
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

FSI304-R

Your blueprint to secure customer-facing applications on AWS

Marc Heil
(He/Him)

Solutions Architect, Financial Services
AWS

Anirudh Menon
(He/Him)

Solutions Architect, Financial Services
AWS

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

Agenda

What are we solving for?

What tools are available to us?

Design decisions at scale

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

Where are your customers?

External		Internal
Business to customer	Business to business	Lines of business
		
Public traffic	Both	Private traffic

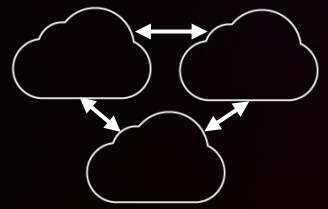
aws

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

Customers have broad needs at scale



Diverse group of applications



Multiple AWS VPCs



On-premises hosted services



Lean network operations



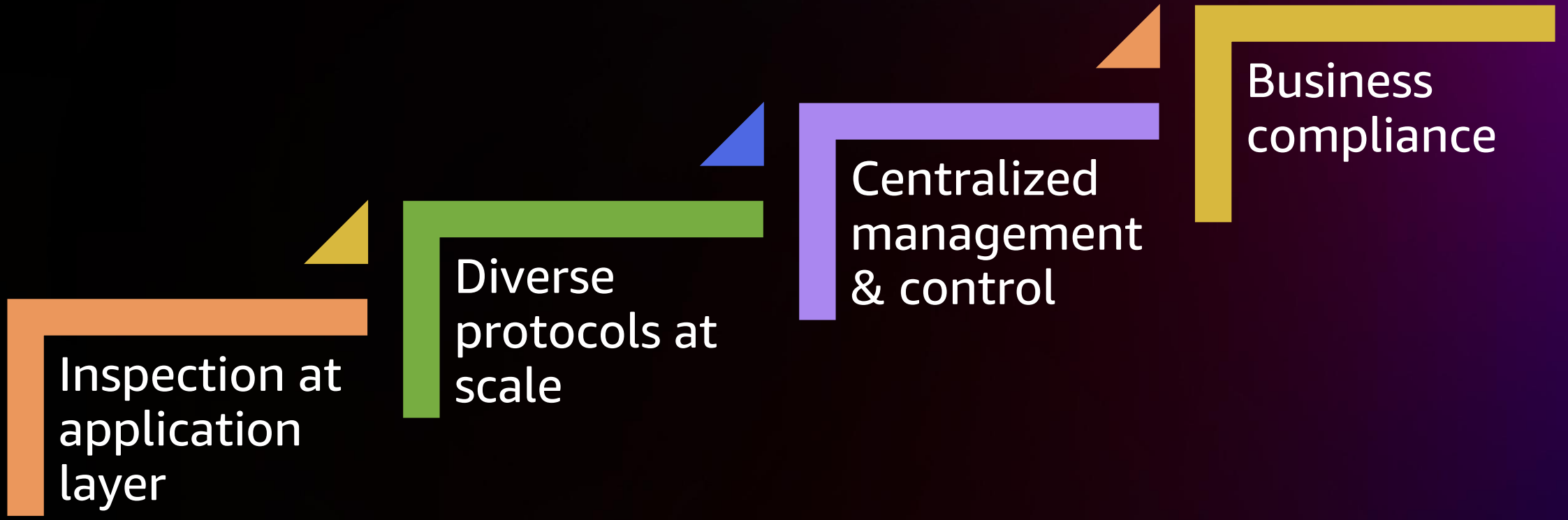
Traffic inspection requirements



Inspection close to boundary

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

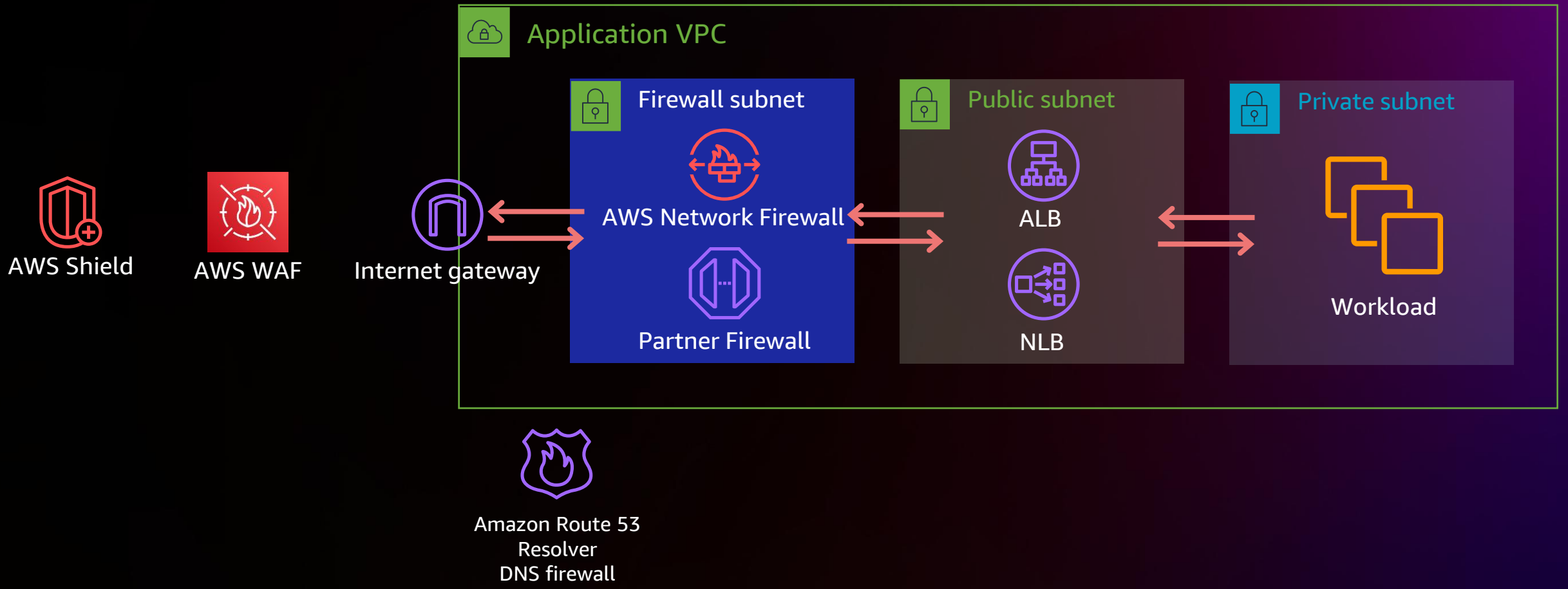
Why go beyond SG and NACLs for network security?



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

Network edge defense in depth

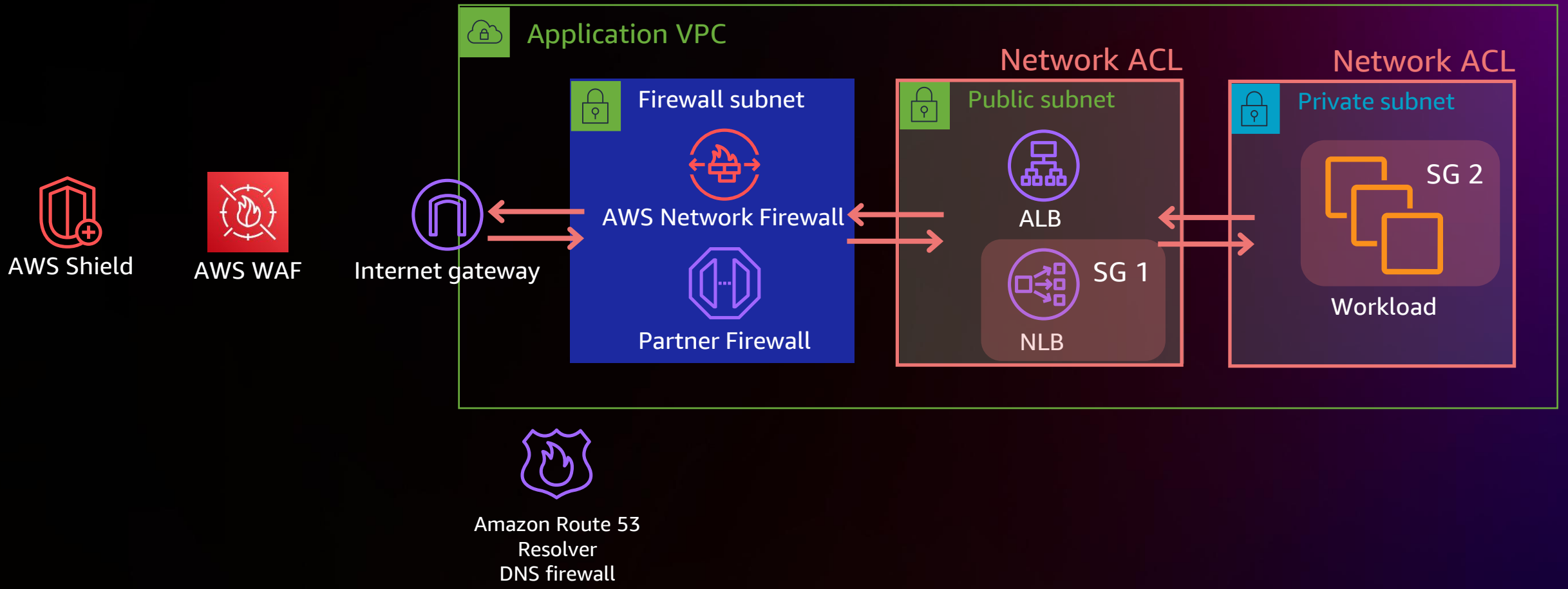
Combine AWS services to protect your workloads



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

Network edge defense in depth

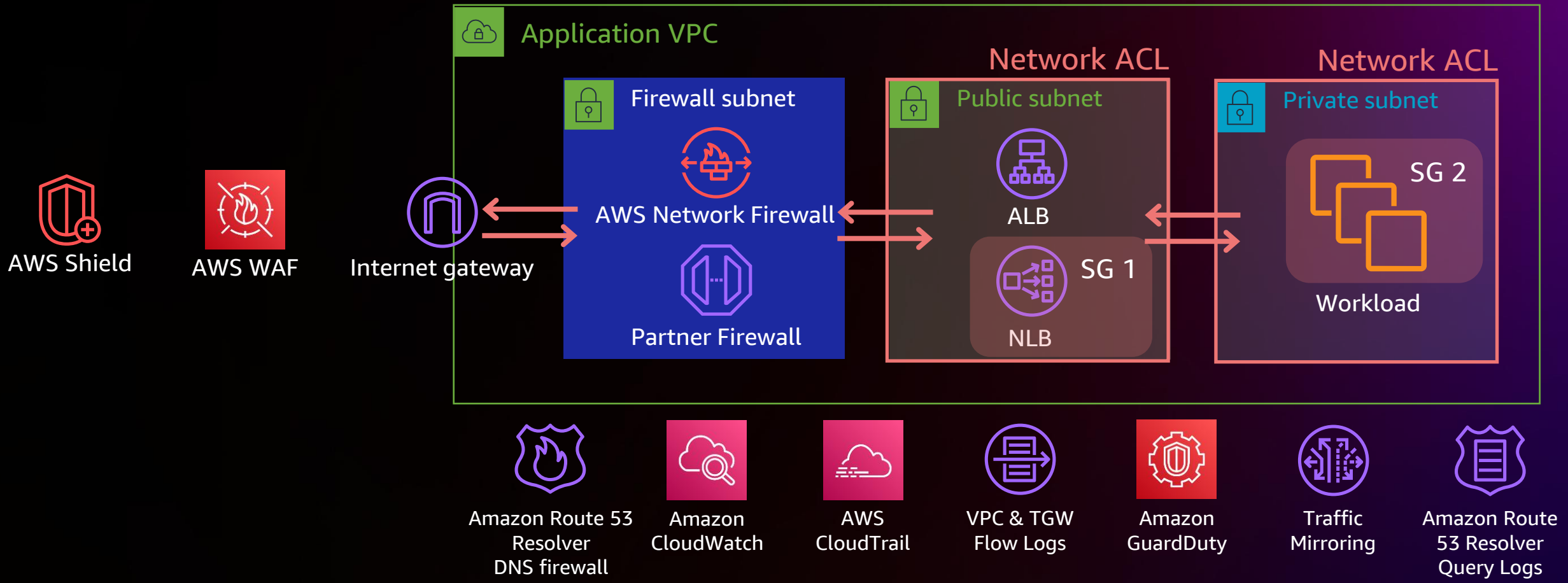
Combine AWS services to protect your workloads



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

Network edge defense in depth

Combine AWS services to protect your workloads



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

AWS native firewall options comparison

Attributes	AWS 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 (Amazon API Gateway, ALB, Amazon CloudFront)
Stateful or stateless?	Both	Stateful	Stateless	Stateless
Which flows are protected?	All ingress/egress flows at perimeter of VPC (IGW, VGW, DX, VPN, VPC-VPC)	All ingress/egress flows at instance level (EC2–EC2, EC2–IGW, EC2-DX)	All ingress/egress flows at subnet level (subnet–subnet, subnet–IGW, subnet–DX)	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

Note – AWS Shield Advanced and Amazon Route53 Resolver DNS Firewall excluded as they are specific to domain resolution and DDoS attacks

aws

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

AWS native firewall options comparison

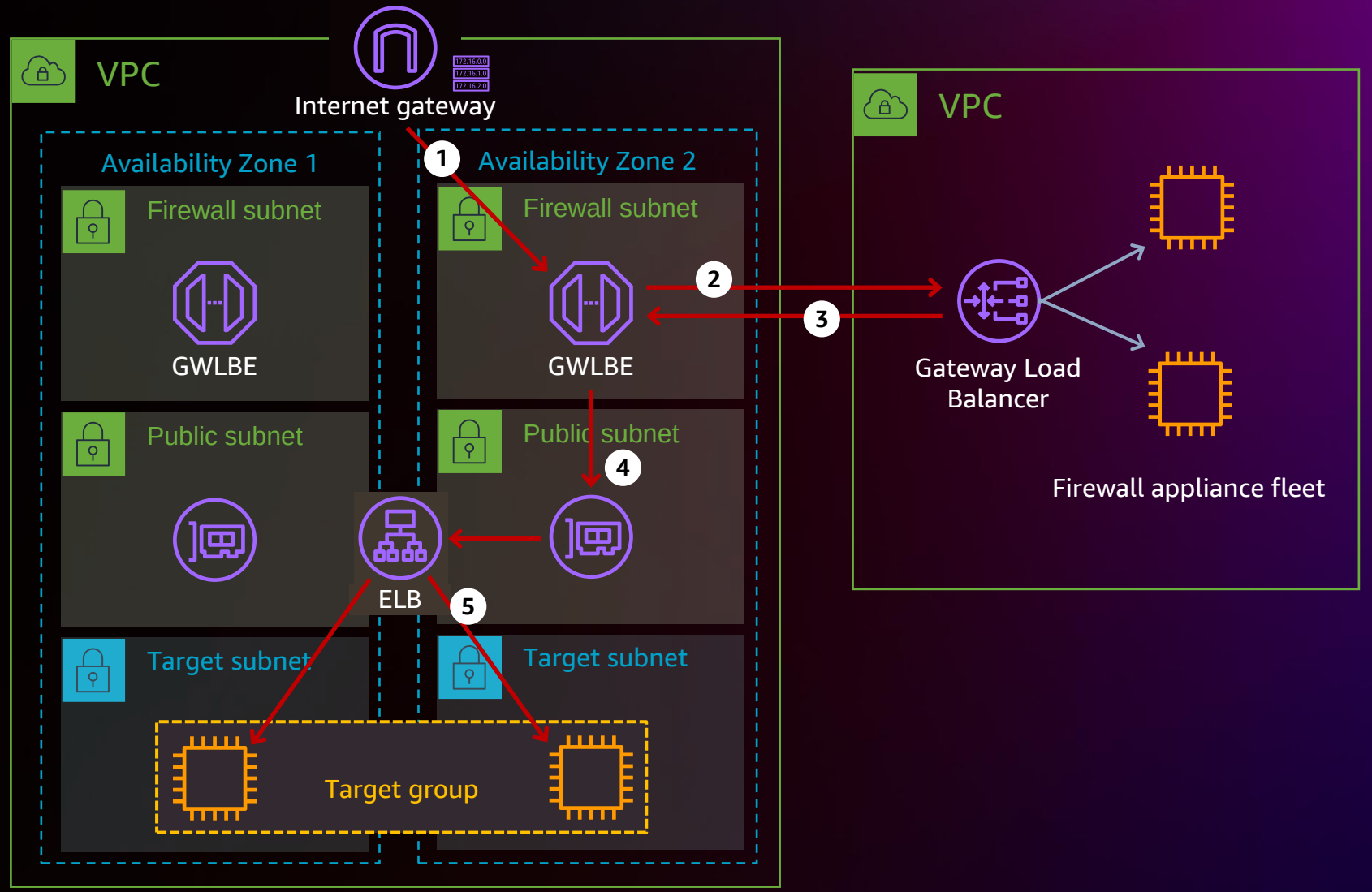
Attributes	AWS Network Firewall	VPC security group	Network ACL	AWS WAF
Where is the protection applied?	Route level, based on VPC routes	Amazon EC2 instance level	Subnet level	Endpoint level (Amazon API Gateway, ALB, Amazon CloudFront)
Stateful or stateless?	Both	Stateful	Stateless	Stateless
Which flows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

Note – AWS Shield Advanced and Amazon Route53 Resolver DNS Firewall excluded as they are specific to domain resolution and DDoS attacks

aws

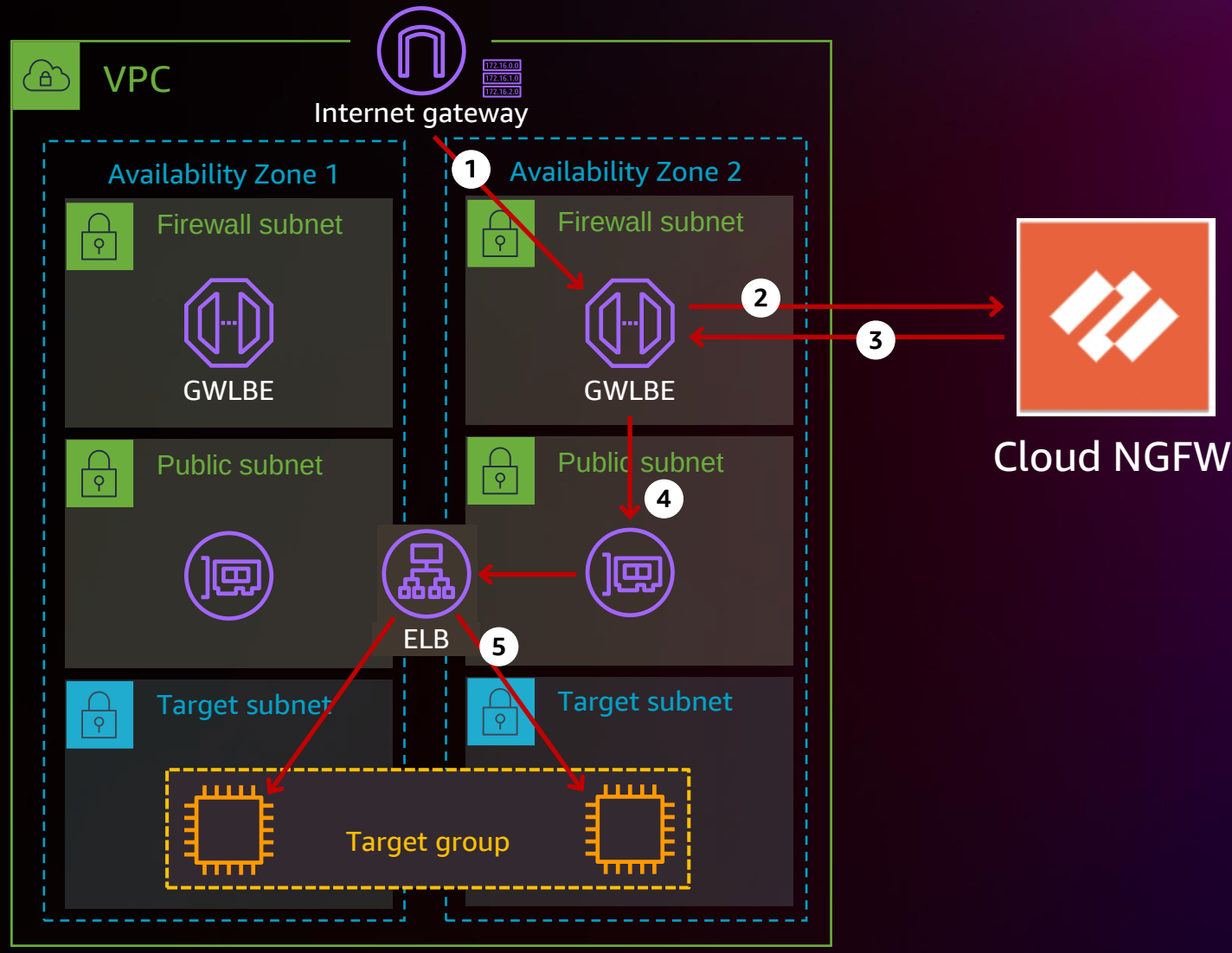
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Gateway Load Balancer



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

Palo Alto – Cloud Next Gen Firewall for AWS



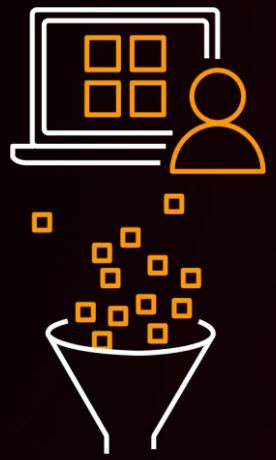
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common use cases

Egress filtering



Ingress filtering



VPC to VPC inspection



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

Related sessions

NET311 – Layered VPC security and inspection

SEC302 – AWS Network Firewall and DNS Firewall security in multi-VPC architectures

SEC317 – Implementing traffic inspection capabilities at scale on AWS

NET321 – Choosing the right firewall for your hybrid network

SEC312 – Deploying egress traffic controls in production environments

aws

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

Thank you!

Marc Heil
marcheil@amazon.com
marc-heil@LinkedIn

Anirudh Menon
amenon@amazon.com
menonanirudh@LinkedIn



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

aws

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