Architect and build IPv6 networks on AWS

Alexandra Huides
Principal Network Specialist Solutions Architect
AWS


The WHYs
IPv6 adoption on AWS

WHY ADOPT IPv6 ON AWS?

Improve network scalability

Start building experience

Minimize NAT (public & private)

Simplify global connectivity

Improve network scalability

SIMPLY MORE ADDRESSES

NO MORE SUBNETTING CHALLENGES

IPV6-ONLY DEPLOYMENTS SUPPORTED

Improve network scalability

SIMPLY MORE ADDRESSES

NO MORE SUBNETTING CHALLENGES

IPV6-ONLY DEPLOYMENTS SUPPORTED

Start building experience

EASY TO DEPLOY & TEST

BUILD BACWARDS COMPATIBILITY WITH IPV4

ADDRESS WHAT BRINGS VALUE

Improve network scalability

SIMPLY MORE ADDRESSES

NO MORE SUBNETTING CHALLENGES

IPV6-ONLY DEPLOYMENTS SUPPORTED

Start building experience

EASY TO DEPLOY & TEST

BUILD BACWARDS COMPATIBILITY WITH IPV4

ADDRESS WHAT BRINGS VALUE

Minimize NAT (public & private)

NO NEED FOR PUBLIC NAT

NO NEED FOR PRIVATE NAT

IMPROVED VISIBILITY & SECURITY

Improve network scalability

SIMPLY MORE ADDRESSES

NO MORE SUBNETTING CHALLENGES

IPV6-ONLY DEPLOYMENTS SUPPORTED

Start building experience

EASY TO DEPLOY & TEST

BUILD BACWARDS COMPATIBILITY WITH IPV4

ADDRESS WHAT BRINGS VALUE

Minimize NAT (public & private)

NO NEED FOR PUBLIC NAT

NO NEED FOR PRIVATE NAT

IMPROVED VISIBILITY & SECURITY

Simplify global connectivity

NO MORE OVERLAPPING IPs

INTEGRATE MERGERS AND ACQUISITIONS

SUMMARIZATION AND EFFICIENT ROUTING

Improve network scalability

SIMPLY MORE ADDRESSES

NO MORE SUBNETTING CHALLENGES

IPV6-ONLY DEPLOYMENTS SUPPORTED

Start building experience

EASY TO DEPLOY & TEST

BUILD BACWARDS COMPATIBILITY WITH IPV4

ADDRESS WHAT BRINGS VALUE

Minimize NAT (public & private)

NO NEED FOR PUBLIC NAT

NO NEED FOR PRIVATE NAT

IMPROVED VISIBILITY & SECURITY

Simplify global connectivity

NO MORE OVERLAPPING IPs

INTEGRATE MERGERS AND ACQUISITIONS

SUMMARIZATION AND EFFICIENT ROUTING

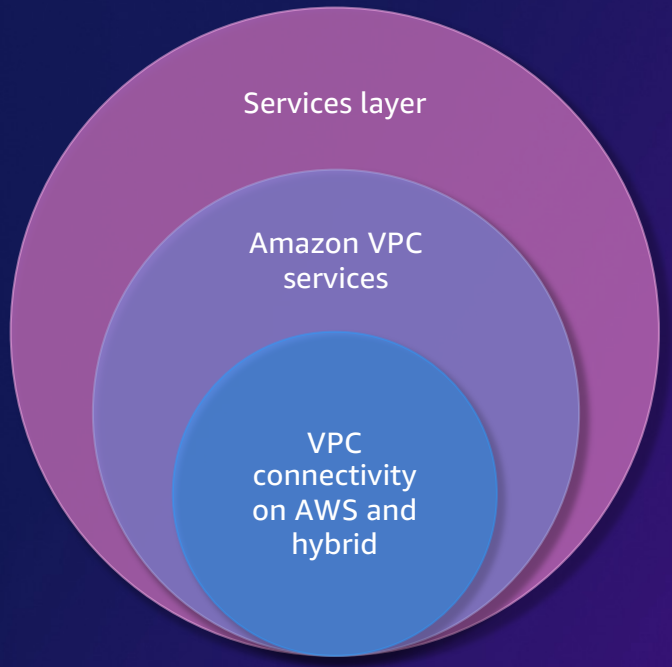

Approaches
IPv6 adoption on AWS
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
NANOG

IPv6 adoption approaches

Outside in (Edge first)

Inside out (Internal first)

Outside in
(Edge first)



Outside in
(Edge first)

- IPv6-enabled end-client experience[1]
- Expanded user base in geographies with high IPv6 adoption
- No CGNAT in Service Provider networks for IPv6 clients
- Contribute to, and facilitate global IPv6 usage increase

[1] Check https://stats.labs.apnic.net/v6perf/XA

Outside in
(Edge first)

Aroundhome

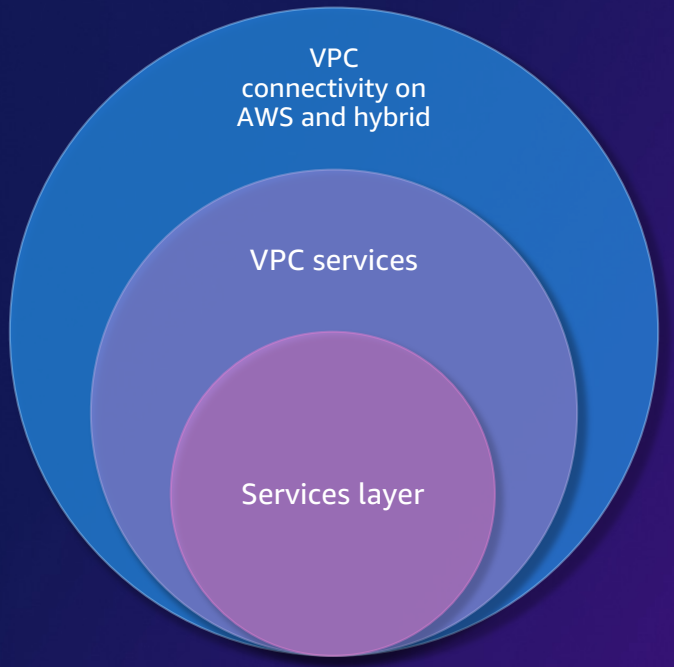
We have enabled IPv6 on our load balancers (ALB) and CloudFront distributions so customers can already reach our services through IPv6. It turned out to be a very smooth process without any hiccups.

Within a short amount of time we were able to report nearly 40 percent of our customer traffic to be IPv6

Hendrik Bergunde, Team Lead Technology - Aroundhome

Read more

Inside out
(Internal first)



Inside out
(Internal first)

- Unlock scale for container and platform deployments
- Scale internal network connectivity
- Accelerate the integration of mergers and acquisitions
- Build familiarity with IPv6, adjust internal tooling

Inside out
(Internal first)

NETFLIX

"IPv6 adoption in the internal network enabled the full IP reachability Netflix needed across the thousands of VPCs without the need for Network Address Translation. Also, the Egress-only Internet Gateway helped maintain the private subnets security posture.

Enabling IPv6 across the Netflix streaming platform in AWS enabled continued hyperscale growth, scalability and innovation."

Donavan Fritz, Senior Network SRE - Netflix

Read more


IPv6 adoption on AWS
More customer stories
infor
NANOG
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IPv6 adoption focus areas

Network

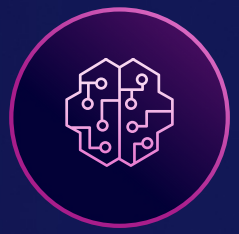
Operating system

App code

Services & tools


2000::/3
2001:db8:1234:1a00:1234:1234:1234:ec2
Where to start with
IPv6 adoption on AWS
fc00::/7

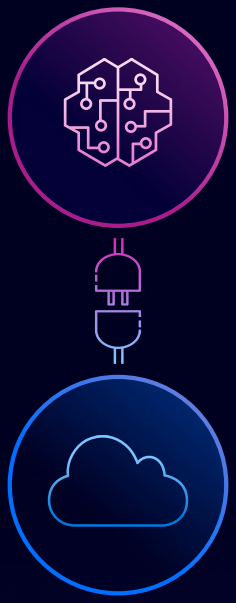
IPv6 adoption
where to start



IPv6 addressing plan

Dual stack Amazon VPC

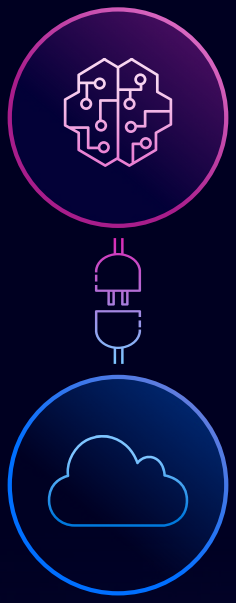
IPv6 addressing plan



Dual stack Amazon VPC

Amazon-provided GUA (VPC-level)

IPv6 addressing plan



Dual stack Amazon VPC

Amazon VPC

10.1.0.0/16

2001:db8:1234:1a00::/56 default IPv6 prefix size

Amazon-provided GUA

Dual stack Amazon VPC

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

- (•) VPC only
- ( ) VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

My-New-VPC

IPv4 CIDR block Info

- (•) IPv4 CIDR manual input
- ( ) IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.1.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- ( ) No IPv6 CIDR block
- ( ) IPAM-allocated IPv6 CIDR block
- (•) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

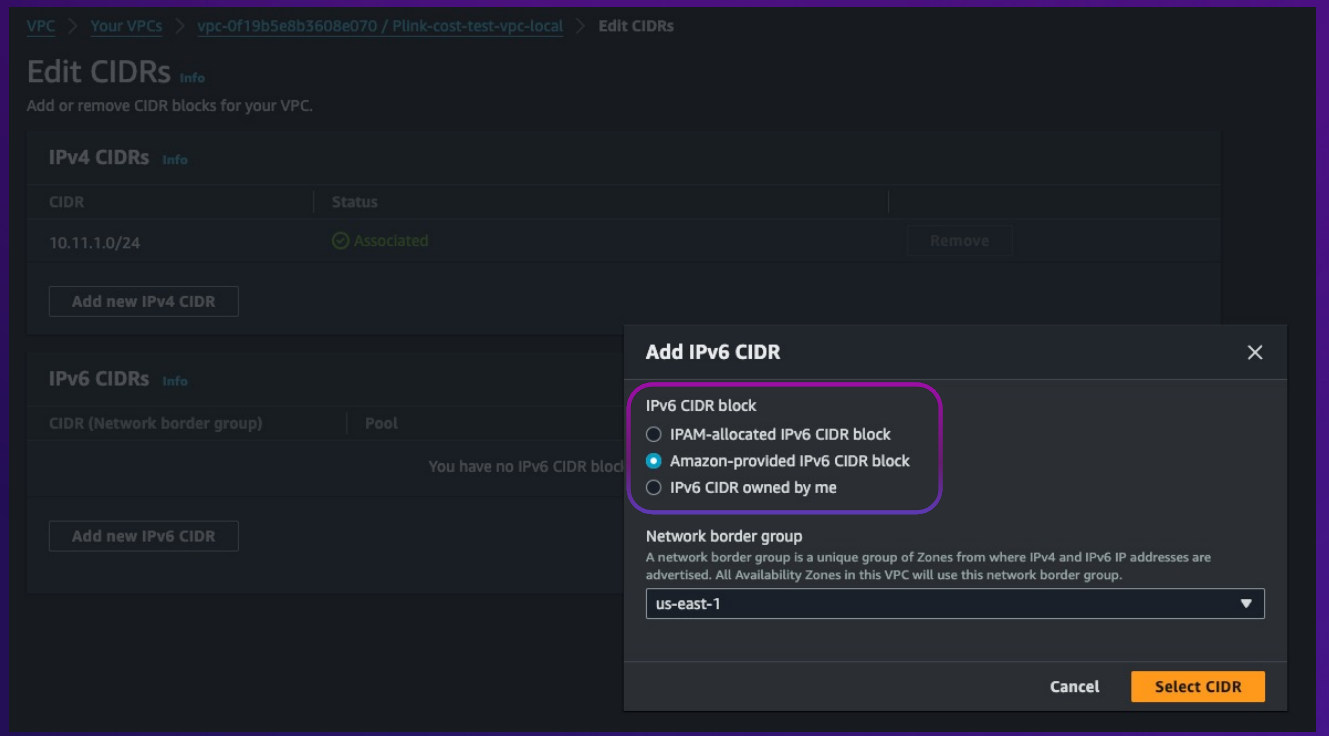
Network border group
A network border group is a unique group of Zones from where IPv4 and IPv6 IP addresses are advertised. All Availability Zones in this VPC will use this network border group.

us-east-1 ▼

Tenancy Info

Default ▼

Dual stack Amazon VPC



Dual stack Amazon VPC

VPC > Your VPCs > vpc-0f19b5e8b3608e070 / Plink-cost-test-vpc-local > Edit CIDRs

Edit CIDRs Info

Add or remove CIDR blocks for your VPC.

IPv4 CIDRs Info

CIDR	Status	
10.11.1.0/24	Associated	Remove

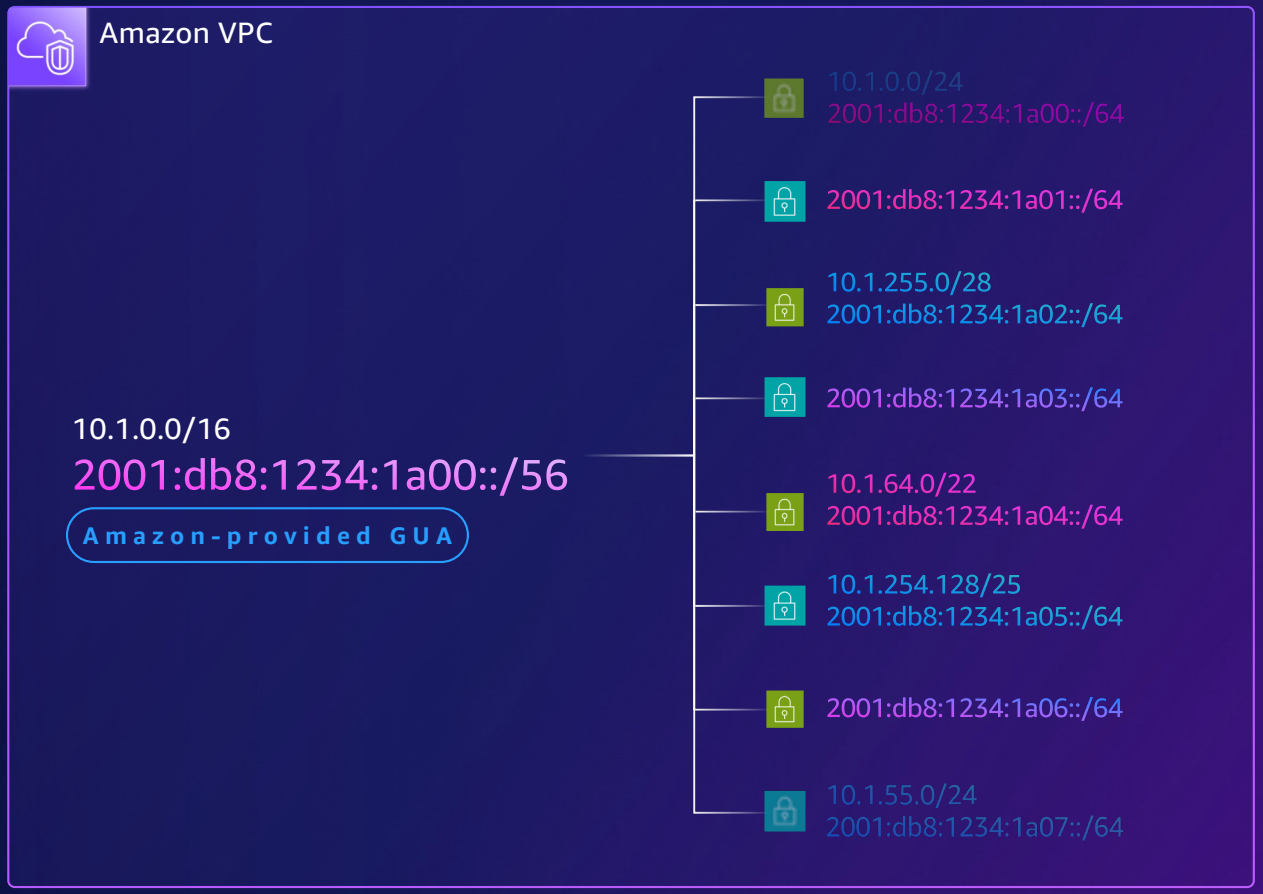
Add new IPv4 CIDR

IPv6 CIDRs Info

CIDR (Network border group)	Pool	Status	
2600:1f18:2992:5500::/56 (us-east-1)	Amazon	Associated	Remove

Add new IPv6 CIDR

Dual stack Amazon VPC



Dual stack Amazon VPC

Amazon VPC

10.1.0.0/16

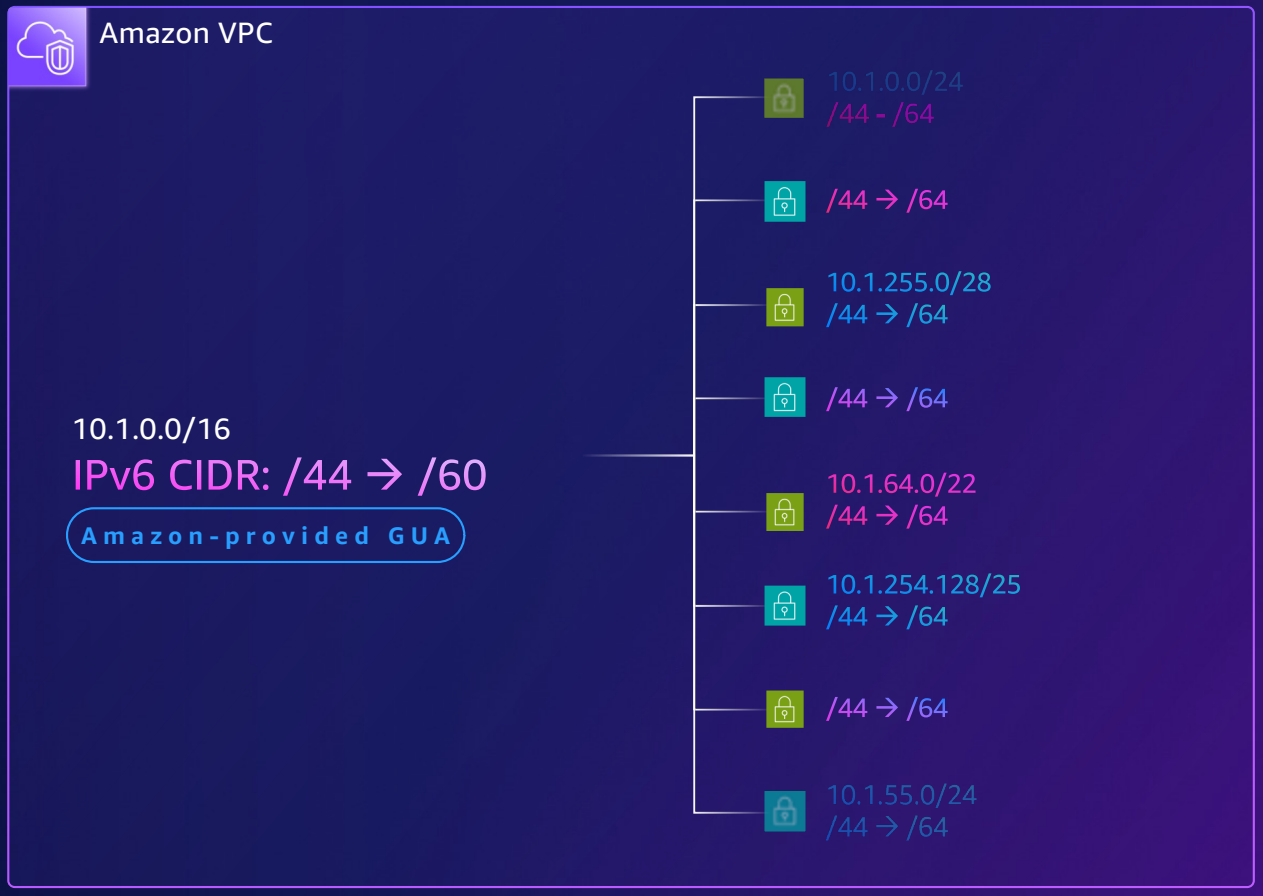
IPv6 CIDR: /44 → /60 tiered IPv6 prefix size

Amazon-provided GUA

aws

NANOG™

Dual stack Amazon VPC



Dual stack Amazon VPC

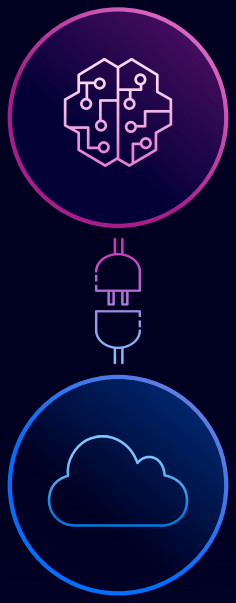
Amazon VPC

10.1.0.0/16

Amazon-provided IPv6 Prefix

Randomly assigned by default

IPv6 addressing plan



Dual stack Amazon VPC

Amazon-provided GUA (VPC-level)

Amazon-provided contiguous IPv6 GUA prefixes

NEW

Amazon VPC IP Address Manager

Amazon-provided contiguous IPv6 prefixes

Amazon VPC IP Address Manager

Free tier

For IP management in a single AWS Region and account

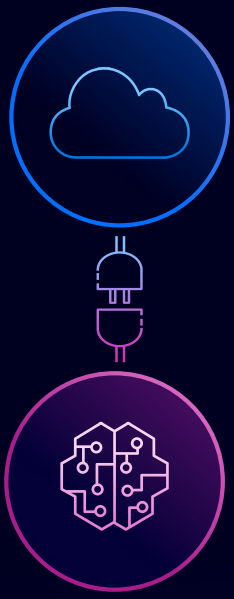
Amazon-provided contiguous IPv6 blocks per Region and account

Advanced tier

For IP management across two or more AWS Regions and accounts

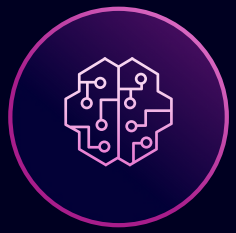
Amazon-provided contiguous IPv6 blocks across multiple Regions and accounts

Dual stack Amazon VPC



IPv6 addressing plan

- Amazon-provided GUA (VPC-level)
- Amazon-provided contiguous IPv6 GUA prefixes
- Bring your own IPv6 (BYOIPv6) GUA prefixes



IPv6 addressing plan

BYOIPv6

	In Amazon EC2	With VPC IPAM
	You can bring each address range to one AWS Region at a time	You can bring each address range to an IPAM top level Pool, and further split it across multiple Regional pools
	You cannot share your IP address range with other accounts	You can share your IP address range with other accounts
	You can control if CIDRs in a pool can be publicly advertisable or not	You can control if CIDRs in a pool can be publicly advertisable or not
	The most specific IPv6 address range that you can bring is **/48** for CIDRs that are publicly advertisable and **/56** for CIDRs that are not publicly advertisable	The most specific IPv6 address range that you can bring is **/48** for CIDRs that are publicly advertisable and **/60** for CIDRs that are not publicly advertisable

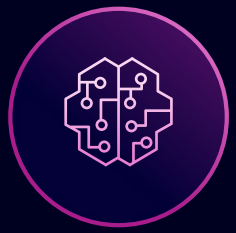
aws

NANOG™

IPv6 addressing plan

BYOIPv6

Note: The prefix used for this presentation is an Amazon-owned IPv6 prefix, and prefix sizes are examples.



IPv6 address planning summary

	Provisioning	Globally Unique	Internet advertisement	Internet Connectivity	NAT66 / NPTv6	Summarization capabilities	Considerations
Amazon-provided IPv6 GUA (VPC-level)	Directly at the VPC level	Yes	AWS advertised	Native on AWS	Not Required	No	Not recommended for large scale deployments (many VPCs)
Amazon-provided contiguous IPv6 prefixes	Amazon VPC IPAM free or advanced tiers	Yes	AWS advertised	Native on AWS	Not Required	Yes, for all VPCs created from the same IPAM Pool	Facilitates growth on AWS, doesn't require you to own IPv6 addresses
BYOIPv6	Amazon EC2 or Amazon VPC IPAM	Yes	Configurable	Native on AWS if advertised from AWS	Not Required	Yes, for all VPCs created from the same BYOIP pool	Facilitates growth on AWS, requires you to own IPv6 addresses, and prove ownership through the BYOIPv6 process.
				On-premises if advertised from on-premises	Not Required		

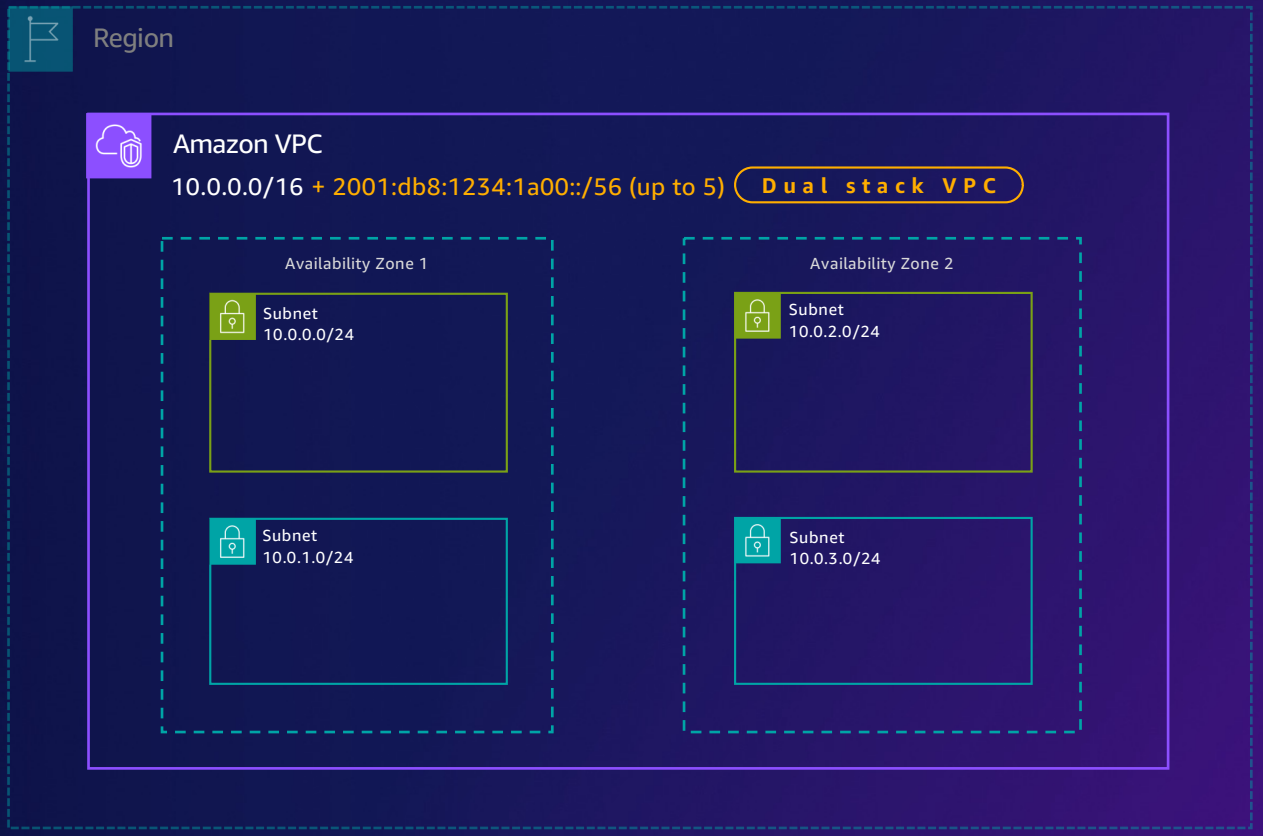

IPv6 adoption
Inside out


Start with
Dual stack Amazon VPC

Dual stack Amazon VPC

IPv6 design

Dual stack VPC

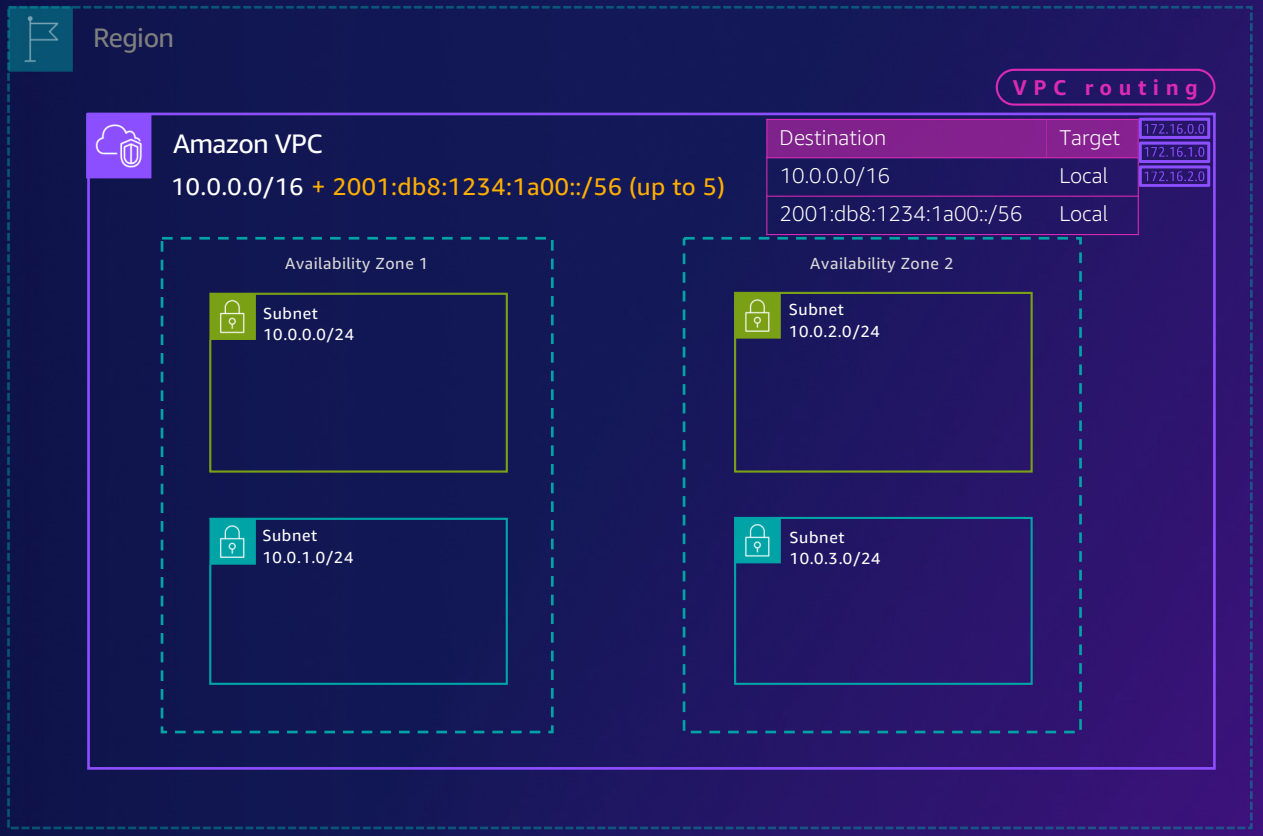


Dual stack Amazon VPC

IPv6 design

Dual stack VPC

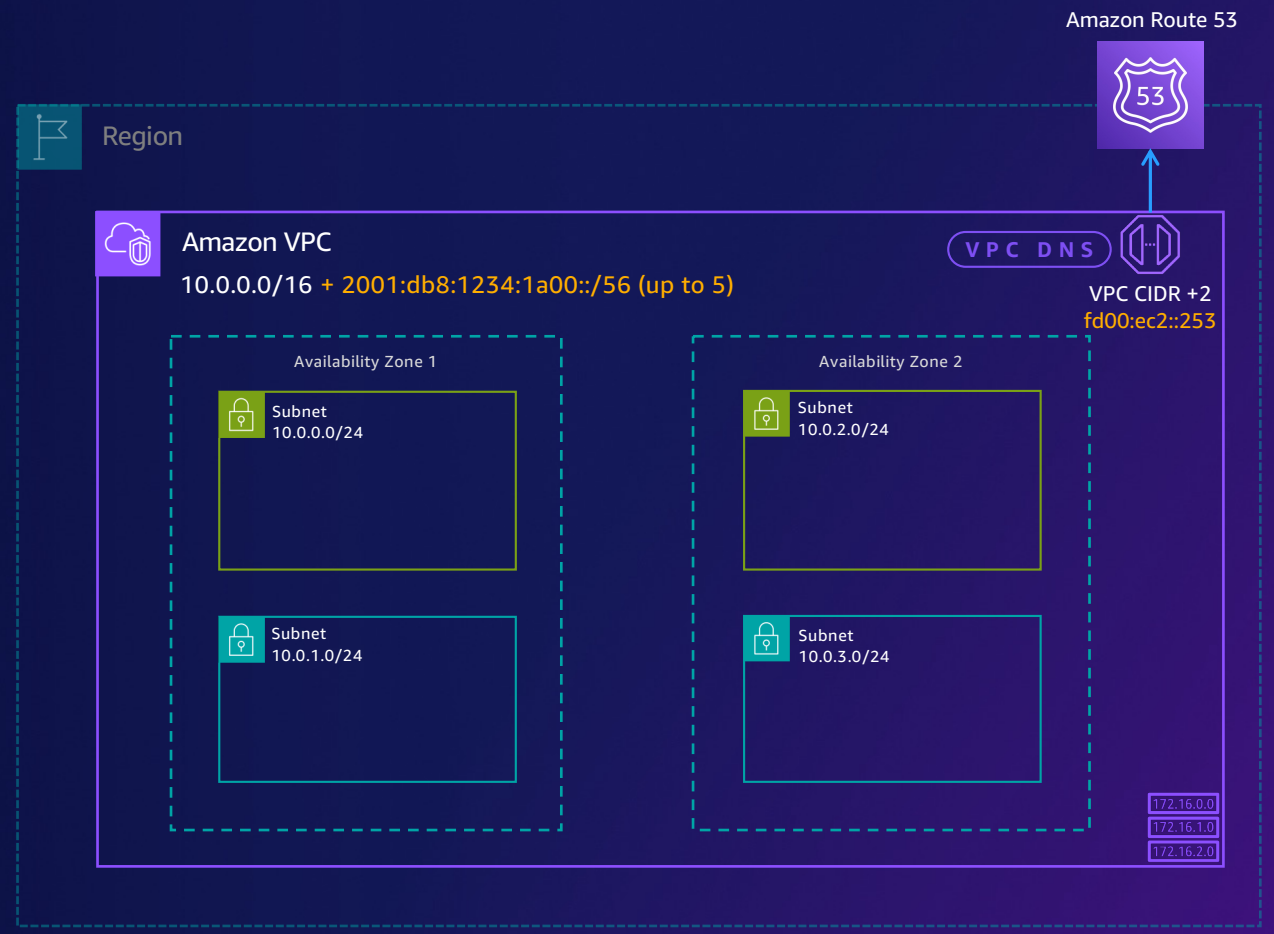
VPC routing



Dual stack Amazon VPC

IPv6 design

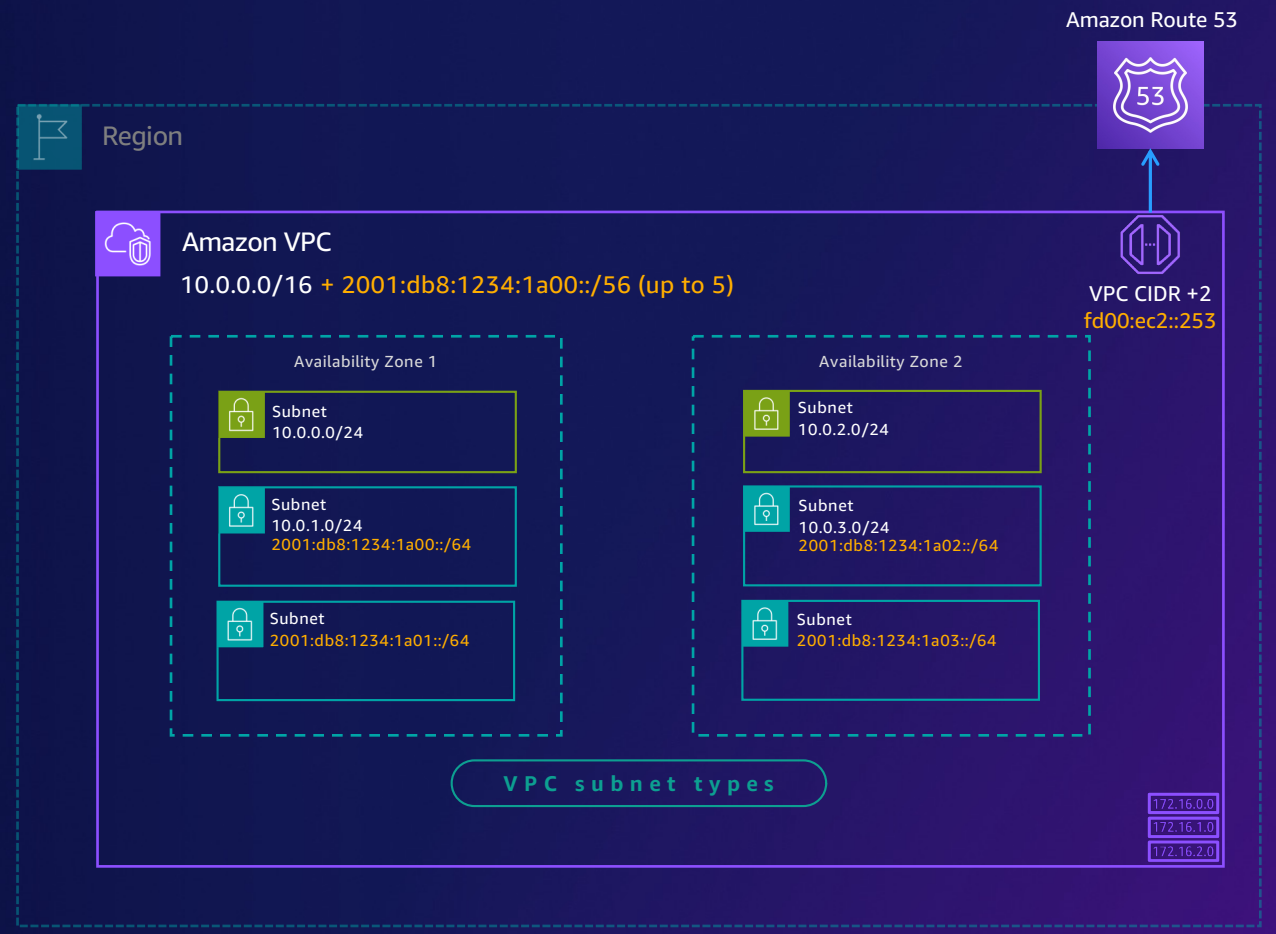
- Dual stack VPC
- VPC routing
- VPC DNS



Dual stack Amazon VPC

IPv6 design

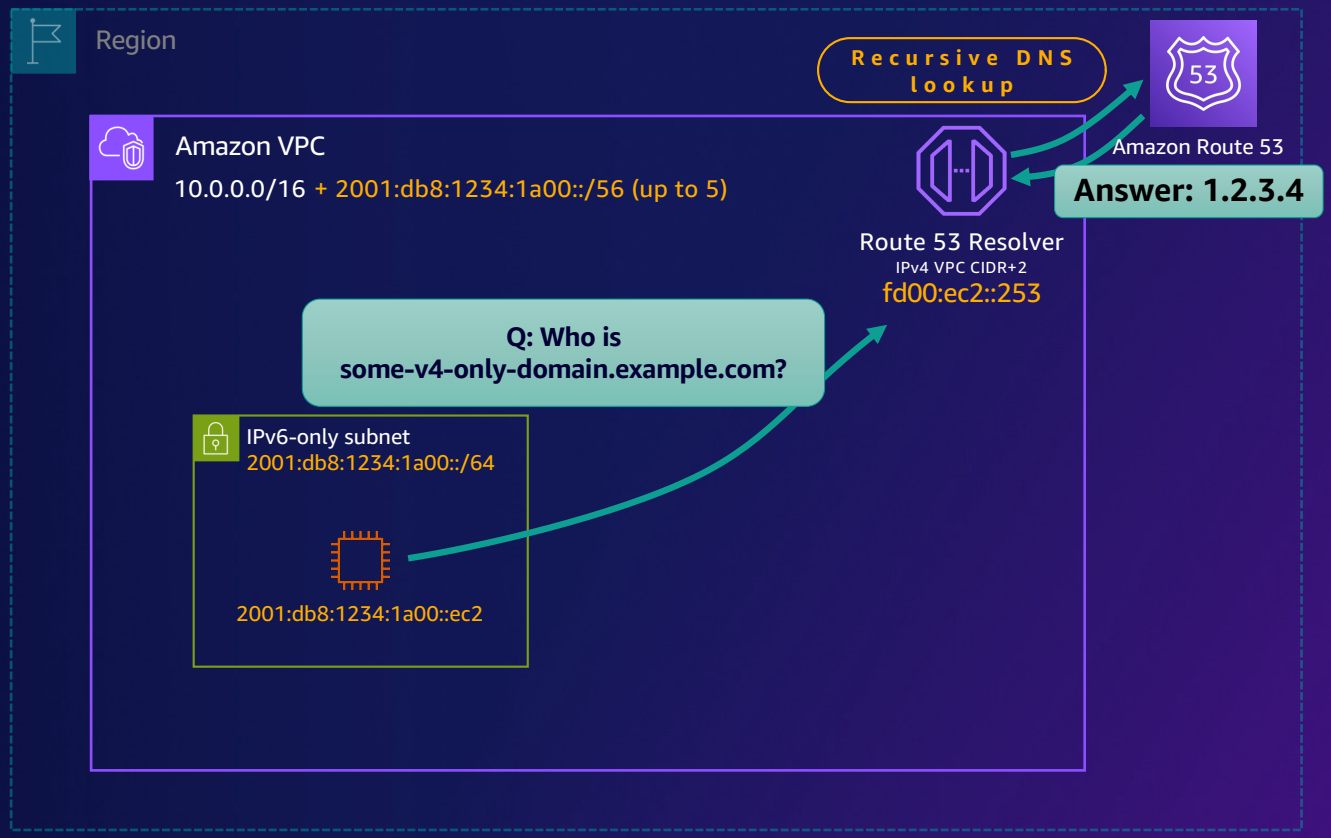
- Dual stack VPC
- VPC routing
- VPC DNS
- VPC Subnets

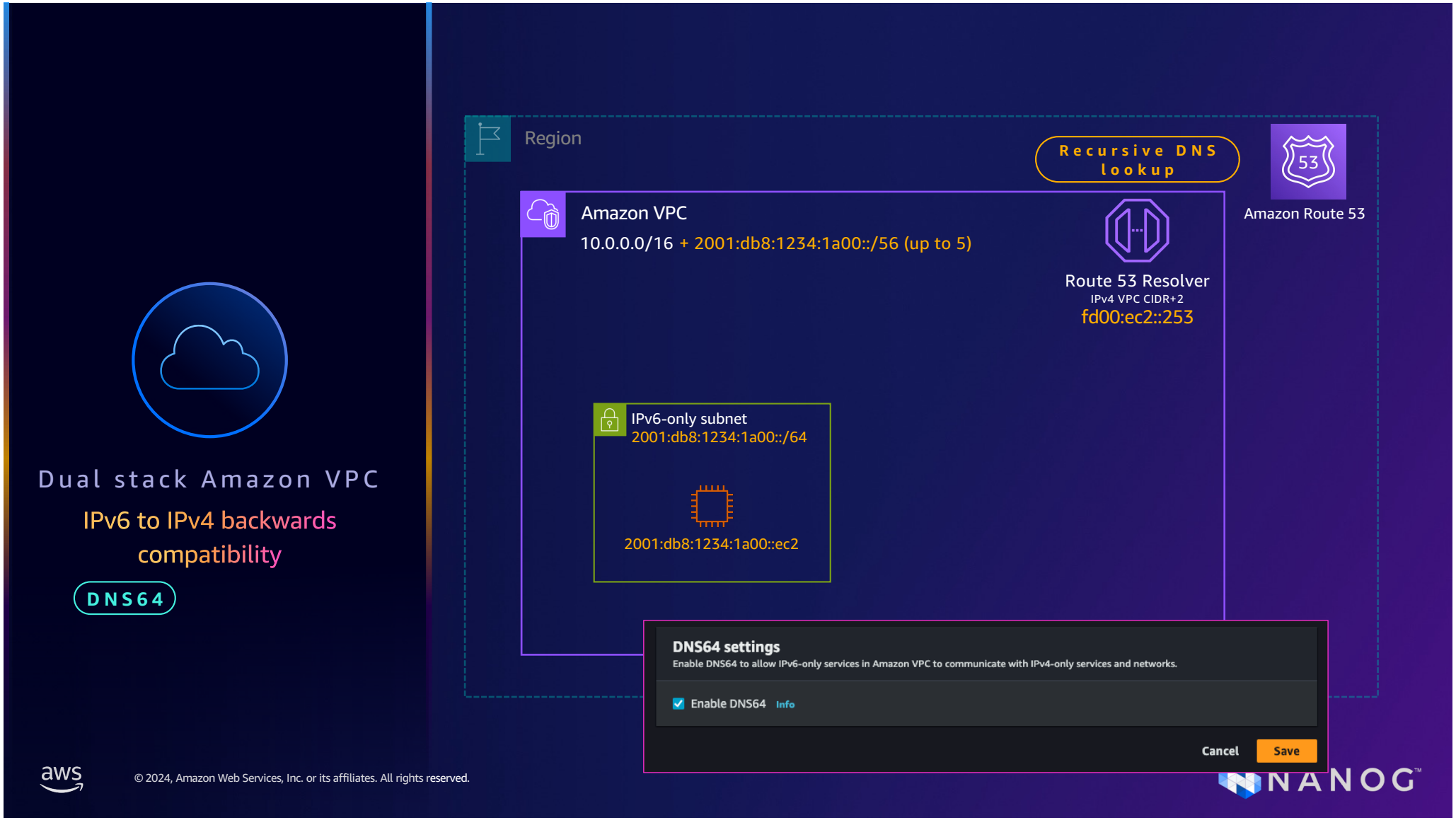



Build backwards compatibility
AWS DNS64 and NAT64
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
NANOG

Dual stack Amazon VPC

IPv6 to IPv4 backwards compatibility

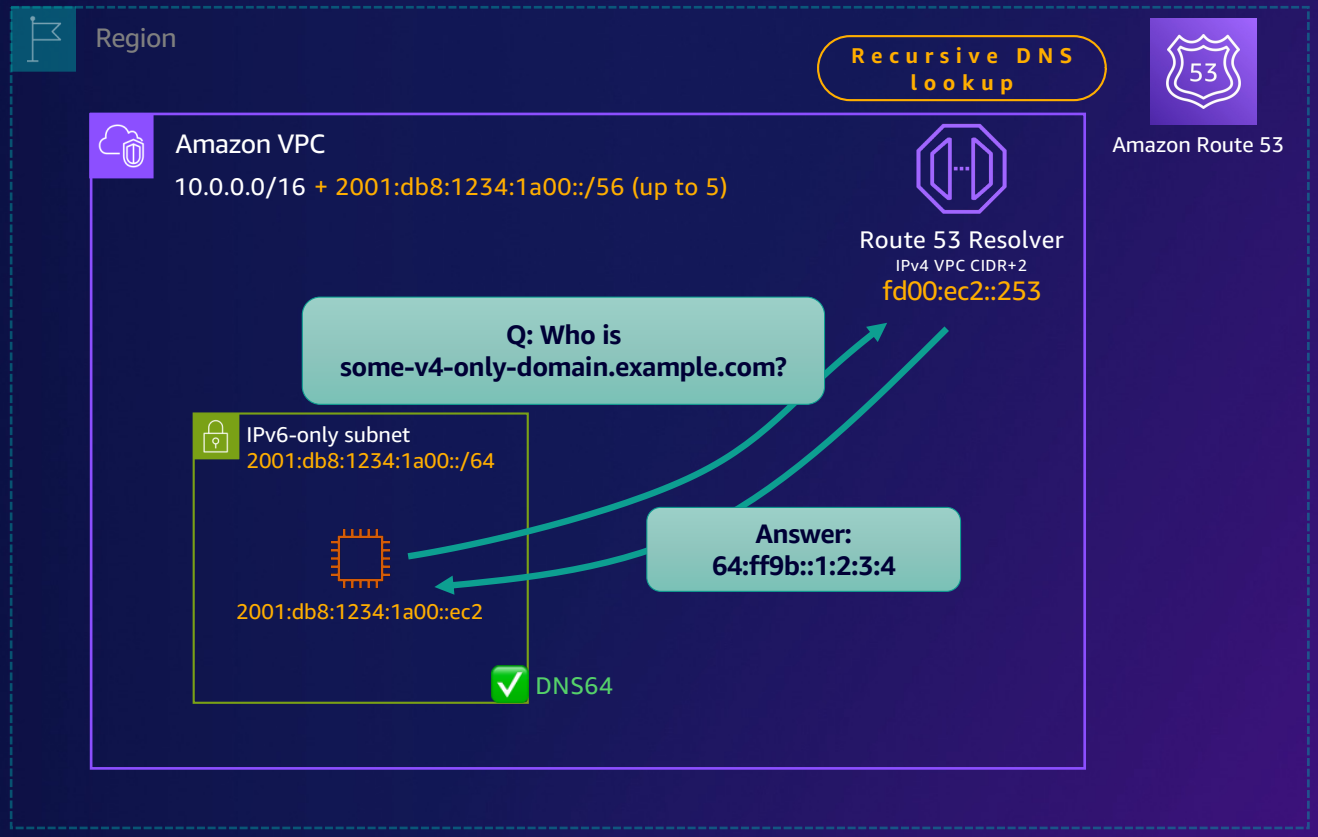




Dual stack Amazon VPC

IPv6 to IPv4 backwards compatibility

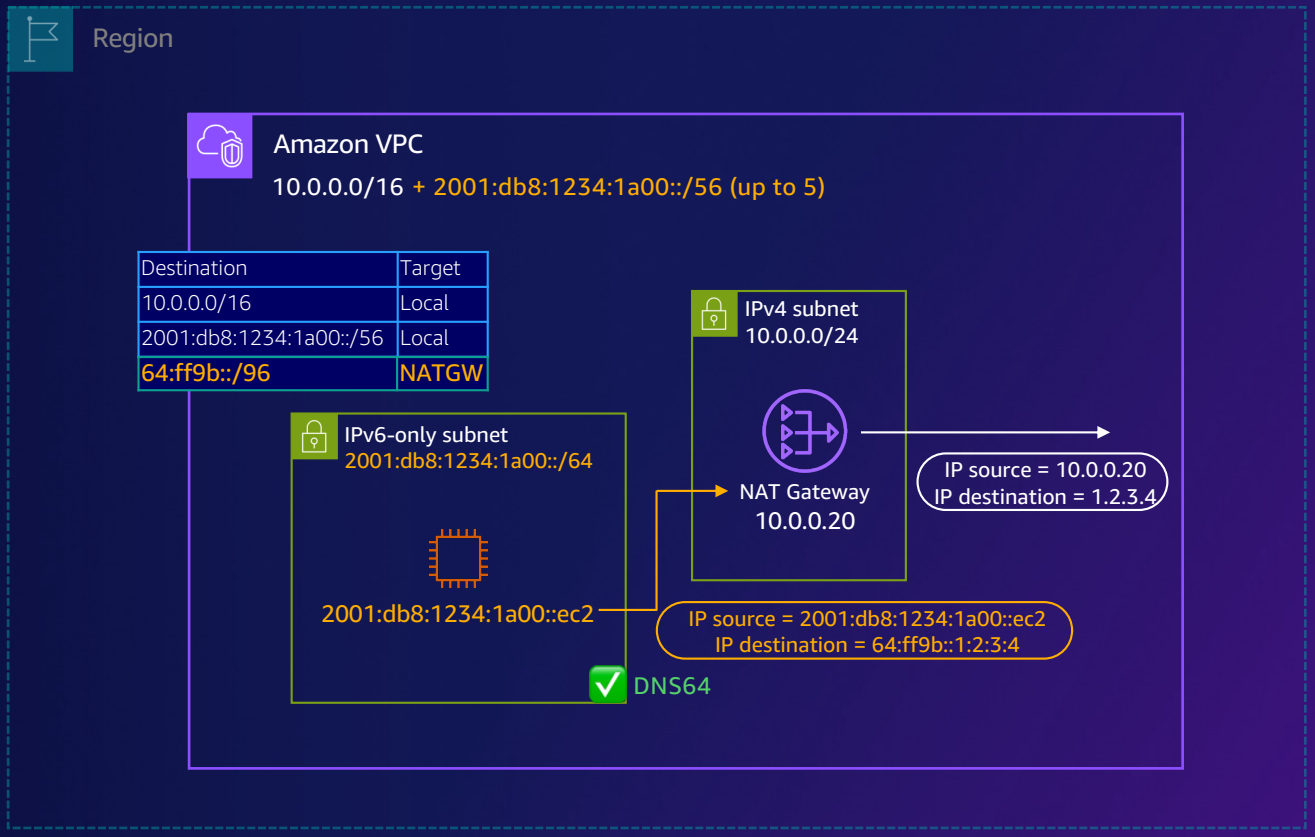
DNS64



Dual stack Amazon VPC

IPv6 to IPv4 backwards compatibility

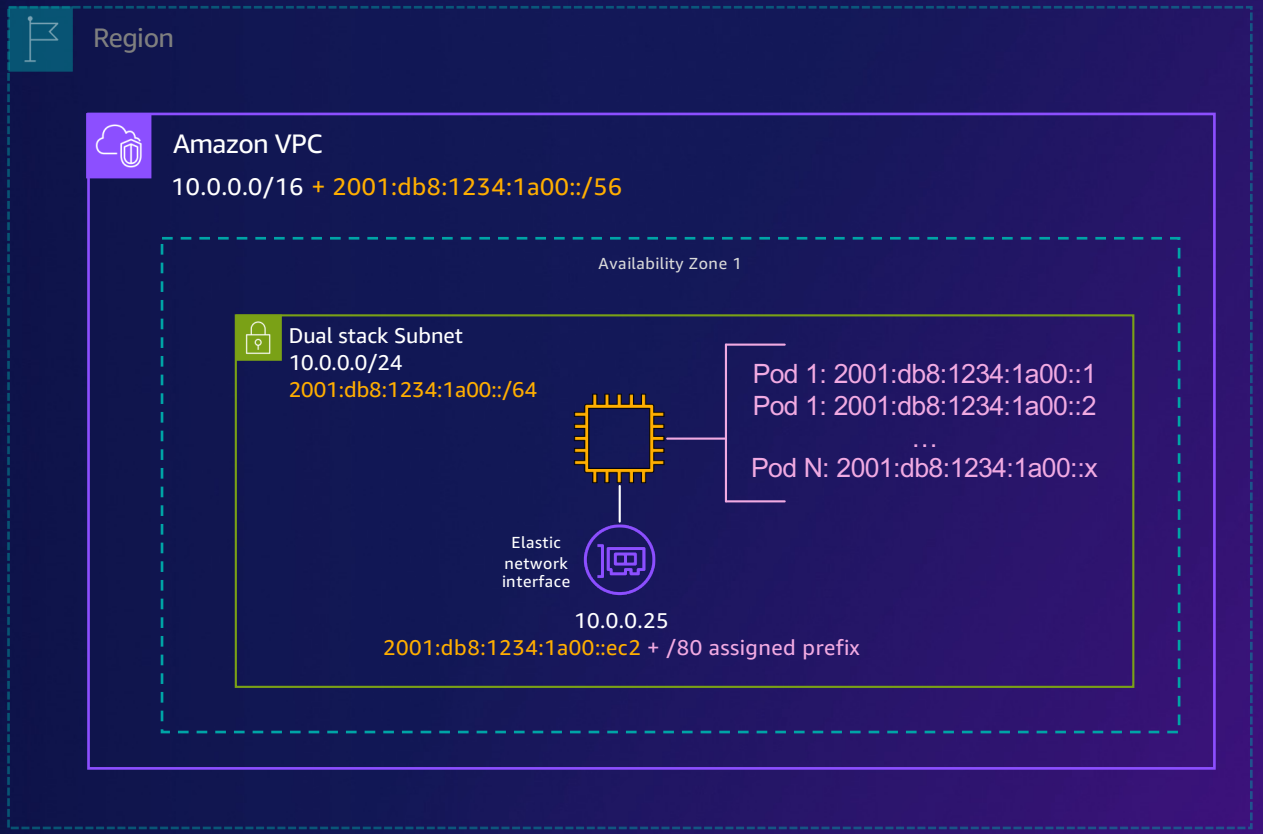
DNS64 + NAT64

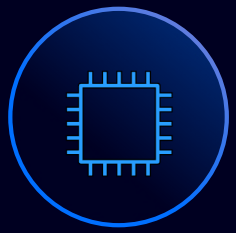



Simplify inside-out IPv6 adoption
Amazon Elastic Kubernetes Service
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
NANOG

IPv6 support for Amazon Compute Services

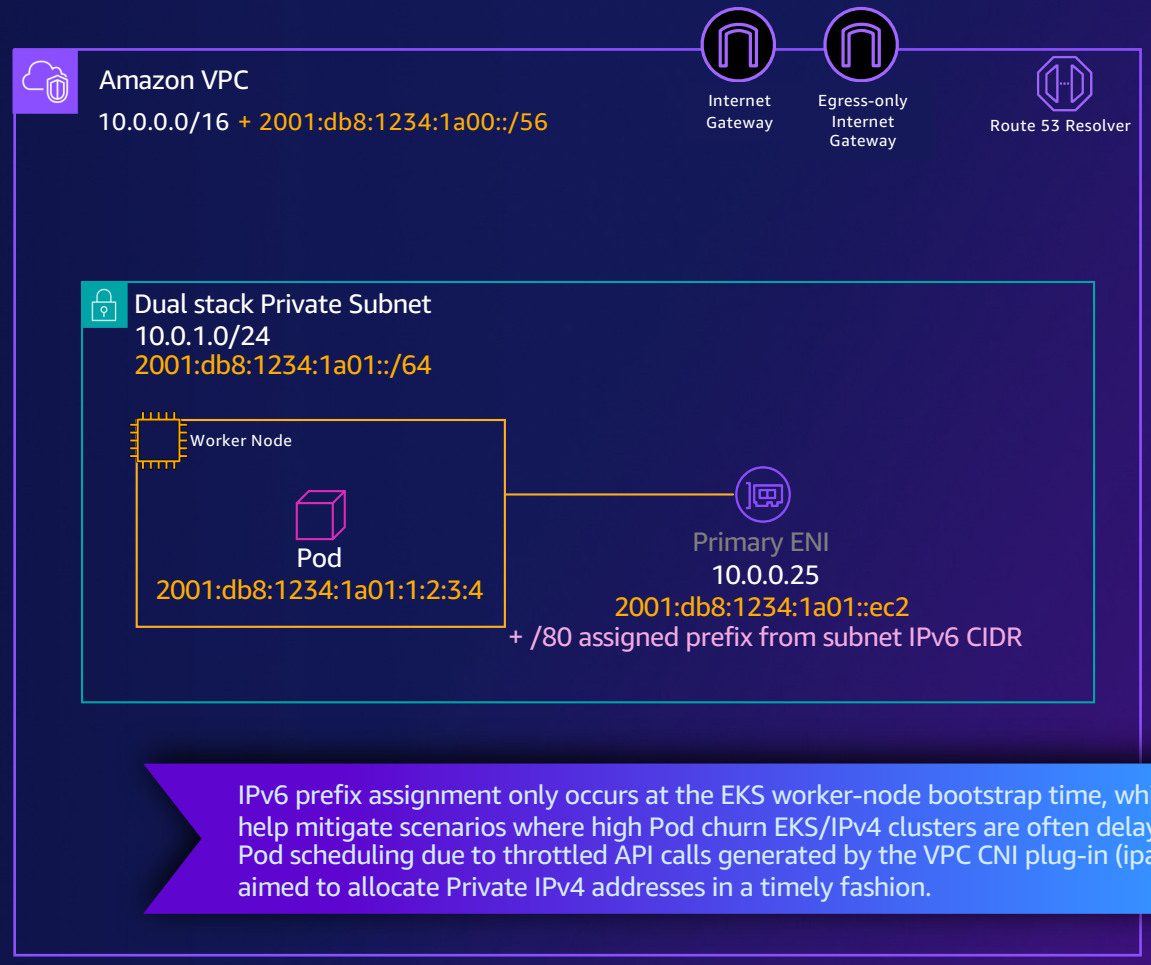
Amazon EKS



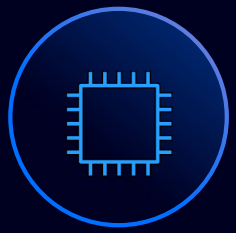


IPv6 support for Amazon EKS

POD ANATOMY

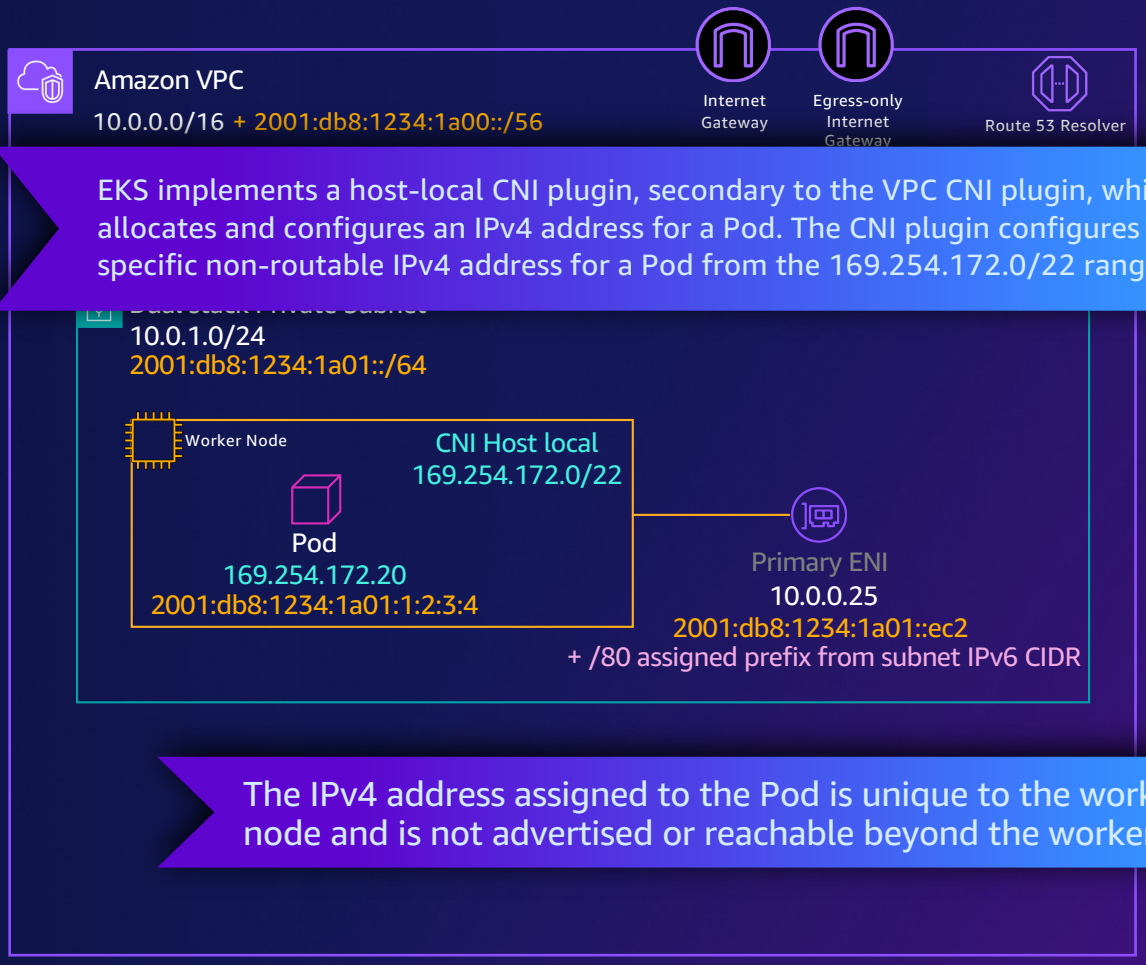


IPv6 prefix assignment only occurs at the EKS worker-node bootstrap time, which can help mitigate scenarios where high Pod churn EKS/IPv4 clusters are often delayed in Pod scheduling due to throttled API calls generated by the VPC CNI plug-in (ipamd) aimed to allocate Private IPv4 addresses in a timely fashion.



IPv6 support for
Amazon EKS

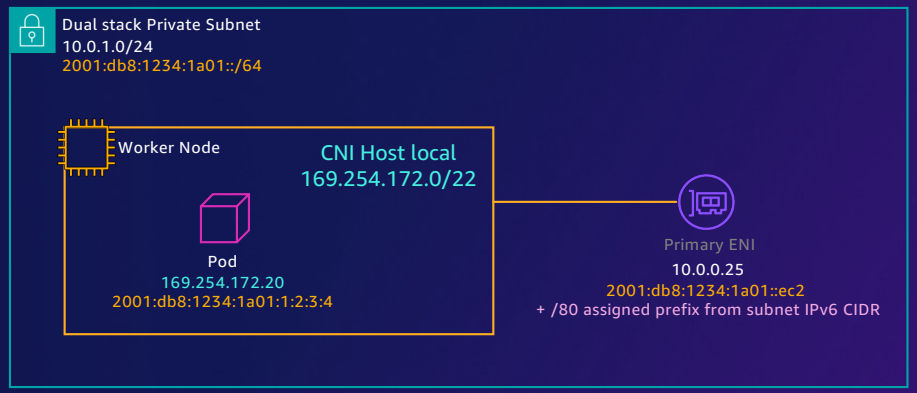
HOST LOCAL IPv4

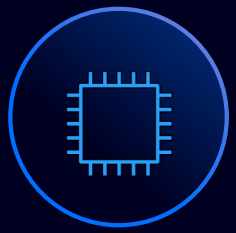


ENABLE_V4_EGRESS (v1.15.1+)
Type: Boolean as a String
Default: true
Specifies whether PODs in an IPv6 cluster support IPv4 egress. If env is set to true, range 169.254.172.0/22 is reserved for IPv4 egress. When enabled, traffic egressing an IPv6 pod destined to an IPv4 endpoint will be SNAT'ed via the node IPv4 address. Note that enabling/disabling this feature only affects whether newly created pods have an IPv4 interface created. Therefore, it is recommended that you reboot existing nodes after enabling/disabling this feature.

IPv6 support for
Amazon EKS

HOST LOCAL IPv4





IPv6 support for Amazon EKS

EKS CONTROL PLANE SERVICE CIDR

EKS Control Plane

Services / ClusterIP range
fd9e:89cb:a3d4::/108

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

Availability Zone 1

Auto-assigned by AWS, immutable, not globally reachable – Private Network scope

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Worker Node

CNI Host local
169.254.172.0/22

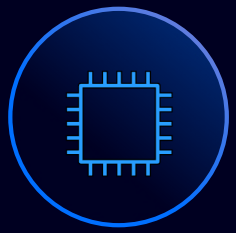
Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

Primary ENI
10.0.0.25
2001:db8:1234:1a01::ec2
+ /80 assigned prefix from subnet IPv6 CIDR

aws

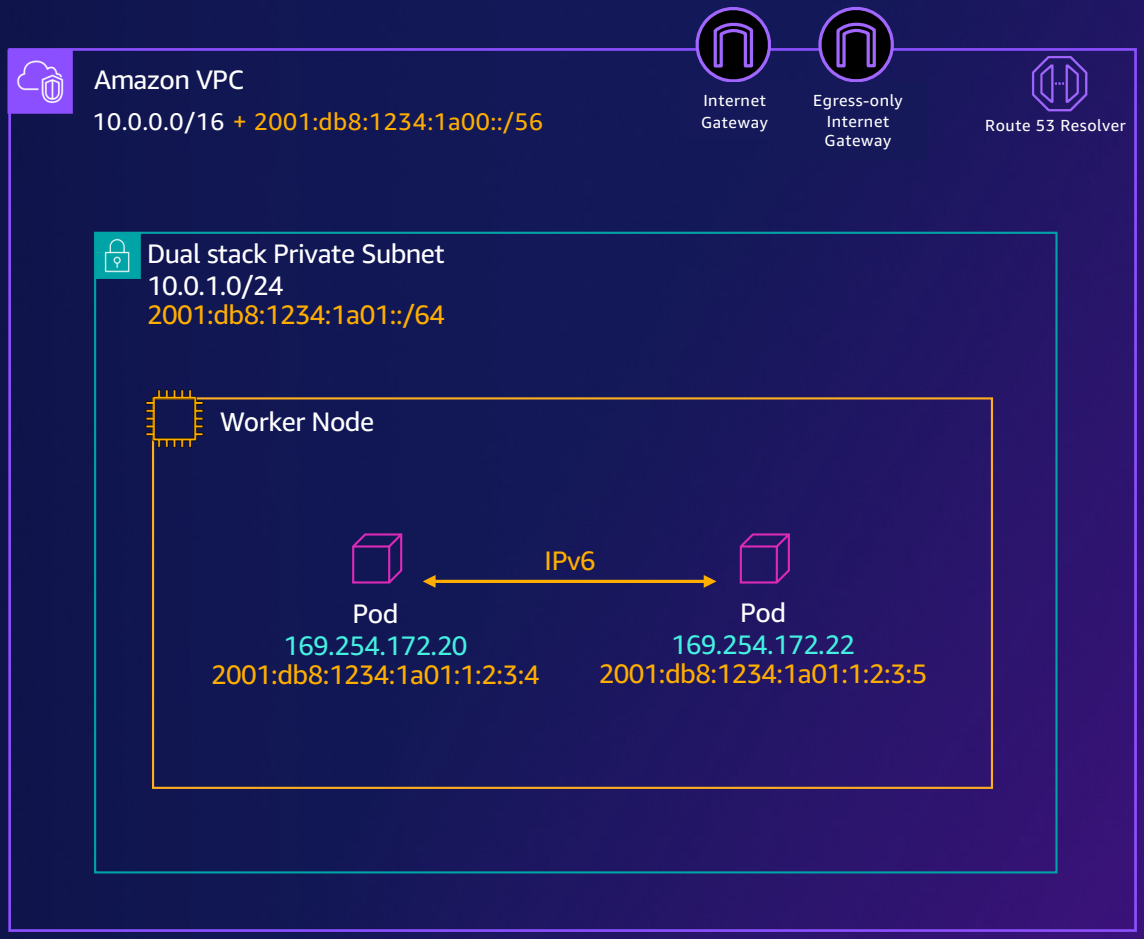
NANOG™

TRAFFIC FLOWS



IPv6 support for
Amazon EKS

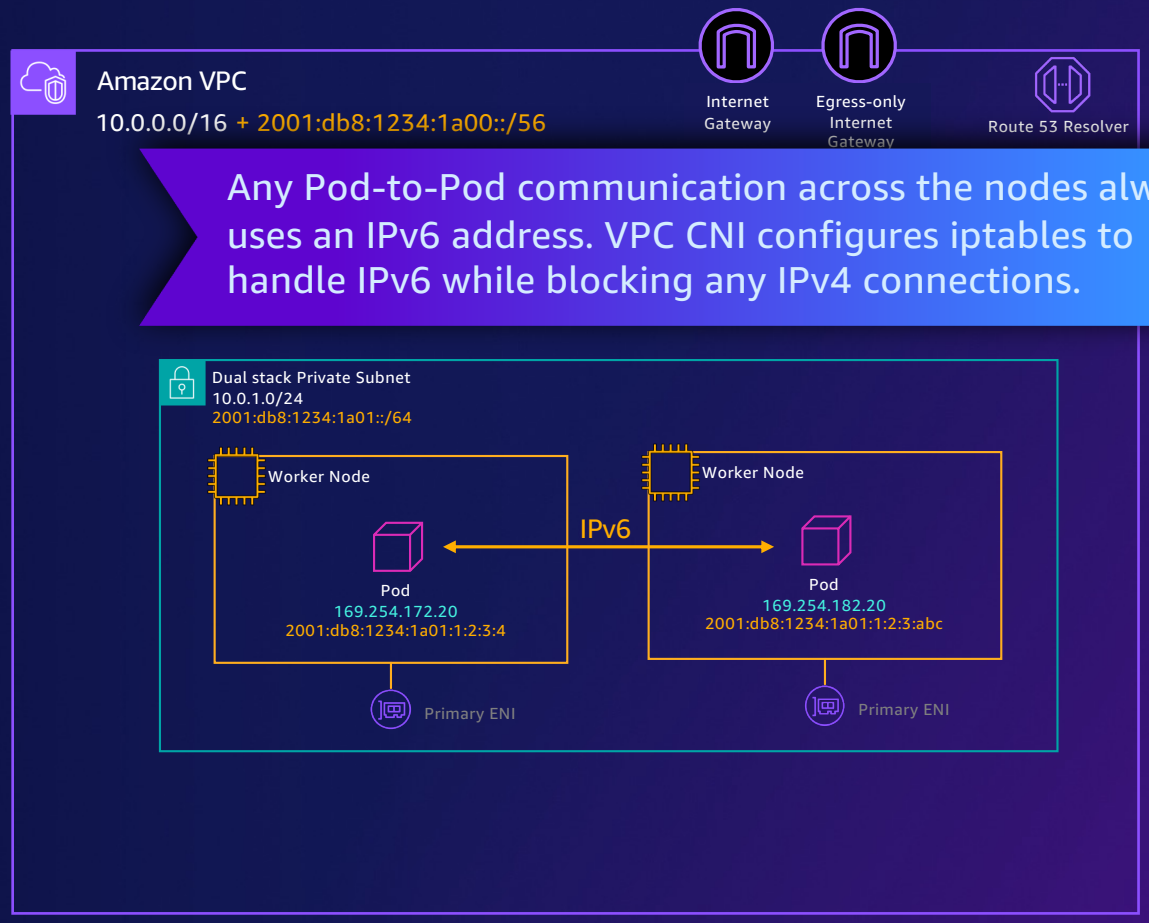
Pod to Pod on the same worker node



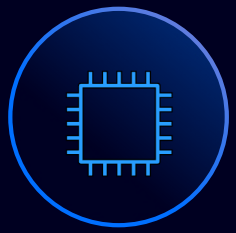
TRAFFIC FLOWS

IPv6 support for
Amazon EKS

Pod to Pod on the different worker nodes

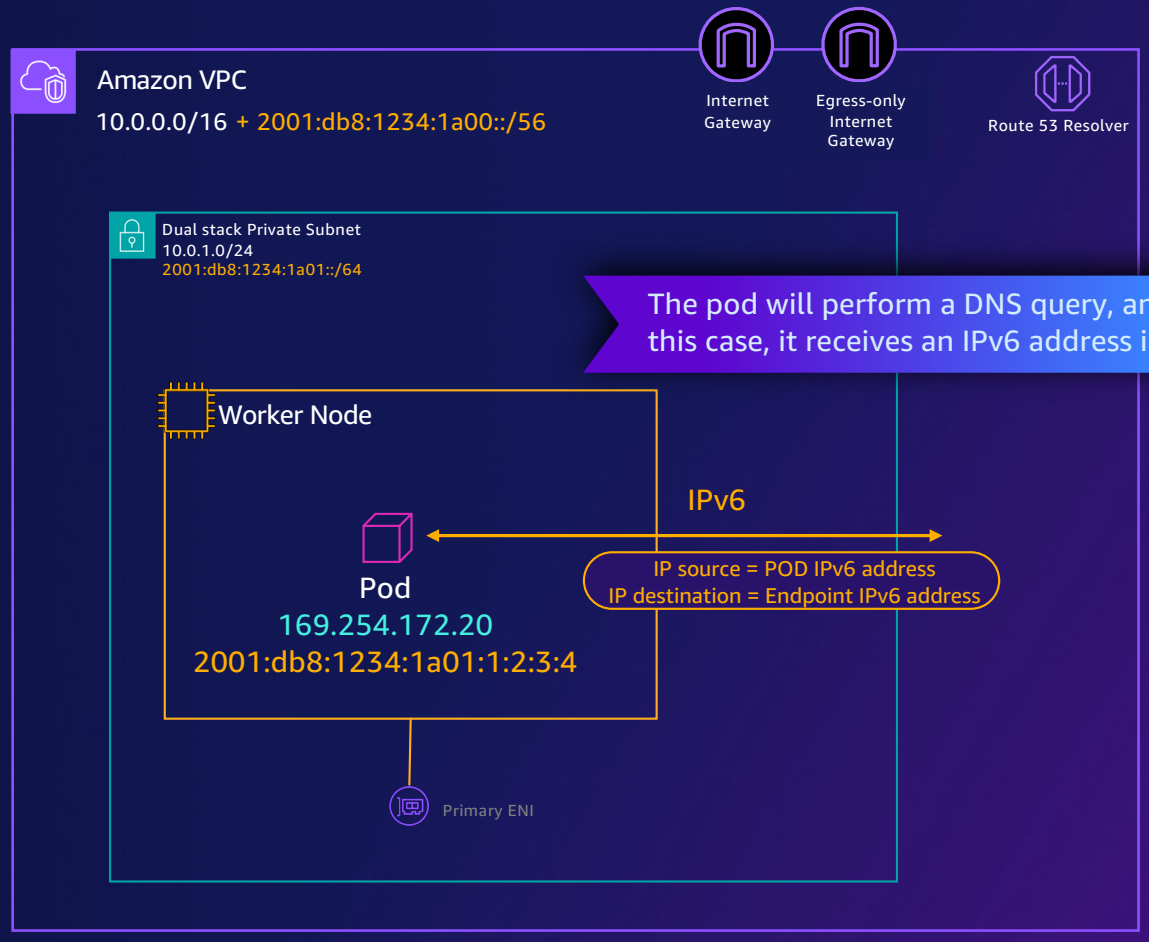


TRAFFIC FLOWS

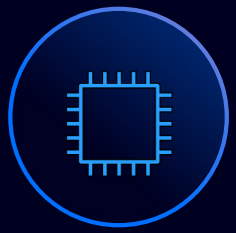


IPv6 support for
Amazon EKS

Pod to IPv6 endpoint outside of cluster

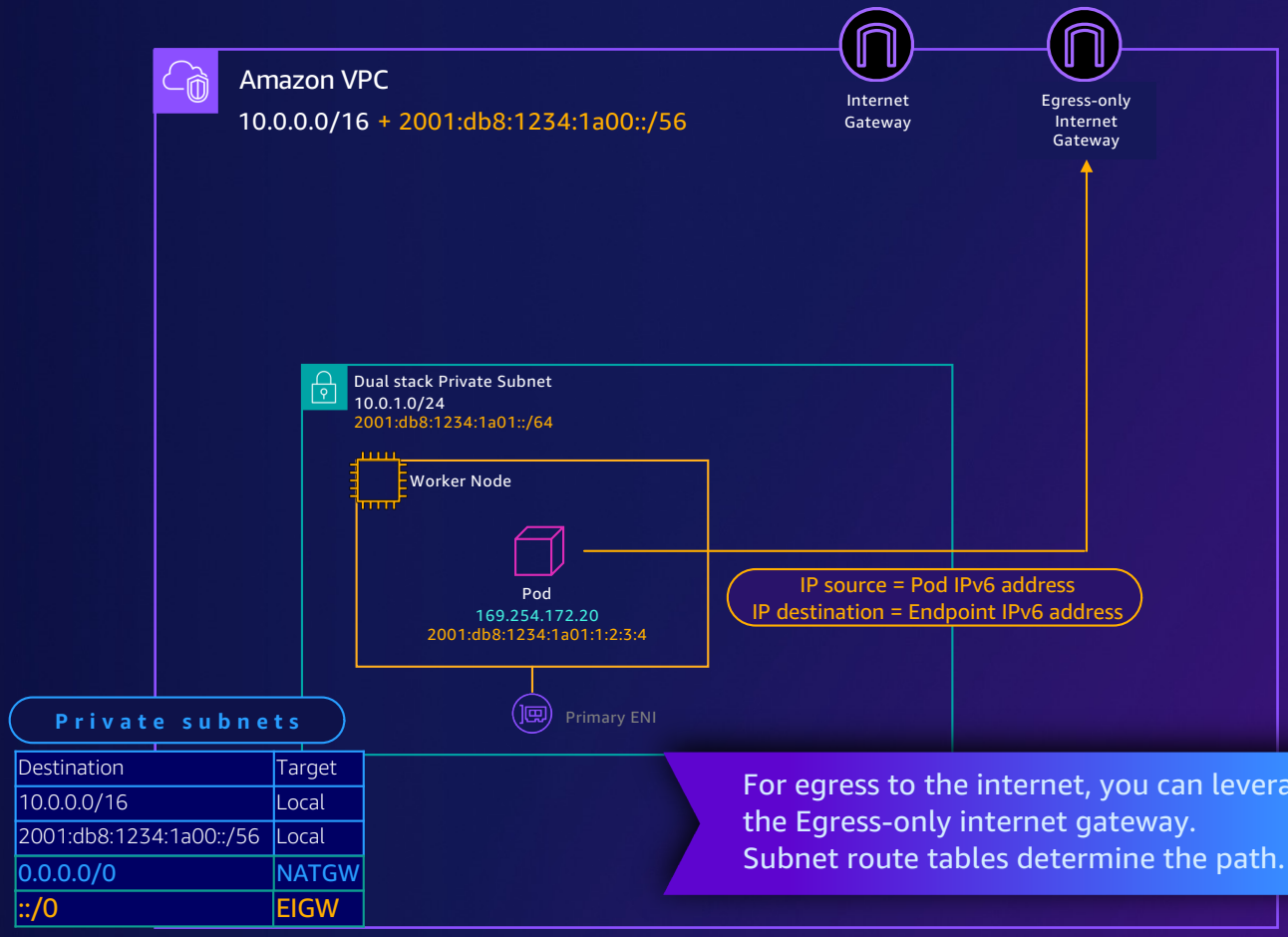


TRAFFIC FLOWS



IPv6 support for
Amazon EKS

Pod to an IPv6 endpoint on the internet



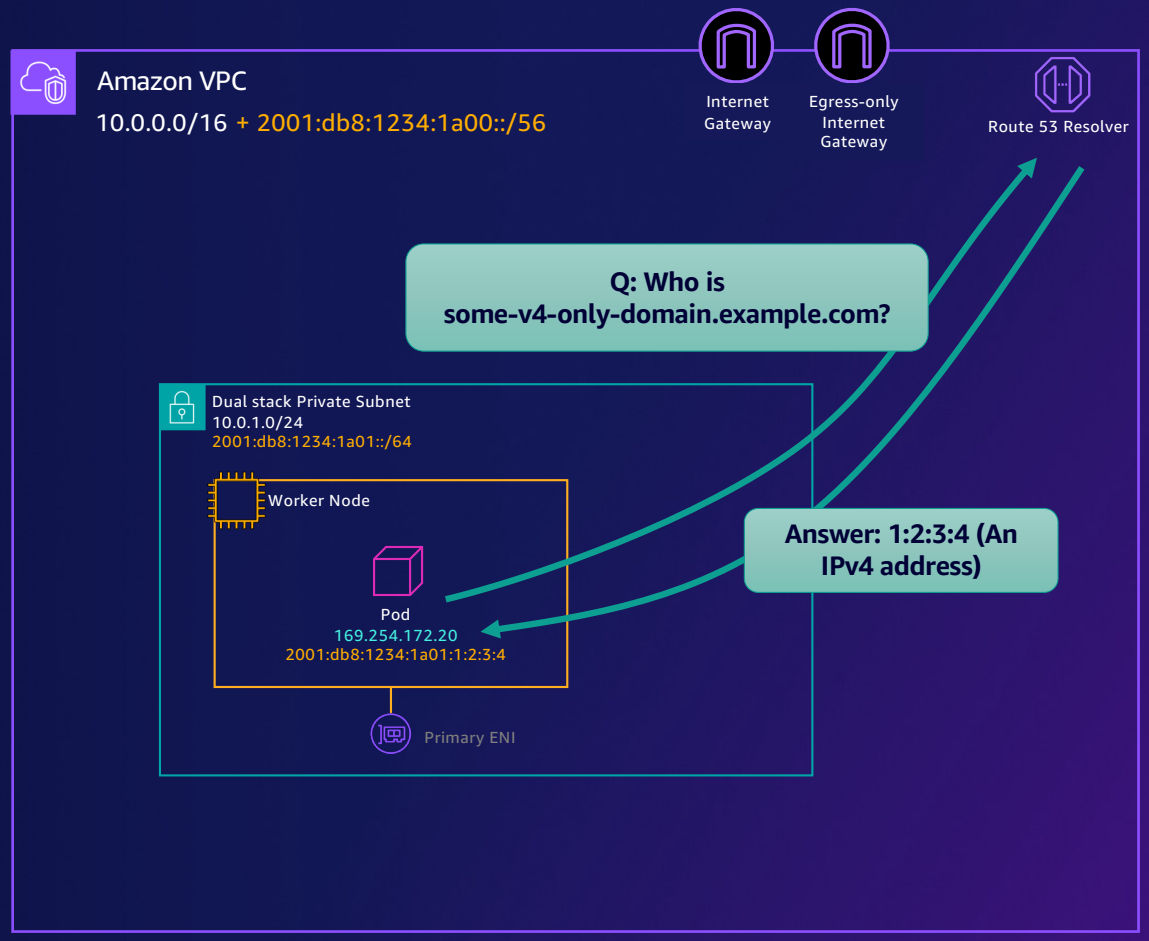
Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	NATGW
::/0	EIGW

For egress to the internet, you can leverage the Egress-only internet gateway.
Subnet route tables determine the path.

TRAFFIC FLOWS

IPv6 support for
Amazon EKS

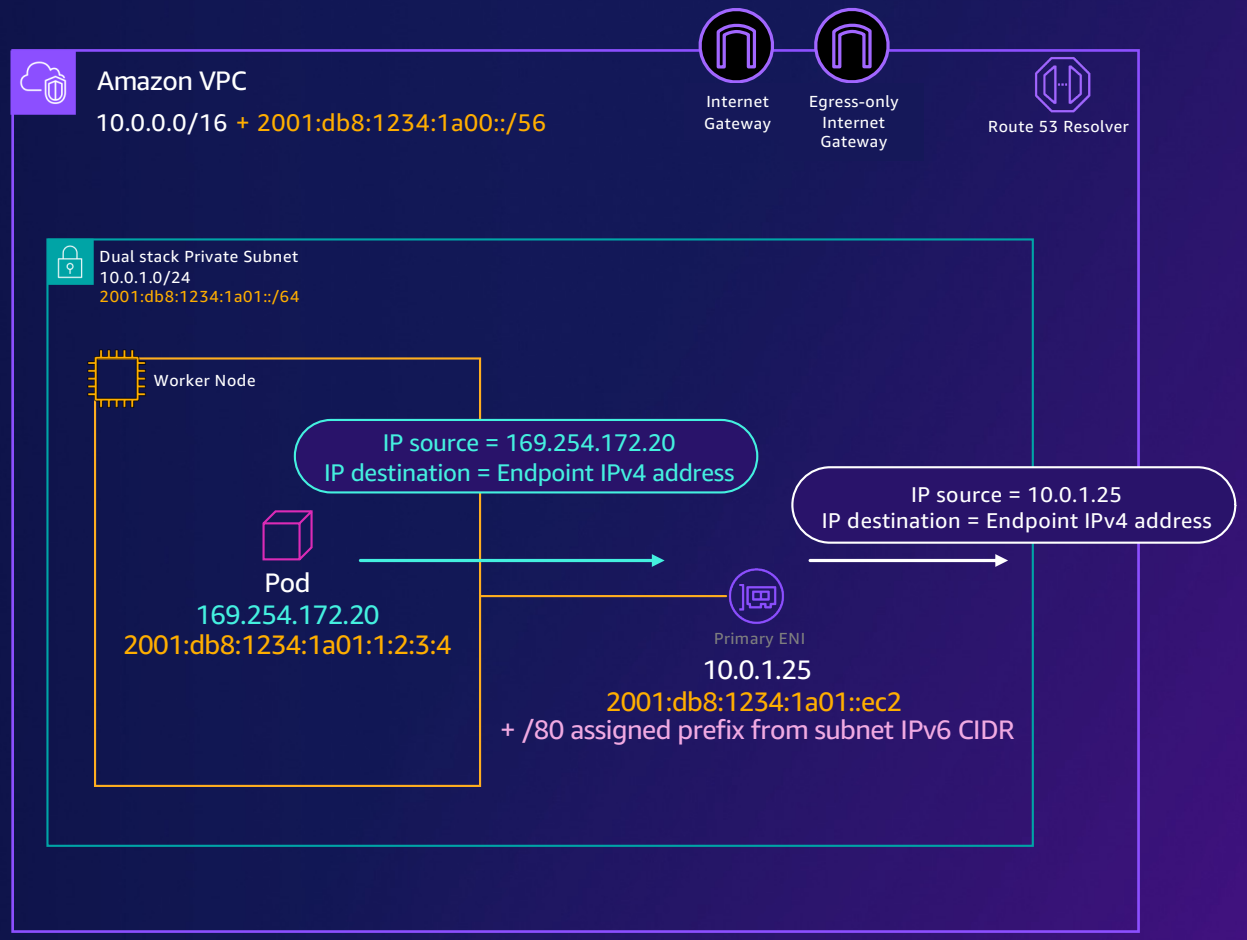
Pod to an IPv4 endpoint



TRAFFIC FLOWS

IPv6 support for
Amazon EKS

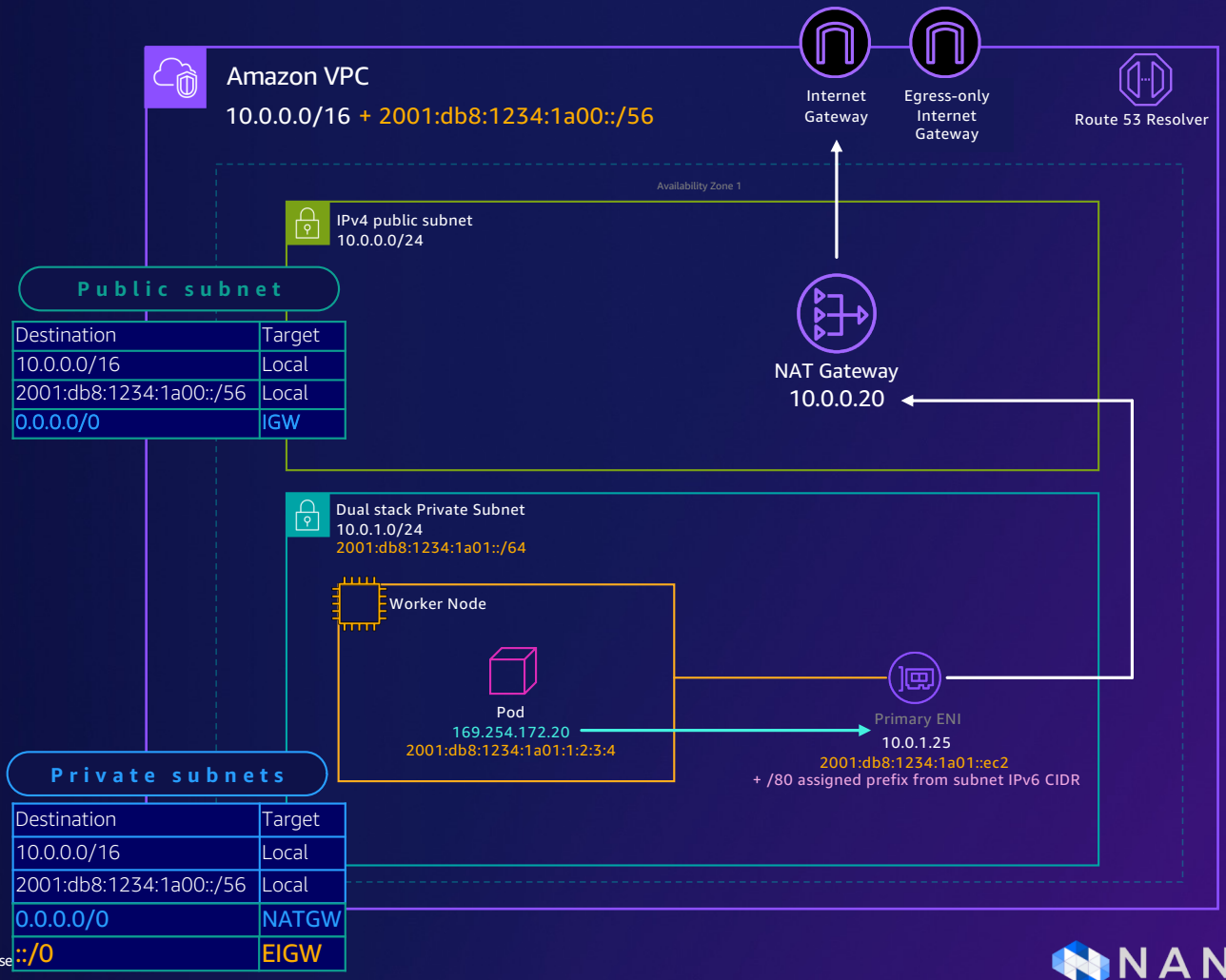
Pod to an IPv4 endpoint



TRAFFIC FLOWS

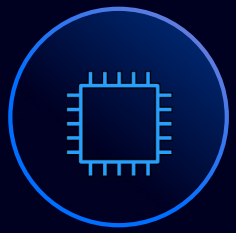
IPv6 support for
Amazon EKS

Pod to an IPv4 endpoint on the internet



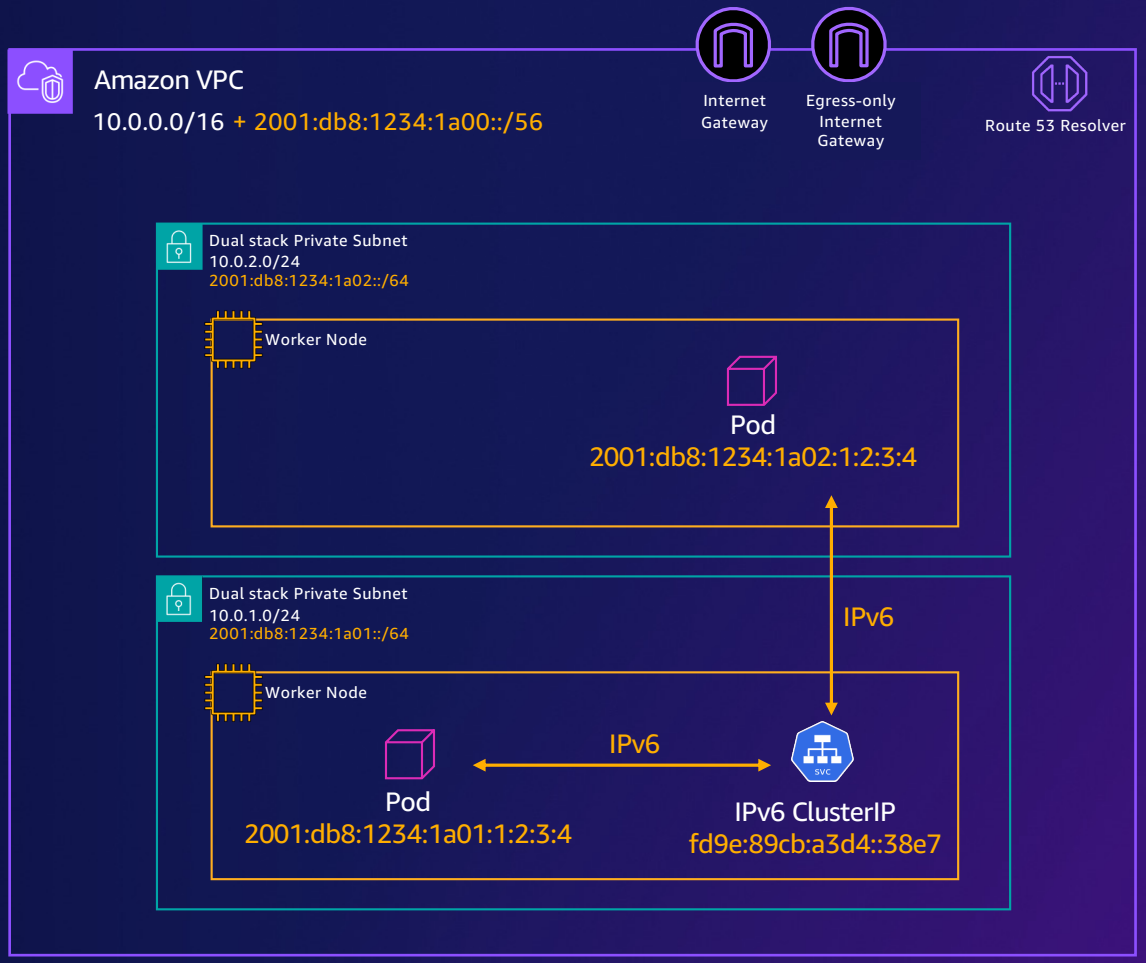
NANOG™

TRAFFIC FLOWS

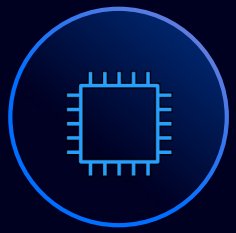


IPv6 support for
Amazon EKS

Pod to Kubernetes service (ClusterIP)



TRAFFIC FLOWS



IPv6 support for
Amazon EKS

Ingress using dual stack load balancers: Public

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

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

Internet Gateway

Egress-only Internet Gateway

Route 53 Resolver

Availability Zone 1

Dual stack Public Subnet
10.0.0.0/24
2001:db8:1234:1a00::/64

AAAA record: IPv6 addresses
A record: Elastic IPv4 addresses

Dual stack Application Load Balancer

Public subnets

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	IGW
::/0	IGW

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

IPv6

Worker Node

Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

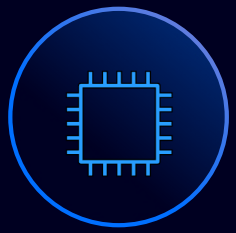
Private subnets

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	NATGW
::/0	EIGW

aws

NANOG™

TRAFFIC FLOWS



IPv6 support for
Amazon EKS

Ingress using dual stack load balancers: Public

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

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

Internet Gateway

Egress-only Internet Gateway

Route 53 Resolver

Availability Zone 1

Dual stack Public Subnet
10.0.0.0/24
2001:db8:1234:1a00::/64

AAAA record: IPv6 addresses
A record: Elastic IPv4 addresses

Dual stack Network Load Balancer

Public subnets

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	IGW
::/0	IGW

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

IPv6

Worker Node

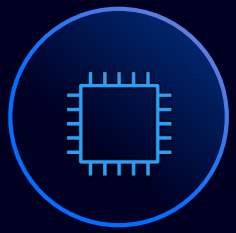
Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

Private subnets

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	NATGW
::/0	EIGW

NANOG™

TRAFFIC FLOWS



IPv6 support for
Amazon EKS

Ingress using dual stack load balancers: Private

ipv6.deny_all_igw_traffic
blocks internet gateway (IGW) access to the load balancer, preventing unintended access to your internal load balancer through an internet gateway. It is set to true for internal load balancers.

Availability Zone 1

Dual stack Public Subnet
10.0.0.0/24
2001:db8:1234:1a00::/64

AAAA record: IPv6 addresses
A record: Private IPv4 addresses

Dual stack Application / Network Load Balancer

Public subnets

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	IGW
::/0	IGW

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

IPv6

Worker Node

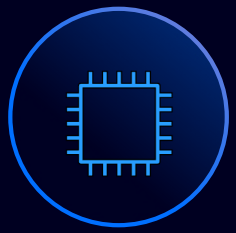
Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

Private subnets

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	NATGW
::/0	EIGW

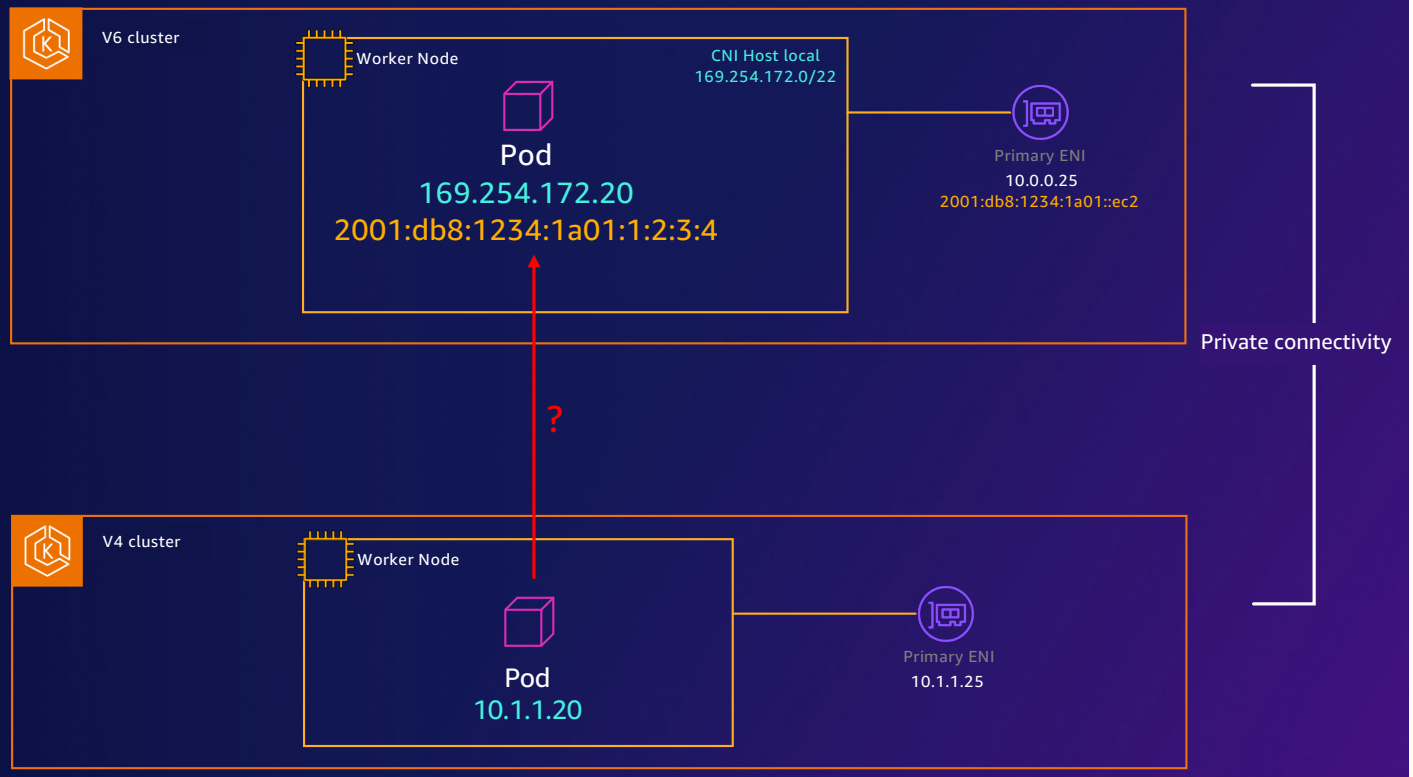
NANOG™

TRAFFIC FLOWS



IPv6 support for
Amazon EKS

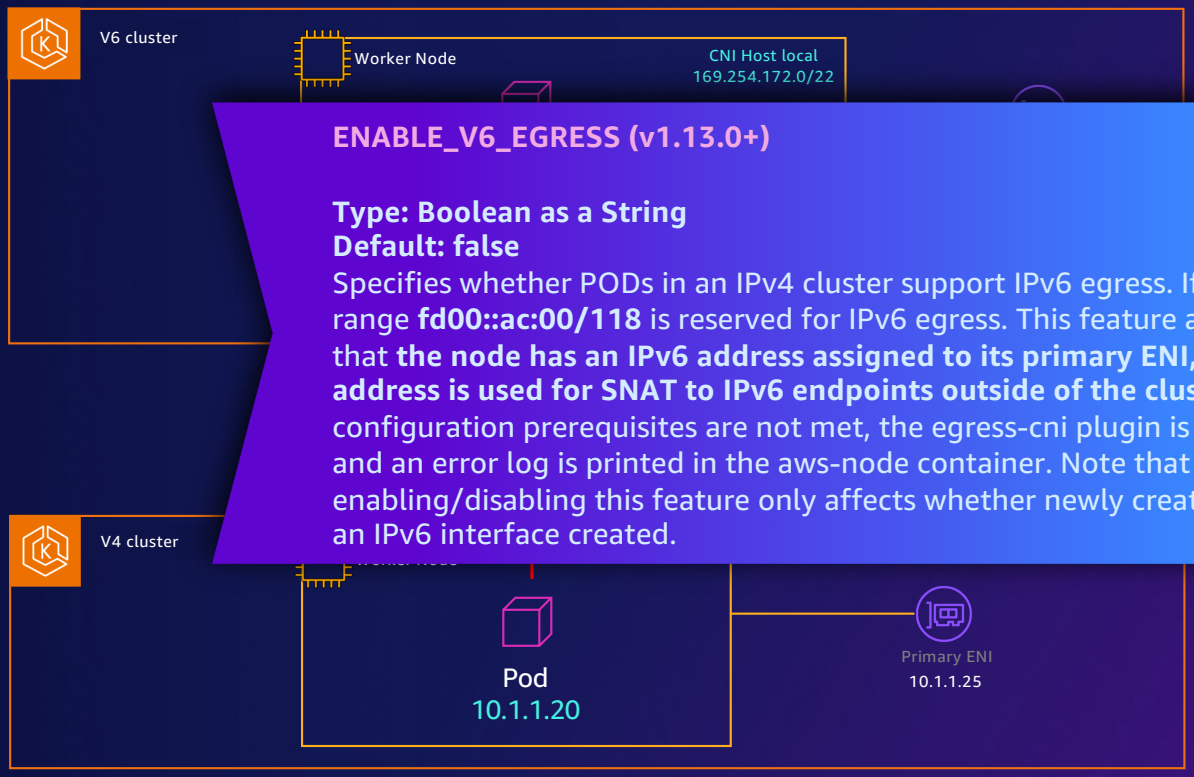
How about Pod v4 to Pod v6?



TRAFFIC FLOWS

IPv6 support for
Amazon EKS

How about Pod v4 to Pod v6?



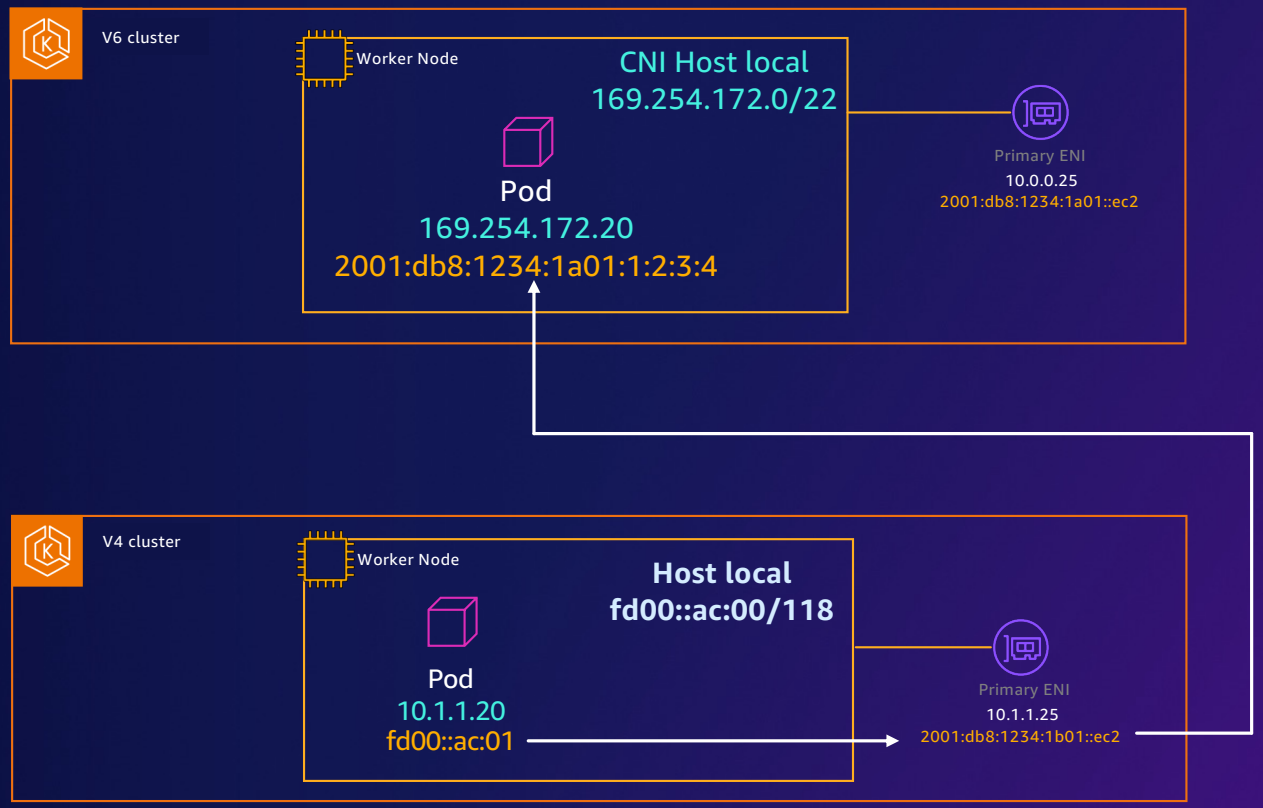
ENABLE_V6_EGRESS (v1.13.0+)

Type: Boolean as a String
Default: false
Specifies whether PODs in an IPv4 cluster support IPv6 egress. If set to true, range **fd00::ac:00/118** is reserved for IPv6 egress. This feature also requires that **the node has an IPv6 address assigned to its primary ENI, as this address is used for SNAT to IPv6 endpoints outside of the cluster**. If the configuration prerequisites are not met, the egress-cni plugin is not enabled and an error log is printed in the aws-node container. Note that enabling/disabling this feature only affects whether newly created pods have an IPv6 interface created.

TRAFFIC FLOWS

IPv6 support for
Amazon EKS

Native v6 egress
for v4 EKS clusters




Build
IPv6 network connectivity

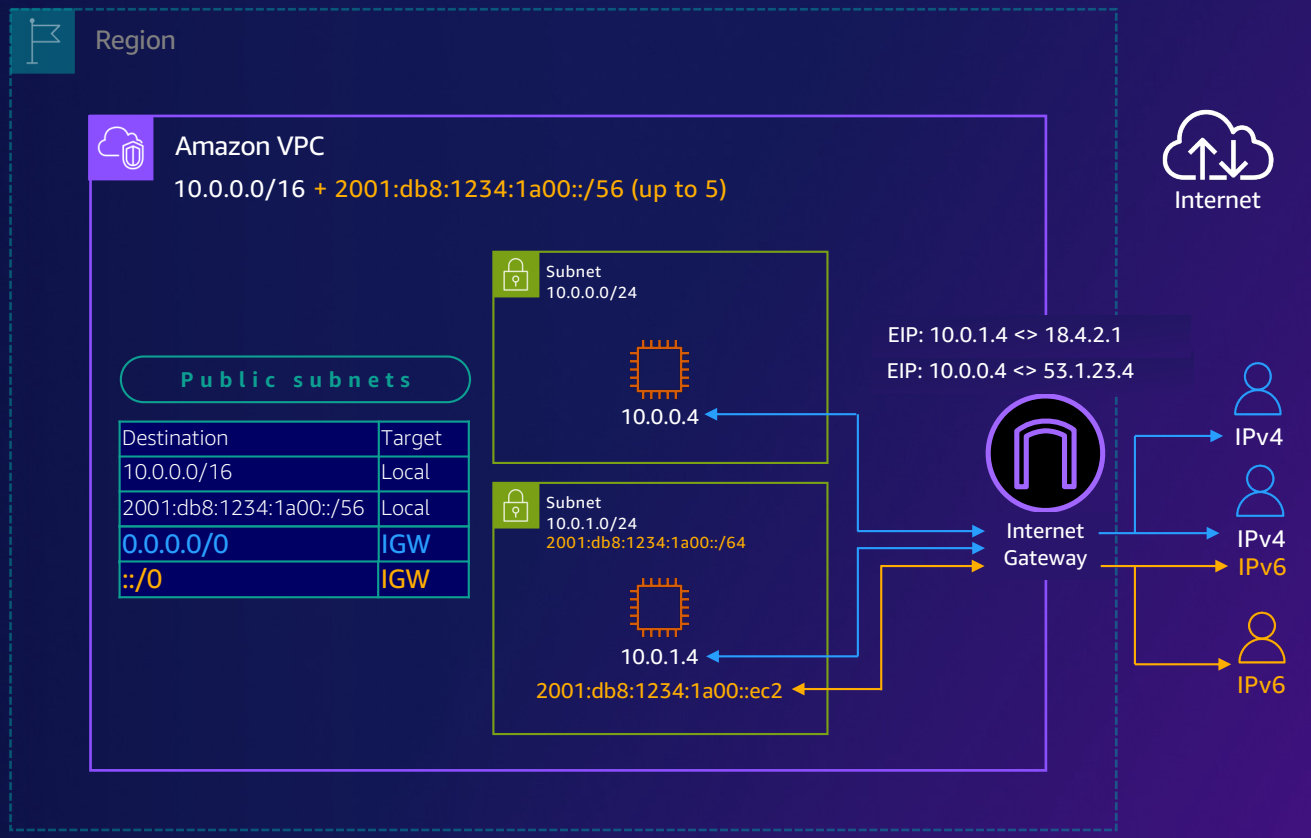
Internet connectivity

IPv6 network connectivity

VPC

Internet connectivity

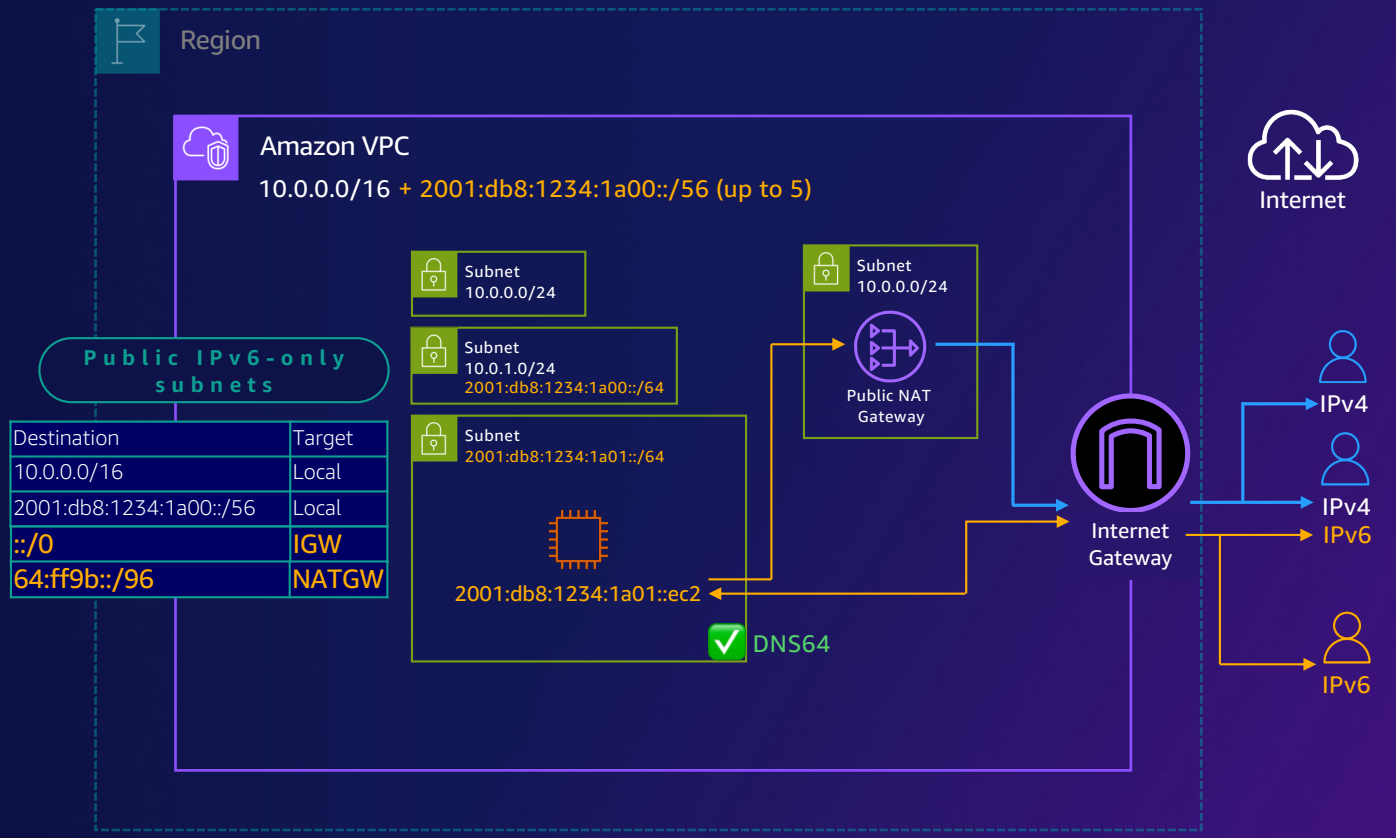
Public subnets

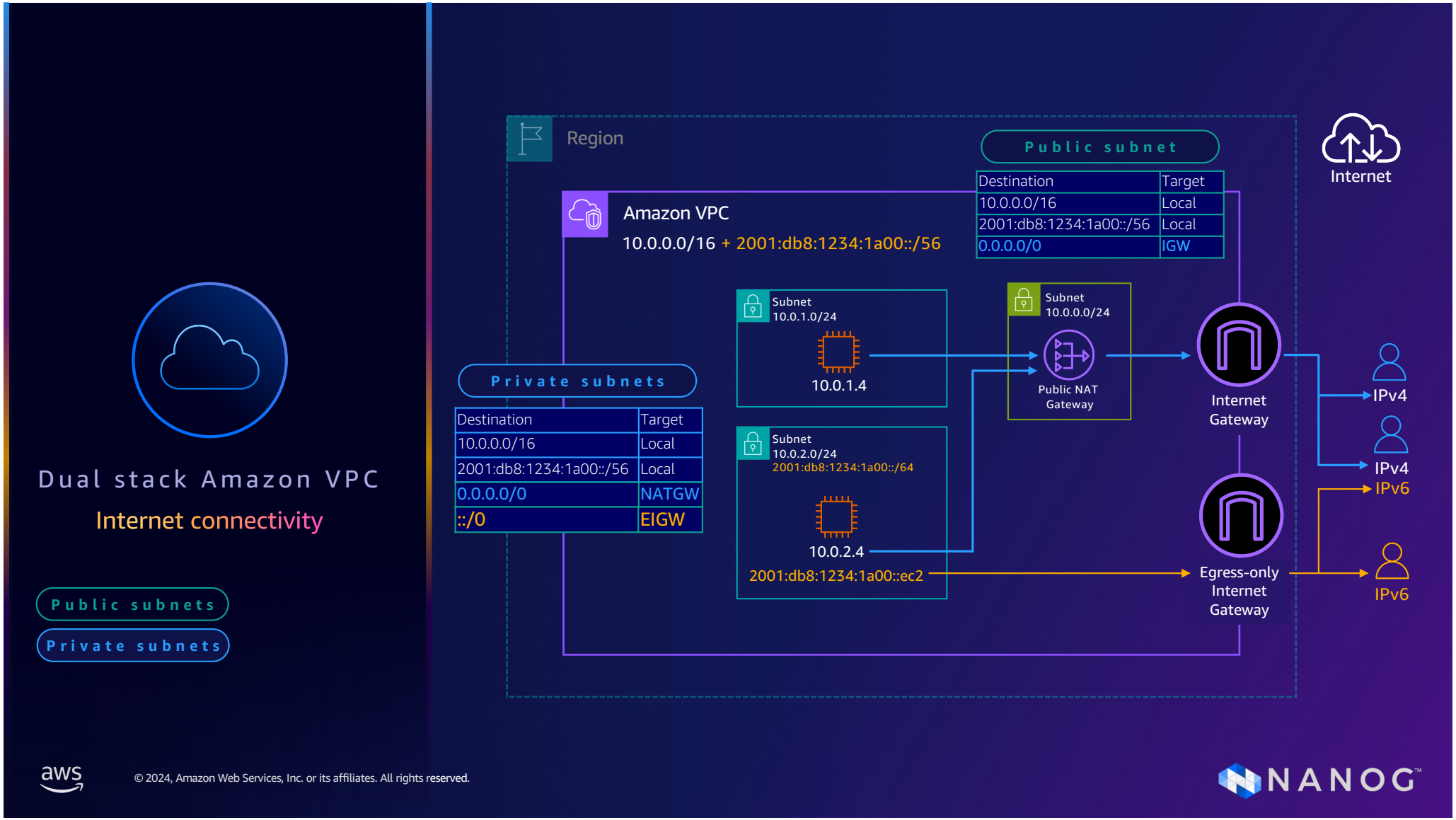


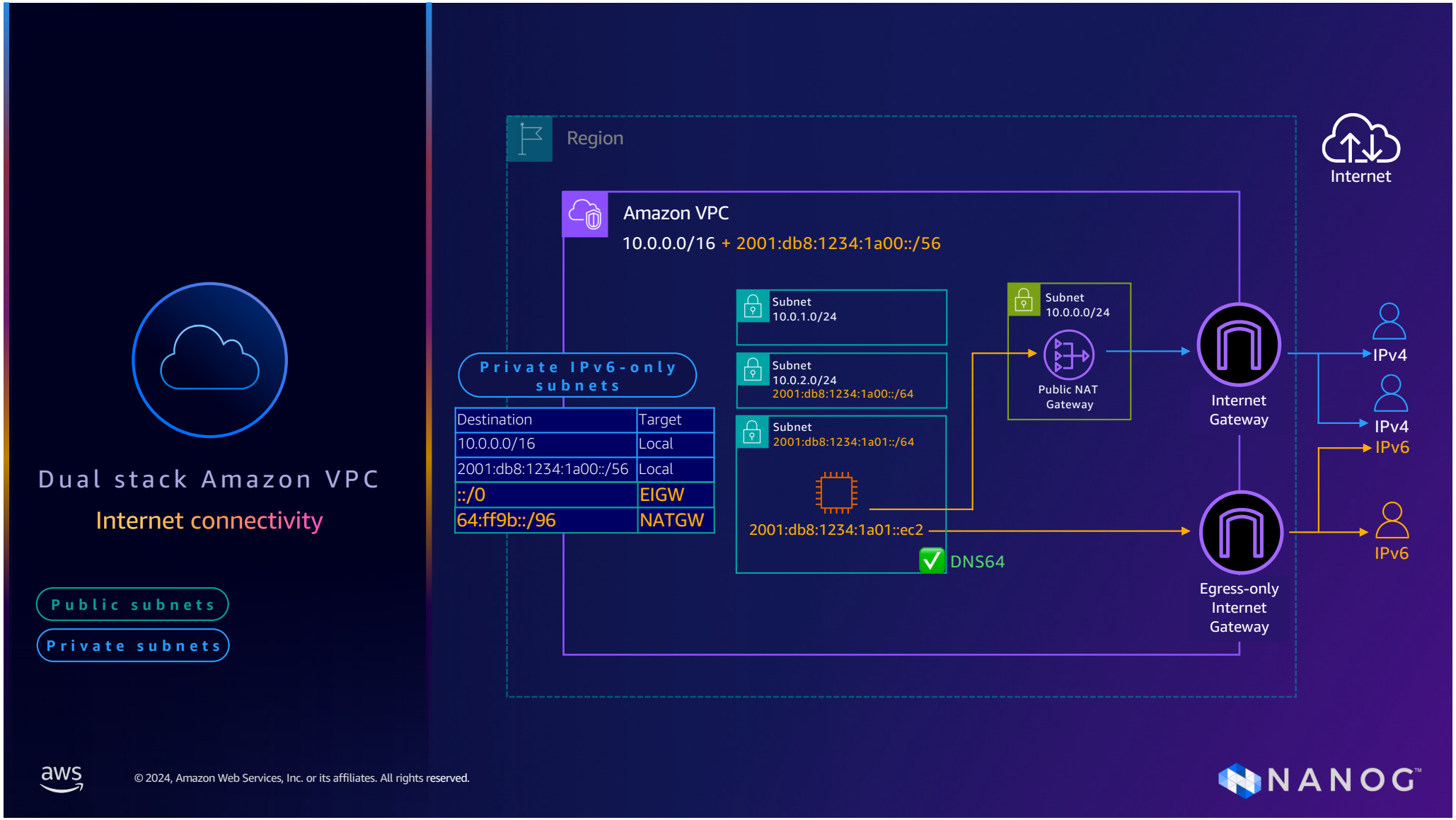
Dual stack Amazon VPC

Internet connectivity

Public subnets







IPv6 network connectivity

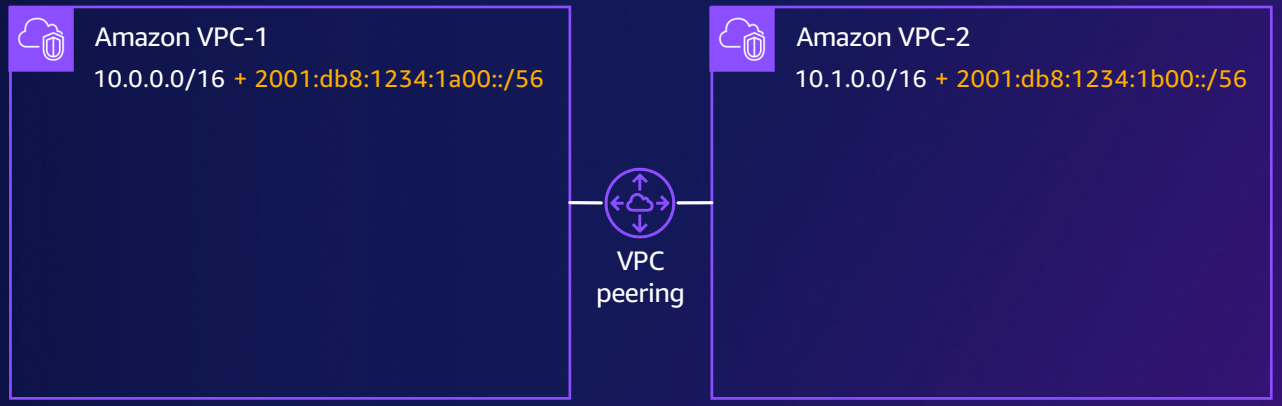
Internet connectivity

VPC to VPC connectivity

Dual stack Amazon VPC

VPC to VPC connectivity

VPC Peering



VPC-1 Route Table(s)

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
10.1.0.0/16	PCX-ID
2001:db8:1234:1b00::/56	PCX-ID

VPC-2 Route Table(s)

Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1b00::/56	Local
10.0.0.0/16	PCX-ID
2001:db8:1234:1a00::/56	PCX-ID

aws

NANOG™

Dual stack Amazon VPC

VPC to VPC connectivity

VPC Peering

AWS Transit Gateway

Region

VPC-1 Route Table(s)

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
::/0	IGW/EIGW
RFC1918	TGW
IPv6 summary route	TGW

VPC-2 Route Table(s)

Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1b00::/56	Local
::/0	IGW/EIGW
RFC1918	TGW
IPv6 summary route	TGW

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

Amazon VPC-2
10.1.0.0/16 + 2001:db8:1234:1b00::/56

Internet Gateway

Egress-only Internet Gateway

DUAL STACK ATTACHMENT SUBNET

TGW ENI

Internet Gateway

Egress-only Internet Gateway

DUAL STACK ATTACHMENT SUBNET

TGW ENI

AWS Transit Gateway

TGW Route Table(s)

Destination	Target
10.0.0.0/16	VPC-1 attachment
2001:db8:1234:1a00::/56	VPC-1 attachment
10.1.0.0/16	VPC-2 attachment
2001:db8:1234:1b00::/56	VPC-2 attachment

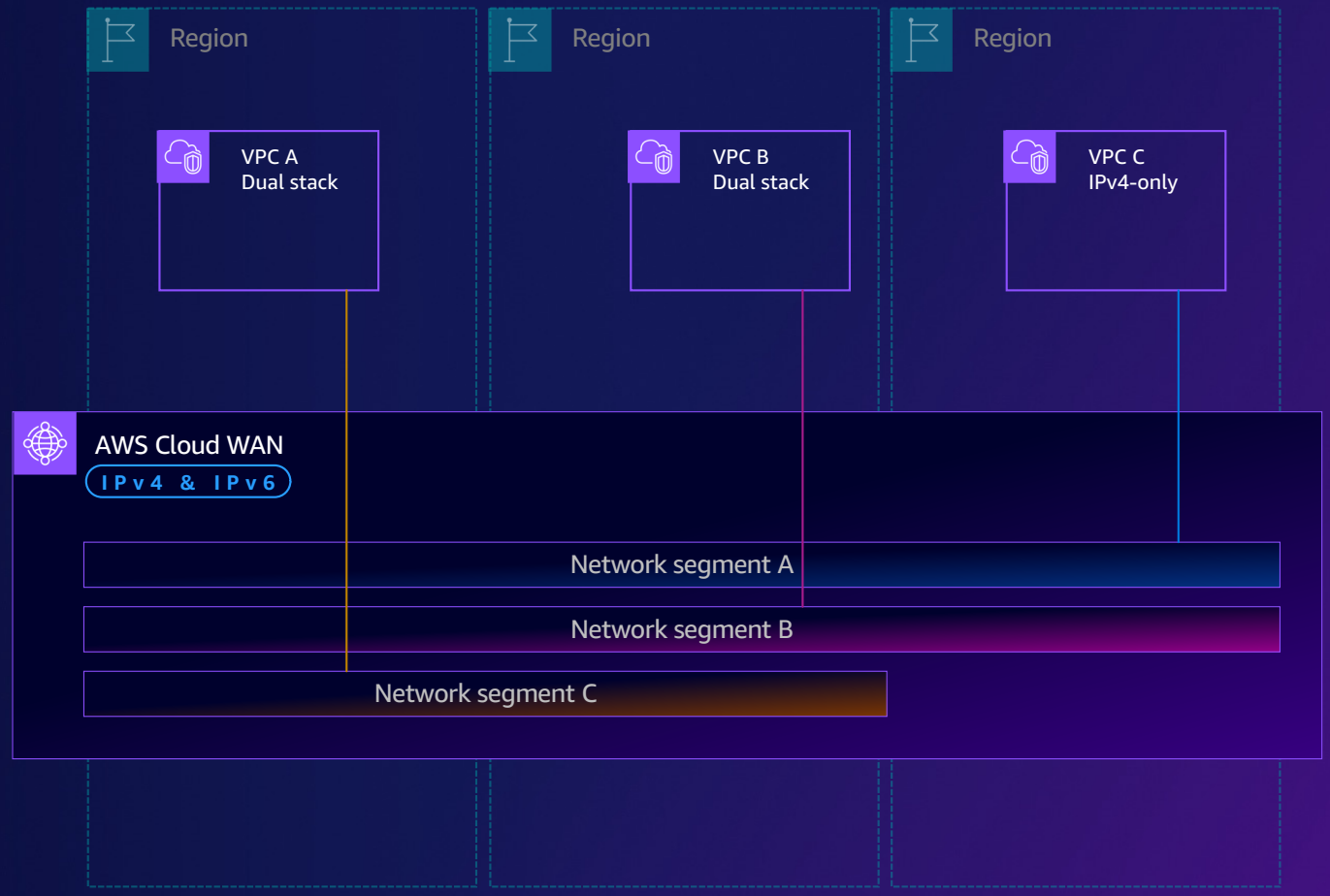
aws

NANOG™

Dual stack Amazon VPC

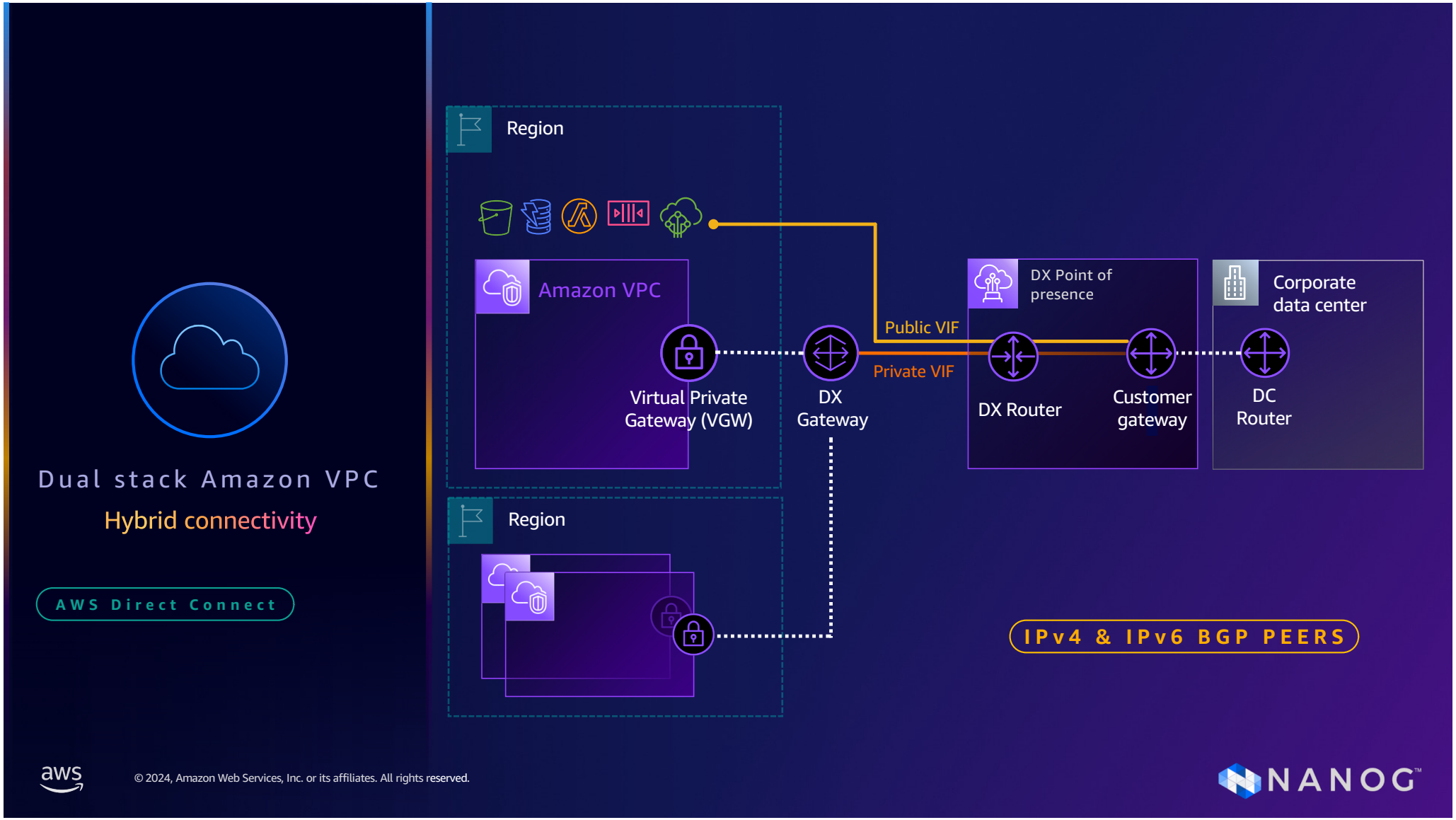
VPC to VPC connectivity

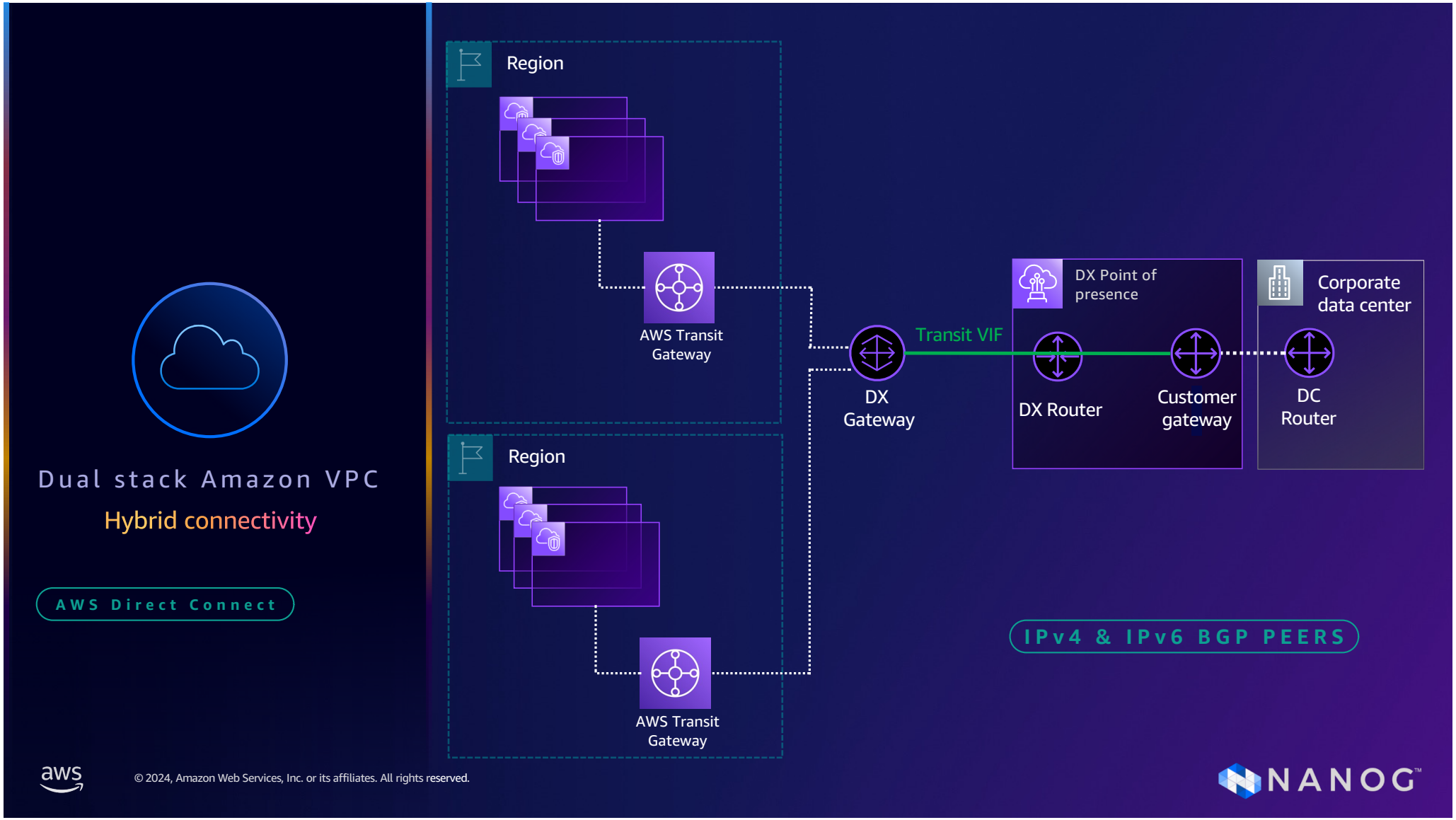
- VPC Peering
- AWS Transit Gateway
- AWS Cloud WAN

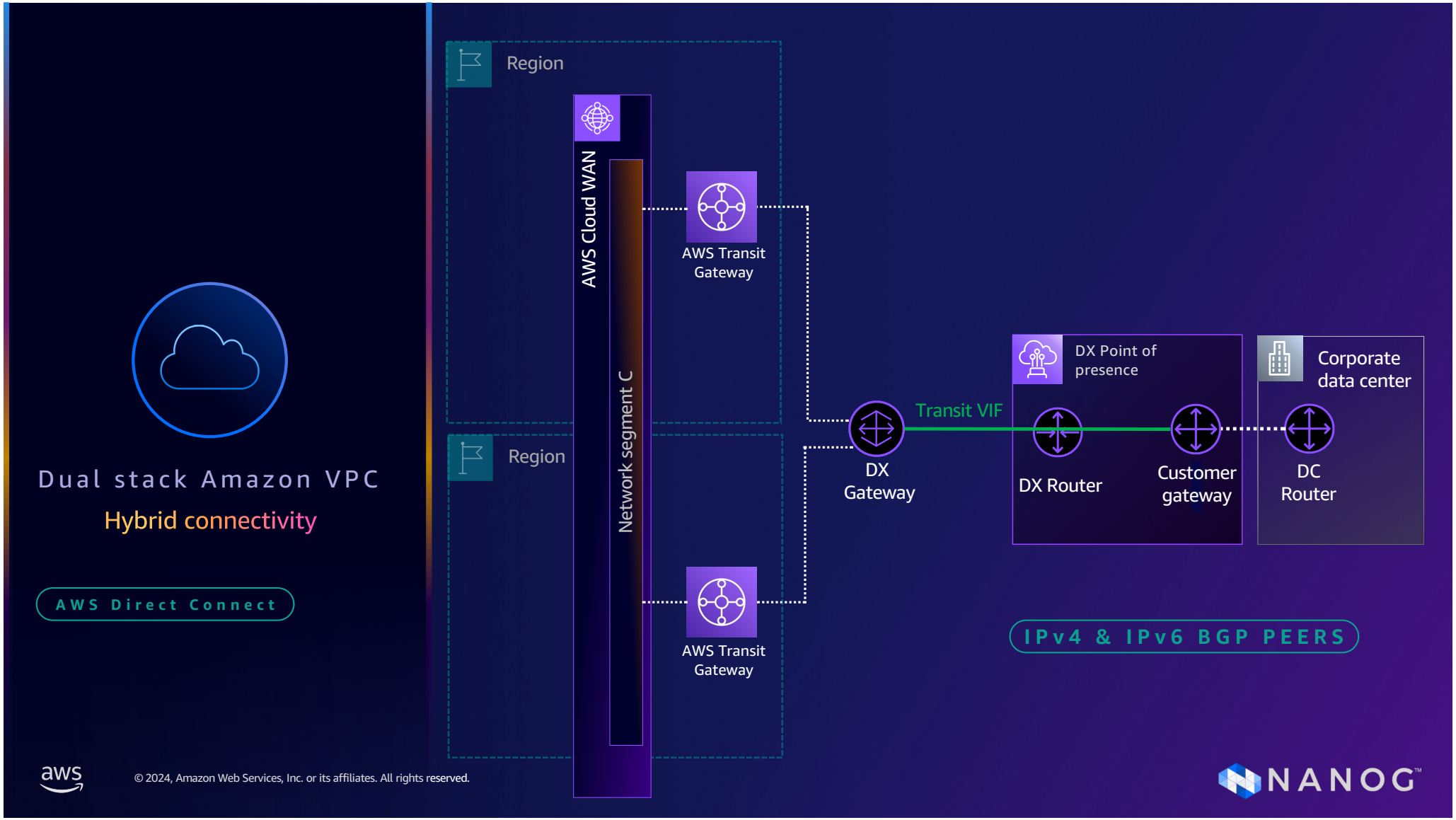


IPv6 network connectivity

- Internet connectivity
- VPC to VPC connectivity
- Hybrid connectivity




Dual stack Amazon VPC
Hybrid connectivity
AWS Direct Connect
Region
AWS Transit Gateway
Region
AWS Transit Gateway
DX Gateway
Transit VIF
DX Point of presence
DX Router
Customer gateway
Corporate data center
DC Router
IPv4 & IPv6 BGP PEERS
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
NANOG™

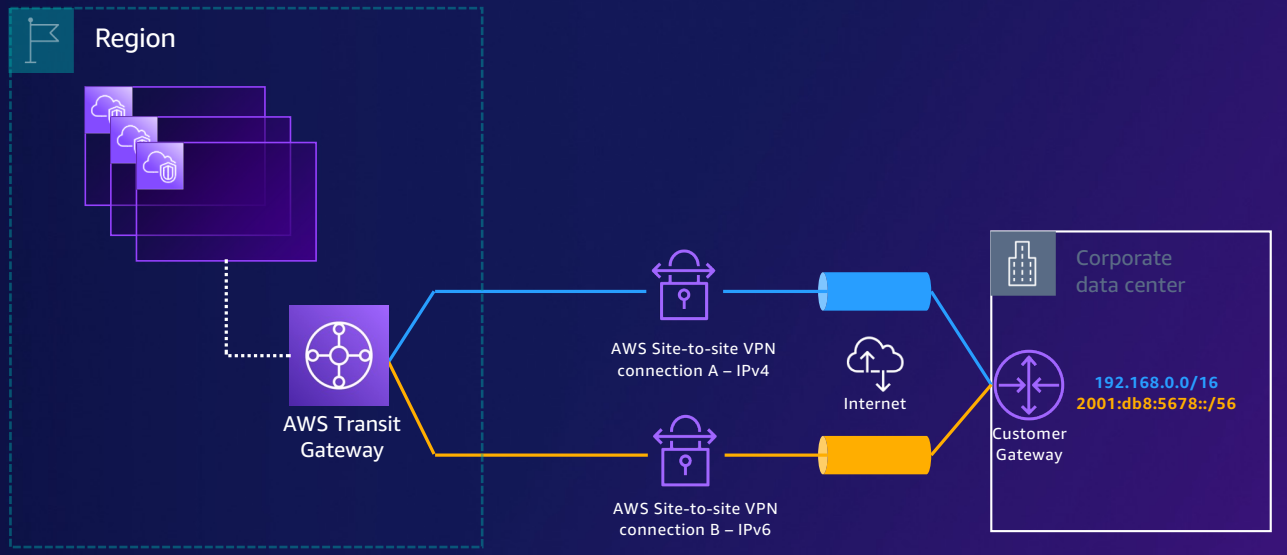

Dual stack Amazon VPC
Hybrid connectivity
AWS Direct Connect
Region
Region
AWS Cloud WAN
Network segment C
AWS Transit Gateway
AWS Transit Gateway
DX Gateway
Transit VIF
DX Point of presence
DX Router
Customer gateway
Corporate data center
DC Router
IPv4 & IPv6 BGP PEERS
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
NANOG™

Dual stack Amazon VPC

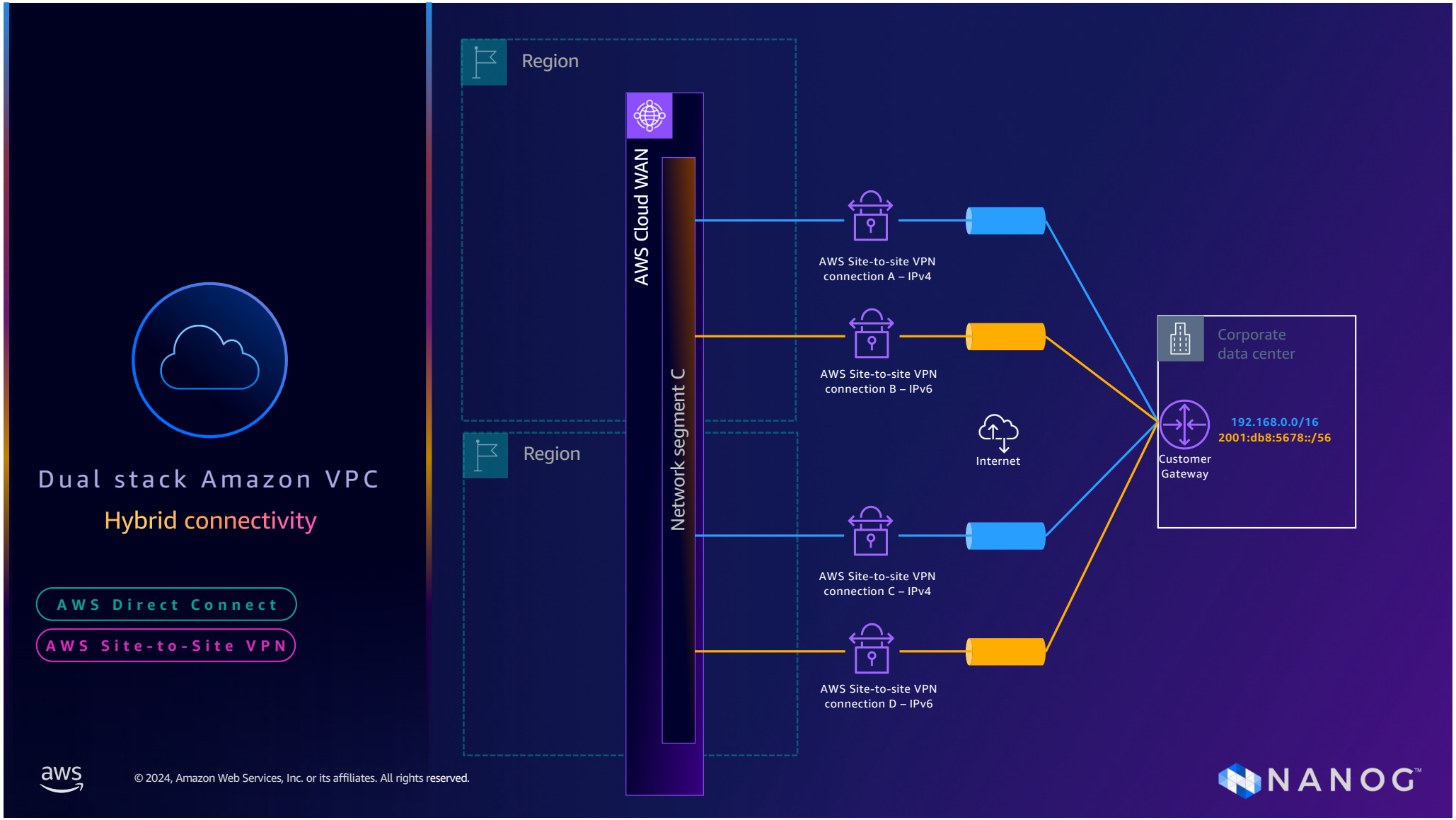
Hybrid connectivity

AWS Direct Connect

AWS Site-to-Site VPN



/30 IPv4 inner Tunnel IPs
/126 IPv6 inner Tunnel IPs


Dual stack Amazon VPC
Hybrid connectivity
AWS Direct Connect
AWS Site-to-Site VPN
Region
Region
AWS Cloud WAN
Network segment C
AWS Site-to-site VPN connection A – IPv4
AWS Site-to-site VPN connection B – IPv6
Internet
AWS Site-to-site VPN connection C – IPv4
AWS Site-to-site VPN connection D – IPv6
Corporate data center
Customer Gateway
192.168.0.0/16
2001:db8:5678::/56
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
NANOG™

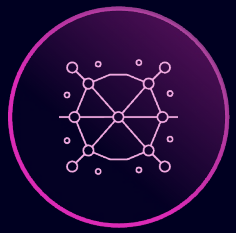

IPv6 adoption
Outside in

Configure IPv6 support for

Internal and external service delivery

Elastic Load Balancing

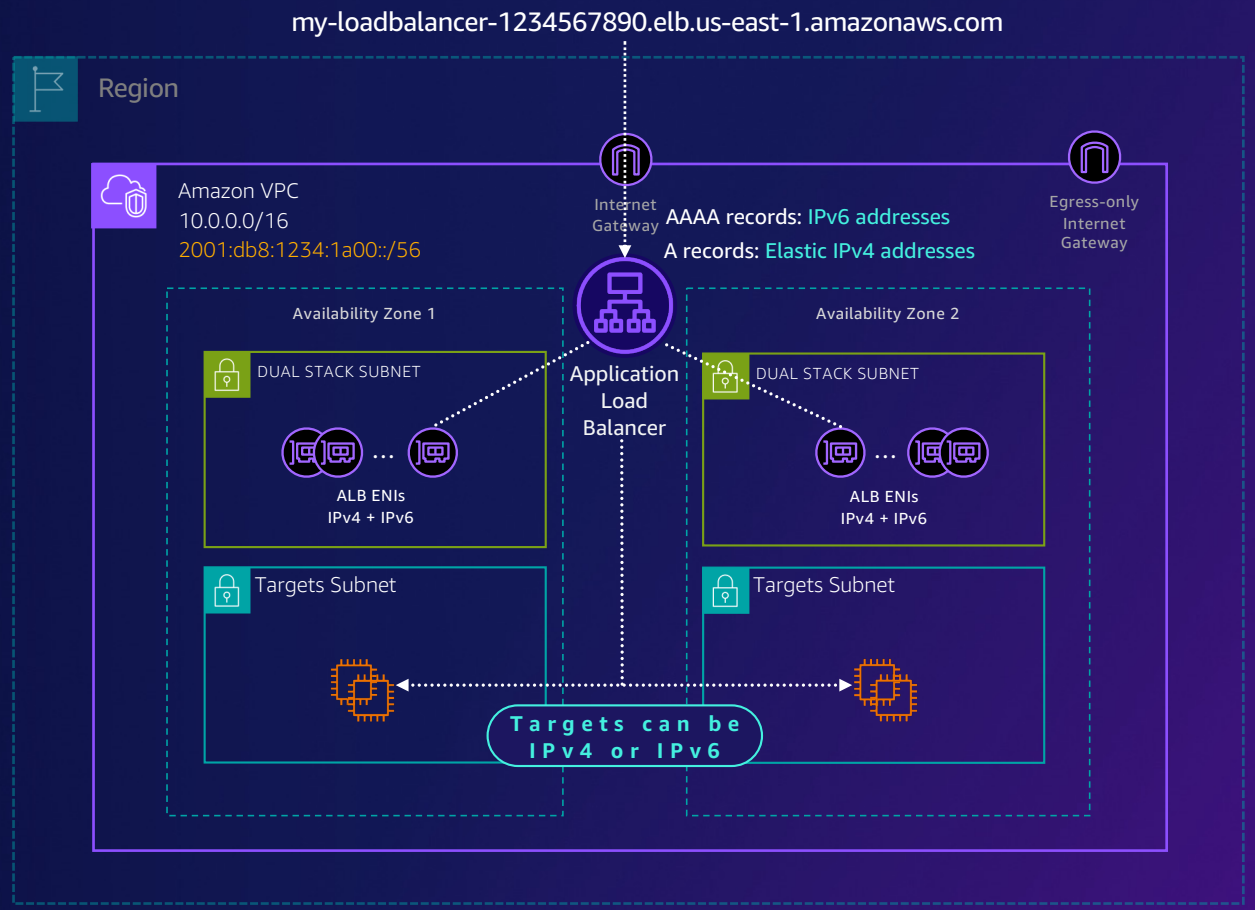
IPv6 for service delivery on AWS



IPv6 for service delivery on AWS

Elastic Load Balancing

Application Load Balancer

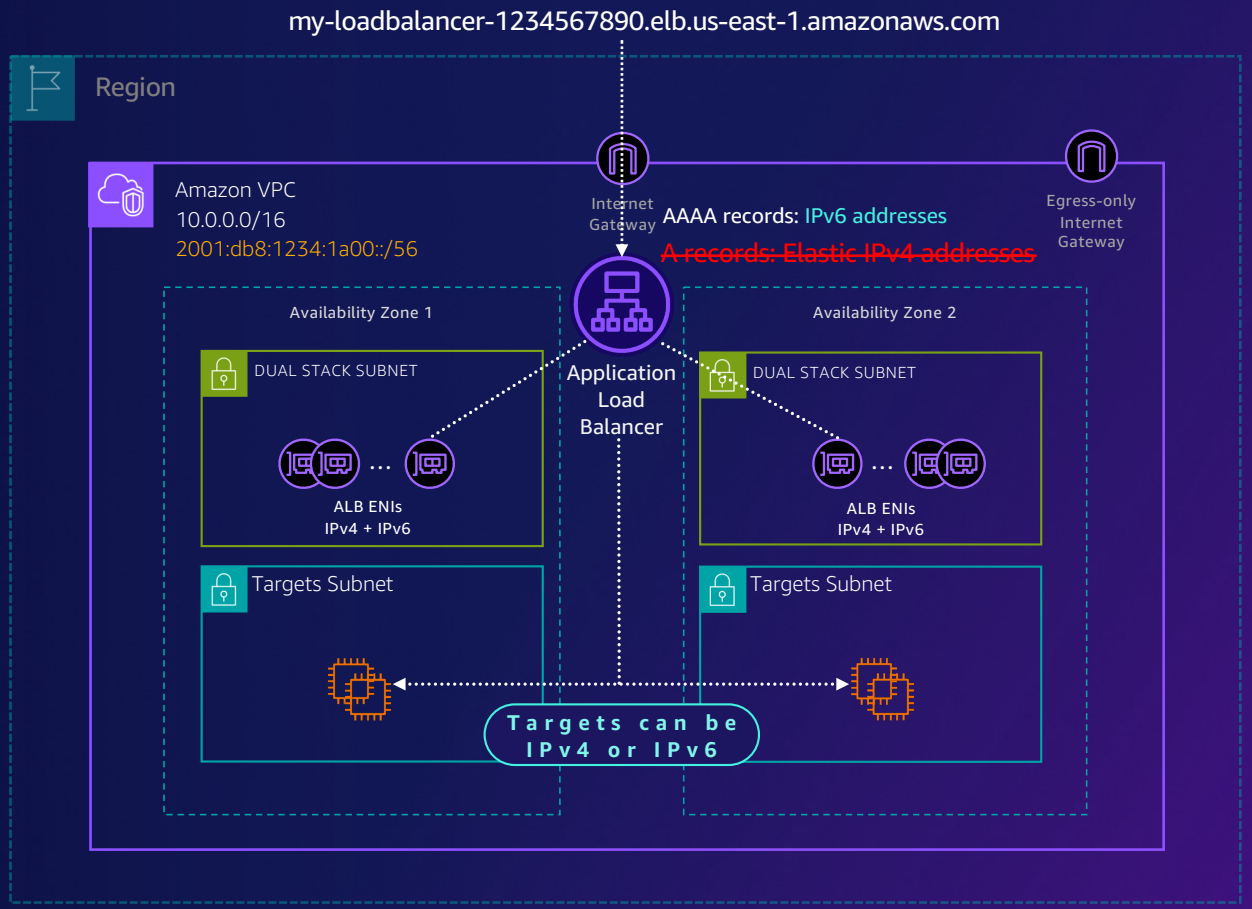


NEW

IPv6 for
service delivery on AWS

Elastic Load Balancing

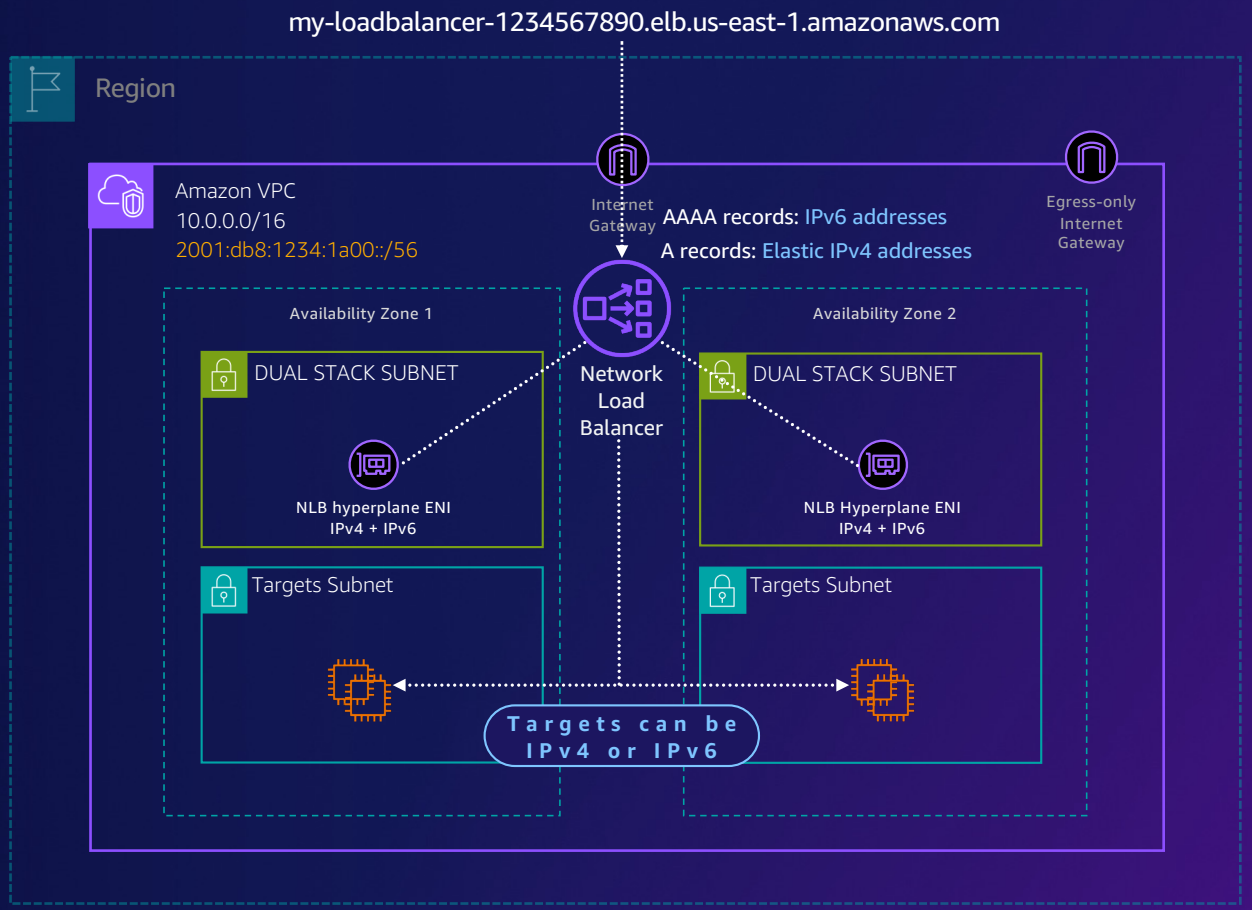
IPv6-ONLY
INTERNET-FACING ALB



IPv6 for service delivery on AWS

Elastic Load Balancing

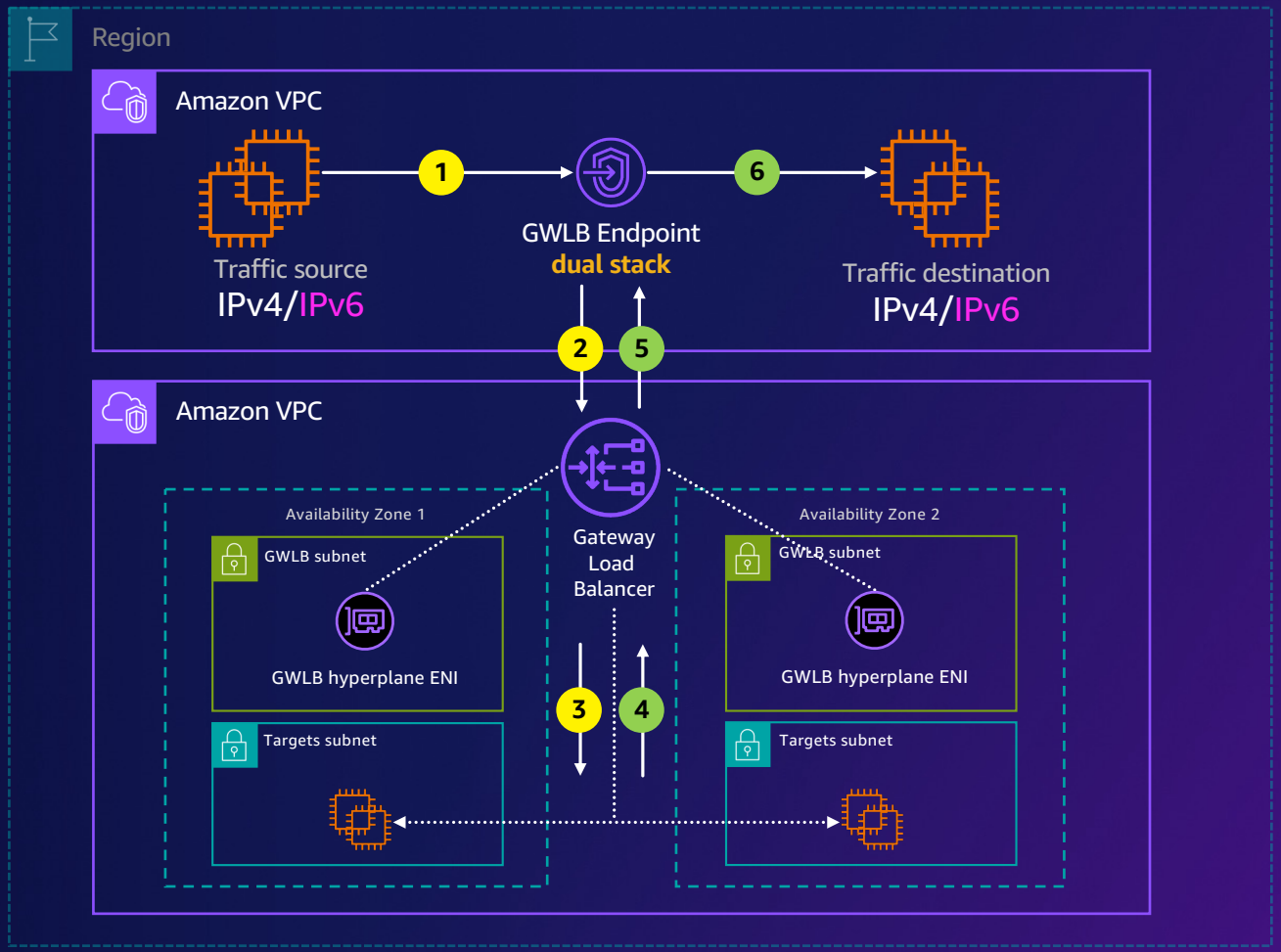
- Application Load Balancer
- Network Load Balancer



IPv6 for service delivery on AWS

Elastic Load Balancing

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



NANOG™

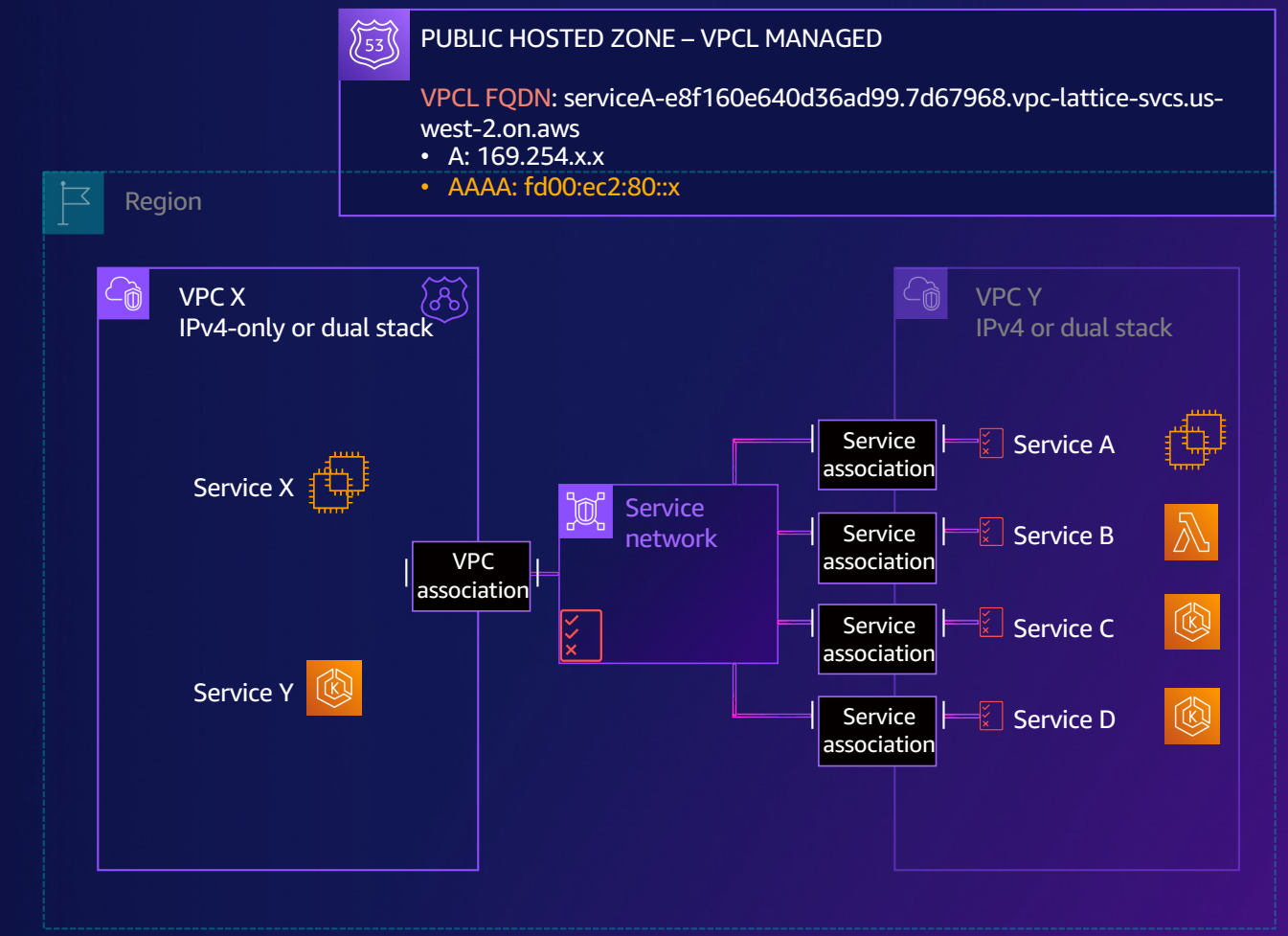
IPv6 for service delivery on AWS

Elastic Load Balancing

Amazon VPC Lattice

IPv6 for service delivery on AWS

Amazon VPC Lattice

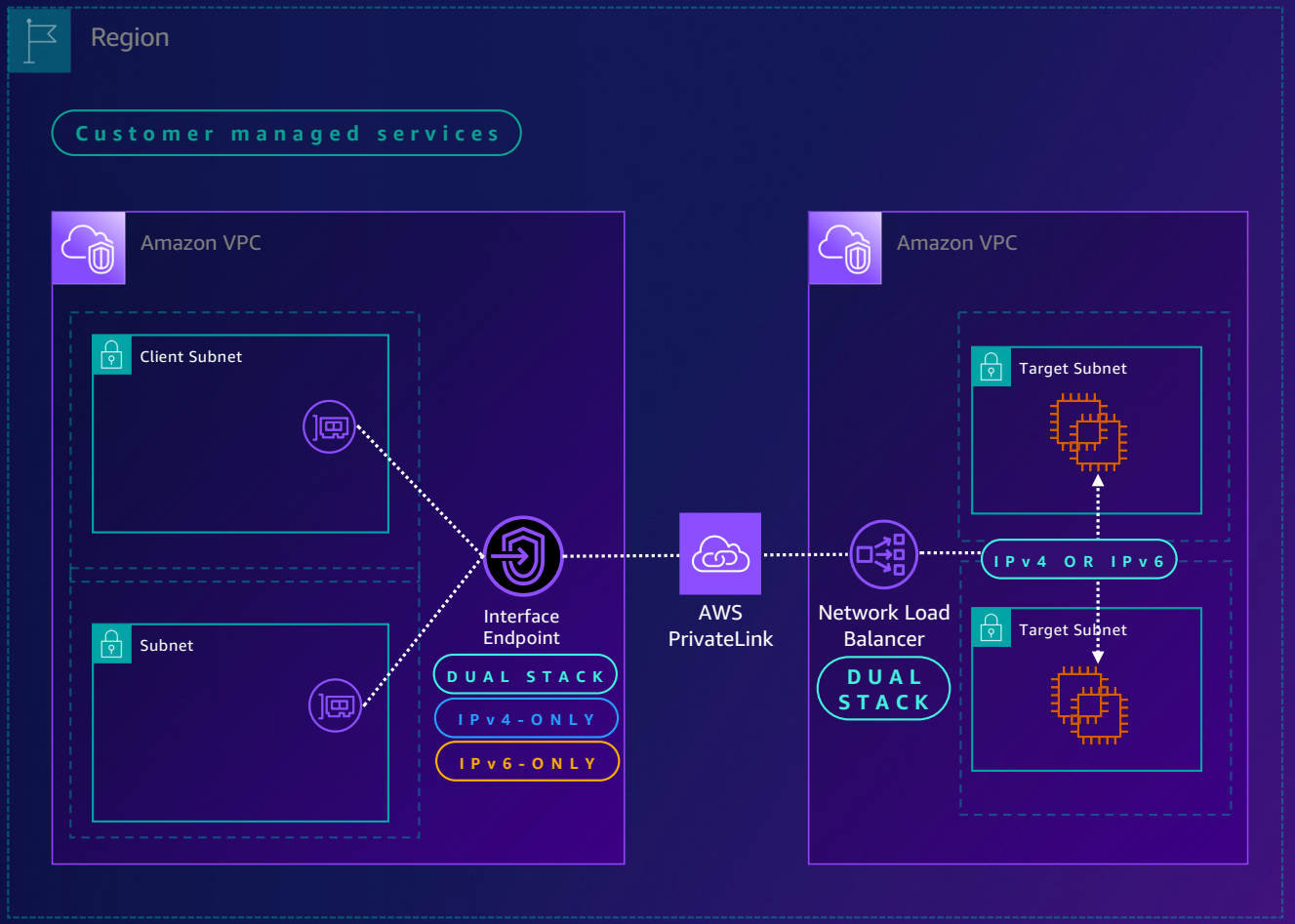


IPv6 for service delivery on AWS

- Elastic Load Balancing
- Amazon VPC Lattice
- AWS PrivateLink

IPv6 for service delivery on AWS

AWS PrivateLink

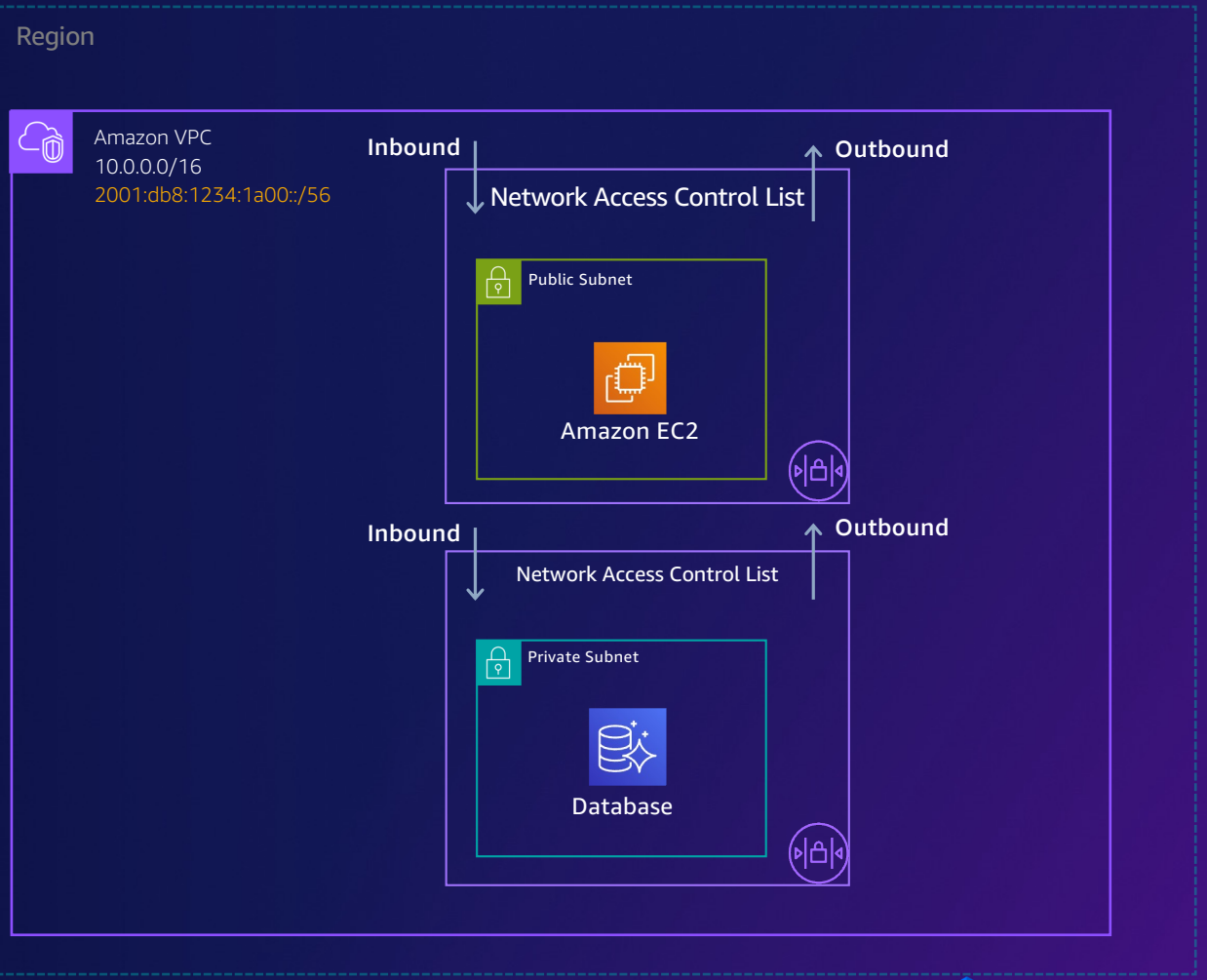



Inside-out and Outside-in
Secure IPv6 connectivity

Secure IPv6 connectivity on AWS

VPC Network Access Control Lists

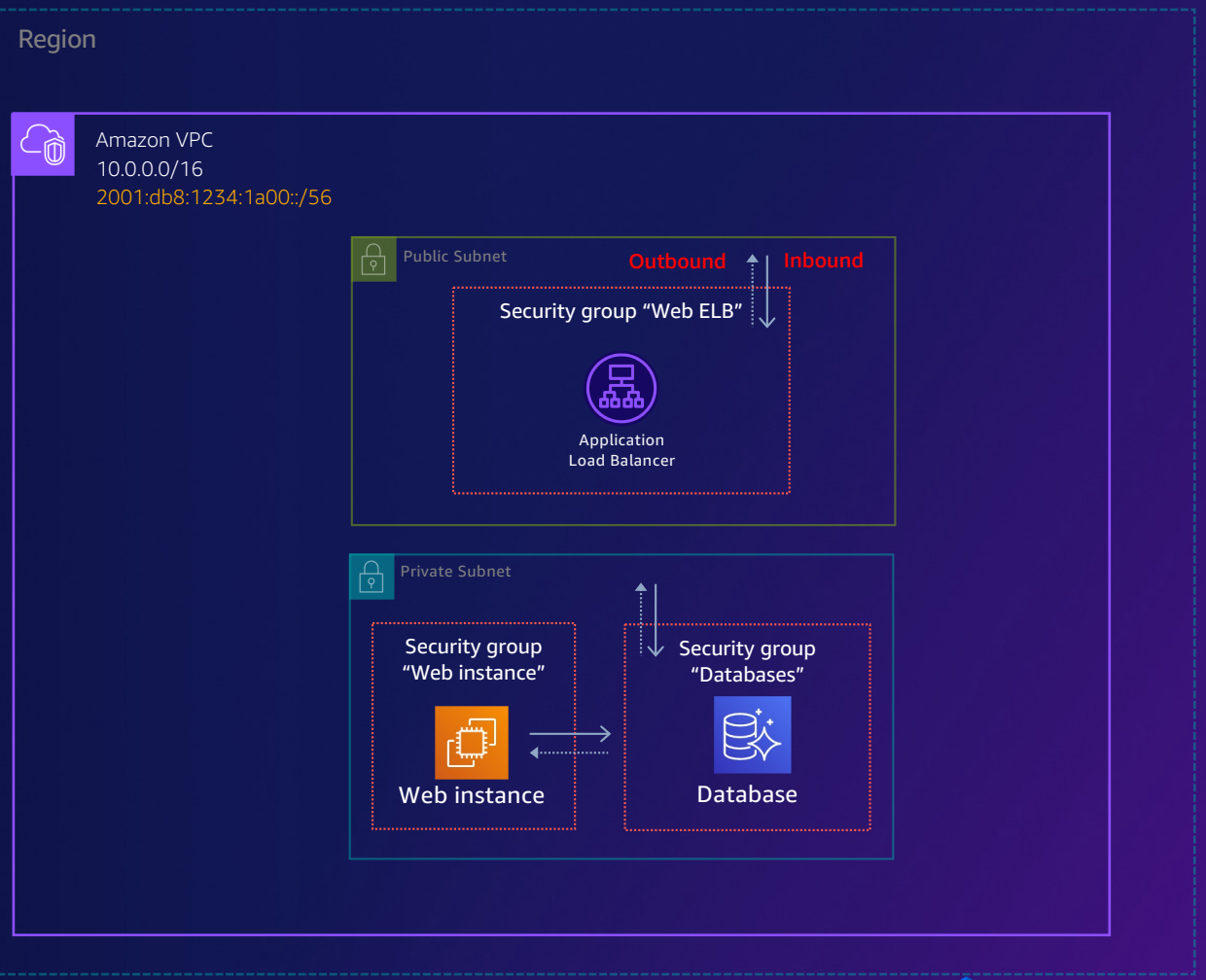
NATIVE IPv4 & IPv6



Secure IPv6 connectivity on AWS

VPC Security Groups

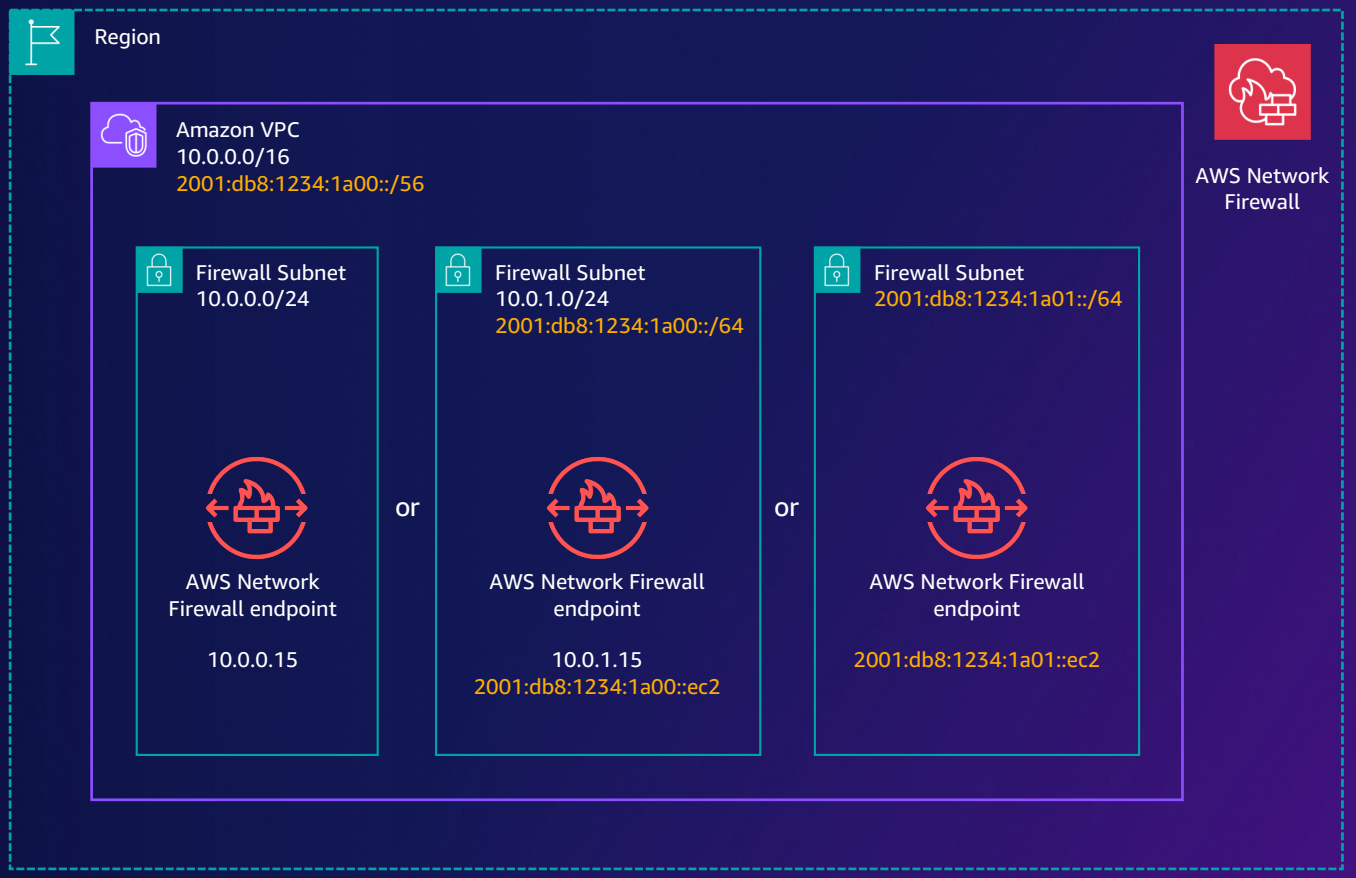
NATIVE IPv4 & IPv6



NANOG™

Secure IPv6 connectivity on AWS

AWS Network Firewall



Secure IPv6 connectivity on AWS

AWS WAF & AWS Shield

AWS WAF

Protects web applications by allowing you to write custom rules or choose managed rules from AWS or the AWS Marketplace.

AWS Shield & Shield Advanced

Managed threat protection that blocks DDoS attacks, vulnerability exploitation, and bad bots

IPv4 & IPv6


Build
Scalable IPv6 internet edge connectivity

Scalable IPv6 edge connectivity

Amazon CloudFront

Scalable IPv6 edge connectivity

Amazon CloudFront

DUAL STACK BY DEFAULT

Scalable IPv6 edge connectivity

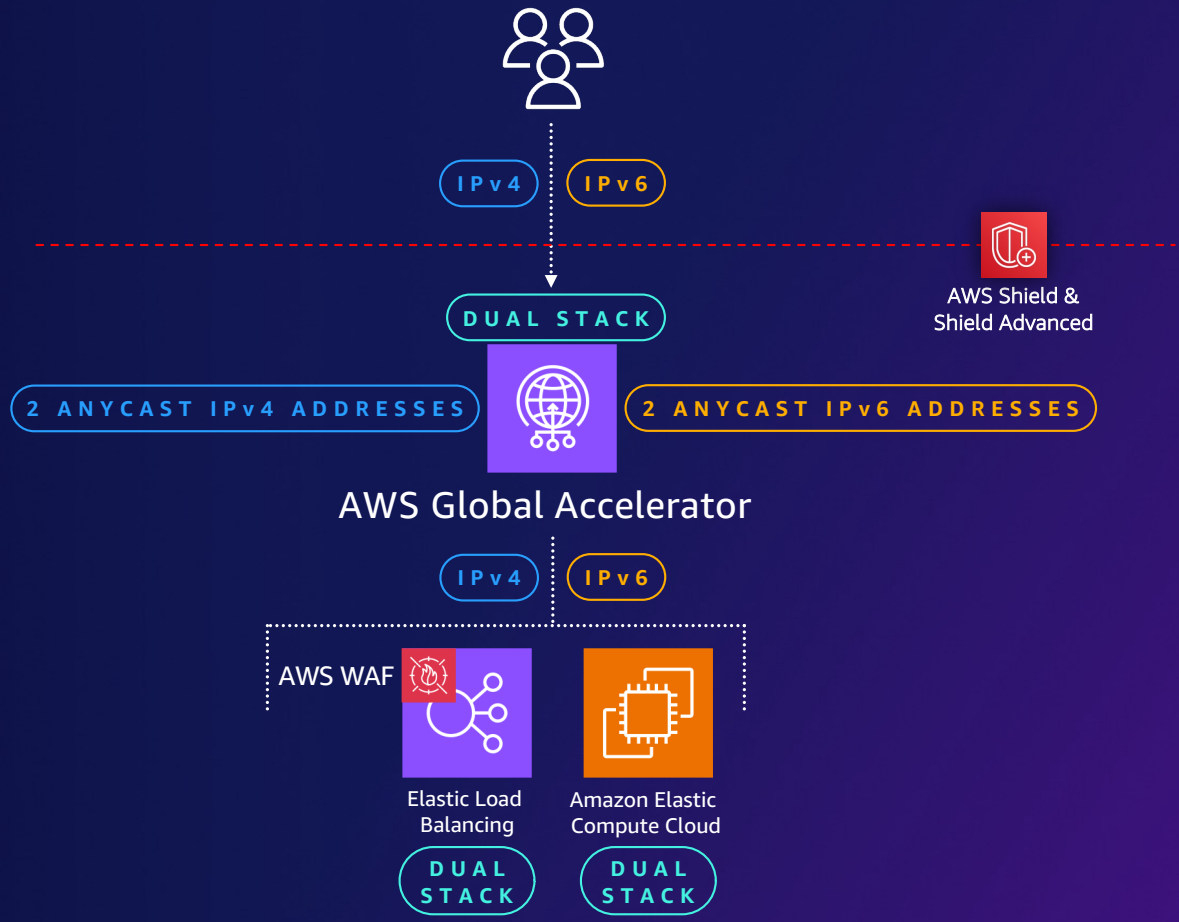
Amazon CloudFront

AWS Global Accelerator

NANOG™

Scalable IPv6 edge connectivity

AWS Global Accelerator



IPv6 on AWS
Service compatibility matrix

IPv6 on AWS

Start now

All resources

Thank you!