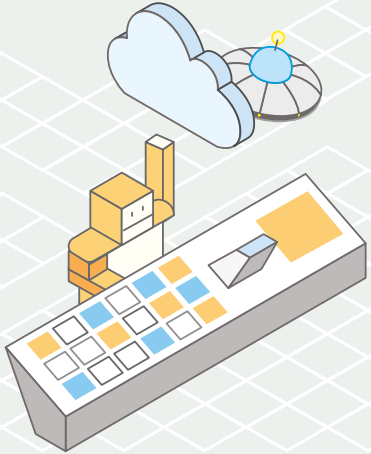
amazon web services | Pop-up Loft LONDON

Amazon Virtual Private Cloud (VPC)

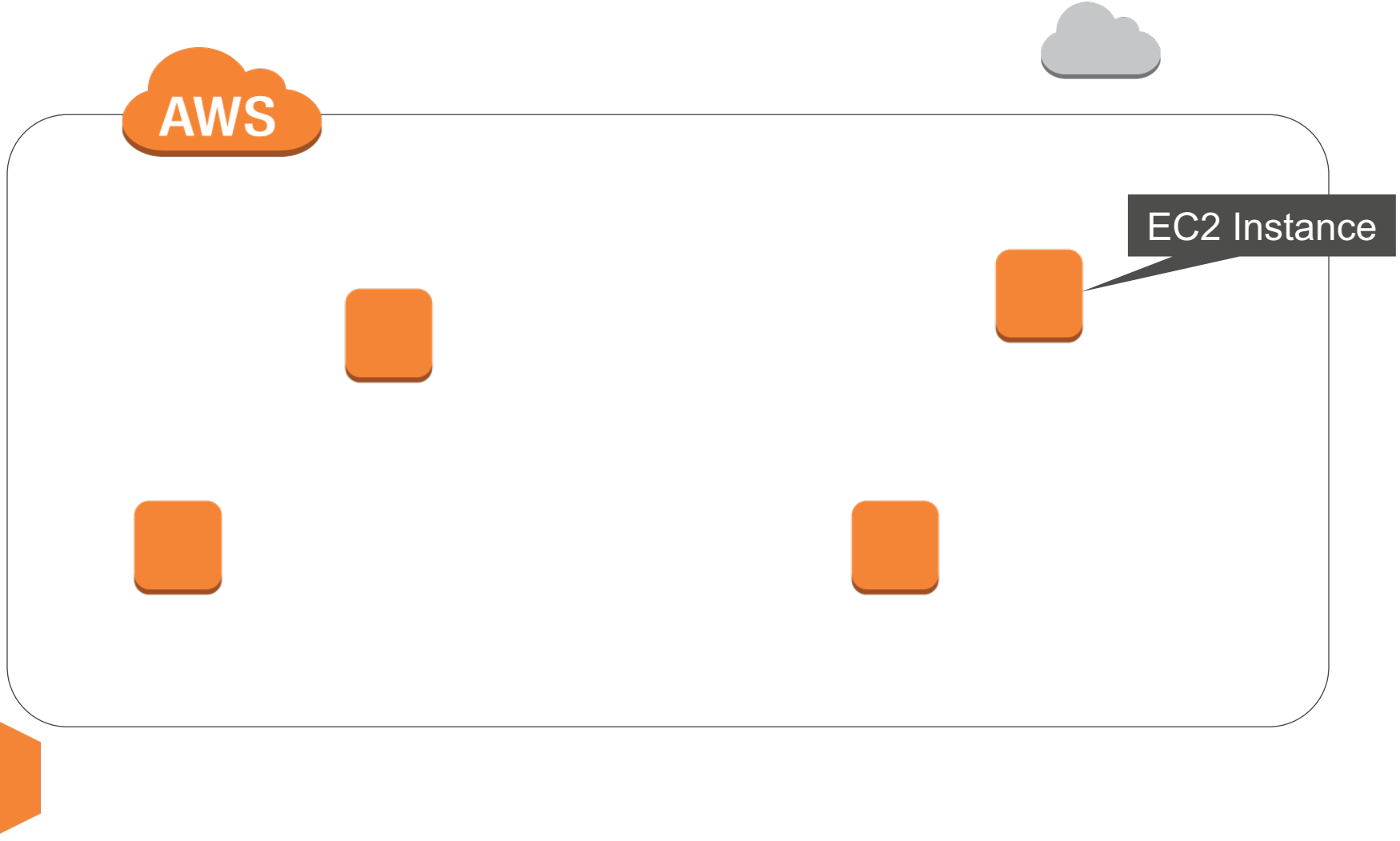
Networking Fundamentals and Connectivity Options

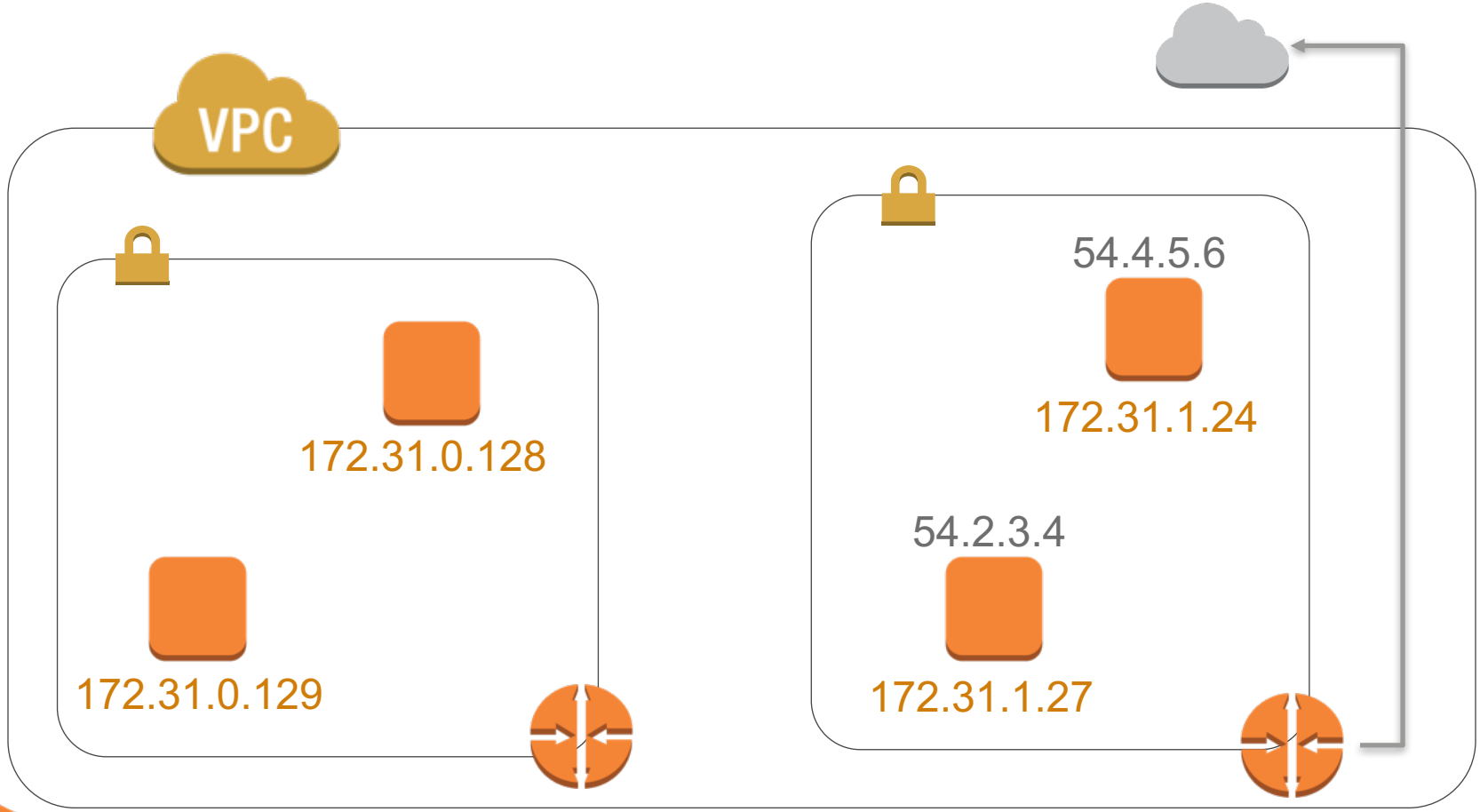
Steve Seymour
Principal Solutions Architect

@sseymour



18th September 2017


AWS
EC2 Instance



VPC

VPC: your private network in AWS

Walkthrough: setting up an Internet-connected VPC

Creating an Internet-connected VPC: steps

Choosing an address range

Setting up subnets in Availability Zones

Creating a route to the Internet

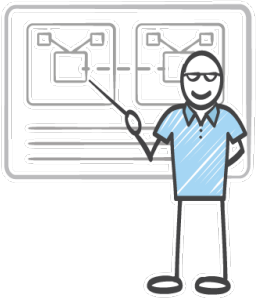
Authorizing traffic to/from the VPC

Choosing an IP address range

CIDR notation review

CIDR range example:

```
172.31.0.0/16
1010 1100 0001 1111 0000 0000 0000 0000
```



Choosing an IPv4 address range for your VPC

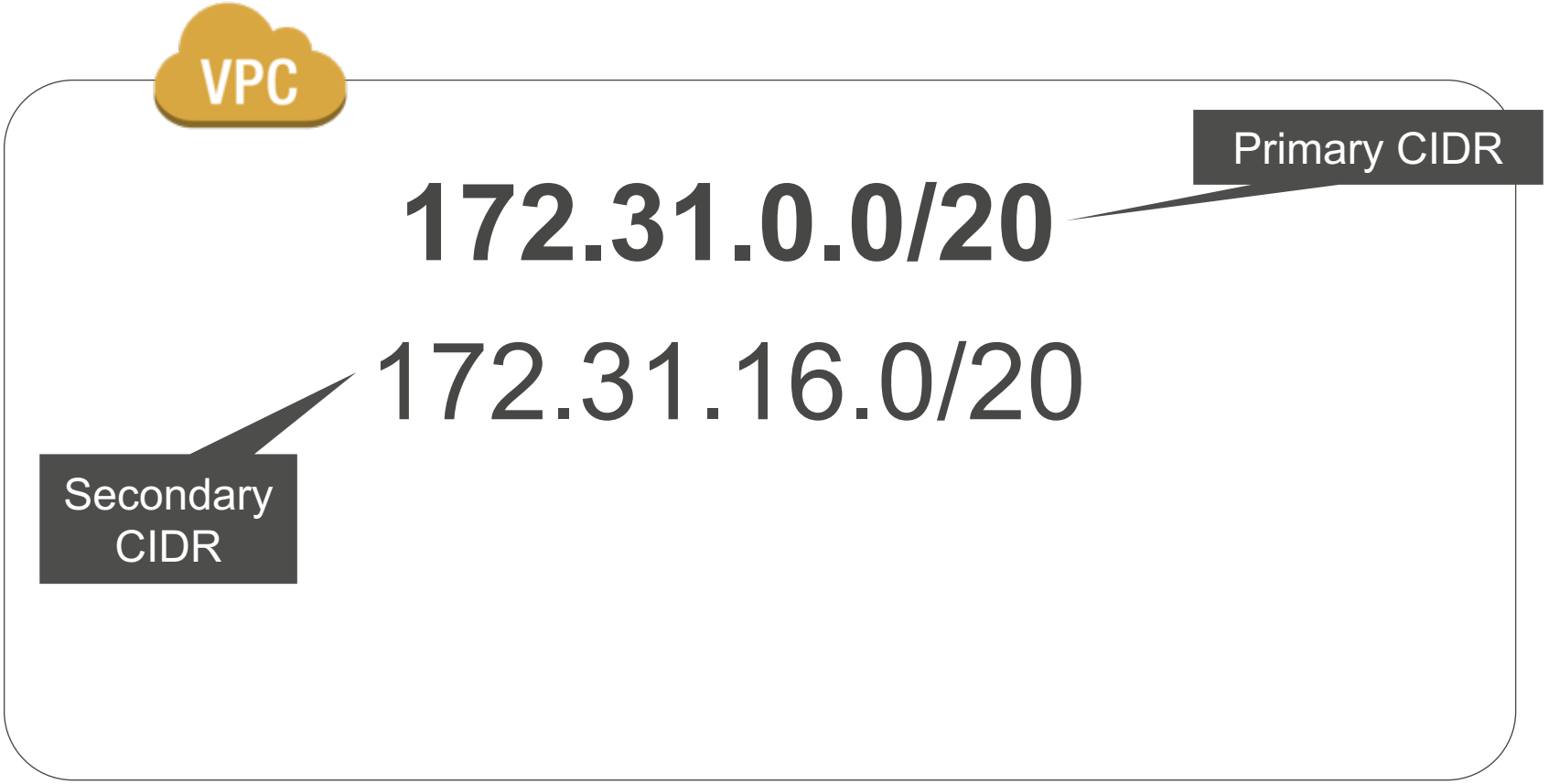
Avoid ranges that overlap with other networks to which you might connect.

172.31.0.0/16

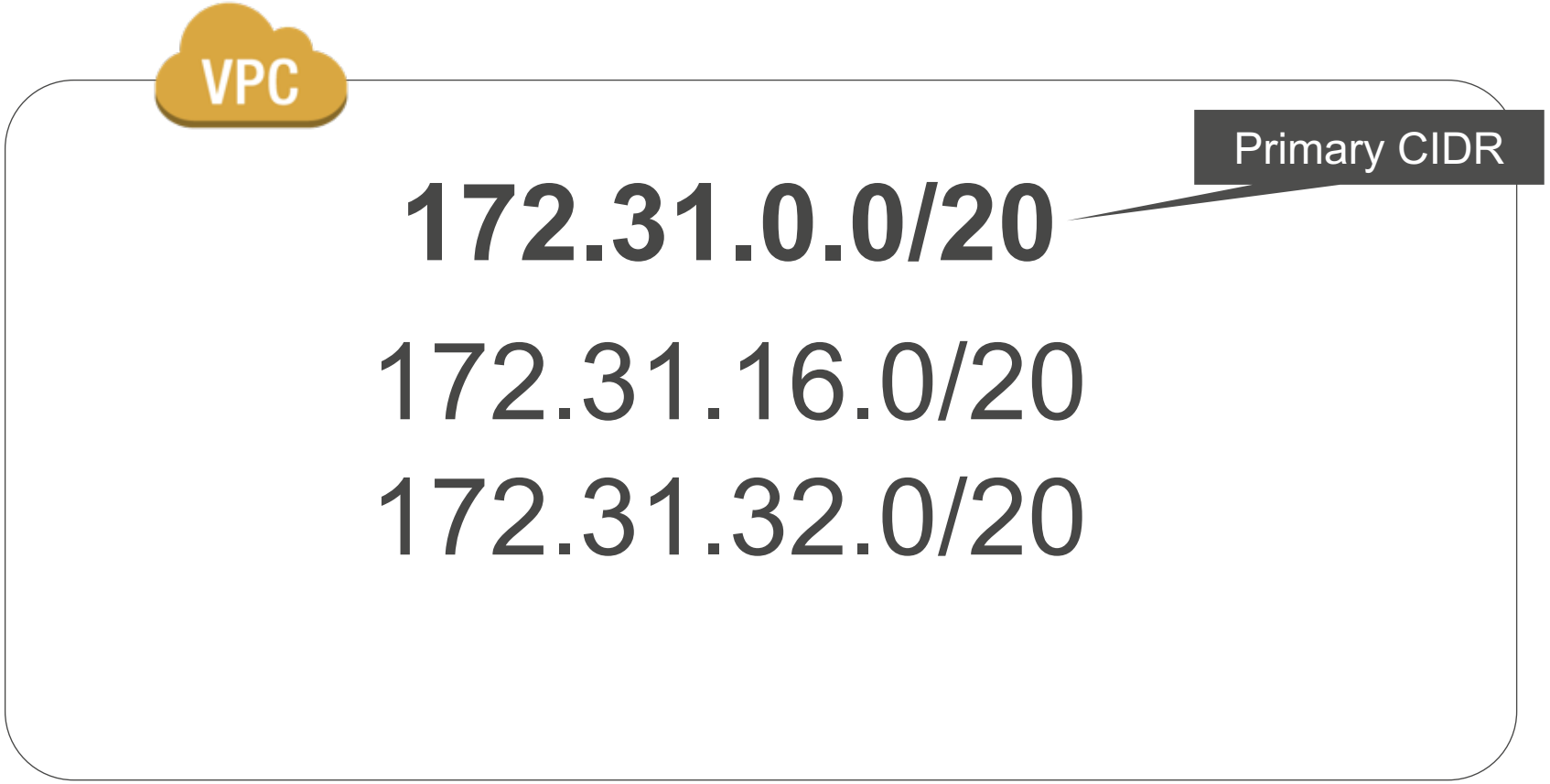
Recommended:
RFC1918 range

Recommended:
/16
(64K addresses)

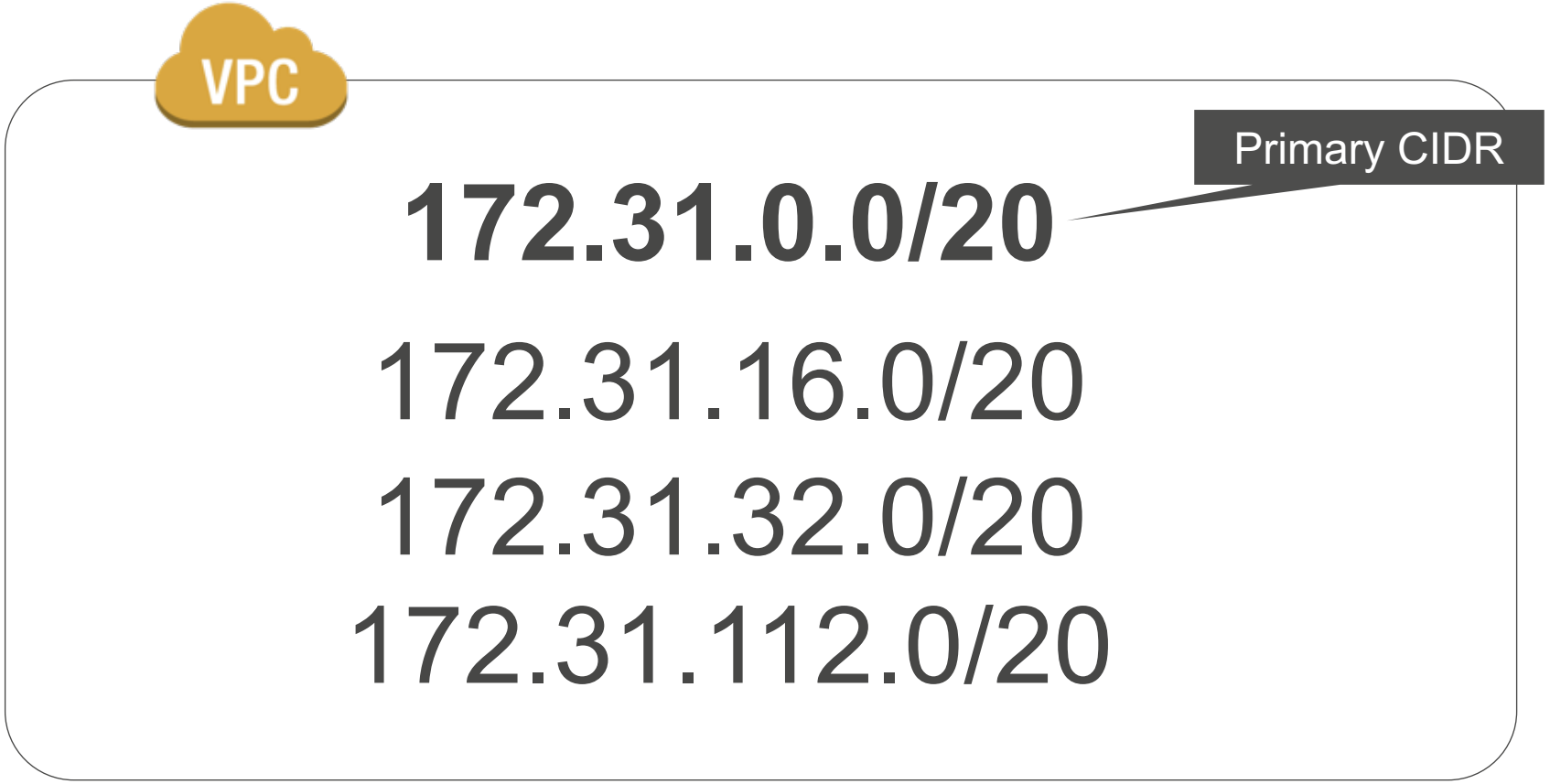
Adding a secondary IPv4 address range



Adding a secondary IPv4 address range



Adding a secondary IPv4 address range



IPv6 in Amazon VPC – Dual-stack

172.31.0.0/16

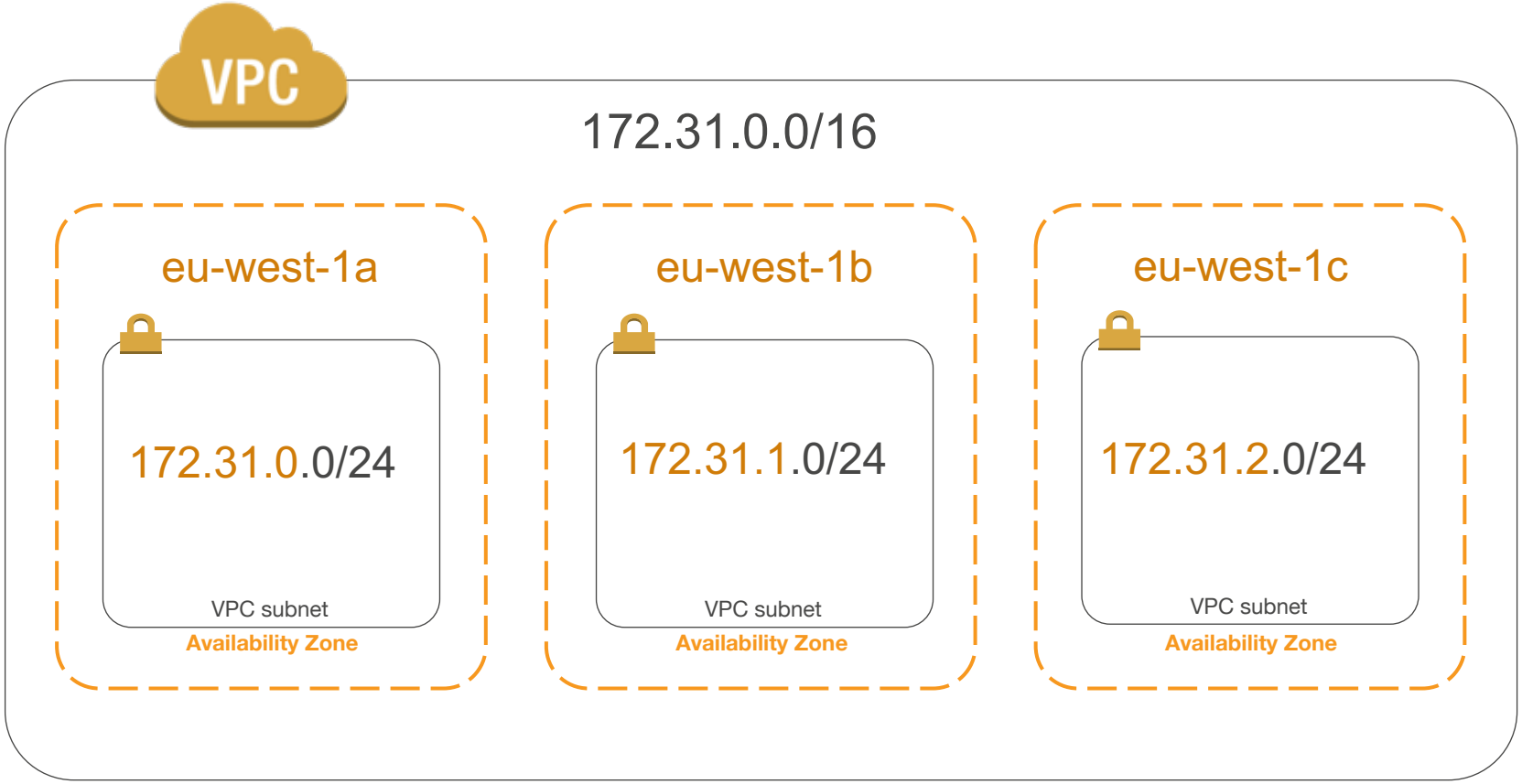
2001:db8:1234:1a00::/56

Amazon Global Unicast Addresses (GUA) – Internet Routable

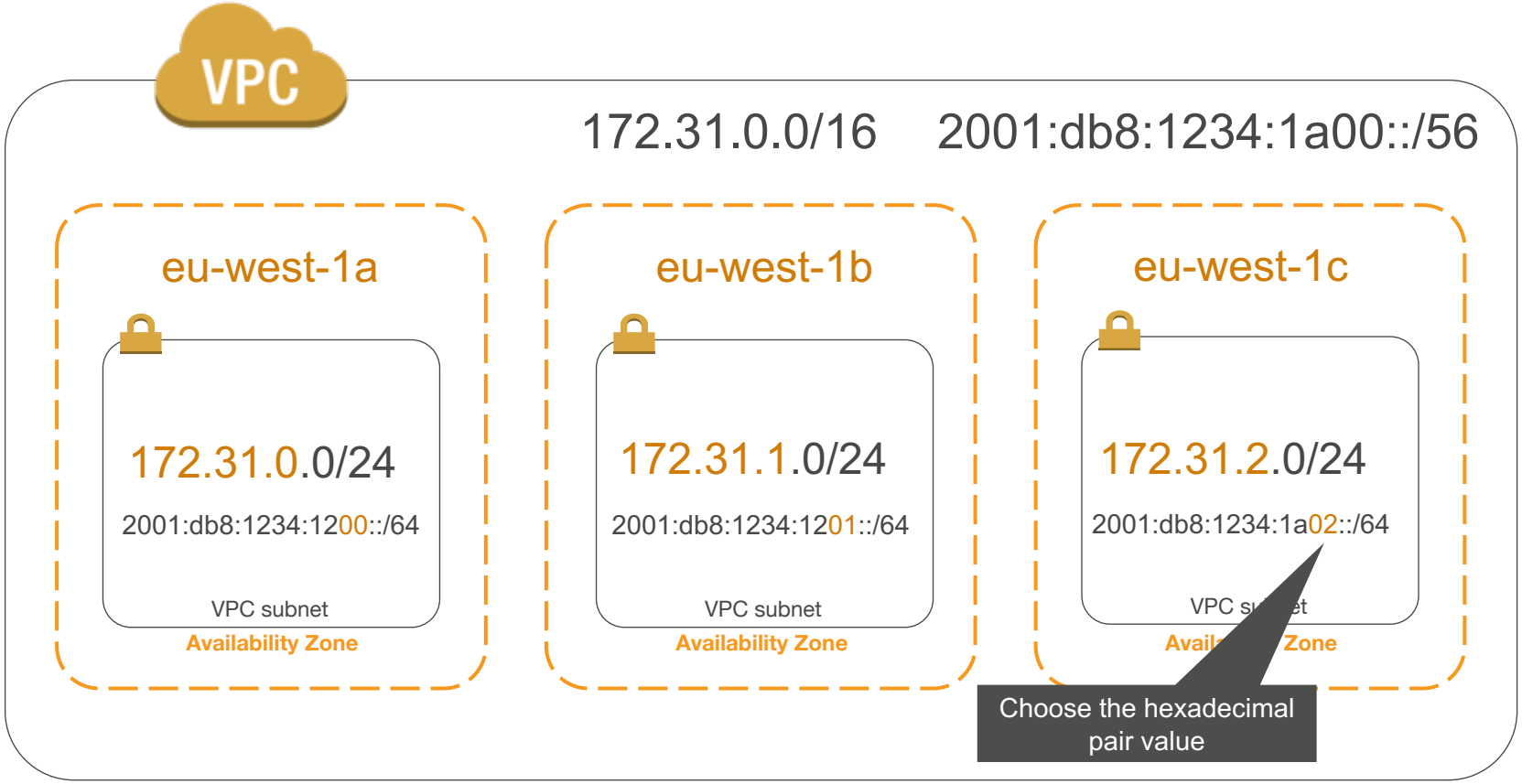
Associate an /56 IPv6 CIDR (Automatically allocated)

Subnets

VPC subnets and Availability Zones

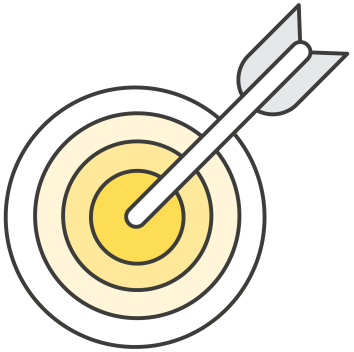


VPC subnets and Availability Zones – IPv6



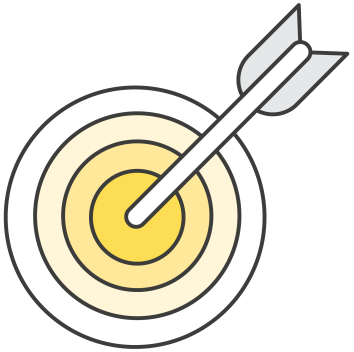
VPC subnet recommendations

- /16 VPC (64K IPv4 addresses)
- /24 subnets (251 IPv4 addresses)
- One subnet per Availability Zone



VPC subnet recommendations

- /16 VPC (64K IPv4 addresses)
- /24 subnets (251 IPv4 addresses)
- One subnet per Availability Zone



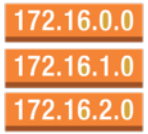
For IPv6 -

- /56 Allocated per VPC (Lots of addresses)
- /64 subnets (256 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

Send packets here if you want them to reach the Internet

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

ID: igw-3376c756

State: attached

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

Attachment state: available

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

Search Route Tables and their

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

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

rtb-04304e

Summary | 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

2.31.0.0/16	local	Active	No
0.0.0.0/0	igw-3376c756	Active	No

Network security in VPC: Network ACLs / Security Groups

Network ACLs: Stateless firewalls

Can be applied on a subnet basis

English translation: Allow all traffic in

Search Network ACLs and the

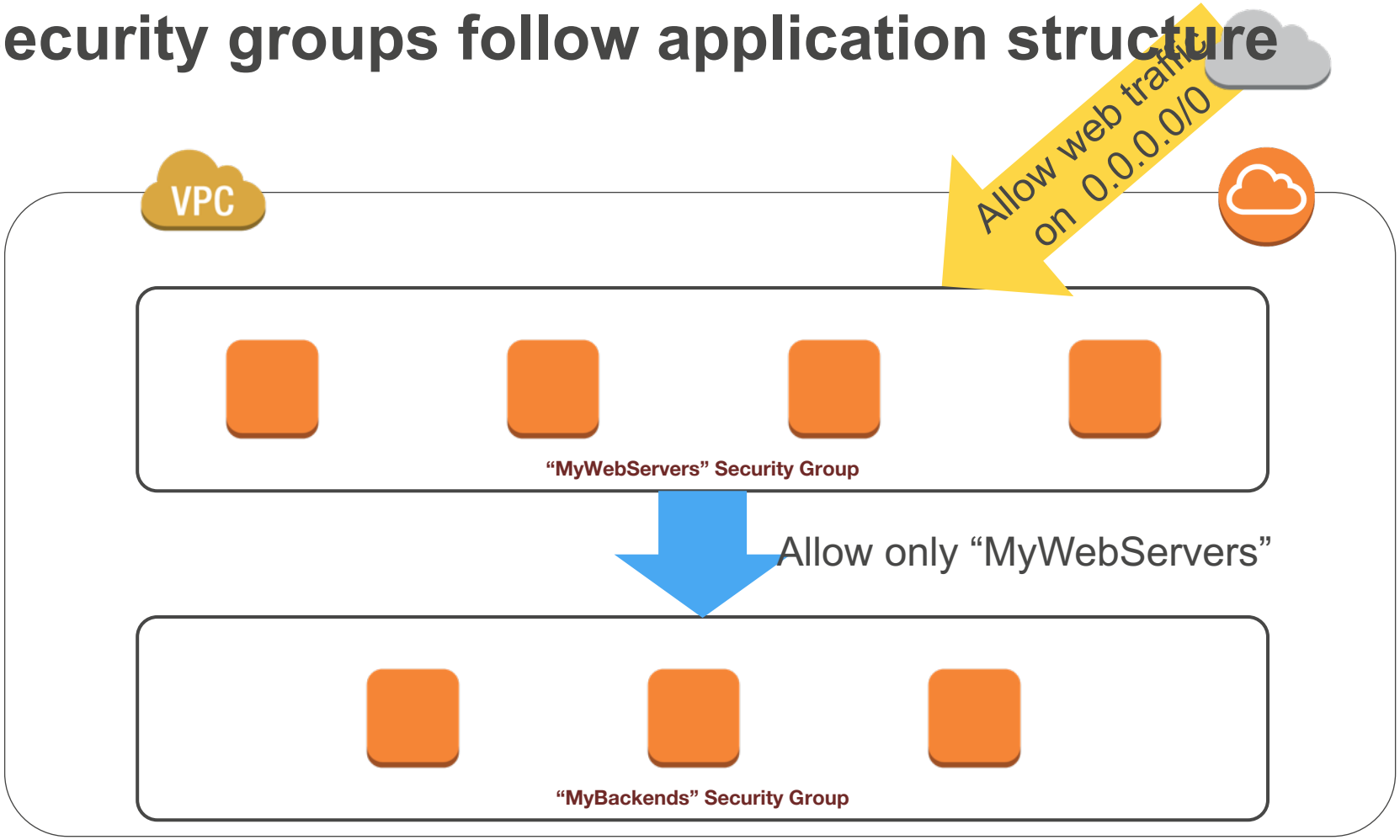
Name	Network ACL ID	Ass		
	acl-5cc5b539	3 Subnets	Yes	vpc-327d1857 (172

acl-5cc5b539

Rule #	Type	Protocol	Port Range	Sour	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Security groups follow application structure



Security groups example: web servers

Create Security Group | Delete Security Group

Filter VPC security groups | Search Security Groups and th | 1 to 3

Name tag	Group ID	Group Name	VPC	Description
MyWebServers	sg-82ba7ee6	MyWebServers	vpc-327d1857	Allows all traffic from the Internet
MyBackends	sg-8fba7eeb	MyBackends	vpc-327d1857	Allows only traffic from MyWebServers
	sg-07996163	default		

In English: Hosts in this group are reachable from the Internet on port 80 (HTTP)

sg-82ba7ee6 | MyW

Summary

Edit

Type	Protocol	Port Range	Source
HTTP (80)	TCP (6)	80	0.0.0.0/0

Type	Protocol	Port Range	Source
HTTP (80)	TCP (6)	80	0.0.0.0/0

Security groups example: backends

Create Security Group | Delete Security Group

Filter VPC security groups | Search Security Groups and tl | 1 to 3 of

Name tag	Group ID	Group Name	VPC	Description
MyWebServers	sg-82ba7ee6	MyWebServers	vpc-327d1857	Allows all traffic from the Internet
MyBackends	sg-8fba7eeb	MyBackends		
	sg-07996163	default		

In English: Only instances in the MyWebServers Security Group can reach instances in this Security Group

sg-8fba7eeb | My

Summary

Edit

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP (6)	2345	sg-82ba7ee6

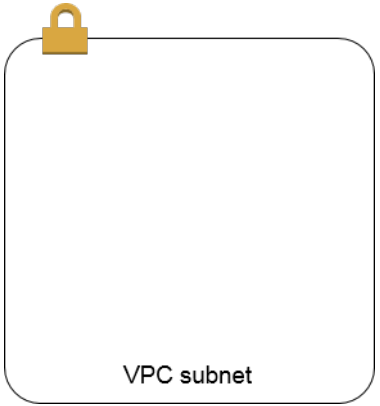
Type			
Custom TCP Rule	TCP (6)	2345	sg-82ba7ee6

Security groups in VPC: additional notes

- Follow the Principle of Least Privilege
- VPC allows creation of egress as well as ingress Security Group rules
- Many application architectures lend themselves to a 1:1 relationship between security groups (who can reach me) and IAM roles (what I can do).

Connectivity options for VPCs

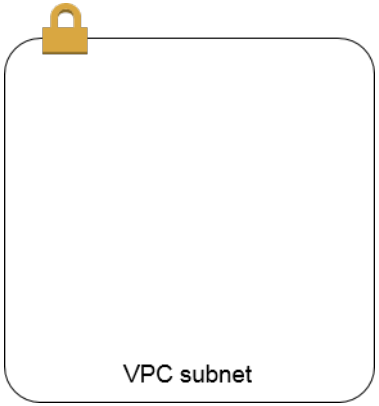
Beyond Internet connectivity



Restricting Internet access

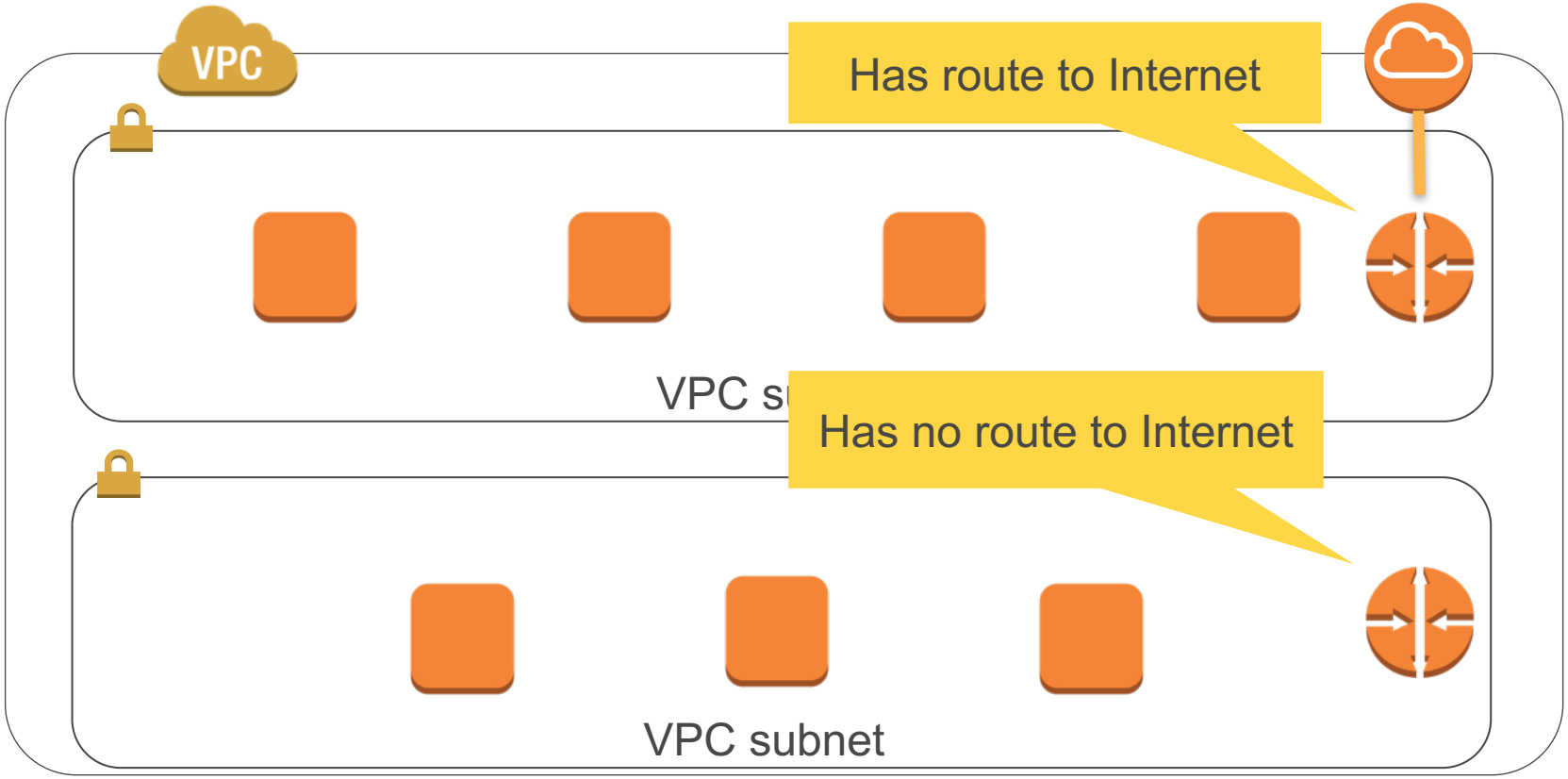
Connecting to other VPCs

Connecting to your corporate network

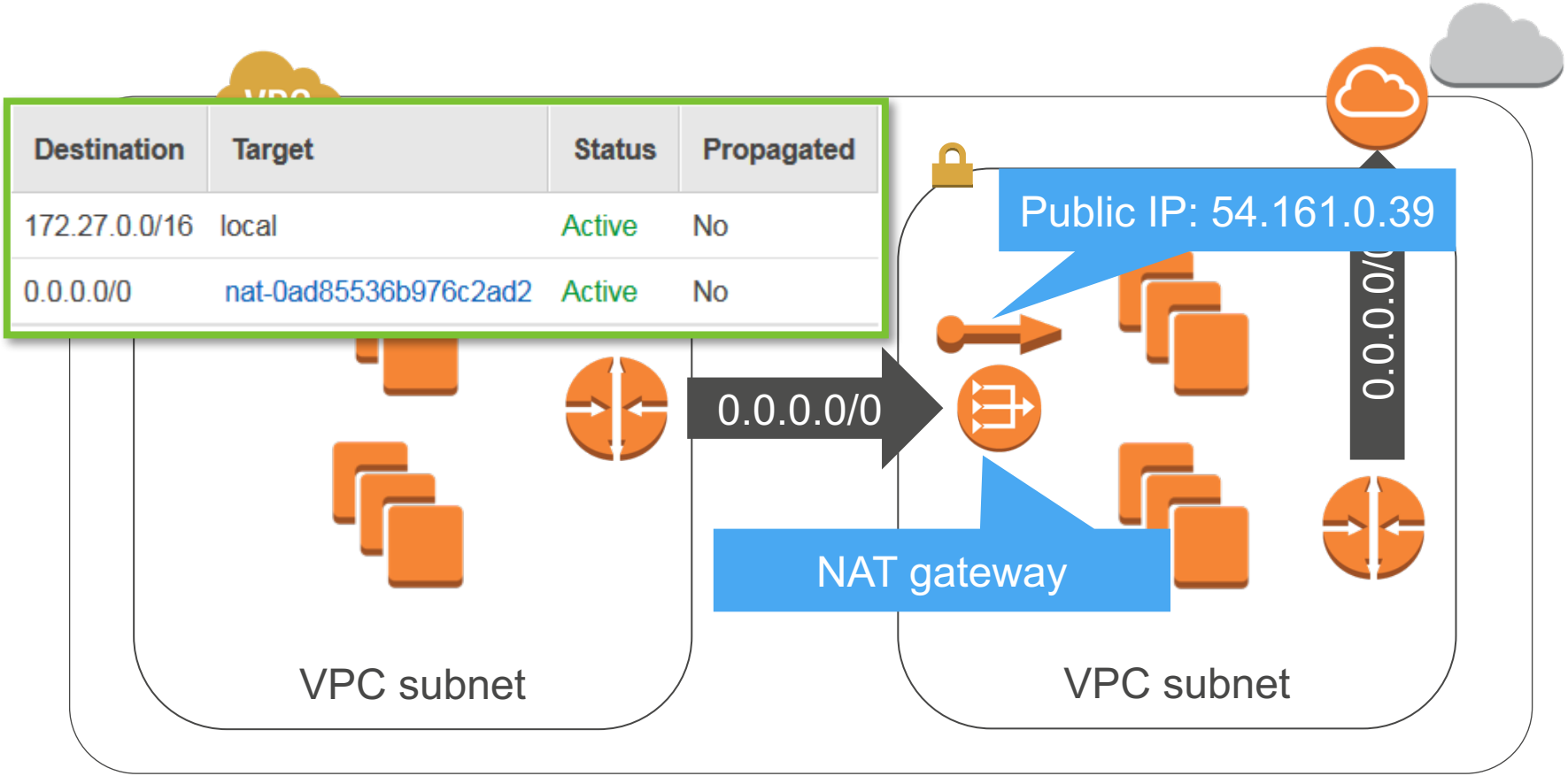


Restricting Internet access: Routing by subnet

Routing by subnet



Outbound-only Internet access: NAT gateway

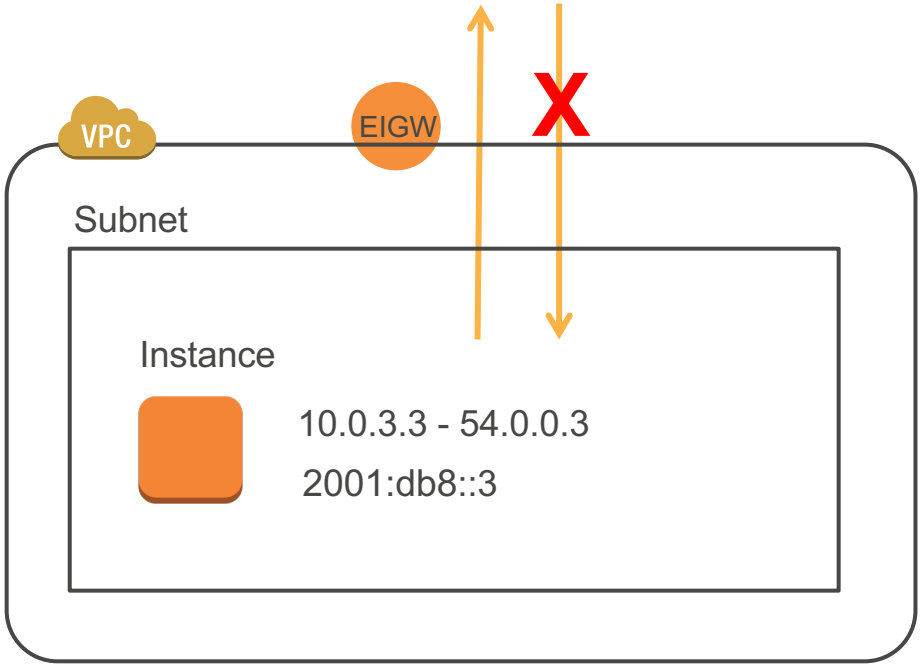


IPv6 GUAs

- For IPv6, Amazon VPC instances receive Global Unicast Addresses (GUA), which are Internet routable
- GUAs directly assigned to instances; <u>there is no 1:1 NAT in the case of Internet access</u>
- Using GUAs does not mean losing security or privacy—to have Internet access, you also need to have proper route tables, security groups, and gateways

IPv6 Egress-only Internet Gateway

- A new virtual device that provides egress-only Internet access over IPv6
  - No middle box to perform NAT, and no additional cost
  - No performance/availability/ connection limits

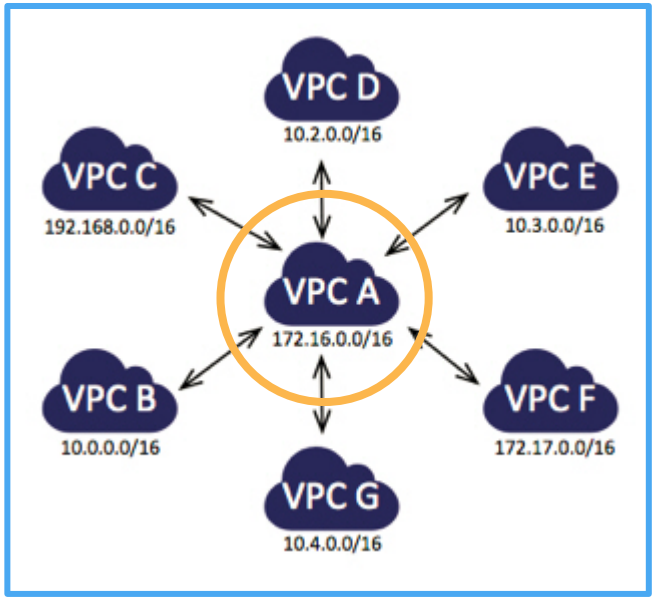


Inter-VPC connectivity: VPC peering

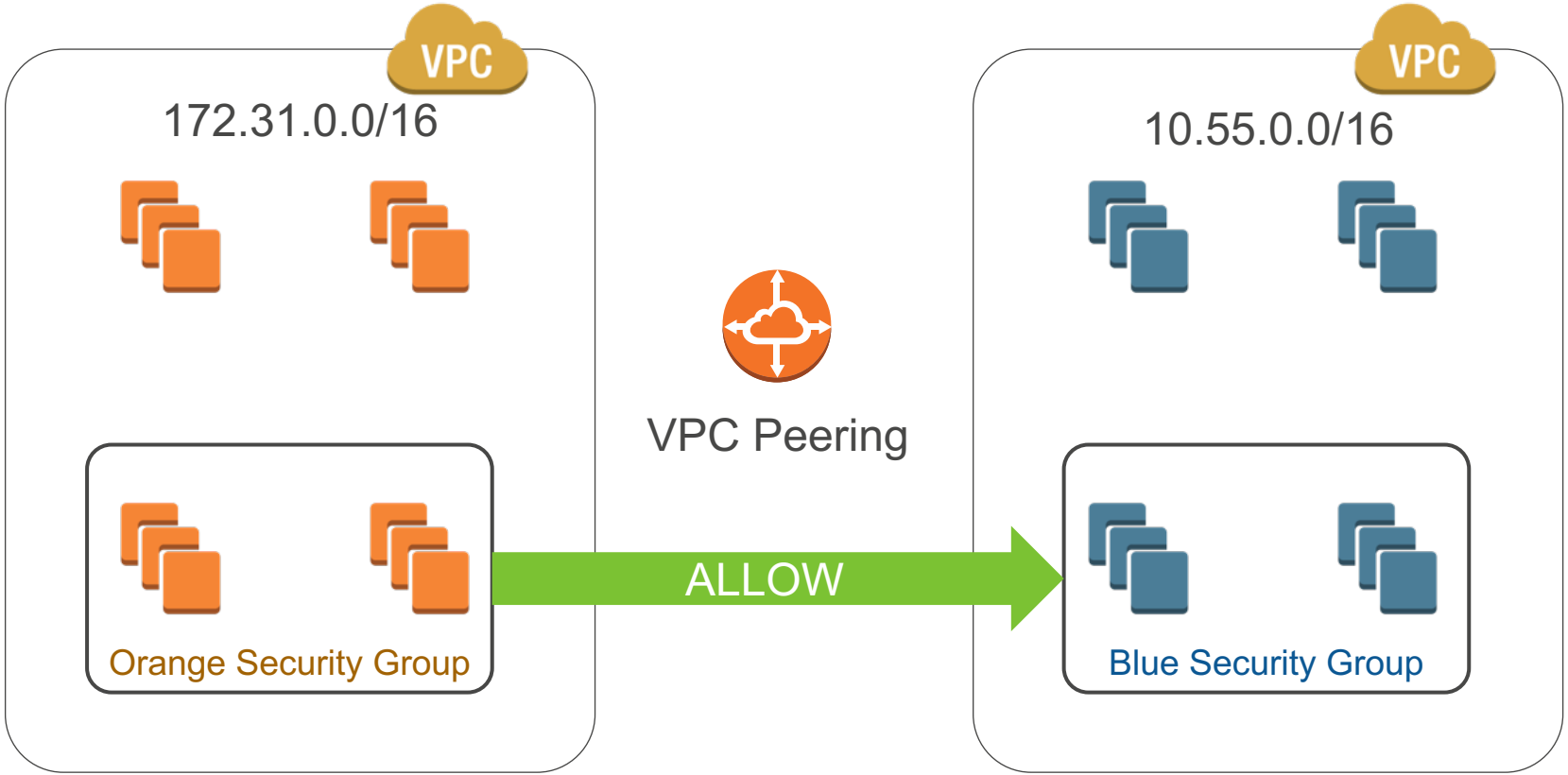
Example VPC peering use: shared services VPC

Common/core services

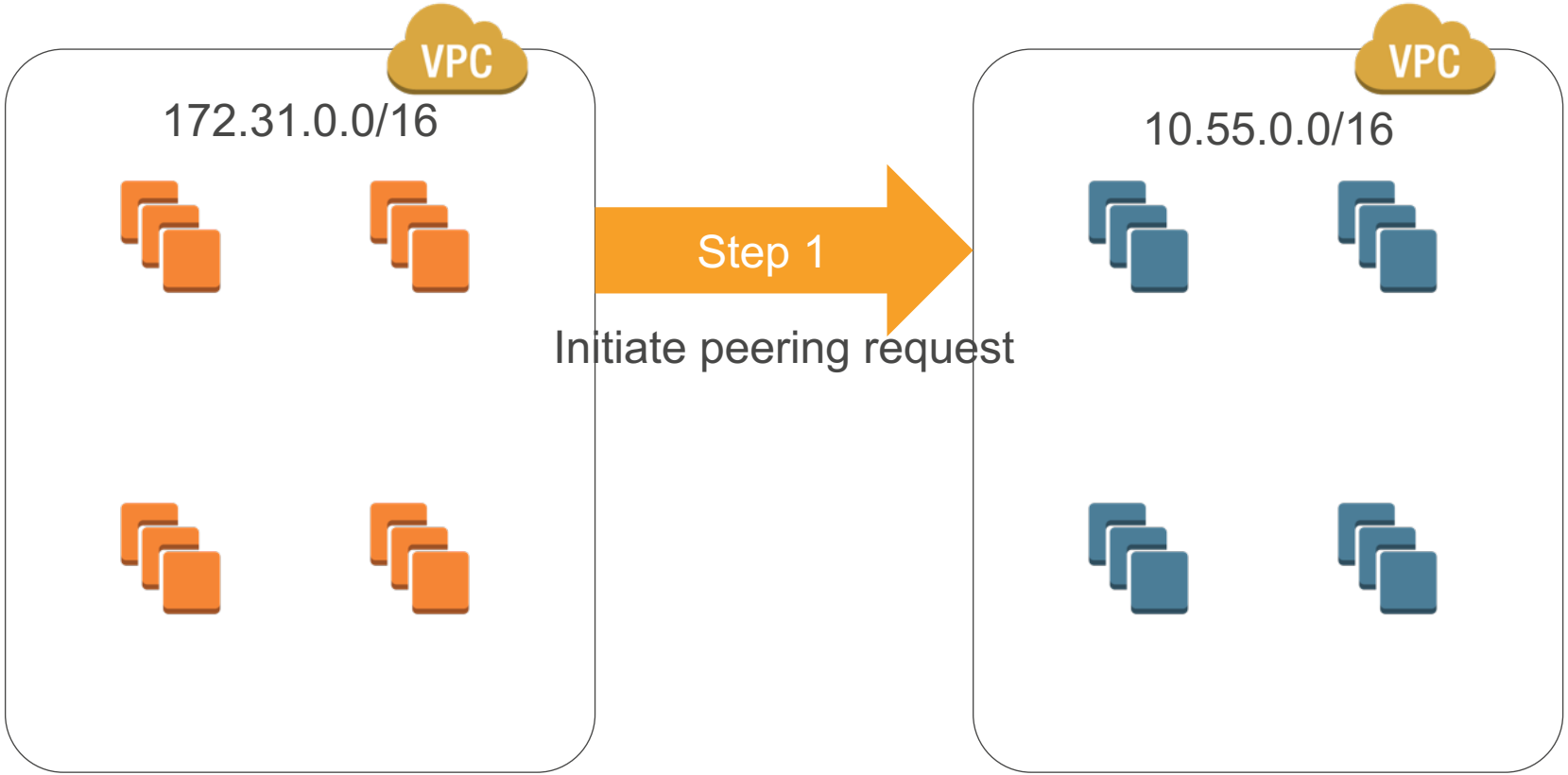
- Authentication/directory
- Monitoring
- Logging
- Remote administration
- Scanning



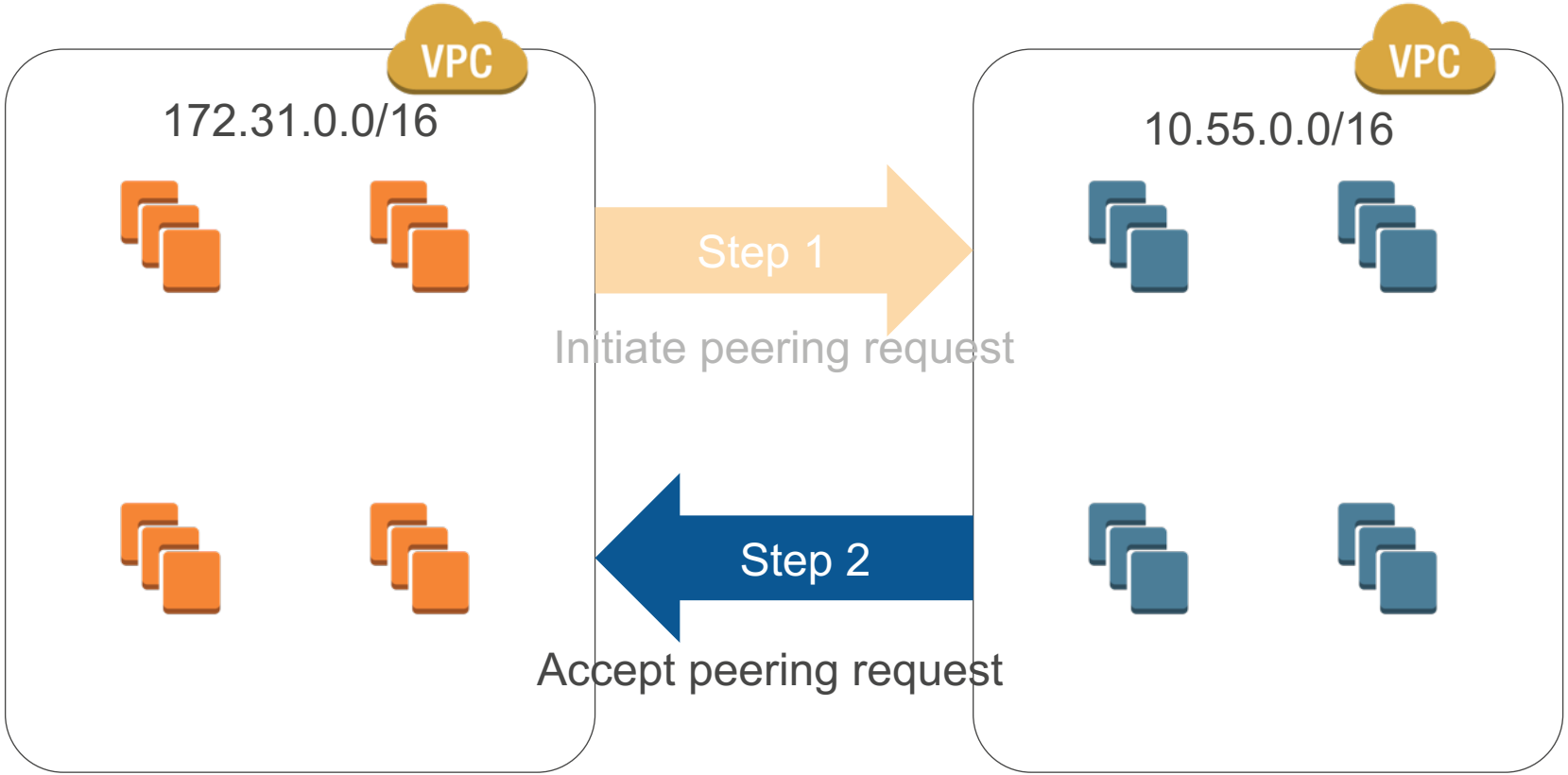
Security groups across peered VPCs



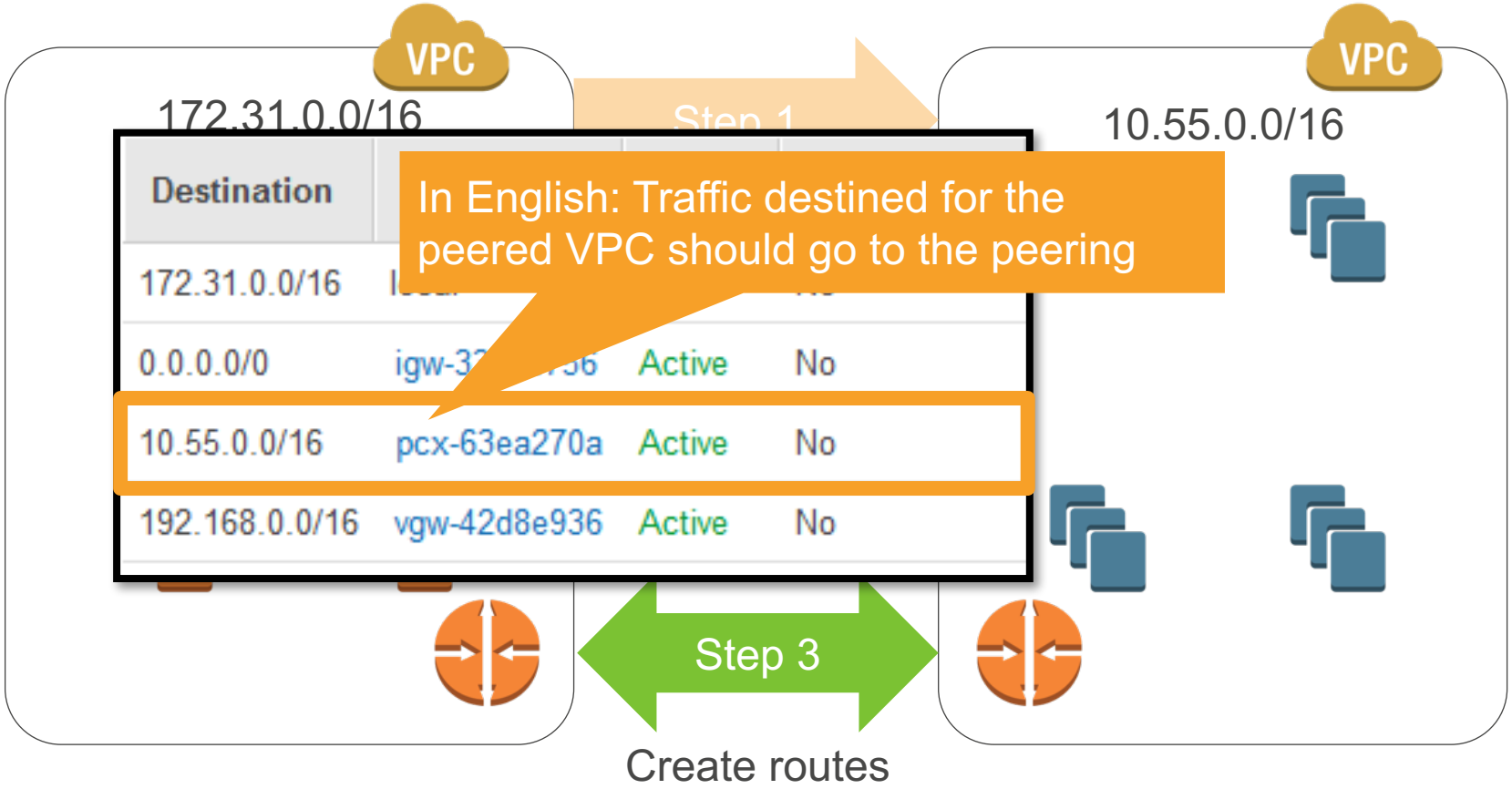
Establish a VPC peering: initiate request



Establish a VPC peering: accept request

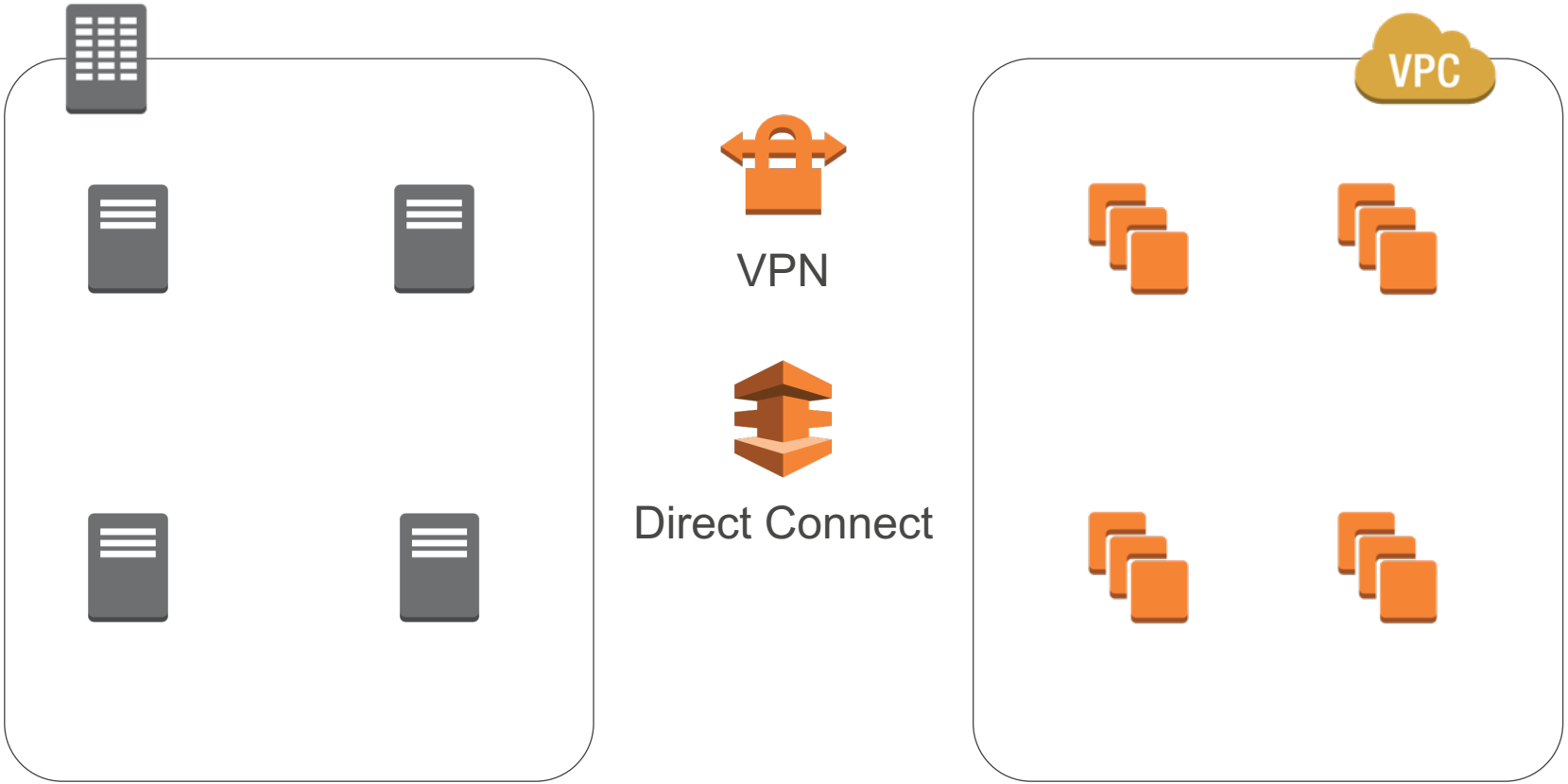


Establish a VPC peering: create route

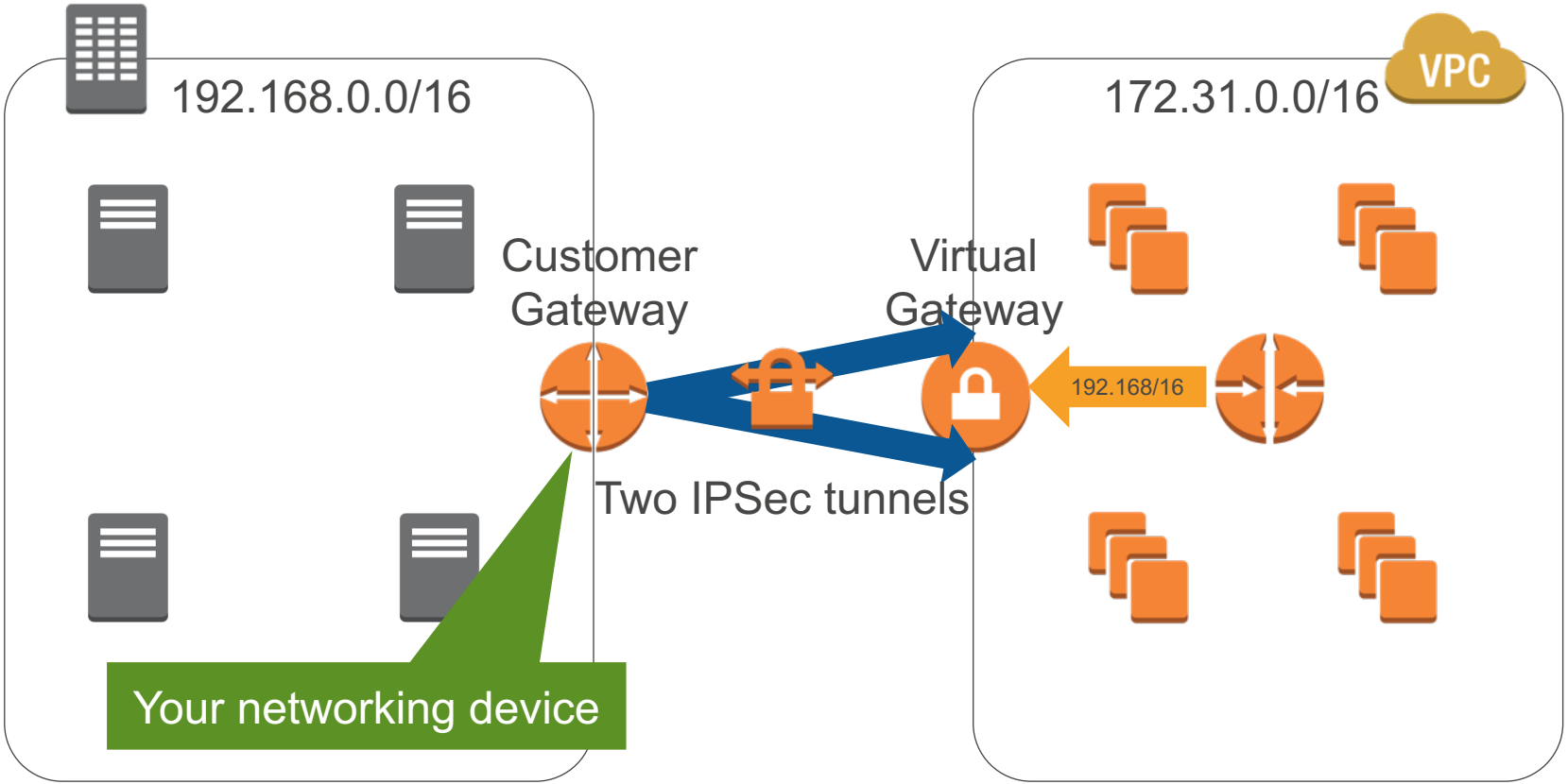


Connecting to on-premises networks: Virtual Private Network & Direct Connect

Extend an on-premises network into your VPC



AWS VPN basics

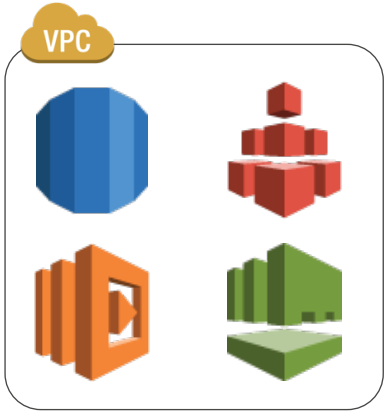


VPN and AWS Direct Connect

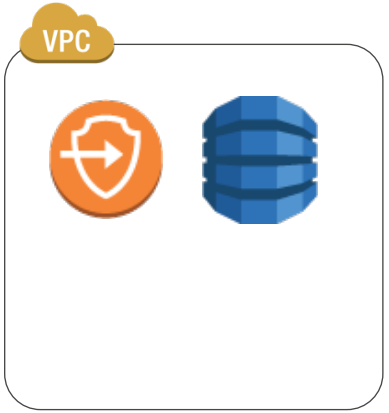
- Both allow secure connections between your network and your VPC
- VPN is a pair of IPSec tunnels over the Internet
- DirectConnect is a dedicated line with lower per-GB data transfer rates
- For highest availability: Use both

VPC and the rest of AWS

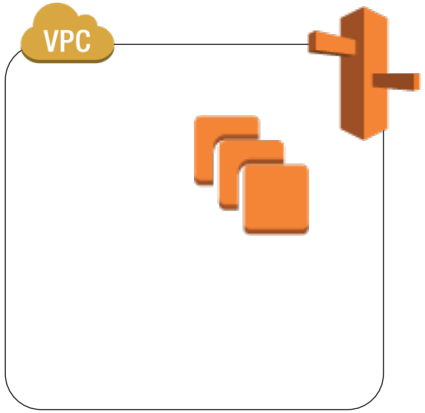
VPC and the rest of AWS



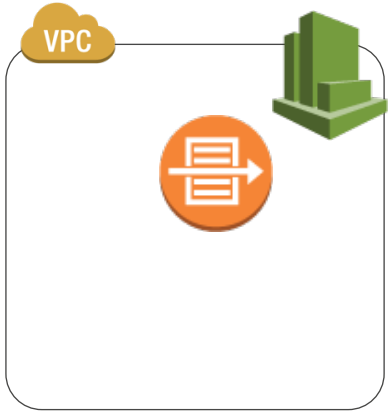
AWS Services in Your VPC



VPC Endpoints for Amazon S3 & DynamoDB



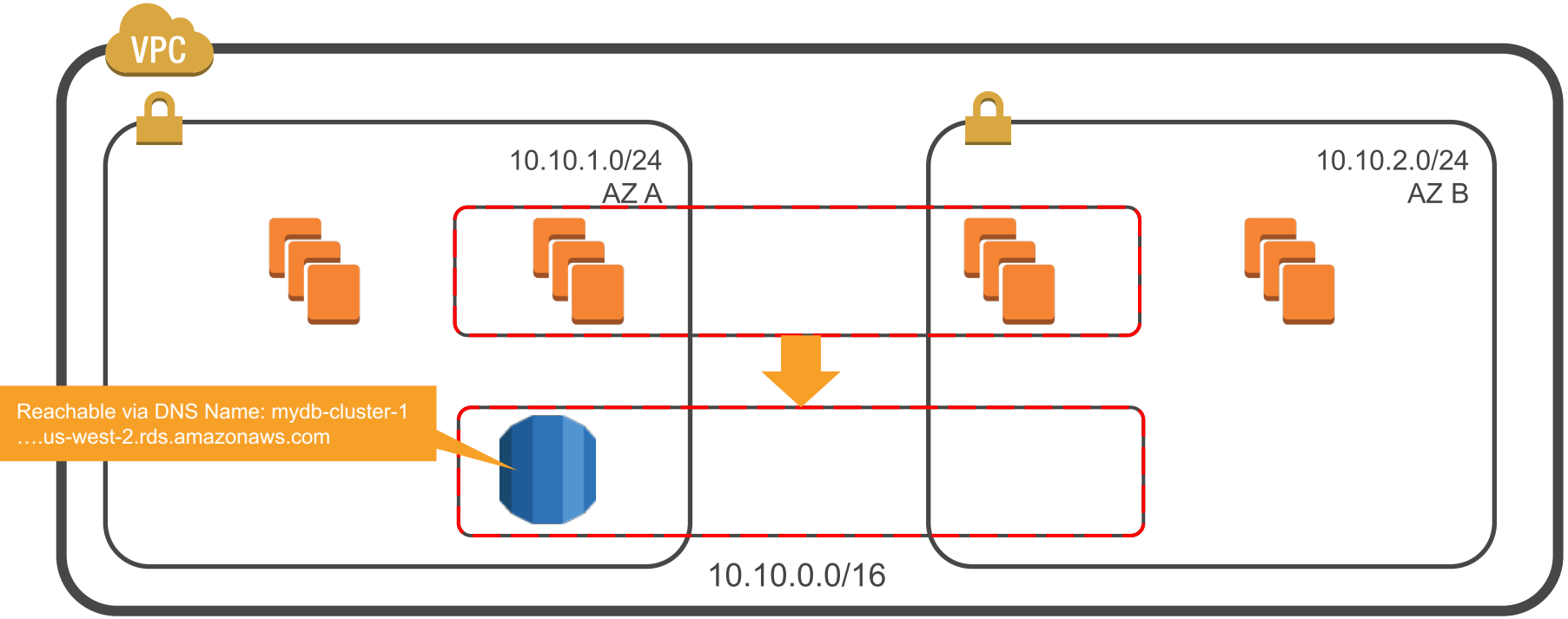
DNS in-VPC with Amazon Route 53



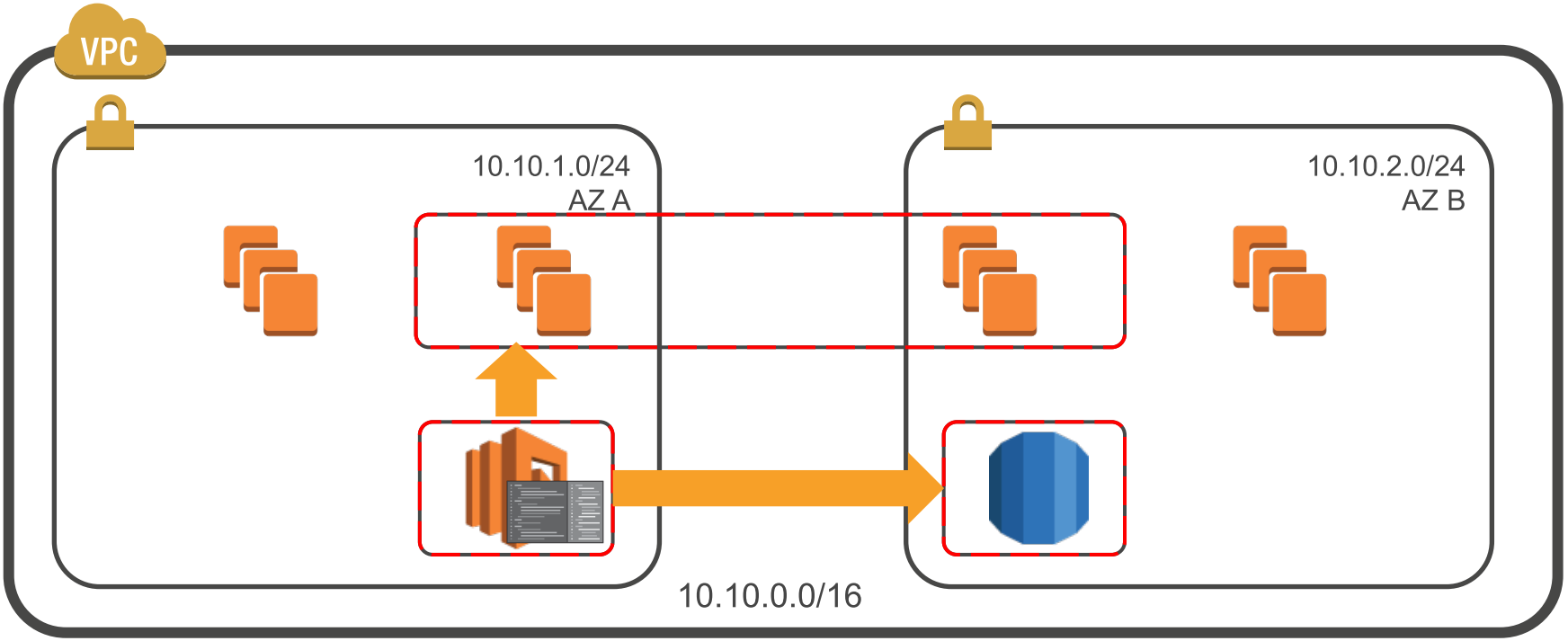
Logging VPC Traffic with VPC Flow Logs

AWS services in your VPC

Example: Amazon RDS database in your VPC

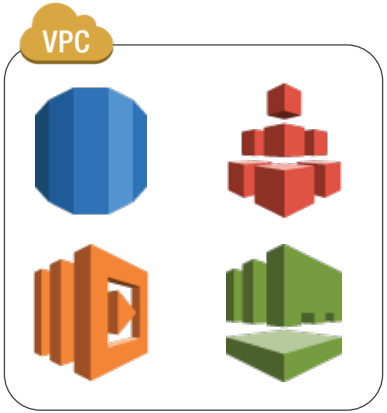


Example: AWS Lambda function in your VPC



Best practices for in-VPC AWS services

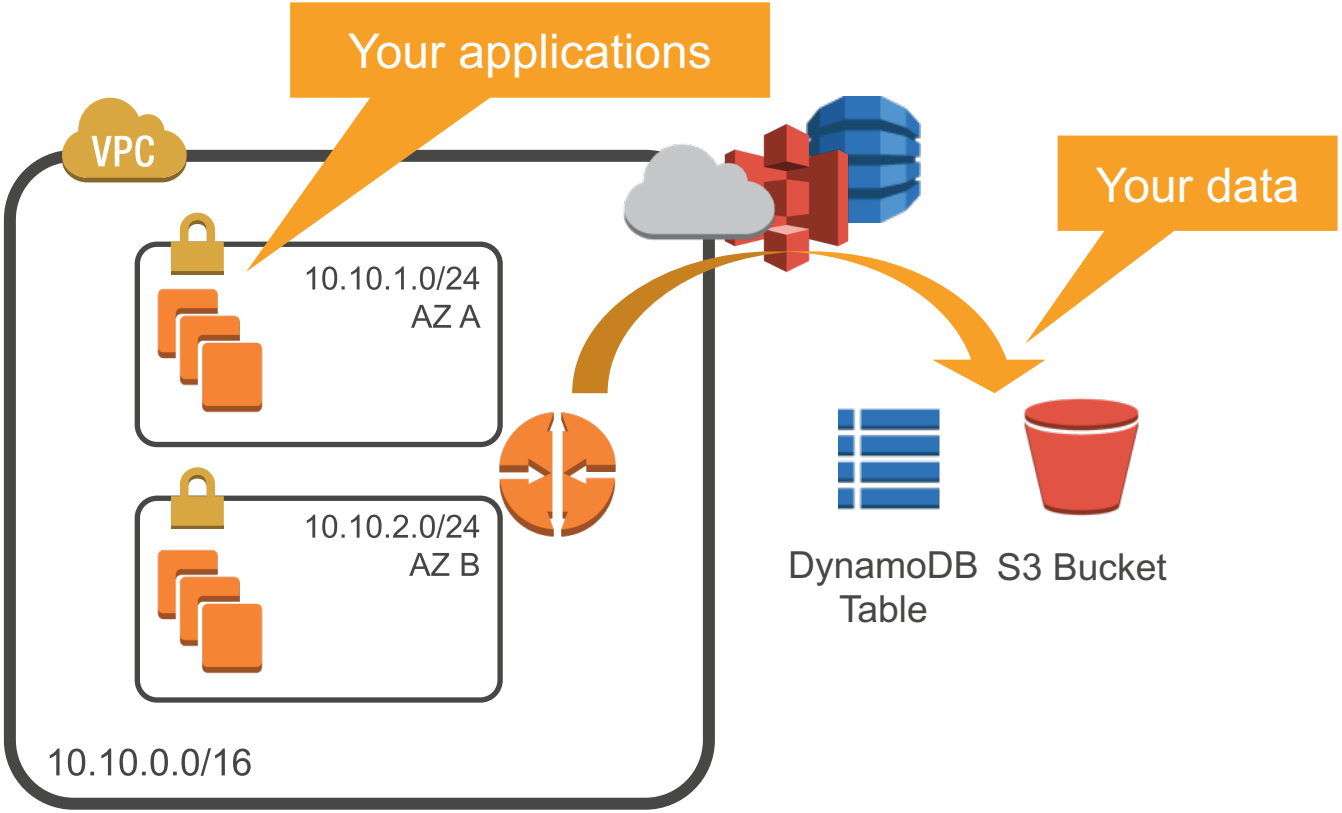
- Many AWS services support running in-VPC.
- Use security groups for Least-Privilege network access.
- For best availability, use multiple Availability Zones. Examples:
    - Multi-zone RDS deployments
    - Use a zonal mount point for EFS access



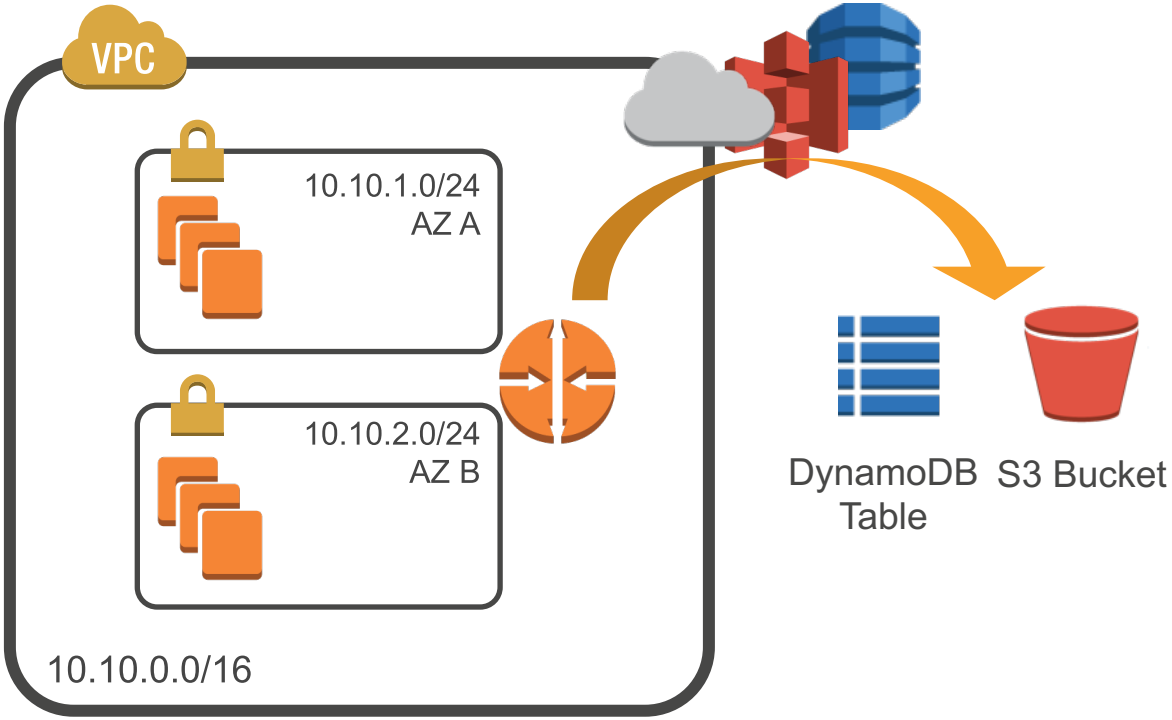
VPC Endpoints for Amazon S3

VPC Endpoints for DynamoDB

S3, DynamoDB and your VPC

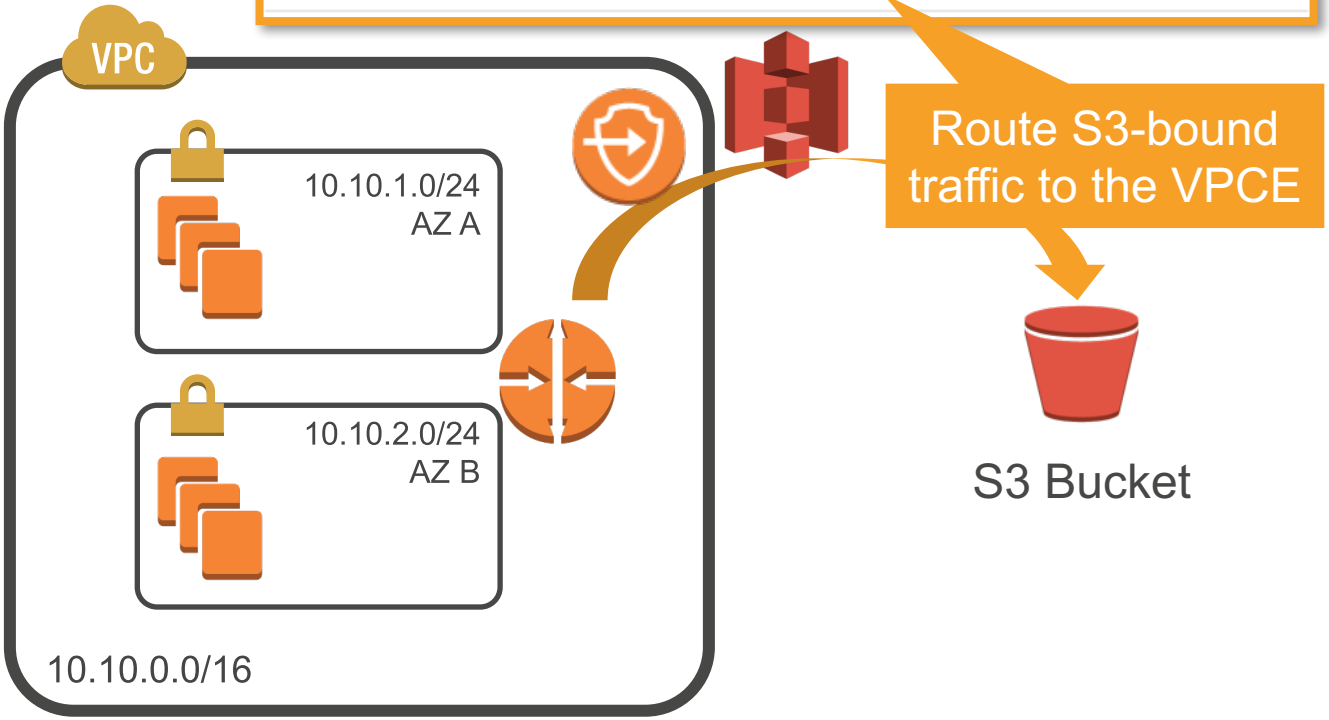


AWS VPC endpoints

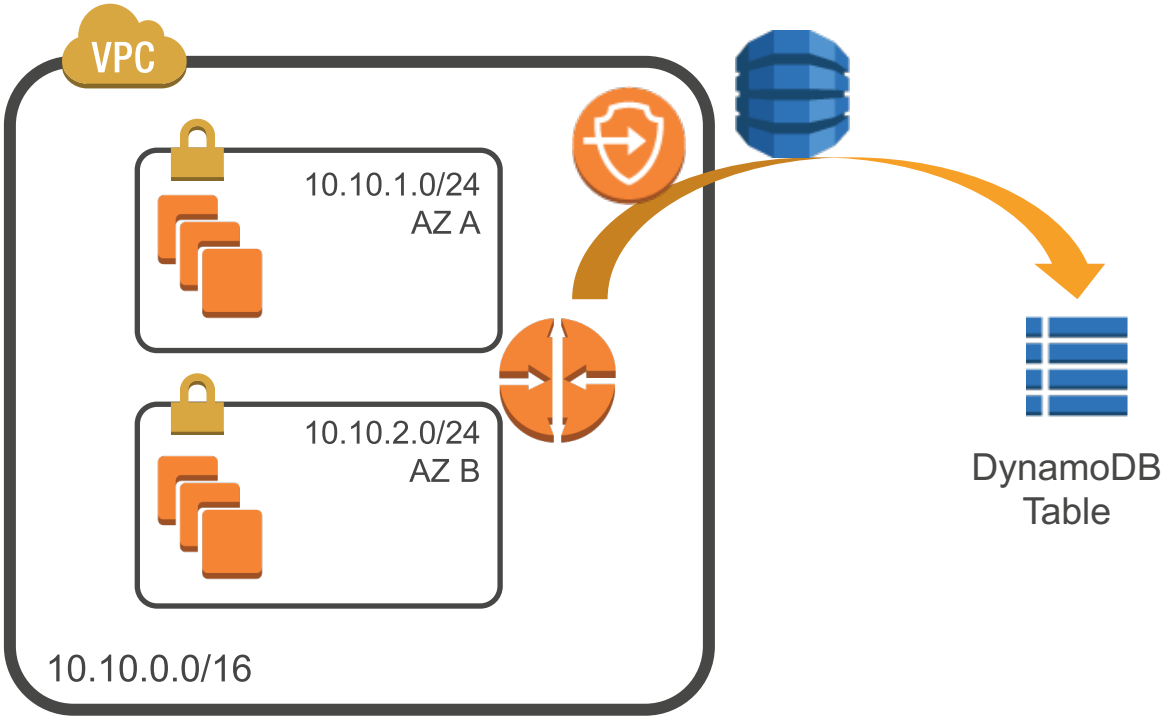


S3

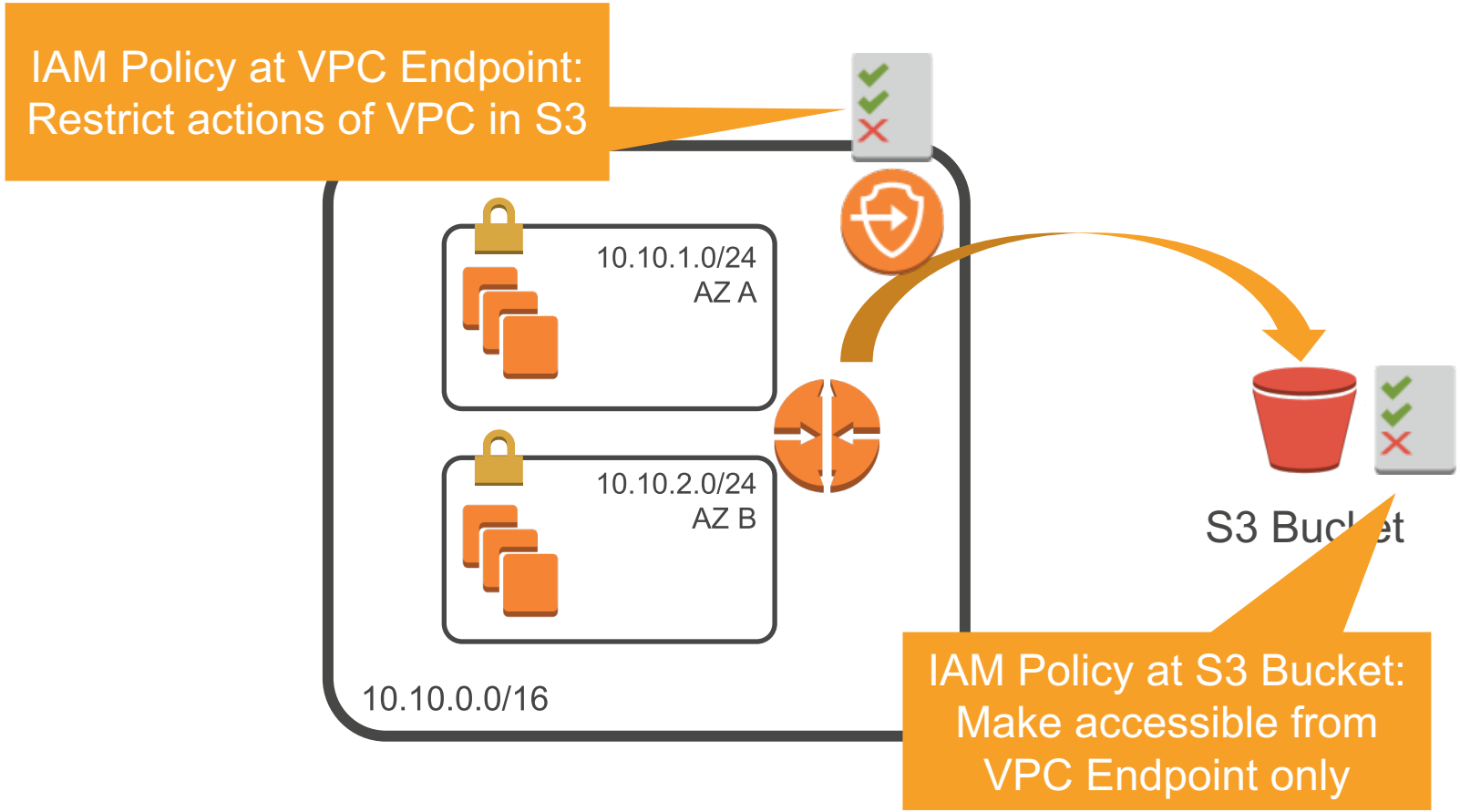
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
pl-68a54001 (com.amazonaws.us-west-2.s3)	vpce-3a14fc53	Active	No



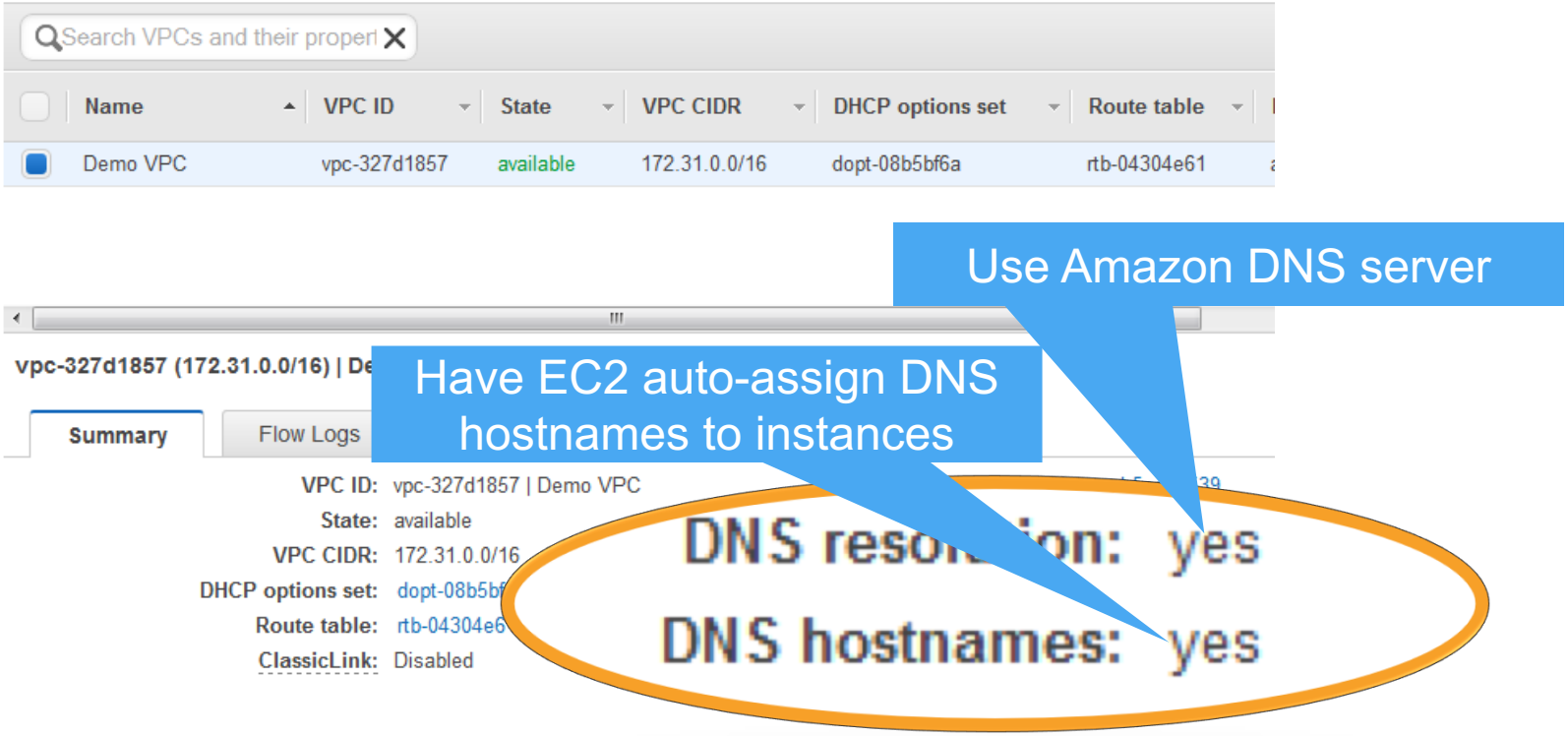
DynamoDB



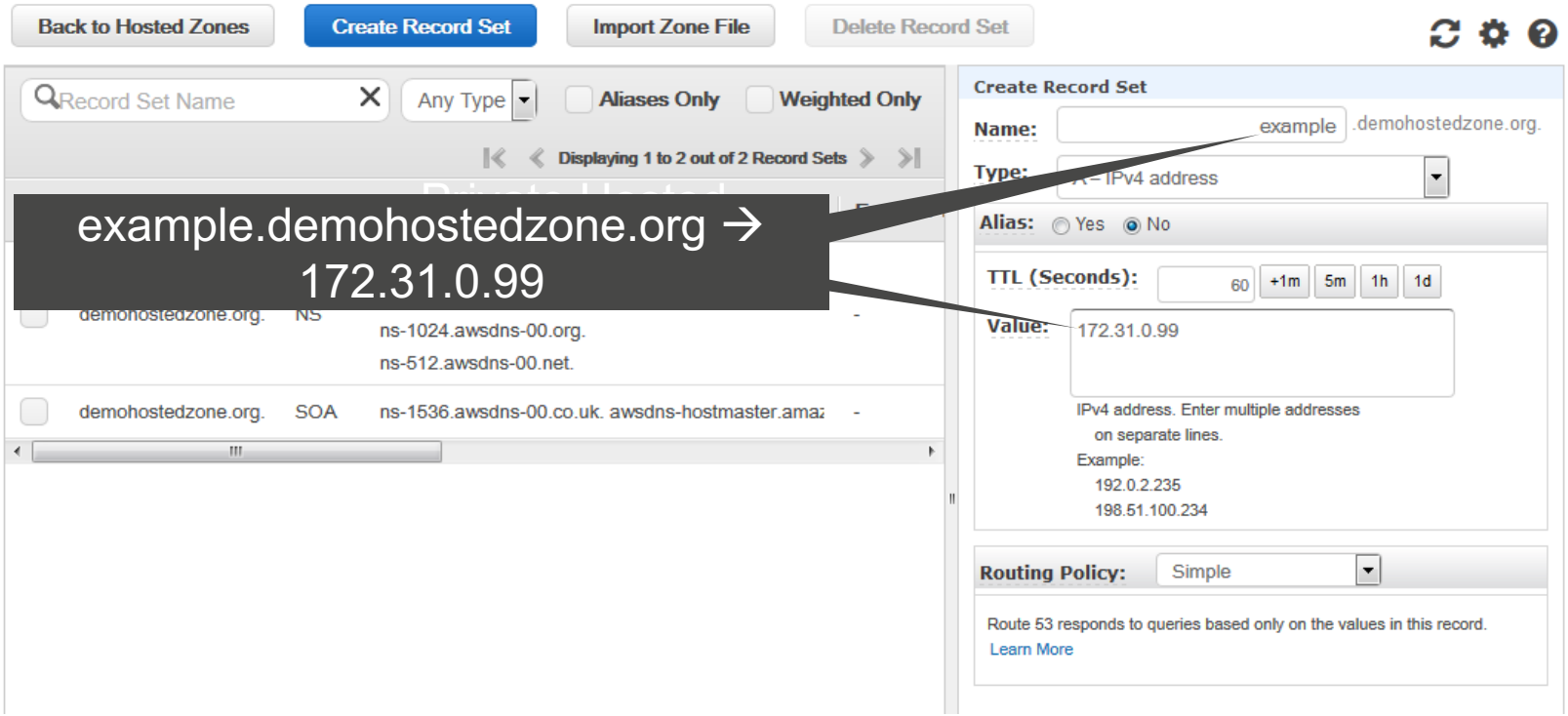
IAM policy for VPC endpoints



VPC DNS options

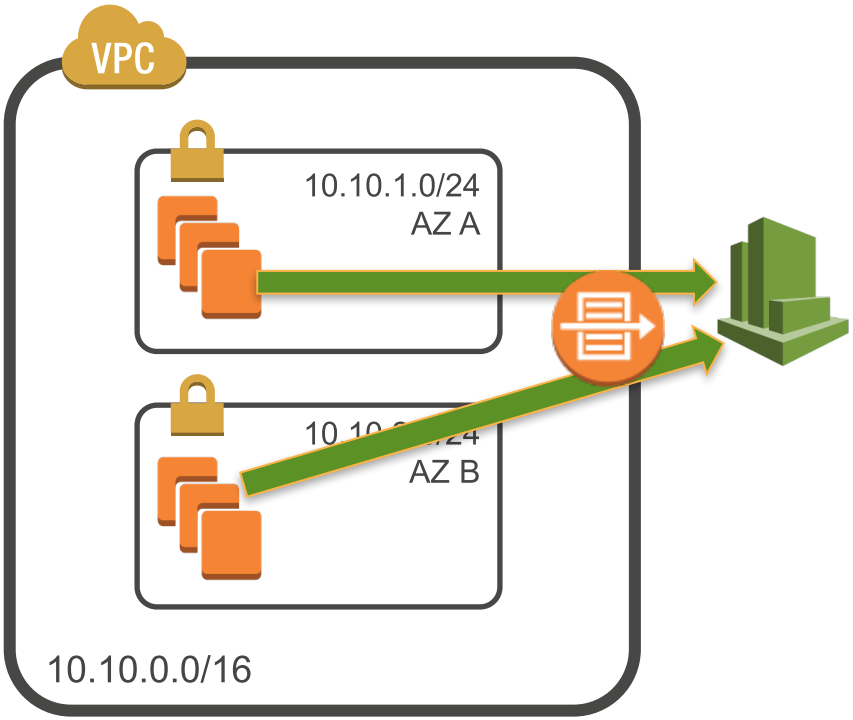


Amazon Route 53 private hosted zones



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

You can create 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 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 4795 OK
16:48:01	2 280328680831 eni- 17 10.0.0.100 8080 4794 OK
16:48:01	2 280328680831 eni-19 117 10.0.0.100 8080 4793 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-19116 .239 10.0.0.117 56978 8080 6 5 373 50081 1474750133 ACCEPT
16:48:01	2 280328680831 eni-19116c4 0.117 10.0.1.239 8080 56950 6 5 650 1 750081 1474750133 ACCEPT
16:48:01	2 280328680831 eni-19116c47 .0.117 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?

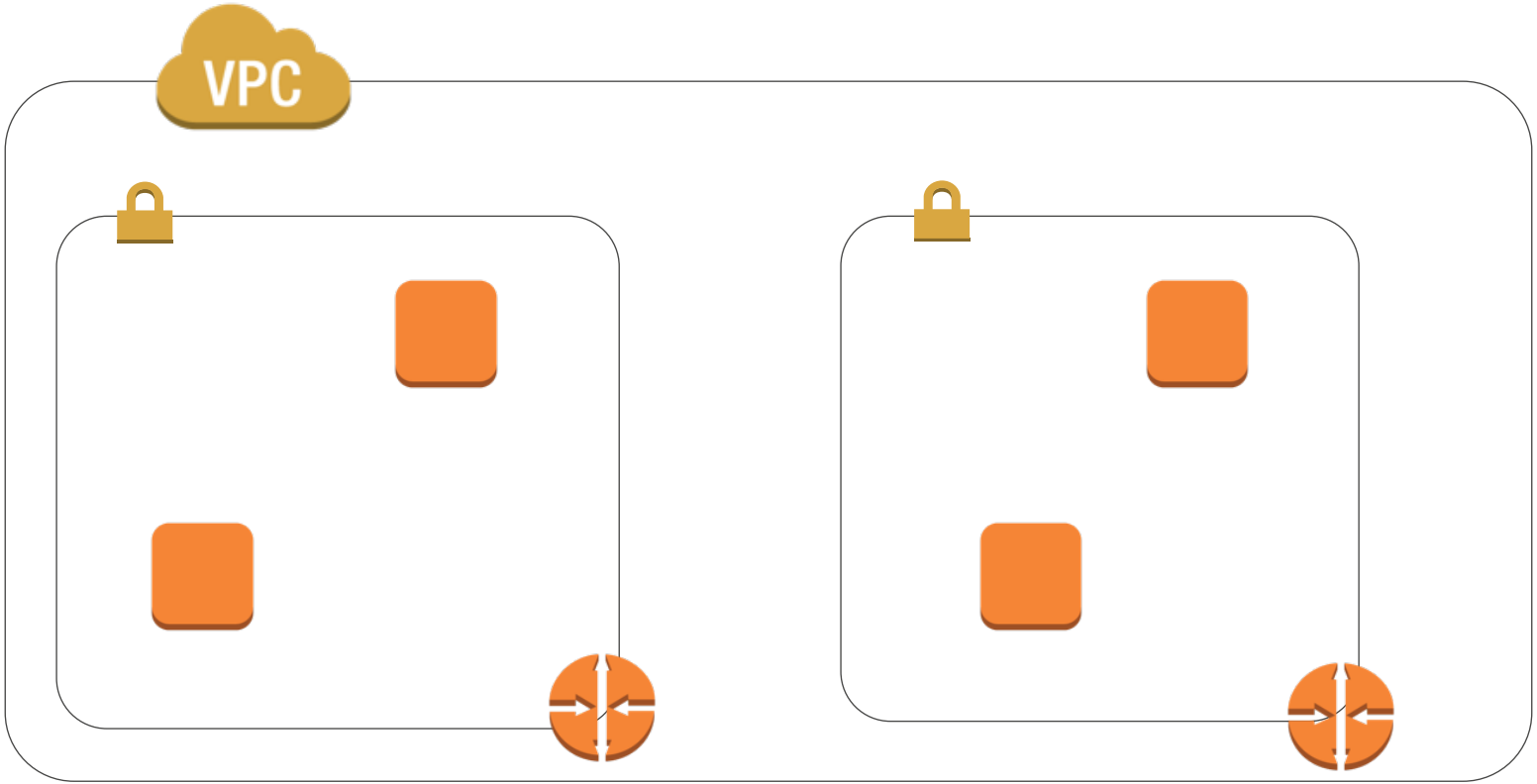
```
# dig +short -x 109.236.86.32
internetpolice.co.
```

UDP Port 53 = DNS

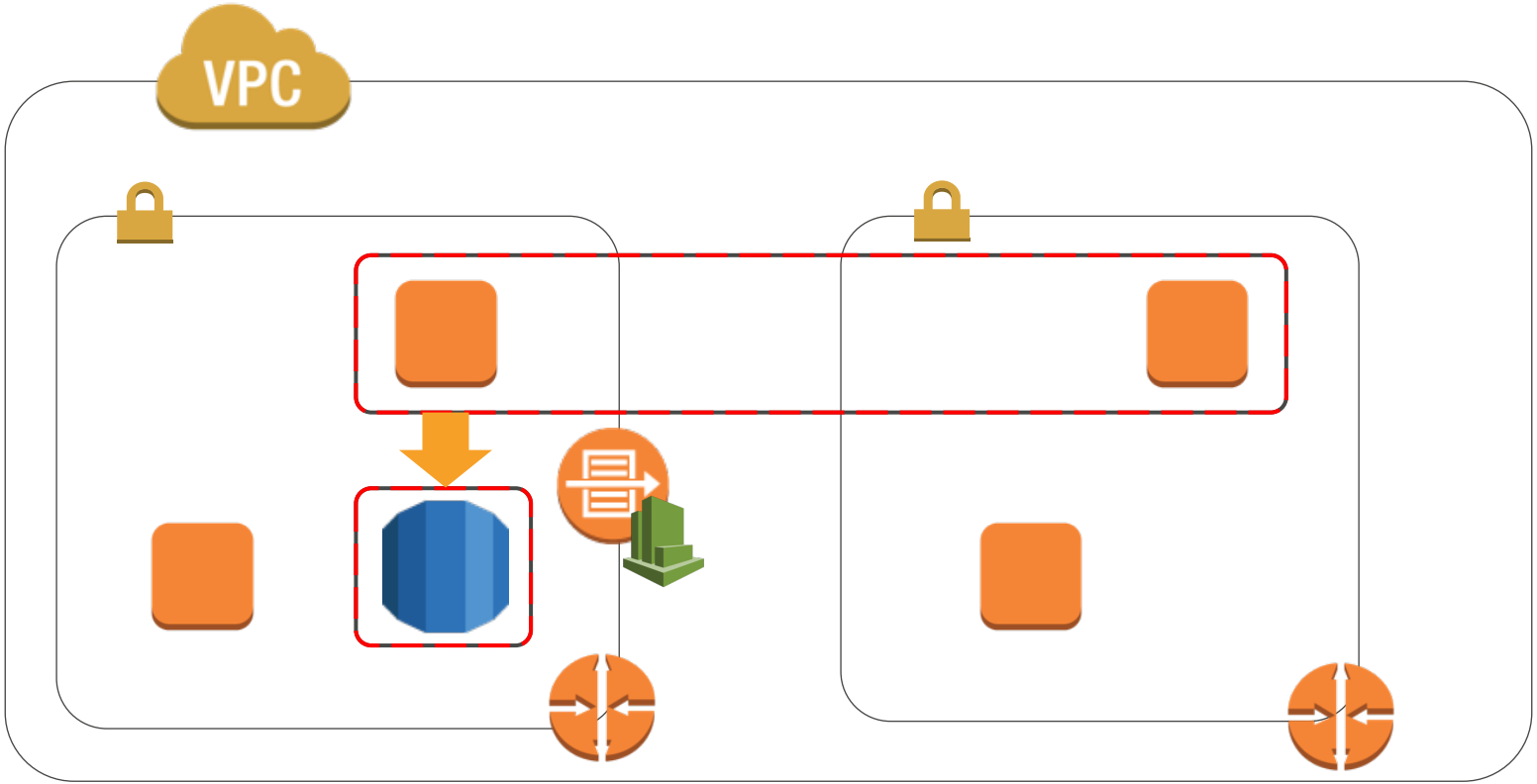
REJECT

VPC: your private network in AWS

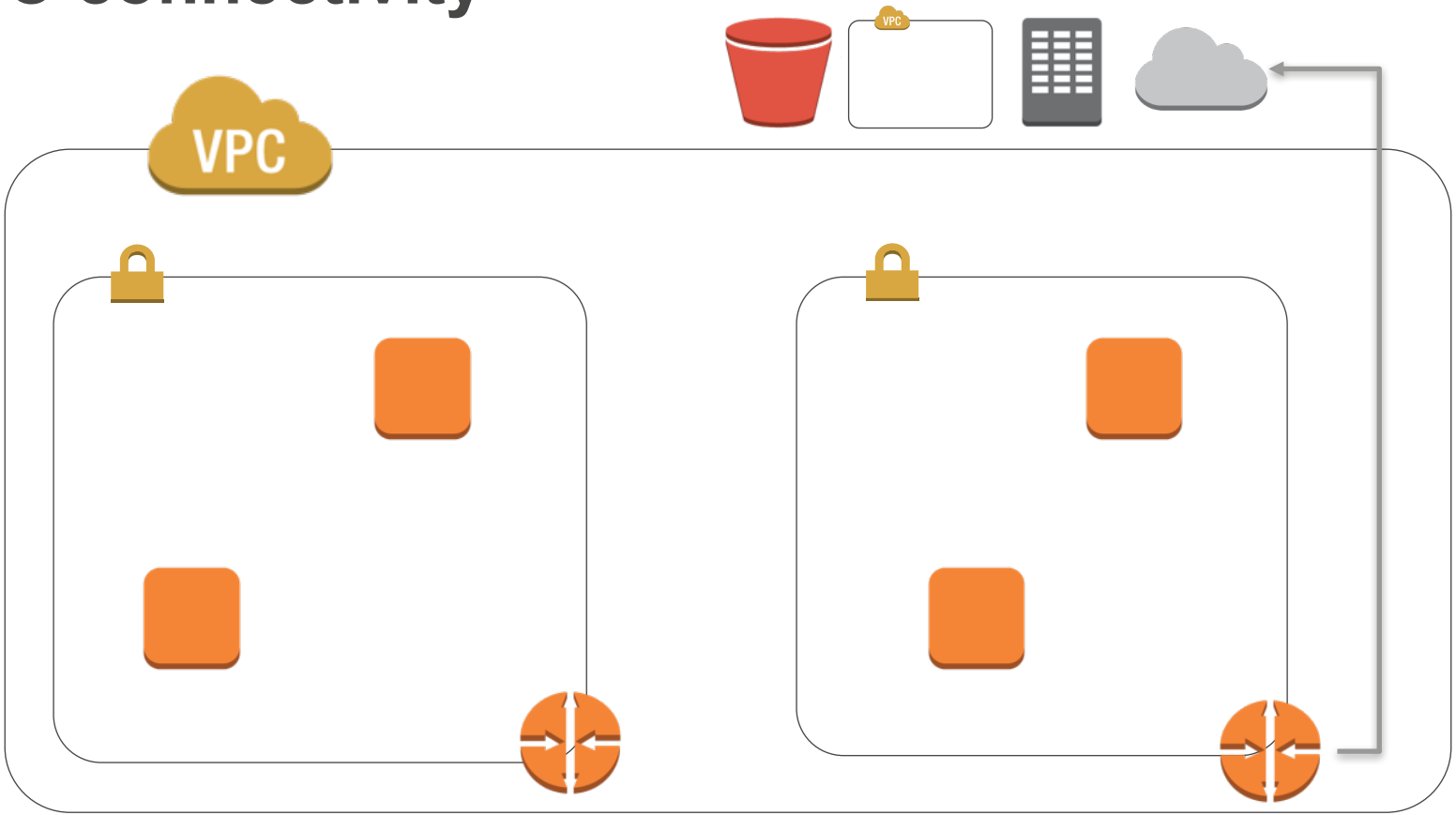
The VPC network



VPC network security



VPC connectivity



amazon web services | Pop-up Loft LONDON

Thank you!

Steve Seymour
Principal Solutions Architect

@sseymour