

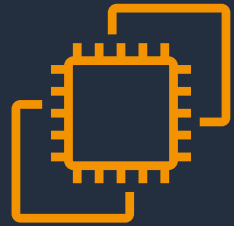
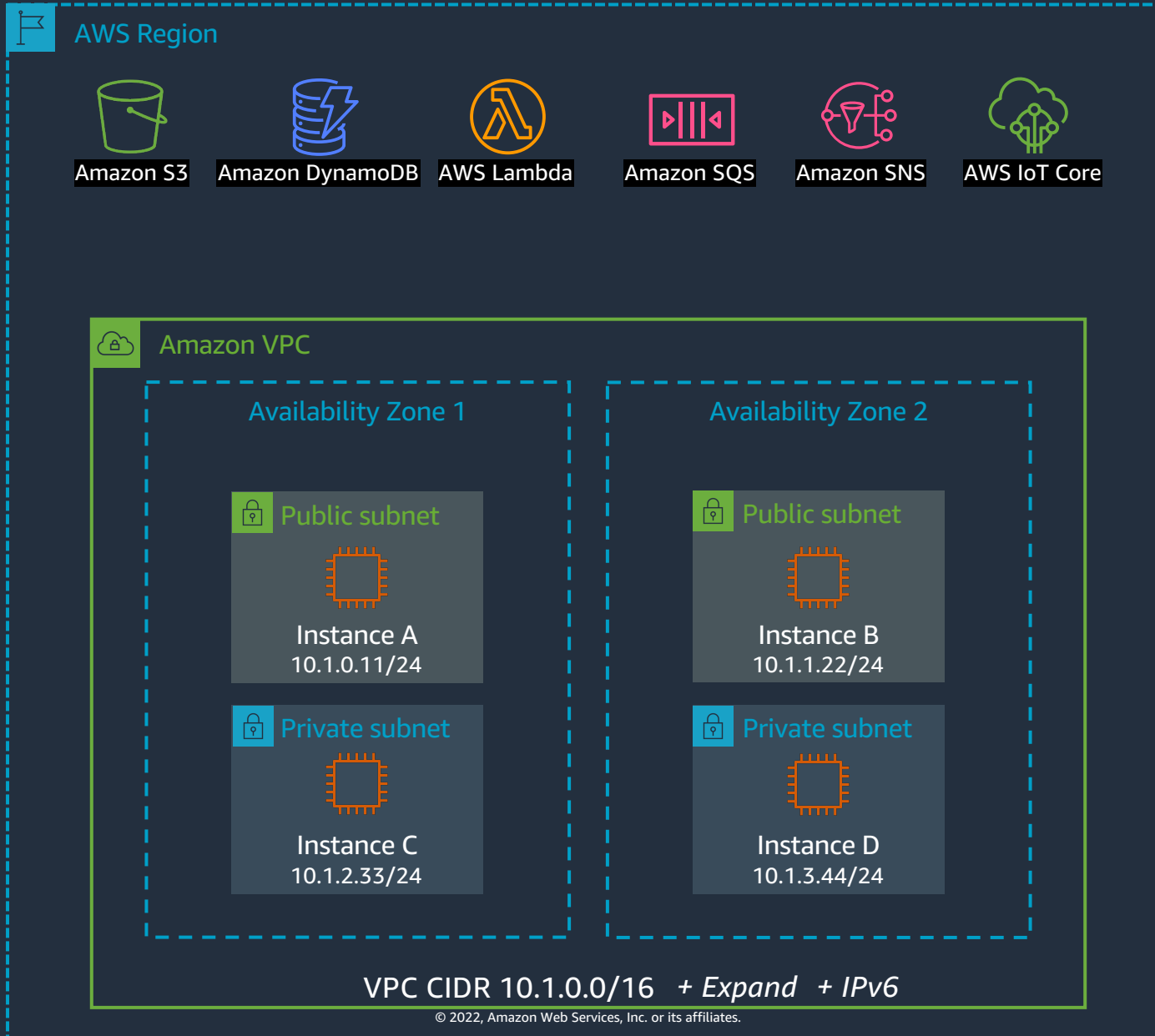


# Advanced Amazon VPC design and new capabilities

Dragos Madarasan (he/him)

Solutions Architect Team Lead  
AWS

# Amazon VPC networking

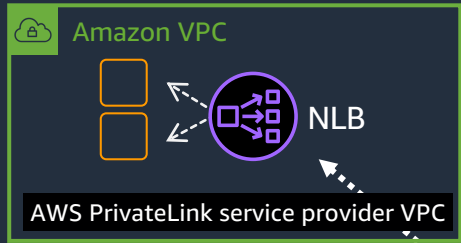


Amazon Elastic Cloud Compute (Amazon EC2)



Amazon Virtual Private Cloud (Amazon VPC)



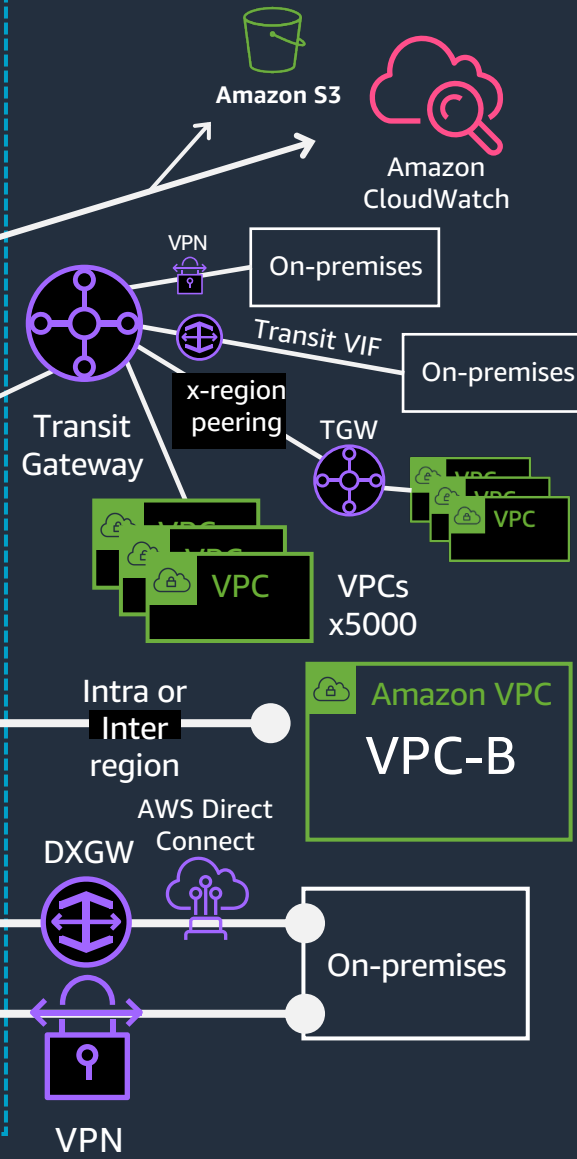
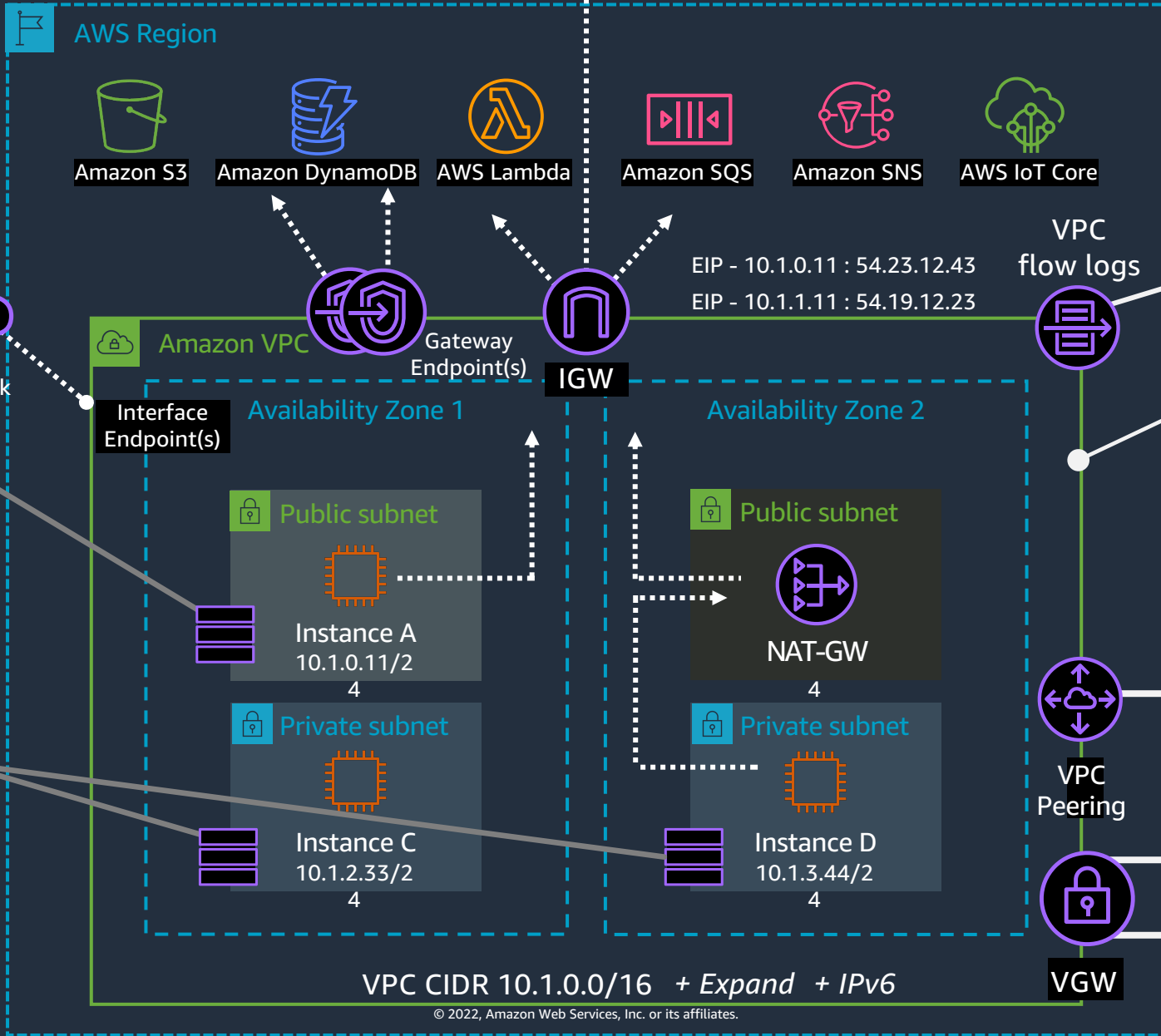


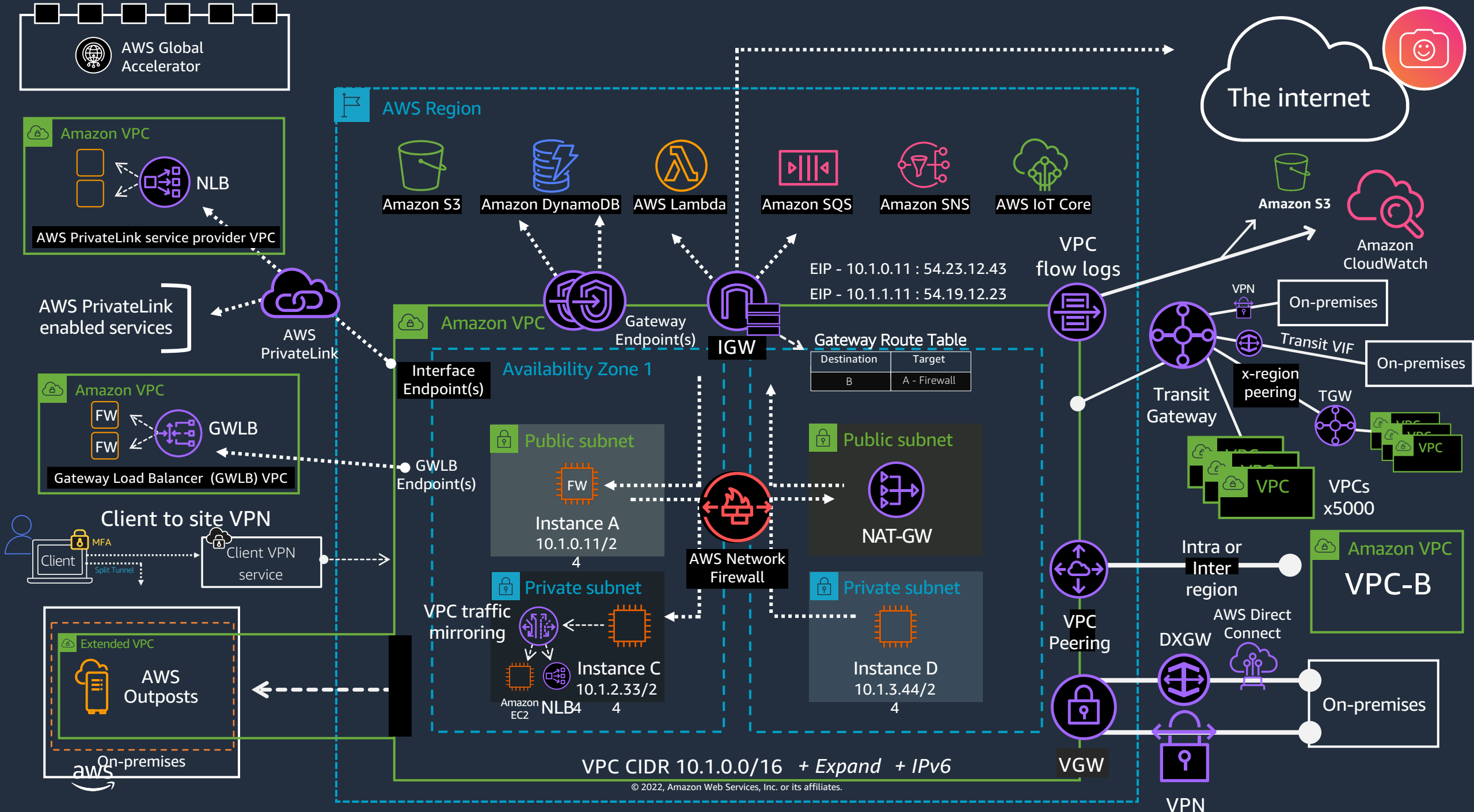
AWS PrivateLink enabled services



Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other routes	TGW

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW
DDB.prefix.list	VPCE-234
On-premises	VGW
VPC-B	PCX-123
Other routes	TGW







**What else have we been up to?**

# IPv6

## **Amazon VPC**

IPv6-only subnets

---

## **NAT64 and DNS64**

Interoperability with IPv4 environments

---

## **Amazon EC2**

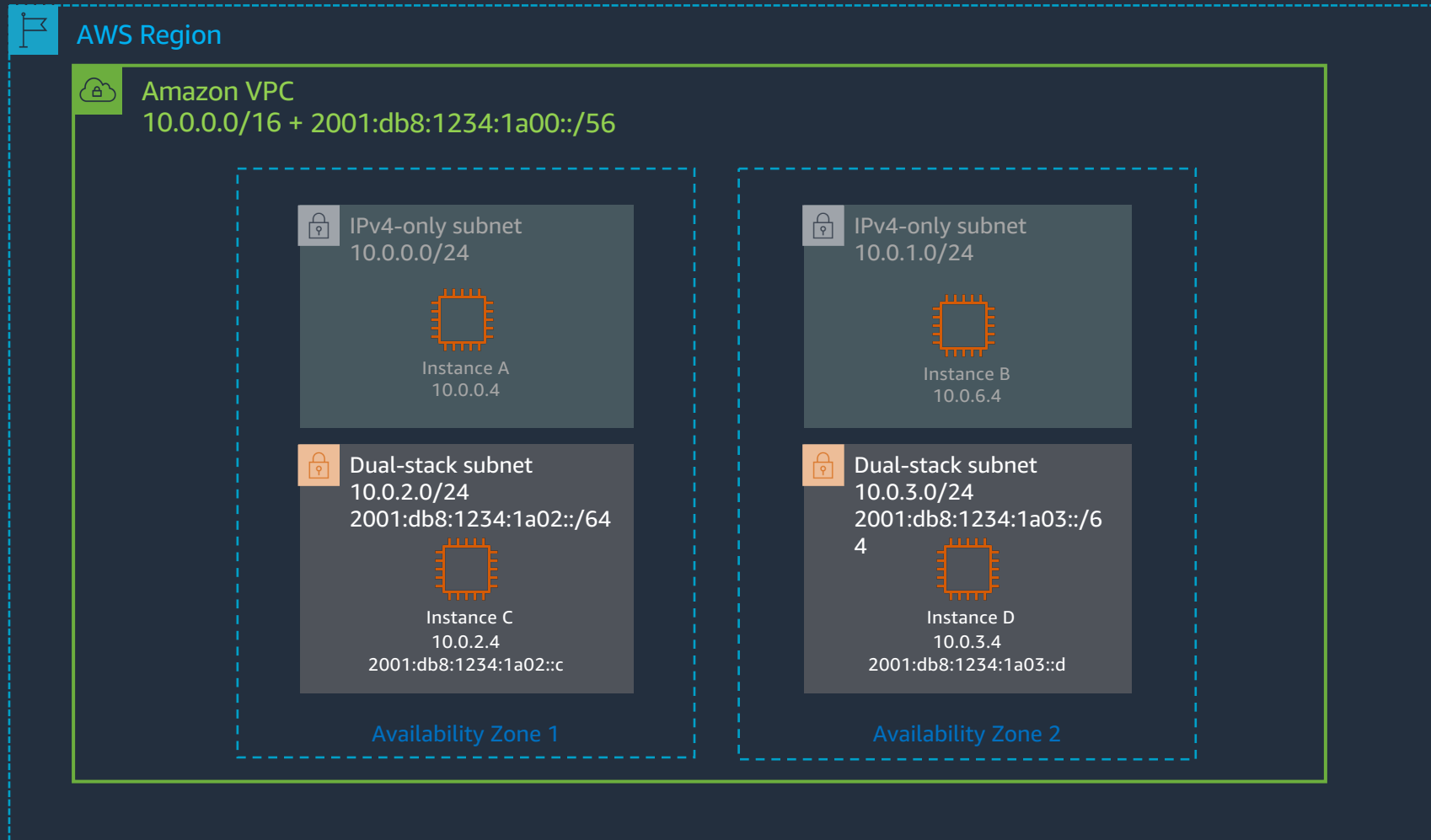
Resource-based instance naming

---

## **Elastic Load Balancing**

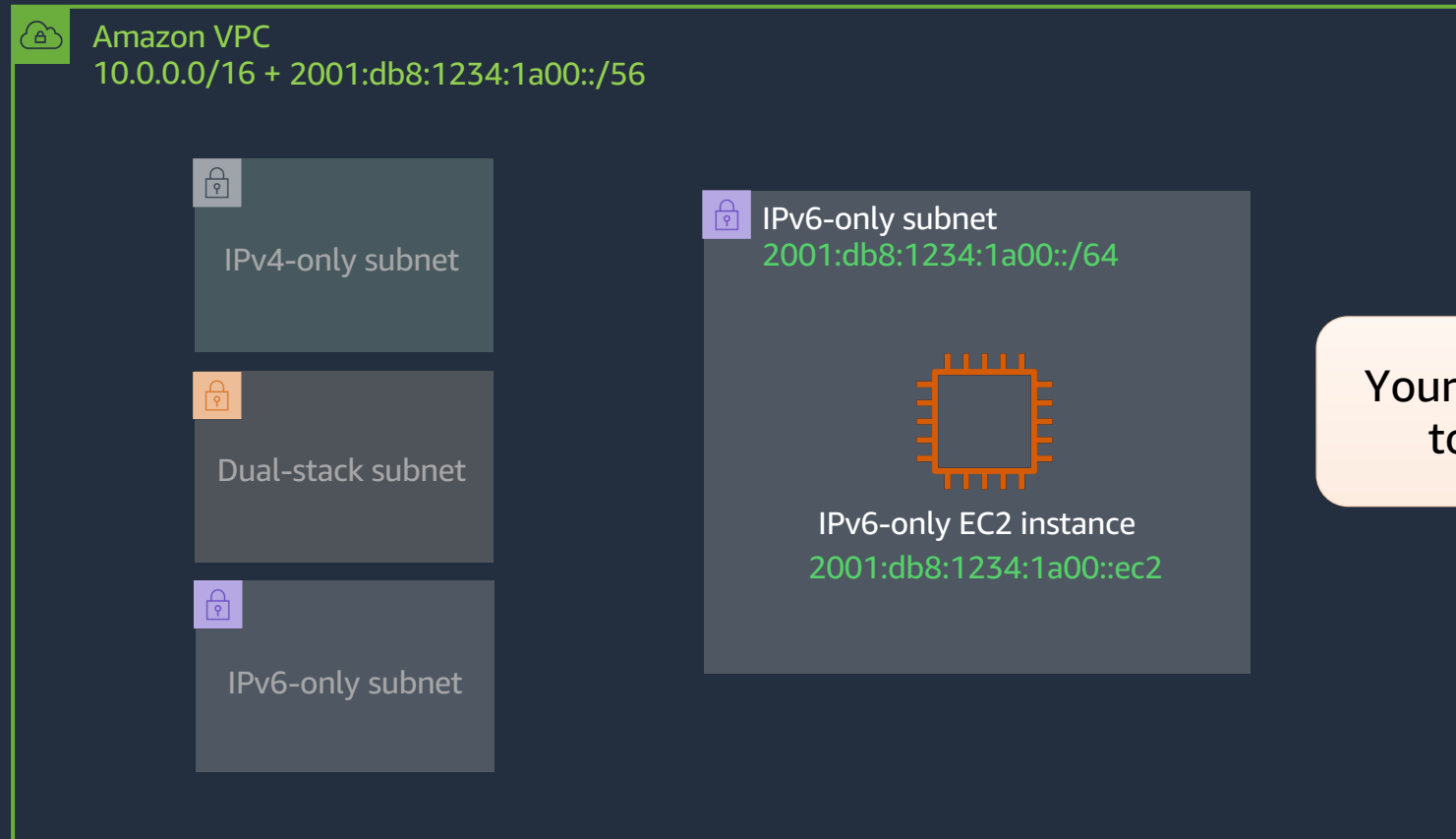
Full dual-stack IPv6 support

# Amazon VPC: Native dual stack



NEW

# Amazon dual-stack VPC: IPv6-only subnets



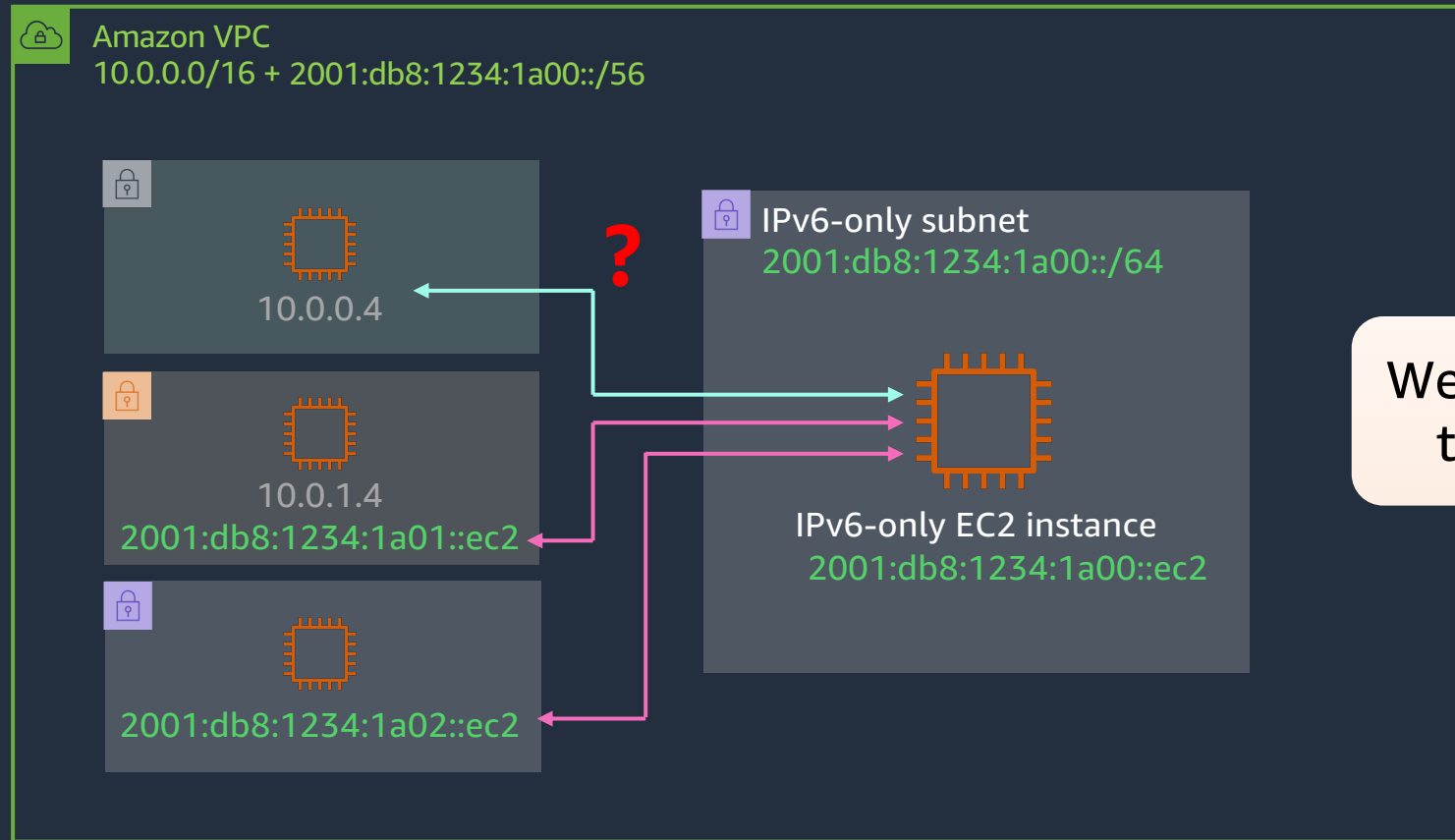
Your VPC will continue to be *dual stack*!



# Traffic flows inside Amazon VPC

# Amazon dual-stack VPC: IPv6 only subnets

## FLAWS



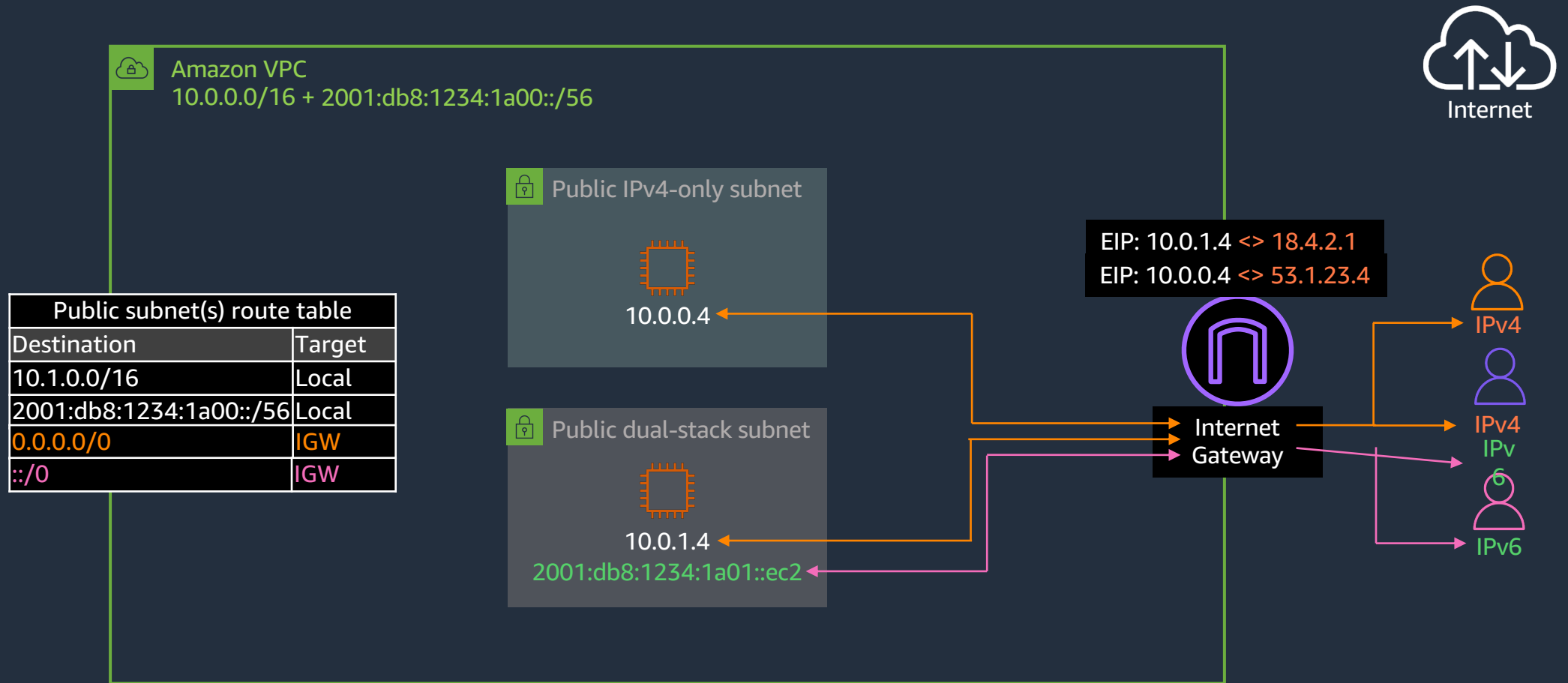
We'll get back to this traffic flow later!



# Public subnets internet connectivity

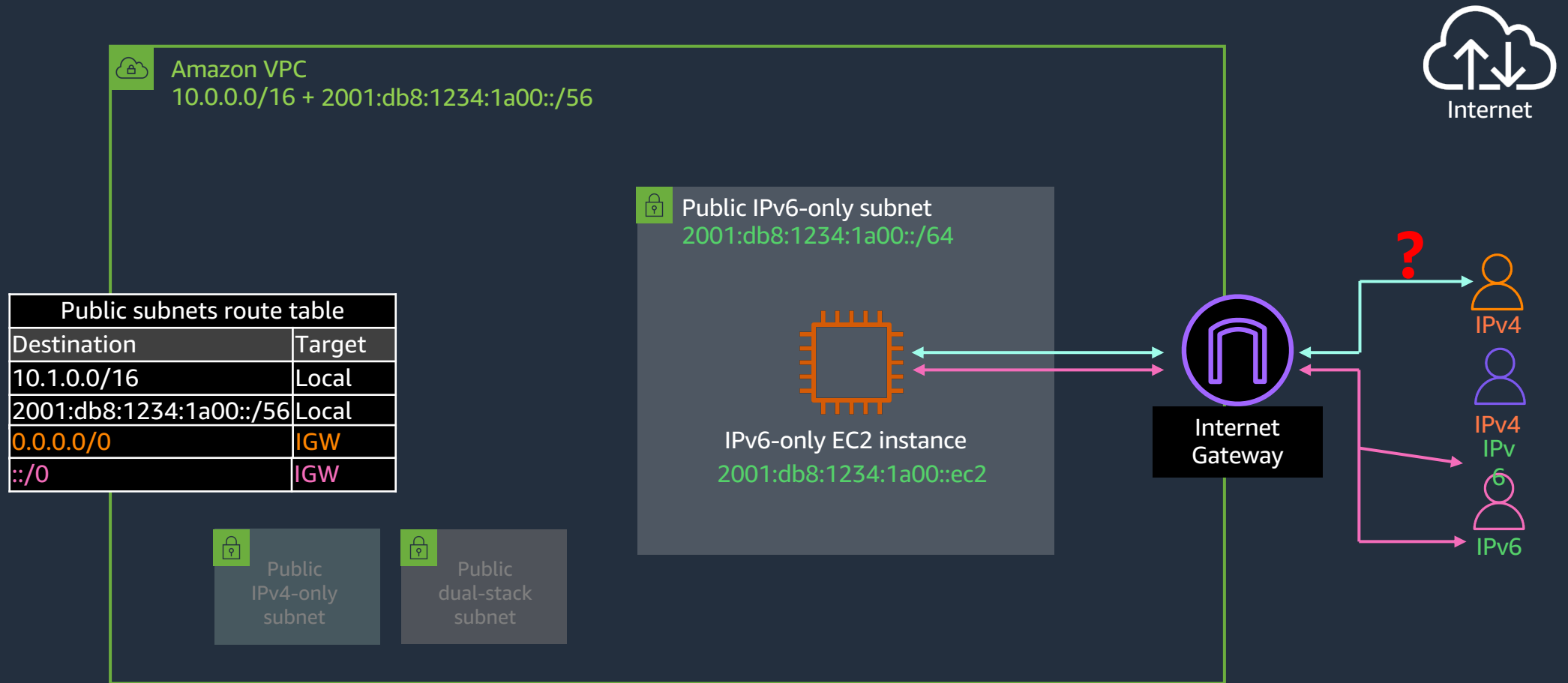
# Amazon dual-stack VPC: Internet connectivity

## PUBLIC SUBNETS



# Amazon dual-stack VPC: Internet connectivity

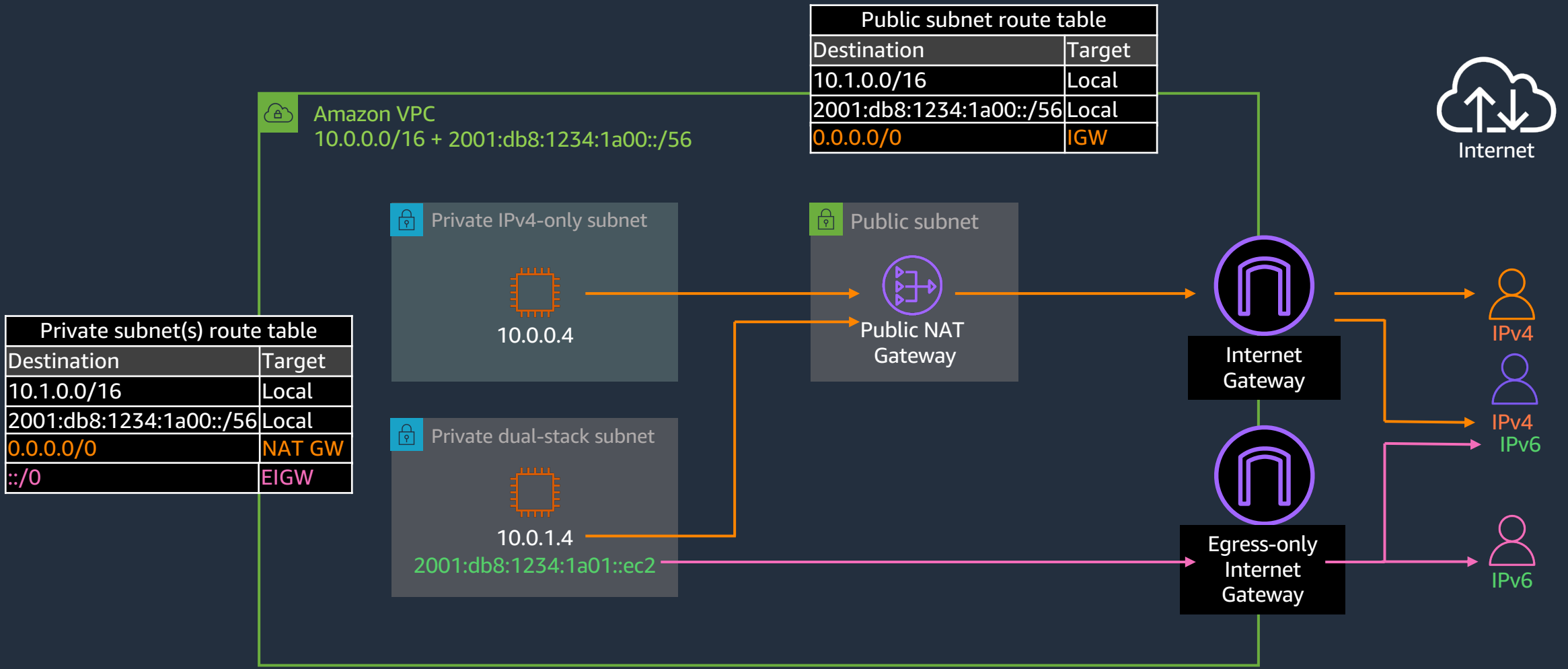
## PUBLIC IPV6-ONLY SUBNETS



# Private subnets internet connectivity

# Amazon dual-stack VPC: Internet connectivity

## PRIVATE SUBNETS

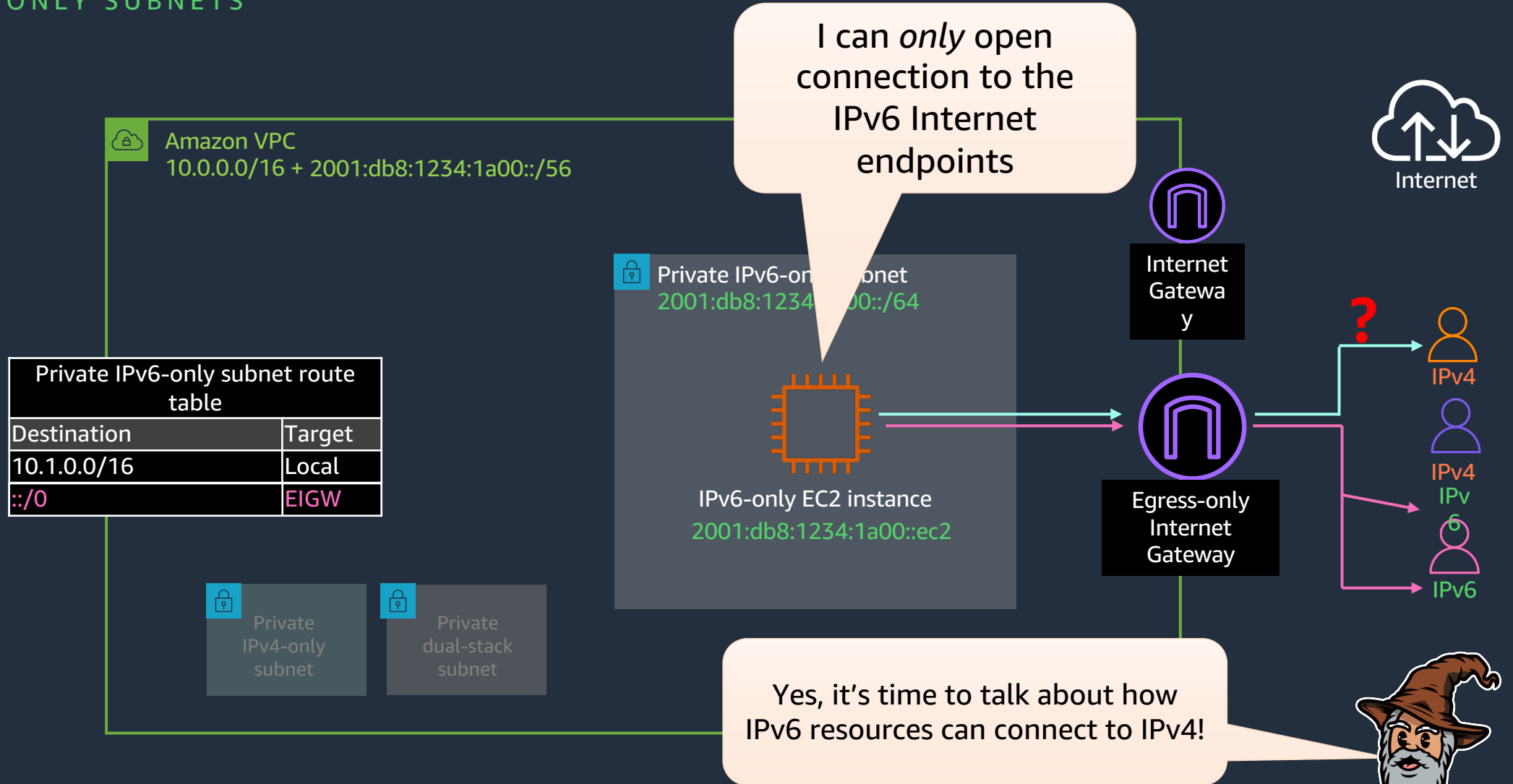


The EIGW does **not** allow internet connections to be opened to IPv6 resources in private subnets



# Amazon dual-stack VPC: Internet connectivity

## PRIVATE IPV6-ONLY SUBNETS



# IPv6

## Amazon VPC

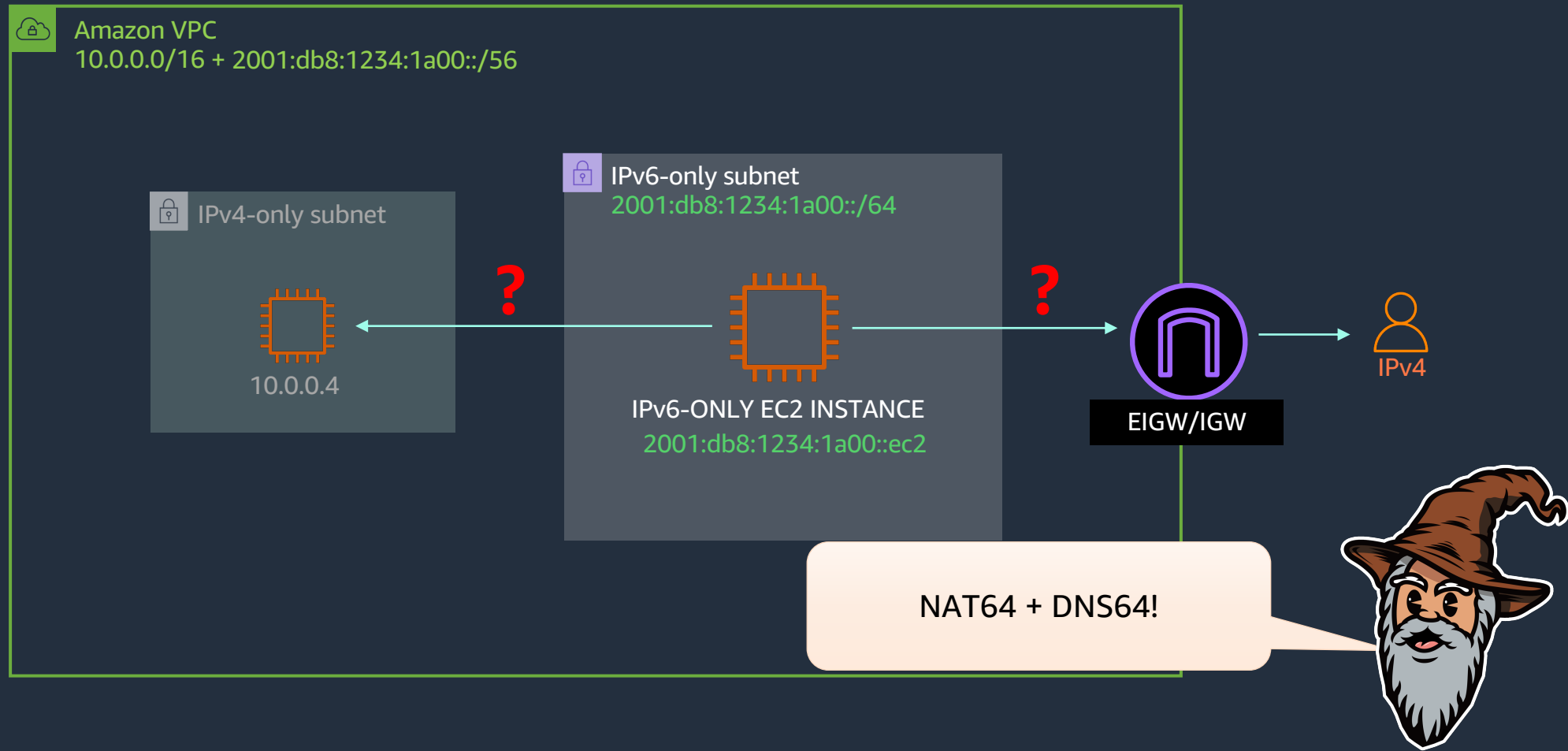
IPv6-only subnets

---

## NAT64 and DNS64

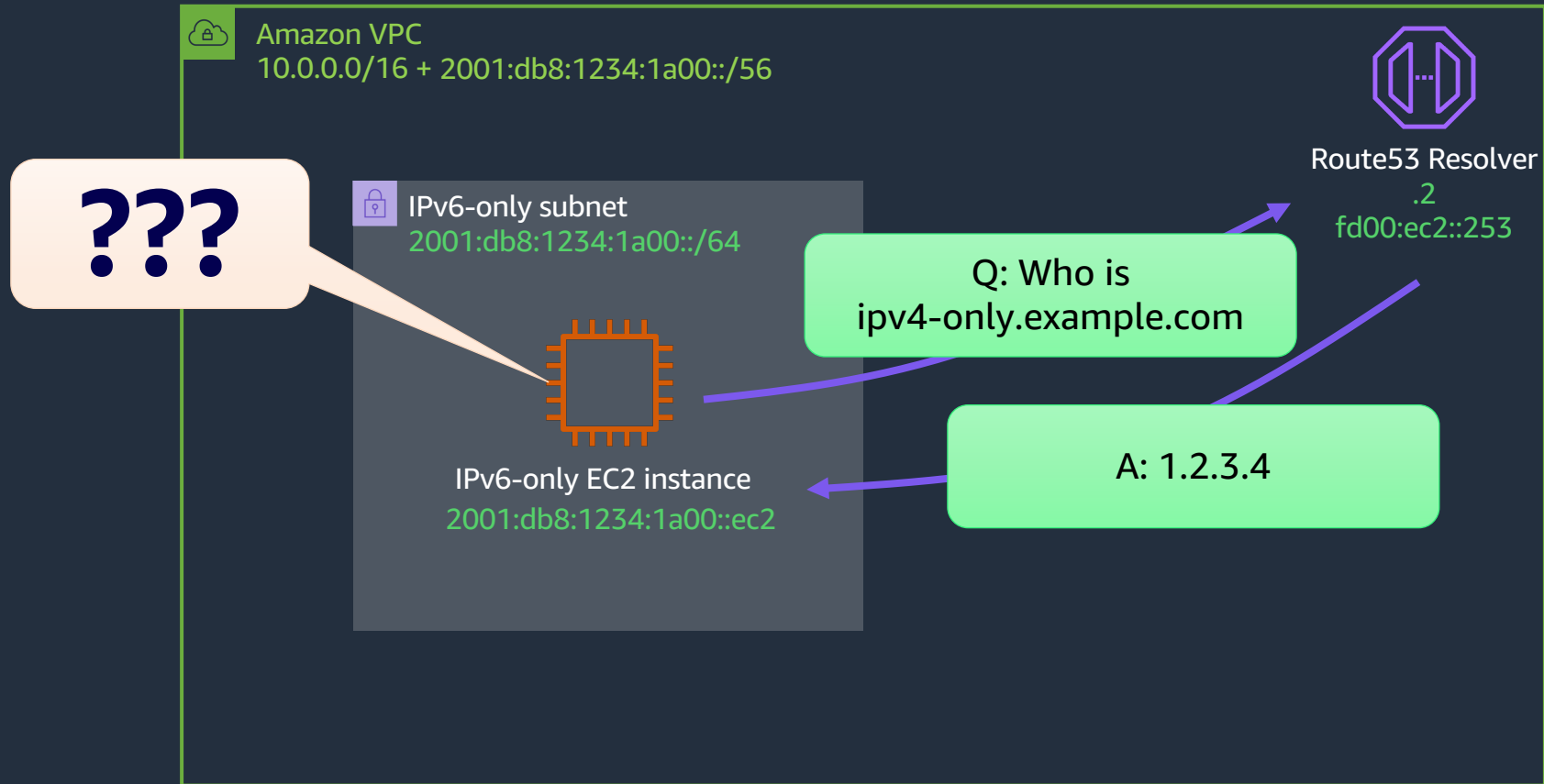
Interoperability with IPv4 environments

# Amazon dual-stack VPC: IPv6 to IPv4



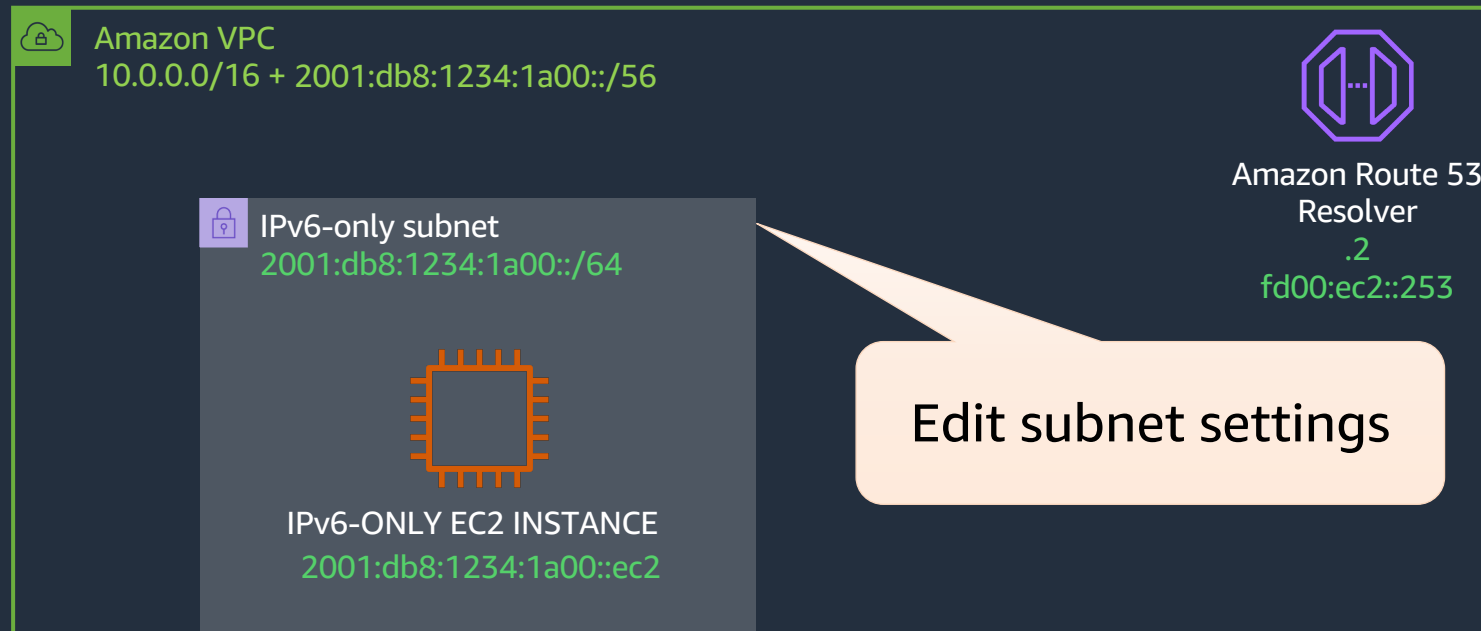
# Amazon VPC DNS

BEFORE



# DNS64

# What is DNS64?



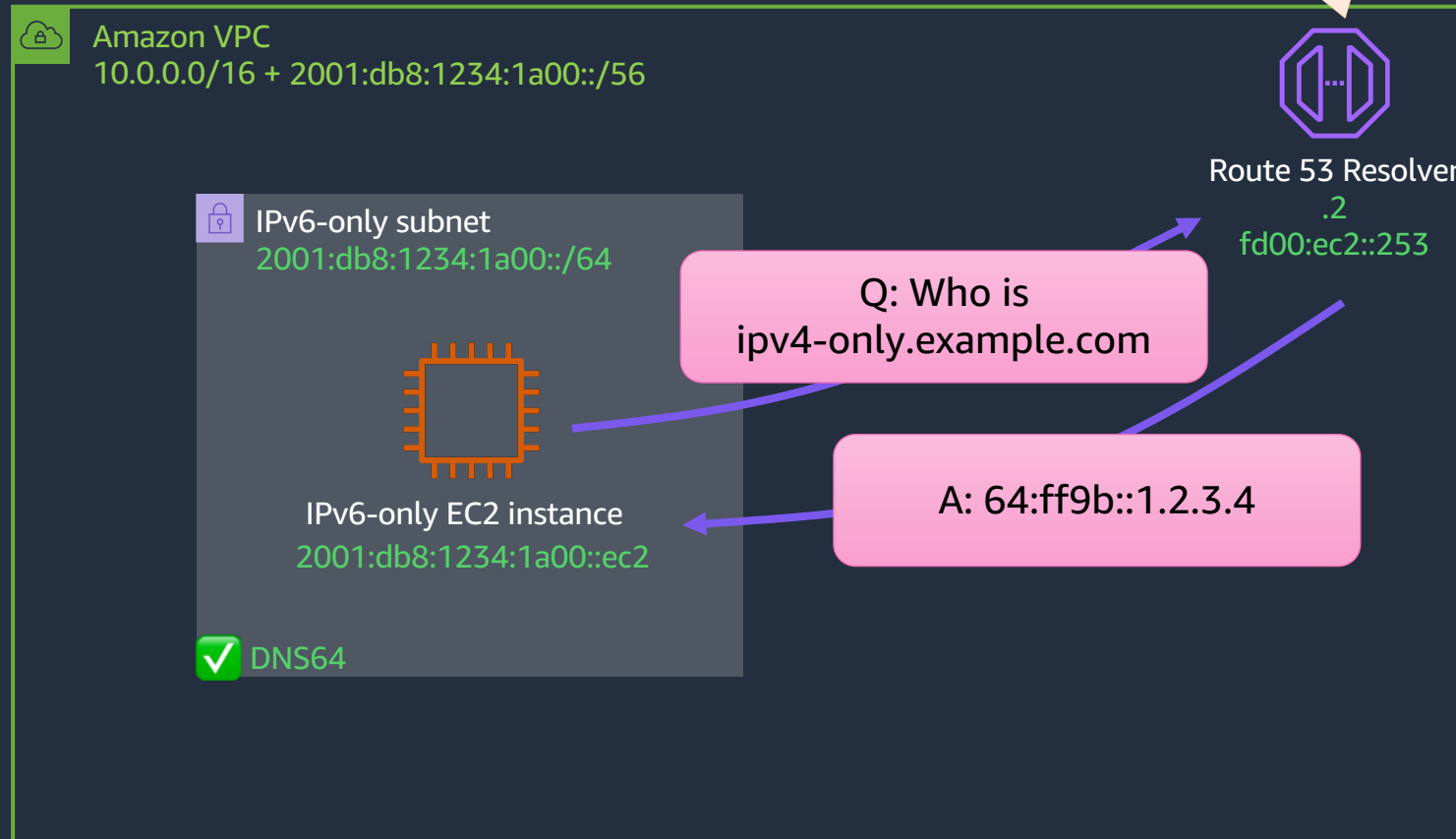
## DNS64 settings

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

Enable DNS64 [Info](#)

# What is DNS64?

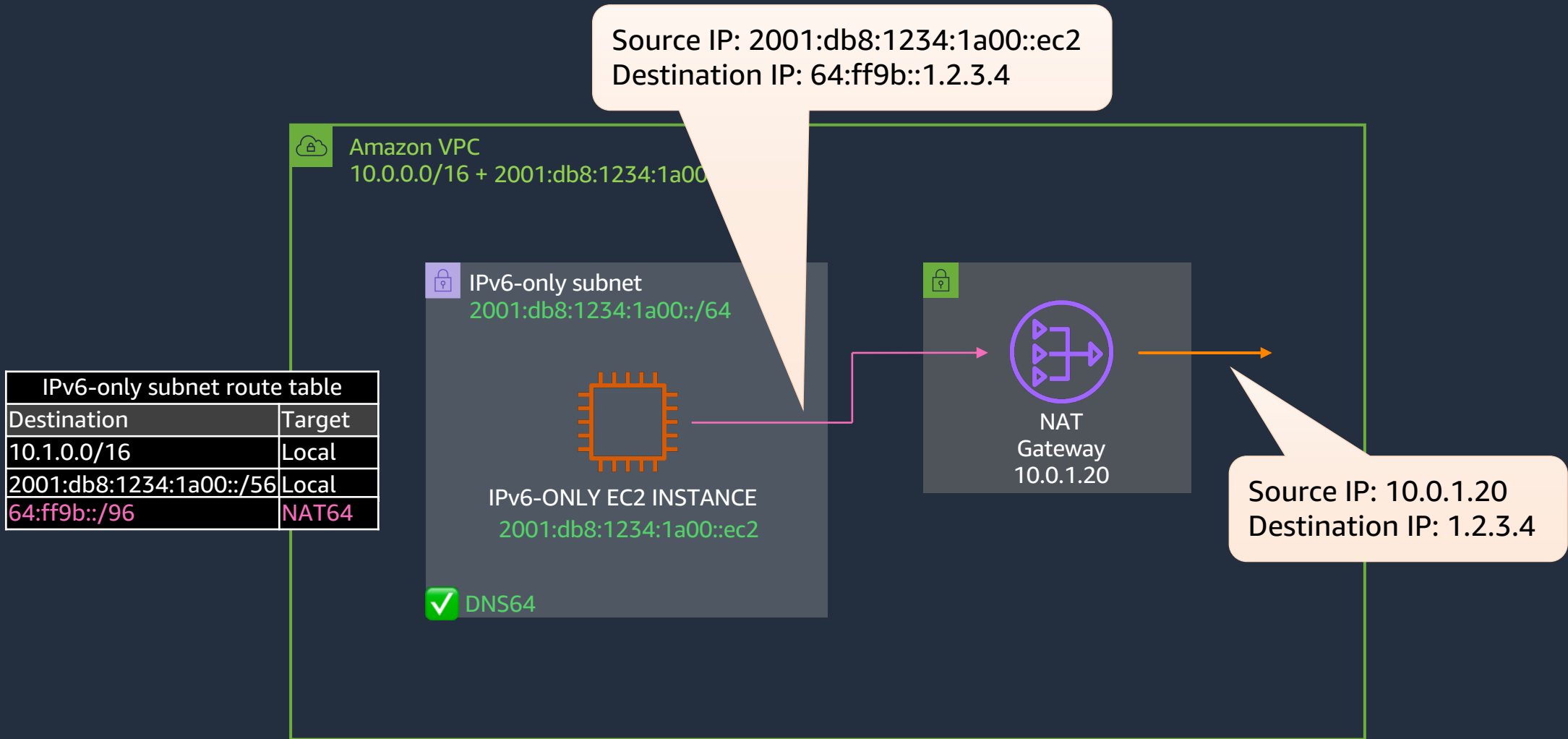
Route 53 Resolver synthesizes an IPv6 address by adding 64:ff9b::/96 to the IPv4 address!



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

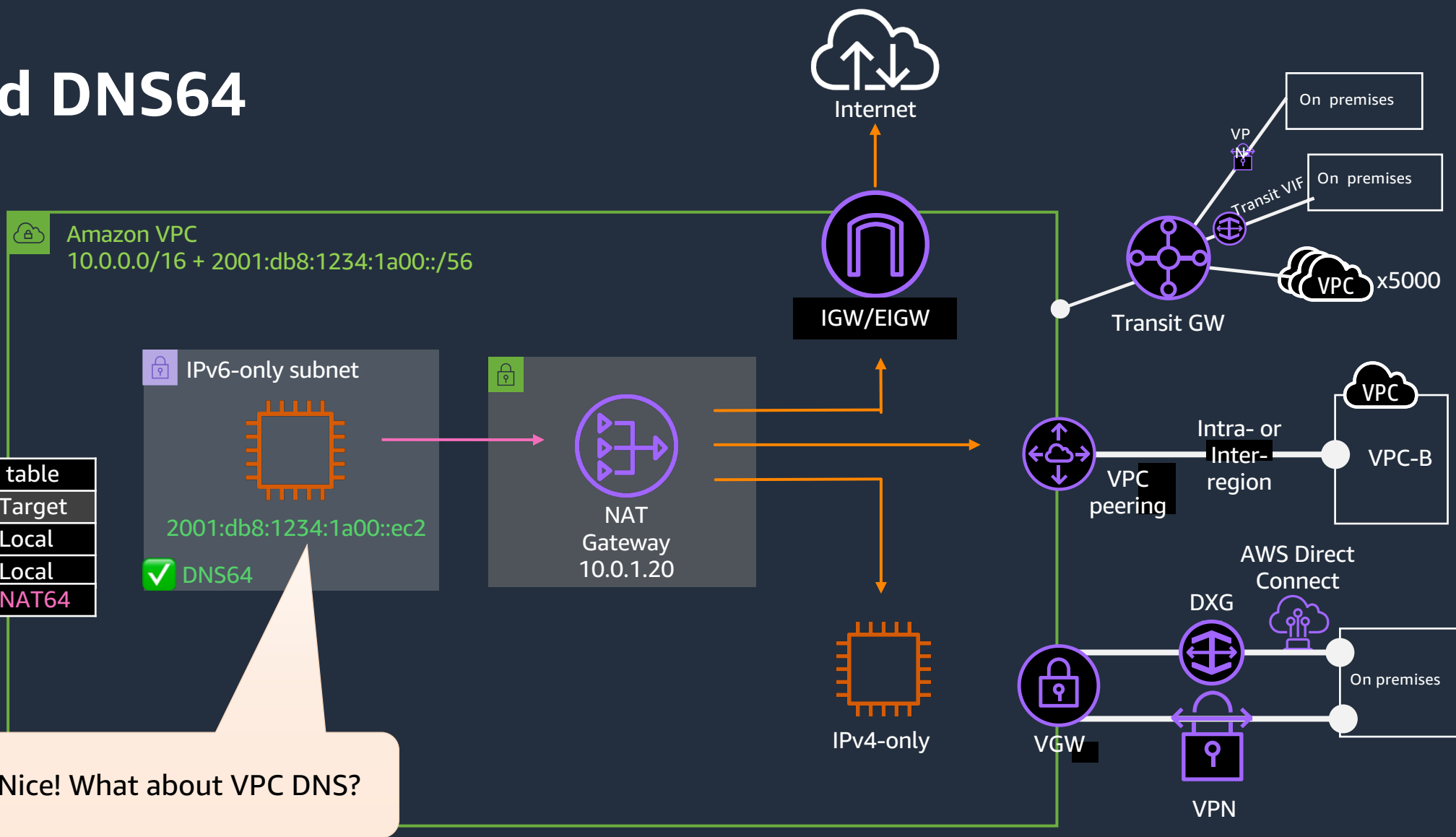


# NAT64 and DNS64

## TRAFFIC FLOWS

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

Nice! What about VPC DNS?



# IPv6

## Amazon VPC

IPv6-only subnets

---

## NAT64 and DNS64

Interoperability with IPv4 environments

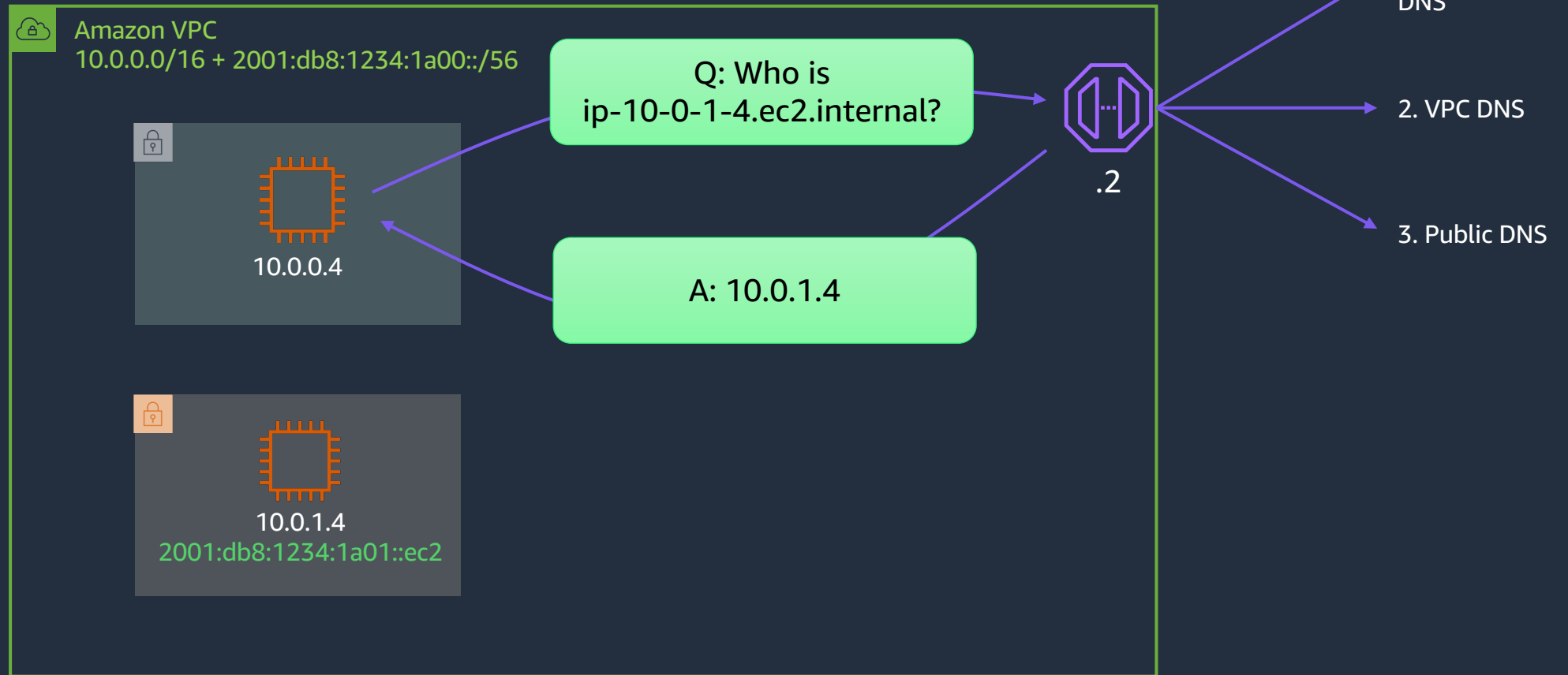
---

## Amazon EC2

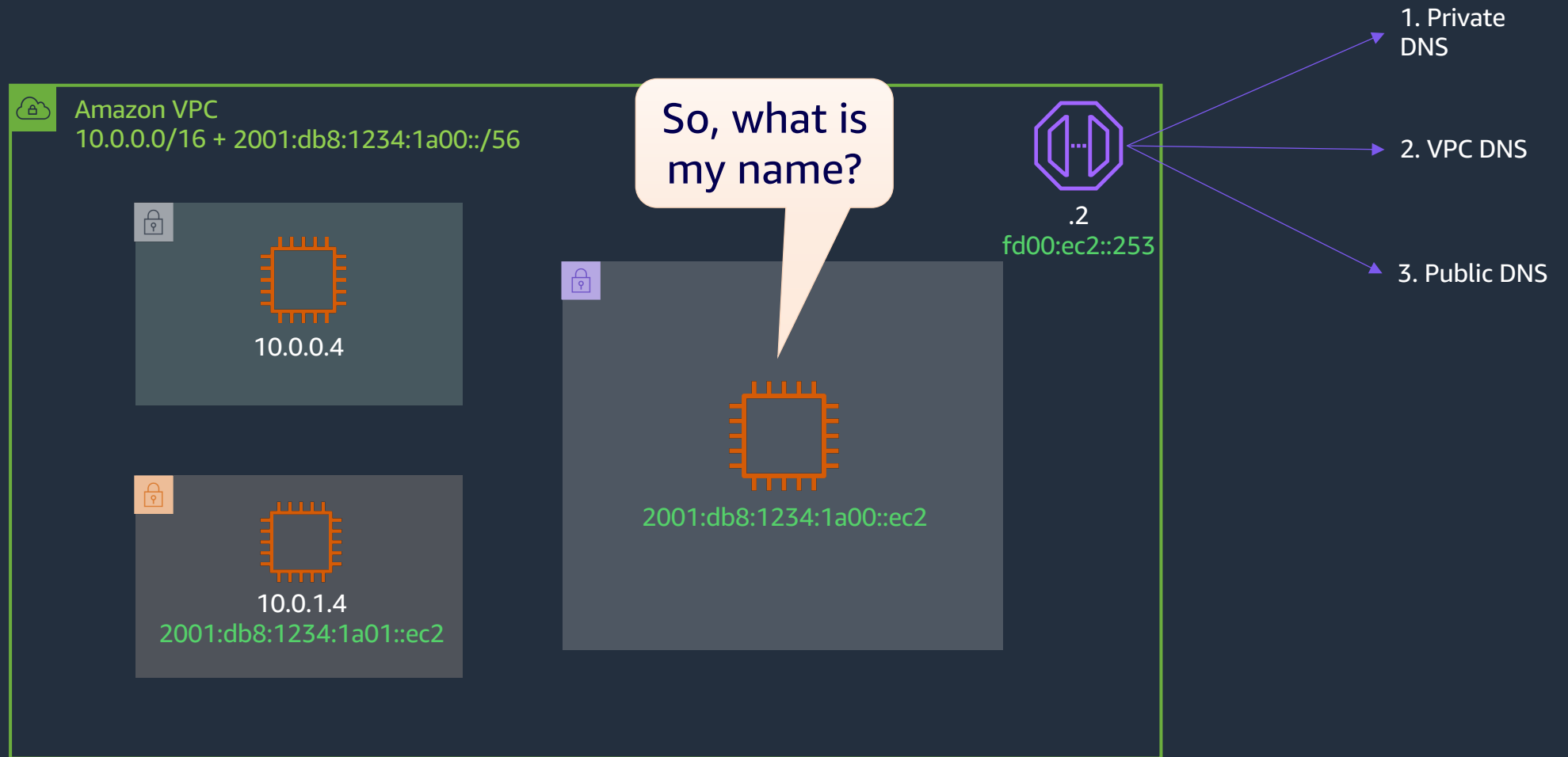
Resource-based instance naming

# 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

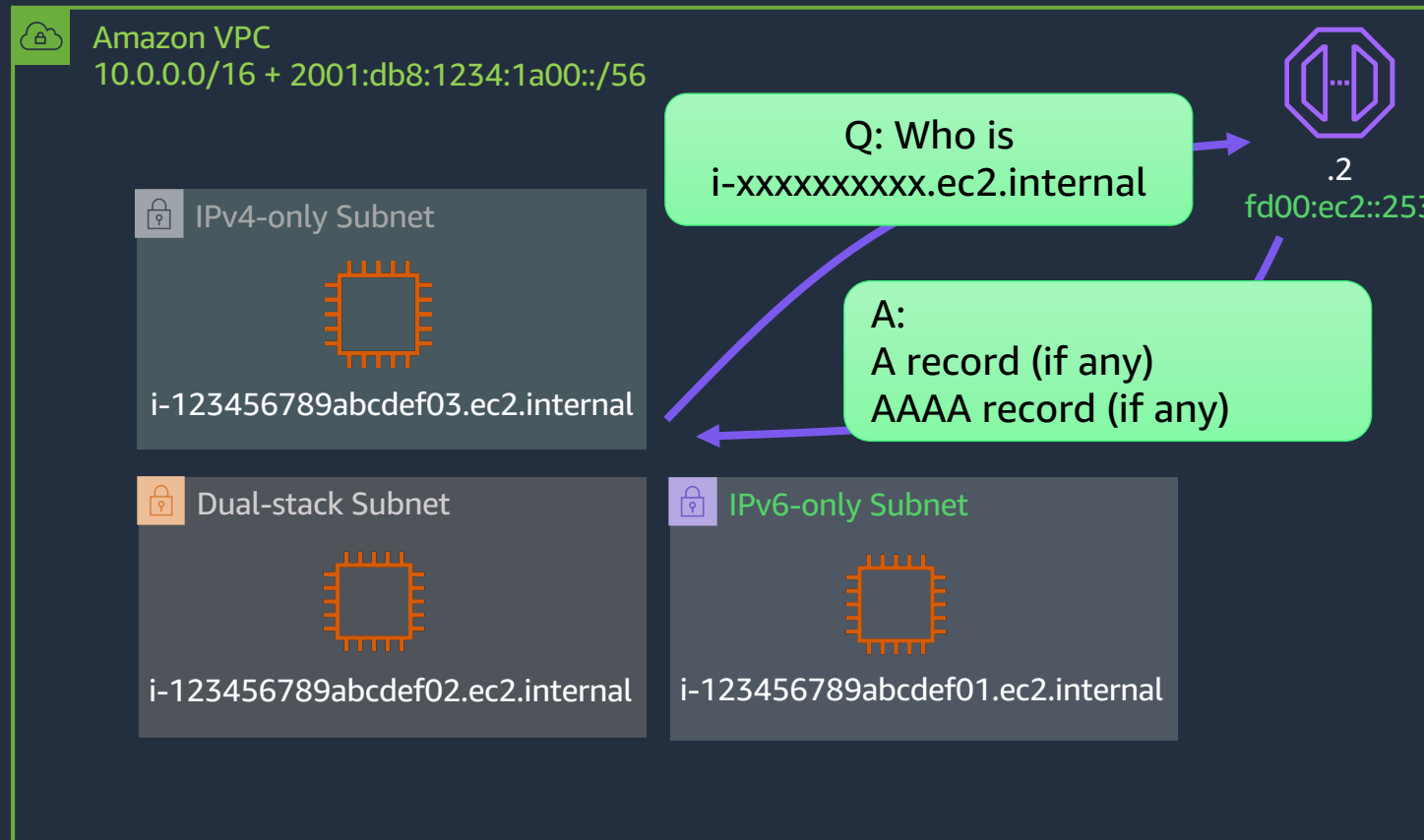
Amazon VPC  
10.0.0.0/16 + 2001:db8::/32

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



Nice!



# IPv6

## Amazon VPC

IPv6-only subnets

---

## NAT64 and DNS64

Interoperability with IPv4 environments

---

## Amazon EC2

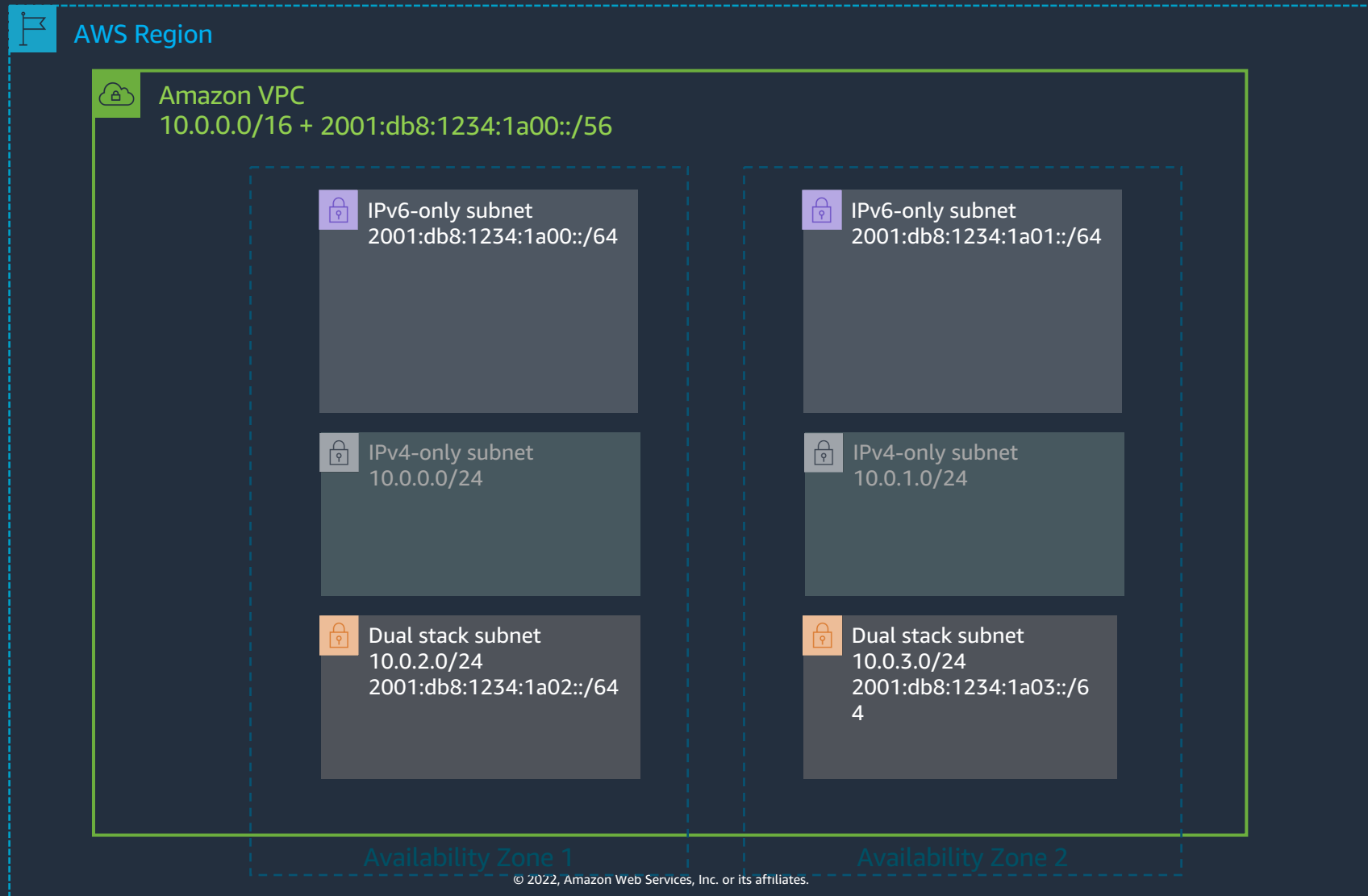
Resource-based instance naming

---

## Elastic Load Balancing

Full Dual-stack IPv6 support

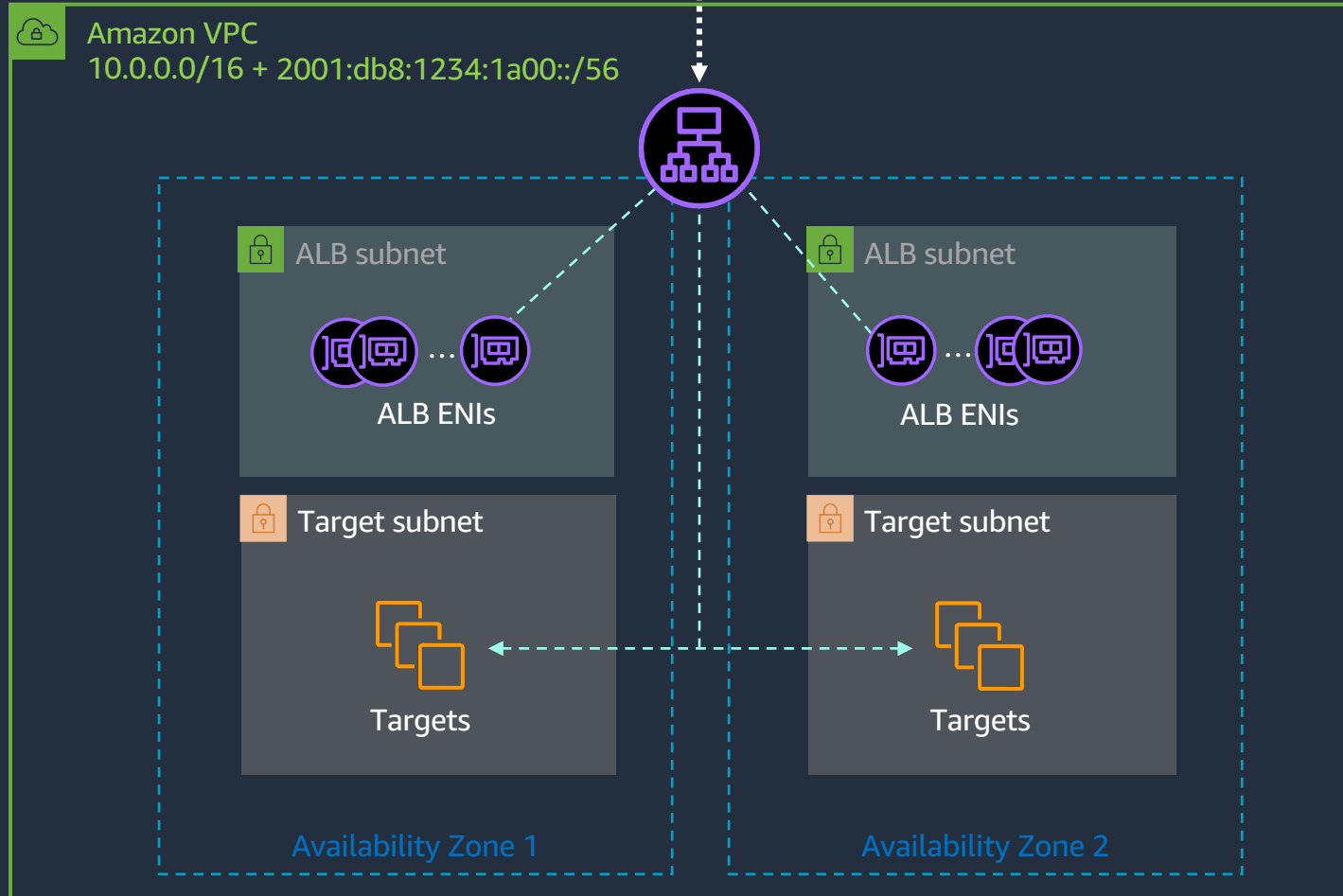
# Starting from the dual-stack VPC



# Application Load Balancer (ALB)

# Application Load Balancer: Deployment

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

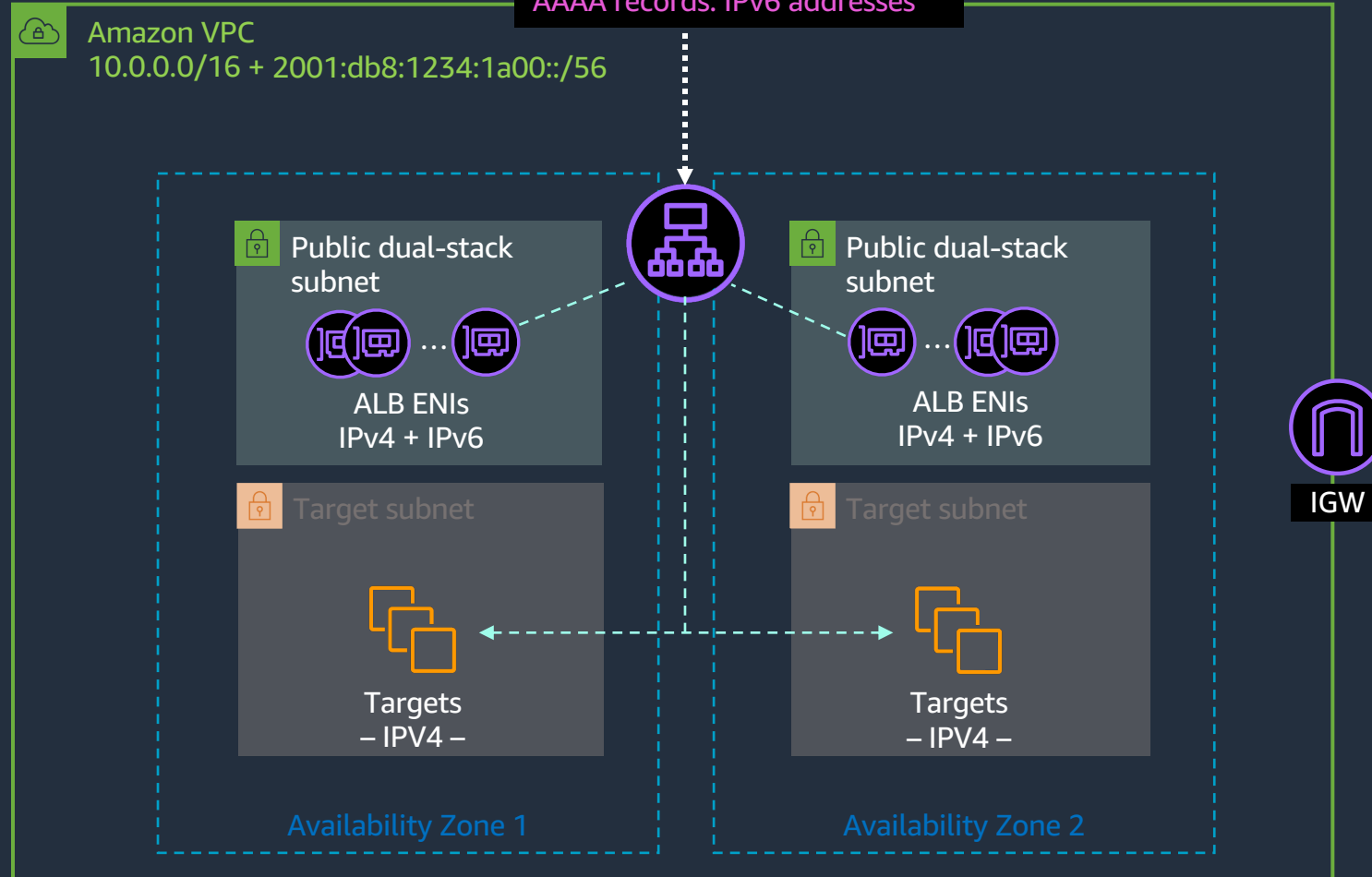


# Application Load Balancer: Dual-stack support

INTERNET-FACING DUAL-STACK

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

A records: Elastic IPv4  
AAAA records: IPv6 addresses

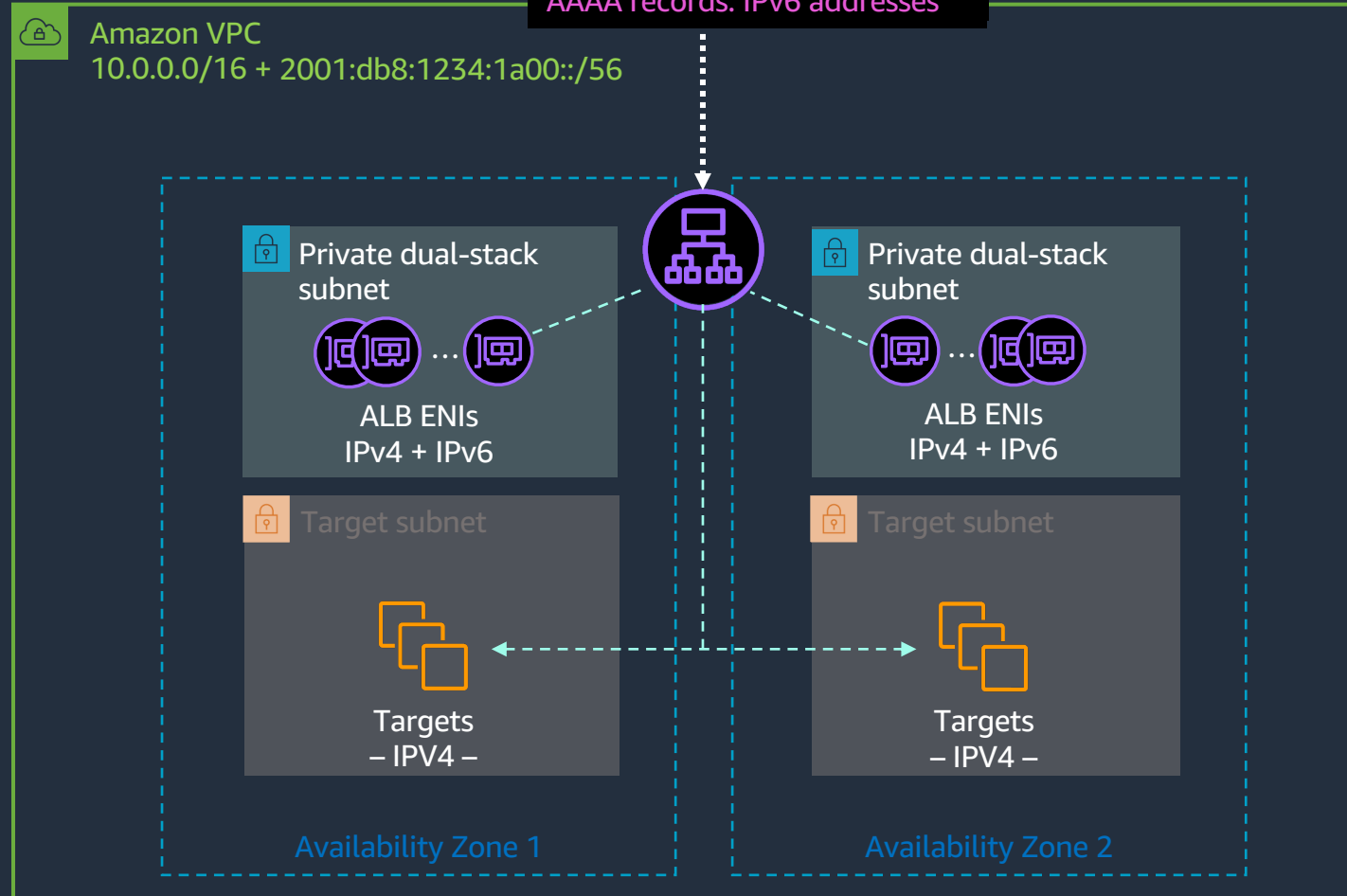


# Application Load Balancer: Dual-stack support

INTERNAL DUAL STACK

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

A records: Elastic IPv4  
AAAA records: IPv6 addresses

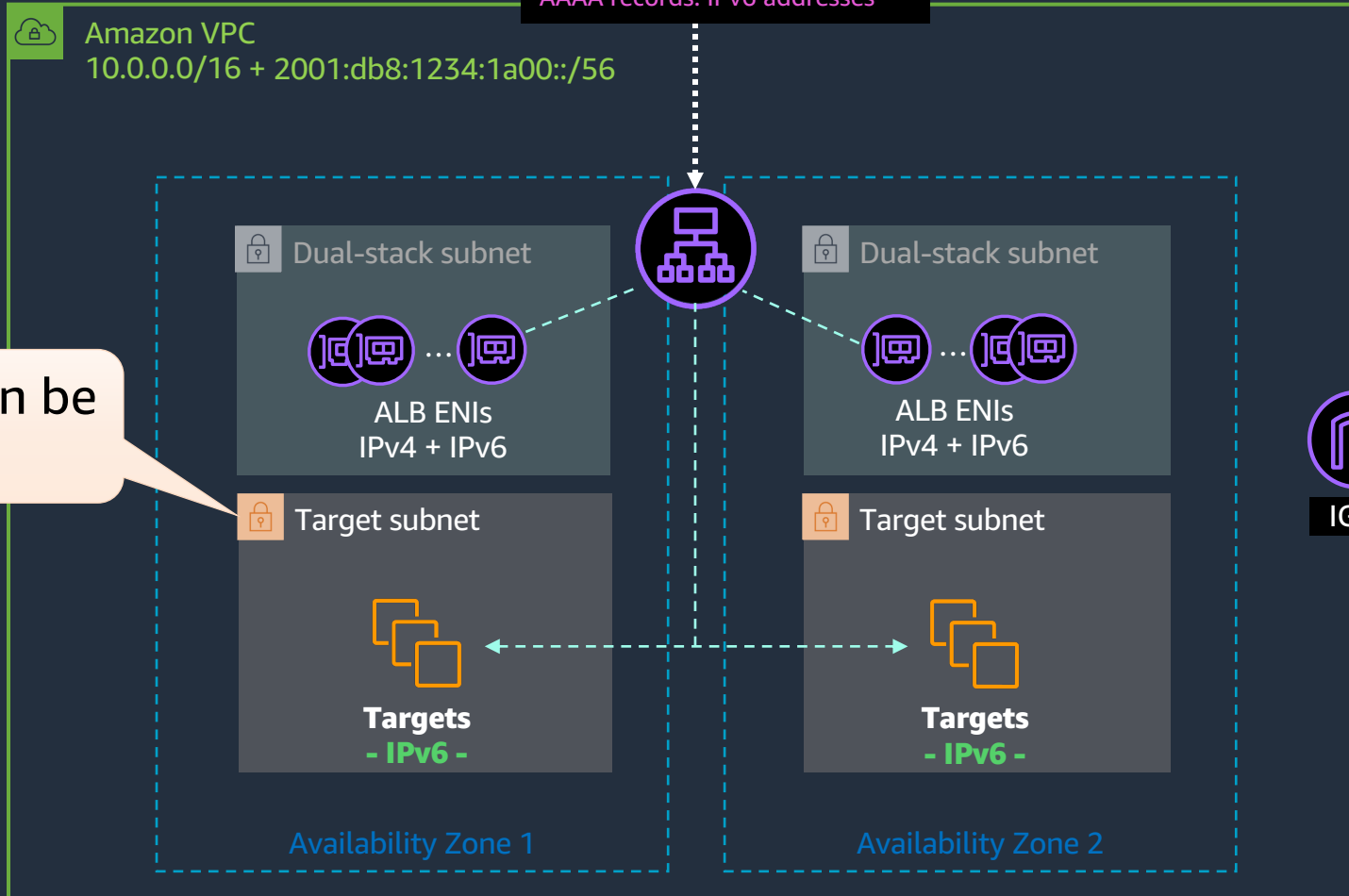


# Application Load Balancer: End-to-end IPv6

## IPV6 TARGETS

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

A records: Elastic IPv4 addresses  
AAAA records: IPv6 addresses



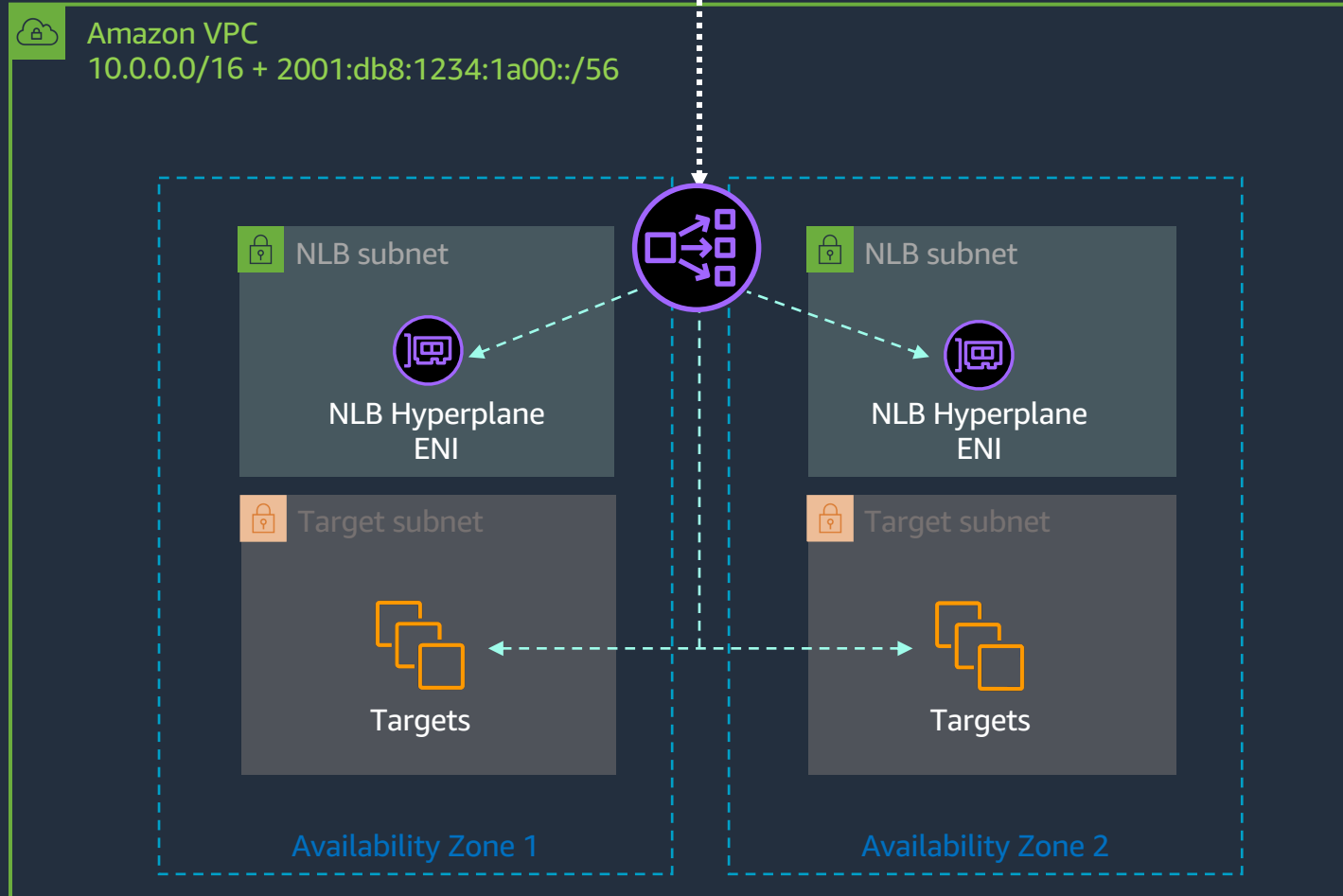
Target subnets can be IPv6-only



# Network Load Balancer (NLB)

# Network Load Balancer: Deployment

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

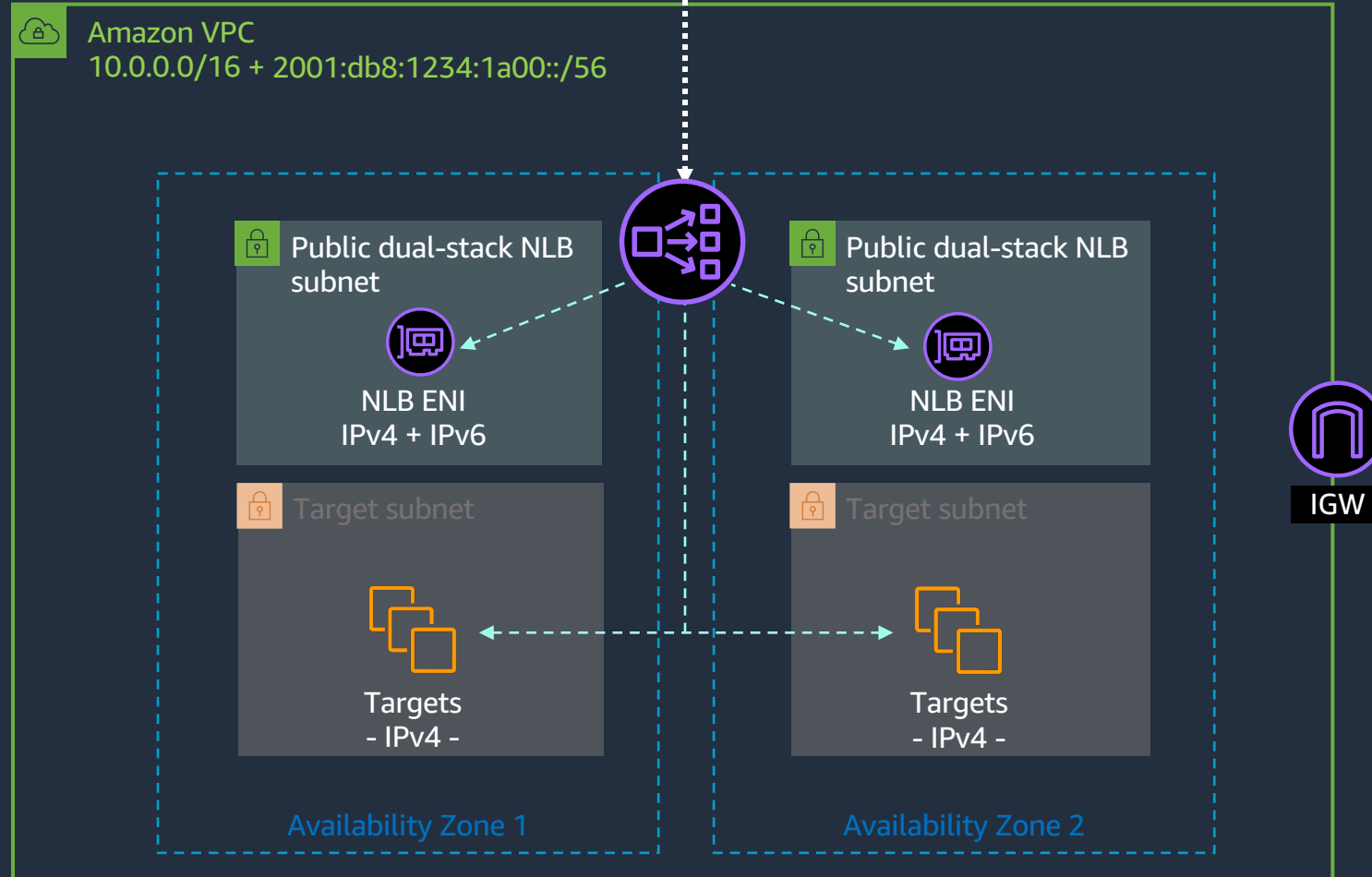


# Network Load Balancer: Dual-stack support

INTERNET-FACING DUAL STACK

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

A records: Elastic IPv4 addresses  
AAAA records: IPv6 addresses

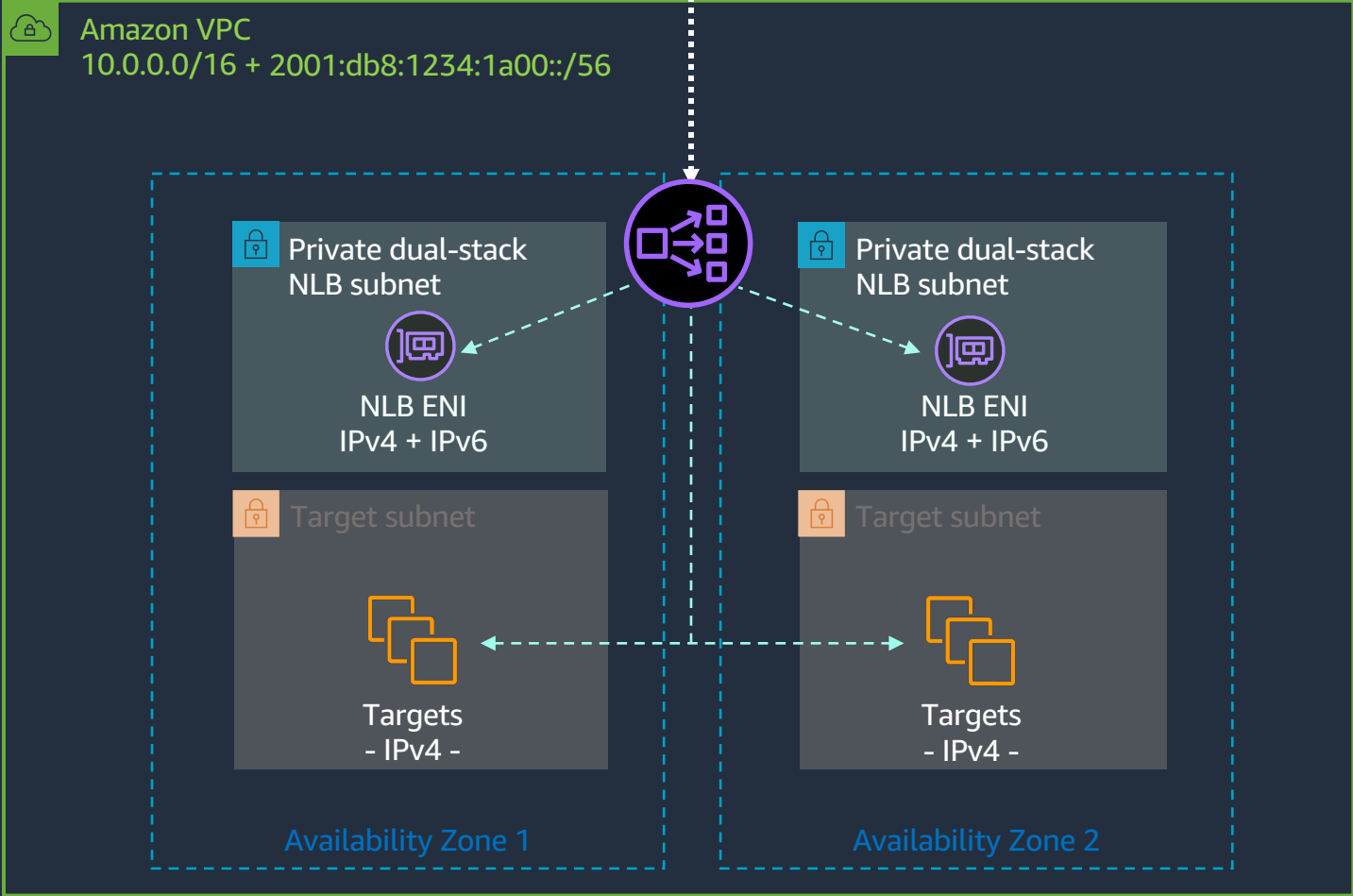


# Network Load Balancer: Dual-stack support

INTERNAL DUAL STACK

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

A records: Private IPv4 addresses  
AAAA records: IPv6 addresses

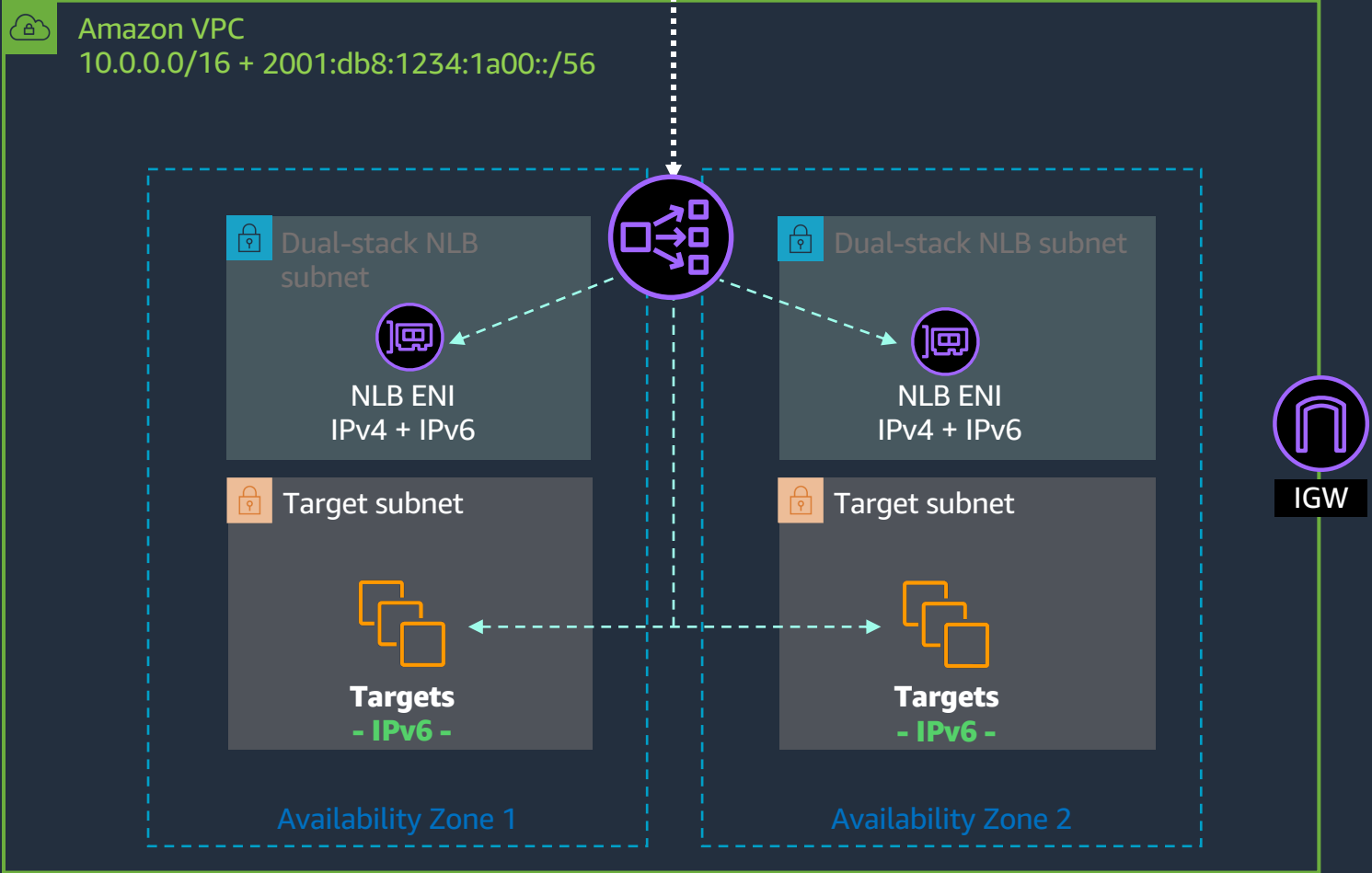


# Network Load Balancer: End-to-end IPv6

IPV6 TARGETS

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

A records: Elastic/Private IPv4  
AAAA records: IPv6 addresses



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



# IPv6

## **Amazon VPC**

IPv6-only subnets

---

## **NAT64 and DNS64**

Interoperability with IPv4 environments

---

## **Amazon EC2**

Resource-based instance naming

---

## **Elastic Load Balancing**

Full dual-stack IPv6 support

Amazon VPC IP  
Address Management

# IPAM

Range	Mask	Available?	User	Description
10.0.1.0	/24	N	Bob	Database
10.0.2.0	/24	N	Cynthia	Kafka
10.0.3.0	/24	N	Steve	Kafka
10.0.4.0	/24	N	Steve	App 321
10.0.5.0	/24	N	Steve	App 321
10.0.6.0	/24	N	Raj	Transit VPC
10.0.7.0	/24	N	Sheryle	Tape backup
10.0.8.0	/24	Y		
10.0.9.0	/24	Y		
10.0.10.0	/24	N	Raj	SDWAN deployment
10.0.11.0	/24	N	Sherlye	Tape backup
10.0.12.0	/24	N	Steve	On-premises connectivity
10.0.13.0	/24	N	Bob	VPN Backup
10.0.14.0	/24	N	Cynthia	VPC Test
10.0.15.0	/24	Y		
10.0.16.0	/24	N	Steve	Dev Environment
10.0.17.0	/24	N	Steve	Tape backup
10.0.18.0	/24	N	Raj	VPN Backup
10.0.19.0	/24	N	Sheryle	App 501
10.0.20.0	/24	Y		
10.0.21.0	/24	Y		
10.0.22.0	/24	Y		

# What's wrong with this picture?

X

Manual updates of  
single spreadsheet

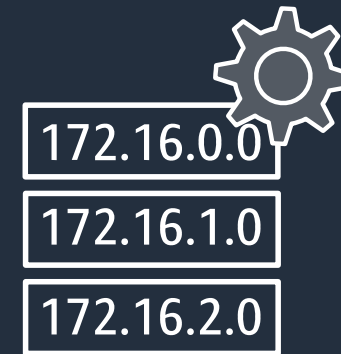
X

Limited visibility into  
allocation and usage

X

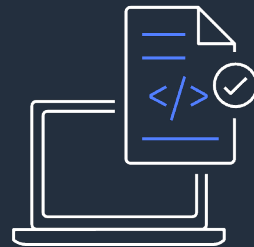
Limited ability to  
manage IP allocations  
at scale

# Introducing Amazon VPC IP Address Manager IPAM



## Automate IP Assignments

Across regions and accounts, based on application networking and security needs



## Monitor across network

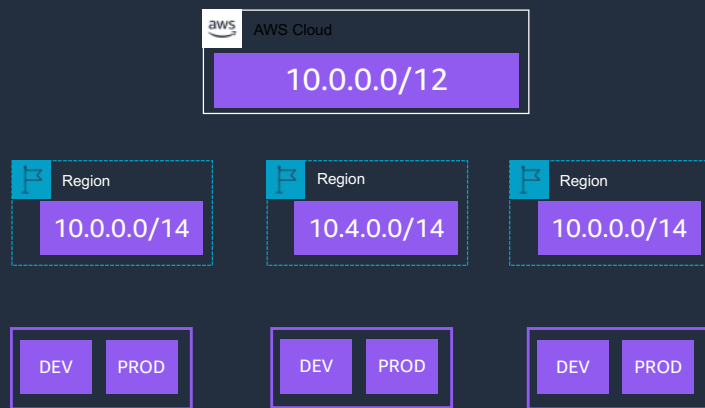
Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends



## Retrospective analysis

Allowing decreased time to troubleshoot and audit

## Arrange IPs based on routing and security needs



An example of organizing IP addresses

## Set business rules for applications



### For example:

- Which account can use IPs
- Regions where IPs can be used

## Automate IP assignment



Developers use IPAM to create VPCs (no more tickets or email)

## Monitor IPs in a single dashboard



- IP utilization for capacity planning
- Alerts on overlapping CIDRs
- Retain monitoring data for up to 3 years for audits and retrospective analysis

# Works for IPv4 and IPv6

# Key IPAM components

## Scope

An IP space for a single network  
Allowing the reuse of IPs across multiple unconnected  
networks

## Pool

A pool is a collection of contiguous IP address ranges –  
helping you organize your IP addresses according to  
your routing and security needs

# Key IPAM components

## Refill policy

Your refill policy determines how IPAM automatically refills a pool, based on thresholds set by you, from another pool

Refill policy helps you to ensure a pool always has IP addresses available for allocation

## Allocation policy

An allocation policy allows you to control IP addresses allocated by IPAM from a pool

Allocation policy enables you to enforce your business rule when developers ask IPAM for IP addresses for their resources



## Amazon VPC IP Address Manager



Dashboard

Resources

IP historical insights

Pools

**IPAMs**

Scopes

Settings



## Create IPAM [Info](#)

### My name replication [Info](#)

Amazon VPC IP Address Manager needs permission to replicate data from the source account(s) into the delegated account. The delegated account will have access to resource and IP usage details from each of the source accounts and the AWS regions selected by those source accounts.

### My cool description

Allow Amazon VPC IP Address Manager to replicate data from the source account(s) into the {1} delegate account.

You must select this checkbox to continue to create an IPAM.

### IPAM settings [Info](#)

#### Name tag - optional

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

Global name

#### Description - optional

Write a brief description for the IPAM.

My IPAM



## Amazon VPC IP Address Manager



Dashboard

Resources

IP historical insights

Pools

### IPAMs

Scopes

Settings

### IPAM settings [Info](#)

#### Name tag - *optional*

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

My name

#### Description - *optional*

Write a brief description for the IPAM.

My cool description

#### Operating regions

Select regions in which the IPAM will discover resources and manage IPs.

Select region(s)



#### Two default scopes will be created

On IPAM creation, two default scopes, one private and one public, will also be created.

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.



## Amazon VPC IP Address Manager



- Dashboard
- Resources
- IP historical insights
- Pools

### IPAMs

- Scopes
- Settings

#### Description - optional

Write a brief description for the IPAM.

My cool description

#### Operating regions

Select regions in which the IPAM will discover resources and manage IPs.

Select region(s)



Select all regions

Africa (Cape Town) - af-south-1

Asia Pacific (Hong Kong) - ap-east-1

Asia Pacific (Tokyo) - ap-northeast-1

Asia Pacific (Seoul) - ap-northeast-2

Asia Pacific (Osaka) - ap-northeast-3

Asia Pacific (Mumbai) - ap-south-1

Asia Pacific (Singapore) - ap-southeast-1

Asia Pacific (Sydney) - ap-southeast-2

Canada (Central) - ca-central-1

Europe (Frankfurt) - eu-central-1

Europe (Stockholm) - eu-north-1

Europe (Milan) - eu-south-1



to be created.





## Amazon VPC IP Address Manager



Dashboard

Resources

IP historical insights

Pools

**IPAMs**

Scopes

Settings

### Description - optional

Write a brief description for the IPAM.

My cool description

### Operating regions

Select regions in which the IPAM will discover resources and manage IPs.

Select region(s)

Asia Pacific (Tokyo) - ap-northeast-1 X

Asia Pacific (Seoul) - ap-northeast-2 X

Asia Pacific (Osaka) - ap-northeast-3 X

Asia Pacific (Mumbai) - ap-south-1 X

Asia Pacific (Singapore) - ap-southeast-1 X

Asia Pacific (Sydney) - ap-southeast-2 X

Canada (Central) - ca-central-1 X

Show more chosen options (+10)



#### Two default scopes will be created

On IPAM creation, two default scopes, one private and one public, will also be create

Create IPAM



## Amazon VPC IP Address Manager



Dashboard

Resources

IP historical insights

Pools

**IPAMs**

Scopes

Settings

### Amazon VPC IP Address Manager > IPAMs



IPAMs (1)



Actions

Create IPAM

Filter IPAMs

< 1 >



IPAM ID



IPAM ARN



[ipam-067b6888cf30d08e7](#)

[arn:aws:ec2::450545058648:ipam/ipam-067b6888cf30d08e7](#)





### Amazon VPC IP Address Manager



Dashboard

Resources

IP historical insights

Pools

IPAMs

Scopes

Settings

## ipam-067b6888cf30d08e7 [Info](#)

[Edit](#) [Delete](#)

### IPAM details [Info](#)

<p>IPAM ID</p> <p> ipam-067b6888cf30d08e7</p> <p>IPAM ARN</p> <p> arn:aws:ec2::450545058648:ipam/ipam-067b6888cf30d08e7</p>	<p>Description</p> <p> My cool description</p> <p>Default public scope</p> <p> <a href="#">ipam-scope-0c3c379b1c35e7a91</a></p>	<p>Owner ID</p> <p> 450545058648</p> <p>Default private scope</p> <p> <a href="#">ipam-scope-054ccce64961a46ba</a></p>	<p>Region</p> <p> us-east-1</p> <p>Scope count</p> <p>2</p>
---	---	--	---

### Operating regions (17)

< 1 2 >

Region





## Amazon VPC IP Address Manager



Dashboard

Resources

IP historical insights

**Pools**

IPAMs

Scopes

Settings

### Amazon VPC IP Address Manager > Pools



#### Pools (0)

View the pools in an IPAM scope.



ipam-scope-054ccce64961a46ba

Actions

Create pool

Find pools



Name / Pool ID

Description



No pools  
No pools to display.



## Amazon VPC IP Address Manager



Dashboard

Resources

IP historical insights

**Pools**

IPAMs

Scopes

Settings



# Create pool in ipam-scope-054ccce64961a46ba

### Pool settings

IPAM ID

ipam-067b6888cf30d08e7 (My cool description)

Scope ID

ipam-scope-054ccce64961a46ba

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.

VPC pool

Description - *optional*

Write a brief description for the pool.

My pool for VPCs

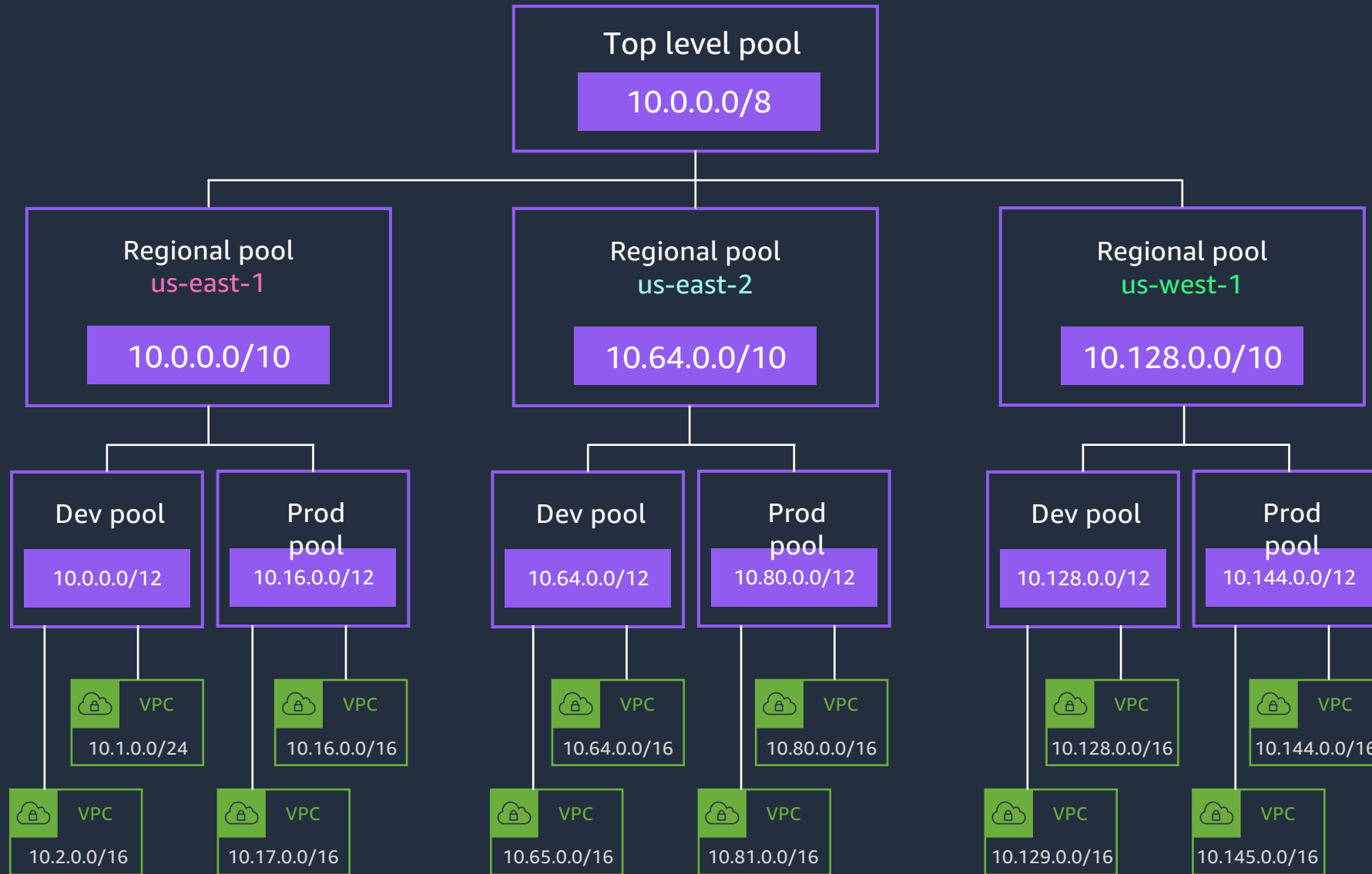
### Pool hierarchy [Info](#)

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.



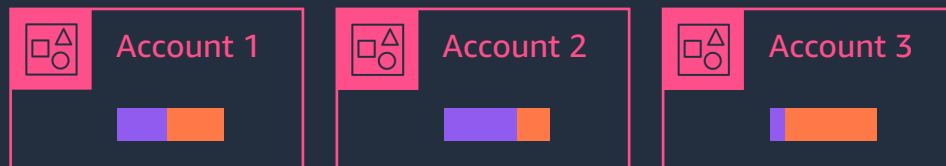
# Private scope



# Bring your own IP (BYOIP) with IPAM



## BYOIP *without* IPAM



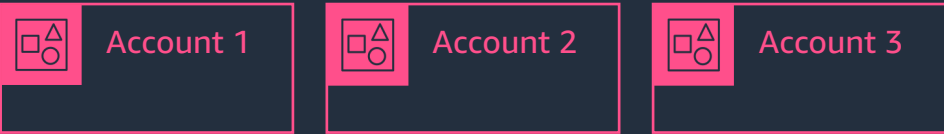
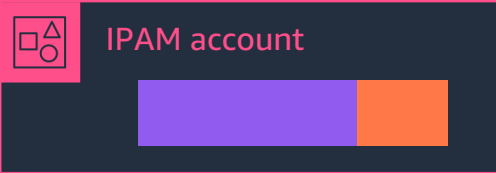
## Benefits:

- Improve IP address utilization (Org wide sharing)

# Bring your own IP (BYOIP) with IPAM



## BYOIP *with* IPAM



## Benefits:

- Improve IP address utilization (Org wide sharing)
- Migrate existing BYOIP IPs
- Simplify BYOIP onboarding to AWS
- Enable both Internet- and VPC- BYOIPv6



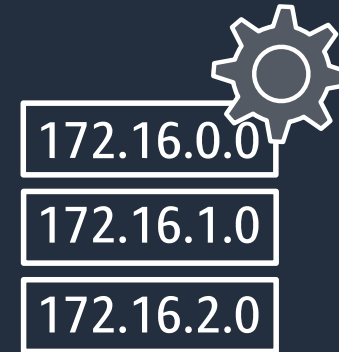
 Used IPs  
 Unused IPs

© 2022, Amazon Web Services, Inc. or its affiliates.

# Amazon VPC IP Address Manager

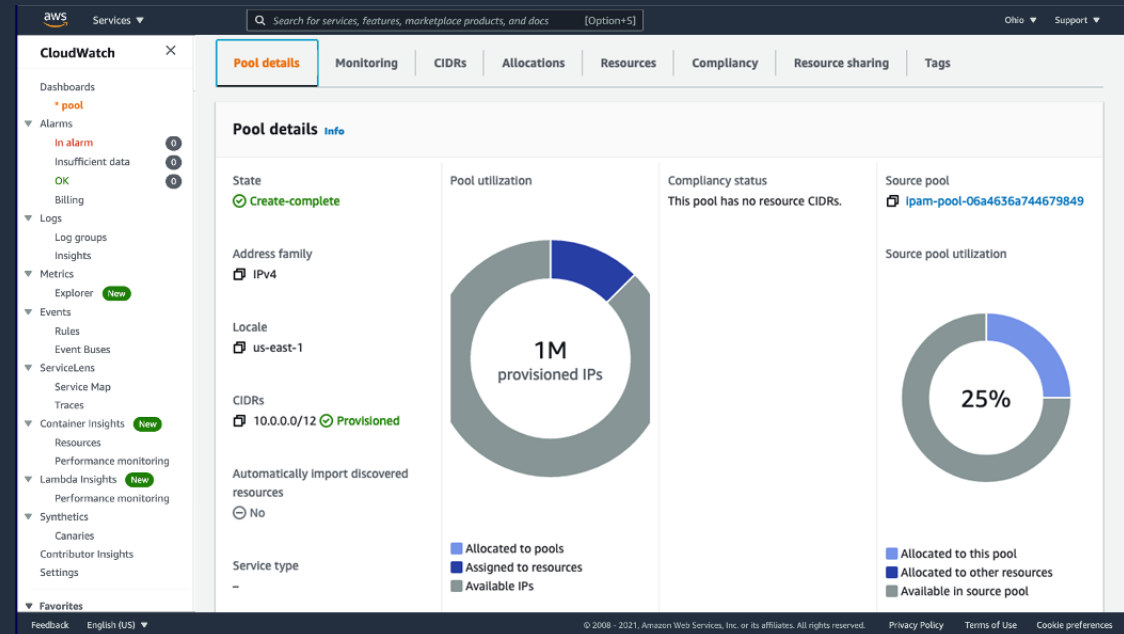
## IPAM

## Monitoring and alerts



Monitor across network

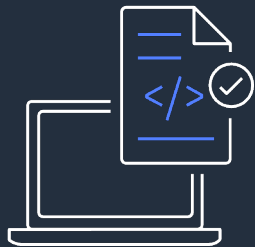
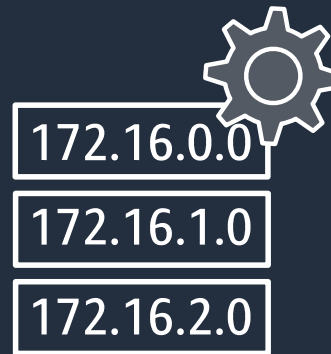
Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends



# Amazon VPC IP Address Manager

## IPAM

## Monitoring and alerts



Monitor across network

Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends



# Amazon VPC IP Address Manager

## IPAM

## Monitoring and alerts



172.16.0.0

172.16.1.0

172.16.2.0



Monitor across network

Avoid downtime with overlap detection,  
IP security policy compliance tracking,  
and utilization trends

### Your VPCs

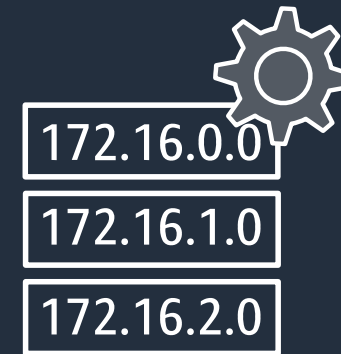
Filter VPCs

Name	VPC ID	Owner ID	Region	State	IPv4 CIDR	IPv6 CIDR	IPv4 Pool	IPv6 Pool
W1-prev-dev-vpc	vpc-6ace2601	075785353725	Us-west-1	Compliant	10.0.0.0/24		Us-west-1-dev	
W1-prev-test-vpc	vpc-6ace2602	111122223333	Us-west-1	Compliant	10.4.0.0/24		Us-west-1-dev	
W1-prev-prod-vpc	vpc-6ace2603	444455556666	Us-west-1	Compliant	Tag on allocation policy don't match		Us-west-1-dev	
E1-prev-dev-vpc	vpc-6ace2604	075785353725	Us-east-1	Non-compliant	10.1.0.0/24		Us-west-1-dev	
E1-prev-test-vpc	vpc-6ace2605	111122223333	Us-east-1	Compliant	10.5.0.0/24		Us-west-1-dev	
E1-prev-prod-vpc	vpc-6ace2606	444455556666	Us-east-1	Compliant	10.9.0.0/24		Us-west-1-dev	
Temp-test-vpc	vpc-234723fxx	777788889999	Us-east-1	Unmanaged	172.31.0.0/24			UNKNOWN

# Amazon VPC IP Address Manager

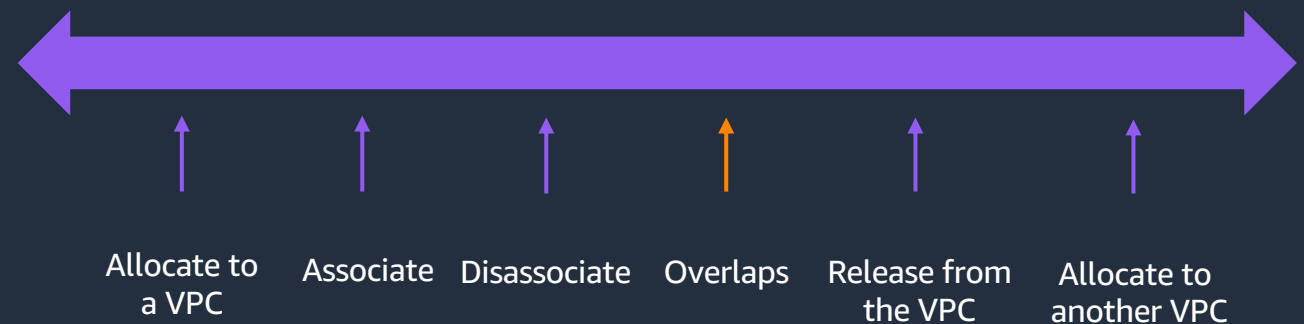
IPAM

Historical insights



## Lifecycle of a private IP

- Provides IP, start time, and end time
- Get lifecycle events associated with EIPs
- Helps troubleshoot and audit



# Amazon VPC Networking

## Amazon VPC

Enhanced routing

---

## AWS NAT Gateway

Private NAT support

---

## AWS PrivateLink

S3 interface endpoint and ALB integration

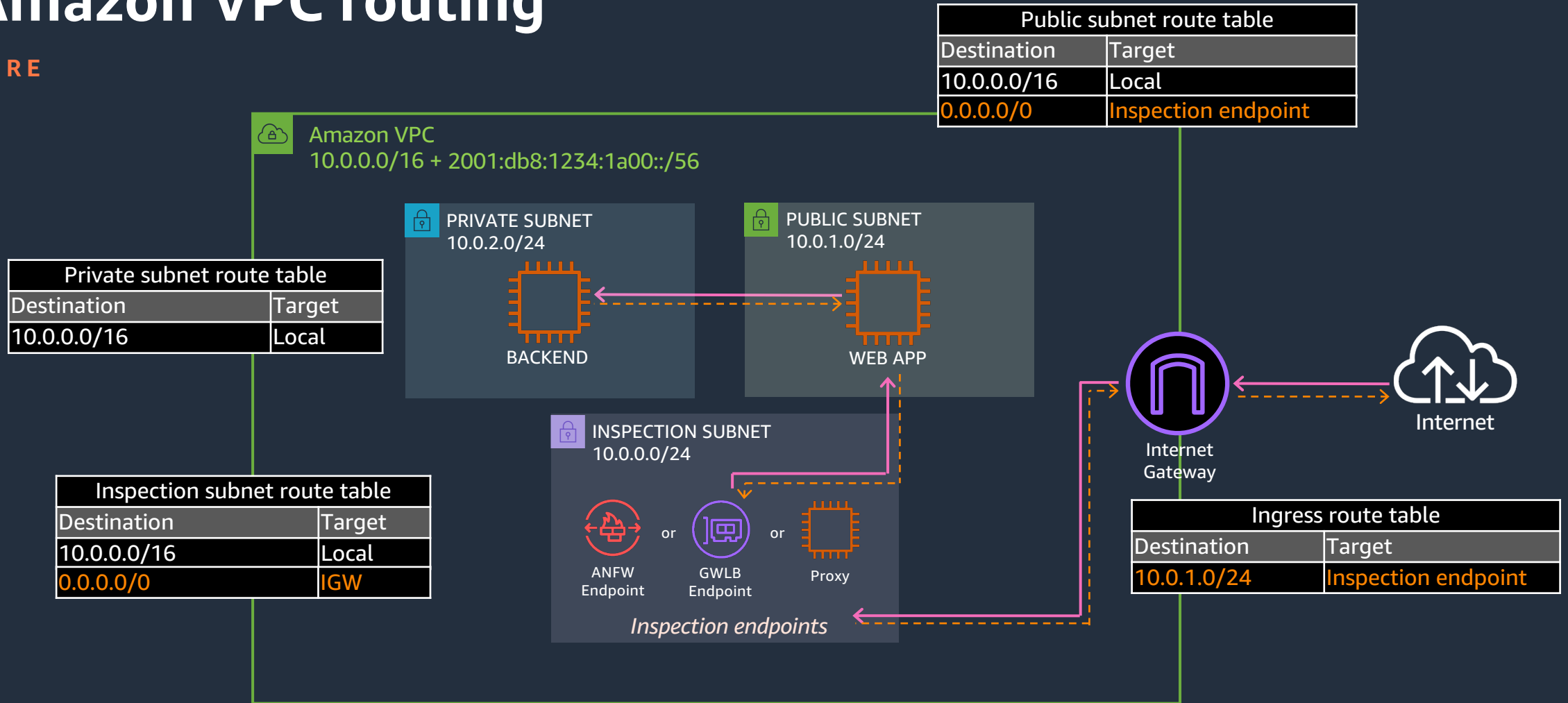
---

## AWS Transit Gateway

TGW Connect and intra-region peering

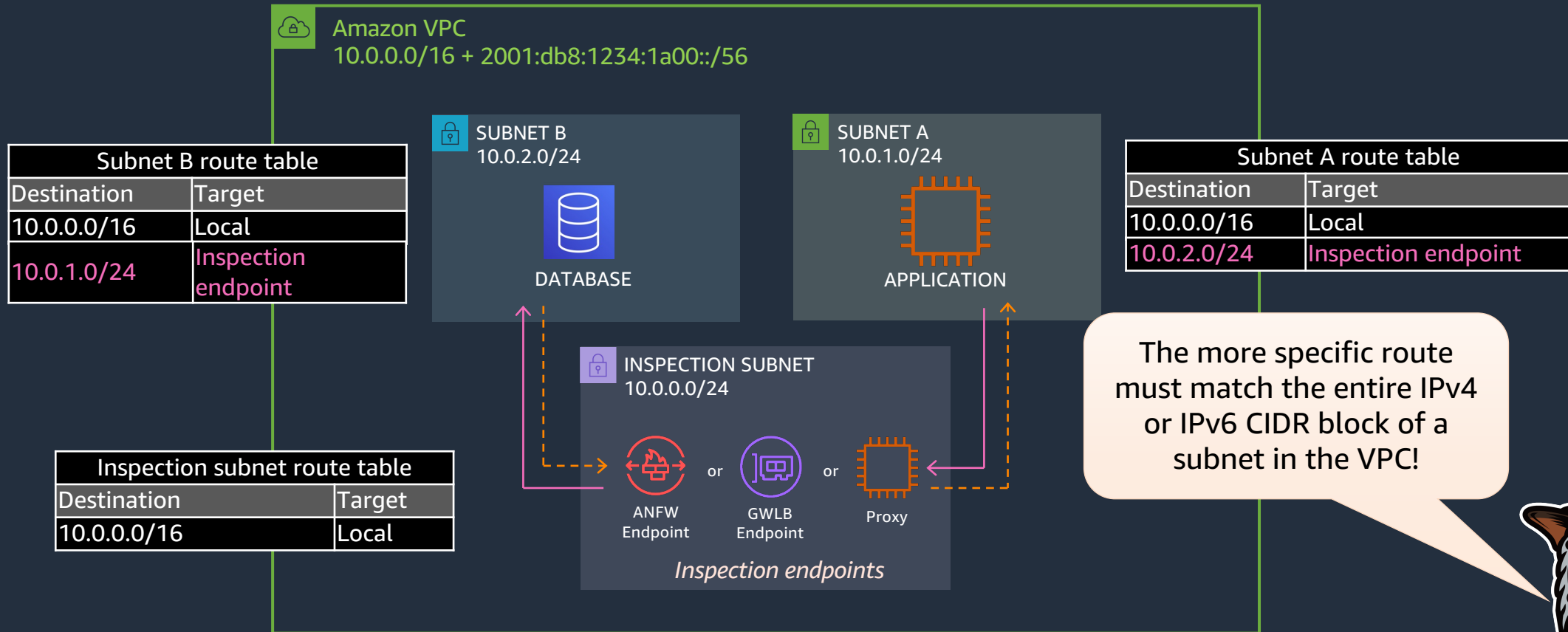
# Amazon VPC routing

BEFORE

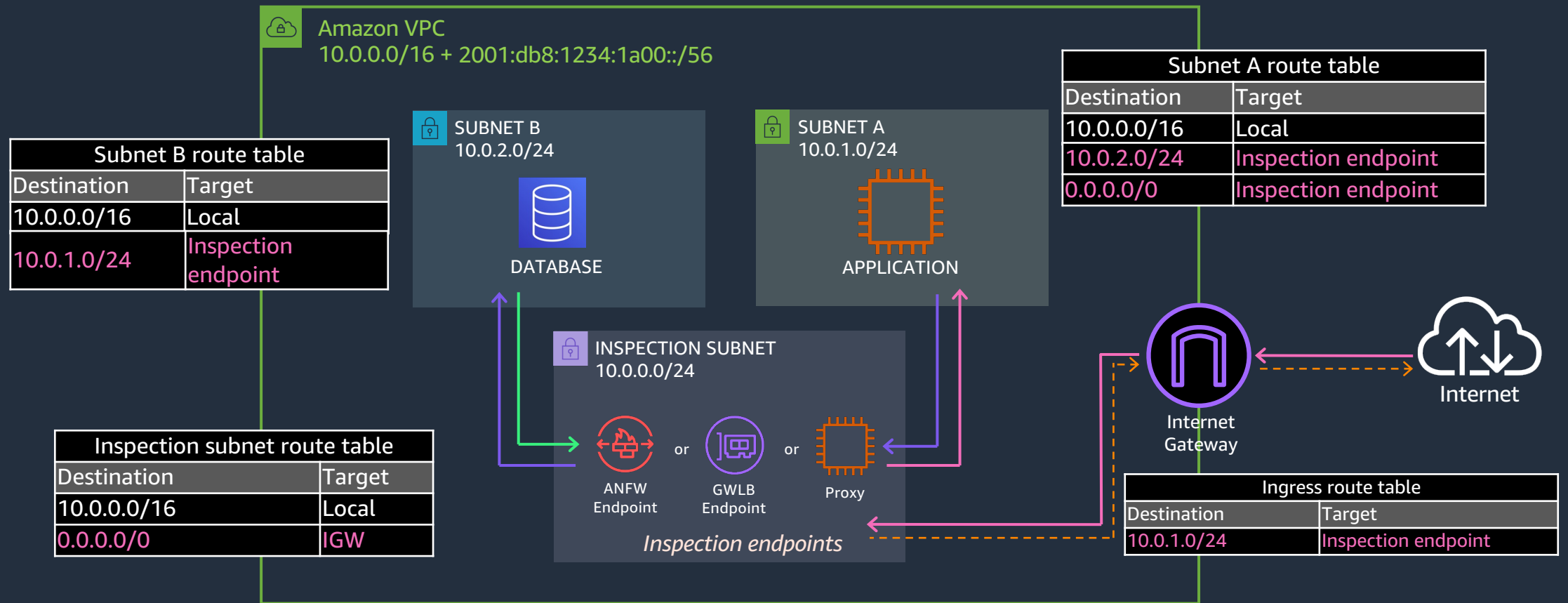


# Amazon VPC routing: Enhanced routing controls

AFTER



# Enhanced VPC routing: Multiple inspection levels



# Amazon VPC Networking

## Amazon VPC

Enhanced routing

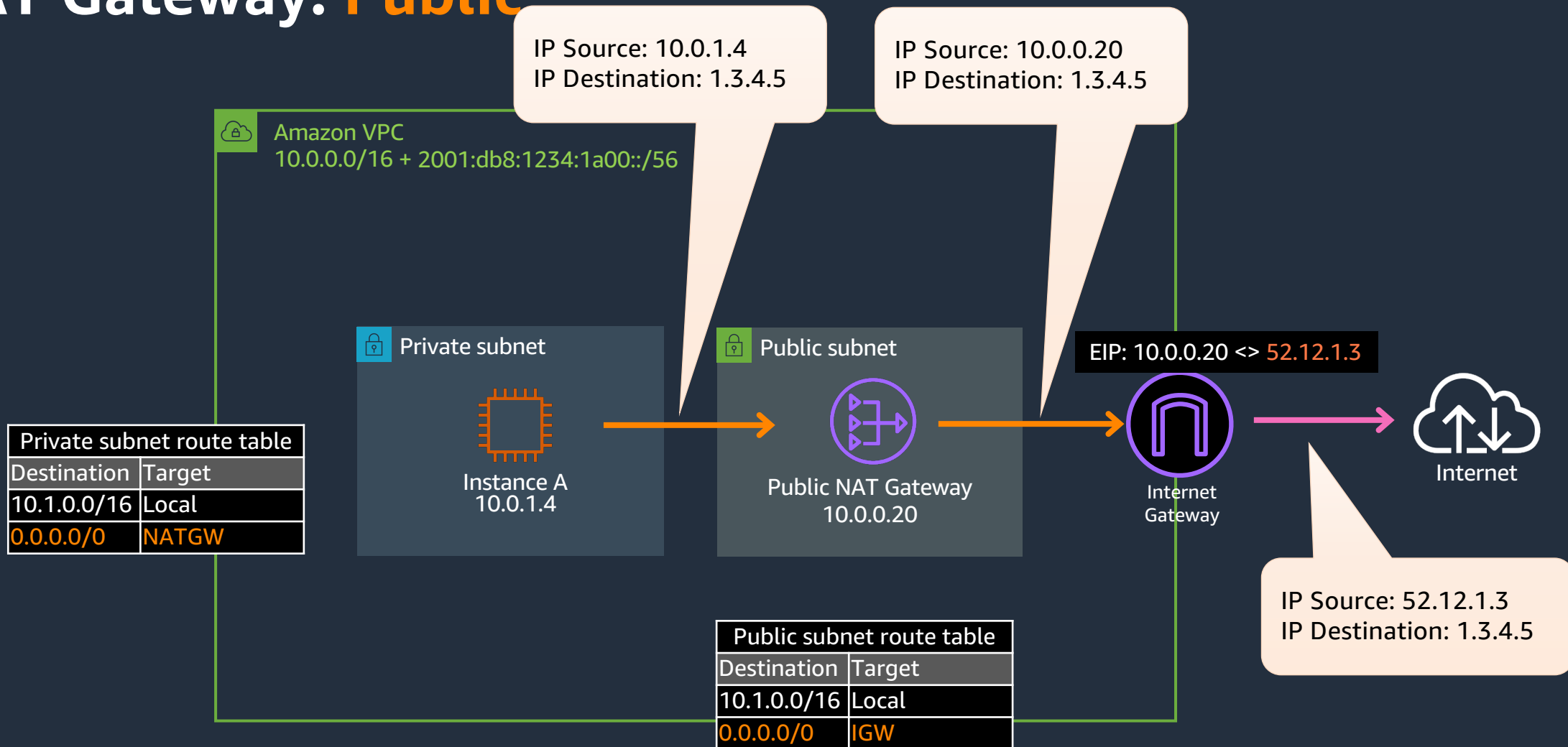
---

## AWS NAT Gateway

Private NAT support

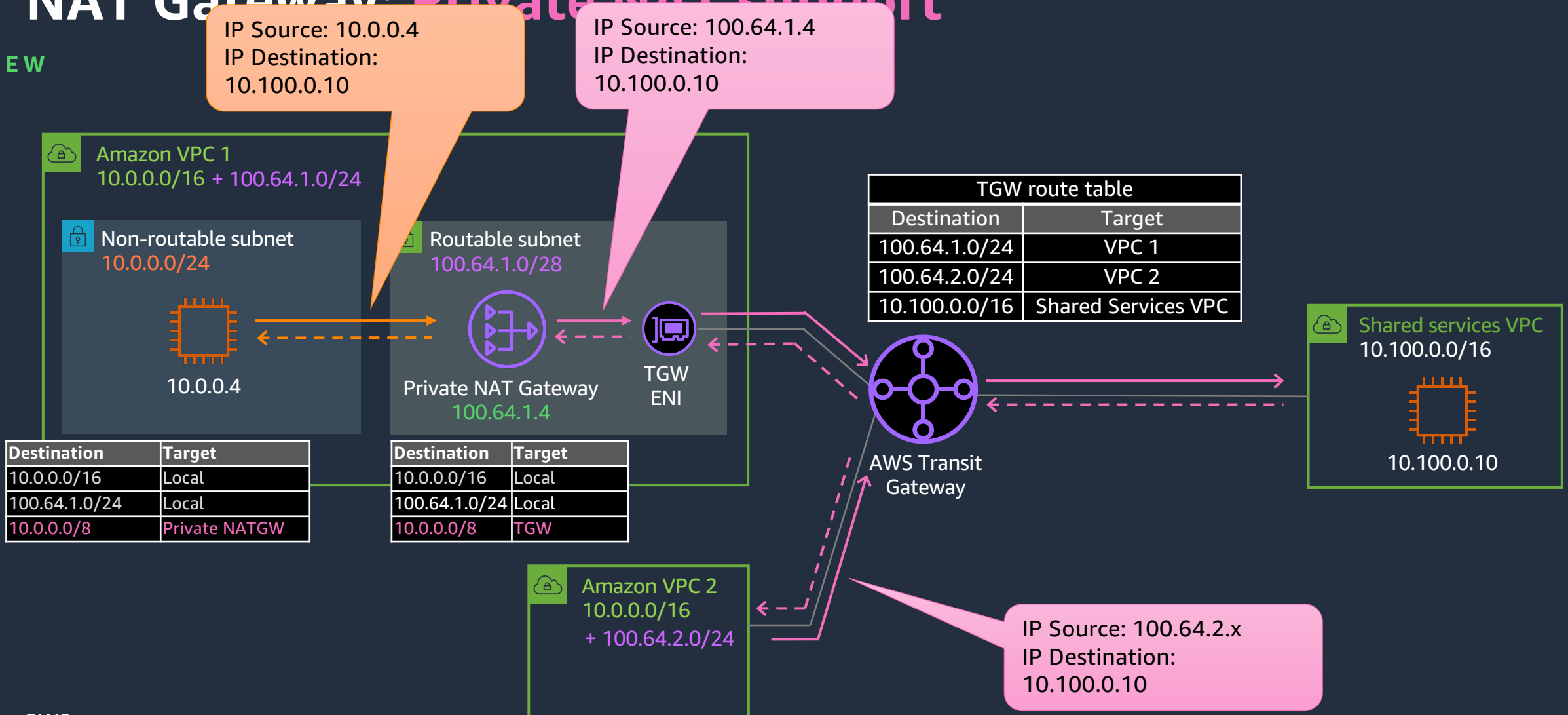
# NAT Gateway: **Public**

BEFORE



# NAT Gateway: Private NAT support

NEW





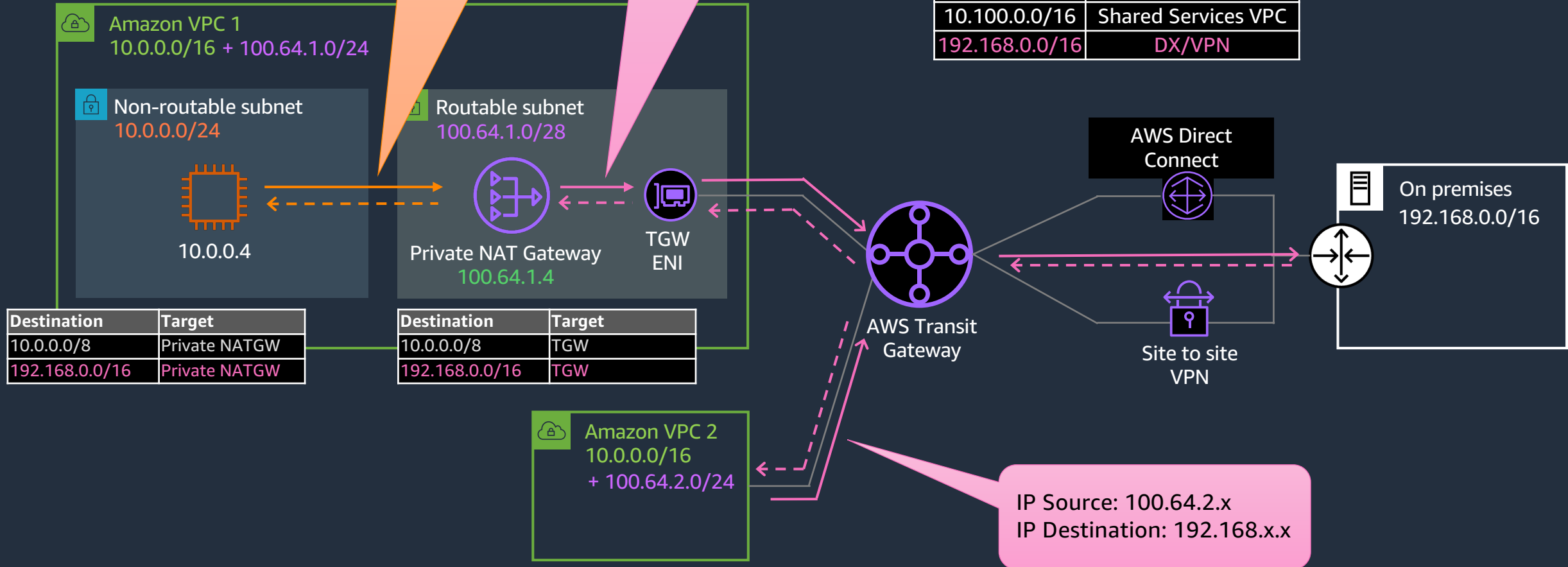
# NAT Gateway: Private NAT support

NEW

IP Source: 10.0.0.4  
IP Destination: 192.168.x.x

IP Source: 100.64.1.4  
IP Destination: 192.168.x.x

TGW route table	
Destination	Target
100.64.1.0/24	VPC 1
100.64.2.0/24	VPC 2
10.100.0.0/16	Shared Services VPC
192.168.0.0/16	DX/VPN



Destination	Target
10.0.0.0/8	Private NATGW
192.168.0.0/16	Private NATGW

Destination	Target
10.0.0.0/8	TGW
192.168.0.0/16	TGW

IP Source: 100.64.2.x  
IP Destination: 192.168.x.x



If you need **bidirectional connectivity** between **overlapping VPCs**, use **ELBs** in the routed space!



# Amazon VPC Networking

## Amazon VPC

Enhanced routing

---

## AWS NAT Gateway

Private NAT support

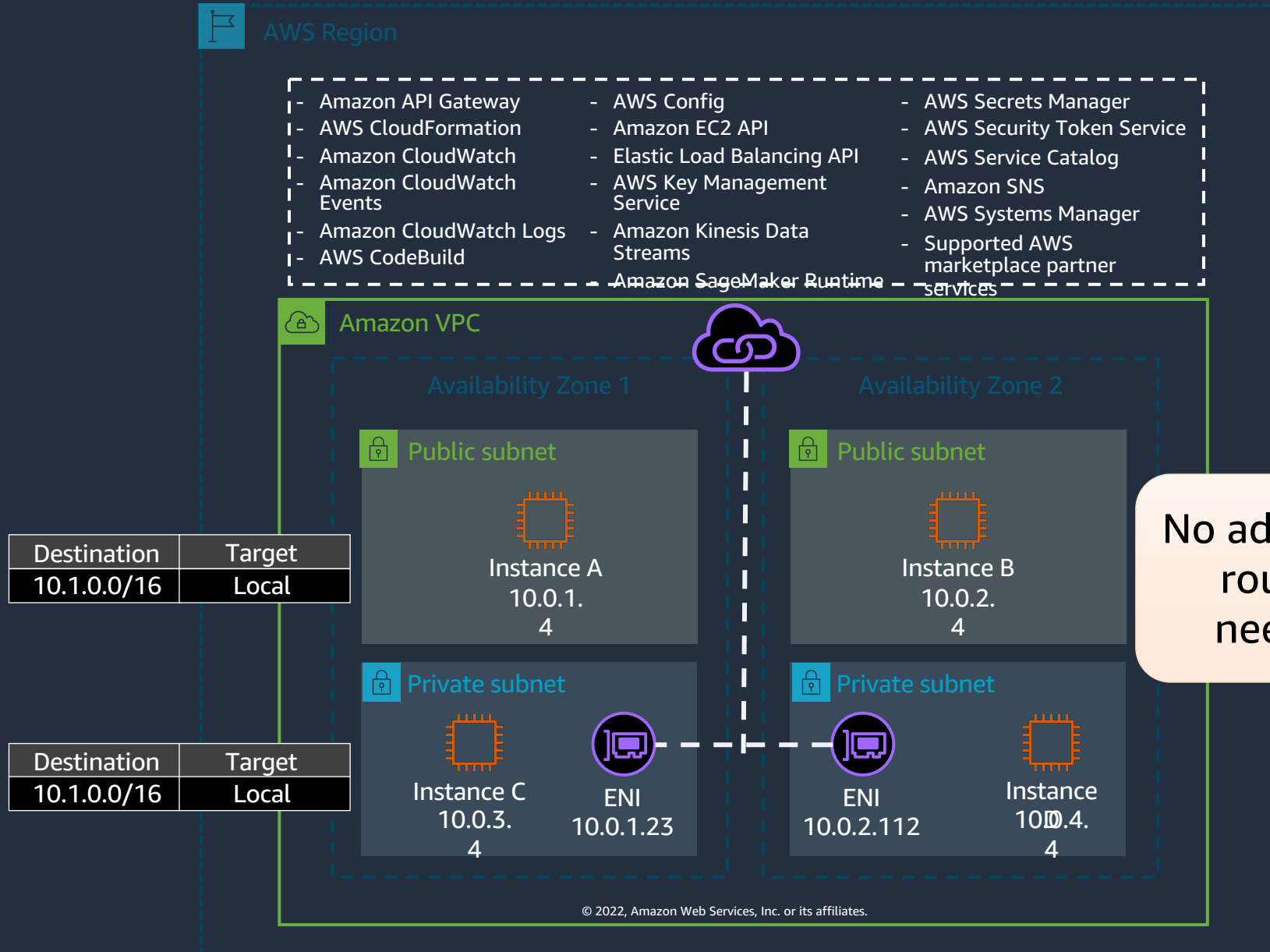
---

## AWS PrivateLink

S3 interface endpoint and ALB integration

# AWS PrivateLink: Interface endpoints

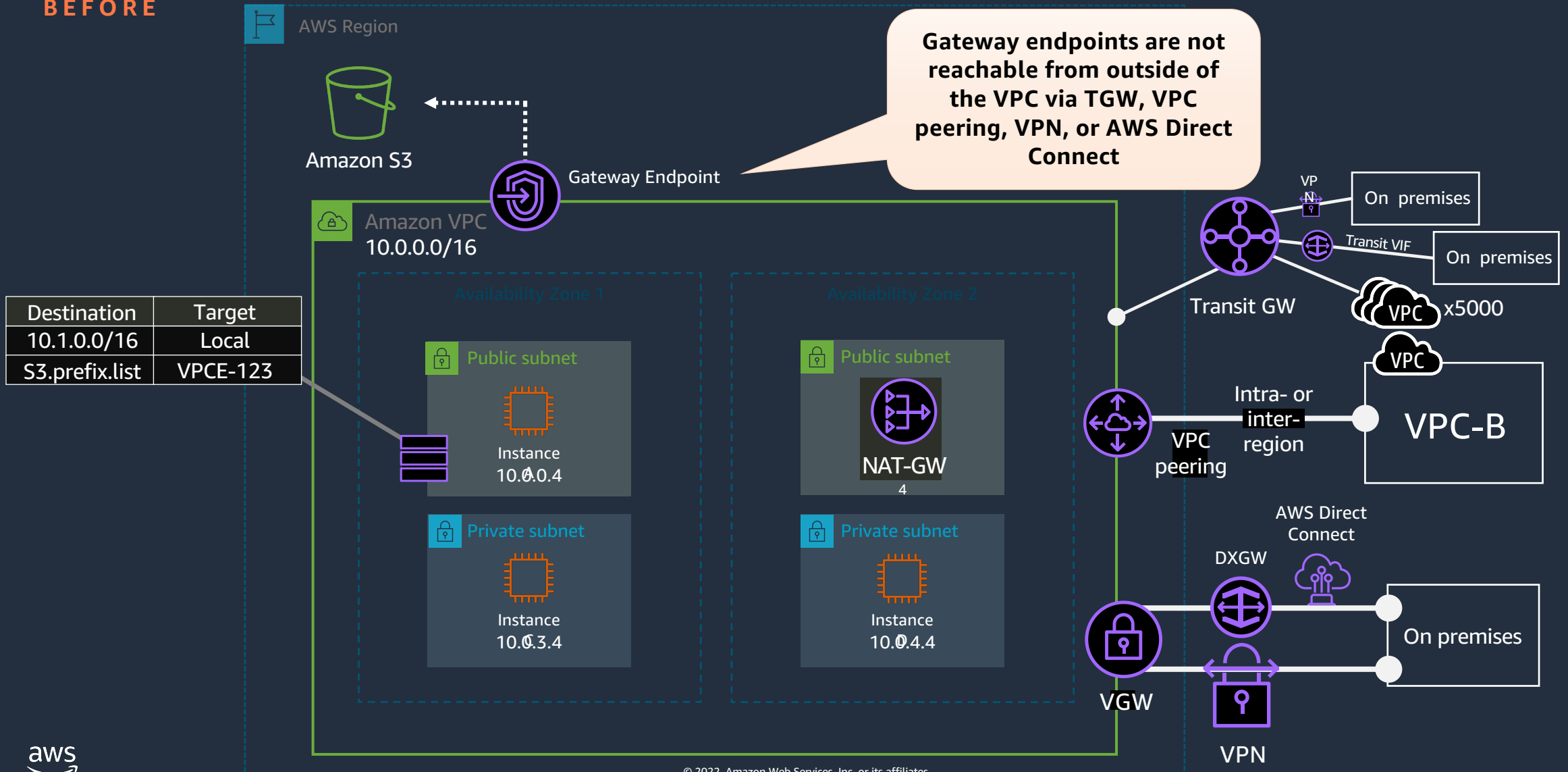
BEFORE



# AWS PrivateLink: S3 Gateway endpoints



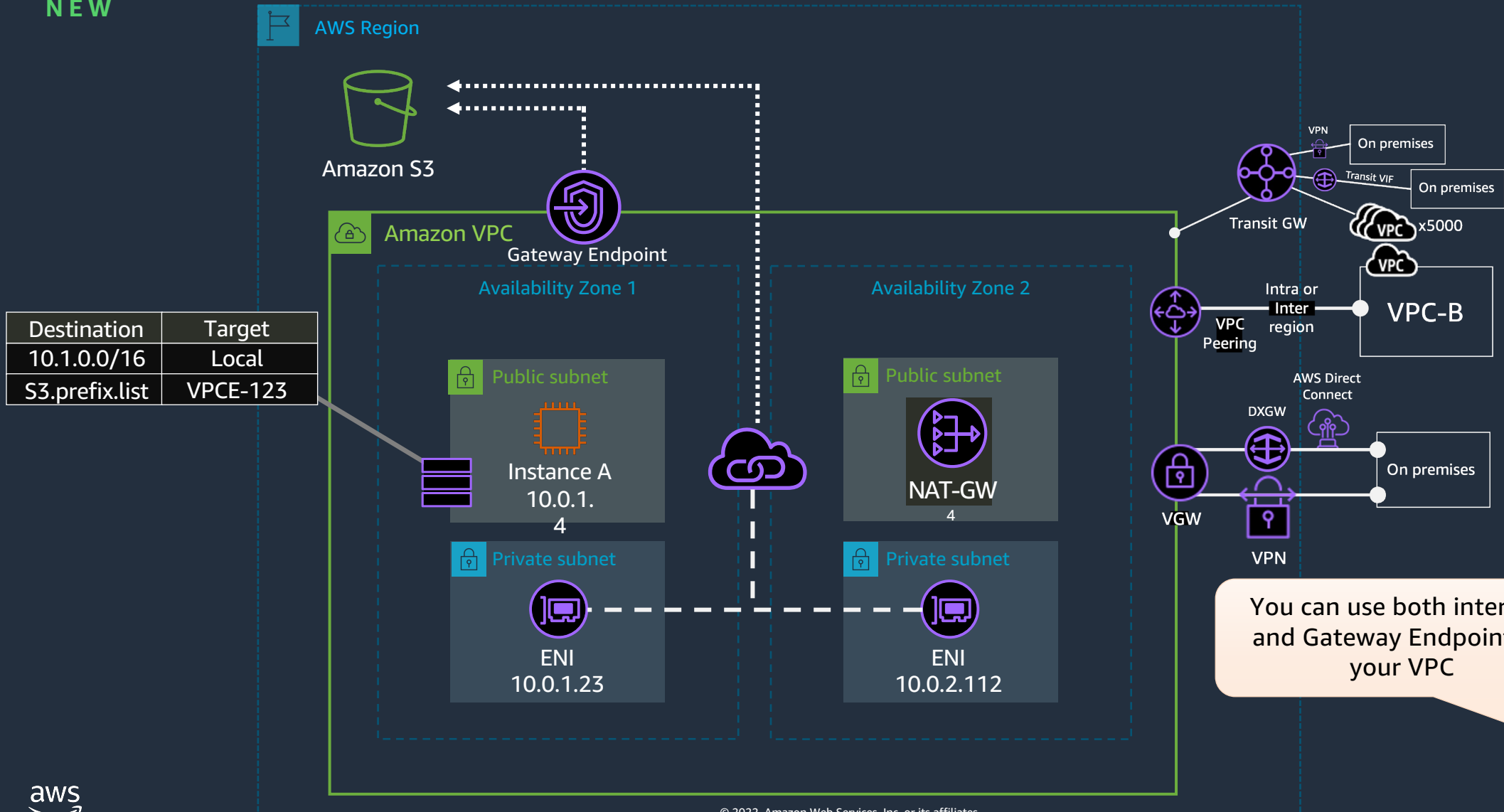
BEFORE



# S3 interface endpoints

# AWS PrivateLink: S3 interface endpoints

NEW



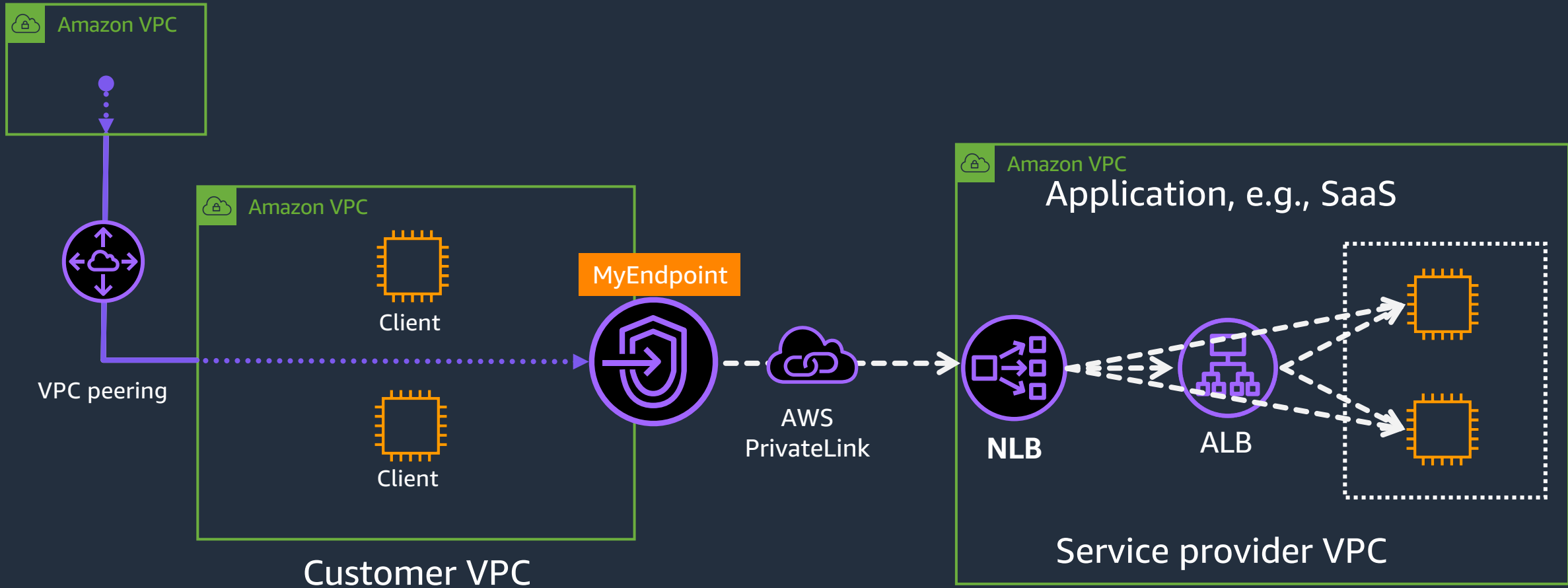
You can use both interface and Gateway Endpoints in your VPC



# ALB support through NLB

# AWS PrivateLink: ALB integration through NLB

NEW



It's recommended to **match ALB and NLB Availability Zones**, and both ALB and NLB must be in the **same account**



# Amazon VPC Networking

## Amazon VPC

Enhanced routing

---

## AWS NAT Gateway

Private NAT support

---

## AWS PrivateLink

S3 interface endpoint and ALB integration

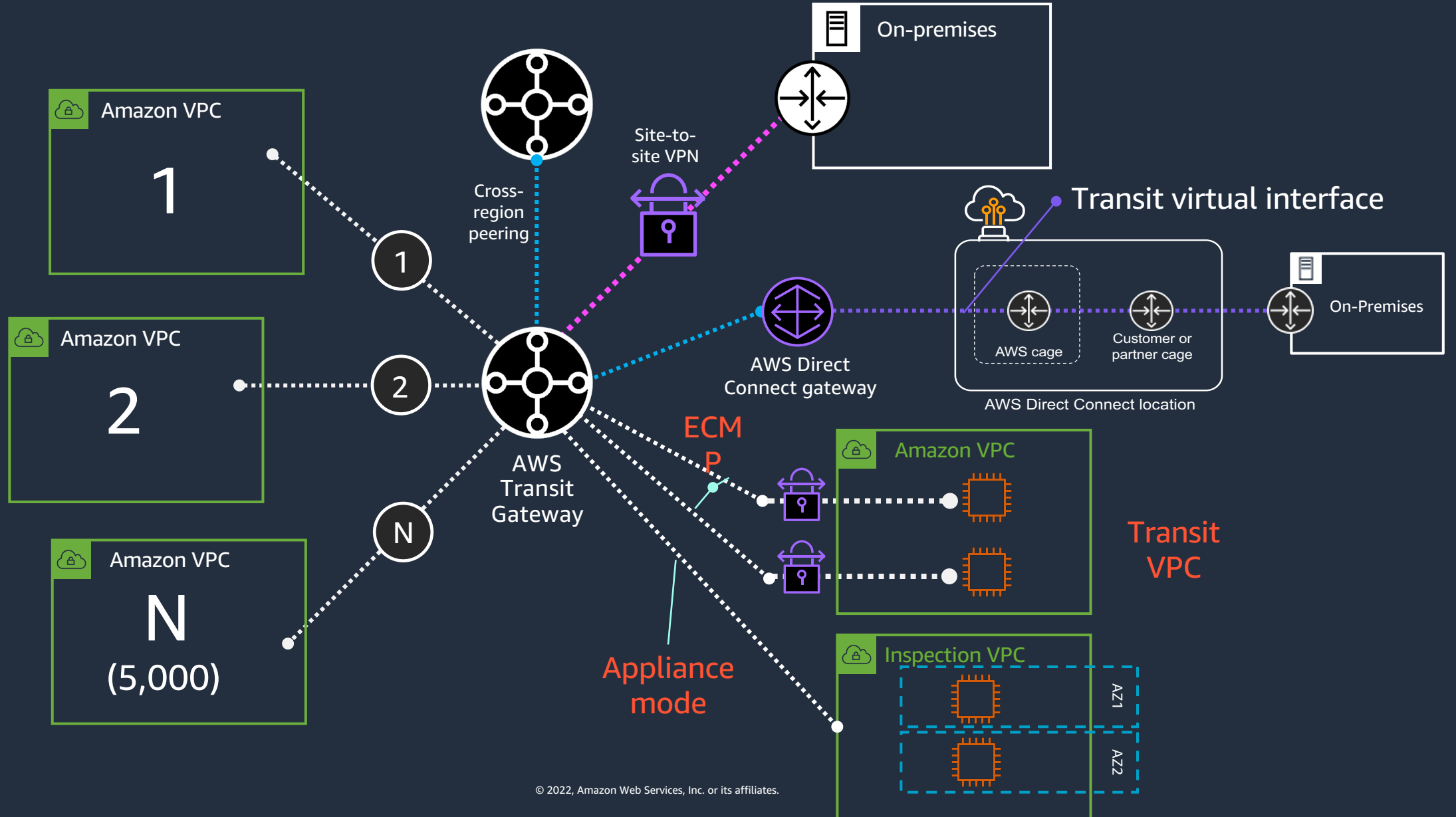
---

## AWS Transit Gateway

TGW Connect and intra-region peering

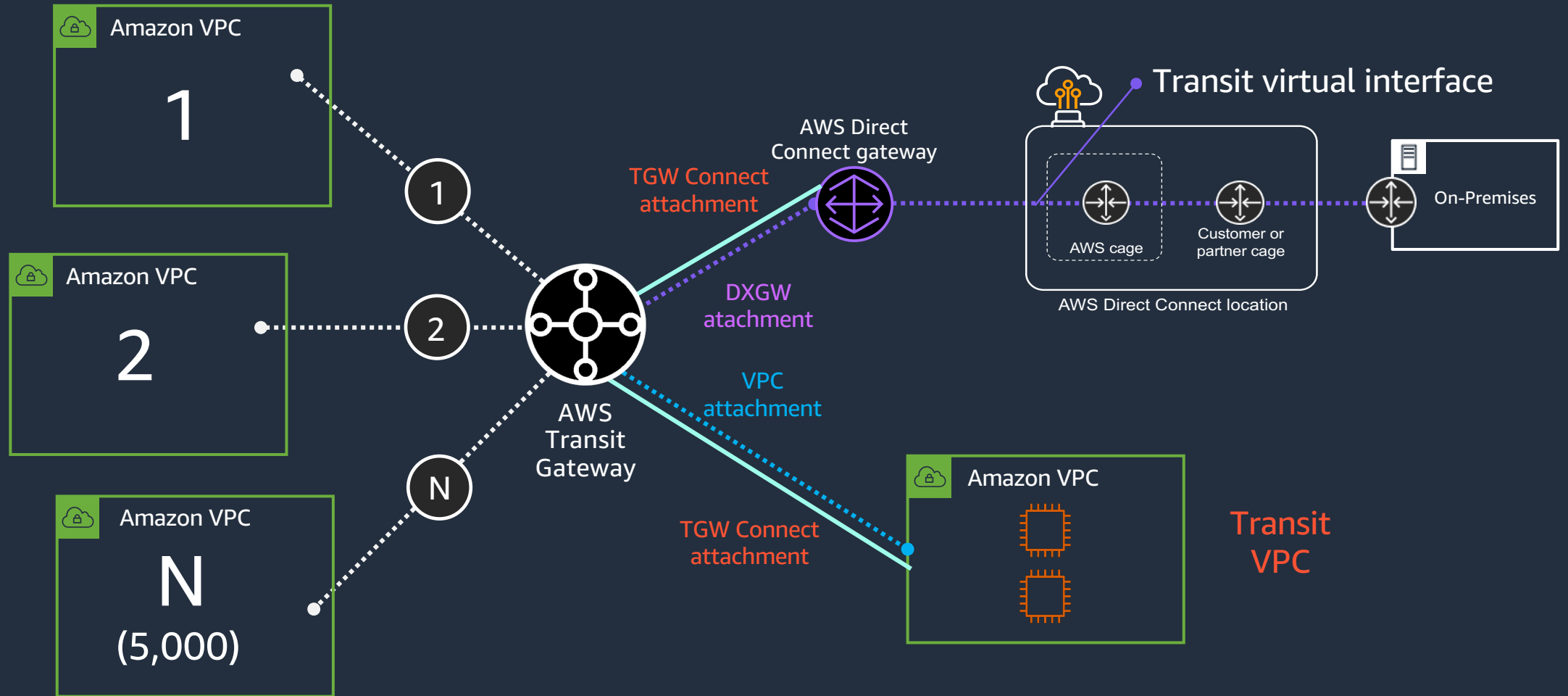
# AWS Transit Gateway

BEFORE



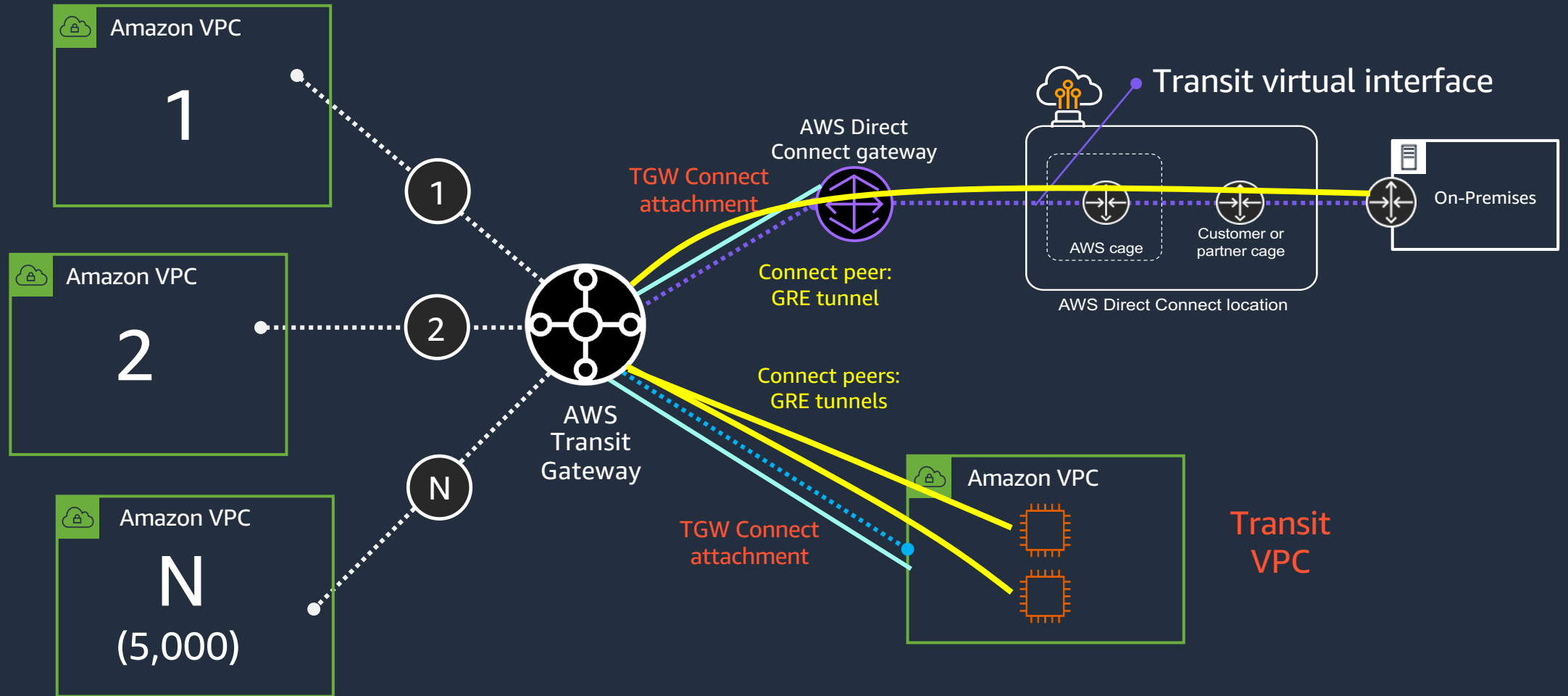
# AWS Transit Gateway **Connect**

AFTER



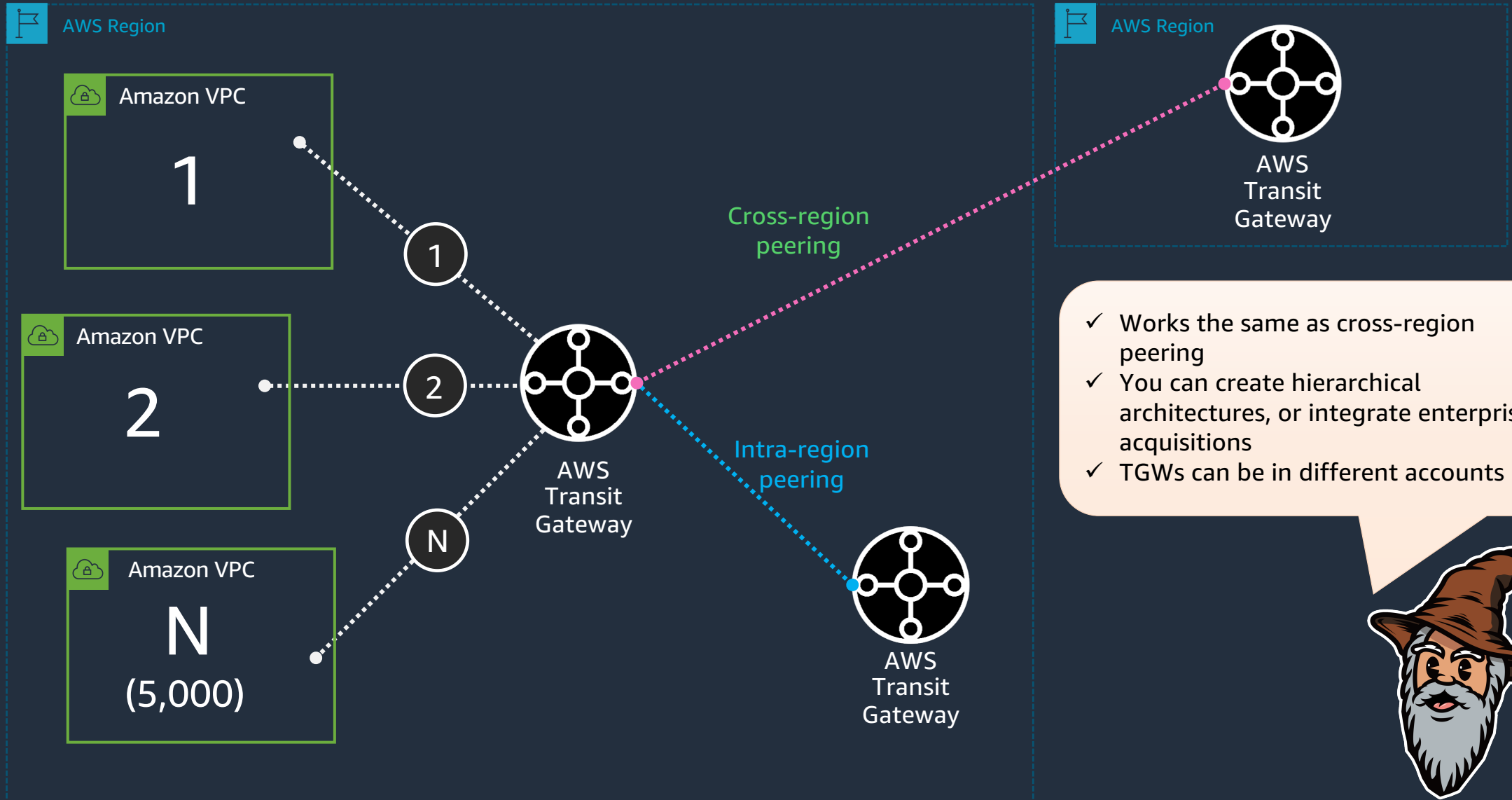
# AWS Transit Gateway **Connect**

AFTER



# AWS Transit Gateway: Intra-region peering

NEW

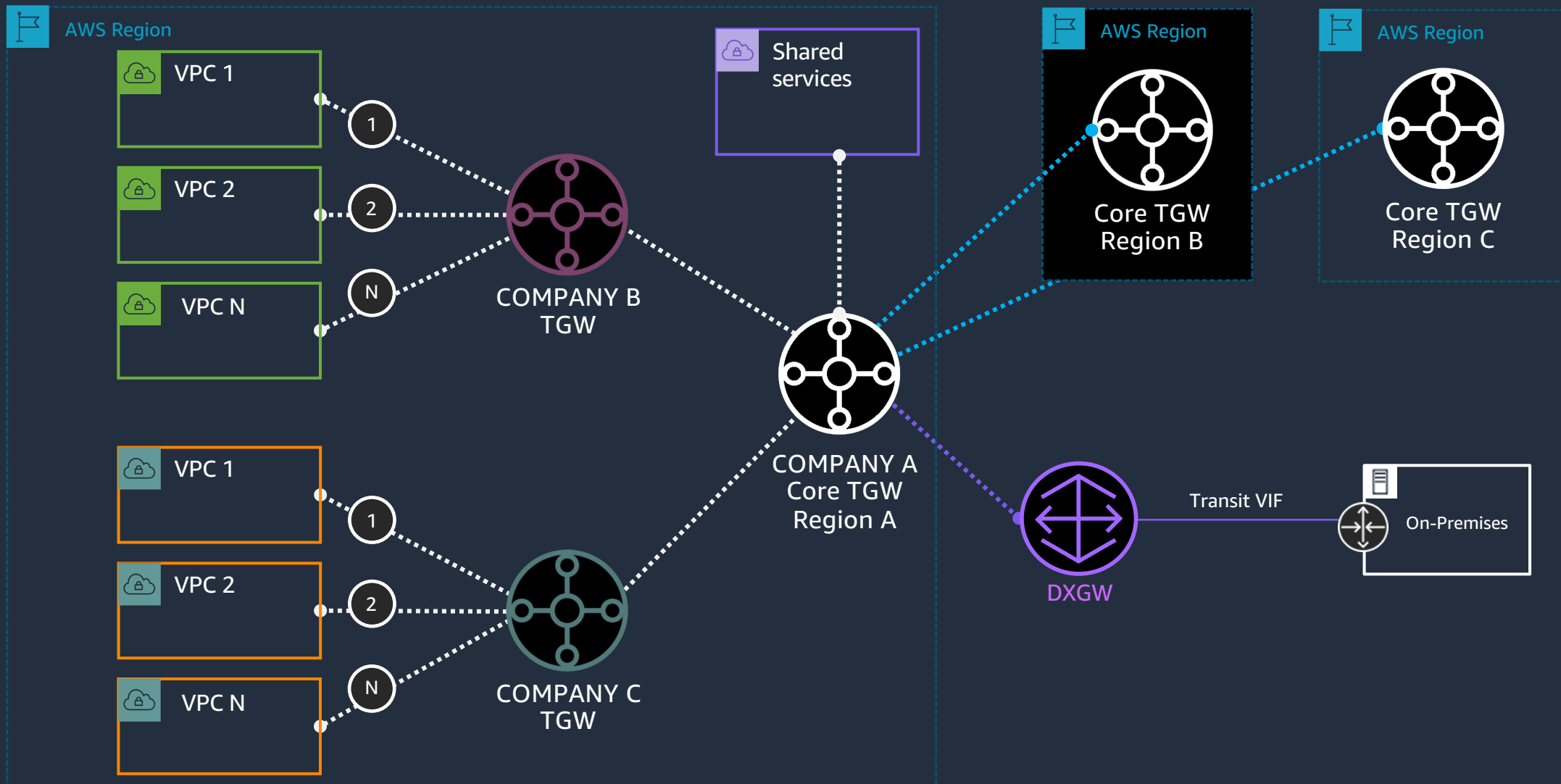


- ✓ Works the same as cross-region peering
- ✓ You can create hierarchical architectures, or integrate enterprise acquisitions
- ✓ TGWs can be in different accounts



# AWS Transit Gateway: Intra-region peering

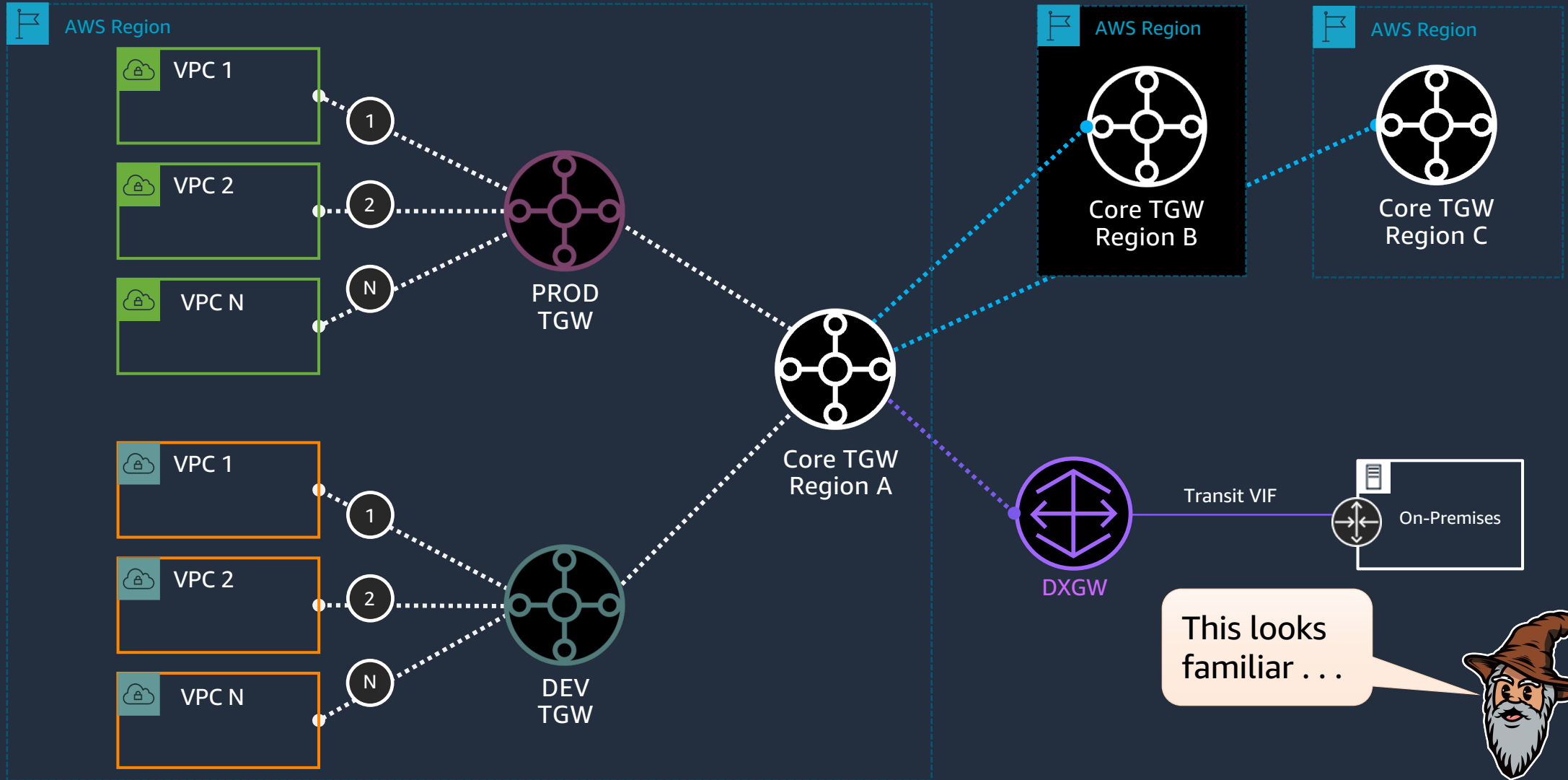
## ACQUISITIONS INTEGRATION



# AWS Transit Gateway: Intra-region peering



## HIERARCHICAL REGIONAL ARCHITECTURE

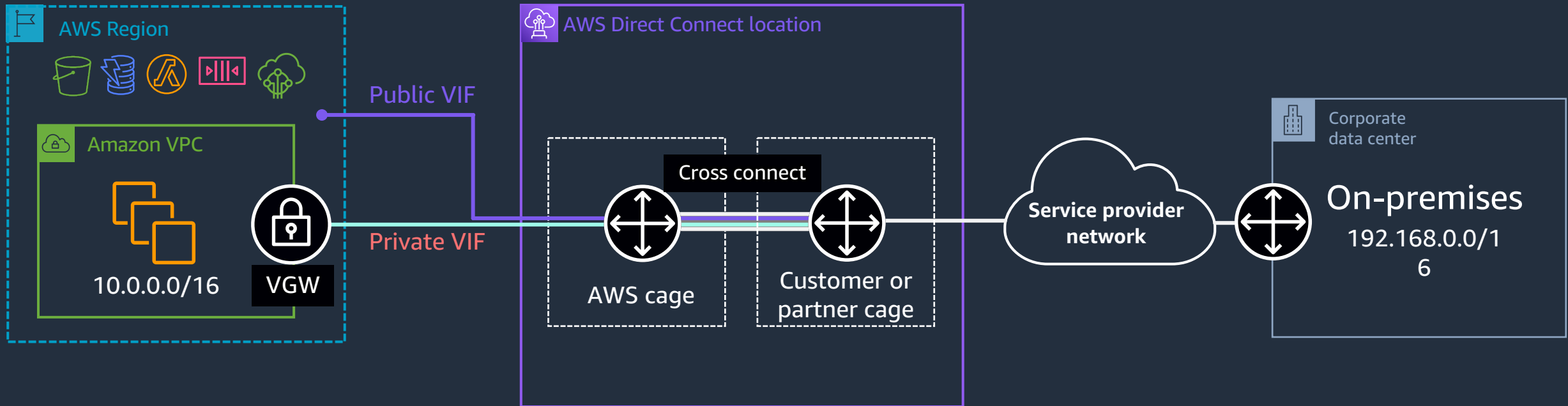


On-premises and  
global connectivity

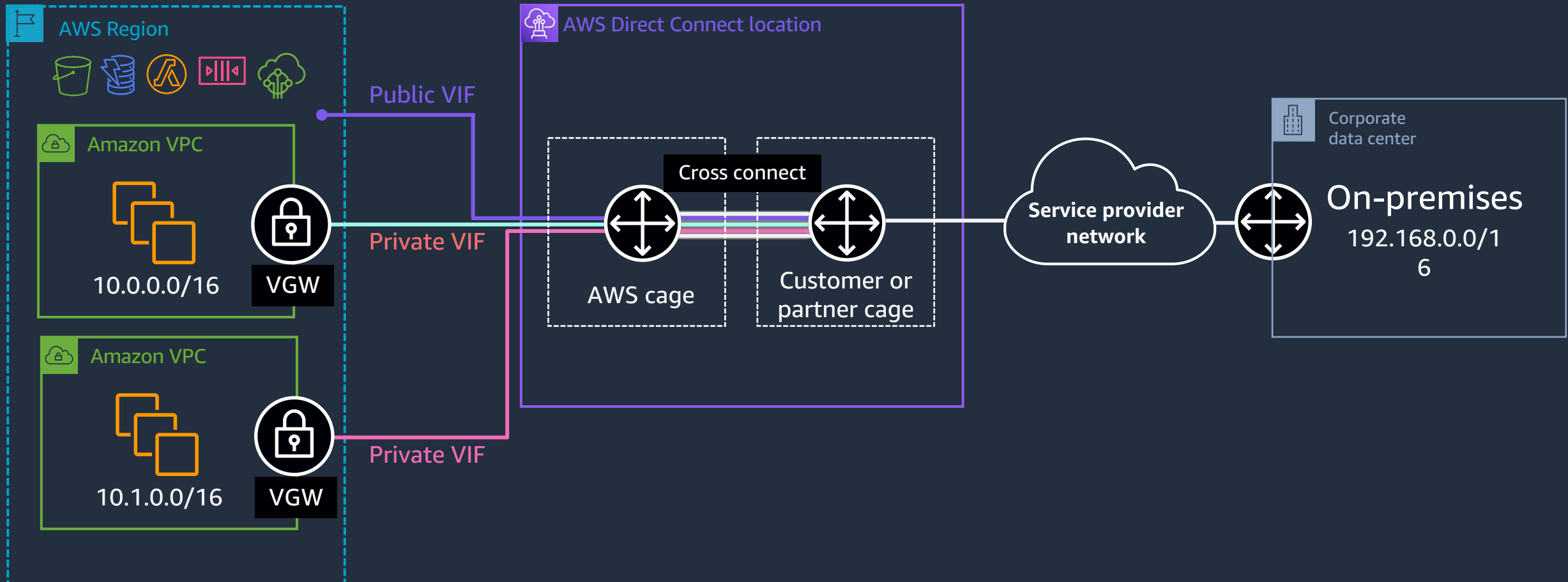
## **AWS Direct Connect**

MACSEC , 100Gbps, and AWS Local Zones

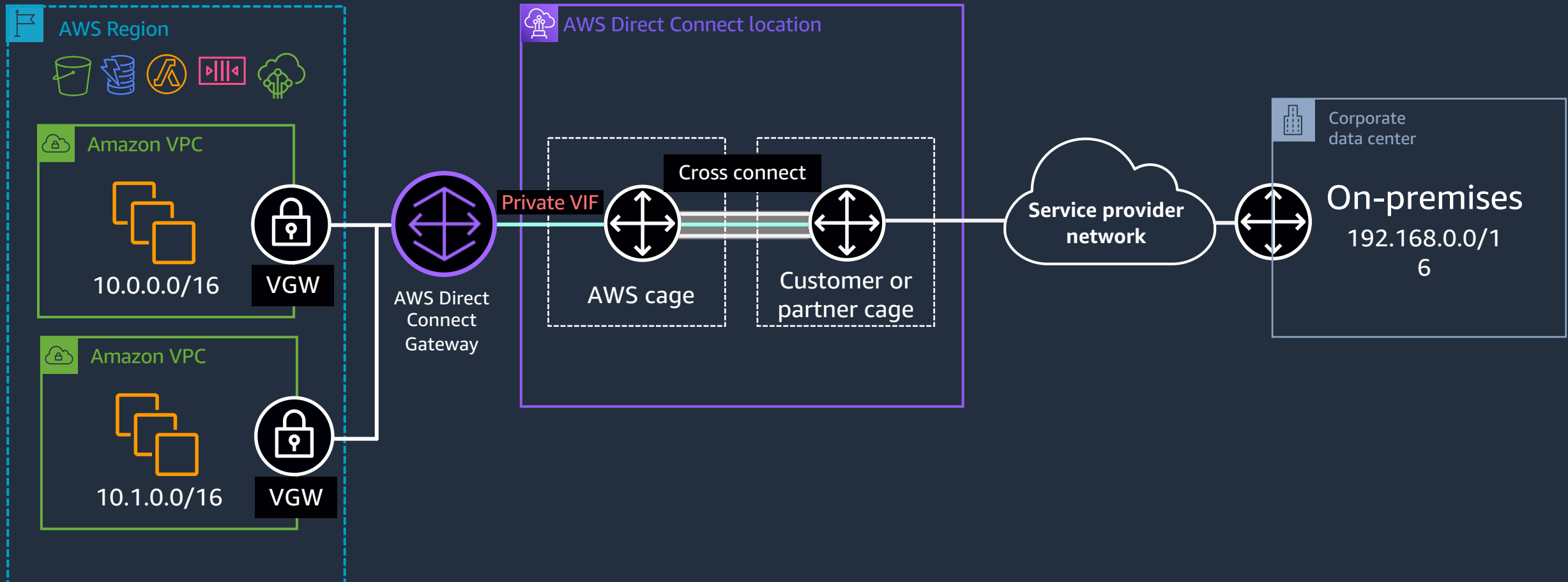
# An overview: AWS Direct Connect



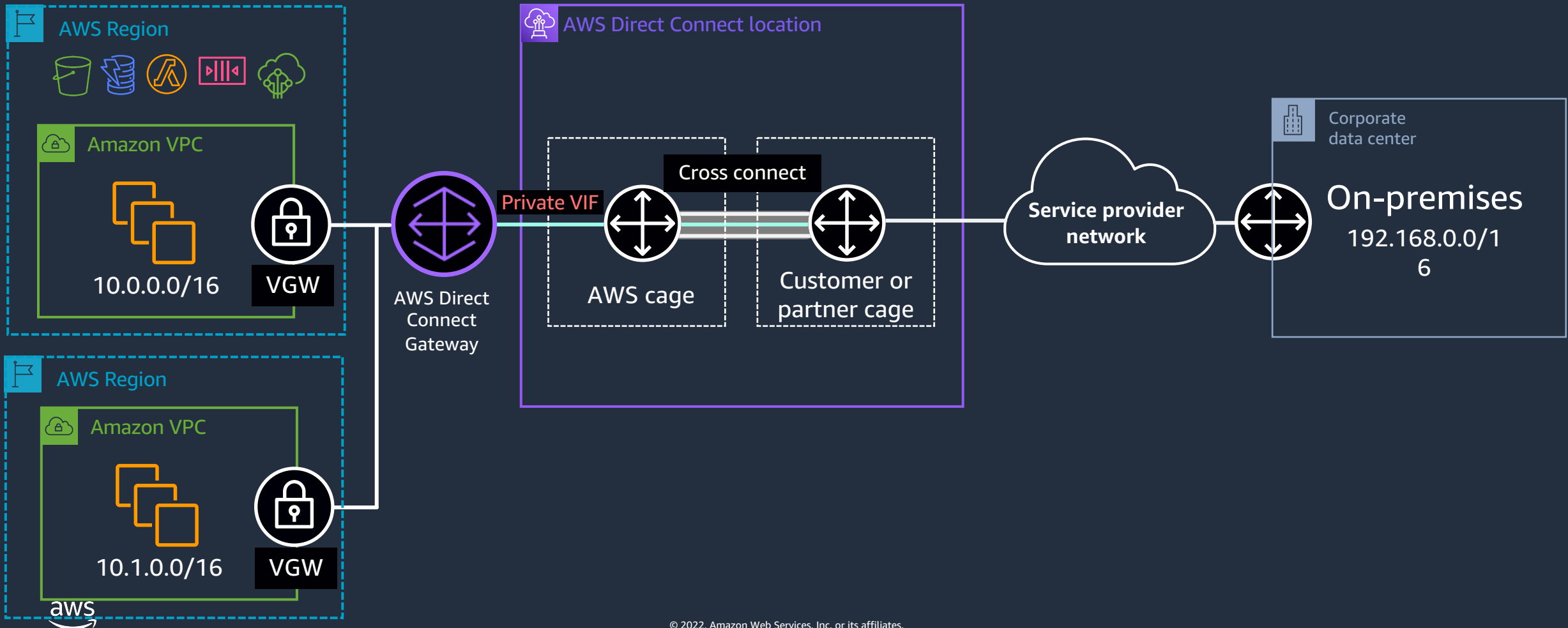
# An overview: AWS Direct Connect



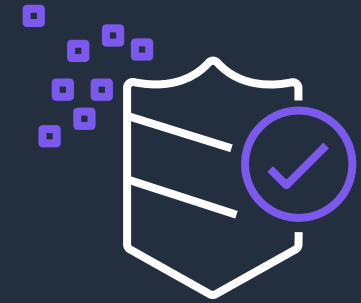
# An overview: AWS Direct Connect



# An overview: AWS Direct Connect



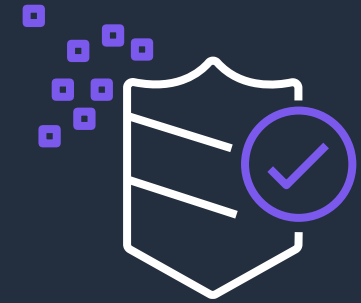
# Introducing: AWS Direct Connect MACsec



---

“Dance like nobody is watching.  
Encrypt like everyone is.”

# Introducing: AWS Direct Connect MACsec



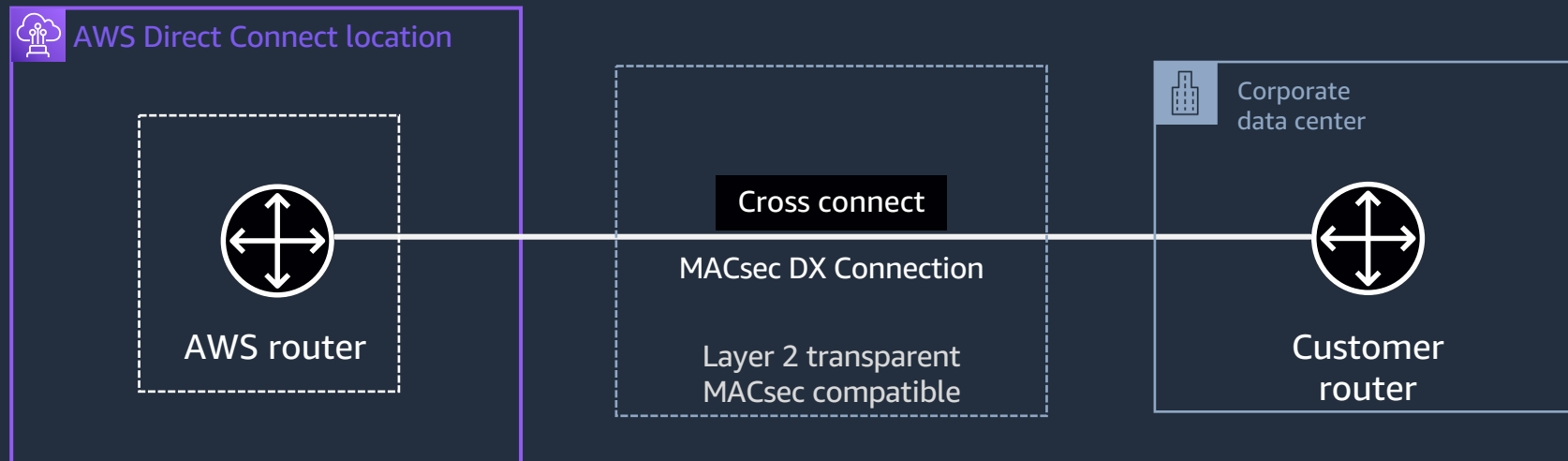
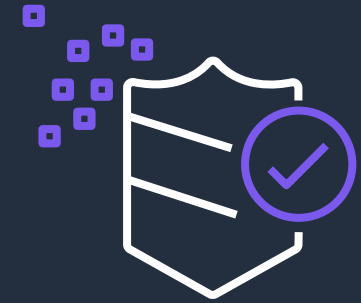
## Layer 2 confidentiality and integrity

MACsec allows you to secure an Ethernet link – including all control plane protocol packets (such as ARP, DHCP, LLDP, and Layer 3 routing protocols like BGP)

## High-speed encryption

Because MACsec encryption is done through hardware, it provides bidirectional line-rate, or near-line-rate, encryption

# Introducing: AWS Direct Connect MACsec



# On-premises and global connectivity

## **AWS Direct Connect**

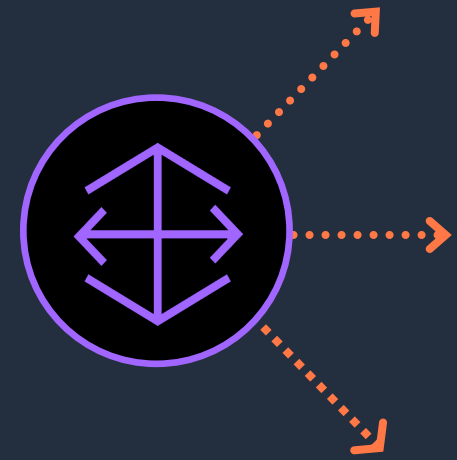
MACSEC , 100Gbps, and AWS Local Zones

---

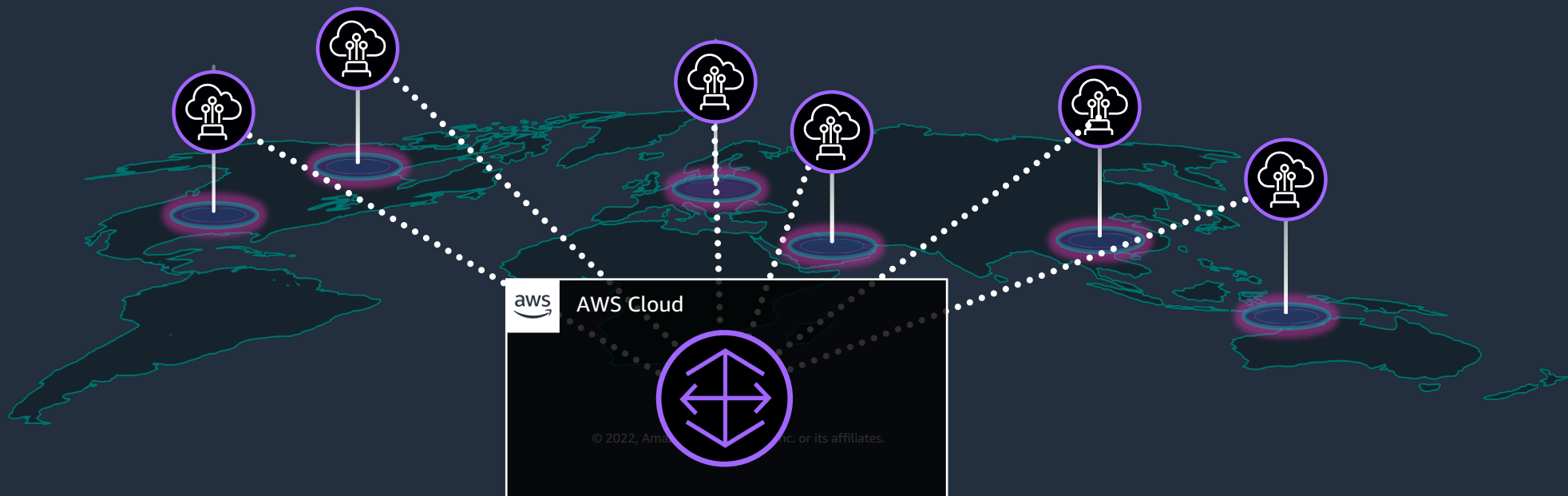
## **AWS Direct Connect SiteLink**

and AWS Direct Connect

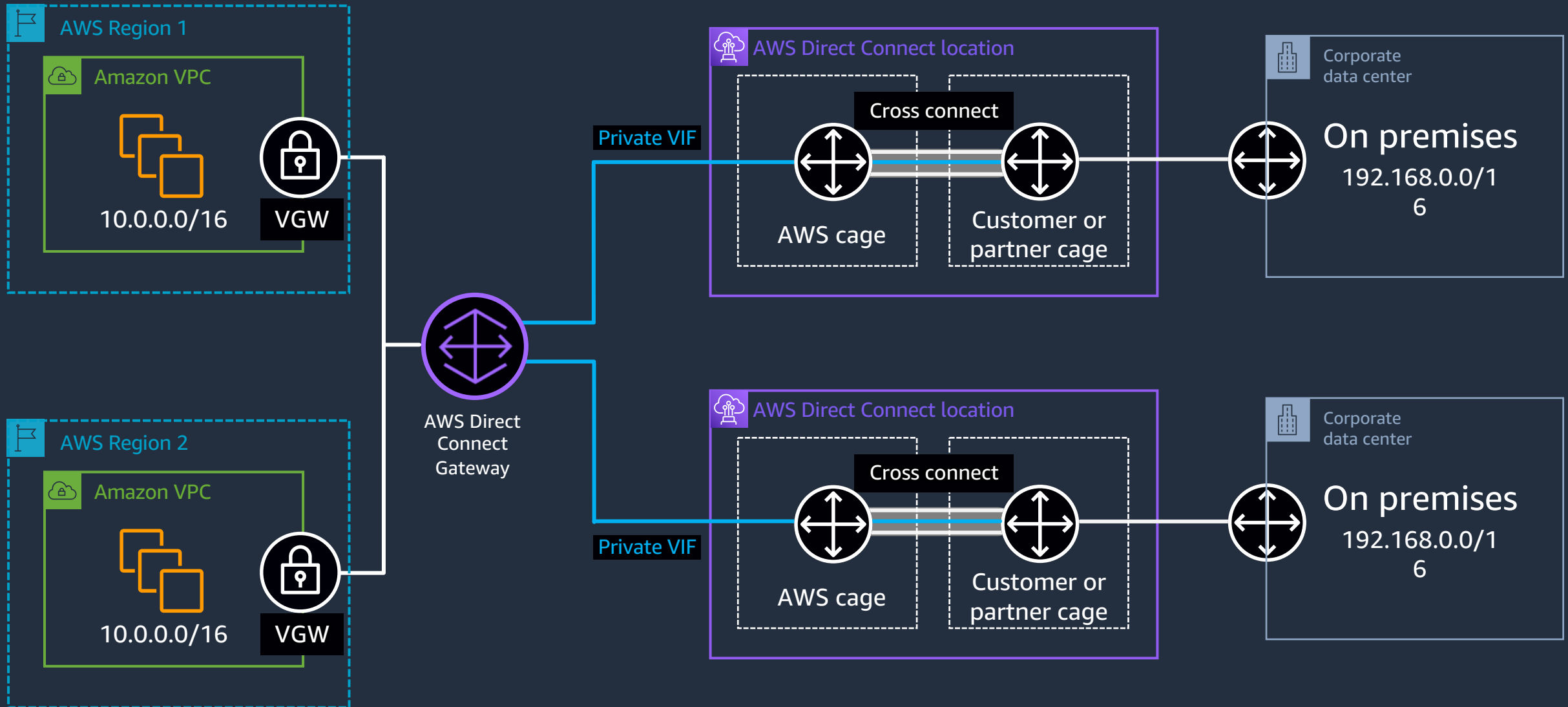
# Introducing: AWS Direct Connect SiteLink



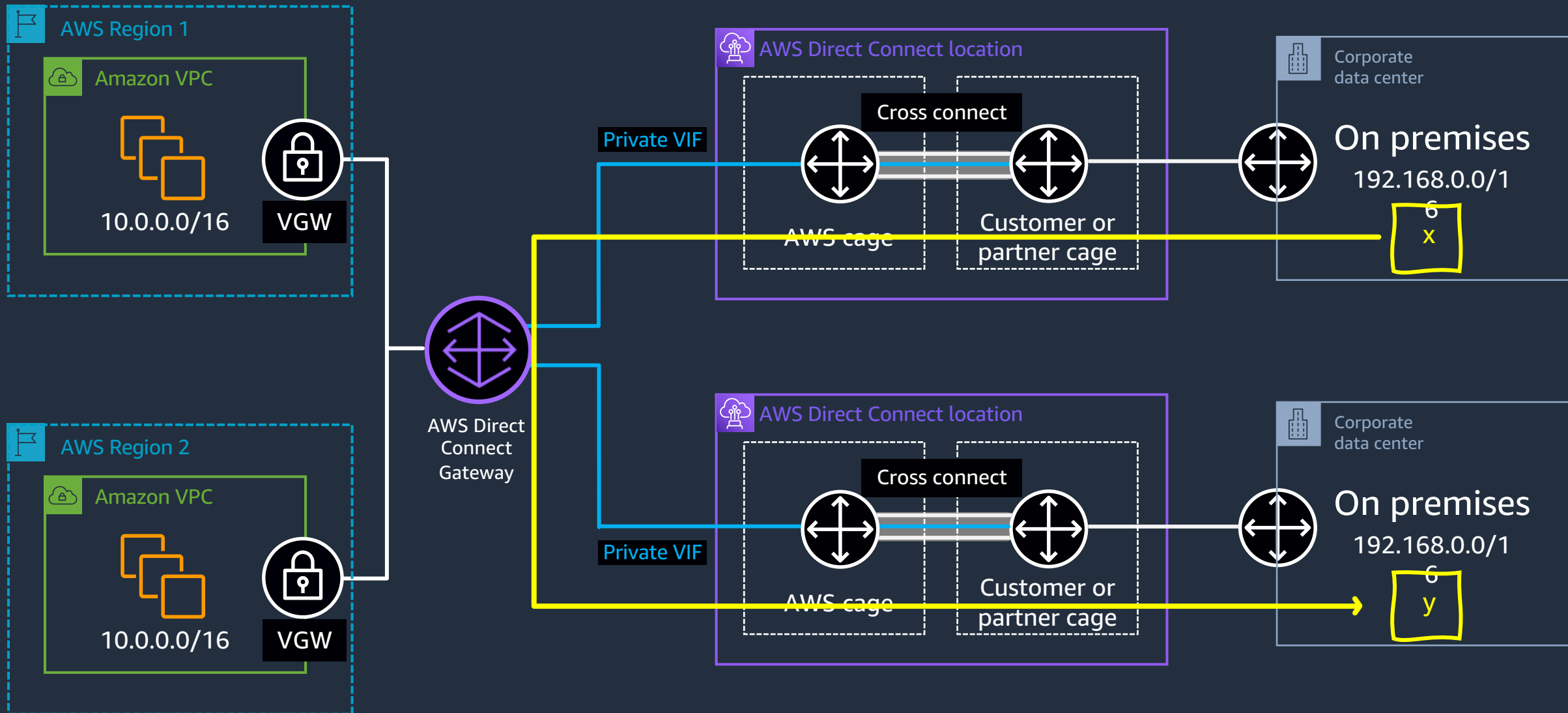
Create connections between your on-premises networks  
through the AWS global network backbone



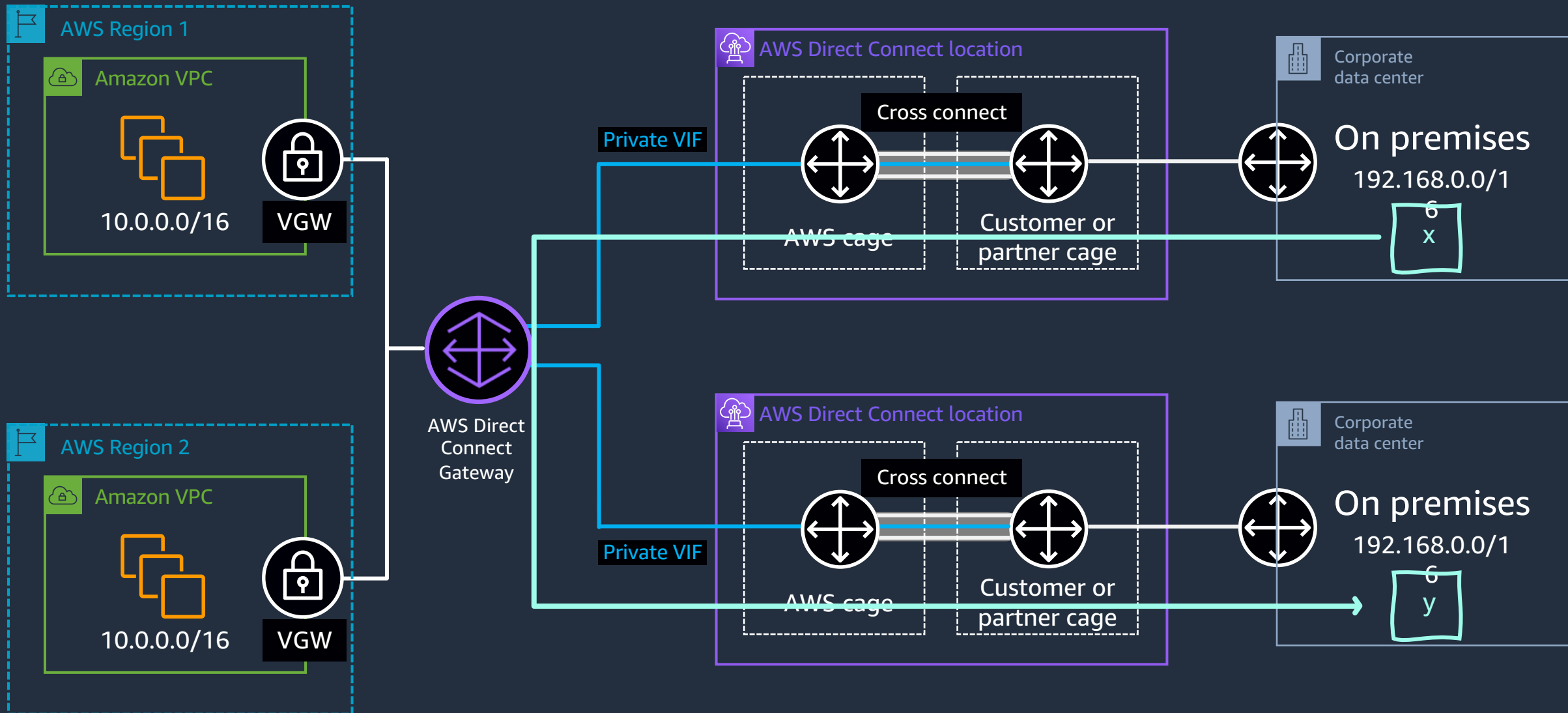
# AWS Direct Connect SiteLink: Before



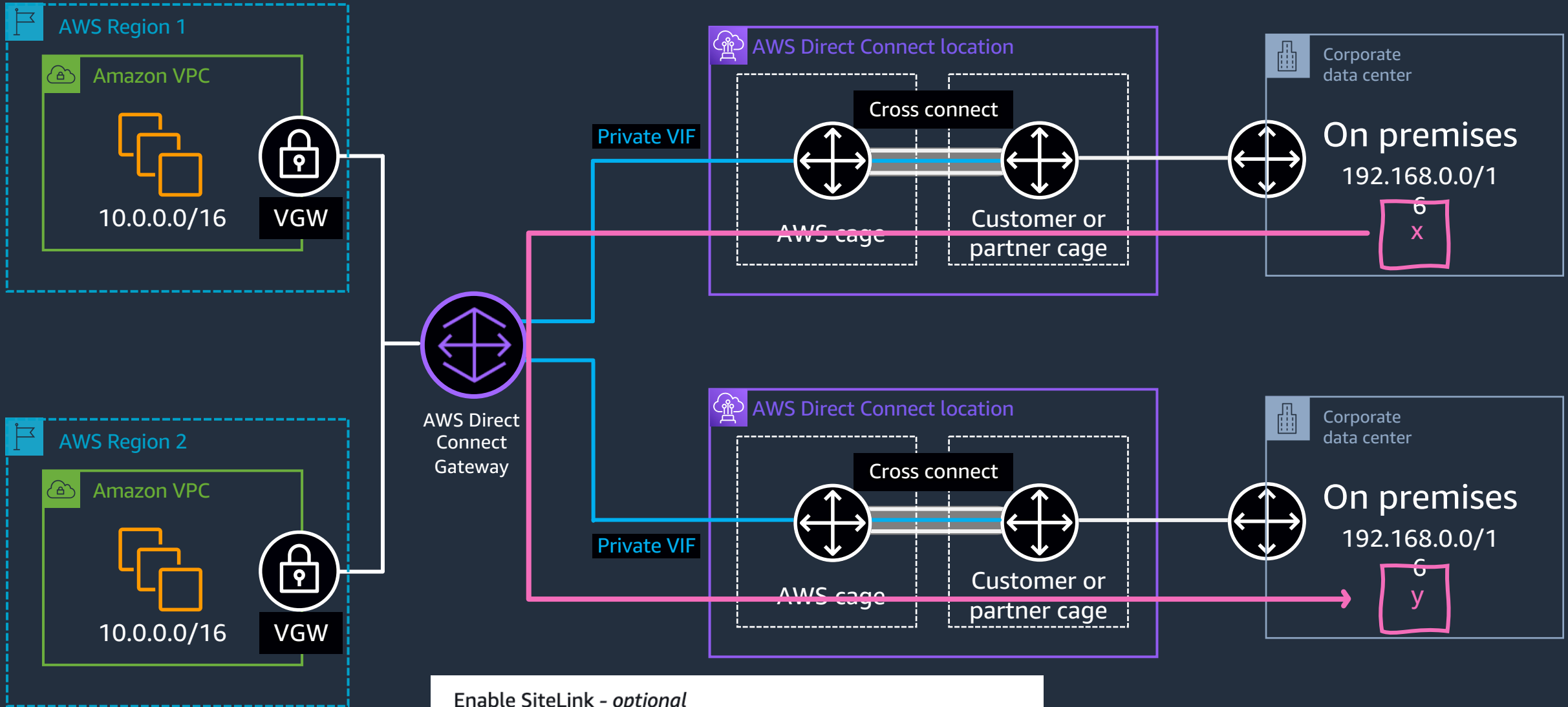
# AWS Direct Connect SiteLink: Before



# AWS Direct Connect SiteLink: Before

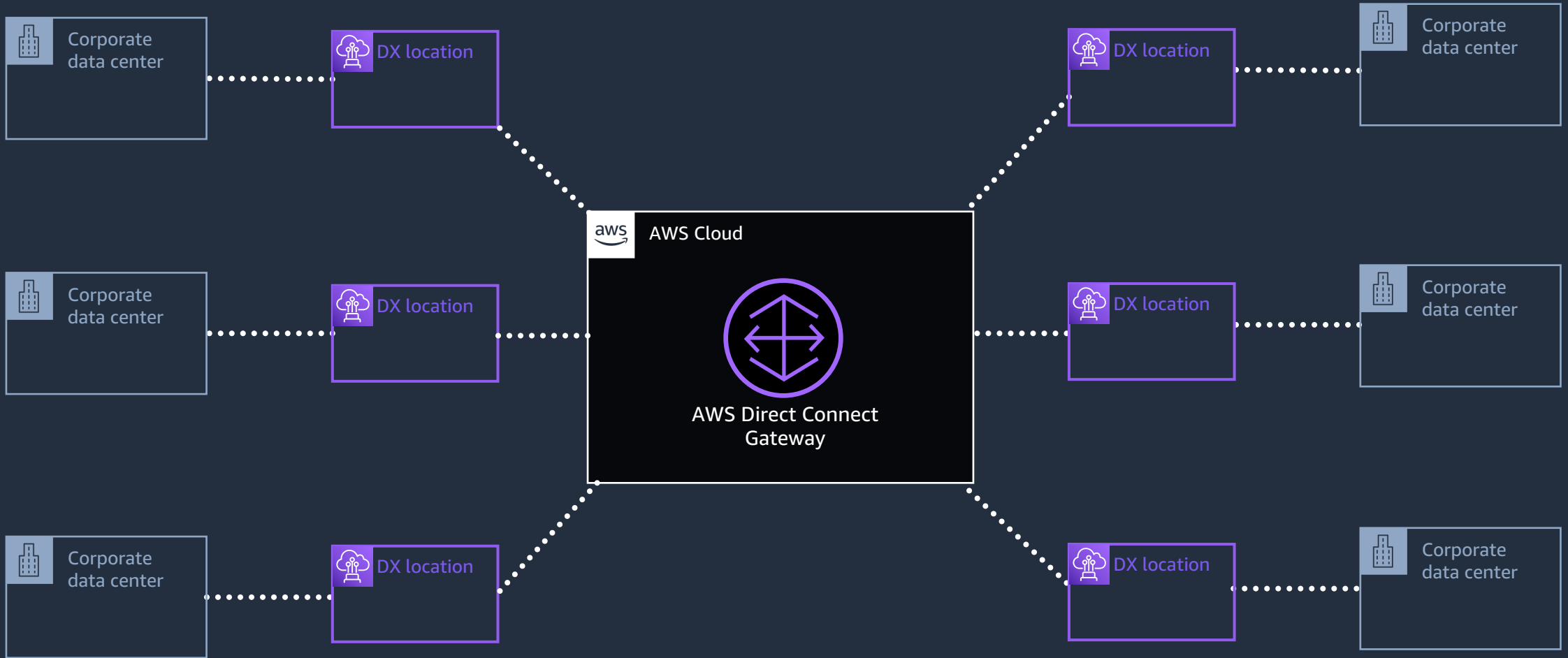


# AWS Direct Connect SiteLink: *After*



Enable SiteLink - *optional*  
Enable direct connectivity between Direct Connect points of presence.

Enabled



Available around the world at all commercial  
AWS Direct Connect PoPs *except China*



# On-premises and global connectivity

## **AWS Direct Connect**

MACSEC , 100Gbps, and AWS Local Zones

---

## **AWS Direct Connect SiteLink**

and AWS Direct Connect

---

## **AWS Cloud WAN**

for managed Wide Area Networking

# Introducing: AWS Cloud WAN



---

GA, June 2022

Build global networks in minutes

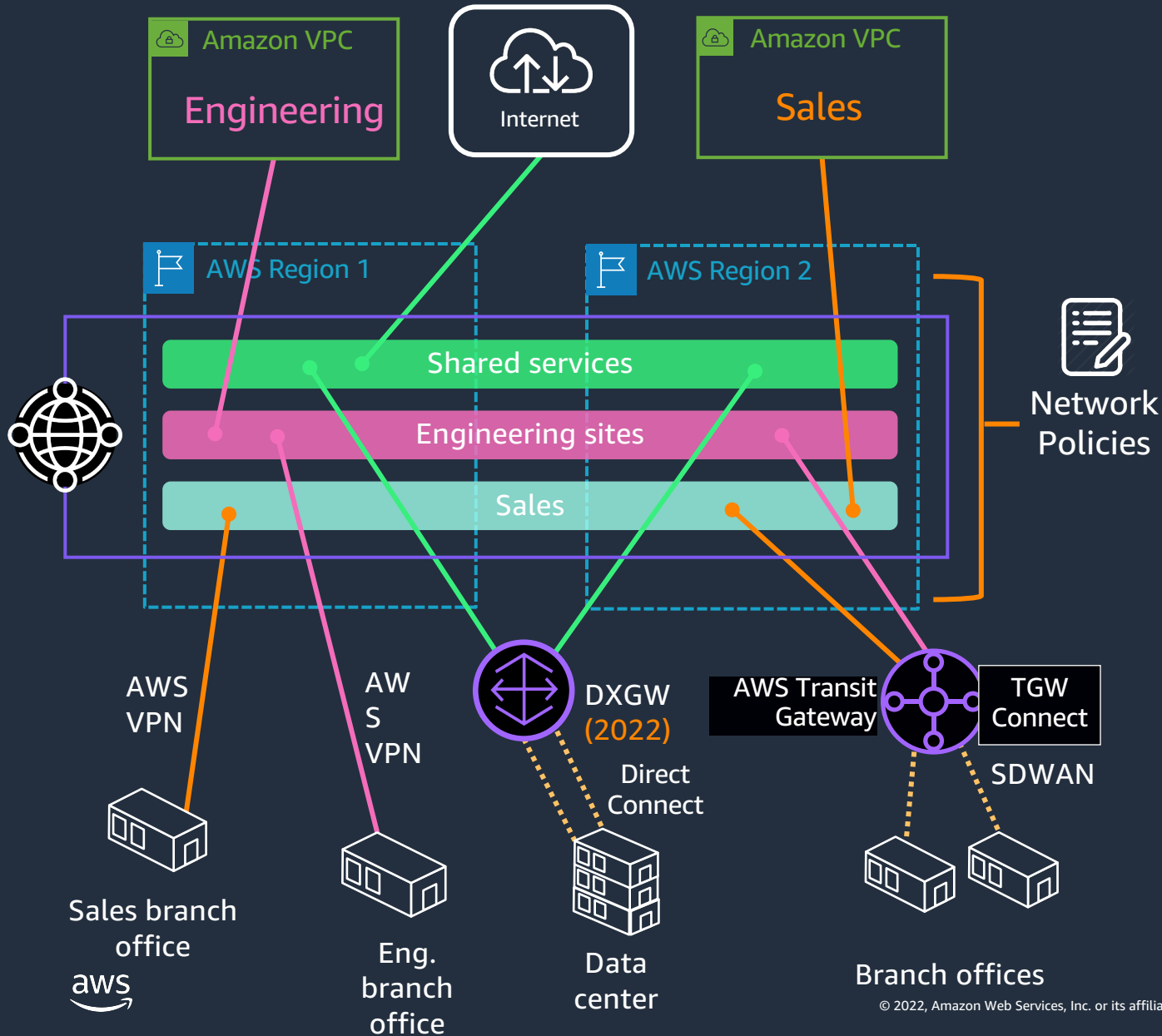
Use the AWS global backbone

Simplify WAN networking

Segment traffic with centralized policy



# AWS Cloud WAN



## Network segments

Isolation between VPCs and on-premises sites

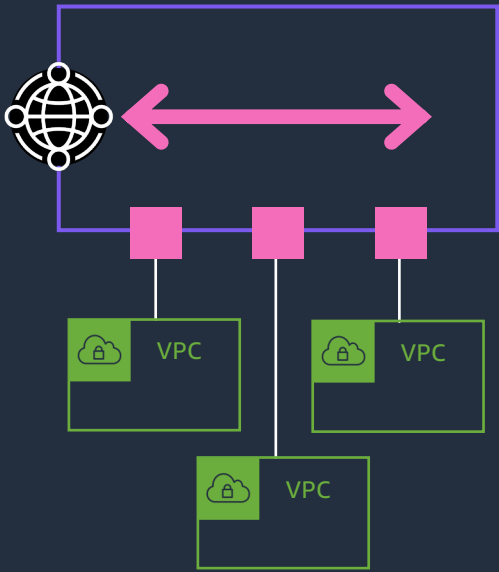
## Network policies

Define L3 routing policies based on attributes and behavior

## Performance monitoring

**2022 roadmap** - Packet loss, jitter, and latency measurements across the backbone.

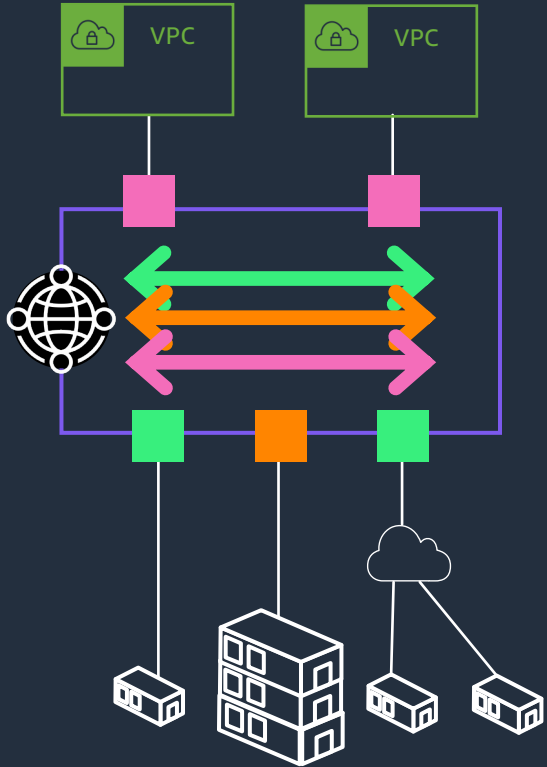
# AWS Cloud WAN use cases



Between VPCs

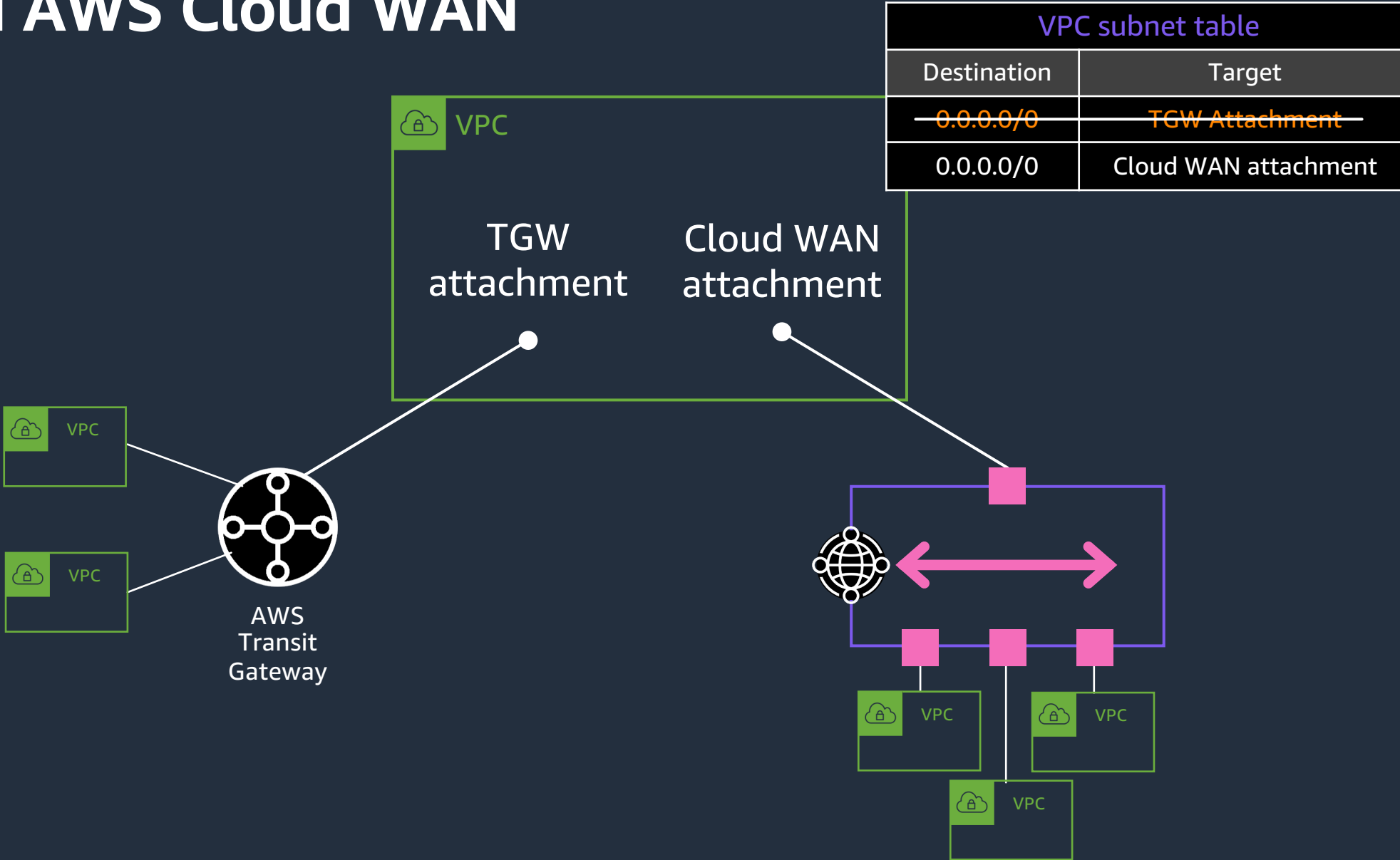


WAN



Hybrid

# TGW and AWS Cloud WAN



# AWS Cloud WAN

VPC-to-VPC

VPN termination

SDWAN integration

Segments

Dashboard and monitoring

Region-based

DX and TGW support on  
roadmap (2022)

# DX SiteLink

DX port-to-port

Not dependent on AWS  
Regions

Support for up to 100 GBPS  
paths

Enabled per virtual interface

# Both

Use AWS backbone

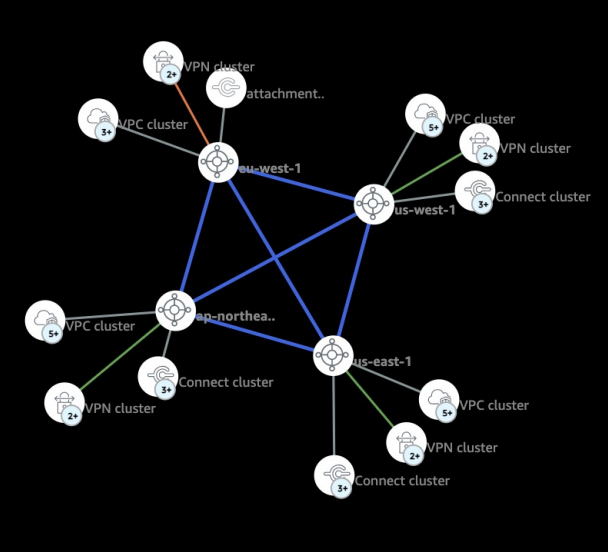
Support encryption  
(MACsec/IPsec)

Pay for what you use

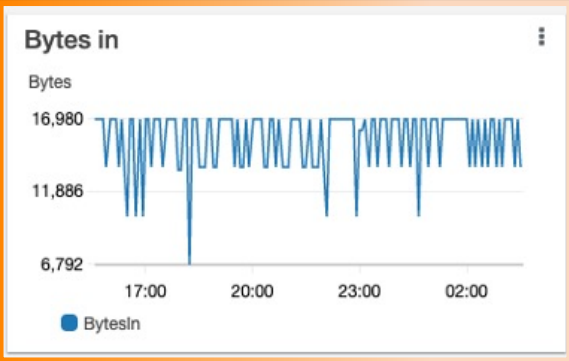
Available globally

Can also be used to  
access AWS resources

# AWS Network Manager



Topologies



Metrics

#	Region	Message	Resource
1		BGP for a Connect peer has been established.	arn:aws:netwo
2		BGP for a Connect peer has been established.	arn:aws:netwo
3		IPsec for a VPN connection has come up.	arn:aws:netwo
4		IPsec for a VPN connection has come up.	arn:aws:netwo
5		BGP for a VPN connection has been established.	arn:aws:netwo
6		IPsec for a VPN connection has come up.	arn:aws:netwo
7		A Connect peer has been created in a Connect attachment.	arn:aws:netwo
8		An attachment has been associated to a Segment.	arn:aws:netwo
9		A Site-to-Site VPN attachment has been created for a Core Network.	arn:aws:netwo
10		IPsec for a VPN connection has come up.	arn:aws:netwo
11		IPsec for a VPN connection has come up.	arn:aws:netwo
12		Routes in one or more Segments have been installed.	arn:aws:netwo
13		IPsec for a VPN connection has come up.	arn:aws:netwo
14		BGP for a VPN connection has been established.	arn:aws:netwo
15		BGP for a VPN connection has gone down.	arn:aws:netwo
16		BGP for a VPN connection has been established.	arn:aws:netwo
17		BGP for a VPN connection has been established.	arn:aws:netwo
18		Routes in one or more Segments have been installed.	arn:aws:netwo
19		Routes in one or more Segments have been installed.	arn:aws:netwo

Events



# Thank you!

Dragos Madarasan



Please complete  
the session survey