
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

BOA320

Demystifying VPC IP addressing & creating a complete routing solution

Du'An Lightfoot
Sr. Developer Advocate
AWS

Ankit Chadha
Sr. Networking Solutions Architect
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

IP addressing at scale

Amazon VPC IP Address Manager (IPAM)

Automating a global network

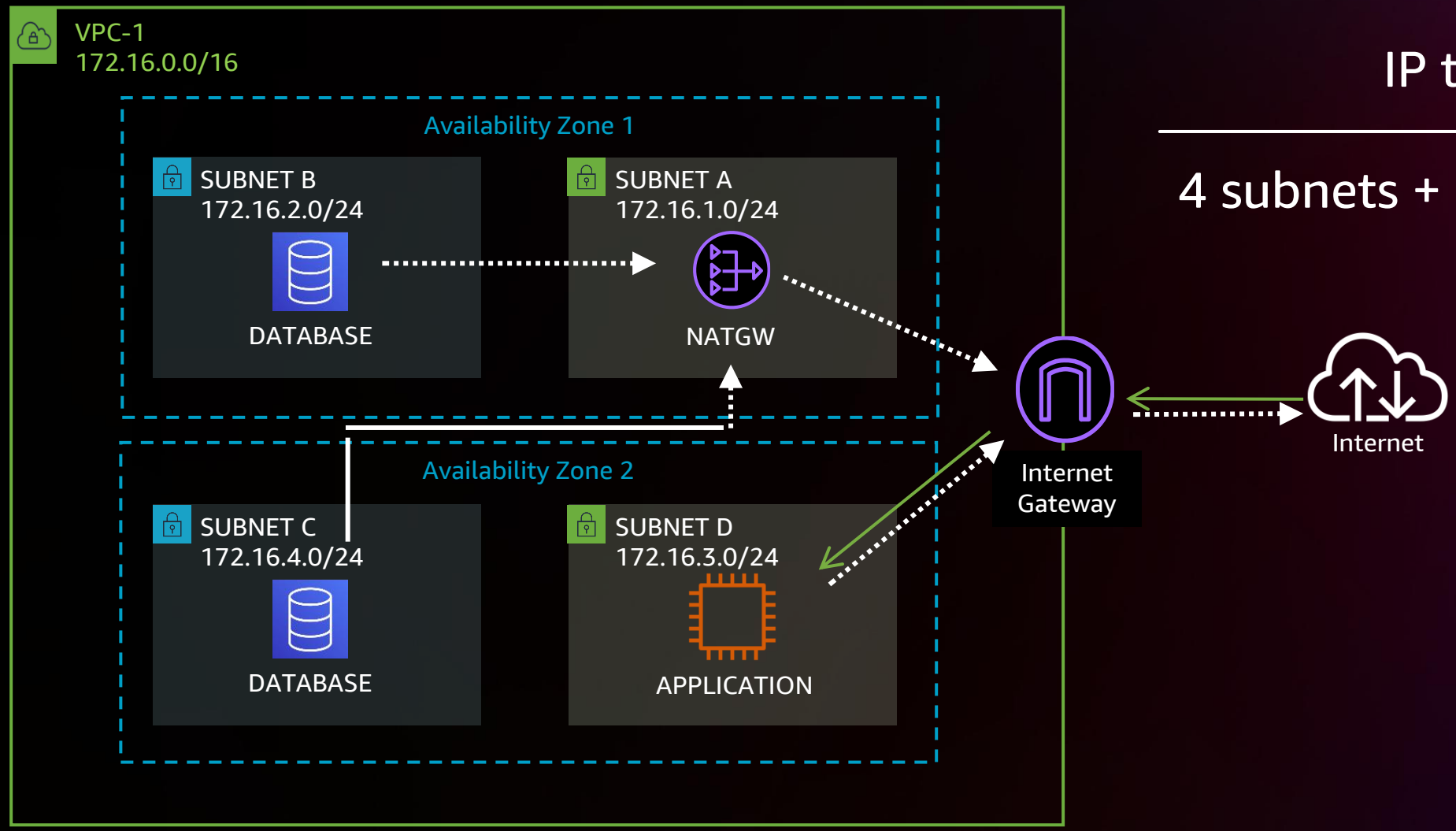
Real world solution

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IP addressing at scale

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IP addressing in Amazon VPC

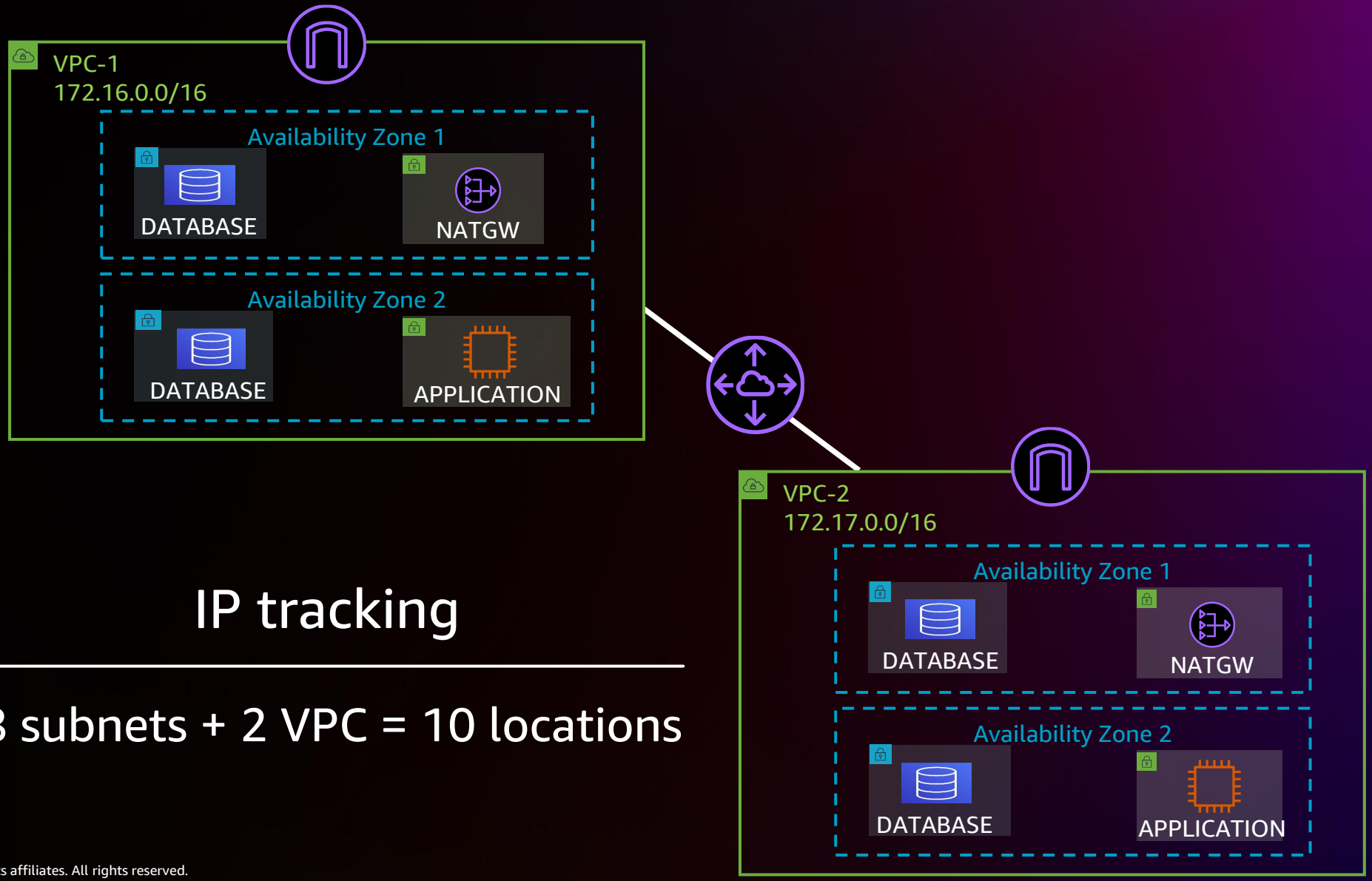


IP tracking

4 subnets + 1 VPC = 5 locations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How networks grow

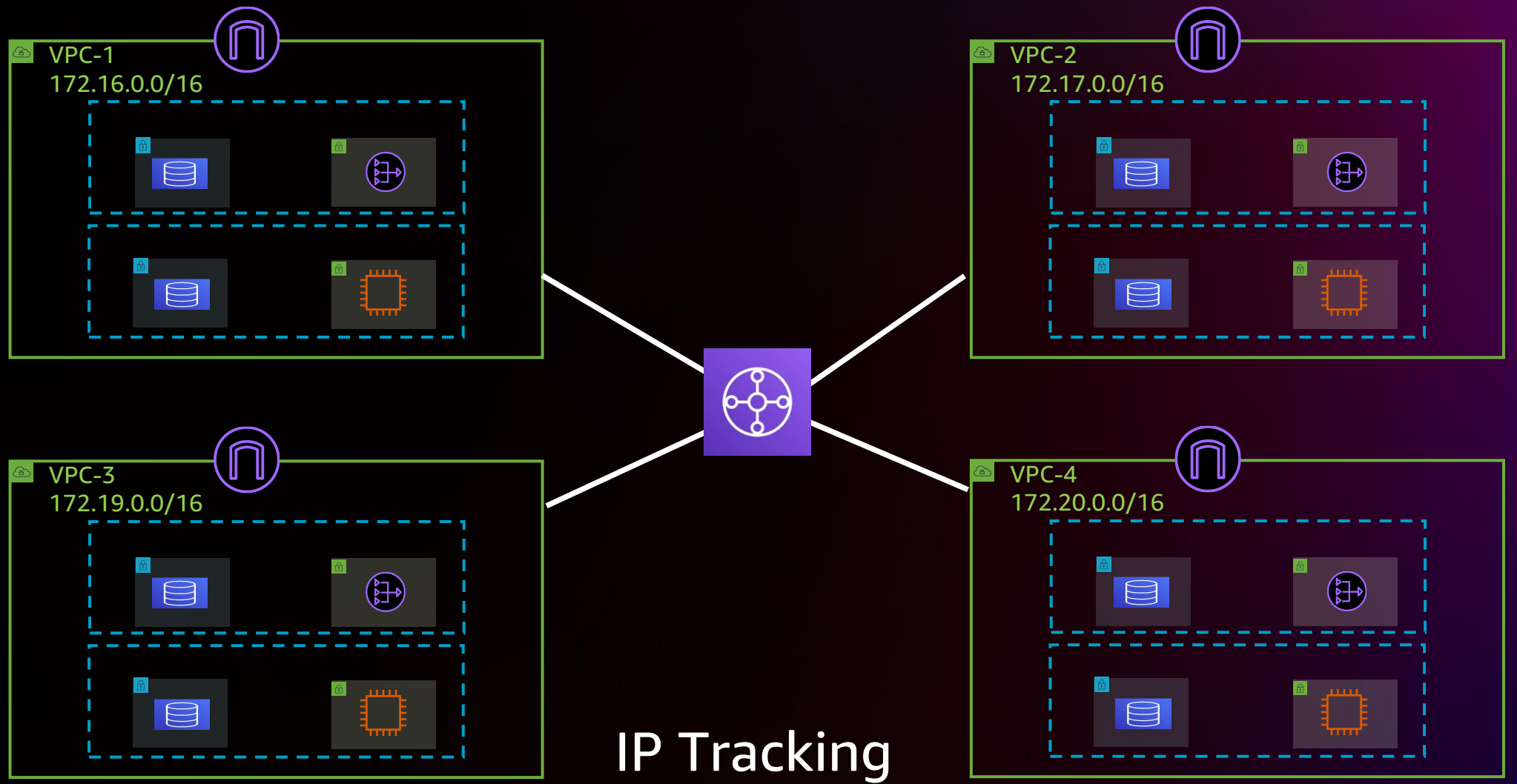


IP tracking

8 subnets + 2 VPC = 10 locations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How networks grow



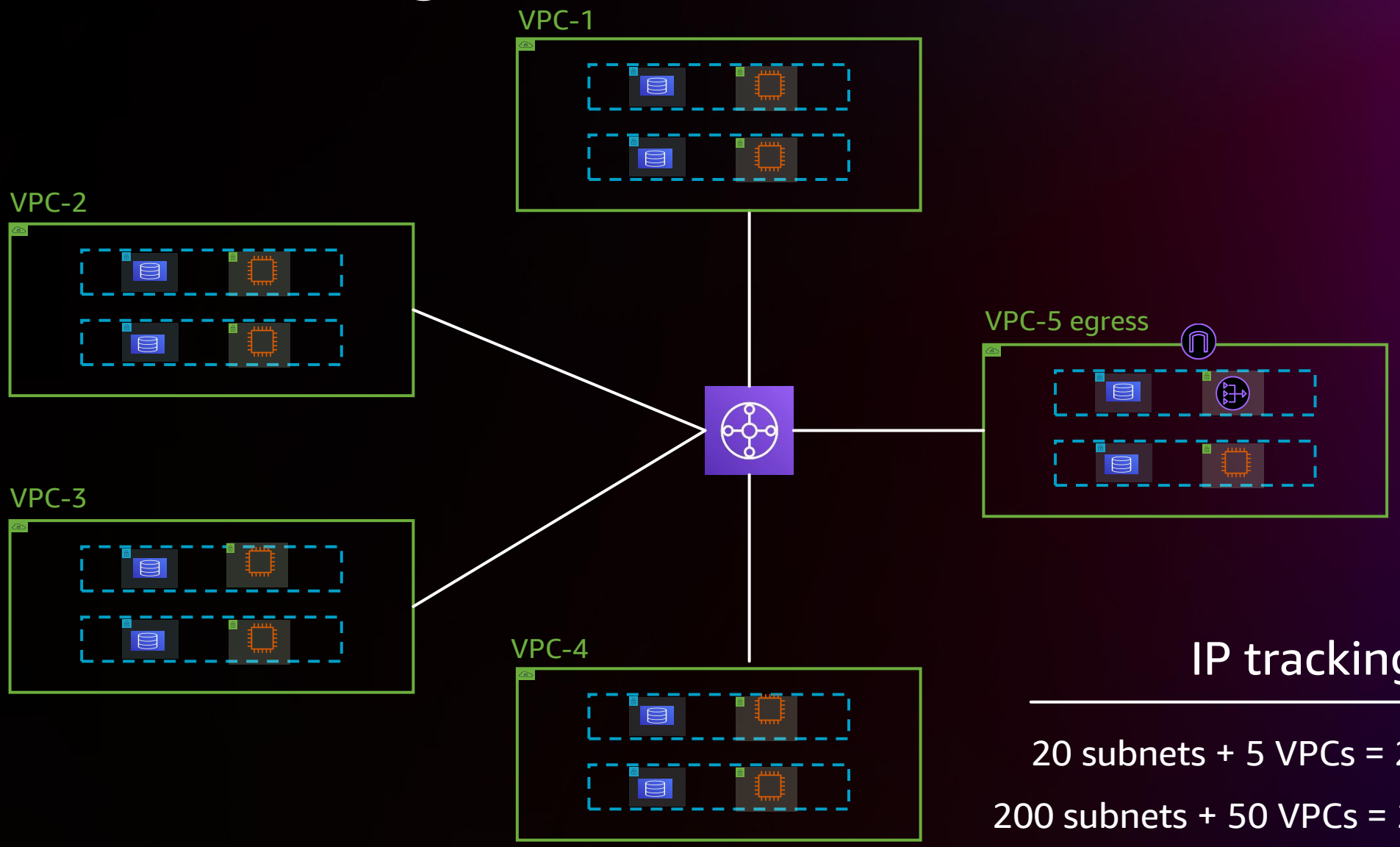
IP Tracking

16 subnets + 4 VPCs = 20 locations

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How networks grow



IP tracking

20 subnets + 5 VPCs = 25 locations

200 subnets + 50 VPCs = 250 locations

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do you manage that?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Simple!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Range	Mask	Available?	User	Description
10.0.1.0	/24	N	Bob	Database
10.0.2.0	/24	N	Mary	Kafka
10.0.3.0	/24	N	Richard	Kafka
10.0.4.0	/24	N	Richard	App 321
10.0.5.0	/24	N	Richard	App 321
10.0.6.0	/24	N	Nikhil	Transit VPC
10.0.7.0	/24	N	Shirley	Tape backup
10.0.8.0	/24	Y		
10.0.9.0	/24	Y		
10.0.10.0	/24	N	Nikhil	SDWAN deployment
10.0.11.0	/24	N	Shirley	Tape backup
10.0.12.0	/24	N	Richard	On-premises connectivity
10.0.13.0	/24	N	Bob	VPN Backup
10.0.14.0	/24	N	Mary	VPC Test
10.0.15.0	/24	Y		
10.0.16.0	/24	N	Richard	Dev Environment
10.0.17.0	/24	N	Richard	Tape backup
10.0.18.0	/24	N	Nikhil	VPN Backup
10.0.19.0	/24	N	Shirley	App 501
10.0.20.0	/24	Y		
10.0.21.0	/24	Y		
10.0.22.0	/24	Y		

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What’s wrong with this picture?



Manual updates of single spreadsheet



Limited visibility into allocation and usage

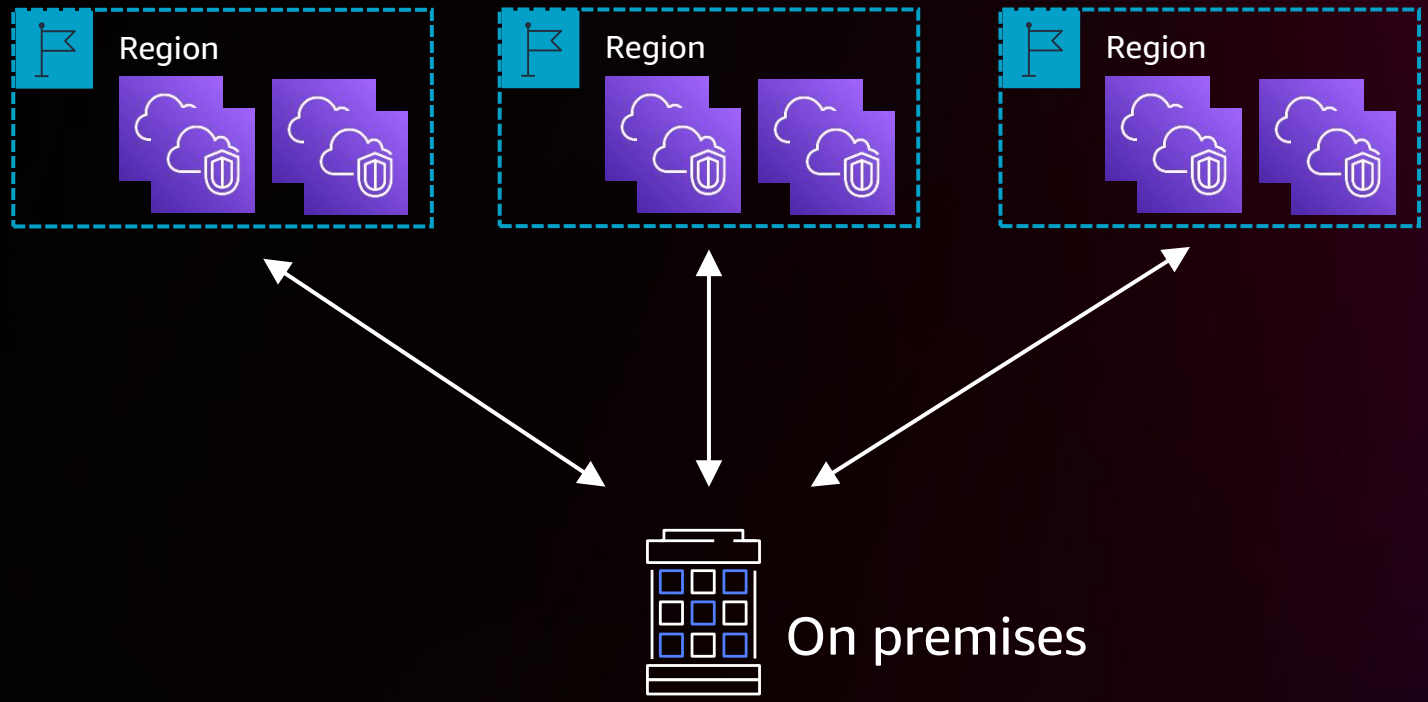


Limited ability to manage IP allocations at scale

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Need to automate IP assignment as you scale

Taking longer to find nonconflicting IPs



Needs to assign CIDRs **faster** to developers

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager (IPAM)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is IPAM?



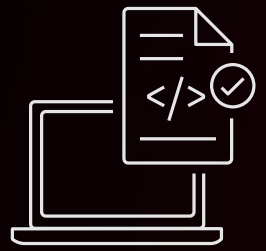
Plan, track, and monitor IP addresses across AWS accounts and AWS Regions

Works for IPv4 and IPv6



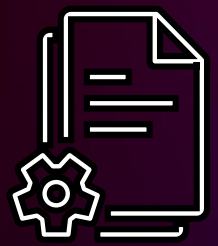
Automate IP assignments

Automate across multiple Regions and accounts based on your application's unique networking and security needs



Monitor across the network

Avoid downtime with overlap detection, tracking IPs in compliance with security policy, and utilization trends



Retrospective analysis

Faster troubleshooting and auditing

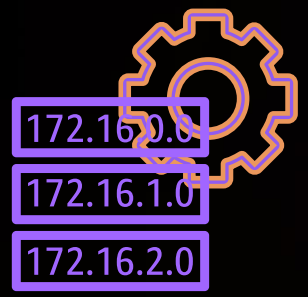
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How IPAM works: IPAM setup

Create IPAM

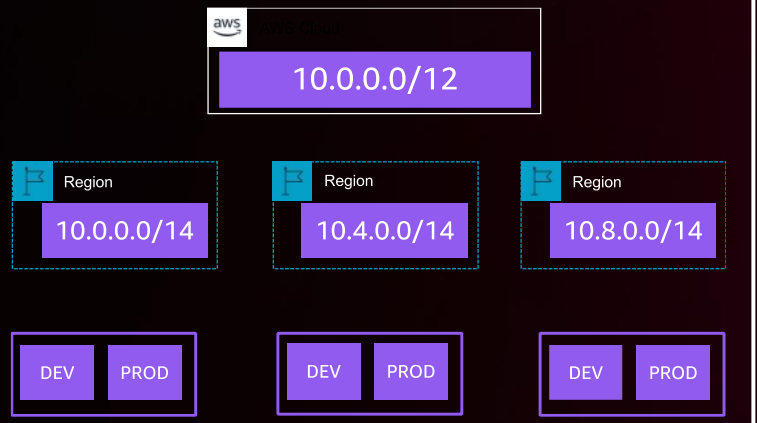
Single IPAM to manage IPs across Regions and accounts



IPAM provides you with the flexibility to host it in any Region

(Typically, you choose the Region where most of your workloads reside.)

Arrange IPs based on routing and security needs



An example for organizing IPs

Set business rules for allocation



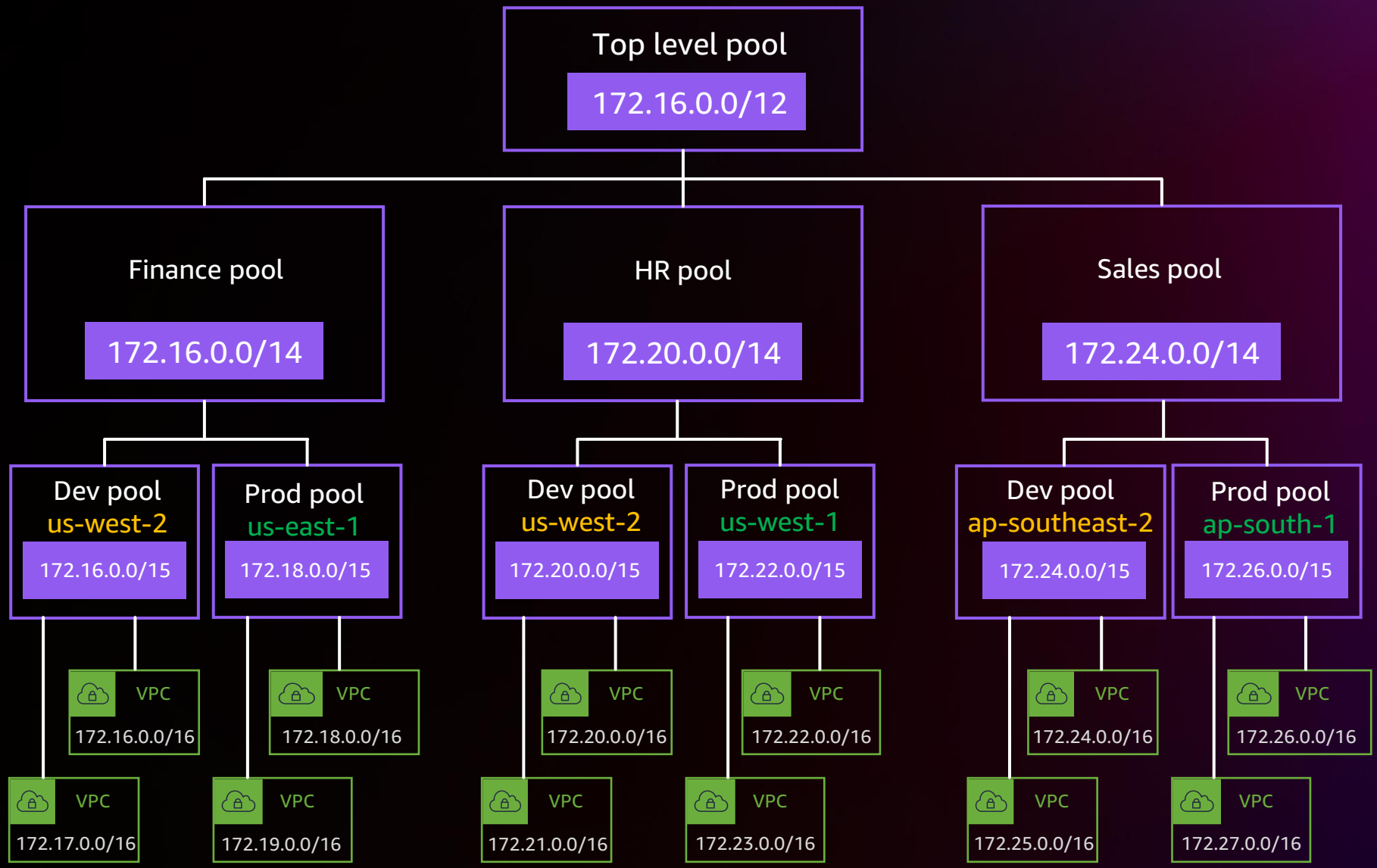
Examples:

- Which account can use IPs
- Regions where IPs can be used

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

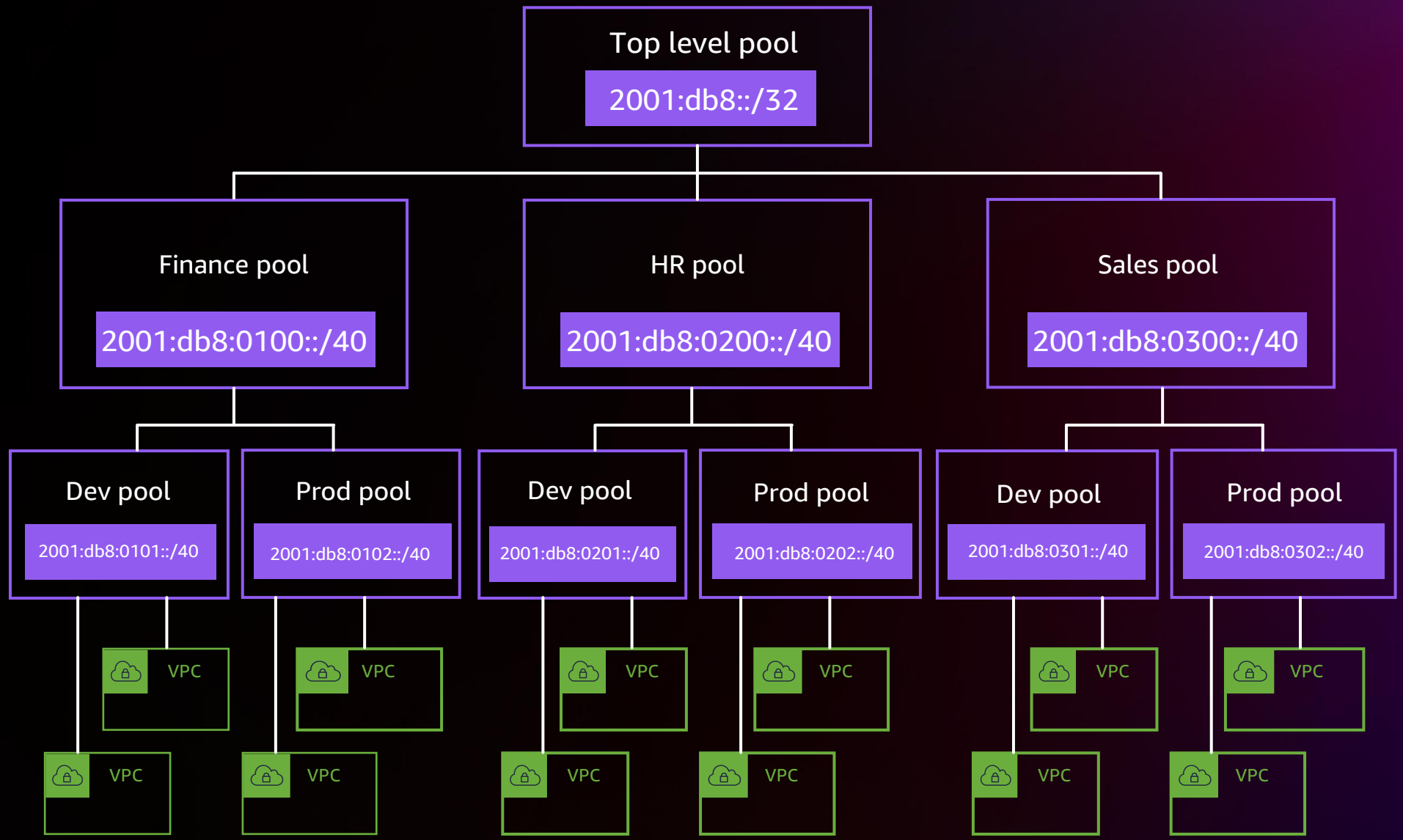
Private scope



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

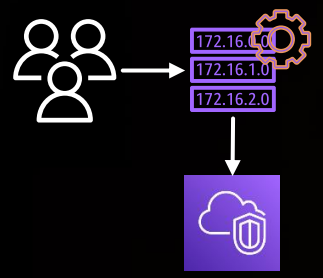
Public scope



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

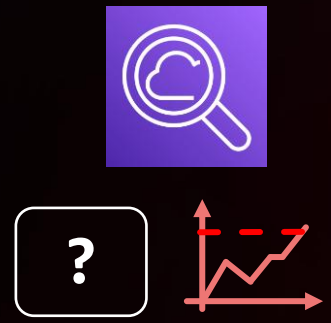
How IPAM Works: Automate Workflow

Automate IP assignment



Developers directly use IPAM for assignment
IPAM assigns based on business rules
(no more tickets or email)

Monitor
Get actionable insights



Track IPs during troubleshooting
IP utilization for capacity planning
Alerts on overlapping CIDRs

Audit
Retain IP monitor data for up to 3 years



Security audits
Routine compliance check

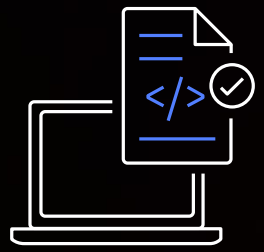
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager

IPAM

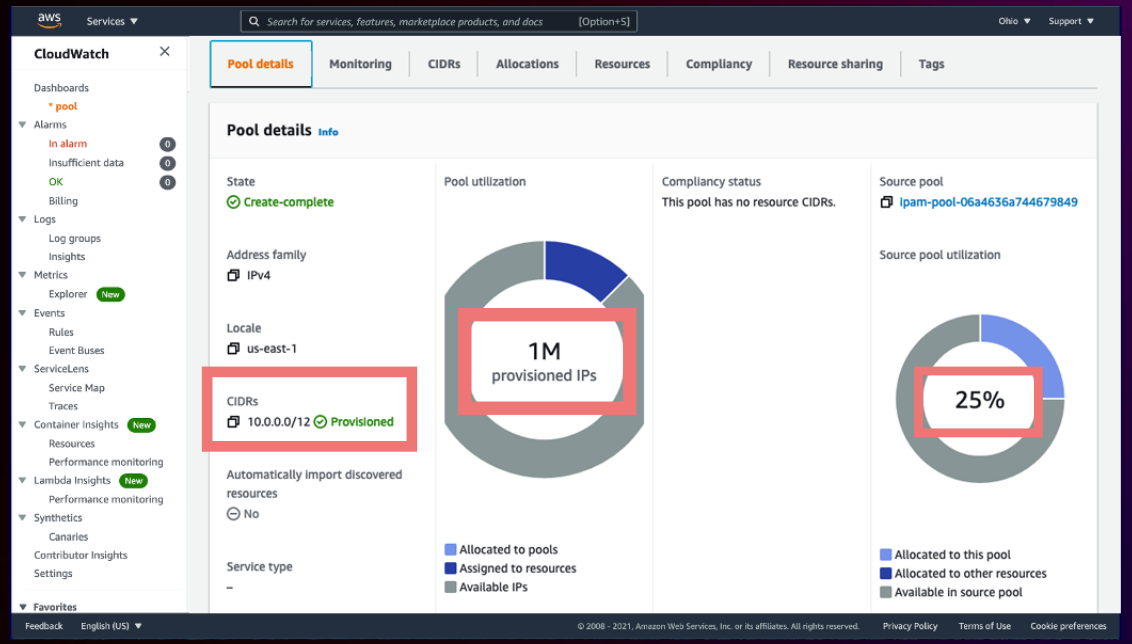
Monitoring and alerts





Monitor across network

Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends



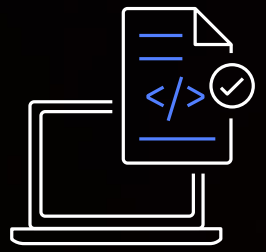
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager

IPAM

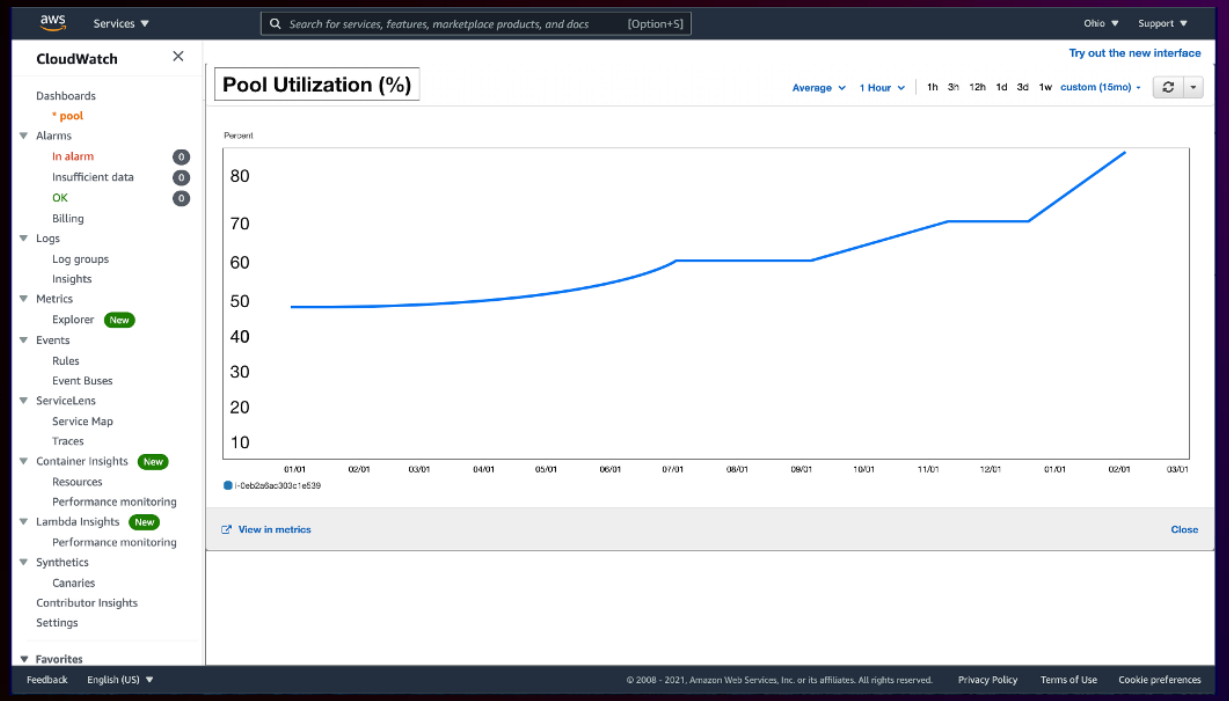
Monitoring and alerts





Monitor across network

Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends



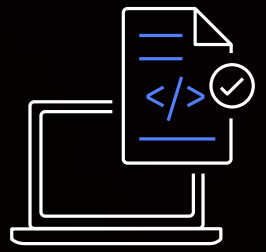
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager

IPAM

Monitoring and alerts





Monitor across network

Avoid downtime with overlap detection, IP security policy compliance tracking, and utilization trends

Your VPCs

Filter VPCs

Name	VPC ID	Owner ID	Region	State	IPv4 CIDR	IPv6 CIDR	IPv4 Pool	IPv6 Pool
W1-prev-dev-vpc	vpc-[redacted]	[redacted]	Us-west-1	Compliant	10.0.0.0/24		Us-west-1-dev	
W1-prev-test-vpc	vpc-[redacted]	[redacted]	Us-west-1	Compliant	10.4.0.0/24		Us-west-1-dev	
W1-prev-prod-vpc	vpc-[redacted]	[redacted]	Us-west-1	Compliant			-west-1-dev	
E1-prev-dev-vpc	vpc-[redacted]	[redacted]	Us-east-1	Non-compliant	10.1.0.0/24		Us-west-1-dev	
E1-prev-test-vpc	vpc-[redacted]	[redacted]	Us-east-1	Compliant	10.5.0.0/24		Us-west-1-dev	
E1-prev-prod-vpc	vpc-[redacted]	[redacted]	Us-east-1	Compliant	10.9.0.0/24		Us-west-1-dev	
Temp-test-vpc	vpc-[redacted]	[redacted]	Us-east-1	Unmanaged	172.31.0.0/24		UNKNOWN	

Tag on allocation policy don't match

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IP Address Manager

IPAM



SCAN ME

https://go.aws/3xLkthD

Amazon VPC IP Address Manager (IPAM)

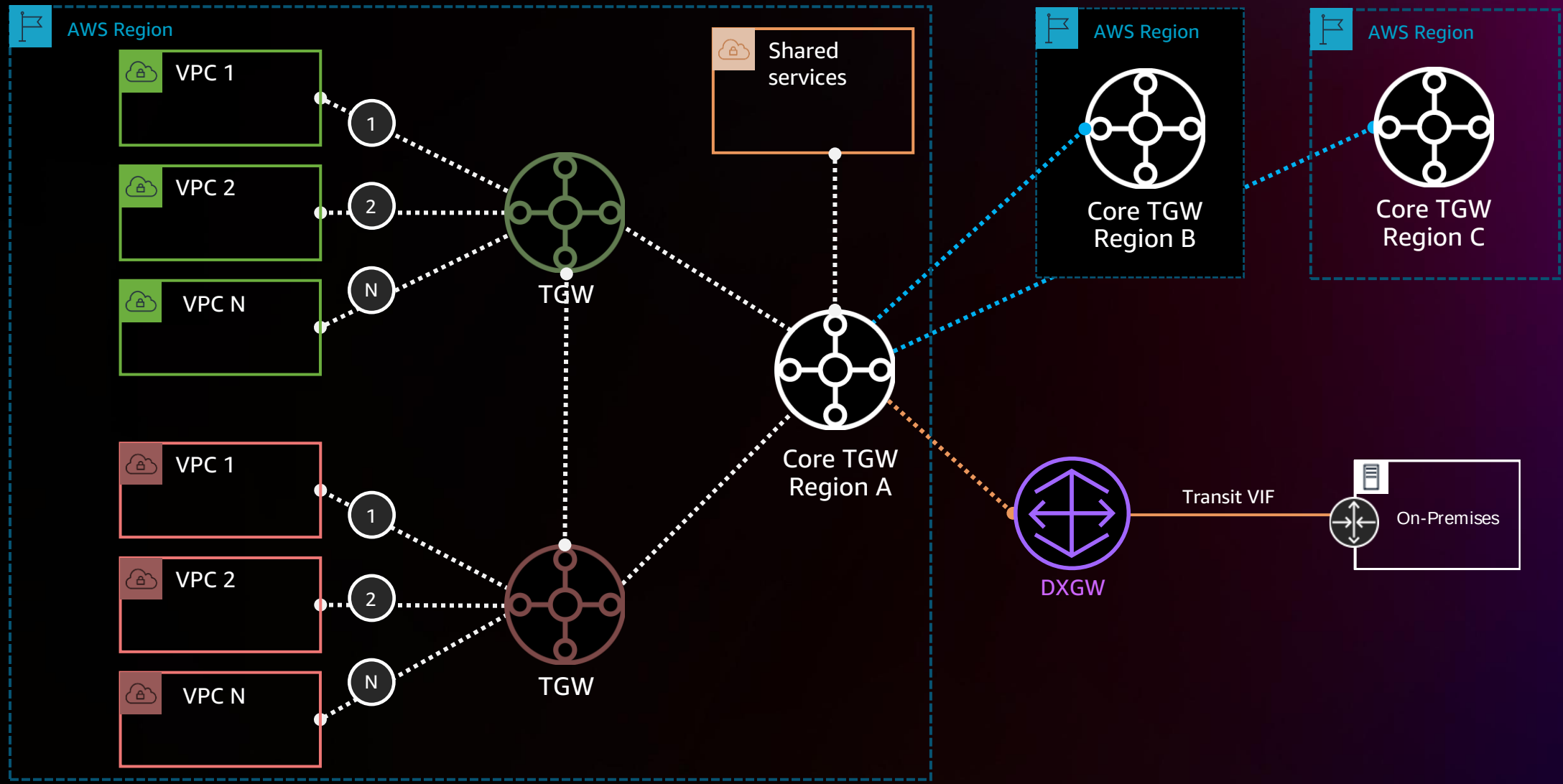
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automating a global network

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Global Network with Transit Gateway

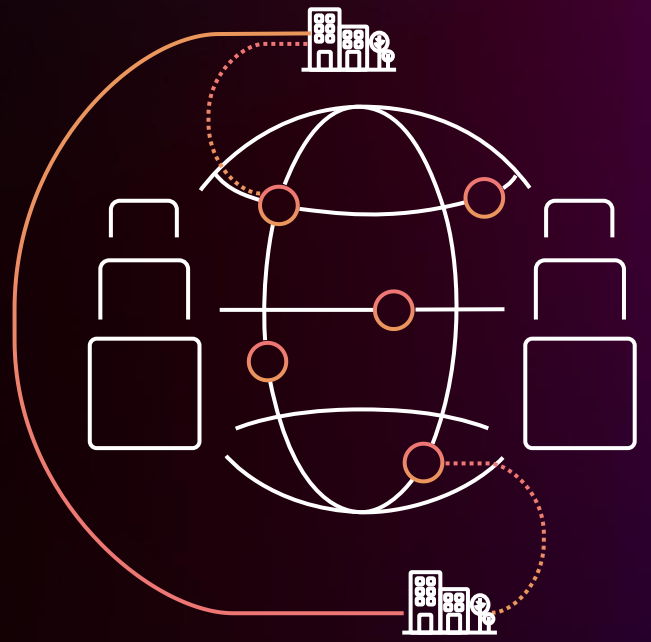


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

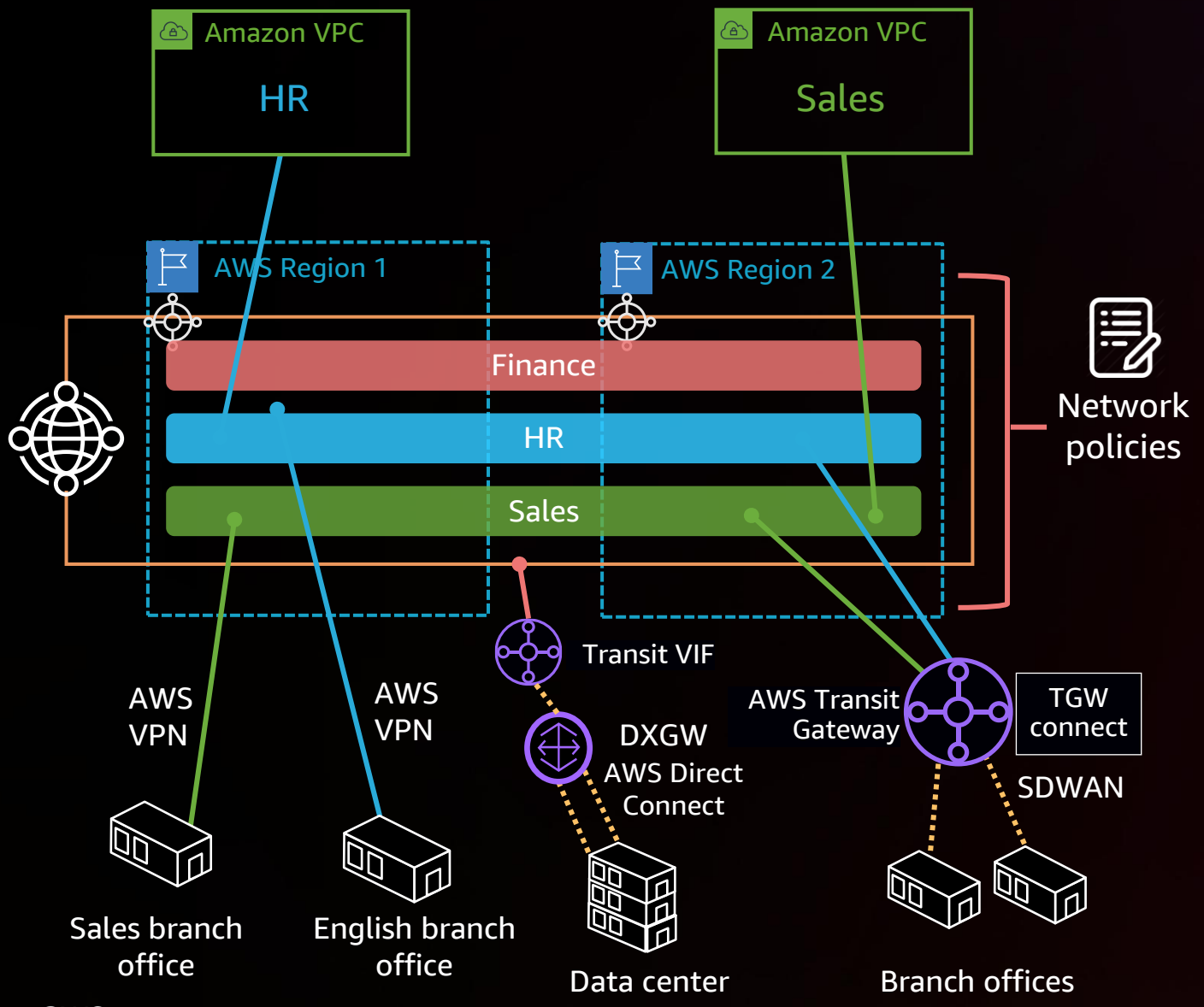
AWS Cloud WAN

BUILD, MANAGE, AND MONITOR GLOBAL WIDE AREA NETWORKS

- Unify your cloud and on-premises networks to reduce complexity
- Increase security with built-in network segmentation
- Visualize and monitor your global network on a single dashboard



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AWS Cloud WAN

Core network

The part of your global network managed by AWS

Core network edge

The regional connection point managed by AWS

Network segments

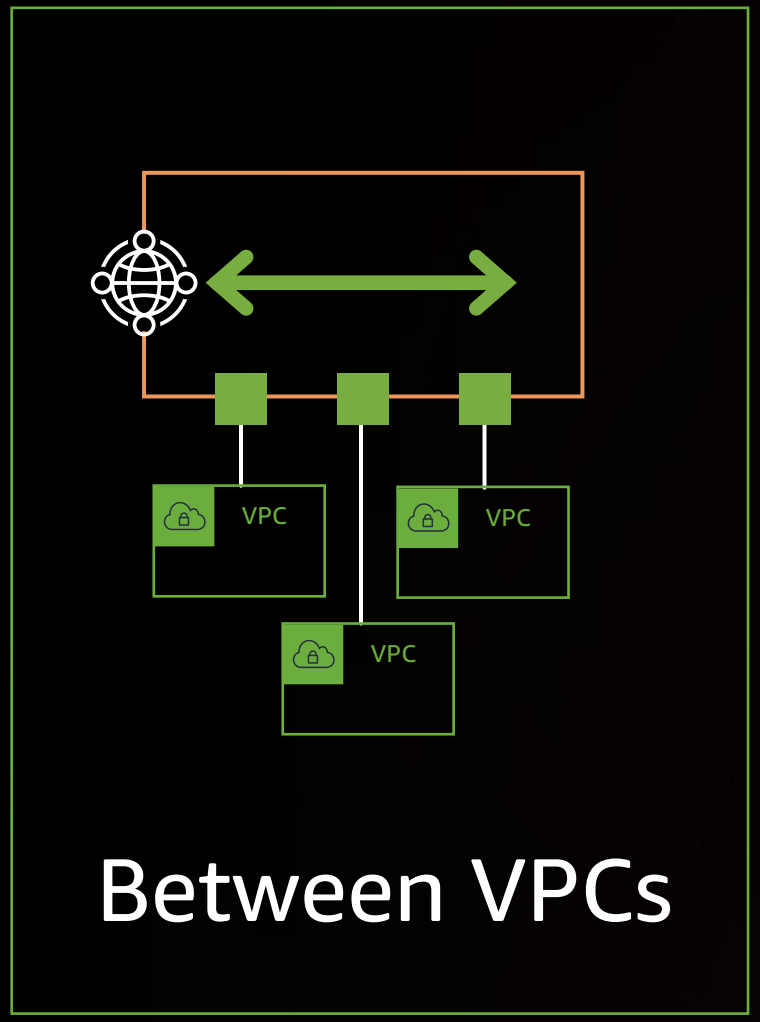
Isolation between VPCs and on-premises sites

Network policies

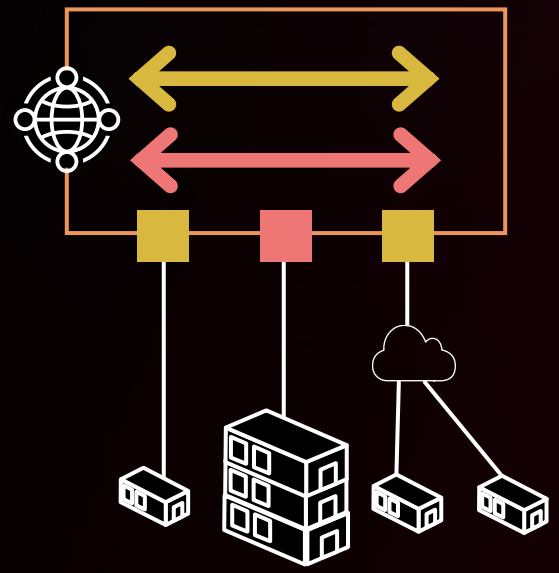
Define L3 routing policies based on attributes and behavior

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

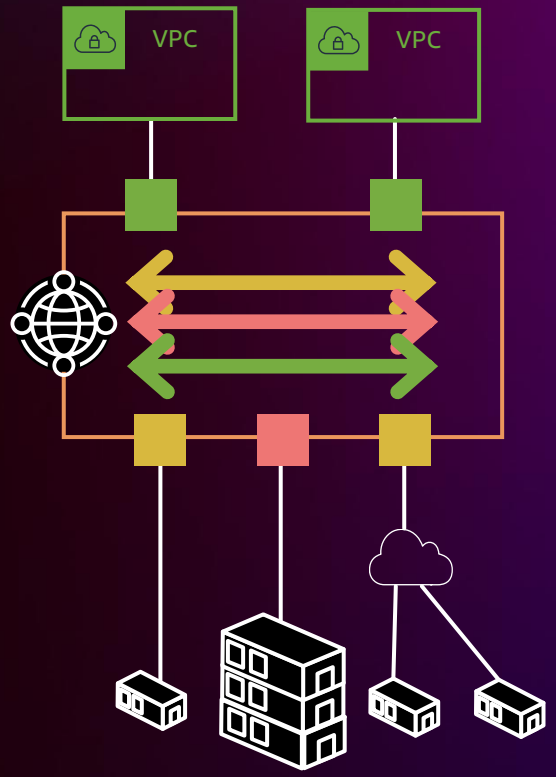
AWS Cloud WAN use cases



Between VPCs



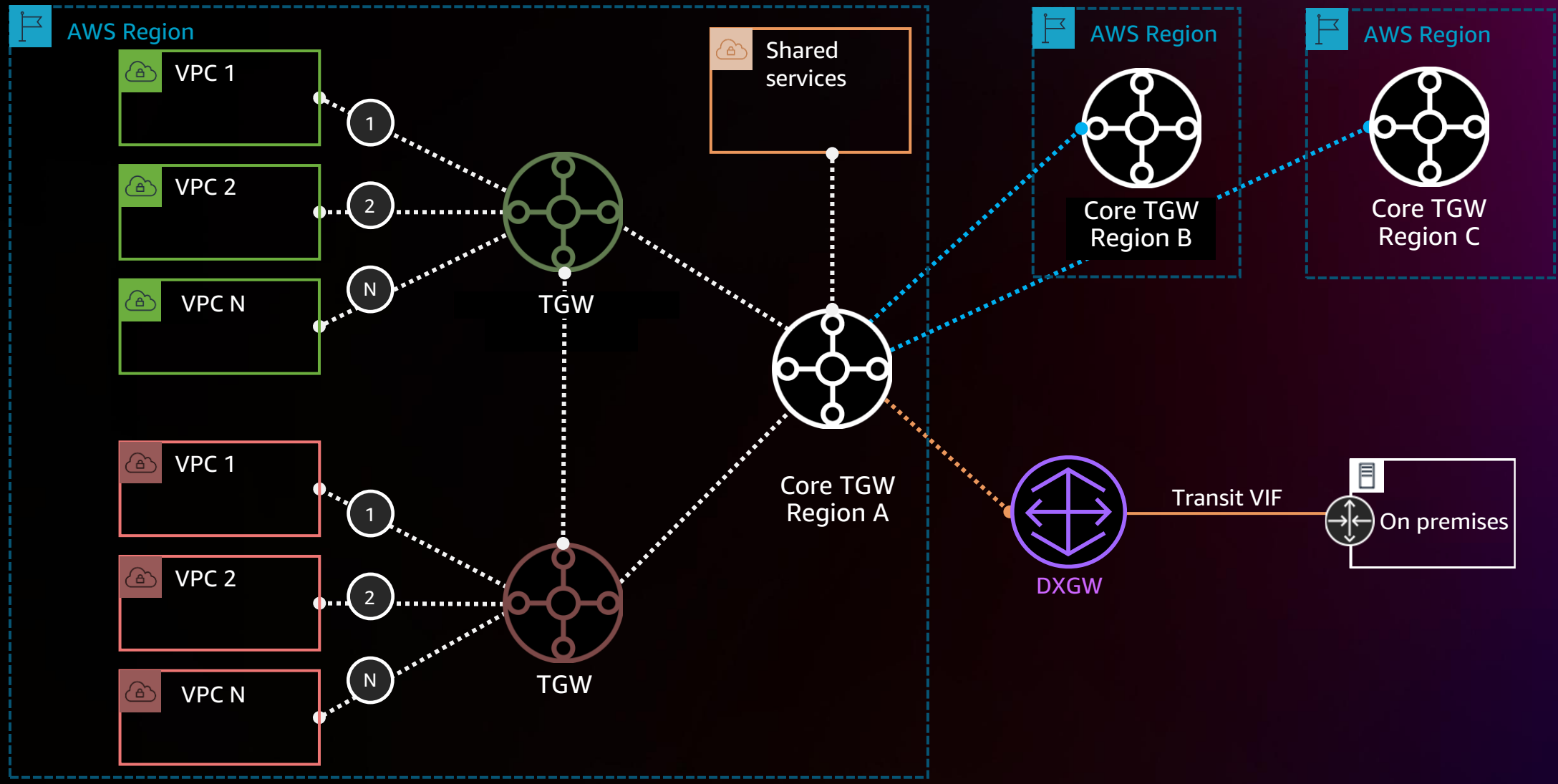
WAN



Hybrid

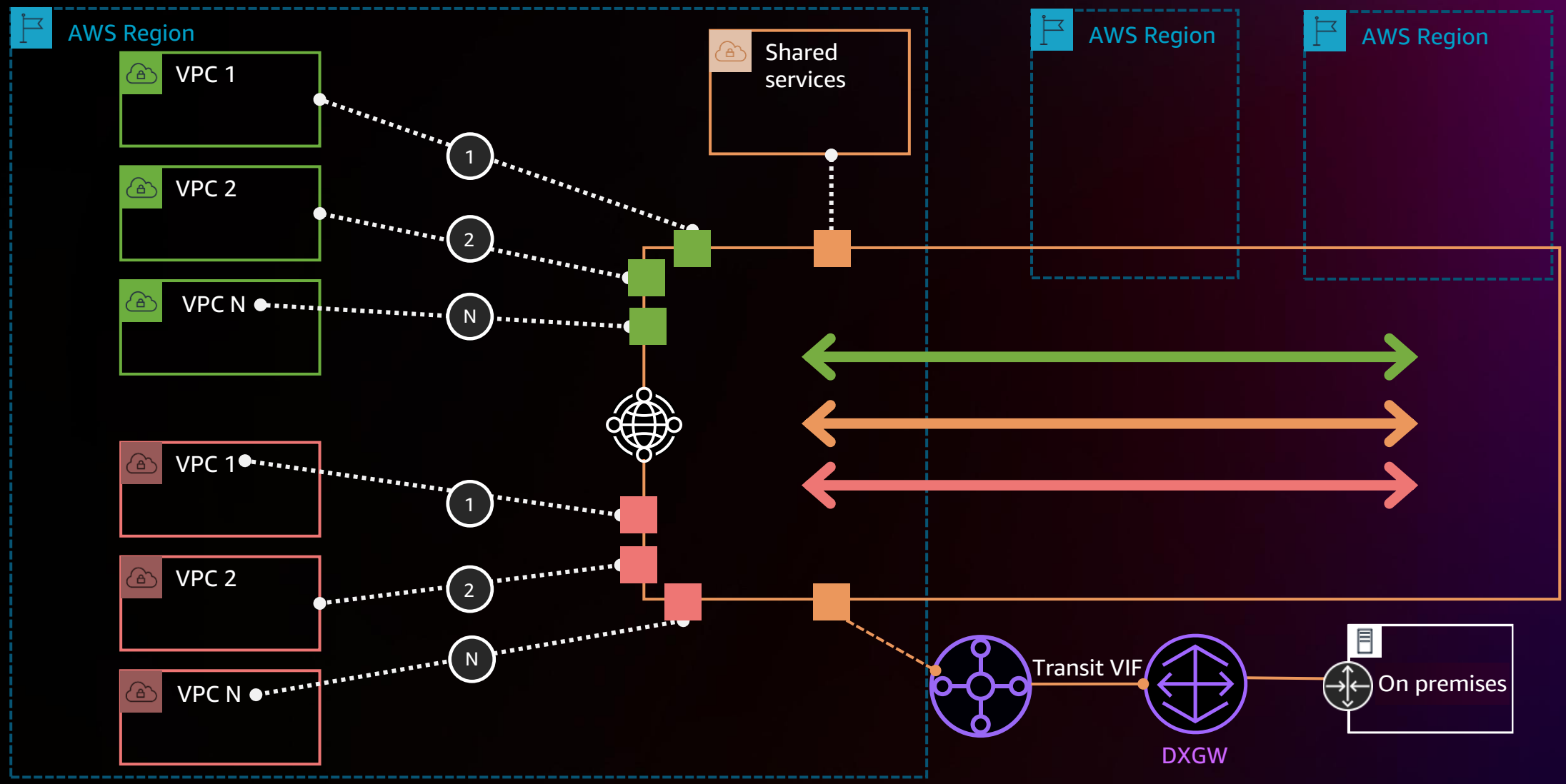
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Global Network: Remember this slide?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Global Network: Now with AWS Cloud WAN



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Cloud WAN



https://go.aws/3rqedL4

AWS Cloud WAN

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Real world solution

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network

us-west-1

us-east-1

ap-southeast-1

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network

us-west-1



us-east-1



ap-southeast-1

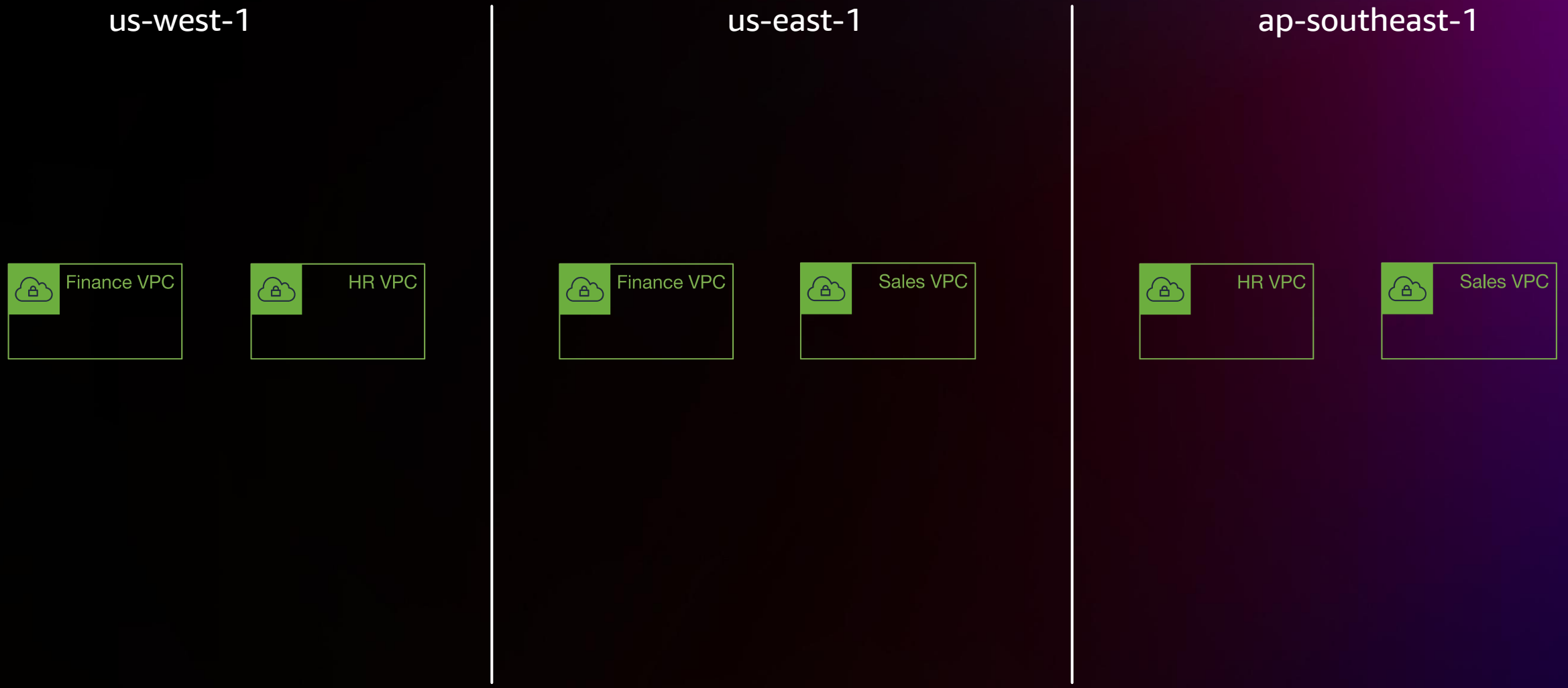
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



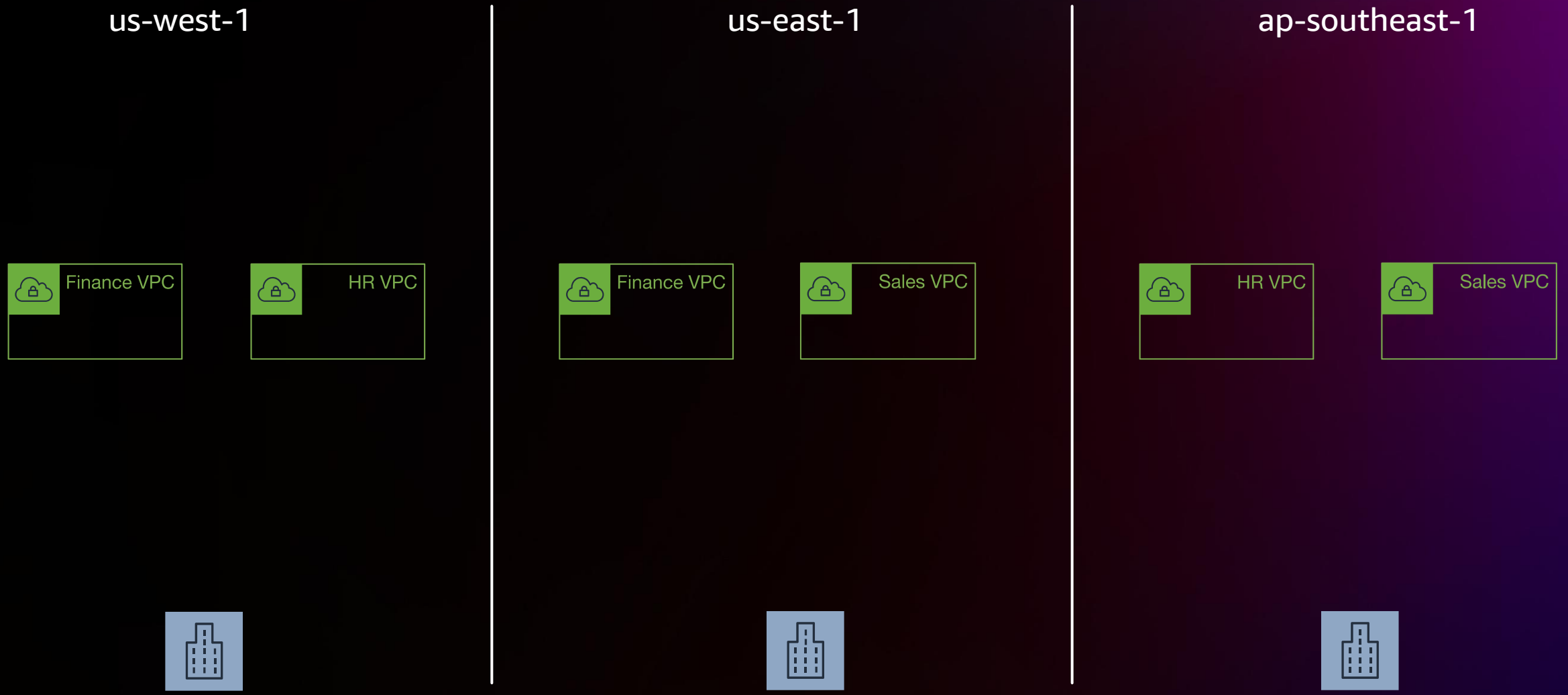
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



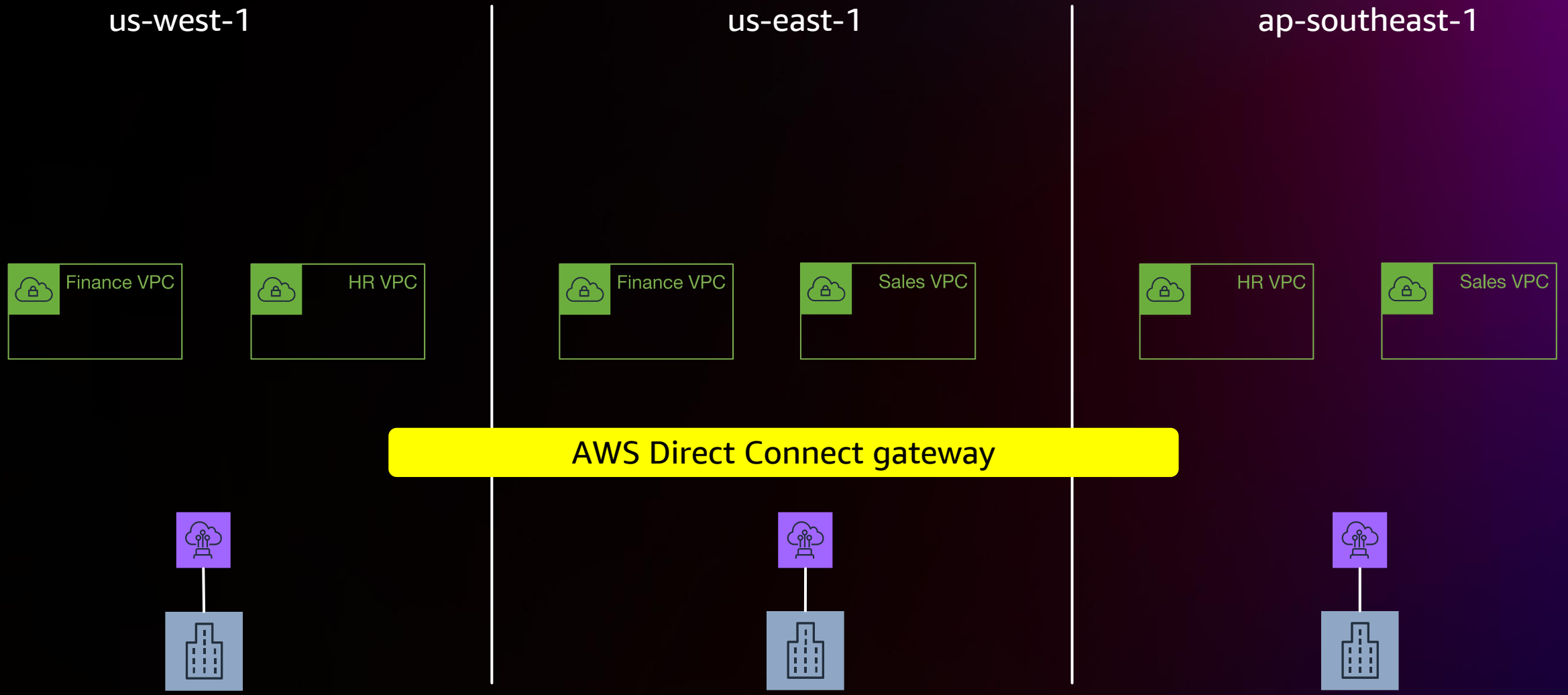
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



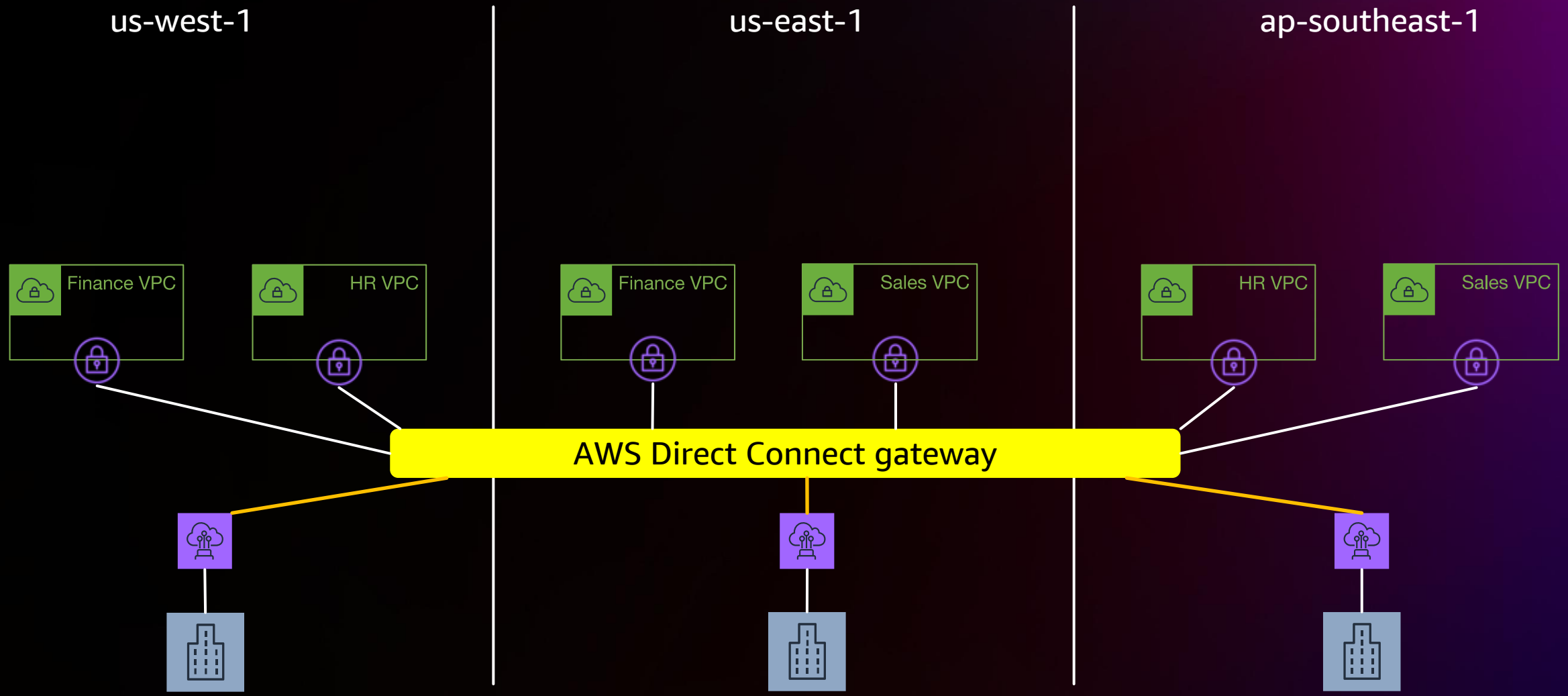
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



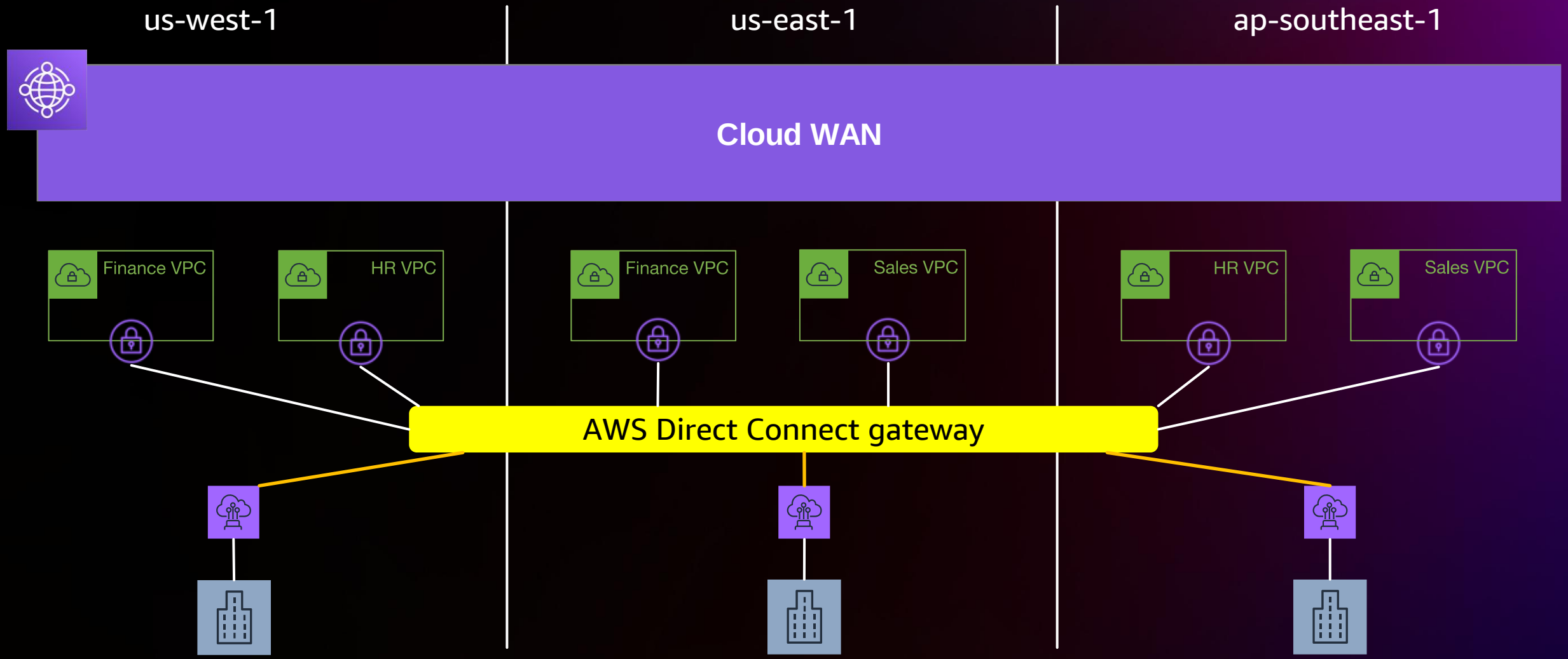
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



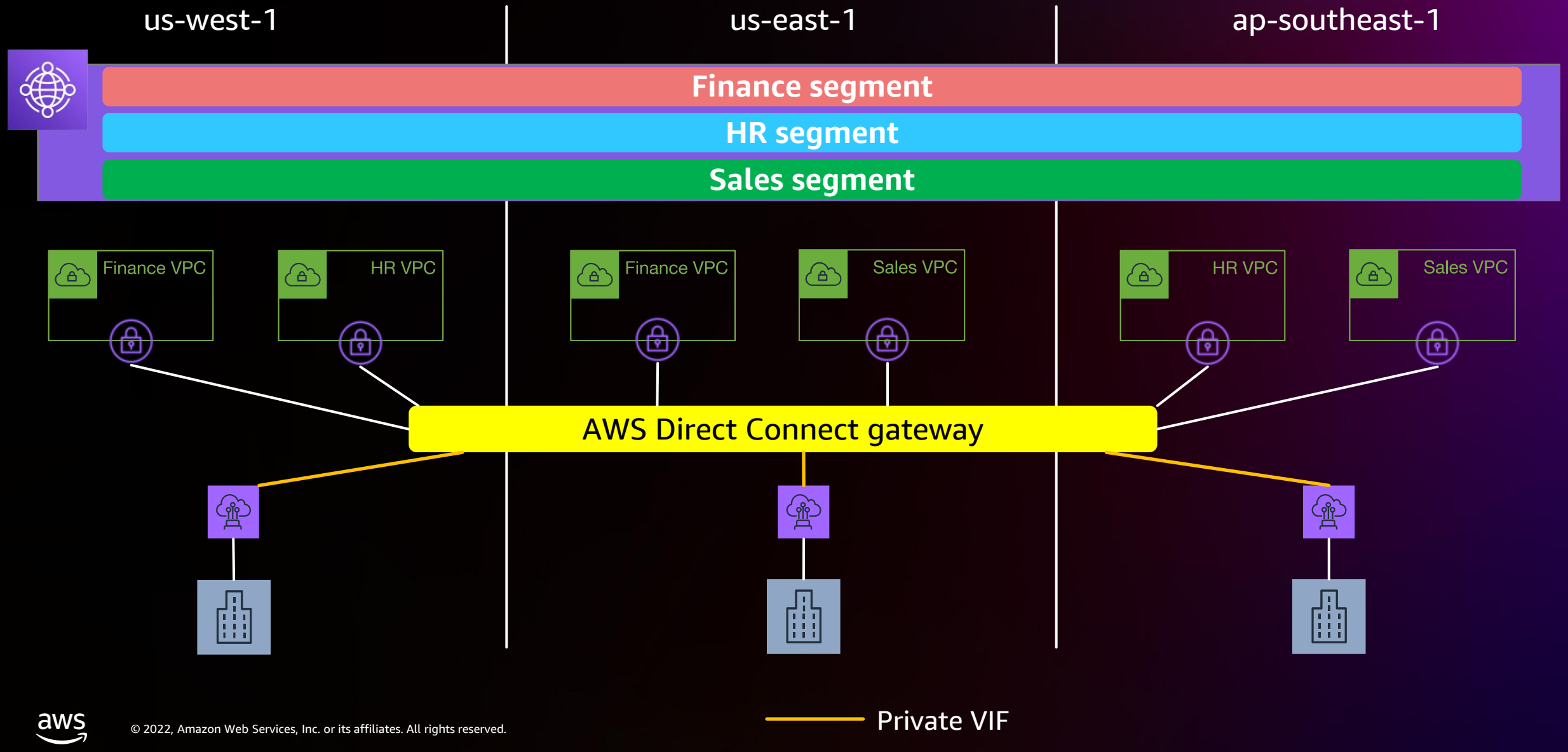
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



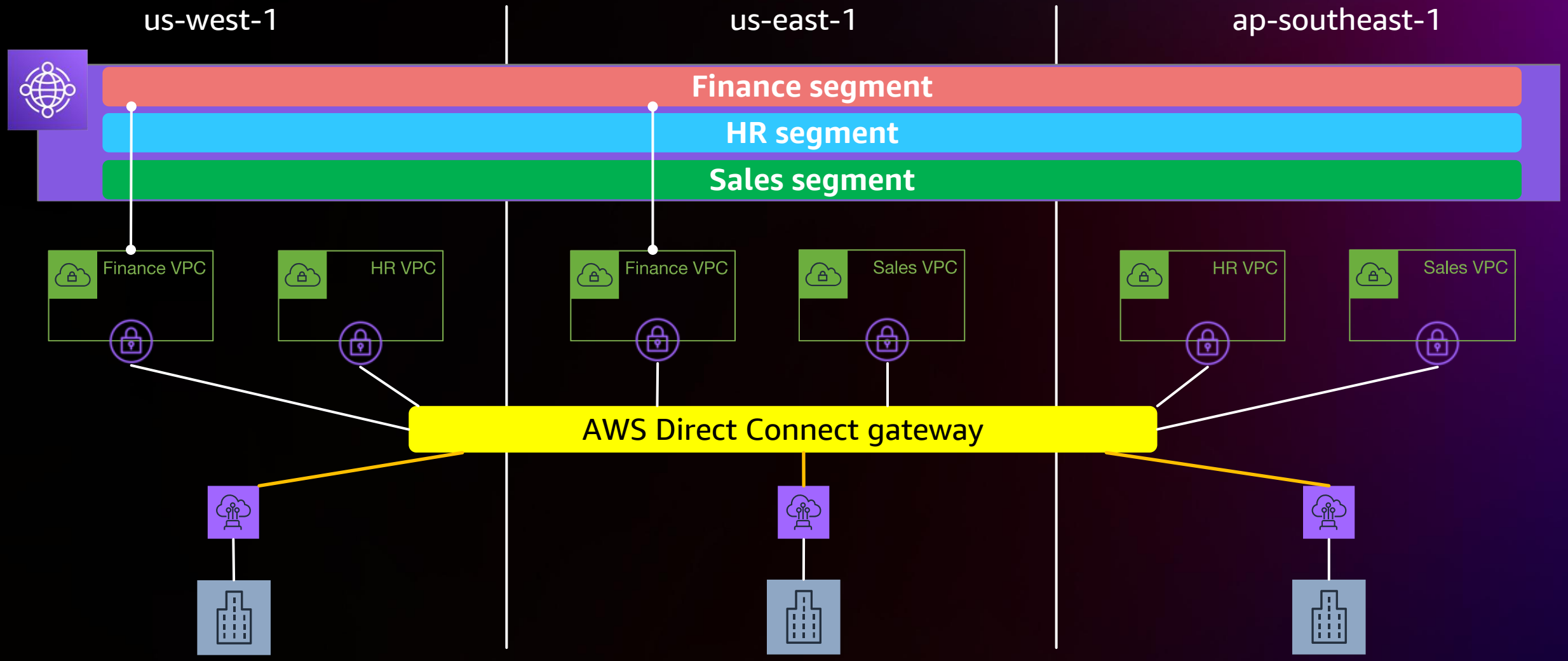
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



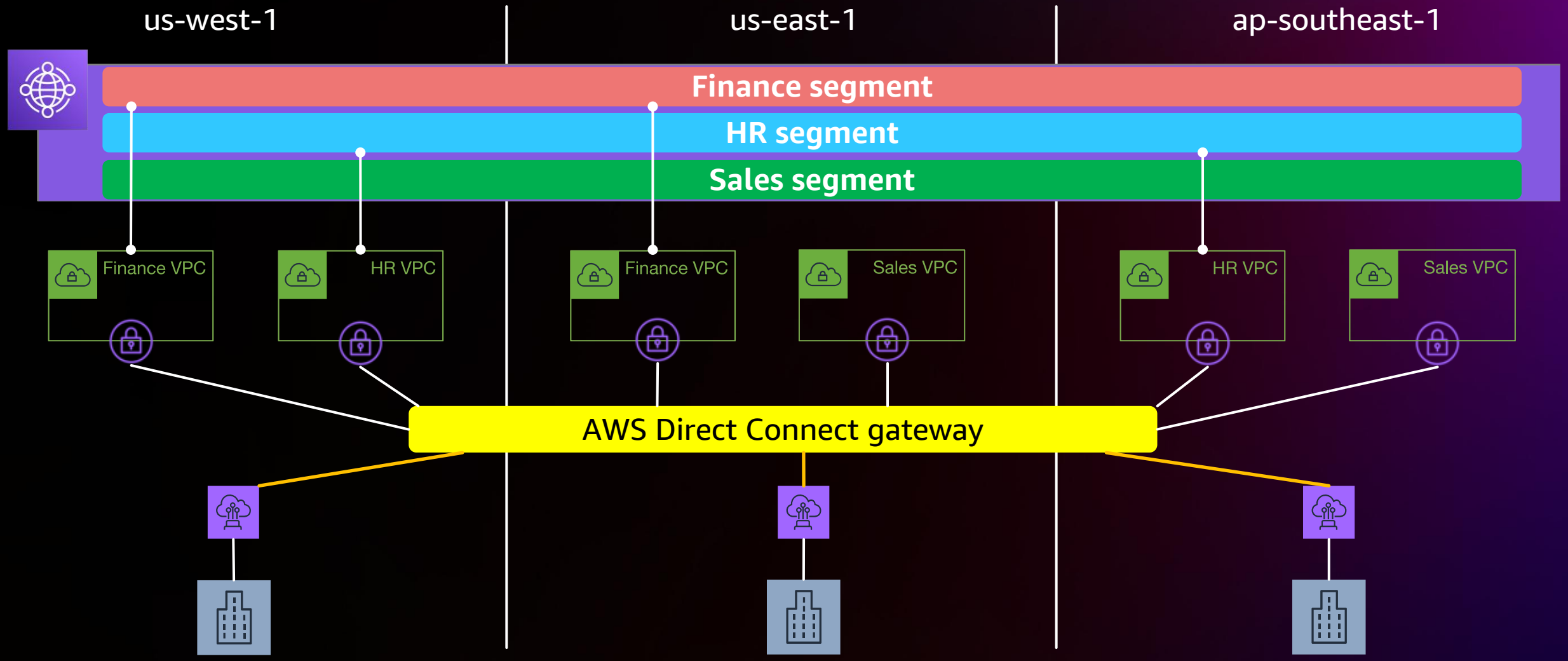
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



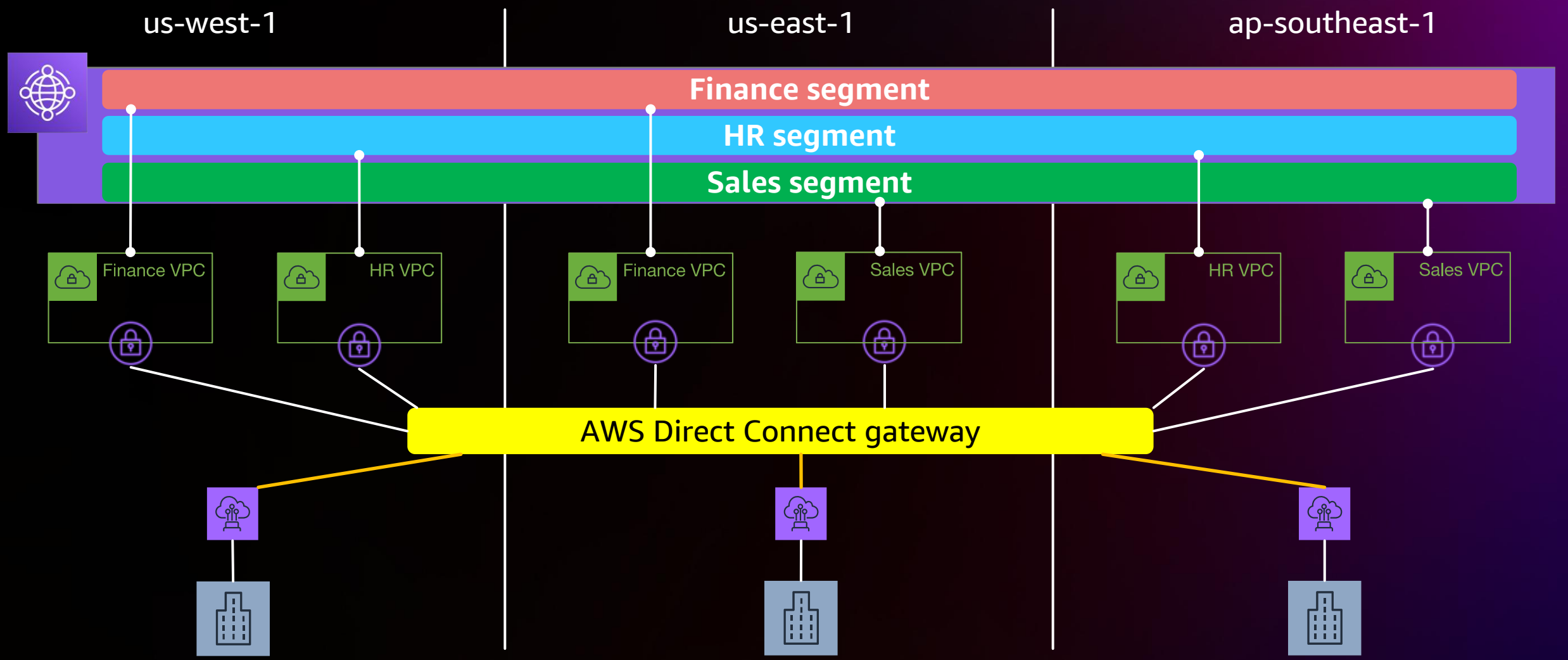
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global network



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Private VIF
Cloud WAN VPC Attachment

But what about routing?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Routing requirements

- Private connectivity only

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Routing requirements

- Private connectivity only
- Intra-department communication

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Routing requirements

- Private connectivity only
- Intra-department communication
- On-premises data centers: 10.0.0.0/8

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

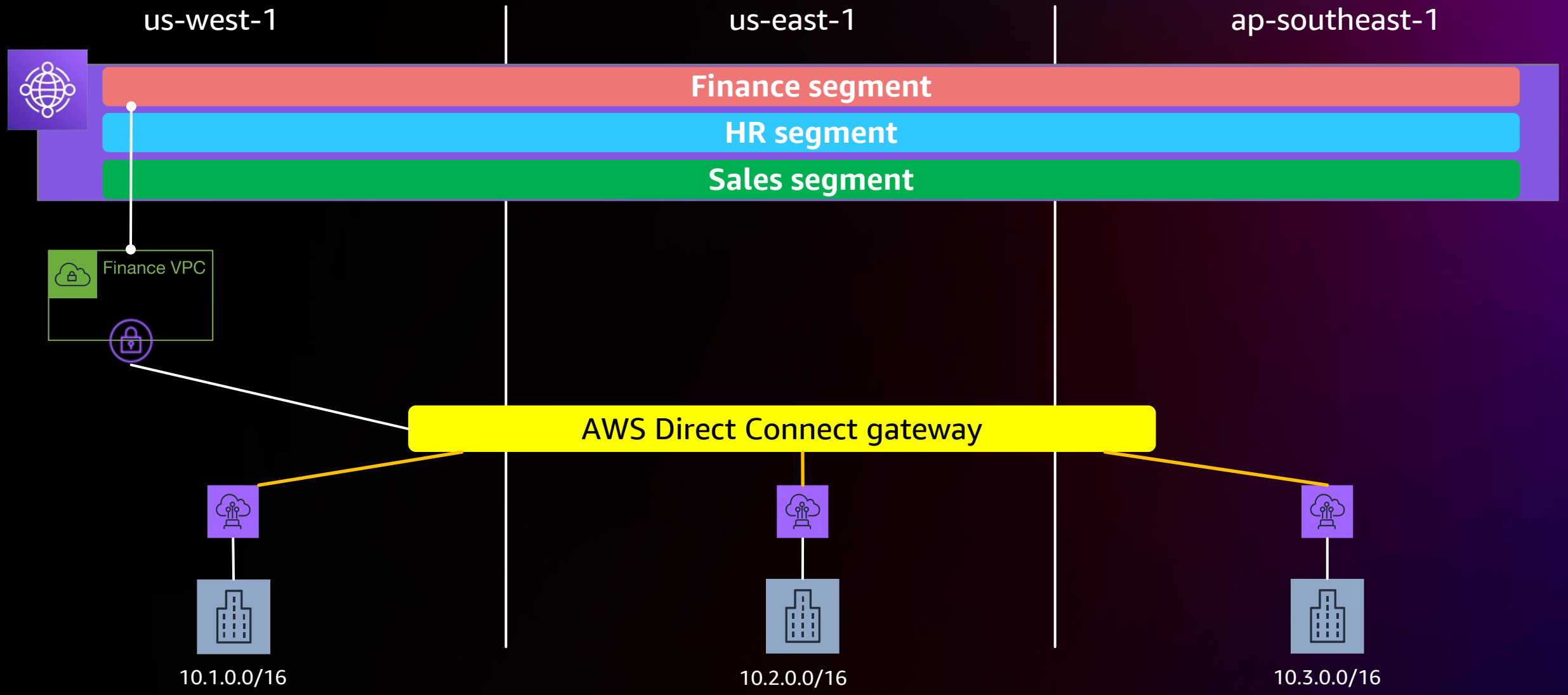
Routing requirements

- Private connectivity only
- Intra-department communication
- On-premises data centers: 10.0.0.0/8
- Department specific CIDRs:

Department	CIDR
Finance	172.16.0.0/16
HR	172.17.0.0/16
Sales	172.18.0.0/16

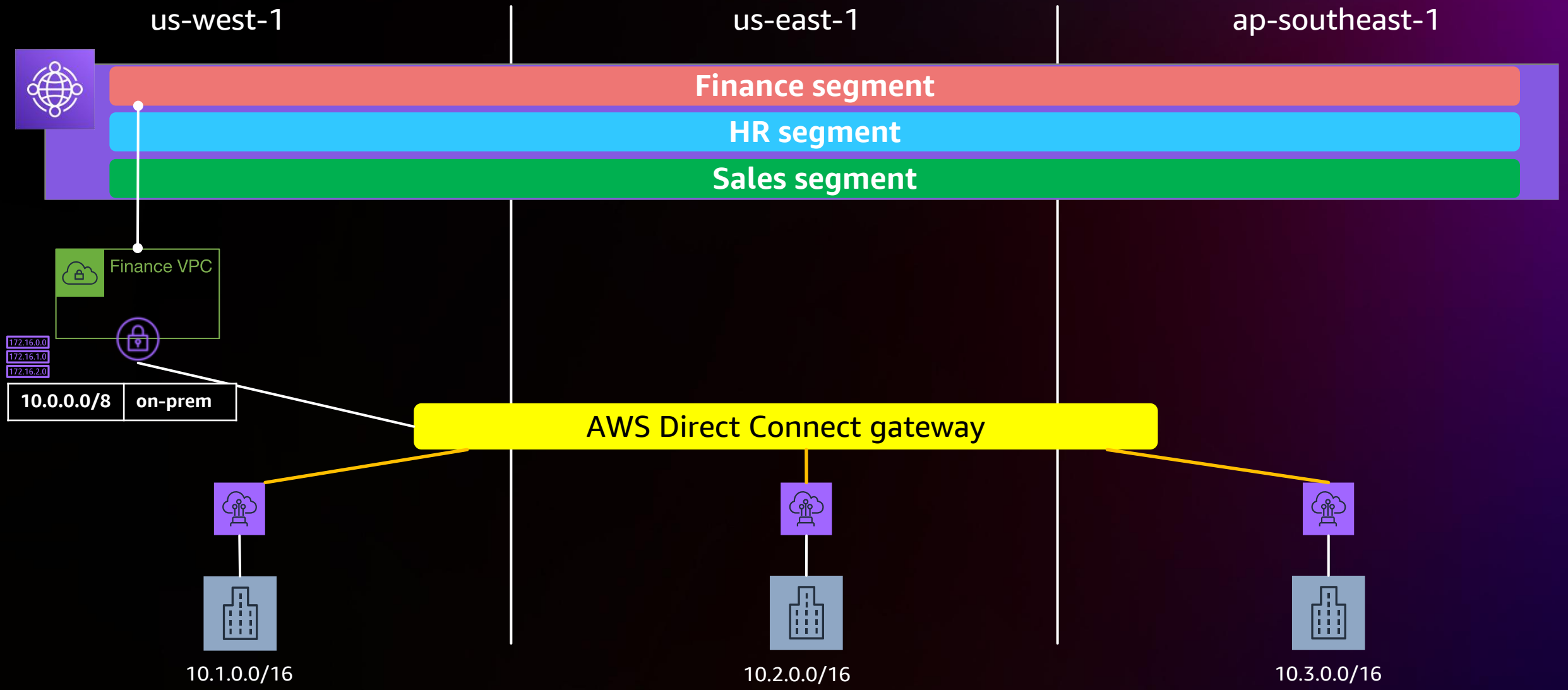
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing



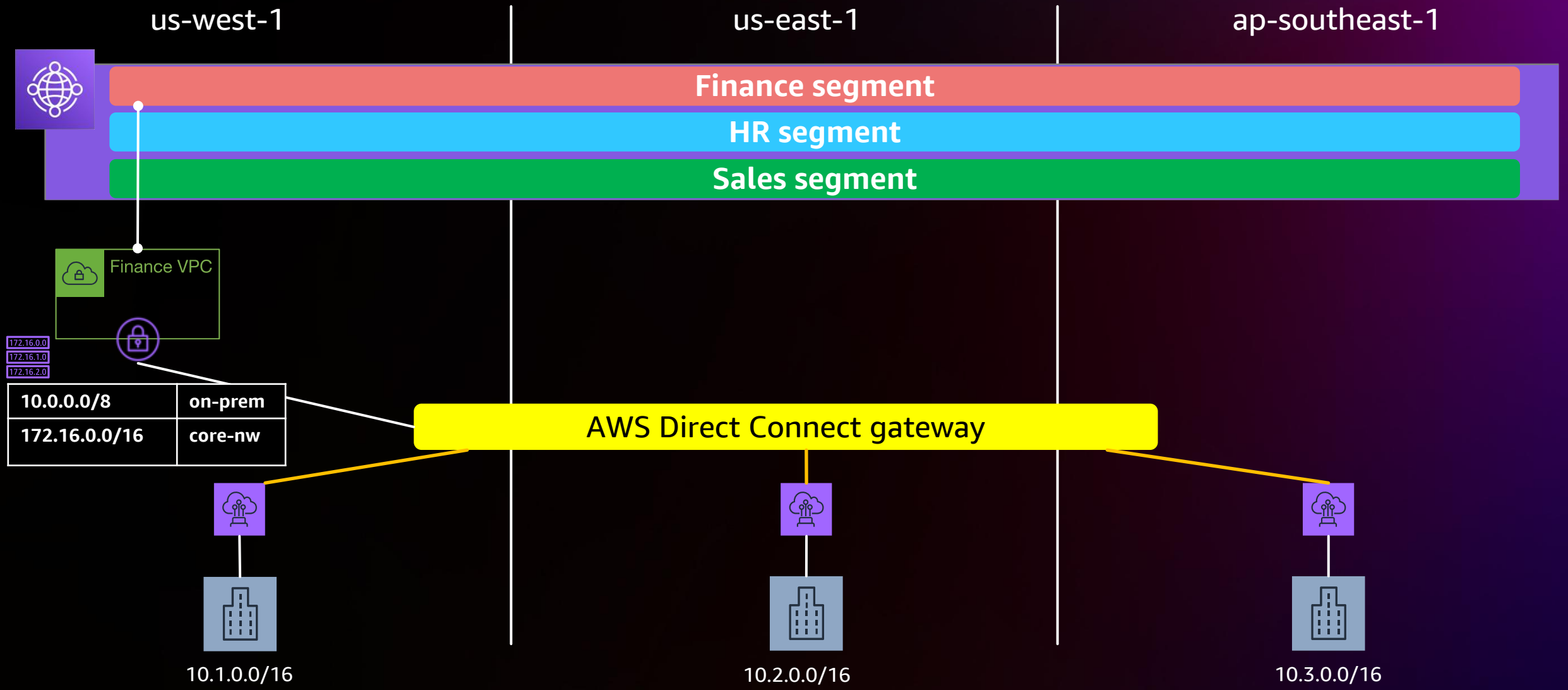
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing



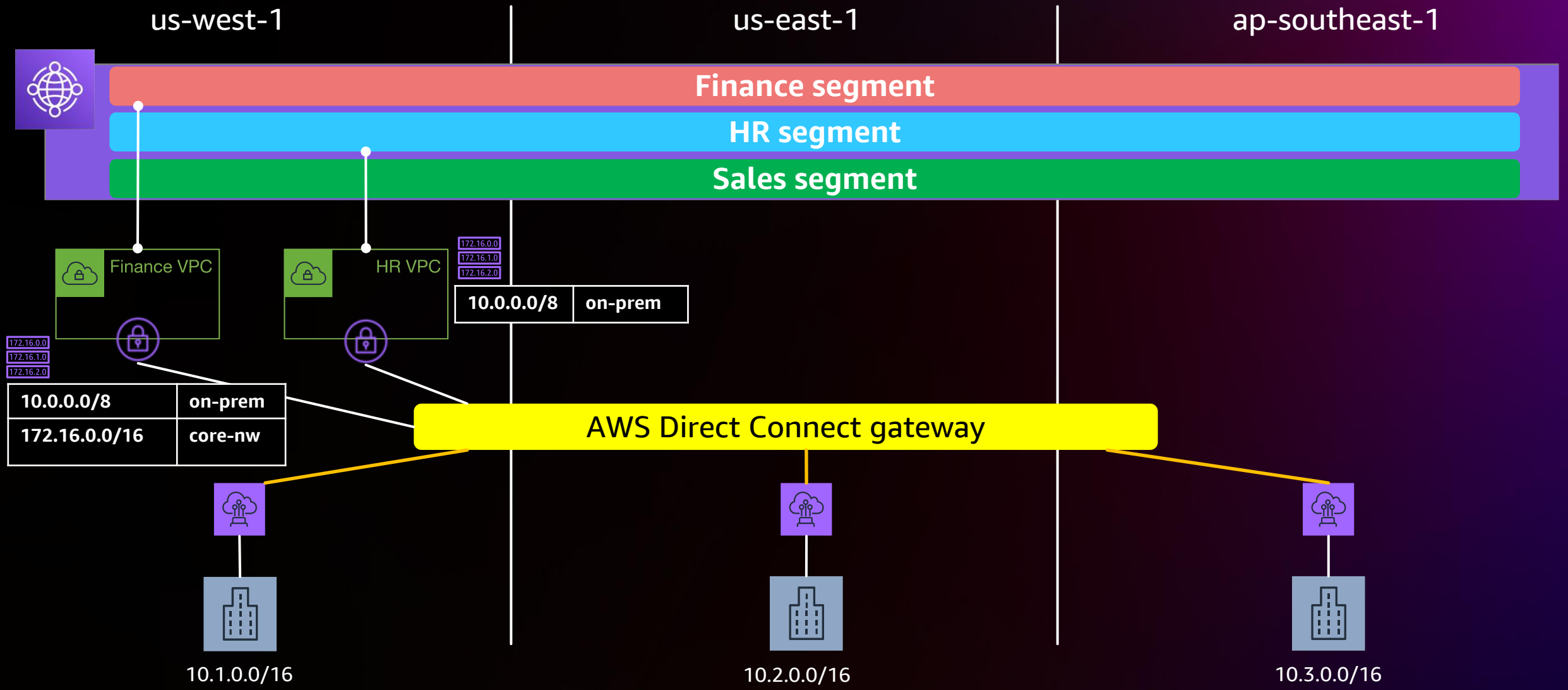
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing



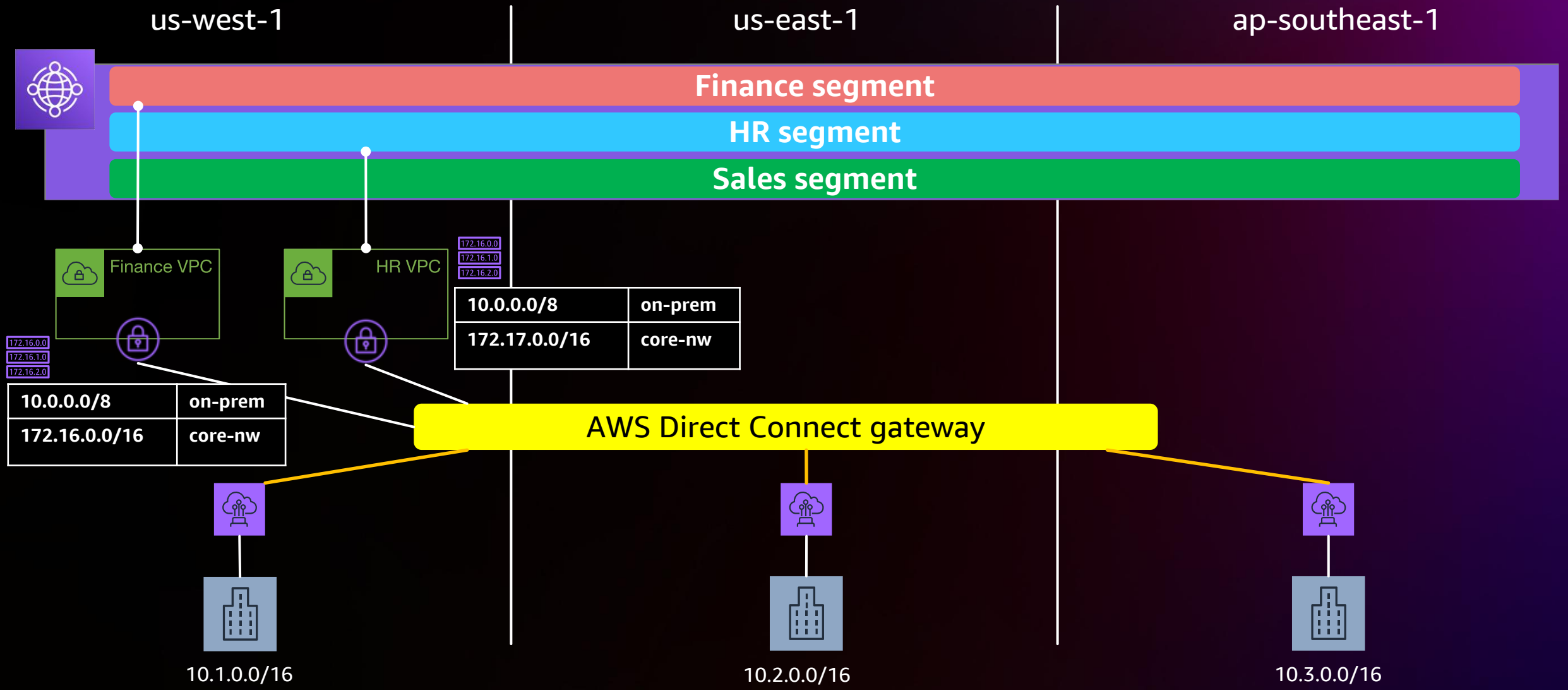
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing



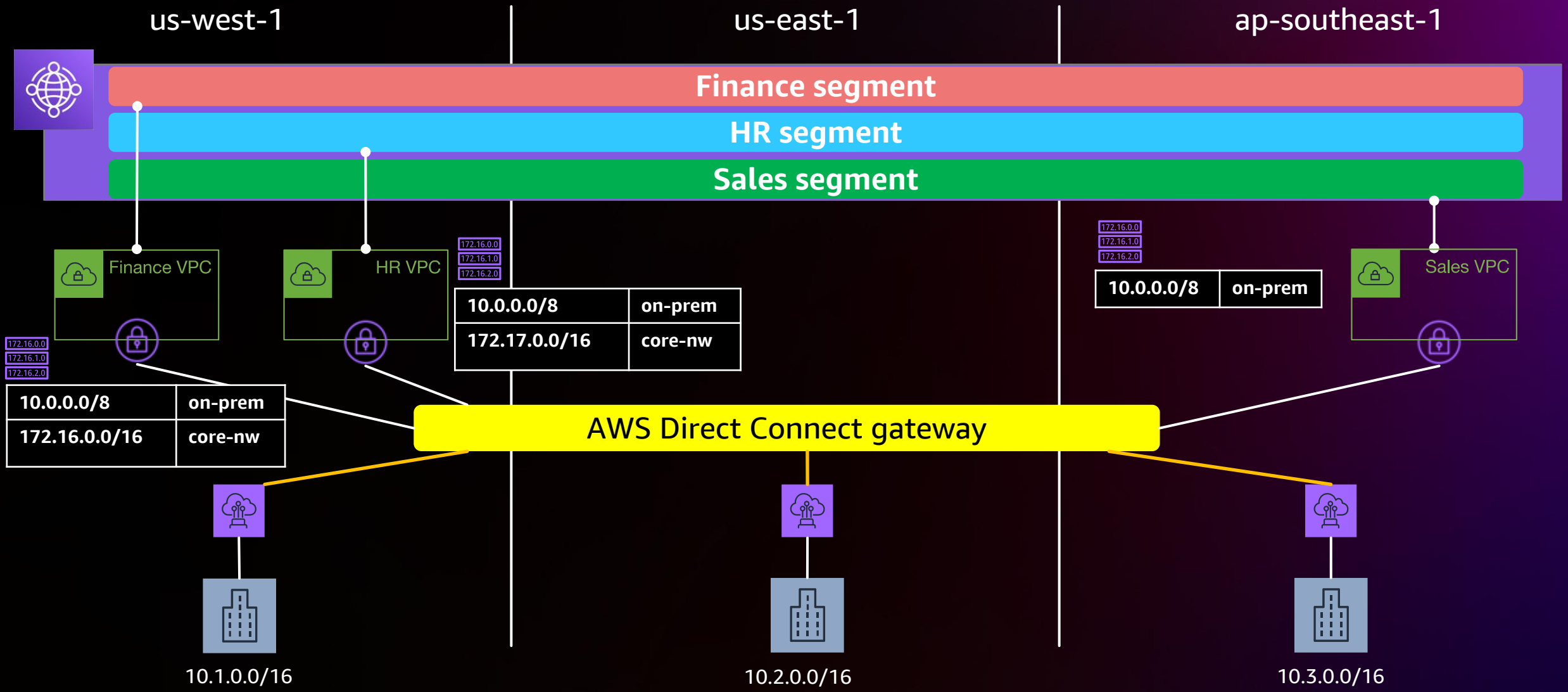
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing



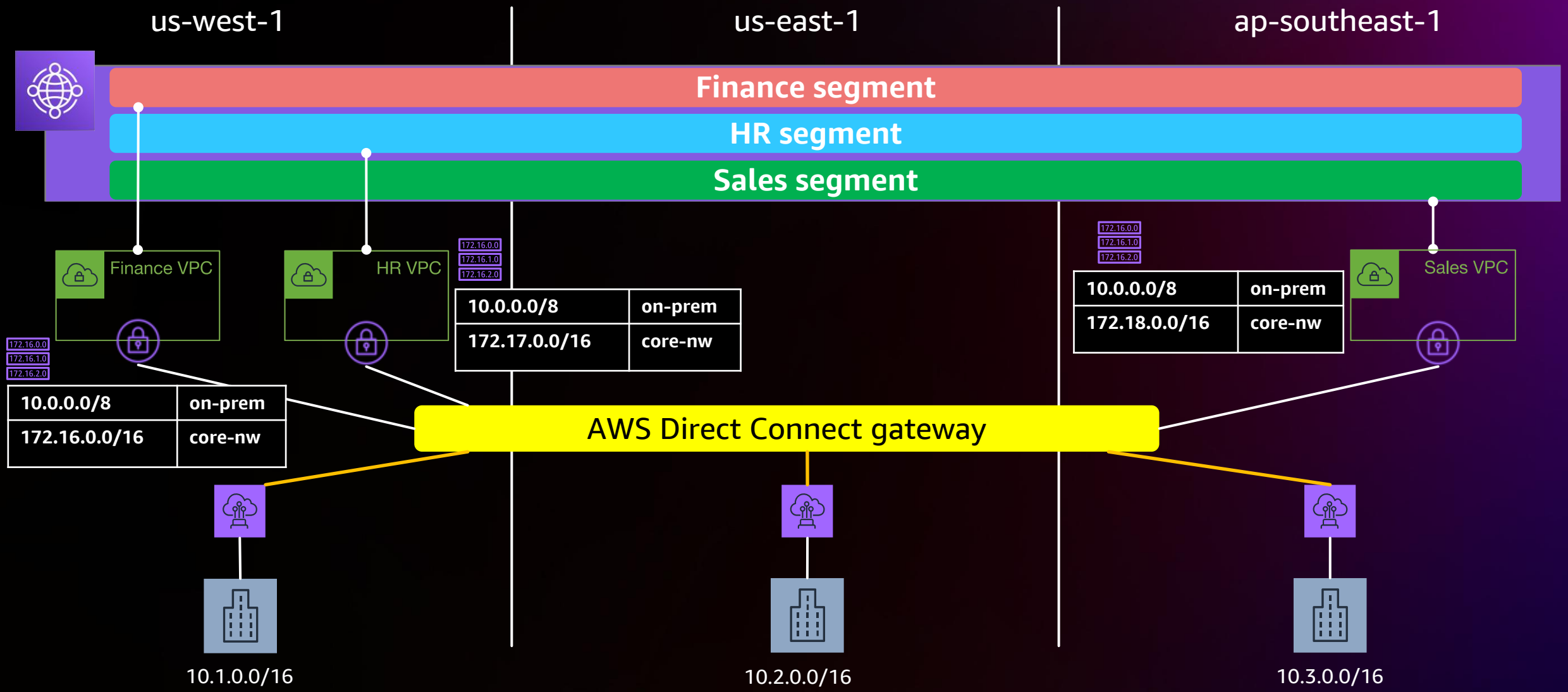
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing

Considerations

- Where to store department CIDRs?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing

Considerations

- Where to store department CIDRs?

Solutions

- Use VPC IPAM to store CIDRs

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing

Considerations

- Where to store department CIDRs?
- Dynamically update the VPC routing table with the **RIGHT** CIDR

Solutions

- Use VPC IPAM to store CIDRs

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing

Considerations

- Where to store department CIDRs?
- Dynamically update the VPC routing table with the **RIGHT** CIDR

Solutions

- Use VPC IPAM to store CIDRs
- Event-driven solution for dynamic routing

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing

Considerations

- Where to store department CIDRs?
- Dynamically update the VPC routing table with the **RIGHT** CIDR

Solutions

- Use VPC IPAM to store CIDRs
- Event-driven solution for dynamic routing
  - Amazon EventBridge: Serverless event bus service

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC routing

Considerations

- Where to store department CIDRs?
- Dynamically update the VPC routing table with the **RIGHT** CIDR

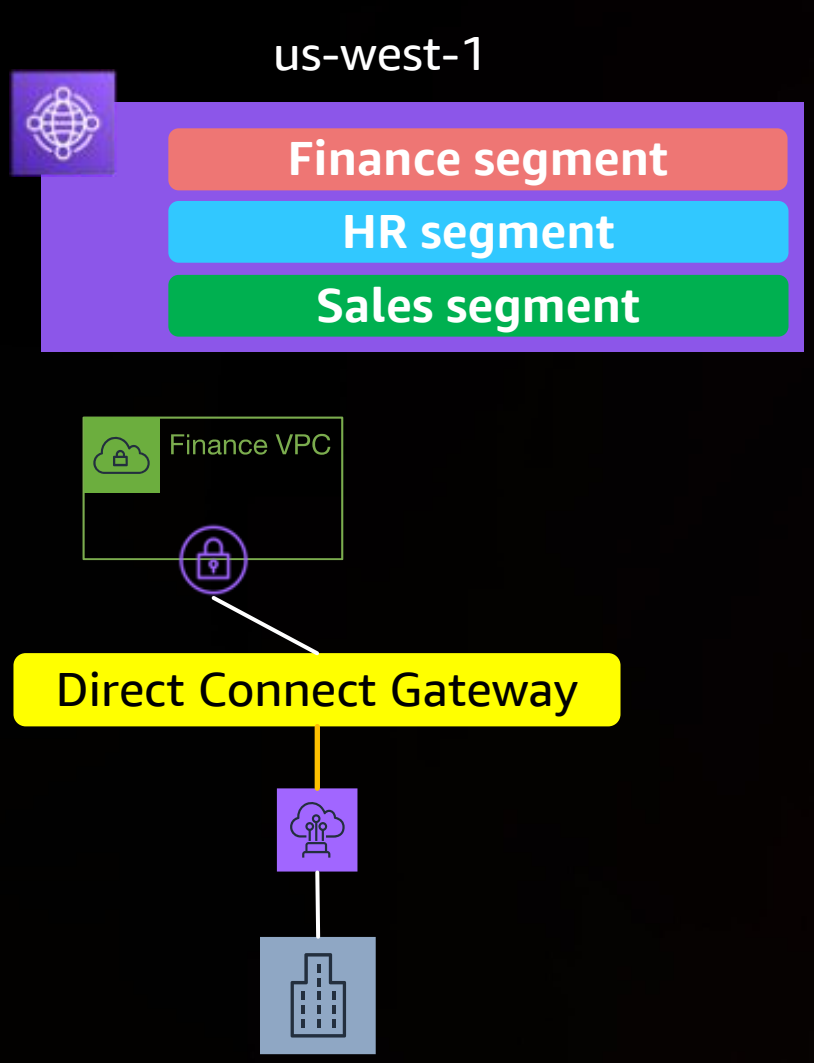
Solutions

- Use VPC IPAM to store CIDRs
- Event-driven solution for dynamic routing
  - Amazon EventBridge: Serverless event bus service
  - AWS Lambda: Serverless compute service

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

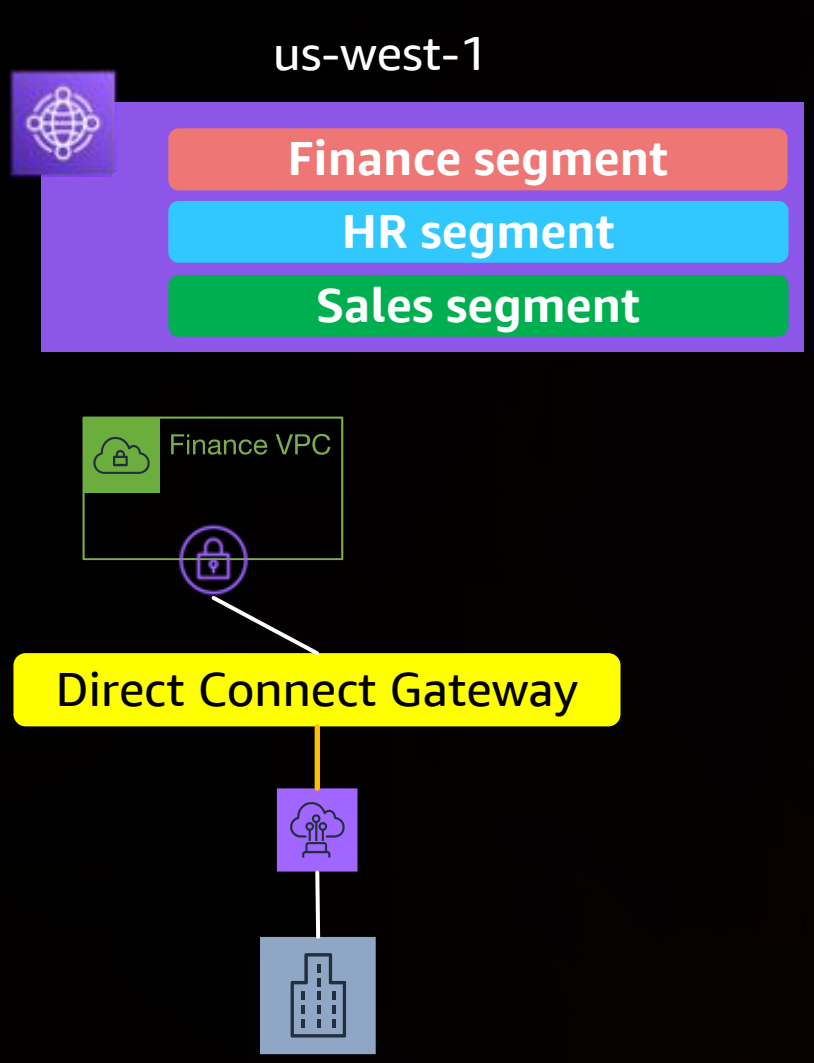
Solution detail – Store CIDRs in IPAM



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

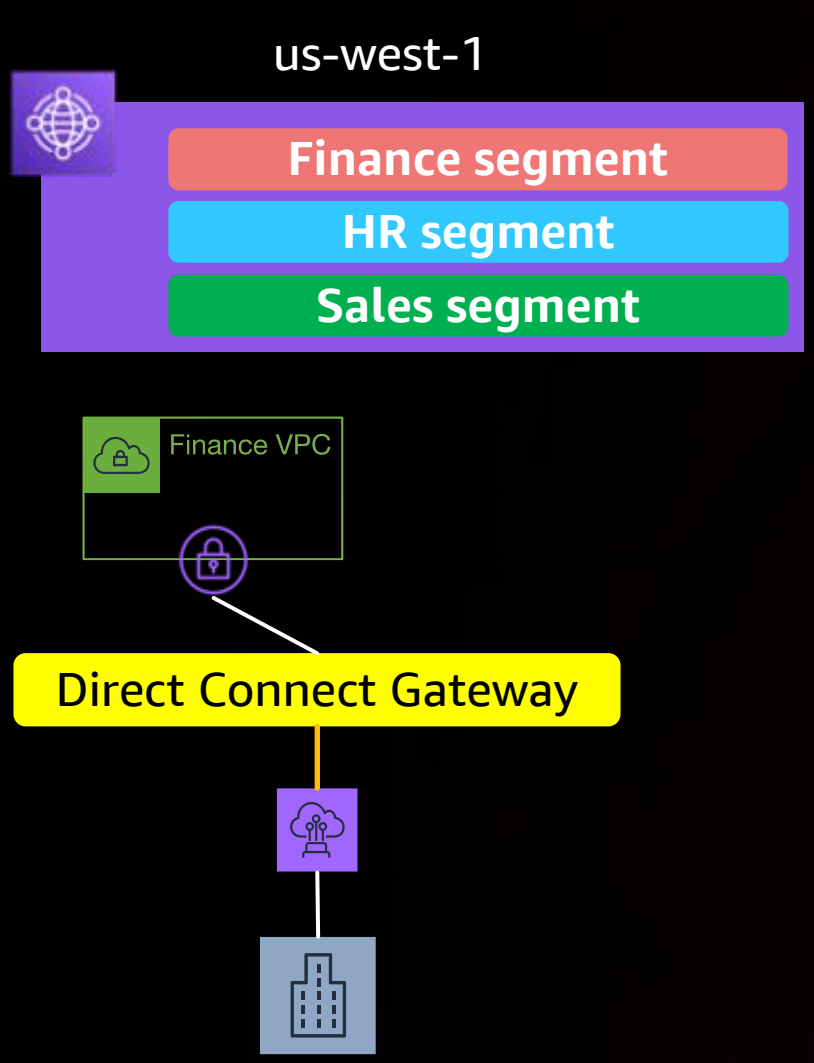
Solution detail – Store CIDRs in IPAM



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

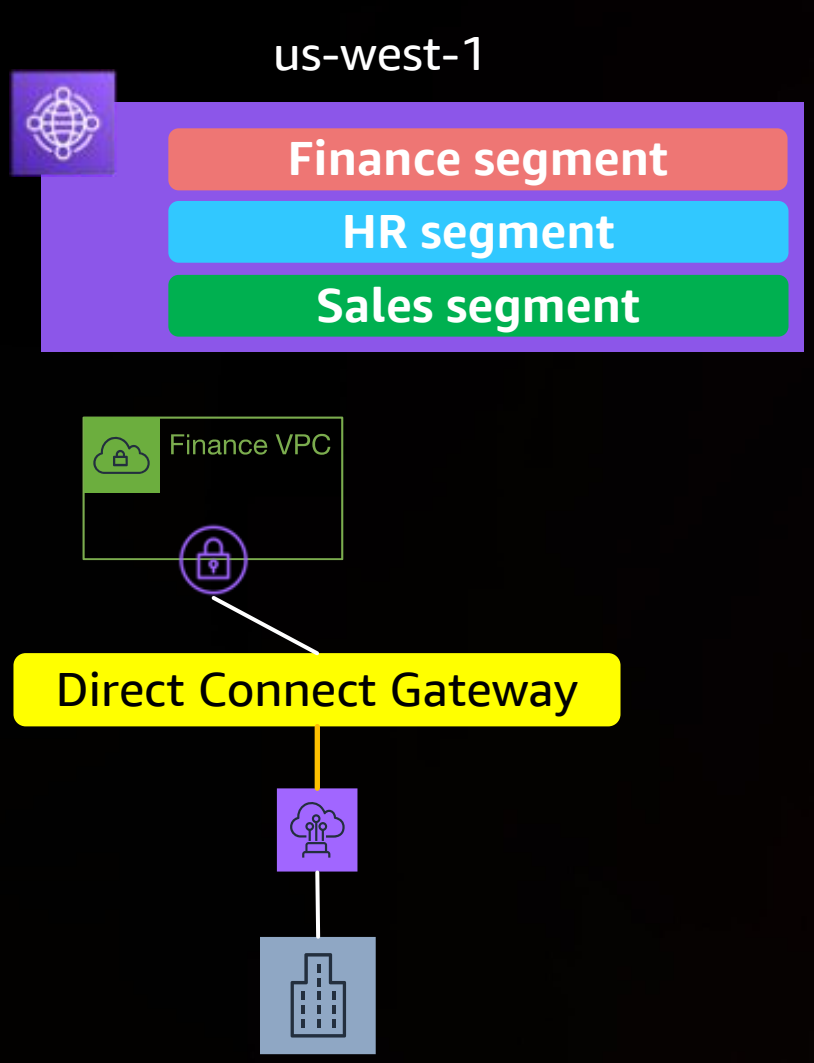
Solution detail – Store CIDRs in IPAM



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution detail – Store CIDRs in IPAM

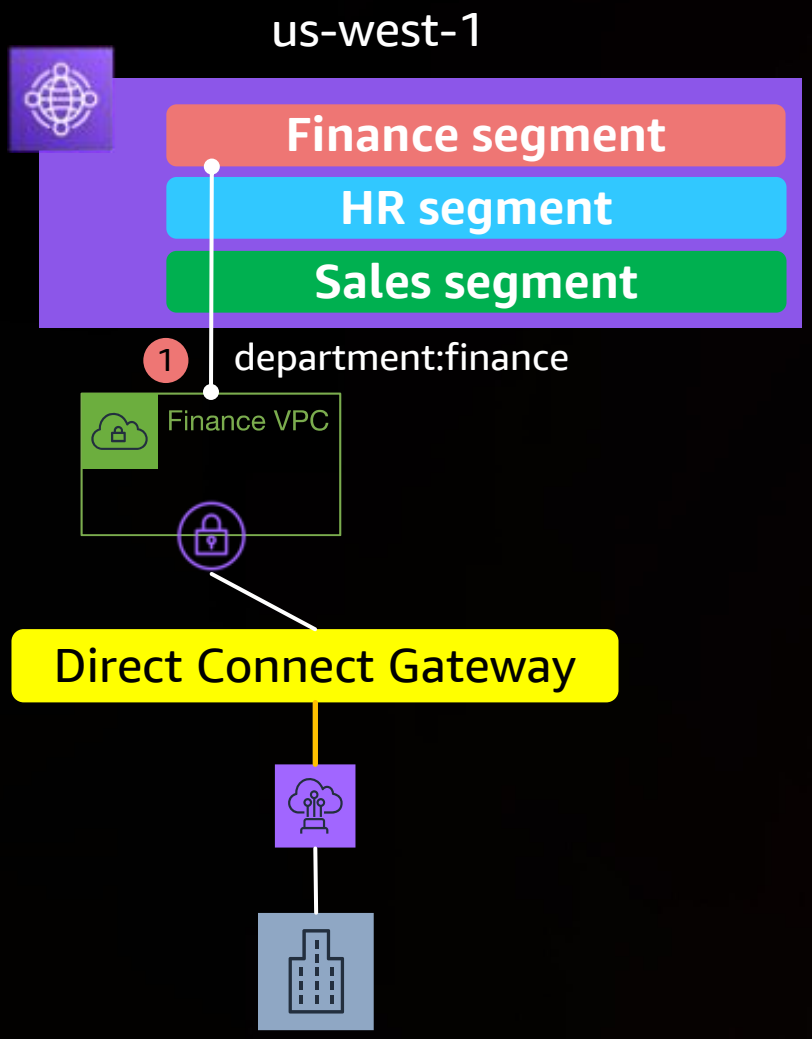


Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

Update VPC routing table with the RIGHT CIDR

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

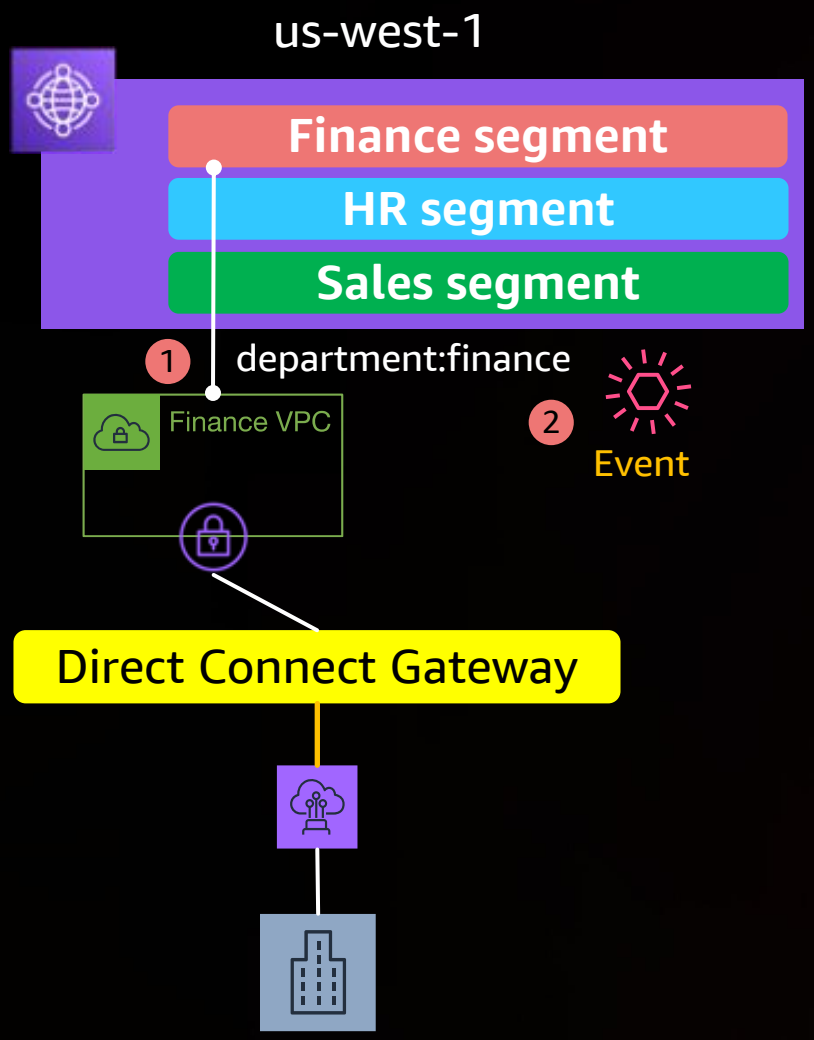
Solution’s workflow



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution’s workflow

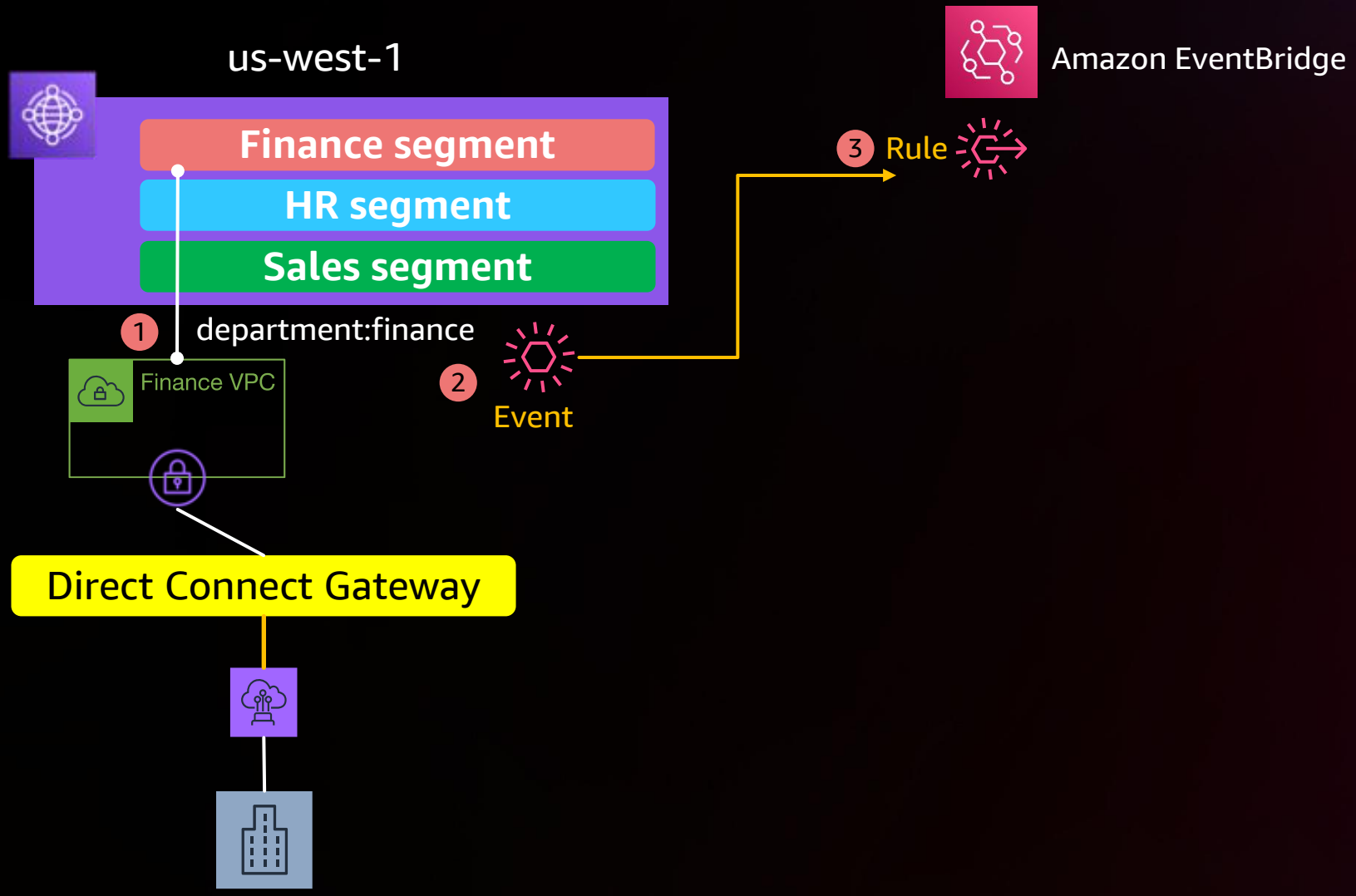


Amazon EventBridge

Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

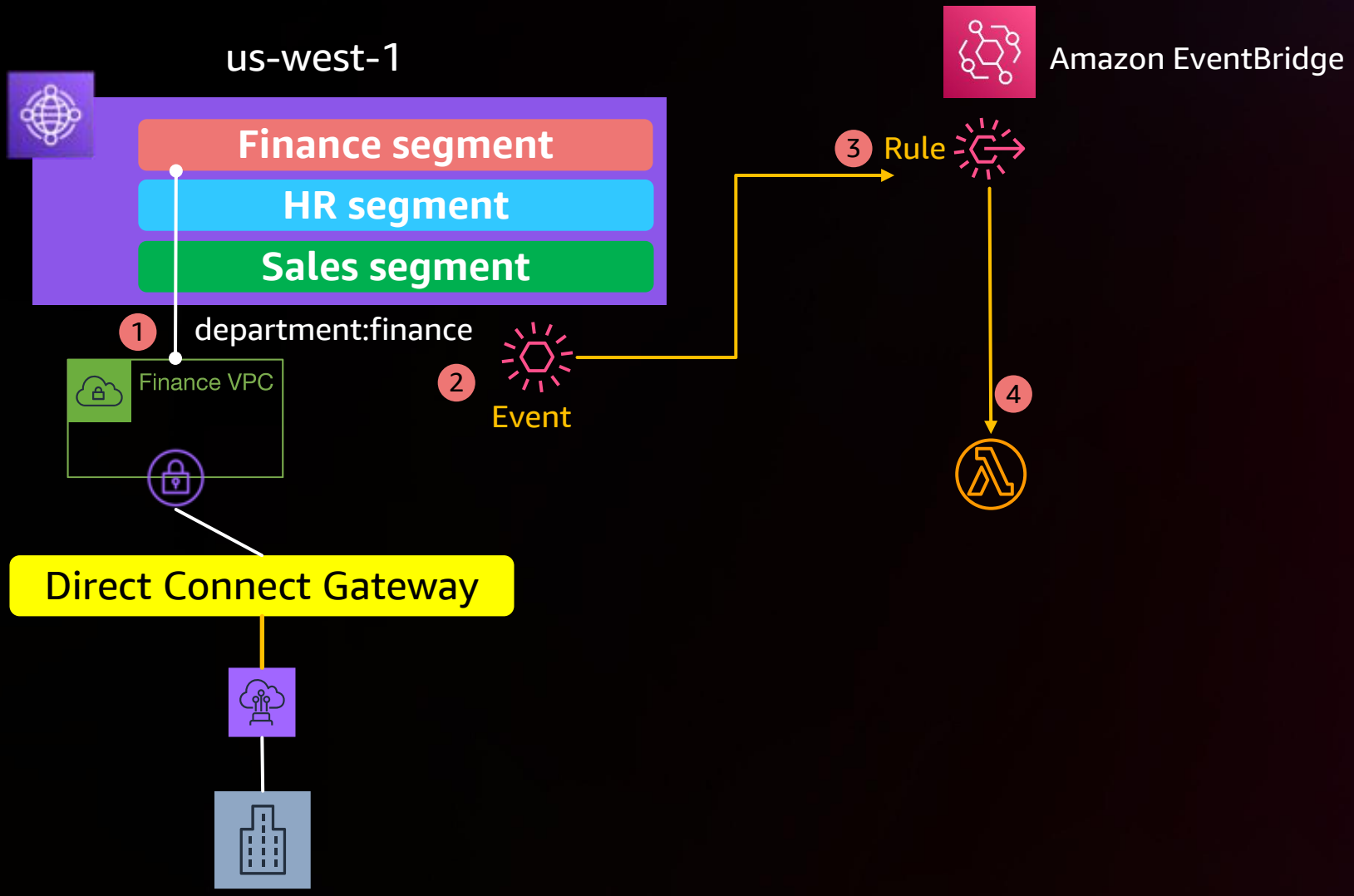
Solution’s workflow



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

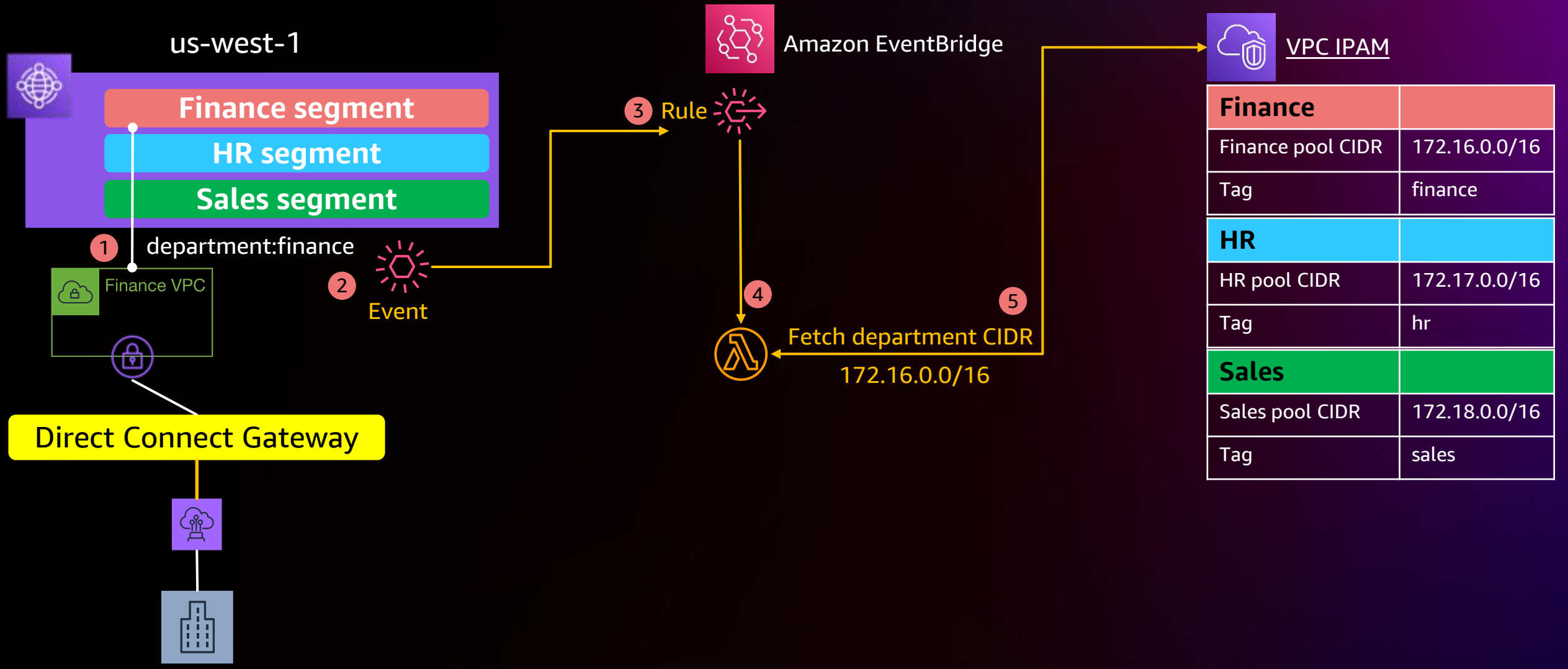
Solution’s workflow



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

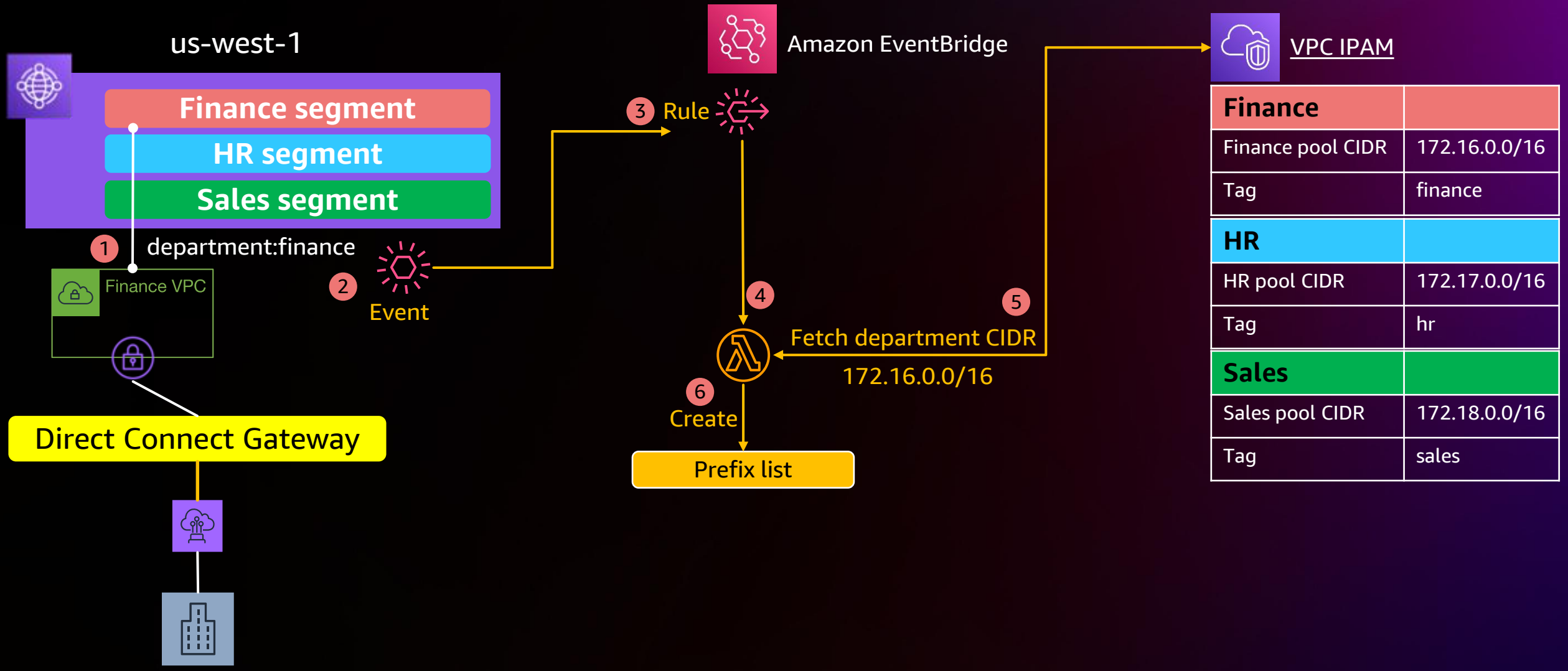
Solution’s workflow



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

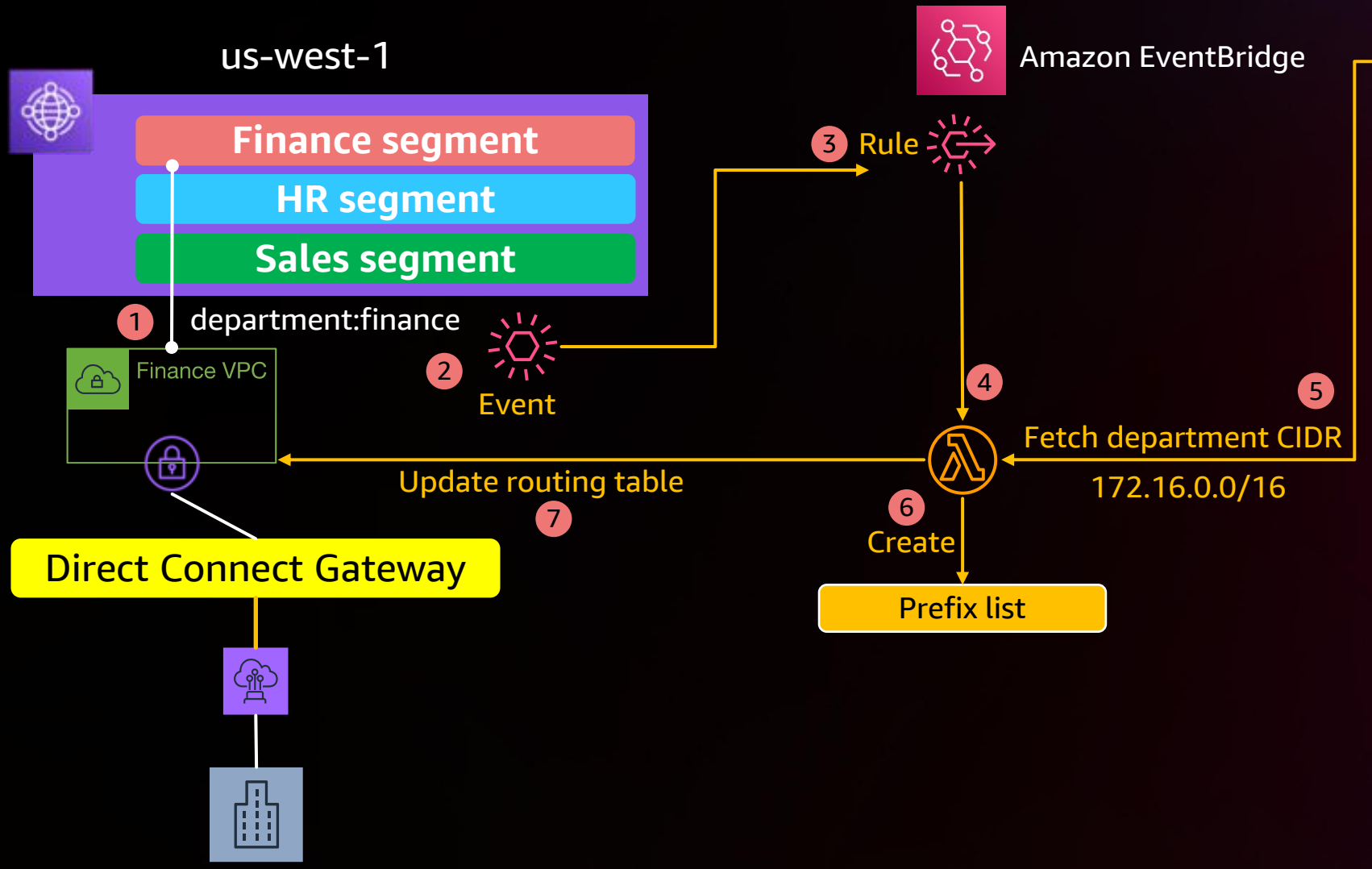
Solution’s workflow



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

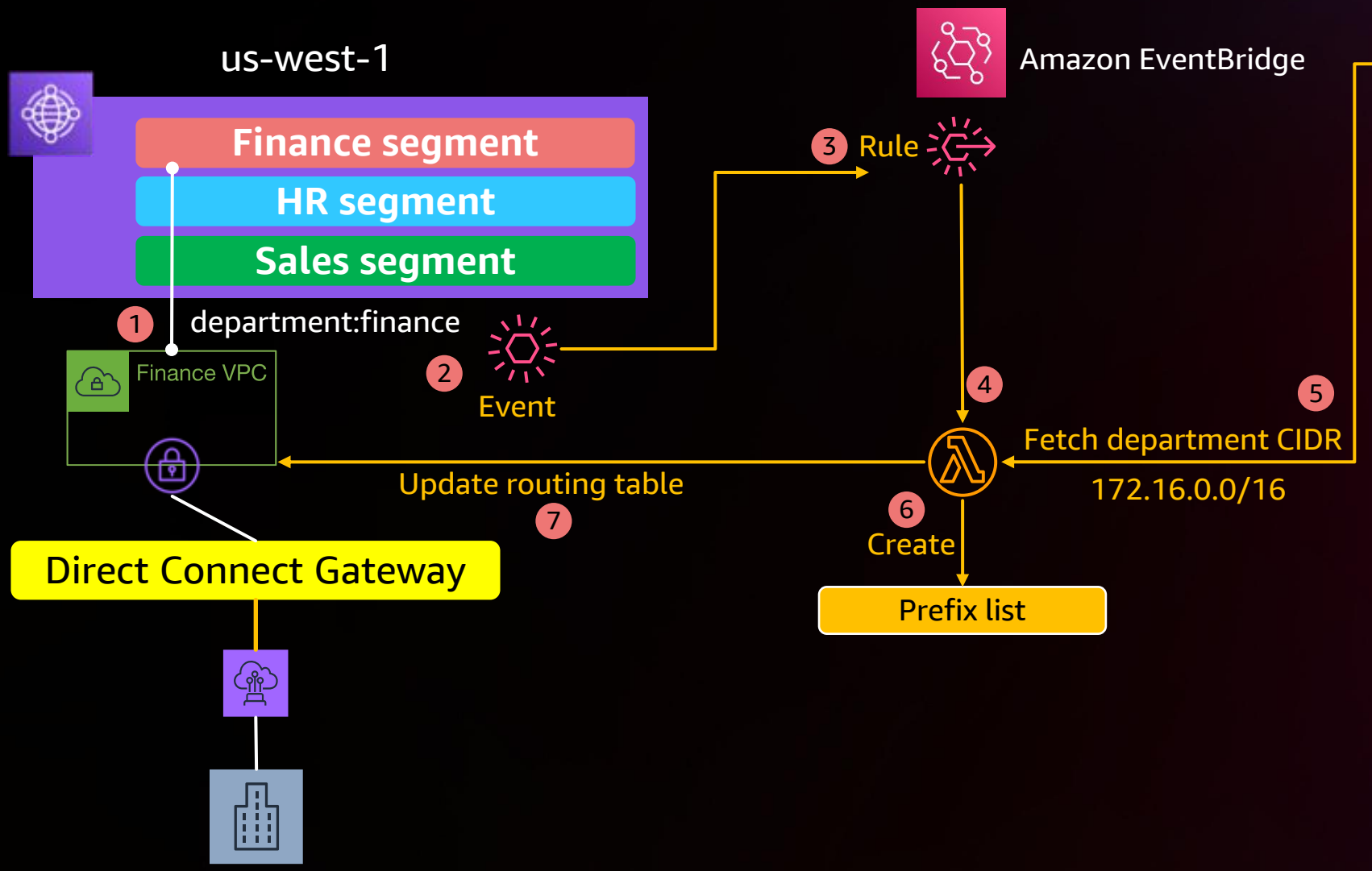
Solution’s workflow



Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution's workflow

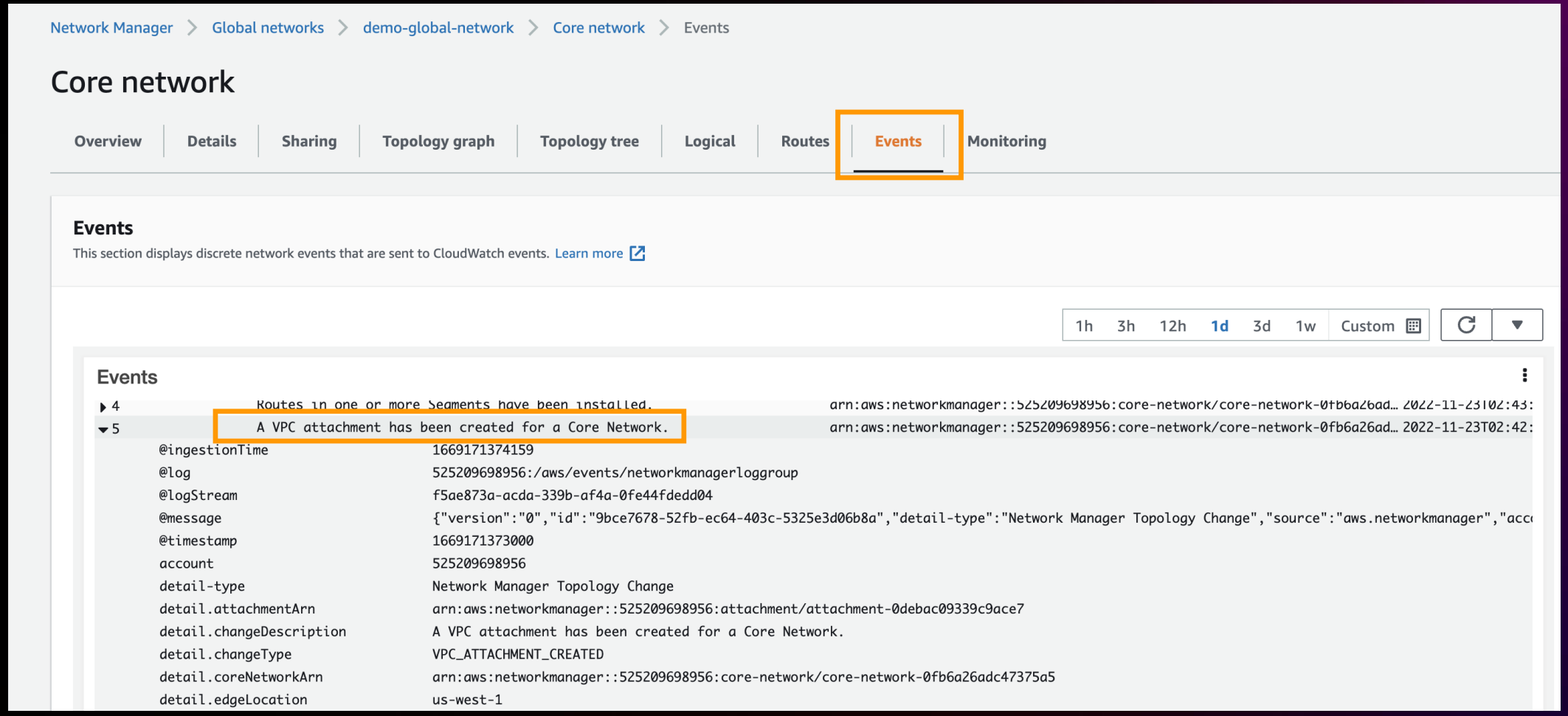


Finance	
Finance pool CIDR	172.16.0.0/16
Tag	finance
HR	
HR pool CIDR	172.17.0.0/16
Tag	hr
Sales	
Sales pool CIDR	172.18.0.0/16
Tag	sales

Update VPC routing table with the RIGHT CIDR

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution deep dive – Cloud WAN Event



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution deep dive – Cloud WAN Event


```
"source": "aws.networkmanager",
"region": "us-west-2",
"detail-type": "Network Manager Topology Change",
"detail":
 {
  "changeType": "VPC_ATTACHMENT_CREATED”,
  "edgeLocation": "us-west-1",
  "attachmentArn": ““ATTACHMENT-ARN”,
  "vpcArn": ”VPC-ARN",
  "coreNetworkArn": ”Cloud WAN Core Network ARN",
 },
}
```


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution deep dive – EventBridge Rule us-west-2

Event Pattern

```
{
"detail-type": ["Network Manager Topology Change"],
"detail": {
  "changeType": ["VPC_ATTACHMENT_CREATED"],
  "edgeLocation": ["us-west-1"]
  }
}
```

Target

EventBridge bus in us-west-1 (the target region)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution deep dive – EventBridge Rule us-west-1

Event Pattern

```
{
"detail-type": ["Network Manager Topology Change"],
"detail": {
  "changeType": ["VPC_ATTACHMENT_CREATED"],
  "edgeLocation": ["us-west-1"]
  }
}
```

Target

Lambda function within us-west-1

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution deep dive – Lambda function

- Correlate attachment's tag with IPAM pool tag
- Fetch the CIDR
- Create a prefix list
- Add route to VPC routing table

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution – Summary

- Event-driven, end-to-end, fully automated routing
- Integrates AWS Cloud WAN and IPAM
- Provides additional layer of intelligence in routing
- Suited when VPC has multiple exit points

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do I set it up?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Related sessions

- Net303: Build your global wide area network using AWS
- Net309: Deploy global wide area networks using AWS Cloud WAN
- API311: Building next-gen applications with event-driven architectures
- Cloud WAN and TGW interoperability patterns
  - https://go.aws/3XNMkKw
- Multi-region traffic segmentation with Cloud WAN and TGW
  - https://go.aws/3ueLjOa

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Du'An Lightfoot
duanlig@amazon.com
LinkedIn:

Ankit Chadha
aichadha@amazon.com
LinkedIn:



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.