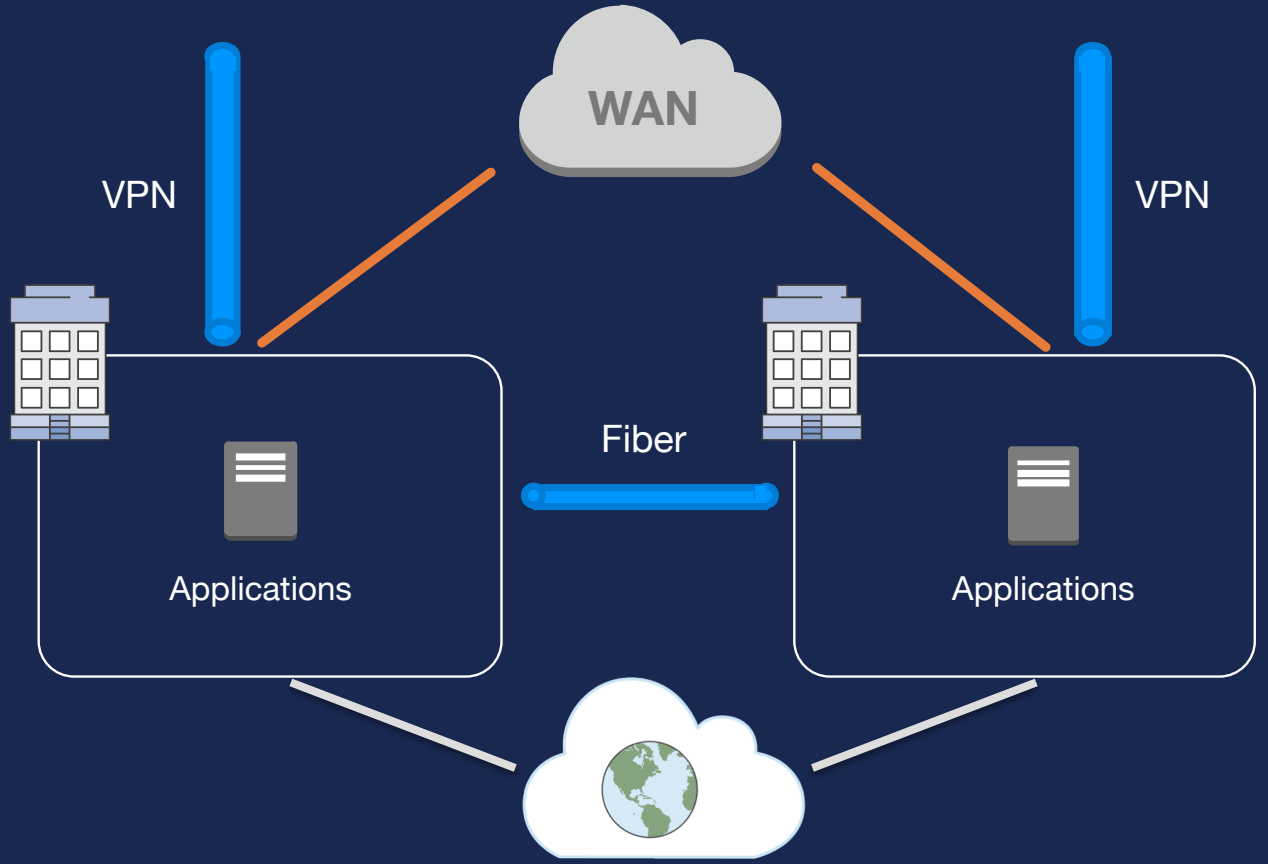
aws SUMMIT

AWS Networking Fundamentals

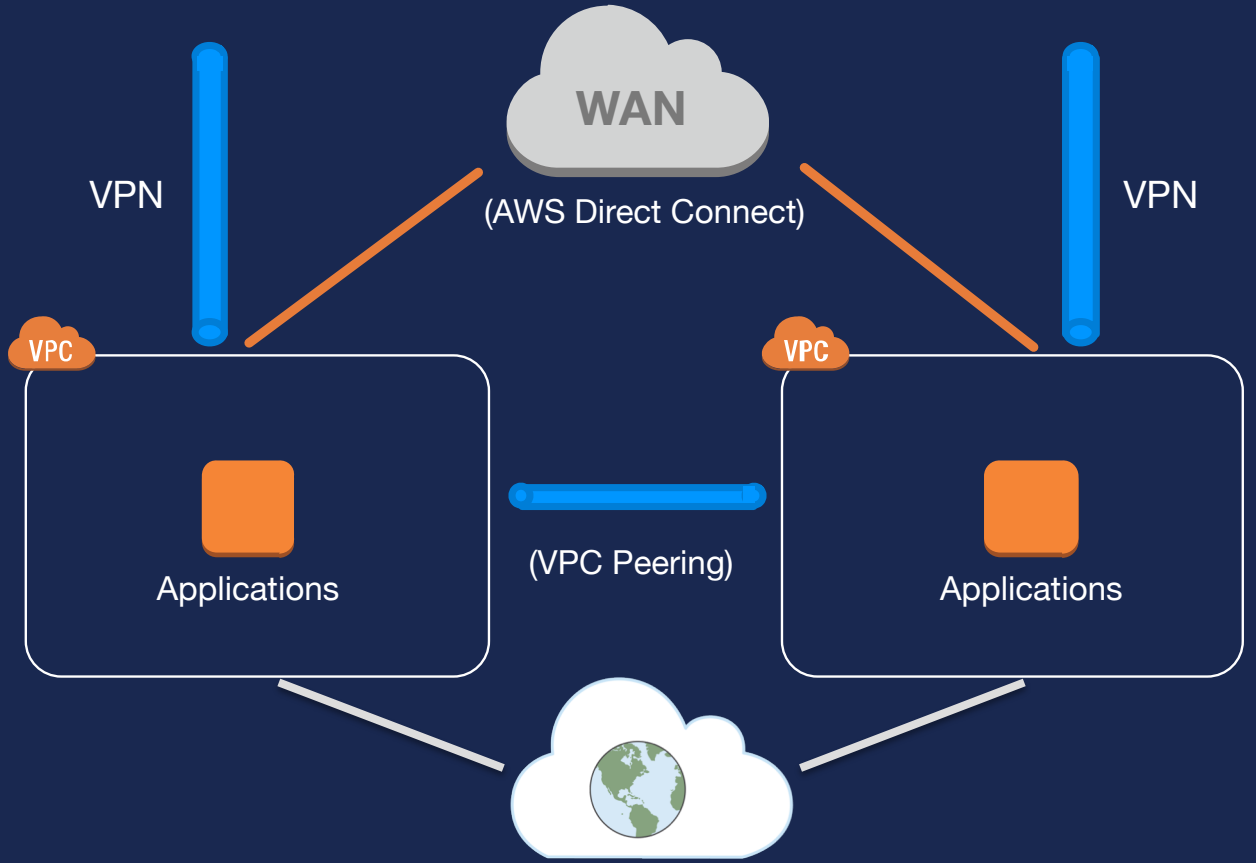
Tom Adamski

Specialist Solutions Architect, AWS

Traditional Network

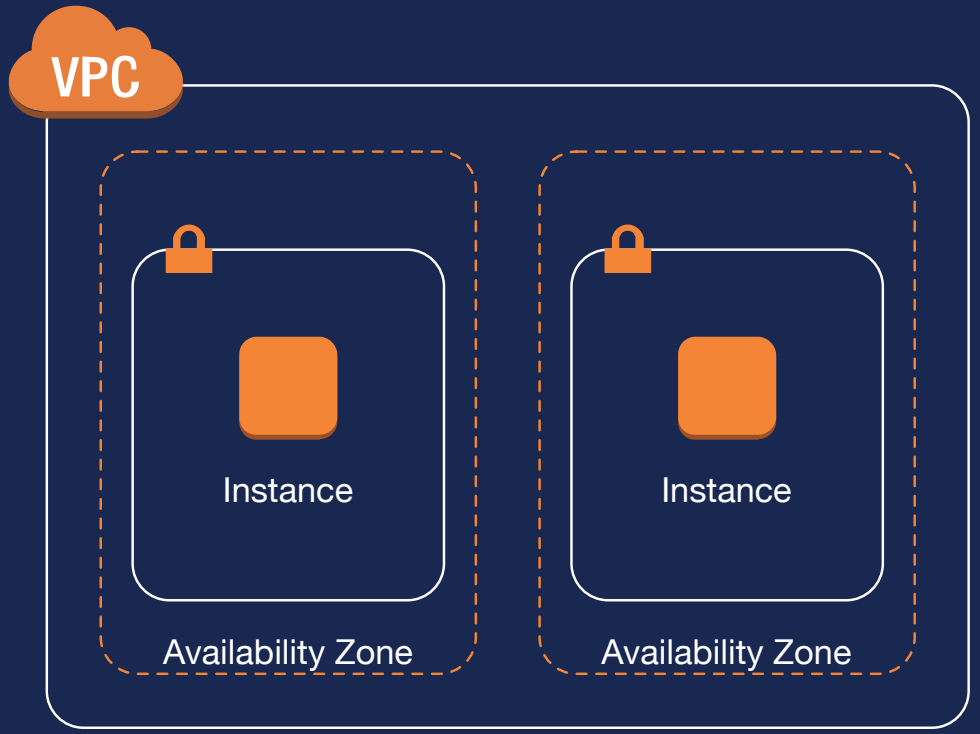


AWS Network



What is an Amazon Virtual Private Cloud (VPC)?

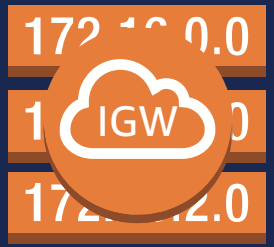
"A virtual network that closely resembles a traditional network that you'd operate in your own data center"



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

Choosing an IP 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
(65,536 addresses)

IPv6 in Amazon VPC – Dual-stack

172.31.0.0/16

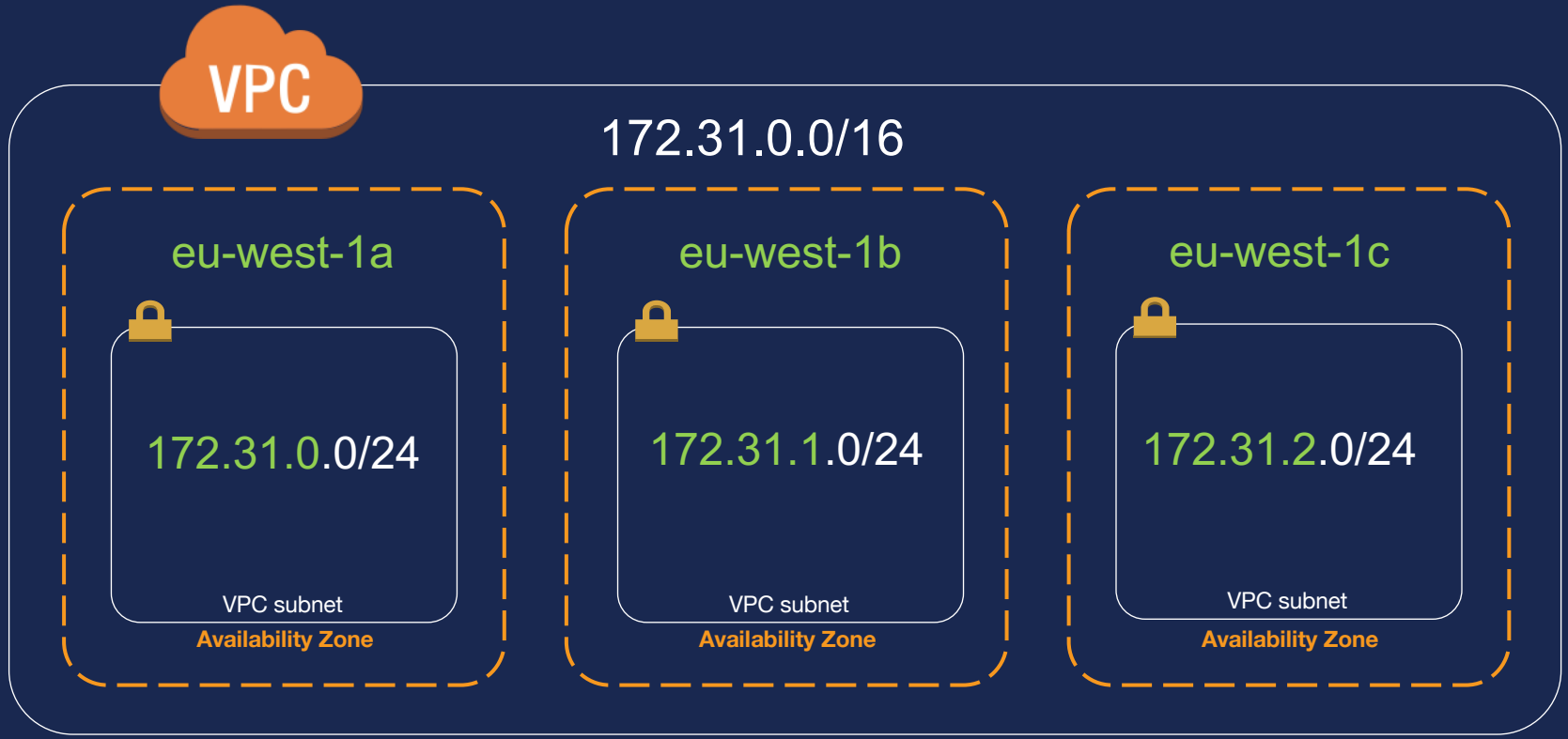
2001:db8:1234:1a00::/56

Amazon Global Unicast Addresses (GUA) – Internet Routable

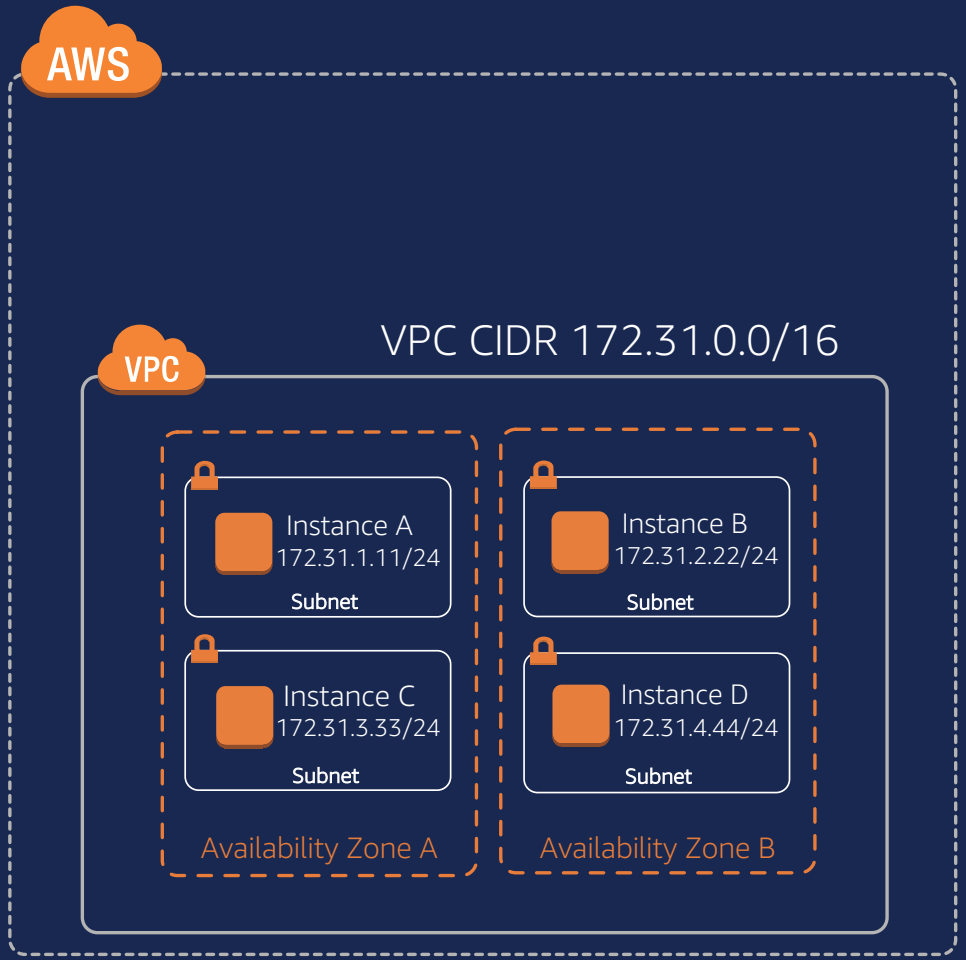
Associate an /56 IPv6 CIDR (Automatically allocated)

Subnets

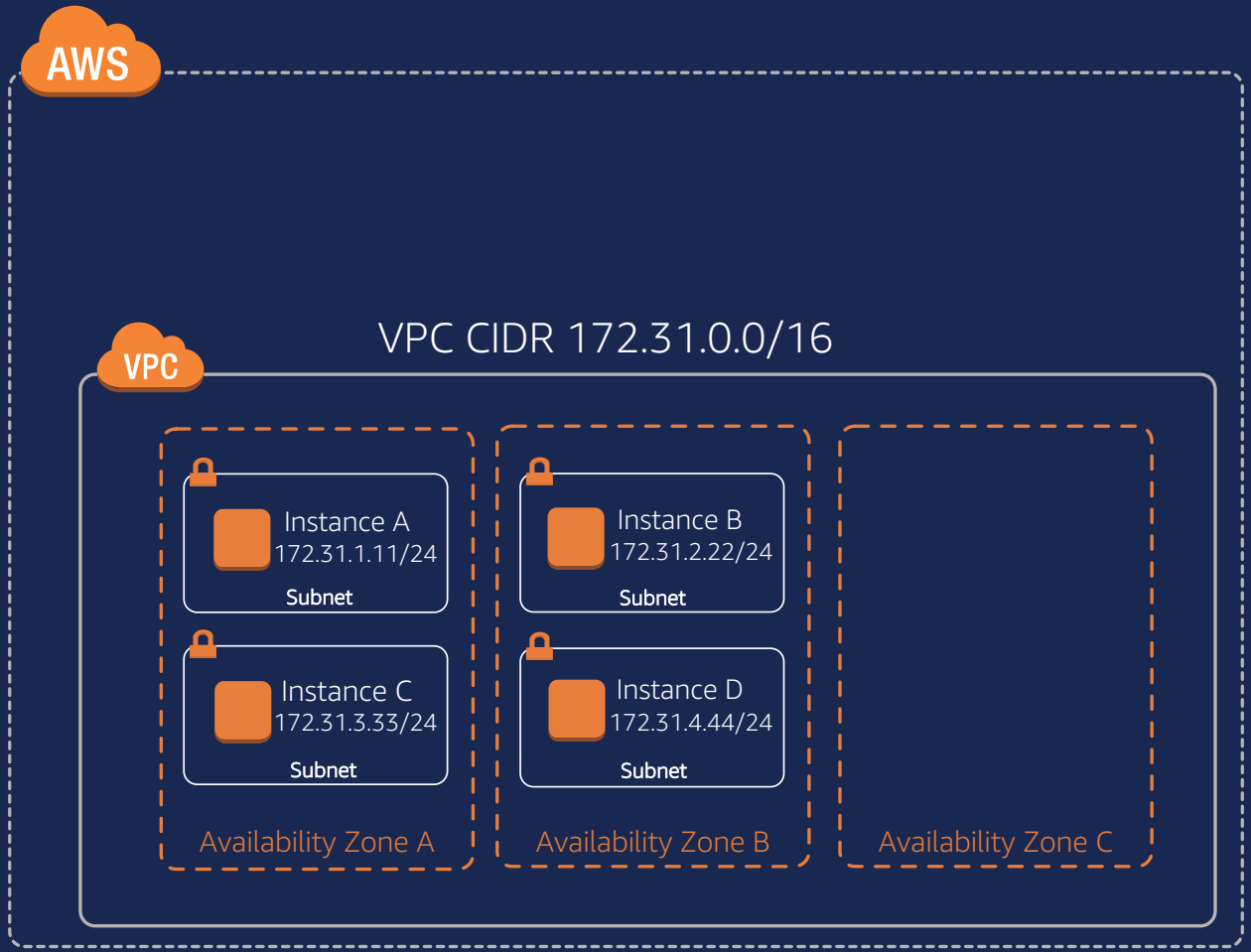
VPC subnets and Availability Zones



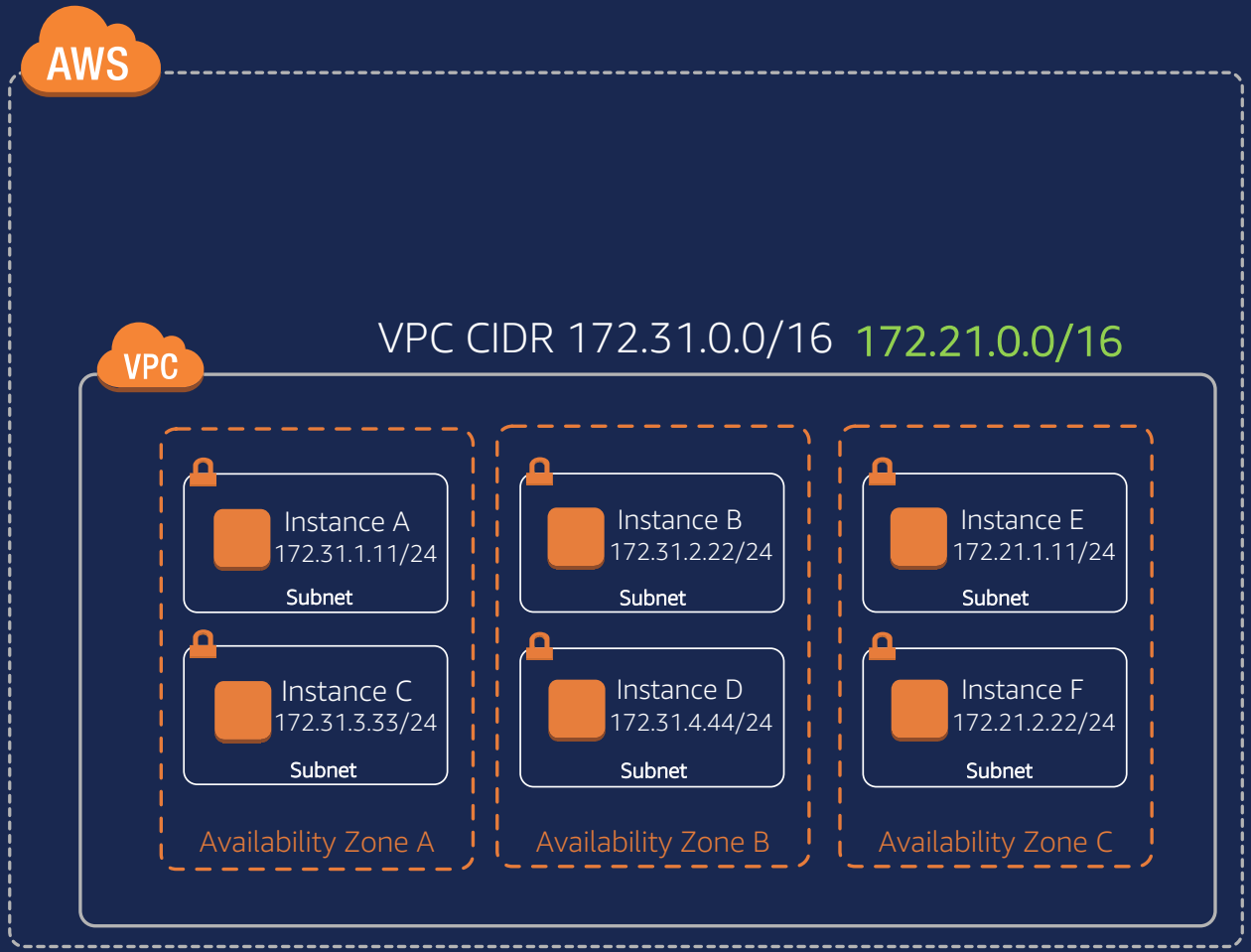
Expand your existing Amazon VPC



Initial VPC CIDR: 172.31.0.0/16



Initial VPC CIDR:
172.31.0.0/16



Initial VPC CIDR: 172.31.0.0/16

Additional VPC CIDR: 172.21.0.0/16

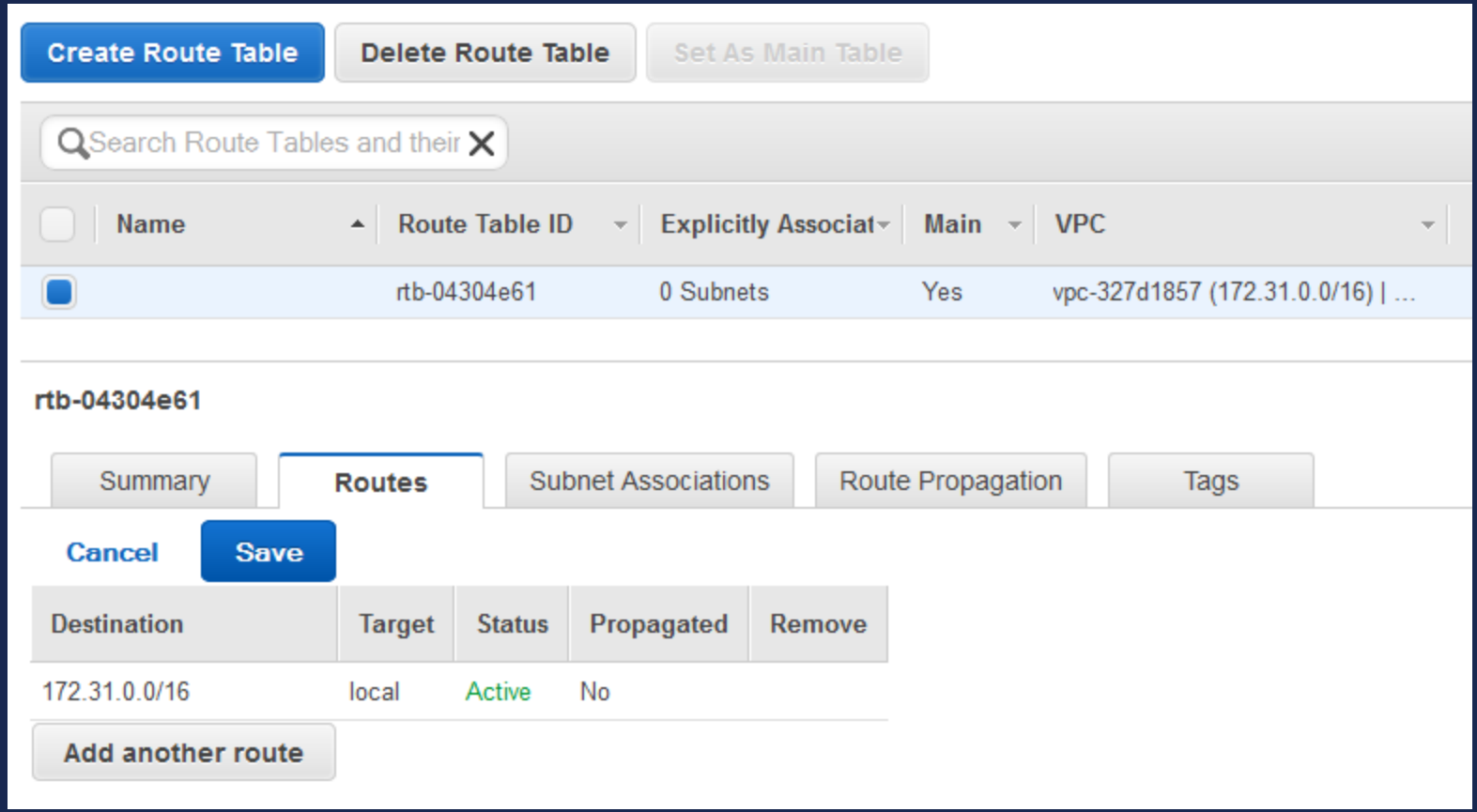
VPC subnet recommendations

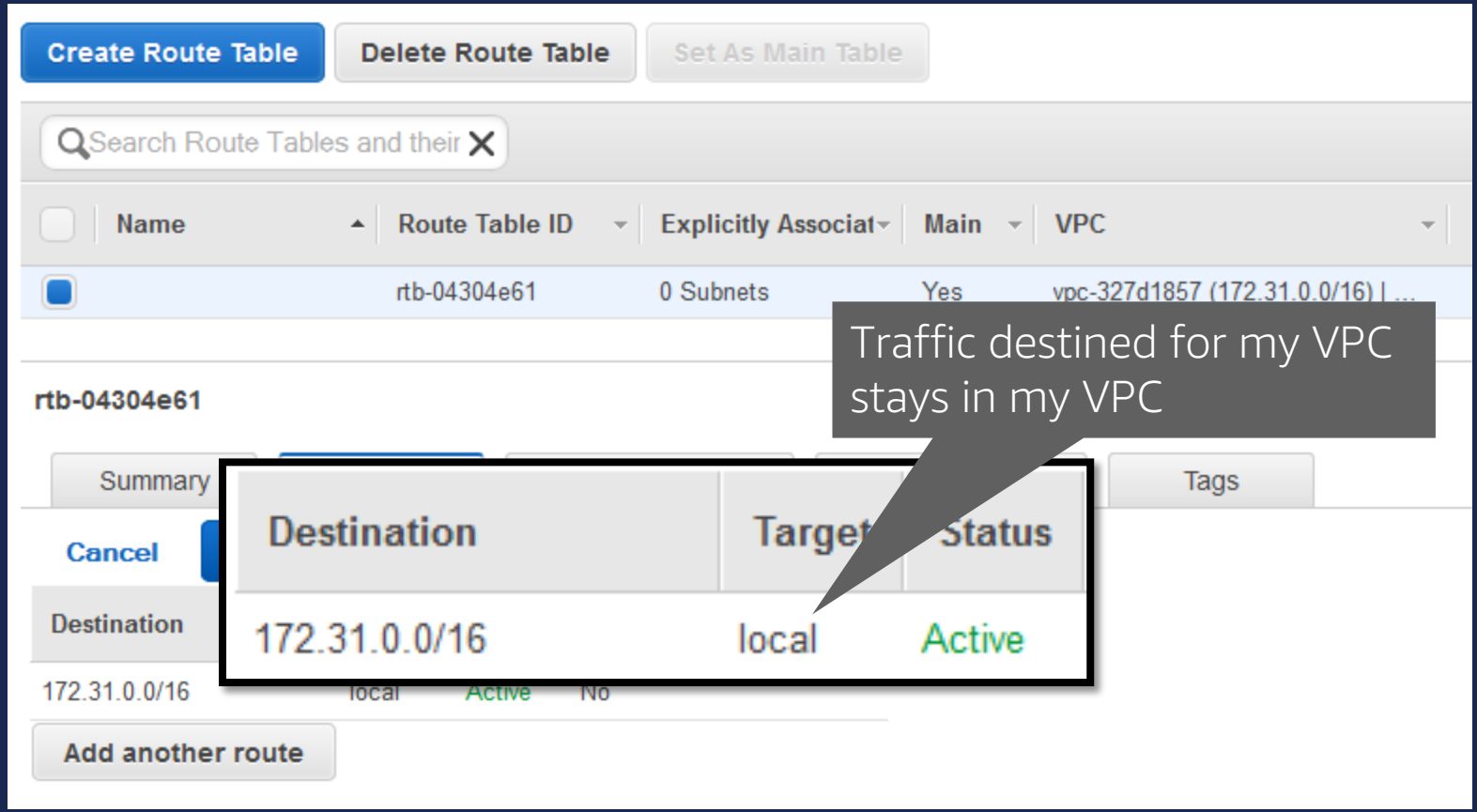
- /16 VPC (65,536 addresses)
- Expand your VPC when necessary
- At least /24 subnets (251 addresses)
- Use multiple Availability Zones per VPC through multiple subnets

Route to the Internet

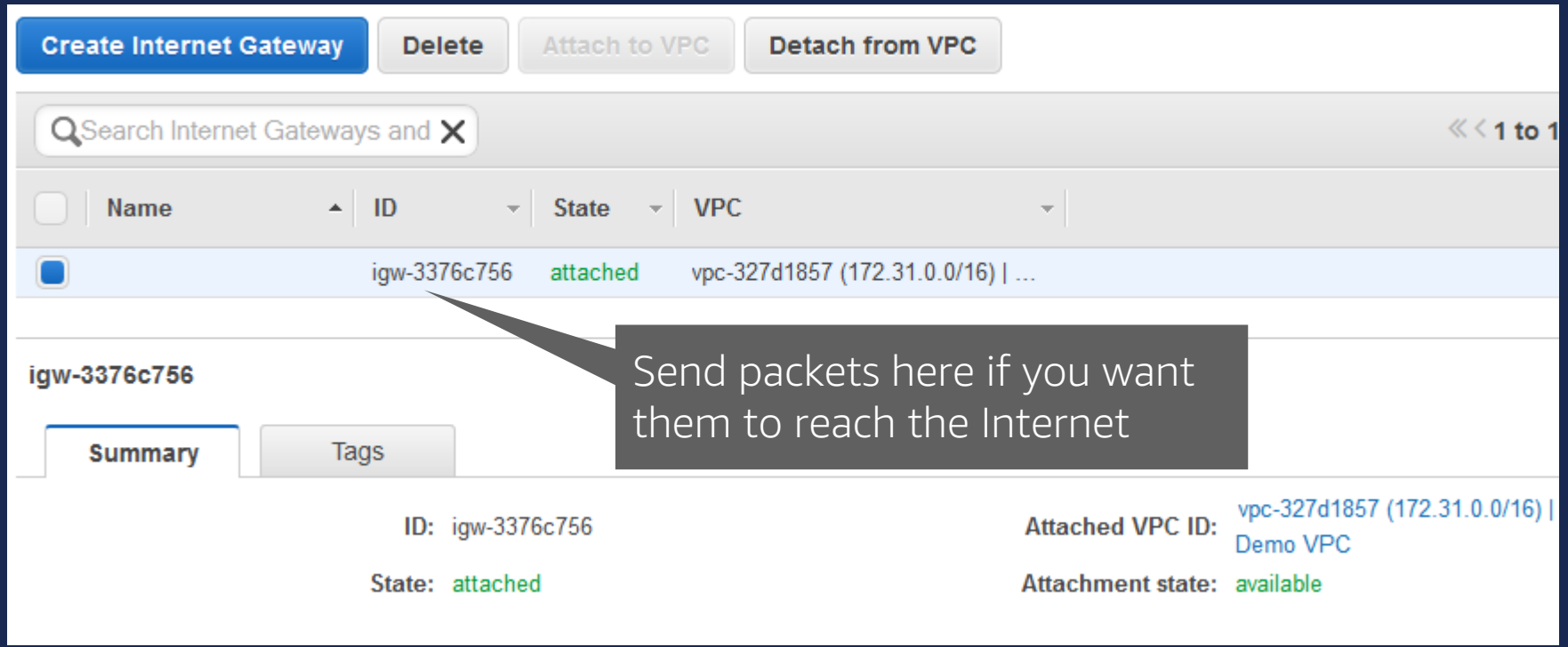
Routing in your VPC

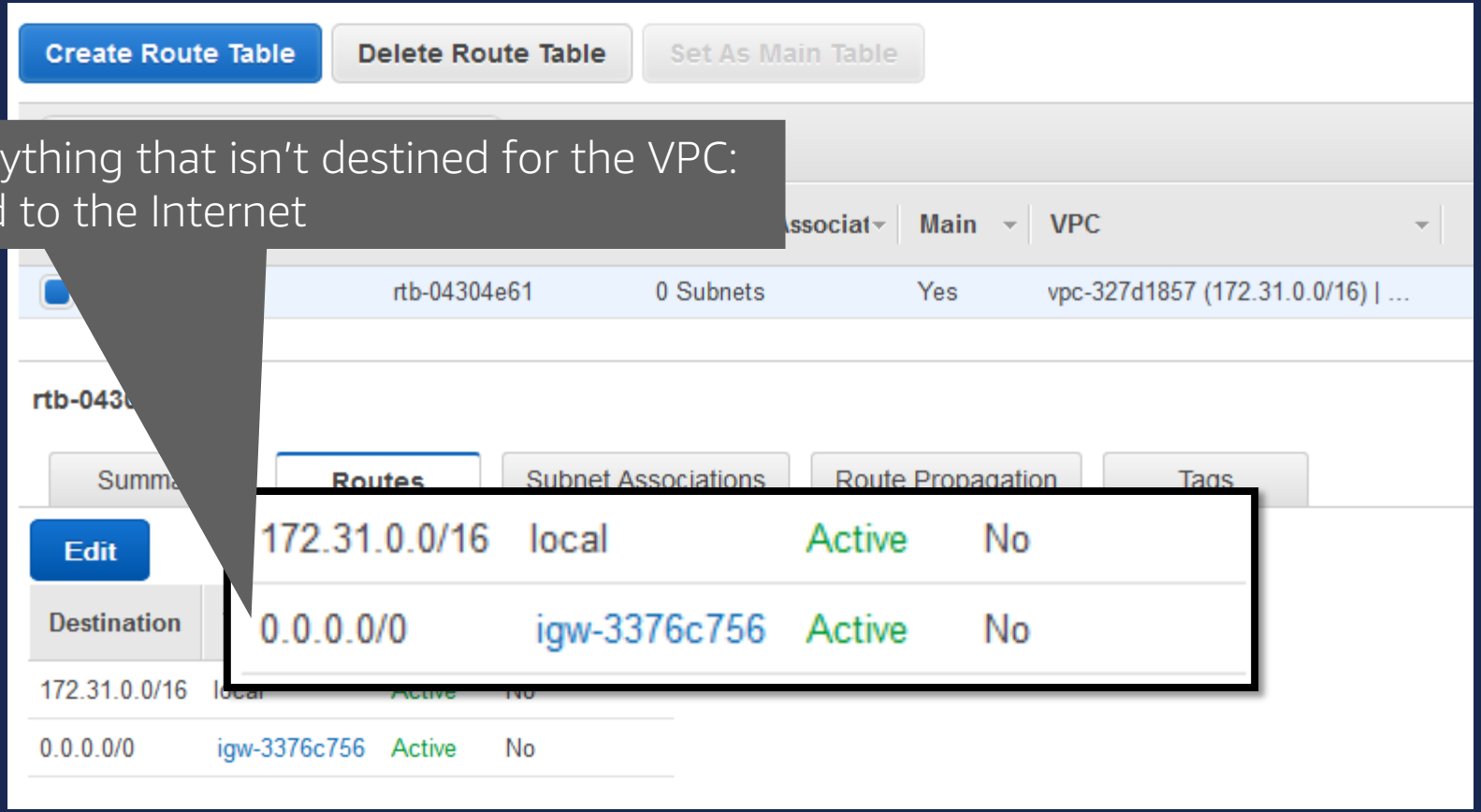
- Route tables contain rules for which packets go where
- Your VPC has a *default* (main) route table
- But, you can assign different route tables to different subnets





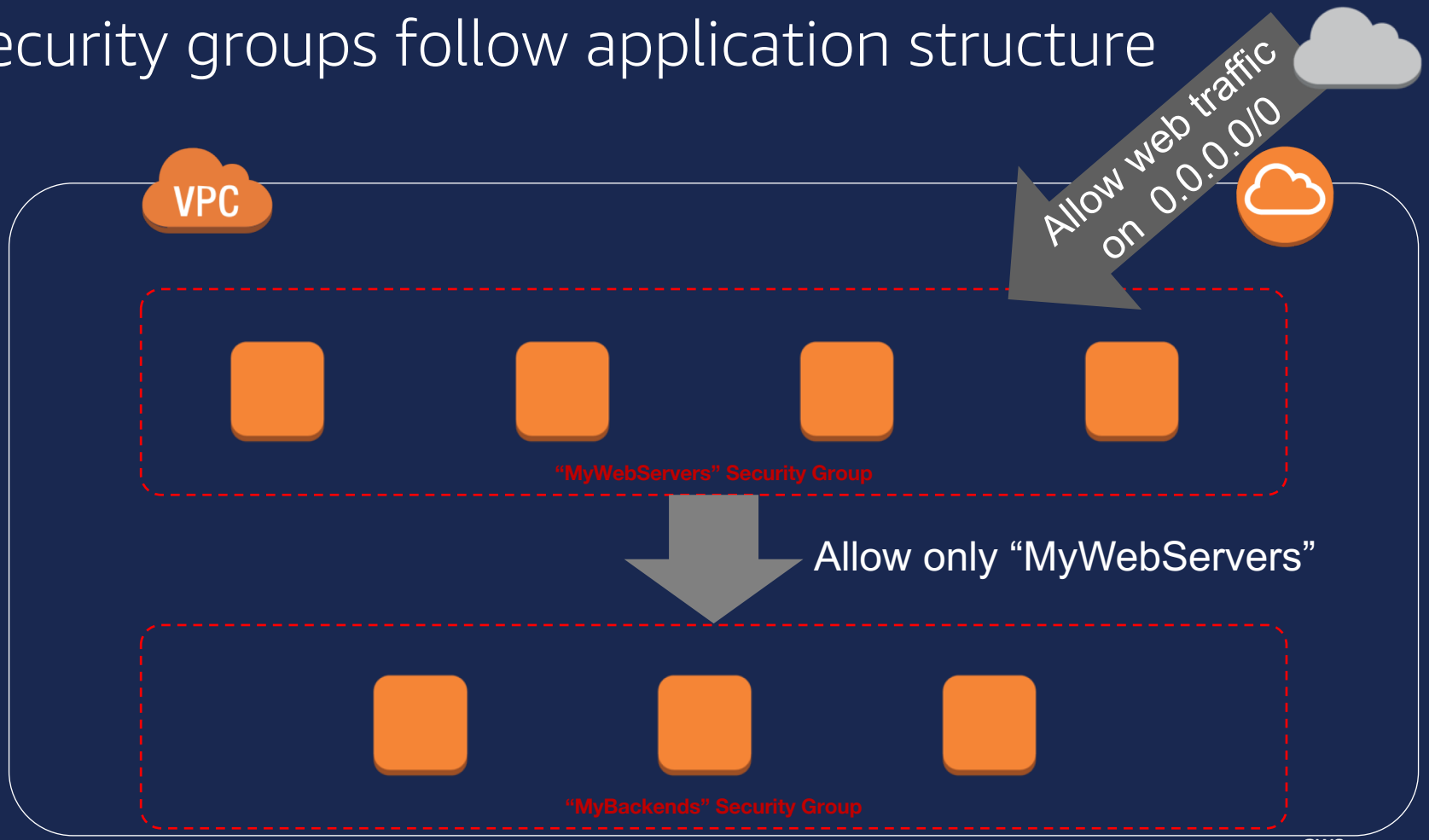
Internet gateway



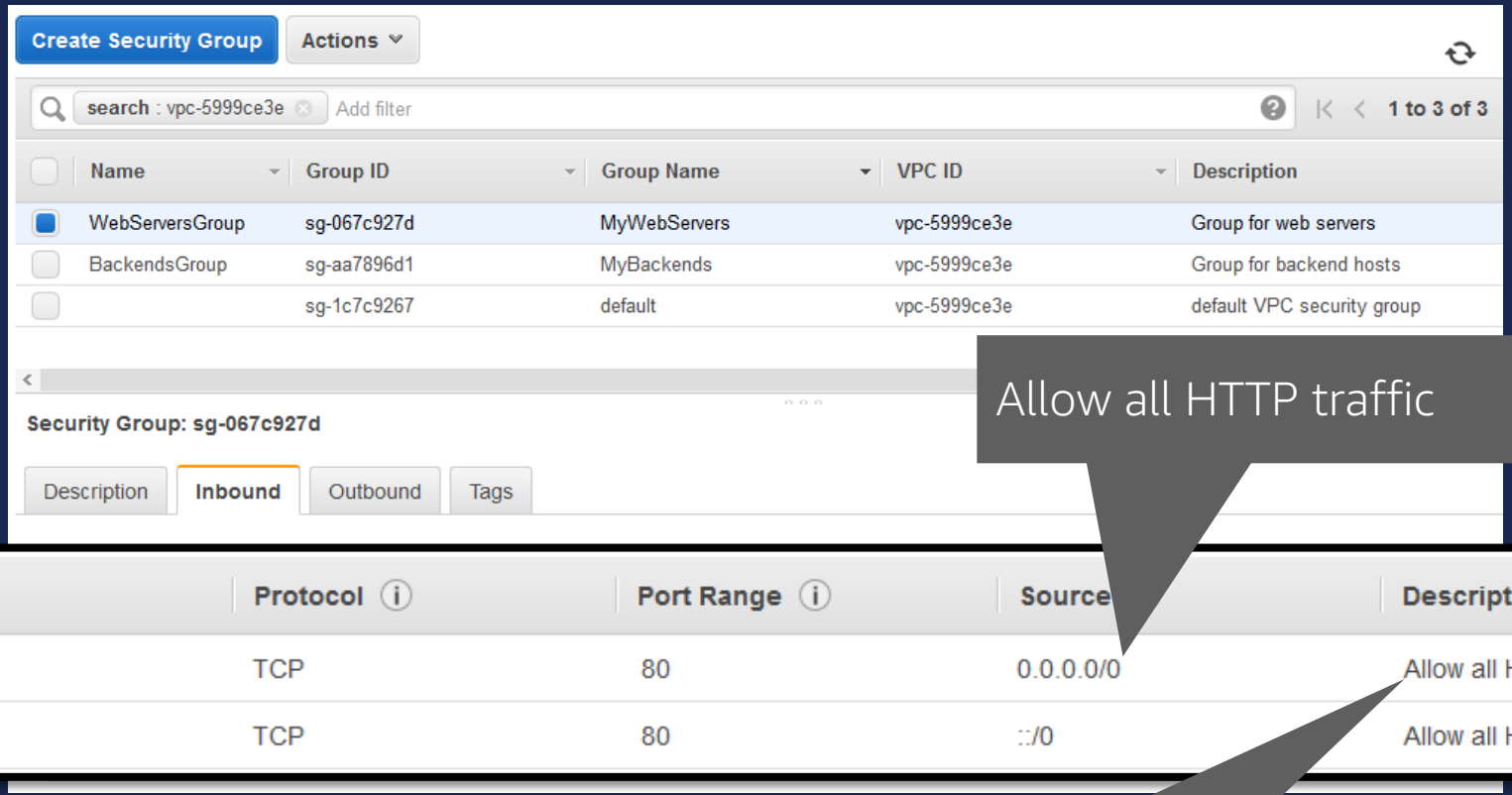


Network security in your VPC:
Security groups

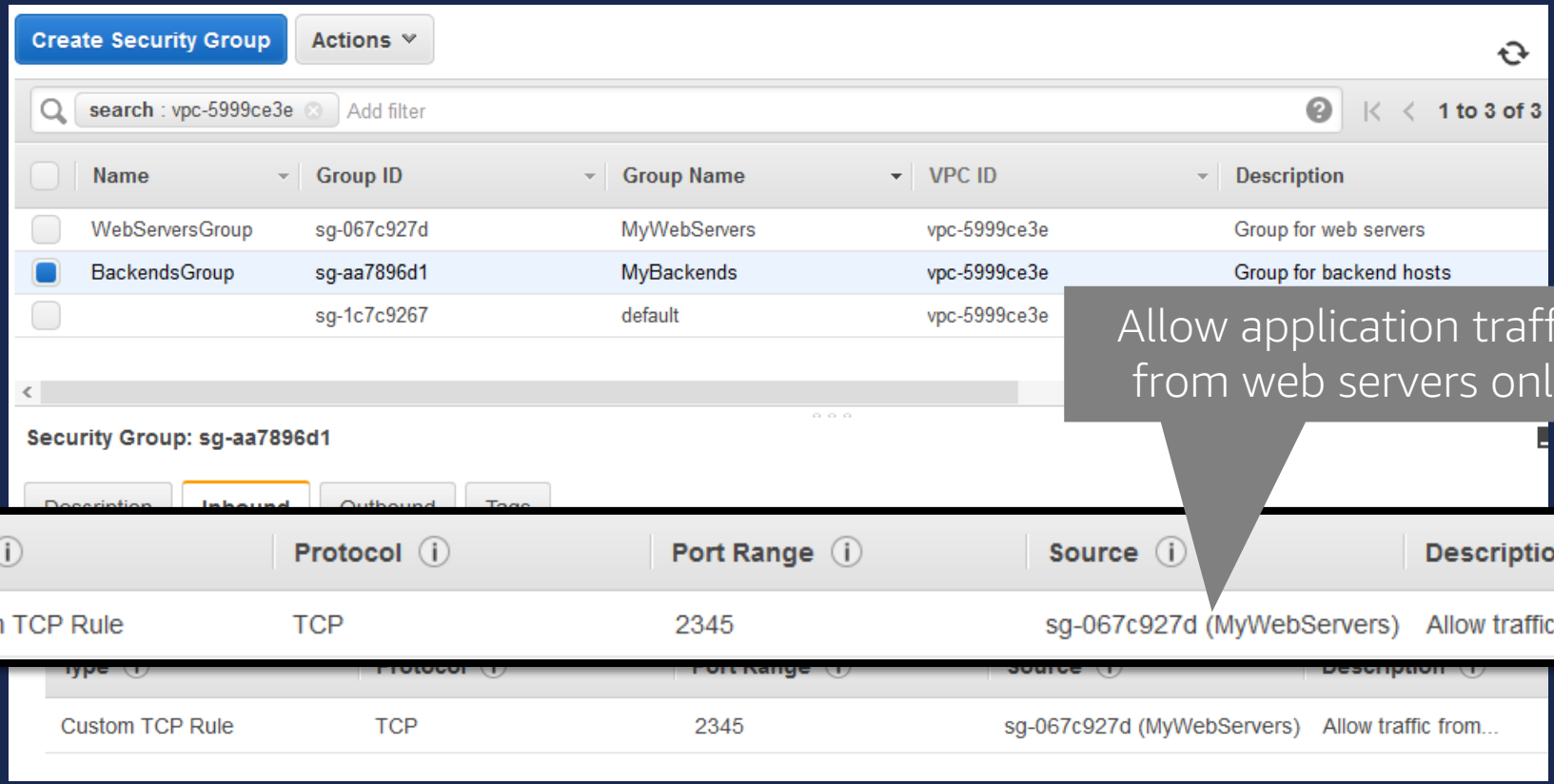
Security groups follow application structure



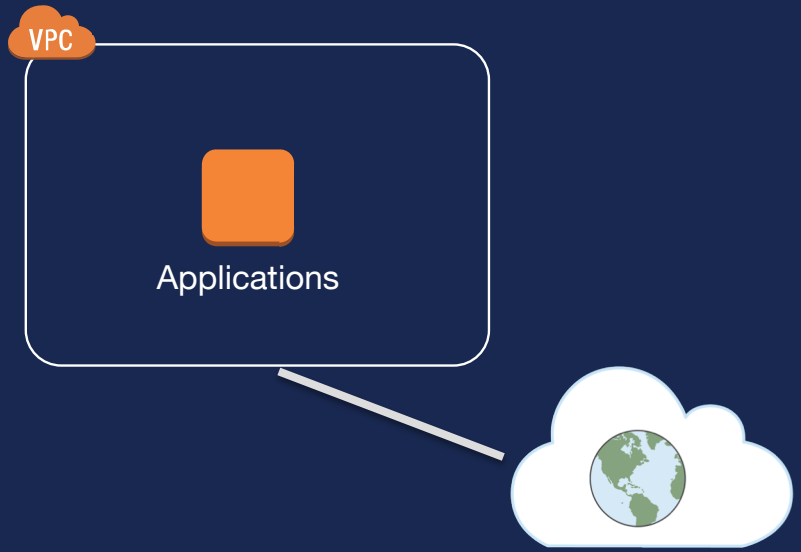
Security groups example: Web servers



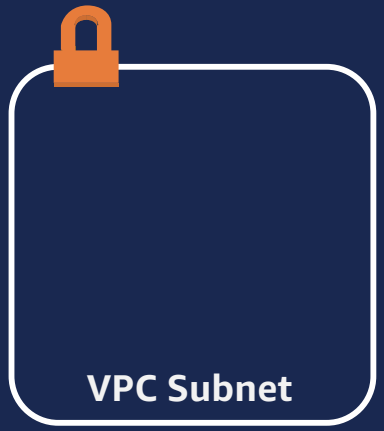
Security groups example: Backends



AWS Network - Progress

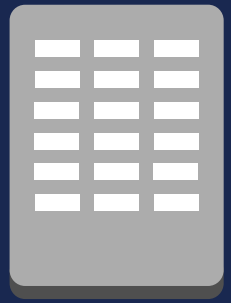


Beyond Internet connectivity

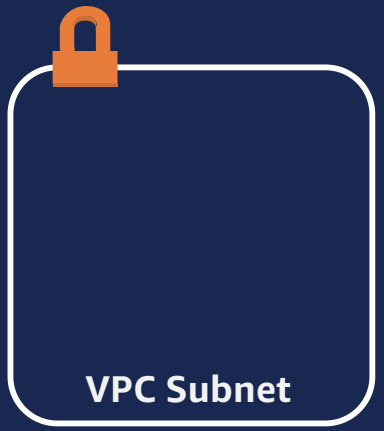


Restricting Internet access

Connecting to other VPCs

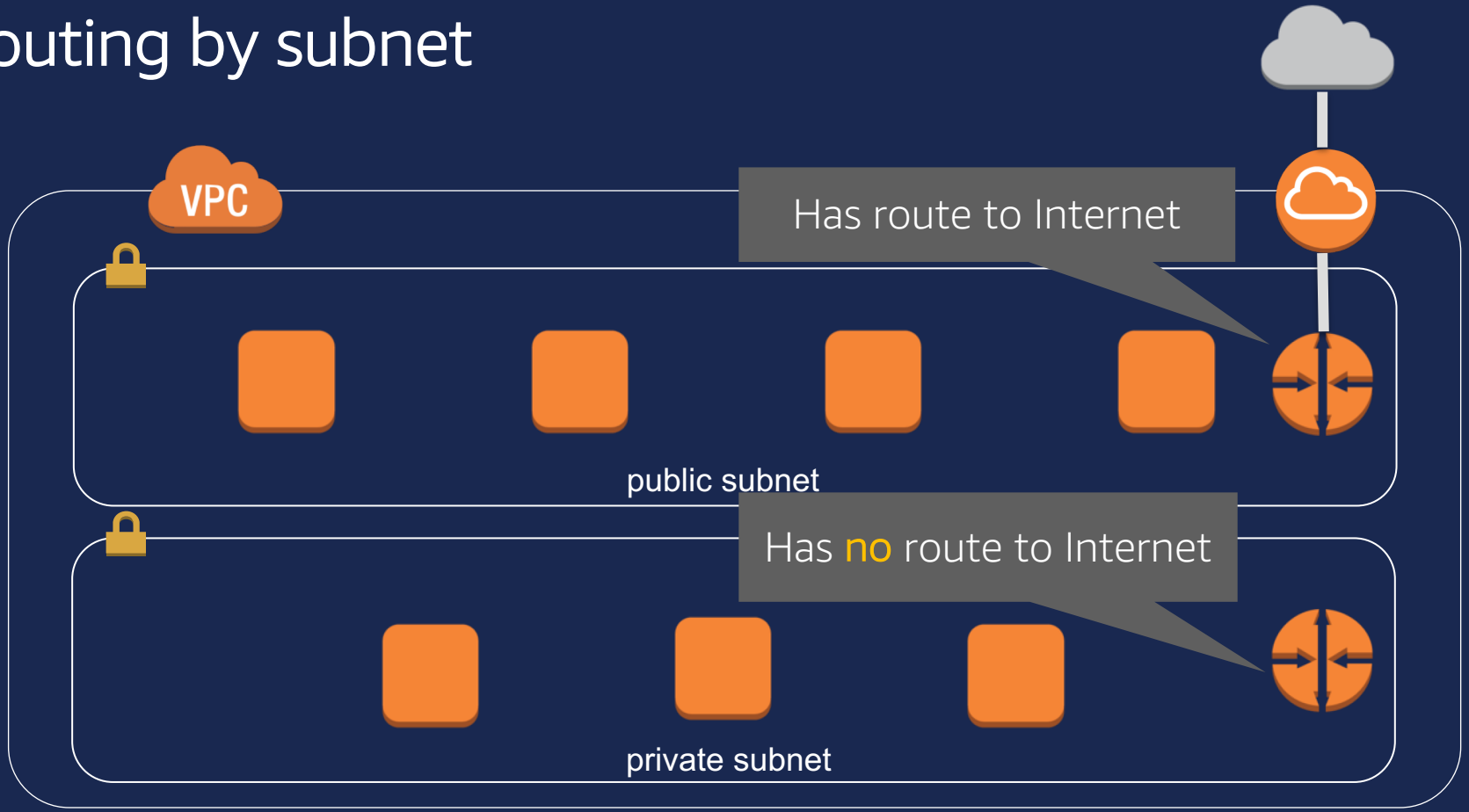


Connecting to your corporate network

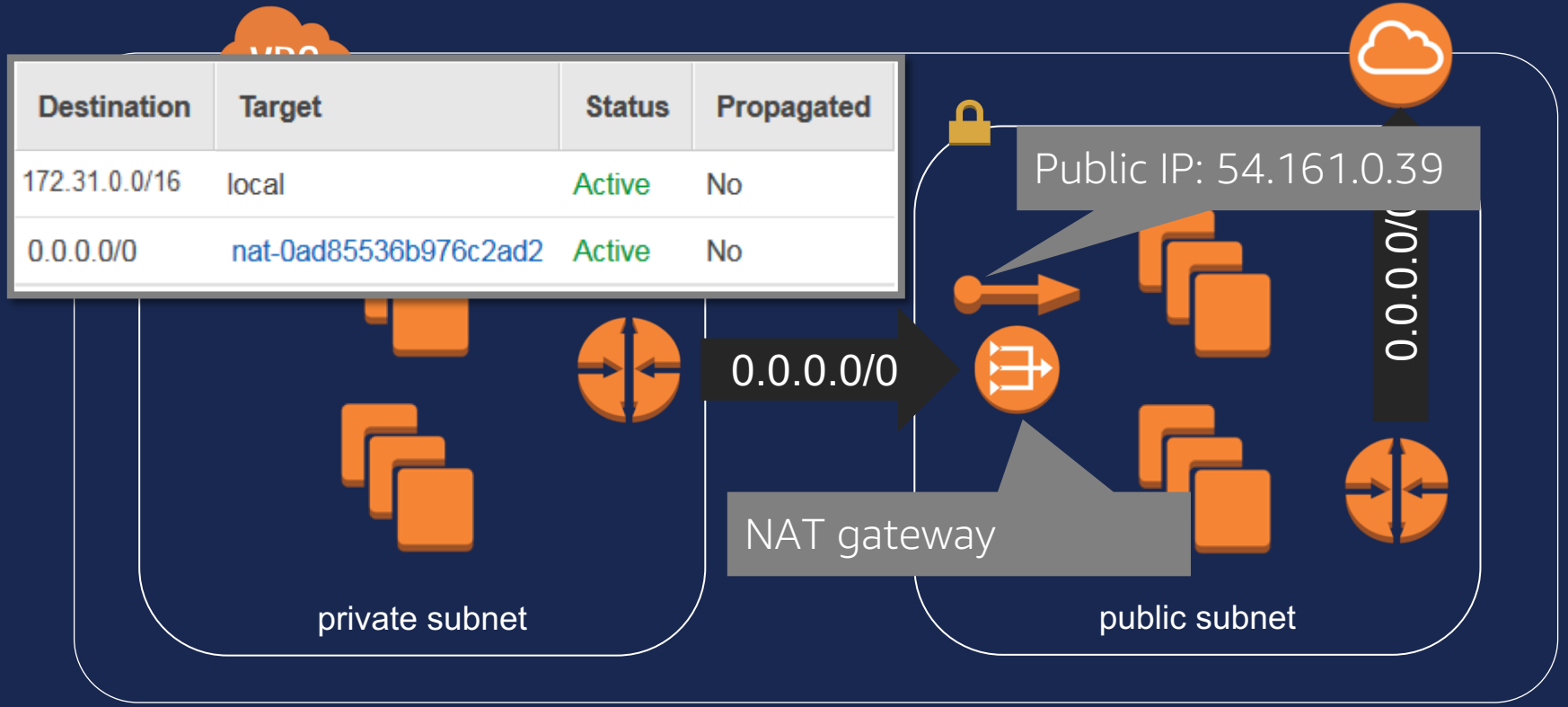


Restricting Internet access:
Routing by subnet

Routing by subnet



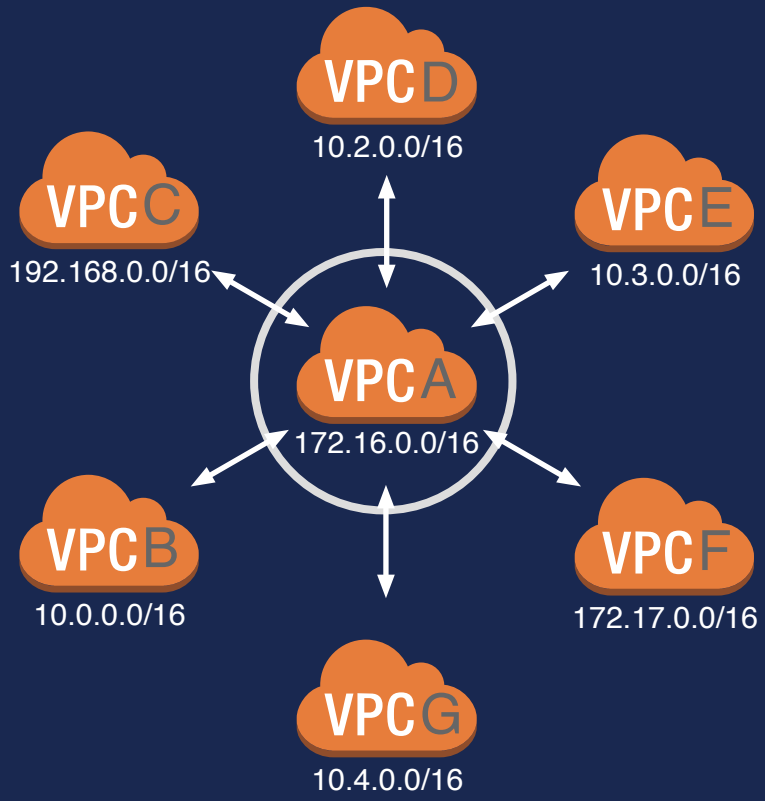
Outbound-only internet access: NAT gateway



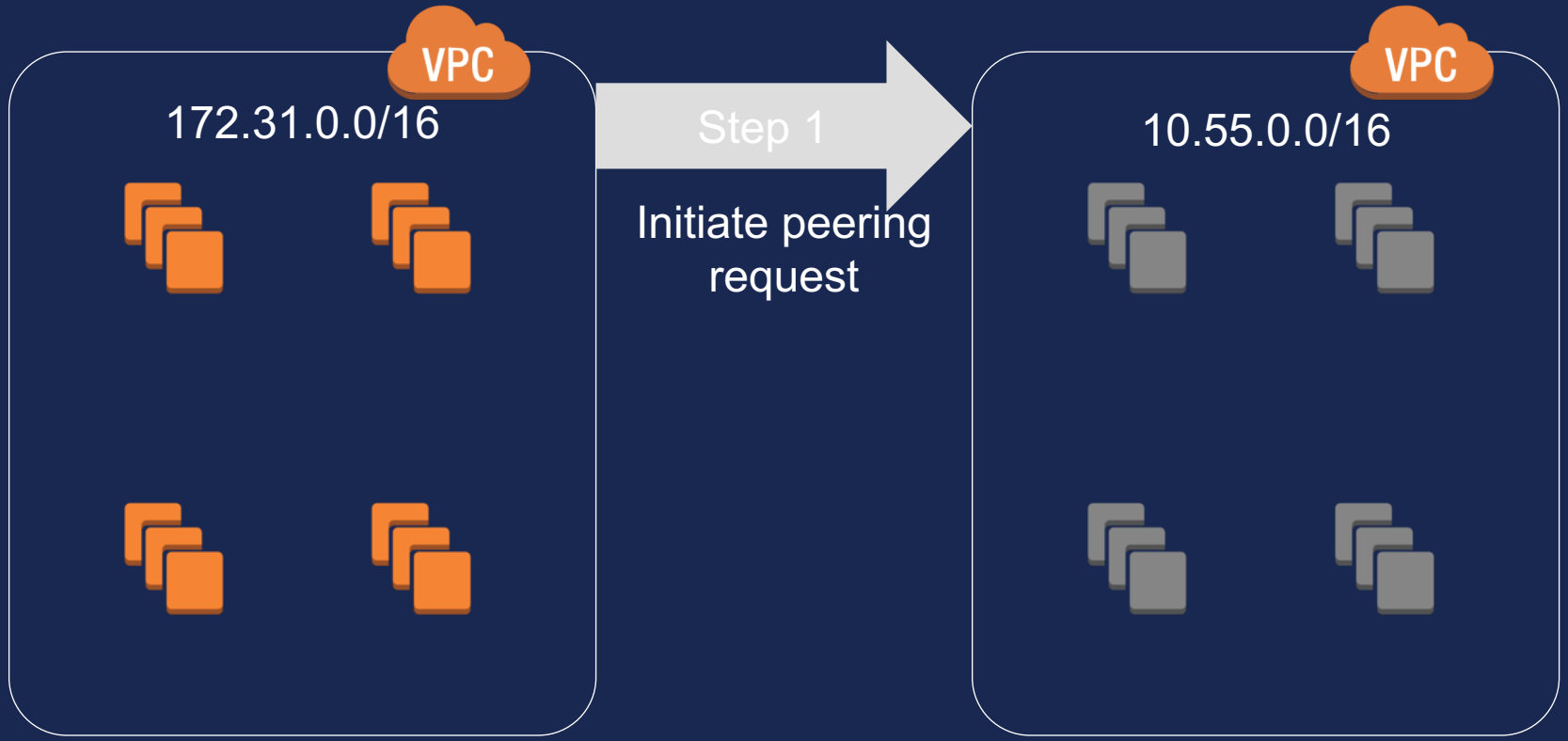
Inter-VPC connectivity:
VPC peering

Example VPC peering use:
Shared services VPC

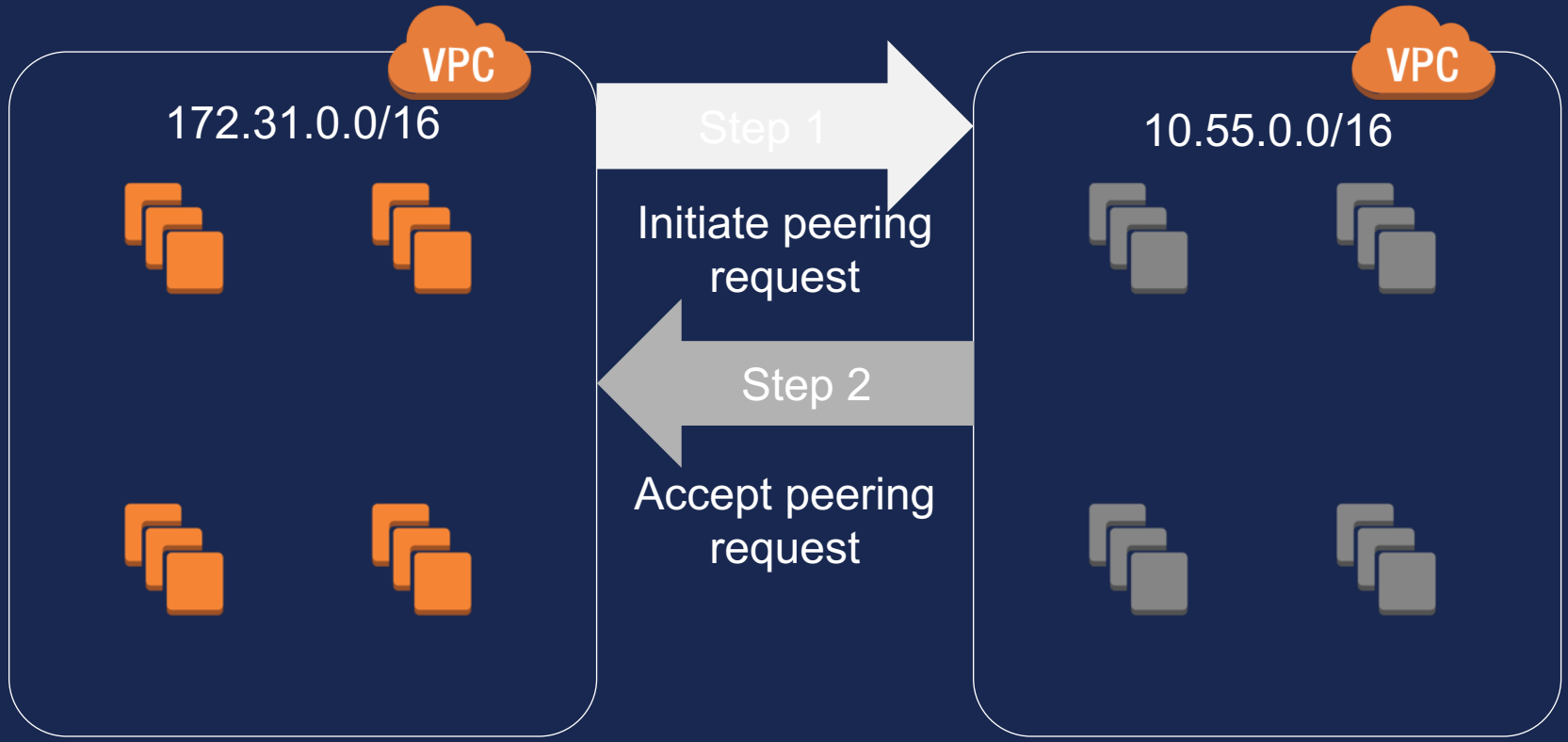
- Common/core services
  - Authentication/directory
  - Monitoring
  - Logging
  - Remote administration
  - Scanning



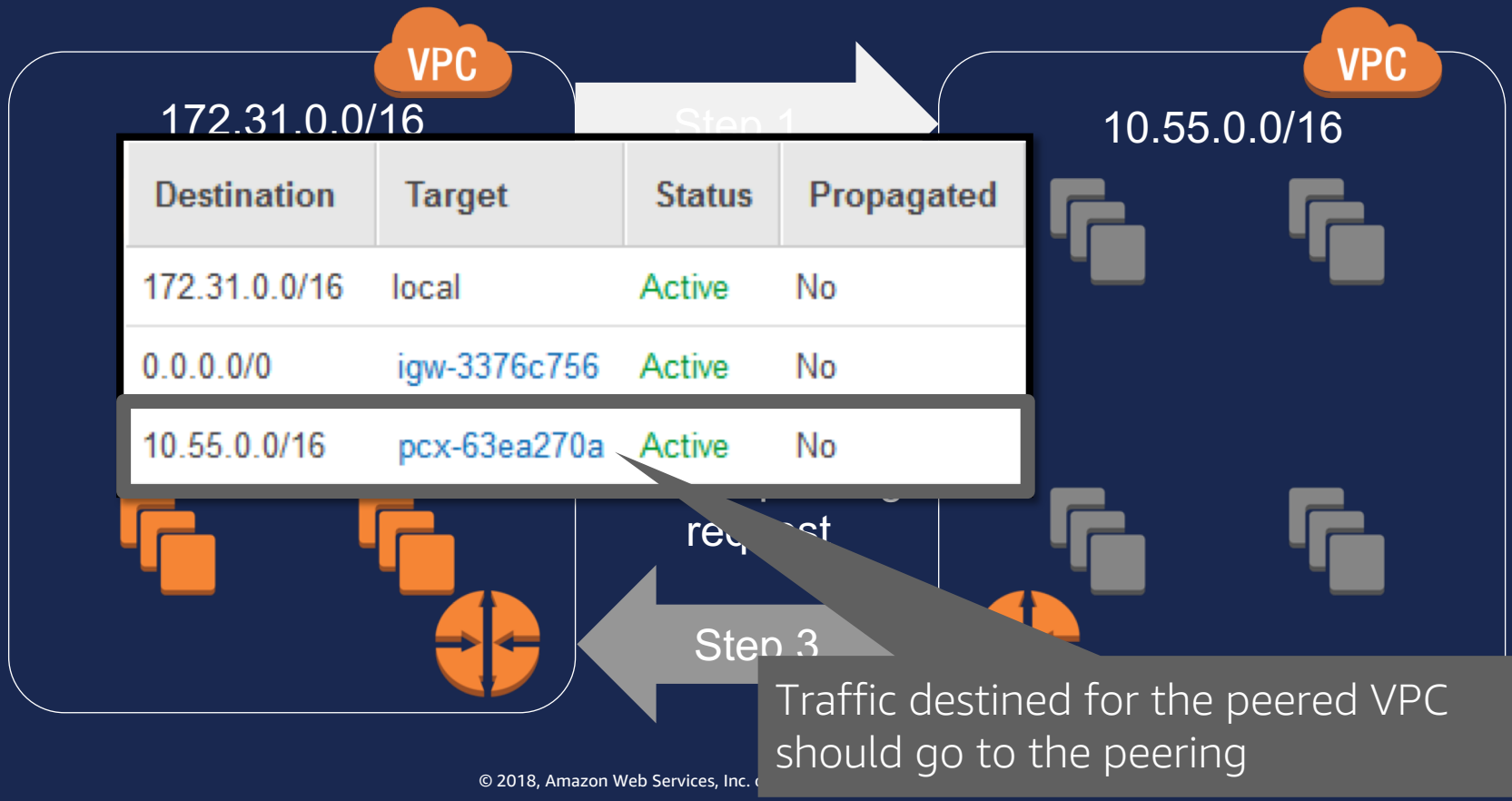
Establish a VPC peering: Initiate request



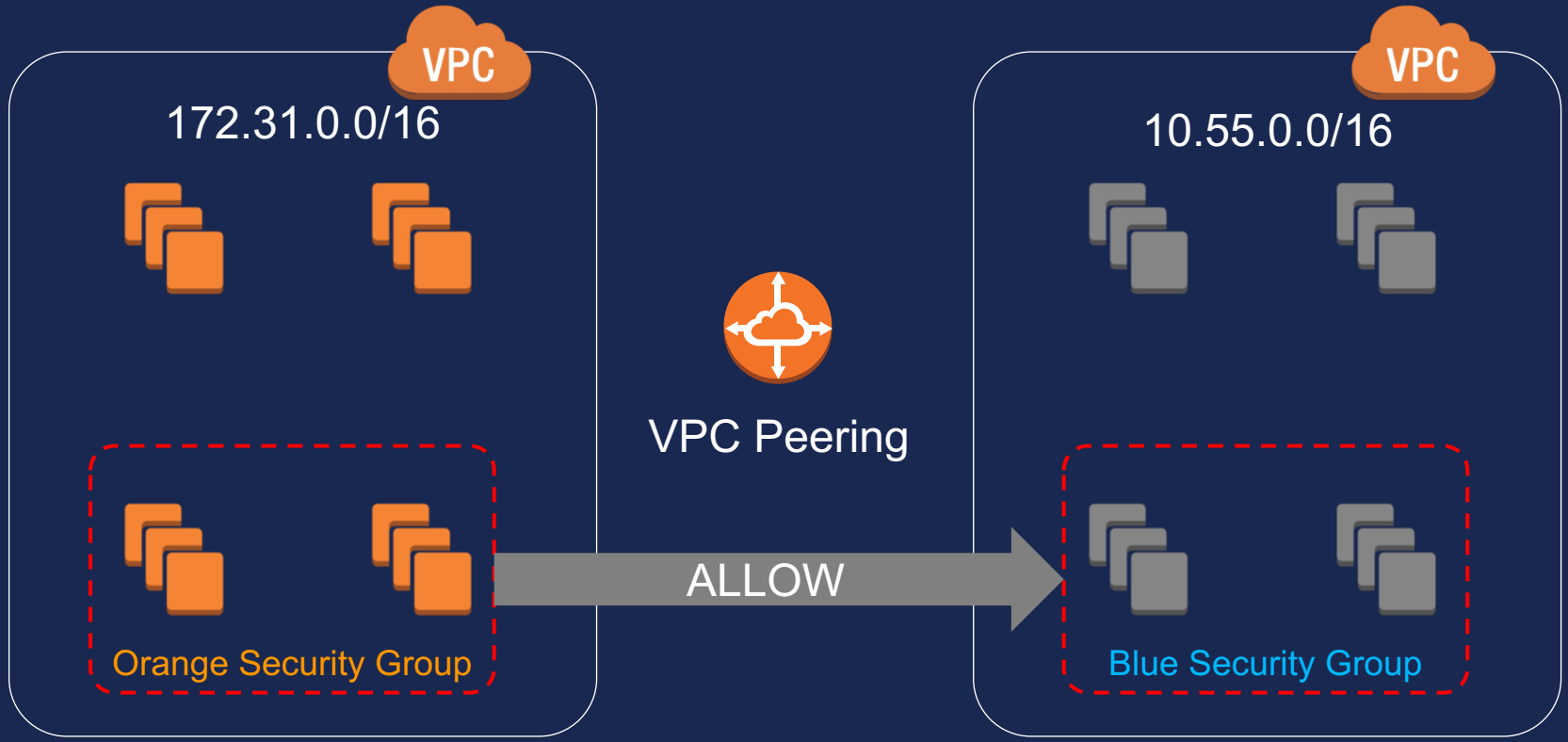
Establish a VPC peering: Accept request



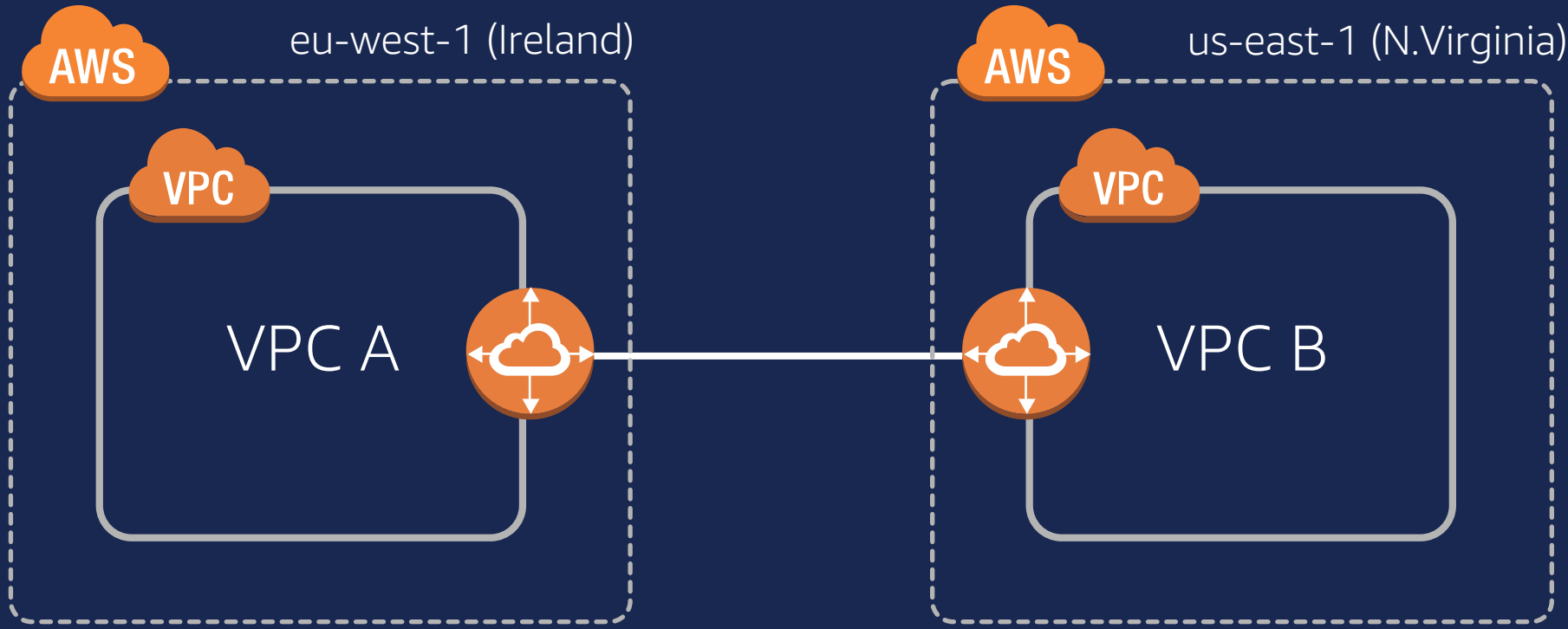
Establish a VPC peering: Create a route



Security groups across peered VPCs



Inter-Region VPC Peering

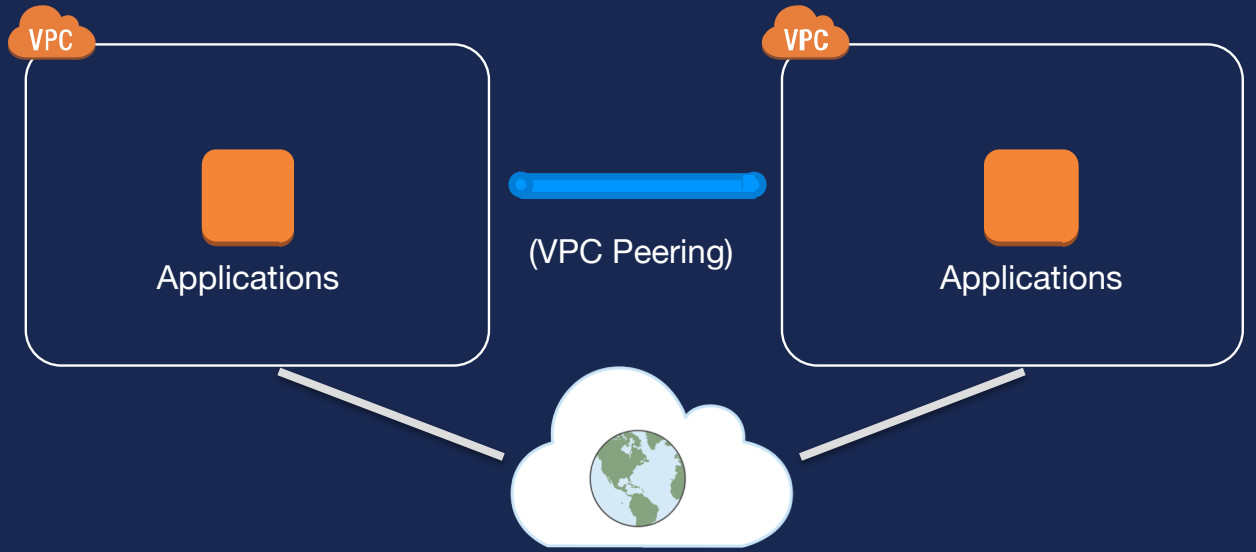


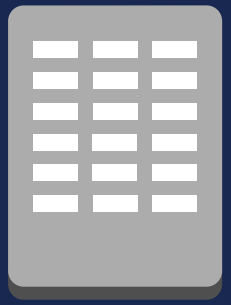
Some notes…

Inter-Region VPC Peering encrypts with no single point of failure or bandwidth bottleneck

Traffic using Inter-Region VPC Peering always stays on the global AWS backbone

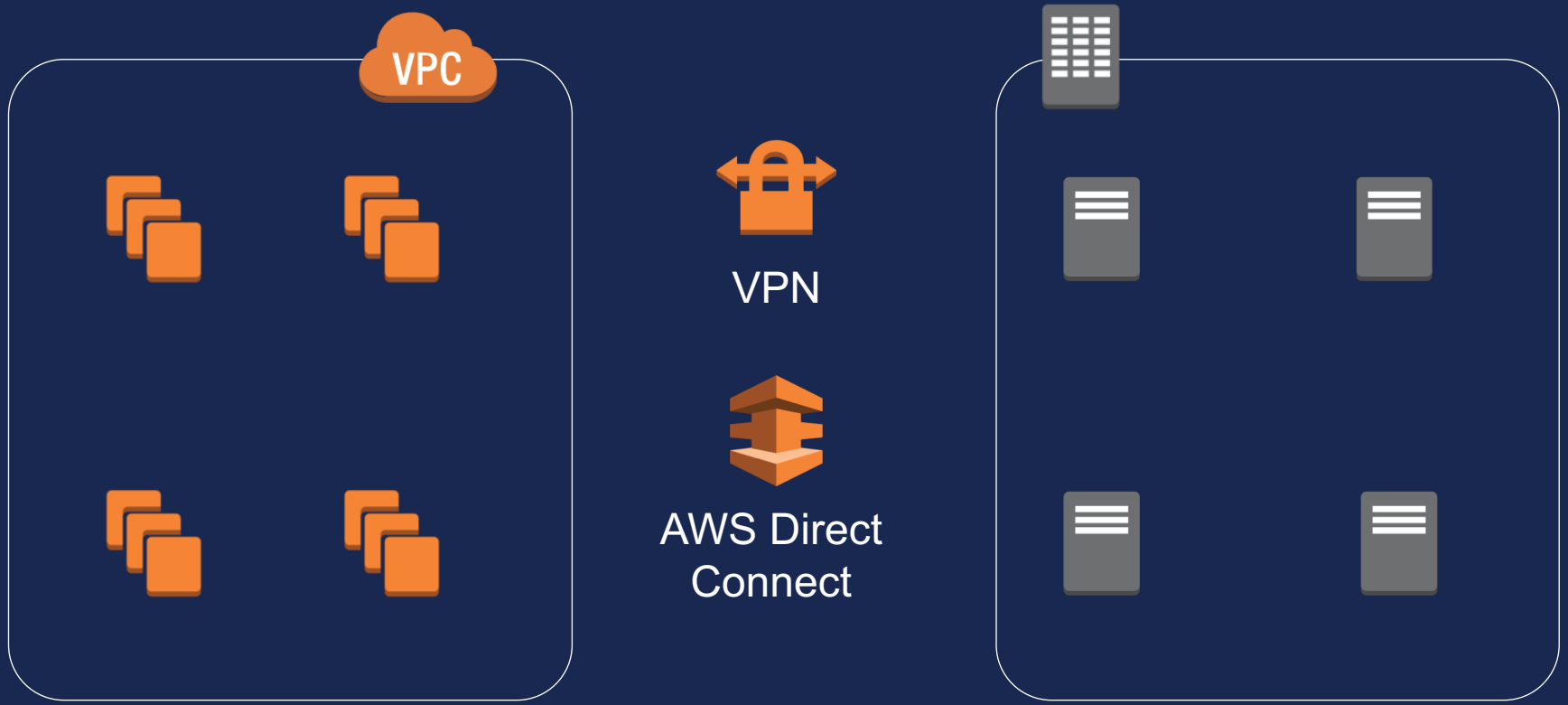
AWS Network - Progress



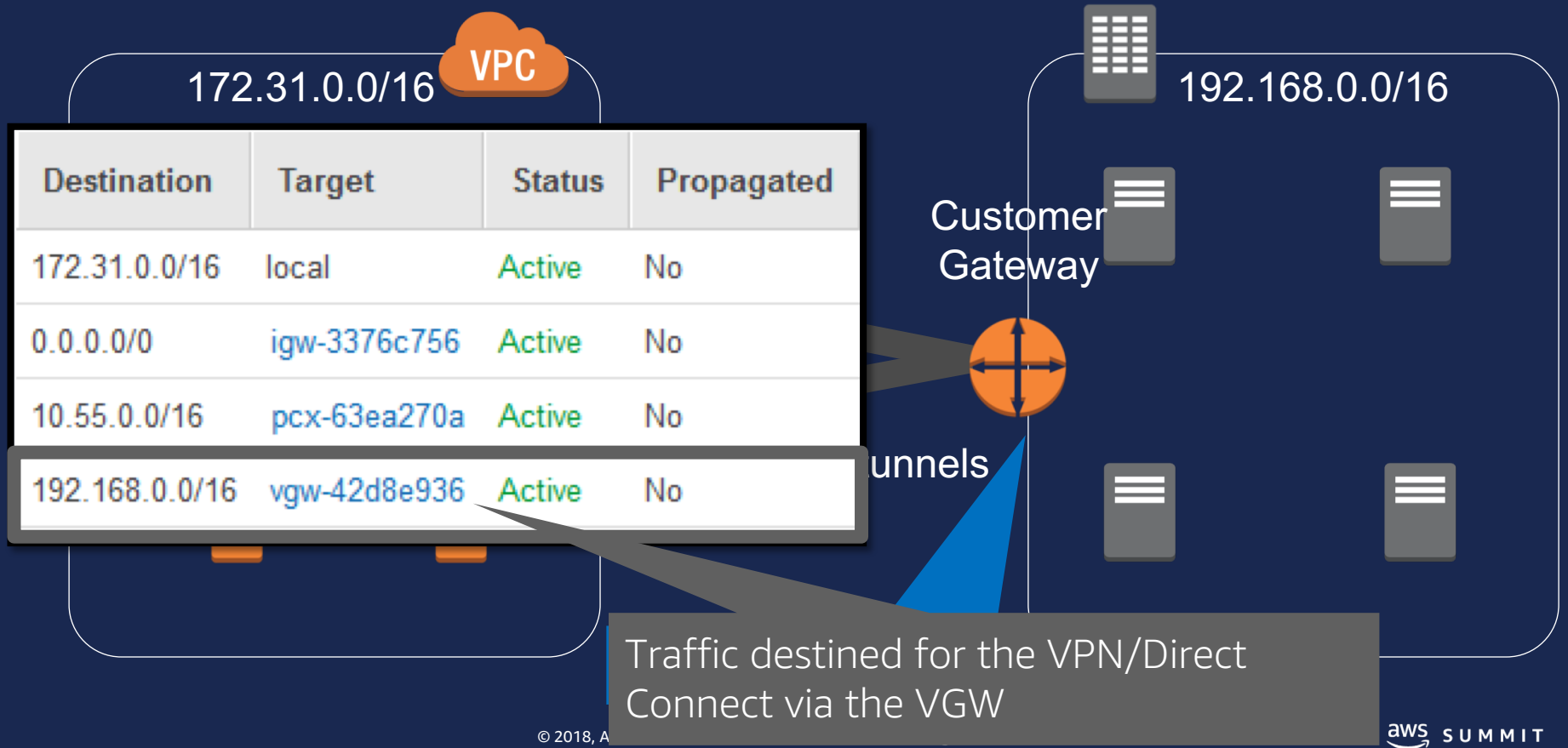


Connecting to on-premises networks: AWS Virtual Private Network and AWS Direct Connect

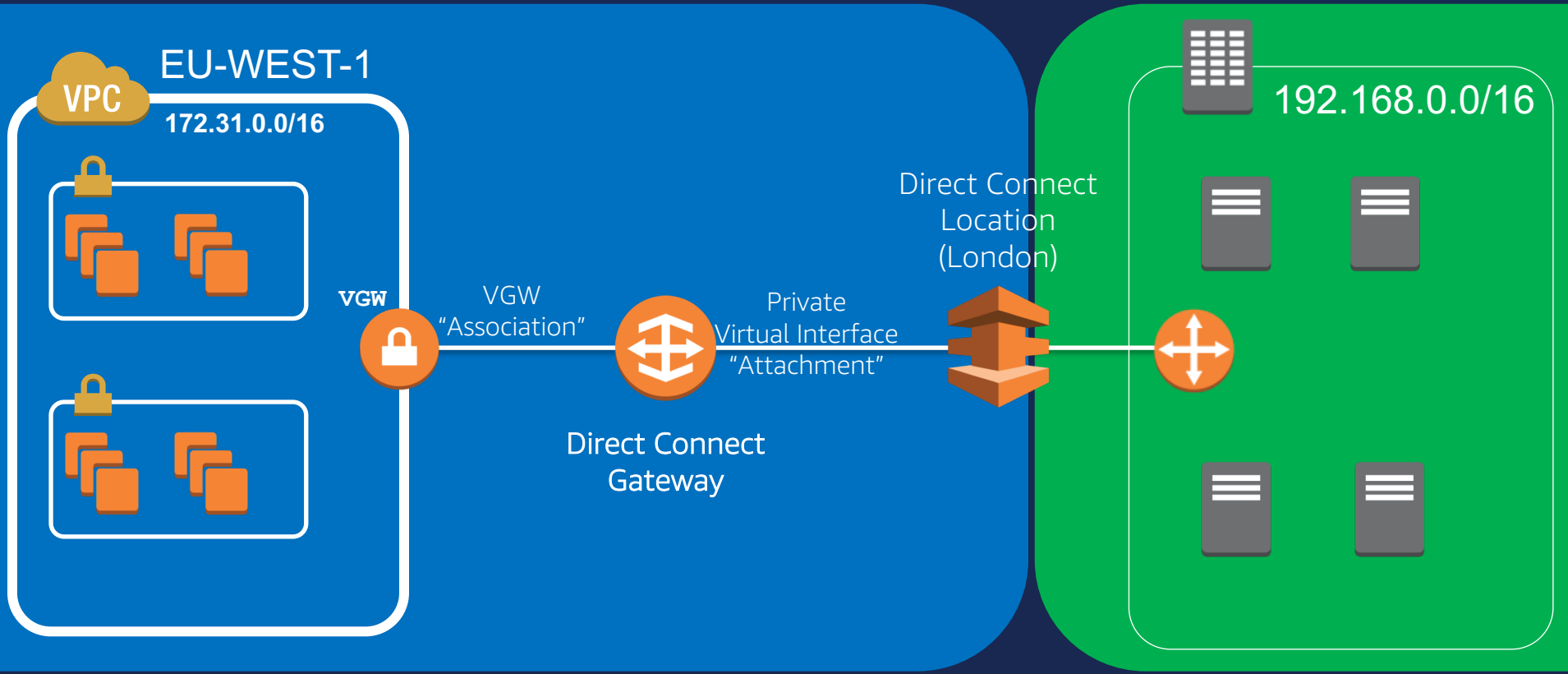
Extend an on-premises network into your VPC



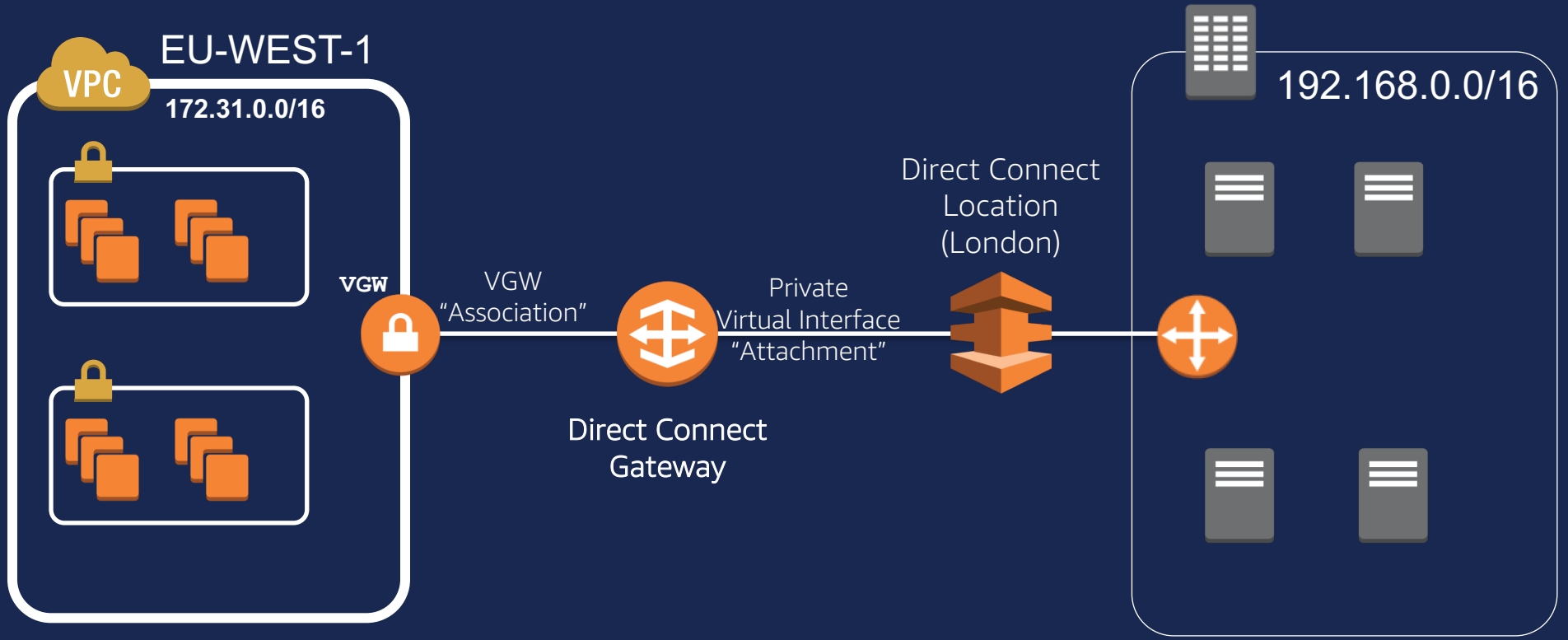
AWS VPN basics



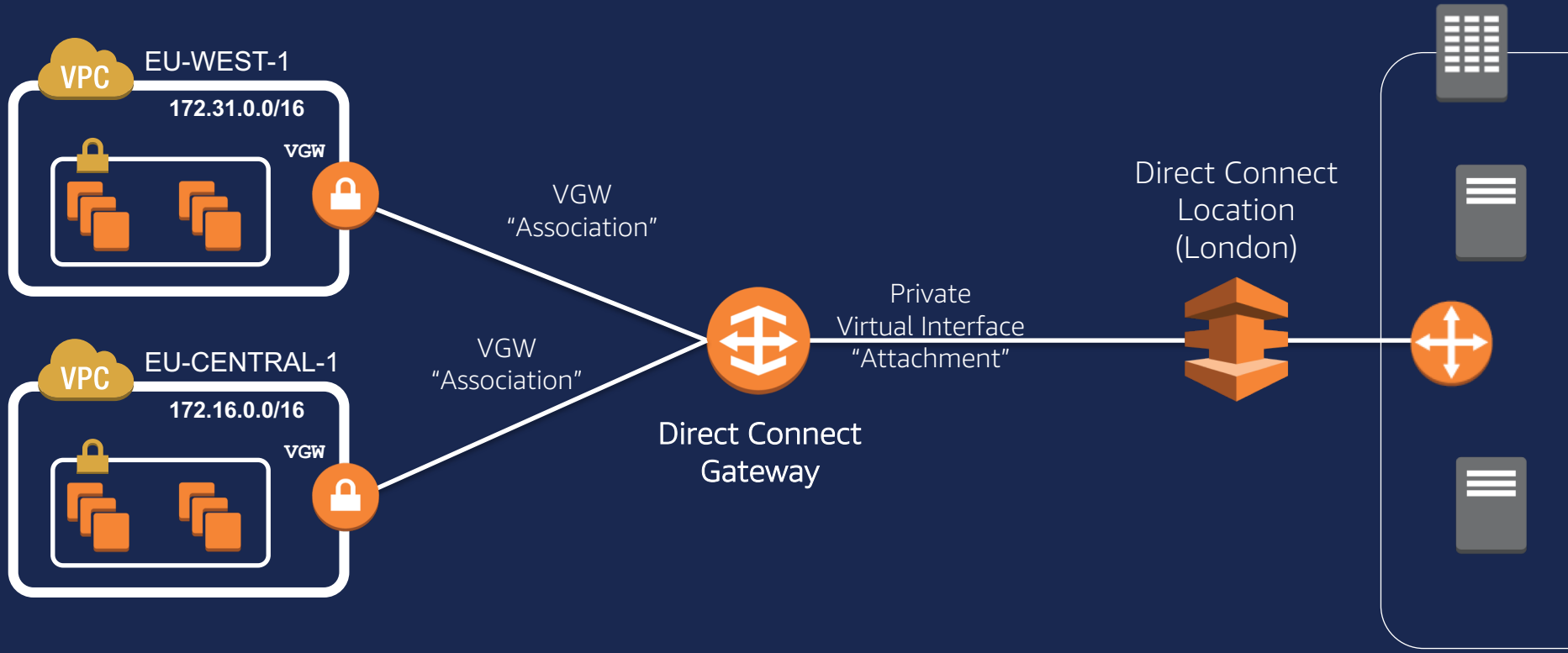
AWS Direct Connect Gateway



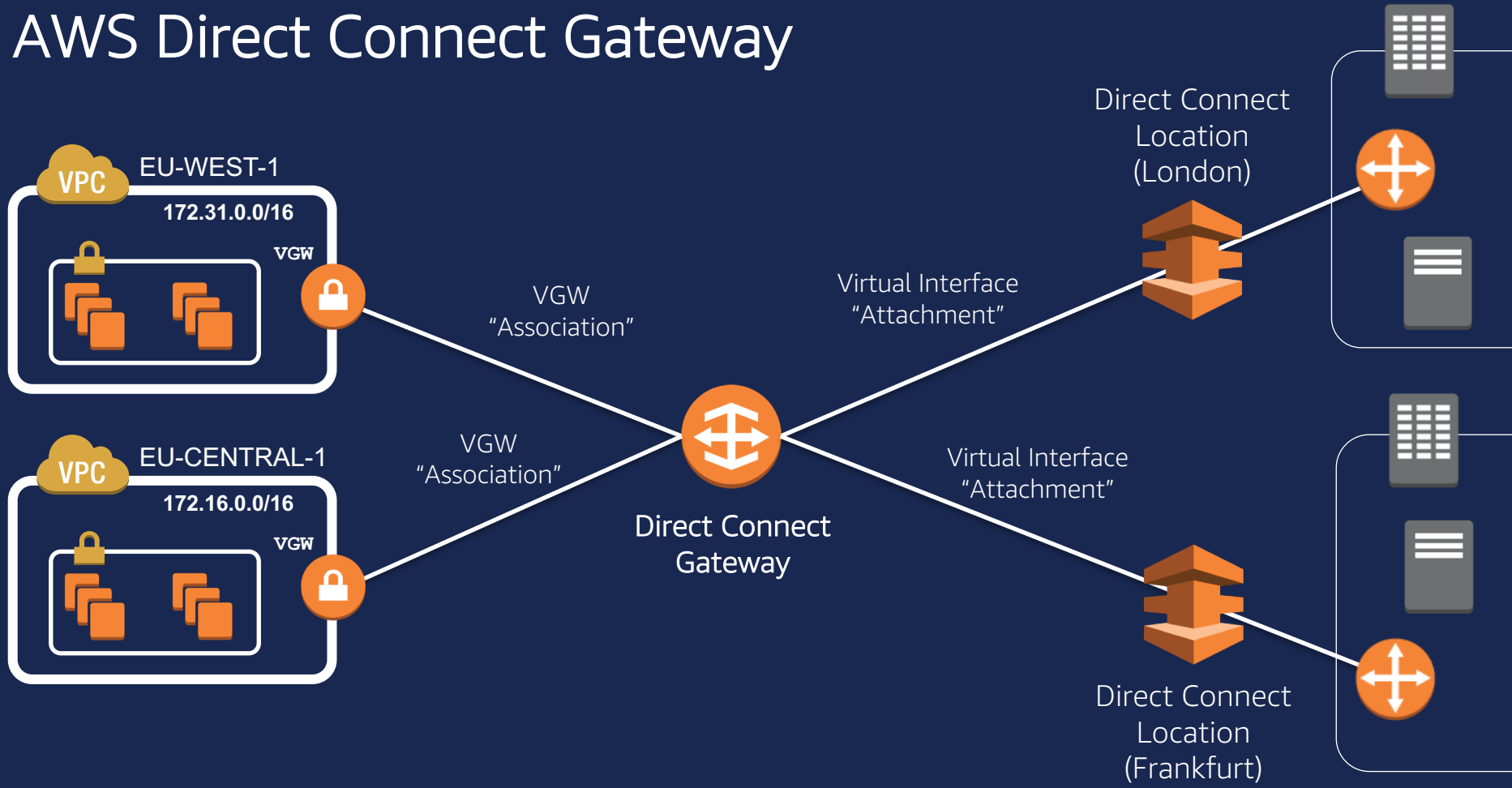
AWS Direct Connect Gateway



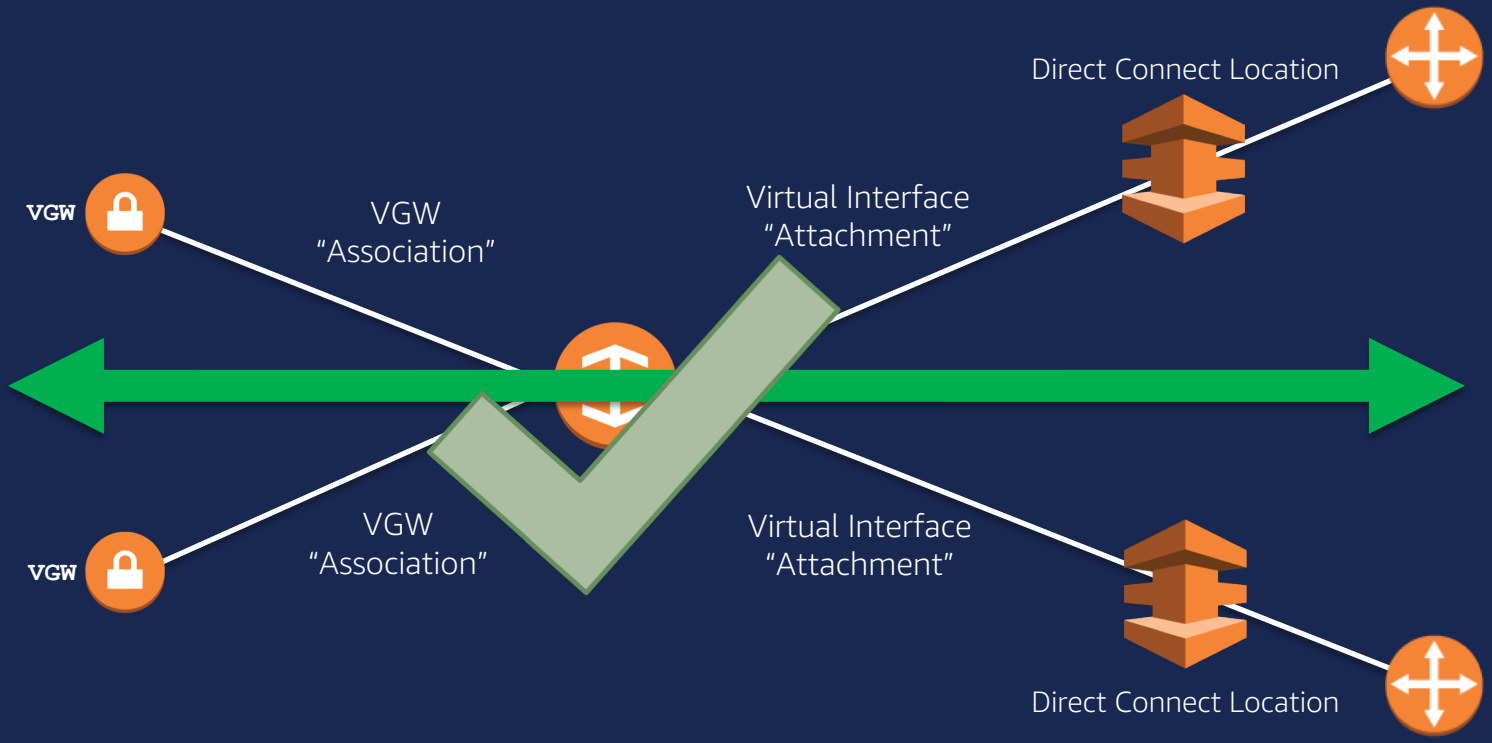
AWS Direct Connect Gateway



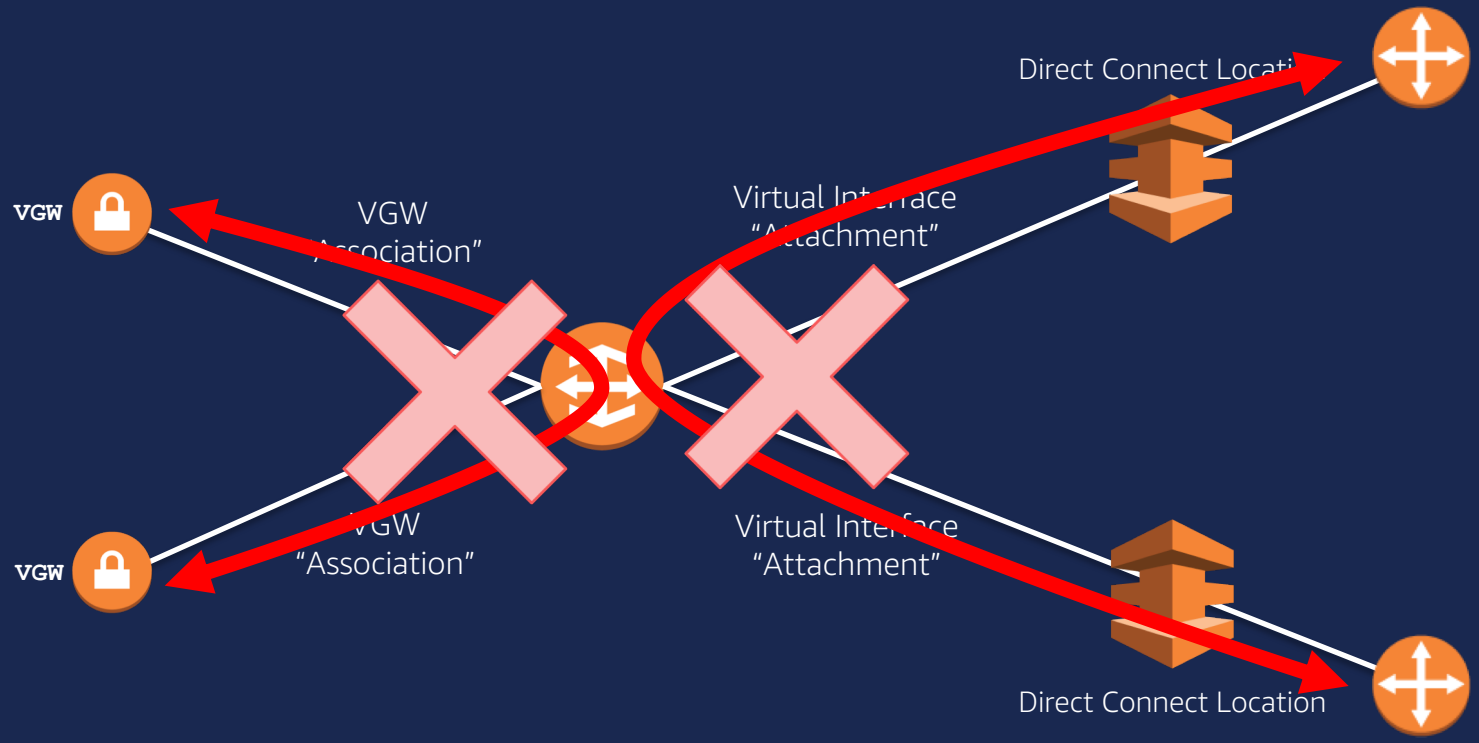
AWS Direct Connect Gateway



Direct Connect Gateway—traffic flows



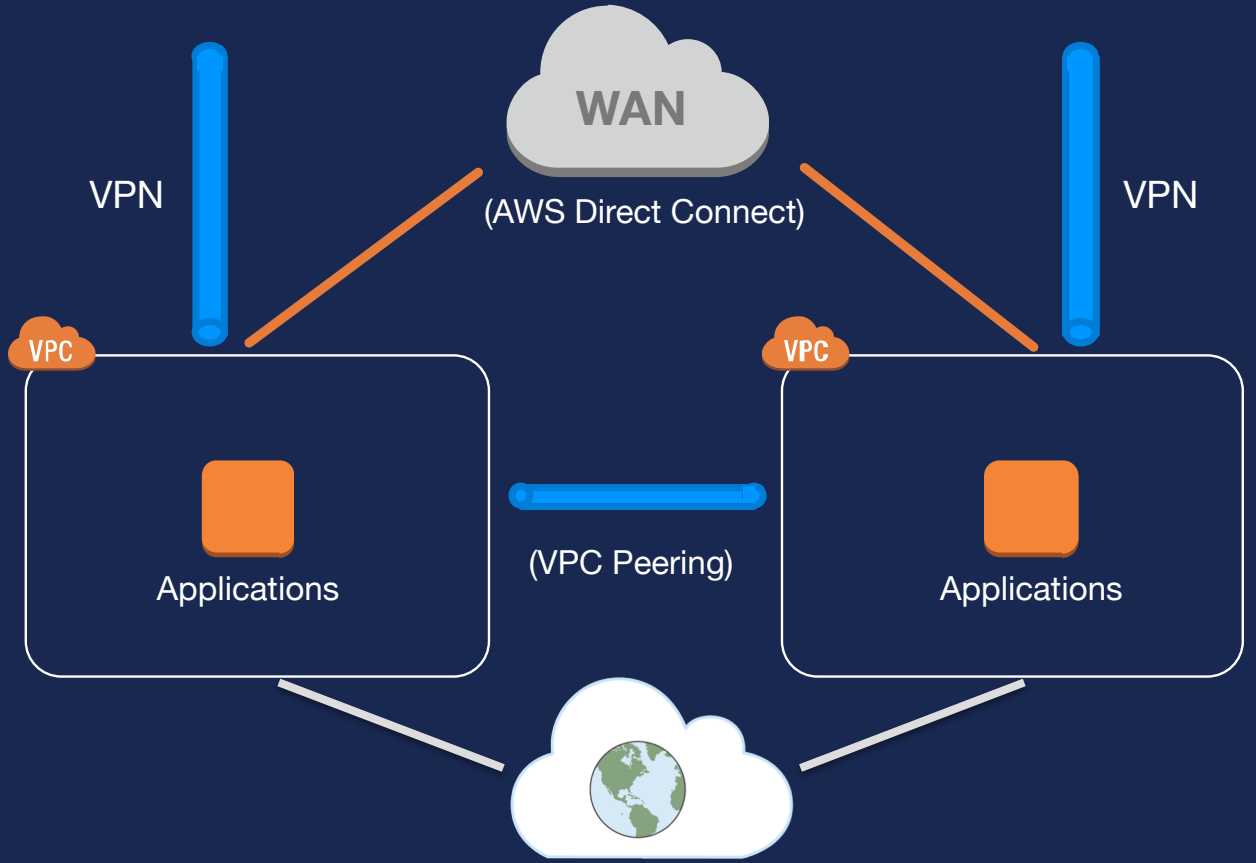
Direct Connect Gateway—traffic flows



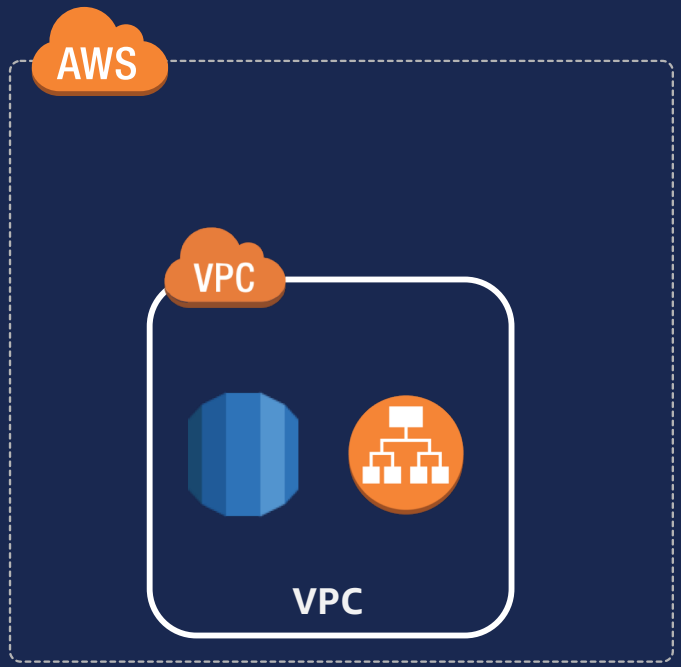
AWS VPN and AWS Direct Connect

- 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

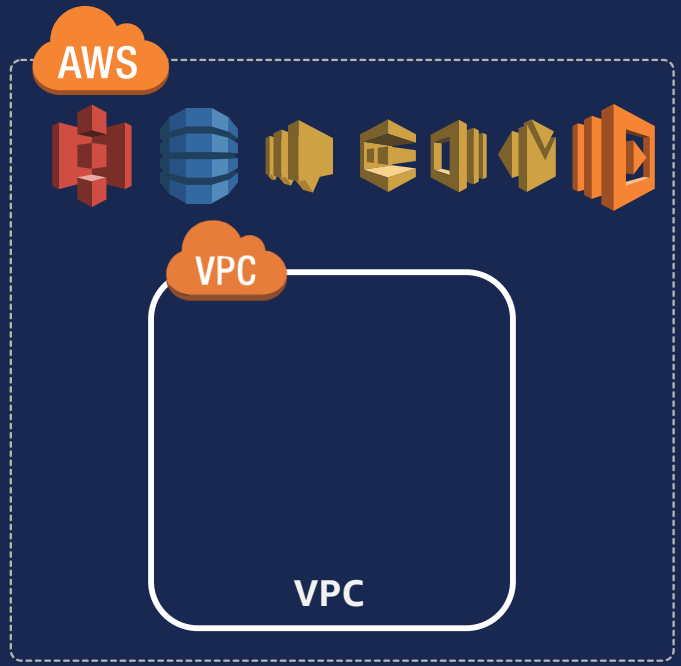
AWS Network - Progress



AWS Services



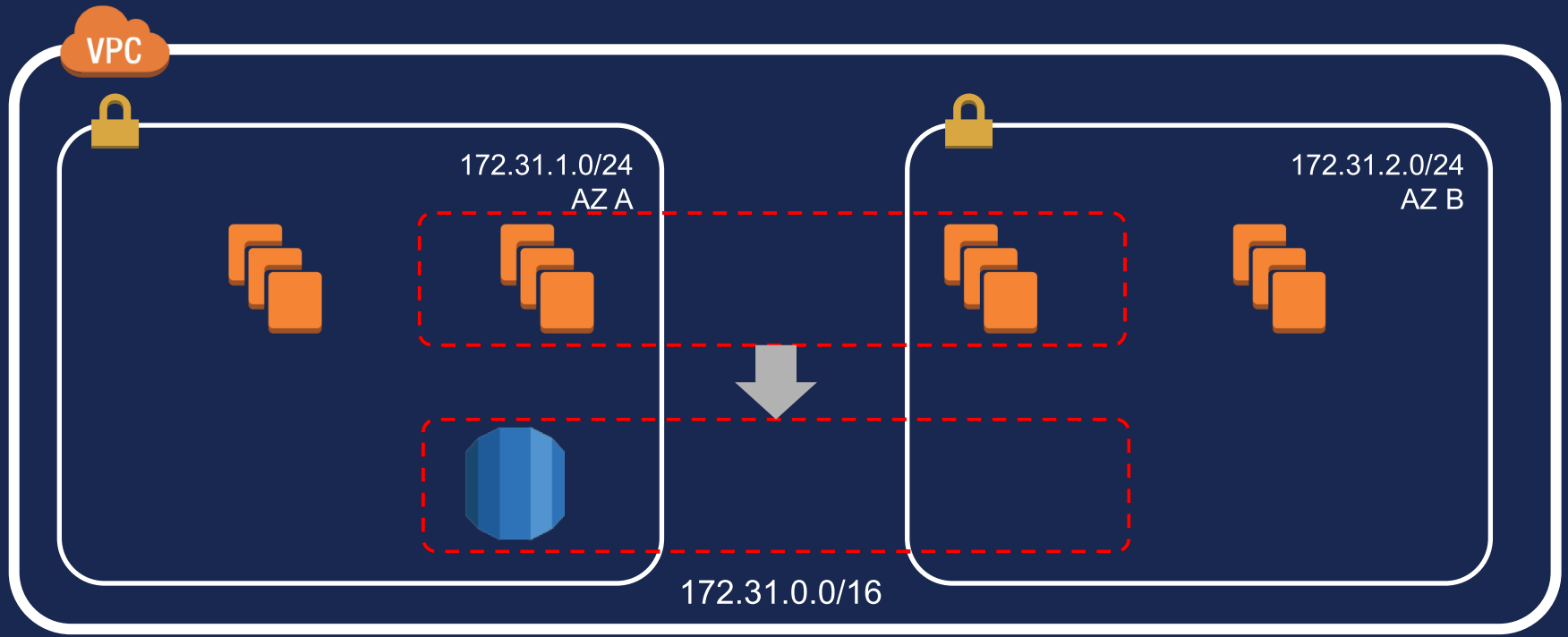
Inside of the VPC



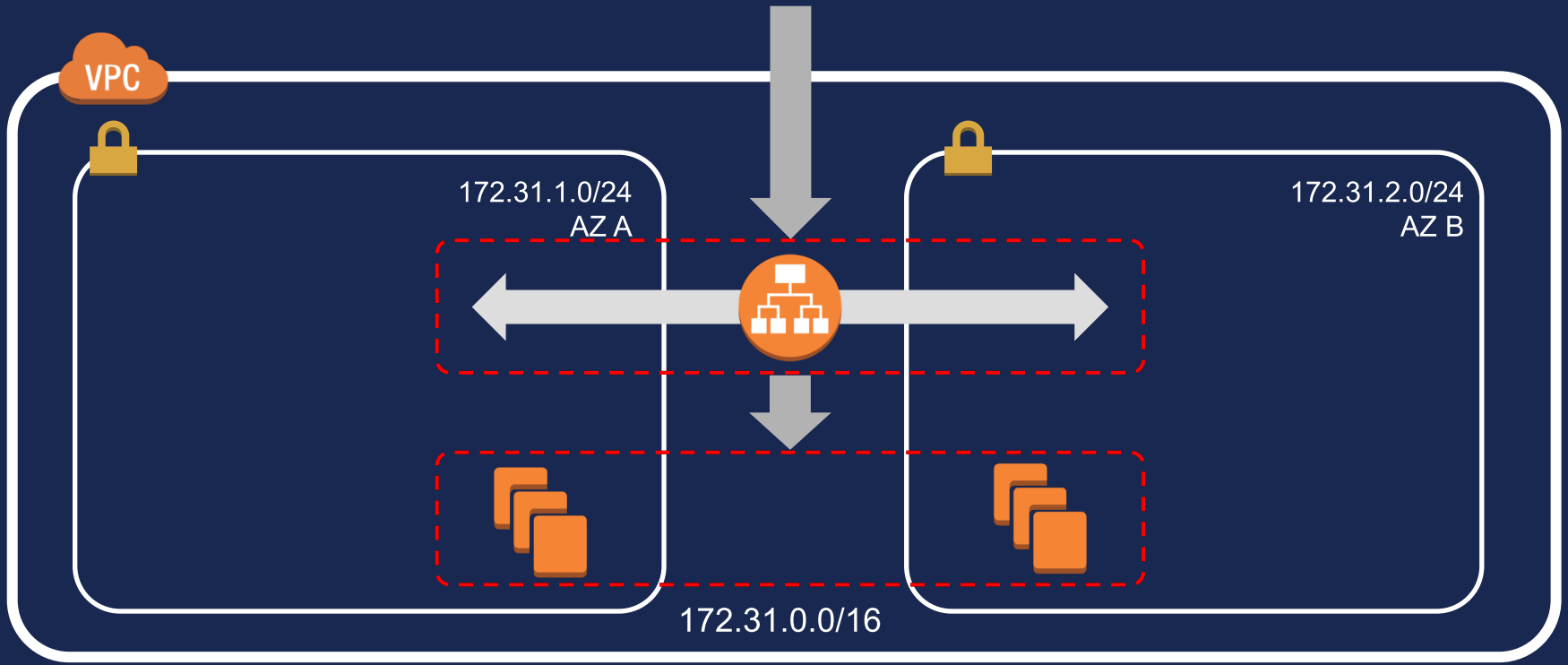
Outside of the VPC

AWS Services in your VPC

Example: Amazon RDS Database in your VPC



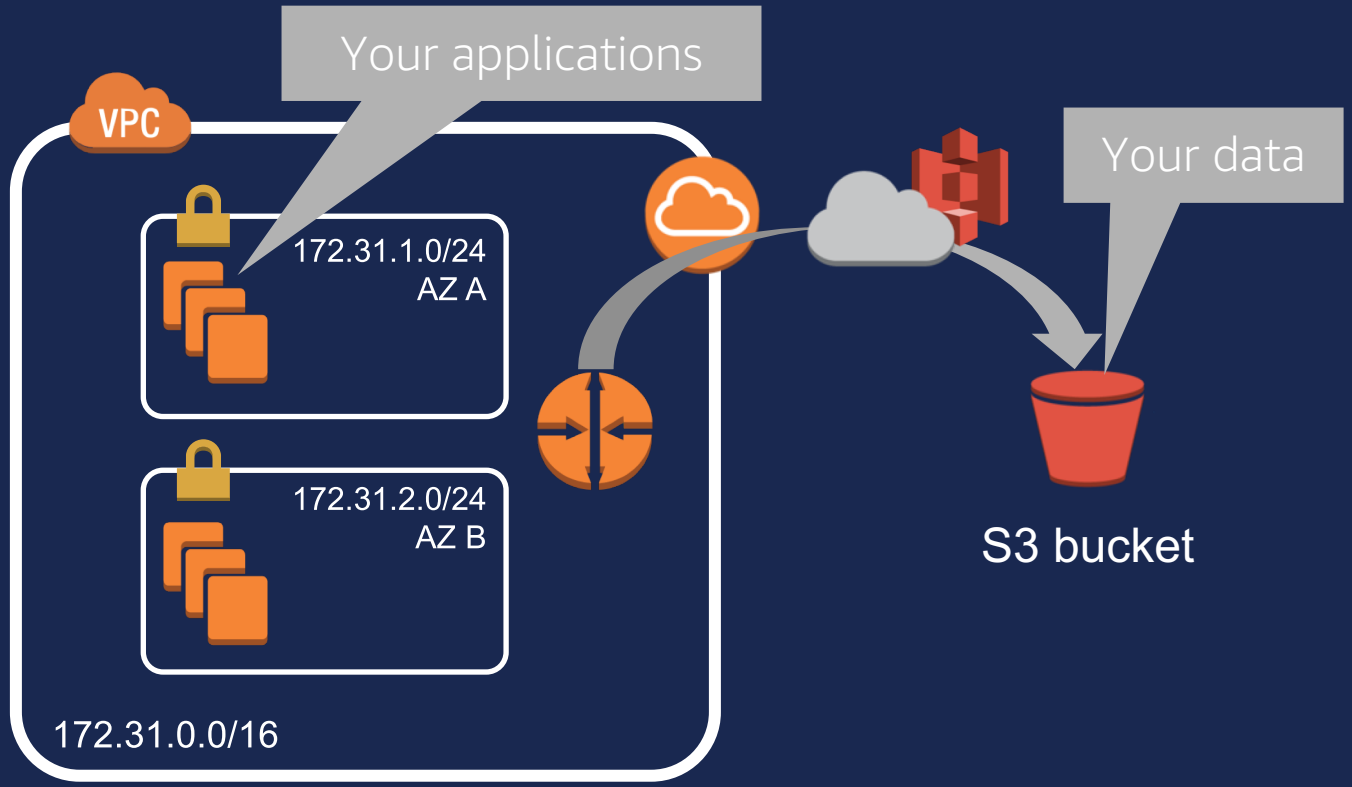
Example: Application Load Balancer in your VPC



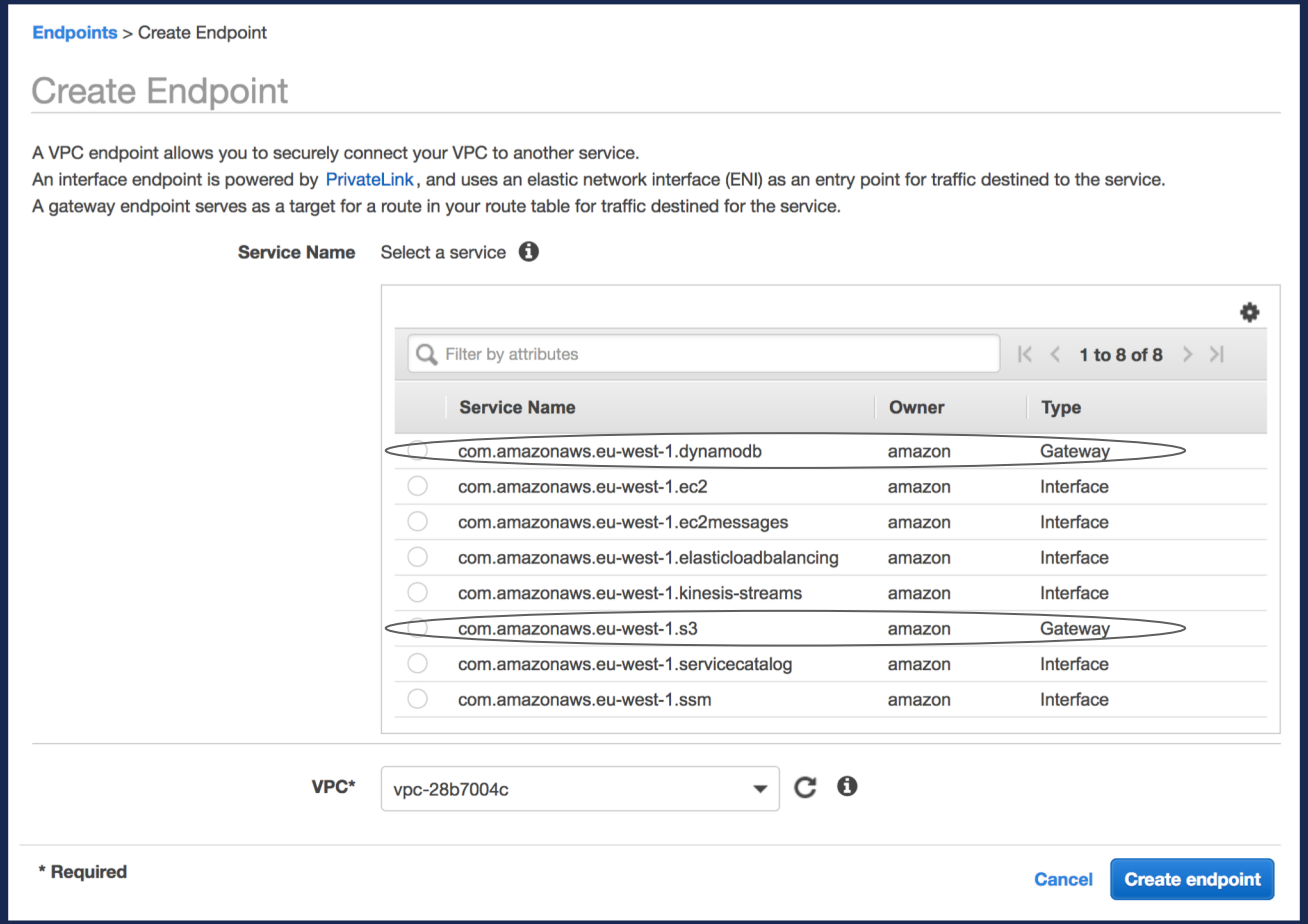
AWS Services outside your VPC

Endpoints for AWS Services

Amazon S3 and your VPC

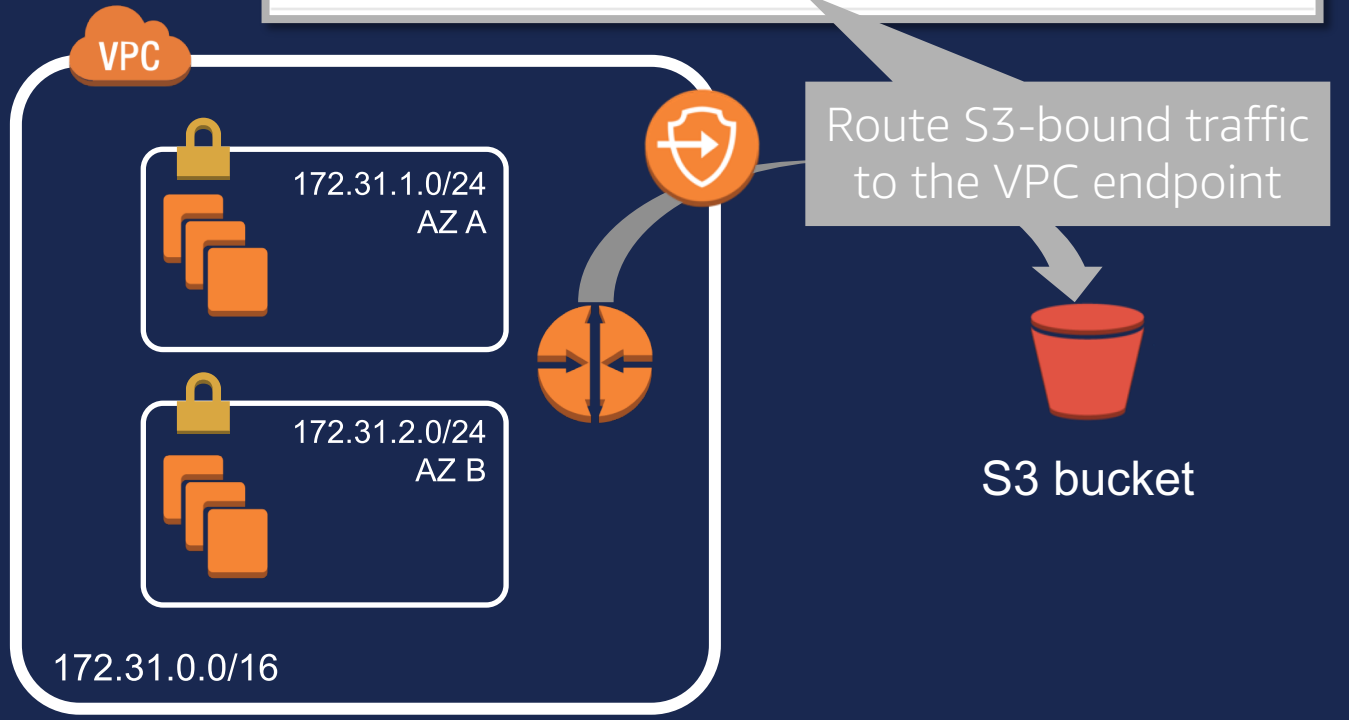


Gateway VPC Endpoints

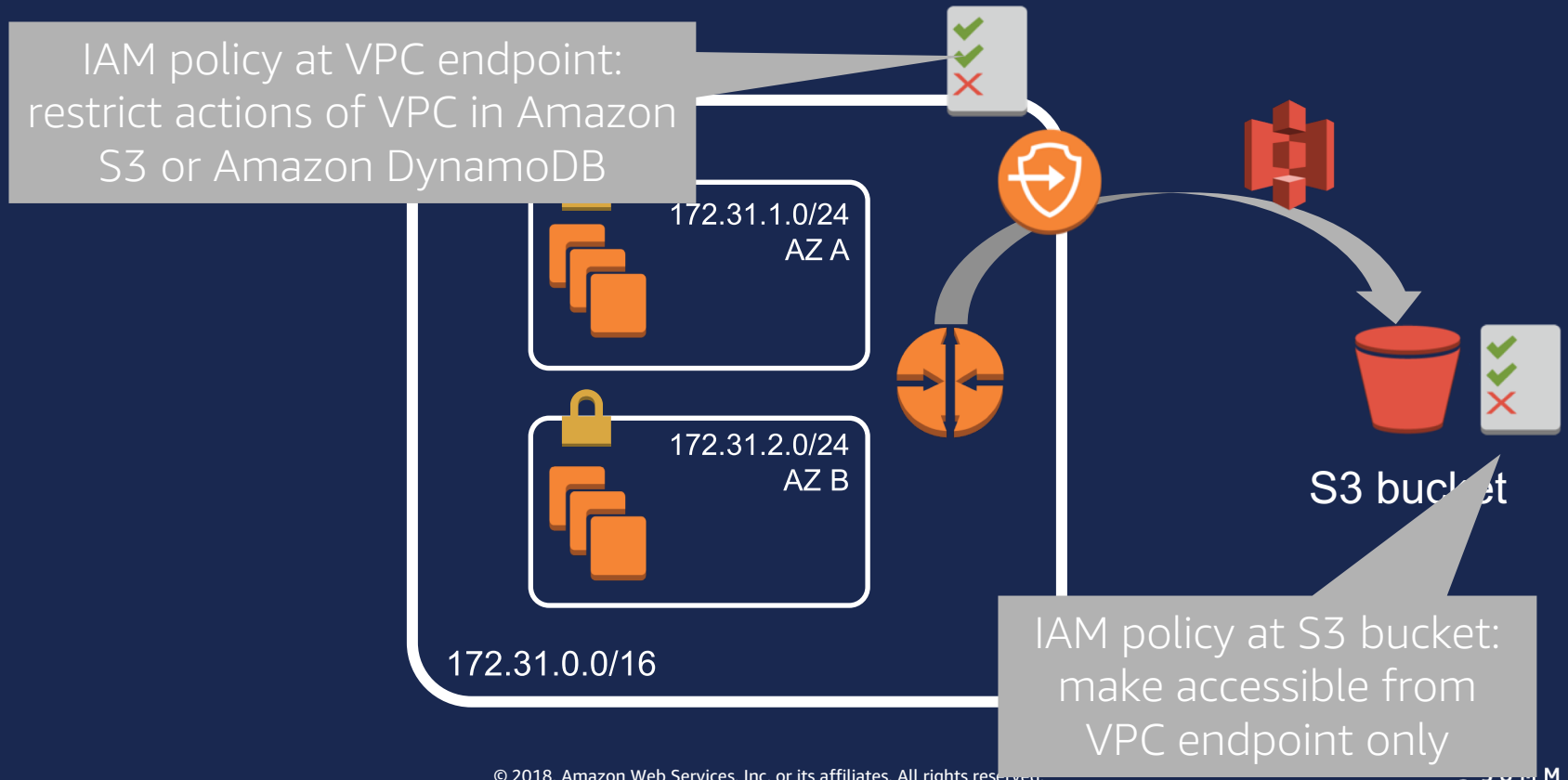


VPC Endpoints: Amazo

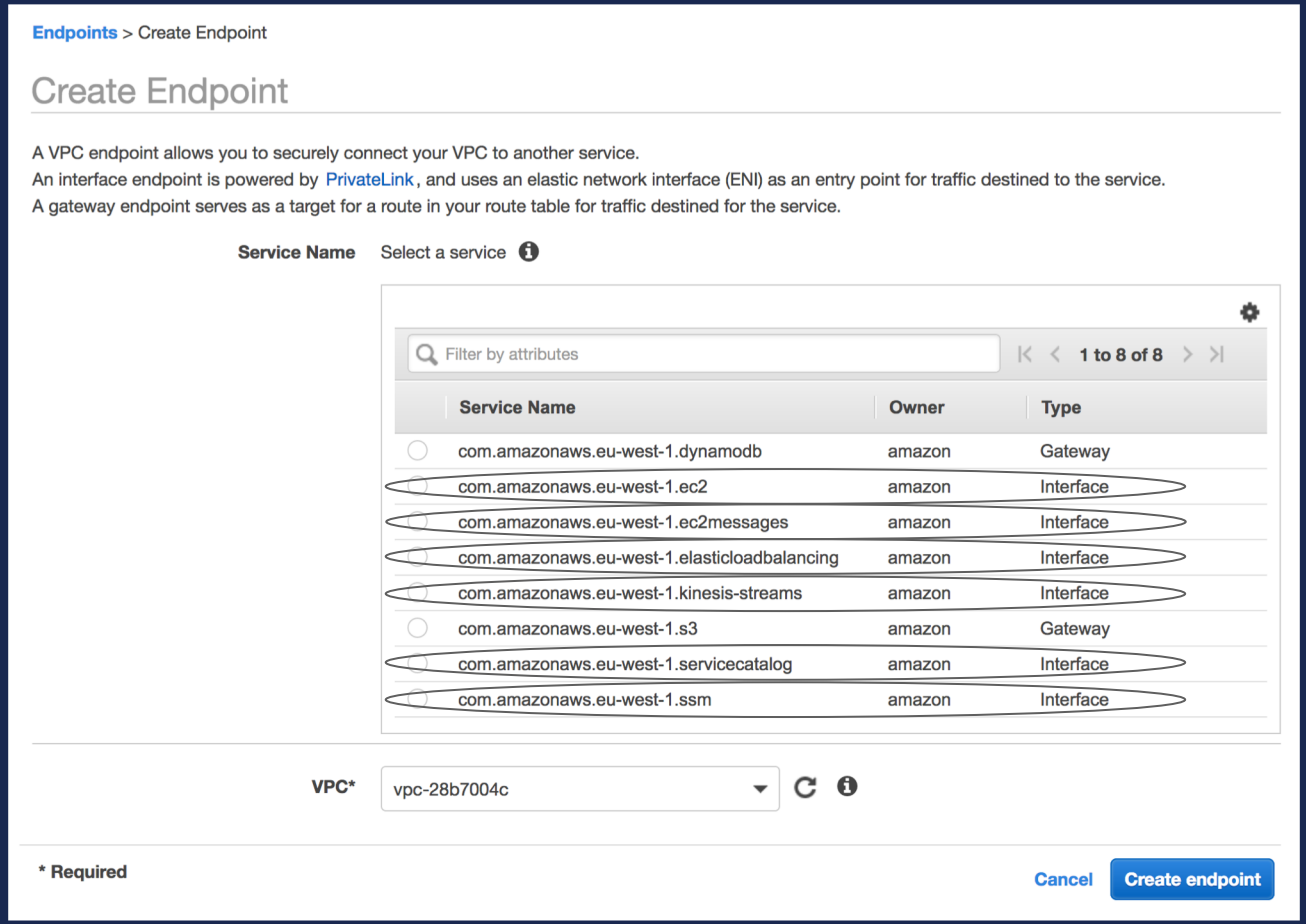
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
pl-68a54001 (com.amazonaws.us-west-2.s3)	vpce-3a14fc53	Active	No



IAM policy for VPC Endpoints



Interface VPC Endpoints



AWS PrivateLink for AWS Services

AWS PrivateLink for Customer & Partner Applications

Share services privately and securely between VPCs, AWS accounts, and on-premises networks

Powered by Network Load Balancer

Secure endpoint within Client VPC

Integrated with AWS Marketplace

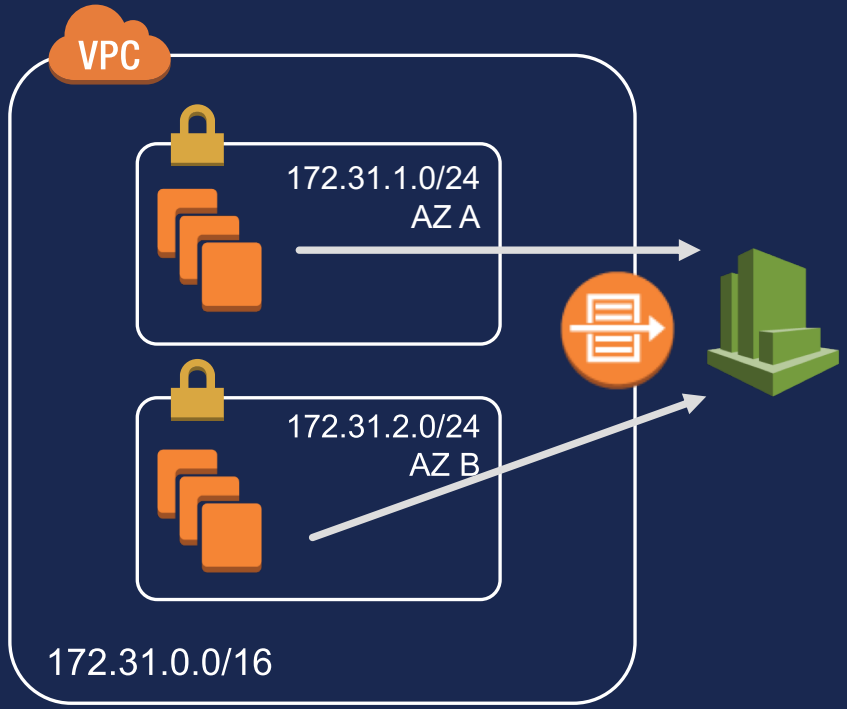
Customers and partners

ca technologies · Vanguard · twilio · TIBCO · snowflake · SIGOPT · salesforce heroku · APPDYNAMICS · GE · Expedia · dynatrace · cisco Stealthwatch Cloud · AUTODESK · aqua · Alfresco

Available in all public AWS regions, except CN-NORTH-1

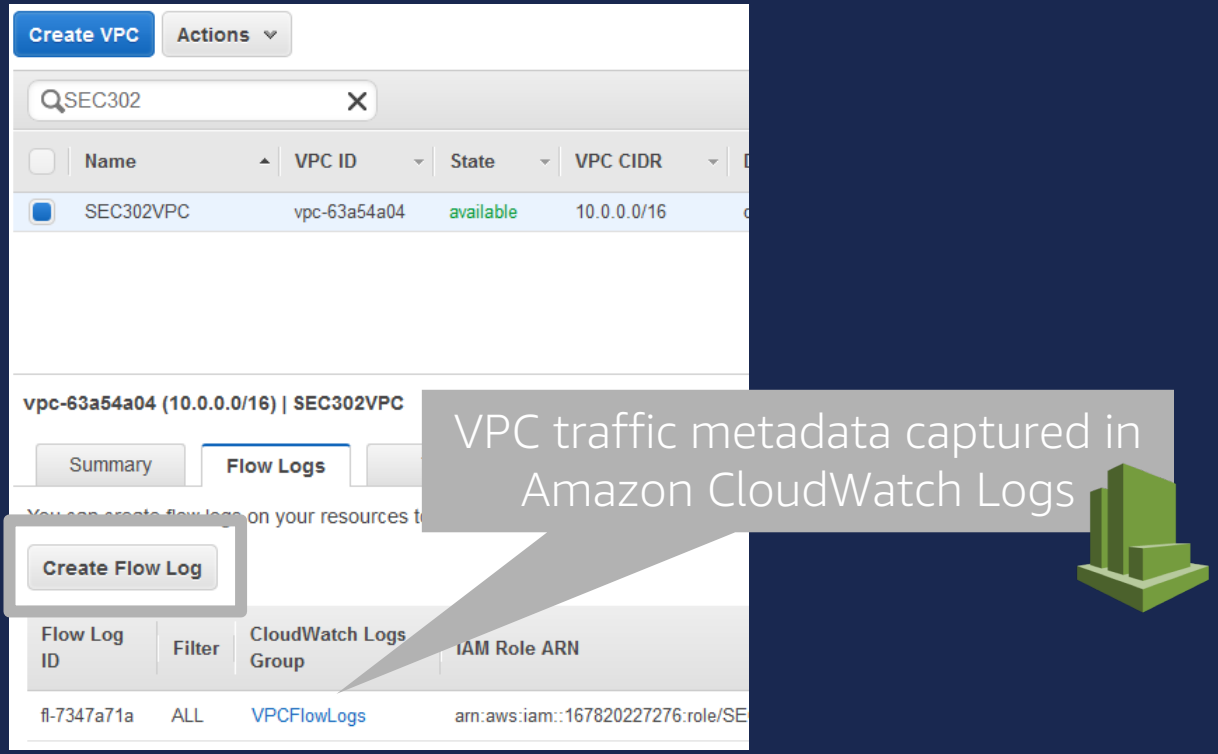
VPC Flow Logs:
VPC traffic metadata in Amazon CloudWatch Logs

VPC Flow Logs

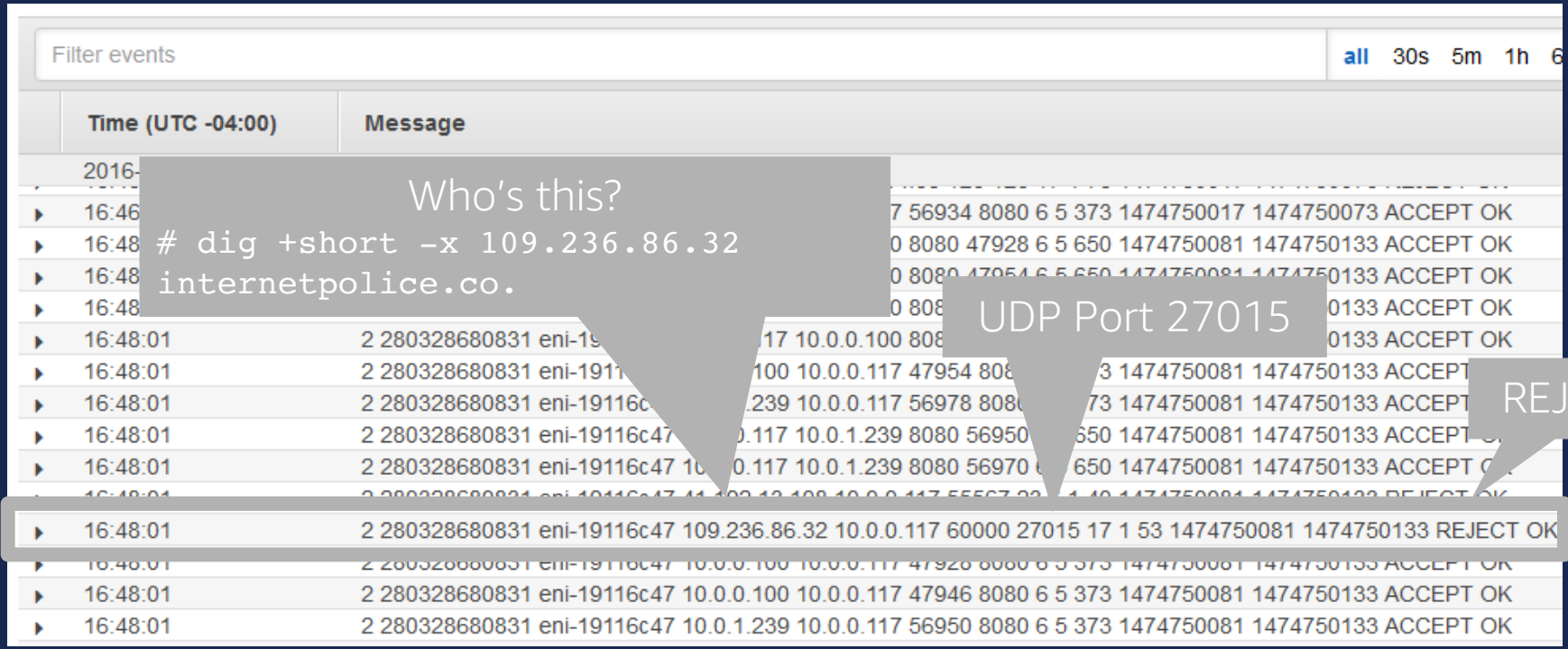


- Visibility into effects of security group rules
- Troubleshooting network connectivity
- Ability to analyze traffic

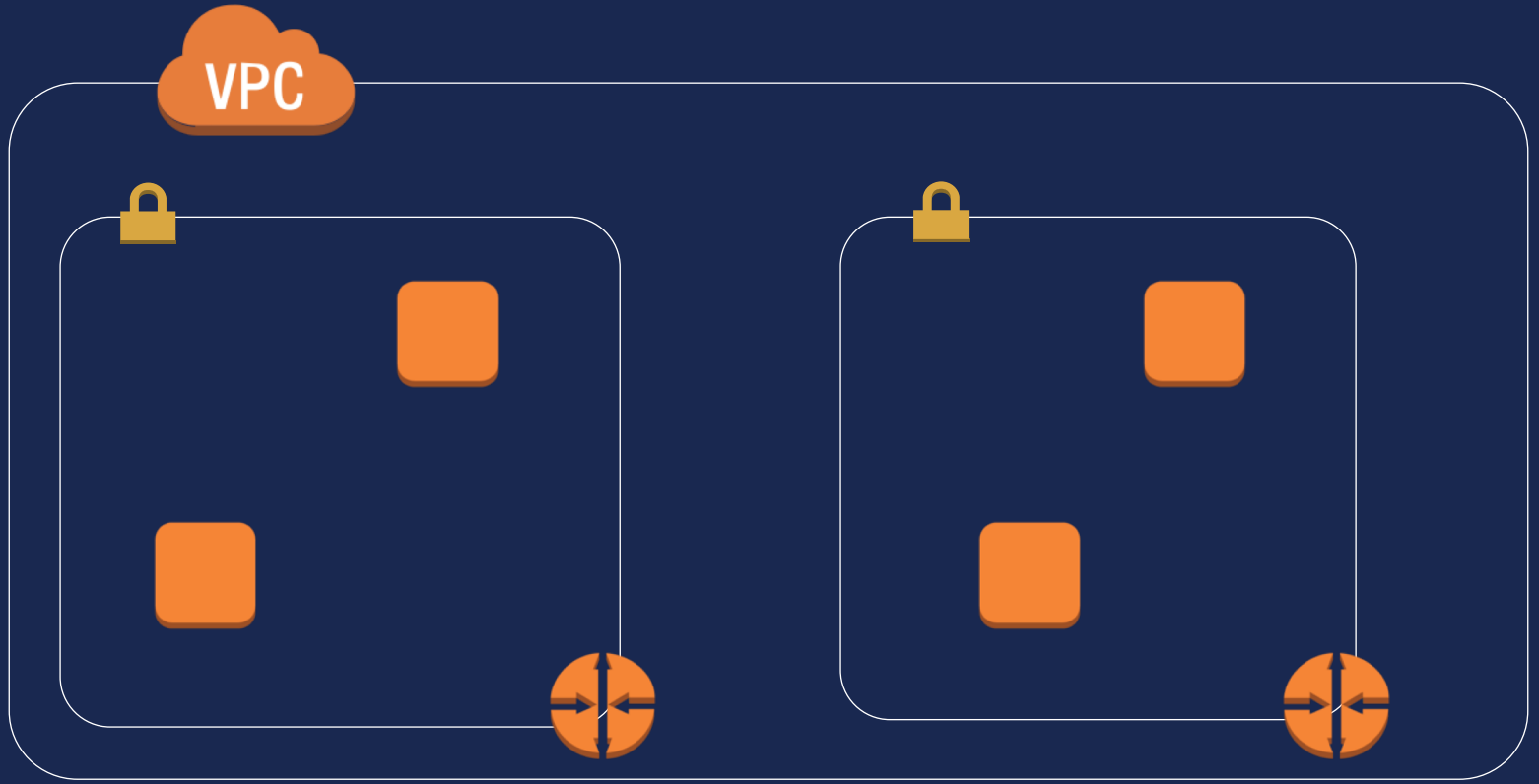
VPC Flow Logs: Setup



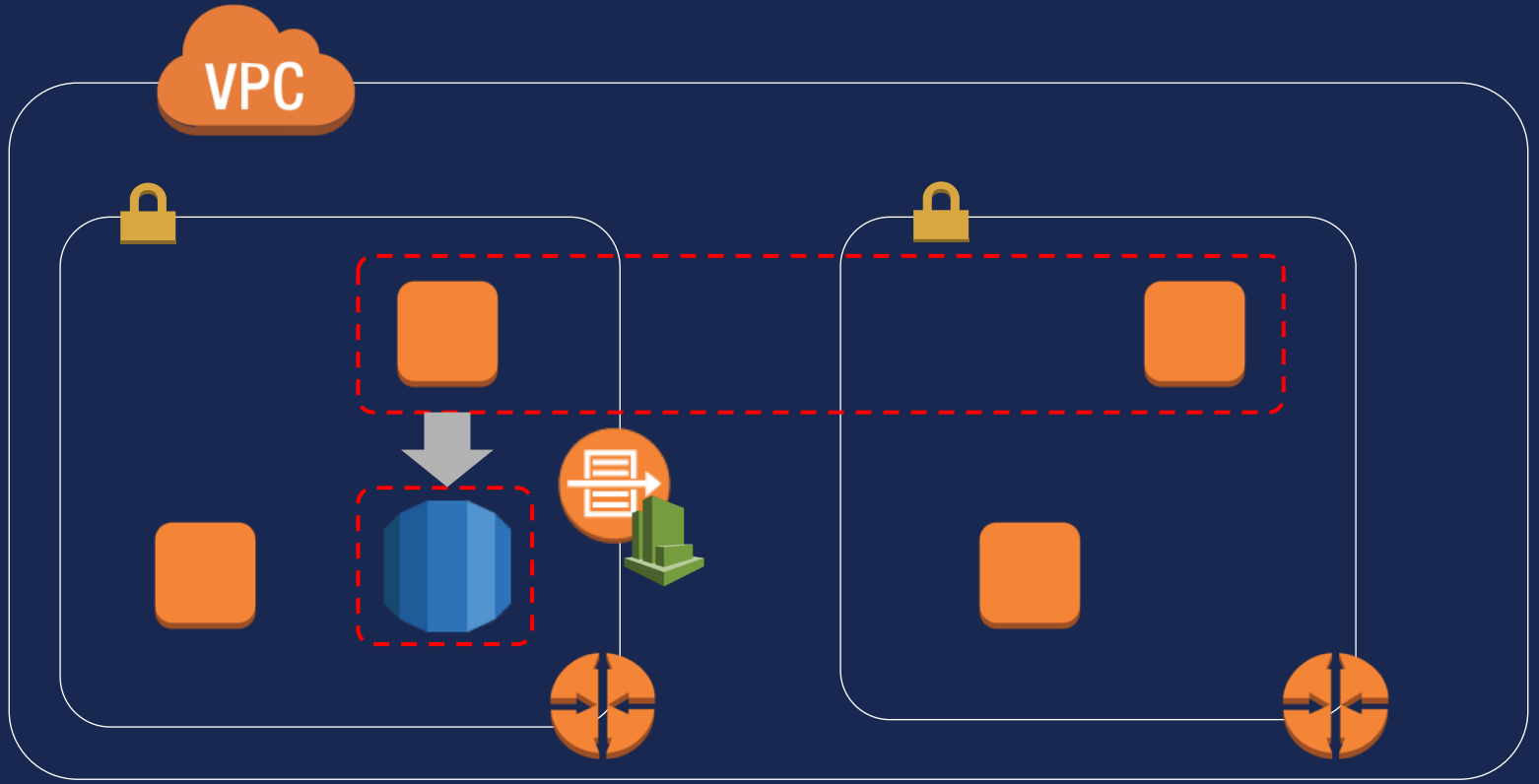
VPC Flow Logs data in CloudWatch Logs



The VPC Network

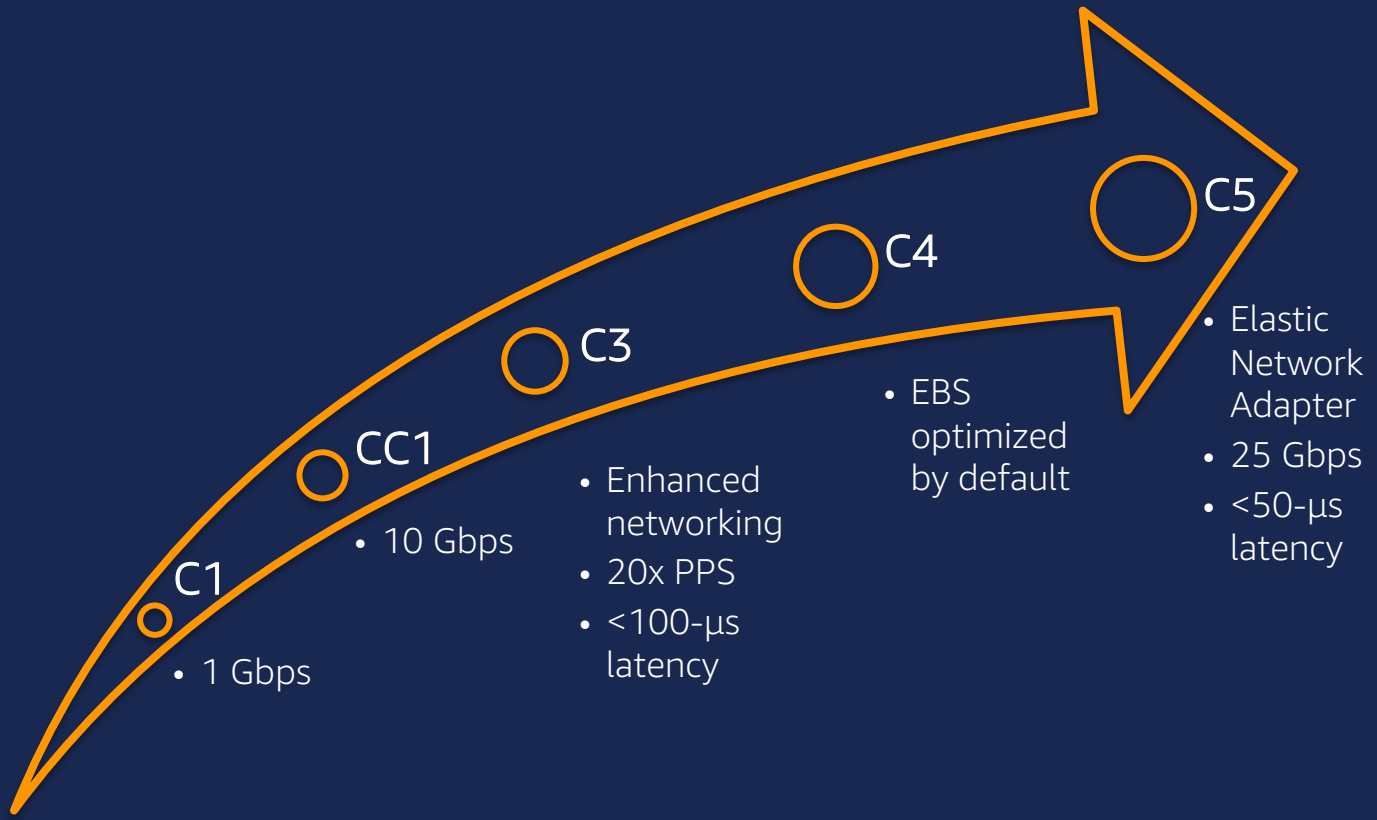


VPC Network Security



VPC Connectivity

On-Instance Networking Improvements



Instance Bandwidth Limits

25 Gbps
within placement group

25 Gbps
within region

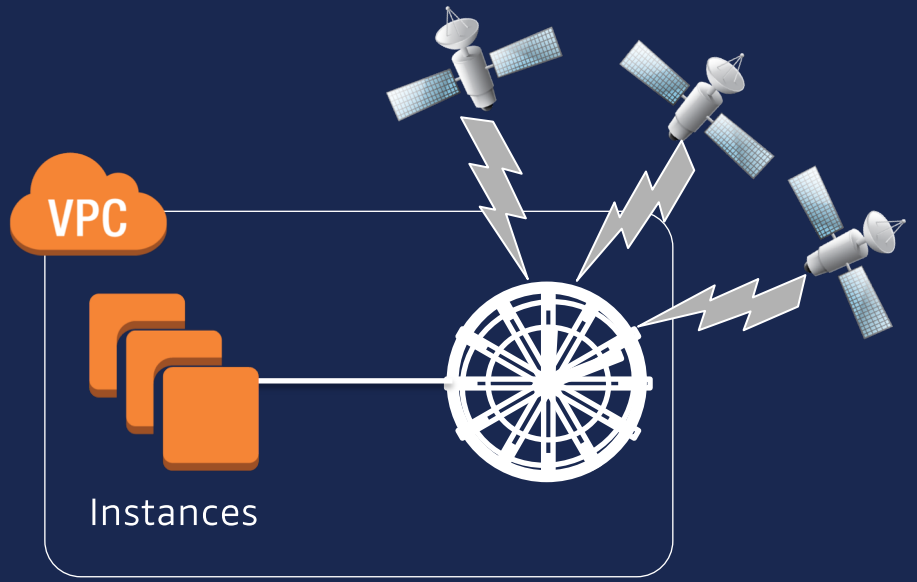
25 Gbps
to Amazon S3

5 Gbps
for other sources

Amazon Time Sync Service

Highly reliable service with a redundant array of satellite and atomic clock sources

Available globally today!



aws SUMMIT

Thank You!

Tom Adamski
Specialist Solutions Architect