aws SUMMIT
London

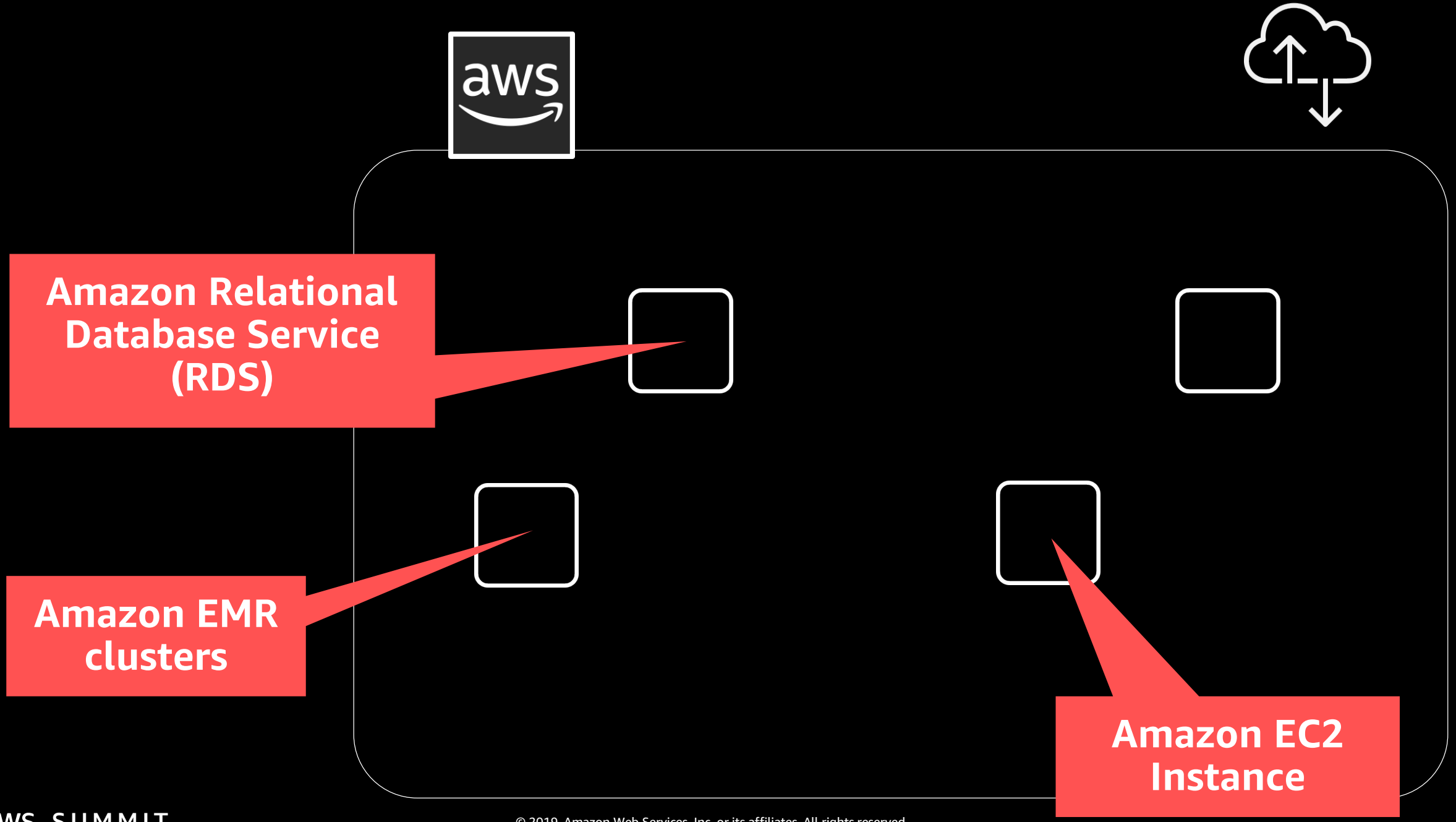
AWS Networking fundamentals

Perry Wald & Tom Adamski
AWS Solutions Architects

aws SUMMIT

Introductory - 200

"These sessions provide an overview of AWS services and features, and they assume that attendees are **new to the topic**. These sessions highlight **basic use cases, features, functions, and benefits**."



Default VPC

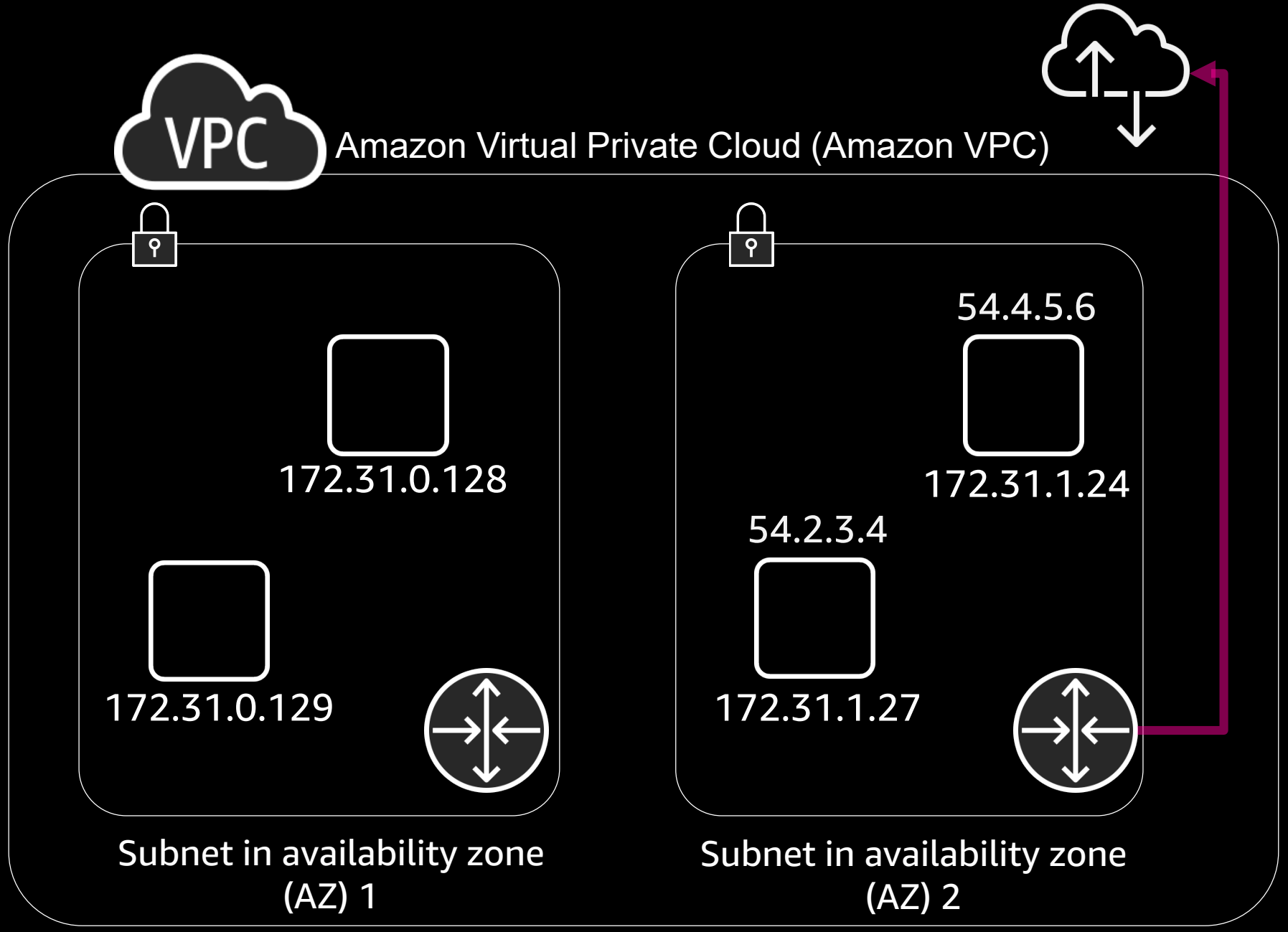
/16 IPv4 CIDR block (172.31.0.0/16).

/20 default subnet

Connected Internet Gateway

Security Group (SG)

Network Access Control List (NACL)



aws SUMMIT

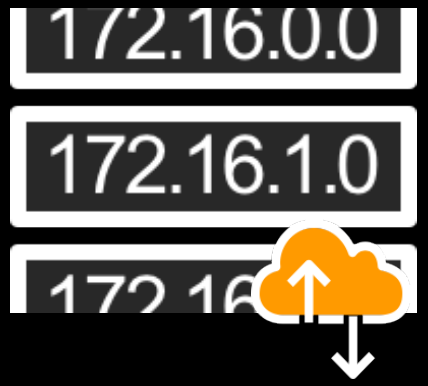
VPC concepts & fundamentals

aws SUMMIT

VPC concepts & fundamentals

IP addressing

Creating subnets



Routing in a VPC

Security

Choosing an IP address range

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

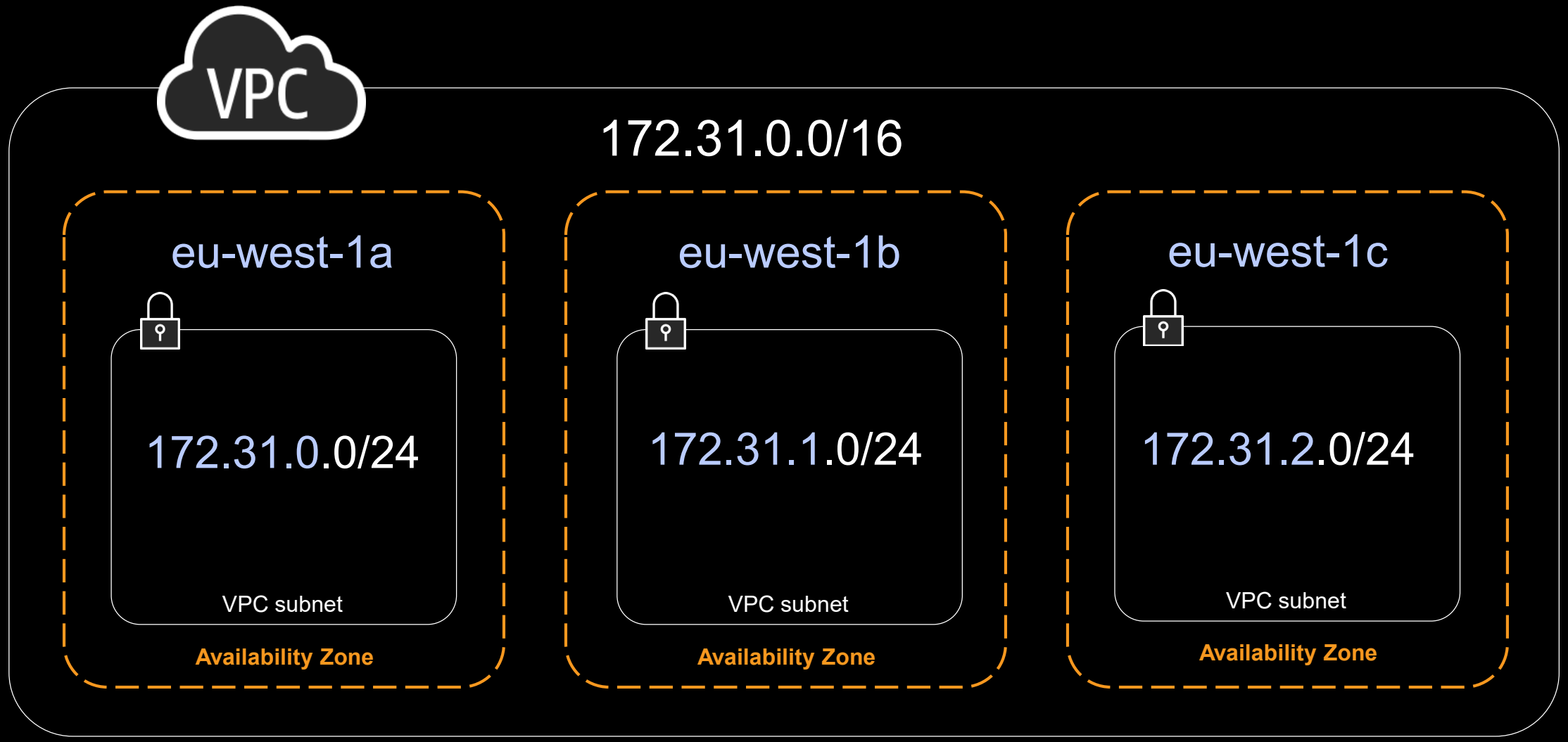
RFC1918 range:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Recommended:
/16
(65,536 addresses)

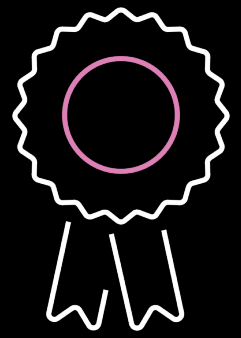
Creating subnets in a VPC

VPC subnets and Availability Zones

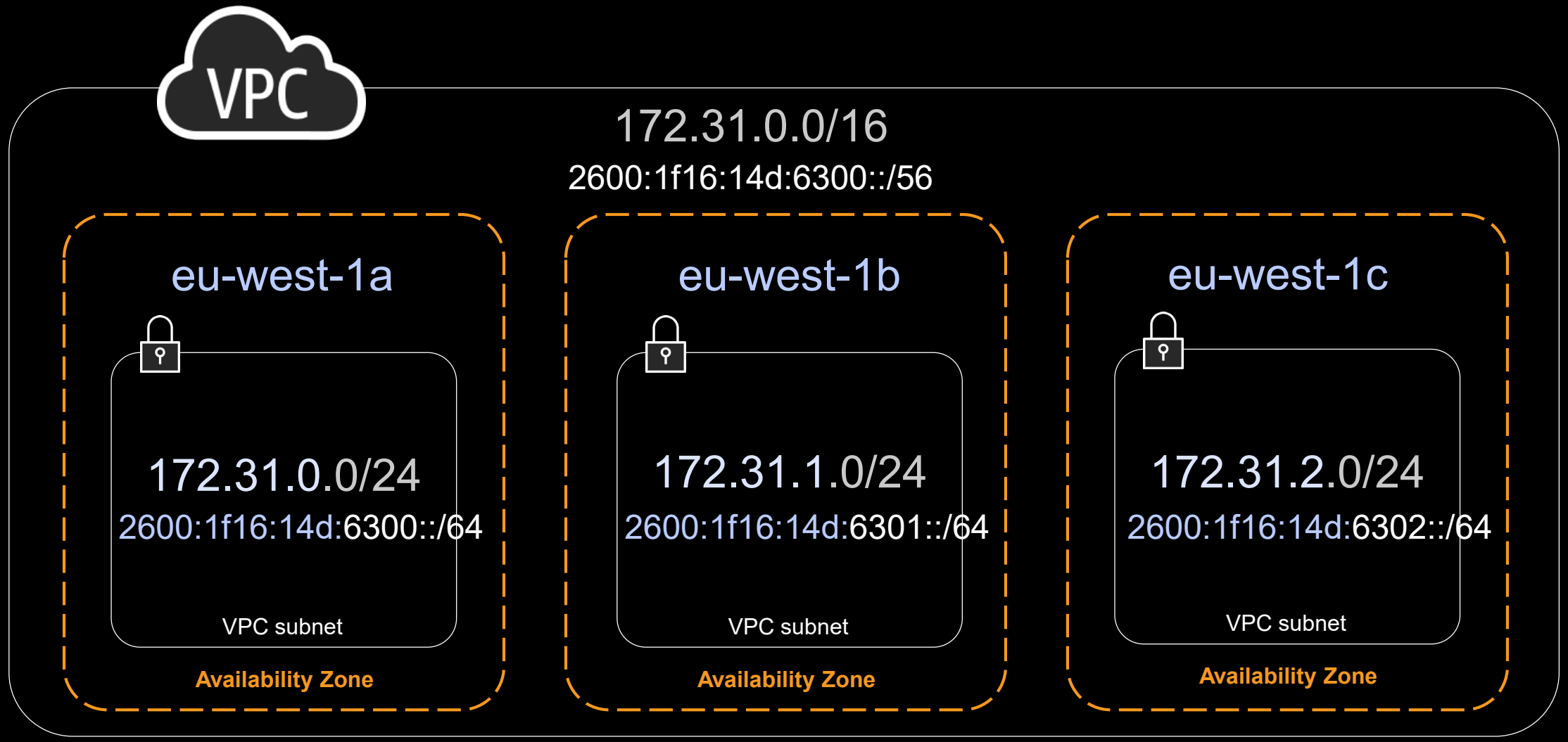


IPv6 in your VPC

- Can have a dual-stack VPC by adding an IPv6 CIDR
- Fixed sizes for VPC and subnets:
  - /56 VPC (4,722,366,482,869,645,213,696 addresses)
  - /64 subnets (18,446,744,073,709,551,616 addresses)



VPC subnets and Availability Zones



Routing in a VPC

Routing in your VPC

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

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

Search Route Tables and thei

Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-0028d8ca88068…	0 Subnets	Yes	vpc-0bcb5110cf0ce088b | myVPC

rtb-0028d8ca88068723d

Summary | **Routes** | Subnet Associations | Route Propagation | Tags

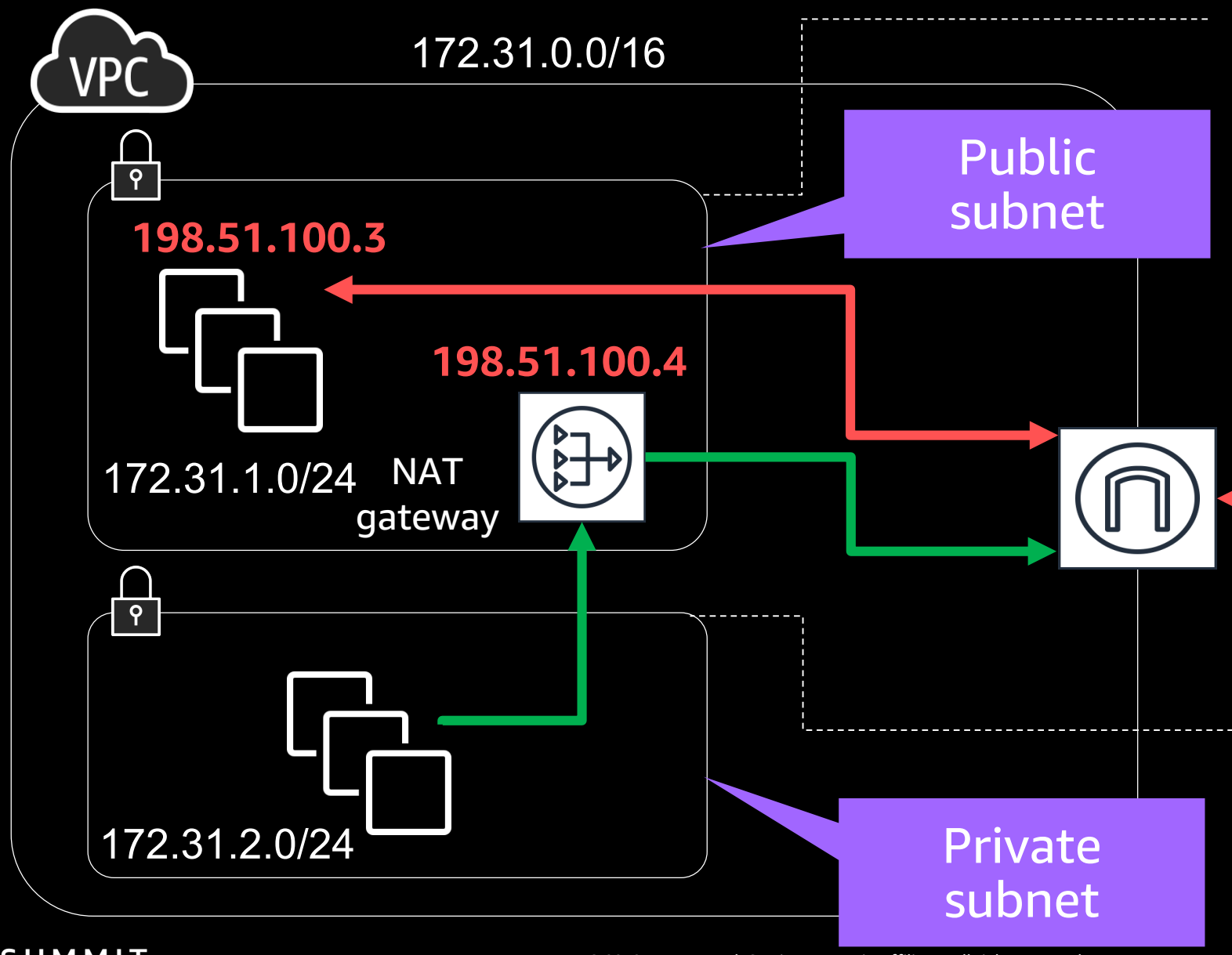
Traffic destined for my VPC stays in my VPC

Edit

View: All rules

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No

But what about the Internet?



Destination	Target
172.31.0.0/16	local

Inbound internet access

Destination	Target
172.31.0.0/16	local

Outbound internet access

aws SUMMIT

Security groups

Network access control list

Flow logs

Network security

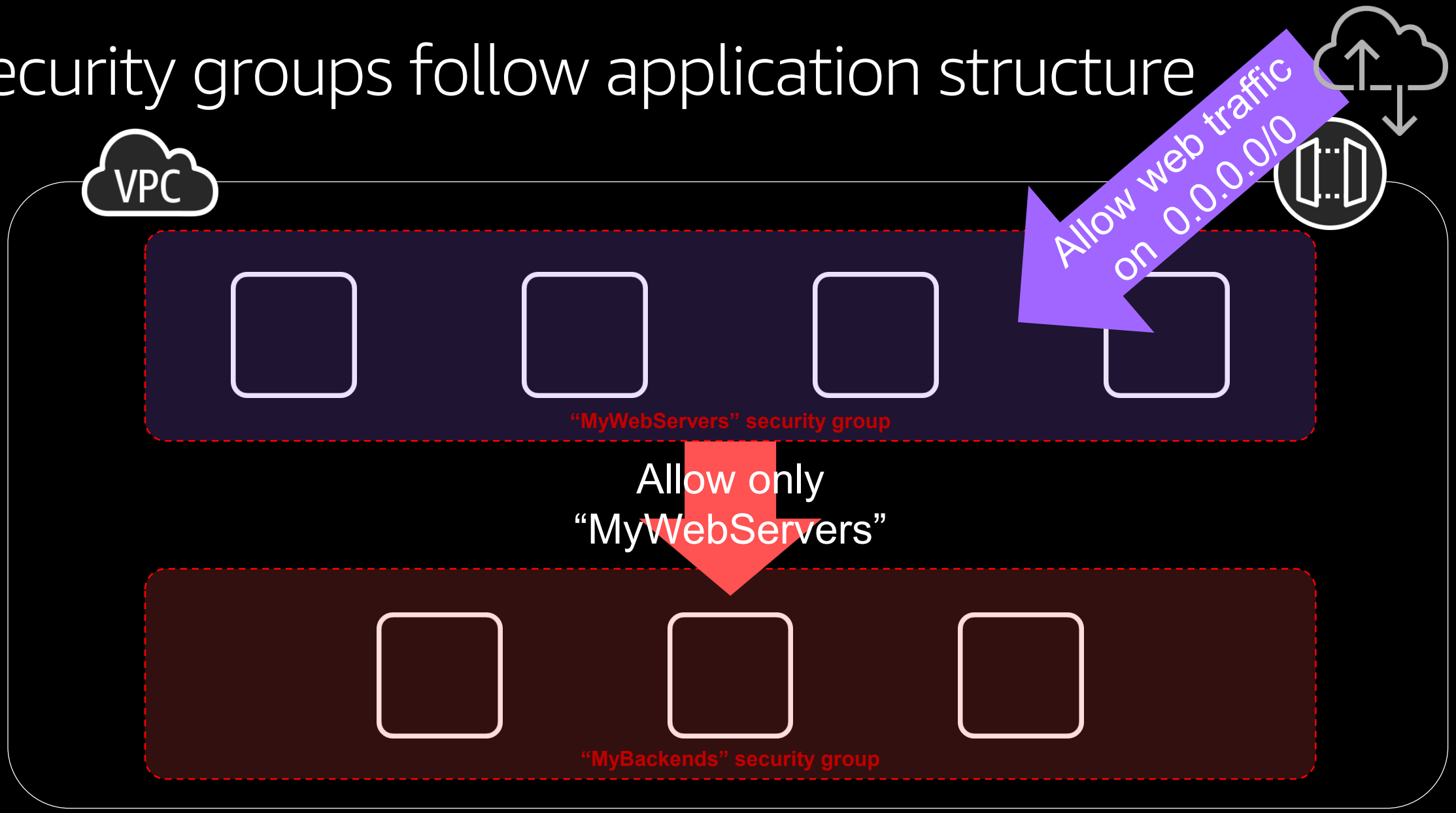
Security groups

Network access control list

Flow logs

Network security

Security groups follow application structure



Security groups example: Web servers

Name	Group ID	Group Name	VPC ID	Description
	sg-0228ccc01e1f02eb7	MyWebServers	vpc-0bcb5110cf0ce088b	group for web servers
	sg-09d98b1a3d09baf45	MyBackends	vpc-0bcb5110cf0ce088b	group for backend hosts
	sg-0e2dc655a56122087	default	vpc-0bcb5110cf0ce088b	default VPC security group

Security Group: sg-0228ccc01e1f02eb7

Description | **Inbound** | Outbound

Allow HTTP traffic from anywhere

Edit

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	allow all HTTP on ...
HTTP	TCP	80	::/0	allow all HTTP on ...

Security groups example: Backends

Name	Group ID	Group Name	VPC ID	Description
	sg-0228ccc01e1f02eb7	MyWebServers	vpc-0bcb5110cf0ce088b	group for web servers
	sg-09d98b1a3d09baf45	MyBackends	vpc-0bcb5110cf0ce088b	group for backend hosts
	sg-0e2dc655a56122087	default	vpc-0bcb5110cf0ce088b	default VPC security group

Security Group: sg-09d98b1a3d09baf45

Description | **Inbound** | Outbound | Tags

Allow application traffic from web servers only

Edit

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	2345	sg-0228ccc01e1f02eb7 (MyV	allow traffic from...

Security groups

Network access control list

Flow logs

Network security

Security groups vs. NACLs

Security group	Network ACL
Operates at instance level	Operates at subnet level
Supports allow rules only	Supports allow and deny rules
Is stateful: return traffic is automatically allowed regardless of any rules	Is stateless: return traffic must be explicitly allowed by rules
All rules evaluated before deciding whether to allow traffic	Rules evaluated in order when deciding whether to allow traffic
Applies only to instances explicitly associated with the security group	Automatically applies to all instances launched into associated subnets
Doesn't filter traffic to or from link-local addresses (169.254.0.0/16) or AWS-reserved IPv4 addresses; these are the first four IPv4 addresses of the subnet (including the Amazon VPC DNS server)	

Security groups

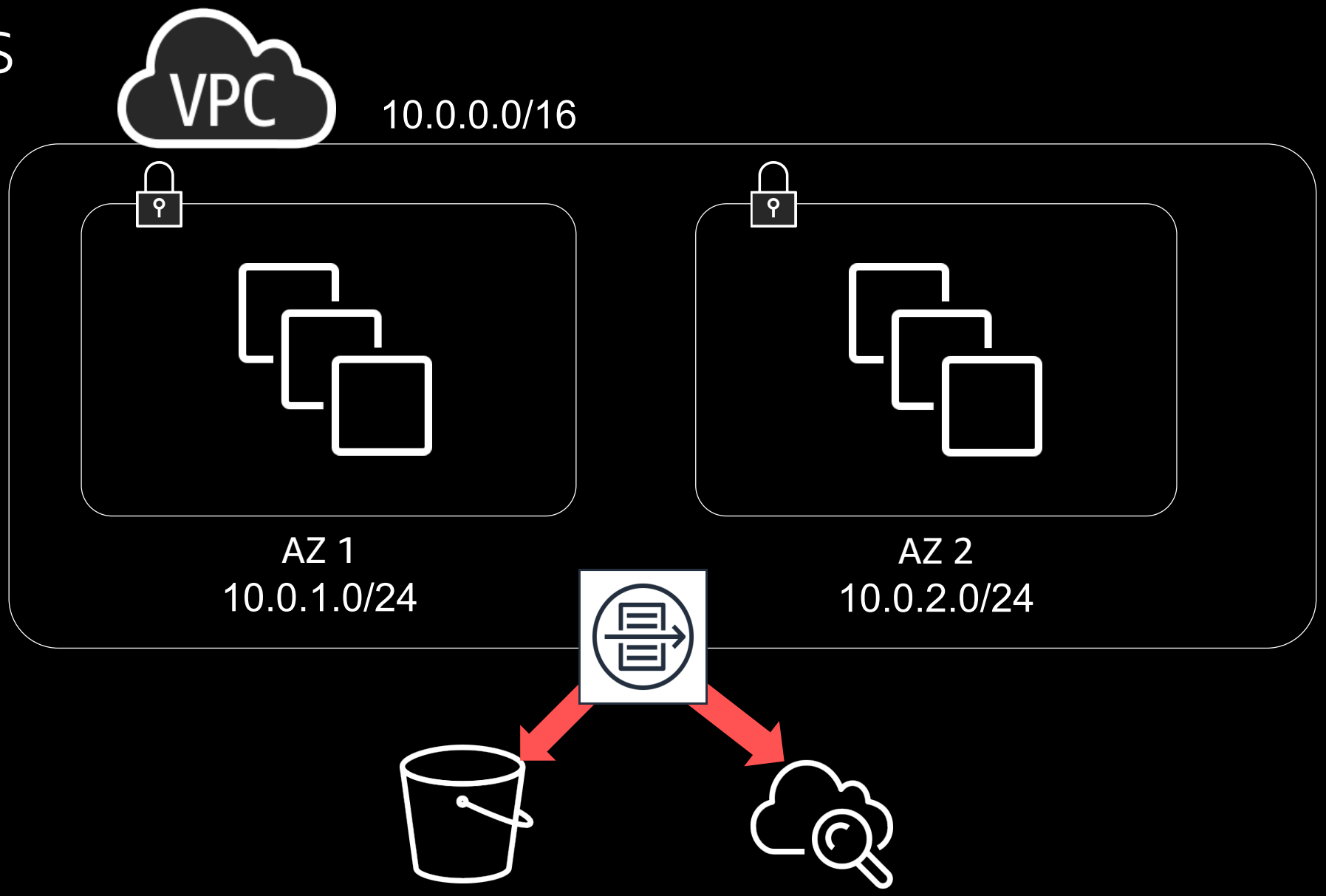
Network access control list

Flow logs

Network security

VPC flow logs

- Visibility
- Troubleshooting
- Analyze traffic flow



VPC flow logs: Setup

Create VPC | Actions

Search VPCs and their proper

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
myVPC	vpc-0bcb5110cf0ce088b	available	172.31.0.0/16	2600:1f16:14d:6300::/56	dopt-c8cf28a1

vpc-0bcb5110cf0ce088b | myVPC

Summary | CIDR Blocks | **Flow Logs** | Tags

You can create flow logs on your resources to capture IP traffic flow information f etwork interfaces for your

Create flow log

Flow Log ID	Filter	Destination Type	Destination Name	IAM Role ARN	Creation
fl-0e6a51c9092741fea	ALL	s3	my-flow-logs	-	October
fl-09a184a919be995ac	ALL	cloud-watch-logs	my-flow-logs-cw	arn:aws:iam::082897841036:role/flowlogsRole	October

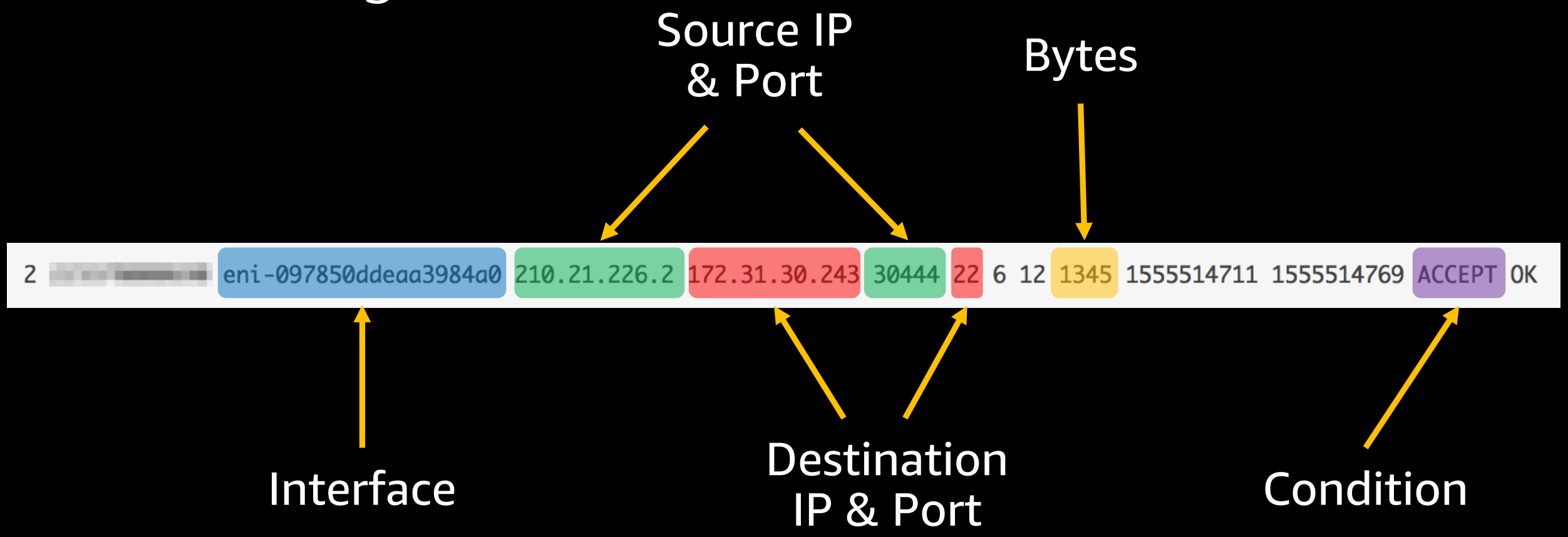
VPC traffic metadata captured in Amazon S3

or Amazon CloudWatch Logs

VPC flow logs format

	Time (UTC +00:00)	Message
	2019-04-17	
		No older events found at the moment. Retry.
▸	15:24:37	2 [redacted] eni-097850ddeaa3984a0 178.19.107.42 172.31.30.243 48335 8545 6 1 40 1555514677 1555514709 REJECT OK
▾	15:25:11	2 [redacted] eni-097850ddeaa3984a0 210.21.226.2 172.31.30.243 30444 22 6 12 1345 1555514711 1555514769 ACCEPT OK
		2 [redacted] eni-097850ddeaa3984a0 210.21.226.2 172.31.30.243 30444 22 6 12 1345 1555514711 1555514769 ACCEPT OK
▸	15:25:11	2 [redacted] eni-097850ddeaa3984a0 207.244.86.222 172.31.30.243 55216 3337 6 1 40 1555514711 1555514769 REJECT OK
▸	15:25:11	2 [redacted] eni-097850ddeaa3984a0 68.183.37.224 172.31.30.243 42222 8088 6 1 40 1555514711 1555514769 REJECT OK
▸	15:25:11	2 [redacted] eni-097850ddeaa3984a0 172.31.30.243 210.21.226.2 22 30444 6 12 2349 1555514711 1555514769 ACCEPT OK
▸	15:26:31	2 [redacted] eni-097850ddeaa3984a0 178.128.249.60 172.31.30.243 60214 8088 6 1 40 1555514791 1555514829 REJECT OK

VPC flow logs format



DNS in a VPC

VPC DNS options

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
myVPC	vpc-0bcb5110cf0ce088b	available	172.31.0.0/16	2600:1f16:14d:6300::/56	dopt-c8cf28a1

vpc-0bcb5110cf0ce088b | myVPC

Have EC2 auto-assign DNS host names to instances

Use Amazon DNS server

Summary | CIDR Blocks | Flow Logs | Tags

VPC ID: vpc-0bcb5110cf0ce088b | myVPC
State: available
IPv4 CIDR: 172.31.0.0/16
IPv6 CIDR: 2600:1f16:14d:6300::/56
DHCP options set: dopt-c8cf28a1
Route table: rtb-0028d8ca88068723d

Network ACL: acl-0eb64 2bbc5a5
Tenancy: Default

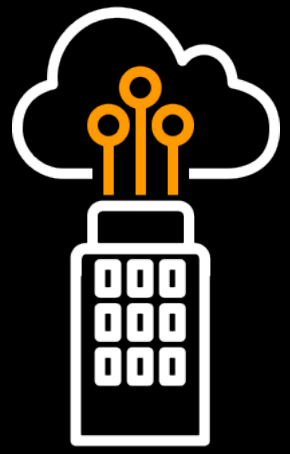
DNS resolution: yes
DNS hostnames: yes

Connectivity options for VPCs

aws SUMMIT

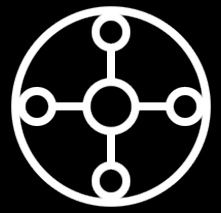
Connecting your VPC

Connecting to
other VPCs



Connecting to your
on-premises network

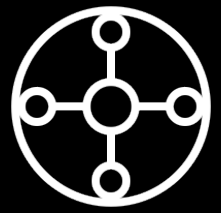
VPC Peering



Transit Gateway

Connecting to other VPCs

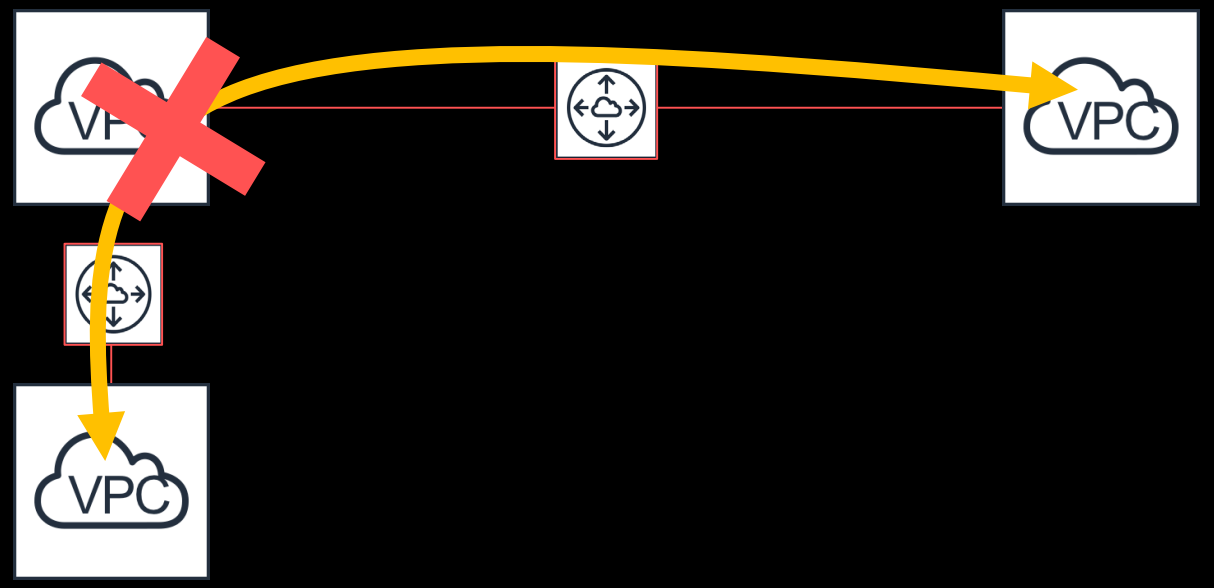
VPC Peering



Transit Gateway

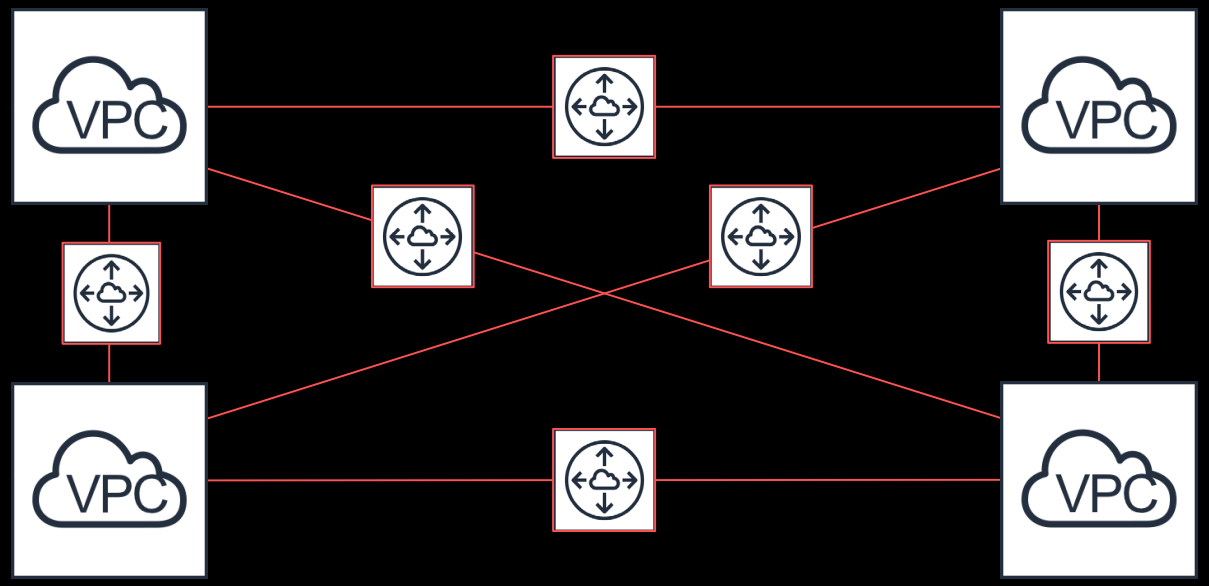
Connecting to other VPCs

VPC peering

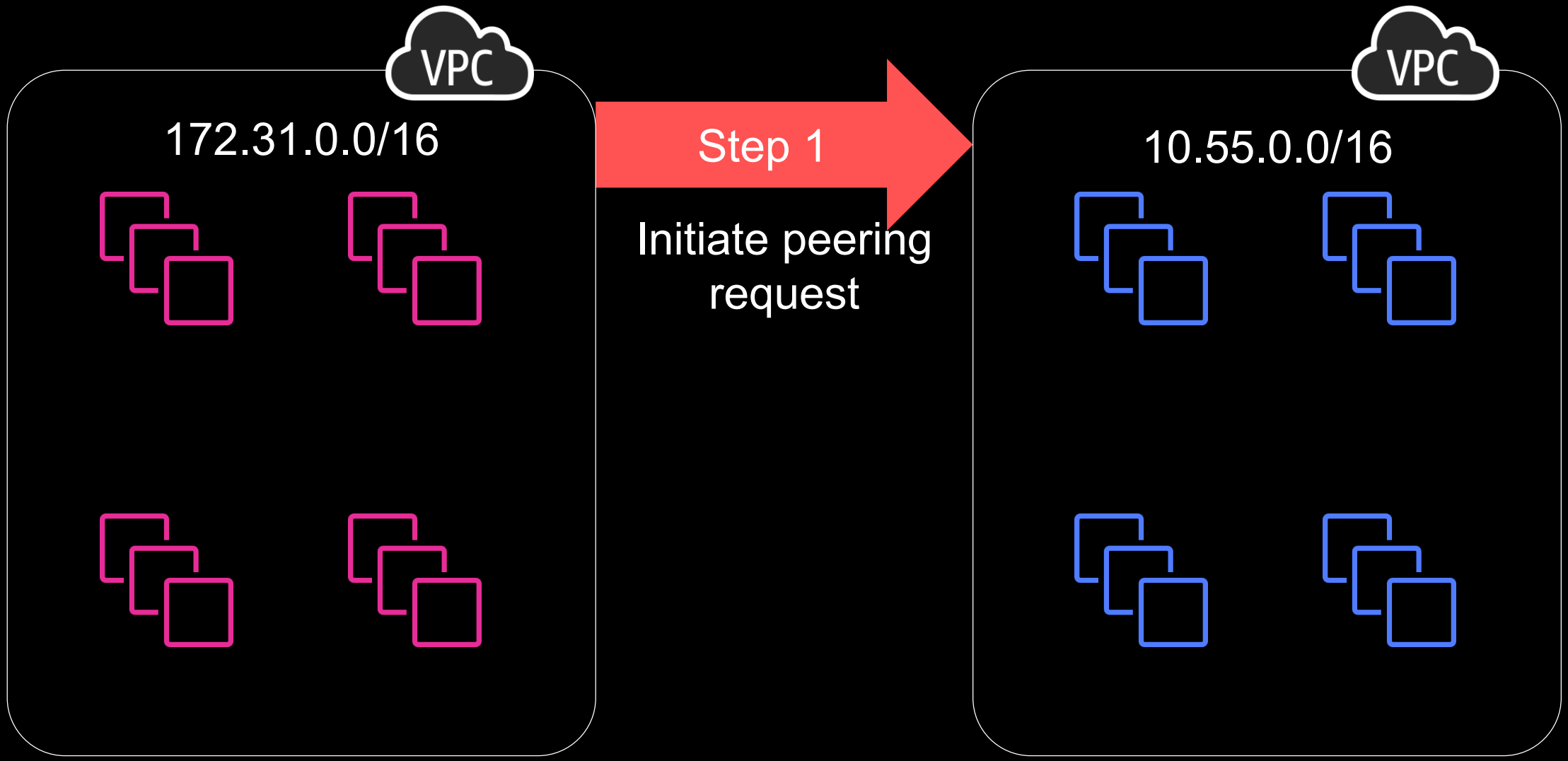


VPC peering

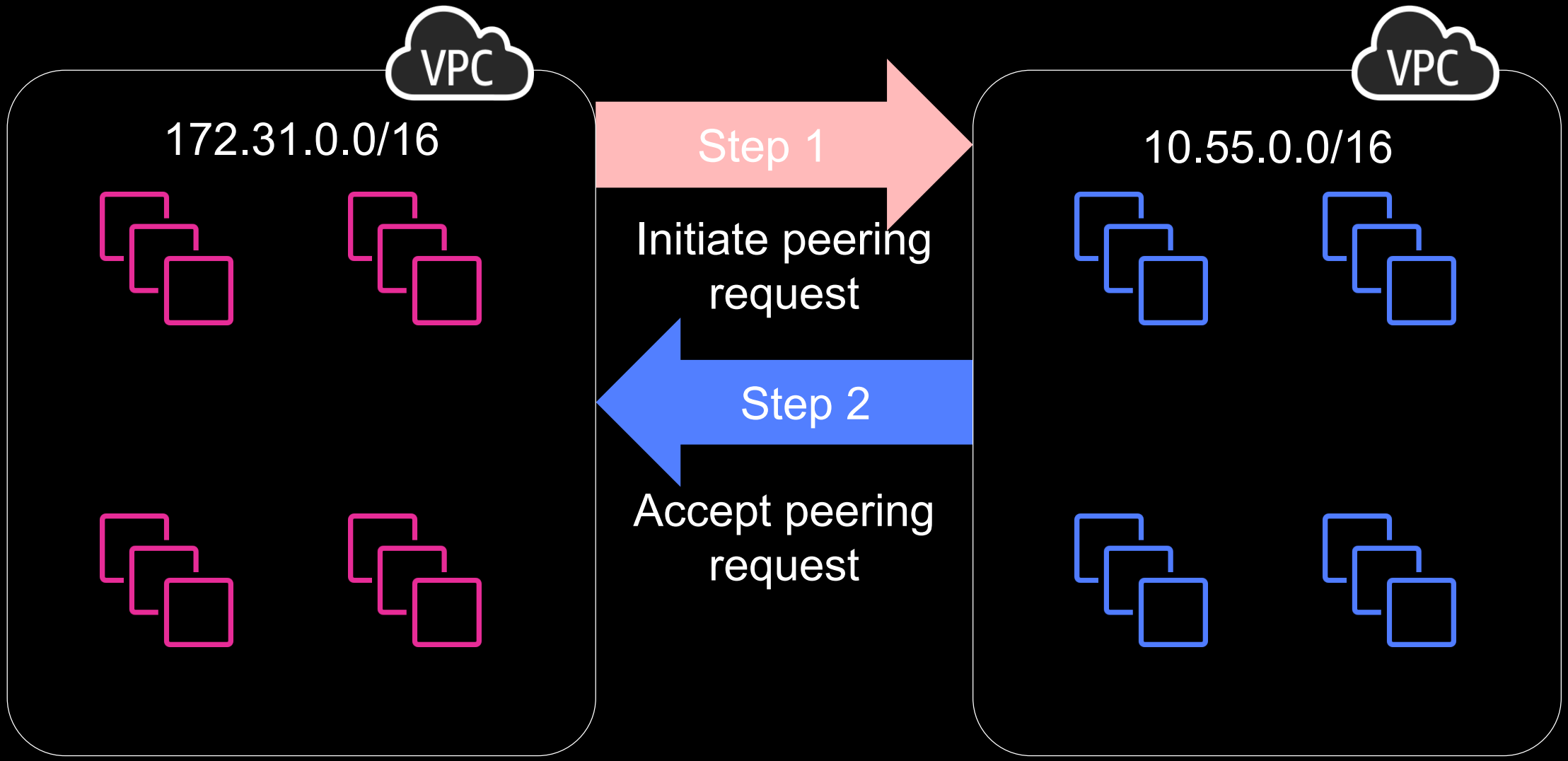
- Full private IP connectivity between two VPCs
- Can peer VPCs across regions
- VPCs can be in different accounts
- VPC CIDR ranges must not overlap



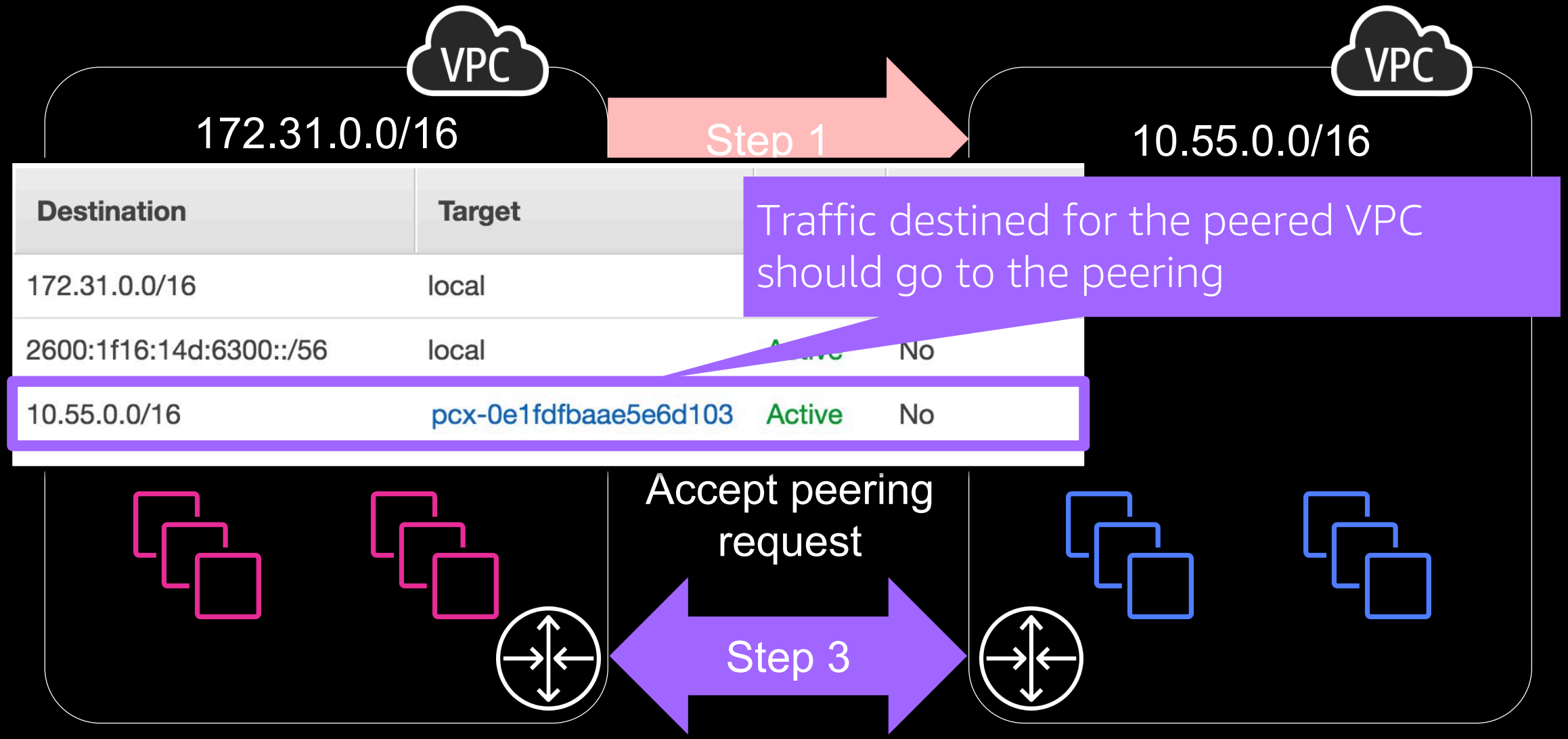
Establish a VPC peering: Initiate request



Establish a VPC peering: Accept request

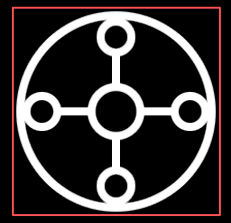


Establish a VPC peering: Create a route



Destination	Target		
172.31.0.0/16	local		
2600:1f16:14d:6300::/56	local	Active	No
10.55.0.0/16	pcx-0e1fdfbaae5e6d103	Active	No

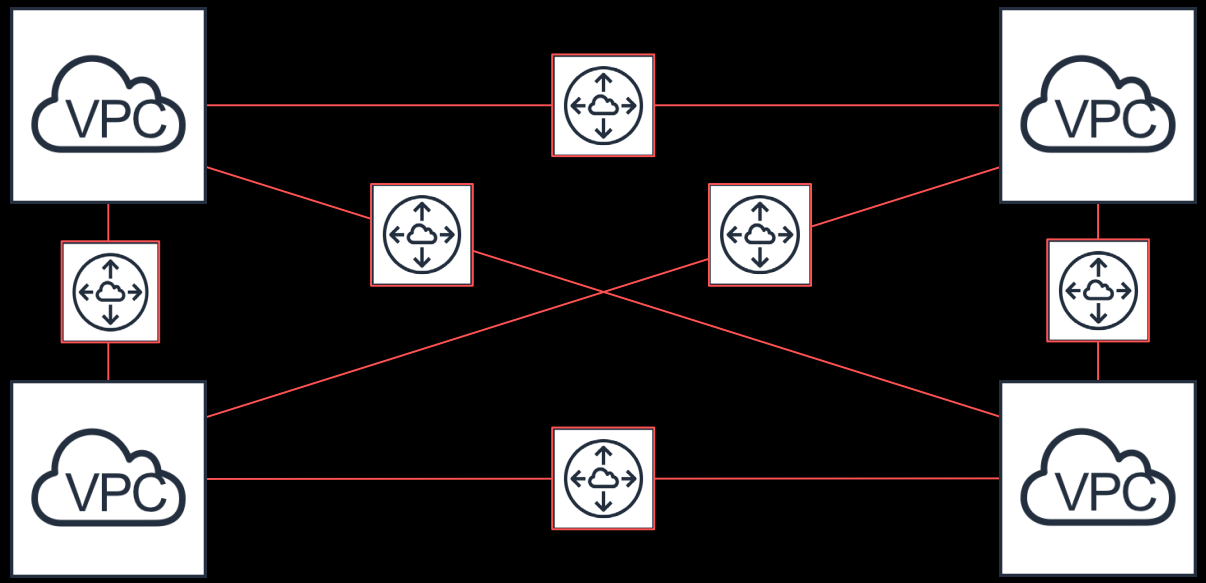
VPC Peering



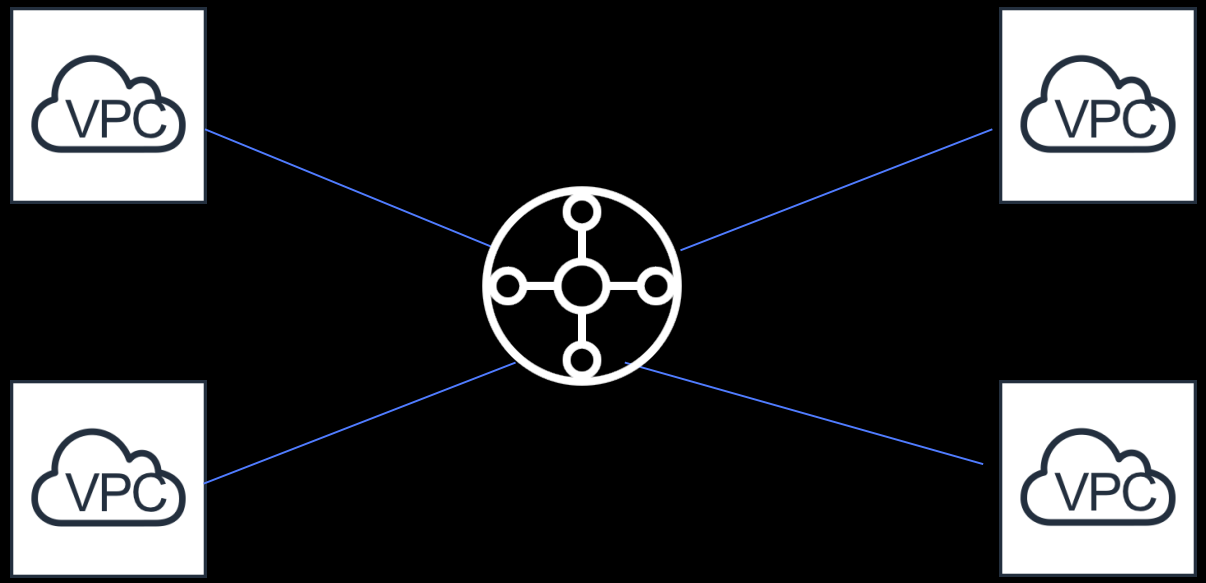
Transit Gateway

Connecting to other VPCs

Before Transit Gateway …



With Transit Gateway …

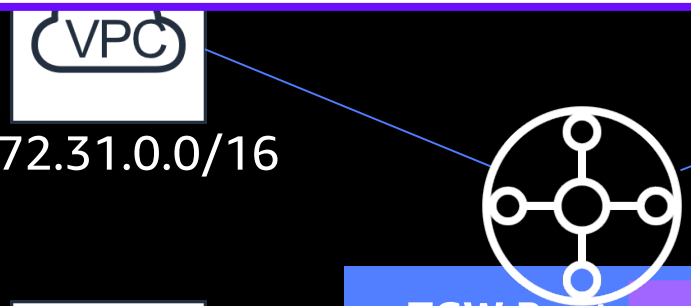


With Transit Gateway …

VPC Route table

Destination	Target
172.31.0.0/16	local
2600:1f16:14d:6300::/56	local
172.16.0.0/12	tgw-0541728e5c83ff1f0

Traffic destined for any VPC in 172.16.0.0/12 range should go via TGW



TGW Route

CIDR	Attachment	
172.29.0.0/16	tgw-attach-014e632db828232dc |	
172.30.0.0/16	tgw-attach-04caee7179f146894 | vpc-15609773	VPC
172.31.0.0/16	tgw-attach-07af5c4fc91783865 | vpc-07bd03ecd2945108a	VPC

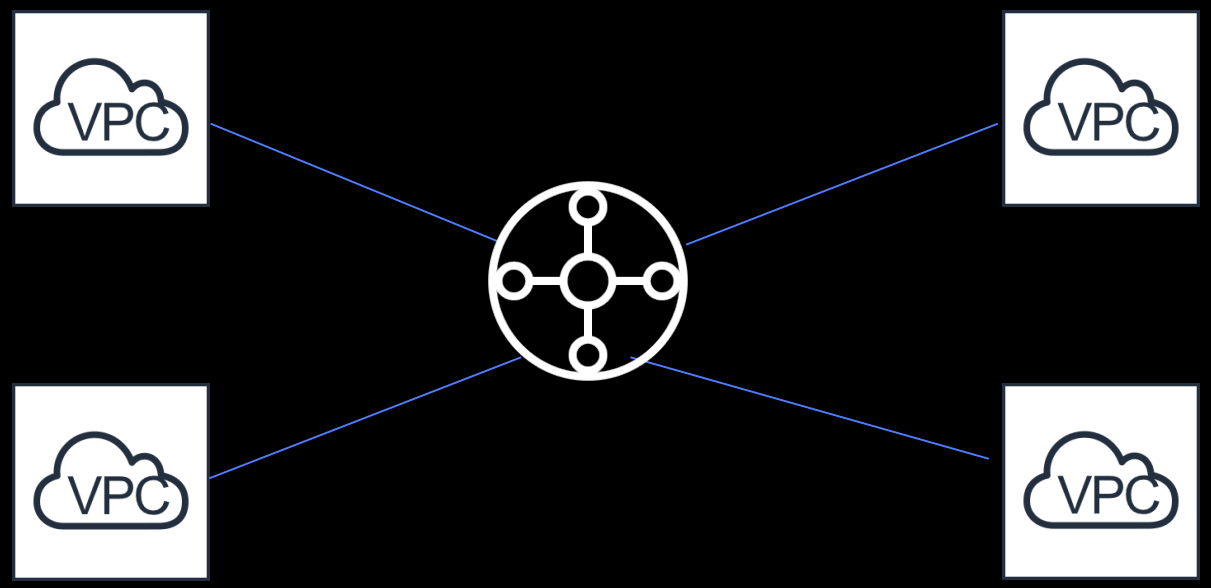
Route back to our VPC

With Transit Gateway …

Centralized private IP connectivity between multiple VPCs

VPCs must be in the same region as Transit Gateway

VPCs can be in different accounts



VPC peering or TGW?

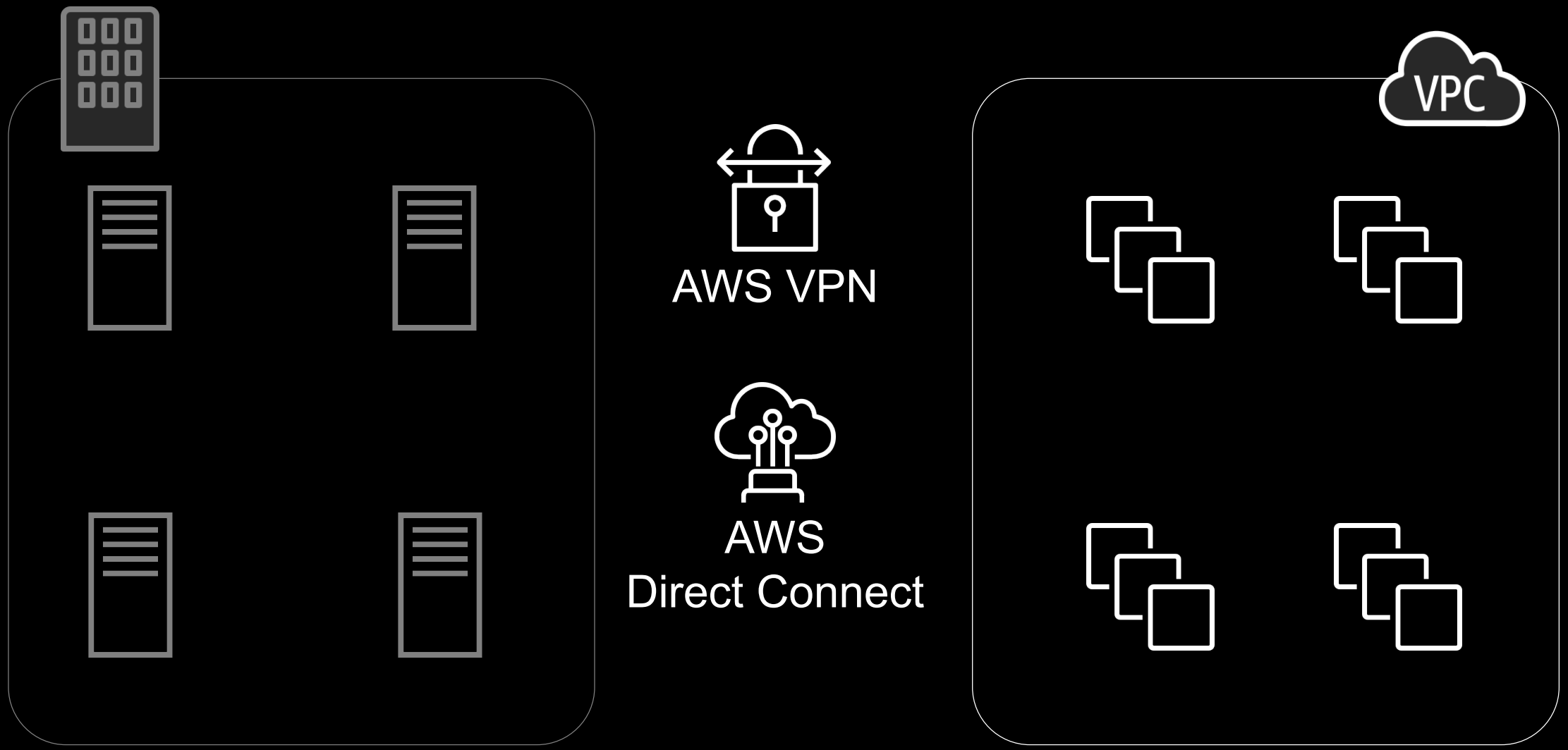
	VPC Peering	Transit Gateway
VPC LIMIT	125 peerings	5,000 attachments
BANDWIDTH LIMIT	N/A (intra-region)	50Gbps per VPC attachment
MANAGEMENT	Decentralised	Centralised
COST DIMENSIONS	Data Transfer	Data Transfer & Attachment

AWS VPN

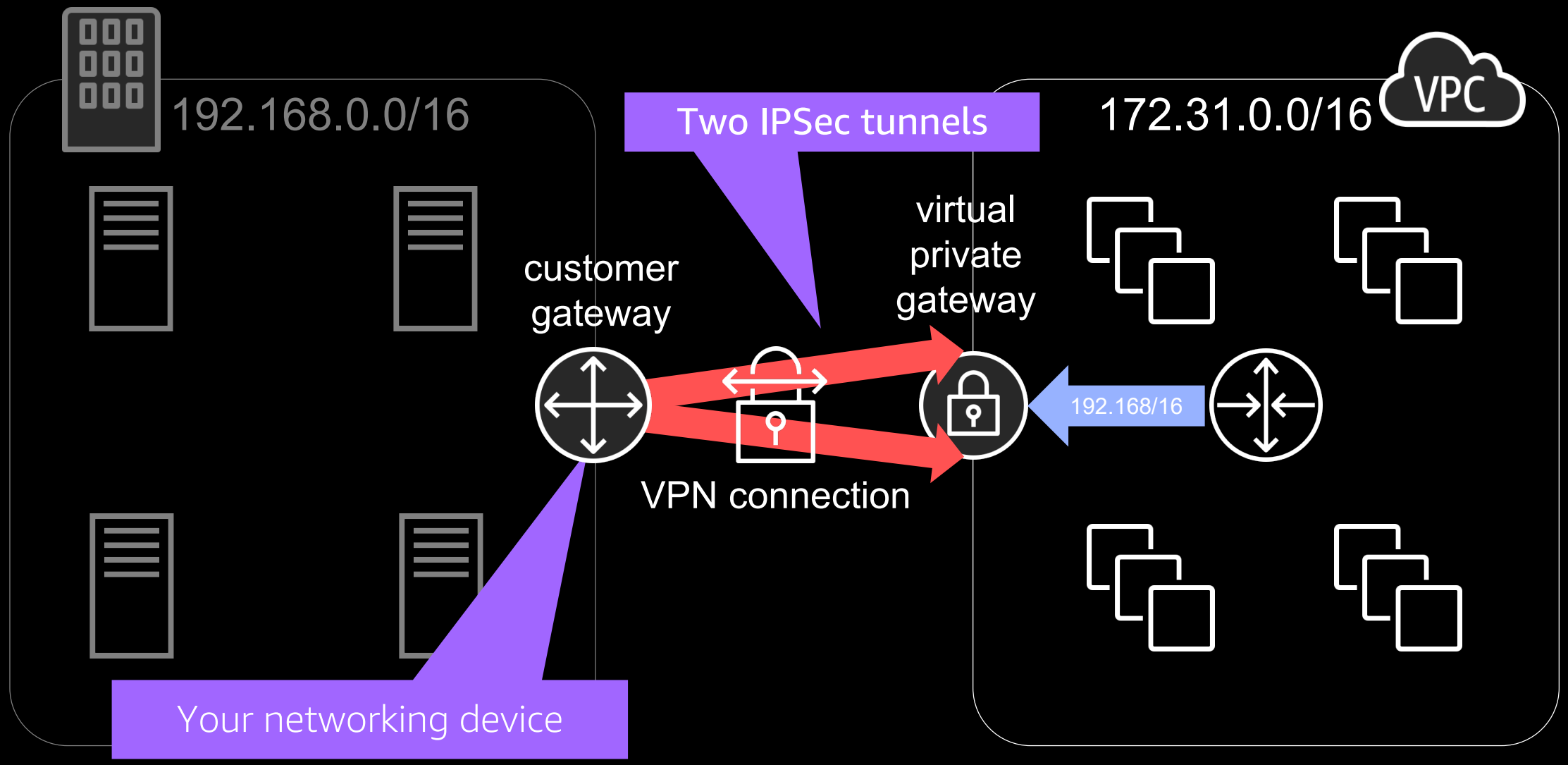
AWS
Direct Connect

Connecting to on-premises networks:

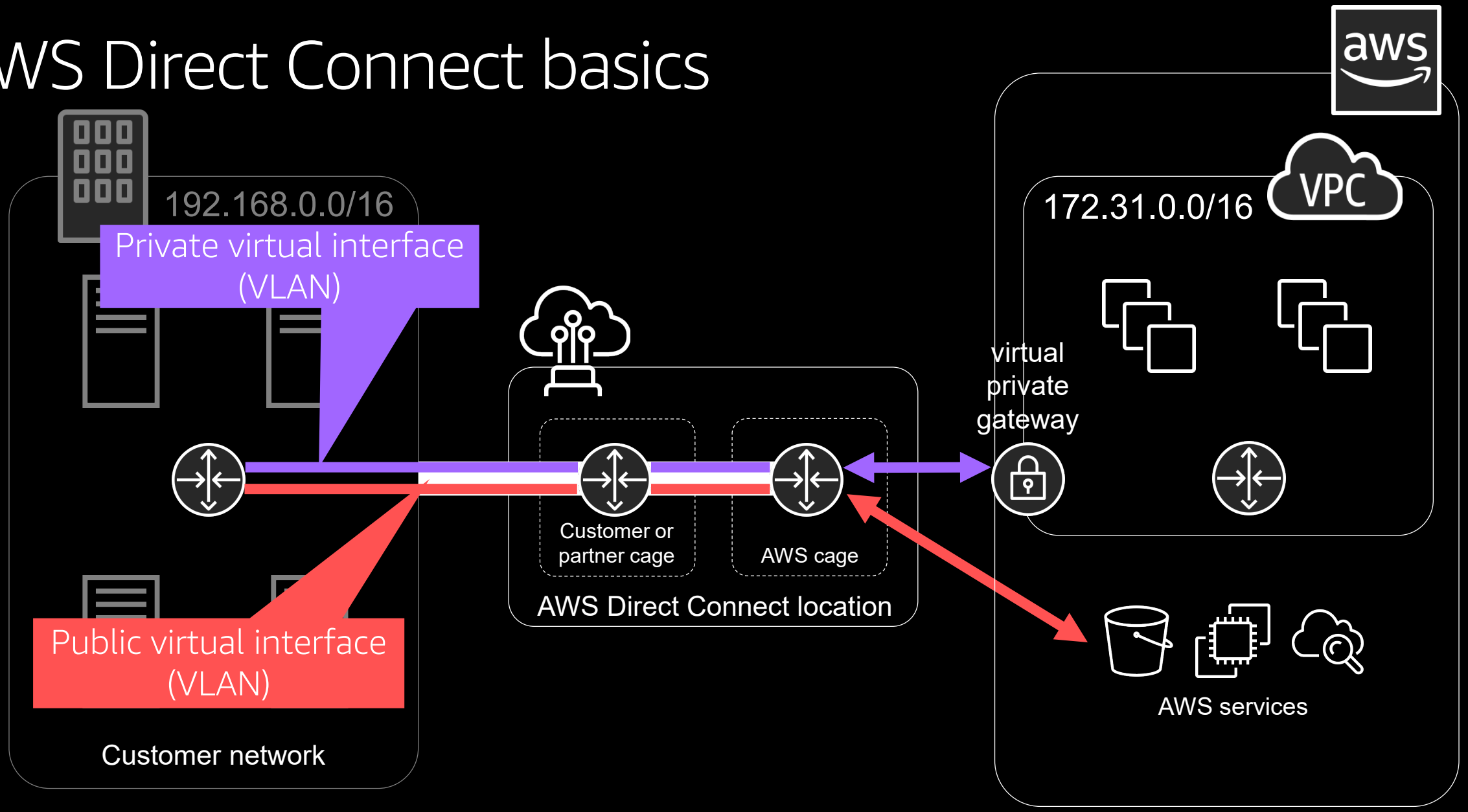
Extend an on-premises network into your VPC



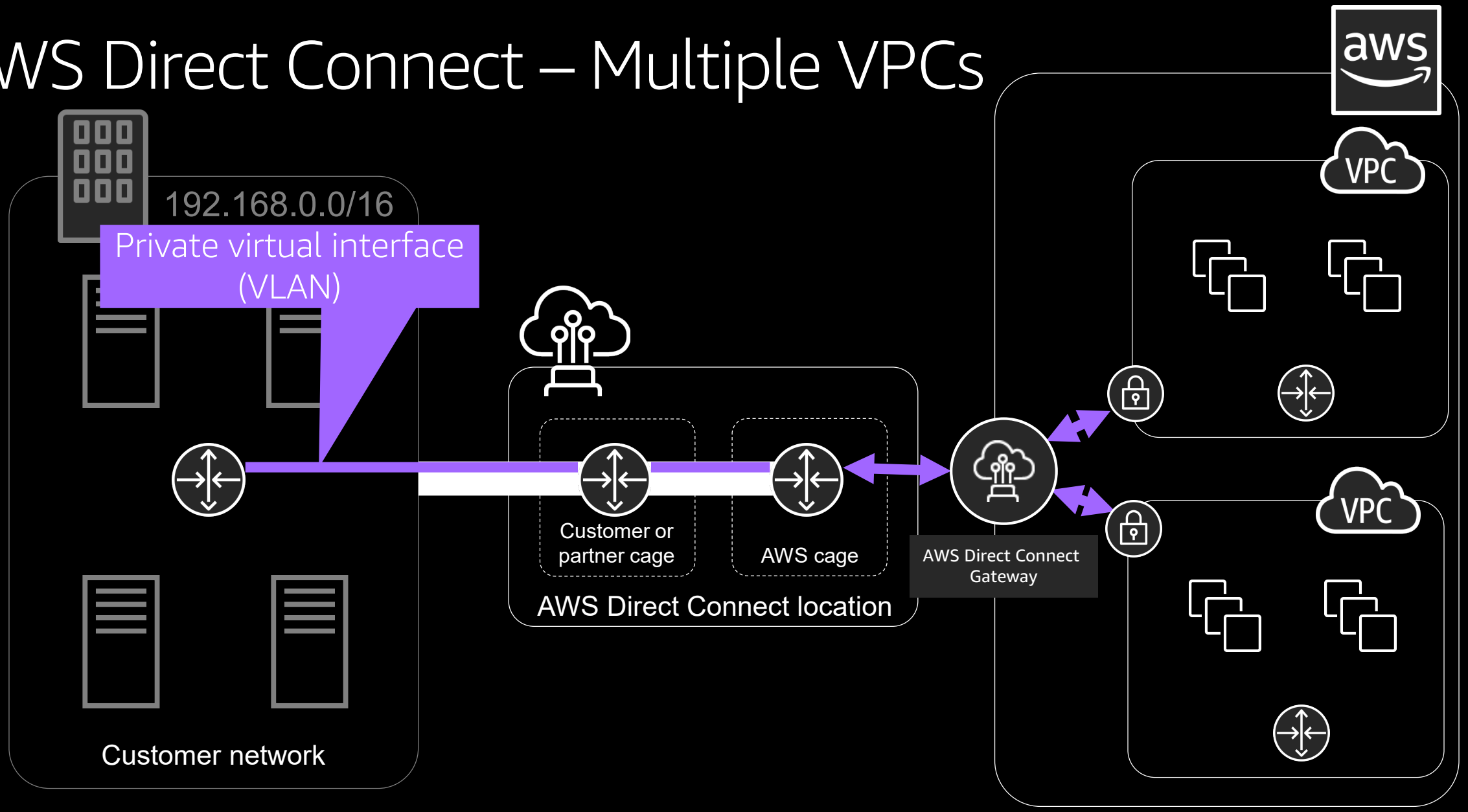
AWS VPN basics



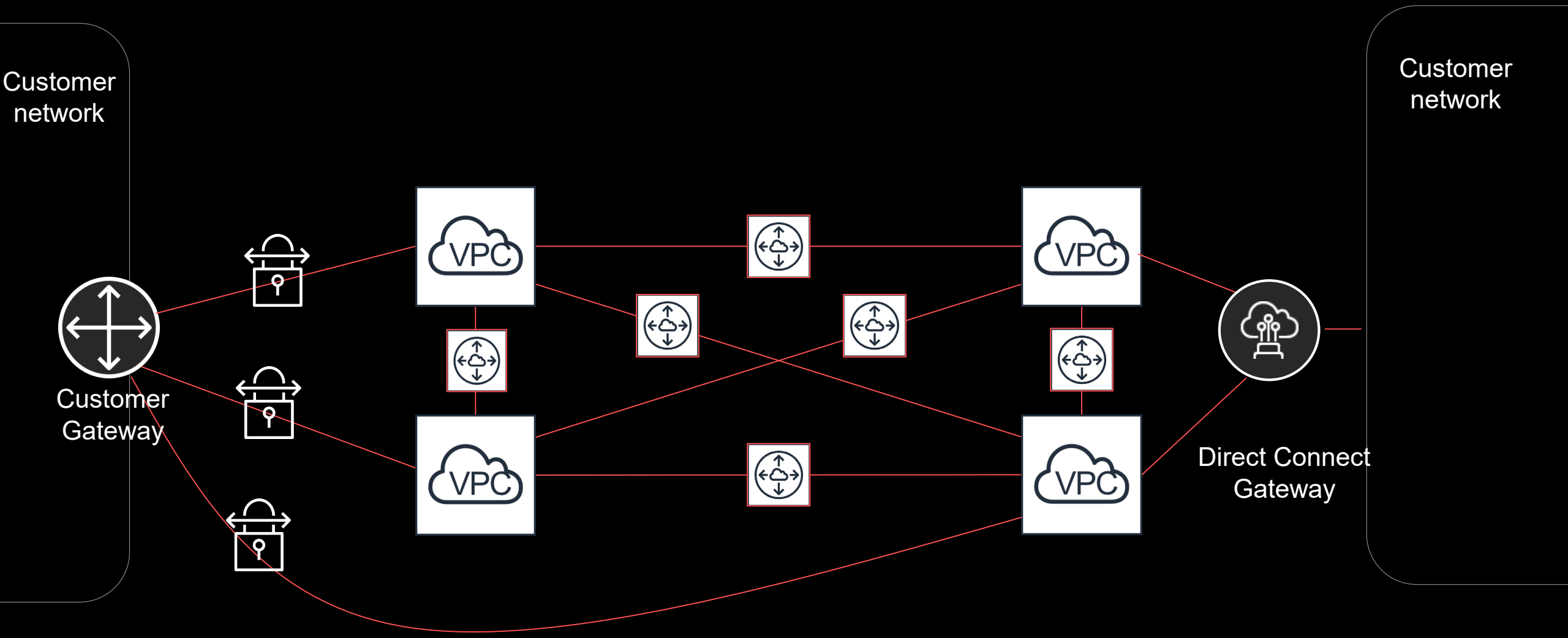
AWS Direct Connect basics



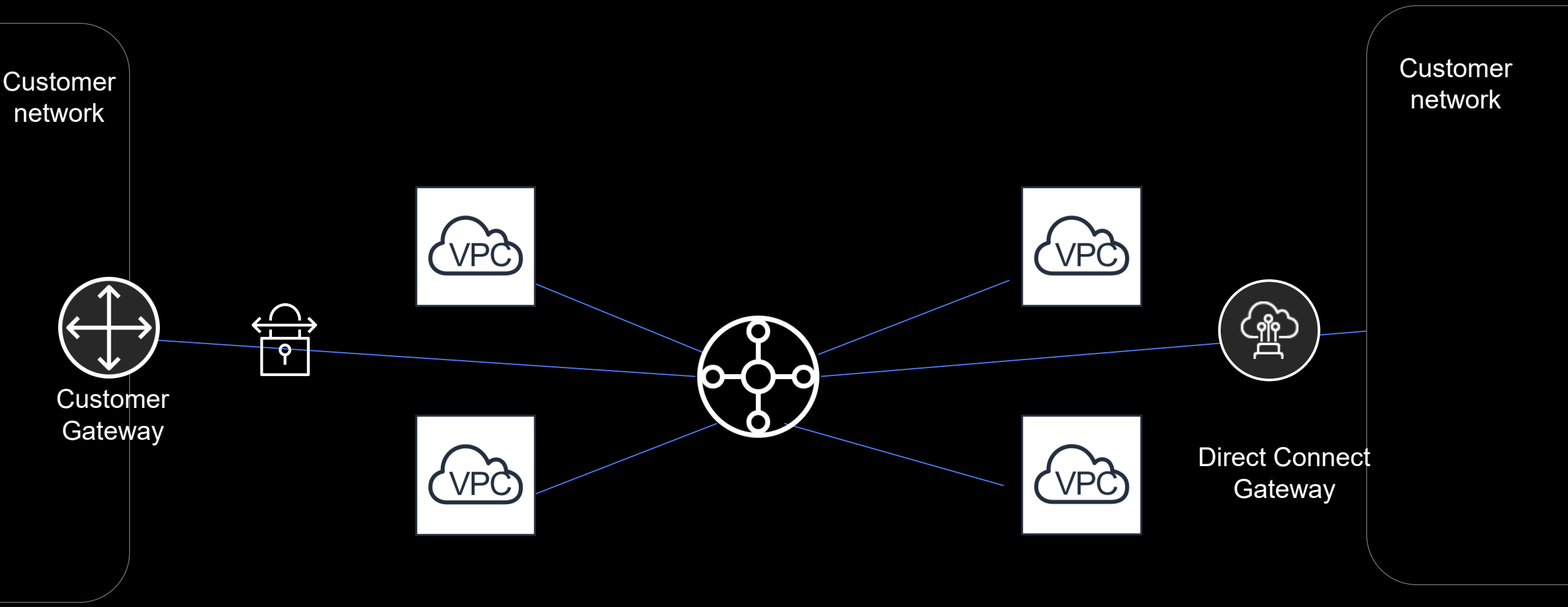
AWS Direct Connect – Multiple VPCs



Before Transit Gateway …



With Transit Gateway …

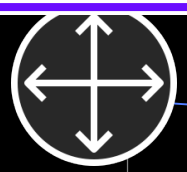


With Transit Gateway …

VPC Route table

Destination	Target
172.31.0.0/16	local
2600:1f16:14d:6300::/56	local
172.16.0.0/12	tgw-0541728e5c83ff1f0
192.168.0.0/16	tgw-0541728e5c83ff1f0

Route to on-premise via TGW



Customer
G

TGW Rou

Route to on-premise via VPN (or Direct Connect)

CIDR	Attachment	
172.29.0.0/16	tgw-attach-014e632db828232dc |	
172.30.0.0/16	tgw-attach-04caee7179f146894 | vpc-15609	VPC
172.31.0.0/16	tgw-attach-07af5c4fc91783865 | vpc-07bd0 cd2945108a	VPC
192.168.0.0/16	2 Attachments	VPN

What about DNS?

Amazon Route 53 Resolver for hybrid clouds

Step1
Configure endpoints

Step2
Configure inbound endpoint

Step3
Configure outbound endpoint

Step4
Create rule

Step5
Review and create

Configure endpoints

Endpoints provide the information that Resolver needs to route DNS queries from your VPCs to your network, from your network to your VPCs, or both.

You are signed in to the following region: us-west-2
To change your region use the region selector in the upper-right corner.

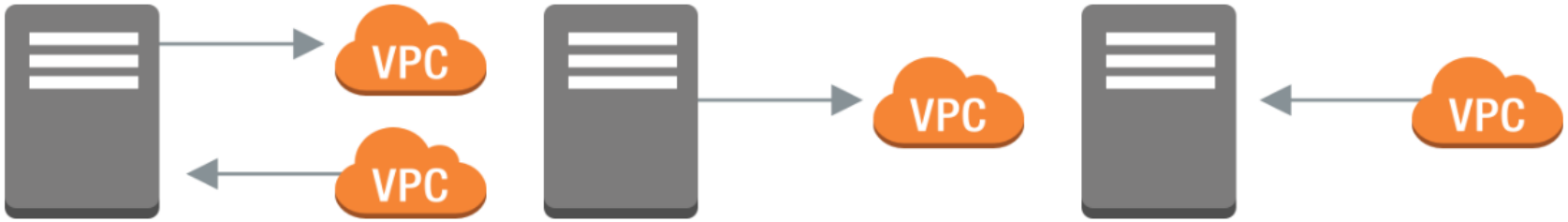
Conditional forwarding rules

Basic configuration

Direction of DNS queries info

You can configure endpoints for inbound DNS queries (to your VPC), outbound DNS queries (from your VPC), or both.

- Inbound and outbound
  Configure endpoints that allows DNS queries both to and from your VPC
- Inbound only
  Configure an endpoint that allows DNS queries to your VPC from an on-premises network or another VPC.
- Outbound Only
  Configure an endpoint that allows DNS queries from your VPC to an on-premises network or another VPC.



Cancel Previous Next

…and there's more

…more AWS networking

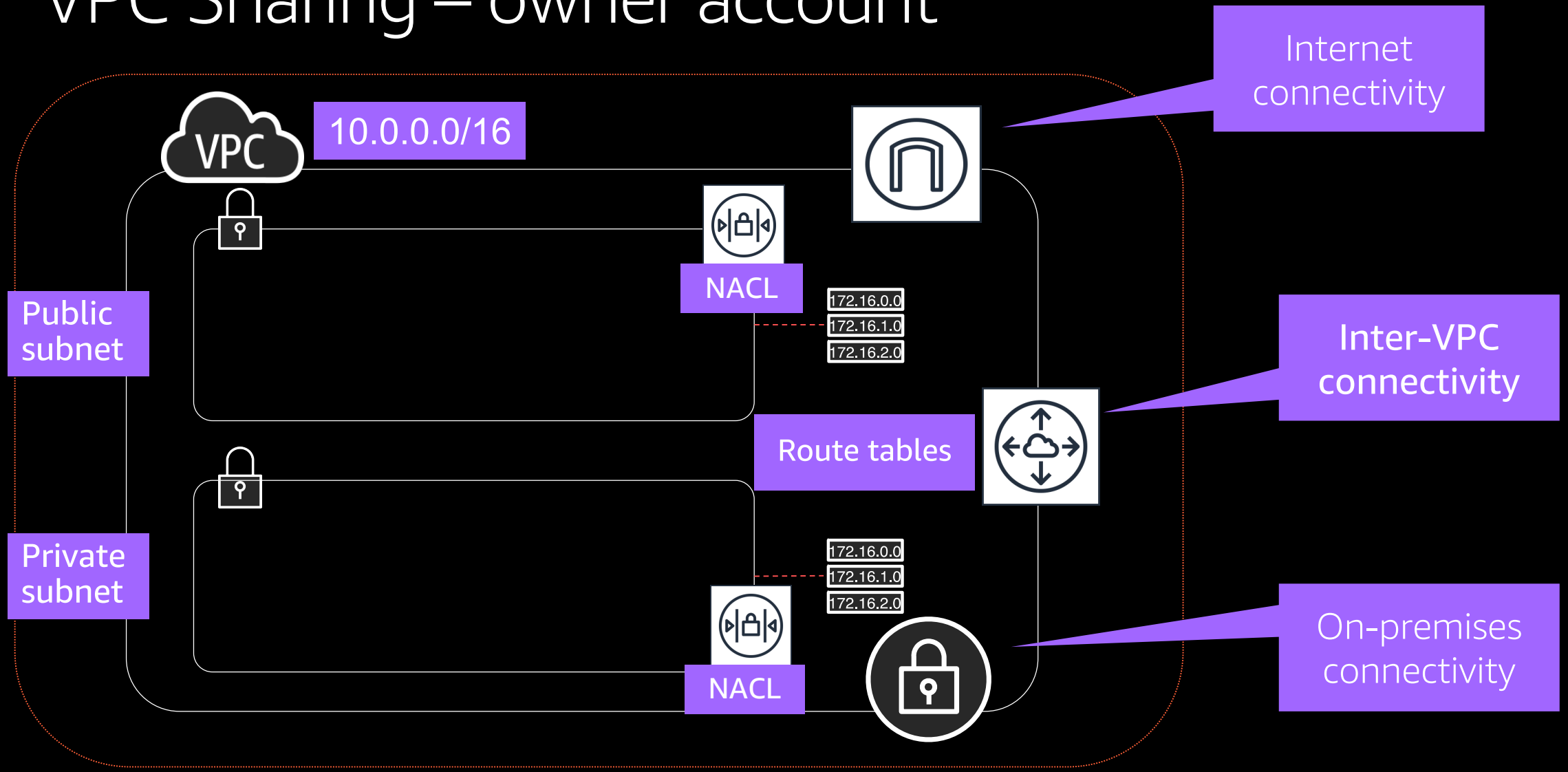
VPC Sharing

VPC endpoints and AWS PrivateLink

Amazon Global Accelerator

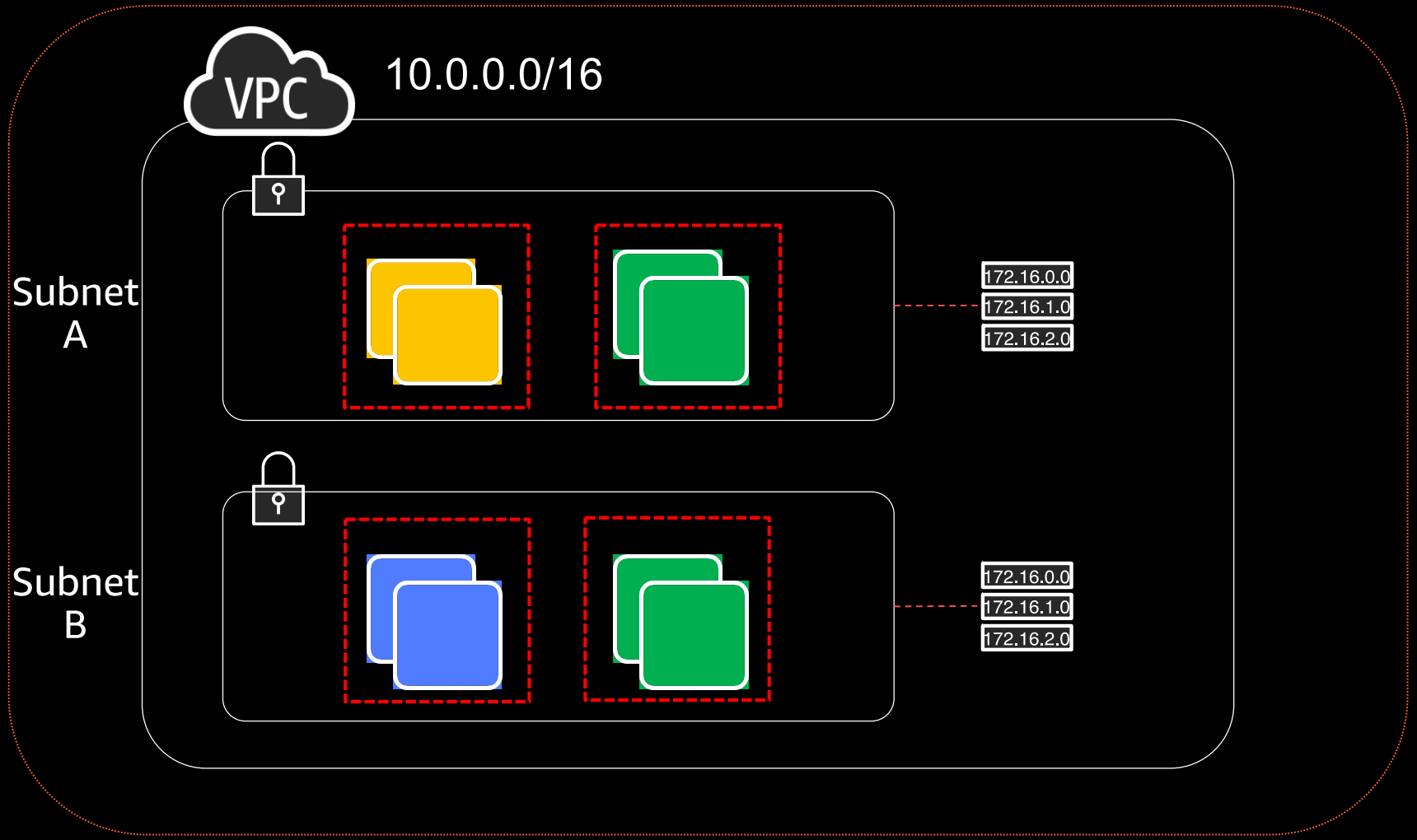
Sharing VPC resources

VPC Sharing – owner account



Infrastructure account

VPC Sharing – participant account



Account Web

- Subnet A

Account DB

- Subnet B

Account APP

- Subnet A
- Subnet B

Why VPC sharing?

Preserve IP space

Use fewer IPv4 CIDRs

Interconnectivity

No VPC Peering required

Separation of duties

A central team can create and manage your Amazon VPC

Billing and Security

Continue to enjoy segregation with multiple accounts

Same AZ cost for data transfer is nil!

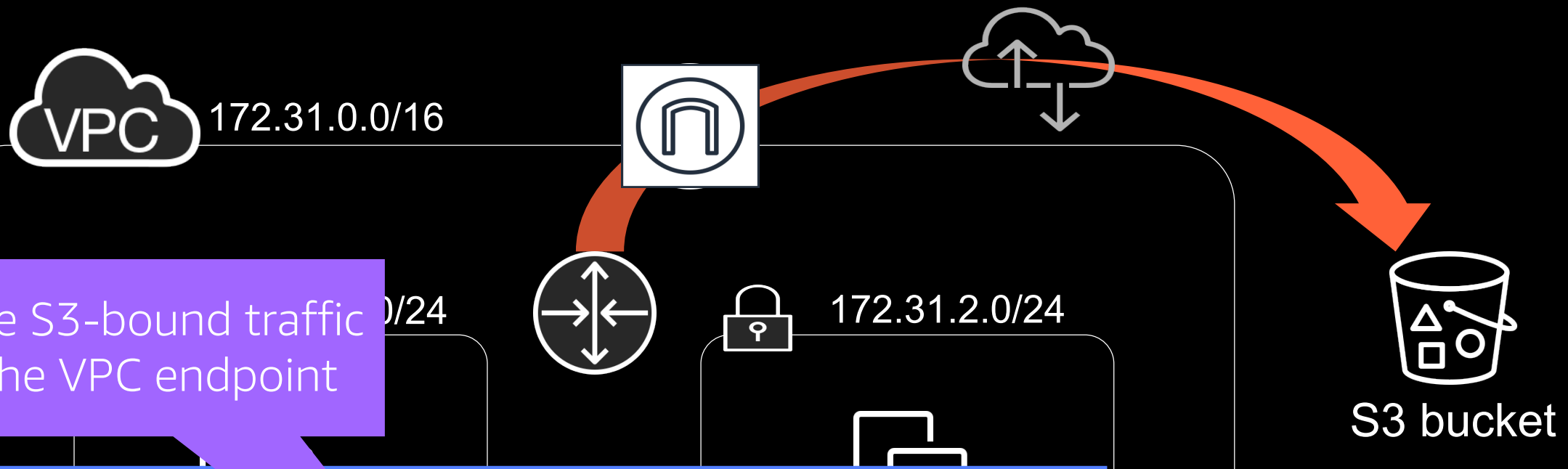
Gateway VPC endpoints

Interface VPC endpoints

PrivateLink

VPC endpoints

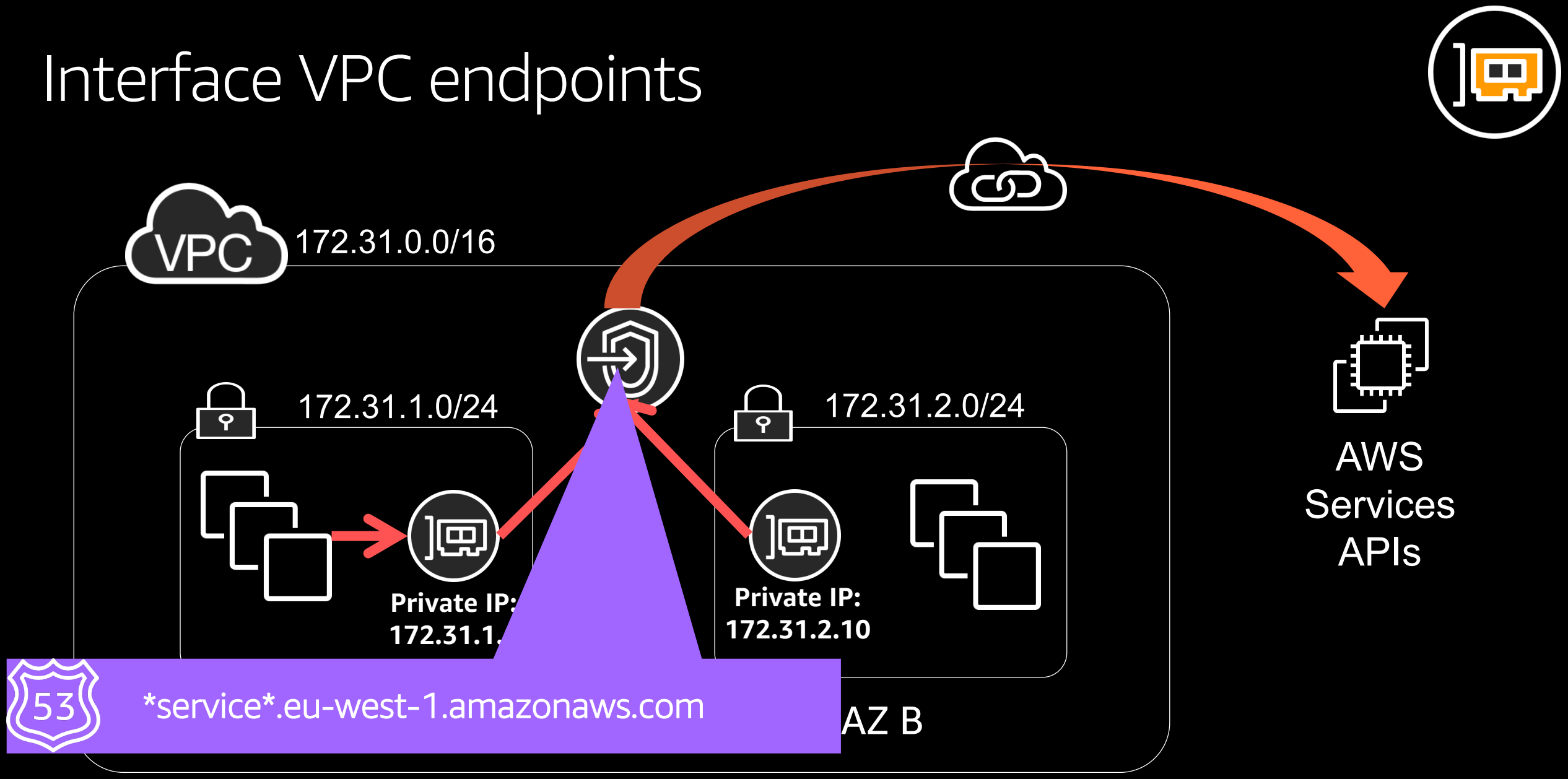
Gateway VPC endpoints: Amazon S3 and DynamoDB



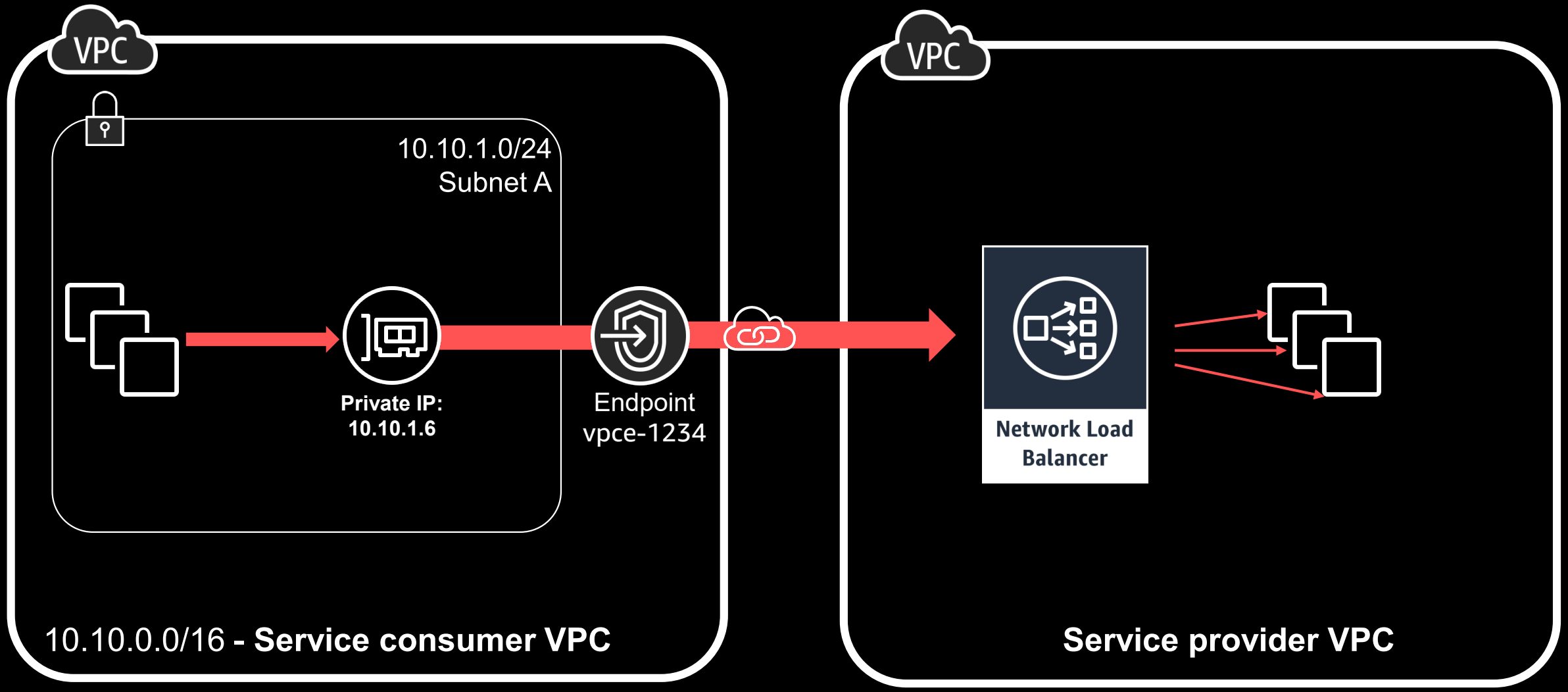
Route S3-bound traffic to the VPC endpoint

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
pl-7ba54012 (com.amazonaws.us-east-2.s3)	vpce-00f8835c705bc0fdb	Active	No

Interface VPC endpoints



AWS PrivateLink: VPC endpoint services



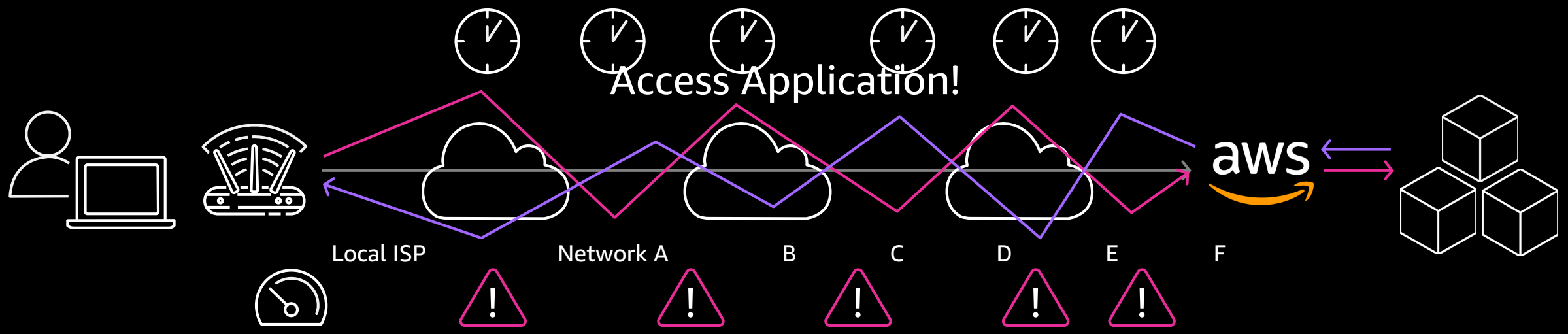
Amazon Global Accelerator

Introducing AWS Global Accelerator

NEW!

A network layer service that you can deploy in front of your Internet facing applications to improve availability and performance for your globally distributed users

Introducing AWS Global Accelerator



Accessing your application is not as straightforward!

Paths to and from the application may differ

Each hop impacts performance and can introduce risk

Accessing your web applications with AWS Global Accelerator

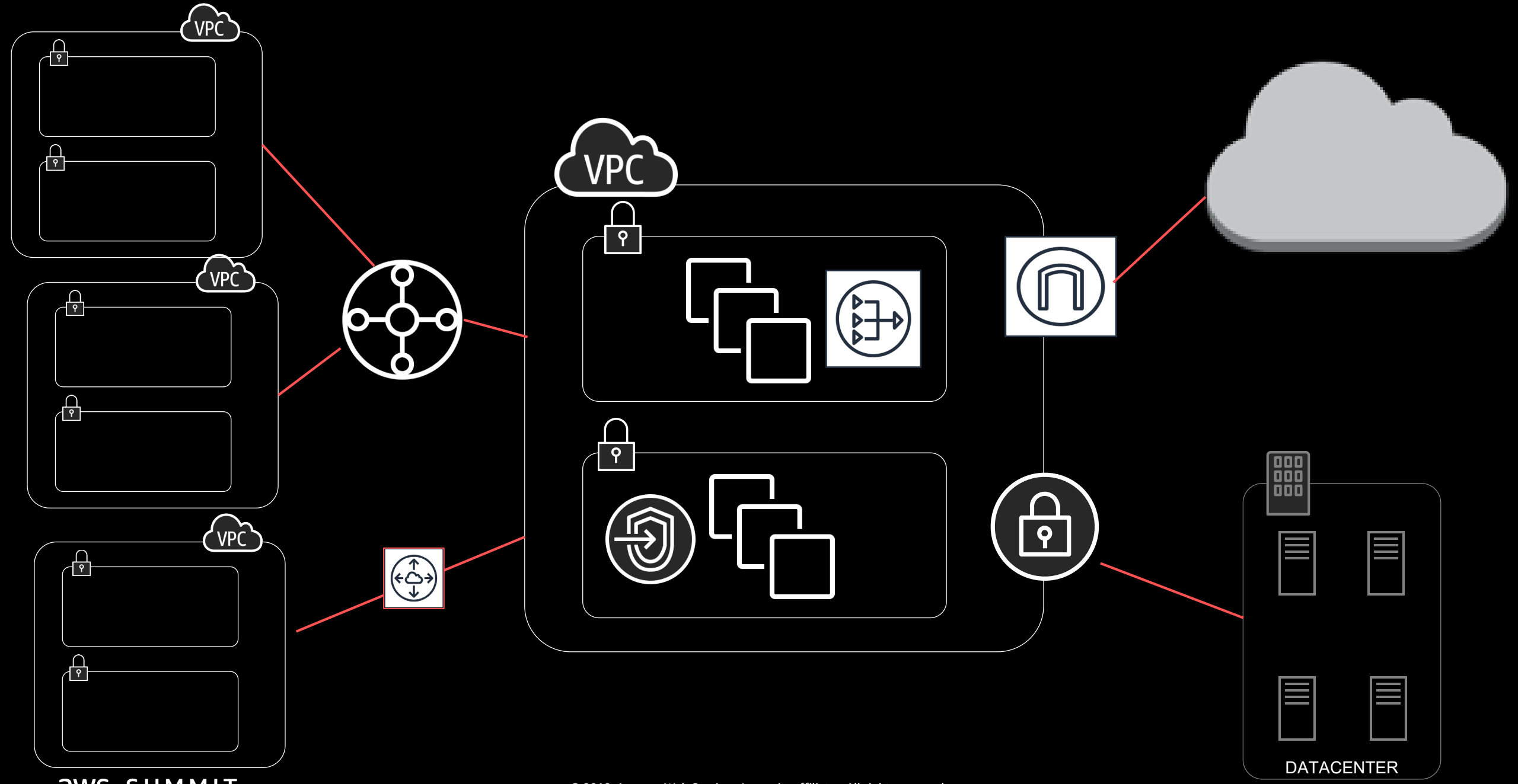
Adding AWS Global Accelerator removes these inefficiencies

Leverages the Global AWS Network

Resulting in improved performance

Wrap-up

aws SUMMIT



aws SUMMIT

Thank you!

Perry Wald
perrwald@amazon.co.uk

Tom Adamski
tomada@amazon.co.uk

aws SUMMIT

Please complete the session survey.