aws SUMMIT ONLINE

TAIWAN | SEPTEMBER 02,2021

KEY402

Amazon Networking Foundations

Shih-Yong Wang

Senior Solutions Architect
Amazon Web Services

aws

Figure 1. Magic Quadrant for Cloud Infrastructure and Platform Services

AWS recognized as a Cloud Leader for the 10th consecutive year [1]

Gartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, Raj Bala, Bob Gill, Dennis Smith, David Wright, July 2019. ID G00365830. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved.

[1] https://aws.amazon.com/blogs/aws/aws-named-as-a-cloud-leader-for-the-10th-consecutive-year-in-gartners-infrastructure-platform-services-magic-quadrant/

AWS Global Infrastructure

AWS global infrastructure

25 geographical regions, 81 availability zones, 230+ POPs

Region & Number of Availability Zones (AZs)

GovCloud (US)
US-East (3), US-West (3)

US West
Oregon (4)
Northern California (3)

US East
N. Virginia (6), Ohio (3)

Canada
Central (3)

South America
São Paulo (3)

Africa
Cape Town (3)

Europe
Frankfurt (3), Paris (3),
Ireland (3), Stockholm (3),
London (3), Milan (3)

Middle East
Bahrain (3)

Asia Pacific
Singapore (3), Sydney (3),
Tokyo (4), Osaka (3)
Seoul (4), Mumbai (3),
Hong Kong (3)

China
Beijing (3), Ningxia (3)

Announced Regions

7 Regions and 21 AZs in Australia, India, Indonesia, Israel, Spain, Switzerland, and United Arab Emirates (UAE)

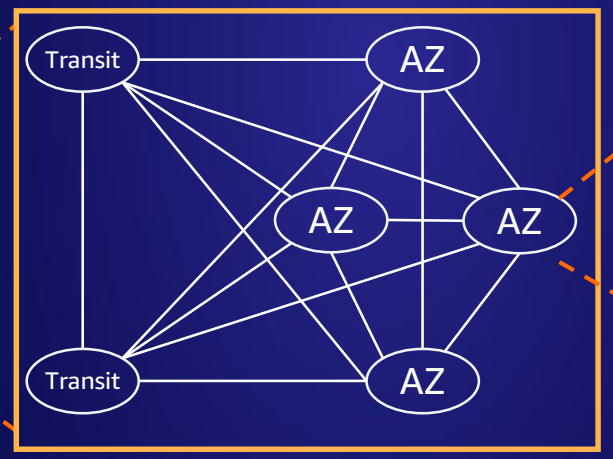
https://aws.amazon.com/about-aws/global-infrastructure/

aws

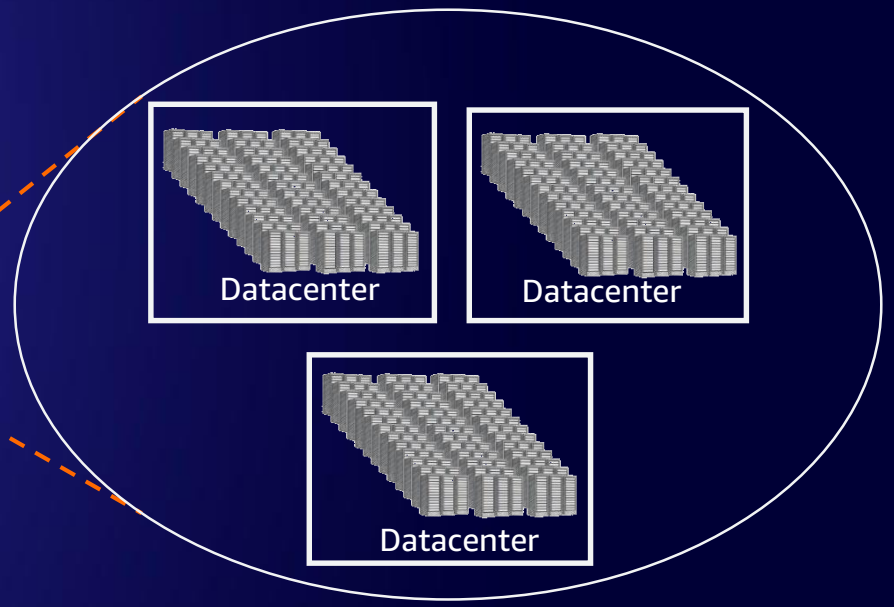
AWS Region design

AWS Regions are comprised of multiple AZs for high availability, high scalability, and high fault tolerance. Applications and data are replicated in real time and consistent in the different AZs.

AWS Region



AWS Availability Zone (AZ)



A Region is a physical location in the world where we have multiple **Availability Zones.**

Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

AWS Availability Zone (AZ) design

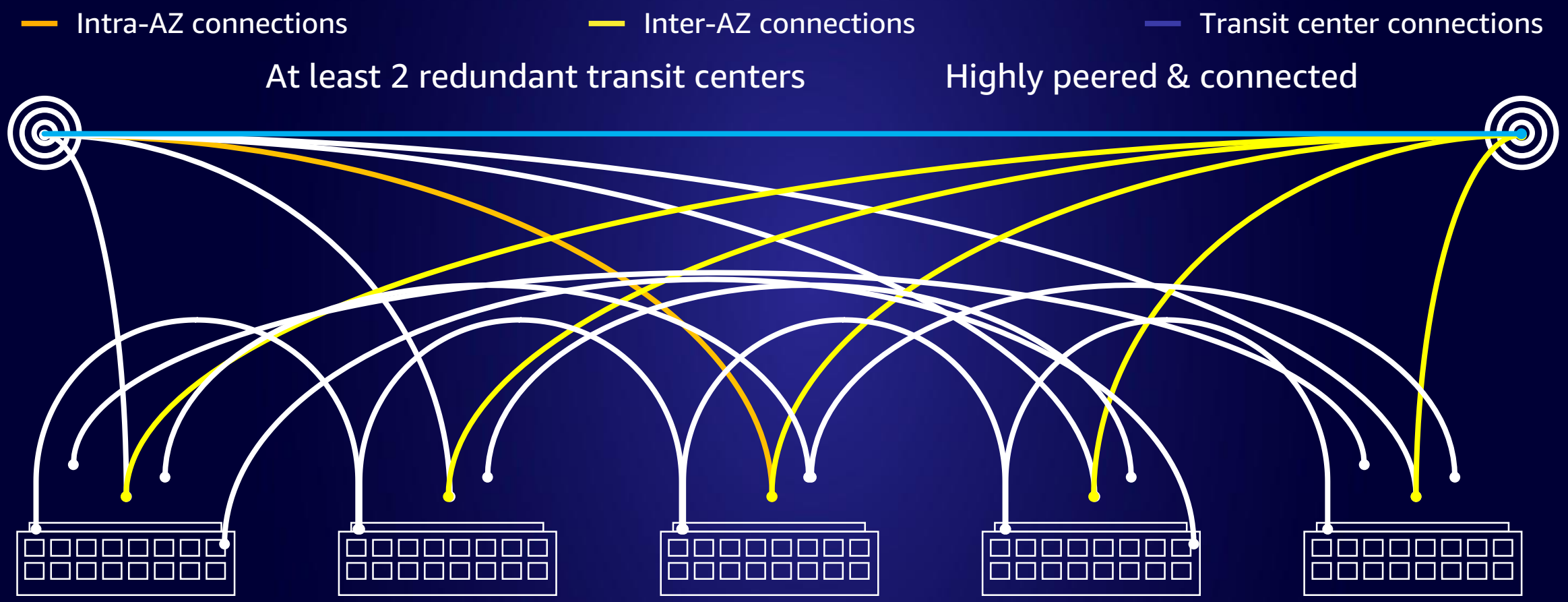
- Fully isolated infrastructure with one or more datacenters
- Meaningful distance of separation
- Unique power infrastructure
- Many 100Ks of servers at scale
- Datacenters connected via fully redundant and isolated metro fiber

Intra-AZ & inter-AZ connectivity

- Dark fiber spans
  - Optimized for low-latency & physical diversity
  - High fiber density
  - Amazon controlled infrastructure

- Dense wavelength division multiplexing (DWDM) for inter-AZ connections
- Optical level failover reducing the impact of physical faults

AWS network connection design



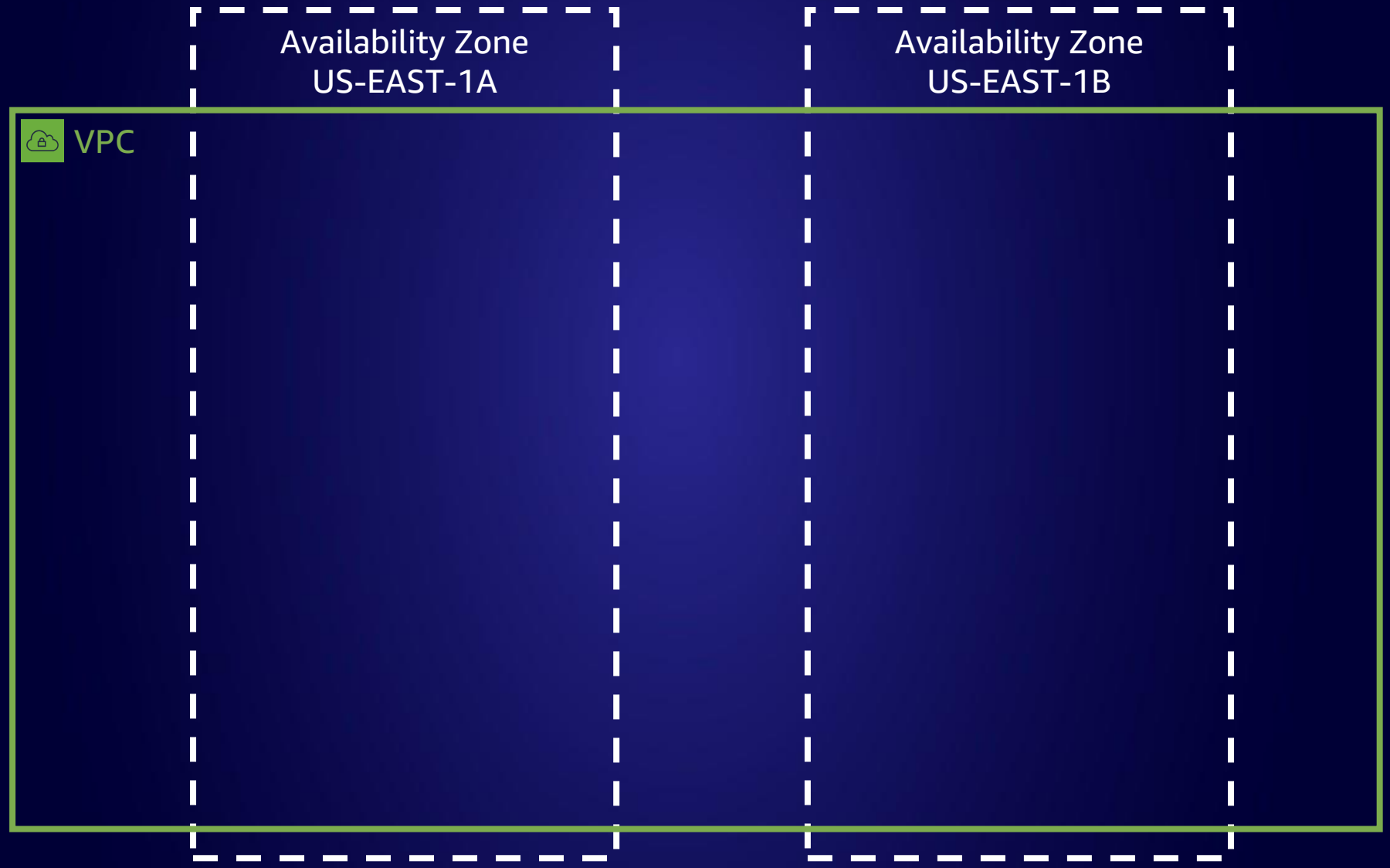
Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC)

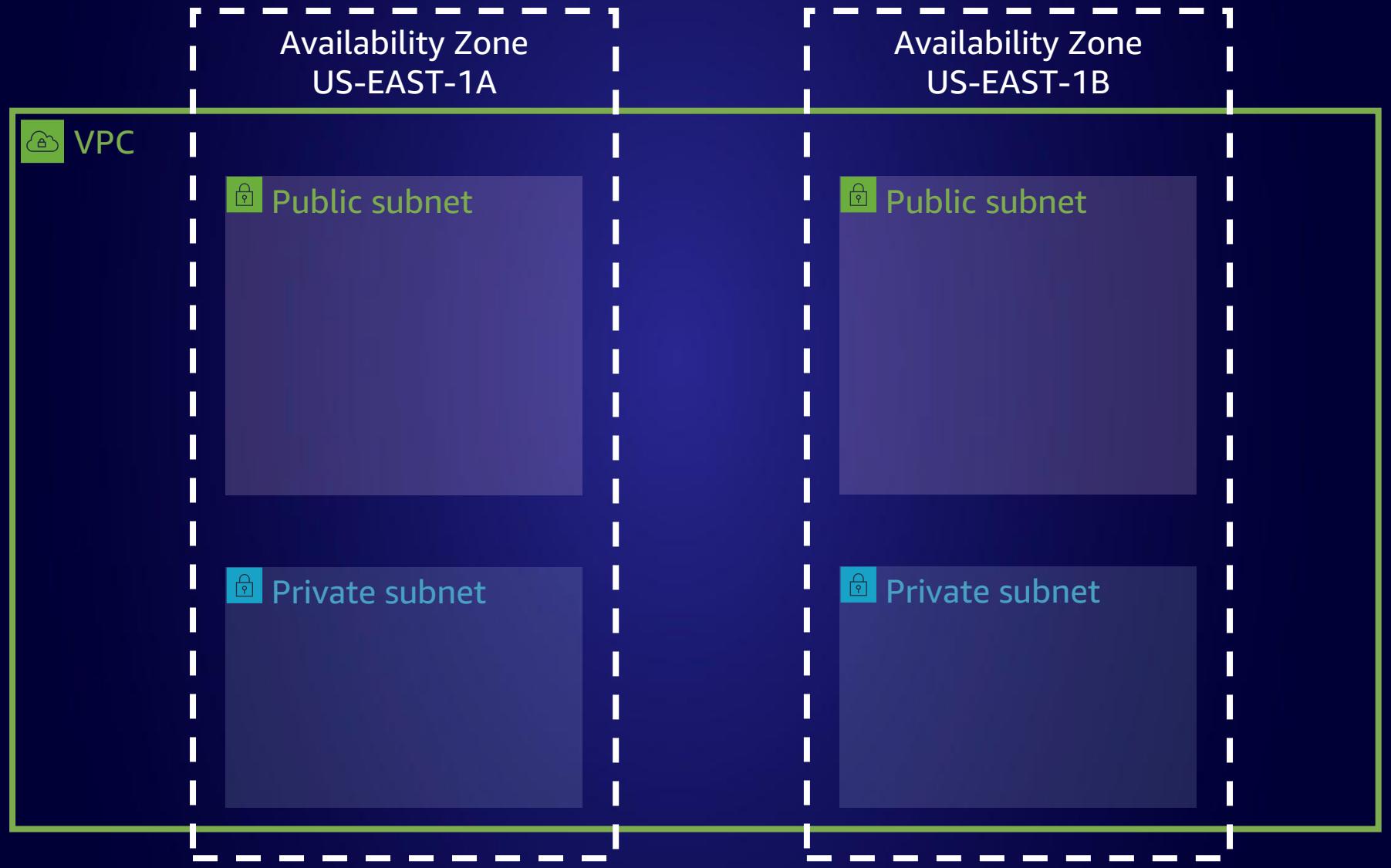
- Lets you provision a logically isolated section of the AWS Cloud
- You can launch AWS resources in a virtual network that you define
- You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways
- You can use both IPv4 and IPv6 in your VPC

aws

Amazon Virtual Private Cloud (VPC)

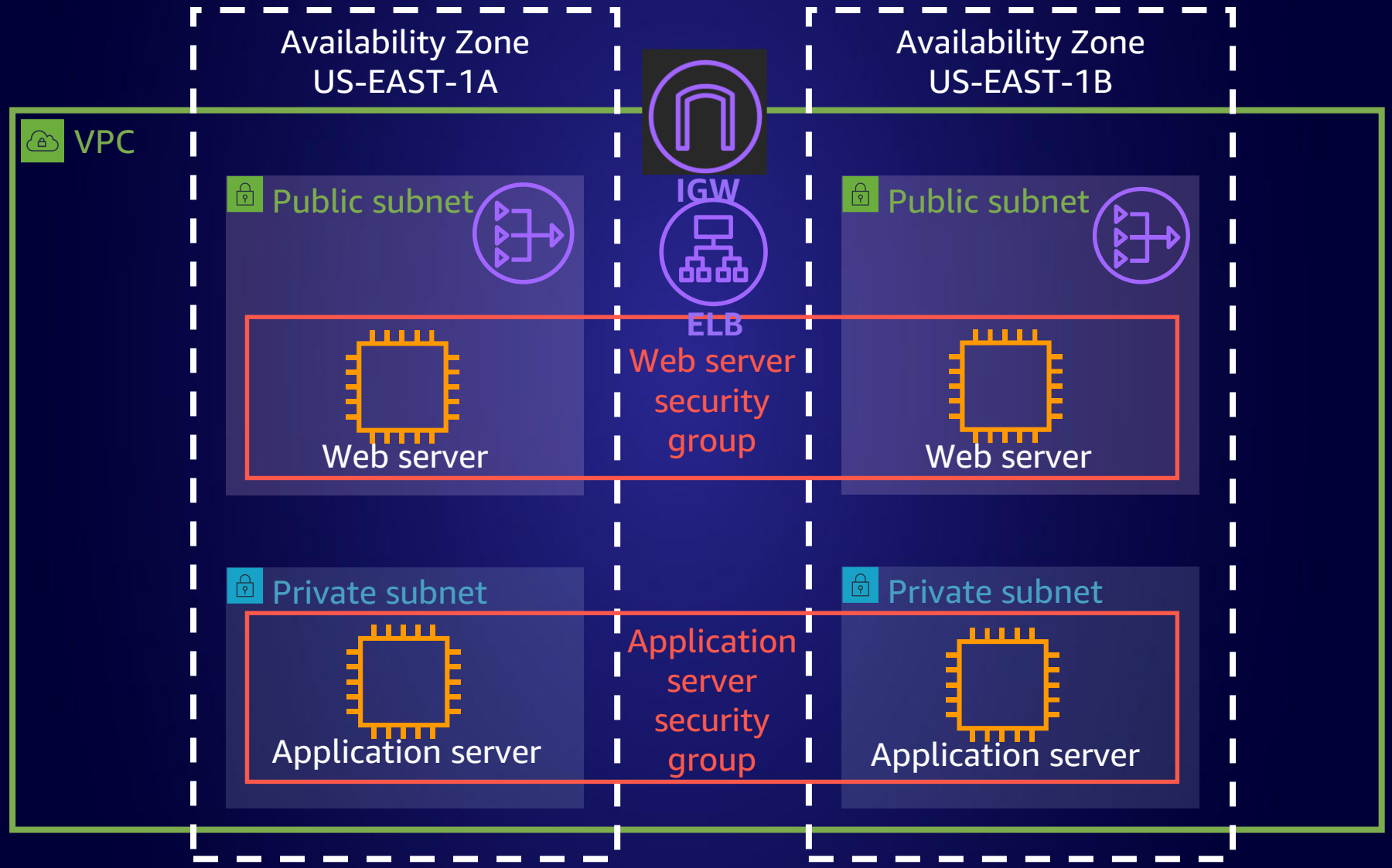


Subnets

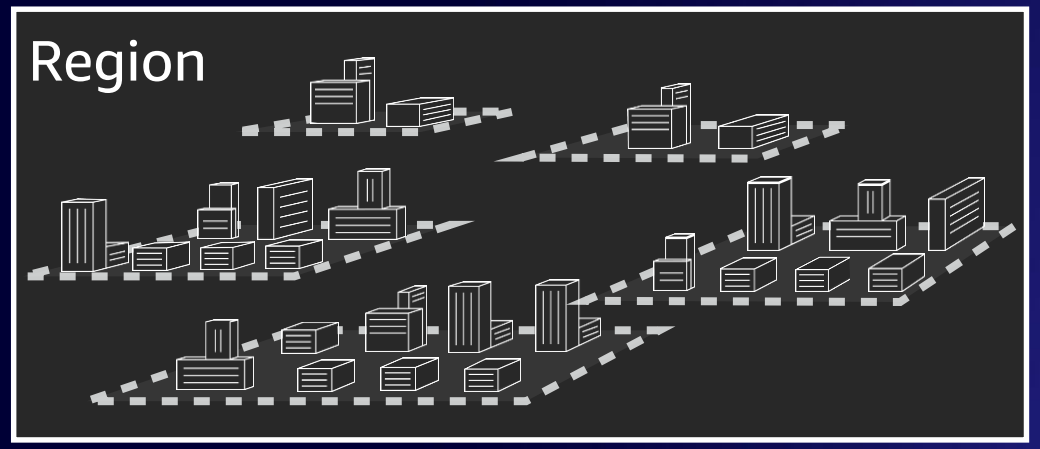


Elastic Compute Cloud (EC2) instances

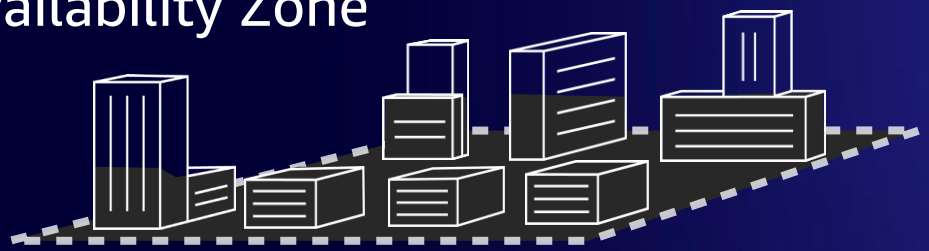
Example web application



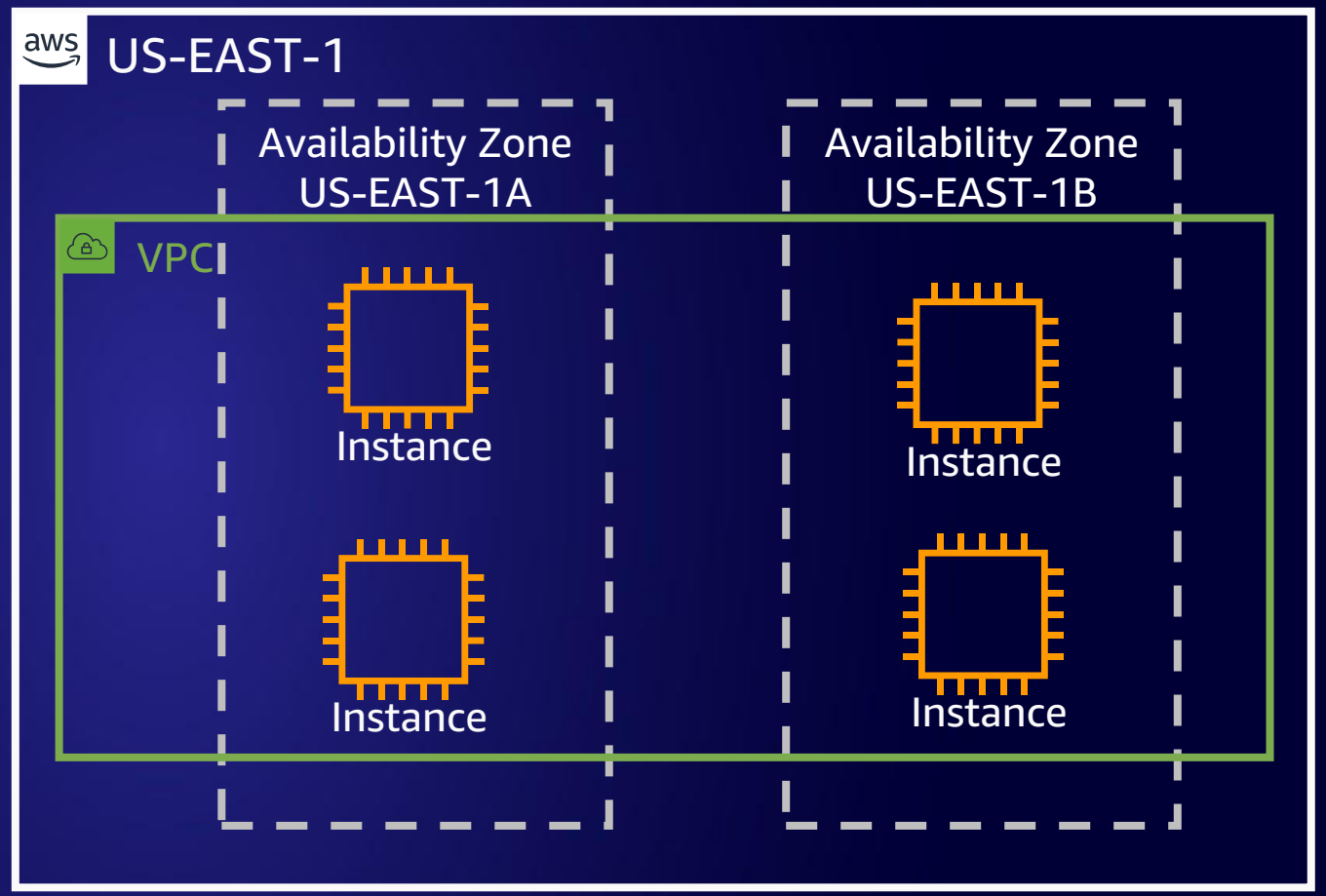
Amazon Regions and AZ



Availability Zone



Data center, rack, host



Gateways

Amazon Internet Gateway (IGW)

- A horizontally scaled, redundant, and highly available VPC component
- Allows communication between instances in your VPC and the internet
- No availability risks or bandwidth constraints on your network traffic

aws

Amazon NAT Gateway (NAT GW)

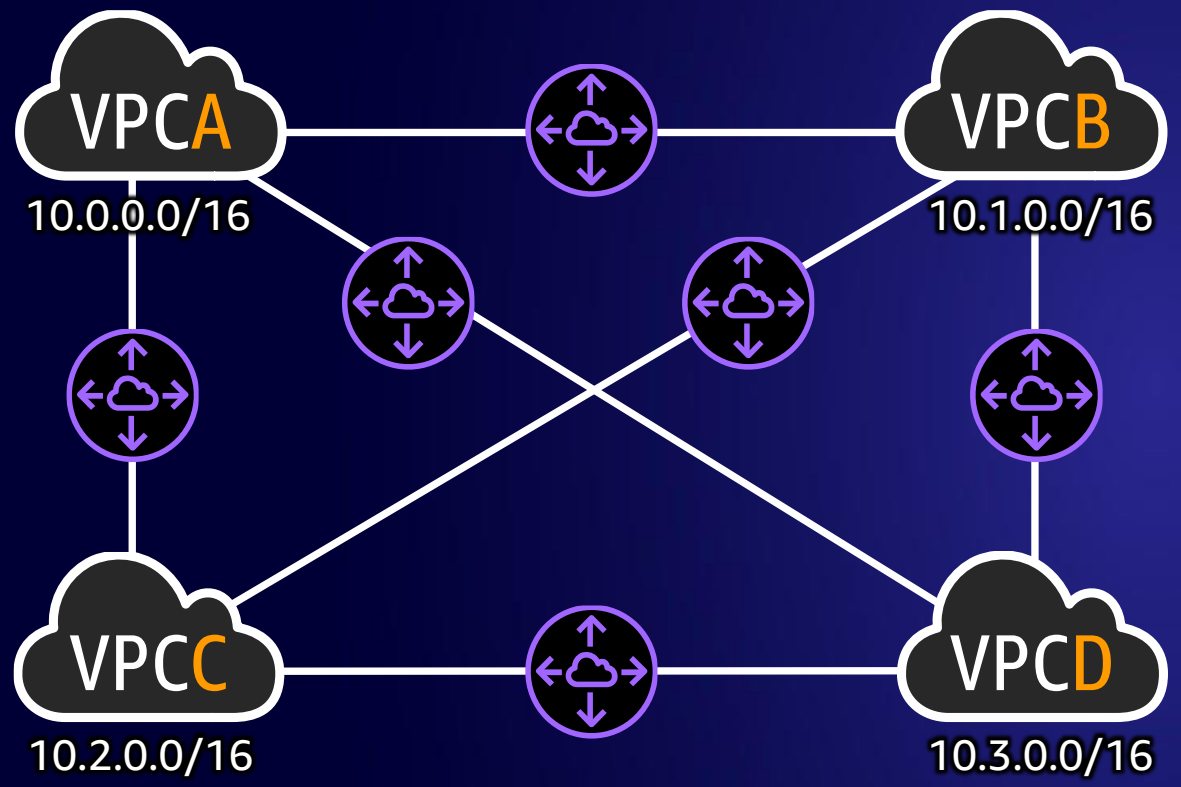
- In a private subnet
  - Instance can connect to services outside your VPC
  - But external services cannot initiate a connection with those instances
- When sending response traffic to the instances, the NAT device translates the addresses back to the original source IPv4 addresses
- Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone

aws

Internet Gateway and NAT Gateway

Connecting to Other VPCs

VPC peering



- Full private IP connectivity between two VPCs
- Can peer VPCs across regions
- VPCs can be in different accounts
- VPC CIDR ranges must not overlap

VPC peering: Things to know

- Can reference security groups from the peer VPC in the same Region
- Can enable DNS hostname resolution to return private IP addresses
- Can peer for both IPv4 and IPv6 addresses
- Cannot have overlapping IP addresses
- Cannot have multiple peers between the same pair of VPCs
- Cannot use jumbo frames across inter-region VPC peering

aws

The calculation sample 1

Full mesh: How many Amazon VPC peering connections do I need (full mesh)?

VPC x 10

45

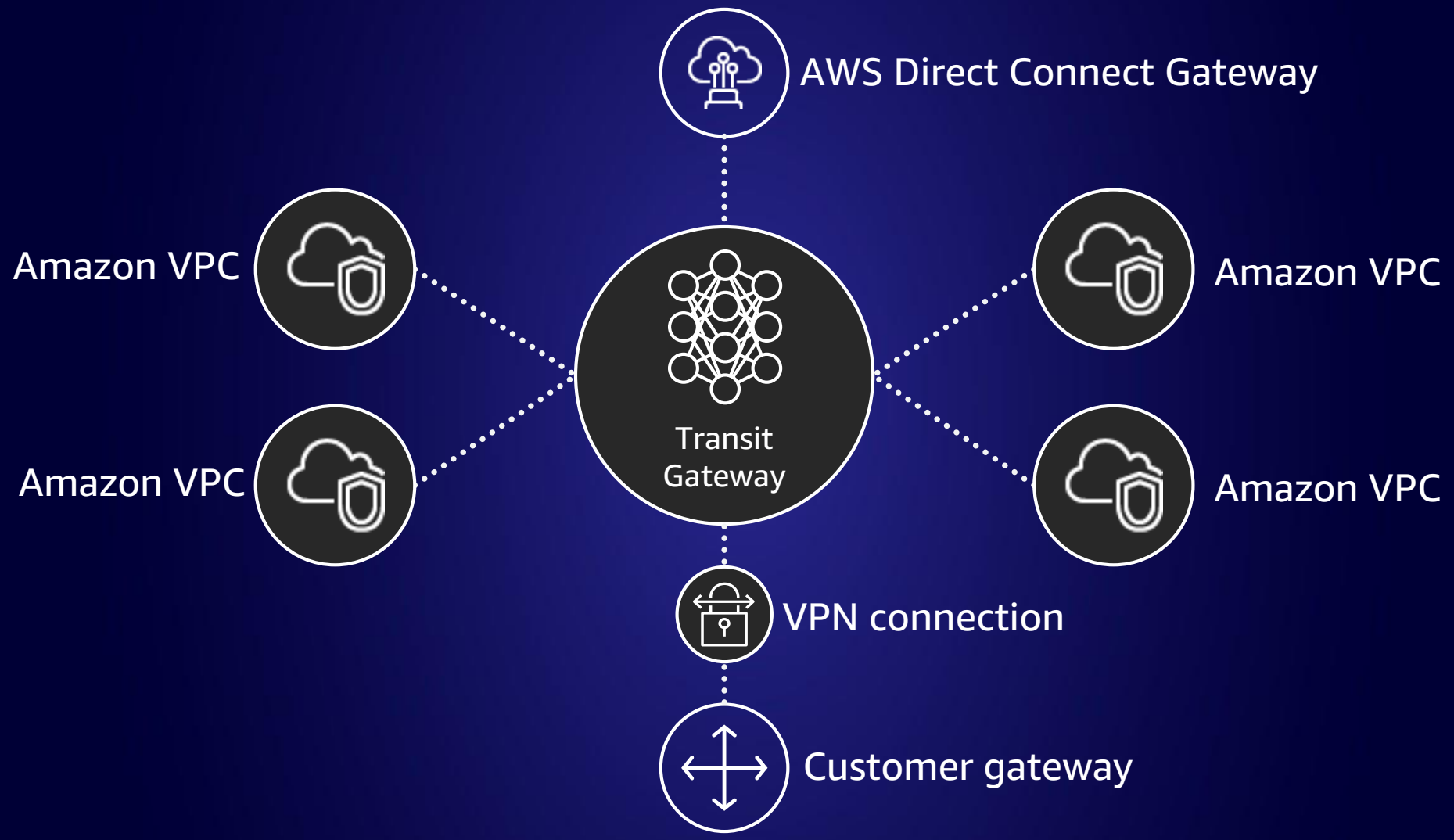
The calculation sample 2

Full mesh: How many Amazon VPC peering connections do I need (full mesh)?

VPC x 100

4,500

With AWS Transit Gateway …



AWS Transit Gateway capability (1/2)

TGWs per account/TGW attachments per Amazon VPC

5

Maximum burstable bandwidth per attachment

50 Gbps

AWS Transit Gateway capability (2/2)

Routes per TGW

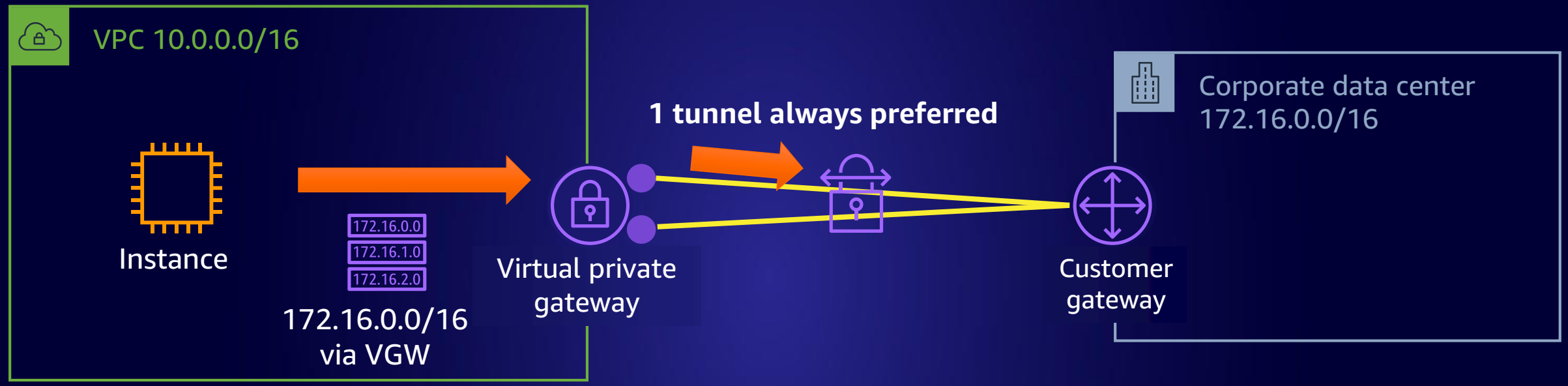
10,000

Number of TGW attachments per region per account

5,000

Connectivity to on-premises networks

AWS site-to-site VPN

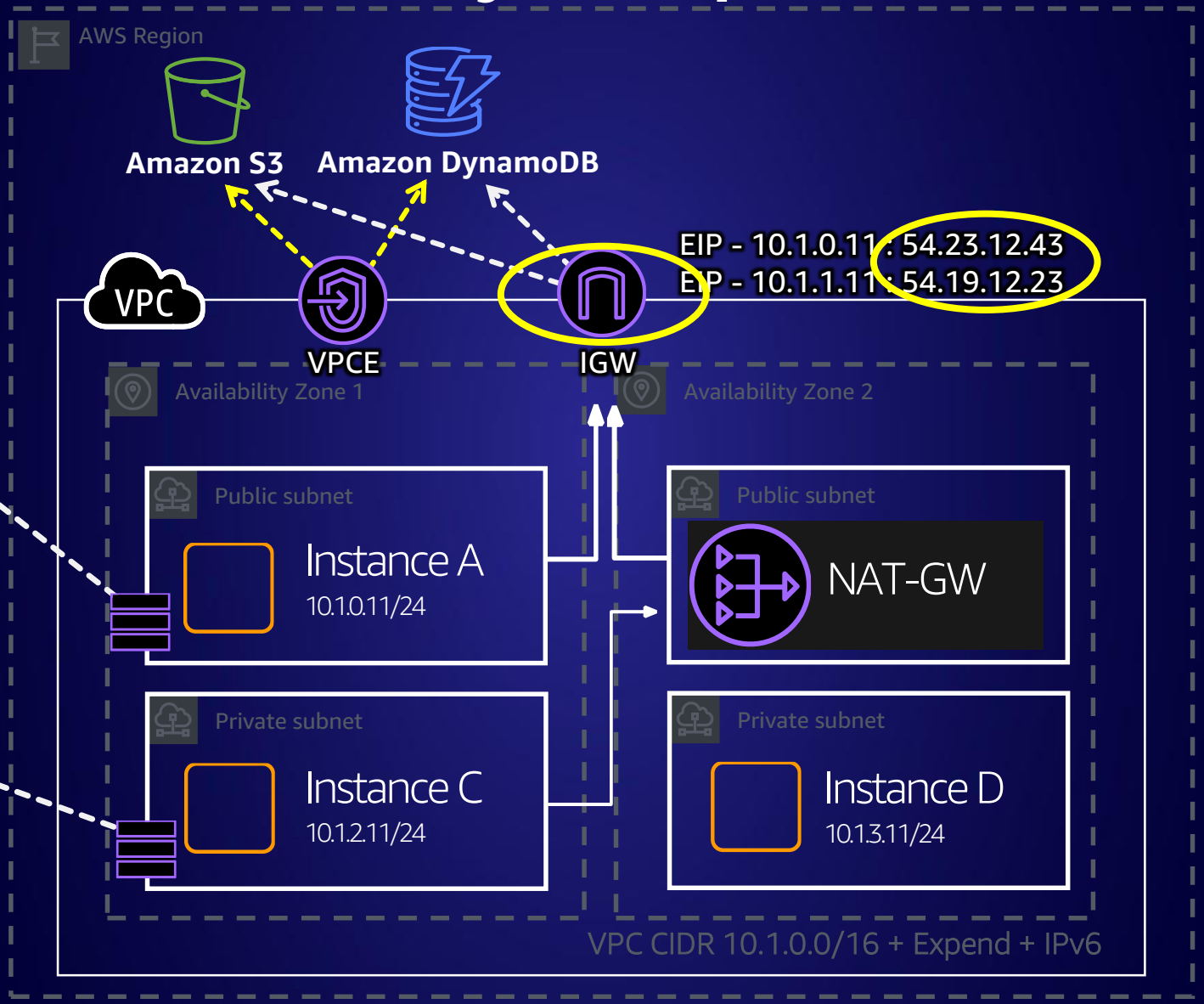


1x VPN connection = 2x VPN tunnels

1x VPN tunnel = 1.25 Gbps

Amazon VPC endpoints

Amazon VPC Gateway endpoints

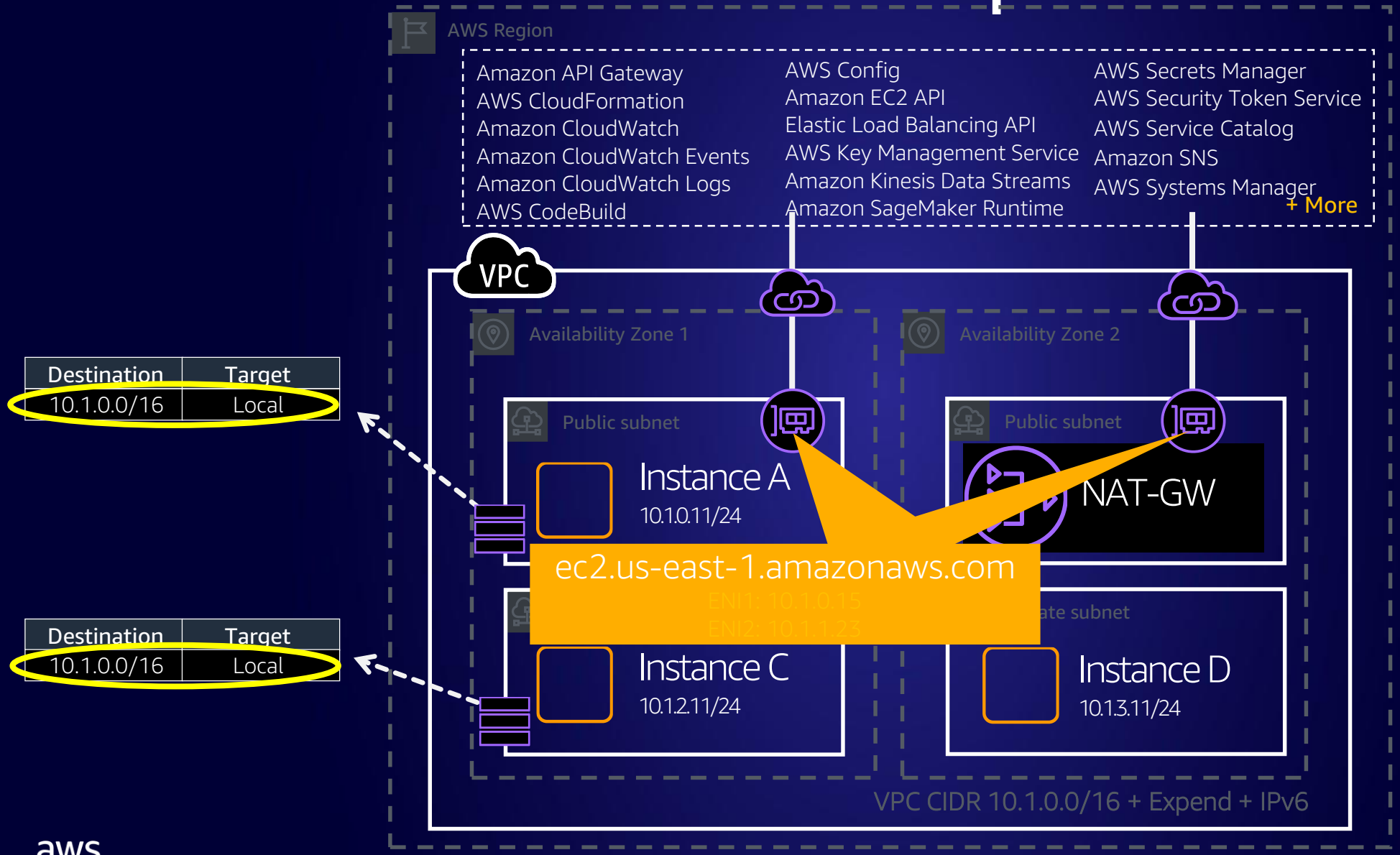


Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW
DDB.prefix.list	VPCE-123

VPCE =
Virtual Private Endpoint
(Type: Gateway)

Amazon VPC Interface endpoints

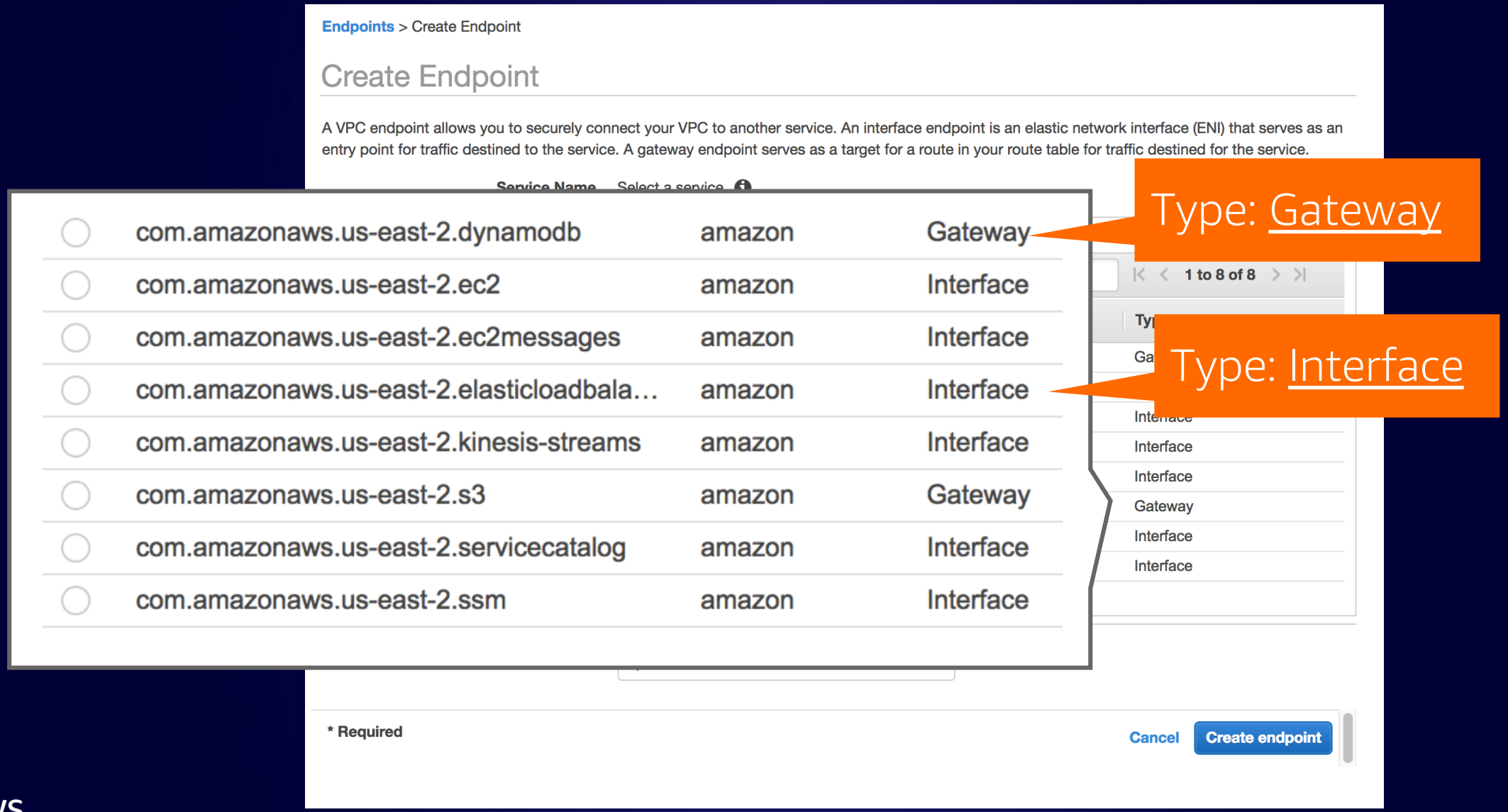


Tens of services now supported over AWS PrivateLink

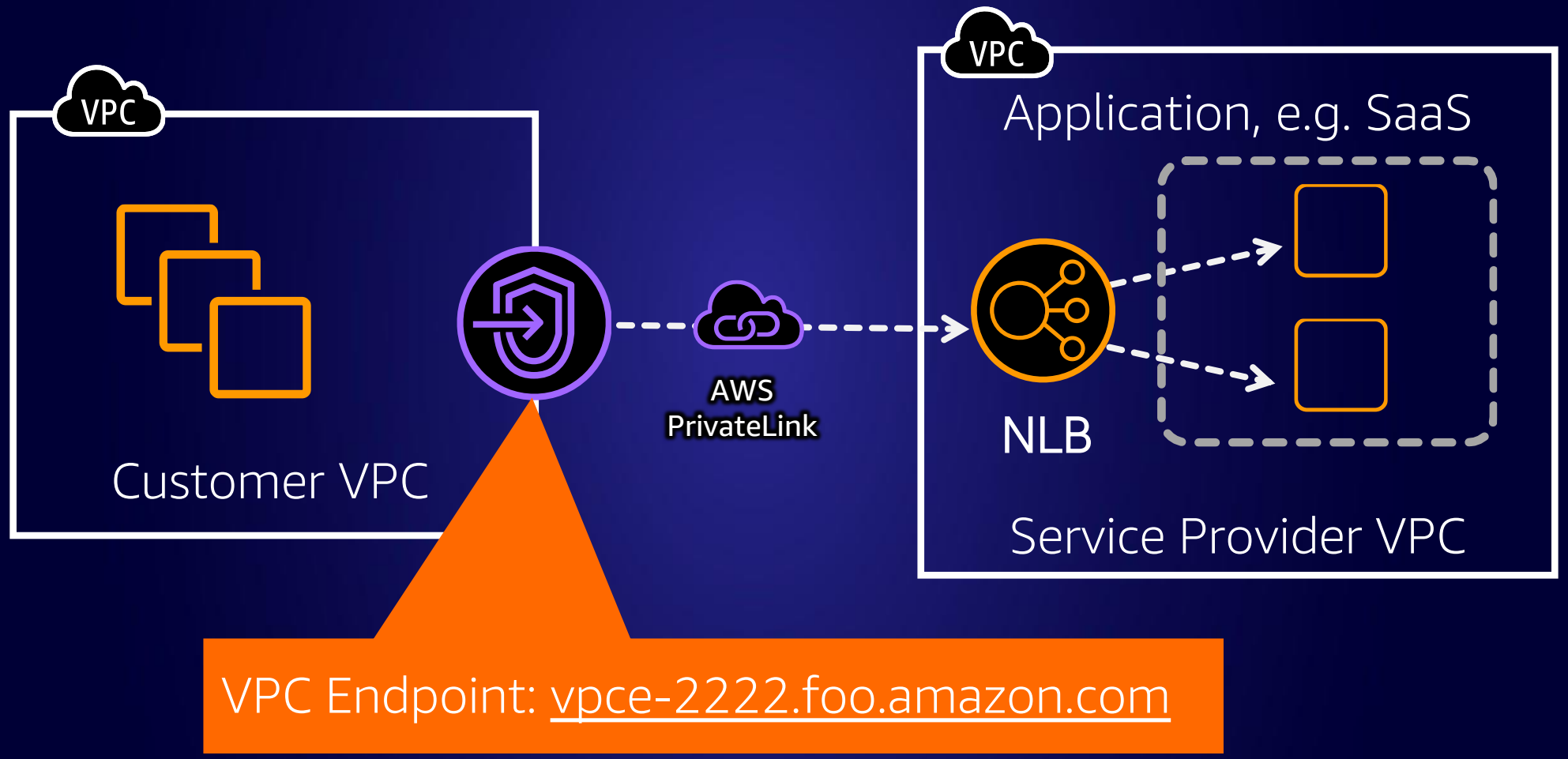
AWS PrivateLink can reach public services, privately from your VPC

No routes needed! (almost)

Amazon VPC endpoints console



AWS PrivateLink for service providers

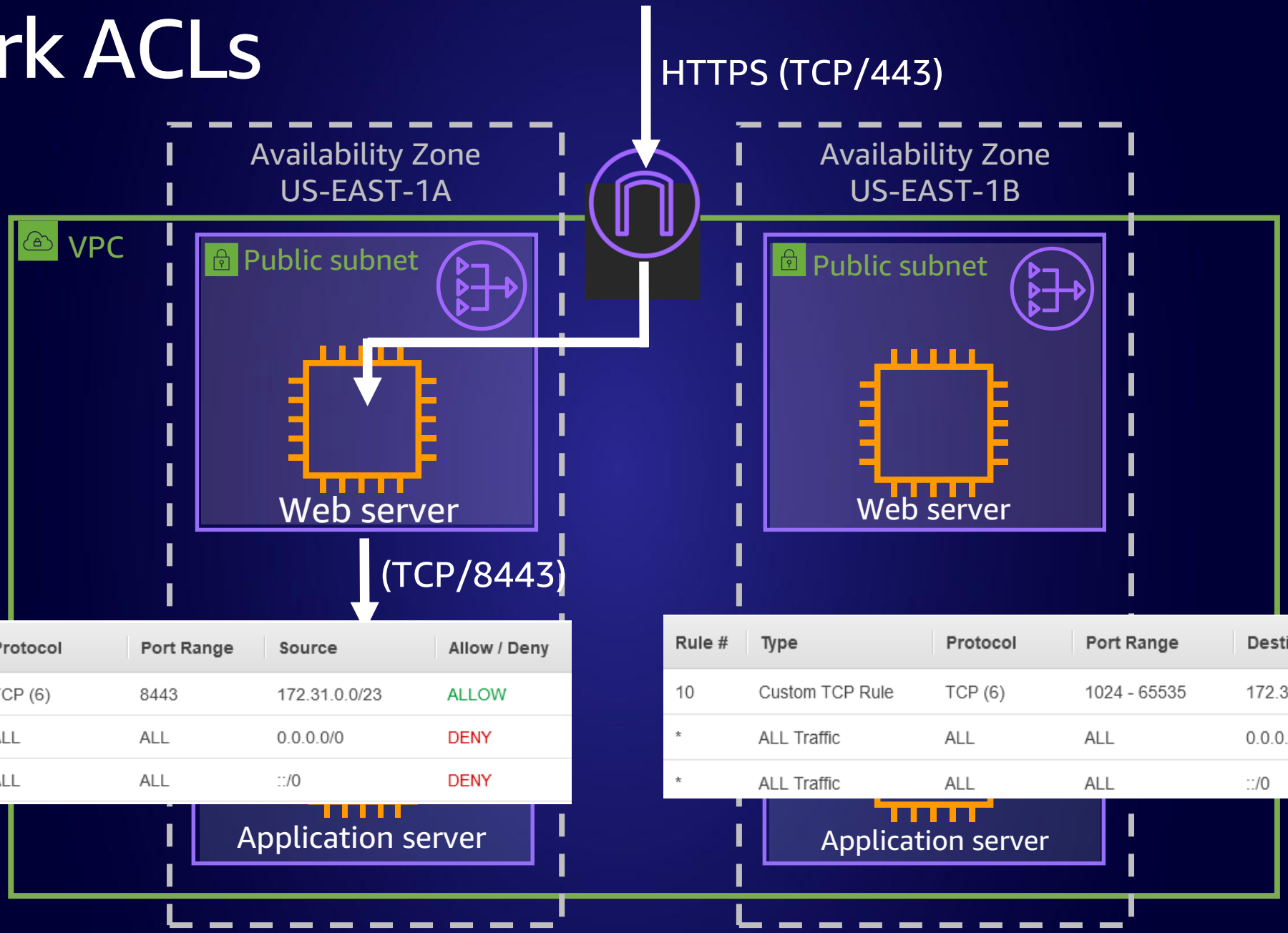


Network Security

Network ACLs

- Subnet based security
- L3/L4 Stateless
- Support ingress and egress rules
- Both “Allow” and “Deny” rules (order matters)
- Default: Allow All
- Limits:
  - Network ACLs per VPC: 200
  - Rules per network ACL: 20/40

Network ACLs



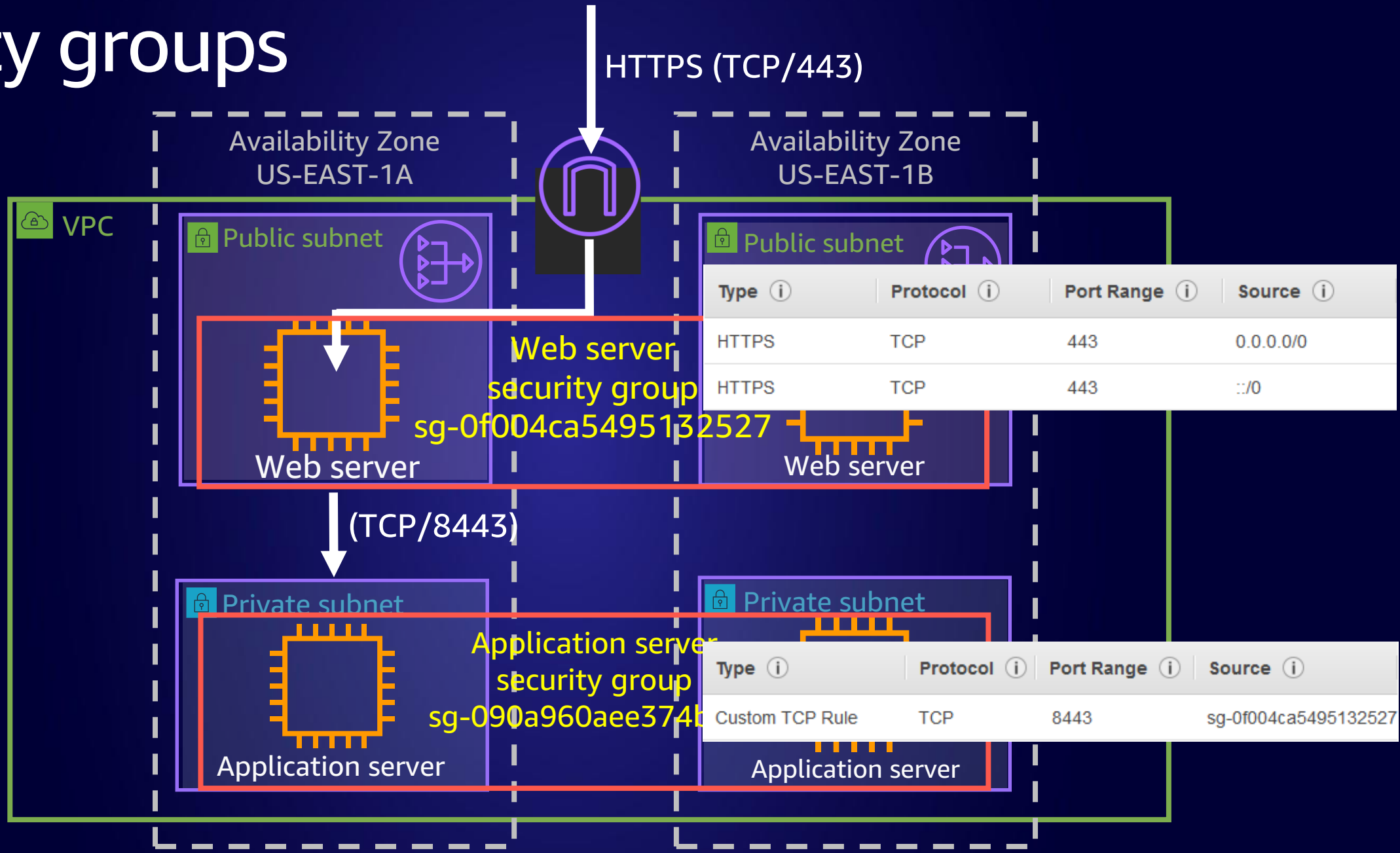
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
10	HTTPS* (8443)	TCP (6)	8443	172.31.0.0/23	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
10	Custom TCP Rule	TCP (6)	1024 - 65535	172.31.0.0/23	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Security groups

- Instance-level security
- Similar to host-based packet filter
- L3/L4 Stateful ⟷
- Only "Allow" rules (order irrelevant)
- Support ingress and egress rules
- Allow reference of other security groups
  - Abstract function from IP addresses
- Limits:
  - Security groups per ENI: 5
  - Rule per security group: 60

Security groups



Type	Protocol	Port Range	Source
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	::/0

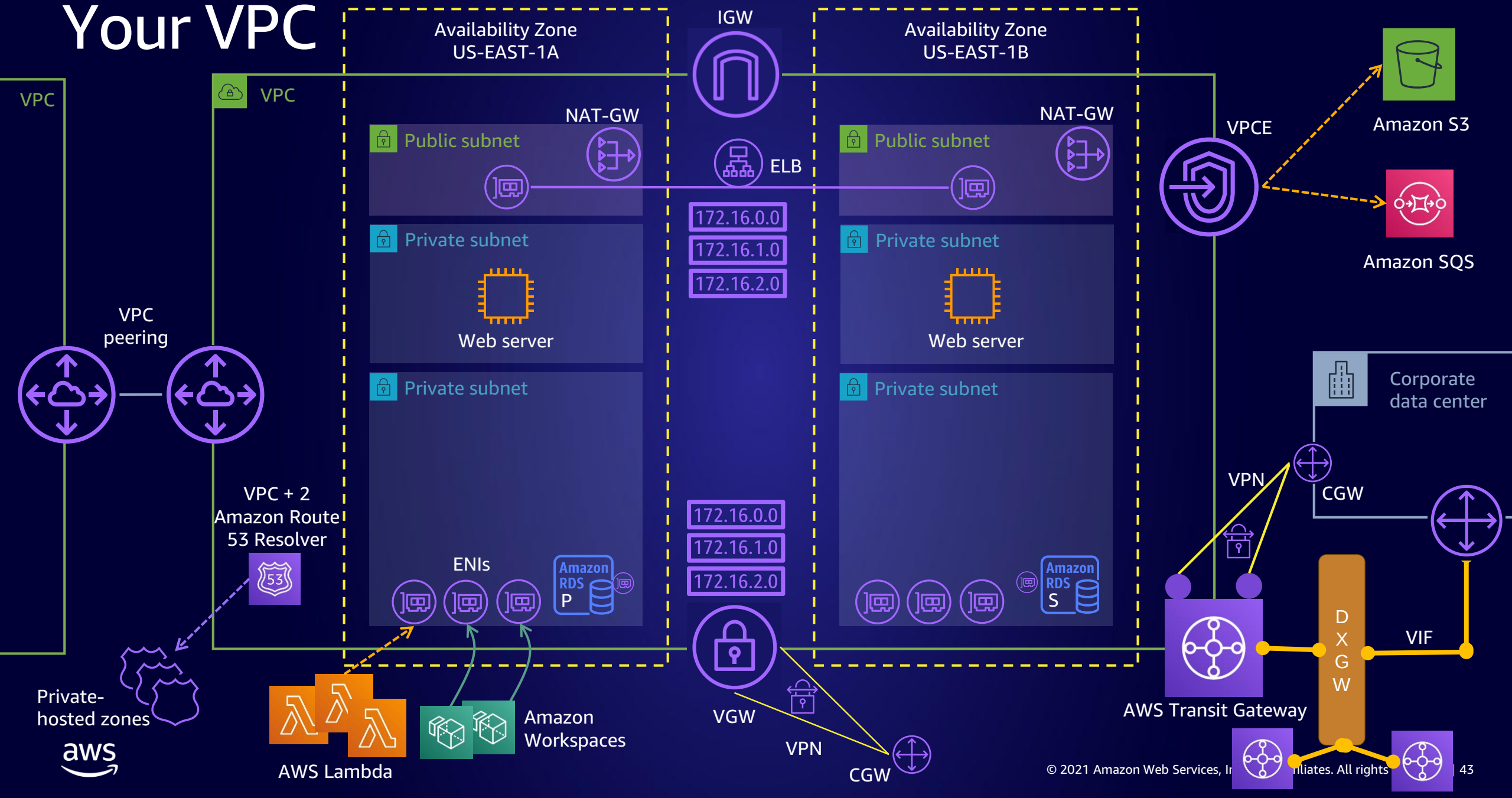
Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	8443	sg-0f004ca5495132527

Security groups versus NACLs

Security group	Network ACL
Operates at instance level	Operates at subnet level
Supports allow rules only	Supports allow and deny rules
Is stateful: return traffic is automatically allowed regardless of any rules	Is stateless: return traffic must be explicitly allowed by rules
All rules evaluated before deciding whether to allow traffic	Rules evaluated in order when deciding whether to allow traffic
Applies only to instances explicitly associated with the security group	Automatically applies to all instances launched into associated subnets
Doesn't filter traffic to or from link-local addresses (169.254.0.0/16) or AWS-reserved IPv4 addresses; these are the first four IPv4 addresses of the subnet (including the Amazon VPC DNS server)	

Bringing It All Together

Your VPC

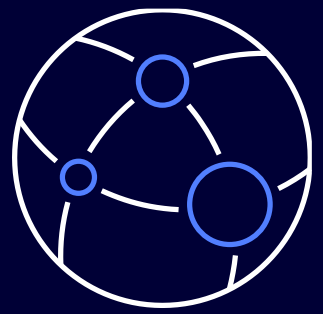


The famous from Amazon CTO Werner Vogels

“Everything fails, all the time”

Learn Networking with 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**

aws

Thank you!

Shih-Yong Wang

shihyong@amazon.com