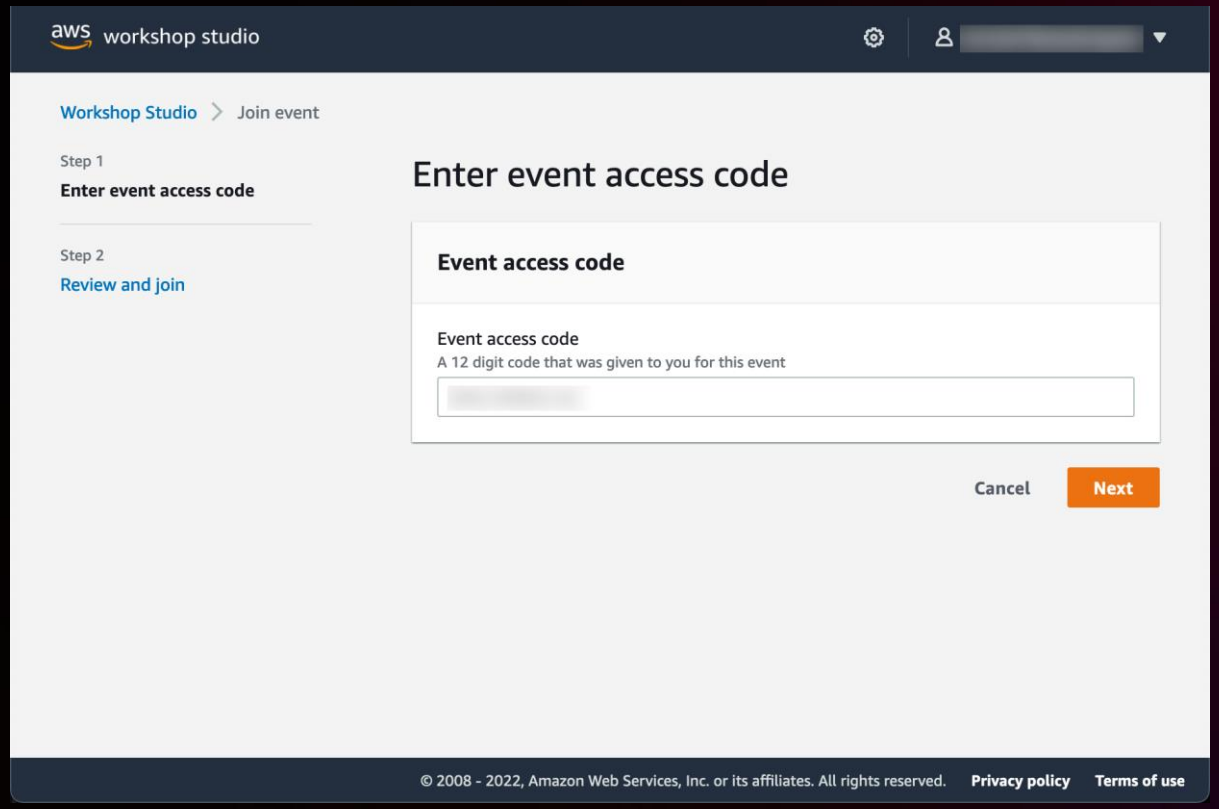
Step 1: Sign in via your preferred method

https://catalog.workshops.aws/join



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.



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

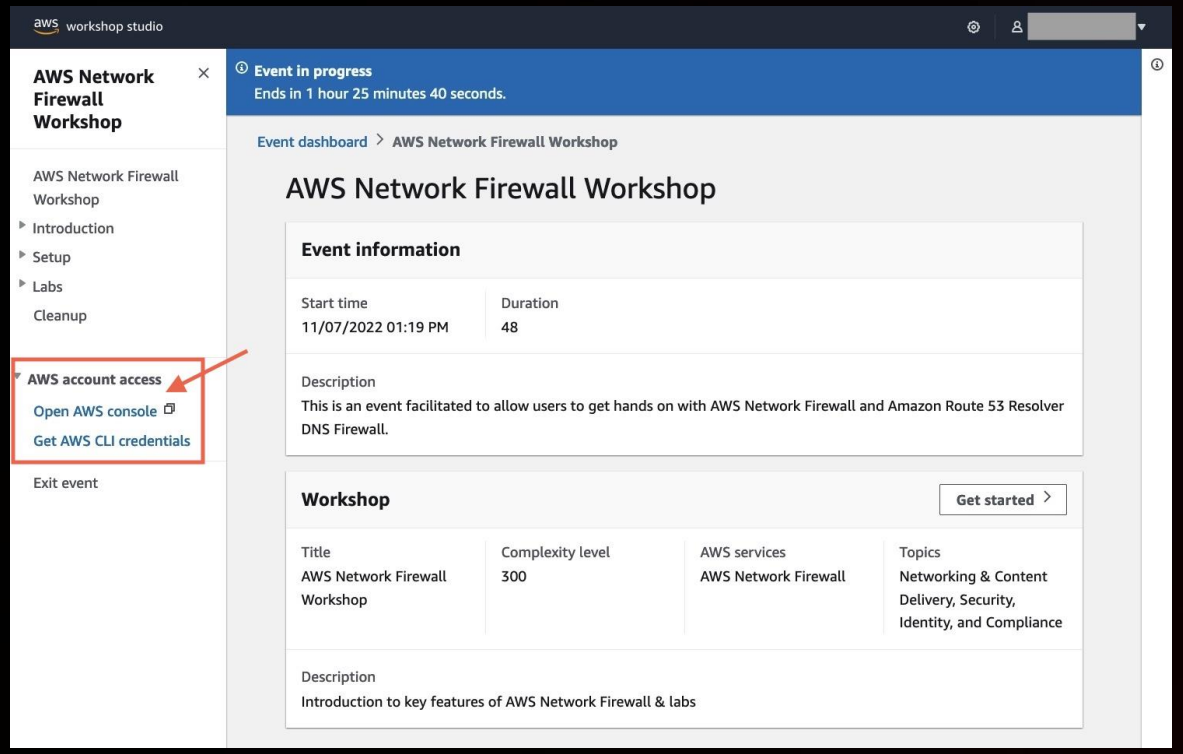
1. By using AWS Workshop Studio for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials 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 derivate 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.

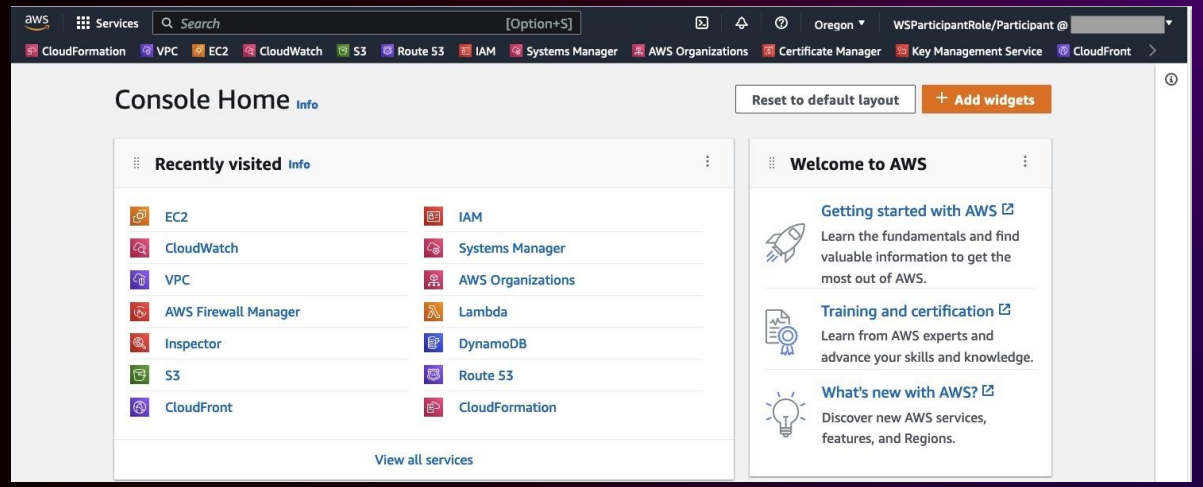
☑ I agree with the Terms and Conditions

Cancel | Previous | Join event

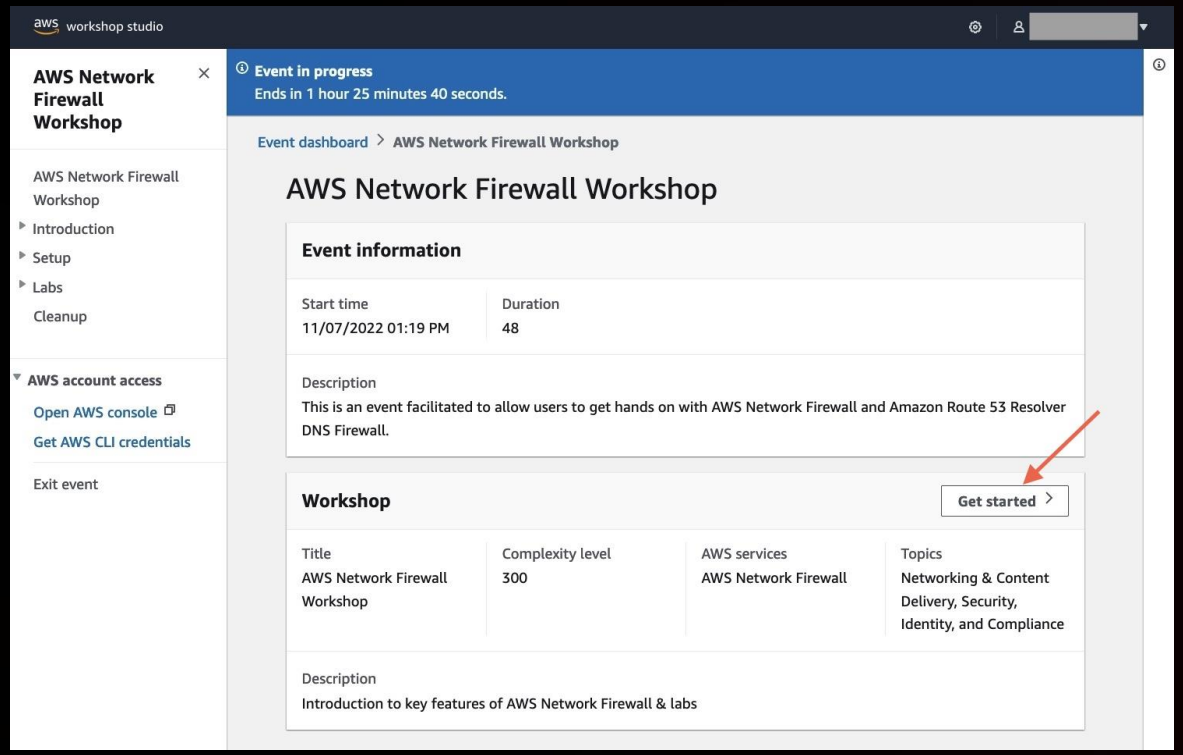
Step 4: Access AWS account

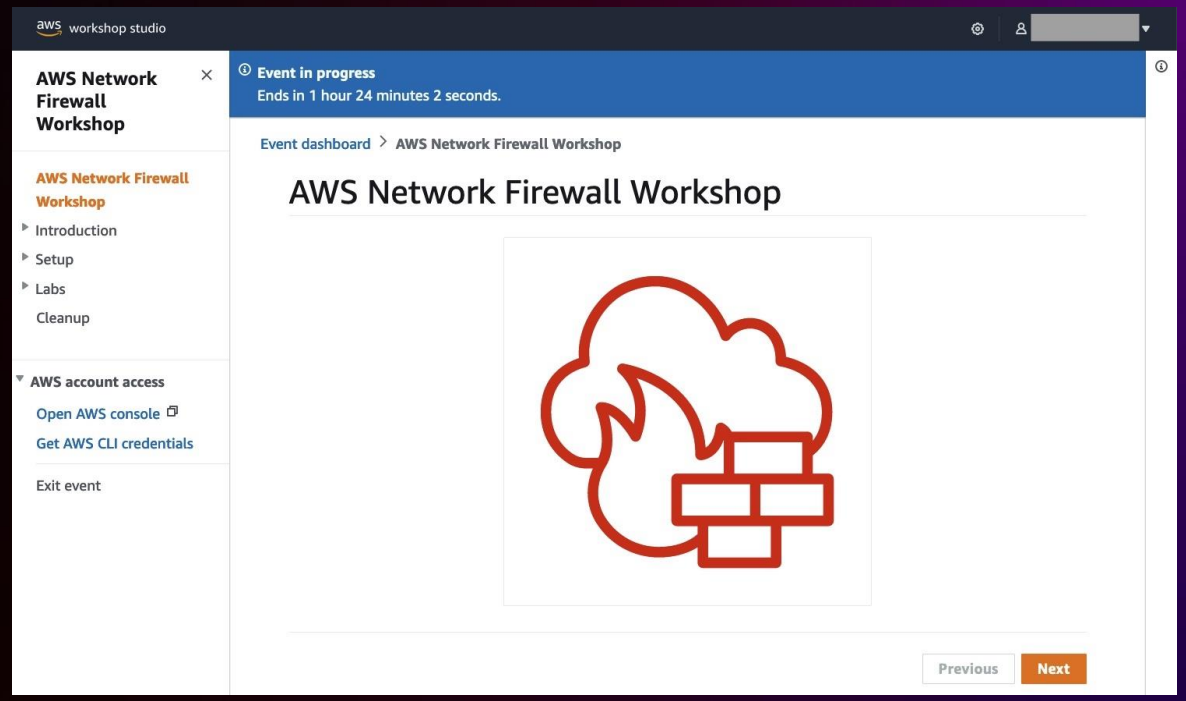
Access the AWS console, or generate AWS Command Line Interface (AWS CLI) credentials as needed





Step 5: Get started with the workshop





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 Surricata 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 Surricata 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/

Pratik Mankad
linkedin.com/in/pratikrmankad/

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