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

NET204

Application networking foundations

Jamie Wenzel (he/him)

Principal SA, Elastic Load Balancing
AWS

Tom Adamski (he/him)

Principal SA, Networking
AWS

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

Takeaways

What is application networking?

Application networking building blocks:

- Service discovery
- Service connectivity

Sample scenario/architecture

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

Application networking vs. networking



re:Invent 2021

AWS Transit Gateway

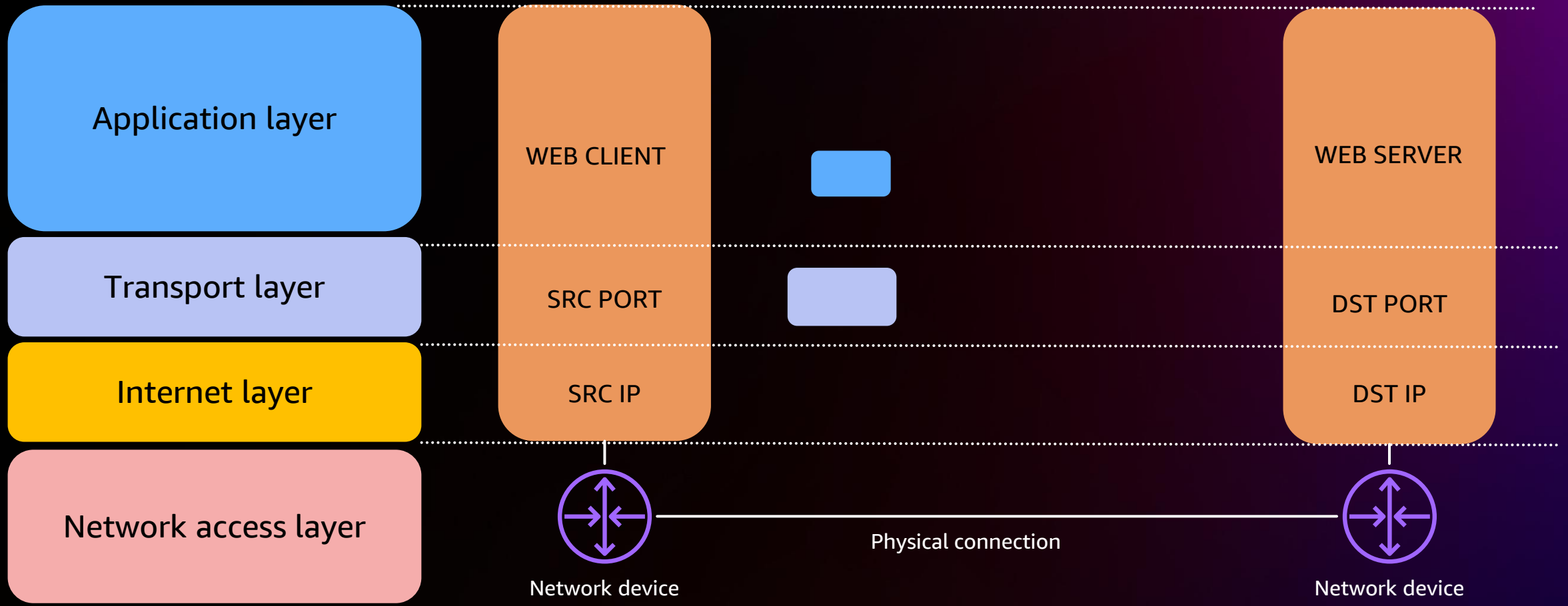
AWS Site-to-Site VPN

Amazon Virtual Private Cloud (Amazon VPC)

AWS Direct Connect

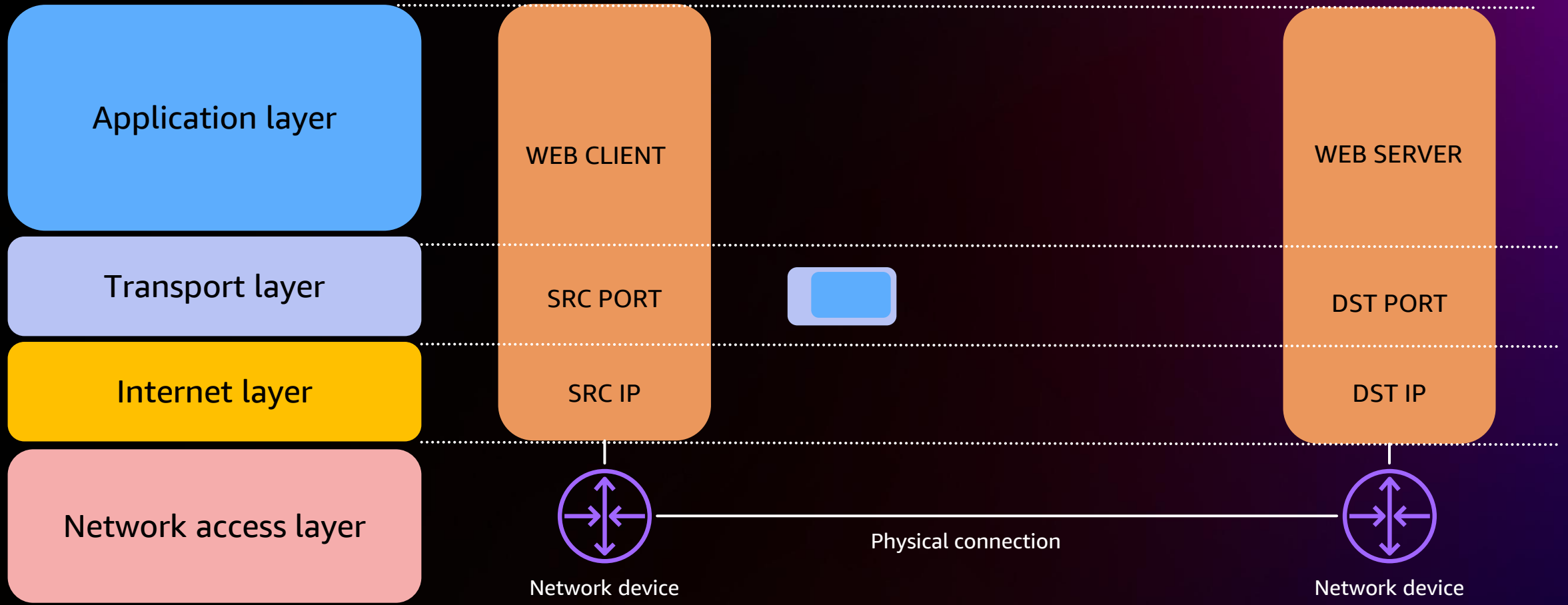
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TCP/IP layers



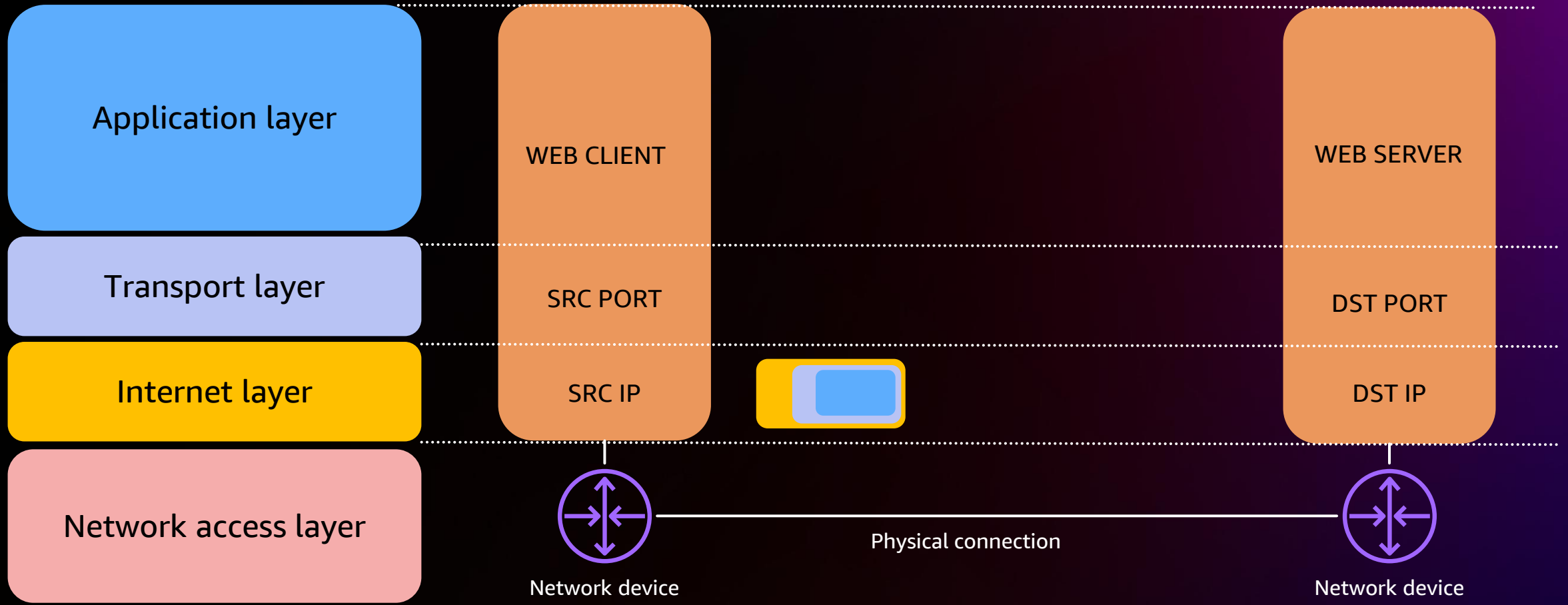
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TCP/IP layers



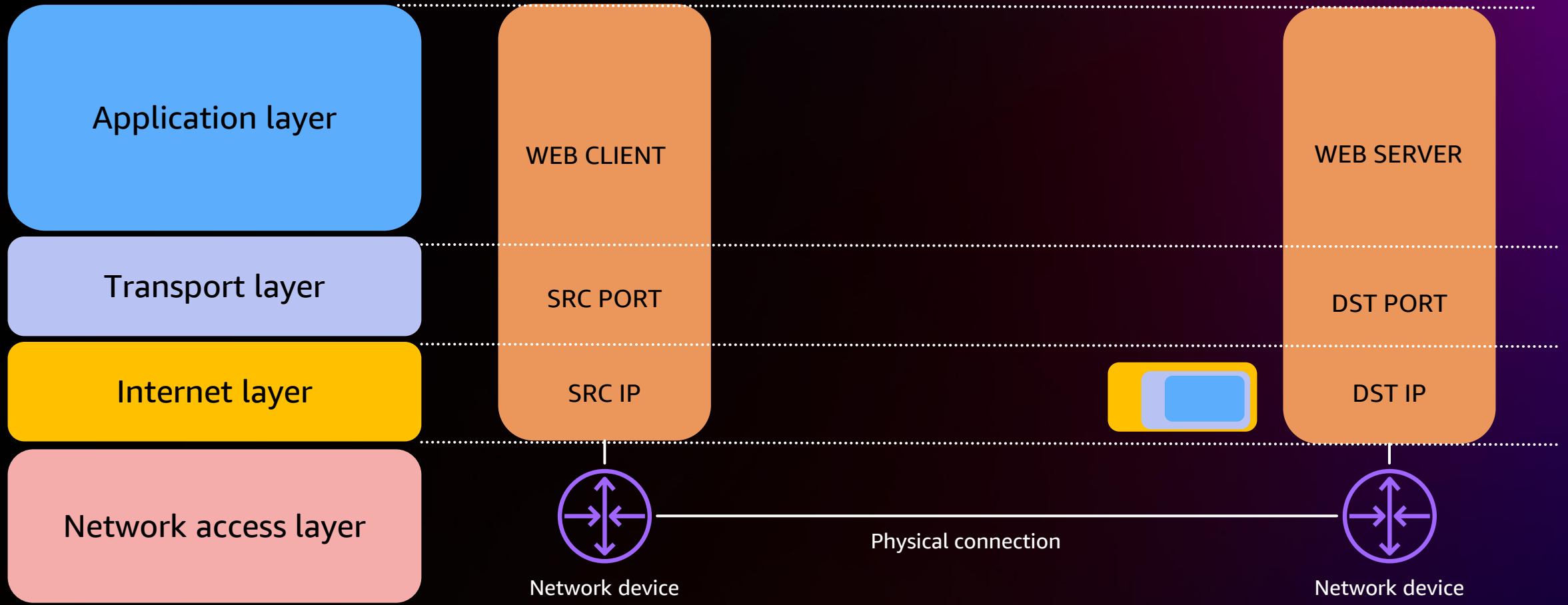
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TCP/IP layers



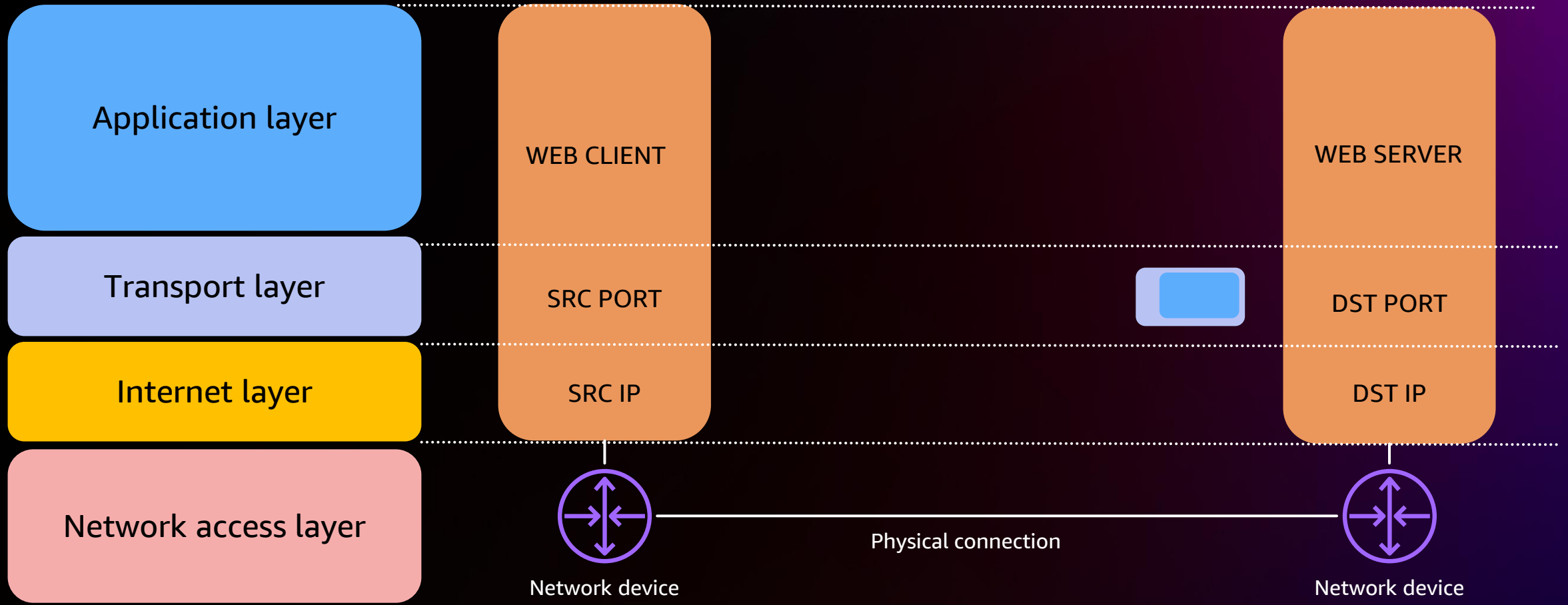
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TCP/IP layers



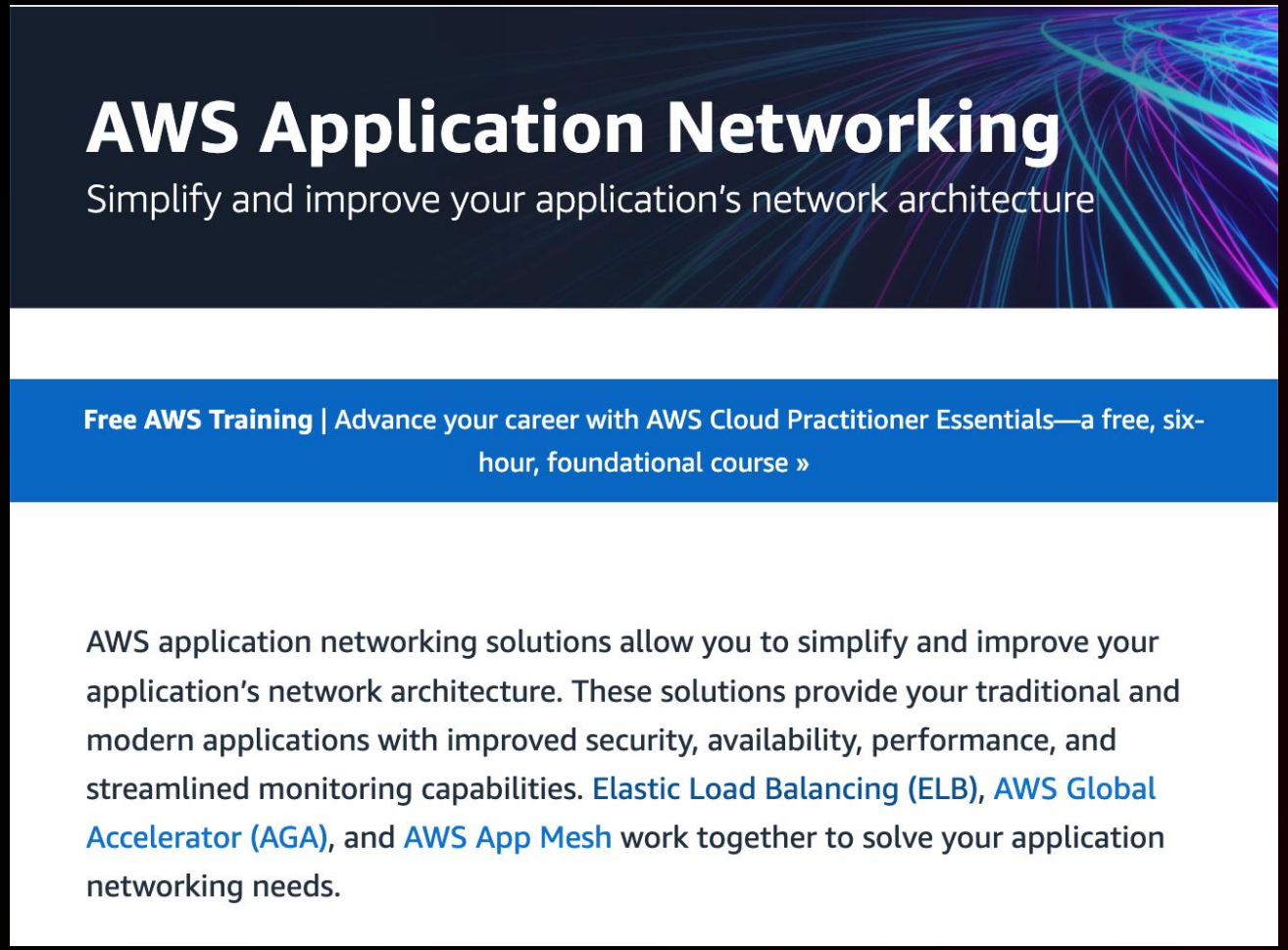
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TCP/IP layers



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

Application networking



Elastic Load Balancing

AWS Global Accelerator

AWS App Mesh

AWS Cloud Map

Amazon CloudFront

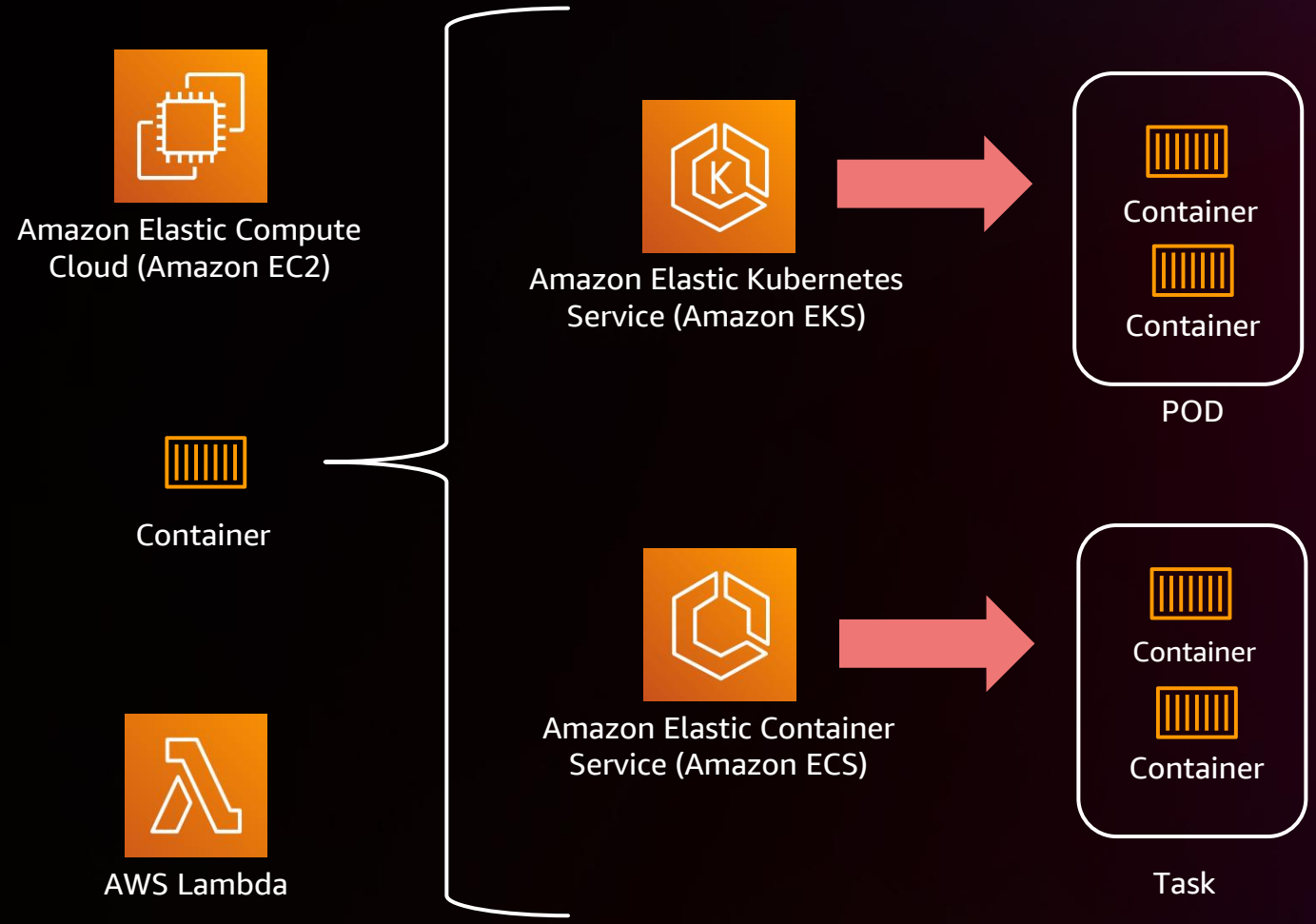
Amazon Route 53

AWS PrivateLink

Amazon API Gateway

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

Compute options



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

Building blocks for application networking

Service
discovery

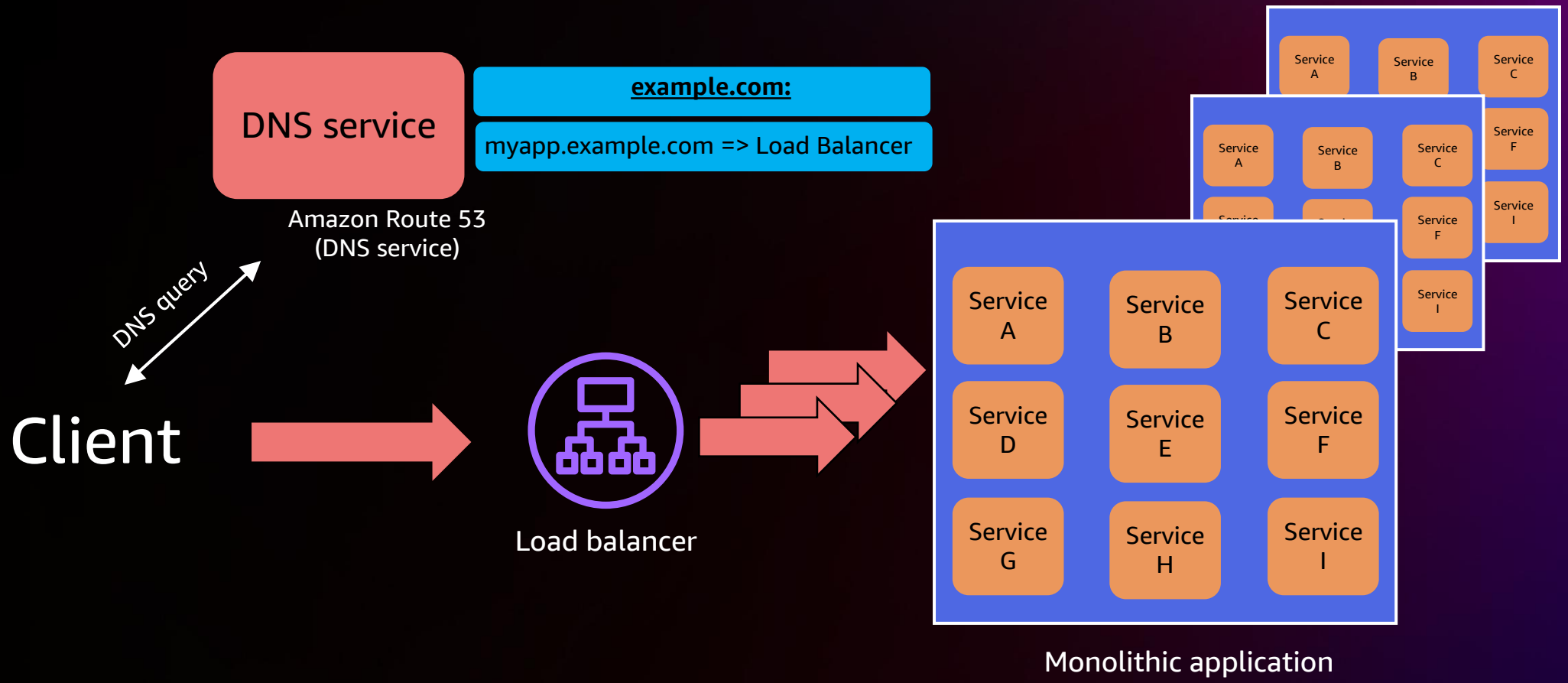
Service
connectivity

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

Service discovery

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

Where is my service?



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

Route 53

Domain registration

Domain hosting (public and private zones)

Resource health checking

Request routing (i.e., failover, latency, geolocation, etc.)

In-VPC resolver with logging and DNS firewall

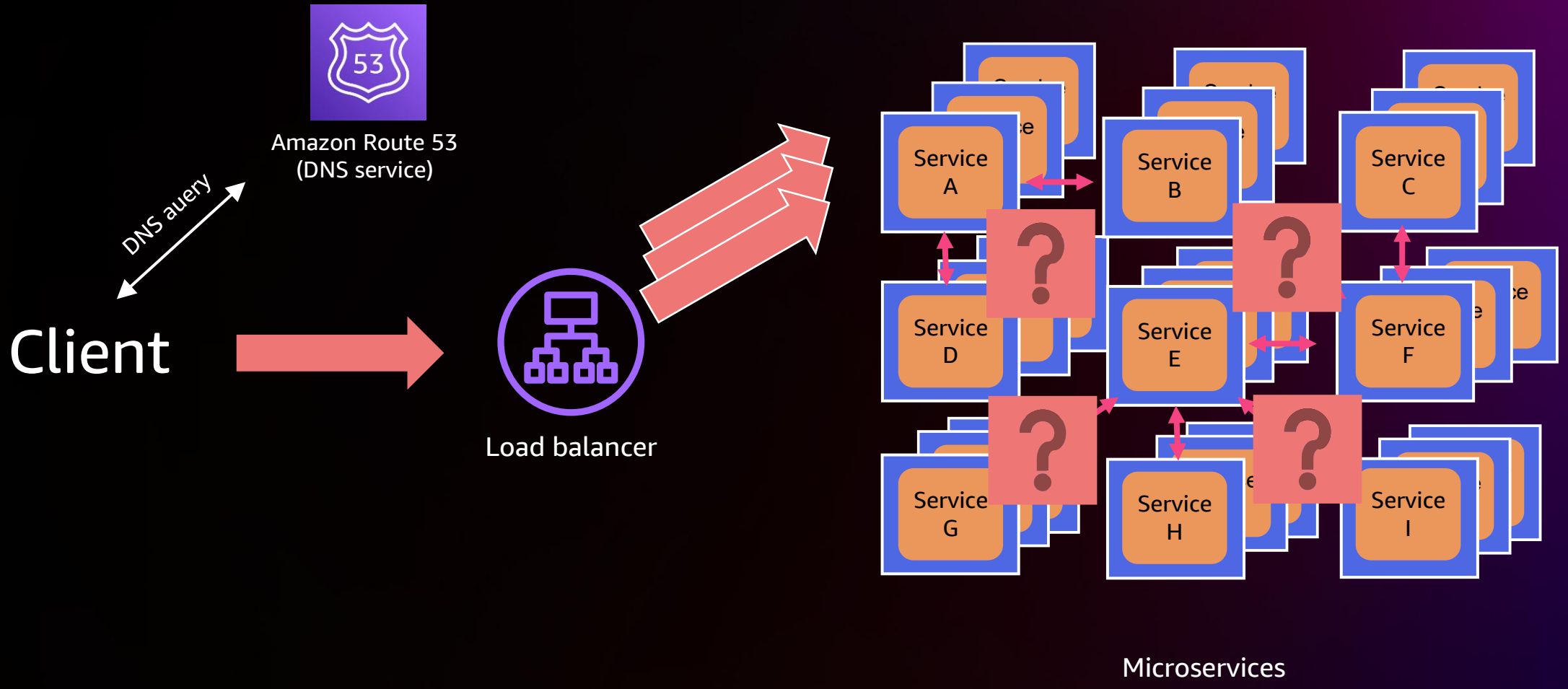


Learn more in session:
NET 206 – Amazon Route 53: What's in a Domain Name? A lot.

aws

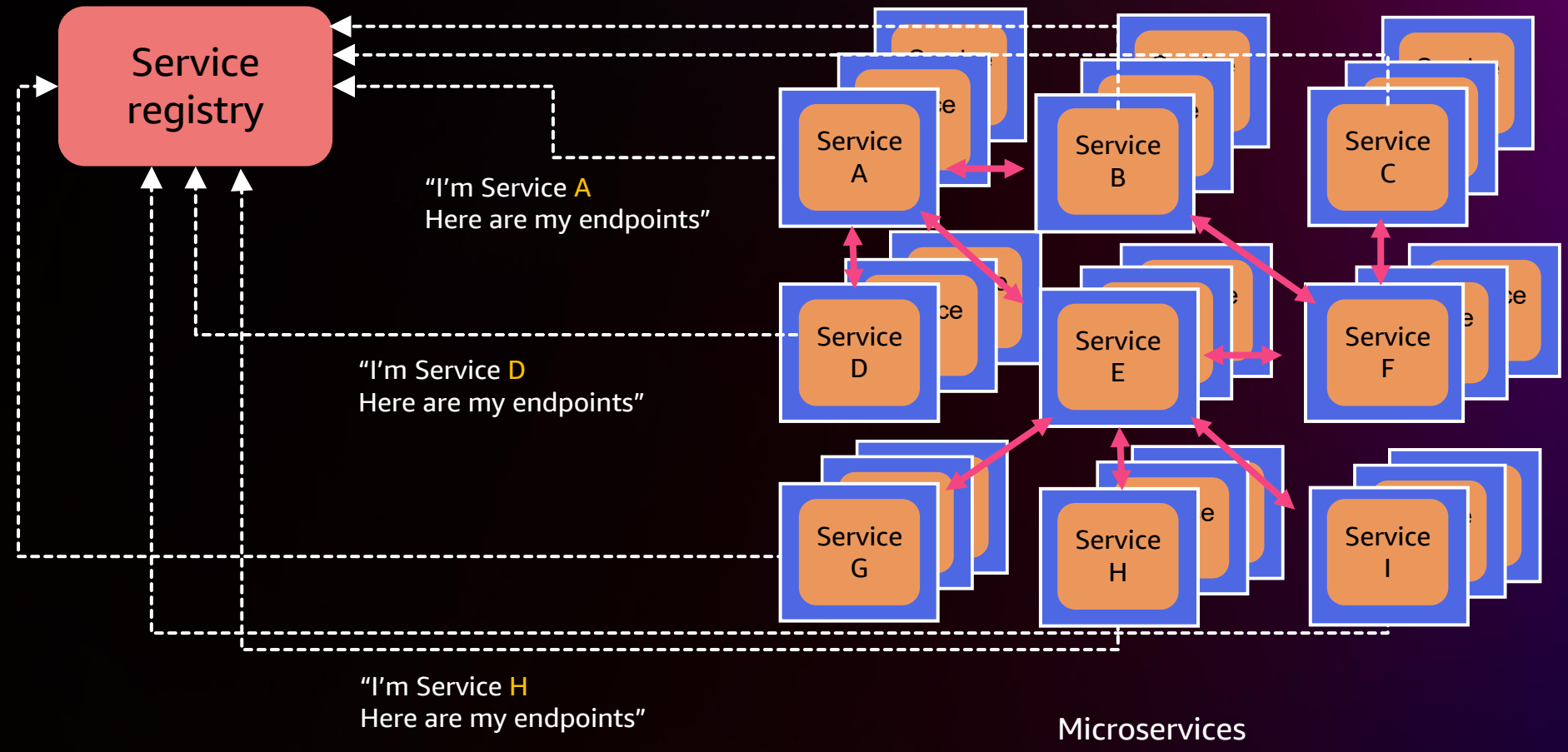
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where is my service?



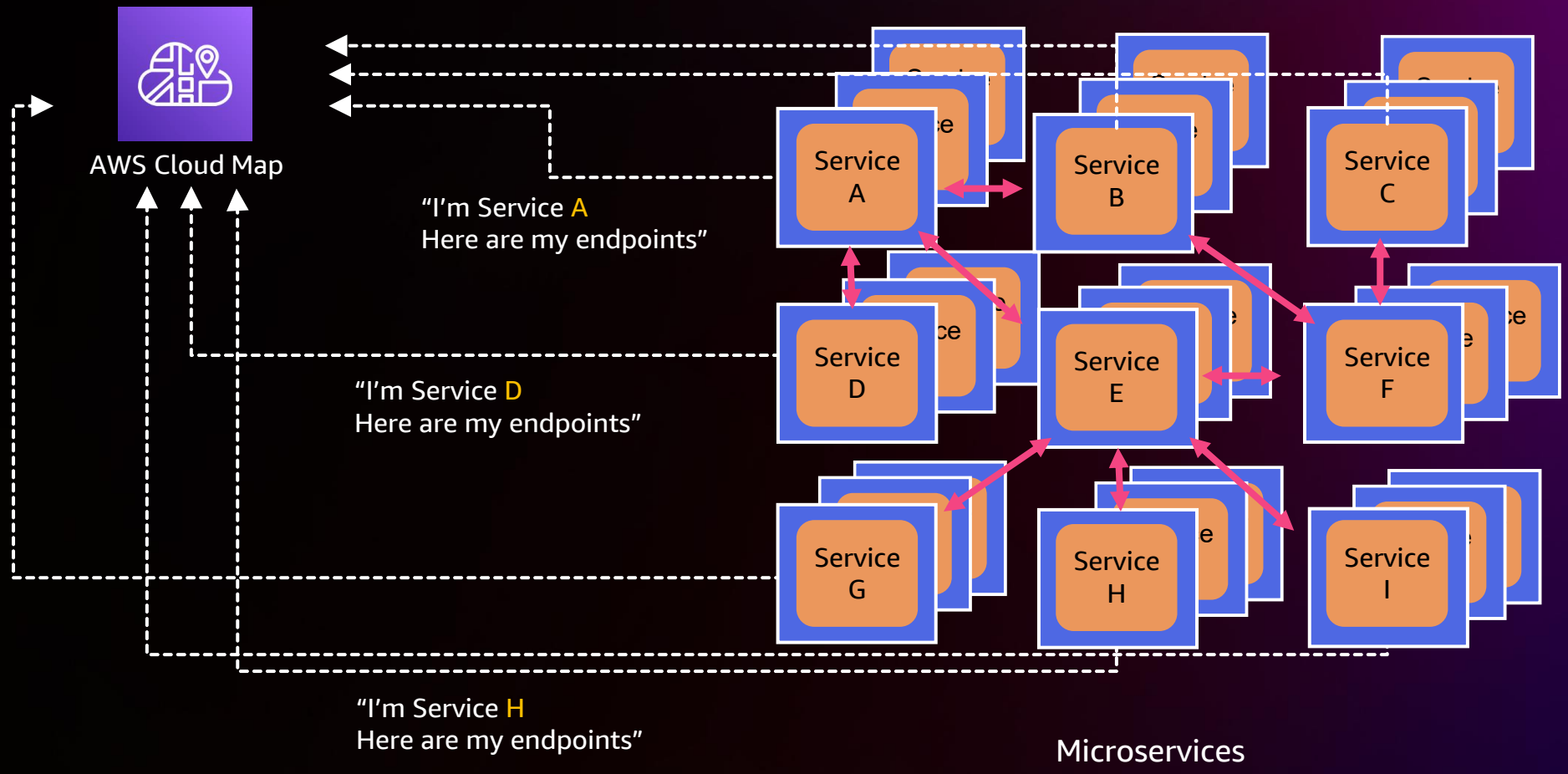
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where is my service?



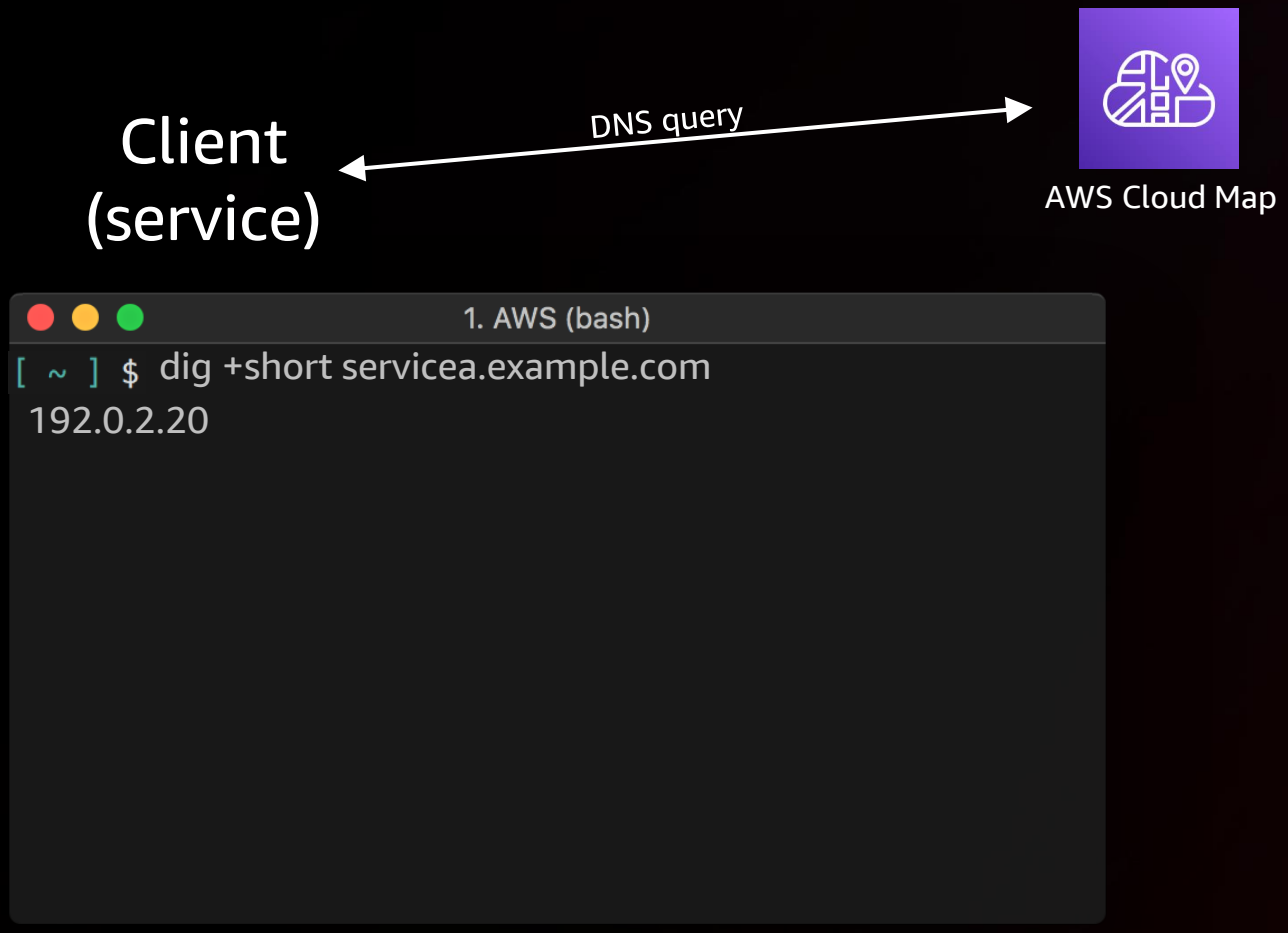
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

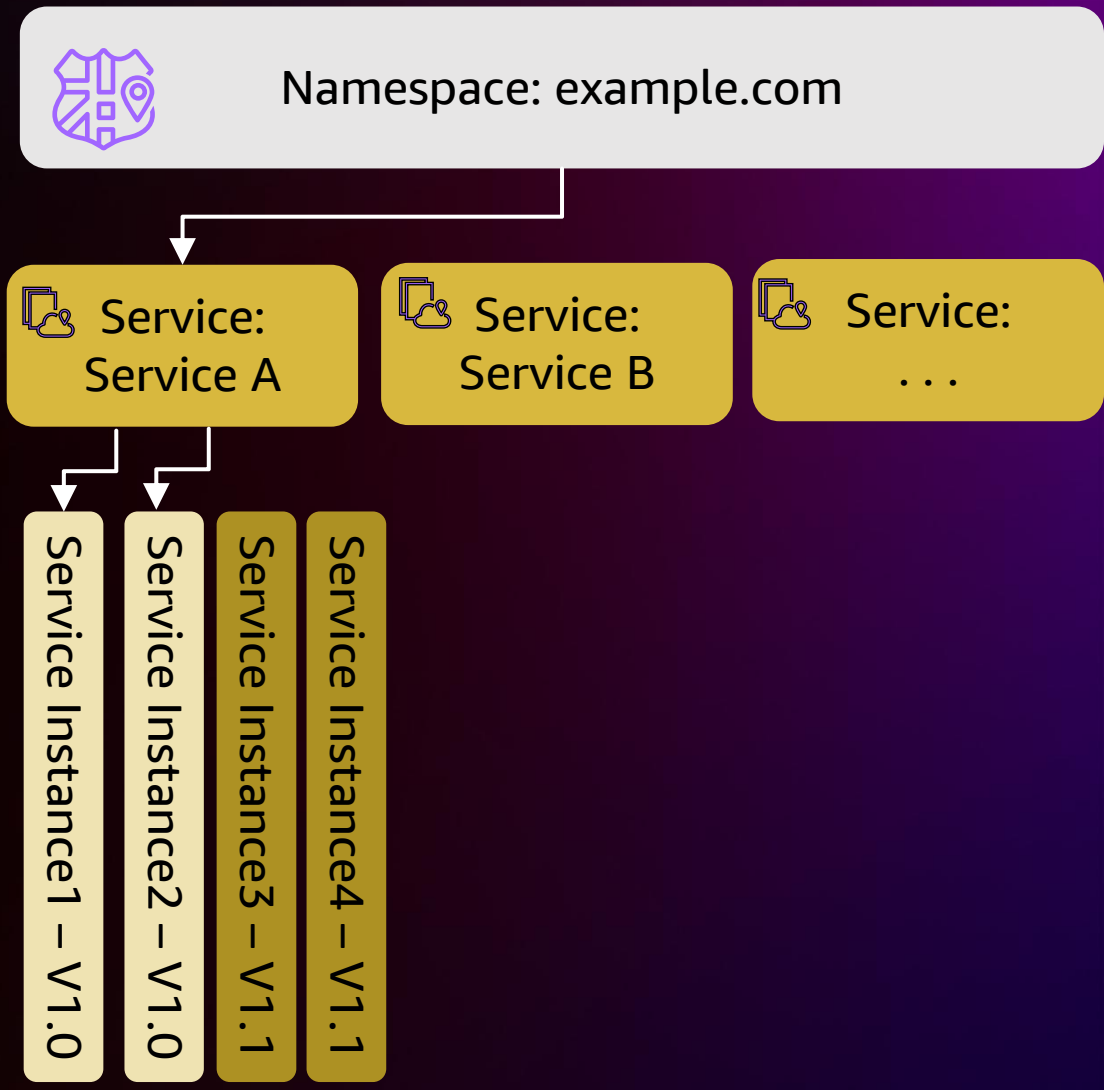
Where is my service?



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

AWS Cloud Map





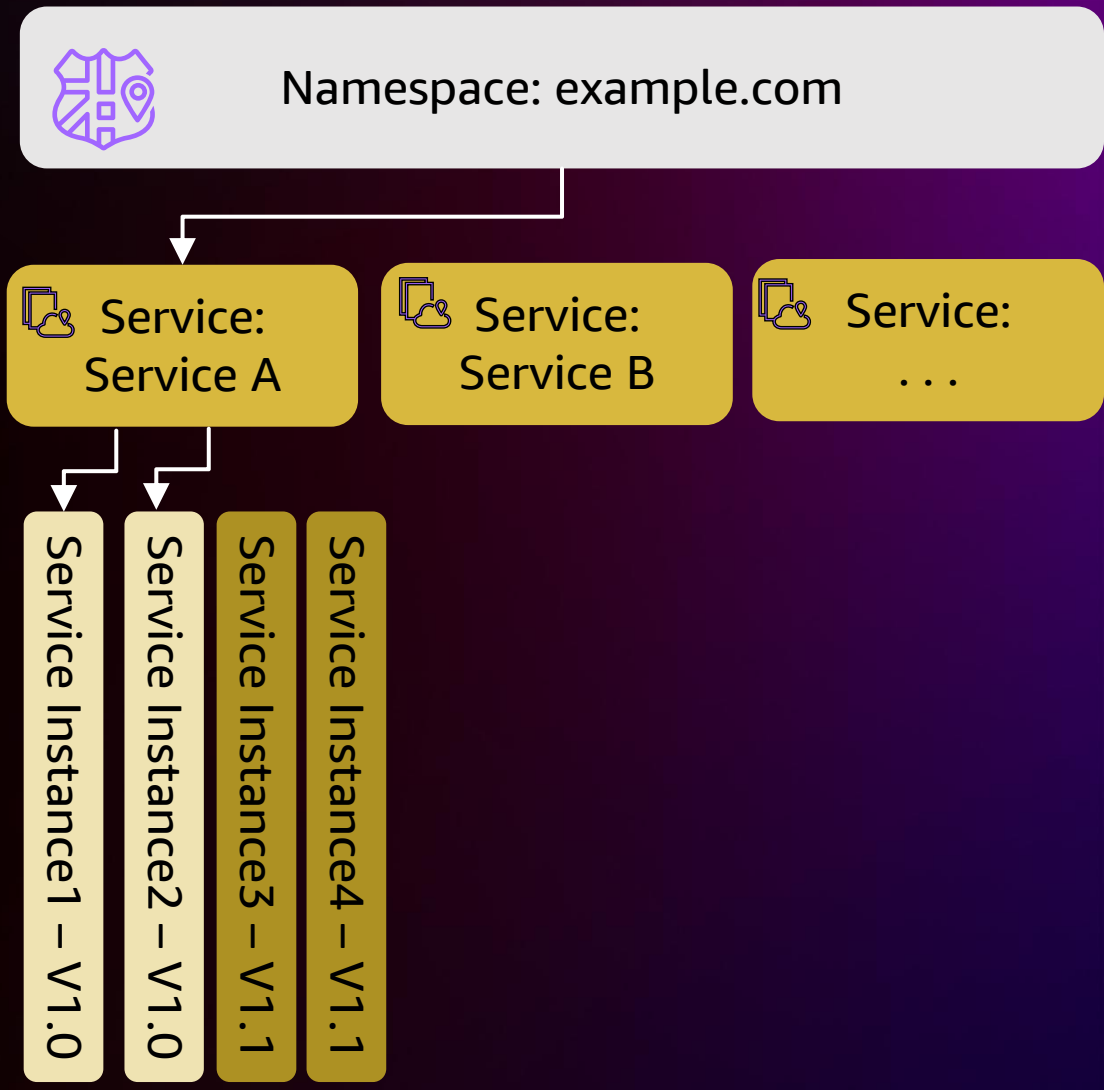
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Cloud Map



1. AWS (bash)

```
[ ~ ] $ aws servicediscovery list-instances --service-id srv-123
{
    "Instances": [
        {
            "Id": "serviceA-instance1",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "192.0.2.20",
                "AWS_INSTANCE_PORT": "8078",
                "PROJECT": "BLUE",
                "VERSION": "1.0"
            }
        },
        {
            "Id": "serviceA-instance2",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "192.0.2.21",
                "AWS_INSTANCE_PORT": "8078",
                "PROJECT": "BLUE",
                "VERSION`": "1.1"
            }
        }
    ]
}
```



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

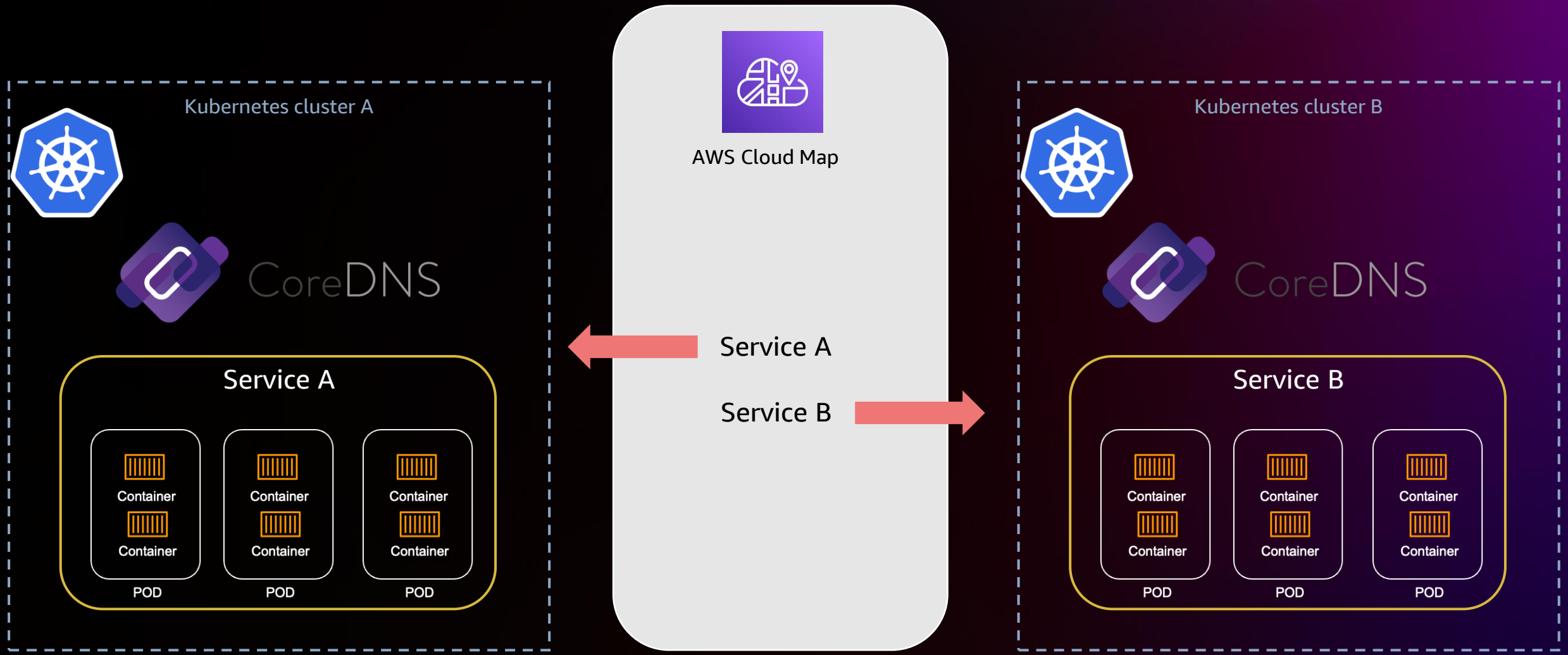
AWS Cloud Map: Benefits

 **Fast and secure**	• Regional service with **99.99%** availability SLA • Fast change propagation – under **5 seconds** • **Authenticated** calls for service discovery • Low latency discovery calls – **2 ms** average
 **Simple service discovery**	• Unified service discovery across all container services • **Attribute-based** service discovery • Discover service location and configuration parameters by a logical and friendly name
 **Name resolution**	• Support for CNAME and A records for ELBs • Multi-value answer routing returns up to 8 addresses • Optional DNS discovery mode for IP-based resources
 **Easy manageability**	• Easily scale applications across regions • Configure **Amazon Route 53 Health Checks** for IP-based resources • Integrates with AWS and open-source solutions

aws

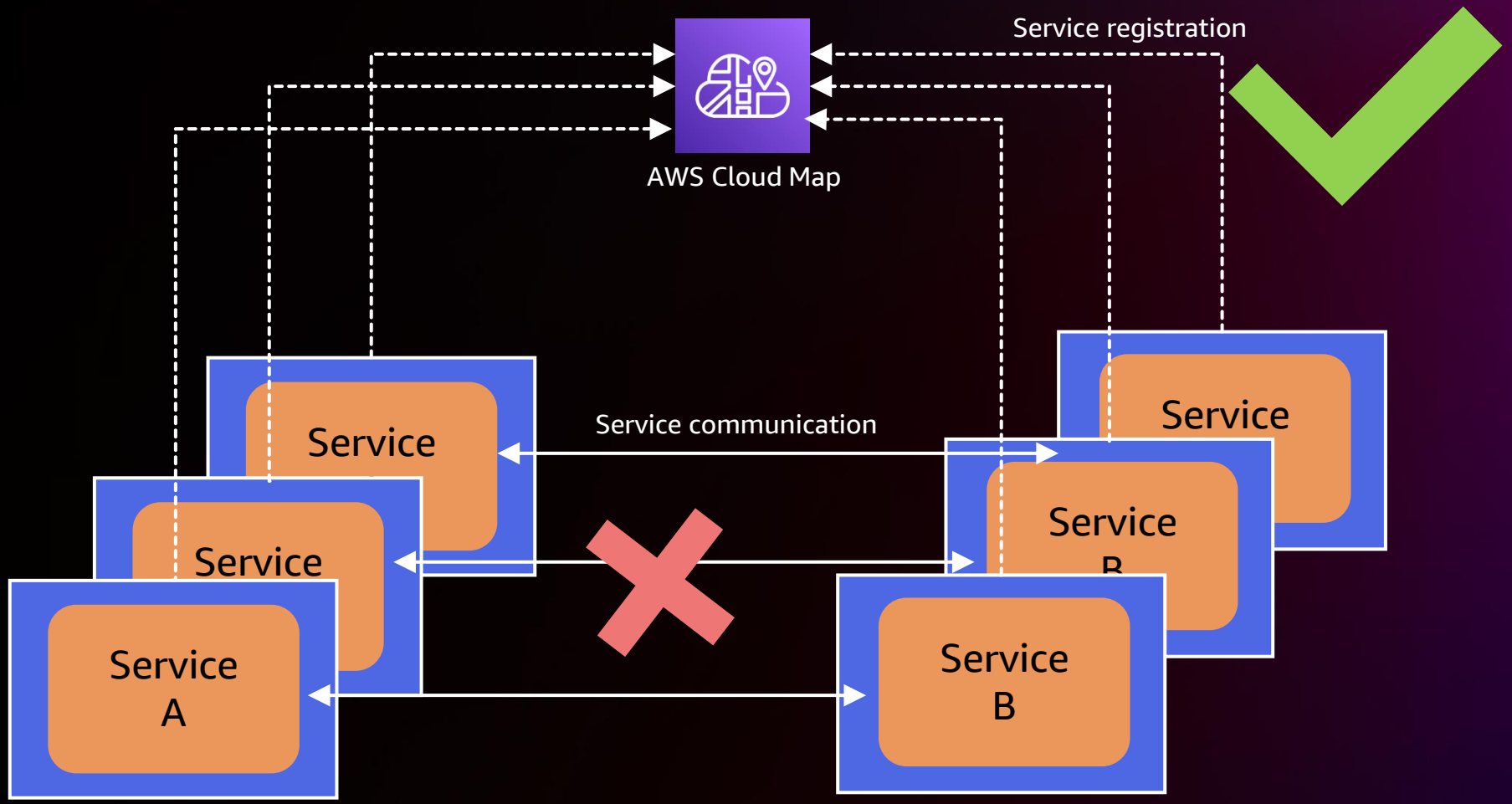
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Cloud Map and Kubernetes?



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

Service discovery



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

Service connectivity

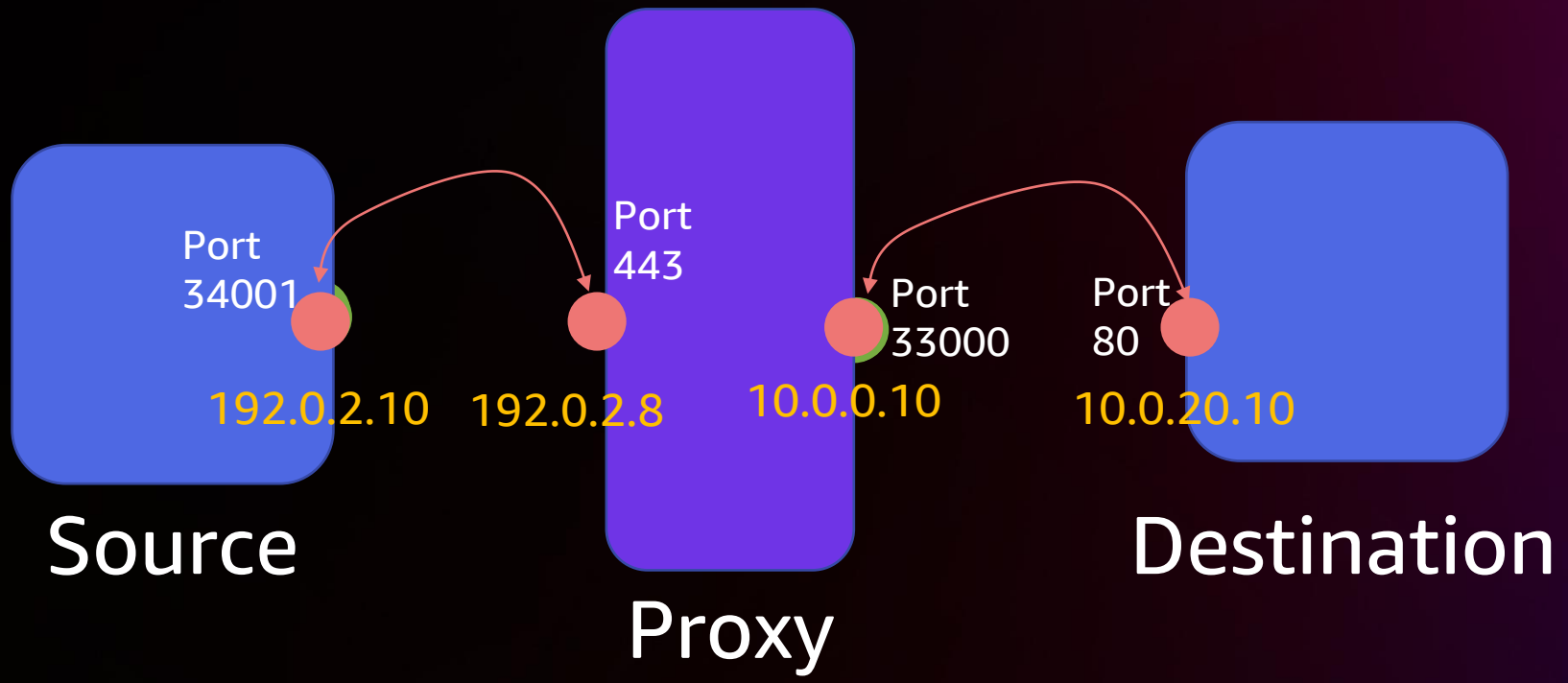
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of a proxy



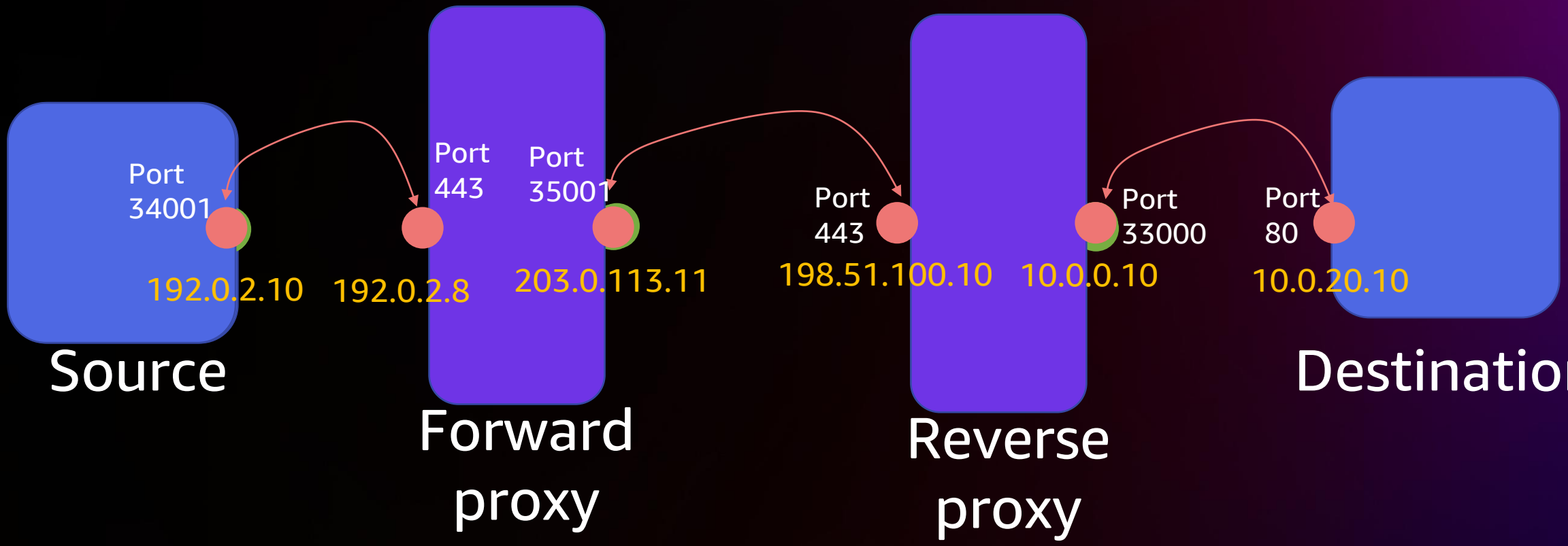
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of a proxy



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

Anatomy of a proxy



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

Why use a proxy?

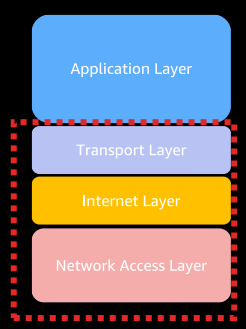
- TLS termination
- Load balancing
- Authentication/authorization
- Tracing, logging
- Security
- Application traffic capture



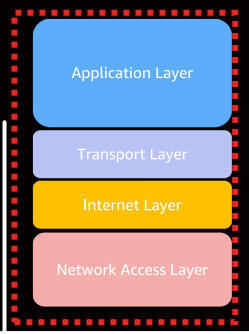
Photo by
Matheus Bertelli

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

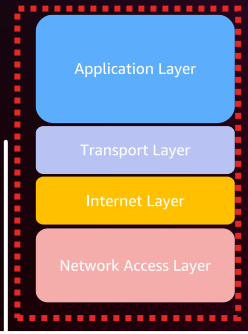
AWS services – Proxy-based



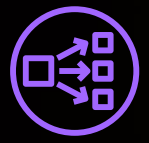
TCP/UDP



Application



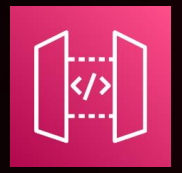
Service mesh
&
beyond



Network Load Balancer



Application Load Balancer



Amazon API Gateway



AWS App Mesh



AWS Global Accelerator



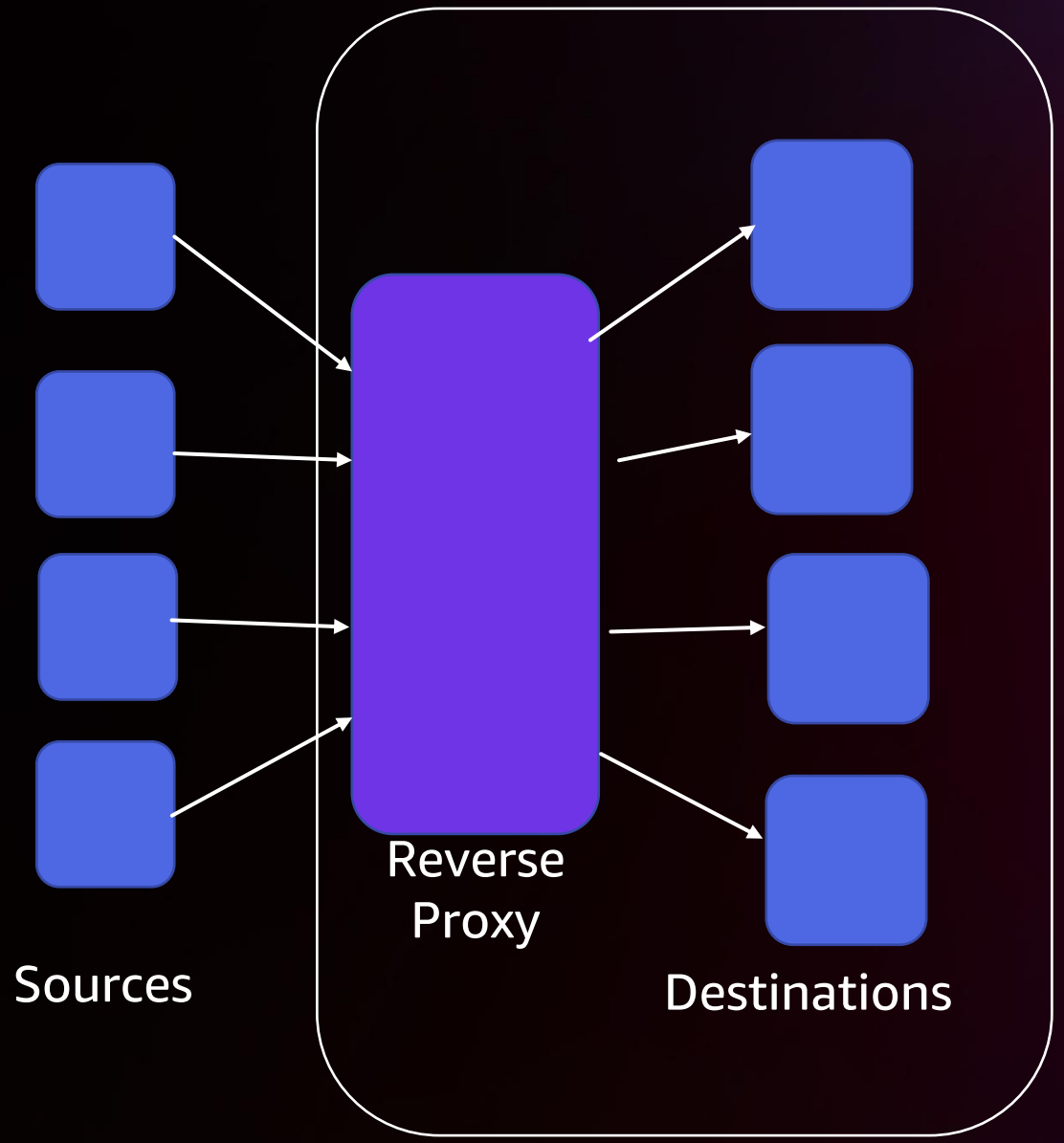
Amazon CloudFront



Amazon VPC Lattice

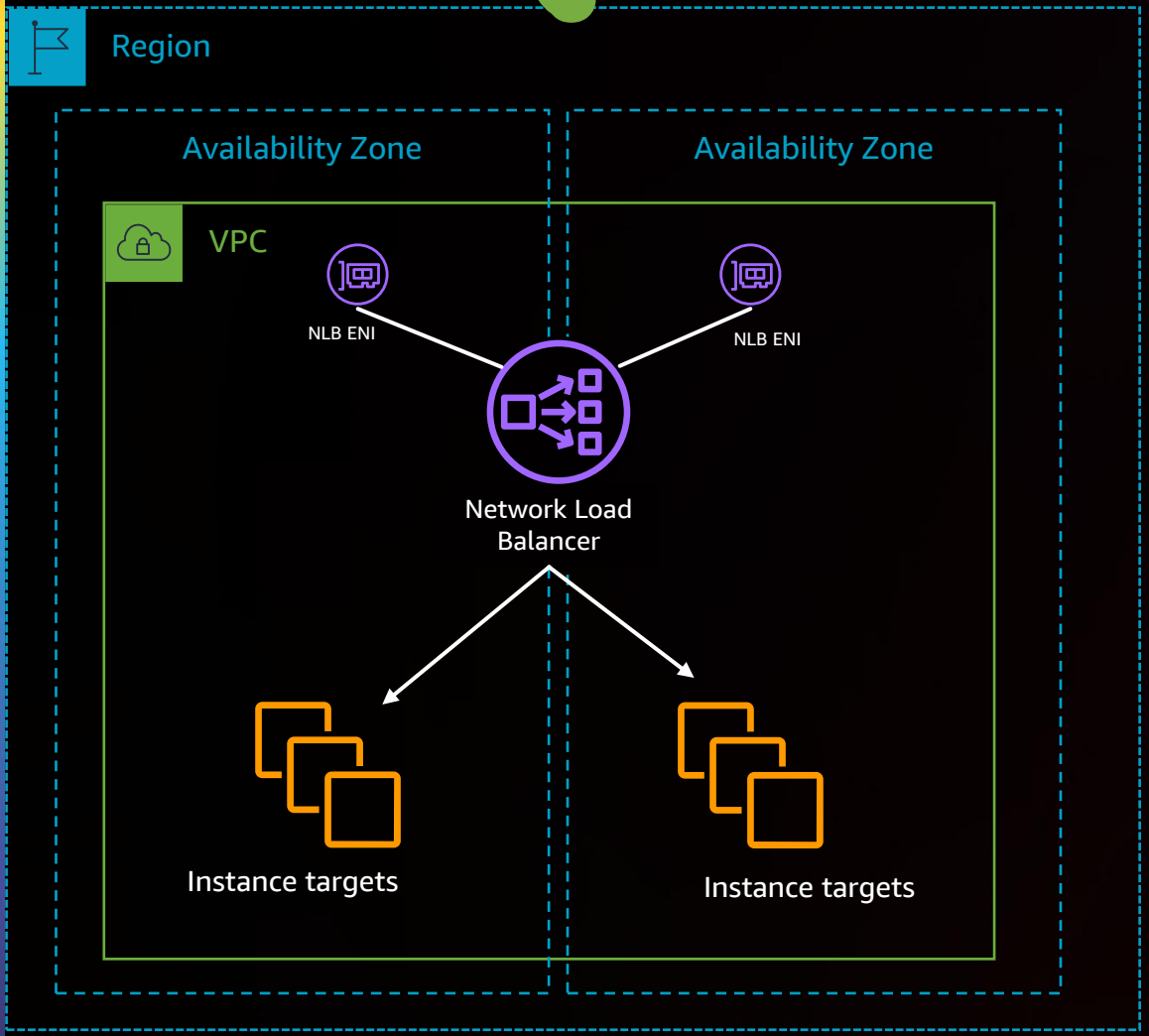
aws

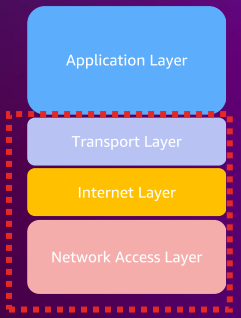
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

Network Load Balancer (NLB)





NLB network characteristics:

- Operates at TCP/UDP Layer + TLS termination
- 1x static IP per AZ (IPv4 & IPv6)
- Supports client IP preservation in packet
- Target options:

Amazon EC2 Instance

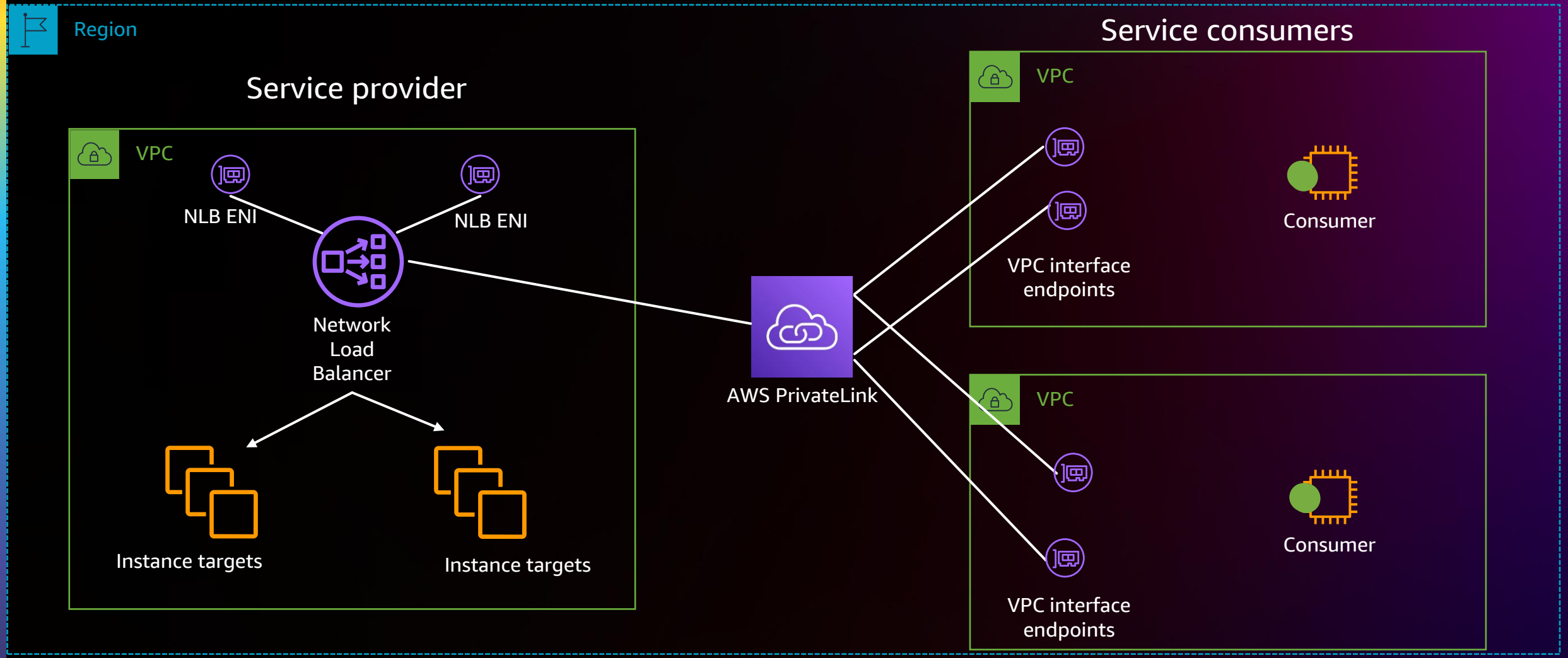
IP address

Application Load Balancer

Containers POD/task

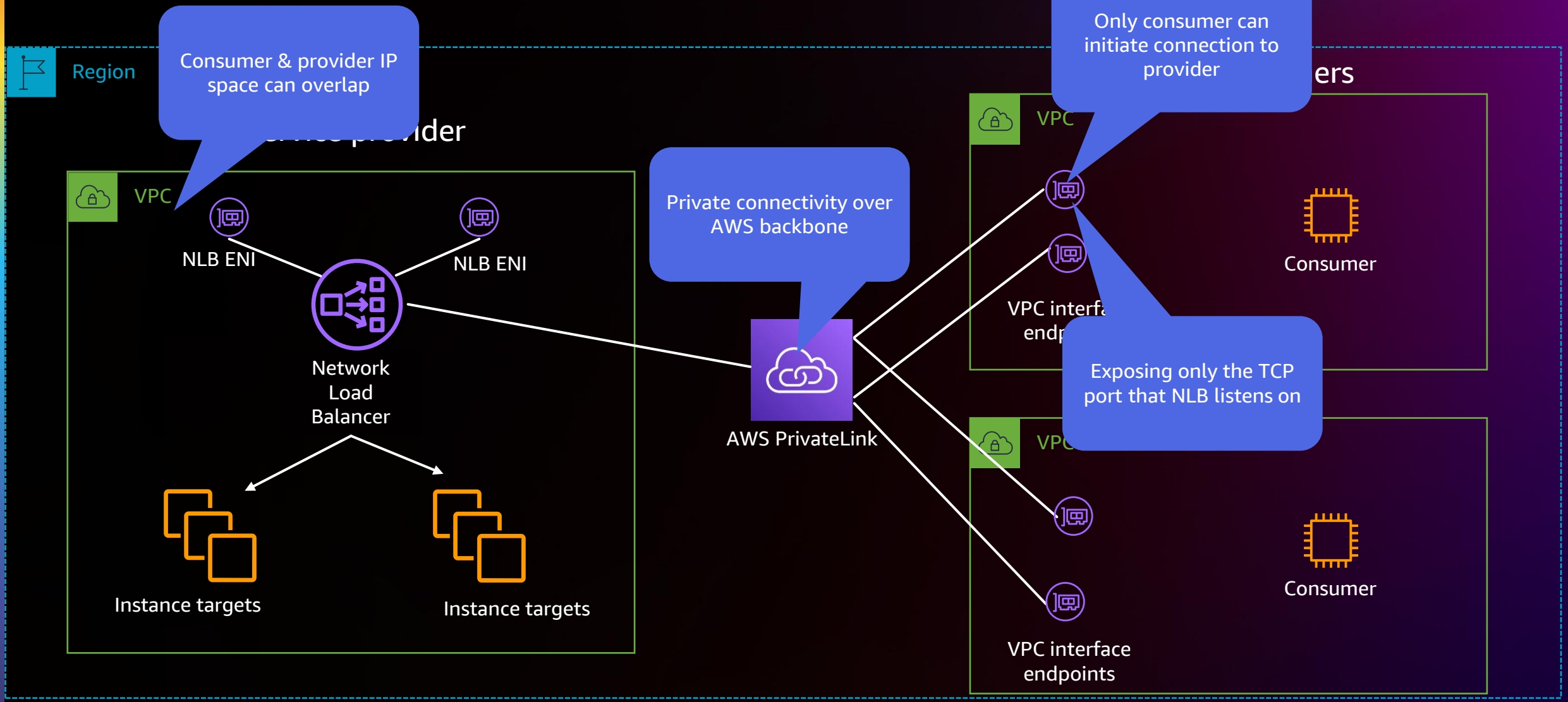
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

PrivateLink

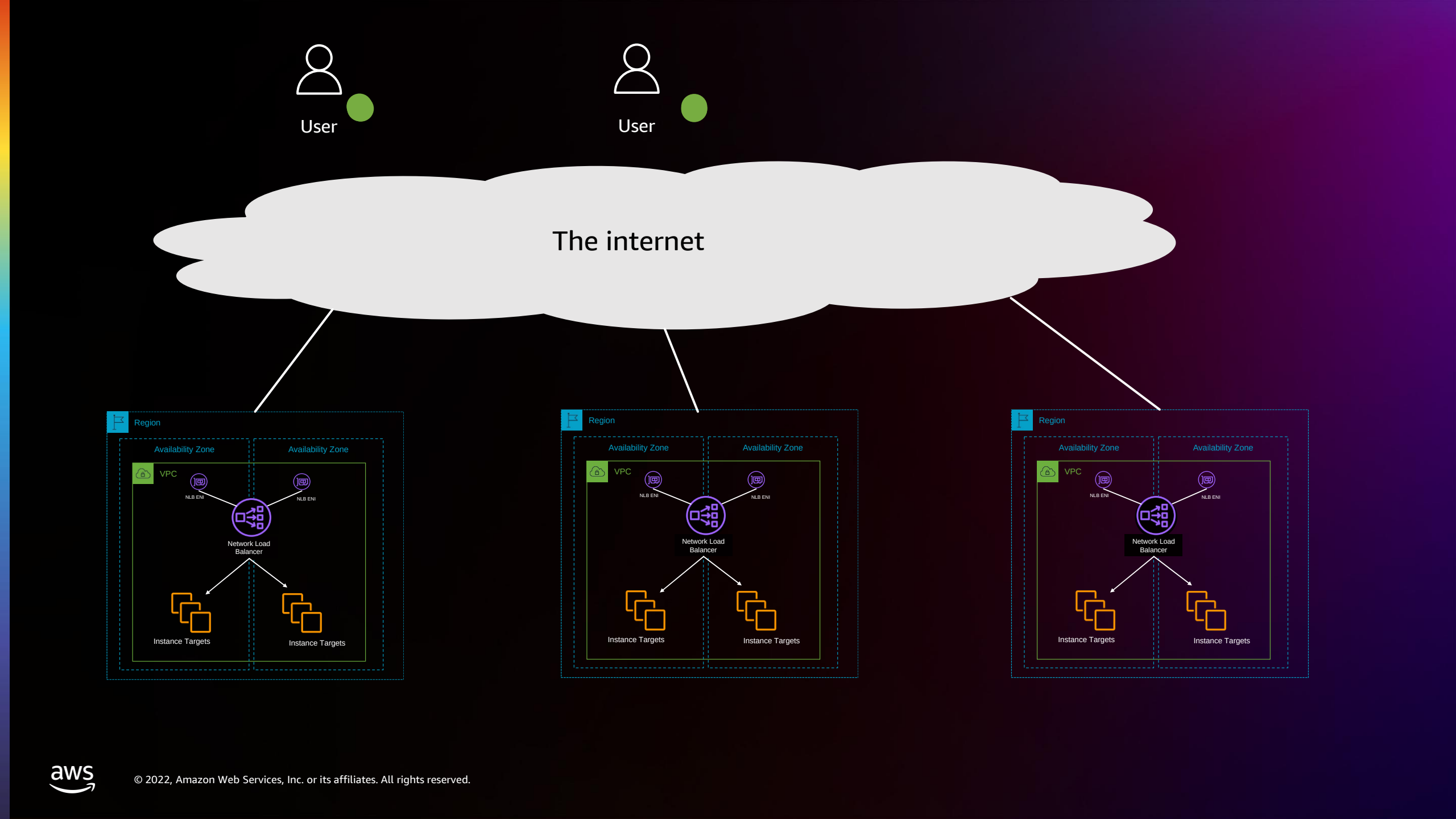


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

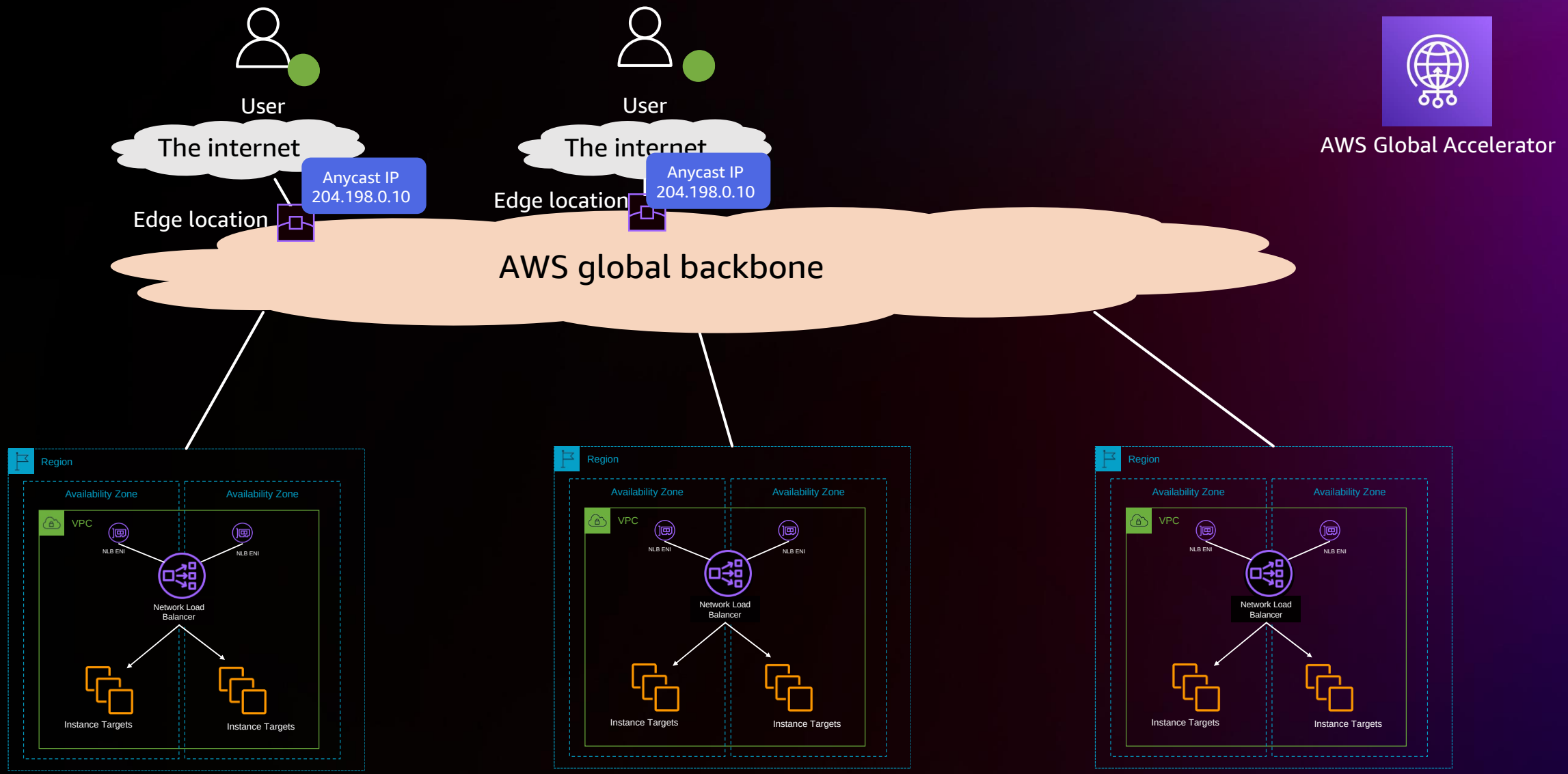
PrivateLink



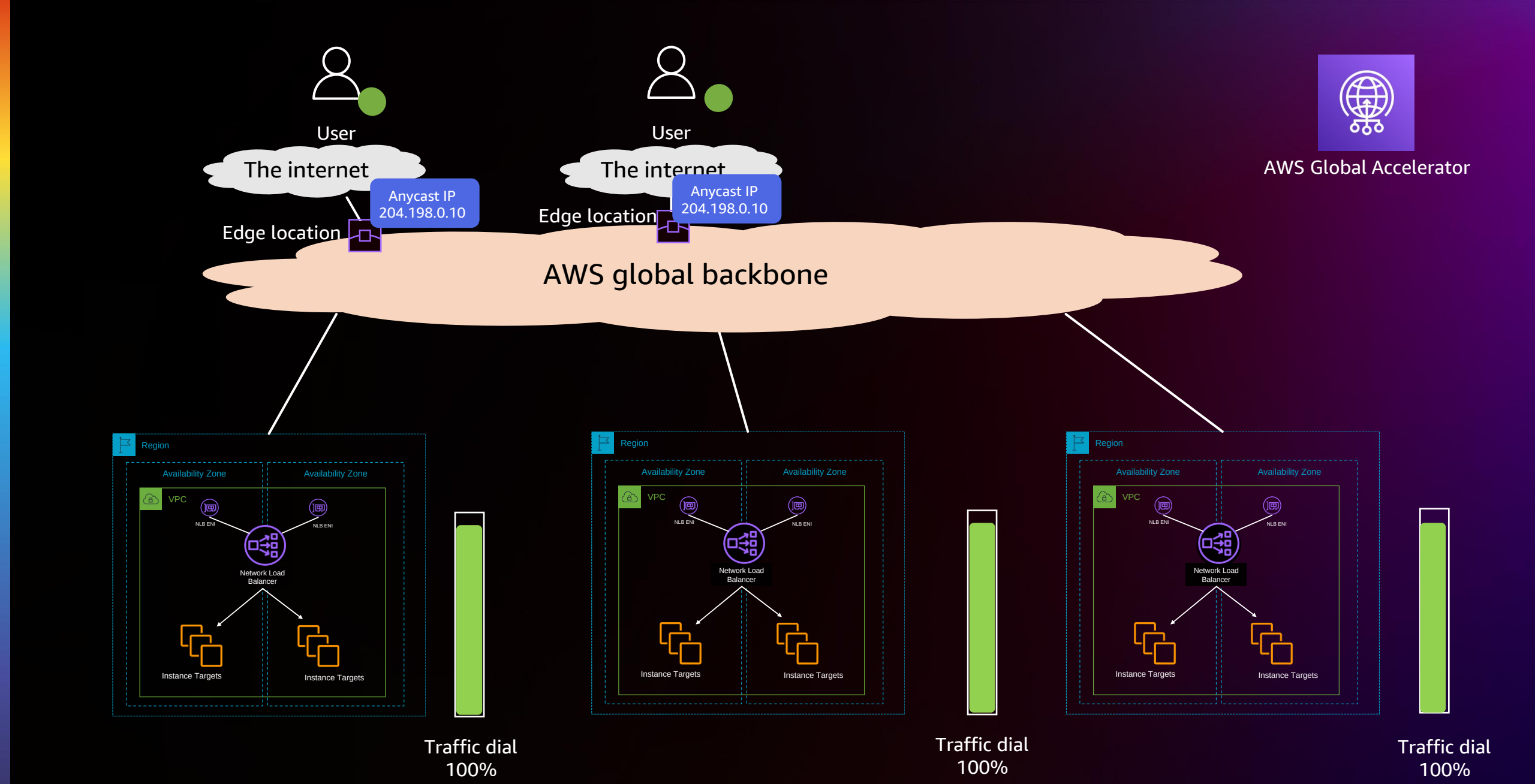
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



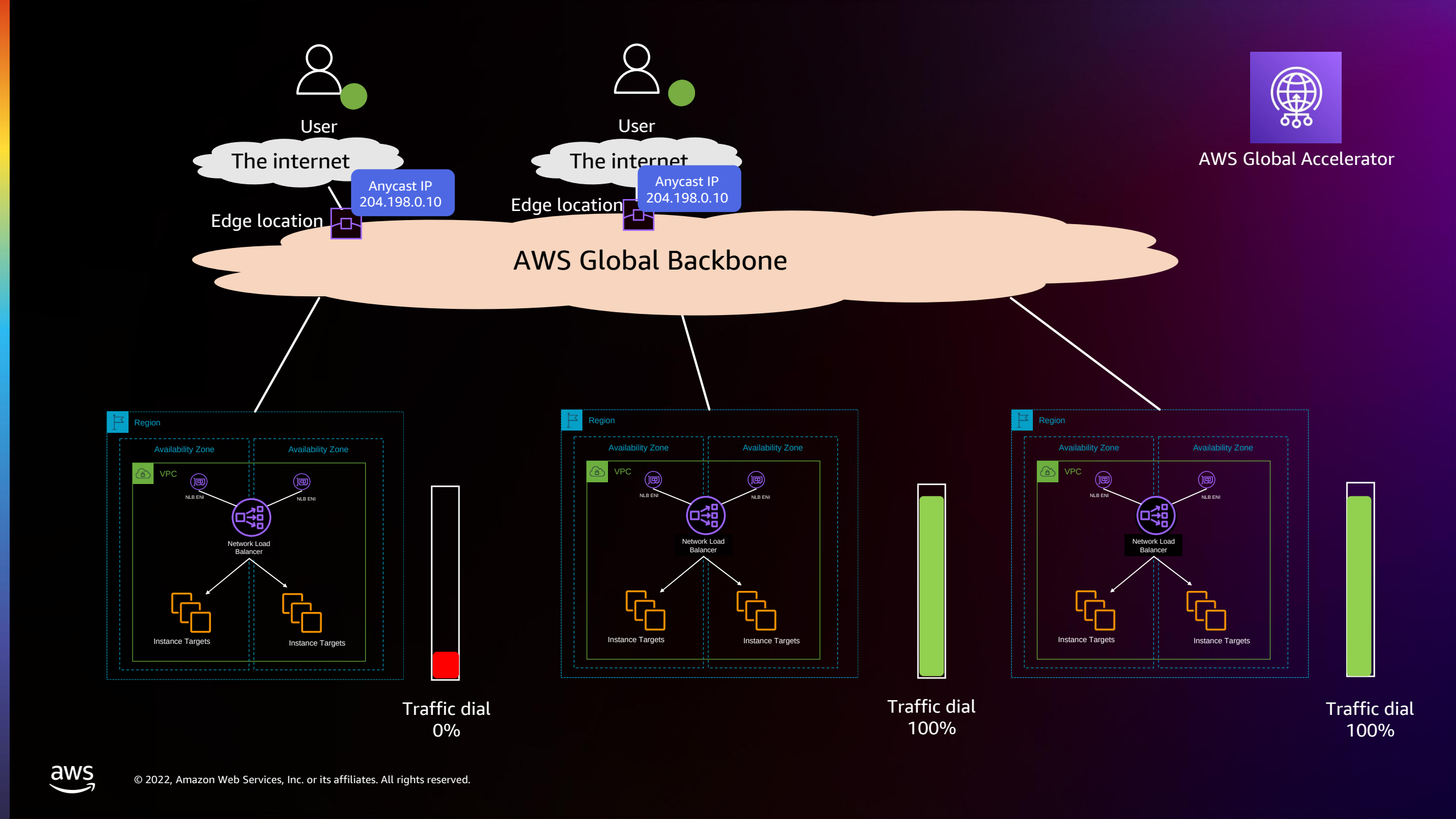
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

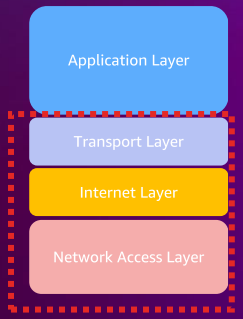


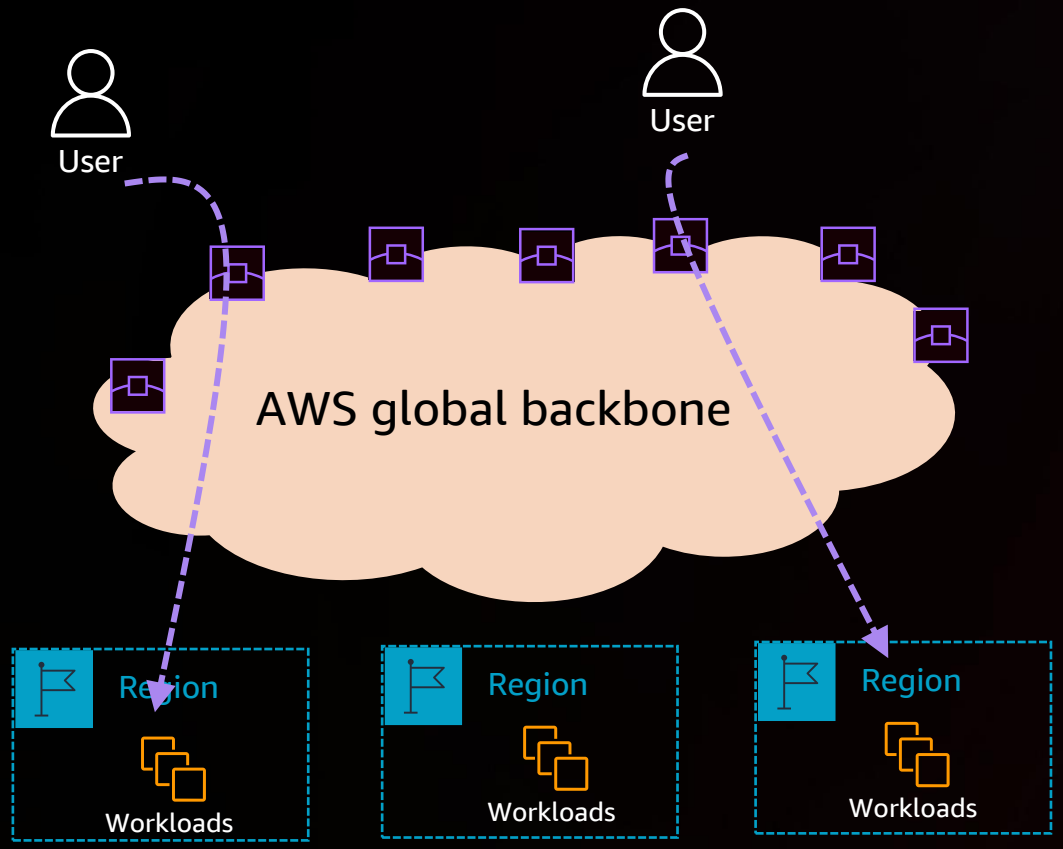
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

AWS Global Accelerator (AGA)





AGA network characteristics:

- Operates at TCP/UDP
- 2x static anycast IPs per deployment (IPv4 & IPv6)
- Supports client IP preservation in packet
- Target (endpoint) options:

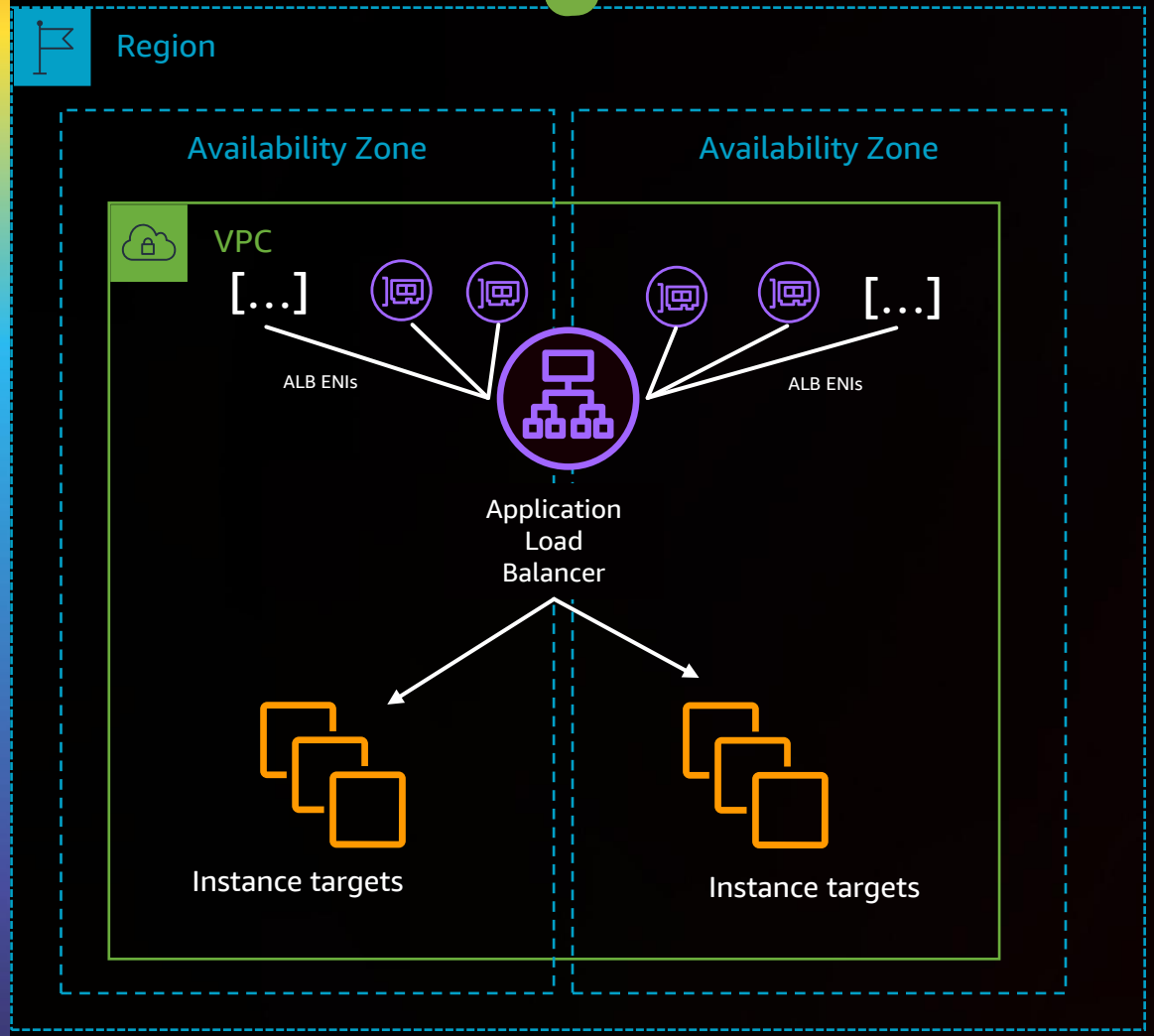
Network Load Balancer

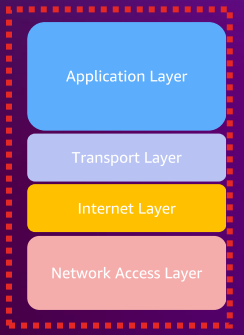
Application Load Balancer

EC2 instance

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

Application Load Balancer (ALB)





ALB network characteristics:

- Operates at application layer (TLS termination, path/host-based routing, etc.)
- Dynamic IPs (IPv4 & IPv6)
- Client IP preserved in HTTP headers (not in packet)
- Target options:



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

ALB vs. NLB

Product comparisons

You can select the appropriate load balancer based on your application needs. If you need flexible application management, we recommend that you use an Application Load Balancer. If extreme performance and static IP is needed for your application, we recommend that you use a Network Load Balancer. If you have an existing application that was built within the EC2-Classic network, then you should use a Classic Load Balancer.

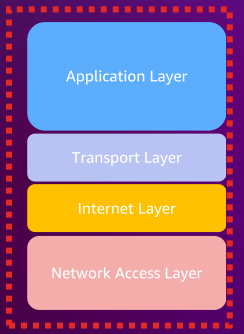
Feature	Application Load Balancer	Network Load Balancer	Gateway Load Balancer	Classic Load Balancer
Load Balancer type	Layer 7	Layer 4	Layer 3 Gateway + Layer 4 Load Balancing	Layer 4/7
Target type	IP, Instance, Lambda	IP, Instance, Application Load Balancer	IP, Instance	
Terminates flow/proxy behavior	Yes	Yes	No	Yes
Protocol listeners	HTTP, HTTPS, gRPC	TCP, UDP, TLS	IP	TCP, SSL/TLS, HTTP, HTTPS
Reachable via	VIP	VIP	Route table entry	
Layer 7				

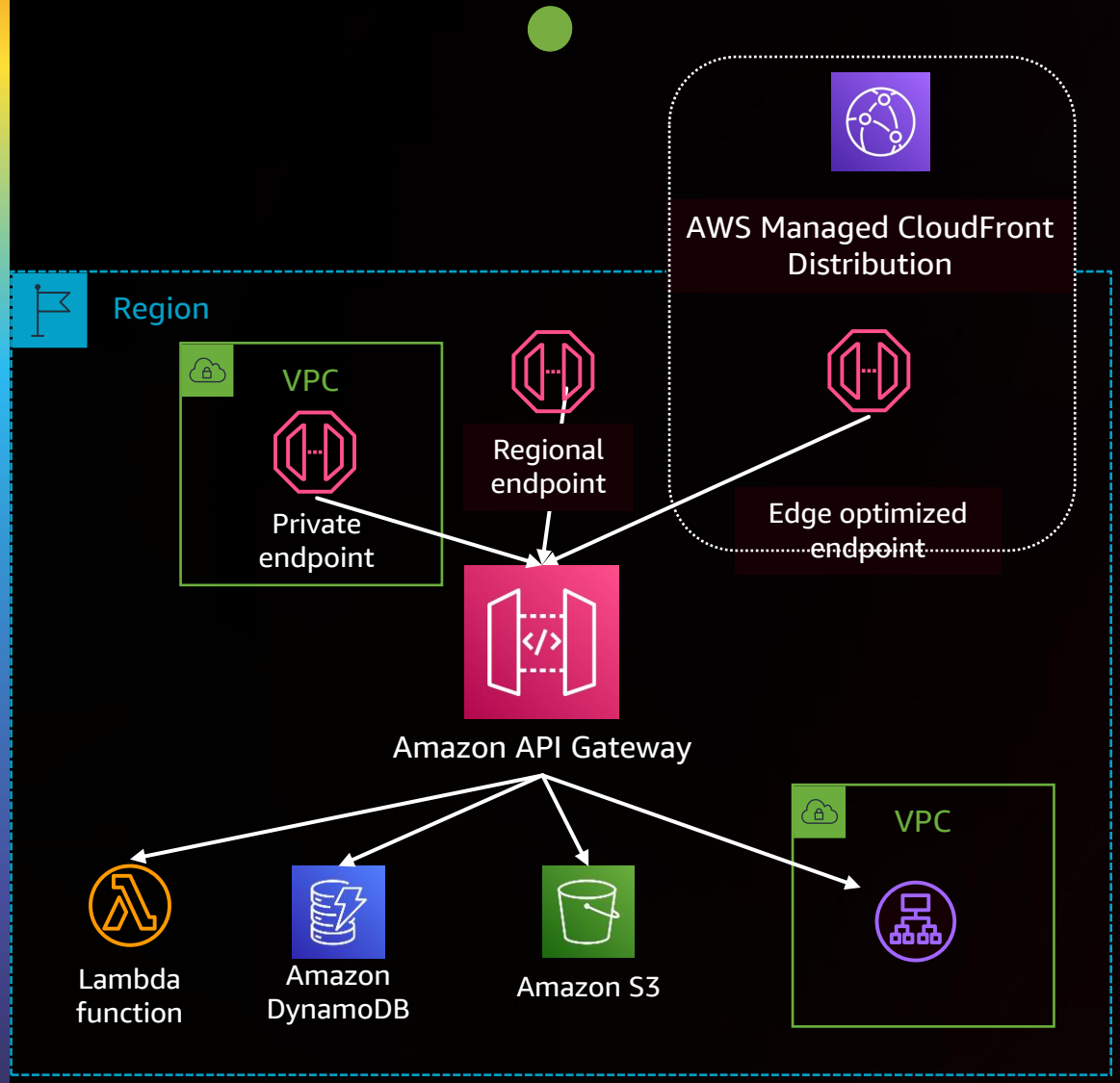


aws

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

Amazon API Gateway (APIGW)





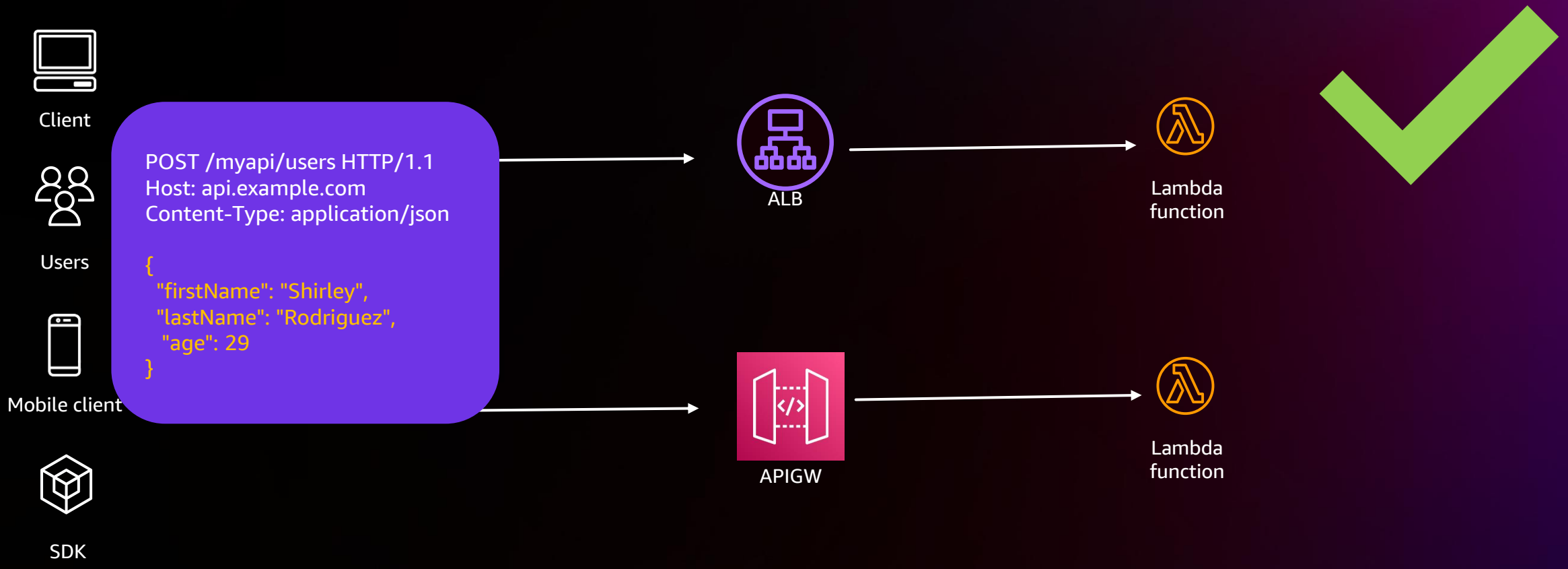
APIGW network characteristics:

- Operates at application layer (REST & HTTP)
- Static IPv4 when private endpoint deployed in an Amazon VPC
- Client IP preserved in HTTP headers (not in packet)
- Backend integration options:

Lambda function | AWS services | Elastic Load Balancing (via VPC link) | HTTP endpoint

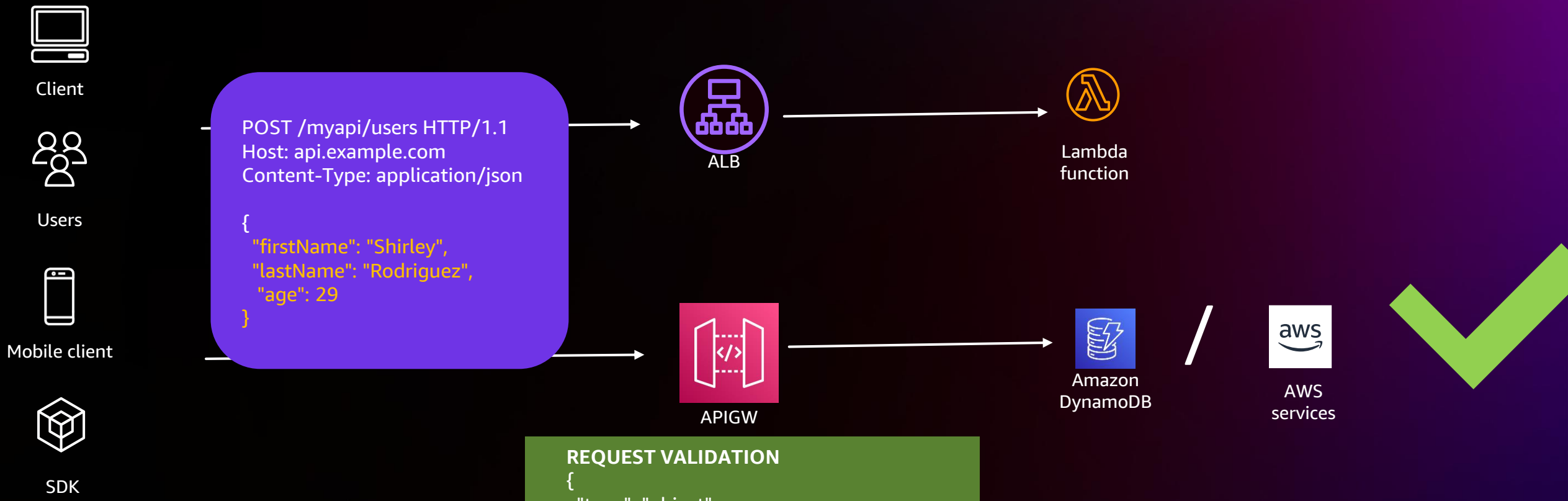
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ALB vs. APIGW



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

ALB vs. APIGW



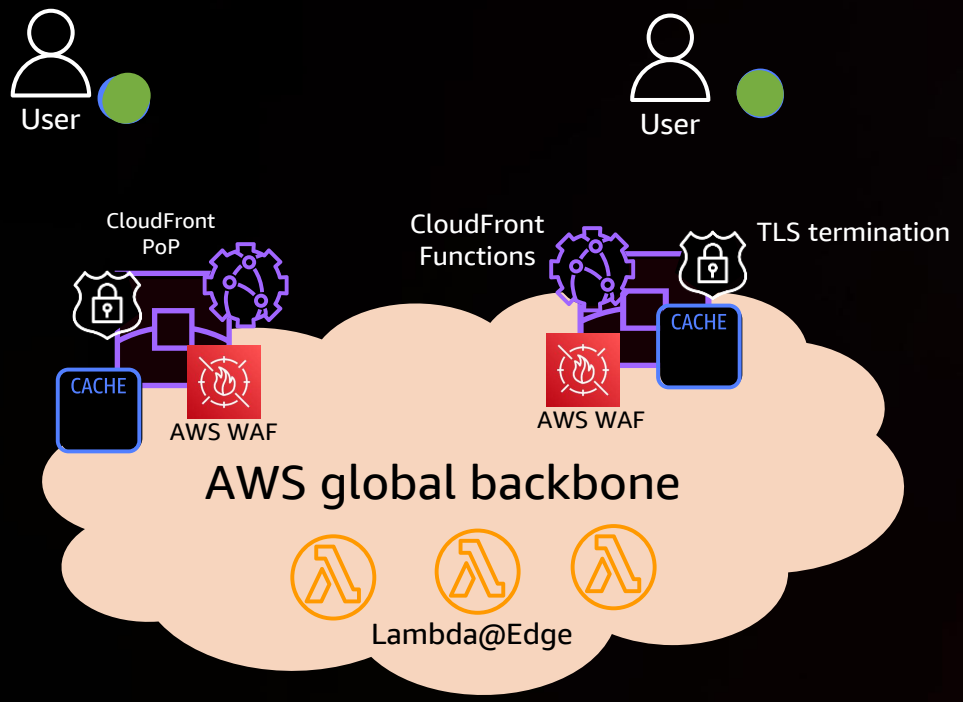
REQUEST VALIDATION

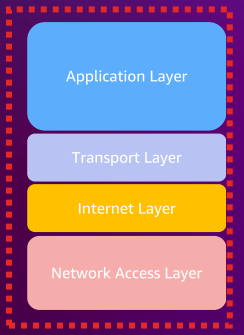
```
{
  "type": "object",
  "required": ["firstName", "lastName"],
  "properties": {
    "firstName": {"type": "string"},
    "lastName": {"type": "string"},
    "age": {"type": "number"}
  }
}
```

- mTLS
- Data transformation
- Request throttling
- Authentication

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

Amazon CloudFront





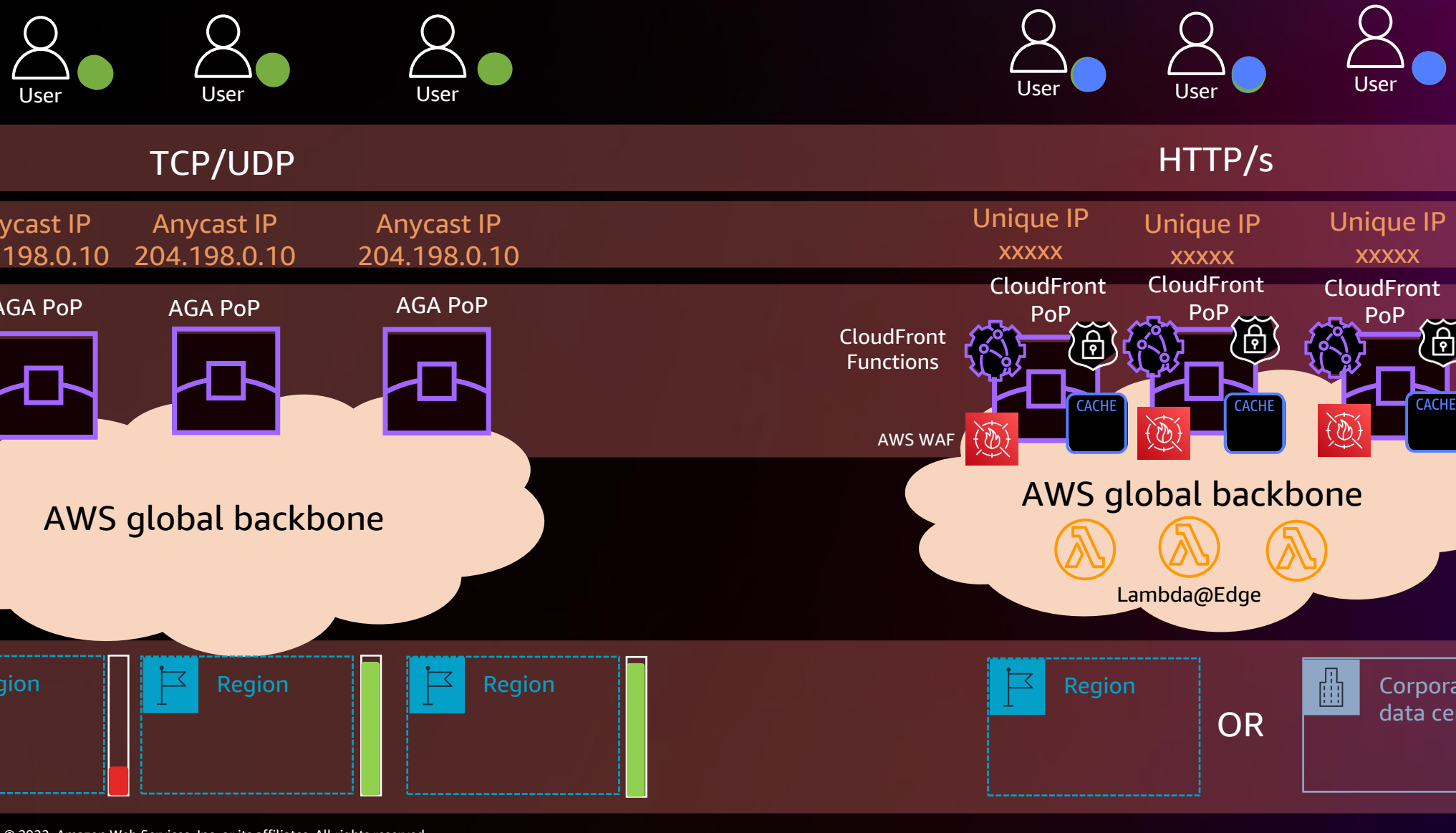
CloudFront network characteristics:

- Operates at application layer (TLS termination, caching, edge functions)
- Dynamic IPs depending on the edge PoP (IPv4 & IPv6)
- Client IP preserved in HTTP headers (not in packet)
- Origin options:

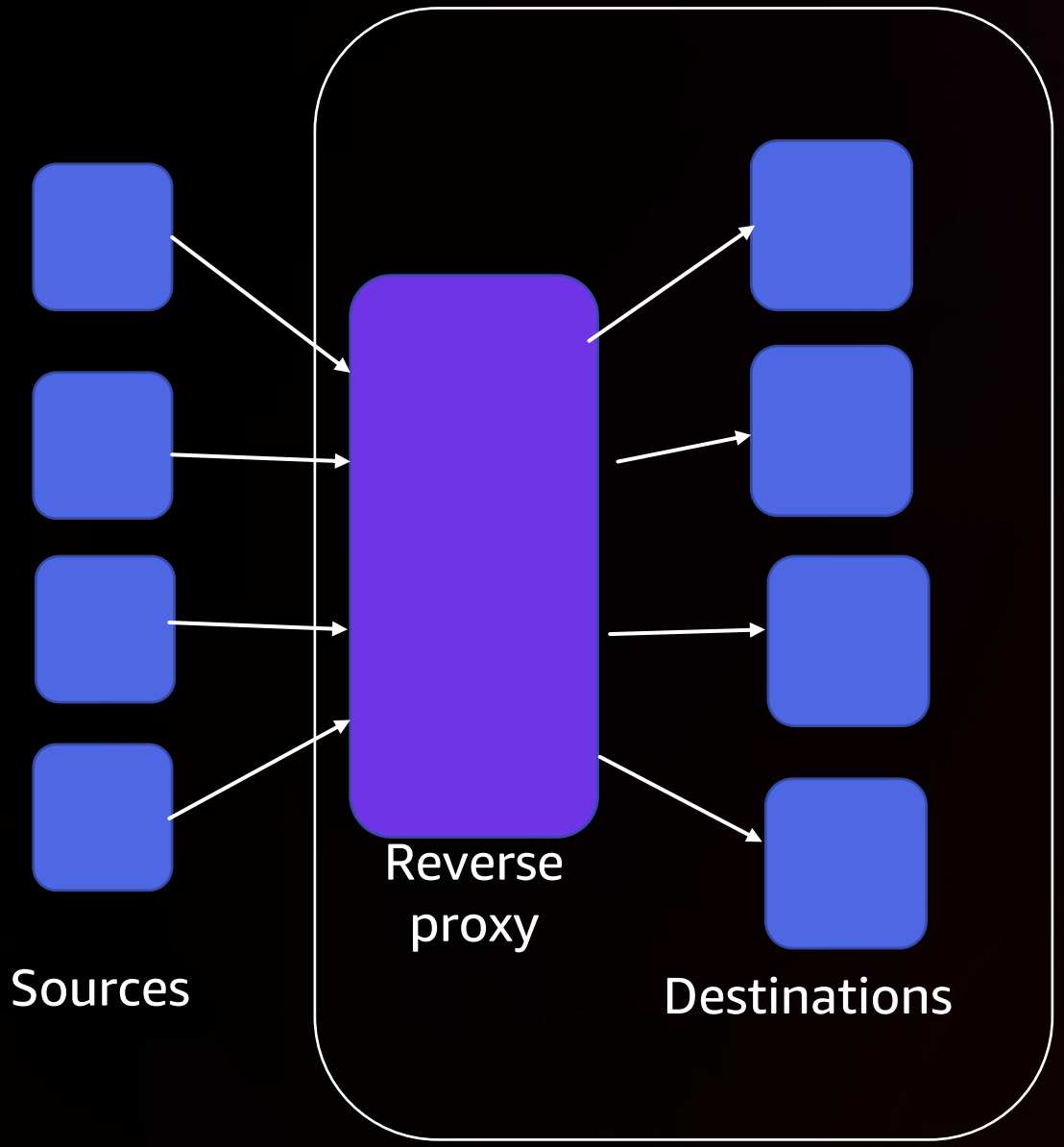
Any HTTP/s endpoint
AWS or on-premises

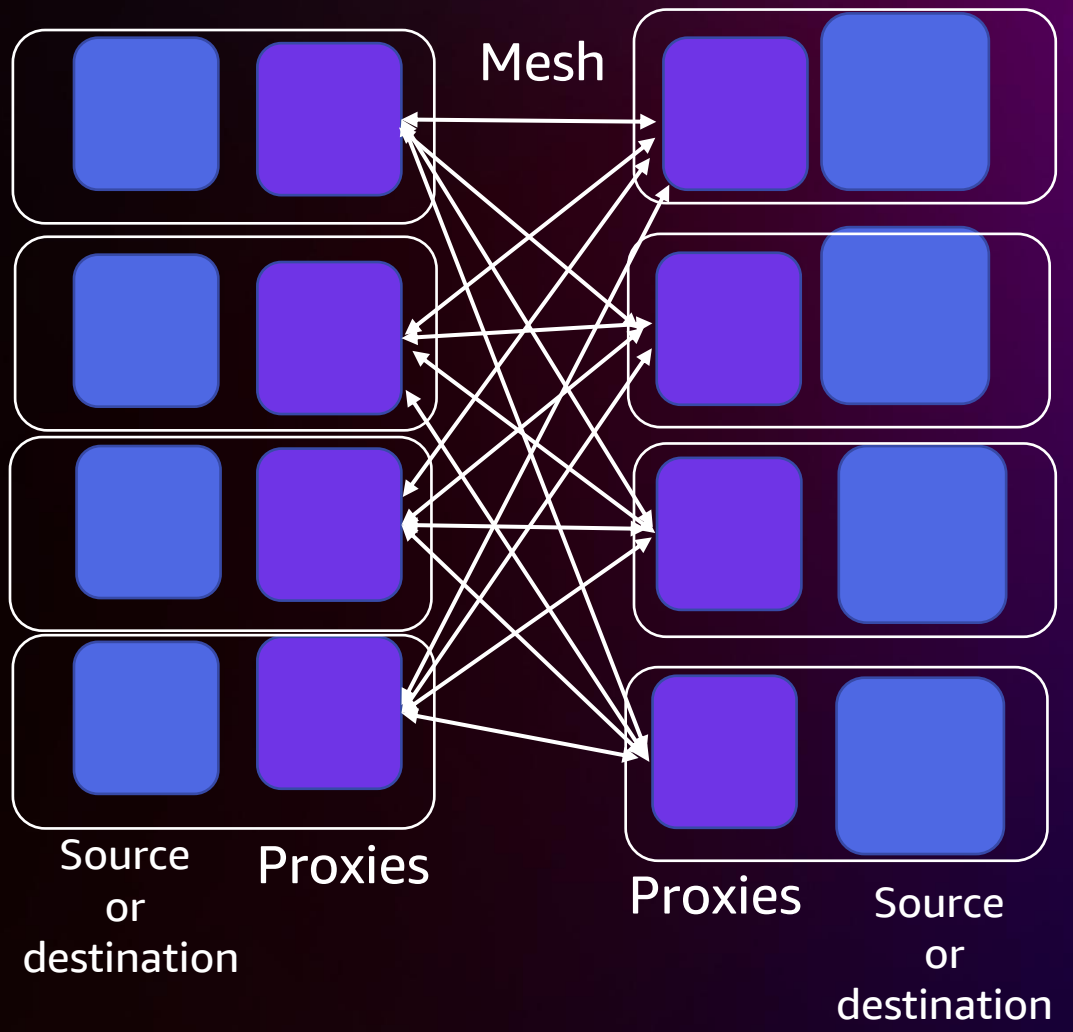
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global Accelerator vs. CloudFront



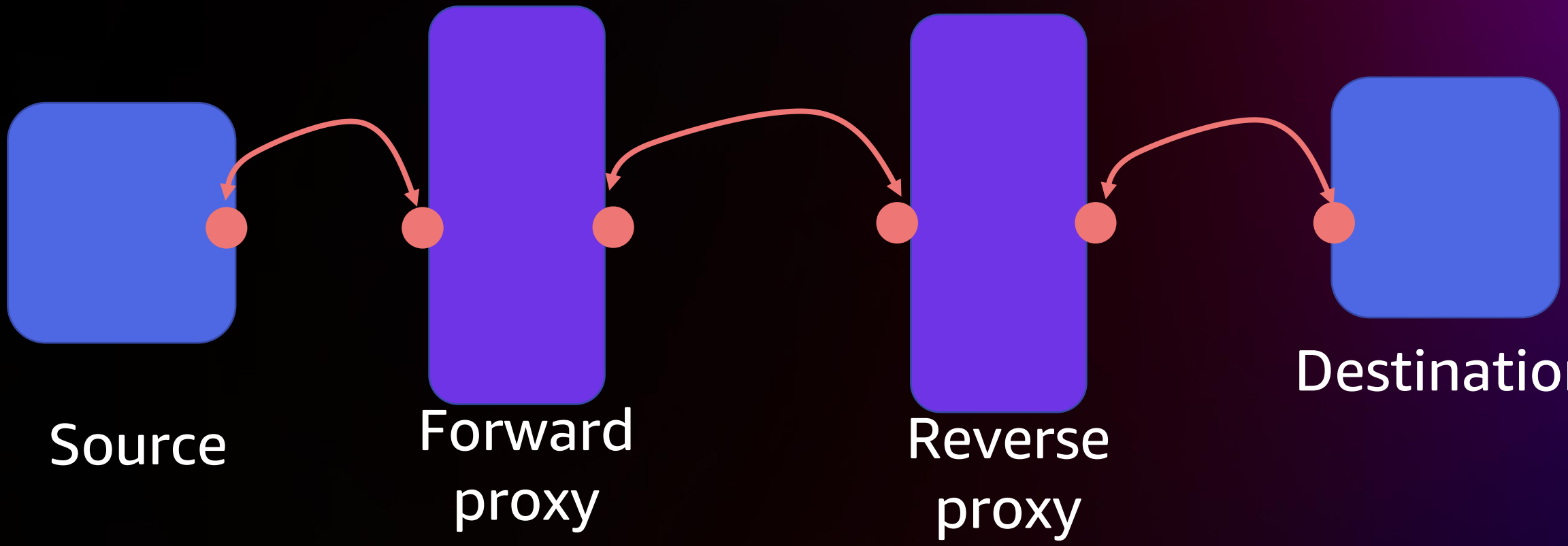
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.





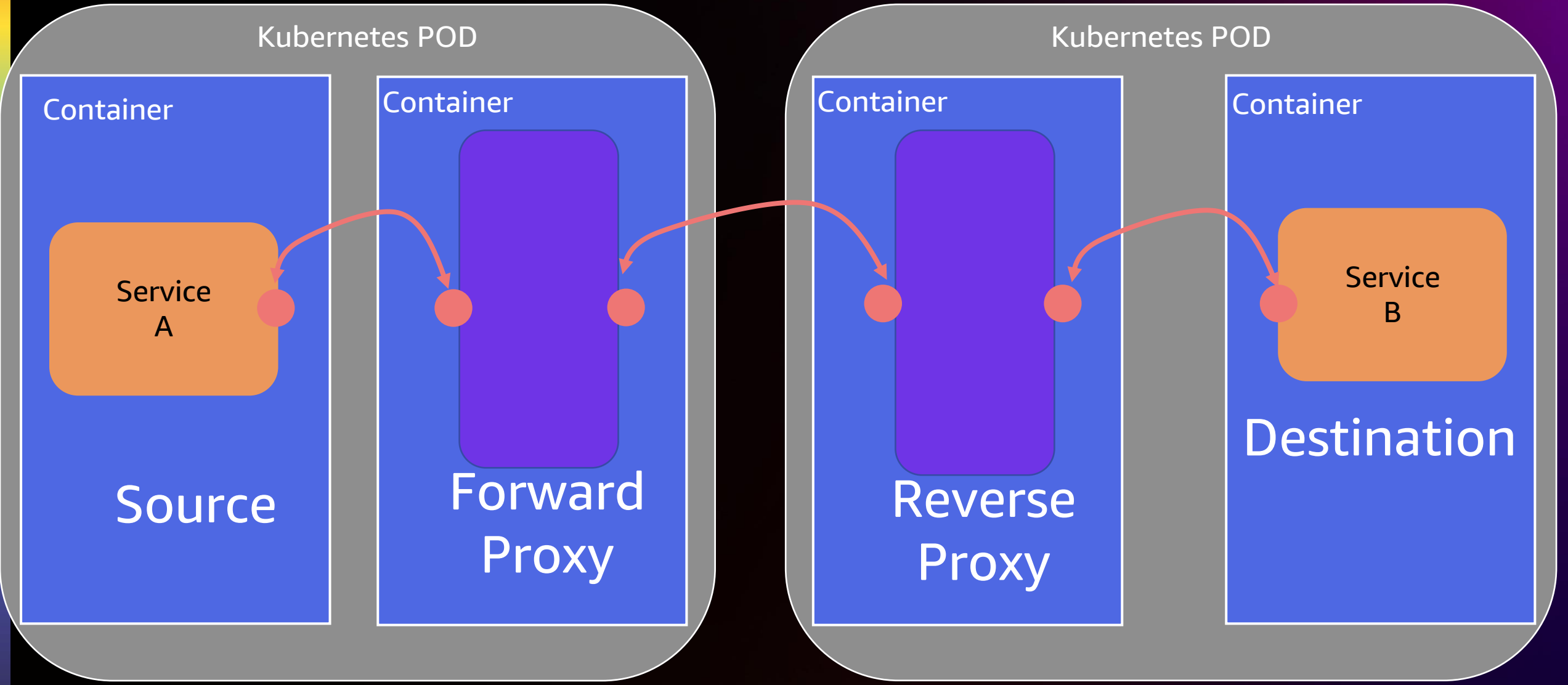
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of a proxy



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

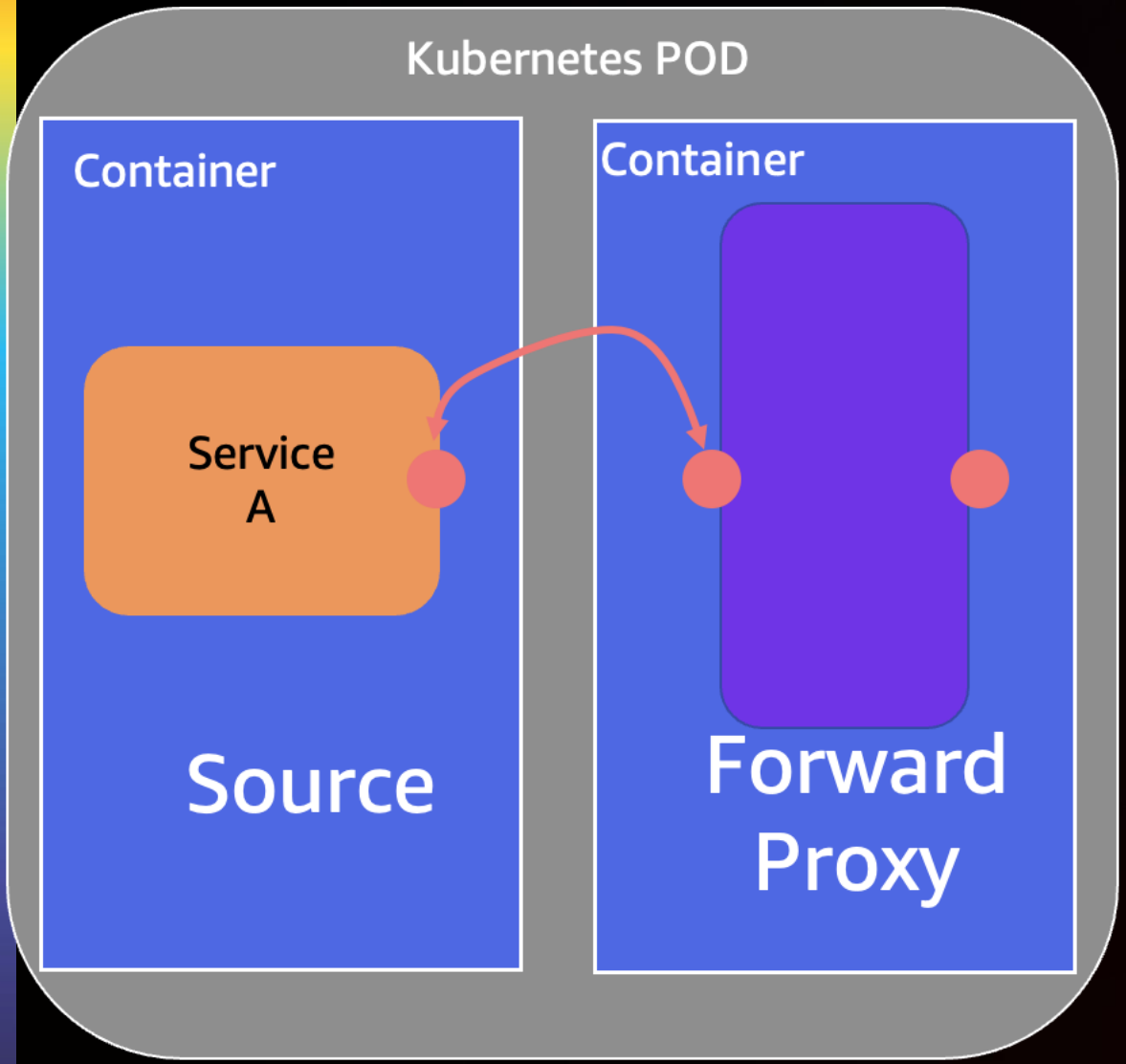
Sidecar proxies

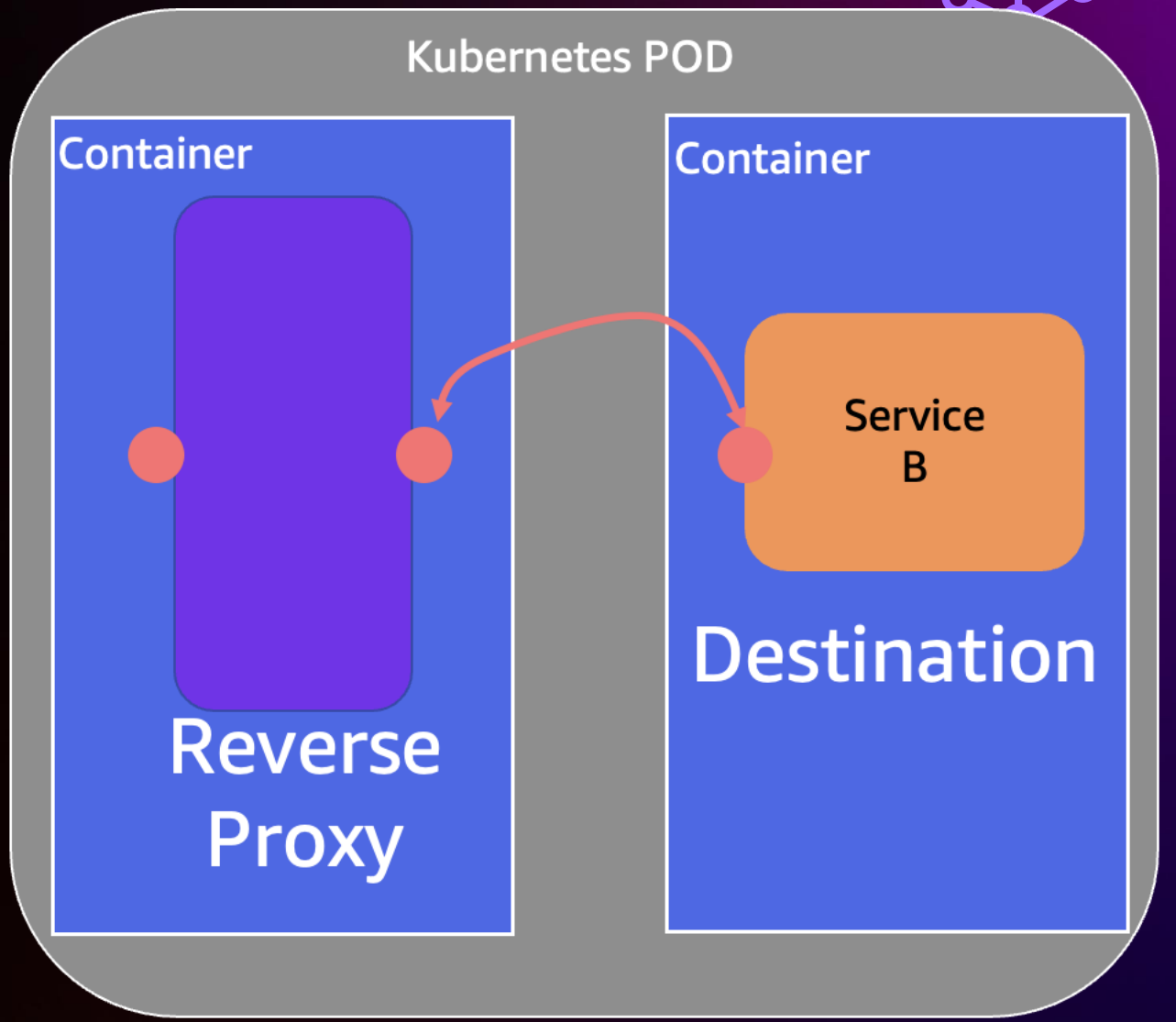


aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Service mesh

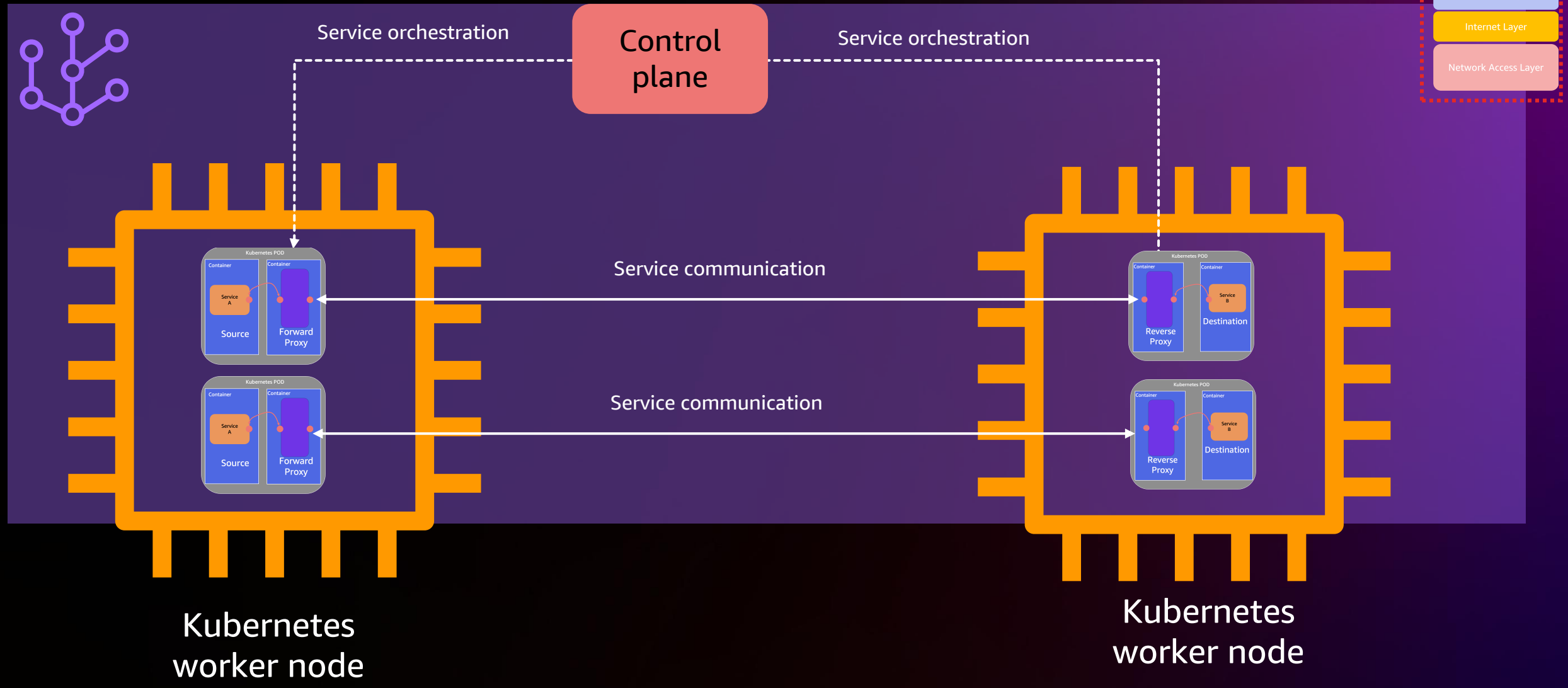






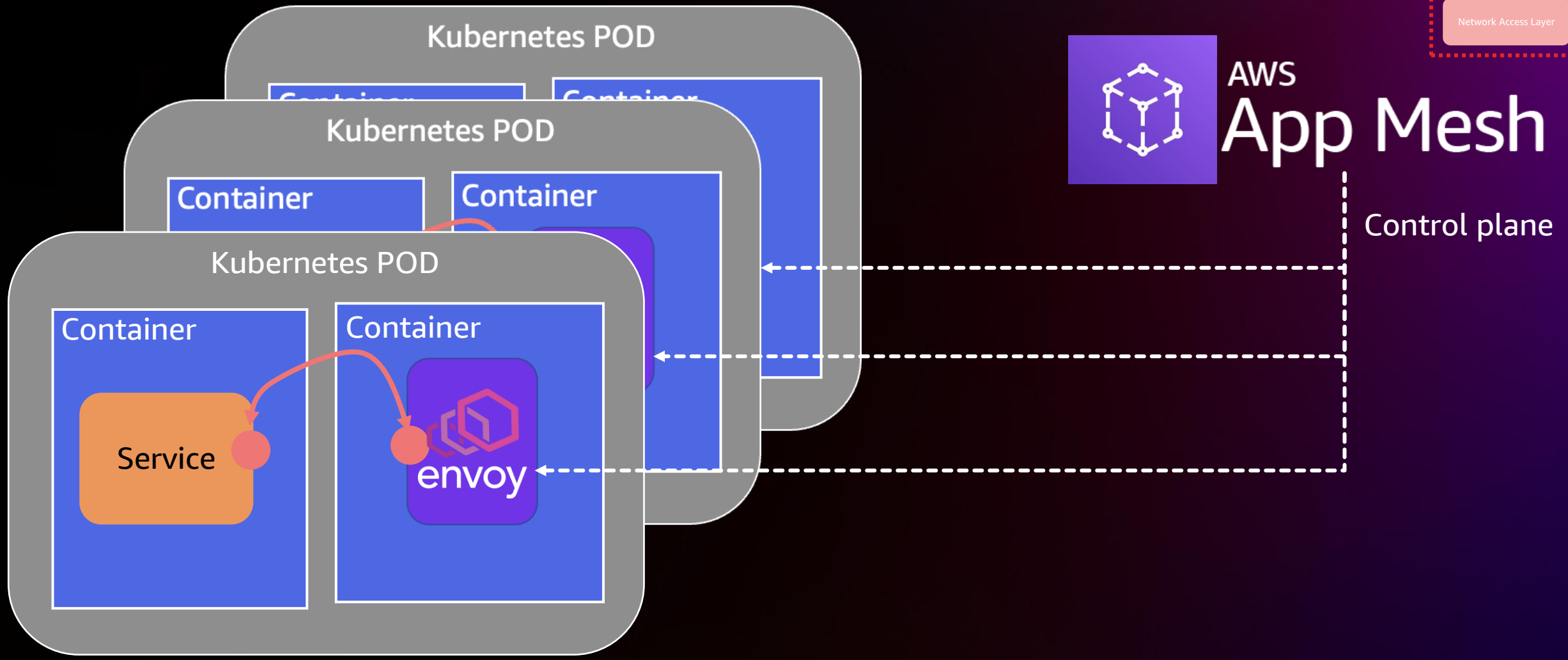
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Service mesh



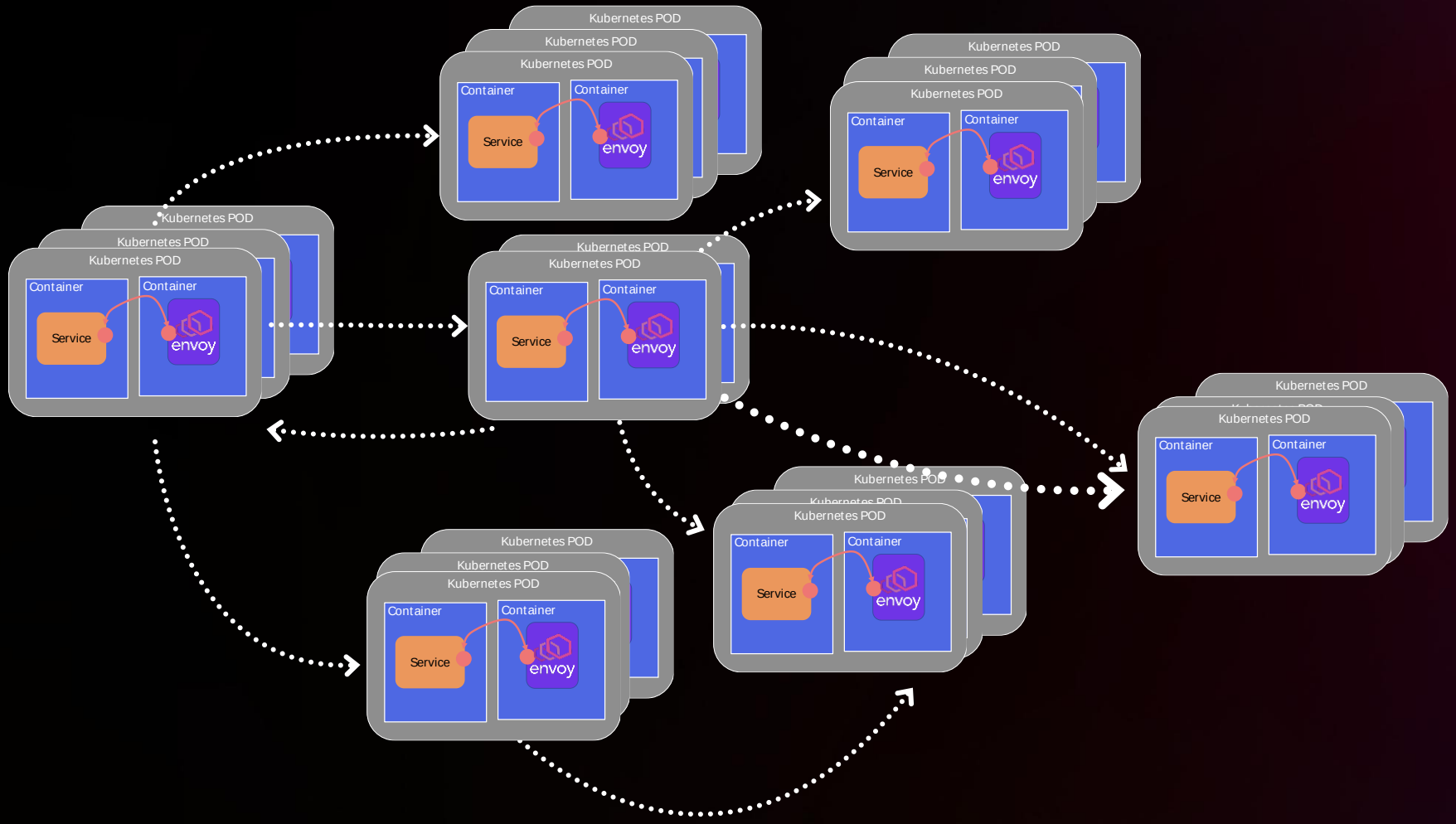
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS App Mesh – Managed service mesh



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

Client-side traffic management



Traffic shaping

Load balancing

Weight targets

Service discovery
(DNS + AWS Cloud Map)

Health checks

Retries

Timeouts

Circuit breakers

Routing controls

Protocols support (HTTP, TCP, gRPC)

Path-based

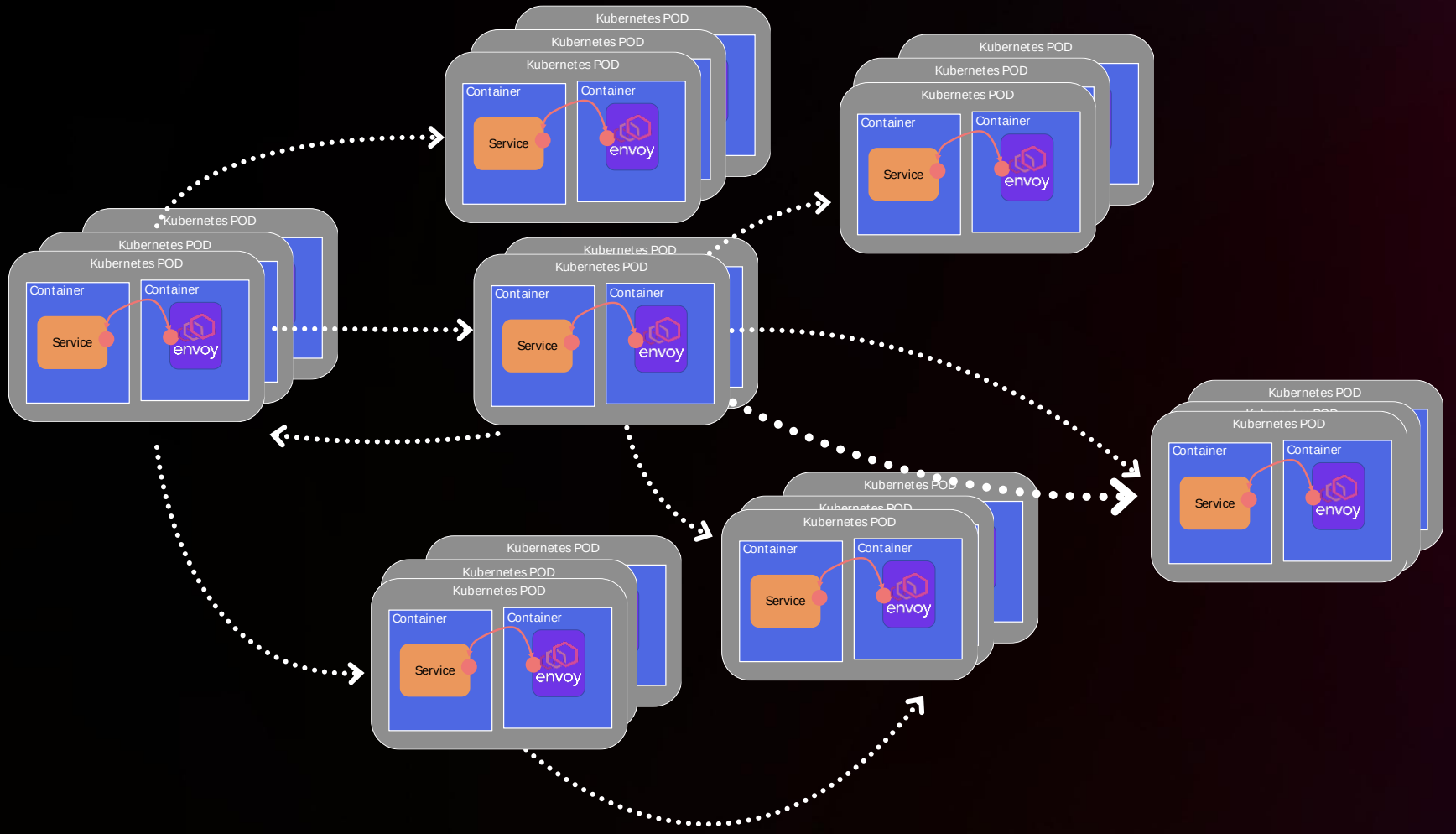
Header-based

Cookie-based

Host-based

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

Application observability



Logging

HTTP access logging

Amazon CloudWatch Logs

Available as container logs on Amazon ECS, Amazon EKS, AWS Fargate

Metrics

CloudWatch metrics

StatsD (with tags)

Prometheus

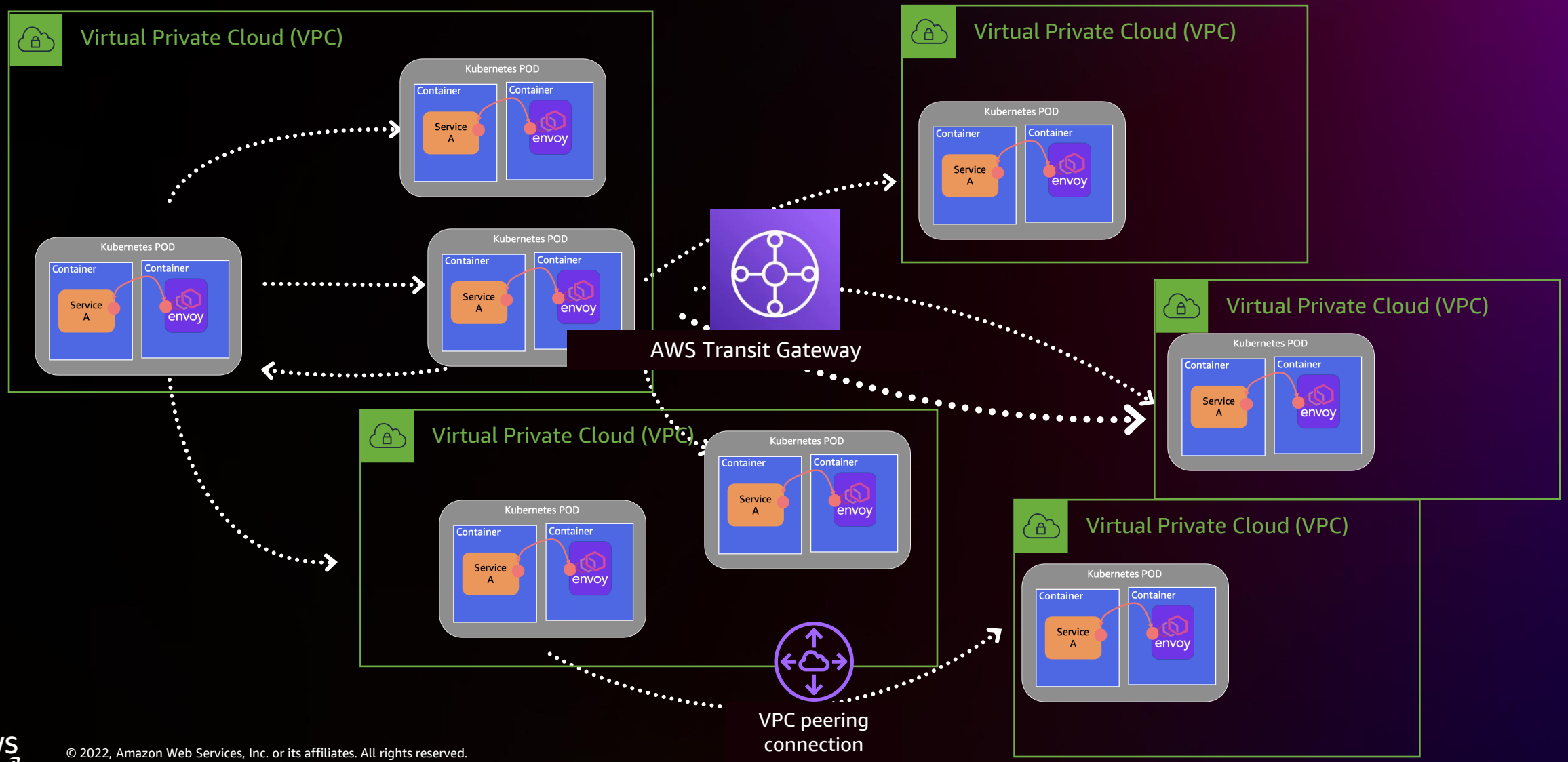
Tracing

AWS X-Ray

Other envoy tracing drivers

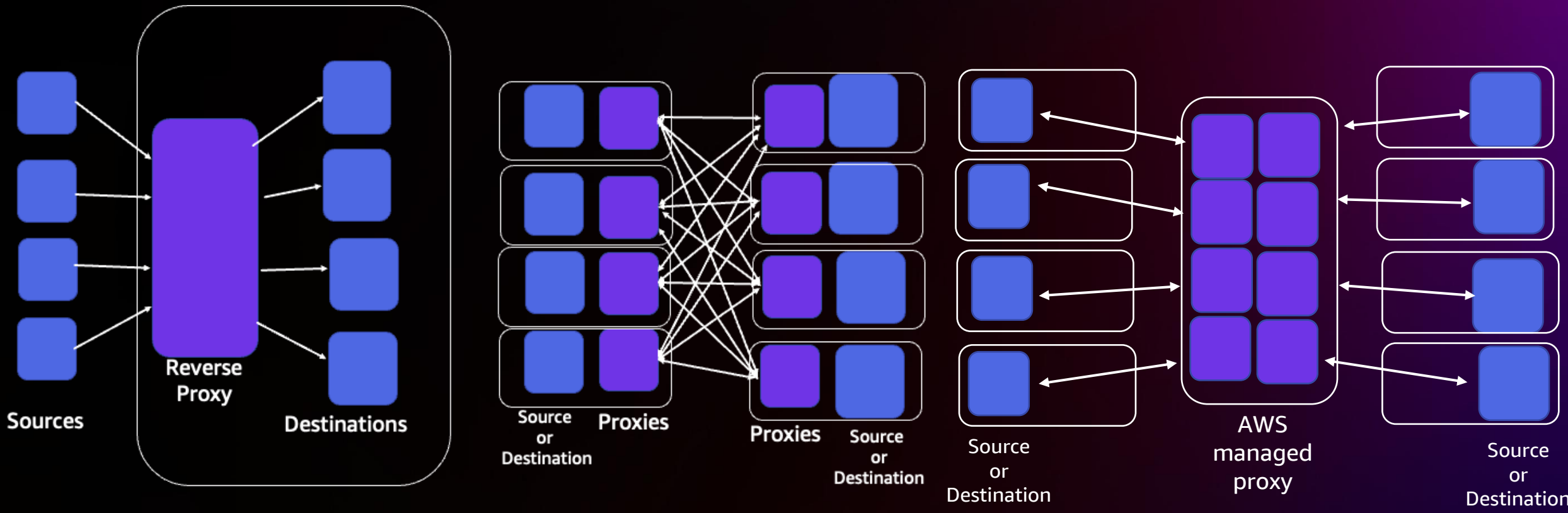
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network



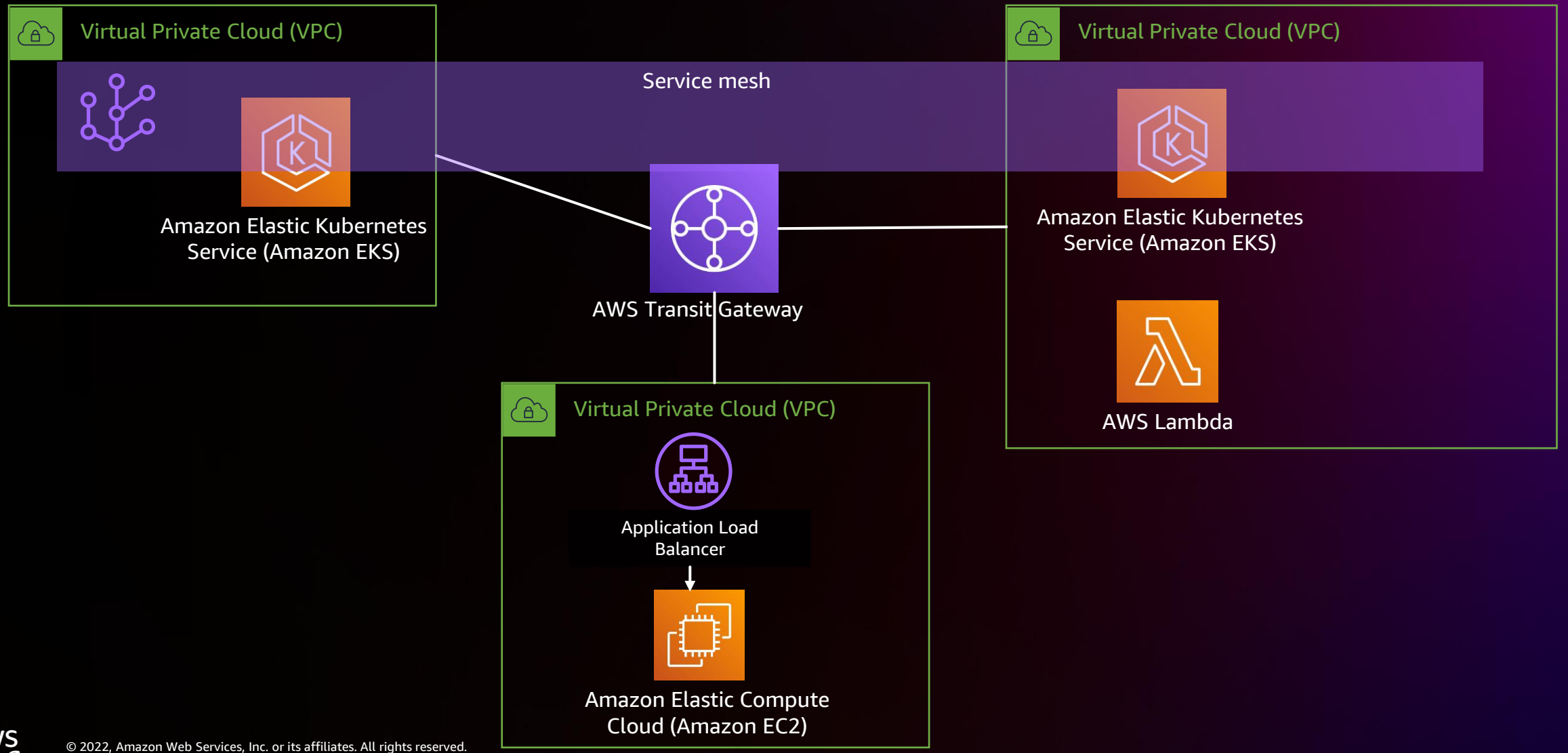
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Going beyond service mesh



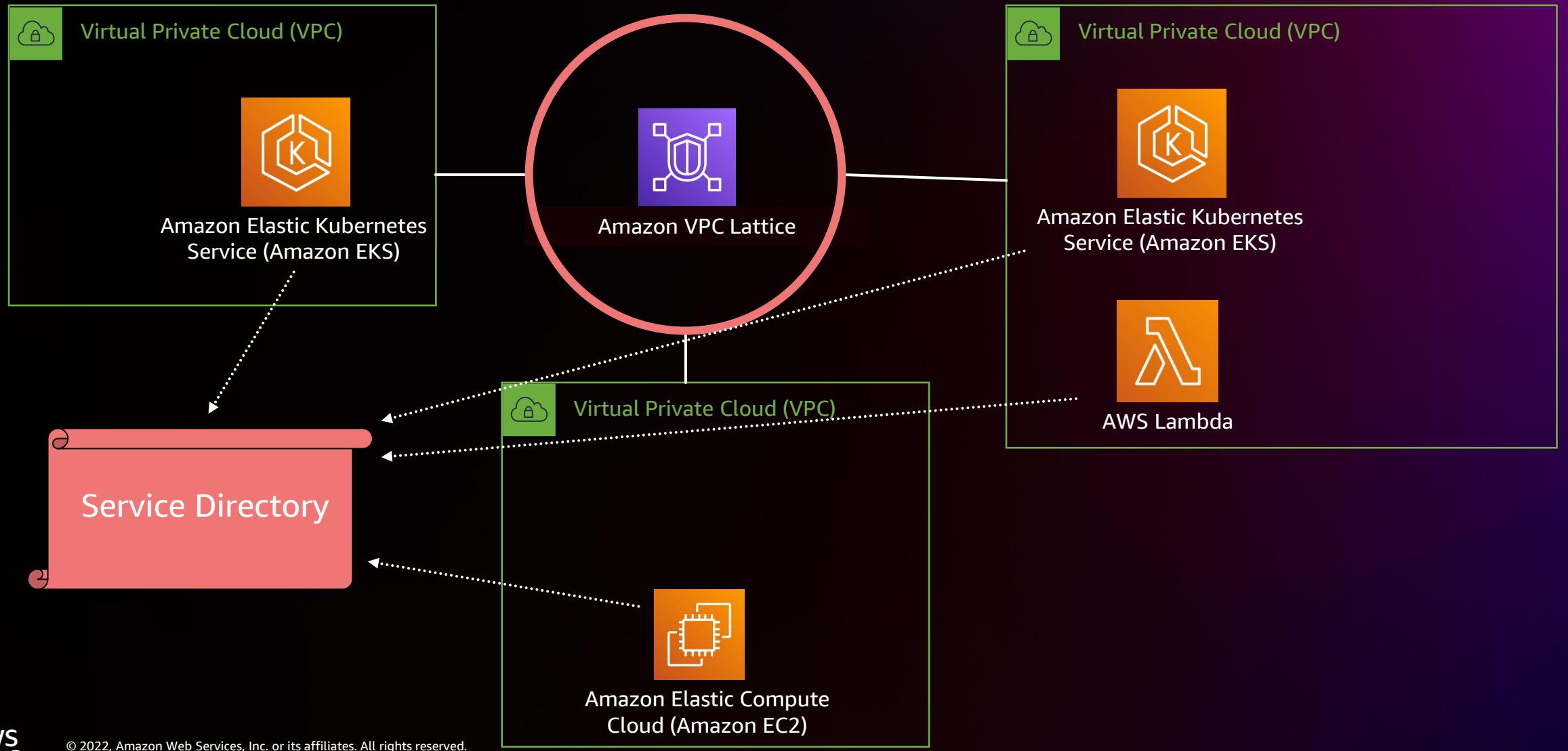
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional deployment



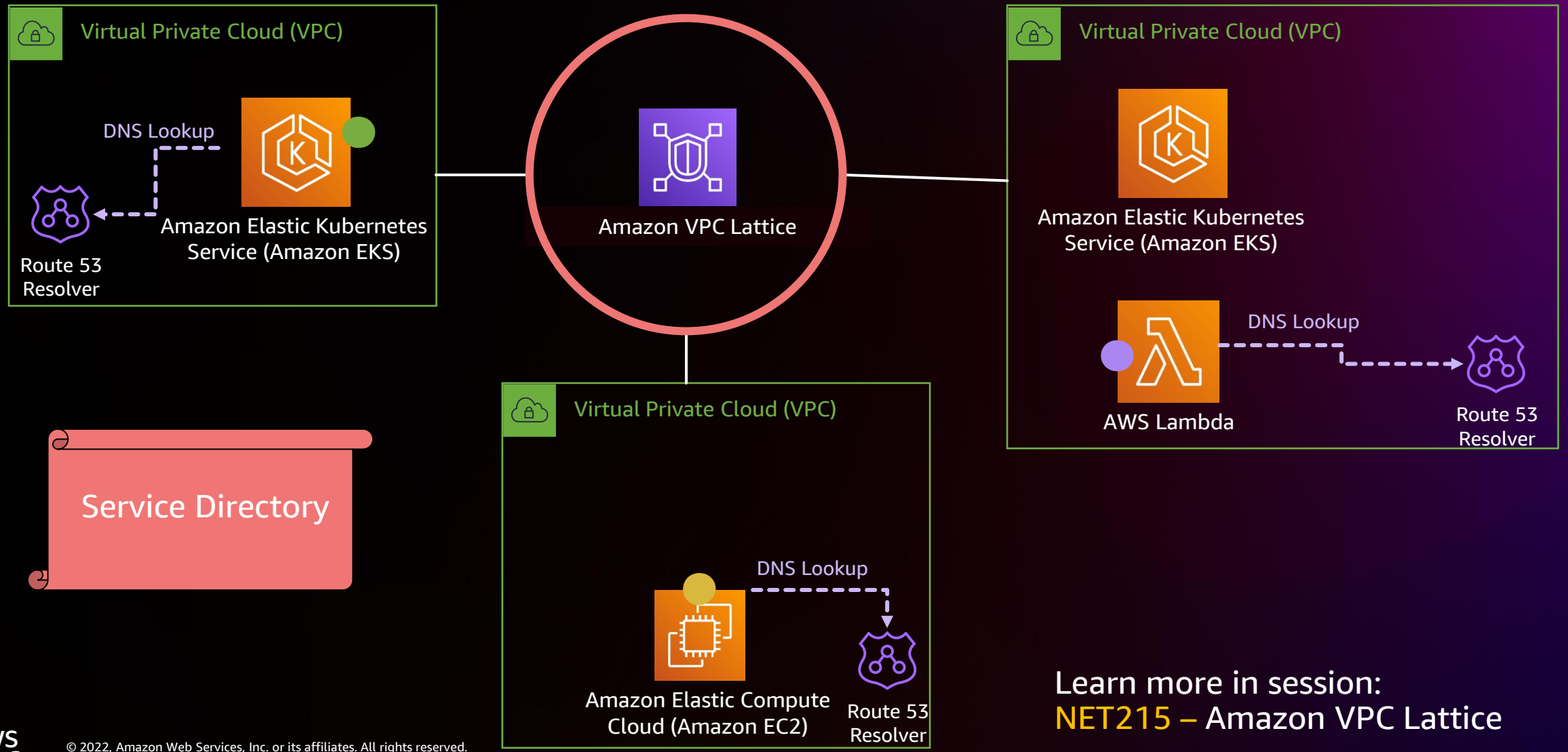
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice – Public preview



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

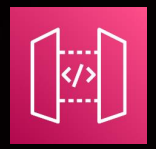
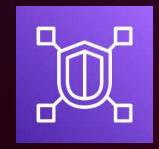
Amazon VPC Lattice – Public preview



Learn more in session:
NET215 – Amazon VPC Lattice

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

API Gateway vs. App Mesh vs. VPC Lattice

	 API Gateway	 App Mesh	 VPC Lattice
Common Use Case	North/South	East/West	East/West
Managed Scope	Data & Control Plane	Control Plane	Data & Control Plane
Supported Services	AWS and customer managed	Customer managed	Customer managed
Lambda support	Yes	No	Yes

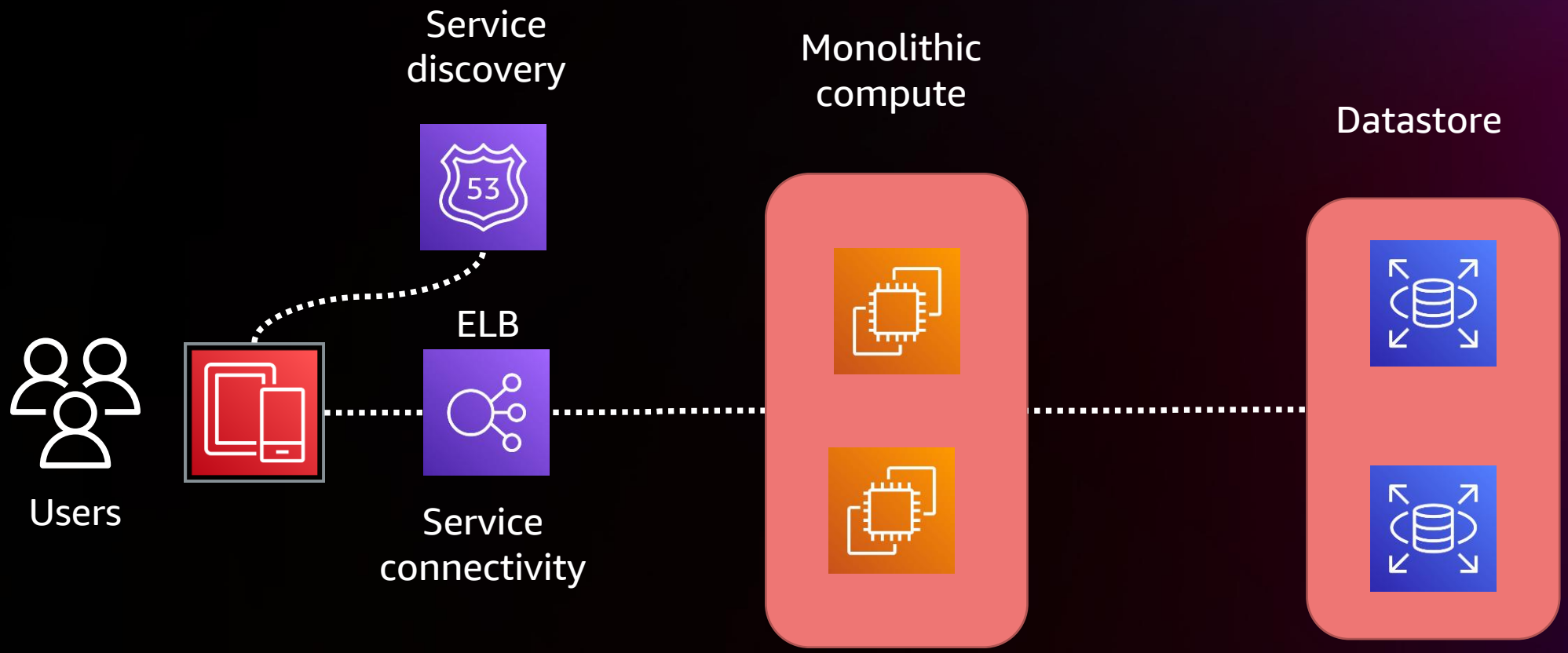
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample Scenario

Putting the building blocks together

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

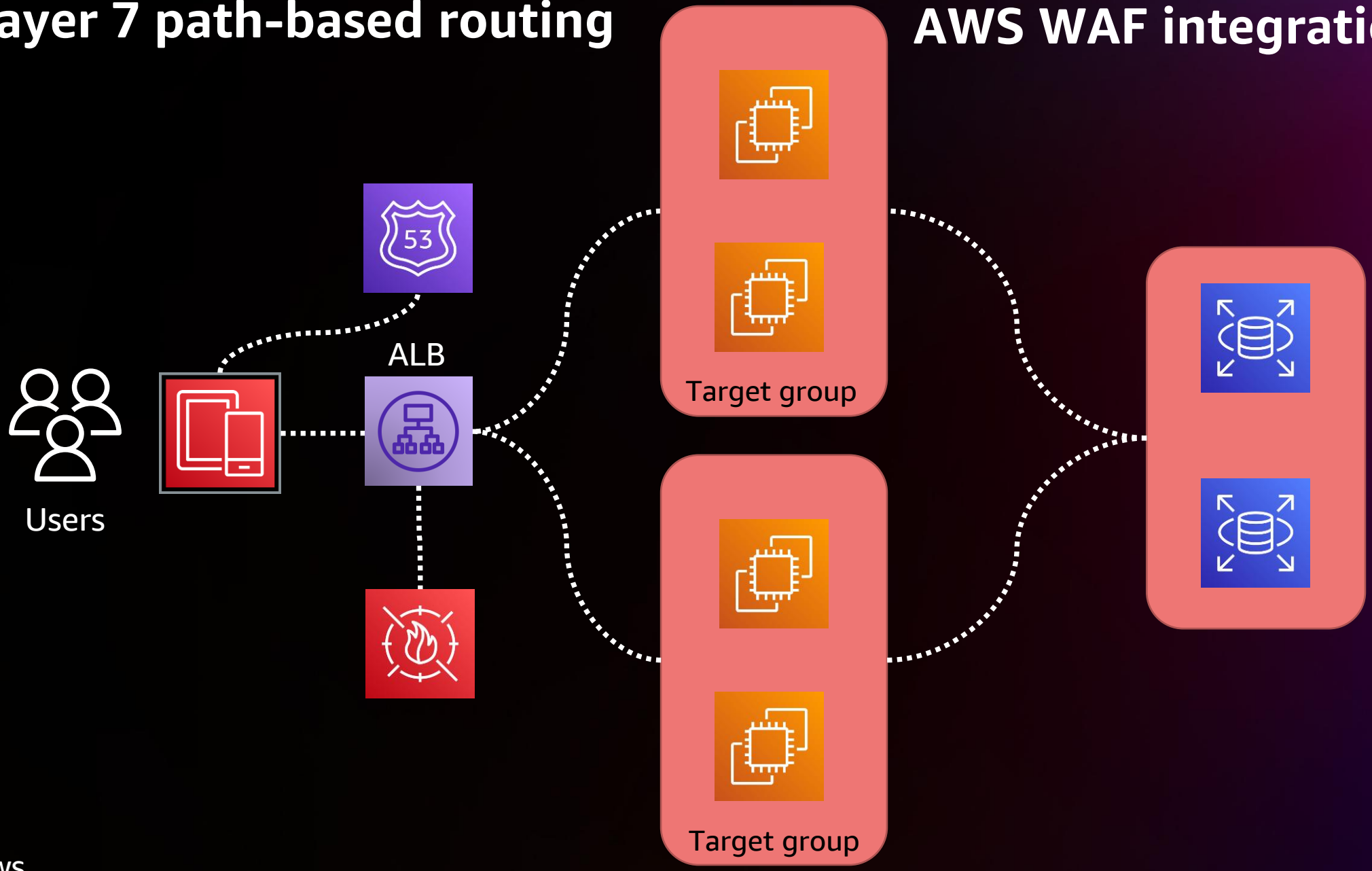
Vertically scaled application



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

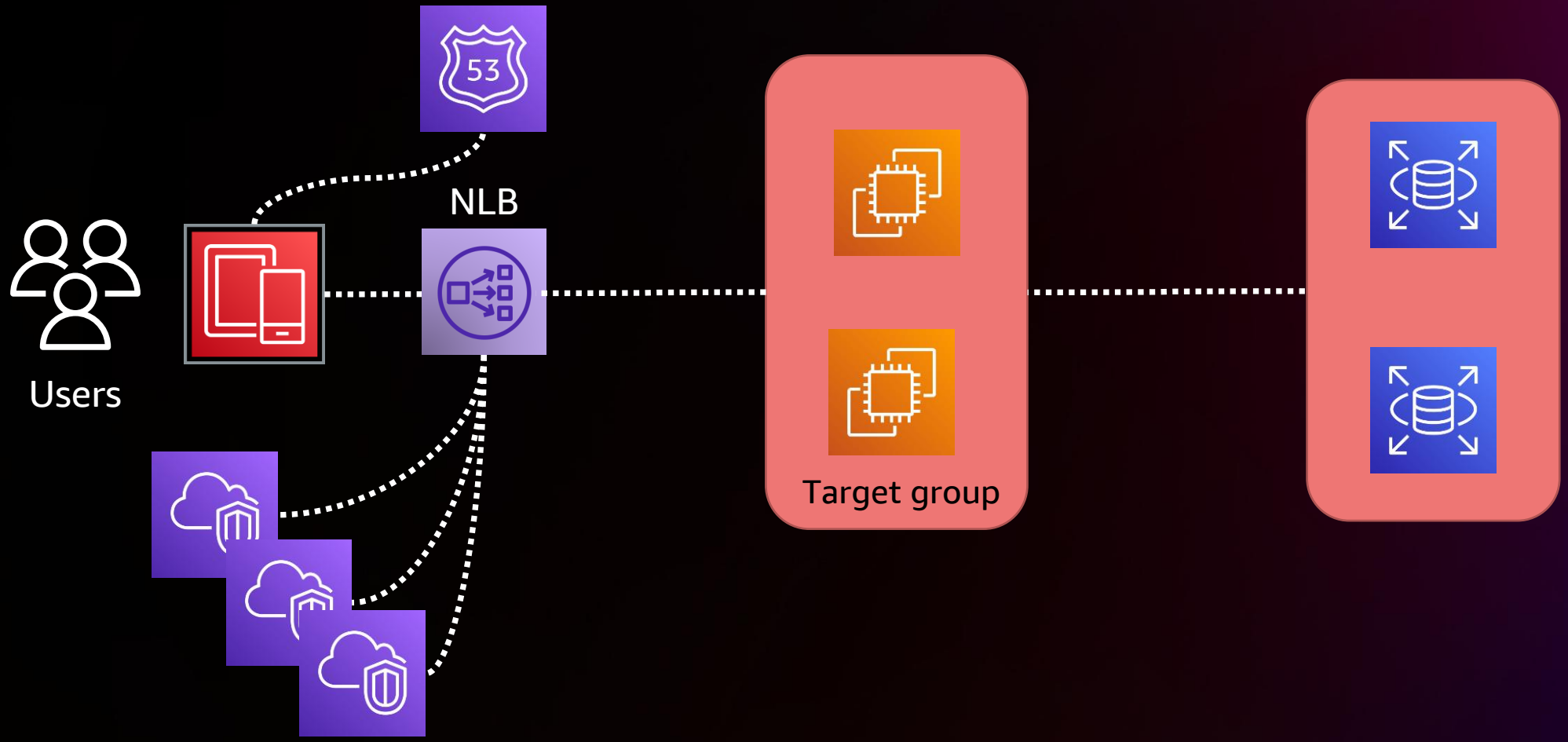
Layer 7 path-based routing

AWS WAF integration



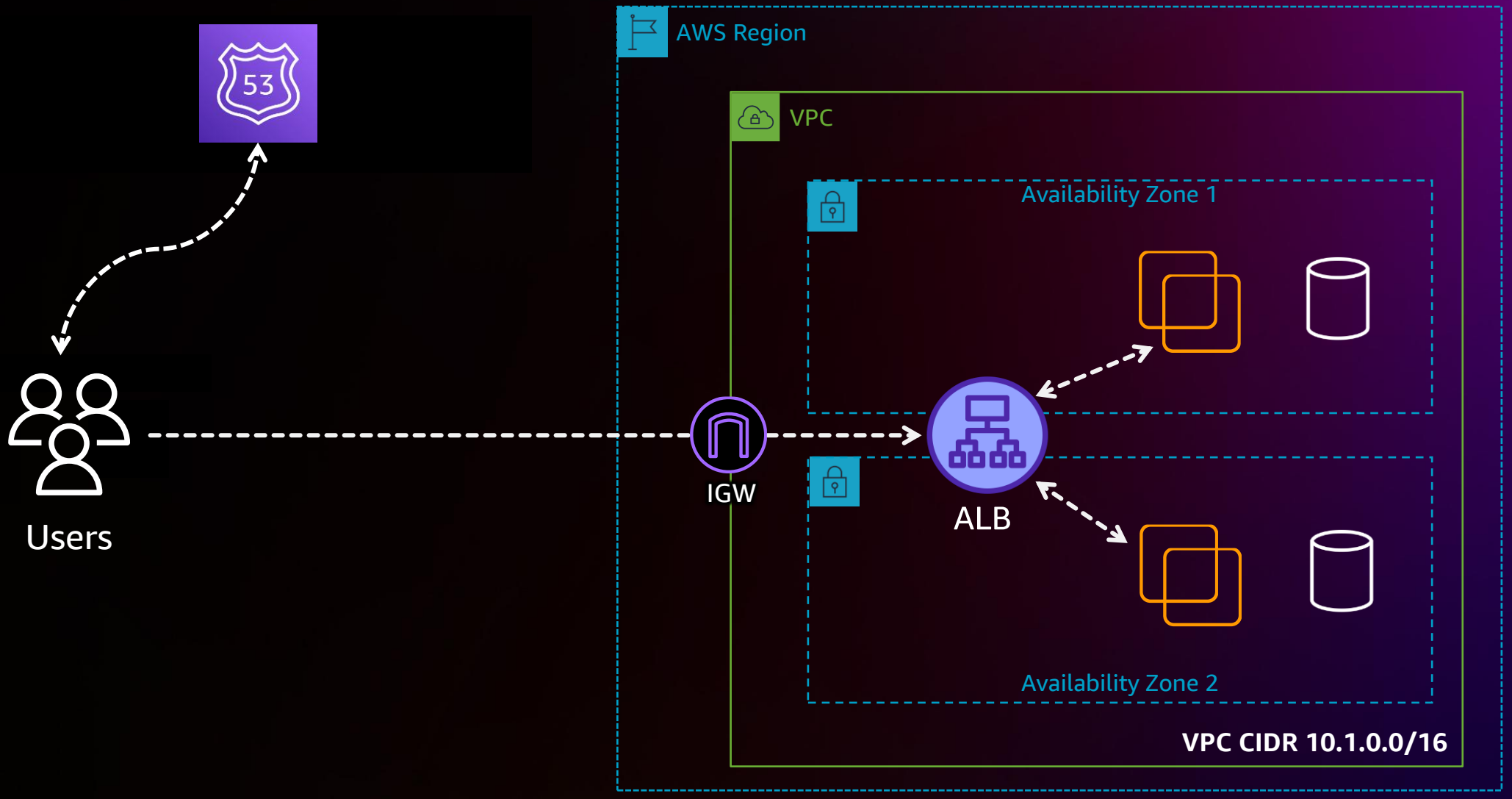
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Layer 4, long-lived flows, fast throughput, PrivateLink



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

Monolithic application in action



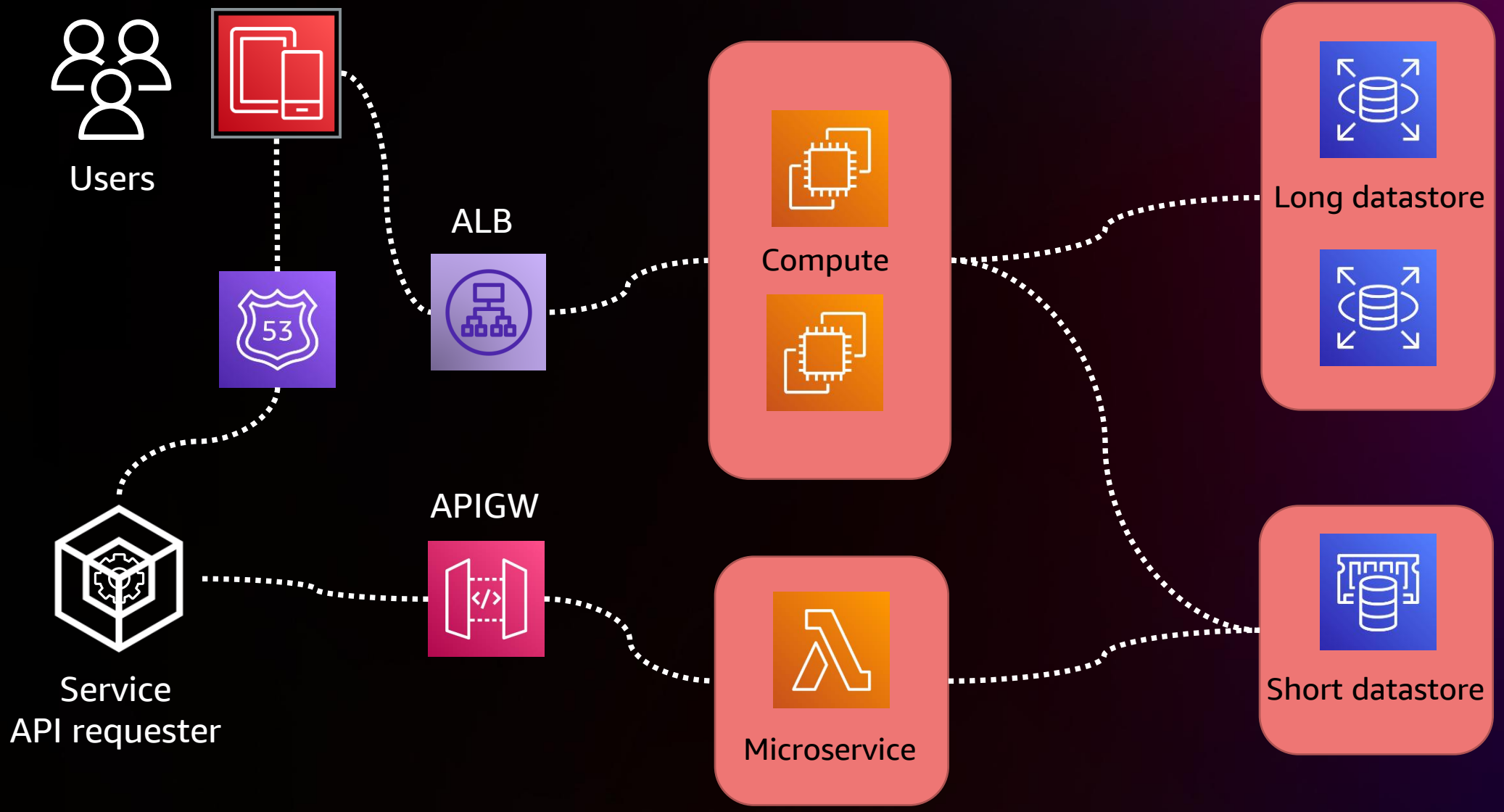
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.





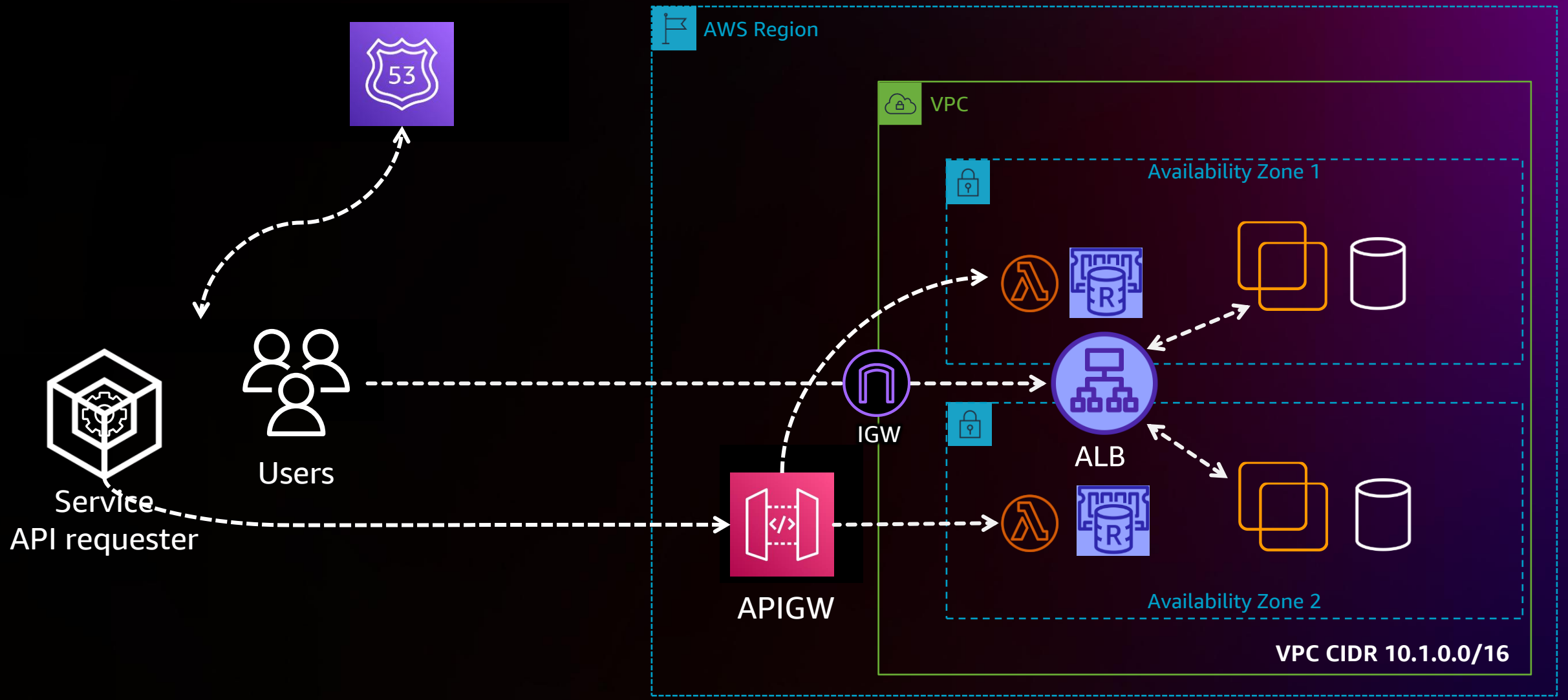
Let’s add an API ingress with data transform requirements, Lambda and some cache

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



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

APIGW and Lambda with cache

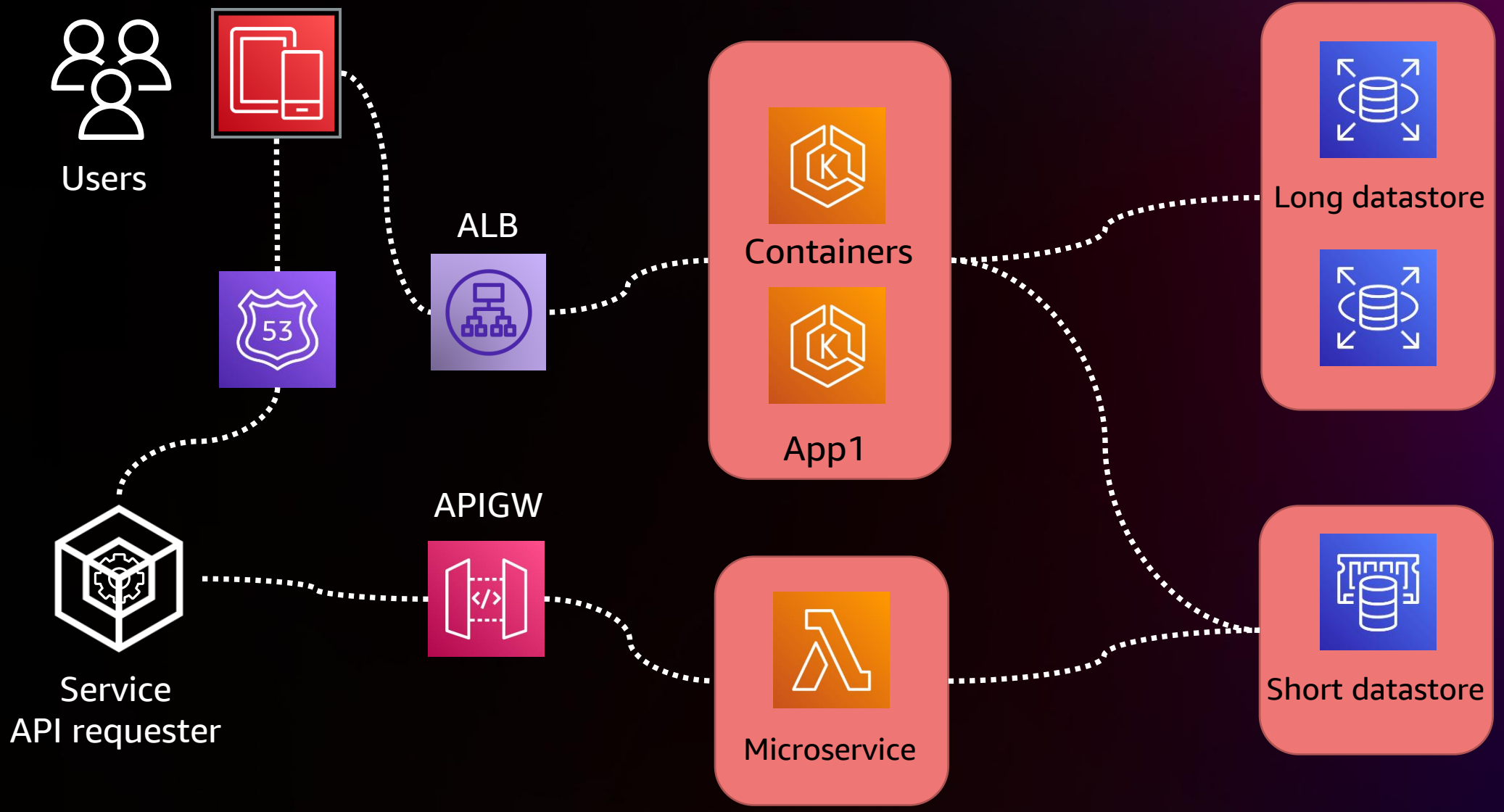


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



We are now containerizing!
Let’s use EKS

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



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

Kubernetes Cloud Controller Service & AWS Load Balancer Controller comparison

AWS cloud provider load balancer controller (native):

- Functionality provided by the AWS cloud controller manager
- Reconciles only Kubernetes Service resources of type LoadBalancer
- Environment and annotations define NLB implementation
- Deploys AWS CLB (default) and NLB in instance mode

AWS Load Balancer Controller (Recommended):

- Reconciles Kubernetes Service Resources of type LoadBalancer and Ingress Resources
- Formerly AWS ALB Ingress Controller
- Deploys NLB in instance and IP mode for service resources
- Deploys ALB in instance & IP mode for ingress resources
- Needs to be installed

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

A note about AWS Load Balancer Controller and Amazon EKS

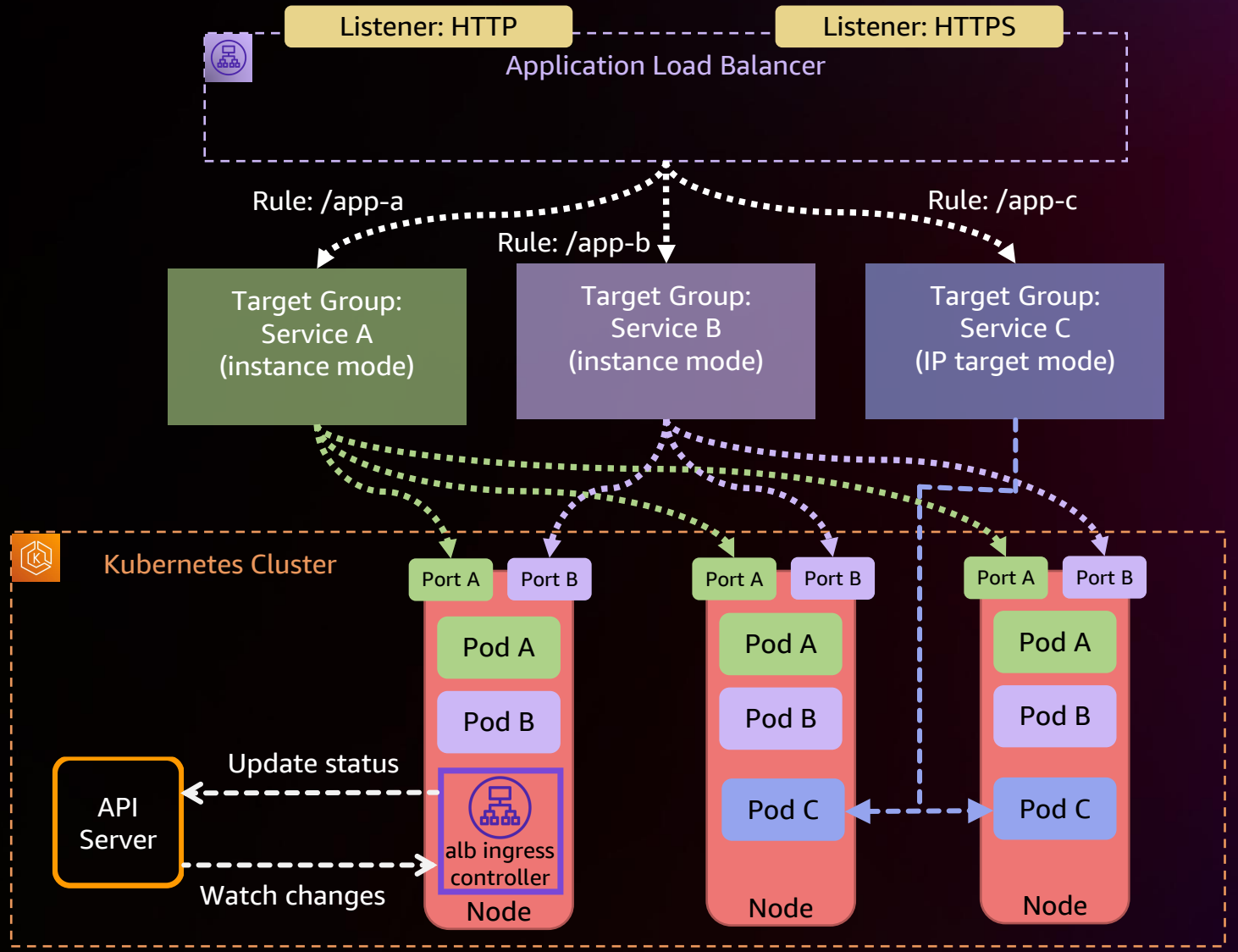
Share ALB with multiple Kubernetes ingress rules:

Share ALB for multiple services and namespaces

Duplicate configurations

Lower costs

Easily provision ALB/NLB from a Kubernetes ingress resource



IP targeting mode:

Can target specific pods that belong to each service are added as targets

Distribute traffic directly to pods

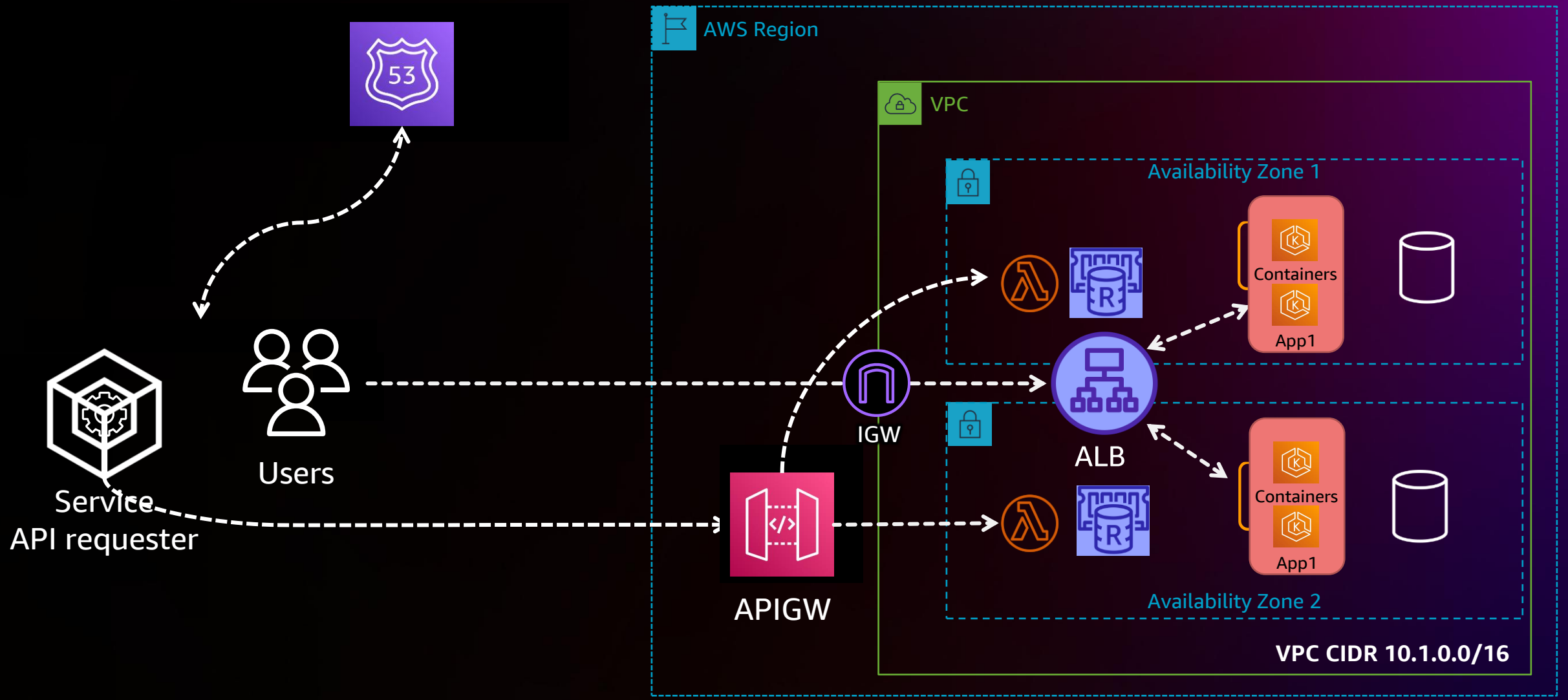
Decreases latency and increases scalability

For more details

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

Add some Amazon EKS pods

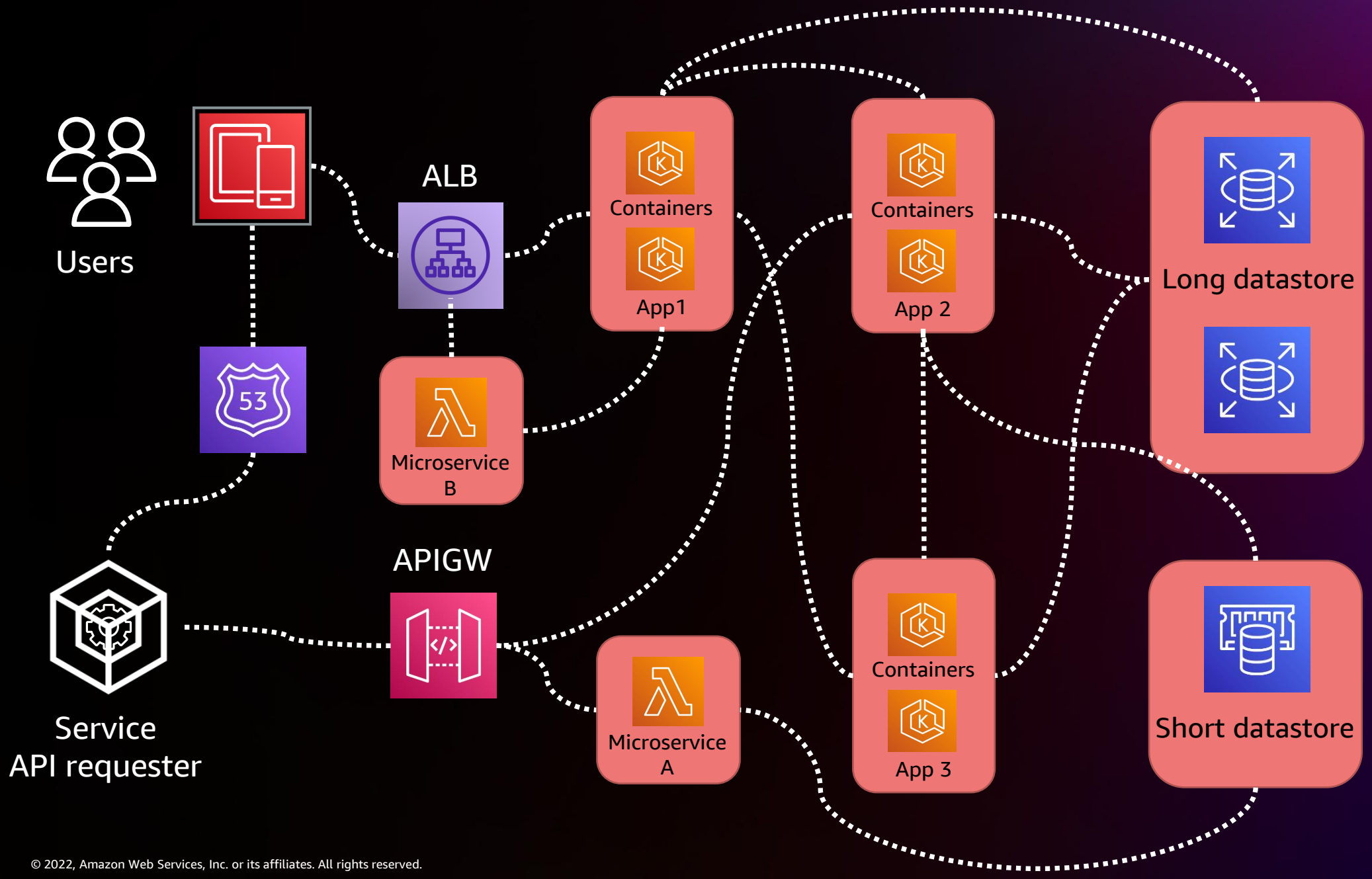
Change to the pods



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

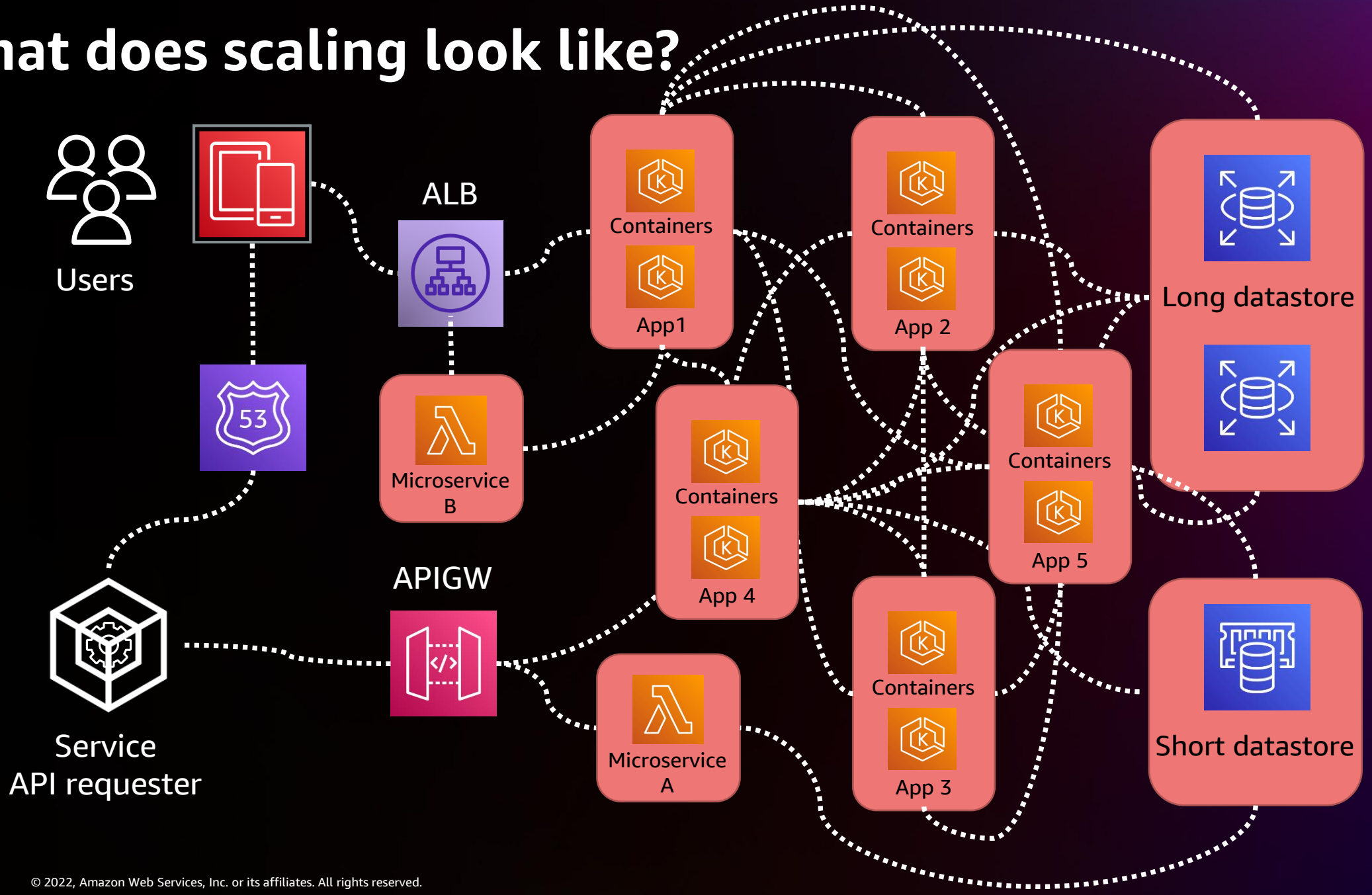
We are now breaking up our services, building modular applications

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



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

What does scaling look like?



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

This looks like . . .

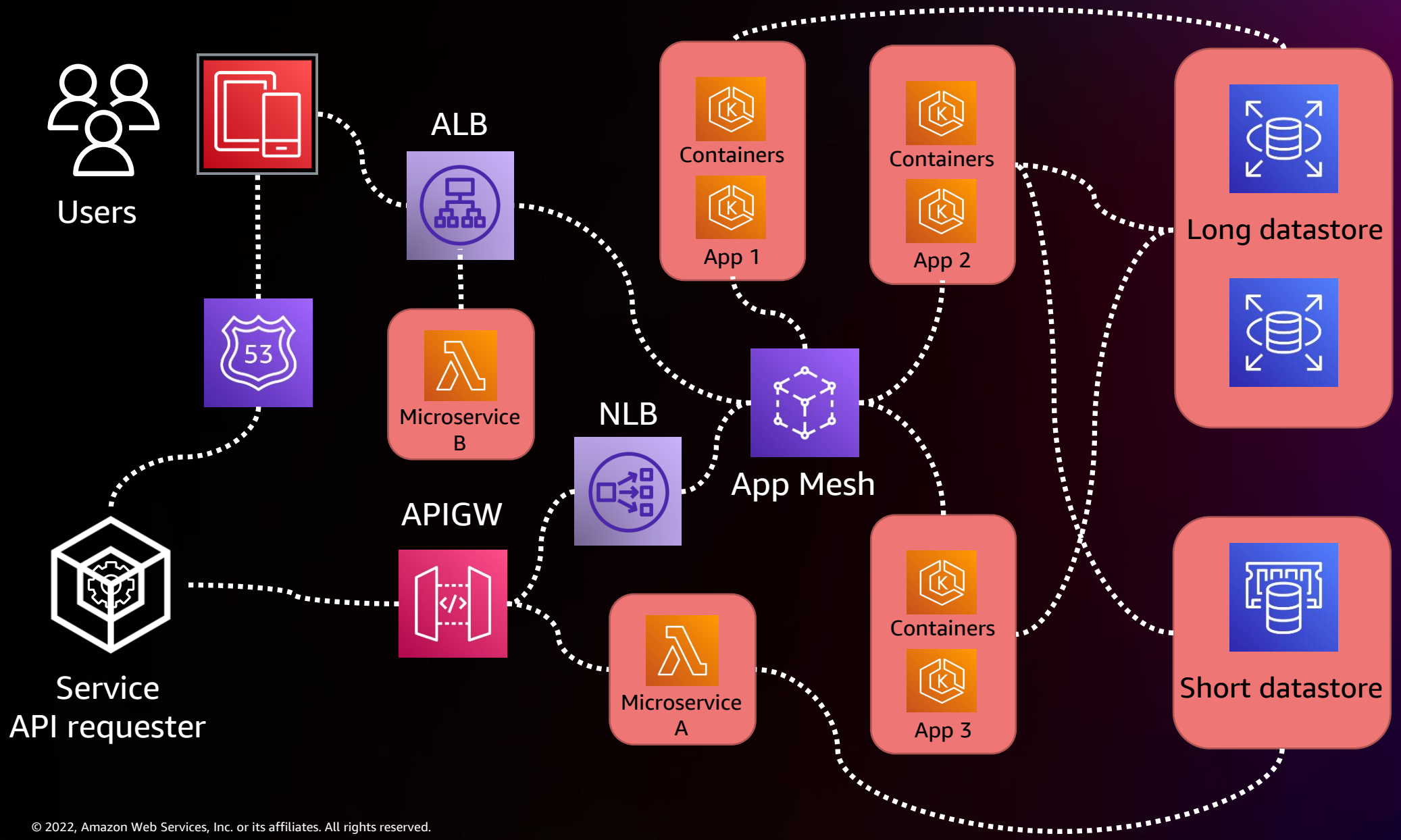
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



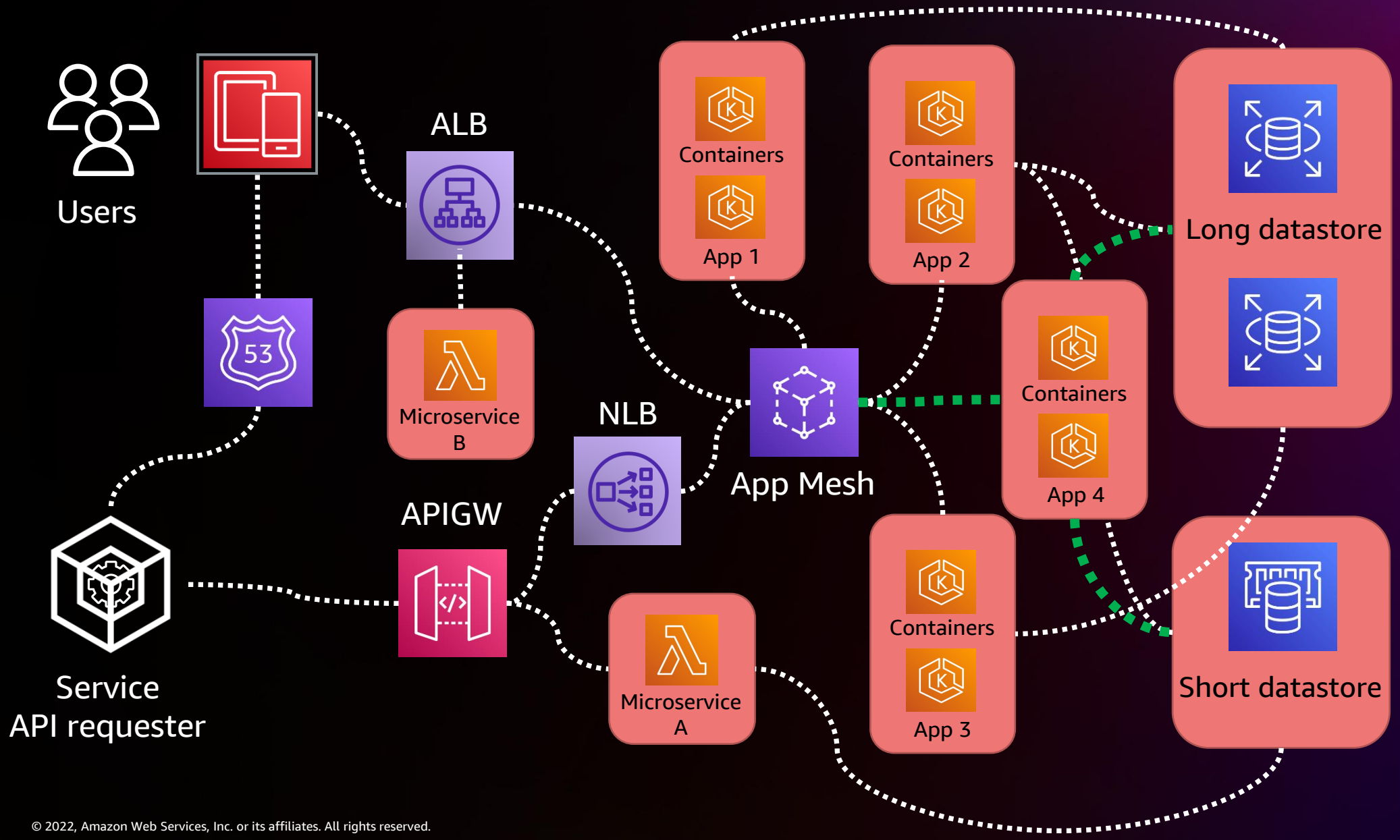


Let’s clean this up a little and add App Mesh so we can scale

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



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

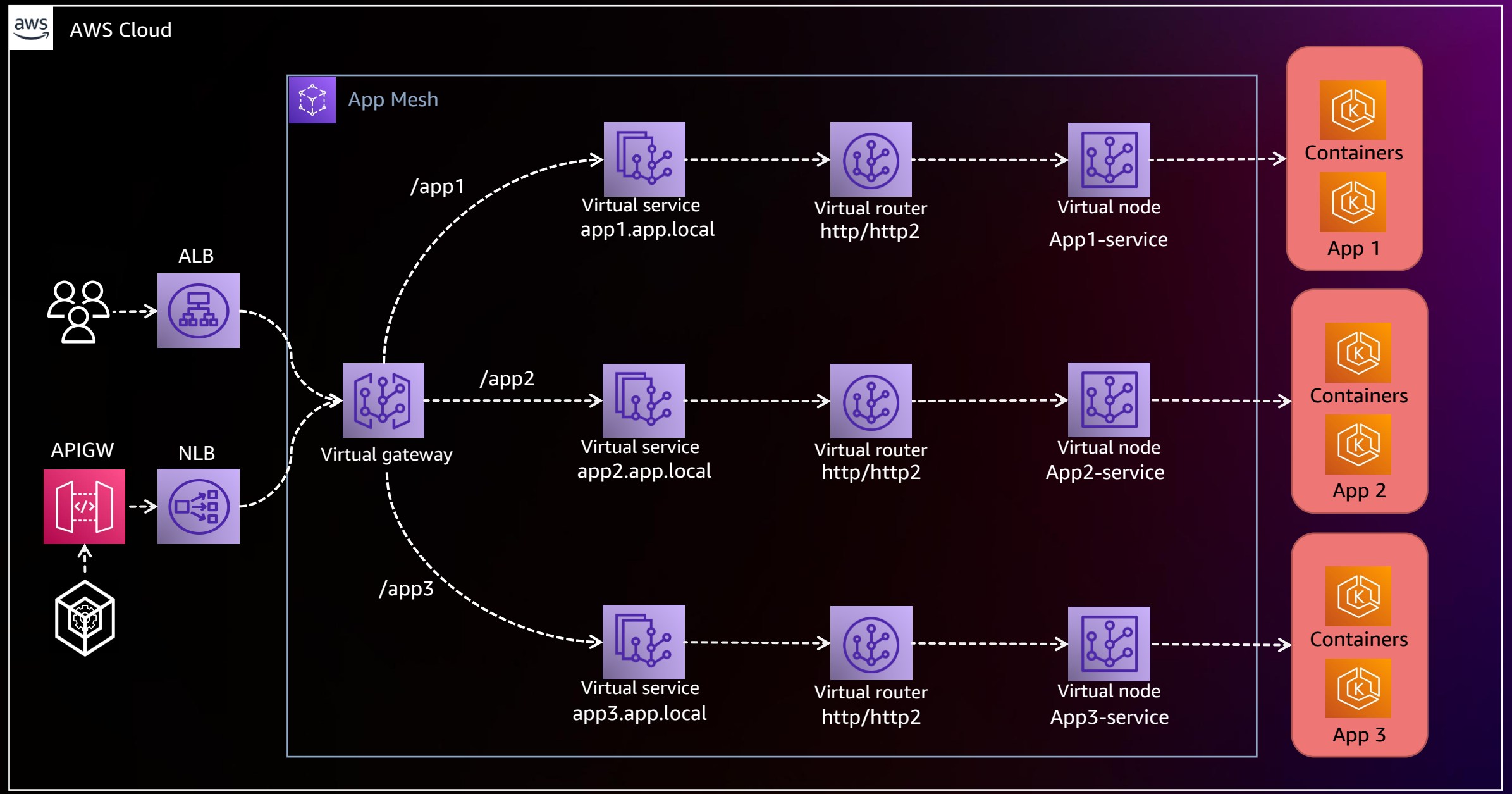


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Let’s dig into App Mesh!

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

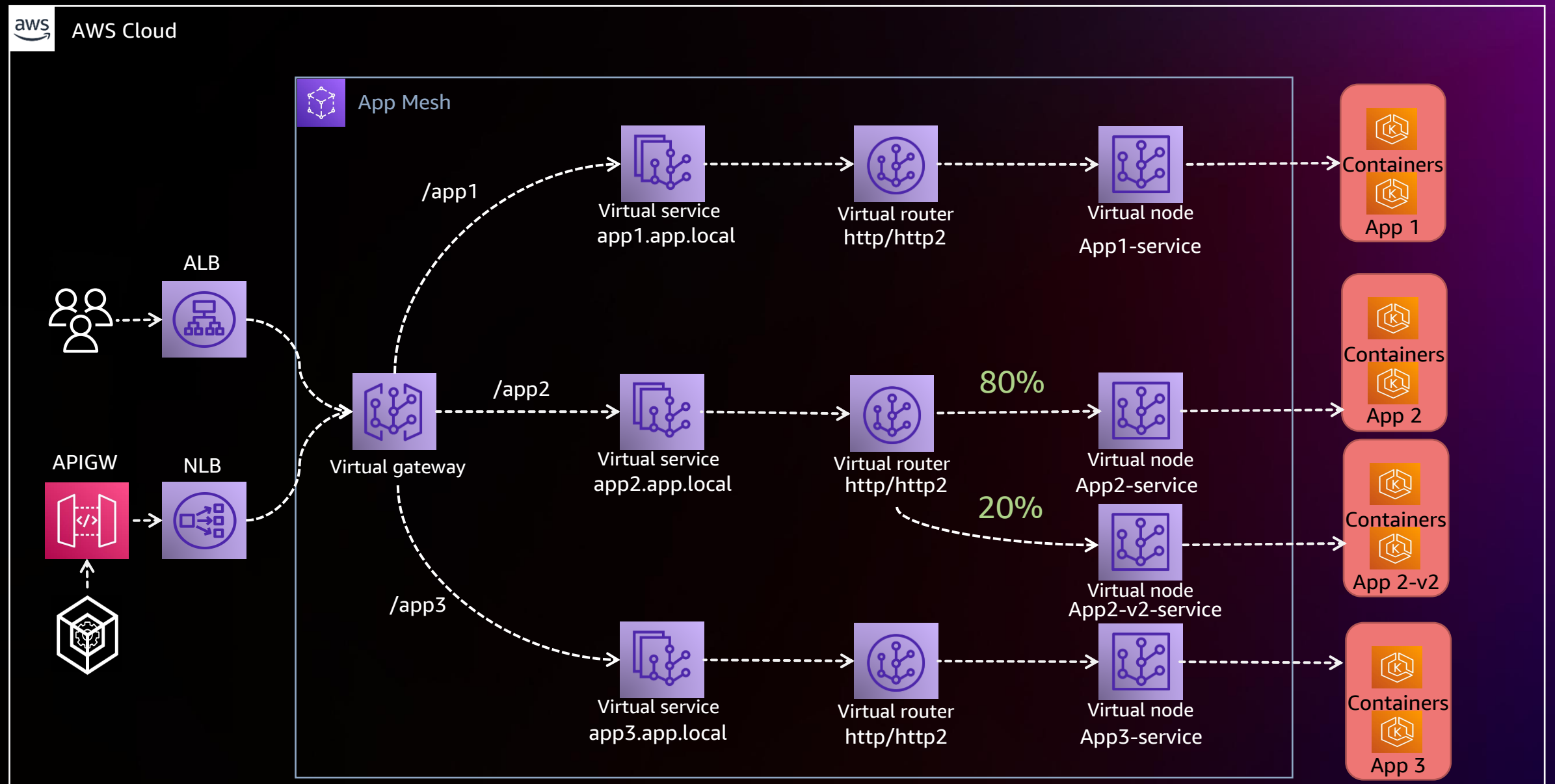


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



What about different versions or blue/green?

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



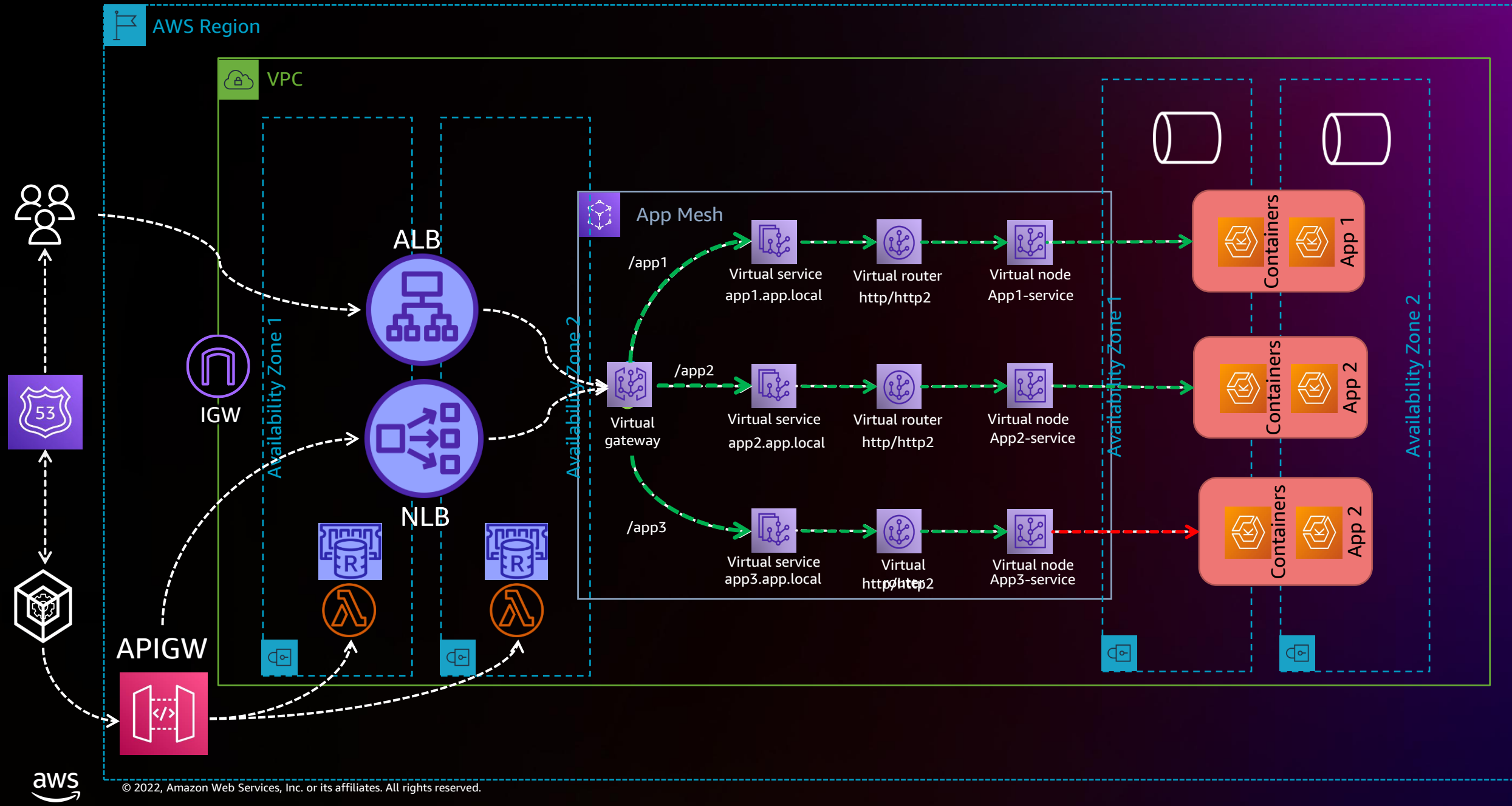
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



How is tracing useful?

aws

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



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

Halfway there!







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

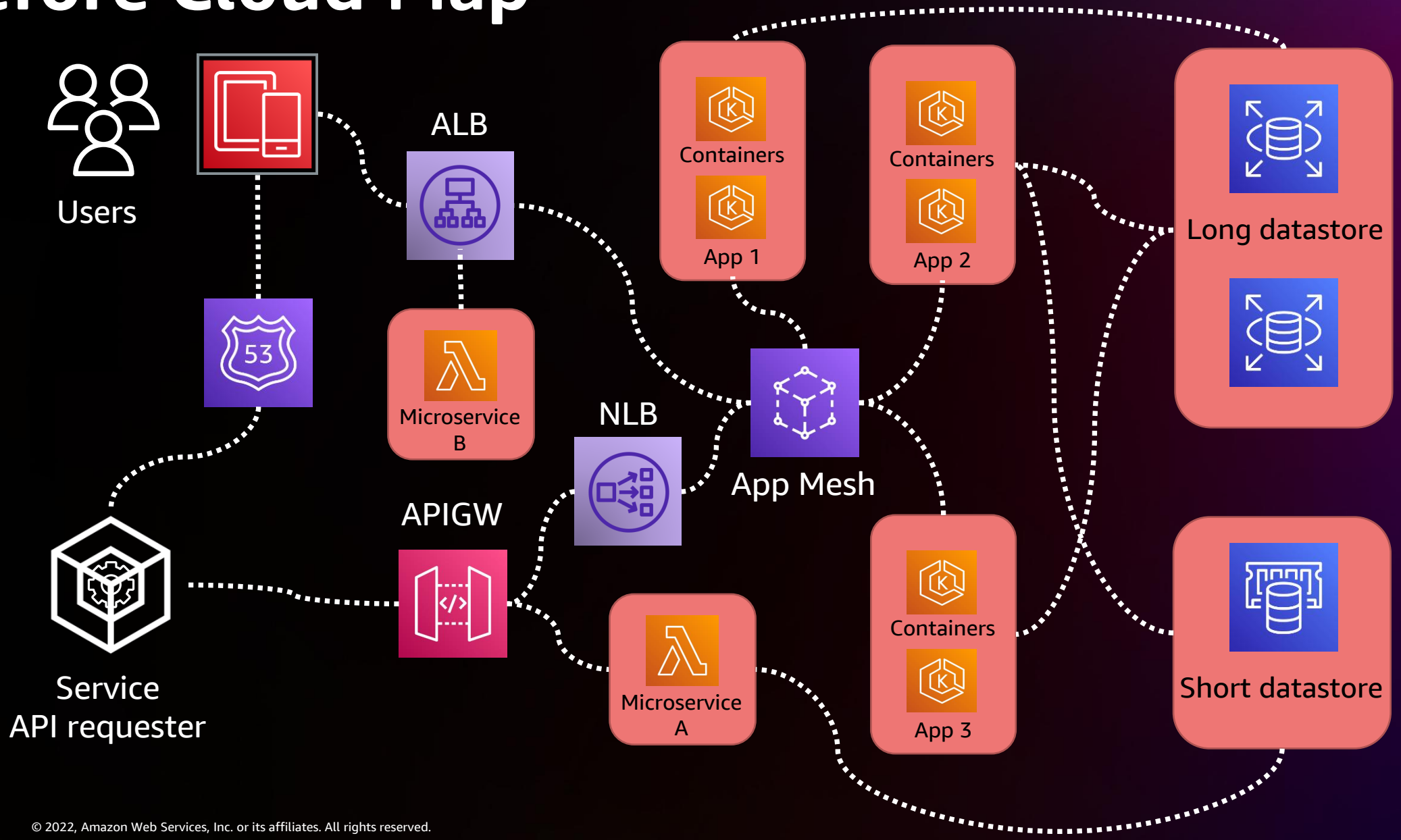


Let’s continue our optimization and talk to our storage with the help of Cloud Map

aws

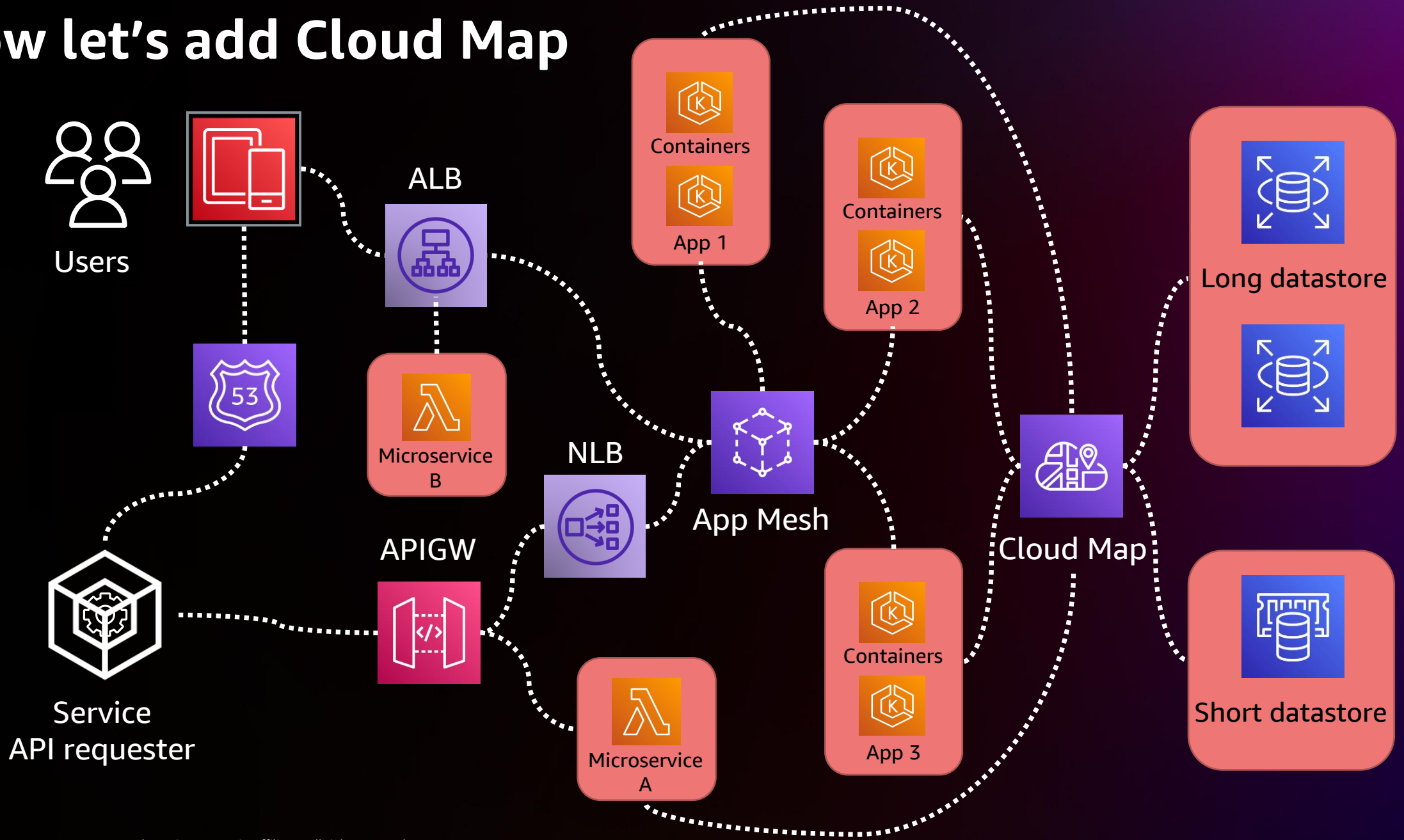
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Before Cloud Map

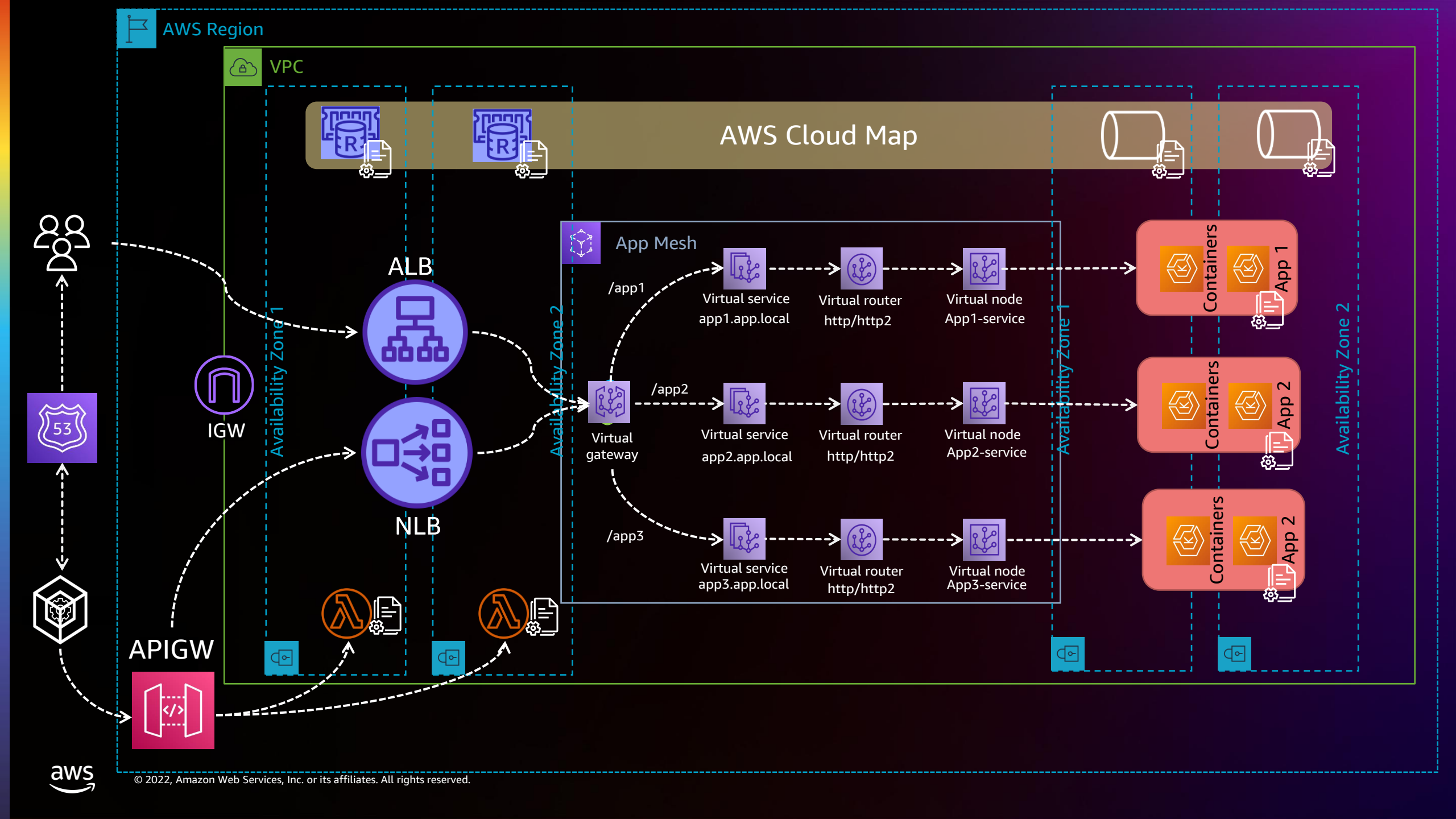


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Now let's add Cloud Map



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



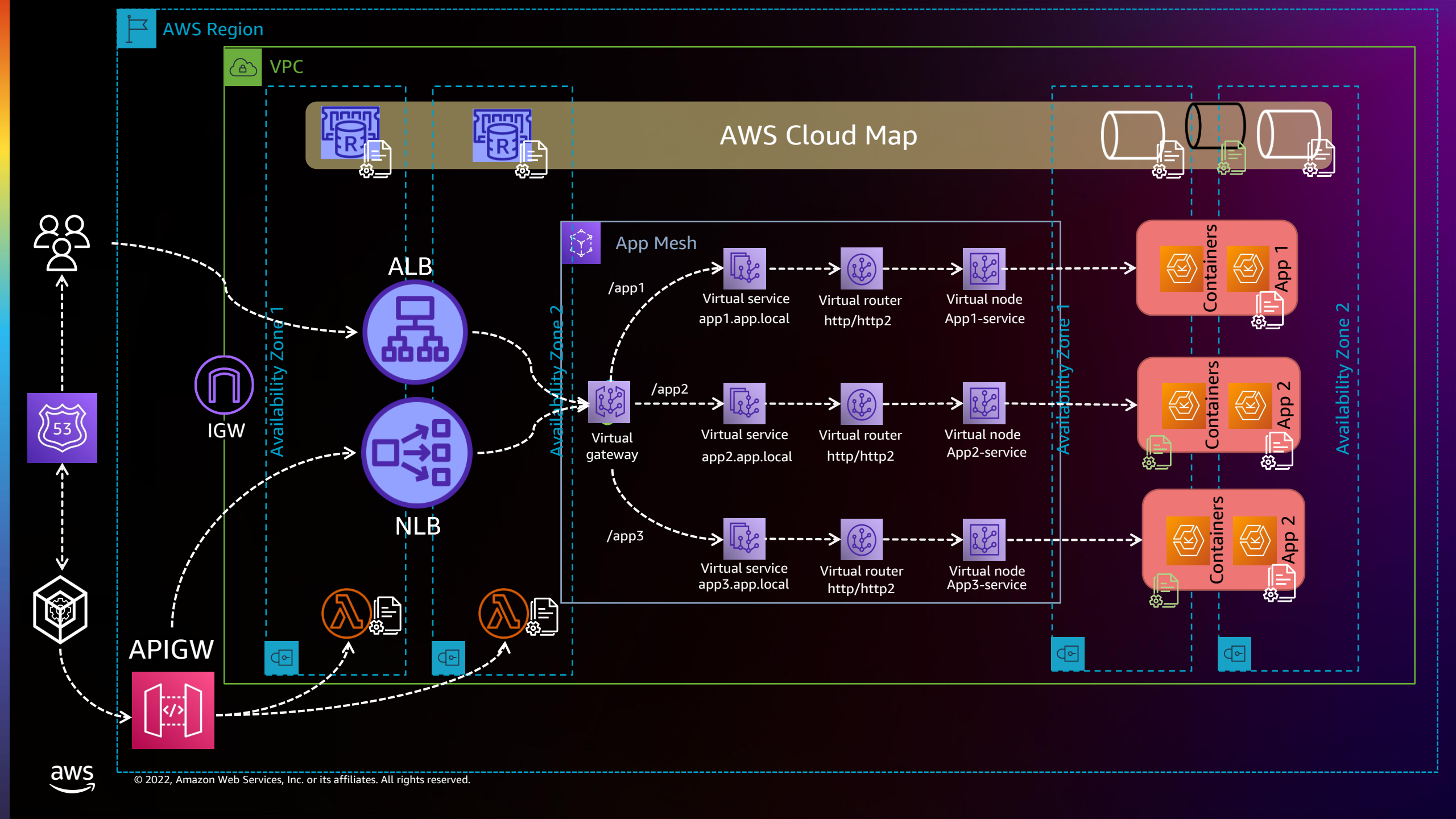
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



What can we do when we release a new schema or DB?

aws

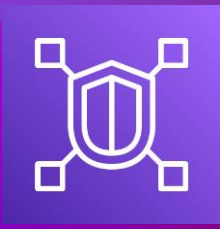
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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



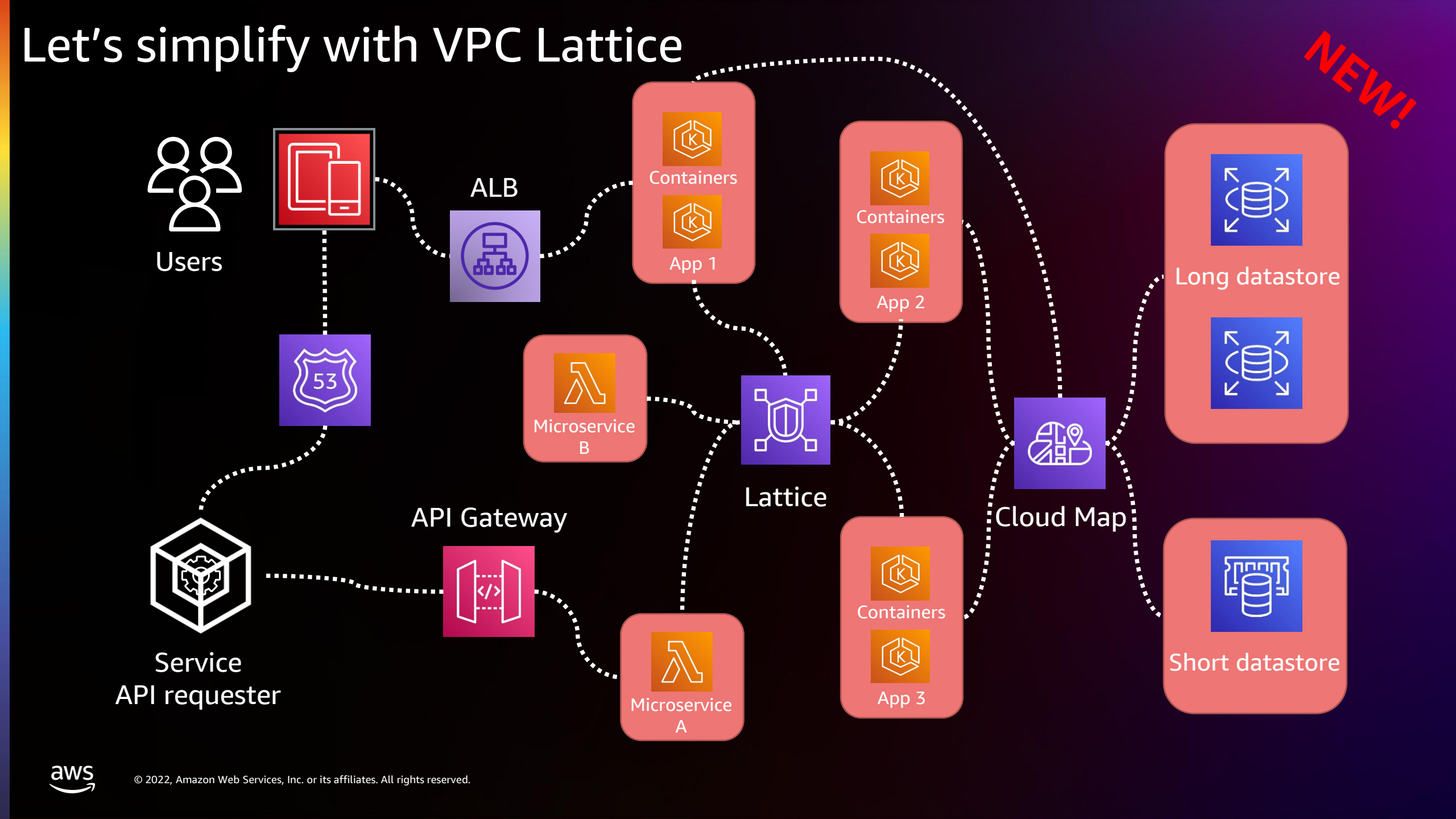
So we are at least more organized!



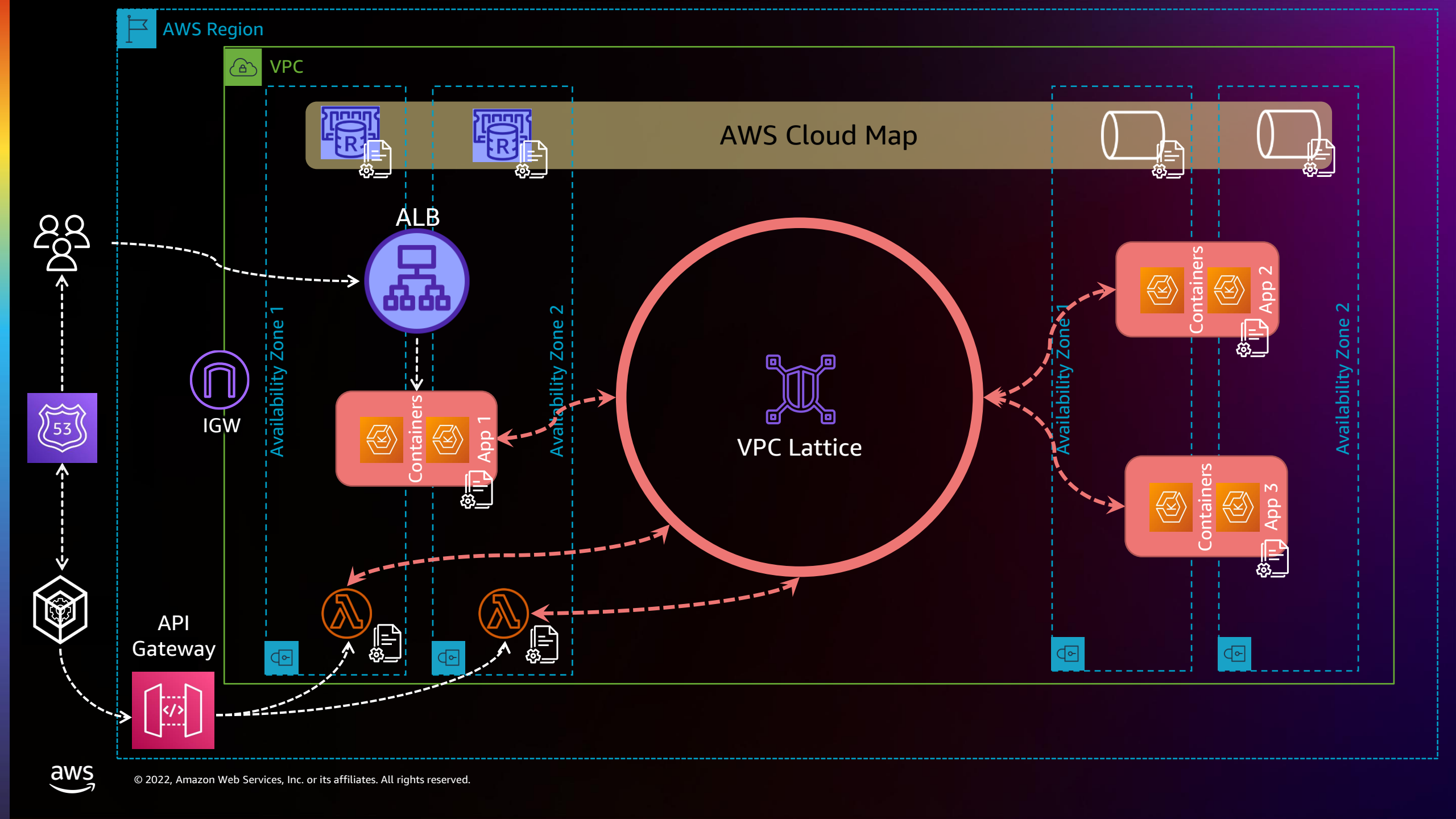
Can we make this a bit easier to manage in a scalable, secure, and performant manner?

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

Let’s simplify with VPC Lattice



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

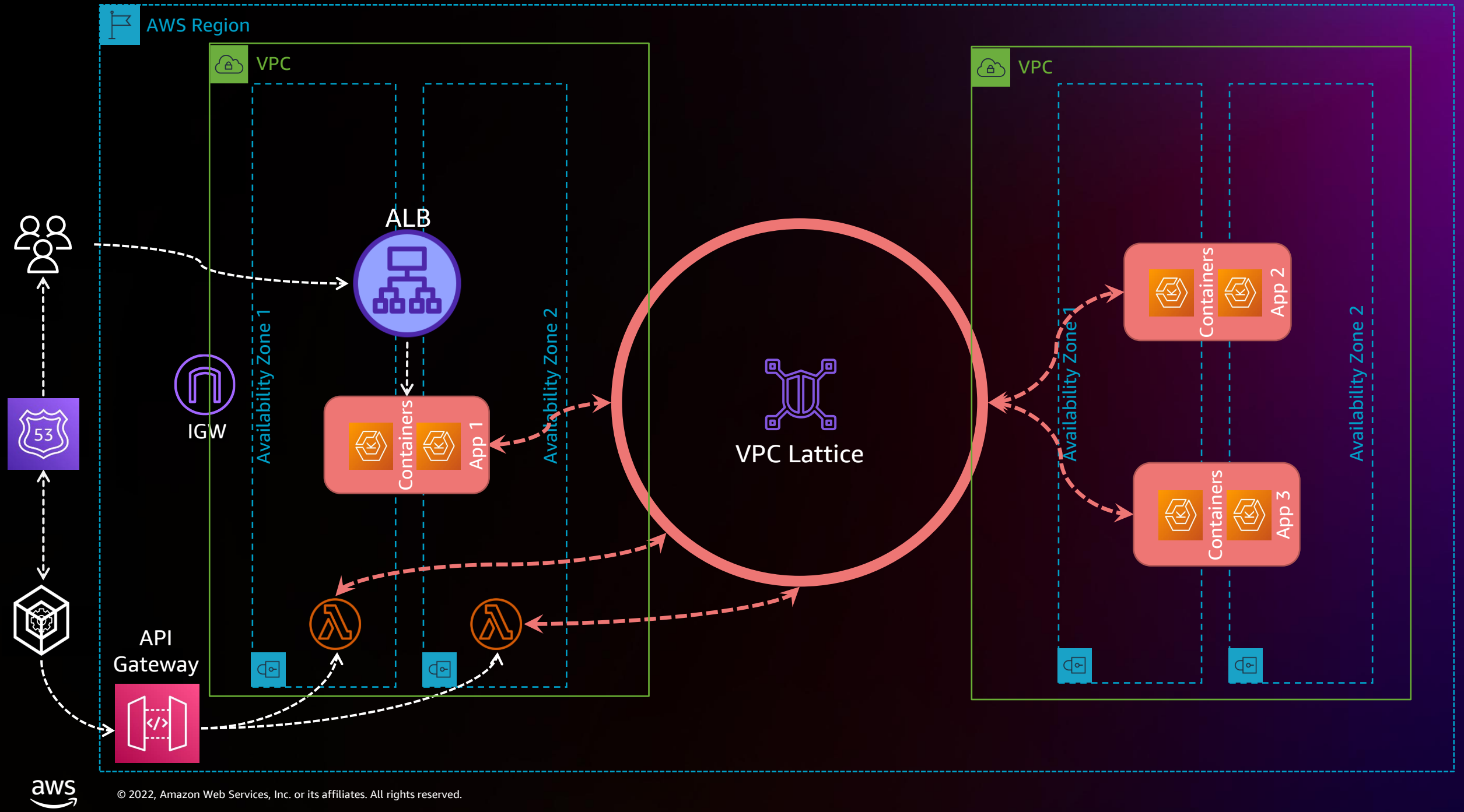


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

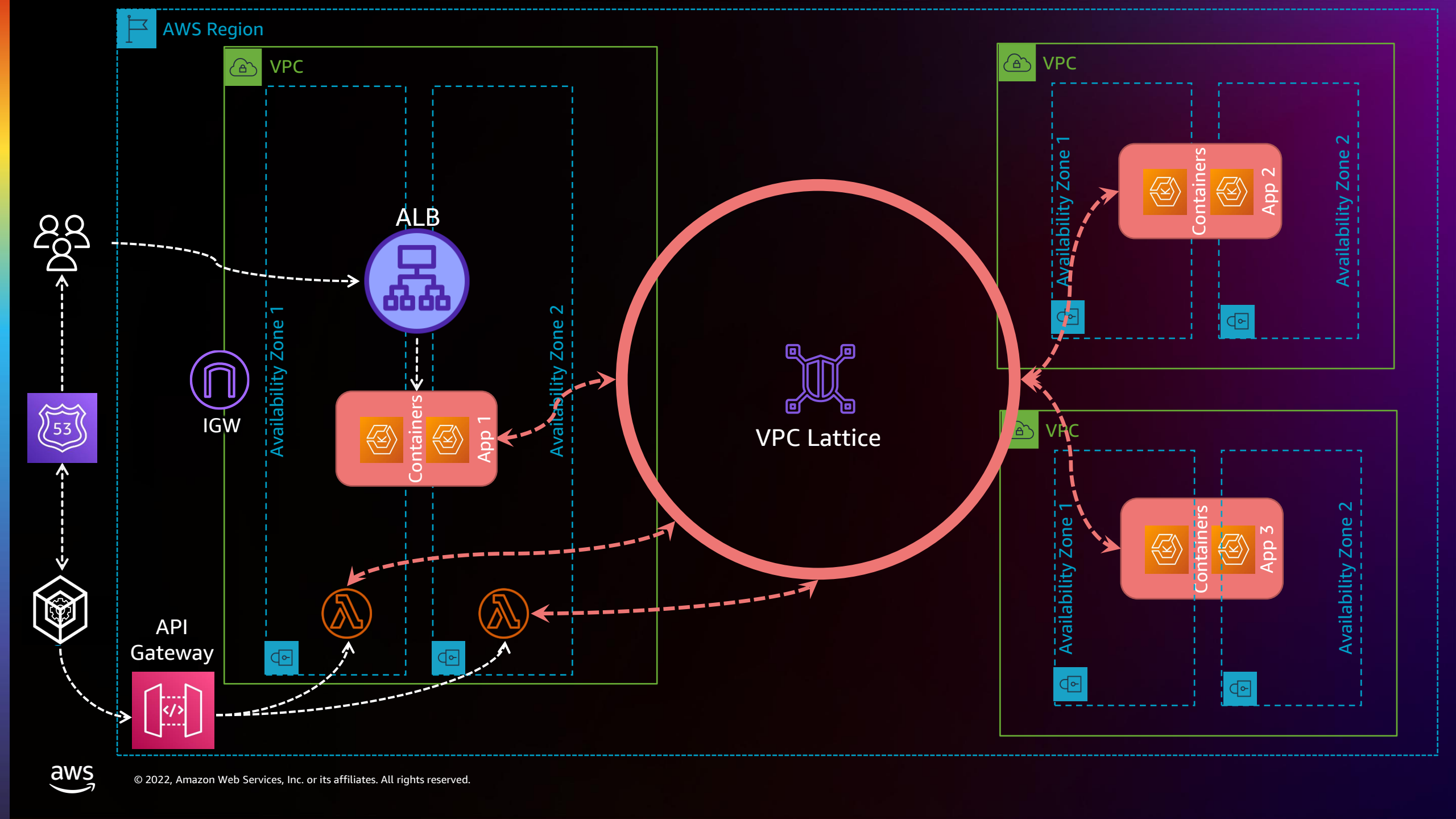


VPC Lattice helps connect your applications across VPCs

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



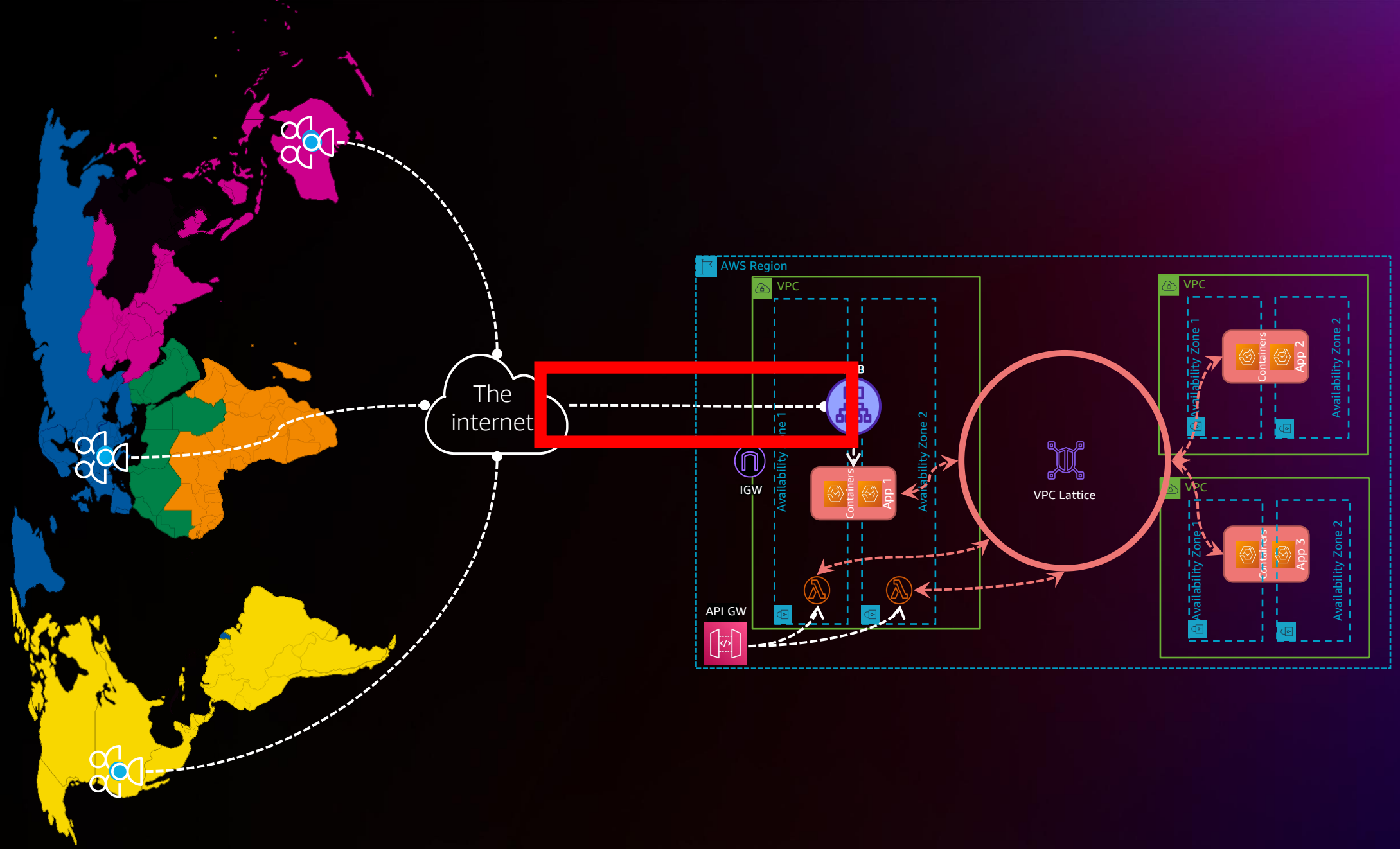
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

What does our global reach currently look like?

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



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

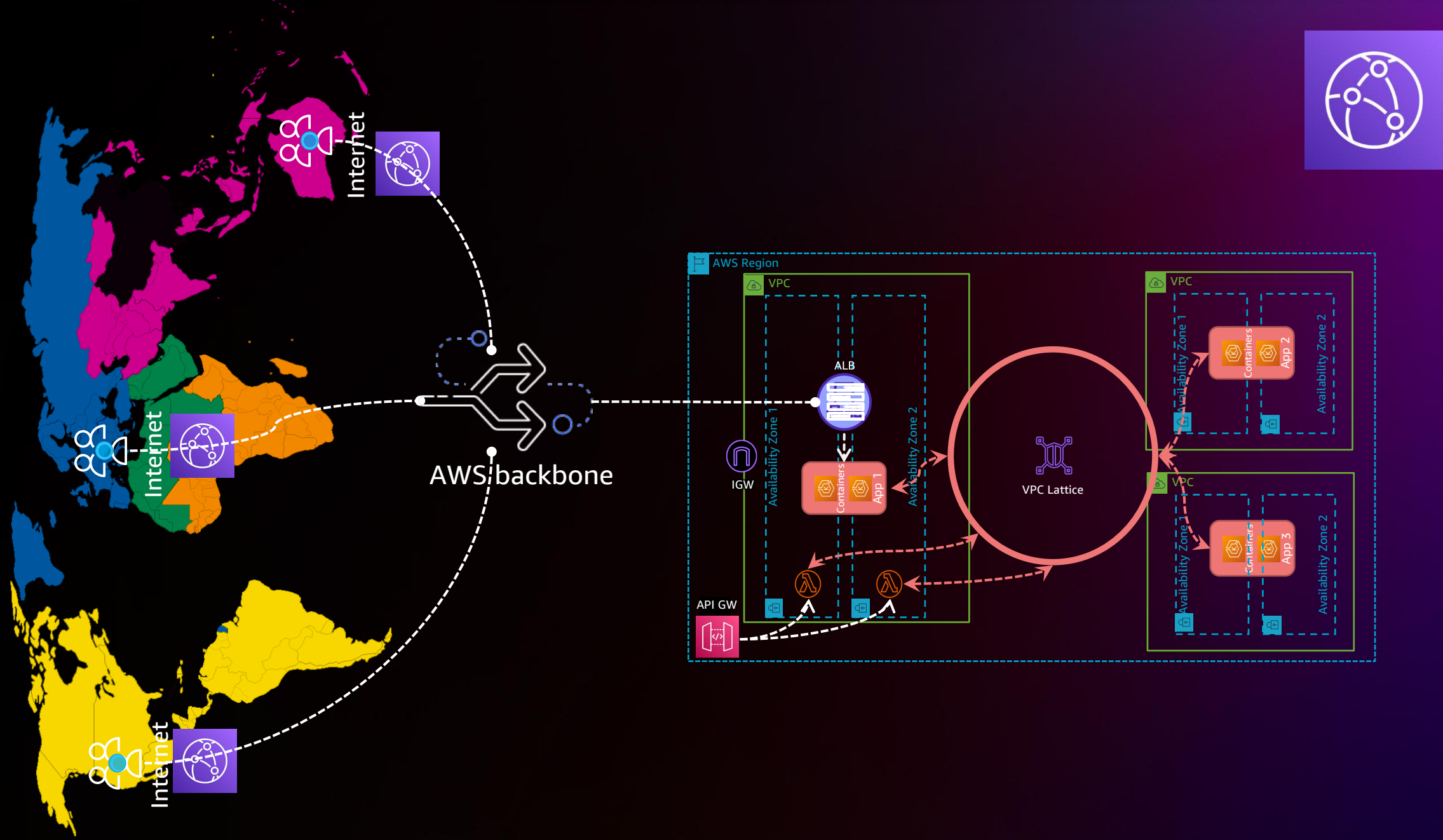


How can we improve performance and reduce load?

Amazon CloudFront

aws

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



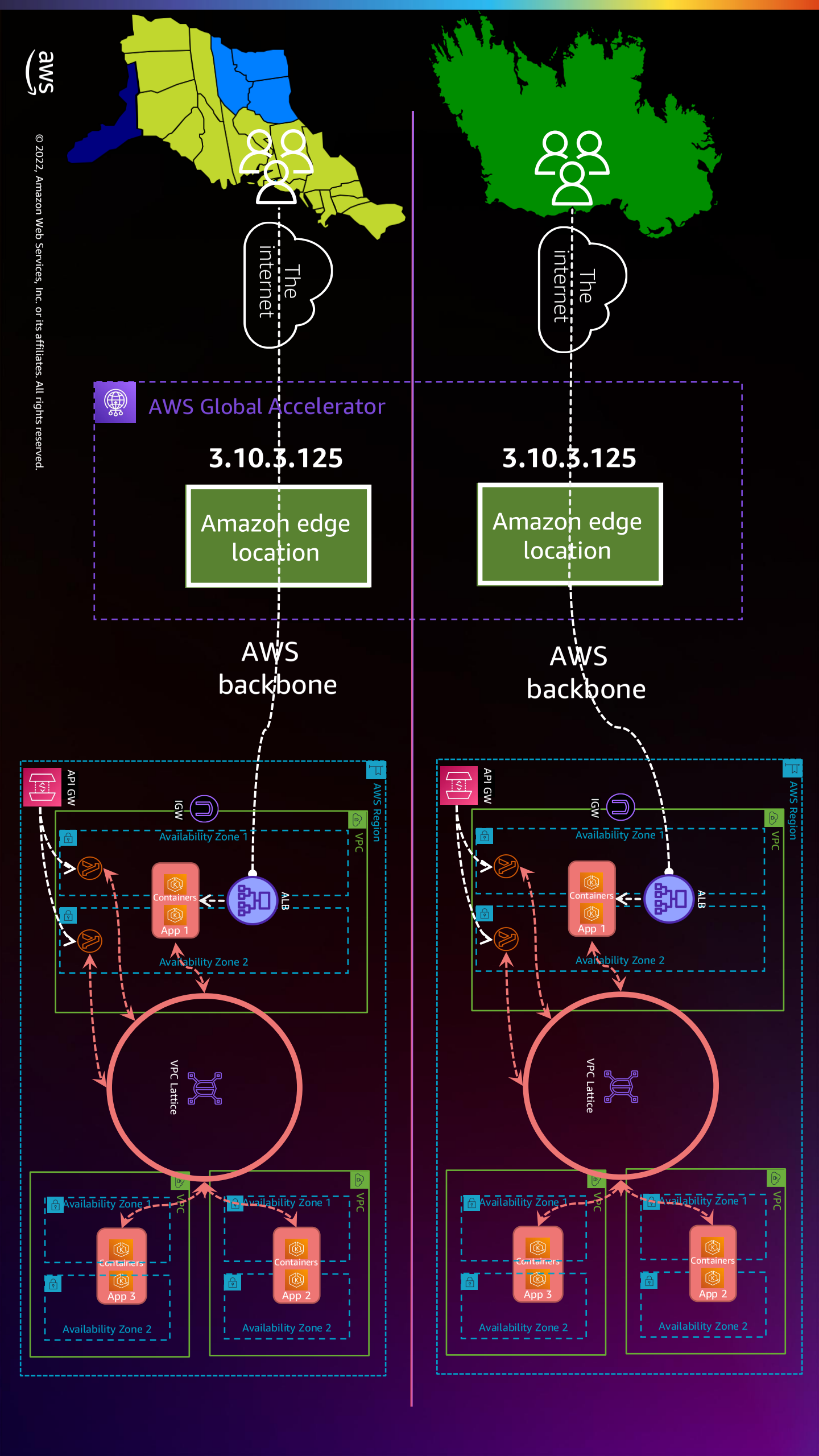
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



We need high availability and a global reach

aws

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

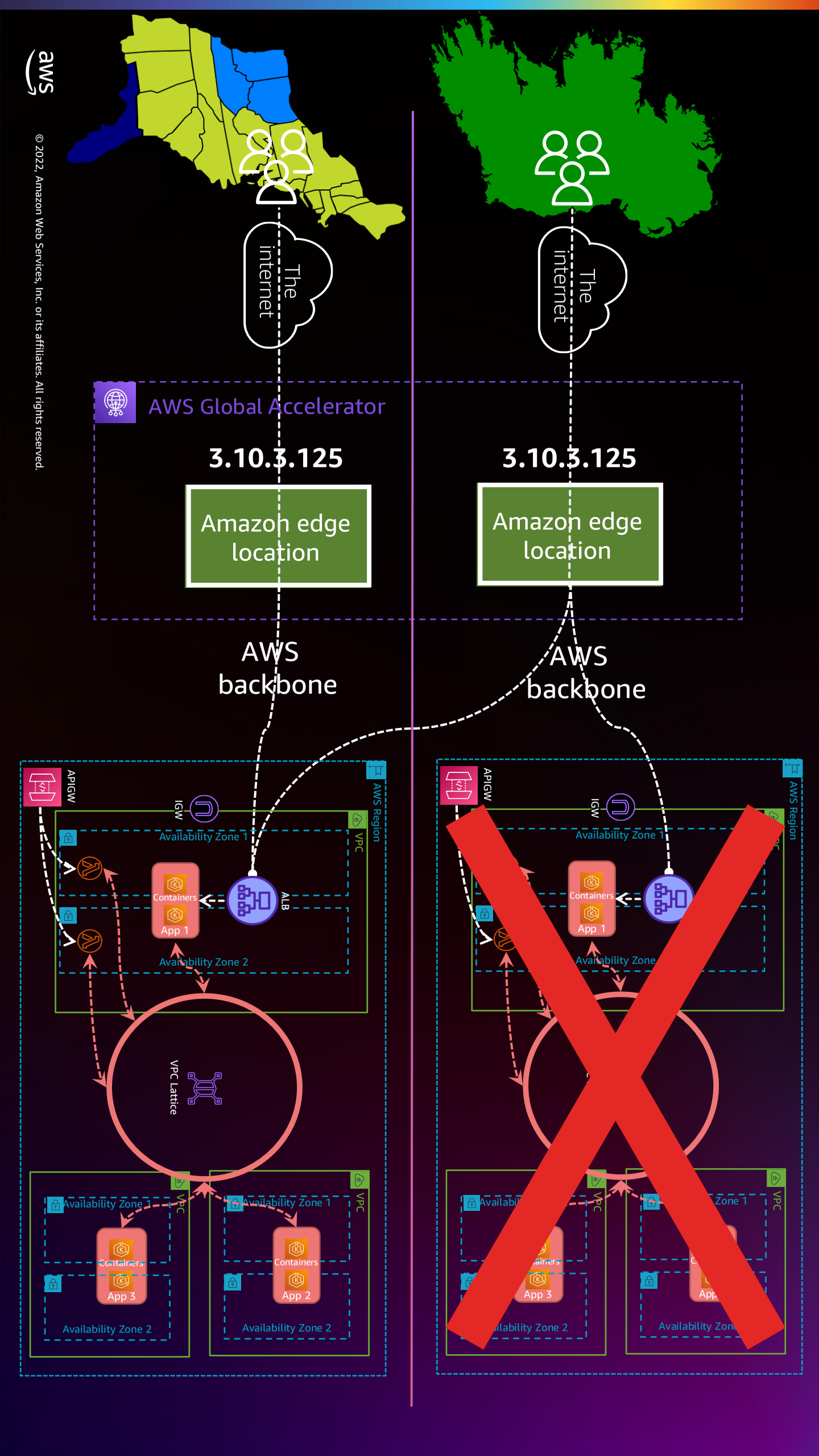

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.
The internet
The internet
AWS Global Accelerator
3.10.3.125
3.10.3.125
Amazon edge location
Amazon edge location
AWS backbone
AWS backbone
API GW
IGW
AWS Region
VPC
Availability Zone 1
Containers
App 1
ALB
Availability Zone 2
VPC Lattice
Availability Zone 1
Containers
App 3
Availability Zone 2
Availability Zone 1
Containers
App 2
Availability Zone 2

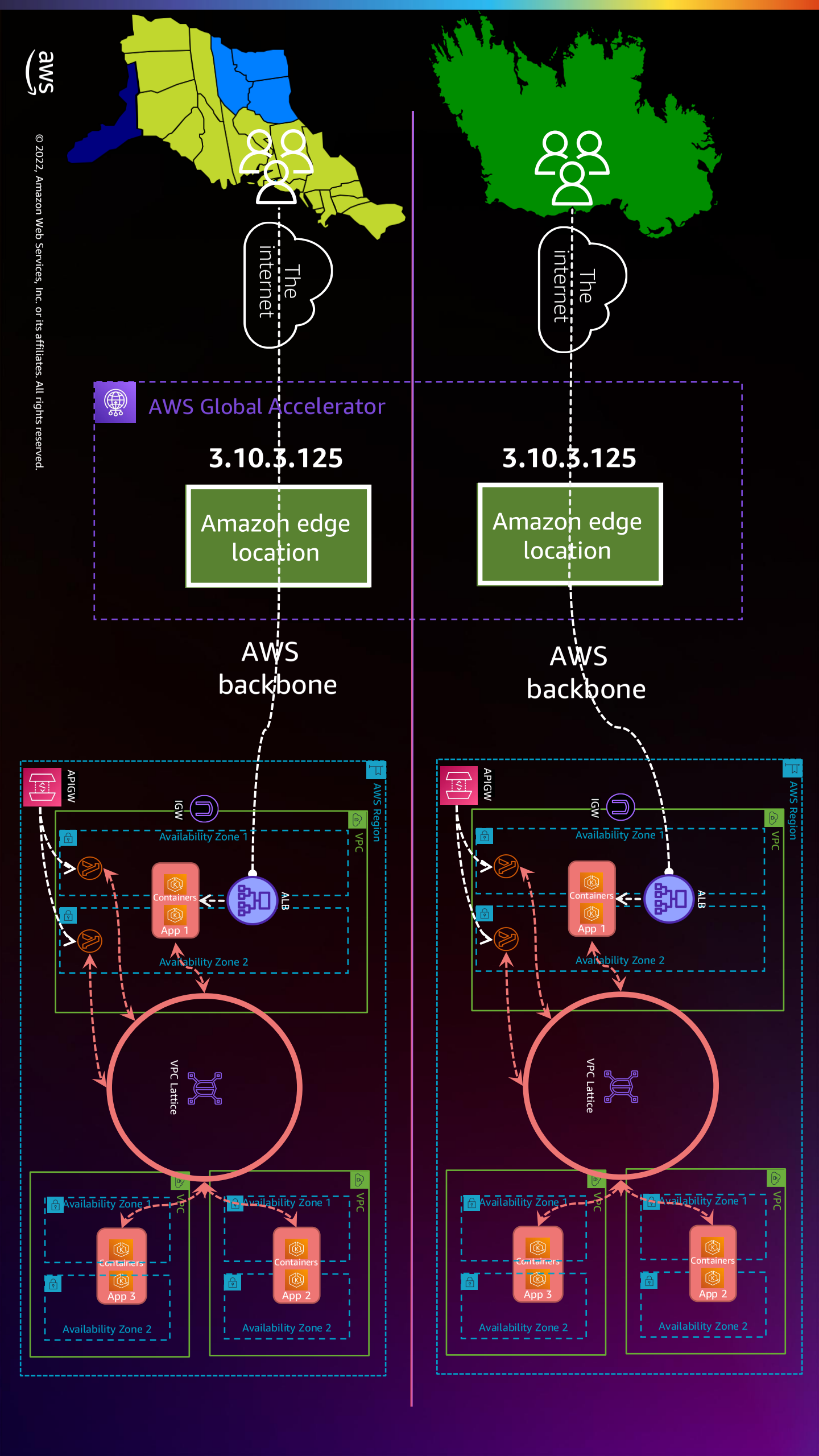


How is this highly available?

aws

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


aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.
The internet
The internet
AWS Global Accelerator
3.10.3.125
3.10.3.125
Amazon edge location
Amazon edge location
AWS backbone
AWS backbone
APIGW
IGW
AWS Region
Availability Zone 1
VPC
Containers
App 1
ALB
Availability Zone 2
VPC Lattice
Availability Zone 1
VPC
Containers
App 3
Availability Zone 2
Availability Zone 1
VPC
Containers
App 2
Availability Zone 2


aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.
The internet
The internet
AWS Global Accelerator
3.10.3.125
3.10.3.125
Amazon edge location
Amazon edge location
AWS backbone
AWS backbone
APIGW
IGW
AWS Region
VPC
Availability Zone 1
Containers
App 1
ALB
Availability Zone 2
VPC Lattice
Availability Zone 1
Containers
App 3
Availability Zone 2
Availability Zone 1
Containers
App 2
Availability Zone 2

Much



better!

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

Thank you!



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

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