

Architecting networks on AWS with IPv6

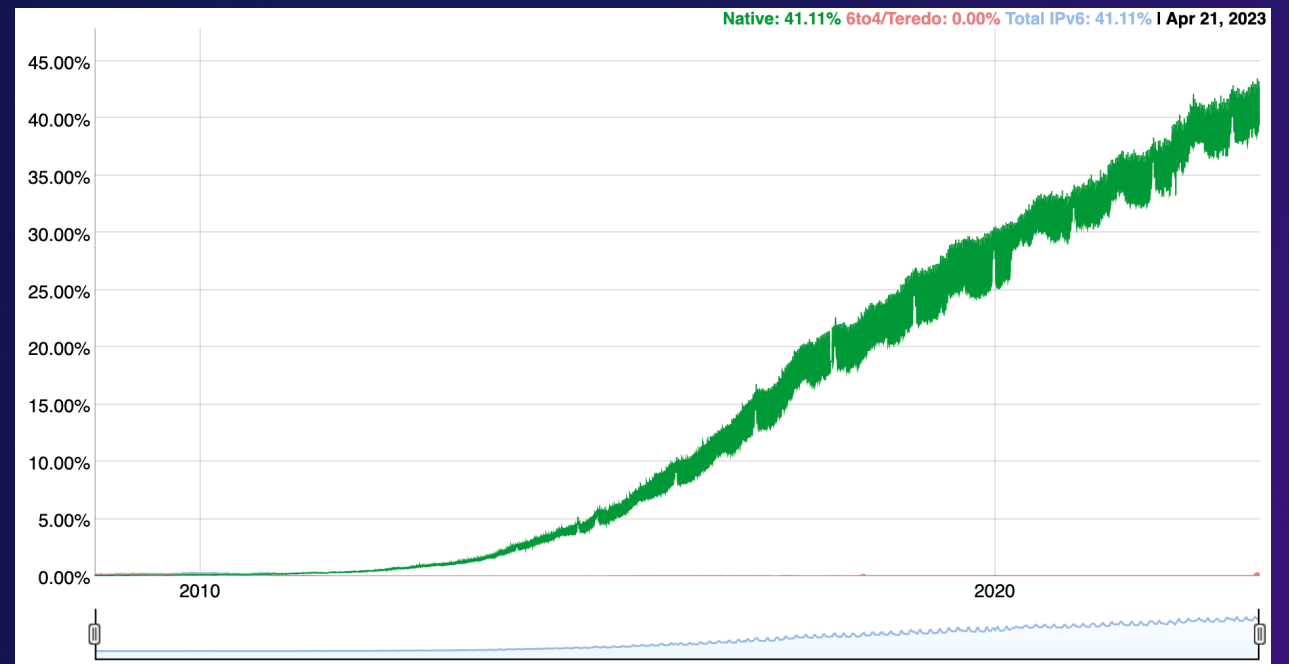
Alexandra Huides

Principal Solutions Architect - Networking Specialist
AWS Strategic Accounts



IPv6 adoption

- Roughly 40% of clients on the internet can connect over IPv6
- France, India, Germany, Greece, Saudi Arabia, Malaysia have over 60% of clients connecting over IPv6
- In Jan 2023, US reached over 50% of clients connecting over IPv6



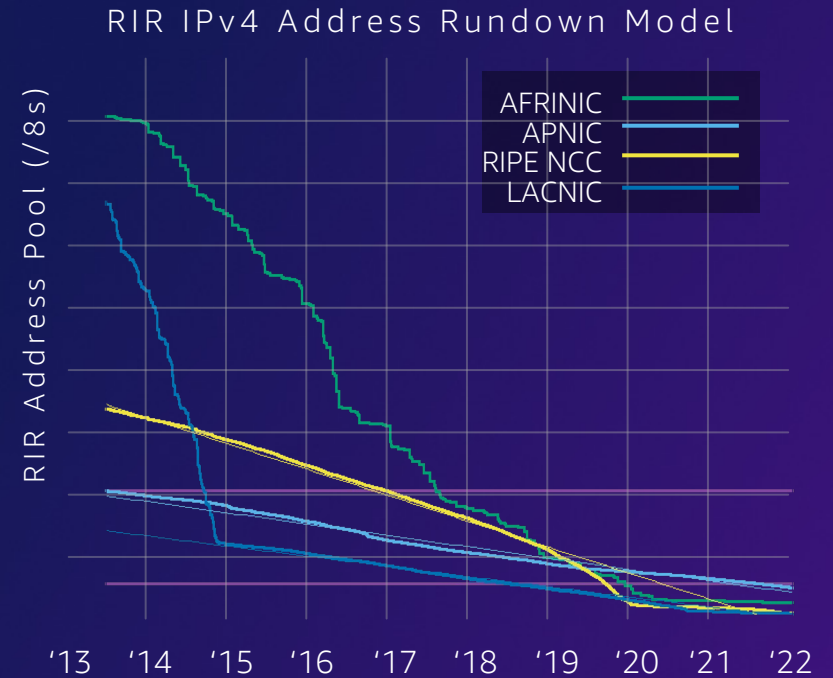
Source: [Google IPv6](#)

IPv4 exhaustion

Private v4

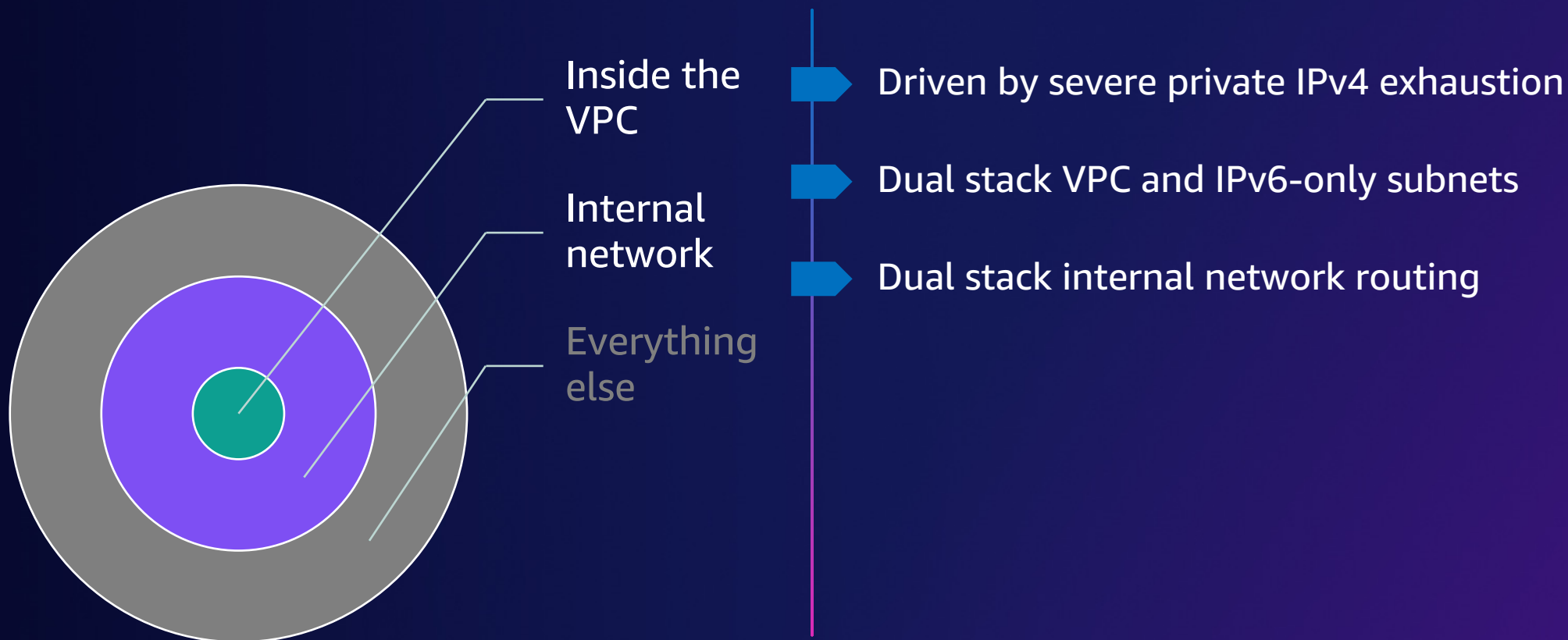
| Class | Private Address Range |
|-------|-------------------------------|
| A | 10.0.0.0 – 10.255.255.255 |
| B | 172.16.0.0 – 172.31.255.255 |
| C | 192.168.0.0 – 192.168.255.255 |

Public v4

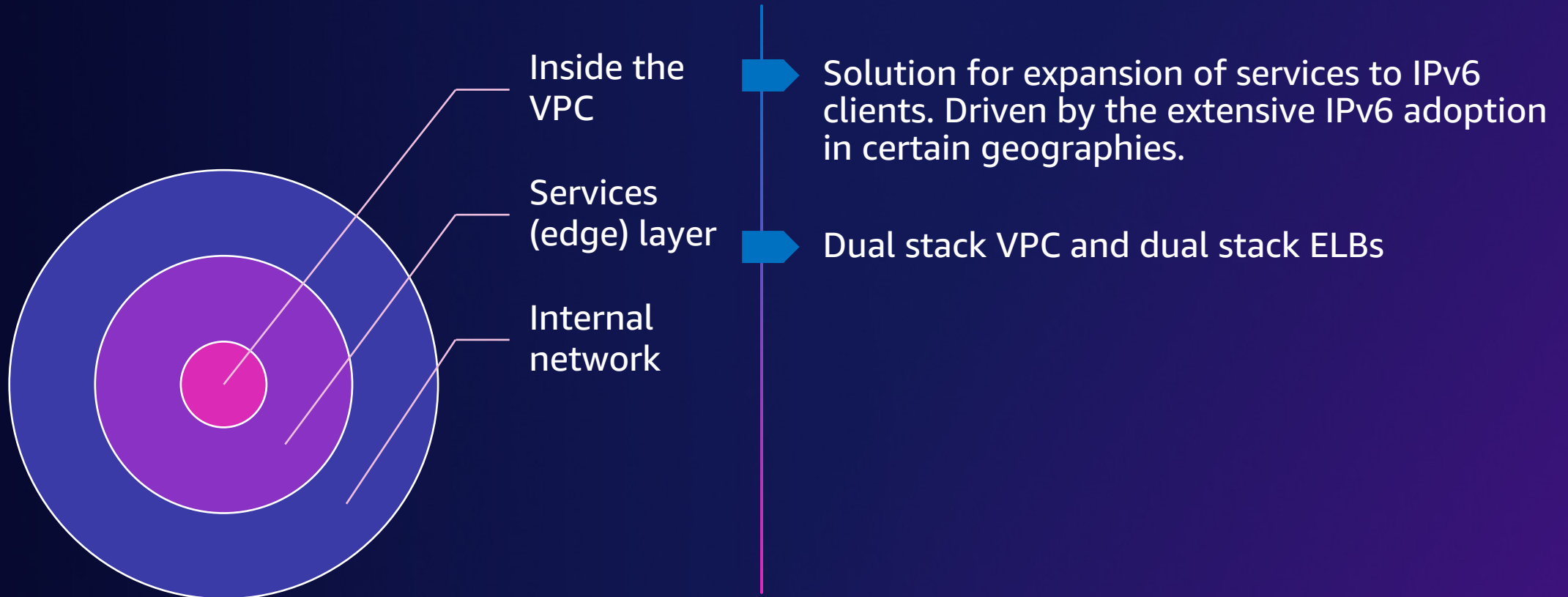


Source: <https://ipv4.potaroo.net/>

Internal IPv6 adoption on AWS



Edge-first IPv6 adoption on AWS



Amazon VPC IP Address Manager

START WITH AN IPV6 ADDRESSING PLAN

Public scope



Amazon VPC and IPv6

ASSIGN IPv6 ADDRESSES TO YOUR VPCs

Dual stack Amazon VPC

 IPv6 CIDR blocks

Edit CIDRs [Info](#)

Add or remove CIDR blocks for your VPC.

IPv4 CIDRs [Info](#)

| CIDR | Status | |
|------------------------------------|--------------|-------------------------|
| 10.0.0.0/16 | ✔ Associated | <button>Remove</button> |
| <button>Add new IPv4 CIDR</button> | | |

AWS assigned CIDR
(random or from a contiguous block)

IPv6 CIDRs [Info](#)

| CIDR (Network border group) | Pool | Status | |
|--------------------------------------|--------|--------------|-------------------------|
| 2600:1f18:46f9:be00::/56 (us-east-1) | Amazon | ✔ Associated | <button>Remove</button> |
| <button>Add new IPv6 CIDR</button> | | | |

Close



Edit CIDRs [Info](#)

Add or remove CIDR blocks for your VPC.

IPv4 CIDRs [Info](#)

| CIDR | Status | |
|------------------------------------|--------------|-------------------------|
| 10.10.10.0/24 | ✔ Associated | <button>Remove</button> |
| <button>Add new IPv4 CIDR</button> | | |

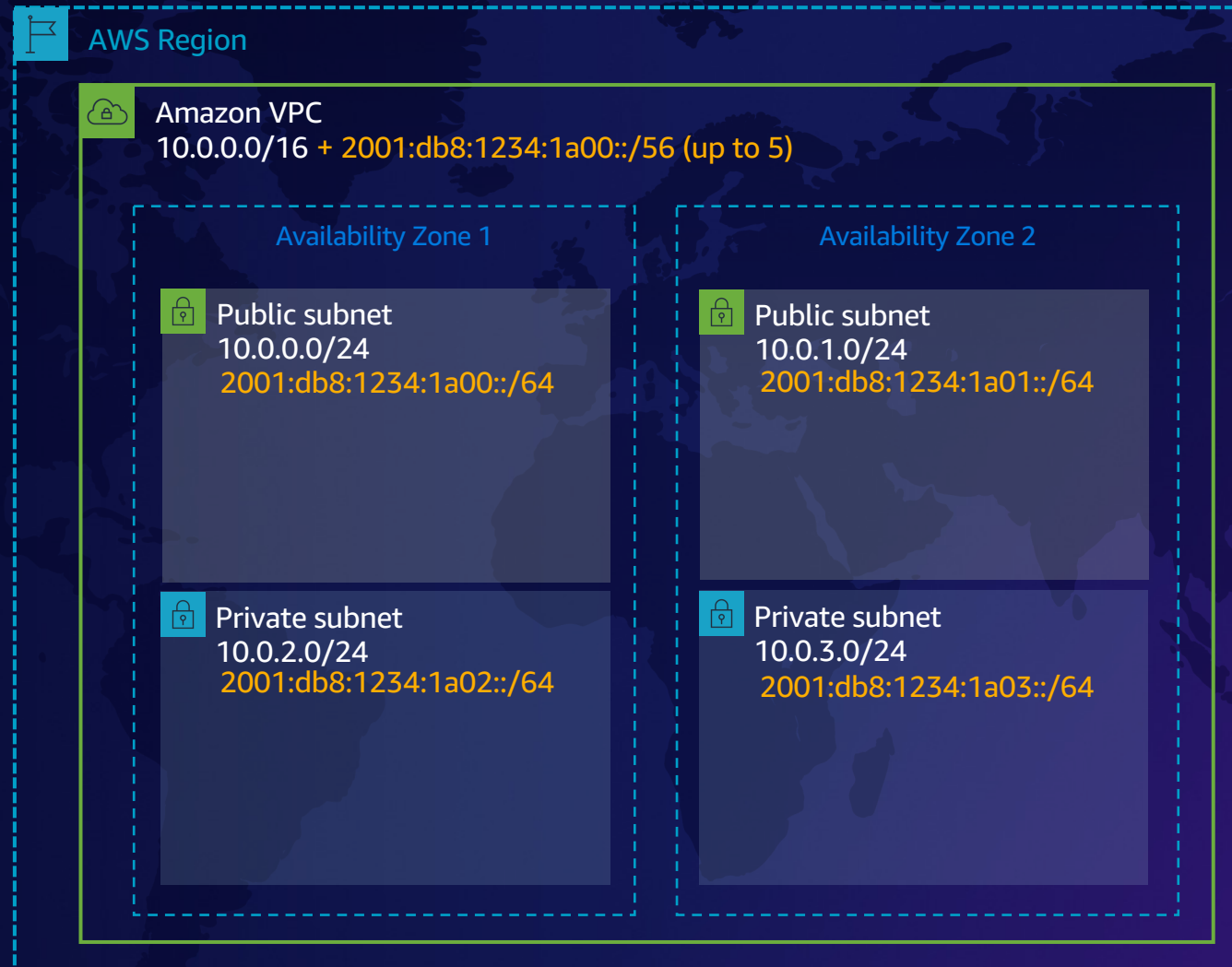
BYOIPv6 contiguous pool

IPv6 CIDRs [Info](#)

| CIDR (Network border group) | Pool | Status | |
|------------------------------------|-----------------------------|--------------|-------------------------|
| 2605:9cc0:1ff0::/56 (us-east-1) | ipam-pool-07e09d88ad9335236 | ✔ Associated | <button>Remove</button> |
| <button>Add new IPv6 CIDR</button> | | | |

Close

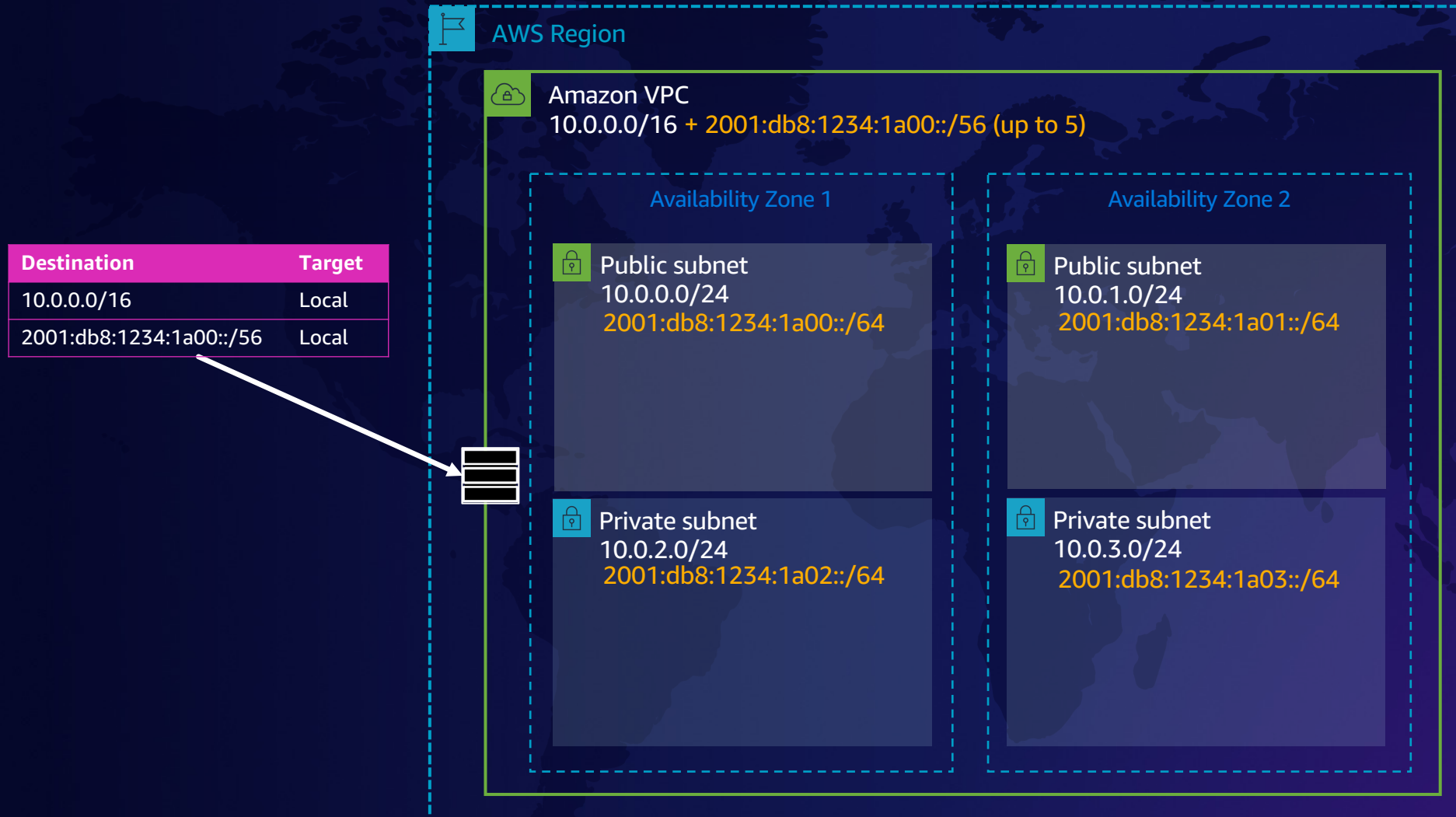
Dual stack Amazon VPC – CIDRs



Dual stack Amazon VPC

- IPv6 CIDR blocks
- IPv6 VPC routing

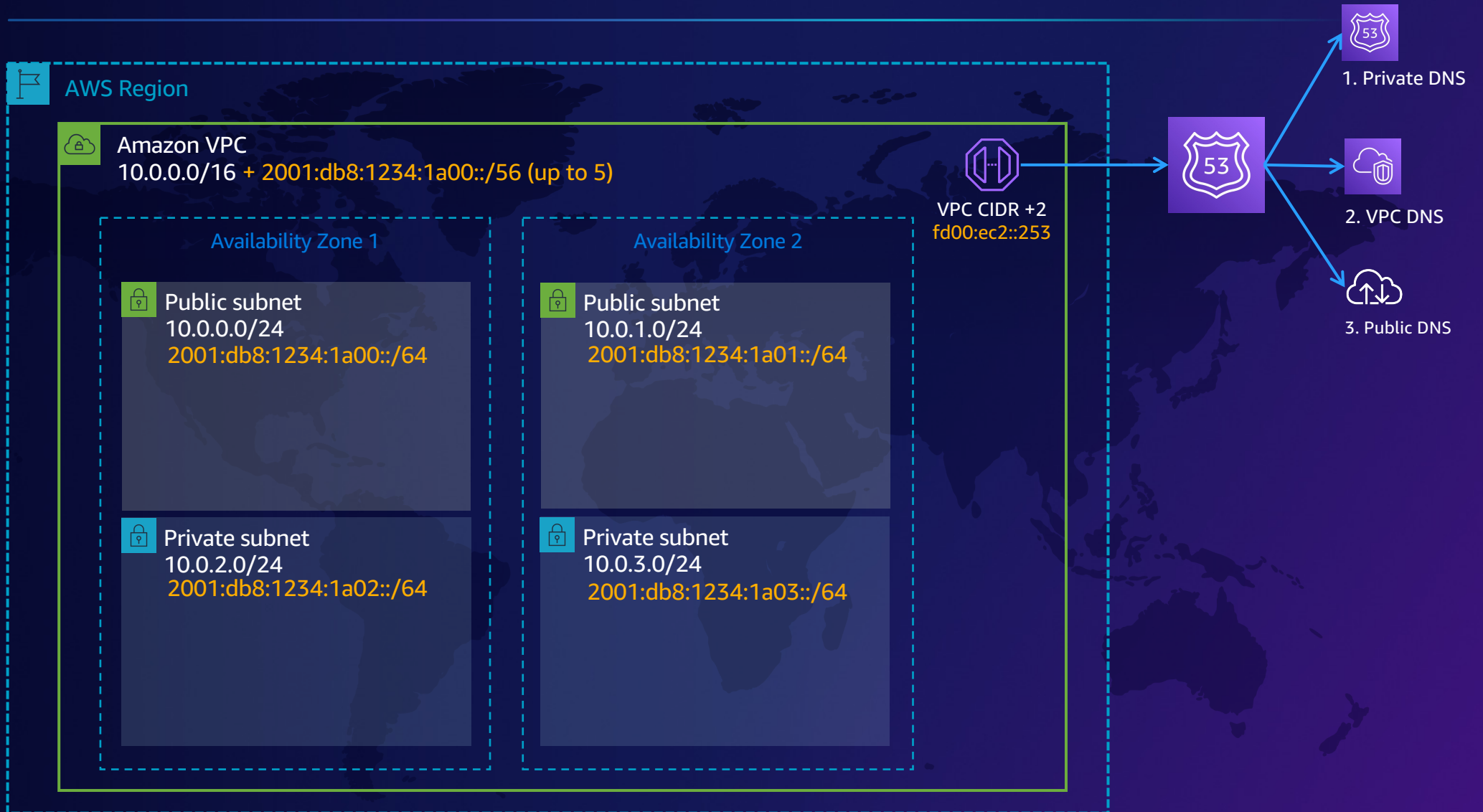
Dual stack Amazon VPC - Routing



Dual stack Amazon VPC

- IPv6 CIDR blocks
- IPv6 VPC routing
- VPC DNS

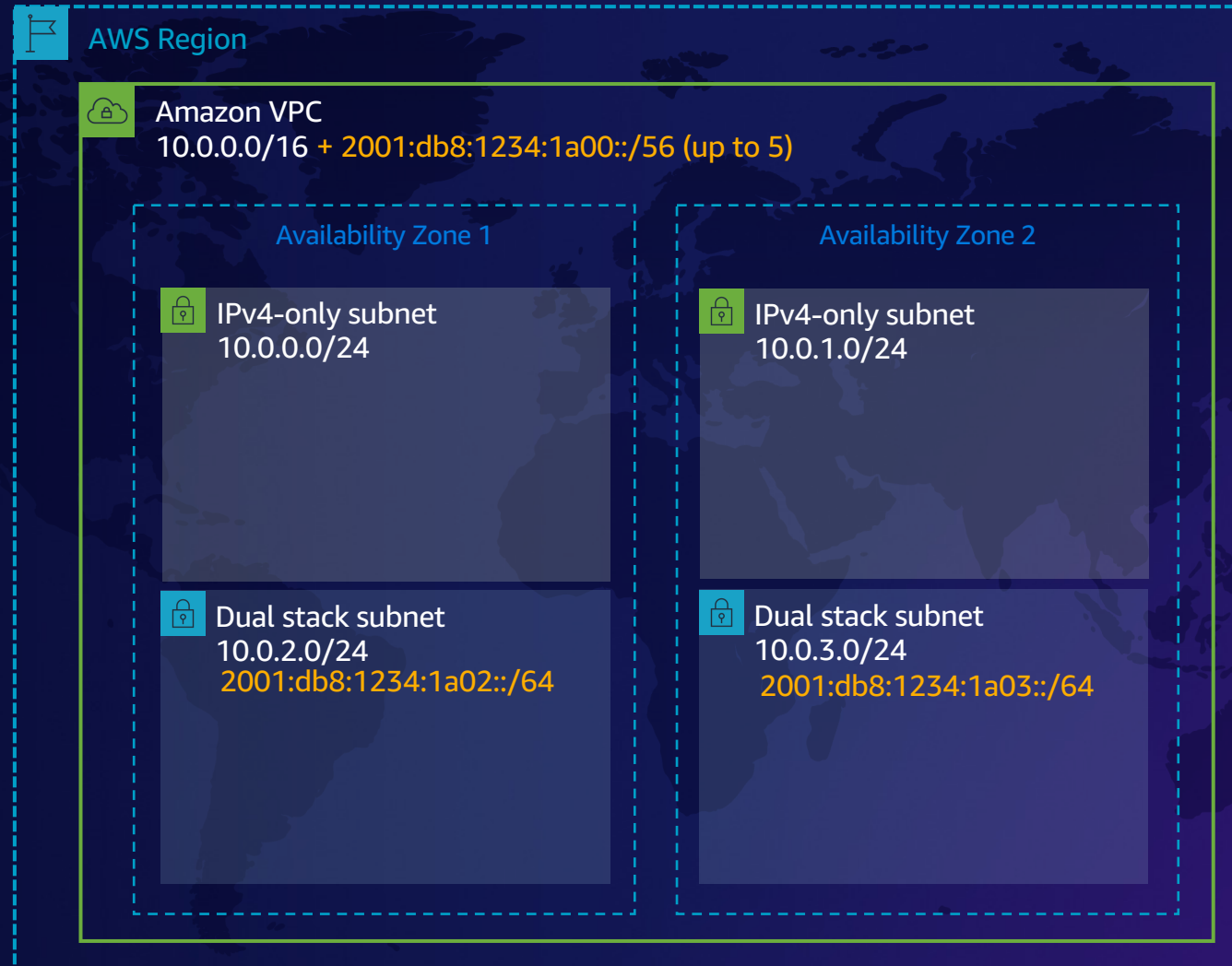
Dual stack Amazon VPC - DNS



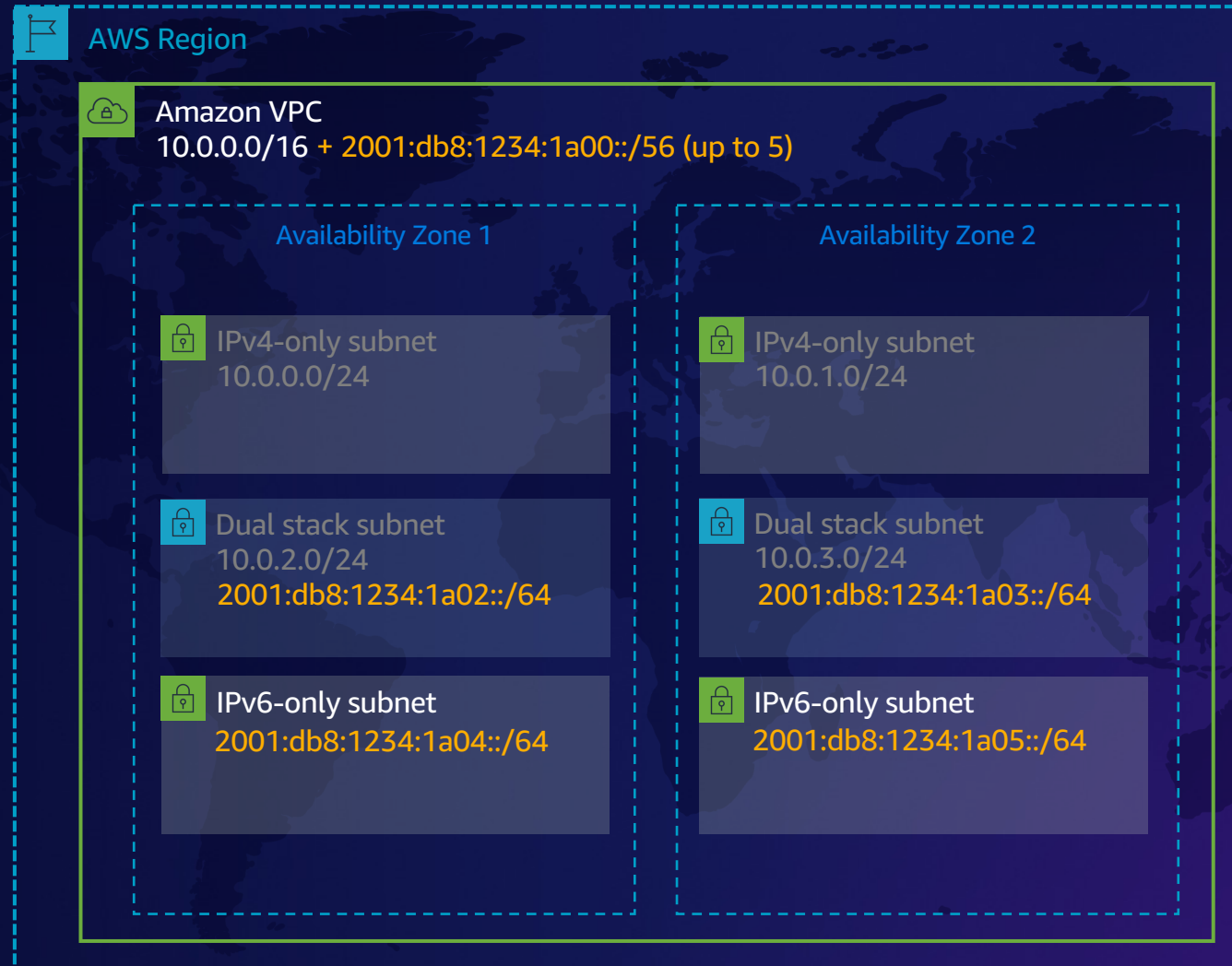
Dual stack Amazon VPC

- IPv6 CIDR blocks
- IPv6 VPC routing
- VPC DNS
- VPC Subnet types

Dual stack Amazon VPC – Subnet types



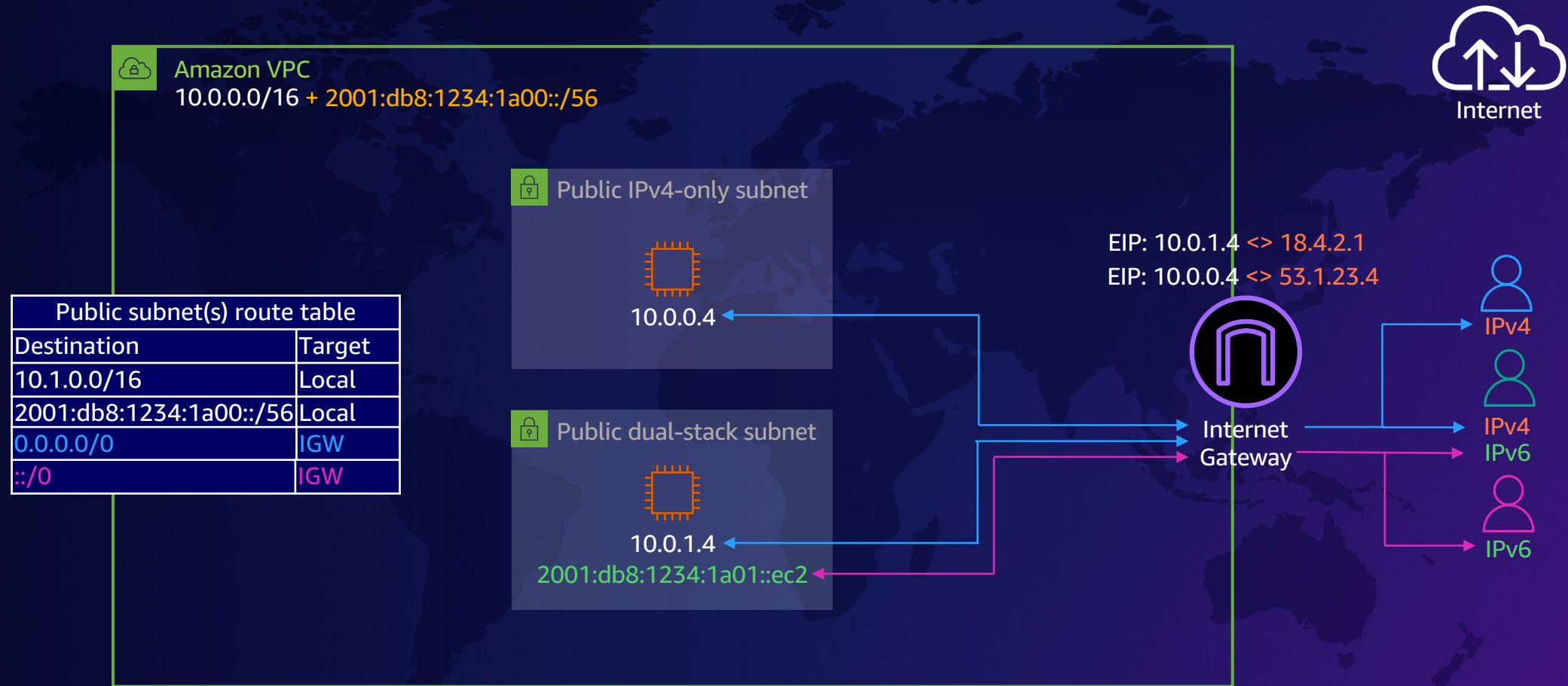
Dual stack Amazon VPC – Subnet types



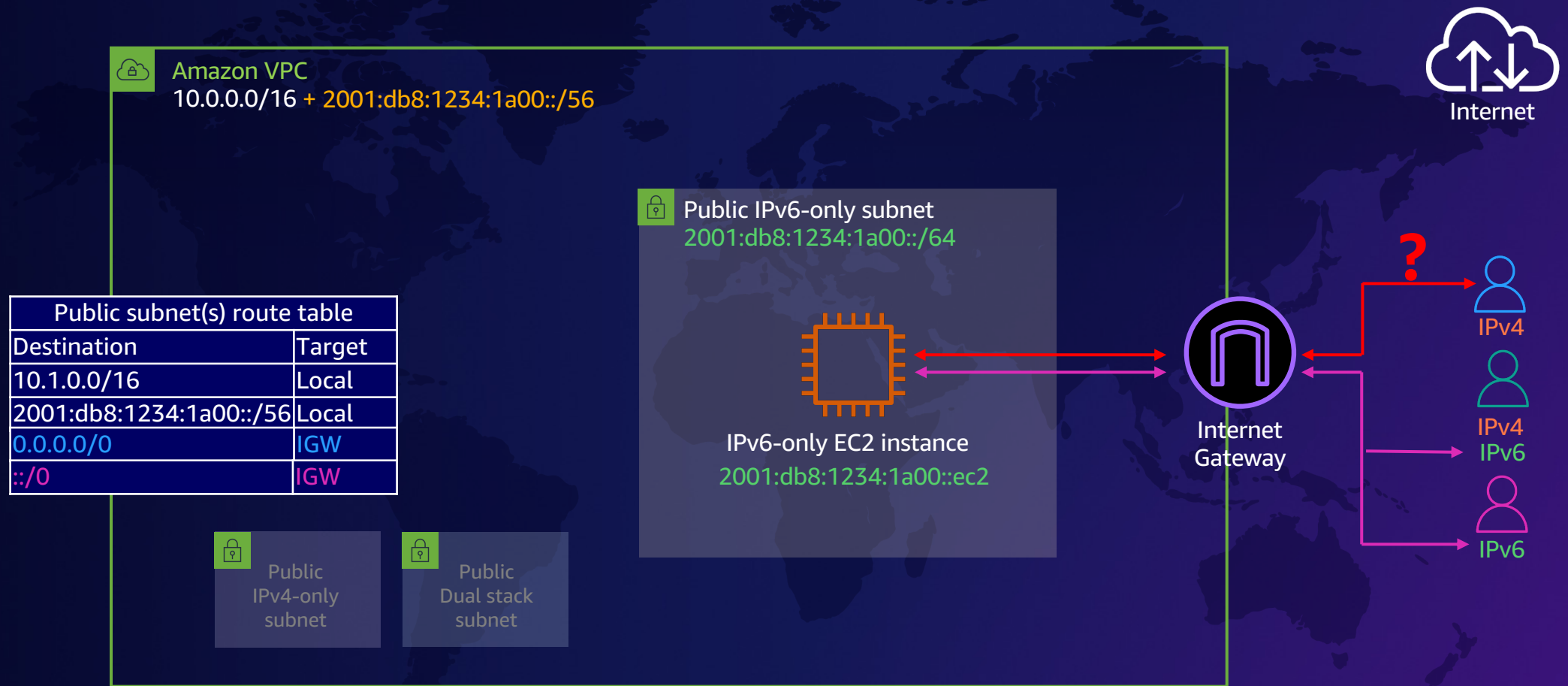
Dual stack Amazon VPC connectivity

 Internet connectivity

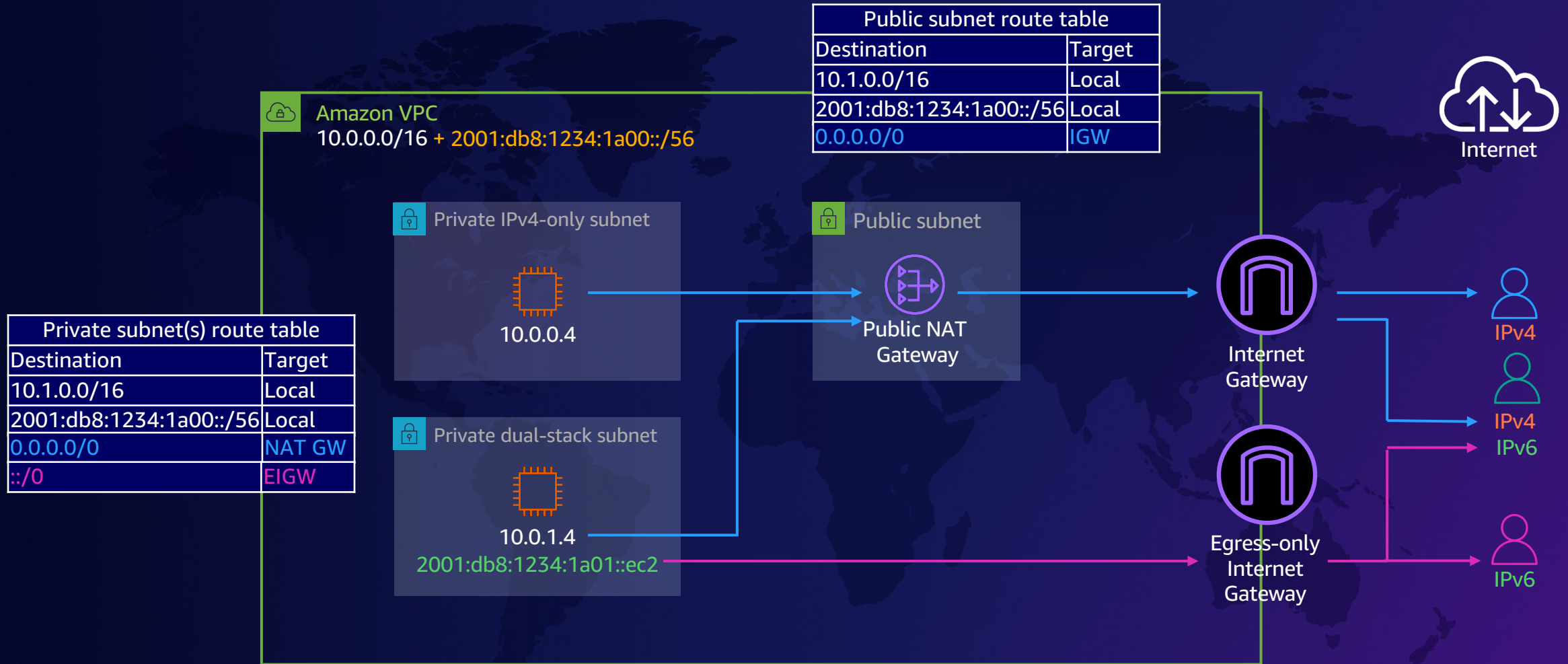
Amazon VPC – Public subnets



Amazon VPC – Public IPv6-only subnets

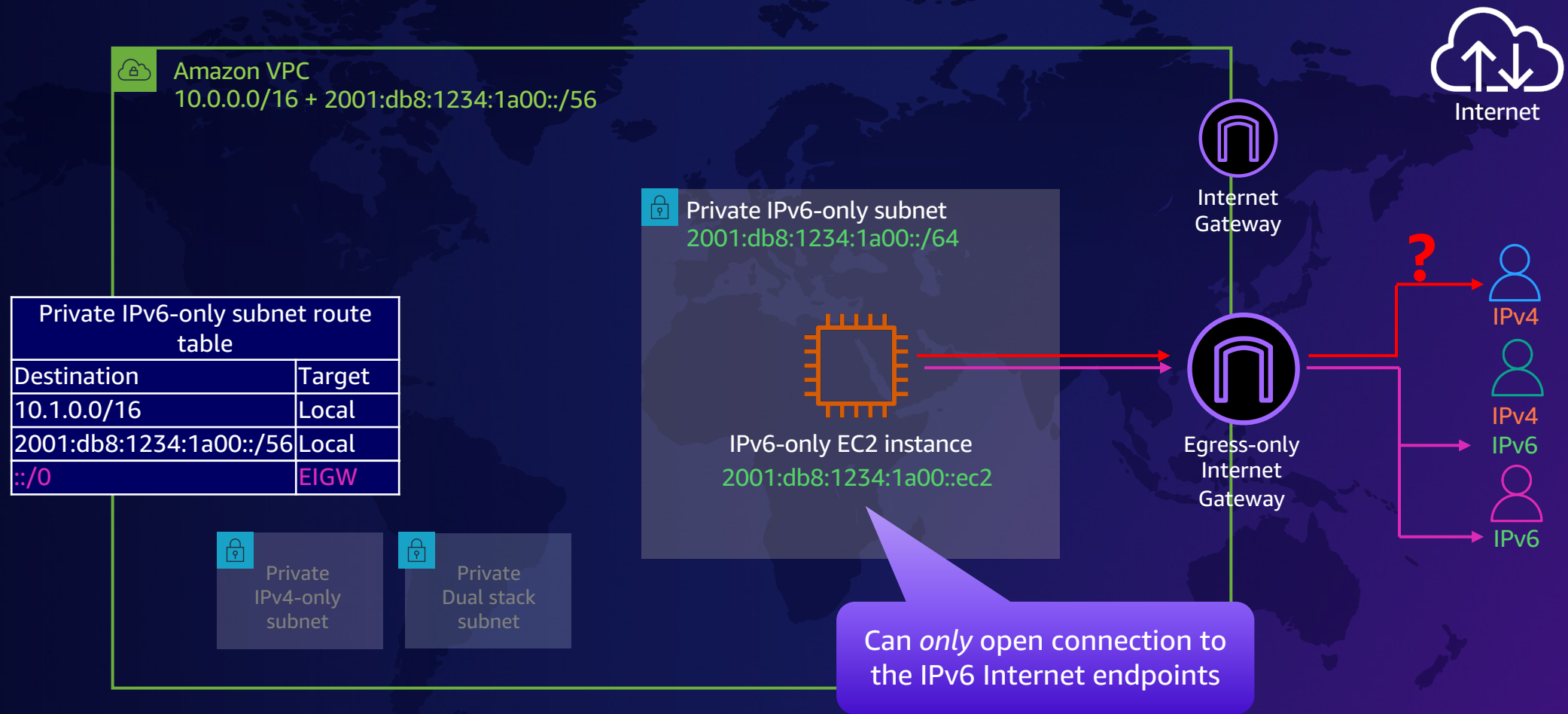


Amazon VPC – Private subnets

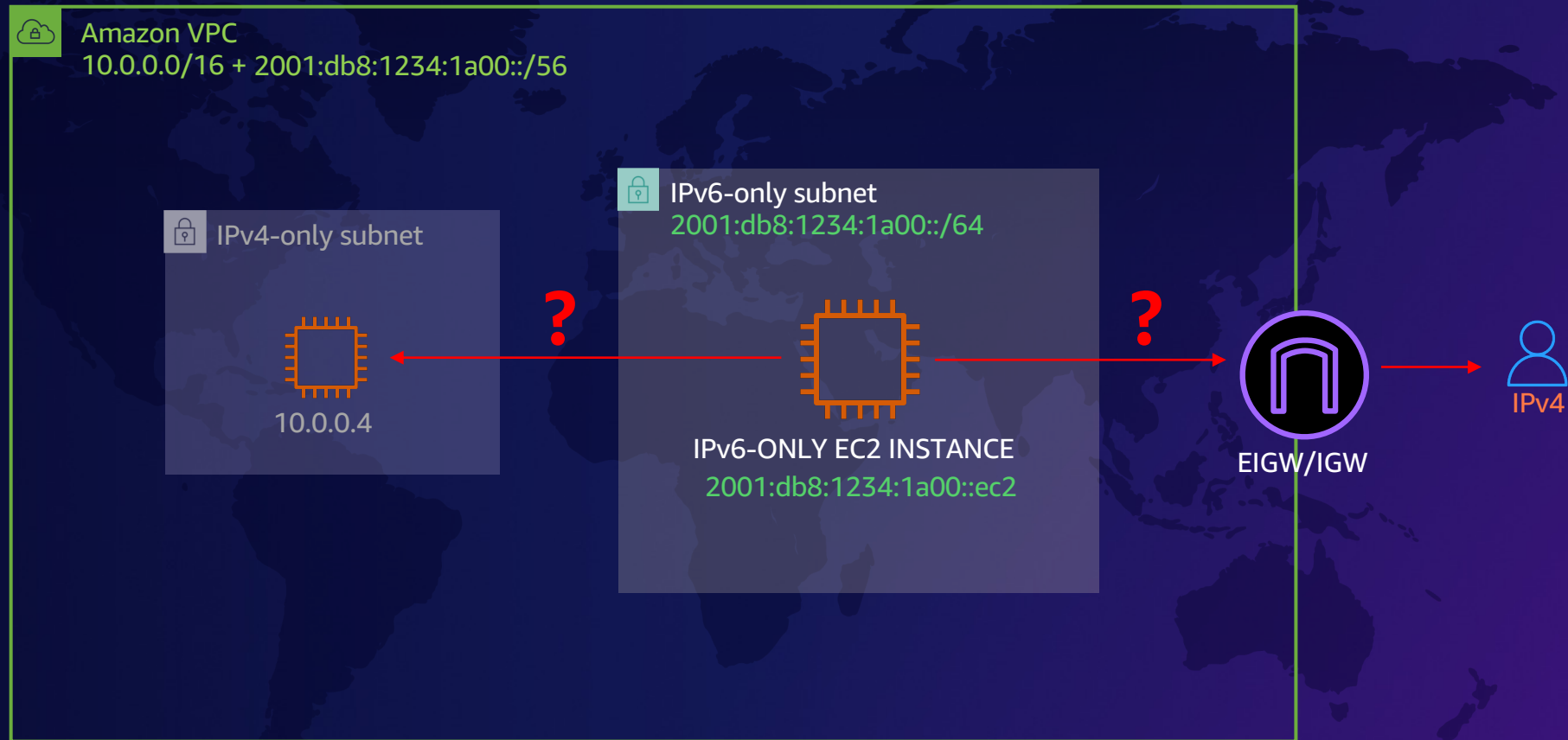


The EIGW does **not** allow internet connections to be opened to IPv6 resources in private subnets

Amazon VPC – Private IPv6-only subnets



Amazon VPC – How about IPv6 to IPv4?

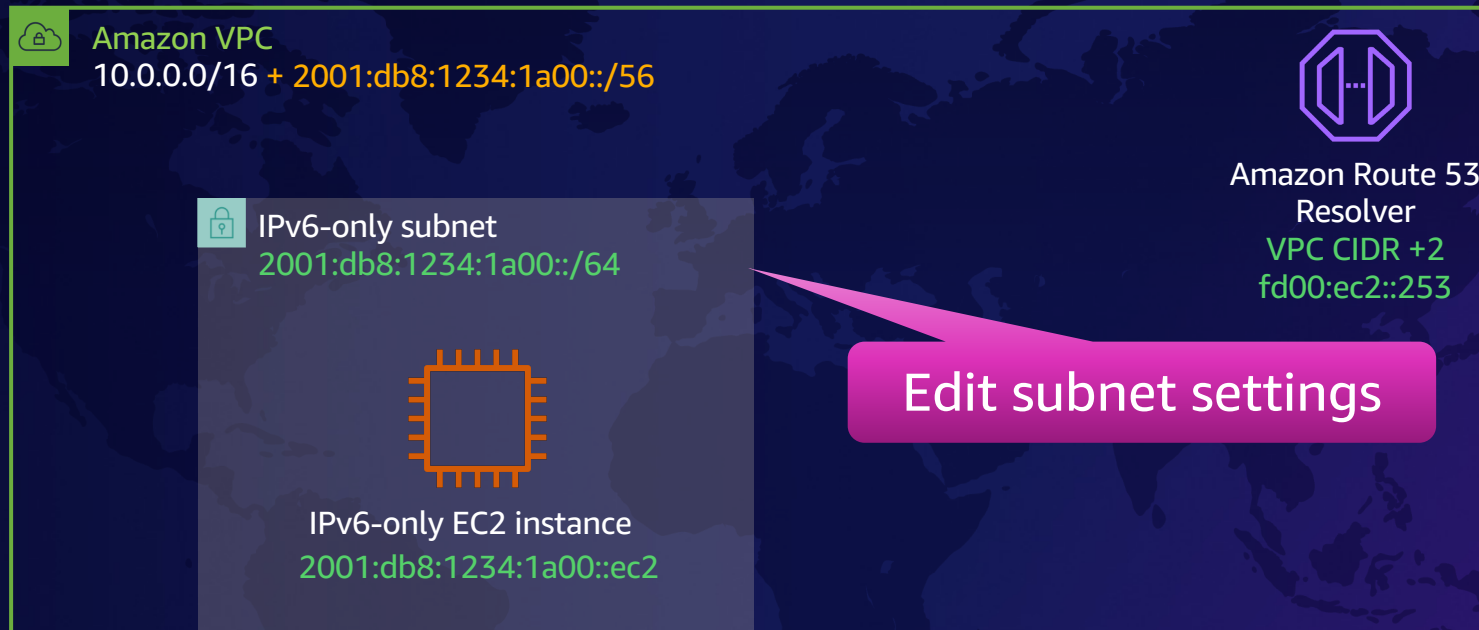


Dual stack

Amazon VPC connectivity

- Internet connectivity
- DNS64 and NAT64

What is DNS64?



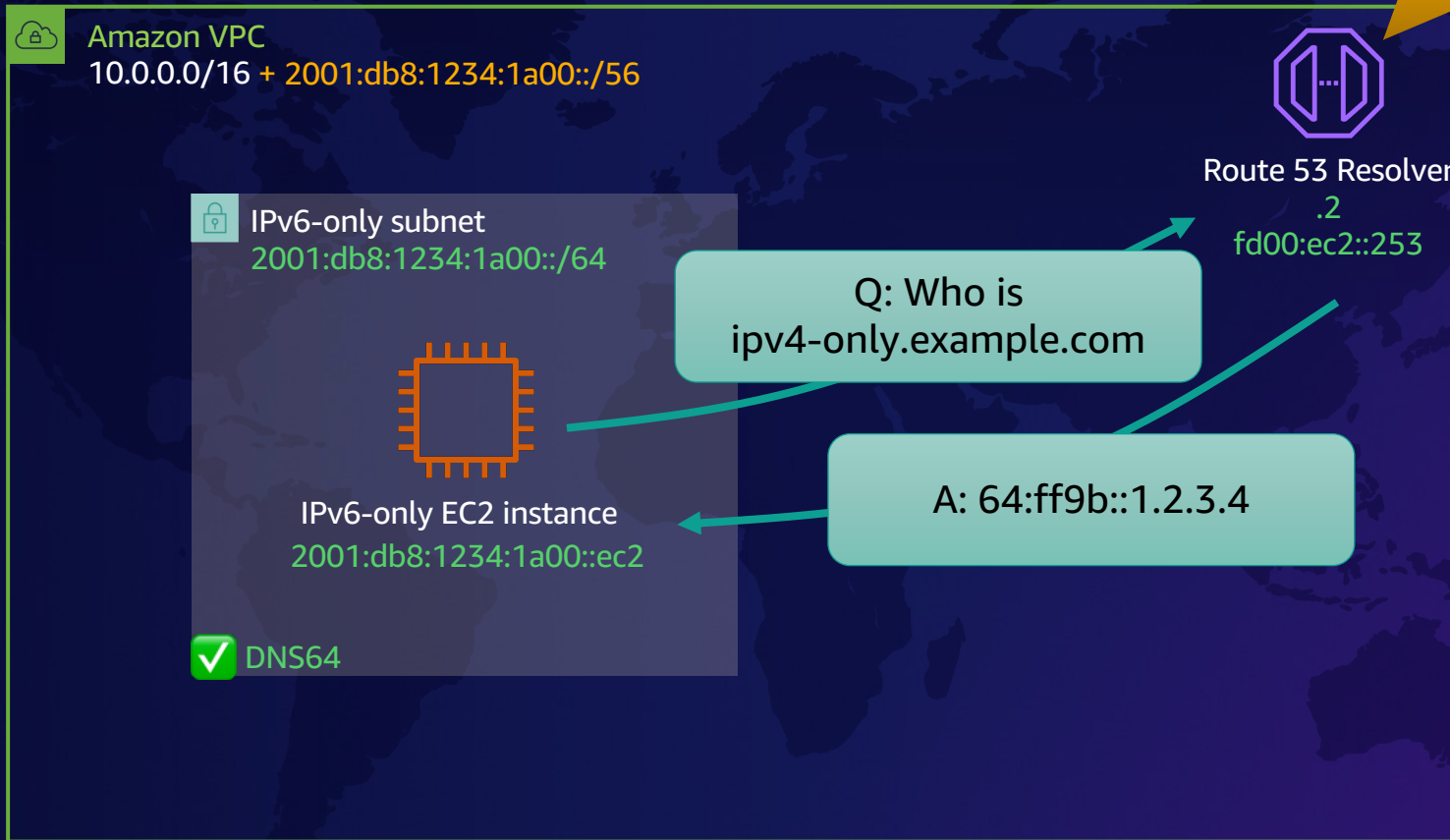
DNS64 settings

Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

Enable DNS64 [Info](#)

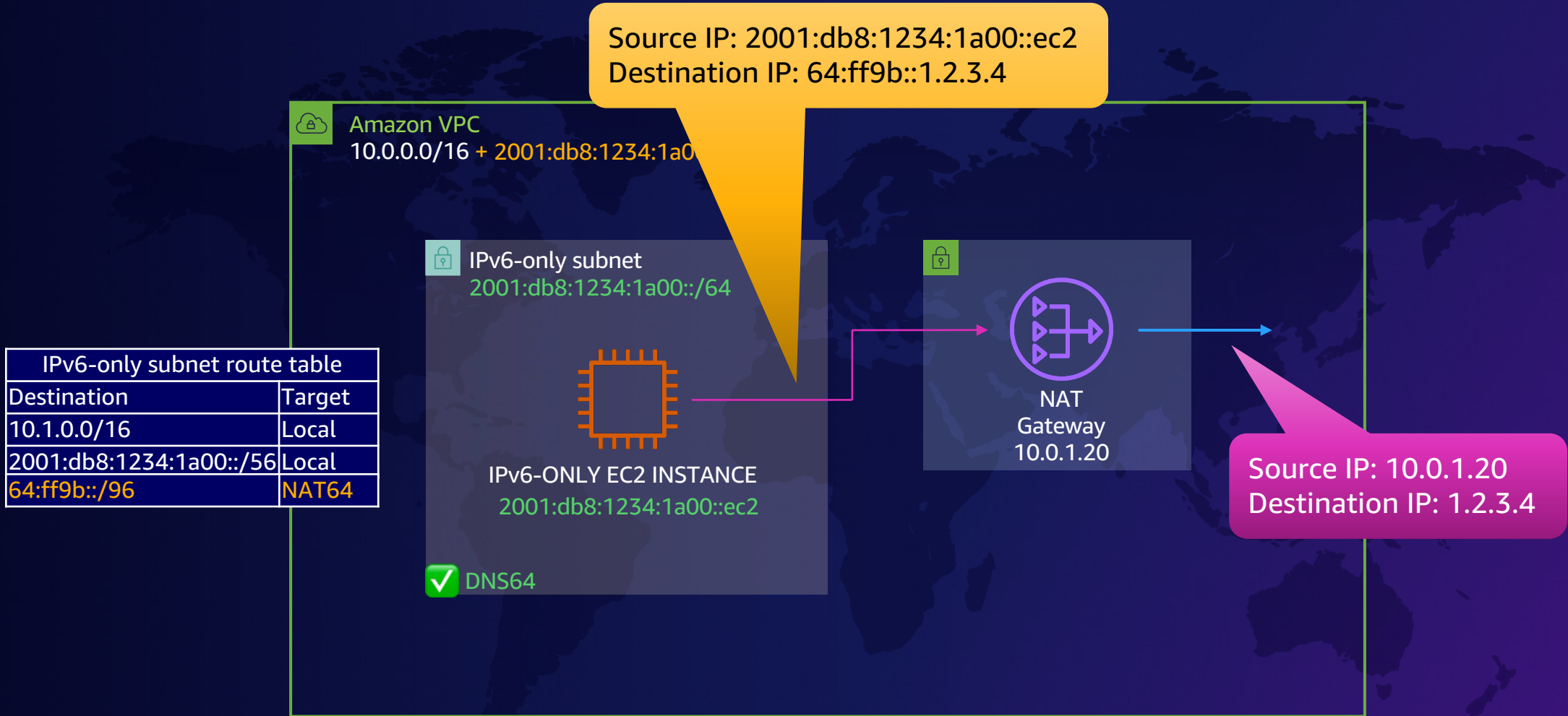
What is DNS64?

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

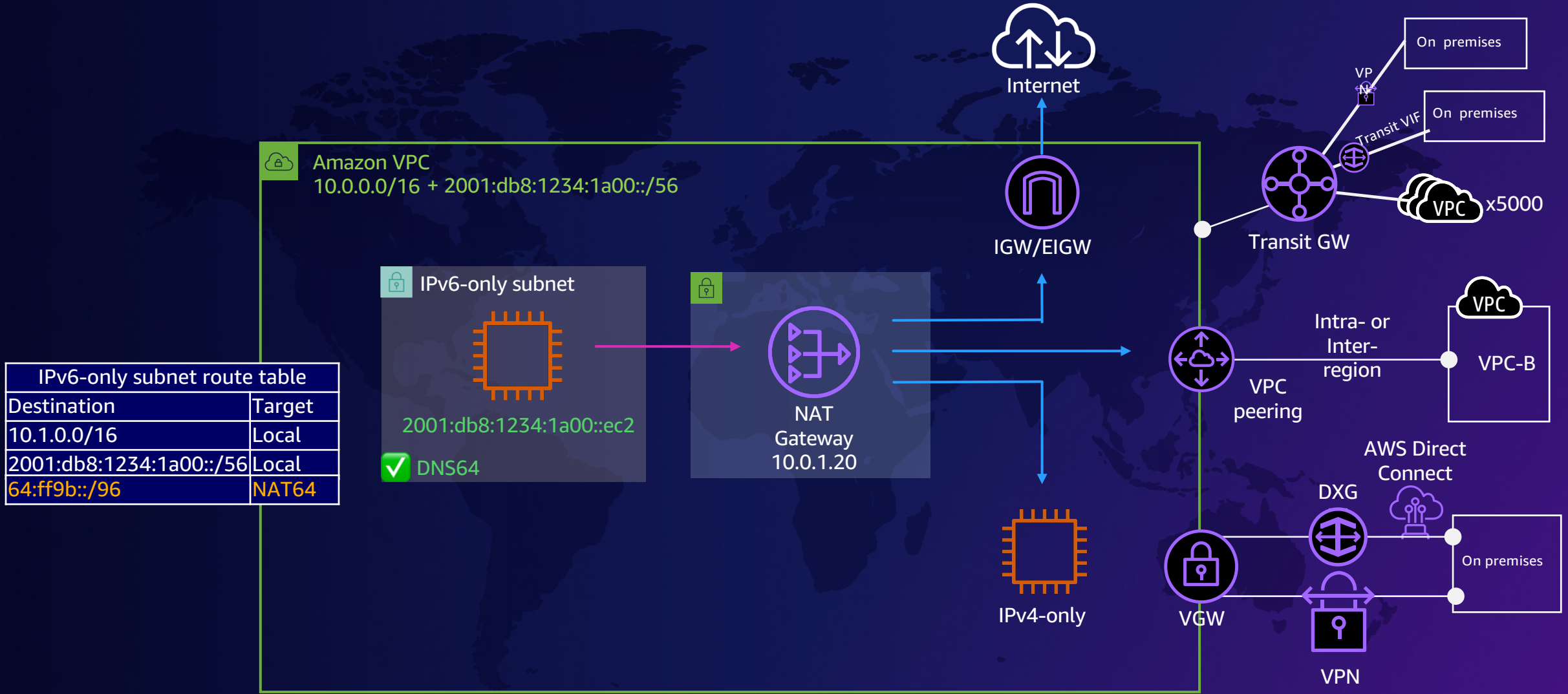


Traffic from the IPv6-only instances to the synthesized IPv6 address needs to go through **NAT64**

How does NAT64 work?



NAT64 and DNS64



| IPv6-only subnet route table | |
|------------------------------|--------|
| Destination | Target |
| 10.1.0.0/16 | Local |
| 2001:db8:1234:1a00::/56 | Local |
| 64:ff9b::/96 | NAT64 |

IPv6-only subnet

2001:db8:1234:1a00::ec2

✓ DNS64

NAT Gateway

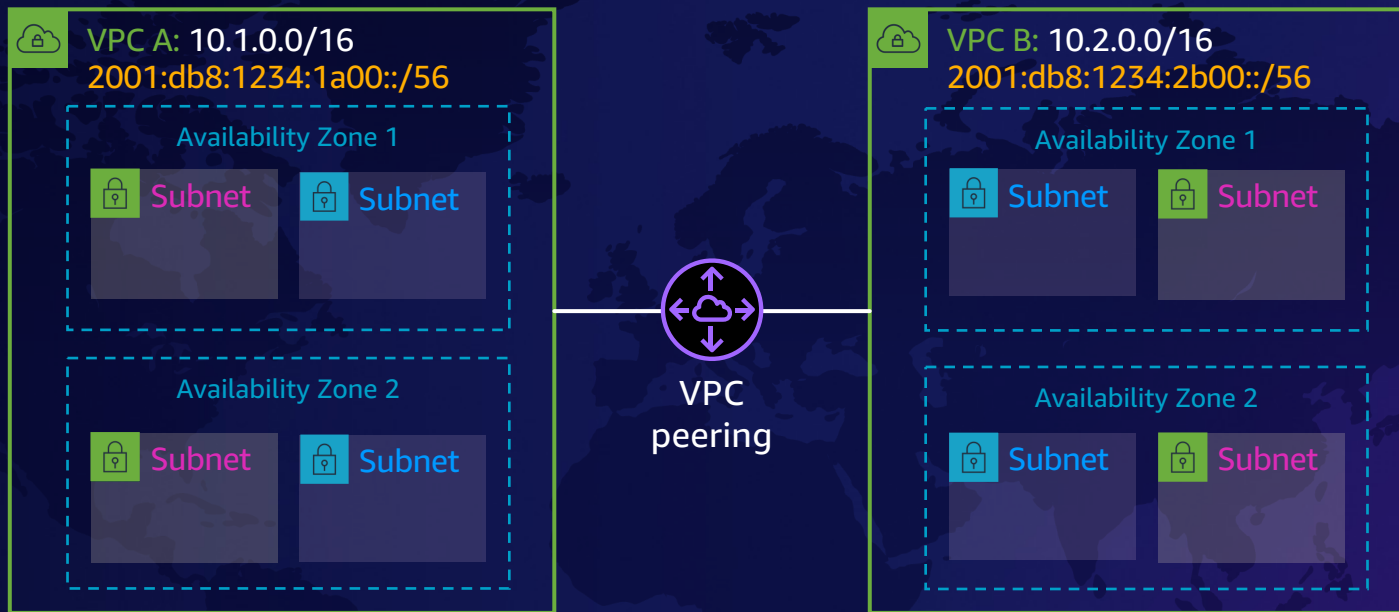
10.0.1.20

Dual stack

Amazon VPC connectivity

- Internet connectivity
- DNS64 and NAT64
- VPC connectivity on AWS

Amazon VPC Peering



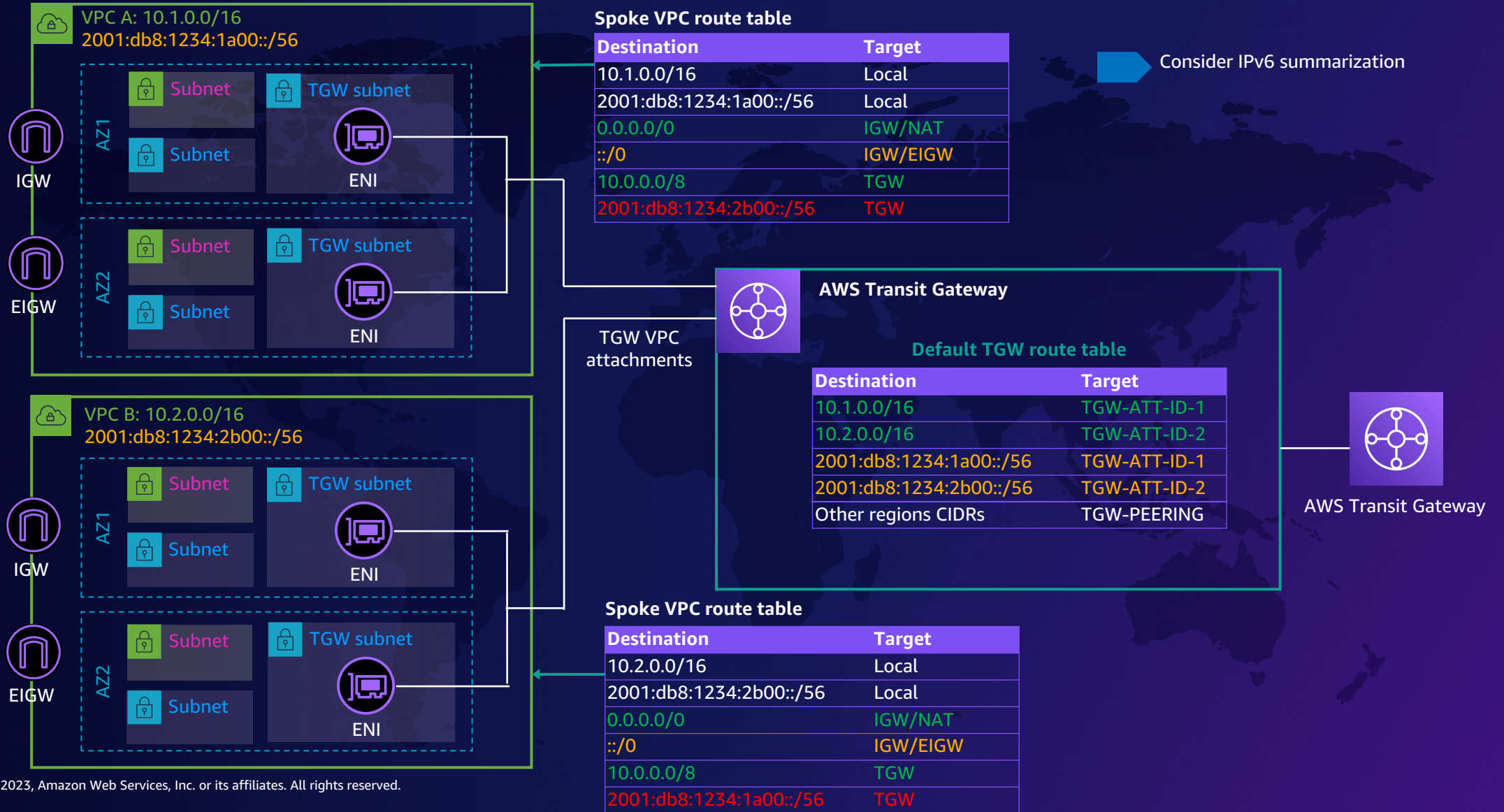
VPC A route table

| Destination | Target |
|-------------------------|--------|
| 10.1.0.0/16 | Local |
| 2001:db8:1234:1a00::/56 | Local |
| 10.2.0.0/16 | PCX-ID |
| 2001:db8:1234:2b00::/56 | PCX-ID |

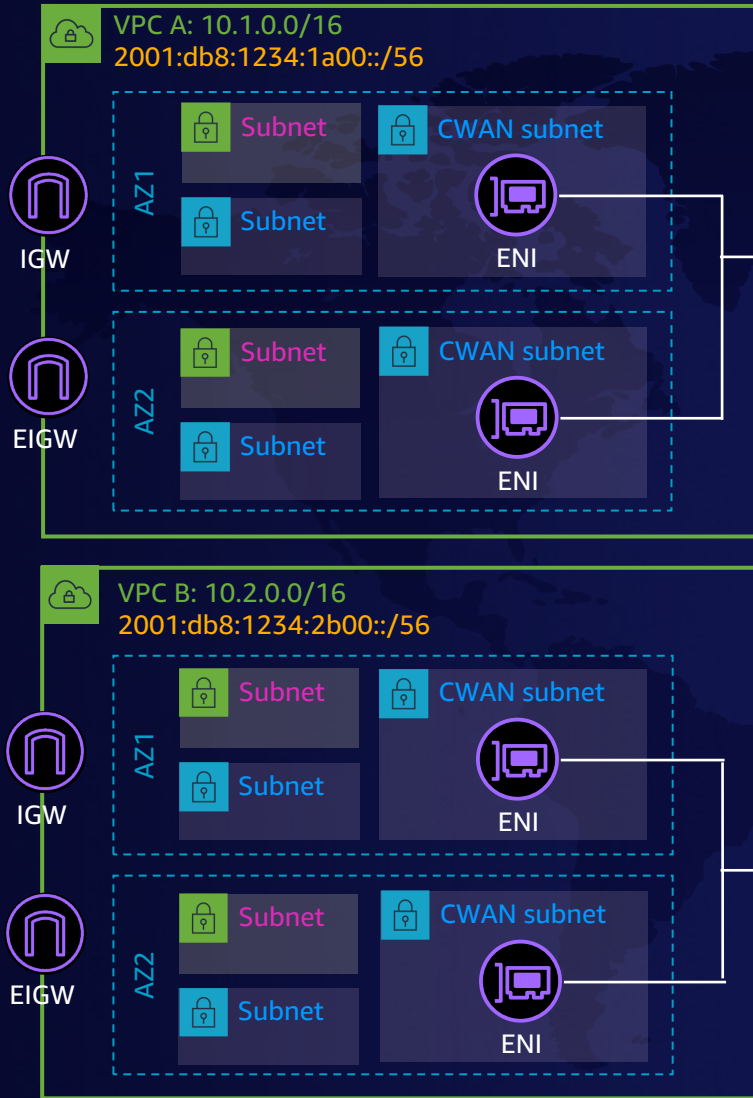
VPC B route table

| Destination | Target |
|-------------------------|--------|
| 10.2.0.0/16 | Local |
| 2001:db8:1234:2b00::/56 | Local |
| 10.1.0.0/16 | PCX-ID |
| 2001:db8:1234:1a00::/56 | PCX-ID |

AWS Transit Gateway



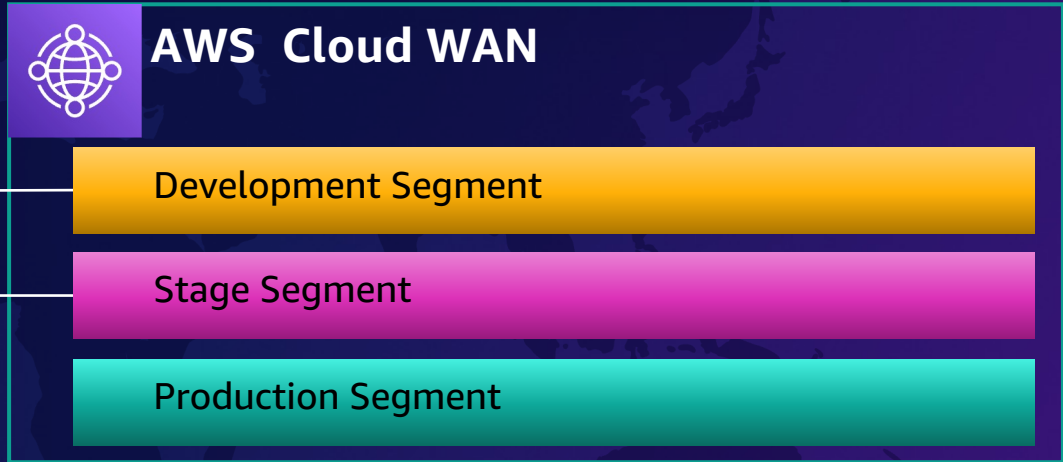
AWS Cloud WAN



Spoke VPC route table

| Destination | Target |
|-------------------------|--------------|
| 10.1.0.0/16 | Local |
| 2001:db8:1234:1a00::/56 | Local |
| 0.0.0.0/0 | IGW/NAT |
| ::/0 | IGW/EIGW |
| 10.0.0.0/8 | TGW |
| 2001:db8:1234:2b00::/56 | Core Network |

➔ Consider IPv6 summarization



Spoke VPC route table

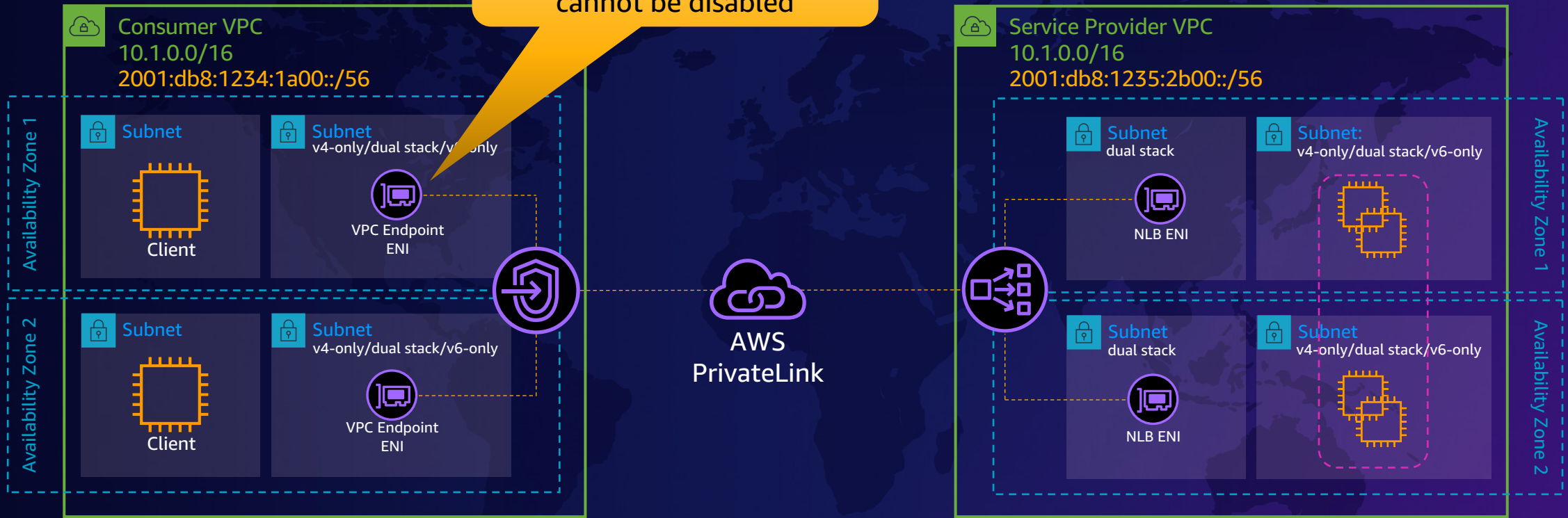
| Destination | Target |
|-------------------------|--------------|
| 10.2.0.0/16 | Local |
| 2001:db8:1234:2b00::/56 | Local |
| 0.0.0.0/0 | IGW/NAT |
| ::/0 | IGW/EIGW |
| 10.0.0.0/8 | TGW |
| 2001:db8:1234:1a00::/56 | Core Network |



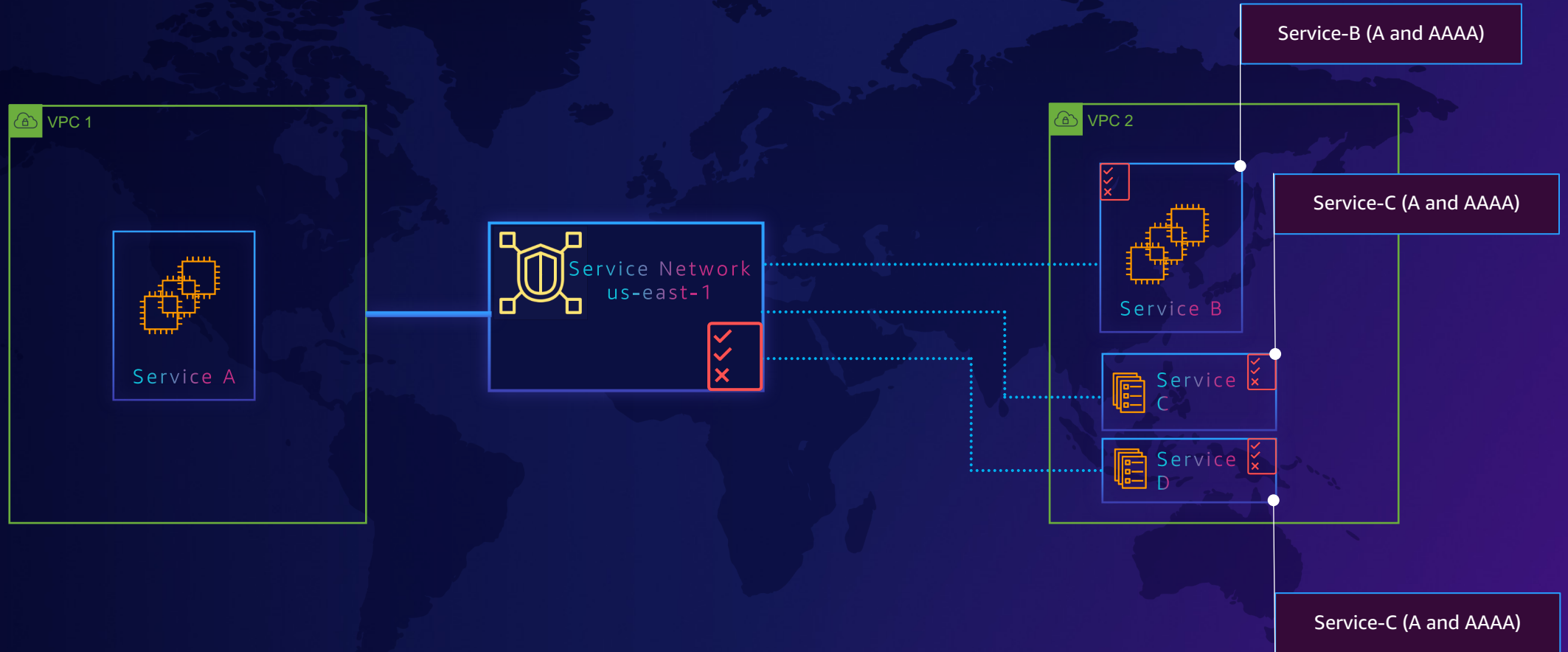
AWS TGW & Cloud WAN natively support IPv6 routing

AWS PrivateLink

For IPv6 – DenyAllIGWTraffic is enabled by default and cannot be disabled



Amazon VPC Lattice

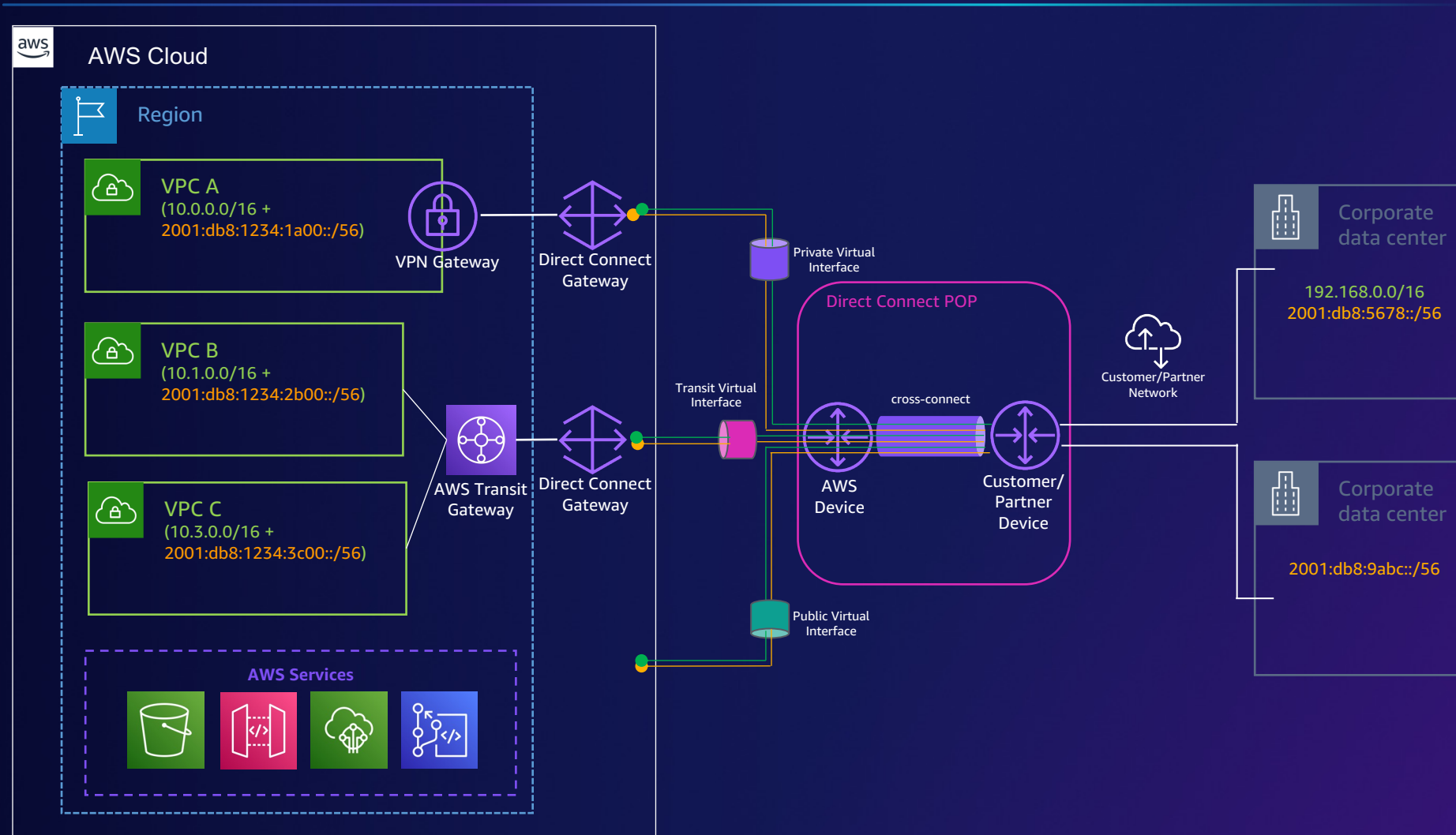


Dual stack

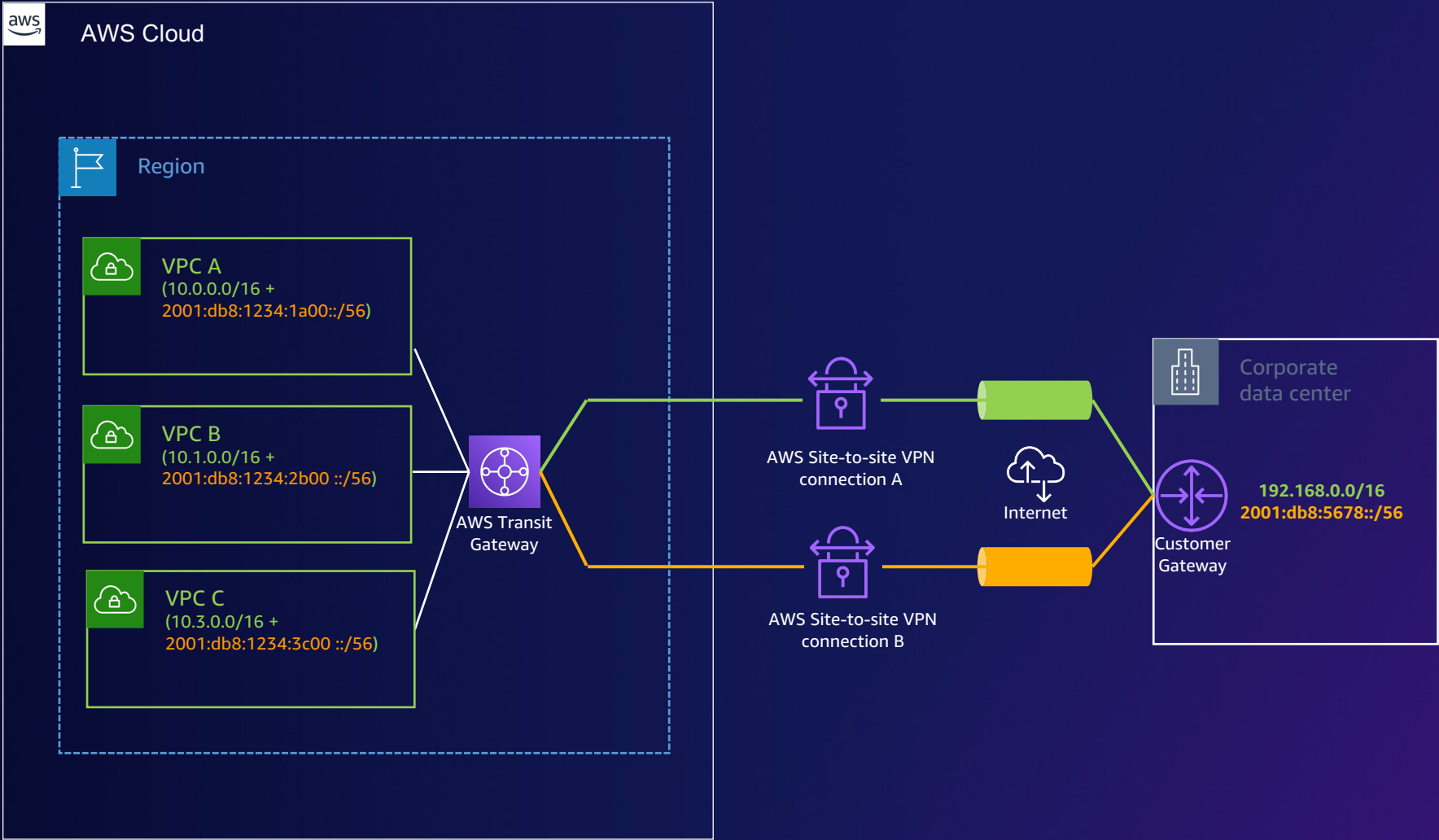
Amazon VPC connectivity

- Internet connectivity
- DNS64 and NAT64
- VPC connectivity on AWS
- VPC hybrid connectivity

AWS Direct Connect



AWS Site-to-Site VPN



Scaling application delivery on IPv6

AWS ELASTIC LOAD BALANCERS

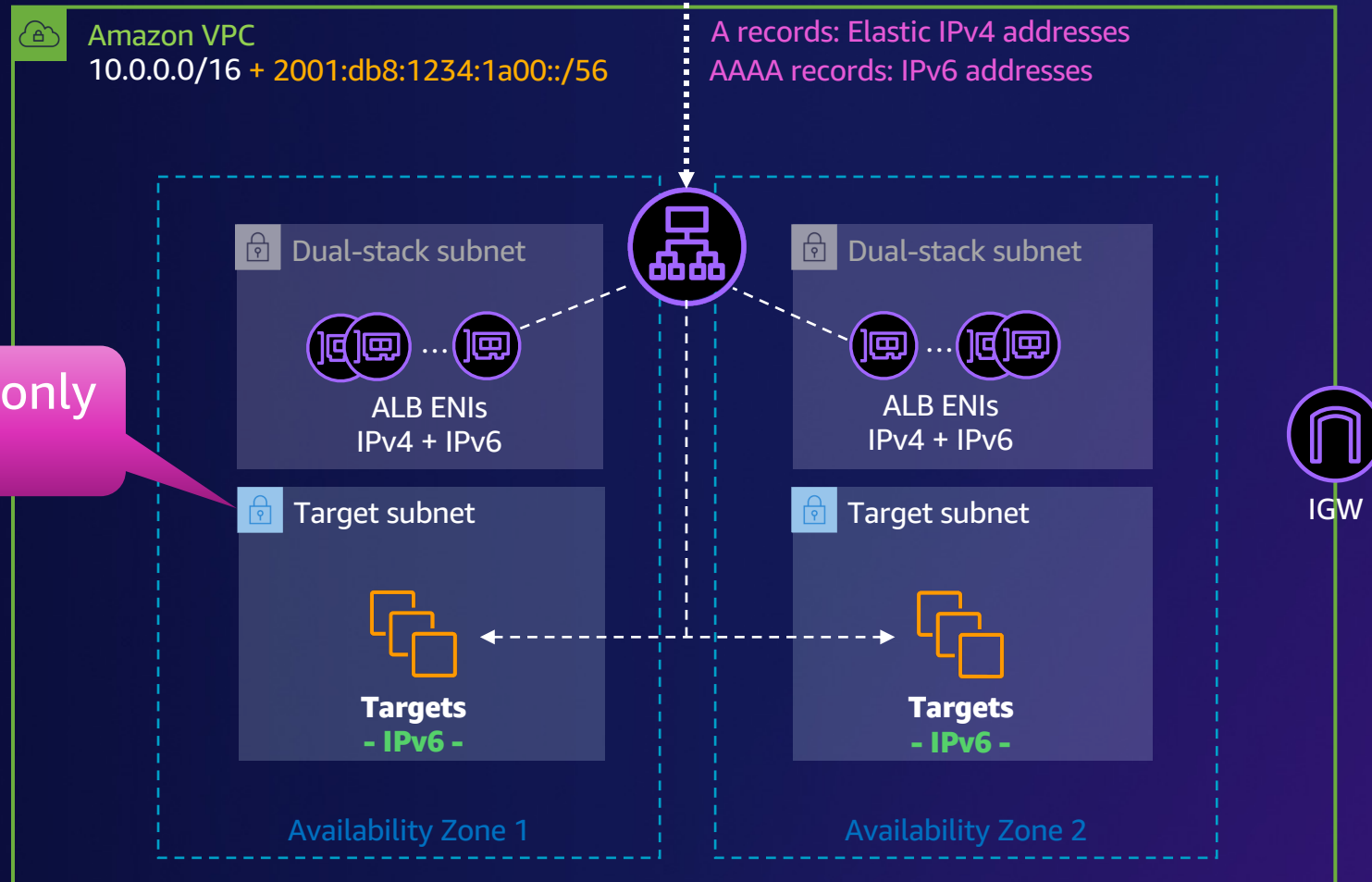


Amazon ELB IPv6 support

- Application Load Balancers
- Network Load Balancers
- Gateway Load Balancer

Application Load Balancers – End-to-end IPv6

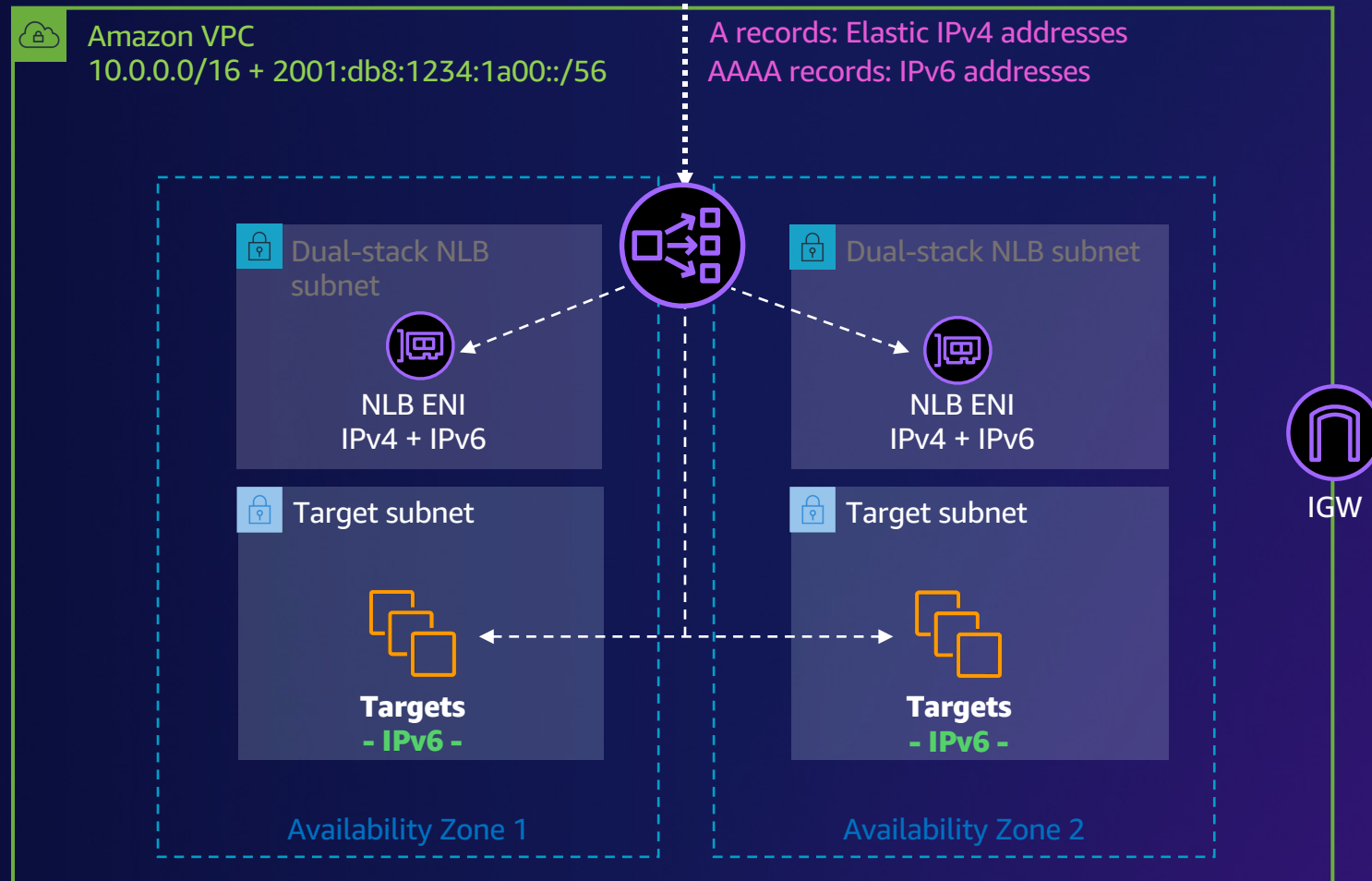
my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com



Support for IPv6-only targets

Network Load Balancers – End-to-end IPv6

my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com

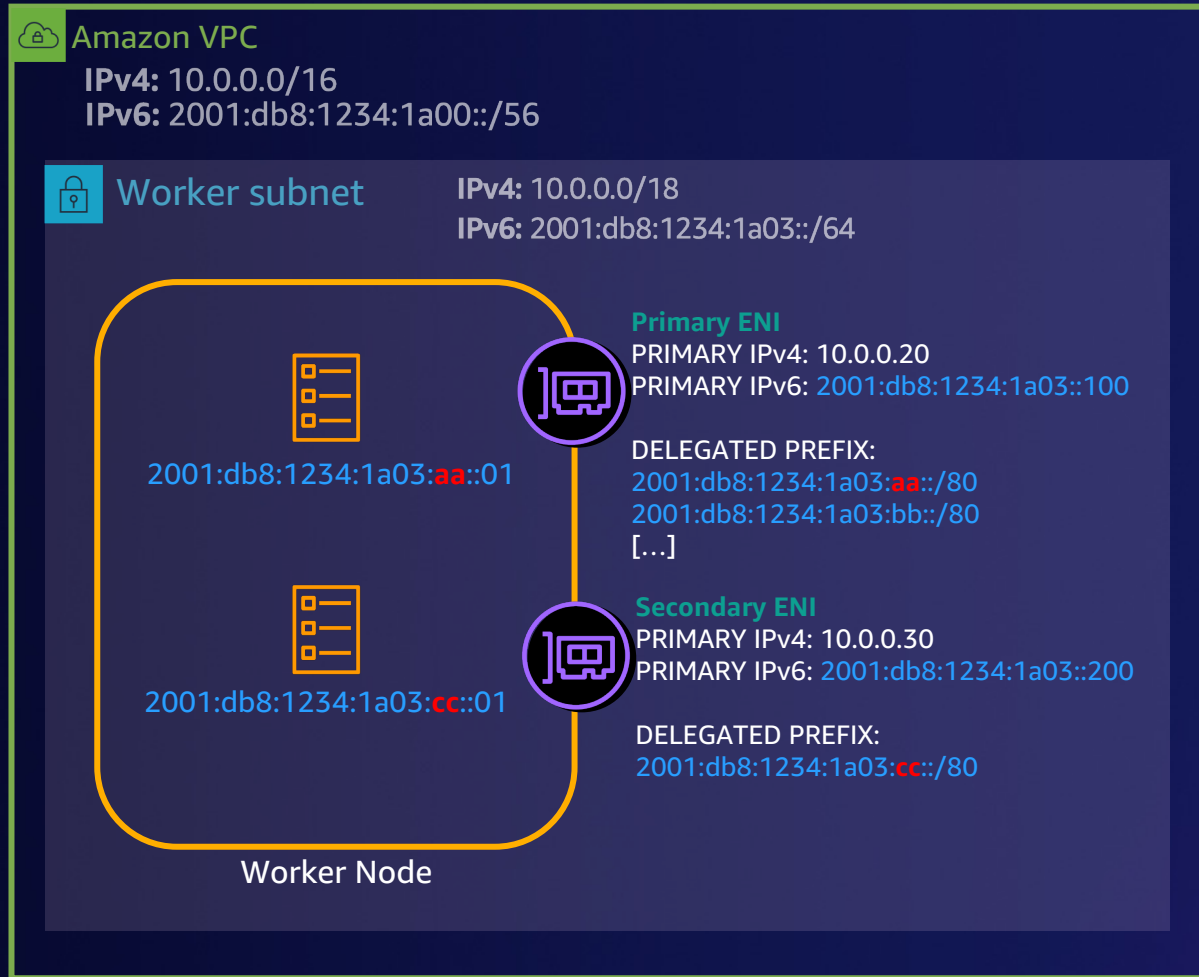


AWS services IPv6 support

2023 updates



Amazon EKS



IPv6
2023

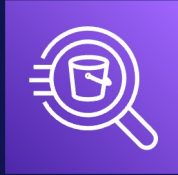
19 launches in total



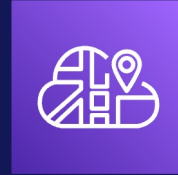
AWS Global Accelerator



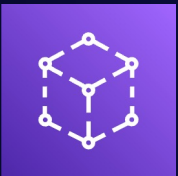
AWS PrivateLink



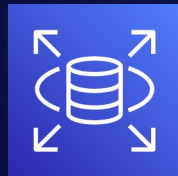
Amazon Athena



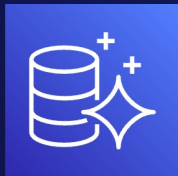
AWS Cloud Map



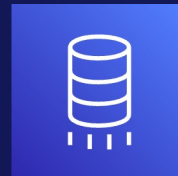
AWS App Mesh



Amazon RDS



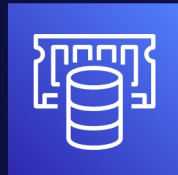
Amazon Aurora



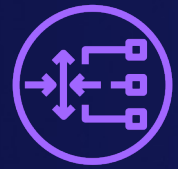
AWS DMS



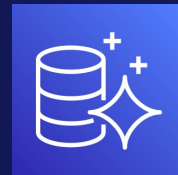
AWS Secrets Manager



Amazon ElastiCache



Gateway Load Balancer



Amazon Aurora

IPv6
2023

AWS services IPv6 support

2023 updates



AWS Network Firewall



IPv6
2023

Amazon Route 53 Resolver Endpoints



IPv4



IPv6



dual stack

IPv6
2023

Amazon-provided contiguous IPv6 CIDRs

Network Manager > Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0c18cf41027a7747b

Pool settings

| | |
|---|---|
| Name (IPAM ID) My Test IPAM (ipam-093e6b9cbea89b688) | Name (Scope ID) ipam-scope-0c18cf41027a7747b |
|---|---|

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify. Tags are not visible to other accounts even if a pool is shared.

Description - optional
Write a brief description for the pool.

Pool hierarchy [Info](#)

Source pool
To provision a CIDR into this pool, it must be available in the source pool. If no source pool is selected, then the space must be available in the scope.

Bring Your Own IP (BYOIP) pools with an AWS service selected for advertising are disabled.

Address family
Select the address family for this pool.

IPv4

IPv6

IPv6
2023



Amazon-provided contiguous IPv6 CIDRs

Address family
Select the address family for this pool.

IPv4

IPv6

Advertisability
Choose whether CIDRs in this pool will be eligible for advertisement from AWS services.

Allow CIDRs in this pool to be publicly advertisable.
CIDRs in a pool with public IP source of Amazon are automatically advertised.

Locale
Select a locale for this pool to reside.

US East (N. Virginia) - us-east-1

A locale can only be selected if there is no source pool, or if the source pool's locale is None.

Service
Name of an AWS service where CIDRs will be advertisable.

None

EC2 (EIP/VPC)

Public IP source
Select the source of CIDRs in this pool.

BYOIP

Amazon owned
By default, CIDRs in a top-level pool in the public scope must be imported through Bring Your Own IP (BYOIP). Pools with address family IPv6, a locale, and service EC2 can use either BYOIP or Amazon-owned CIDR blocks.

CIDRs to provision [Info](#)
CIDRs to be provisioned must either be available in the source pool's space, or in the scope's space if no source pool.

[Add Amazon-owned CIDR](#)

IPv6
2023

Amazon-provided contiguous IPv6 CIDRs

Advertisability
Choose whether CIDRs in this pool will be eligible for advertisement from AWS services.

Allow CIDRs in this pool to be publicly advertisable.
CIDRs in a pool with public IP source of Amazon are automatically advertised.

Locale
Select a locale for this pool to reside.

US East (N. Virginia) - us-east-1

A locale can only be selected if there is no source pool, or if the source pool's locale is None.

Q Filter by netmask length

| | |
|-----------------------|--|
| /40 (65536 /56 CIDRs) | |
| /41 (32768 /56 CIDRs) | |
| /42 (16384 /56 CIDRs) | |
| /43 (8192 /56 CIDRs) | |
| /44 (4096 /56 CIDRs) | |
| /45 (2048 /56 CIDRs) | |
| /46 (1024 /56 CIDRs) | Bring Your Own IP (BYOIP). Pools with address family |
| /47 (512 /56 CIDRs) | |
| /48 (256 /56 CIDRs) | /47 (512 /56 CIDRs) |
| /49 (128 /56 CIDRs) | |
| /50 (64 /56 CIDRs) | scope's space if no source pool. |
| /51 (32 /56 CIDRs) | |
| /52 (16 /56 CIDRs) | ✓ |
| /52 (16 /56 CIDRs) | ▲ Remove |

Add Amazon-owned CIDR

IPv6
2023

Amazon Athena support IPv6 for inbound connections



IPv6
2023

Amazon VPC CNI now supports IPv6 Egress for Pods in IPv4 enabled Kubernetes Clusters



IPv6
2023

IPv6 on AWS Webpage



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

IPv6 on AWS Compatibility



<https://docs.aws.amazon.com/general/latest/gr/aws-ipv6-support.html>

Thank you!

