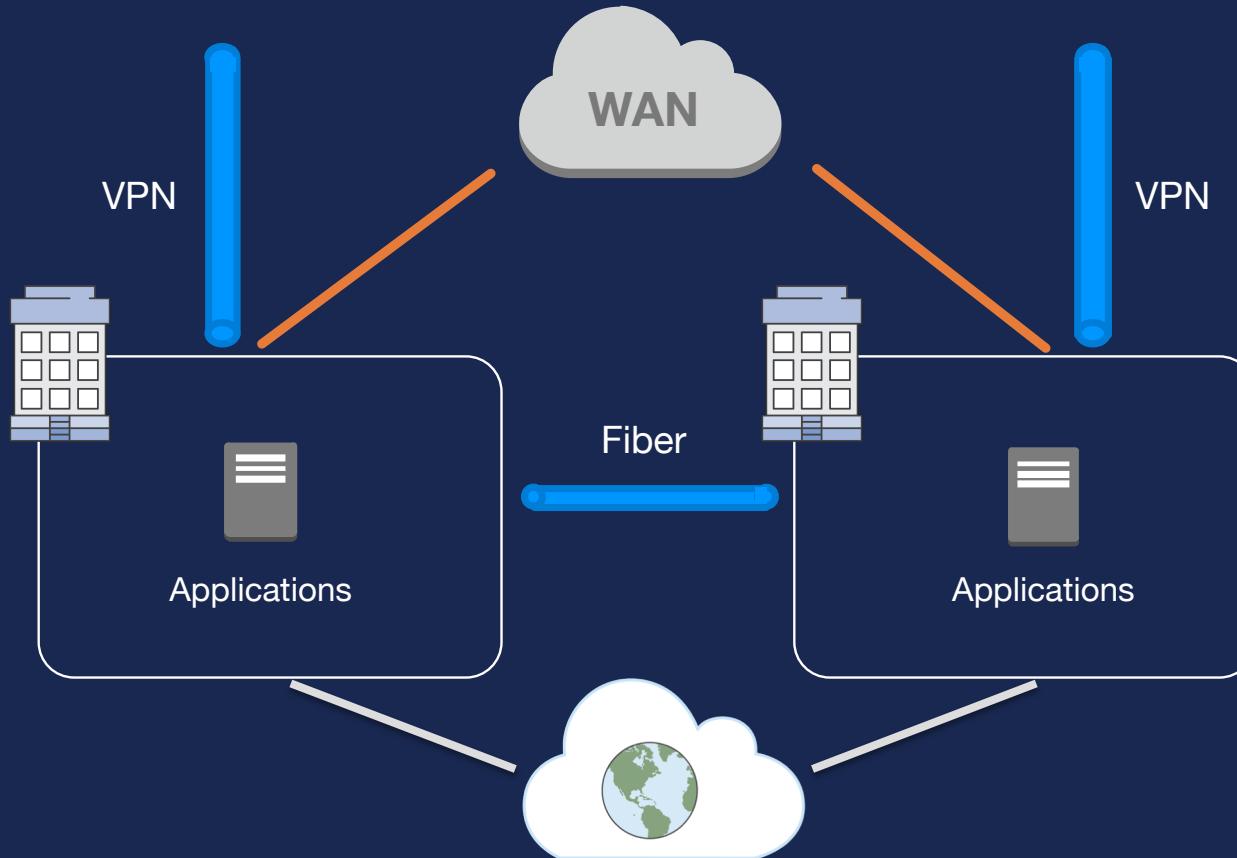




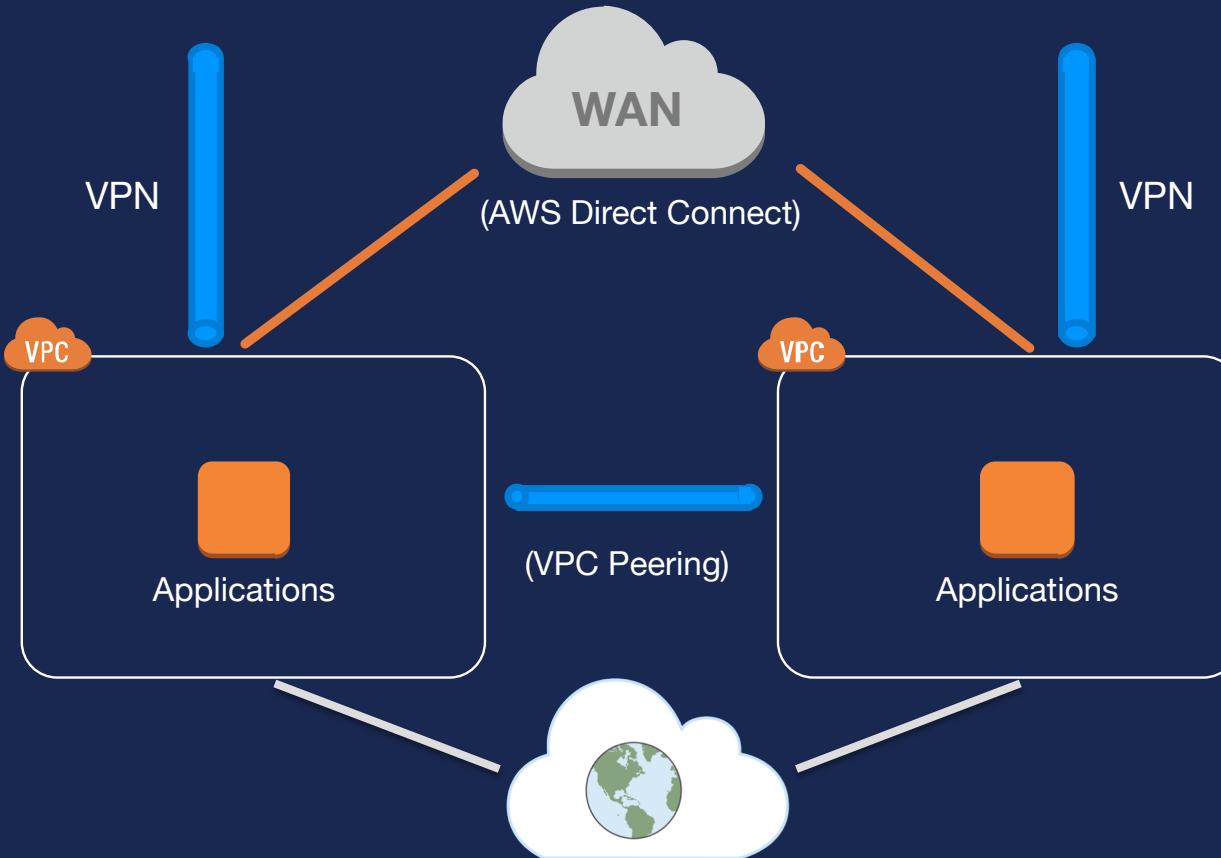
AWS Networking Fundamentals

Tom Adamski
Specialist Solutions Architect, AWS

Traditional Network

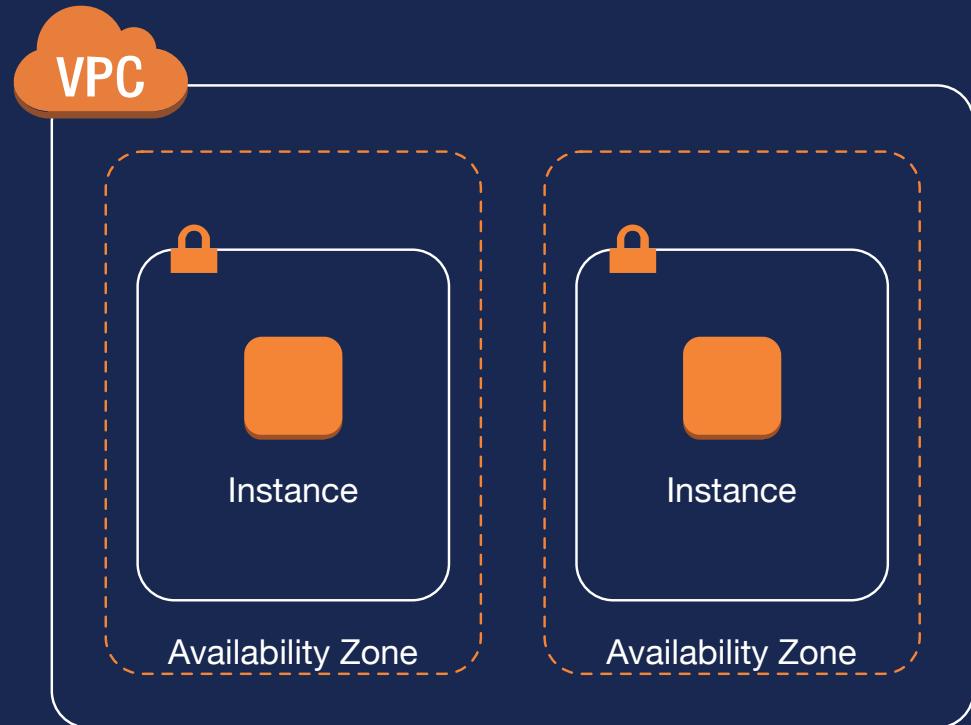


AWS Network



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

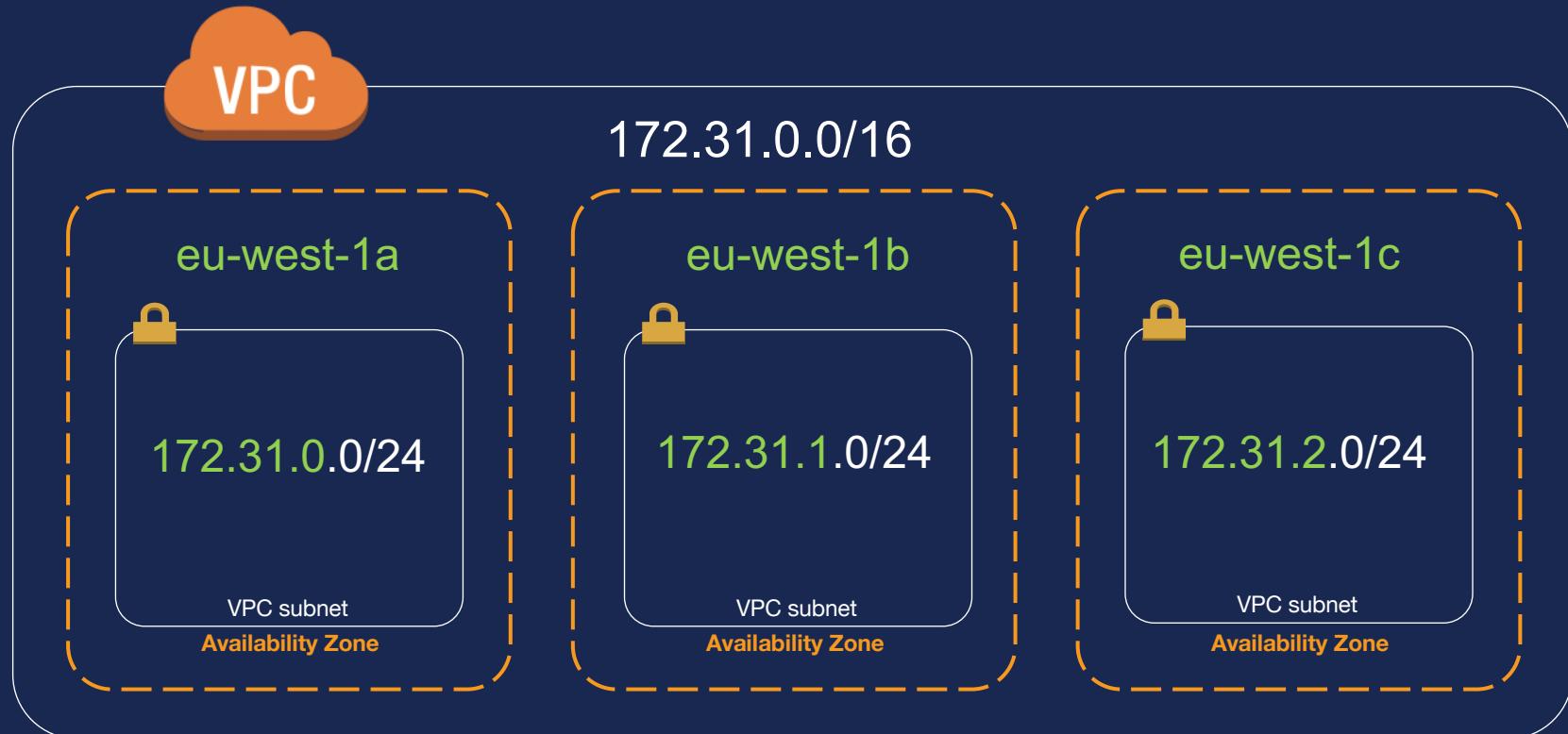
Amazon Global Unicast
Addresses (GUA) –
Internet Routable

Associate an /56 IPv6 CIDR
(Automatically allocated)



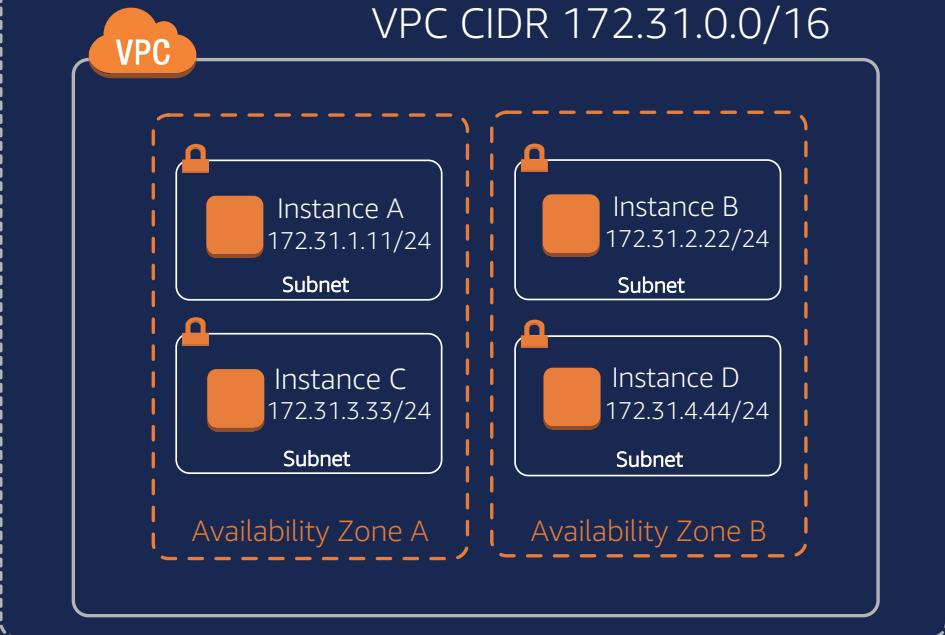
Subnets

VPC subnets and Availability Zones

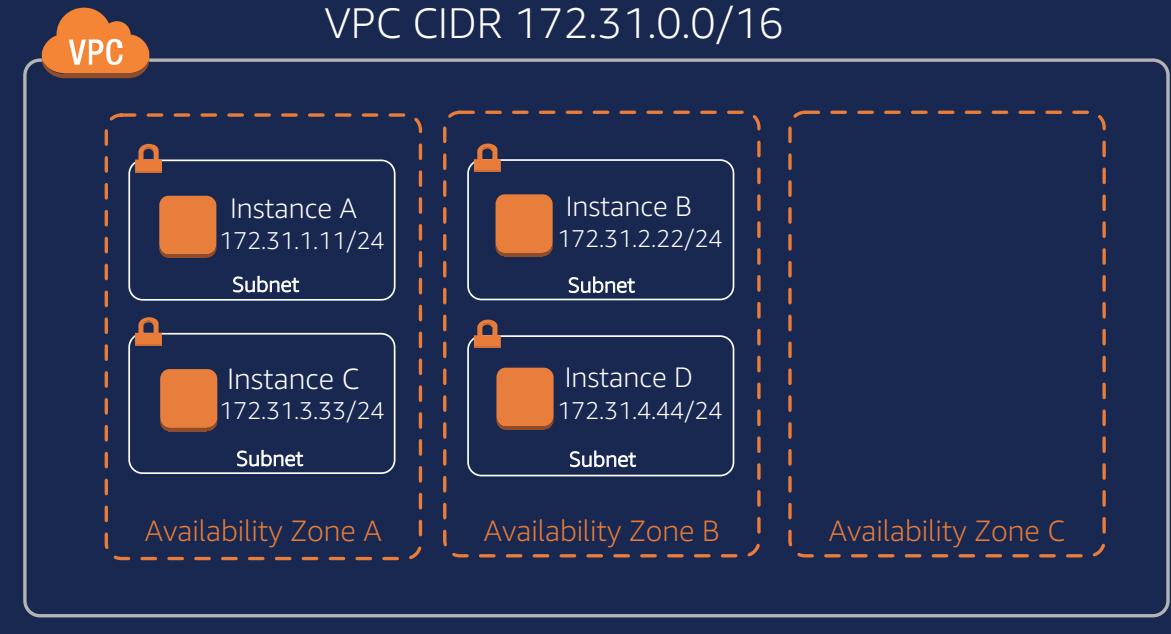


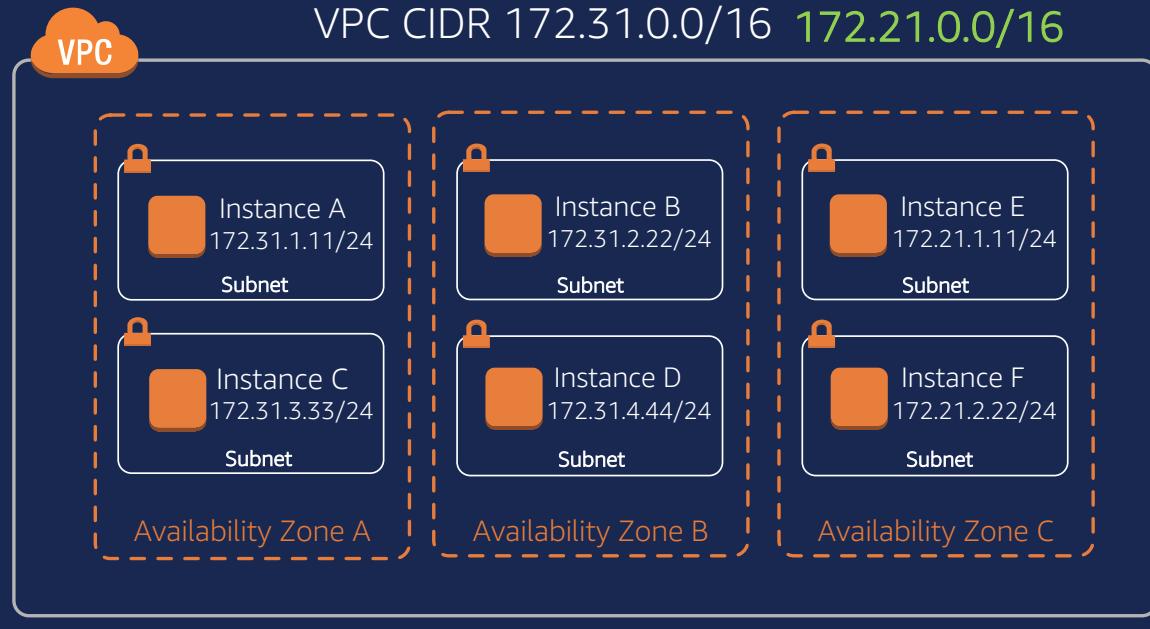
Expand your existing Amazon VPC

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

[Create Route Table](#) [Delete Route Table](#) [Set As Main Table](#)

Search Route Tables and their [X](#)

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associated	Main	VPC
<input checked="" type="checkbox"/>	rtb-04304e61	0 Subnets	Yes	vpc-327d1857 (172.31.0.0/16) ...	

rtb-04304e61

[Summary](#) [Routes](#) [Subnet Associations](#) [Route Propagation](#) [Tags](#)

[Cancel](#) [Save](#)

Destination	Target	Status	Propagated	Remove
172.31.0.0/16	local	Active	No	Remove

[Add another route](#)

Create Route Table **Delete Route Table** **Set As Main Table**

Search Route Tables and their X

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

rtb-04304e61

Summary **Cancel** **Tags**

Destination	Target	Status
172.31.0.0/16	local	Active
172.31.0.0/16	local	Active

Add another route

Traffic destined for my VPC stays in my VPC

Internet gateway

The screenshot shows the AWS VPC Internet Gateway management interface. At the top, there are four buttons: 'Create Internet Gateway' (blue), 'Delete' (grey), 'Attach to VPC' (grey), and 'Detach from VPC' (grey). Below this is a search bar with placeholder text 'Search Internet Gateways and' and a clear button 'X'. To the right of the search bar are navigation links '« « 1 to 1'.

The main table has columns: Name, ID, State, and VPC. A checkbox header is present for the first column. The table contains one row for an internet gateway named 'igw-3376c756' with ID 'igw-3376c756', state 'attached', and VPC 'vpc-327d1857 (172.31.0.0/16) | ...'. A large grey arrow points from the text in the callout box to the 'igw-3376c756' link in the table.

igw-3376c756

Summary **Tags**

ID: igw-3376c756 Attached VPC ID: [vpc-327d1857 \(172.31.0.0/16\)](#) | Demo VPC
State: attached Attachment state: available

Send packets here if you want them to reach the Internet

Create Route Table

Delete Route Table

Set As Main Table

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

Associate

Main

VPC

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

rtb-04304e61

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

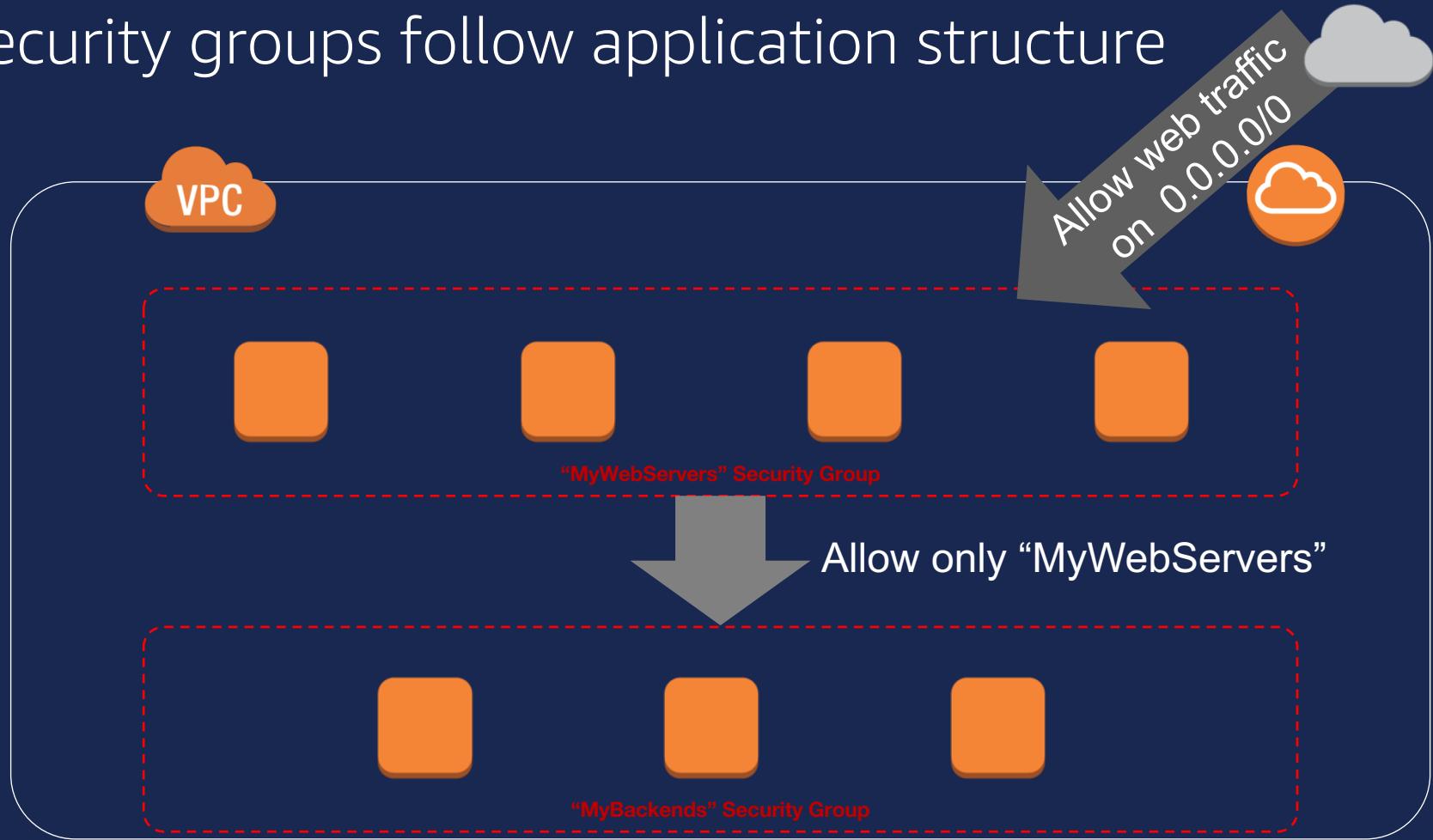
172.31.0.0/16 local Active No

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

The screenshot shows the AWS VPC Security Groups console. At the top, there is a search bar with the text "search : vpc-5999ce3e" and a "Create Security Group" button. Below the search bar is a table with columns: Name, Group ID, Group Name, VPC ID, and Description. The table contains three rows:

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

A callout bubble points to the "WebServersGroup" row with the text "Allow all HTTP traffic". Below the table, a modal window is open for the "WebServersGroup". The modal has tabs for "Description", "Inbound" (which is selected), "Outbound", and "Tags". The "Inbound" tab shows two rules:

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...

A callout bubble points to the "Description" column of the second rule with the text "Rule descriptions".

Security groups example: Backends

The screenshot shows the AWS Security Groups console. At the top, there is a search bar with the text "vpc-5999ce3e" and a "Create Security Group" button. Below the search bar is a table with columns: Name, Group ID, Group Name, VPC ID, and Description. The table contains three rows:

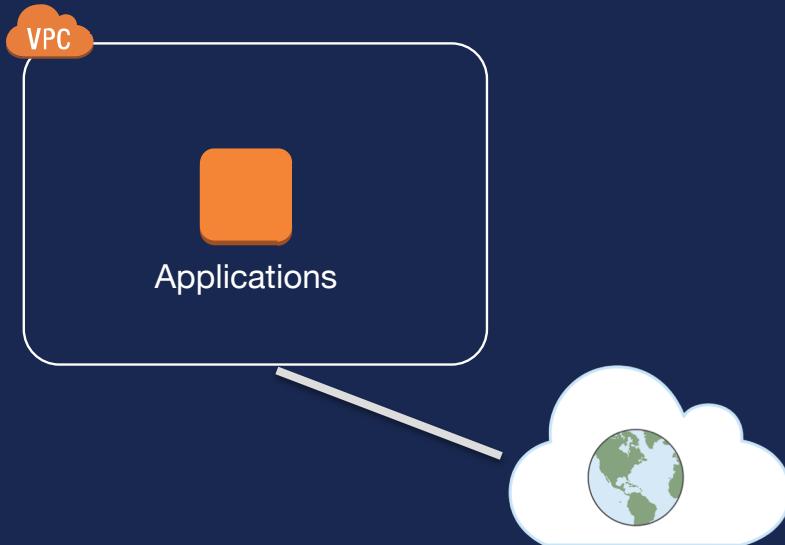
Name	Group ID	Group Name	VPC ID	Description
WebServersGroup	sg-067c927d	MyWebServers	vpc-5999ce3e	Group for web servers
BackendsGroup	sg-aa7896d1	MyBackends	vpc-5999ce3e	Group for backend hosts

A tooltip with the text "Allow application traffic from web servers only" points to the "MyBackends" security group. Below the table, a modal window is open for the "BackendsGroup" security group. The modal has tabs for "Description", "Inbound", "Outbound", and "Tags". The "Inbound" tab is selected, showing a table of rules:

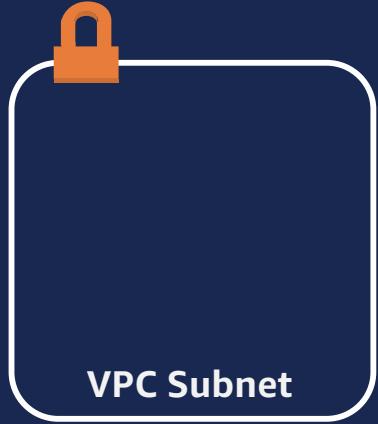
Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	2345	sg-067c927d (MyWebServers)	Allow traffic from...

Below the modal, another instance of the same table is shown, indicating that the rule has been applied.

AWS Network - Progress



Beyond Internet connectivity

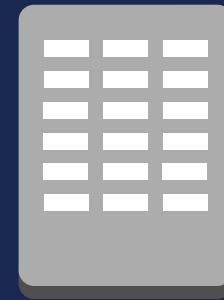


VPC Subnet

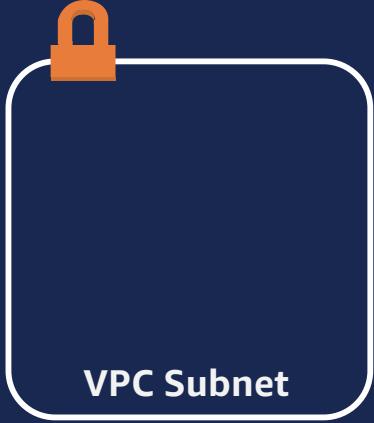
Restricting
Internet access



Connecting to other
VPCs

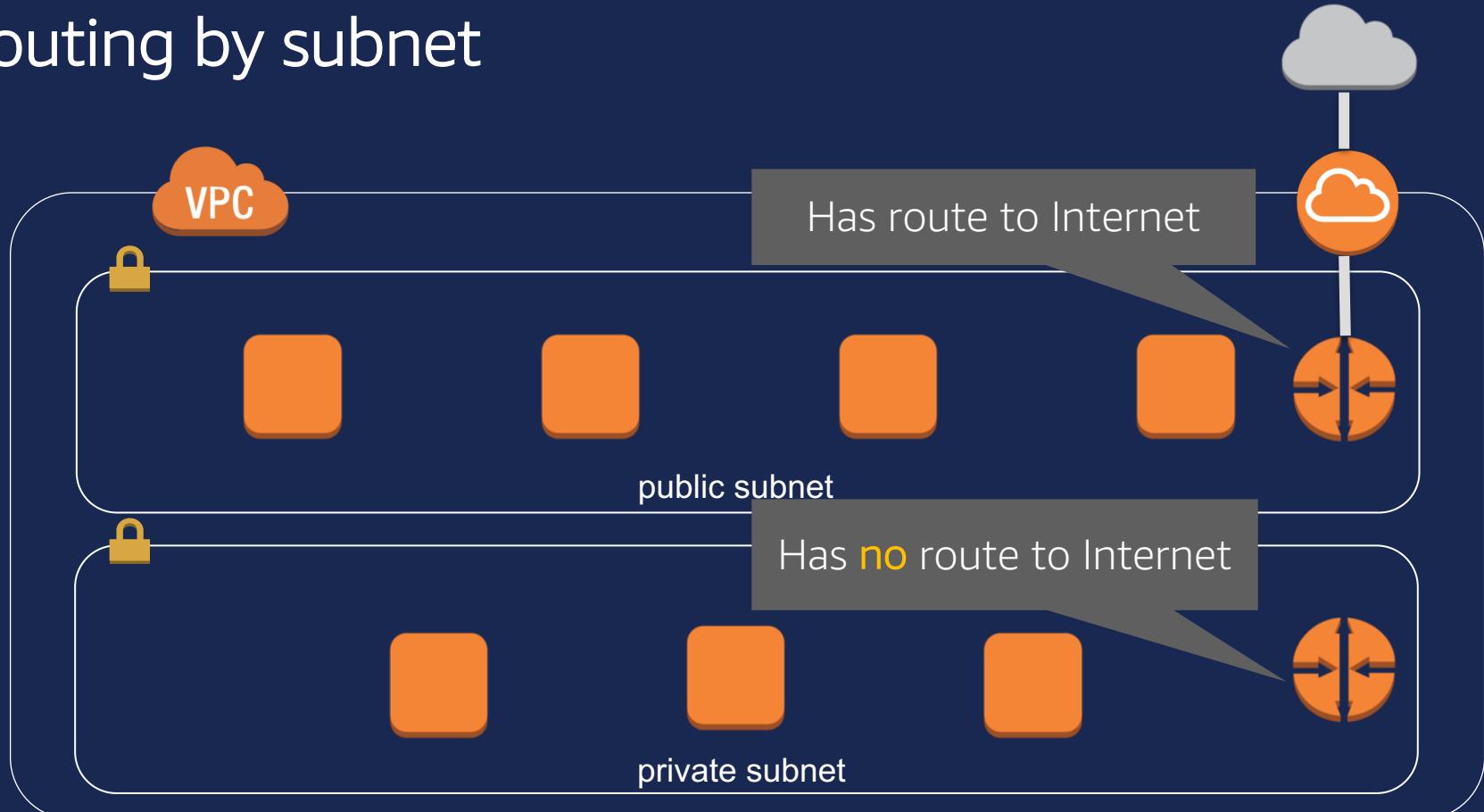


Connecting to your
corporate network

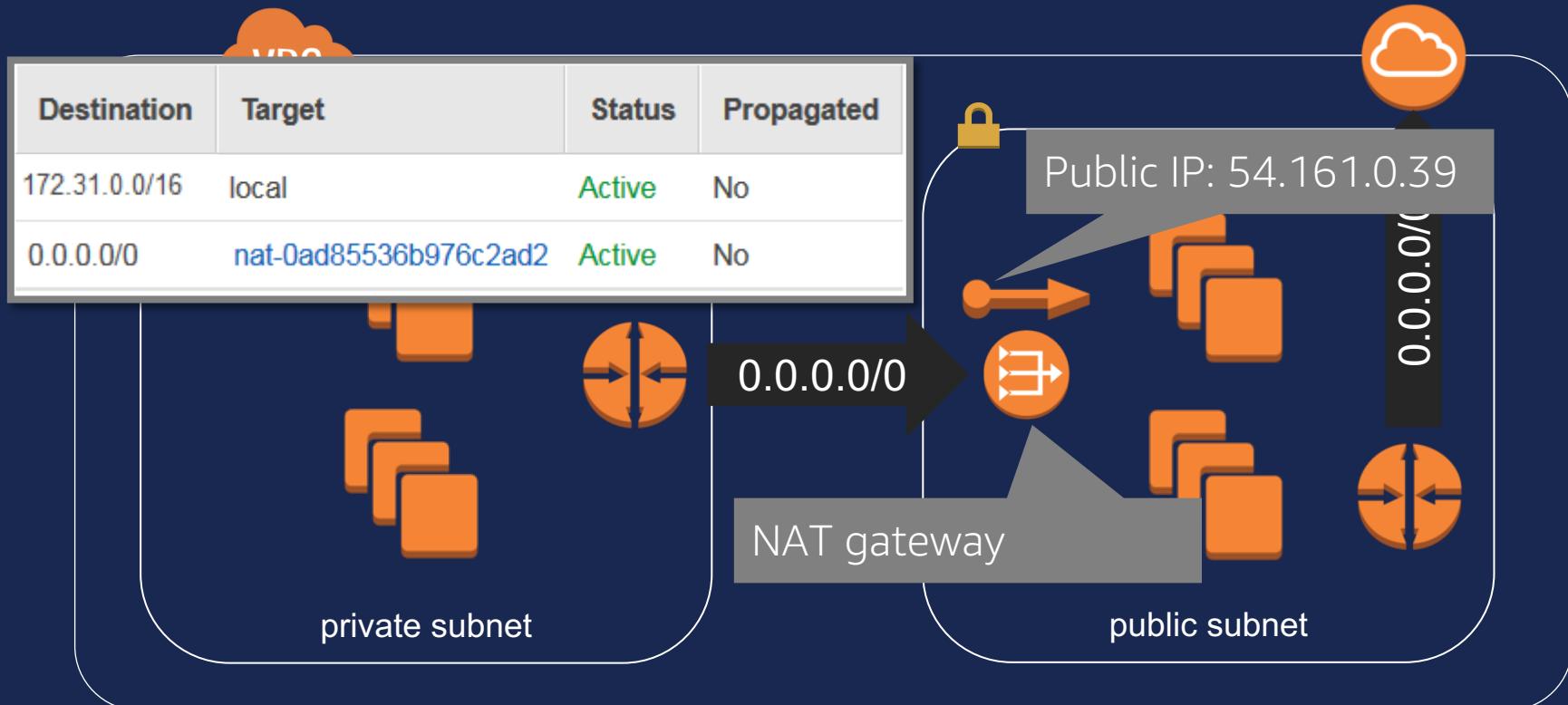


Restricting Internet access: Routing by subnet

Routing by subnet



Outbound-only internet access: NAT gateway

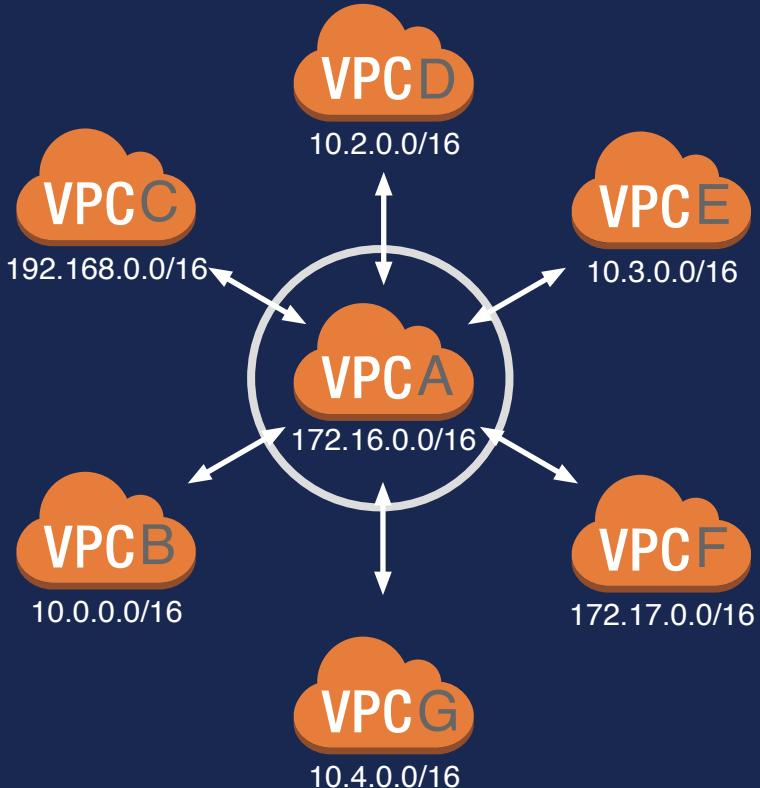




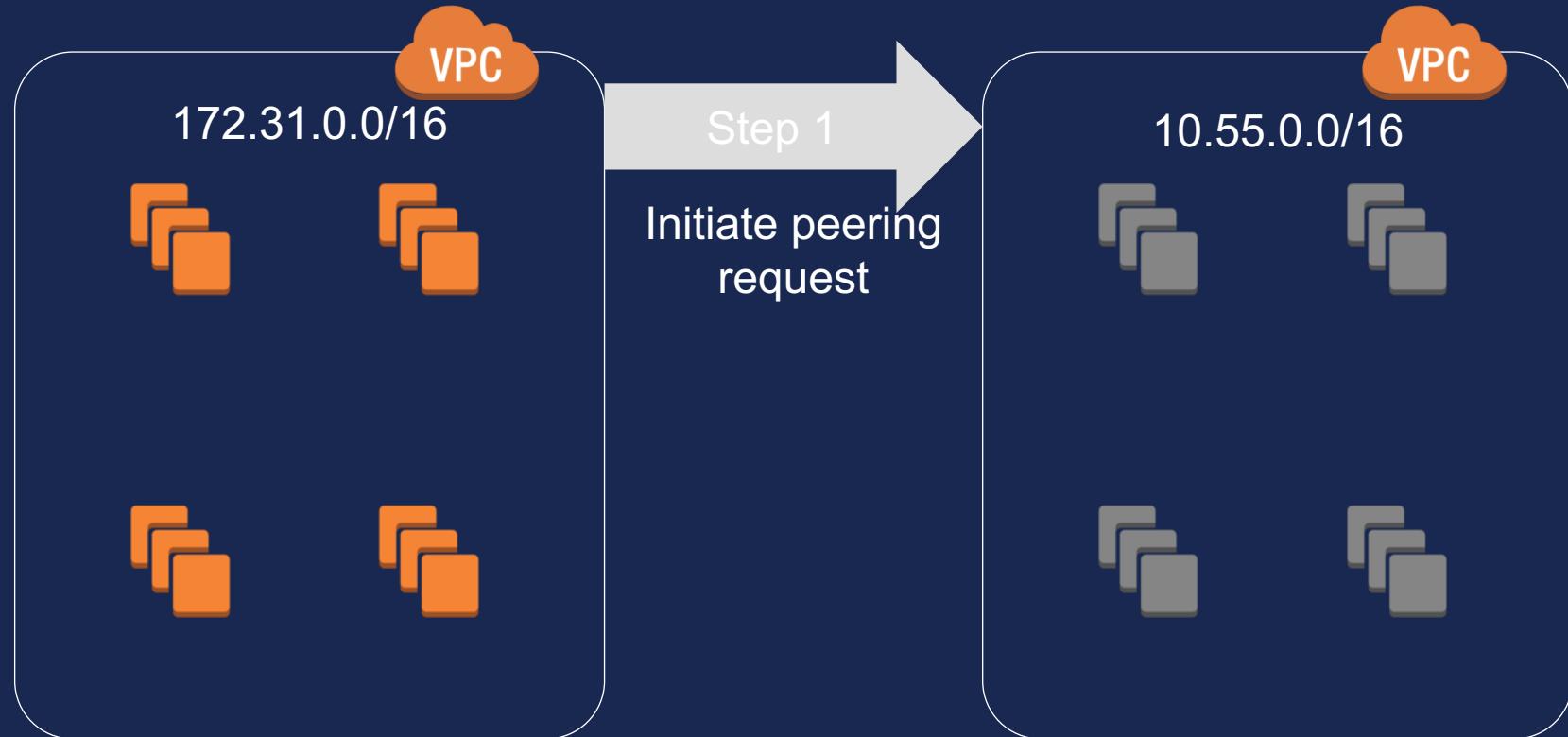
Inter-VPC connectivity: VPC peering

Example VPC peering use: Shared services VPC

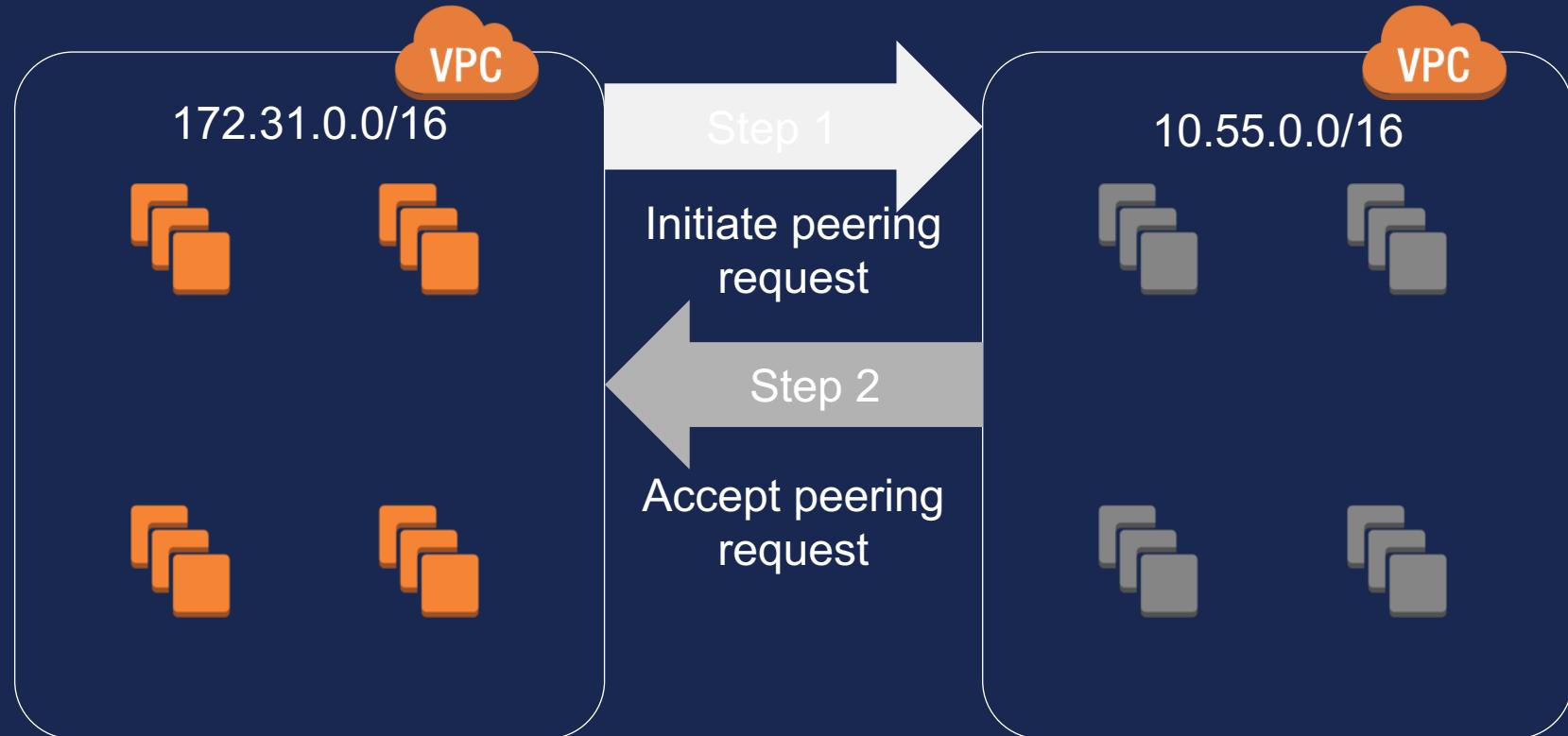
- Common/core services
 - Authentication/directory
 - Monitoring
 - Logging
 - Remote administration
 - Scanning



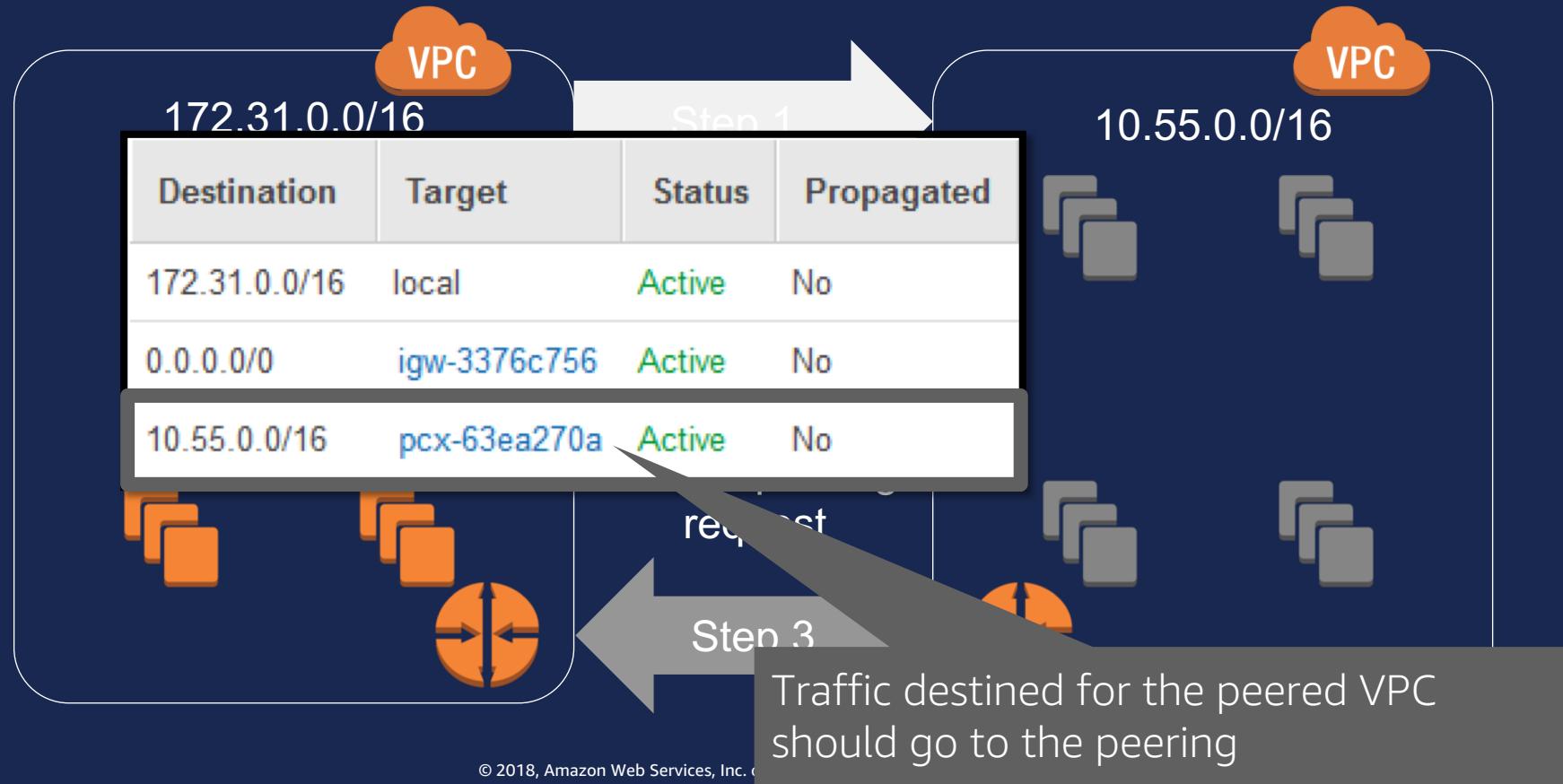
Establish a VPC peering: Initiate request



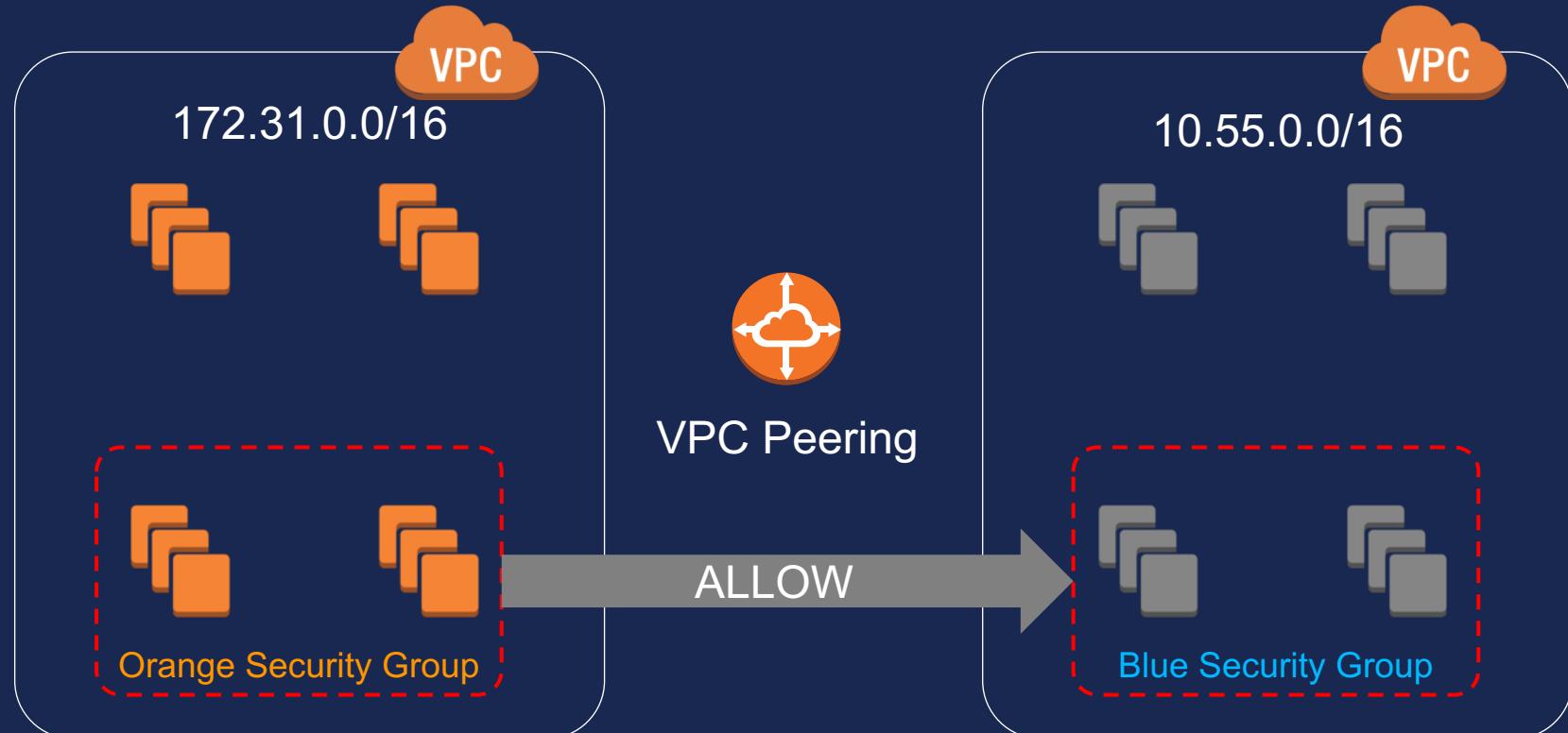
Establish a VPC peering: Accept request



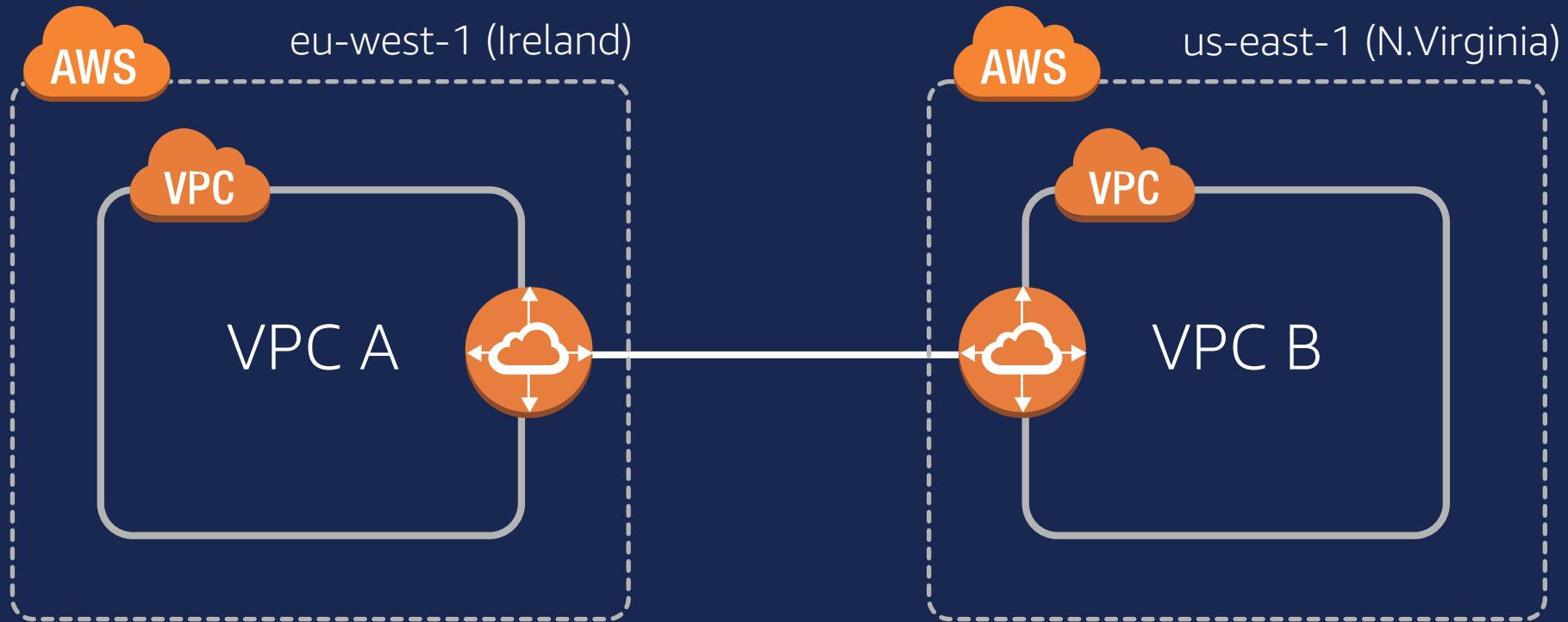
Establish a VPC peering: Create a route



Security groups across peered VPCs



Inter-Region VPC Peering

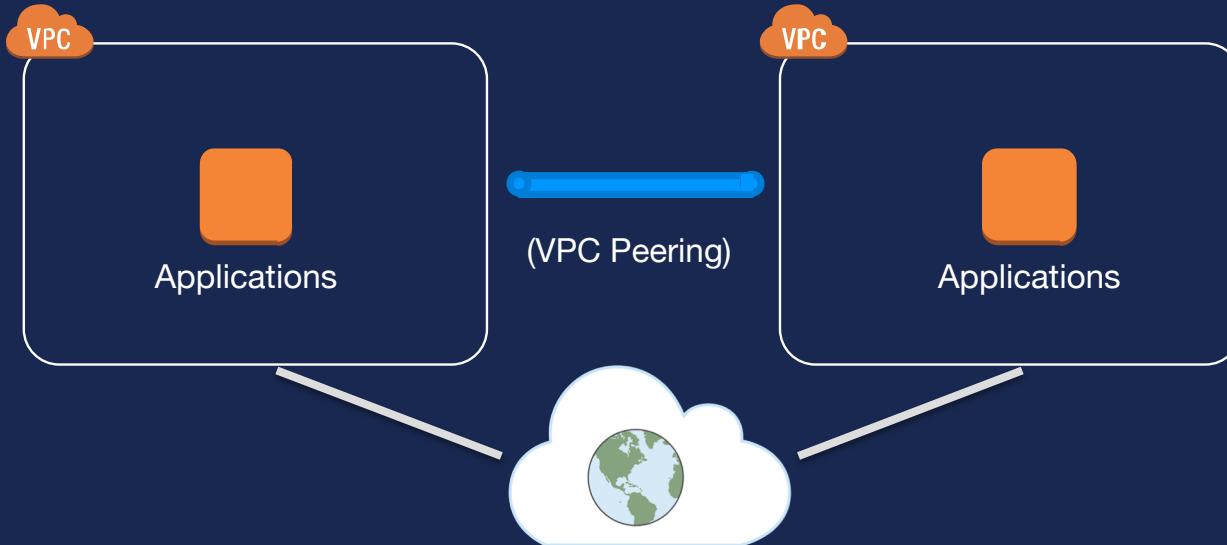


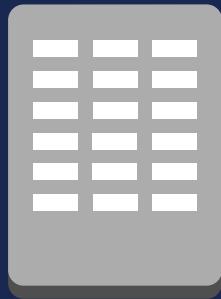
Some notes...

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

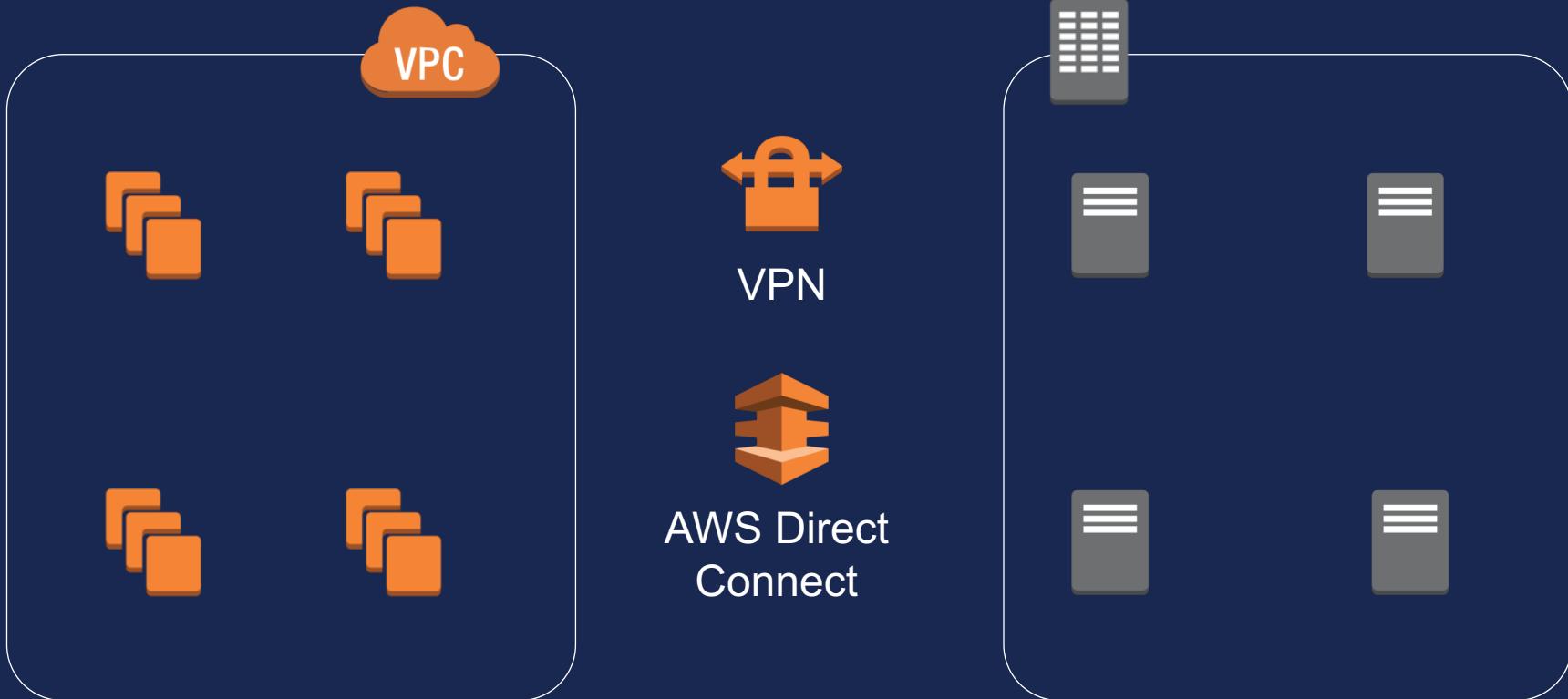
AWS Network - Progress



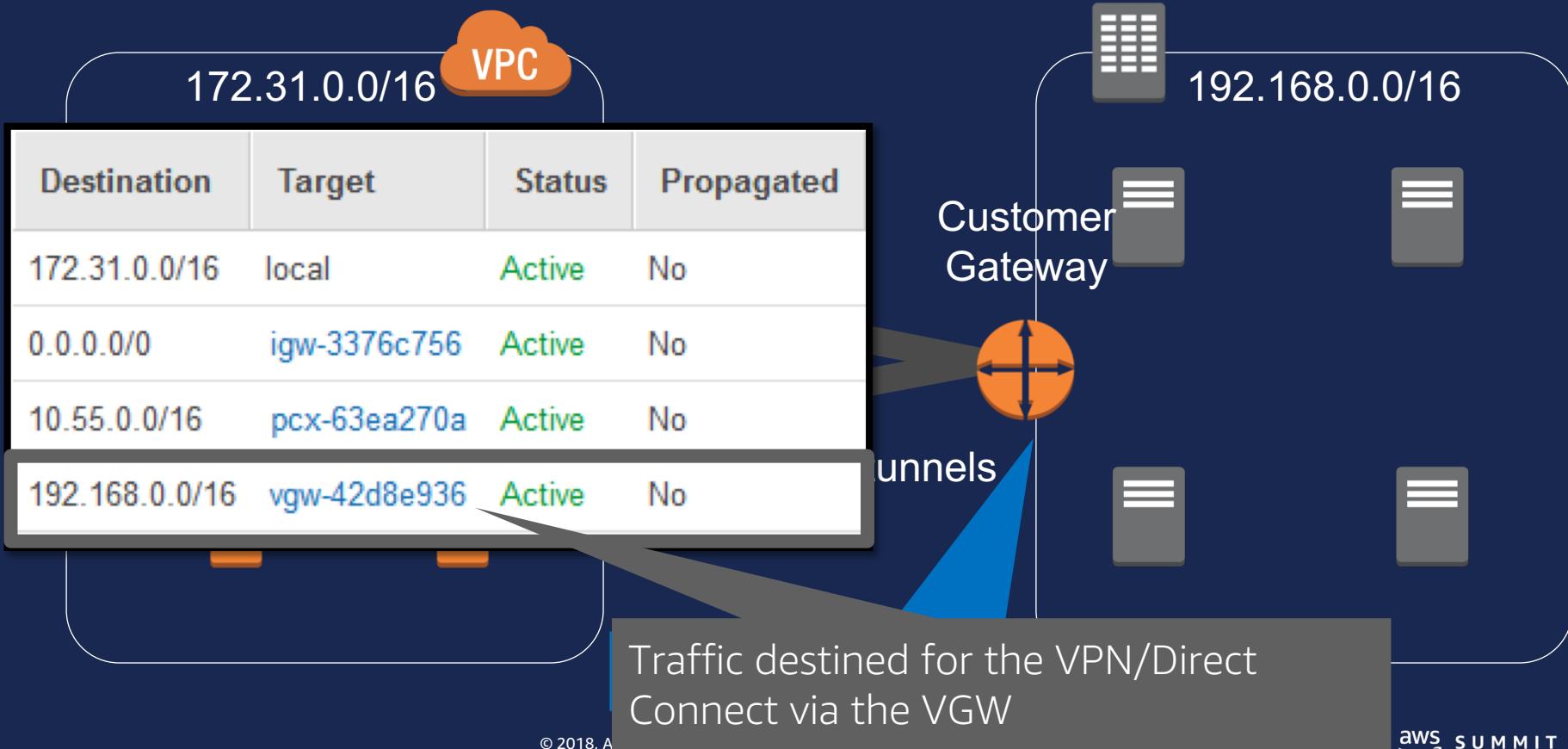


Connecting to on-premises networks: AWS Virtual Private Network and AWS Direct Connect

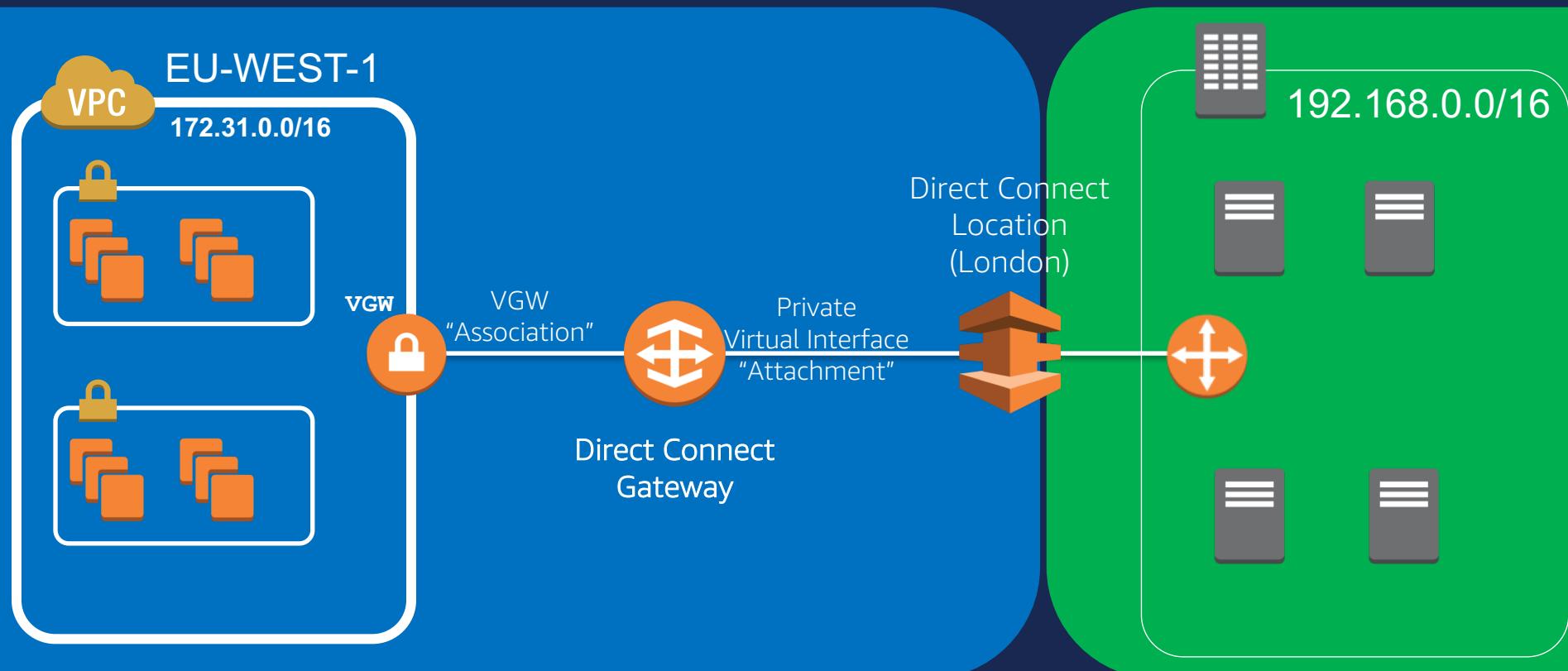
Extend an on-premises network into your VPC



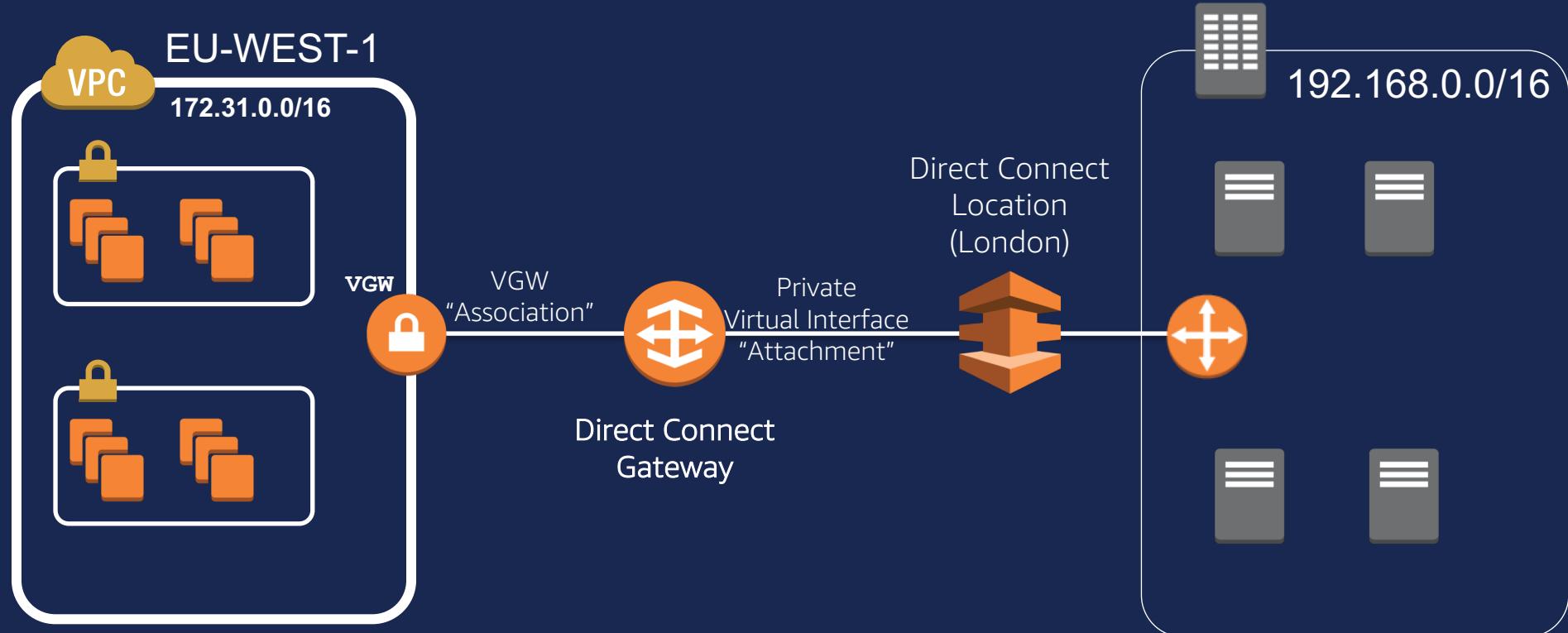
AWS VPN basics



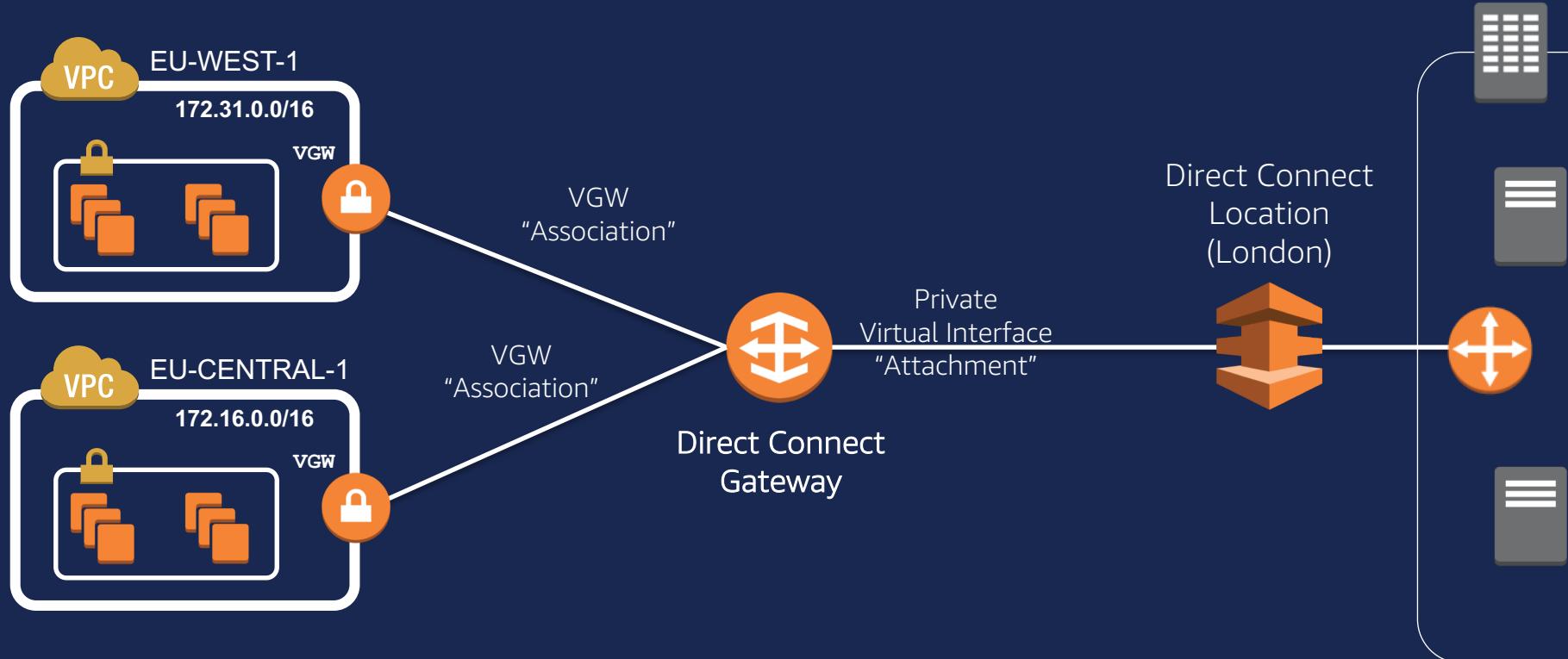
AWS Direct Connect Gateway



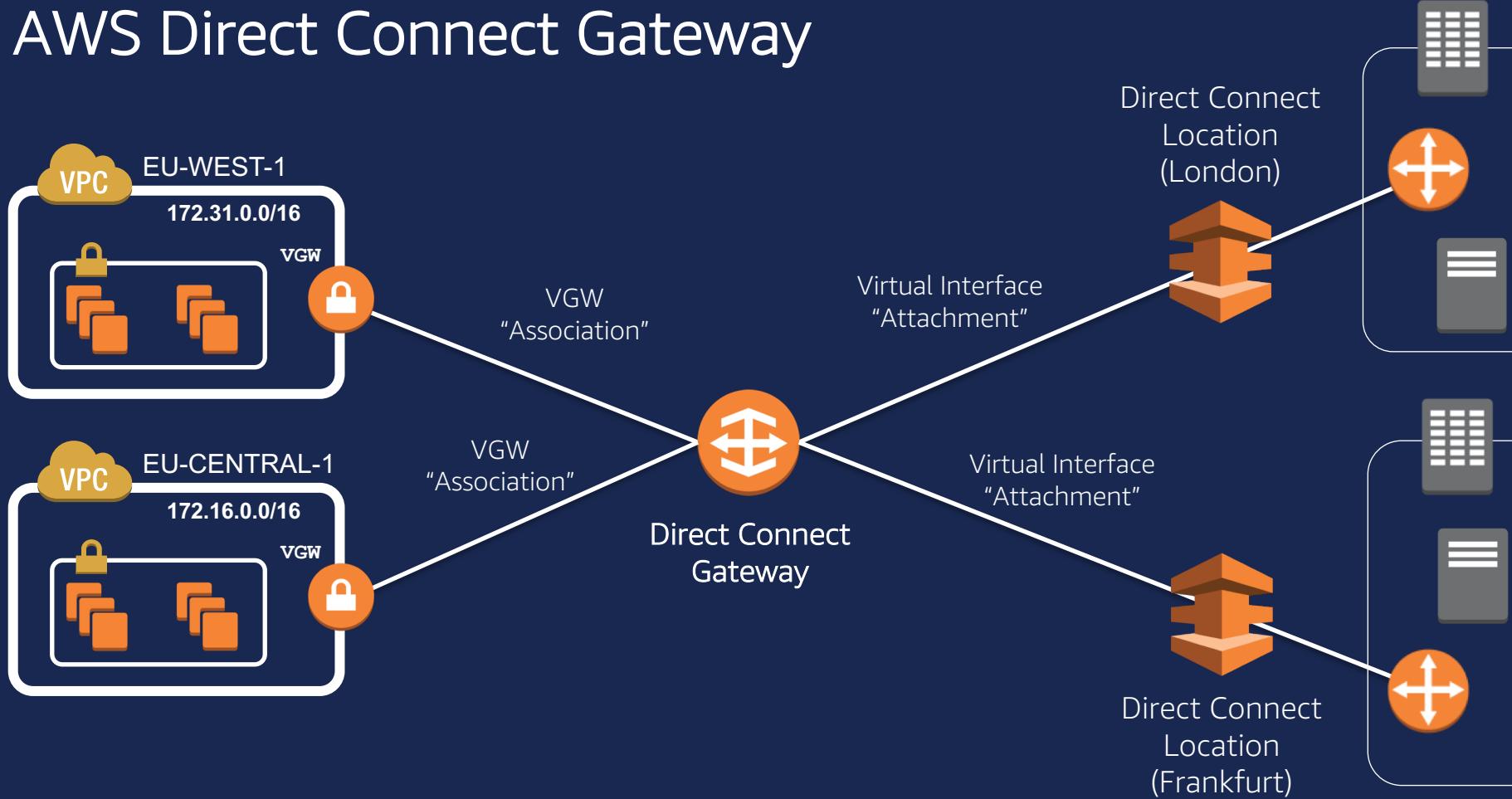
AWS Direct Connect Gateway



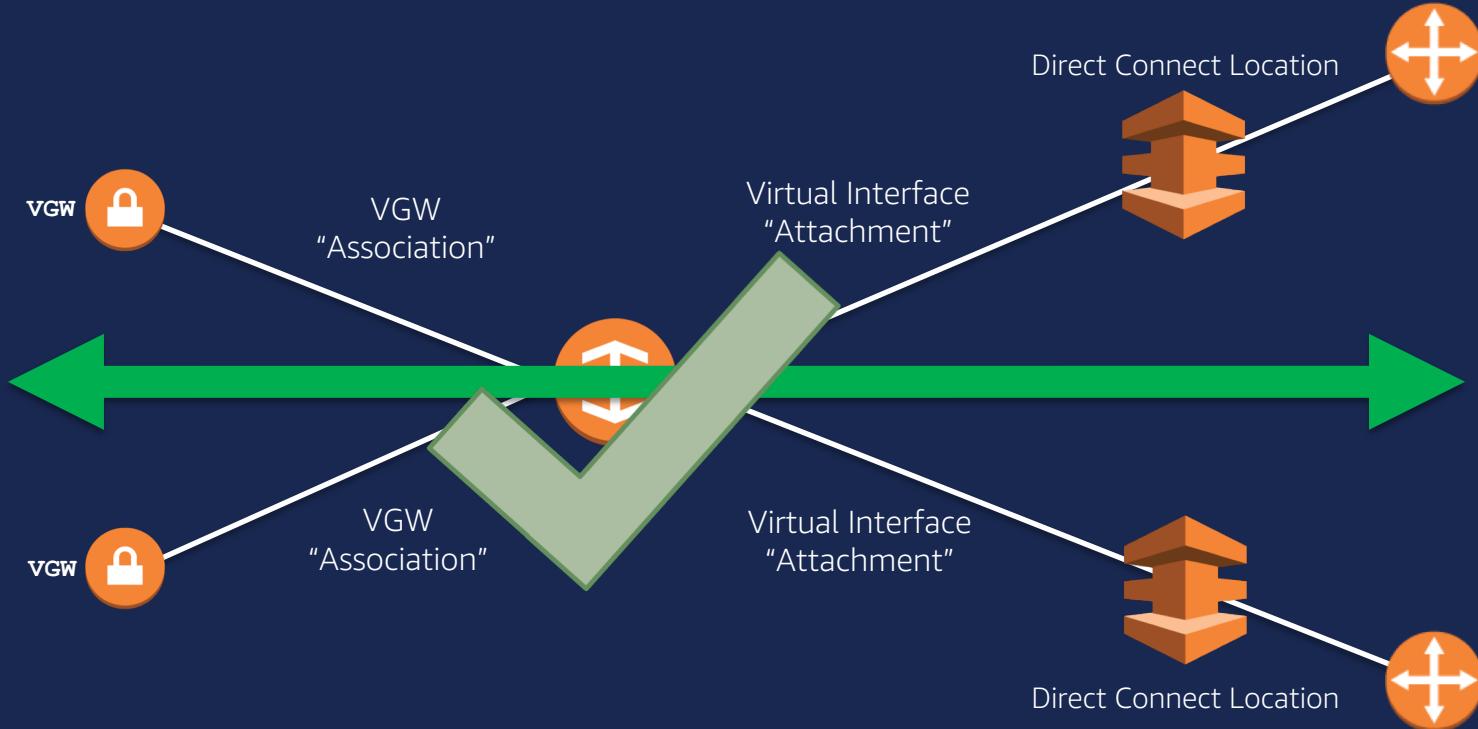
AWS Direct Connect Gateway



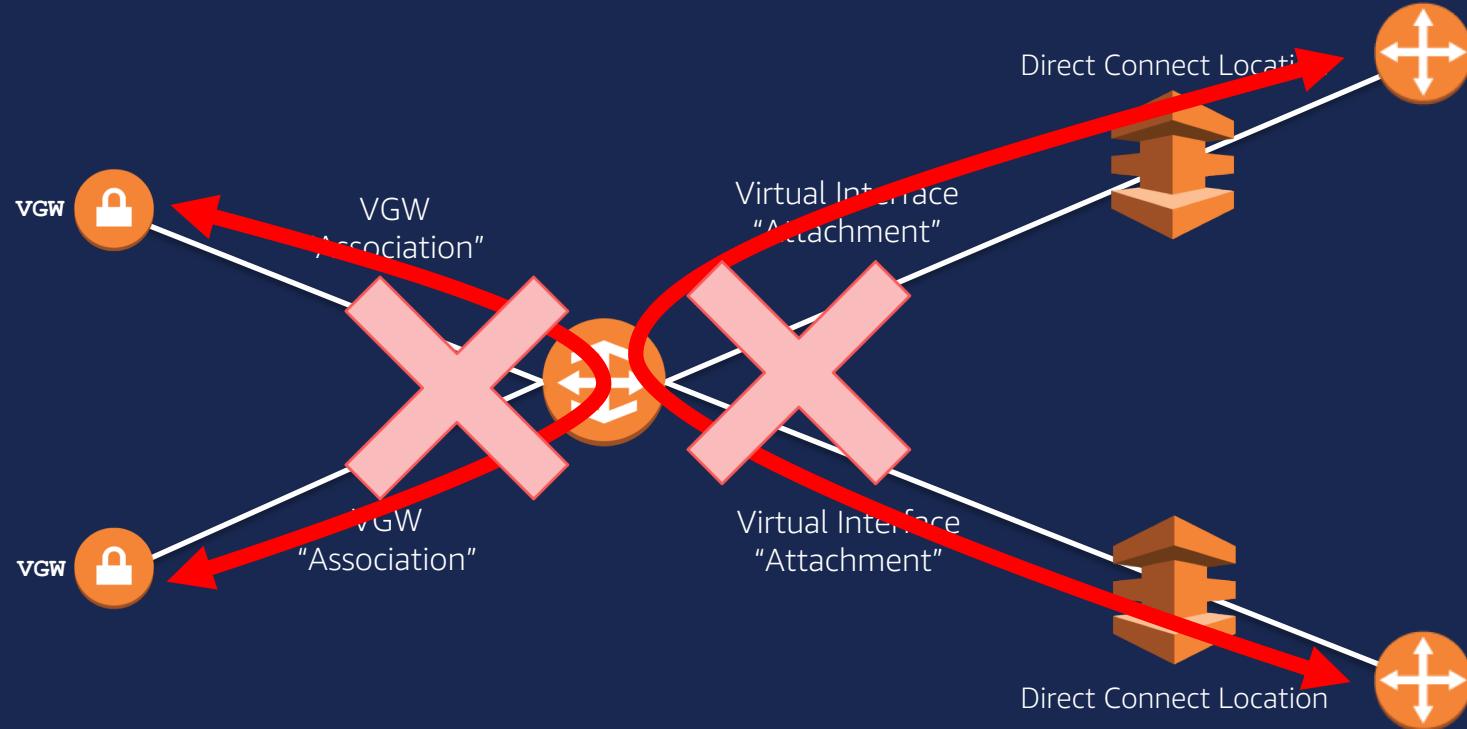
AWS Direct Connect Gateway



Direct Connect Gateway—traffic flows



Direct Connect Gateway—traffic flows

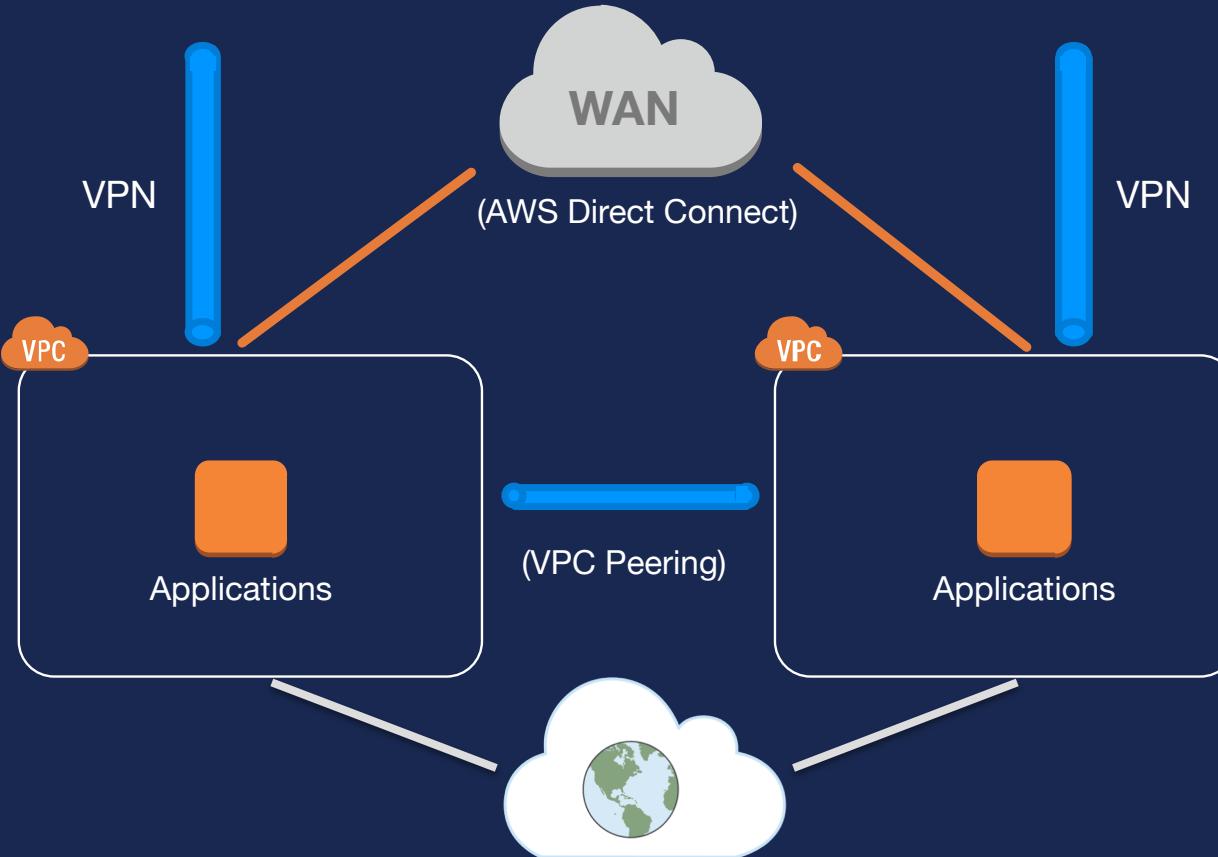


AWS VPN and AWS Direct Connect

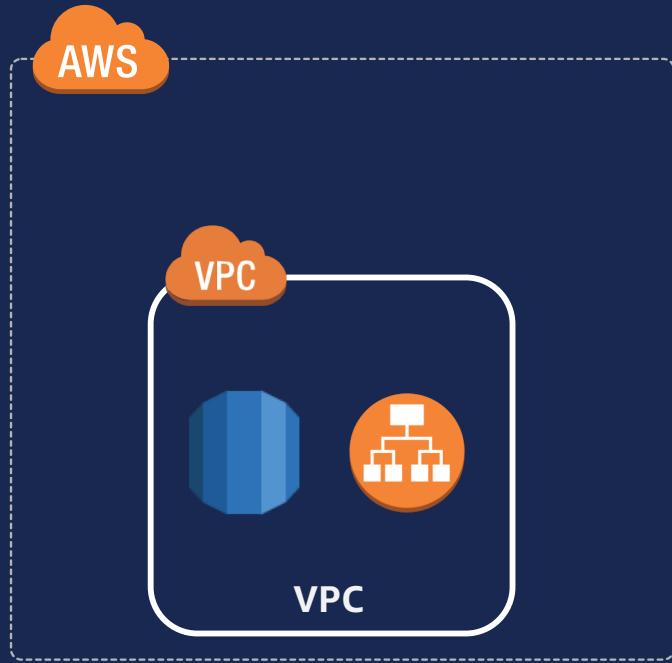
- Both allow **secure connections** between your network and your VPC
- **VPN** is a pair of IPSec tunnels over the Internet
- **AWS Direct Connect** is a dedicated line with lower per-GB data transfer rates
- For **highest availability**: Use both



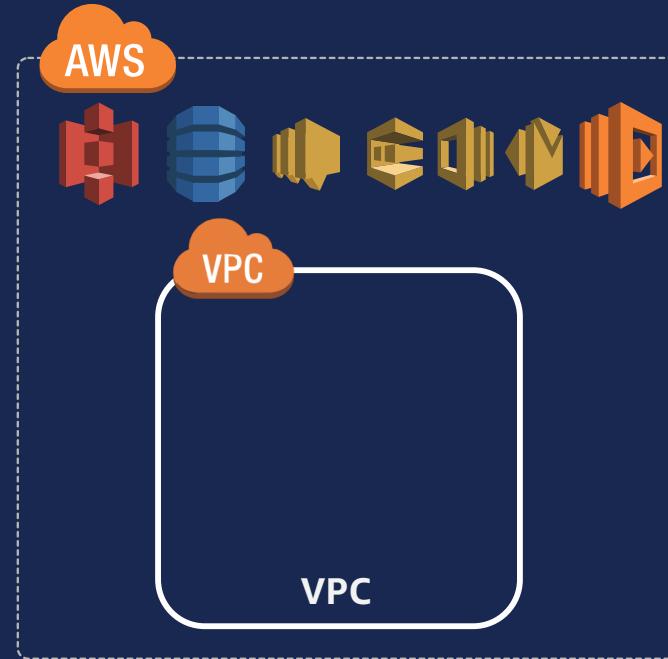
AWS Network - Progress



AWS Services



Inside of the VPC

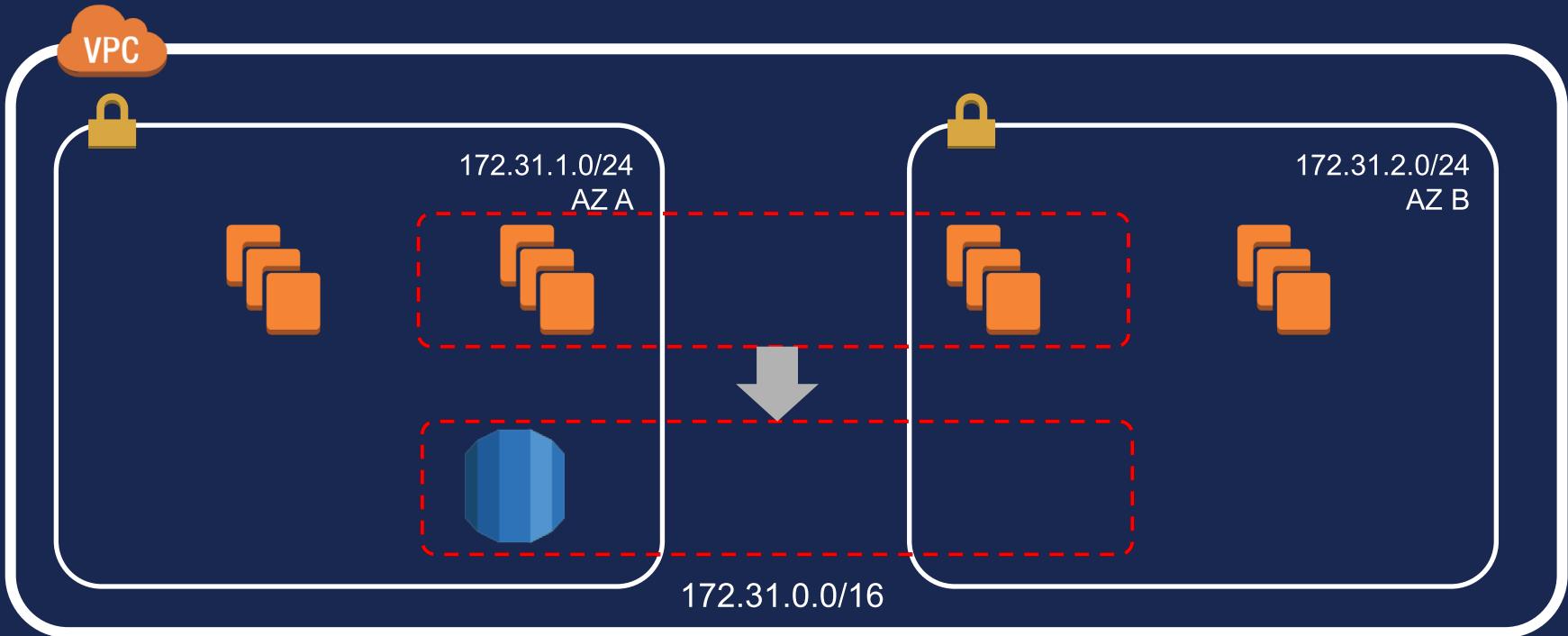


Outside of the VPC

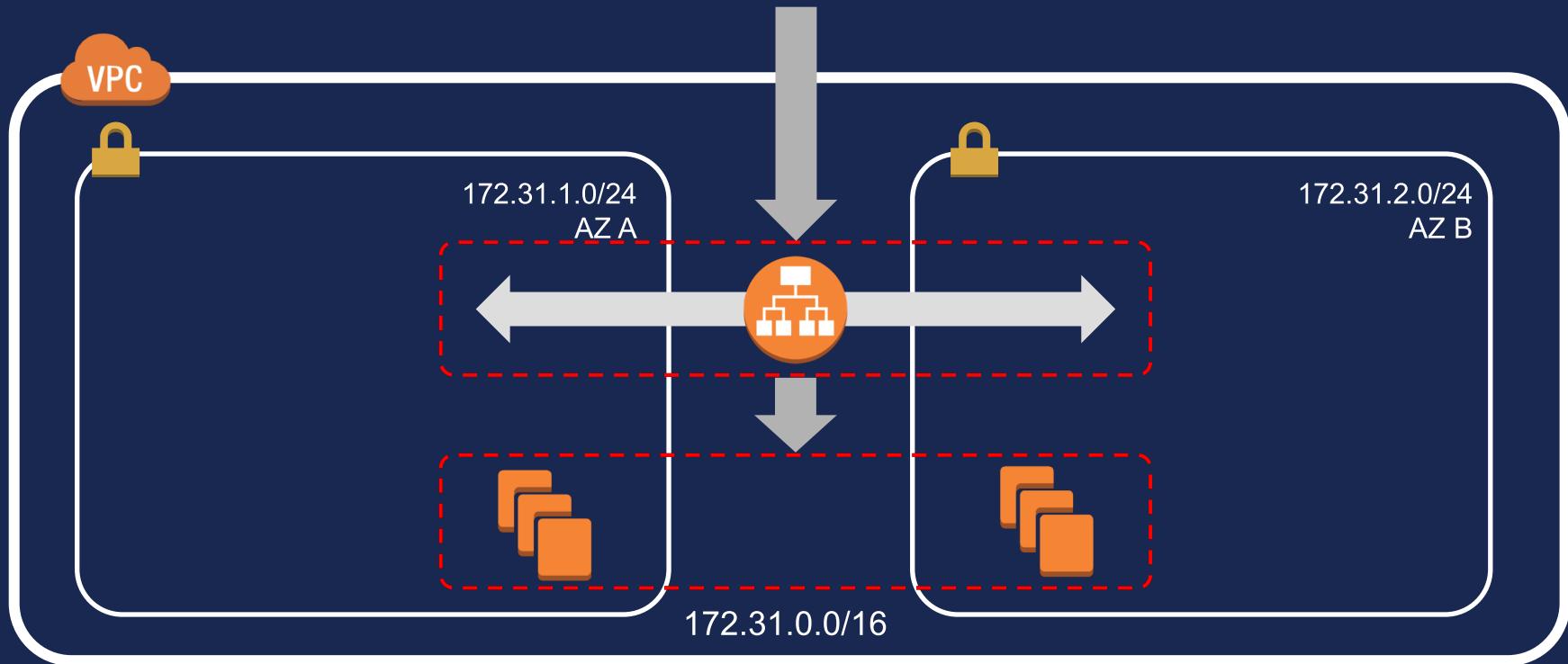


AWS Services in your VPC

Example: Amazon RDS Database in your VPC



Example: Application Load Balancer in your VPC



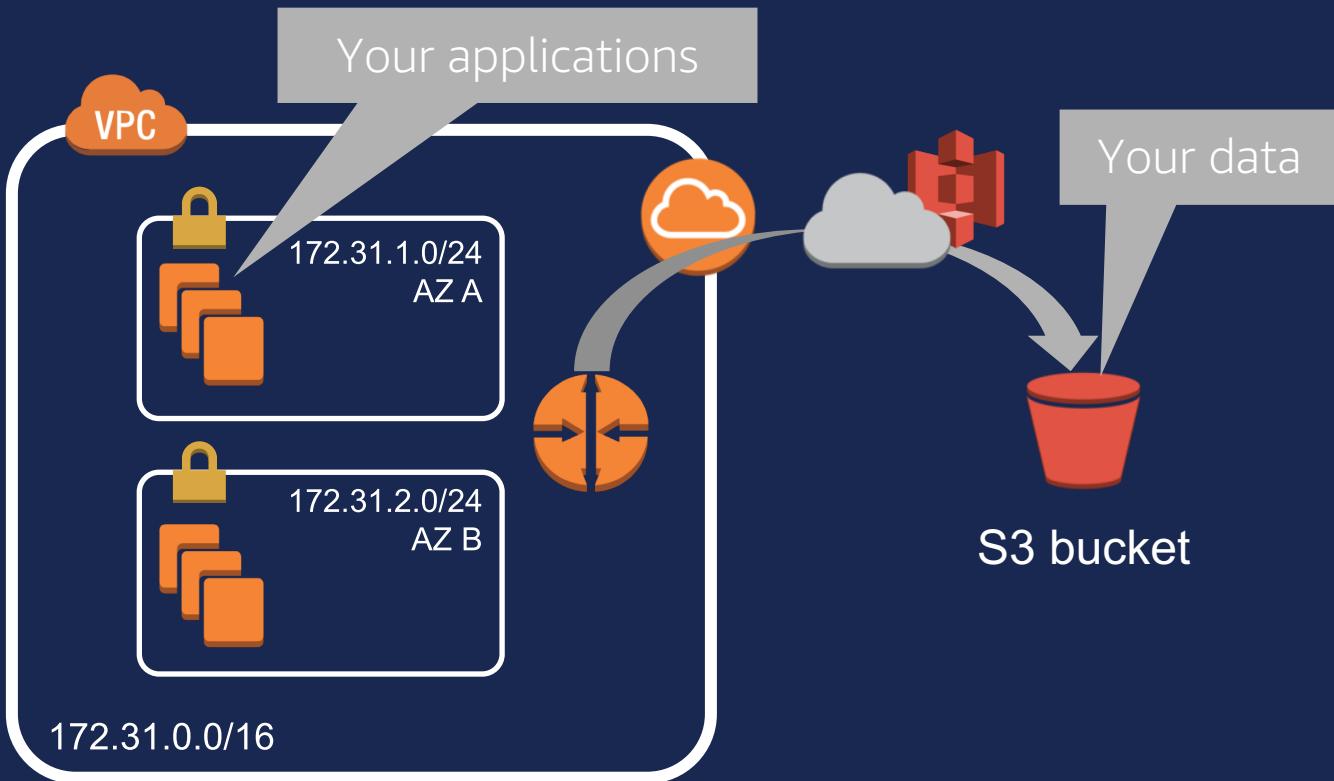


AWS Services outside your VPC



Endpoints for AWS Services

Amazon S3 and your VPC



Gateway VPC Endpoints

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 [i](#)

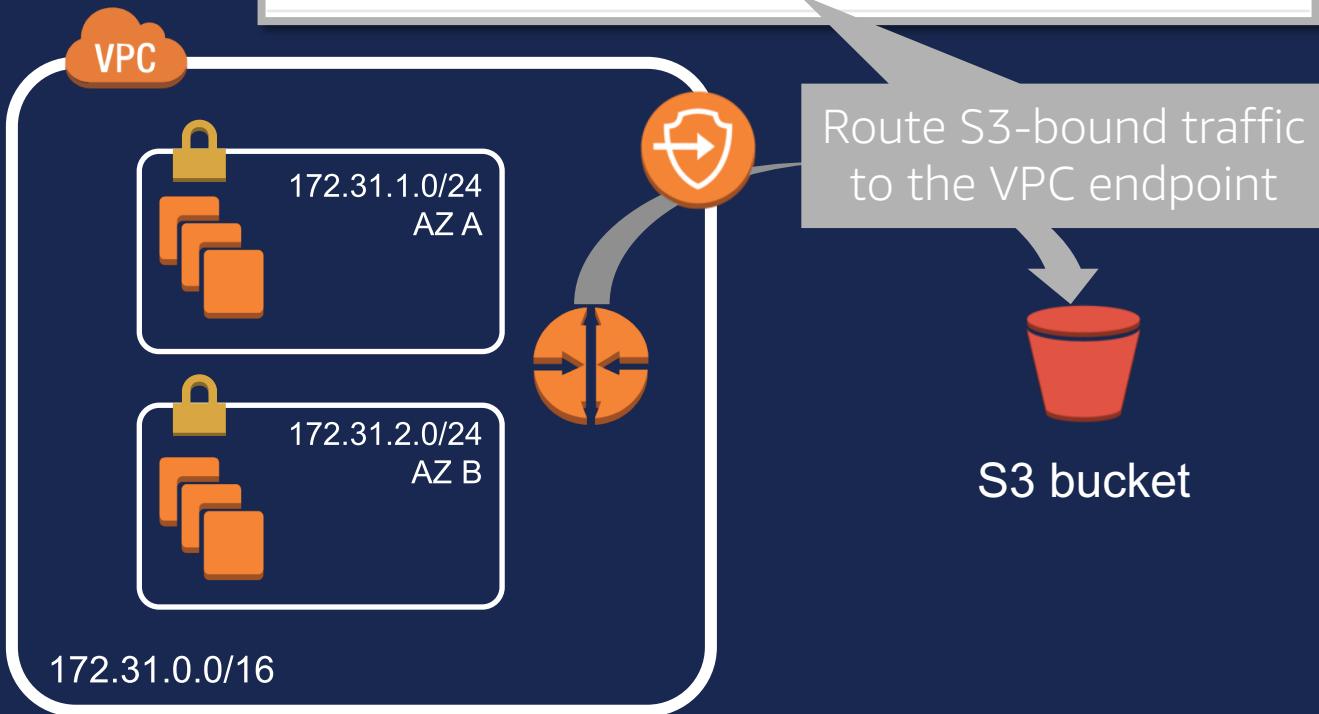
Service Name	Owner	Type
com.amazonaws.eu-west-1.dynamodb	amazon	Gateway
com.amazonaws.eu-west-1.ec2	amazon	Interface
com.amazonaws.eu-west-1.ec2messages	amazon	Interface
com.amazonaws.eu-west-1.elasticloadbalancing	amazon	Interface
com.amazonaws.eu-west-1.kinesis-streams	amazon	Interface
com.amazonaws.eu-west-1.s3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

VPC* [C](#) [i](#)

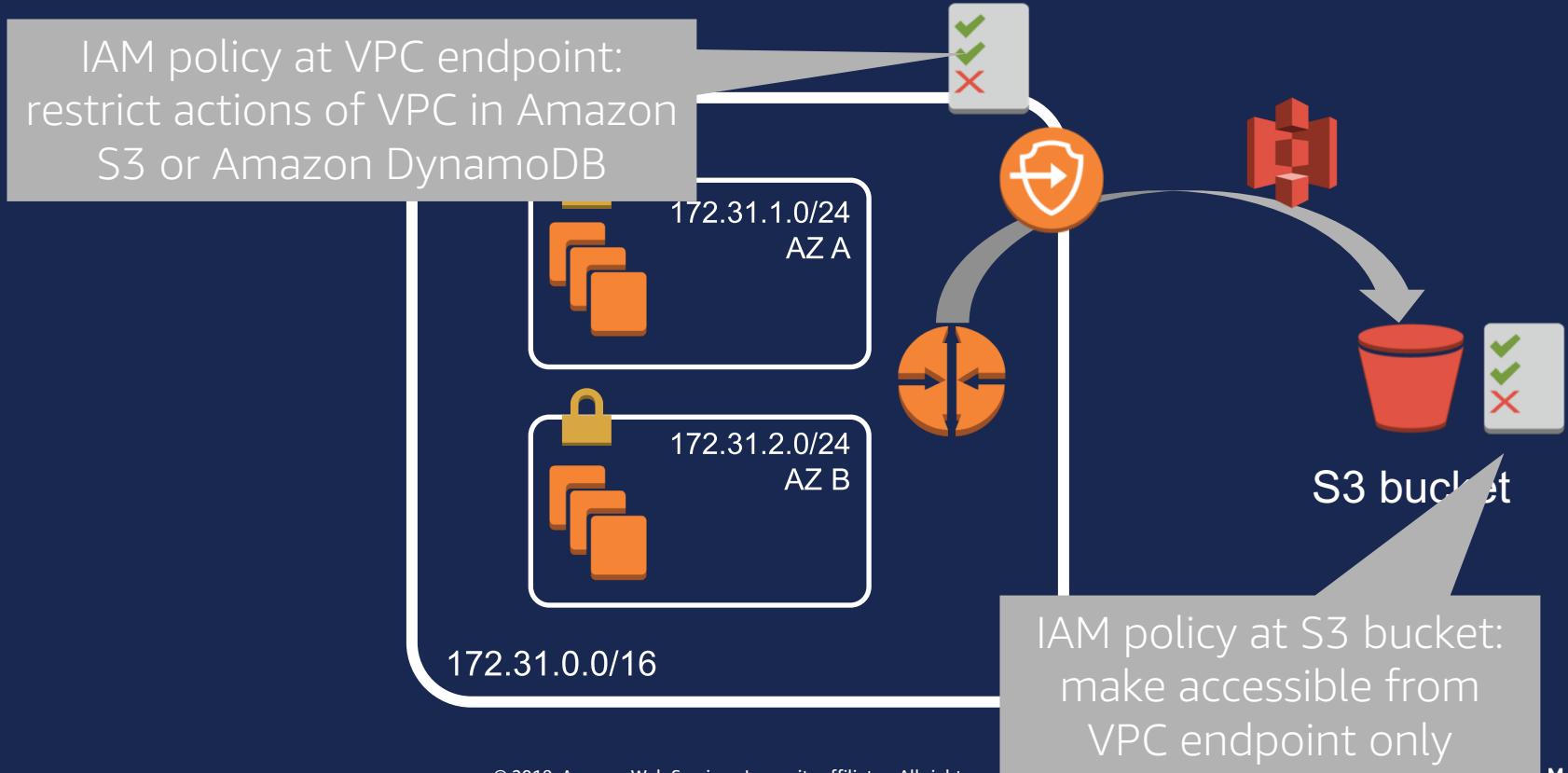
* Required [Cancel](#) [Create endpoint](#)

VPC Endpoints: Amazon 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



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.

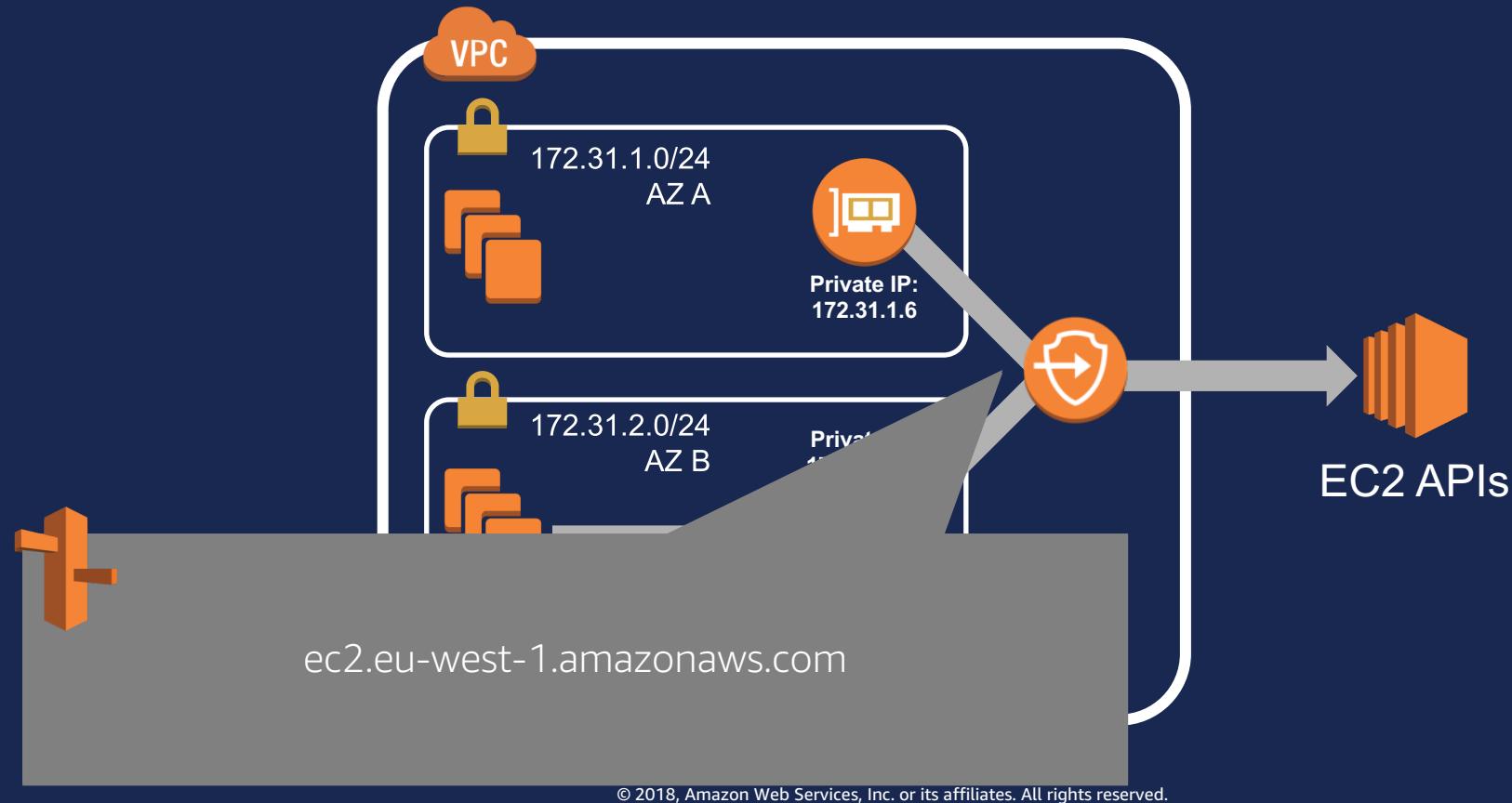
Service Name Select a service [i](#)

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* [C](#) [i](#)

* Required [Cancel](#) [Create endpoint](#)

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



Vanguard®



APPDYNAMICS



Expedia®



cisco
Stealthwatch
Cloud



aqua

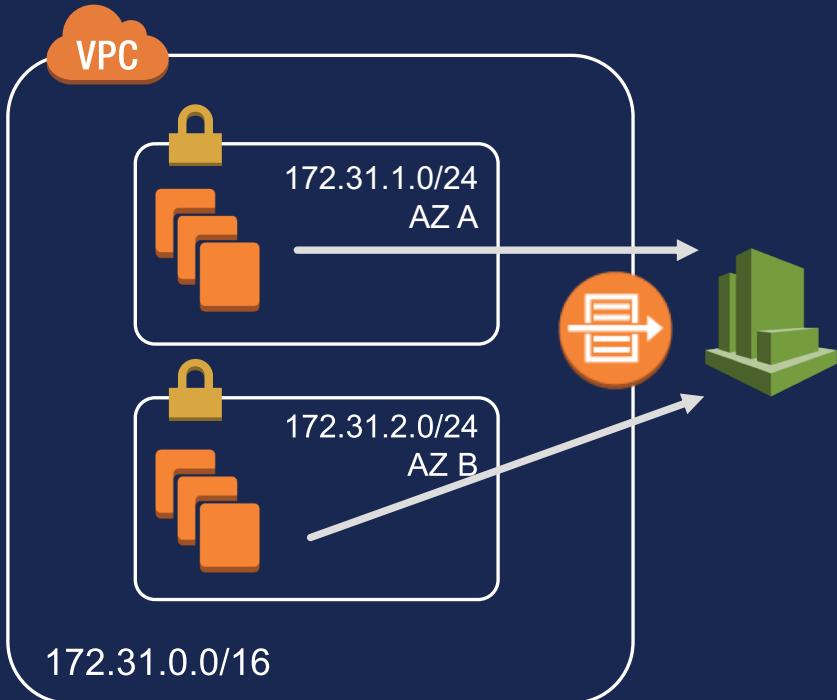
Alfresco®

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

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 to monitor traffic.

Create Flow Log

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

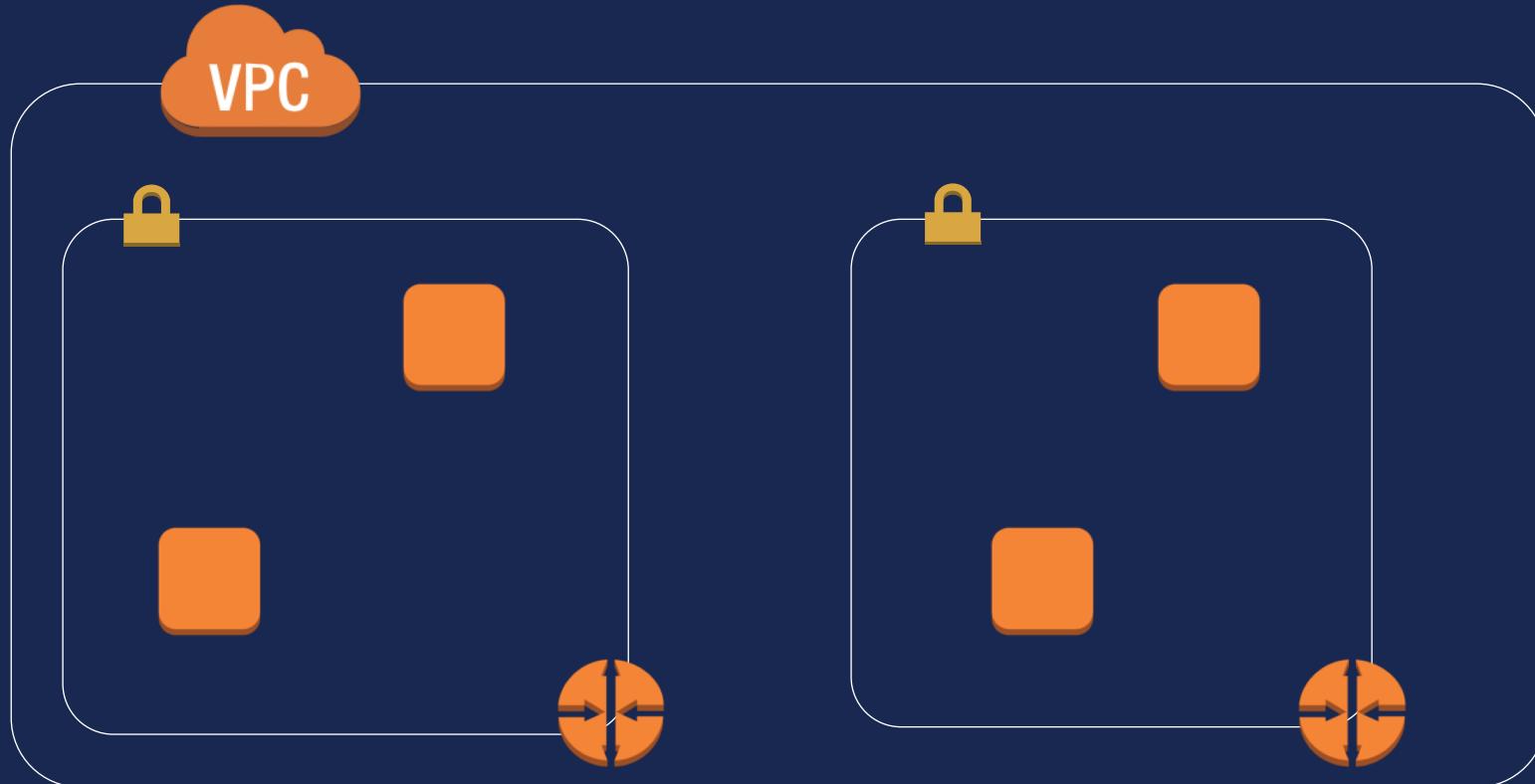
VPC traffic metadata captured in Amazon CloudWatch Logs



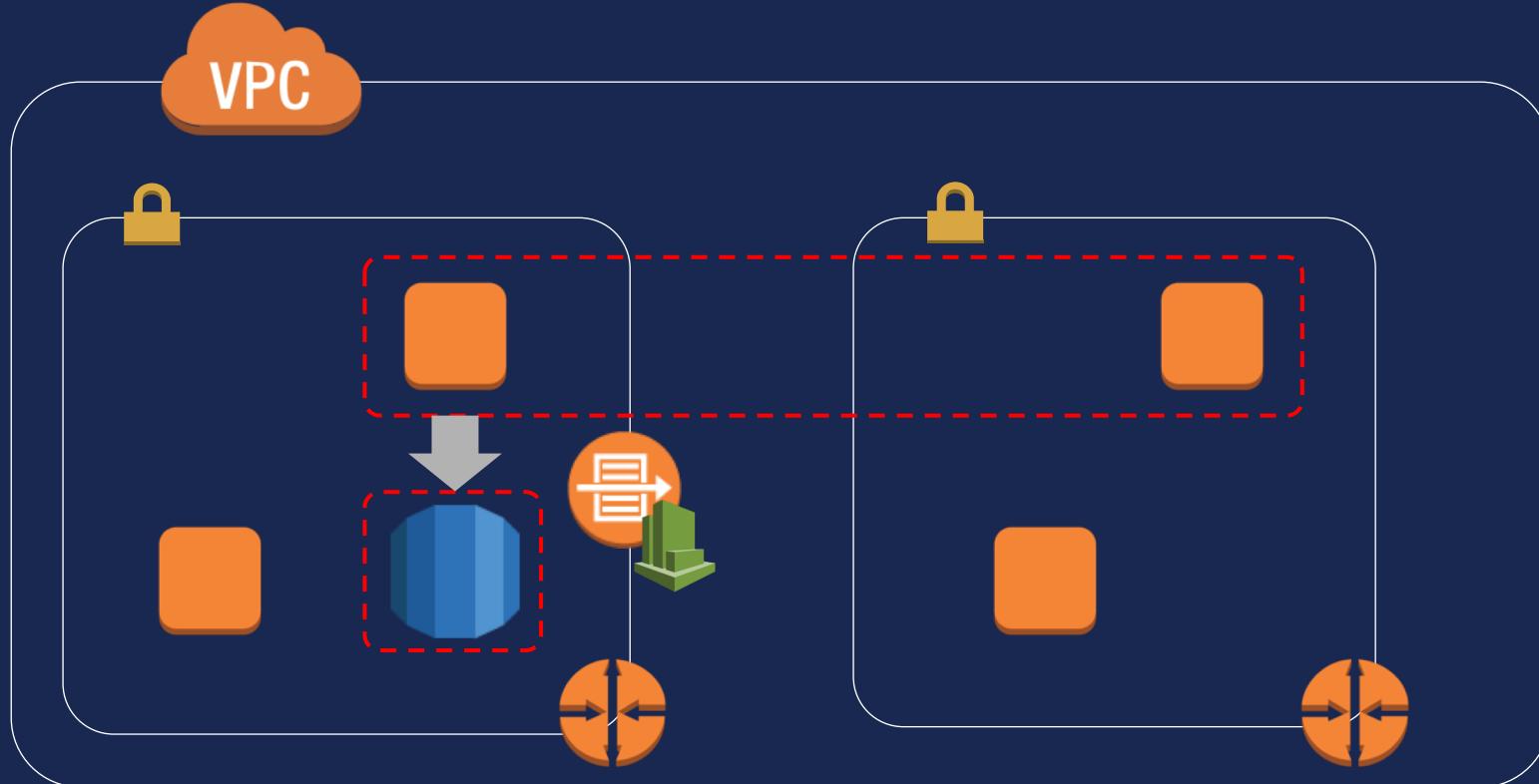
VPC Flow Logs data in CloudWatch Logs

Filter events		all 30s 5m 1h 6
Time (UTC -04:00)	Message	
2016-01-16T16:46:00Z	Who's this?	
▶ 16:46:00	# dig +short -x 109.236.86.32	7 56934 8080 6 5 373 1474750017 1474750073 ACCEPT OK
▶ 16:46:00	internetpolice.co.	0 8080 47928 6 5 650 1474750081 1474750133 ACCEPT OK
▶ 16:46:00		0 8080 47954 6 5 650 1474750081 1474750133 ACCEPT OK
▶ 16:46:00		0 8080 47954 6 5 650 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	0 8080 47954 6 5 650 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	100 10.0.0.117 47954 8080 6 5 373 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	1239 10.0.0.117 56978 8080 6 5 373 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	10.0.0.117 10.0.1.239 8080 56950 6 5 373 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	10.0.0.117 10.0.1.239 8080 56970 6 5 373 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	10.0.0.117 10.0.0.117 55567 22 6 5 373 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	10.0.0.117 10.0.0.117 47926 8080 6 5 373 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	10.0.0.117 10.0.0.117 47946 8080 6 5 373 1474750081 1474750133 ACCEPT OK
▶ 16:48:01	2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK	10.0.1.239 10.0.0.117 56950 8080 6 5 373 1474750081 1474750133 ACCEPT OK

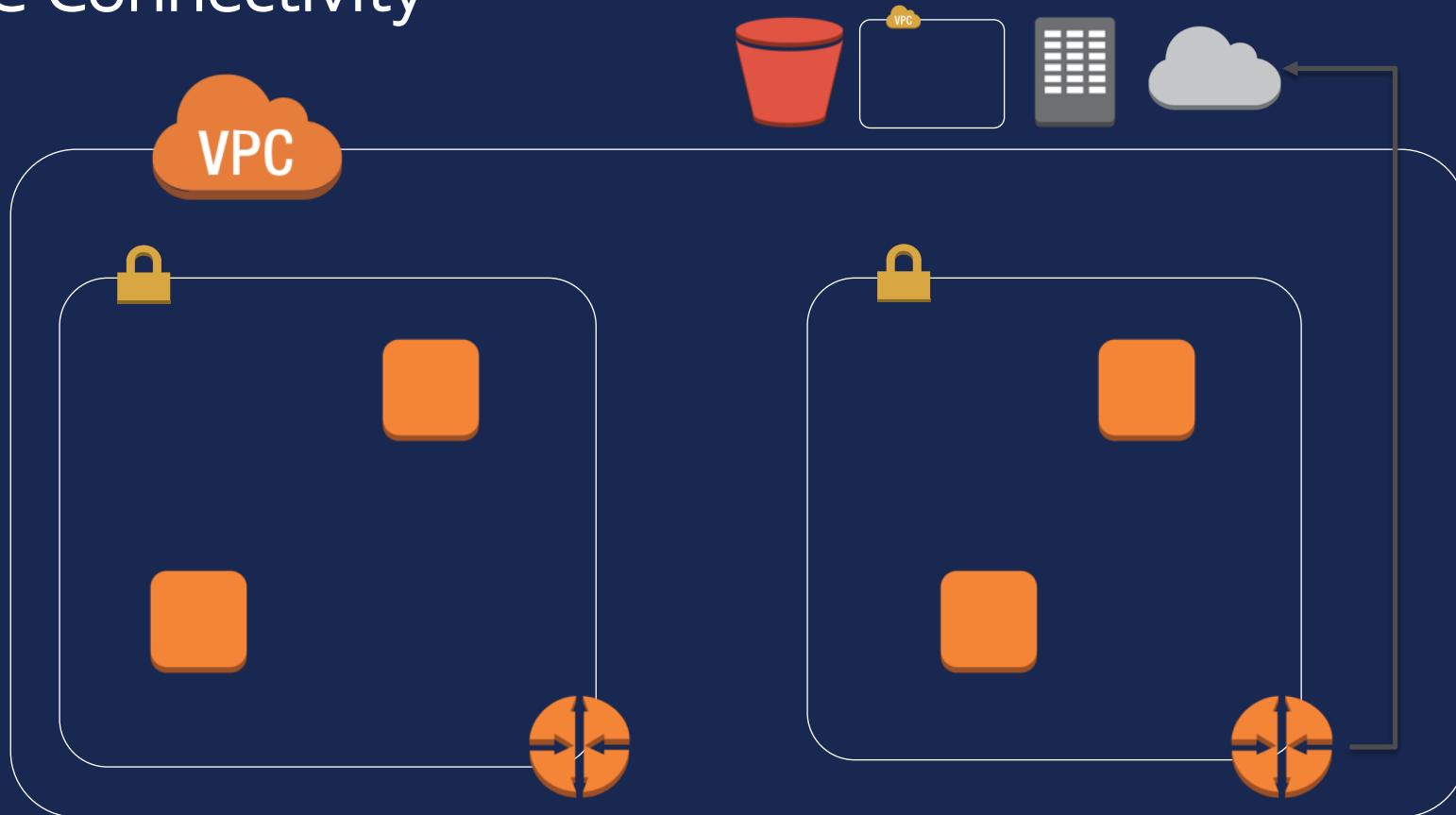
The VPC Network



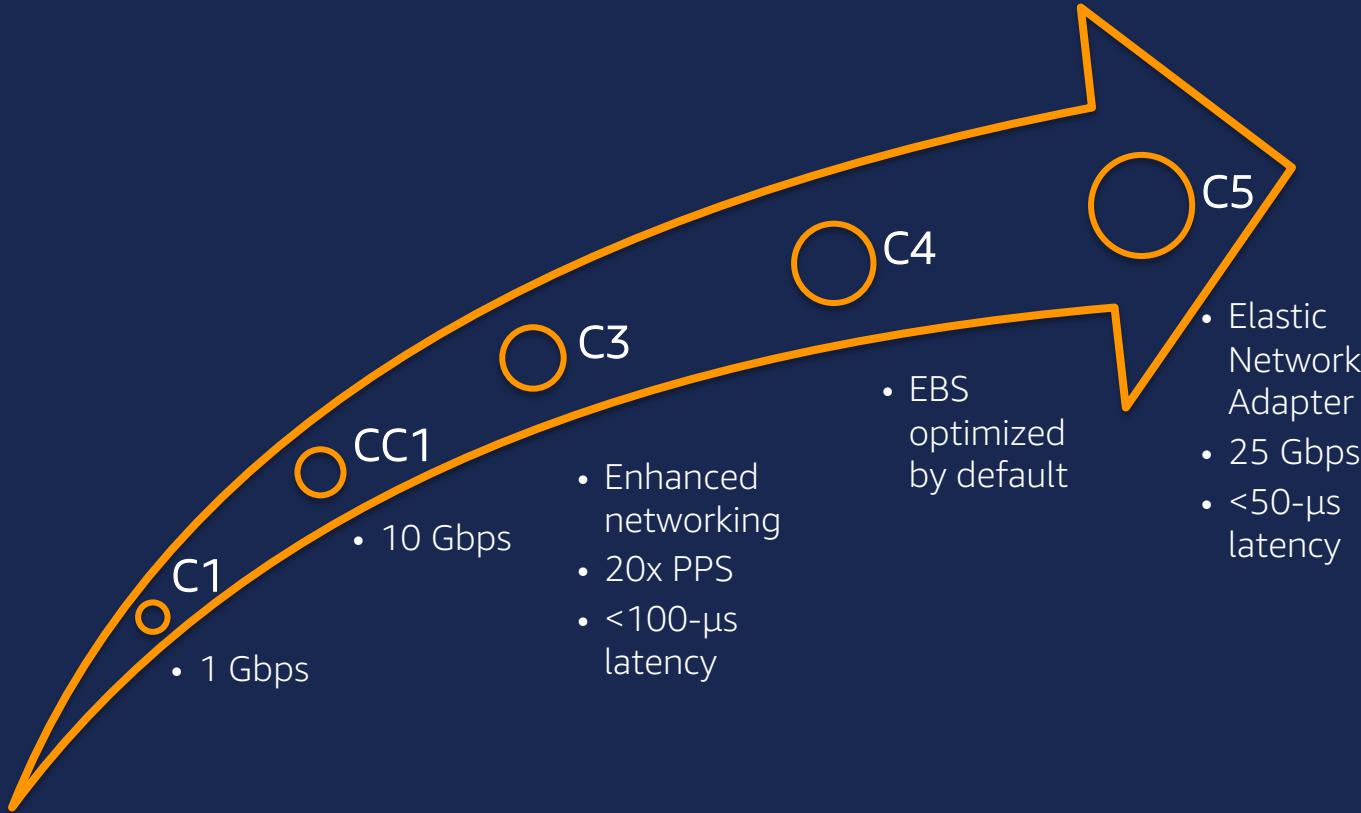
VPC Network Security



VPC Connectivity



On-Instance Networking Improvements



Instance Bandwidth Limits



25 Gbps
within placement group



25 Gbps
within region



25 Gbps
to Amazon S3

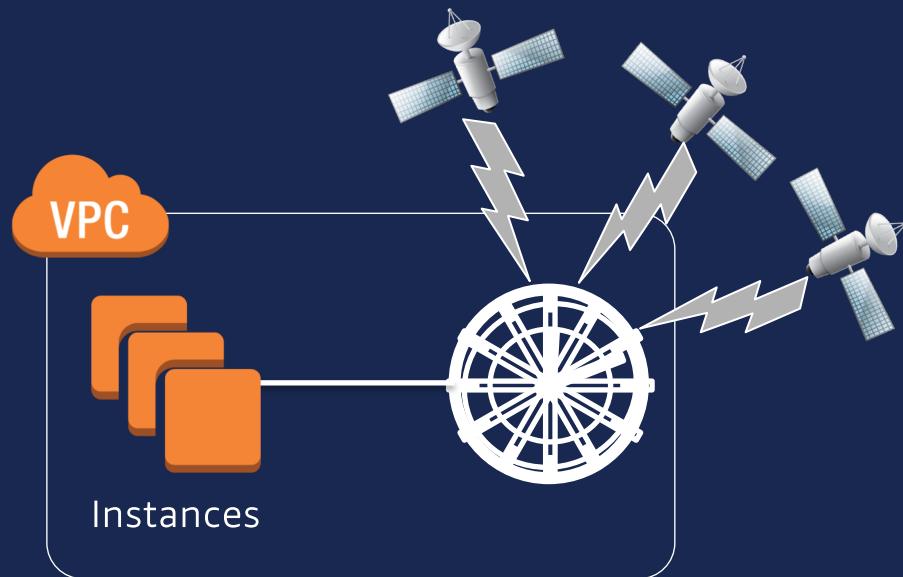


5 Gbps
for other sources

Amazon Time Sync Service

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

Available globally today!



Thank You!

Tom Adamski
Specialist Solutions Architect