AWS re:Invent

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

NET313-R2

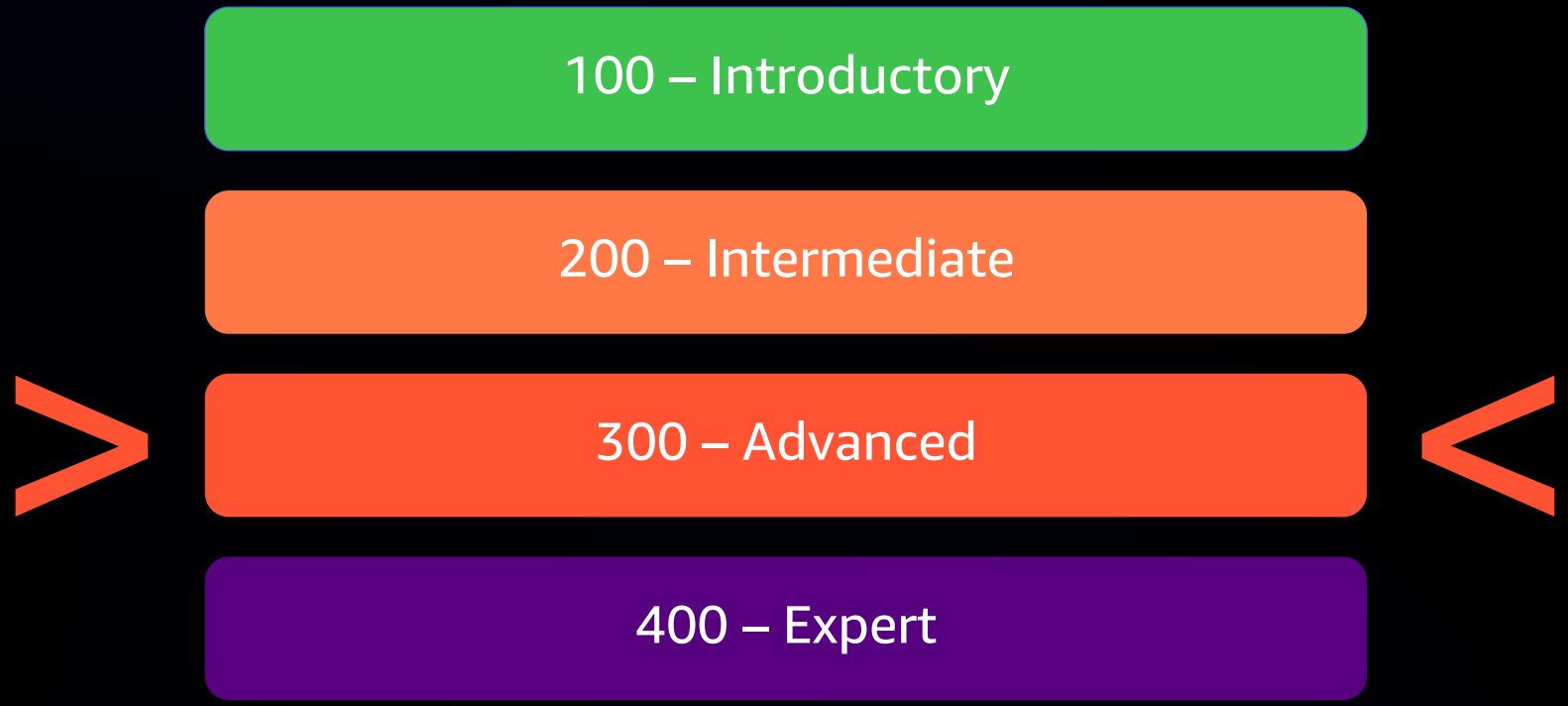
Defining your VPC architecture

Sohaib Tahir
Sr. Solutions Architect, WWPS
AWS

Shirin Bhambhani
Telco Solutions Architect, WWCO
AWS

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

Session level



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

What are we going to cover?

VPC design

Shared VPC

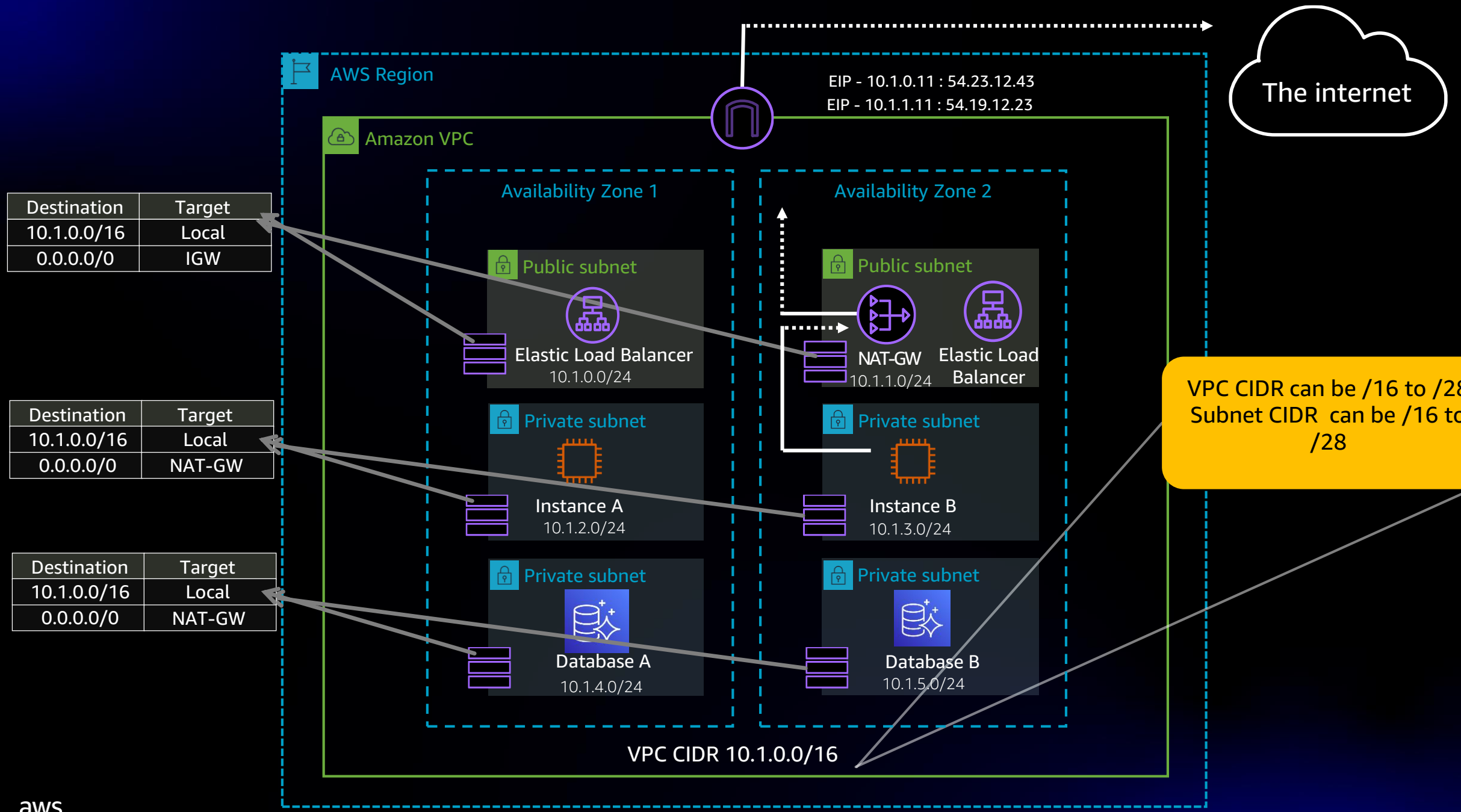
VPC connectivity

Best practices

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

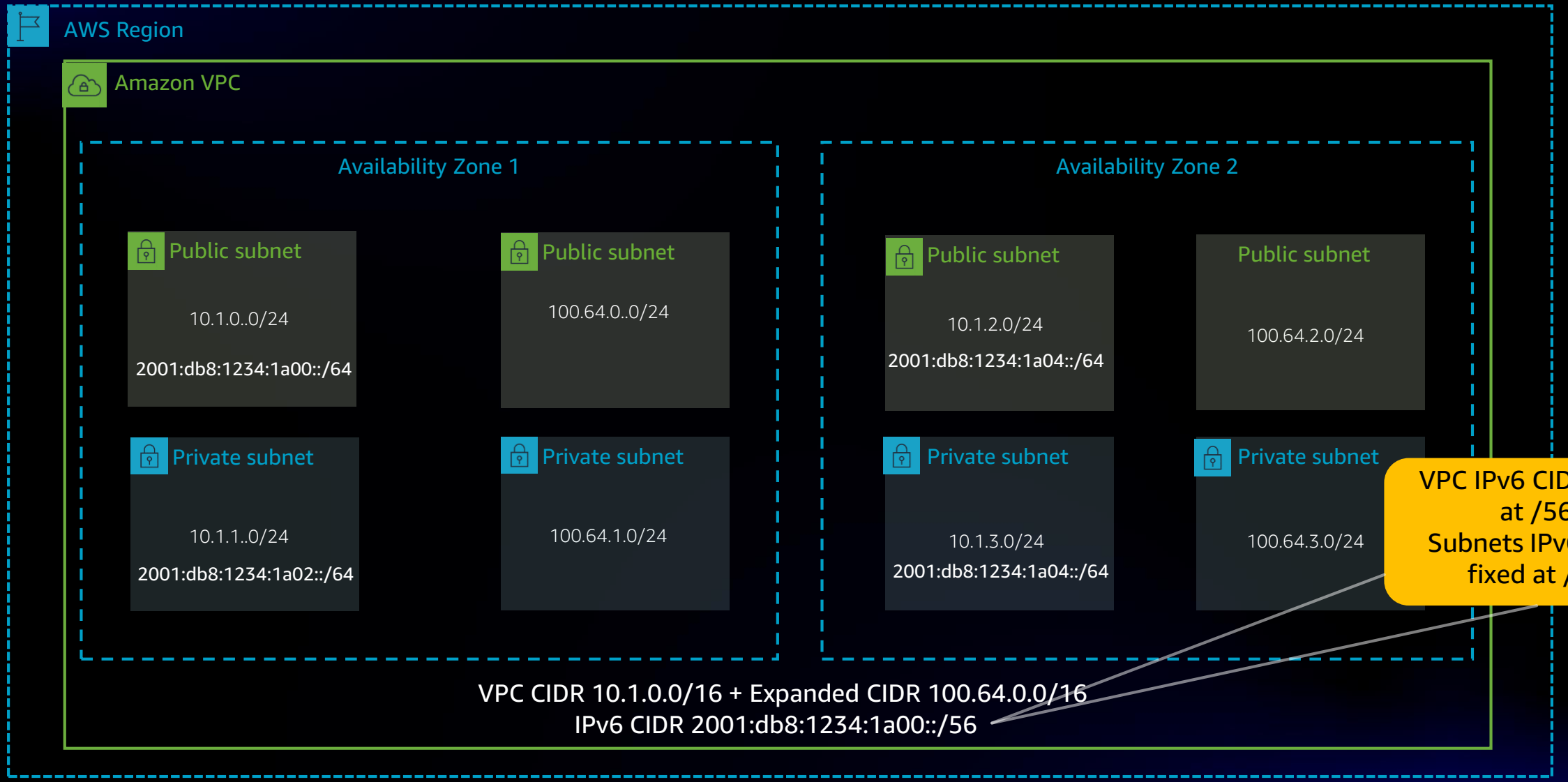
Amazon VPC

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



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

Amazon VPC – Expanded CIDR + Ipv6



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

Shared VPC

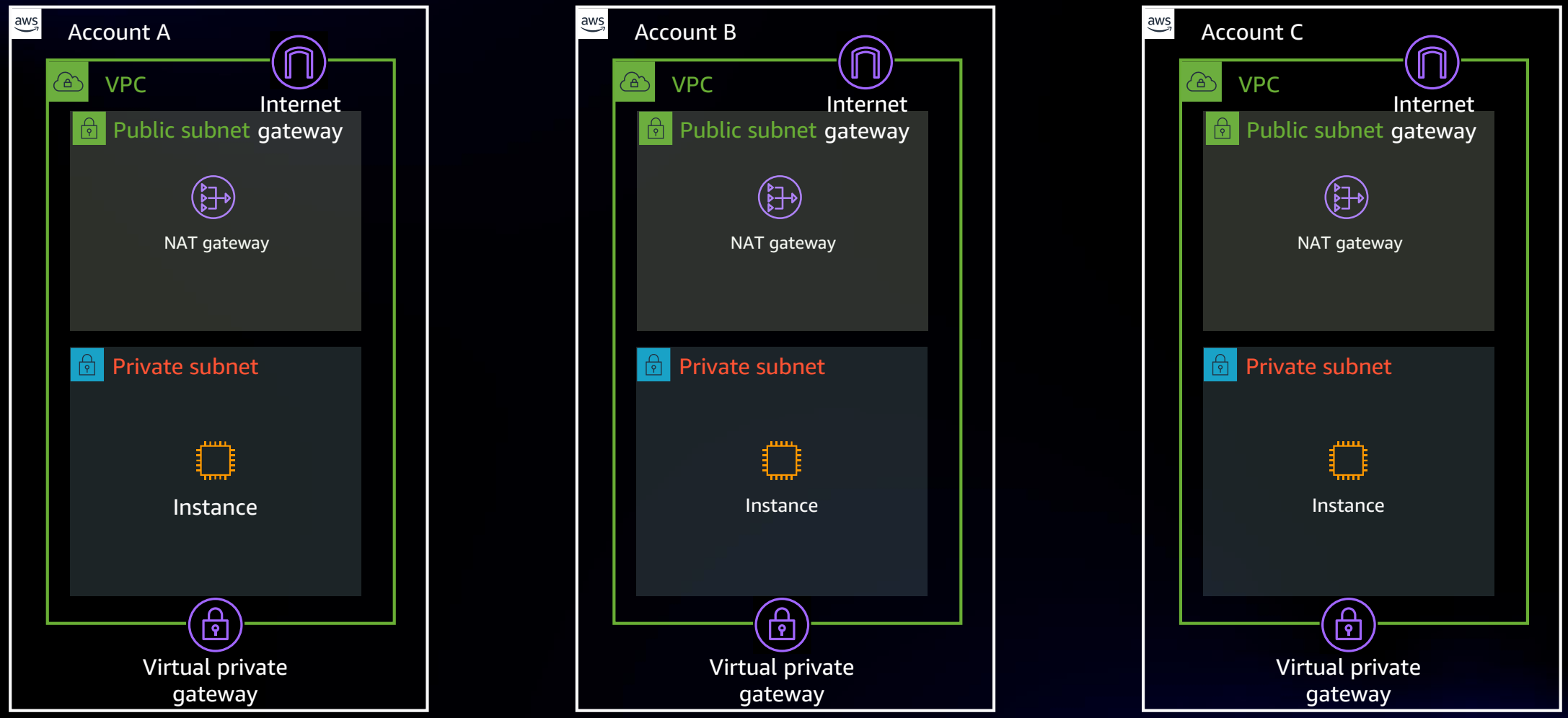
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is VPC sharing ?

VPC sharing is when multiple AWS accounts are allowed to create their resources, such as Amazon EC2 instance, Amazon Relational Database Service (RDS) databases, Amazon Redshift clusters, and AWS Lambda functions, into shared, centrally managed virtual private clouds (VPCs).

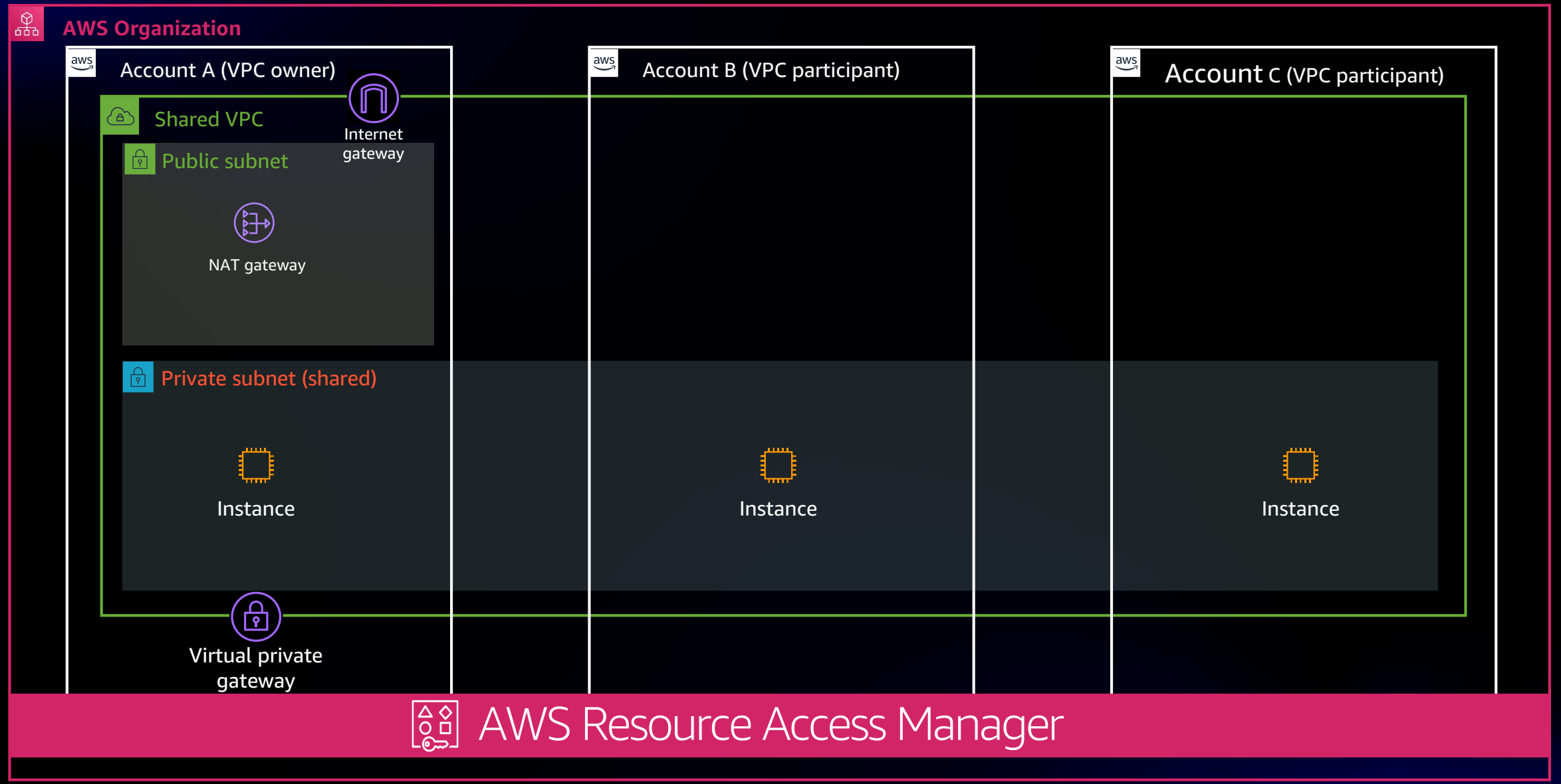
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Before VPC sharing



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

After VPC sharing



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

Best Practices

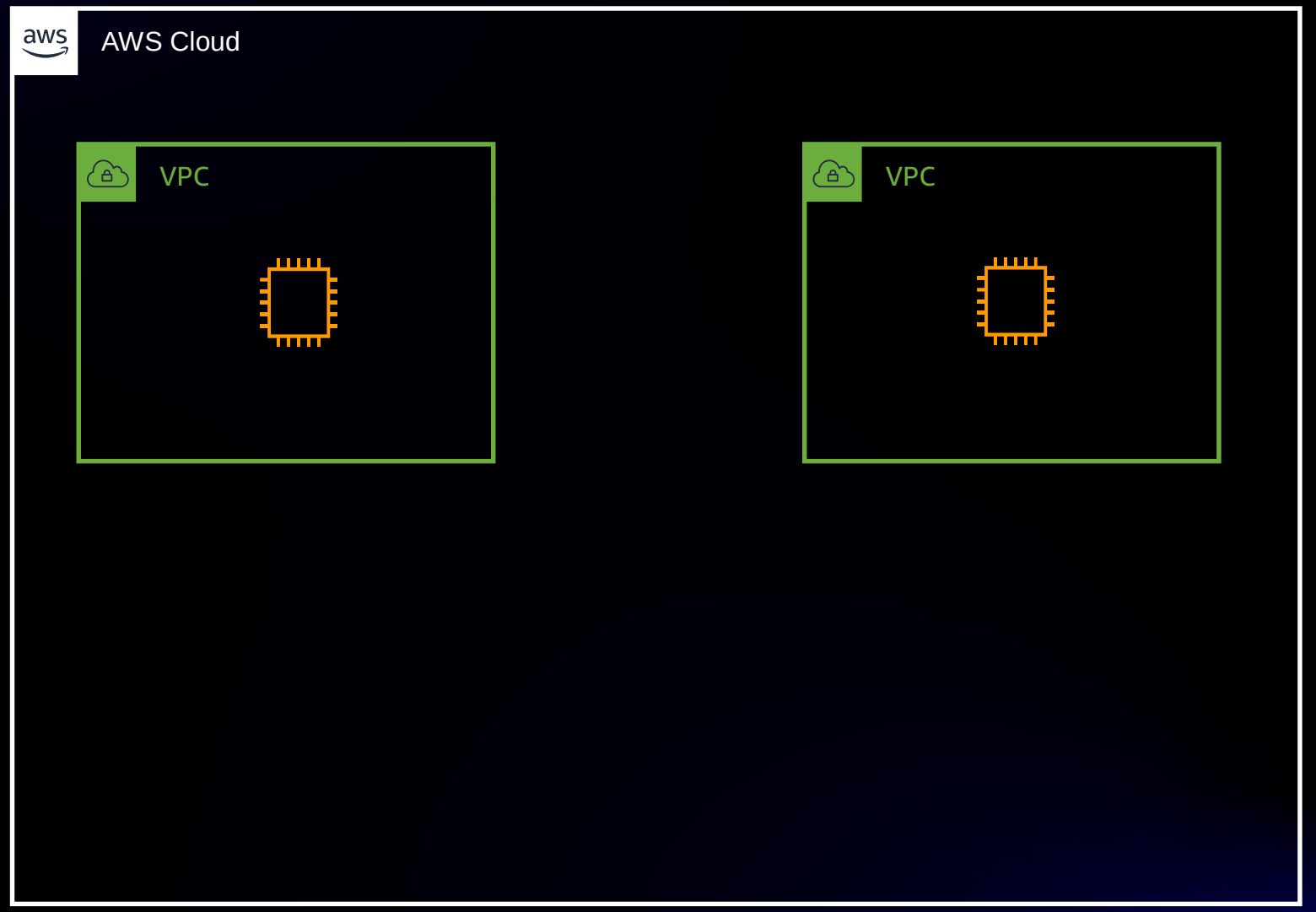
- Plan IP addressing for VPC Designing
- Create separate shared VPCs per environment
- Shared VPC and Security Zones
- Use larger subnets to reduce IP wastage
- Use dedicated subnets to reduce radius to a single VPC participant
- Use Network ACLs to isolate VPC participants
- Enable VPC flow logs and DNS query logs
- Enable Network Access Analyzer: NEW

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

Connectivity options

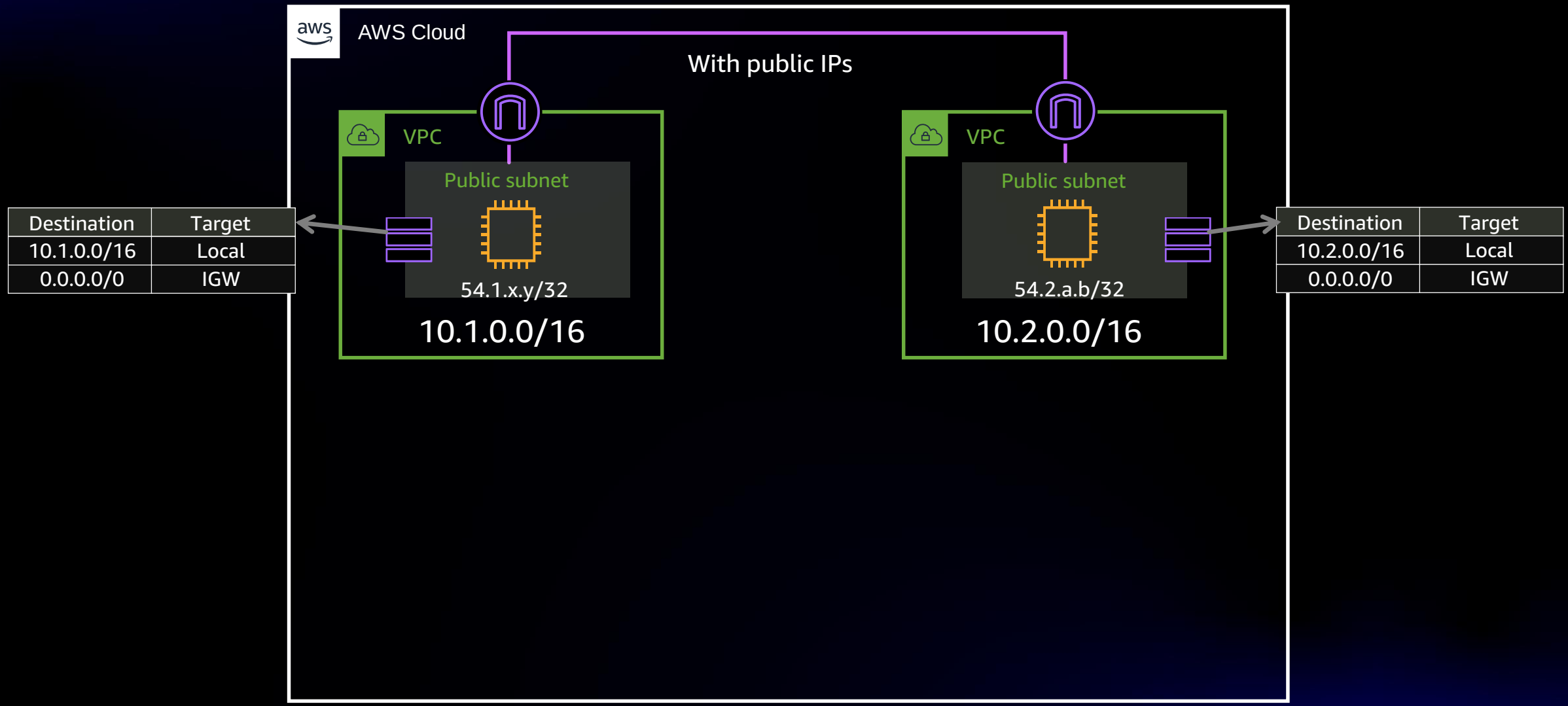
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC-to-VPC connectivity options



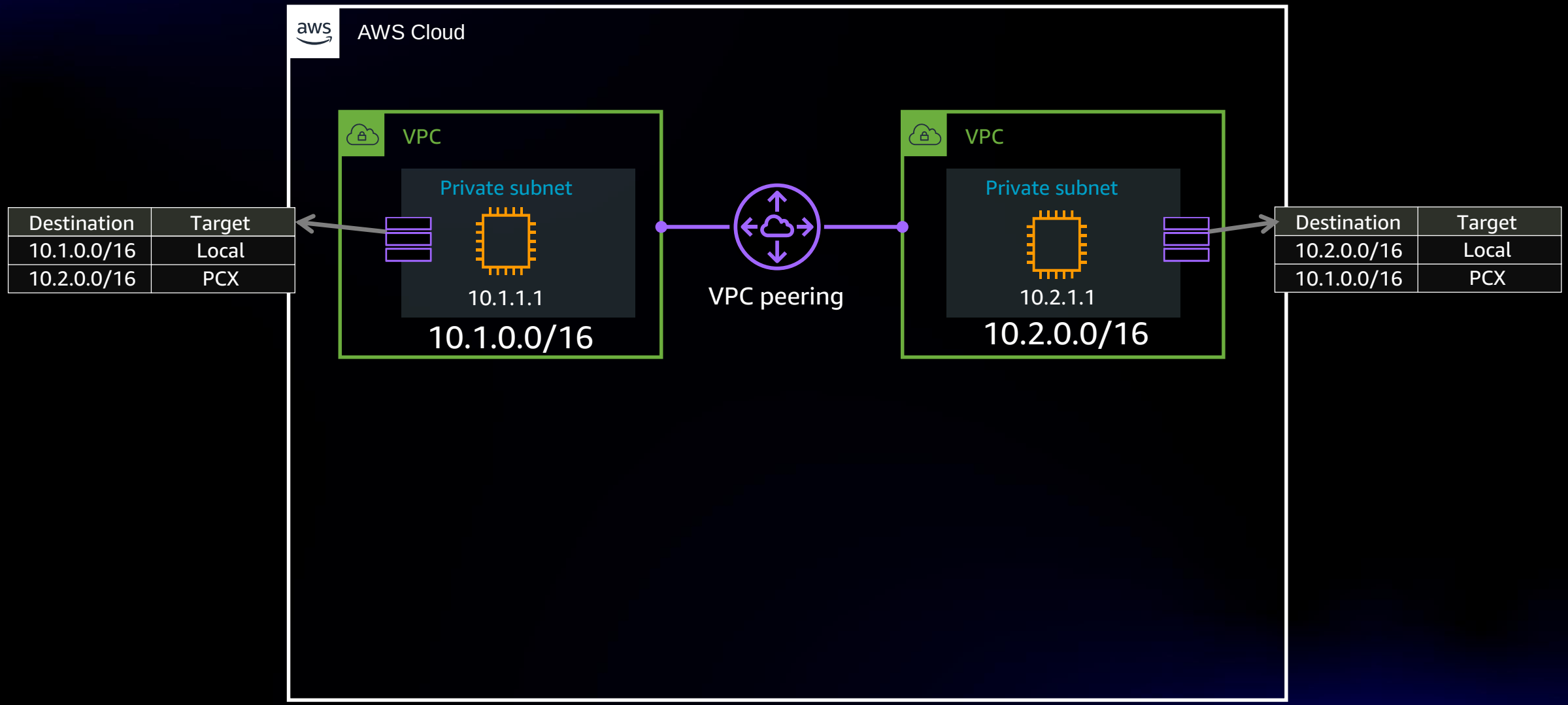
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC-to-VPC connectivity – Internet



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

VPC-to-VPC connectivity – VPC peering



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

VPC-to-VPC connectivity – VPC peering

Full mesh: How many Amazon VPC peering connections do I need to achieve full mesh?

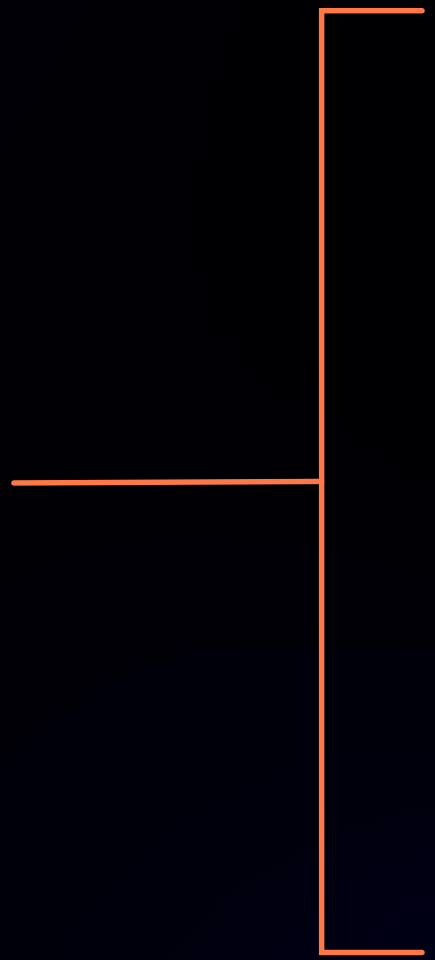
$$\frac{n(n-1)}{2}$$

VPCs x 10

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

VPC-to-VPC connectivity – VPC peering

Full mesh: How many Amazon VPC peering connections do I need to achieve full mesh?

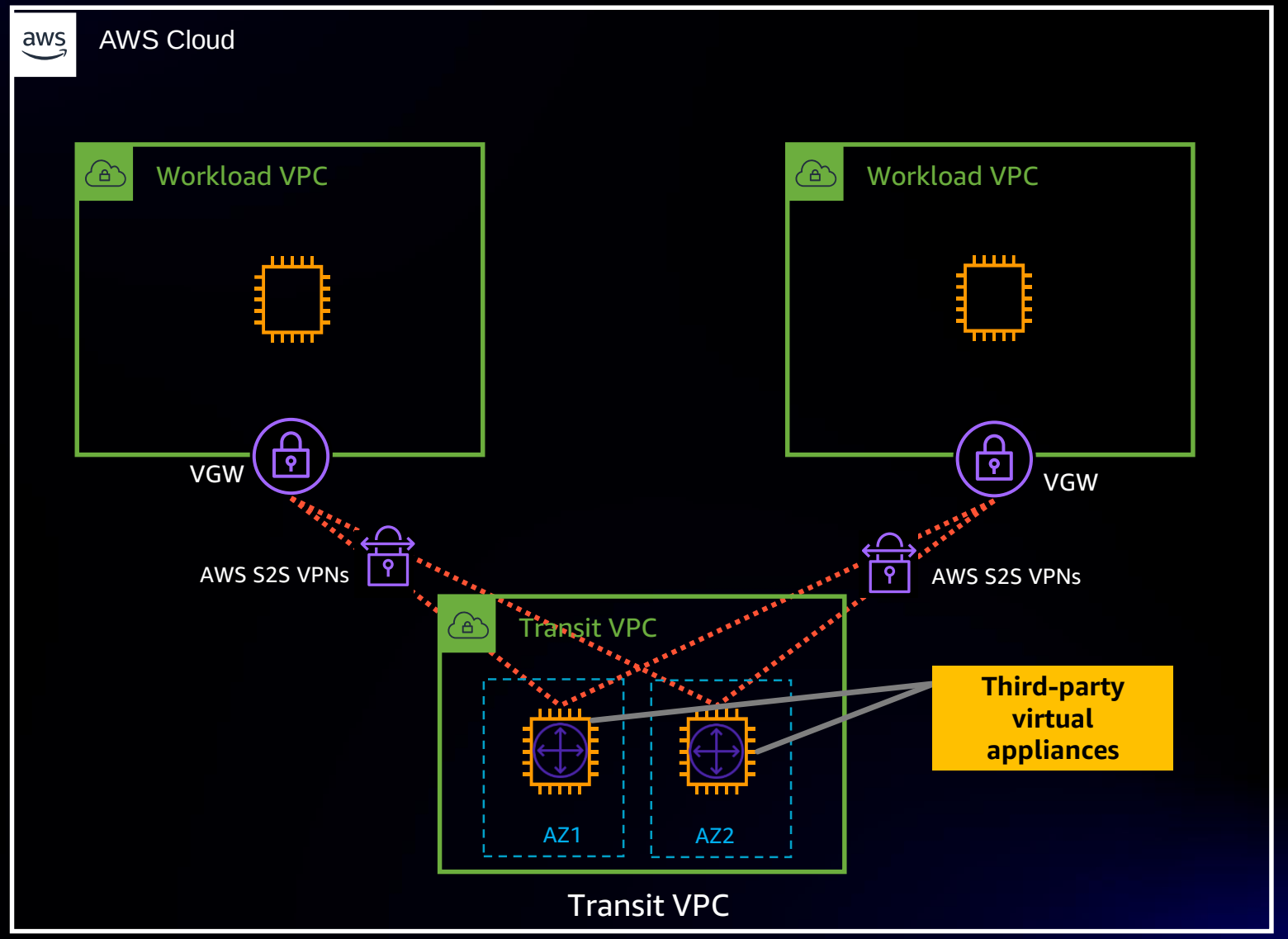


45

VPCs x 10

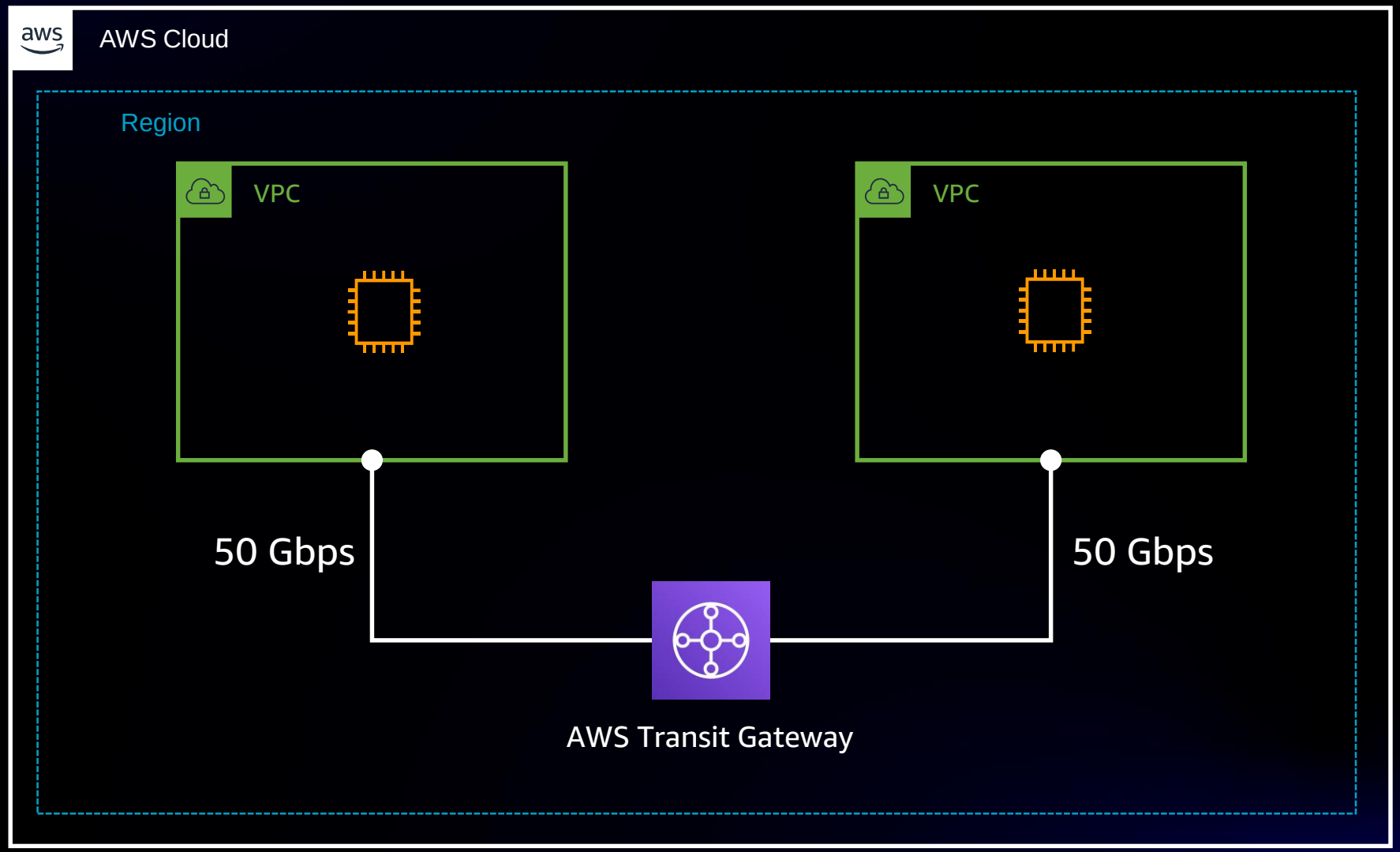
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC-to-VPC connectivity – Transit VPC



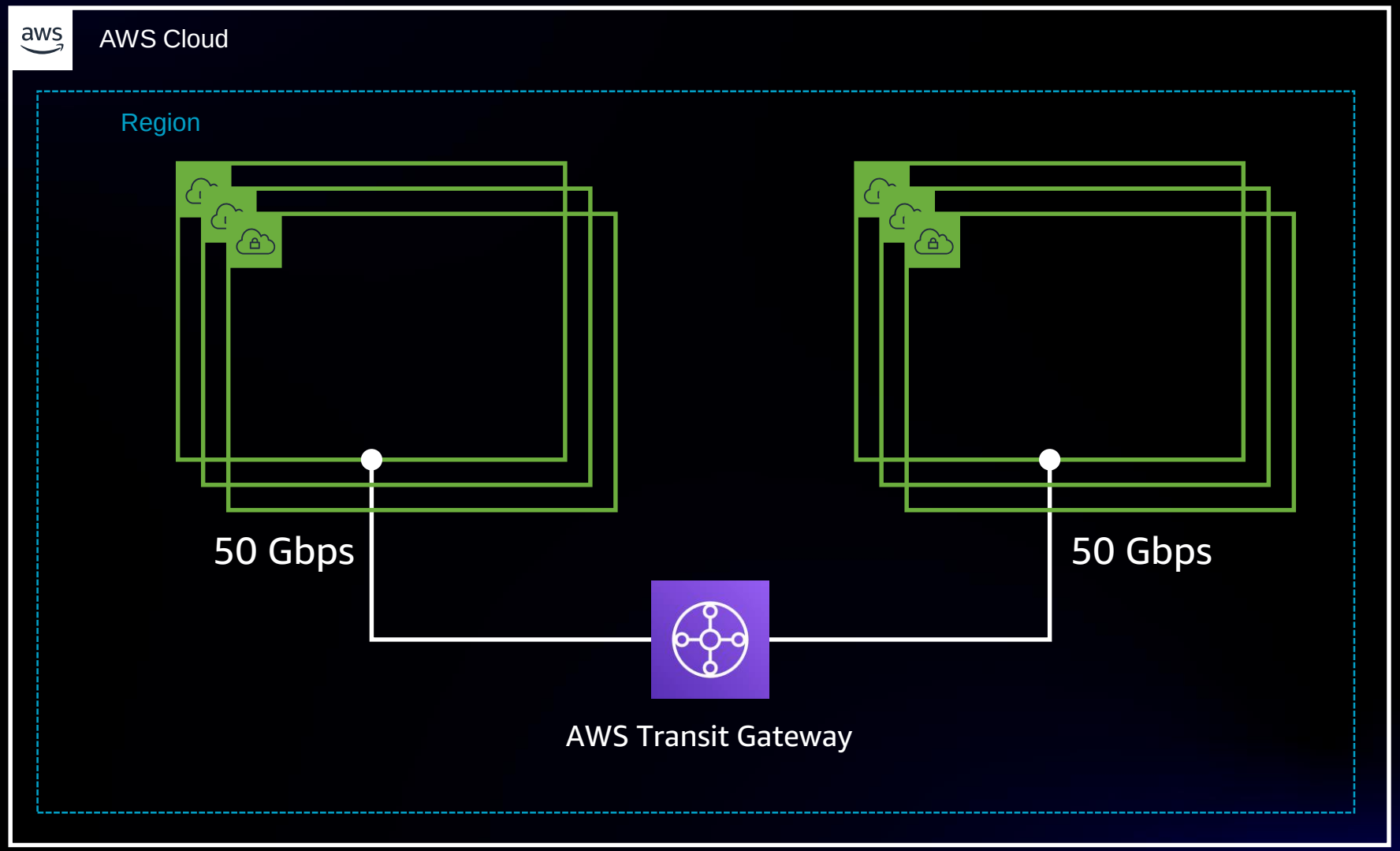
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC-to-VPC connectivity – AWS Transit Gateway



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

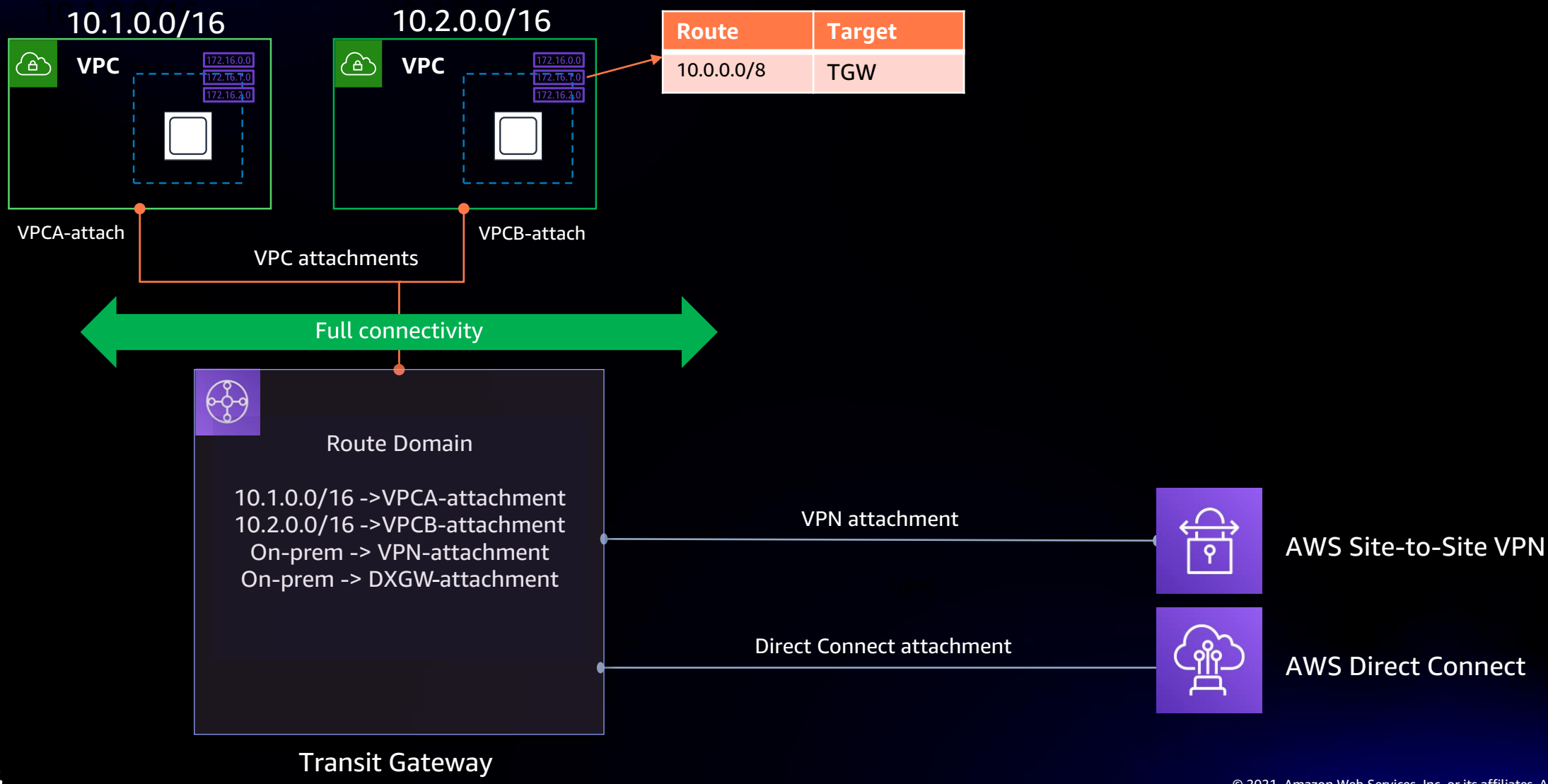
VPC-to-VPC connectivity – AWS Transit Gateway



VPCs
x5000

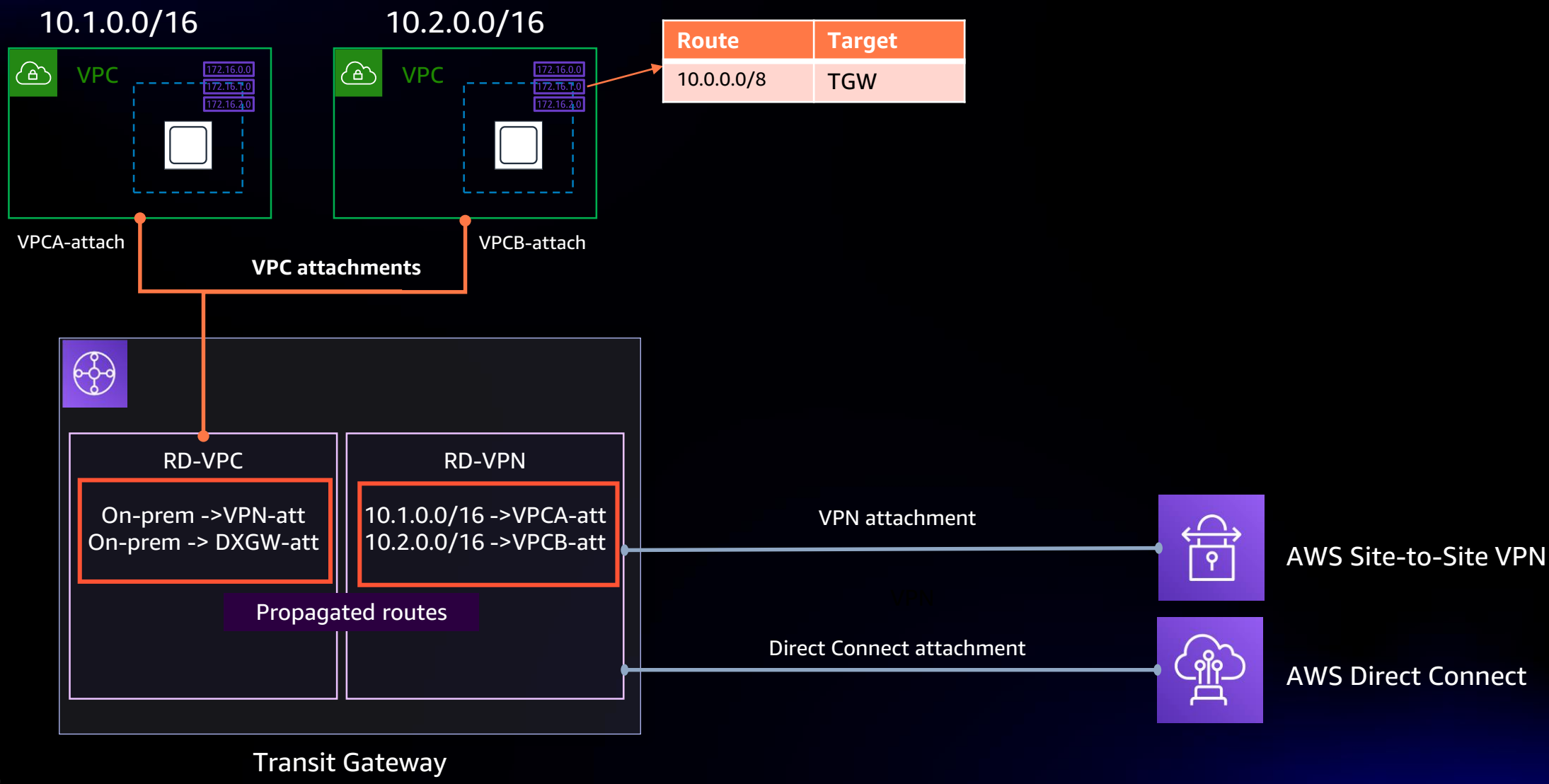
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway – Flat network



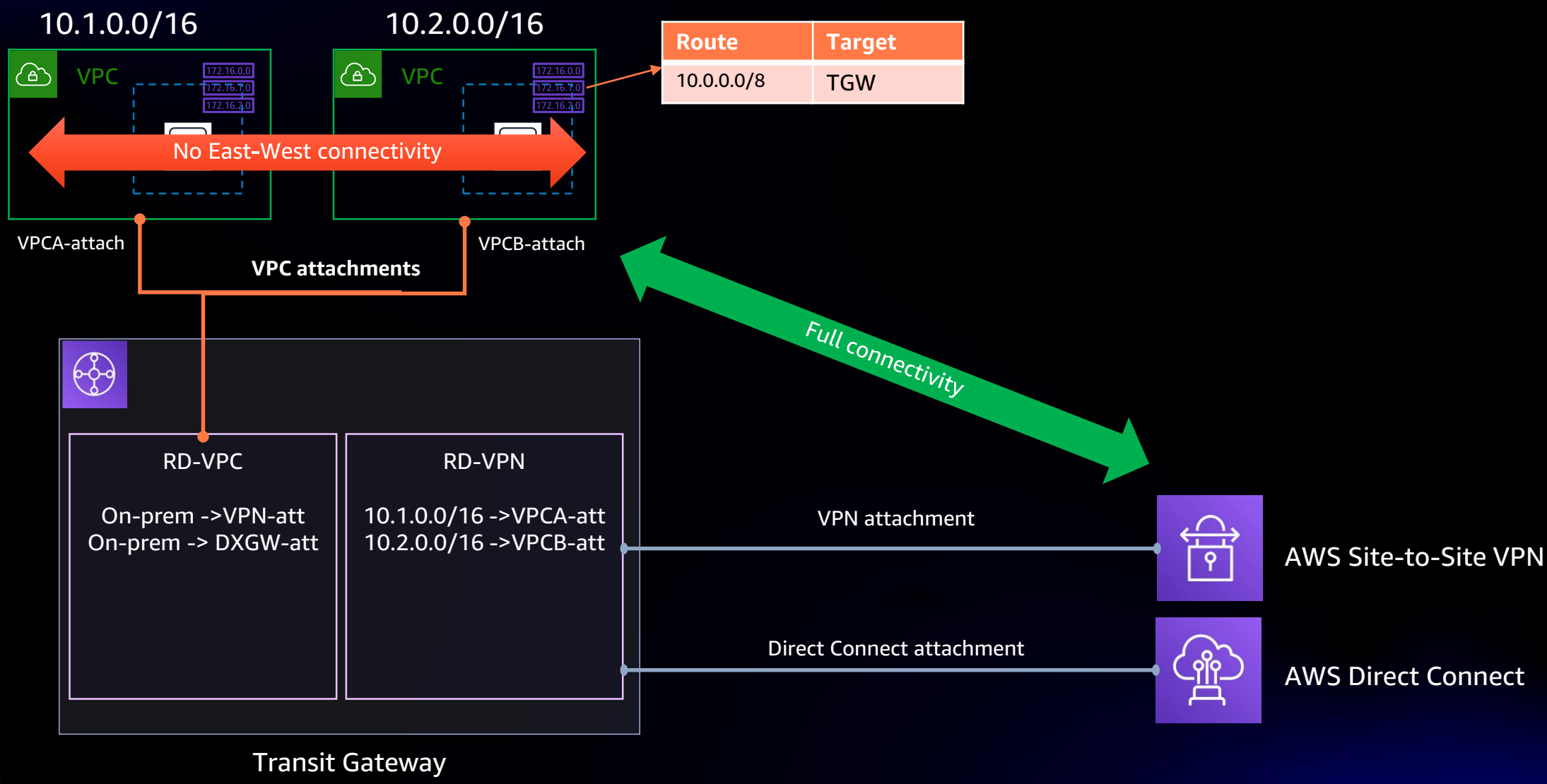
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway – Isolated network



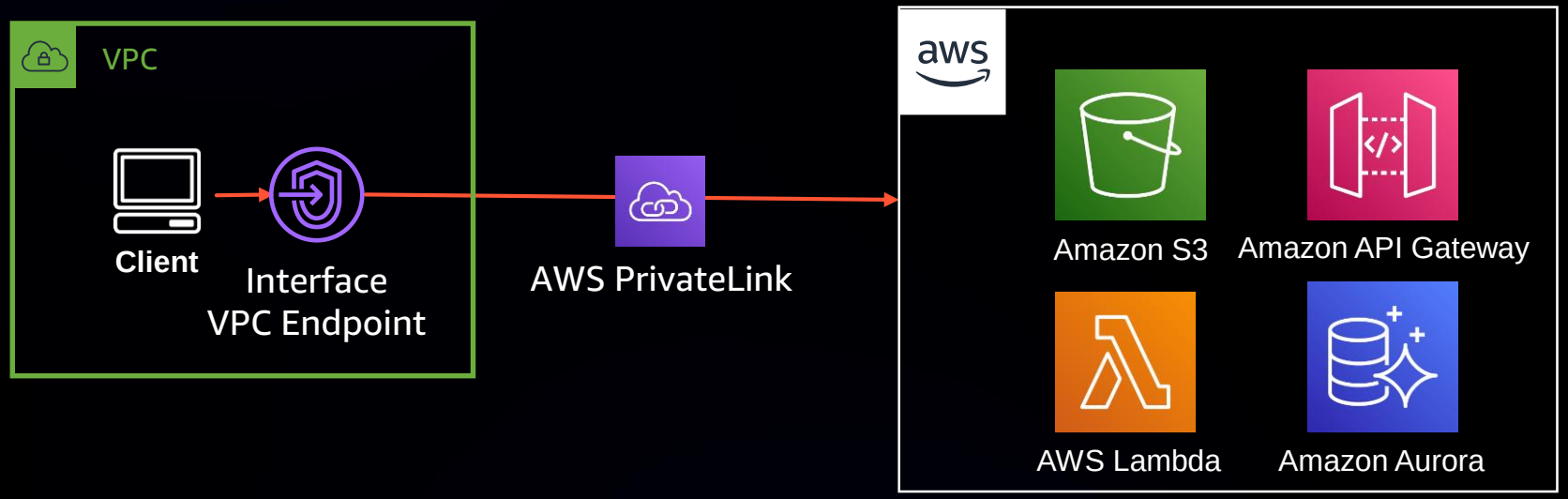
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway – Isolated network



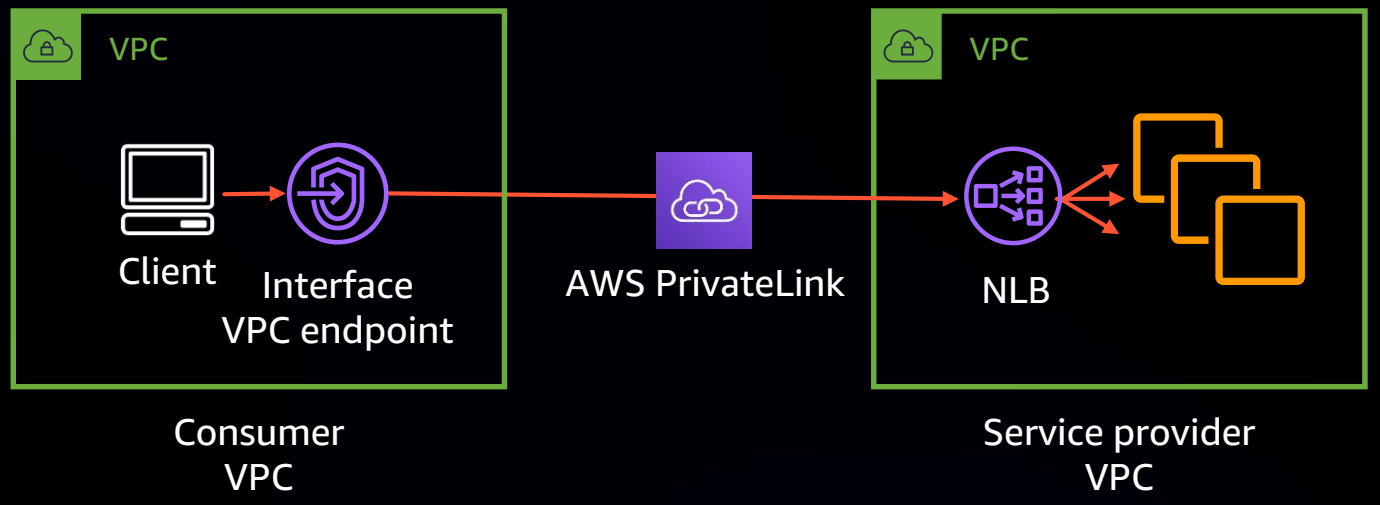
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink



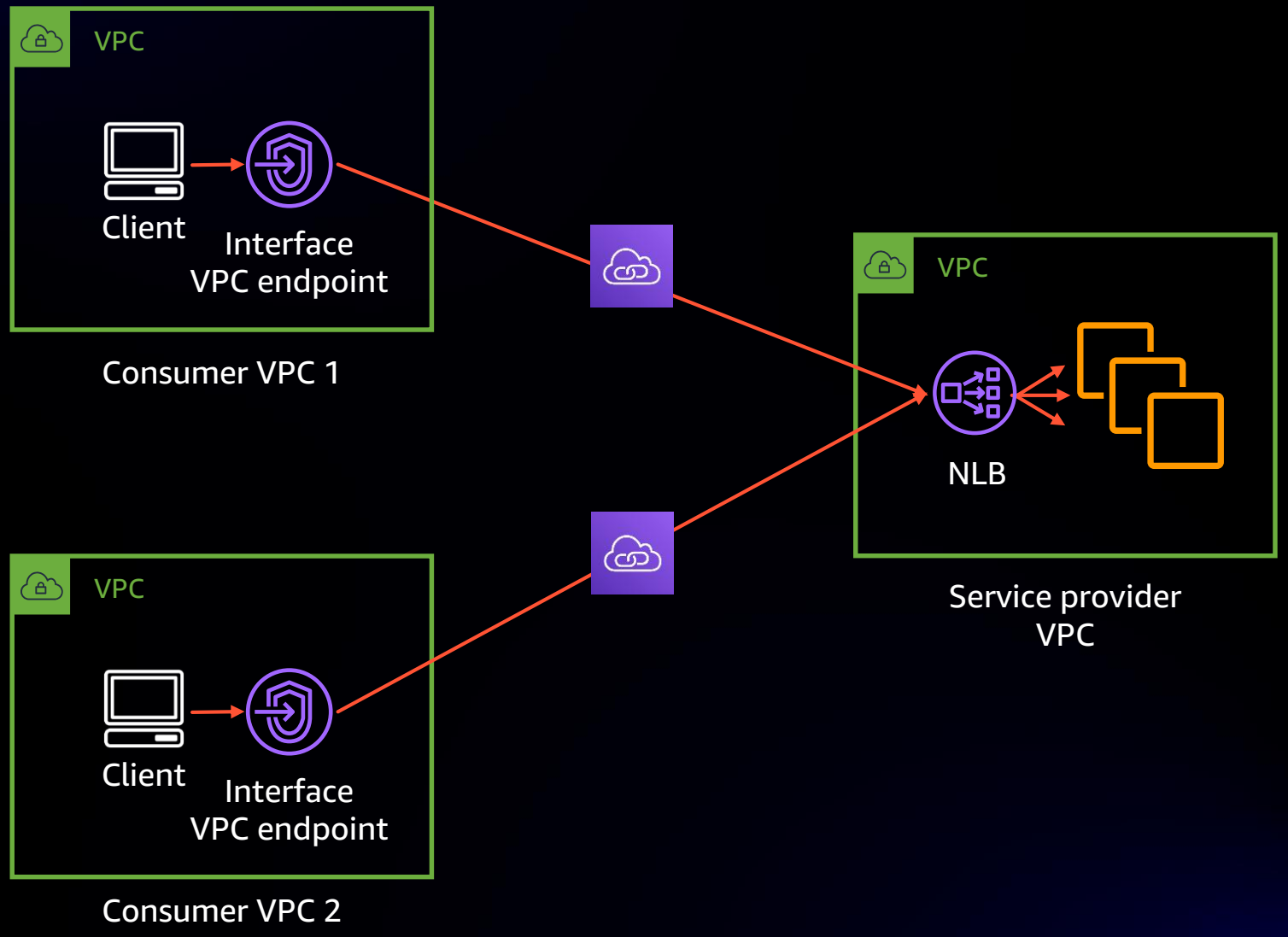
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink



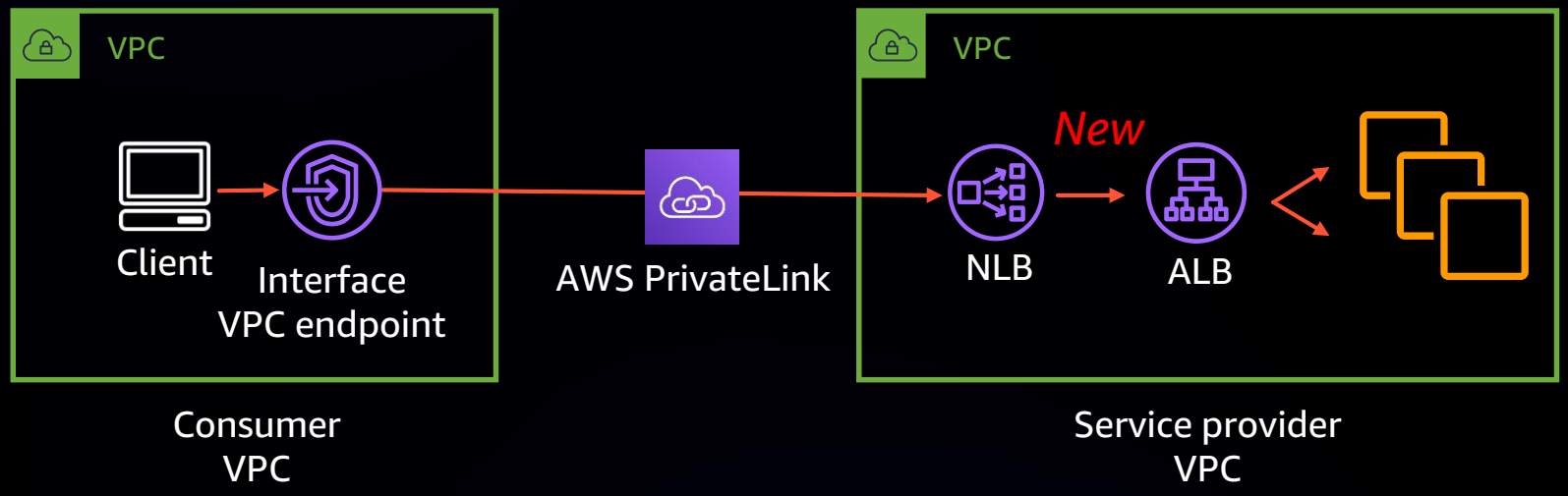
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink



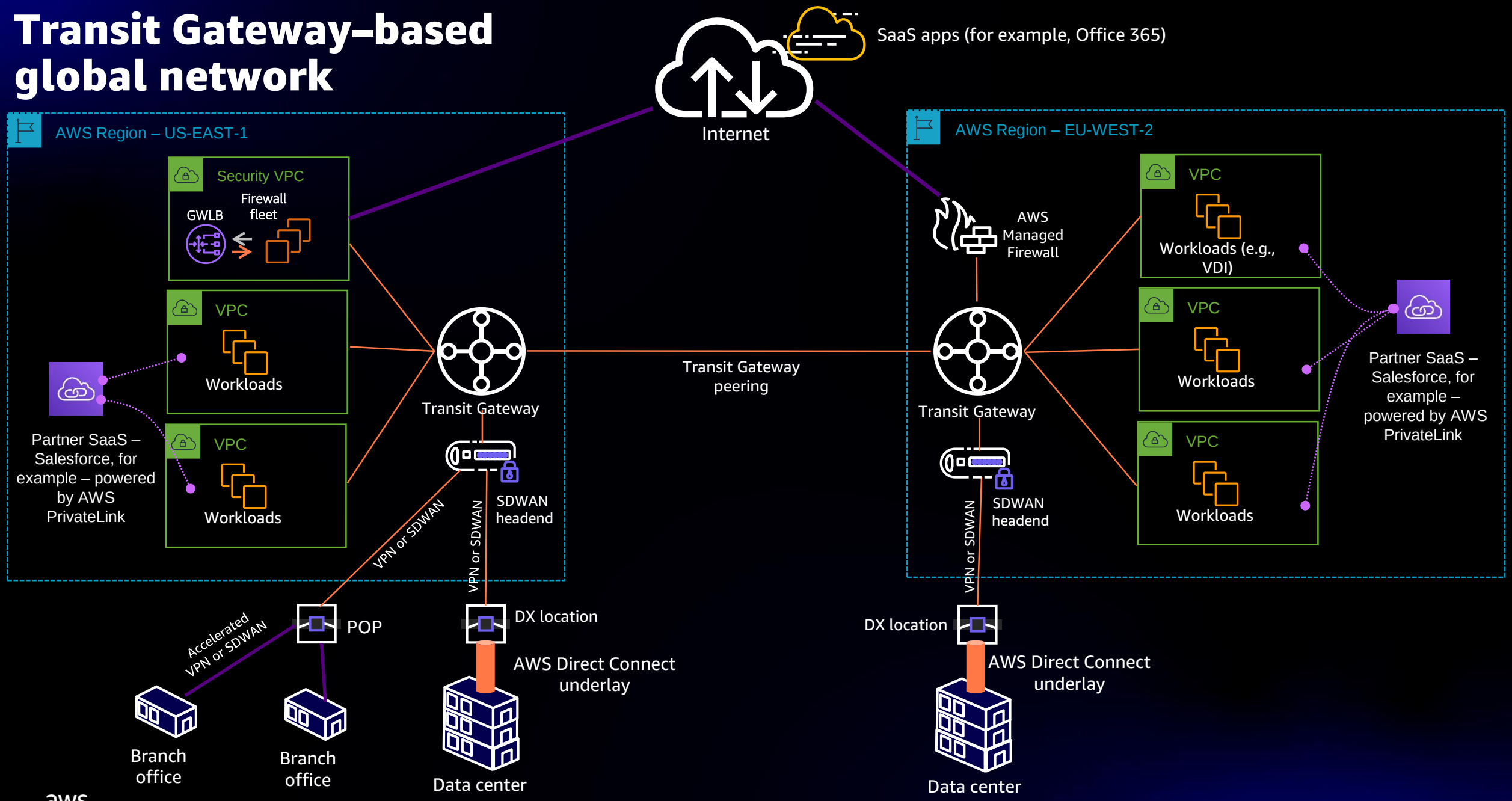
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS PrivateLink – ALB integration



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

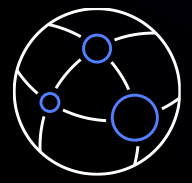
Transit Gateway–based global network



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

AWS training and certification

RESOURCES CREATED BY THE EXPERTS AT AWS TO HELP YOU BUILD AND VALIDATE NETWORKING SKILLS



Learn online with 15+ free digital courses, including *Configuring and Deploying VPCs with Multiple Subnets* (1 hour) and *Transit Gateway Networking and Scaling* (2 hours)



Build credibility and confidence with AWS Certification, including *AWS Certified Advanced Networking – Specialty*

Visit aws.training/Networking

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

Thank you!

Sohaib Tahir
sohaibt@amazon.com

Shirin Bhambhani
sbhambha@amazon.com

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