AWS re:Invent

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

NET205-R2

How to build scalable hybrid connectivity architectures

Alexandra Huides

Senior Solutions Architect – Networking Specialist
AWS

Nicola Arnoldi

Senior Solutions Architect
AWS

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

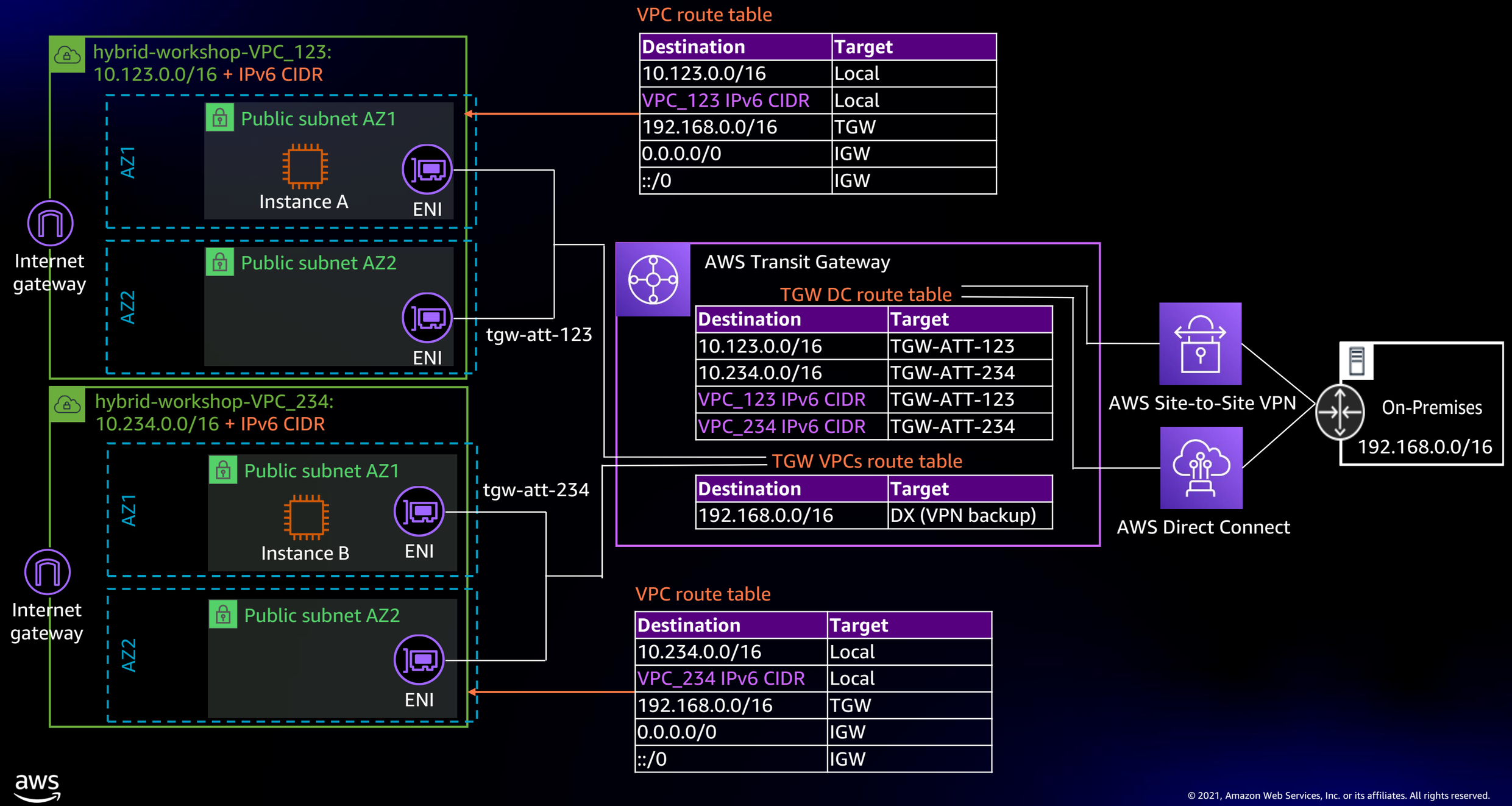
Agenda

- What are we building today
- Dual stack Amazon VPC design
- Hybrid VPC connectivity at scale
- AWS Transit Gateway and AWS Direct Connect review
- DNS in the hybrid connectivity context
- Start building

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

What are we building today

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



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

Amazon VPC capabilities

- Subnets and Availability Zones
- Enabling dual stack IPv6 operation
- VPC routing
- VPC DNS

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

Amazon VPC capabilities

Subnets and Availability Zones

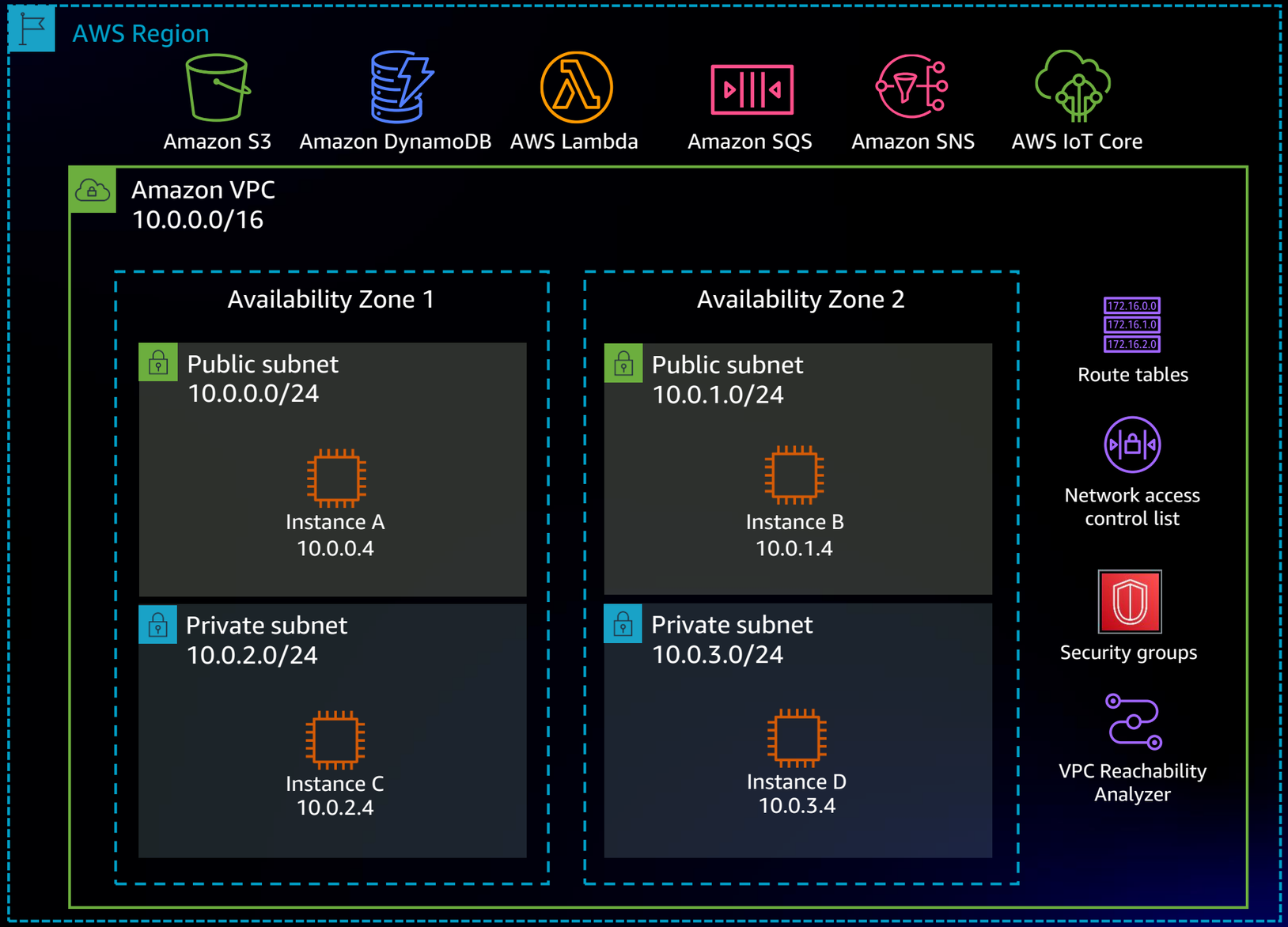
Enabling dual stack IPv6 operation

VPC routing

VPC DNS

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

VPC subnets and Availability Zones



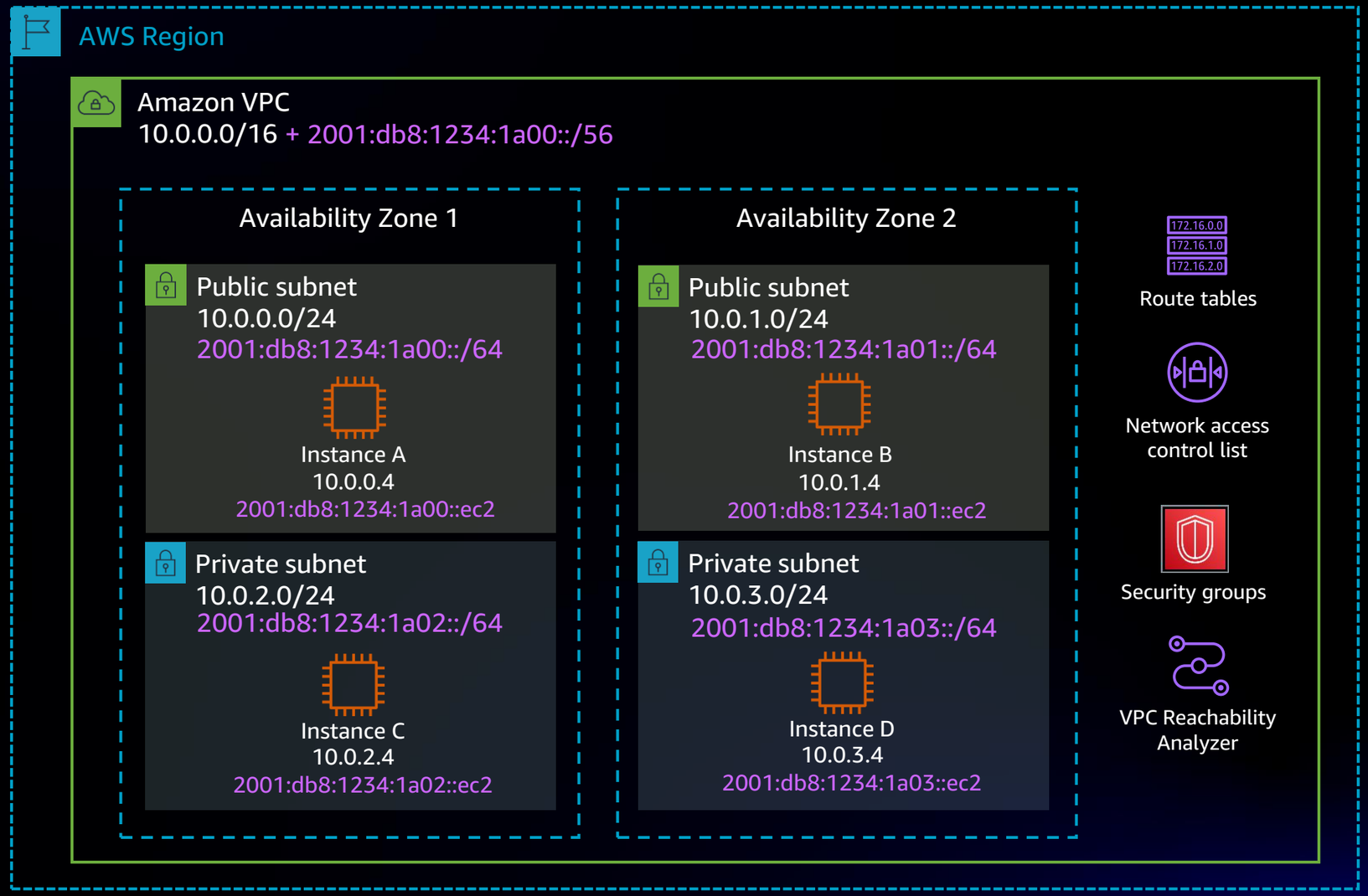
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC capabilities

- Subnets and Availability Zones
- **Enabling dual stack IPv6 operation**
- VPC routing
- VPC DNS

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

Adding IPv6 to your VPC



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

Amazon VPC capabilities

Subnets and Availability Zones

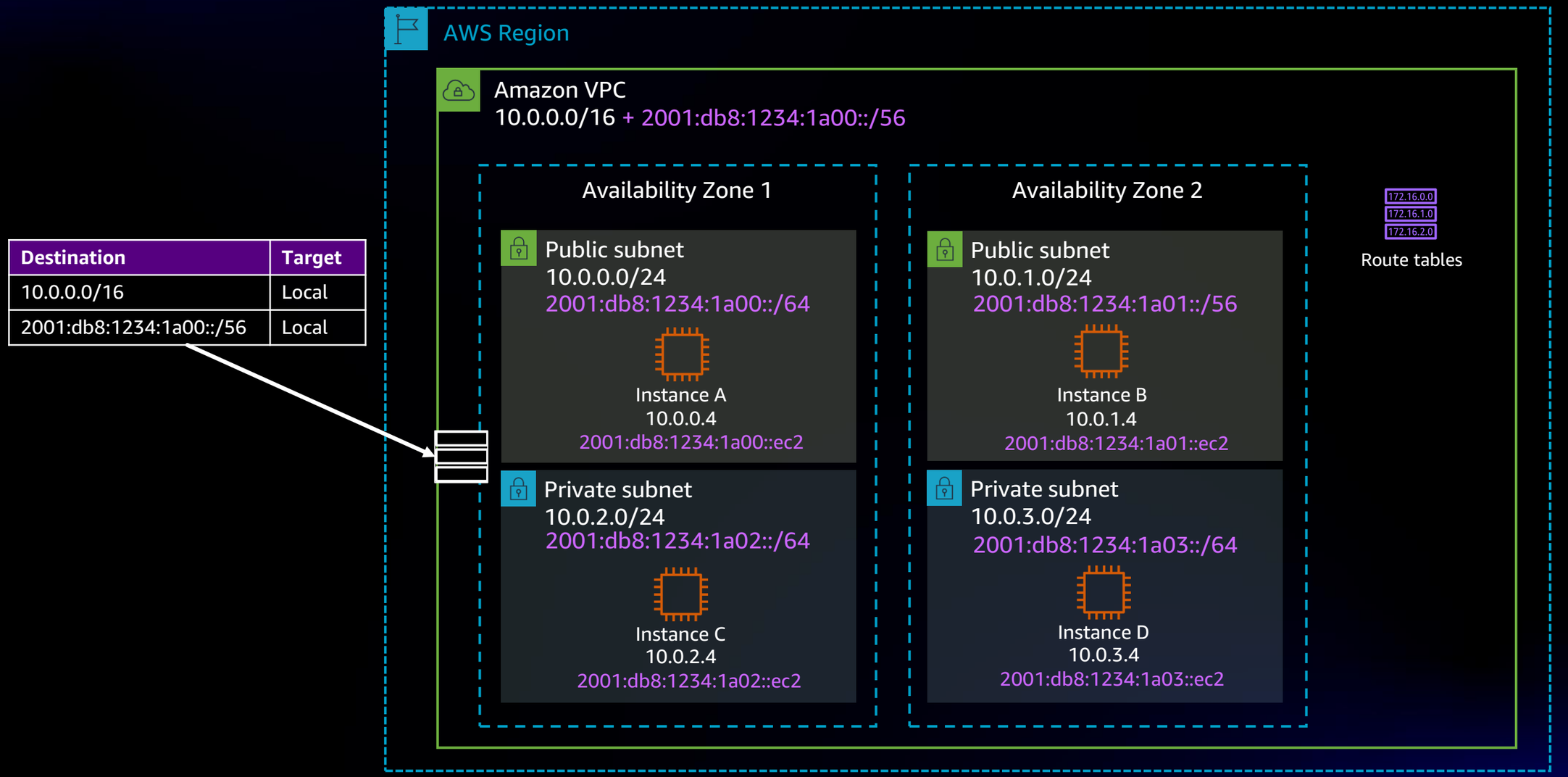
Enabling dual stack IPv6 operation

VPC routing

VPC DNS

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

VPC routing



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

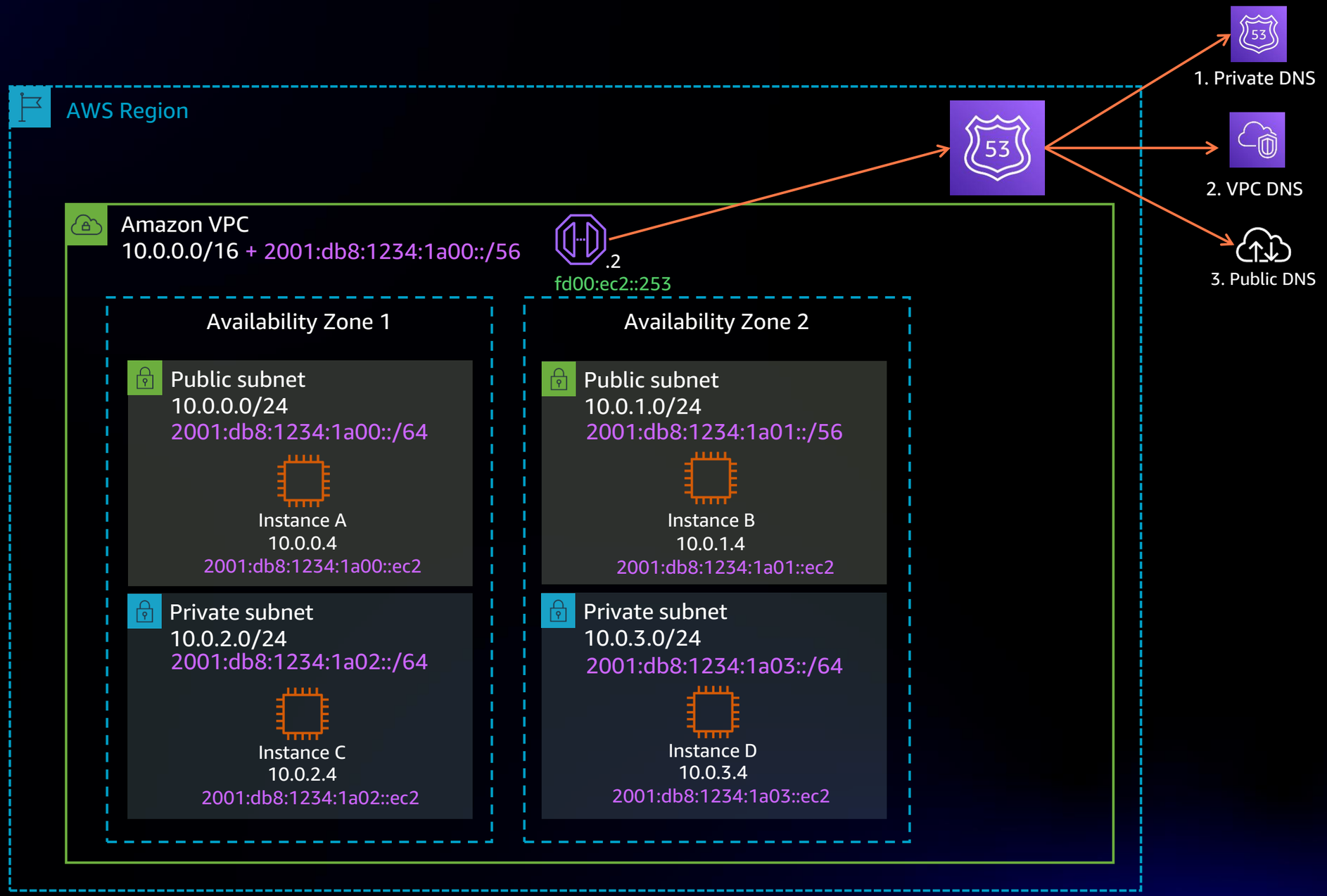
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC capabilities

- Subnets and Availability Zones
- Enabling dual stack IPv6 operation
- VPC routing
- **VPC DNS**

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

VPC DNS



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

VPC connectivity options

To the Internet

To other VPCs

To on-premises networks

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

VPC connectivity options

To the Internet

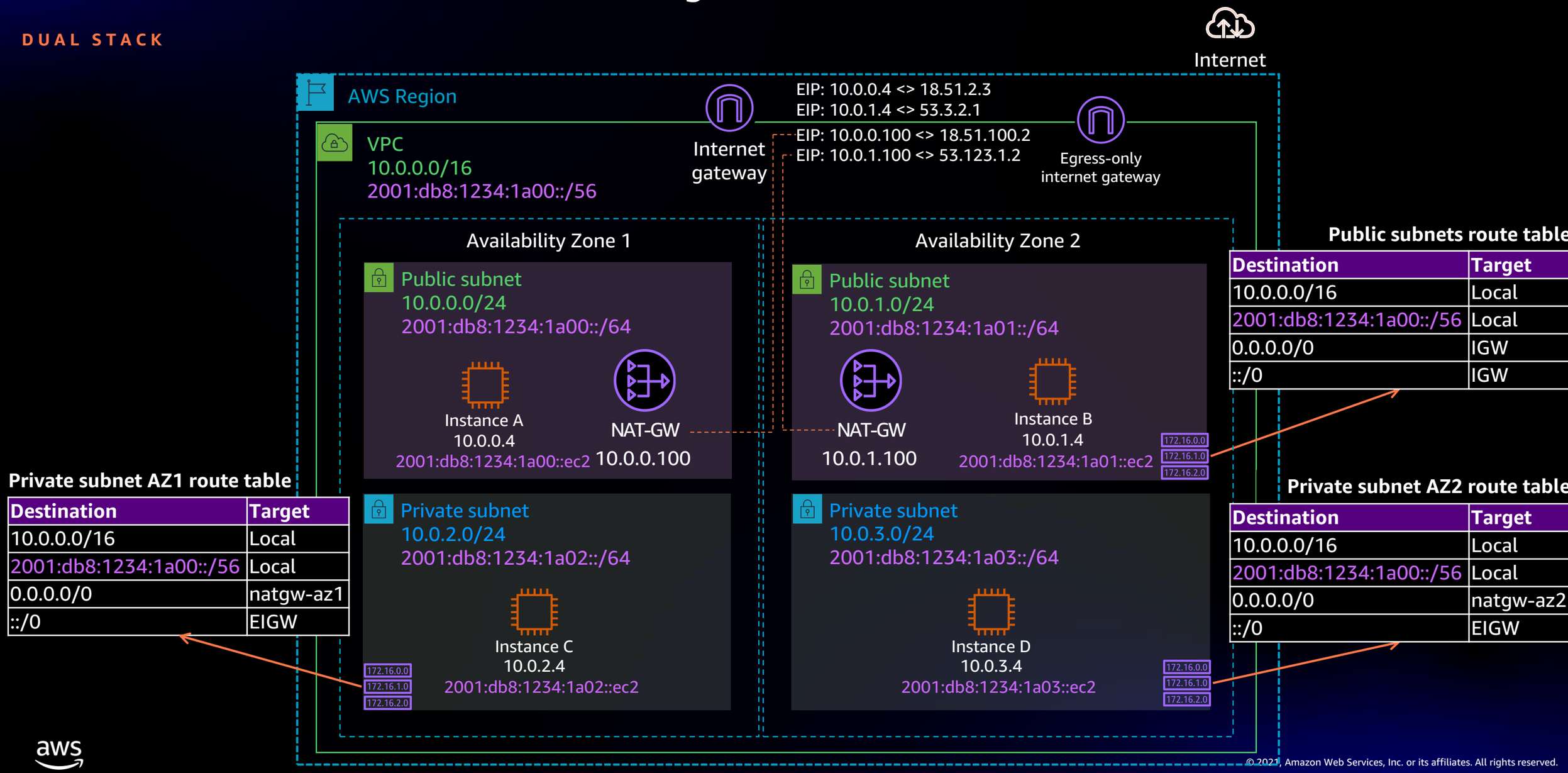
To other VPCs

To on-premises networks

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

VPC internet connectivity

DUAL STACK



Public subnets route table

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

Private subnet AZ1 route table

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	natgw-az1
::/0	EIGW

Private subnet AZ2 route table

Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	natgw-az2
::/0	EIGW

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

VPC connectivity options

To the Internet

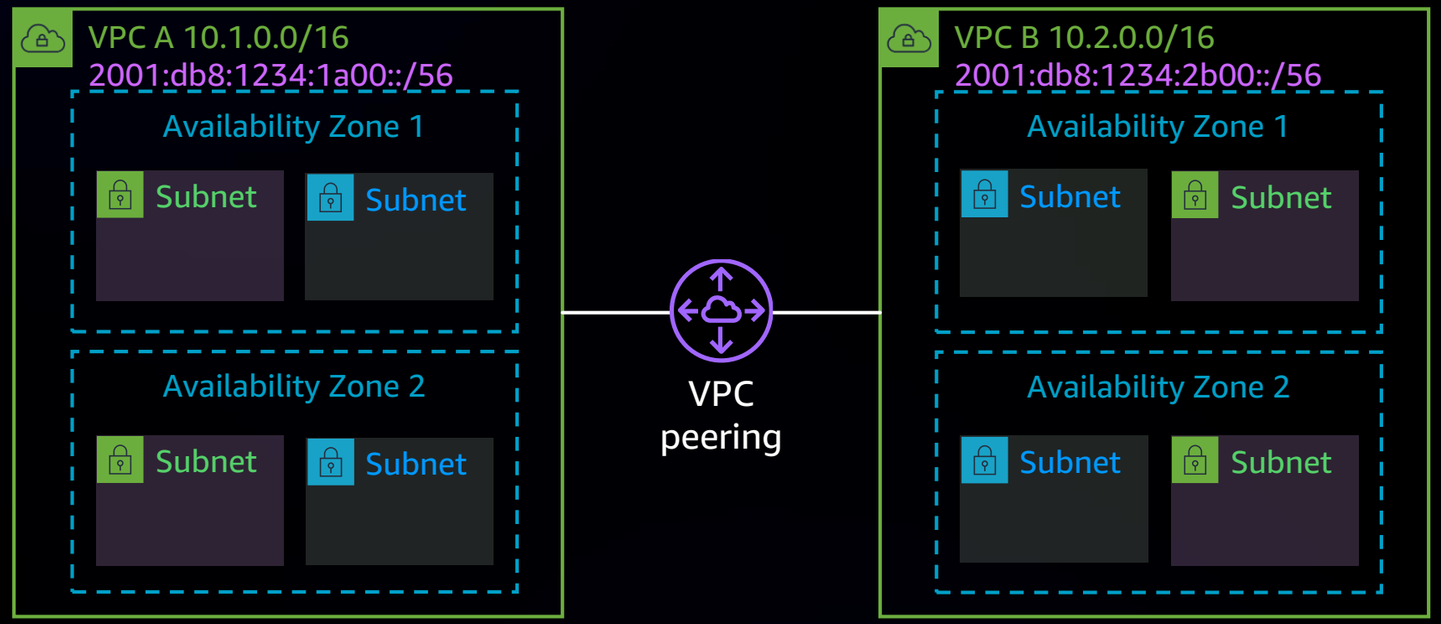
To other VPCs

To on-premises networks

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

Dual stack VPC-to-VPC connectivity

VPC PEERING



VPC A route table

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

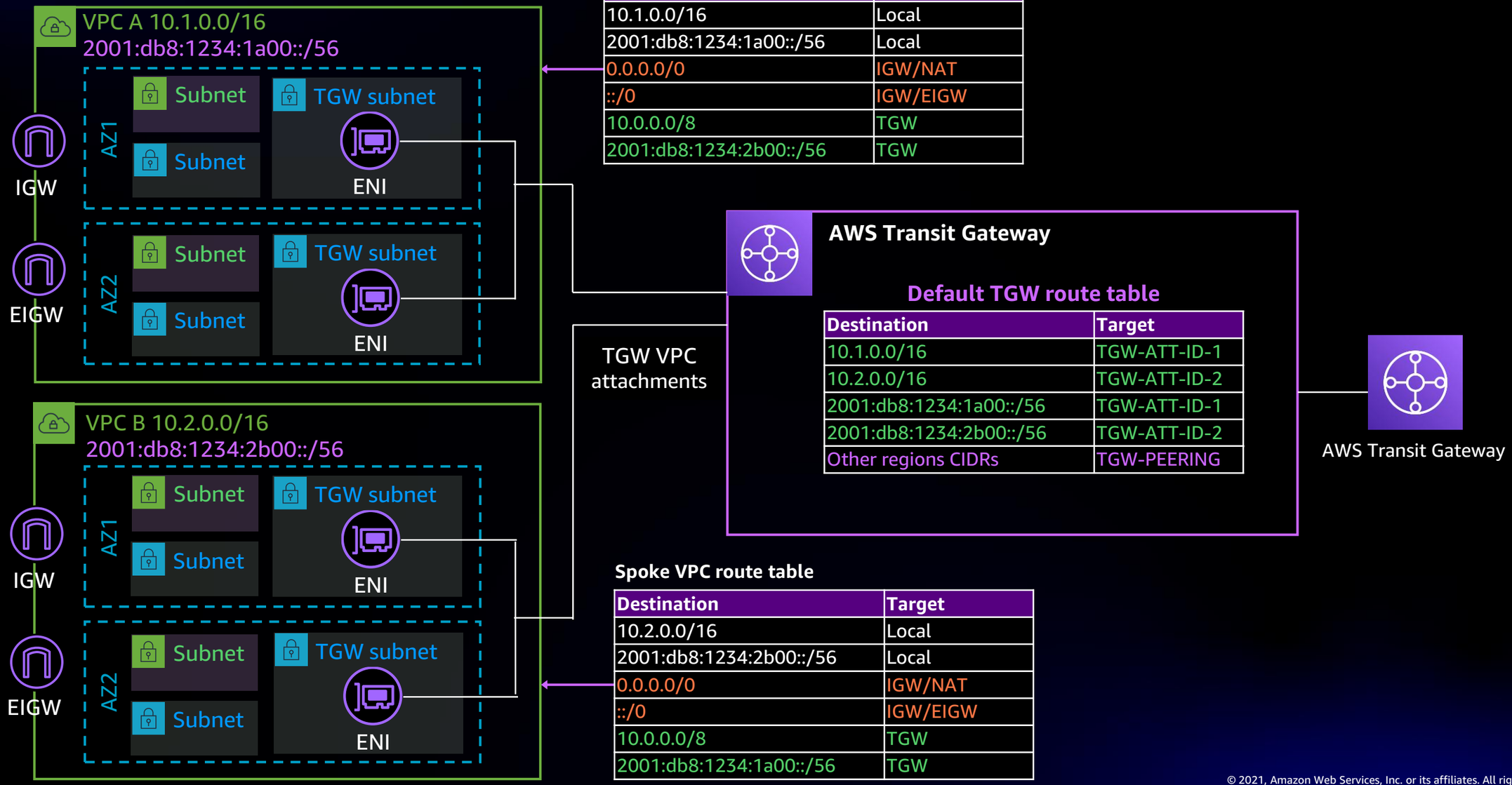
VPC B route table

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

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

Dual stack VPC-to-VPC connectivity at scale

AWS TRANSIT GATEWAY



Spoke VPC route table

Destination	Target
10.1.0.0/16	Local
2001:db8:1234:1a00::/56	Local
0.0.0.0/0	IGW/NAT
::/0	IGW/EIGW
10.0.0.0/8	TGW
2001:db8:1234:2b00::/56	TGW

Default TGW route table

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

Spoke VPC route table

Destination	Target
10.2.0.0/16	Local
2001:db8:1234:2b00::/56	Local
0.0.0.0/0	IGW/NAT
::/0	IGW/EIGW
10.0.0.0/8	TGW
2001:db8:1234:1a00::/56	TGW

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

VPC connectivity options

To the Internet

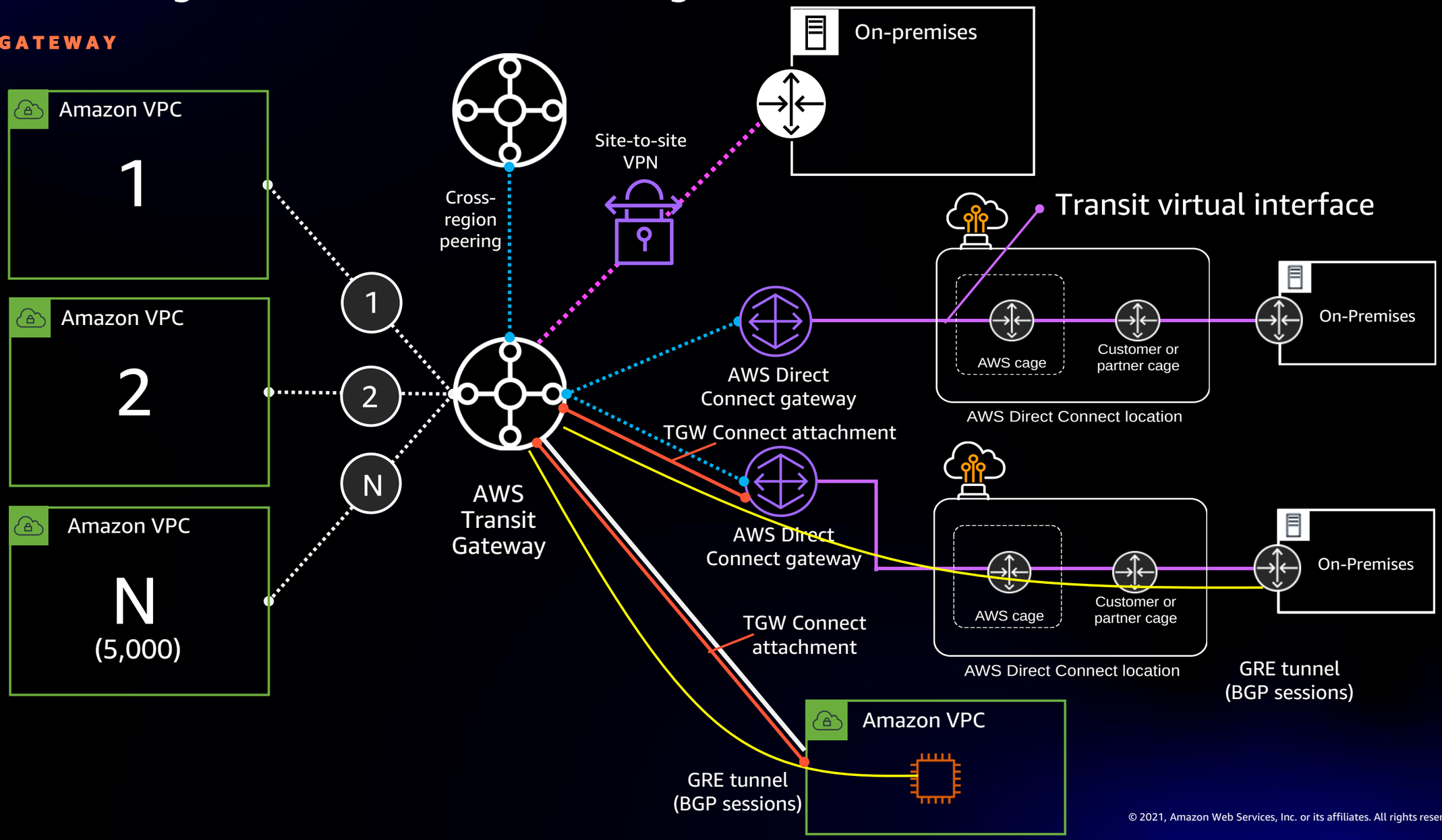
To other VPCs

To on-premises networks

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

Dual stack hybrid connectivity at scale

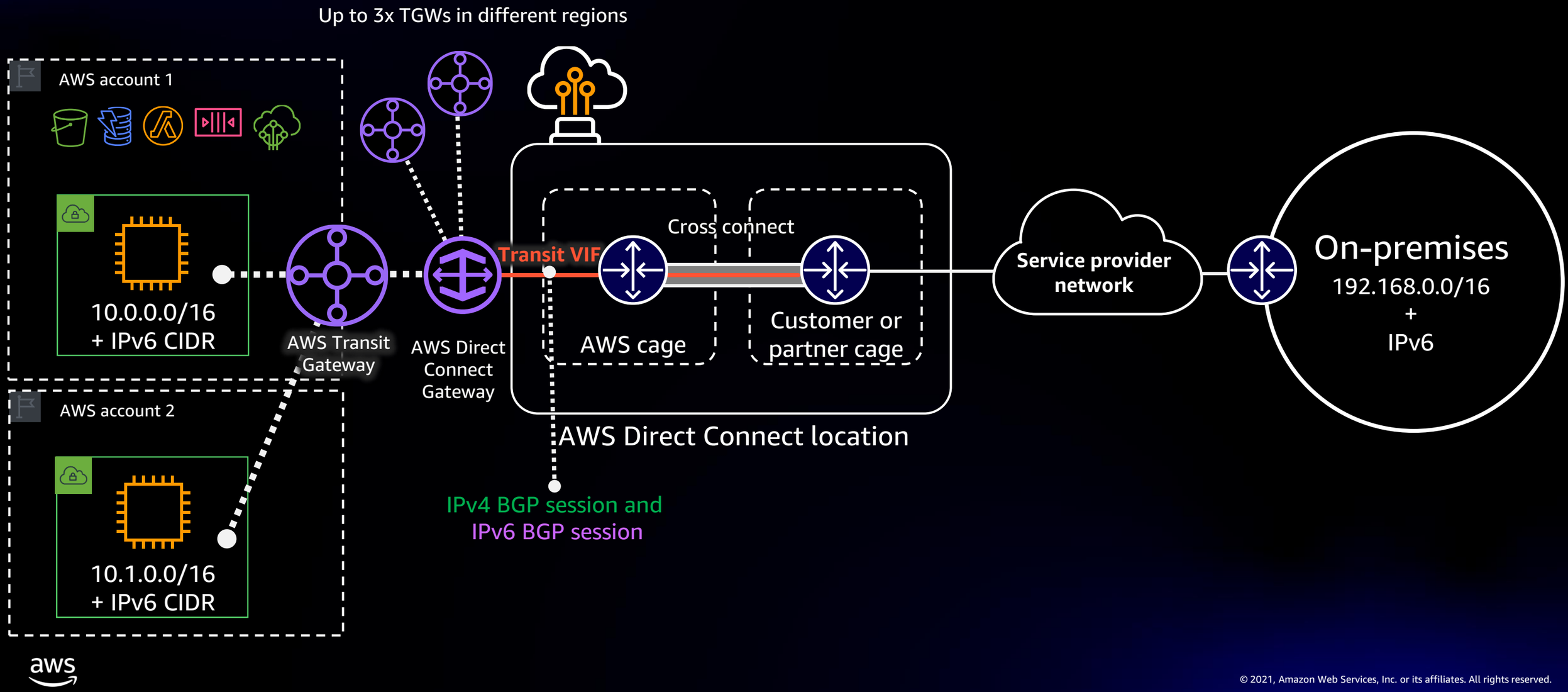
AWS TRANSIT GATEWAY



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

Transit Gateway and Direct Connect

A CLOSER LOOK



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

DNS in AWS and hybrid networks

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

DNS in a hybrid network



Inbound resolver endpoints

Managed DNS resolver service from Amazon Route 53



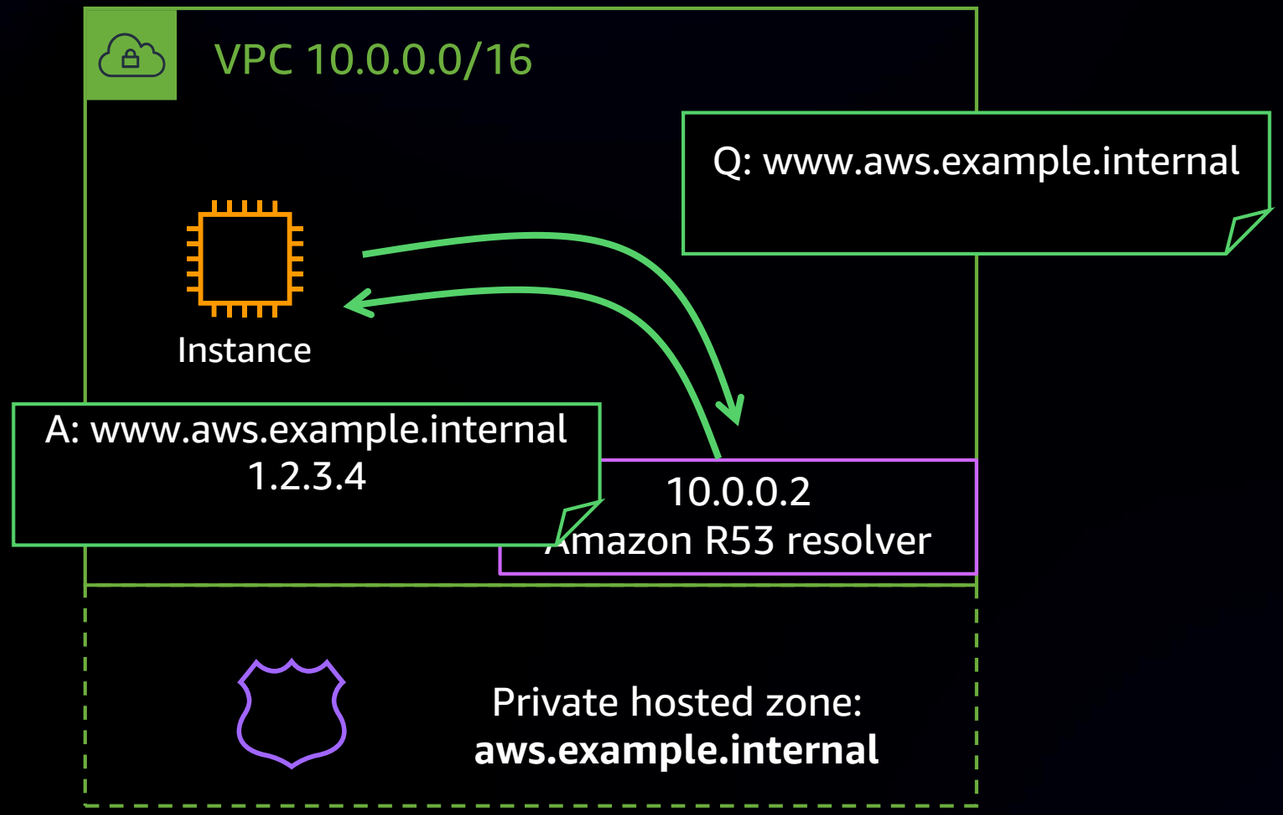
Outbound resolver endpoints

Provides hybrid DNS resolution over AWS Direct Connect and managed VPN

Makes use of conditional forwarding rules to re-direct query traffic

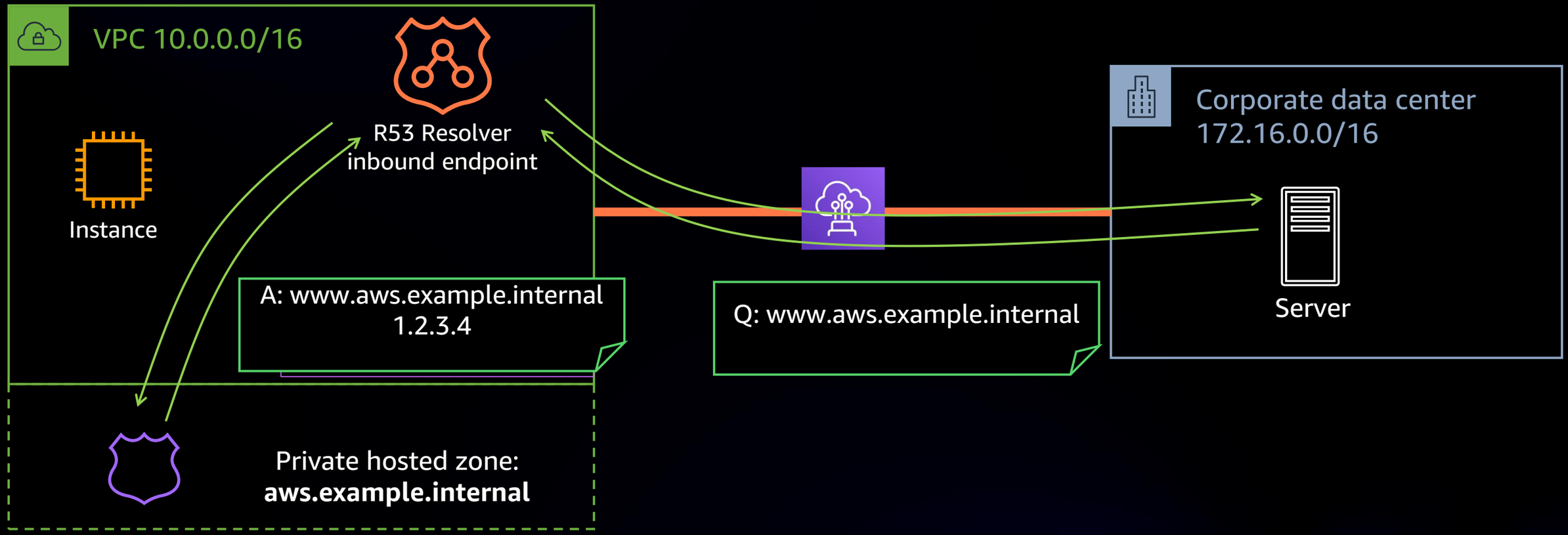
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resolving AWS domains within a VPC



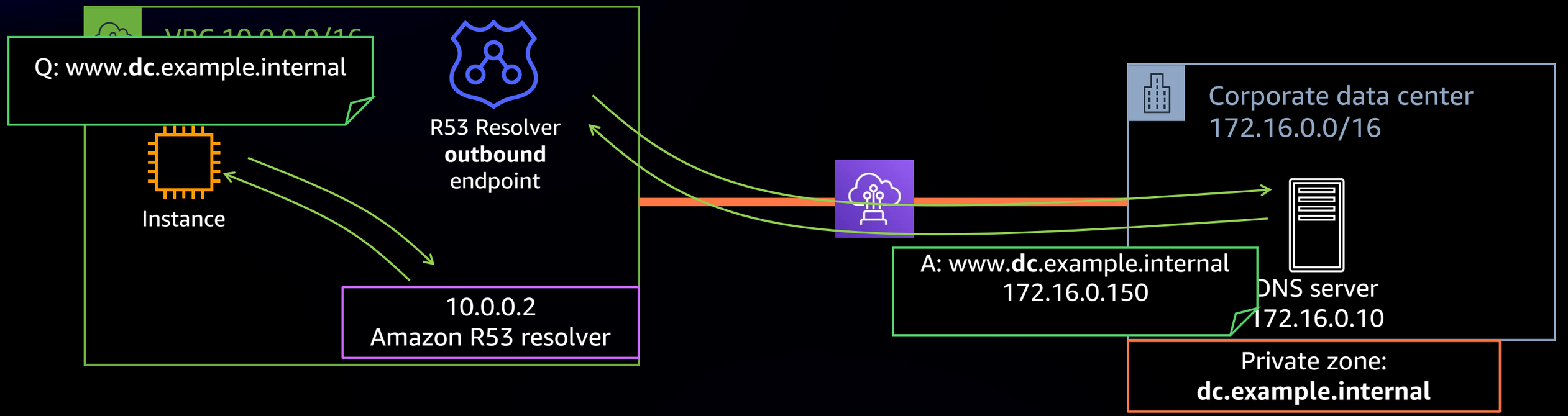
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resolving AWS domains in hybrid networks



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

Resolving on-premises domains in hybrid networks

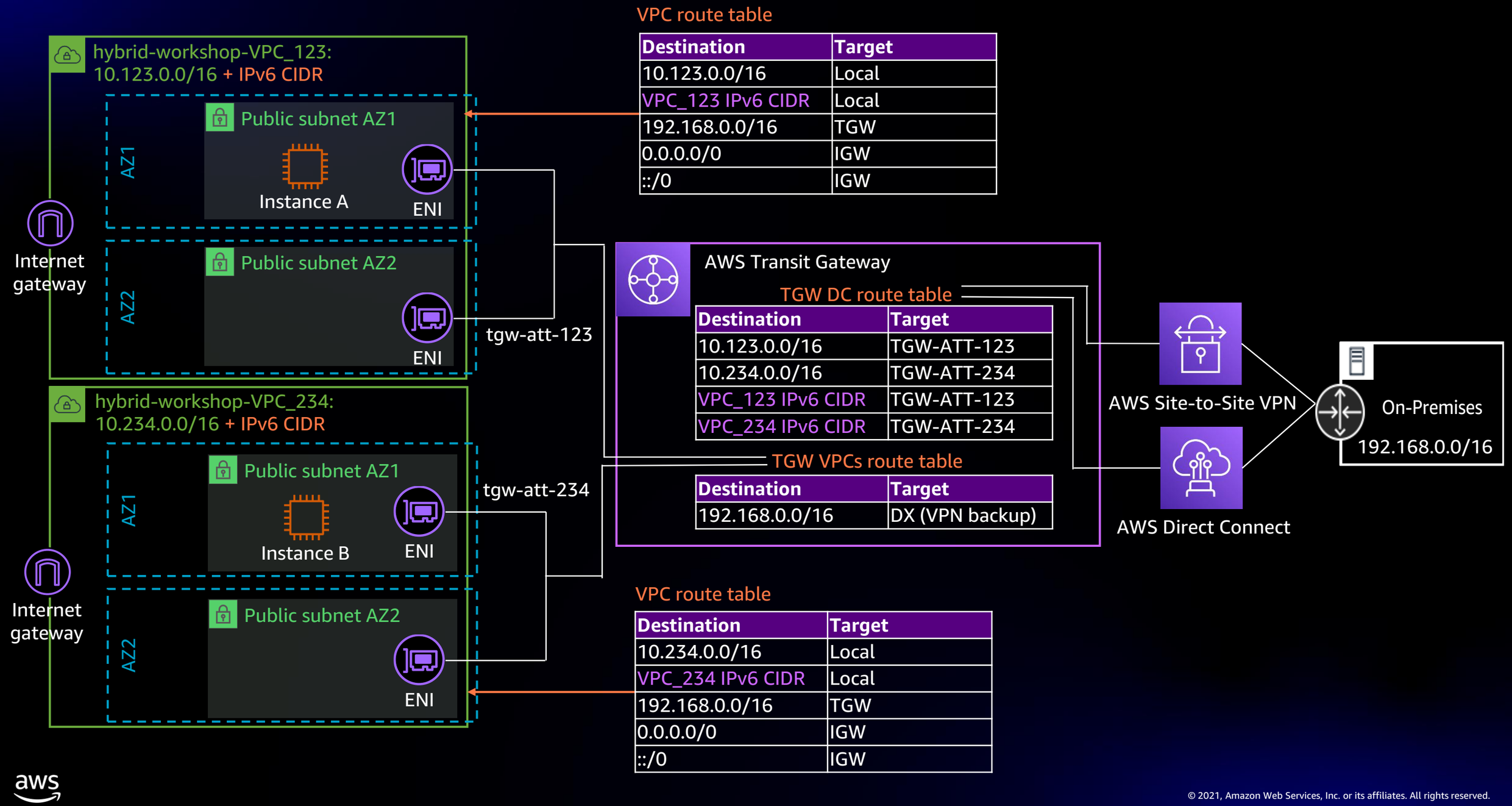


Name	Type	Domain name	IP address	Port
dcRule	Forward	dc.example.internal.	172.16.0.10	53

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

Before we start building...

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



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

Let’s build!

Step 1 - Go to the workshop page

https://workshop.awshybridnetworking.net/

- user: builder/pass: hybridworkshop2021
- instructions & tasks
- DO NOT CHANGE YOUR BROWSER!*



Step 2 - Activate your account

https://dashboard.eventengine.run/login

- Use the event hash you received
- Get console access
- Name your account for easy t-shoot

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

Thank you!

Alexandra Huides
linkedin.com/in/rodicaalexandrahuides

Nicola Arnoldi
linkedin.com/in/nicolaarnoldi

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