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

NET302

# Advanced VPC design and new Amazon VPC capabilities


Matt Lehwess

Sr. Principal Solutions Architect
Amazon EC2 Networking

Alexandra Huides

Principal Networking Specialist Solutions Architect
AWS Strategic Accounts



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

# Some housekeeping items

300

NET302 is a 300-level session, not entry level, nor expert



We'll let you know when a buildout is complete for photos

QR Codes instead of links – feel free to take a photo



aws

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

# From the beginning

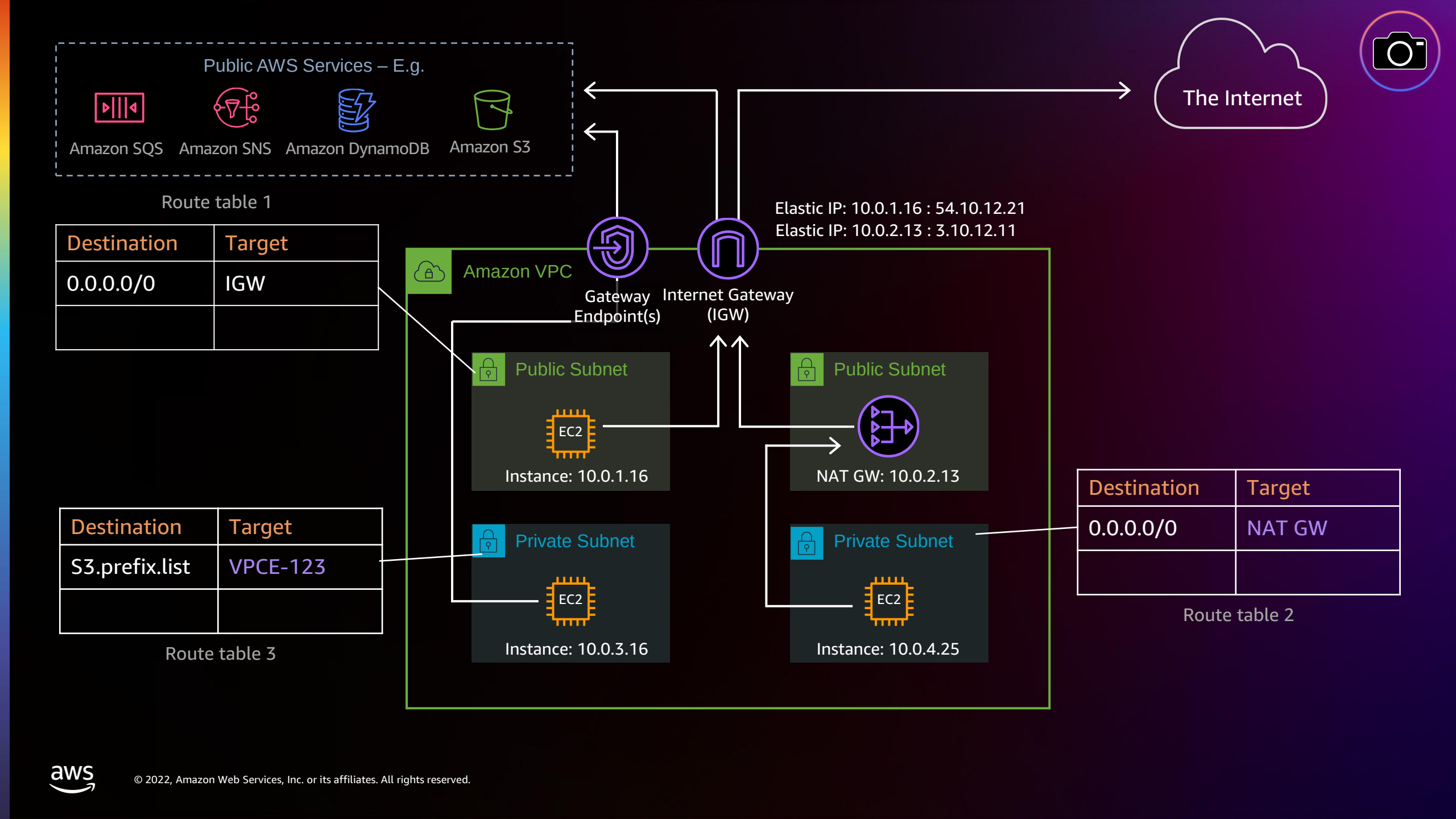



Instance:
203.0.113.54

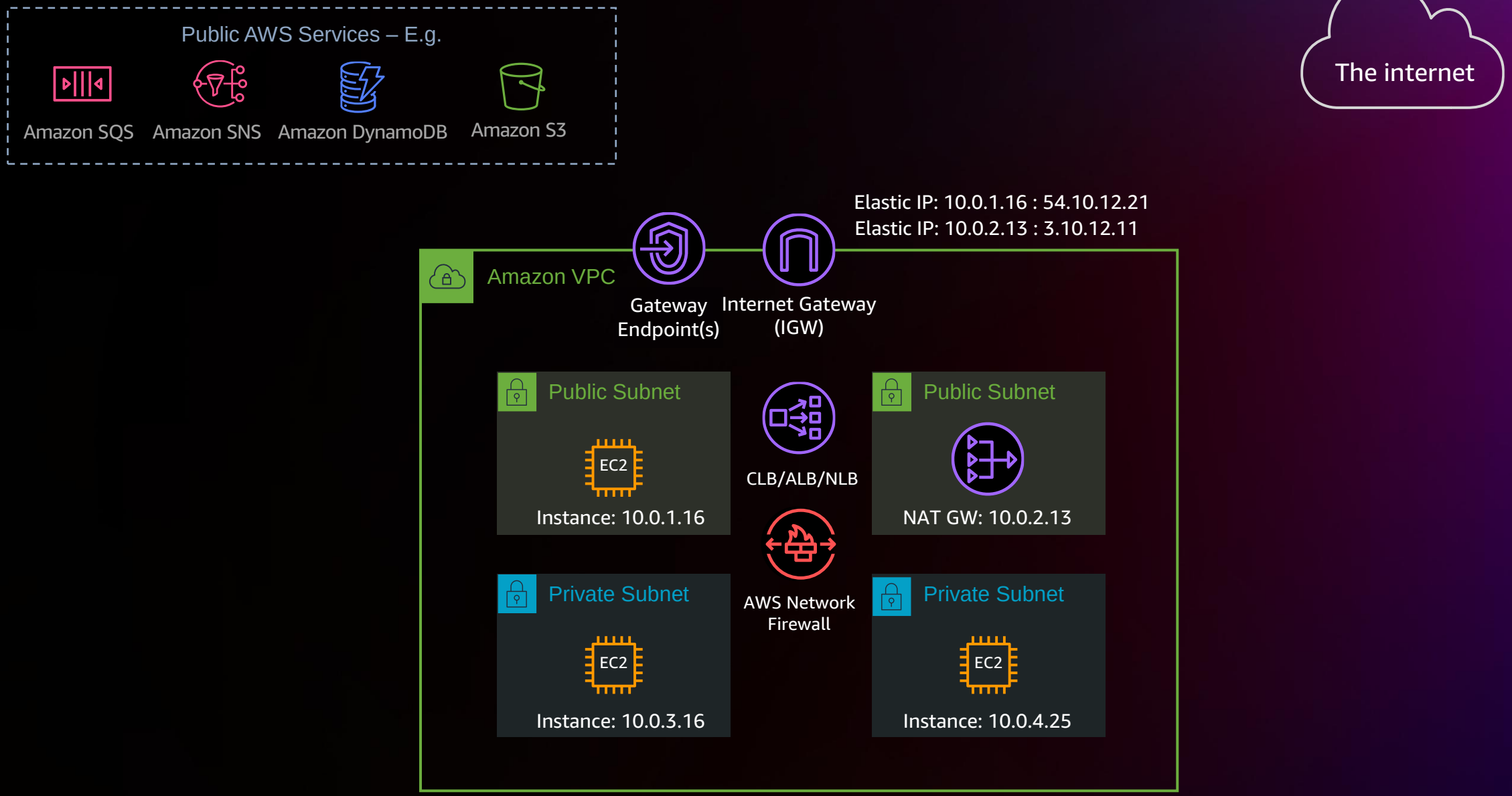
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



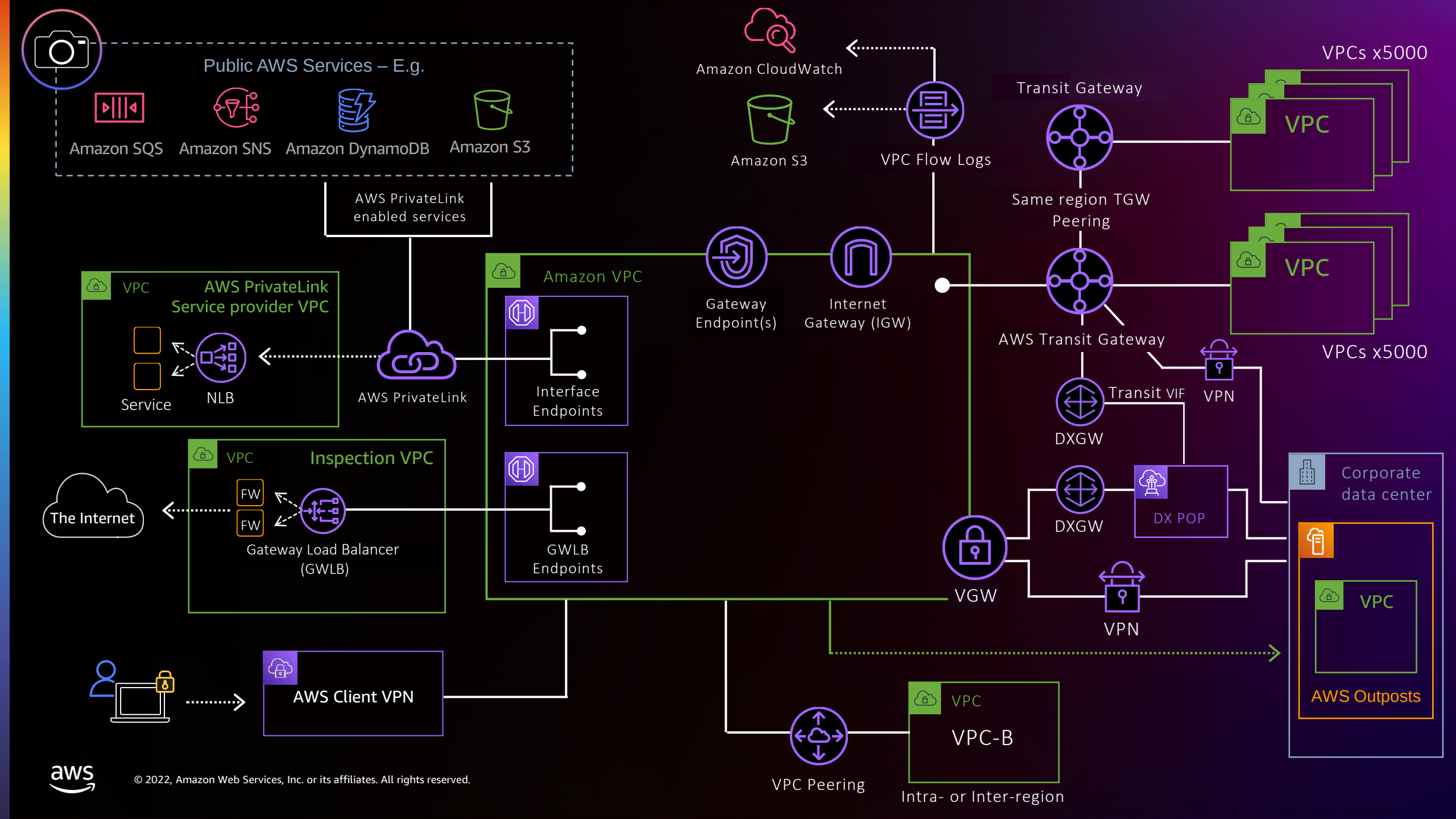

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.




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

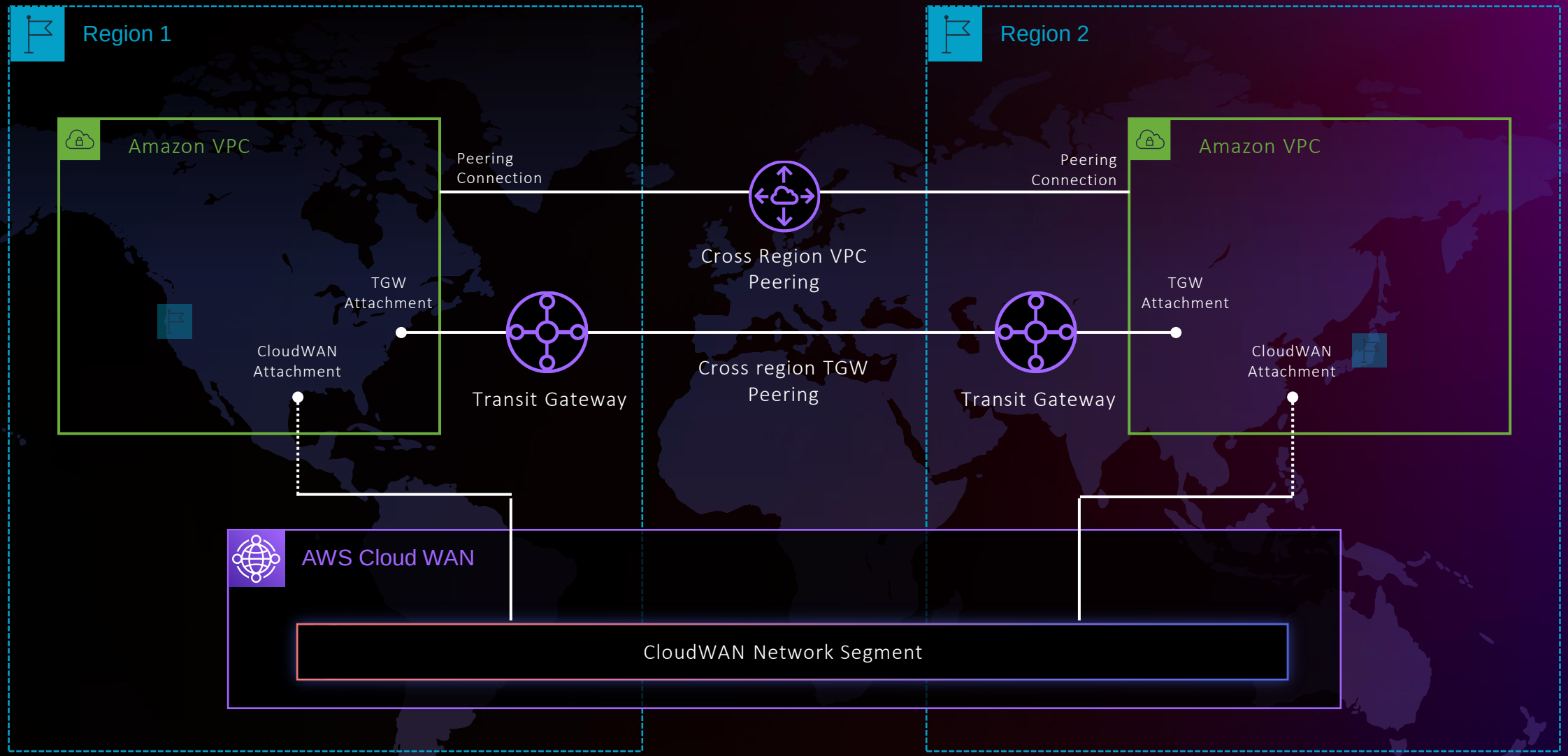



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Public AWS Services – E.g.
Amazon SQS
Amazon SNS
Amazon DynamoDB
Amazon S3
AWS PrivateLink enabled services
Amazon CloudWatch
Amazon S3
VPC Flow Logs
Transit Gateway
VPCs x5000
VPC
Same region TGW Peering
VPC
VPCs x5000
VPC
AWS PrivateLink Service provider VPC
Service
NLB
AWS PrivateLink
Amazon VPC
Interface Endpoints
Gateway Endpoint(s)
Internet Gateway (IGW)
AWS Transit Gateway
Transit VIF
VPN
DXGW
VPC
Inspection VPC
FW
FW
Gateway Load Balancer (GWLB)
The Internet
GWLB Endpoints
DXGW
DX POP
Corporate data center
VGW
VPN
VPC
AWS Outposts
AWS Client VPN
VPC Peering
VPC
VPC-B
Intra- or Inter-region
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.




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

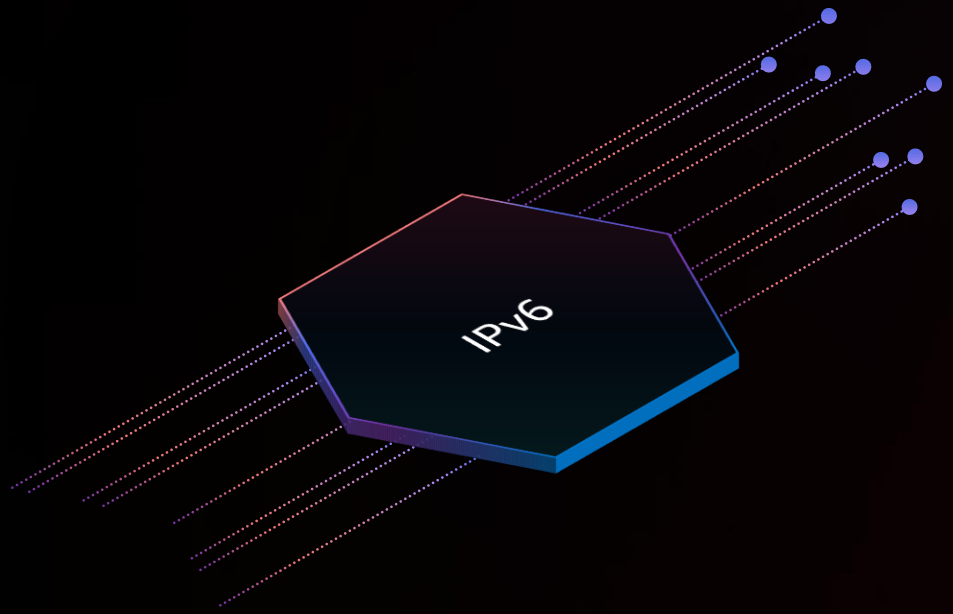



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# New capabilities

## Amazon VPC Networking






# Amazon VPC

## IPv6

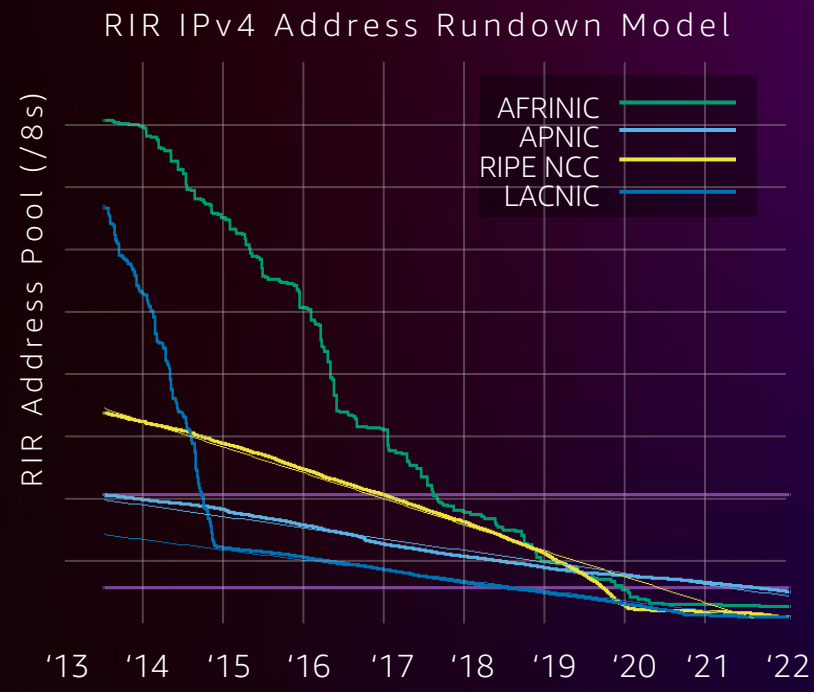
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IPv4 exhaustion

## Private v4

| Class | Private Address Range |
|---|---|
| A | 10.0.0.0 – 10.255.255.255 |
| B | 172.16.0.0 – 172.31.255.255 |
| C | 192.168.0.0 – 192.168.255.255 |

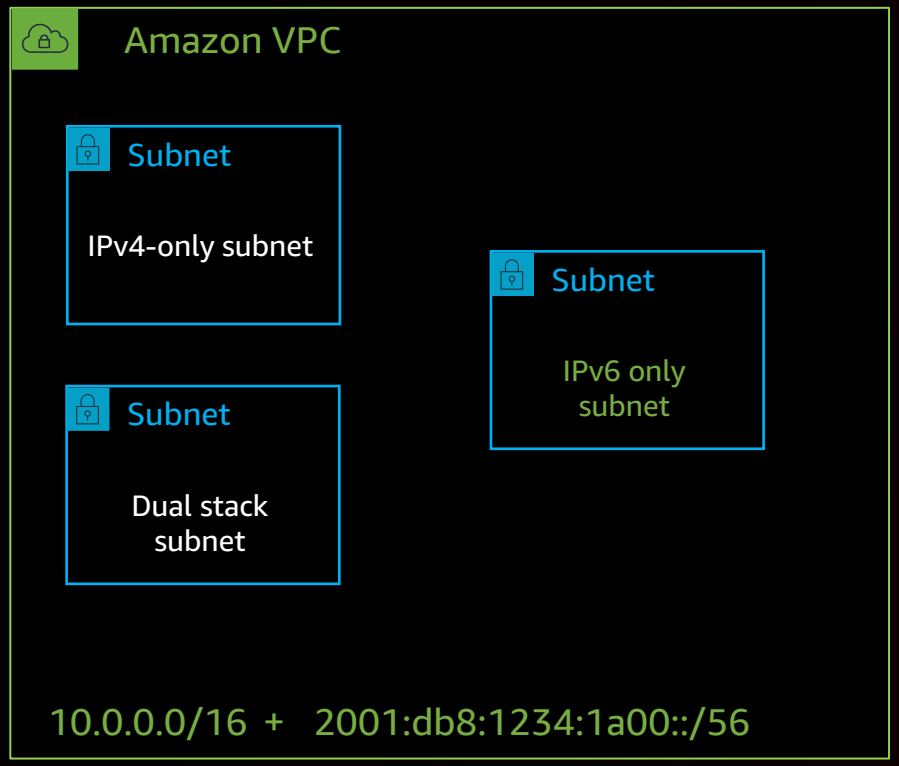
## Public v4




Source: https://ipv4.potaroo.net/

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

# IPv6-only subnets




IPv6

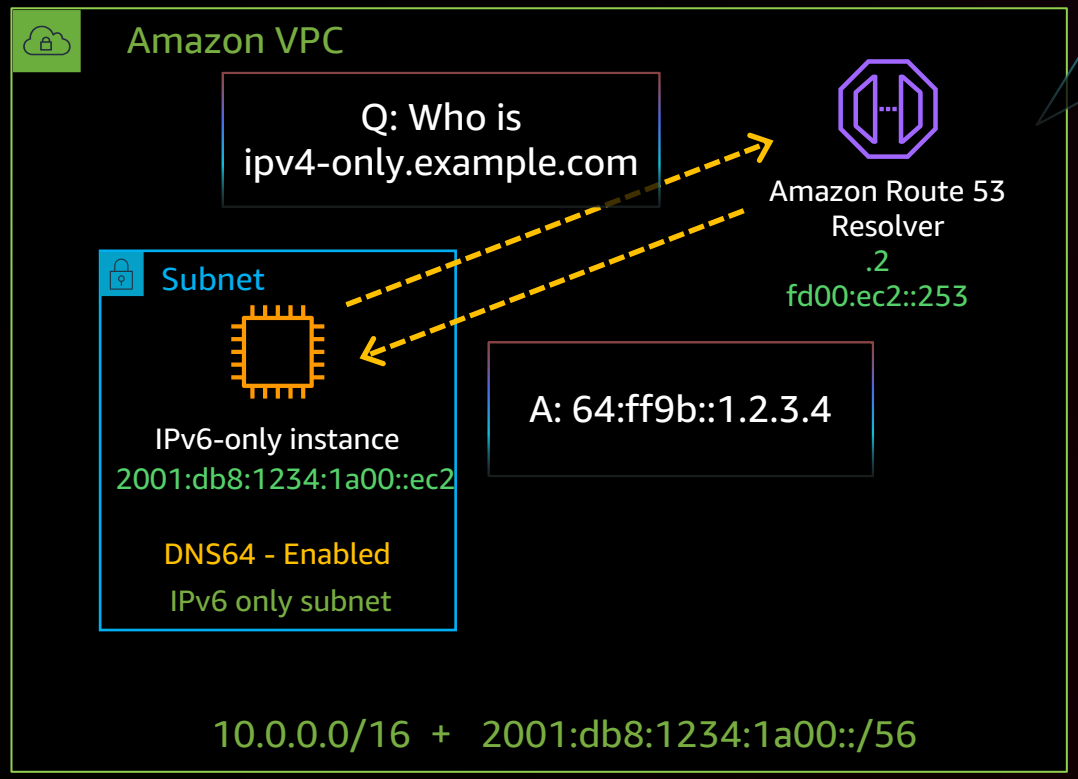
2021 releases

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

# DNS64

(DNS six to four)

Route 53 Resolver synthesizes an IPv6 address by adding 64:ff9b::/96 to the IPv4 address!



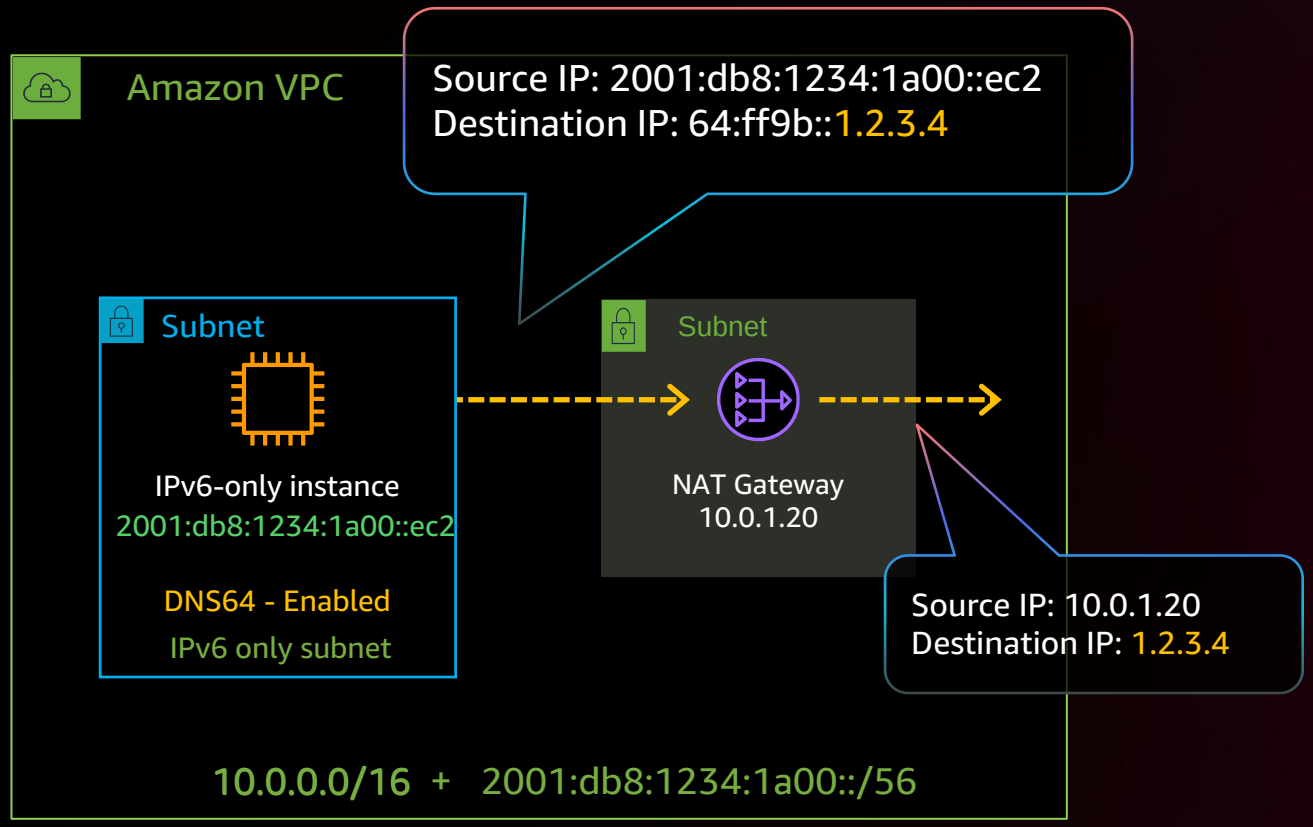

IPv6

2021 releases

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

# NAT64

(NAT six to four)



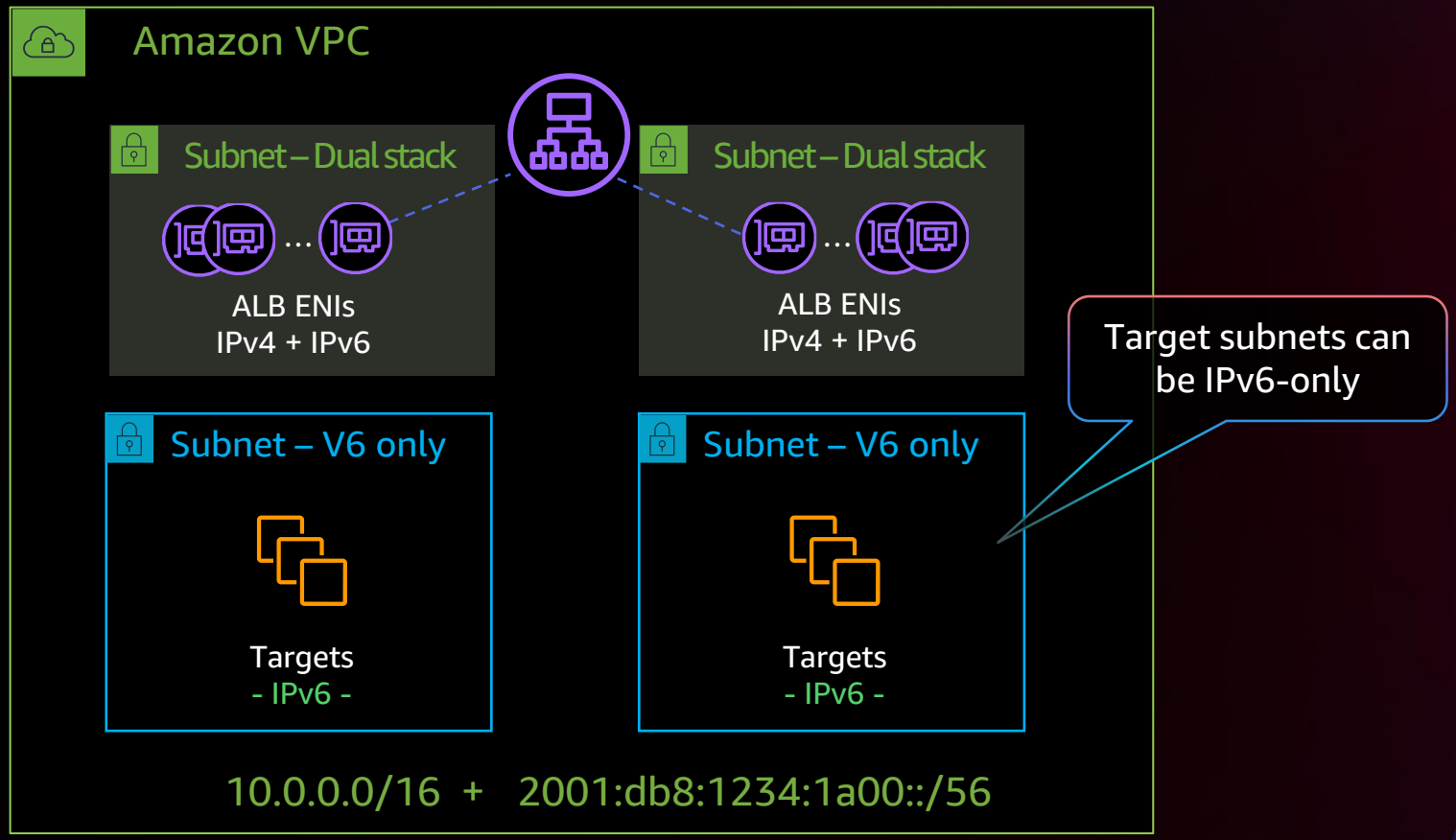

IPv6

2021 releases

aws

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

# ALB IPv6 targets

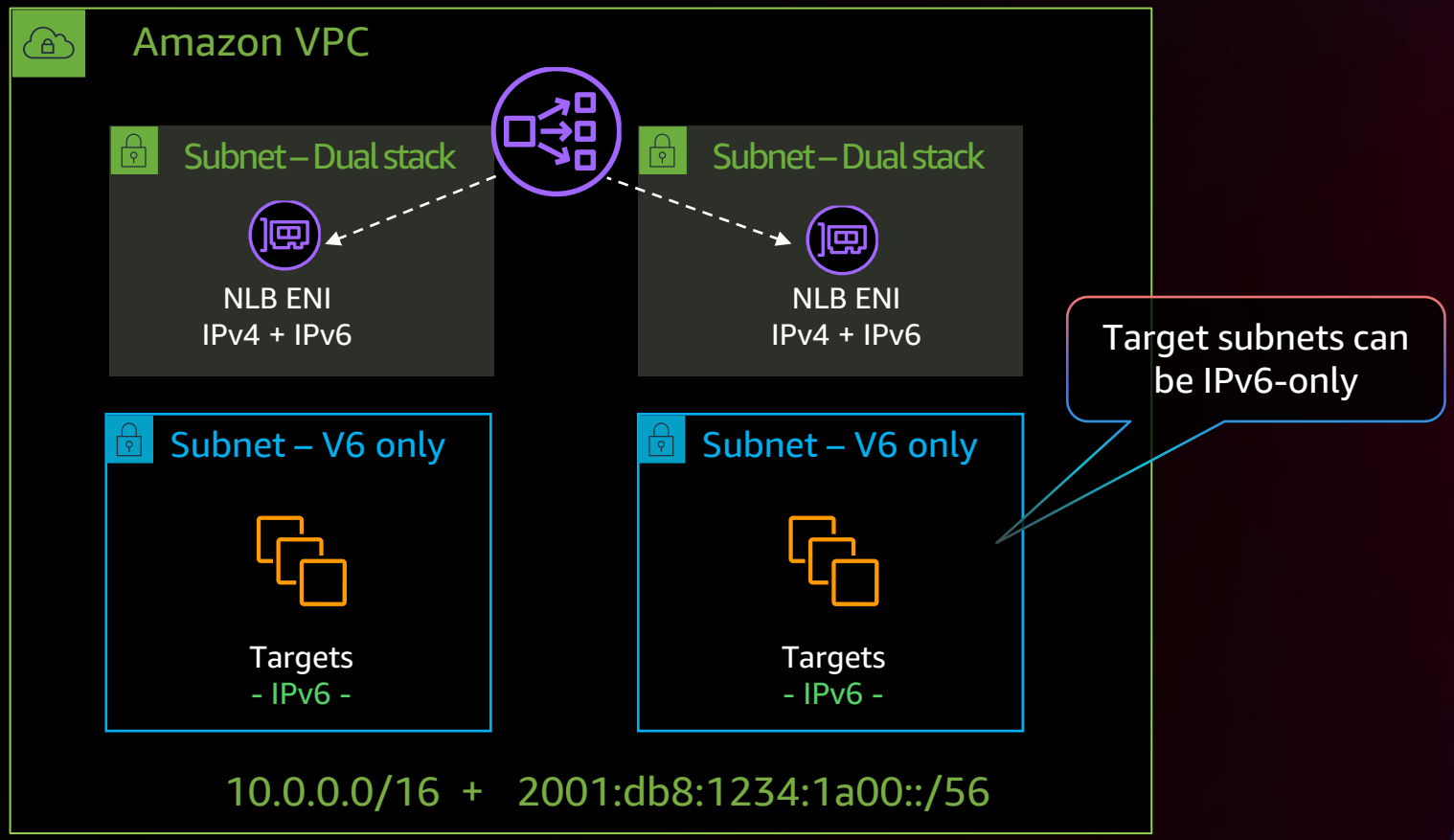



IPv6

2021 releases

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

# NLB IPv6 targets




IPv6

2021 releases

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

NEW

# IPv6 on AWS

## 2022 updates

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

# AWS services – IPv6 support


Amazon EC2


Amazon S3


Amazon VPC


Amazon CloudFront


Elastic Load Balancing (ELB)


Amazon Lightsail


IAM


AWS Transit Gateway


AWS IoT


Amazon ECS


AWS Shield



Amazon Route 53


AWS WAF


AWS Site-to-Site VPN


Amazon EKS


Amazon WorkSpaces


AWS Direct Connect


AWS Fargate

# New for 2022


AWS Global Accelerator


AWS PrivateLink


Amazon Athena


AWS Cloud Map


AWS App Mesh


Amazon RDS


Amazon Aurora


AWS DMS


AWS Lambda

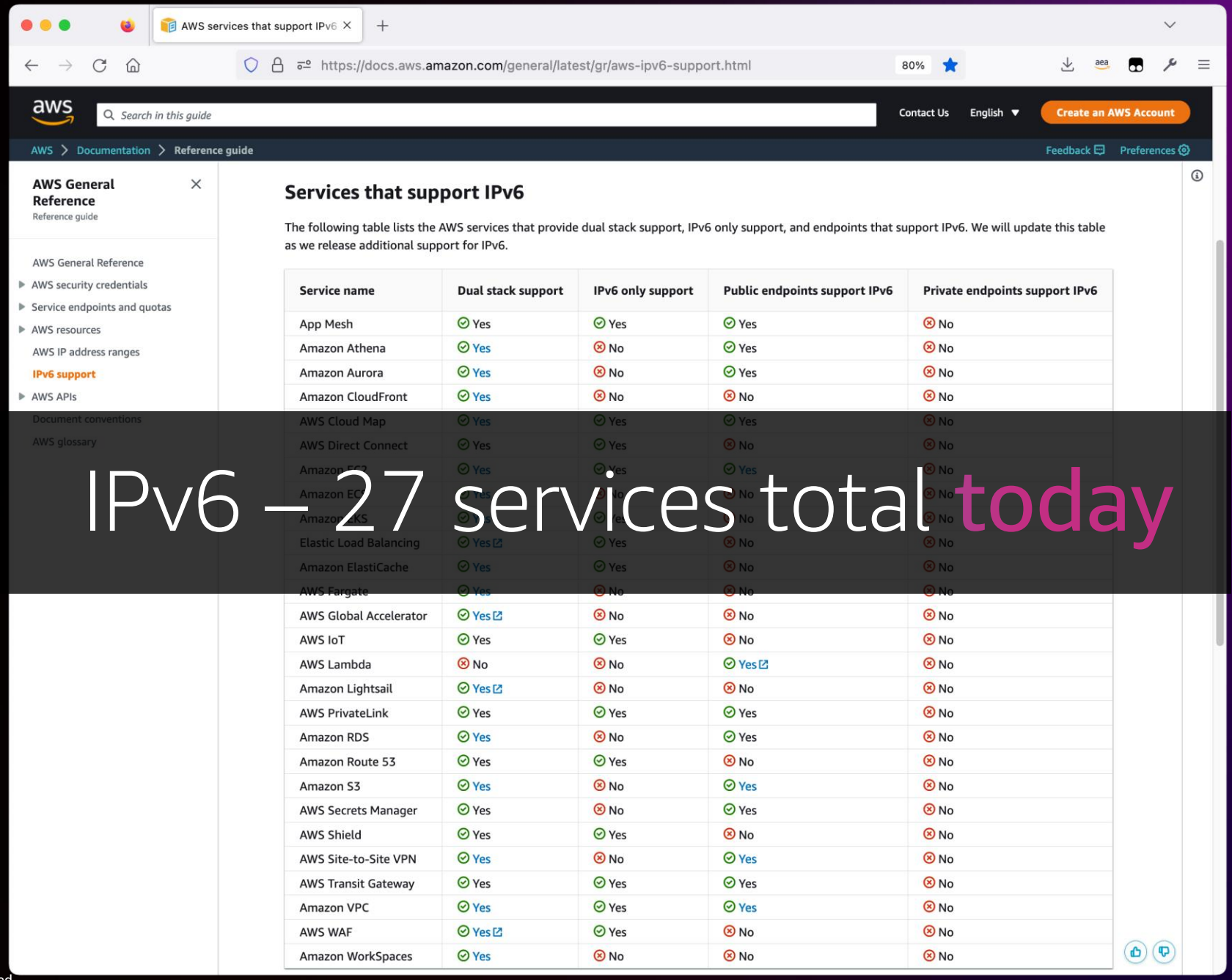

AWS Secrets Manager


Amazon ElastiCache

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

# IPv6 service support dashboard

https://go.aws/3inffFc




| Service name | Dual stack support | IPv6 only support | Public endpoints support IPv6 | Private endpoints support IPv6 |
|---|---|---|---|---|
| App Mesh | Yes | Yes | Yes | No |
| Amazon Athena | Yes | No | Yes | No |
| Amazon Aurora | Yes | No | Yes | No |
| Amazon CloudFront | Yes | No | No | No |
| AWS Cloud Map | Yes | Yes | Yes | No |
| AWS Direct Connect | Yes | Yes | No | No |
| Amazon EC2 | Yes | Yes | Yes | No |
| Amazon ECS | Yes | Yes | No | No |
| Amazon EKS | Yes | Yes | No | No |
| Elastic Load Balancing | Yes | Yes | No | No |
| Amazon ElastiCache | Yes | Yes | No | No |
| AWS Fargate | Yes | No | No | No |
| AWS Global Accelerator | Yes | No | No | No |
| AWS IoT | Yes | Yes | No | No |
| AWS Lambda | No | No | Yes | No |
| Amazon Lightsail | Yes | No | No | No |
| AWS PrivateLink | Yes | Yes | Yes | No |
| Amazon RDS | Yes | No | Yes | No |
| Amazon Route 53 | Yes | Yes | No | No |
| Amazon S3 | Yes | No | Yes | No |
| AWS Secrets Manager | Yes | No | Yes | No |
| AWS Shield | Yes | Yes | No | No |
| AWS Site-to-Site VPN | Yes | No | Yes | No |
| AWS Transit Gateway | Yes | Yes | Yes | No |
| Amazon VPC | Yes | Yes | Yes | No |
| AWS WAF | Yes | Yes | No | No |
| Amazon WorkSpaces | Yes | No | No | No |

IPv6 – 27 services total today

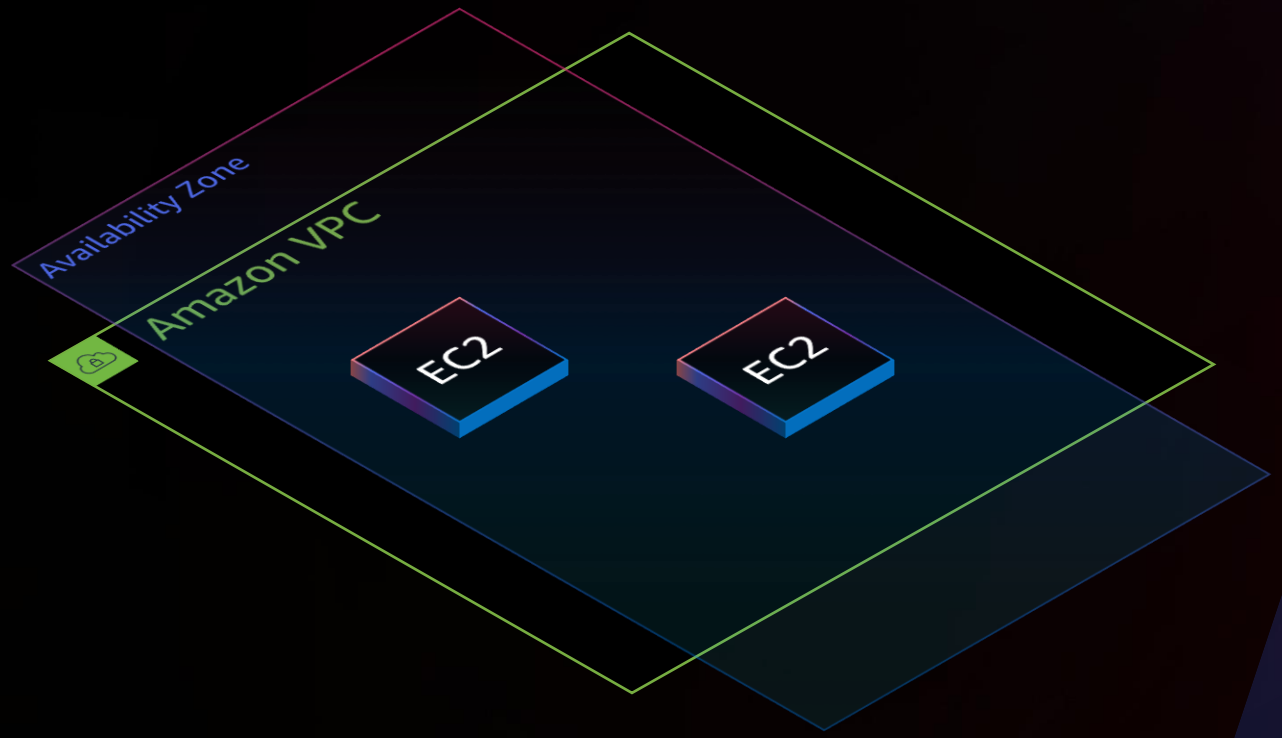
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# IPv6
## on AWS



https://aws.amazon.com/vpc/ipv6/

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

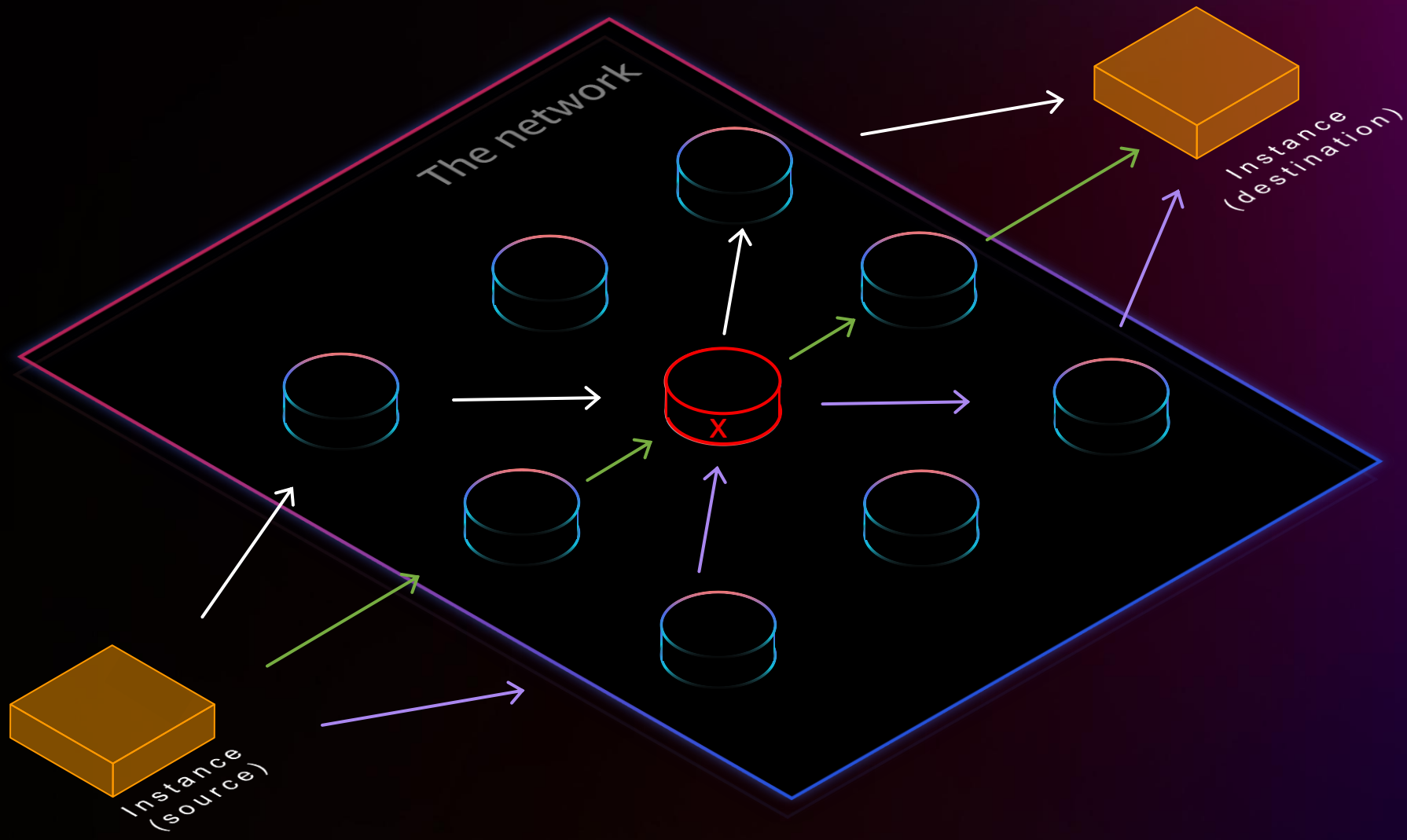



# Amazon VPC

## ENA Express

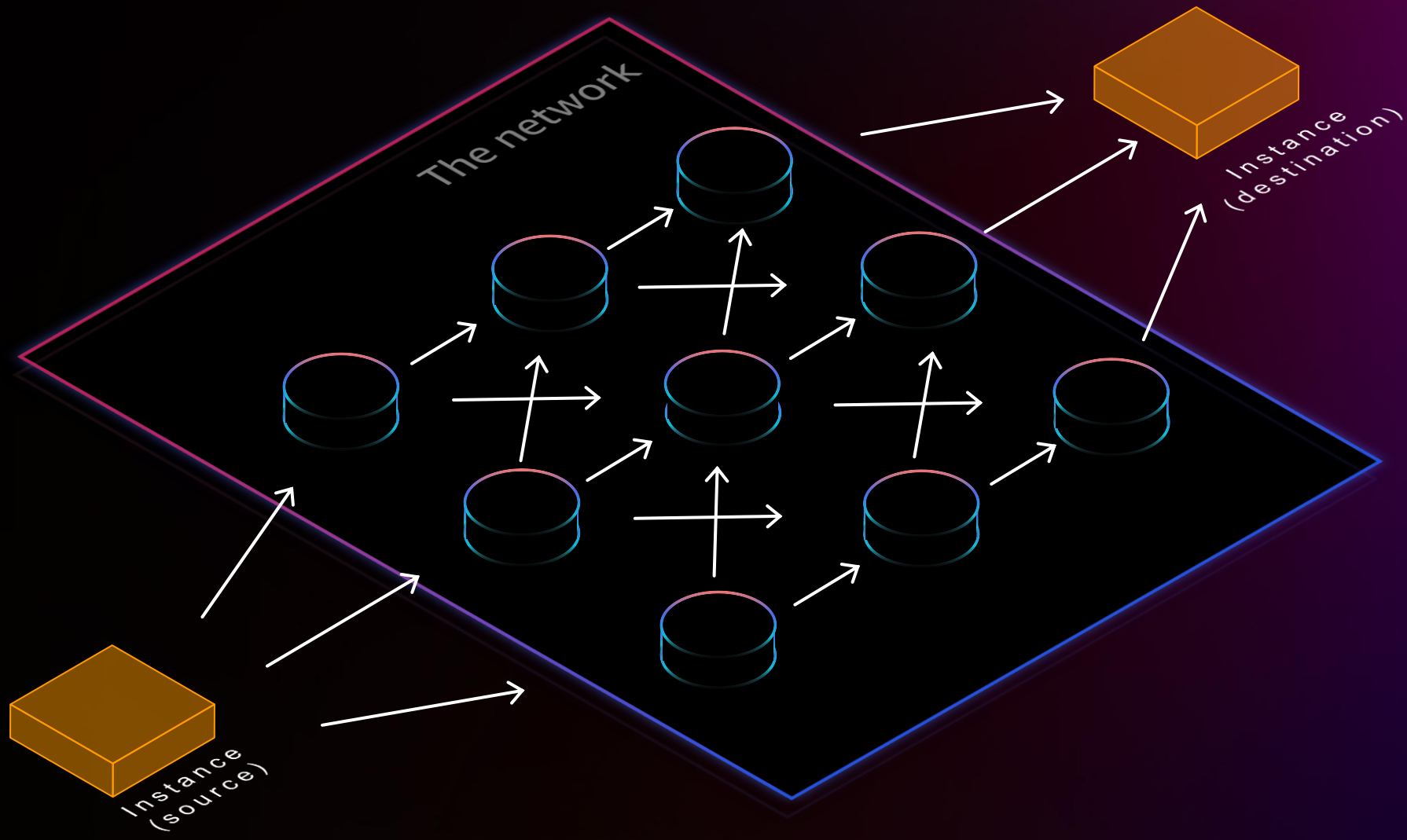
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Traditional TCP routing




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

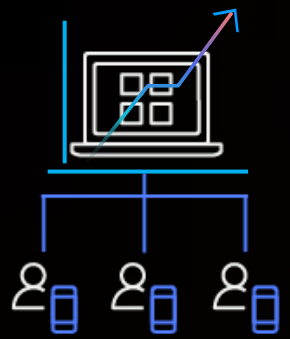
# Scalable Reliable Datagram (SRD) routing




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

# Amazon VPC ENA Express

## POWERED BY SCALABLE RELIABLE DATAGRAM (SRD) PROTOCOL



### Improved network performance

Reduced latency, jitter, and packet drops. Up to 82% lower P99 and 93% lower for P99.9.



### Transport protocol independent

Can be used with both TCP and UDP



### 25 Gbps flow throughput

Between two Amazon EC2 instances in an Availability Zone

aws

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

# ENA Express

## Considerations

- ✓ No additional changes needed after enabling it on an ENA
- ✓ Can be enabled for Nitro-based Amazon EC2 Instances in the same Availability Zone
- ✓ ENA Express is currently supported for traffic directly between Amazon EC2 instances

aws

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

# Amazon VPC ENA Express

PERFORMANCE

## 25 Gbps

5x INCREASE

Up to 25 Gbps of single flow bandwidth- up from 5 Gbps

## 50%

LOWER P99 LATENCY

ENA Express reduces p99 network latency by up to 50%

## 83%

LOWER P99.9 LATENCY

ENA Express reduces p99.9 network latency by up to 83%

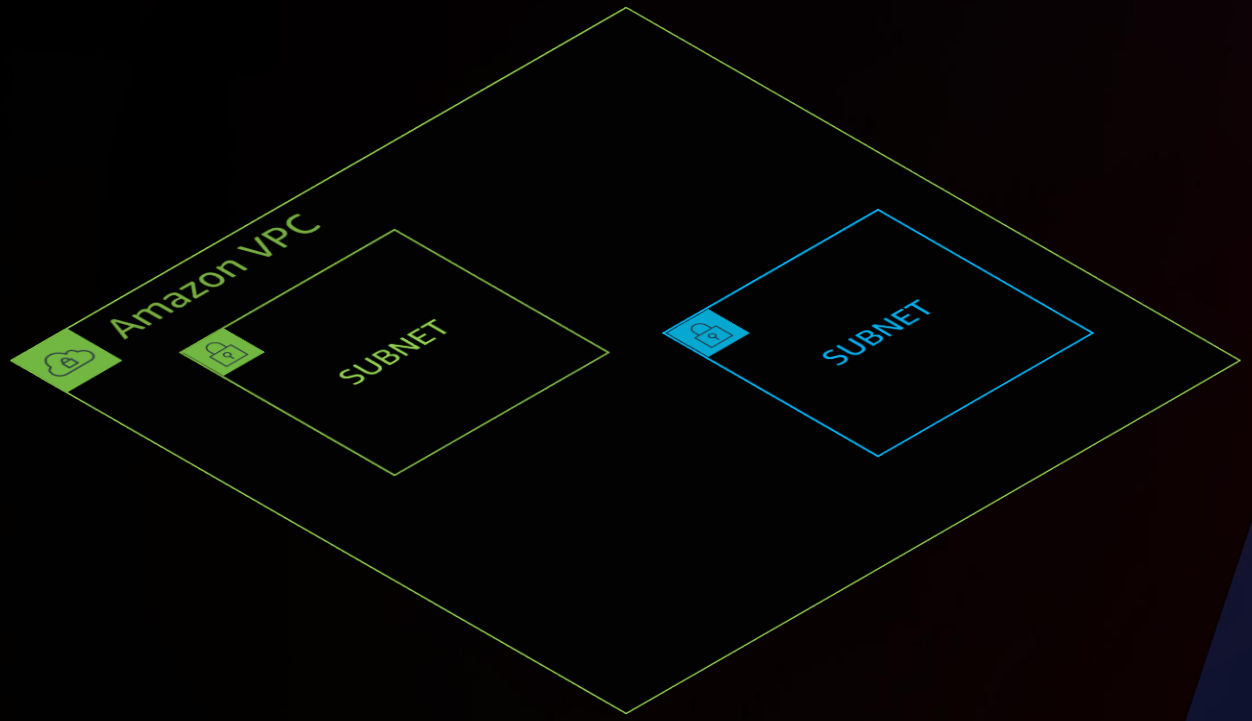
aws

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

# ENA Express



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




# Amazon VPC

## Advanced Architectures

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

# How do you define VPC size?

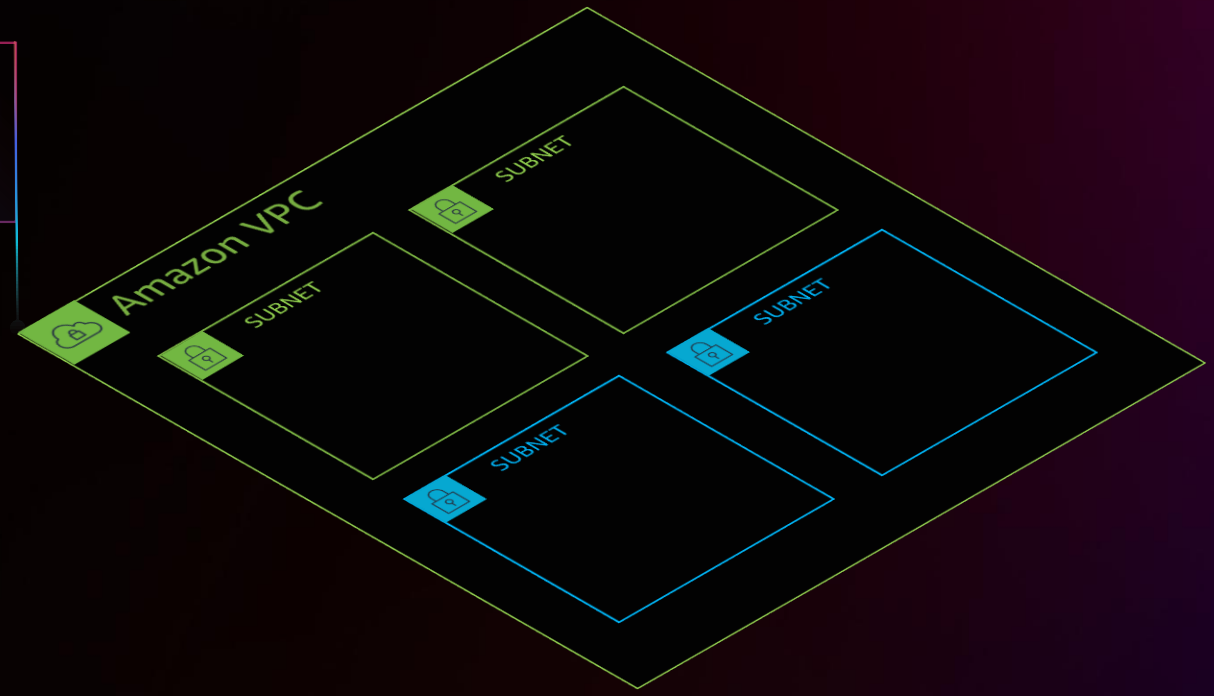



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon VPC Network Address Usage

SINGLE VPC

256,000 IPs




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

# Amazon VPC Network Address Usage

MULTIPLE VPCs

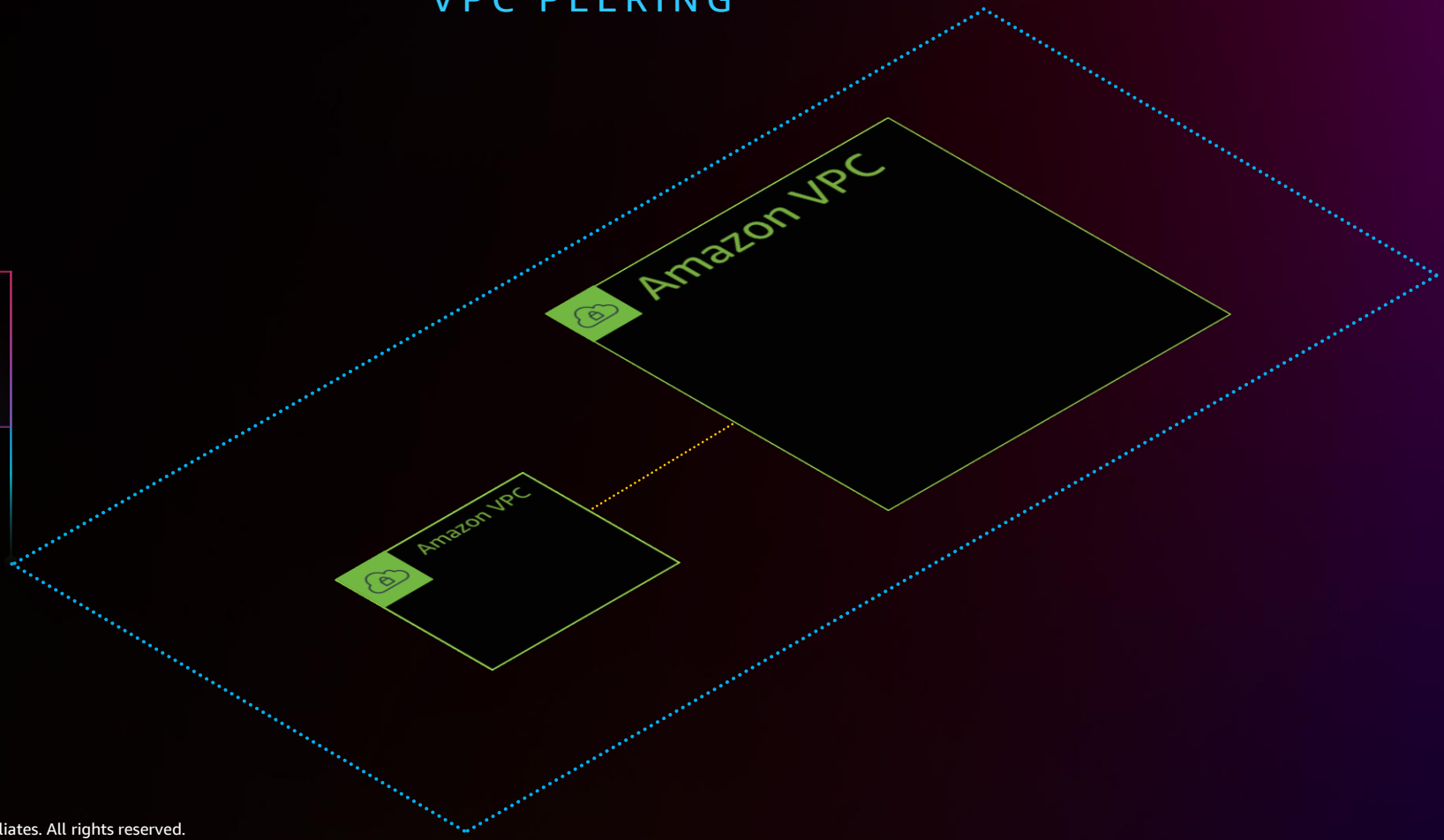



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon VPC Network Address Usage

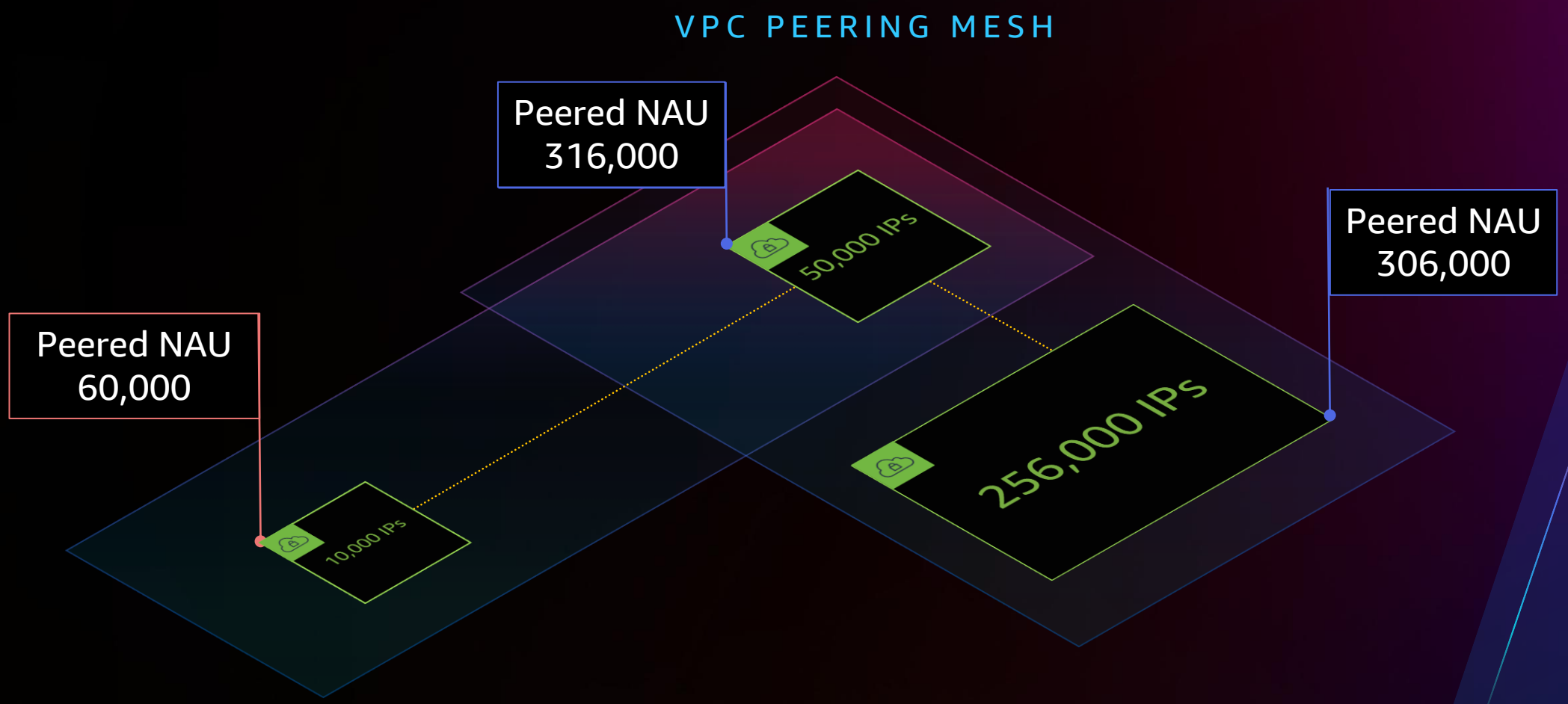
VPC PEERING

512,000 IPs




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

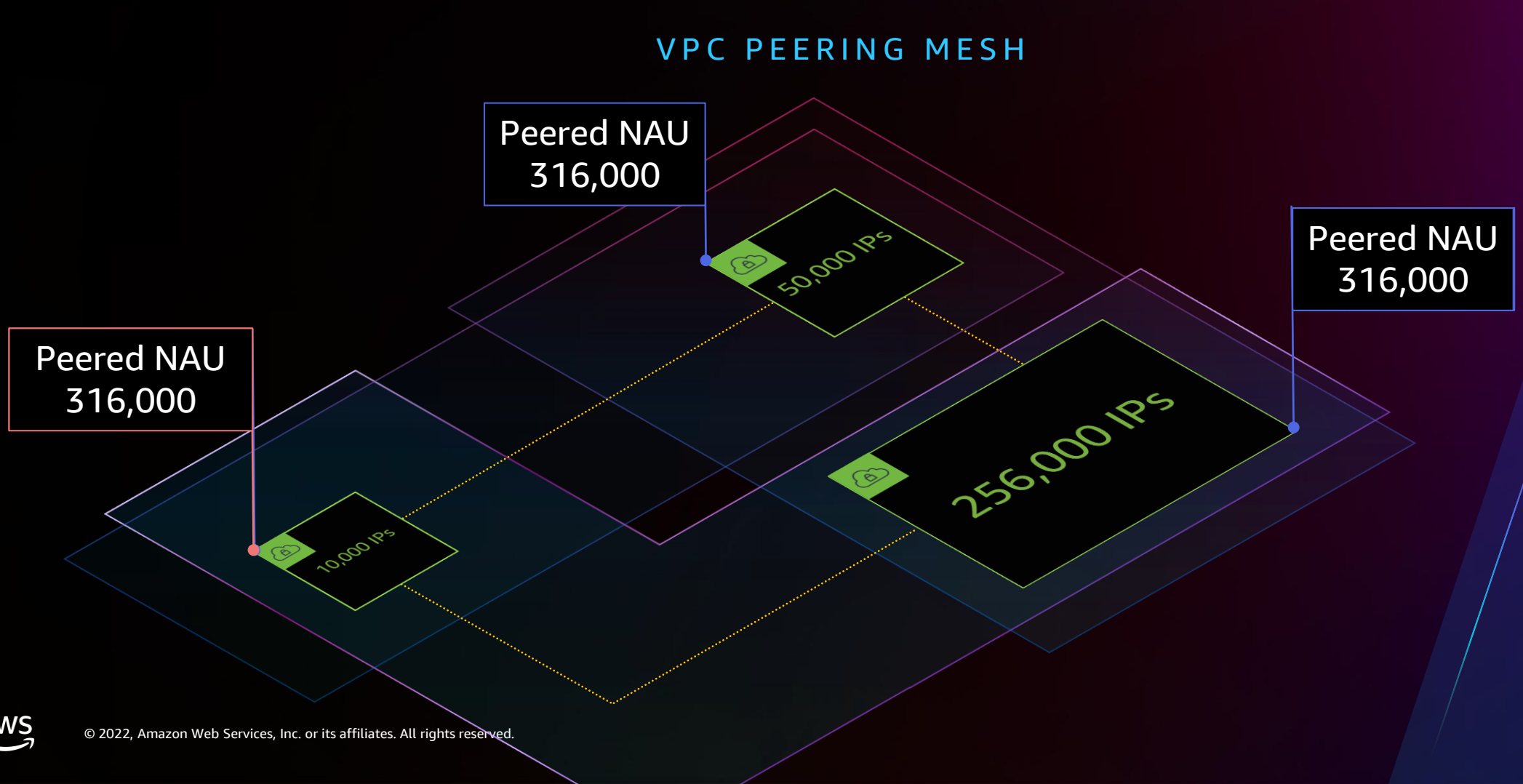
# Amazon VPC Network Address Usage




Partial mesh

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

# Amazon VPC Network Address Usage



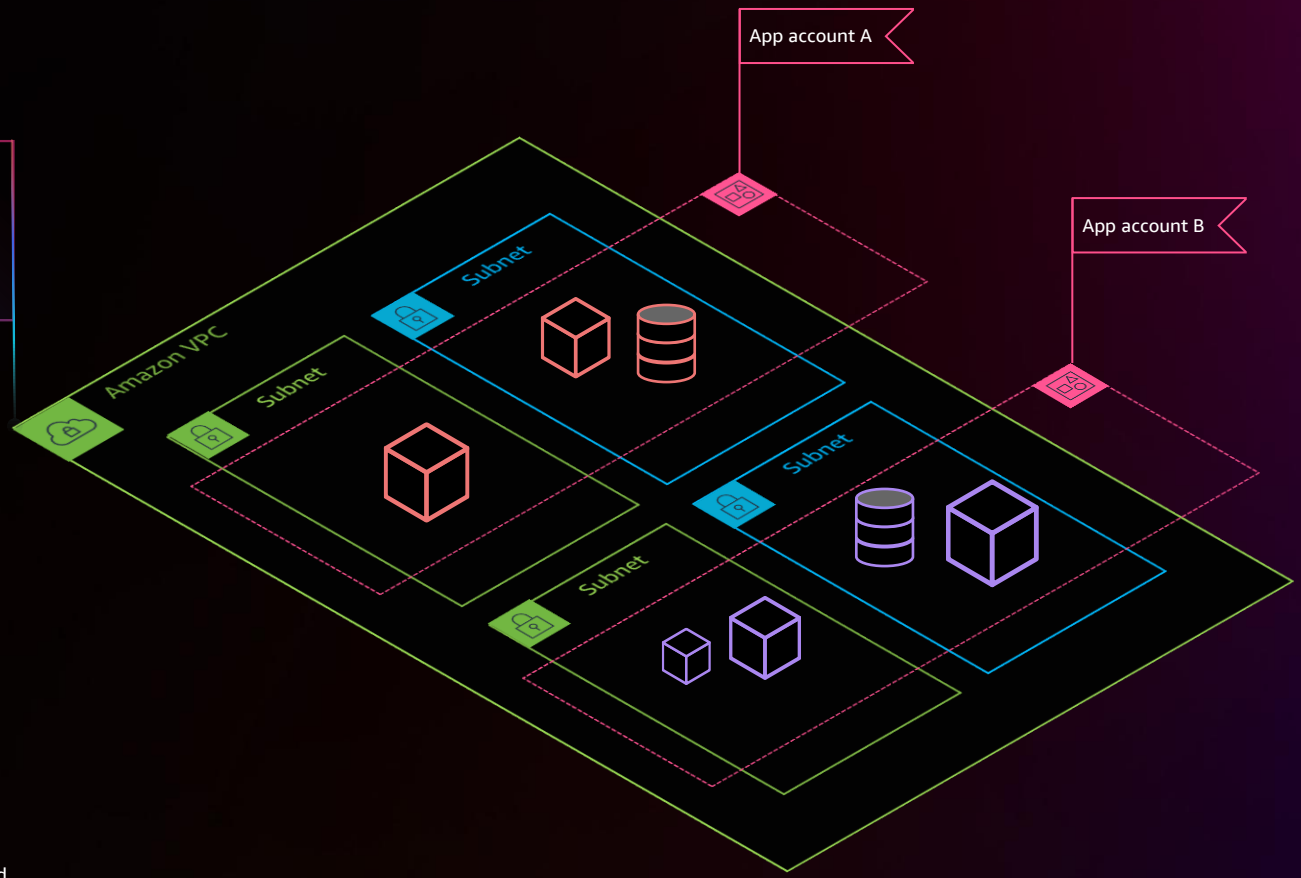

Full mesh

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

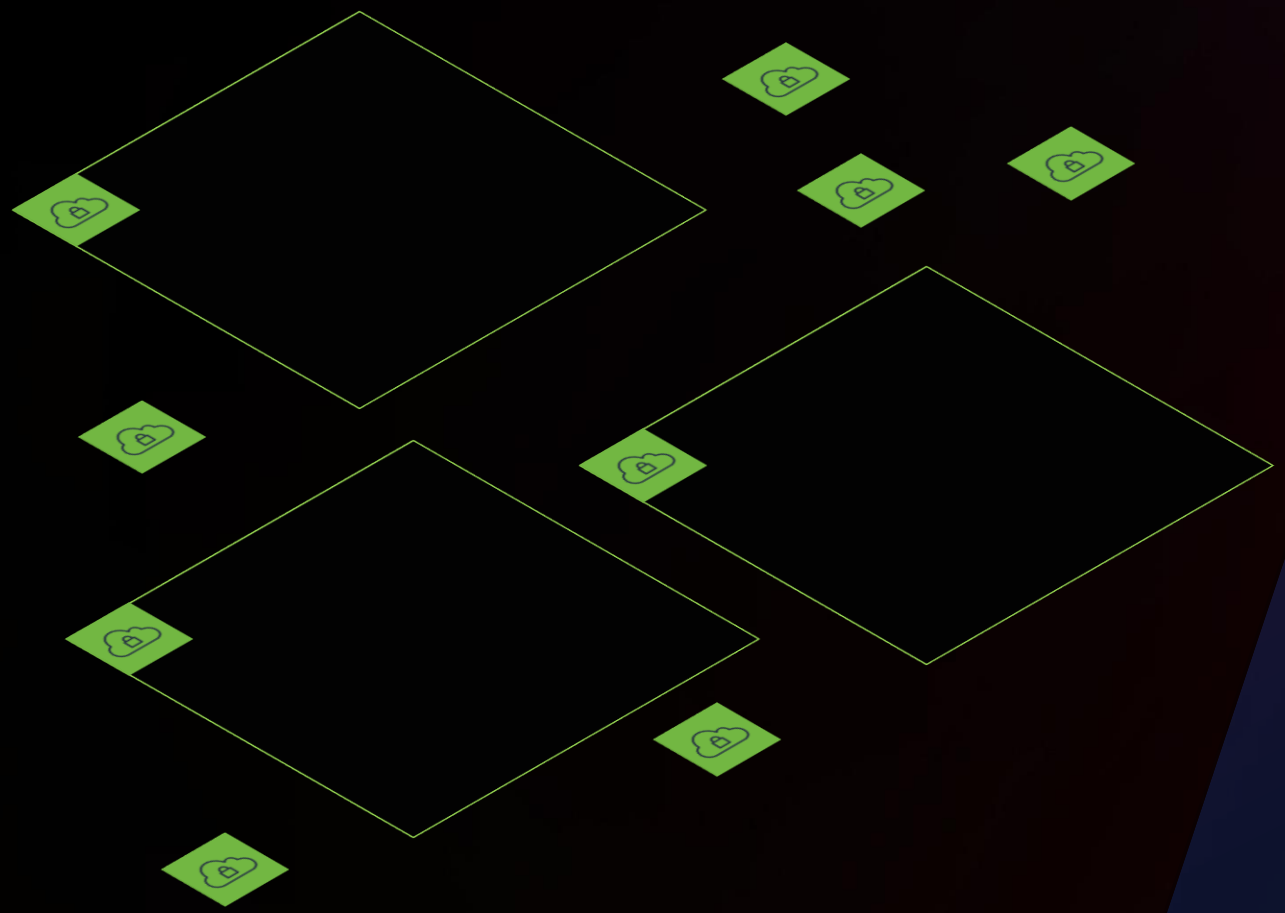
# Amazon VPC Network Address Usage

## VPC SHARING

256,000 IPs




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

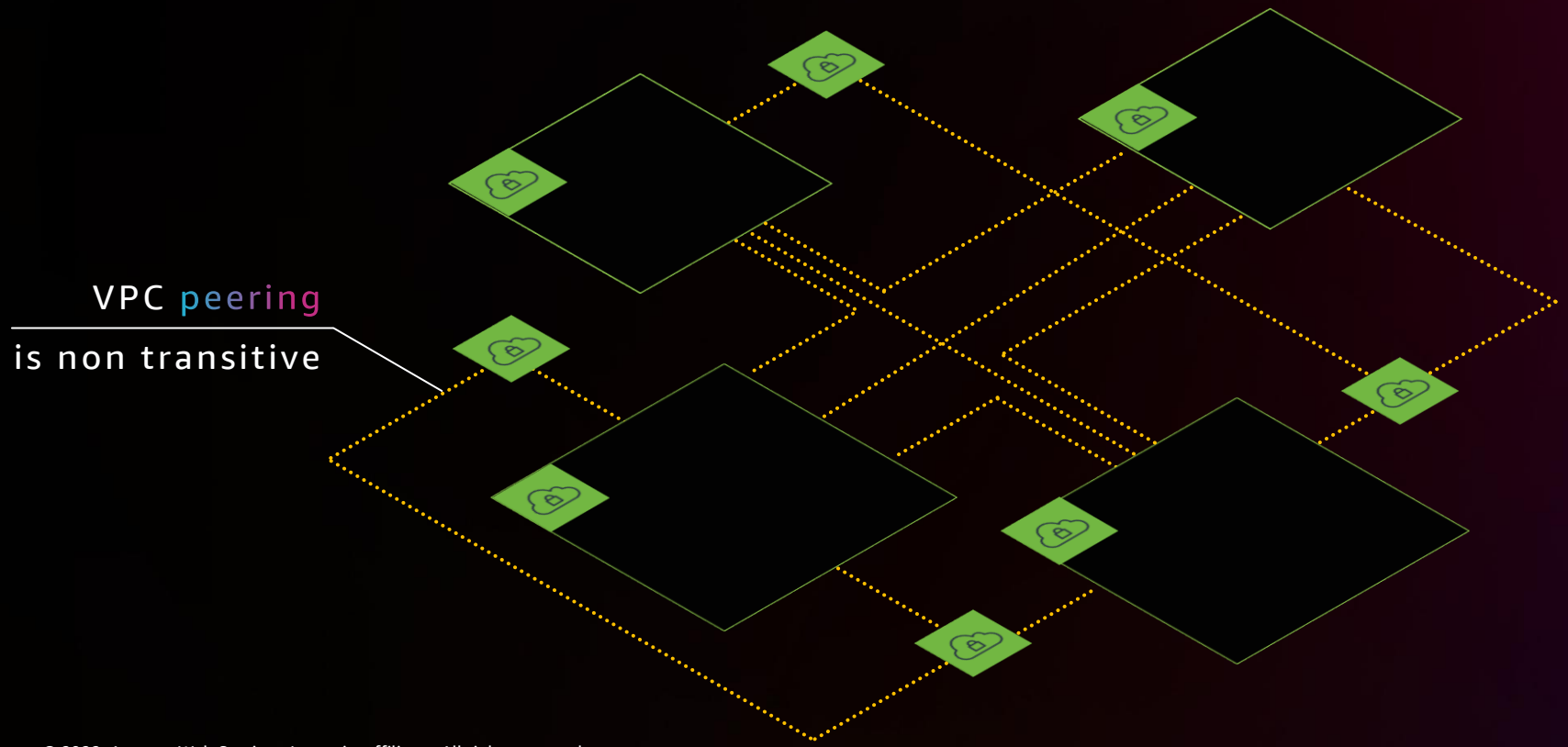


# Amazon VPC
## scaling out

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

# VPC Peering

SMALL SCALE

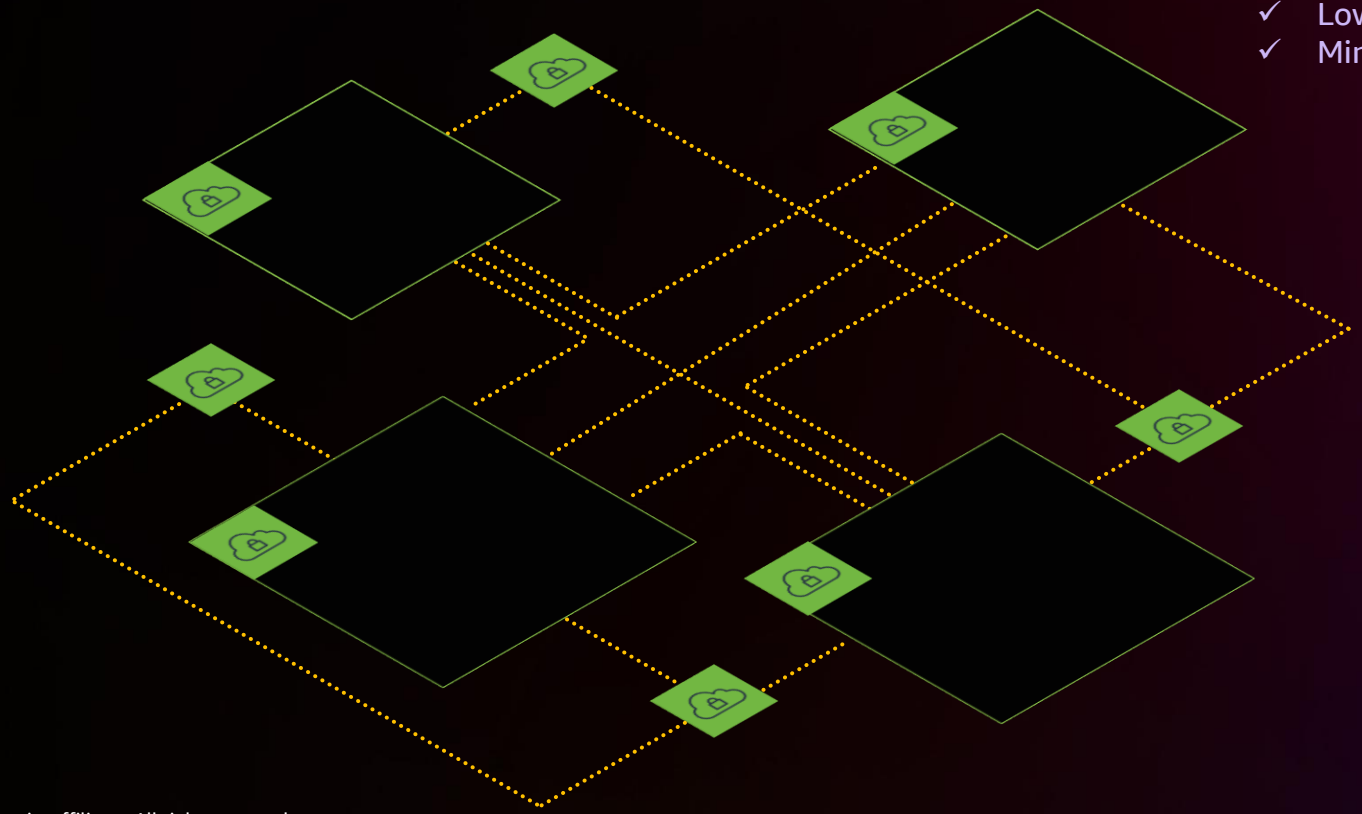



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# VPC Peering

## USE CASES

- ✓ High throughput
- ✓ Low latency
- ✓ Minimize data transfer costs

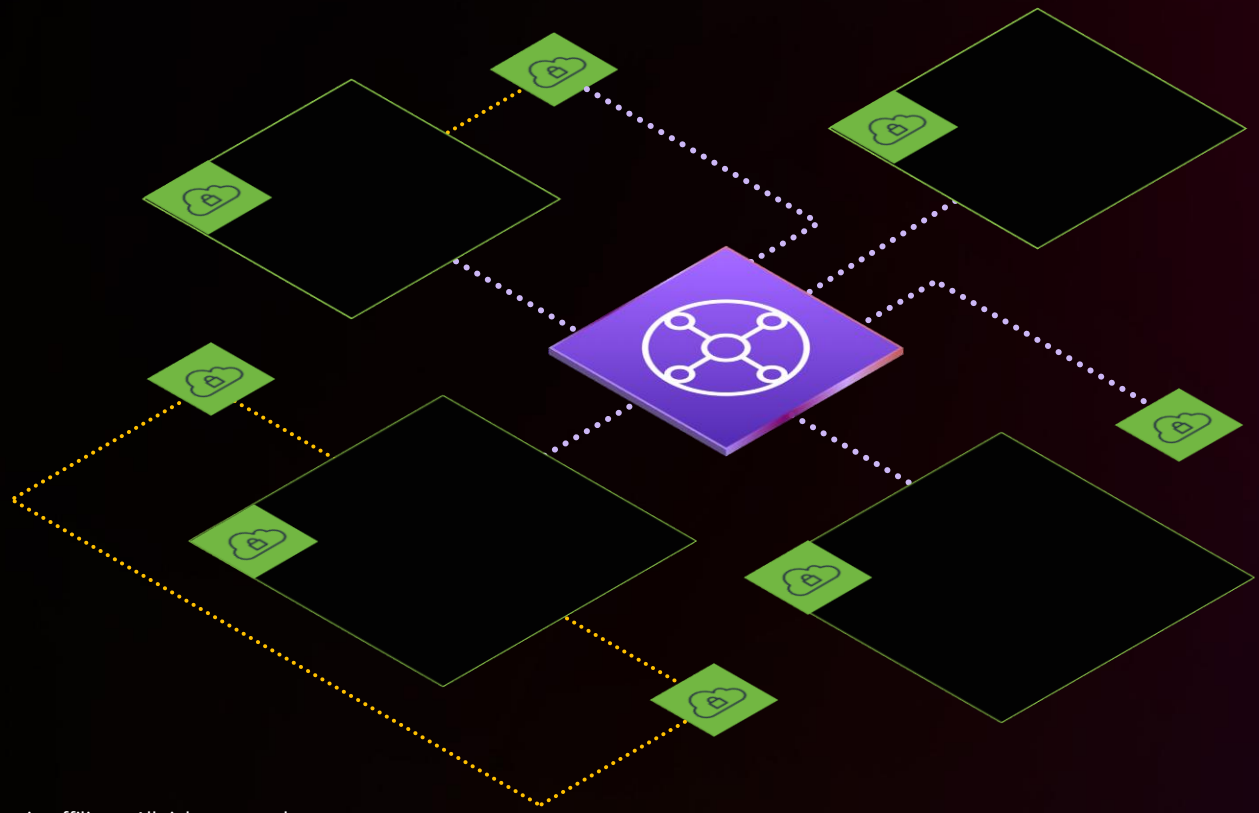


Pretty crowded

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

# AWS Transit Gateway

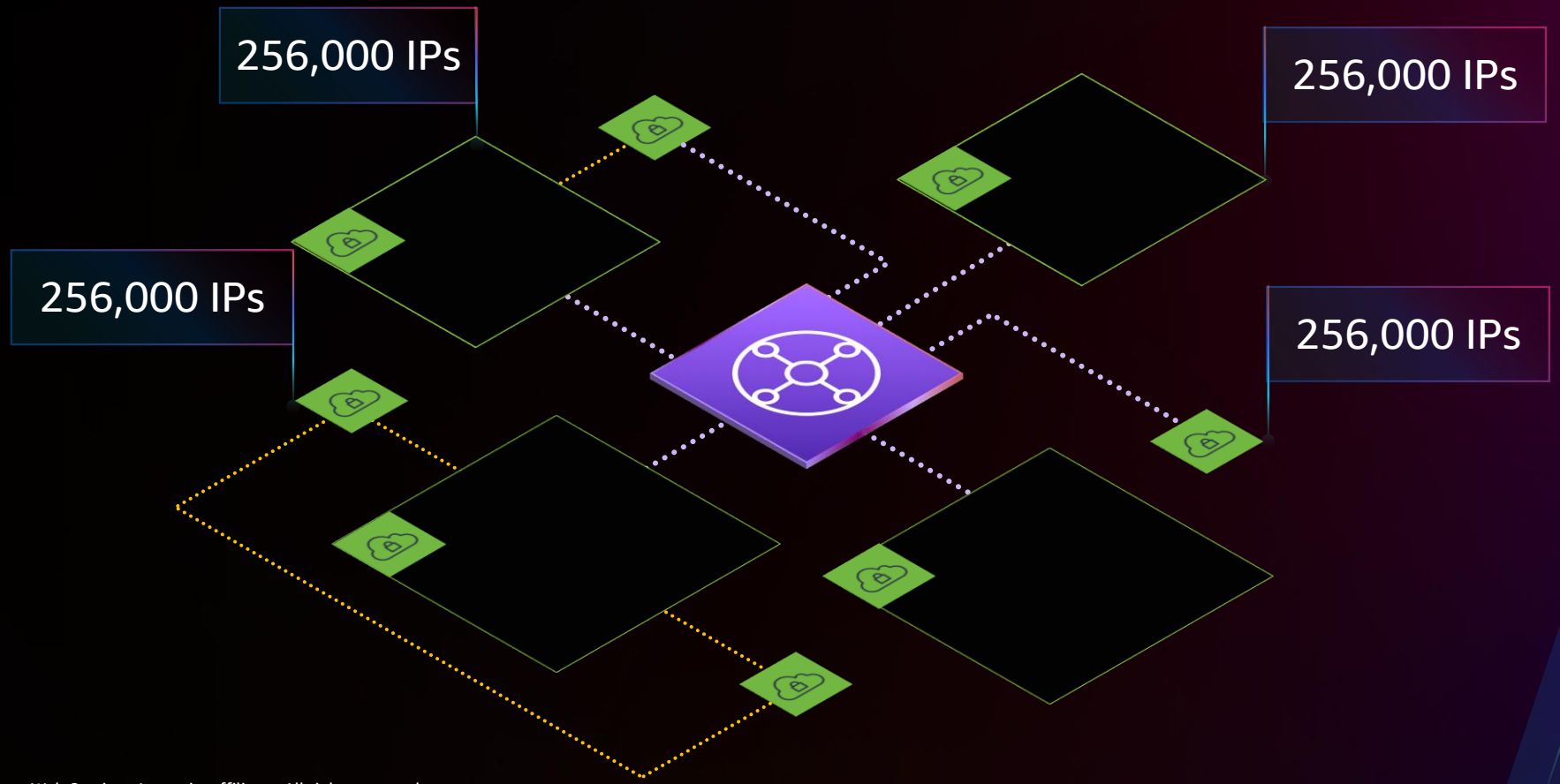
## VPC CONNECTIVITY AT SCALE



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

# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE

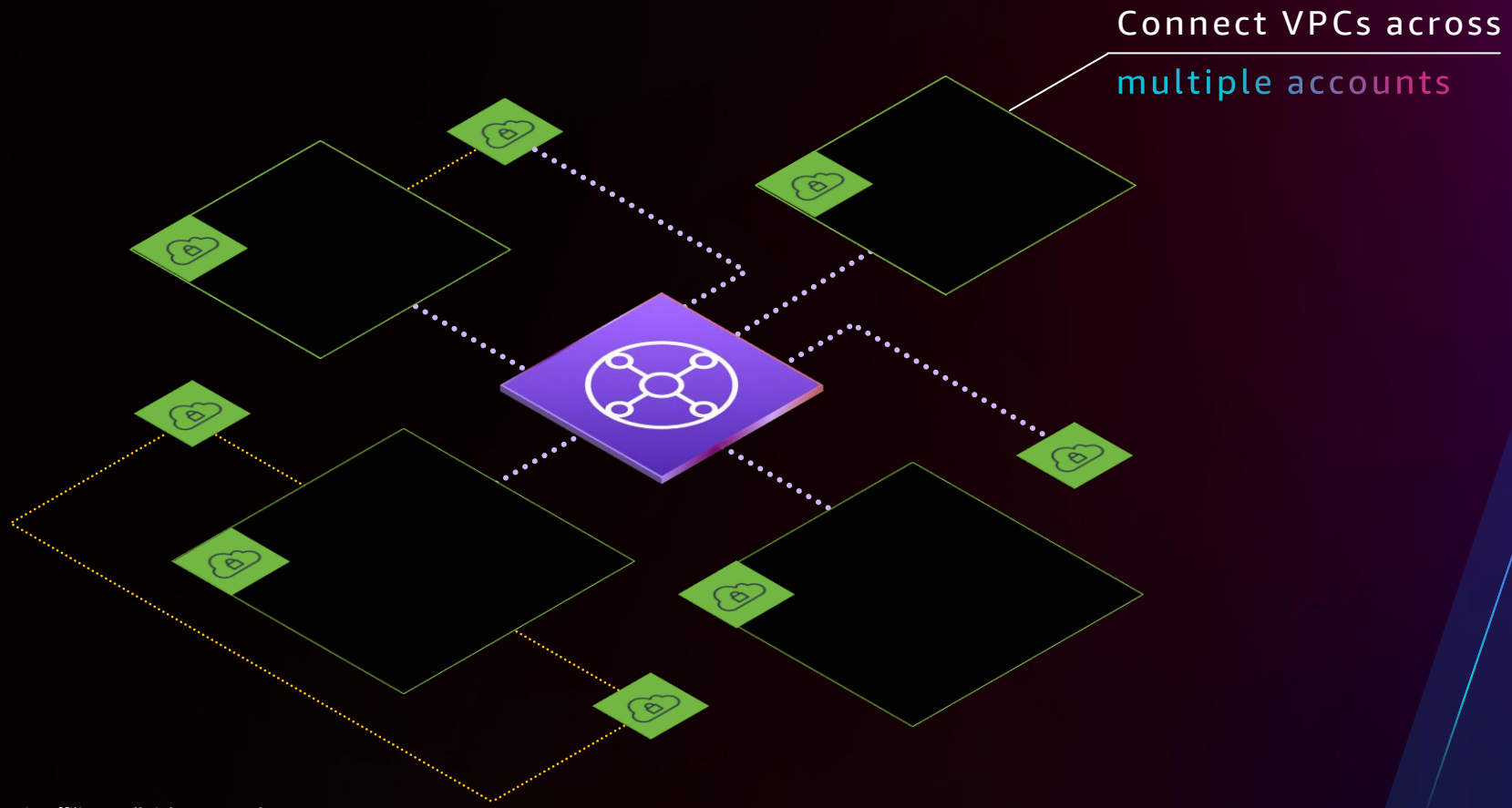



Network
Address Usage

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

# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE




Use cases

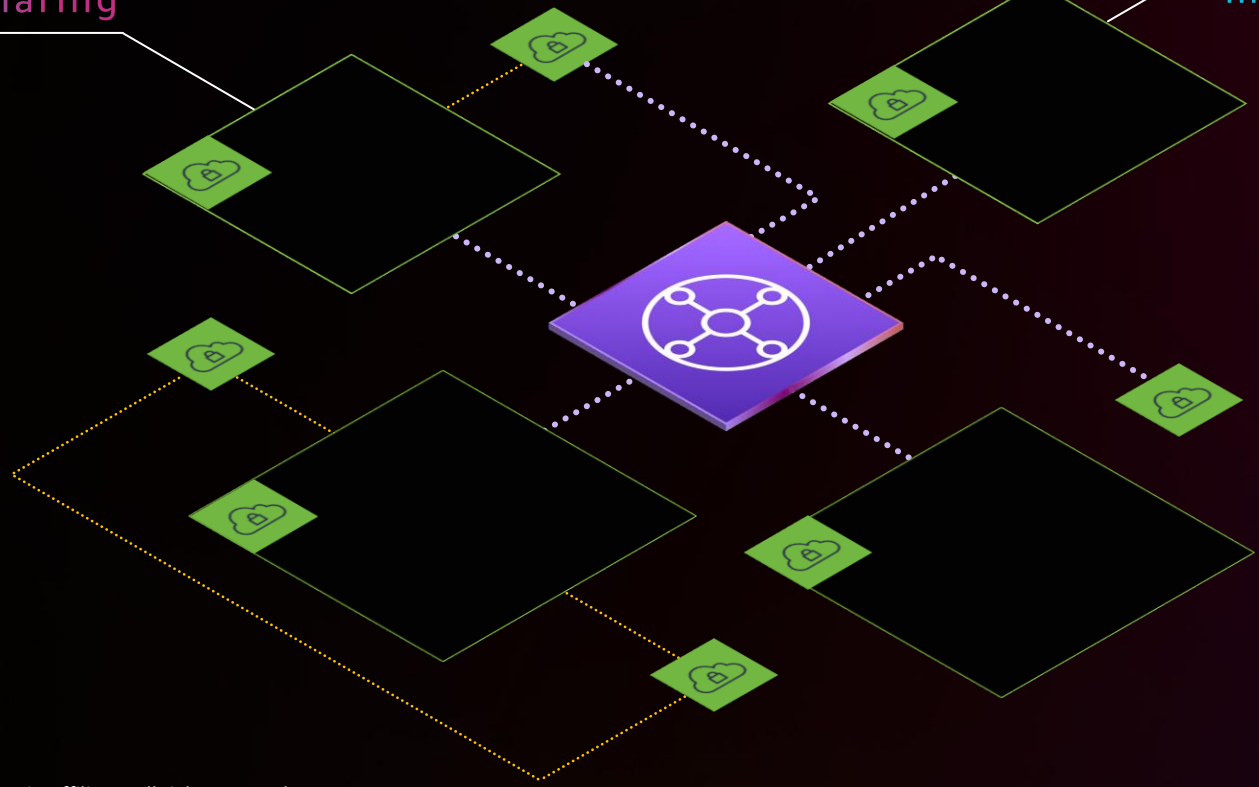
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE

Works with VPC sharing

Connect VPCs across multiple accounts



Use cases

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

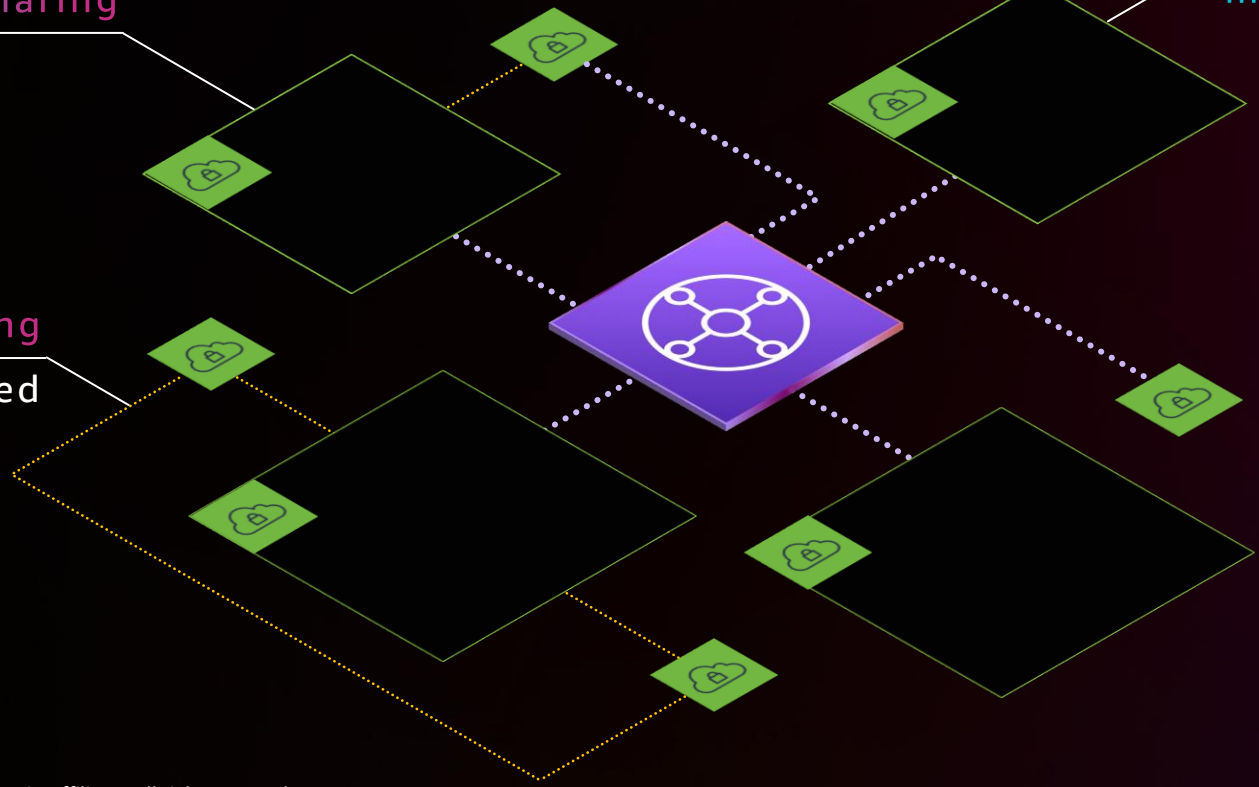
# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE

Works with VPC sharing

Connect VPCs across multiple accounts

VPC Peering is also supported



Use cases

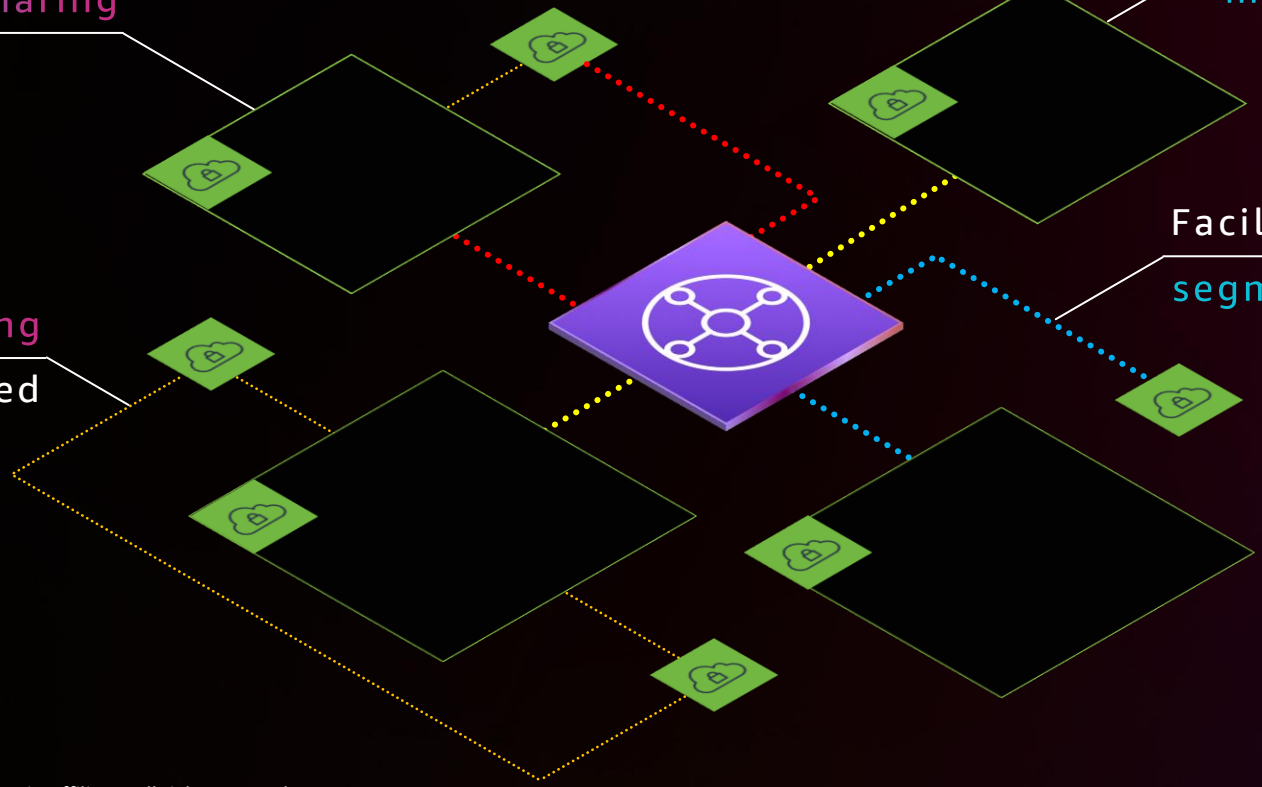
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE

Works with VPC sharing

Connect VPCs across multiple accounts



Facilitates network-level segmentation

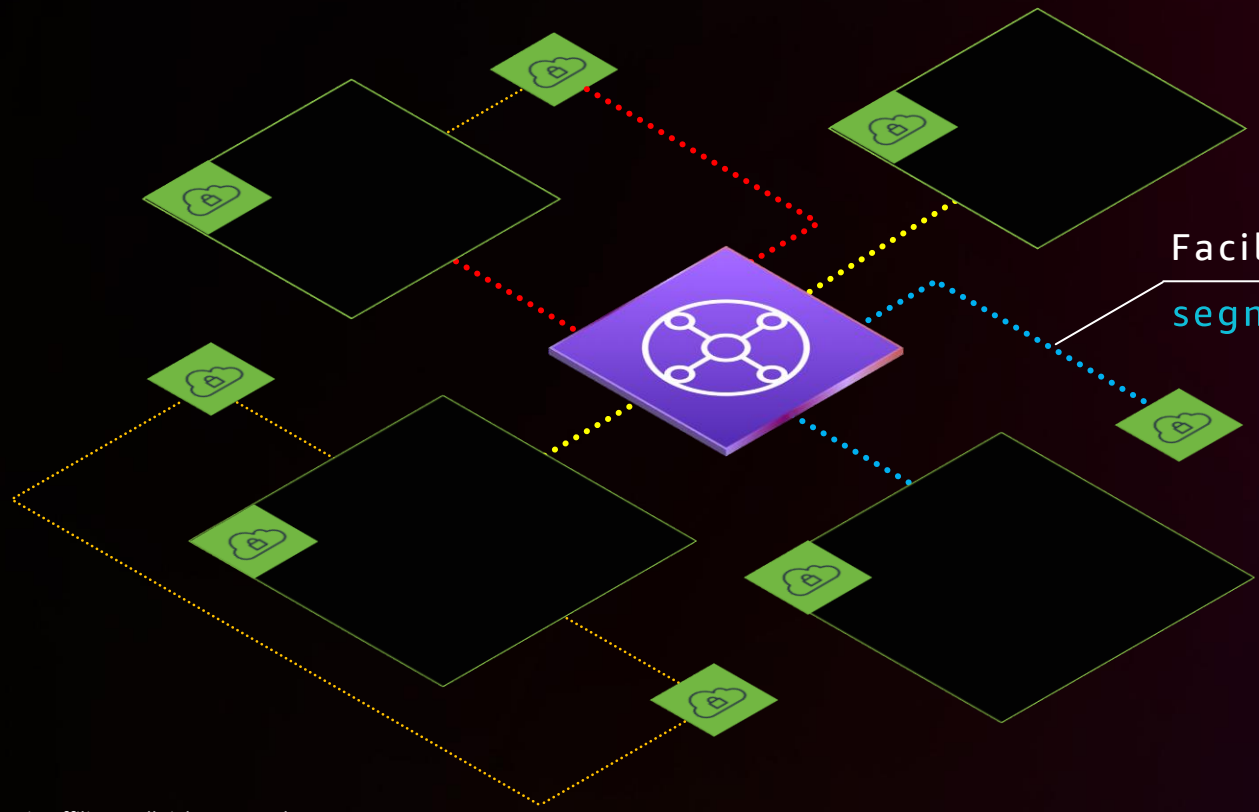
VPC Peering is also supported

Use cases

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

# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE



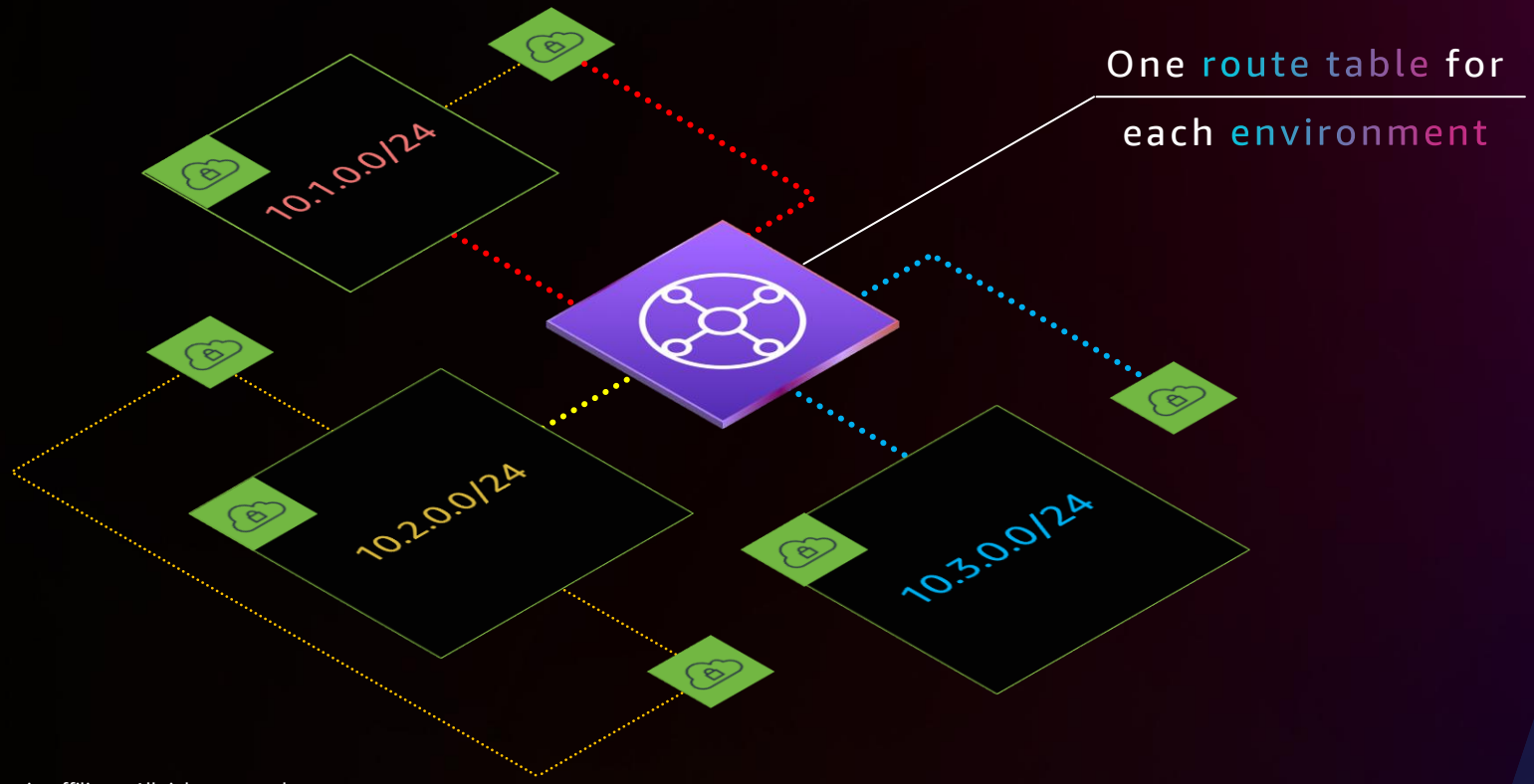
Facilitates network-level segmentation

Use cases

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

# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE

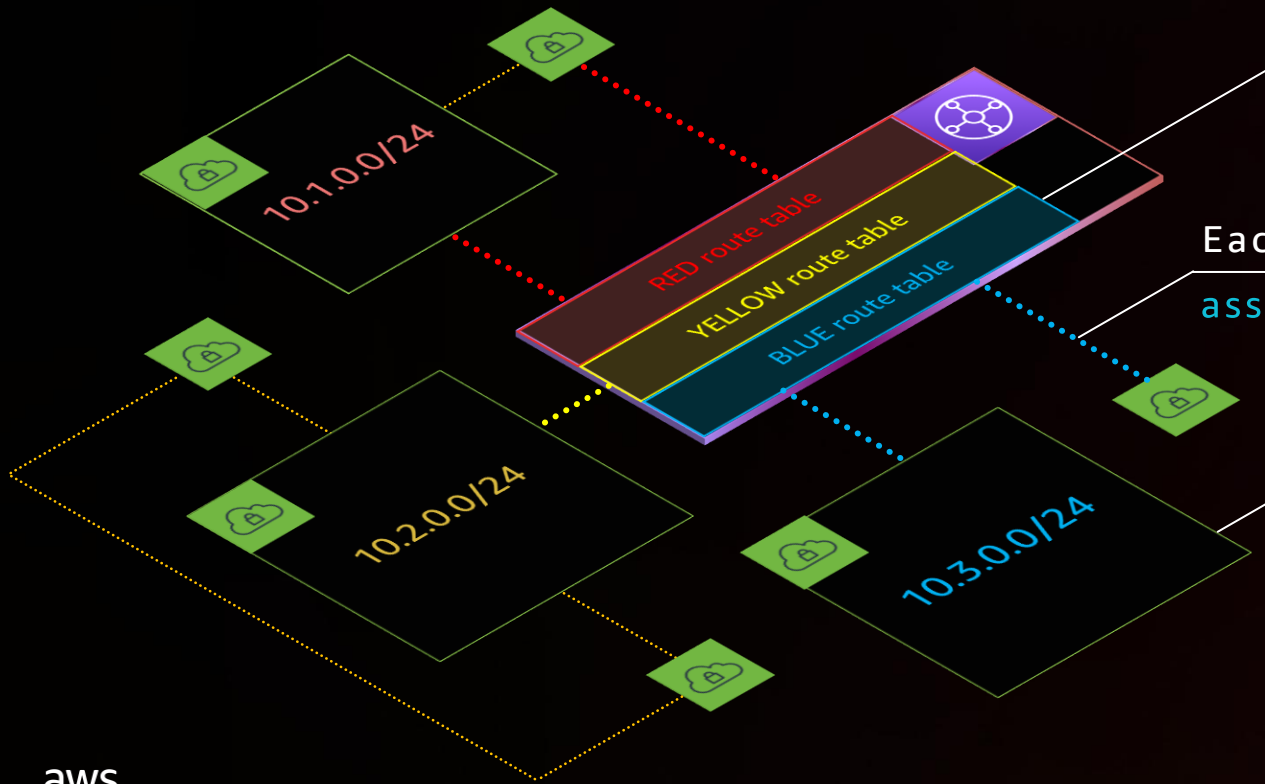



Routing detail

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

# AWS Transit Gateway

## VPC CONNECTIVITY AT SCALE




Attachments are propagated to the correct route tables

Each VPC attachment is associated to a route table

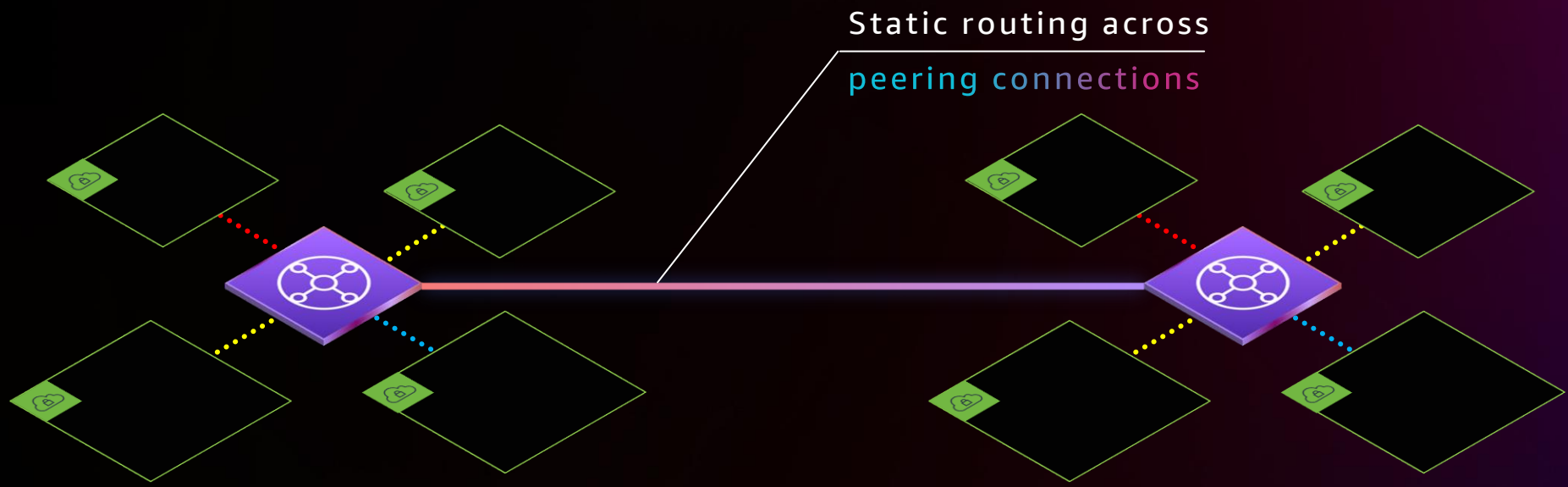
Each VPC route table needs to have routes to the TGW

Routing detail

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

# AWS Transit Gateway

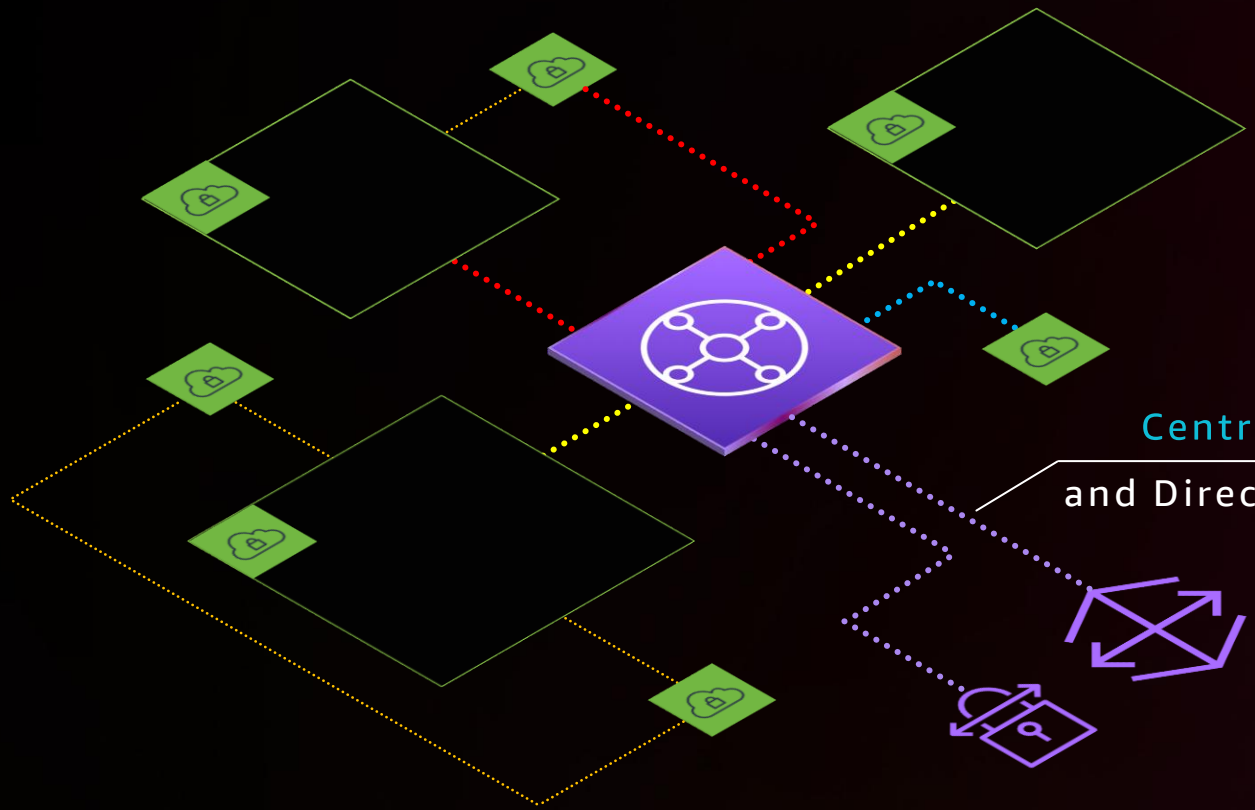
## MULTI-REGION CONNECTIVITY




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

# AWS Transit Gateway

## HYBRID CONNECTIVITY AT SCALE



Centralized Site-to-site VPN

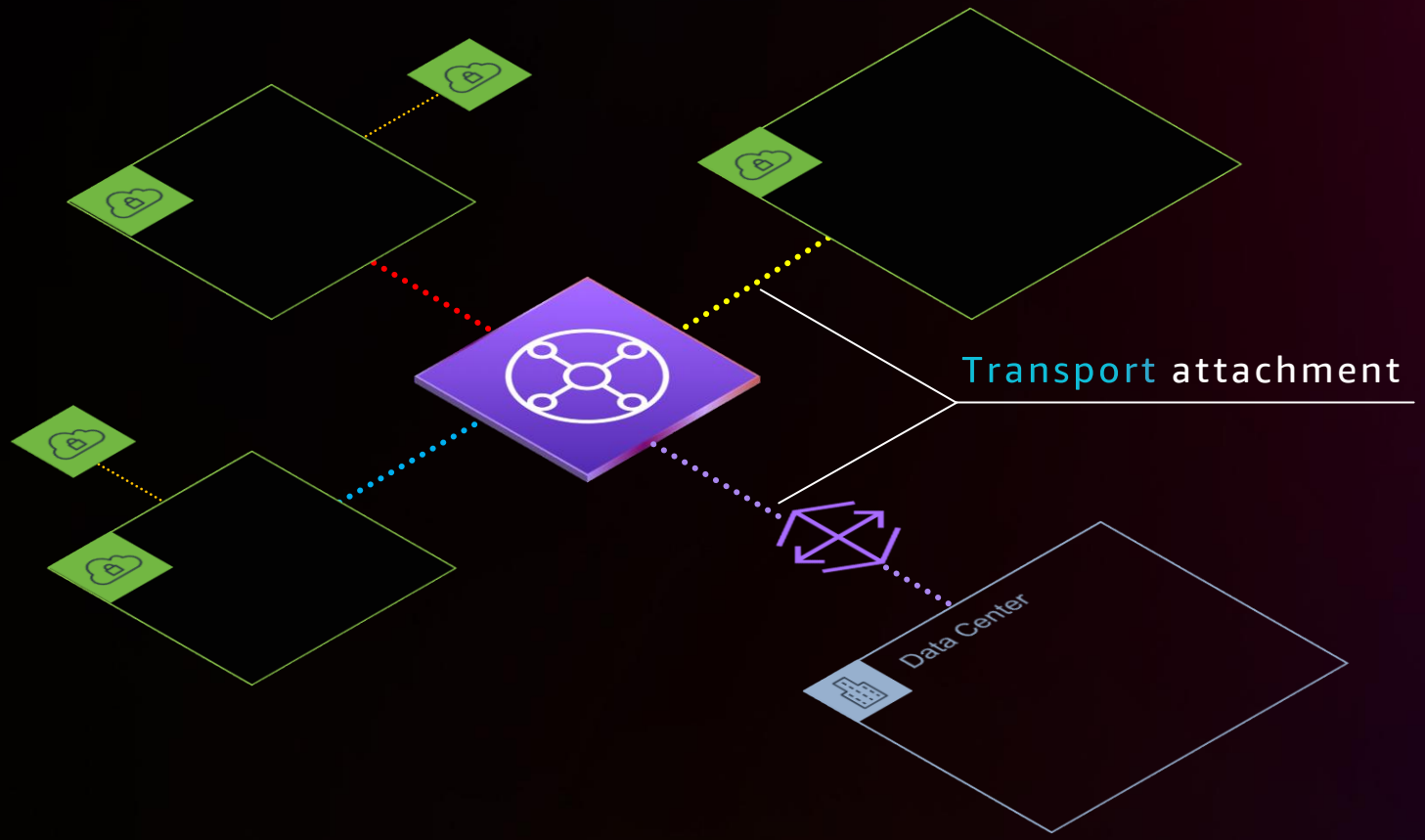
and Direct Connect connectivity

Use cases

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

# AWS Transit Gateway

## SD-WAN INTEGRATION WITH TGW CONNECT

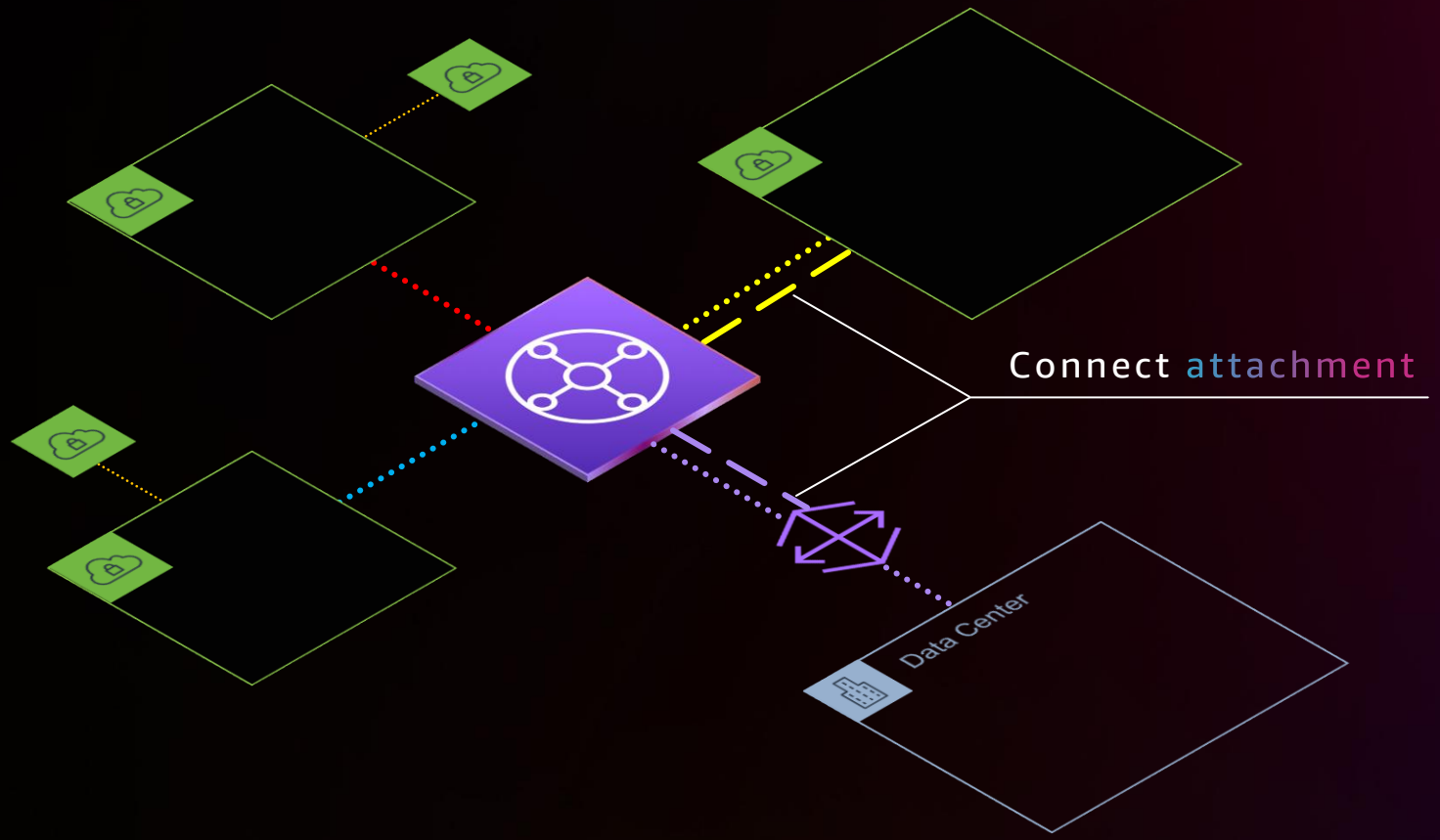



Use cases

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

# AWS Transit Gateway

## SD-WAN INTEGRATION WITH TGW CONNECT

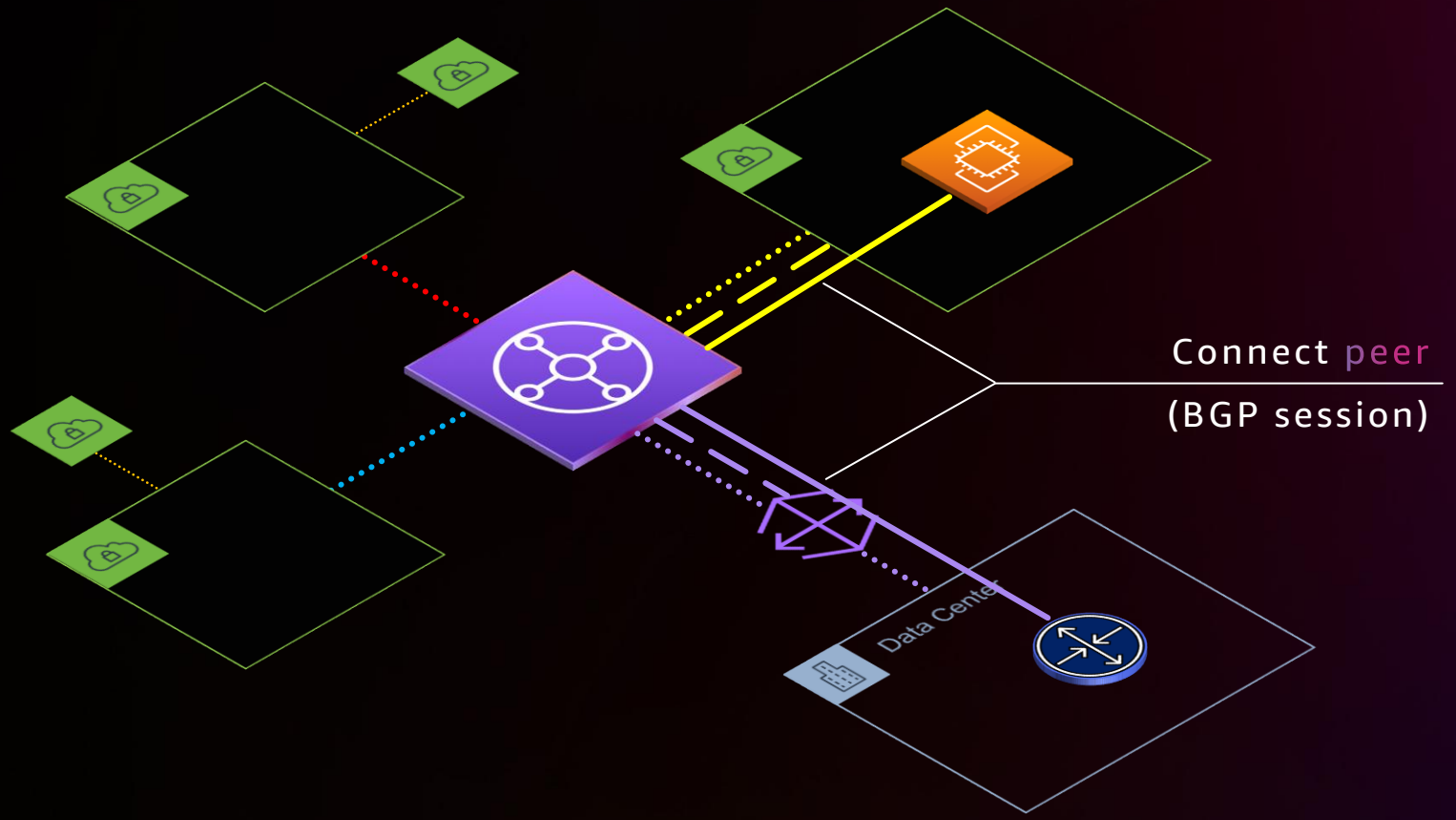



Use cases

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

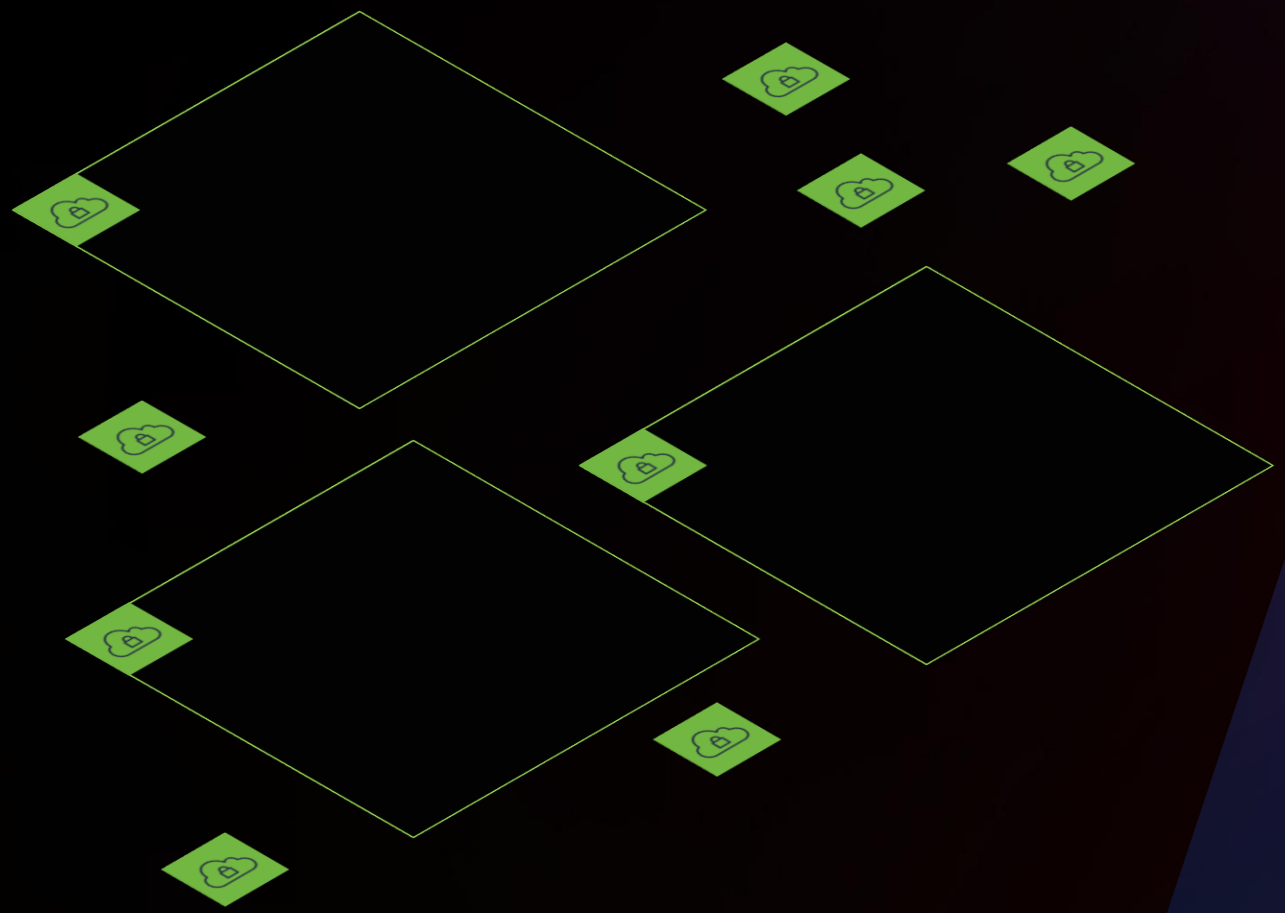
# AWS Transit Gateway

## SD-WAN INTEGRATION WITH TGW CONNECT




Use cases

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



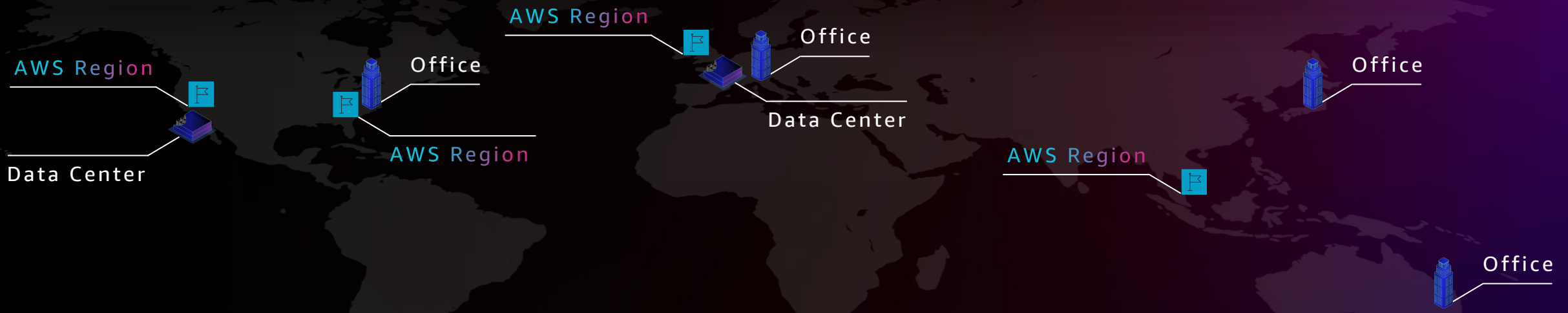
# Amazon VPC

## Build global networks

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

# AWS Cloud WAN

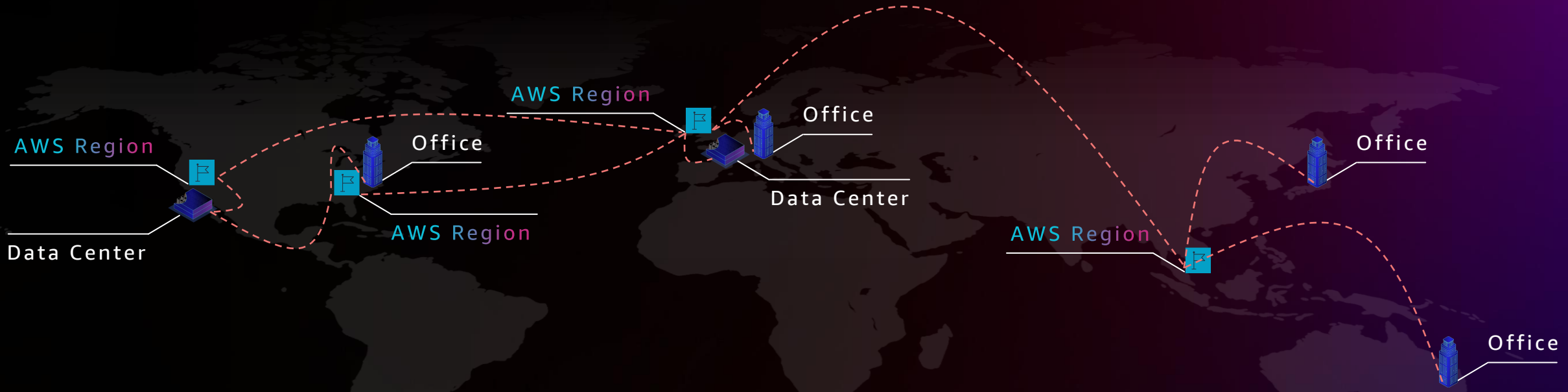
## BUILD GLOBAL NETWORKS ON AWS




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

# AWS Cloud WAN

## BUILD GLOBAL NETWORKS ON AWS




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

# AWS Cloud WAN

## BUILD GLOBAL NETWORKS ON AWS



Use the AWS global network for hybrid connectivity



Simplify WAN deployments, monitoring, and visibility



Centralize traffic segmentation policy across Regions

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

# AWS Cloud WAN

## Components

### Core Network

The part of your global network managed by AWS, operating in the AWS Regions defined in your Core Network Policy document

### Core Network Policy

A single document that defines the global configuration of your Core Network

### Core Network Edge

The Regional connection point managed by AWS in each Region. Every Cloud WAN attachment connects to a Core Network Edge

### Segments

Dedicated routing domains (e.g. prod, dev, engineering, etc.)

### Attachments

Attachments are any connections or resources you want to add to your Core Network

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

# AWS Cloud WAN

## HOW IT WORKS

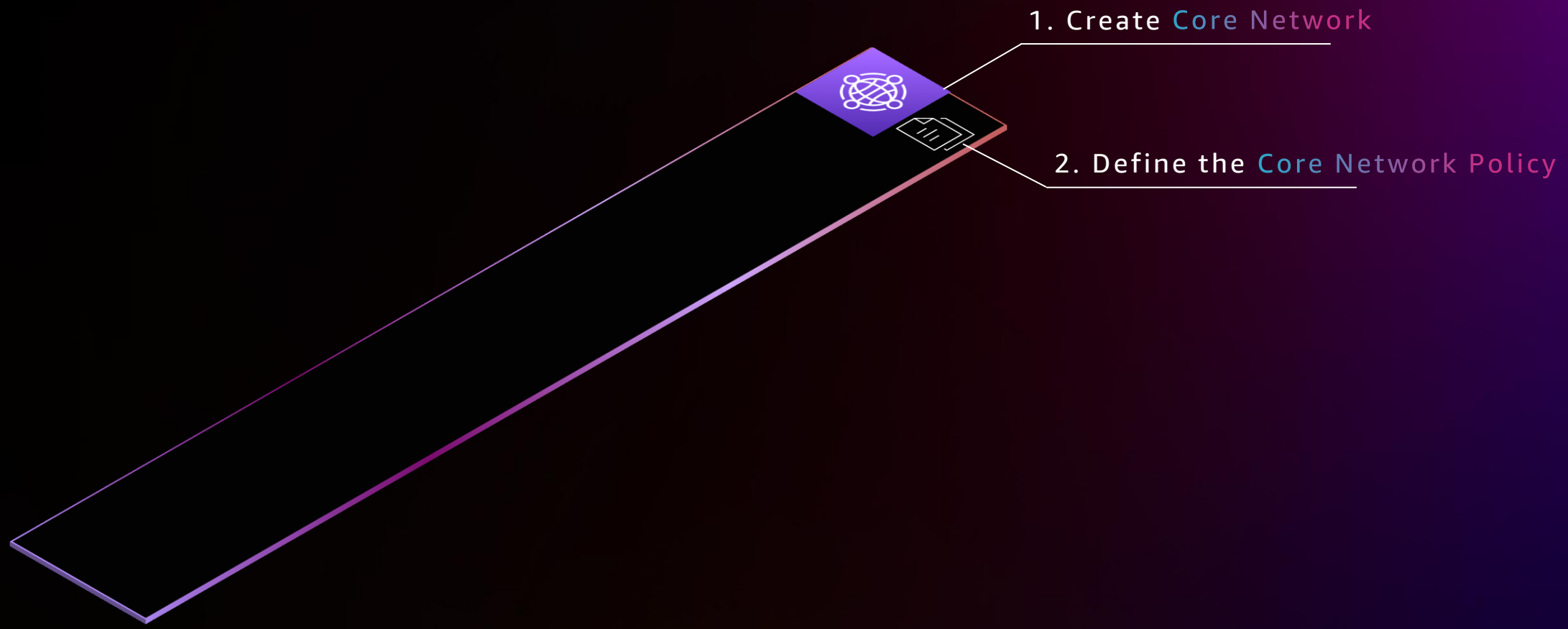
1. Create Core Network



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

# AWS Cloud WAN

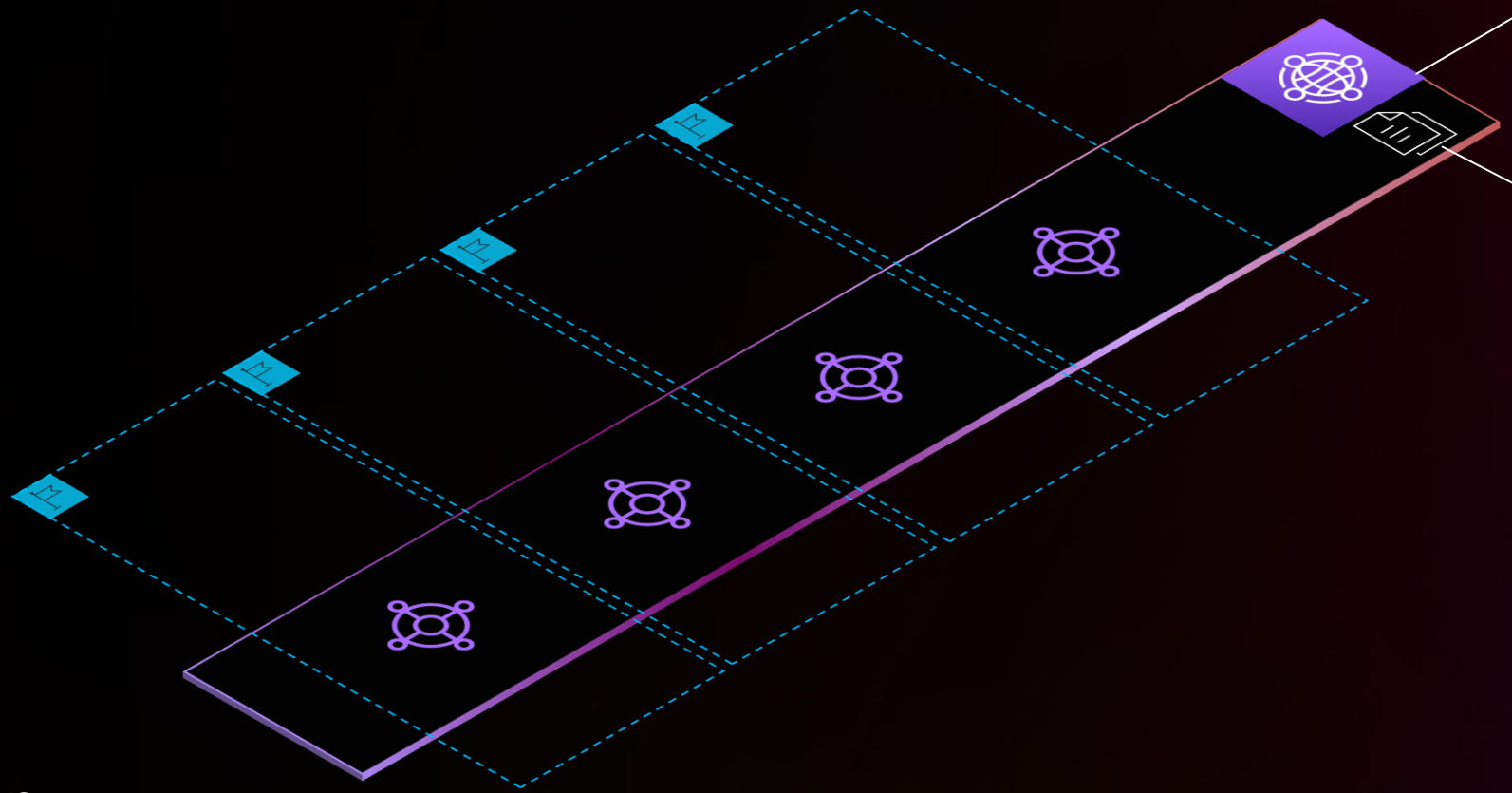
## HOW IT WORKS




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

# AWS Cloud WAN

## HOW IT WORKS



1. Create Core Network

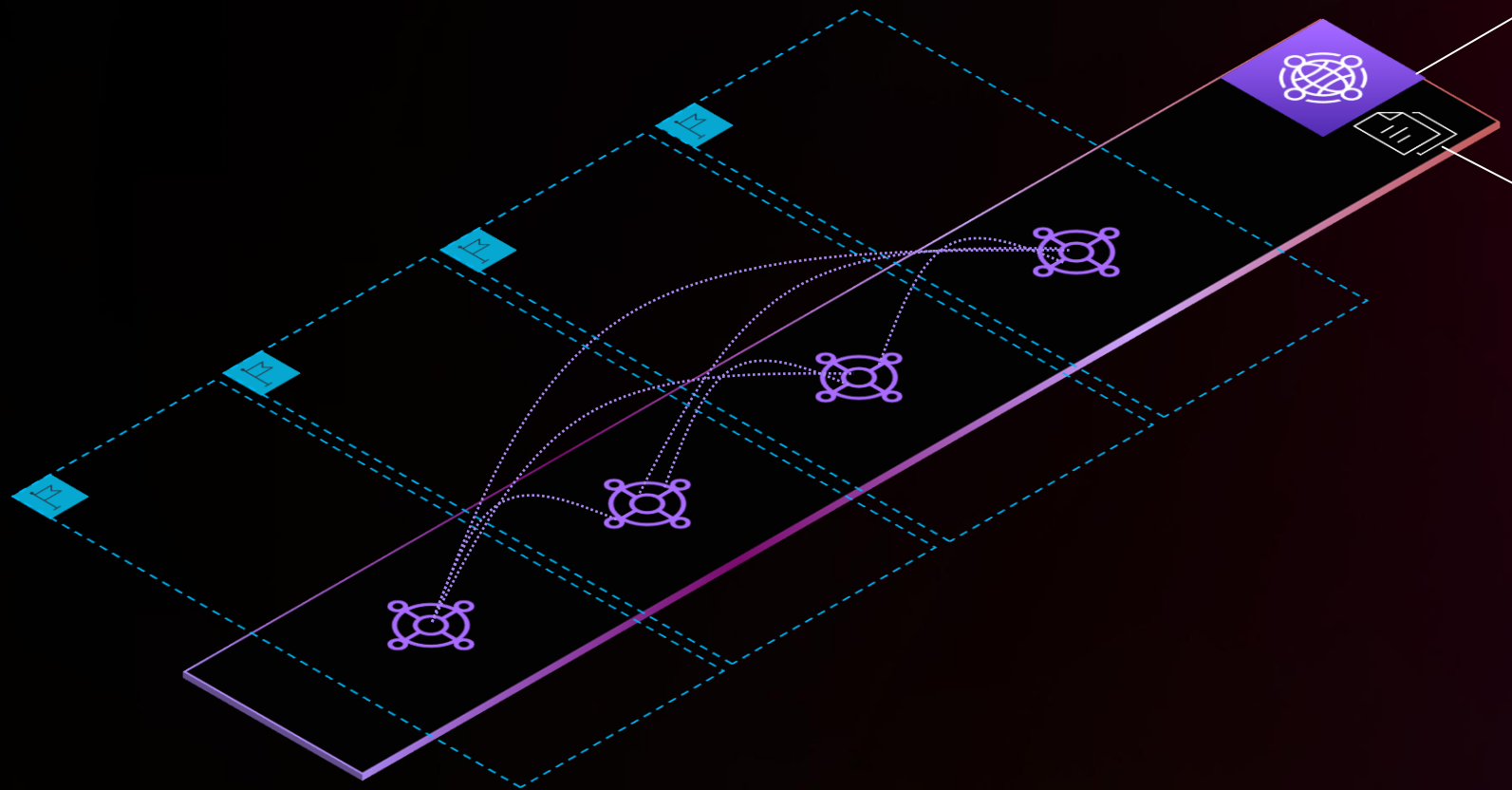
2. Define the Core Network Policy

- ✓ A Core Network Edge is created in each Region

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

# AWS Cloud WAN

## HOW IT WORKS



1. Create Core Network

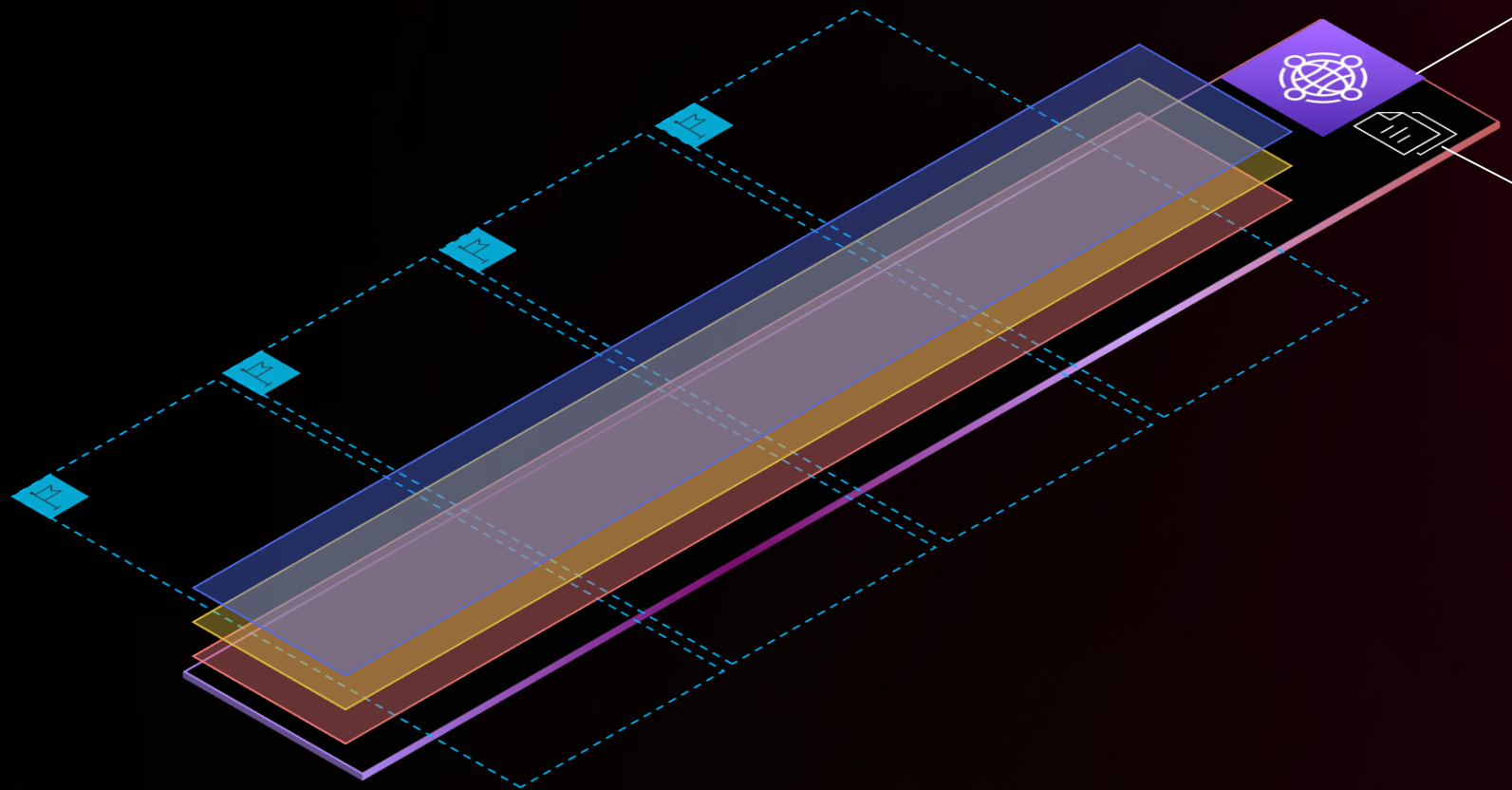
2. Define the Core Network Policy

- ✓ A Core Network Edge is created in each Region
- ✓ Peering connections and dynamic route propagation are fully managed

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

# AWS Cloud WAN

## HOW IT WORKS



### 1. Create Core Network

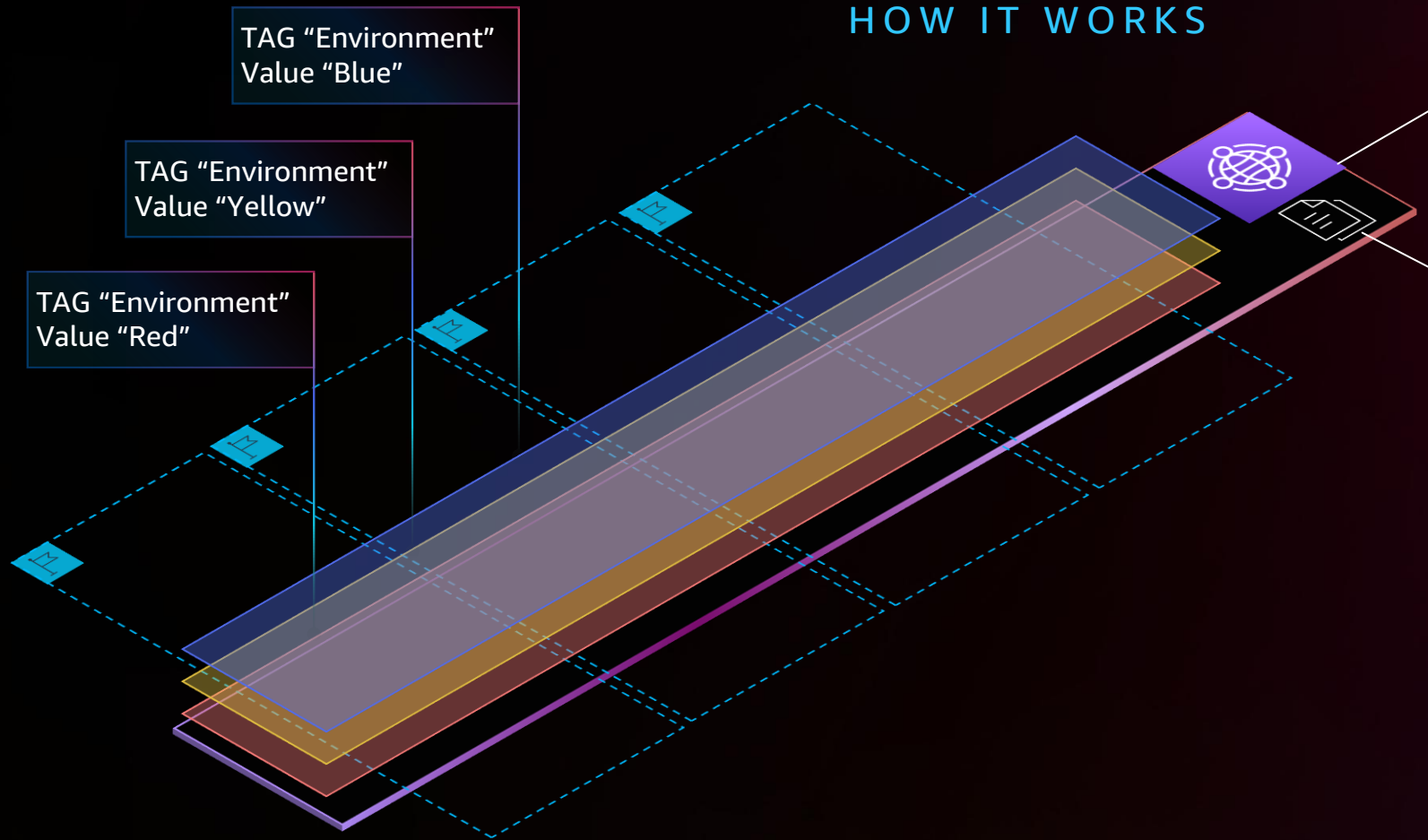
### 2. Define the Core Network Policy

- ✓ A Core Network Edge is created in each Region
- ✓ Peering connections and dynamic route propagation are fully managed
- ✓ Define Segments for end-to-end traffic segmentation across Regions

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

# AWS Cloud WAN

## HOW IT WORKS




### 1. Create Core Network

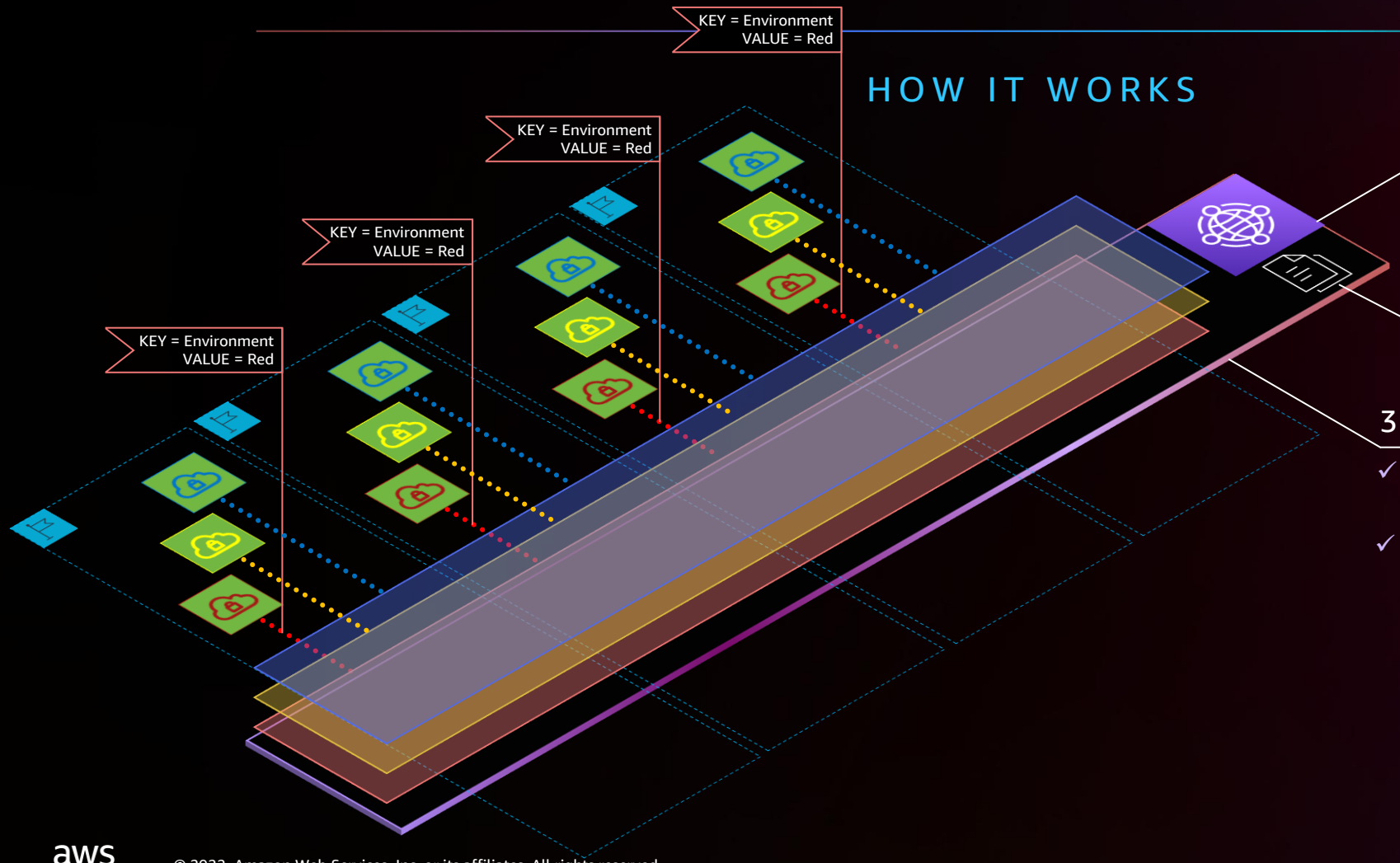
### 2. Define the Core Network Policy

- ✓ A Core Network Edge is created in each Region
- ✓ Peering connections and dynamic route propagation are fully managed
- ✓ Define Segments for end-to-end traffic segmentation across Regions
- ✓ Define policies for dynamic attachment-to-segment association and route propagation

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

# AWS Cloud WAN

## HOW IT WORKS




1. Create Core Network

2. Define the Core Network Policy

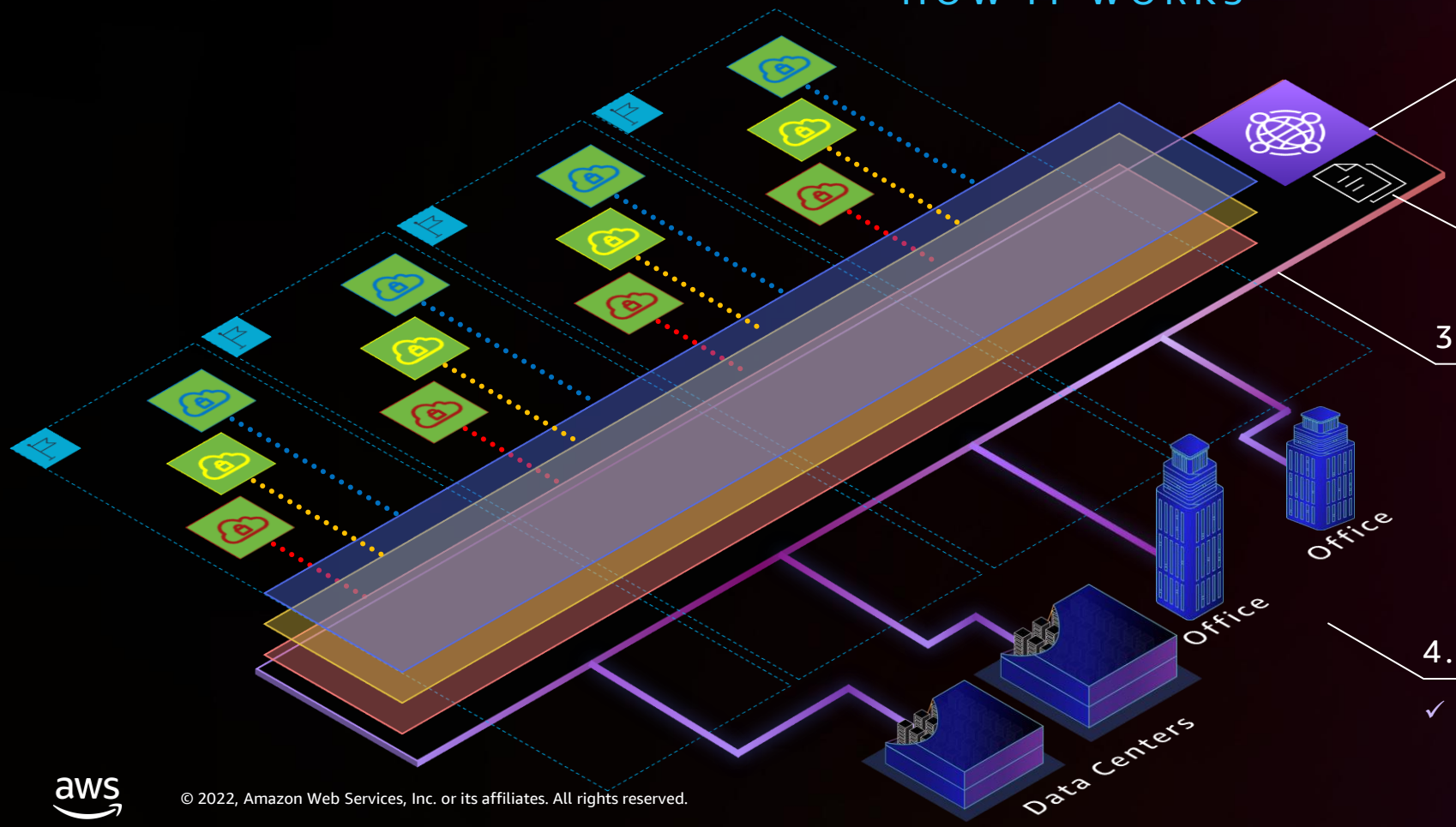
3. Create attachments with the right tags

- ✓ Attachments are automatically associated to Segments
- ✓ VPC CIDR blocks are added to the Segment route table

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

# AWS Cloud WAN

## HOW IT WORKS




1. Create Core Network

2. Define the Core Network Policy

3. Attach VPCs with the right Tags

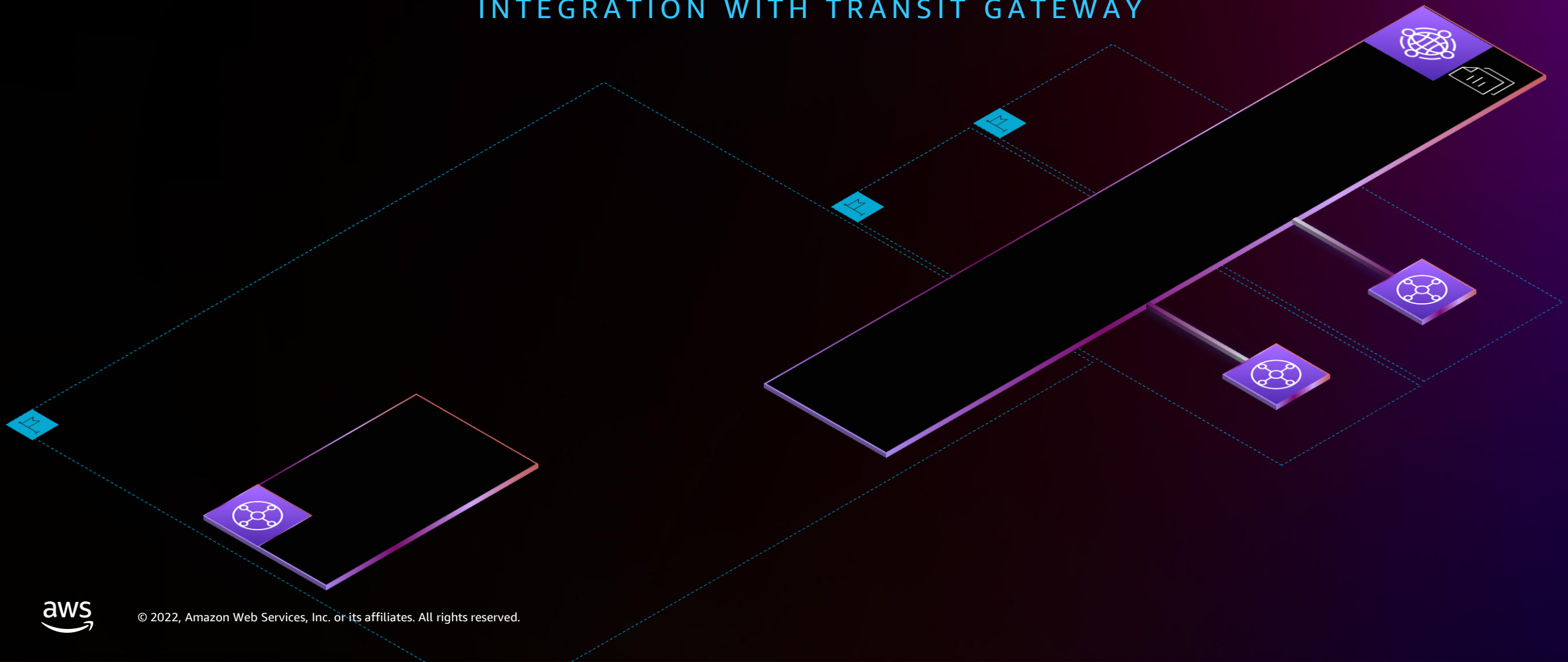
4. Centralize global hybrid connectivity

- ✓ Full dynamic routing support for hybrid connectivity integration

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

# AWS Cloud WAN

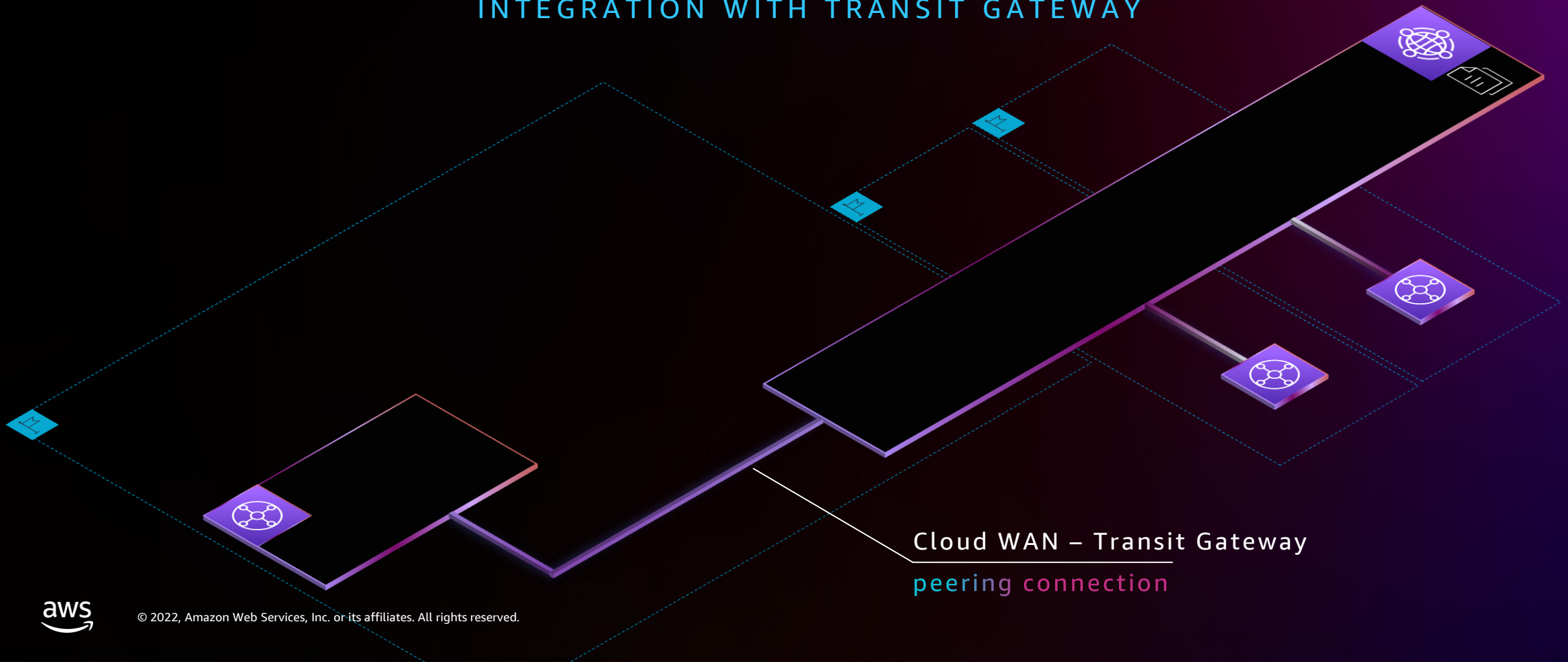
## INTEGRATION WITH TRANSIT GATEWAY



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

# AWS Cloud WAN

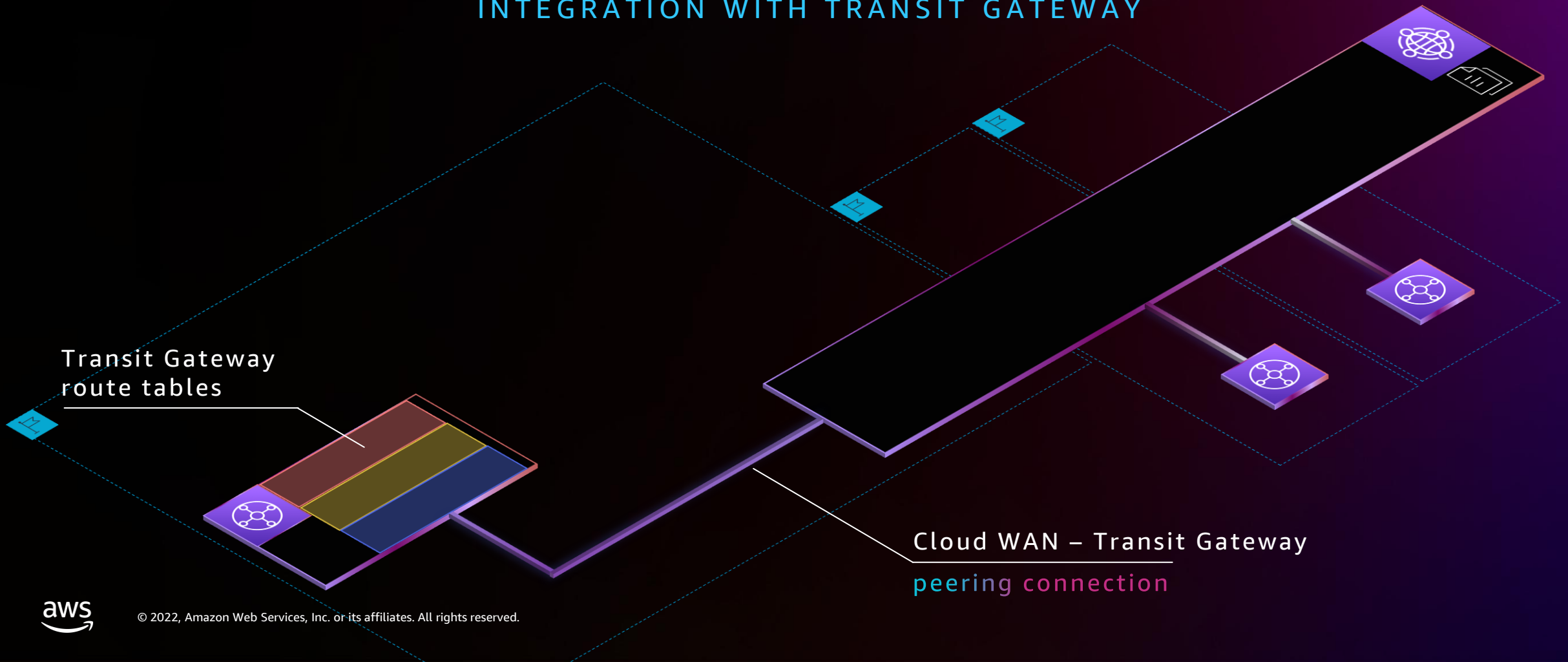
## INTEGRATION WITH TRANSIT GATEWAY




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

# AWS Cloud WAN

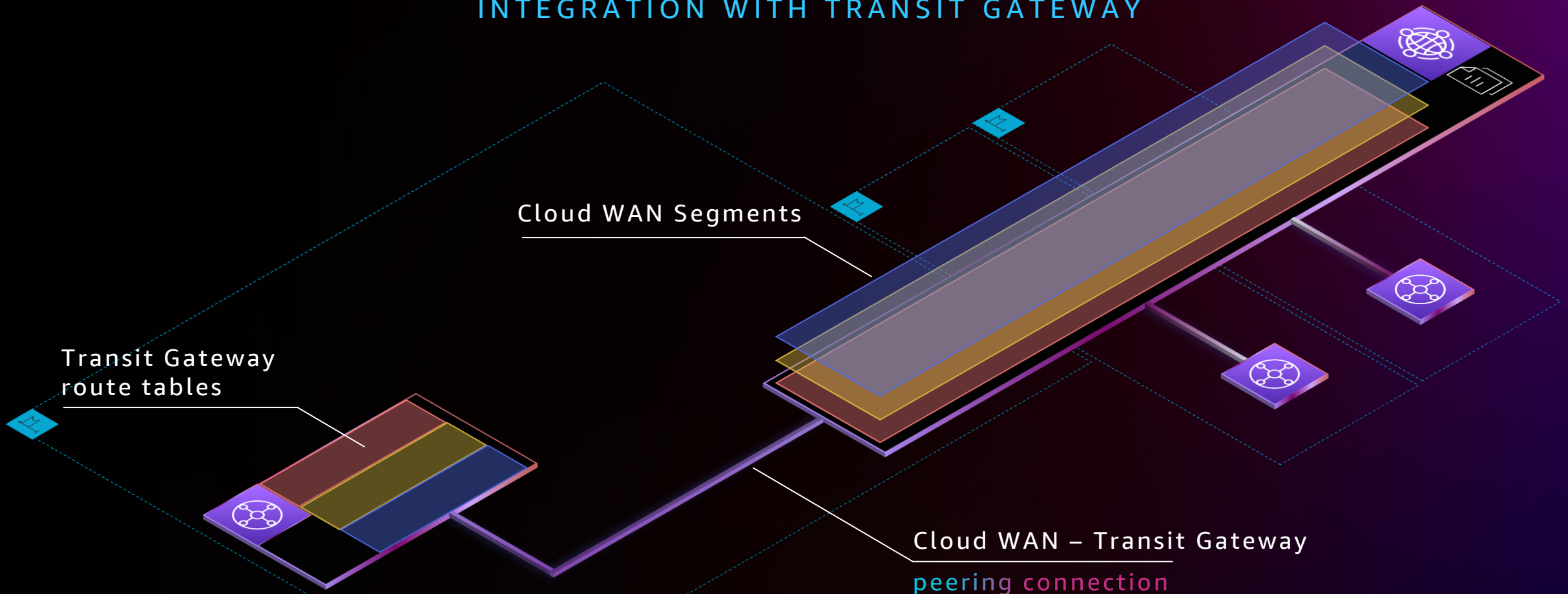
## INTEGRATION WITH TRANSIT GATEWAY




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

# AWS Cloud WAN

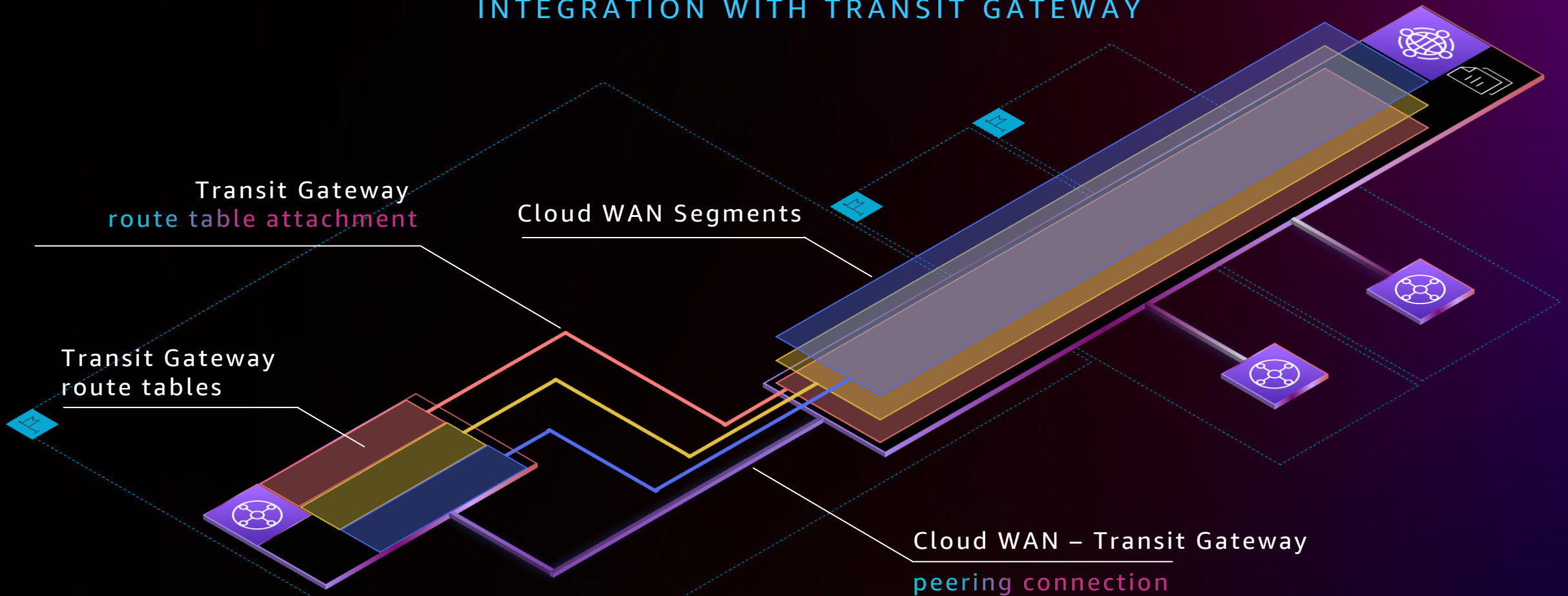
## INTEGRATION WITH TRANSIT GATEWAY




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

# AWS Cloud WAN

## INTEGRATION WITH TRANSIT GATEWAY

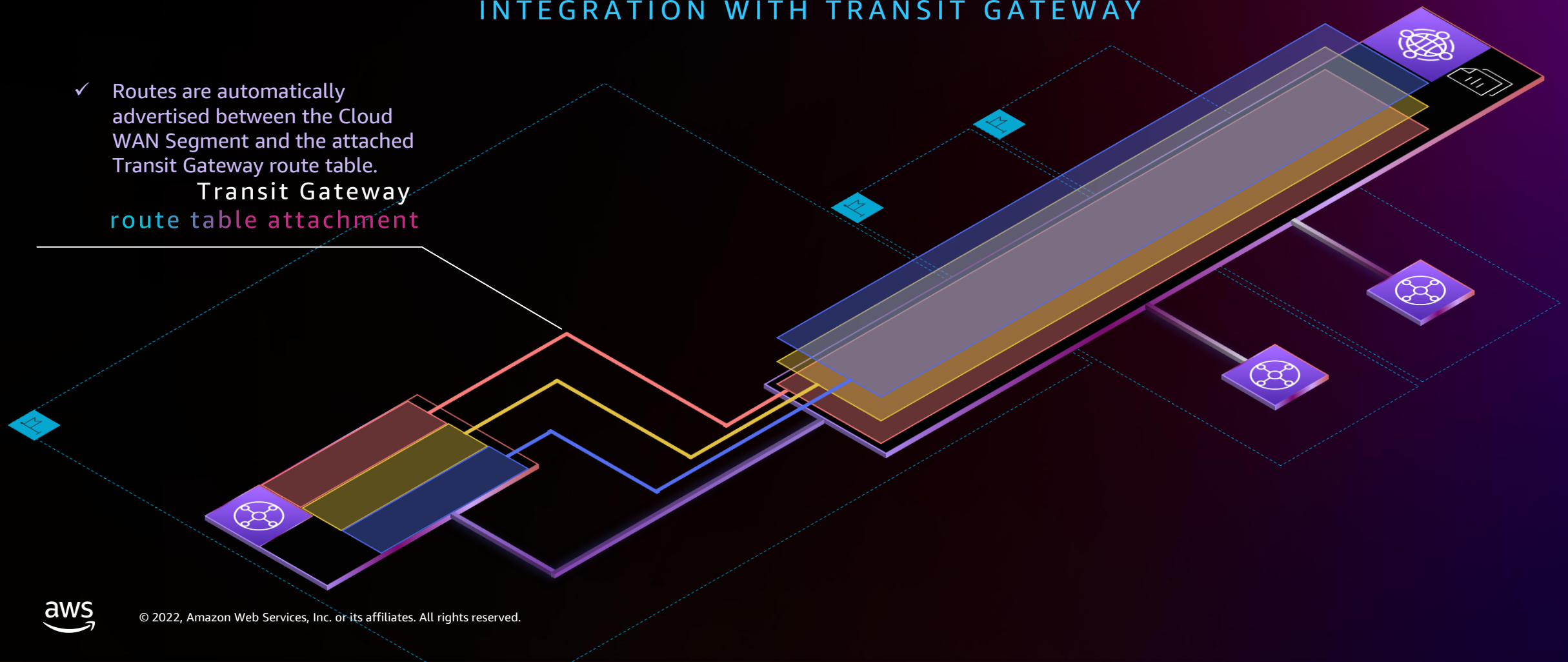



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Cloud WAN

## INTEGRATION WITH TRANSIT GATEWAY

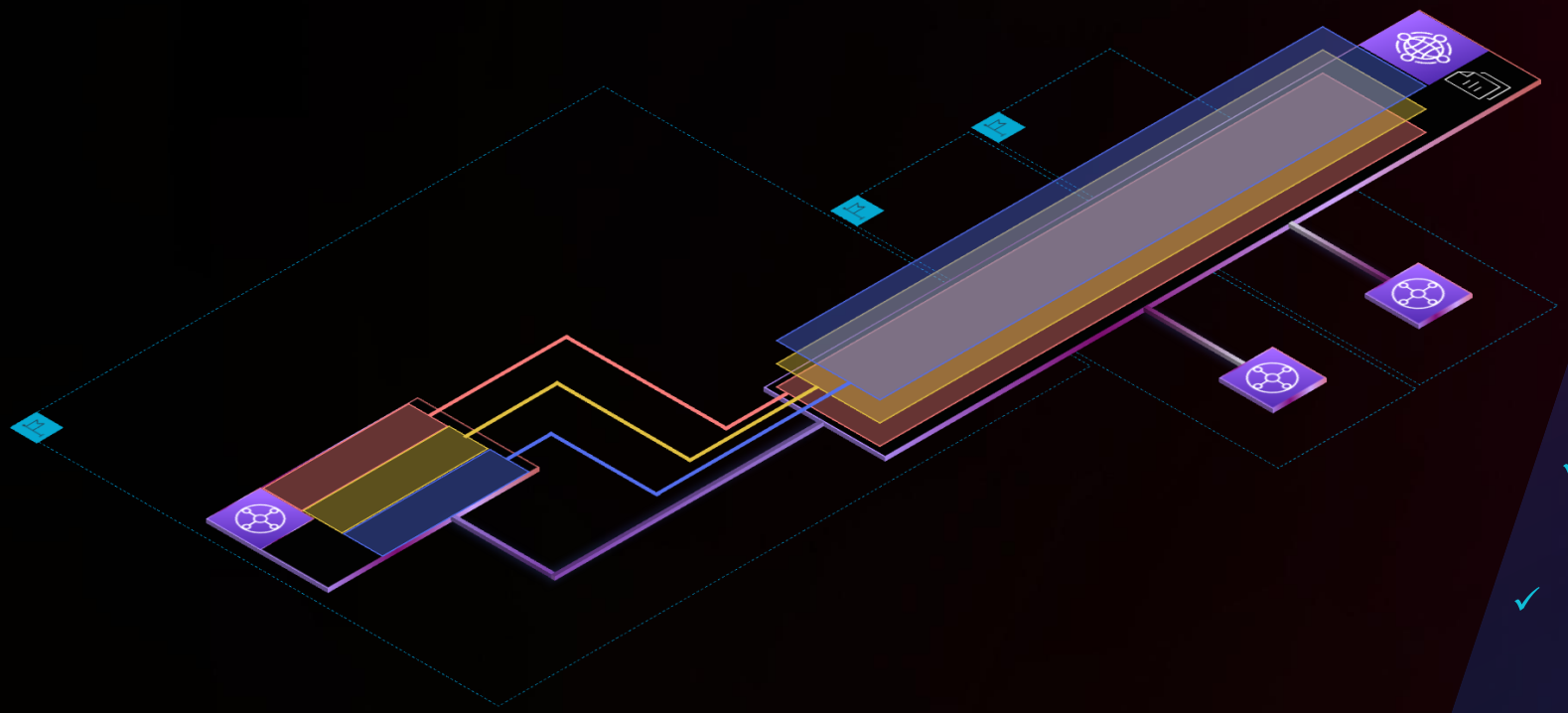
- ✓ Routes are automatically advertised between the Cloud WAN Segment and the attached Transit Gateway route table.




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

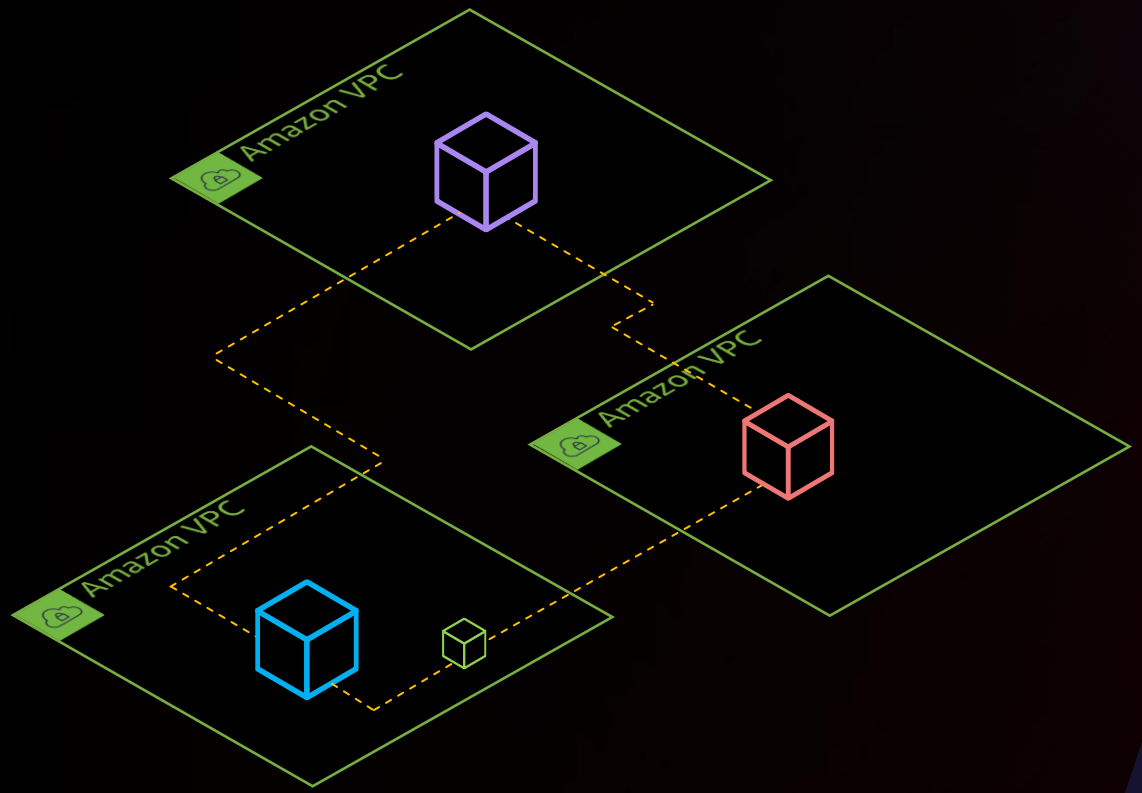
# AWS Cloud WAN

## TRANSIT GATEWAY & CLOUD WAN CONSIDERATIONS



- ✓ Cloud WAN peering to Transit Gateway is regional; it enables the creation of route table attachments.
- ✓ Route table attachments enable end-to-end segmentation between Cloud WAN and Transit Gateway.
- ✓ Both dynamically learned and static routes are advertised over a route table attachment.
- ✓ Direct Connect Gateway integration is supported through Transit Gateway route table attachment.

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

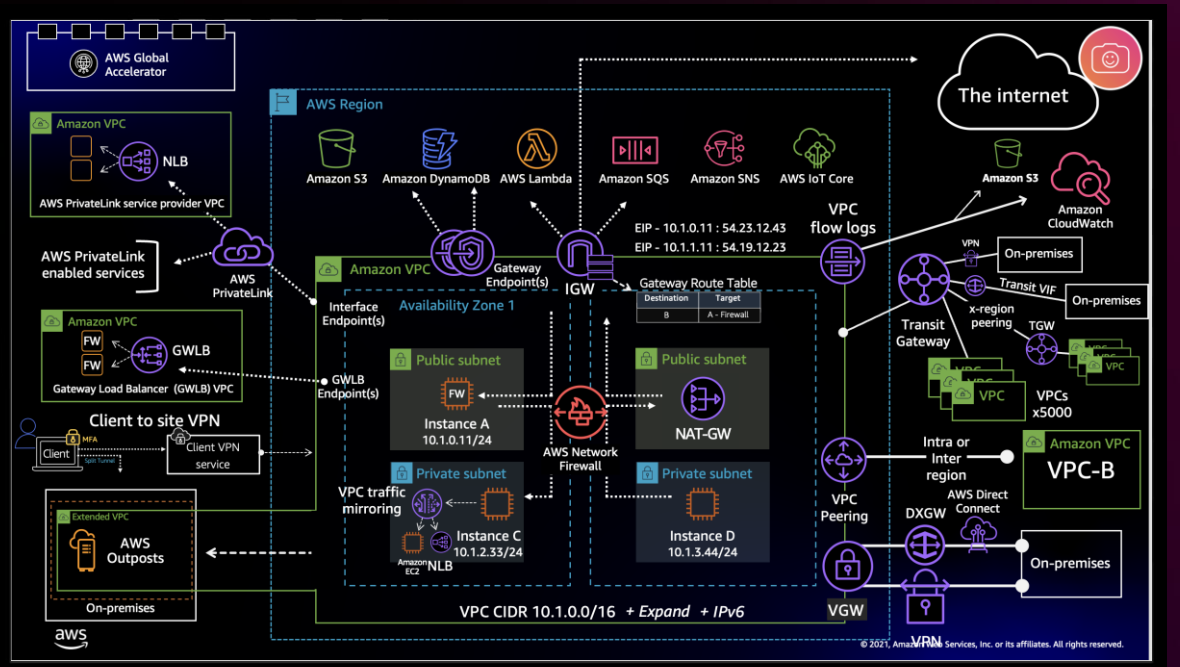



# Application networking

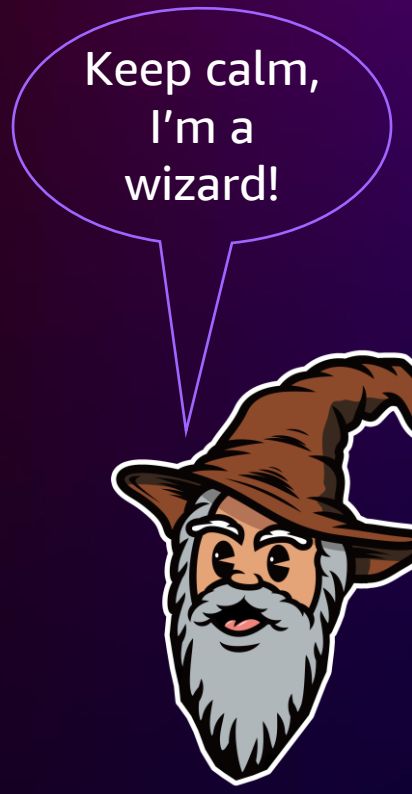
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Networking






AWS re:Invent




aws

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



# Developers

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



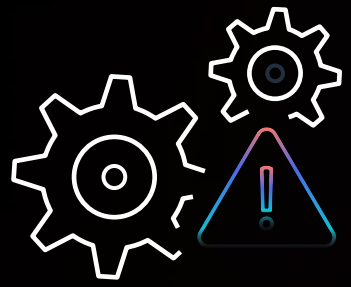
# Security

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

# What about service meshes?

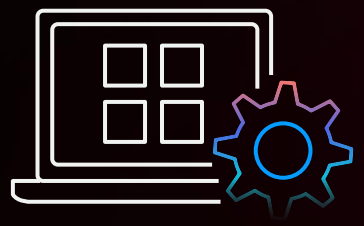
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Service mesh challenges



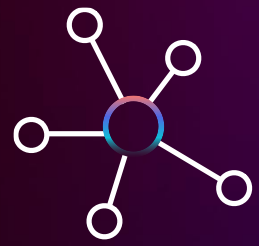
## SIDECAR PROXIES REQUIRED

Deploying and maintaining proxies at scale can be difficult



## ONLY FOR CONTAINER-BASED WORKLOADS

Does not work for other workloads such as serverless and Amazon EC2



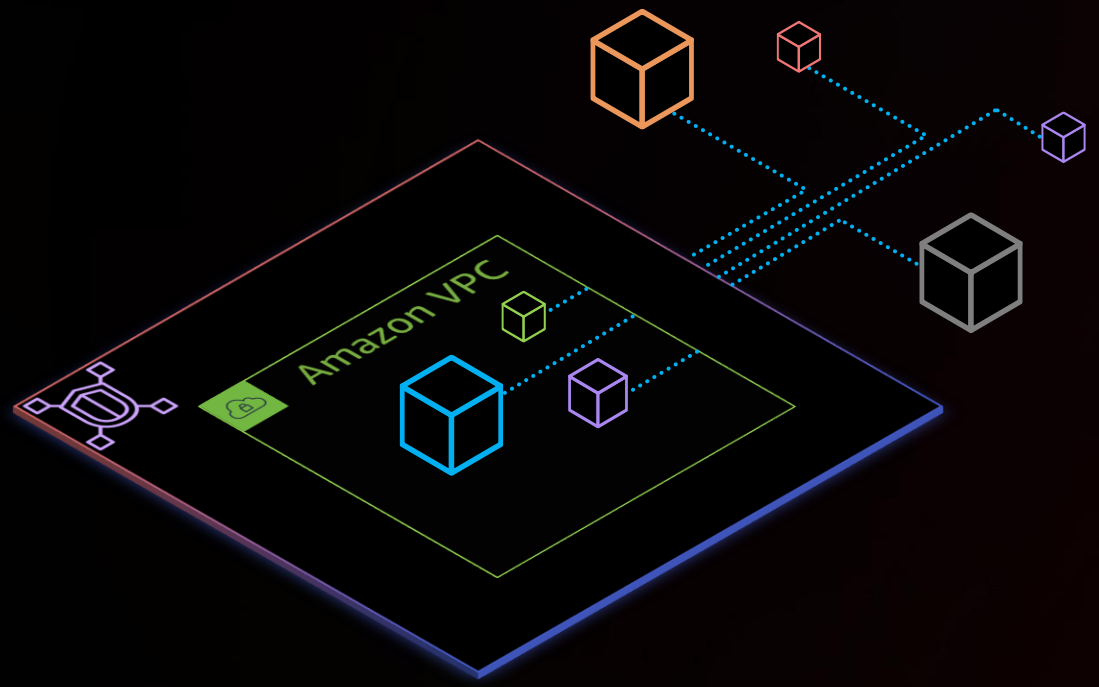
## NETWORK CONNECTIVITY REQUIRED

Inter-VPC networking is not mapped to application and security needs

aws

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

PREVIEW




# Amazon VPC Lattice

aws

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

# Amazon VPC Lattice

## Components

### Service network

A logical grouping mechanism to simplify how users enable connectivity and apply common policies.

### Service

Represents an Application Unit and can extend across all compute – instances, containers, serverless.

### Service directory

A centralized registry of all services that have been registered with Amazon VPC Lattice.

### Security policies

You can apply AWS Identity and Access Management (IAM) resource policies both at the Service Network and at the service level.

aws

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

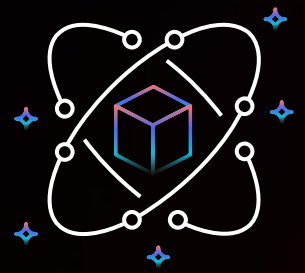
# Amazon VPC Lattice

## SIMPLIFY APPLICATION LAYER NETWORKING



### NO SIDECAR PROXIES REQUIRED

Fully managed control plane with no proxies to deploy and maintain



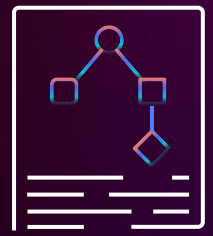
### WORKS ACROSS ALL COMPUTE OPTIONS

Works across Amazon EC2, Amazon EKS, Amazon ECS, and AWS Lambda



### TRAFFIC AND ACCESS CONTROLS

Improved security posture and rich traffic controls and segmentation



### NO NETWORKING EXPERTISE REQUIRED

Simplified connectivity and security across VPCs and accounts

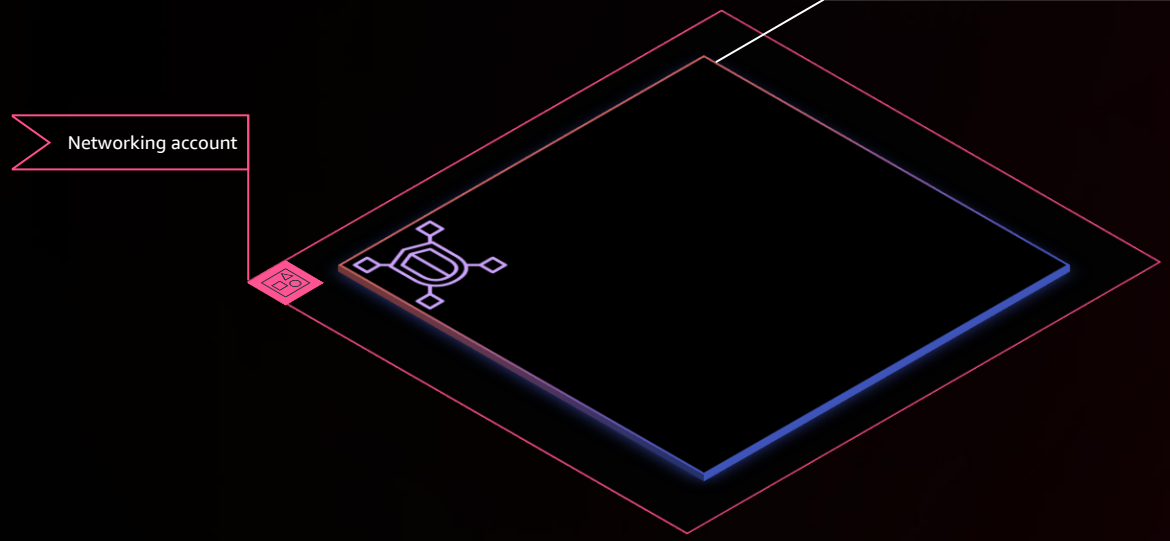
aws

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

# Amazon VPC Lattice

## HOW IT WORKS

1. Create service network




Network admin

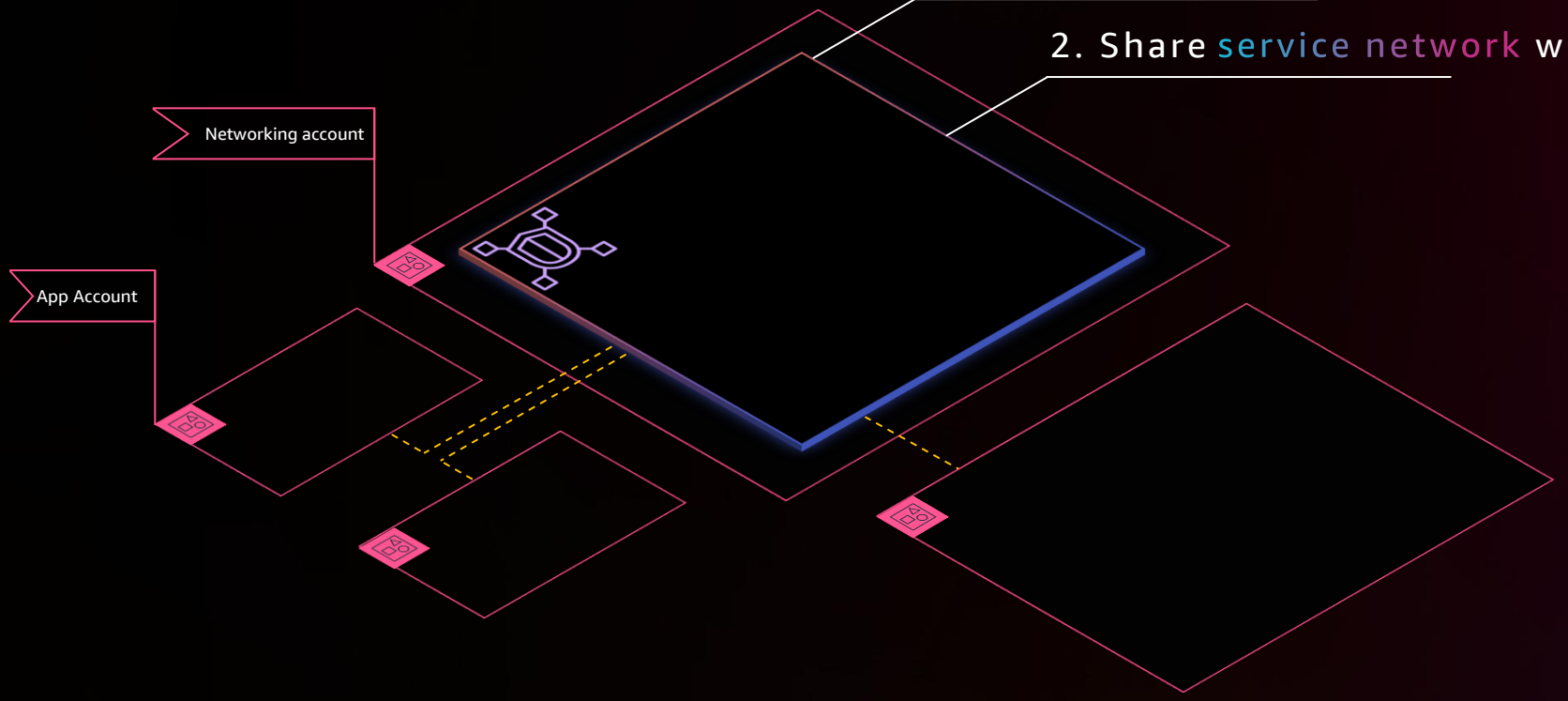
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon VPC Lattice

## HOW IT WORKS

1. Create service network

2. Share service network with other accounts

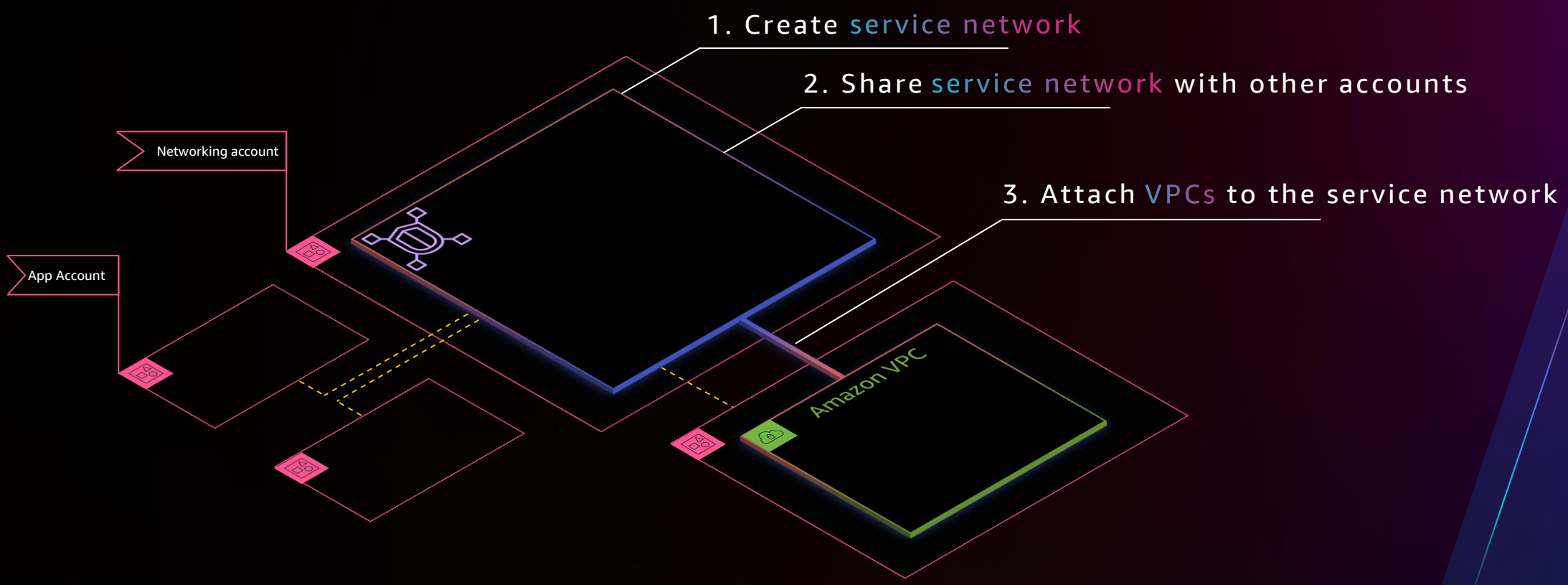



Network admin

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

# Amazon VPC Lattice

## HOW IT WORKS




Network admin

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

# Amazon VPC Lattice

## HOW IT WORKS



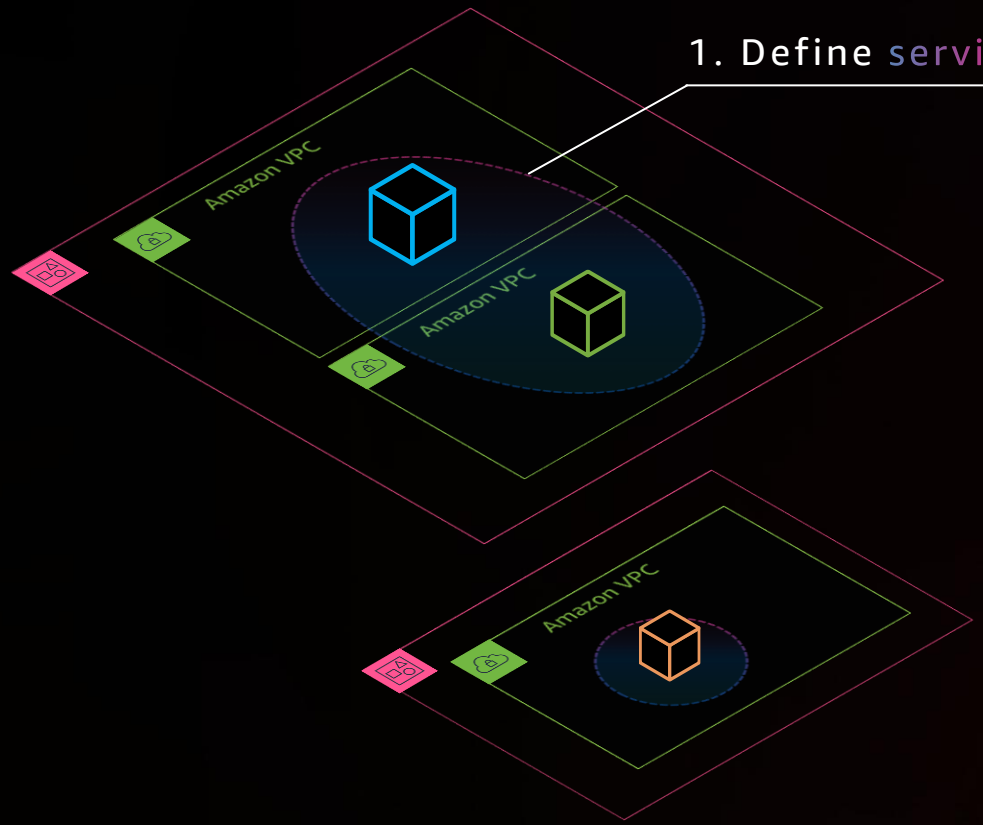

Network admin

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

# Amazon VPC Lattice

## HOW IT WORKS

1. Define services

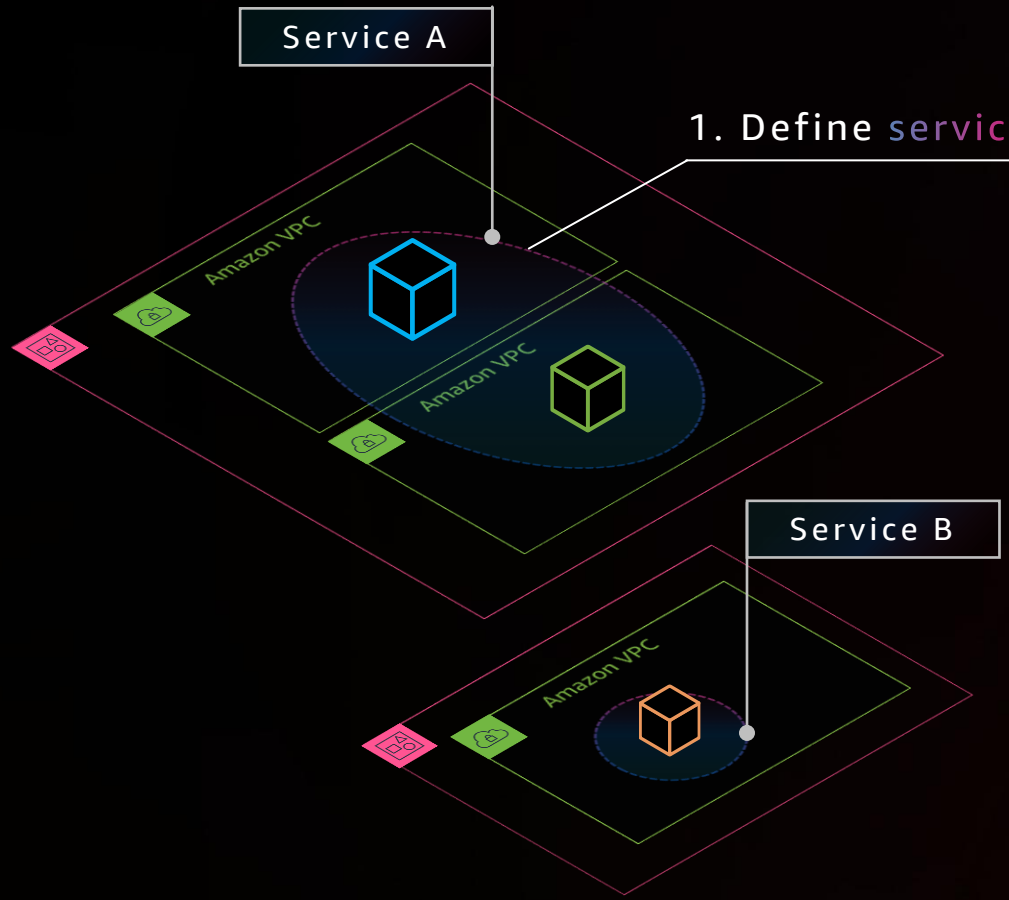



Developers

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

# Amazon VPC Lattice

## HOW IT WORKS

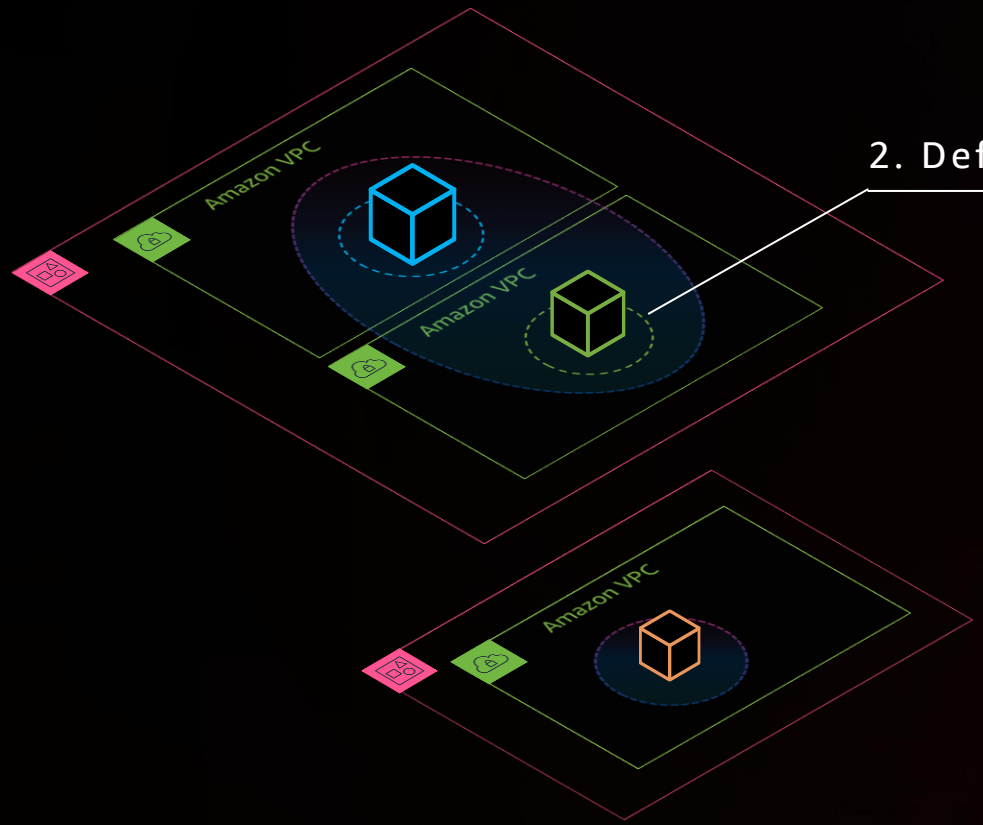



Developers

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

# Amazon VPC Lattice

## HOW IT WORKS



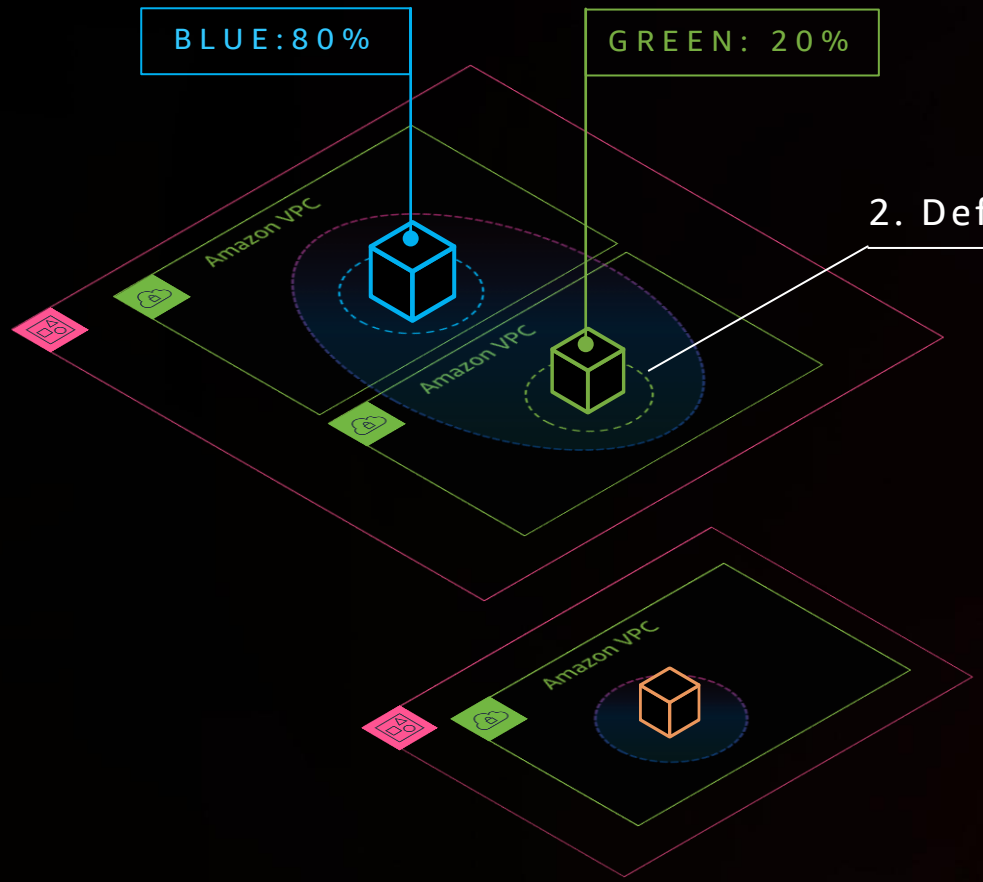

2. Define routing policies

Developers

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

# Amazon VPC Lattice

## HOW IT WORKS



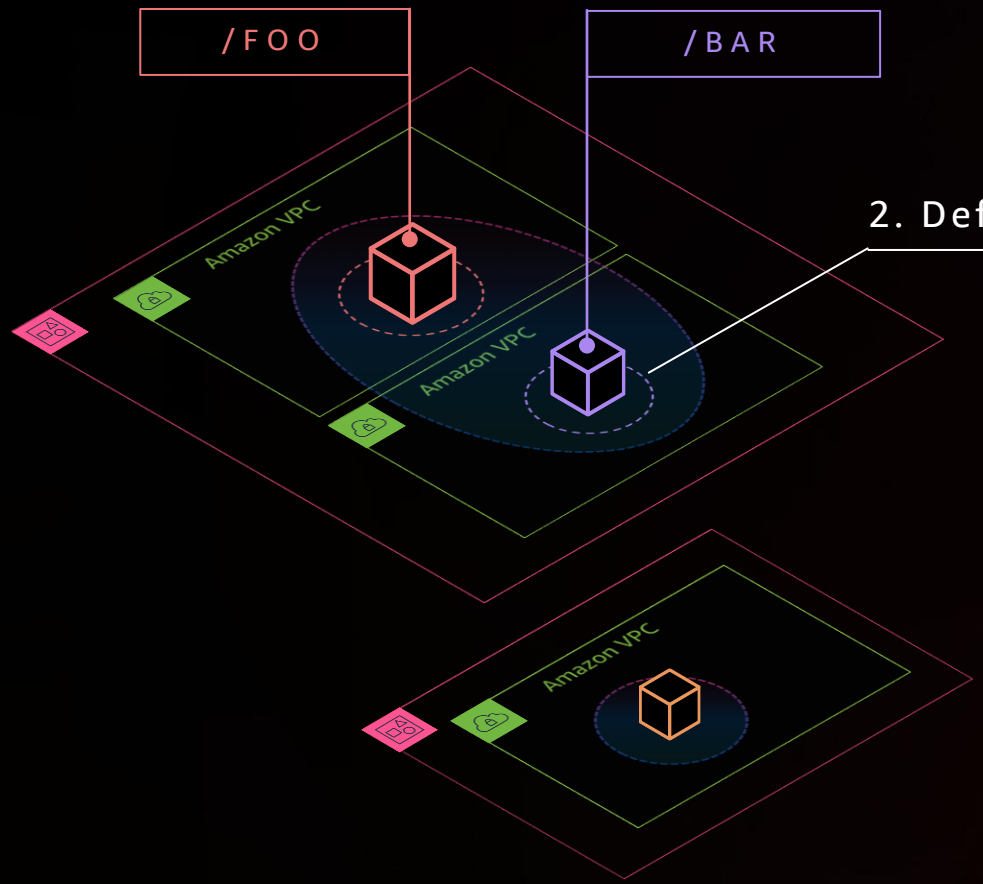

2. Define routing policies

Developers

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

# Amazon VPC Lattice

## HOW IT WORKS



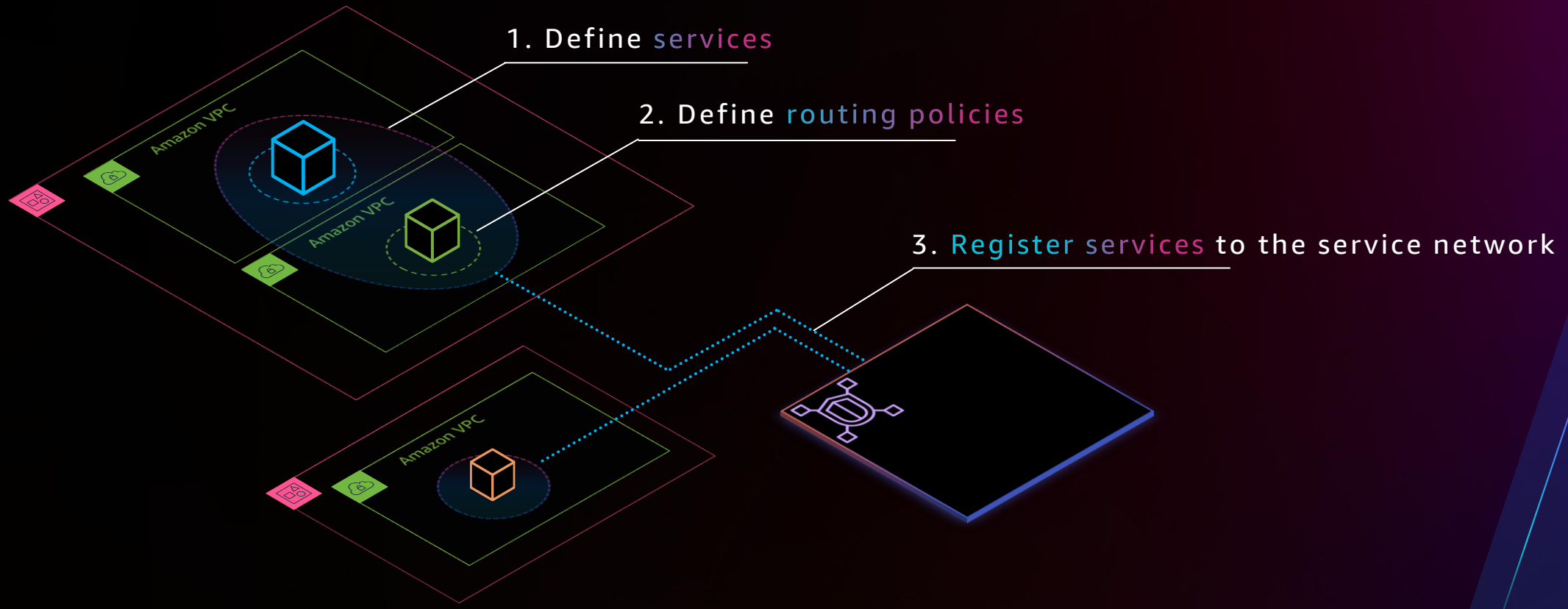

2. Define routing policies

Developers

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

# Amazon VPC Lattice

## HOW IT WORKS

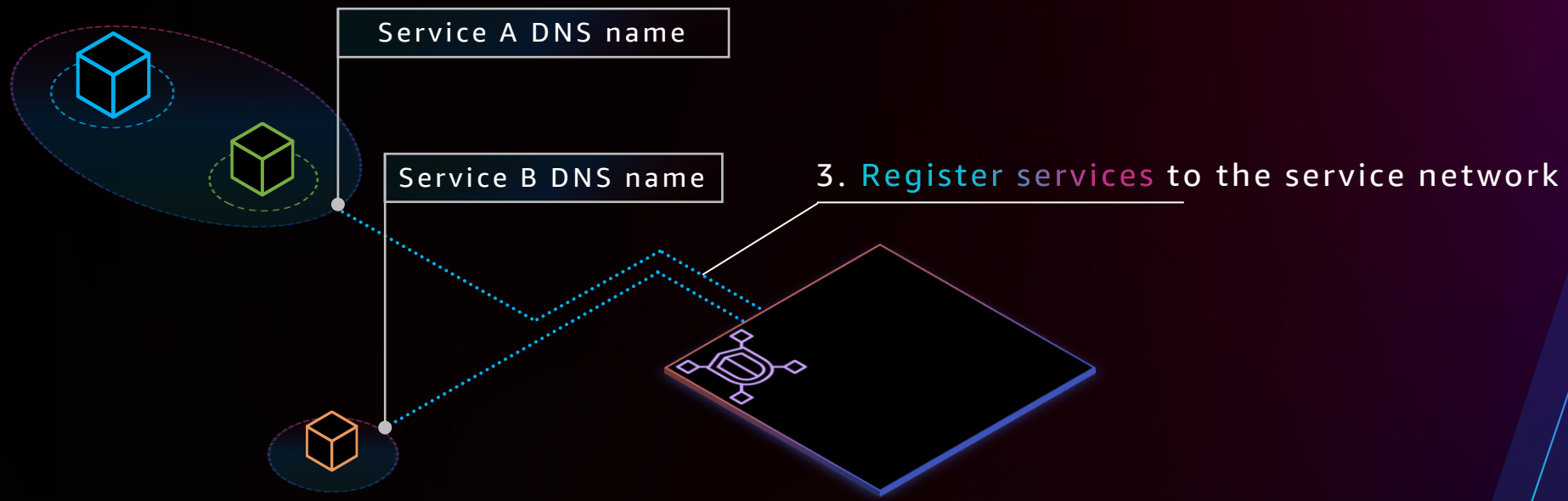



Developers

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

# Amazon VPC Lattice

## HOW IT WORKS

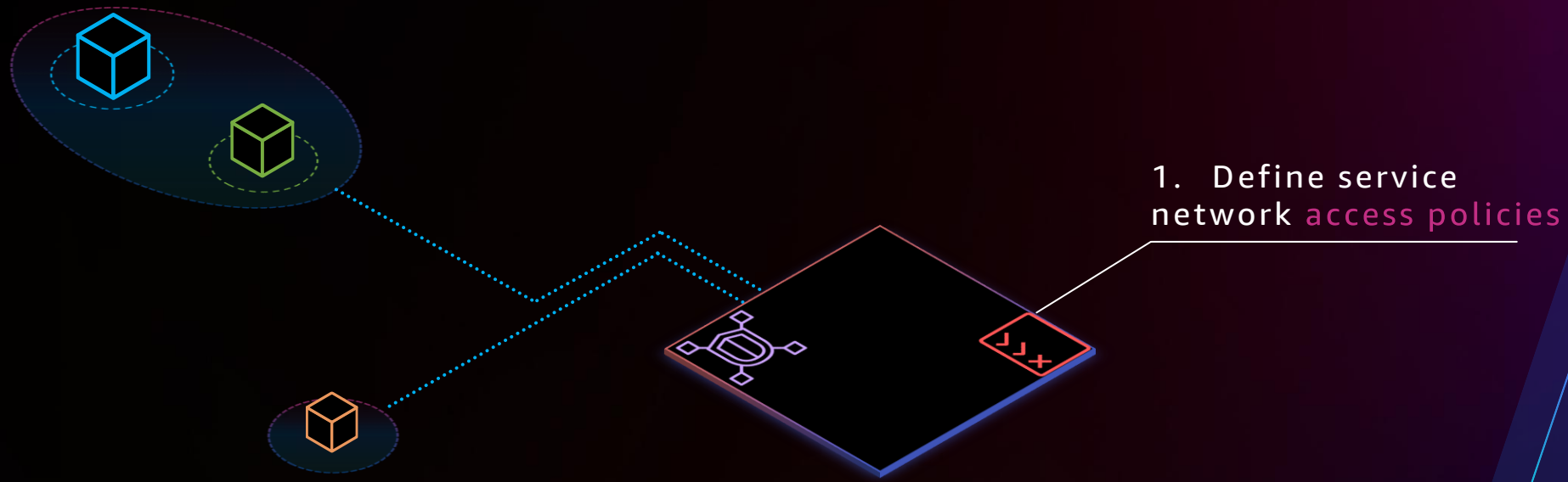



Developers

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

# Amazon VPC Lattice

## HOW IT WORKS



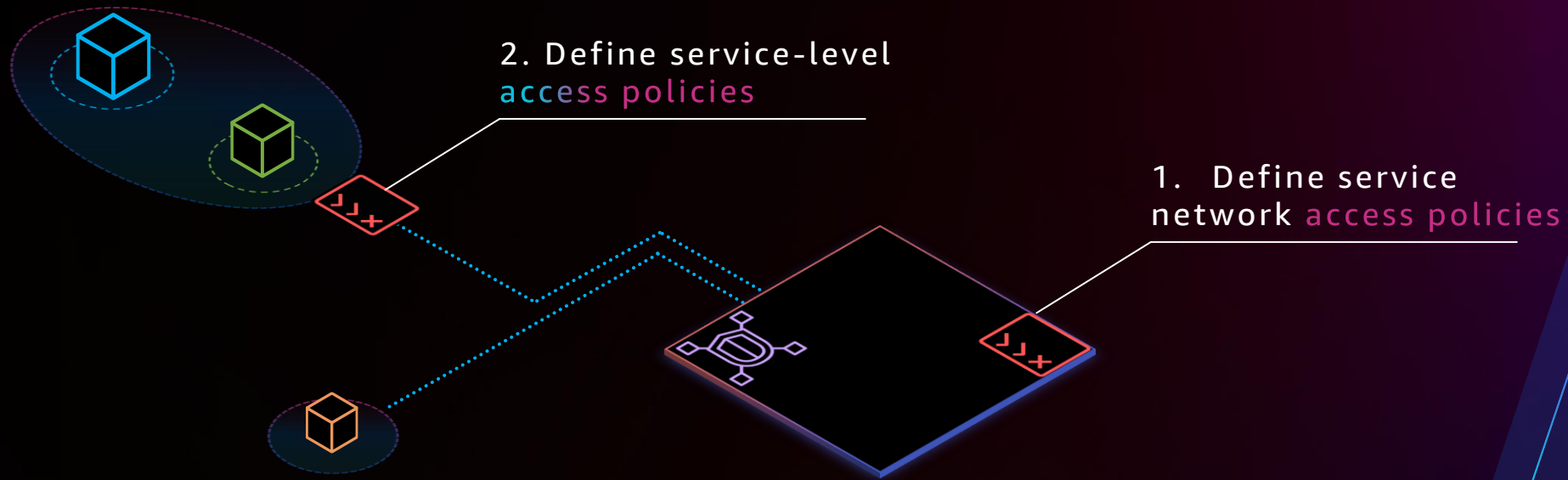

Security

aws

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

# Amazon VPC Lattice

## HOW IT WORKS

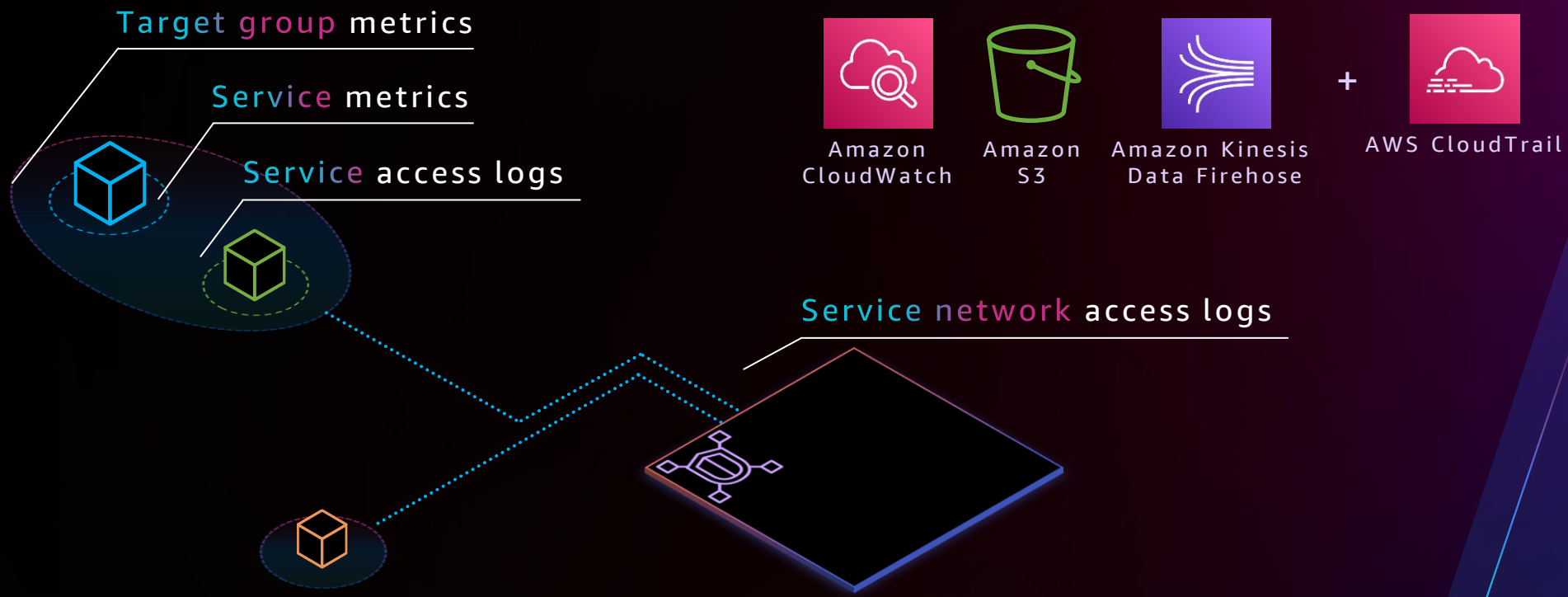



Security

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

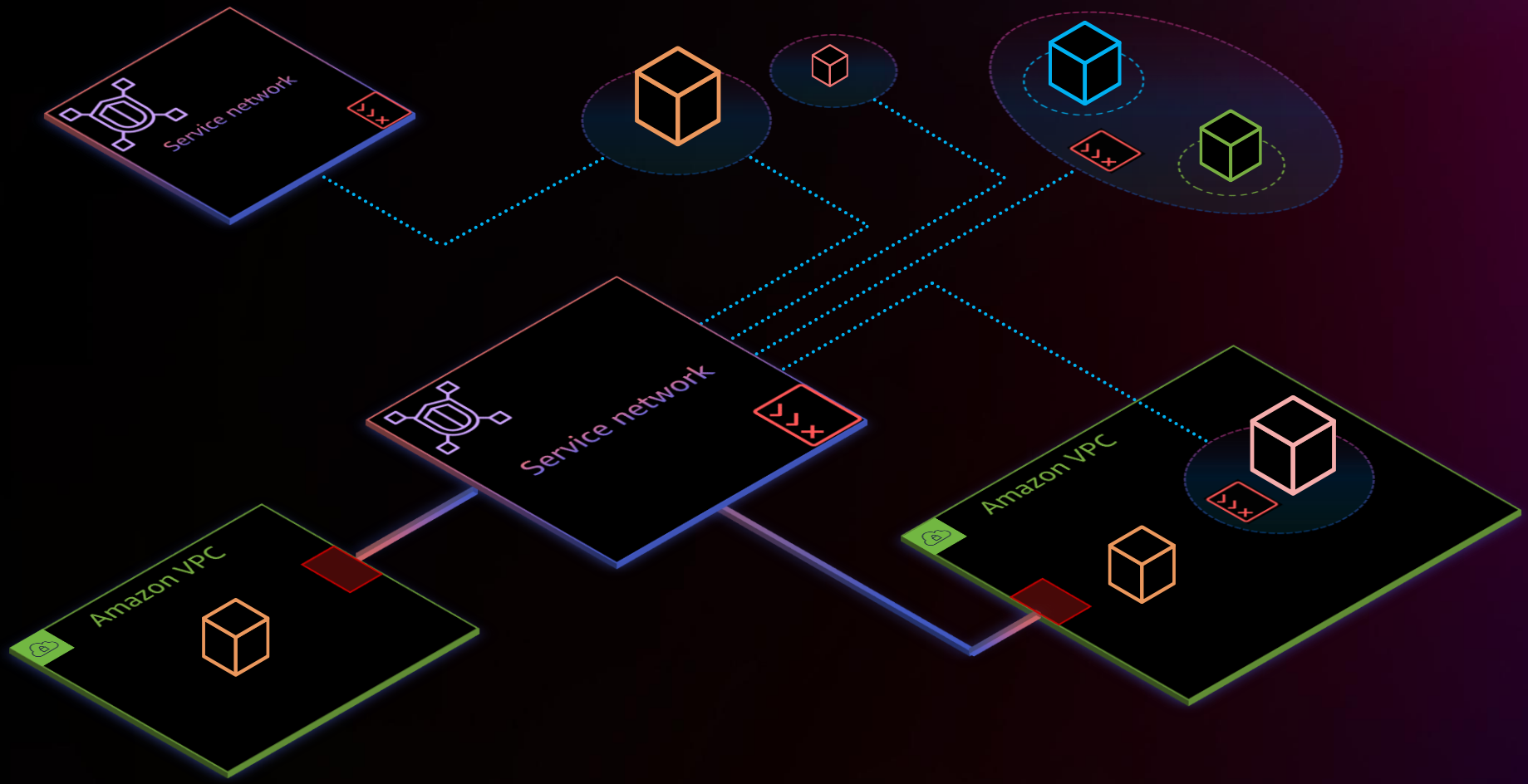
# Amazon VPC Lattice

## HOW IT WORKS




Monitoring

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




# Putting everything together

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

# Amazon VPC Lattice

## Considerations

- ✓ Doesn't require managing network connectivity
- ✓ Accommodates for existing network connectivity
- ✓ Accommodates for overlapping IP addresses
- ✓ You can use security groups in your VPCs to control access to the service network
- ✓ One VPC can be attached to one service network at a time
- ✓ A Service can be registered too multiple service networks at a time

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

# Amazon VPC Lattice



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

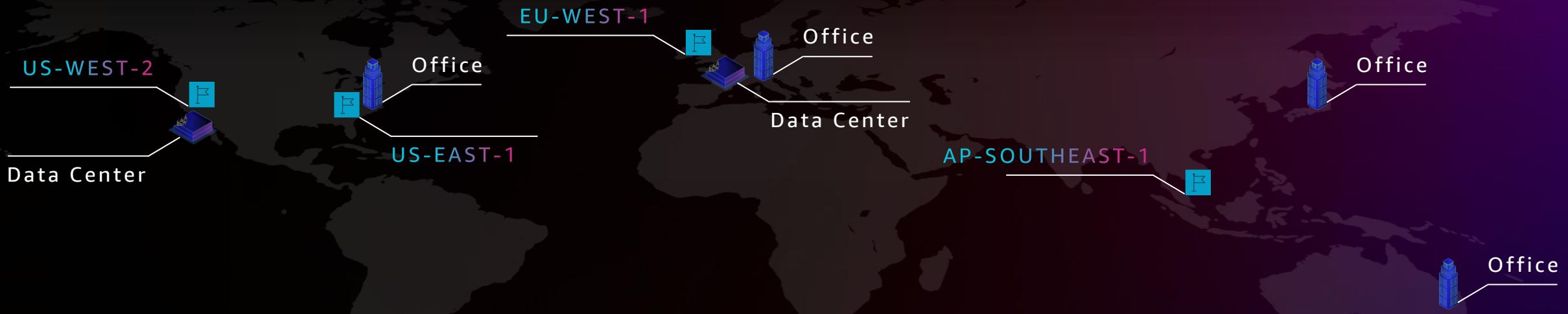


# AWS Network Operations

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

# Your global network

ON AWS




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

Networking & Content Delivery

# Network Manager

## Manage and monitor your AWS network

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network monitoring and troubleshooting, IP management, and network security and governance.

CONNECTIVITY

### Cloud WAN

AWS Cloud WAN is a managed wide area networking (WAN) service that makes it simpler to build and operate a unified global network. Cloud WAN features a centralized dashboard along with powerful policy management tools, with built-in support for network segmentation. Explore >

Create global network

CONNECTIVITY

### Transit Gateway Networ

AWS Transit Gateway Networ
centrally manage your netw
Regions, and on-premises
network in a centralized
them using CloudWatch

Create global ne

MONITORING AND TROUBLESHOOTING

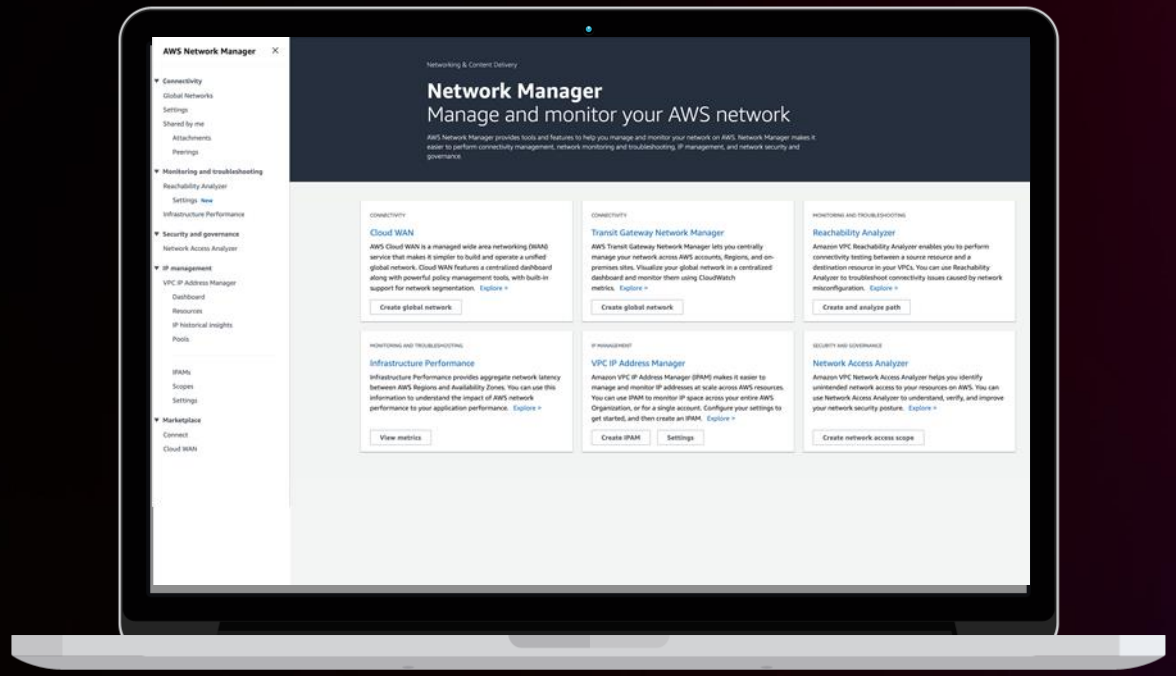
IP MANAGEMENT

AWS Network Manager

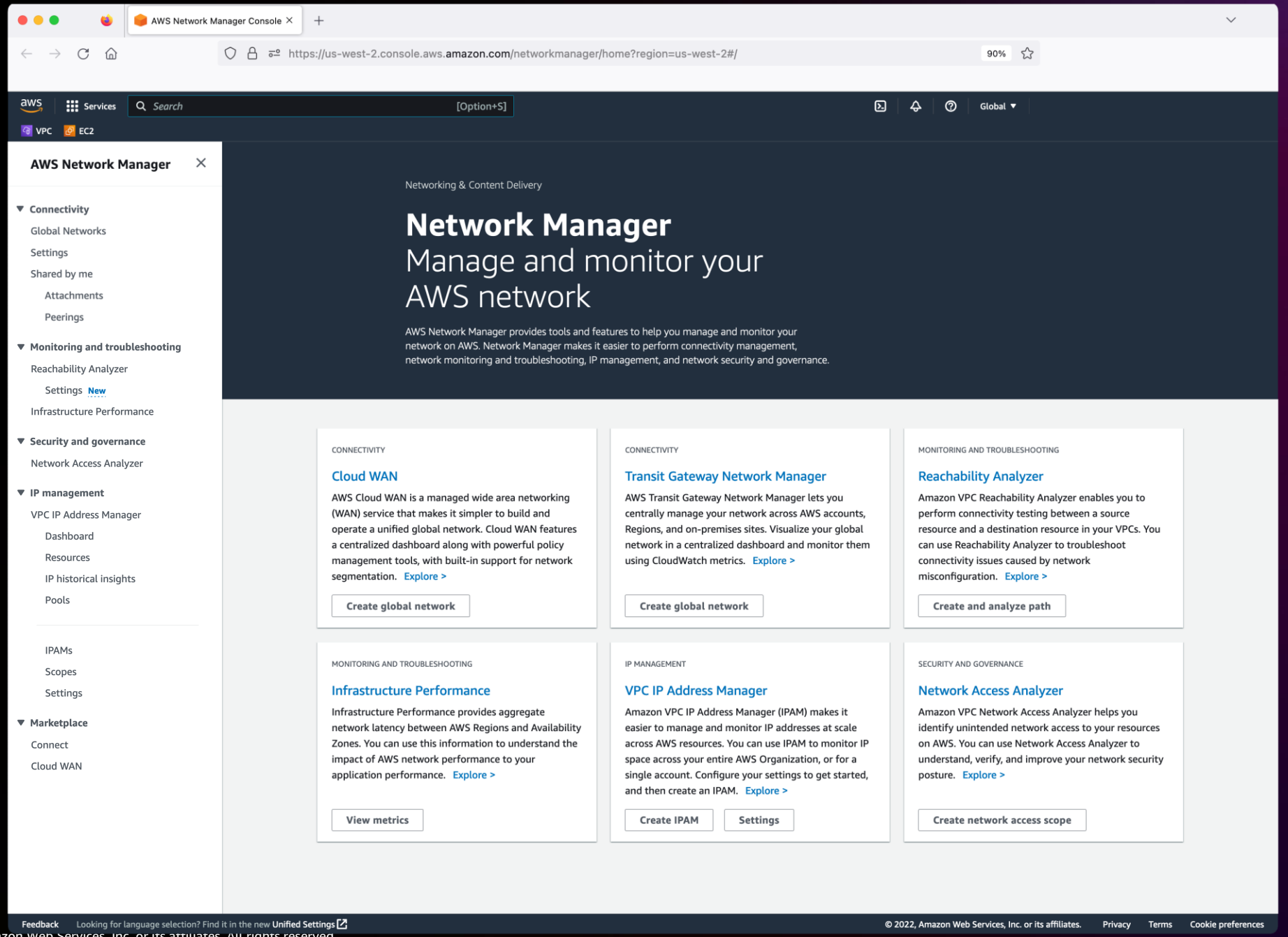
NEW

# AWS Network Manager

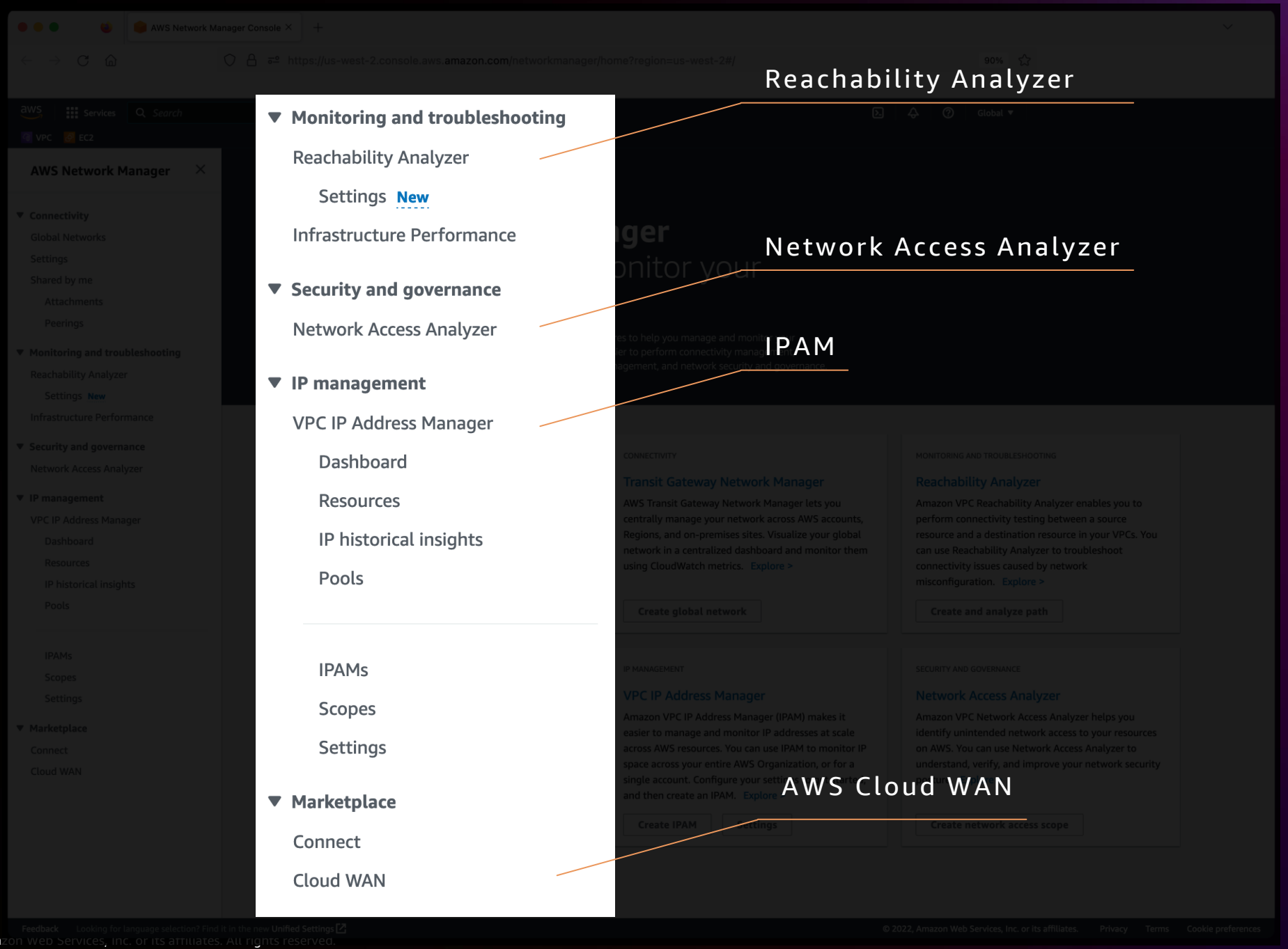
## A CENTRAL LOCATION FOR MANAGING AND MONITORING YOUR AWS NETWORK



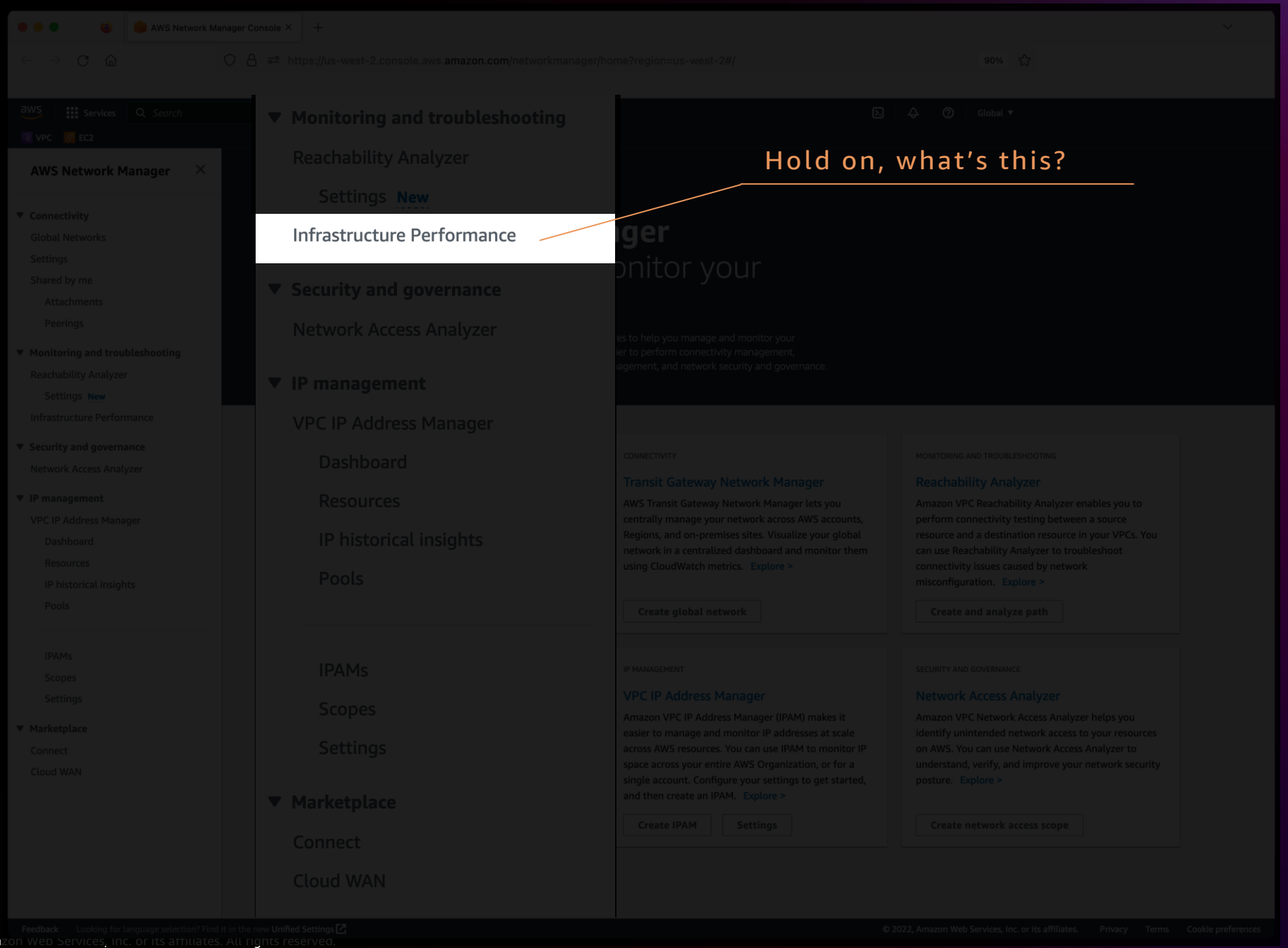

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



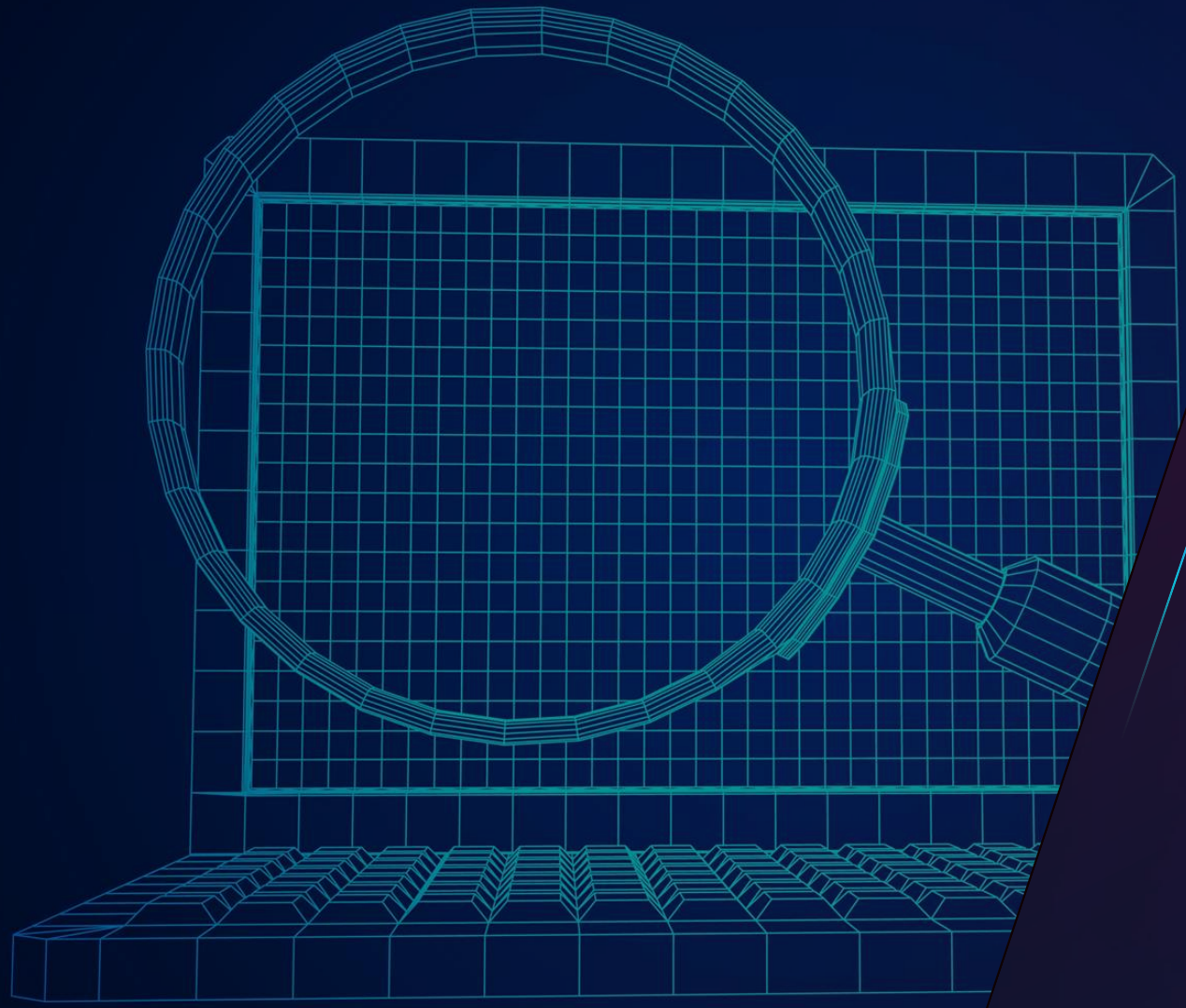

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.




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




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

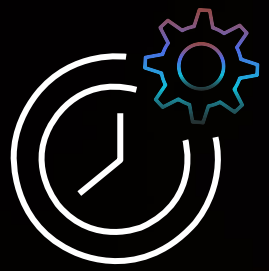


# AWS Network Infrastructure Performance

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

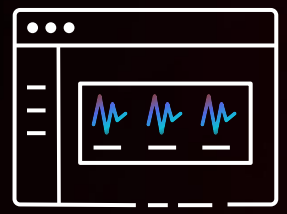
# AWS Network Infrastructure Performance

## MONITORING AND OBSERVABILITY



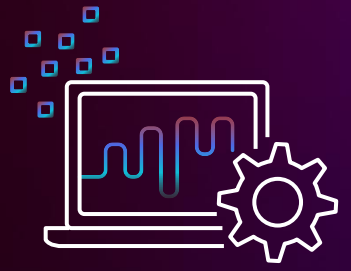
### MONITOR LATENCY

Monitor latency of AWS global network using console or Amazon CloudWatch



### UNDERSTAND HEALTH

Understand the health status of AWS global network between Regions and Availability Zones

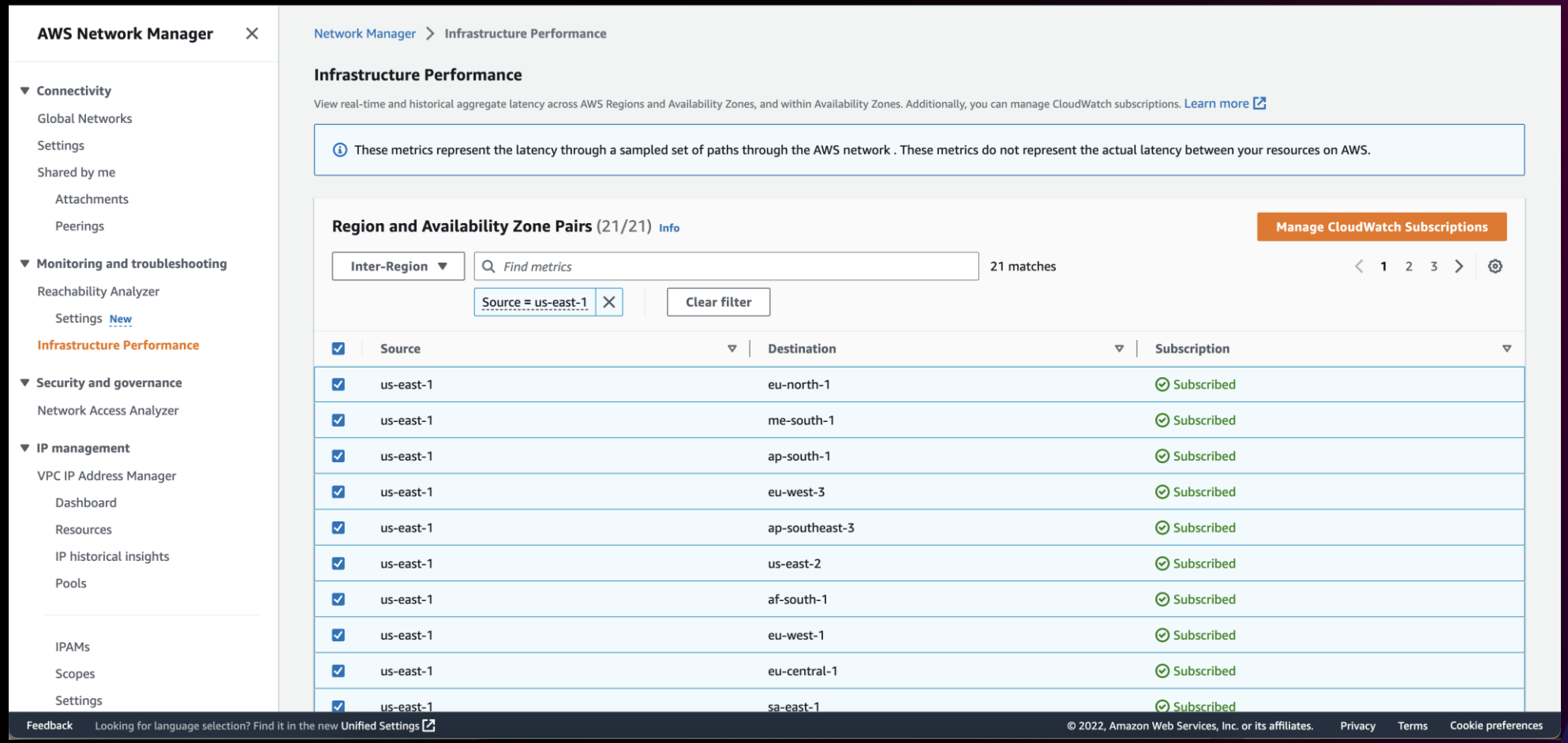


### PLAN GROWTH

Plan Region expansion

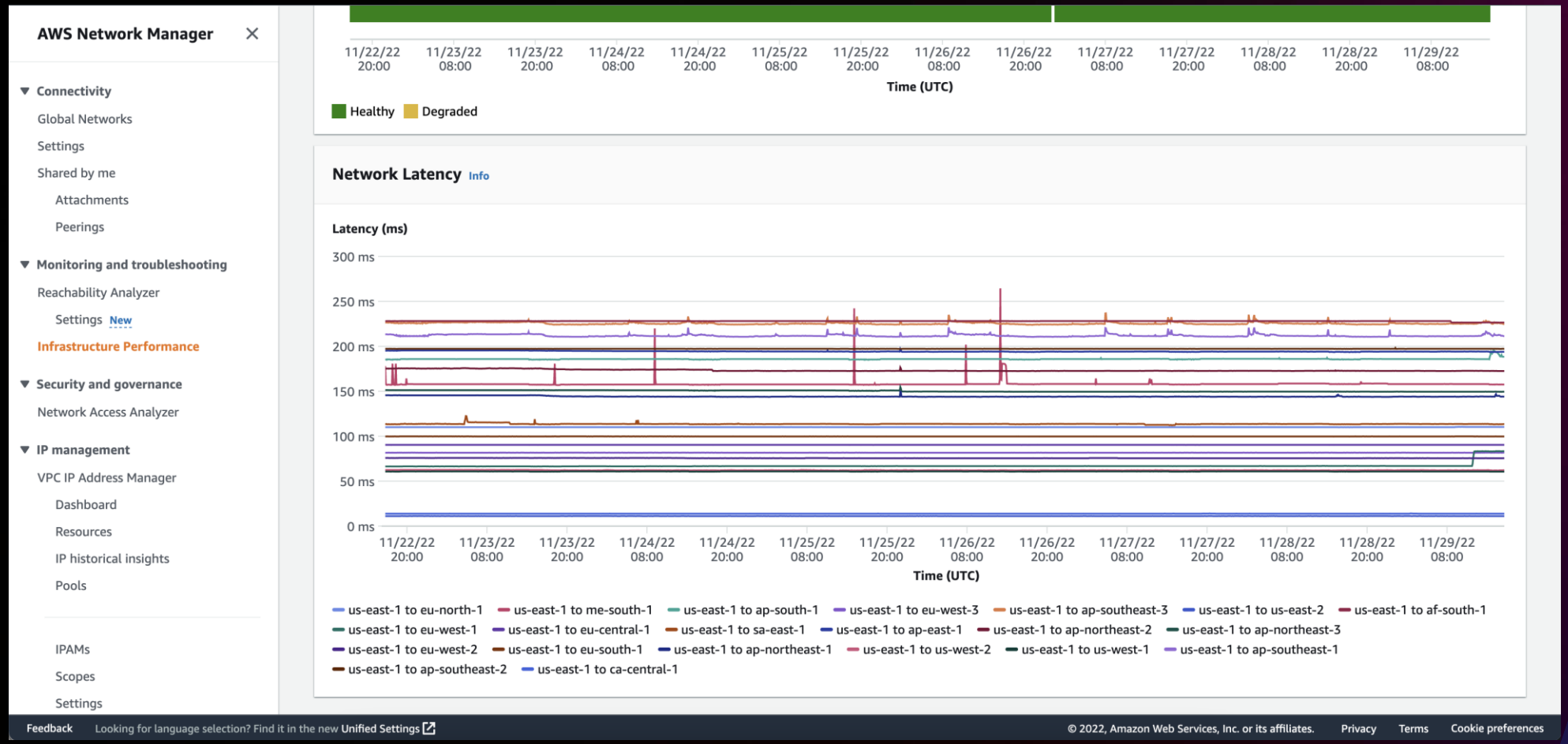
aws

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



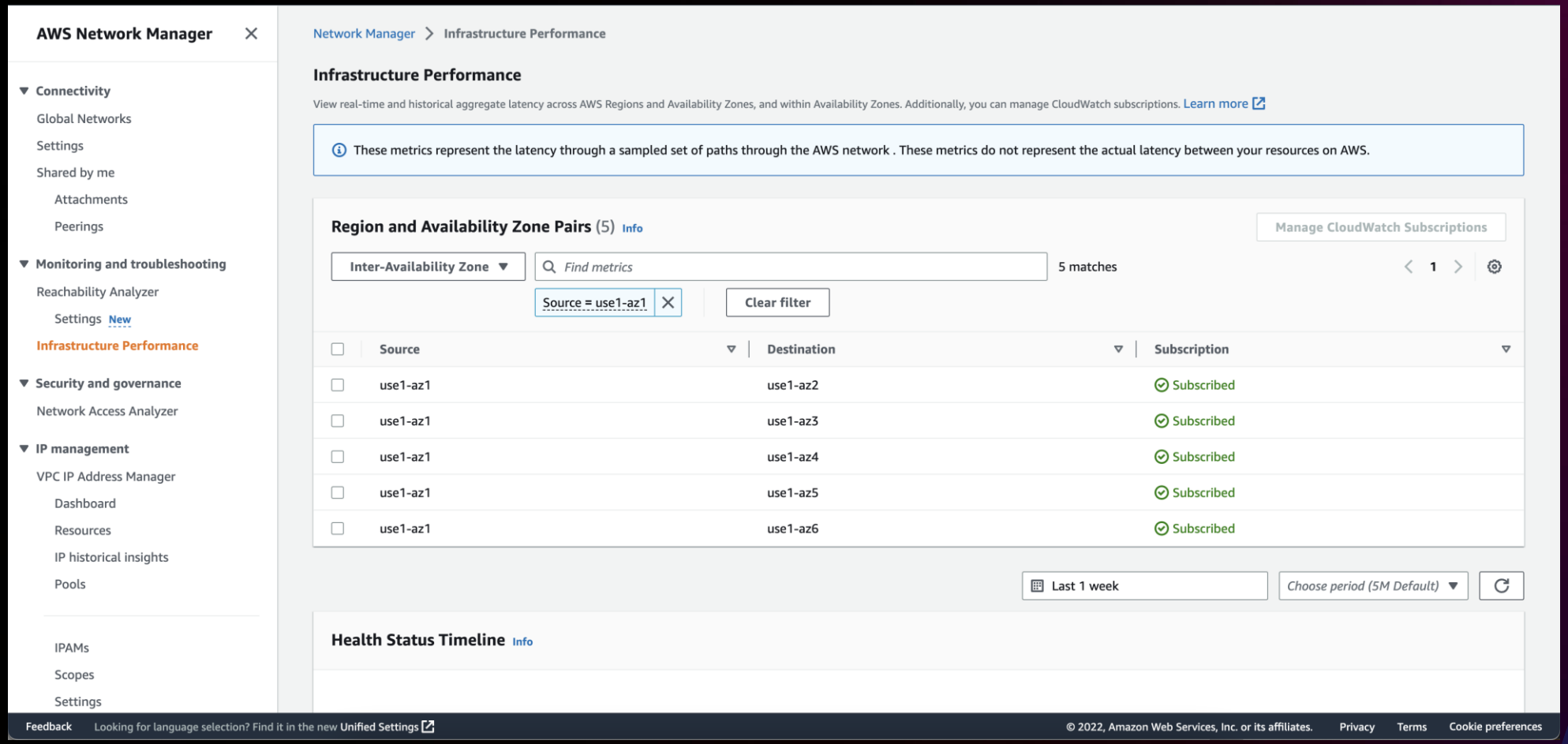

# Inter-Region

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



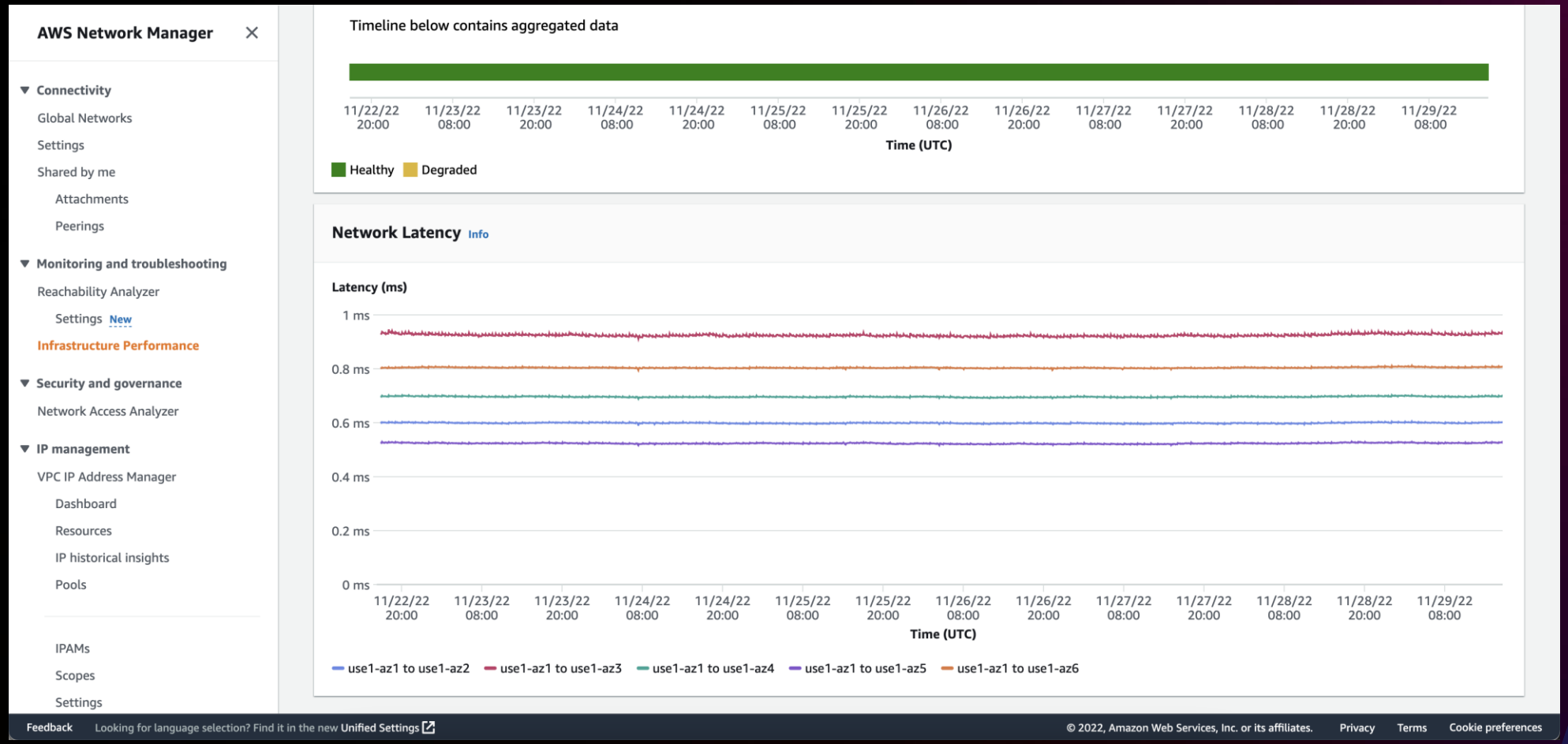

# Inter-Region

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



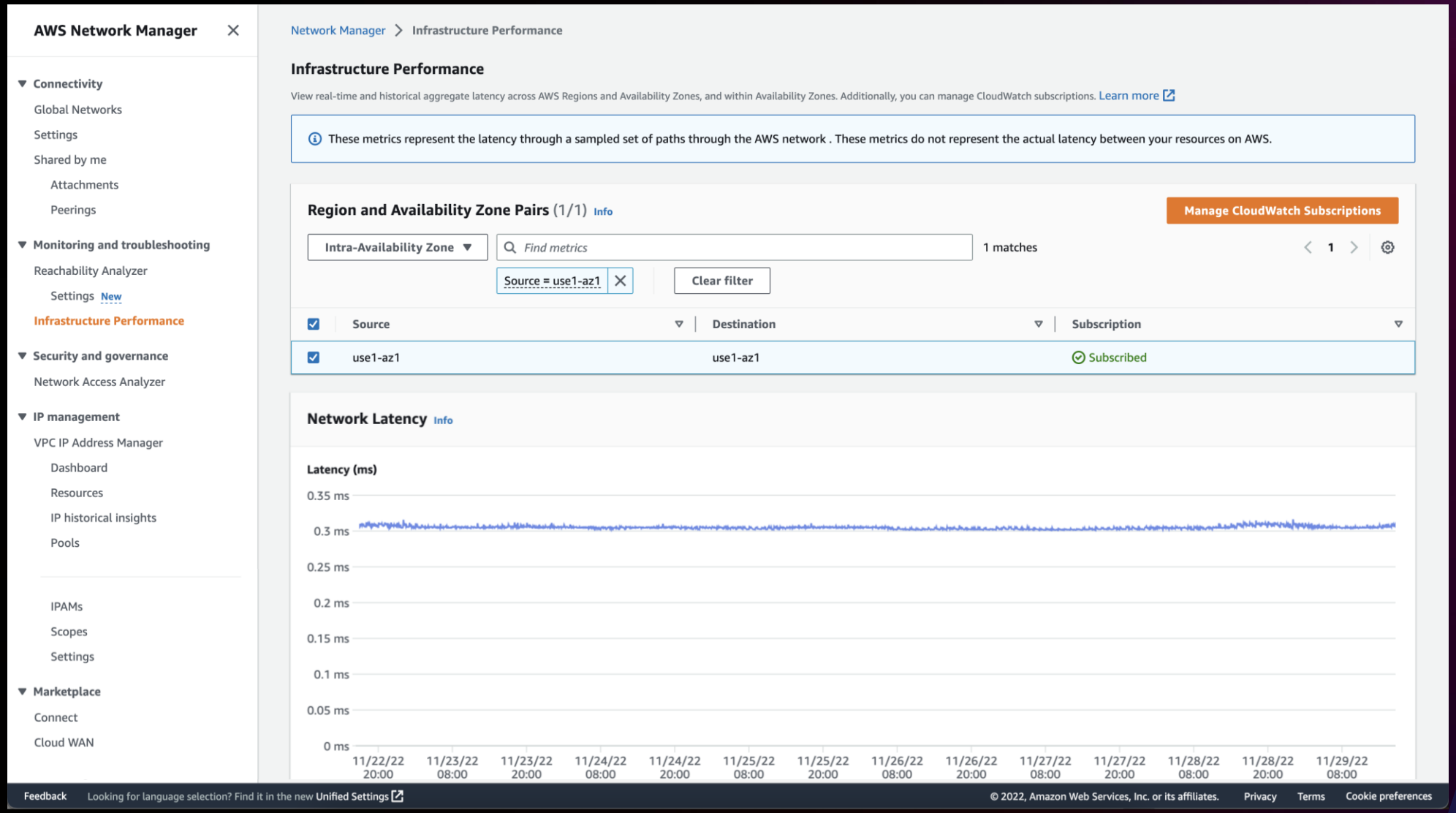

# Inter-AZ

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




# Inter-AZ

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




Intra-AZ

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

PREVIEW



# Amazon CloudWatch
# Internet Monitor

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

# Amazon CloudWatch Internet Monitor

INTERNET MONITORING AND OBSERVABILITY

**MONITOR**

VPCs, CloudFront distributions, or Amazon WorkSpaces directories

**TRACK**

real-time performance and availability of your endpoints

**EXPLORE**

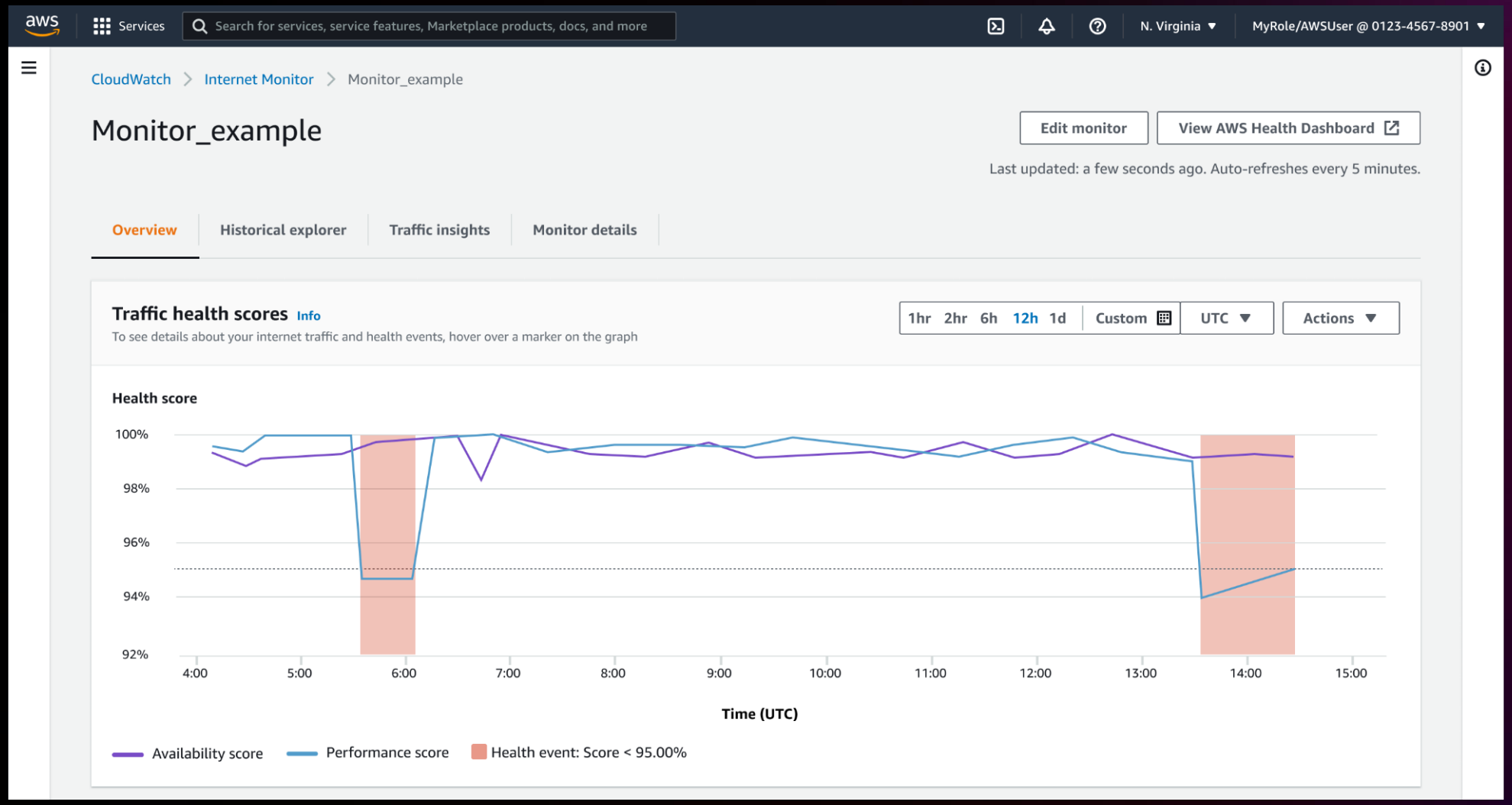
historical data related to your application performance

**OPTIMIZE**

getting insights for improving application performance and delivery

aws

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



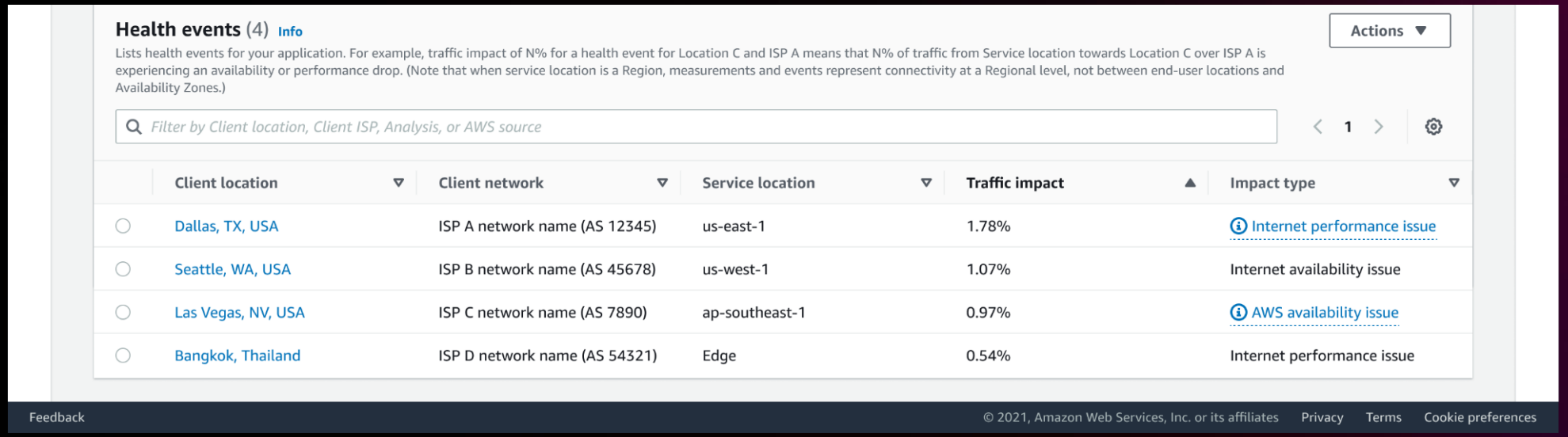

# Monitor details

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




# Traffic overview

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




# Health events

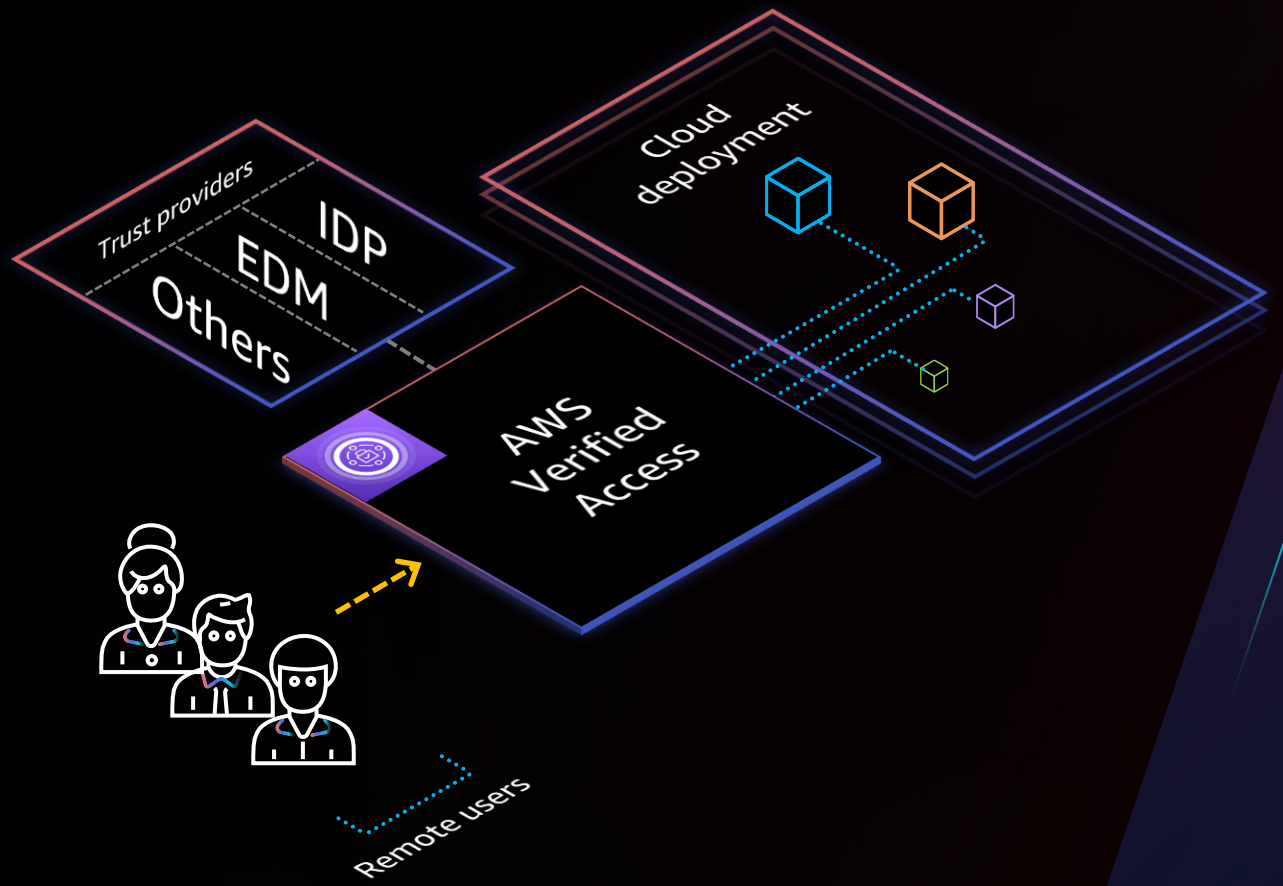
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon CloudWatch Internet Monitor



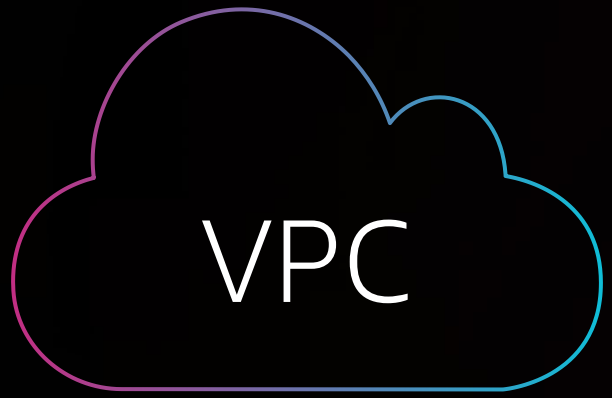
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

PREVIEW




# AWS Verified Access (AVA)

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




Virtual Private Cloud



Security groups and ACLs



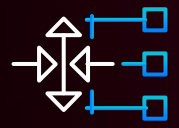
NAT gateway



Network firewall



Partner Appliances



Gateway Load Balancer



Encryption



DNS Firewall



AWS WAF



AWS Shield

aws

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

# Zero Trust

A security model centered on the idea that access to data should not be solely made based on network location

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

# AWS Client VPN




# AWS Site-to-Site VPN – with VGW




Existing remote access methods

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

# AWS Client VPN



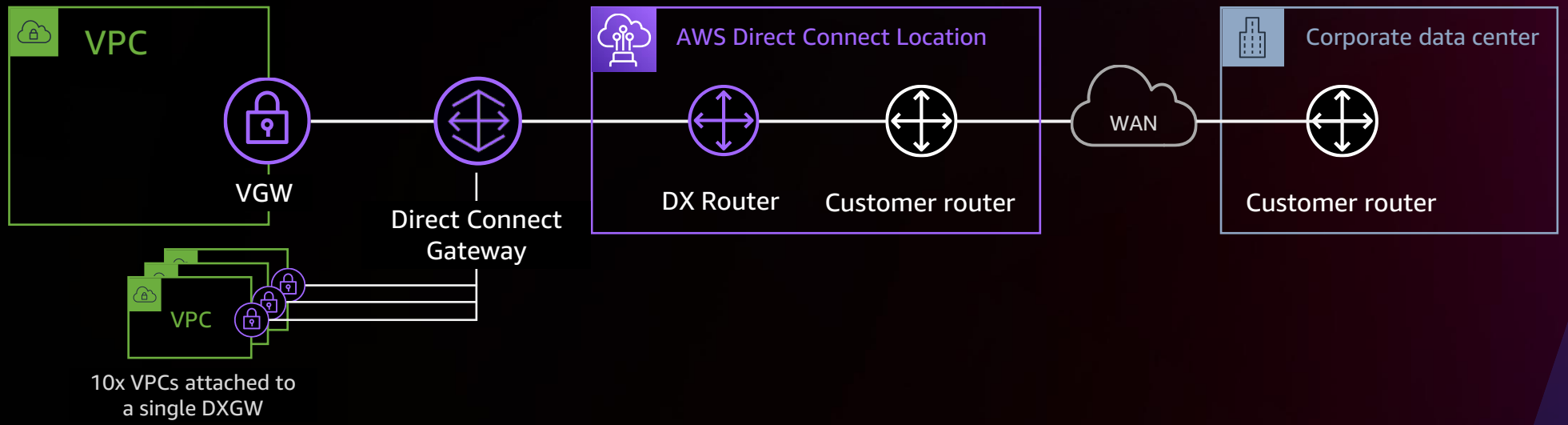

# AWS Site-to-Site VPN – with Transit Gateway




Existing remote access methods

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

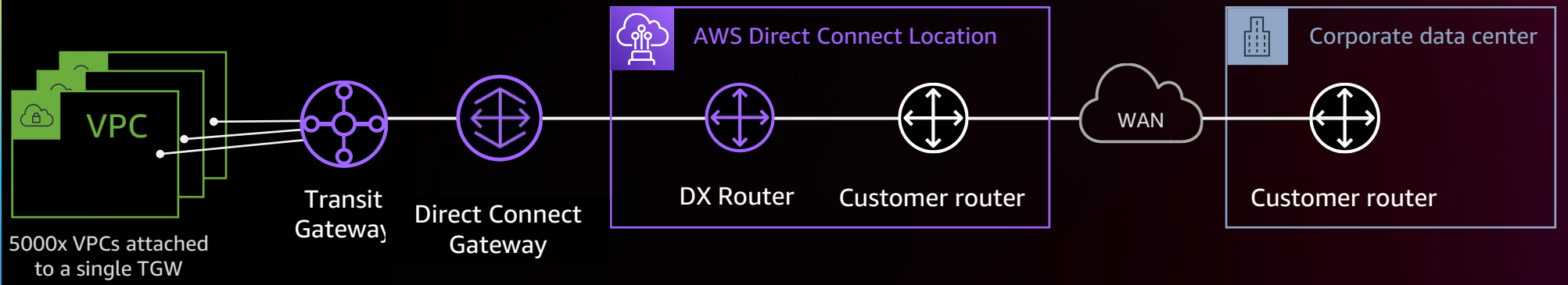
# AWS Direct Connect
# with DXGW




Existing remote access methods

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

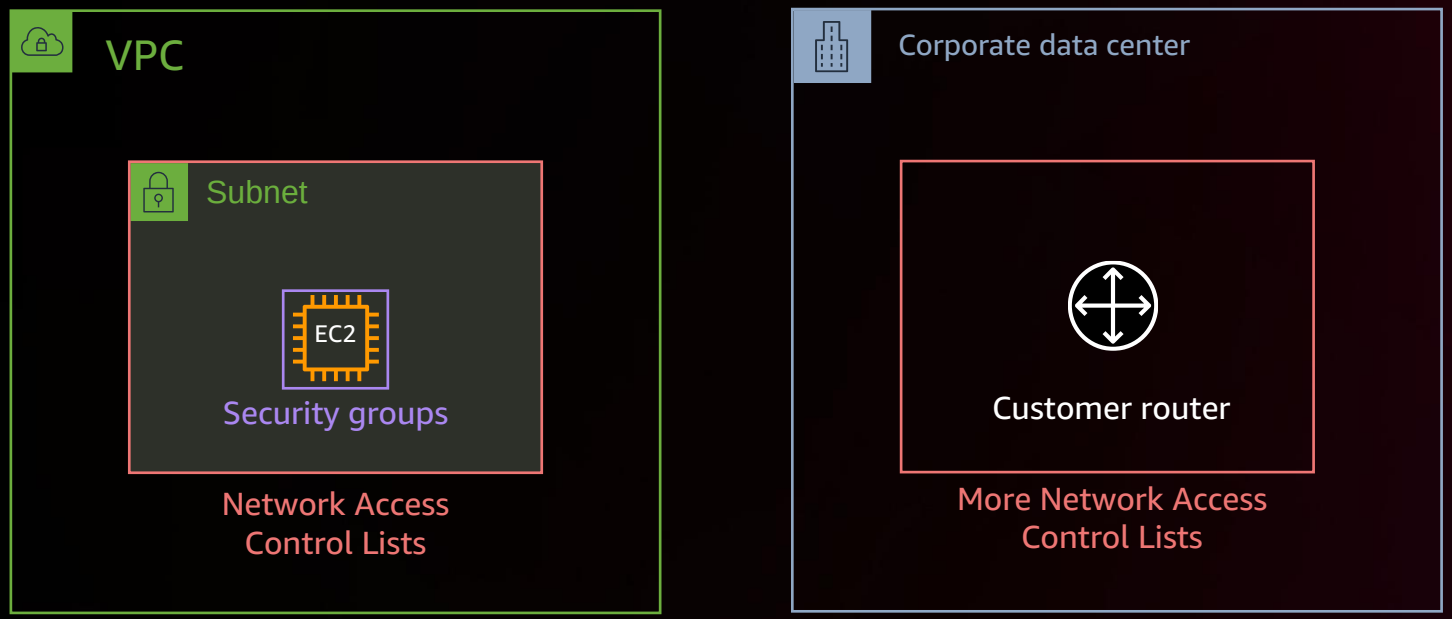
# AWS Direct Connect
## with Transit Gateway




Existing remote access methods

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

# Today, in many cases:
# Access control is done via the network




Existing remote access methods

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

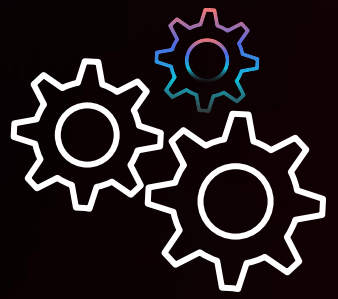
# AWS Verified Access

## SECURE ACCESS TO CORPORATE APPLICATIONS WITHOUT A VPN



### IMPROVE SECURITY POSTURE

Evaluates each user request in real-time using identity and device posture



### SIMPLIFY OPERATIONS

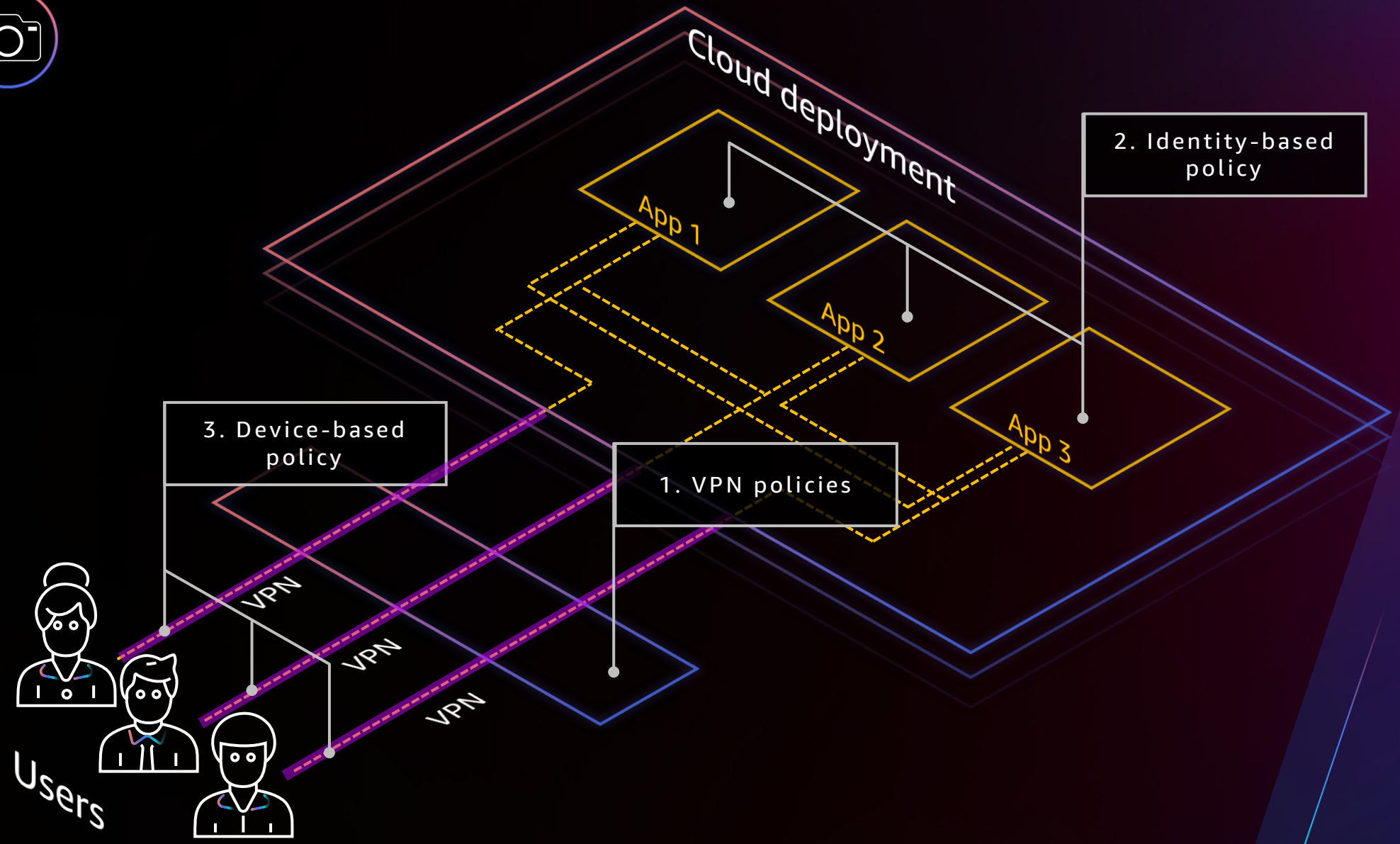
Onboard applications using a few clicks, manage all policies centrally



### INCREASE WORKFORCE MOBILITY

Users access applications with a web-browser, without any additional agents

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

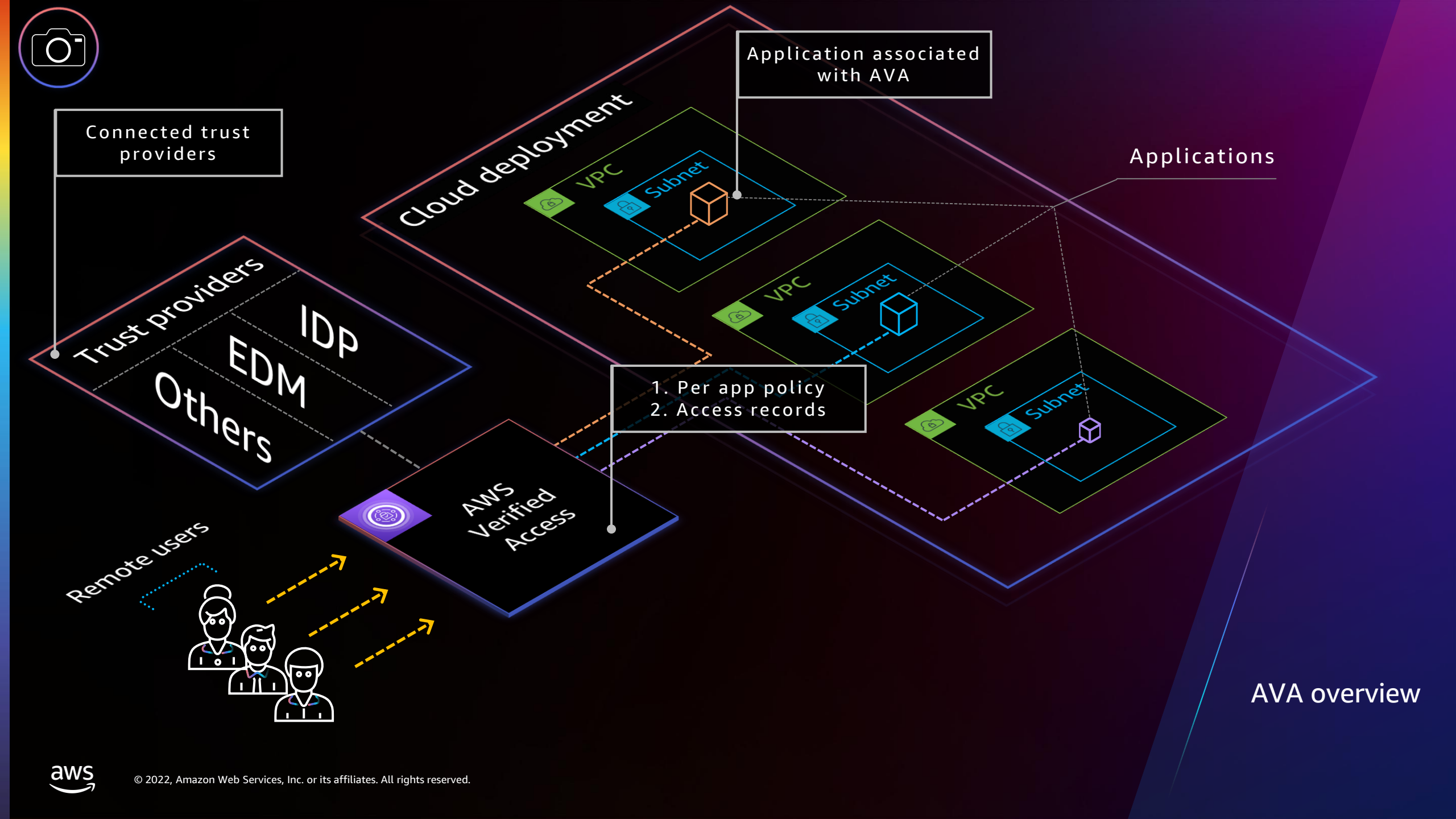



1
VPN policies

2
Identity-based policy

3
Device-based policy

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




# AVA overview

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

# AWS Verified Access
# Partners

## Trust providers

### Contextual data partners

Behavioral analytics & geolocation and more

### IdP partners

Provides users identity

### Device security partners

Provides device context

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

# AWS Verified Access Partners

## SIEM/OBSERVABILITY PARTNERS

Onboard applications using a few clicks, manage all policies centrally

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

# AWS Verified Access Partners

## Network management providers

Use Verified Access to build a managed Network

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

# AWS Verified Access Partners

## Trust/Network Providers

























## SIEM/Observability Providers

















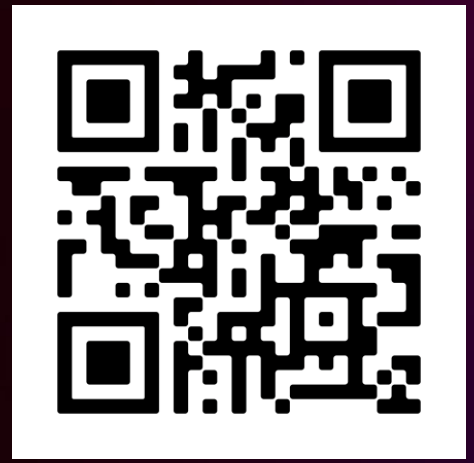





aws

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

# AWS Verified Access



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

# Thank you!

Matt Lehwess
@mlehwess

Alex Huides
linkedin.com/in/rodicaalexandrahuides/



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

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