

IPv6 architectures on AWS

IPv6 Council - Belgium

Alexandra Huides

Sr. Networking Specialist Solutions Architect, Strategic Accounts

AWS



Questions of The Universe...

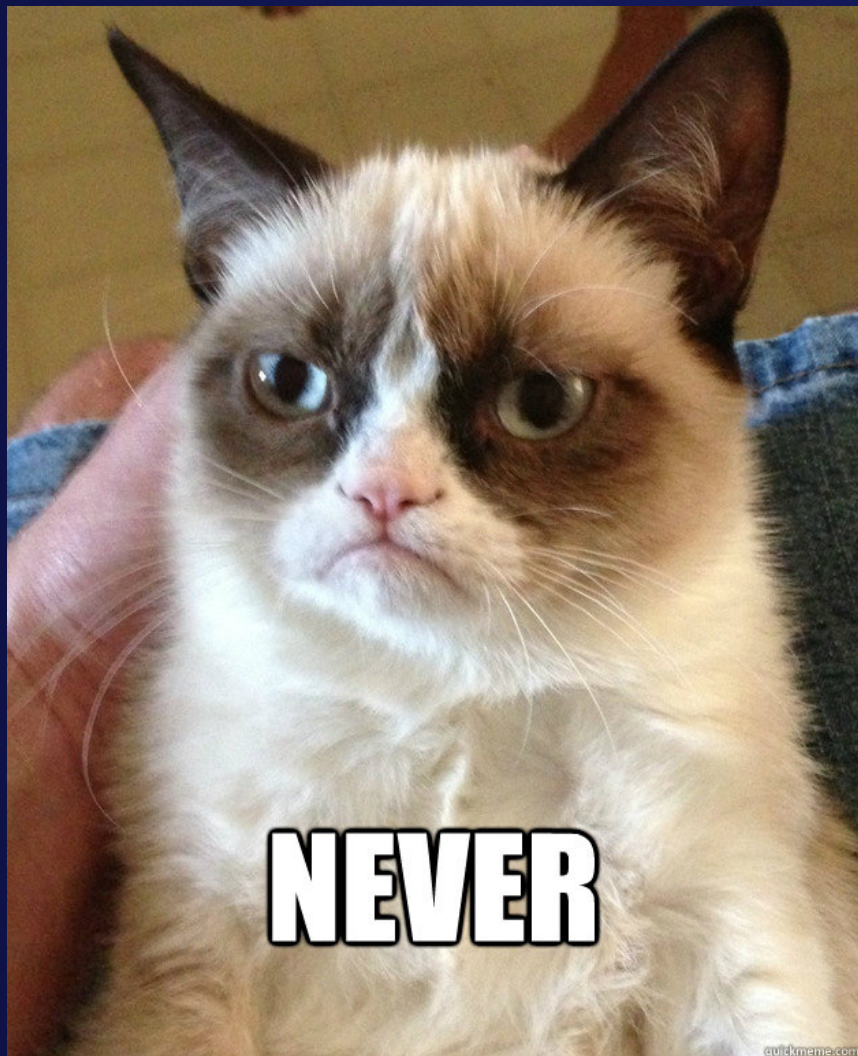
Are Aliens real?

...

What's inside a black hole?

...

When will we go to IPv6?



(A pessimist)



(An optimist)

It depends...

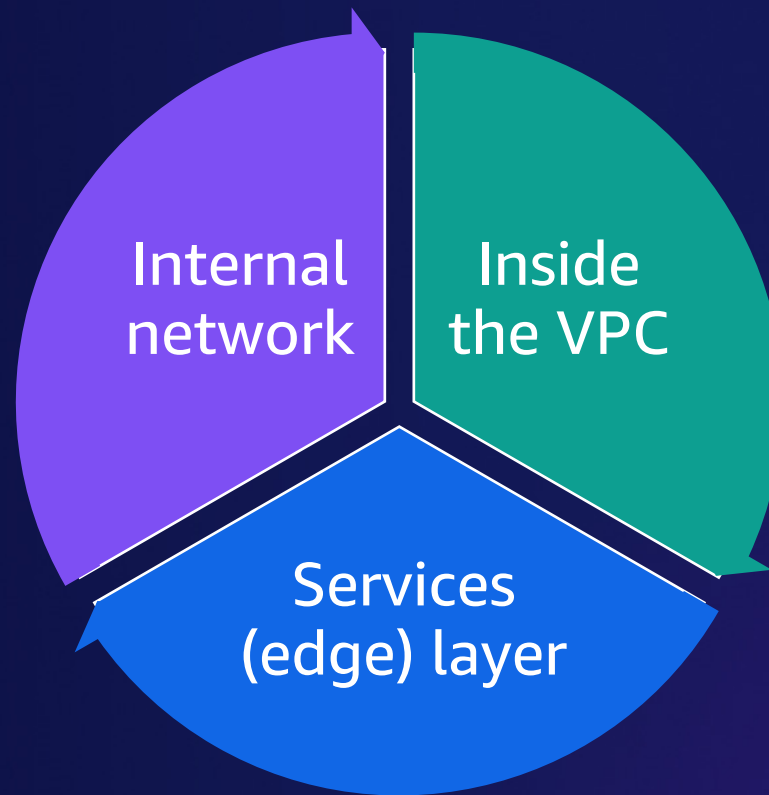
(A network engineer)

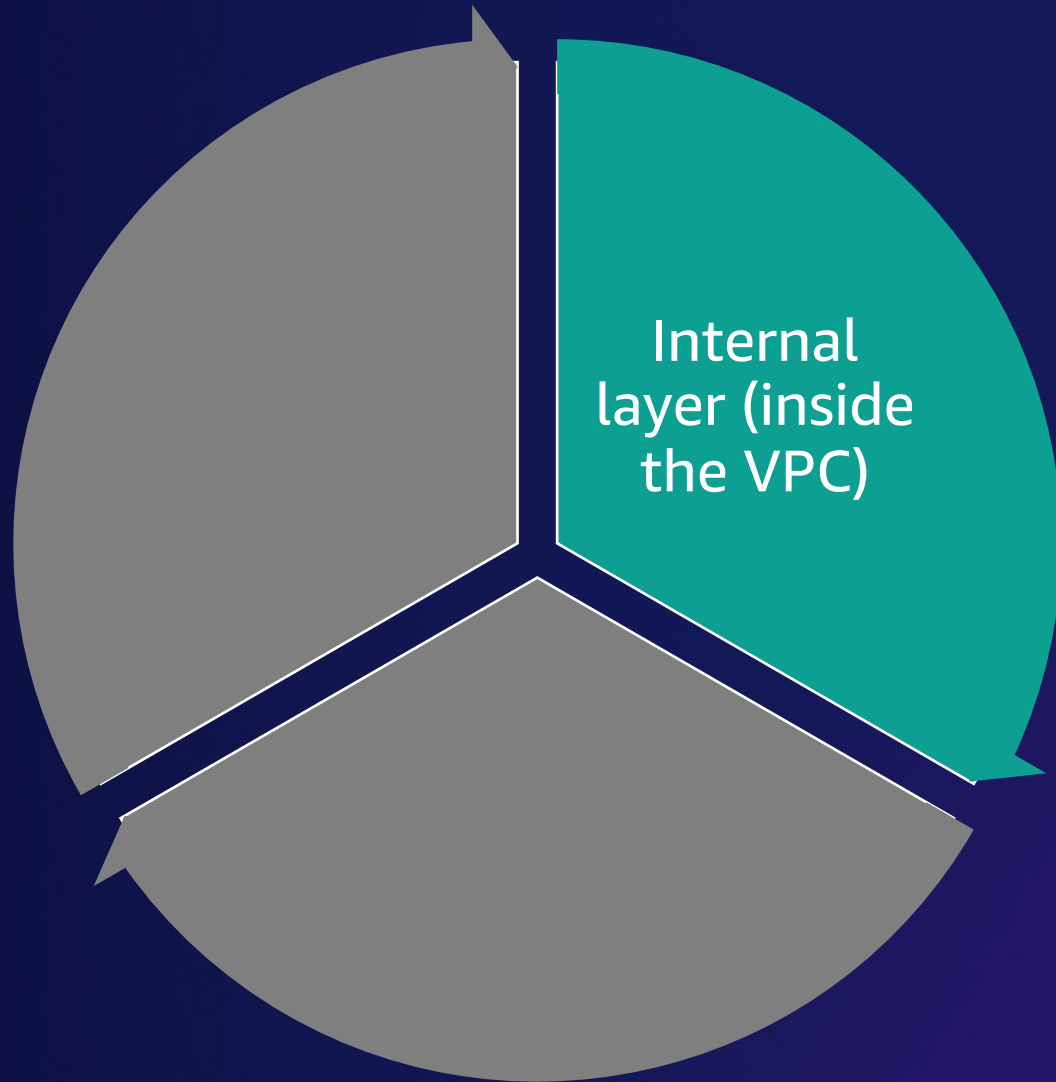


The real answer is...no one knows

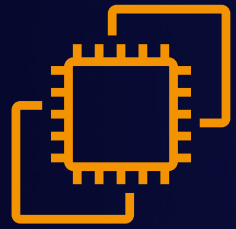
Let's focus on what we know then...

There are three areas of focus for IPv6 adoption





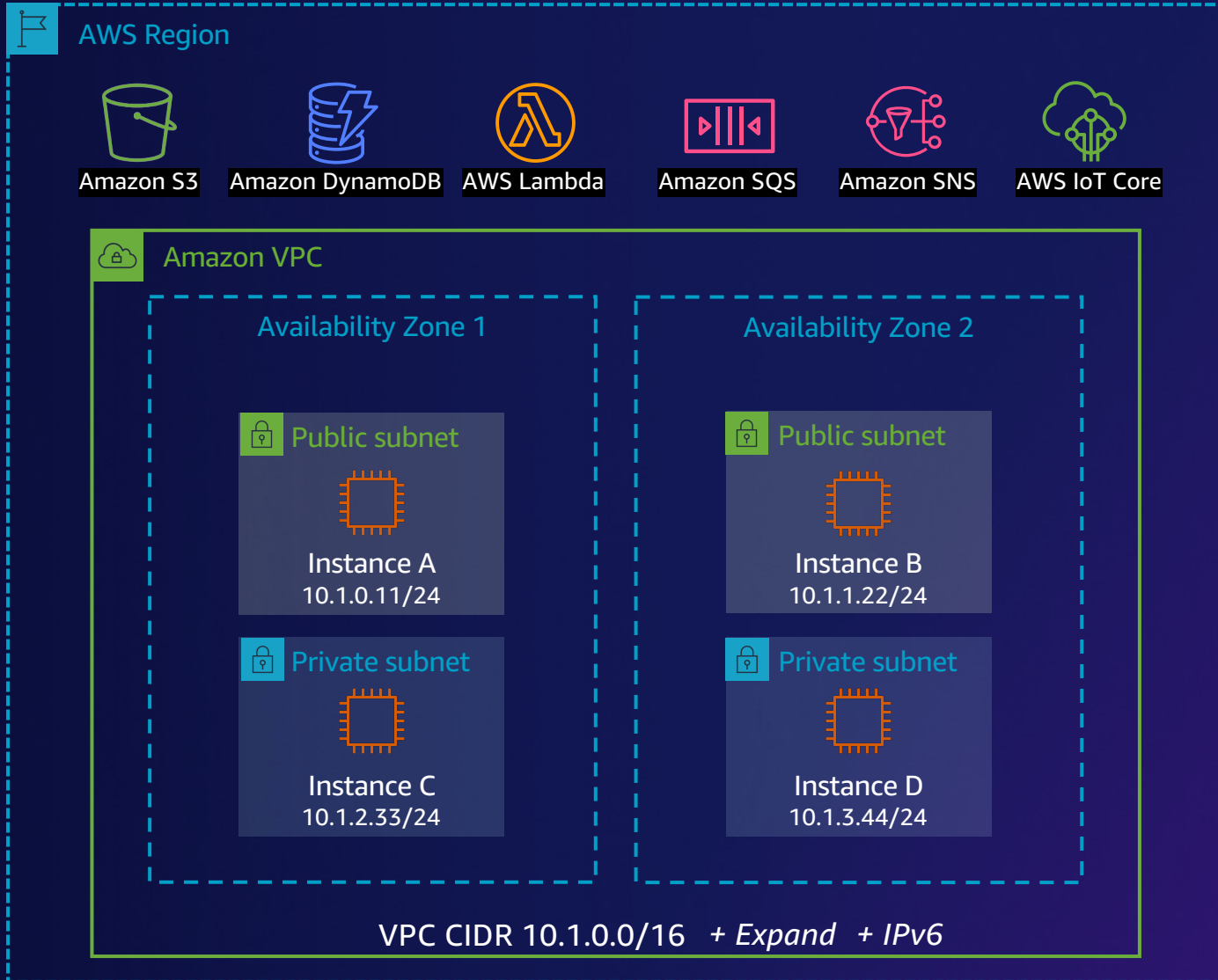
Amazon VPC networking



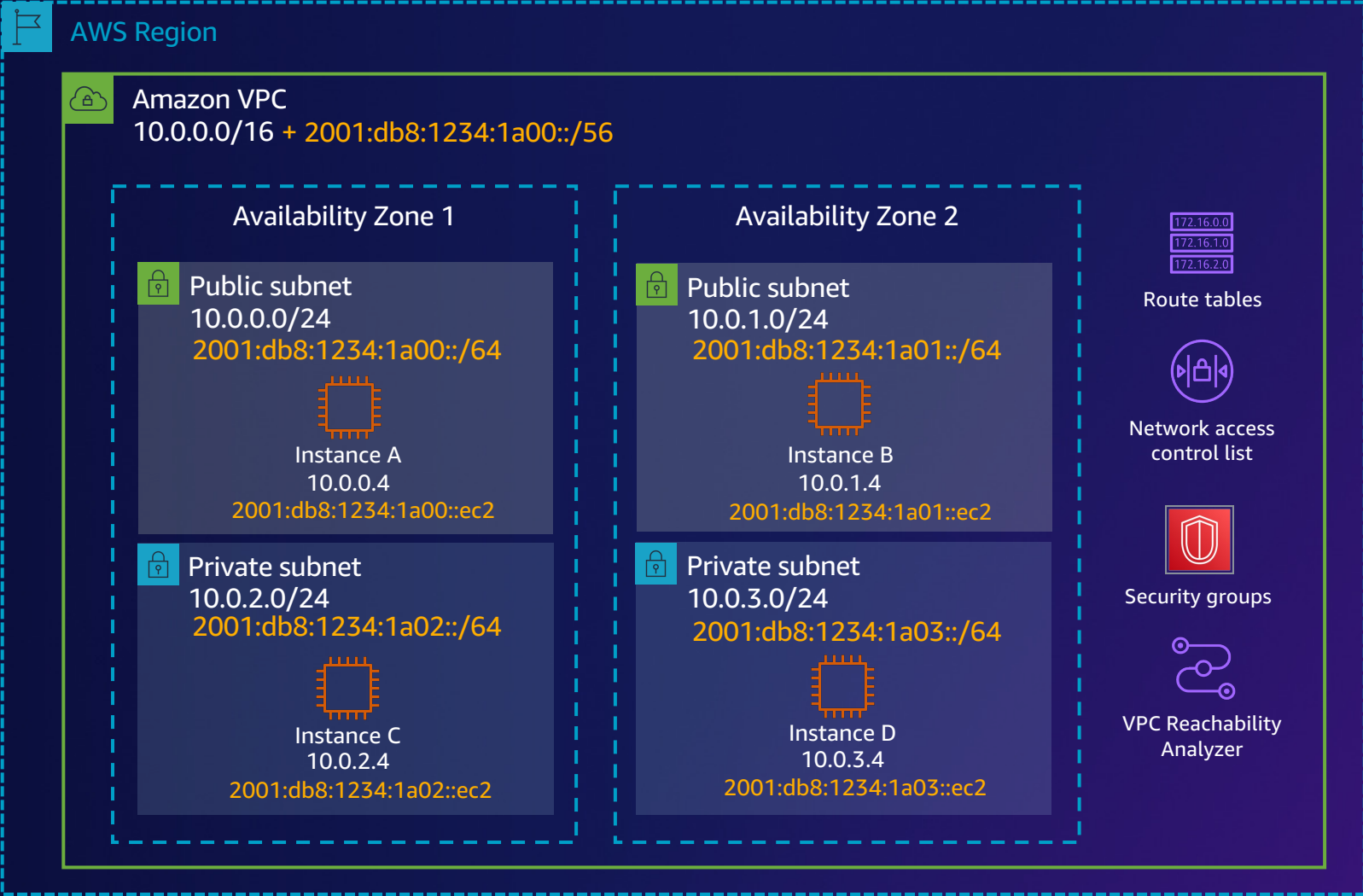
Amazon Elastic
Cloud Compute
(Amazon EC2)



Amazon Virtual
Private Cloud
(Amazon VPC)

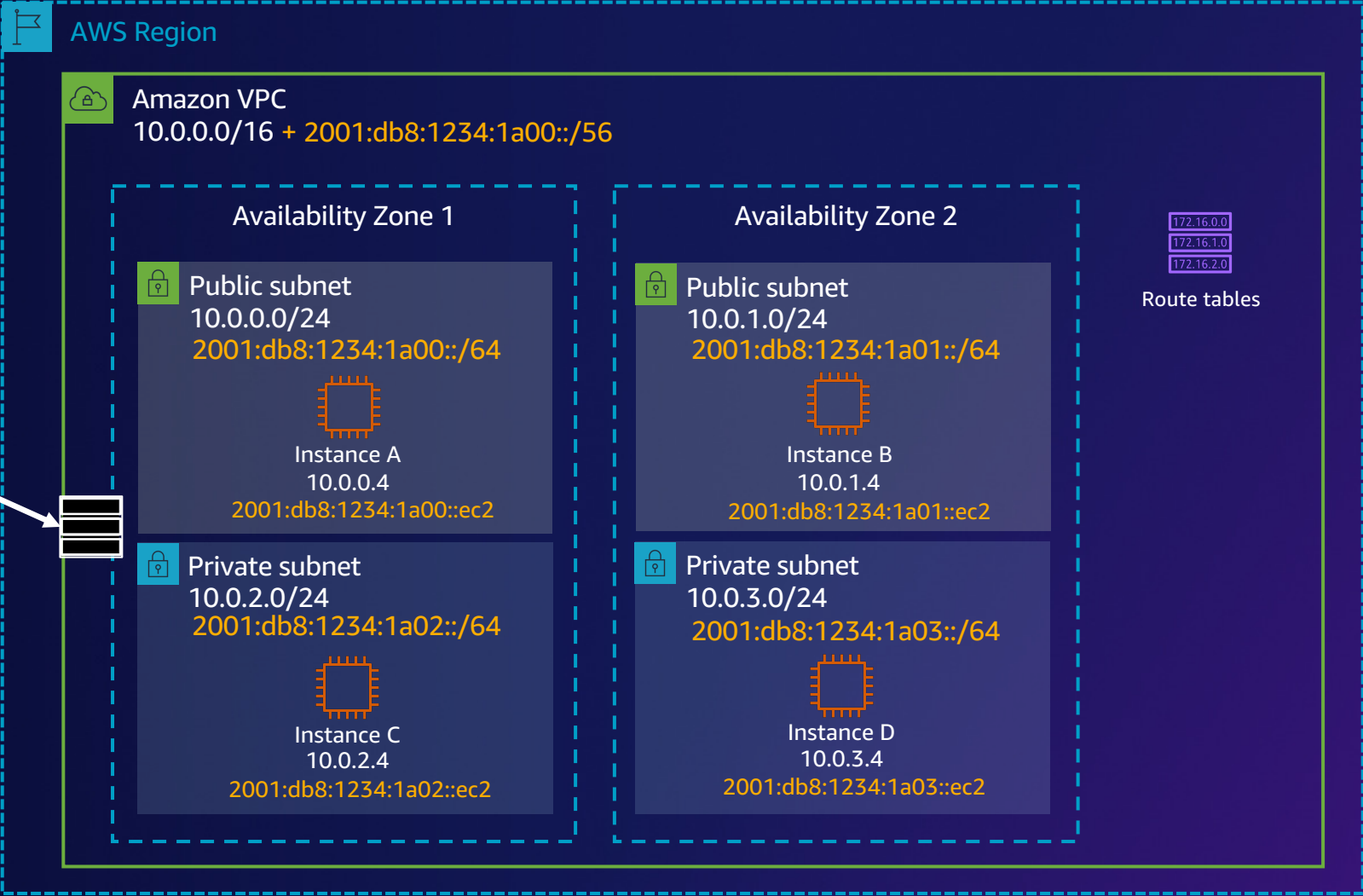


Adding IPv6 to your VPC

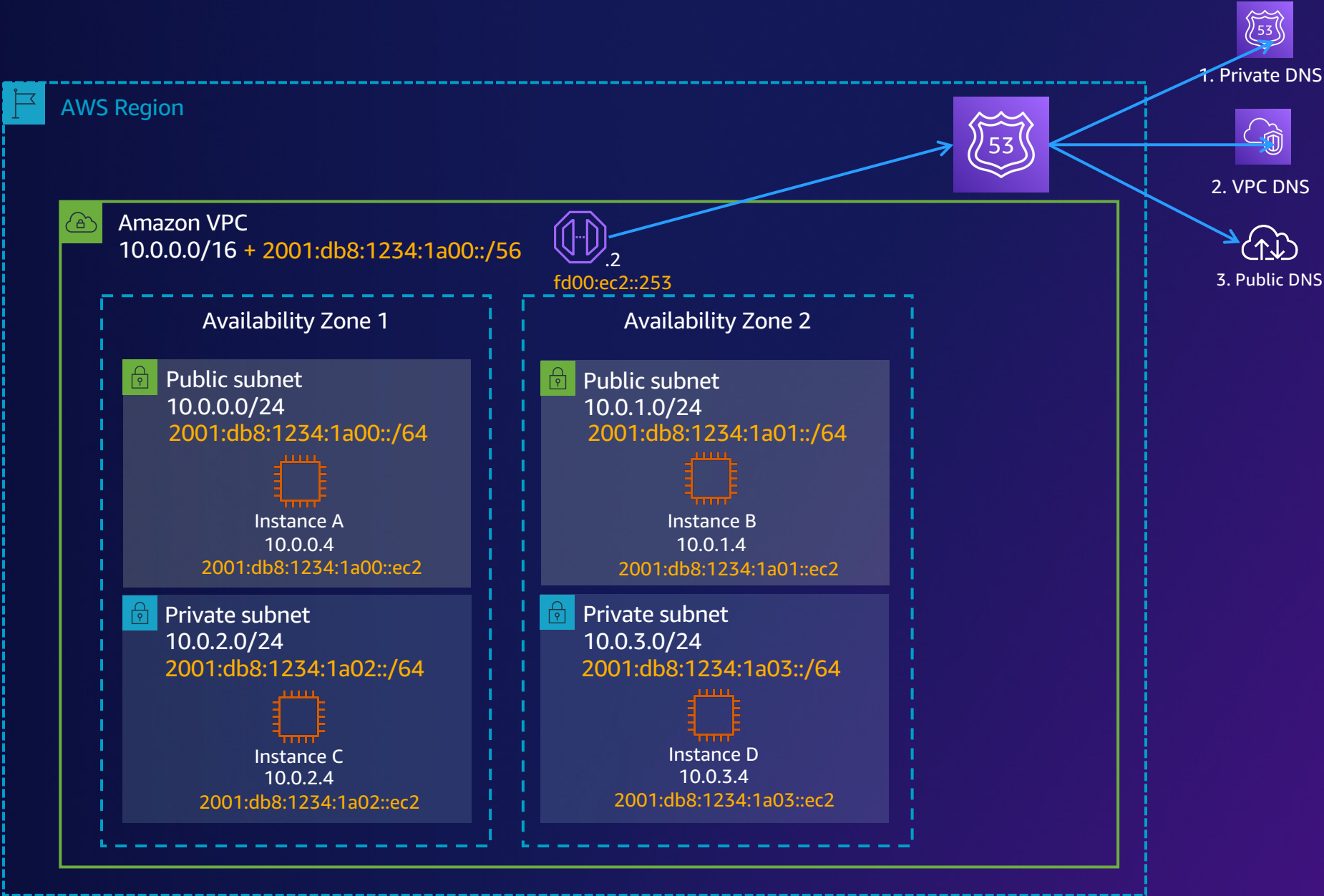


VPC routing

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local



VPC DNS



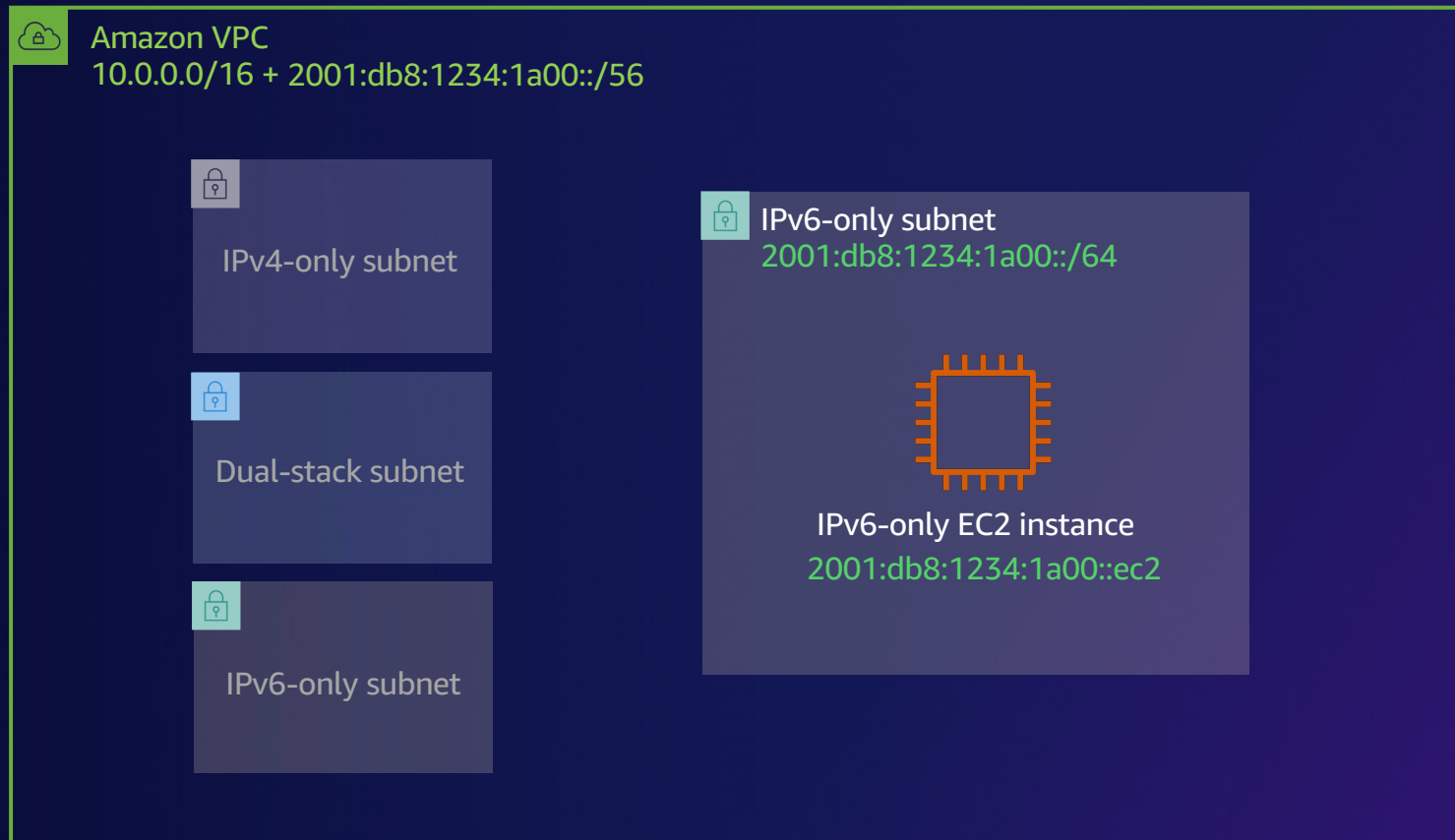
Amazon dual stack VPC

IPV4-ONLY AND DUAL STACK SUBNETS



Amazon dual-stack VPC

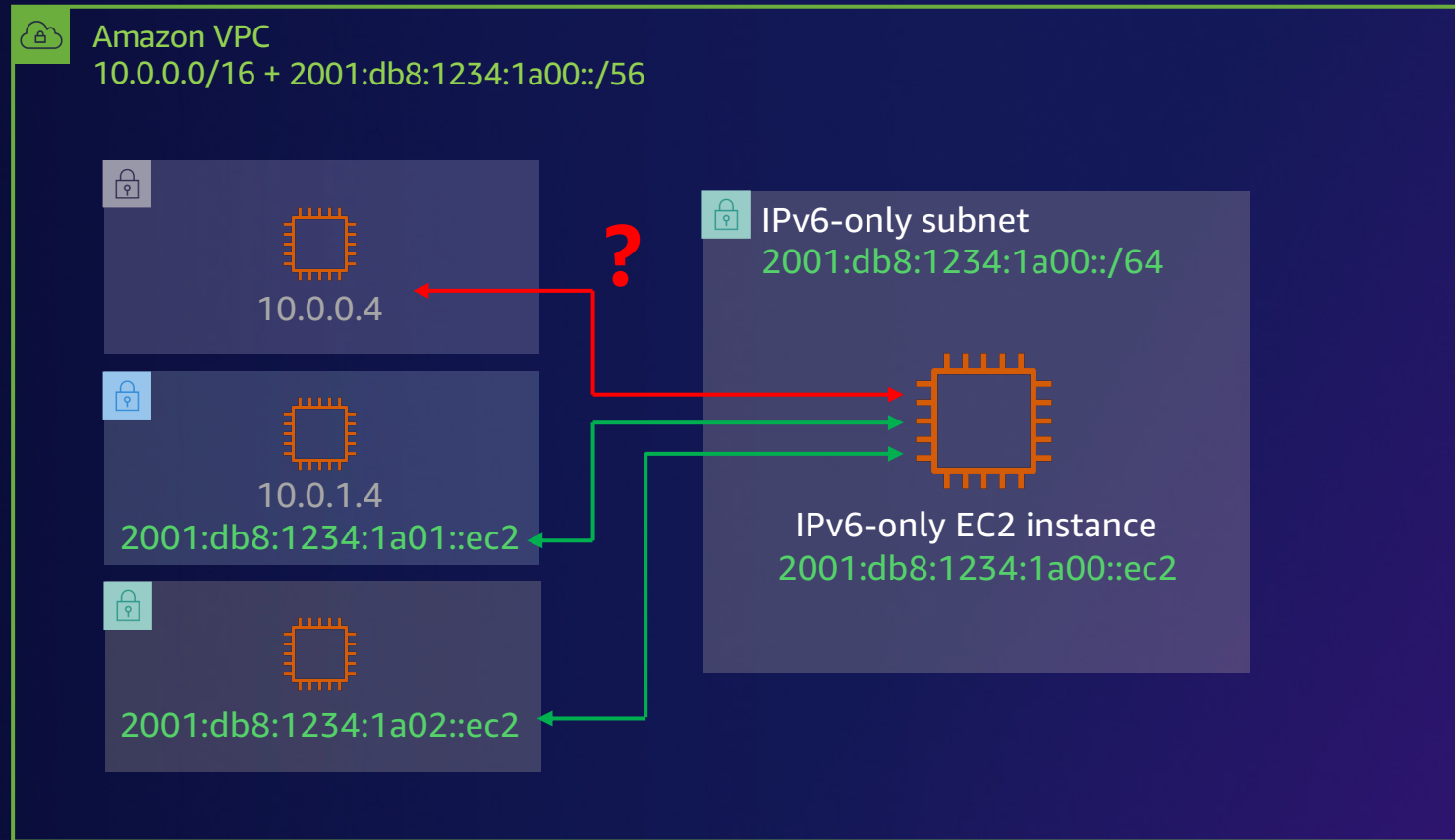
IPV6-ONLY SUBNETS



Traffic flows inside the Amazon VPC

Amazon dual-stack VPC: IPv6 only subnets

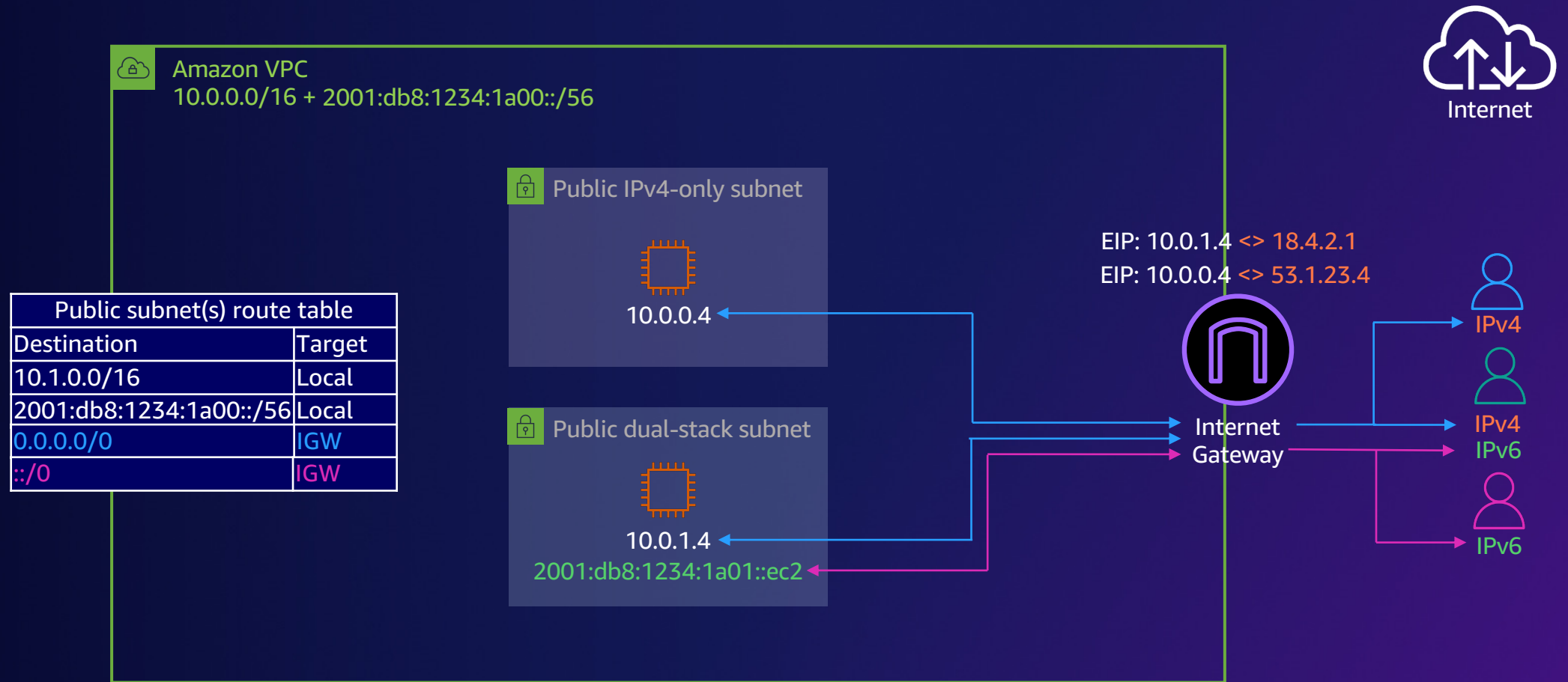
FLAWS



Public subnets internet connectivity

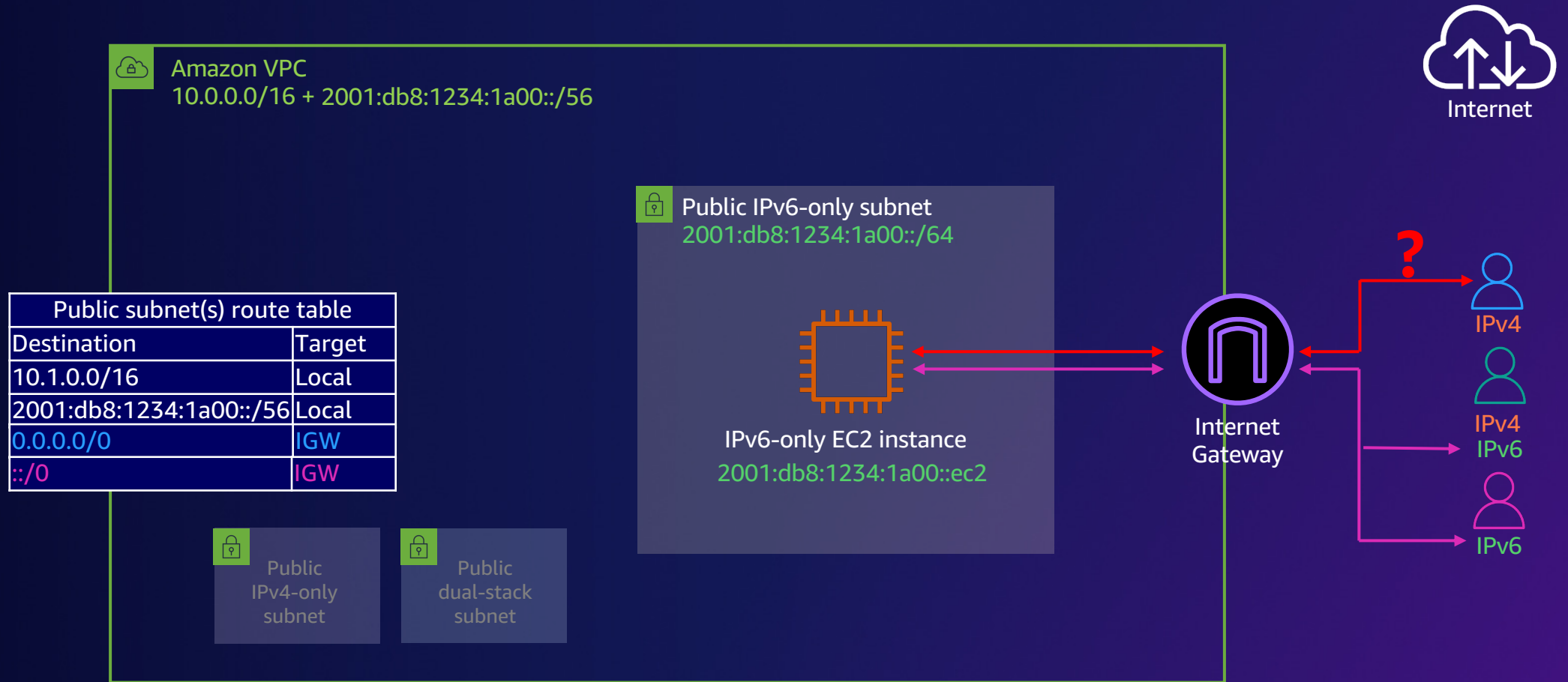
Amazon dual-stack VPC: Internet connectivity

PUBLIC SUBNETS



Amazon dual-stack VPC: Internet connectivity

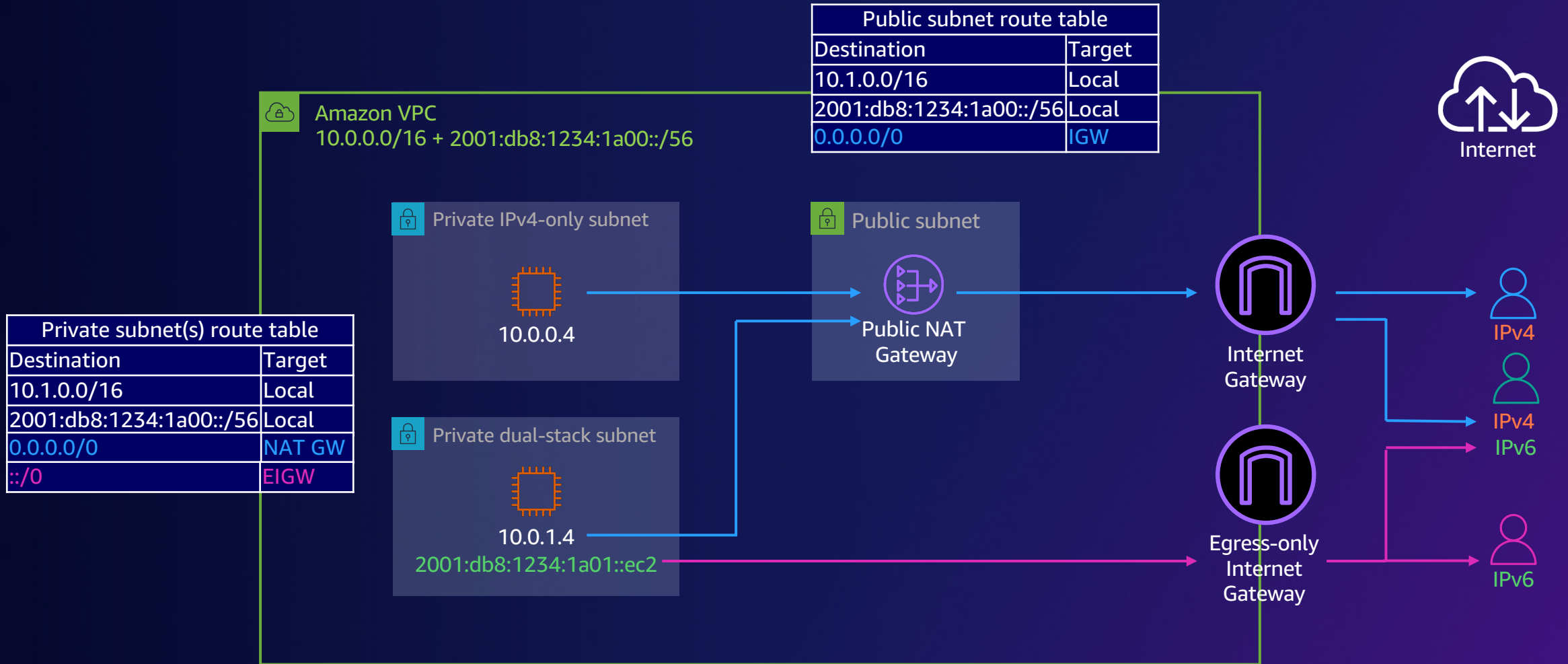
PUBLIC IPV6-ONLY SUBNETS



Private subnets internet connectivity

Amazon dual-stack VPC: Internet connectivity

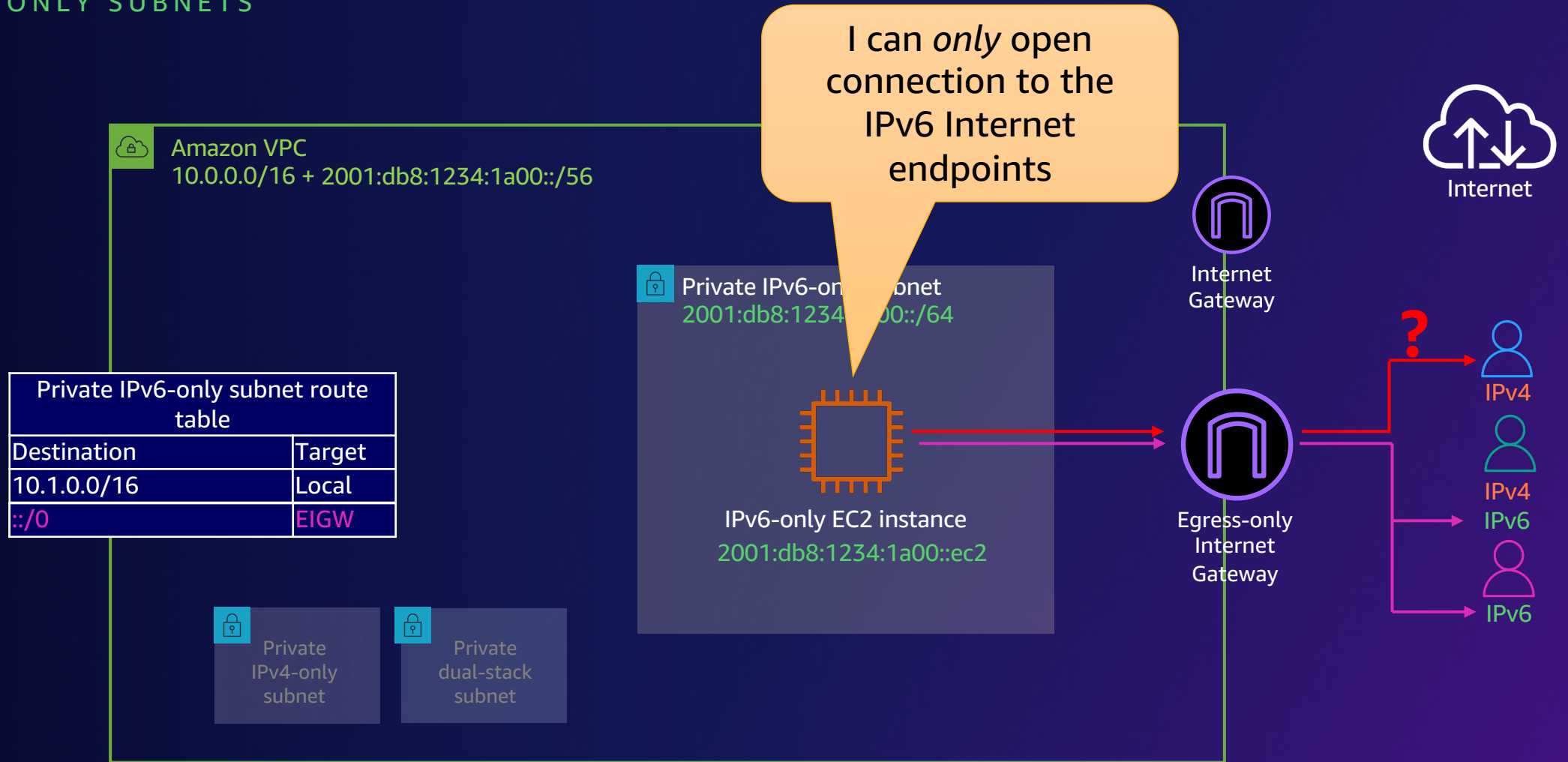
PRIVATE SUBNETS



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

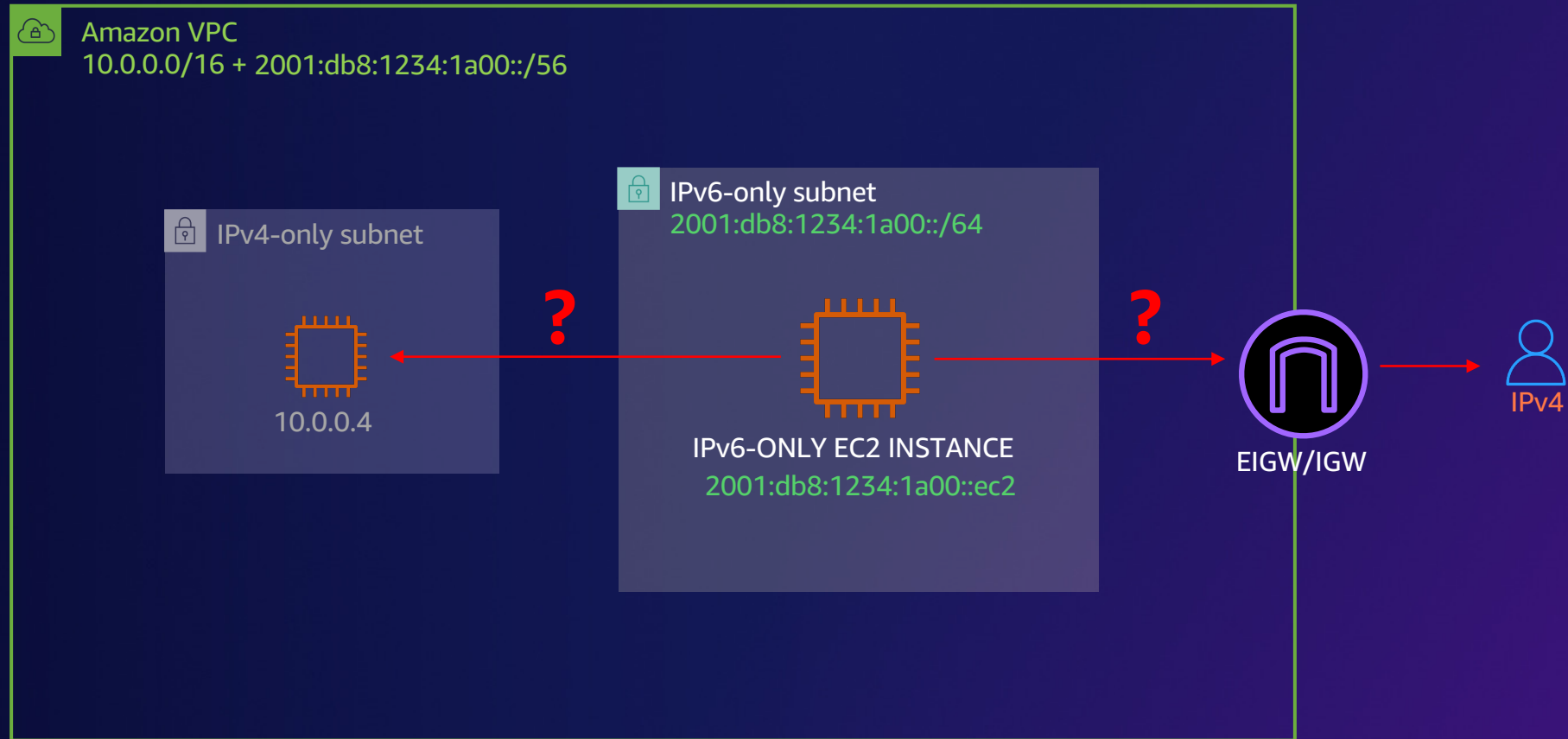
Amazon dual-stack VPC: Internet connectivity

PRIVATE IPV6-ONLY SUBNETS



There's *that* **flow**
we haven't talked about, yet...

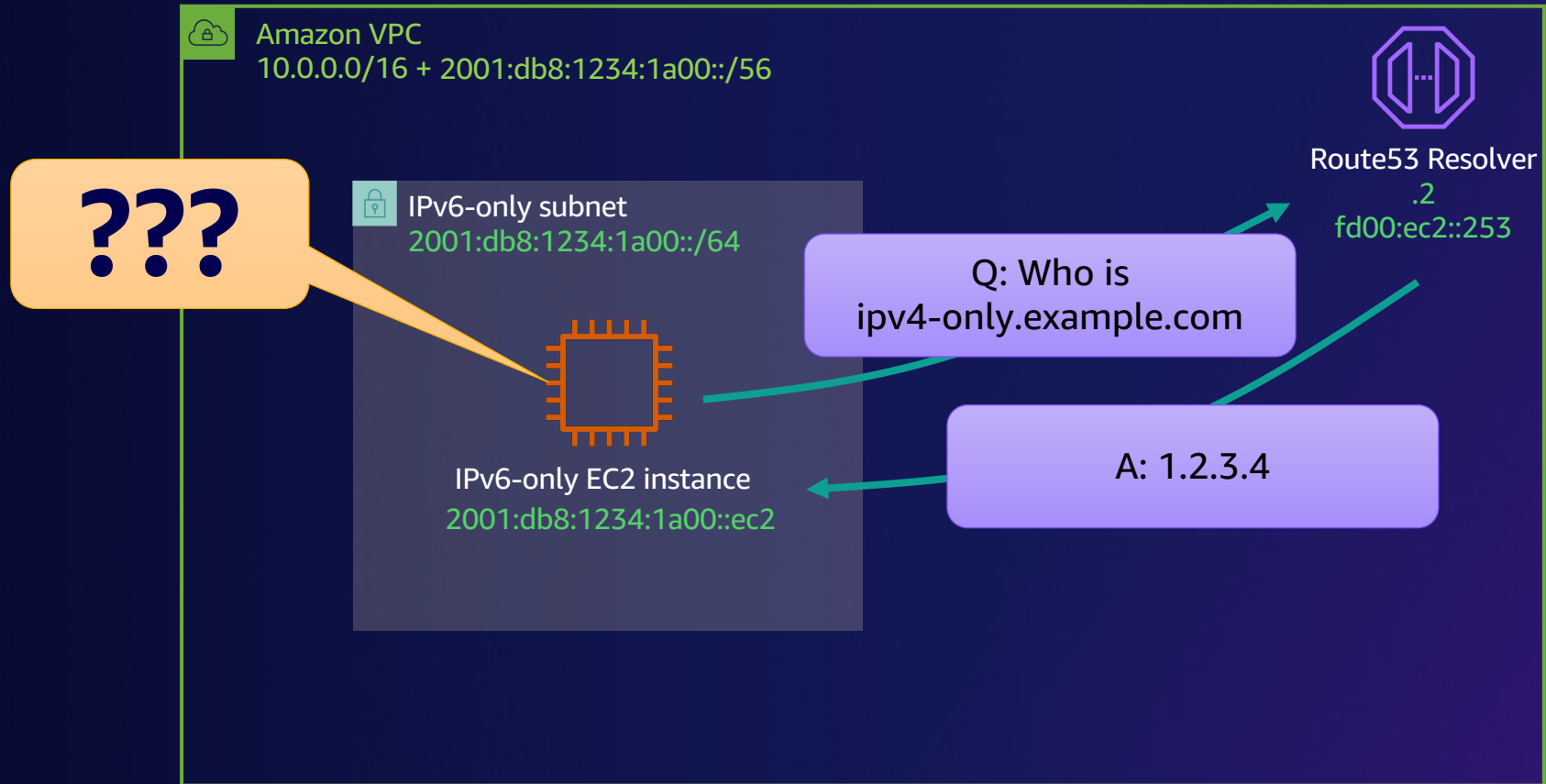
Amazon dual-stack VPC: IPv6 to IPv4



IPv6 to IPv4 and the beauty of NAT

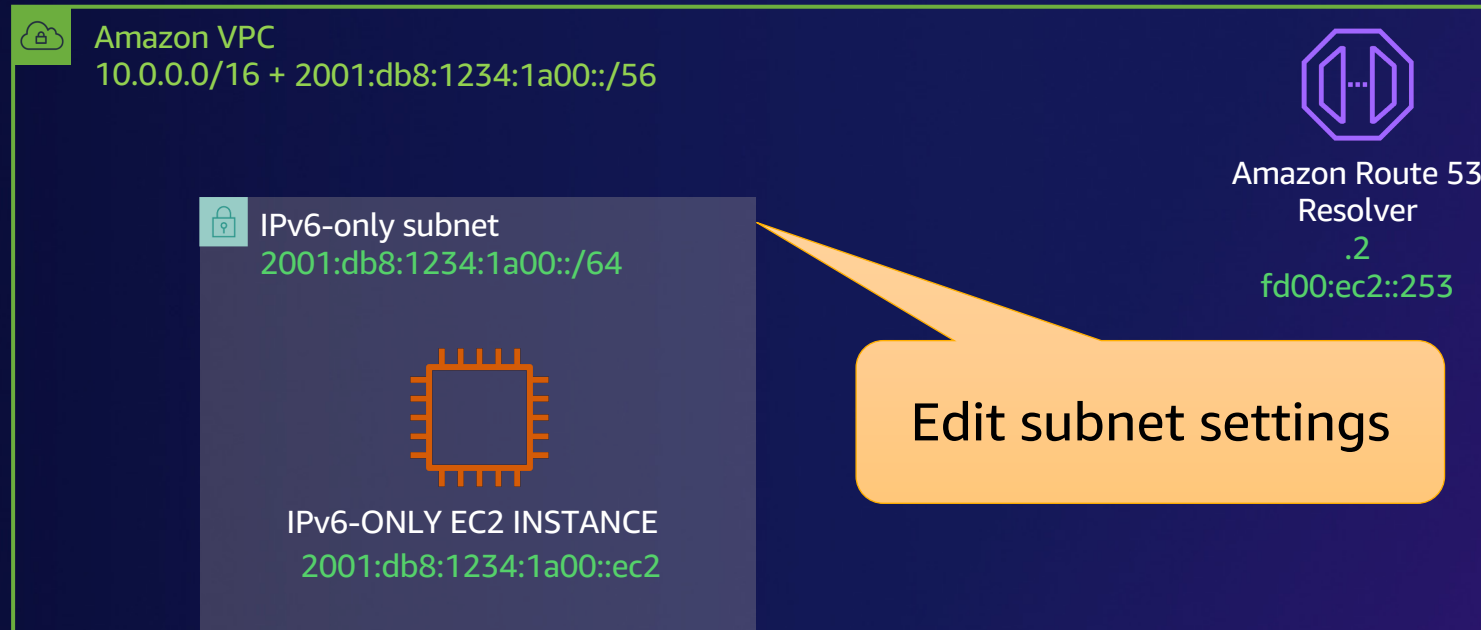
Amazon VPC DNS

BEFORE



DNS64

What is DNS64?



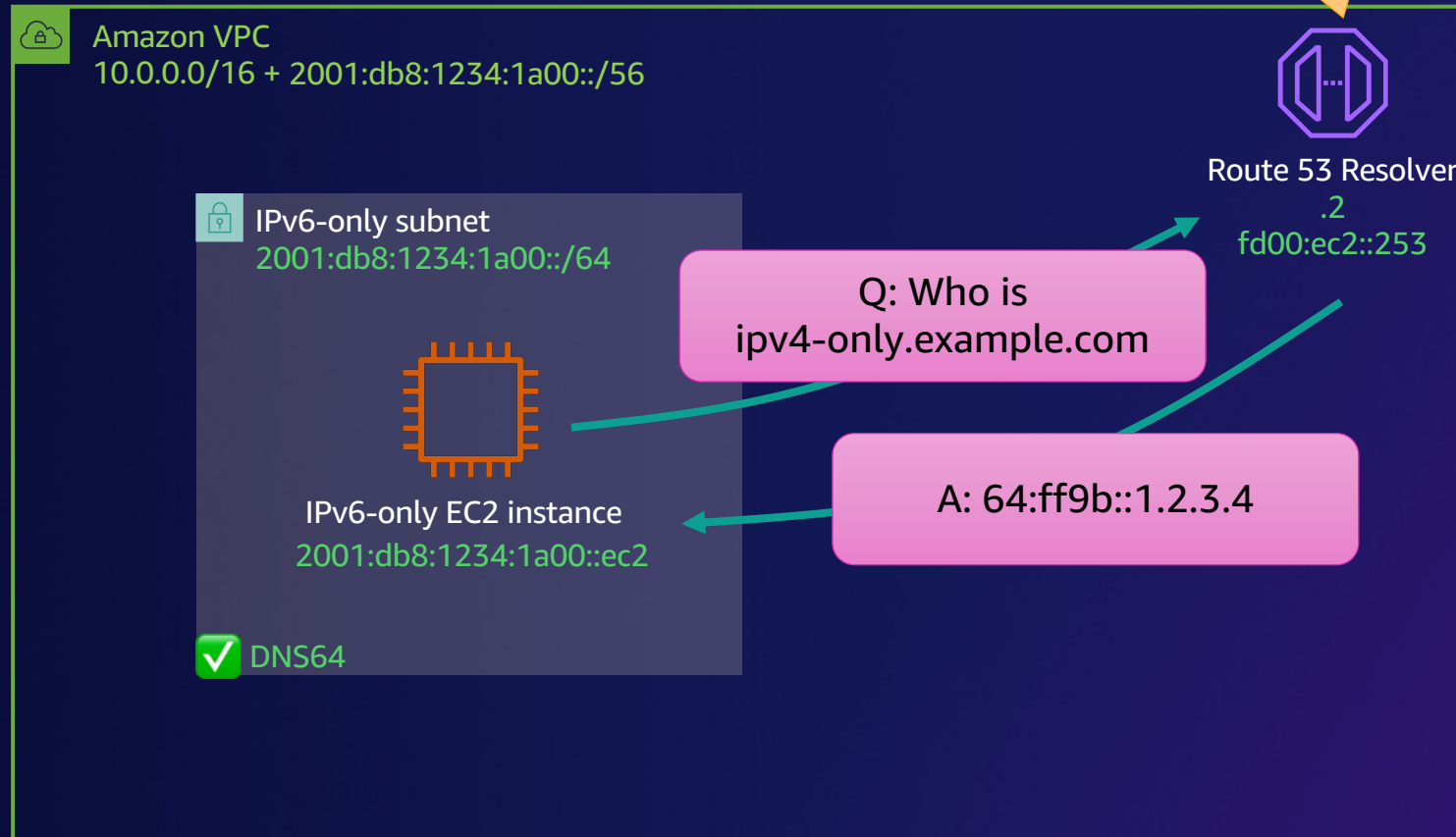
DNS64 settings

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

Enable DNS64 [Info](#)

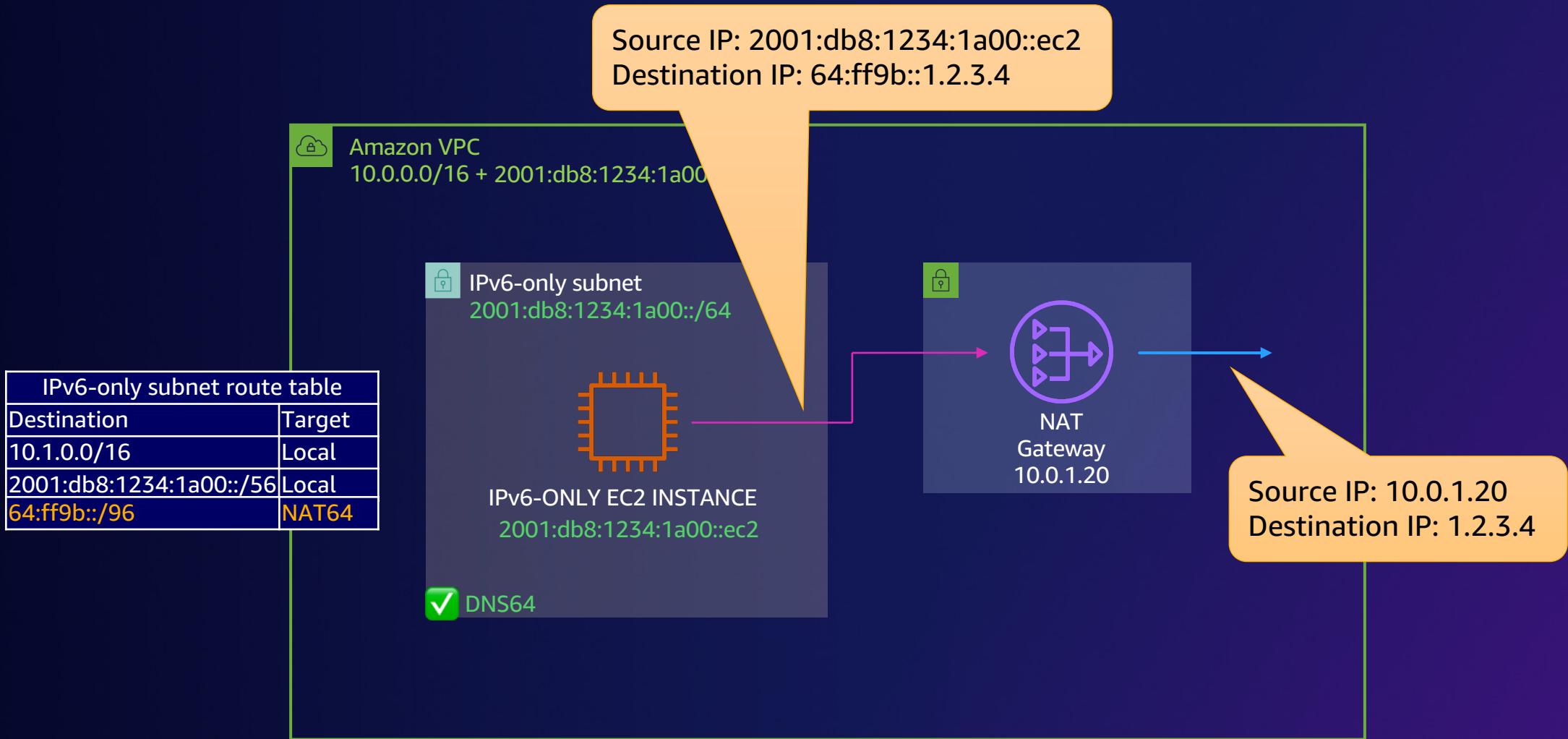
What is DNS64?

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**

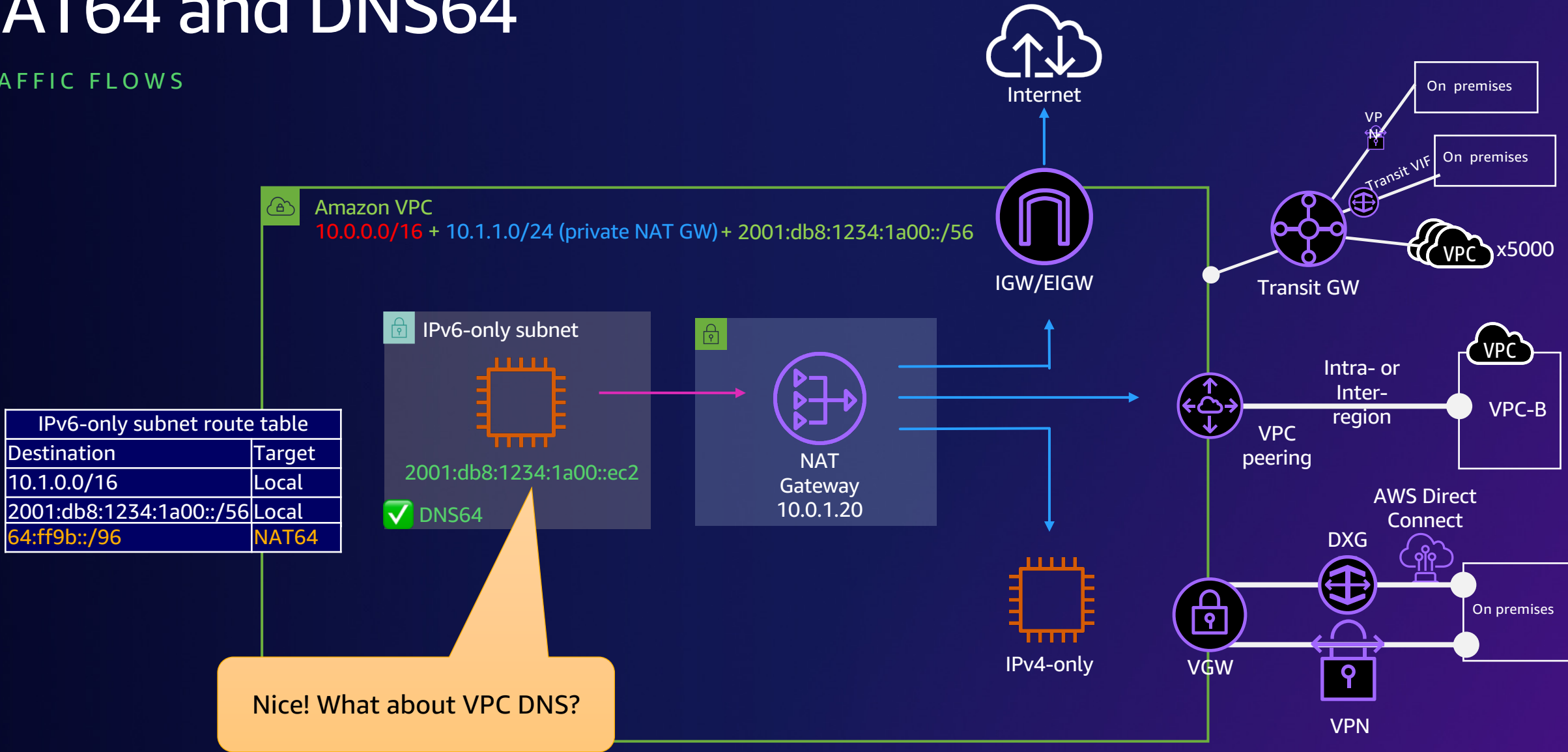
How does NAT64 work?



NAT64 is automatically available on your **existing** NAT gateways or on **any new** NAT gateways you create

NAT64 and DNS64

TRAFFIC FLOWS

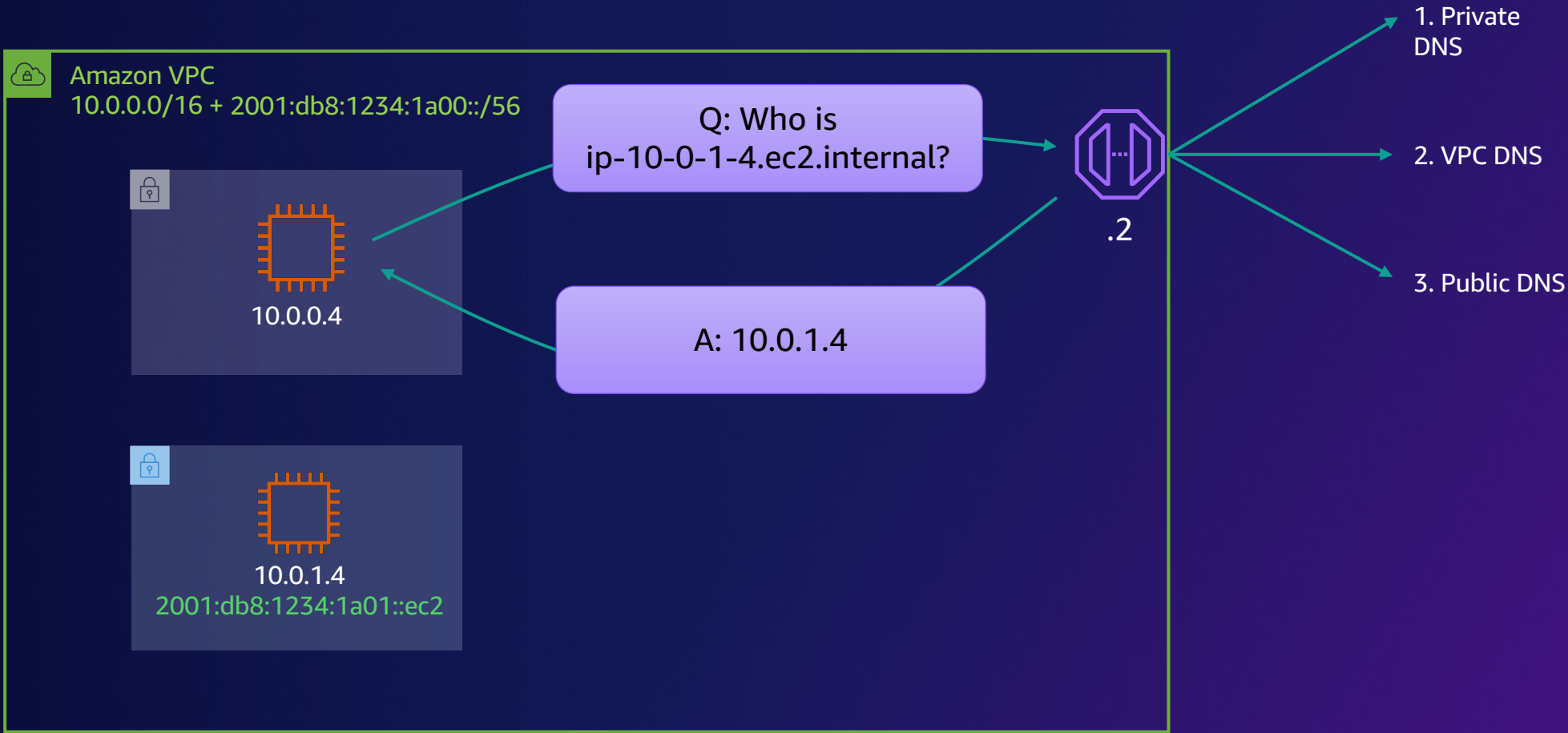


Another throwback:

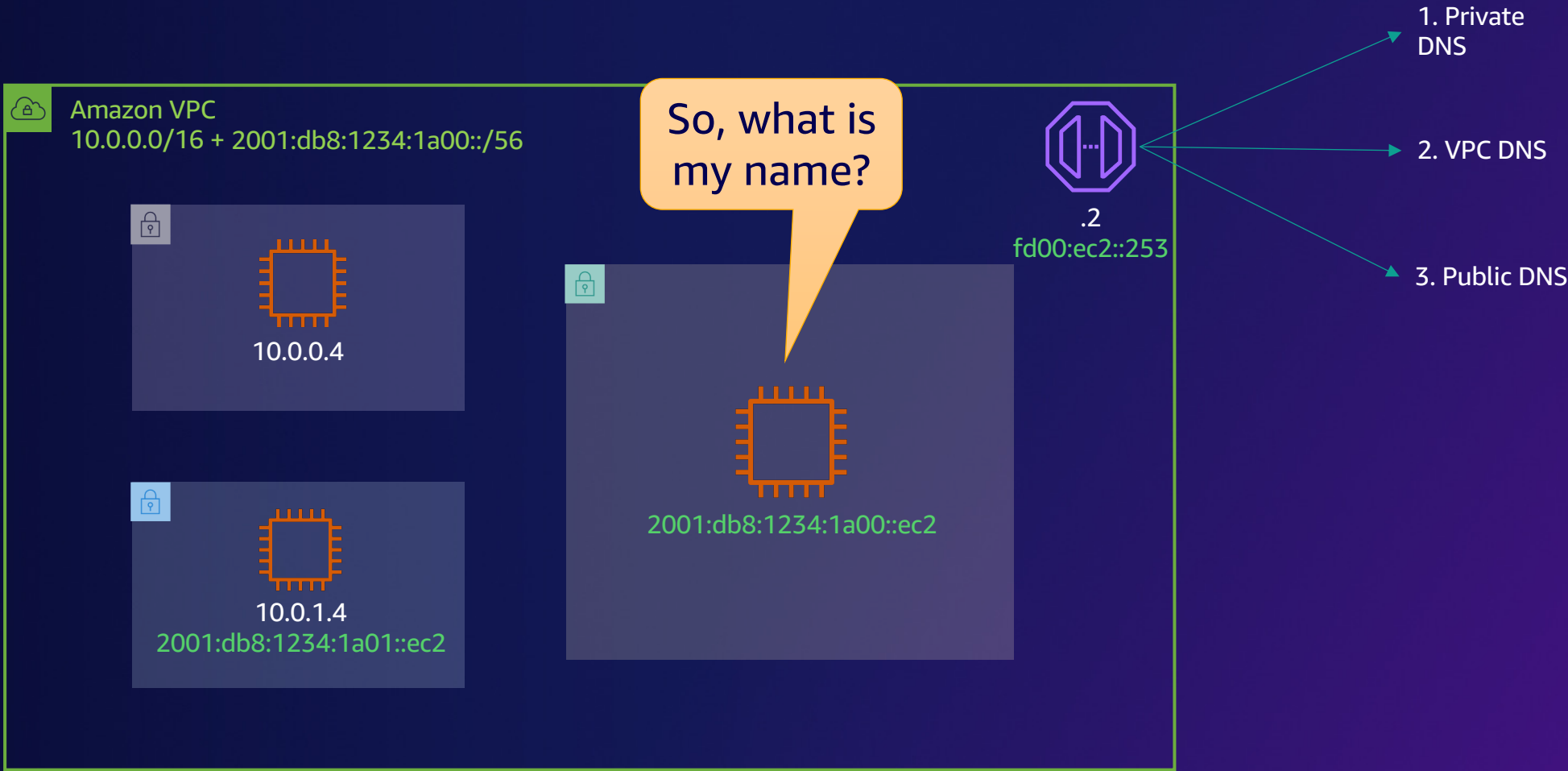
Remember *ip-10-1-1-2.ec.internal*?

Amazon EC2 instance naming

IPV4-BASED NAMING (IPBN)



Amazon EC2 instance naming



Amazon EC2: Resource-based naming (RBN)

SETTINGS FOR EACH SUBNET TYPE

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56

IPv6-only subnets default to RBN



1. Private DNS

2. VPC DNS

3. Public DNS

Resource-based Name (RBN) settings [Info](#)

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch [Info](#)

Enable resource name DNS AAAA record on launch [Info](#)

Hostname type [Info](#)

Resource name

IP name

Amazon EC2: Resource-based naming

SETTINGS FOR EACH SUBNET TYPE

Edit subnet settings

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56

IPv4-only Subnet



.2

fd00:ec2::253

1. Private DNS

2. VPC DNS

public DNS

Resource-based Name (RBN) settings [Info](#)

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch [Info](#)

Enable resource name DNS AAAA record on launch [Info](#)

Hostname type [Info](#)

Resource name

IP name



Amazon EC2: Resource-based naming

SETTINGS FOR EACH SUBNET TYPE

Edit subnet settings

Resource-based Name (RBN) settings [Info](#)
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

- Enable resource name DNS A record on launch [Info](#)
- Enable resource name DNS AAAA record on launch [Info](#)

Hostname type [Info](#)

Resource name

IP name

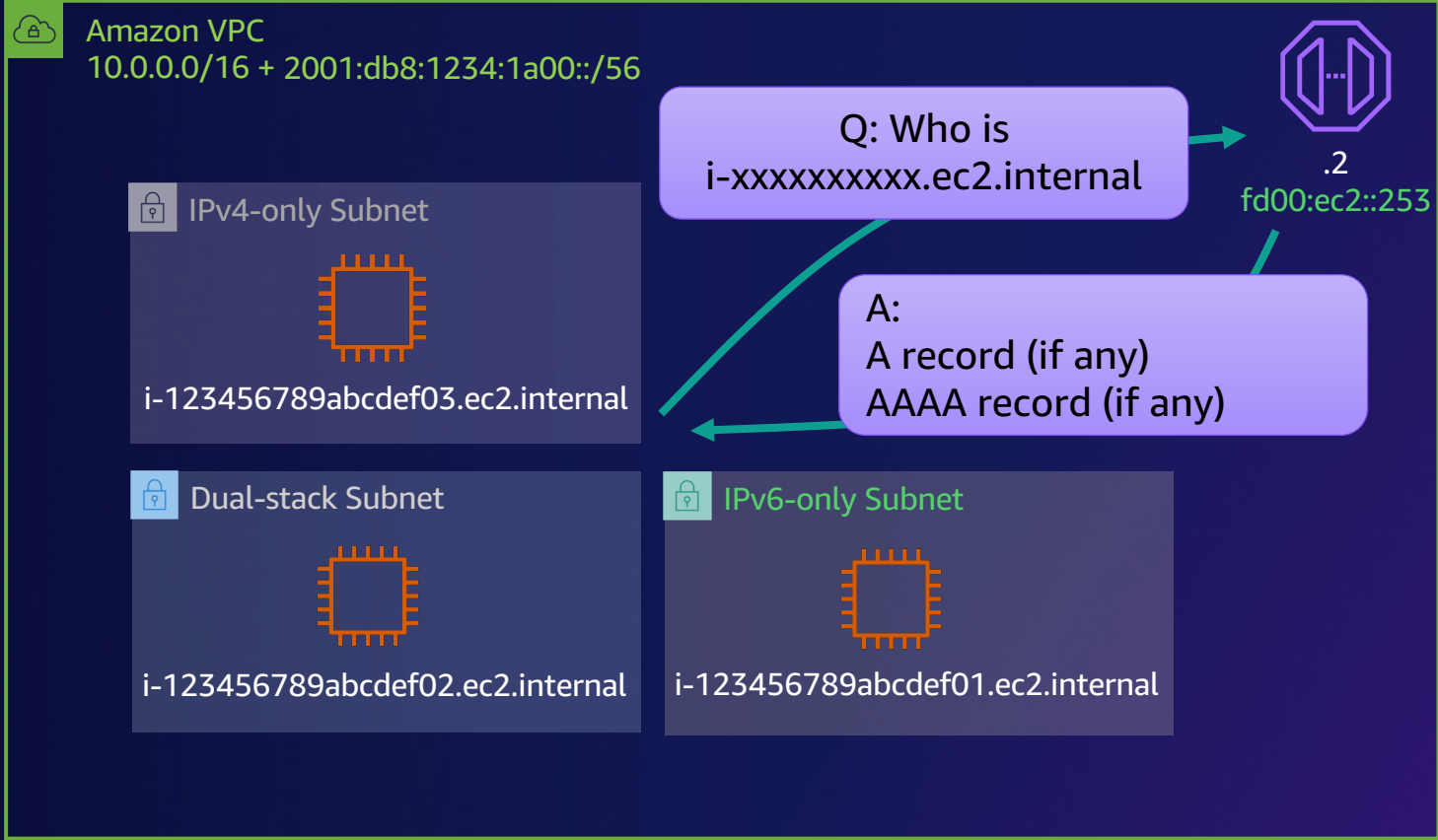
Amazon VPC
10.0.0.0/16 + 2001:db8::/32

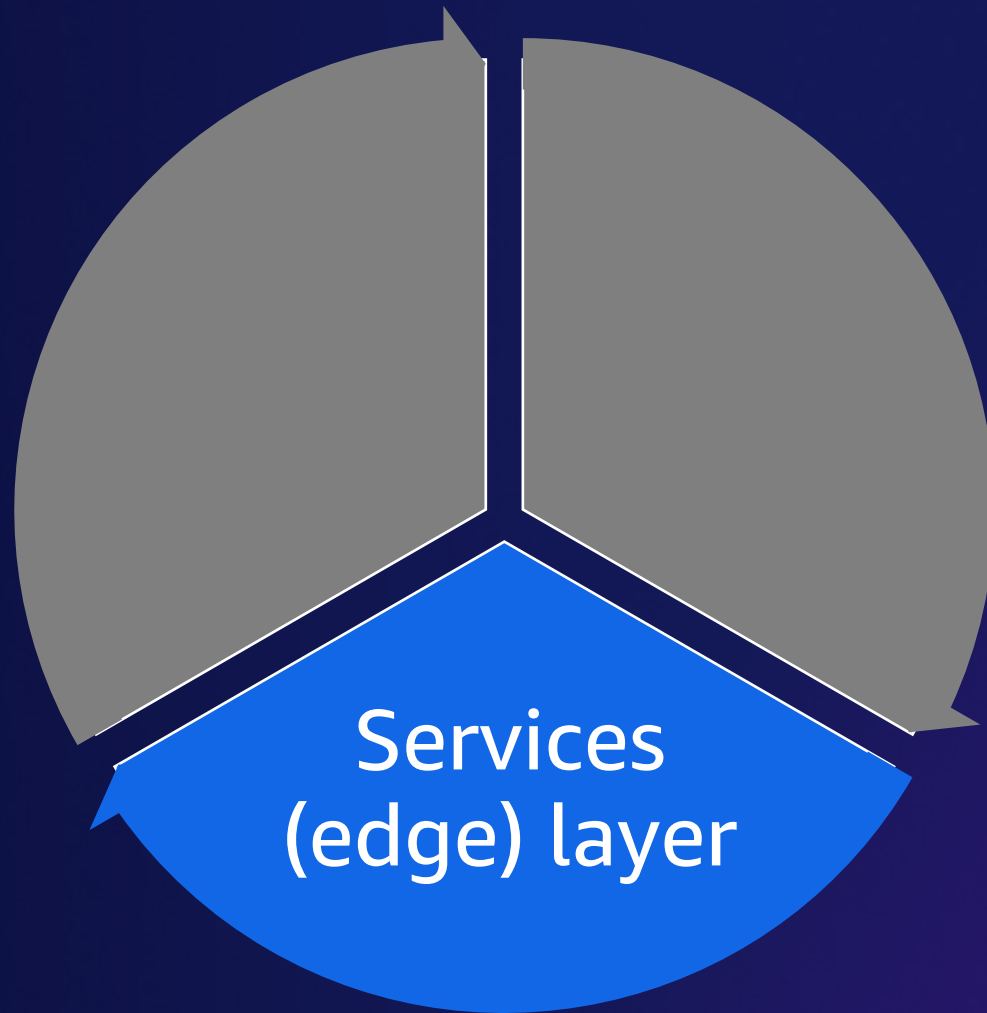
IPv4-only Subnet
10.0.0.0/24

Dual-stack subnet
10.0.1.4
2001:db8:1234:1a01::ec2

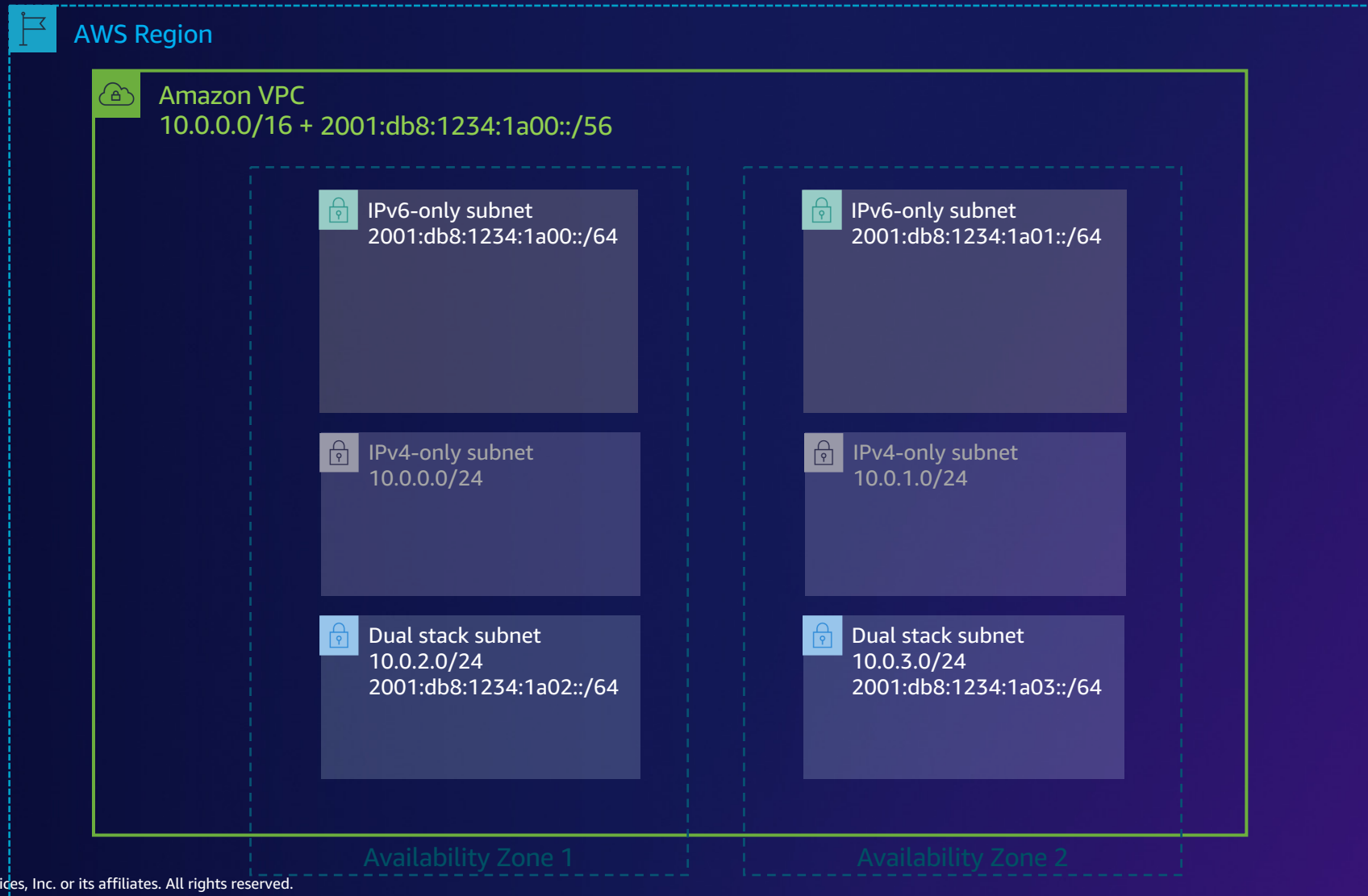
2001:db8:1234:1a00::ec2

Amazon EC2: Resource-based naming





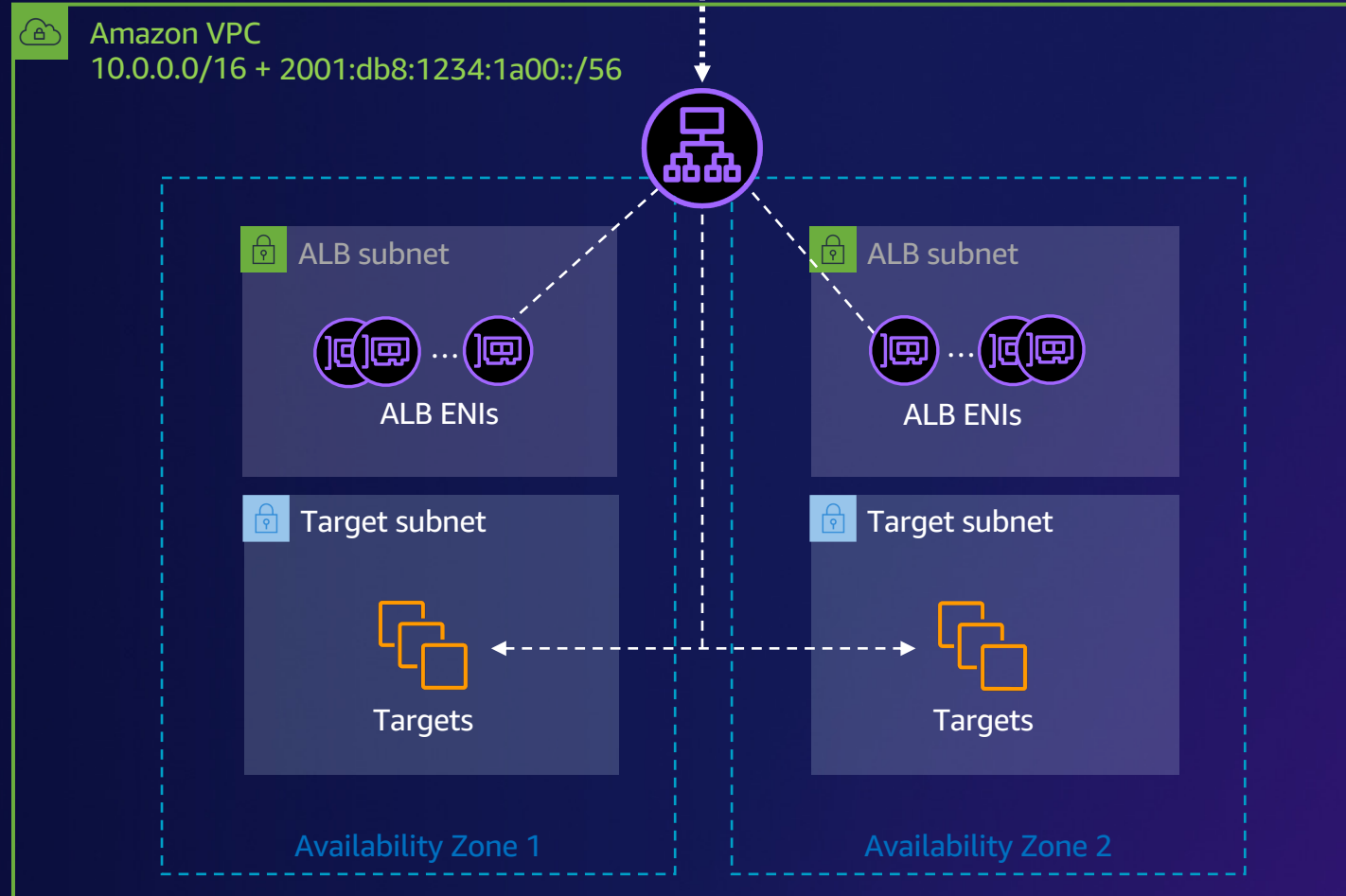
Starting from the dual-stack VPC



Application Load Balancer (ALB)

Application Load Balancer: Deployment

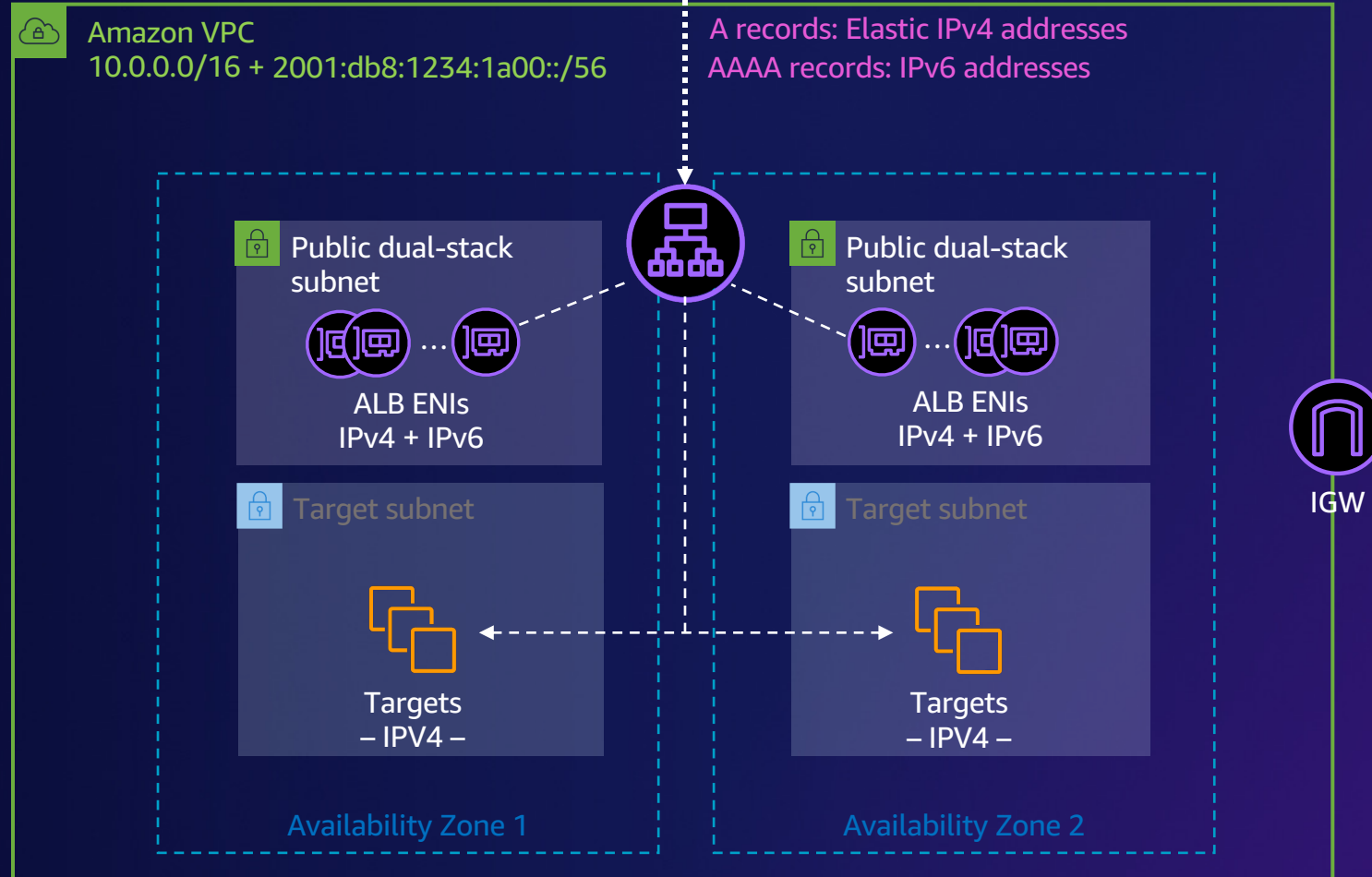
my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com



Application Load Balancer: Dual-stack support

INTERNET-FACING DUAL-STACK

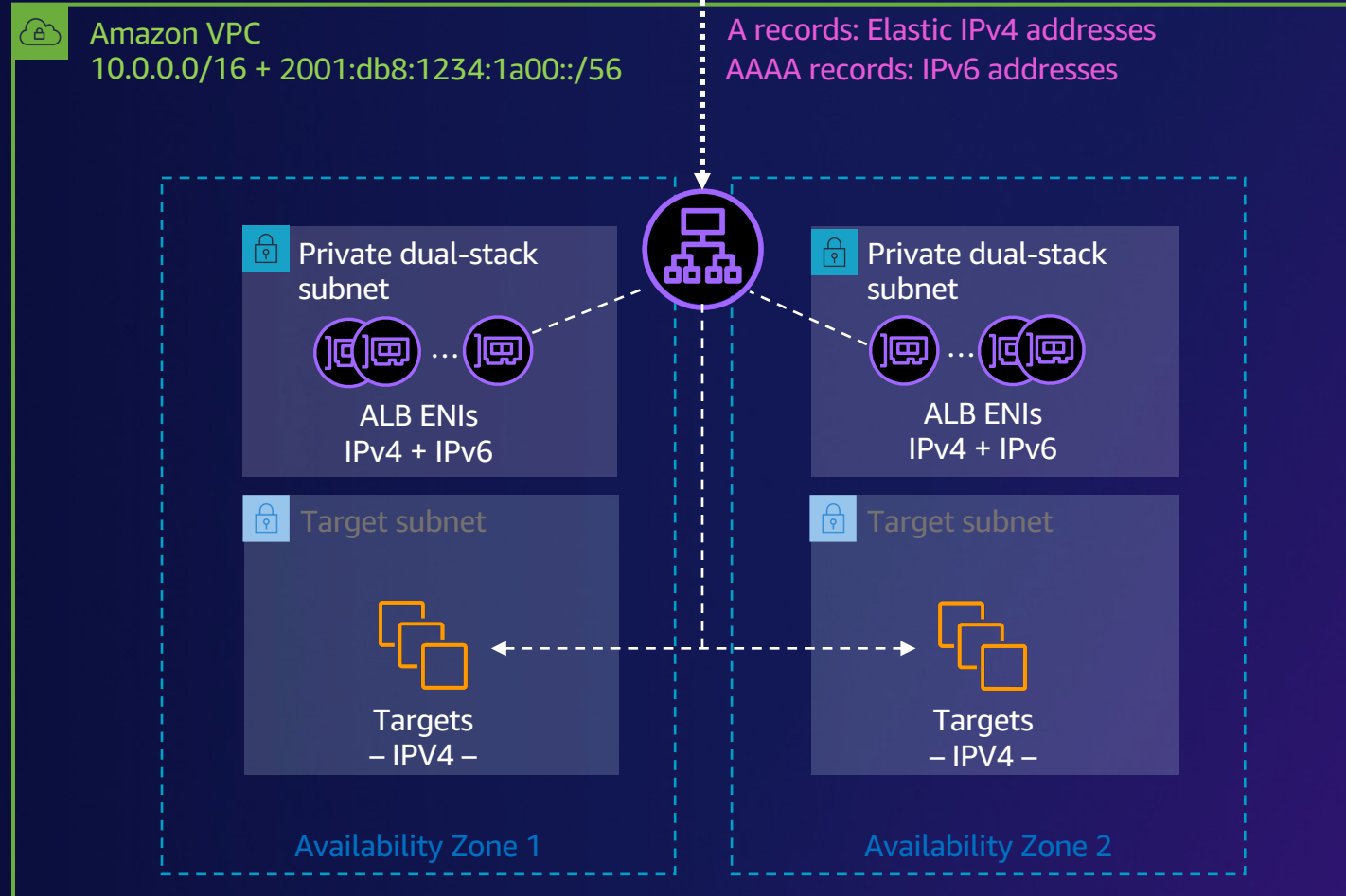
my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com



Application Load Balancer: Dual-stack support

INTERNAL DUAL STACK

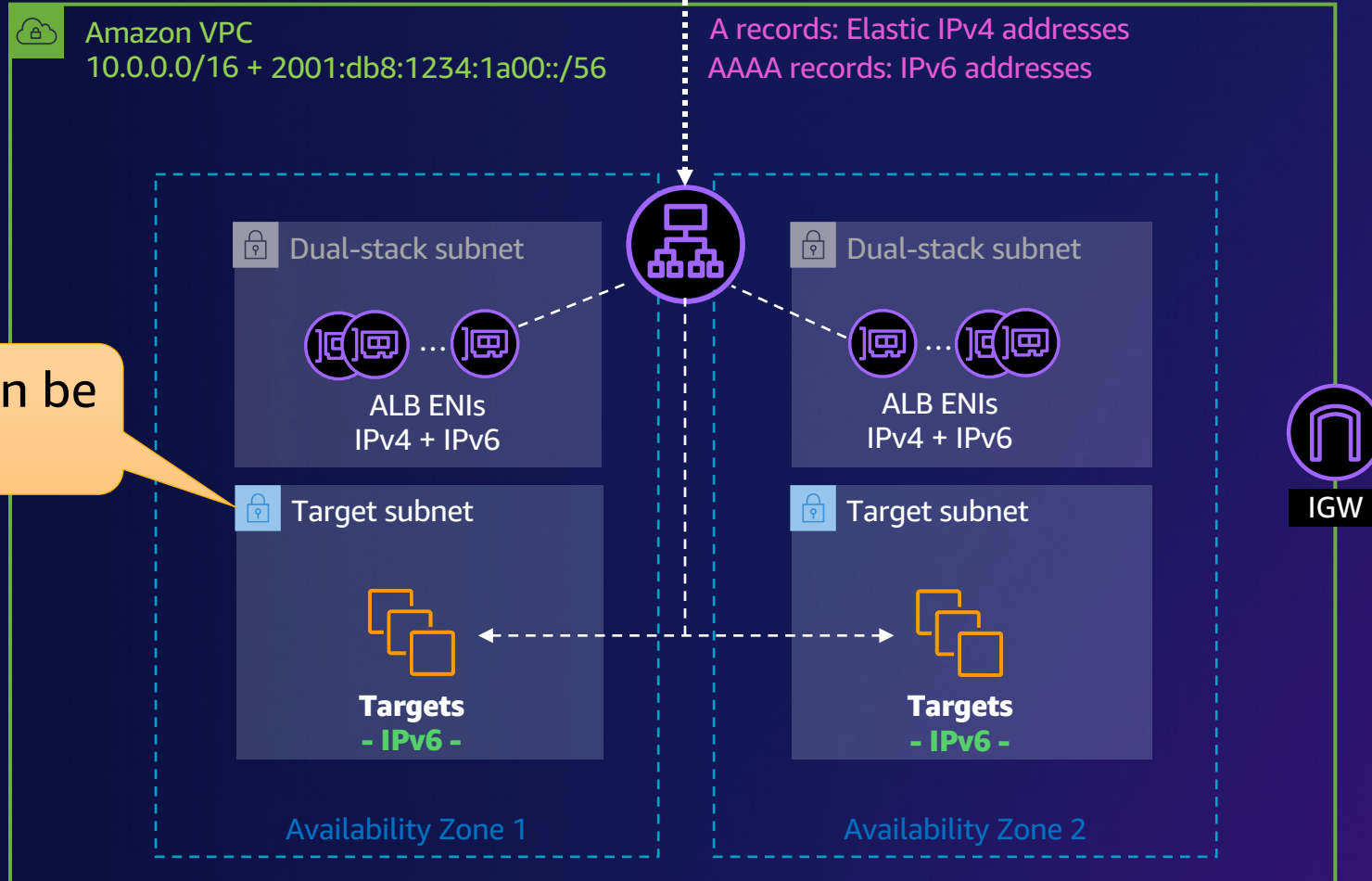
my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com



Application Load Balancer: End-to-end IPv6

IPV6 TARGETS

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

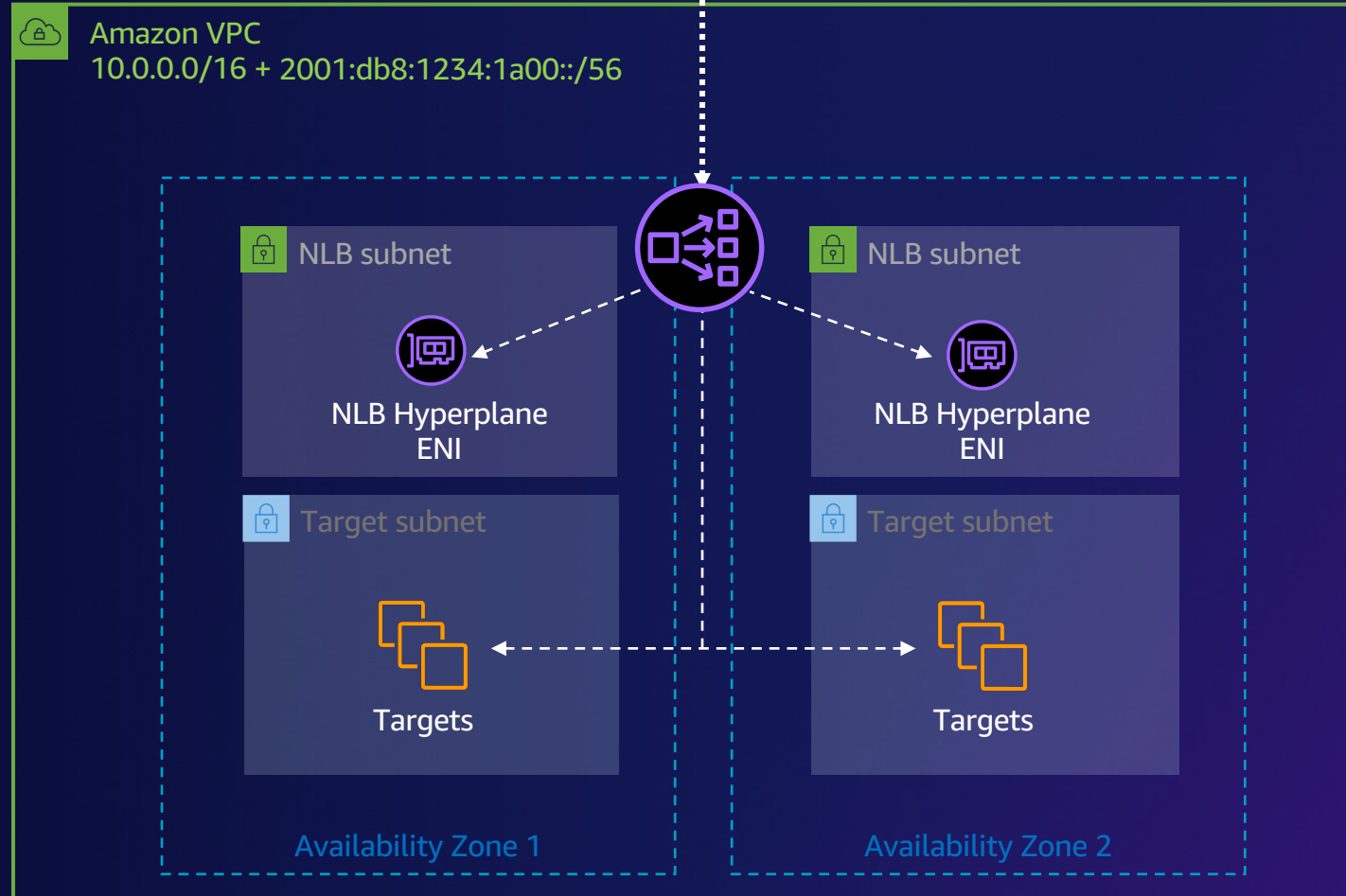


Target subnets can be IPv6-only

Network Load Balancer (NLB)

Network Load Balancer: Deployment

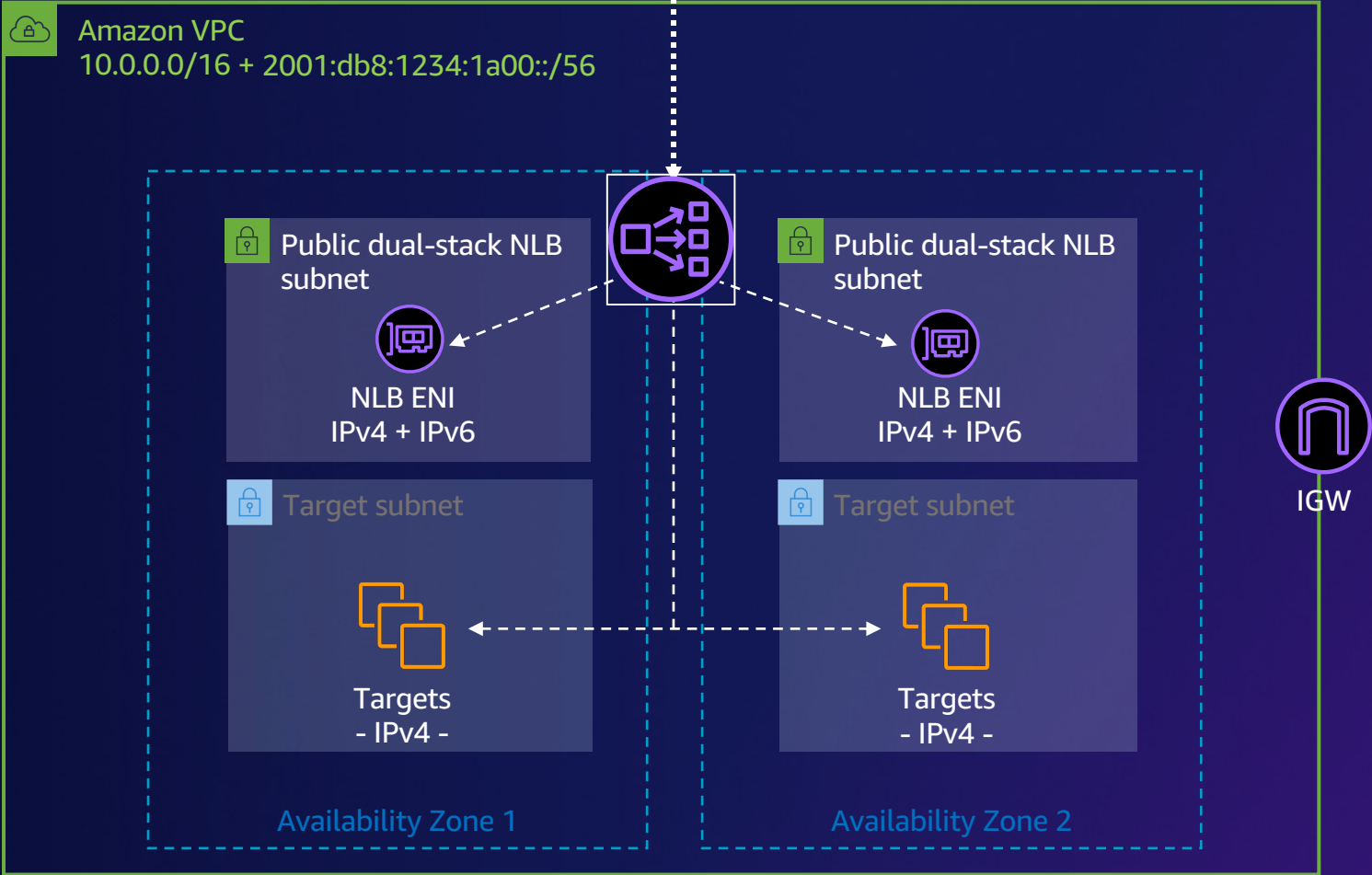
my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com



Network Load Balancer: Dual-stack support

INTERNET-FACING DUAL STACK

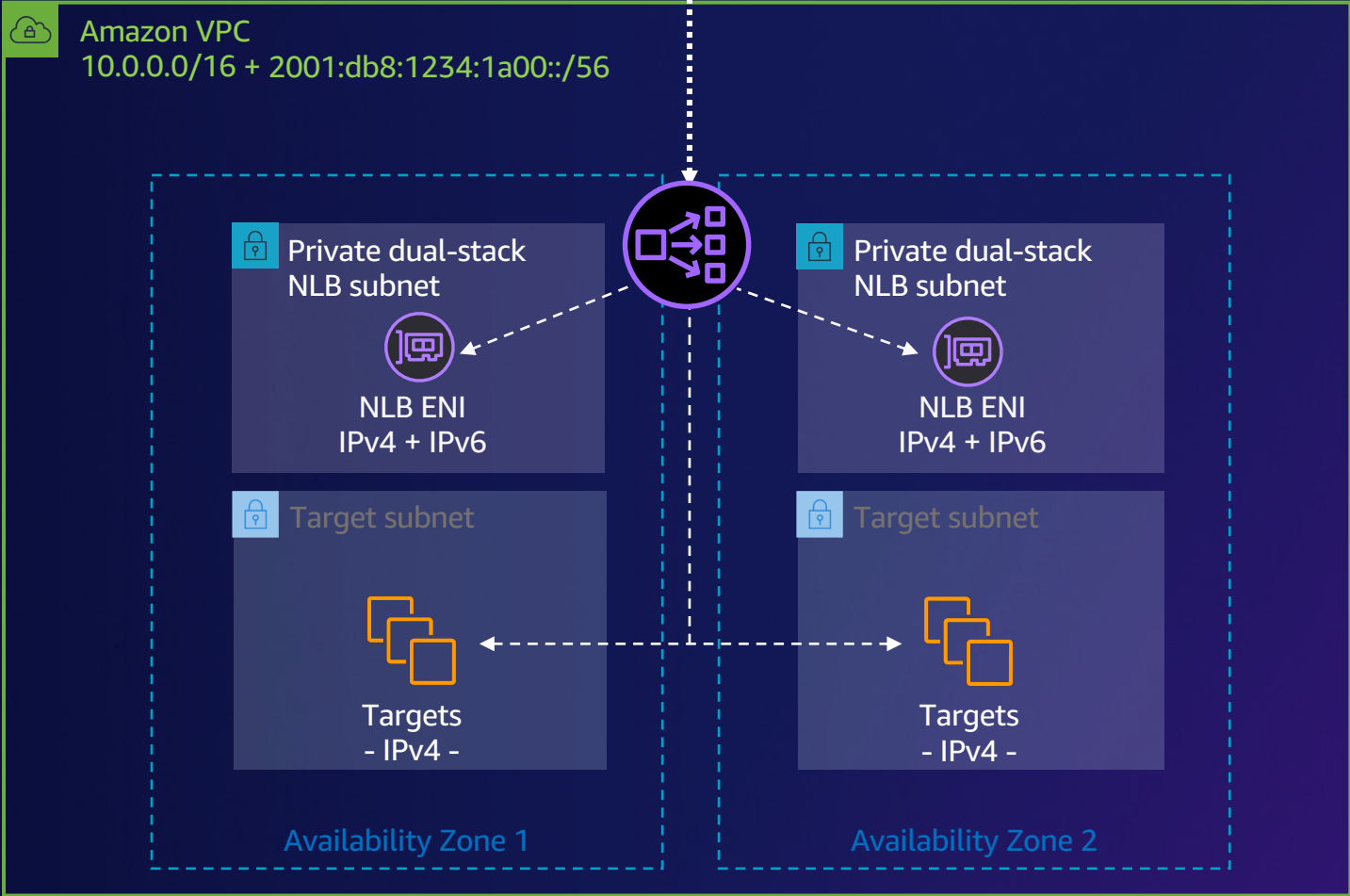
my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com



Network Load Balancer: Dual-stack support

INTERNAL DUAL STACK

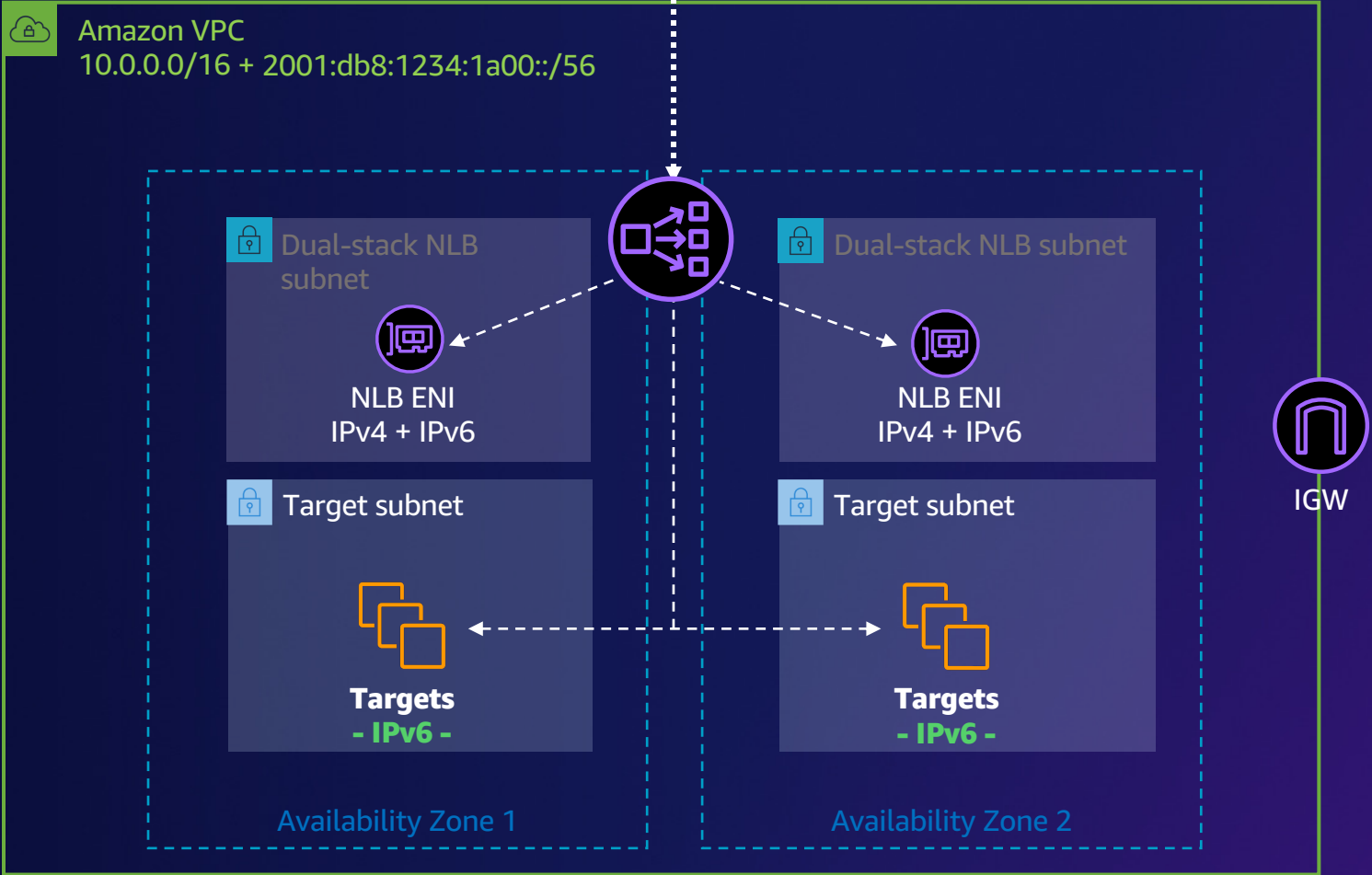
my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com



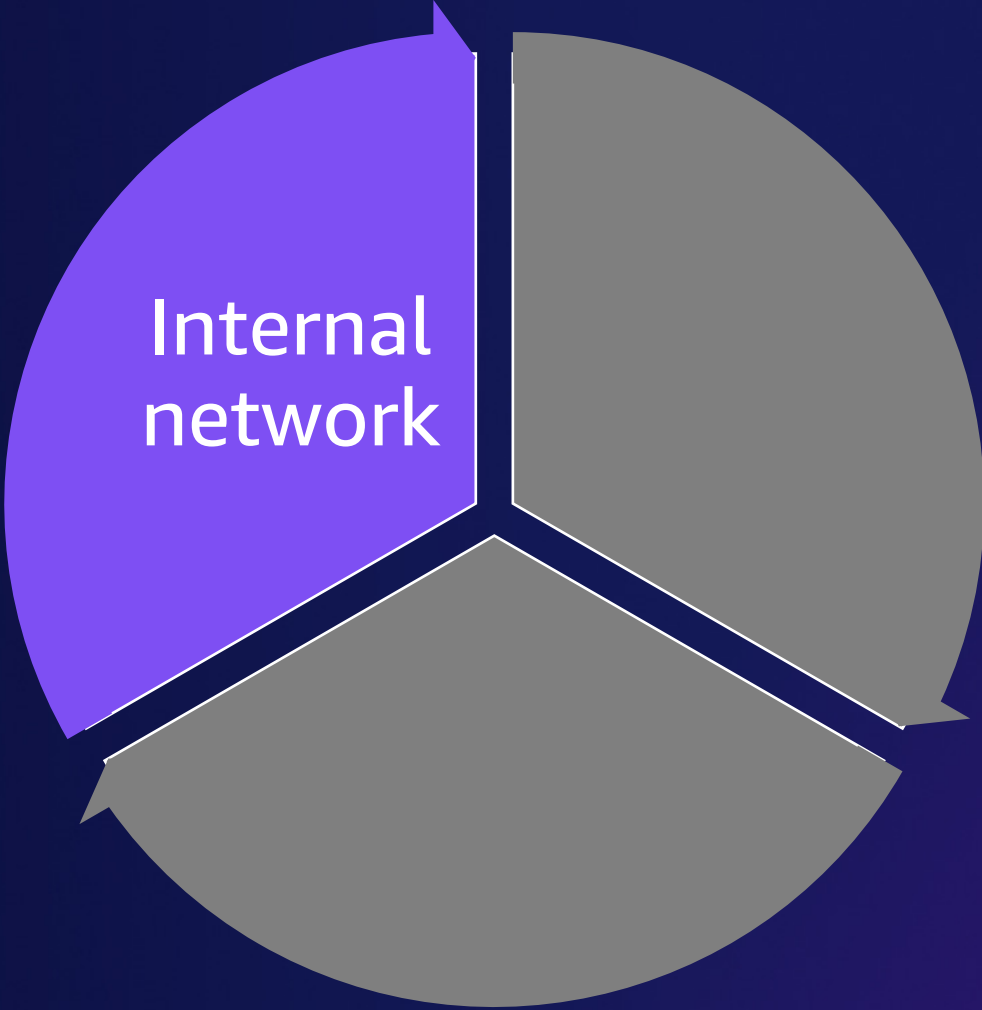
Network Load Balancer: End-to-end IPv6

IPV6 TARGETS

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

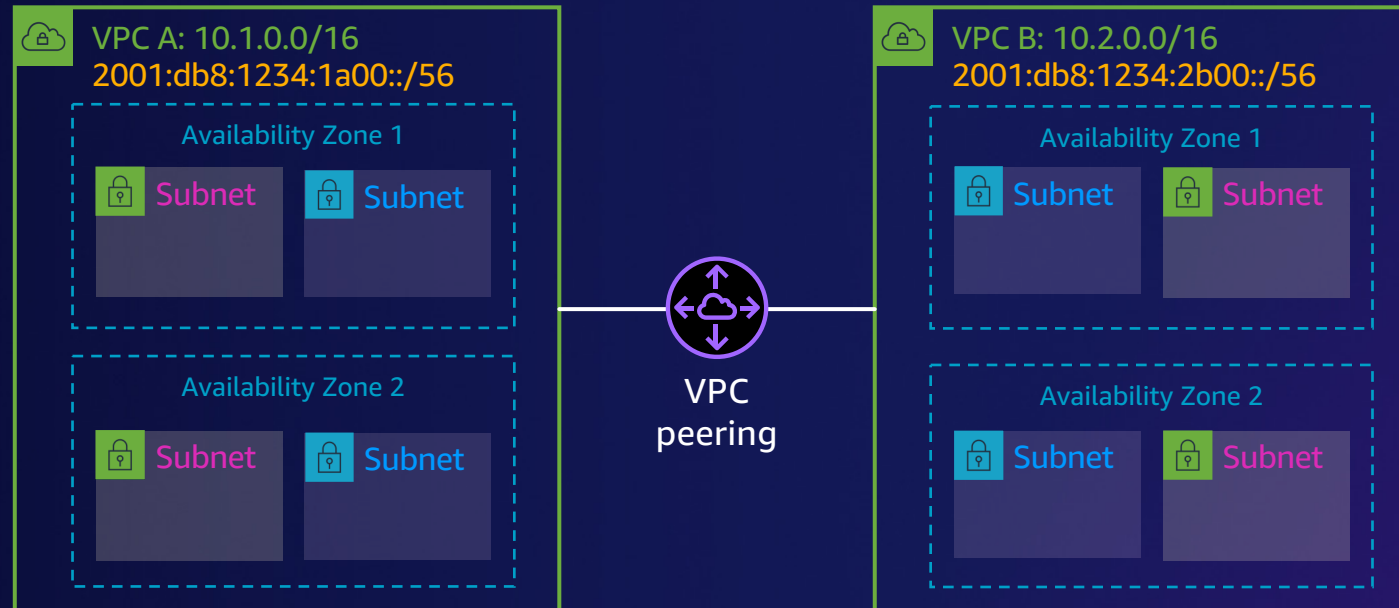


For both ALB and NLB, IPv6 targets must be IP-type, in your VPC or in a peered VPC



Dual stack VPC-to-VPC connectivity

VPC PEERING



VPC A route table

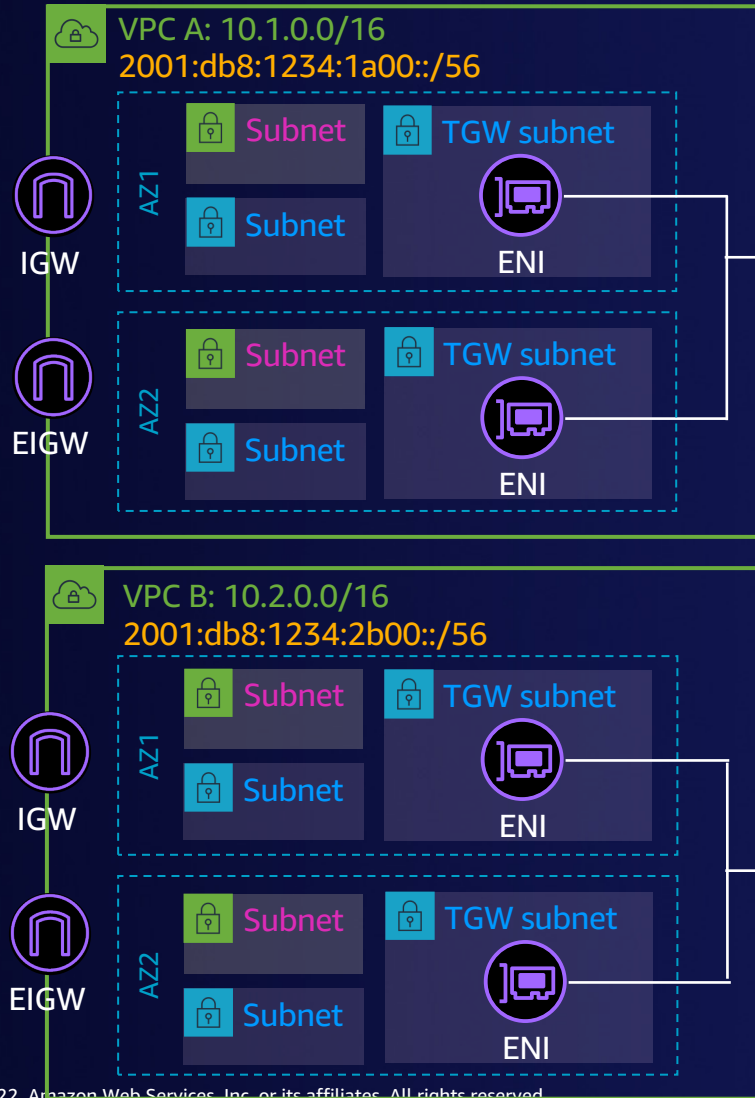
Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1a00::/56	Local
10.2.0.0/16	PCX-ID
2001:db8:1234:2b00::/56	PCX-ID

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

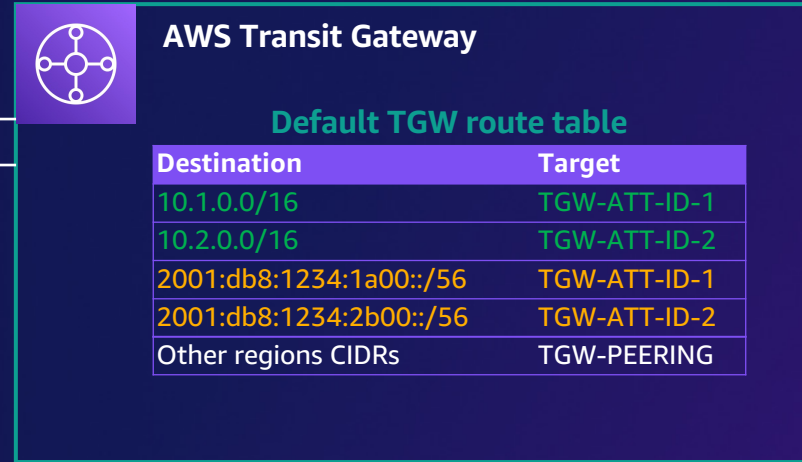
Dual stack VPC-to-VPC connectivity at scale

AWS TRANSIT GATEWAY



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	TGW



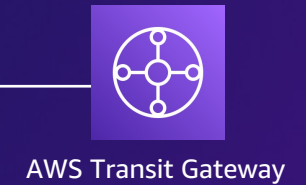
Default TGW route table

Destination	Target
10.1.0.0/16	TGW-ATT-ID-1
10.2.0.0/16	TGW-ATT-ID-2
2001:db8:1234:1a00::/56	TGW-ATT-ID-1
2001:db8:1234:2b00::/56	TGW-ATT-ID-2
Other regions CIDRs	TGW-PEERING

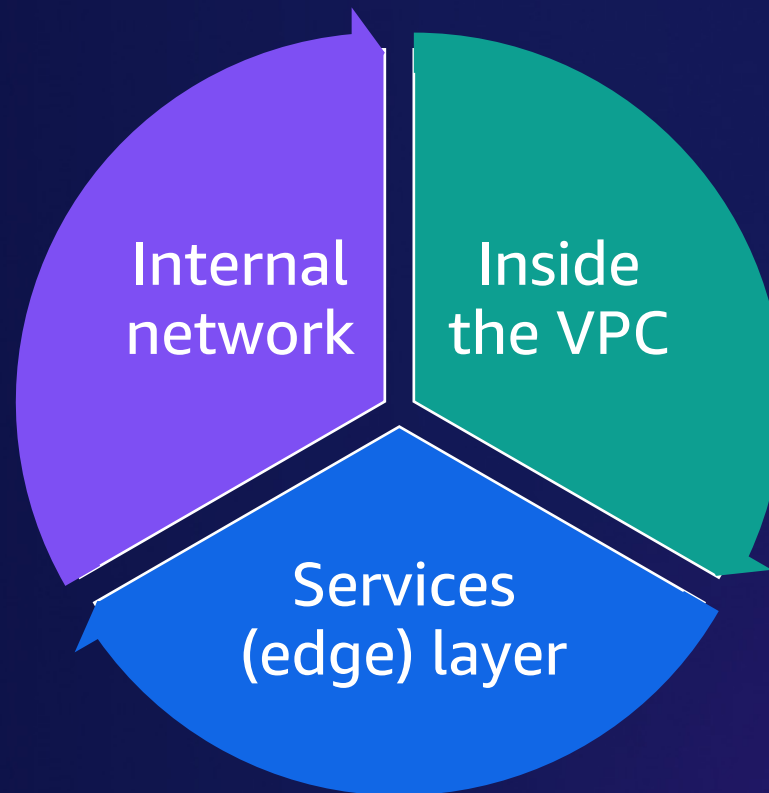
TGW VPC attachments

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	TGW



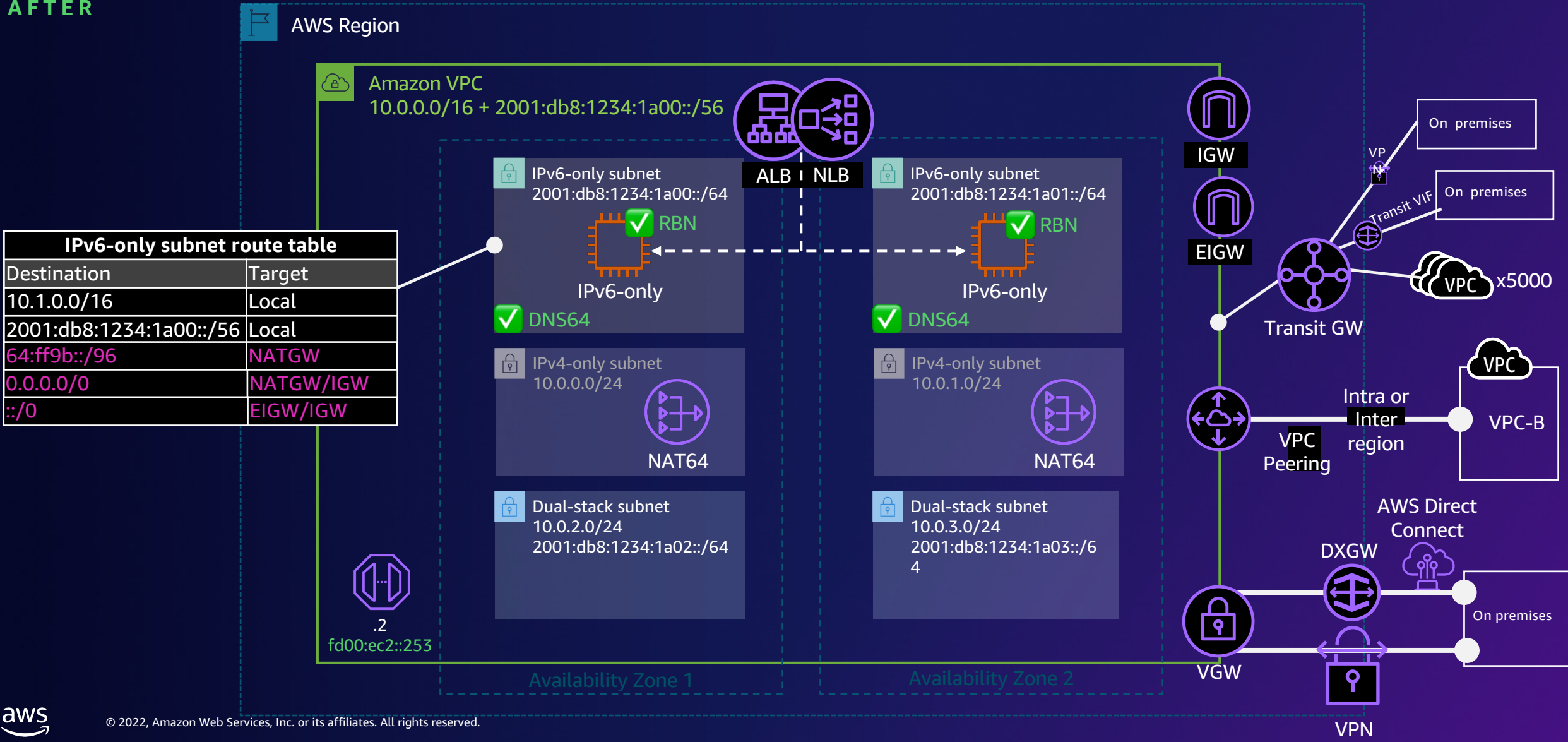
Putting everything together



Dual-stack Amazon VPC: IPv6 native



AFTER



Thank you!

Alexandra Huides

huidesa@amazon.com

