AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

NET206

Advanced Amazon VPC design and new capabilities

Matt Lehwess
Principal Solutions Architect
EC2 Networking
AWS

Alexandra Huides
Senior Networking Specialist Solutions Architect
Strategic Accounts
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Some housekeeping items

SCAN ME

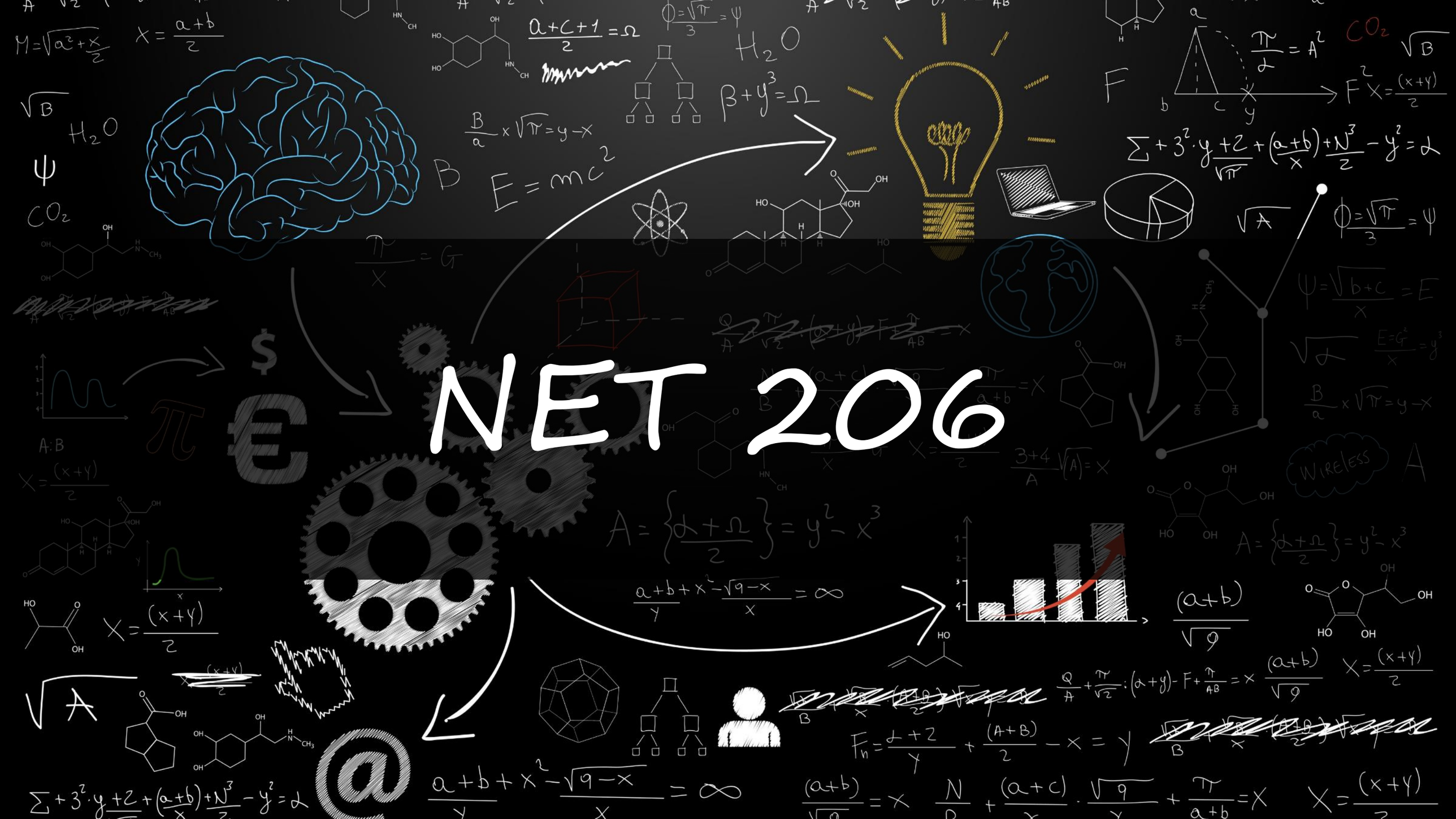
QR codes are sprinkled throughout



Our work-from- home networking wizard offers helpful hints

We'll let you know when a buildout is complete for photos

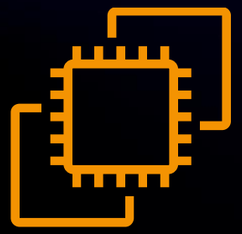
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.


NET 206



We became experts in baking

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

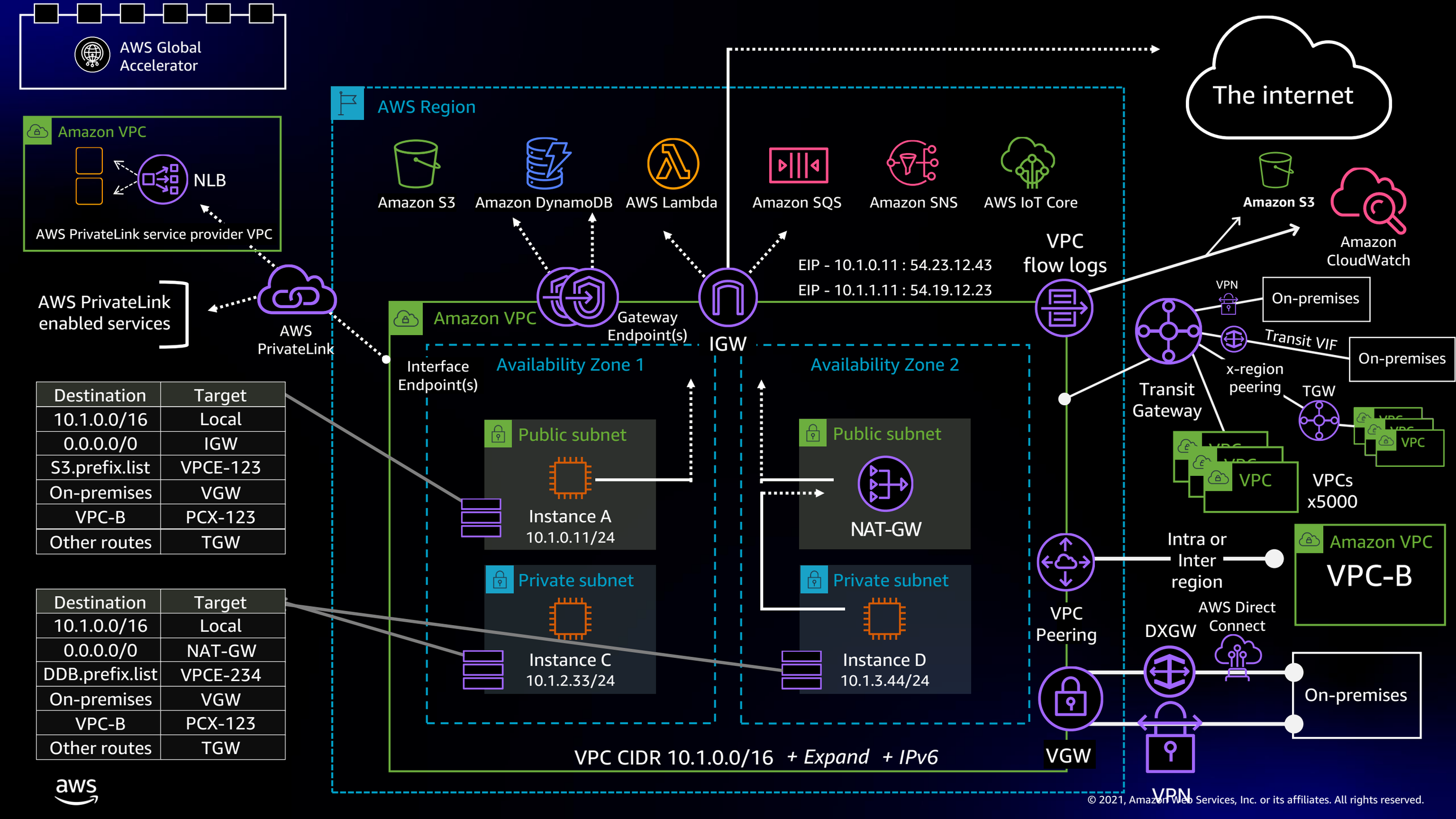
Private subnet

Instance D
10.1.3.44/24

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

aws

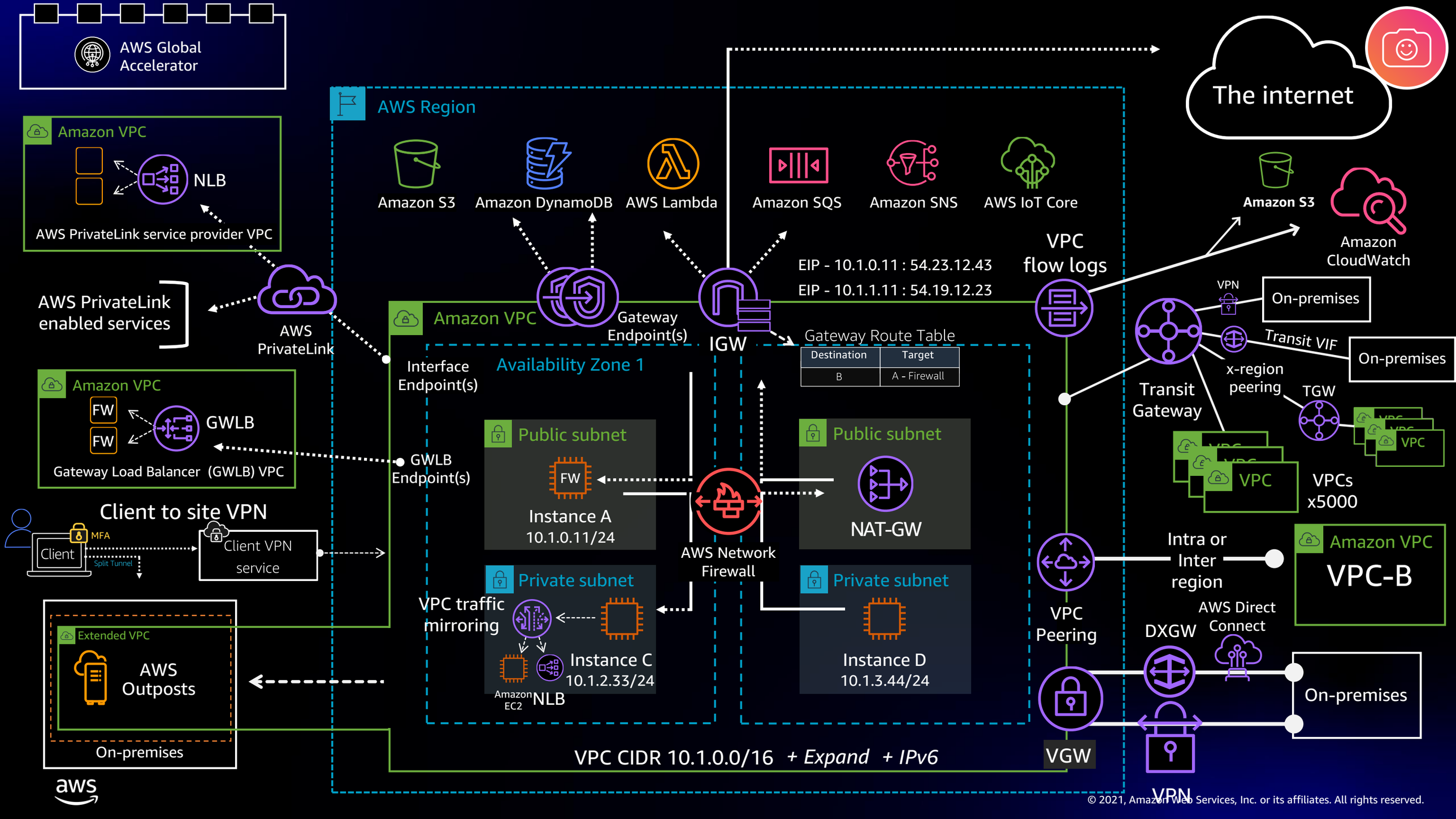
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

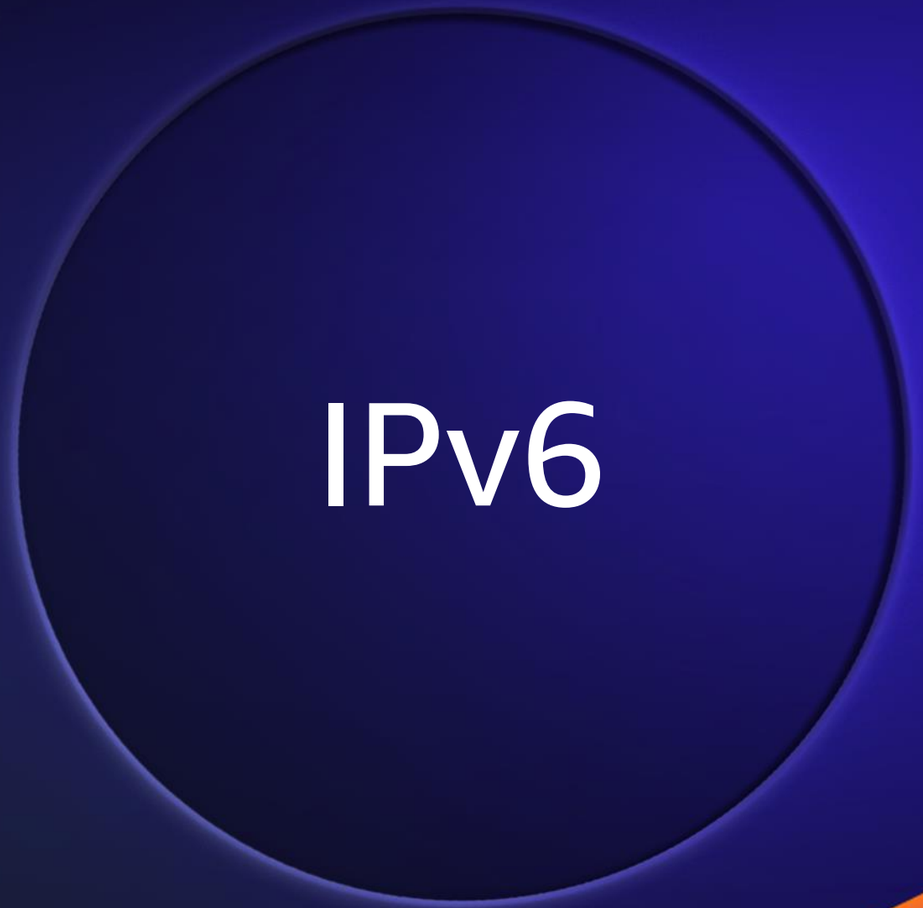
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



What else have we been up to?



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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

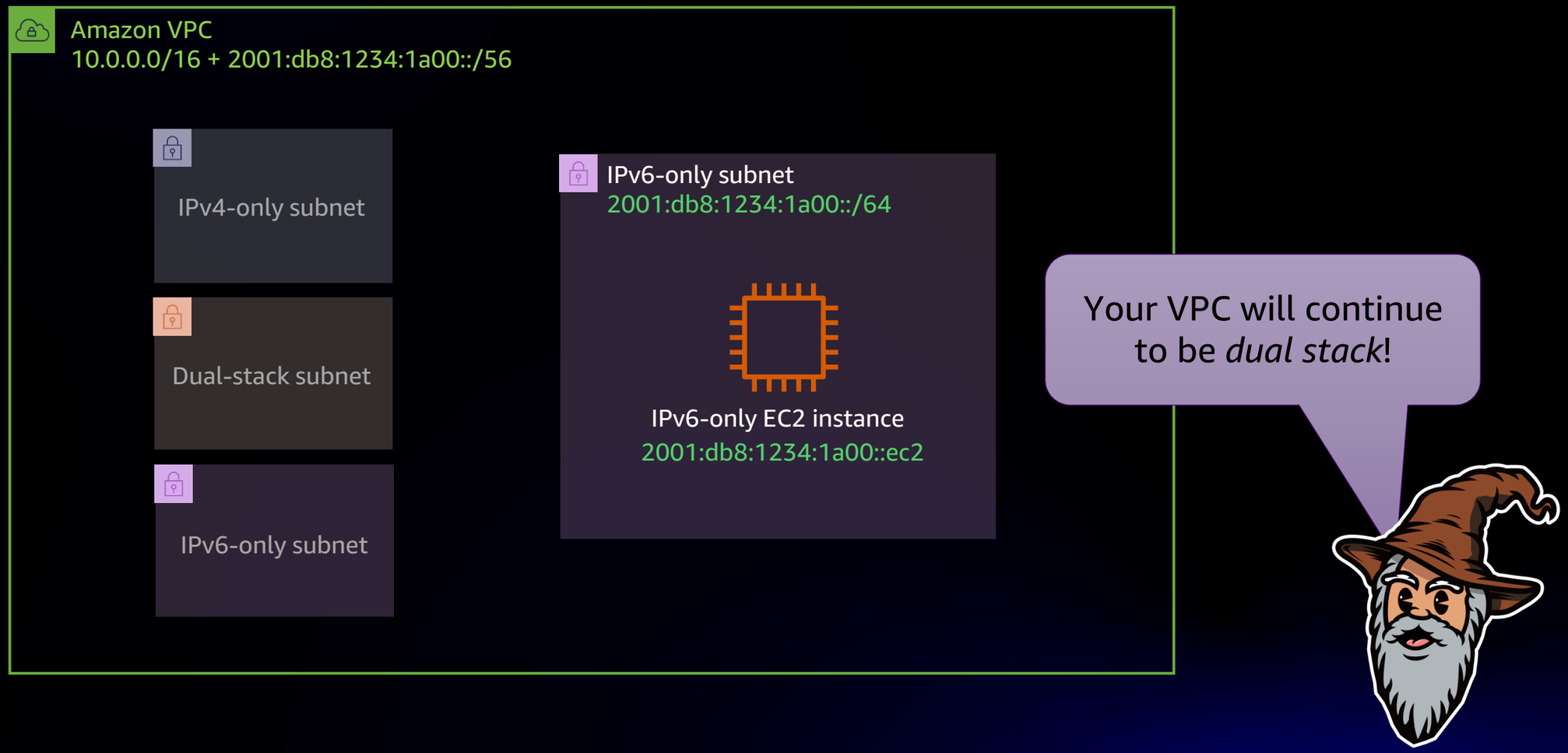
Amazon VPC: Native dual stack



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon dual-stack VPC: IPv6-only subnets

NEW



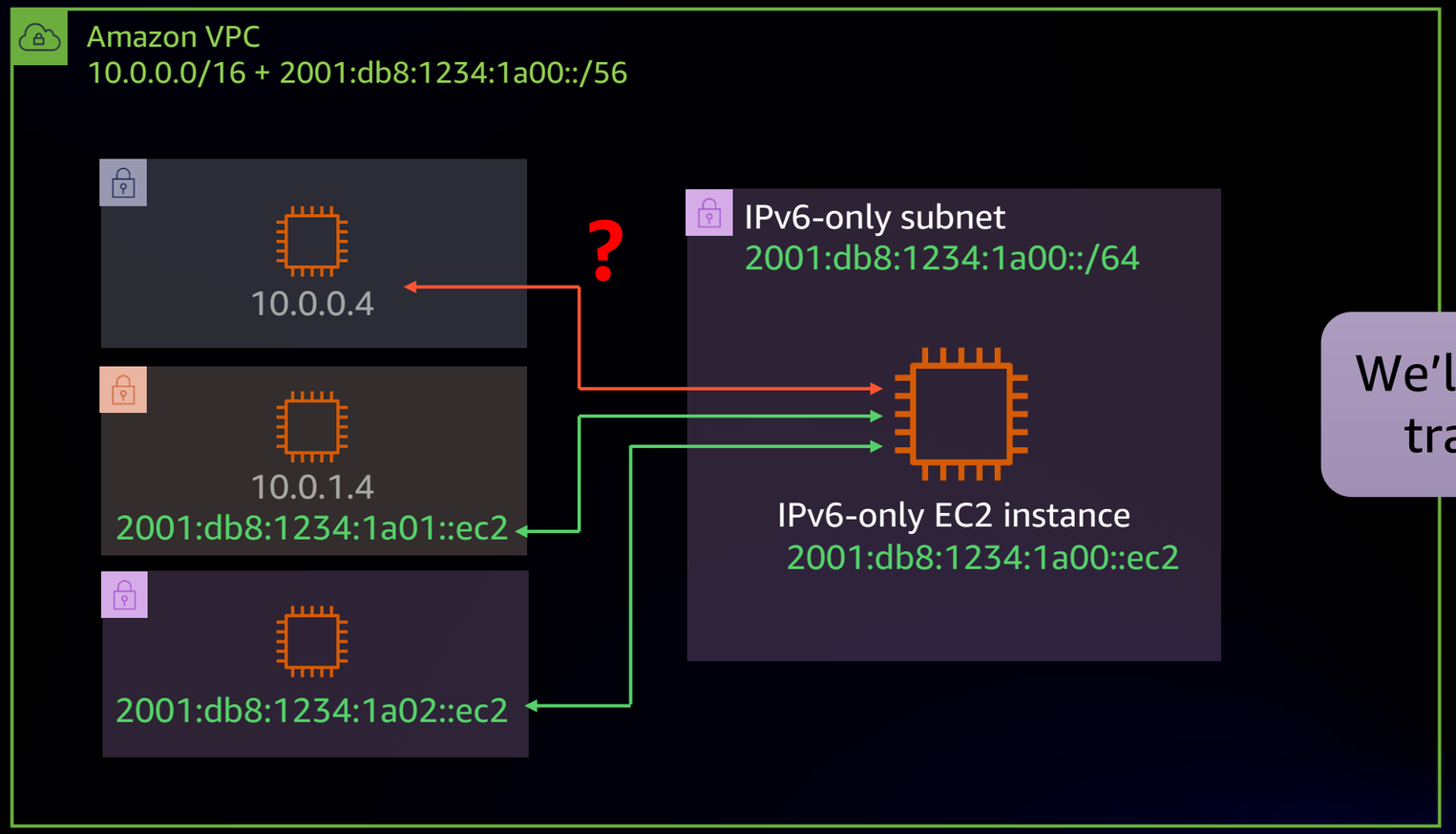
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traffic flows inside Amazon VPC

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon dual-stack VPC: IPv6 only subnets

FLOWS



We'll get back to this traffic flow later!



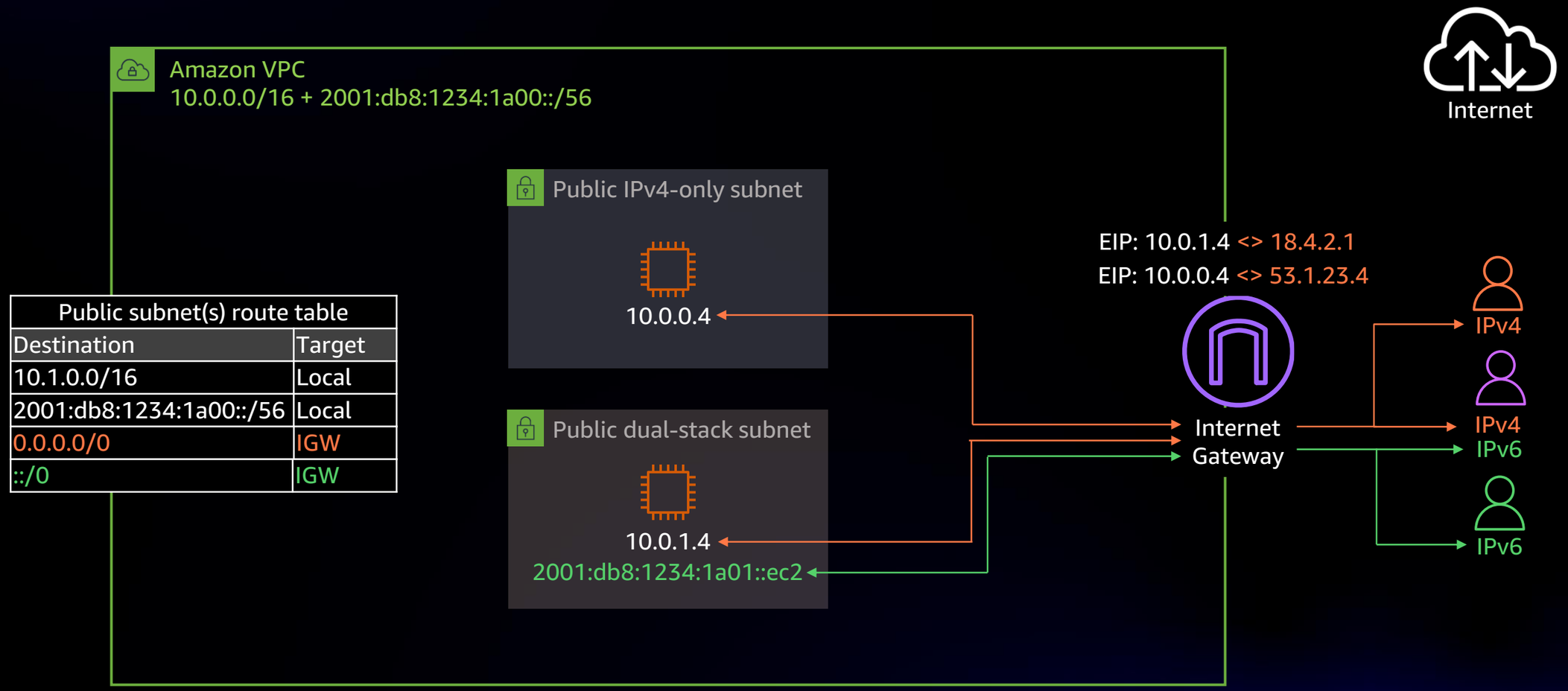
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Public subnets internet connectivity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon dual-stack VPC: Internet connectivity

PUBLIC SUBNETS

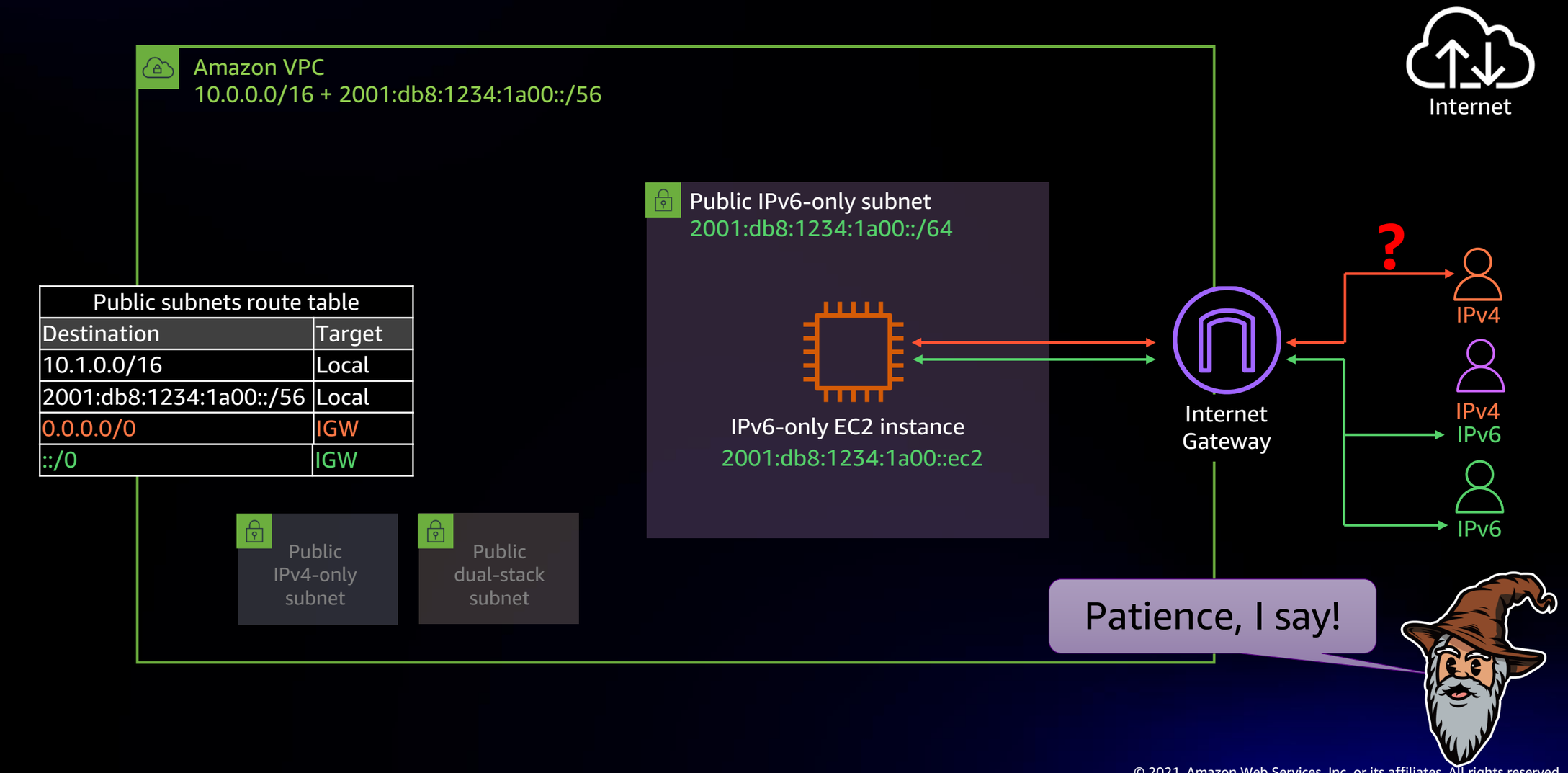


Public subnet(s) route table	
Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	IGW
::/0	IGW

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon dual-stack VPC: Internet connectivity

PUBLIC IPV6-ONLY SUBNETS



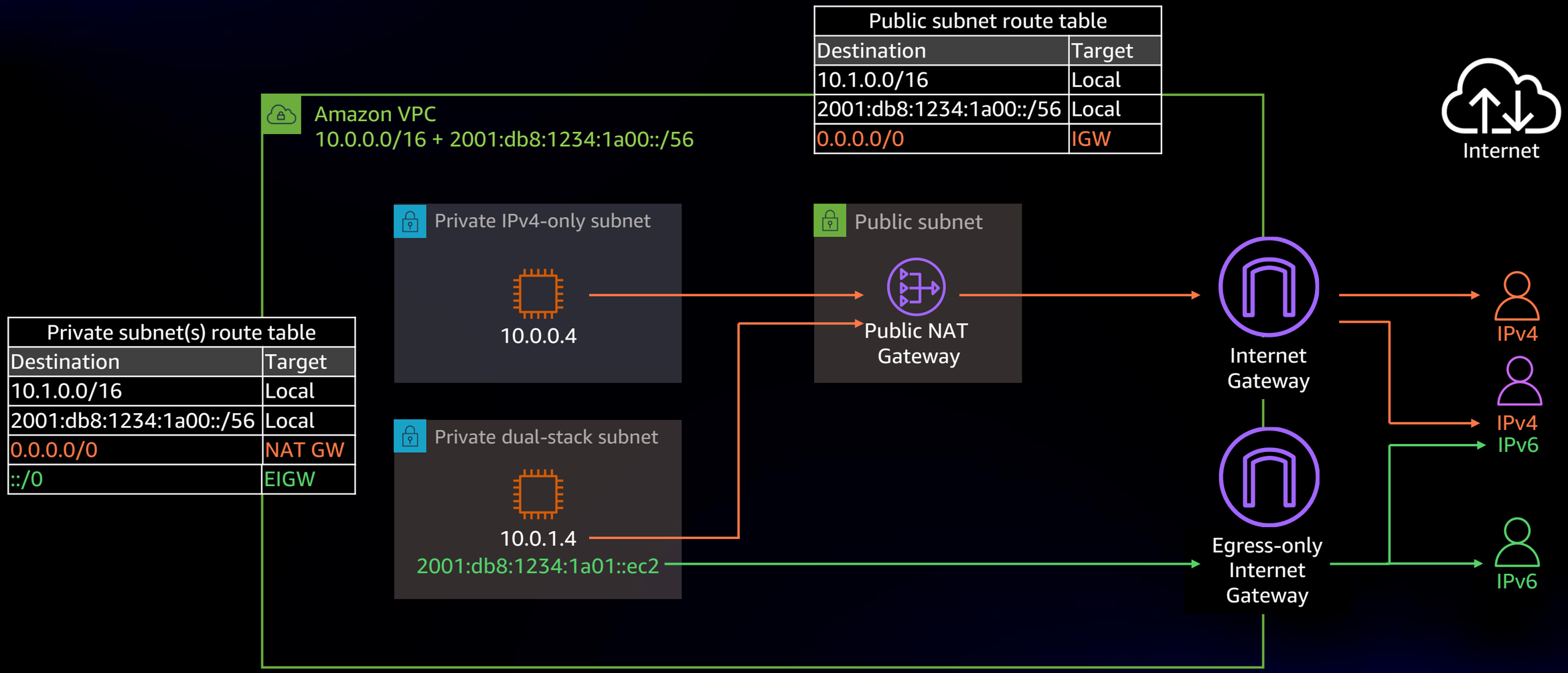
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Private subnets internet connectivity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon dual-stack VPC: Internet connectivity

PRIVATE SUBNETS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

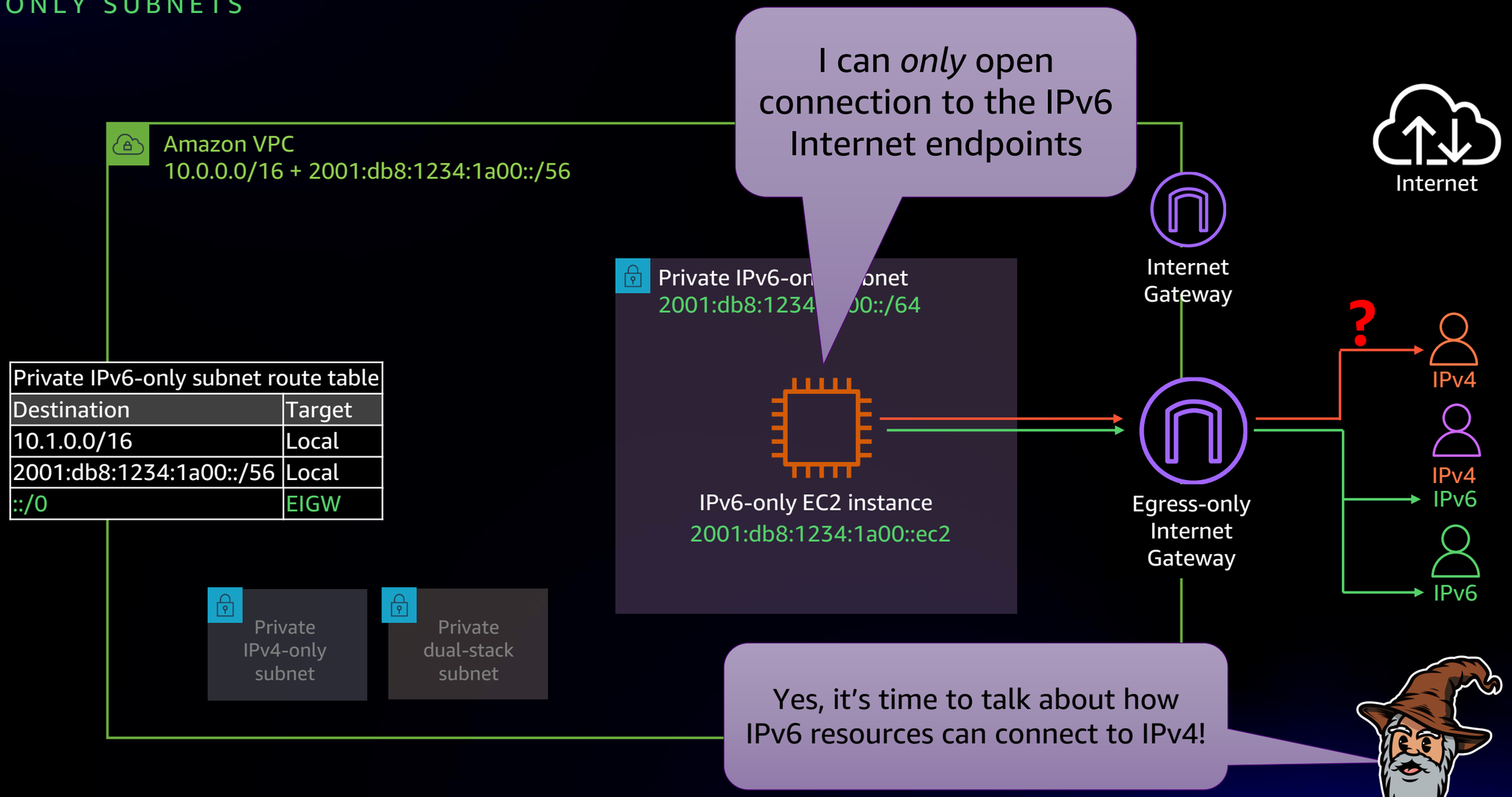
The EIGW does not allow internet connections to be opened to IPv6 resources in private subnets



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon dual-stack VPC: Internet connectivity

PRIVATE IPV6-ONLY SUBNETS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IPv6

Amazon VPC

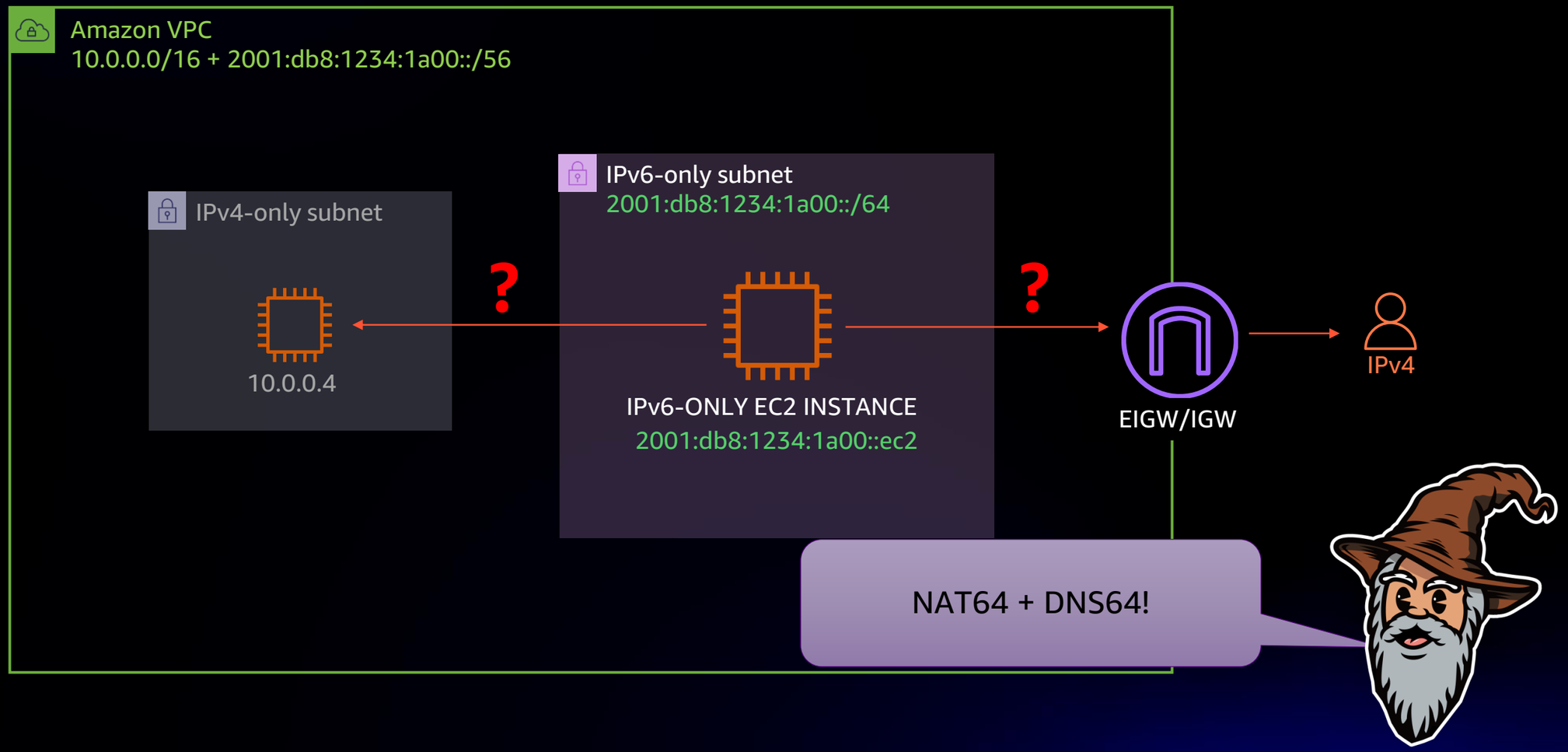
IPv6-only subnets

NAT64 and DNS64

Interoperability with IPv4 environments

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

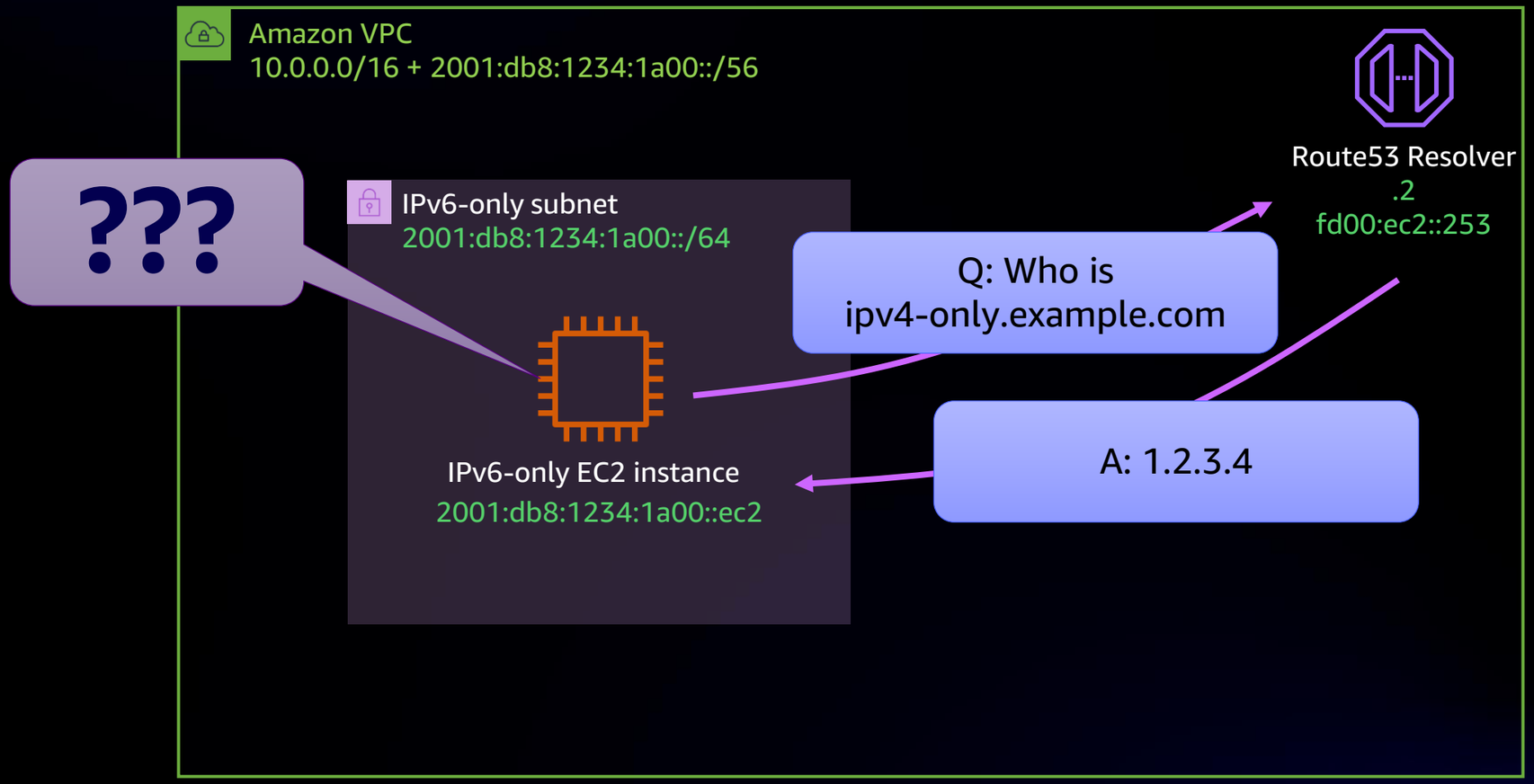
Amazon dual-stack VPC: IPv6 to IPv4



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC DNS

BEFORE

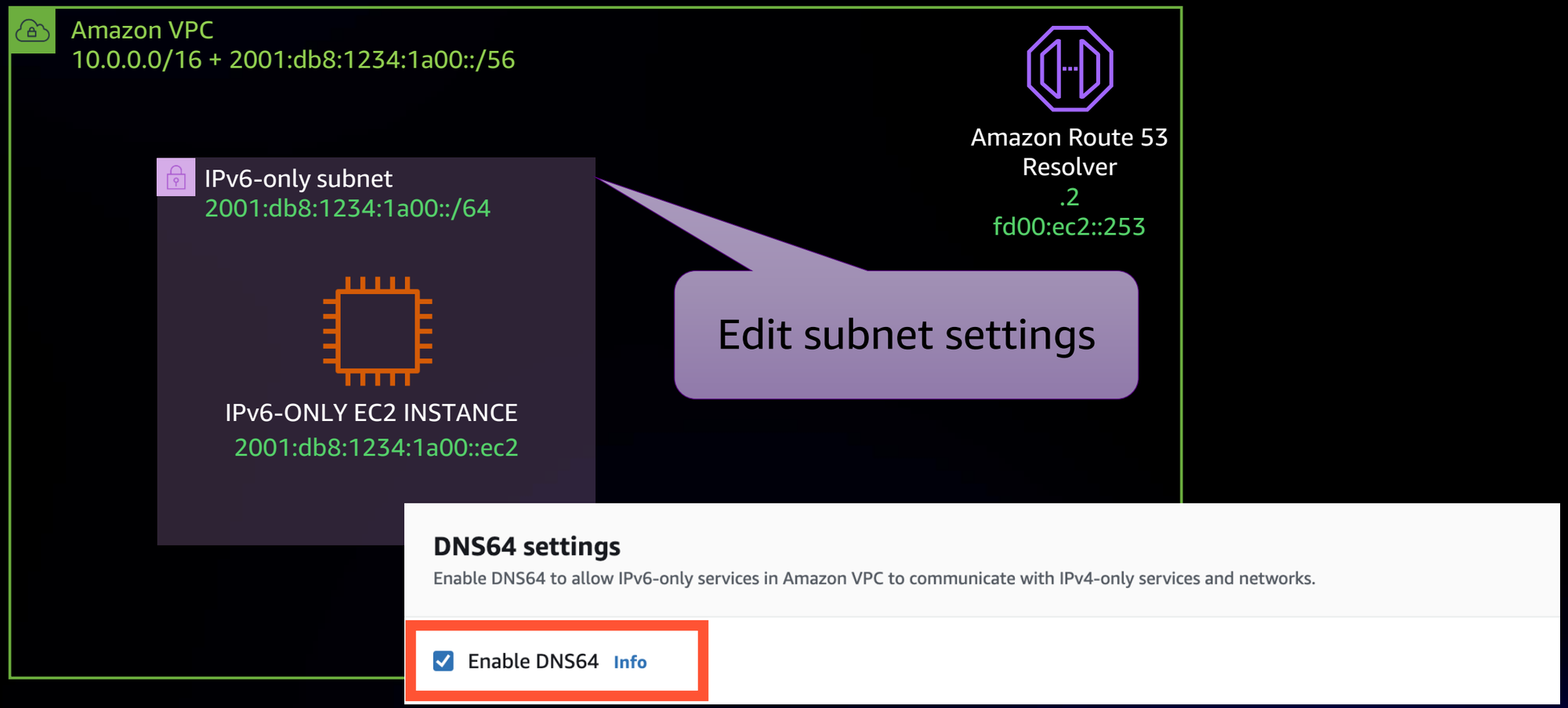


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DNS64

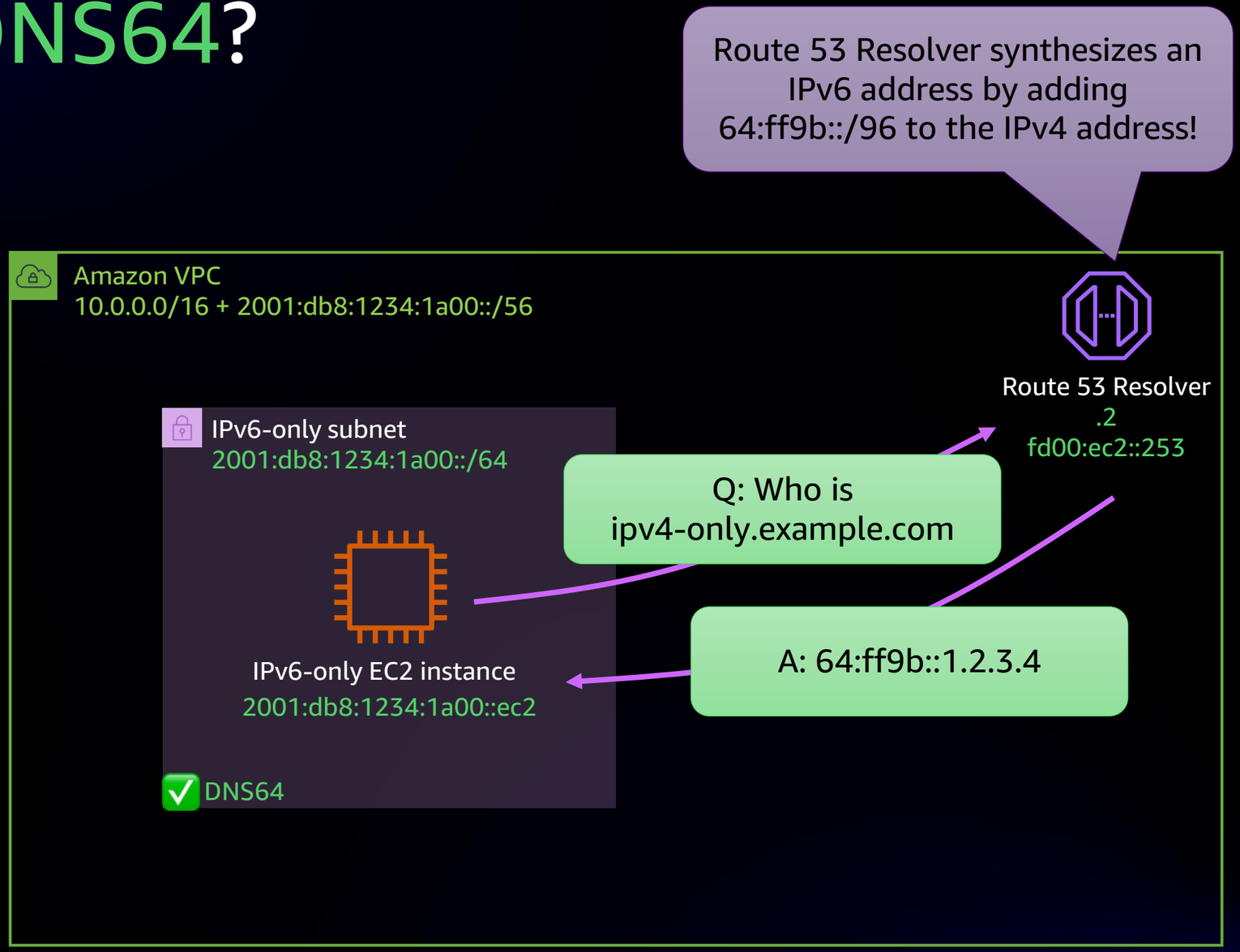
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is DNS64?



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is DNS64?



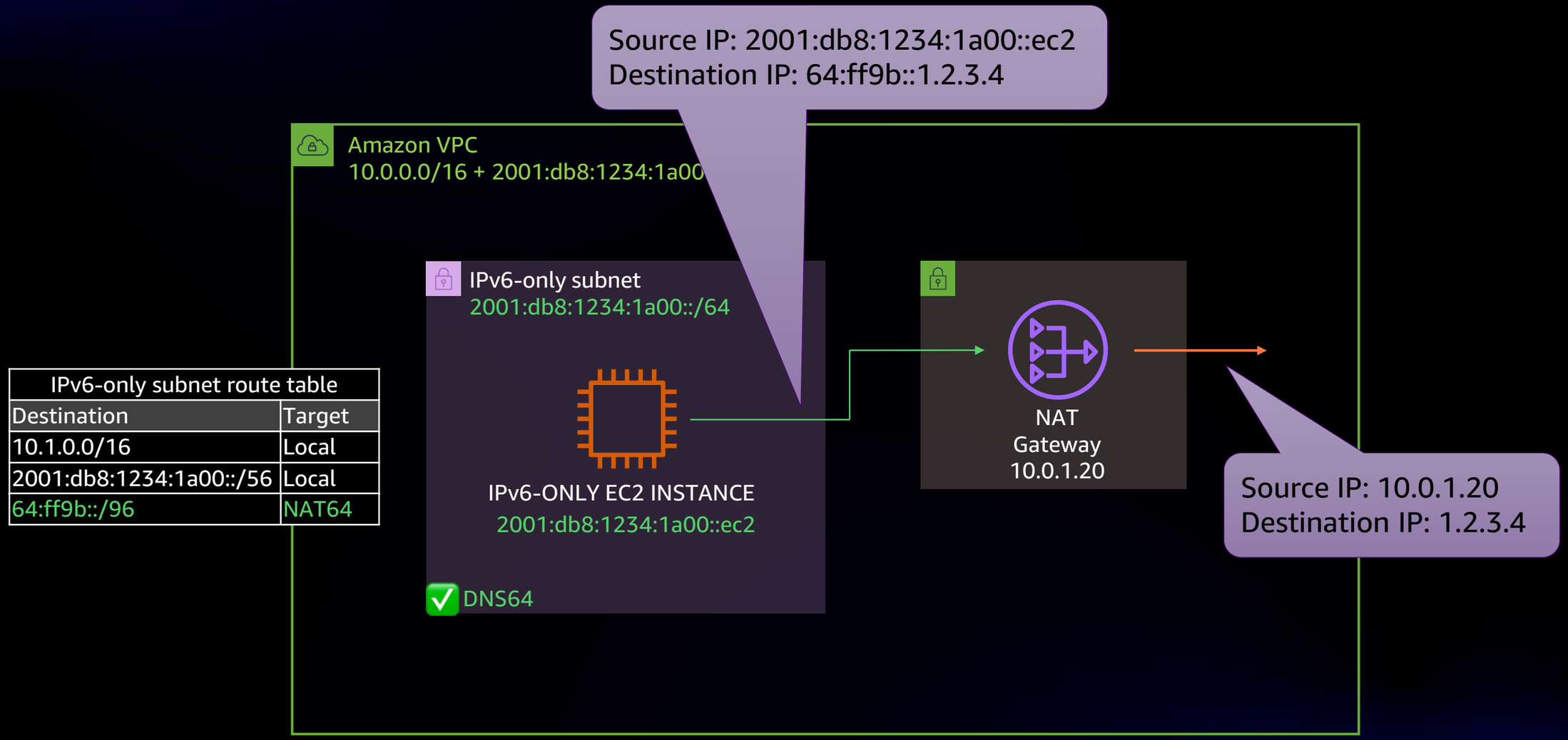
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

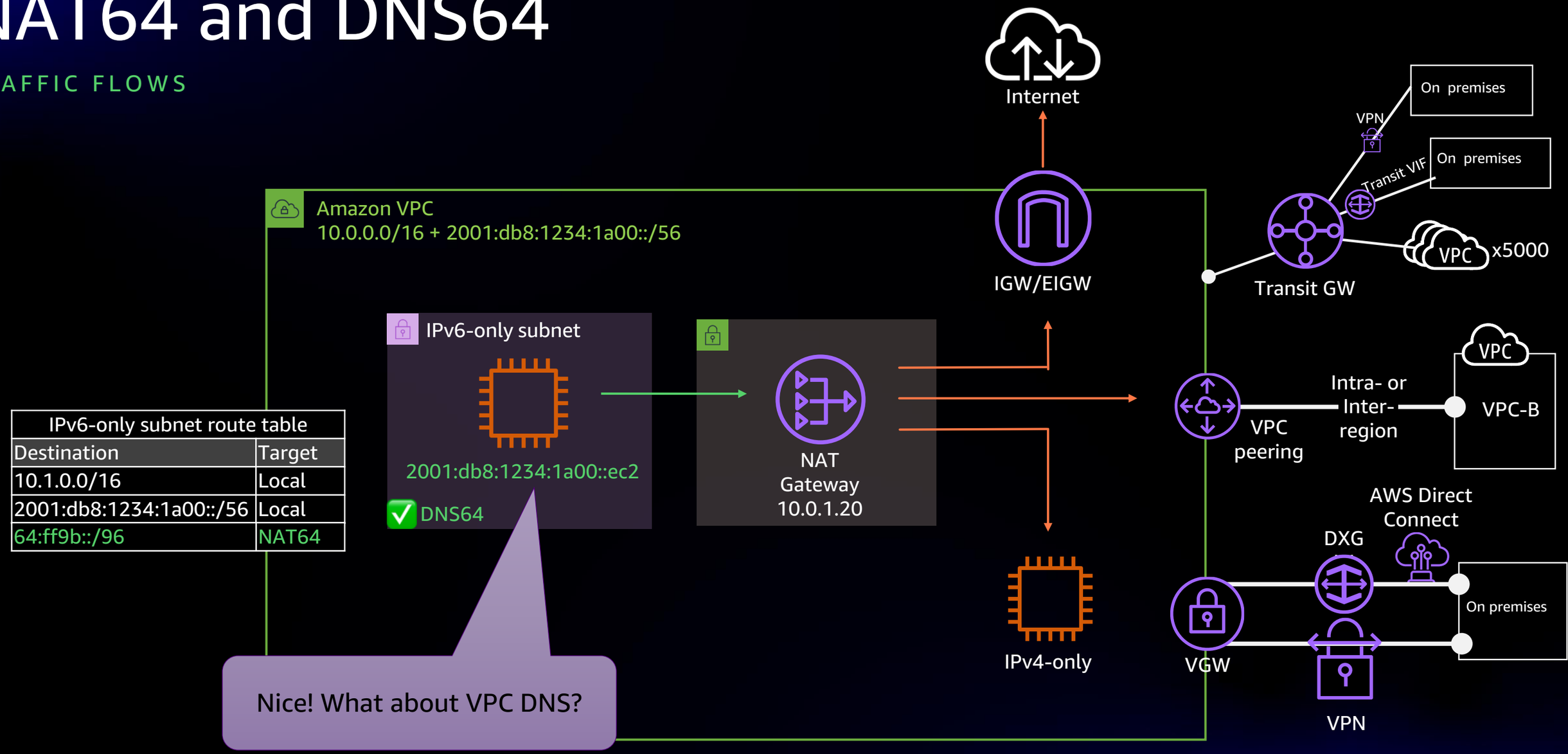
NAT64 is automatically available on your existing NAT gateways or on any new NAT gateways you create



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IPv6

Amazon VPC

IPv6-only subnets

NAT64 and DNS64

Interoperability with IPv4 environments

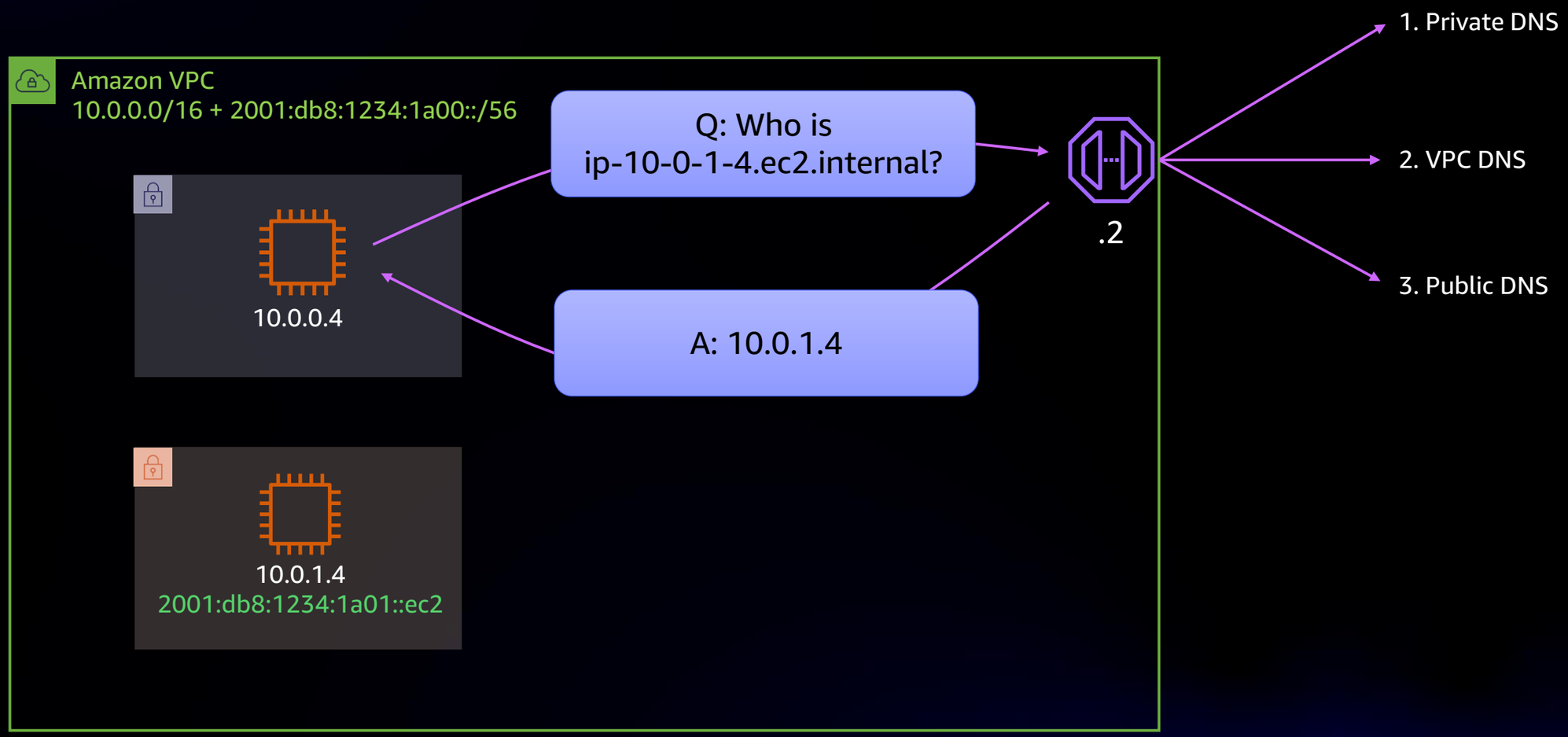
Amazon EC2

Resource-based instance naming

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

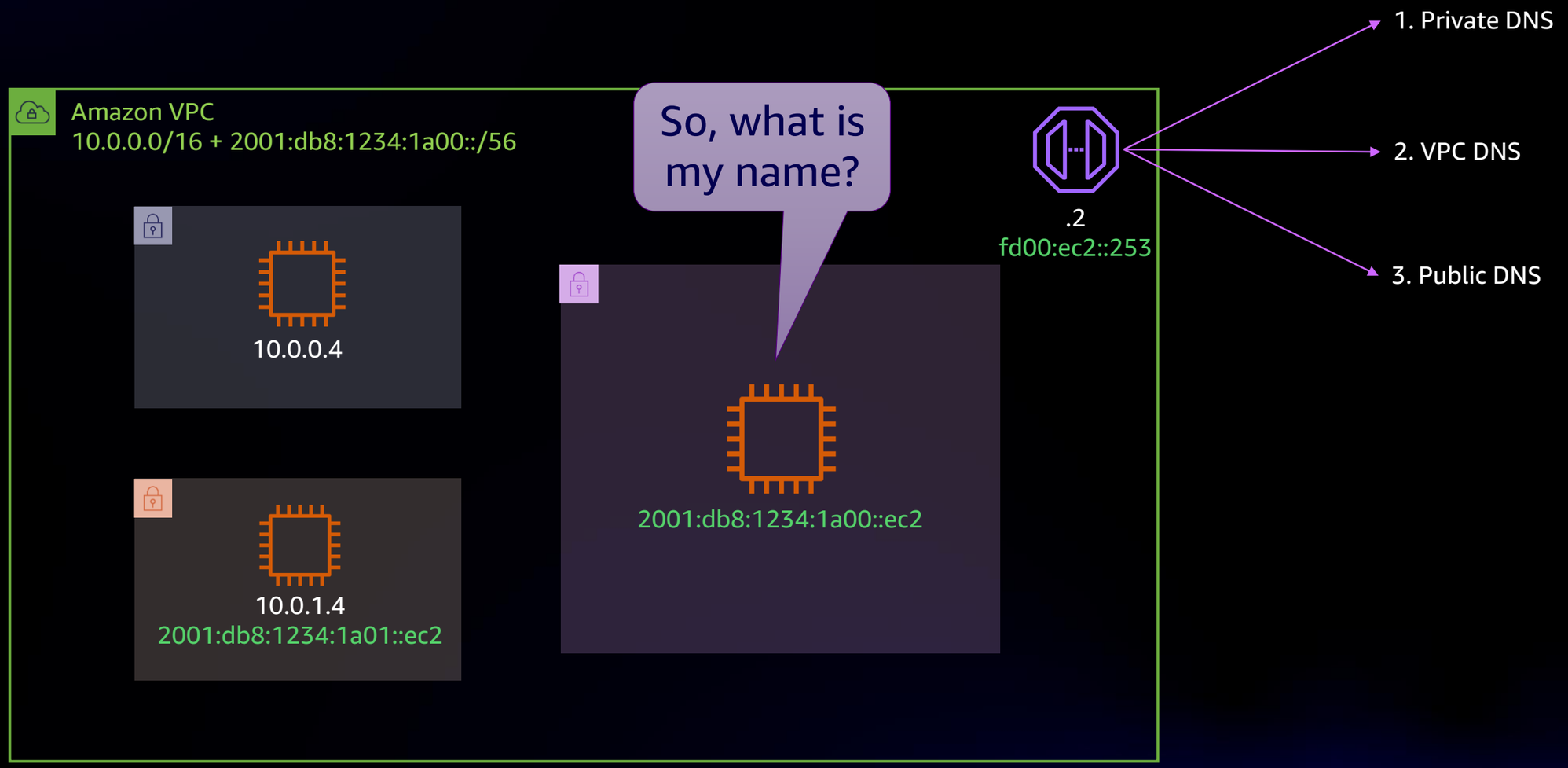
Amazon EC2 instance naming

IPV4-BASED NAMING (IPBN)



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

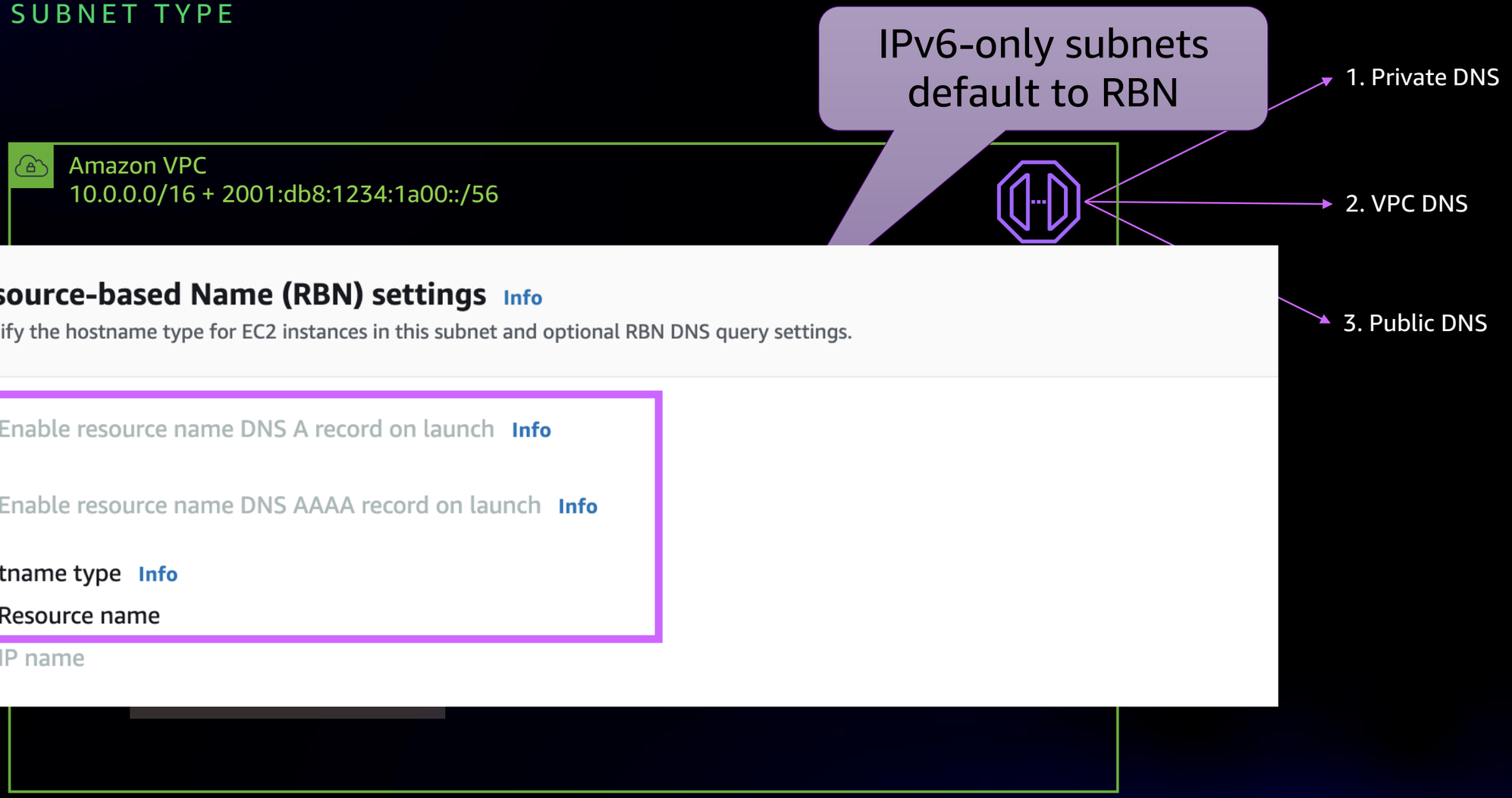
Amazon EC2 instance naming



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EC2: Resource-based naming (RBN)

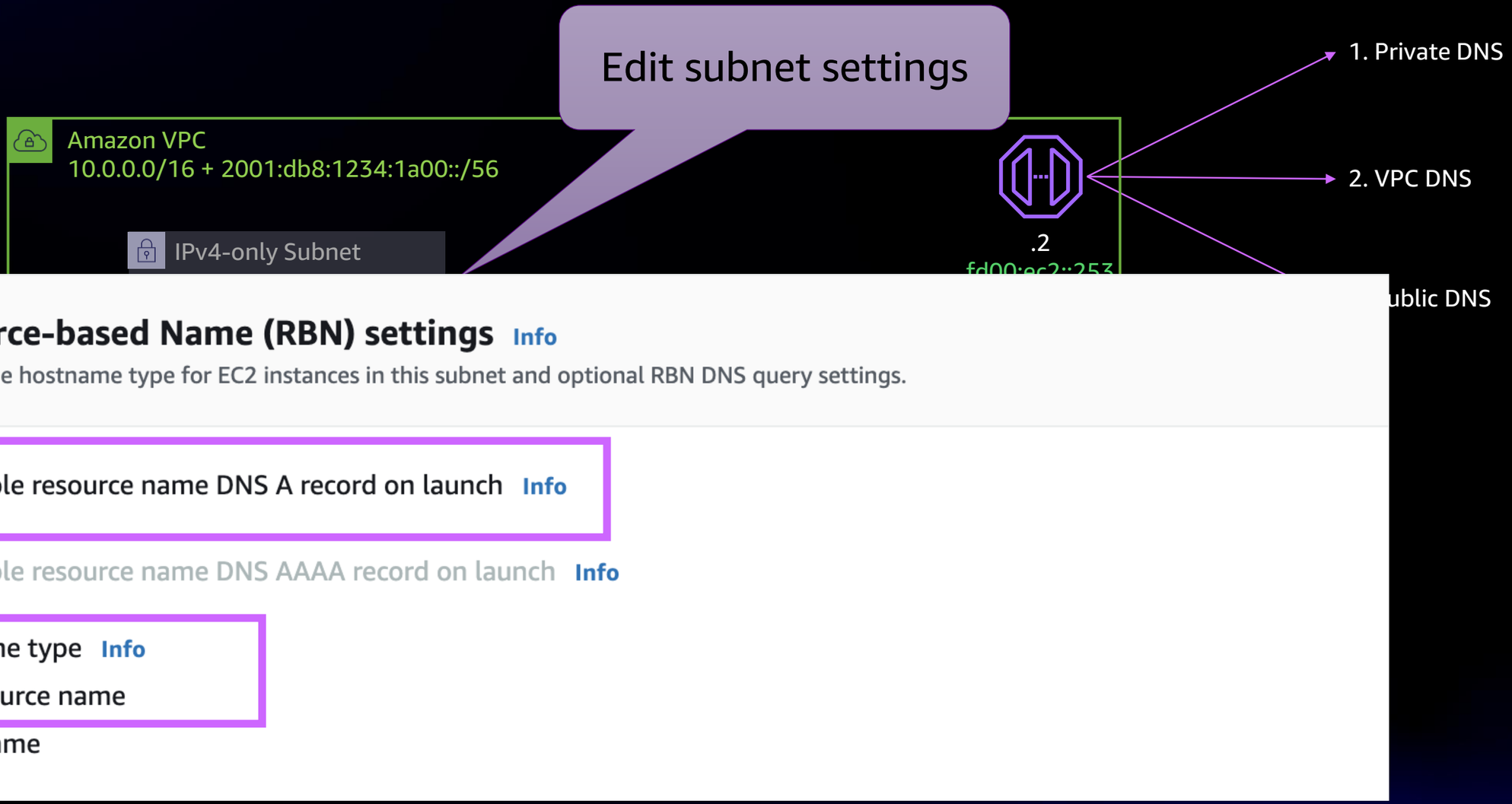
SETTINGS FOR EACH SUBNET TYPE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EC2: Resource-based naming

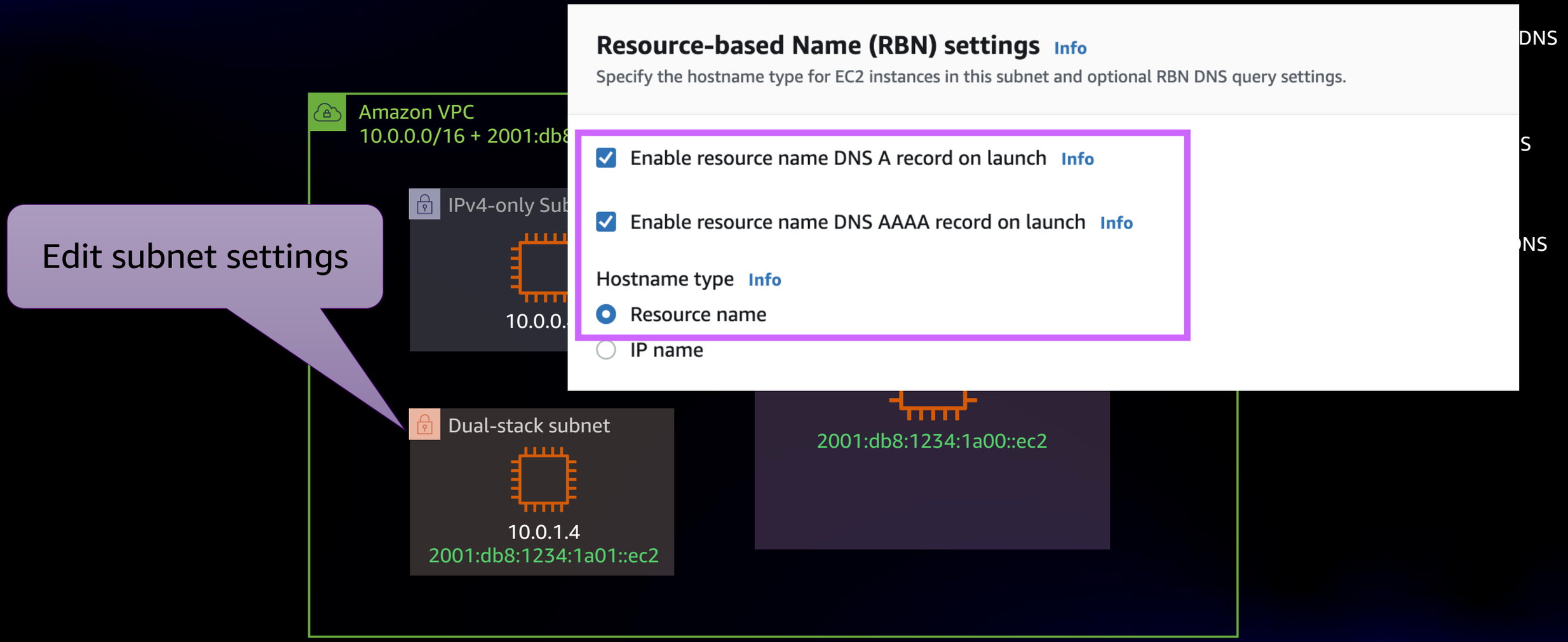
SETTINGS FOR EACH SUBNET TYPE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

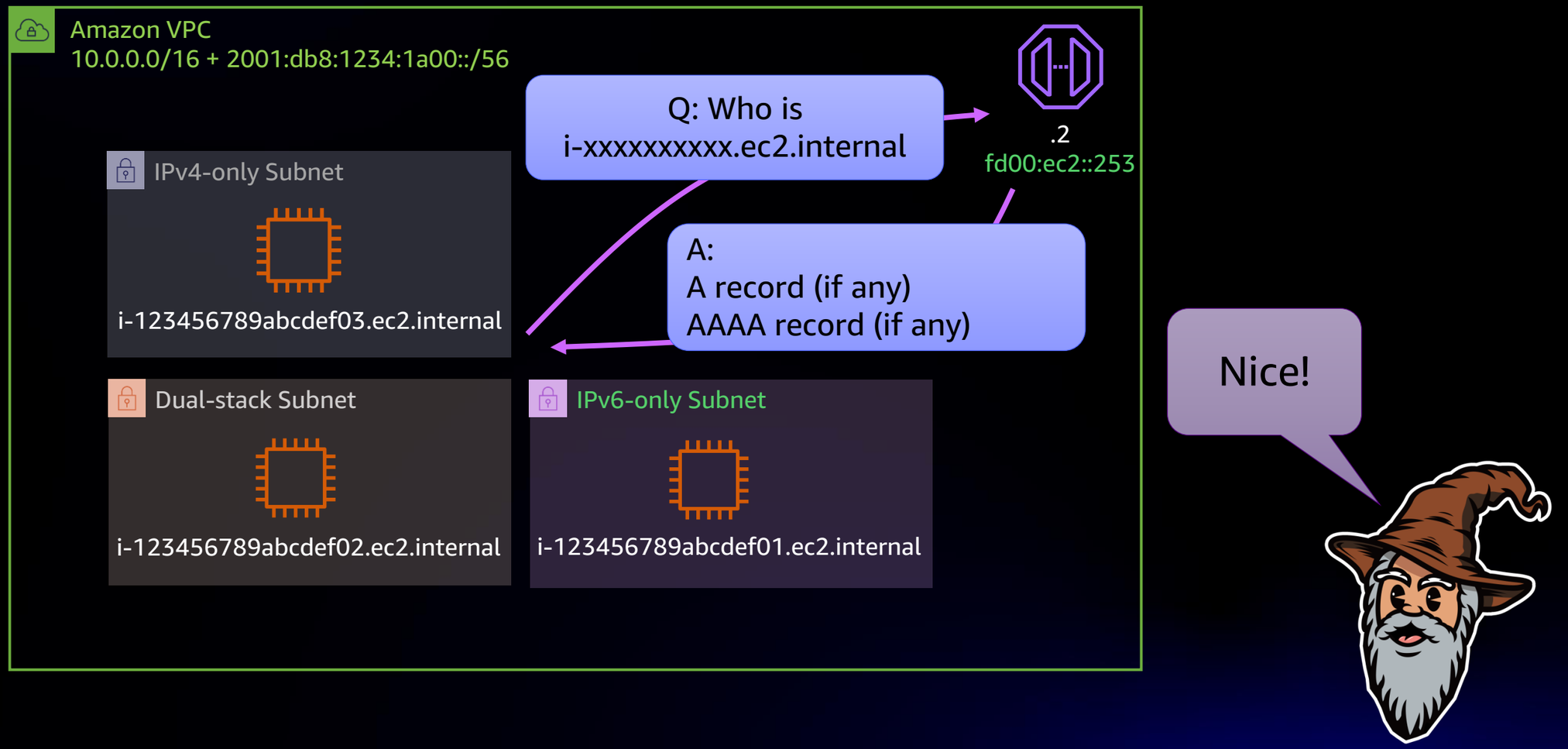
Amazon EC2: Resource-based naming

SETTINGS FOR EACH SUBNET TYPE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EC2: Resource-based naming



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IPv6

Amazon VPC
IPv6-only subnets

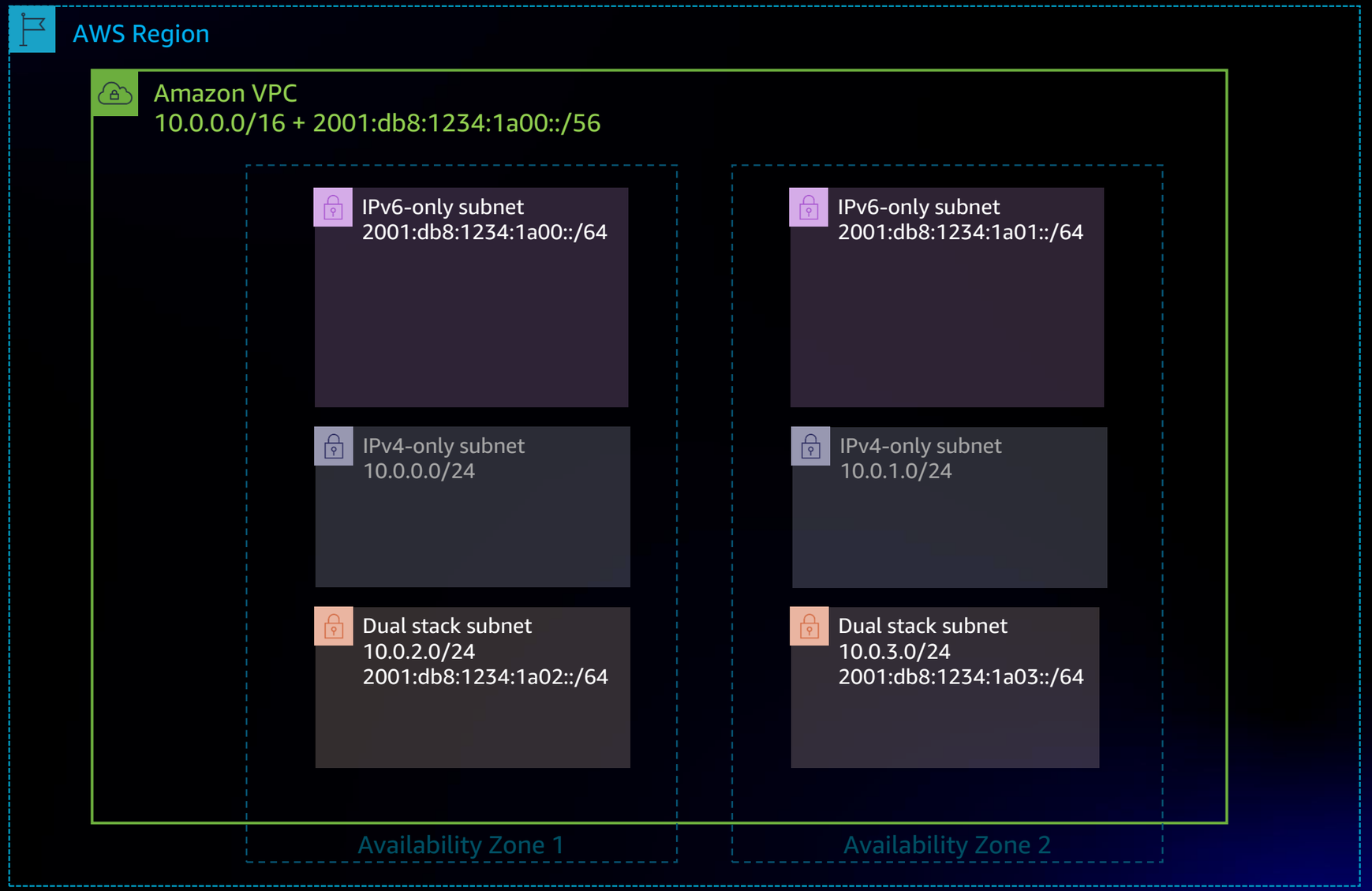
NAT64 and DNS64
Interoperability with IPv4 environments

Amazon EC2
Resource-based instance naming

Elastic Load Balancing
Full Dual-stack IPv6 support

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Starting from the dual-stack VPC

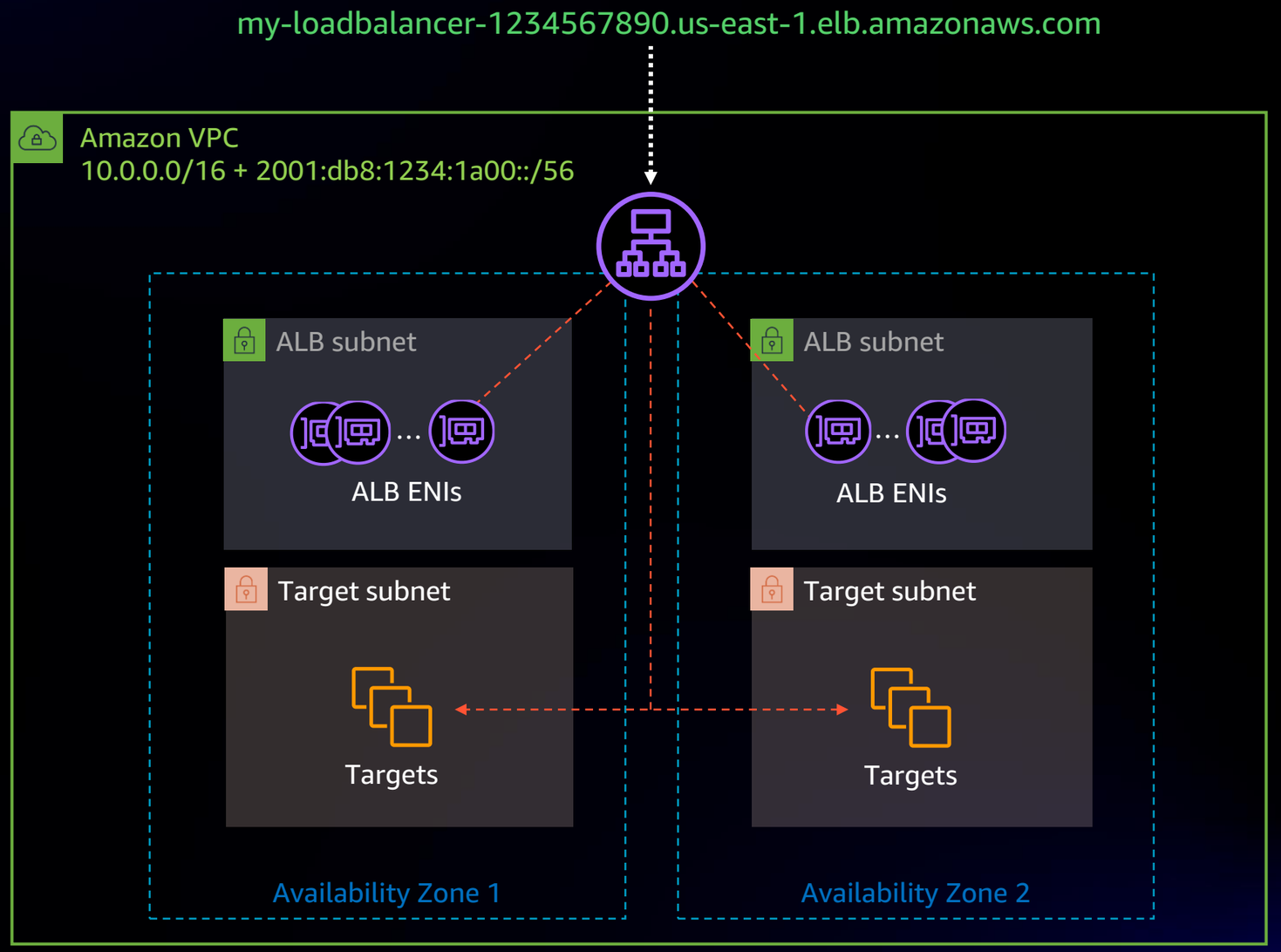


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application Load Balancer (ALB)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

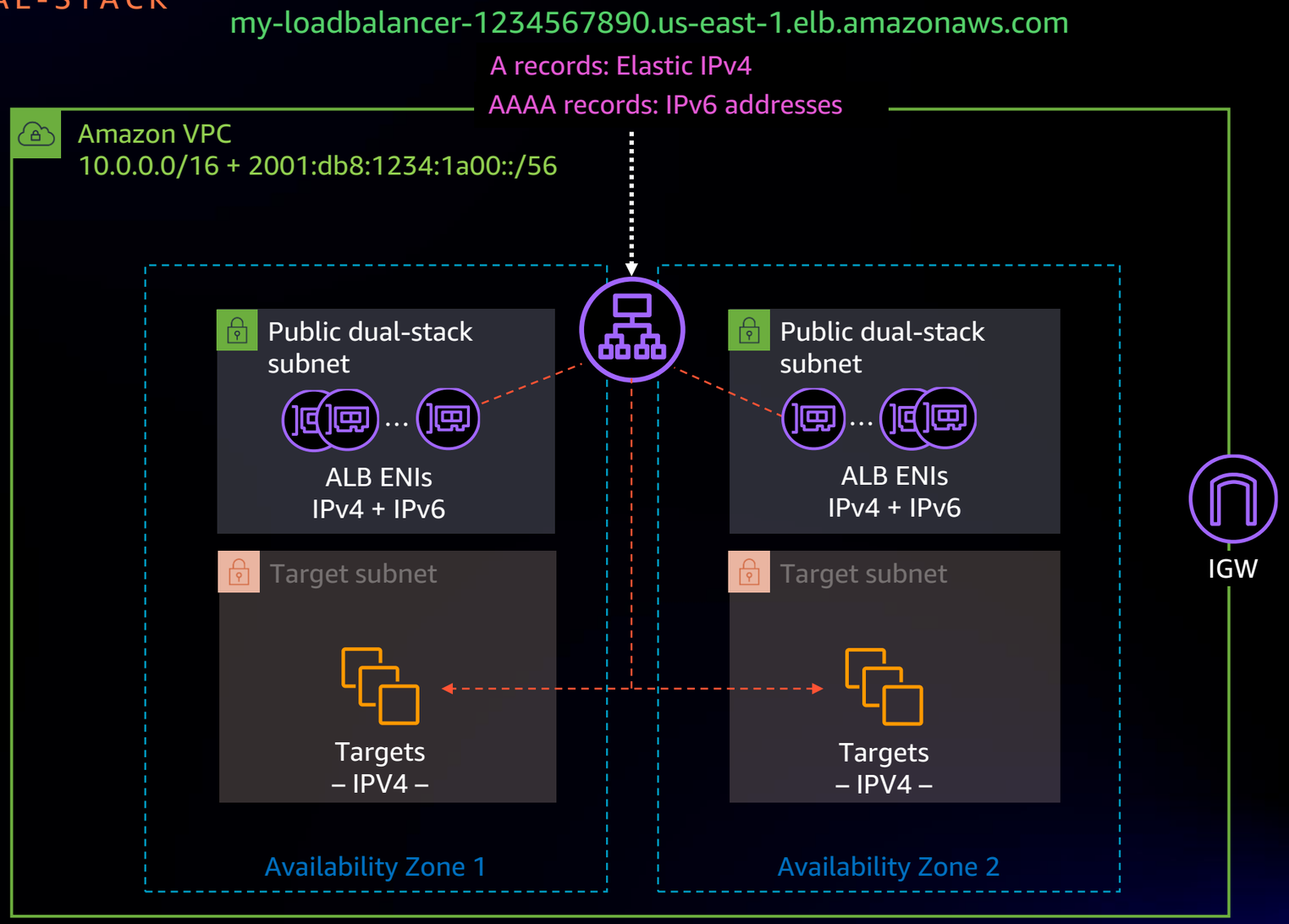
Application Load Balancer: Deployment



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application Load Balancer: Dual-stack support

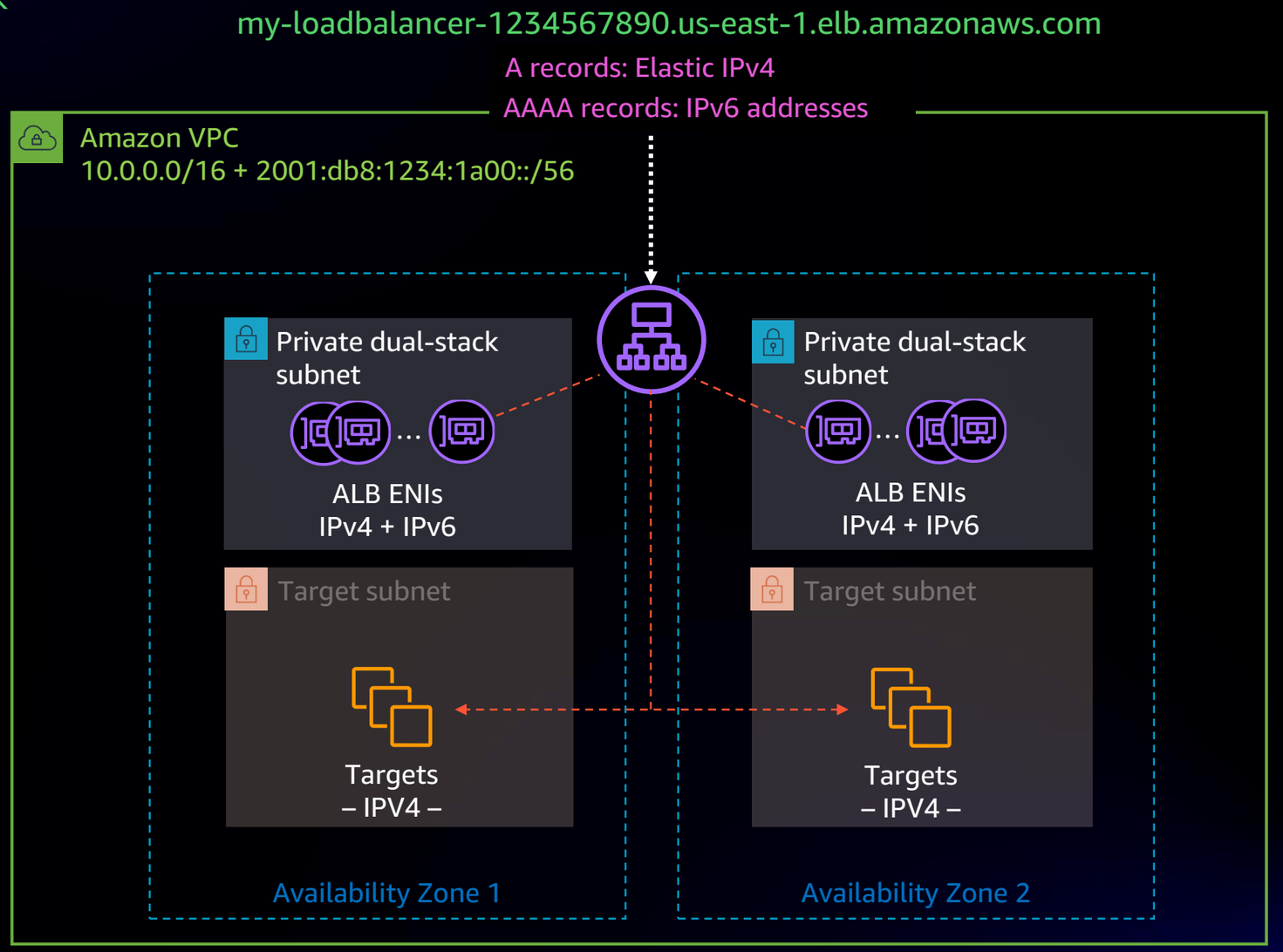
INTERNET-FACING DUAL-STACK



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application Load Balancer: Dual-stack support

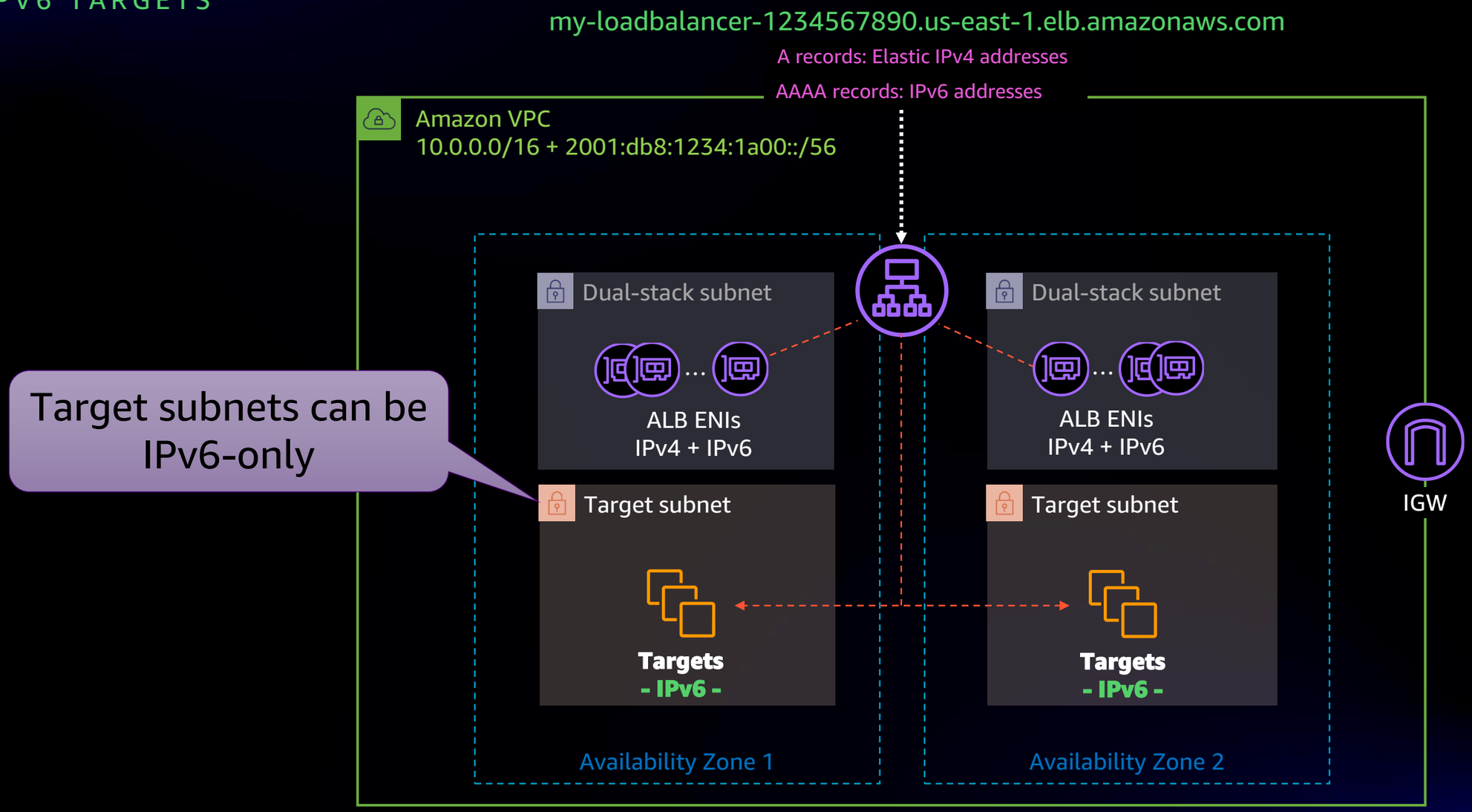
INTERNAL DUAL STACK



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application Load Balancer: End-to-end IPv6

IPV6 TARGETS

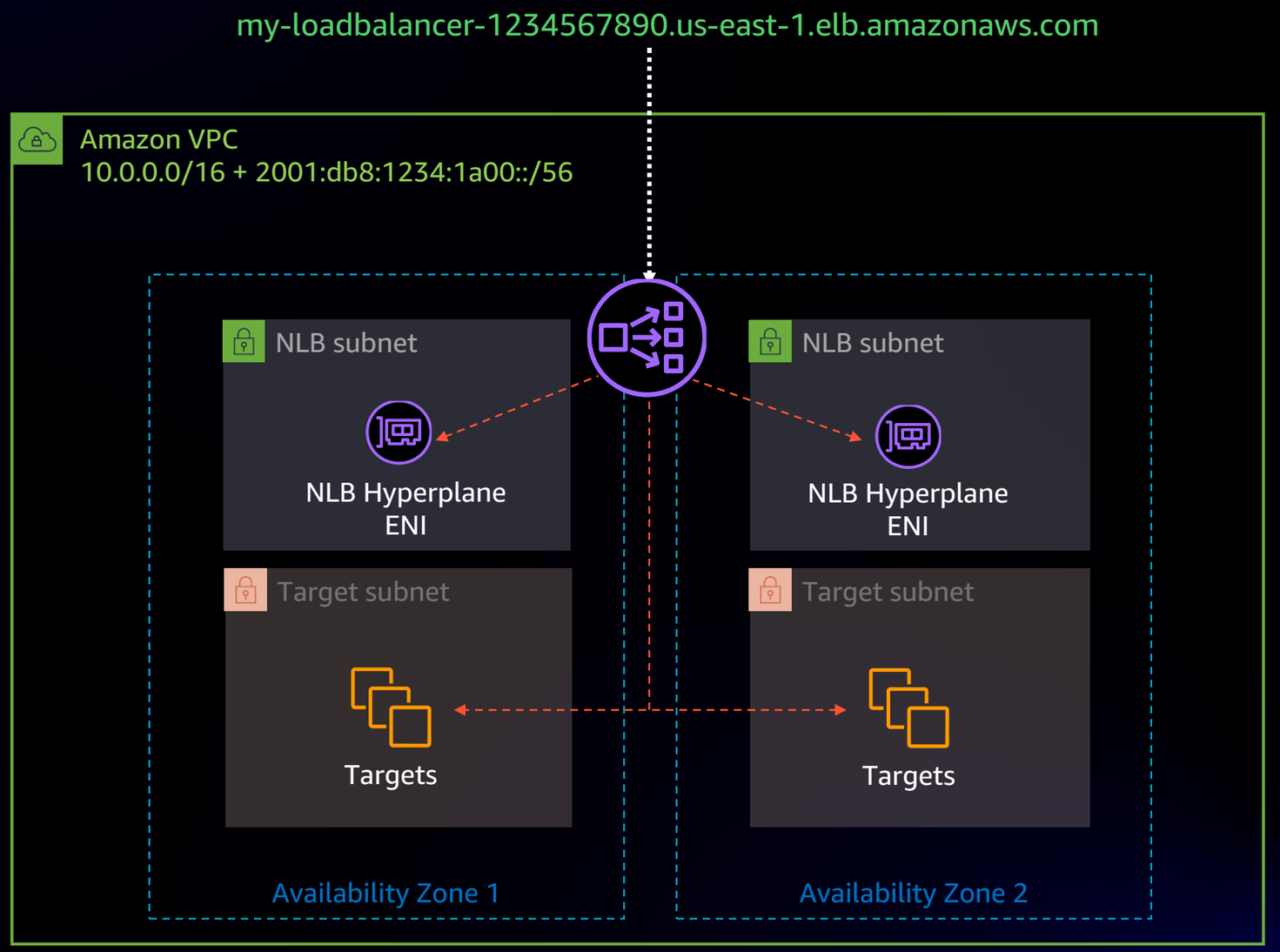


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Load Balancer (NLB)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

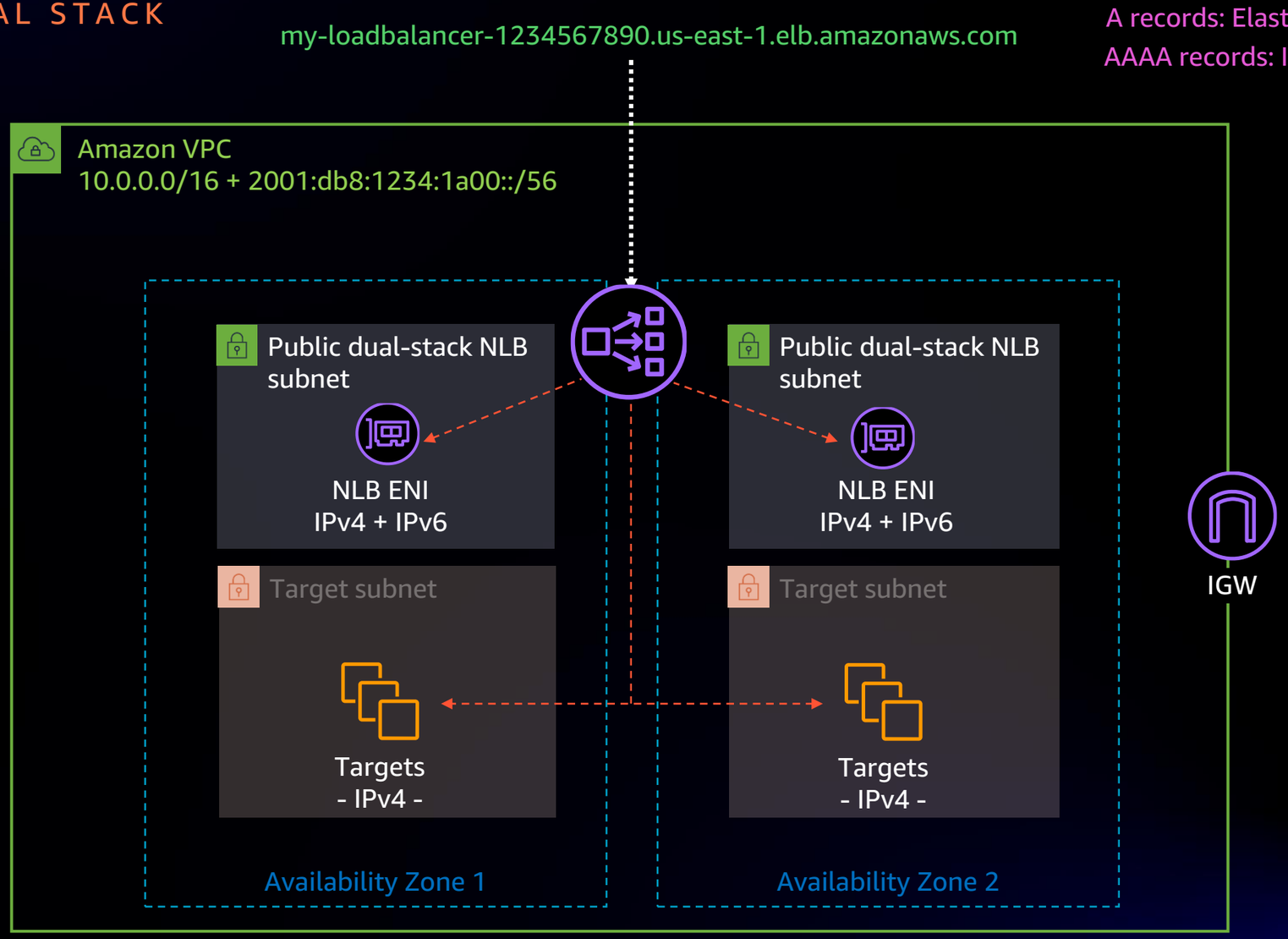
Network Load Balancer: Deployment



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Load Balancer: Dual-stack support

INTERNET-FACING DUAL STACK

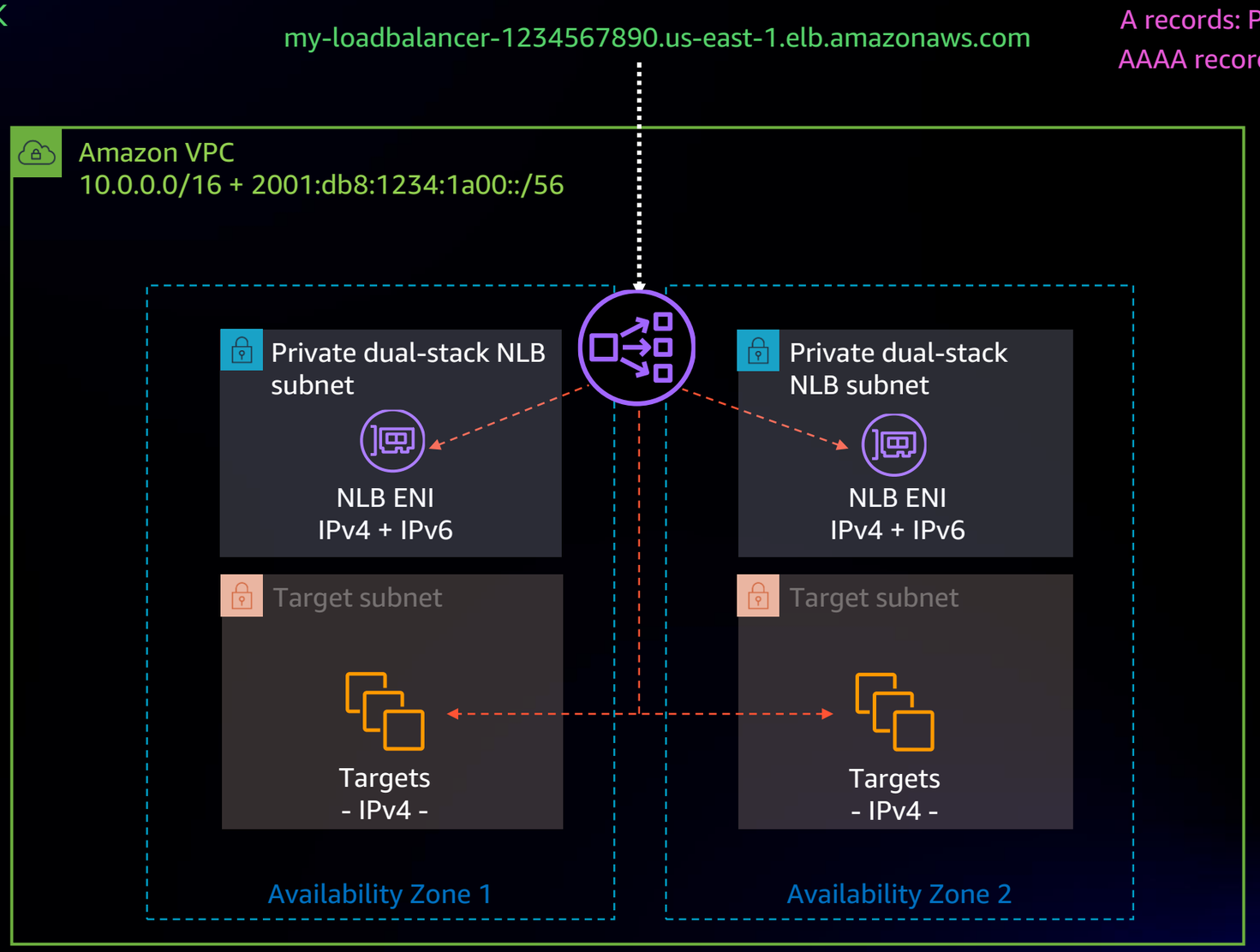


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Load Balancer: Dual-stack support

INTERNAL DUAL STACK

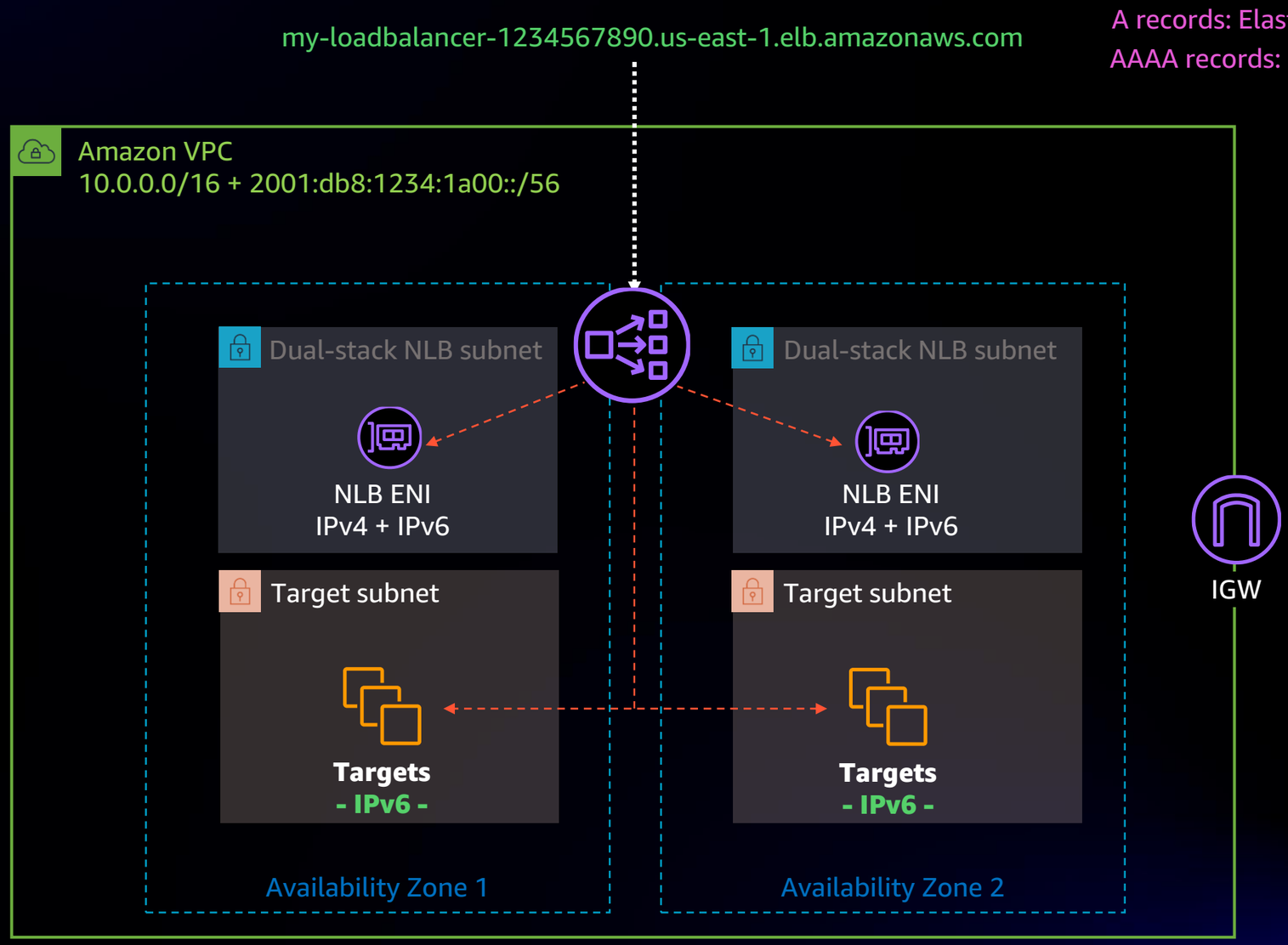
A records: Private IPv4 addresses
AAAA records: IPv6 addresses



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Load Balancer: End-to-end IPv6

IPV6 TARGETS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IPv6

- Putting it all together -

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

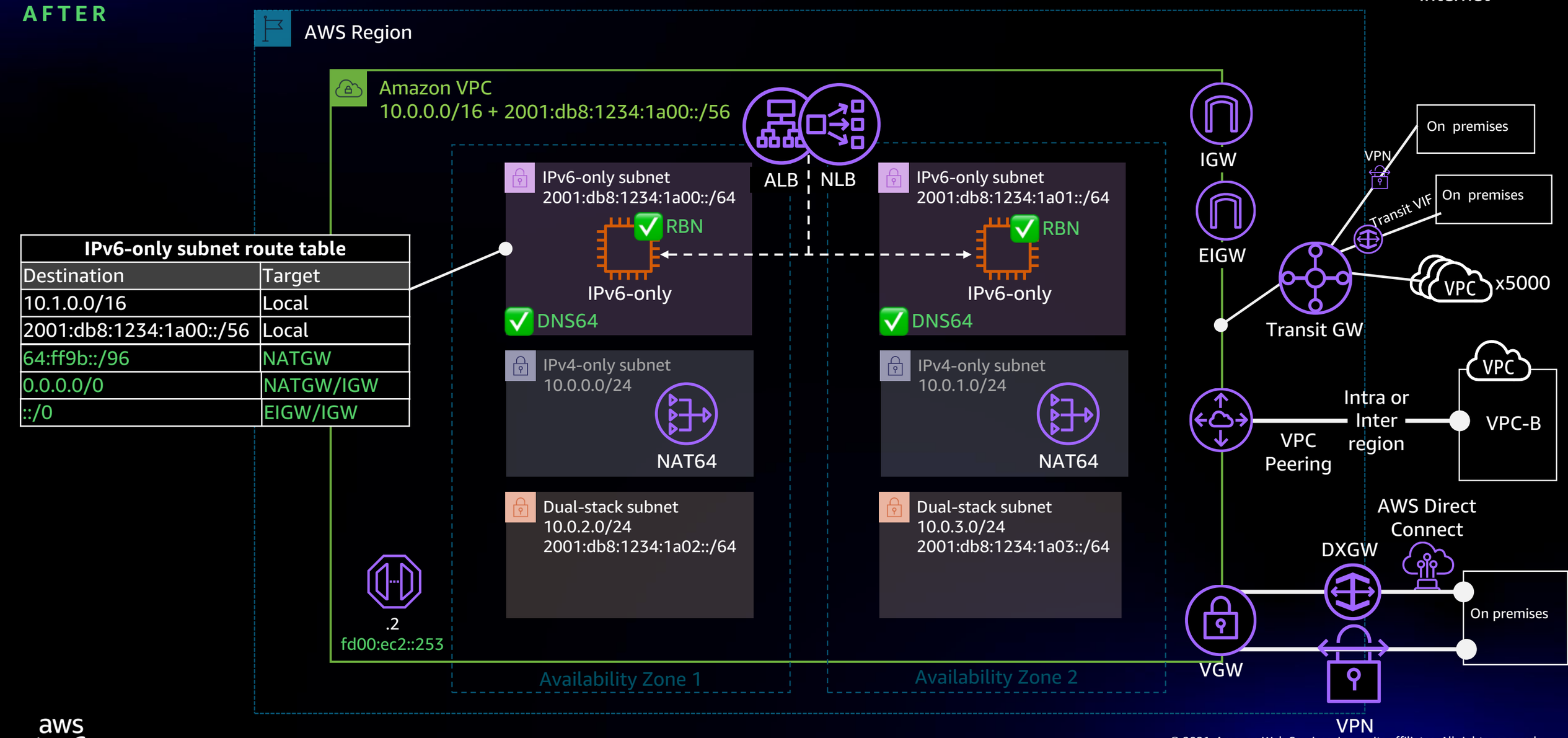
Amazon VPC: Native dual stack



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Dual-stack Amazon VPC: IPv6 native

AFTER



IPv6-only subnet route table	
Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1a00::/56	Local
64:ff9b::/96	NATGW
0.0.0.0/0	NATGW/IGW
::/0	EIGW/IGW

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

All things IPv6



https://bit.ly/2ZMf6lC

IPv6 on AWS whitepaper

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Management

IPAM

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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		

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What’s wrong with this picture?



Manual updates of single spreadsheet



Limited visibility into allocation and usage

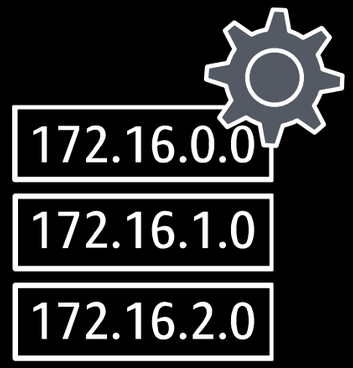


Limited ability to manage IP allocations at scale

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



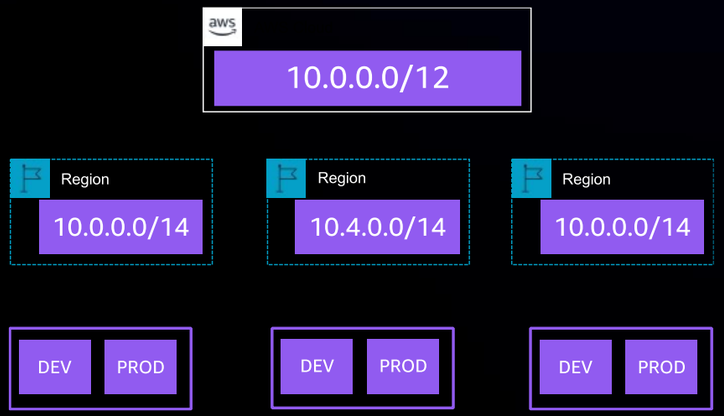
Retrospective analysis

Allowing decreased time to troubleshoot and audit

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key IPAM components

Refill policy

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

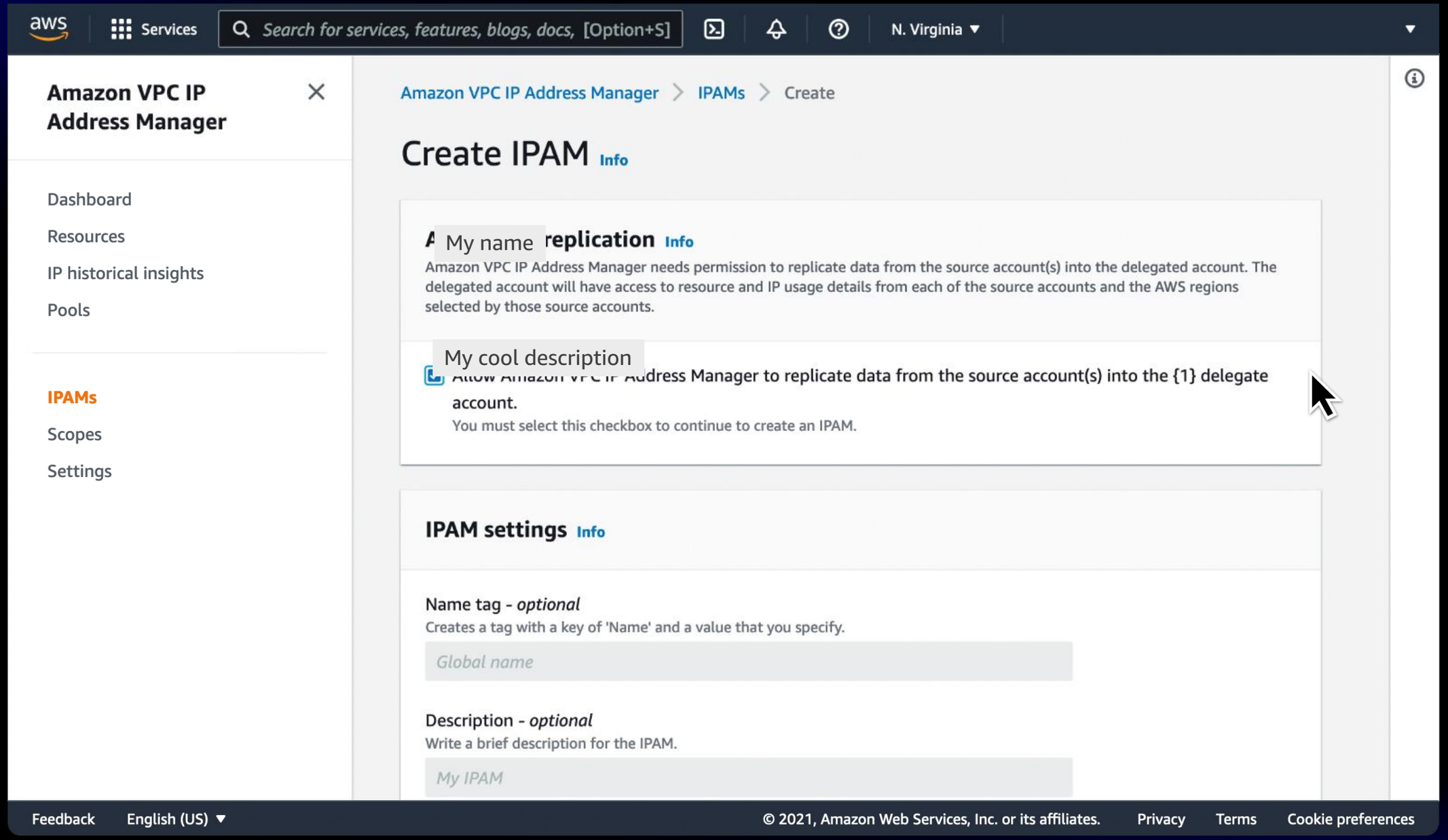
Refill policy helps you to ensure a pool always has IP addresses available for allocation

Allocation policy

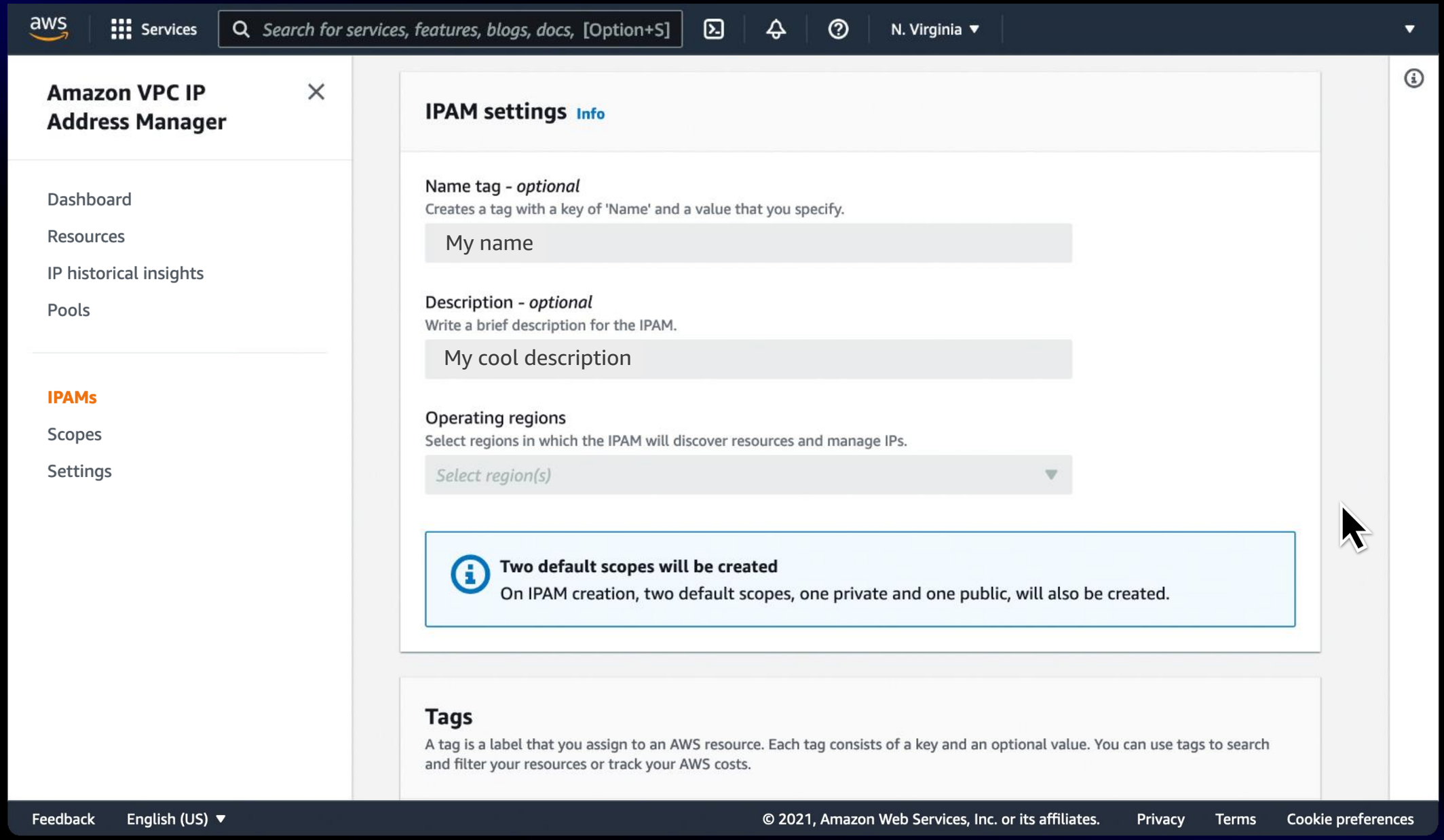
An allocation policy allows you to control IP addresses allocated by IPAM from a pool

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

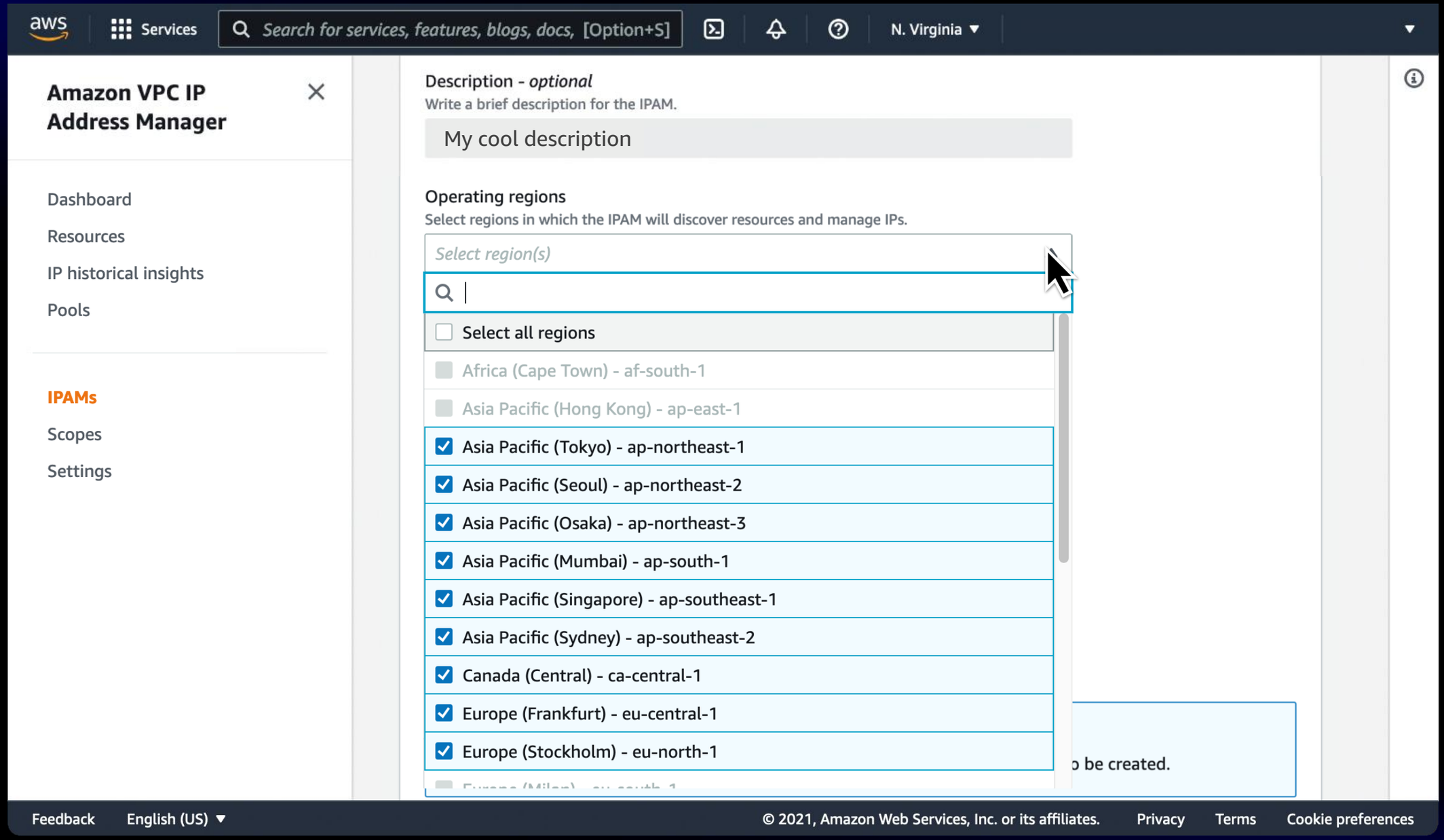
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



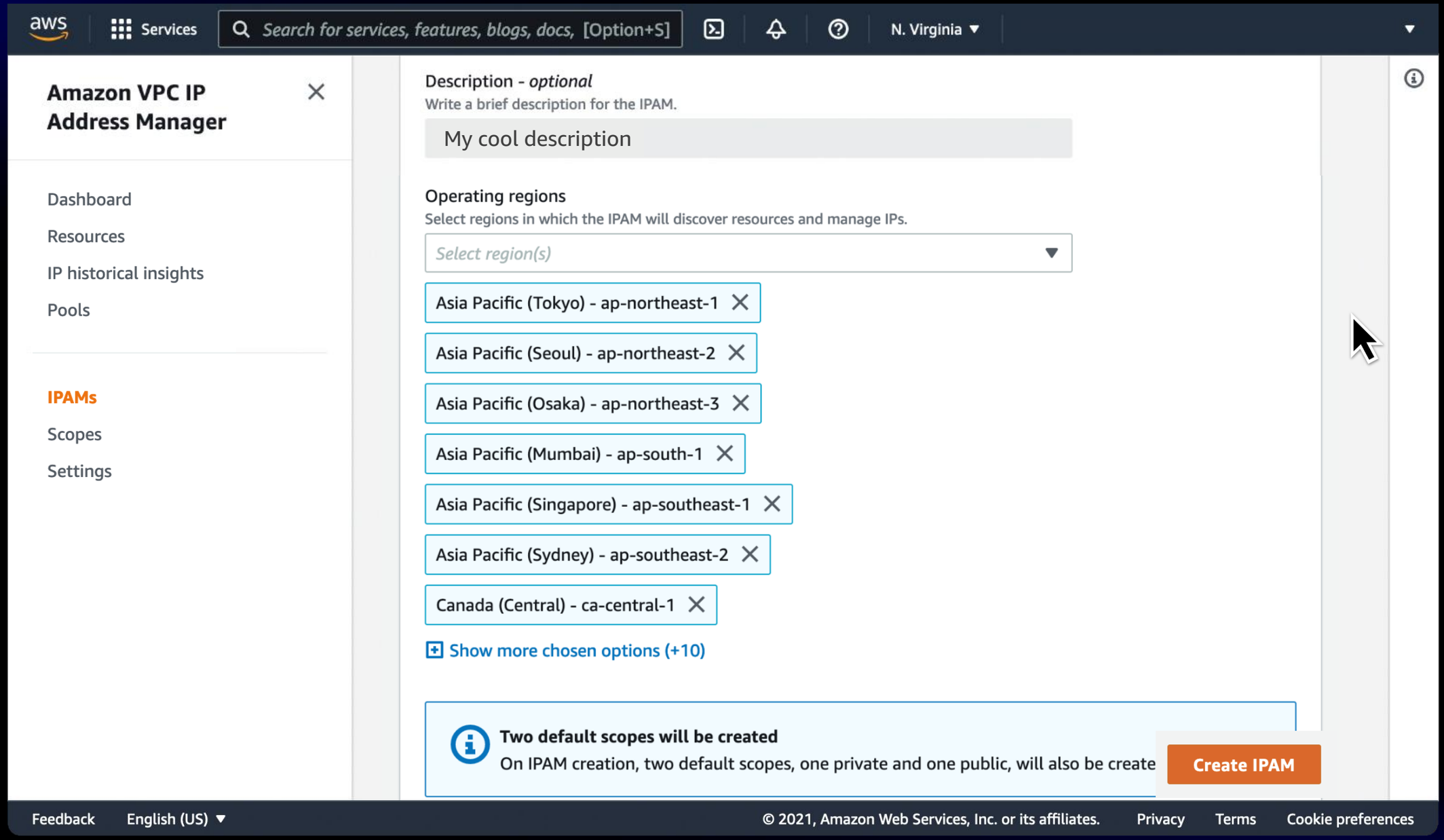
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



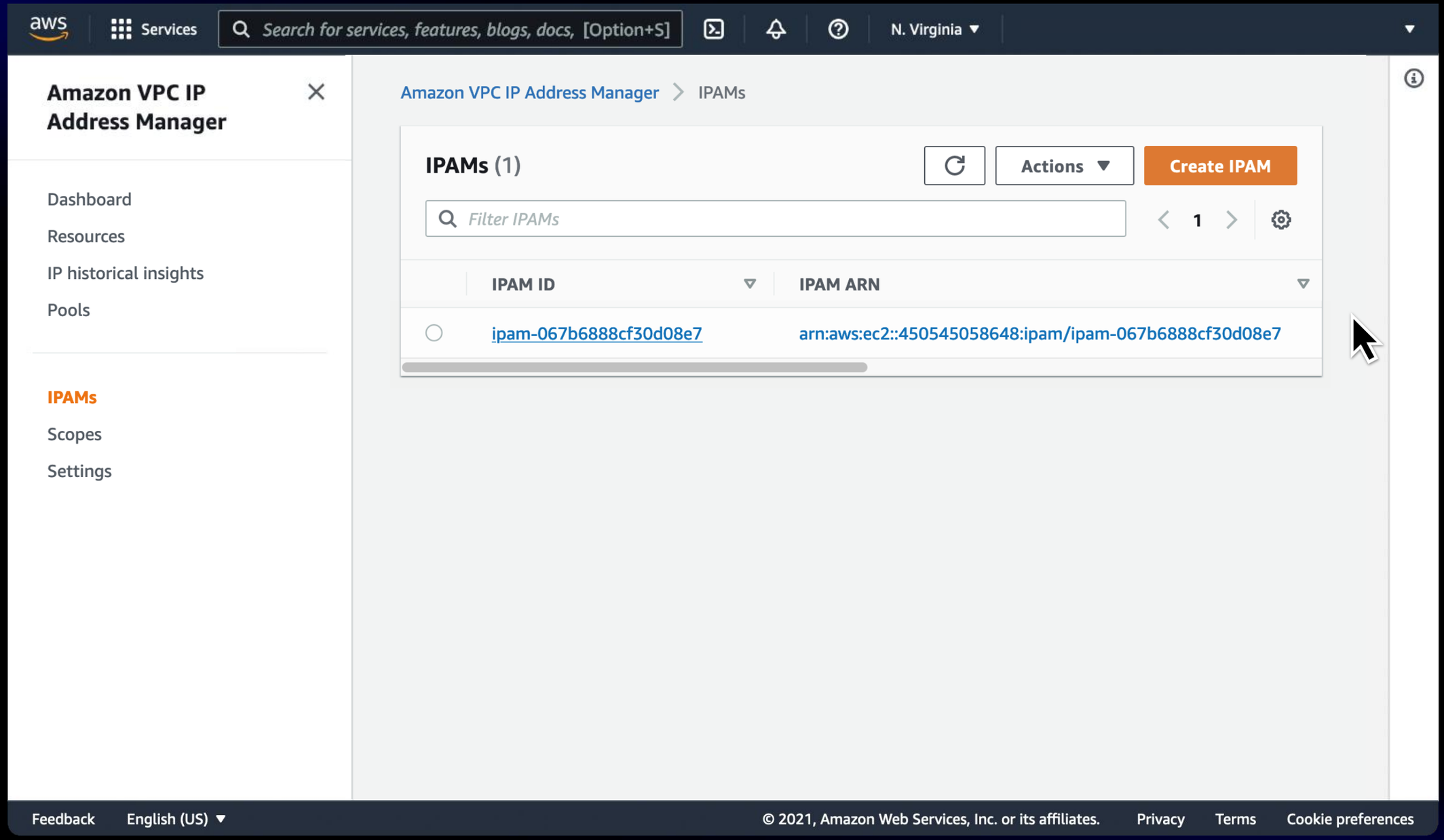
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



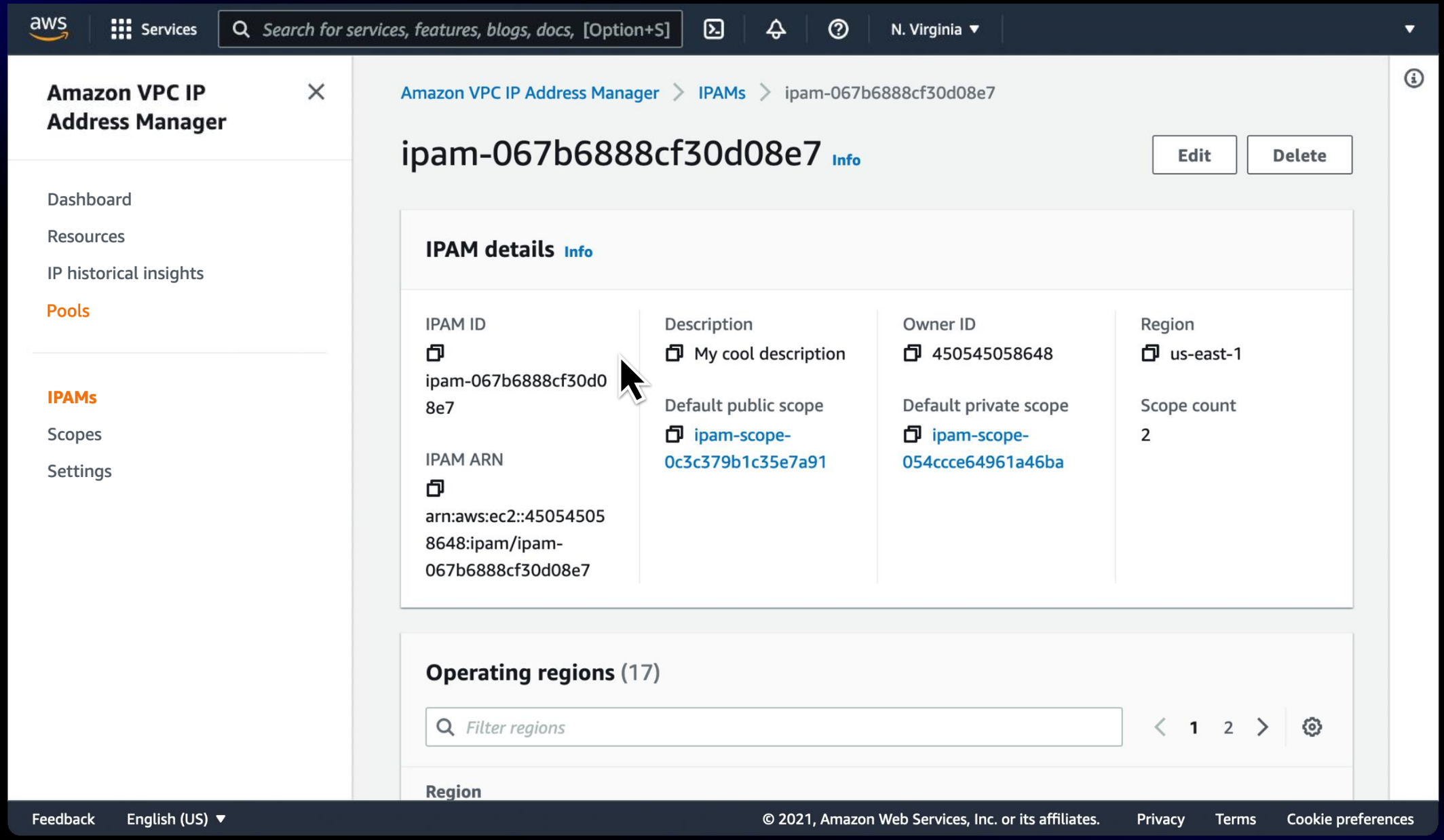
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



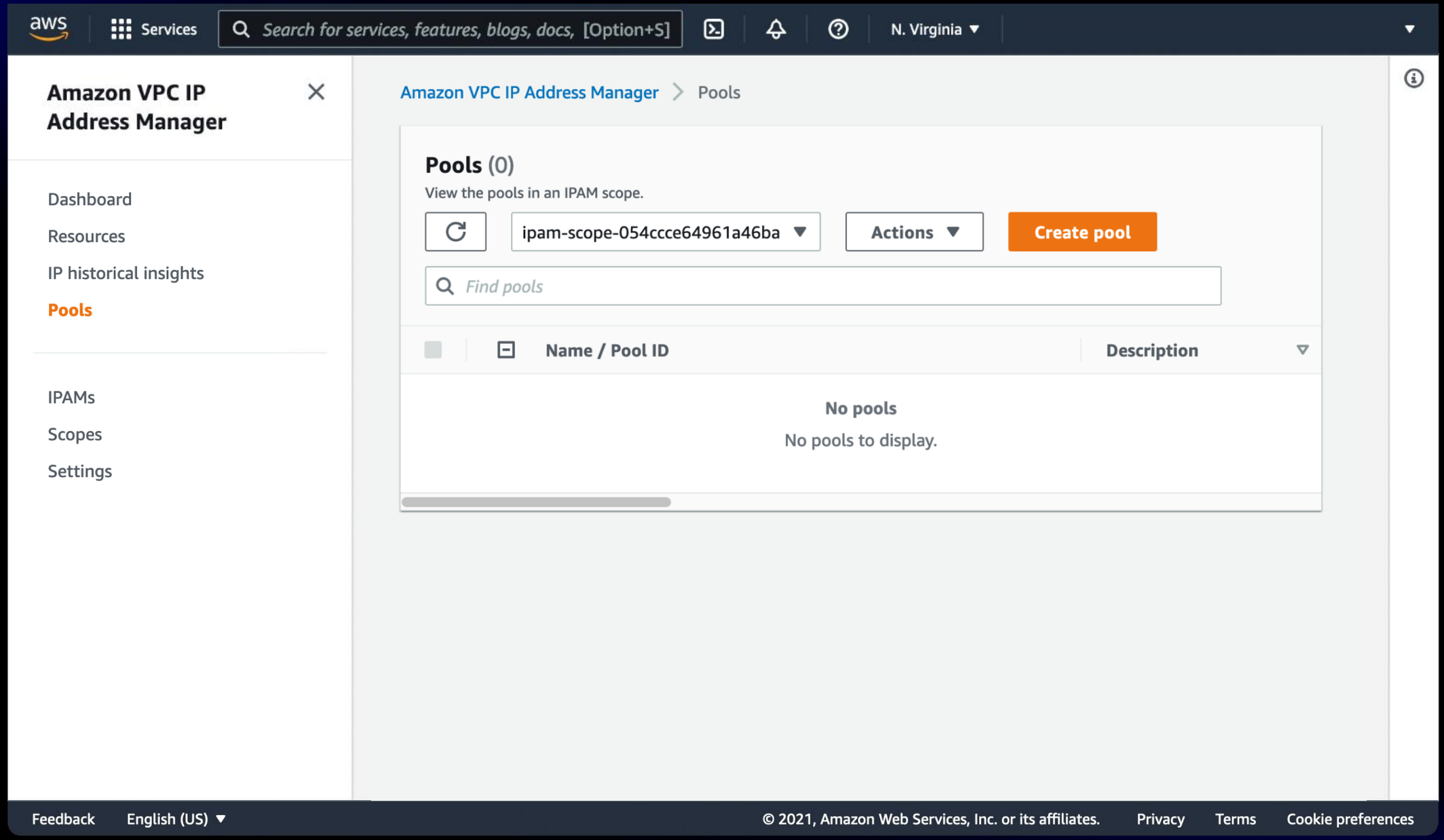
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



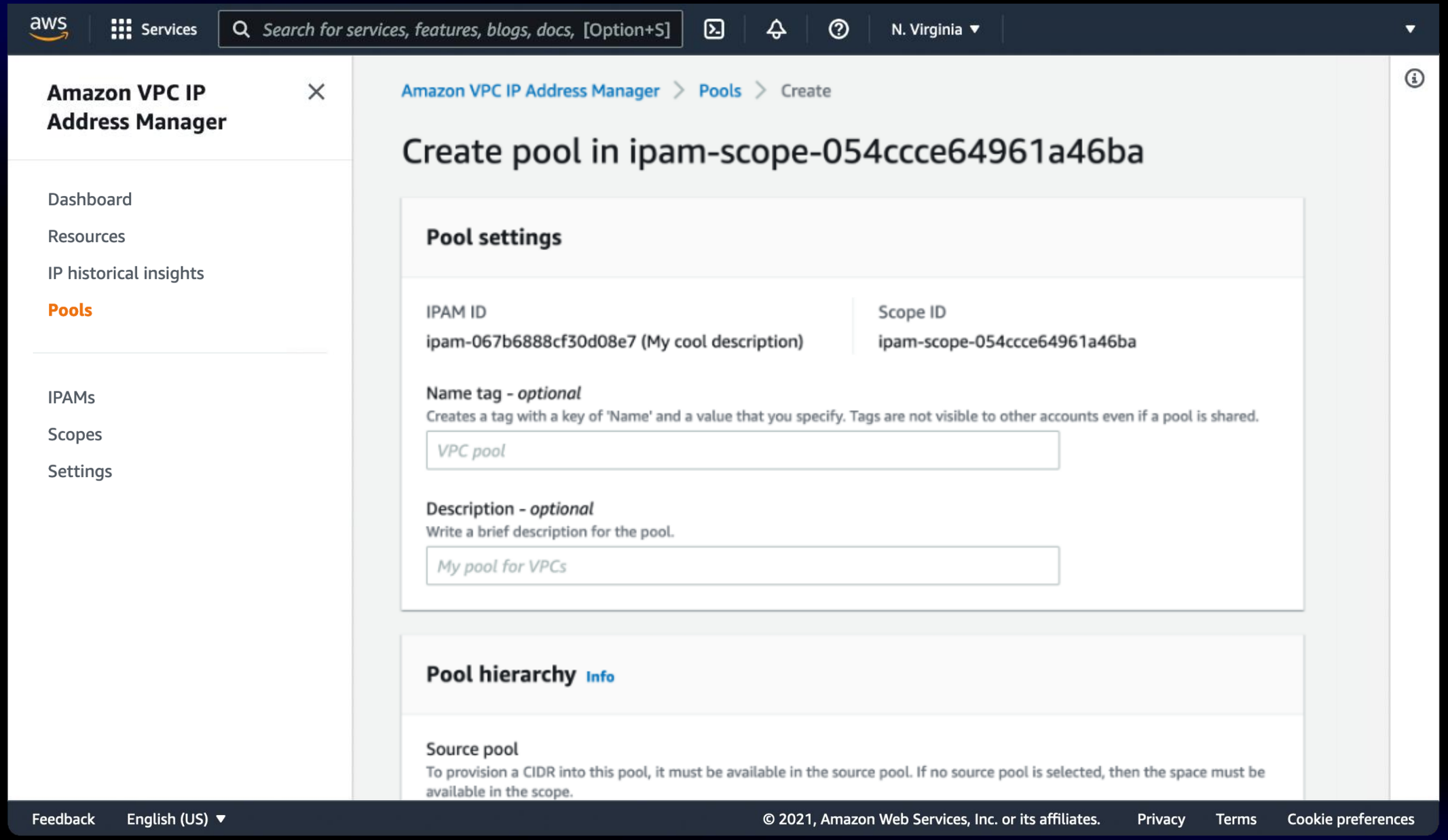
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



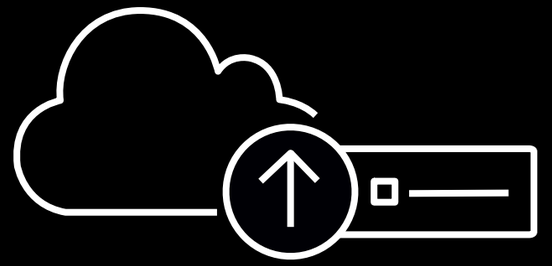
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Private scope

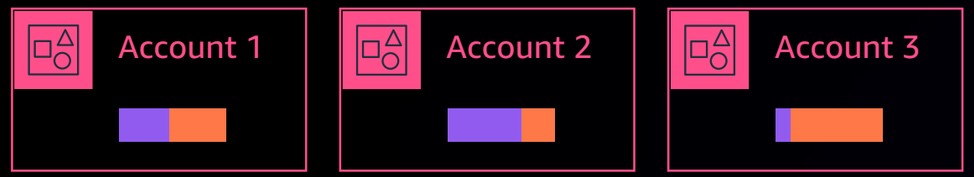


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bring your own IP (BYOIP) with IPAM



BYOIP *without* IPAM



Used IPs

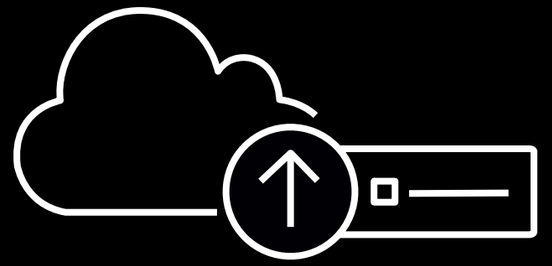
Unused IPs

Benefits:

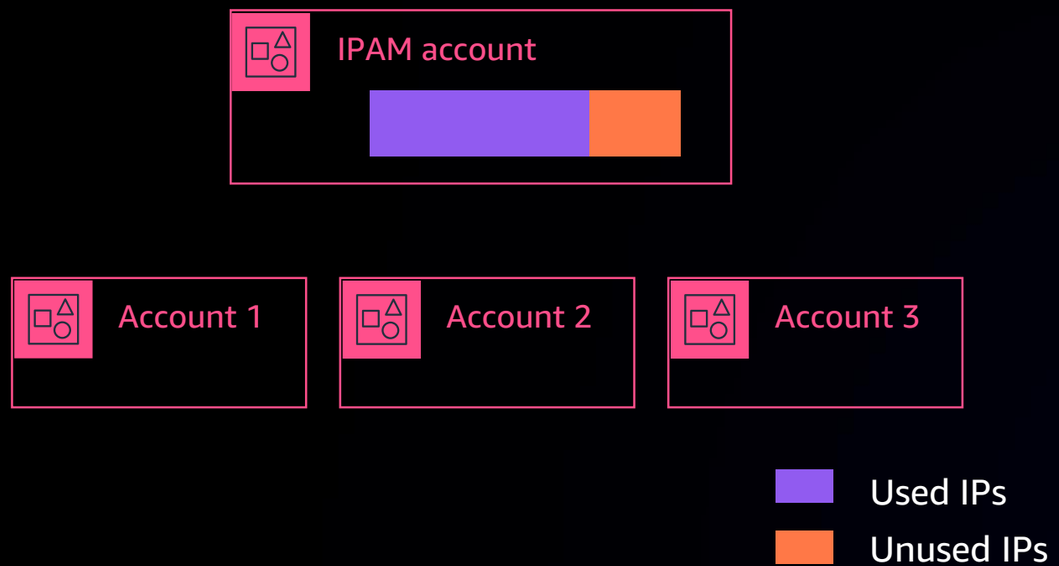
- Improve IP address utilization (Org wide sharing)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bring your own IP (BYOIP) with IPAM



BYOIP *with* IPAM



Benefits:

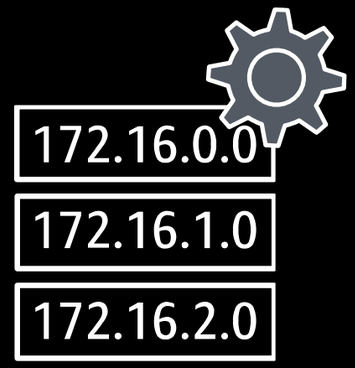
- Improve IP address utilization (Org wide sharing)
- Migrate existing BYOIP IPs
- Simplify BYOIP onboarding to AWS
- Enable both Internet- and VPC- BYOIPv6

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager

IPAM

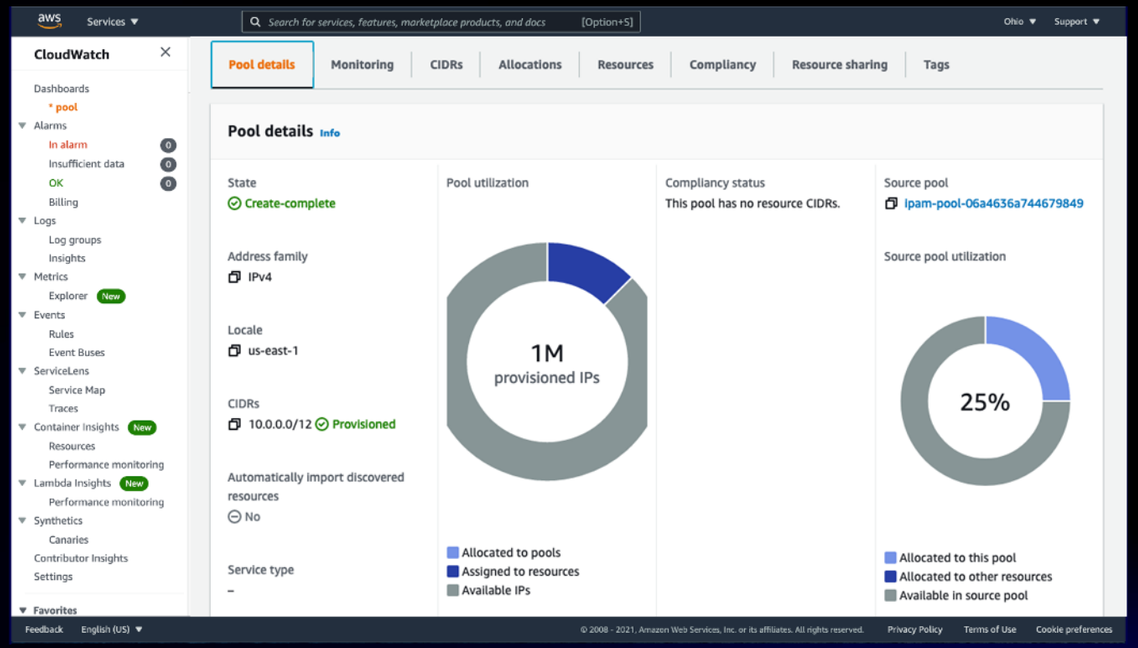
Monitoring and alerts





Monitor across network

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

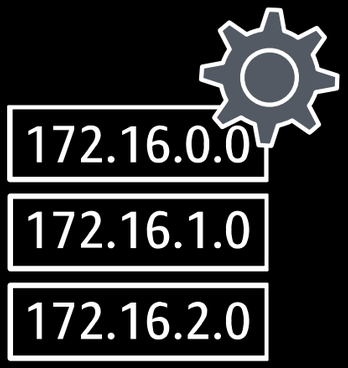


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager

IPAM

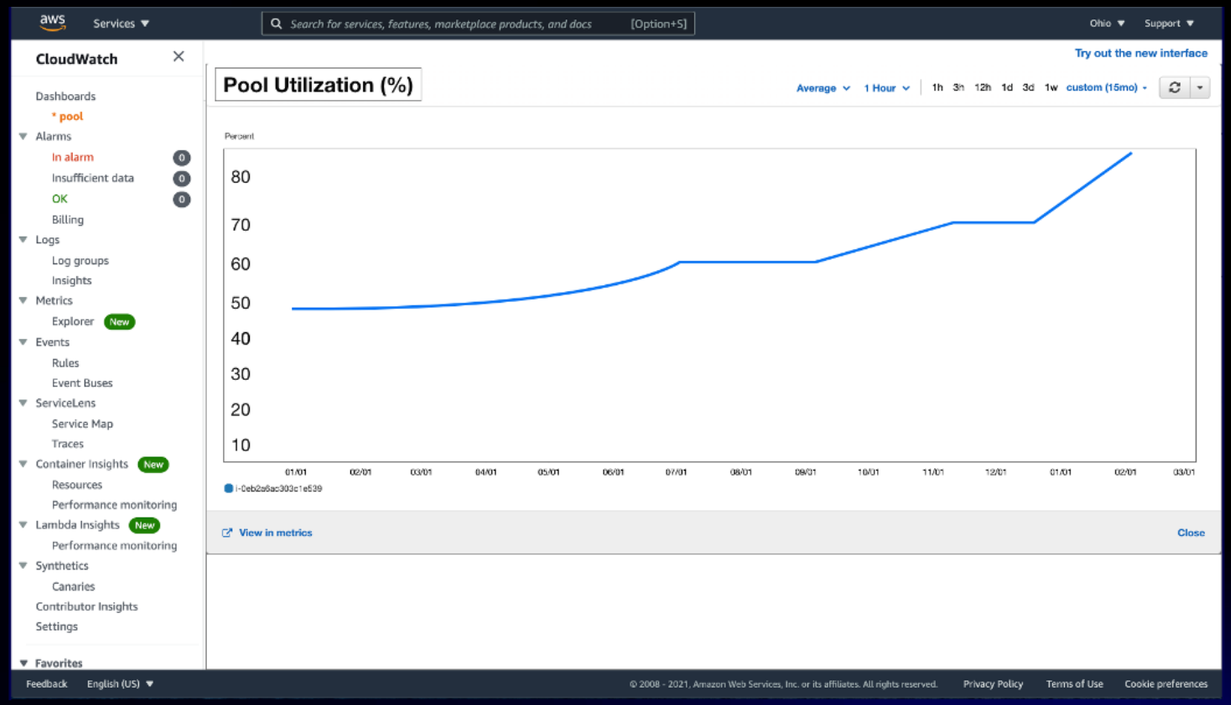
Monitoring and alerts





Monitor across network

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

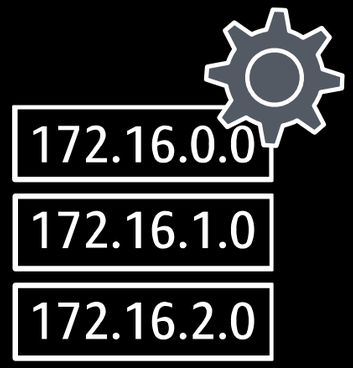


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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	

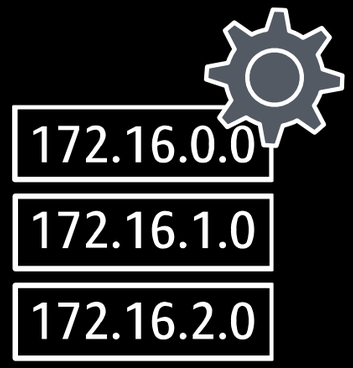
Tag on allocation policy don't match

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager

IPAM

Historical insights



Lifecycle of a private IP

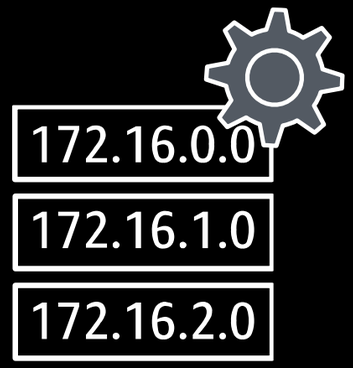
- Provides IP, start time, and end time
- Get lifecycle events associated with EIPs
- Helps troubleshoot and audit



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing
Amazon VPC IP Address Manager

IPAM



SCAN ME

https://go.aws/3xLkthD

Amazon VPC IP Address Manager (IPAM)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Networking

Amazon VPC
Enhanced routing

AWS NAT Gateway
Private NAT support

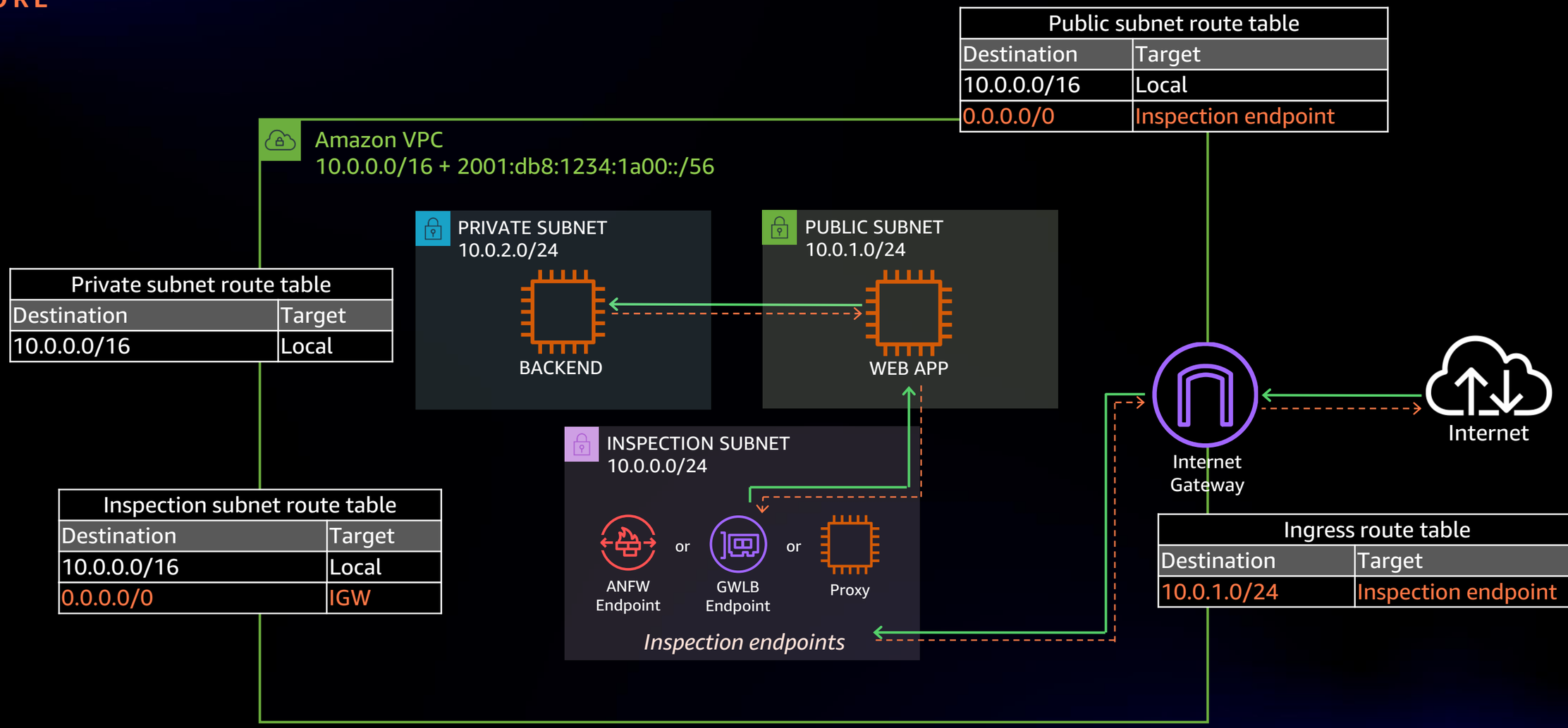
AWS PrivateLink
S3 interface endpoint and ALB integration

AWS Transit Gateway
TGW Connect and intra-region peering

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC routing

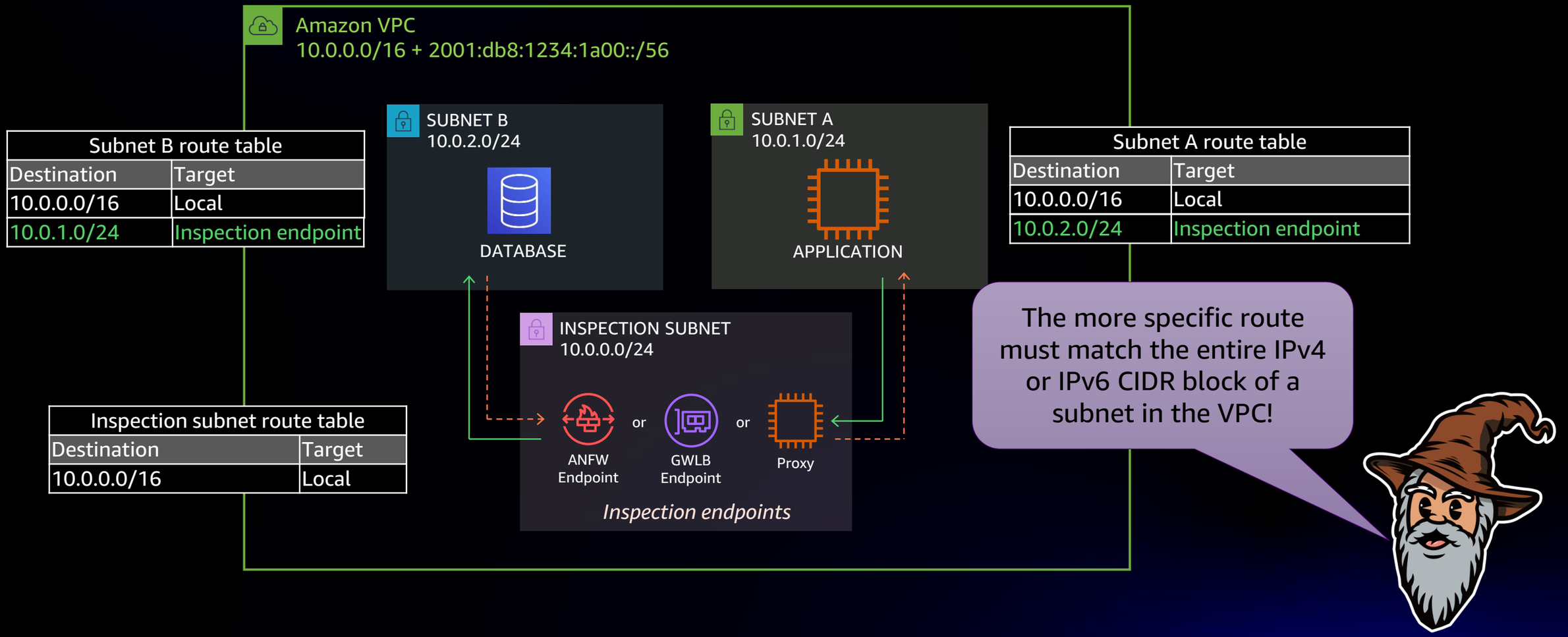
BEFORE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

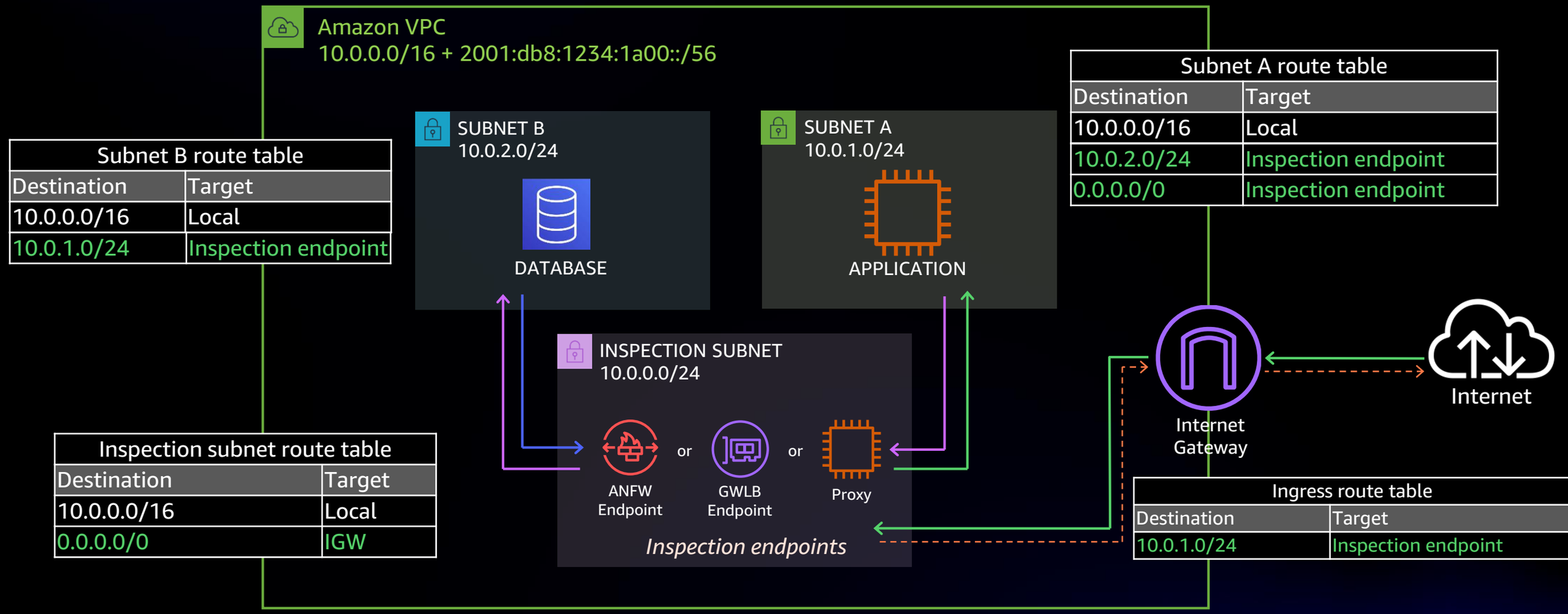
Amazon VPC routing: Enhanced routing controls

AFTER



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enhanced VPC routing: Multiple inspection levels



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
0.0.0.0/0	Inspection endpoint

Inspection subnet route table	
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	IGW

Ingress route table	
Destination	Target
10.0.1.0/24	Inspection endpoint

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Networking

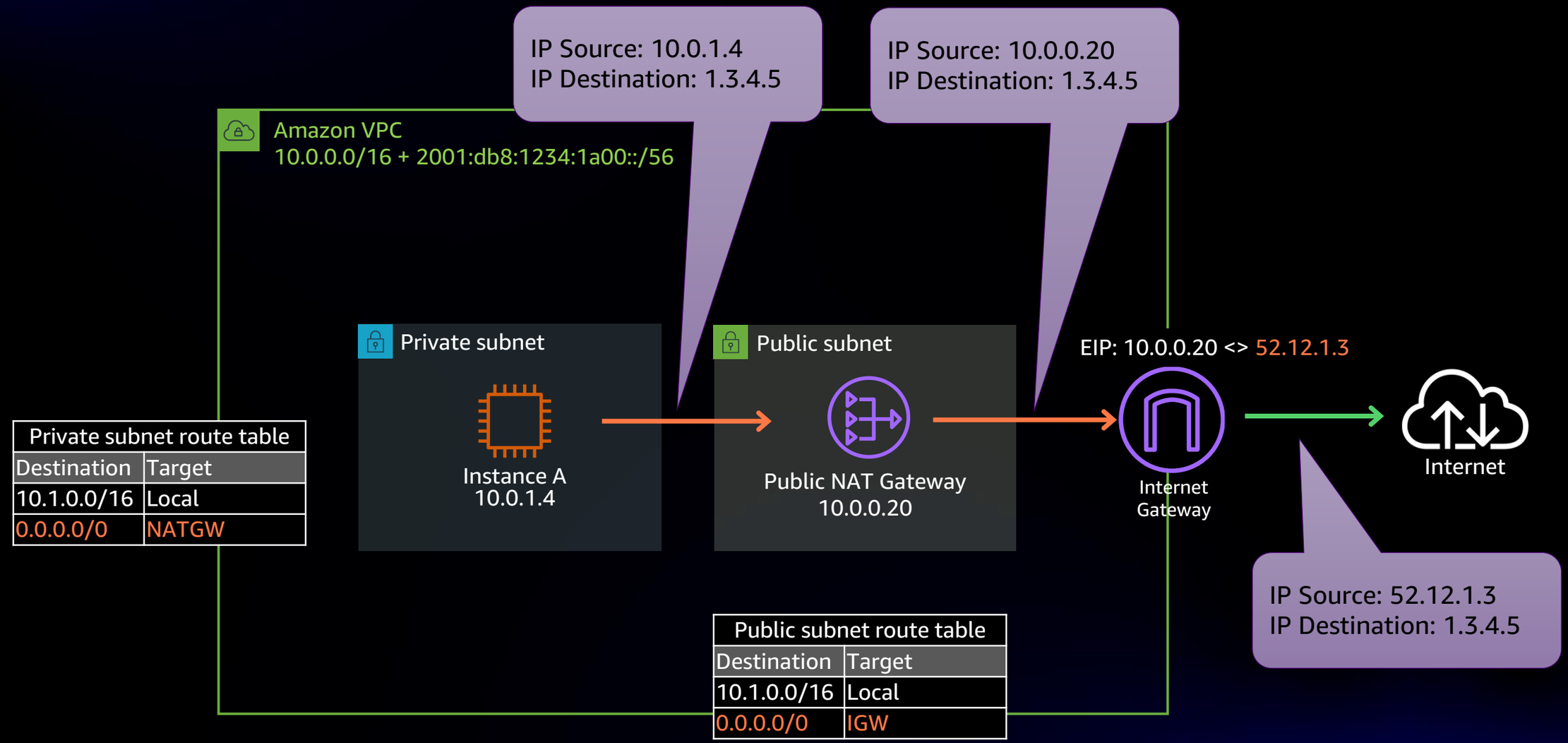
Amazon VPC
Enhanced routing

AWS NAT Gateway
Private NAT support

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NAT Gateway: Public

BEFORE



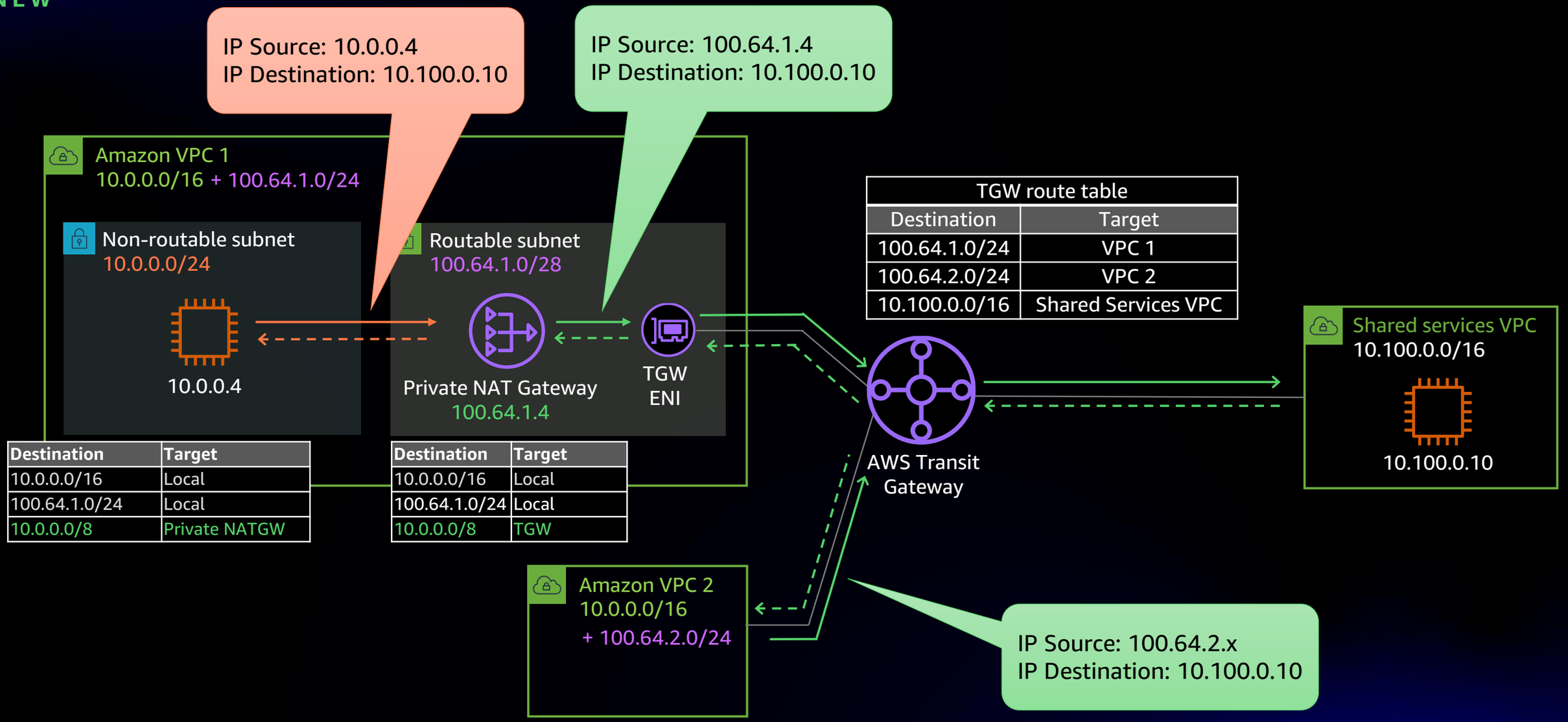
Private subnet route table	
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NATGW

Public subnet route table	
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NAT Gateway: Private NAT support

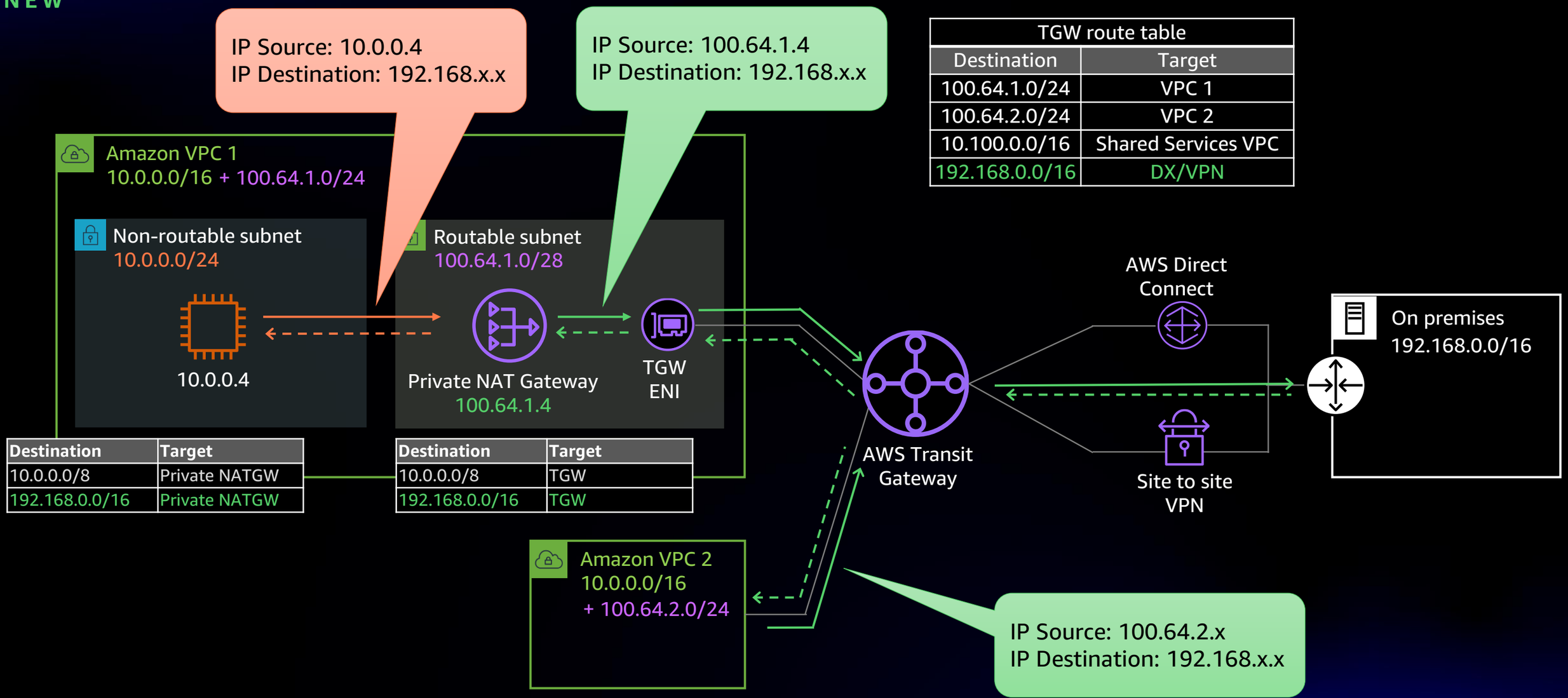
NEW



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Networking

Amazon VPC
Enhanced routing

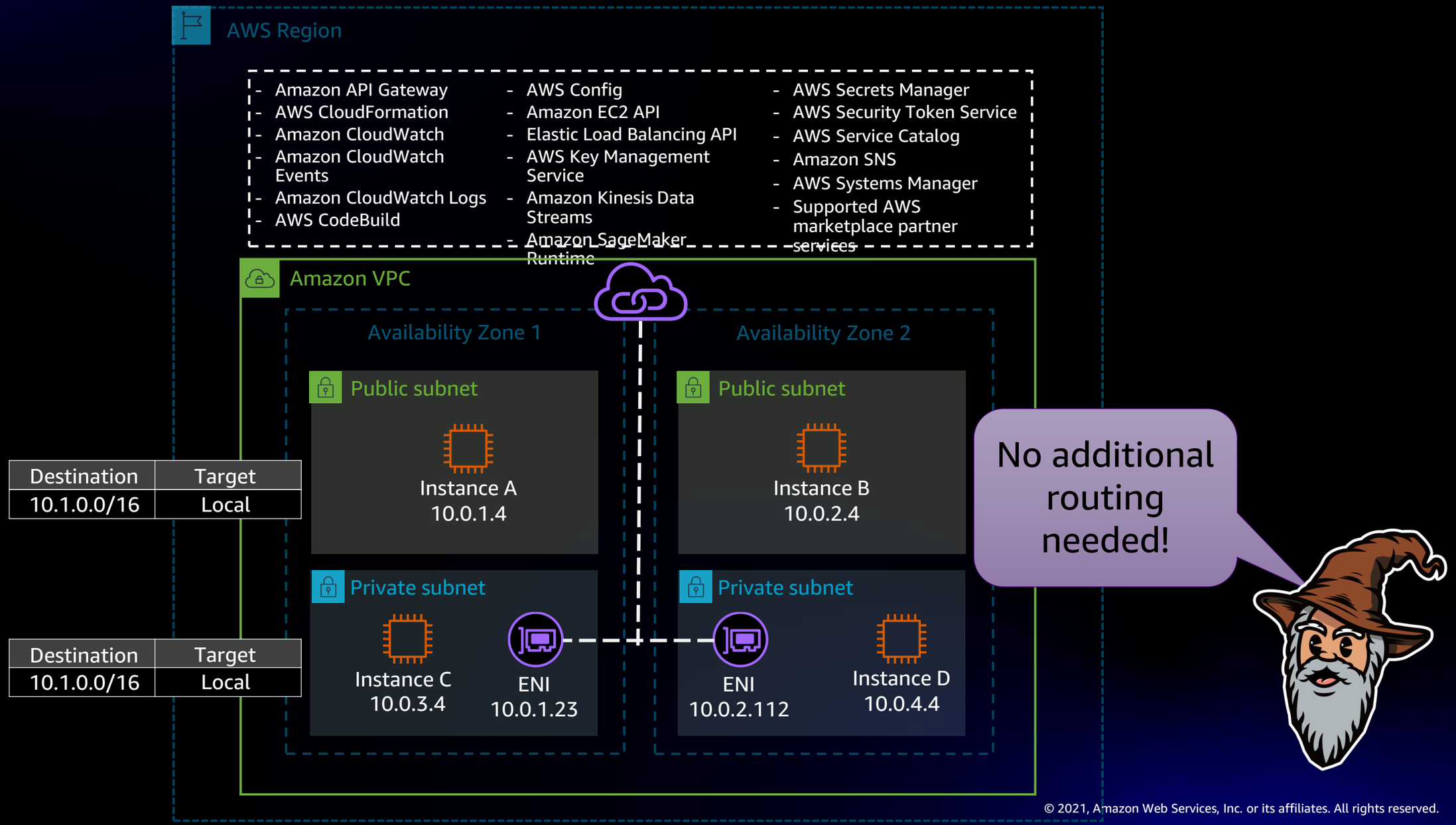
AWS NAT Gateway
Private NAT support

AWS PrivateLink
S3 interface endpoint and ALB integration

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink: Interface endpoints

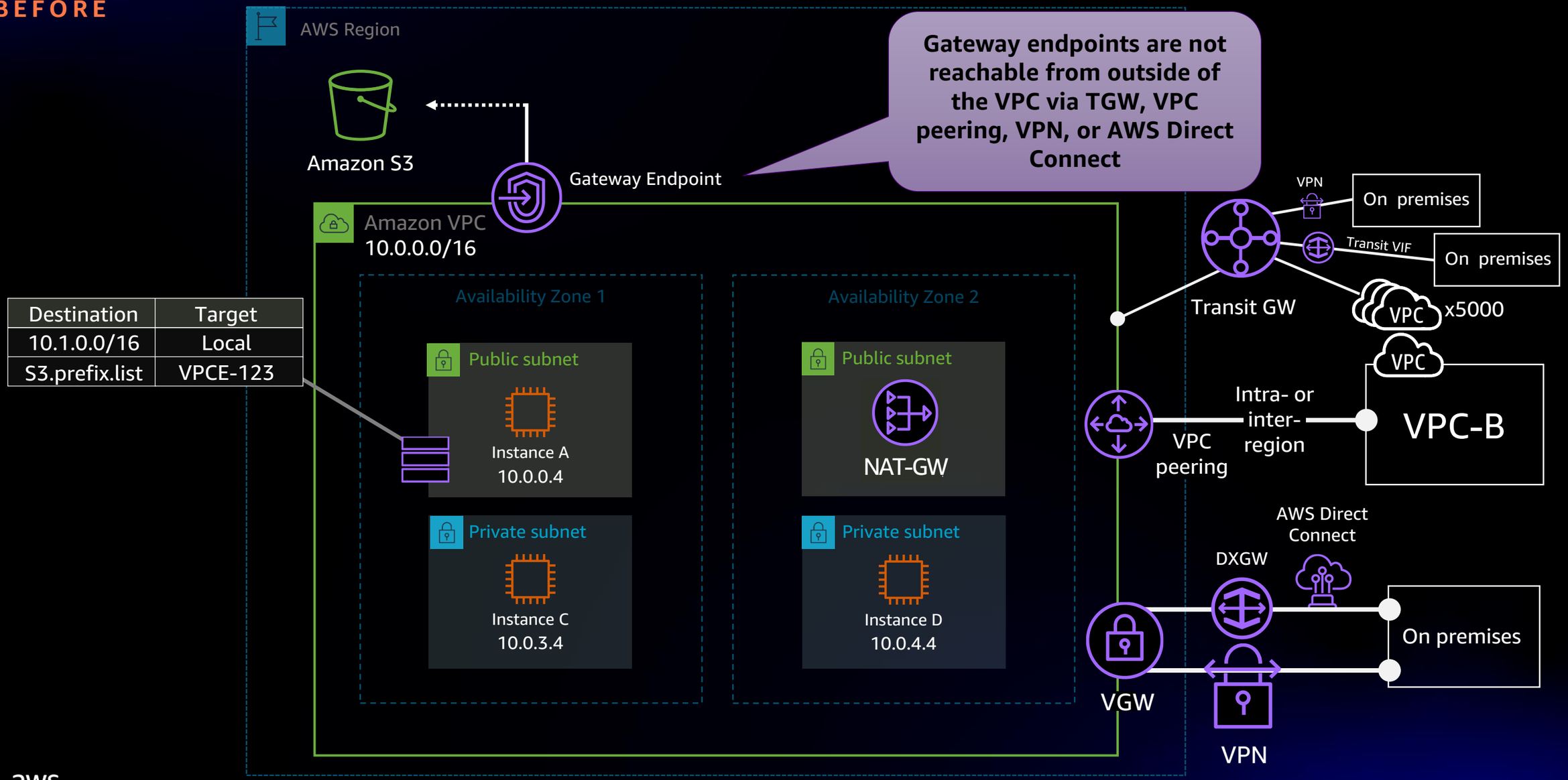
BEFORE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink: S3 Gateway endpoints

BEFORE



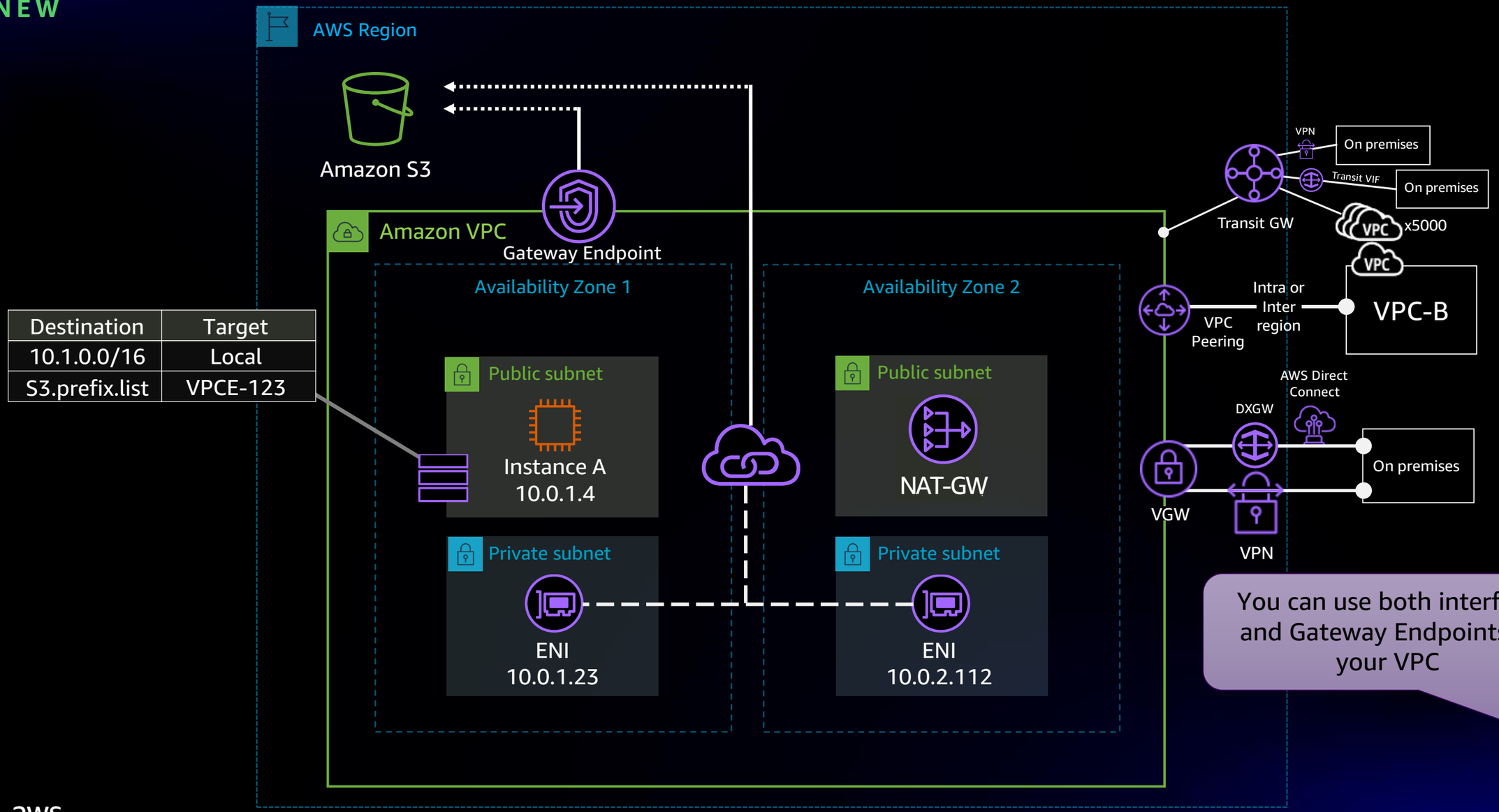
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3 interface endpoints

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink: S3 interface endpoints

NEW



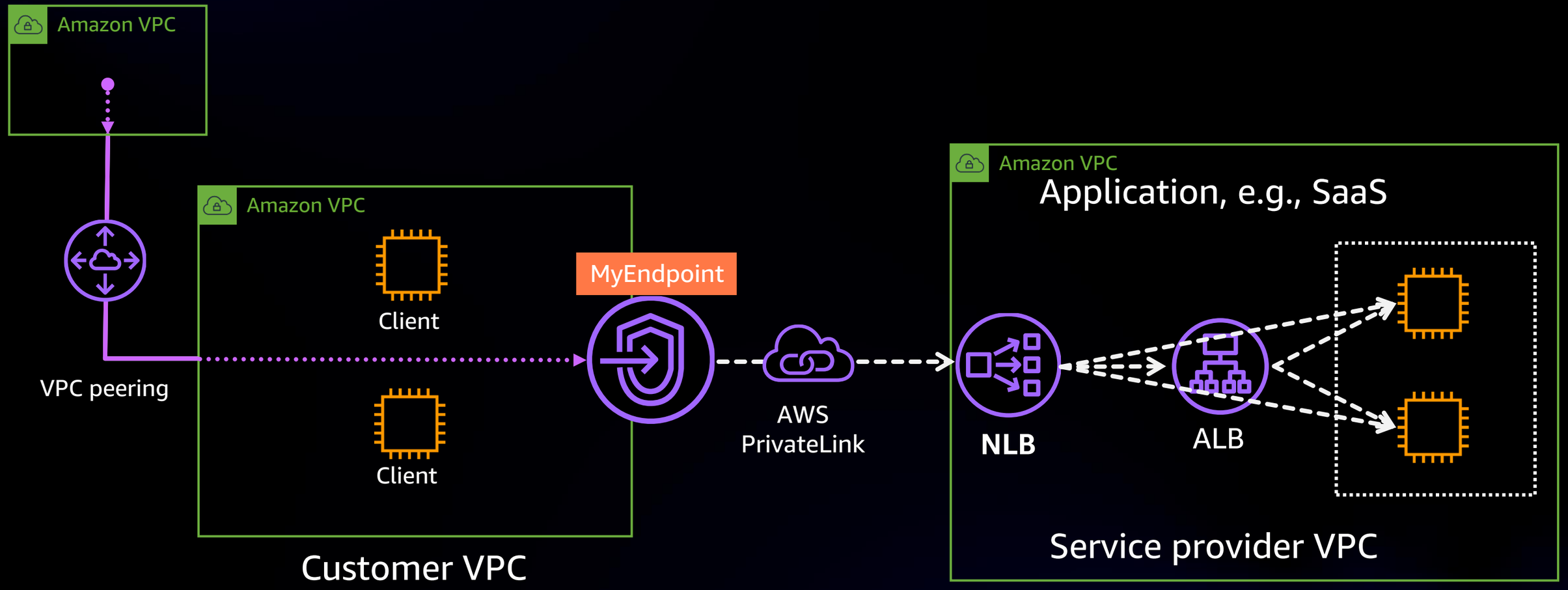
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ALB support through NLB

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink: ALB integration through NLB

NEW



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Networking

Amazon VPC
Enhanced routing

AWS NAT Gateway
Private NAT support

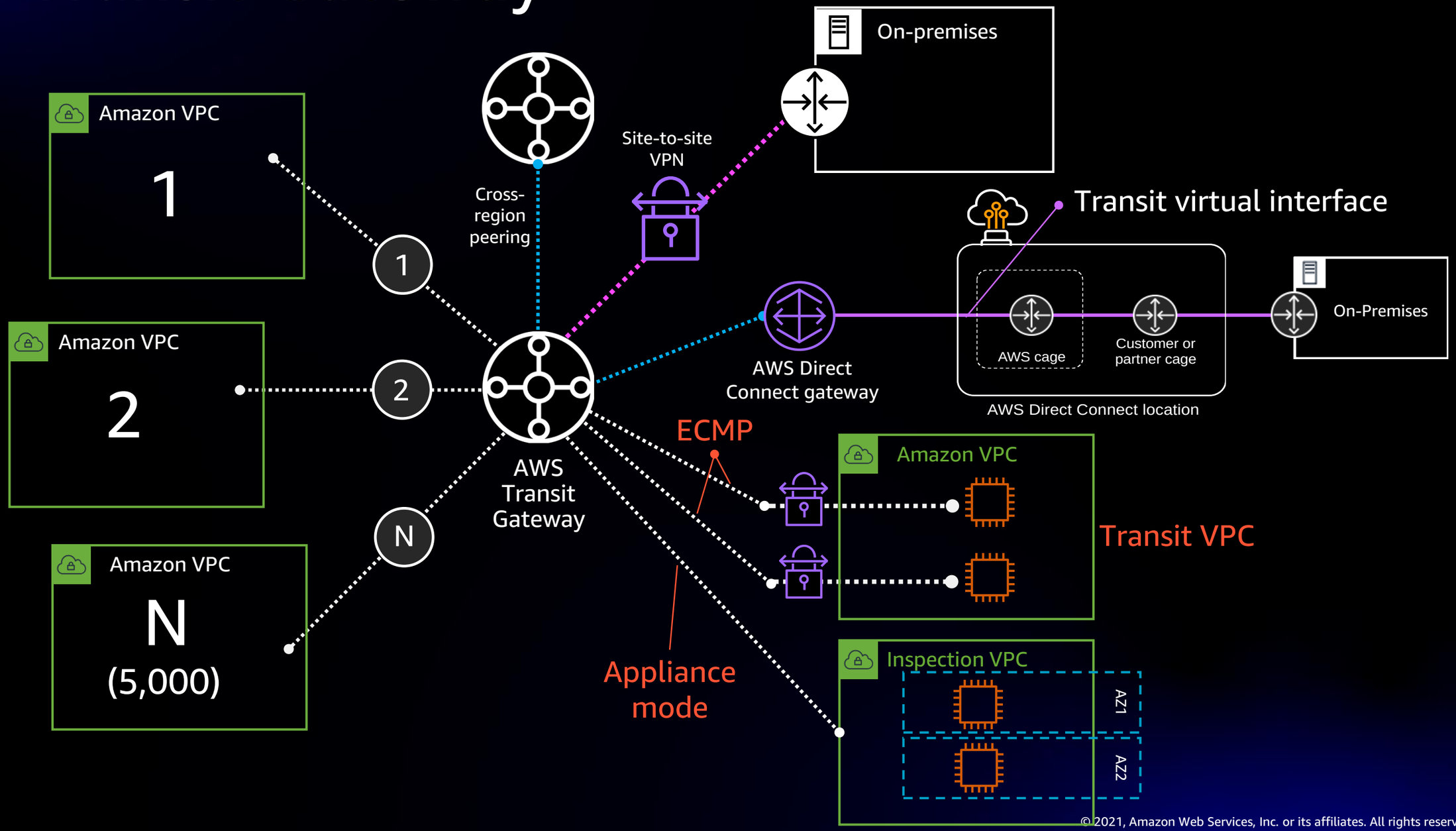
AWS PrivateLink
S3 interface endpoint and ALB integration

AWS Transit Gateway
TGW Connect and intra-region peering

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway

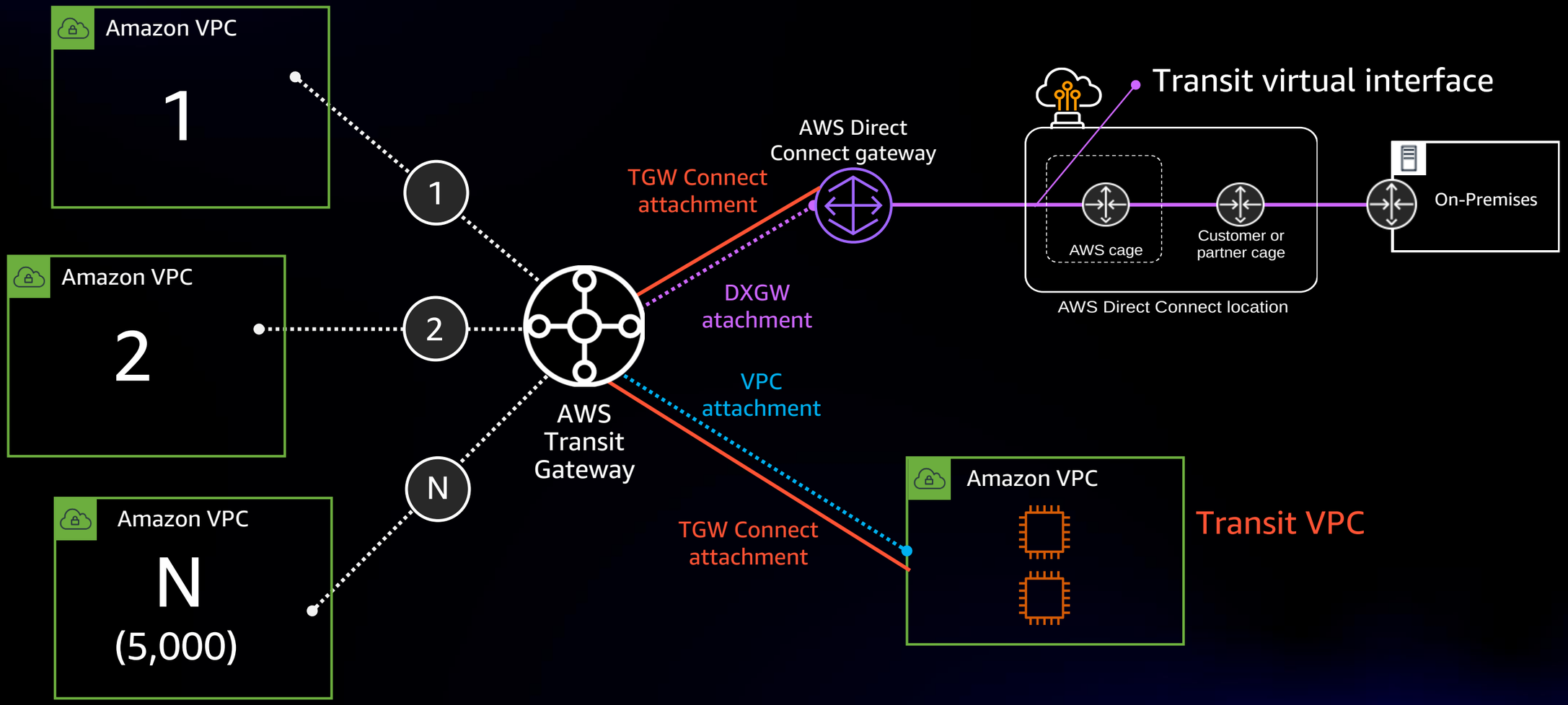
BEFORE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway Connect

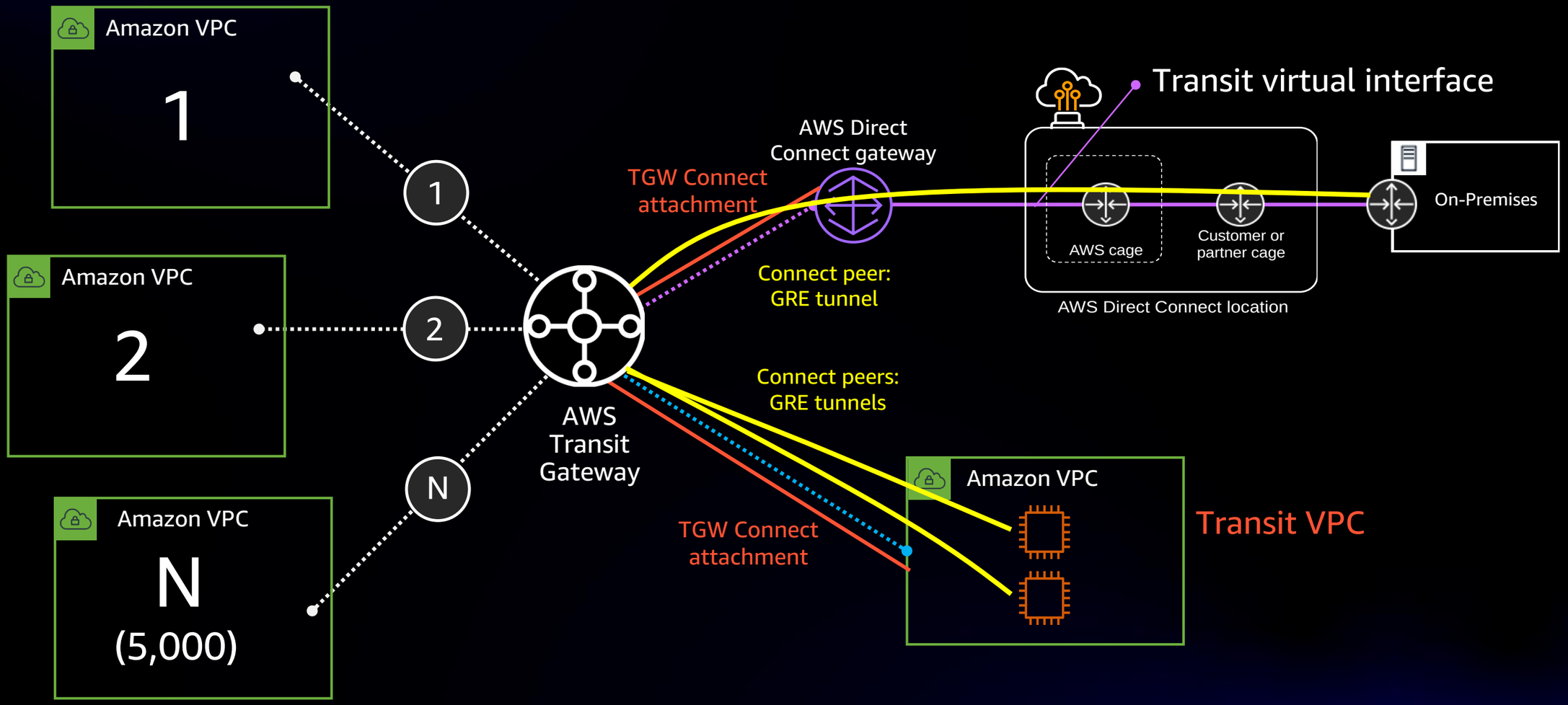
AFTER



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway Connect

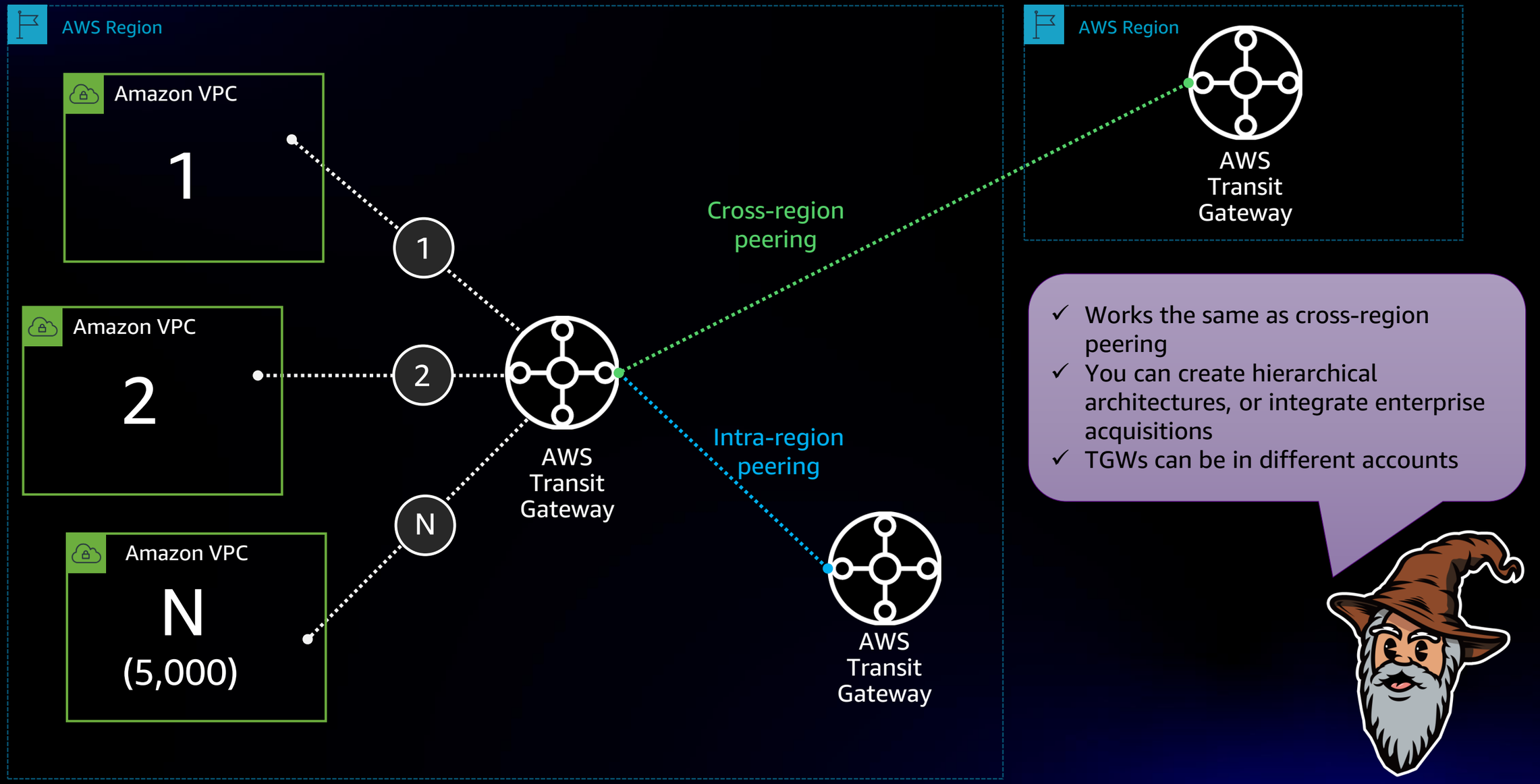
AFTER



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway: Intra-region peering

NEW

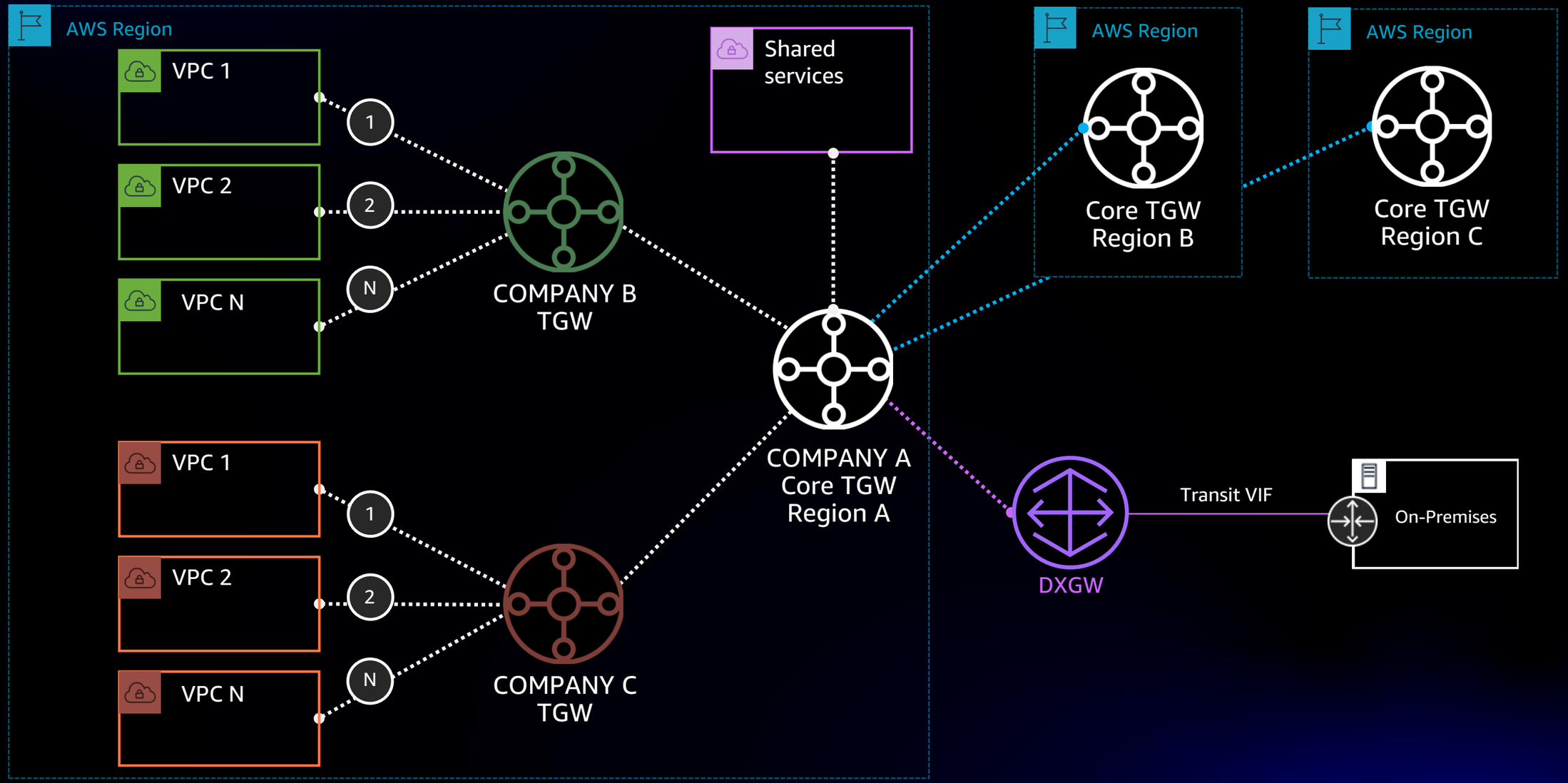


- ✓ Works the same as cross-region peering
- ✓ You can create hierarchical architectures, or integrate enterprise acquisitions
- ✓ TGWs can be in different accounts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway: Intra-region peering

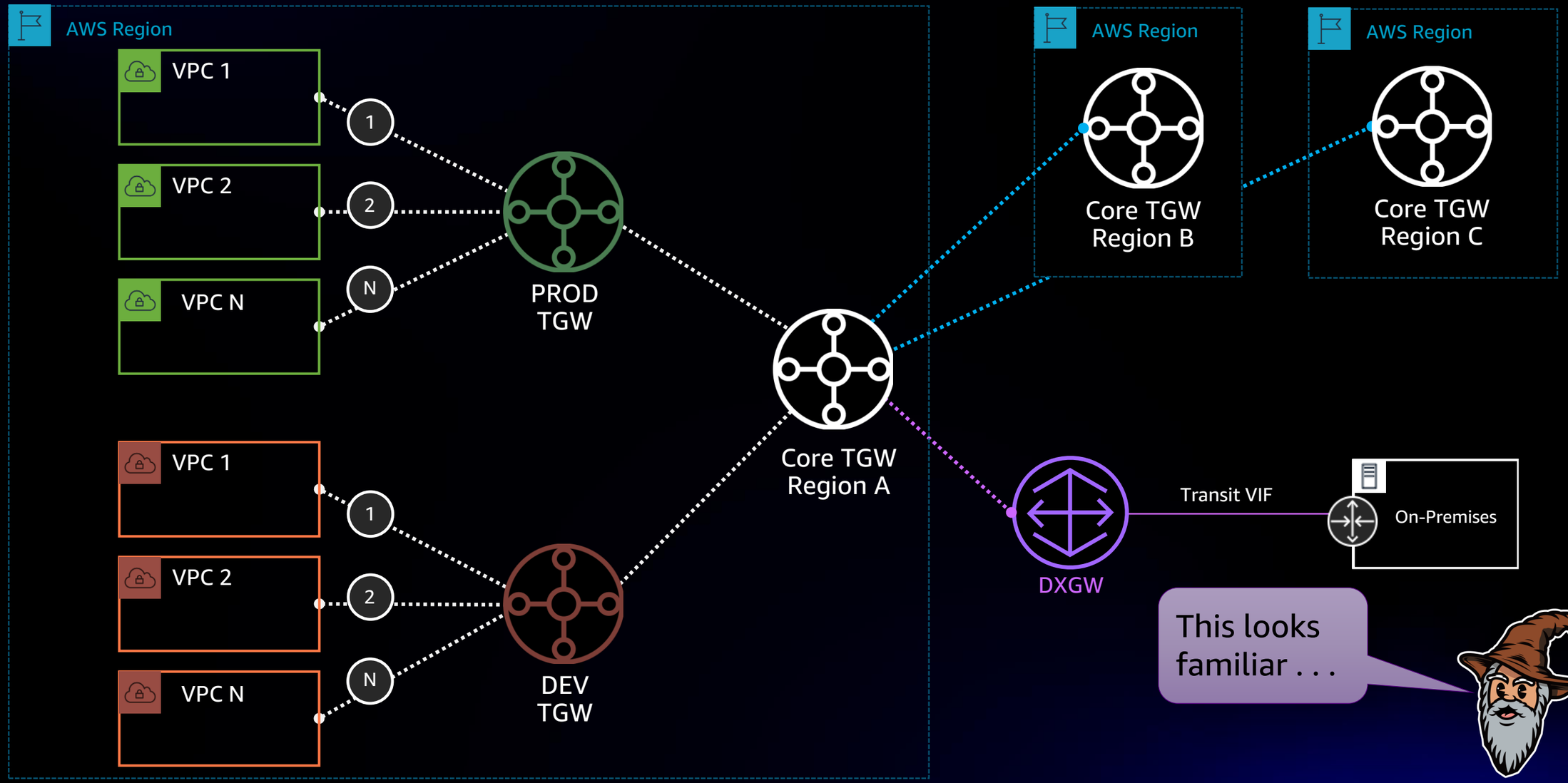
ACQUISITIONS INTEGRATION



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway: Intra-region peering

HIERARCHICAL REGIONAL ARCHITECTURE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

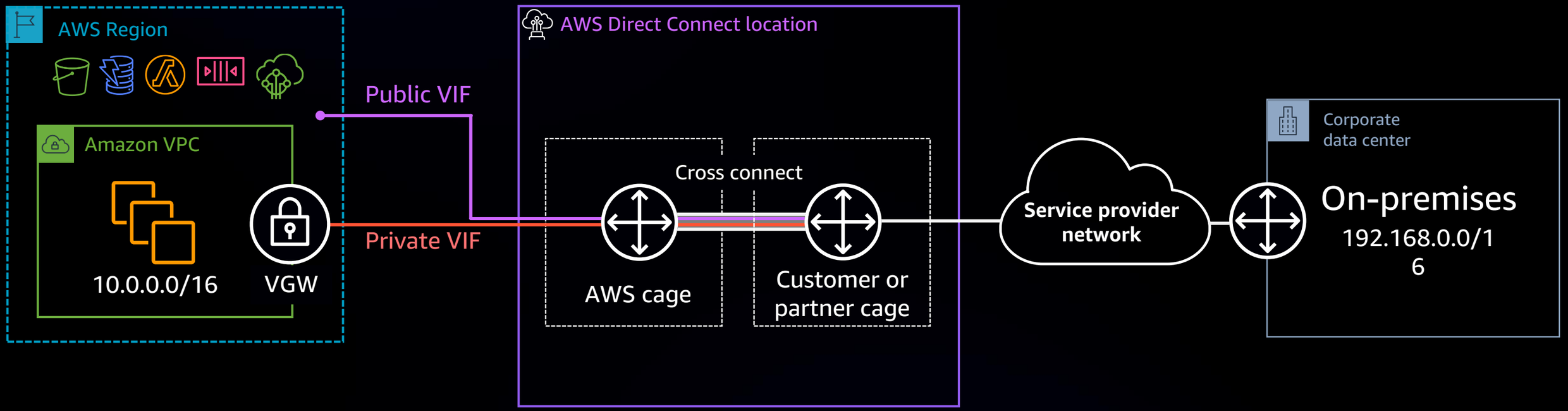
On-premises and global connectivity

AWS Direct Connect

MACSEC , 100Gbps, and AWS Local Zones

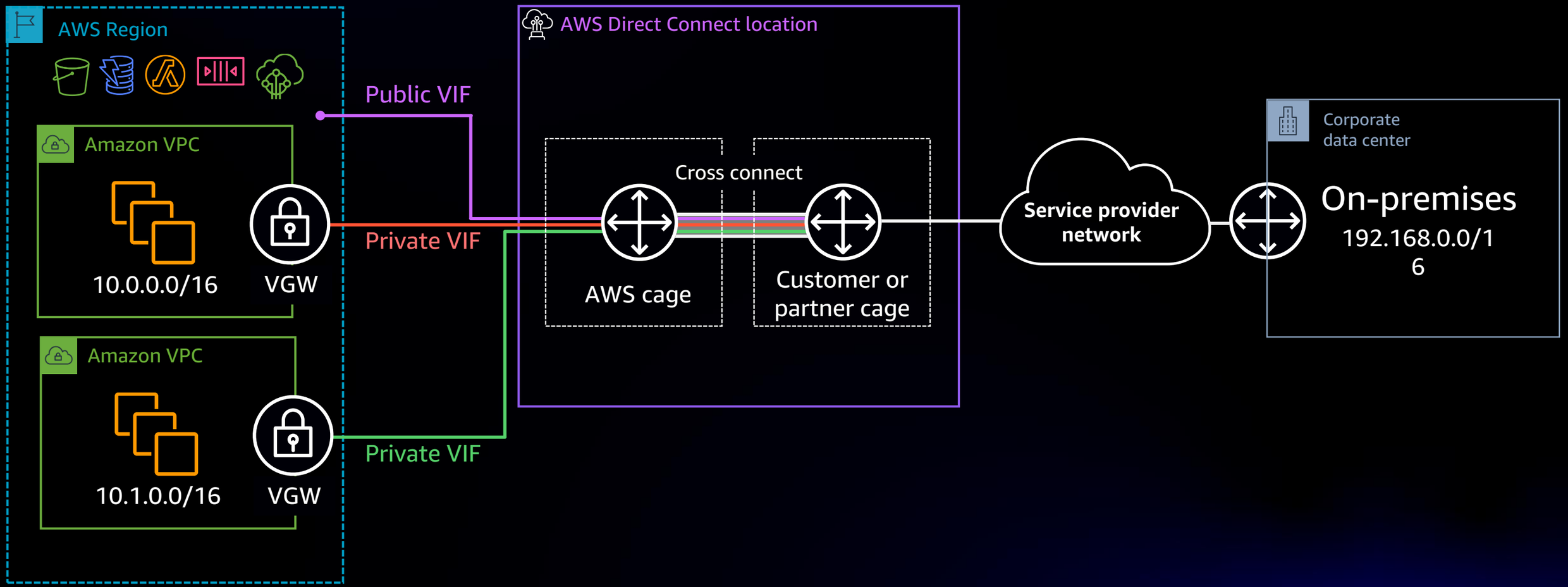
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An overview: AWS Direct Connect



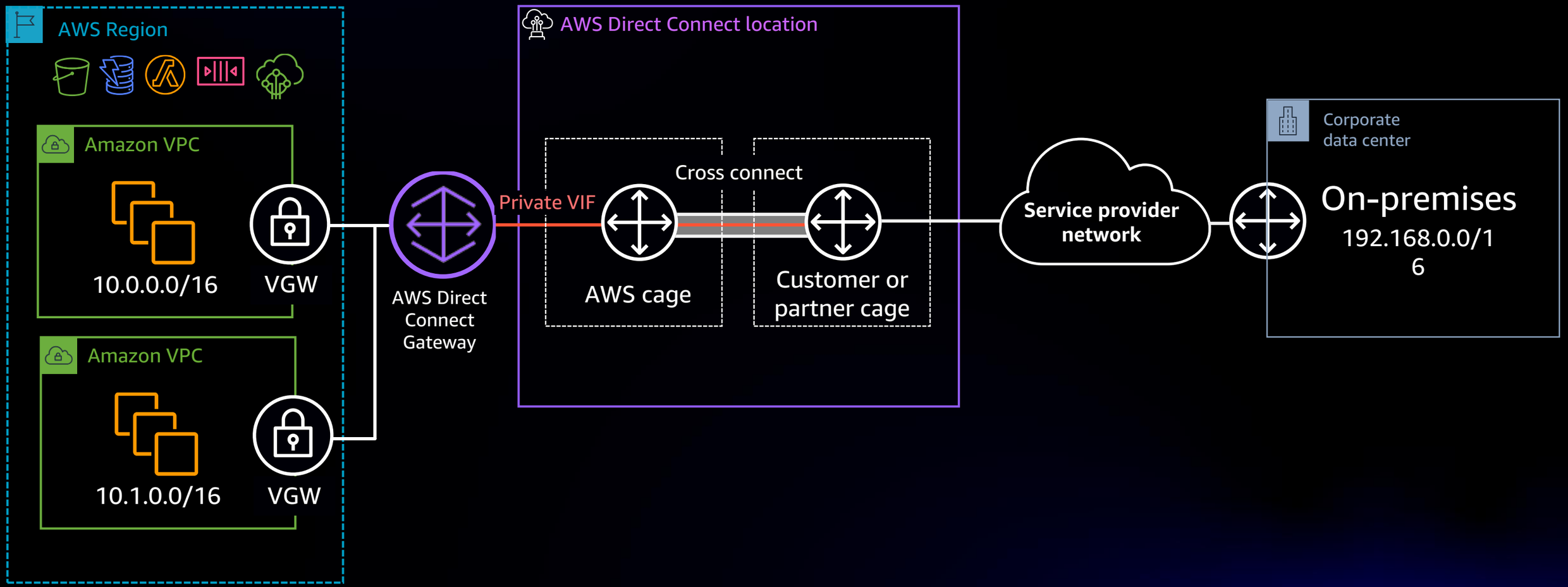
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An overview: AWS Direct Connect



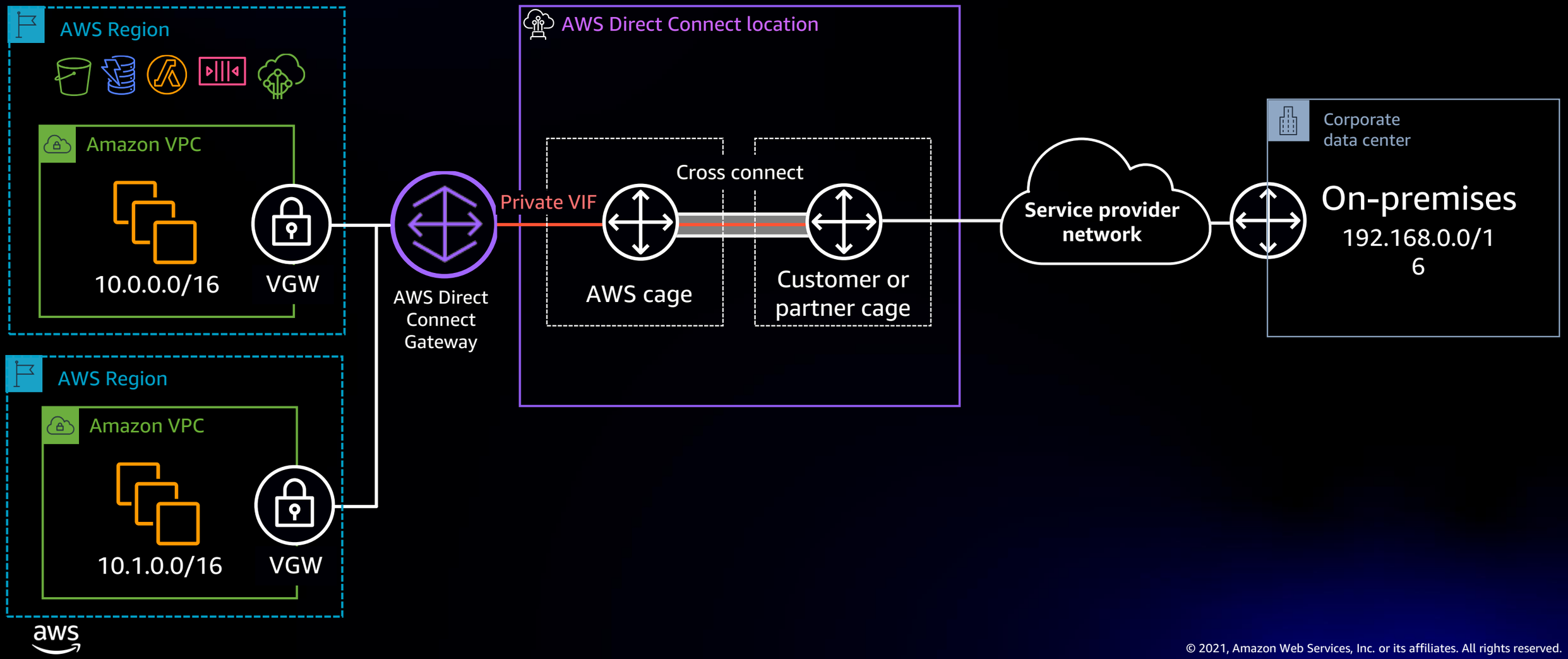
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An overview: AWS Direct Connect



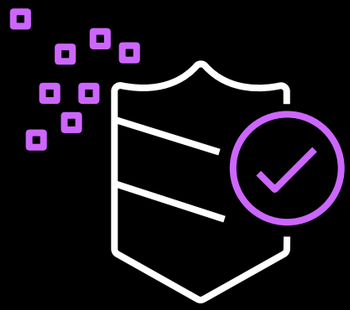
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An overview: AWS Direct Connect



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

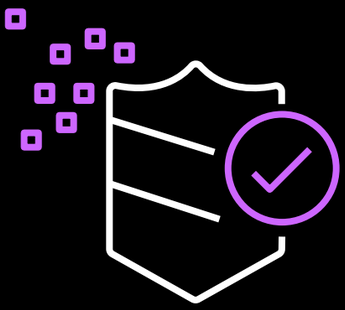
Introducing: AWS Direct Connect MACsec



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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing: AWS Direct Connect MACsec



Layer 2 confidentiality and integrity

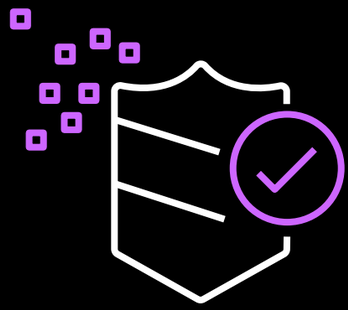
MACsec allows you to secure an Ethernet link – including all control plane protocol packets (such as ARP, DHCP, LLDP, and Layer 3 routing protocols like BGP)

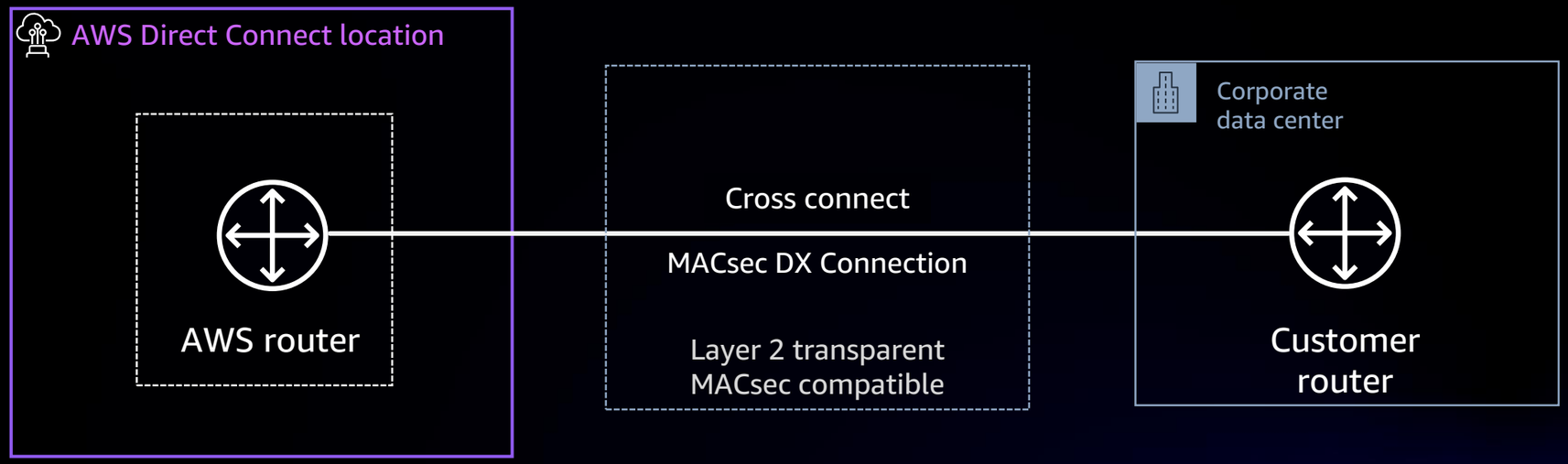
High-speed encryption

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing: AWS Direct Connect MACsec





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Coming soon

Expanded Direct Connect support for AWS Local Zones

Private dedicated connections to Local Zones in more locations



Expanded Local Zones support for Direct Connect in Boston, New York, and Chicago

Use existing Direct Connect connections to connect to AWS Regions and Local Zones

Route traffic directly from your data center to the Local Zone

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

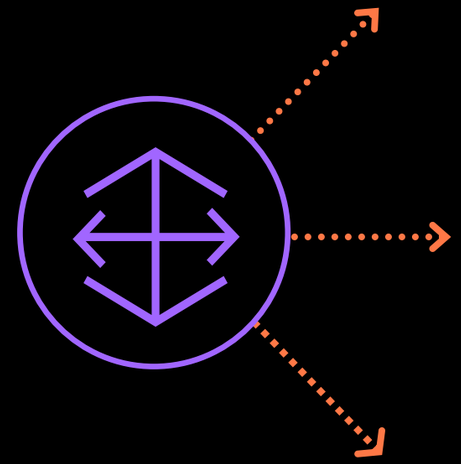
On-premises and global connectivity

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

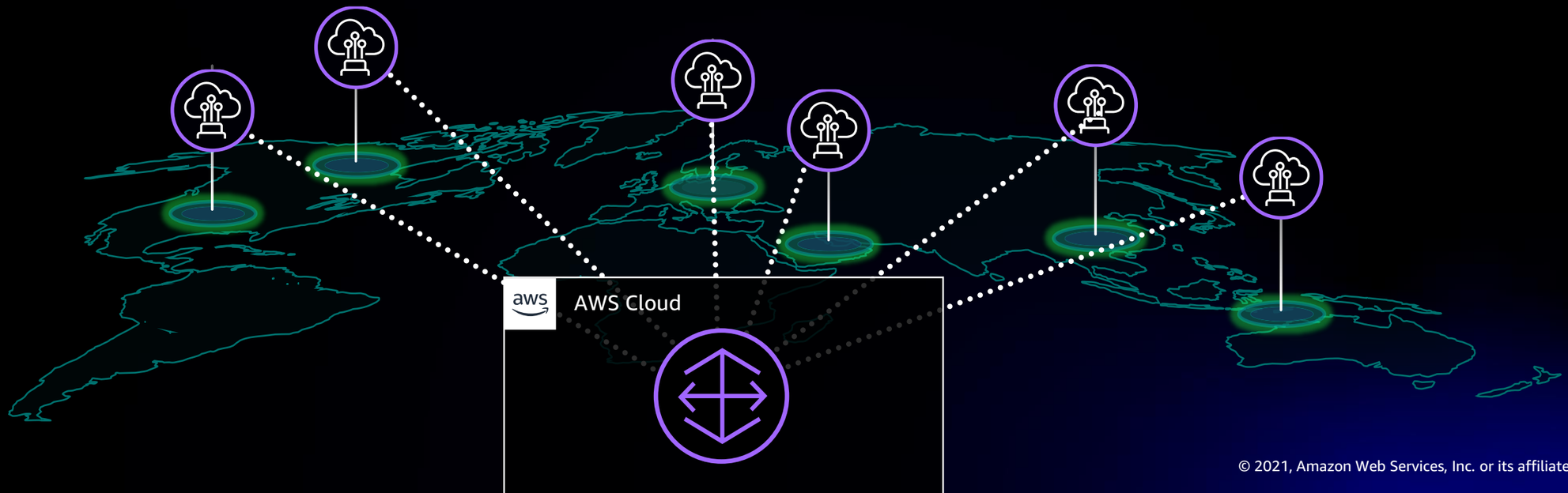
AWS Direct Connect SiteLink
and AWS Direct Connect

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing: AWS Direct Connect SiteLink



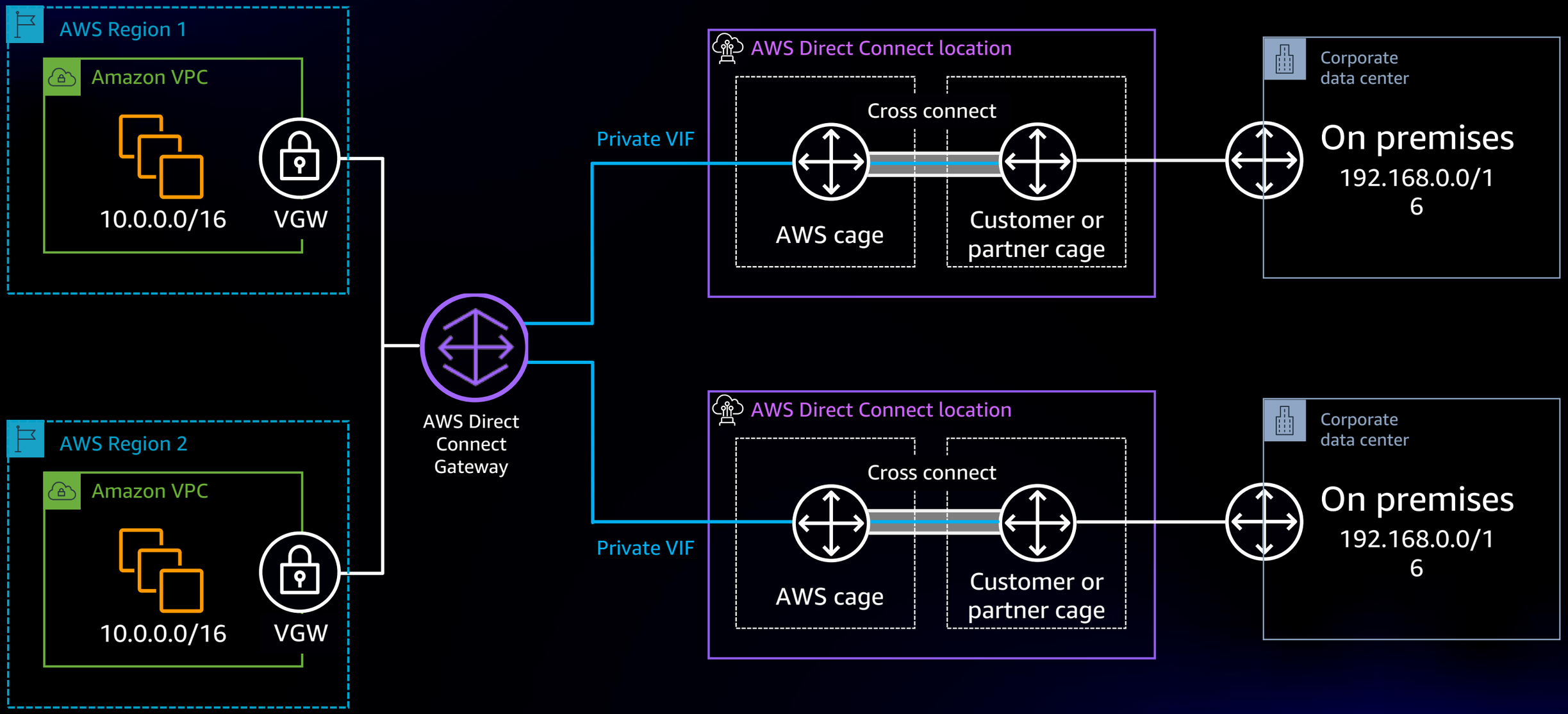
Create connections between your on-premises networks through the AWS global network backbone



aws

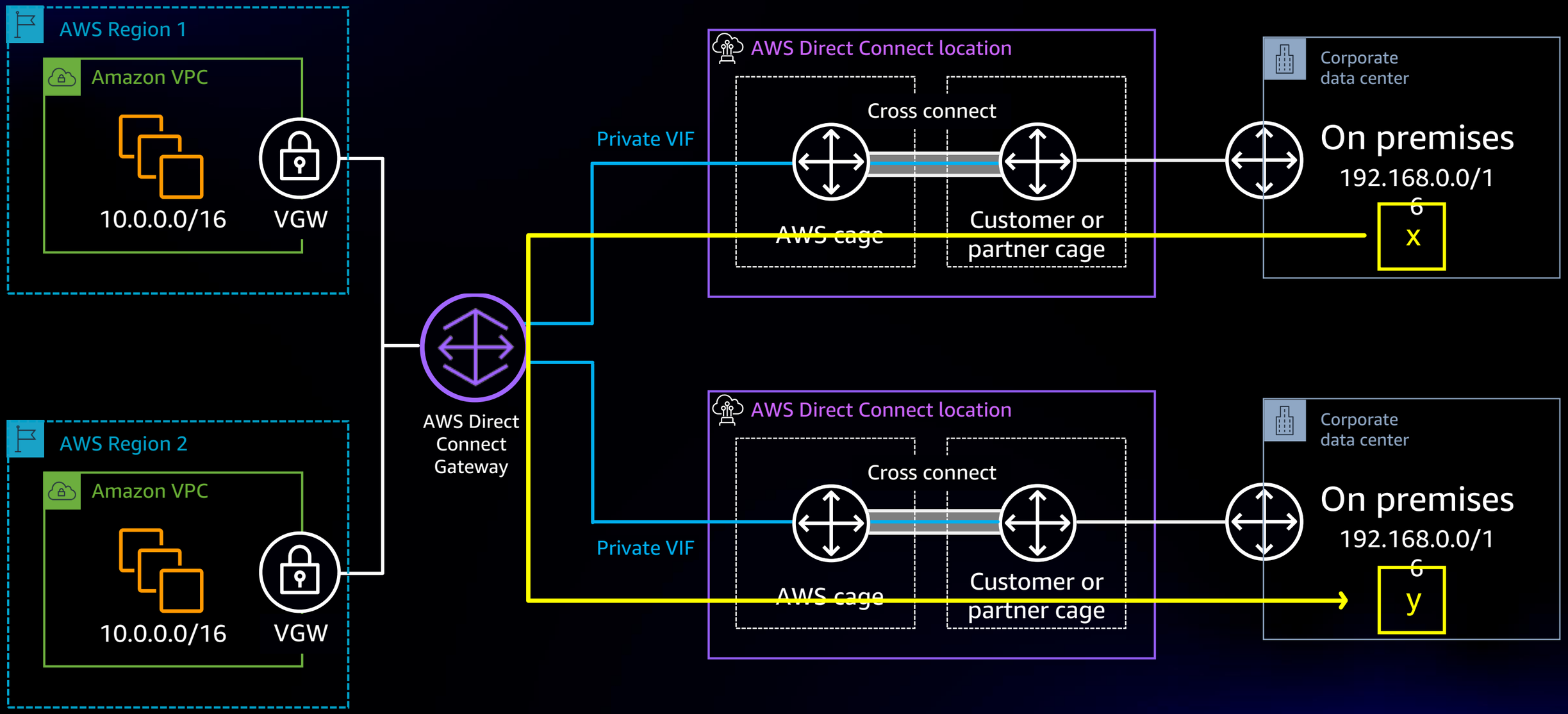
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect SiteLink: Before



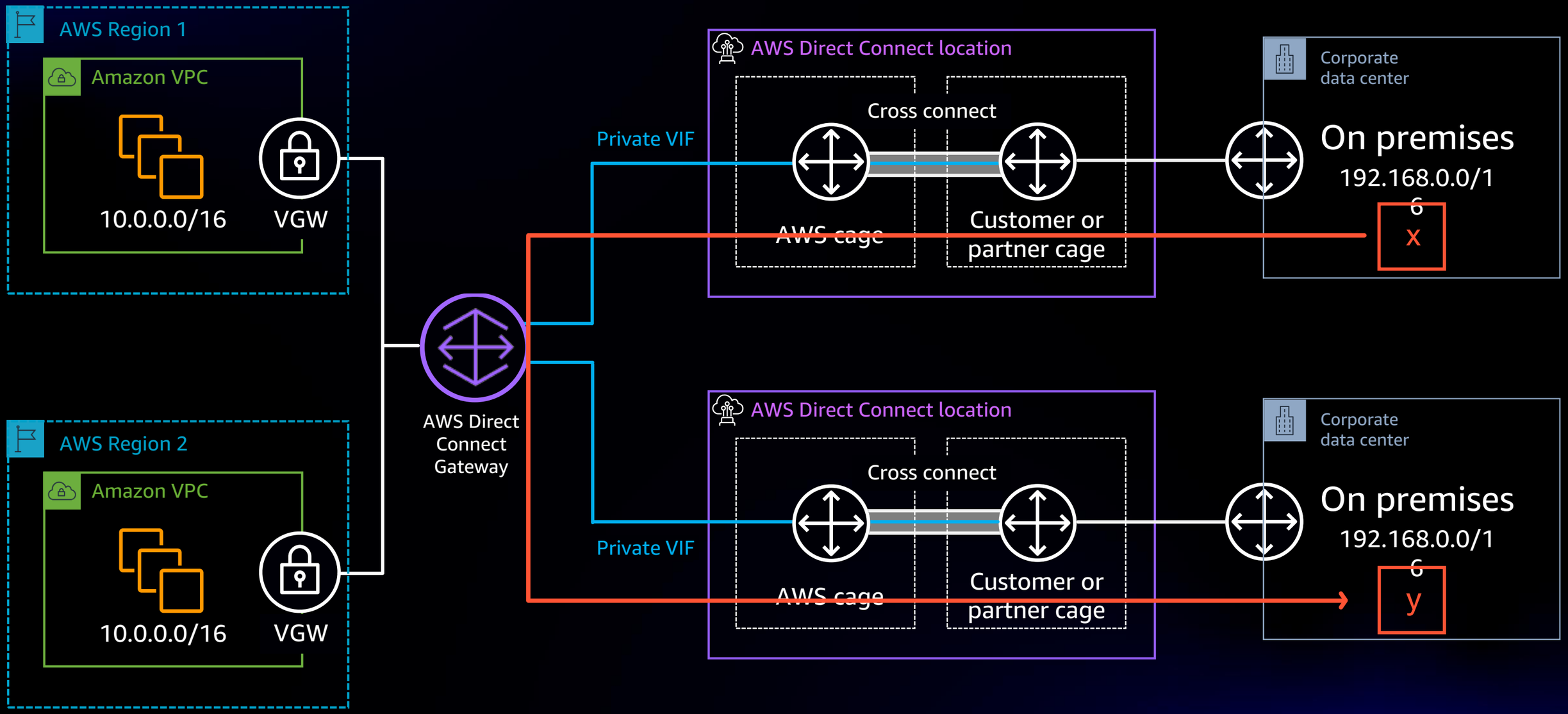
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect SiteLink: Before



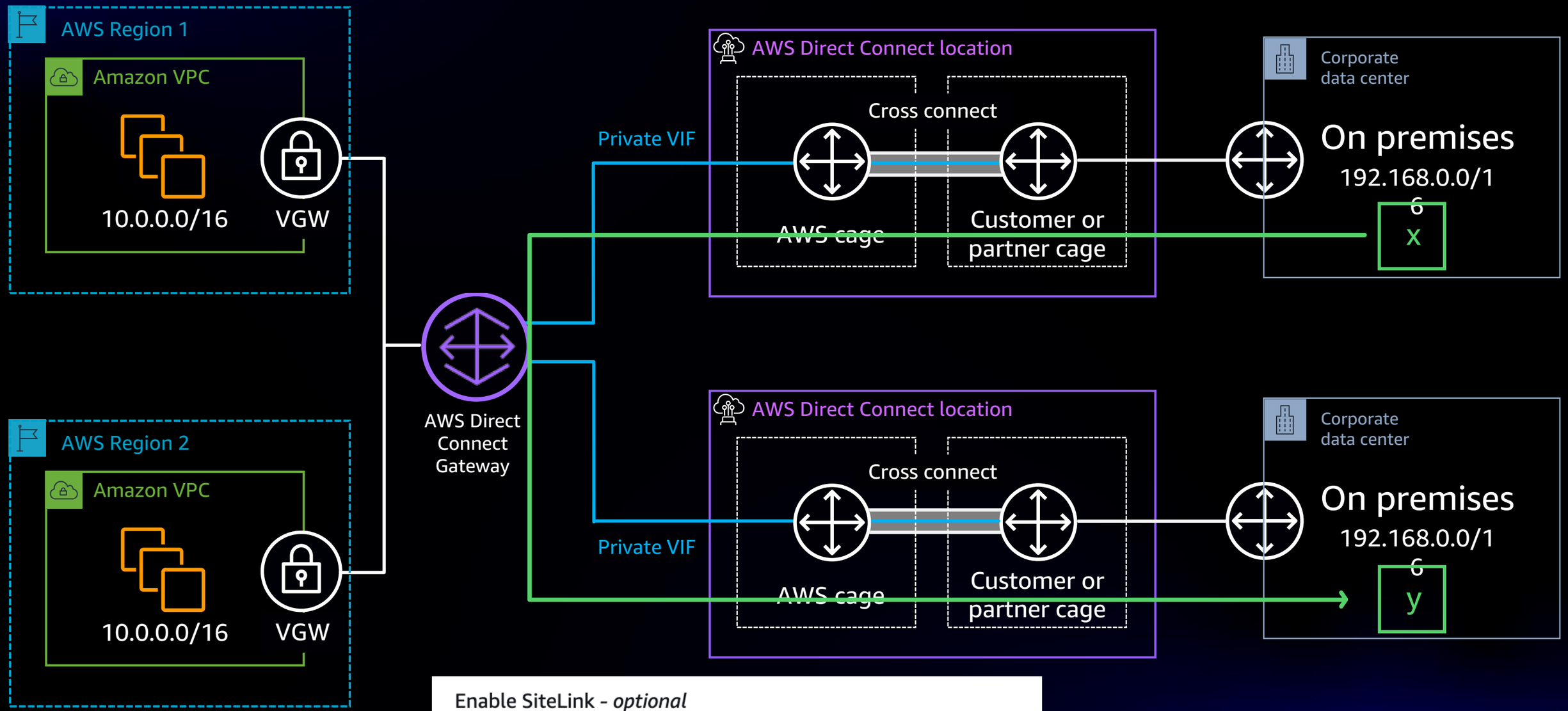
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect SiteLink: Before



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect SiteLink: After

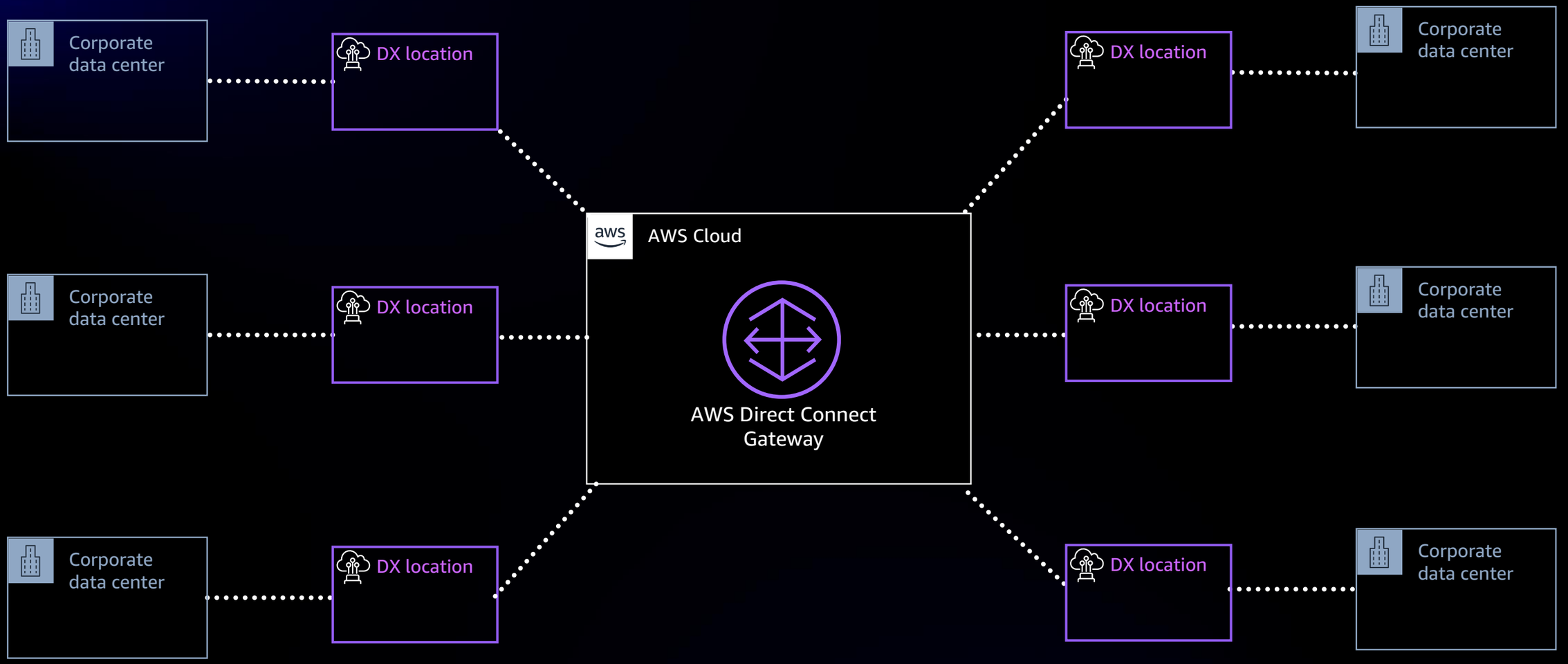


Enable SiteLink - *optional*

Enable direct connectivity between Direct Connect points of presence.

☑ Enabled

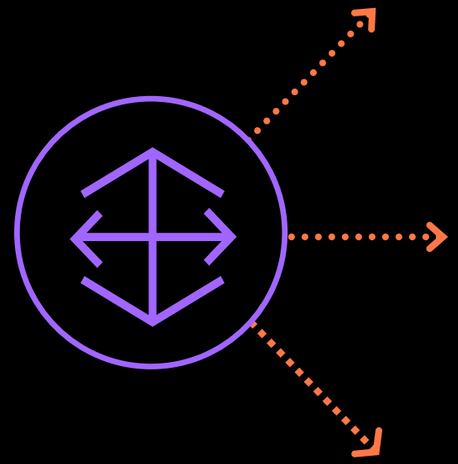
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing: AWS Direct Connect SiteLink



SCAN ME

https://go.aws/2ZTiRG8

AWS Direct Connect SiteLink

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing: AWS Cloud WAN



Available in public preview

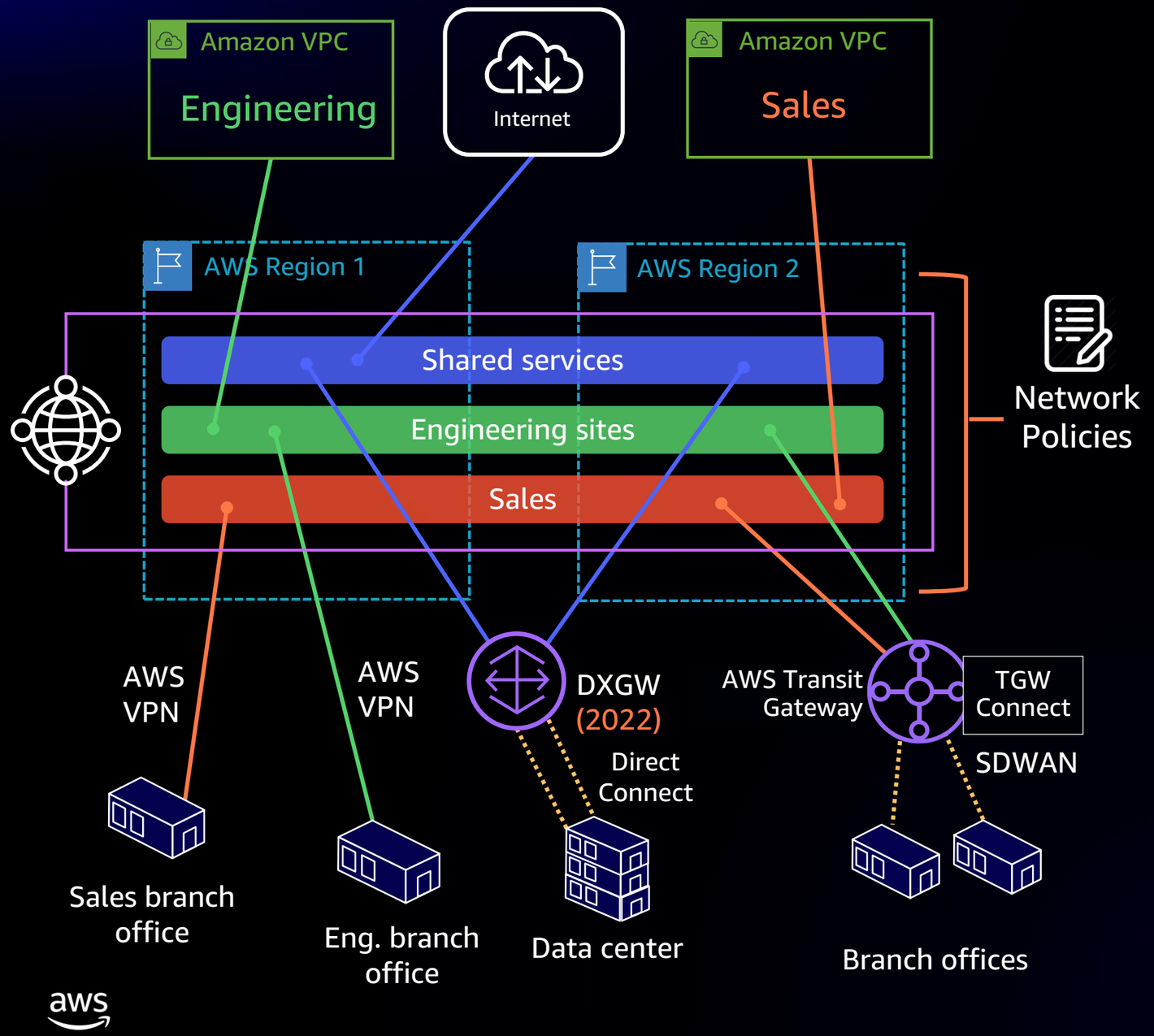
Build global networks in minutes

Use the AWS global backbone

Simplify WAN networking

Segment traffic with centralized policy

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AWS Cloud WAN

Network segments

Isolation between VPCs and on-premises sites

Network policies

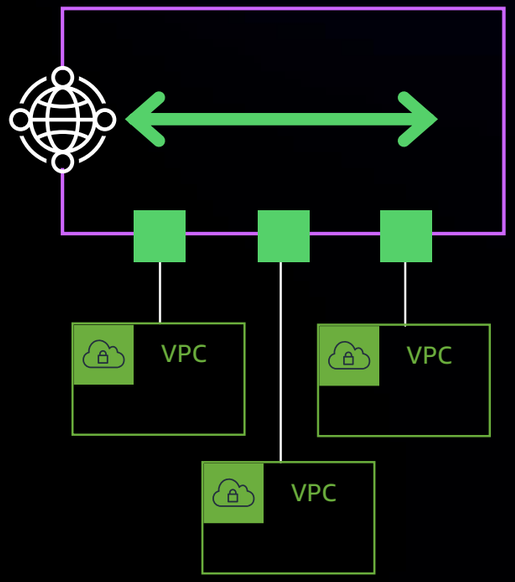
Define L3 routing policies based on attributes and behavior

Performance monitoring

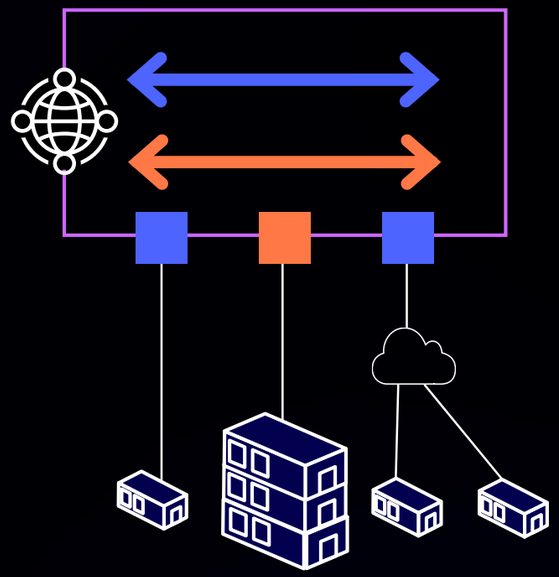
2022 roadmap - Packet loss, jitter, and latency measurements across the backbone.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

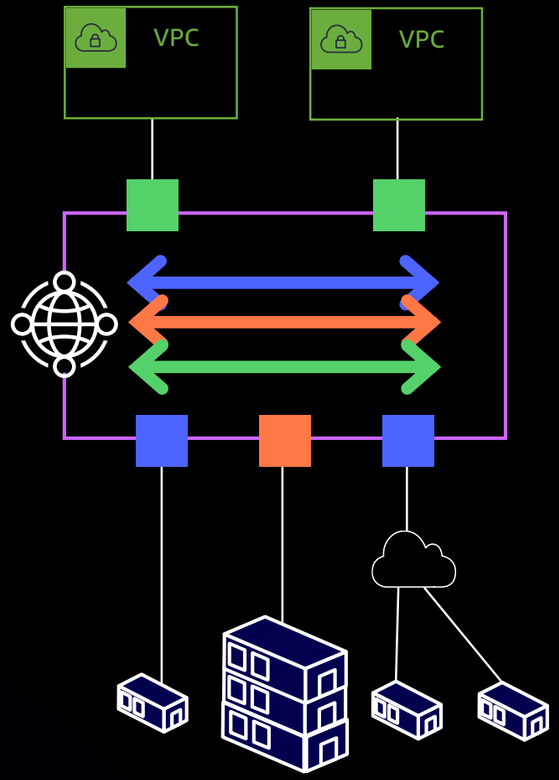
AWS Cloud WAN use cases



Between VPCs



WAN

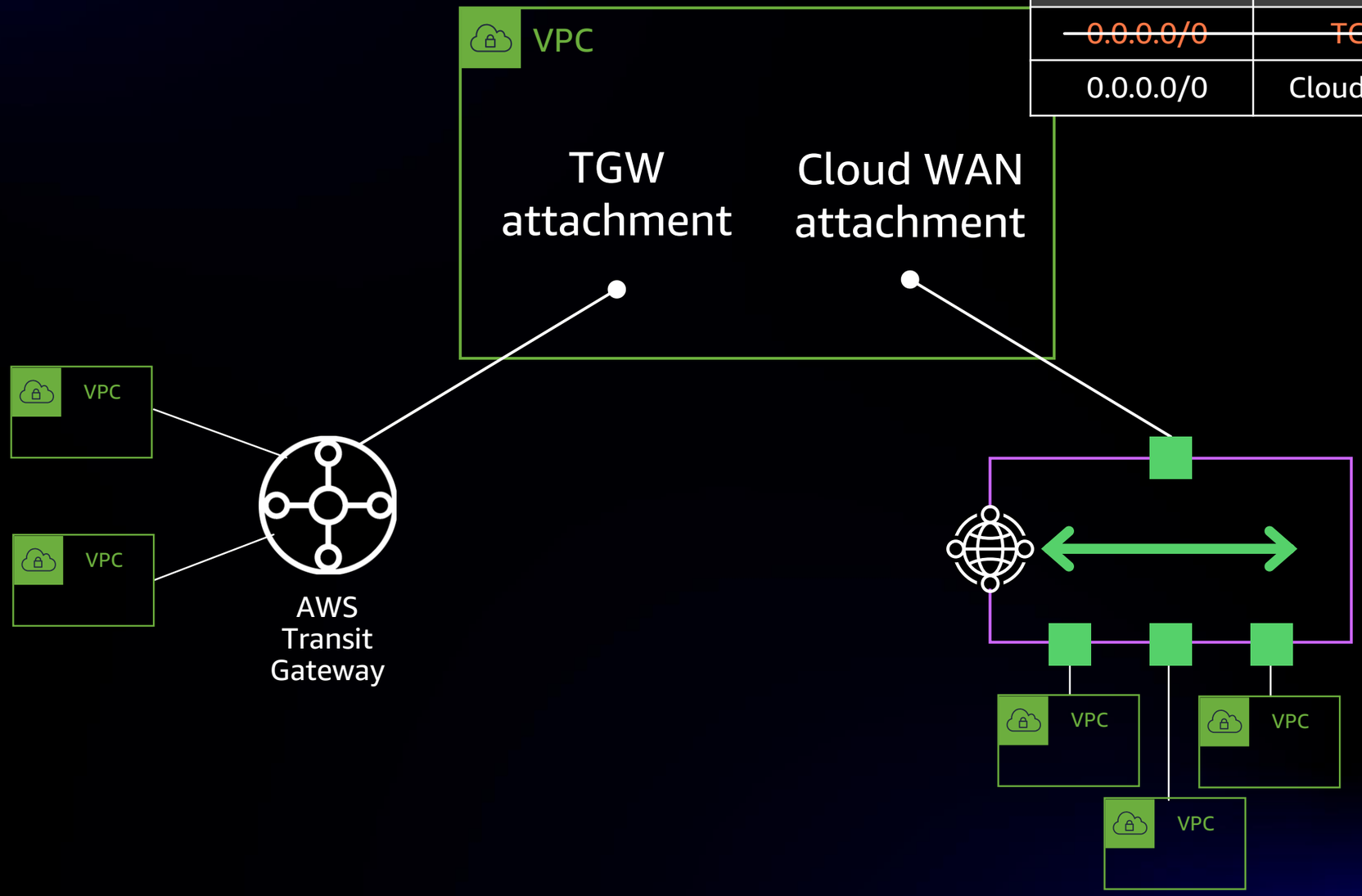


Hybrid

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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)

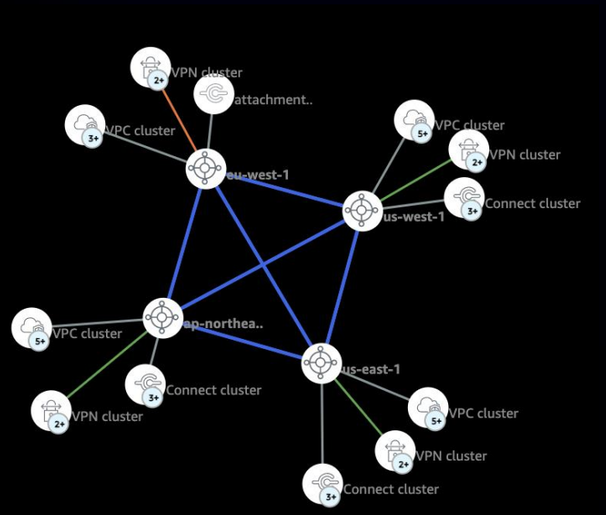
Pay for what you use

Available globally

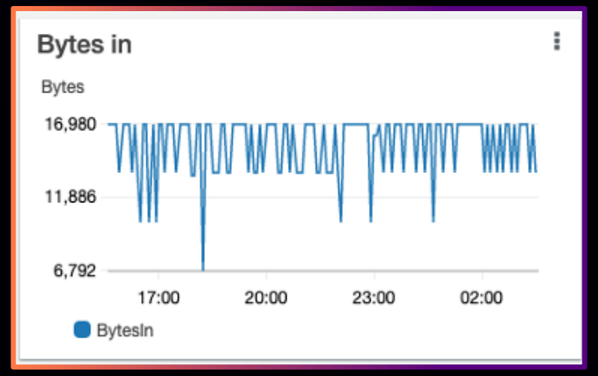
Can also be used to access AWS resources

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Network Manager



Topologies



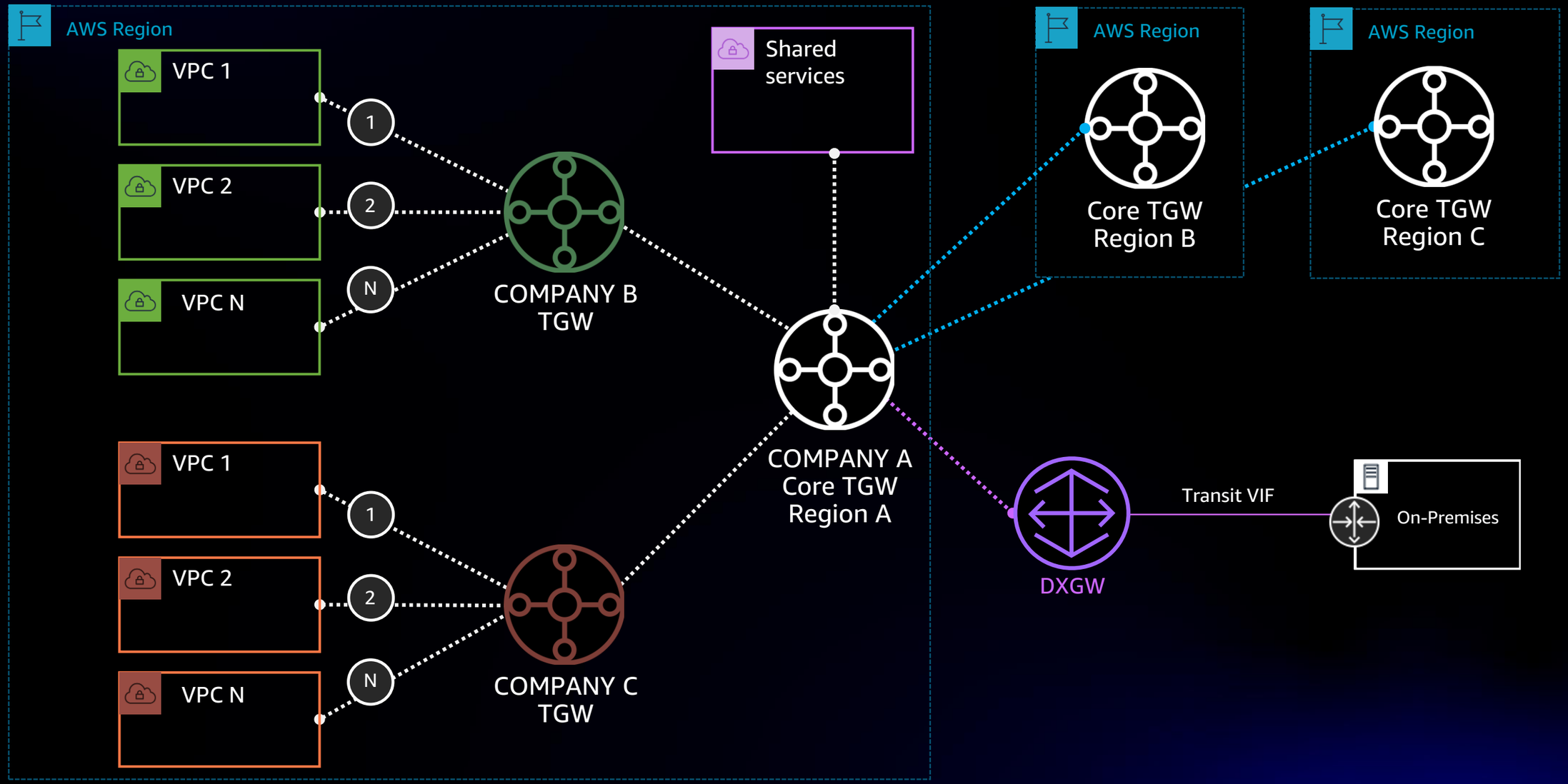
Metrics



Events

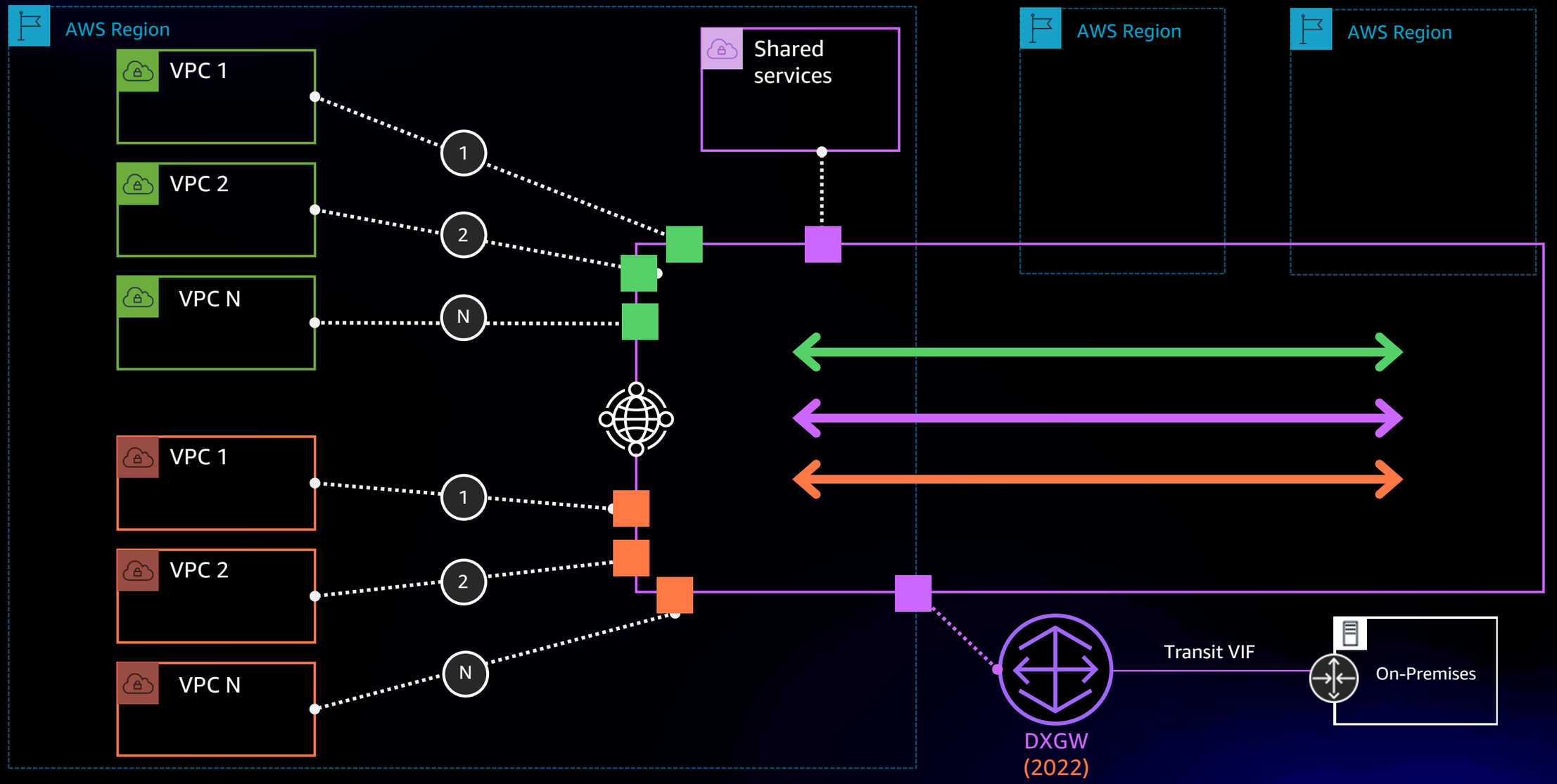
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway: Remember this slide?



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway: Now with AWS Cloud WAN



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing: AWS Cloud WAN



Public preview for AWS Cloud WAN

Anyone can use the service

Not intended for production applications (e.g. no SLA available)

Allowing early access for feedback, and for customers to become familiar with the concepts

Coming in 2022

AWS Transit Gateway attachments

Native AWS Direct Connect attachments

Performance monitoring

More AWS Region support

General availability

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing: AWS Cloud WAN



https://go.aws/3rqedL4

Introducing AWS Cloud WAN

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring and visibility

Network Access Analyzer
Discover and validate network paths

VPC Reachability Analyzer
Troubleshoot connectivity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Network Access Analyzer

VERIFY WHETHER YOUR NETWORK MEETS YOUR ACCESS POLICY



Define your network access policy as Network Access Scopes



Run analyses to evaluate your network access



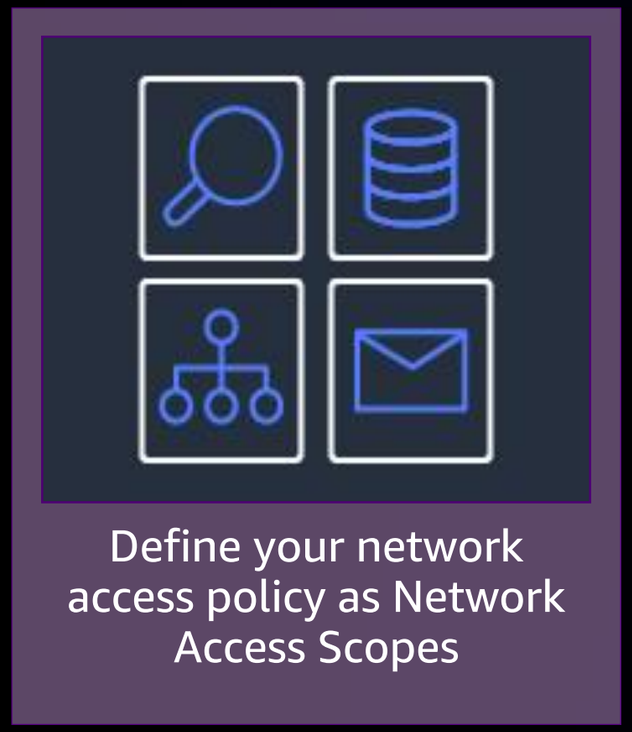
Review network paths compliance with the access requirements

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Network Access Analyzer

VERIFY WHETHER YOUR NETWORK MEETS YOUR ACCESS POLICY



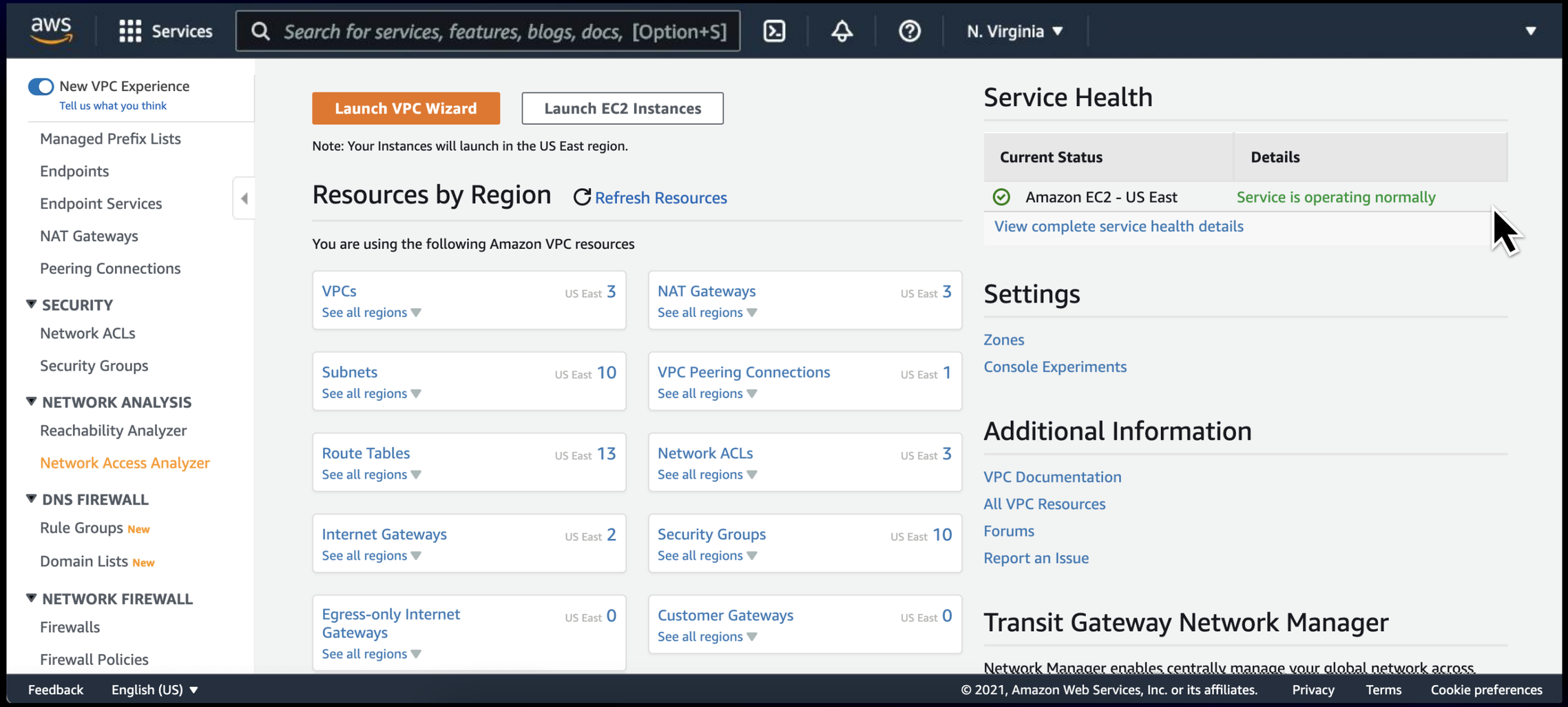
Define your network access policy as Network Access Scopes

VPC internet accessibility

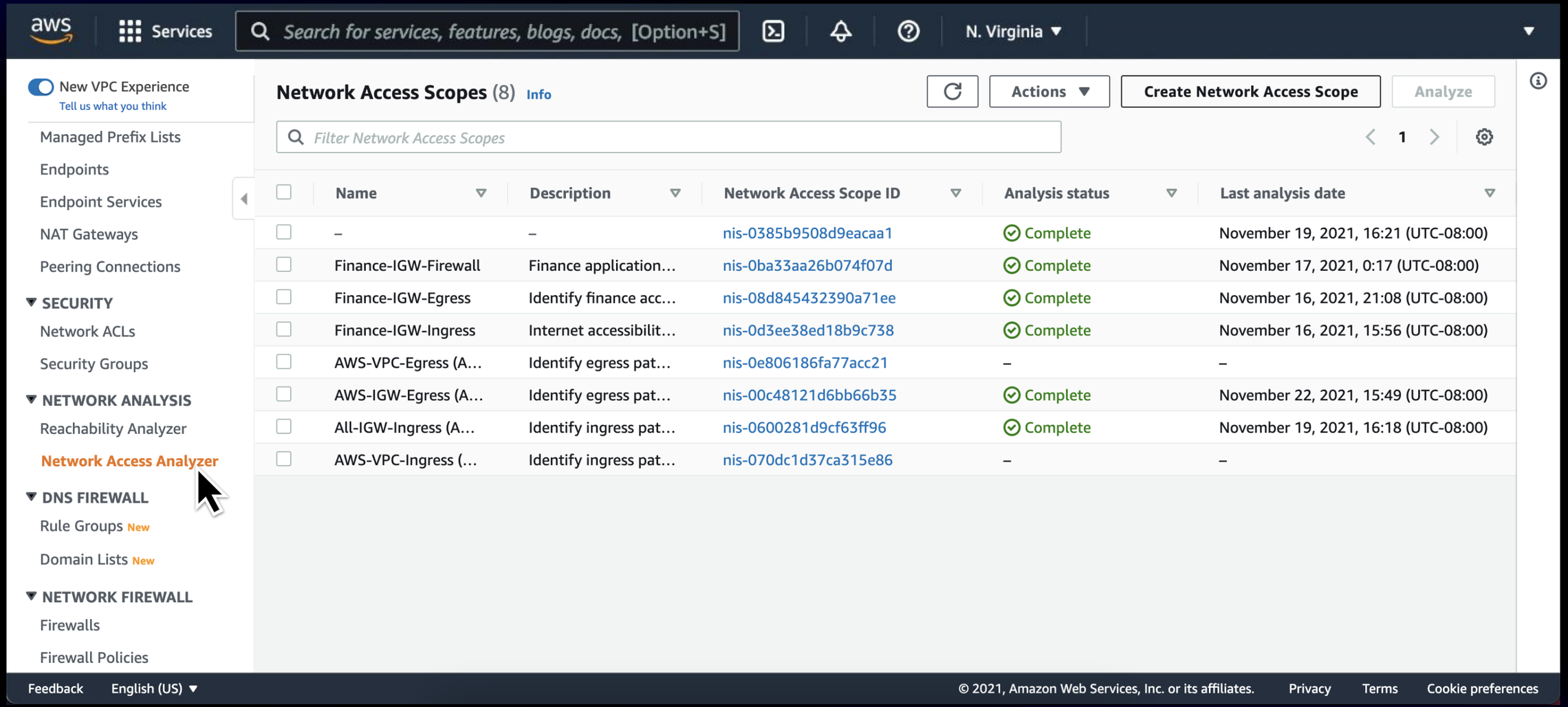
Internal network segmentation

Trusted access validation

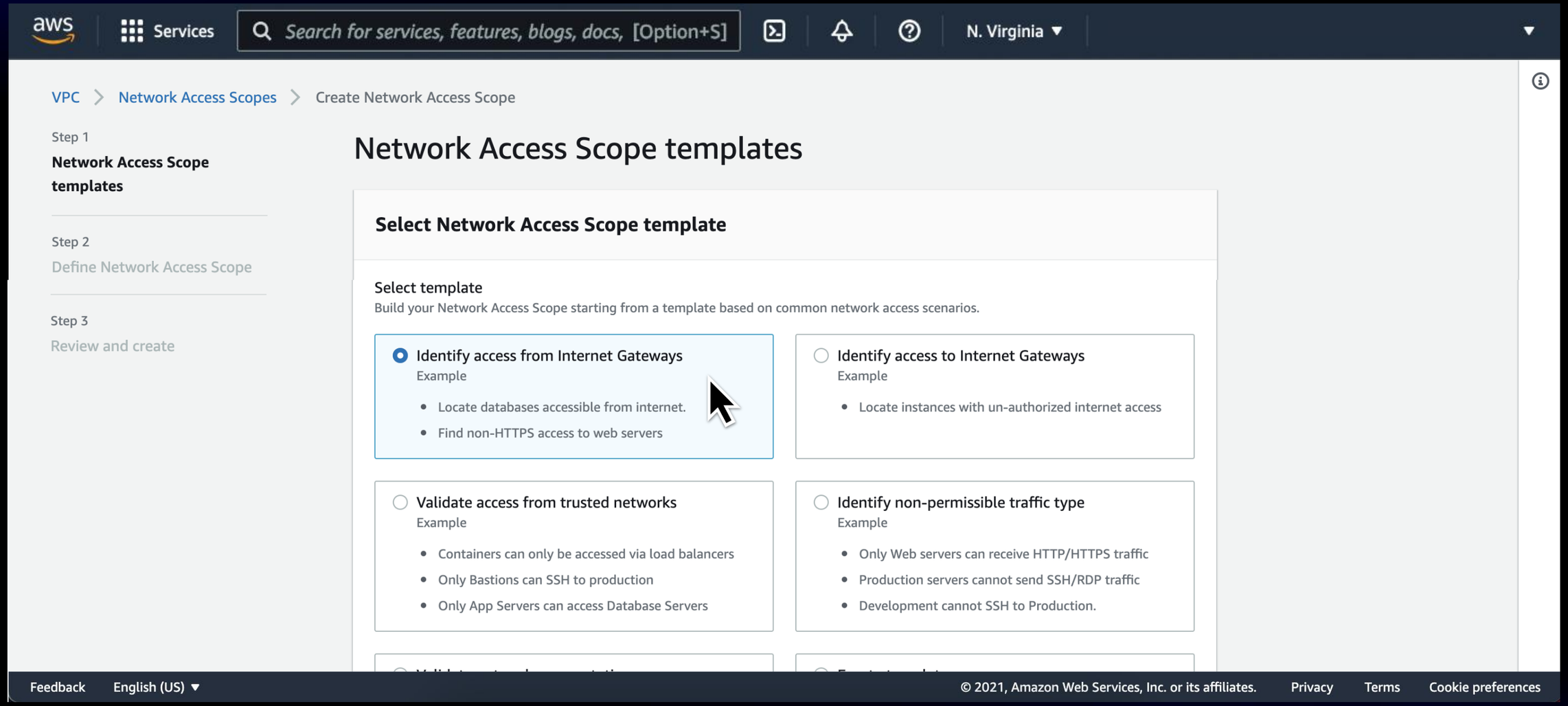
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



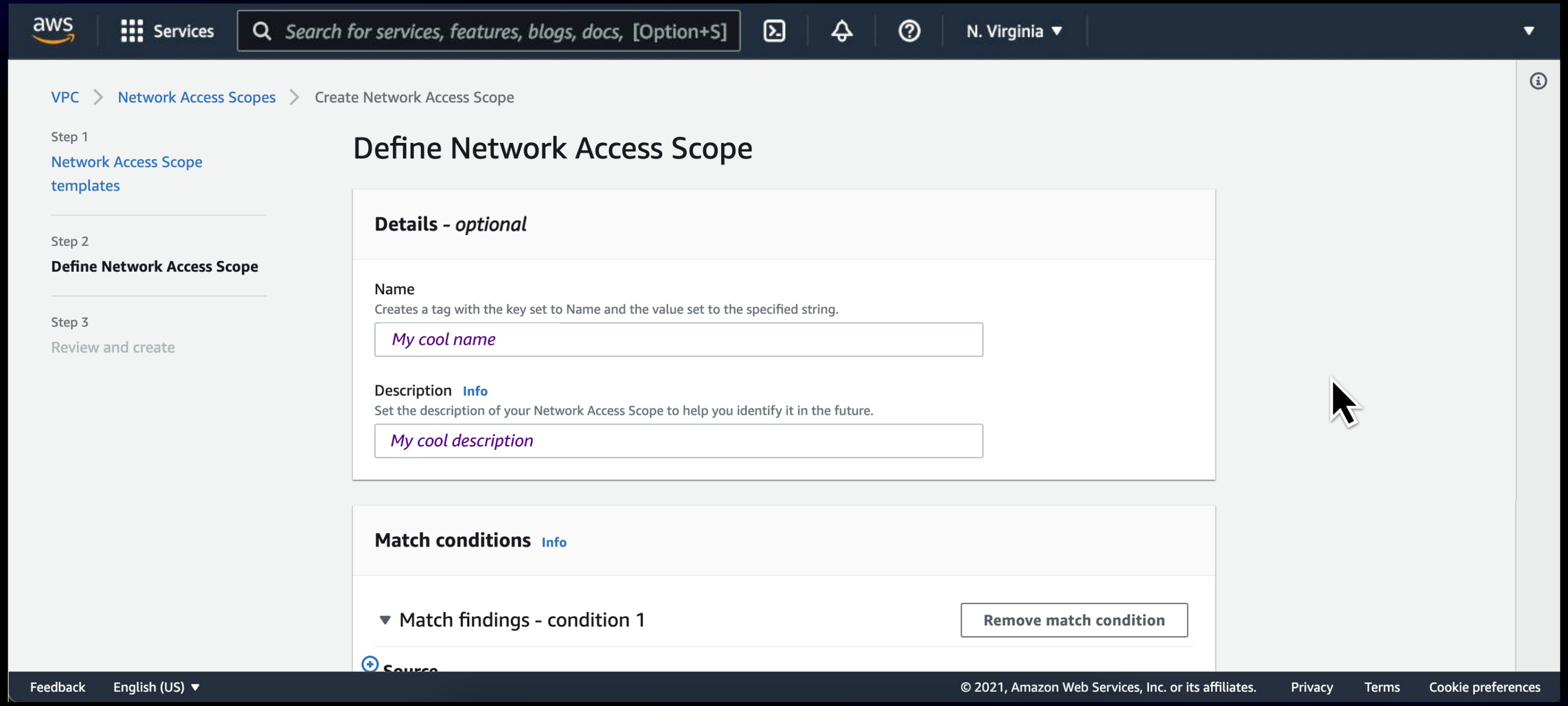
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



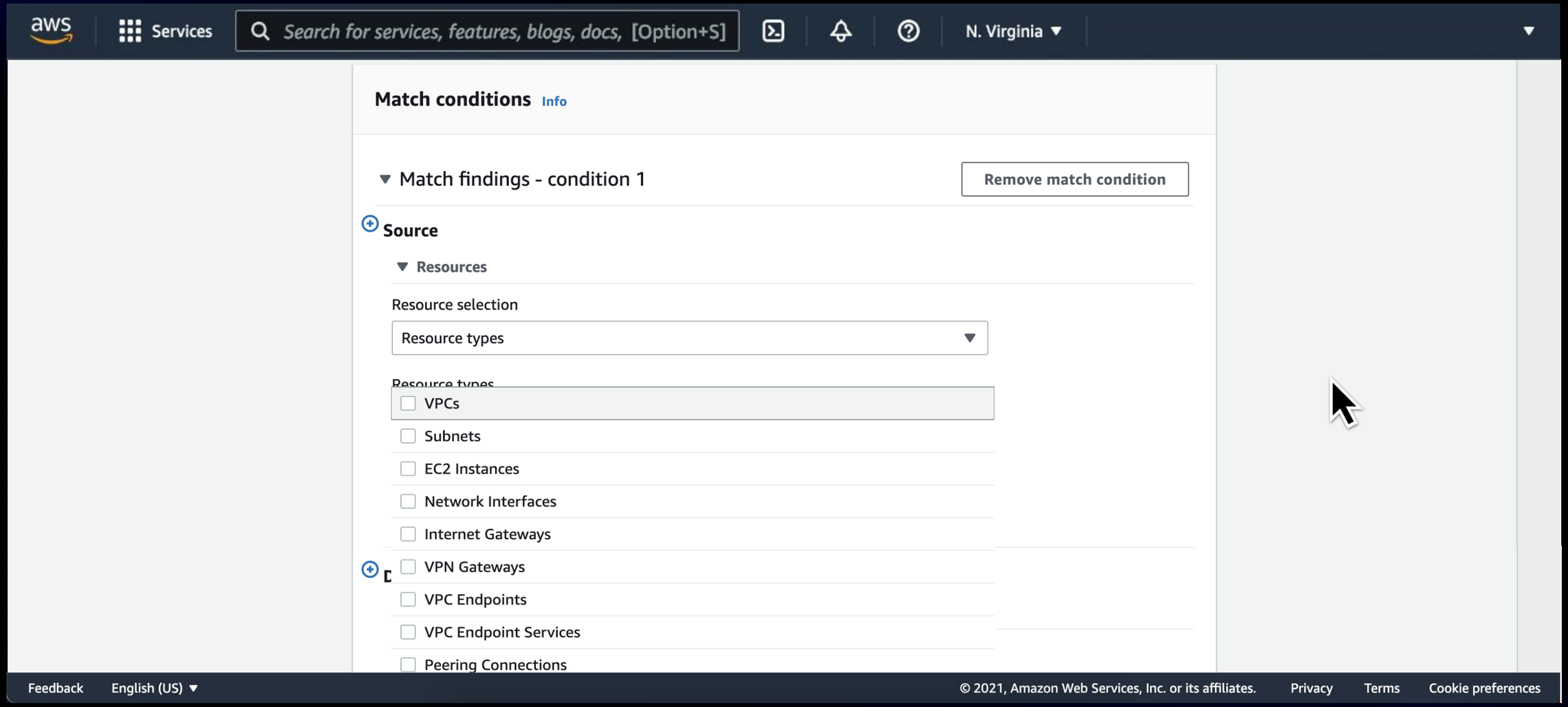
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



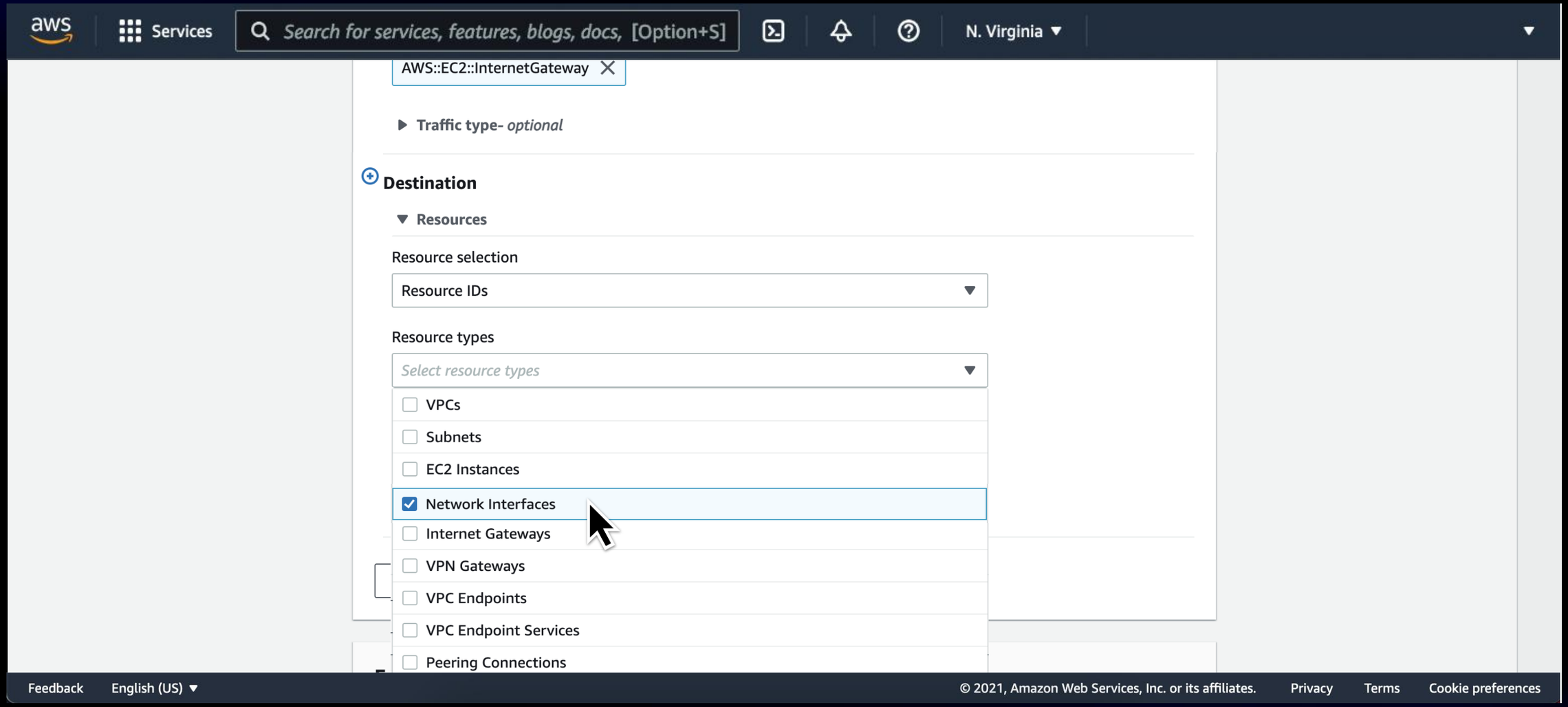
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



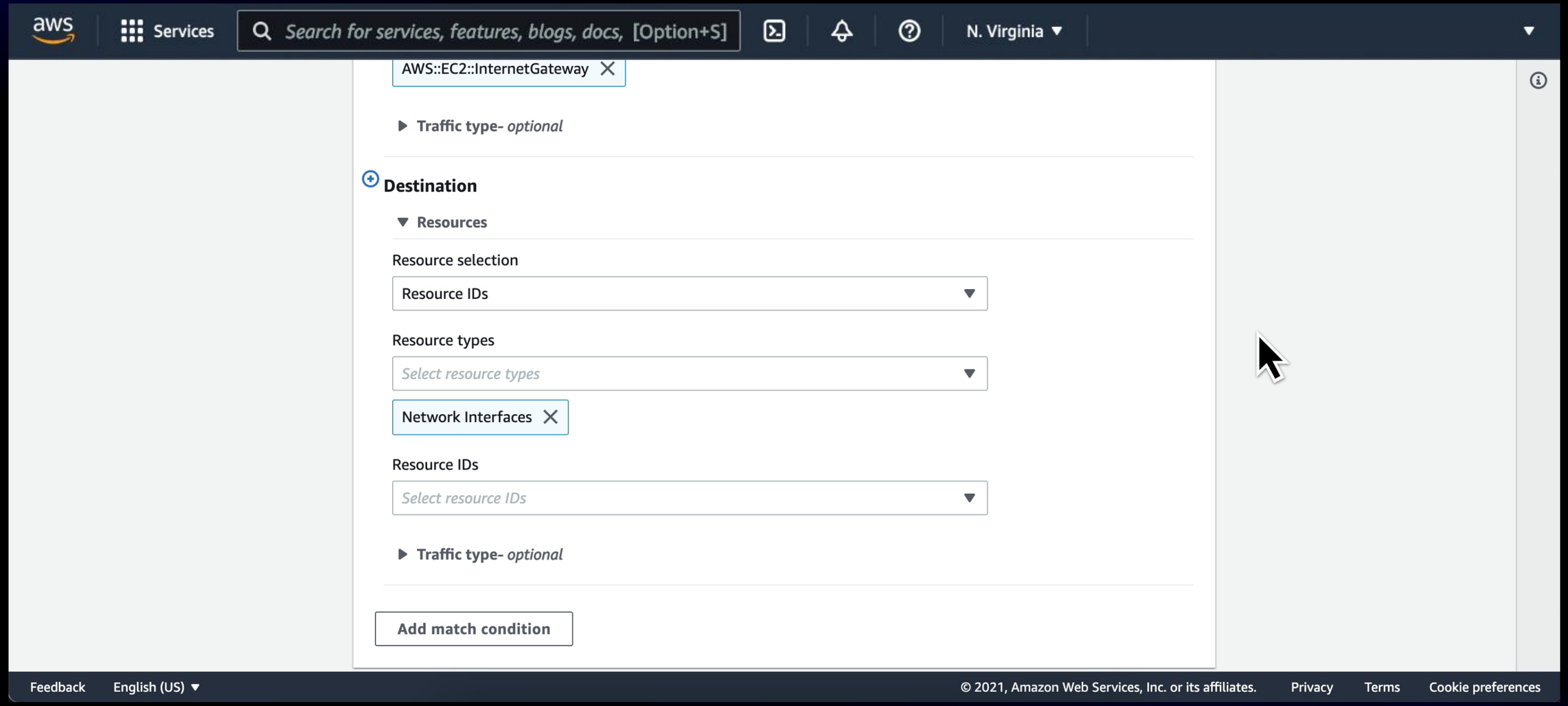
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



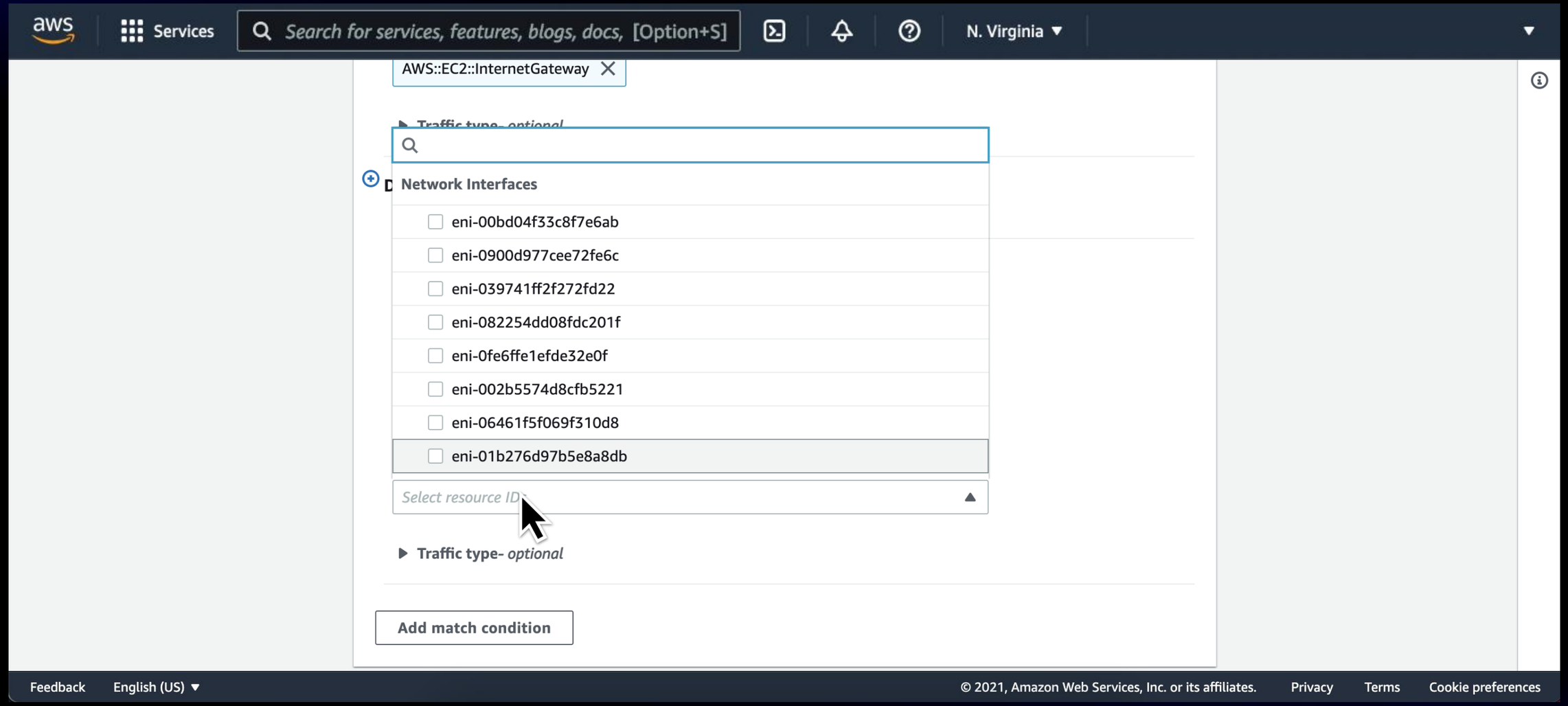
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



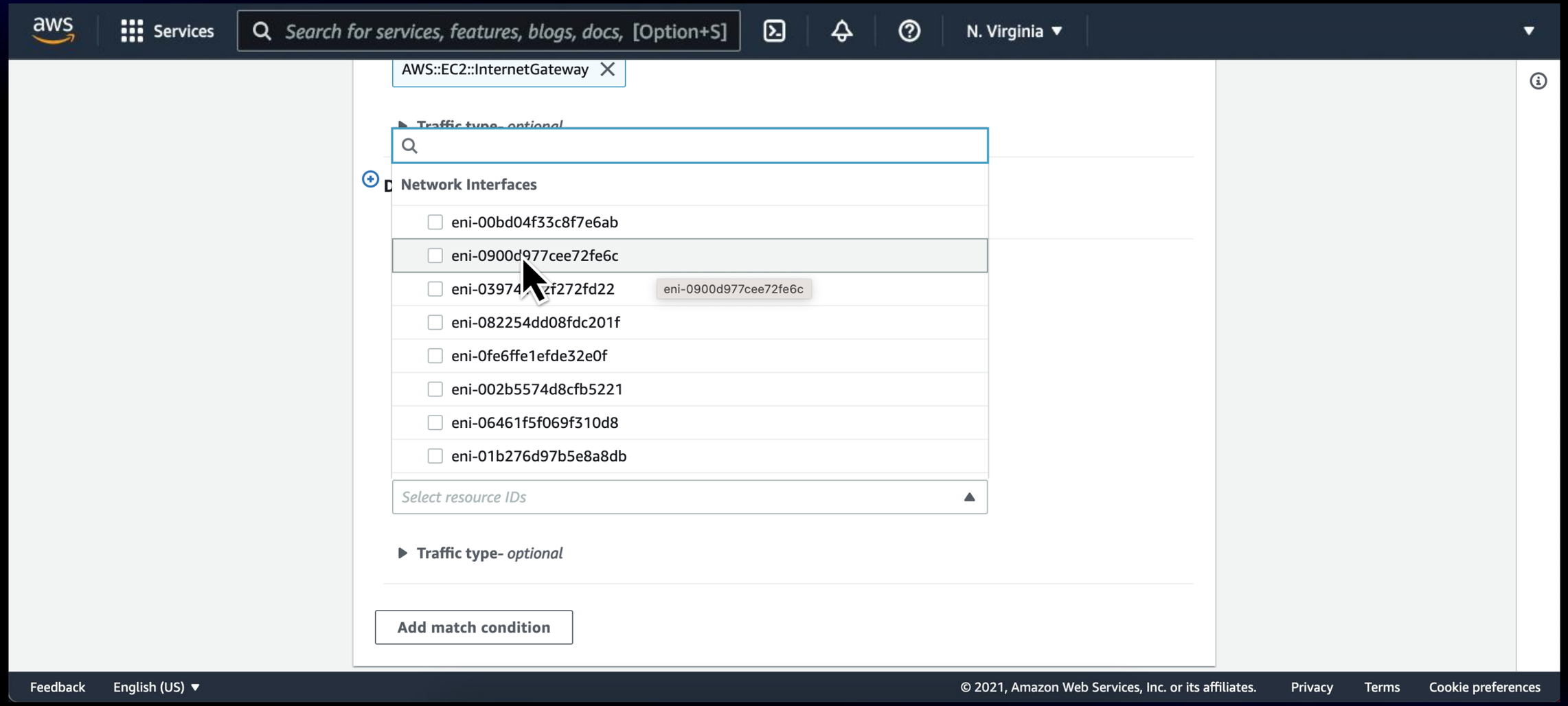
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



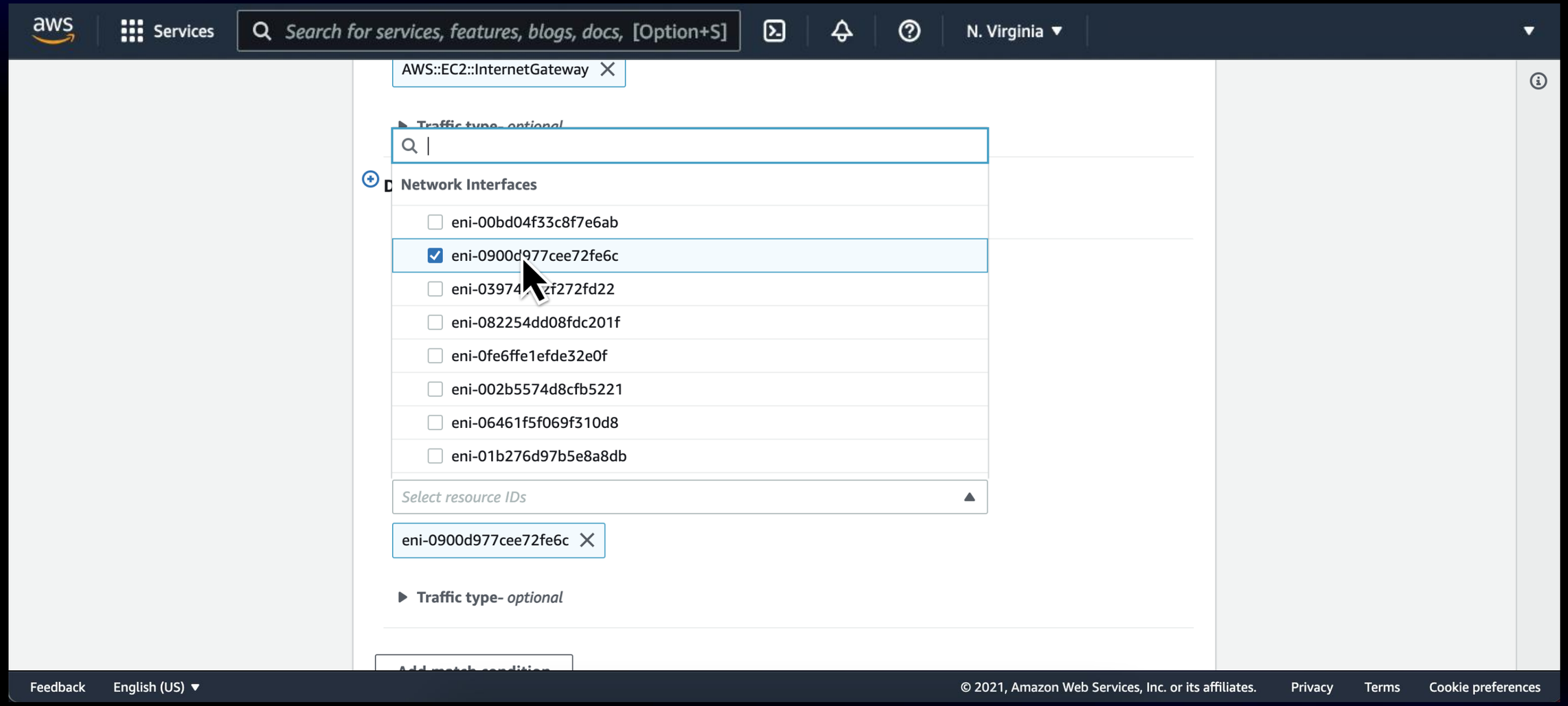
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



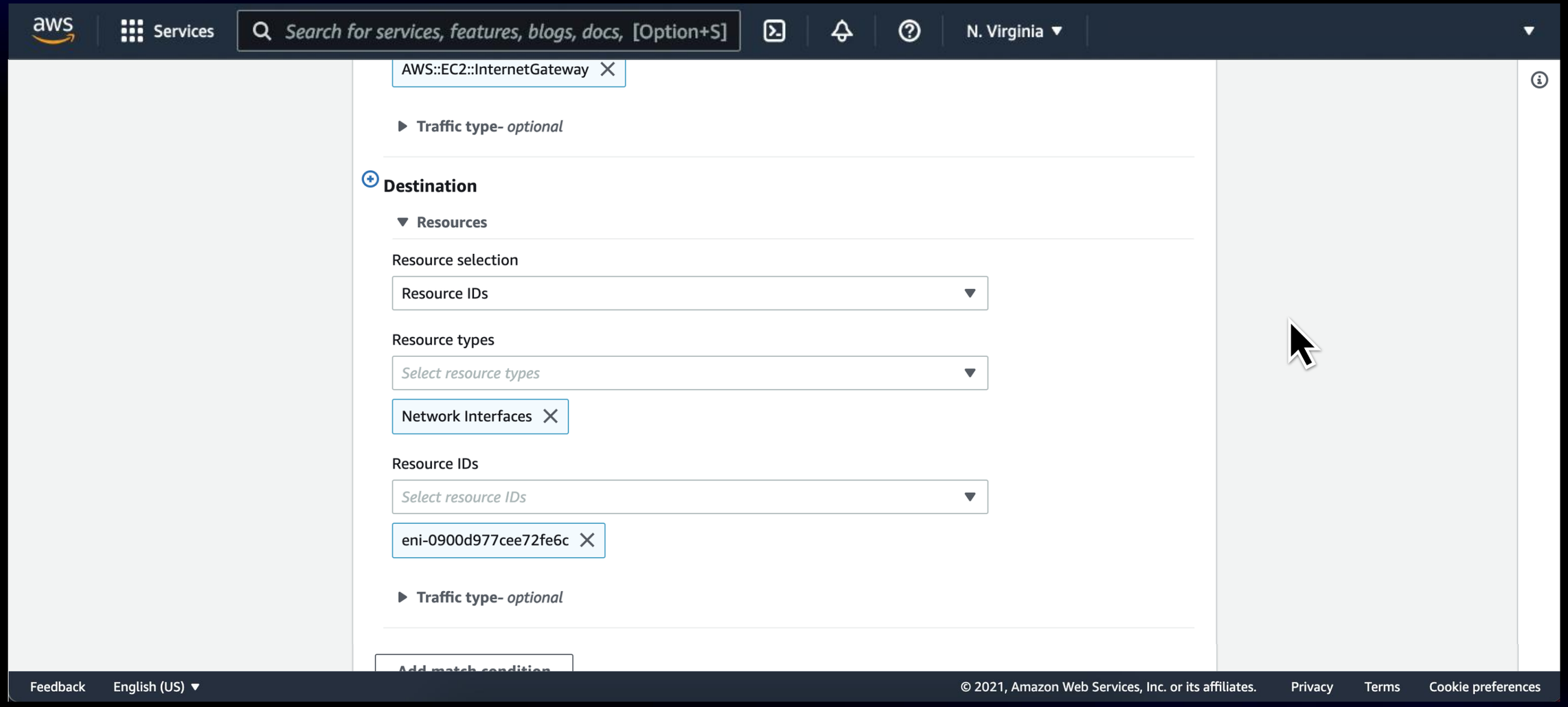
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



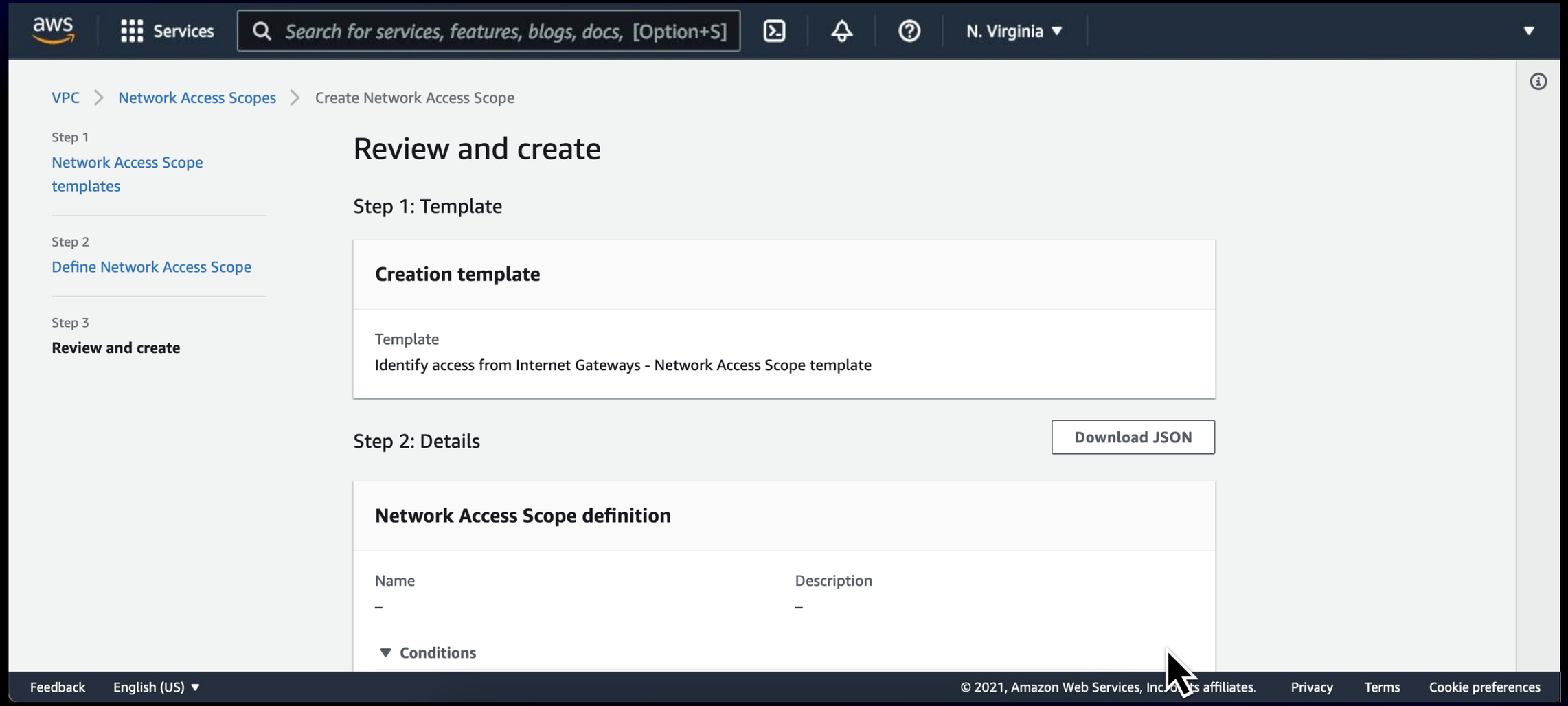
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



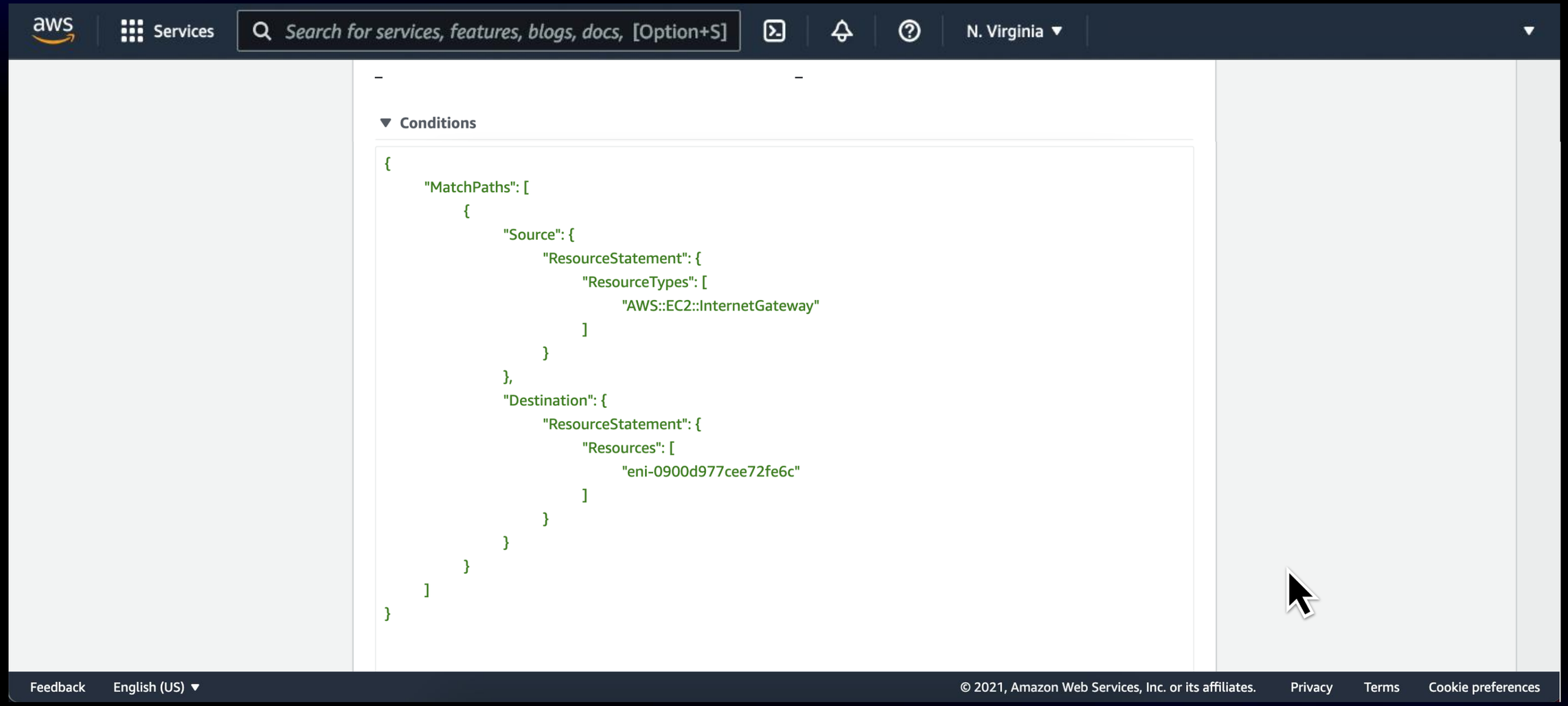
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



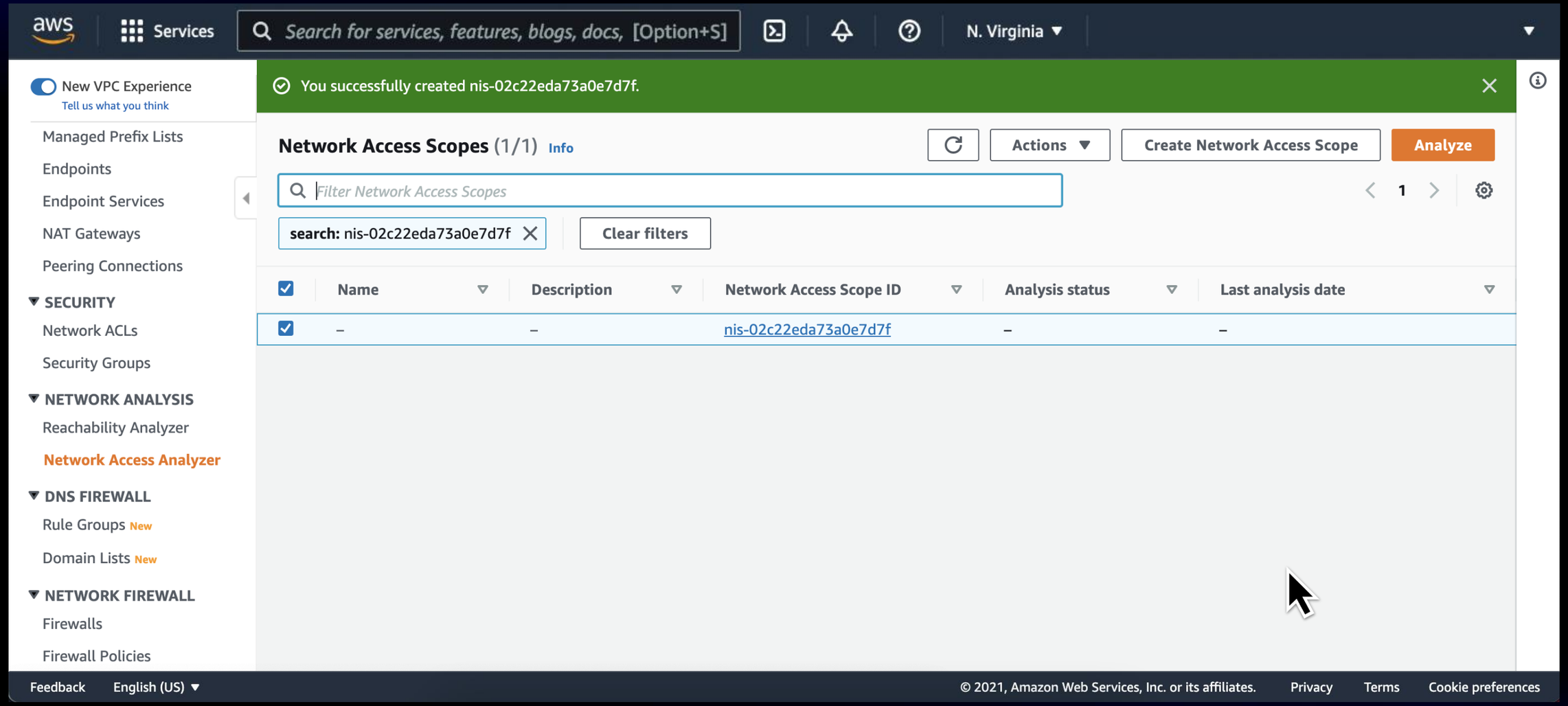
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



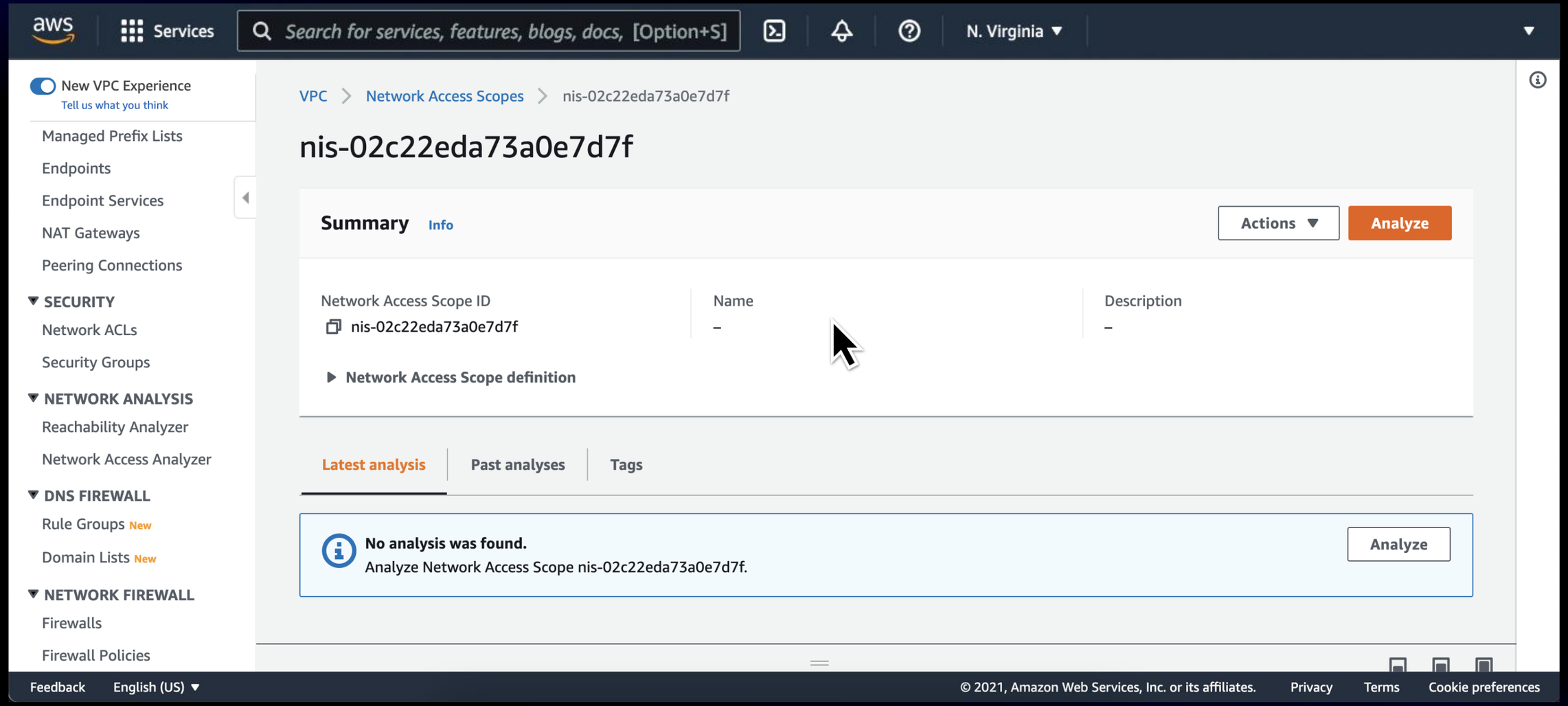
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



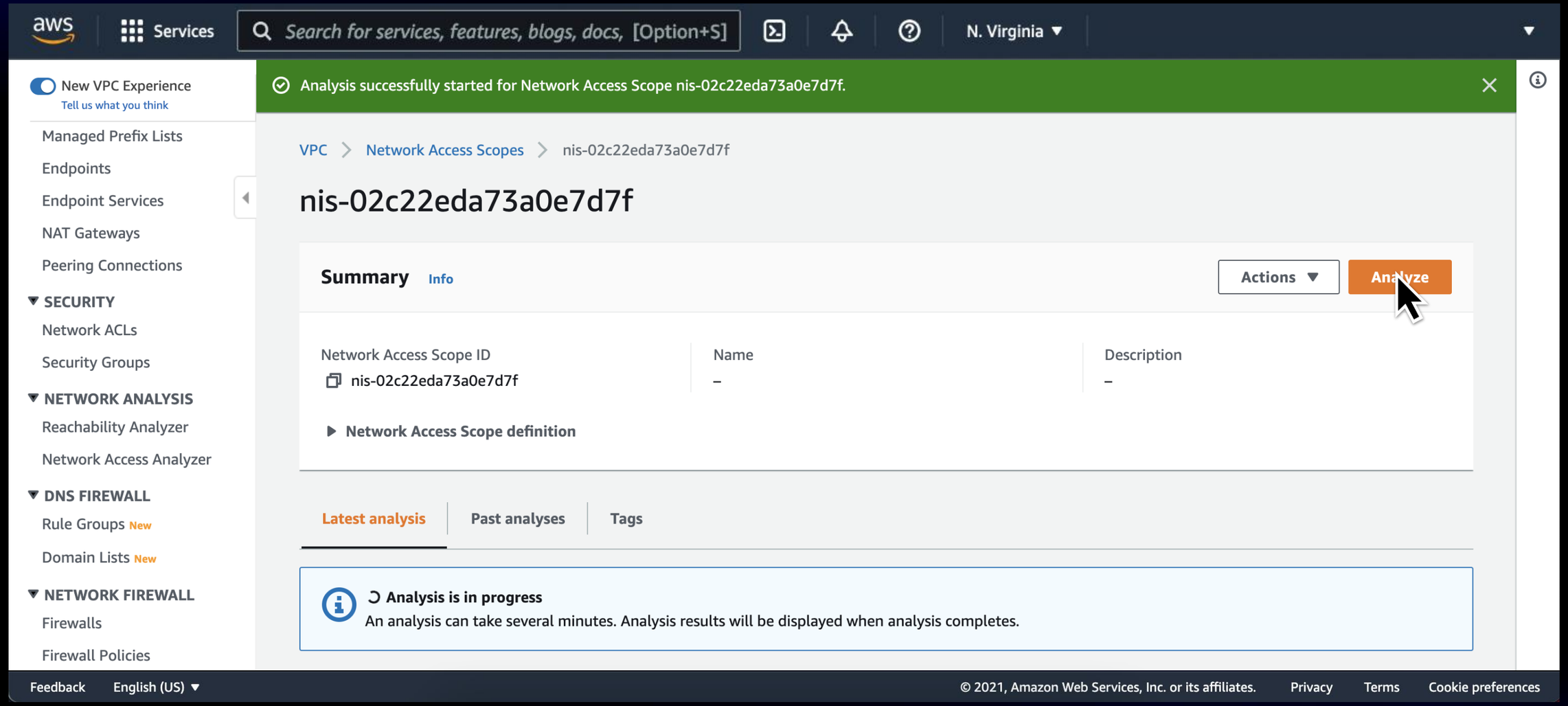
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



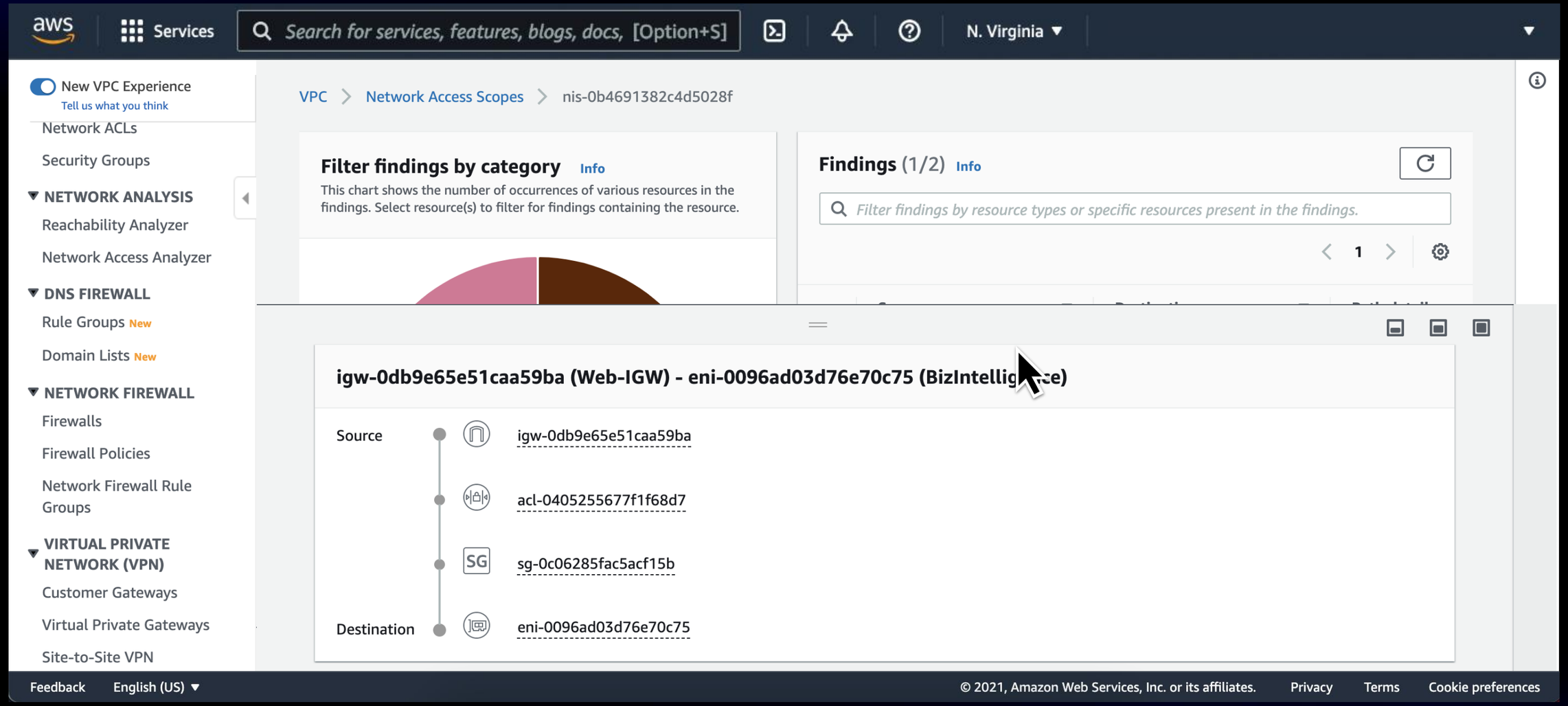
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Network Access Analyzer



https://go.aws/3ojoabk

Amazon VPC Network Access Analyzer

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring and visibility

Network Access Analyzer
Discover and validate network paths

VPC Reachability Analyzer
Troubleshoot connectivity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Reachability Analyzer

VERIFY REACHABILITY CONFIGURATION



Troubleshoot connectivity issues caused by network misconfiguration



Verify that your network configuration matches your intended connectivity

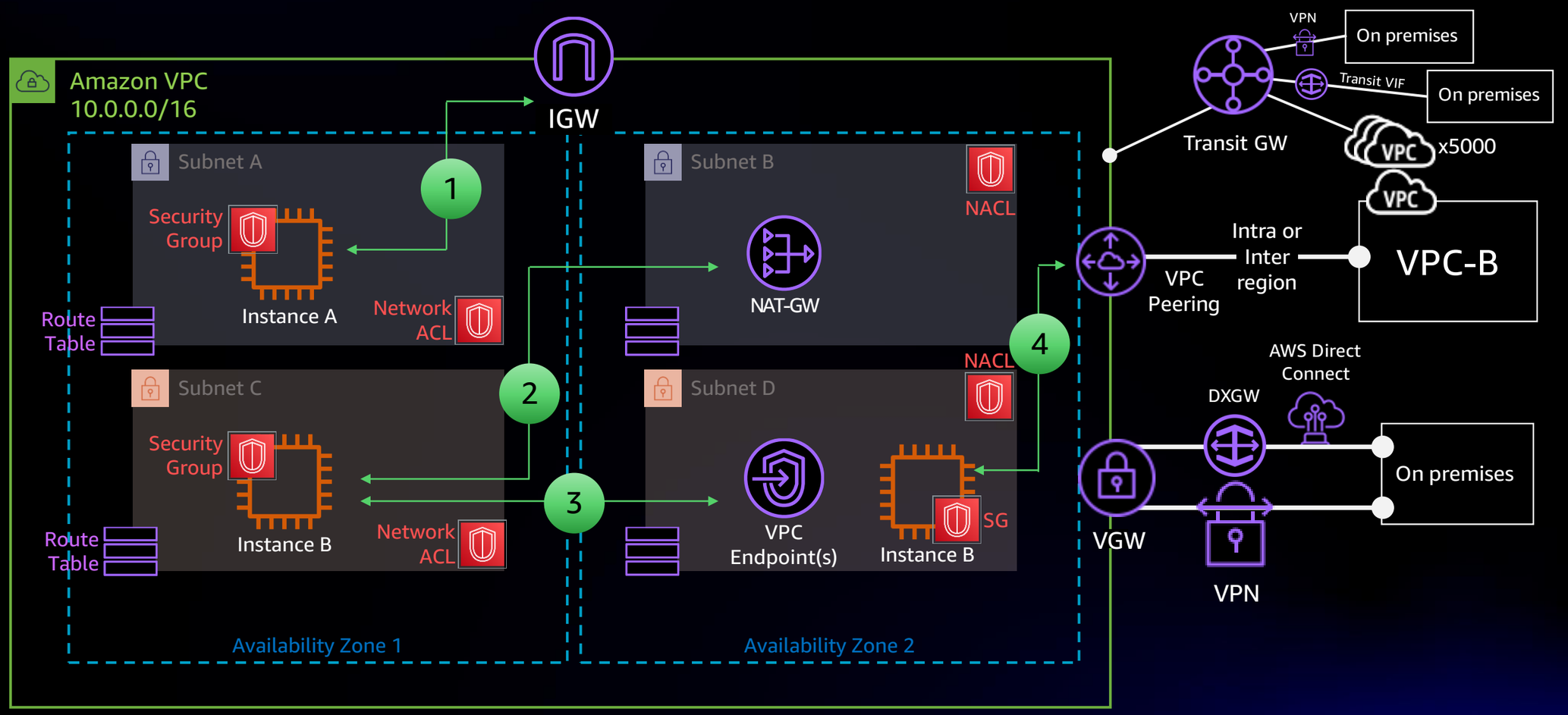


Automate the verification of your connectivity intent as your network configuration changes

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Reachability Analyzer

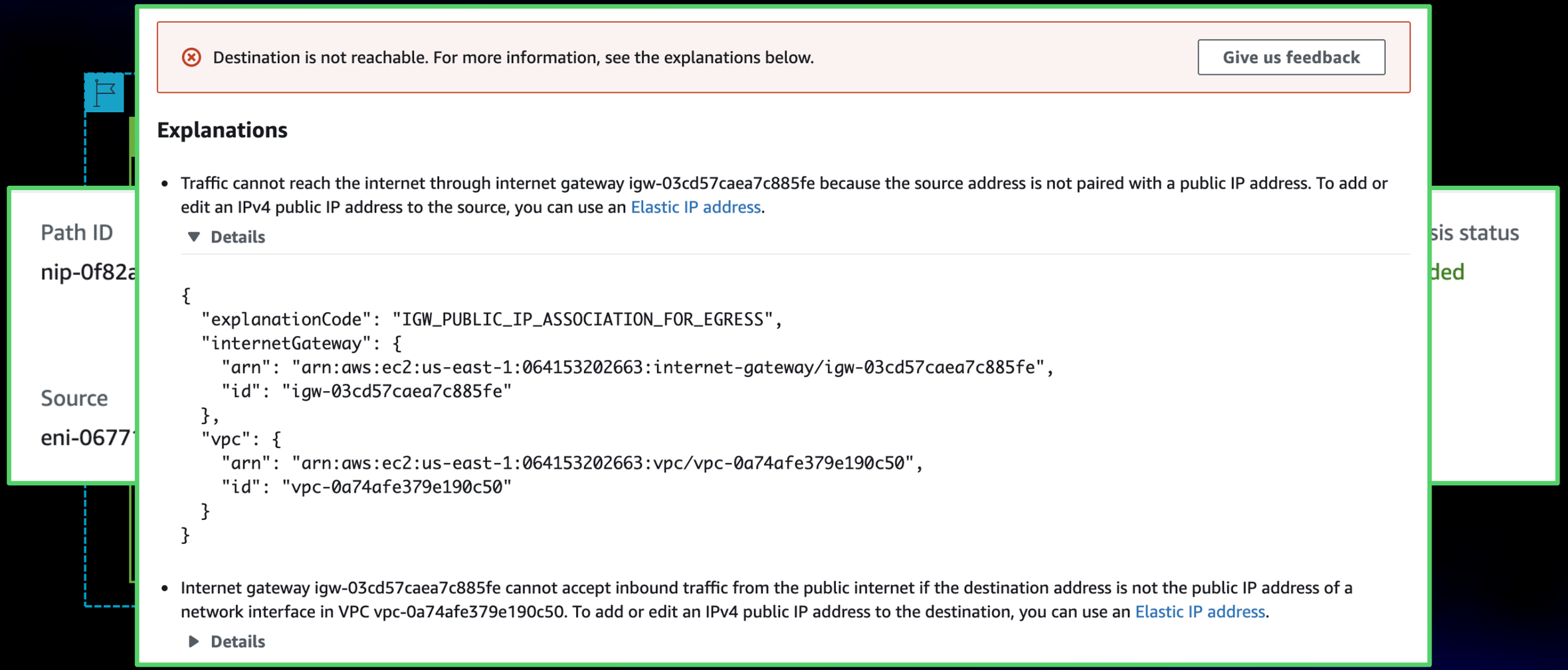
TROUBLESHOOT NETWORK REACHABILITY



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Reachability Analyzer

TROUBLESHOOT NETWORK REACHABILITY



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Reachability Analyzer

SCAN ME

https://go.aws/3ojoabk

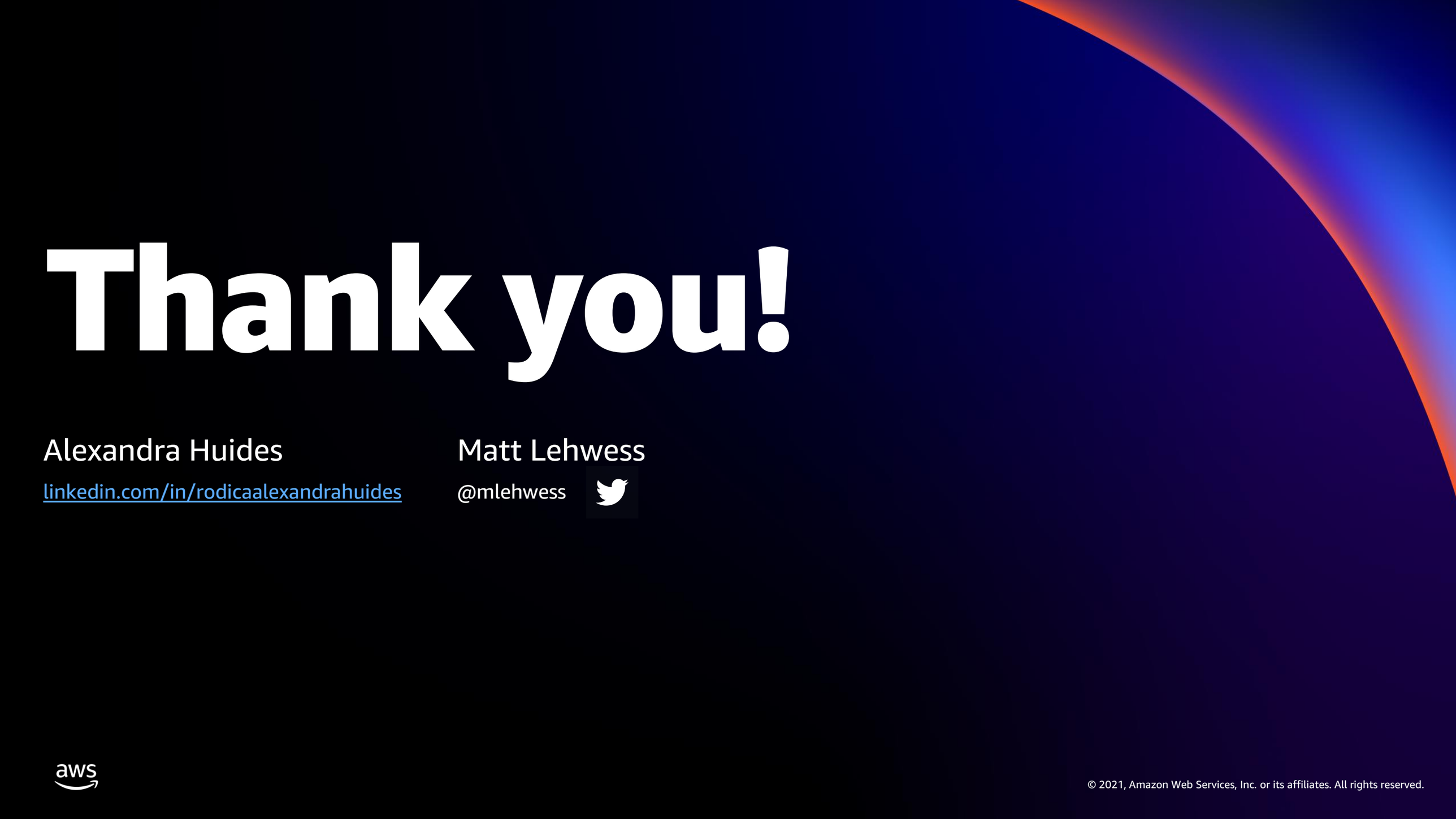
Introducing Amazon VPC Reachability Analyzer

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Alexandra Huides
linkedin.com/in/rodicaalexandrahuides

Matt Lehwess
@mlehwess



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.