NET201

AWS re:Invent

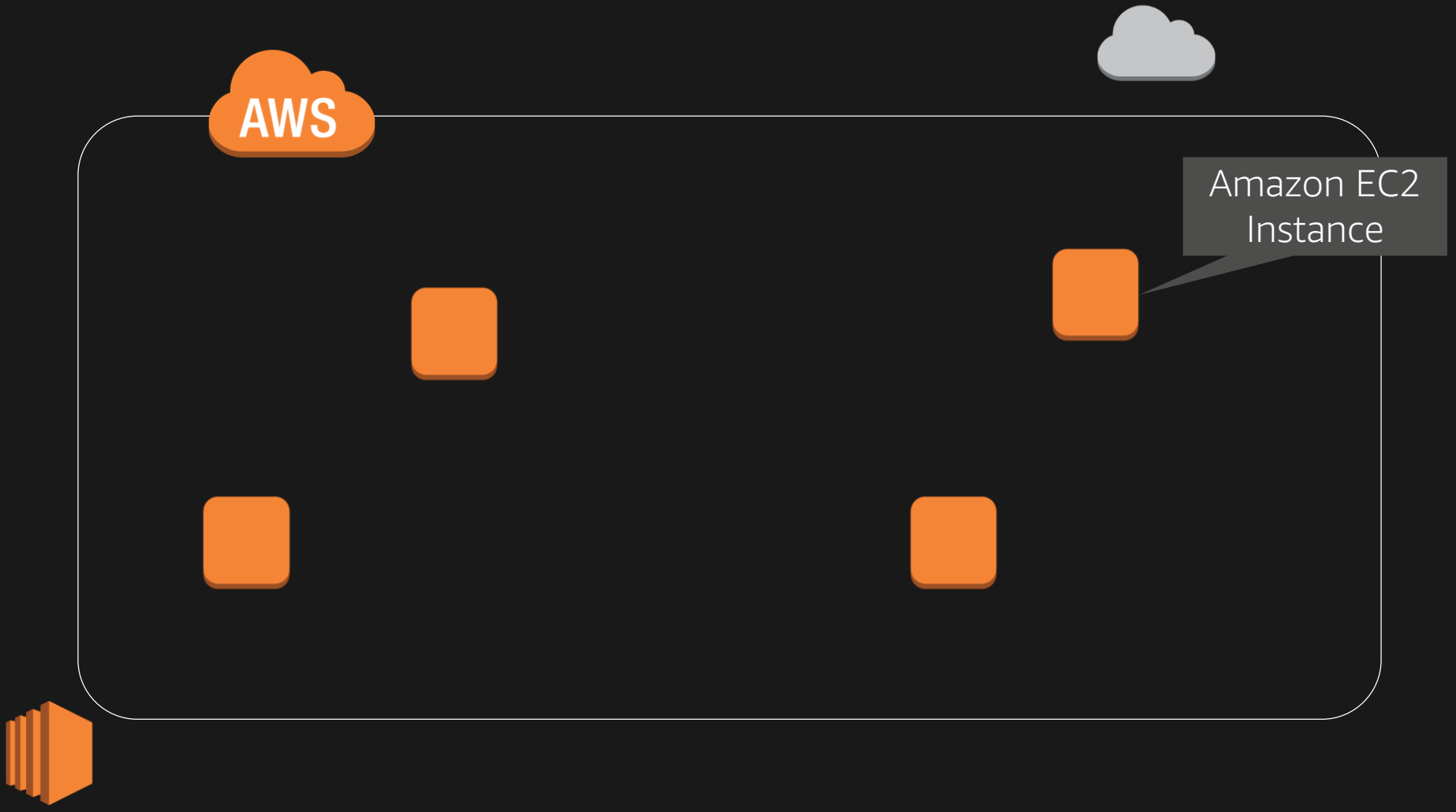
Creating Your Virtual Data Center: VPC Fundamentals and Connectivity

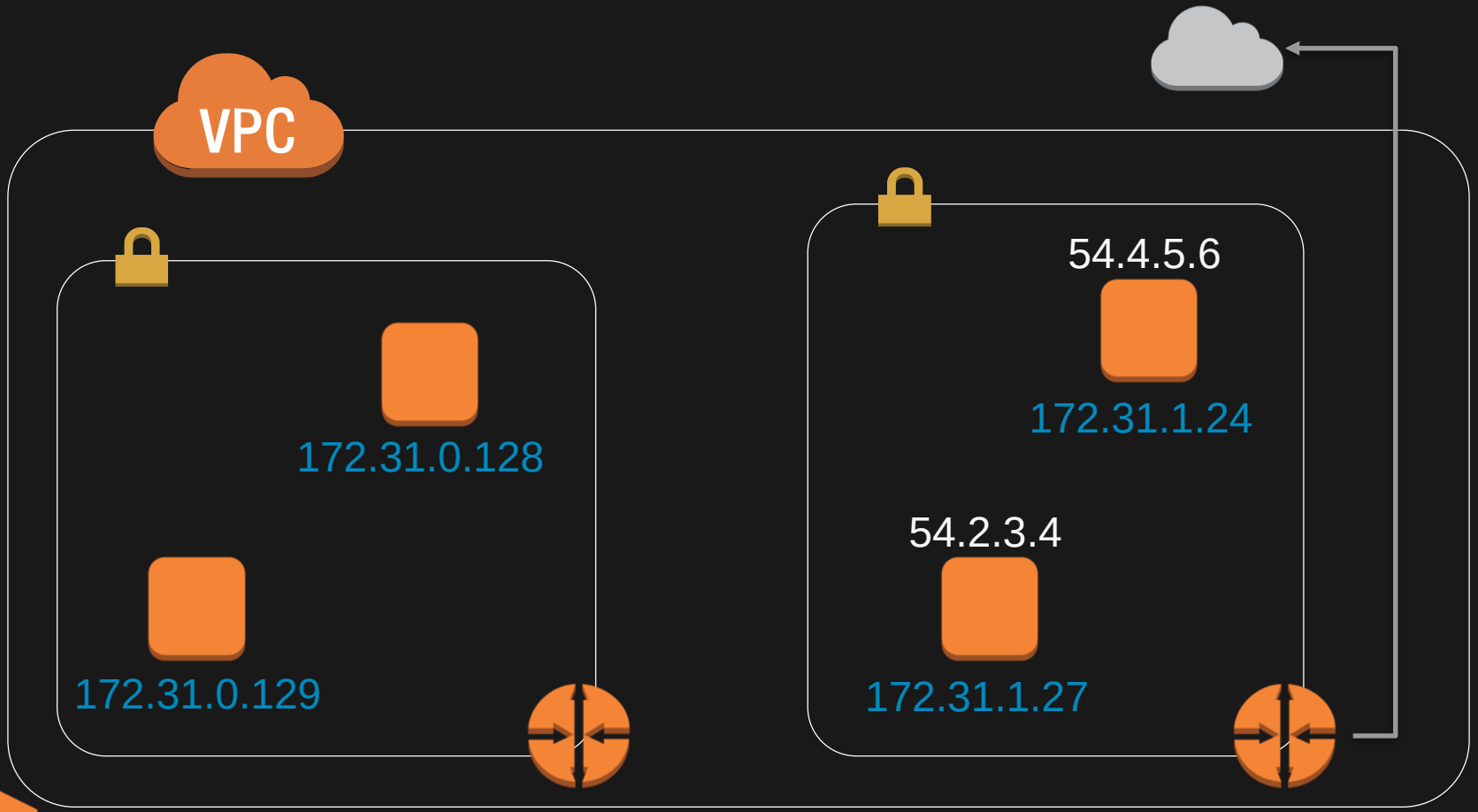
Gina Morris, Engineering Manager, EC2 Networking

November 28, 2017

AWS re:Invent

aws





Amazon Virtual Private Cloud (Amazon VPC)

What to expect from this session

- Get familiar with VPC concepts
- Walk through a basic VPC setup
- Learn about the ways in which you can tailor your virtual network to meet your needs

Walkthrough:

Setting up an Internet-connected VPC

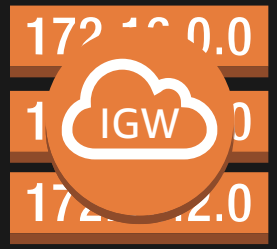
AWS re:Invent

aws

Creating an Internet-connected VPC: Steps

Choosing an address range

Create subnets in Availability Zones



Creating a route to the Internet

Authorizing traffic to/from the VPC

Choosing an IP address range

CIDR notation review

CIDR range example:

172.31.0.0/16

1010 1100 0001 1111 0000 0000 0000 0000

NET202 - IPv6 in the Cloud: Protocol and AWS Service Overview

Choosing an IP address range for your VPC

VPC

Avoid ranges that overlap with other networks to which you might connect.

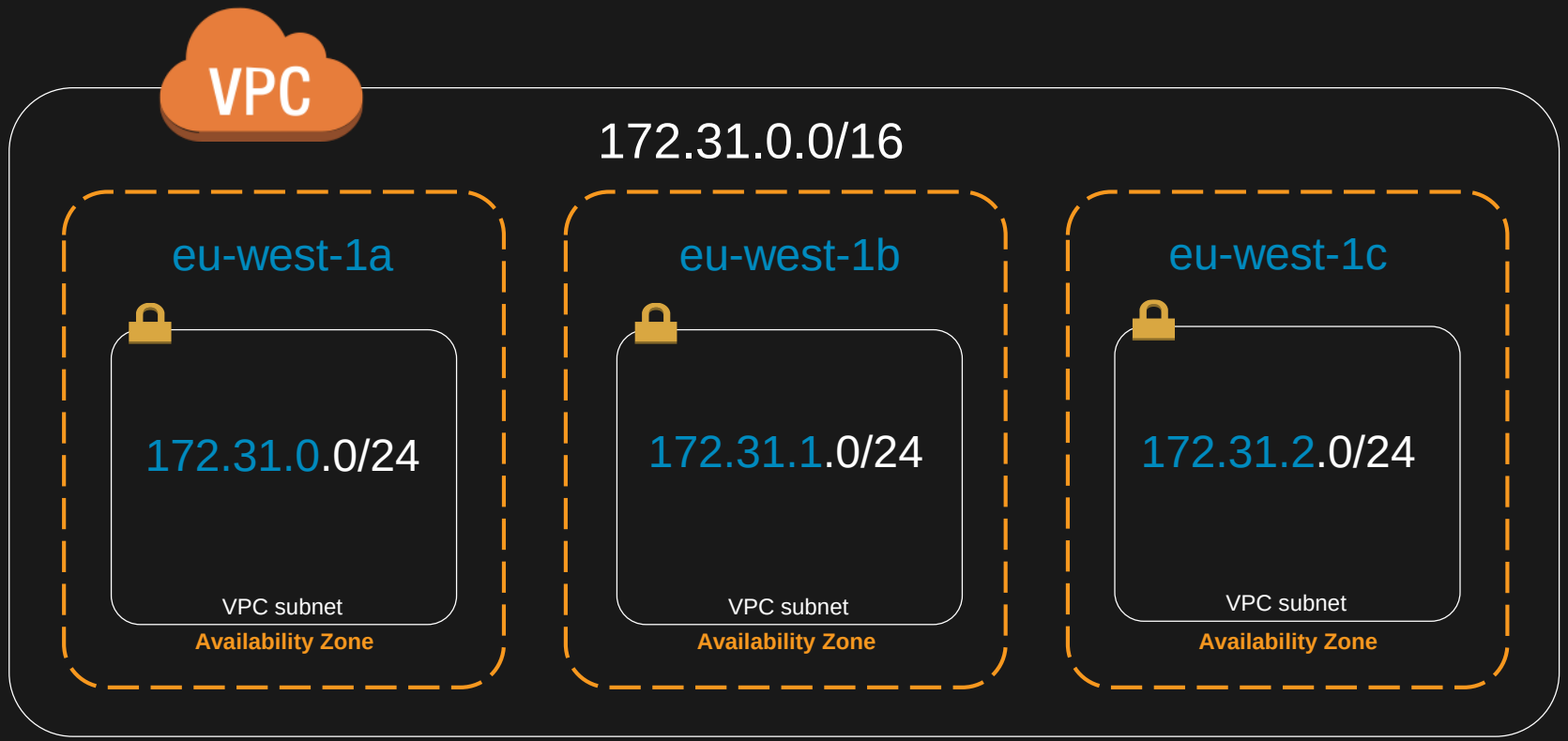
172.31.0.0/16

Recommended:
RFC1918 range

Recommended:
/16
(65,536 addresses)

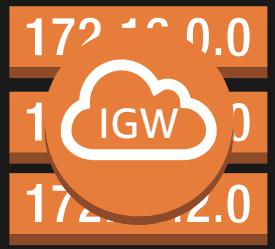
Subnets

VPC subnets and Availability Zones



VPC subnet recommendations

- /16 VPC (65,536 addresses)
- At least /24 subnets (251 addresses)
- Use multiple Availability Zones per VPC through multiple subnets



Route to the Internet

Routing in your VPC

- Route tables contain rules for which packets go where
- Your VPC has a *default* route table
- But, you can assign different route tables to different subnets

Create Route Table | Delete Route Table | Set As Main Table

Search Route Tables and their

Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-04304e61	0 Subnets	Yes	vpc-327d1857 (172.31.0.0/16) | ...

rtb-04304e61

Summary | Tags

Cancel

Destination	Target	Status
172.31.0.0/16	local	Active

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No

Add another route

Traffic destined for my VPC stays in my VPC

Internet gateway

Create Internet Gateway | Delete | Attach to VPC | Detach from VPC

Search Internet Gateways and

1 to 1

Name	ID	State	VPC
	igw-3376c756	attached	vpc-327d1857 (172.31.0.0/16) | ...

igw-3376c756

Summary | Tags

Send packets here if you want them to reach the Internet

ID: igw-3376c756

State: attached

Attached VPC ID: vpc-327d1857 (172.31.0.0/16) | Demo VPC

Attachment state: available

Everything that isn't destined for the VPC: send to the Internet

Create Route Table | Delete Route Table | Set As Main Table

			Associat	Main	VPC
	rtb-04304e61	0 Subnets		Yes	vpc-327d1857 (172.31.0.0/16) | ...

rtb-043

Summa | Routes | Subnet Associations | Route Propagation | Tags

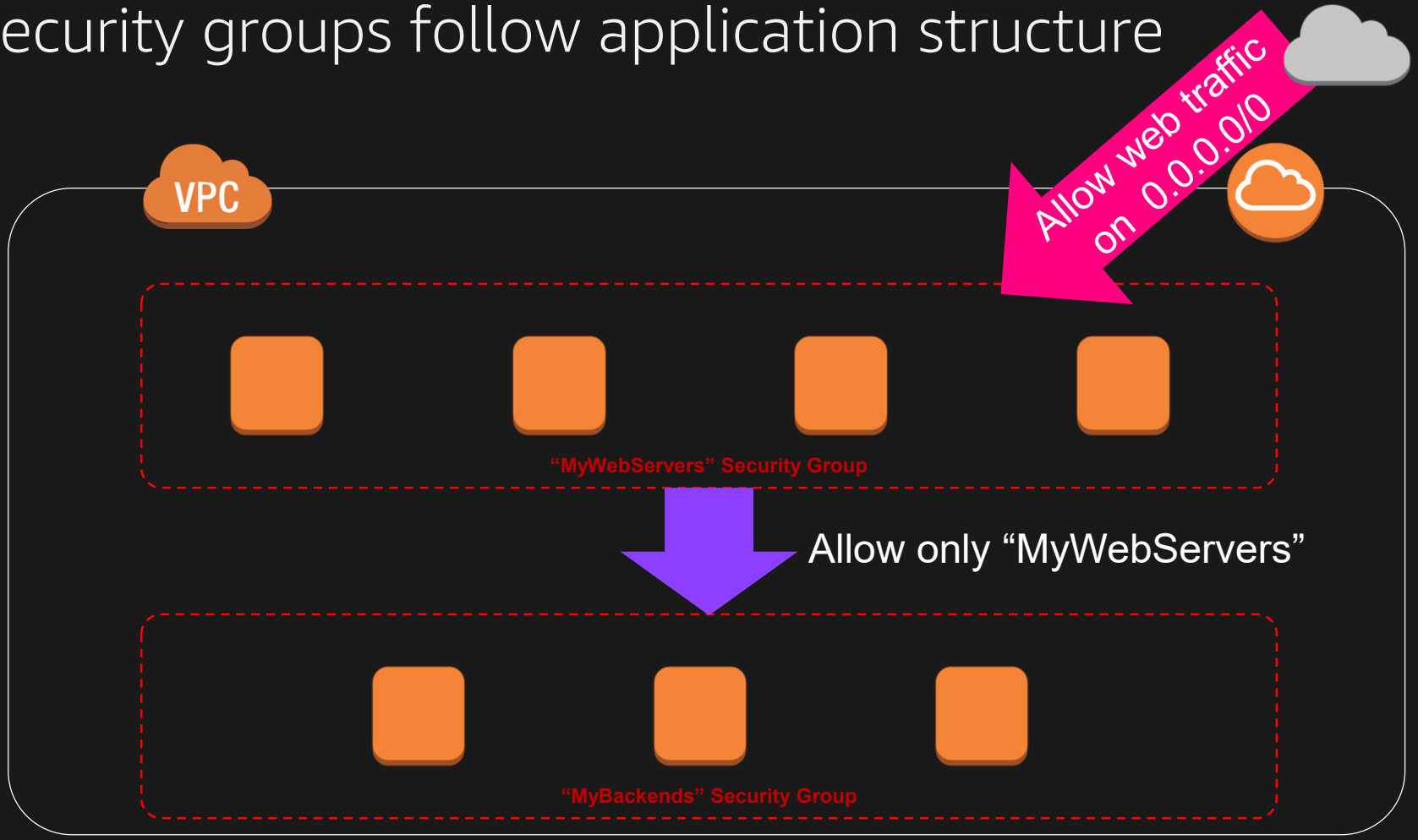
Edit

Destination			
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-3376c756	Active	No

172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-3376c756	Active	No

Network security in your VPC:
Security groups

Security groups follow application structure



Security groups example: Web servers

Create Security Group | Actions

search : vpc-5999ce3e | Add filter | 1 to 3 of 3

Name	Group ID	Group Name	VPC ID	Description
WebServersGroup	sg-067c927d	MyWebServers	vpc-5999ce3e	Group for web servers
BackendsGroup	sg-aa7896d1	MyBackends	vpc-5999ce3e	Group for backend hosts
	sg-1c7c9267	default	vpc-5999ce3e	default VPC security group

Security Group: sg-067c927d

Description | Inbound | Outbound | Tags

Allow all HTTP traffic

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	Allow all HTTP tra...
HTTP	TCP	80	::/0	Allow all HTTP tra...

Rule descriptions

Security groups example: Backends

Create Security Group | Actions

search : vpc-5999ce3e | Add filter | 1 to 3 of 3

Name	Group ID	Group Name	VPC ID	Description
WebServersGroup	sg-067c927d	MyWebServers	vpc-5999ce3e	Group for web servers
BackendsGroup	sg-aa7896d1	MyBackends	vpc-5999ce3e	Group for backend hosts
	sg-1c7c9267	default	vpc-5999ce3e	

Security Group: sg-aa7896d1

Description | Inbound | Outbound | Tags

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	2345	sg-067c927d (MyWebServers)	Allow traffic from...

Allow application traffic from web servers only

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	2345	sg-067c927d (MyWebServers)	Allow traffic from...

Security groups in VPC: Additional notes

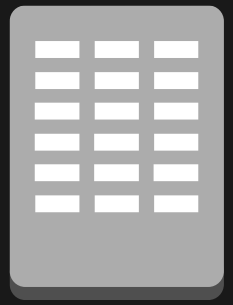
- Follow the *"principle of least privilege"*
- VPC allows creation of egress as well as ingress security group rules

Connectivity options for VPCs

Beyond Internet connectivity

Restricting Internet access

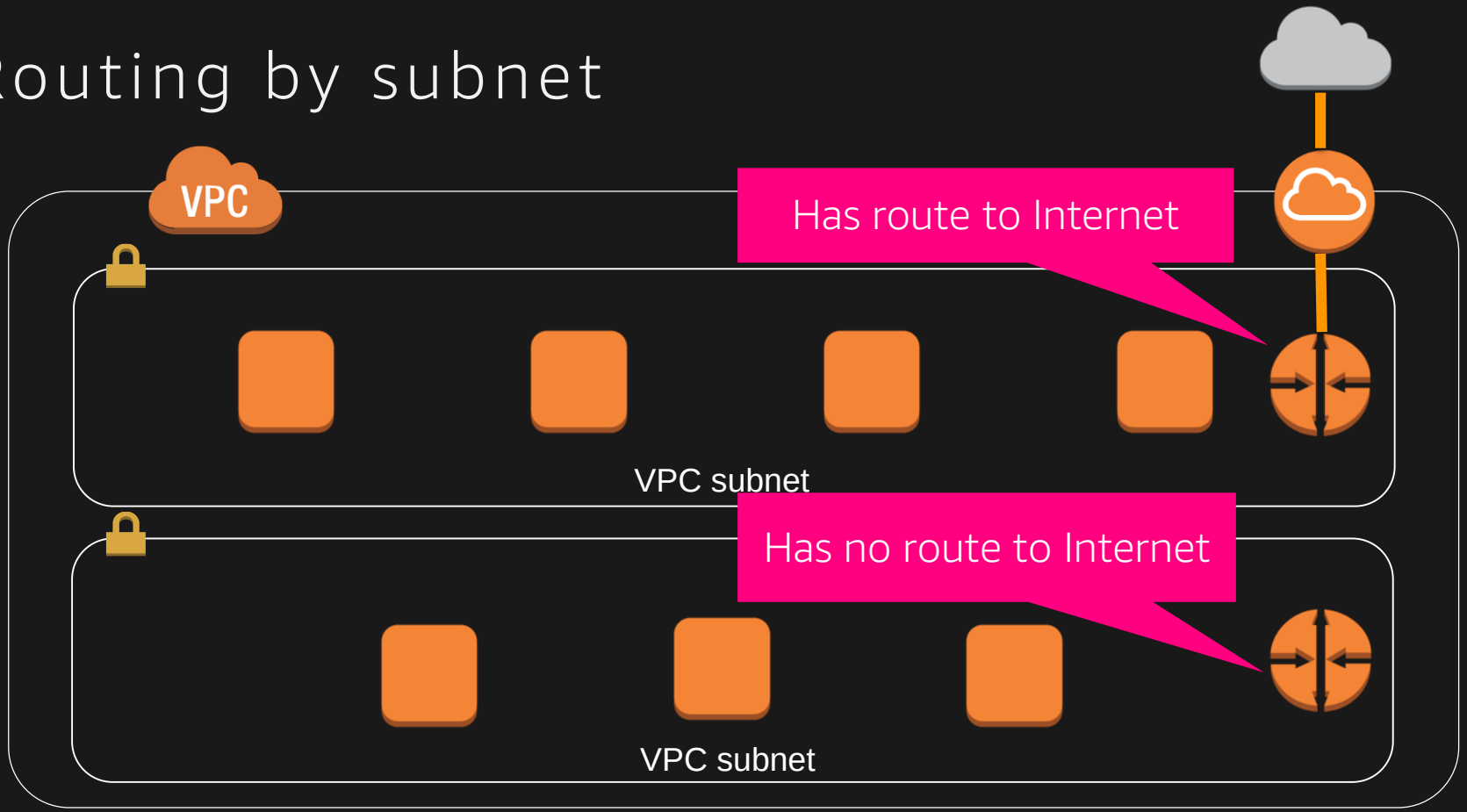
Connecting to other VPCs



Connecting to your corporate network

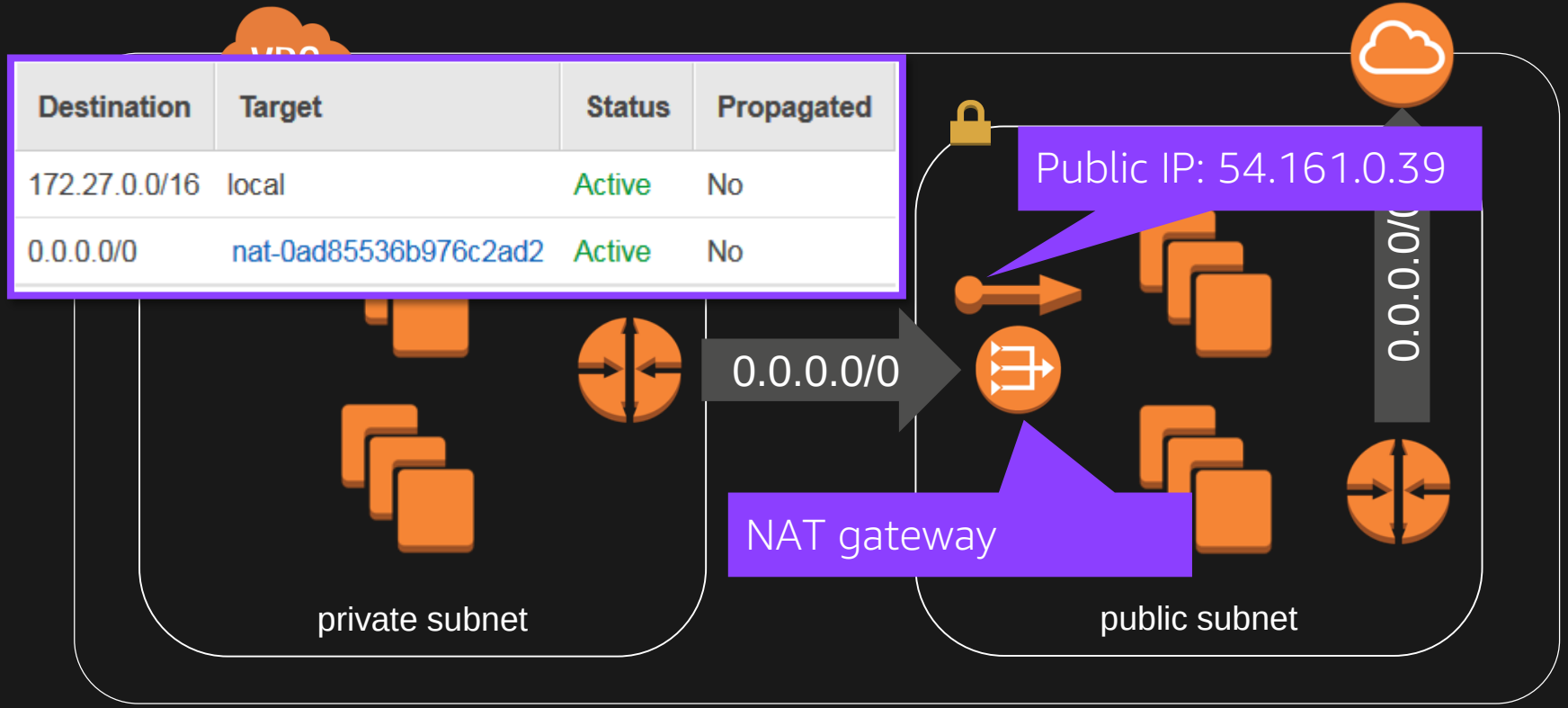
Restricting Internet access:
Routing by subnet

Routing by subnet

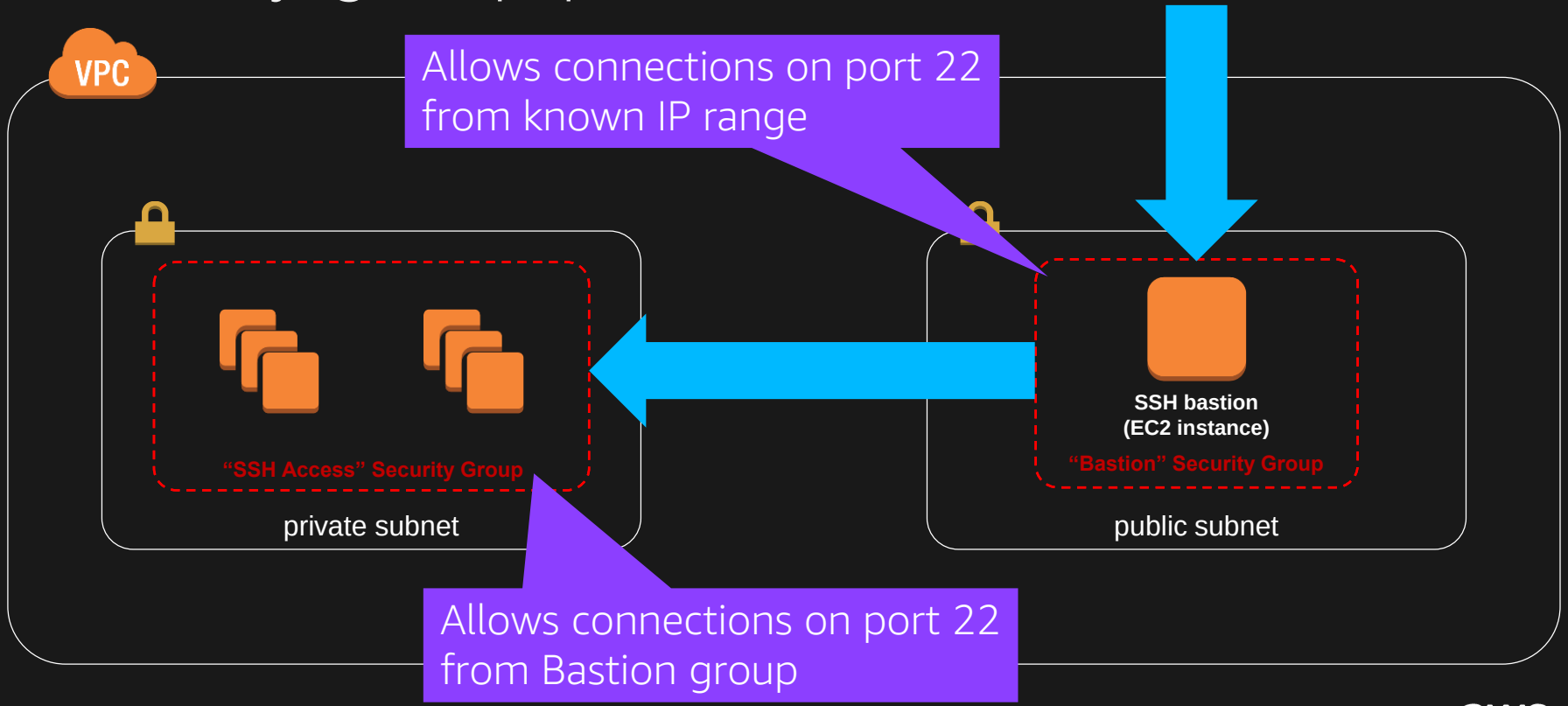


Outbound-only internet access: NAT gateway

Destination	Target	Status	Propagated
172.27.0.0/16	local	Active	No
0.0.0.0/0	nat-0ad85536b976c2ad2	Active	No



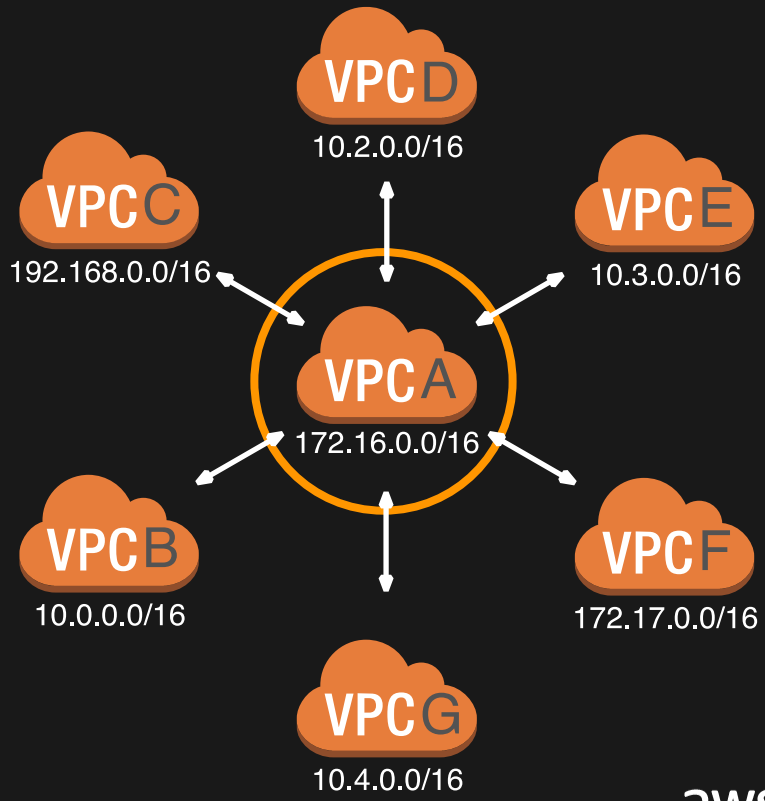
Security group pattern for SSH bastion



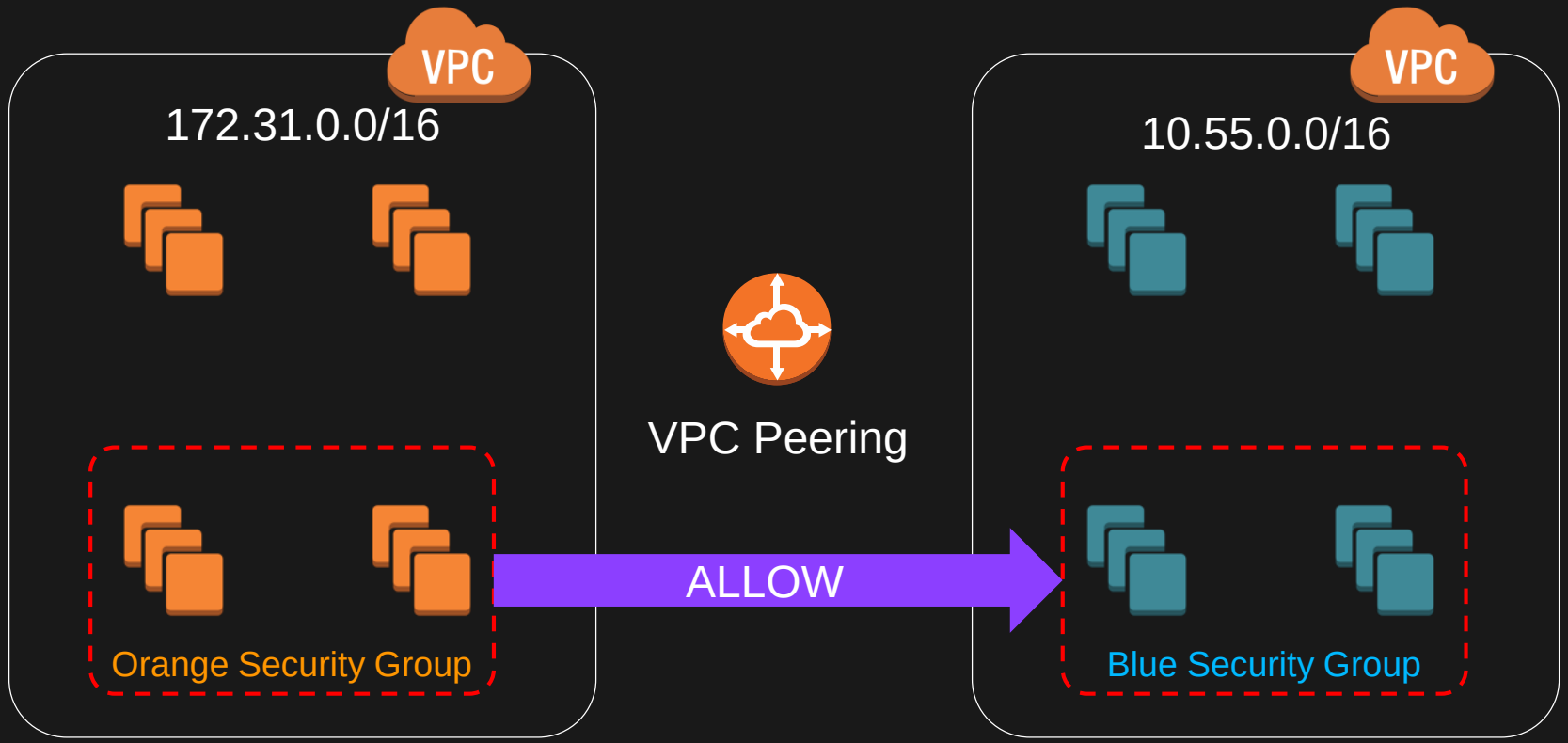
Inter-VPC connectivity:
VPC peering

Example VPC peering use:
Shared services VPC

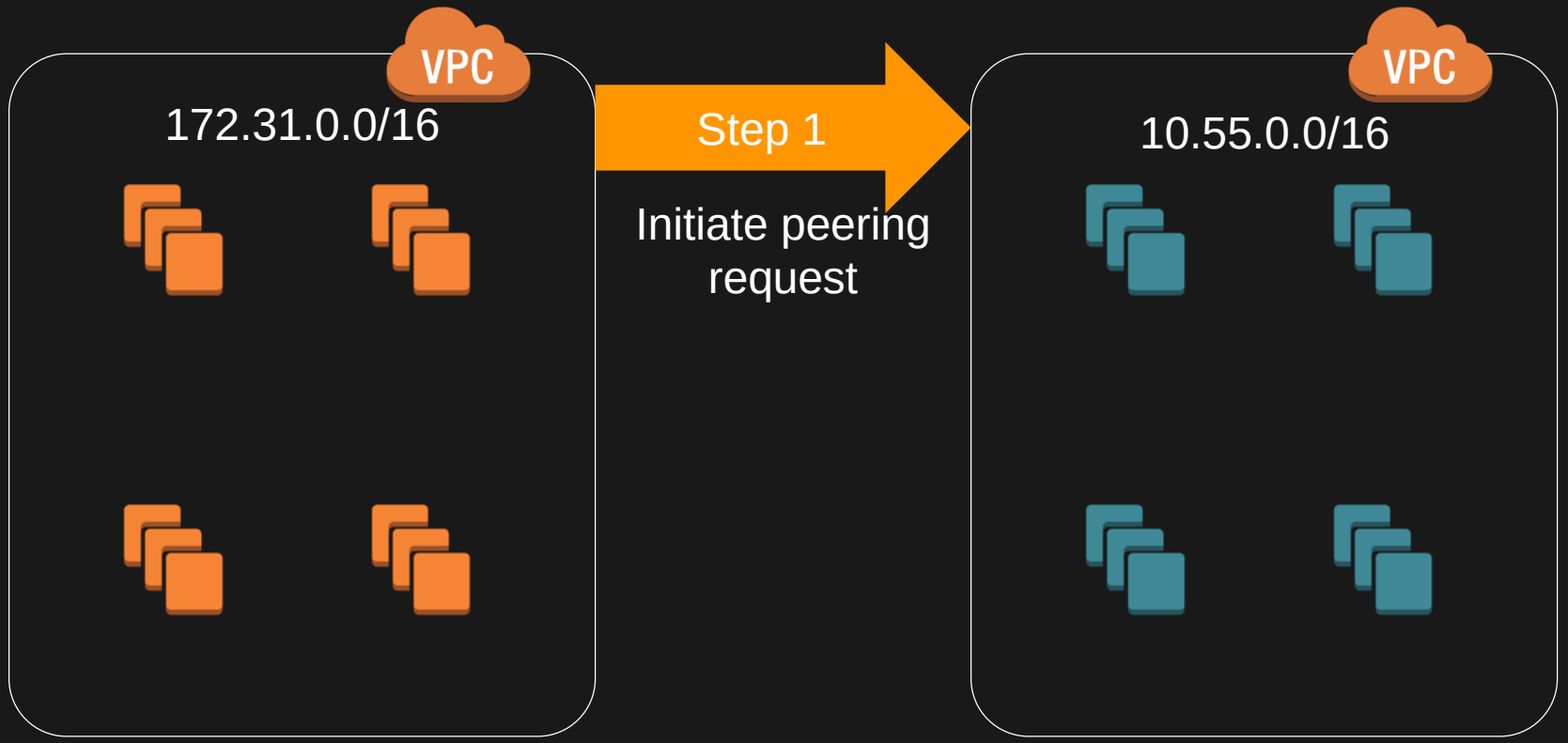
- Common/core services
  - Authentication/directory
  - Monitoring
  - Logging
  - Remote administration
  - Scanning



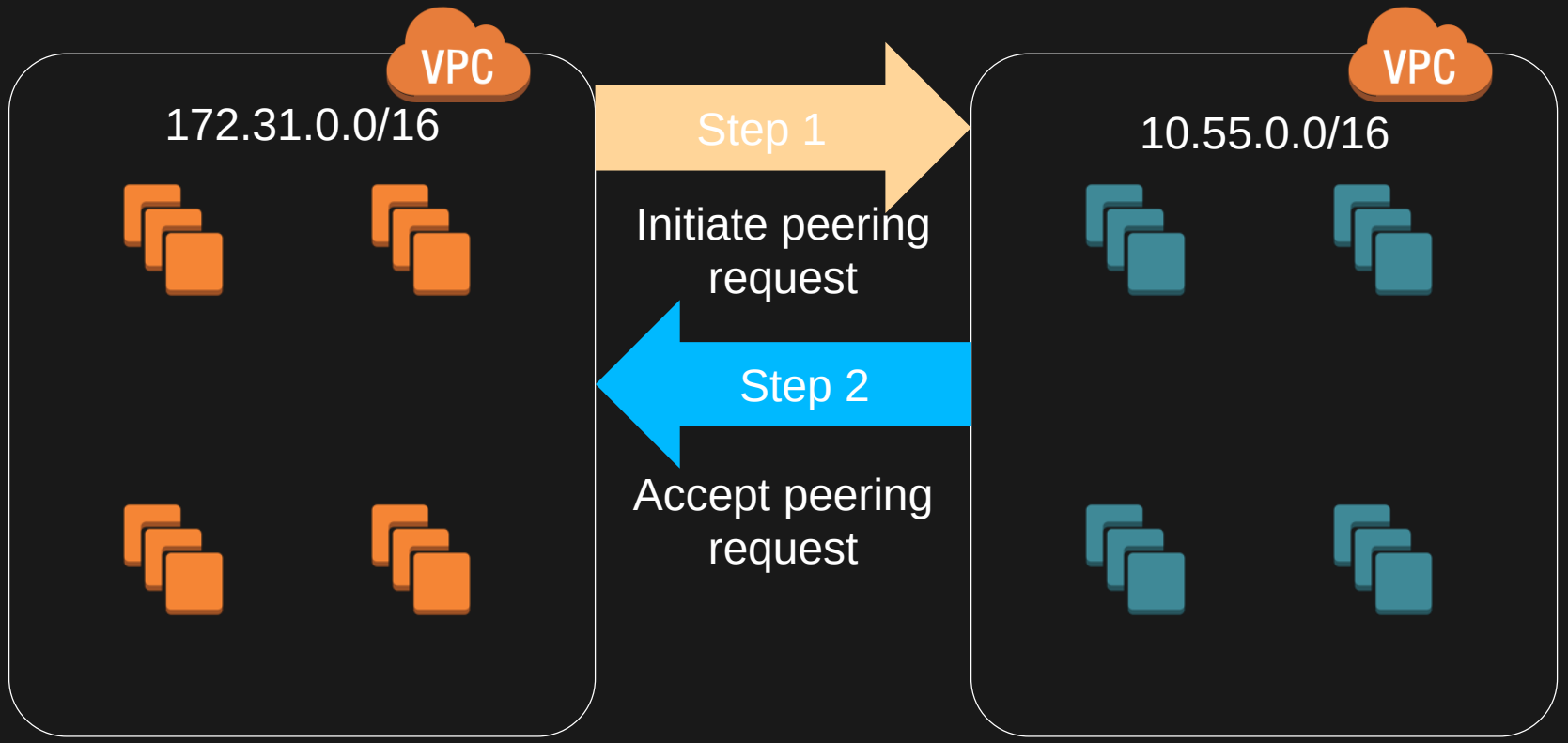
Security groups across peered VPCs



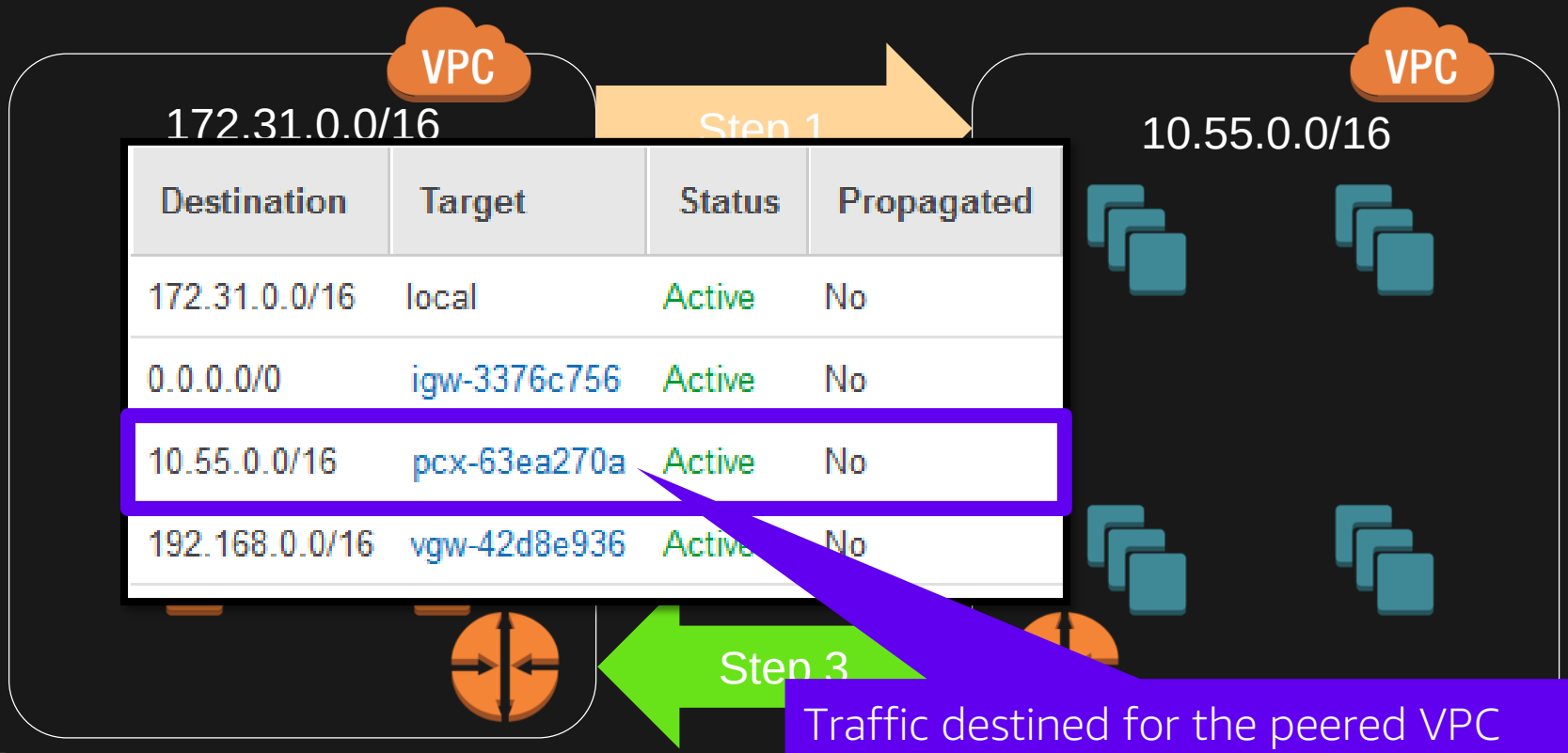
Establish a VPC peering: Initiate request



Establish a VPC peering: Accept request



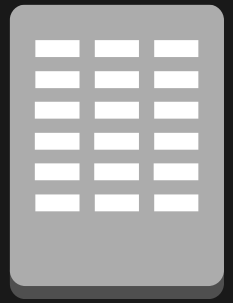
Establish a VPC peering: Create a route



Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-3376c756	Active	No
10.55.0.0/16	pcx-63ea270a	Active	No
192.168.0.0/16	vgw-42d8e936	Active	No

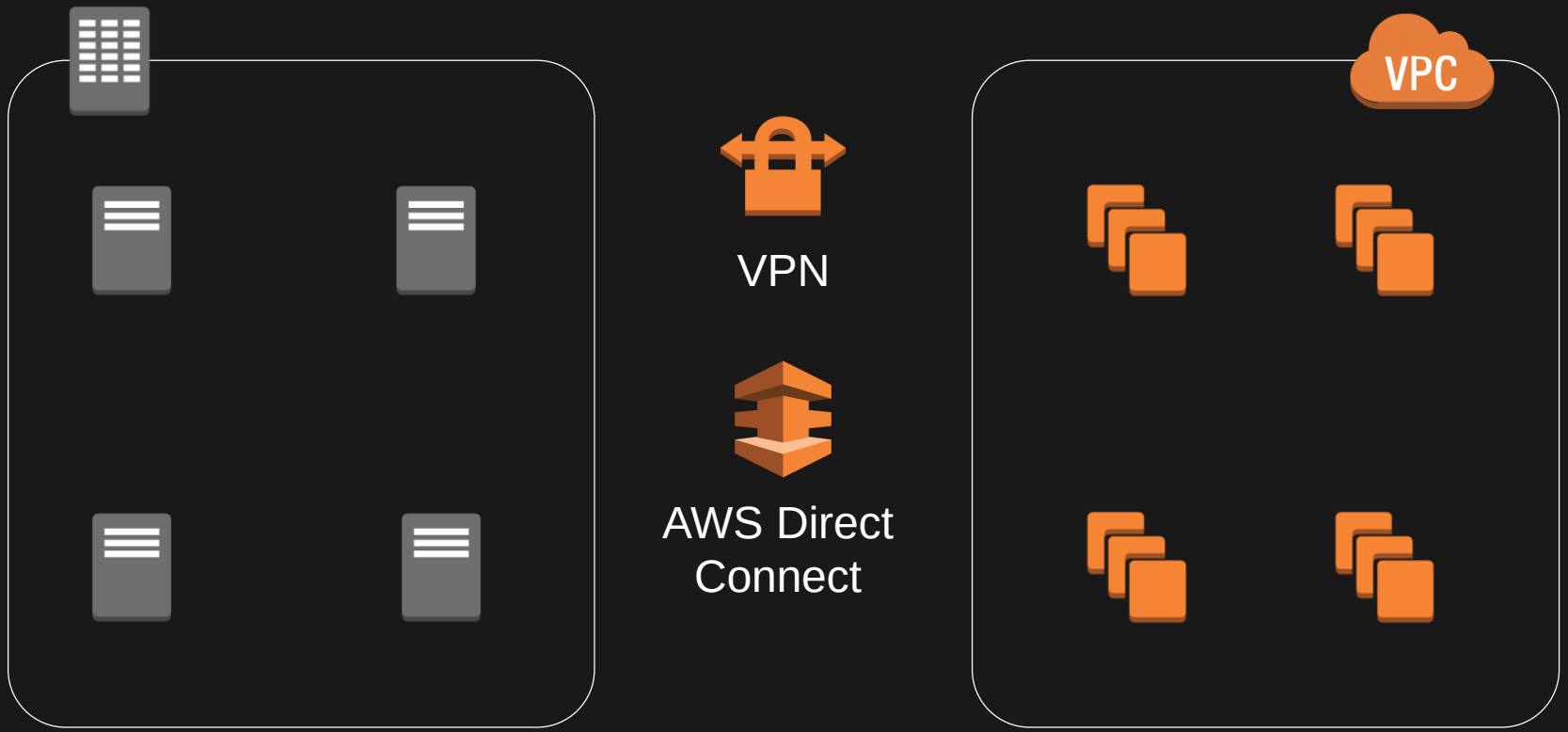
Traffic destined for the peered VPC should go to the peering

AWS re:Invent

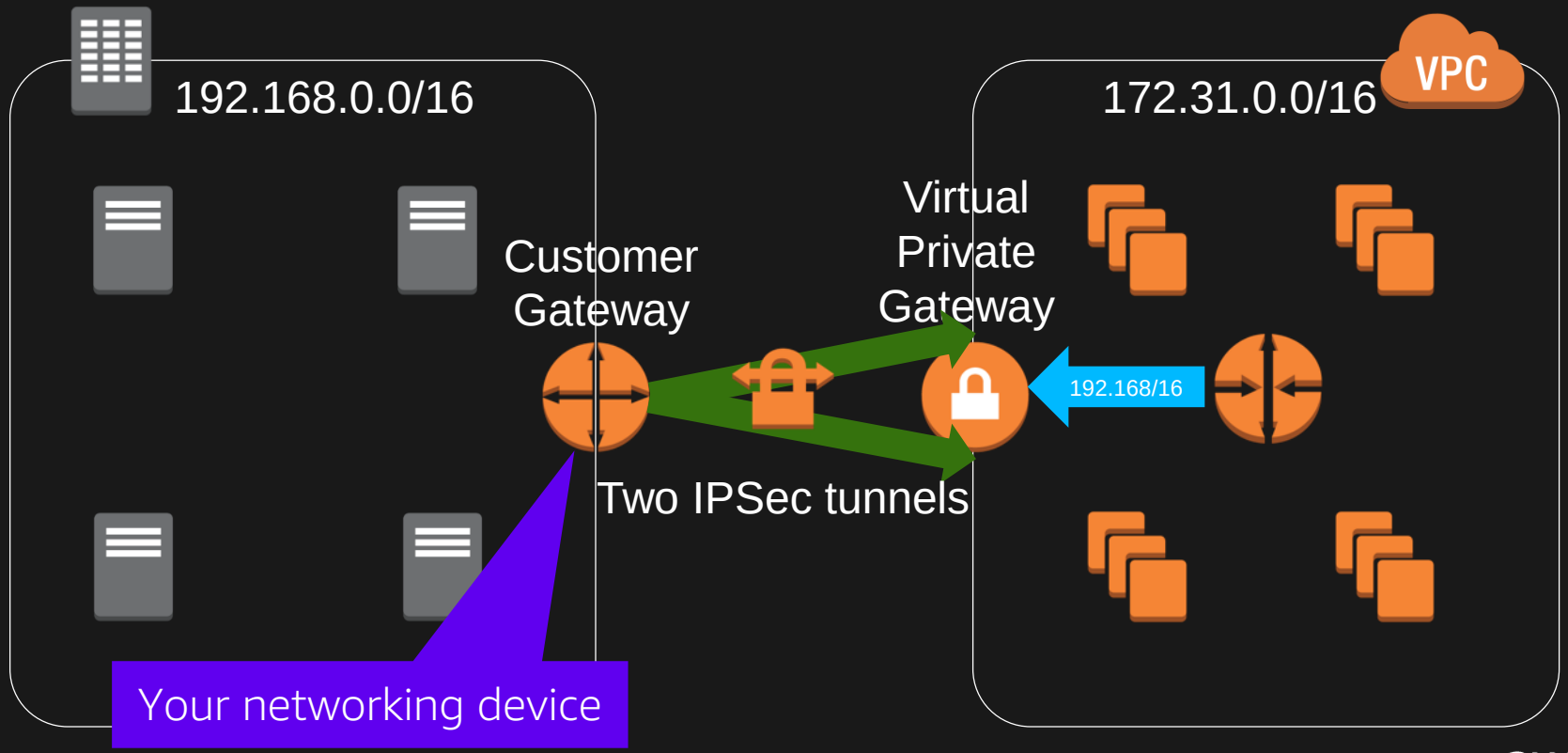


Connecting to on-premises networks: AWS Virtual Private Network and AWS Direct Connect

Extend an on-premises network into your VPC



AWS VPN basics



AWS VPN and AWS Direct Connect

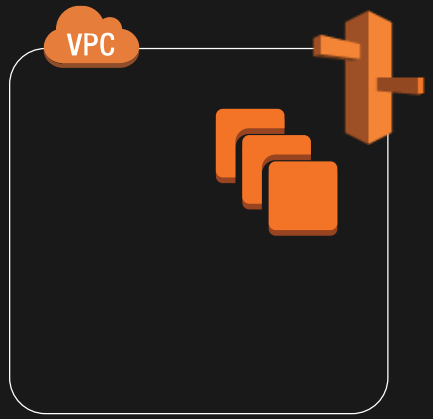
- Both allow secure connections between your network and your VPC
- VPN is a pair of IPSec tunnels over the Internet
- AWS Direct Connect is a dedicated line with lower per-GB data transfer rates
- For highest availability: Use both

VPC and the rest of AWS

AWS re:Invent

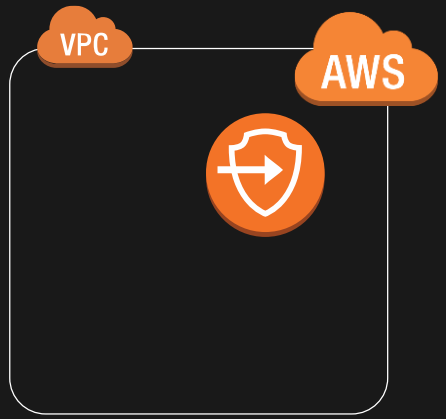
aws

VPC and the rest of AWS

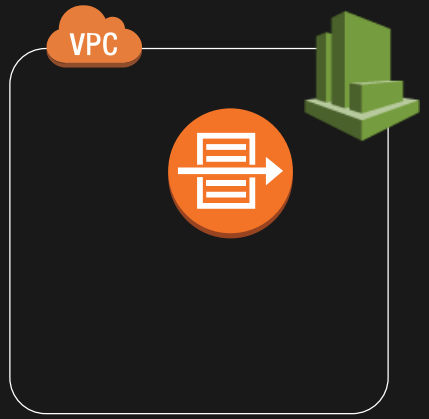


DNS in-VPC with Amazon Route 53

AWS Services in your VPC



VPC endpoints for AWS Services



Logging VPC traffic with VPC flow logs

DNS in a VPC

VPC DNS options

Search VPCs and their propert

Name	VPC ID	State	VPC CIDR	DHCP options set	Route table
Demo VPC	vpc-327d1857	available	172.31.0.0/16	dopt-08b5bf6a	rtb-04304e61

vpc-327d1857 (172.31.0.0/16) | De

Summary | Flow Logs

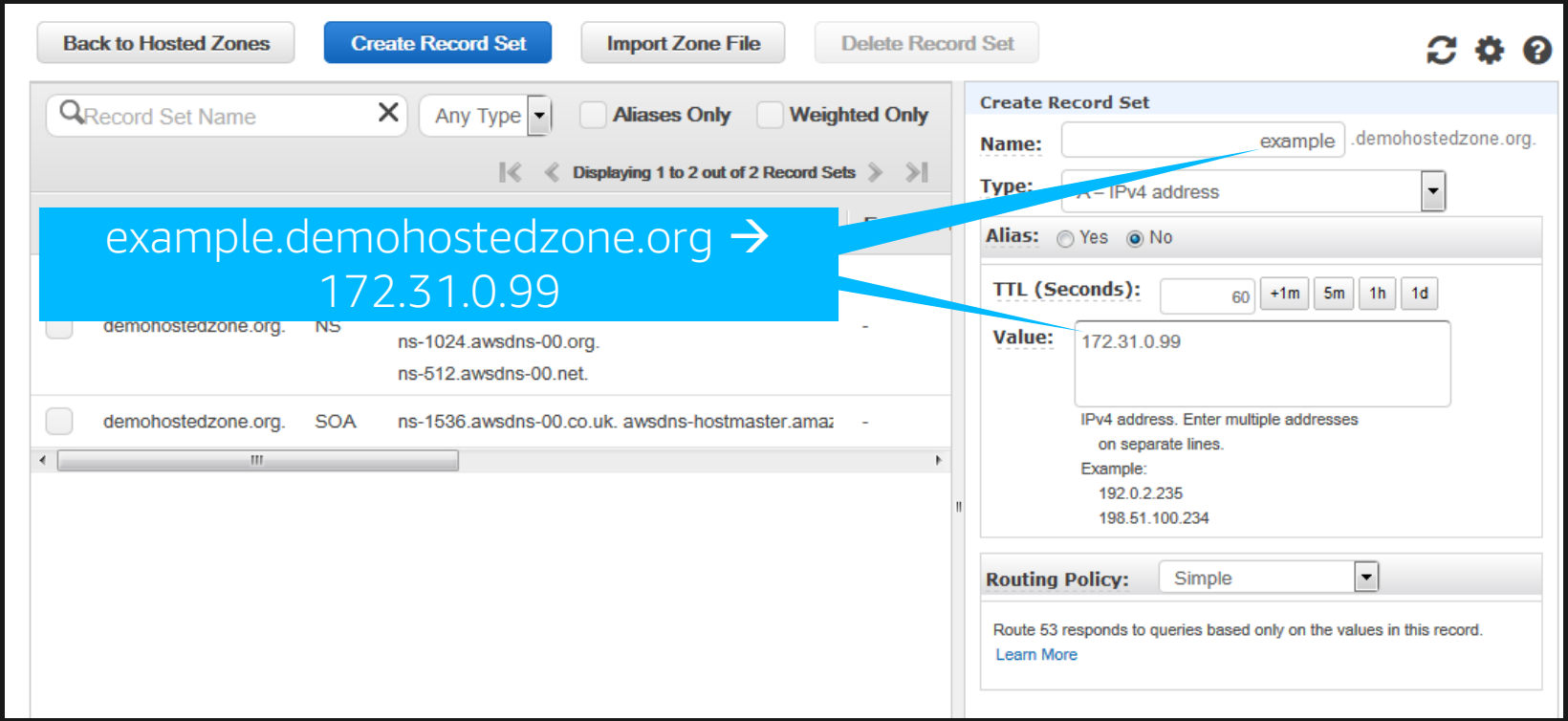
VPC ID: vpc-327d1857 | Demo VPC
State: available
VPC CIDR: 172.31.0.0/16
DHCP options set: dopt-08b5bf
Route table: rtb-04304e6
ClassicLink: Disabled

Use Amazon DNS server

Have EC2 auto-assign DNS hostnames to instances

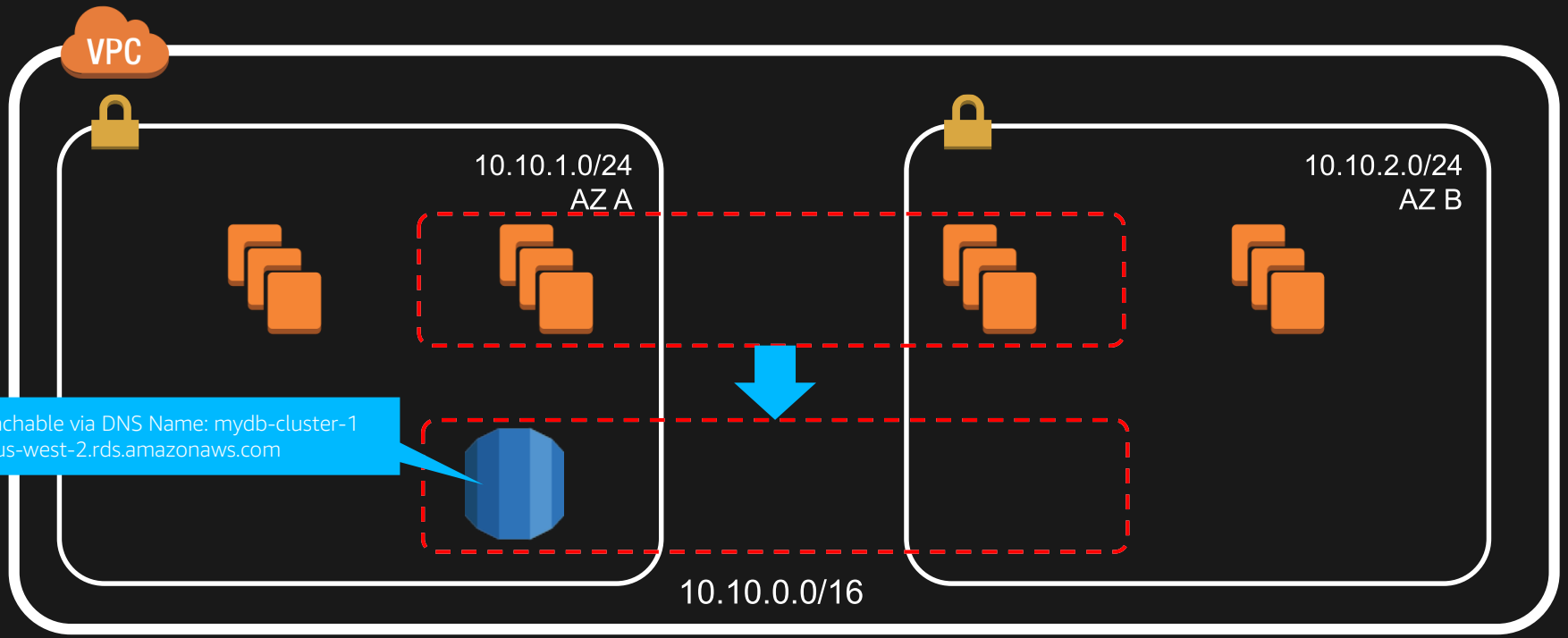
DNS resolution: yes
DNS hostnames: yes

Amazon Route 53 private hosted zones

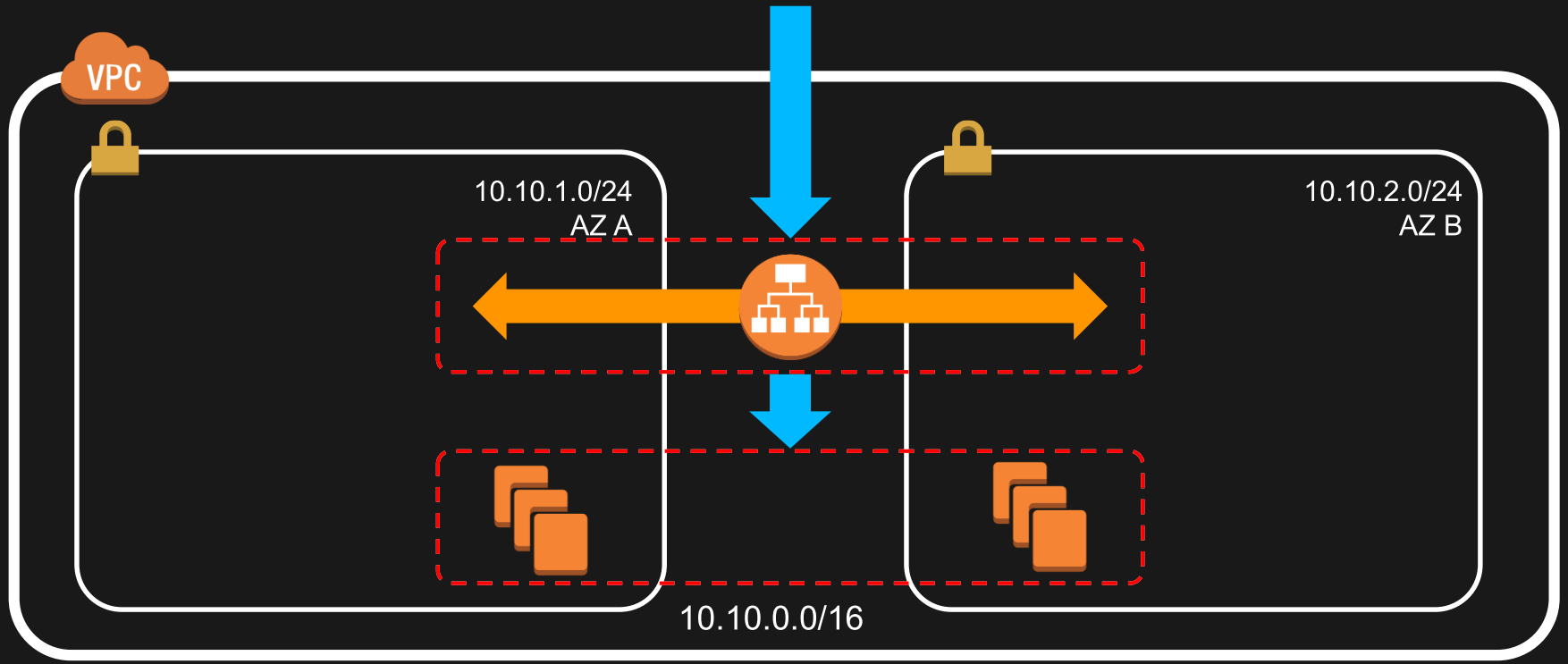


AWS Services in your VPC

Example: Amazon RDS Database in your VPC

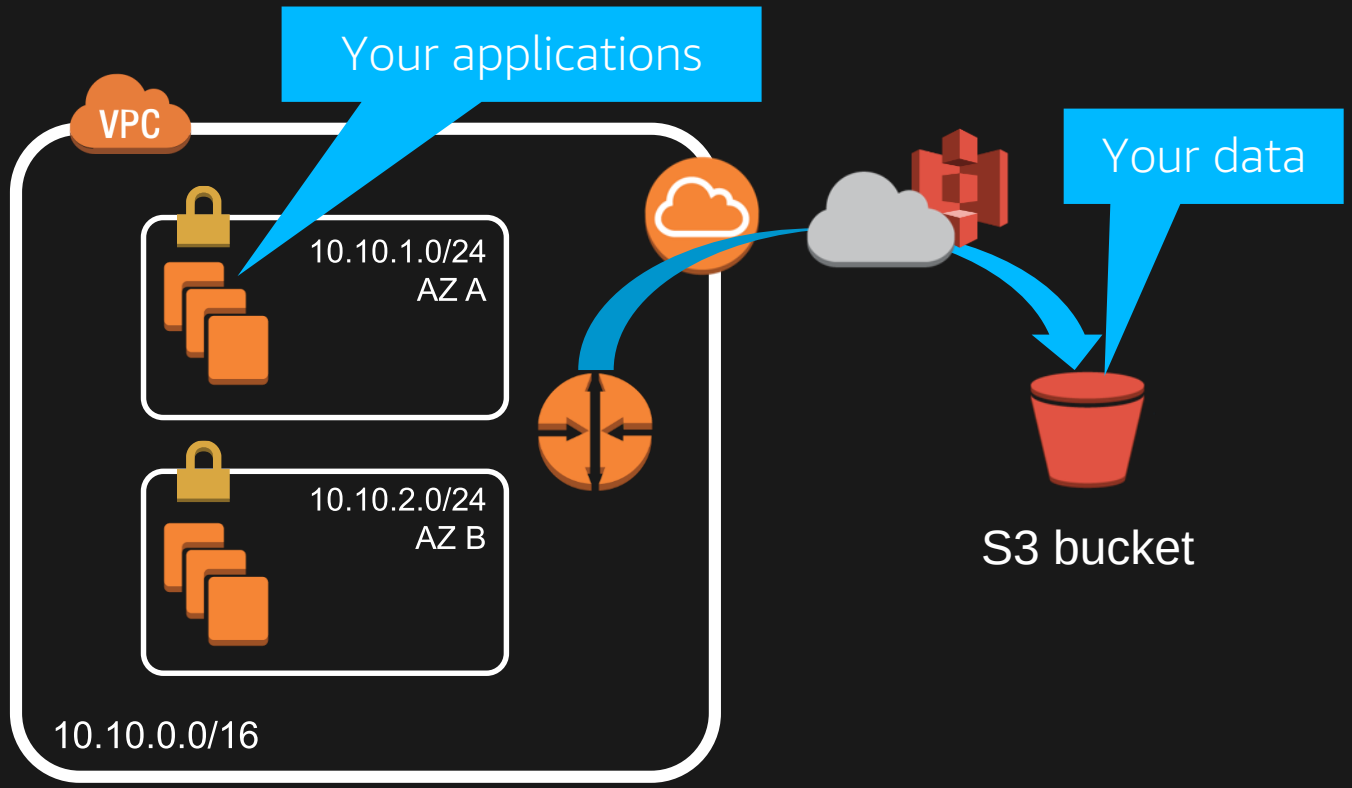


Example: Application Load Balancer in your VPC



VPC Endpoints for AWS Services

Amazon S3 and your VPC



Gateway VPC Endpoints

Endpoints > Create Endpoint

Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.
An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service Name Select a service

Filter by attributes

1 to 8 of 8

Service Name	Owner	Type
com.amazonaws.eu-west-1.dynamodb	amazon	Gateway
com.amazonaws.eu-west-1.ec2	amazon	Interface
com.amazonaws.eu-west-1.ec2messages	amazon	Interface
com.amazonaws.eu-west-1.elasticloadbalancing	amazon	Interface
com.amazonaws.eu-west-1.kinesis-streams	amazon	Interface
com.amazonaws.eu-west-1.s3	amazon	Gateway
com.amazonaws.eu-west-1.servicecatalog	amazon	Interface
com.amazonaws.eu-west-1.ssm	amazon	Interface

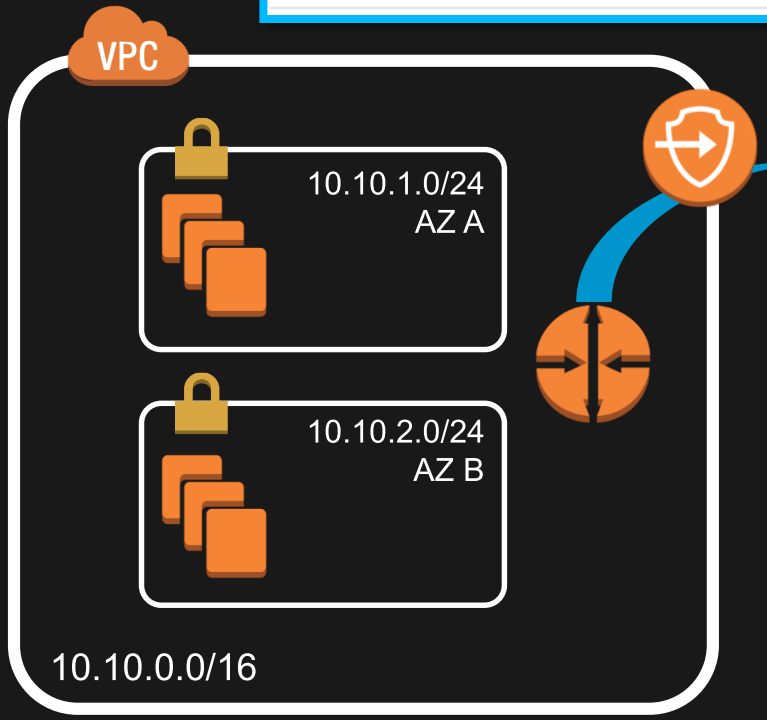
VPC* vpc-28b7004c

* Required

Cancel Create endpoint

VPC Endpoints: An

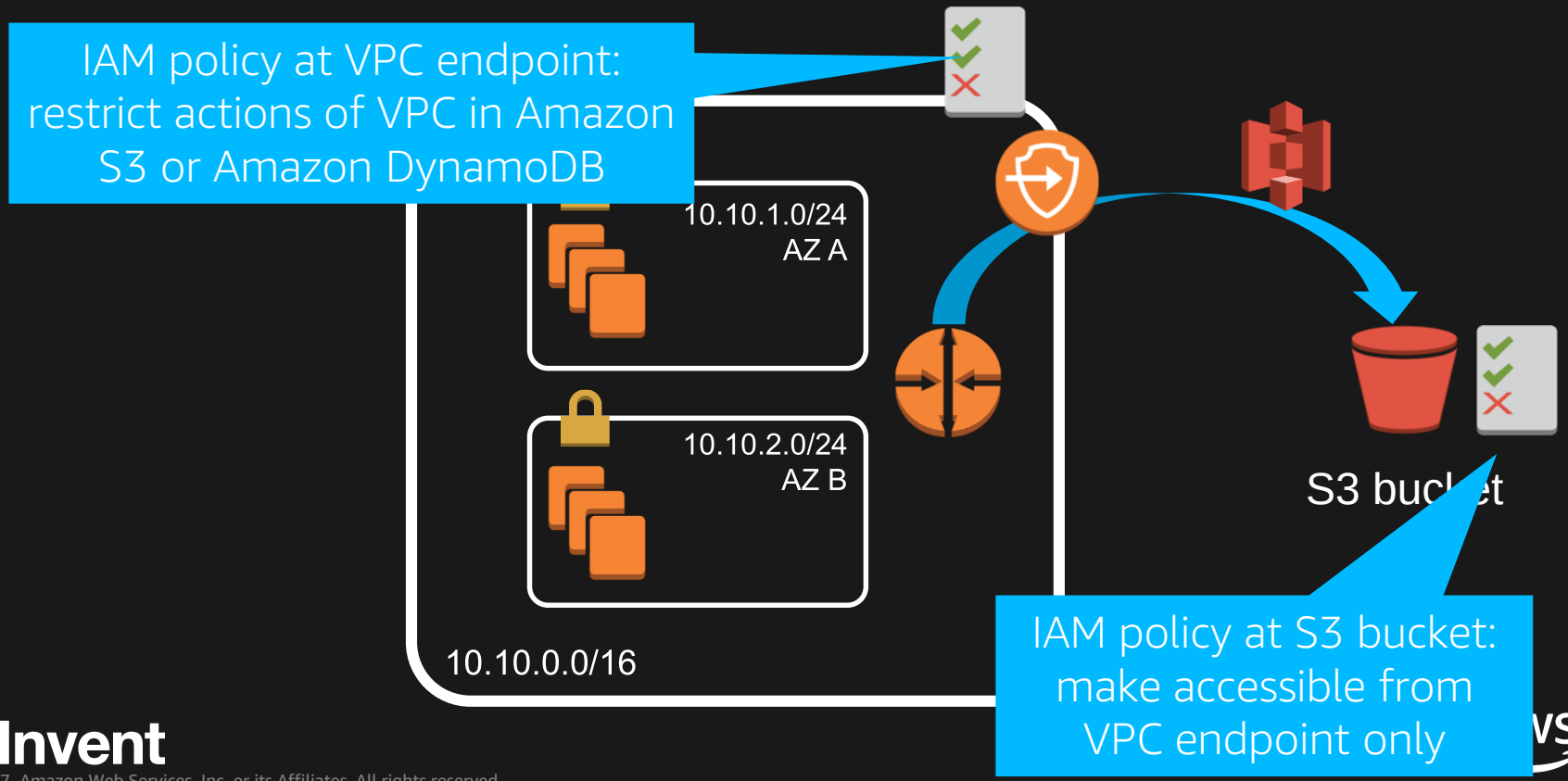
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
pl-68a54001 (com.amazonaws.us-west-2.s3)	vpce-3a14fc53	Active	No



Route S3-bound traffic to the VPC endpoint

S3 bucket

IAM policy for VPC Endpoints



Interface VPC Endpoints

Endpoints > Create Endpoint

Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.
An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service Name Select a service

Filter by attributes

1 to 8 of 8

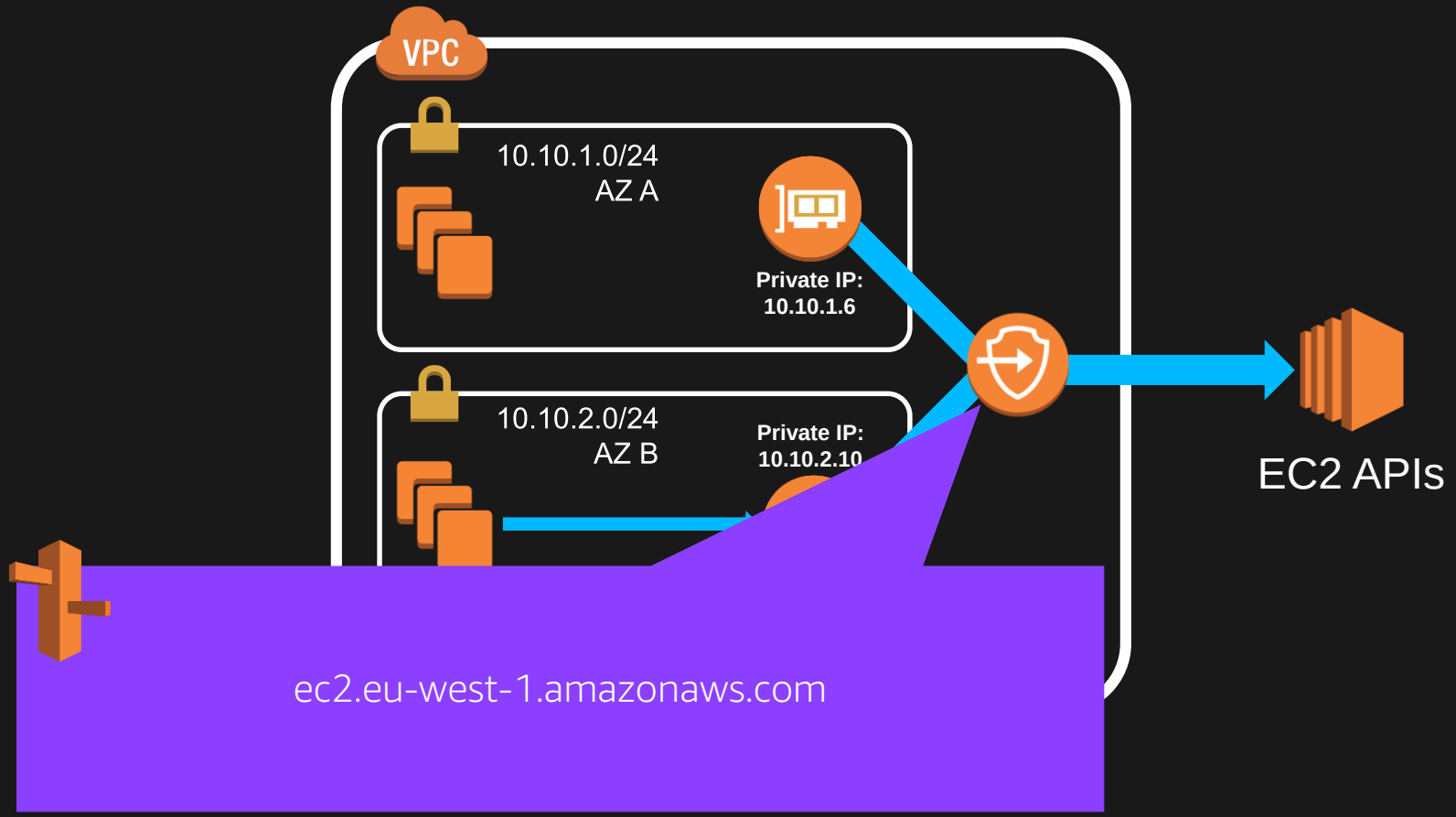
Service Name	Owner	Type
com.amazonaws.eu-west-1.dynamodb	amazon	Gateway
com.amazonaws.eu-west-1.ec2	amazon	Interface
com.amazonaws.eu-west-1.ec2messages	amazon	Interface
com.amazonaws.eu-west-1.elasticloadbalancing	amazon	Interface
com.amazonaws.eu-west-1.kinesis-streams	amazon	Interface
com.amazonaws.eu-west-1.s3	amazon	Gateway
com.amazonaws.eu-west-1.servicecatalog	amazon	Interface
com.amazonaws.eu-west-1.ssm	amazon	Interface

VPC* vpc-28b7004c

* Required

Cancel Create endpoint

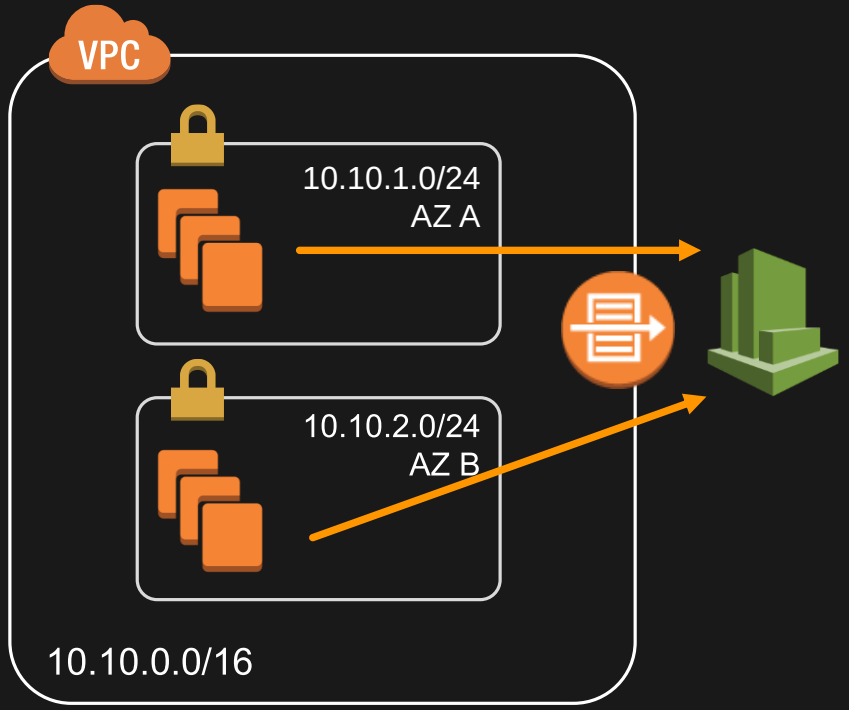
AWS PrivateLink for AWS Services



VPC Flow Logs:

VPC traffic metadata in Amazon CloudWatch Logs

VPC Flow Logs



- Visibility into effects of security group rules
- Troubleshooting network connectivity
- Ability to analyze traffic

VPC Flow Logs: Setup

Create VPC | Actions

SEC302

Name	VPC ID	State	VPC CIDR
SEC302VPC	vpc-63a54a04	available	10.0.0.0/16

vpc-63a54a04 (10.0.0.0/16) | SEC302VPC

Summary | Flow Logs

on your resources t

Create Flow Log

Flow Log ID	Filter	CloudWatch Logs Group	IAM Role ARN
fl-7347a71a	ALL	VPCFlowLogs	arn:aws:iam::167820227276:role/SE

VPC traffic metadata captured in Amazon CloudWatch Logs

VPC Flow Logs data in CloudWatch Logs

Filter events

all 30s 5m 1h 6

Time (UTC -04:00)	Message
2016-	
16:46	7 56934 8080 6 5 373 1474750017 1474750073 ACCEPT OK
16:48	0 8080 47928 6 5 650 1474750081 1474750133 ACCEPT OK
16:48	0 8080 47954 OK
16:48	0 8080 47946 OK
16:48:01	2 280328680831 eni-19 17 10.0.0.100 8080 47938 OK
16:48:01	2 280328680831 eni-1911 100 10.0.0.117 47954 8080 6 5 373 0081 1474750133 ACCEPT
16:48:01	2 280328680831 eni-19116c .239 10.0.0.117 56978 8080 6 5 373 50081 1474750133 ACCEPT
16:48:01	2 280328680831 eni-19116c47 .117 10.0.1.239 8080 56950 6 5 650 1 750081 1474750133 ACCEPT
16:48:01	2 280328680831 eni-19116c47 10 .117 10.0.1.239 8080 56970 6 5 650 14 4750081 1474750133 ACCEPT
16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK
16:48:01	2 280328680831 eni-19116c47 10.0.0.100 10.0.0.117 47946 8080 6 5 373 1474750081 1474750133 ACCEPT OK
16:48:01	2 280328680831 eni-19116c47 10.0.1.239 10.0.0.117 56950 8080 6 5 373 1474750081 1474750133 ACCEPT OK

Who's this?

```
# dig +short -x 109.236.86.32
internetpolice.co.
```

UDP Port 53 = DNS

REJECT

AWS re:Invent

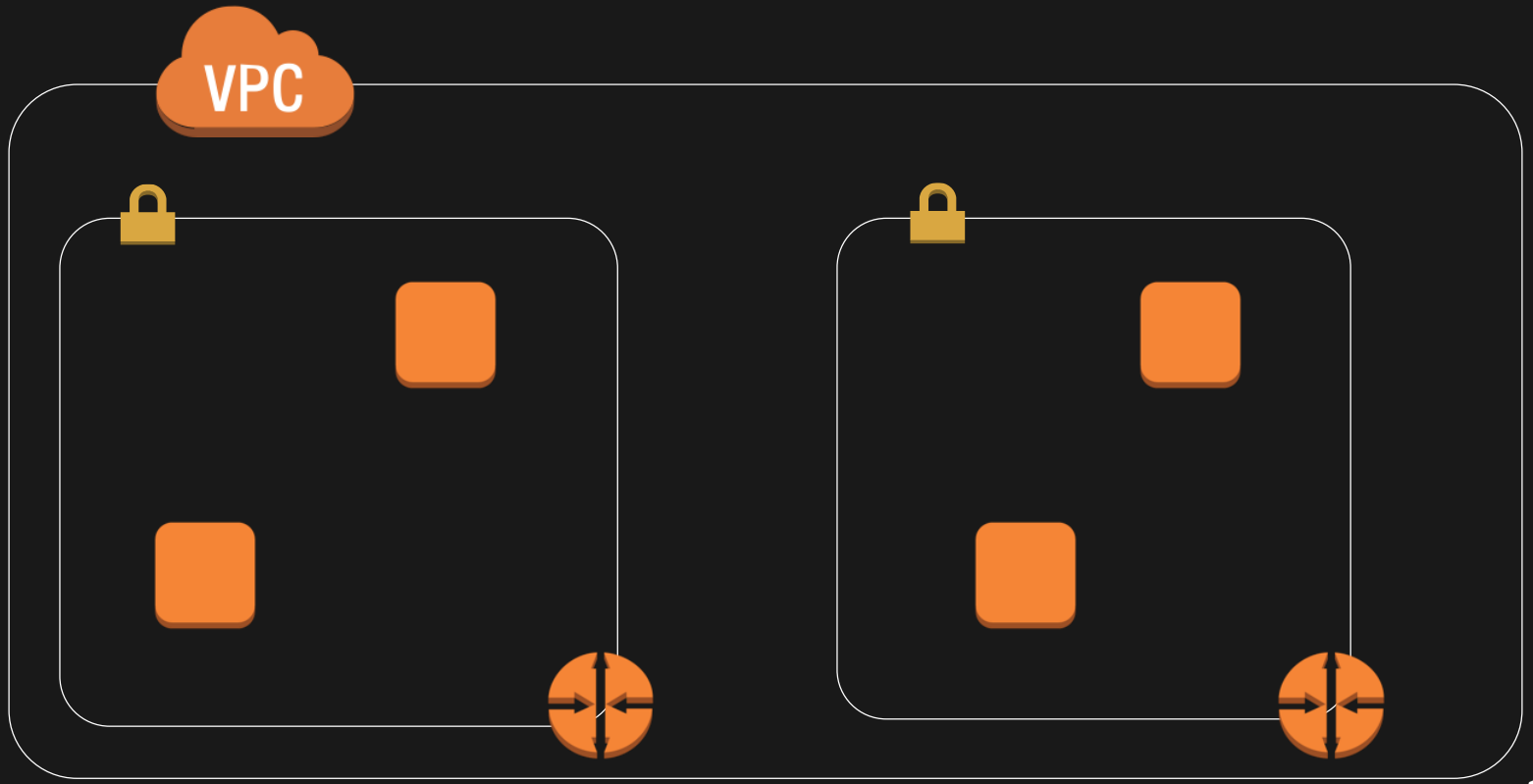
aws

VPC: Your Private Network in AWS

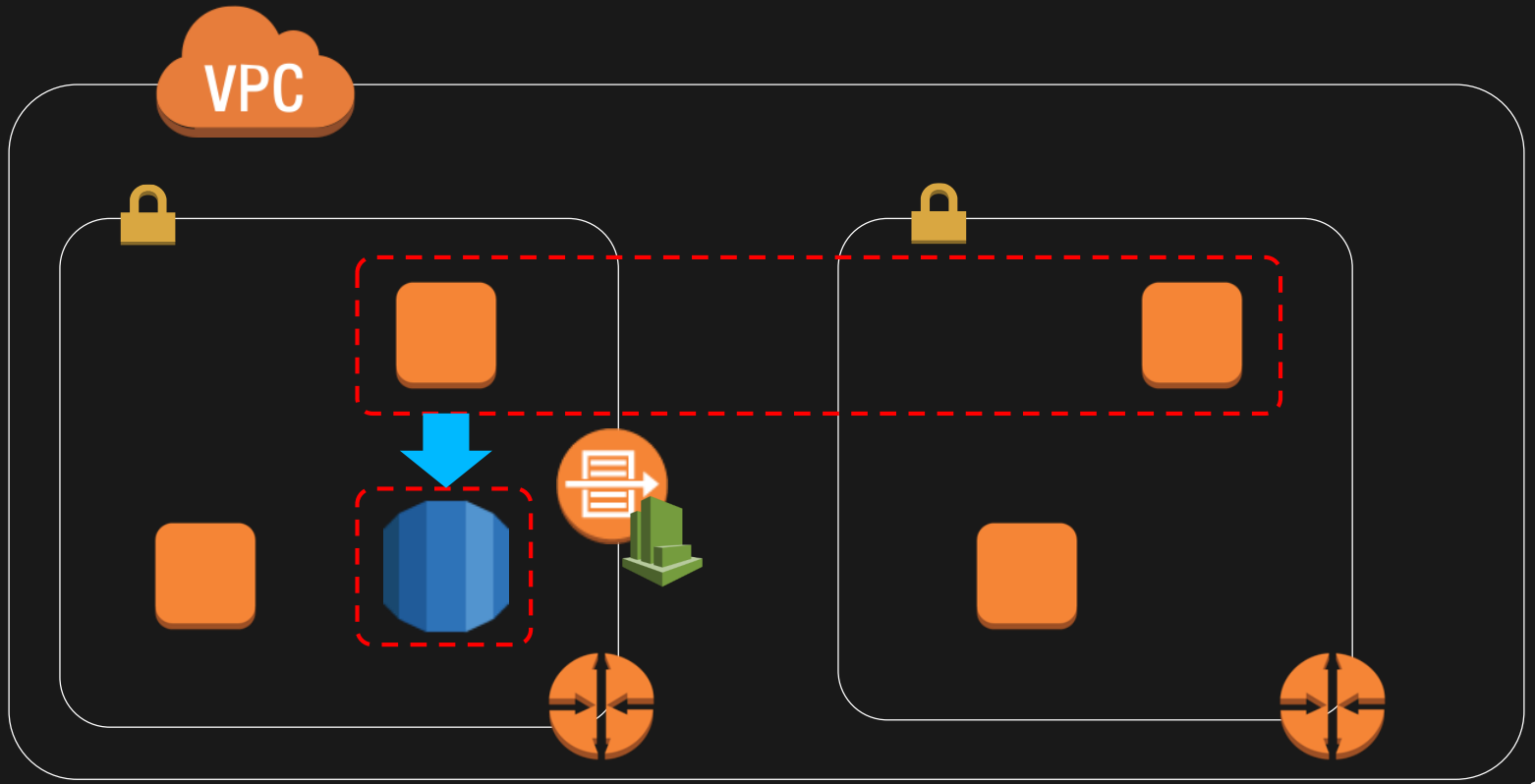
AWS re:Invent

aws

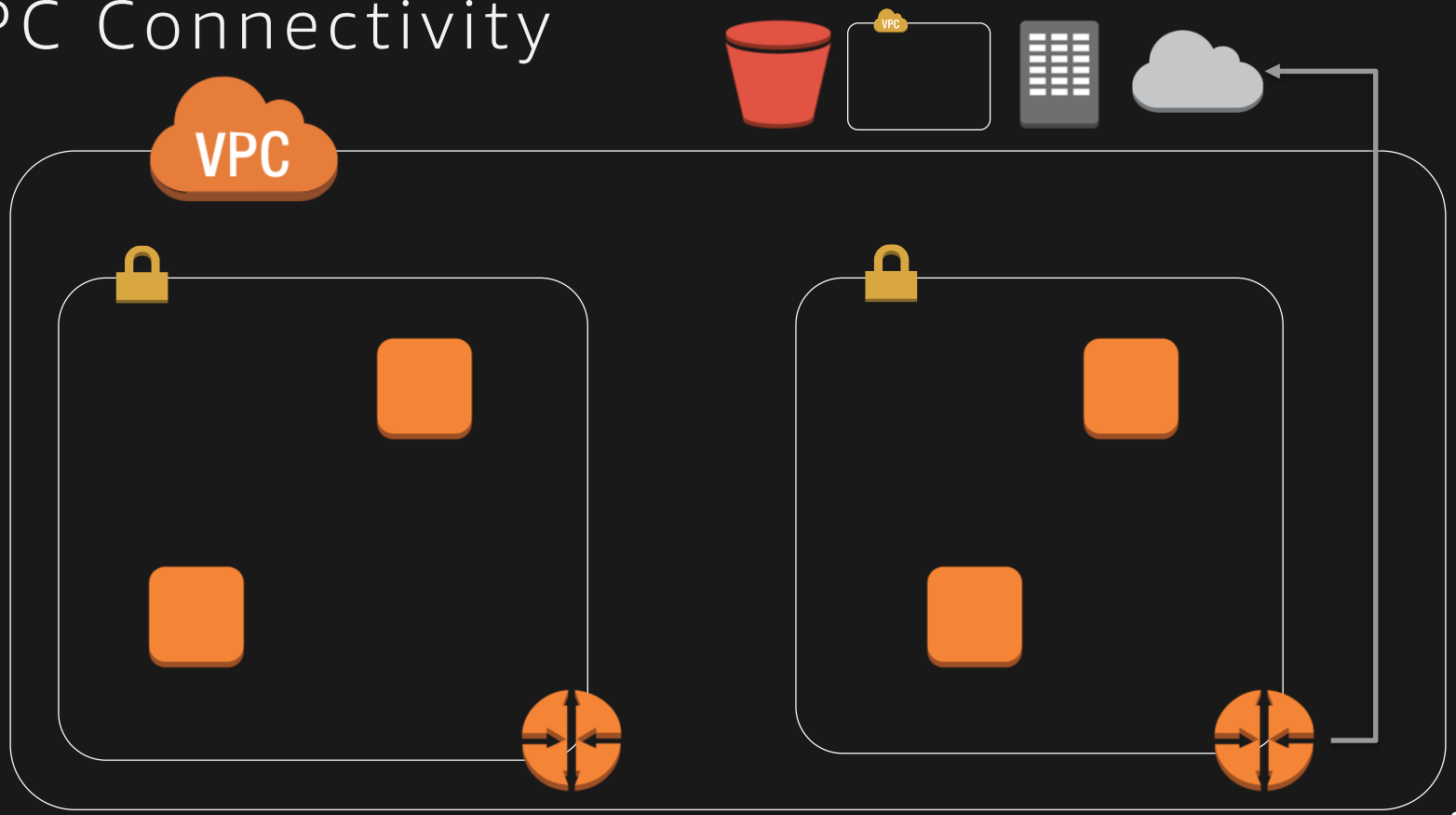
The VPC Network



VPC Network Security



VPC Connectivity



Related Sessions

- NET202 - IPv6 in the Cloud: Protocol and AWS Service Overview
- NET303 - A Day in the Life of a Cloud Network Engineer at Netflix
- NET305 - Advanced VPC Design and New Capabilities for Amazon VPC
- NET308 - VPC Design Scenarios for Real-Life Use Cases
- NET309 - Best Practices for Securing an Amazon VPC
- NET403 - Deep Dive: AWS Direct Connect and VPNs
- NET405 - Another Day, Another Billion Flows

AWS re:Invent

Thank you!