

The background of the image is a vibrant blue with a complex, abstract pattern of overlapping, curved lines that create a sense of depth and movement. The lines are in various shades of blue and purple, creating a dynamic, almost architectural feel. The overall composition is modern and tech-oriented.

AWS re:Inforce

JULY 26 – 27, 2022 | BOSTON, MA

NIS377-R1

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

Anandprasanna Gaitonde (he/him)

Sr. Solutions Architect, Digital Native Business
AWS

Pratik R. Mankad (he/him)

Sr. Specialist SA, Networking
AWS



Agenda

- 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

AWS Network Firewall

Managed infrastructure for high availability

Flexible protection through fine-grained controls

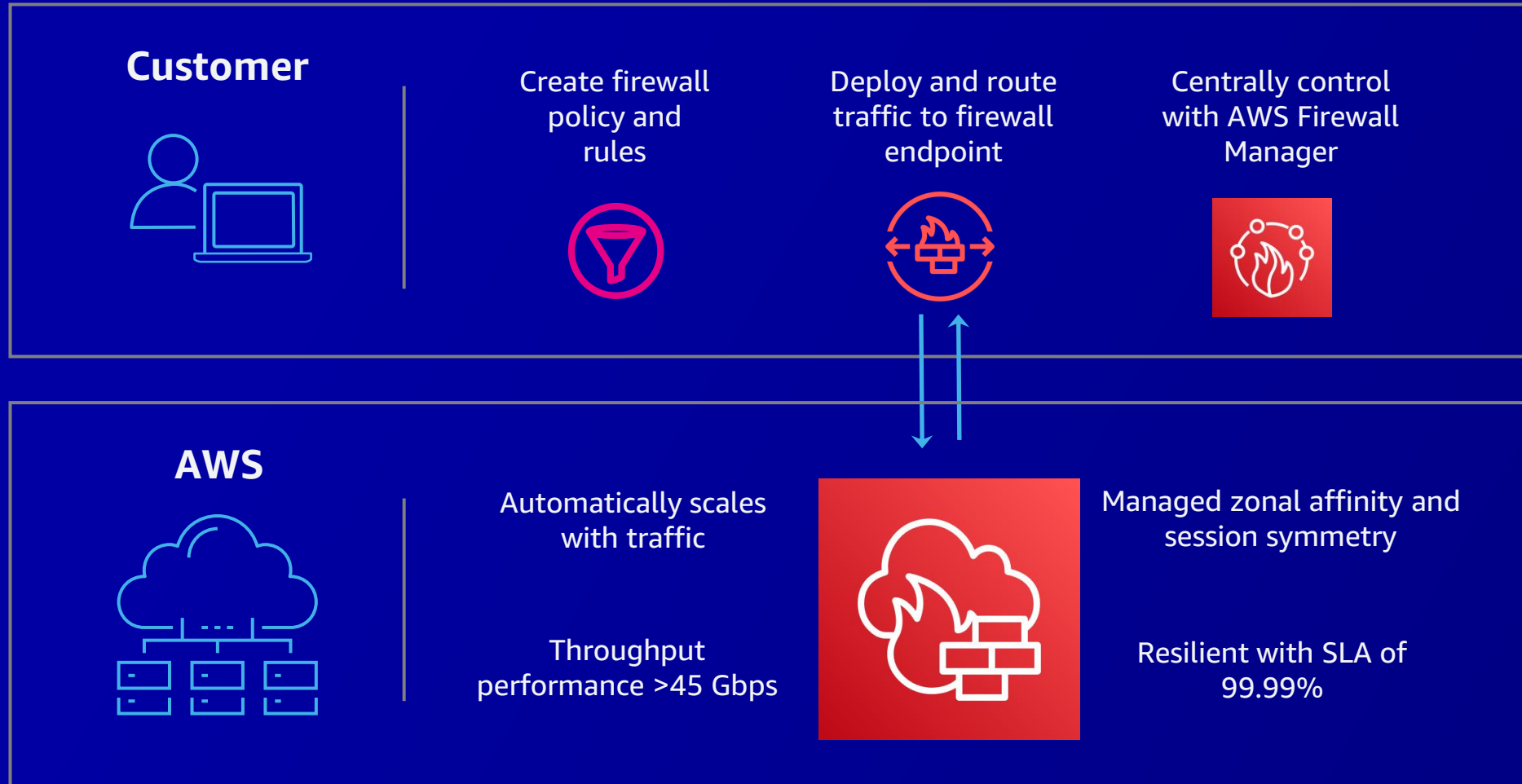
Consistent policy across VPCs and AWS accounts



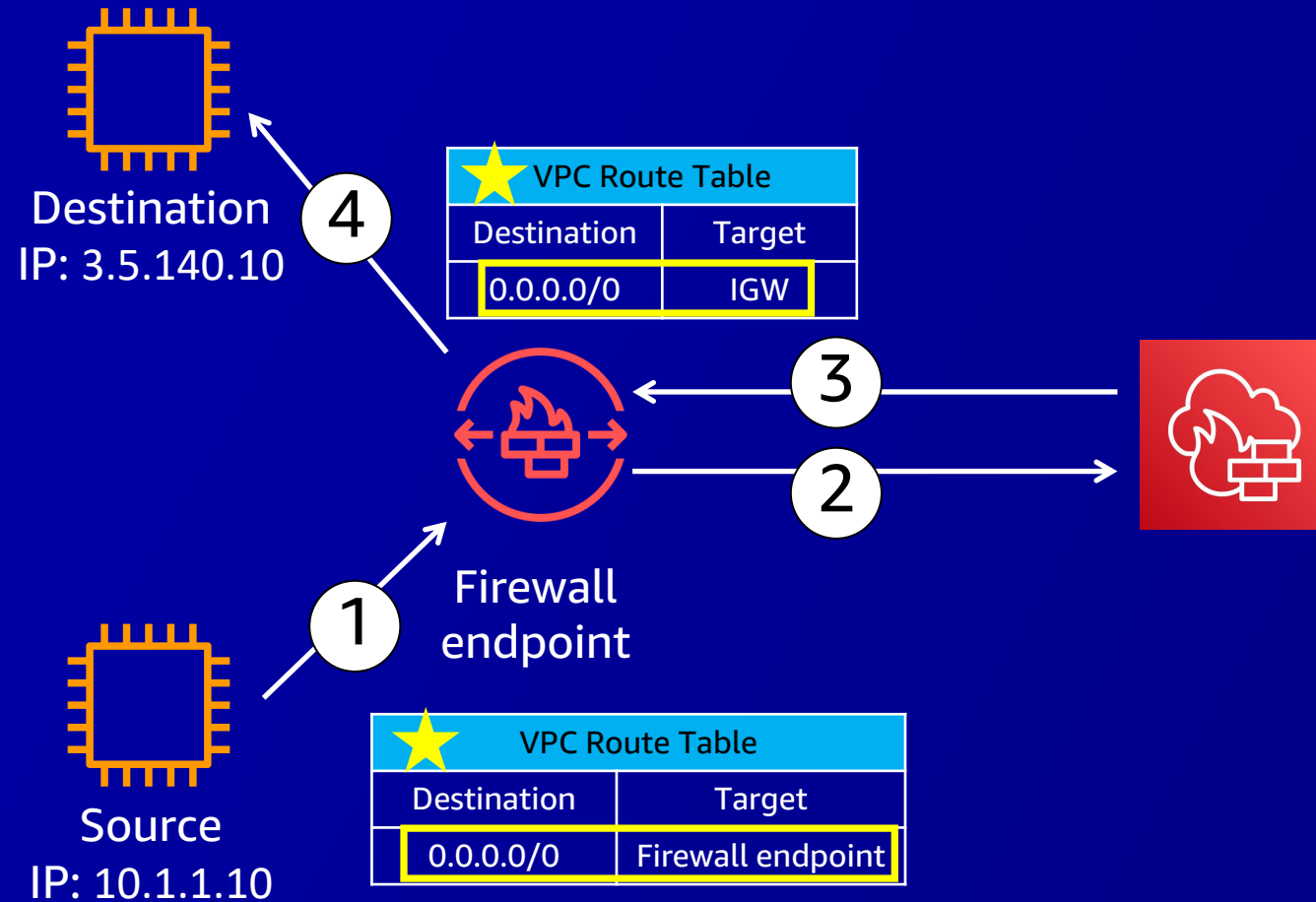
Network Firewall constructs



Network Firewall: At a glance



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

- 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

Network Firewall pricing

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

Network Firewall

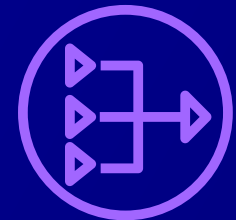
You pay an hourly rate for each firewall endpoint, and also for the amount of traffic (billed by the gigabyte) processed by your firewall endpoint

- \$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



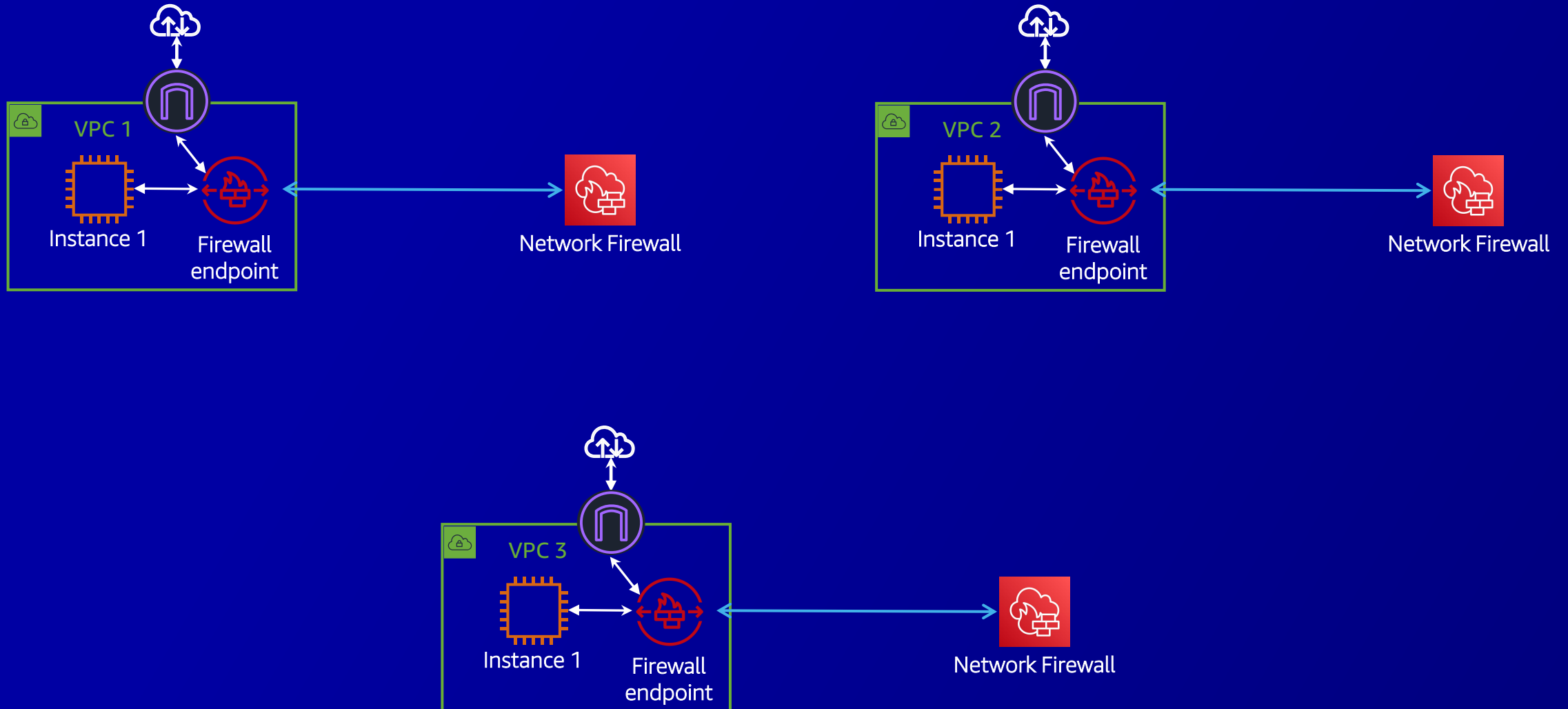
Network Firewall and other AWS security services

	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

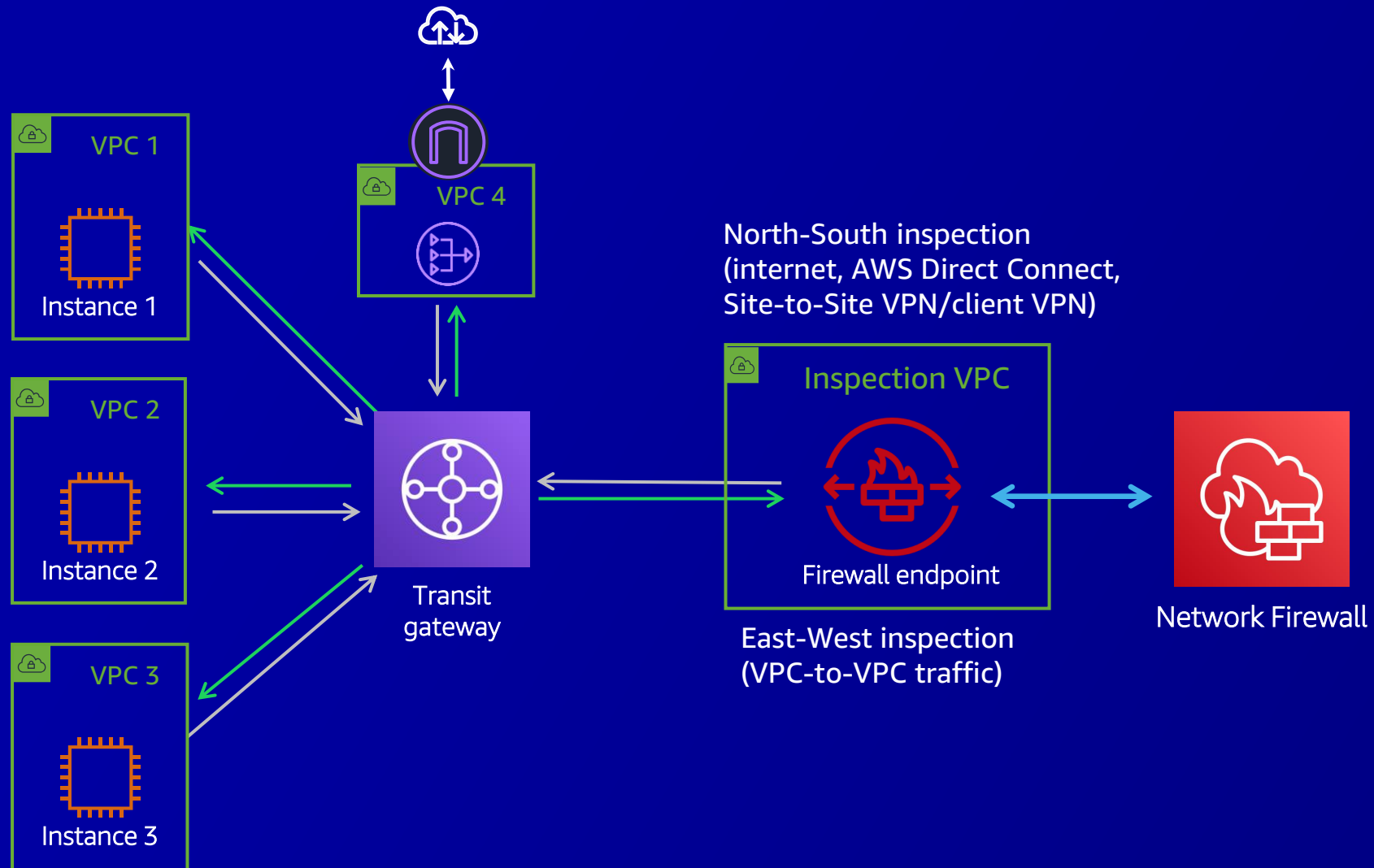
Deployment patterns



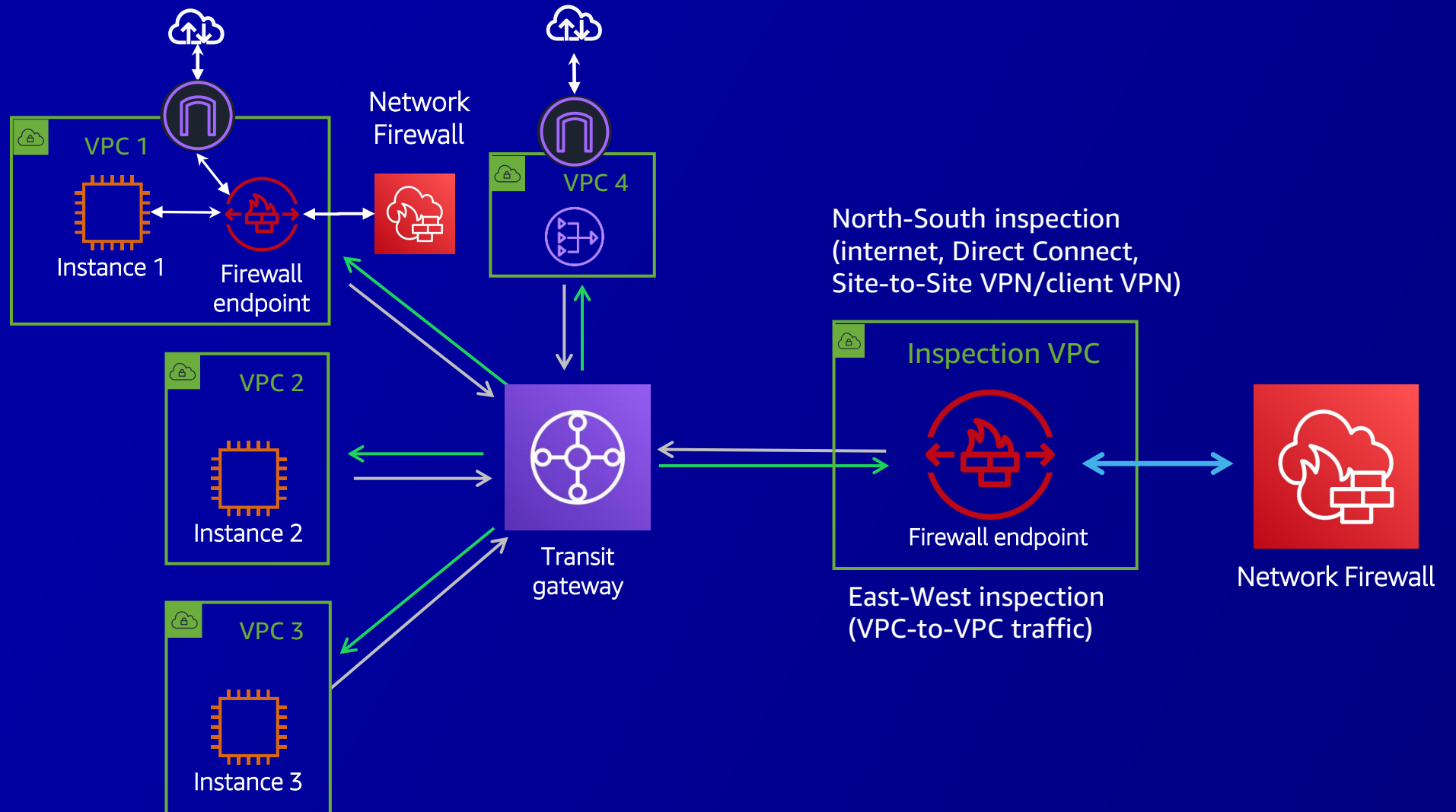
Distributed deployment model



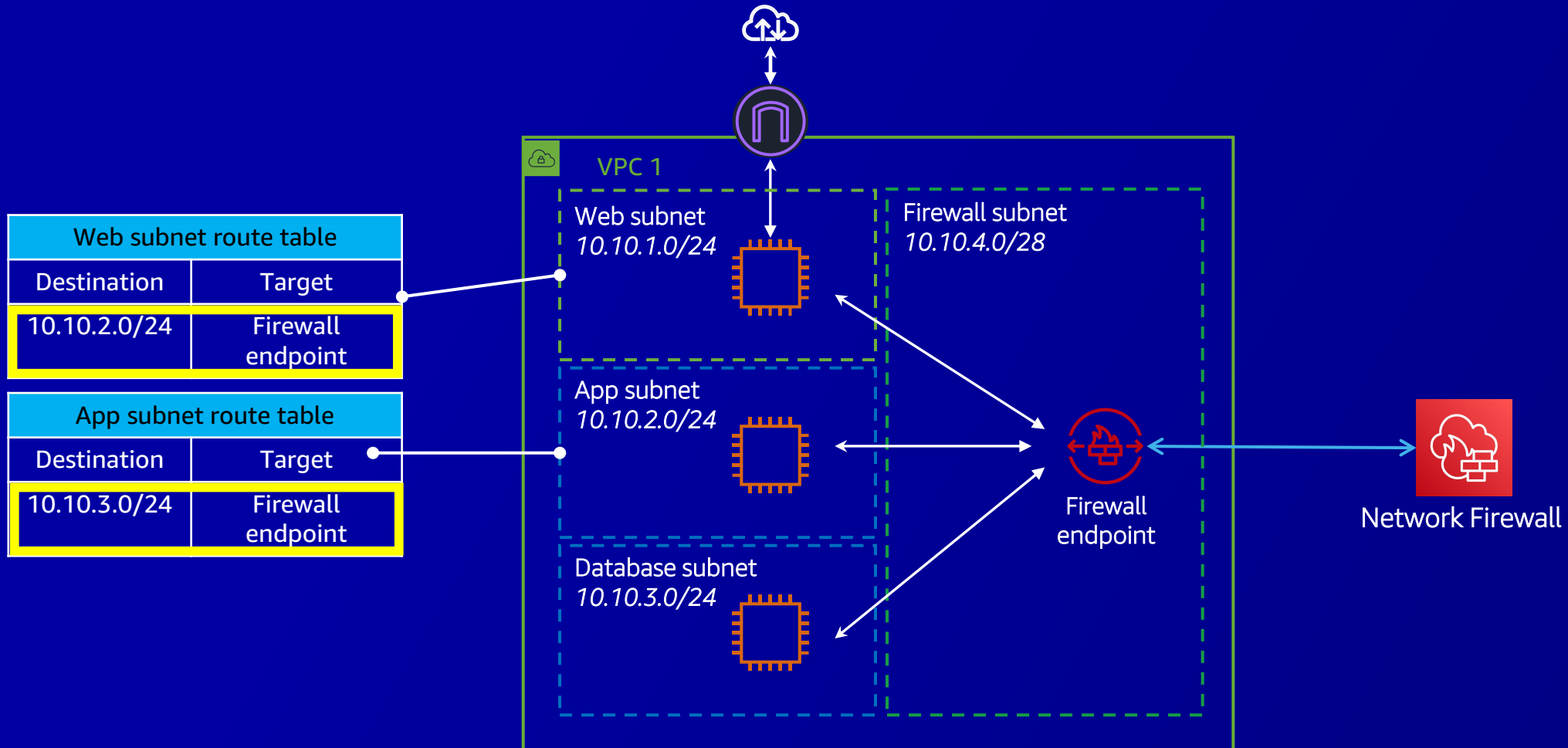
Centralized deployment model



Combined deployment model



Network Firewall with VPC routing enhancements



Deployment model resources

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



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



Amazon Route 53 DNS Firewall



Amazon Route 53 Resolver DNS Firewall

Firewall for the 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)

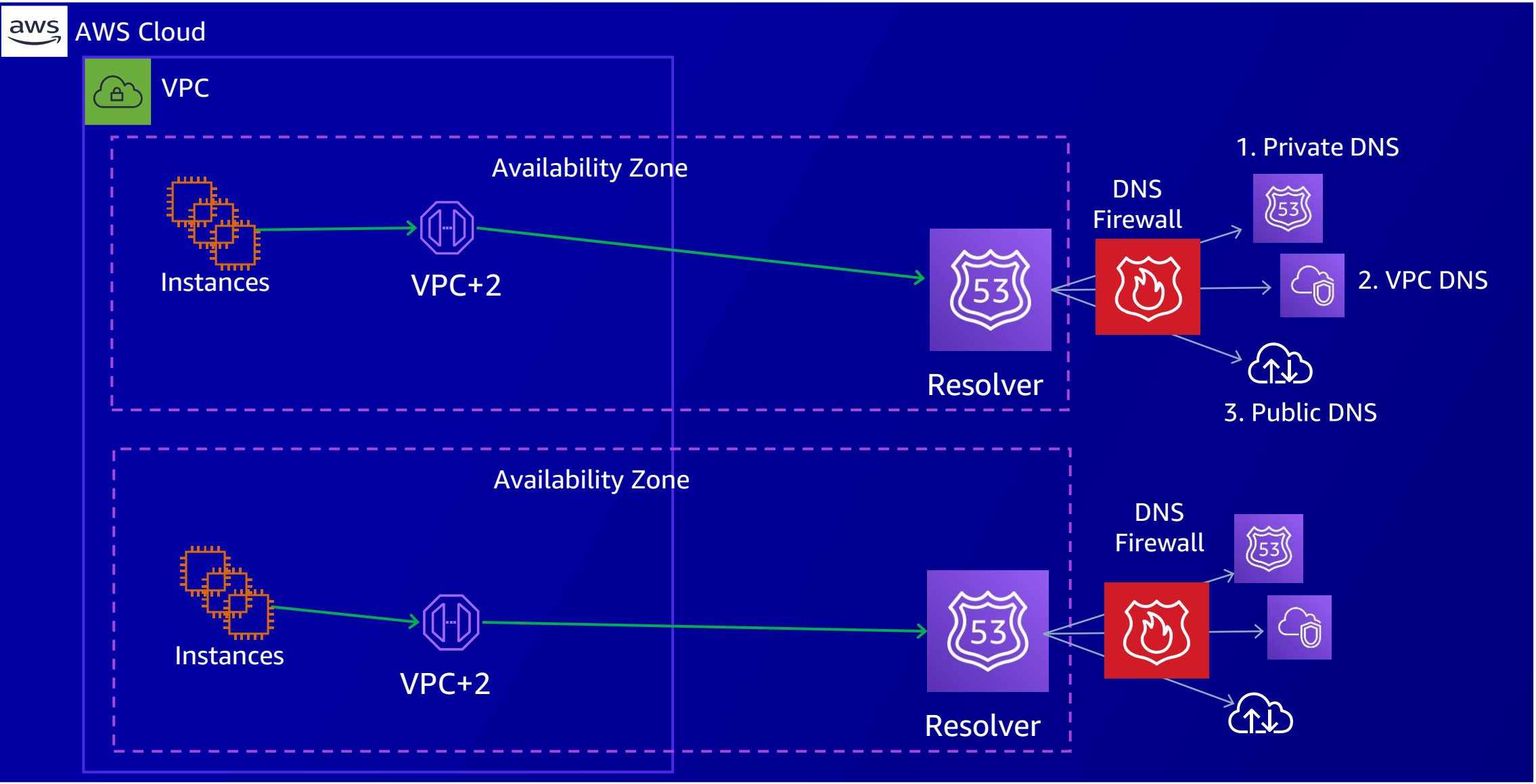
Central Management

- 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



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



Event Engine

<https://dashboard.eventengine.run>



Event Engine

Terms & Conditions:

1. By using the Event Engine 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 the Event Engine will comply with these terms and all applicable laws, and your access to Event Engine will immediately and automatically terminate if you do not comply with any of these terms or conditions.

123456789012

This is the 12 or 16 digit hash that was given to you for this event or for a specific team.

✓ [Accept Terms & Login](#)

<https://dashboard.eventengine.run>



Event Engine

Sign in with

Pick the sign-in method you prefer

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

(For Amazon Employees Only) Login with your Amazon Corporate account

[Get help signing in](#)

<https://dashboard.eventengine.run>



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

Event Engine

Dashboard

Exit Event

Team Dashboard

Event

Survey

AWS Console

SSH Key

View Content Guide

Event: AWS Network Firewall Workshop
Team Name: (Team Name Not Set Yet)

Event ID: 02e80d1f05e94cd1a50f09d6c4ce3fbf
Team ID: f8355b0beae44d918d1305d25c1ae267

Modules

Module 2 - Optional Lab5

Readme

Outputs:
No outputs defined

Module 1 - Centralized

Readme

Outputs:
No outputs defined

<https://dashboard.eventengine.run>



Event Engine

AWS Console Login

Remember to only use "us-west-2" as your region, unless otherwise directed by the event operator.

Login Link



Open AWS Console



Copy Login Link

Credentials / CLI Snippets

Mac / Linux

Windows

Mac or Linux

```
export AWS_DEFAULT_REGION=us-west-2
export AWS_ACCESS_KEY_ID=ASIA5ZK
export AWS_SECRET_ACCESS_KEY=xgf
export AWS_SESSION_TOKEN=IQoJb3J
```

How do I use the AWS CLI?

Checkout the AWS CLI documentation here: <https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html>

OK

<https://dashboard.eventengine.run>



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

A diagram illustrating the AWS Network Firewall architecture. It features a large red outline of a cloud. Inside the cloud, there is a red outline of a firewall icon, which consists of a central vertical rectangle with two horizontal rectangles on either side, and another horizontal rectangle below the central one. The entire diagram is enclosed in a thin gray border.

Previous

Next

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

► Lab 5 (Optional): Ingress Traffic Inspection - DIY

▼ Build version

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](#)

Previous

Next



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

Event Engine hash



- Event URL: <https://dashboard.eventengine.run>
- Workshop URL: <https://catalog.workshops.aws/networkfirewall>
- Event hash: 4f0f-143c89e954-43

After-session event support:
anandprg@amazon.com / pmankad@amazon.com

Related Sessions

Upcoming Sessions

NIS332-R2 - Implementing traffic inspection capabilities at scale on AWS (Chalk Talk)

NIS341-R2 - Manage your network security infrastructure at scale with AWS Network Firewall, AWS Transit Gateway, and IaC (Code Talk)

Prior Sessions

NIS253 - Audit and manage firewall rules at scale with AWS Firewall Manager (Builder's Session)

NIS301 - Design your firewall deployments to protect your internet applications (Breakout –Silent)

NIS308 - Deploying AWS Network Firewall at scale: athenahealth's journey (Breakout)



Thank you!

Anandprasanna Gaitonde

<https://www.linkedin.com/in/anandprasannag>

Pratik R. Mankad

<http://linkedin.com/in/pratikrmankad/>

