# AWS re:Invent

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

NET201

# Networking foundations

Alan Halachmi
Director, Solutions Architecture, WWPS
Amazon Web Services

Madhura Kale
Principal Product Manager, Amazon EC2
Amazon Web Services

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

# Agenda

Global infrastructure

Amazon Virtual Private Cloud (Amazon VPC)

Basics of VPC security

Peering, endpoints, and gateways

Load balancing and traffic management

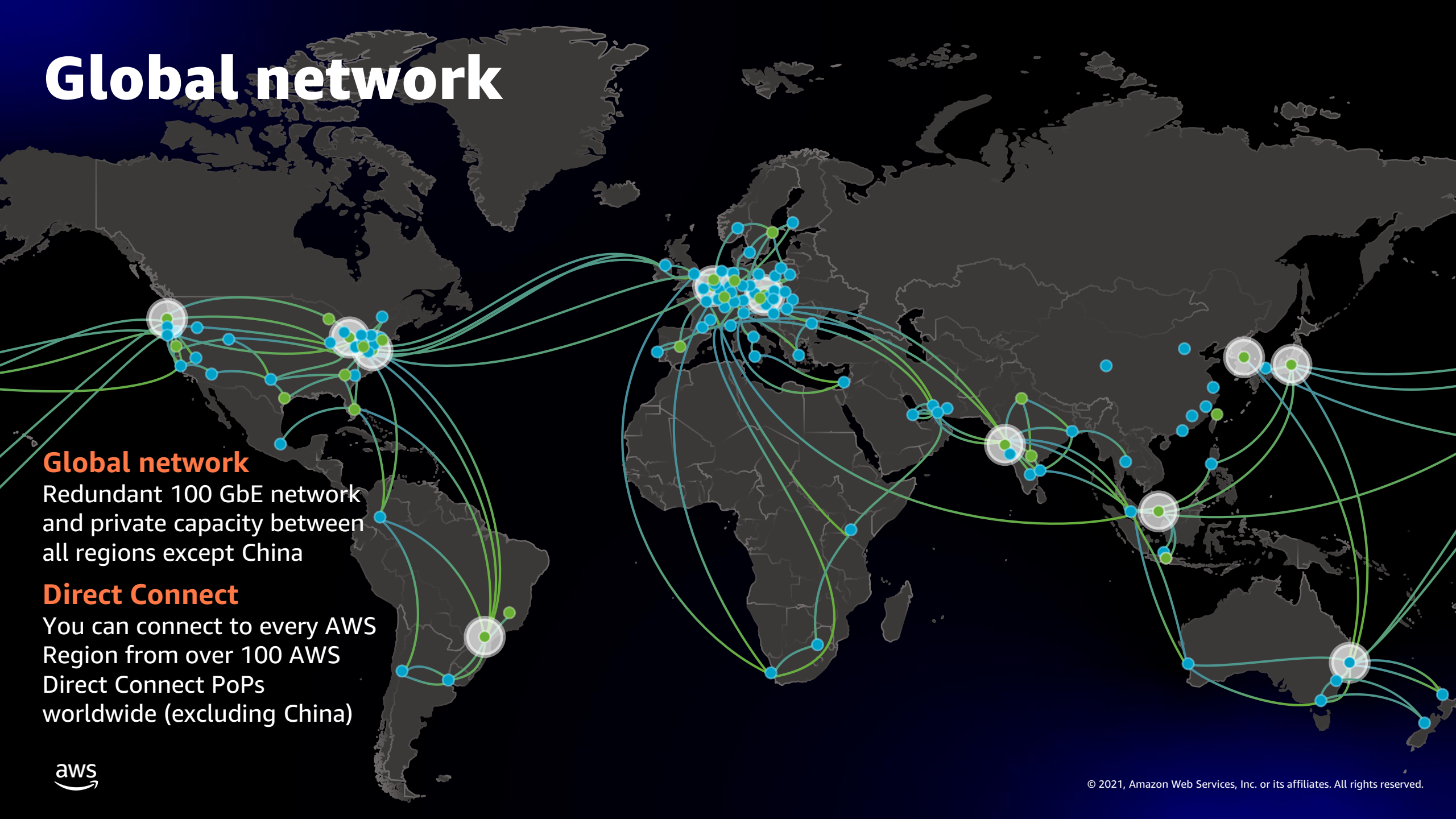
Security services

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

# Global infrastructure

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

# Global network



## Global network

Redundant 100 GbE network and private capacity between all regions except China

## Direct Connect

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

aws

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

# AWS global infrastructure

25 GEOGRAPHICAL REGIONS, 81 AVAILABILITY ZONES, 275+ POPS

## Region & number of Availability Zones (AZs)

**GovCloud (U.S.)**
U.S.-East (3), US-West (3)

**U.S. West**
Oregon (4)
Northern California (3)

**U.S. 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), Jakarta (3),
Tokyo (4), Osaka (3)
Seoul (4), Mumbai (3), Hong Kong (3)

**China**
Beijing (2), Ningxia (3)

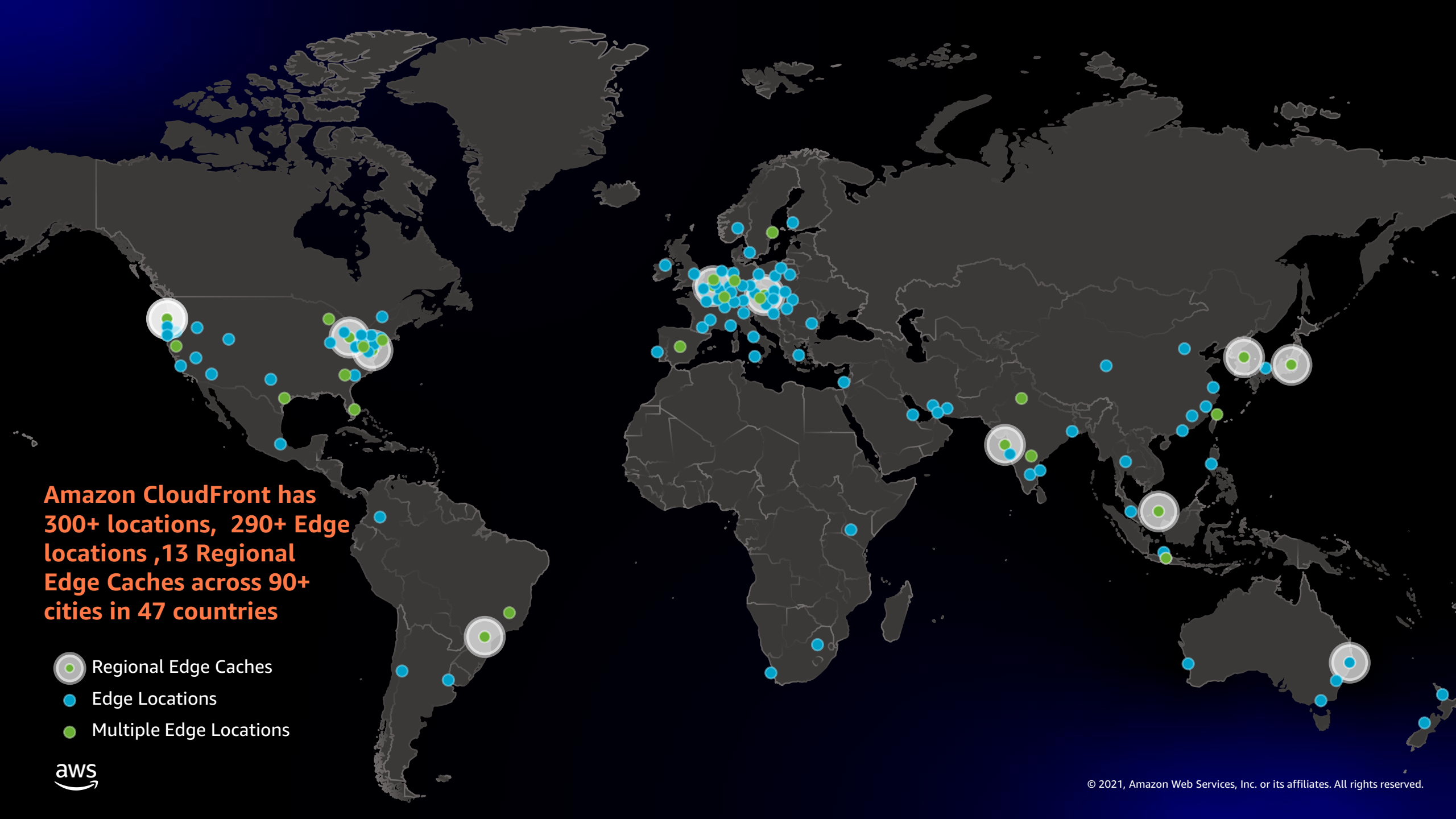


## Announced Regions

8 Regions and 24 AZs in Australia, Canada, India, Indonesia, Israel, Australia, Switzerland, Spain, and United Arab Emirates (UAE)

aws

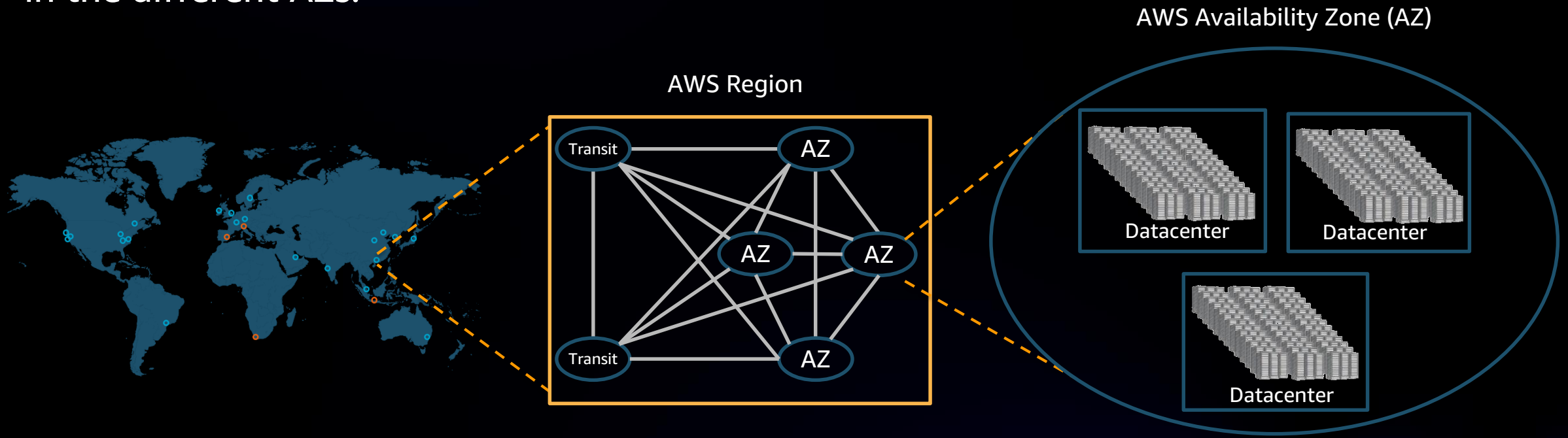
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.




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

# AWS Region design

AWS Regions are composed 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.



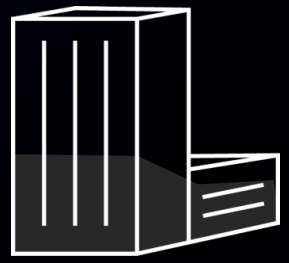

**A Region** is a physical location in the world where we have multiple **Availability Zones.**

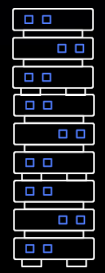
**Availability Zones** consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

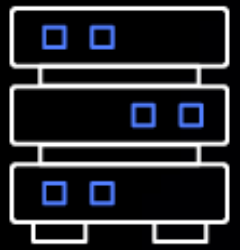
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

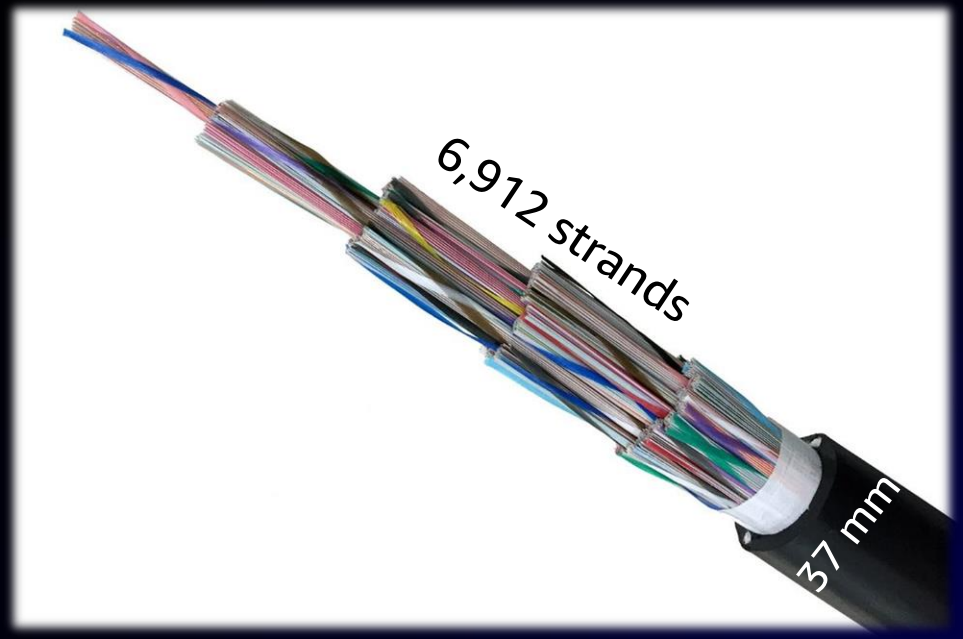
# Data centers

DATA CENTER, RACK, HOST










aws

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

# Cloud continuum

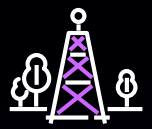
**AWS Regions**



On premises



Metro centers



5G networks

IoT



Rugged edge

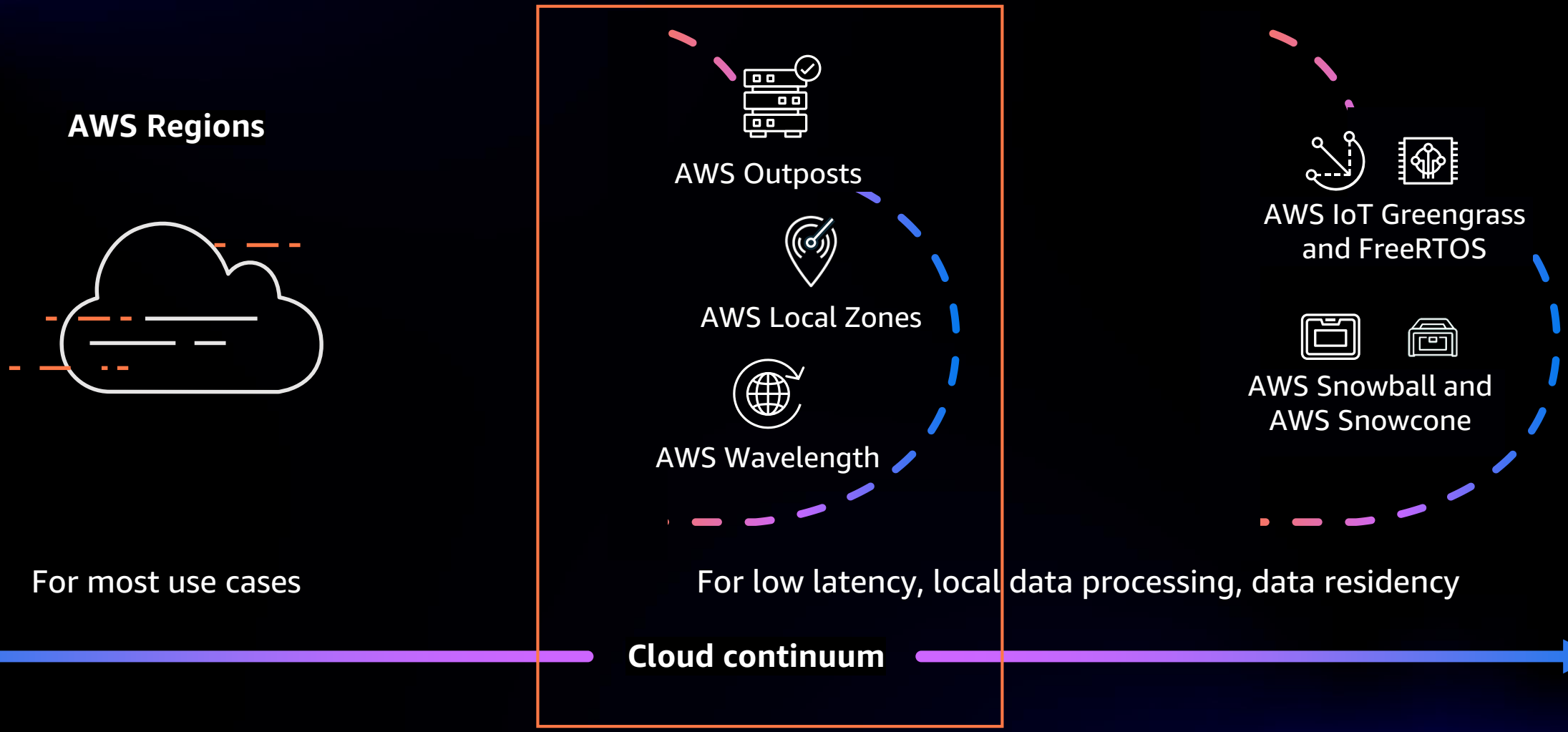
For most use cases

For low latency, local data processing, data residency




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

# Bringing the cloud to where you need it



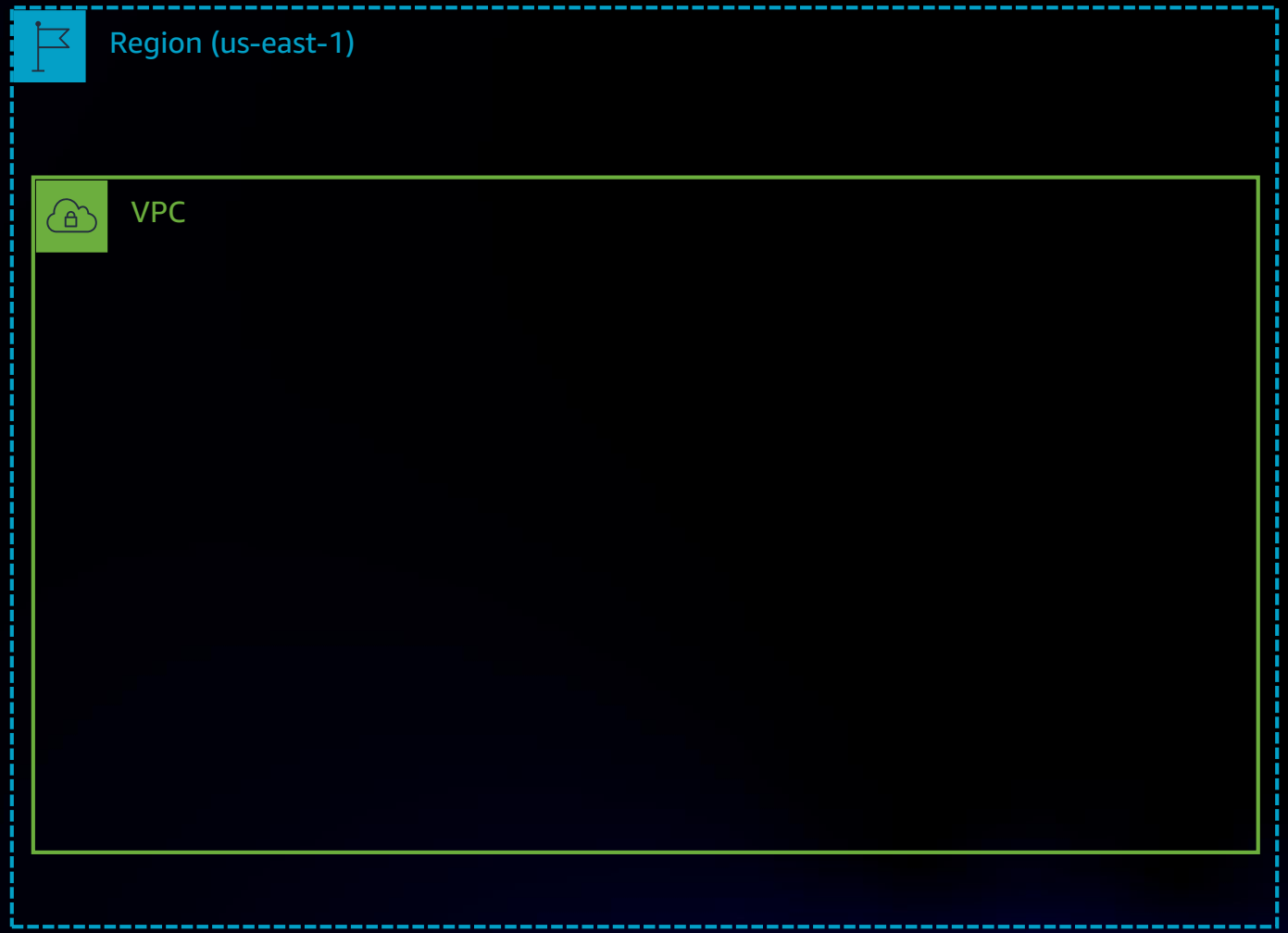

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon Virtual Private Cloud (Amazon VPC)

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

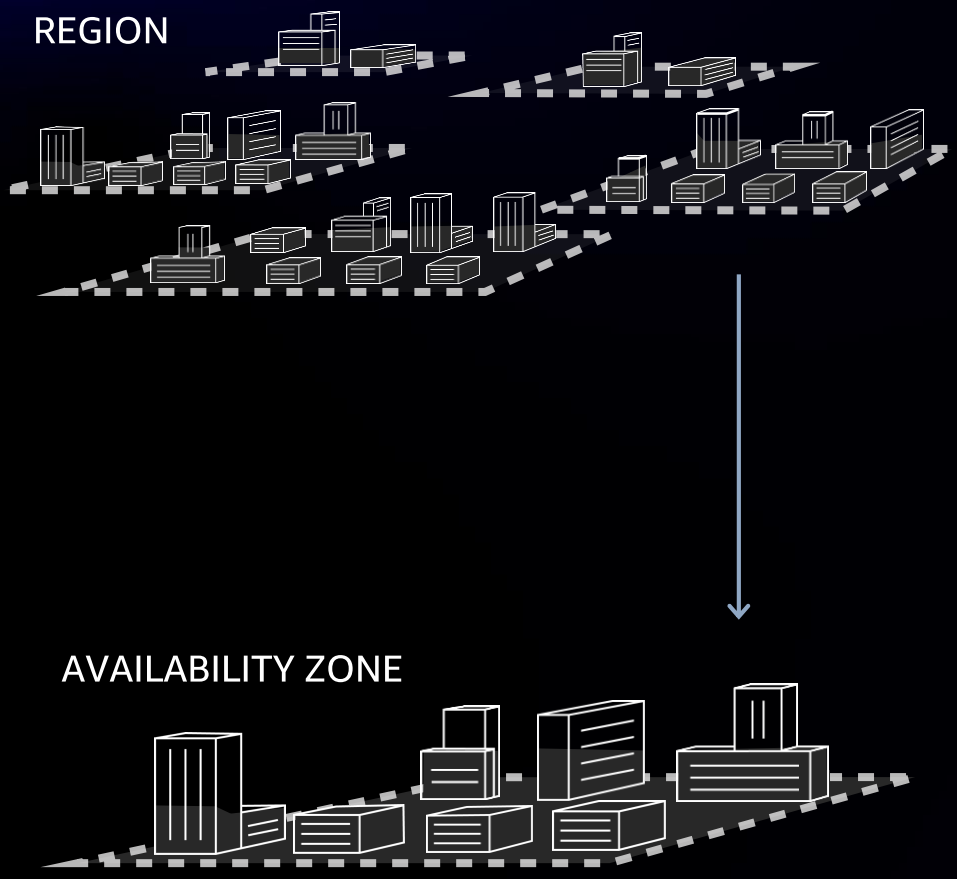
# Building a VPC

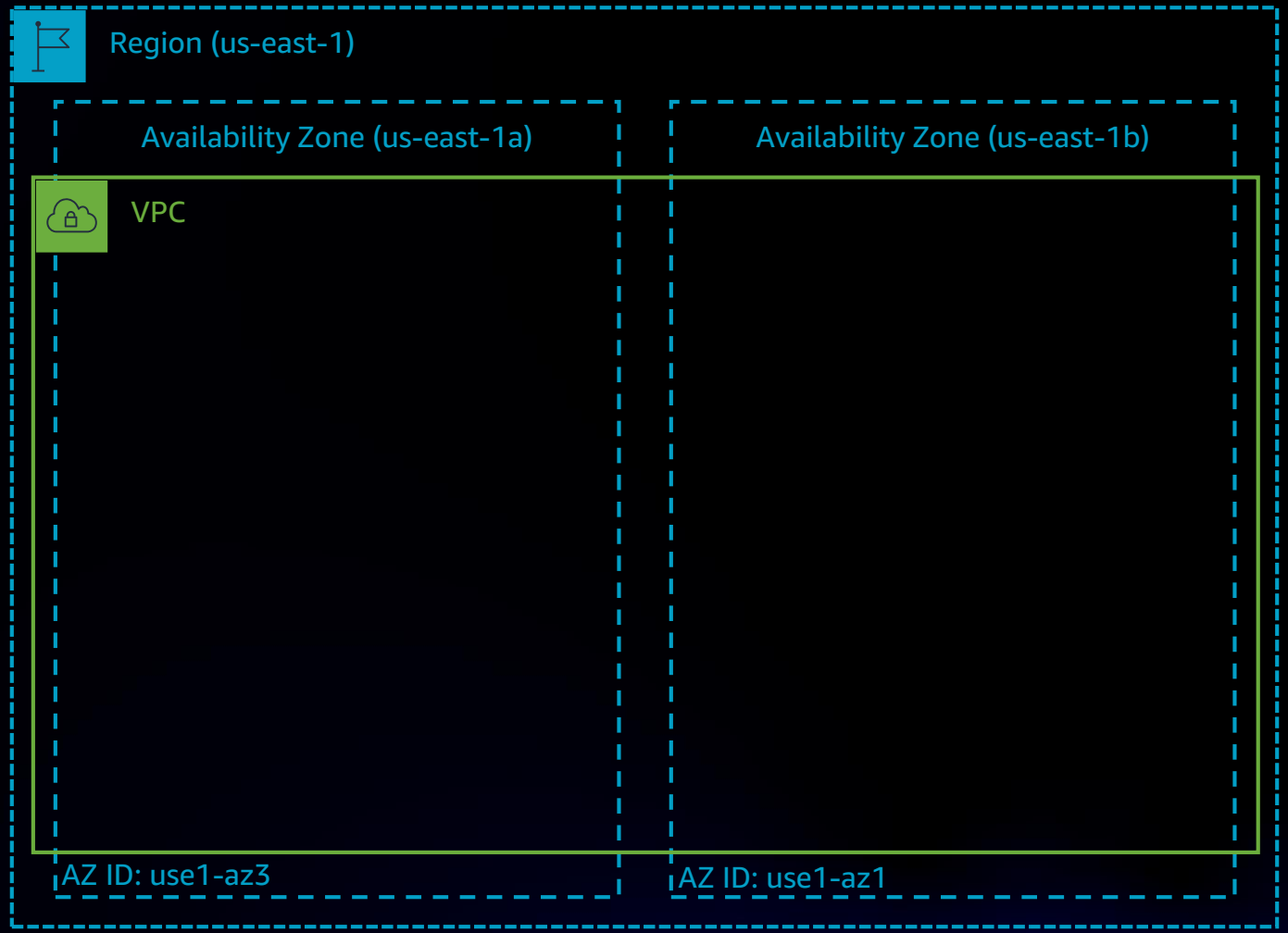



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Building a VPC

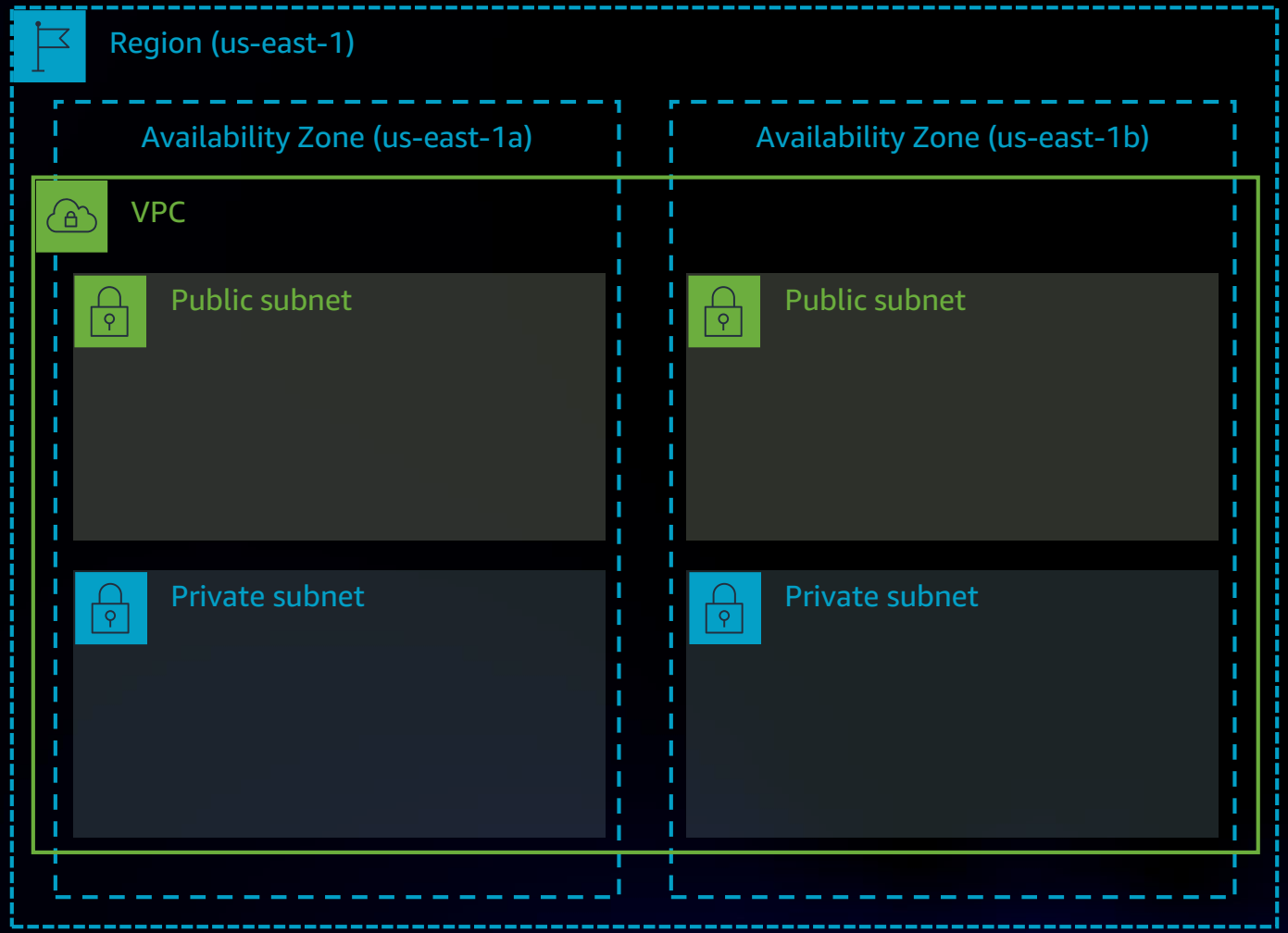



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

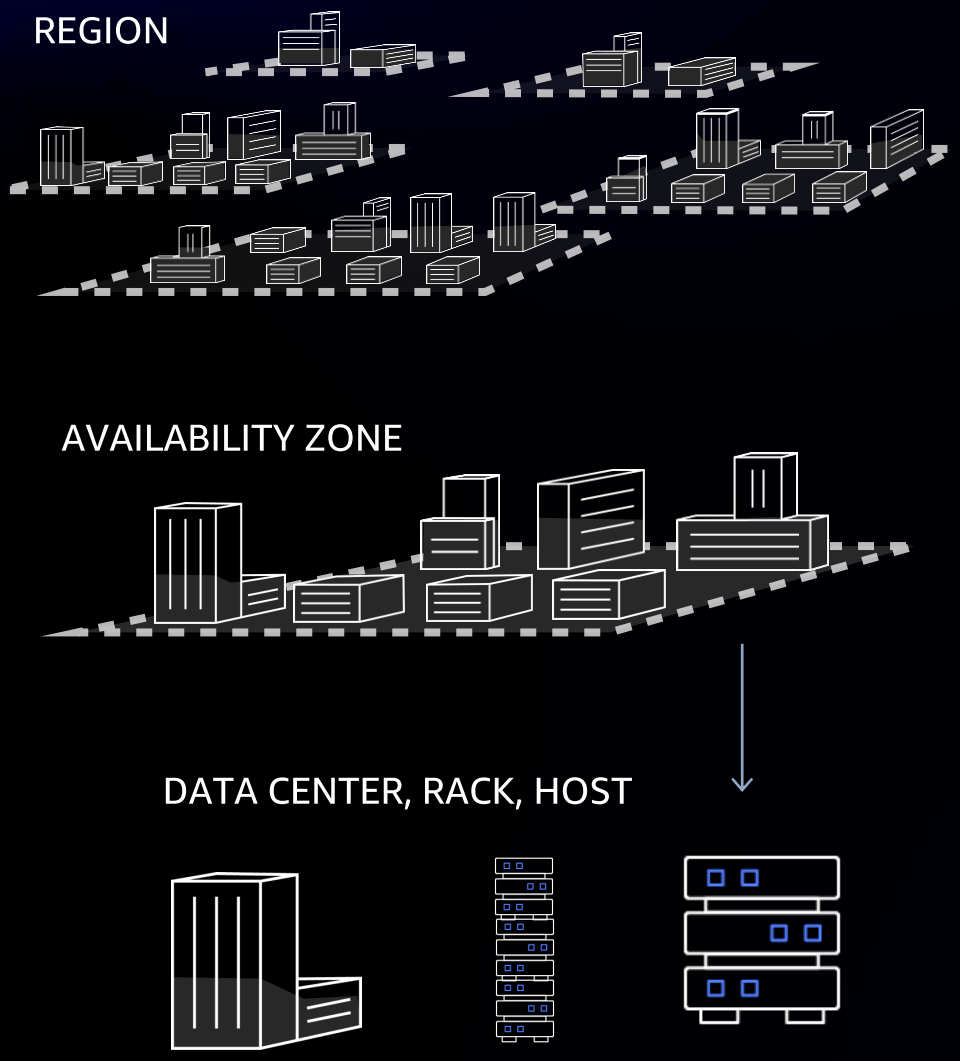
# Building a VPC




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

# Building a VPC







aws

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

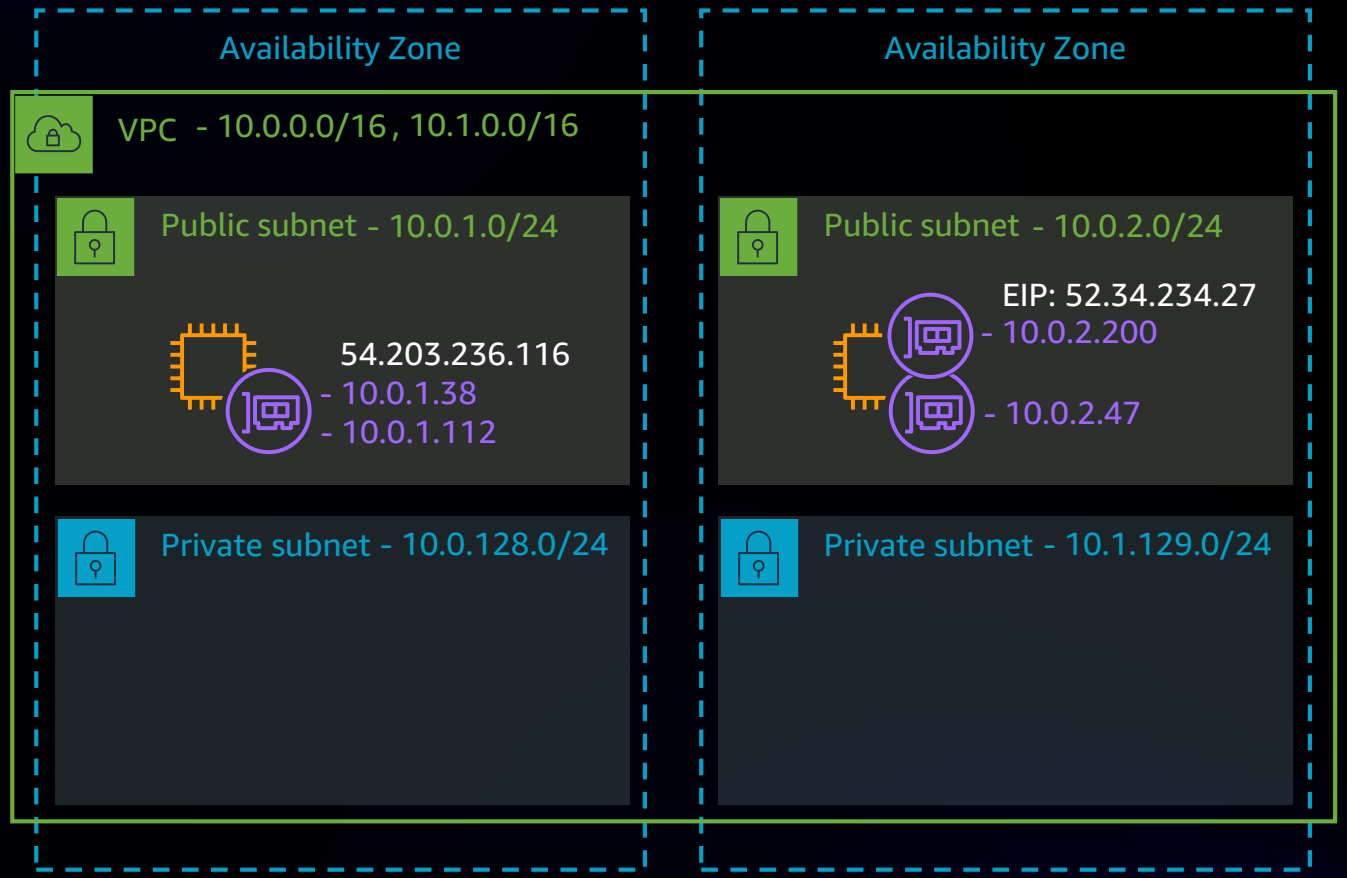
# IPv4 addressing

Reserved
10.0.0.0 – VPC Base
+ 2
---
10.0.0.2 – Route 53 Resolver

10.0.1.0 – Network Address
10.0.1.1 – VPC Router
10.0.1.2 – Reserved
10.0.1.3 – Reserved
10.0.1.255 – Network Broadcast

. . .

10.0.128.0 – Network Address
10.0.128.1 – VPC Router
10.0.128.2 – Reserved
10.0.128.3 – Reserved
10.0.128.255 – Network Broadcast




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

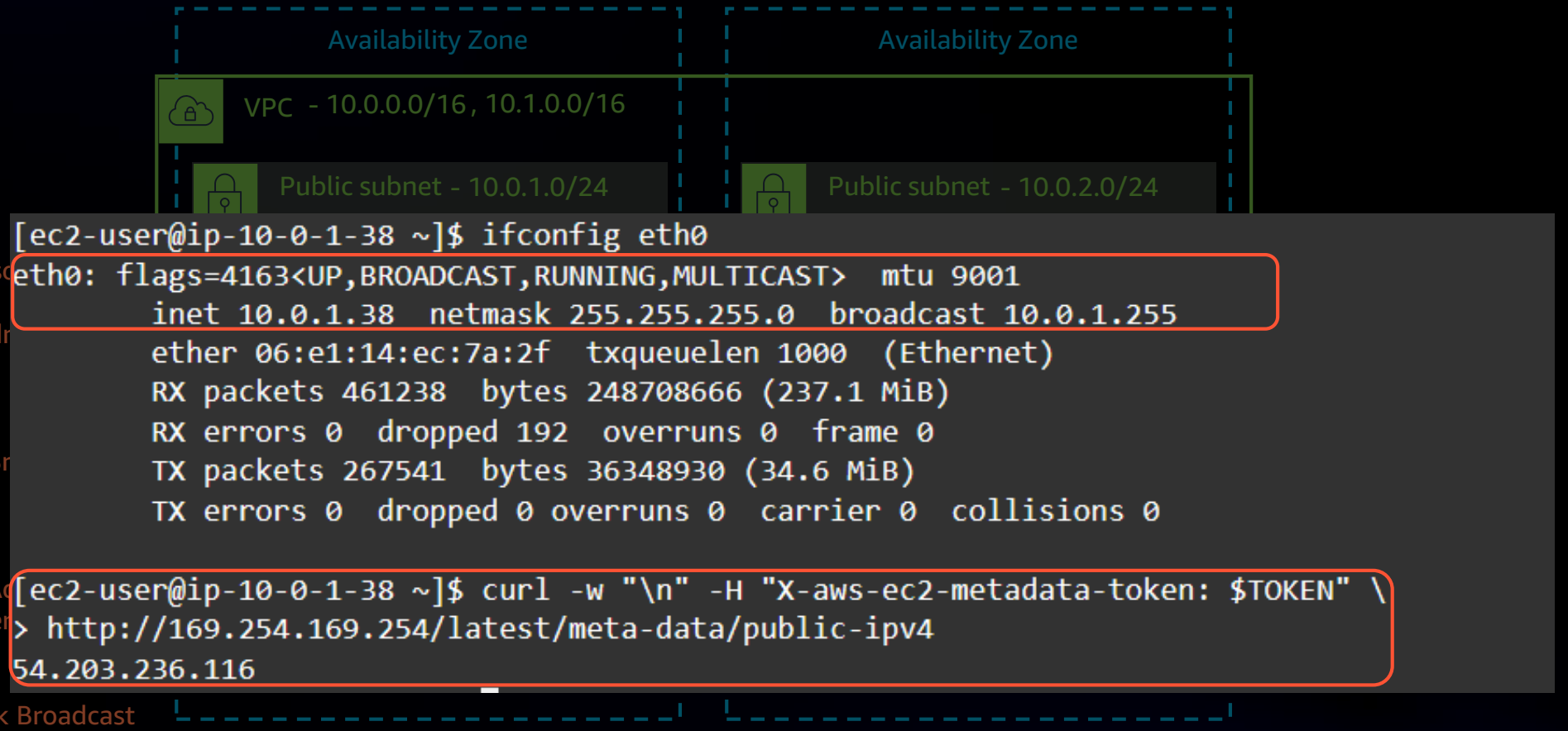
# IPv4 addressing

Reserved
10.0.0.0 – VPC Base
+ 2
---
10.0.0.2 – Route 53 Reso

10.0.1.0 – Network Addr
10.0.1.1 – VPC Router
10.0.1.2 – Reserved
10.0.1.3 – Reserved
10.0.1.255 – Network Br

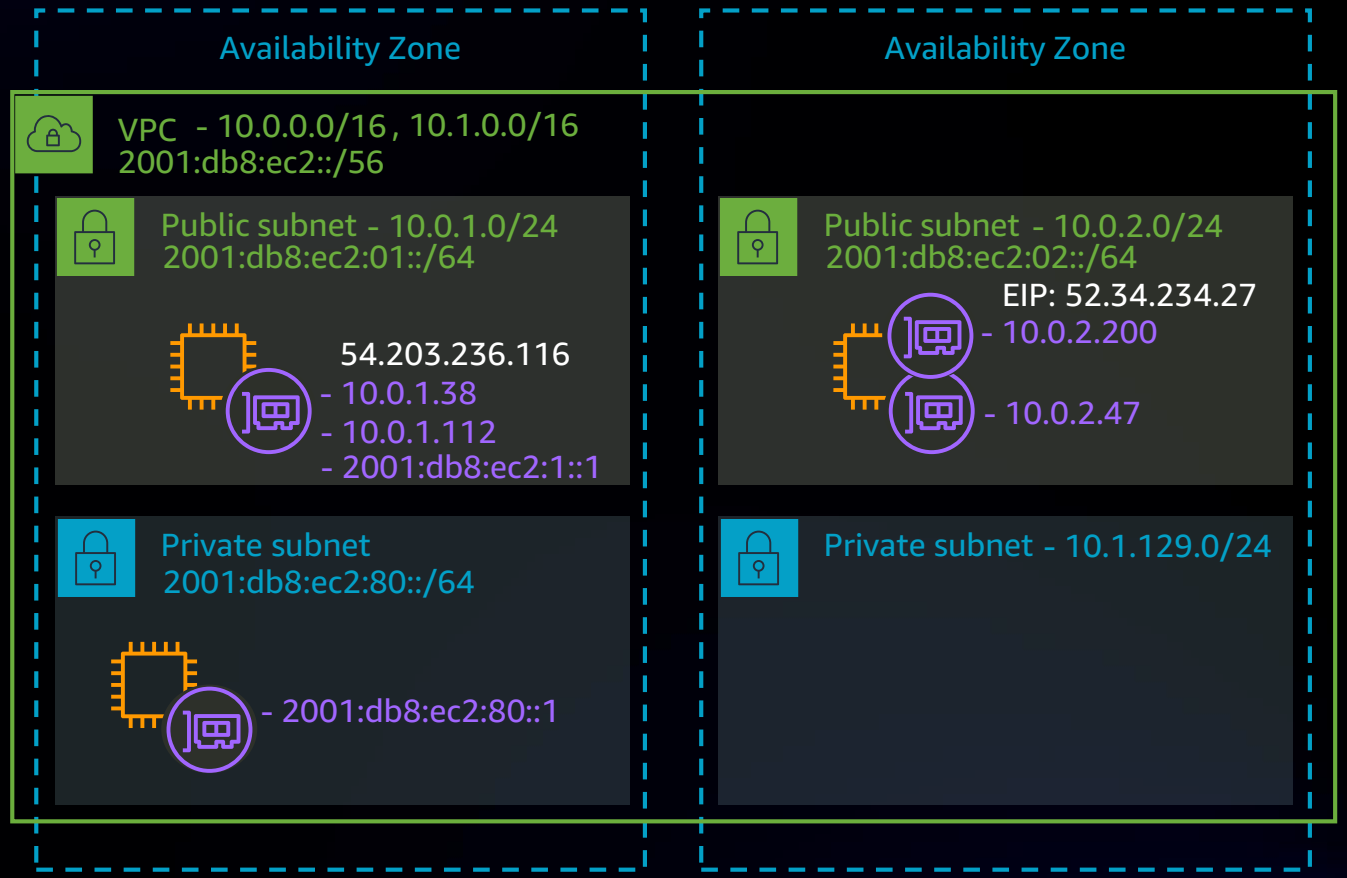
. . .

10.0.128.0 – Network A
10.0.128.1 – VPC Router
10.0.128.2 – Reserved
10.0.128.3 – Reserved
10.0.128.255 – Network Broadcast




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

# IPv6 addressing




Reserved
fd00:ec2::/32 - Reserved
fe80::X:Xff:feX:X/64 – VPC Router

2001:db8:ec2:01::0
2001:db8:ec2:01::1
2001:db8:ec2:01::2
2001:db8:ec2:01::3
2001:db8:ec2:01:ffff:ffff:ffff:ffff
. . .

2001:db8:ec2:80::0
2001:db8:ec2:80::1
2001:db8:ec2:80::2
2001:db8:ec2:80::3
2001:db8:ec2:80:ffff:ffff:ffff:ffff

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

# IPv6 addressing

Availability Zone

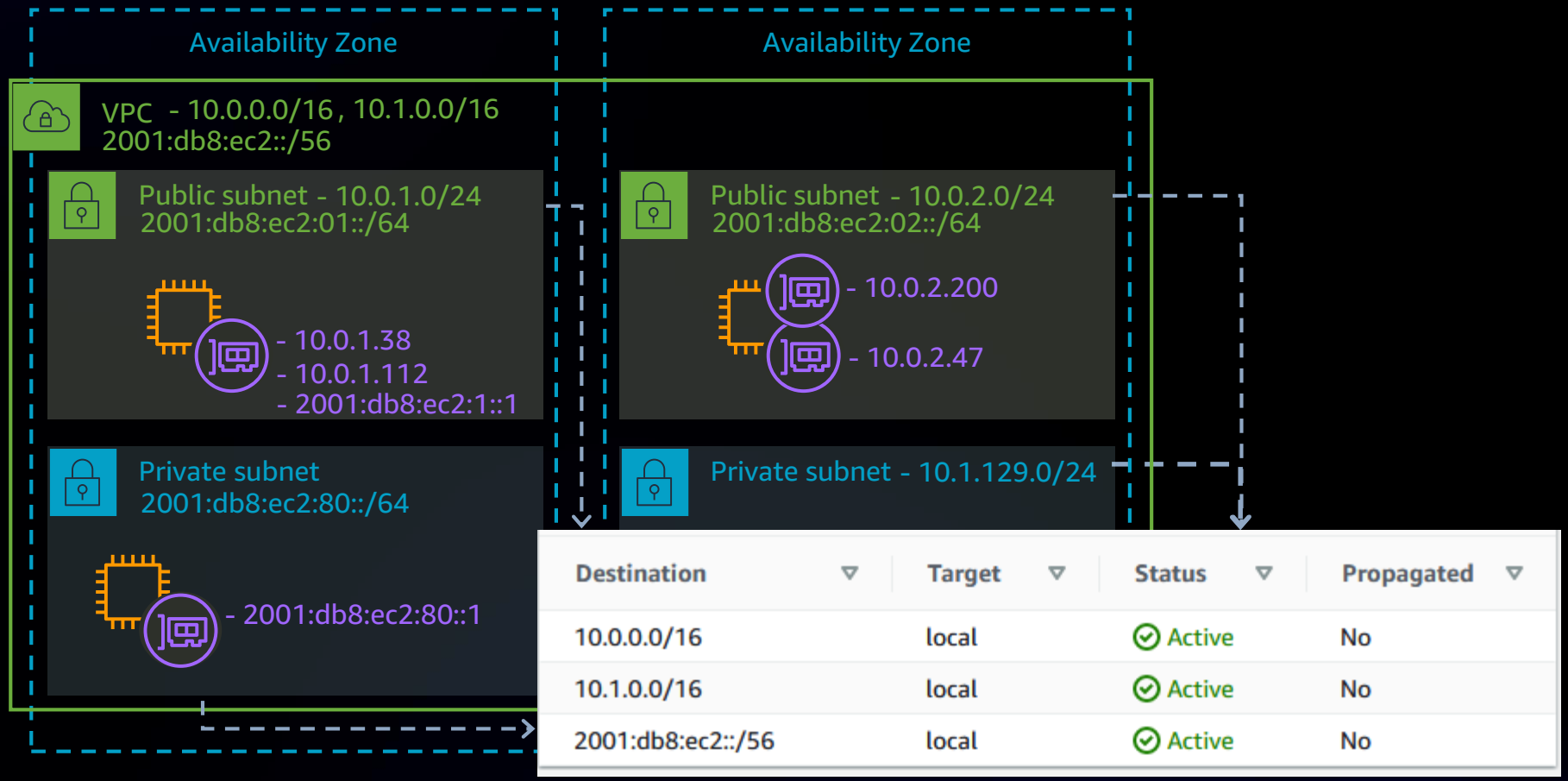
Availability Zone

```
[ec2-user@ip-10-0-1-38 ~]$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.0.1.38  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 2600:1f14:dd8:f101:7f03:5c08:bd69:fd24  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::4fb:62ff:fee7:ee9b  prefixlen 64  scopeid 0x20<link>
        ether 06:fb:62:e7:ee:9b  txqueuelen 1000  (Ethernet)
        RX packets 62056  bytes 65406176 (62.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35285  bytes 3231120 (3.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[ec2-user@ip-10-0-1-38 ~]$ ip -6 route show dev eth0
2600:1f14:dd8:f101:7f03:5c08:bd69:fd24 proto kernel metric 256 expires 403sec pref medium
2600:1f14:dd8:f101::/64 proto kernel metric 256 pref medium
fe80::/64 proto kernel metric 256 pref medium
default via fe80::4d7:4cff:fe5a:9cc9 proto ra metric 1024 expires 1790sec hoplimit 255 pref medium
```

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

# Intra-VPC routing

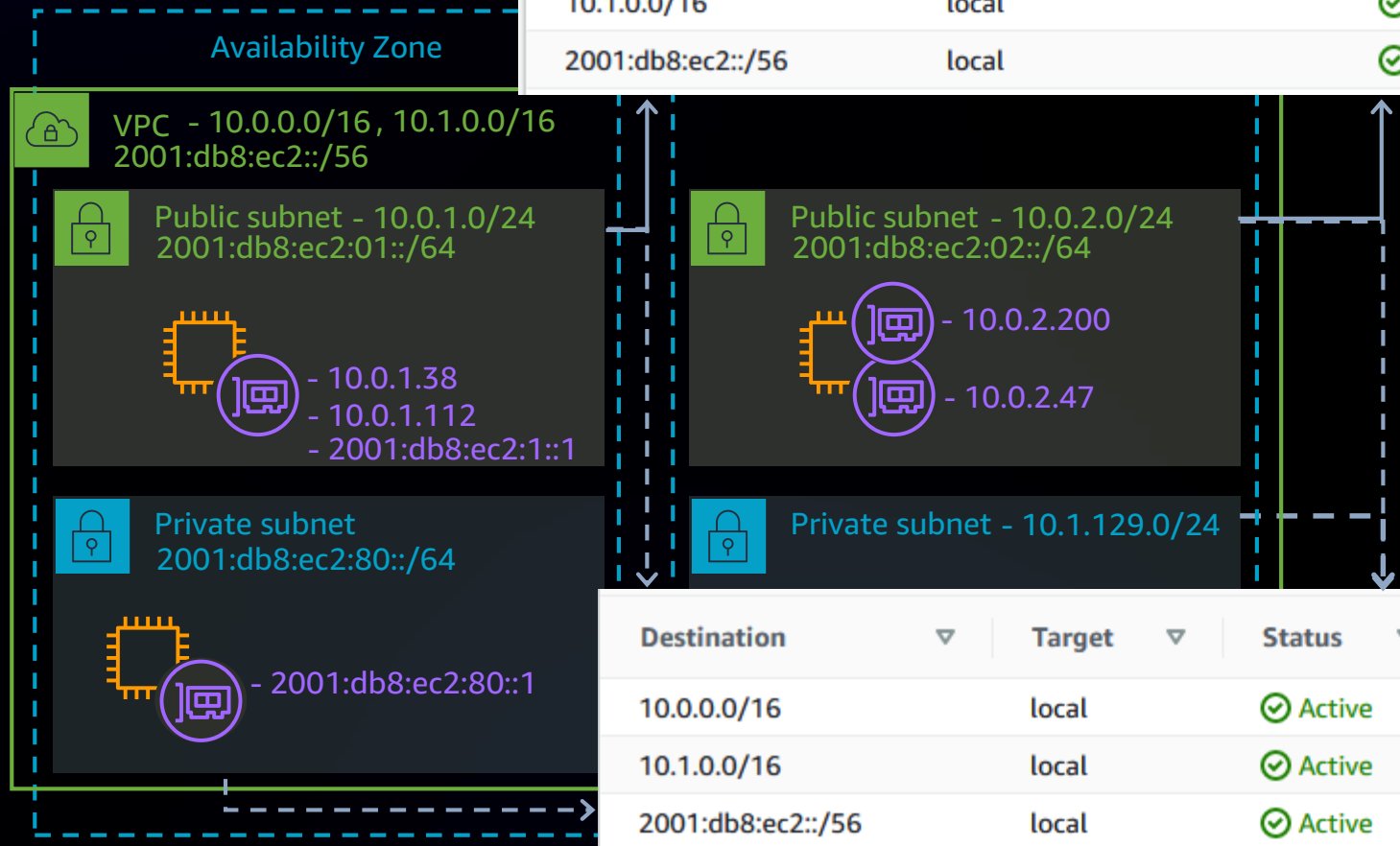



| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.0.0.0/16 | local | Active | No |
| 10.1.0.0/16 | local | Active | No |
| 2001:db8:ec2::/56 | local | Active | No |

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

# Intra-VPC routing

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.1.129.0/24 | eni-03b4676c7ac10c670 | Active | No |
| 10.0.0.0/16 | local | Active | No |
| 10.1.0.0/16 | local | Active | No |
| 2001:db8:ec2::/56 | local | Active | No |




| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.0.0.0/16 | local | Active | No |
| 10.1.0.0/16 | local | Active | No |
| 2001:db8:ec2::/56 | local | Active | No |

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

# Networking at the instance level

## Amazon EC2 Instance Metadata Service (IMDS)

169.254.169.254 fd00:ec2::254

## Amazon Time Sync Service

169.254.169.123 fd00:ec2::123

## Amazon Route 53 Resolver

169.254.169.253 fd00:ec2::253

```
[ec2-user@ip-10-0-1-38 ~]$ curl -w "\n" -H "X-aws-ec2-metadata-token: $TOKEN" \
> http://[fd00:ec2::254]/latest/meta-data/hostname
ip-10-0-1-38.us-west-2.compute.internal
[ec2-user@ip-10-0-1-38 ~]$
[ec2-user@ip-10-0-1-38 ~]$ chronyc tracking
Reference ID    : 9C6F5832 (fd00:ec2::123)
Stratum         : 4
Ref time (UTC)  : Fri Oct 15 17:11:40 2021
System time     : 0.000001282 seconds slow of NTP time
Last offset     : +0.000001382 seconds
RMS offset      : 0.000003336 seconds
Frequency       : 91.249 ppm fast
Residual freq   : +0.000 ppm
Skew            : 0.063 ppm
Root delay      : 0.000477255 seconds
Root dispersion : 0.000269519 seconds
Update interval : 16.1 seconds
Leap status     : Normal
[ec2-user@ip-10-0-1-38 ~]$
[ec2-user@ip-10-0-1-38 ~]$ host -6 ripe.net fd00:ec2::253
Using domain server:
Name: fd00:ec2::253
Address: fd00:ec2::253#53
Aliases:

ripe.net has address 193.0.6.139
ripe.net has IPv6 address 2001:67c:2e8:22::c100:68b
ripe.net mail is handled by 200 mahimahi.ripe.net.
ripe.net mail is handled by 250 molamola.ripe.net.
[ec2-user@ip-10-0-1-38 ~]$
```

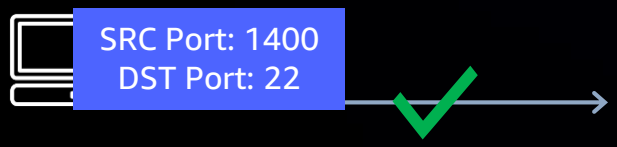
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

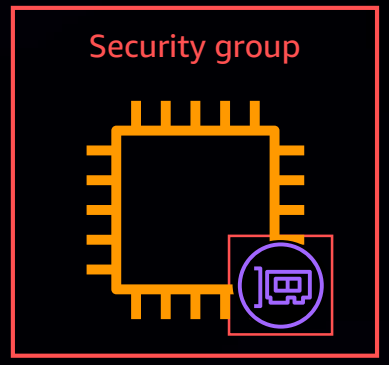


# Basics of VPC security

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

# Security groups



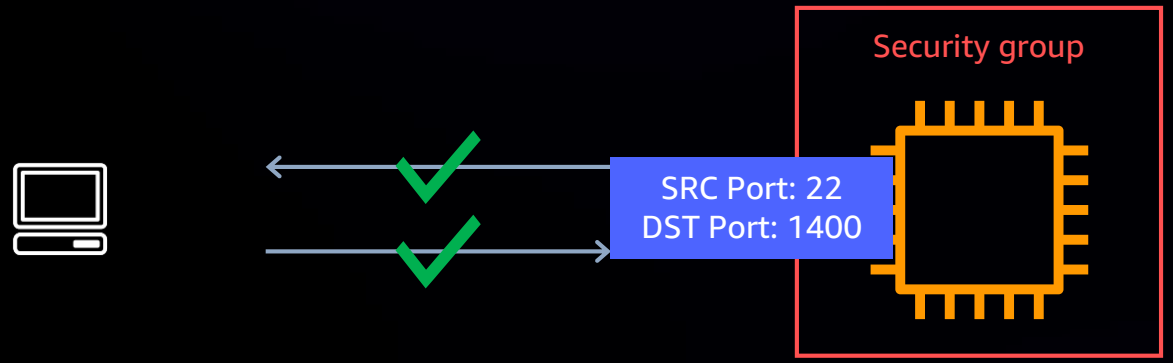

Inbound

| IP version | Type | Protocol | Port range | Source |
|---|---|---|---|---|
| IPv4 | SSH | TCP | 22 | 0.0.0.0/0 |
| IPv6 | SSH | TCP | 22 | ::/0 |

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

# Security groups



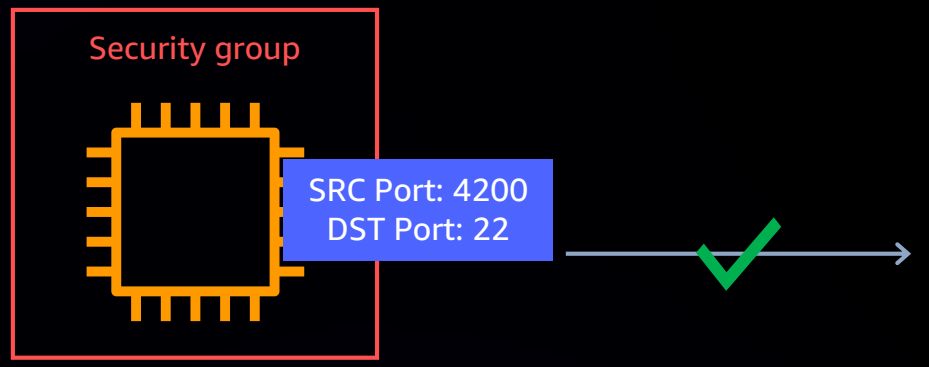



Inbound

| IP version | Type | Protocol | Port range | Source |
|---|---|---|---|---|
| IPv4 | SSH | TCP | 22 | 0.0.0.0/0 |
| IPv6 | SSH | TCP | 22 | ::/0 |

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

# Security groups






52.34.234.27
2001:db8:ec2:2::27

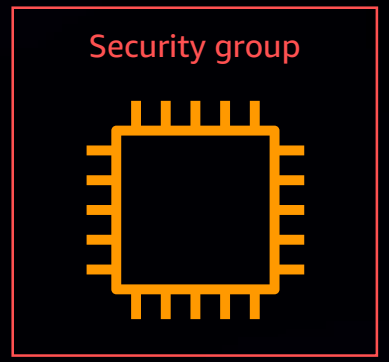
Outbound

| IP version | Type | Protocol | Port range | Destination |
|---|---|---|---|---|
| IPv4 | All traffic | TCP | All | 52.34.234.27/32 |
| IPv6 | All traffic | TCP | All | 2001:db8:ec2:2::27/128 |

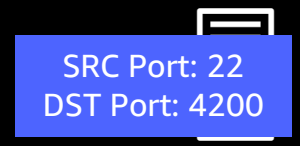
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Security groups







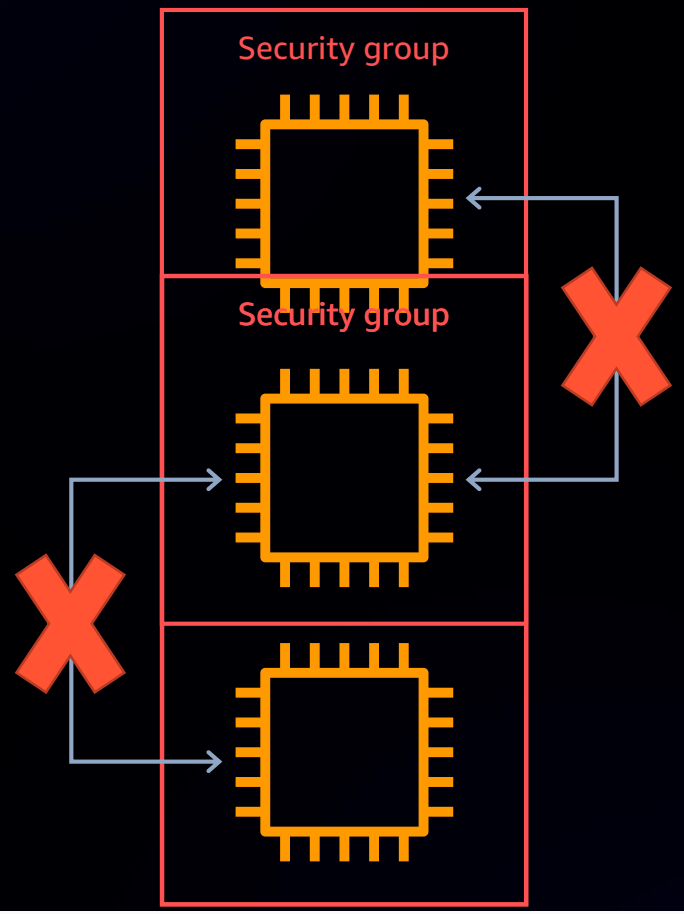

52.34.234.27
2001:db8:ec2:02::27

Outbound

| IP version | Type | Protocol | Port range | Destination |
|---|---|---|---|---|
| IPv4 | All traffic | TCP | All | 52.34.234.27/32 |
| IPv6 | All traffic | TCP | All | 2001:db8:ec2:2::27/128 |

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

# Security groups

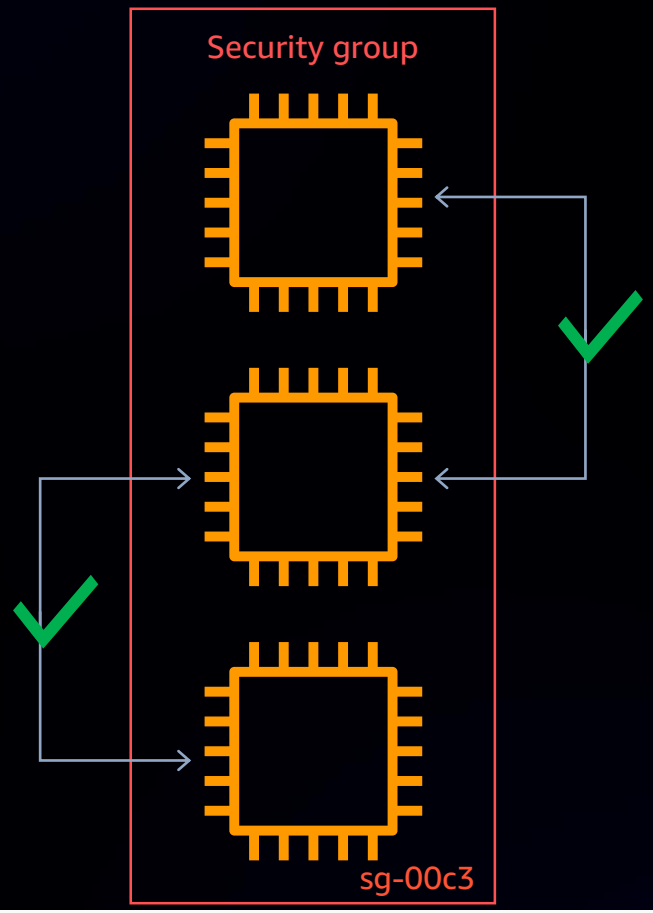



Inbound

| IP version | Type | Protocol | Port range | Source |
|---|---|---|---|---|
| IPv4 | SSH | TCP | 22 | 0.0.0.0/0 |
| IPv6 | SSH | TCP | 22 | ::/0 |

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

# Security groups




Inbound

| IP version | Type | Protocol | Port range | Source |
|---|---|---|---|---|
| IPv4 | SSH | TCP | 22 | 0.0.0.0/0 |
| IPv6 | SSH | TCP | 22 | ::/0 |
| – | All traffic | All | All | sg-00c3 |

© 2021, 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 |

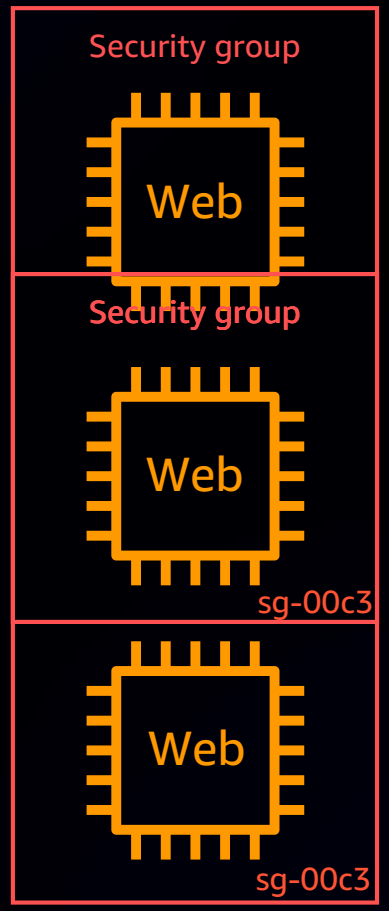
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Security groups



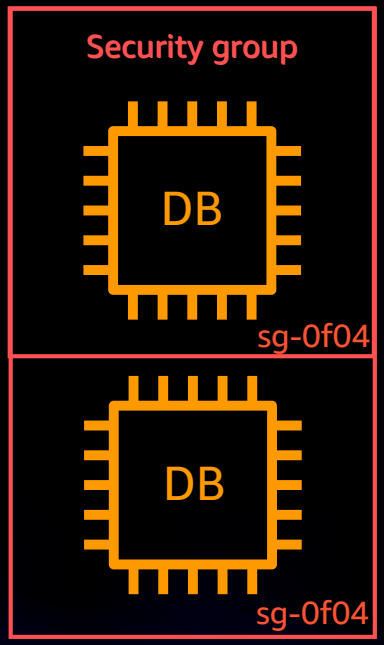










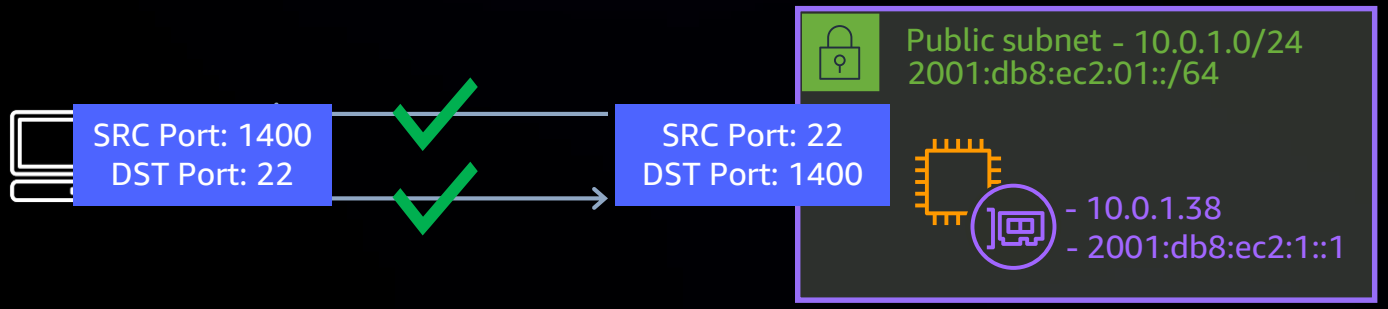

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

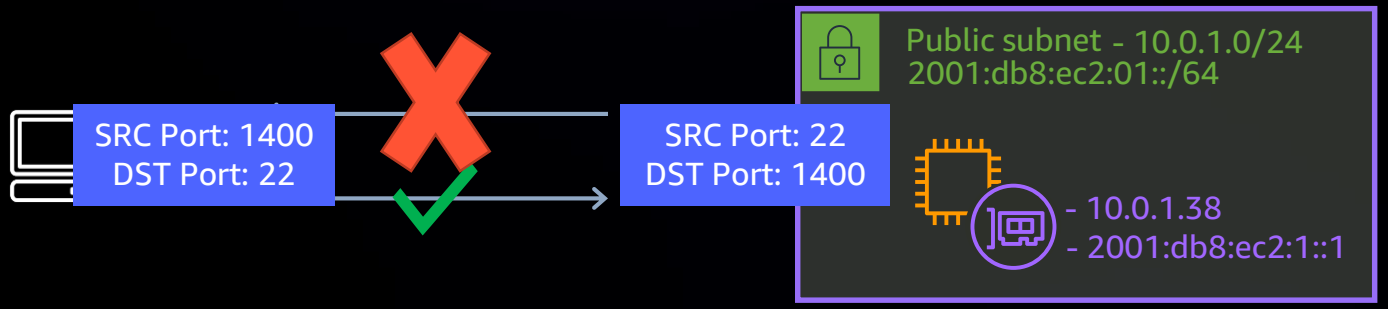
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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 |




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

Outbound

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

# Network access control lists (NACLs)



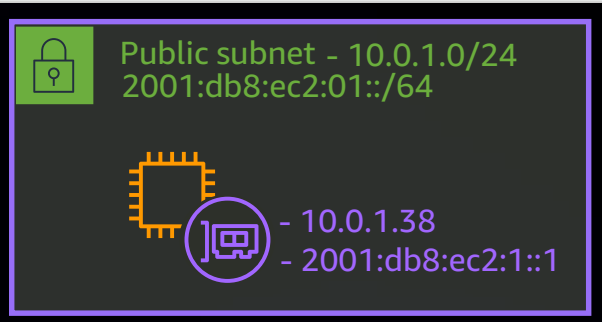
Inbound

| Rule number | Type | Protocol | Port range | Source | Allow/Deny |
|---|---|---|---|---|---|
| 100 | SSH (22) | TCP (6) | 22 | 203.0.113.10/32 | Allow |
| 101 | SSH (22) | TCP (6) | 22 | 2001:db8:cafe::10/128 | Allow |
| * | All traffic | All | All | 0.0.0.0/0 | Deny |
| * | All traffic | All | All | ::/0 | Deny |



203.0.113.10
2001:db8:cafe::10



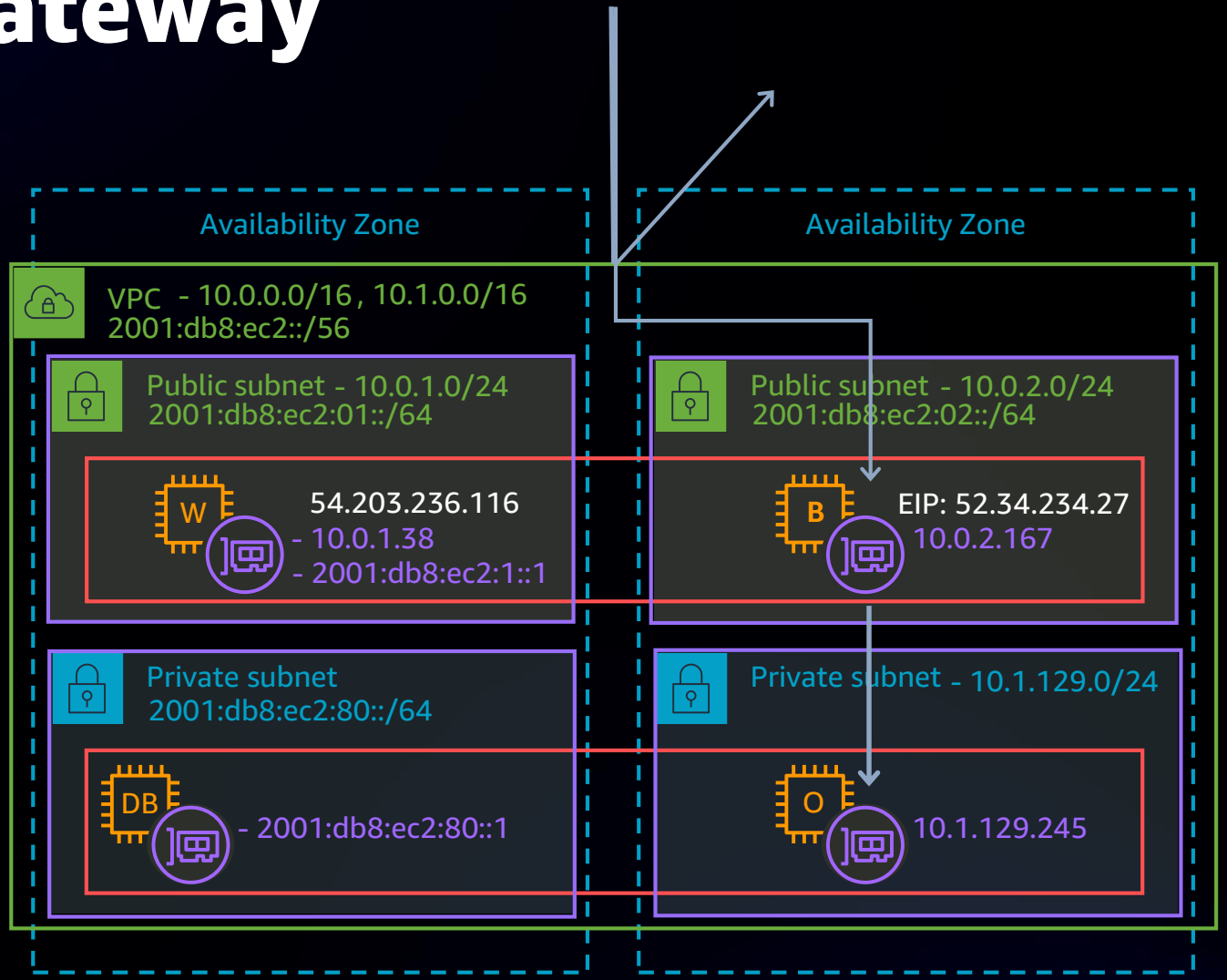



| Rule number | Type | Protocol | Port range | Destination | Allow/Deny |
|---|---|---|---|---|---|
| 100 | Custom TCP | TCP (6) | 1024 - 65535 | 203.0.113.10/32 | Allow |
| 101 | Custom TCP | TCP (6) | 1024 - 65535 | 2001:db8:cafe::10/128 | Allow |
| * | All traffic | All | All | 0.0.0.0/0 | Deny |
| * | All traffic | All | All | ::/0 | Deny |

Outbound

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

# Internet gateway

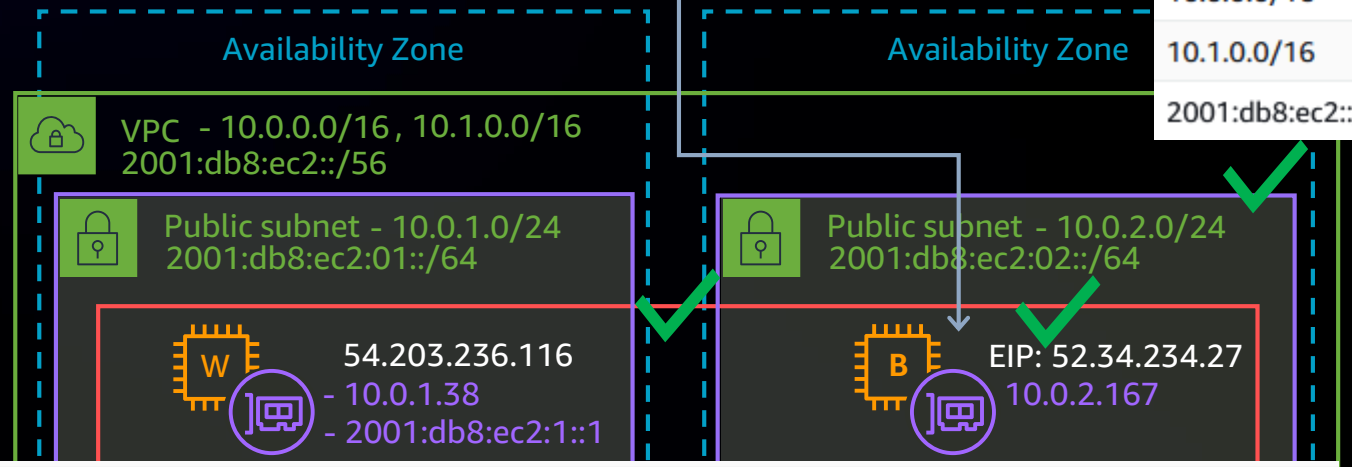



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Internet gateway

**5 things**

1) Public IP
2) SGs allow
3) NACLs allow
4) Attached internet gateway (IGW)
5) Route to IGW




| Destination | Target |
|---|---|
| 0.0.0.0/0 | igw-0399a4d55f |
| ::/0 | igw-0399a4d55f |
| 10.0.0.0/16 | local |
| 10.1.0.0/16 | local |
| 2001:db8:ec2::/56 | local |

Inbound

| IP version | Type | Protocol | Port range | Source |
|---|---|---|---|---|
| IPv4 | SSH | TCP | 22 | 0.0.0.0/0 |
| IPv6 | SSH | TCP | 22 | ::/0 |

Inbound

| 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 |

Outbound

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

# Peering, endpoints, and gateways

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

# Peering, endpoints, and gateways



AWS Client VPN endpoint



Virtual private gateway



Direct Connect gateway



NAT gateway



Internet gateway



AWS Transit Gateway



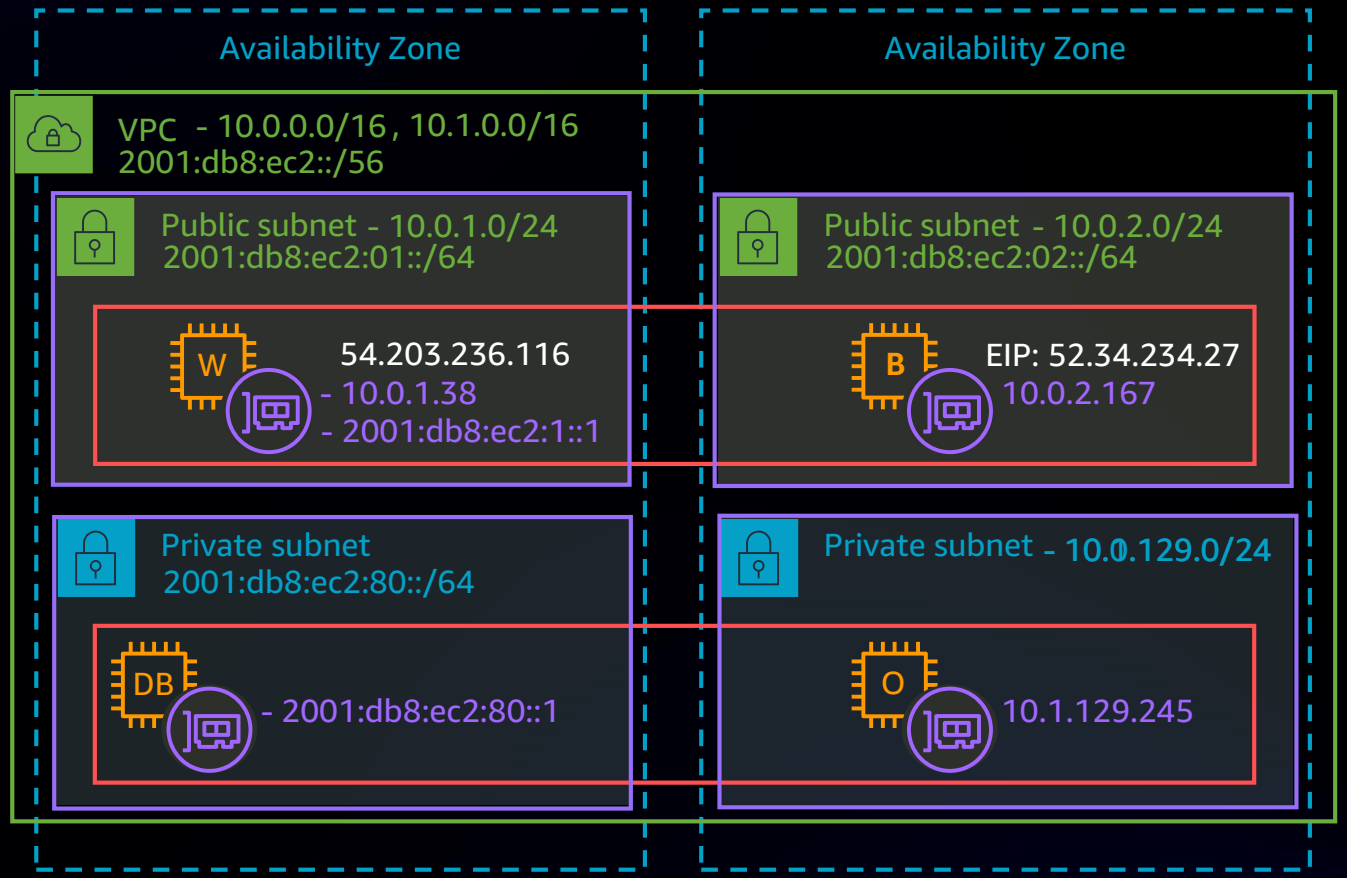
Endpoints



Peering connection

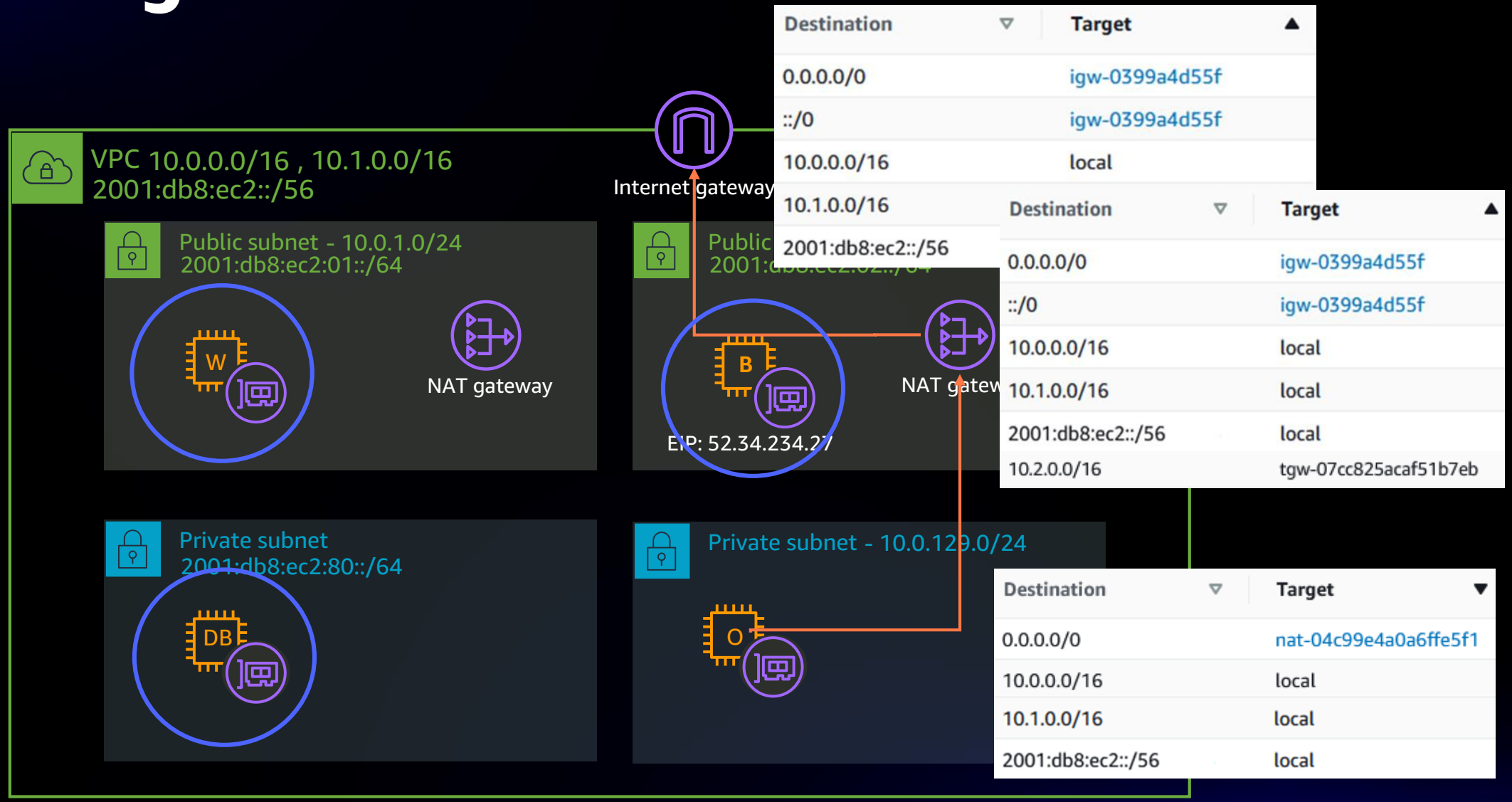
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Connecting to the internet



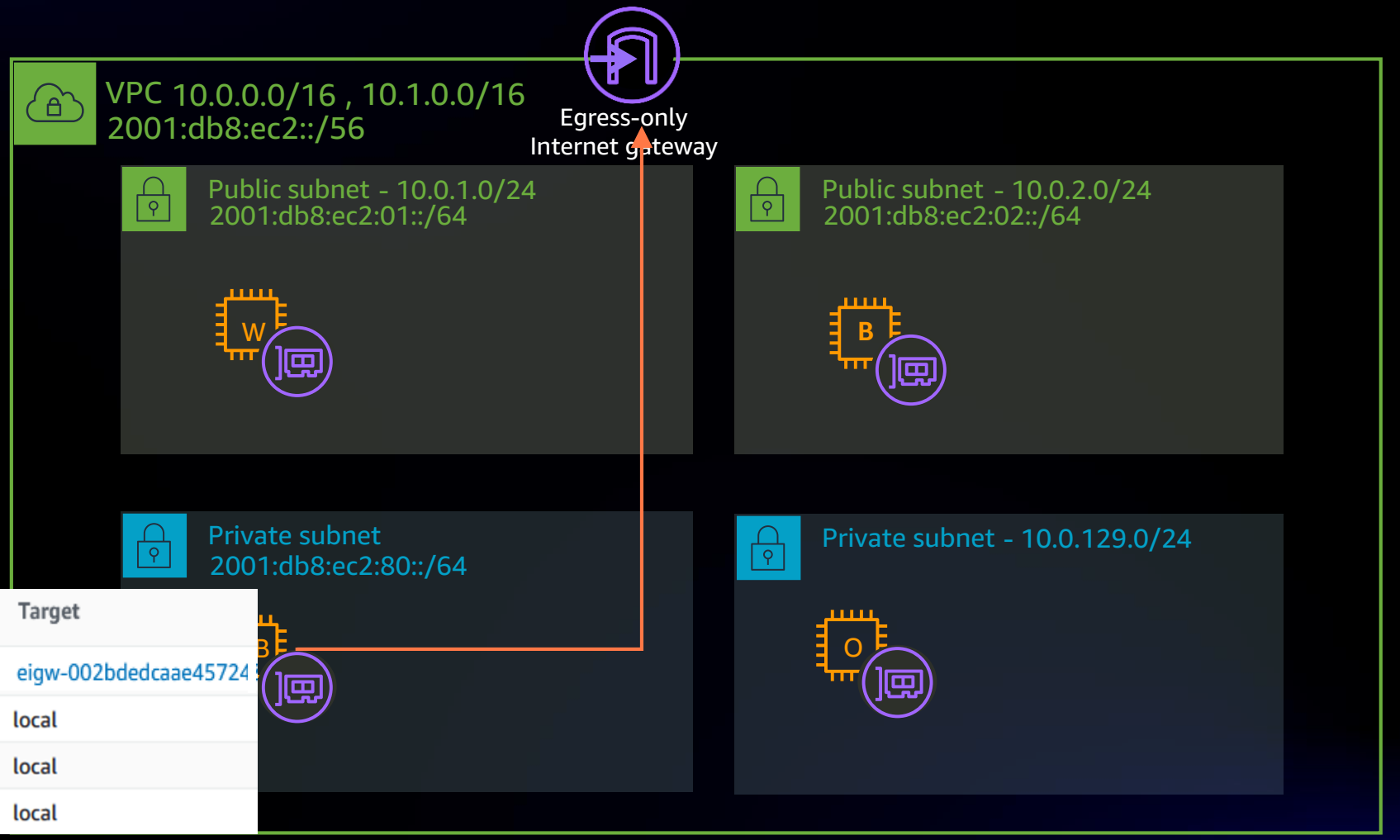

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Connecting to the internet




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

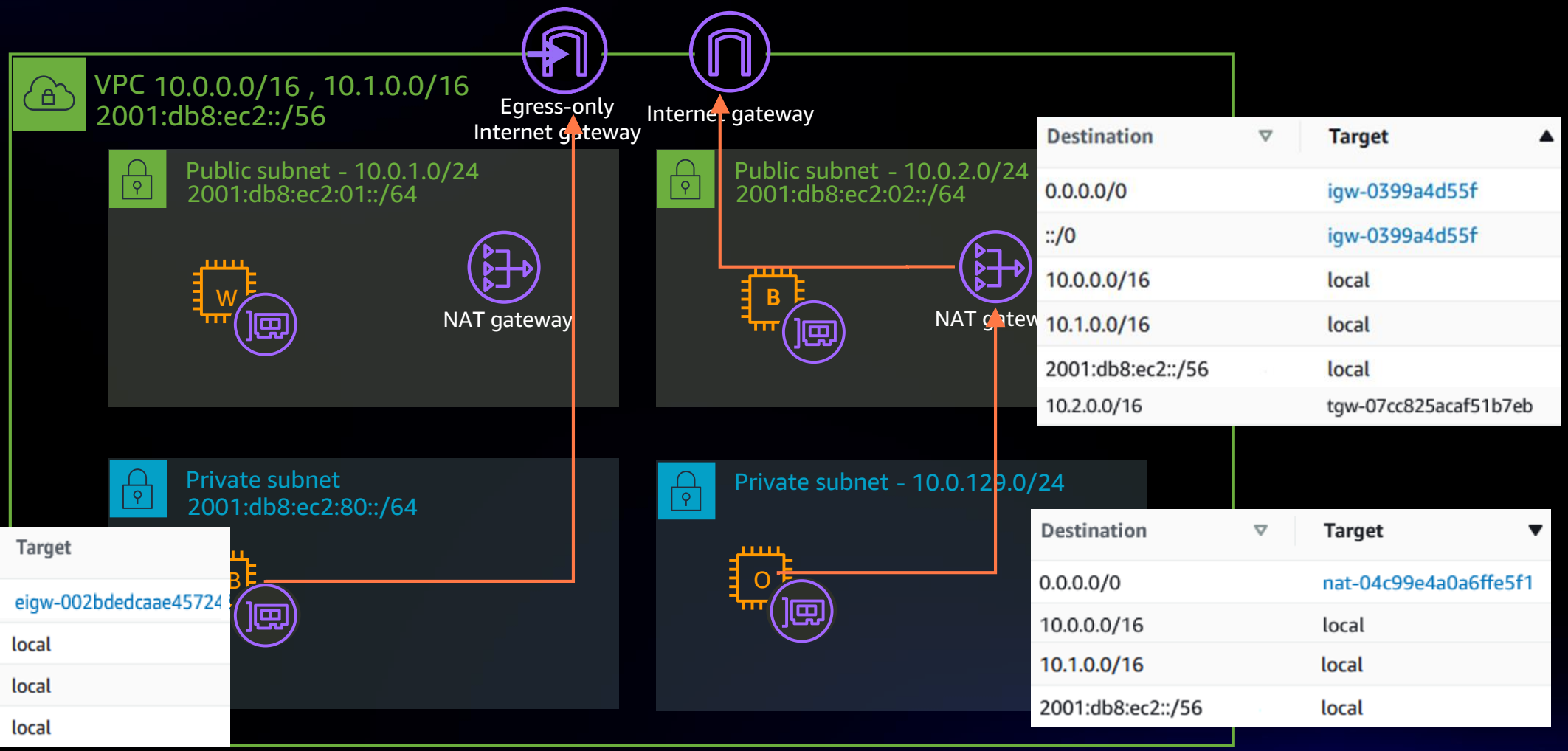
# Connecting to the internet




| Destination | Target |
|---|---|
| ::/0 | eigw-002bdedcaae45724 |
| 10.0.0.0/16 | local |
| 10.1.0.0/16 | local |
| 2001:db8:ec2::/56 | local |

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

# Connecting to the internet




| Destination | Target |
|---|---|
| 0.0.0.0/0 | igw-0399a4d55f |
| ::/0 | igw-0399a4d55f |
| 10.0.0.0/16 | local |
| 10.1.0.0/16 | local |
| 2001:db8:ec2::/56 | local |
| 10.2.0.0/16 | tgw-07cc825acaf51b7eb |

| Destination | Target |
|---|---|
| ::/0 | eigw-002bdedcaae45724 |
| 10.0.0.0/16 | local |
| 10.1.0.0/16 | local |
| 2001:db8:ec2::/56 | local |

| Destination | Target |
|---|---|
| 0.0.0.0/0 | nat-04c99e4a0a6ffe5f1 |
| 10.0.0.0/16 | local |
| 10.1.0.0/16 | local |
| 2001:db8:ec2::/56 | local |

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

# Peering, Endpoints and Gateways



AWS Client VPN Endpoint



Virtual Private Gateway



Direct Connect Gateway



NAT Gateway



Internet Gateways



AWS Transit Gateway



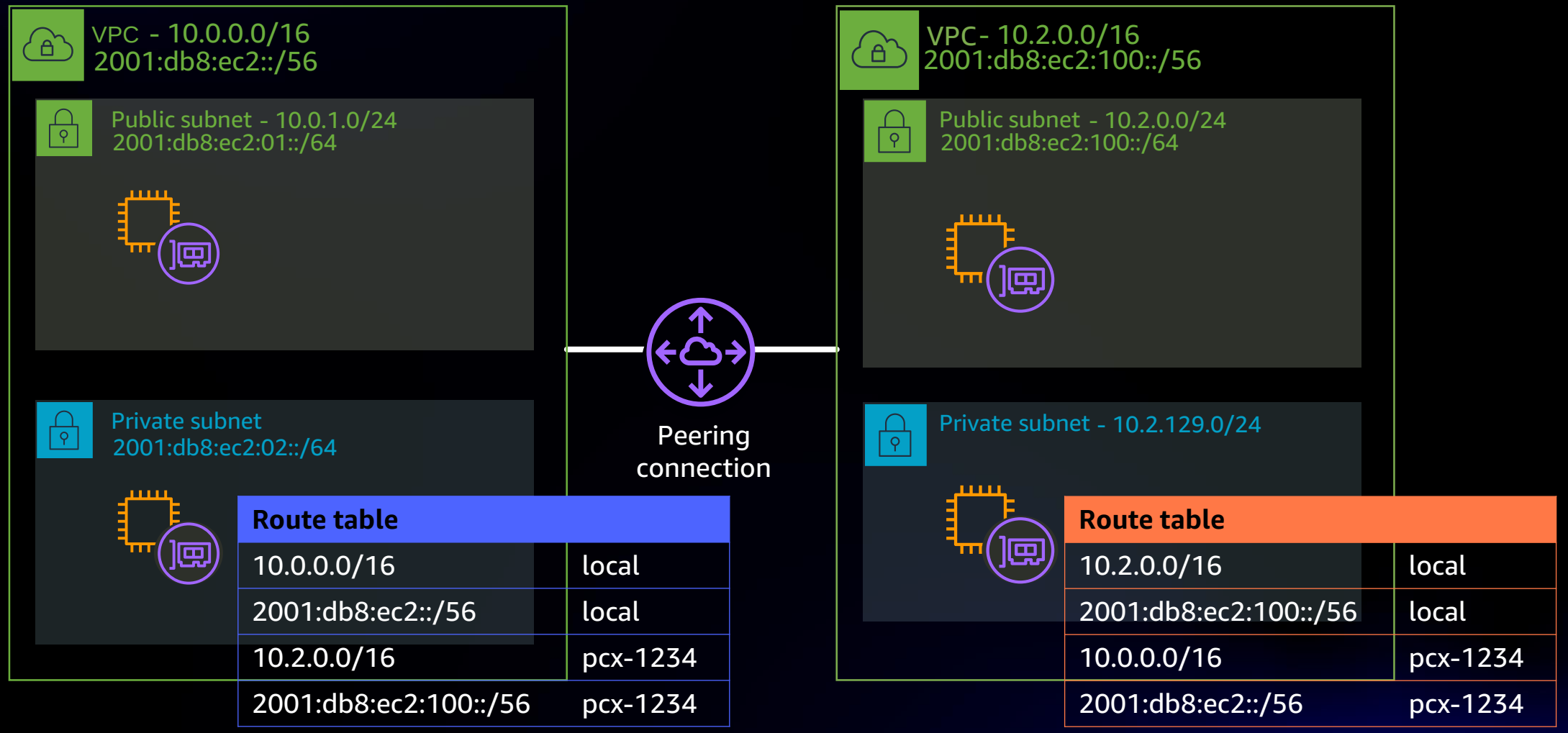
Endpoints



Peering connection

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

# VPC Peering

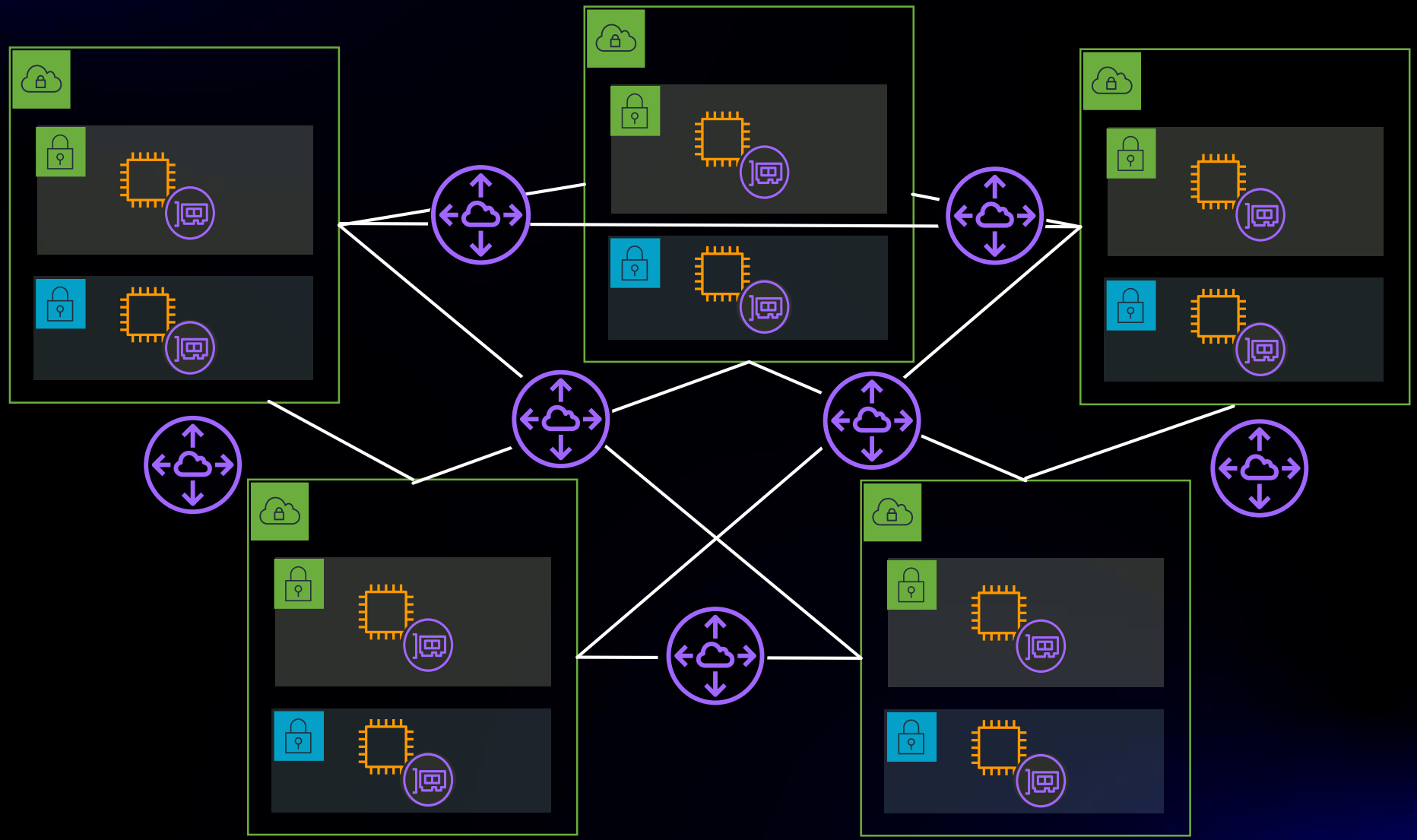



| Route table | |
|---|---|
| 10.0.0.0/16 | local |
| 2001:db8:ec2::/56 | local |
| 10.2.0.0/16 | pcx-1234 |
| 2001:db8:ec2:100::/56 | pcx-1234 |

| 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 |

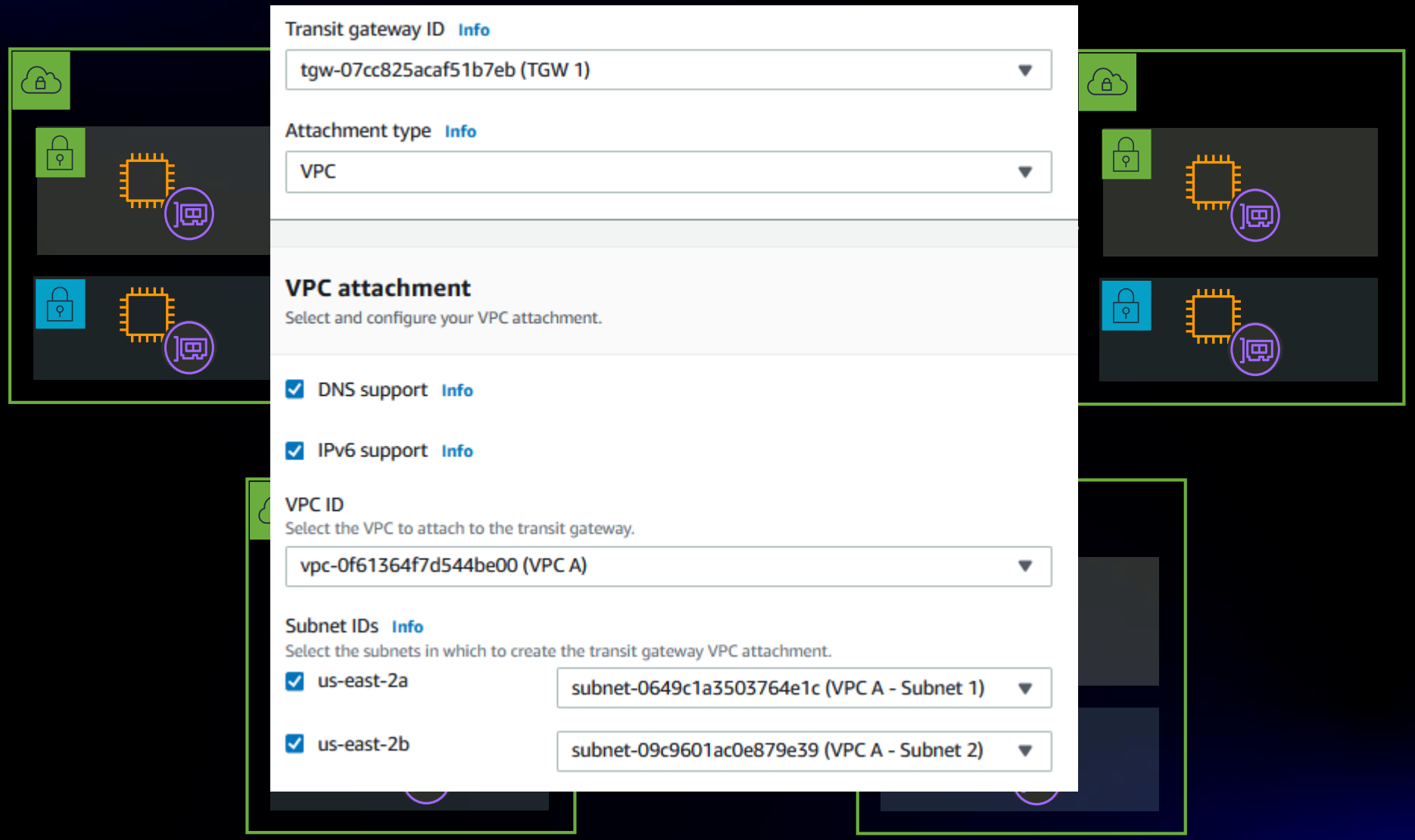
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# VPC Peering



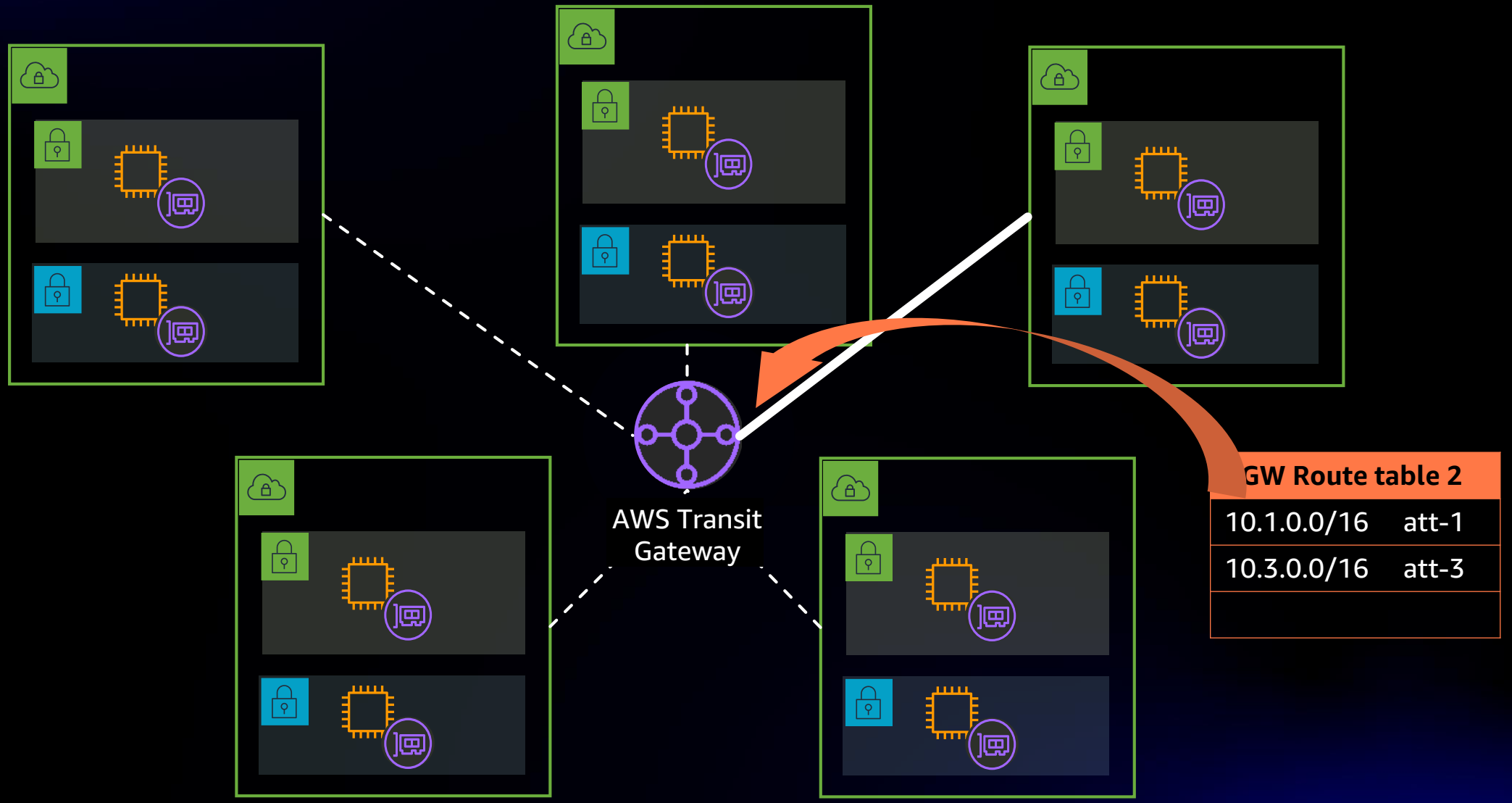
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Transit Gateway



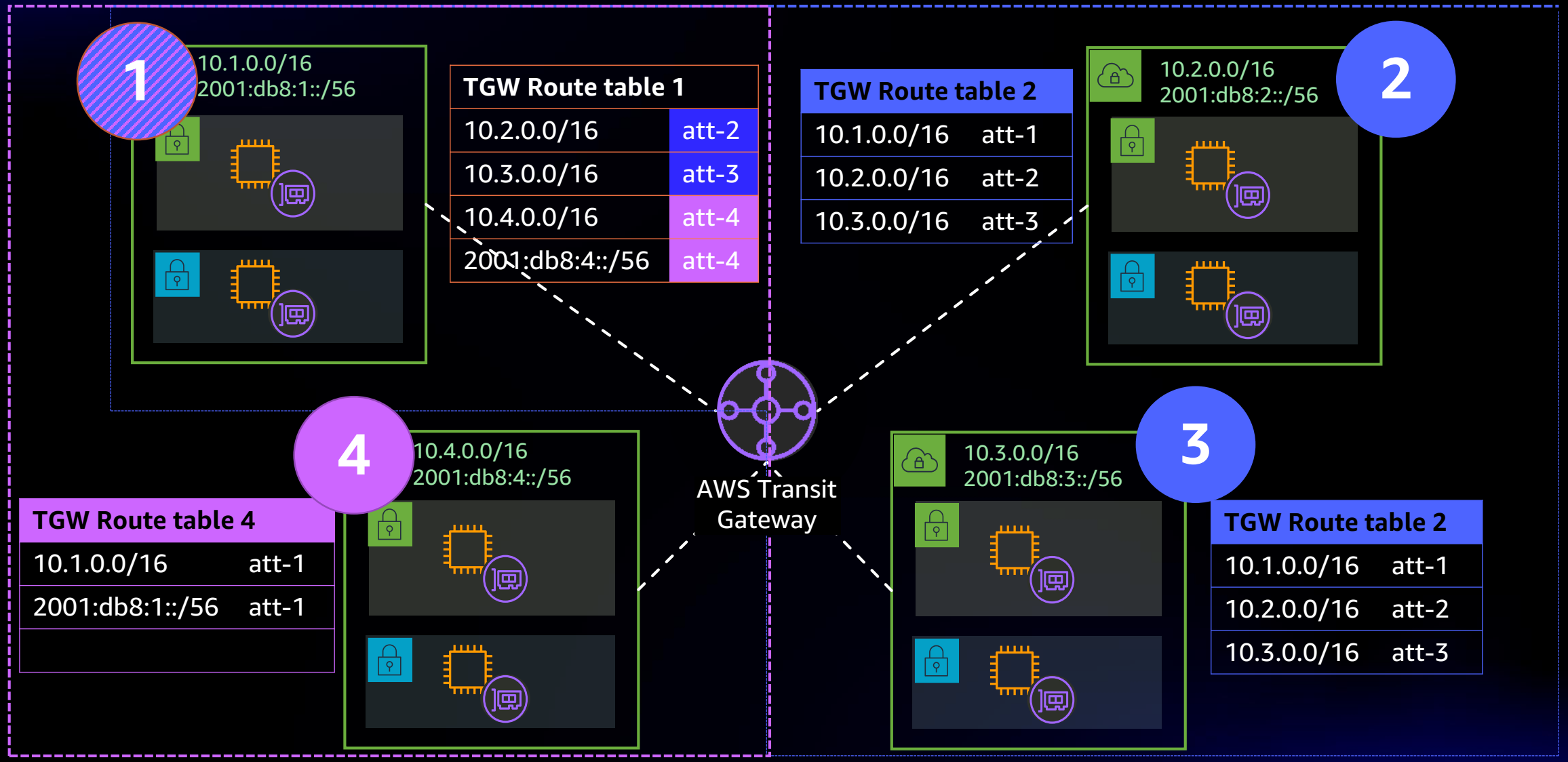

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Transit Gateway



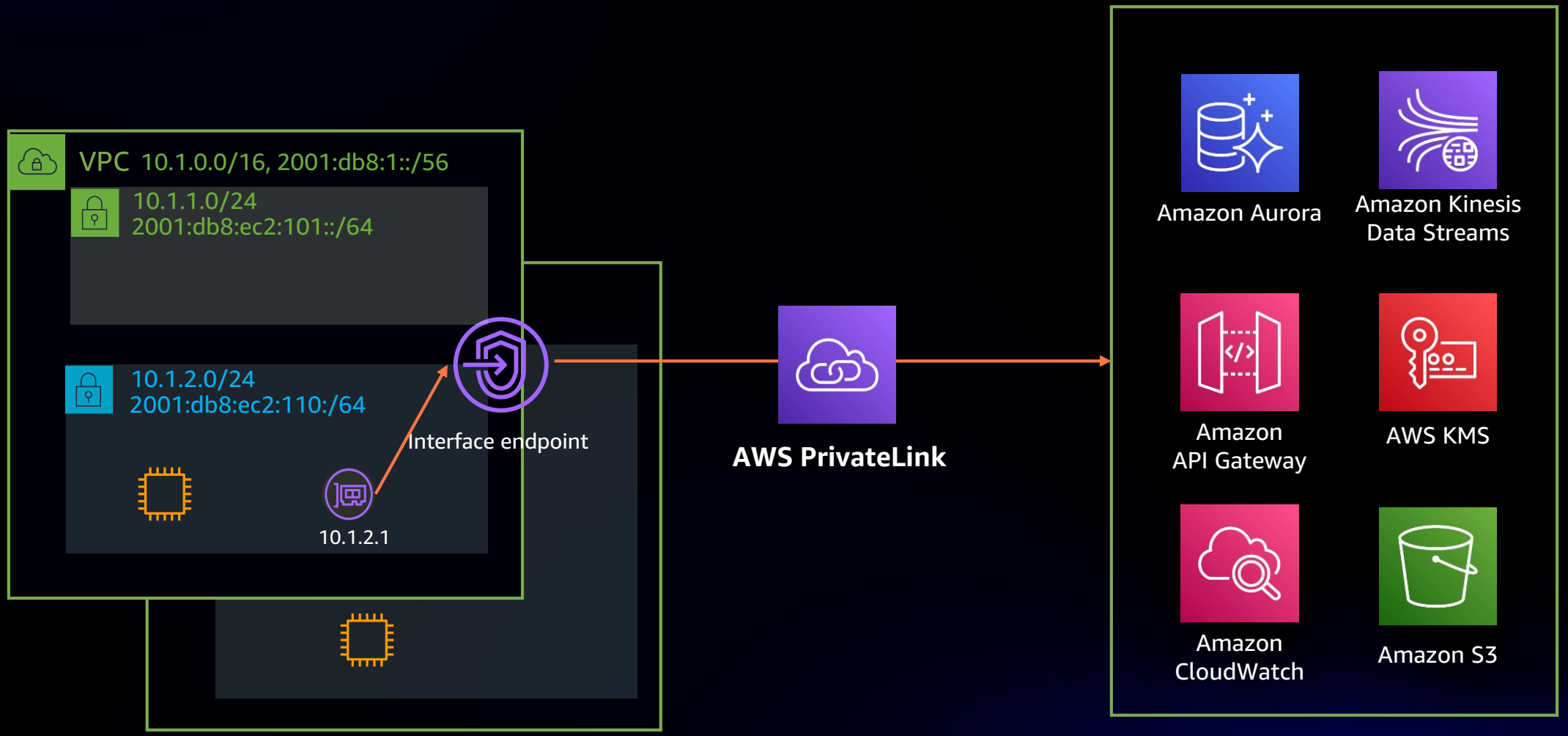

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Transit Gateway route tables and domains



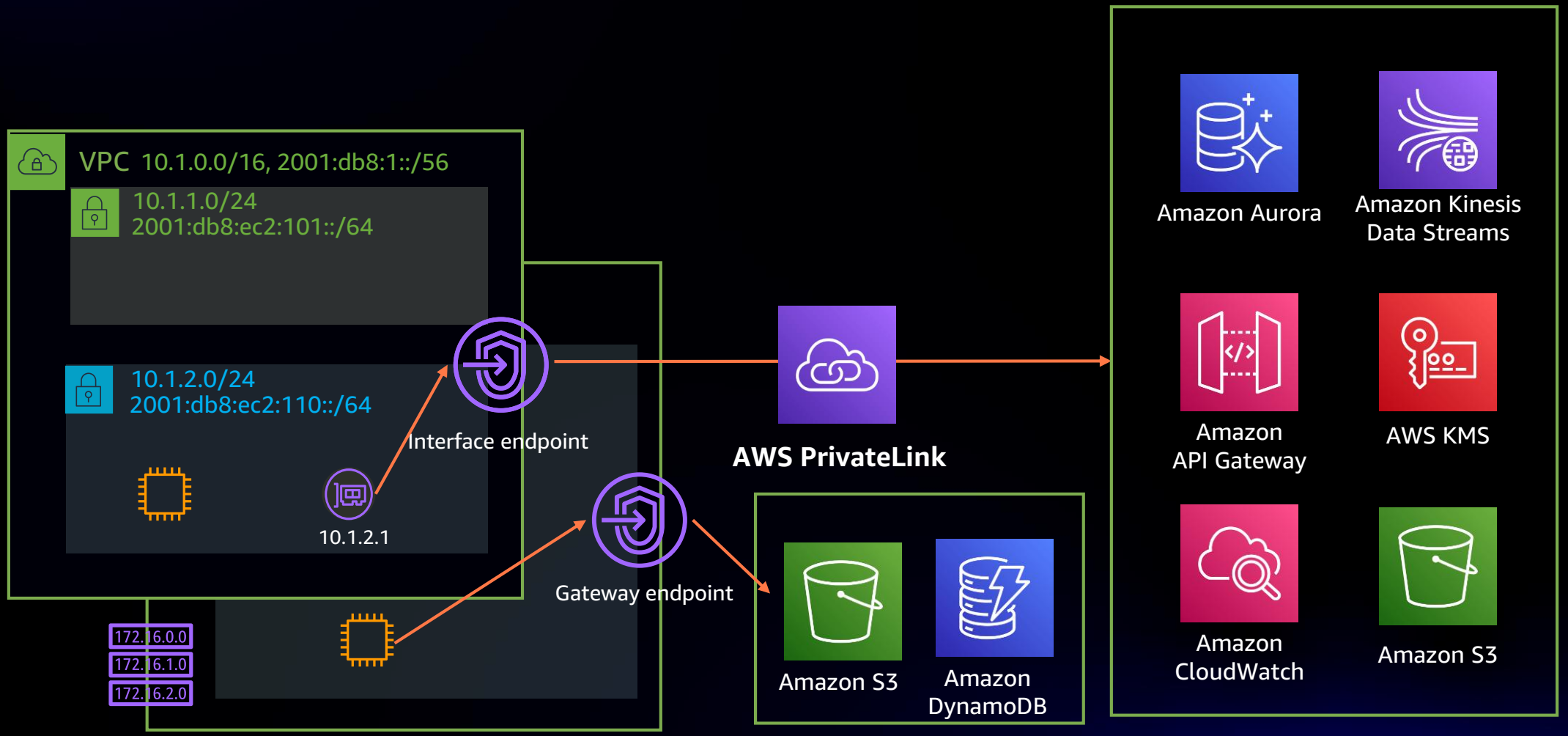

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# VPC interface endpoints



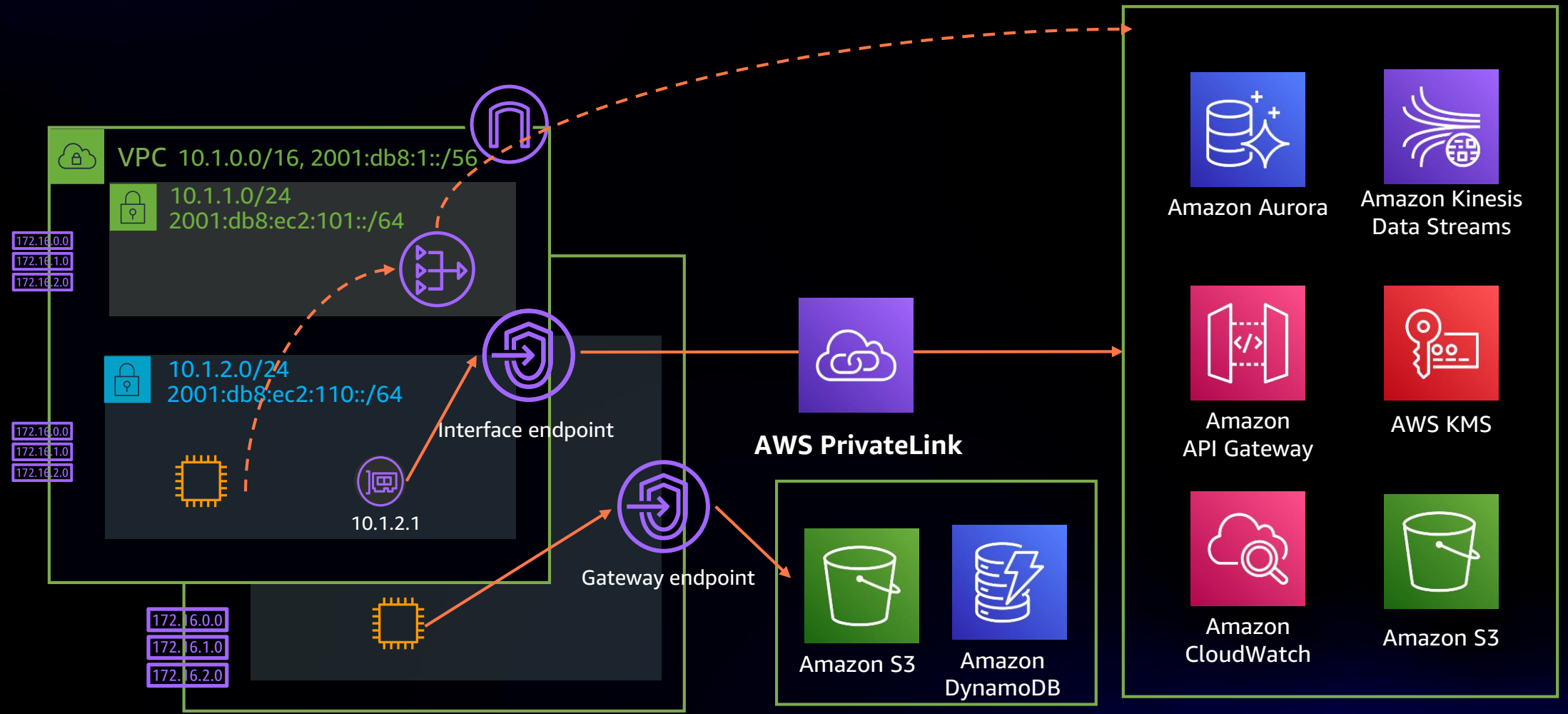

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# VPC gateway endpoints




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

# Without VPC endpoints




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

# VPC endpoint policies



```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

172.16.0.0
172.16.1.0
172.16.2.0

Amazon S3

Amazon DynamoDB

Amazon Aurora

Amazon Kinesis Data Streams

Amazon API Gateway

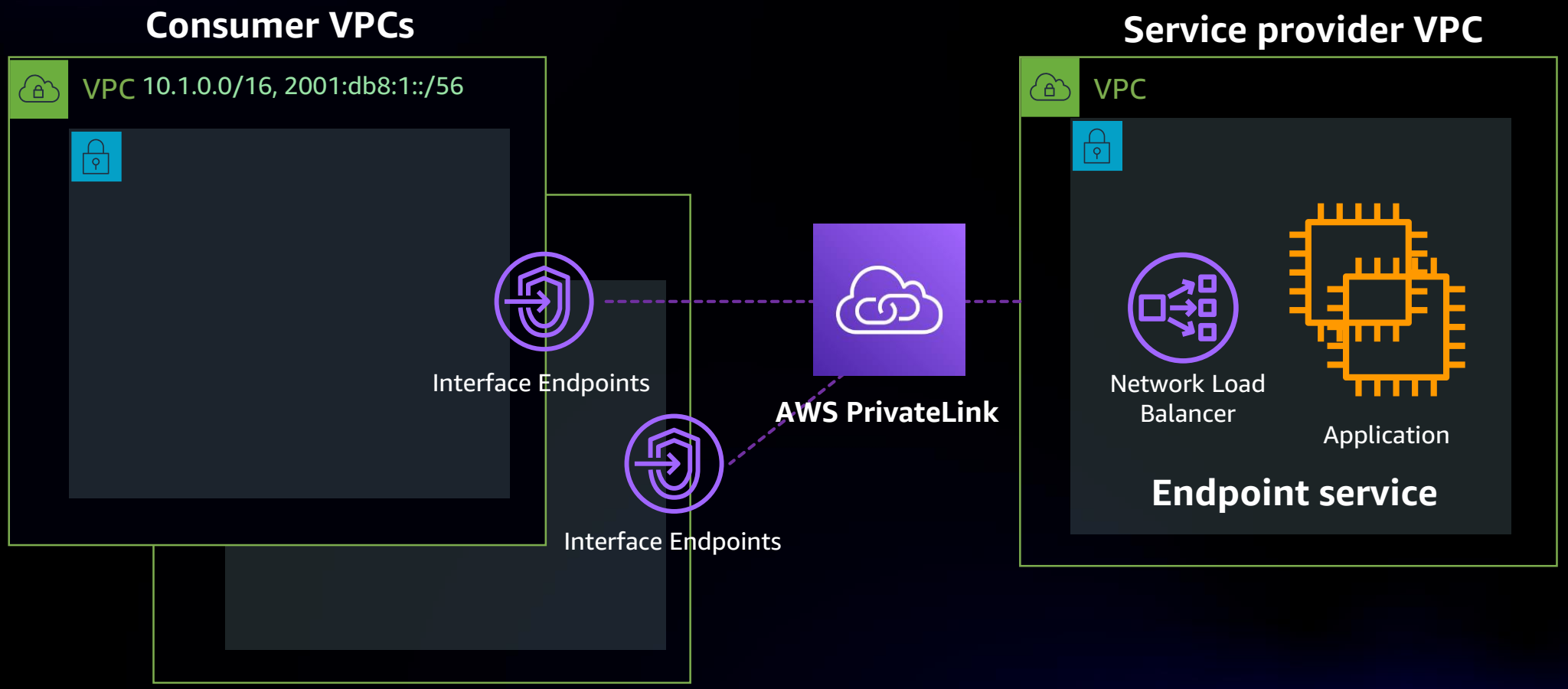
AWS KMS

Amazon CloudWatch

Amazon S3

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

# AWS PrivateLink




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

# Peering, endpoints, and gateways



AWS Client VPN endpoint



Virtual private gateway



Direct Connect gateway



NAT gateway



Internet gateway



Peering connection



AWS Transit Gateway



Endpoints

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

# Hybrid connectivity and gateways



AWS Direct Connect



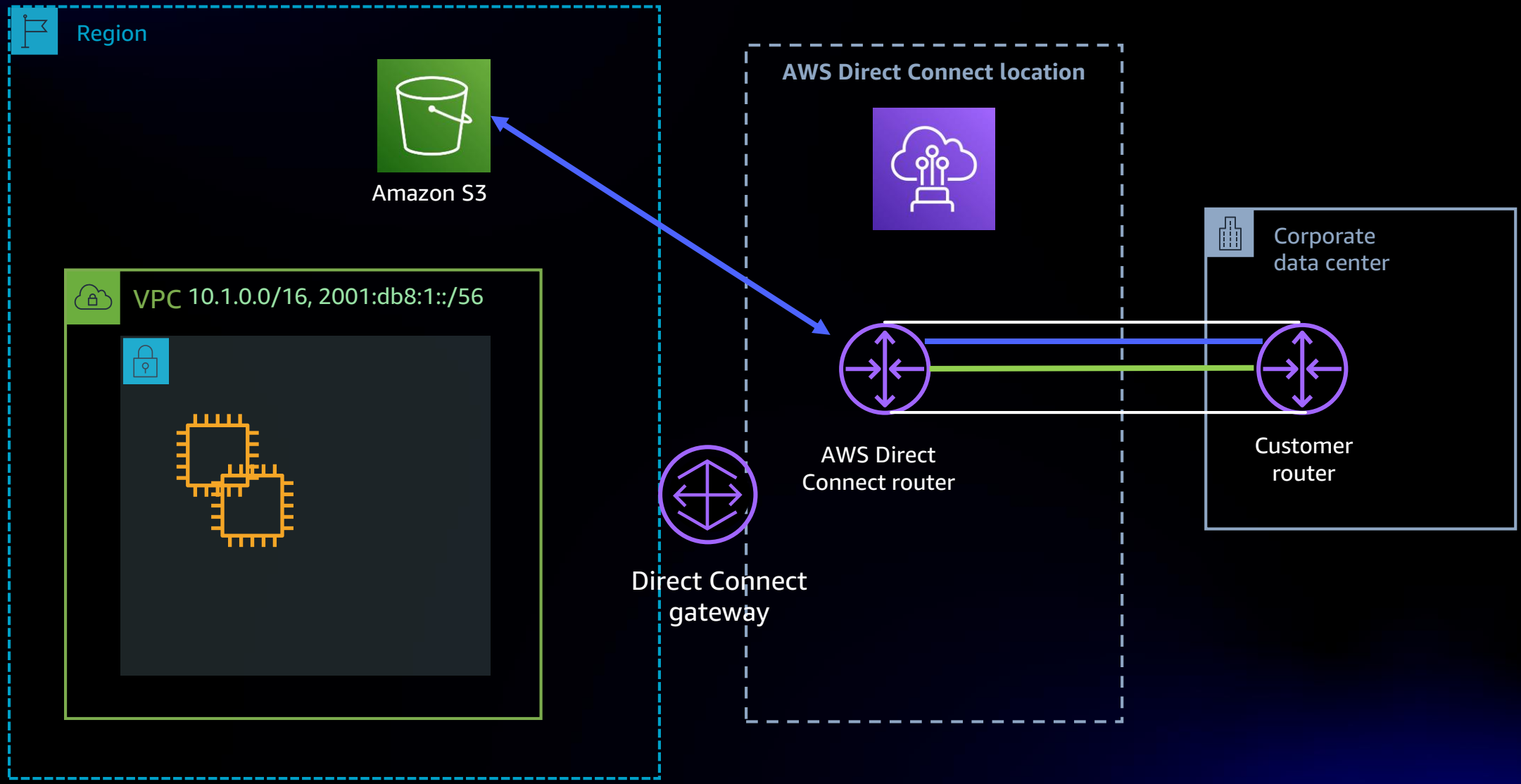
AWS Site-to-Site VPN



AWS Client VPN

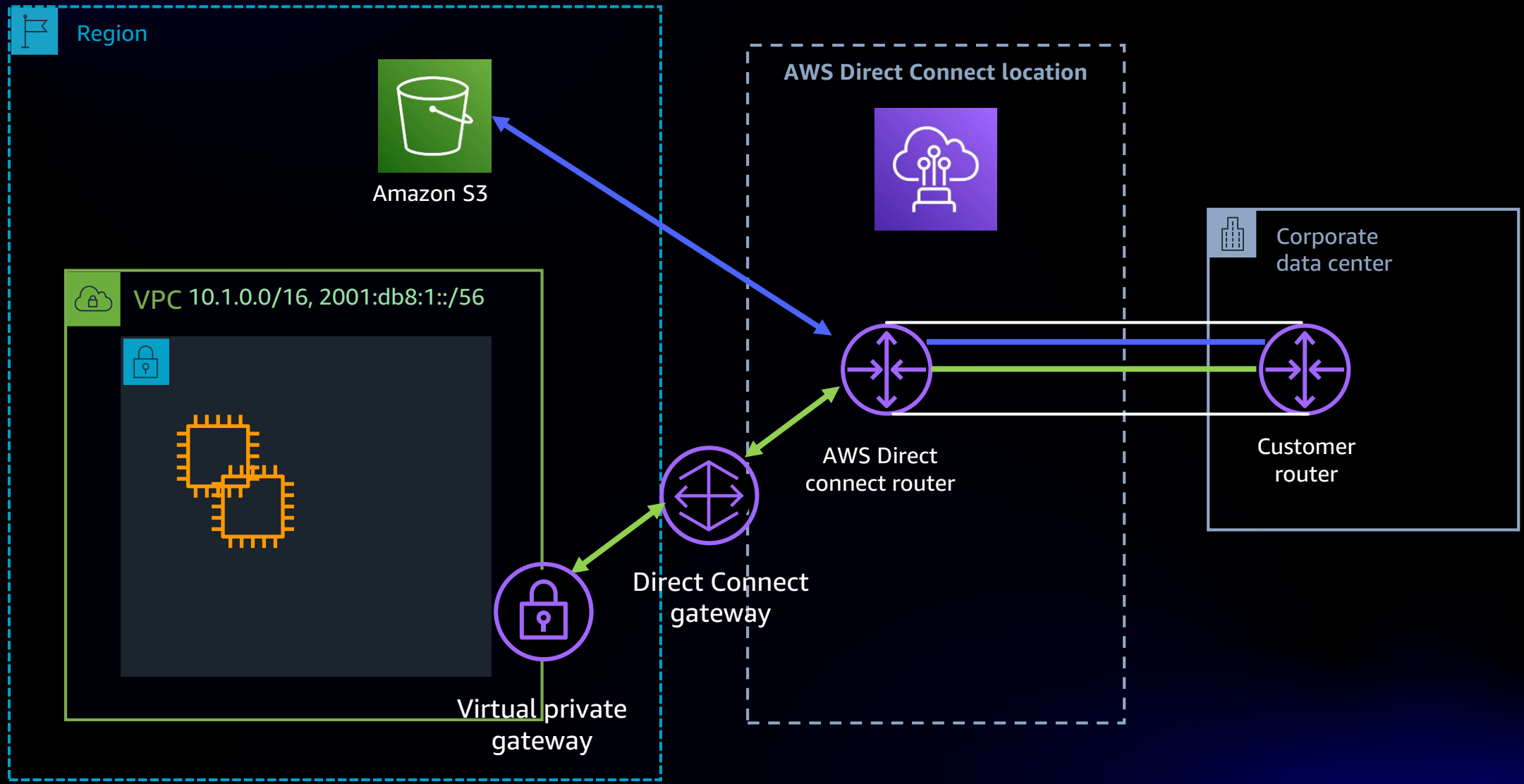
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Direct Connect



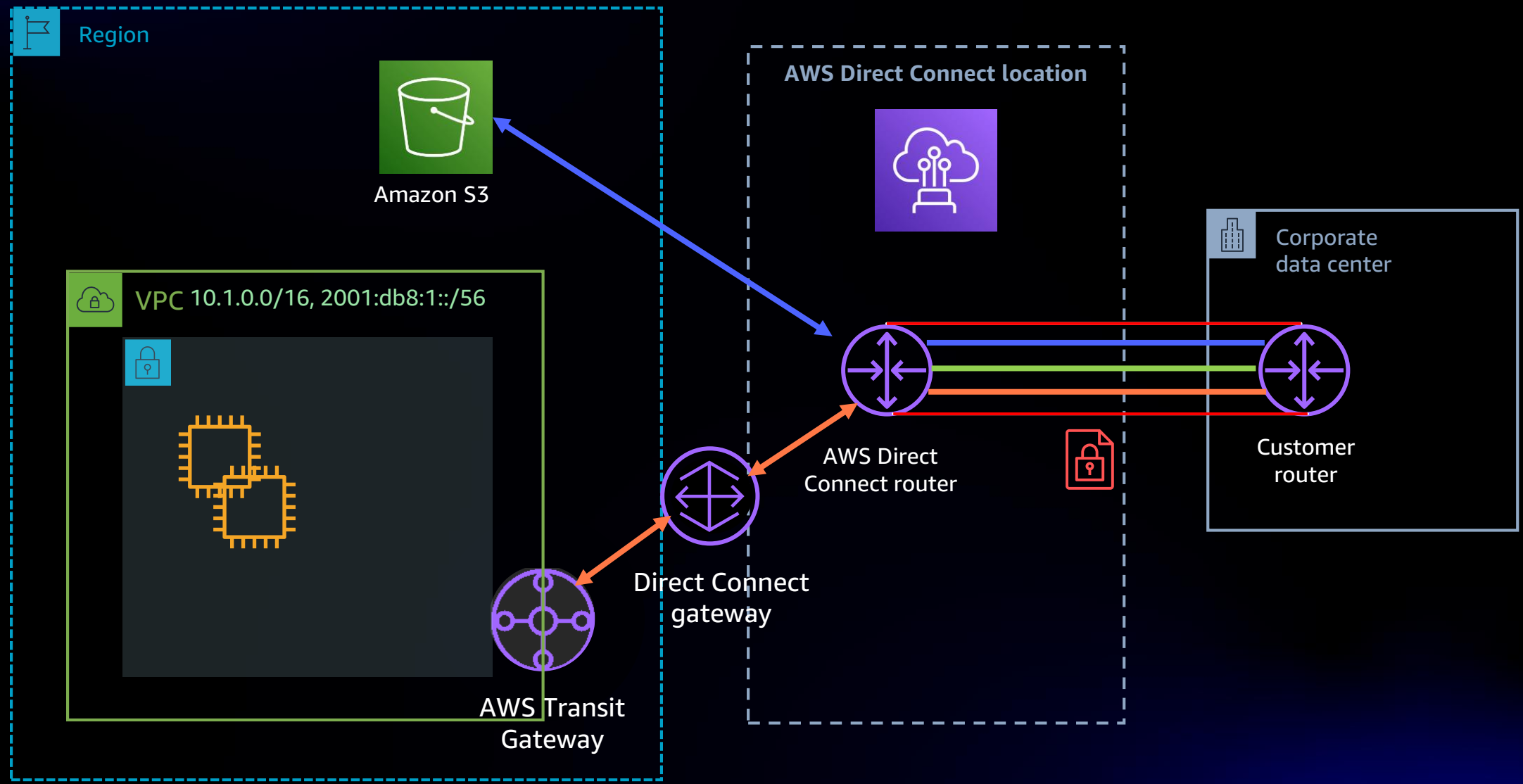

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Direct Connect



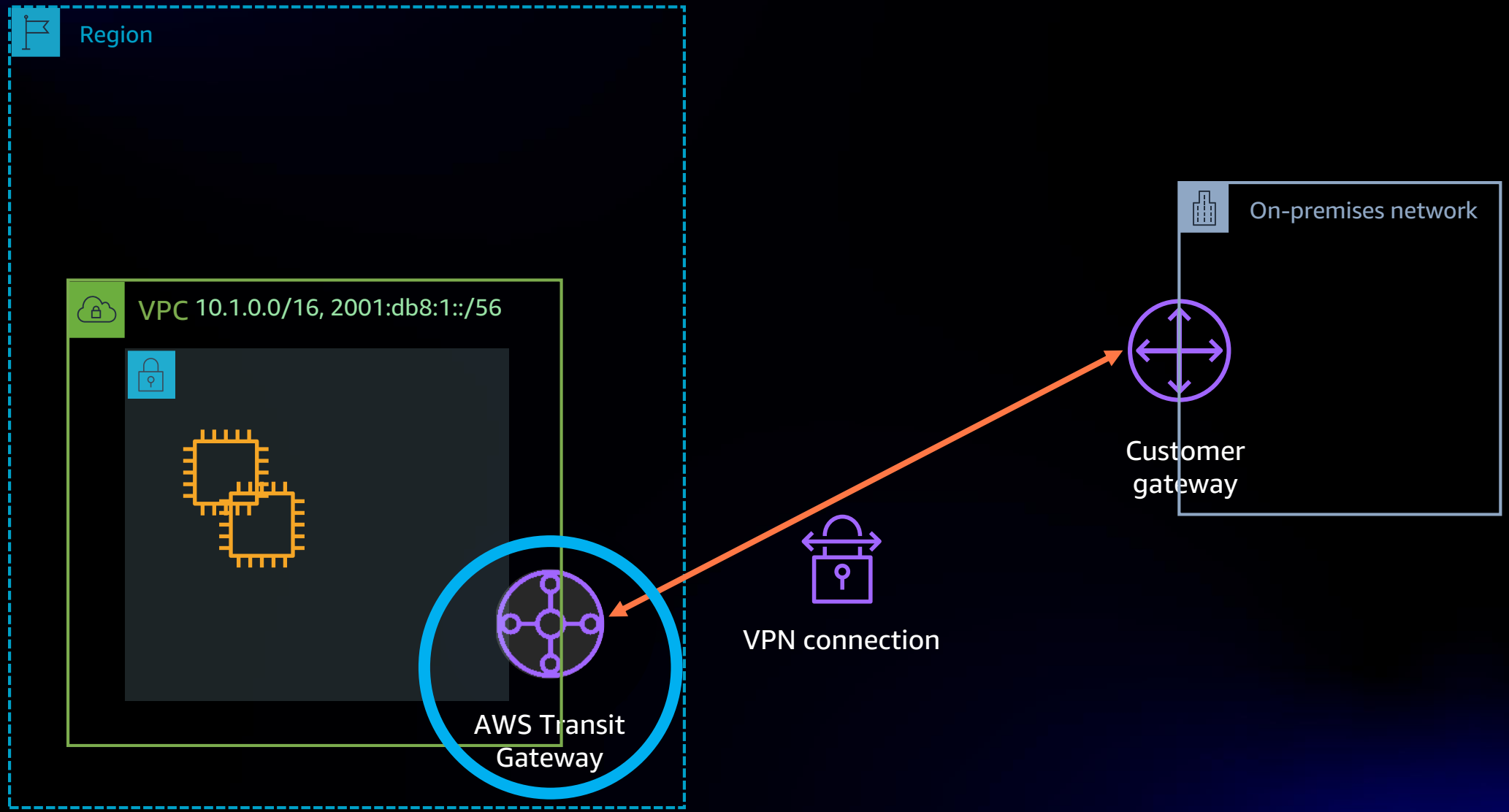

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Direct Connect



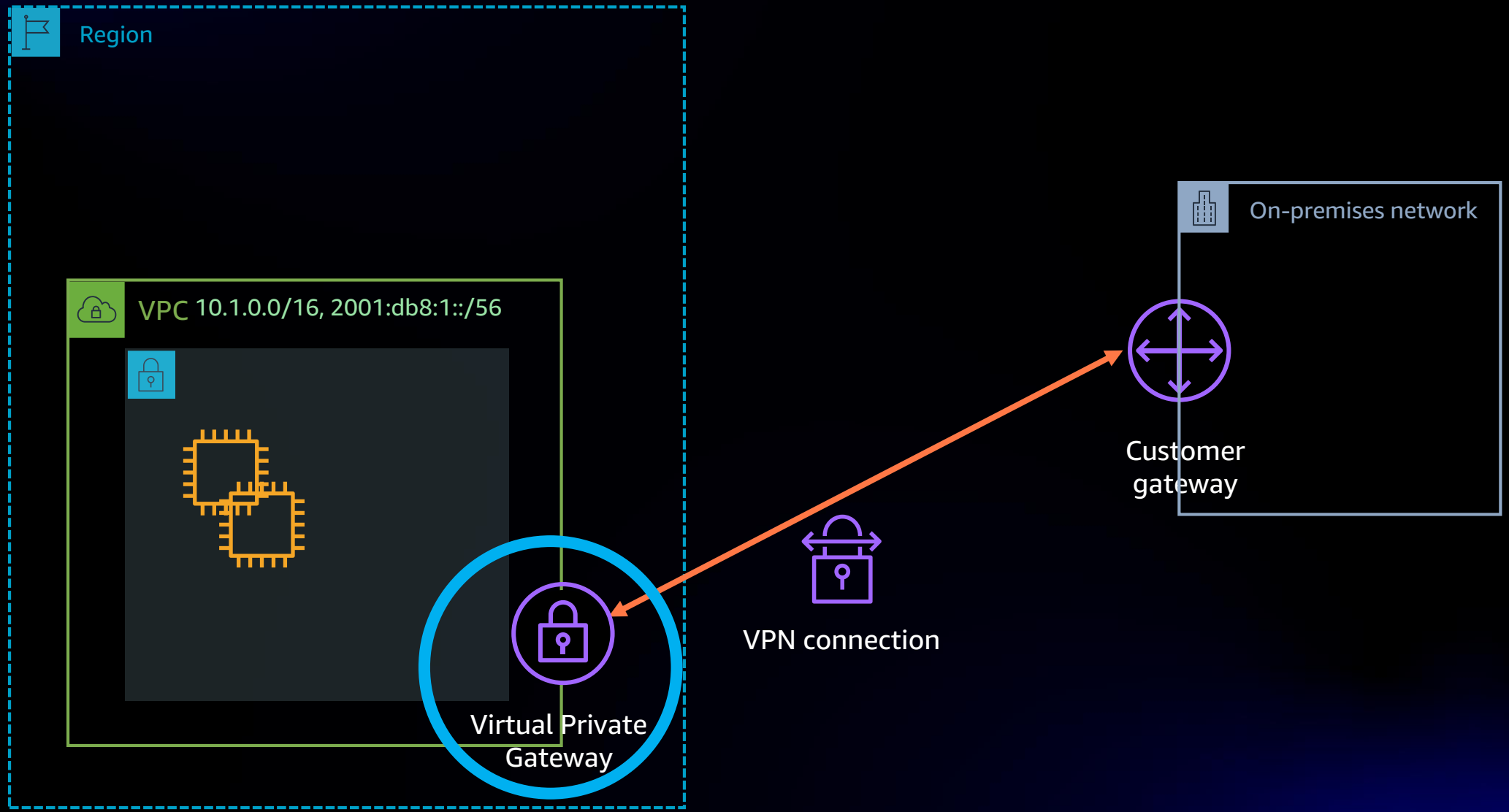

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Site-to-Site VPN



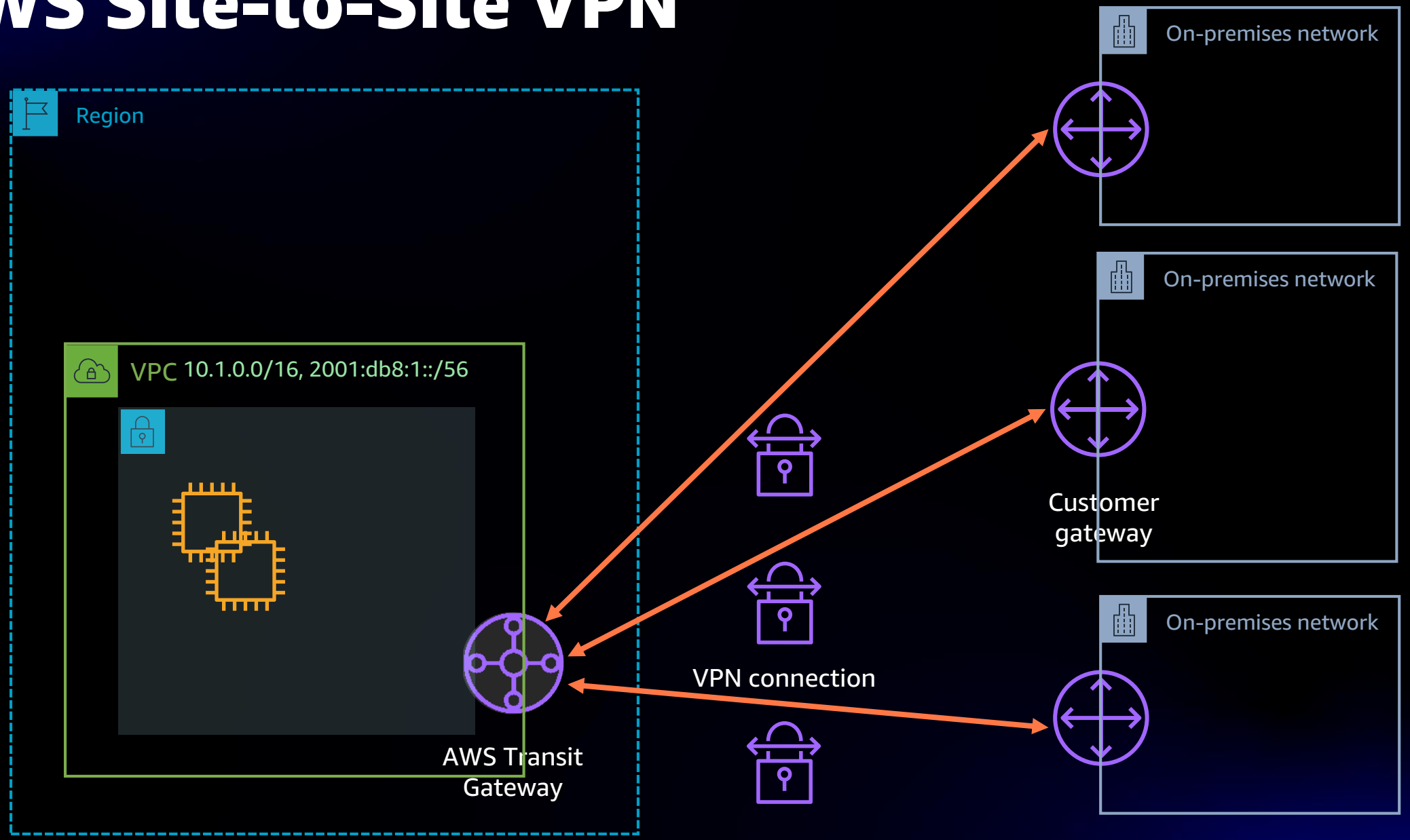

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Site-to-Site VPN



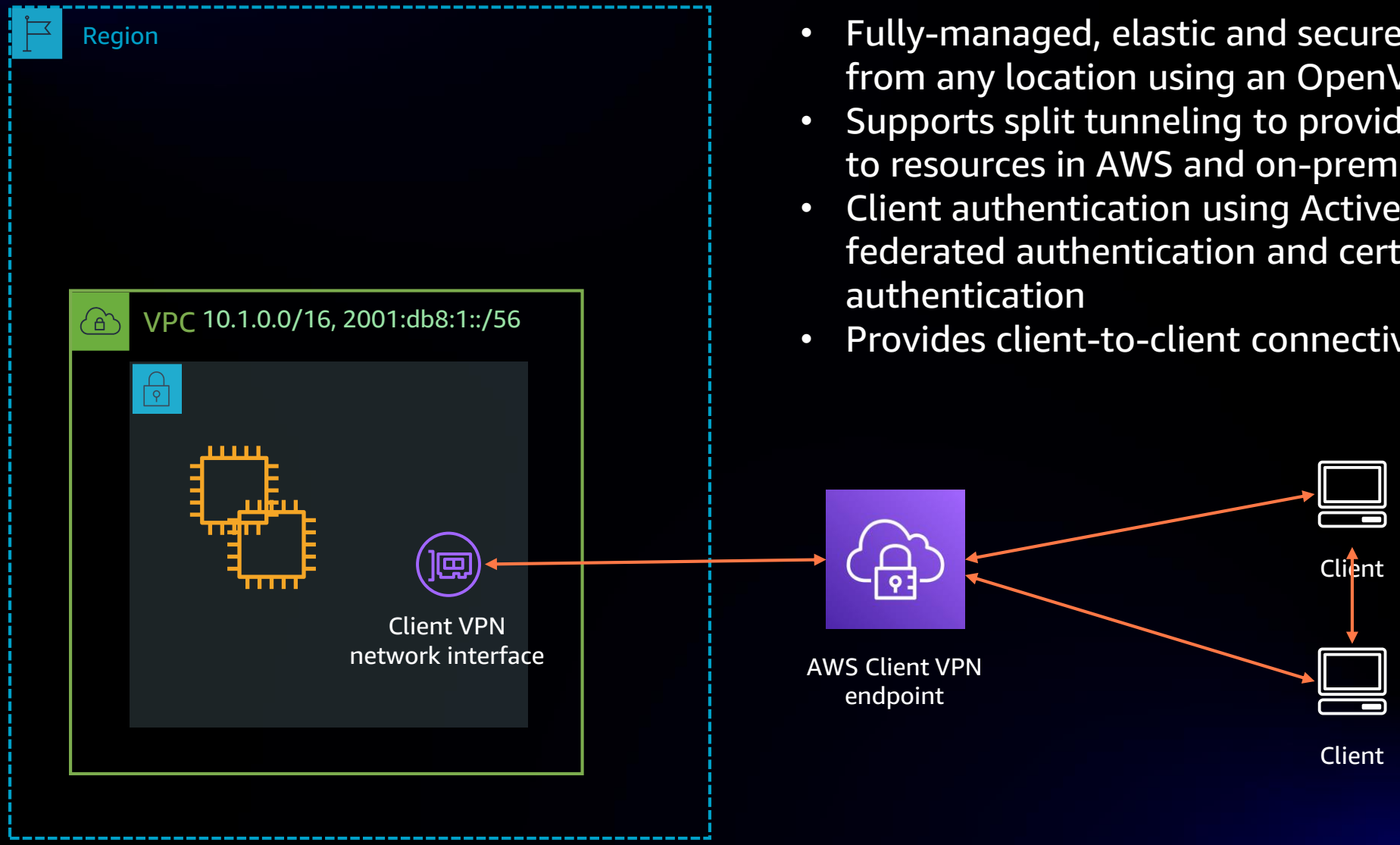

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Site-to-Site VPN




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

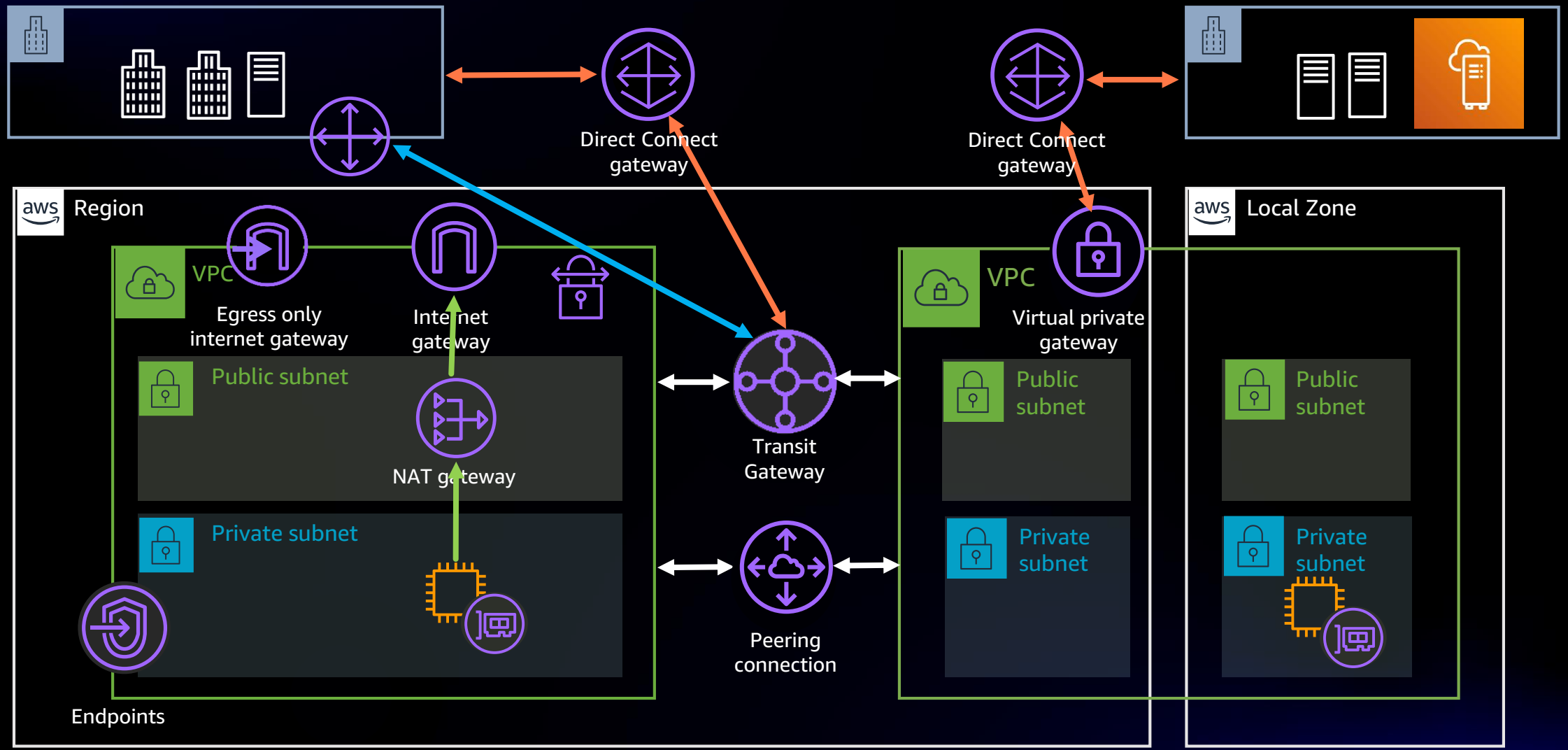
# AWS Client VPN




- Fully-managed, elastic and secure TLS connections from any location using an OpenVPN based client
- Supports split tunneling to provide secured access to resources in AWS and on-premises network
- Client authentication using Active Directory, federated authentication and certificate-based authentication
- Provides client-to-client connectivity

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

# Bringing it all together

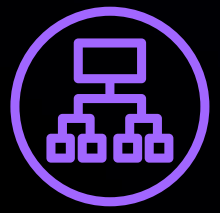



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

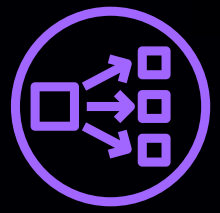
# Load balancing and traffic management

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

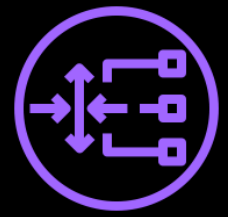
# Elastic Load Balancing



Application Load Balancer



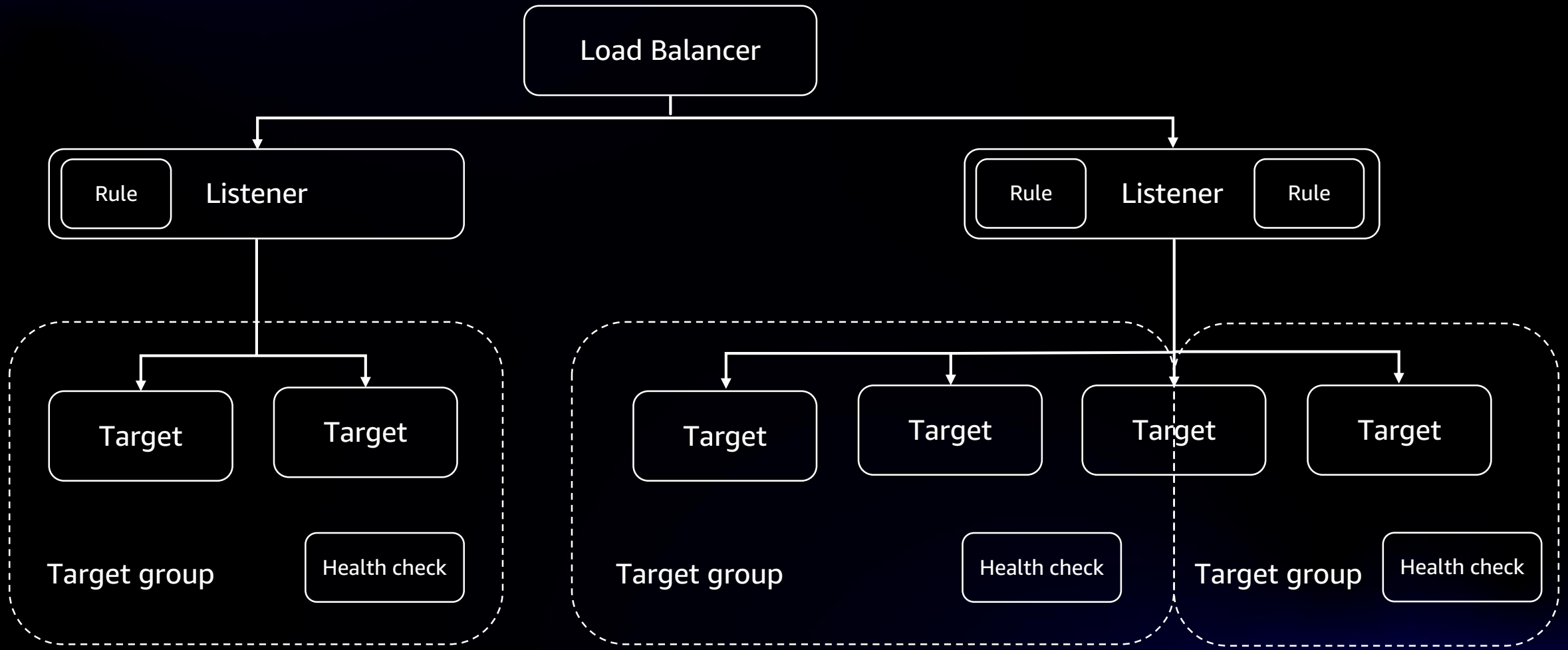
Network Load Balancer



Gateway Load Balancer

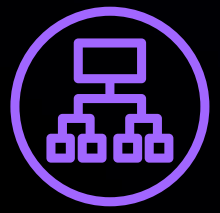
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Elastic Load Balancing

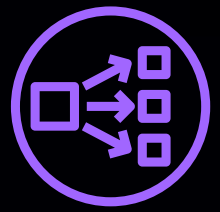



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

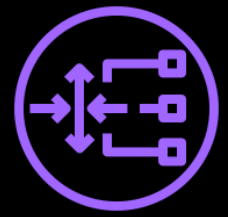
# Elastic Load Balancing



Application Load Balancer



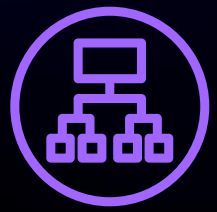
Network Load Balancer



Gateway Load Balancer

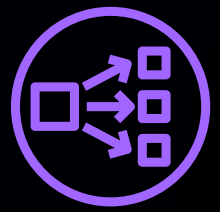
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Elastic Load Balancing



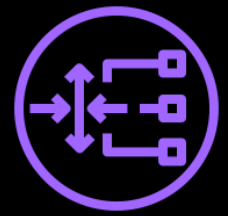
Application Load Balancer

- Layer 7
- Targets: IP, instance, AWS Lambda
- Terminates flows
- Listener: HTTP, HTTPS, gRPC
- Front end: virtual IP



Network Load Balancer

- Layer 4
- Targets: IP, instance, Application Load Balancer
- Terminates flows
- Listener: TCP, UDP, TLS
- Front end: virtual IP



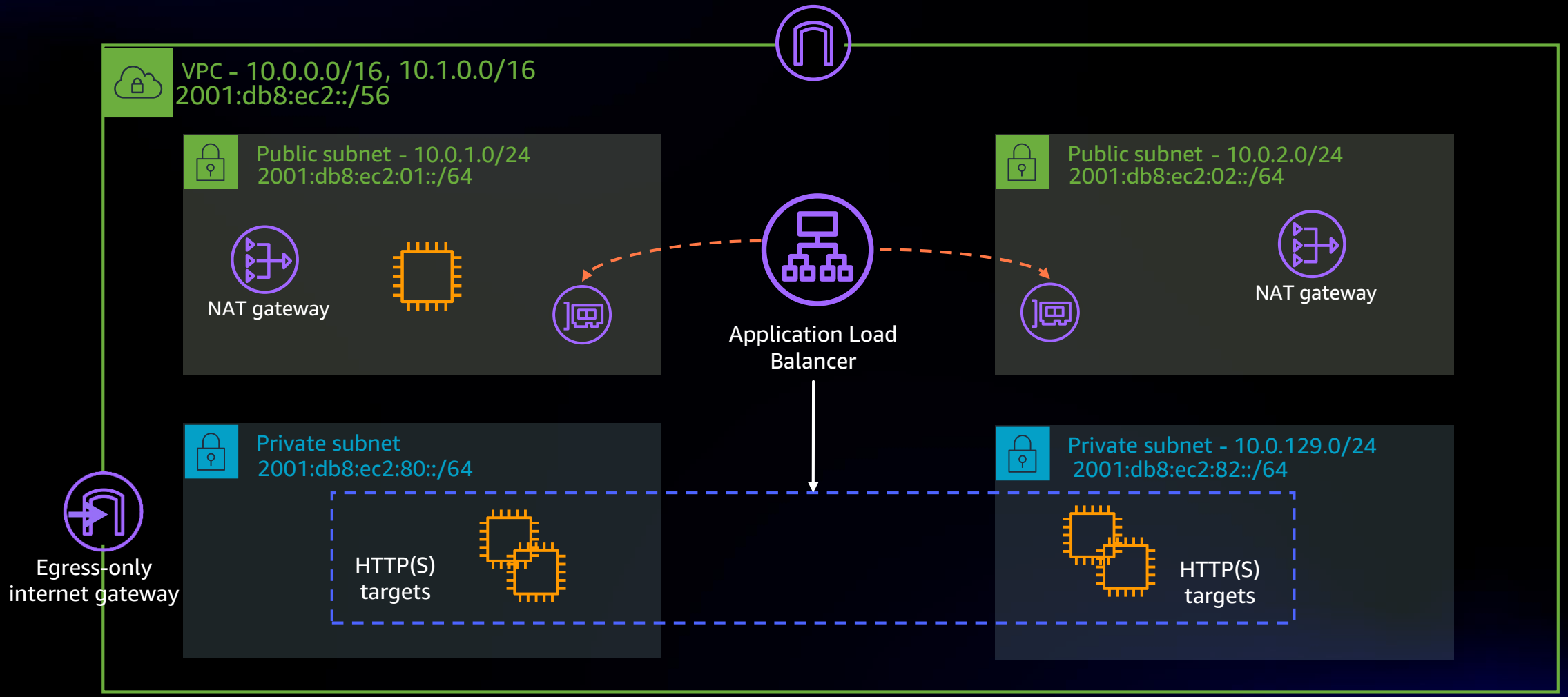
Gateway Load Balancer

- Layer 3 gateway and Layer 4 load balancing
- Targets: IP, instance
- Transparent pass through of flows
- Listener: IP
- Route table entry

aws

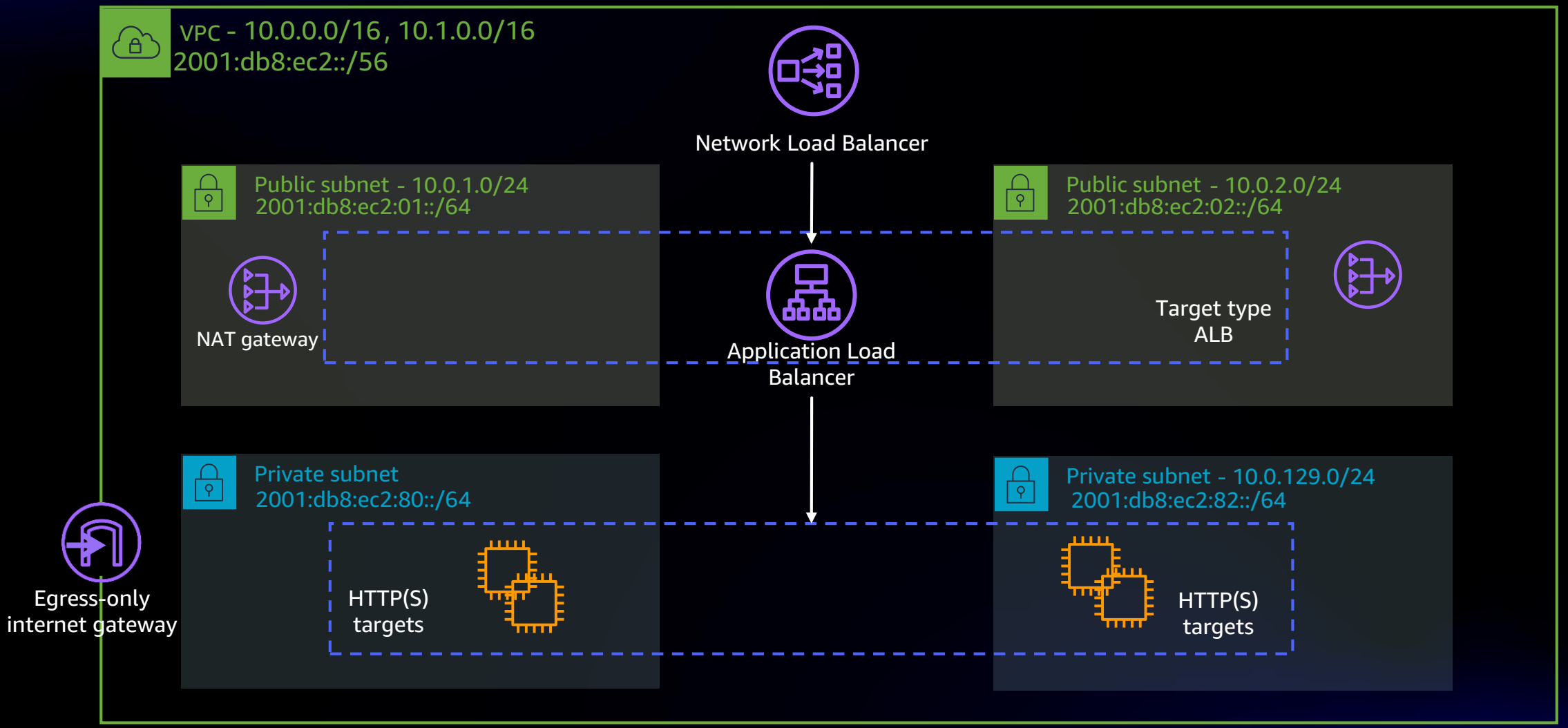
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Elastic Load Balancing




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

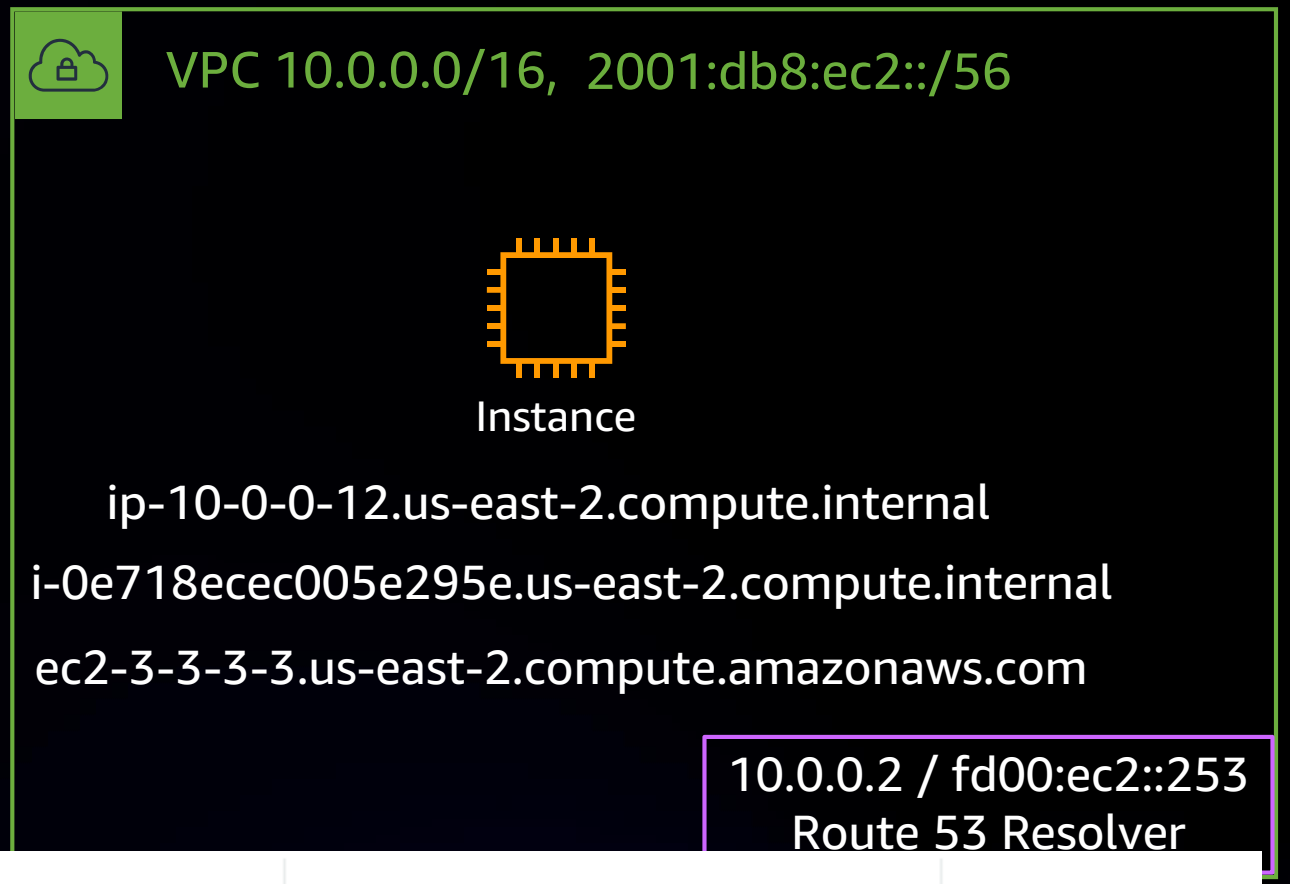
# Elastic Load Balancing




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

# Amazon Route 53 Resolver for VPC

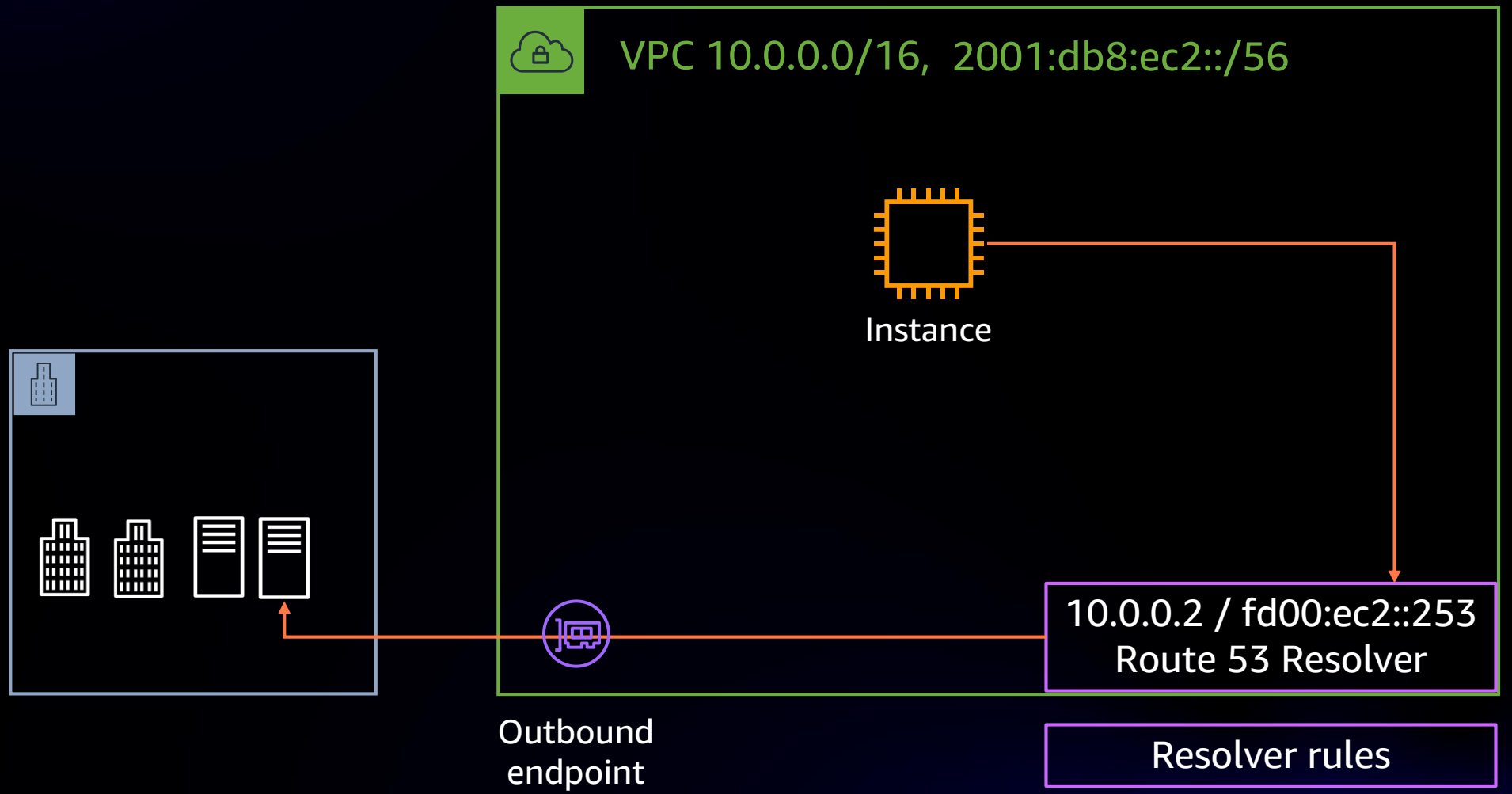
- AmazonProvidedDNS
  - VPC+2 resolver
  - 169.254.169.253
  - fd00:ec2::253
- DNS host names
  - Private DNS name
  - Resource based private DNS name
  - Public DNS name




| VPC ID | State | DNS hostnames | DNS resolution |
|---|---|---|---|
| vpc-0f61364f7d544be00 | Available | Enabled | Enabled |

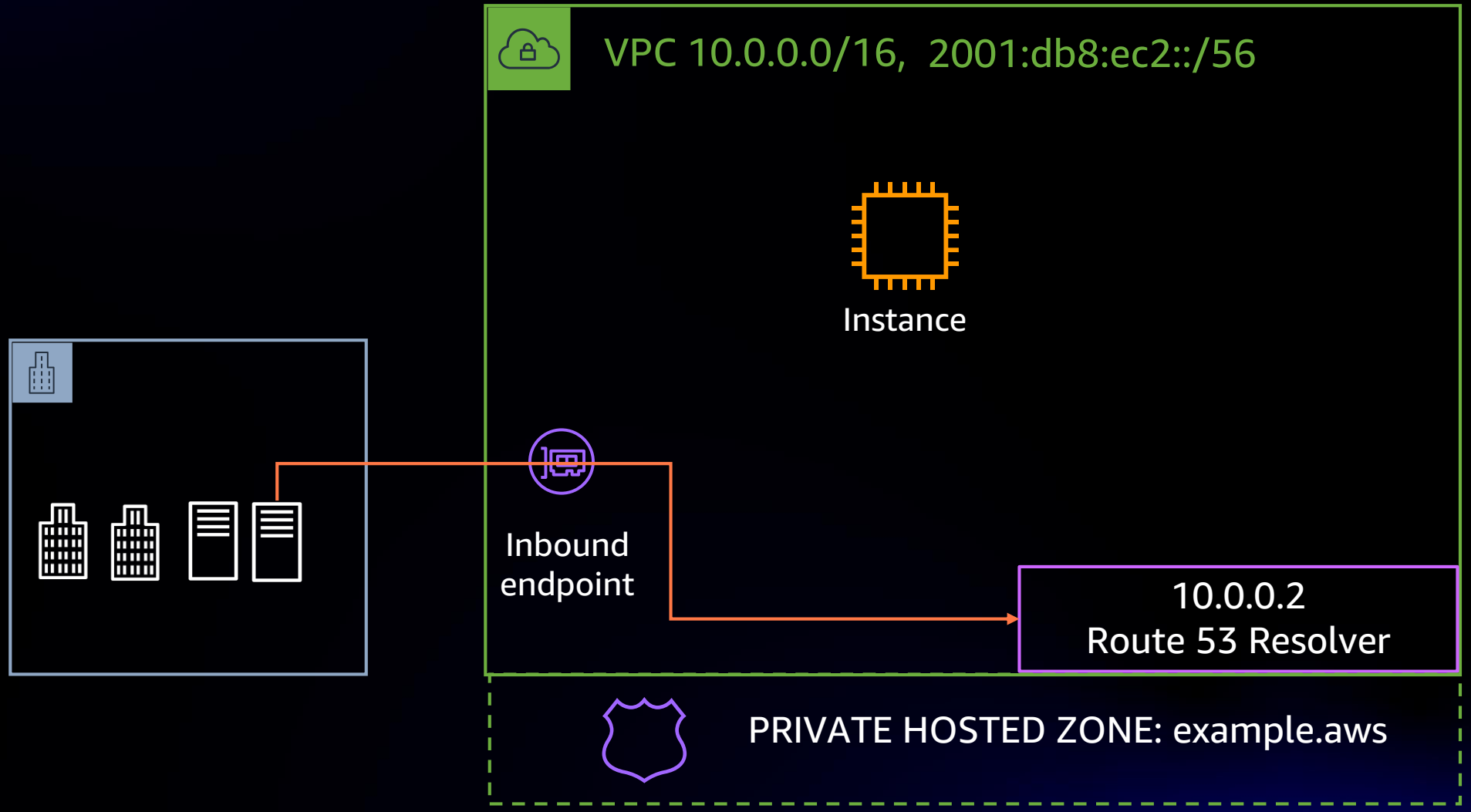
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Route 53 Resolver endpoints



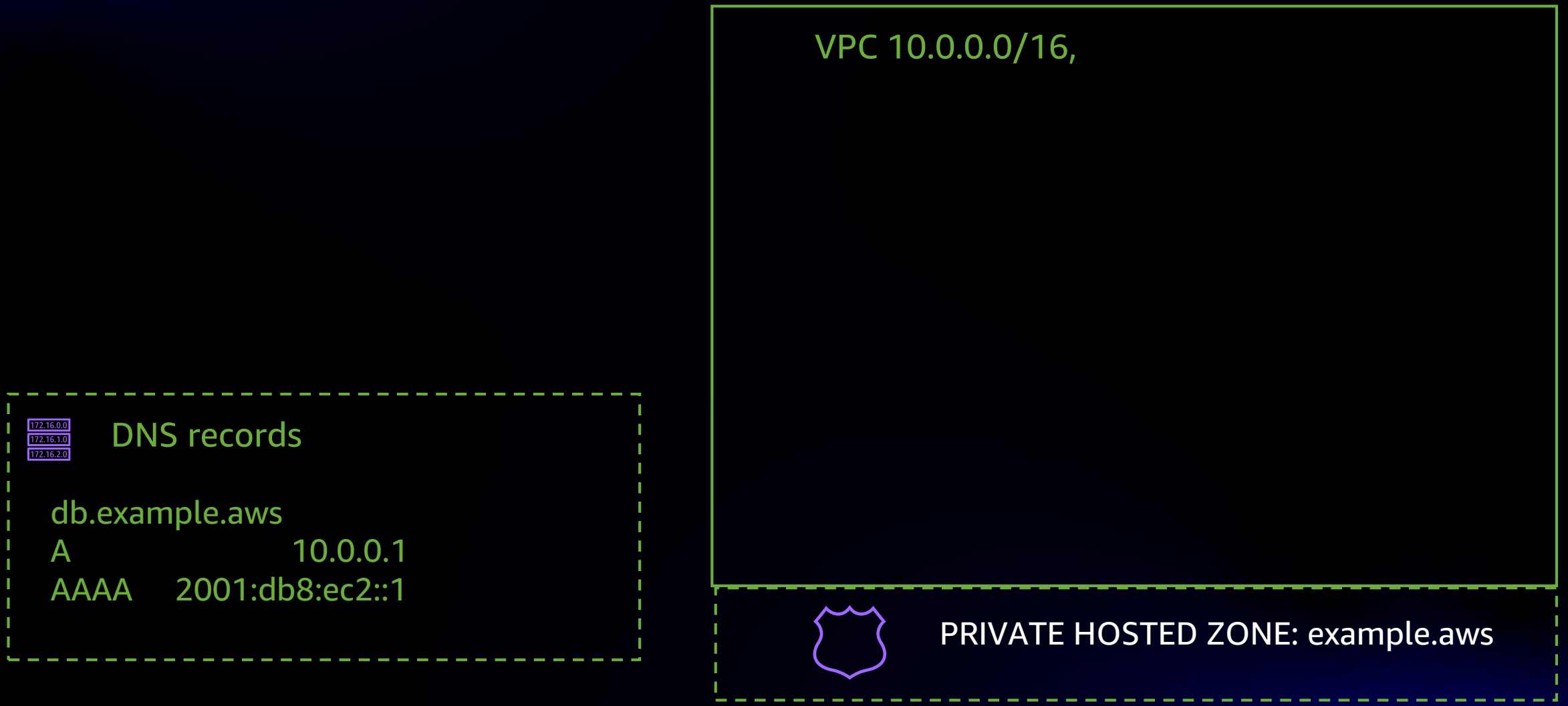

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Route 53 Resolver endpoints



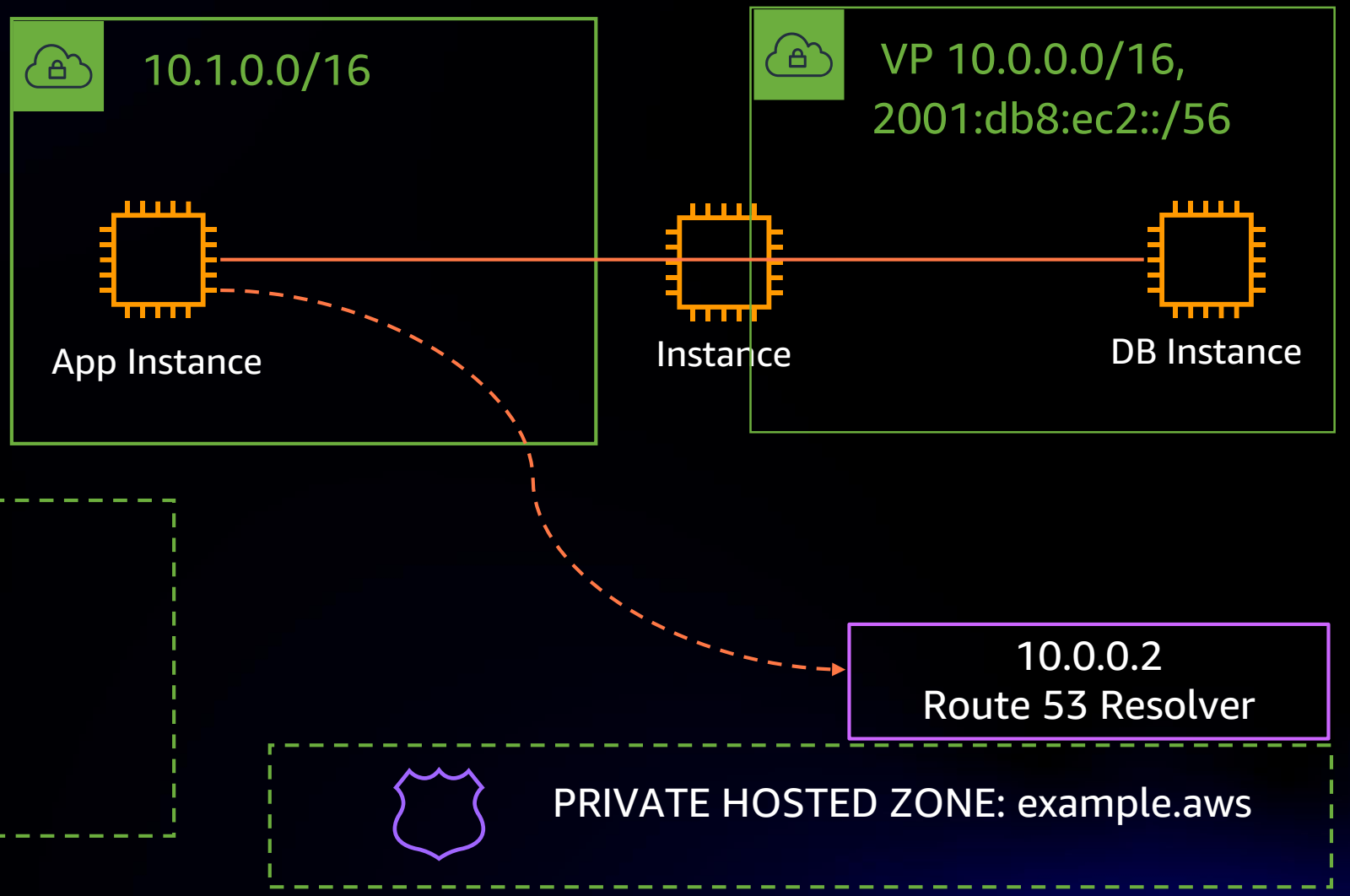

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Route 53 private hosted zones



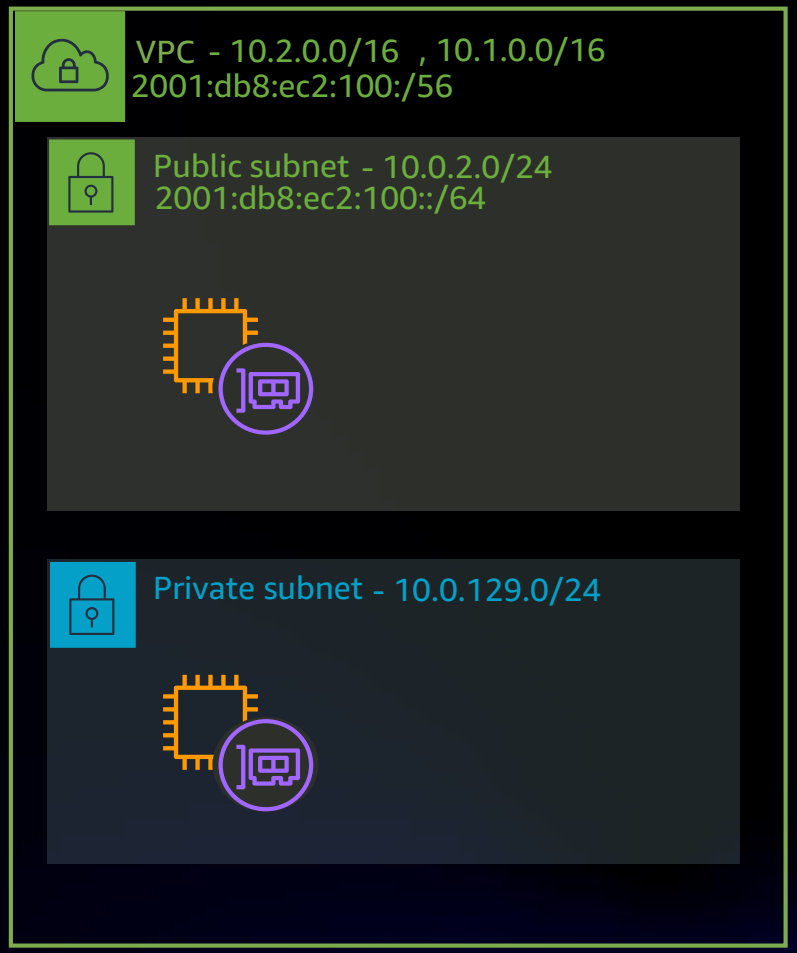

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Route 53 private hosted zones



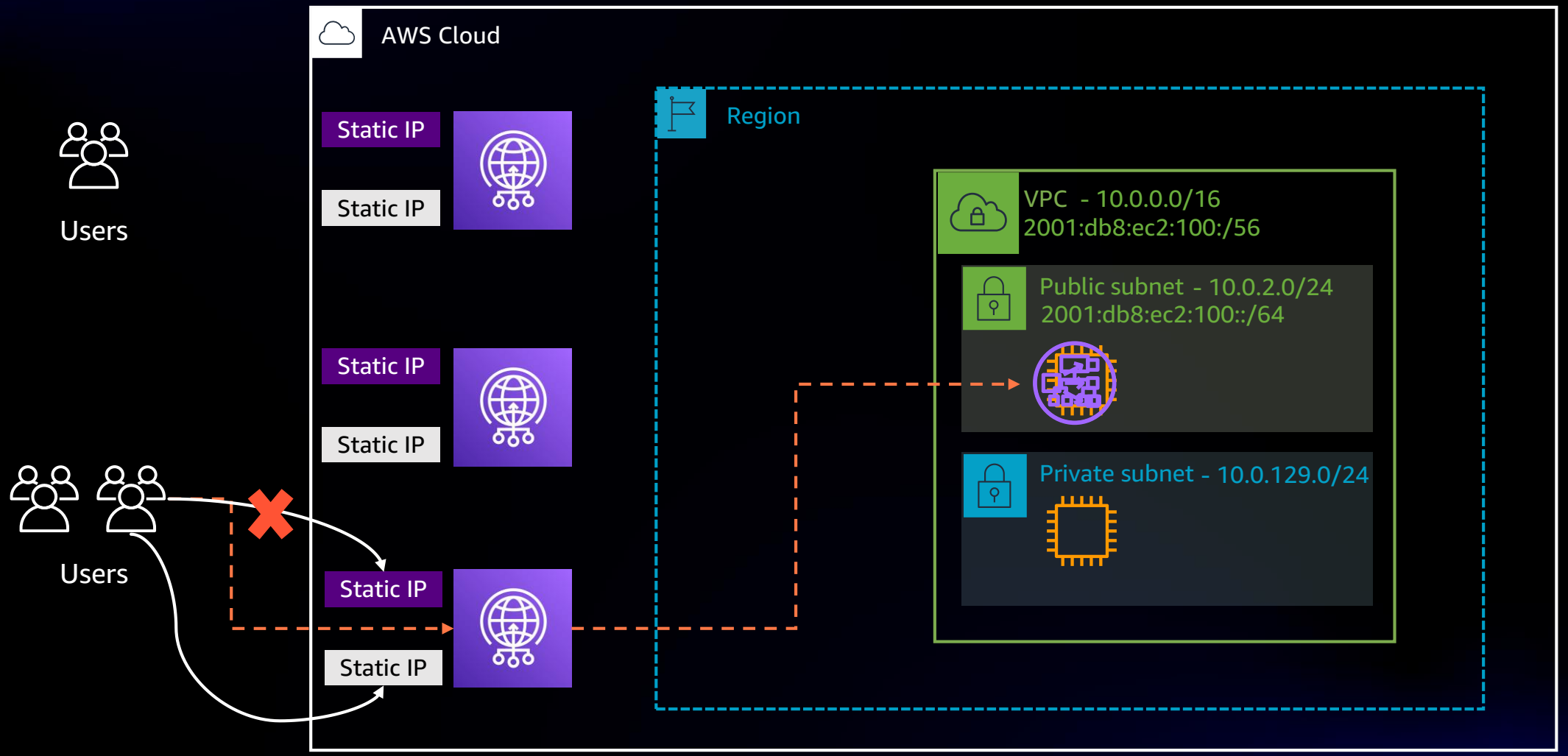

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Global Accelerator



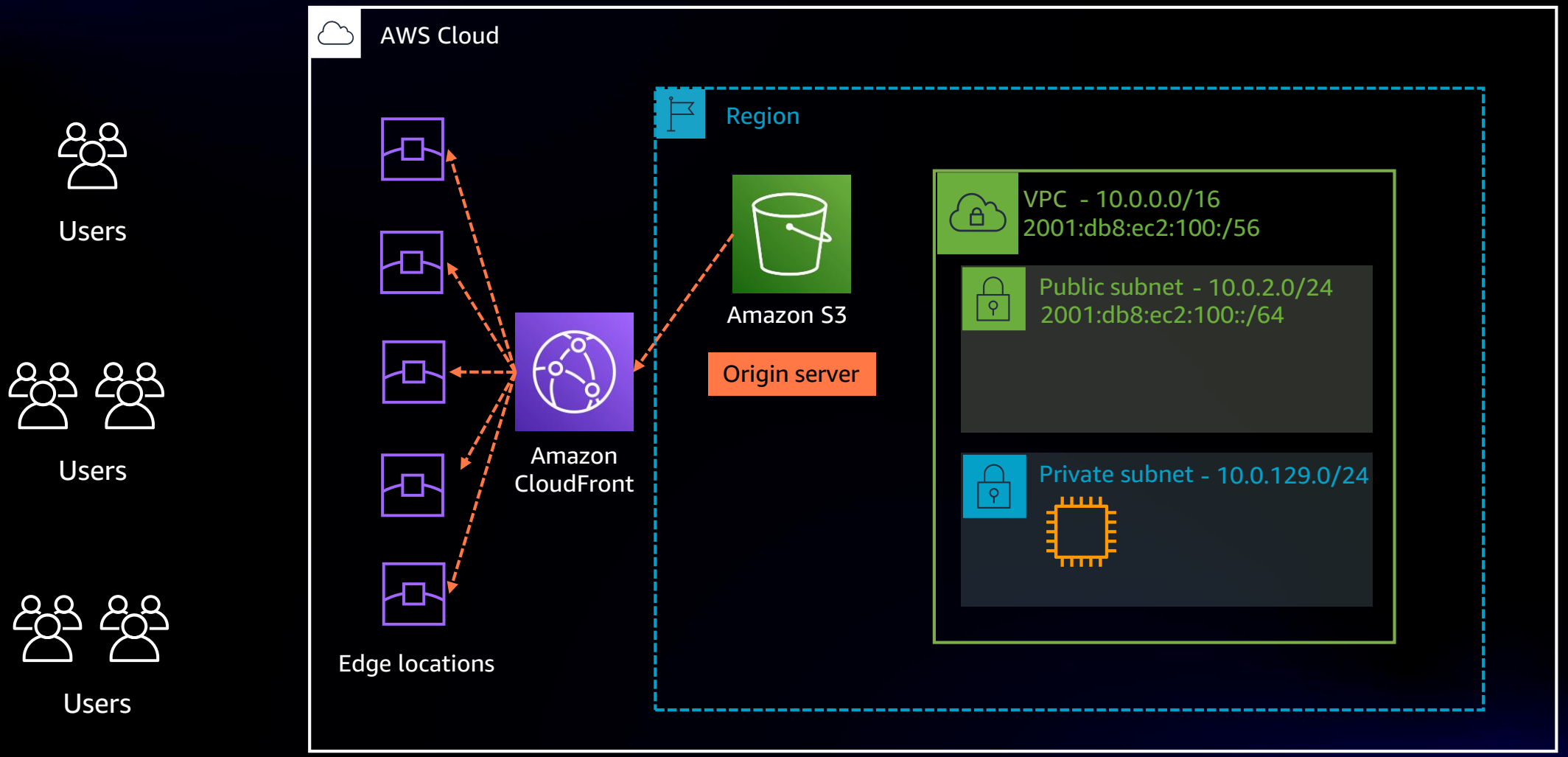

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Global Accelerator



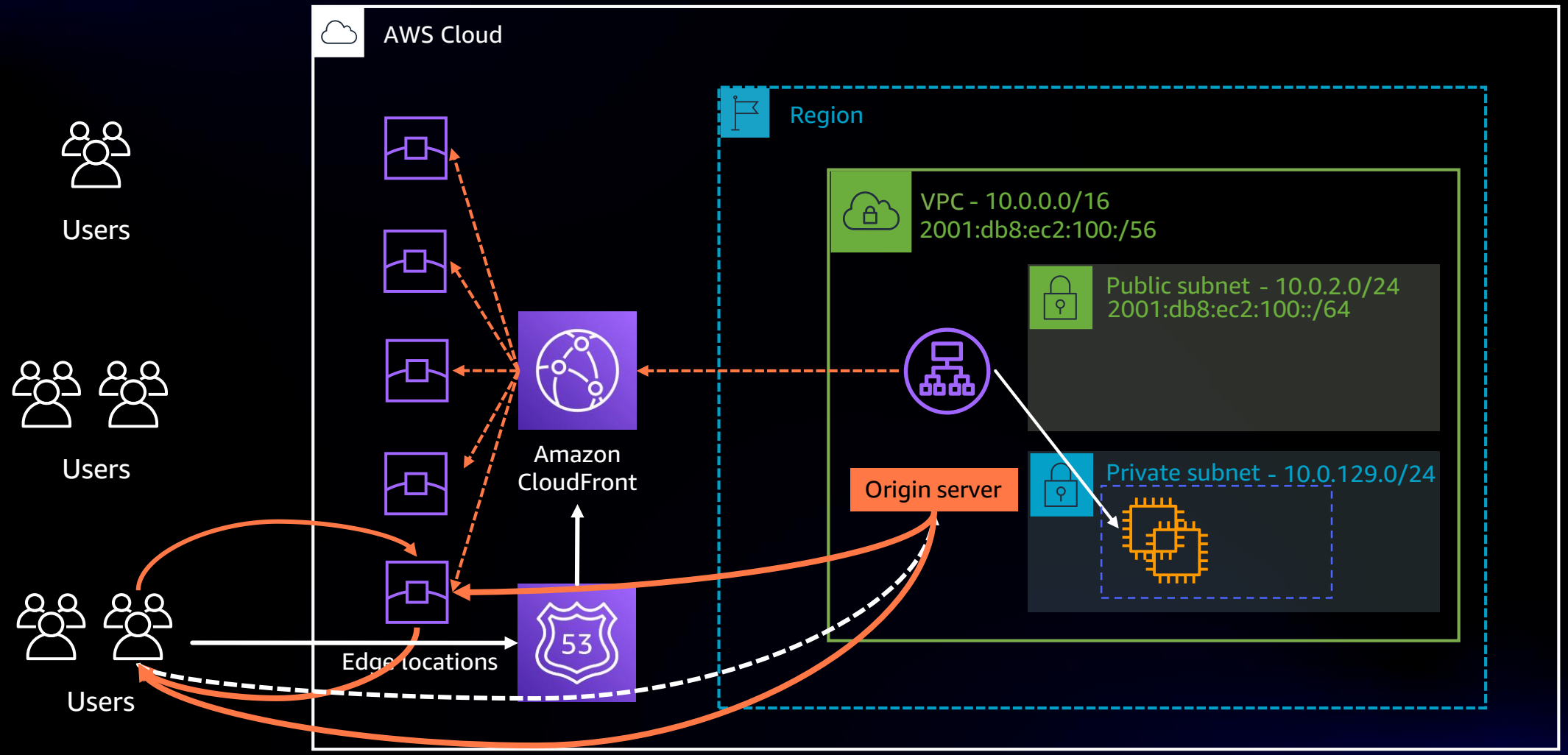

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon CloudFront




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

# Bringing it all together




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



# Security services

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

# AWS Shield



24/7 access to DDoS Response Team (DRT)

Point and Protect Wizard

Amazon CloudWatch Metrics

Enhanced protection baselined to you

Built-in DDoS protection for everyone

Application Load Balancer

Classic Load Balancer

Elastic IP Address

Network Load Balancer

AWS Global Accelerator

Automatic protection across customers

Amazon CloudFront

Amazon Route 53

EC2 Instances

Attack diagnostics

Global threat environment dashboard

Cost protection for scaling

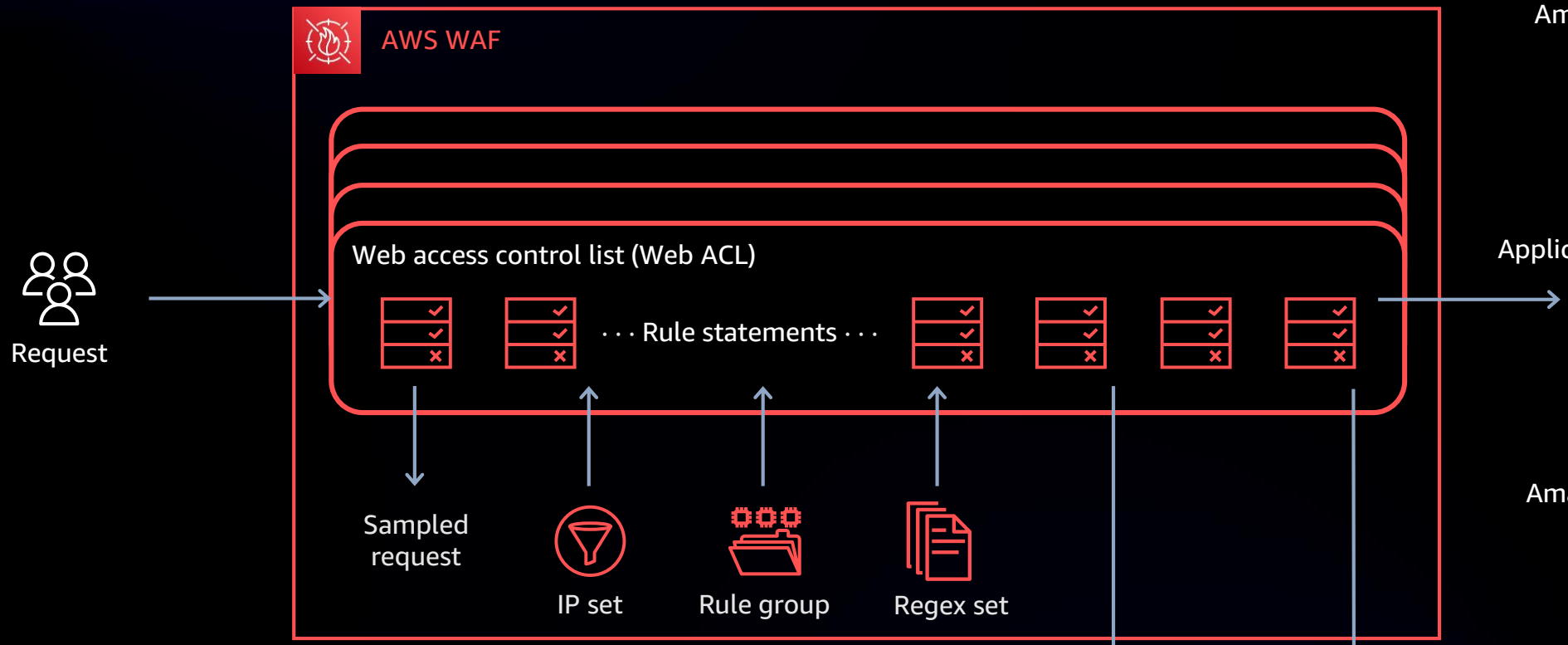
Quarterly security review

aws

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

# AWS WAF






Amazon CloudFront

Application Load Balancer

Amazon API Gateway

AWS AppSync

Amazon Kinesis Data Firehose

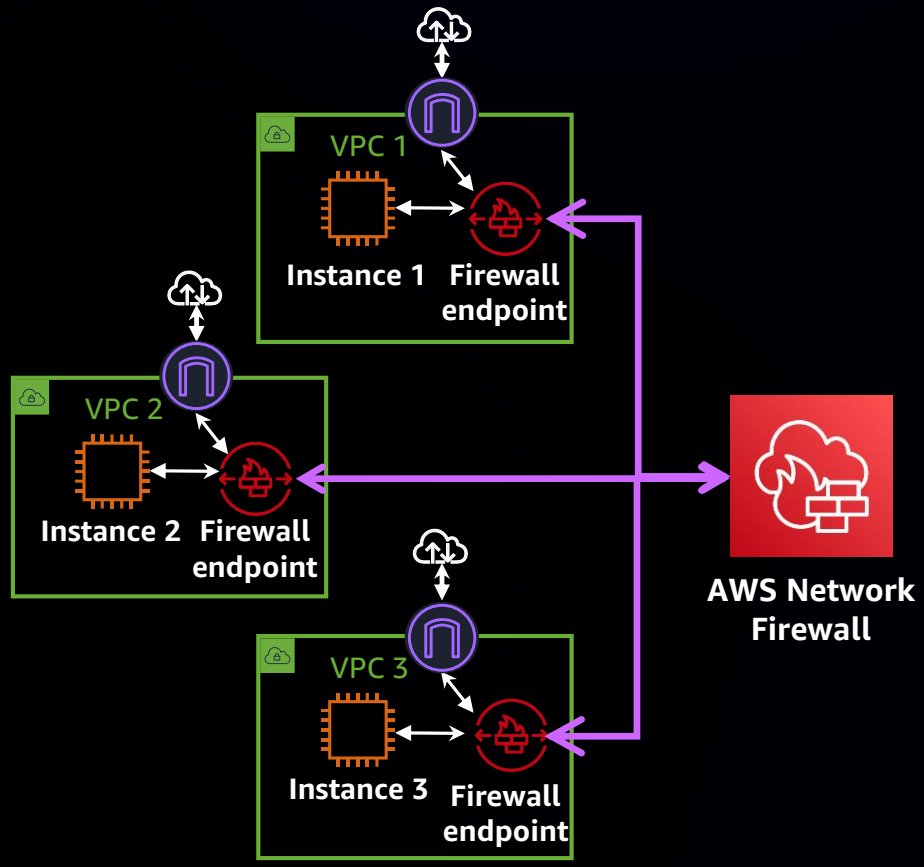
Amazon CloudWatch

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

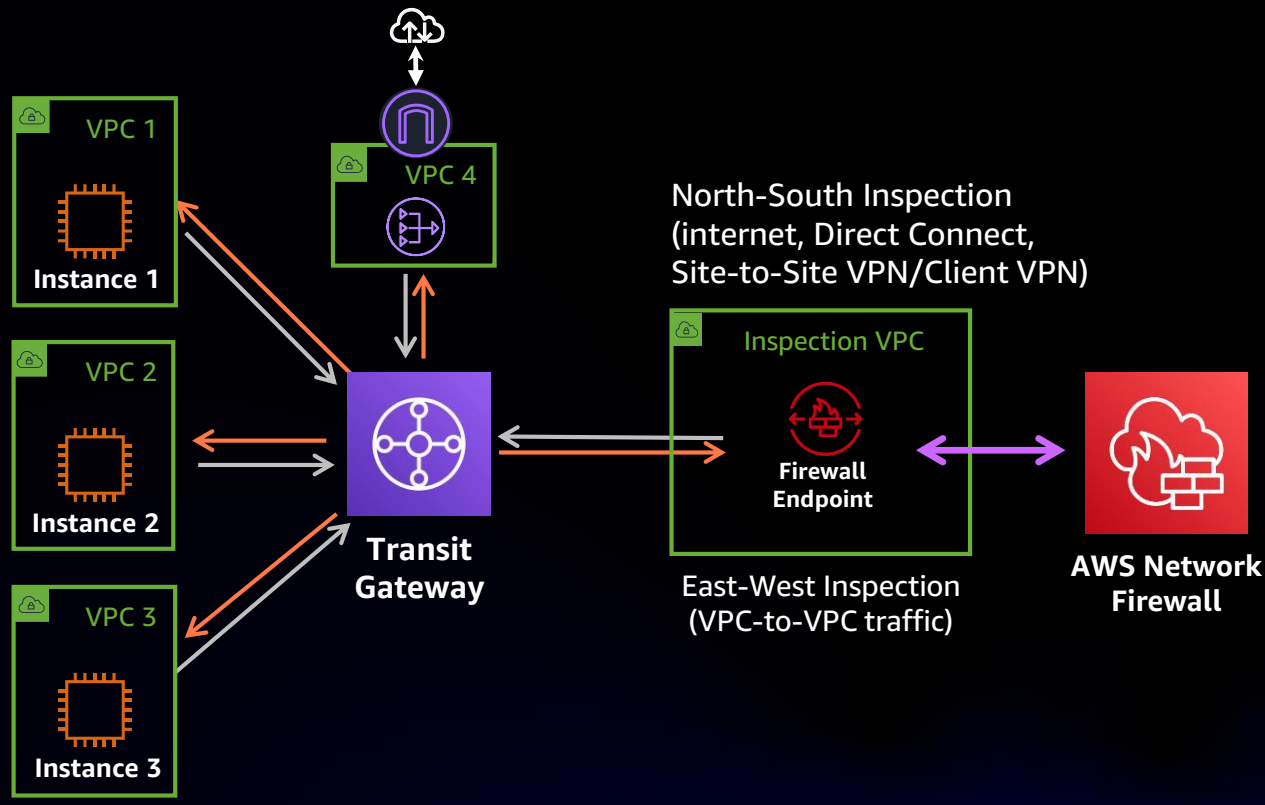
# AWS Network Firewall



## Distributed security inspection

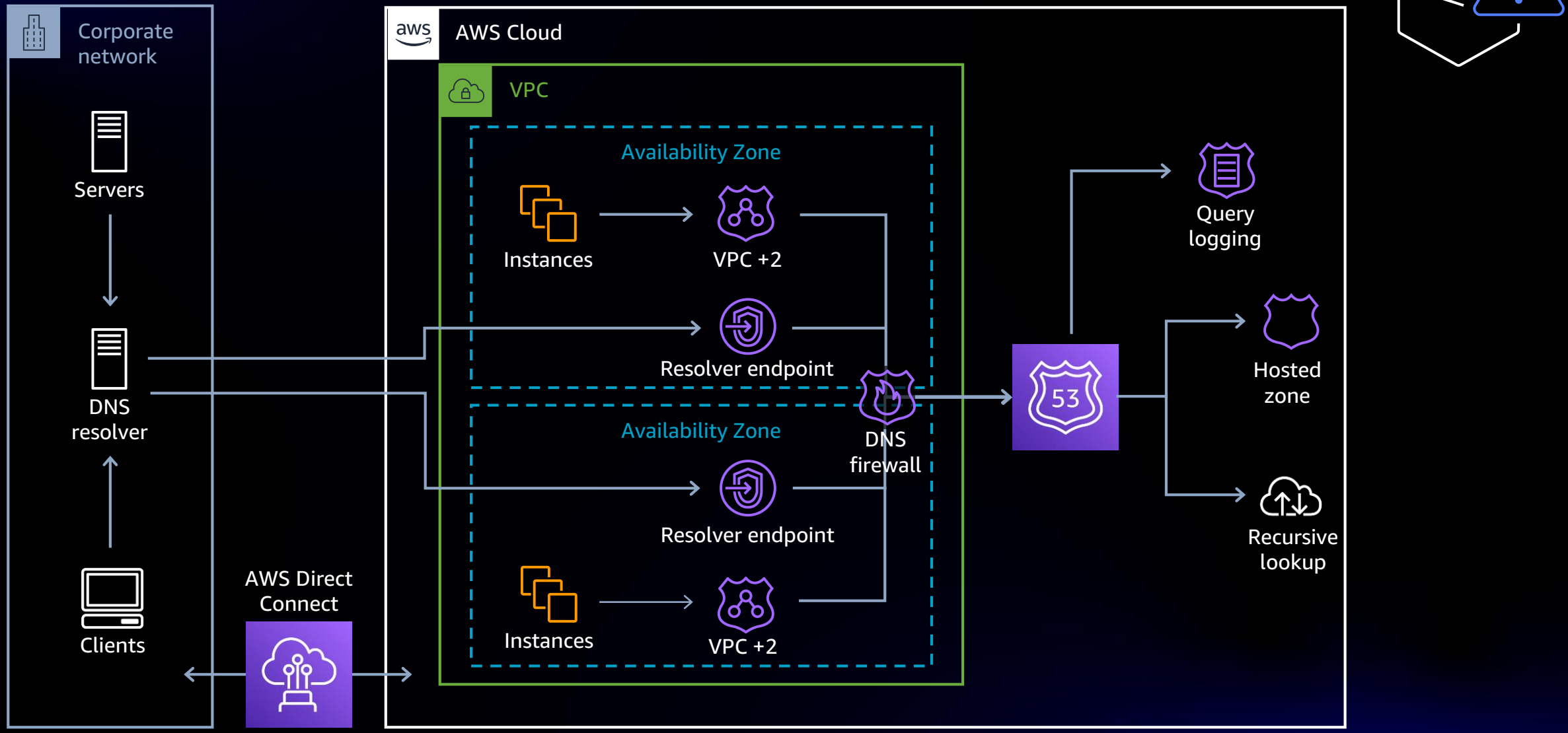



## Centralized security inspection




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

# Amazon Route 53




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

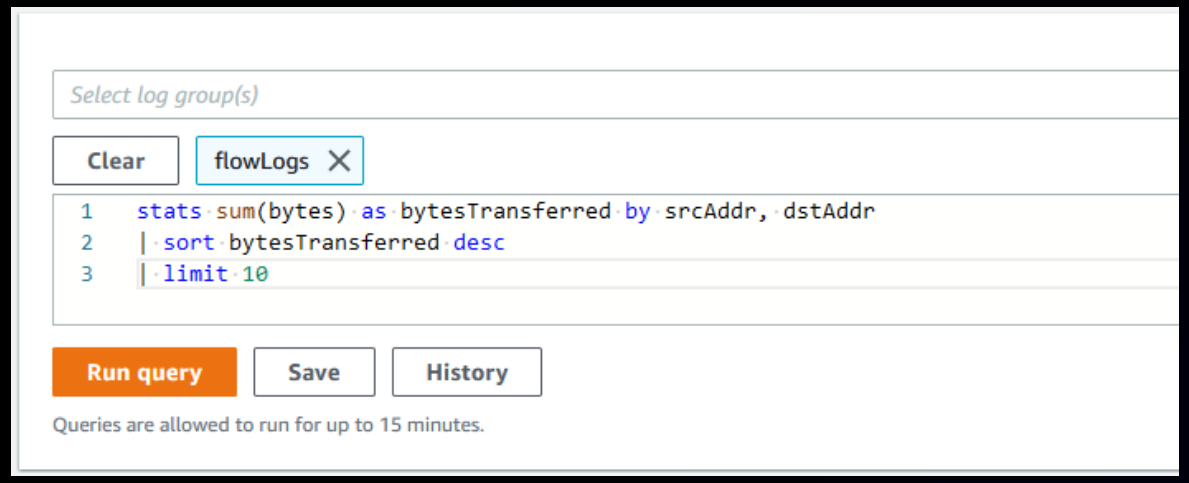
# VPC Flow Logs

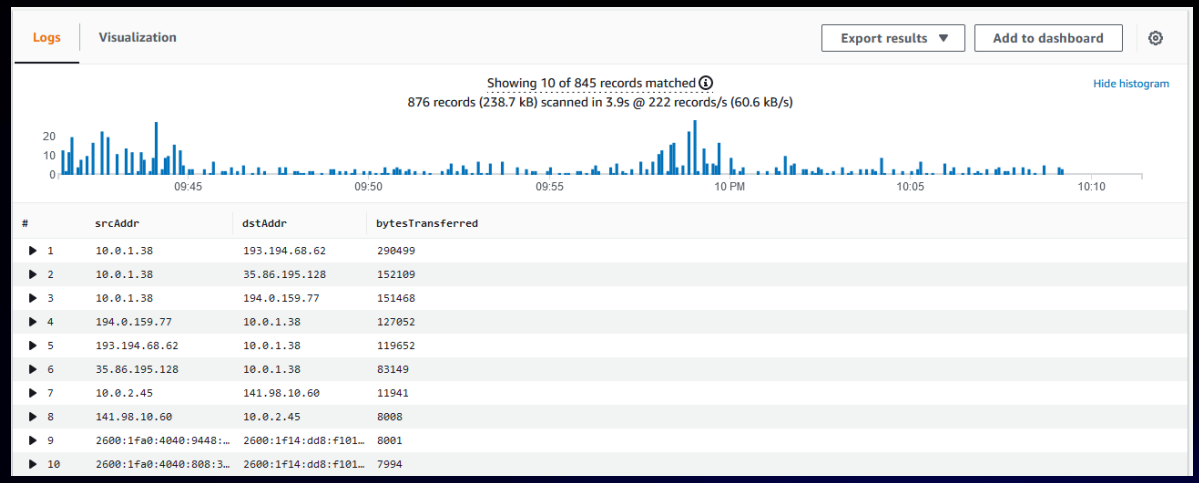


```
version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status vpc-id
subnet-id instance-id tcp-flags type pkt-srcaddr pkt-dstaddr region az-id sublocation-type sublocation-id pkt-src-aws-
service pkt-dst-aws-service flow-direction traffic-path

5 123456789097 eni-044feef0 52.218.241.56 10.0.1.38 443 58460 6 19 7710 1634606470 1634606481 ACCEPT OK vpc-
0a19b648 subnet-094ee201 i-08bcbe49 19 IPv4 52.218.241.56 10.0.1.38 us-west-2 usw2-az2 - - S3 - ingress -

5 123456789097 eni-044feef0 2001:db2:1:f102::6 2001:db2:1:f101::f 0 0 58 10 1040 1634606496 1634606497 ACCEPT OK vpc-
0a19b648 subnet-094ee201 i-08bcbe49 0 IPv6 2001:db2:1:f102::6 2001:db2:1:f101::f us-west-2 usw2-az2 - - EC2 EC2 ingress -
```

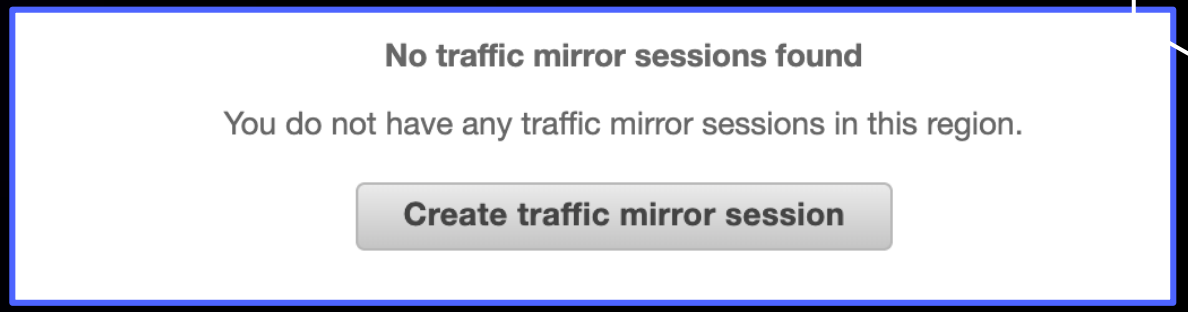


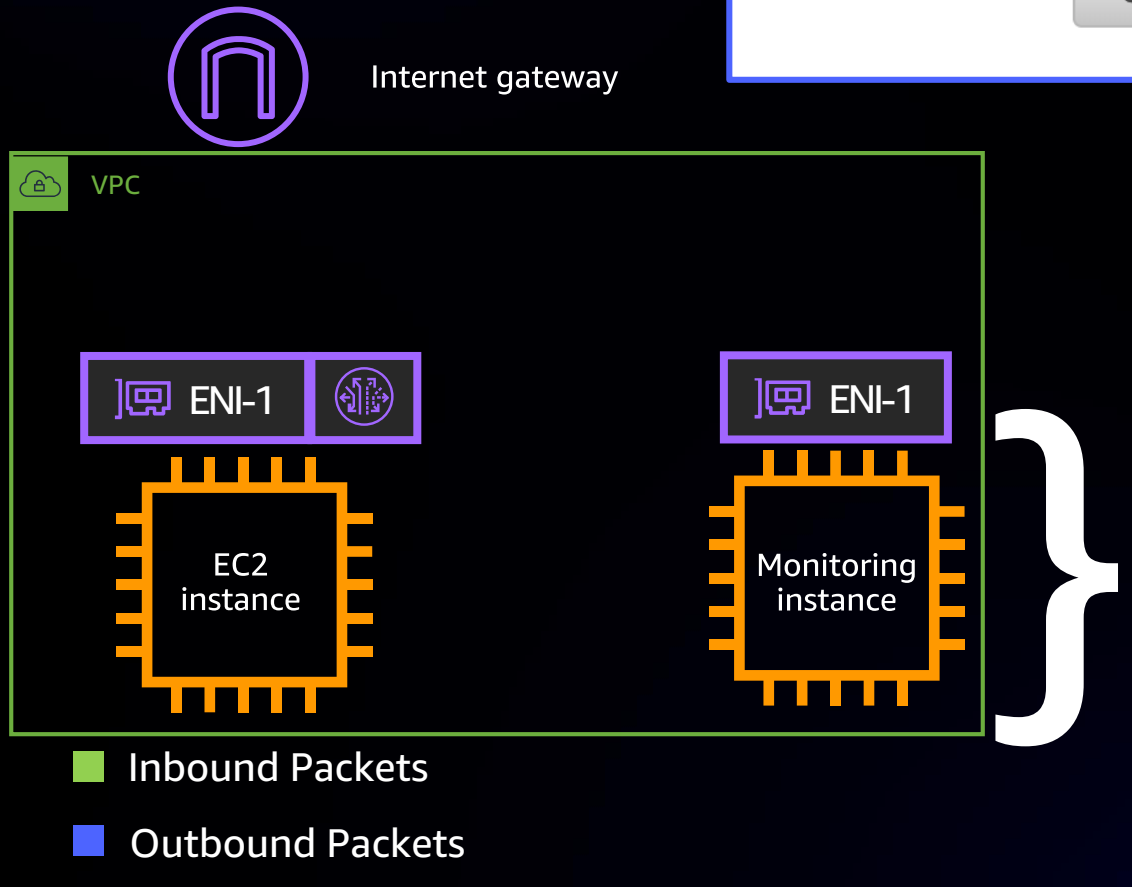




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# VPC Traffic Mirroring






Build your own traffic analyzer

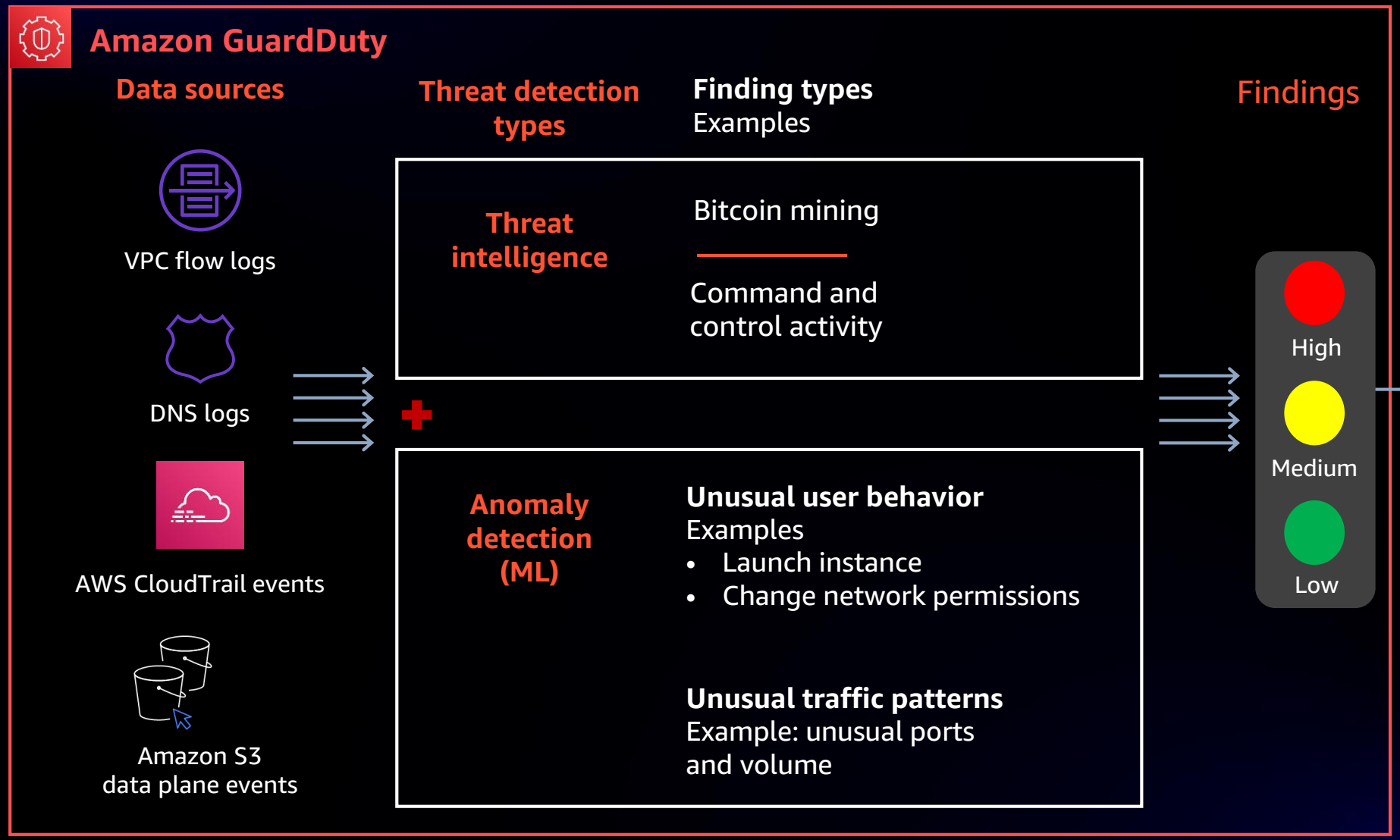
Open-source traffic analysis

AWS Traffic Mirroring Partners



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

# Amazon GuardDuty: How it works




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

# Thank you!

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