
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

BOA101-R

Journey to cloud networking

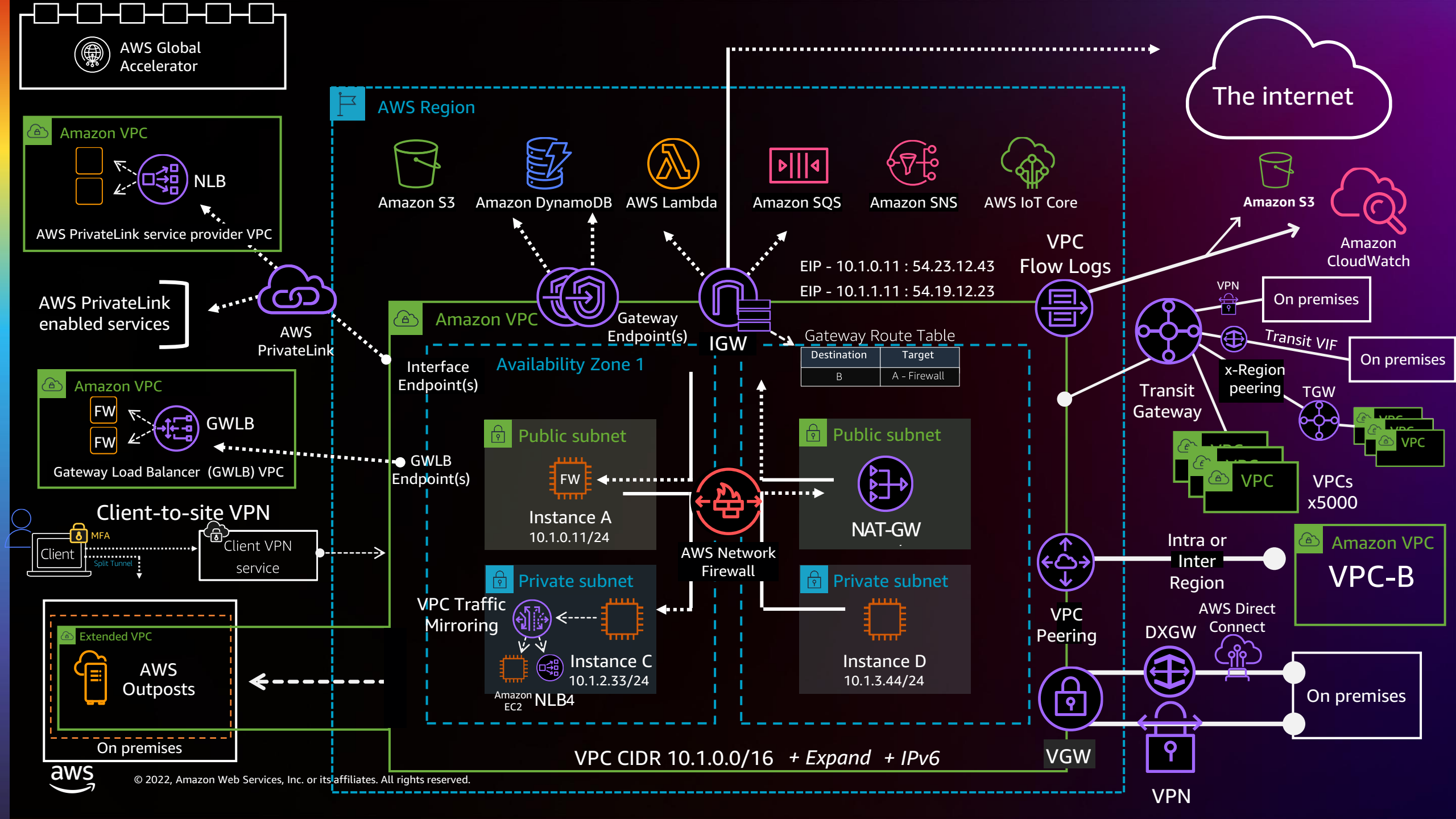
Viktor Vedmich

Senior Developer Advocate
AWS

Manish Dhawaria

Senior Solutions Architect
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


AWS Global Accelerator
AWS Region
The internet
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
x-Region peering
TGW
Transit Gateway
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
Client-to-site VPN
MFA
Client
Split Tunnel
Client VPN service
AWS Network Firewall
Private subnet
VPC Traffic Mirroring
Instance C
10.1.2.33/24
Amazon EC2
NLB4
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
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

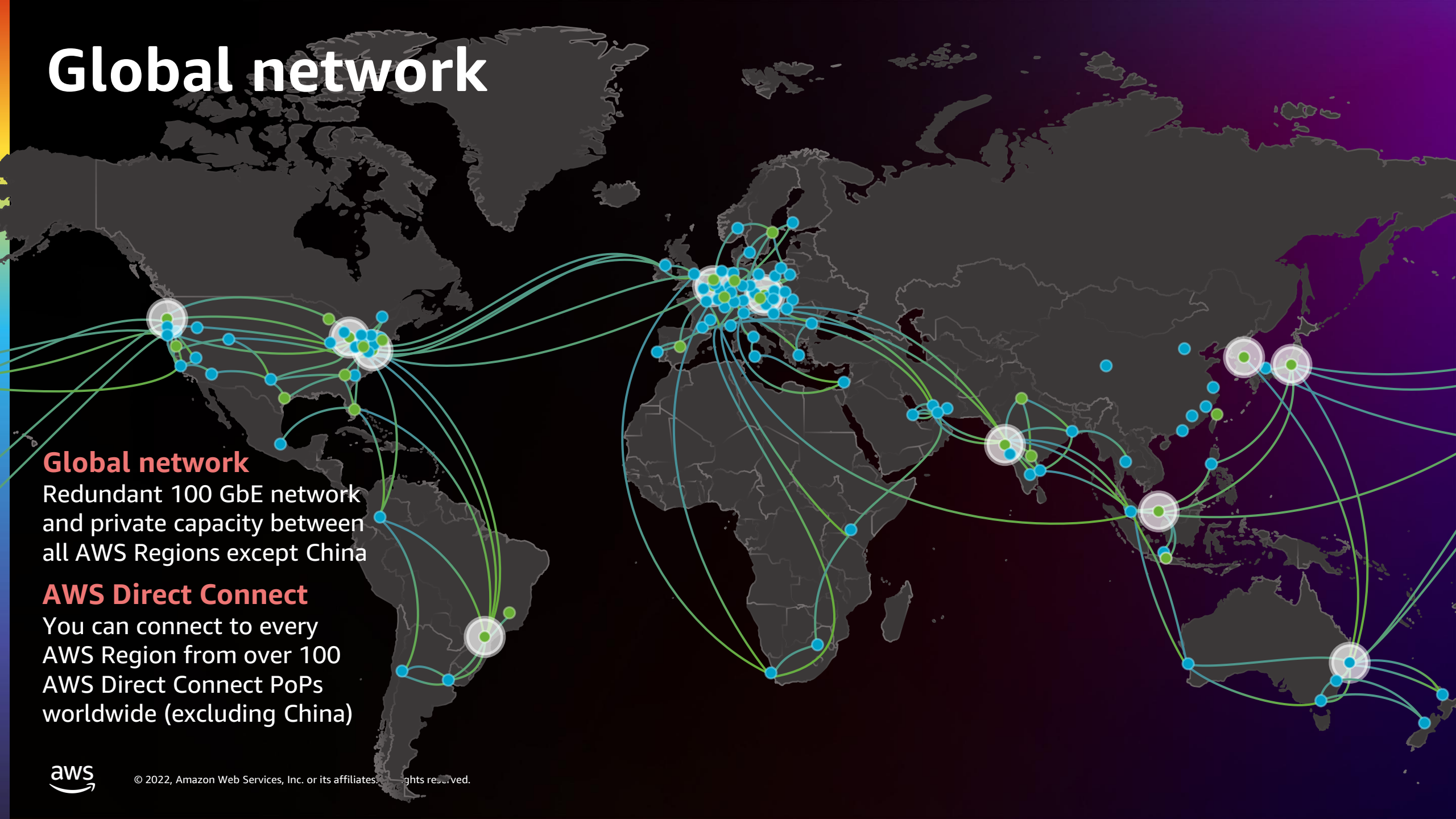
- Global infrastructure
- Amazon Virtual Private Cloud (Amazon VPC) concepts
- Basics of VPC security
- Peering, endpoints, gateways, and global connectivity
- Traffic visibility and monitoring

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global infrastructure

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



Global network

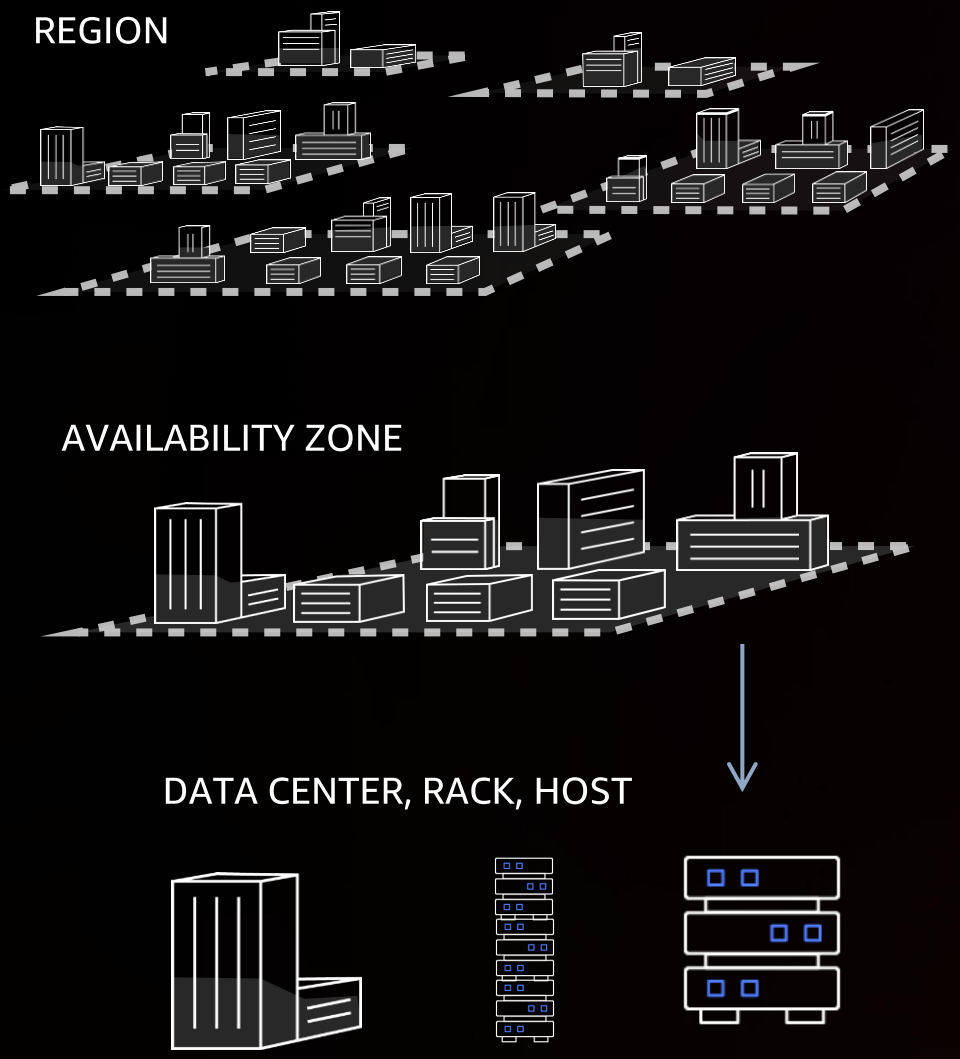
Redundant 100 GbE network and private capacity between all AWS Regions except China

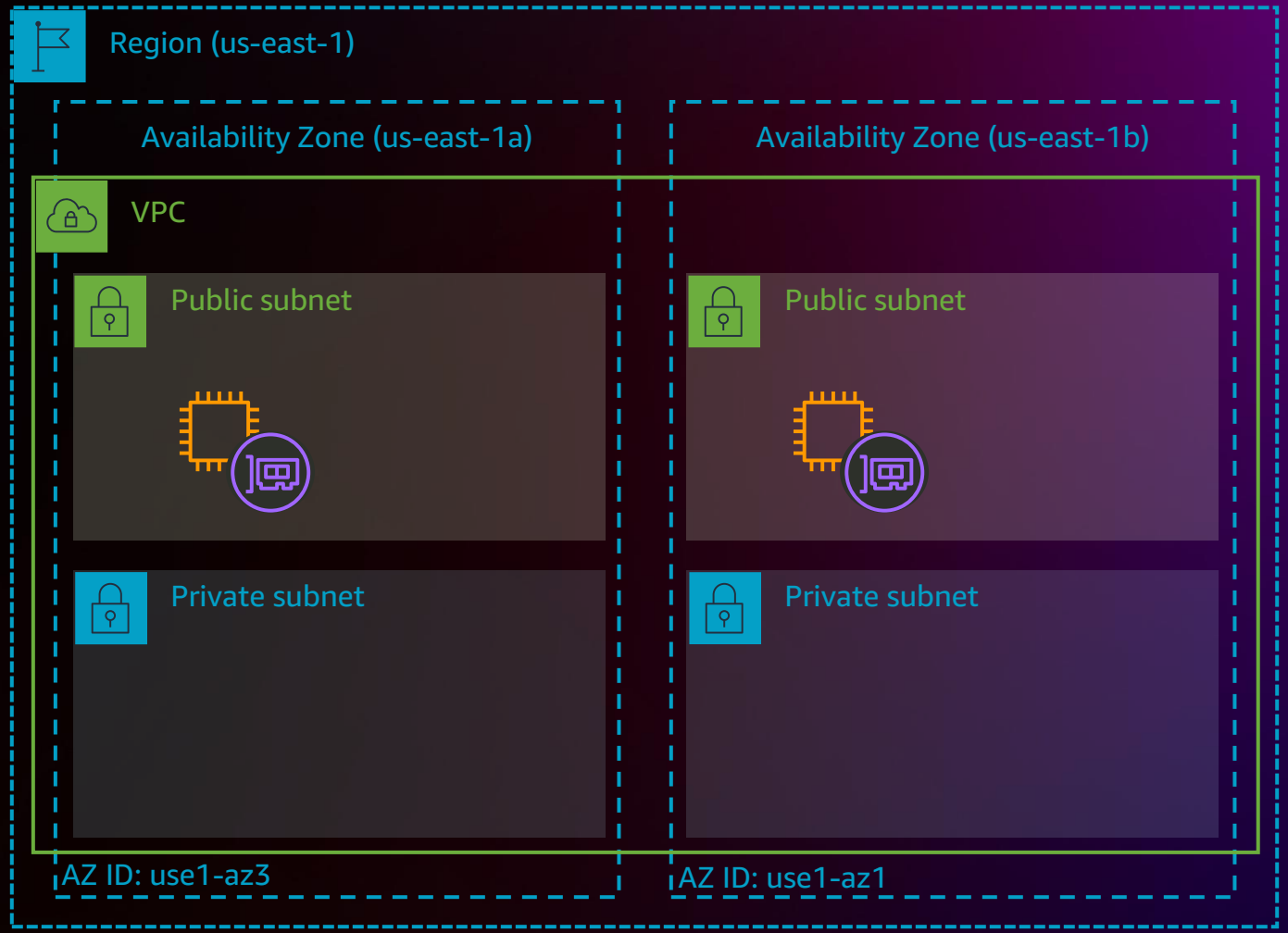
AWS Direct Connect

You can connect to every AWS Region from over 100 AWS Direct Connect PoPs worldwide (excluding China)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Building a VPC





aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting up an internet-connected VPC

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

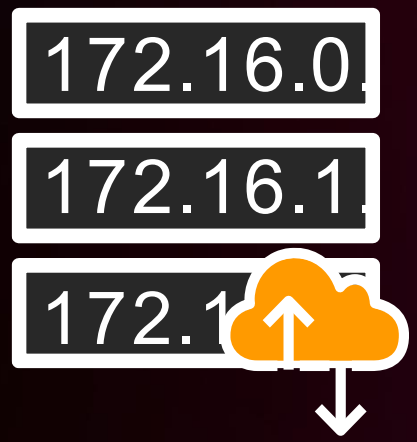
Steps for creating an internet-connected VPC



Choosing an address range



Creating subnets in Availability Zones



Creating a route to the internet



Security

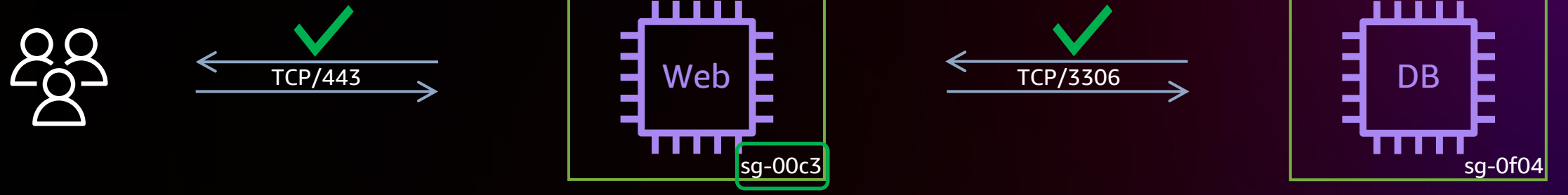
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security groups



IP version	Type	Protocol	Port range	Source
IPv4	HTTPS	TCP	443	0.0.0.0/0
IPv6	HTTPS	TCP	443	::/0
–	All traffic	All	All	sg-00c3



IP version	Type	Protocol	Port range	Source
–	MYSQL/Aurora	TCP	3306	sg-00c3
–	All traffic	TCP	All	sg-0f04

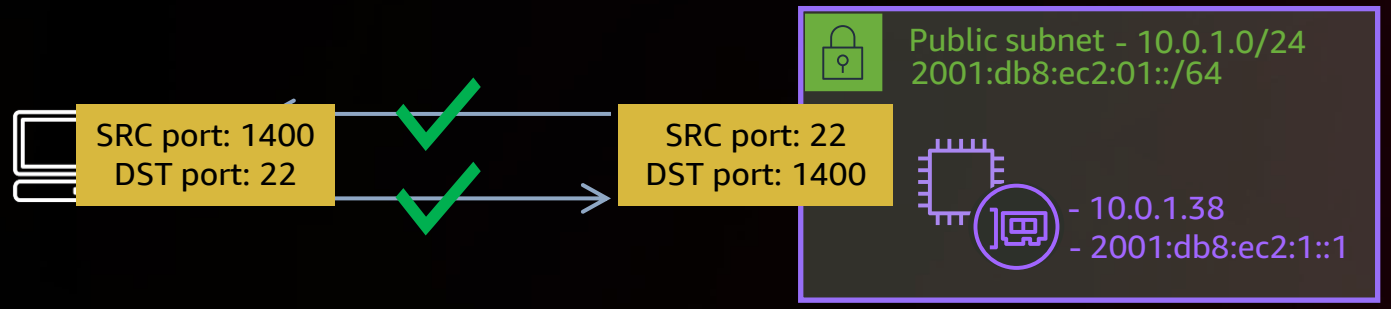
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network access control lists (NACLs)



Inbound

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny



Outbound

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Connectivity options for VPCs

Peering, endpoints, gateways, and global connectivity

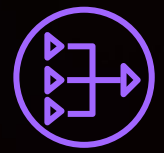
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Peering, endpoints, gateways, and global connectivity


AWS Client VPN


Virtual private gateway


Direct Connect Gateway


NAT gateway


Internet gateways


AWS Transit Gateway


Endpoints

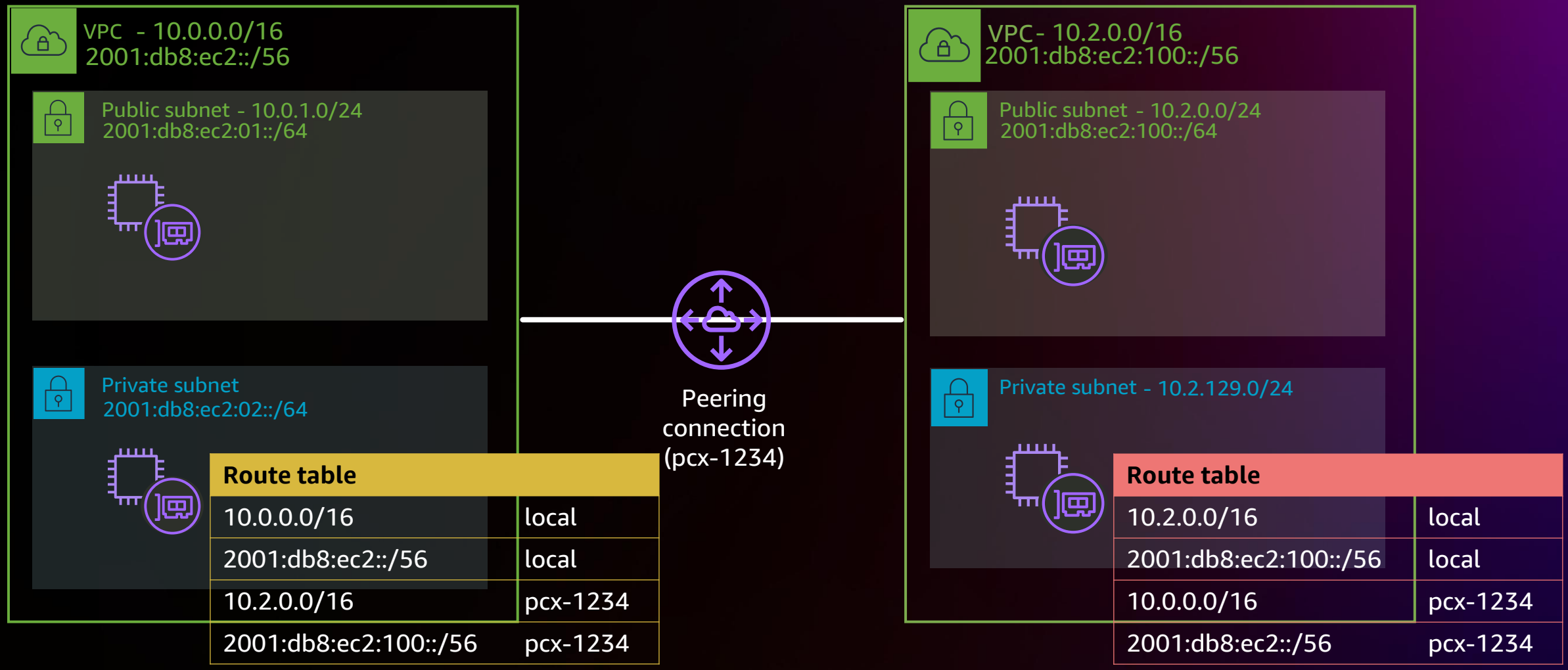

Peering connection


AWS Cloud WAN

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC peering

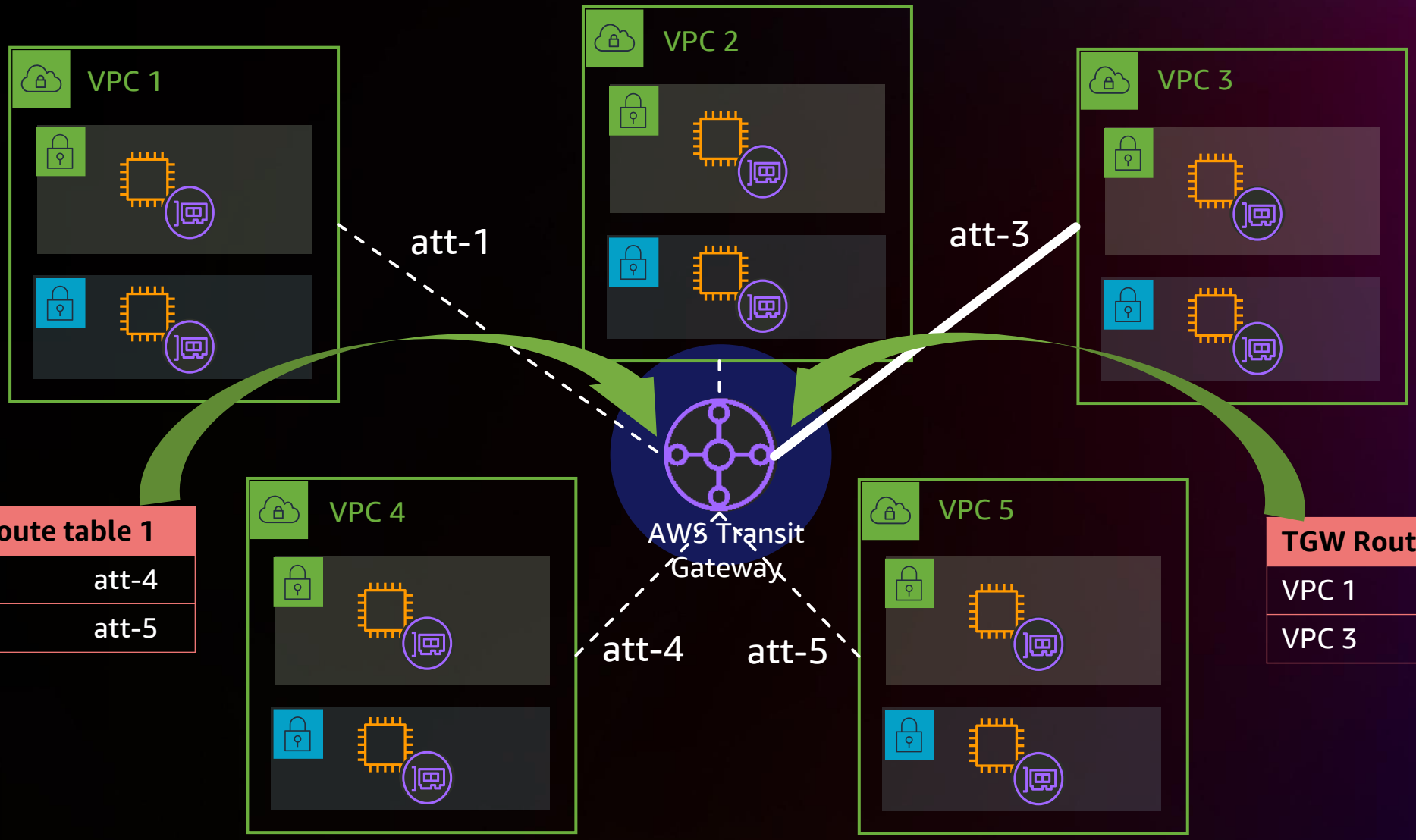


Route table	
10.0.0.0/16	local
2001:db8:ec2::/56	local
10.2.0.0/16	pcx-1234
2001:db8:ec2:100::/56	pcx-1234

Route table	
10.2.0.0/16	local
2001:db8:ec2:100::/56	local
10.0.0.0/16	pcx-1234
2001:db8:ec2::/56	pcx-1234

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway (single Region)

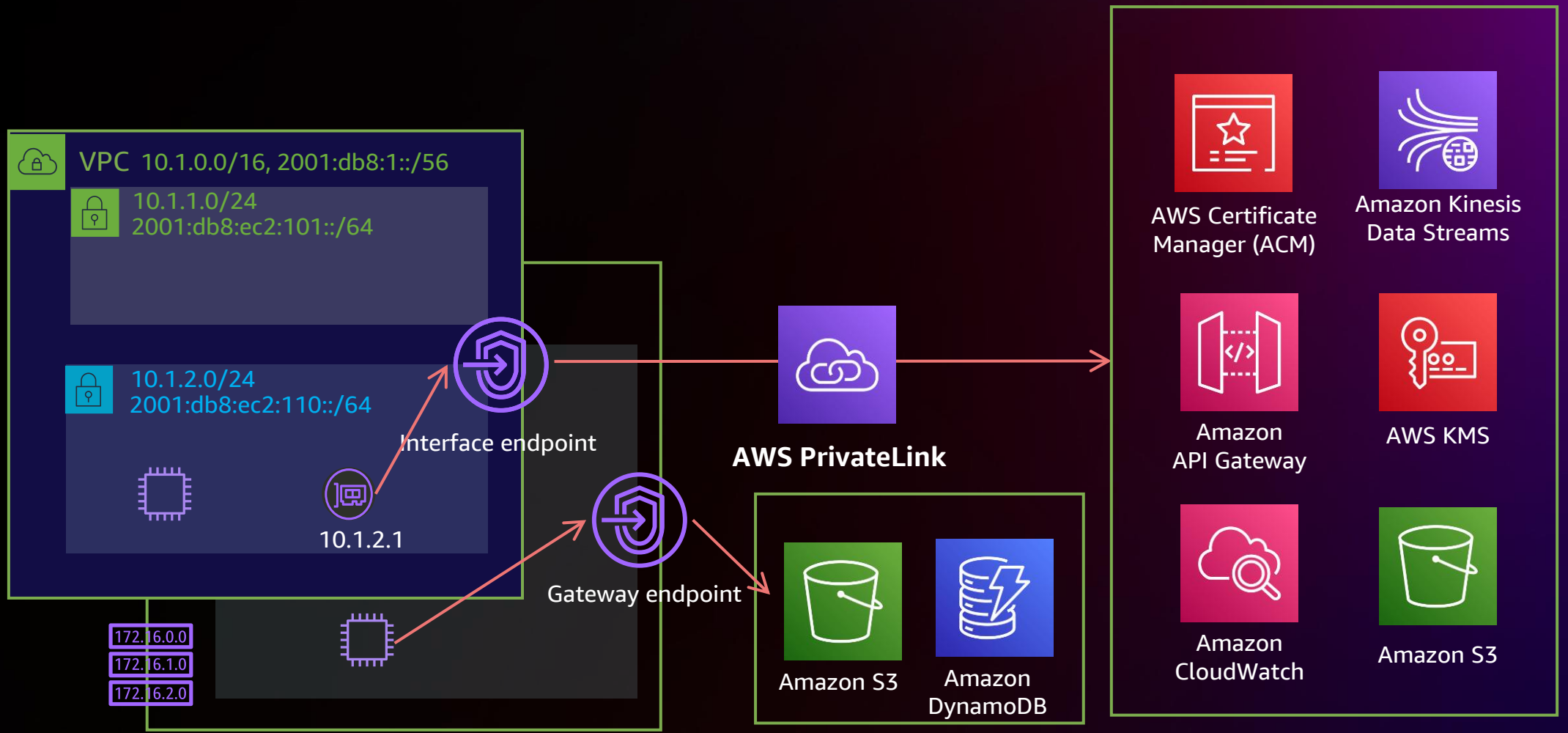


TGW Route table 1	
VPC 4	att-4
VPC 5	att-5

TGW Route table 2	
VPC 1	att-1
VPC 3	att-3

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC gateway endpoints



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hybrid connectivity



AWS Direct Connect



AWS Site-to-Site VPN



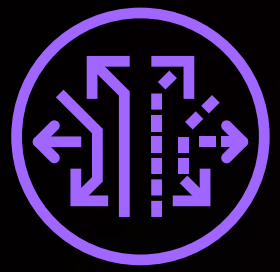
AWS Client VPN

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traffic visibility and monitoring

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traffic visibility options and use cases



Amazon VPC Traffic Mirroring

- Diagnosing overly restrictive security group rules
- Monitoring the traffic that is reaching your instance
- Determining the direction of the traffic to and from the network interfaces
- Copies network traffic, including payload

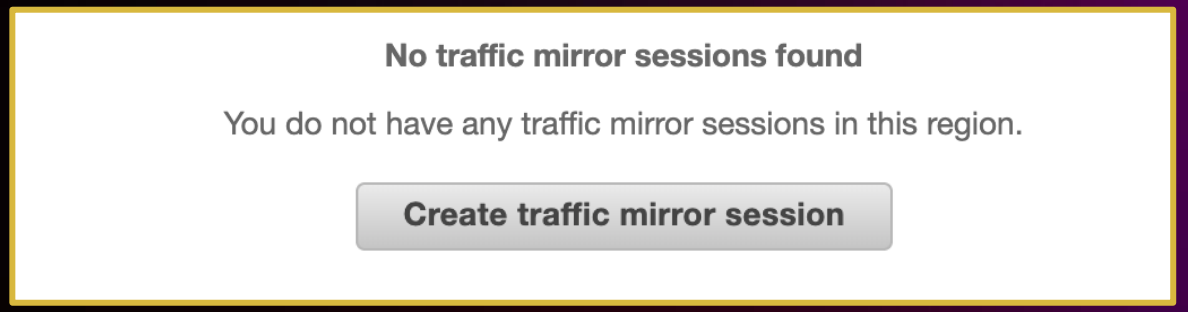


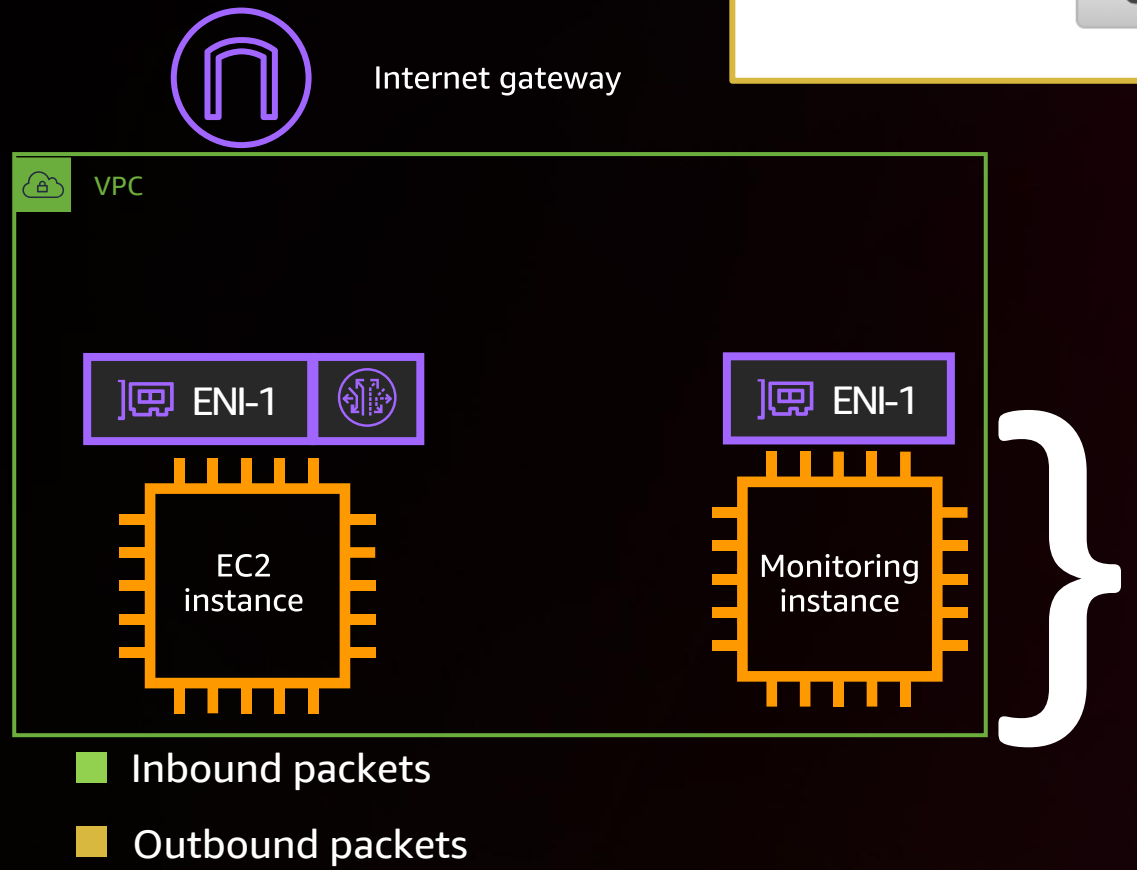
Amazon VPC Flow Logs

- Content inspection
- Threat monitoring
- Troubleshooting
- Collect and store header information

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Traffic Mirroring





Build your own traffic analyzer

Open-source traffic analysis

AWS Traffic Mirroring Partners

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure monitoring



CloudWatch metrics

Automatically collects default metrics from more than 70 AWS services



CloudWatch alarms

Allows you to set a threshold on metrics and trigger an action

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.