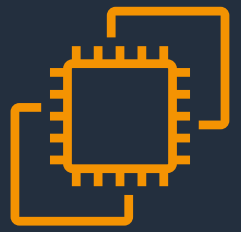
Advanced Amazon VPC

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)

The internet

AWS Region

Amazon S3 | Amazon DynamoDB | AWS Lambda | Amazon SQS | Amazon SNS | AWS IoT Core

Amazon VPC

Availability Zone 1

Public subnet

Instance A
10.1.0.11/24

Private subnet

Instance C
10.1.2.33/24

Availability Zone 2

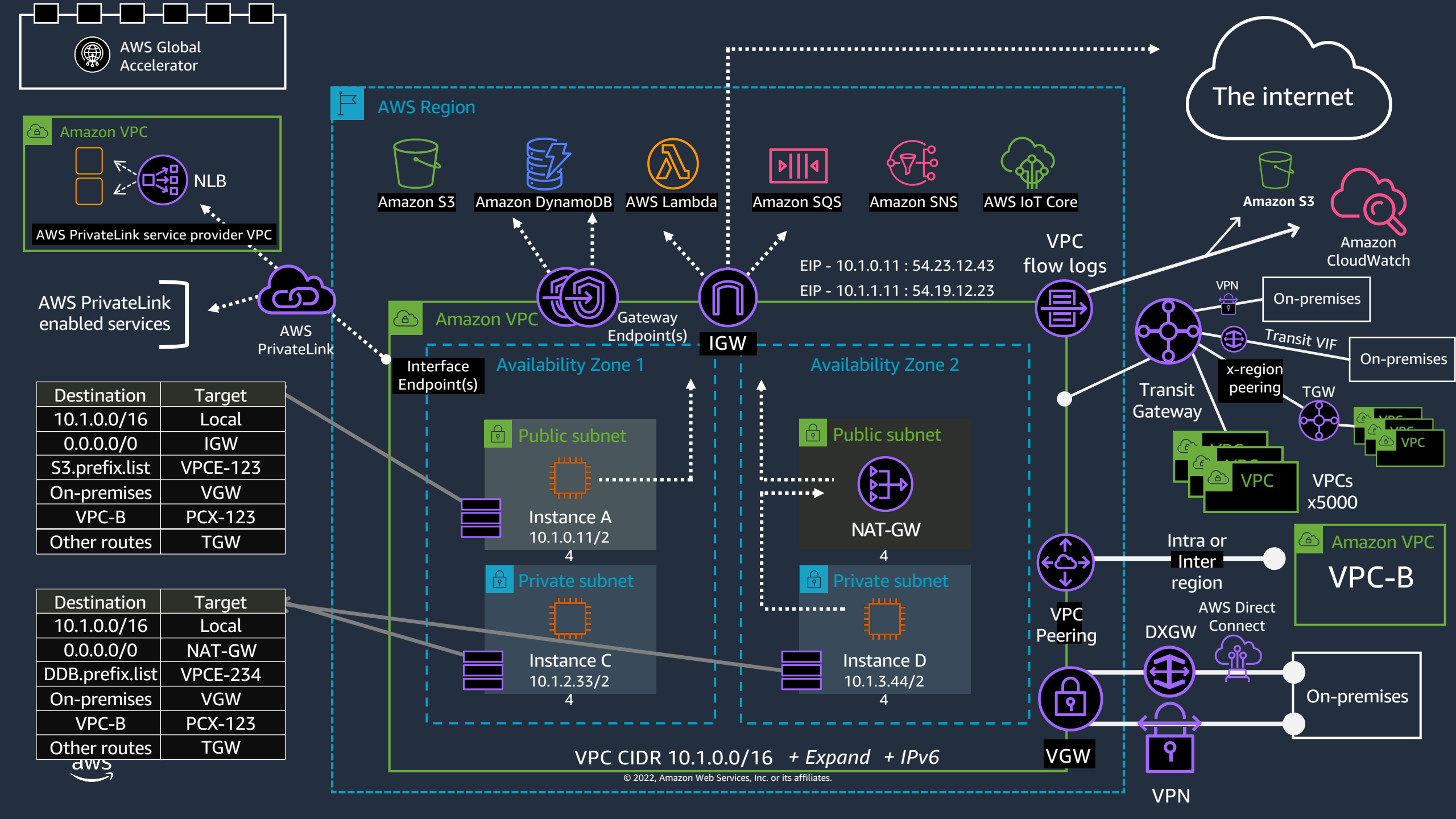
Public subnet

Instance B
10.1.1.22/24

Private subnet

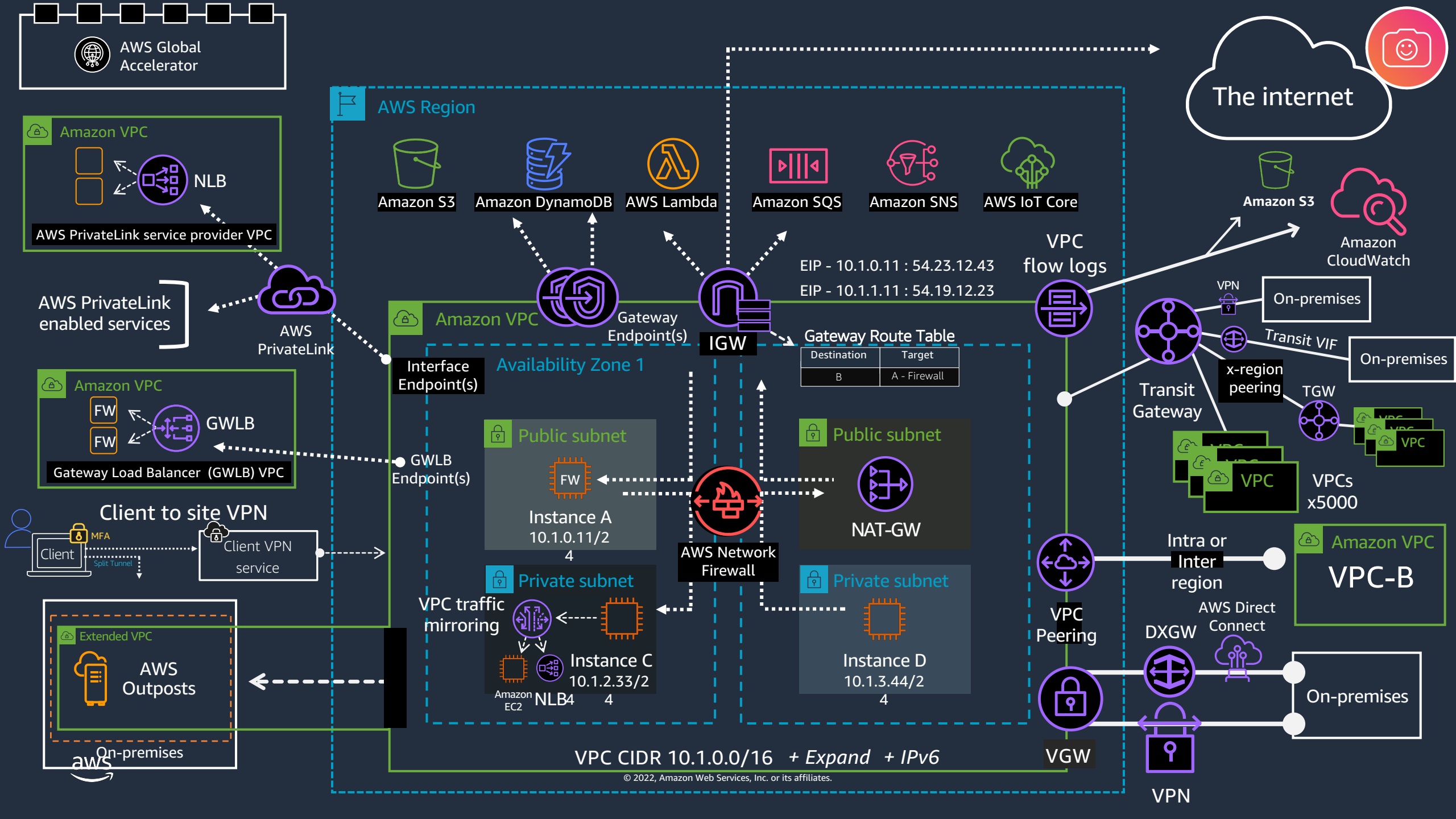
Instance D
10.1.3.44/24

VPC CIDR 10.1.0.0/16 *+ Expand* *+ IPv6*



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


AWS Global Accelerator
The internet
AWS Region
Amazon VPC
NLB
AWS PrivateLink service provider VPC
Amazon S3
Amazon DynamoDB
AWS Lambda
Amazon SQS
Amazon SNS
AWS IoT Core
Amazon S3
Amazon CloudWatch
AWS PrivateLink enabled services
AWS PrivateLink
Gateway Endpoint(s)
IGW
EIP - 10.1.0.11 : 54.23.12.43
EIP - 10.1.1.11 : 54.19.12.23
VPC flow logs
Amazon VPC
Interface Endpoint(s)
Availability Zone 1
Gateway Route Table
Destination
Target
B
A - Firewall
VPN
On-premises
Transit VIF
On-premises
Transit Gateway
x-region peering
TGW
VPC
VPCs x5000
Amazon VPC
FW
FW
GWLB
Gateway Load Balancer (GWLB) VPC
GWLB Endpoint(s)
Public subnet
FW
Instance A
10.1.0.11/24
Public subnet
NAT-GW
AWS Network Firewall
Client to site VPN
Client
MFA
Split Tunnel
Client VPN service
Private subnet
VPC traffic mirroring
Instance C
10.1.2.33/24
Amazon EC2
NLB
Private subnet
Instance D
10.1.3.44/24
Intra or Inter region
Amazon VPC
VPC-B
VPC Peering
AWS Direct Connect
DXGW
Extended VPC
AWS Outposts
On-premises
VPC CIDR 10.1.0.0/16 + Expand + IPv6
VGW
On-premises
VPN
© 2022, Amazon Web Services, Inc. or its affiliates.


What else have we been up to?

IPv6

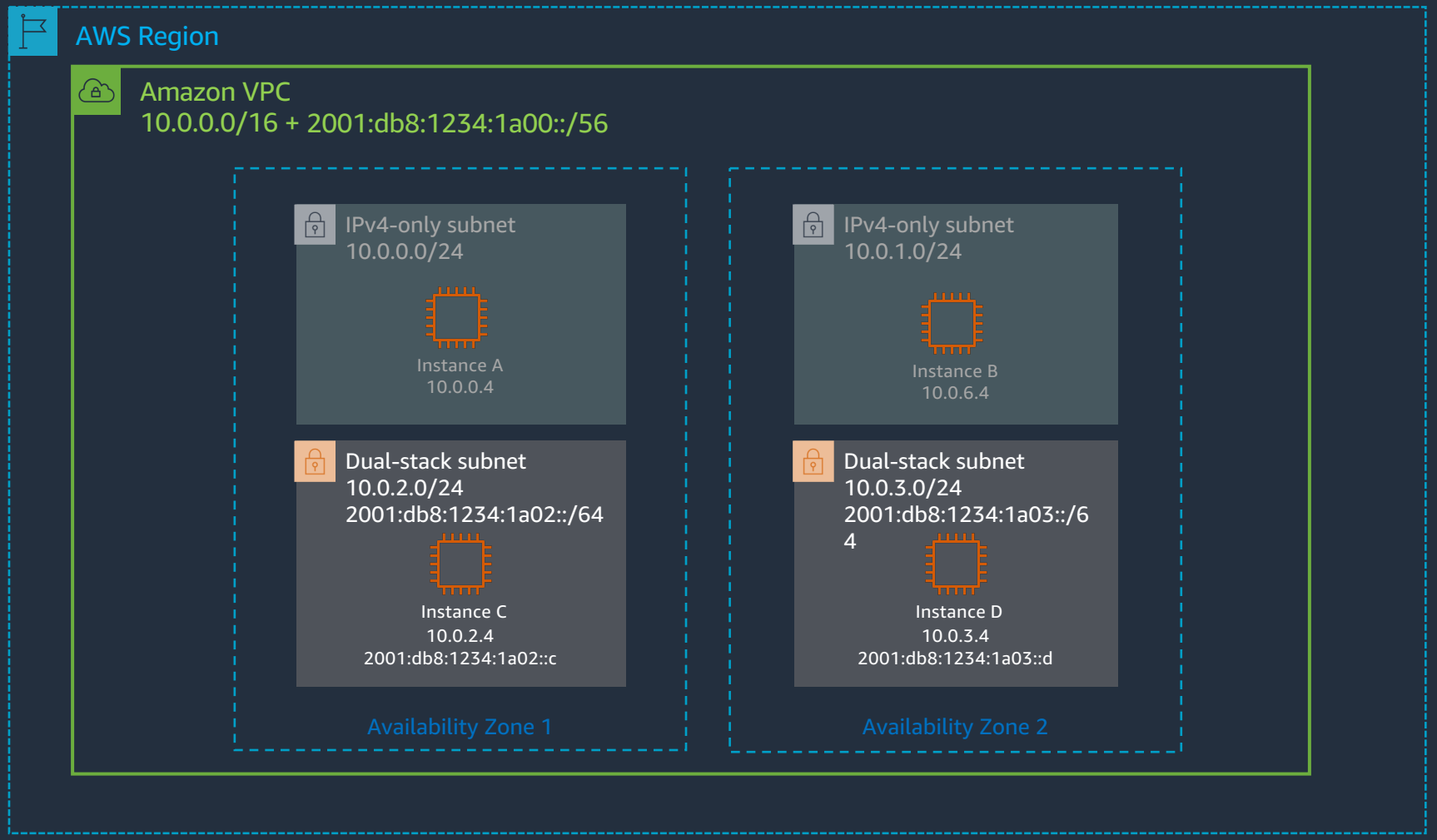
Amazon VPC
IPv6-only subnets

NAT64 and DNS64
Interoperability with IPv4 environments

Amazon EC2
Resource-based instance naming

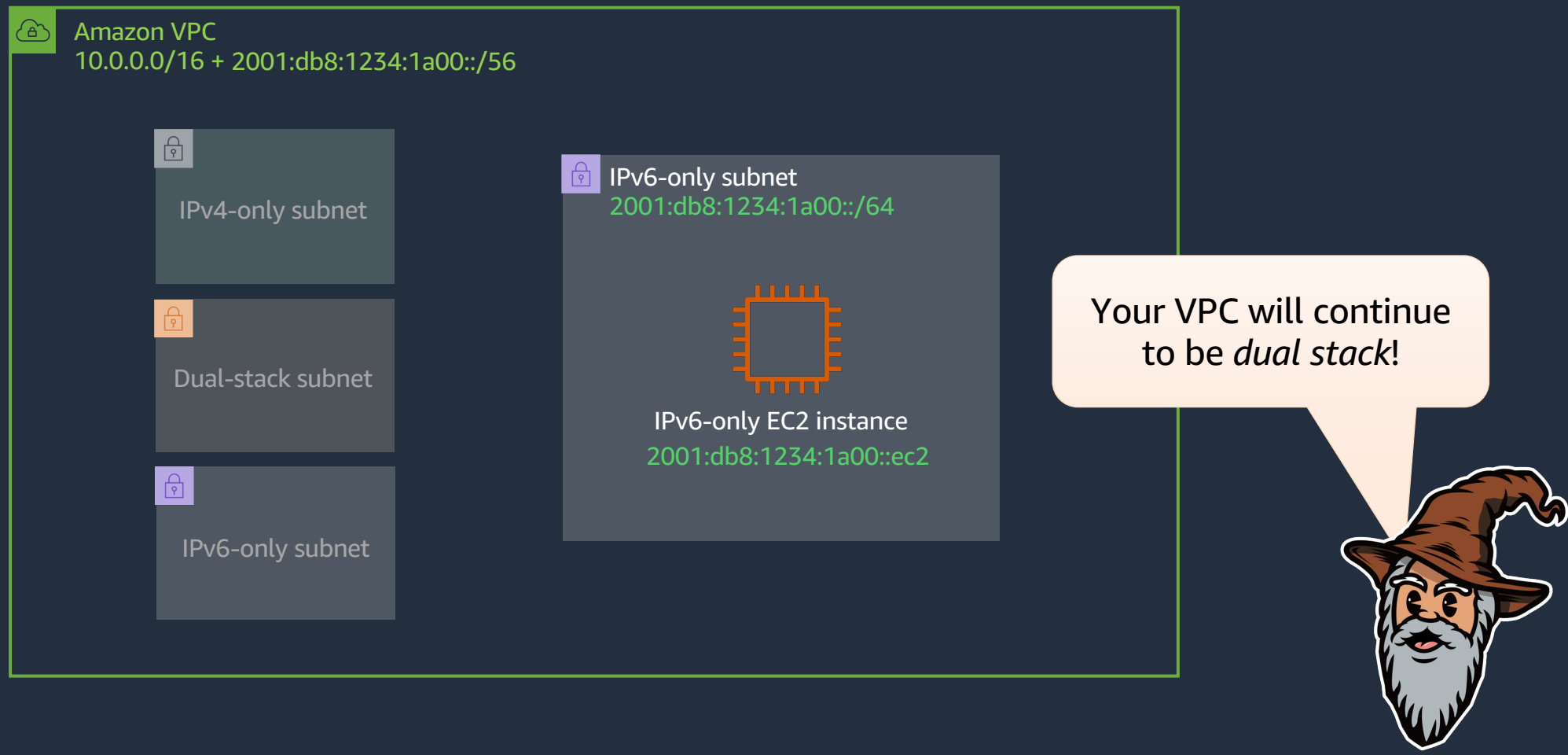
Elastic Load Balancing
Full dual-stack IPv6 support

Amazon VPC: Native dual stack



NEW

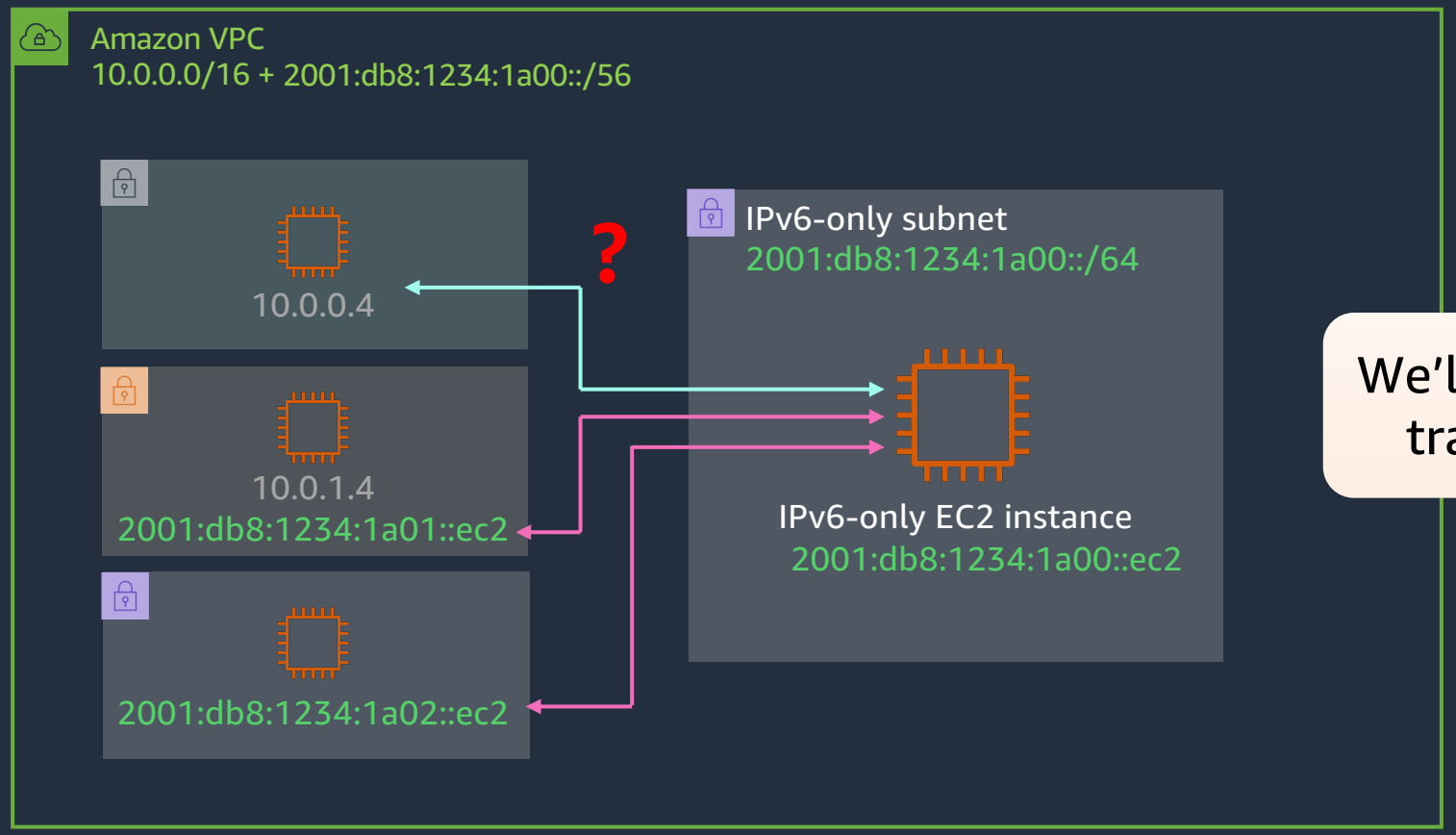
Amazon dual-stack VPC: IPv6-only subnets



Traffic flows inside Amazon VPC

Amazon dual-stack VPC: IPv6 only subnets

FLOWS

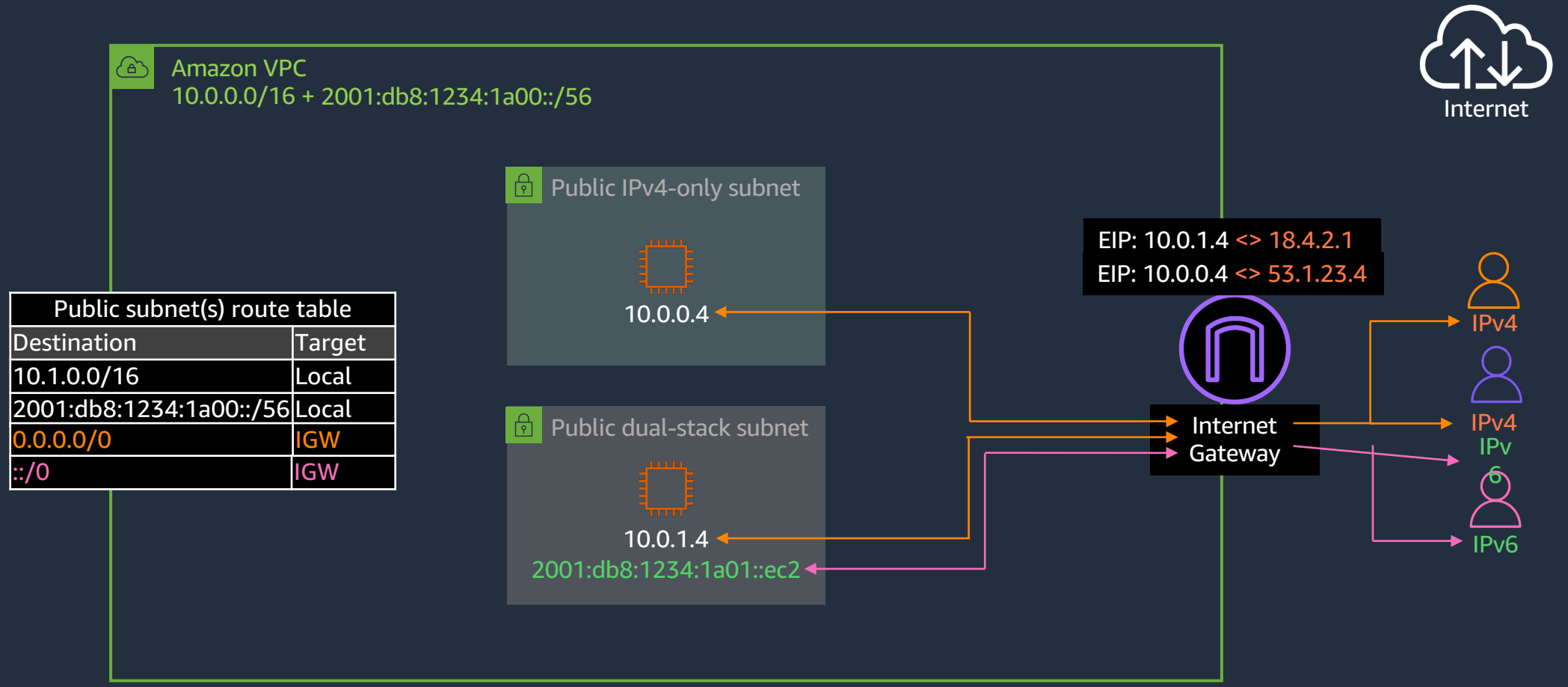


We'll get back to this traffic flow later!

Public subnets internet connectivity

Amazon dual-stack VPC: Internet connectivity

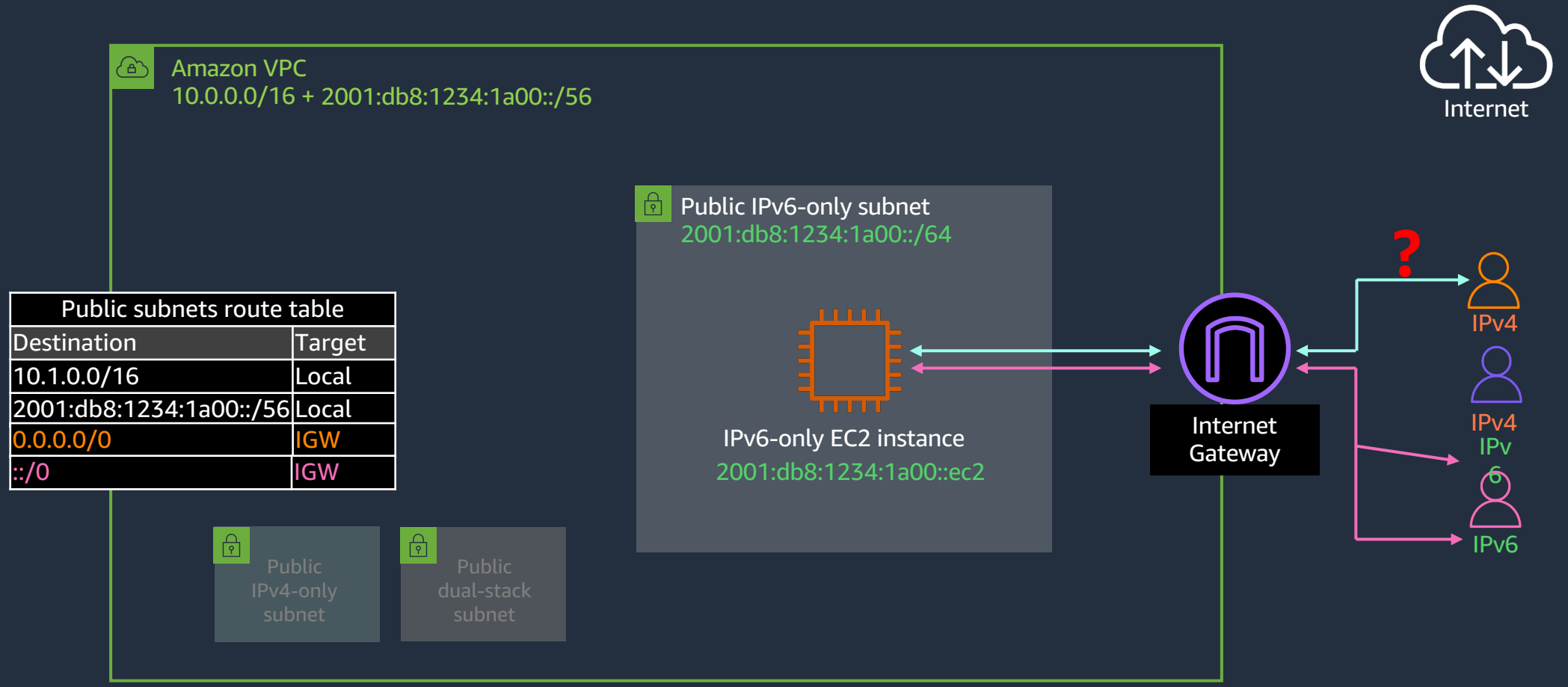
PUBLIC SUBNETS



Public subnet(s) route table	
Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	IGW
::/0	IGW

Amazon dual-stack VPC: Internet connectivity

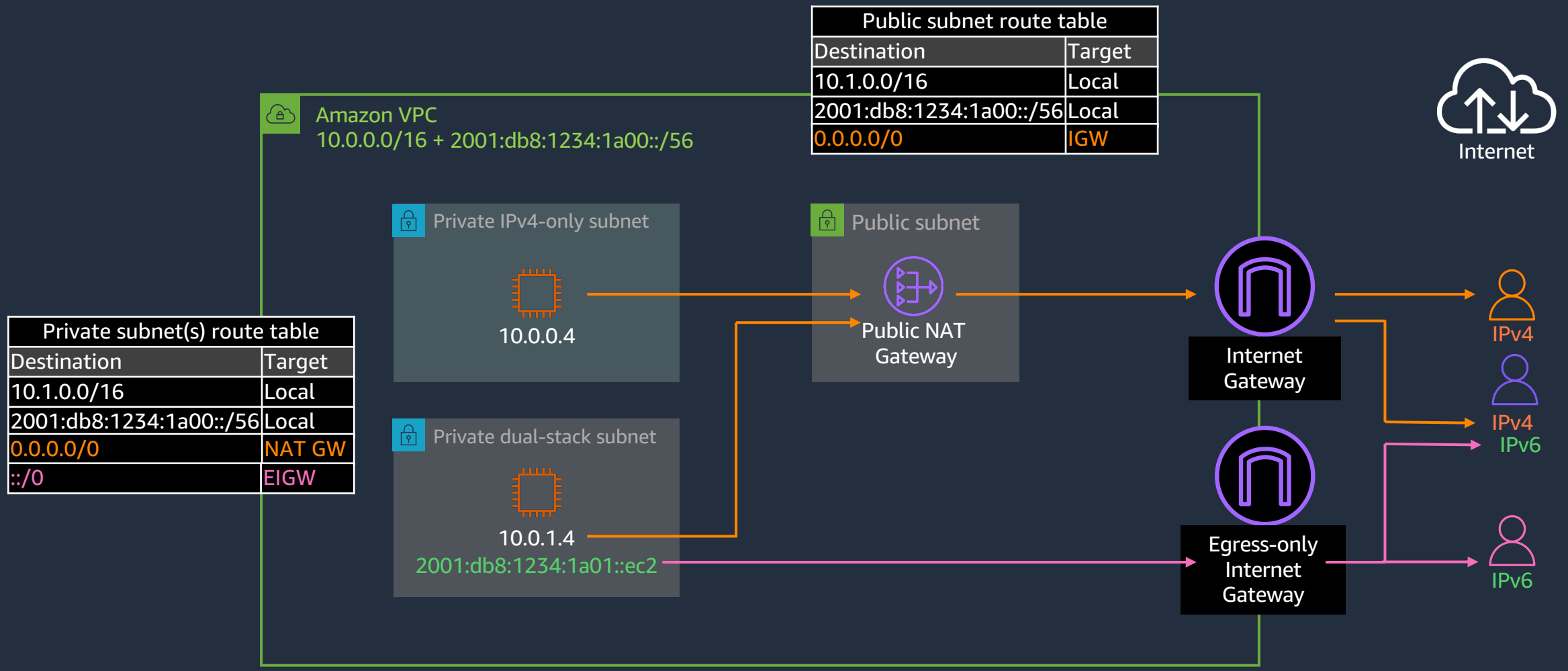
PUBLIC IPV6-ONLY SUBNETS



Private subnets internet connectivity

Amazon dual-stack VPC: Internet connectivity

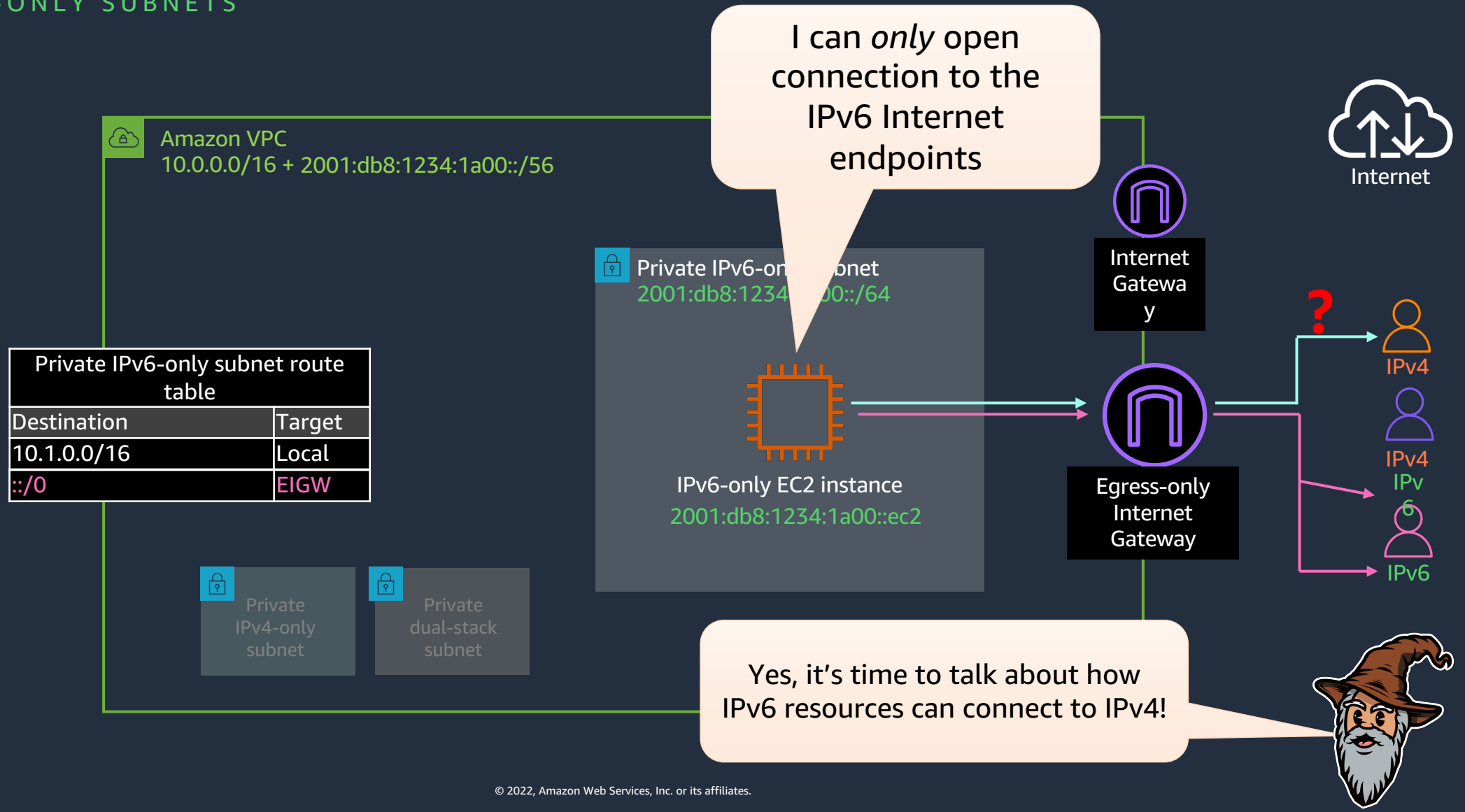
PRIVATE SUBNETS



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

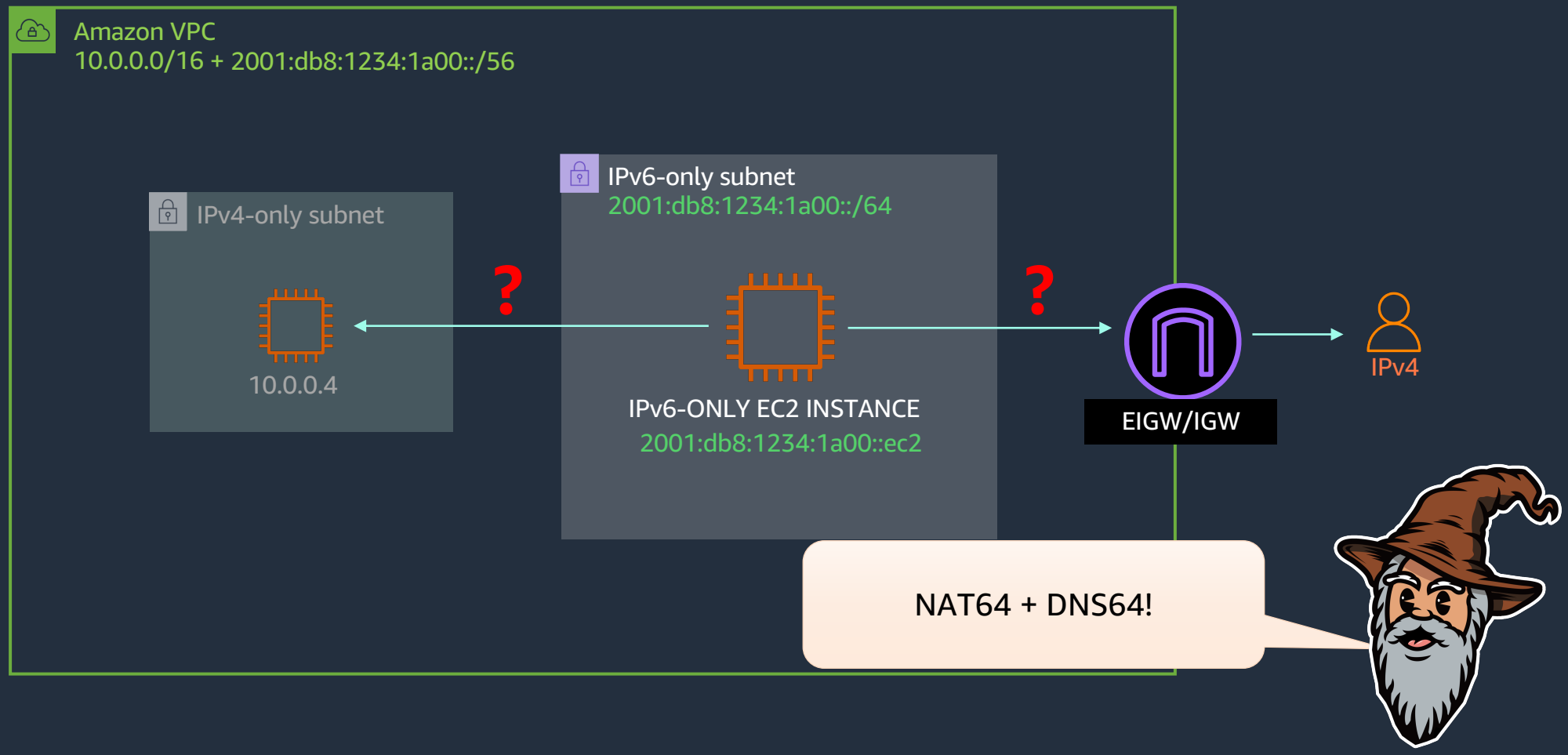
Amazon VPC

IPv6-only subnets

NAT64 and DNS64

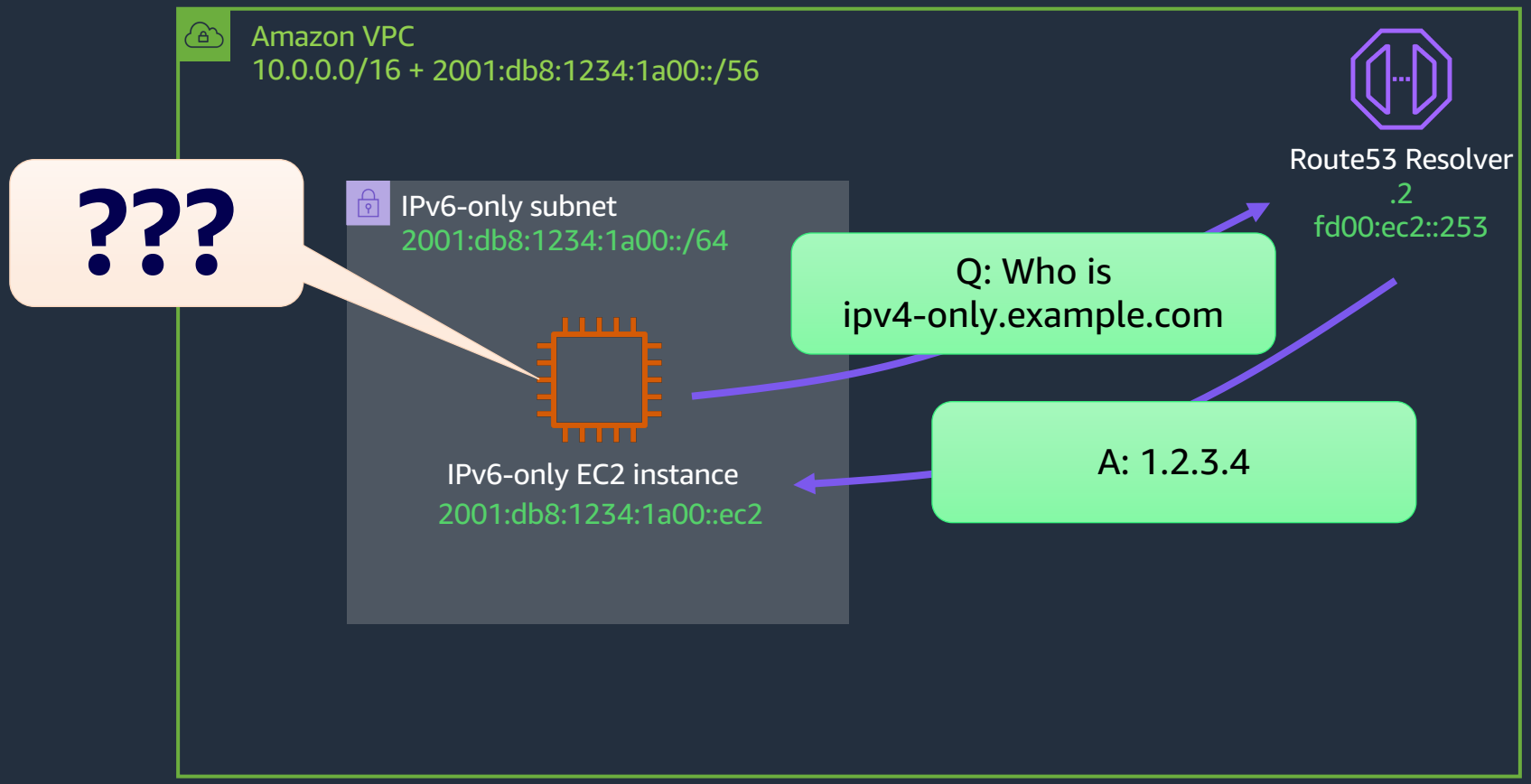
Interoperability with IPv4 environments

Amazon dual-stack VPC: IPv6 to IPv4



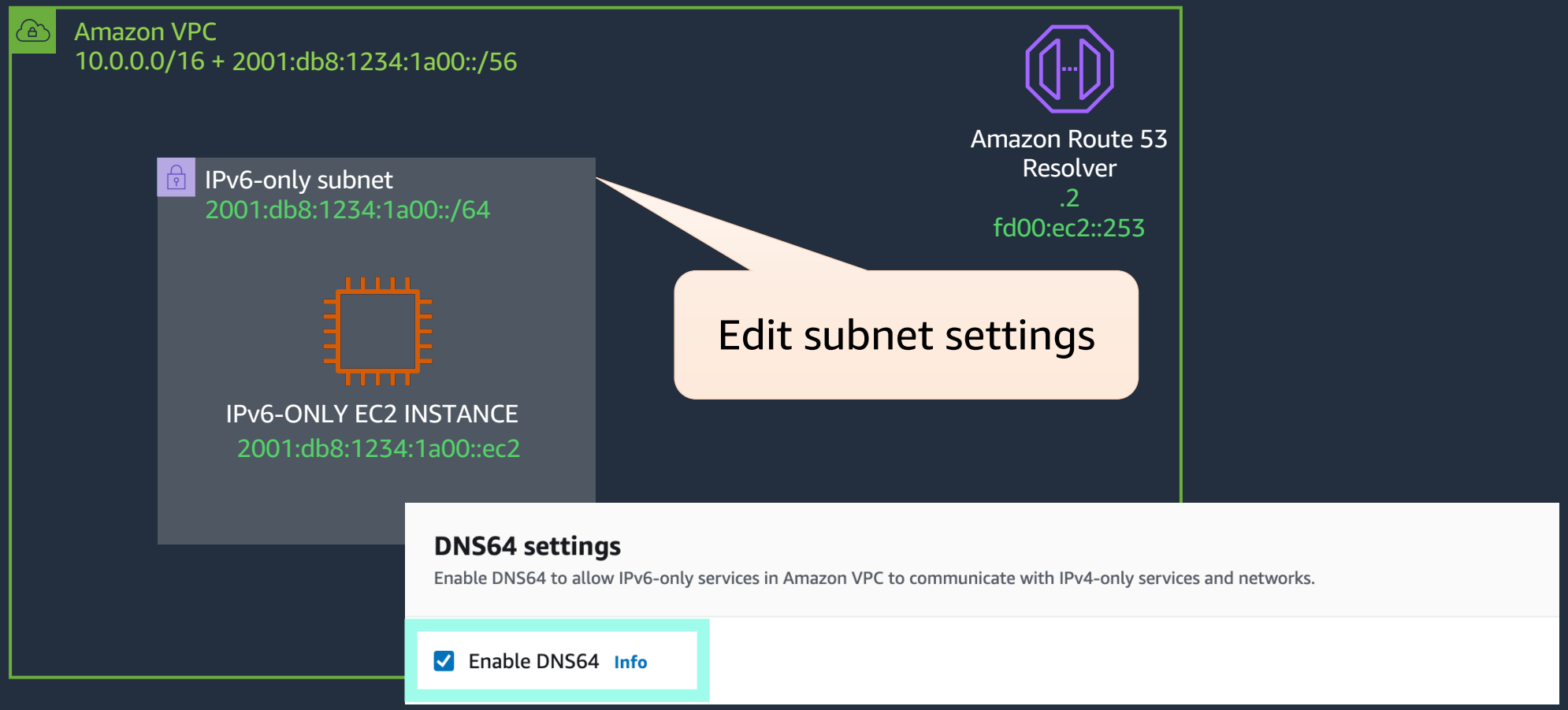
Amazon VPC DNS

BEFORE

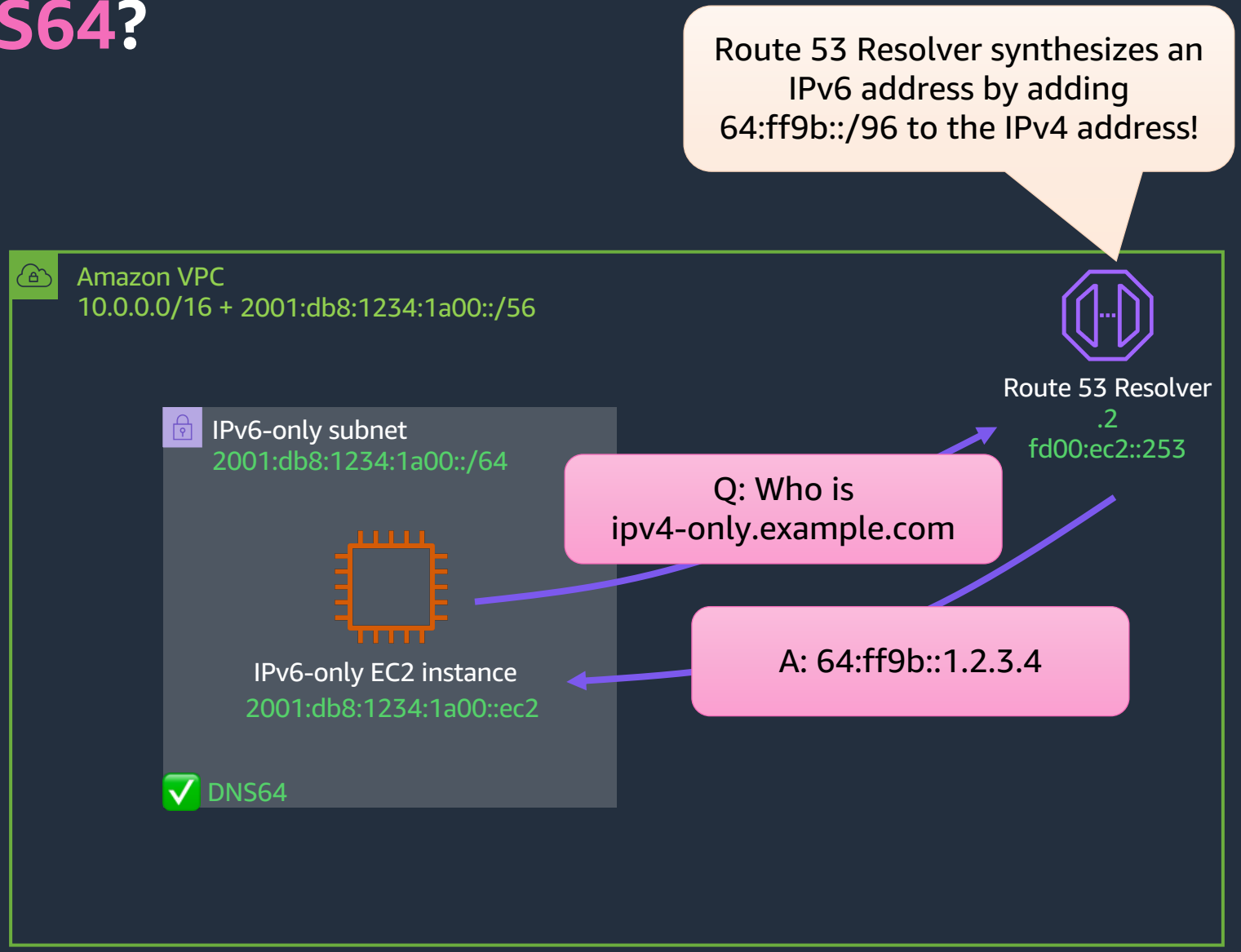


DNS64

What is DNS64?

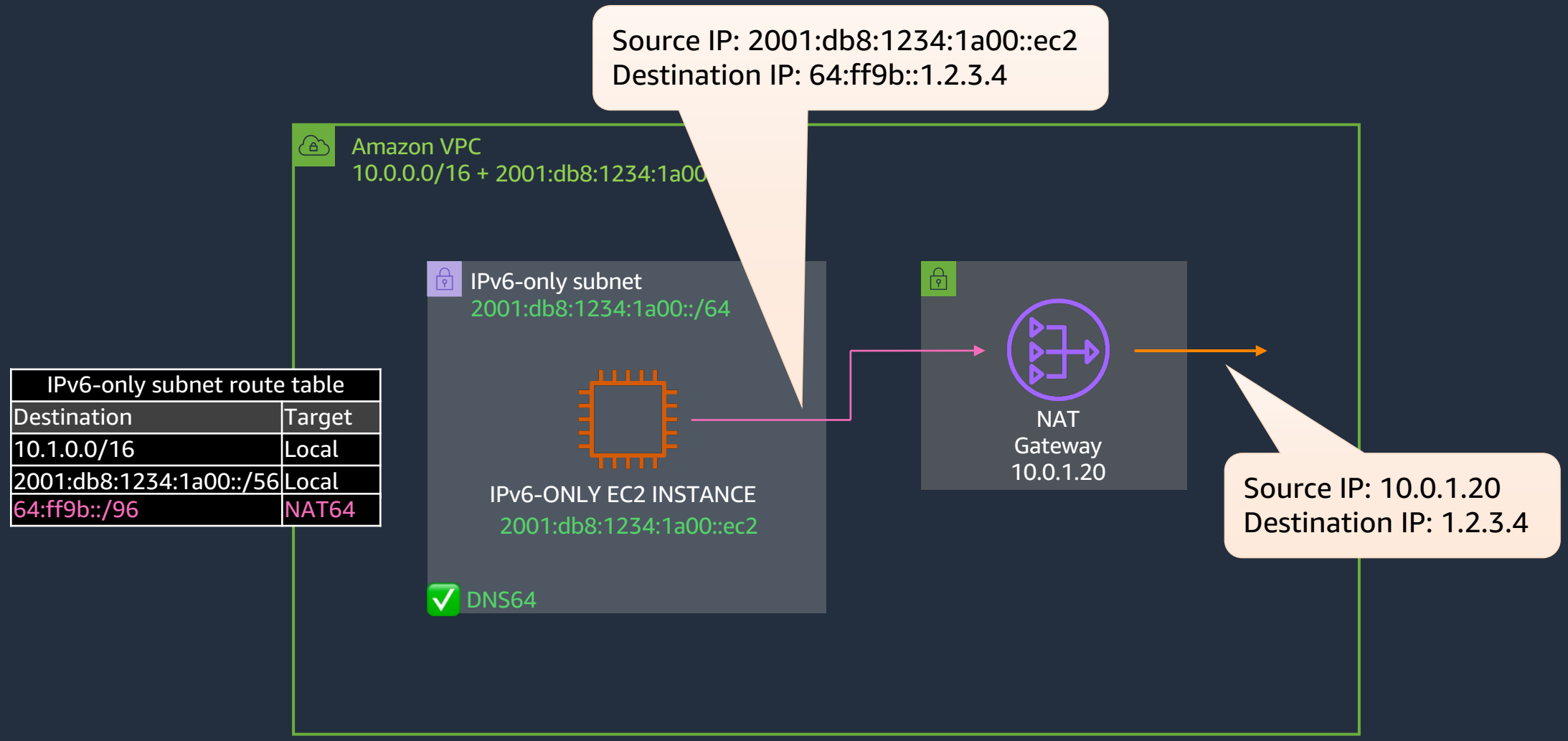


What is DNS64?



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

How does NAT64 work?

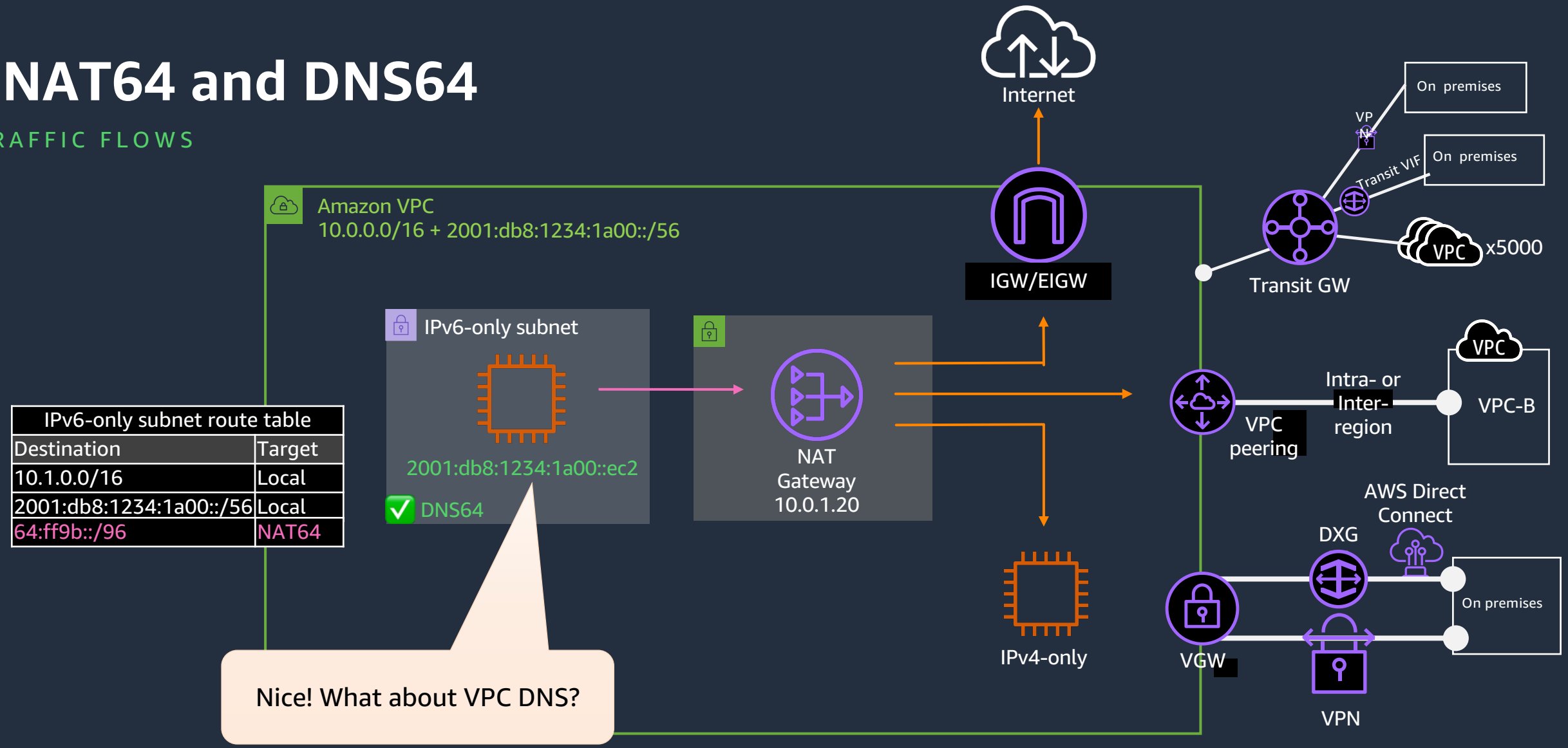


IPv6-only subnet route table	
Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1a00::/56	Local
64:ff9b::/96	NAT64

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

NAT64 and DNS64

TRAFFIC FLOWS



IPv6

Amazon VPC

IPv6-only subnets

NAT64 and DNS64

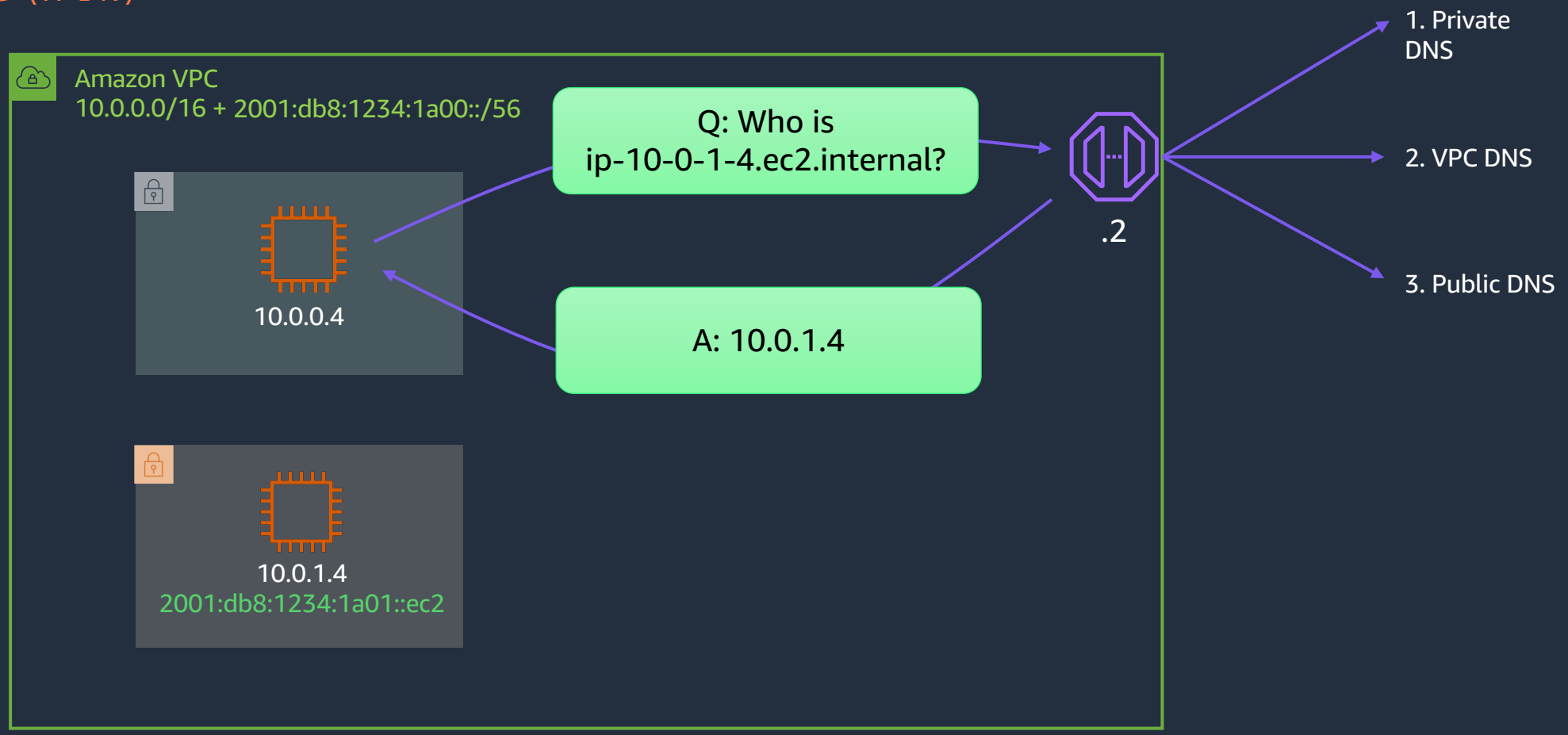
Interoperability with IPv4 environments

Amazon EC2

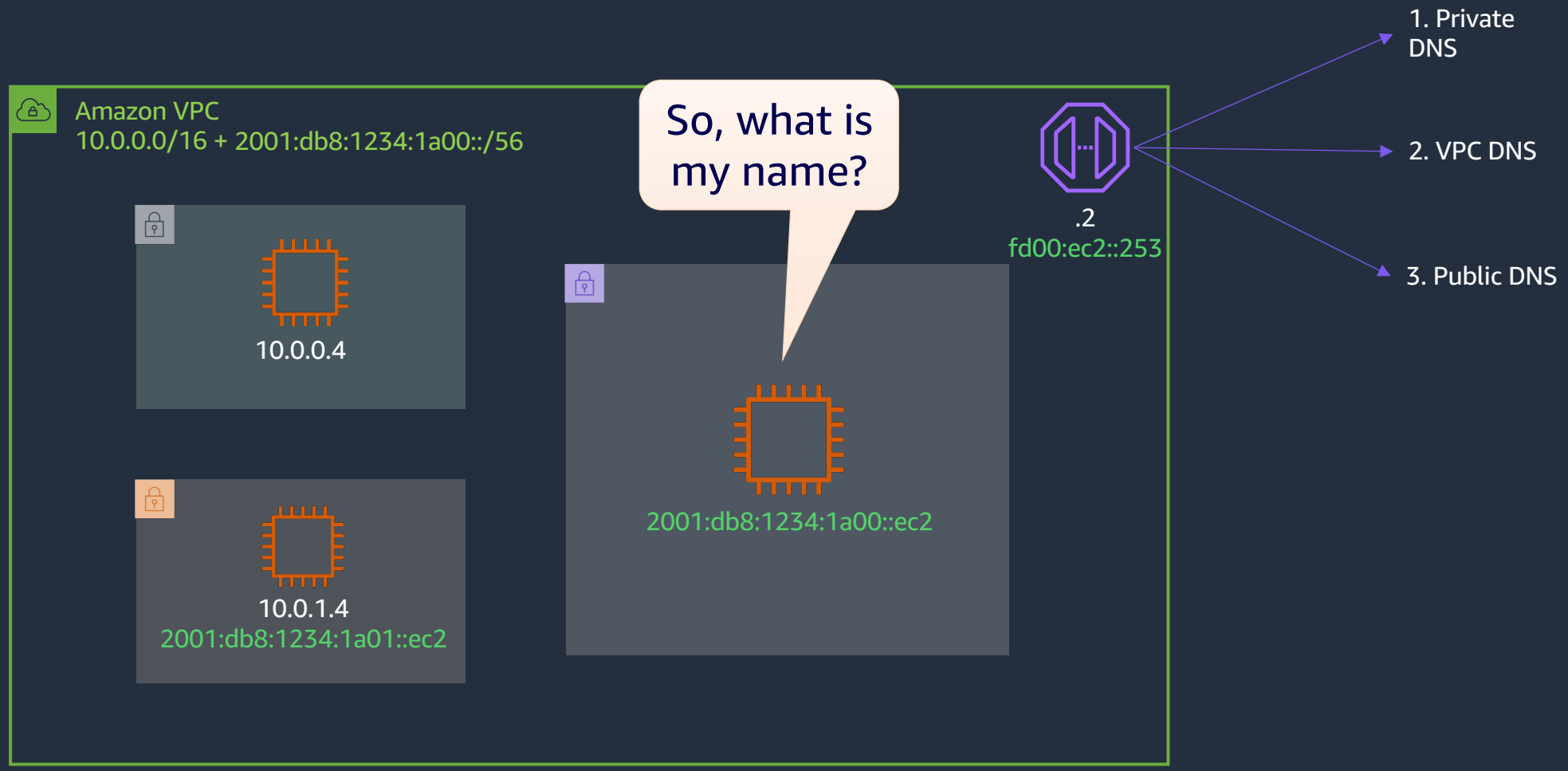
Resource-based instance naming

Amazon EC2 instance naming

IPV4-BASED NAMING (IPBN)

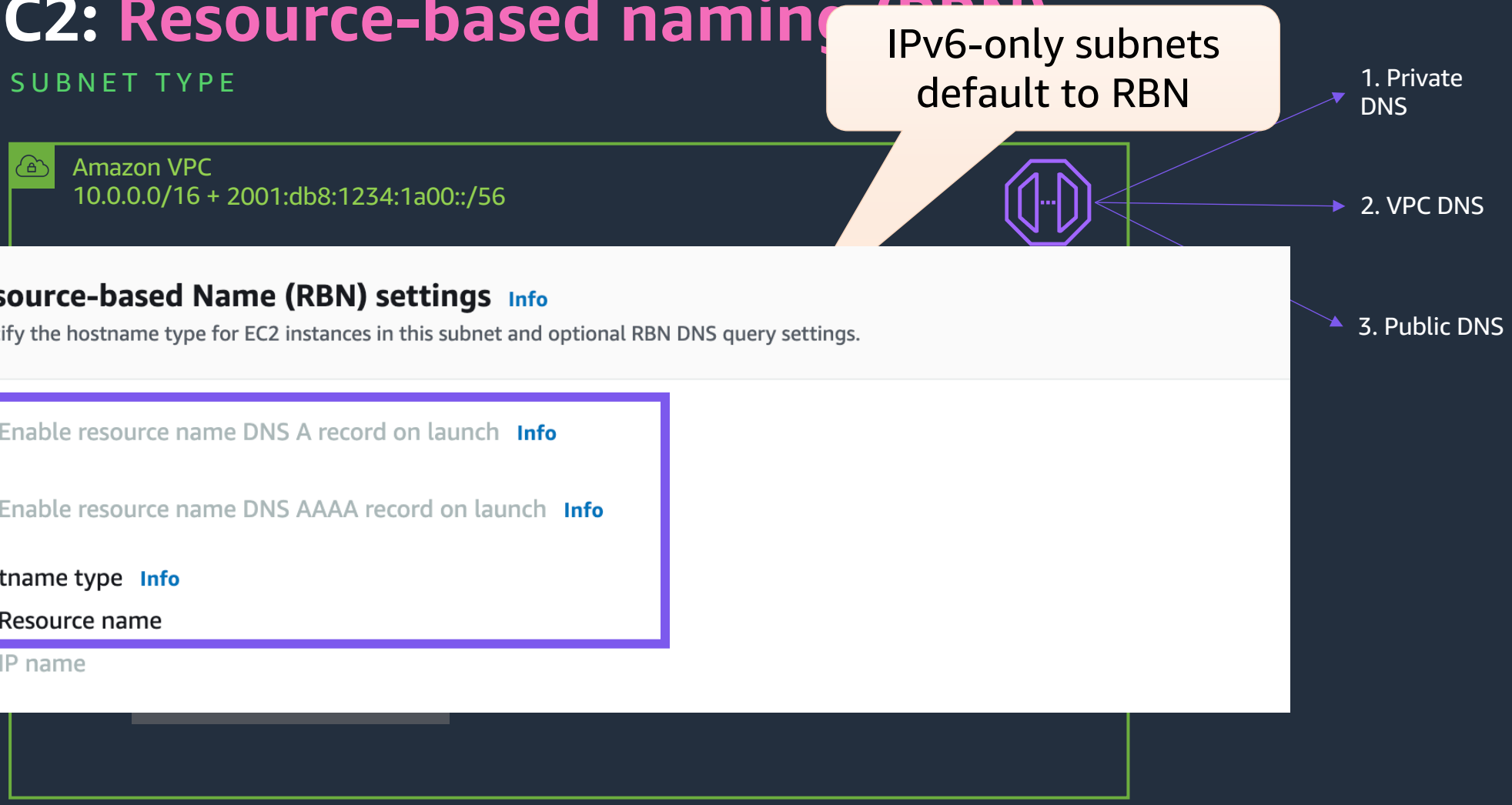


Amazon EC2 instance naming



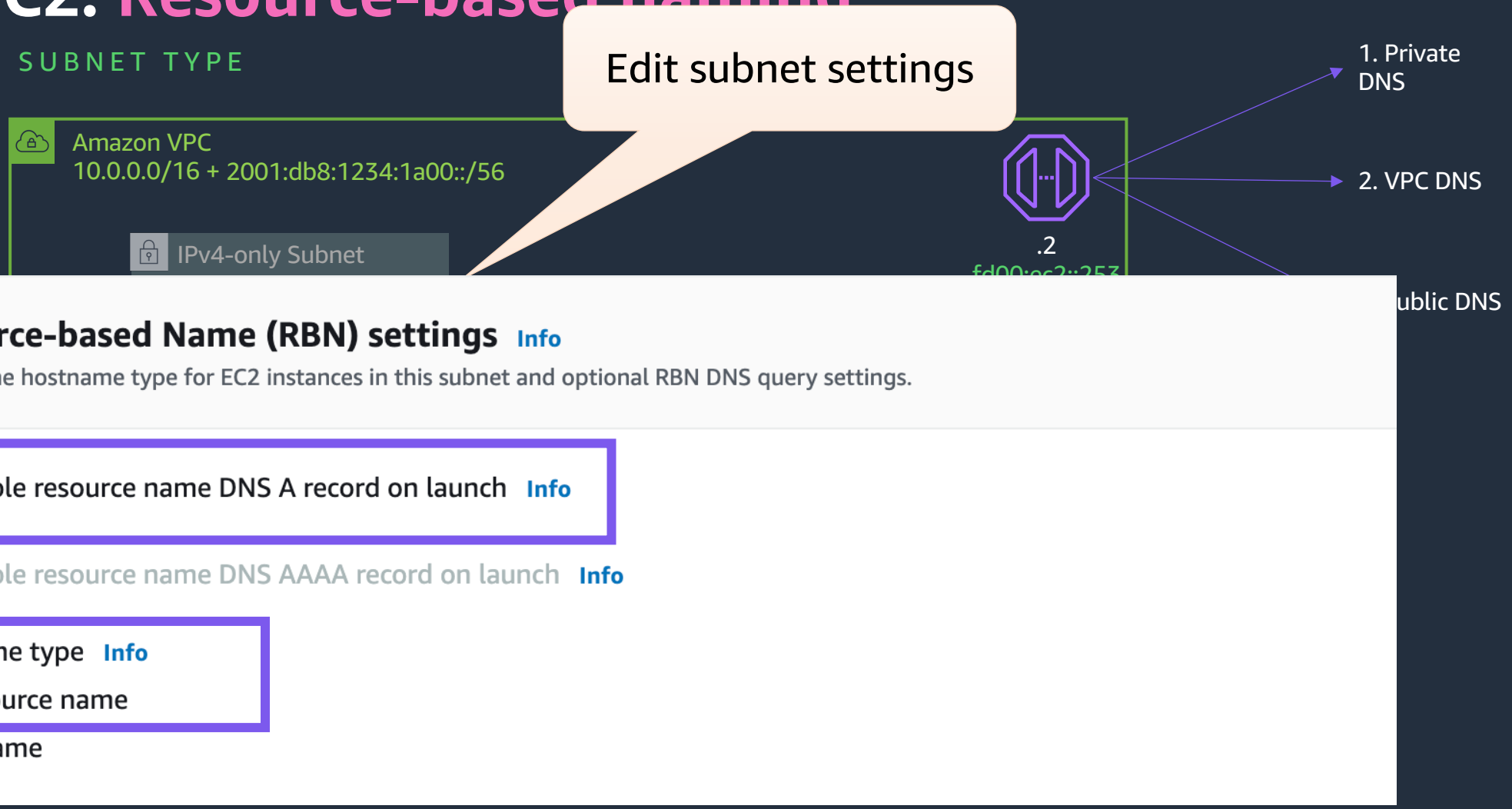
Amazon EC2: Resource-based naming (RBN)

SETTINGS FOR EACH SUBNET TYPE



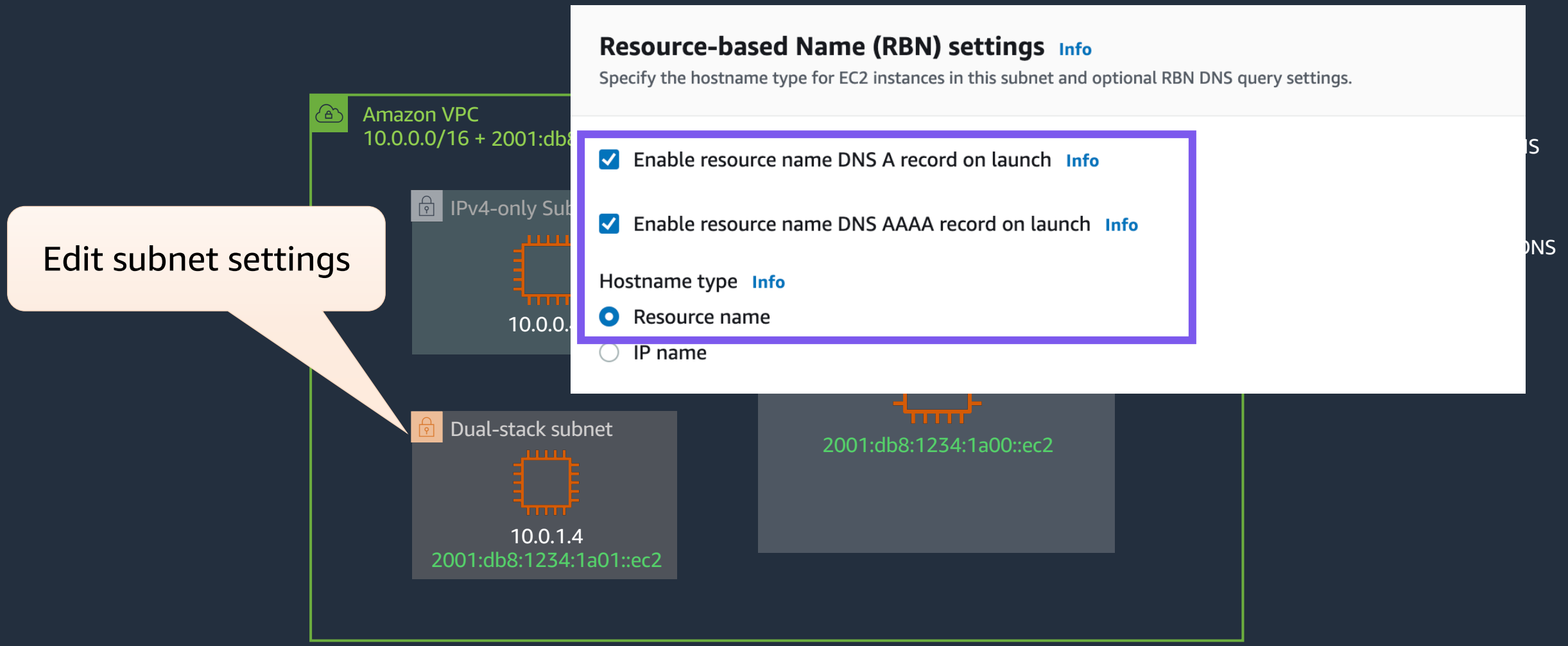
Amazon EC2: Resource-based naming

SETTINGS FOR EACH SUBNET TYPE

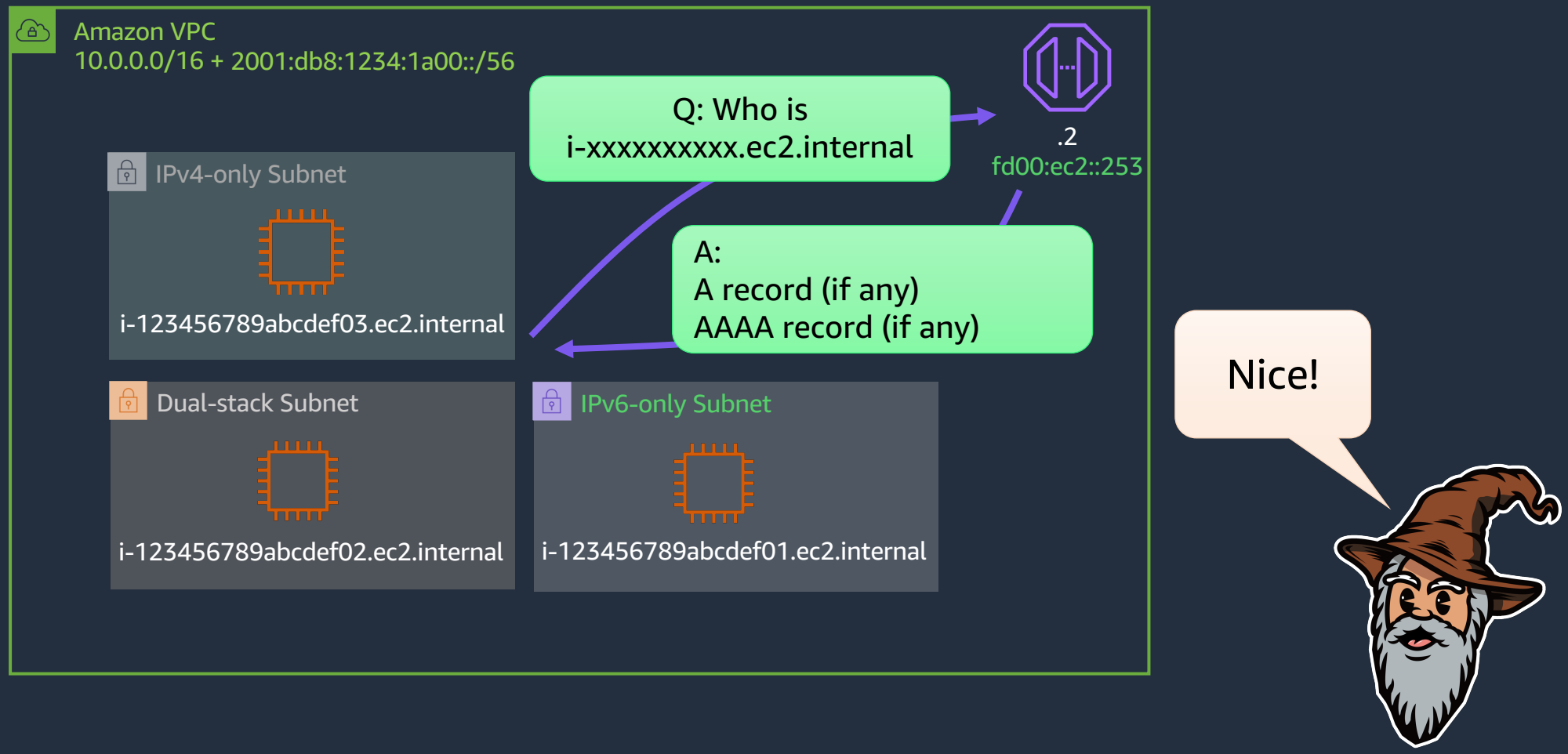


Amazon EC2: Resource-based naming

SETTINGS FOR EACH SUBNET TYPE



Amazon EC2: Resource-based naming



IPv6

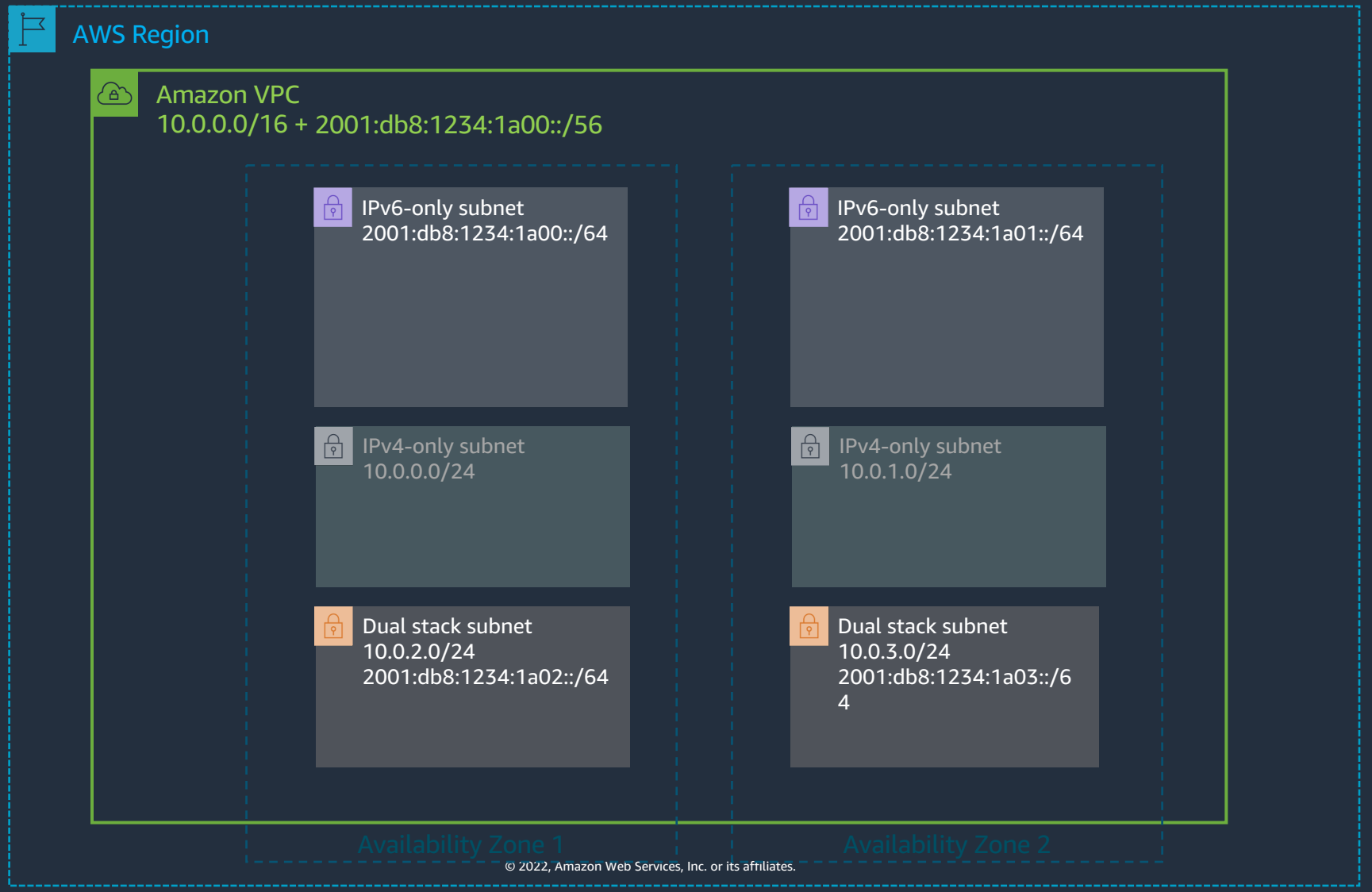
Amazon VPC
IPv6-only subnets

NAT64 and DNS64
Interoperability with IPv4 environments

Amazon EC2
Resource-based instance naming

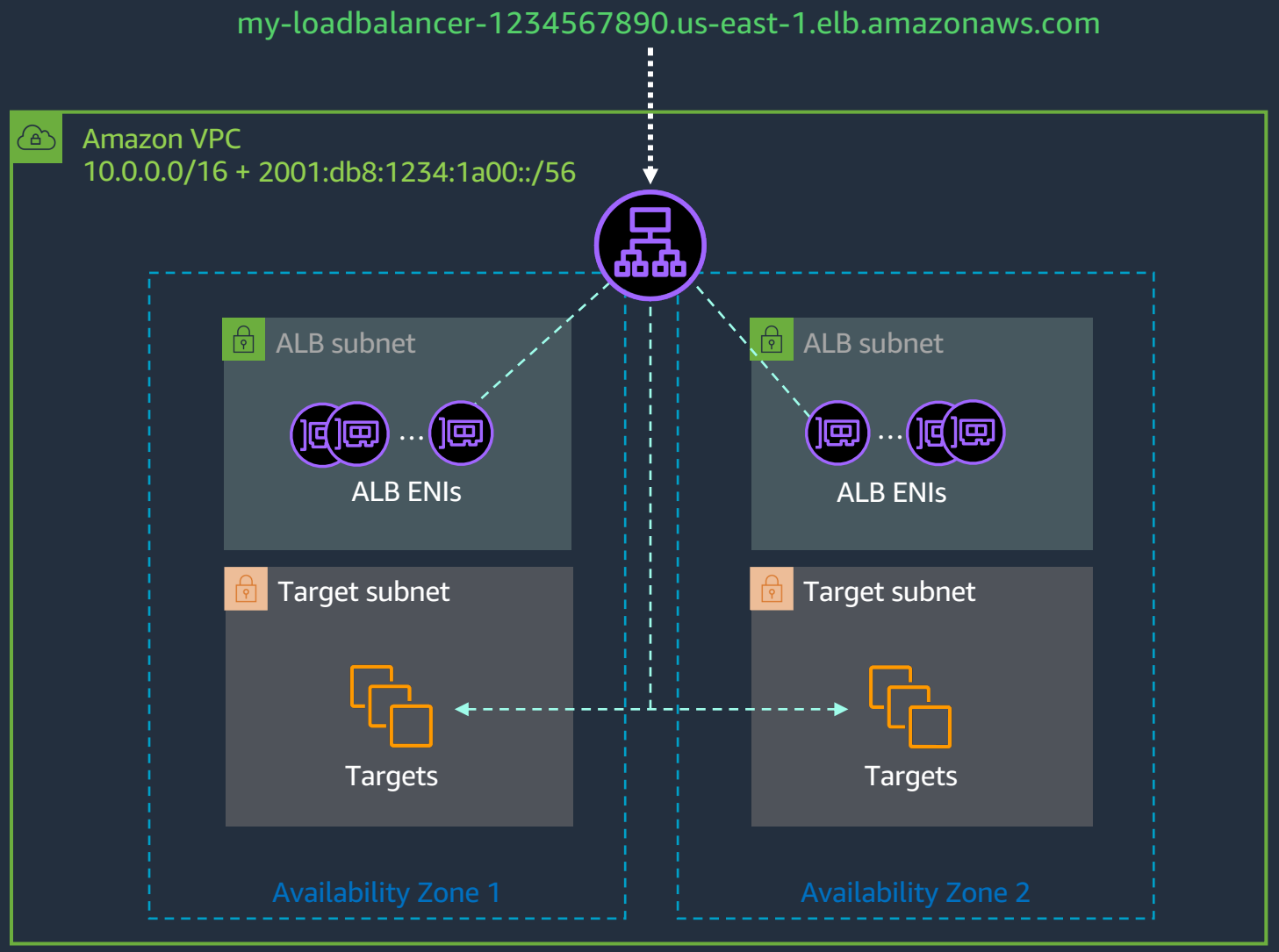
Elastic Load Balancing
Full Dual-stack IPv6 support

Starting from the dual-stack VPC



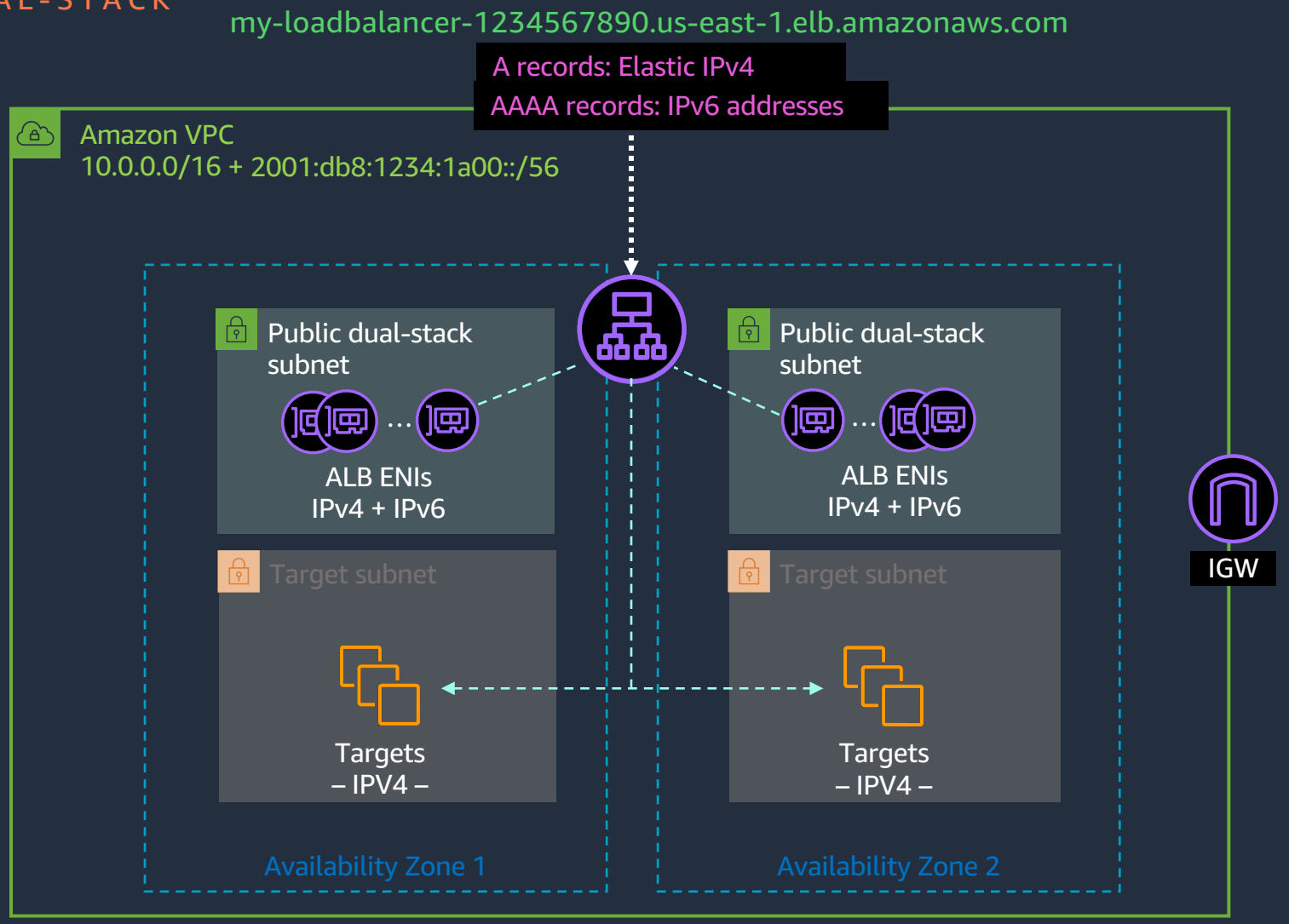
Application Load Balancer (ALB)

Application Load Balancer: Deployment



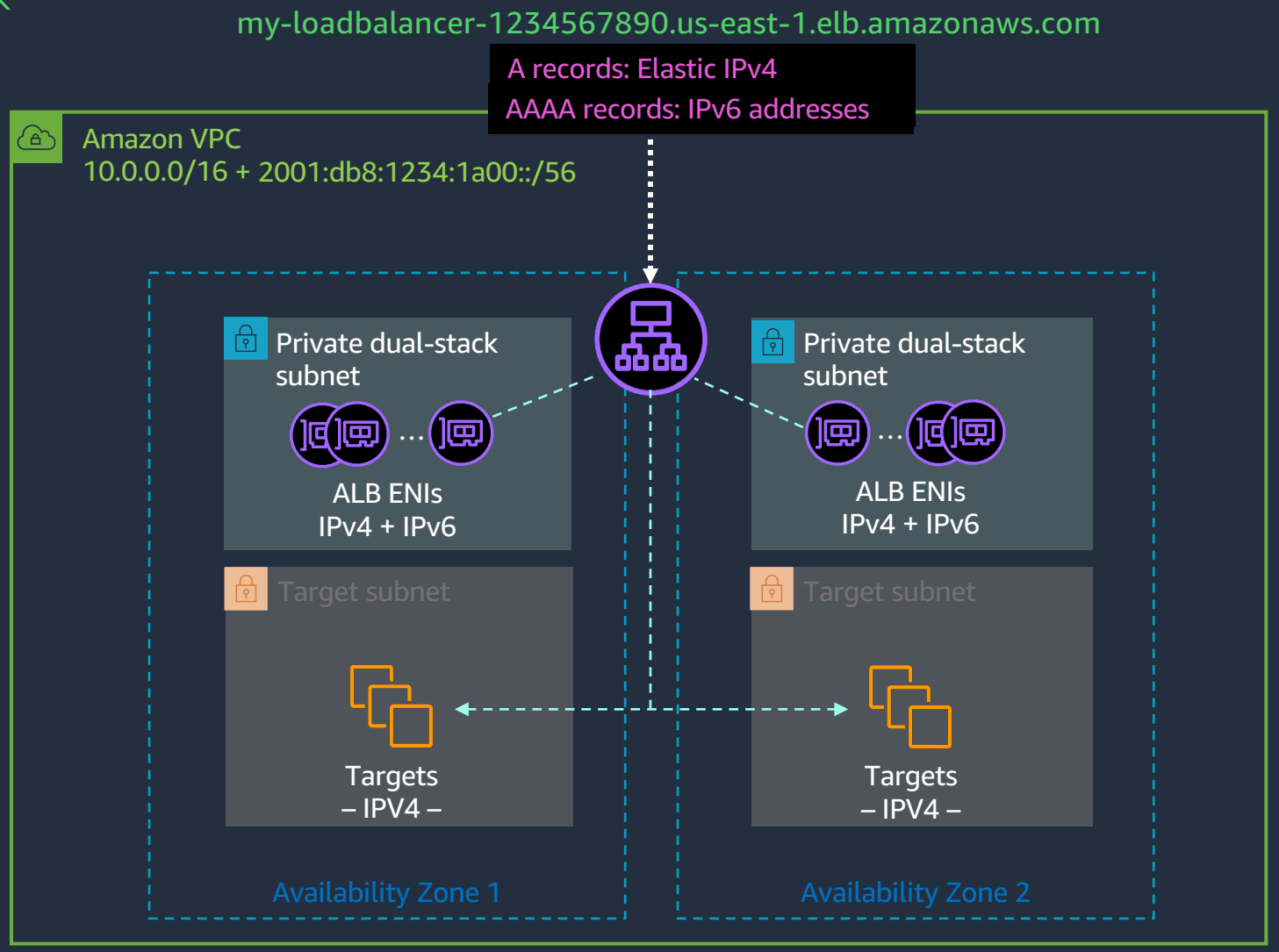
Application Load Balancer: Dual-stack support

INTERNET-FACING DUAL-STACK



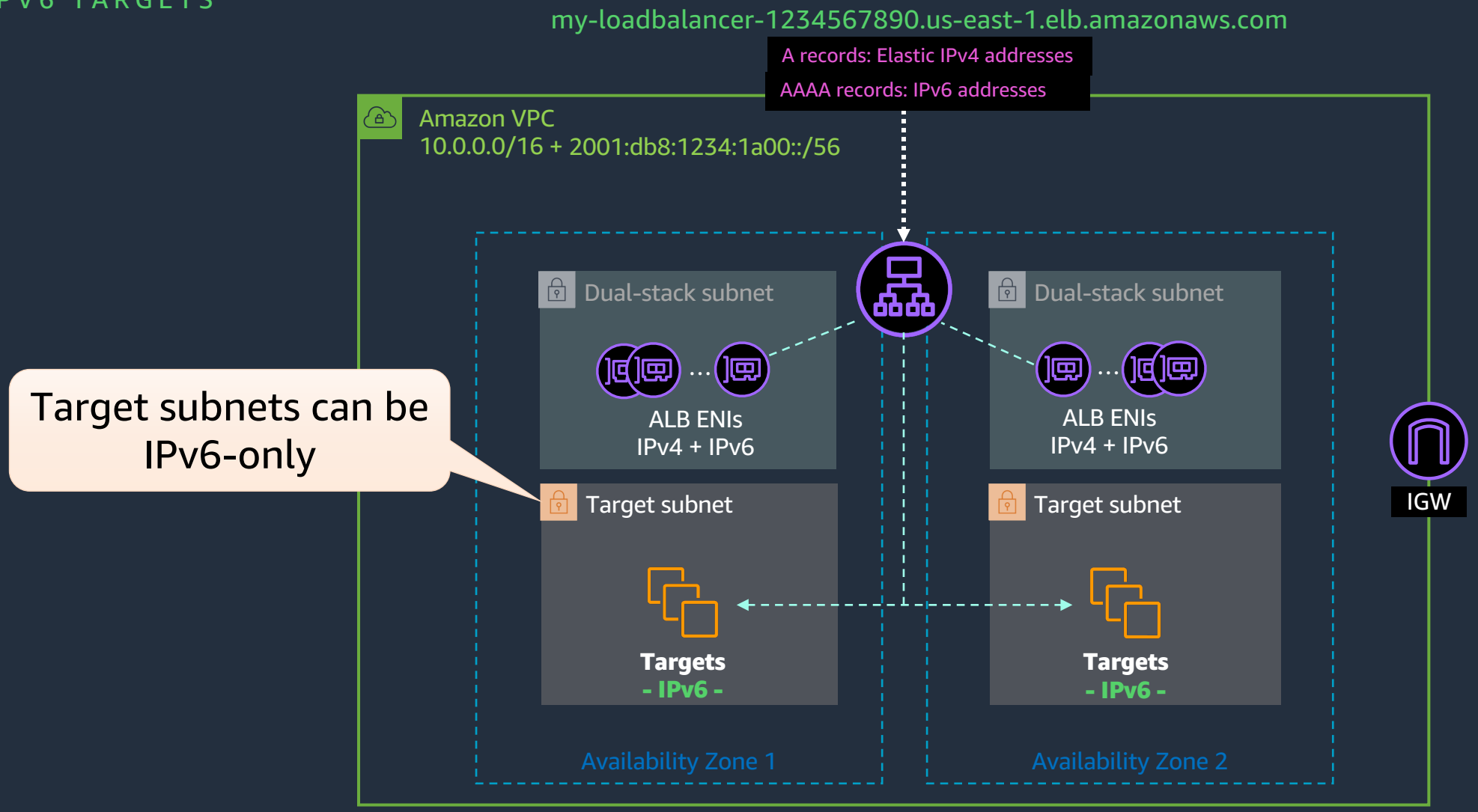
Application Load Balancer: Dual-stack support

INTERNAL DUAL STACK



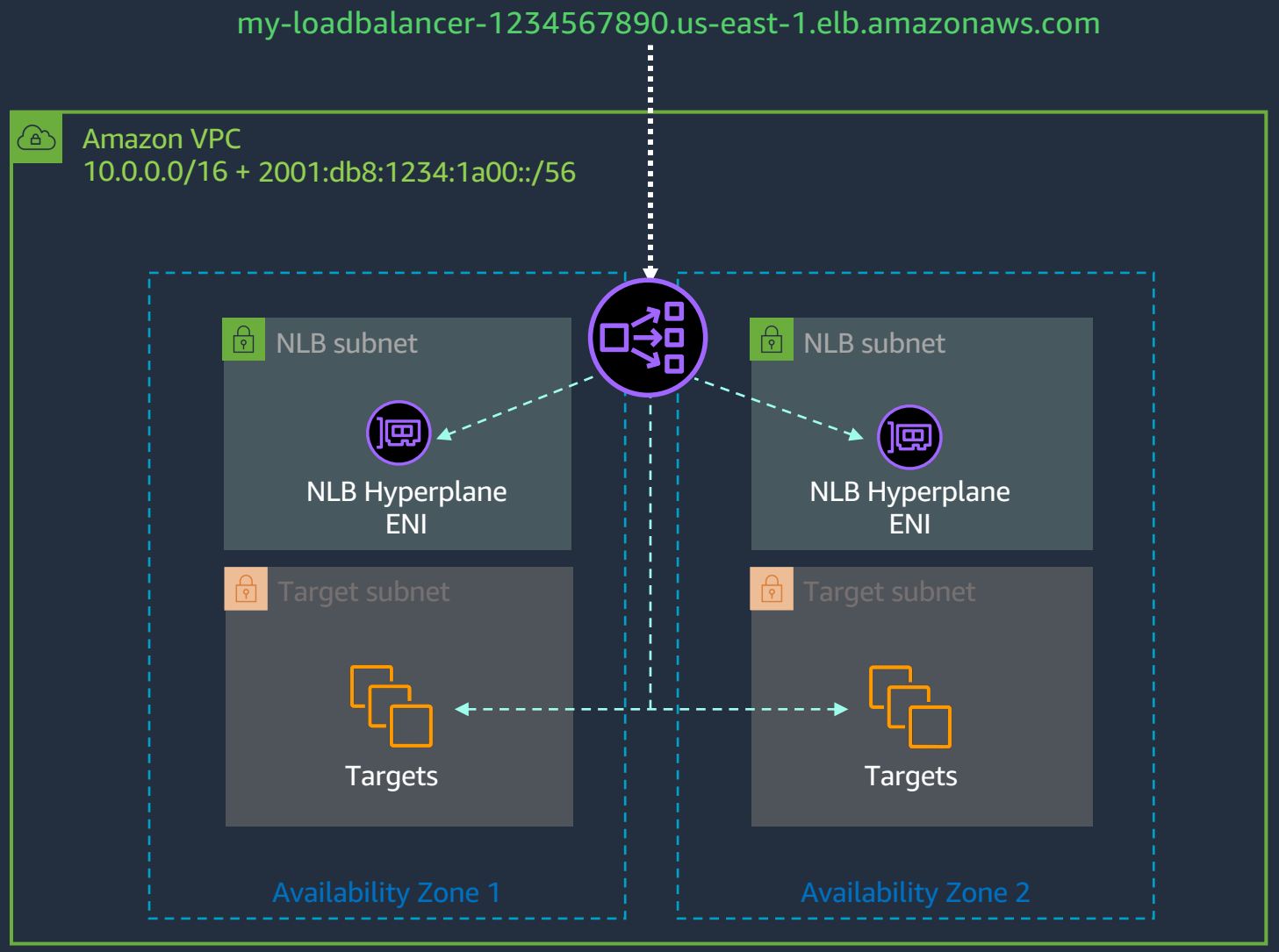
Application Load Balancer: End-to-end IPv6

IPV6 TARGETS



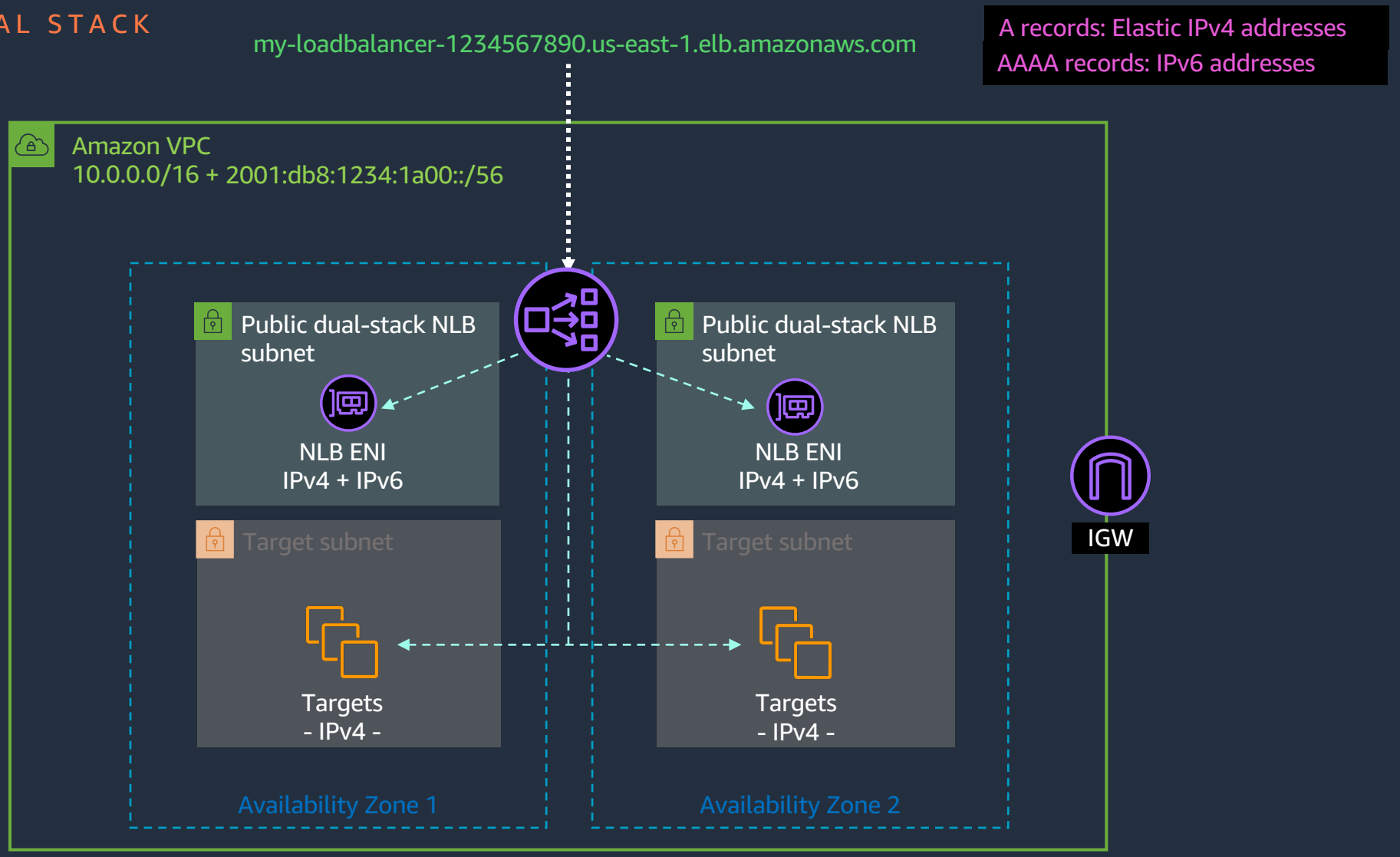
Network Load Balancer (NLB)

Network Load Balancer: Deployment



Network Load Balancer: Dual-stack support

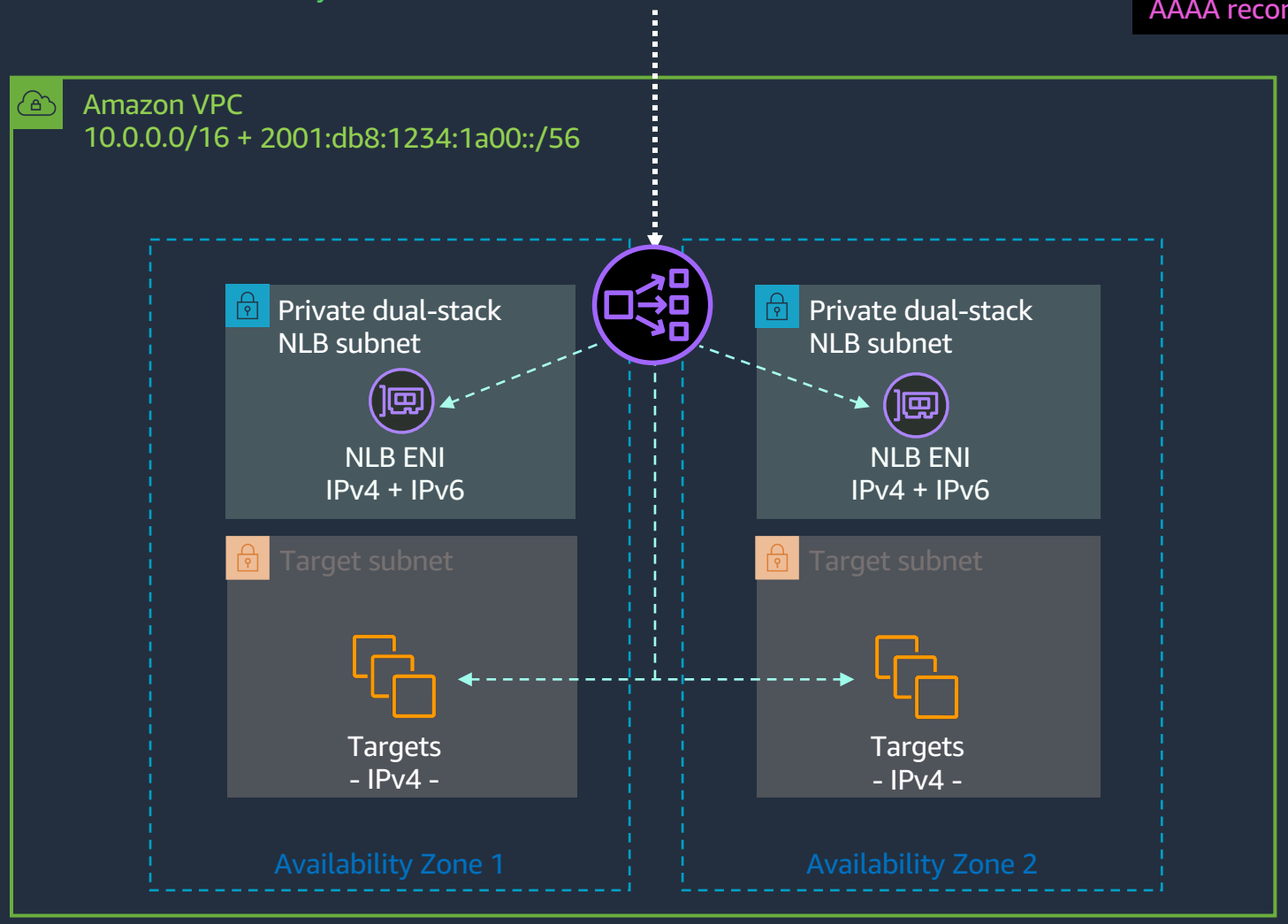
INTERNET-FACING DUAL STACK



Network Load Balancer: Dual-stack support

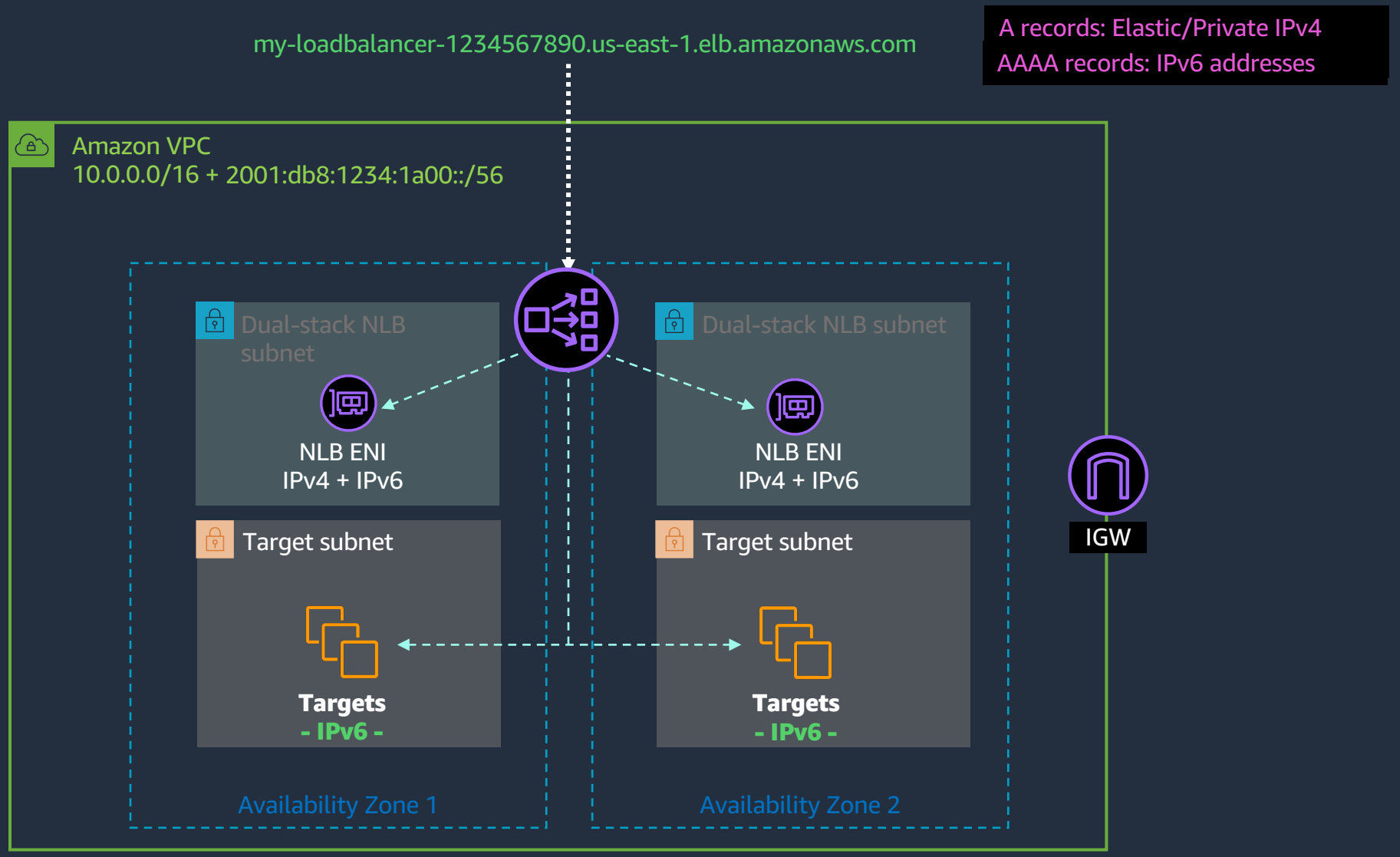
INTERNAL DUAL STACK

A records: Private IPv4 addresses
AAAA records: IPv6 addresses



Network Load Balancer: End-to-end IPv6

IPV6 TARGETS



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?

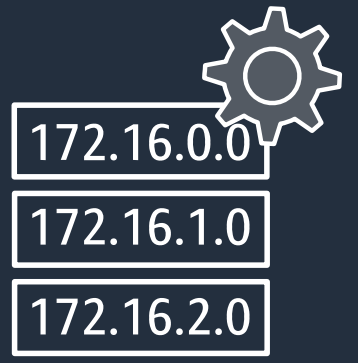
Manual updates of single spreadsheet

Limited visibility into allocation and usage

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

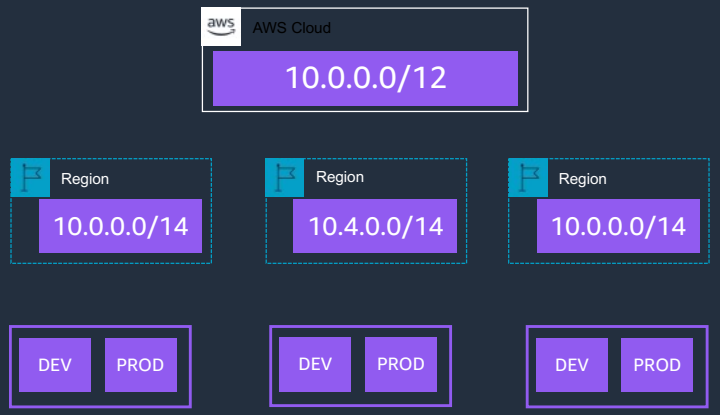
Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends

Retrospective analysis

Allowing decreased time to troubleshoot and audit

aws

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

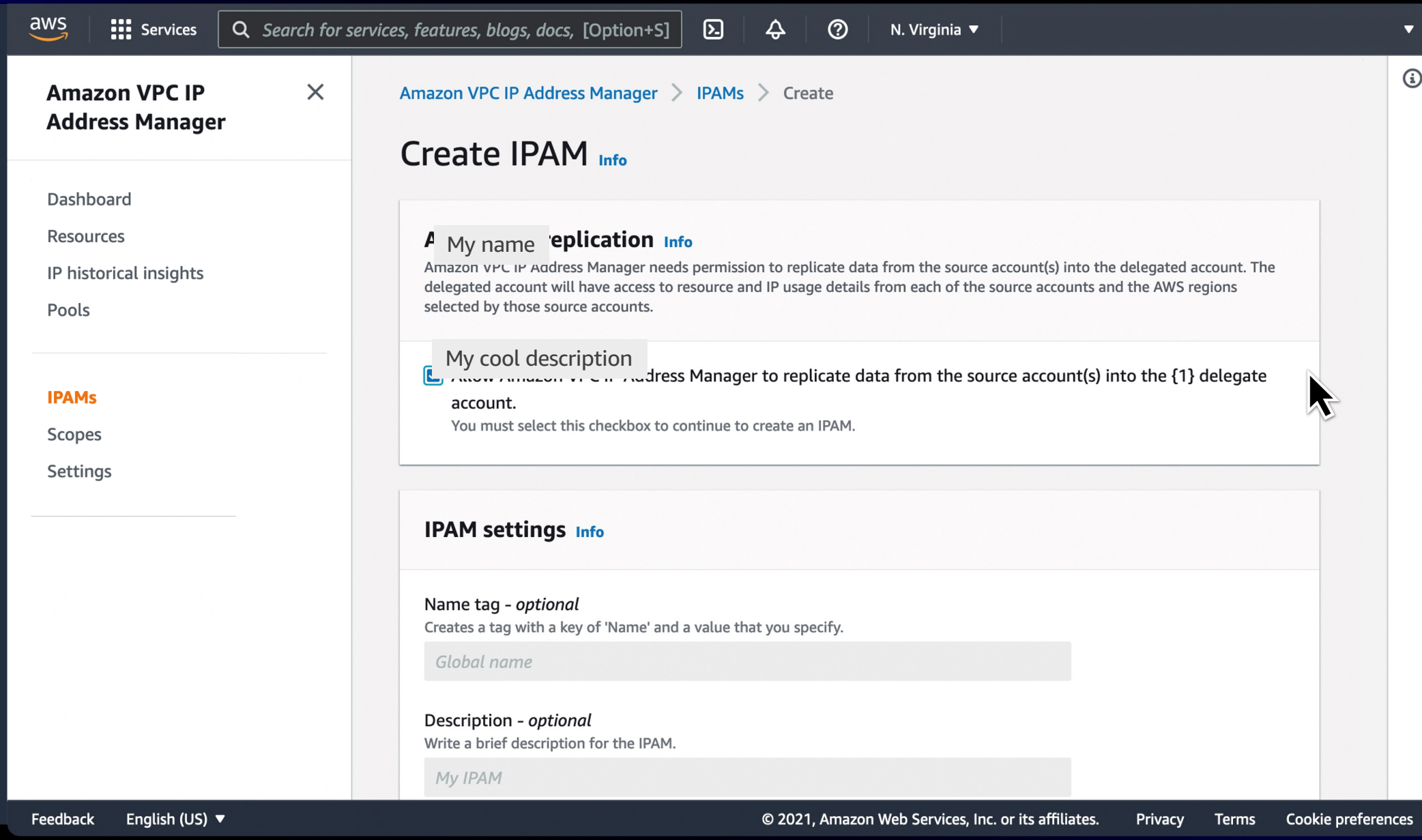
Your refill policy determines how IPAM automatically refills a pool, based on thresholds set by you, from another pool

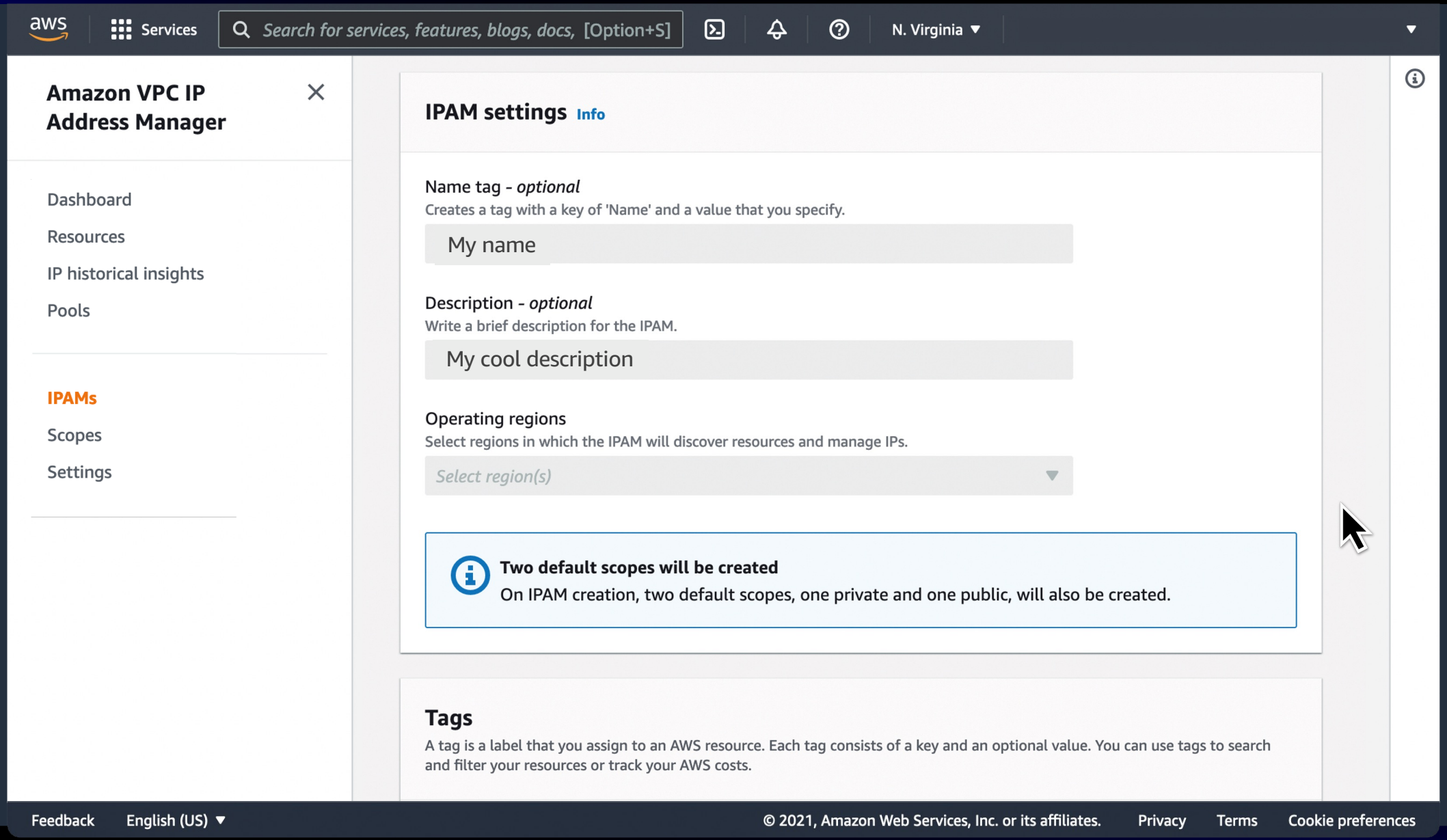
Refill policy helps you to ensure a pool always has IP addresses available for allocation

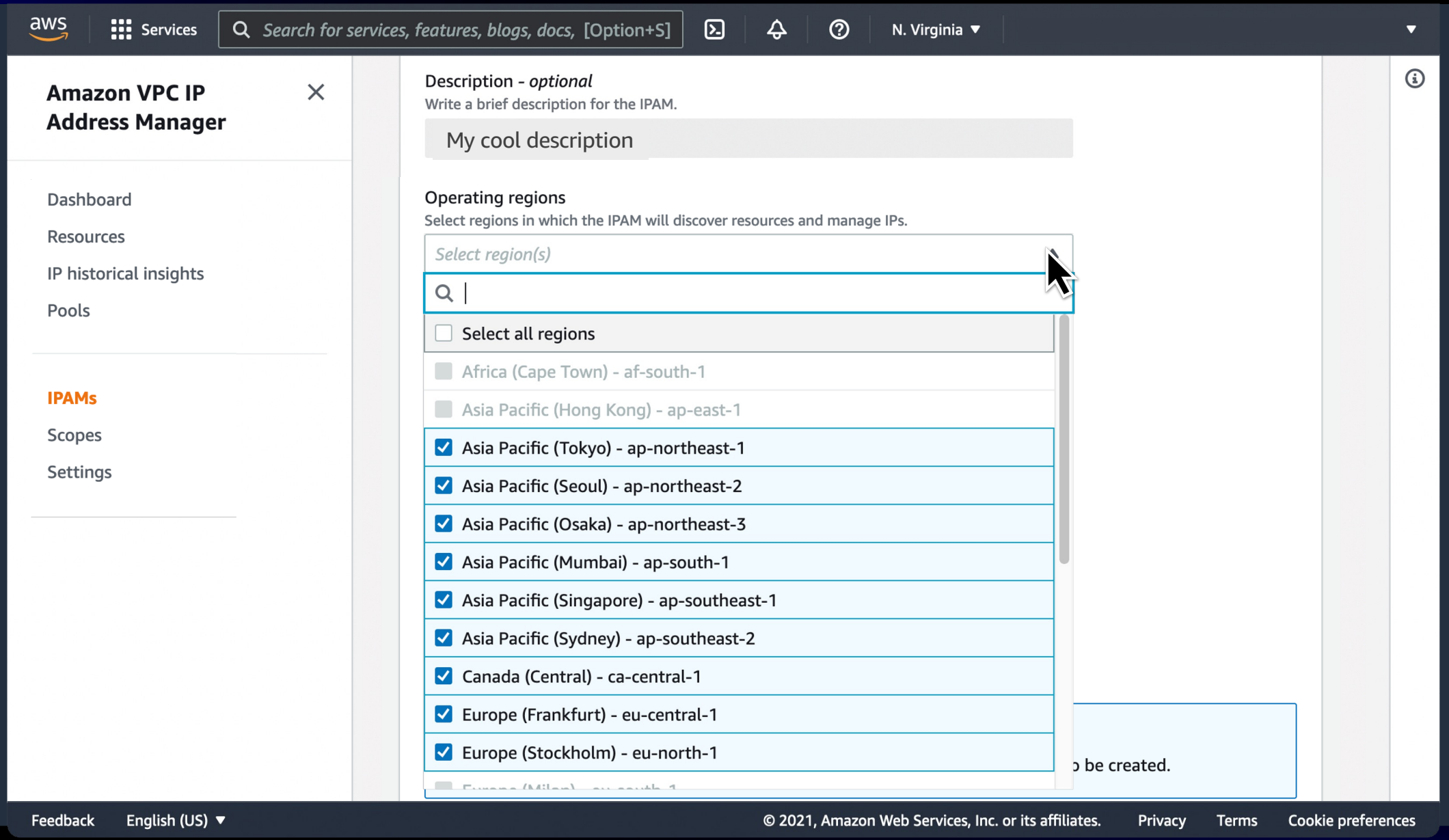
Allocation policy

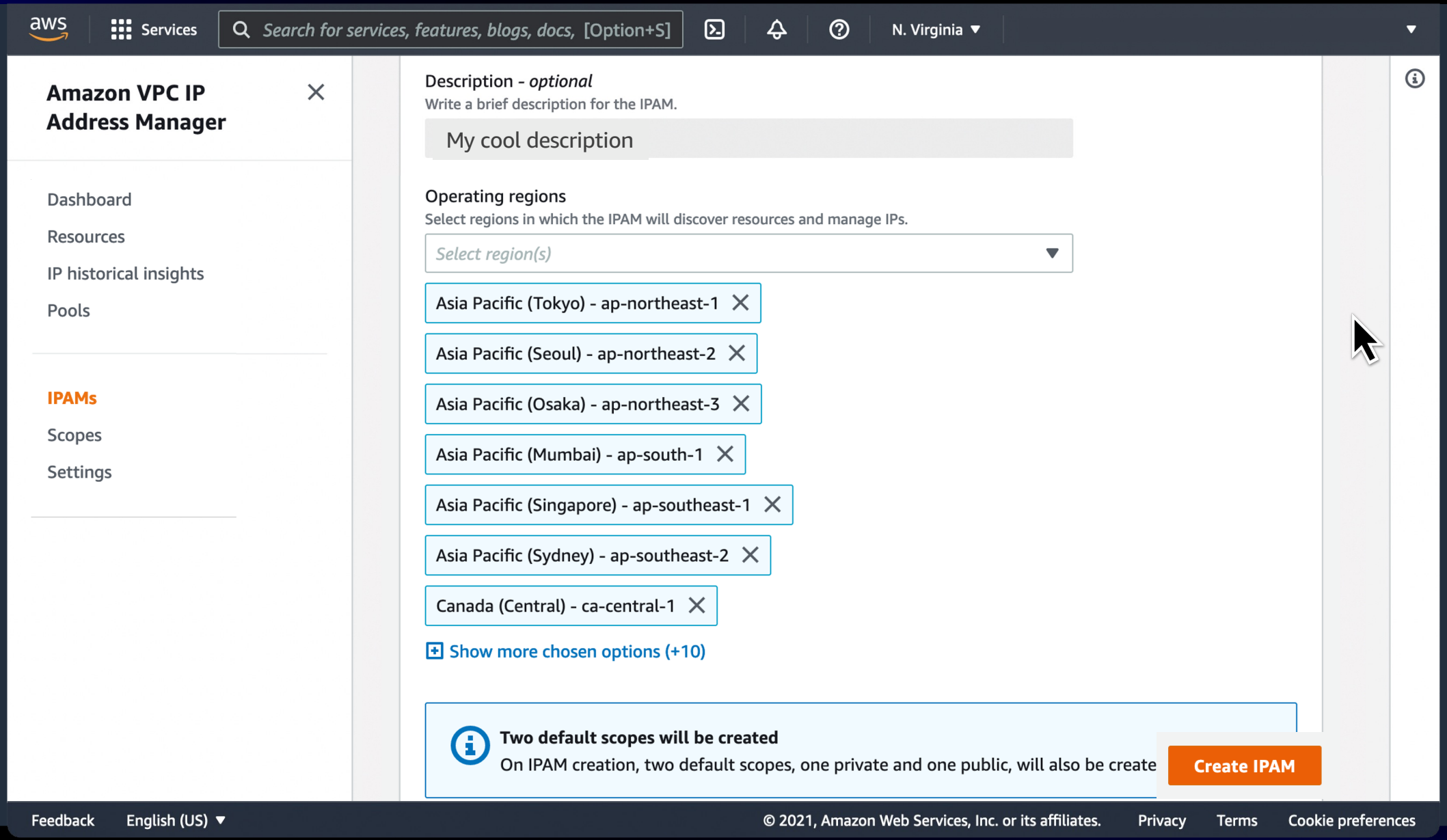
An allocation policy allows you to control IP addresses allocated by IPAM from a pool

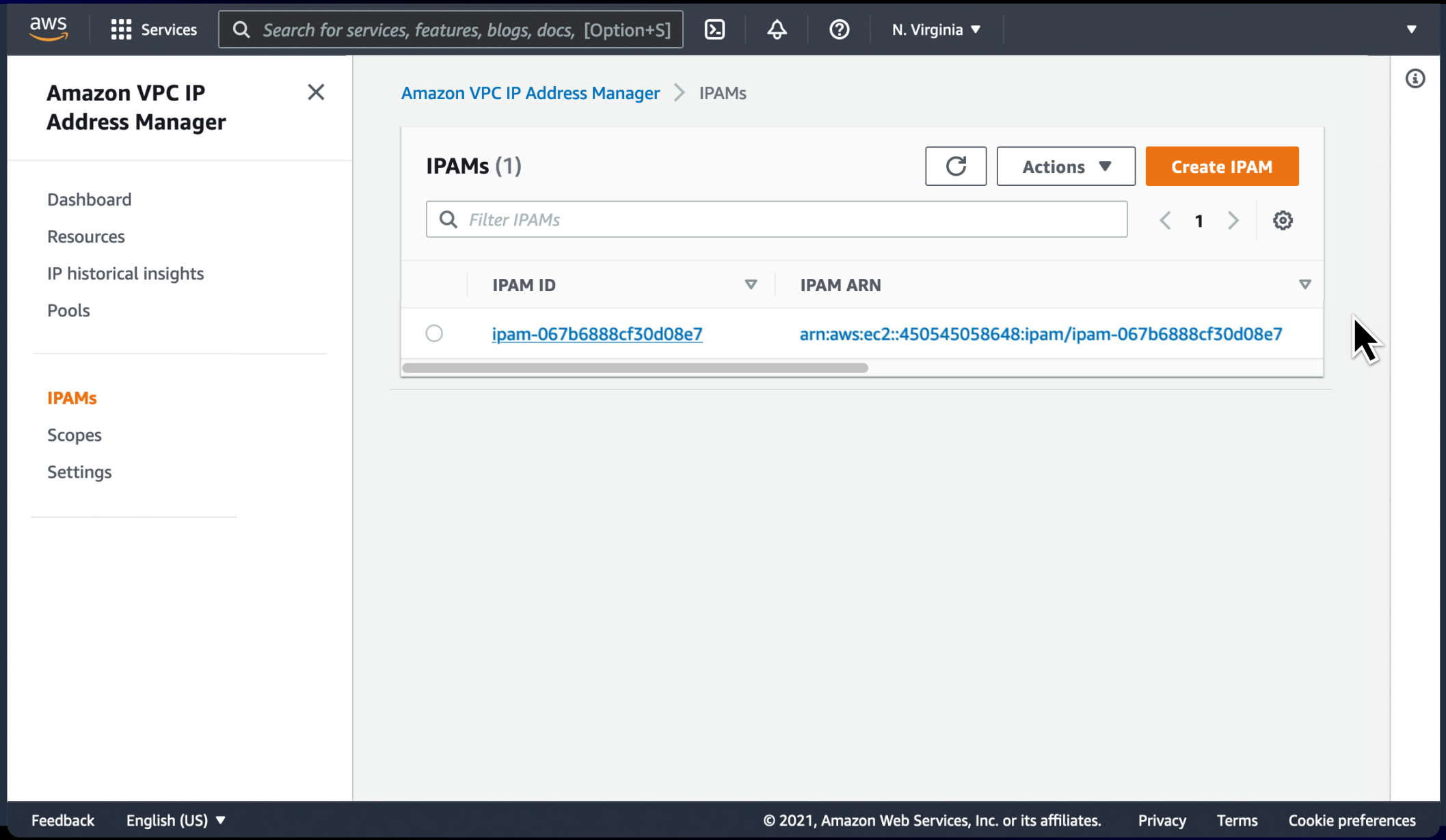
Allocation policy enables you to enforce your business rule when developers ask IPAM for IP addresses for their resources

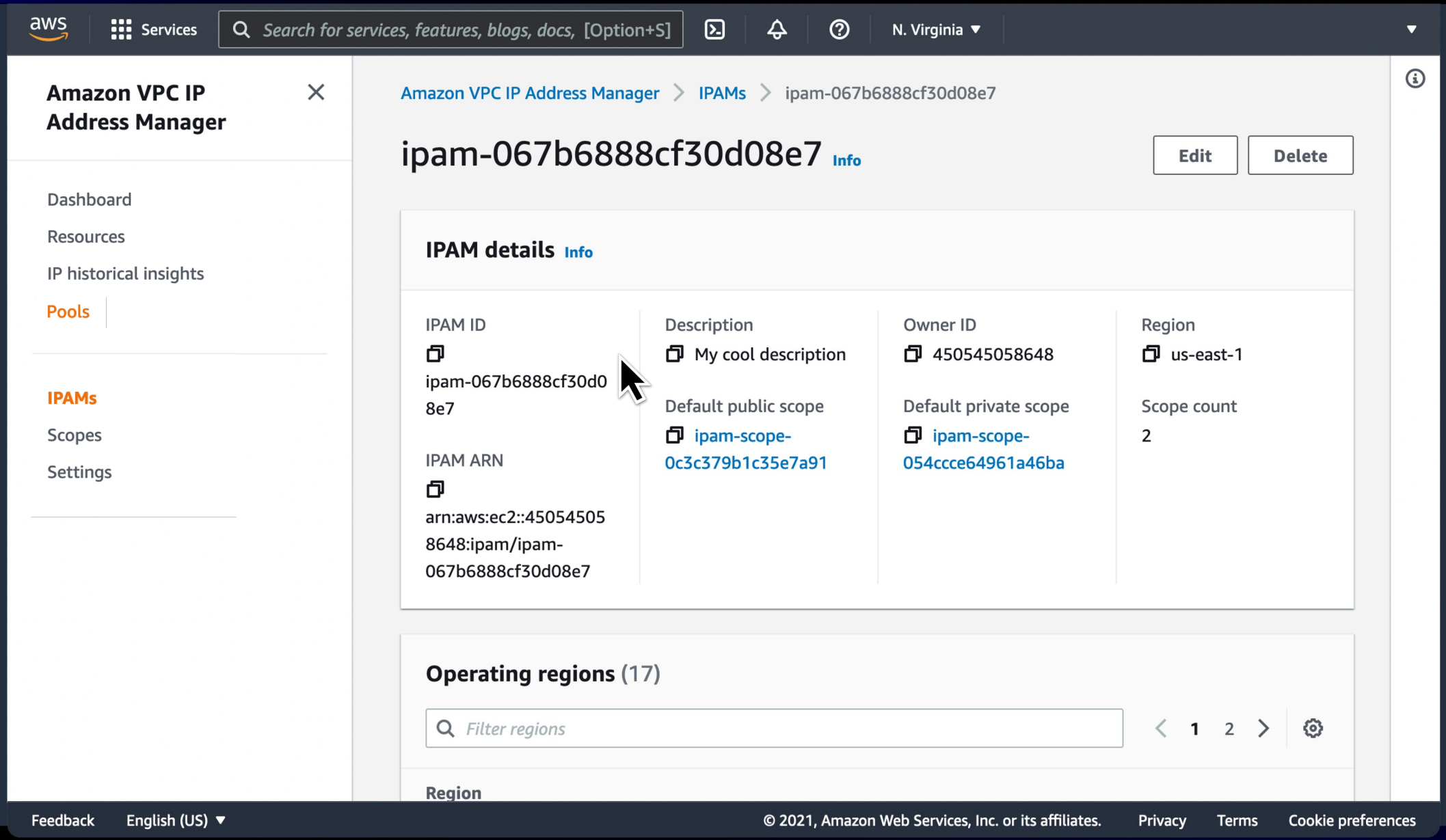


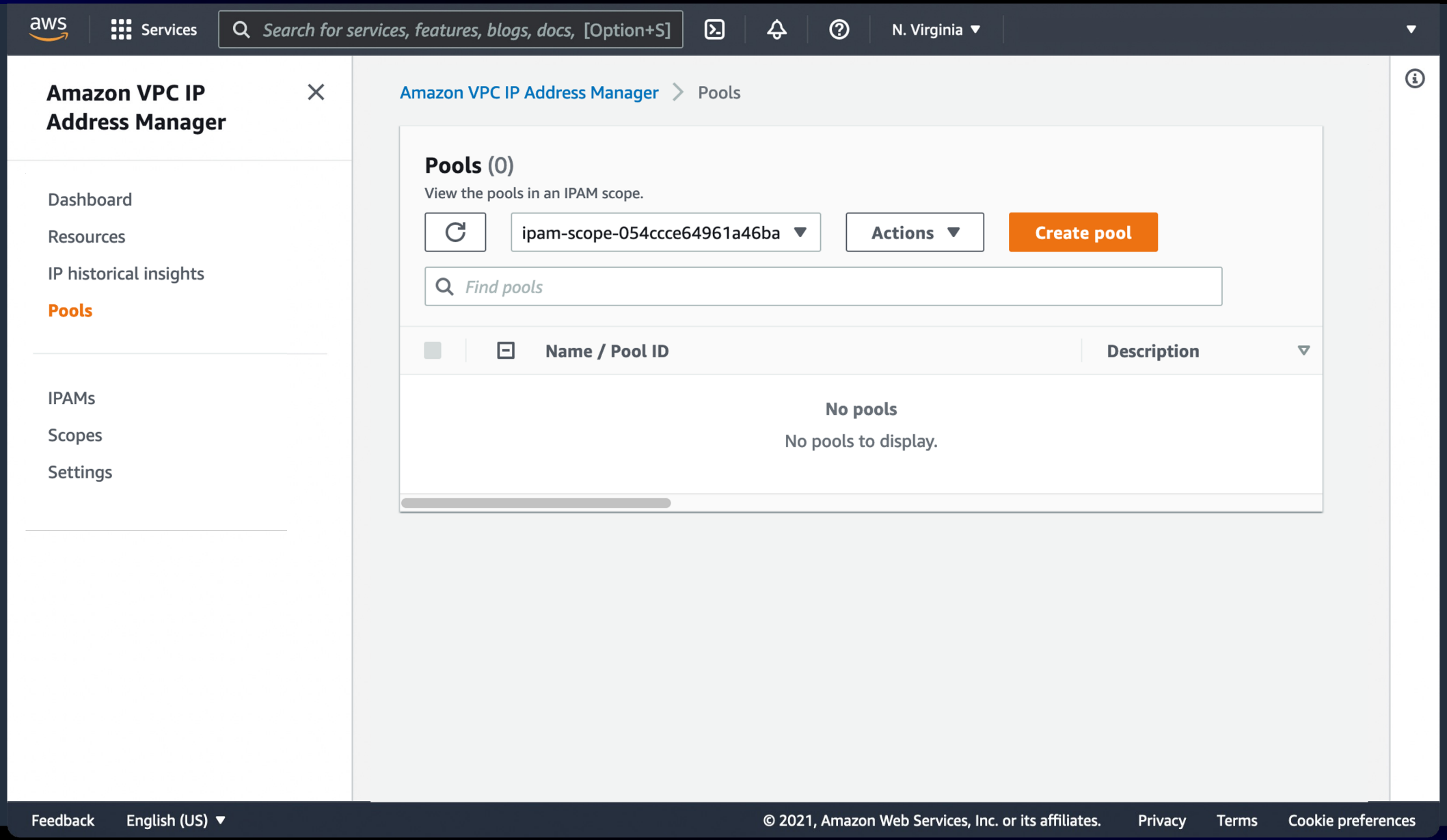


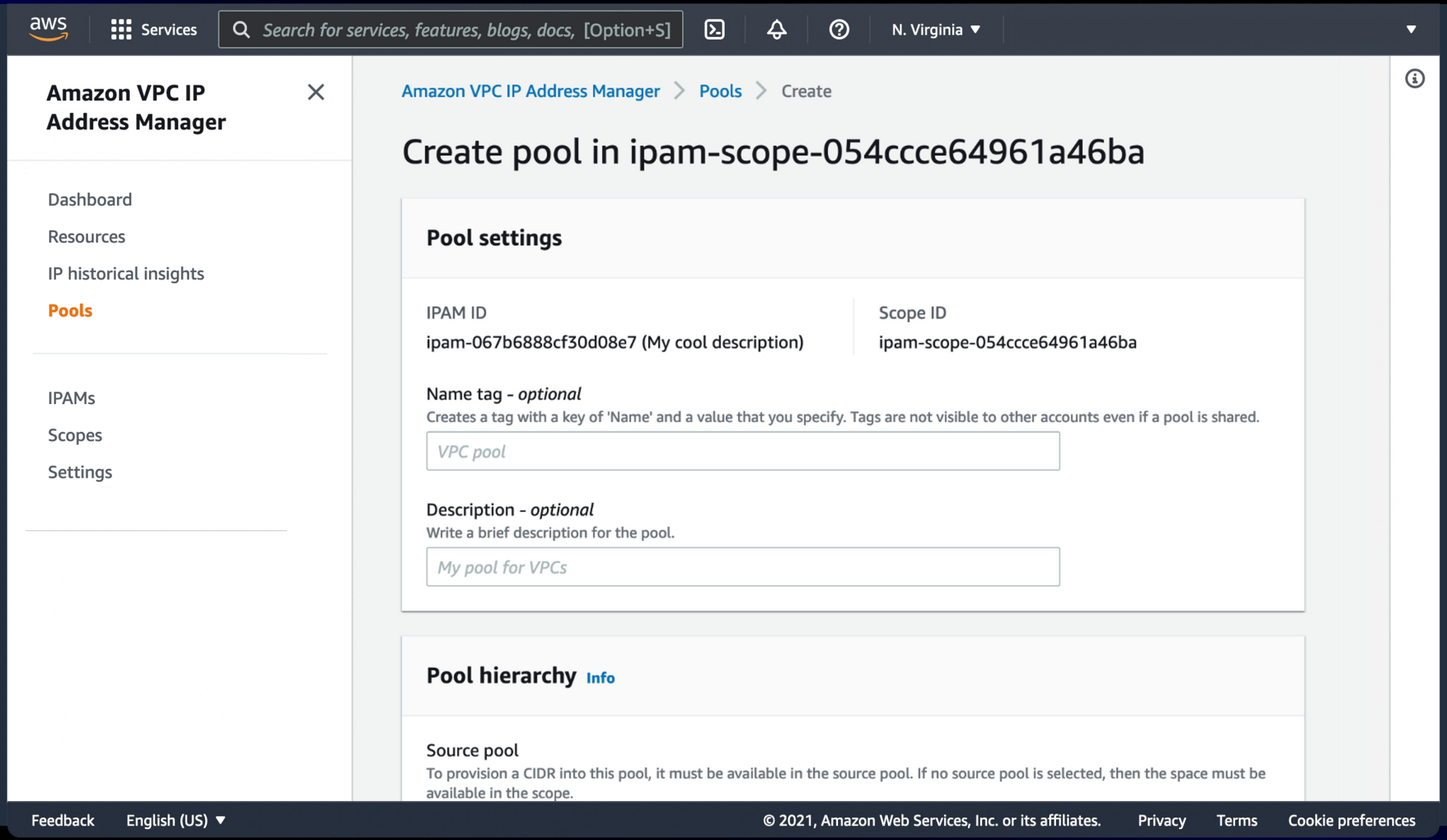




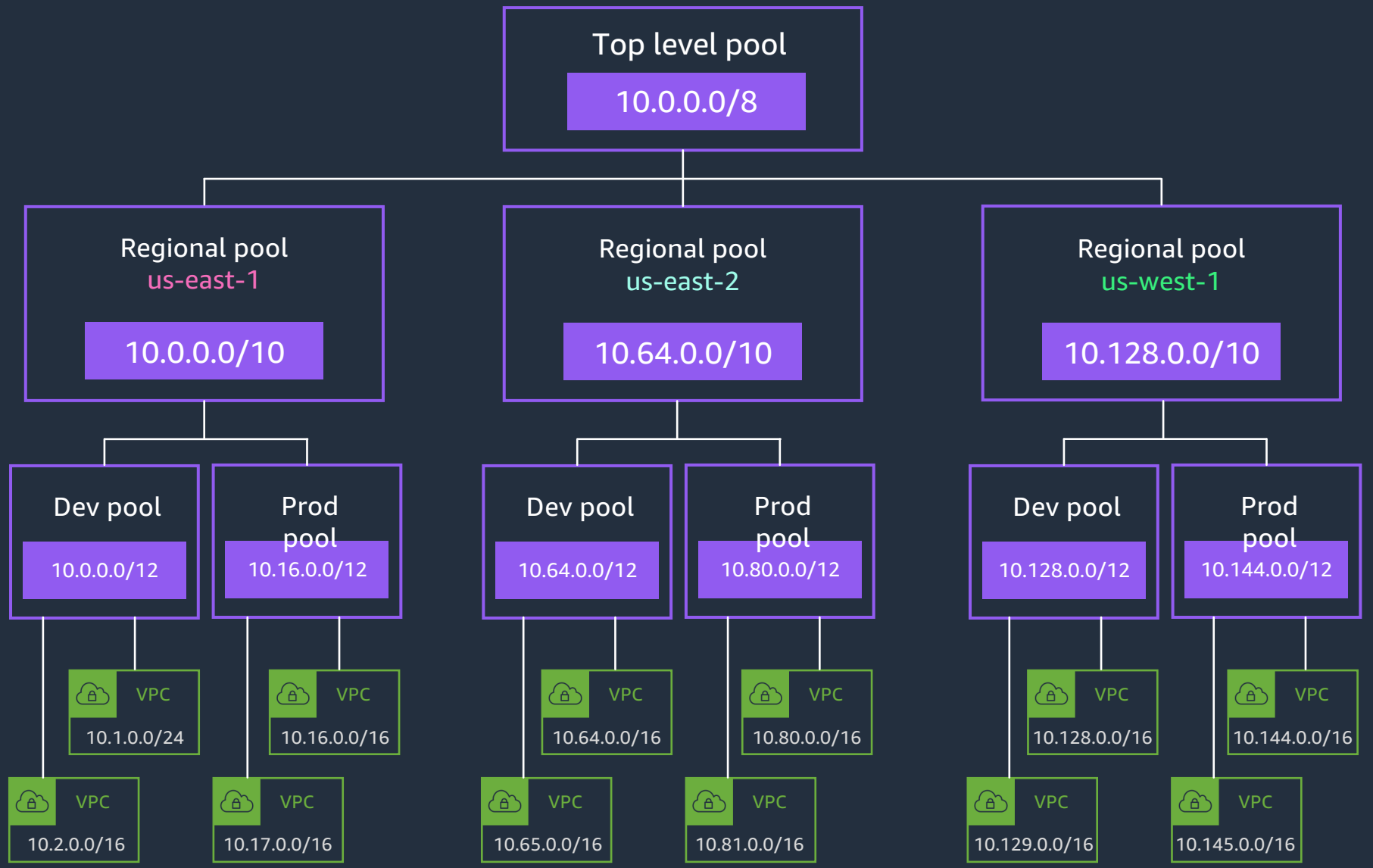






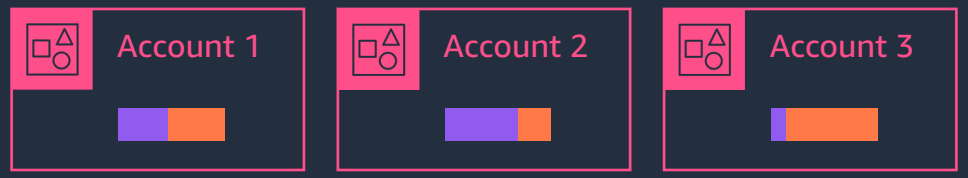


Private scope



Bring your own IP (BYOIP)
with IPAM

BYOIP *without* IPAM



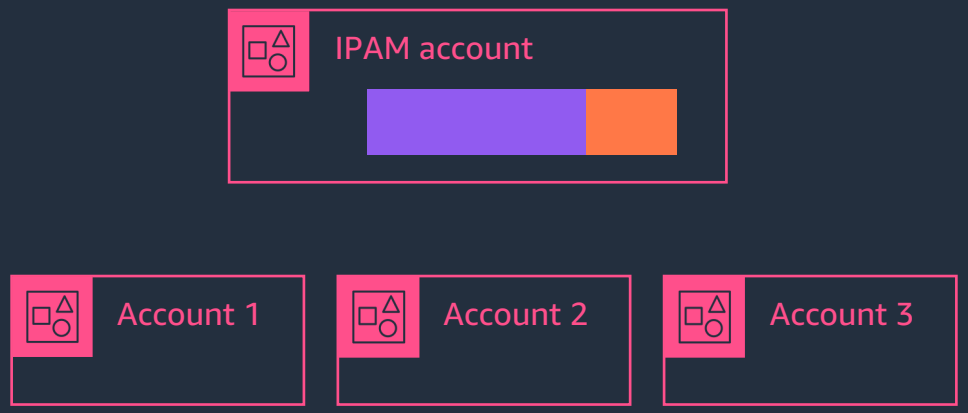
Benefits:

- Improve IP address utilization (Org wide sharing)

Used IPs
Unused IPs

Bring your own IP (BYOIP)
with IPAM

BYOIP *with* IPAM



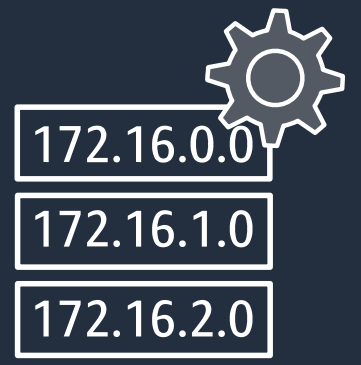
Benefits:

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

Amazon VPC IP Address Manager

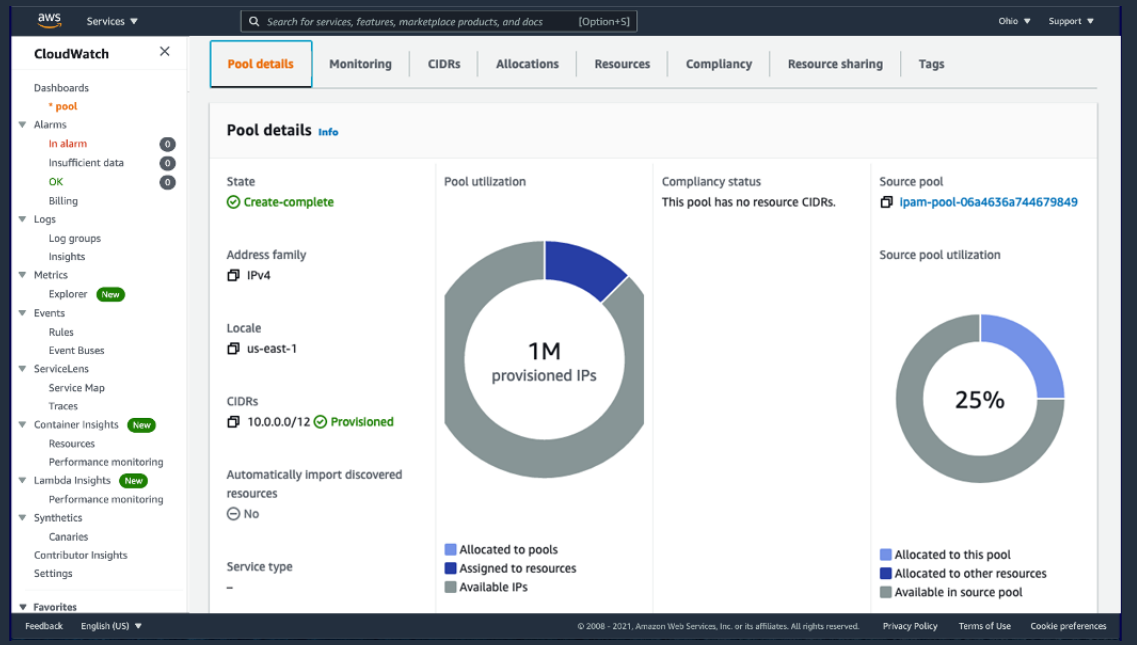
IPAM

Monitoring and alerts



Monitor across network

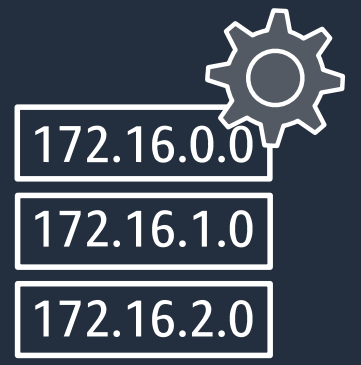
Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends



Amazon VPC IP Address Manager

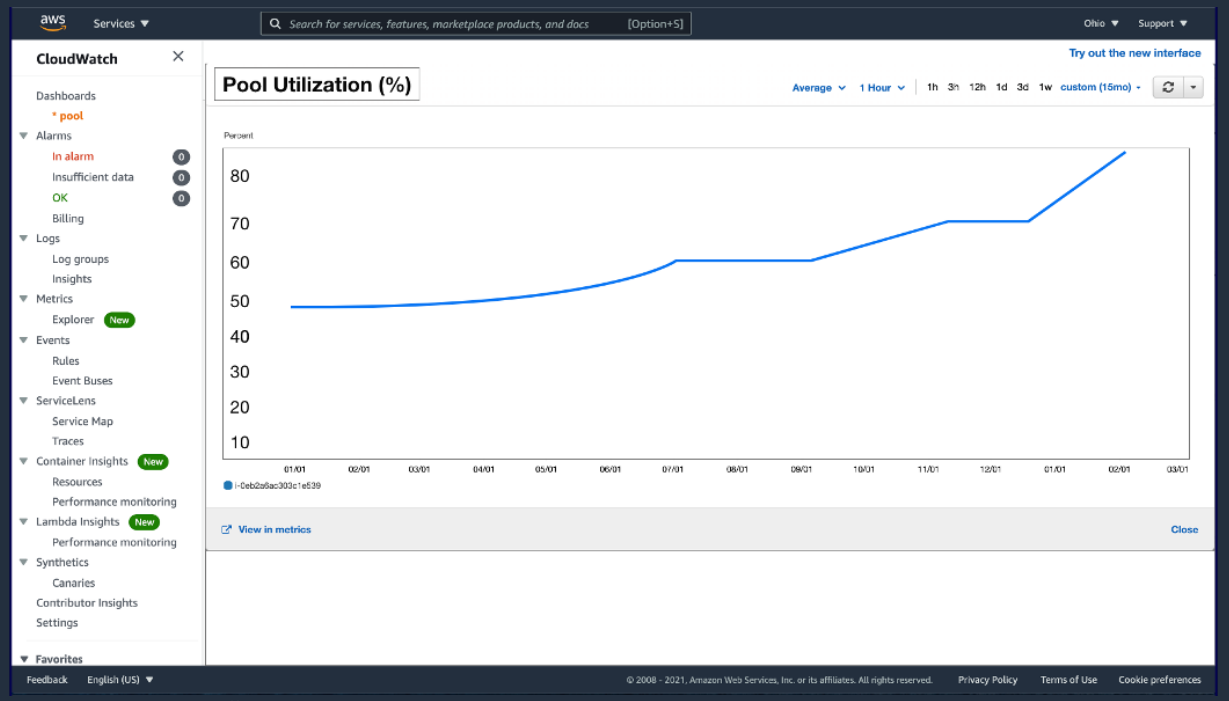
IPAM

Monitoring and alerts



Monitor across network

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

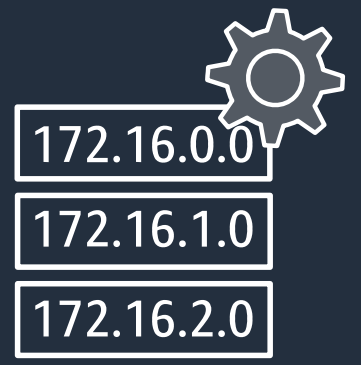


aws

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

Your VPCs

Filter VPCs

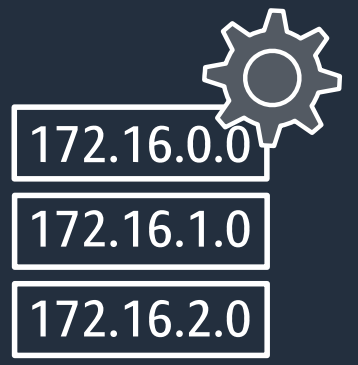
Name	VPC ID	Owner ID	Region	State	IPv4 CIDR	IPv6 CIDR	IPv4 Pool	IPv6 Pool
W1-prev-dev-vpc	vpc-6ace2601	075785353725	Us-west-1	Compliant	10.0.0.0/24		Us-west-1-dev	
W1-prev-test-vpc	vpc-6ace2602	111122223333	Us-west-1	Compliant	10.4.0.0/24		Us-west-1-dev	
W1-prev-prod-vpc	vpc-6ace2603	444455556666	Us-west-1	Compliant			-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-234723fxk	777788889999	Us-east-1	Unmanaged	172.31.0.0/24		UNKNOWN	

Tag on allocation policy don't match

Amazon VPC IP Address Manager

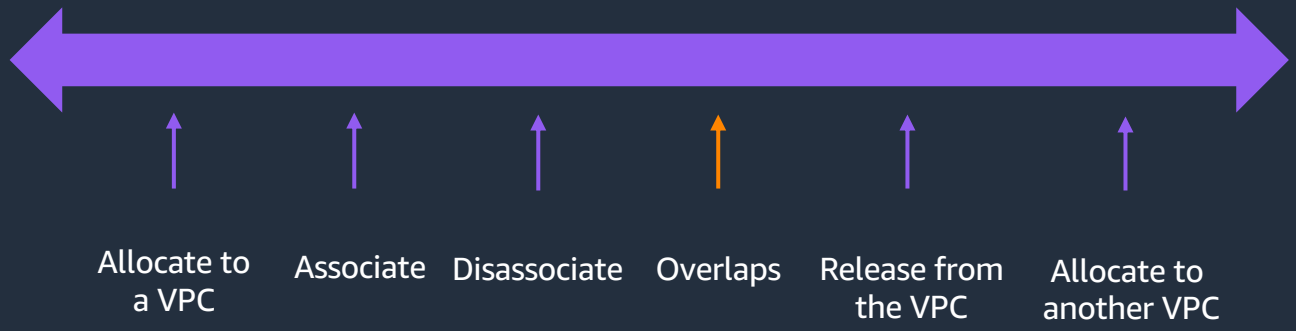
IPAM

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

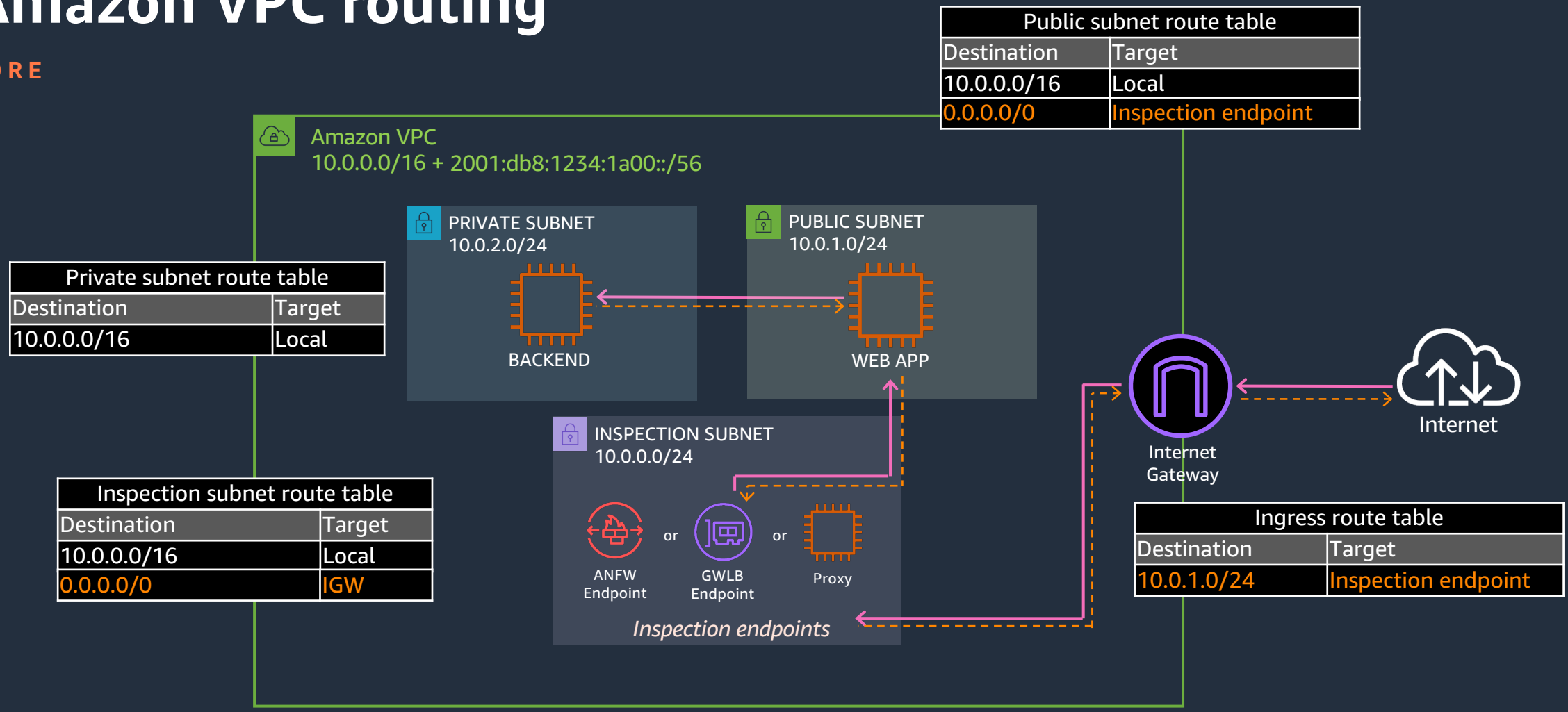
AWS NAT Gateway
Private NAT support

AWS PrivateLink
S3 interface endpoint and ALB integration

AWS Transit Gateway
TGW Connect and intra-region peering

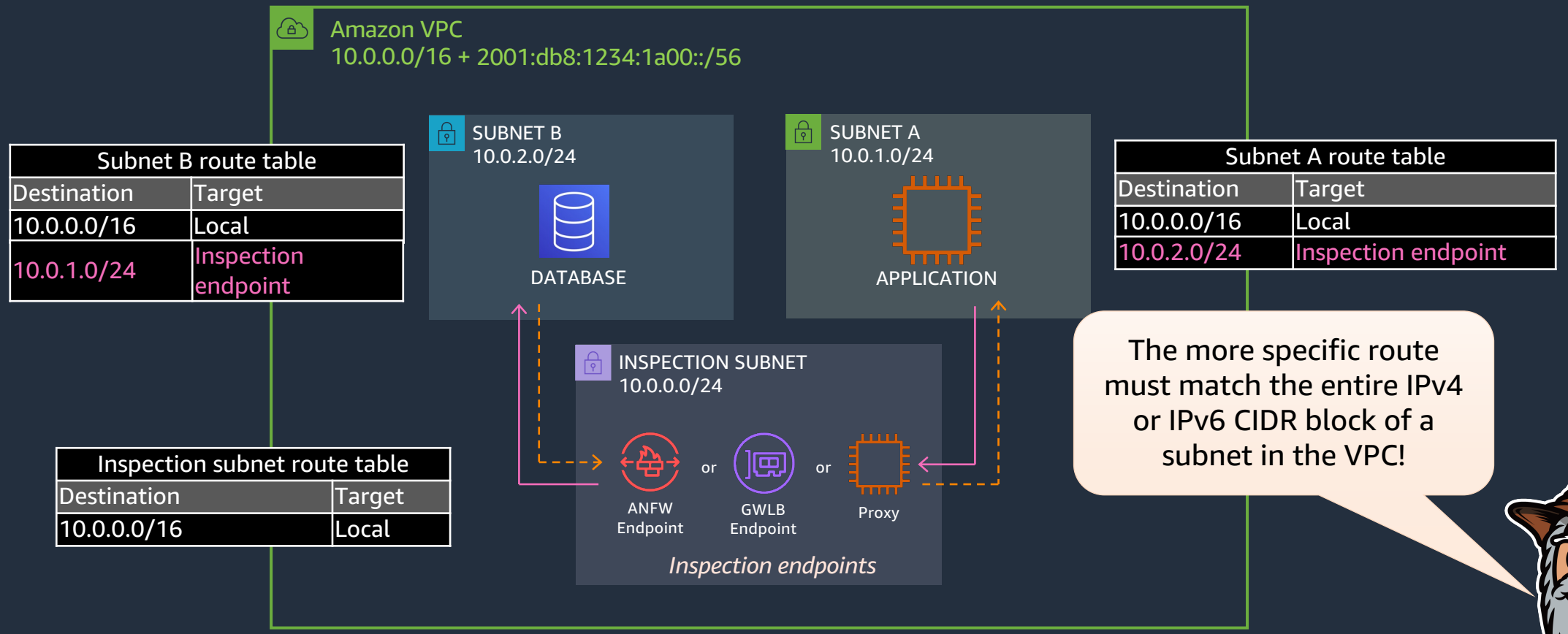
Amazon VPC routing

BEFORE



Amazon VPC routing: Enhanced routing controls

AFTER



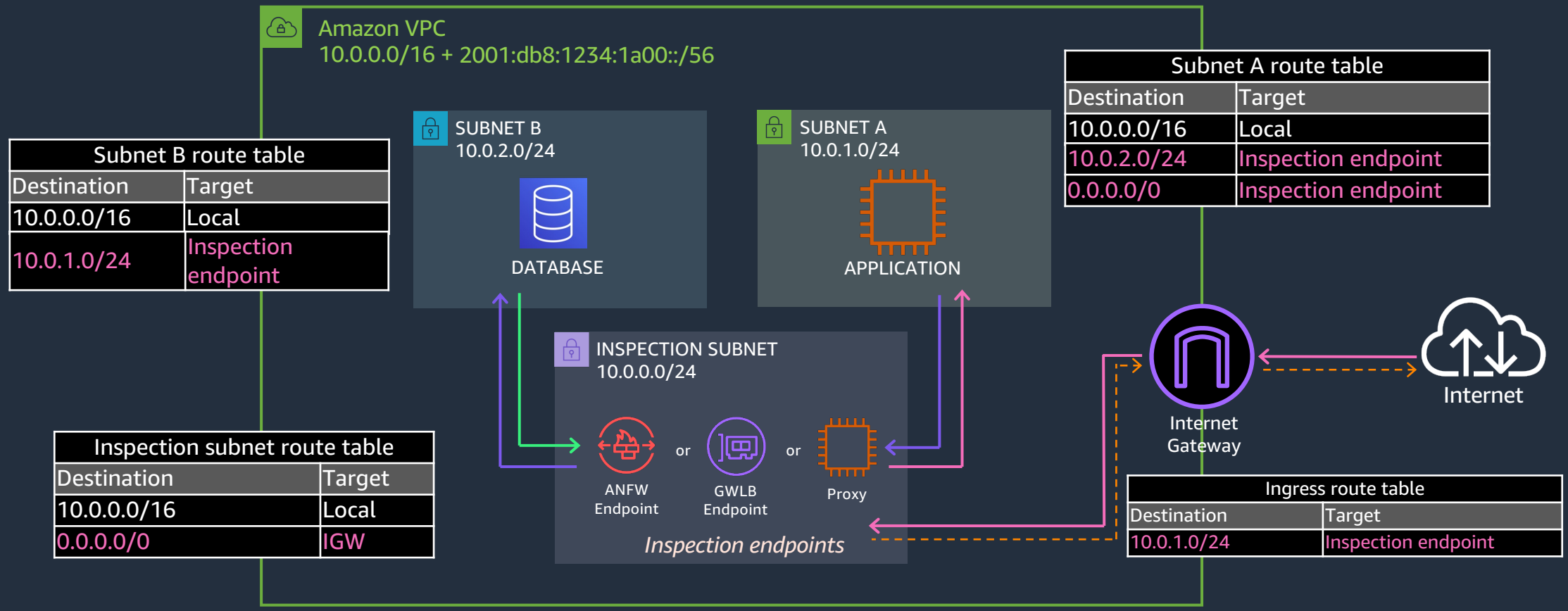
Subnet B route table	
Destination	Target
10.0.0.0/16	Local
10.0.1.0/24	Inspection endpoint

Subnet A route table	
Destination	Target
10.0.0.0/16	Local
10.0.2.0/24	Inspection endpoint

Inspection subnet route table	
Destination	Target
10.0.0.0/16	Local

The more specific route must match the entire IPv4 or IPv6 CIDR block of a subnet in the VPC!

Enhanced VPC routing: Multiple inspection levels



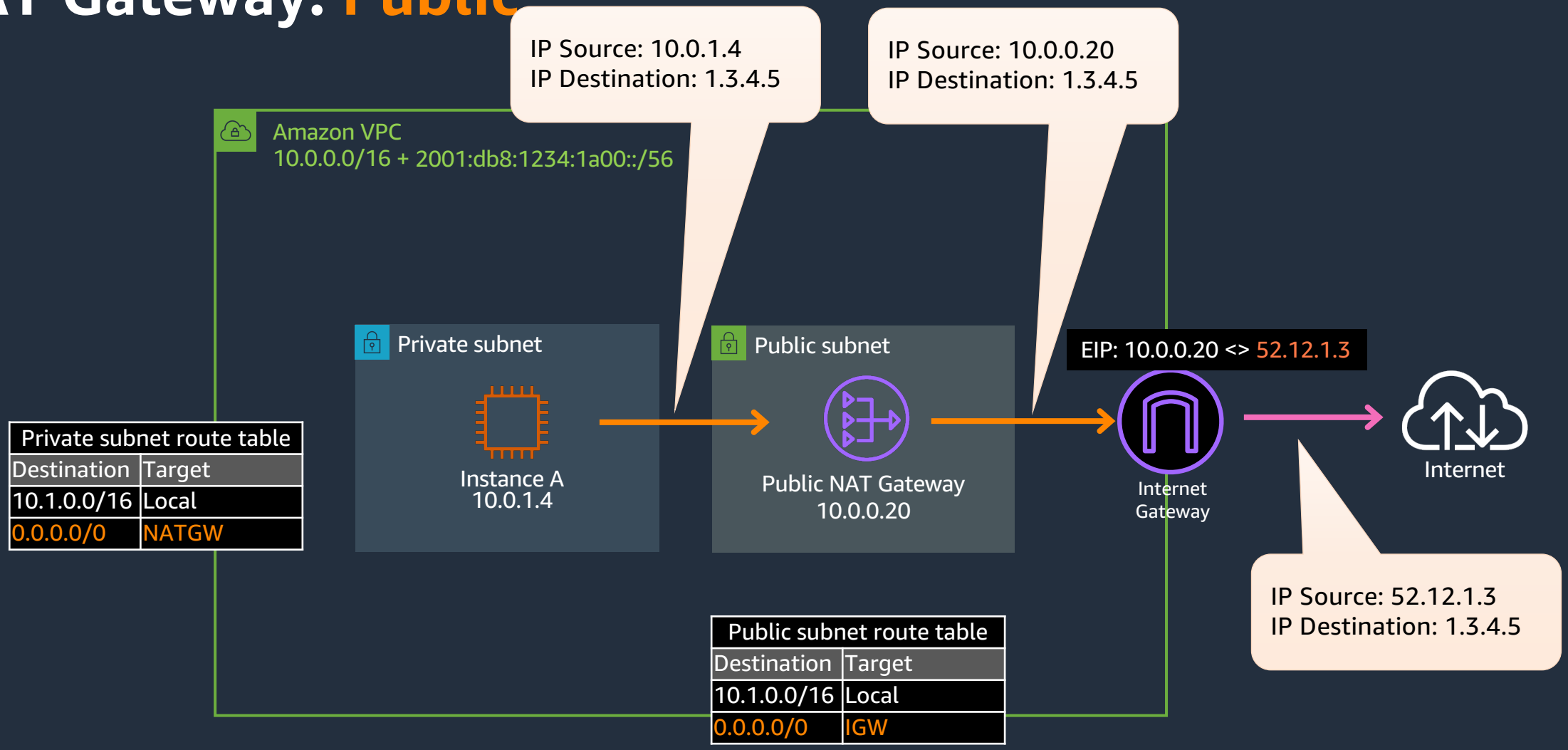
Amazon VPC Networking

Amazon VPC
Enhanced routing

AWS NAT Gateway
Private NAT support

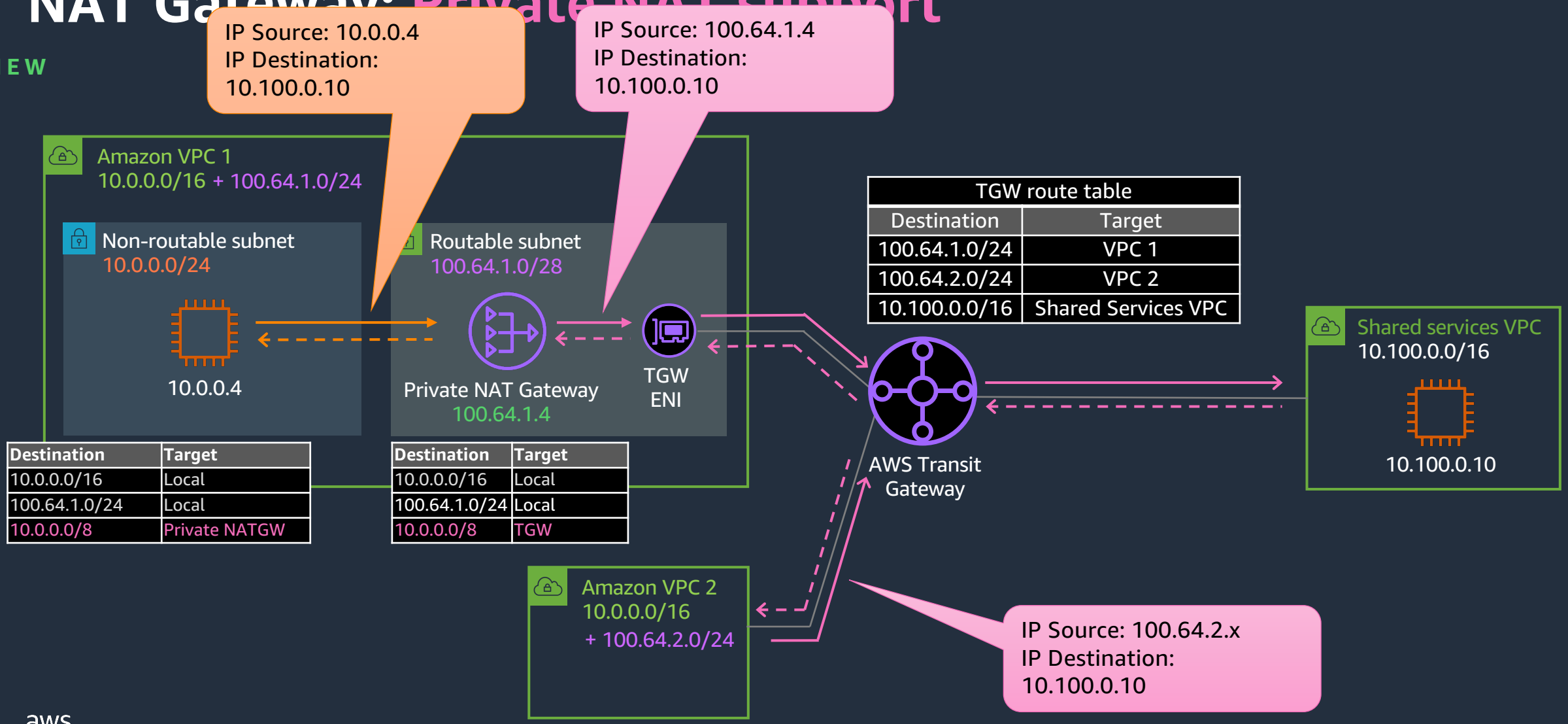
NAT Gateway: Public

BEFORE



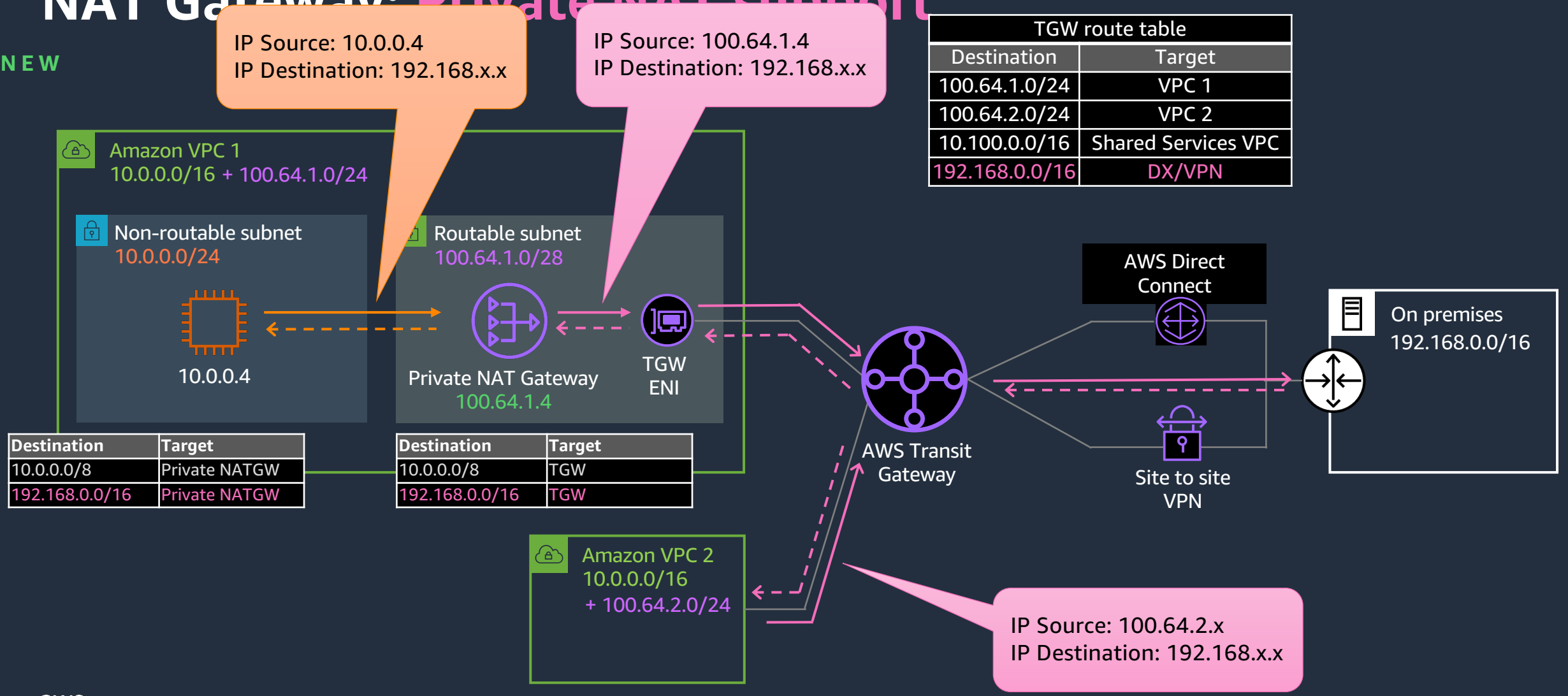
NAT Gateway: Private NAT support

NEW



NAT Gateway: Private NAT support

NEW



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

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

Amazon VPC Networking

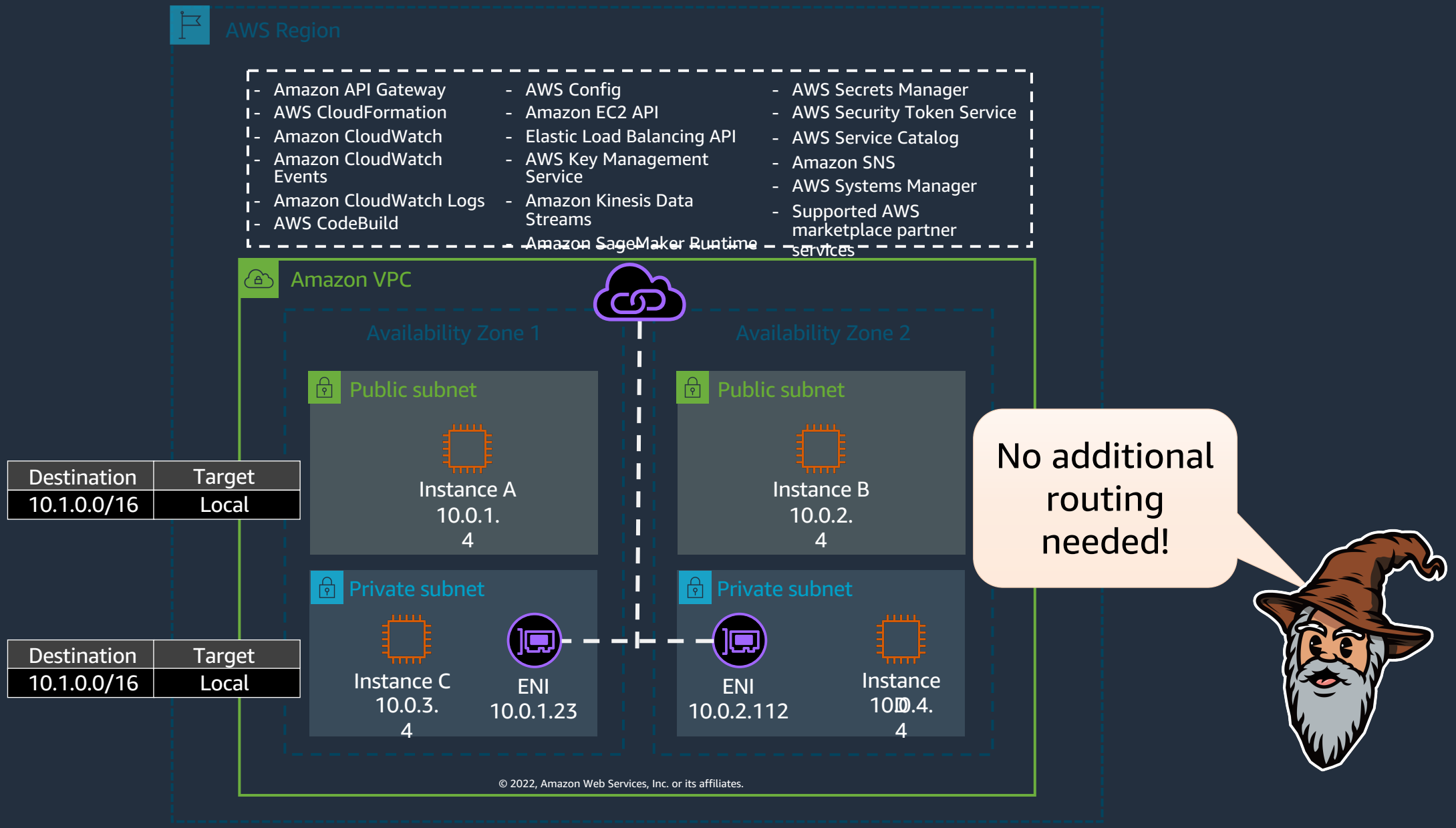
Amazon VPC
Enhanced routing

AWS NAT Gateway
Private NAT support

AWS PrivateLink
S3 interface endpoint and ALB integration

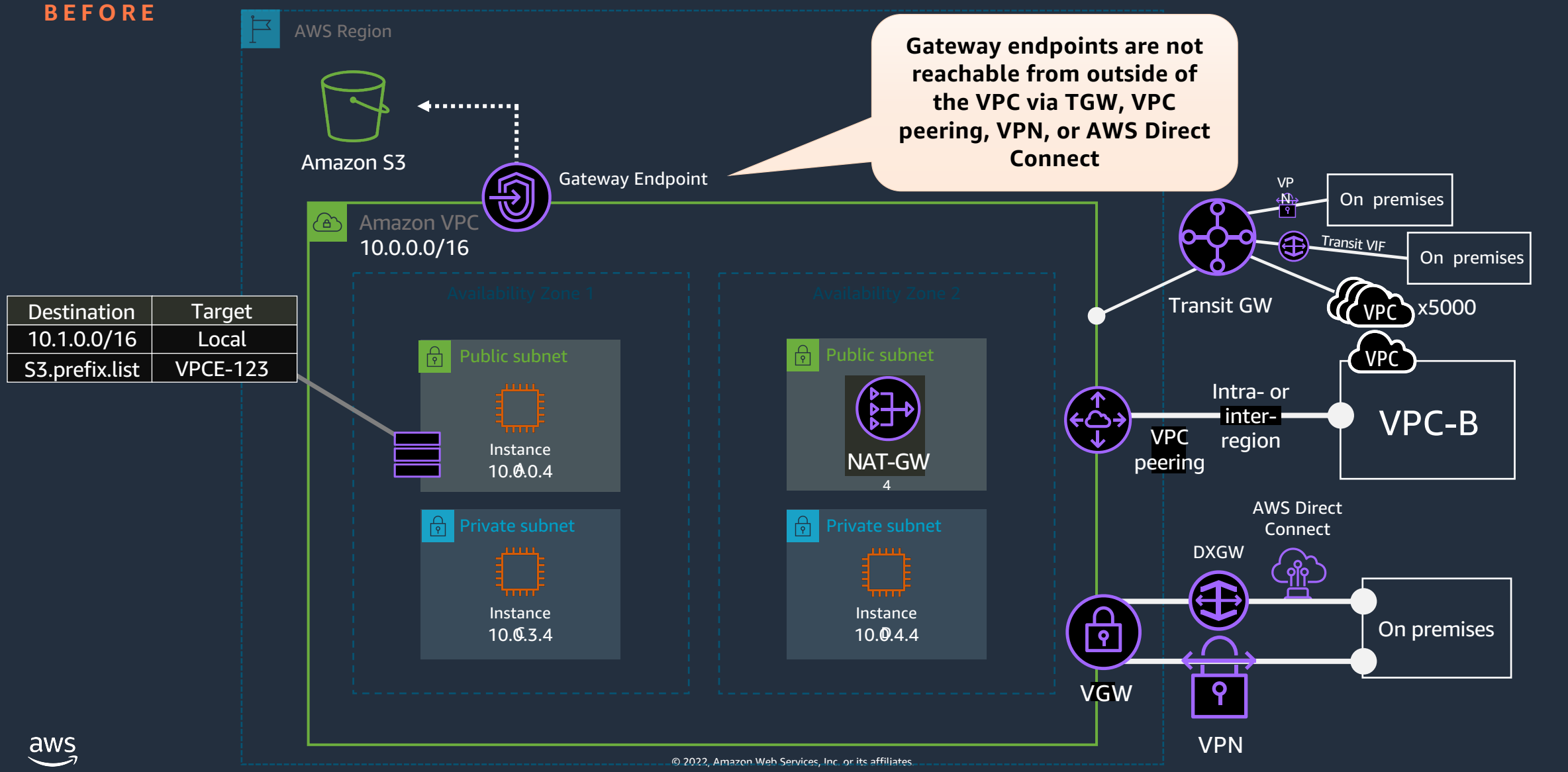
AWS PrivateLink: Interface endpoints

BEFORE



AWS PrivateLink: S3 Gateway endpoints

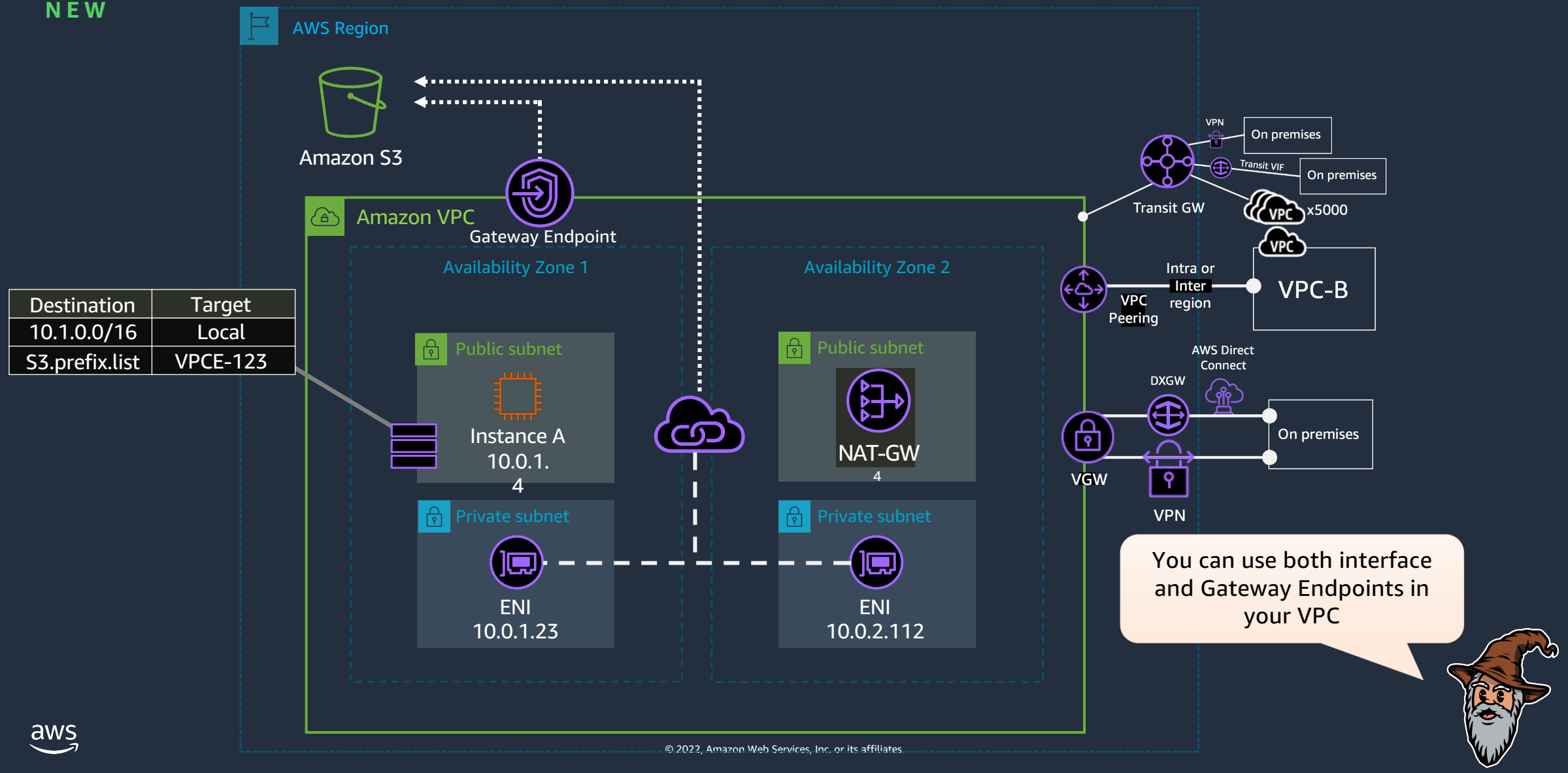
BEFORE



S3 interface endpoints

AWS PrivateLink: S3 interface endpoints

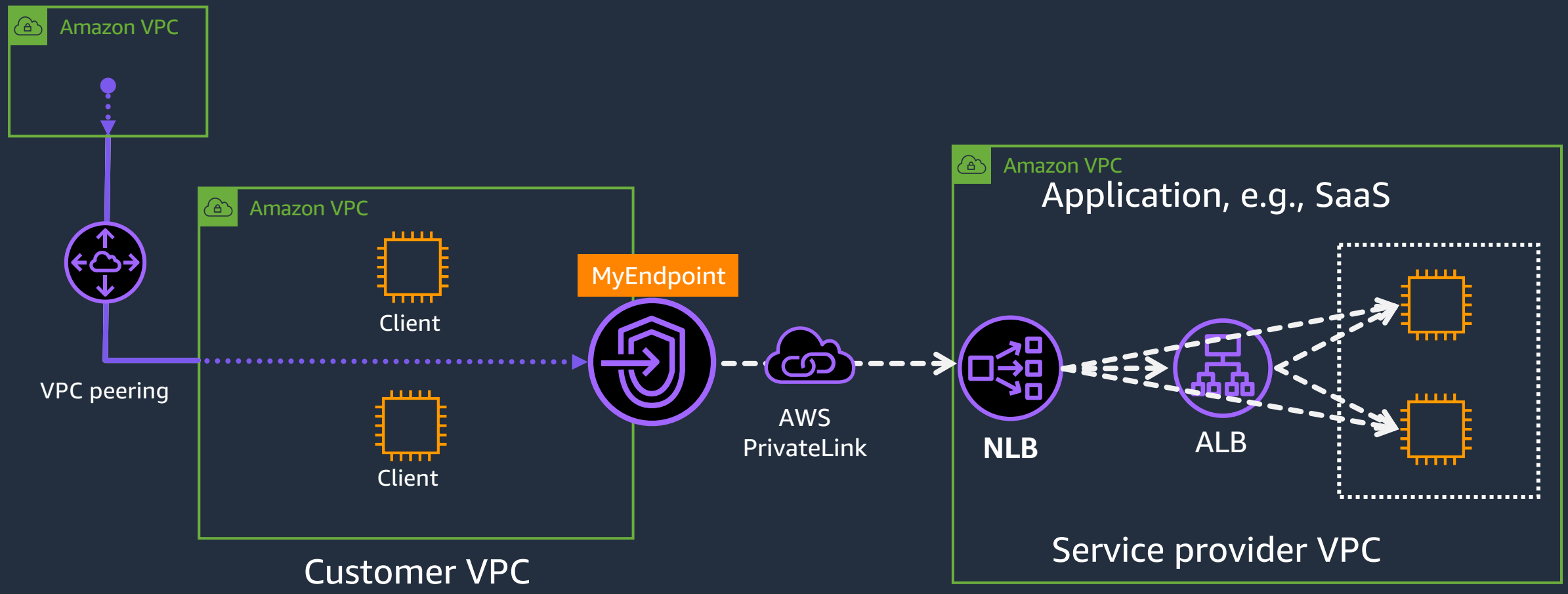
NEW



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

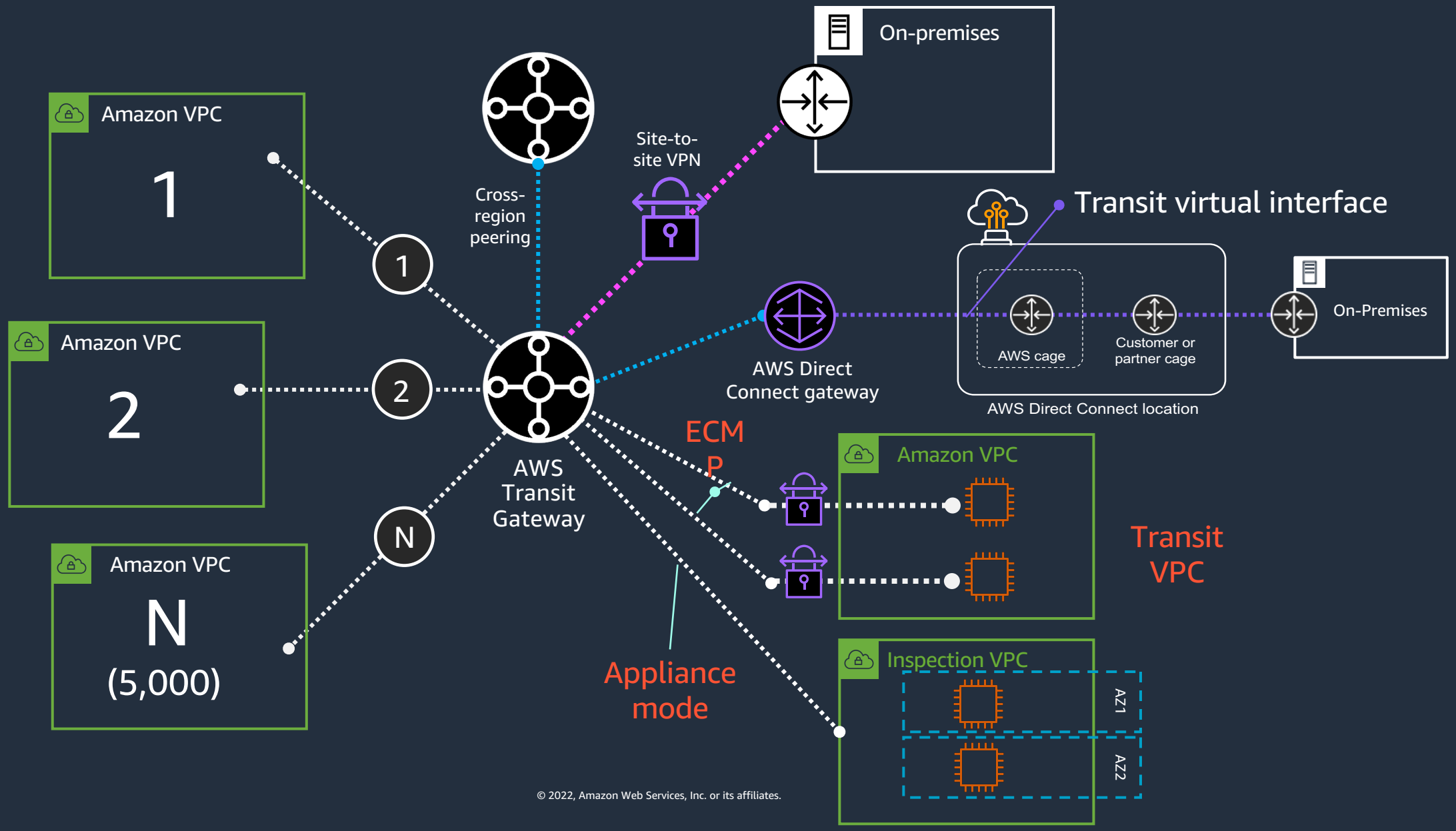
AWS NAT Gateway
Private NAT support

AWS PrivateLink
S3 interface endpoint and ALB integration

AWS Transit Gateway
TGW Connect and intra-region peering

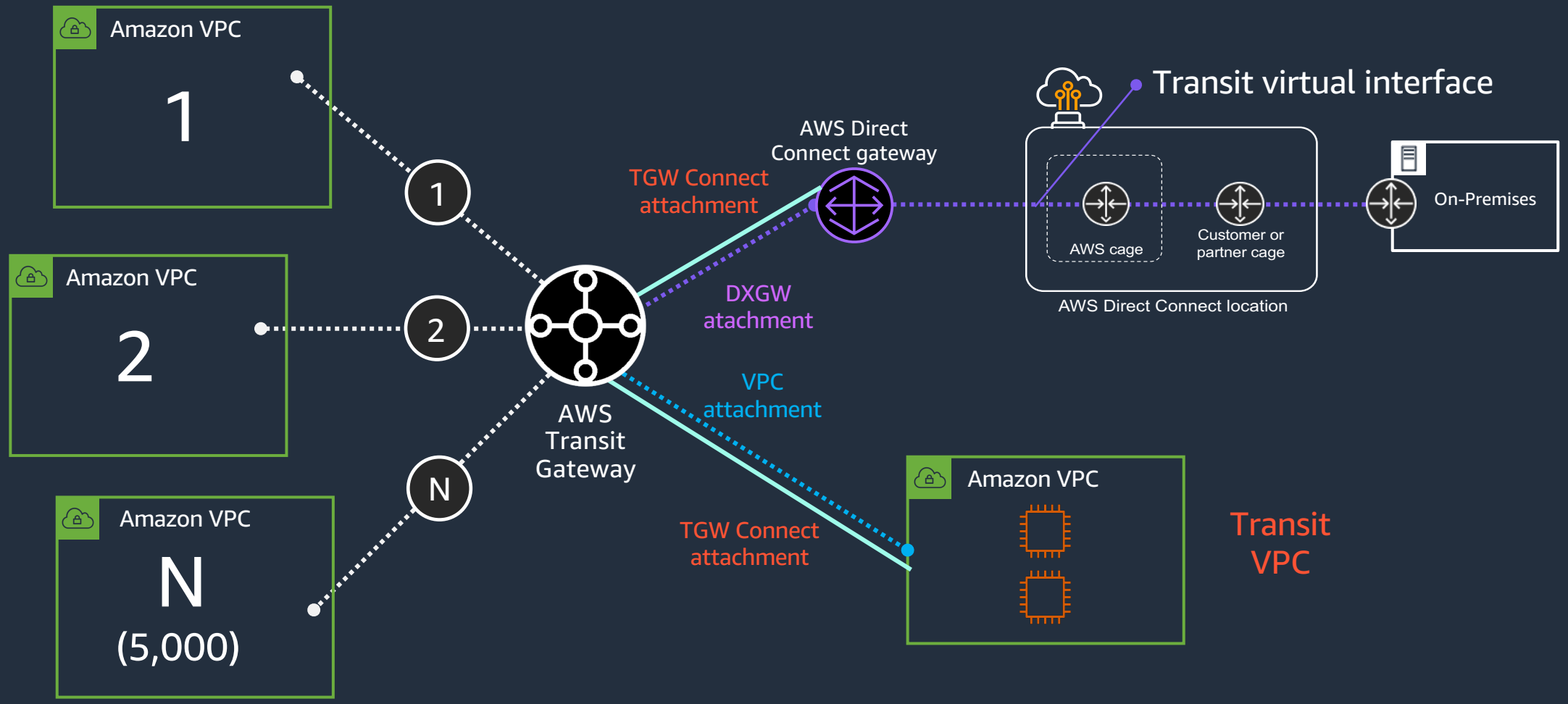
AWS Transit Gateway

BEFORE



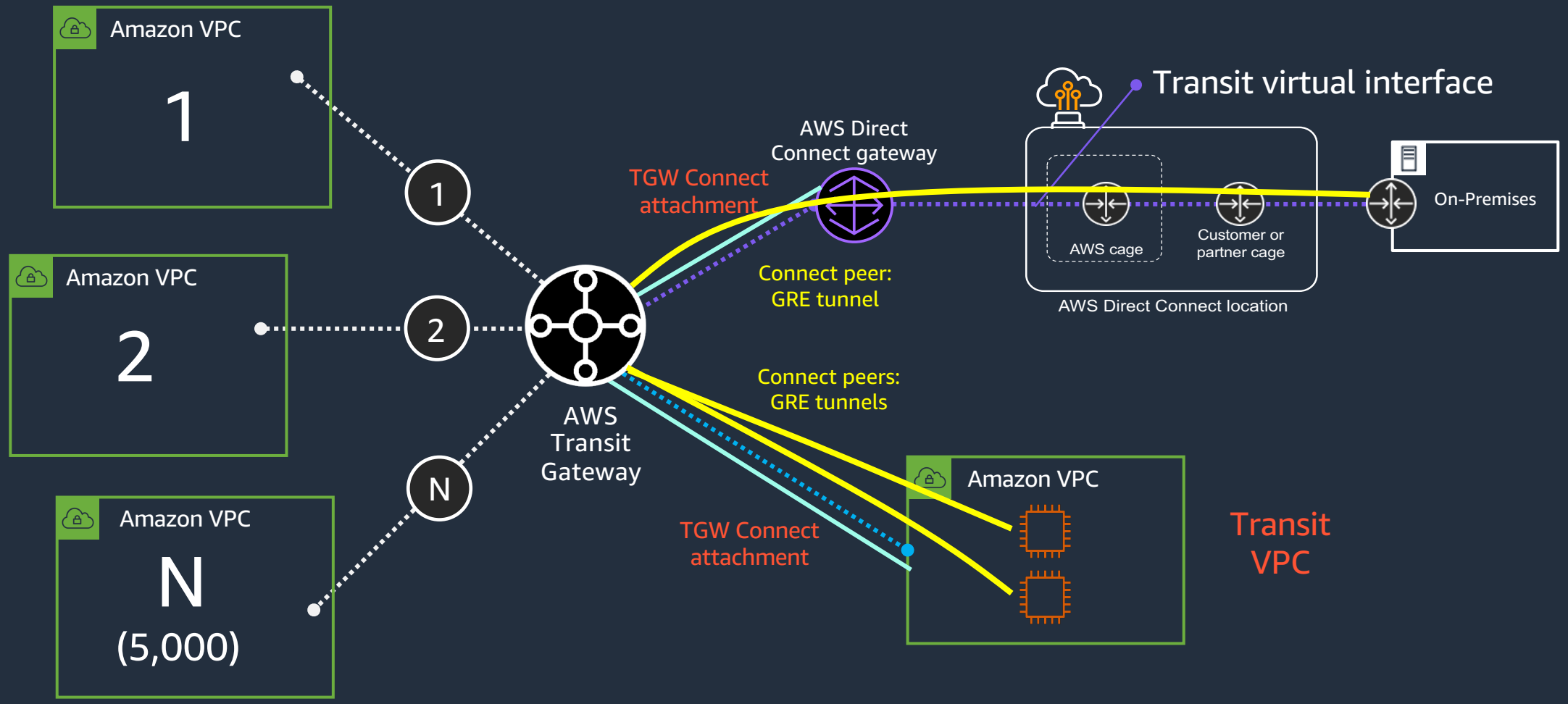
AWS Transit Gateway Connect

AFTER



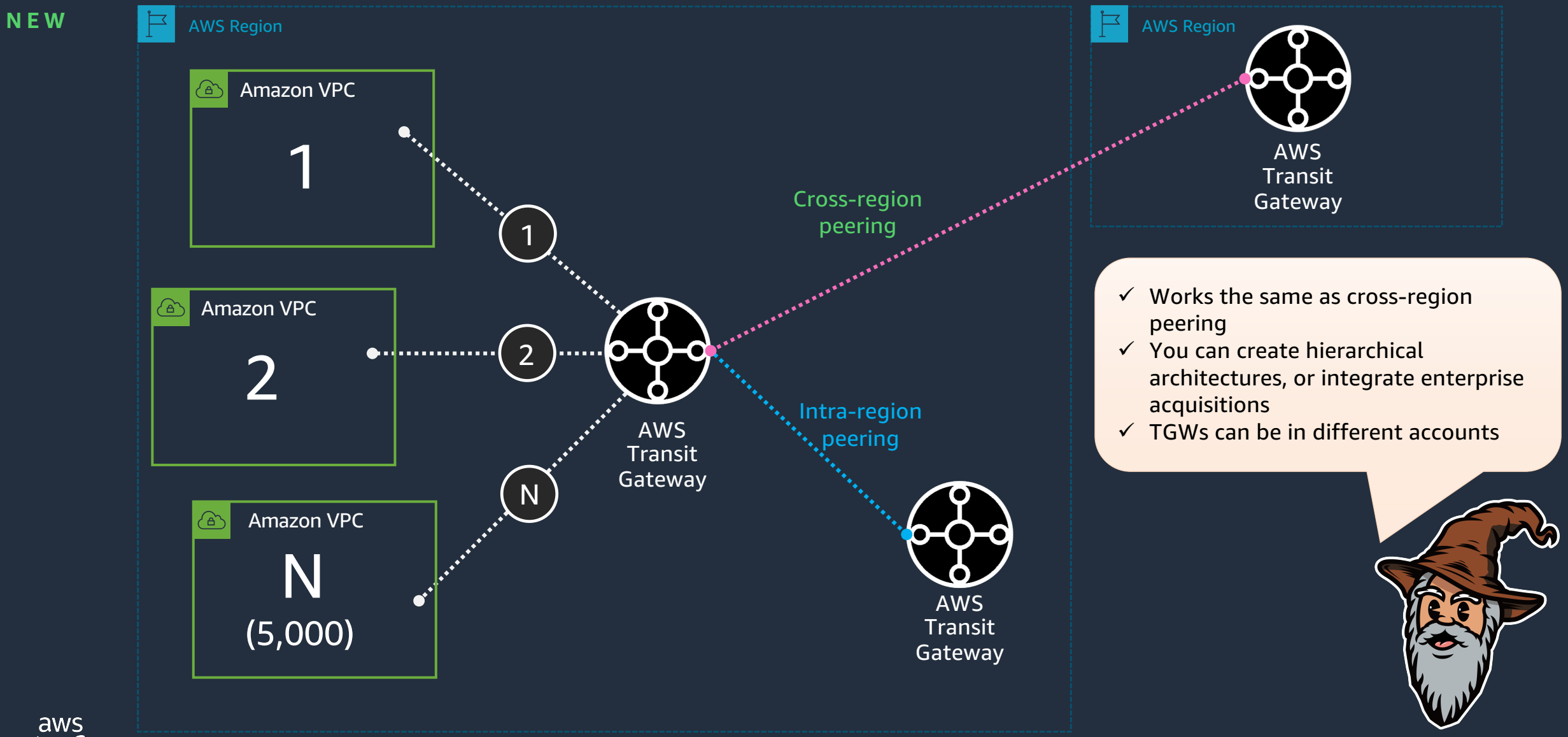
AWS Transit Gateway Connect

AFTER



AWS Transit Gateway: Intra-region peering

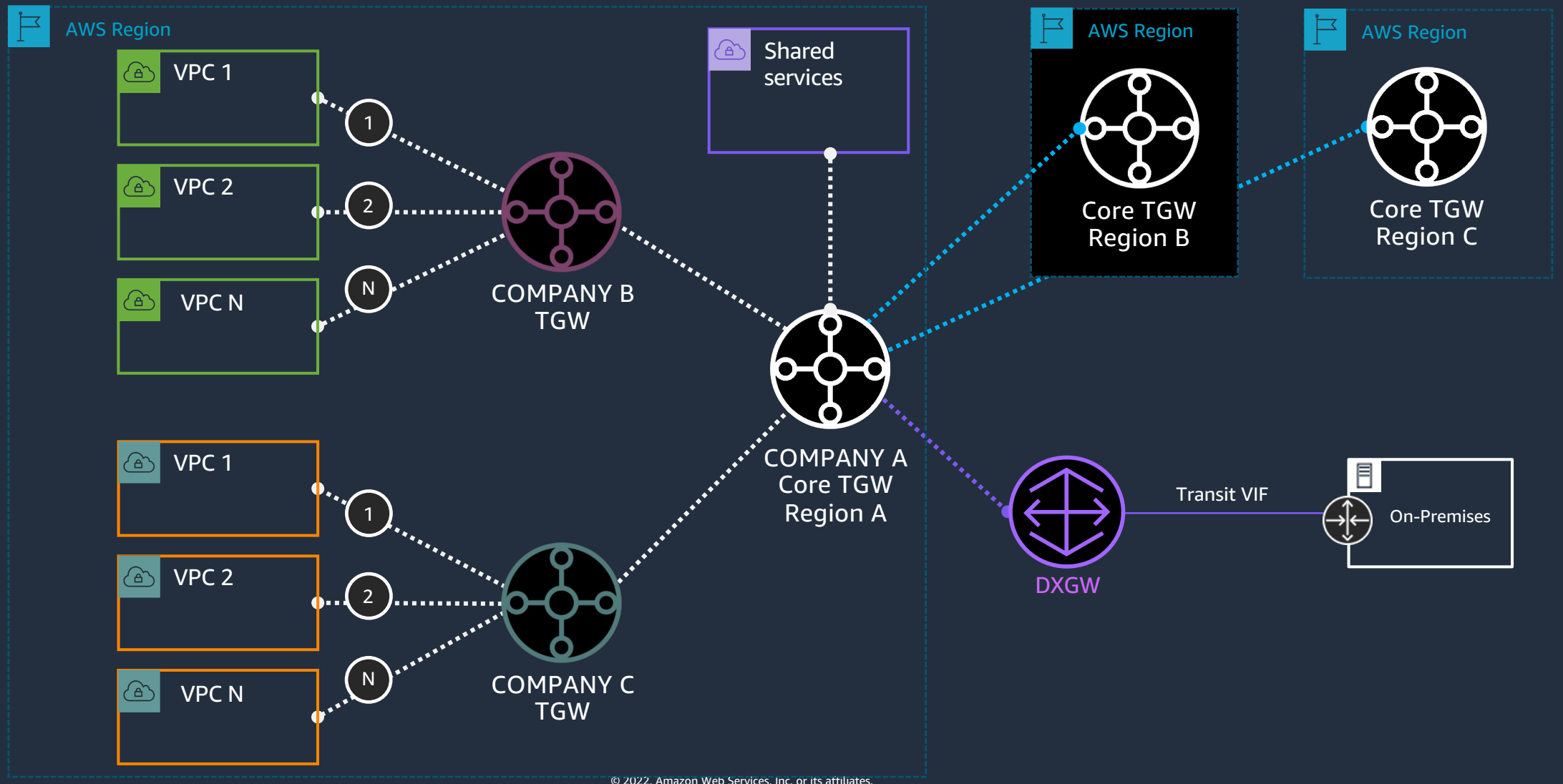
NEW



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

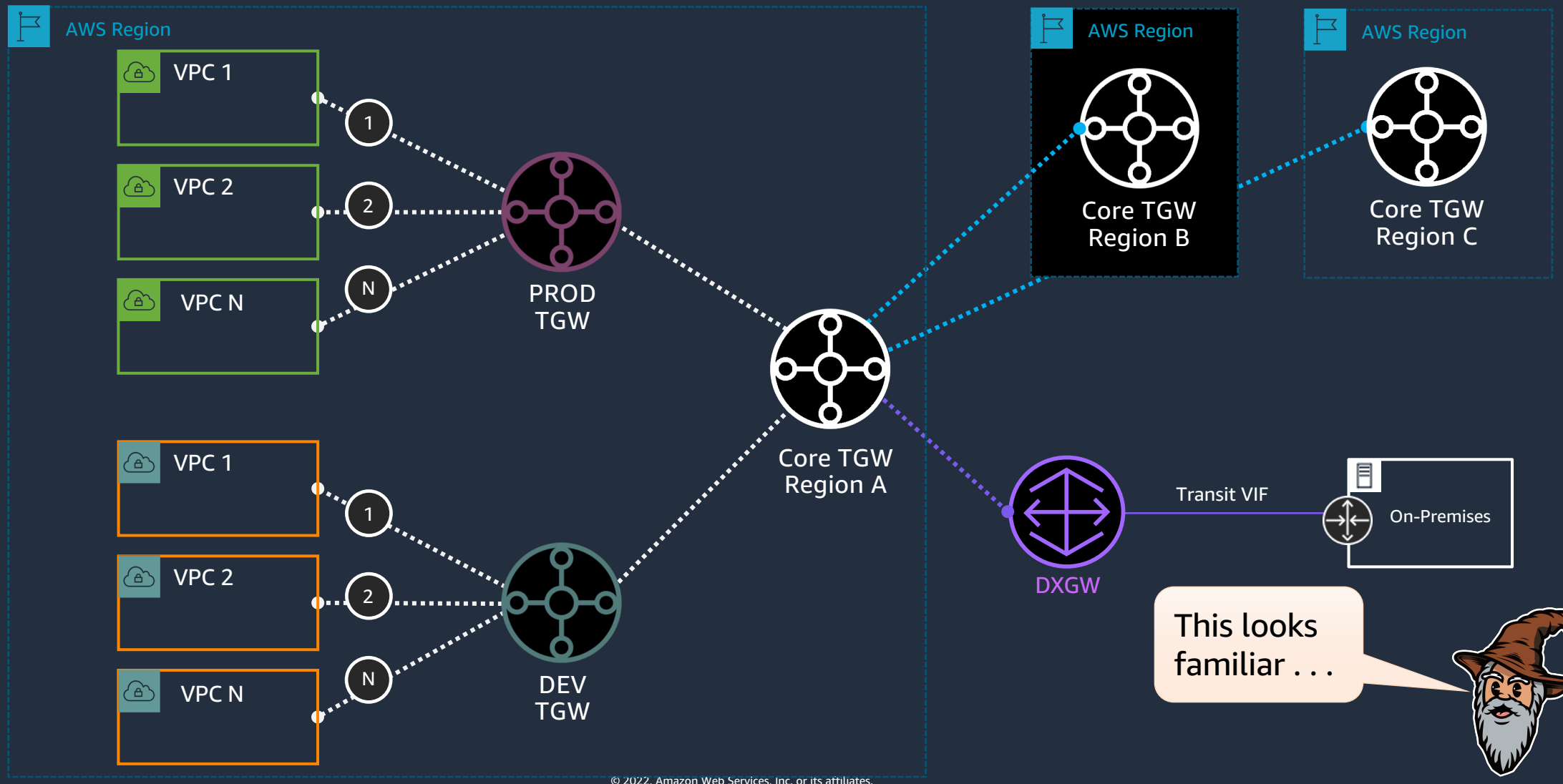
AWS Transit Gateway: Intra-region peering

ACQUISITIONS INTEGRATION



AWS Transit Gateway: Intra-region peering

HIERARCHICAL REGIONAL ARCHITECTURE

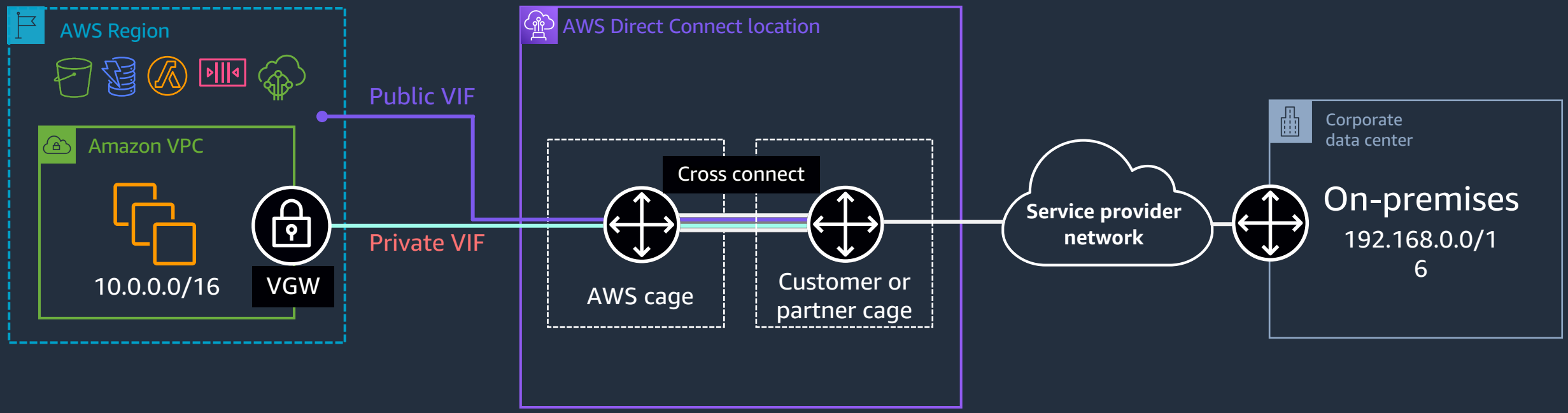


AWS Direct Connect

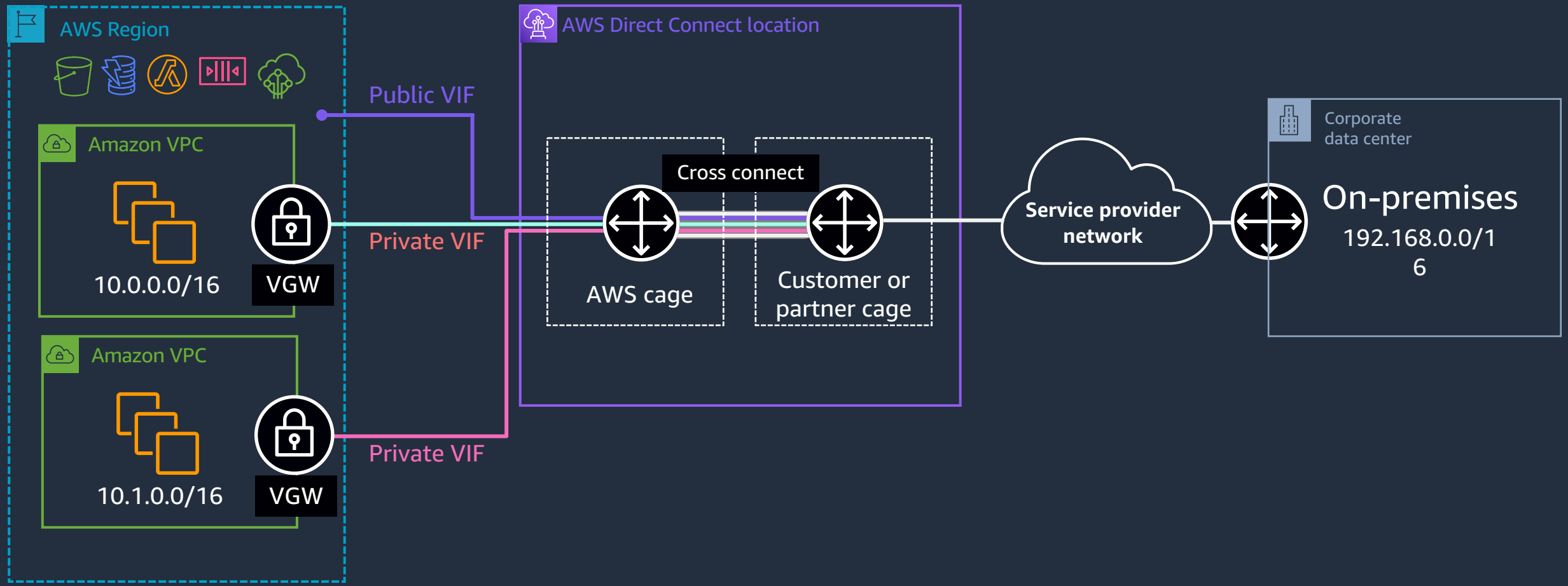
MACSEC , 100Gbps, and AWS Local Zones

On-premises and global connectivity

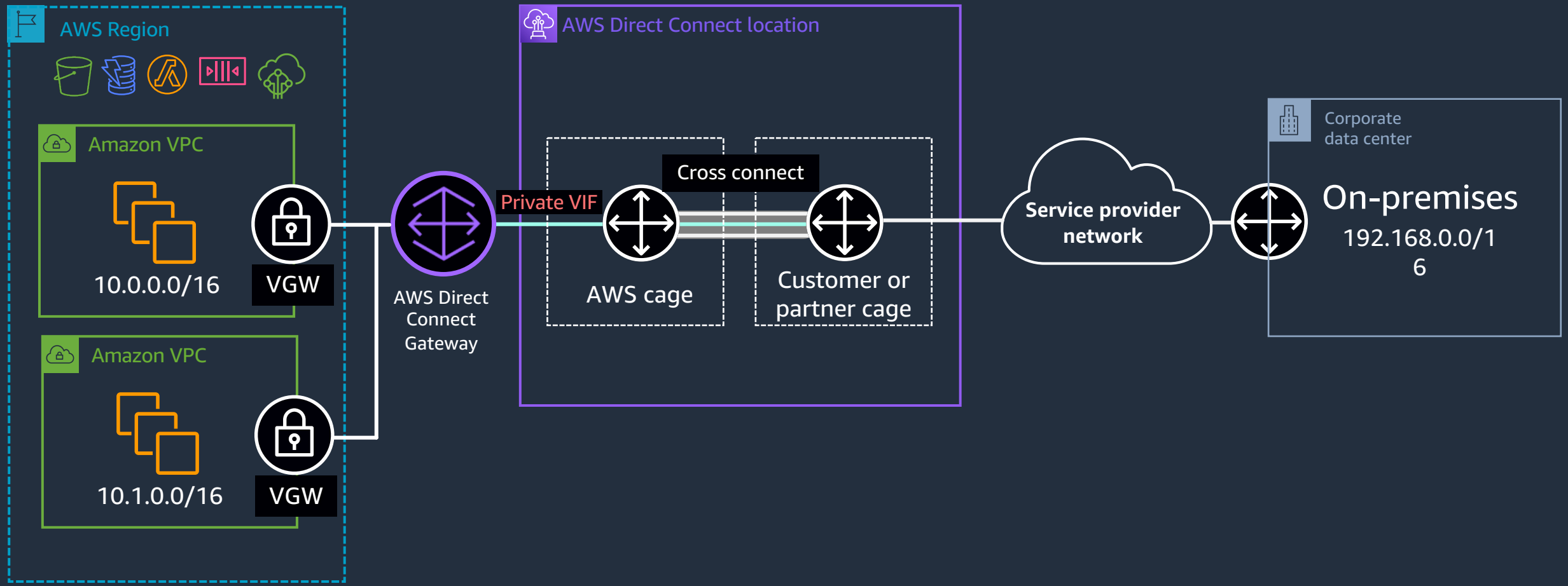
An overview: AWS Direct Connect



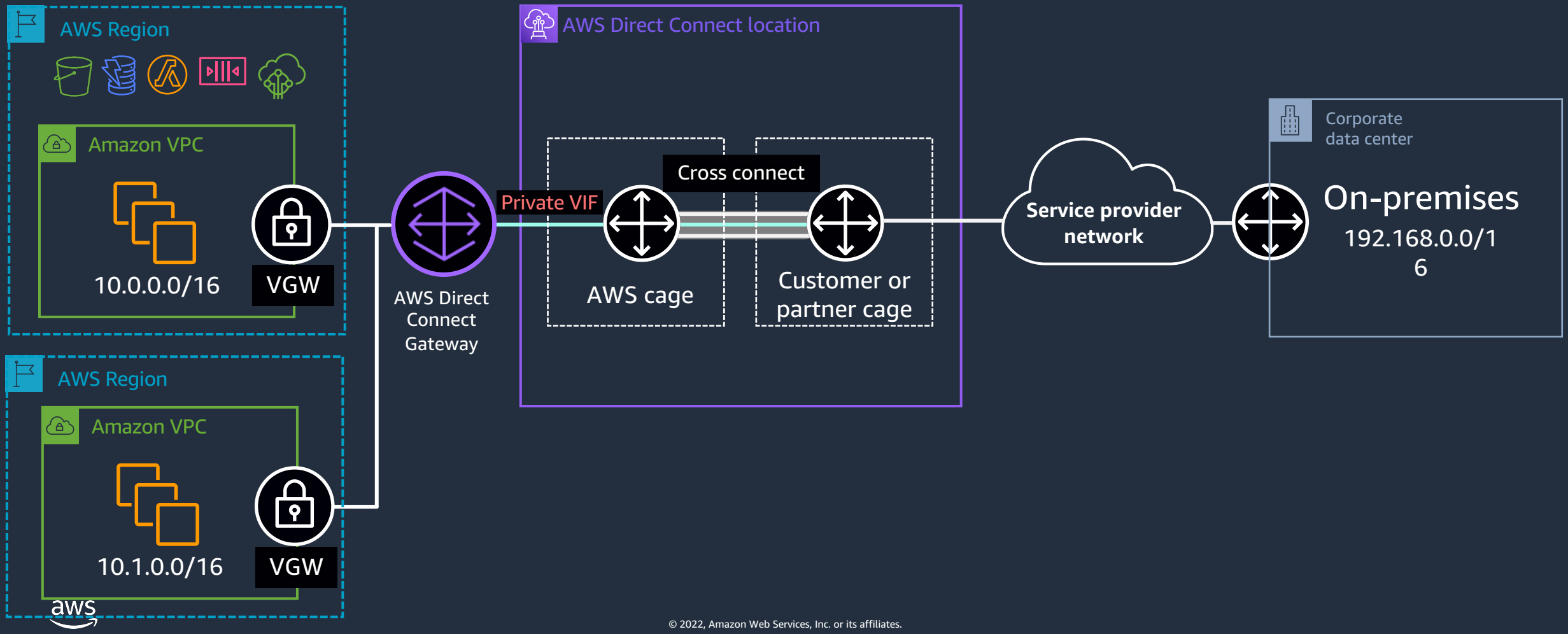
An overview: AWS Direct Connect



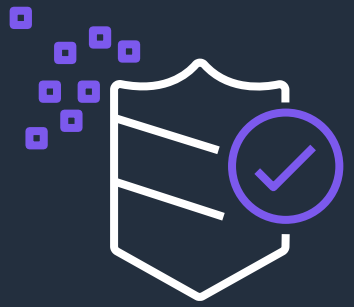
An overview: AWS Direct Connect



An overview: AWS Direct Connect

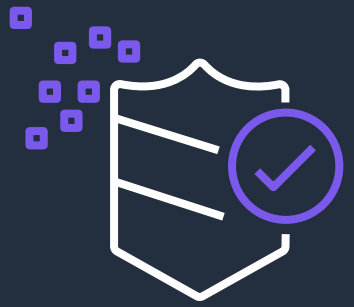


Introducing: AWS Direct Connect MACsec



"Dance like nobody is watching.
Encrypt like everyone is."

Introducing: AWS Direct Connect MACsec



Layer 2 confidentiality and integrity

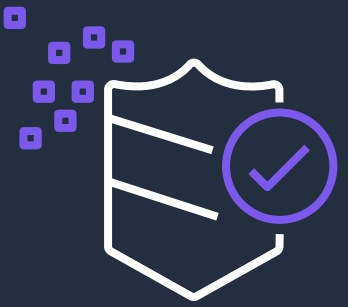
MACsec allows you to secure an Ethernet link – including all control plane protocol packets (such as ARP, DHCP, LLDP, and Layer 3 routing protocols like BGP)

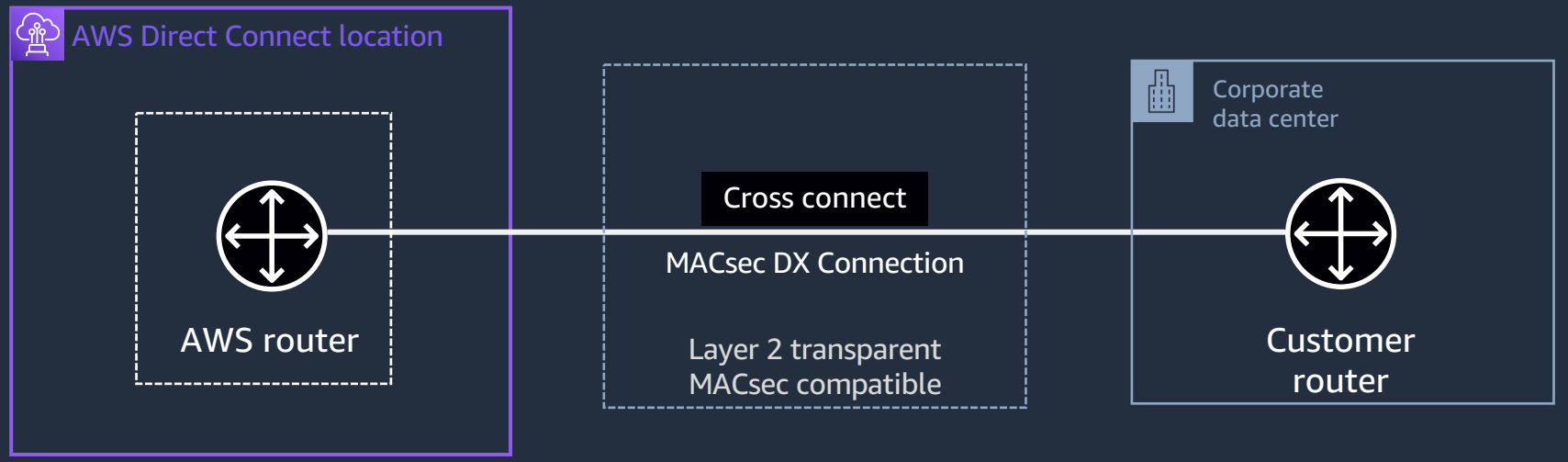
High-speed encryption

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

aws

Introducing: AWS Direct Connect MACsec



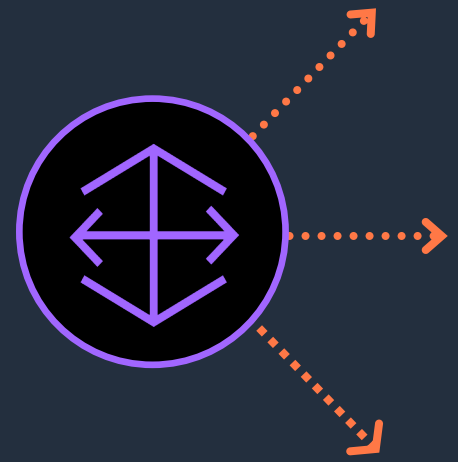


On-premises and global connectivity

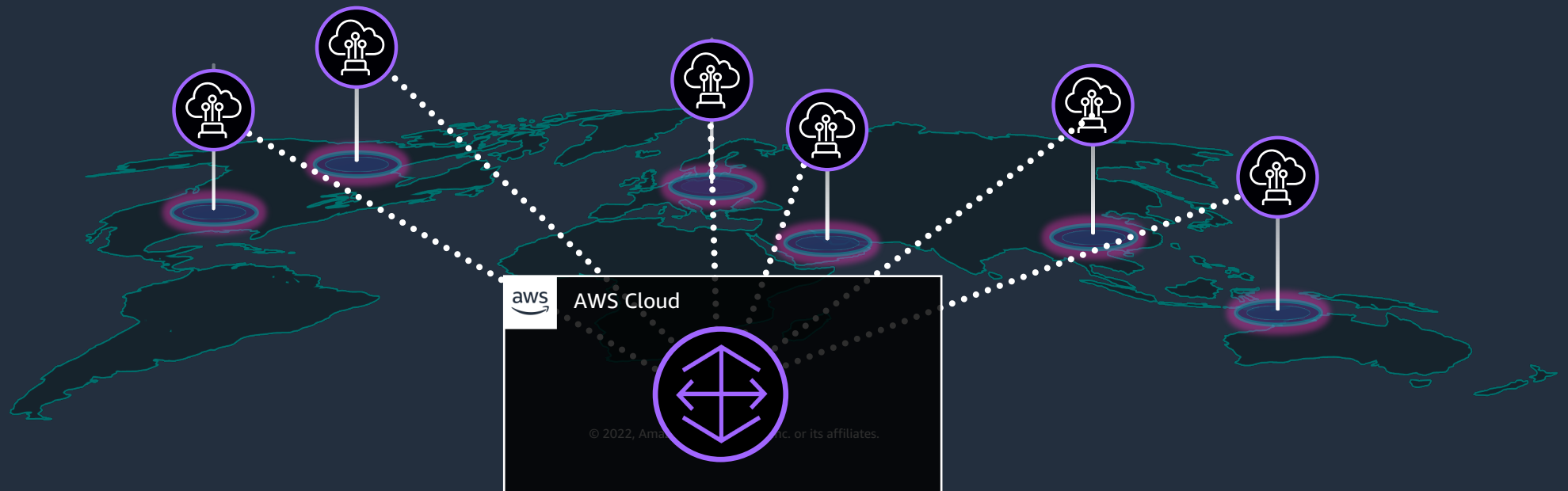
AWS Direct Connect
MACSEC , 100Gbps, and AWS Local Zones

AWS Direct Connect SiteLink
and AWS Direct Connect

Introducing: AWS Direct Connect SiteLink

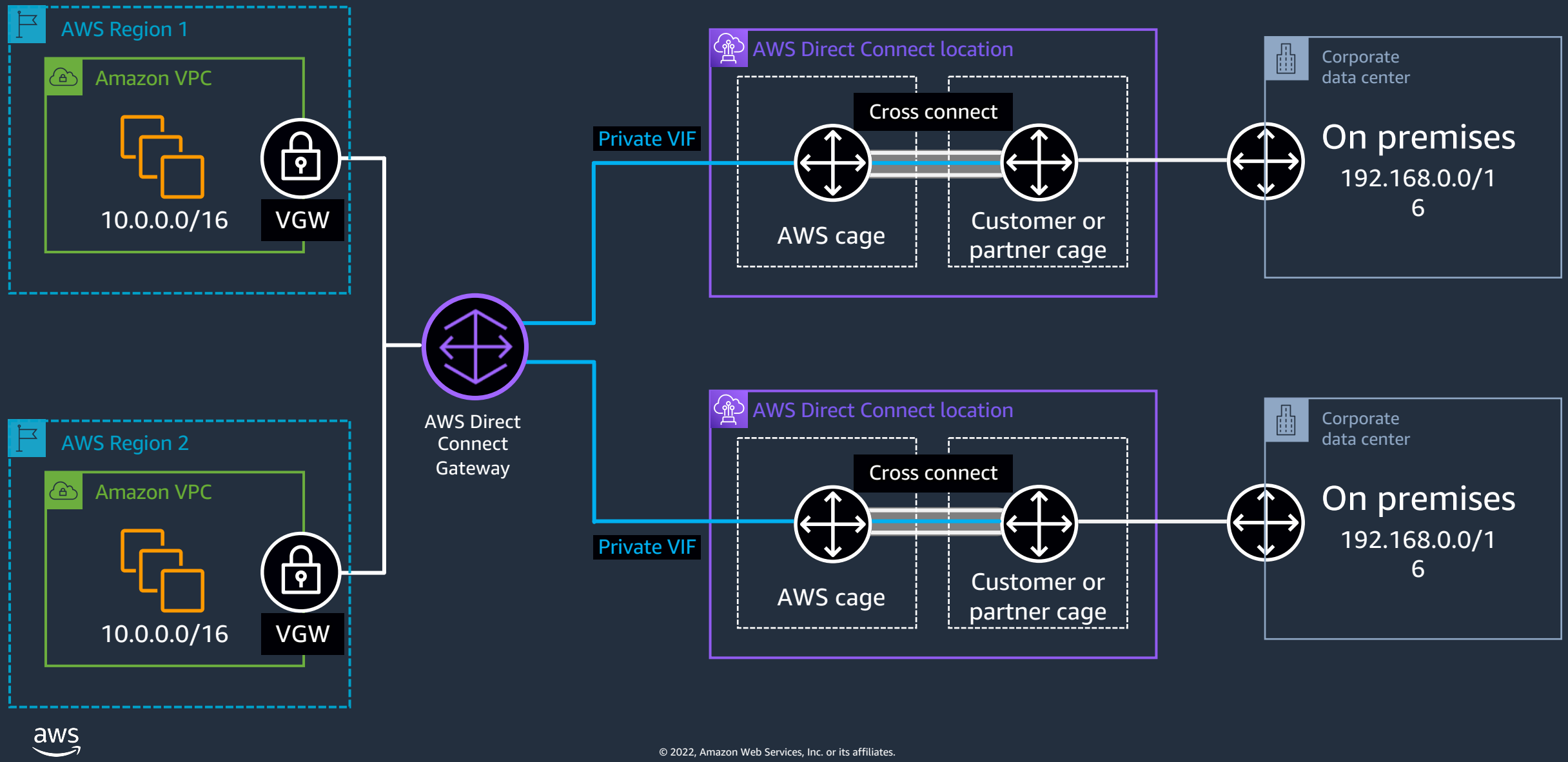


Create connections between your on-premises networks through the AWS global network backbone

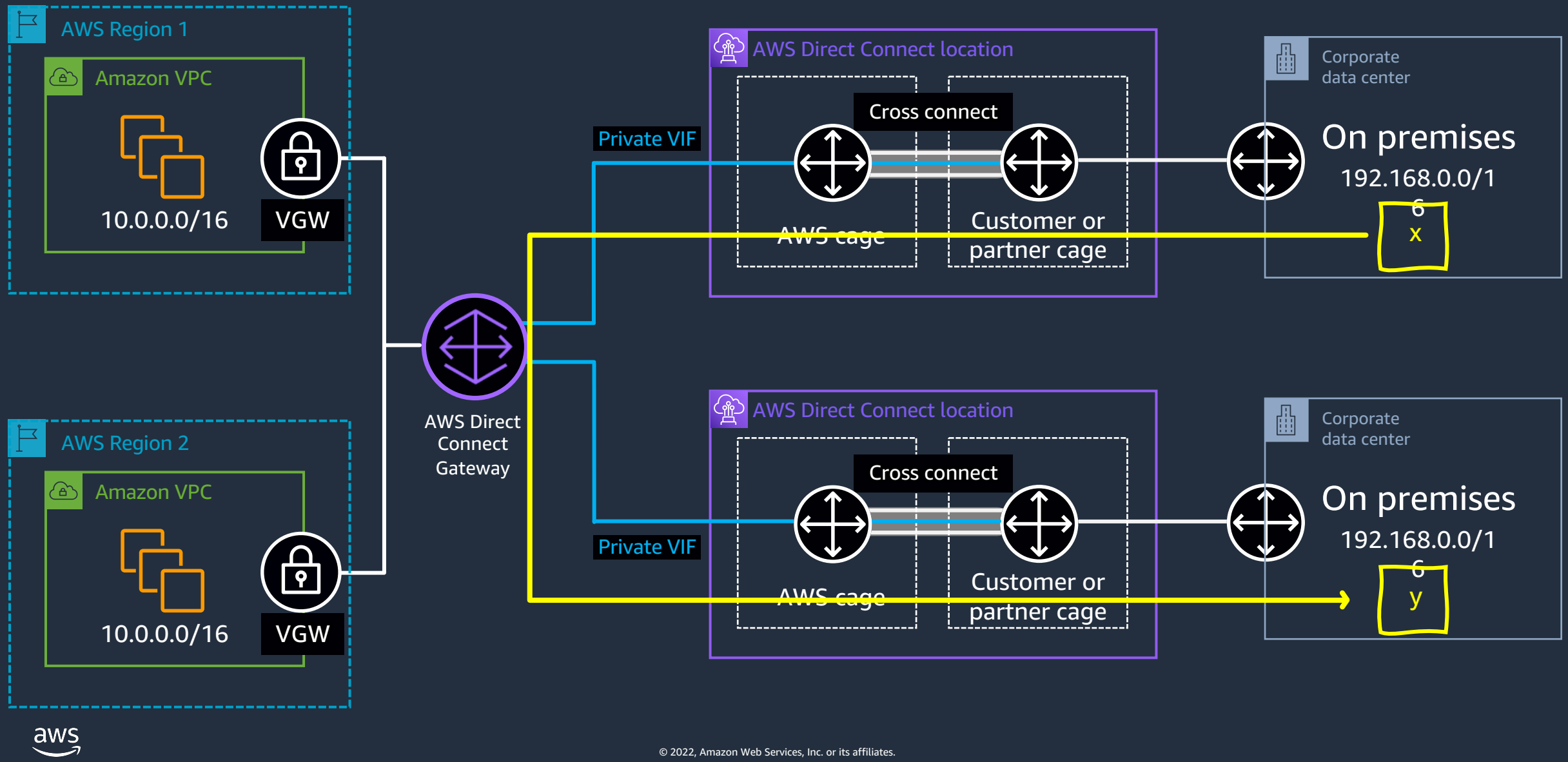


aws

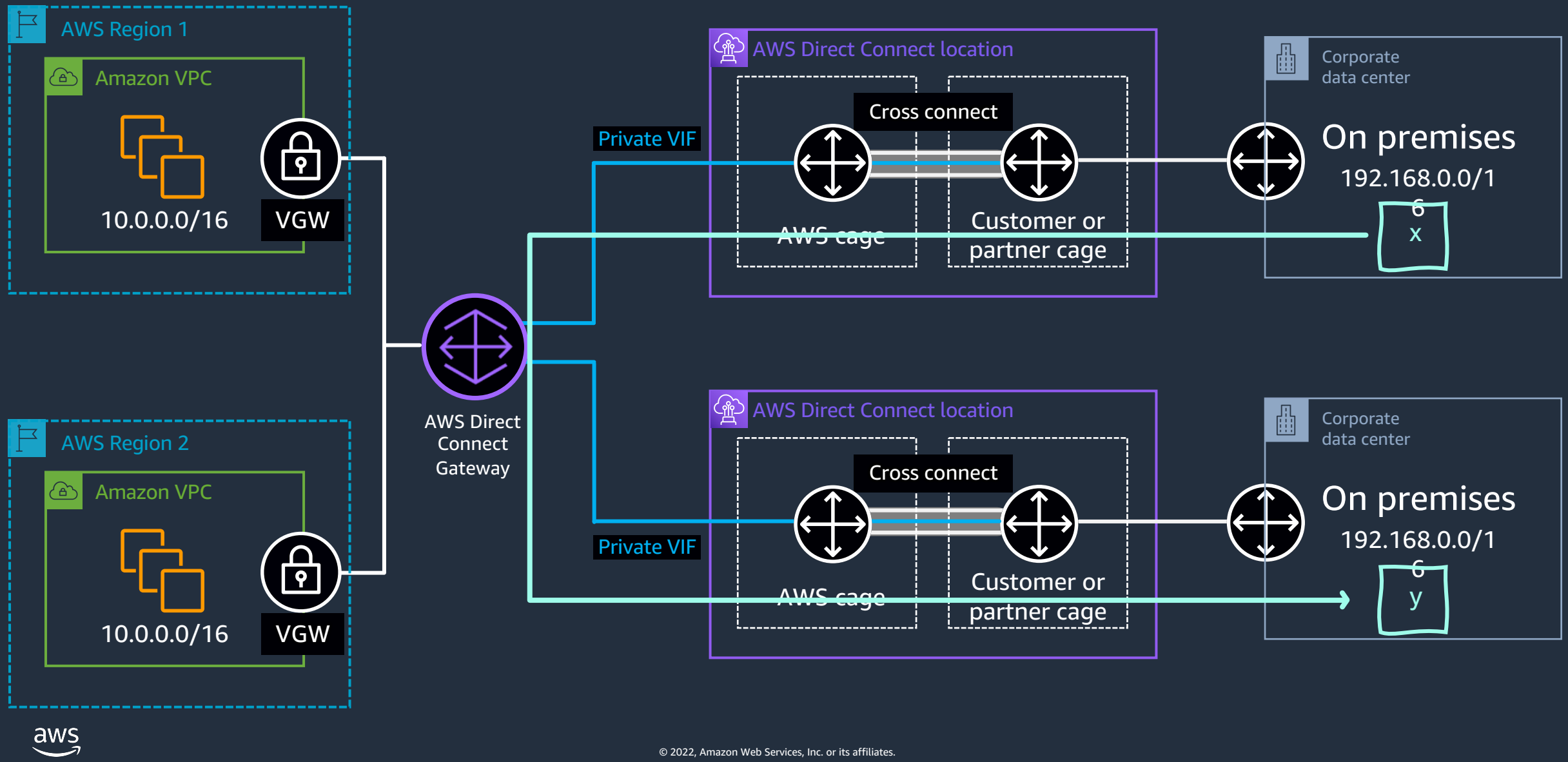
AWS Direct Connect SiteLink: Before



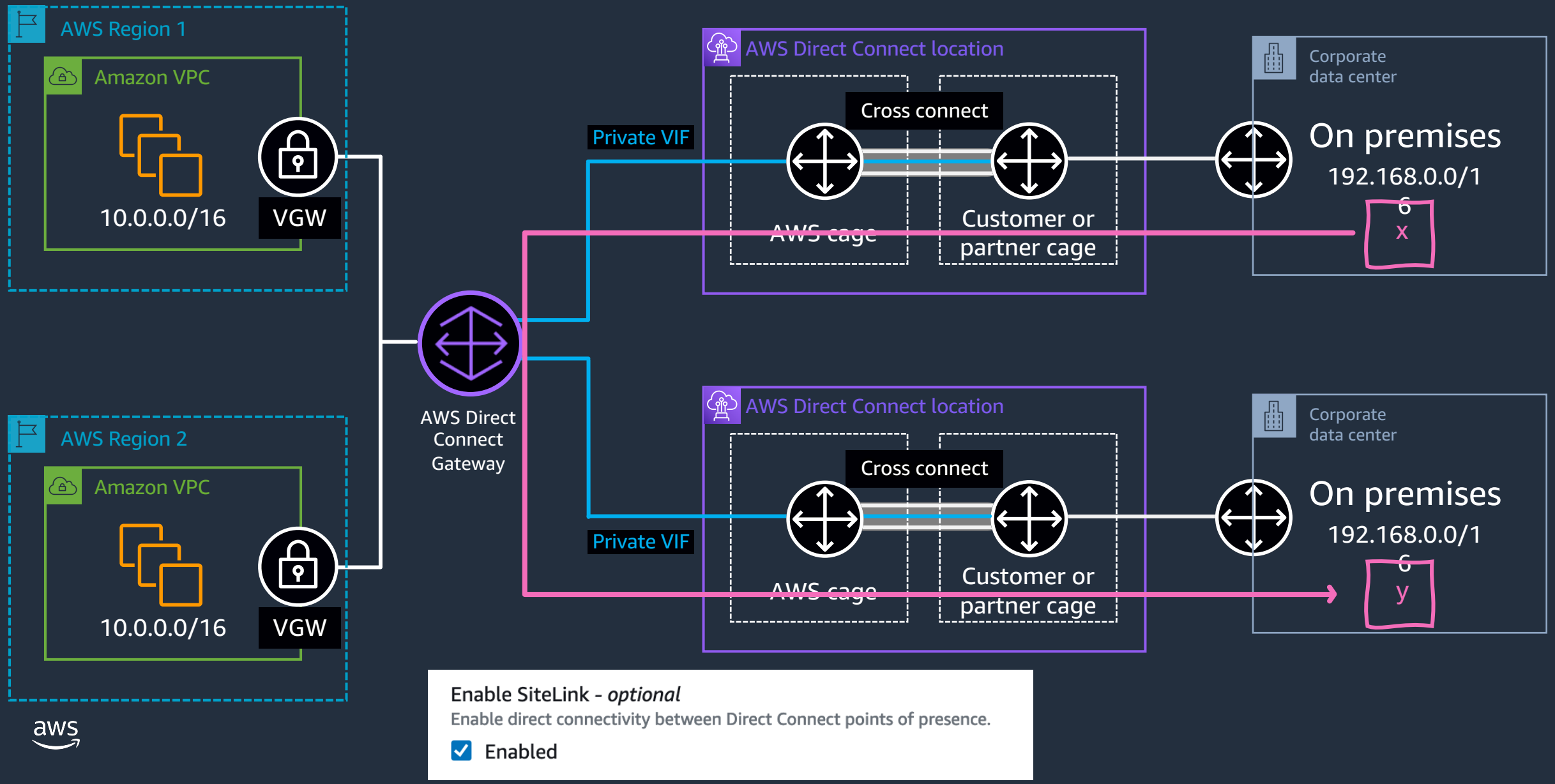
AWS Direct Connect SiteLink: Before

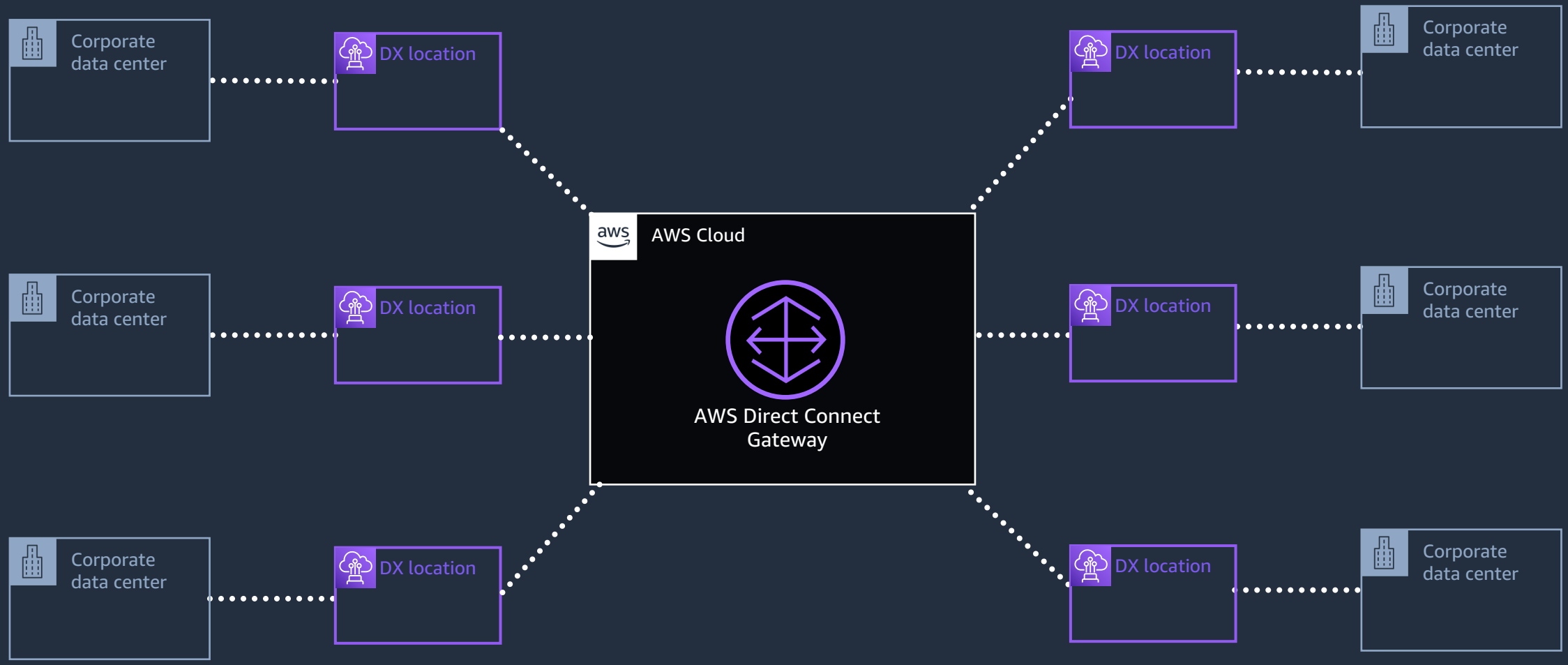


AWS Direct Connect SiteLink: Before



AWS Direct Connect SiteLink: After





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

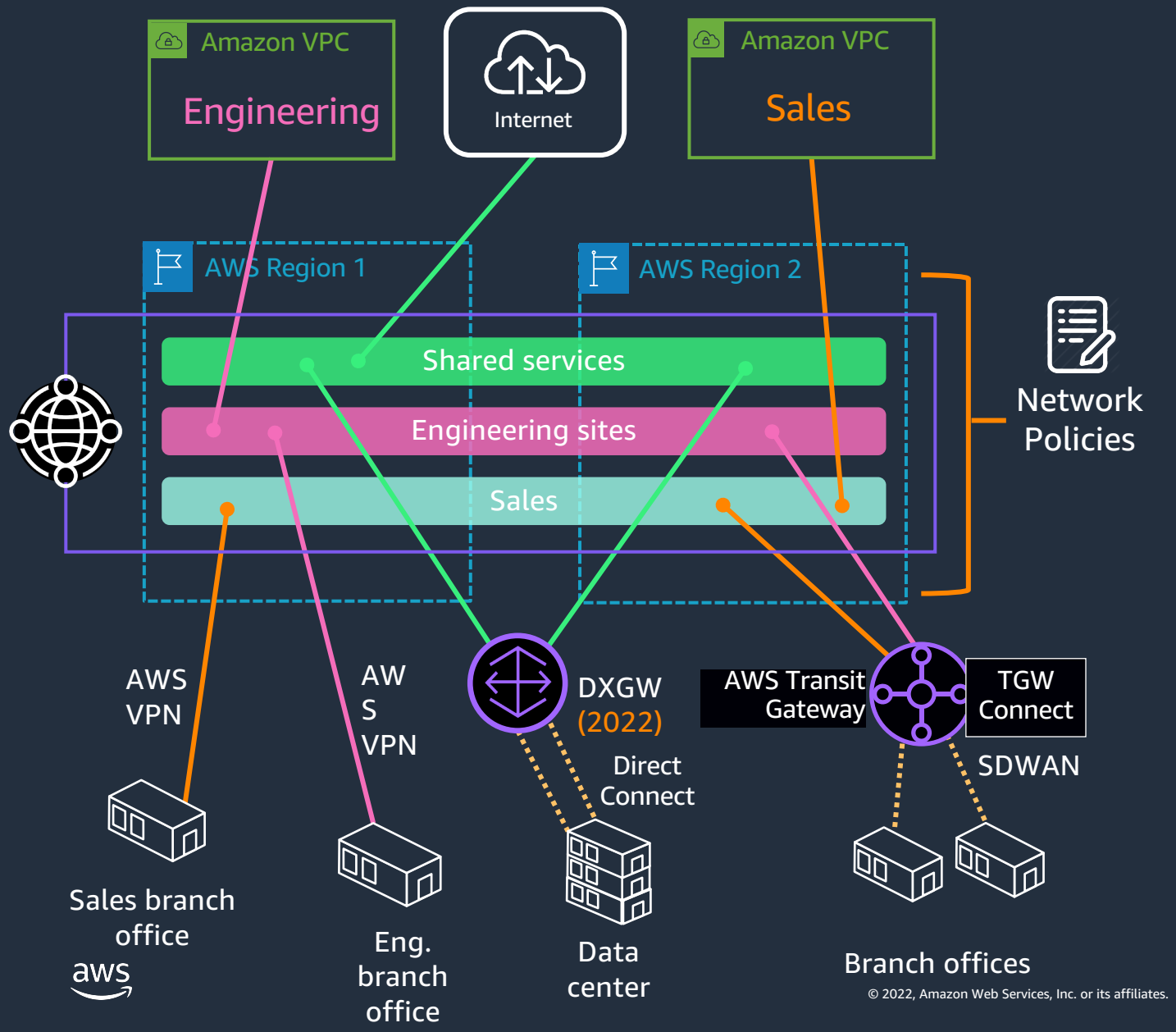
Build global networks in minutes

Use the AWS global backbone

Simplify WAN networking

Segment traffic with centralized policy

aws



AWS Cloud WAN

Network segments

Isolation between VPCs and on-premises sites

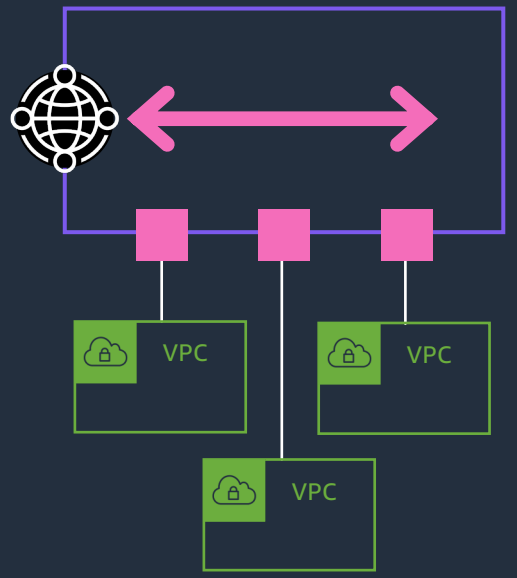
Network policies

Define L3 routing policies based on attributes and behavior

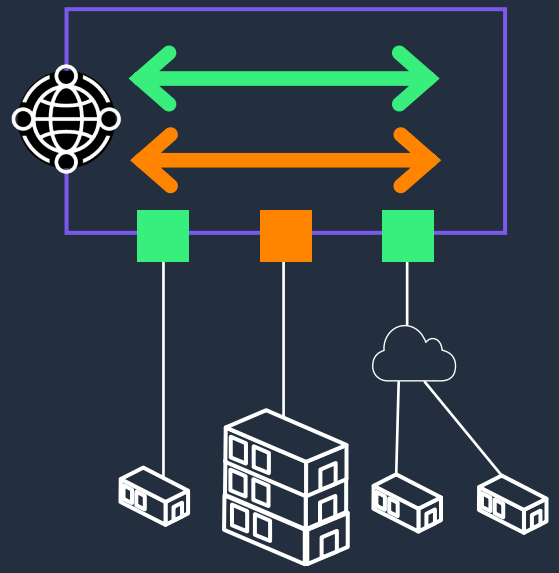
Performance monitoring

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

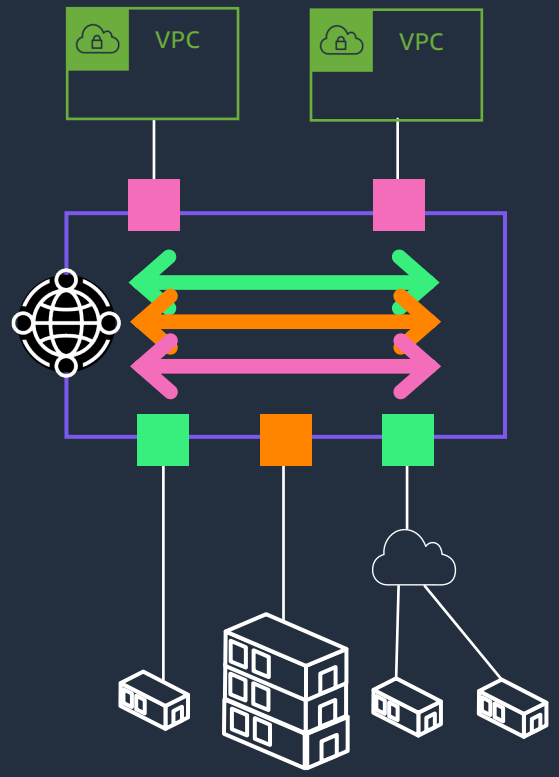
AWS Cloud WAN use cases



Between VPCs



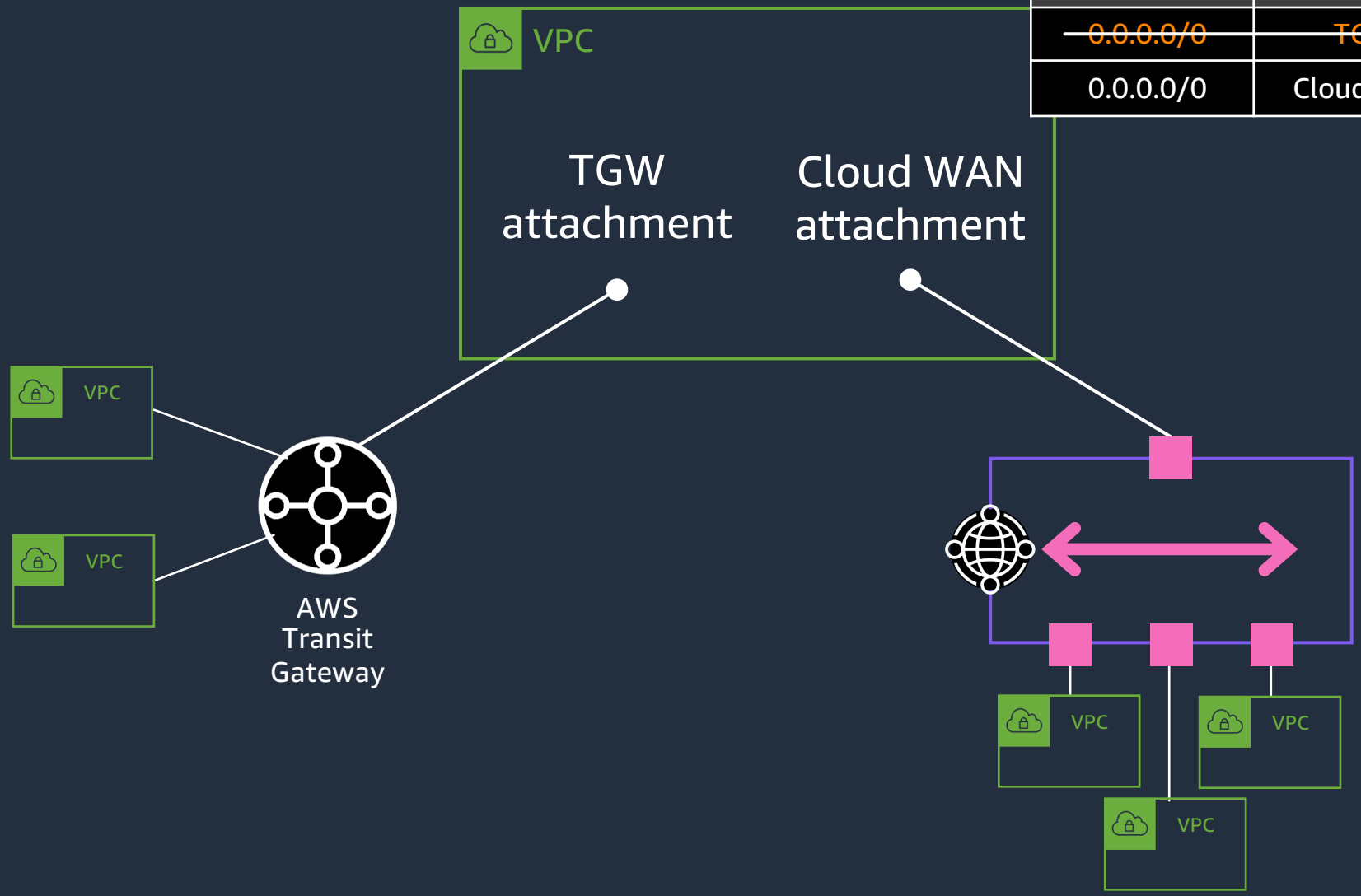
WAN



Hybrid

TGW and AWS Cloud WAN

VPC subnet table	
Destination	Target
~~0.0.0.0/0~~	~~TGW Attachment~~
0.0.0.0/0	Cloud WAN attachment



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

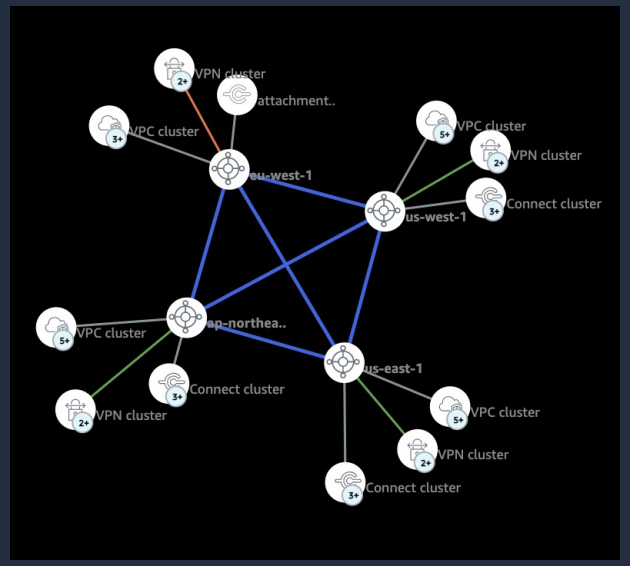
Support encryption (MACsec/IPsec)

Pay for what you use

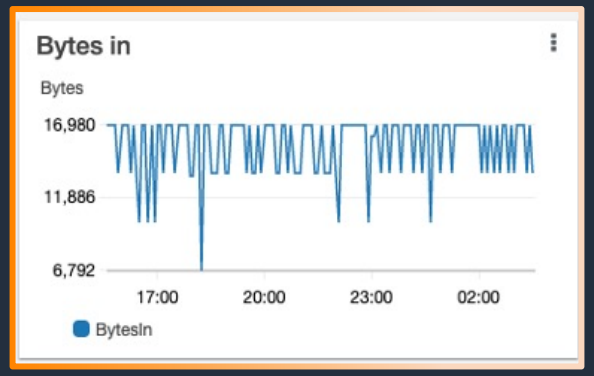
Available globally

Can also be used to access AWS resources

AWS Network Manager



Topologies



Metrics

Events

Thank you!

Dragos Madarasan

Please complete the session survey